Implemente o BGP EVPN DHCP Layer 2 Relay nos switches Catalyst 9000 Series

Contents

Introdução

Este documento descreve como configurar, verificar e solucionar problemas do recurso EVPN VxLAN DHCP L2 Relay.

Pré-requisitos

Requisitos

- Esse recurso é usado em qualquer implantação do tipo CGW em que o DHCP é usado
- Se estiver implementando a Segmentação Protegida, revise estes documentos
  - Implemente a política de roteamento BGP EVPN nos switches Catalyst 9000 Series
  - Implemente a segmentação BGP EVPN Protected Overlay em switches Catalyst 9000 Series

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 e versões posteriores

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Detalhes do documento

Este documento pode ser usado para qualquer implantação do CGW em que o DHCP precise ser retransmitido de uma folha sem SVI para o gateway central.

- Se você não estiver usando segmentação protegida, use a seção do documento em que o SVI é anunciado na malha

Se você estiver implementando a segmentação protegida, este documento será a parte 2 de 3 documentos inter-relacionados:

- Documento 1:Implementar a política de roteamento BGP EVPN nos switches Catalyst 9000 Series aborda como controlar o tráfego BGP BUM na sobreposição e deve ser configurado primeiro

- Documento 2:Implemente a segmentação de sobreposição protegida BGP EVPN nos switches Catalyst 9000 Series com base no projeto e na política de sobreposição do documento 1, descreve a implementação da palavra-chave 'protected'.
- Documento 3: Este documento. Baseia-se nos dois últimos documentos e descreve a forma como a retransmissão DHCP é implementada com Leafs e CGW somente da camada 2

Comportamento de L2 Relay

Retransmissão	Espionagem	Inundação de núcleo	Inundação de acesso	IPv4
sim	sim	não	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vni-mod-port) é preenchido com snooping dhcp • Pode-se limitar o lado do acesso com a configuração de confiança de dhcp * MODELO RECOMENDADO
sim	não	sim	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vlan-mod-port) é preenchido com snooping dhcp
não	sim	não	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vni-mod-port) é preenchido com snooping dhcp • Pode-se limitar o lado do acesso com a configuração de confiança de dhcp
Retransmissão	Espionagem	Inundação de núcleo	Inundação de acesso	IPv6
sim	sim	sim	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vni-mod-port) é preenchido com snooping dhcp • Pode-se limitar o lado do acesso com a configuração de confiança de dhcp
sim	não	sim	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vlan-mod-port) é preenchido com snooping dhcp

não	sim	sim	sim	• Opção 82 Subopção: (1) ID de circuito do agente (vni-mod-port) é preenchido com snooping dhcp • Pode-se limitar o lado do acesso com a configuração de confiança de dhcp
não	não	sim	sim	

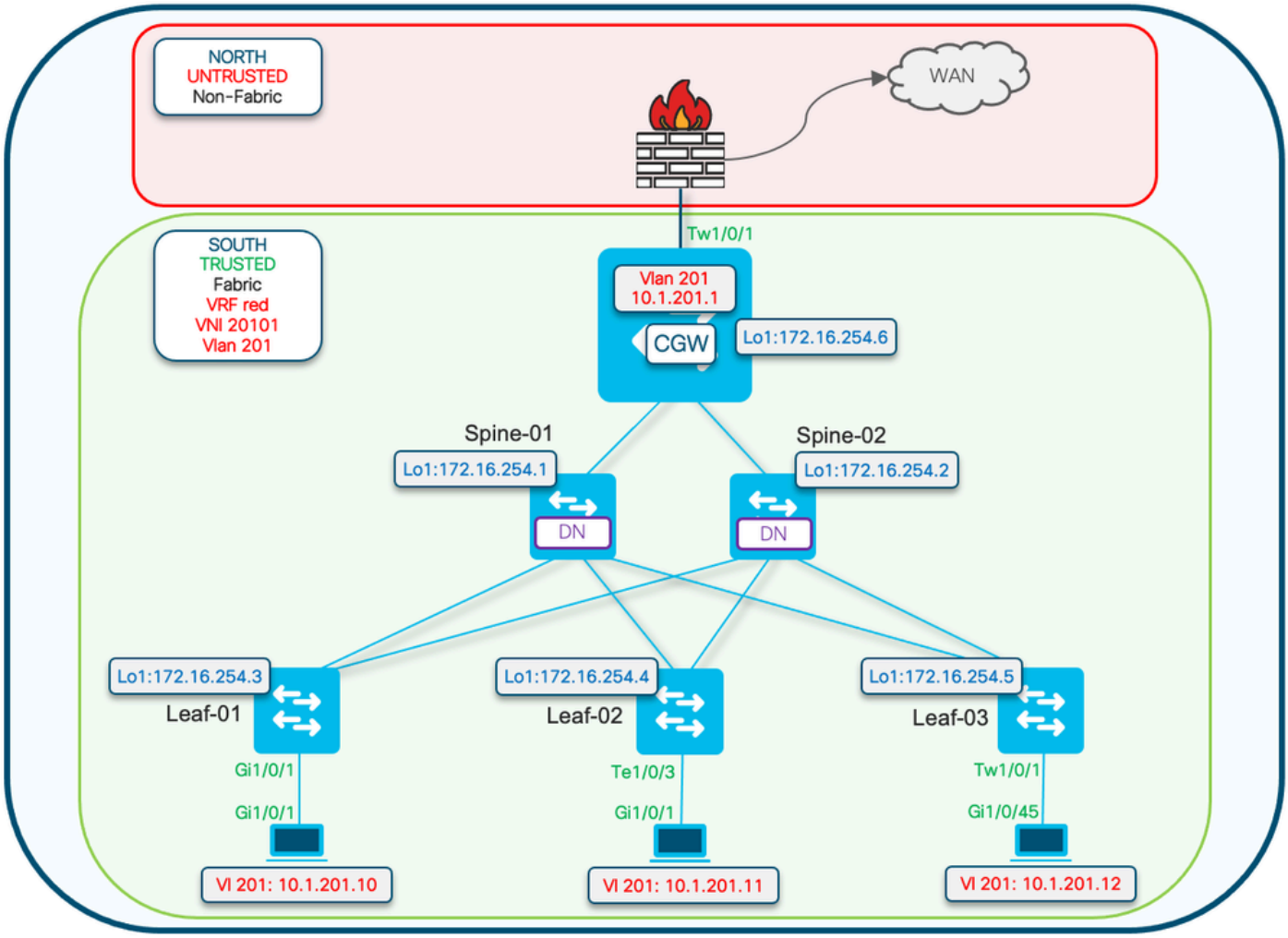
Terminologia

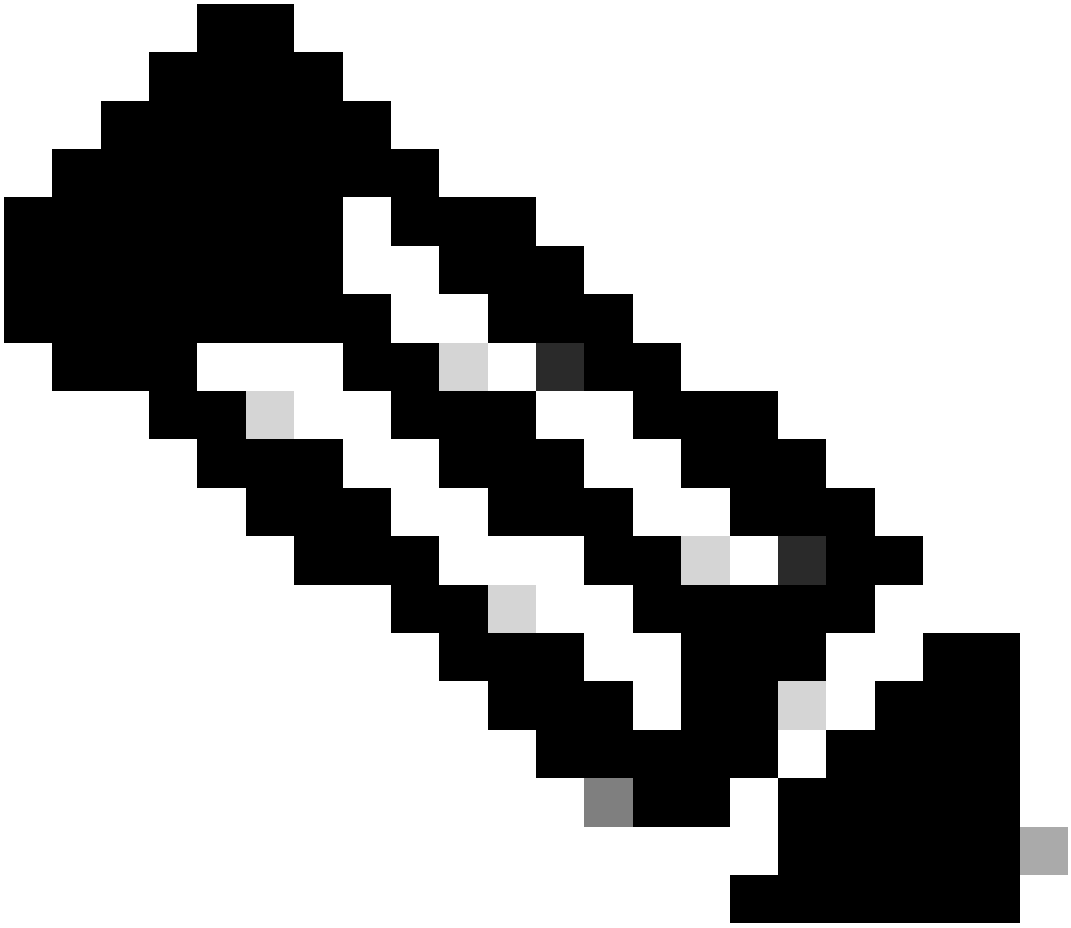
VRF	Encaminhamento de roteamento virtual	Define um domínio de roteamento de camada 3 que deve ser separado de outros domínios de roteamento VRF e IPv4/IPv6 global
AF	Família de Endereços	Define quais prefixos de tipo e informações de roteamento o BGP trata
COMO	Sistema autônomo	Um conjunto de prefixos IP roteáveis da Internet que pertencem a uma rede ou a um conjunto de redes gerenciadas, controladas e supervisionadas por uma única entidade ou organização
EVPN	Rede Privada Virtual Ethernet	A extensão que permite que o BGP transporte informações de MAC de Camada 2 e IP de Camada 3 é o EVPN e usa o Protocolo de Gateway de Borda Multiprotocolo (MP-BGP - Multi-Protocol Border Gateway Protocol) como o protocolo para distribuir informações de alcance que pertencem à rede de sobreposição de VXLAN.
VXLAN	LAN virtual extensível (rede local)	A VXLAN foi projetada para superar as limitações inerentes de VLANs e STP. É um padrão IETF proposto [RFC 7348] para fornecer os mesmos serviços de rede Ethernet de Camada 2 que as VLANs, mas com maior flexibilidade. Funcionalmente, é um protocolo de encapsulamento MAC-em-UDP executado como uma sobreposição virtual em uma rede de camada 3 subjacente.
CGW	Gateway centralizado	E a implementação do EVPN onde o SVI do gateway não está em cada folha. Em vez disso, todo o roteamento é feito por uma folha específica usando IRB assimétrico (Integrated Routing and Bridging)
DEF	Gateway padrão	Um atributo de comunidade estendida de BGP adicionado ao prefixo

GW		MAC/IP através do comando "default-gateway advertise enable" na seção de configuração 'l2vpn evpn'.
IMET (RT3)	Tag Ethernet Multicast Inclusiva (Rota)	Também chamada de rota BGP tipo 3. Esse tipo de rota é usado no EVPN para fornecer tráfego BUM (broadcast / unicast desconhecido / multicast) entre VTEPs.
RT2	Tipo de rota 2	Prefixo MAC ou MAC/IP de BGP que representa um MAC de host ou MAC-IP de gateway
Gerente de EVPN	Gerenciador EVPN	Componente de gerenciamento central para vários outros componentes (exemplo: aprende do SISF e envia sinais para o L2RIB)
SISF	Recurso de segurança integrada do switch	Uma tabela de rastreamento de host independente usada pelo EVPN para saber quais hosts locais estão presentes em uma folha
L2RIB	Base de informações de roteamento da camada 2	Em componente intermediário para gerenciar interações entre BGP, EVPN Mgr, L2FIB
FED	Driver do mecanismo de encaminhamento	Programa da camada ASIC (hardware)
MATM	Gerenciador de Tabelas de Endereços Mac	IOS MATM: tabela de software que instala somente endereços locais e FED MATM: tabela de hardware que instala endereços locais e remotos aprendidos do plano de controle e faz parte do plano de encaminhamento de hardware

Configurar (implantação padrão do CGW)

Diagrama de Rede


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



Observação: esta seção aborda uma implantação CGW padrão sem o uso do recurso protegido.

- As depurações que mostram a troca de pacotes DHCP DORA são mostradas apenas no exemplo de segmento protegido

Detalhes da chave L2 VTEP (Leaf)

O pacote de solicitação vem do cliente

- Use o mac CGW anunciado Gw padrão.
- Se houver mais de um gw, o primeiro gw mac será usado.
- Converta o MAC de broadcast externo (iniciado pelo cliente: D e R em DORA) para o mac GW unicast e encaminhe para o CGW

O rastreamento de DHCP adiciona: opção 82 subopções: circuito e RID

(O RID é usado pelo processamento de pacotes de resposta no CGW)

(Informa ao CGW que não é local e ao fabric relay de volta para 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')

- Pacotes de resposta recebidos do CGW pelo túnel vxlan.
- Leaf Strips opção 82.
- Adiciona entradas de associação com a interface de origem do cliente. (vxlan-mod-port fornece a interface de origem do cliente).
- Pacote de resposta encaminhado ao cliente.

Detalhes principais do L3 VTEP (CGW)

- Habilite o RASTREAMENTO DHCP
- Habilite o DHCP RELAY no SVI
- A solicitação é recebida do L2VTEP e é fornecida ao relé.
- Relay adiciona outras subopções da opção 82 (gi, substituição de servidor, etc.) e envia para o servidor DHCP
- A resposta DHCP do servidor DHCP primeiro chega ao componente RELAY.
- Depois que RELAY retira os parâmetros da opção 82 (endereço gi, substituição de servidor e assim por diante), o pacote é passado para o componente de snooping dhcp
- O componente de rastreamento verifica o RID (ID do roteador) e, se seu local não remover a opção 82, subopções 1 e 2

- O pacote Fabric Relays (já que o RID não é local) é encaminhado diretamente ao cliente remoto
- Usa o cliente Mac e faz a injeção de bridge. O hardware faz a consulta do cliente mac e encaminha o pacote com vxlan encap para o L2VTEP de origem.

L2VTEP

Configurar a instância de evpn

<#root>

```
Leaf-01#
show run | beg l2vpn evpn instance 201

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

Habilitar rastreamento de DHCP

<#root>

```
Leaf-01#
show run | sec dhcp snoop

ip dhcp snooping vlan 101,
201

ip dhcp snooping
```

CGW

Configurar a instância de evpn

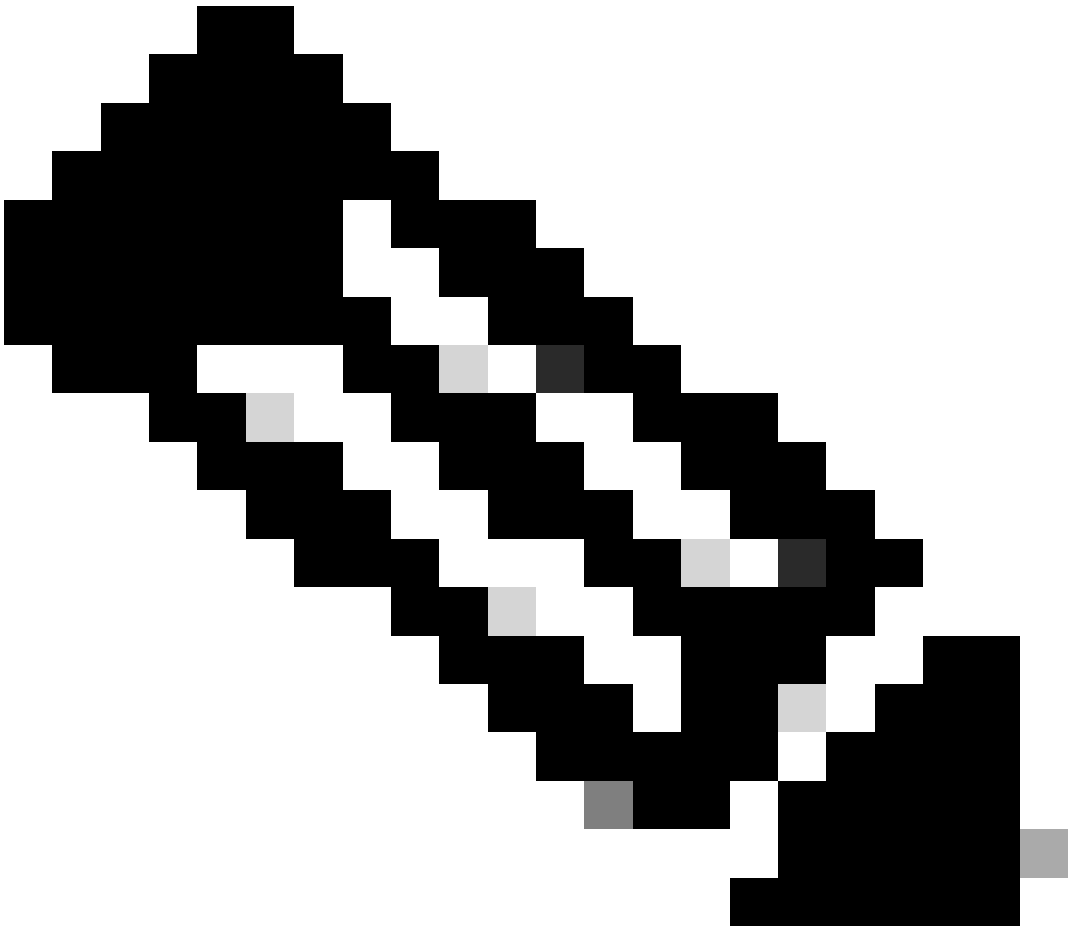
<#root>

```
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

---



> Observação: o atributo DEF GW é crítico para que o L2 Relay saiba para quem encapsular e enviar o pacote DHCP.

Habilitar rastreamento de DHCP

<#root>

```
Border#
```

sh run | s dhcp snoop

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

201

ip dhcp snooping

Verifique se o relé DHCP tem a configuração correta para lidar com as opções adicionais

<#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 (implantação padrão do CGW)

Prefixo do gateway (folha)

<#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 (Folha)

<#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 (Folha)

<#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
```

Rastreamento de DHCP (Leaf e CGW)

<#root>

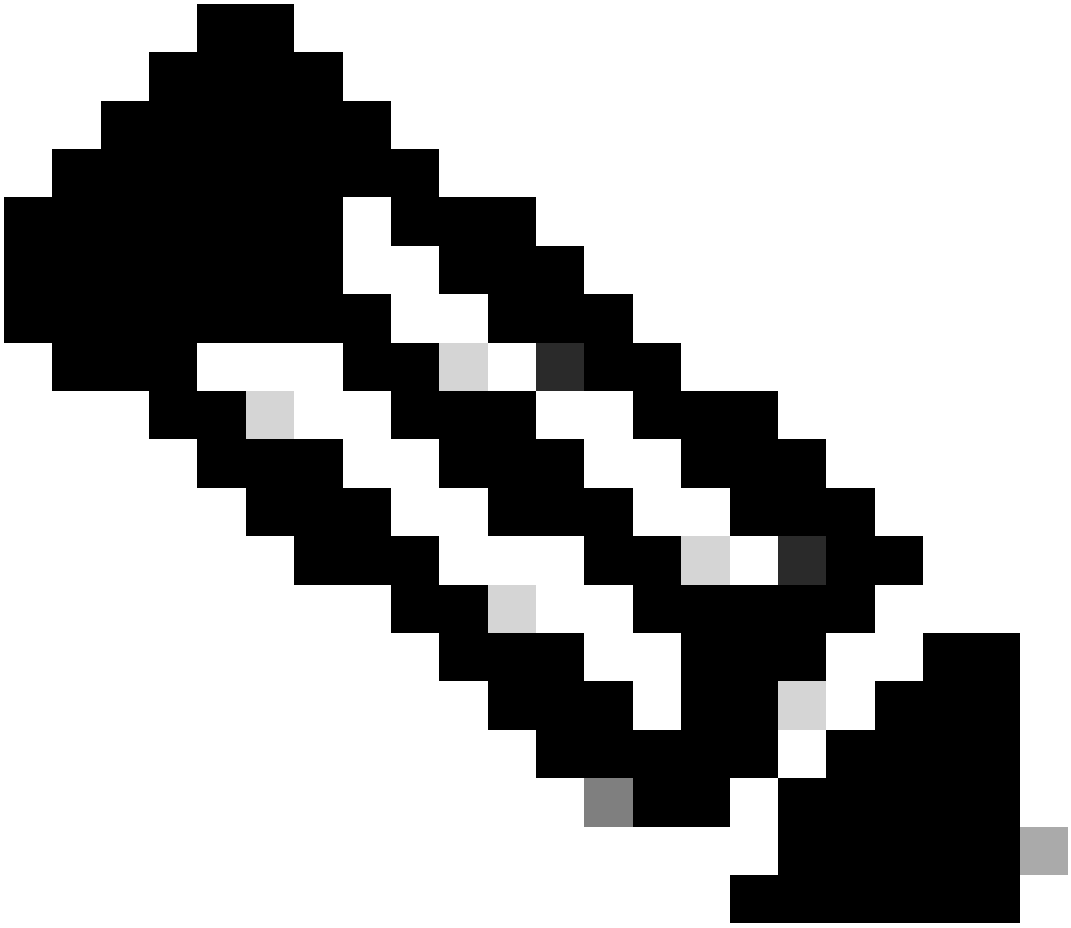
```
Leaf-01#

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 isolado protegido)

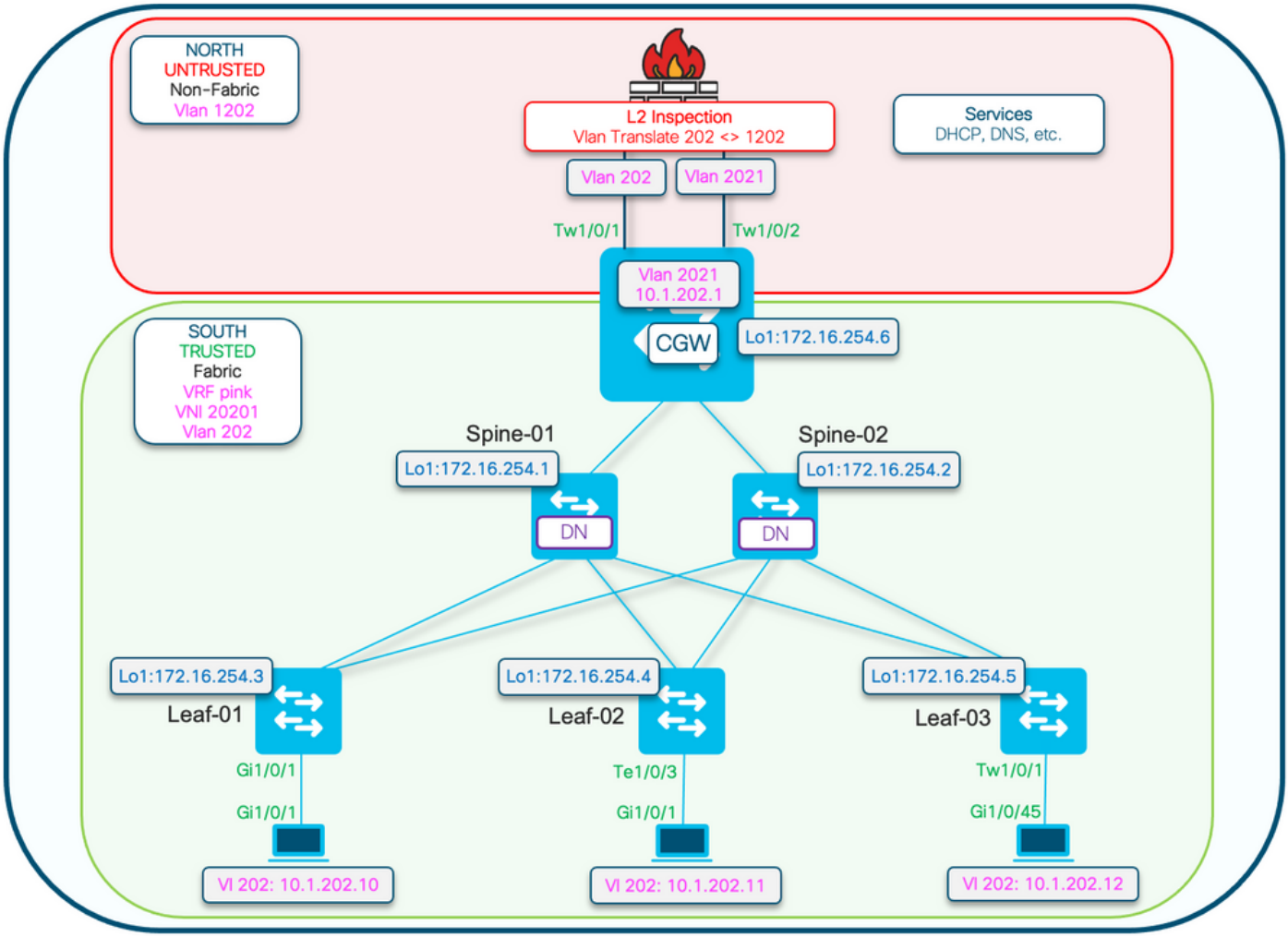
O rastreamento de DHCP na folha de acesso depende da rota de gateway padrão do CGW para aprender o MAC do gateway para o qual encaminhar pacotes DHCP.

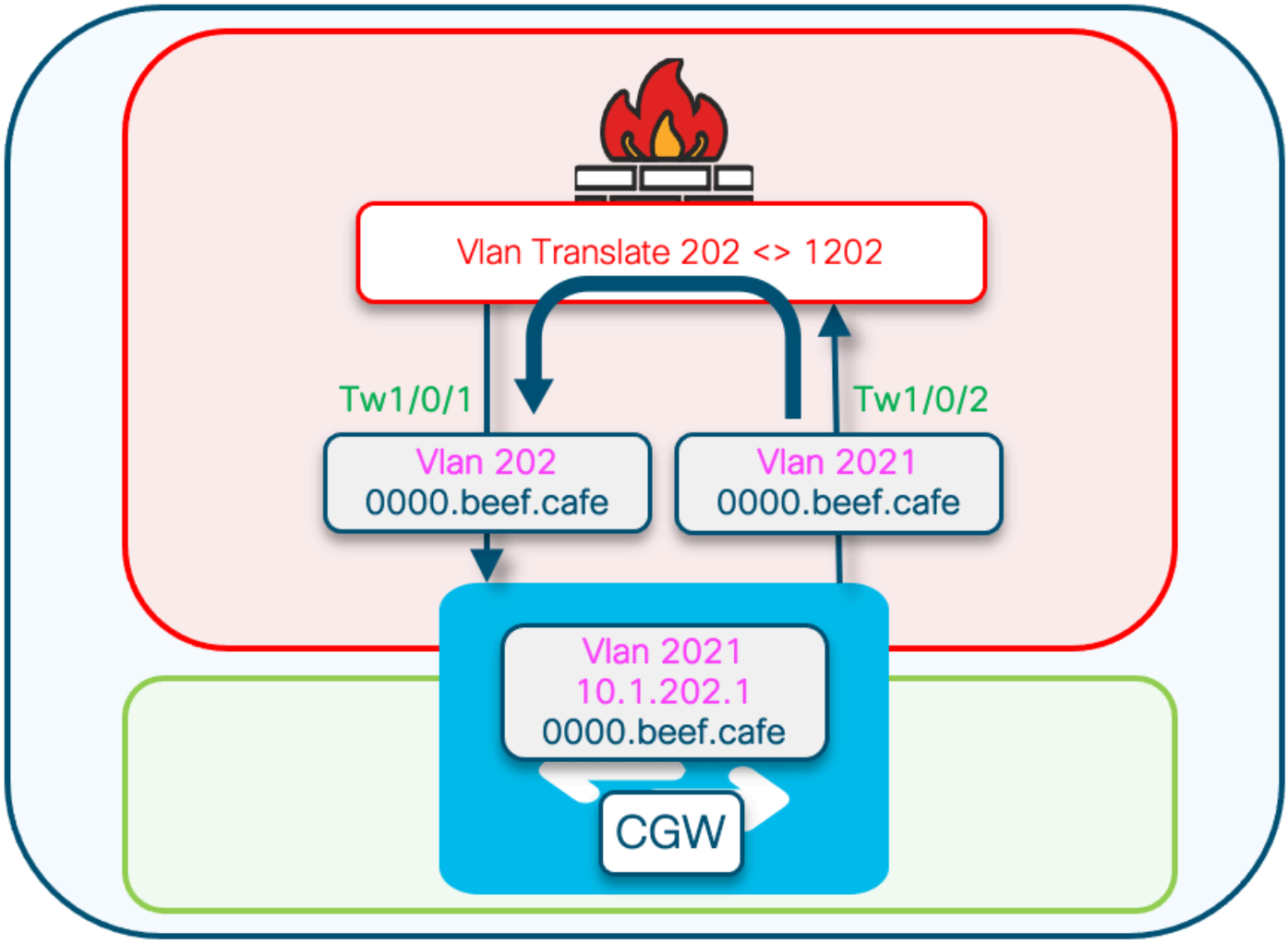
- Ao usar o design Parcialmente isolado com gateway externo, configurações adicionais são necessárias no CGW para anunciar o MAC-IP RT2 com o atributo de gateway padrão (DEF GW).



Observação: observação: esta seção também funciona para descrever uma implementação de Segmento Protegido Totalmente Isolado, que também usa um GW que é anunciado na estrutura (em comparação com GW fora da estrutura).

Diagrama de Rede


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



Detalhes da chave L2 VTEP (Leaf)

O pacote de solicitação vem do cliente

- Use o mac CGW anunciado Gw padrão.
- Se houver mais de um gw, o primeiro gw mac será usado.
- Converta o MAC de broadcast externo (iniciado pelo cliente: D e R em DORA) para o mac GW unicast e encaminhe para o CGW

O rastreamento de DHCP adiciona: opção 82 subopções: circuito e RID

(O RID é usado pelo processamento de pacotes de resposta no CGW)

(Informa ao CGW que não é local e ao fabric relay de volta para 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')

- Pacotes de resposta recebidos do CGW pelo túnel vxlan.
- Leaf Strips opção 82.
- Adiciona entradas de associação com a interface de origem do cliente. (vxlan-mod-port fornece a interface de origem do cliente).
- Pacote de resposta encaminhado ao cliente.

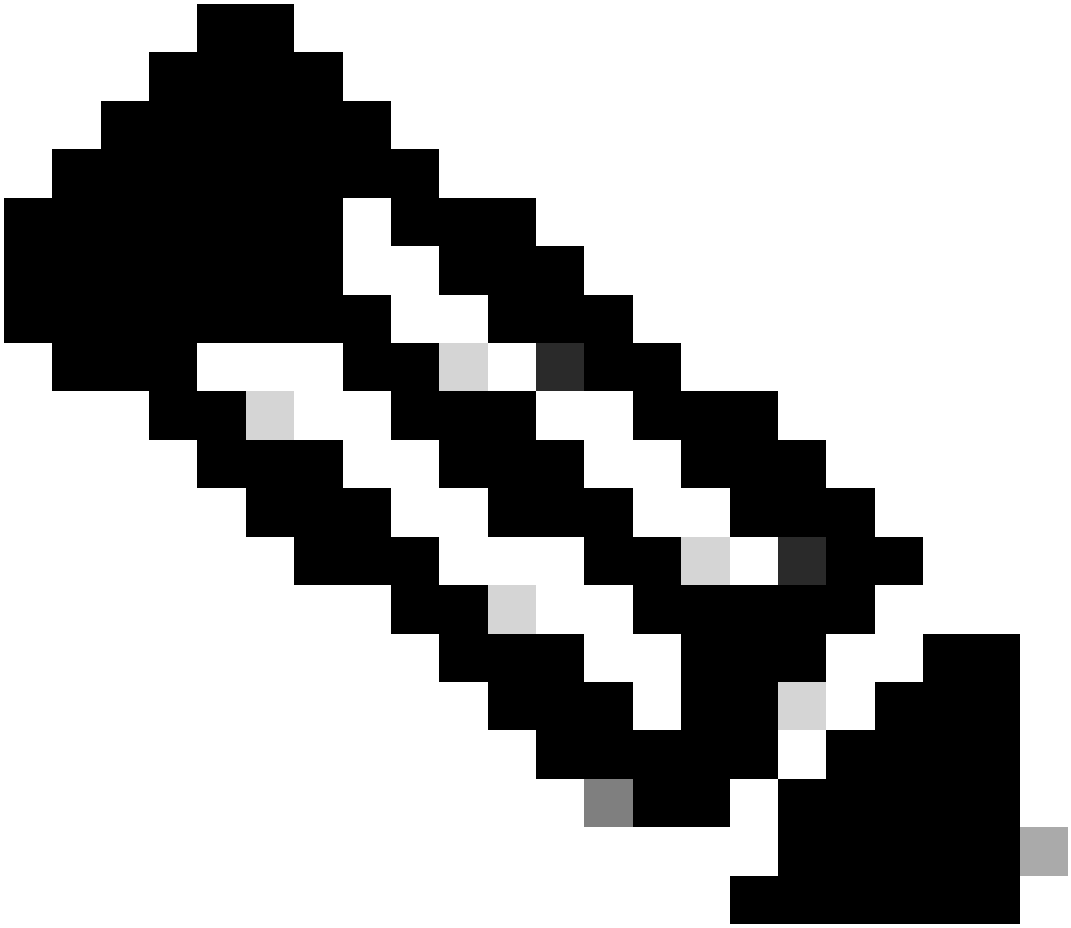
Detalhes principais do L3 VTEP (CGW)

- Habilite o RASTREAMENTO DHCP
- Habilite o DHCP RELAY no SVI
- A solicitação é recebida do L2VTEP e é fornecida ao relé.
- Relay adiciona outras subopções da opção 82 (gi, substituição de servidor, etc.) e envia para o servidor DHCP
- A resposta DHCP do servidor DHCP primeiro chega ao componente RELAY.
- Depois que RELAY retira os parâmetros da opção 82 (endereço gi, substituição de servidor e assim por diante), o pacote é passado para o componente de snooping dhcp
- O componente de rastreamento verifica o RID (ID do roteador) e, se seu local não remover a opção 82, subopções 1 e 2
- O pacote Fabric Relays (já que o RID não é local) é encaminhado diretamente ao cliente remoto
- Usa o cliente Mac e faz a injeção de bridge. O hardware faz a consulta do cliente mac e encaminha o pacote com vxlan encap para o L2VTEP de origem.

Etapas necessárias para oferecer suporte ao DHCP L2 Relay:

1. Habilitar aprendizagem local de IP
2. Criar uma política com a limpeza desabilitada
3. Anexar a evi/vlans de gateway externo
4. Adicione entradas estáticas na tabela de controle de dispositivos para o gateway externo mac-ip
5. Crie o mapa de rotas BGP para corresponder aos prefixos MAC-IP de RT2 e defina a comunidade estendida do gateway padrão
6. Aplicar mapa de rota aos vizinhos do refletor de rota BGP
7. Verifique se o relé DHCP tem a configuração correta para lidar com a opção adicional
8. Configurar o DHCP Snooping na vlan da estrutura e na vlan GW externa

---



Observação: nenhuma alteração de configuração é necessária nos Leafs de acesso para oferecer suporte ao DHCP L2 Relay com gateway externo.

CGW

Habilitar aprendizagem 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
```

Criar uma política com a limpeza desabilitada

<#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
```

Anexar a evi/vlans 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
```

Adicionar entradas estáticas na tabela de controle de dispositivos para o gateway externo 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
```

Crie o mapa de rotas BGP para corresponder aos prefixos MAC-IP de RT2 e defina a comunidade estendida do gateway padrão

<#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
```

Aplicar mapa de rota aos vizinhos do refletor de rota BGP

<#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
```

Verifique se o relé DHCP tem a configuração correta para lidar com as opções adicionais

<#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
```

Configurar o DHCP Snooping em vlans de estrutura e a vlan GW externa

<#root>

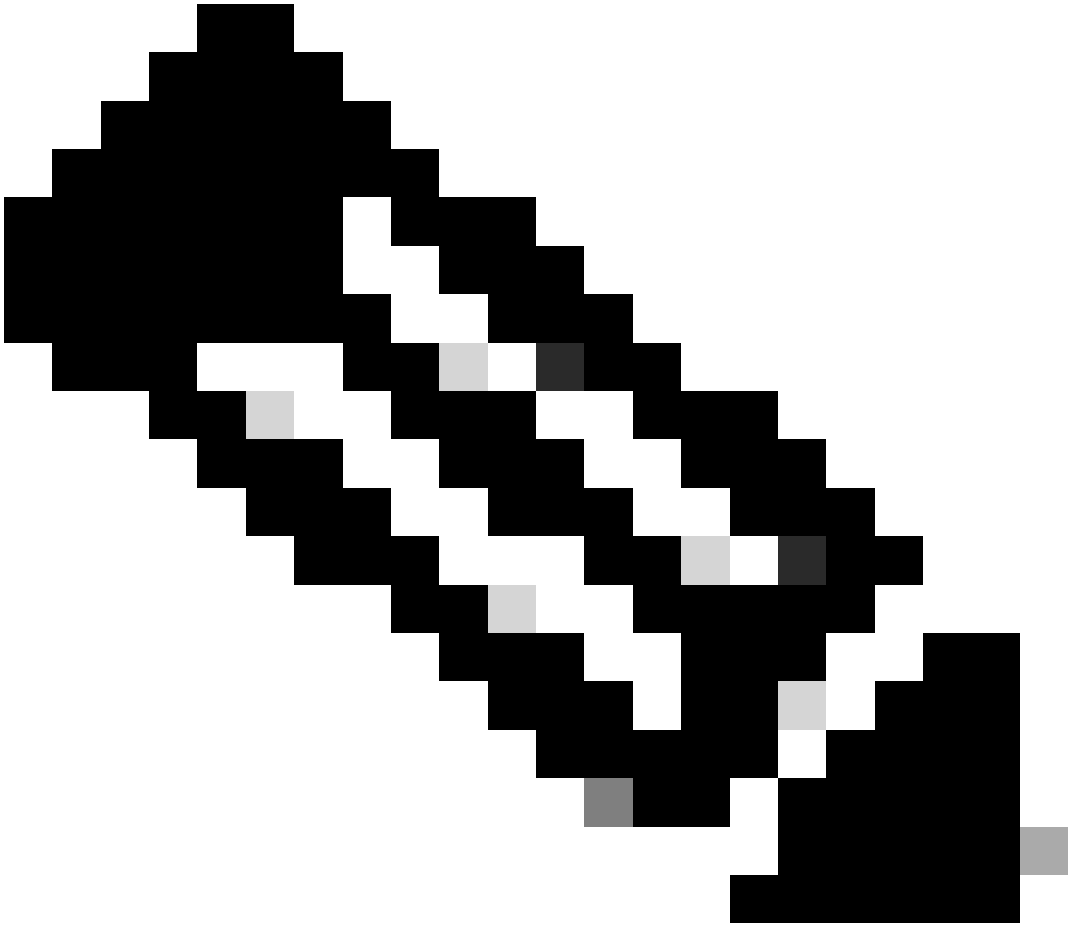
```
Leaf01#

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
```

Verifique se o uplink para o servidor DHCP é confiável no 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
```



Observação: devido à forma como o servidor é colocado no dispositivo de firewall, a

---

confiança do dispositivo foi configurada em ambos os links voltados para este dispositivo. No diagrama ampliado, você pode ver que a oferta chega a Tw1/0/1 e Tw1/0/2 neste design.

Verificar (Parcialmente isolado protegido)

Prefixo do gateway (folha)

<#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 (Folha)

Confirme se o Leaf instalou o CGW remote MAC no 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 (Folha)

<#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

Rastreamento de DHCP (Leaf e CGW)

Confirme se o rastreamento de DHCP está habilitado na folha na vlan da estrutura

<#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 se o rastreamento de DHCP está habilitado no CGW na malha e nas vlans do gateway externo

<#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

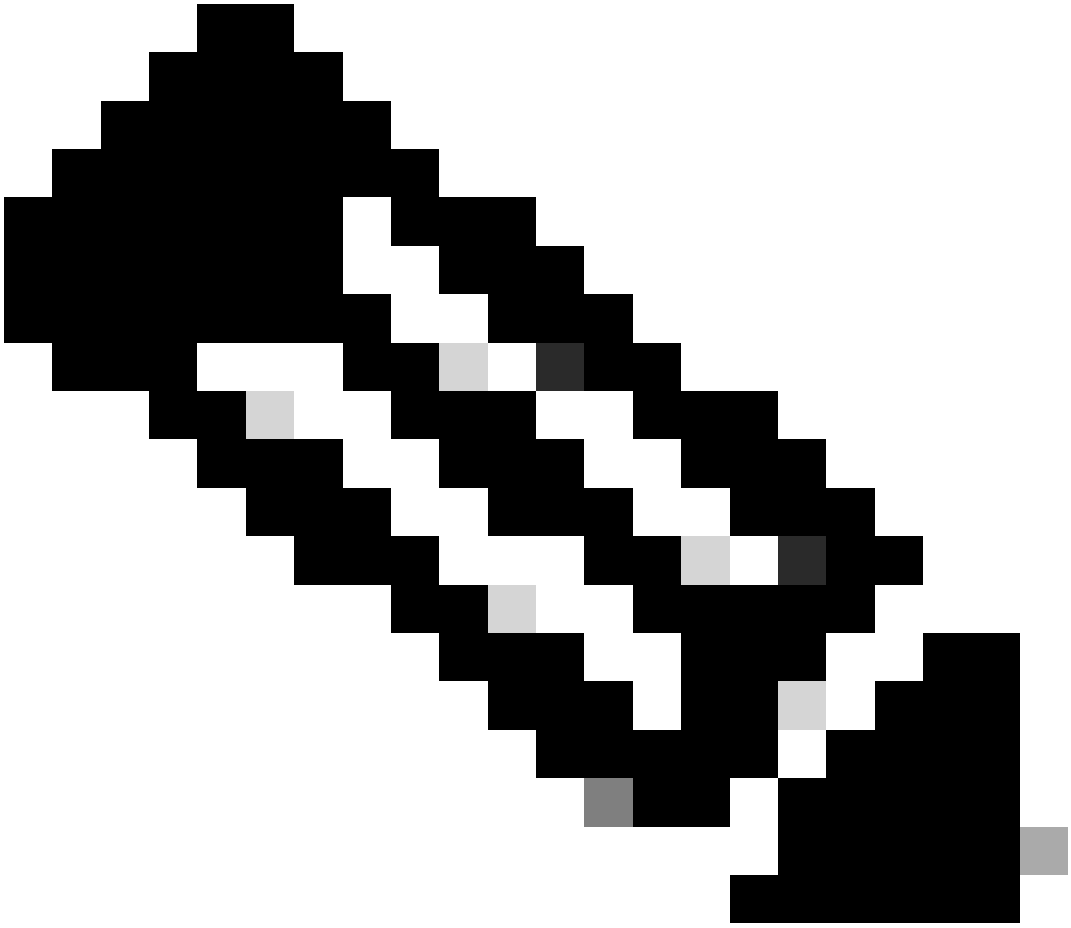
```
  Custom circuit-ids:
```

Confirme se a associação de rastreamento de DHCP foi criada

```
<#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
```

Solução de problemas (qualquer tipo de CGW)

As depurações são úteis para mostrar como os processos de rastreamento de DHCP e de L2 Relay estão lidando com pacotes DHCP.



Observação: essas depurações podem ser usadas para qualquer tipo de implantação que use o CGW com Relay DCHP L2.

Depurações de rastreamento de DHCP (Folha)

Debug Snooping para confirmar o processamento de pacotes

<#root>

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

Iniciar a tentativa de endereço DHCP do host

- Para este documento, um fechamento/não fechamento do SVI que é endereçado via DHCP foi executado para acionar a troca DORA
- Para o host Windows, você pode fazer um ipconfig /release > ipconfig /renew

Colete as depurações do show logging ou da janela do terminal

DHCP DISCOVER

A descoberta é vista vindo da porta voltada para o 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 DHCP

A oferta é vista chegando da interface de túnel de estrutura

<#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

SOLICITAÇÃO DHCP

A solicitação é vista da porta voltada para o 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
```

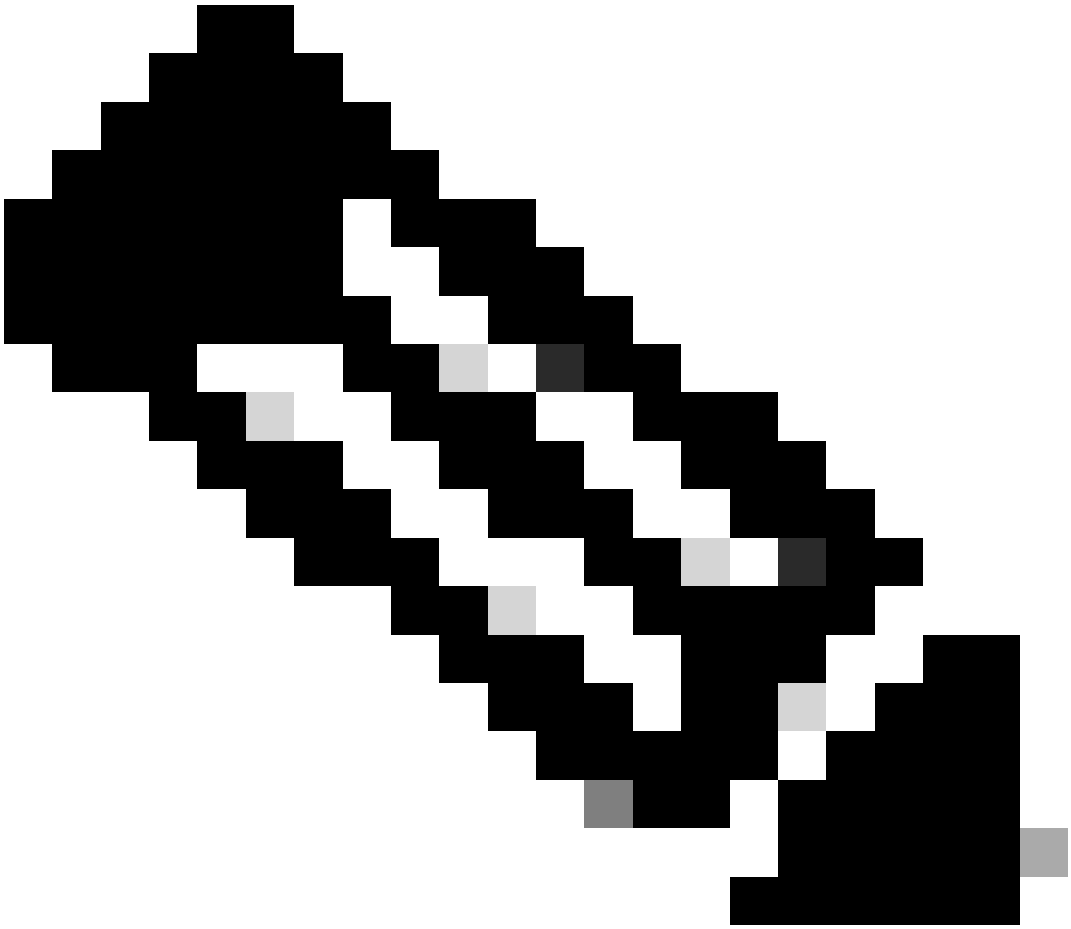
DHCP ACK

A confirmação é vista chegando da interface de túnel de estrutura

```
<#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.



> Observação: essas depurações são cortadas. Eles produzem um dump de memória do pacote, mas a anotação dessa parte do resultado da depuração está fora do escopo deste documento.

Depurações de rastreamento de DHCP (CGW)

DHCP DISCOVER

Devido à forma como o pacote é enviado e recebido de volta no CGW (com hairpin no firewall), as depurações são acionadas duas vezes

Chegando da estrutura na interface do túnel e enviando Tw 1/0/1 para o firewall na vlan da estrutura 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

Chegando do Firewall em Tw 1/0/2 na Vlan 2021 para ser enviado ao SVI e auxiliar para o 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 DHCP

Chega do servidor DHCP de volta ao SVI 2021, onde o auxiliar é configurado e encaminhado ao 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

Chega do firewall na vlan da estrutura e é enviado do CGW para a estrutura em direção à Leaf

<#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

SOLICITAÇÃO 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

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

Captura integrada

Use EPC para confirmar se a troca de pacotes DHCP e os parâmetros estão corretos

- Isso é mostrado da perspectiva do CGW, mas o processo pode ser repetido na Folha para verificar a troca de pacotes
- Este exemplo mostra a Descoberta, pois o processo e a análise são os mesmos para os outros pacotes DHCP

Verificar a rota para o Loopback Leaf

<#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
```

Configurar captura para execução em links voltados para o 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 a captura, acione seu host para solicitar um endereço IP DHCP, interrompa a captura

<#root>

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

Exibir o resultado da captura começando com a Descoberta de DHCP (Preste atenção na ID da transação para confirmar se este é o mesmo 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

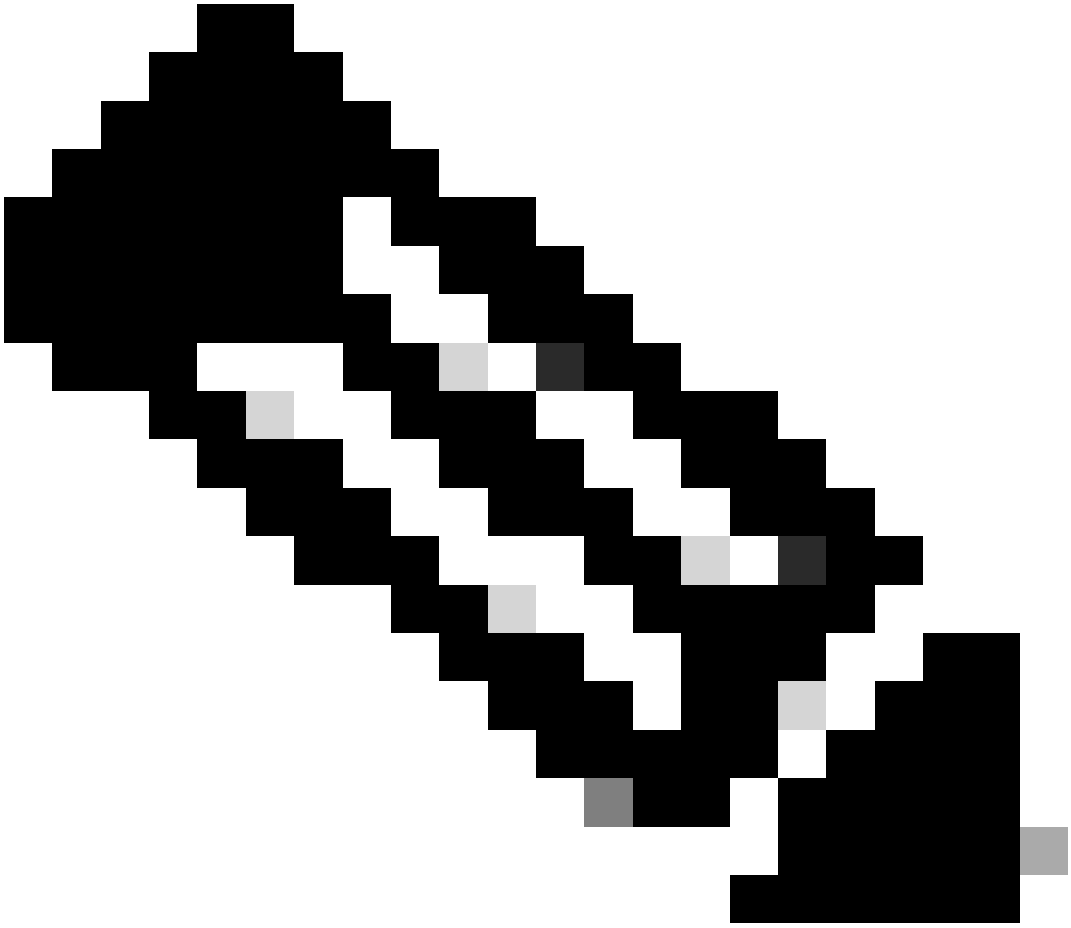
Option: (53) DHCP Message Type (Discover)

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
```



Observação: a ferramenta Capture pode ser usada em qualquer Leafs ou CGW para determinar o último ponto em que uma parte da troca DHCP DORA é suspeita de estar falhando.

Verificar estatísticas de rastreamento para de erros

<#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 caminho de punt para rastreamento de DHCP

- CoPP é o componente principal que descarta pacotes no caminho 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
```

Outro comando muito útil para localizar onde uma possível inundação de pacotes está ocorrendo é 'show platform software fed switch ative punt rates interfaces"

- Isso é muito útil para encontrar uma interface de origem onde a inundação está ocorrendo, o que está congestionando o caminho de punt e afetando o tráfego legítimo limitado pela 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...>
```

Estatísticas do Cliente de Rastreamento de DHCP

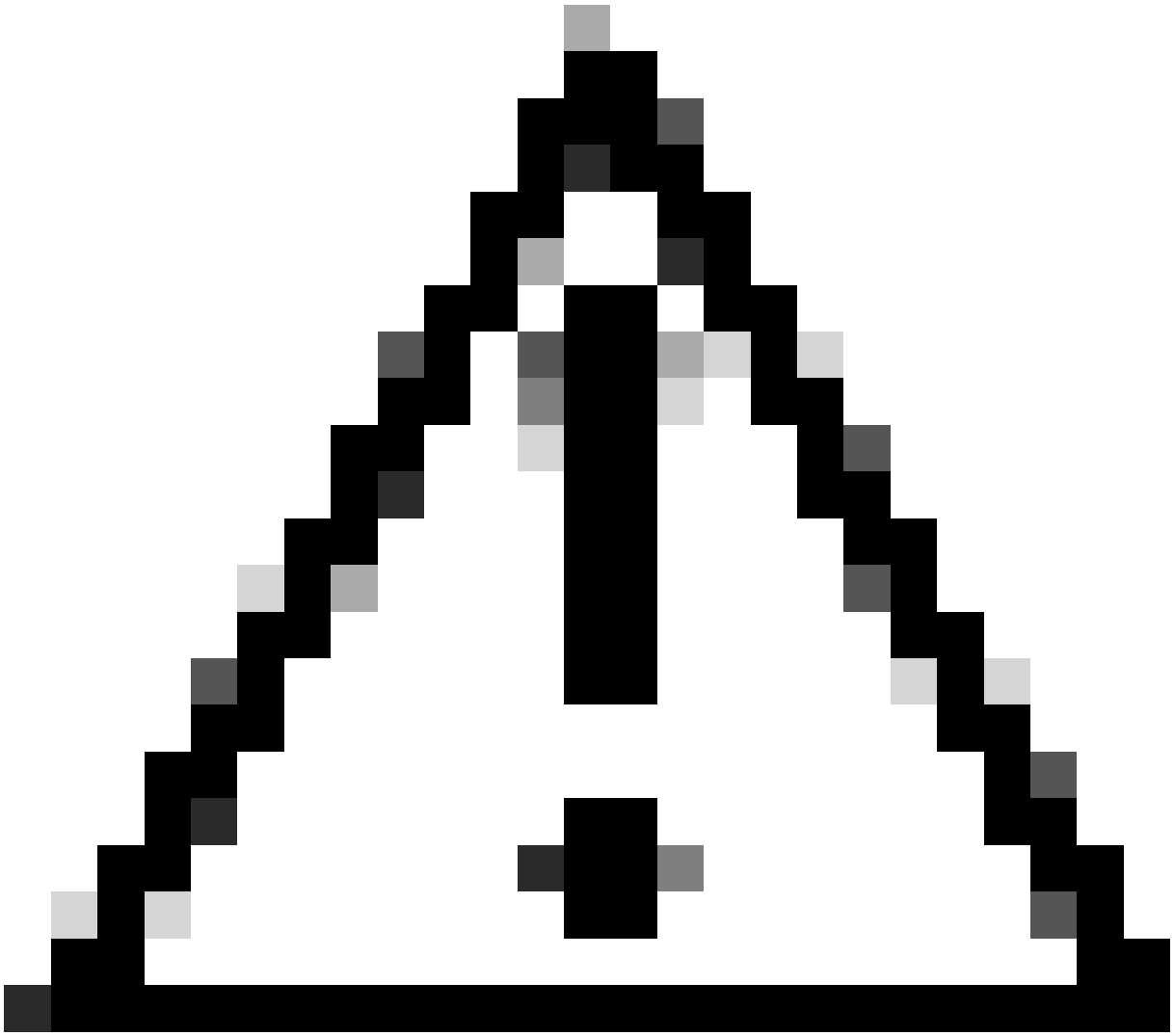
Observe a troca de mensagens DHCP usando esse comando. Isso pode ser executado no Leaf ou no CGW para ver o rastreamento de eventos

<#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
```

Depurações adicionais

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



Cuidado: tenha cuidado ao executar depurações!

Informações Relacionadas

- Implemente a política de roteamento BGP EVPN nos switches Catalyst 9000 Series
- Implemente a segmentação BGP EVPN Protected Overlay em switches Catalyst 9000 Series
- Operar e solucionar problemas de rastreamento de DHCP em switches Catalyst 9000

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.