Implementierung eines BGP EVPN DHCP Layer 2-Relays auf Catalyst Switches der Serie 9000

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
  - Dokumentdetails
  - L2-Relayverhalten
- Terminologie
- Konfigurieren (Standard-CGW-Bereitstellung)
  - Netzwerkdiagramm
  - L2 VTEP (Leaf) - Schlüsseldetails
  - L3 VTEP (CGW) - Hauptdetails
  - L2VTEP
  - CGW
- Verifizieren (Standard-CGW-Bereitstellung)
  - Gateway-Präfix (Leaf)
  - FED-MATM (Leaf)
  - Lokale MAC (Leaf)
  - DHCP-Snooping (Leaf und CGW)
- Konfigurieren (teilweise isoliert, geschützt)
  - Netzwerkdiagramm
  - L2 VTEP (Leaf) - Schlüsseldetails
  - L3 VTEP (CGW) - Hauptdetails
  - CGW
- Überprüfen (teilweise isoliert und geschützt)
  - Gateway-Präfix (Leaf)
  - FED-MATM (Leaf)
  - Lokale MAC (Leaf)
  - DHCP-Snooping (Leaf und CGW)
- Fehlerbehebung (jeder CGW-Typ)
  - Debuggen von DHCP-Snooping (Leaf)
  - DHCP Snooping Debugs (CGW)
  - Eingebettete Erfassung
  - Statistiken des DHCP-Snooping-Clients
  - Zusätzliche Debugs
- Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie die DHCP L2-Relay-Funktion von EVPN VxLAN konfigurieren, überprüfen und Fehler beheben.

Voraussetzungen

Anforderungen

- Diese Funktion wird bei allen CGW-Bereitstellungen verwendet, bei denen DHCP verwendet wird.
- Wenn Sie Protected Segmentation implementieren, lesen Sie diese Dokumente.
  - Implementierung einer BGP-EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000
  - Implementierung der BGP EVPN Protected Overlay-Segmentierung auf Catalyst Switches der Serie 9000

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 und neuere Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dokumentdetails

Dieses Dokument kann für alle CGW-Bereitstellungen verwendet werden, bei denen DHCP von einem Leaf ohne SVI zum zentralen Gateway weitergeleitet werden muss.

- Wenn Sie keine geschützte Segmentierung verwenden, verwenden Sie den Abschnitt im Dokument, in dem die SVI in der Fabric angekündigt wird.

Wenn Sie eine geschützte Segmentierung implementieren, ist dieses Dokument Teil 2 von drei zusammenhängenden Dokumenten:

- Dokument 1: Implementierung der BGP EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000 beschreibt die Steuerung des BGP BUM-Datenverkehrs im Overlay und muss zuerst konfiguriert werden
- Dokument 2: Implementierung der BGP EVPN Protected Overlay-Segmentierung auf Catalyst Switches der Serie 9000 baut auf dem Overlay-Design und der Overlay-Richtlinie von Dokument 1 auf und beschreibt die Implementierung des Stichworts "protected".
- Dokument 3: Dieses Dokument. Baut auf den letzten beiden Dokumenten auf und beschreibt die Implementierung des DHCP-Relay mit Leafs nur auf Layer 2 und dem CGW

L2-Relayverhalten

Relais	Snooping	Core Flood	Access Flood	IPv4
ja	ja	nein	ja	• Option 82 Suboption: (1) Agent Circuit ID (vni-mod-port) wird mit DHCP Snooping gefüllt • Die Zugriffsseite kann mit der DHCP-Trust-Konfiguration eingeschränkt werden. * EMPFOHLENES MODELL
ja	nein	ja	ja	• Option 82 Suboption: (1) Agent Circuit ID (vlan-mod-port) wird mit DHCP Snooping gefüllt
nein	ja	nein	ja	• Option 82 Suboption: (1) Agent Circuit ID (vni-mod-port) wird mit DHCP Snooping gefüllt • Die Zugriffsseite kann mit der DHCP-Trust-Konfiguration eingeschränkt werden.
Relais	Snooping	Core Flood	Access Flood	IPv6
ja	ja	ja	ja	• Option 82 Suboption: (1) Agent Circuit ID (vni-mod-port) wird mit DHCP Snooping gefüllt • Die Zugriffsseite kann mit der DHCP-Trust-Konfiguration eingeschränkt werden.
ja	nein	ja	ja	• Option 82 Suboption: (1) Agent Circuit ID (vlan-mod-port) wird mit DHCP Snooping gefüllt
nein	ja	ja	ja	• Option 82 Suboption: (1) Agent Circuit ID (vni-mod-

				port) wird mit DHCP Snooping gefüllt • Die Zugriffsseite kann mit der DHCP-Trust-Konfiguration eingeschränkt werden.
nein	nein	ja	ja	

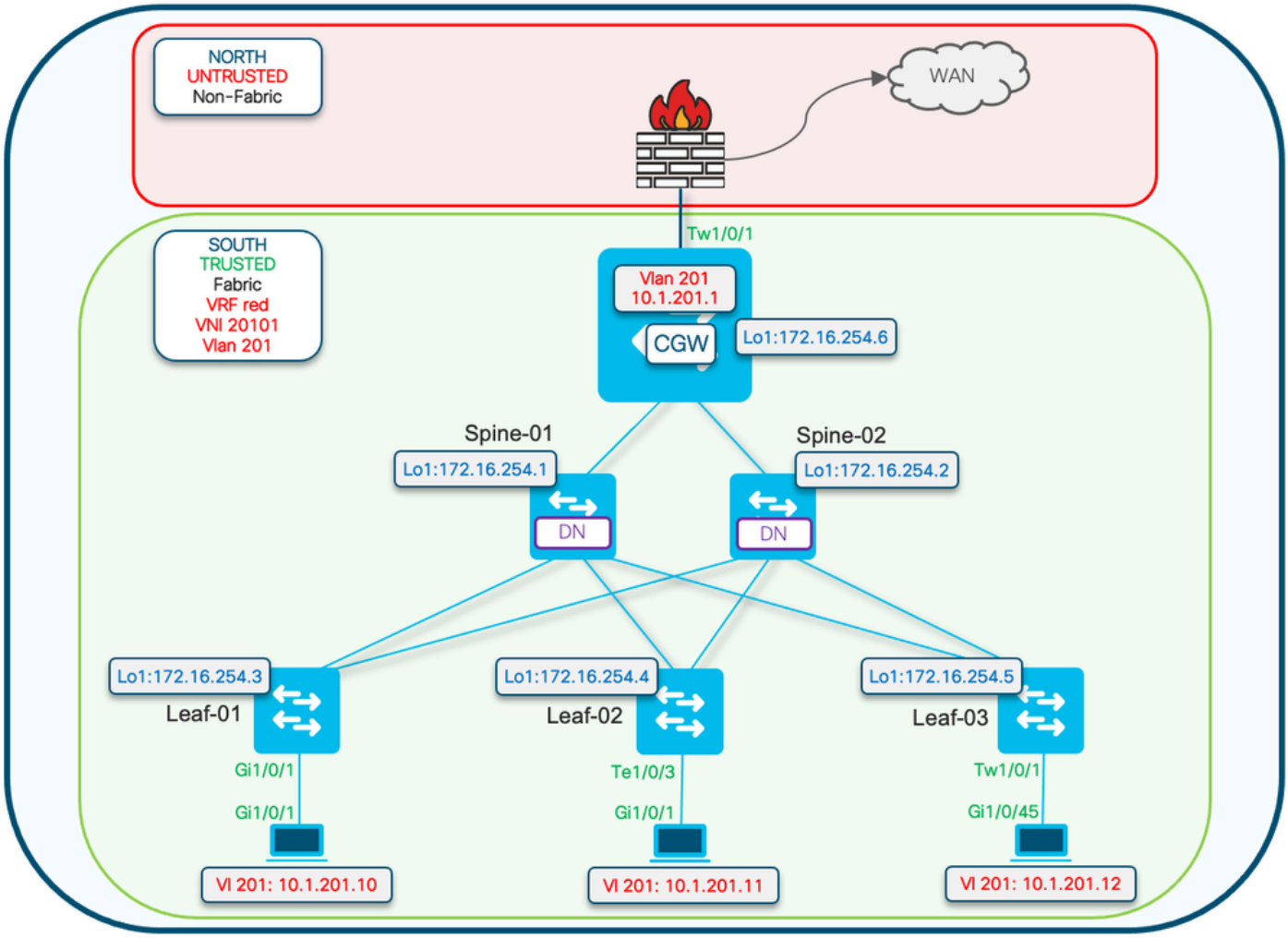
Terminologie

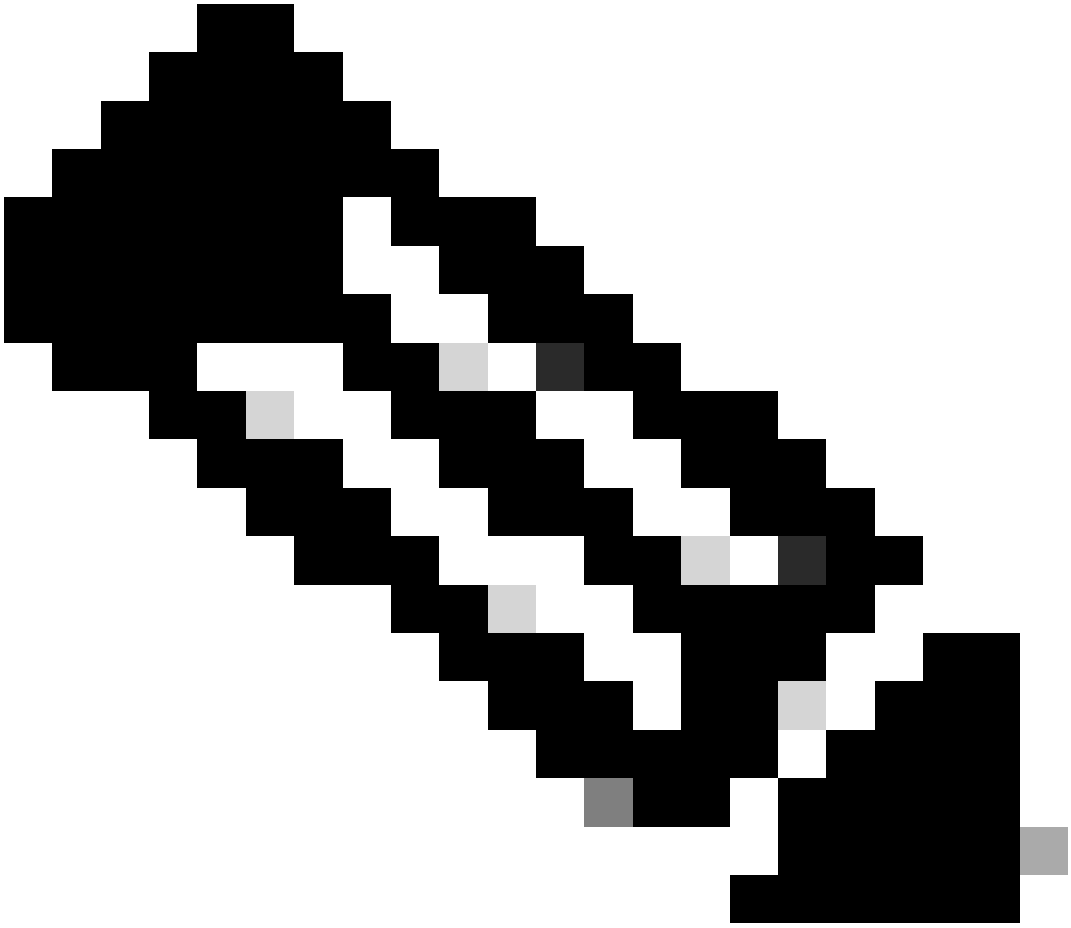
VRF	Virtual Routing-Weiterleitung	Definiert eine Layer-3-Routing-Domäne, die von anderen VRFs und der globalen IPv4/IPv6-Routing-Domäne getrennt wird.
AF	Adressfamilie	Legt fest, welche Typpräfixe und Routing-Informationen vom BGP verarbeitet werden.
ALS	Autonomes System	Ein Satz von über das Internet routbaren IP-Präfixen, die zu einem Netzwerk gehören, oder eine Sammlung von Netzwerken, die alle von einer einzigen Einheit oder Organisation verwaltet, gesteuert und überwacht werden.
EVPN	Ethernet Virtual Private Network	Die Erweiterung, die es dem BGP ermöglicht, Layer-2-MAC- und Layer-3-IP-Informationen zu übertragen, ist EVPN und verwendet das Multi-Protocol Border Gateway Protocol (MP-BGP) als Protokoll zur Verteilung von Erreichbarkeitsinformationen für das VXLAN-Overlay-Netzwerk.
VXLAN	Virtuelles erweiterbares LAN (Local Area Network)	VXLAN wurde entwickelt, um die Einschränkungen von VLANs und STP zu überwinden. Es handelt sich um einen vorgeschlagenen IETF-Standard [RFC 7348], der dieselben Ethernet-Layer-2-Netzwerkdienste wie VLANs bereitstellt, jedoch mit größerer Flexibilität. Funktionell handelt es sich um ein MAC-in-UDP-Kapselungsprotokoll, das als virtuelles Overlay auf einem Layer-3-Underlay-Netzwerk ausgeführt wird.
CGW	Zentrales Gateway	Implementierung von EVPN, wobei sich die Gateway-SVI nicht auf jedem Leaf befindet Stattdessen erfolgt das gesamte Routing über ein spezielles Leaf mit asymmetrischem IRB (Integrated Routing and Bridging).
DEF	Standardgateway	Ein erweitertes BGP-Community-Attribut, das dem MAC/IP-Präfix

GW		über den Befehl "default-gateway advertise enable" im Konfigurationsabschnitt "l2vpn evpn" hinzugefügt wird.
IMET (RT3)	Inklusives Multicast Ethernet-Tag (Route)	Wird auch als BGP-Typ-3-Route bezeichnet. Dieser Routing-Typ wird im EVPN verwendet, um BUM-Datenverkehr (Broadcast/unbekanntes Unicast/Multicast) zwischen VTEPs zu übertragen.
RT2	Routentyp 2	BGP-MAC- oder MAC/IP-Präfix, das eine Host-MAC- oder Gateway-MAC-IP-Adresse darstellt
EVPN-Manager	EVPN-Manager	Zentrale Verwaltungskomponente für verschiedene andere Komponenten (Beispiel: lernt von SISF und signalisiert L2RIB)
SISF	Integrierte Switch-Sicherheitsfunktion	Eine unabhängige Host-Tracking-Tabelle, die von EVPN verwendet wird, um festzustellen, welche lokalen Hosts auf einem Leaf vorhanden sind.
L2RIB	Layer 2 Routing Information Base	Zwischenprodukt für das Management von Interaktionen zwischen BGP, EVPN Mgr, L2FIB
FED	Forwarding-Engine-Treiber	Programmierung der ASIC-Ebene (Hardware)
MATM	MAC-Adresstabellen-Manager	IOS MATM: Softwaretabelle, die nur lokale Adressen und FED-MATM: Hardwaretabelle, die von der Kontrollebene empfangene lokale und Remote-Adressen installiert und Teil der Hardware-Weiterleitungsebene ist

Konfigurieren (Standard-CGW-Bereitstellung)

Netzwerkdiagramm


NORTH
UNTRUSTED
Non-Fabric
WAN
SOUTH
TRUSTED
Fabric
VRF red
VNI 20101
Vlan 201
Tw1/0/1
Vlan 201
10.1.201.1
CGW
Lo1:172.16.254.6
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Gi1/0/1
Gi1/0/1
Vl 201: 10.1.201.10
Lo1:172.16.254.4
Leaf-02
Te1/0/3
Gi1/0/1
Vl 201: 10.1.201.11
Lo1:172.16.254.5
Leaf-03
Tw1/0/1
Gi1/0/45
Vl 201: 10.1.201.12



Hinweis: In diesem Abschnitt wird eine Standard-CGW-Bereitstellung ohne die Verwendung der geschützten Funktion beschrieben.

- Debugger, die den DHCP DORA-Paketaustausch anzeigen, werden nur im Beispiel für das geschützte Segment angezeigt.

L2 VTEP (Leaf) - Schlüsseldetails

Anforderungspaket kommt vom Client

- Verwenden Sie die von GW angegebene Standard-CGW-MAC.
- Wenn mehr als ein GW vorhanden ist, wird zuerst GW MAC verwendet.
- Wandelt die äußere MAC-Adresse (vom Client initiiert: D und R in DORA) in die Unicast-GW-MAC um und leitet sie an den CGW weiter

DHCP Snooping fügt hinzu: Option 82 Unteroptionen: Circuit und RID

(RID wird von der Response Pkt-Verarbeitung auf dem CGW verwendet)

(Informiert CGW über sein nicht lokales und auf Fabric basierendes Relay zurück zu L2VTEP)

<#root>

```
Option: (82) Agent Information Option
        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a000800000277501010000

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000

682c7bf88700 <-- switch base mac 682c.7bf8.8700 (from 'show switch')
```

- Vom CGW empfangene Response-Pakete über den VXLAN-Tunnel
- Leaf Strips Option 82.
- Fügt Bindungseinträge mit der Clientquellenschnittstelle hinzu. (vxlan-mod-port gibt die Client-Quellschnittstelle an)..
- Antwortpaket an Client weitergeleitet

L3 VTEP (CGW) - Hauptdetails

- Aktivieren Sie DHCP SNOOPING
- Aktivieren Sie DHCP RELAY in SVI
- Die Anfrage wird von L2VTEP empfangen und an das Relay weitergeleitet
- Relay fügt weitere Option 82 Unteroptionen hinzu (gi, server override, usw.) und sendet an DHCP-Server
- Die DHCP-Antwort des DHCP-Servers kommt zuerst zur RELAY-Komponente
- Nachdem RELAY die Parameter der Option 82 (gi-Adresse, Server-Außerkraftsetzung usw.) entfernt hat, wird das Paket an die DHCP-Snooping-Komponente übergeben
- Die Snooping-Komponente überprüft die RID (Router-ID) und entfernt, wenn sie nicht lokal ist, nicht die Option 82, Unteroption 1 und 2

- Fabric-Relays (da RID nicht lokal ist) - Paket wird direkt an Remote-Client weitergeleitet
- Verwendet den Client-Mac und injiziert die Bridge. Die Hardware führt eine Client-MAC-Suche durch und leitet das Paket mit VXLAN-Encap an den ursprünglichen L2VTEP weiter.

L2VTEP

Konfigurieren der evpn-Instanz

<#root>

```
Leaf-01#
```

show run | beg l2vpn evpn instance 201

```
l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress
```

DHCP-Snooping aktivieren

<#root>

Leaf-01#

show run | sec dhcp snoop

ip dhcp snooping vlan 101,

201

ip dhcp snooping

CGW

Konfigurieren der evpn-Instanz

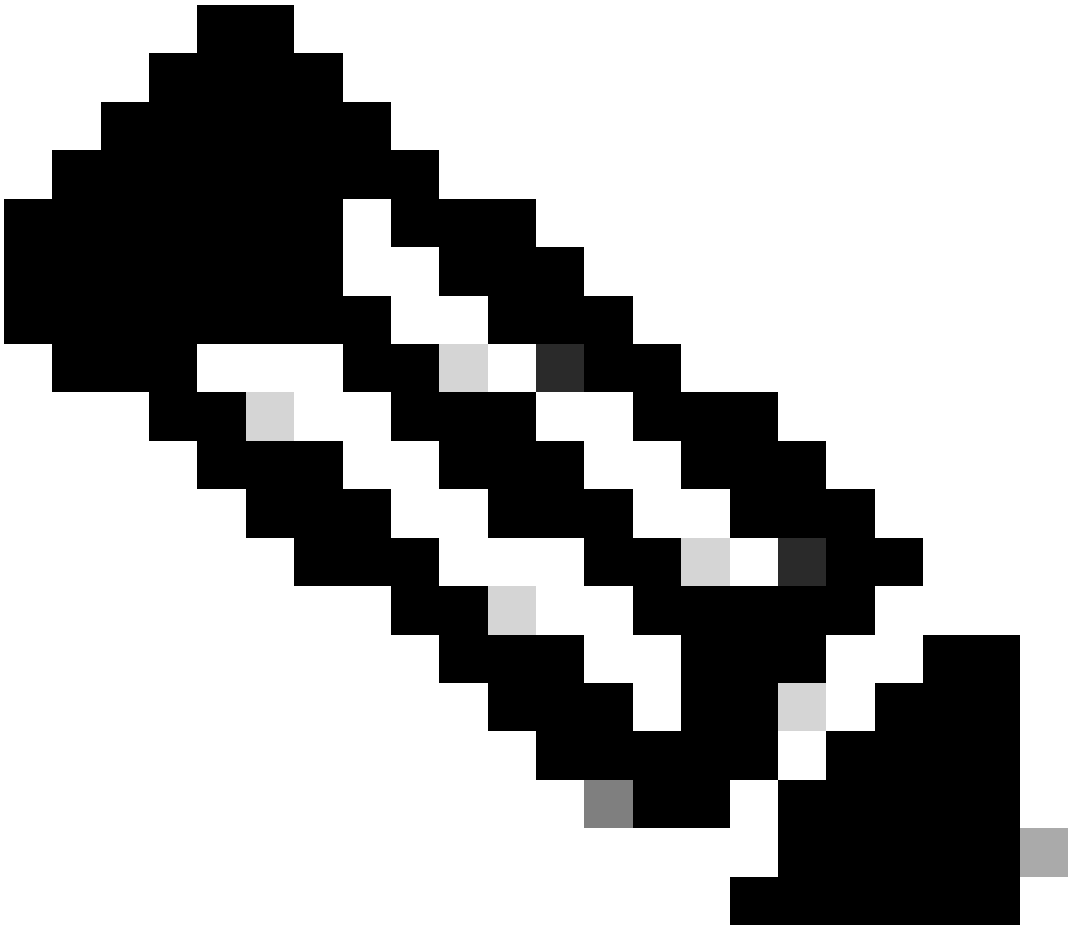
<#root>

```
Border#
```

sh run | s l2vpn evpn instance 201

```
l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
```

```
 replication-type ingress

default-gateway advertise enable  <-- Enable to add BGP DEF GW ext. community attribute
```



> Hinweis: Das Attribut "DEF GW" ist wichtig, damit L2-Relay weiß, wer das DHCP-Paket kapseln und senden muss.

DHCP-Snooping aktivieren

<#root>

```
Border#

sh run | s dhcp snoop

ip dhcp snooping vlan 101,
```

```
201

ip dhcp snooping
```

Stellen Sie sicher, dass das DHCP-Relay die richtige Konfiguration für die Handhabung der zusätzlichen Optionen aufweist.

```
<#root>

Border#

sh run int vl 201


Building configuration...

interface Vlan201
 mac-address 0000.beef.cafe
 vrf forwarding red

 ip dhcp relay information option vpn-id  <-- Ensure the vrf info is passed to the server



ip dhcp relay source-interface Loopback0 <-- Sets the relay source interface to the loopback


 ip address 10.1.201.1 255.255.255.0

ip helper-address global 10.1.33.33      <-- In this scenario the DHCP server is in the global routing t
```

Verifizieren (Standard-CGW-Bereitstellung)

Gateway-Präfix (Leaf)

```
<#root>

Leaf-01#

sh bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.201.1


BGP routing table entry for [2][172.16.255.3:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24, version 8964
Paths: (1 available, best #1,

table evi_201

)

<-- In the EVI context for the segment


Not advertised to any peer
```

```
Refresh Epoch 3
Local, imported path from [2][172.16.255.6:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24 (global)
  172.16.255.6 (metric 30) (via default) from 172.16.255.1 (172.16.255.1)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    EVPN ESI: 00000000000000000000,
```

Label1 20101 <-- Correct segment ID

```
    Extended Community: RT:65001:201 ENCAP:8
```

EVPN DEF GW:0:0 <-- GW attribute added indicating this is GW prefix which L2 Relay uses

Originator: 172.16.255.6

```
, Cluster list: 172.16.255.1
```

<-- Learned from the Border (CGW)

```
    rx pathid: 0, tx pathid: 0x0
    Updated on Nov 14 2023 16:06:40 UTC
```

FED-MATM (Leaf)

<#root>

```
Leaf-01#
```

show platform software fed switch active matm macTable vlan 201

```
VLAN   MAC                 Type  Seq#    EC_Bi  Flags  machandle          siHandle           riHandl
-------------------------------------------------------------------------------------------------------
201    0006.f601.cd42       0x1   32436      0      0  0x71e058dc3368      0x71e058655018      0x0
201    0006.f601.cd01       0x1   32437      0      0  0x71e058dae308      0x71e058655018      0x0
```

201 0000.beef.cafe 0x5000001

```
       0      0     64  0x71e059177138      0x71e058eeb418      0x71e058df81f8      0x0
```

VTEP 172.16.255.6 adj_id 1371

No

<--- The GW MAC shows learnt via the Border Leaf Loopback with the right flags

```
Total Mac number of addresses:: 3
Summary:
Total number of secure addresses:: 0
```

```
Total number of drop addresses:: 0
Total number of lisp local addresses:: 0

Total number of lisp remote addresses:: 1          <---


*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:

MAT_DYNAMIC_ADDR           0x1

  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR               0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS              0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR           0x40  MAT_RES
MAT_DO_NOT_AGE            0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DRO
MAT_DUP_ADDR             0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROU
MAT_WIRELESS_ADDR       0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIR
MAT_DLR_ADDR           0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LIS

MAT_LISP_REMOTE_ADDR 0x1000000

  MAT_VPLS_ADDR        0x2000000

MAT_LISP_GW_ADDR     0x4000000                                  <-- these 3 values added = 0x5000001 (not
```

Lokale MAC (Leaf)

<#root>

```
Leaf-01#

show switch


Switch/Stack Mac Address : 682c.7bf8.8700 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------
*1       Active

682c.7bf8.8700

     1      V01     Ready

<--- Use to validate the Agent ID in DHCP Option 82
```

DHCP-Snooping (Leaf und CGW)

<#root>

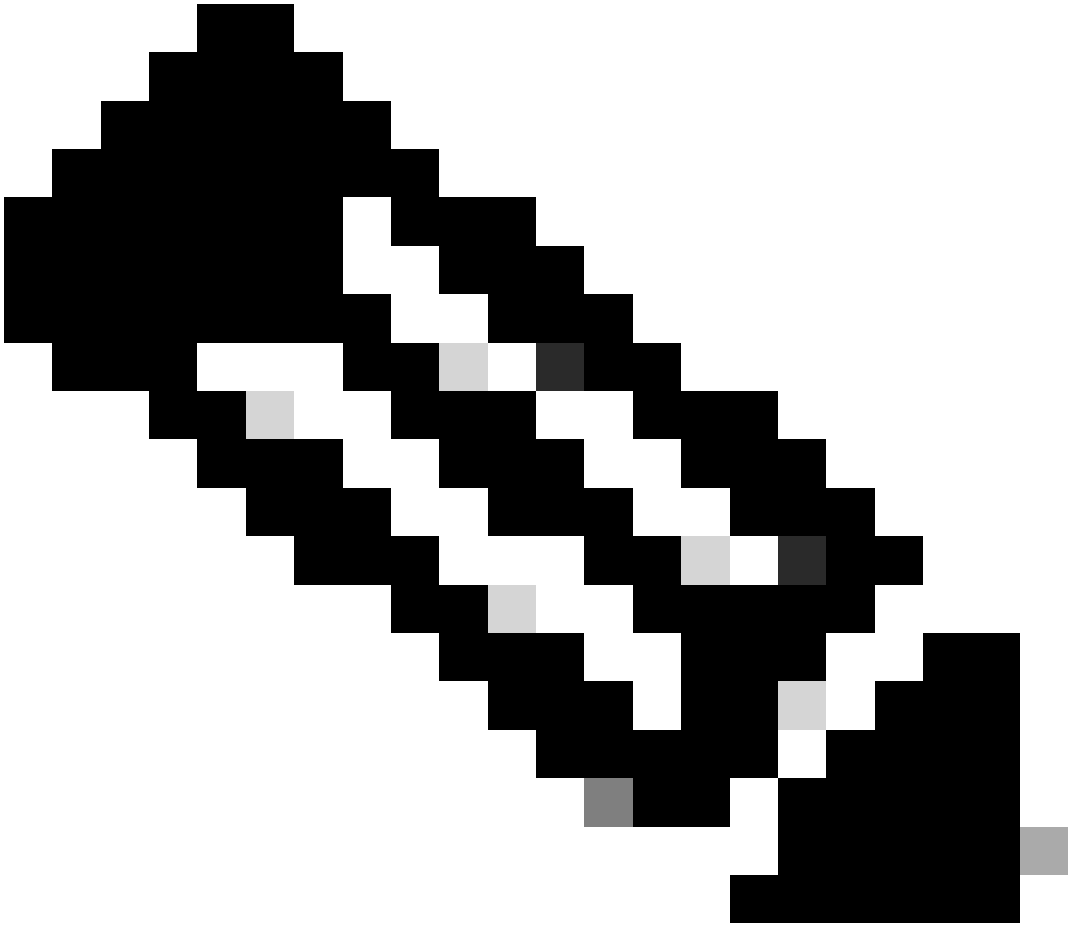
```
Leaf-01#

show ip dhcp snooping


Switch DHCP snooping is enabled
```

```
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
101,201

DHCP snooping is operational on following VLANs:


101,201



Insertion of option 82 is enabled
circuit-id default format: vlan-mod-port
remote-id: 682c.7bf8.8700 (MAC)          <--- Leaf-01 adds the switch MAC to Option 82 to indicate to CG



CGW#

show ip dhcp snooping



Switch DHCP snooping is enabled


Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
101,201

DHCP snooping is operational on following VLANs:


101,201
```

Konfigurieren (teilweise isoliert, geschützt)

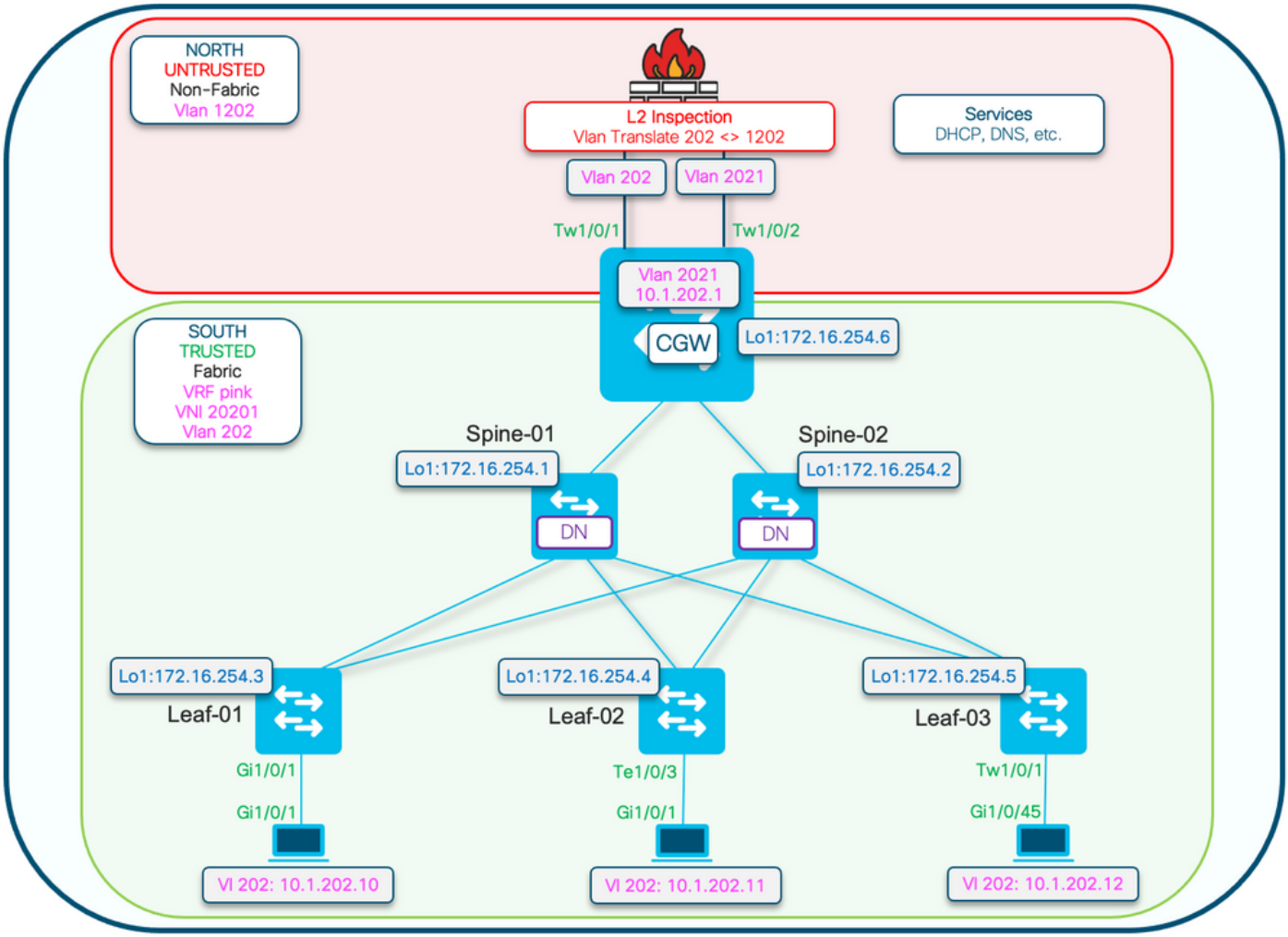
DHCP-Snooping auf dem Access Leaf verlässt sich auf die Standard-Gateway-Route vom CGW, um die Gateway-MAC zum Weiterleiten von DHCP-Paketen zu erlernen.

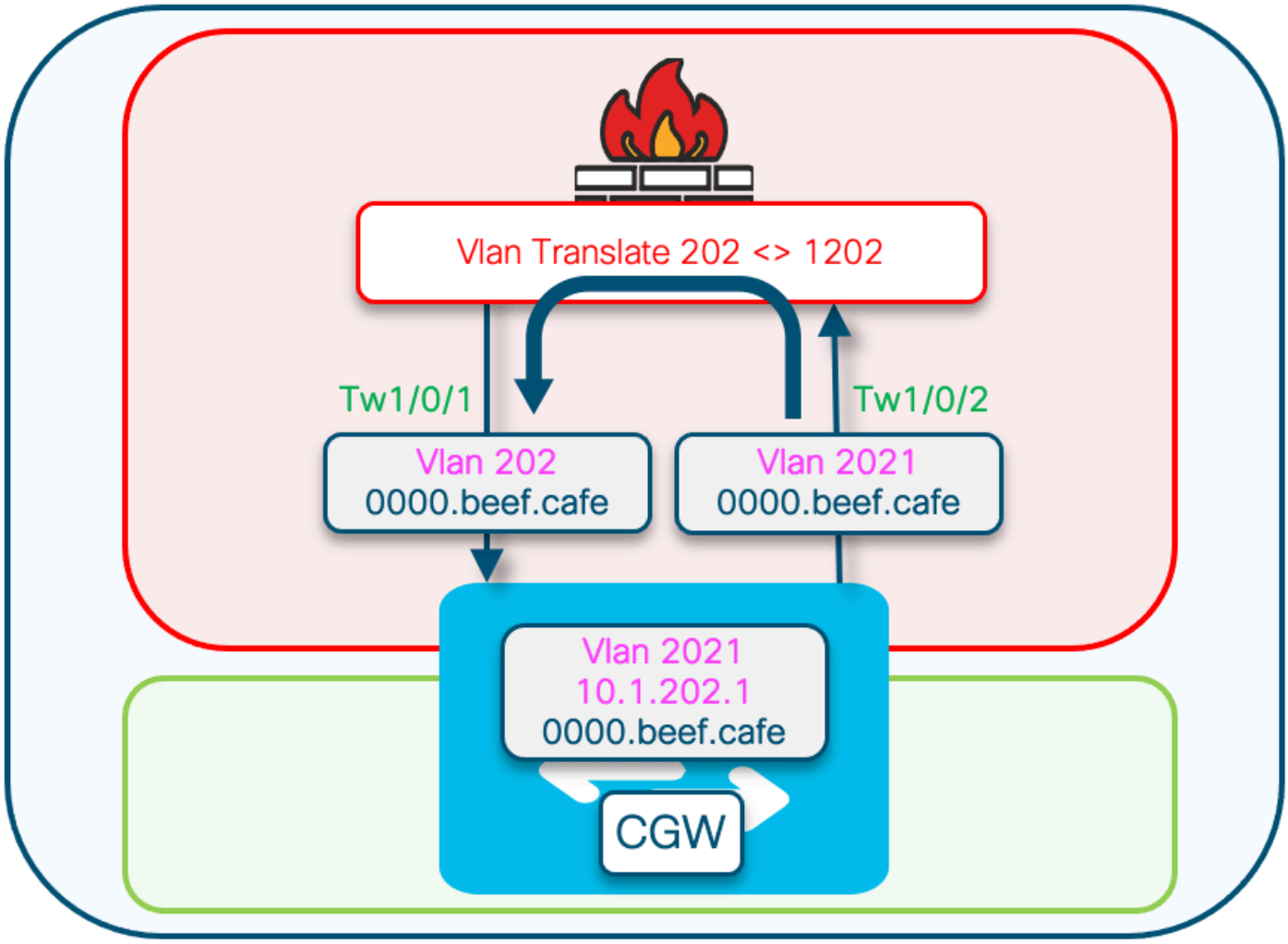
- Bei Verwendung des partiell isolierten Designs mit externem Gateway sind auf dem CGW zusätzliche Konfigurationen erforderlich, um die MAC-IP RT2 mit dem DEF GW-Attribut (Default Gateway) anzukündigen.



Hinweis: Hinweis: In diesem Abschnitt wird auch eine Implementierung eines vollständig isolierten geschützten Segments beschrieben, bei der ebenfalls ein GW verwendet wird, das in der Fabric angezeigt wird (im Gegensatz zu GW außerhalb der Fabric).

Netzwerkdiagramm


NORTH
UNTRUSTED
Non-Fabric
Vlan 1202
L2 Inspection
Vlan Translate 202 <> 1202
Services
DHCP, DNS, etc.
Vlan 202
Vlan 2021
Tw1/0/1
Tw1/0/2
Vlan 2021
10.1.202.1
CGW
Lo1:172.16.254.6
SOUTH
TRUSTED
Fabric
VRF pink
VNI 20201
Vlan 202
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Lo1:172.16.254.4
Leaf-02
Lo1:172.16.254.5
Leaf-03
Gi1/0/1
Gi1/0/1
Te1/0/3
Gi1/0/1
Tw1/0/1
Gi1/0/45
Vl 202: 10.1.202.10
Vl 202: 10.1.202.11
Vl 202: 10.1.202.12



L2 VTEP (Leaf) - Schlüsseldetails

Anforderungspaket kommt vom Client

- Verwenden Sie die von GW angegebene Standard-CGW-MAC.
- Wenn mehr als ein GW vorhanden ist, wird zuerst GW MAC verwendet.
- Wandelt die äußere MAC-Adresse (vom Client initiiert: D und R in DORA) in die Unicast-GW-MAC um und leitet sie an den CGW weiter

DHCP Snooping fügt hinzu: Option 82 Unteroptionen: Circuit und RID

(RID wird von der Response Pkt-Verarbeitung auf dem CGW verwendet)

(Informiert CGW über sein nicht lokales und auf Fabric basierendes Relay zurück zu L2VTEP)

<#root>

```
Option: (82) Agent Information Option
        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a00080000277501010000

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000
```

682c7bf88700 <-- switch base mac 682c.7bf8.8700 (from 'show switch')

- Vom CGW empfangene Response-Pakete über den VXLAN-Tunnel
- Leaf Strips Option 82.
- Fügt Bindungseinträge mit der Clientquellenschnittstelle hinzu. (vxlan-mod-port gibt die Client-Quellschnittstelle an)..
- Antwortpaket an Client weitergeleitet

L3 VTEP (CGW) - Hauptdetails

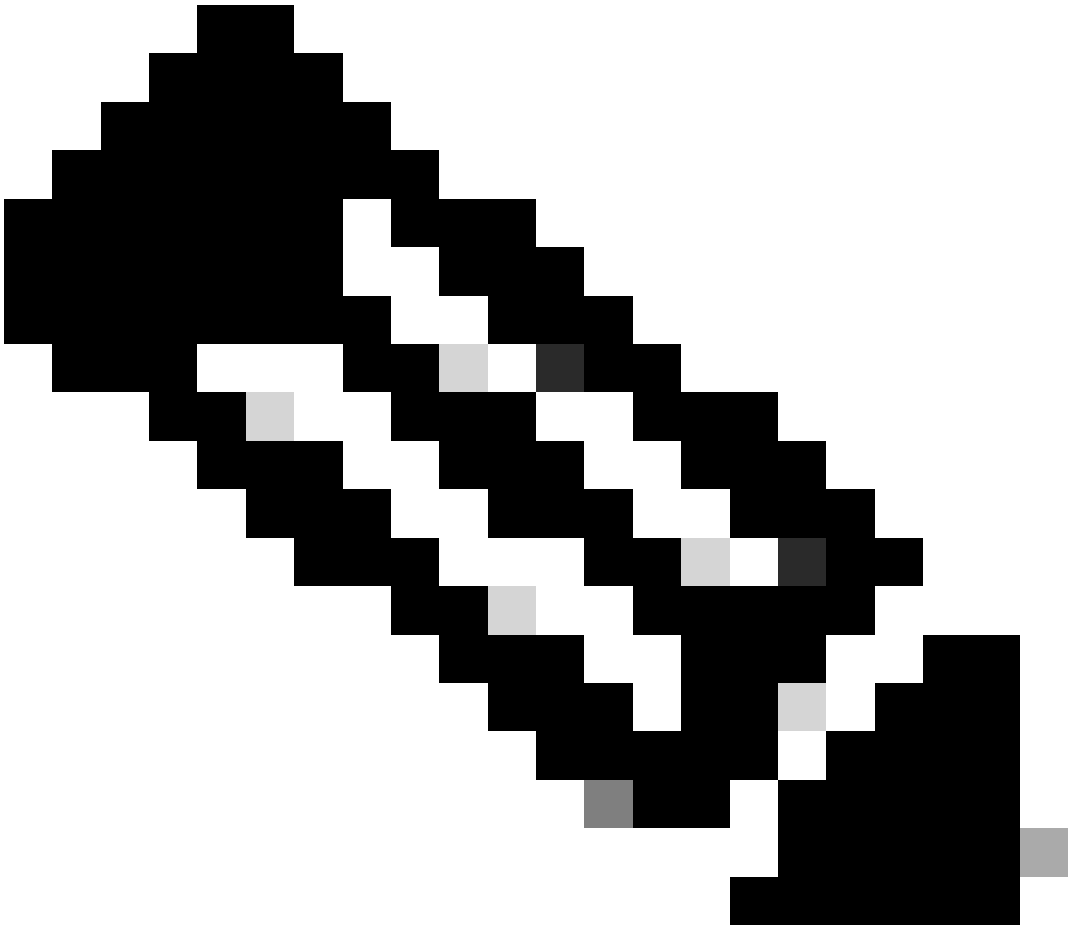
- Aktivieren Sie DHCP SNOOPING
- Aktivieren Sie DHCP RELAY in SVI
- Die Anfrage wird von L2VTEP empfangen und an das Relay weitergeleitet
- Relay fügt weitere Option 82 Unteroptionen hinzu (gi, server override, usw.) und sendet an DHCP-Server
- Die DHCP-Antwort des DHCP-Servers kommt zuerst zur RELAY-Komponente
- Nachdem RELAY die Parameter der Option 82 (gi-Adresse, Server-Außerkraftsetzung usw.) entfernt hat, wird das Paket an die DHCP-Snooping-Komponente übergeben
- Die Snooping-Komponente überprüft die RID (Router-ID) und entfernt, wenn sie nicht lokal ist, nicht die Option 82, Unteroption 1 und 2
- Fabric-Relays (da RID nicht lokal ist) - Paket wird direkt an Remote-Client weitergeleitet
- Verwendet den Client-Mac und injiziert die Bridge. Die Hardware führt eine Client-MAC-Suche durch und leitet das Paket mit VXLAN-Encap an den ursprünglichen L2VTEP weiter.

Erforderliche Schritte zur Unterstützung von DHCP L2 Relay:

1. Lokales IP-Lernen aktivieren
2. Erstellen einer Richtlinie mit deaktivierter Entschlackung
3. Verbindung zu externen Gateway-EVI/VLANs
4. Hinzufügen statischer Einträge zur Nachverfolgungstabelle für externe Gateway-MAC-IP
5. Erstellen einer BGP-Routenübersicht für RT2-MAC-IP-Präfixe und Festlegen der erweiterten Standard-Gateway-Community
6. Routing-Map auf Nachbarn des BGP-Routen-Reflektors anwenden

7. Stellen Sie sicher, dass das DHCP-Relay die richtige Konfiguration für die Handhabung der zusätzlichen Option aufweist.

8. Konfigurieren von DHCP-Snooping für Fabric-VLAN und externes GW-VLAN



Hinweis: Auf den Access-Leafs sind keine Konfigurationsänderungen erforderlich, um DHCP L2-Relay mit externem Gateway zu unterstützen.

CGW

Lokales IP-Lernen aktivieren

<#root>

```
CGW#

show running-config | beg l2vpn evpn instance 202

l2vpn evpn instance 202 vlan-based
 encapsulation vxlan
 replication-type ingress

 ip local-learning enable


<-- to advertise RT-2 with default gateway EC, ip local-learning must be enabled on the CGW.


    Use additional device-tracking policy shown in the next output to prevent MAC-IP binding flapping wh

 multicast advertise enable

<--- There is no default-gateway advertise enable cli here, as the SVI (Vlan 2021) used by this segment
```

Erstellen einer Richtlinie mit deaktivierter Entschlackung

<#root>

```
device-tracking policy dt-no-glean <-- Configure device tracking policy to prevent MAC-IP flapping

 security-level glean
 no protocol ndp
 no protocol dhcp6
 no protocol arp
 no protocol dhcp4
```

Verbindung zu externen Gateway-EVI/VLANs

<#root>

```
CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

 device-tracking attach-policy dt-no-glean <-- apply the new device tracking policy to the vlan configur
```

Hinzufügen statischer Einträge zur Geräteverfolgungstabelle für externe Gateway-MAC-IP

<#root>

```
device-tracking binding vlan 202 10.1.202.1 interface TwentyFiveGigE1/0/1 0000.beef.cafe
```

<-- All static entries in device tracking table should be for external gateway mac-ip's.

If there is any other static entry in device tracking table, match ip/ipv6 configurations in route m

Erstellen einer BGP-Routenübersicht für RT2-MAC-IP-Präfixe und Festlegen der erweiterten Standard-Gateway-Community

<#root>

```
route-map CGW_DEF_GW permit 10
```

match evpn route-type 2-mac-ip <-- match RT2 type MAC-IP

set extcommunity default-gw <-- Set Default-gateway (DEF GW 0:0) extended community

```
route-map CGW_DEF_GW permit 20
```

Routing-Map auf Nachbarn des BGP-Routen-Reflektors anwenden

<#root>

```
CGW#
```

sh run | sec router bgp

```
address-family l2vpn evpn
 neighbor 172.16.255.1 activate
 neighbor 172.16.255.1 send-community both
 neighbor 172.16.255.1
```

route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR

```
 neighbor 172.16.255.2 activate
 neighbor 172.16.255.2 send-community both
 neighbor 172.16.255.2
```

route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR

Stellen Sie sicher, dass das DHCP-Relay die richtige Konfiguration für die Handhabung der

zusätzlichen Optionen aufweist.

<#root>

```
CGW#

show run int vl 2021

Building configuration...

Current configuration : 315 bytes
!
interface Vlan2021
 mac-address 0000.beef.cafe
 vrf forwarding pink

 ip dhcp relay information option vpn-id   <-- Ensure the vrf info is passed to the server
 ip dhcp relay source-interface Loopback0  <-- sets the relay source interface to the loopback

 ip address 10.1.202.1 255.255.255.0

 ip helper-address global 10.1.33.33       <-- In this scenario the next hop to the DHCP server is in th

 no ip redirects
 ip local-proxy-arp
 ip route-cache same-interface
 no autostate
```

Konfigurieren von DHCP-Snooping für Fabric-VLANs und das externe GW-VLAN

<#root>

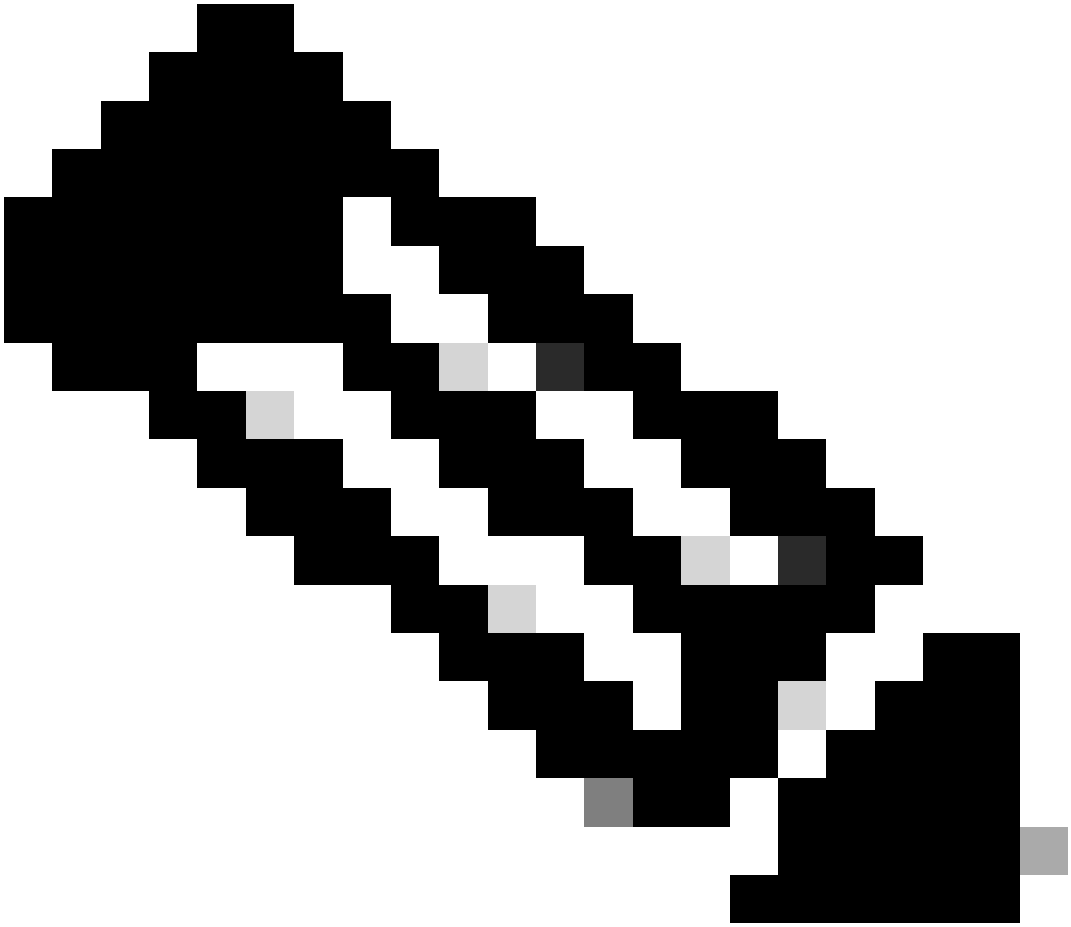
```
Leaf01#

sh run | s dhcp snoop

ip dhcp snooping vlan 202
ip dhcp snooping

CGW#

sh run | s dhcp snoop

ip dhcp snooping vlan 202,2021  <-- snooping is required in both the fabric vlan and the external GW vla

ip dhcp snooping
```

Stellen Sie sicher, dass der Uplink zum DHCP-Server auf dem CGW vertrauenswürdig ist.

<#root>

```
CGW#

sh run int tw 1/0/1
```

```
interface TwentyFiveGigE1/0/1
 switchport trunk allowed vlan 202
 switchport mode trunk

 ip dhcp snooping trust

end

CGW#

sh run int tw 1/0/2


interface TwentyFiveGigE1/0/2
 switchport trunk allowed vlan 33,2021
 switchport mode trunk

 ip dhcp snooping trust

end
```



Hinweis: Aufgrund der Platzierung des Servers auf dem Firewall-Gerät wurde die

---

Vertrauensstellung auf beiden Verbindungen konfiguriert, die zu diesem Gerät führen. In dem vergrößerten Diagramm können Sie sehen, dass das Angebot in diesem Design sowohl bei Tw1/0/1 als auch bei Tw1/0/2 ankommt.

Überprüfen (teilweise isoliert und geschützt)

Gateway-Präfix (Leaf)

<#root>

```
Leaf01#

show bgp l2vpn evpn route-type 2 0 0000.beef.cafe 10.1.202.1

BGP routing table entry for [2][172.16.254.3:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24, version 3411
Paths: (1 available, best #1, table evi_202)
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000, Label1 20201
      Extended Community: RT:65001:202 ENCAP:8

EVPN DEF GW:0:0       <-- GW attribute added indicating this is GW prefix which L2 Relay uses

      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 19 2023 19:57:25 UTC
```

FED-MATM (Leaf)

Bestätigen Sie, dass der Leaf die CGW-Remote-MAC in der Hardware installiert hat.

<#root>

```
Leaf01#

show platform software fed switch active matm macTable vlan 202

VLAN   MAC                 Type  Seq#    EC_Bi  Flags  machandle          siHandle           riHandl
-------------------------------------------------------------------------------------------------------
202    0006.f601.cd01       0x1    1093      0      0  0x71e05918f138     0x71e05917a1a8     0x0

202    0006.f601.cd44       0x1   14309      0      0  0x71e058cdc208     0x71e05917a1a8     0x0

202

 0000.beef.cafe  0x5000001
```

```
       0      0     64  0x71e058ee5d88      0x71e059195f88      0x71e059171678      0x0
```

<--- The GW MAC shows learnt via the Border Leaf Loopback

```
Total Mac number of addresses:: 3
Summary:
Total number of secure addresses:: 0
Total number of drop addresses:: 0
Total number of lisp local addresses:: 0
Total number of lisp remote addresses:: 1
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
```

MAT_DYNAMIC_ADDR 0x1

```
  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR               0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS              0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR           0x40  MAT_RES
MAT_DO_NOT_AGE            0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DRO
MAT_DUP_ADDR             0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROU
MAT_WIRELESS_ADDR       0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIR
MAT_DLR_ADDR           0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LIS
```

MAT_LISP_REMOTE_ADDR 0x1000000

```
  MAT_VPLS_ADDR
```

0x2000000 MAT_LISP_GW_ADDR   0x4000000

<-- these 3 values added = 0x5000001 (note that 0x4000000 = GW type address

Lokale MAC (Leaf)

<#root>

```
Leaf01#
```

show switch

```
Switch/Stack Mac Address : 682c.7bf8.8700 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
------------------------------------------------------------------------------------
*1       Active
```

682c.7bf8.8700

```
     1      V01     Ready
```

<-- this is the MAC that will be added to DHCP Agent Remote ID

DHCP-Snooping (Leaf und CGW)

Bestätigen, dass DHCP-Snooping auf dem Leaf im Fabric-VLAN aktiviert ist

<#root>

Leaf01#

show ip dhcp snooping

Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
202

DHCP snooping is operational on following VLANs: <-- Snooping on in the Fabric Vlan 202

<...snip...>

Insertion of option 82 is enabled
**   circuit-id default format: vlan-mod-port**
**   remote-id: 682c.7bf8.8700 (MAC) <--- Remote ID (RID) inserted by Leaf to DHCP packets**

<...snip...>

Vergewissern Sie sich, dass DHCP-Snooping auf dem CGW in der Fabric und den externen Gateway-VLANs aktiviert ist.

<#root>

CGW#

show ip dhcp snooping

Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
202,2021

DHCP snooping is operational on following VLANs: <-- Snooping on in the Fabric and External GW Vlans 202,2021

<...snip...>

DHCP snooping trust/rate is configured on the following Interfaces:

Interface Trusted Allow option Rate limit (pps)
--- --- --- ---

TwentyFiveGigE1/0/1

yes yes unlimited

<-- Trust set on ports the OFFER arrives on

Interface Trusted Allow option Rate limit (pps)
--- --- --- ---
  Custom circuit-ids:

TwentyFiveGigE1/0/2

yes yes unlimited

<-- Trust set on ports the OFFER arrives on

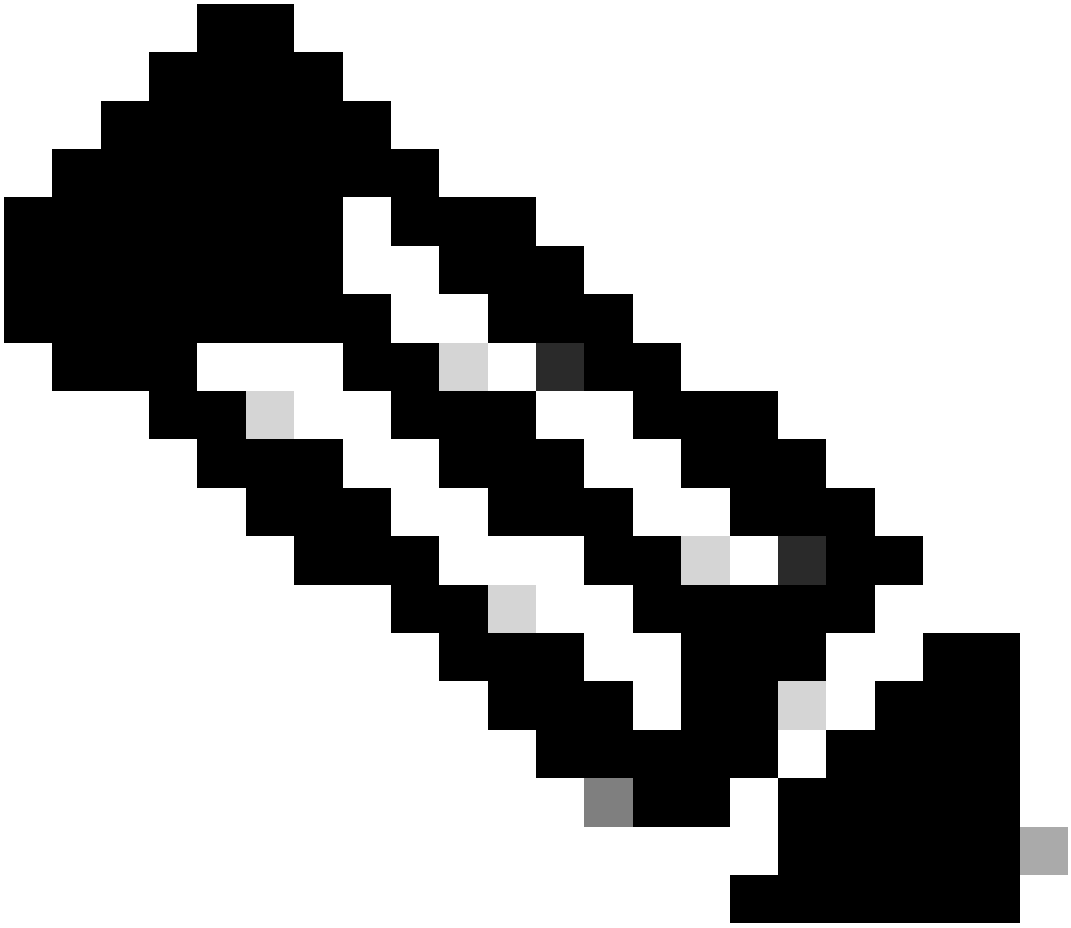
```
  Custom circuit-ids:
```

Bestätigen, dass die DHCP-Snooping-Bindung erstellt wurde

```
<#root>
Leaf01#
show ip dhcp snooping binding
MacAddress


IpAddress
        Lease(sec)  Type           VLAN
Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:06:F6:01:CD:43
10.1.202.10
      34261       dhcp-snooping   202
GigabitEthernet1/0/1  <-- DHCP Snooping has created the binding
Total number of bindings: 1
```

Fehlerbehebung (jeder CGW-Typ)

Mithilfe von Debugging-Programmen kann veranschaulicht werden, wie DHCP-Snooping- und L2-Relay-Prozesse DHCP-Pakete verarbeiten.



Hinweis: Diese Debugging-Typen können für alle Bereitstellungsarten verwendet werden, die CGW mit DHCP L2-Relay verwenden.

Debuggen von DHCP-Snooping (Leaf)

Debug-Snooping zur Bestätigung der Paketverarbeitung

<#root>

```
Leaf01#
debug ip dhcp snooping packet
DHCP Snooping Packet debugging is on
Leaf01#
show debugging
DHCP Snooping packet debugging is on
```

Starten des DHCP-Adressenversuchs für den Host

- Für dieses Dokument wurde ein "shutdown/no shutdown" der SVI durchgeführt, die über DHCP adressiert wird, um den DORA-Austausch auszulösen.
- Für Windows-Server können Sie Folgendes ausführen: ipconfig /release **>** ipconfig /renew

Sammeln Sie die Fehlerbehebungen aus der Anzeigeprotokollierung oder aus dem Terminalfenster.

DHCP-ERKENNUNG

Erkennung erfolgt über den Host-seitigen Port

<#root>

```
*Sep 19 20:16:31.164:

DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)  <-- host facing por


*Sep 19 20:16:31.177:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Gi1/0/1

, MAC da: ffff.ffff.ffff,

MAC sa: 0006.f601.cd43

, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.
*Sep 19 20:16:31.177: DHCP_SNOOPING: add relay information option.
*Sep 19 20:16:31.177:

DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format         <-- Option 82 encoding


*Sep 19 20:16:31.177: DHCP_SNOOPING:VxLAN : vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:31.177:

DHCP_SNOOPING: Encoding opt82 RID in MAC address format           <-- Encoding the switch Remote ID (loc

*Sep 19 20:16:31.177: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6

0x68 0x2C 0x7B 0xF8 0x87 0x0  <-- the switch local MAC 682c.7bf8.8700

*Sep 19 20:16:31.177: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Sep 19 20:16:31.177: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Sep 19 20:16:31.177:

DHCP_SNOOPING: L2RELAY: sent unicast packet to default gw: 0000.beef.cafe vlan 0 src intf GigabitEtherne
```

DHCP-ANGEBOT

Angebot wird über die Fabric Tunnel-Schnittstelle angezeigt

<#root>

*Sep 19 20:16:33.180:

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)

*Sep 19 20:16:33.194:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Tu0, MAC da: 0006.f601

, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.202.18, DHCP siadd
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Sep 19 20:16:33.194: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6

0x68 0x2C 0x7B 0xF8 0x87 0x0 <-- the switch local MAC 682c.7bf8.8700

*Sep 19 20:16:33.194: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_
*Sep 19 20:16:33.194: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Sep 19 20:16:33.194:

DHCP_SNOOPING: opt82 data indicates local packet <-- switch found its own RID in Option 82 paramete

*Sep 19 20:16:33.194: DHCP_SNOOPING: remove relay information option.
*Sep 19 20:16:33.194: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.194:

DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1

*Sep 19 20:16:33.194:

DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43

*Sep 19 20:16:33.194: DHCP_SNOOPING: calling forward_dhcp_reply
*Sep 19 20:16:33.194: platform lookup dest vlan for input_if: Tunnel0, is tunnel, if_output: NULL, if_
*Sep 19 20:16:33.194: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.194: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.194: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
*Sep 19 20:16:33.194: DHCP_SNOOPING: vlan 202 after pvlan check
*Sep 19 20:16:33.207:

DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet1/0/1. <-- sending packet to hos

DHCP-ANFRAGE

Die Anfrage wird vom Host-seitigen Port aus gesehen.

<#root>

*Sep 19 20:16:33.209:

DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet1/0/1)

*Sep 19 20:16:33.222:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

```
, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP
*Sep 19 20:16:33.222: DHCP_SNOOPING: add relay information option.
*Sep 19 20:16:33.222: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Sep 19 20:16:33.222: DHCP_SNOOPING:VxLAN : vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.222: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
*Sep 19 20:16:33.222: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.222: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Sep 19 20:16:33.222: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Sep 19 20:16:33.222:
```

DHCP_SNOOPING: L2RELAY: sent unicast packet to default gw: 0000.beef.cafe vlan 0 src intf GigabitEtherne

DHCP-ACK

Bestätigung wird von der Fabric Tunnel-Schnittstelle empfangen

<#root>

```
*Sep 19 20:16:33.225:
```

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)

```
*Sep 19 20:16:33.238:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Tu0, MAC da: 0006.f601.c

```
, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 10.1.202.10, DHCP siadd
*Sep 19 20:16:33.238: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Sep 19 20:16:33.239: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Sep 19 20:16:33.239: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Sep 19 20:16:33.239:  actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_
*Sep 19 20:16:33.239: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Sep 19 20:16:33.239:
```

DHCP_SNOOPING: opt82 data indicates local packet

```
*Sep 19 20:16:33.239:
```

dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan_id 202

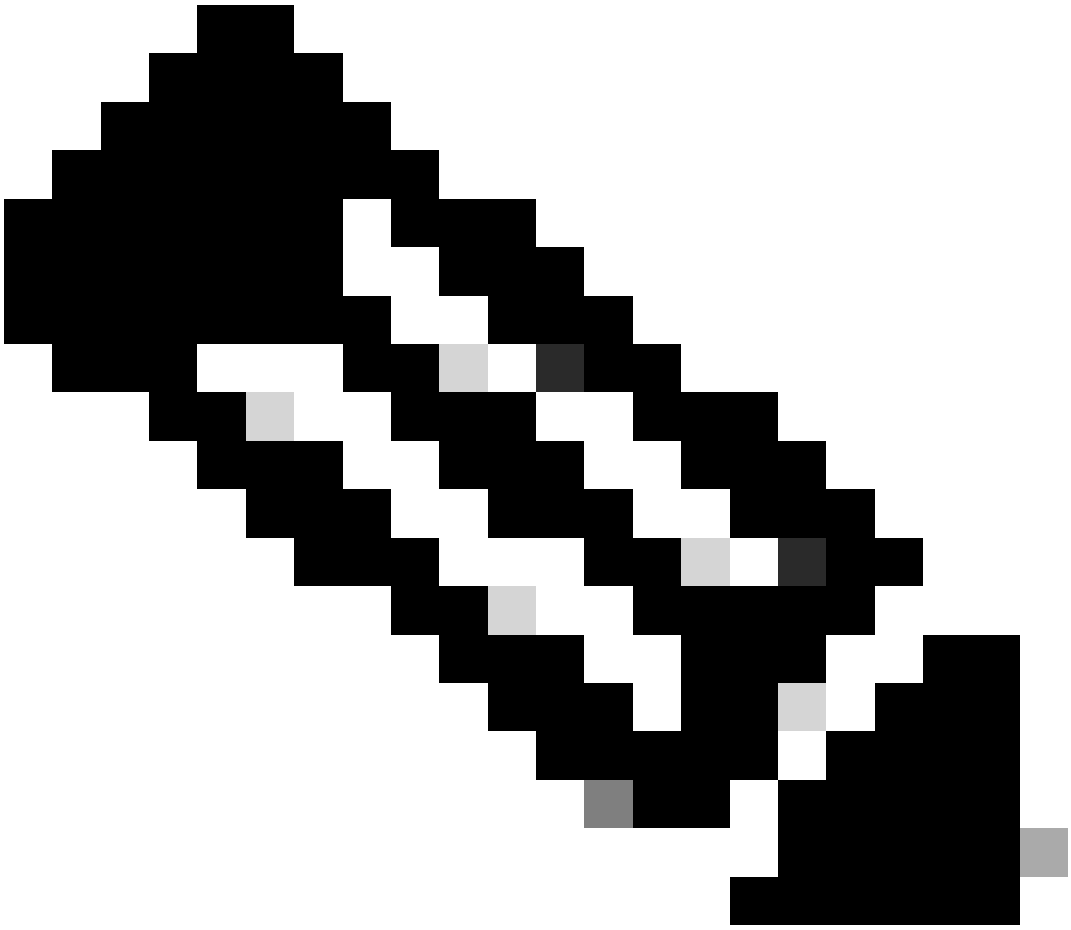
```
*Sep 19 20:16:33.239: DHCP_SNOOPING: opt82 data indicates local packet
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239:
```

DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43

```
*Sep 19 20:16:33.239: DHCP_SNOOPING: Reroute dhcp pak, message type: DHCPACK
*Sep 19 20:16:33.239: DHCP_SNOOPING: remove relay information option.
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
*Sep 19 20:16:33.239: DHCP_SNOOPING: calling forward_dhcp_reply
*Sep 19 20:16:33.239: platform lookup dest vlan for input_if: Tunnel0, is  tunnel, if_output: NULL, if_
*Sep 19 20:16:33.239: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Sep 19 20:16:33.239: DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1
*Sep 19 20:16:33.239: DHCP_SNOOPING: mod 1 port 1 idb Gi1/0/1 found for 0006.f601.cd43
```

```
*Sep 19 20:16:33.239: DHCP_SNOOPING: vlan 202 after pvlan check
*Sep 19 20:16:33.252:
```

DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet1/0/1.



Hinweis: Diese Debugs werden ausgeschnitten. Sie erzeugen einen Speicherauszug des Pakets, die Anmerkung zu diesem Teil des Debugergebnisses ist jedoch nicht Bestandteil des vorliegenden Dokuments.

DHCP Snooping Debugs (CGW)

DHCP-ERKENNUNG

Aufgrund der Art und Weise, wie das Paket über den CGW gesendet und empfangen wird (über die Firewall verteilt), werden die Fehlerbehebungsmaßnahmen zweimal ausgelöst.

Von Fabric an Tunnelschnittstelle eingegangen und Tw 1/0/1 an Firewall in Fabric VLAN 202

gesendet

<#root>

```
*Apr 16 14:37:43.890:
```

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0) <-- Discover sent from Leaf01 a

```
*Apr 16 14:37:43.901: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interfa
*Apr 16 14:37:43.901: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Apr 16 14:37:43.901:
```

DHCP_SNOOPING: bridge packet send packet to port: TwentyFiveGigE1/0/1, pak_vlan 202. <-- Sent to Firewal

Von Firewall auf Tw 1/0/2 in VLAN 2021 ankommen, um an SVI und Helper an DHCP-Server gesendet zu werden

<#root>

```
*Apr 16 14:37:43.901:
```

DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/2) <-- Firewall sends di

```
*Apr 16 14:37:43.911: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interfa
*Apr 16 14:37:43.911:
```

DHCPS BRIDGE PAK: vlan=2021 platform_flags=1   <-- Vlan discover seen is now 2021

```
*Apr 16 14:37:43.911:
```

DHCP_SNOOPING: Packet destined to SVI Mac:0000.beef.cafe

```
*Apr 16 14:37:43.911:
```

DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan2021. <-- Packet punted to CPU for handling b

DHCP-ANGEBOT

Geht vom DHCP-Server zurück zur SVI 2021, wo der Helfer konfiguriert und an die Firewall weitergeleitet wird

<#root>

```
*Apr 16 14:37:45.913:
```

DHCP_SNOOPING: received new DHCP packet from input interface (Vlan2021) <-- Arriving from the DHCP serv

```
*Apr 16 14:37:45.923:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Vl2021

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:45.923: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.924: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.924: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.924:

DHCP_SNOOPING: opt82 data indicates not a local packet

*Apr 16 14:37:45.924: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong fo

<-- This is expected even in working scenario (disregard it)

*Apr 16 14:37:45.924: DHCP_SNOOPING: calling forward_dhcp_reply
*Apr 16 14:37:45.924: platform lookup dest vlan for input_if: Vlan2021, is NOT tunnel, if_output: Vlan2
*Apr 16 14:37:45.924: DHCP_SNOOPING: vlan 2021 after pvlan check
*Apr 16 14:37:45.934:

DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/2. <-- sending back toward the

Von Firewall im Fabric-VLAN und vom CGW an Fabric in Richtung Leaf gesendet

<#root>

*Apr 16 14:37:45.934:

DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1)

*Apr 16 14:37:45.944:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input interface: Twe1/0/1

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.944: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.944: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.945:

DHCP_SNOOPING: opt82 data indicates not a local packet

*Apr 16 14:37:45.945: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Apr 16 14:37:45.945: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:45.945: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:45.945:

DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 202 from Twe1/0/1 <-- L2 RELAY f

DHCP-ANFRAGE

<#root>

*Apr 16 14:37:45.967:

DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)

*Apr 16 14:37:45.978:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

, input interface: Tu0, MAC da: 0000.beef.cafe, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP sa:
*Apr 16 14:37:45.978: DHCPS BRIDGE PAK: vlan=202 platform_flags=1
*Apr 16 14:37:45.978:

DHCP_SNOOPING: bridge packet send packet to port: TwentyFiveGigE1/0/1, pak_vlan 202. <-- Send toward Fir

<#root>

*Apr 16 14:37:45.978:

DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/2) <-- Receive from Fire

*Apr 16 14:37:45.989:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

, input interface: Twe1/0/2, MAC da: 0000.beef.cafe, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP
*Apr 16 14:37:45.989: DHCPS BRIDGE PAK: vlan=2021 platform_flags=1
*Apr 16 14:37:45.989: DHCP_SNOOPING: Packet destined to SVI Mac:0000.beef.cafe
*Apr 16 14:37:45.989:

DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan2021. <-- Punt to CPU / DHCP helper

DHCP-ACK

<#root>

*Apr 16 14:37:45.990:

DHCP_SNOOPING: received new DHCP packet from input interface (Vlan2021) <-- Packet back to SVI from DHC

*Apr 16 14:37:46.000:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Vl2021

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:46.000: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:46.001: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:46.001: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:46.001:

DHCP_SNOOPING: opt82 data indicates not a local packet <-- found this is coming from Leaf01 RID

*Apr 16 14:37:46.001: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong fo
*Apr 16 14:37:46.001: DHCP_SNOOPING: calling forward_dhcp_reply
*Apr 16 14:37:46.001: platform lookup dest vlan for input_if: Vlan2021, is NOT tunnel, if_output: Vlan2
*Apr 16 14:37:46.001: DHCP_SNOOPING: vlan 2021 after pvlan check
*Apr 16 14:37:46.011:

DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/2. <-- Send to Firewall

<#root>

*Apr 16 14:37:46.011:

DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1) <-- Coming back in f

*Apr 16 14:37:46.022:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Twe1/0/1,

 MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:46.022: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:46.022: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:46.022:

DHCP_SNOOPING: opt82 data indicates not a local packet

*Apr 16 14:37:46.022: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022: DHCP_SNOOPING: can't find client's destination port, packet is assumed to be not
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022:

DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 202 from Twe1/0/1 <-- Send packe

Eingebettete Erfassung

Verwendung von EPC zur Überprüfung des DHCP-Paketaustauschs und der korrekten Parameter

- Dies wird aus der Perspektive des CGW gezeigt, aber der Prozess kann auf Leaf wiederholt werden, um den Paketaustausch zu überprüfen.
- Dieses Beispiel zeigt die Erkennung, da Prozess und Analyse für die anderen DHCP-Pakete identisch sind.

Überprüfen der Route zum Leaf-Loopback

<#root>

```
CGW#

show ip route 172.16.254.3

Routing entry for 172.16.254.3/32
  Known via "ospf 1", distance 110, metric 3, type intra area
  Last update from 172.16.1.25 on TwentyFiveGigE1/0/47, 2w6d ago
  Routing Descriptor Blocks:
  * 172.16.1.29, from 172.16.255.3, 2w6d ago,

via TwentyFiveGigE1/0/48

      Route metric is 3, traffic share count is 1
    172.16.1.25, from 172.16.255.3, 2w6d ago,

via TwentyFiveGigE1/0/47

      Route metric is 3, traffic share count is 1
```

Konfigurieren Sie die Erfassung für Links, die dem Leaf01 gegenüberliegen.

```
monitor capture 1 interface TwentyFiveGigE1/0/47 BOTH
monitor capture 1 interface TwentyFiveGigE1/0/48 BOTH
monitor capture 1 match any
monitor capture 1 buffer size 100
monitor capture 1 limit pps 1000
```

Starten der Erfassung, Auslösen der Anforderung einer DHCP-IP-Adresse durch den Host, Beenden der Erfassung

<#root>

```
monitor capture 1 start
  (have the host request dhcp ip)
monitor capture 1 stop
```

Zeigen Sie das Erfassungsergebnis an, beginnend mit der DHCP-Erkennung (achten Sie auf die Transaktions-ID, um sicherzustellen, dass es sich um dasselbe DORA-Ereignis handelt).

<#root>

```
CGW#
show monitor cap 1 buff brief | i DHCP


 16
  12.737135      0.0.0.0 -> 255.255.255.255 DHCP 434
DHCP Discover
 -
Transaction ID 0x78b <-- Discover starts at Frame 16 with all same transaction ID
   18  14.740041   10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP
Offer
    - Transaction ID
0x78b
   19  14.742741      0.0.0.0 -> 255.255.255.255 DHCP 452 DHCP
Request
  - Transaction ID
0x78b
   20  14.745646   10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP
ACK
      - Transaction ID
0x78b
```

<#root>

```
CGW#
sh mon cap 1 buff detailed | b Frame 16
Frame 16:
 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface /tmp/epc_ws/wif_to_ts_pipe,
    [Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]
Ethernet II,
Src: dc:77:4c:8a:6d:7f
 (dc:77:4c:8a:6d:7f),
Dst: 10:f9:20:2e:9f:82
 (10:f9:20:2e:9f:82)
```

<-- Underlay Interface MACs

    Type: IPv4 (0x0800)
Internet Protocol Version 4,

Src: 172.16.254.3, Dst: 172.16.254.6

User Datagram Protocol, Src Port: 65281,

Dst Port: 4789   <-- VXLAN Port

Virtual eXtensible Local Area Network
    VXLAN Network Identifier

(VNI): 20201   <-- Correct VNI / Segment

    Reserved: 0
Ethernet II,

Src: 00:06:f6:01:cd:43

 (00:06:f6:01:cd:43),

Dst: 00:00:be:ef:ca:fe

 (00:00:be:ef:ca:fe)

<-- Inner Packet destined to CGW MAC

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

Src Port: 68, Dst Port: 67   <-- DHCP ports

Dynamic Host Configuration Protocol (Discover)   <-- DHCP Discover Packet

 Client MAC address: 00:06:f6:01:cd:43

 (00:06:f6:01:cd:43)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP

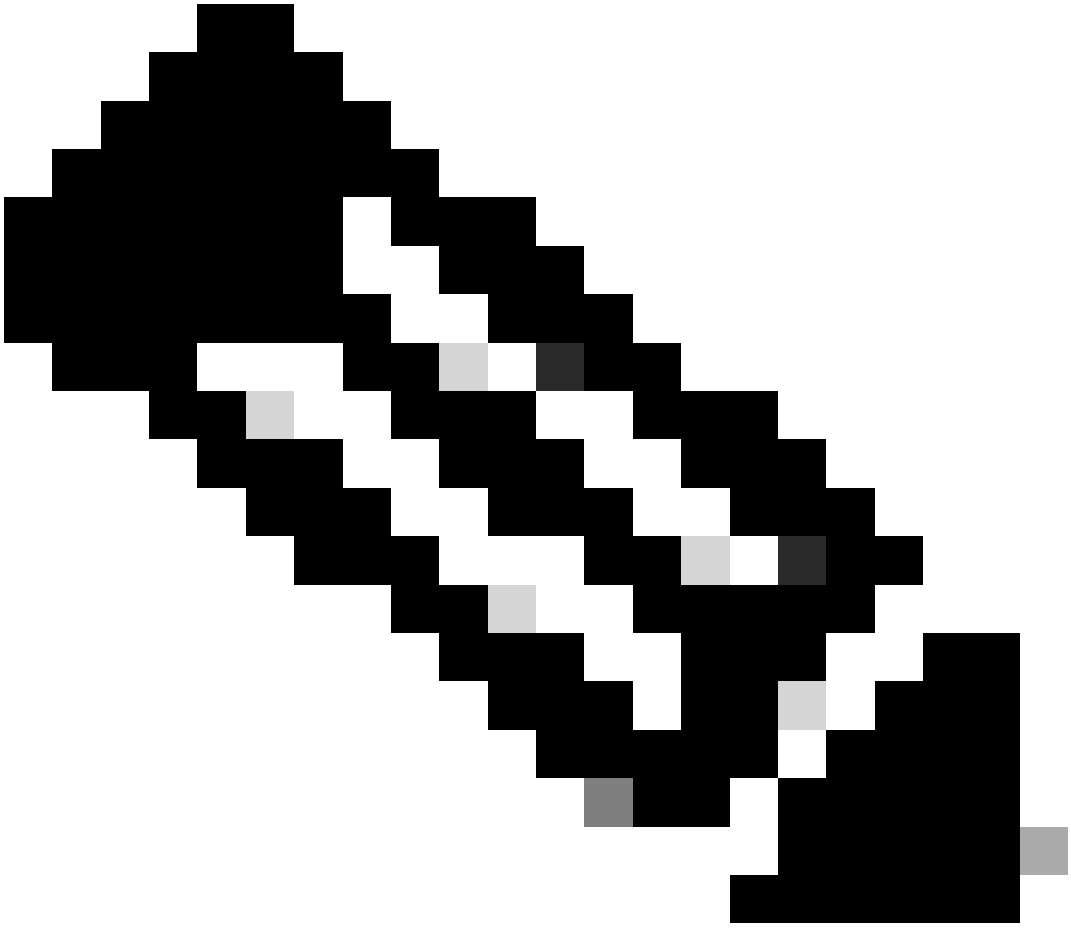
 Option: (53) DHCP Message Type (Discover)

        Length: 1
        DHCP: Discover (1)
    Option: (57) Maximum DHCP Message Size
        Length: 2
        Maximum DHCP Message Size: 1152
    Option: (61) Client identifier
        Length: 27
        Type: 0
        Client Identifier: cisco-0006.f601.cd43-Vl202
    Option: (12) Host Name
        Length: 17

Host Name: 9300-HOST-3750X-2

    Option: (55) Parameter Request List

```
        Length: 8
        Parameter Request List Item: (1) Subnet Mask
        Parameter Request List Item: (6) Domain Name Server
        Parameter Request List Item: (15) Domain Name
        Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
        Parameter Request List Item: (3) Router
        Parameter Request List Item: (33) Static Route
        Parameter Request List Item: (150) TFTP Server Address
        Parameter Request List Item: (43) Vendor-Specific Information
    Option: (60) Vendor class identifier
        Length: 8
        Vendor class identifier: ciscopnp


Option: (82) Agent Information Option

        Length: 24
        Option 82 Suboption: (1) Agent Circuit ID
            Length: 12
            Agent Circuit ID: 010a000800004ee901010000


Option 82 Suboption: (2) Agent Remote ID

            Length: 8


Agent Remote ID:

000

6682c7bf88700  <-- switch base mac 682c.7bf8.8700 (from 'show switch')

    Option: (255) End
        Option End: 255
```



Hinweis: Das Erfassungstool kann für alle Leafs oder CGW verwendet werden, um den letzten Punkt zu bestimmen, an dem ein Teil des DHCP-DORA-Austauschs fehlerhaft ist.

Überprüfen Sie die Snooping-Statistiken für

<#root>

```
Leaf01#

show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping                  = 1288


Packets Dropped Because

   IDB not known                                     = 0
   Queue full                                        = 0
   Interface is in errdisabled                       = 0
   Rate limit exceeded                               = 0
   Received on untrusted ports                       = 0
```

```
   Nonzero giaddr                                  = 0
   Source mac not equal to chaddr                  = 0
   No binding entry                                = 0
   Insertion of opt82 fail                         = 0
   Unknown packet                                  = 0
   Interface Down                                  = 0
   Unknown output interface                        = 0
   Misdirected Packets                             = 0
   Packets with Invalid Size                       = 0
   Packets with Invalid Option                     = 0

<-- Look for any drop counter that is actively incrementing when the issue is seen.
```

Überprüfen des Puntpfads für DHCP-Snooping

- CoPP ist die Hauptkomponente, bei der Pakete im Punktpfad verworfen werden.

<#root>

```
Leaf01#

show platform hardware switch active qos queue stats internal cpu policer

                          CPU Queue Statistics
============================================================================================
                                             (default) (set)     Queue        Queue
QId

PlcIdx

  Queue Name                Enabled   Rate     Rate      Drop(Bytes)

Drop(Frames)

--------------------------------------------------------------------------------------------
17

6


DHCP Snooping

               Yes     400       400      0

 0

              CPU Queue Policer Statistics
============================================================================

Policer

    Policer Accept   Policer Accept  Policer Drop  Policer Drop

Index

         Bytes          Frames        Bytes          Frames
----------------------------------------------------------------------
```

```
6          472723           1288            0             0
```

Ein weiterer sehr hilfreicher Befehl, um festzustellen, wo eine mögliche Paketflut auftritt, ist "show platform software fed switch active puntrates interfaces".

- Dies ist sehr hilfreich, um eine Quellschnittstelle zu finden, bei der Flooding auftritt, das den Punt-Pfad überlastet und legitimen CPU-gebundenen Datenverkehr beeinträchtigt.

<#root>

```
Leaf01#
show platform software fed switch active punt rates interfaces
Punt Rate on Interfaces Statistics
Packets per second averaged over 10 seconds, 1 min and 5 mins
================================================================================================
                              |           |  Recv |  Recv |  Recv |  Drop |  Drop  |  Drop
<-- Receive and drop rates for this port
 Interface Name               |  IF_ID    |  10s  |  1min |  5min |  10s  |  1min  |  5min
================================================================================================

GigabitEthernet1/0/1          0x0000000a
       2       2       2       0       0       0
<-- the port and its IF-ID which can be used in the next command

------------------------------------------------------------------------------------------------
```

<#root>

```
Leaf01#
show platform software fed switch active punt rates interfaces 0xa  <-- From previous command (omit the
Punt Rate on Single Interfaces Statistics

Interface : GigabitEthernet1/0/1 [if_id: 0xA]

  Received                        Dropped
  --------                        -------
   Total          : 8032546         Total           : 0
   10 sec average : 2               10 sec average  : 0
    1 min average : 2                1 min average  : 0
    5 min average : 2                5 min average  : 0

Per CPUQ punt stats on the interface

 (rate averaged over 10s interval)
```

```
=============================================================================
 Q  |         Queue                |  Recv   |  Recv  |  Drop  |  Drop  |
 no |         Name                 |  Total  |  Rate  |  Total |  Rate  |
=============================================================================
 17

 CPU_Q_DHCP_SNOOPING

                 1216        0        0        0
<...snip...>
```

Statistiken des DHCP-Snooping-Clients

Beobachten Sie den DHCP-Nachrichtenaustausch mit diesem Befehl. Diese Funktion kann auf Leaf oder CGW ausgeführt werden, um die Ereignisablaufverfolgung anzuzeigen.

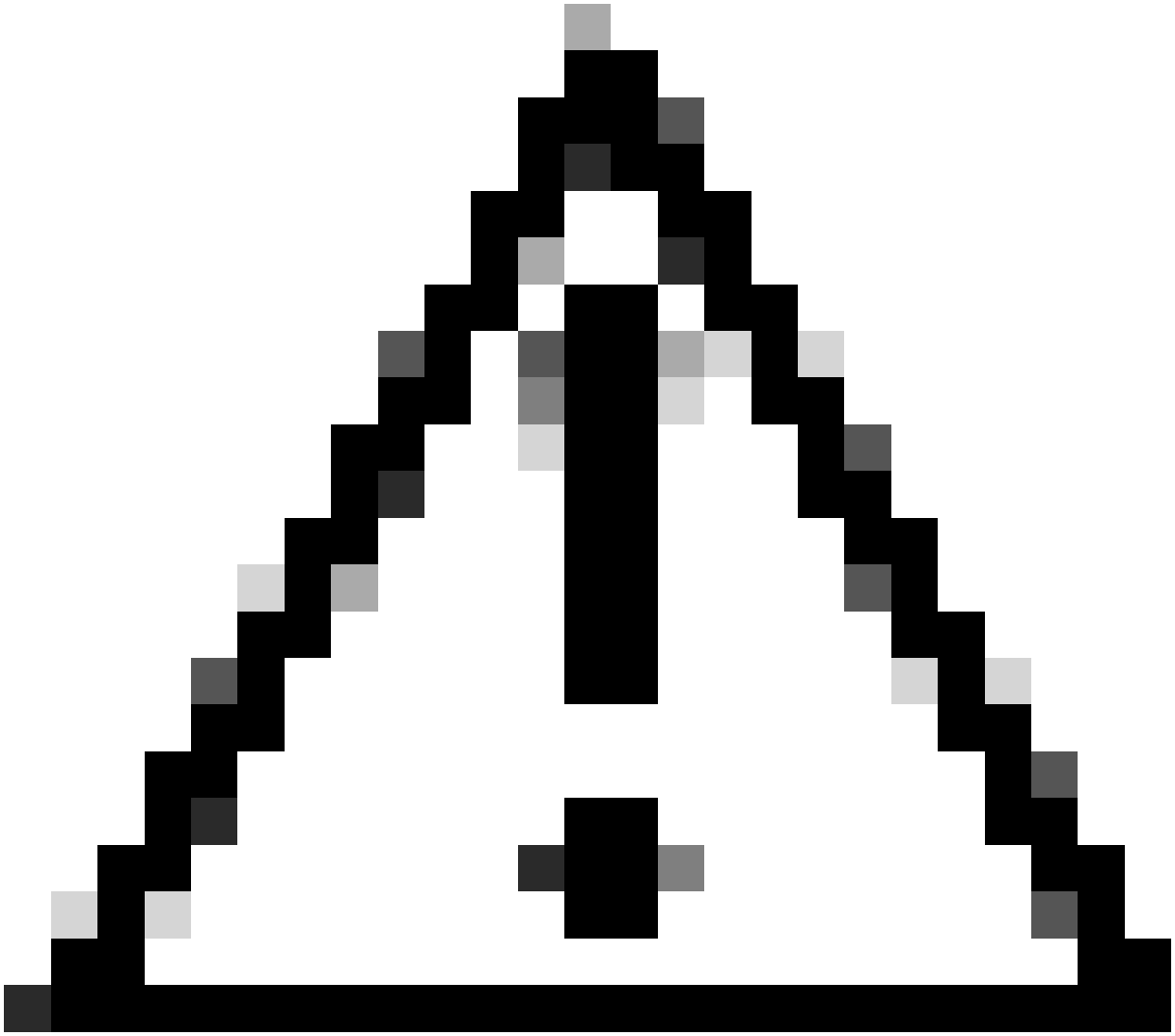
<#root>

```
Leaf01#

show platform dhcpsnooping client stats 0006.F601.CD43

DHCPSN: DHCP snooping server
DHCPD: DHCP protocol daemen
L2FWD: Transmit Packet to driver in L2 format
FWD: Transmit Packet to driver

(B): Dhcp message's response expected as 'B'roadcast
(U): Dhcp message's response expected as 'U'nicast

Packet Trace for client MAC 0006.F601.CD43:

Timestamp                Destination MAC  Destination Ip  VLAN  Message      Handler:Action
------------------------ ---------------- --------------- ----  ------------ ----------------
2023/09/28 14:53:59.866  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) PUNT:RECEIVED
2023/09/28 14:53:59.866  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) PUNT:TO_DHCPSN
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) BRIDGE:RECEIVED
2023/09/28 14:53:59.867  0000.BEEF.CAFE   255.255.255.255 202  DHCPDISCOVER(B) L2INJECT:TO_FWD
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) BRIDGE:TO_INJECT
2023/09/28 14:53:59.867  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPDISCOVER(B) L2INJECT:TO_FWD
2023/09/28 14:54:01.871  0006.F601.CD43   255.255.255.255 202  DHCPOFFER(B)    PUNT:RECEIVED
2023/09/28 14:54:01.871  0006.F601.CD43   255.255.255.255 202  DHCPOFFER(B)    PUNT:TO_DHCPSN
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  PUNT:RECEIVED
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  PUNT:TO_DHCPSN
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  BRIDGE:RECEIVED
2023/09/28 14:54:01.874  0000.BEEF.CAFE   255.255.255.255 202  DHCPREQUEST(B)  L2INJECT:TO_FWD
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  BRIDGE:TO_INJECT
2023/09/28 14:54:01.874  FFFF.FFFF.FFFF   255.255.255.255 202  DHCPREQUEST(B)  L2INJECT:TO_FWD
2023/09/28 14:54:01.877  0006.F601.CD43   255.255.255.255 202  DHCPACK(B)      PUNT:RECEIVED
2023/09/28 14:54:01.877  0006.F601.CD43   255.255.255.255 202  DHCPACK(B)      PUNT:TO_DHCPSN
```

Zusätzliche Debugs

```
debug ip dhcp server packet detail
```

```
debug ip dhcp server packet
debug ip dhcp server events
debug ip dhcp snooping packet
debug dhcp detail
```



Vorsicht: Vorsicht beim Ausführen von Debugs!

Zugehörige Informationen

- Implementierung einer BGP-EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000
- Implementierung der BGP EVPN Protected Overlay-Segmentierung auf Catalyst Switches der Serie 9000
- Betrieb und Fehlerbehebung bei DHCP-Snooping auf Catalyst Switches der Serie 9000

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.