# Implemente BGP EVPN DHCP Layer 2 Relay en los Catalyst 9000 Series Switches

## Contenido

# Introducción

Este documento describe cómo configurar, verificar y resolver problemas de la función EVPN VxLAN DHCP L2 Relay.

# Prerequisites

## Requirements

- Esta función se utiliza en cualquier implementación de tipo CGW en la que se utilice DHCP
- Si está implementando la segmentación protegida, revise estos documentos
  - Implemente la Política de Ruteo BGP EVPN en los Catalyst 9000 Series Switches
  - Implemente la segmentación de superposición protegida BGP EVPN en los switches Catalyst serie 9000

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 y versiones posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Antecedentes

## Detalles del documento

Este documento se puede utilizar para cualquier implementación de CGW en la que sea necesario retransmitir DHCP desde una hoja sin SVI hacia la puerta de enlace central.

- Si no utiliza la segmentación protegida, utilice la sección del documento en la que se anuncia SVI en el fabric

Si está implementando la segmentación protegida, este documento es la parte 2 de 3 documentos interrelacionados:

- Documento 1:Implementación de la Política de Ruteo BGP EVPN en los Catalyst 9000 Series Switches cubre cómo controlar el tráfico BGP BUM en la superposición, y debe

configurarse primero

- Documento 2:Implemente la segmentación de superposición protegida BGP EVPN en los switches Catalyst de la serie 9000 se basa en el diseño y la política de superposición del documento 1 y describe la implementación de la palabra clave 'protected'.
- Documento 3: Este documento. Se basa en los dos últimos documentos y describe la forma en que se implementa la retransmisión DHCP sólo con hojas de capa 2 y CGW

## Comportamiento de retransmisión L2

| Relay | Snooping | Inundación de núcleo | Inundación de acceso | IPv4 |
|---|---|---|---|---|
| sí | sí | no | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vni-mod-port) se rellena con indagación DHCP<br>• Se puede limitar el lado de acceso con la configuración de confianza dhcp<br><br>* MODELO RECOMENDADO |
| sí | no | sí | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vlan-mod-port) se rellena con indagación DHCP |
| no | sí | no | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vni-mod-port) se rellena con indagación DHCP<br>• Se puede limitar el lado de acceso con la configuración de confianza dhcp |
| Relay | Snooping | Inundación de núcleo | Inundación de acceso | IPv6 |
| sí | sí | sí | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vni-mod-port) se rellena con indagación DHCP<br>• Se puede limitar el lado de acceso con la configuración de confianza dhcp |
| sí | no | sí | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vlan-mod-port) se rellena con indagación DHCP |

| | | | | |
|---|---|---|---|---|
| no | sí | sí | sí | • Subopción de la opción 82: (1) La ID del circuito del agente (vni-mod-port) se rellena con indagación DHCP<br>• Se puede limitar el lado de acceso con la configuración de confianza dhcp |
| no | no | sí | sí | |

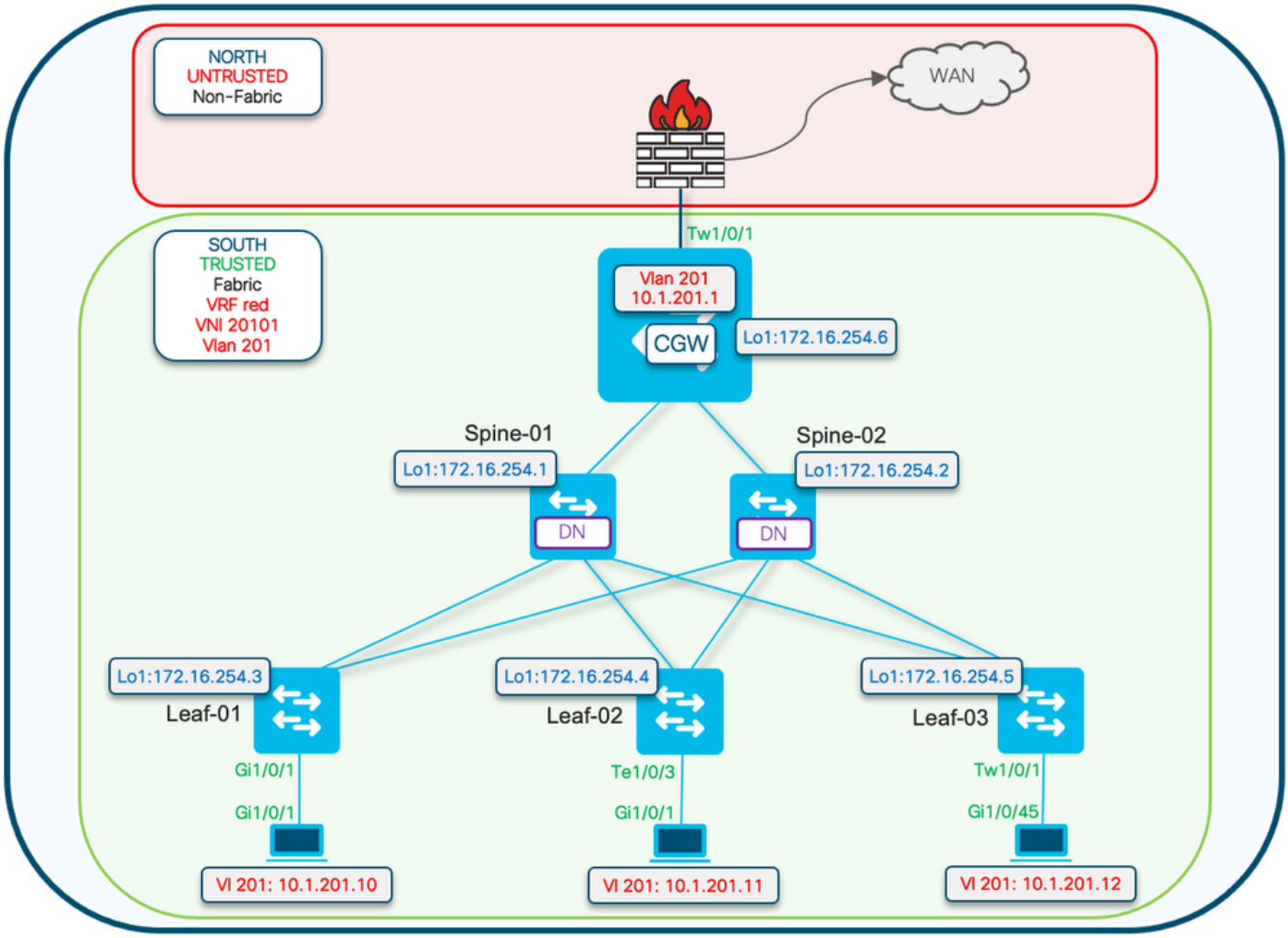
# Terminology

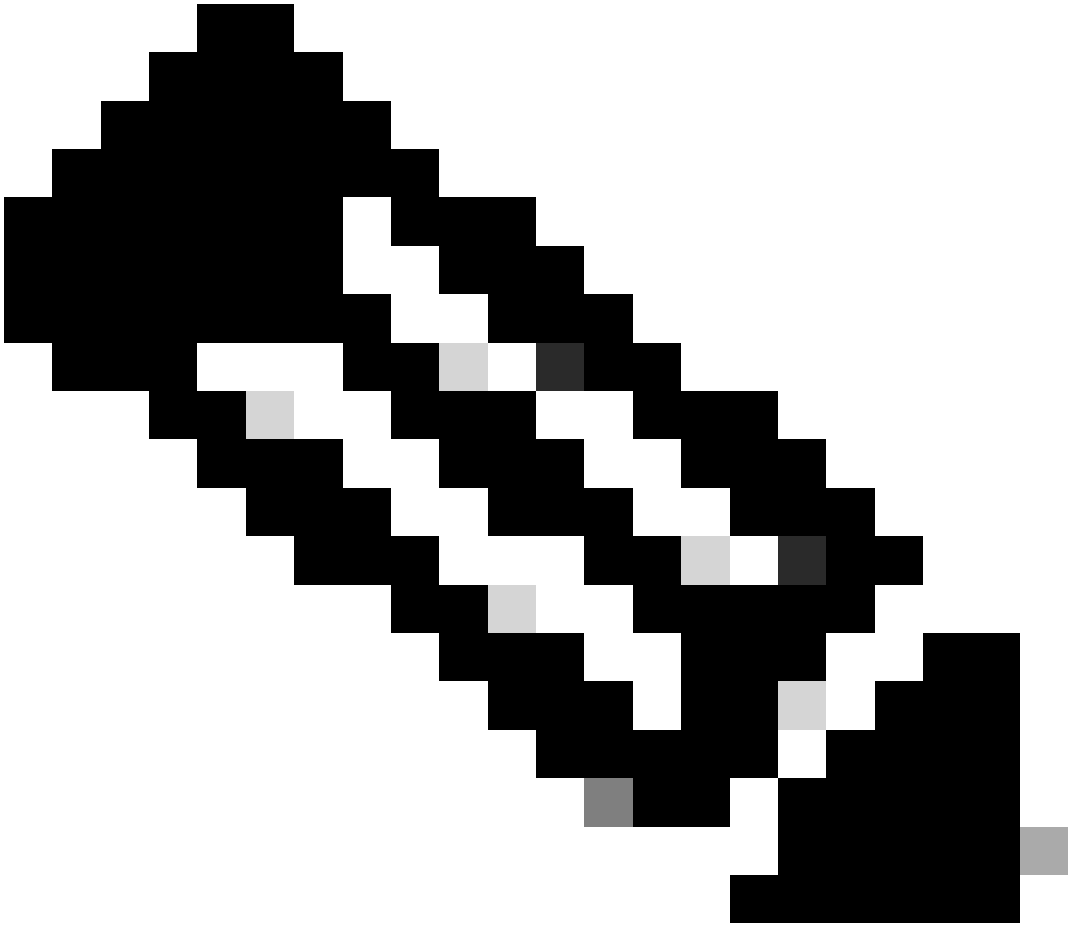
| | | |
|---|---|---|
| VRF | Reenvío de routing virtual | Define un dominio de routing de capa 3 que se puede separar de otro VRF y de un dominio de routing IPv4/IPv6 global |
| AF | Familia de direcciones | Define qué prefijos de tipo y manejos BGP de información de ruteo |
| AS | Sistema autónomo | Conjunto de prefijos IP enrutables de Internet que pertenecen a una red o a un conjunto de redes administradas, controladas y supervisadas por una sola entidad u organización |
| EVPN | Red privada virtual Ethernet | La extensión que permite que BGP transporte la información de IP de Capa 2 MAC y Capa 3 es EVPN y utiliza Multi-Protocol Border Gateway Protocol (MP-BGP) como protocolo para distribuir la información de alcance que pertenece a la red superpuesta VXLAN. |
| VXLAN | LAN extensible virtual (red de área local) | VXLAN está diseñado para superar las limitaciones inherentes de las VLAN y el STP. Se propone un estándar IETF [RFC 7348] para proporcionar los mismos servicios de red Ethernet de capa 2 que las VLAN, pero con mayor flexibilidad. Funcionalmente, es un protocolo de encapsulación MAC-in-UDP que se ejecuta como una superposición virtual en una red subyacente de Capa 3. |
| CGW | Gateway centralizado | Implementación de EVPN donde la SVI del gateway no está en cada hoja. En su lugar, todo el ruteo se realiza mediante una hoja específica que utiliza IRB asimétrico (Ruteo y Bridging Integrados) |
| GW DEF | Gateway predeterminado | Atributo de comunidad ampliada BGP agregado al prefijo MAC/IP mediante el comando "default-gateway advertise enable" en la sección de configuración 'l2vpn evpn'. |

| | | |
|---|---|---|
| IMET (RT3) | Etiqueta Ethernet Multicast Inclusiva (Route) | También se denomina ruta BGP de tipo 3. Este tipo de ruta se utiliza en EVPN para entregar el tráfico BUM (difusión/unidifusión desconocida/multidifusión) entre VTEP. |
| RT2 | Tipo de ruta 2 | Prefijo BGP MAC o MAC/IP que representa un MAC de host o MAC-IP de gateway |
| Gestor de EVPN | Administrador de EVPN | Componente de administración central para varios otros componentes (ejemplo: aprende de SISF y envía señales a L2RIB) |
| SISF | Función de seguridad integrada en el switch | Una tabla de seguimiento de host agnóstico que es utilizada por EVPN para aprender qué hosts locales están presentes en una hoja |
| L2RIB | Base de información de routing de capa 2 | En componente intermedio para la administración de interacciones entre BGP, EVPN Mgr y L2FIB |
| FED | Controlador de motor de reenvío | Programas para la capa ASIC (hardware) |
| MATM | Administrador de tabla de direcciones MAC | IOS MATM: tabla de software que instala sólo direcciones locales y<br>FED MATM: tabla de hardware que instala las direcciones locales y remotas aprendidas del plano de control, y es parte del plano de reenvío de hardware |

# Configurar (implementación estándar de CGW)

## Diagrama de la red


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



Nota: esta sección trata sobre una implementación CGW estándar sin el uso de la función protegida.

- Las depuraciones que muestran el intercambio de paquetes DHCP DORA sólo se muestran en el ejemplo de segmento protegido

---

## Detalles clave de VTEP (hoja) de L2

El paquete de solicitud proviene del cliente

conservado

- Utilice el gw predeterminado anunciado CGW mac.
- Si existe más de un gw, se utilizará el primer gw mac.
- Convertir MAC de difusión externa (iniciado por el cliente: D y R en DORA) en MAC GW de unidifusión y reenviar a CGW

conservado

El snooping DHCP añade: subopciones de la opción 82: circuito y RID

(RID es utilizado por el procesamiento de paquetes de respuesta en CGW)

(Informa a CGW que no es local y a la retransmisión de fabric de vuelta a 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')
```

- Paquetes de respuesta recibidos de CGW a través del túnel vxlan
- Opción de tiras de hojas 82.
- Agrega entradas de enlace con la interfaz de origen del cliente. (vxlan-mod-port proporciona la interfaz de origen del cliente)
- Paquete de respuesta reenviado al cliente

## Detalles clave de VTEP de nivel 3 (CGW)

- Active DHCP SNOOPING
- Habilite DHCP RELAY en SVI
- La solicitud se recibe de L2VTEP y se envía a relay
- Relay agrega otras subopciones de la opción 82 (gi, invalidación del servidor, etc.) y las envía al servidor DHCP
- La respuesta DHCP del servidor DHCP llega primero al componente RELAY
- Después de que RELAY elimina los parámetros de la opción 82 (dirección gi, invalidación del servidor, etc.), el paquete se pasa al componente de indagación dhcp
- El componente de indagación comprueba el RID (ID del router) y, si no es local, no elimina las subopciones 1 y 2 de la opción 82

- Los relés de fabric (dado que el RID no es local) se reenvían directamente al cliente remoto
- Utiliza el cliente Mac y hace la inyección de bridge.  El hardware realiza la búsqueda de mac de cliente y reenvía el paquete con la encapsulación vxlan al L2VTEP de origen.

  conservado

## L2VTEP

Configuración de la instancia de evpn

<#root>

```
Leaf-01#
```

**show run | beg l2vpn evpn instance 201**

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

Activar indagación DHCP

<#root>

```
Leaf-01#
```

**show run | sec dhcp snoop**

```
ip dhcp snooping vlan 101,
```

**201**

```
ip dhcp snooping
```

## CGW

Configuración de la instancia de evpn

<#root>

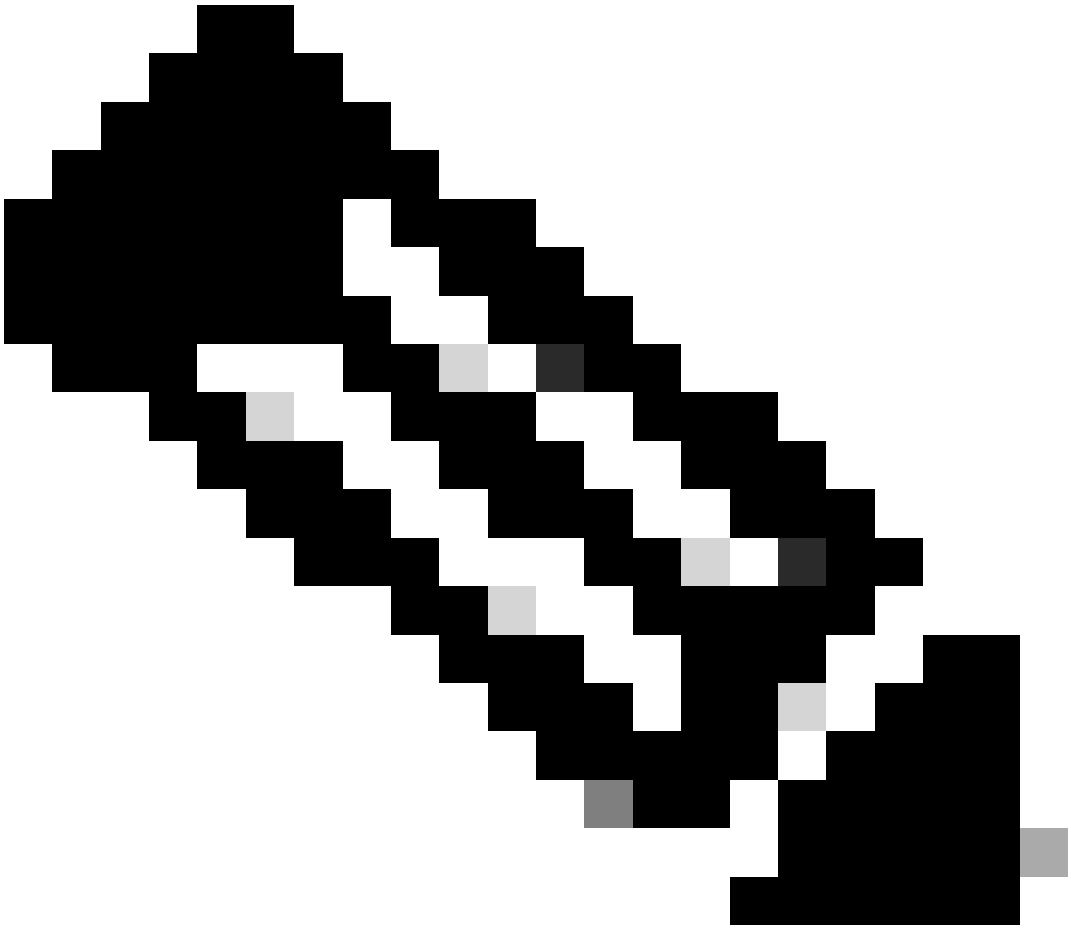
```
Border#
```

**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
```

---



> Nota: El atributo DEF GW es crítico para que la retransmisión L2 sepa a quién encapsular y enviar el paquete DHCP.

---

Activar snooping DHCP

<#root>

```
Border#

sh run | s dhcp snoop

ip dhcp snooping vlan 101,
```

**201**

ip dhcp snooping

Asegúrese de que el relé DHCP tenga la configuración correcta para manejar las opciones adicionales

<#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**

# Verificar (implementación estándar de CGW)

## Prefijo de gateway (hoja)

<#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 (hoja)

### <#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**

## MAC local (hoja)

### <#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**

## Detección DHCP (hoja y CGW)

### <#root>

```
Leaf-01#
```

**show ip dhcp snooping**

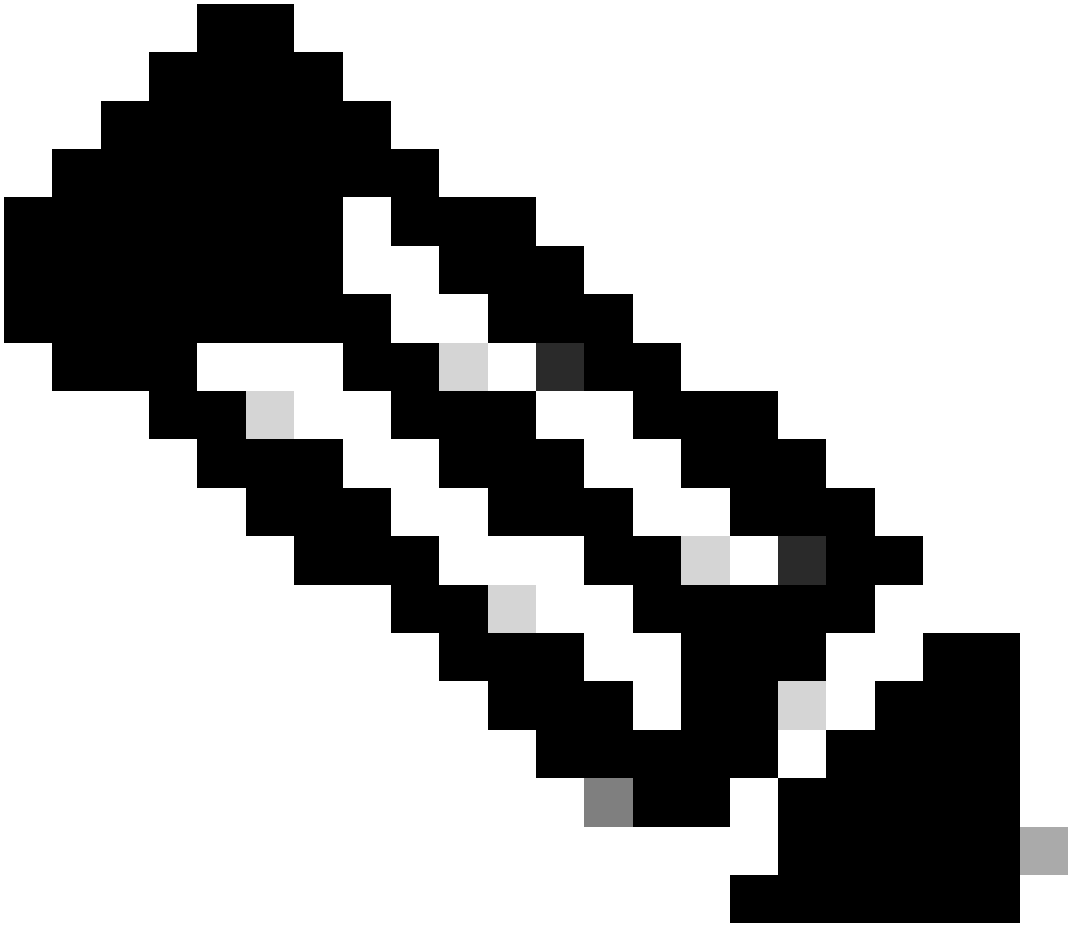
**Switch DHCP snooping is enabled**

```
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
```

# Configurar (Parcialmente aislado y protegido)

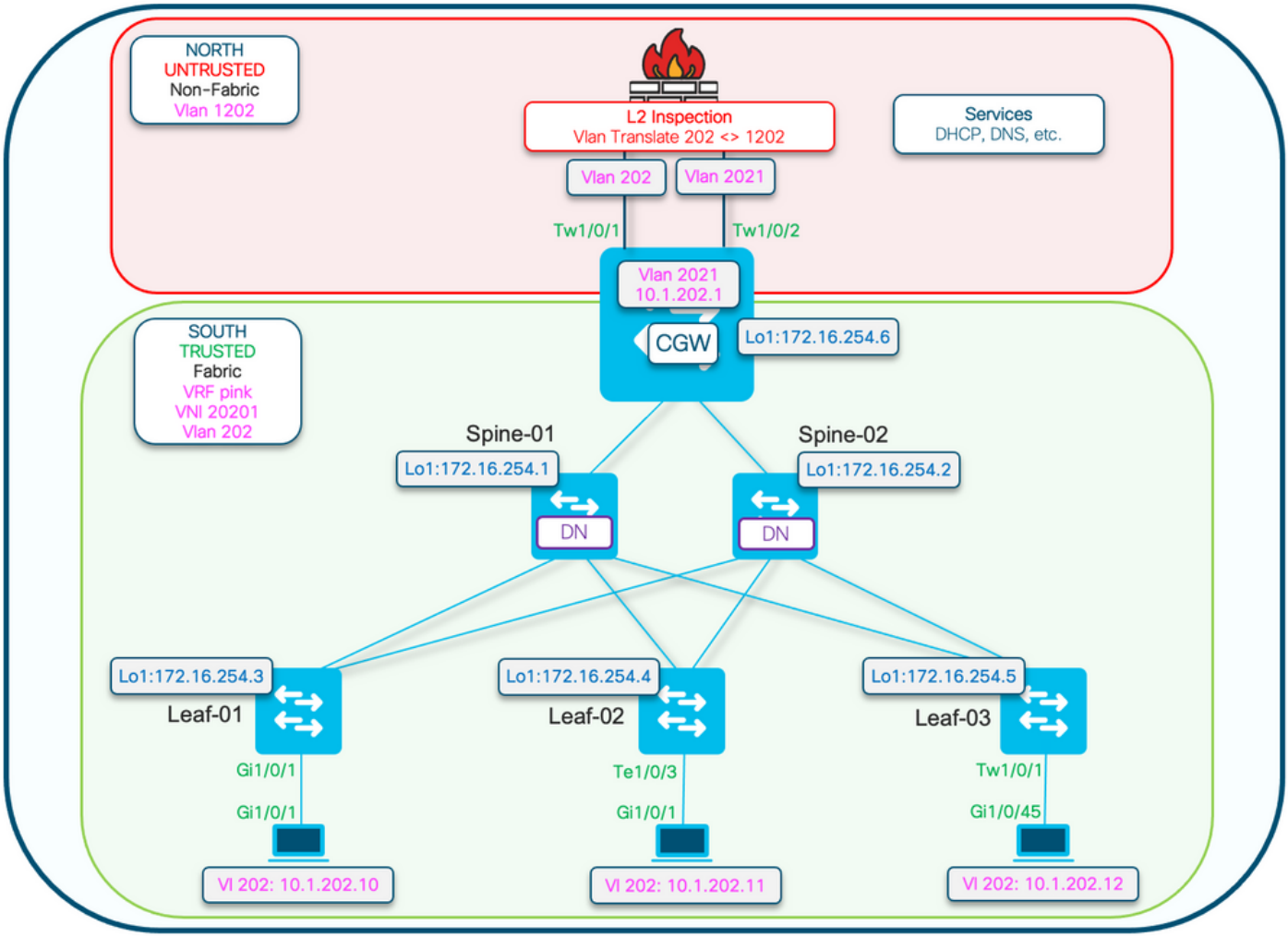
La indagación DHCP en la hoja de acceso se basa en la ruta de gateway predeterminada de CGW para aprender la MAC de gateway a la que se reenvían los paquetes DHCP.

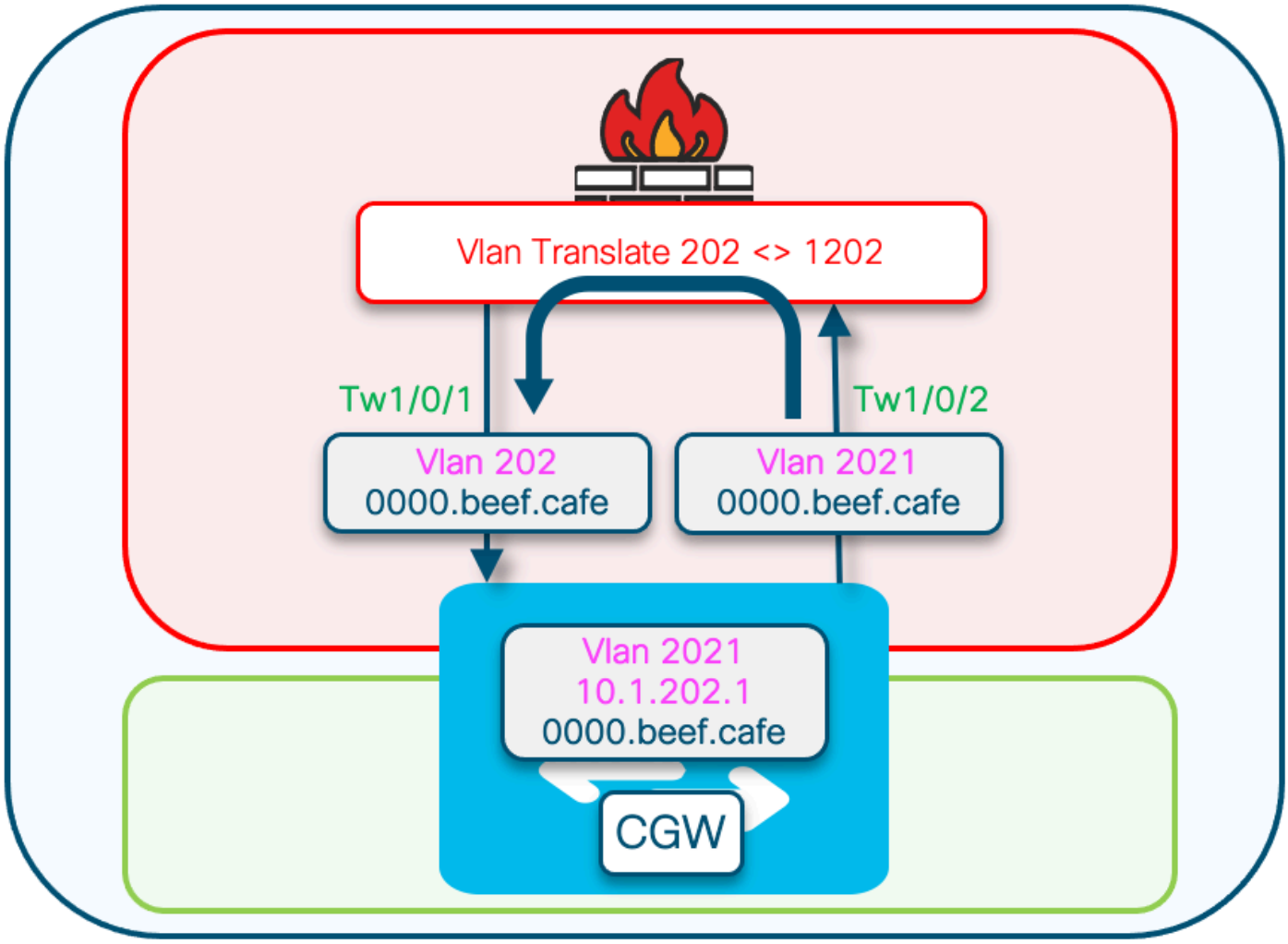
- Cuando se utiliza el diseño Parcialmente aislado con gateway externo, se requieren configuraciones adicionales en CGW para anunciar el MAC-IP RT2 con el atributo de gateway predeterminado (DEF GW).



Nota: Esta sección también describe una implementación de segmento protegido totalmente aislado, que también utiliza un GW que se anuncia en el fabric (frente a GW fuera del fabric).

## Diagrama de la red


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




## Detalles clave de VTEP (hoja) de L2

El paquete de solicitud proviene del cliente

conservado

- Utilice el gw predeterminado anunciado CGW mac.
- Si existe más de un gw, se utilizará el primer gw mac.
- Convertir MAC de difusión externa (iniciado por el cliente: D y R en DORA) en MAC GW de unidifusión y reenviar a CGW

conservado

El snooping DHCP añade: subopciones de la opción 82: circuito y RID

(RID es utilizado por el procesamiento de paquetes de respuesta en CGW)

(Informa a CGW que no es local y a la retransmisión de fabric de vuelta a 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')**

- Paquetes de respuesta recibidos de CGW a través del túnel vxlan
- Opción de tiras de hojas 82.
- Agrega entradas de enlace con la interfaz de origen del cliente. (vxlan-mod-port proporciona la interfaz de origen del cliente)
- Paquete de respuesta reenviado al cliente

## Detalles clave de VTEP de nivel 3 (CGW)

- Active DHCP SNOOPING
- Habilite DHCP RELAY en SVI
- La solicitud se recibe de L2VTEP y se envía a relay
- Relay agrega otras subopciones de la opción 82 (gi, invalidación del servidor, etc.) y las envía al servidor DHCP
- La respuesta DHCP del servidor DHCP llega primero al componente RELAY
- Después de que RELAY elimina los parámetros de la opción 82 (dirección gi, invalidación del servidor, etc.), el paquete se pasa al componente de indagación dhcp
- El componente de indagación comprueba el RID (ID del router) y, si no es local, no elimina las subopciones 1 y 2 de la opción 82
- Los relés de fabric (dado que el RID no es local) se reenvían directamente al cliente remoto
- Utiliza el cliente Mac y hace la inyección de bridge.  El hardware realiza la búsqueda de mac de cliente y reenvía el paquete con la encapsulación vxlan al L2VTEP de origen.

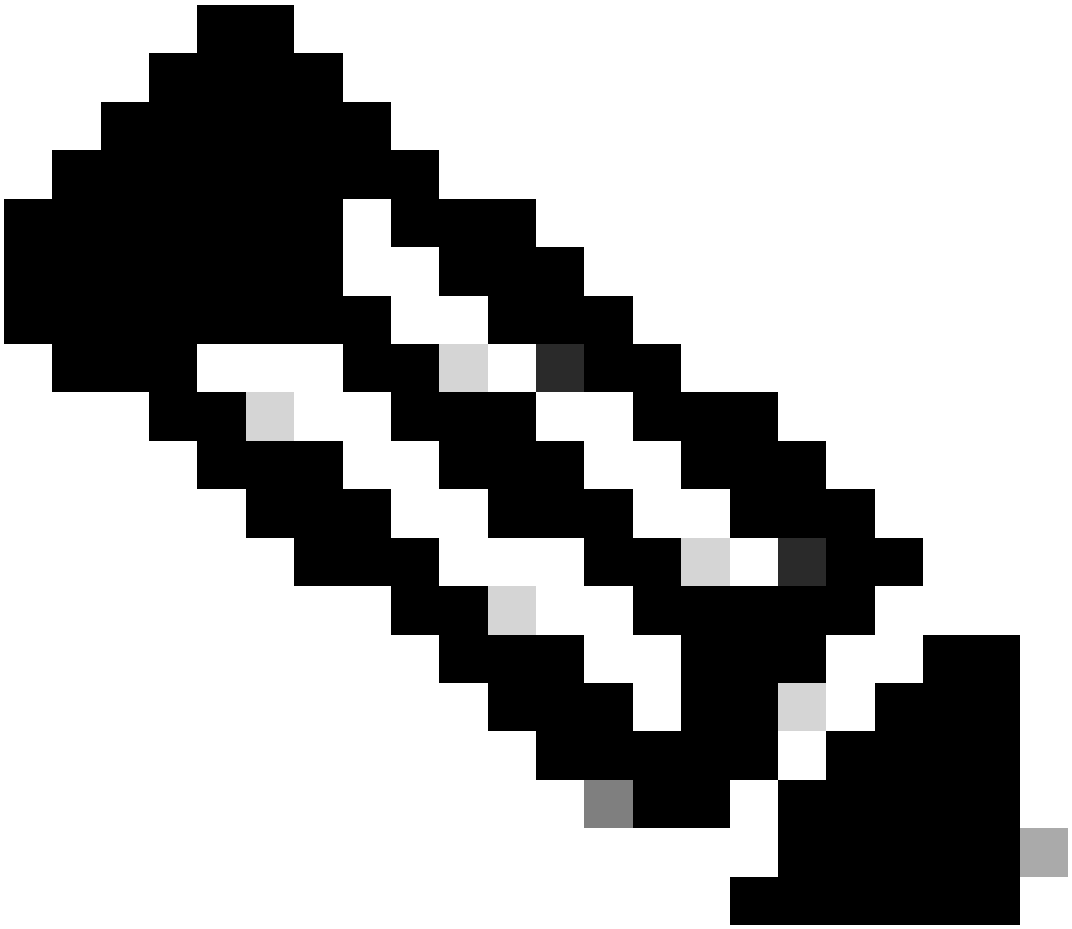
  conservado

conservado

Pasos requeridos para soportar DHCP L2 Relay:

1. Habilitar aprendizaje local de IP
2. Crear una política con la limpieza desactivada
3. Adjuntar a la puerta de enlace externa evi/vlan
4. Agregue entradas estáticas a la tabla de seguimiento de dispositivos para mac-ip de gateway externo
5. Cree el route map BGP para que coincida con los prefijos RT2 MAC-IP y establezca la comunidad ampliada de gateway predeterminada
6. Aplique route-map a los vecinos BGP Route Reflector
7. Asegúrese de que el relé DHCP tenga la configuración correcta para manejar la opción adicional
8. Configuración de DHCP Snooping en la VLAN de entramado y la VLAN GW externa

---



Nota: No se requieren cambios de configuración en las hojas de acceso para soportar DHCP L2 Relay con gateway externo.

---

# CGW

## Habilitar aprendizaje local de IP

### <#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
```

## Crear una política con la limpieza desactivada

### <#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
```

## Adjuntar a evi/vlan de gateway externo

### <#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
```

Agregar entradas estáticas a la tabla de seguimiento de dispositivos para mac-ip de gateway externo

<#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**

Cree el route map BGP para que coincida con los prefijos RT2 MAC-IP y establezca la comunidad ampliada de gateway predeterminada

<#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
```

Aplique route-map a los vecinos BGP Route Reflector

<#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**

Asegúrese de que el relé DHCP tenga la configuración correcta para manejar las opciones adicionales

<#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
```

Configuración de DHCP Snooping en las VLAN de estructura y la VLAN GW externa

<#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
```

Asegúrese de que el link ascendente al servidor DHCP sea confiable en el CGW

<#root>

```
CGW#
```

**sh run int tw 1/0/1**

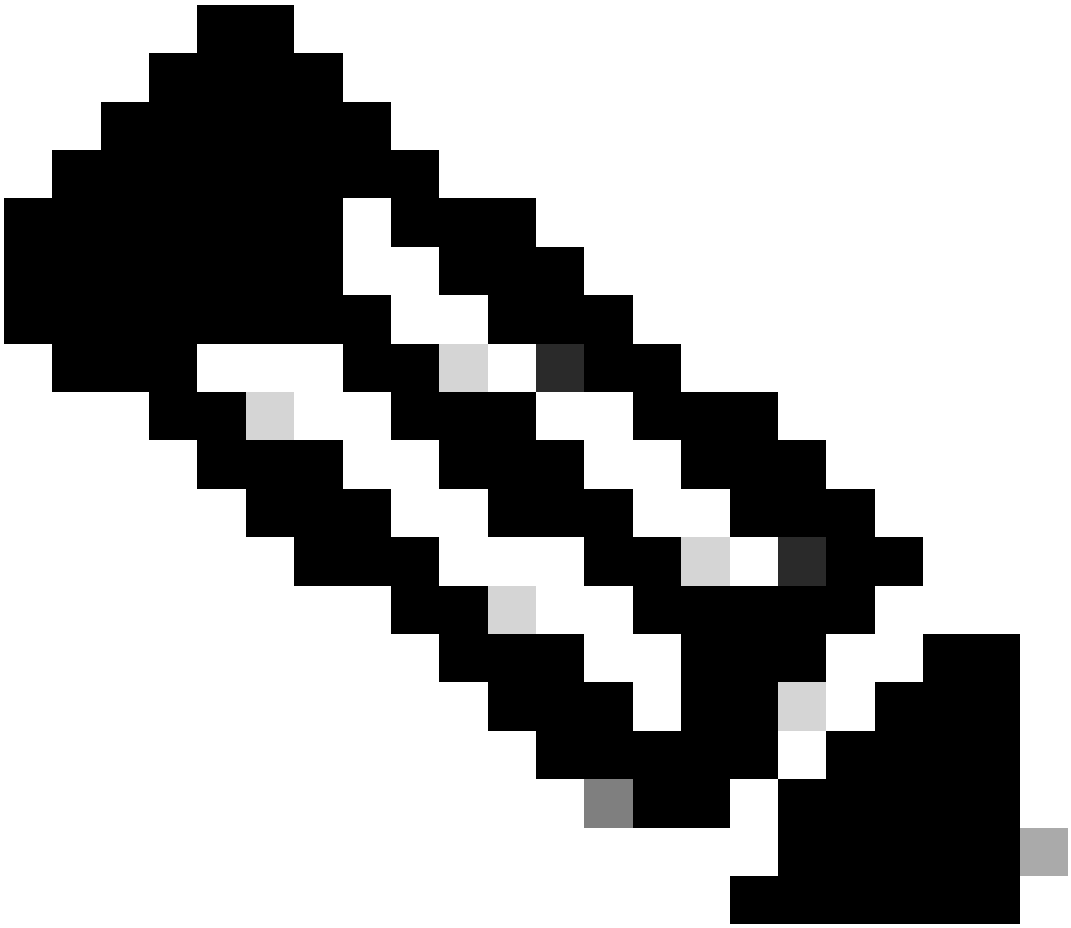
```
interface TwentyFiveGigE1/0/1
 switchport trunk allowed vlan 202
 switchport mode trunk
 ip dhcp snooping trust
end
```

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
```

---



---

Nota: debido a la forma en que se coloca el servidor en la confianza del dispositivo Firewall, se configuró en ambos enlaces que dan a este dispositivo. En el diagrama ampliado puede ver que la oferta llega a Tw1/0/1 y Tw1/0/2 en este diseño.

# Verificar (parcialmente aislado y protegido)

## Prefijo de gateway (hoja)

<#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 (hoja)

Confirme que Leaf haya instalado el MAC remoto CGW en el hardware

<#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**

## MAC local (hoja)

**<#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**

## Detección DHCP (hoja y CGW)

Confirme que la indagación DHCP esté habilitada en la hoja en la VLAN de entramado

<#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...>

Confirme que la indagación DHCP esté habilitada en el CGW en el entramado y las vlan de gateway externas

<#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**

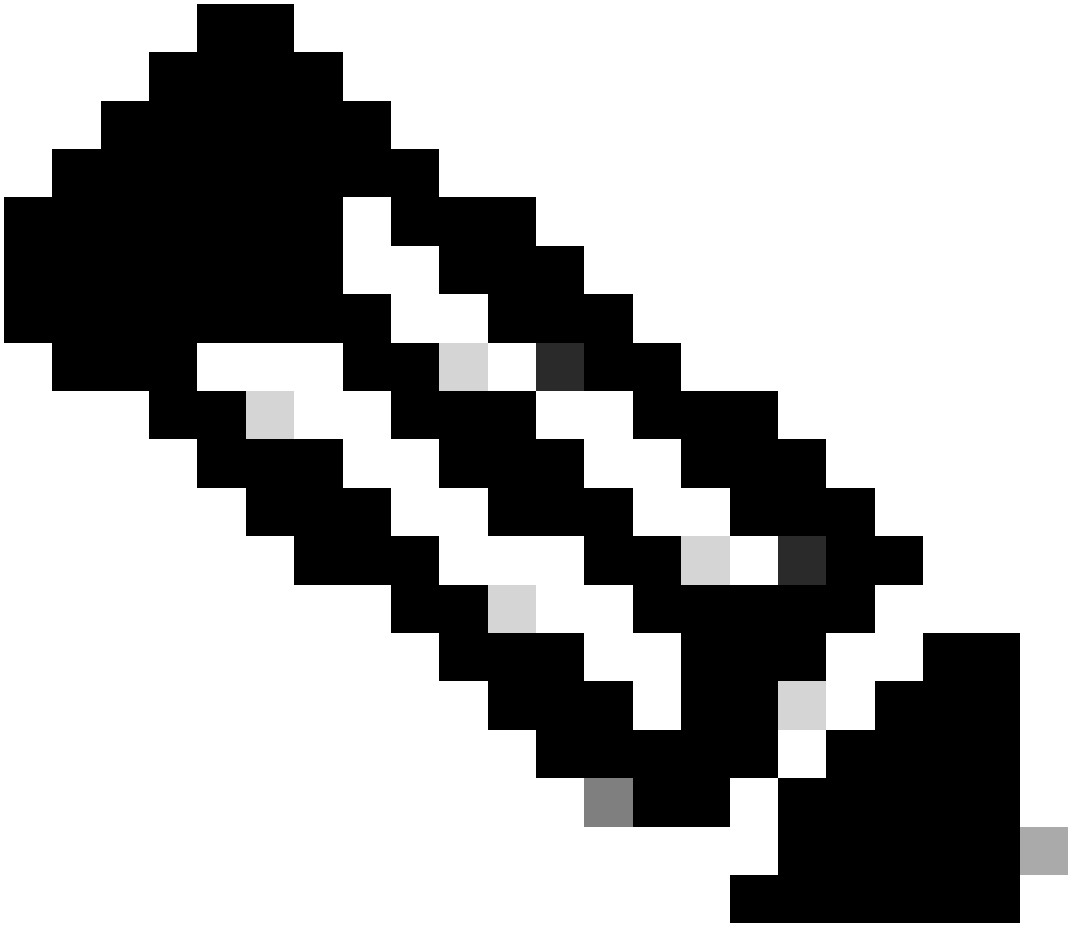
```
  Custom circuit-ids:
```

Confirme que se ha creado el enlace de snooping DHCP

```
<#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
```

# Localización de averías (cualquier tipo de CGW)

Los debugs son útiles para mostrar cómo los procesos de snooping DHCP y L2 Relay están manejando paquetes DHCP.



Nota: Estas depuraciones se pueden utilizar para cualquier tipo de implementación que utilice CGW con DCHP L2 Relay.

## Depuraciones de indagación DHCP (hoja)

Debug Snooping para confirmar el procesamiento de paquetes

<#root>

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

Iniciar el intento de dirección DHCP del host

- Para este documento se realizó un cierre/no cierre de la SVI que se dirige a través de DHCP para activar el intercambio DORA
- Para el host de Windows puede hacer un ipconfig /release > ipconfig /renew

Recopile las depuraciones de show logging o de la ventana de terminal

DHCP DISCOVER

Se observa que Discover proviene del puerto orientado al host

<#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
```

OFERTA DE DHCP

La oferta se ve llegar desde la interfaz de túnel de fabric

<#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
```

## SOLICITUD DHCP

La solicitud se ve desde el puerto de cara al host

<#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
```

ACK DHCP

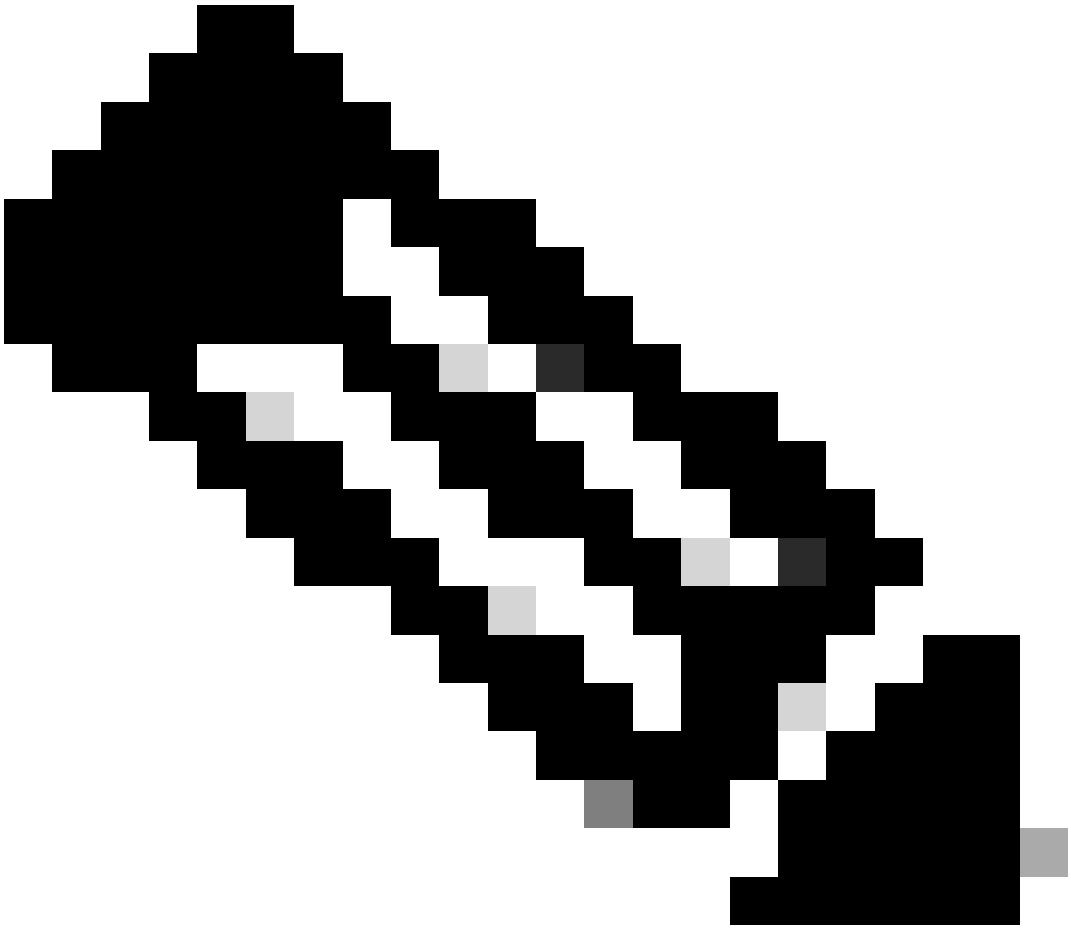
Se observa que el ack llega desde la interfaz del túnel de fabric

<#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.
```

---



> Nota: Estos debugs se recortan. Producen un volcado de memoria del paquete, pero la anotación de esta parte del resultado de la depuración está fuera del alcance de este documento.

---

## Depuraciones de detección DHCP (CGW)

DHCP DISCOVER

Debido a cómo se envía y recibe el paquete en el CGW (anclado en el firewall), las depuraciones se activan dos veces

Llegada desde el fabric en la interfaz del túnel y envío de Tw 1/0/1 hacia el firewall en el fabric vlan 202

<#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**

Llegada del firewall en Tw 1/0/2 en Vlan 2021 para enviarla a la SVI y ayudante al servidor DHCP

<#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**

OFERTA DE DHCP

Vuelve del servidor DHCP al SVI 2021, donde se configura el ayudante y se reenvía al firewall

<#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**

Llega desde el firewall en la vlan de fabric y se envía desde CGW al fabric hacia la hoja

<#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**

SOLICITUD DHCP

<#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**

ACK DHCP

<#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**

## Captura integrada

Utilice EPC para confirmar que el intercambio de paquetes DHCP y los parámetros son correctos

- Esto se muestra desde la perspectiva del CGW, pero el proceso se puede repetir en Leaf para verificar el intercambio de paquetes
- En este ejemplo se muestra el método Discover, ya que el proceso y el análisis son los mismos para los otros paquetes DHCP

Verifique la ruta al Loopback de Hoja

<#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
```

Configure la captura para que se ejecute en los links que se encuentran frente a Leaf01

<#root>

```
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
```

Inicie la captura, active el host para solicitar una dirección IP DHCP y detenga la captura

<#root>

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

Ver el resultado de la captura a partir de la detección de DHCP (preste atención a la ID de transacción para confirmar que se trata del mismo evento DORA)

<#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

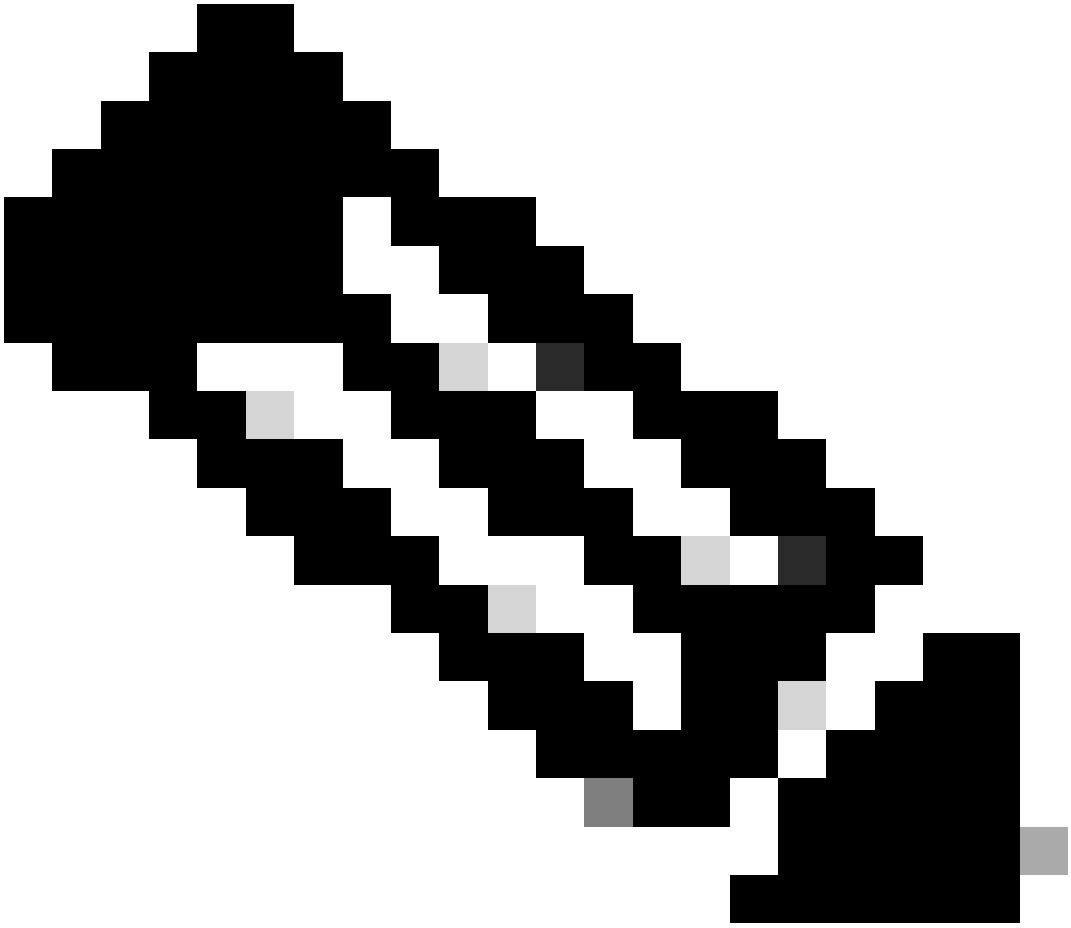
Option: (53) DHCP Message Type (Discover)

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
```



Nota: La herramienta de captura se puede utilizar en cualquier hoja o CGW para determinar el último punto en el que se sospecha que falla una parte del intercambio DHCP DORA.

---

Verificar estadísticas de snooping para errores

<#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.**

Verificar ruta de punt para detección DHCP

- CoPP es el componente principal que descarta paquetes en la trayectoria de punt

<#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
```

Otro comando muy útil para ubicar dónde se está produciendo una posible inundación de paquetes es 'show platform software fed switch active punt rates interfaces"

- Esto es muy útil para encontrar una interfaz de origen donde se produce la inundación que está congestionando el trayecto de punt y afectando el tráfico legítimo de la CPU

<#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...>
```

## DHCP Snooping Client Stats

Observe el intercambio de mensajes DHCP con este comando. Esto se puede ejecutar en Leaf o CGW para ver el seguimiento de eventos

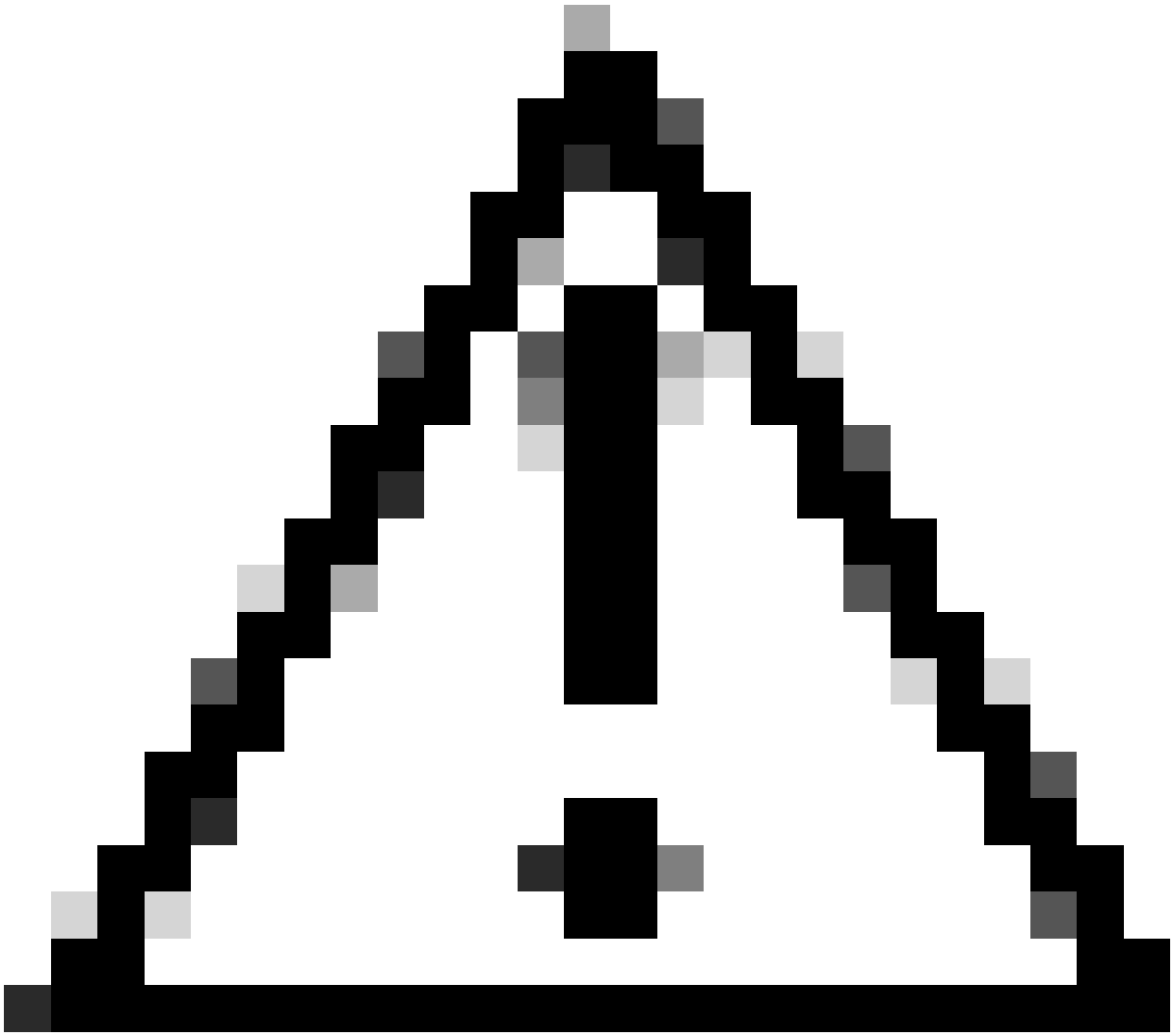
<#root>

```
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
```

## Depuraciones adicionales

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

---



Precaución: ¡tenga cuidado al ejecutar los debugs!

---

## Información Relacionada

- Implemente la Política de Ruteo BGP EVPN en los Catalyst 9000 Series Switches
- Implemente la segmentación de superposición protegida BGP EVPN en los switches Catalyst serie 9000
- Funcionamiento y solución de problemas de detección DHCP en switches Catalyst 9000

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).