Fehlerbehebung bei DHCP im Nur-Layer-2-VLAN - Wireless

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei DHCP für Wireless-Endgeräte in einem Layer-2 Only-Netzwerk in einer SD-Access (SDA)-Struktur 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
- Fabric-fähiges Wireless

Hardware- und Softwareanforderungen

- Catalyst Switches der Serie 9000
- Catalyst Center Version 2.3.7.9
- Catalyst Wireless LAN Controller der Serie 9800
- Catalyst Access Points der Serie 9100
- 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.

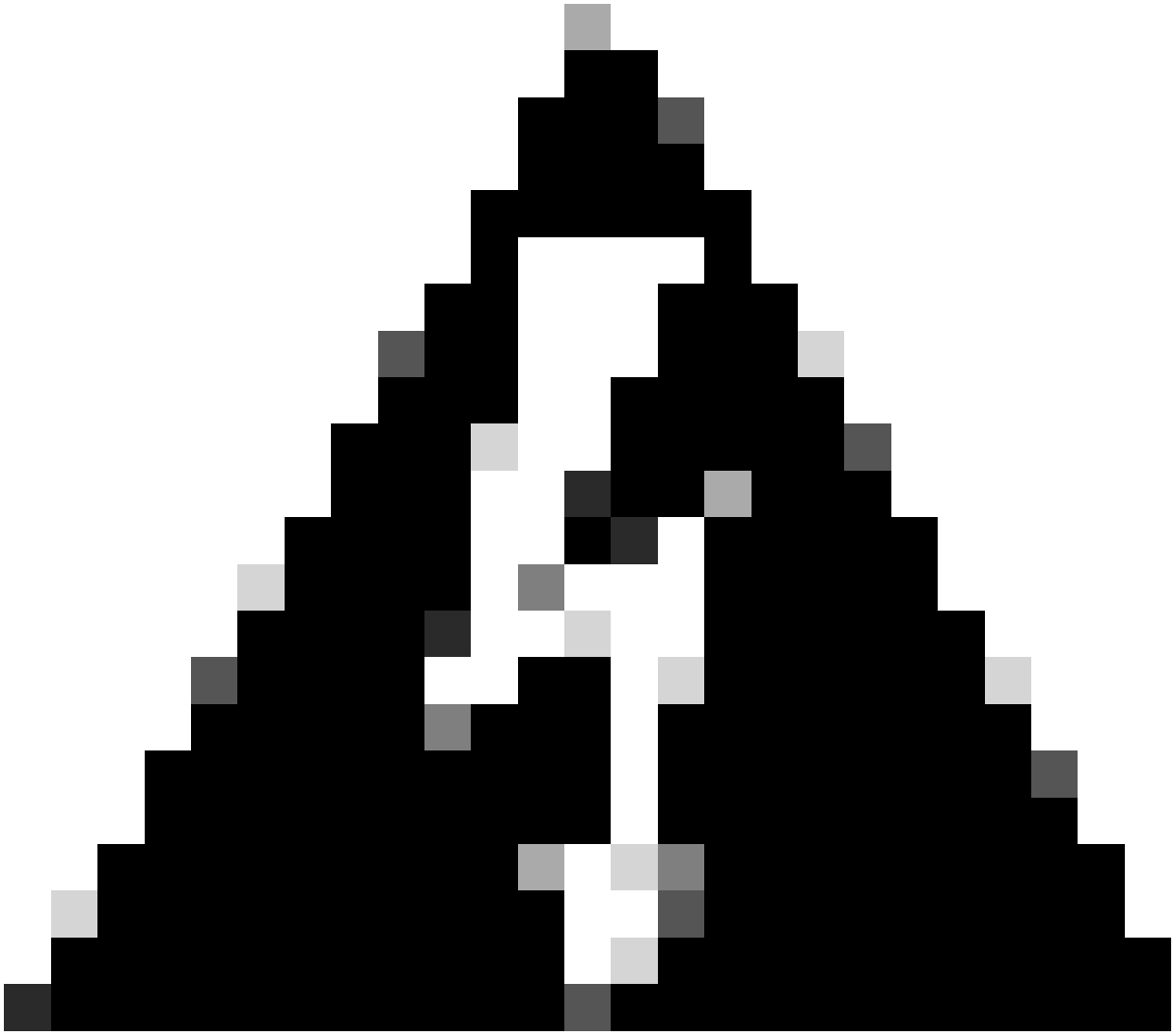
Innerhalb eines LISP-Kontexts verfolgt die Standortkontrollebene MAC-Adressen und die zugehörigen MAC-zu-IP-Bindungen im Wesentlichen wie traditionelle ARP-Einträge. Reine L2 VNI/L2-Pools erleichtern die Registrierung, Auflösung und Weiterleitung ausschließlich auf Basis dieser beiden EID-Typen. Daher 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).

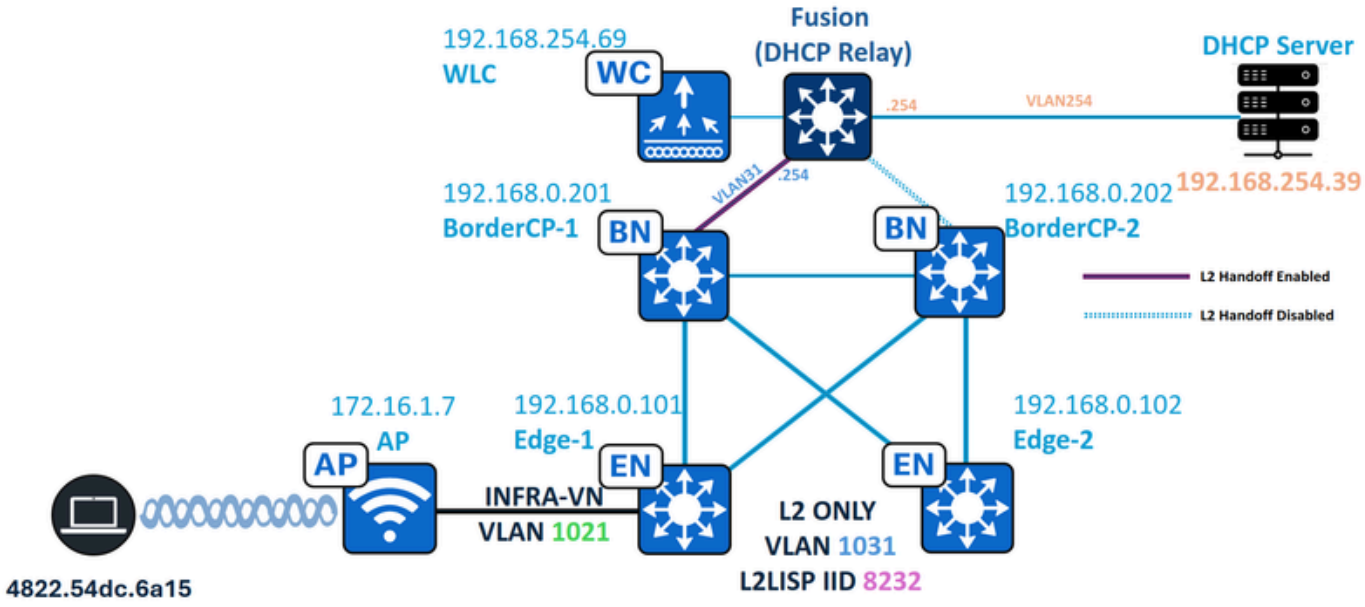
- Aktivieren Sie IP-Multicast-Routing auf allen Knoten (Grenzen, Kanten, Zwischenknoten usw.).
- Konfigurieren Sie den PIM Sparse-Mode an der Loopback0-Schnittstelle jedes Border- und

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.

Broadcast über Access-Tunnel-Schnittstellen

Fabric Enabled Wireless nutzt lokale Switching- und VTEP-Funktionen am AP und FE. Eine IOS-XE 16.10+-Einschränkung verhindert jedoch die Broadcast-Ausgangsweiterleitung über VXLAN an die APs. In reinen L2-Netzwerken verhindert dies, dass DHCP-Angebote/ACKs Wireless-Clients erreichen. Die Funktion "Flood Access Tunnel" löst dieses Problem, indem sie die Broadcast-Weiterleitung an Fabric Edge Access Tunnel-Schnittstellen ermöglicht.

Topologie



Netzwerktopologie

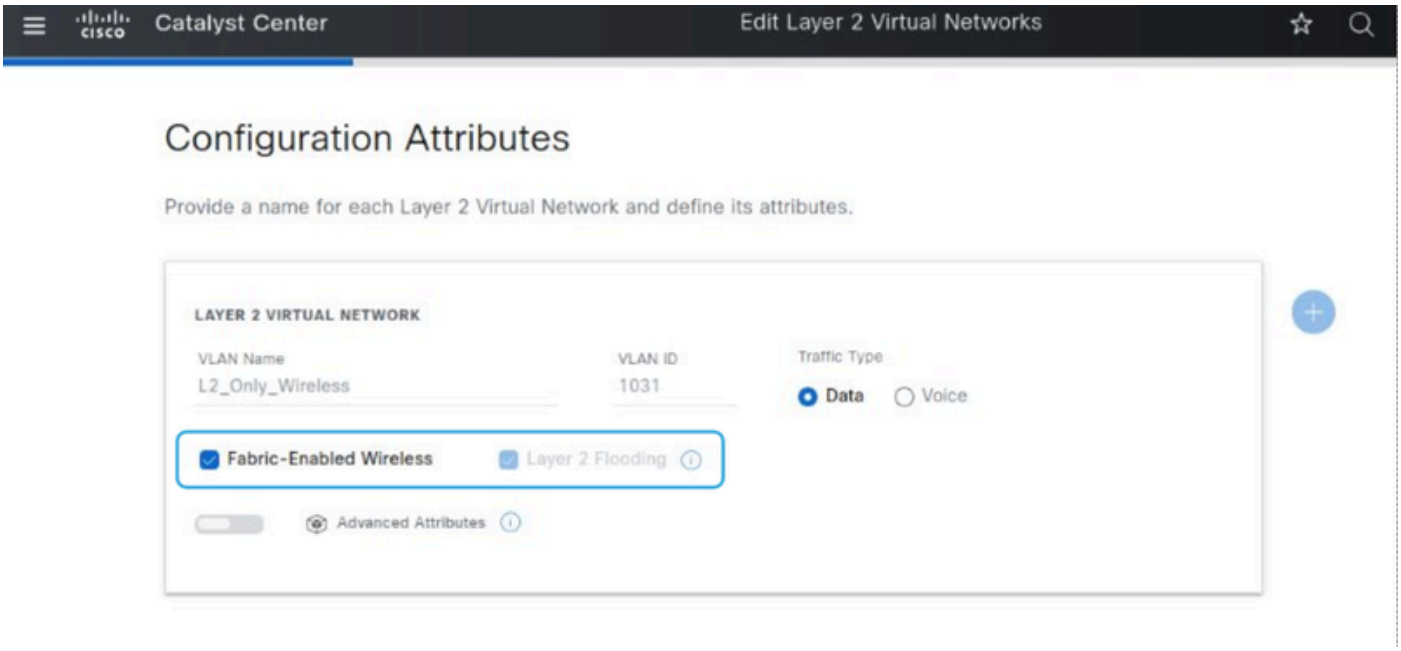
In dieser Topologie gilt Folgendes:

- 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
- 172.16.1.7 ist der Access Point in INFRA-VN mit VLAN 1021.
- 192.168.254.39 ist der DHCP-Server
- 192.168.254.69 ist der Wireless LAN Controller
- 4822.54dc.6a15 ist das DHCP-fähige Endgerät.
- 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 mit Fabric-fähigem Wireless

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 ein Wireless-Pool. Daher werden Funktionen konfiguriert, die in der Regel nur in L2-Wireless-Pools zu finden sind, z. B. RA-Guard, DHCPGuard und Flood Access Tunnel. ARP Flooding ist in einem Wireless-Pool nicht aktiviert.

Fabric Edge-Konfiguration (192.168.0.101)

<#root>

```
ipv6 nd raguard policy
```

dnac-sda-permit-nd-raguardv6

```
 device-role router
ipv6 dhcp guard policy
```

dnac-sda-permit-dhcpv6

```
 device-role server

vlan configuration
```

```
1031

 ipv6 nd raguard attach-policy
dnac-sda-permit-nd-raguardv6

 ipv6 dhcp guard attach-policy
dnac-sda-permit-dhcpv6


cts role-based enforcement vlan-list
1031

vlan
1031


name L2_Only_Wireless



ip igmp snooping querier
no ip igmp snooping vlan 1031 querier


no ip igmp snooping vlan 1031


no ipv6 mld snooping vlan 1031



router lisp

 instance-id
8240

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

 eid-table vlan 1031



 broadcast-underlay 239.0.17.1


   flood unknown-unicast
   flood access-tunnel 232.255.255.1 vlan 1021
```

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

Der Befehl "flood-access tunnel" wird in der Multicast-Replikationsvariante konfiguriert, bei der der gesamte BUM-Datenverkehr mithilfe der quellenspezifischen Multicast-Gruppe (232.255.255.1) mit dem INFRA-VN Access Point VLAN als VLAN gekapselt wird, das vom IGMP-Snooping zum Weiterleiten des BUM-Datenverkehrs abgefragt wird.

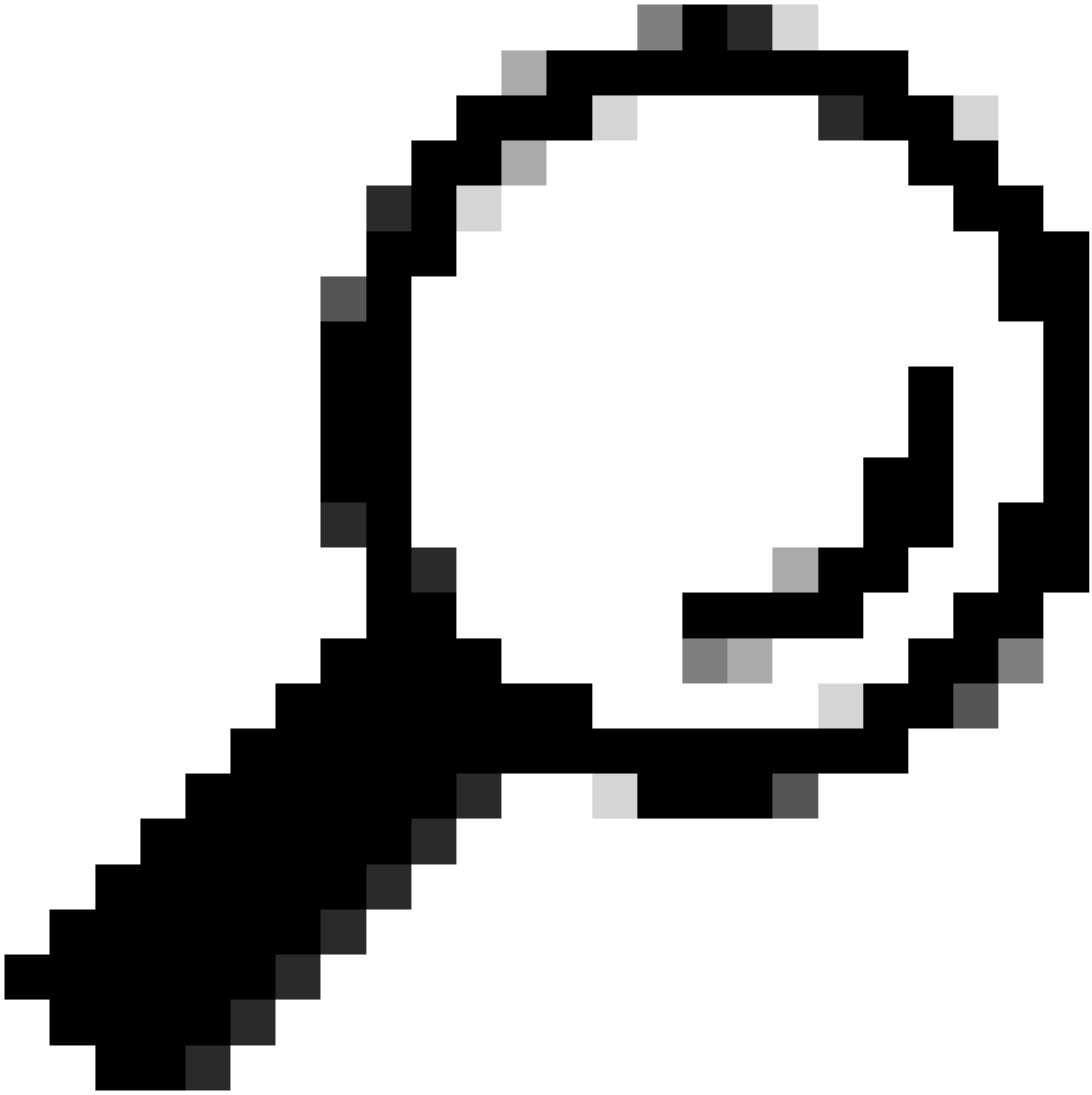
Reine L2-VLAN-Konfiguration - Wireless LAN-Controller

Auf der Seite des WLC (Wireless LAN Controller) müssen mit Fabric Access Points verknüpfte Site-Tags so konfiguriert werden, dass "kein Fabric-AP-ARP-Caching" zum Deaktivieren der Proxy-ARP-Funktion ausgeführt wird. Außerdem muss "Fabric ap-dhcp-broadcast" aktiviert sein. Diese Konfiguration ermöglicht die Weiterleitung von DHCP-Broadcast-Paketen vom WAP an Wireless-Endpunkte.

Fabric WLC (192.168.254.69)-Konfiguration

<#root>

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

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



Tipp: Die Wireless-Multicast-Gruppe 232.255.255.1 ist die Standardgruppe, die von allen Site-Tags verwendet wird.

<#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

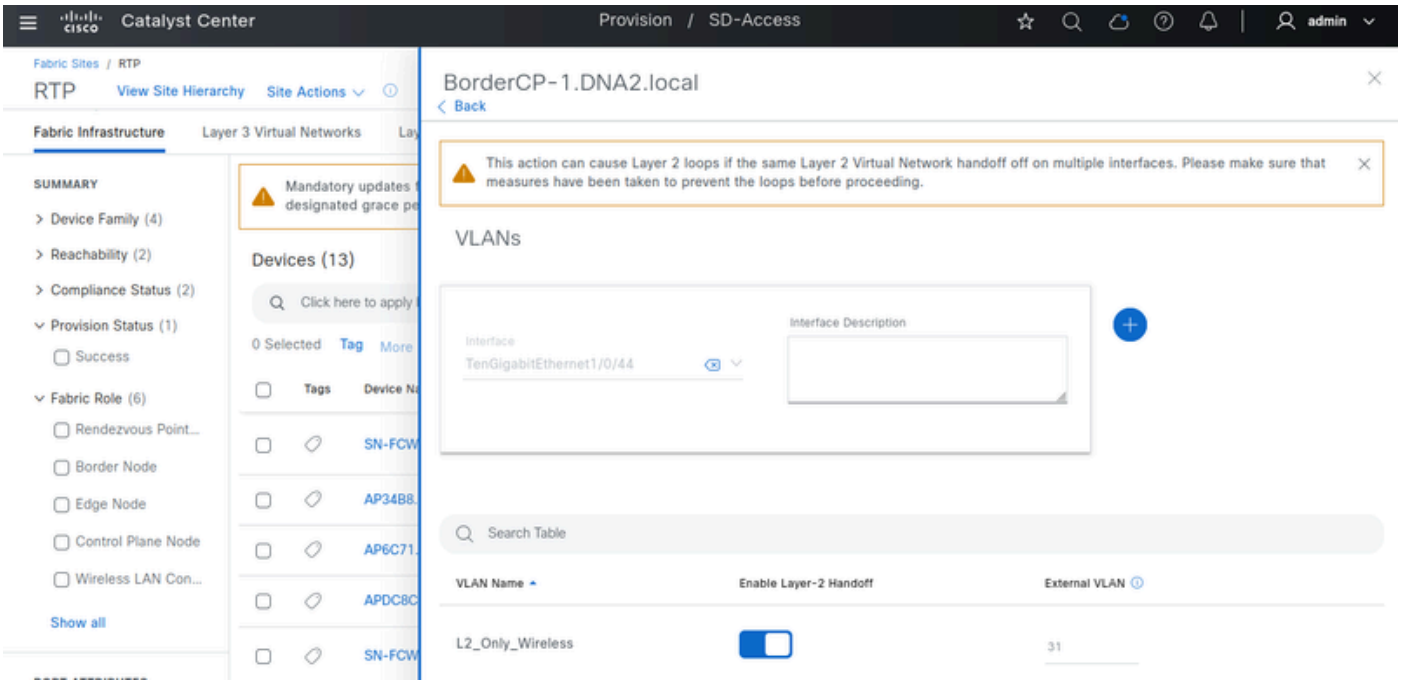
```
RTP-Site-Tag-3 Load : 0
```

L2-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/CP (192.168.0.201)-Konfiguration

<#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
```

Wireless Multicast-Unterstützung

Fabric-Edges sind für die Weiterleitung von Broadcast-Paketen an Access Points über den Flood Access-Tunnel-Mechanismus konfiguriert. Diese Pakete werden in die Multicast-Gruppe 232.255.255.1 im INFRA-VN-VLAN gekapselt. Access Points treten dieser Multicast-Gruppe automatisch bei, da ihr Site-Tag für ihre Nutzung vorkonfiguriert ist.

```
<#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
```

Vom Access Point wird bei Zuordnung eines Wireless-Fabric-Endpunkts ein VXLAN-Tunnel gebildet (auf AP-Seite dynamisch, auf Fabric-Edge-Seite stets aktiv). Innerhalb dieses Tunnels wird die CAPWAP-Fabric-Multicast-Gruppe mithilfe von Befehlen des AP-Terminals verifiziert.

<#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
```

Überprüfen Sie auf der Fabric Edge-Seite, ob IGMP-Snooping für das INFRA-VN AP-VLAN aktiviert ist, ob die Access Points eine Access-Tunnel-Schnittstelle gebildet haben und der Multicast-Gruppe 232.255.255.1 beigetreten sind.

<#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

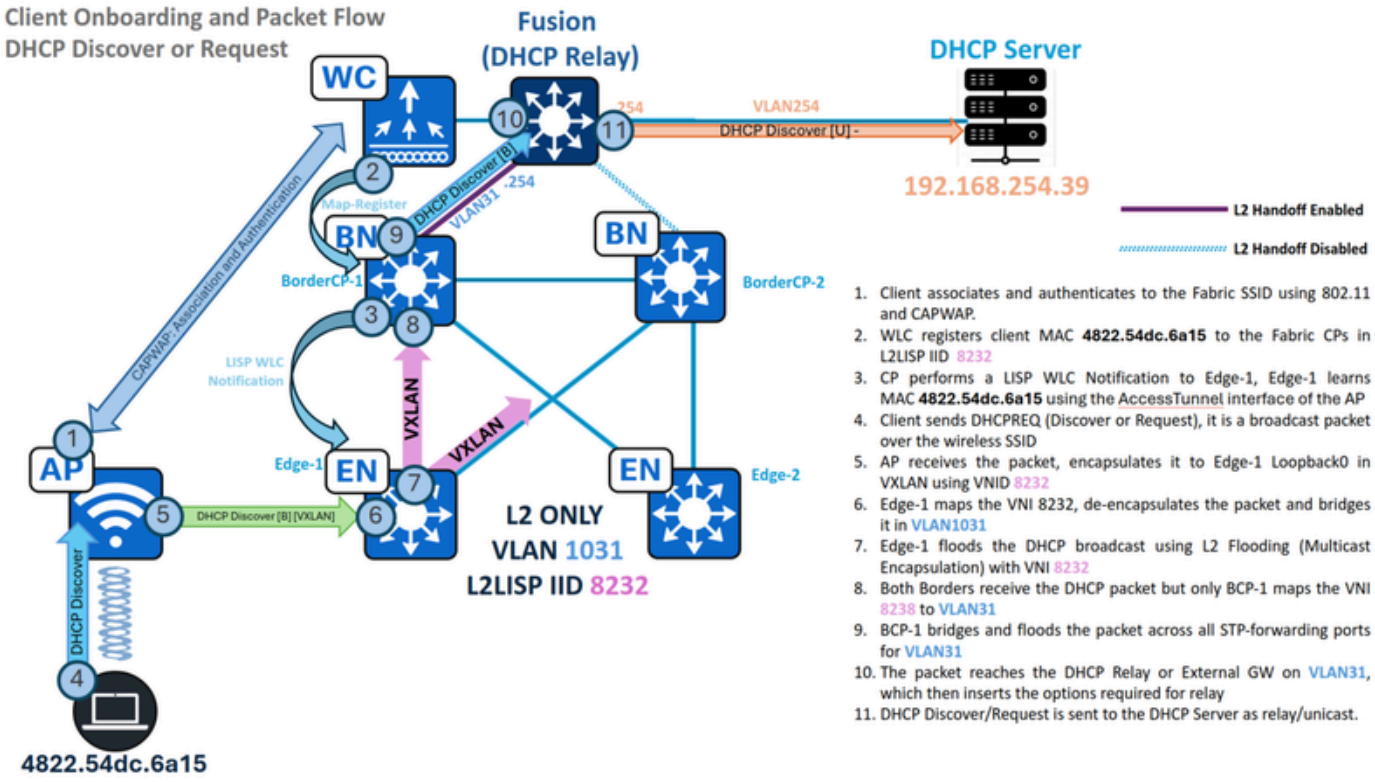
```
           igmp        v2
```

```
 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>
```

Diese Überprüfungen bestätigen die erfolgreiche Aktivierung von Wireless Multicast über den Access Point, Fabric Edge und Wireless LAN Controller hinweg.

DHCP-Datenverkehrsfluss

DHCP-Erkennung und -Anforderung - Wireless-Seite



Datenverkehrsfluss - DHCP-Erkennung und -Anforderung nur in L2

den Status des Wireless-Endpunkts, den verbundenen Access Point und die zugehörigen Fabric-Eigenschaften.

<#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

Stellen Sie sicher, dass im Richtlinienprofil sowohl die Funktionen für zentrales Switching als auch die Funktionen für zentrales DHCP deaktiviert sind. Die Befehle "no central dhcp" und "no central switching" müssen im Richtlinienprofil für die SSID konfiguriert werden.

<#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

Diese Überprüfungen bestätigen, dass der Endpunkt mit "AP1" verbunden ist, das dem Fabric Edge RLOC 192.168.0.101 zugeordnet ist. Demzufolge wird sein Datenverkehr über VXLAN mit der VNID 8232 gekapselt, um ihn vom Access Point zum Fabric Edge zu übertragen.

DHCP-Erkennung und -Anforderung - Fabric Edge

MAC-Lernen mit WLC-Benachrichtigung

Beim Onboarding der Endgeräte registriert der WLC die MAC-Adresse des Wireless-Endgeräts bei der Fabric-Kontrollebene. Gleichzeitig benachrichtigt die Kontrollebene den Fabric-Edge-Knoten (mit dem der Access Point verbunden ist), einen speziellen "CP_LEARN"-MAC-Lerneintrag zu erstellen, der auf die Access-Tunnel-Schnittstelle des Access Points verweist.

<#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
```

Wenn die MAC-Adresse des Endpunkts über die dem verbundenen Access Point entsprechende Access-Tunnel-Schnittstelle korrekt ermittelt 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 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>
```

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 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:

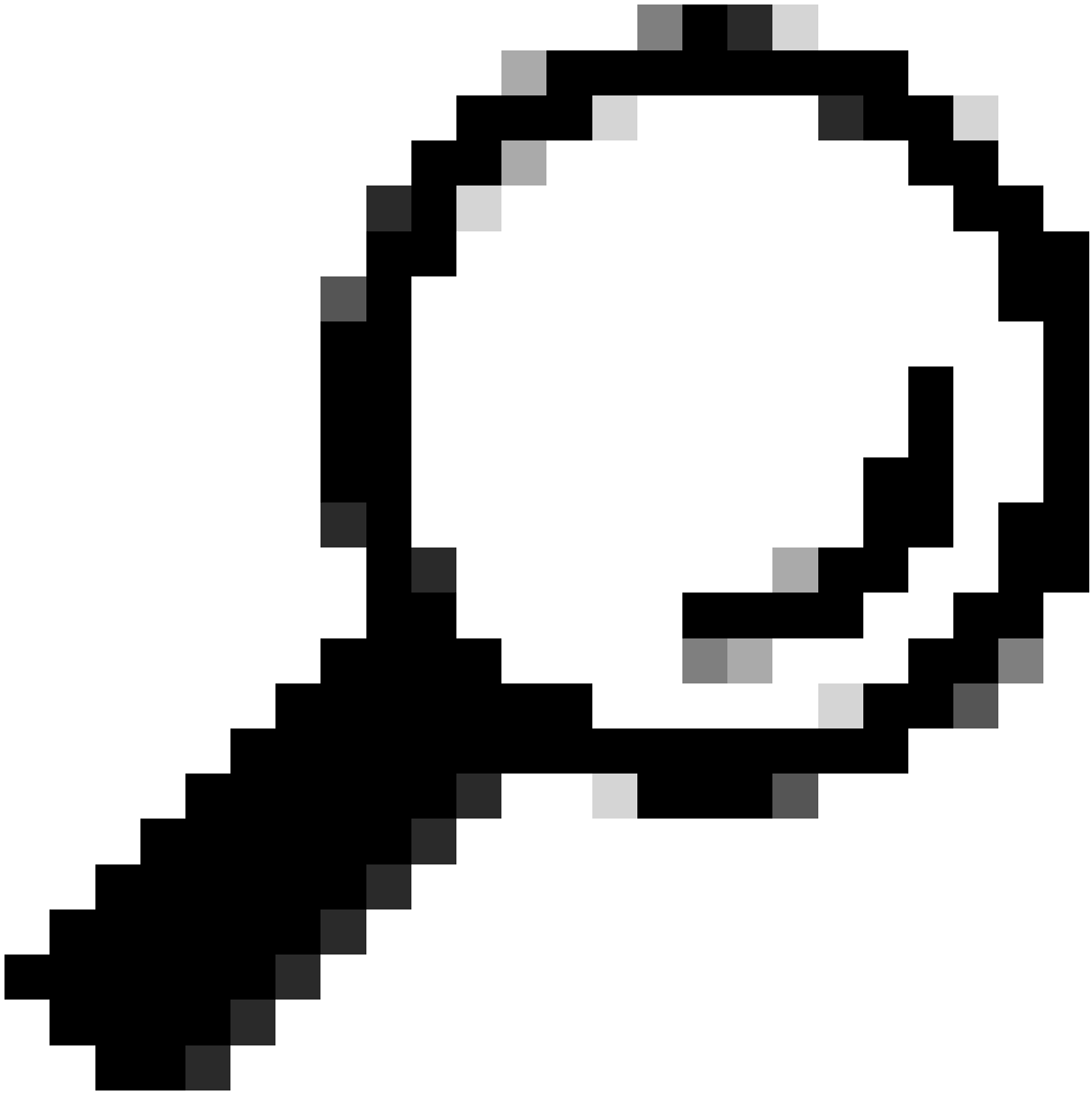
7

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

<--

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

  Totals - Source count: 1, Packet count: 8



Tipp: 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 integrierte Paketerfassung auf dem Switch, um das eingehende DHCP-Paket vom Access Point und das entsprechende Ausgangspaket für L2 Flooding aufzuzeichnen.

Fabric Edge (192.168.0.101) - Paketerfassung

```
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
```

Bei der Paketerfassung müssen drei verschiedene Pakete beobachtet werden:

- DHCP Discovery - VXLAN - AP-to-Edge
- DHCP Discovery - CAPWAP - AP an WLC
- DHCP Discovery - VXLAN - Edge to Multicast Group

<#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

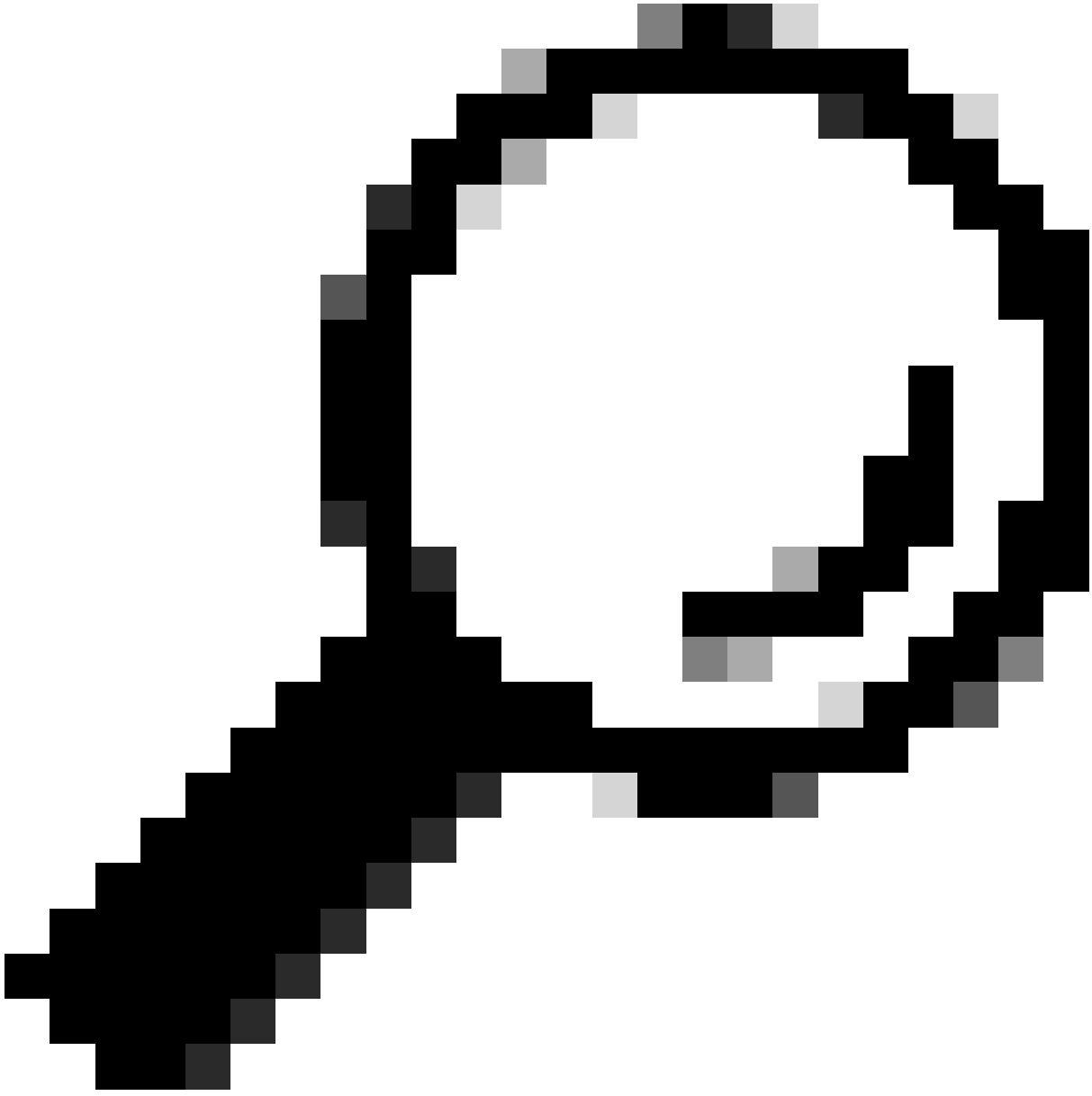
```
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
Internet Protocol Version 4, Src:
```

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



Tipp: Auf Fabric Enabled Wireless übermitteln VXLAN-gekapselte Pakete DHCP-Datenverkehr an Clients oder Server. CAPWAP DATA (UDP 5247)-gekapselte Pakete werden jedoch nur zu Nachverfolgungszwecken an den WLC übertragen, z. B. für den IP-Lernstatus oder die drahtlose Geräteverfolgung.

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 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,

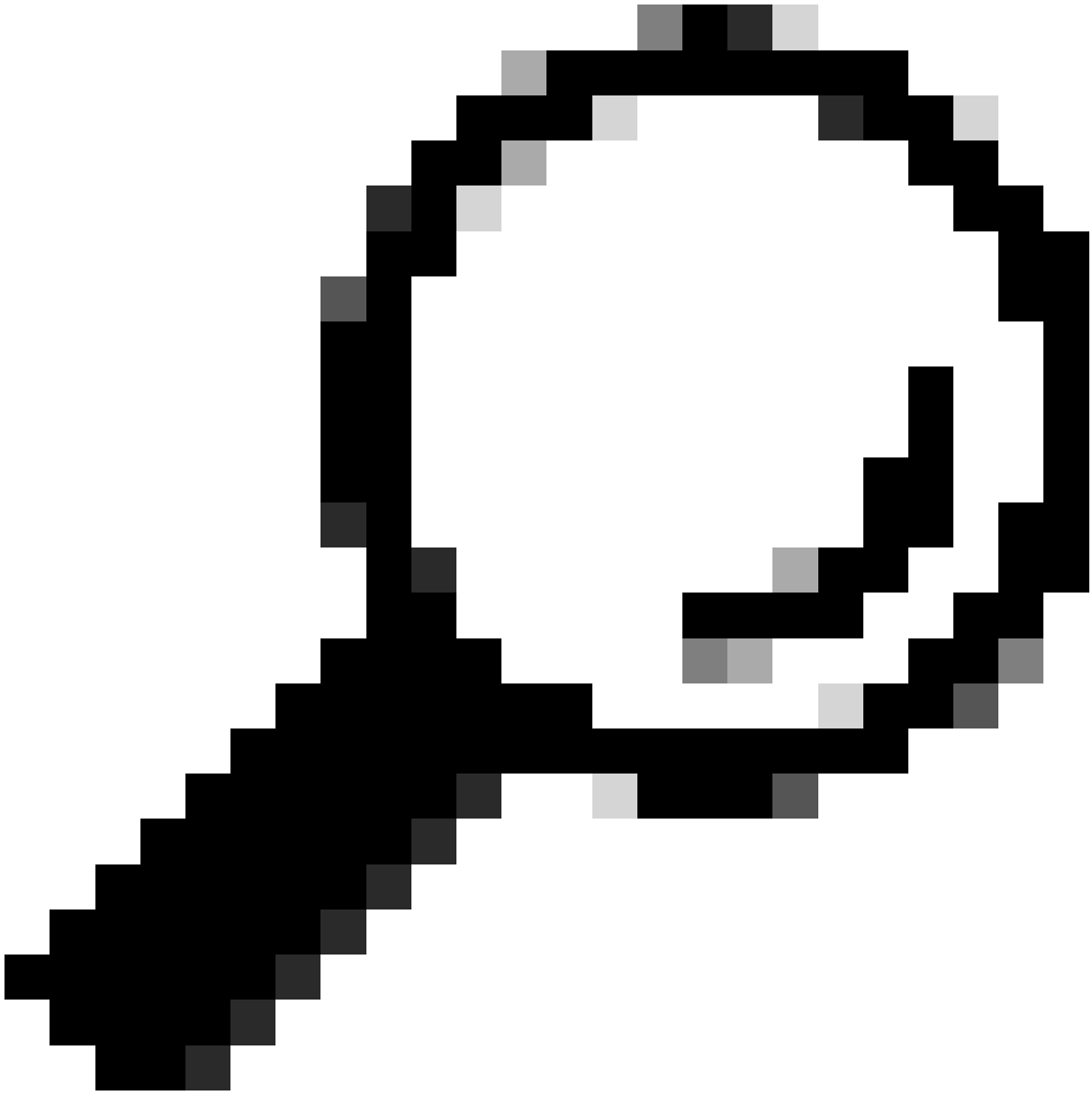
SW Forwarding: 1/0/392/0, Other: 0/0/0
HW Forwarding:

3

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

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

Totals - Source count: 1, Packet count: 4



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 eingehende DHCP-Paket an der L2LISP0-Schnittstelle verweigert.

<#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
```

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 31 | 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        state      Time left
ARP

172.16.131.254

                        f87b.2003.7fd5

Te1/0/44

 31

       0005       34s       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

<--

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

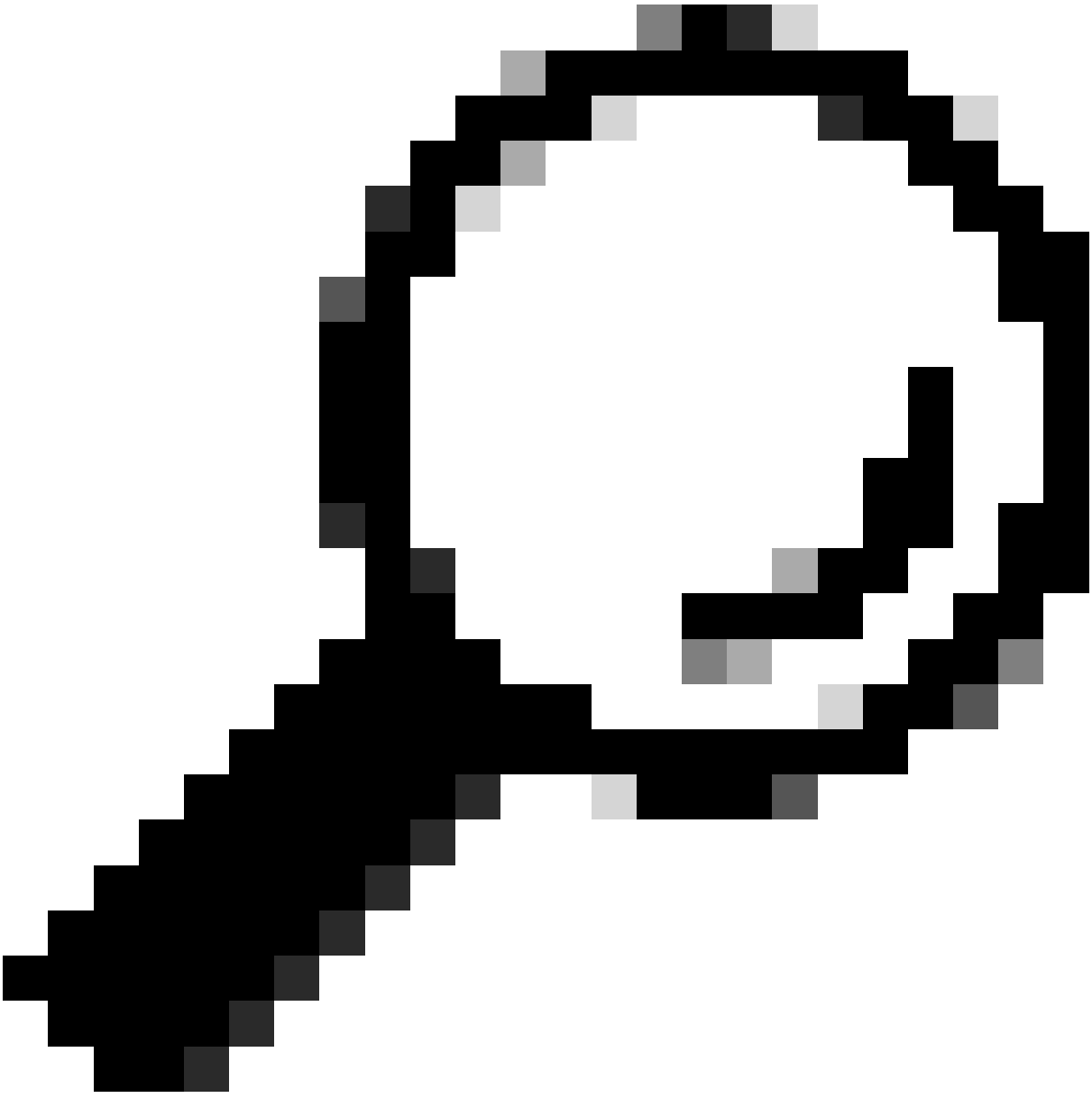
```
  326  16.695053      0.0.0.0 -> 255.255.255.255 DHCP
352
 DHCP Discover - Transaction ID 0x824bdf45
<-- 352 is the Lenght of the VXLAN encapsulated packet



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
```

An diesem Punkt wurde das Ermittlungs-/Anforderungspaket aus der SD-Access-Fabric entfernt, und dieser Abschnitt wird zum Abschluss gebracht. Bevor Sie jedoch fortfahren, bestimmt ein wichtiger Parameter - die DHCP-Broadcast-Markierung, die vom Endpunkt selbst bestimmt wird - das Weiterleitungsszenario für nachfolgende Offer- oder ACK-Pakete. Wir können eines unserer Discover-Pakete untersuchen, um diese Flagge zu überprüfen.

<#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
```

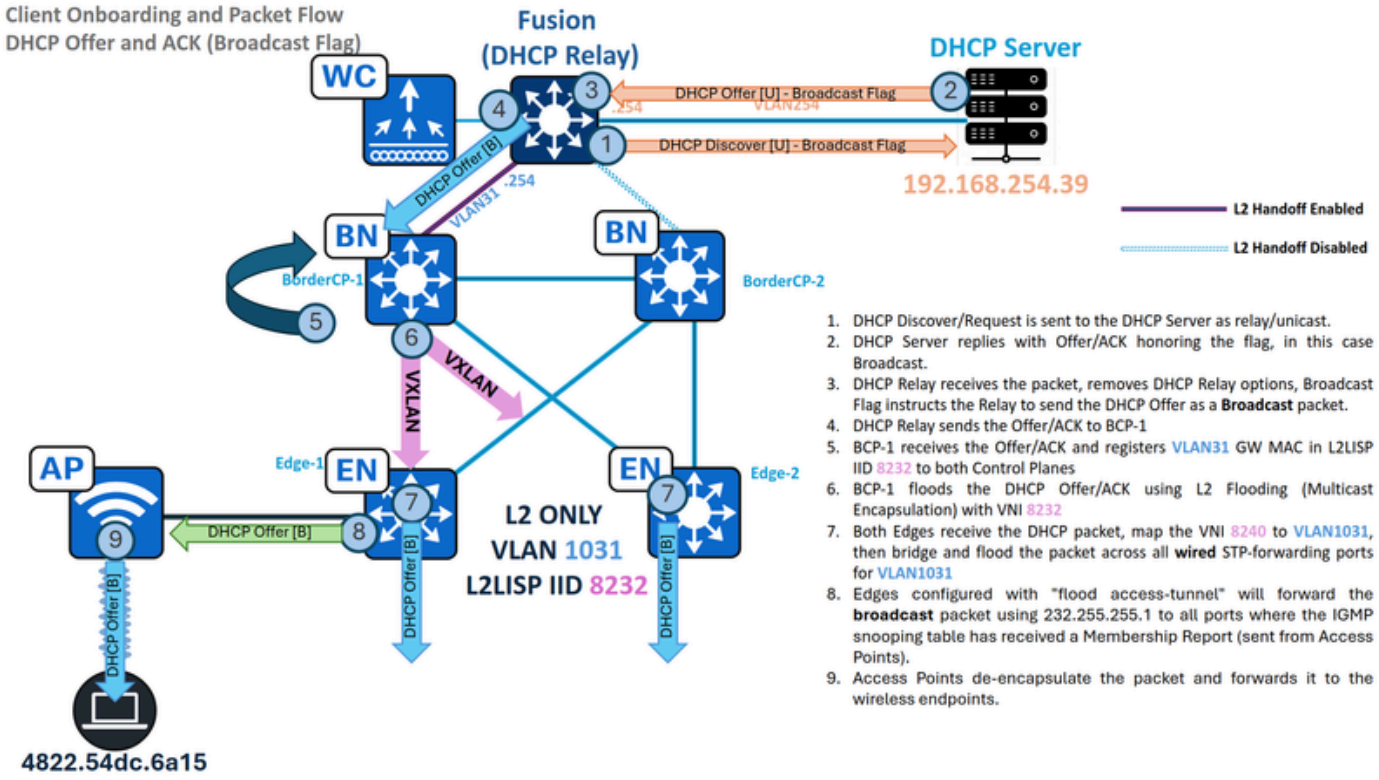


Tipp: bootp.type==1 kann nur zum Filtern von Discover- und Request-Paketen verwendet

---

werden.

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 (z. B. GiAddr/GatewayIPAddress) ein 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 der 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 8232 zugeordnet ist.

<#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

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 <-- 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
```

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 zu anderen Fabric-Knoten überbrückt. 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 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

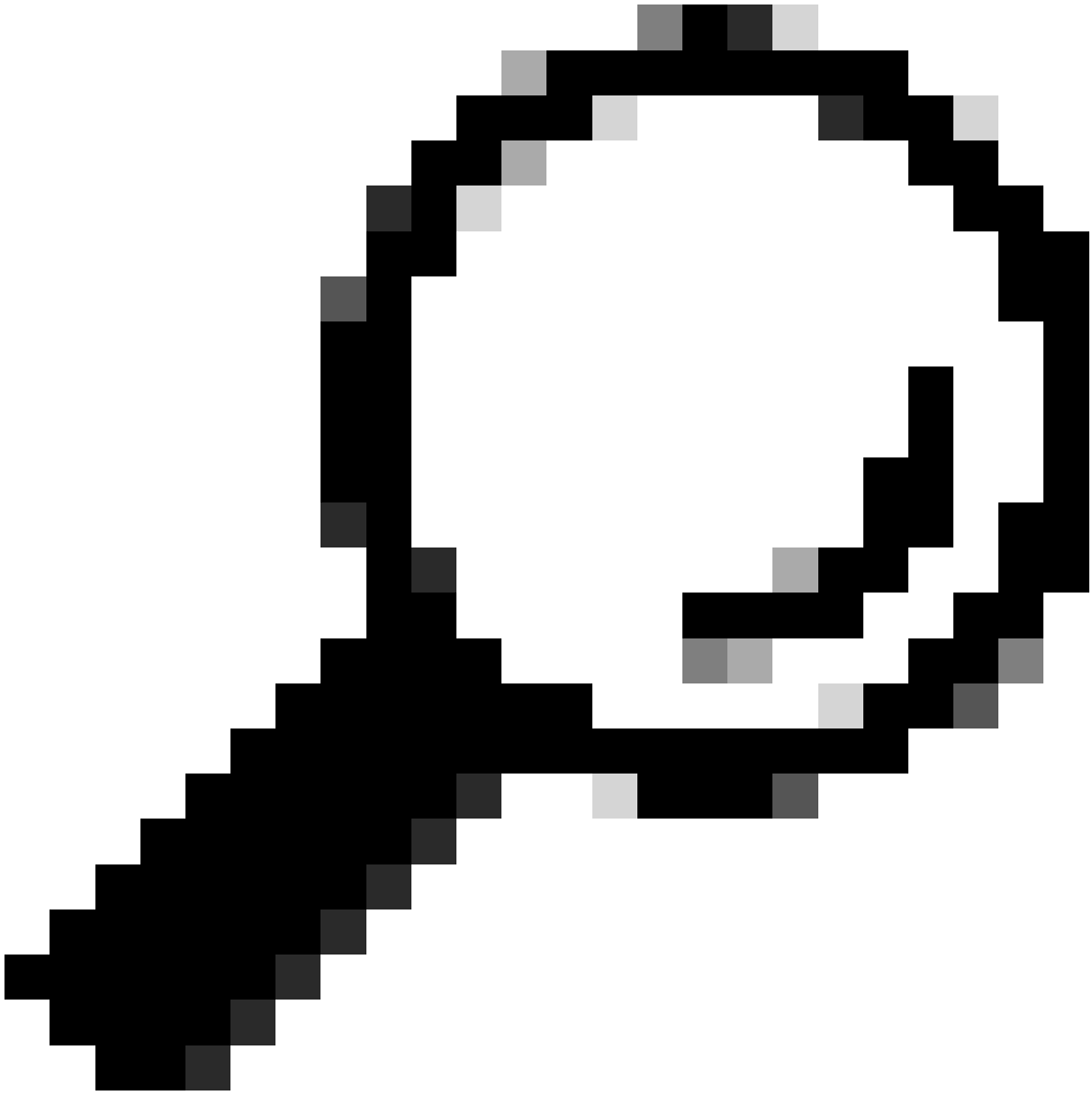
,
   SW Forwarding: 1/0/392/0, Other: 1/1/0
   HW Forwarding:

92071

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

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

  Totals - Source count: 1, Packet count: 92071



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, schließen wir diesen Abschnitt ab, 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

Genau wie beim vorherigen Datenstrom wird nun das L2Border S,G im Fabric Edge überprüft. Dort zeigt die eingehende Schnittstelle zum L2BN und das OIL enthält die L2LISP-Instanz, die VLAN 1031 zugeordnet ist.

<#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,

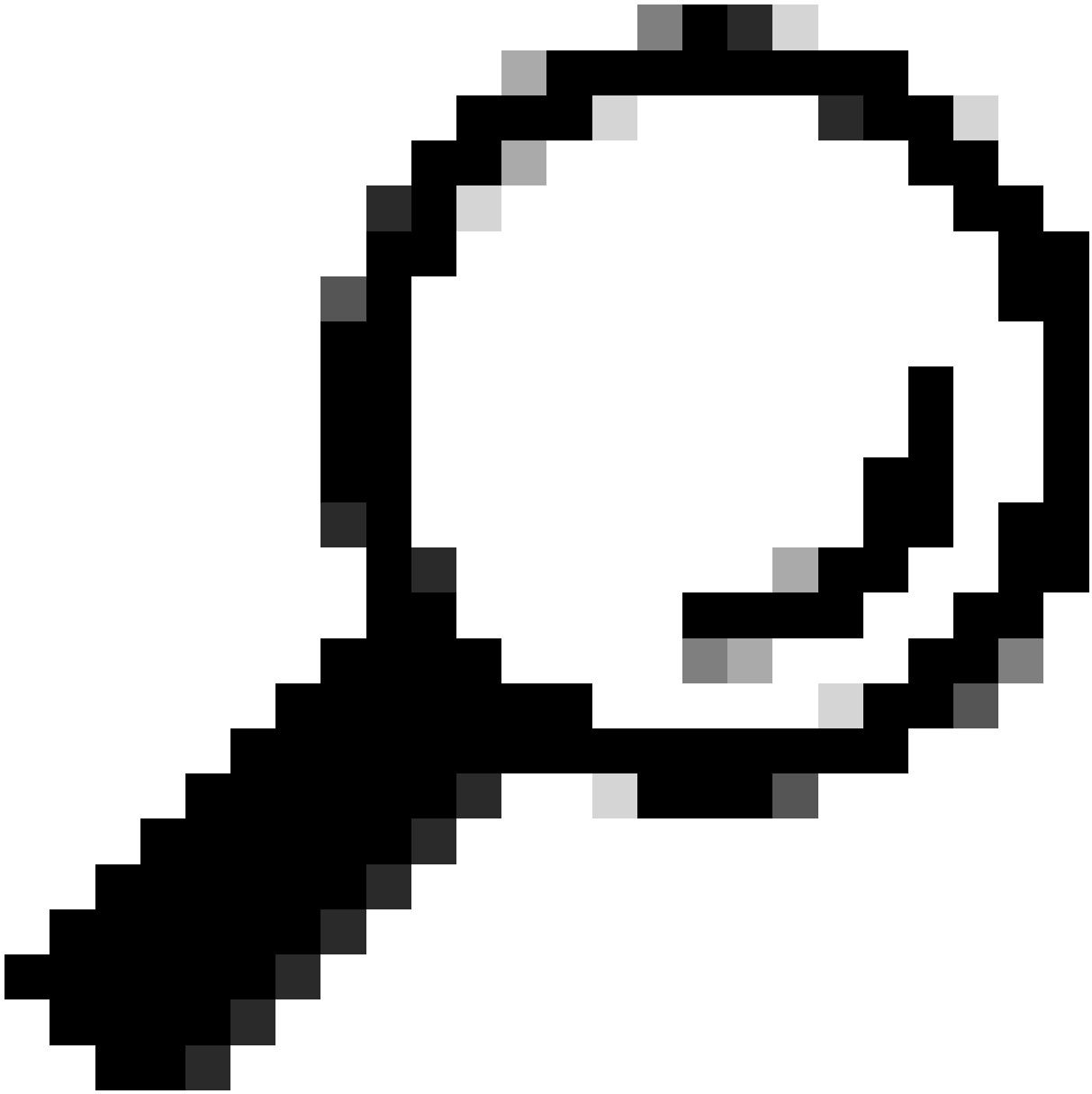
```
   SW Forwarding: 1/0/96/0, Other: 0/0/0
   HW Forwarding:
```

76236

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

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

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



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.

Nach der Entkapselung des Pakets und seiner Platzierung im VLAN mit VNI 8232 bestimmt dessen Broadcast-Charakter, dass alle kabelgebundenen Spanning Tree Protocol-Weiterleitungs-Ports für VLAN1031 überflutet werden.

<#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
```

Die Schnittstelle, die wir für die Übertragung des DHCP-Angebots benötigen, ist jedoch die mit dem Access Point verknüpfte Access-Tunnel-Schnittstelle. Dies ist nur möglich, weil auf der L2LISP-ID 8232 "flood access-tunnel" aktiviert ist, andernfalls wird dieses Paket für die Weiterleitung an die AccessTunnel-Schnittstelle blockiert.

<#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
```

Mit dem IGMP-Snooping-Eintrag für die Multicast-Flooding-Gruppe werden DHCP-Angebote und ACKs an den physischen Port des AP weitergeleitet.

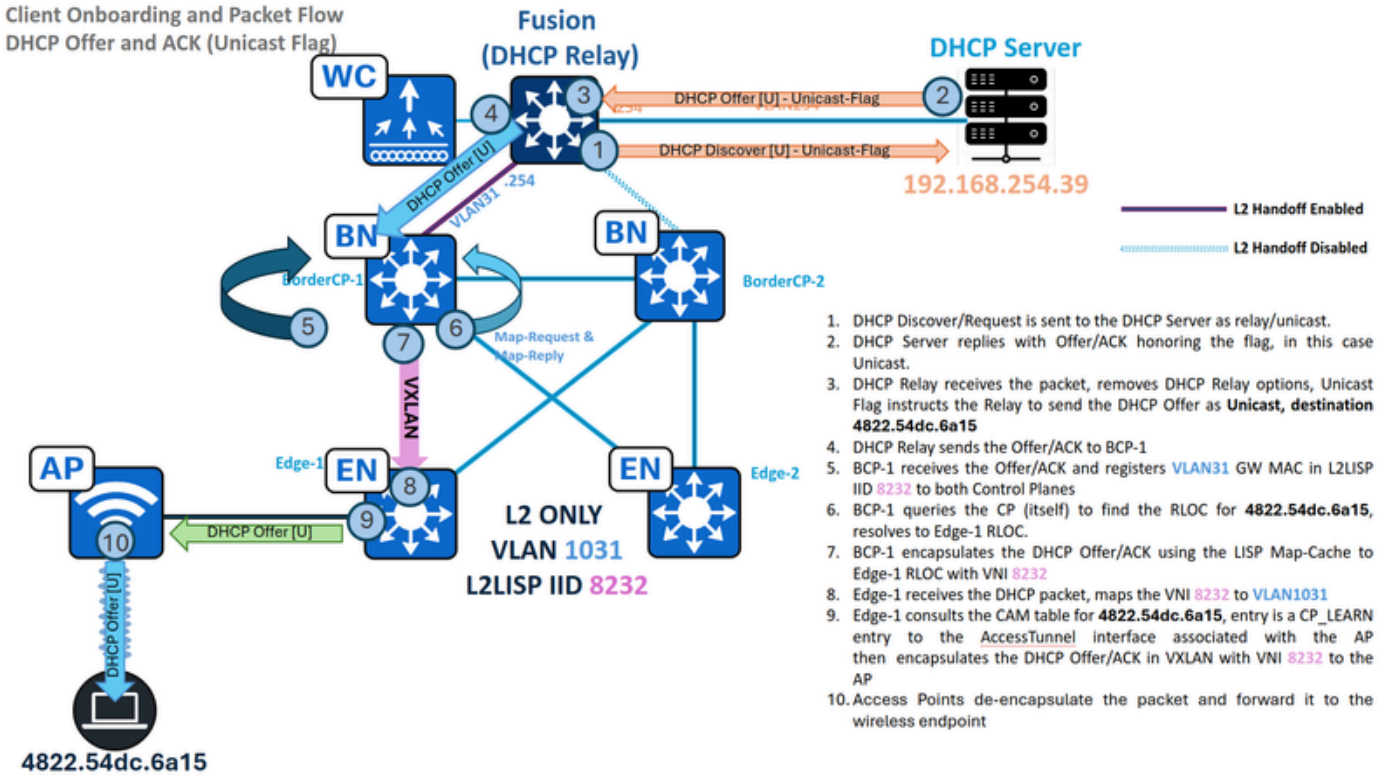
Das DHCP-Angebot und der ACK-Prozess bleiben konsistent. Wenn DHCP Snooping nicht aktiviert ist, werden keine Einträge in der DHCP Snooping-Tabelle erstellt. Folglich wird der Device-Tracking-Eintrag für den DHCP-fähigen Endpunkt durch gelesene ARP-Pakete generiert. Es wird außerdem erwartet, dass Befehle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

<#root>

```
Edge-1#
show device-tracking database interface 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-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==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)
```

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 Ziel-MAC-Adresse ab. Unter der Annahme eines erfolgreichen "MAC Learning und WLC Notification" am Fabric Edge verfügt die Kontrollebene über eine registrierte Endpunkt-ID (EID).

```
<#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
```

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 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        -
```

Wenn das RLOC aufgelöst ist, wird das DHCP-Angebot in Unicast gekapselt und direkt an Edge-1 mit der Nummer 192.168.0.101 und VNI 8240 gesendet.

```
<#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
```

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 dann nur an den spezifischen Zugriffstunnel weiter, mit dem der Endpunkt verbunden ist, anstatt es an alle Ports zu fluten.

In der MAC-Adresstabelle wird der Port AccessTunnel2 als der virtuelle Port identifiziert, der mit AP1 verknüpft ist.

<#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

Das DHCP-Angebot und der ACK-Prozess bleiben konsistent. Wenn DHCP Snooping nicht aktiviert ist, werden keine Einträge in der DHCP Snooping-Tabelle erstellt. Dementsprechend wird der Device-Tracking-Eintrag für den DHCP-fähigen Endpunkt nicht durch DHCP, sondern durch gelesene 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 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
```

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.

DHCP-Transaktion - Wireless-Überprüfung

Vom WLC aus wird die DHCP-Transaktion über RA-Traces überwacht.

<#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
```

Am Ende der Transaktion wird der Endpunkt der Geräteverfolgungsdatenbank auf dem Wireless LAN Controller hinzugefügt.

<#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
```

Die gesamte DHCP-Transaktion wird auf dem Access Point selbst gedebuggt.

<#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: 1
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: 1754890669.367
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**

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.