在Catalyst 9000系列交換機上實施BGP EVPN DHCP第2層中繼

目錄

簡介

本文檔介紹如何配置、驗證EVPN VxLAN DHCP L2中繼功能並對其進行故障排除。

必要條件

需求

- 在使用DHCP的任何CGW型別部署中都使用此功能
- 如果實施保護分段，請查閱這些文檔
  - 在Catalyst 9000系列交換器上實作BGP EVPN路由原則
  - 在Catalyst 9000系列交換機上實施BGP EVPN保護覆蓋分段

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

檔案詳細資訊

本文檔可用於任何CGW部署，其中DHCP需要從沒有SVI的枝葉中繼到中央網關。

- 如果您未使用受保護的分段，請使用文檔中SVI通告到交換矩陣中的部分

如果要實施受保護分段，本文檔是3個相互關聯的文檔中的第2部分：

- 文檔1：在Catalyst 9000系列交換機上實施BGP EVPN路由策略介紹了如何控制重疊中的BGP BUM流量，必須首先進行配置
- 文檔2：在Catalyst 9000系列交換機上實施BGP EVPN受保護的重疊分段在文檔1的重疊設計和策略的基礎上實施，描述「protected」關鍵字的實施。
- 檔案3：本檔案。以上兩個文檔為基礎，描述了僅使用第2層枝葉和CGW實現DHCP中繼的方式

L2中繼行為

轉送	窺探	核心泛洪	訪問泛洪	IPv4
是	是	否	是	• 選項82子選項：(1)代理電路ID (vni-mod-port)使用dhcp監聽填充 • 可以使用dhcp trust配置限制接入端 *建議機型
是	否	是	是	• 選項82子選項：(1)代理電路ID (vlan-mod-port)使用dhcp監聽填充
否	是	否	是	• 選項82子選項：(1)代理電路ID (vni-mod-port)使用dhcp監聽填充 • 可以使用dhcp trust配置限制接入端
轉送	窺探	核心泛洪	訪問泛洪	IPv6
是	是	是	是	• 選項82子選項：(1)代理電路ID (vni-mod-port)使用dhcp監聽填充 • 可以使用dhcp trust配置限制接入端
是	否	是	是	• 選項82子選項：(1)代理電路ID (vlan-mod-port)使用dhcp監聽填充
否	是	是	是	• 選項82子選項：(1)代理電路ID (vni-mod-port)使用dhcp監聽填充 • 可以使用dhcp trust配置限制接入端
否	否	是	是	

技術

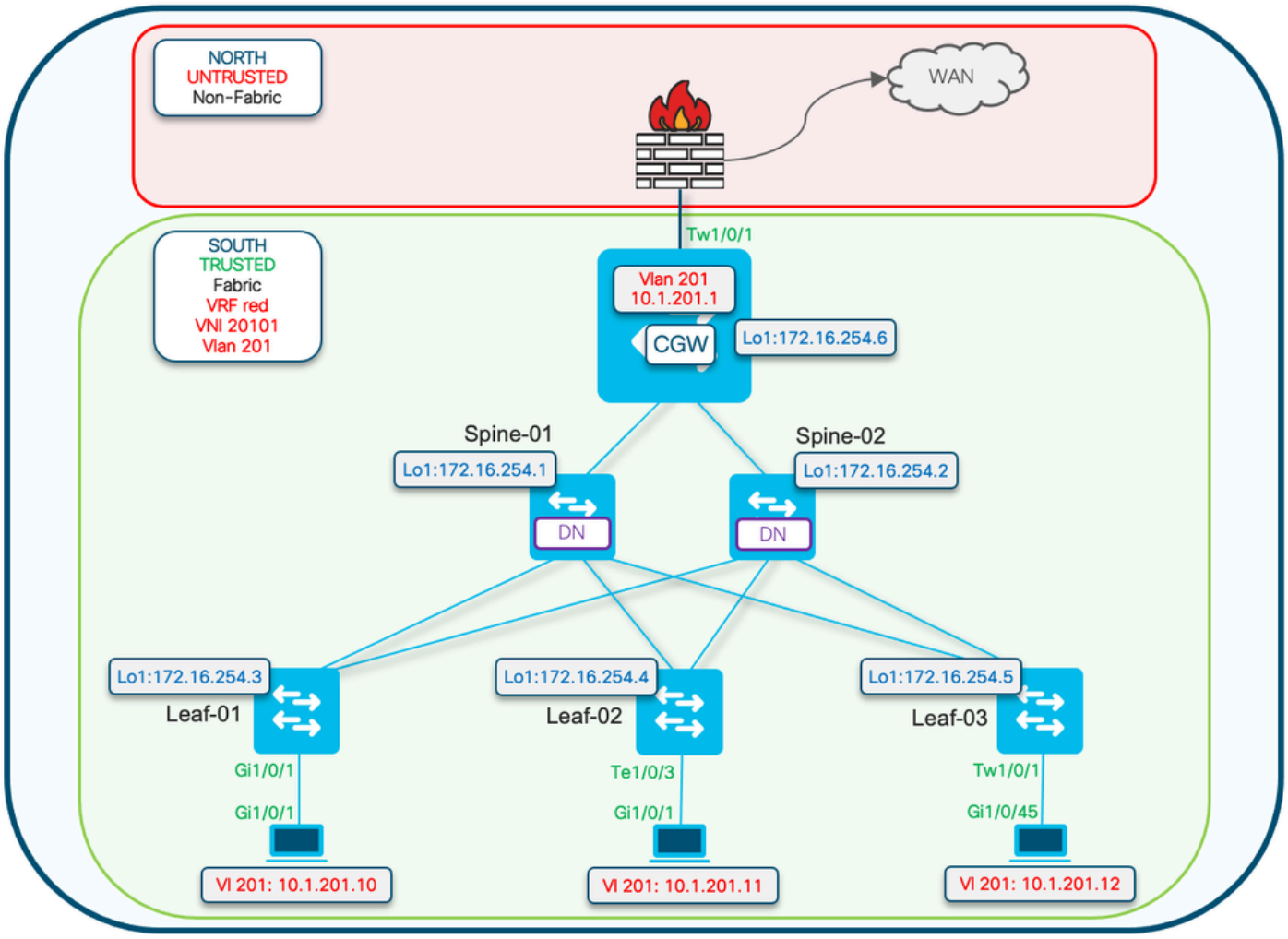
VRF	虛擬路由轉送	定義與其他VRF和全局IPv4/IPv6路由域分開的第3層路由域
AF	地址系列	定義BGP處理的型別字首和路由資訊

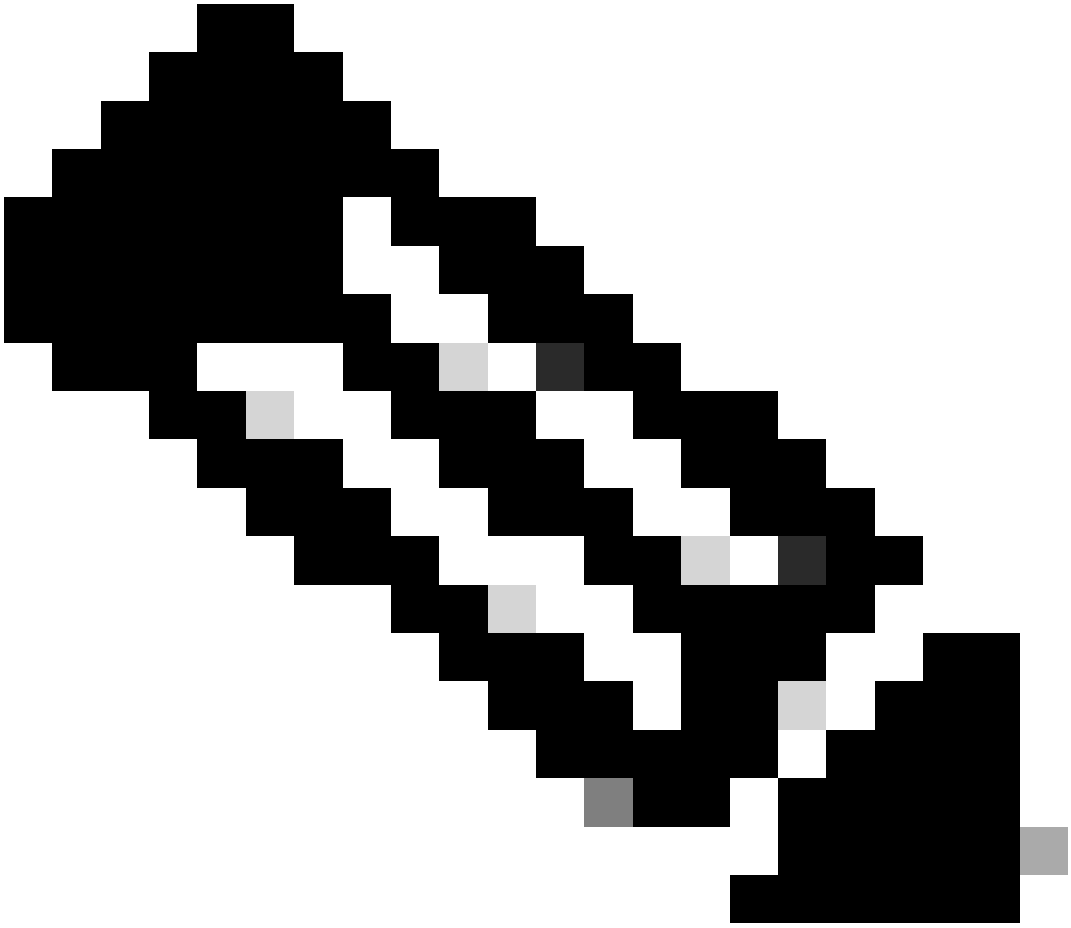
AS	自治系統	屬於某個網路或網路集合的一組網際網路可路由IP字首，它們全部由單個實體或組織管理、控制和監督
EVPN	乙太網路虛擬私人網路	允許BGP傳輸第2層MAC和第3層IP資訊的擴展是EVPN，它使用多協定邊界網關協定(MP-BGP)作為協定，以分發屬於VXLAN重疊網路的可達性資訊。
VXLAN	虛擬可擴充LAN（區域網路）	VXLAN的用途是克服VLAN和STP的固有限制。建議的IETF標準[RFC 7348]可提供與VLAN相同的乙太網第2層網路服務，但具有更高的靈活性。從功能上講，它是UDP內MAC封裝協定，在第3層底層網路上作為虛擬重疊運行。
CGW	集中網關	以及網關SVI不在每個枝葉上的EVPN的實施。相反，所有路由都由使用不對稱IRB（整合路由和橋接）的特定枝葉完成
DEF網關	預設閘道	在「l2vpn evpn」配置部分下，透過「default-gateway advertise enable」命令增加到MAC/IP字首的BGP擴展社群屬性。
IMET (RT3)	內含組播乙太網標籤（路由）	也稱為BGP型別3路由。此路由型別用於EVPN中在VTEP之間傳送BUM（廣播/未知單點傳播/多點傳送）流量。
RT2	路由型別2	代表主機MAC或閘道MAC-IP的BGP MAC或MAC/IP首碼
EVPN管理器	EVPN管理員	各種其他元件的中央管理元件（例如：從SISF獲知並向L2RIB傳送訊號）
SISF	交換機整合安全功能	EVPN使用的唯一主機跟蹤表，用於瞭解枝葉上存在哪些本地主機
L2RIB	第2層路由資訊庫	在用於管理BGP、EVPN管理器、L2FIB之間的互動的中間元件中
FED	轉發引擎驅動程式	對ASIC（硬體）層進行程式設計
MATM	Mac位址表管理員	IOS MATM：僅安裝本地地址和 FED MATM：安裝從控制平面獲知的本地和遠端地址的硬體表，屬於硬體

		轉發平面的一部分

配置（標準CGW部署）

網路圖表





注意：本部分介紹不使用受保護功能的標準CGW部署。

- 顯示DHCP DORA資料包交換的調試僅在受保護網段示例中顯示

L2 VTEP（枝葉）金鑰詳細資訊

請求資料包來自客戶端

- 使用預設gw通告CGW MAC。
- 如果存在多個gw，則使用第一個gw mac。
- 將外部廣播MAC（客戶端發起：DORA中的D和R）轉換為單播GW MAC並轉發到CGW

DHCP監聽增加：選項82子選項：電路和RID

（RID由CGW上的響應pkt處理使用）。

（通知CGW其非本地和交換矩陣中繼返回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')
```

- 透過vxlan隧道從CGW收到響應資料包。
- 分葉帶選項82。
- 增加具有客戶端源介面的繫結條目。（vxlan-mod-port提供客戶端源介面）。
- 將響應資料包轉發到客戶端。

L3 VTEP (CGW)主要詳細資訊

- 啟用DHCP監聽
- 在SVI中啟用DHCP中繼
- 從L2VTEP接收請求，並將其提供給中繼。
- 中繼增加其他選項82子選項（gi、伺服器覆蓋等）並傳送到DHCP伺服器。
- 來自dhcp伺服器的DHCP響應首先進入RELAY元件。
- 在RELAY刪除選項82引數（gi地址、伺服器覆蓋等）後，資料包將傳遞到dhcp監聽元件。
- 監聽元件會檢查RID （路由器ID），如果它不是本機的，就不會移除選項82子選項1和2。
- 交換矩陣中繼（因為RID不是本地的）資料包直接轉發到遠端客戶端。
- 使用客戶端Mac並進行網橋插入。 硬體執行客戶端mac查詢，並將具有vxlan封裝的資料包轉發到始發L2VTEP。

L2VTEP

配置EVPN例項

<#root>

```
Leaf-01#
```

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

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

啟用DHCP監聽

<#root>

```
Leaf-01#
```

```
show run | sec dhcp snoop
```

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

```
201
```

```
ip dhcp snooping
```

CGW

配置EVPN例項

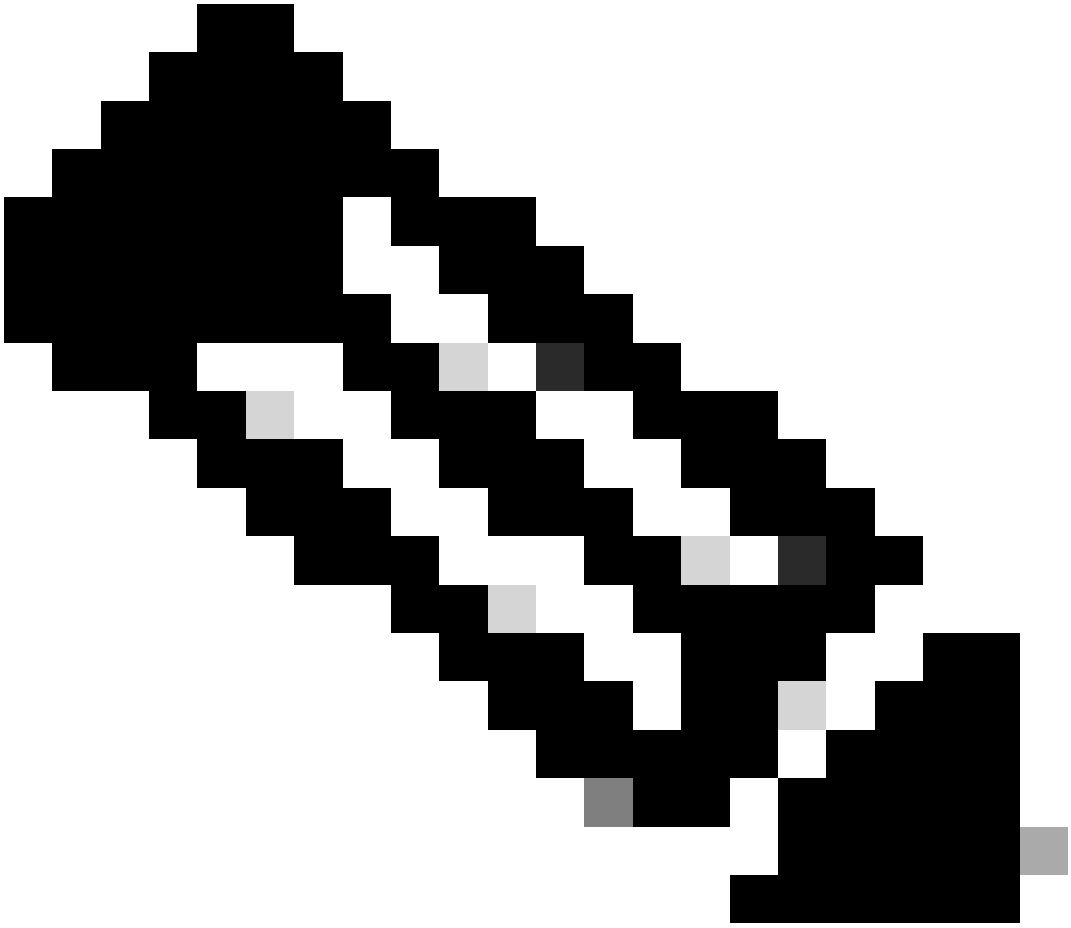
<#root>

```
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
```



注意： DEF GW屬性對於L2中繼瞭解要將DHCP資料包封裝和傳送到誰至關重要。

啟用DHCP監聽

<#root>

Border#

sh run | s dhcp snoop

ip dhcp snooping vlan 101,

201

ip dhcp snooping

確保DHCP中繼具有正確的配置以處理附加選項

<#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

驗證（標準CGW部署）

網關字首（枝葉）

<#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（分葉）

<#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
```

本地MAC（枝葉）

<#root>

```
Leaf-01#

show switch


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

682c.7bf8.8700

     1      V01     Ready

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

DHCP監聽（枝葉和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
```

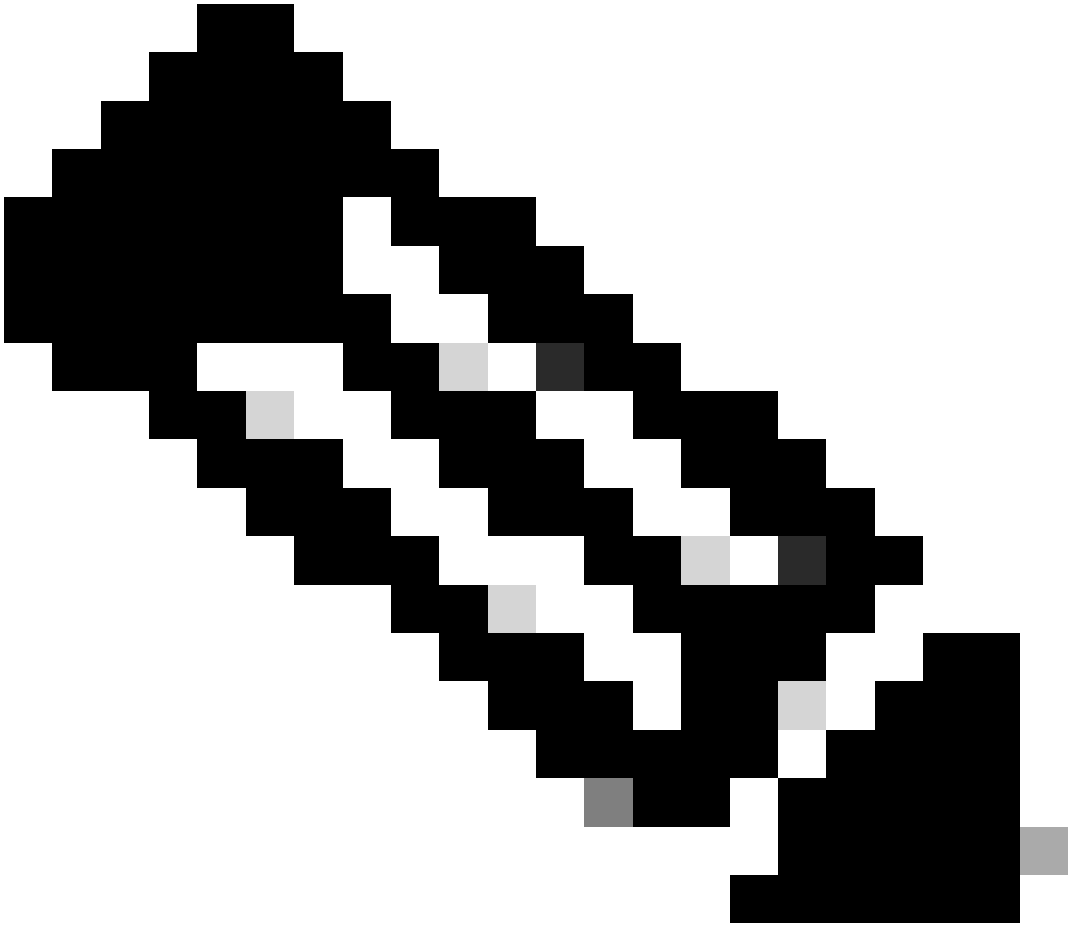
```
DHCP snooping is operational on following VLANs:
```

```
101,201
```

配置（部分隔離保護）

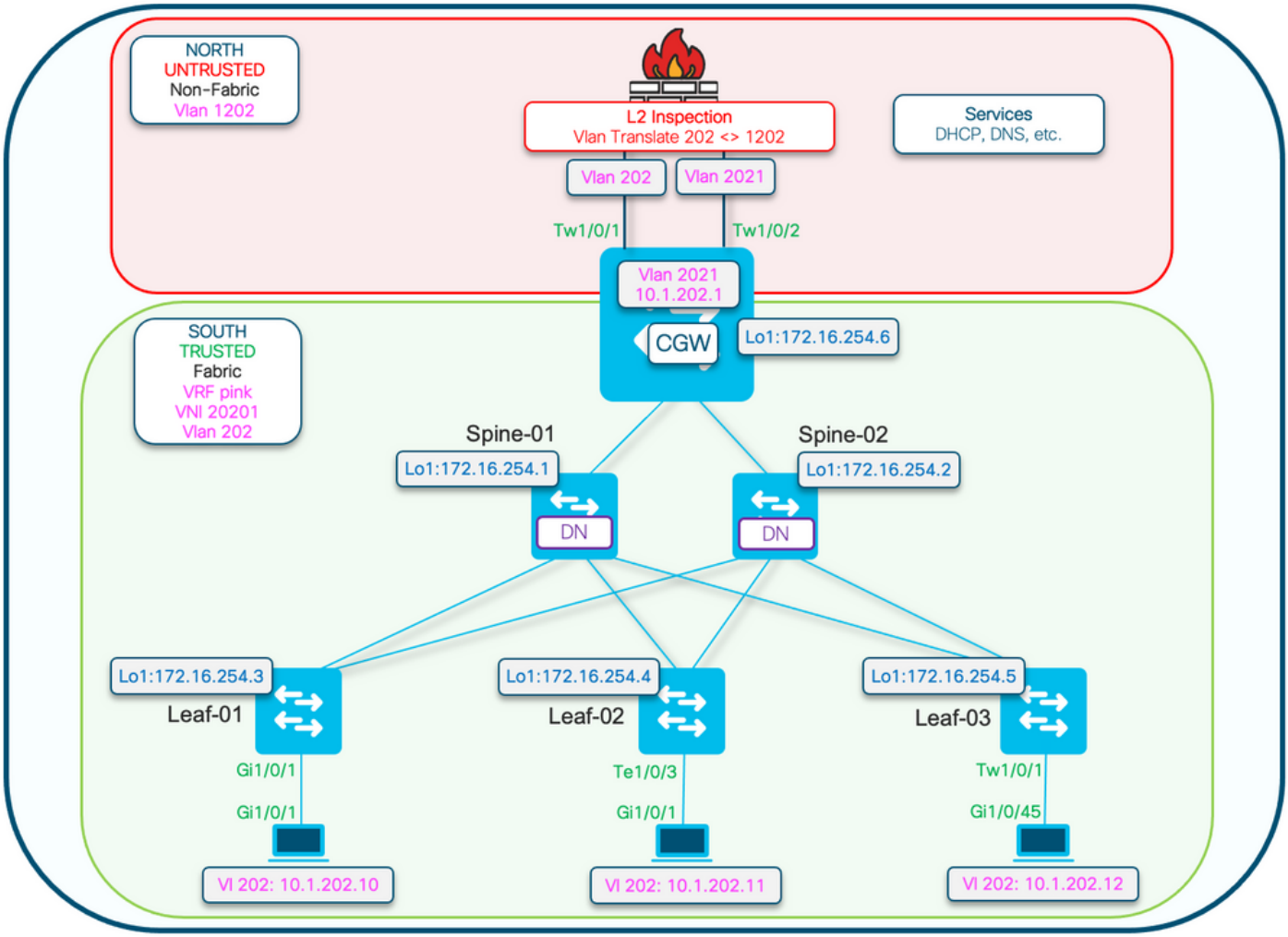
接入枝葉上的DHCP監聽依賴於來自CGW的預設網關路由來學習網關MAC以將DHCP資料包轉發到。

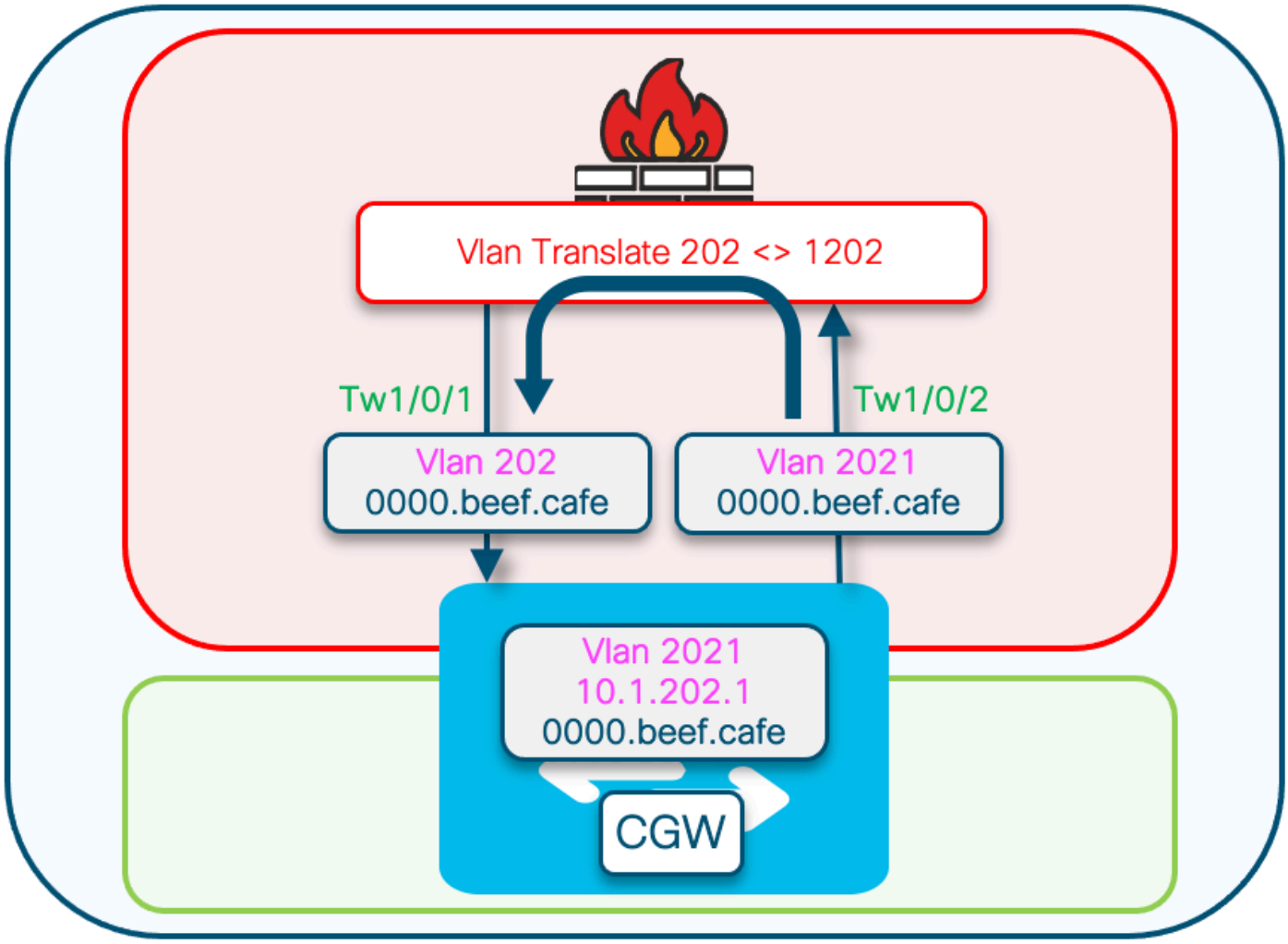
- 使用部分隔離設計和外部網關時，CGW上需要額外的配置來使用預設網關(DEF GW)屬性通告MAC-IP RT2。



注意：本部分還介紹完全隔離的受保護分段實施，該實施還使用通告到交換矩陣中的GW（與交換矩陣外部的GW相比）。

網路圖表


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



L2 VTEP（枝葉）金鑰詳細資訊

請求資料包來自客戶端

- 使用預設gw通告CGW MAC。
- 如果存在多個gw，則使用第一個gw mac。
- 將外部廣播MAC（客戶端發起：DORA中的D和R）轉換為單播GW MAC並轉發到CGW

DHCP監聽增加：選項82子選項：電路和RID

（RID由CGW上的響應pkt處理使用）。

（通知CGW其非本地和交換矩陣中繼返回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')
```

- 透過vxlan隧道從CGW收到響應資料包。
- 分葉帶選項82。
- 增加具有客戶端源介面的繫結條目。（vxlan-mod-port提供客戶端源介面）。
- 將響應資料包轉發到客戶端。

L3 VTEP (CGW)主要詳細資訊

- 啟用DHCP監聽
- 在SVI中啟用DHCP中繼
- 從L2VTEP接收請求，並將其提供給中繼。
- 中繼增加其他選項82子選項（gi、伺服器覆蓋等）並傳送到DHCP伺服器。
- 來自dhcp伺服器的DHCP響應首先進入RELAY元件。
- 在RELAY刪除選項82引數（gi地址、伺服器覆蓋等）後，資料包將傳遞到dhcp監聽元件。
- 監聽元件會檢查RID （路由器ID），如果它不是本機的，就不會移除選項82子選項1和2。
- 交換矩陣中繼（因為RID不是本地的）資料包直接轉發到遠端客戶端。
- 使用客戶端Mac並進行網橋插入。 硬體執行客戶端mac查詢，並將具有vxlan封裝的資料包轉發到始發L2VTEP。

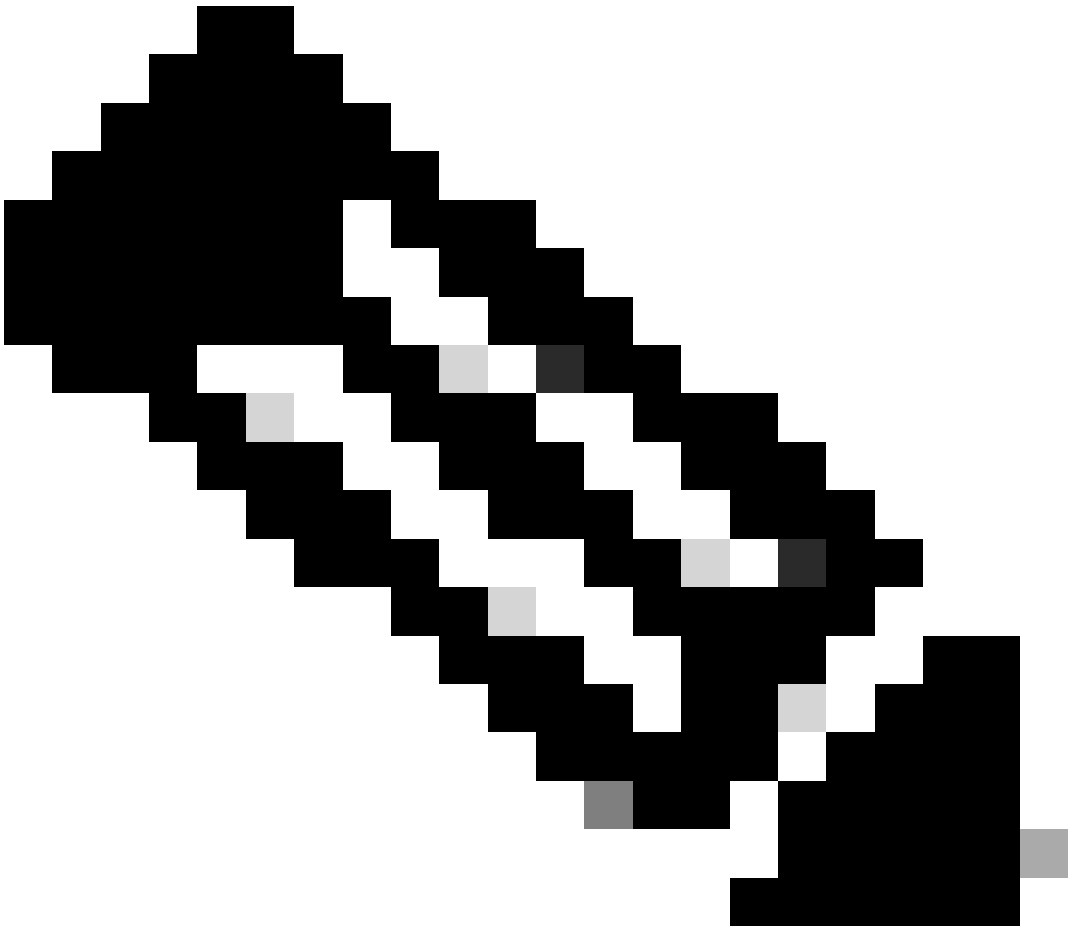
支援DHCP L2中繼所需的步驟：

1. 啟用ip local learning
2. 建立停用收集功能的策略
3. 連線到外部網關evi/vlan
4. 將靜態條目增加到外部網關mac-ip的裝置跟蹤表中
5. 建立BGP路由對映以匹配RT2 MAC-IP字首並設定預設網關擴展社群

6. 將路由對映應用到BGP路由反射器鄰居

7. 確保DHCP中繼具有正確的配置以處理附加選項

8. 在交換矩陣VLAN和外部GW VLAN上配置DHCP監聽



注意：無需對接入枝葉進行任何配置更改，即可支援帶有外部網關的DHCP L2中繼。

CGW

啟用ip local learning

<#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
```

建立停用收集功能的策略

<#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
```

連線到外部網關evi/vlan

<#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
```

將靜態條目增加到外部網關mac-ip的裝置跟蹤表中

<#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
```

建立BGP路由對映以匹配RT2 MAC-IP字首並設定預設網關擴展社群

<#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
```

將路由對映應用到BGP路由反射器鄰居

<#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
```

確保DHCP中繼具有正確的配置以處理附加選項

<#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
```

配置交換矩陣vlan和外部GW vlan上的DHCP監聽

<#root>

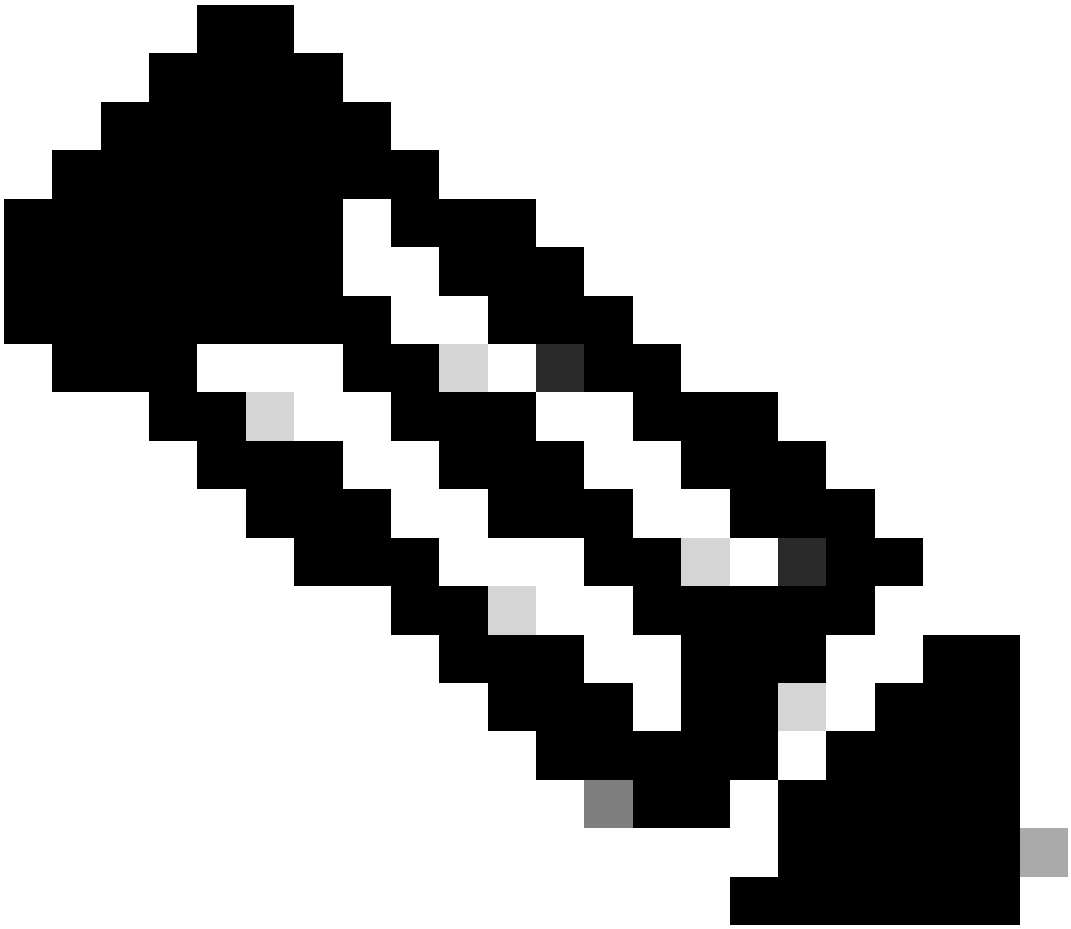
```
Leaf01#

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
```

確保到DHCP伺服器的上行鏈路在CGW上受信任

<#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
```



注意：由於伺服器置於防火牆裝置信任上的方式是在面向此裝置的兩個鏈路上配置的。在放大圖中，您可以看到此設計中的Offer同時到達Tw1/0/1和Tw1/0/2。

驗證（部分隔離保護）

網關字首（枝葉）

```
<#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（分葉）

確認枝葉已在硬體中安裝CGW遠端MAC

<#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

本地MAC（枝葉）

<#root>

Leaf01#

show switch

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

682c.7bf8.8700

```
     1      V01     Ready
```

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

DHCP監聽（枝葉和CGW）

確認已在交換矩陣VLAN中的枝葉上啟用DHCP監聽

<#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...>

確認已在交換矩陣和外部網關VLAN中的CGW上啟用DHCP監聽

<#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:

確認已建立DHCP監聽繫結

<#root>

Leaf01#

show ip dhcp snooping binding

MacAddress

IpAddress

        Lease(sec) Type   VLAN

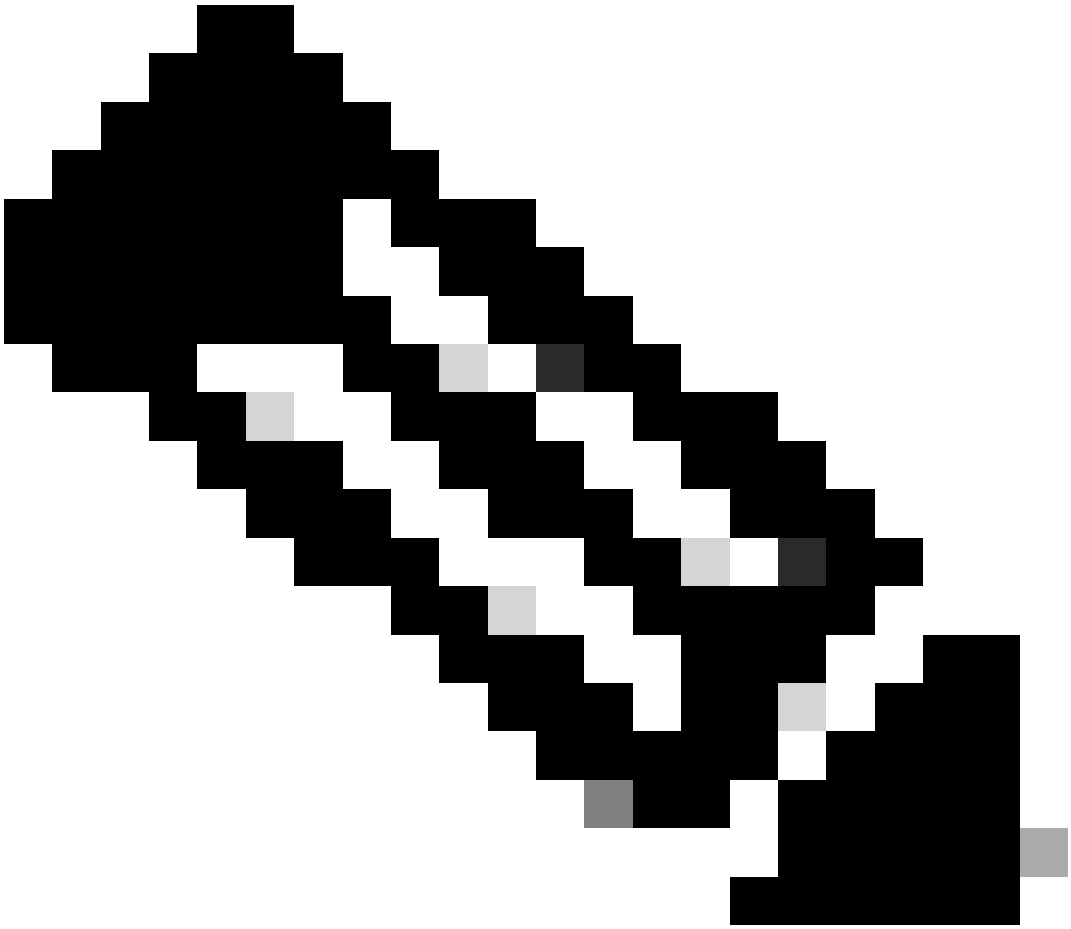
Interface

----------------- --------------- ---------- ------------- ---- --------------------

```
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
```

故障排除（任何CGW型別）

調試有助於顯示DHCP監聽和L2中繼進程如何處理DHCP資料包。



注意：這些調試可用於任何型別的使用帶DCHP L2中繼的CGW的部署。

DHCP監聽偵錯（分葉）

調試監聽以確認資料包處理

<#root>

Leaf01#

debug ip dhcp snooping packet

DHCP Snooping Packet debugging is on

Leaf01#

show debugging

DHCP Snooping packet debugging is on

開始主機DHCP地址嘗試

- 對於本文檔，透過DHCP定址的SVI執行shut/no shut以觸發DORA交換
- 對於Windows主機，可以執行ipconfig /release > ipconfig /renew

透過show logging或從終端窗口收集debug

DHCP發現

發現來自面向主機的埠

<#root>

*Sep 19 20:16:31.164:

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

*Sep 19 20:16:31.177:

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

, MAC da: ffff.ffff.ffff,

MAC sa: 0006.f601.cd43

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

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

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

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

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

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

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

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

DHCP提供

發現優惠從交換矩陣隧道介面到達

<#root>

```
*Sep 19 20:16:33.180:

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

*Sep 19 20:16:33.194:

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

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

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

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

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


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

DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1

*Sep 19 20:16:33.194:

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

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

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

DHCP請求

從面向主機的埠看到請求

<#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

發現確認從交換矩陣隧道介面到達

<#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:

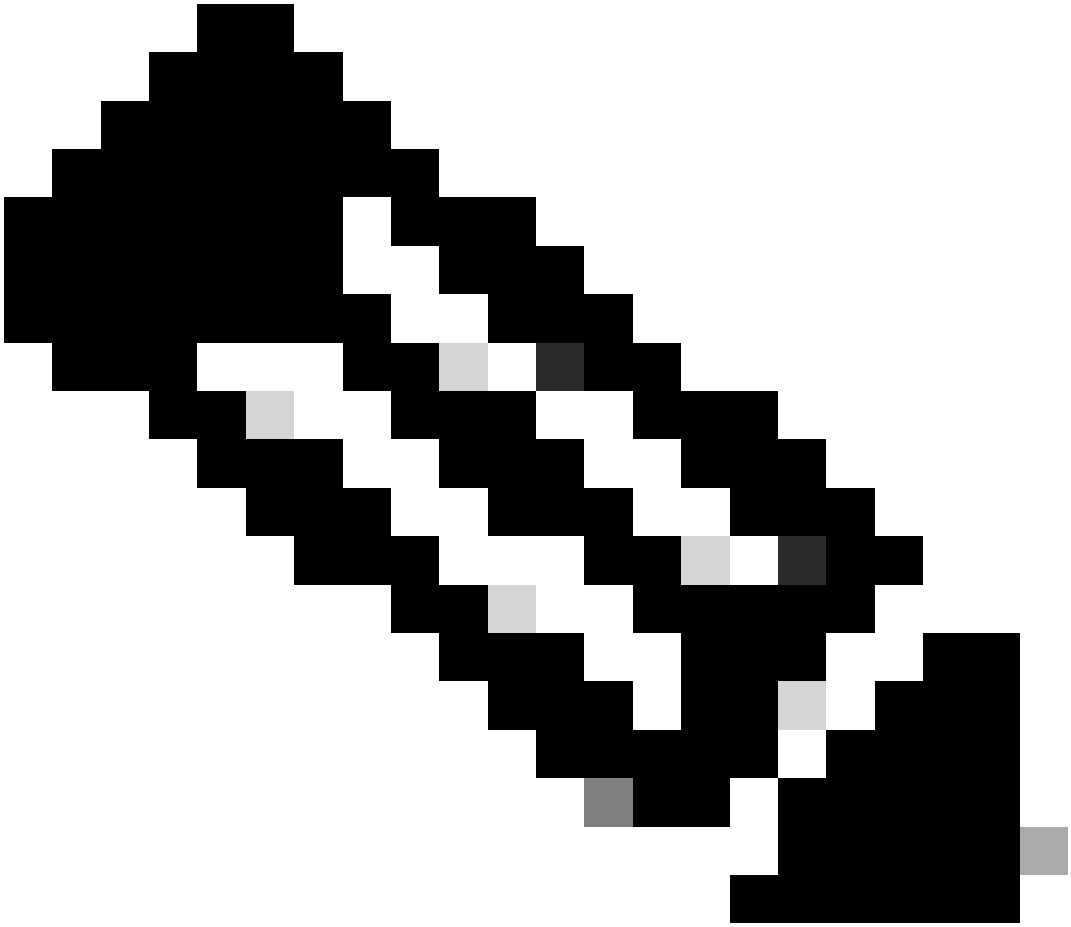
dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan_id 202

```
*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.



注意：這些調試被截斷。它們會產生封包的記憶體傾印，但偵錯結果此部分的註釋不在本檔案範圍內。

DHCP監聽偵錯(CGW)

DHCP發現

由於資料包在CGW上傳送和接收的方式（在防火牆上髮夾連線），調試會觸發兩次

從隧道介面上的交換矩陣到達並傳送Tw 1/0/1到交換矩陣VLAN 202中的防火牆

```
<#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
```

從Vlan 2021中Tw 1/0/2上的防火牆到達，將傳送到SVI和幫助程式到DHCP伺服器

```
<#root>

*Apr 16 14:37:43.901:

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


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

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


*Apr 16 14:37:43.911:

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


*Apr 16 14:37:43.911:

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

DHCP提供

從DHCP伺服器返回配置幫助程式的SVI 2021並將其轉發到防火牆

<#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

從交換矩陣VLAN中的防火牆到達，從CGW傳送到交換矩陣到枝葉

<#root>

*Apr 16 14:37:45.934:

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

*Apr 16 14:37:45.944:

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

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:45.944: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:

```
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.944: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.944: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.945:
```

DHCP_SNOOPING: opt82 data indicates not a local packet

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

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

DHCP請求

<#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

內嵌式擷取

使用EPC確認DHCP資料包交換和引數正確

- 這從CGW的角度顯示，但可以在枝葉上重複該過程以驗證資料包交換
- 此示例顯示Discover，因為其他DHCP資料包的過程和分析是相同的

檢查到枝葉環回的路由

<#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
```

配置在面向Leaf01的鏈路上運行的捕獲

```
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
```

啟動捕獲，觸發主機請求DHCP IP地址，停止捕獲

<#root>

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

檢視以DHCP發現開頭的捕獲結果（注意事務ID以確認此事件是否完全相同）

<#root>

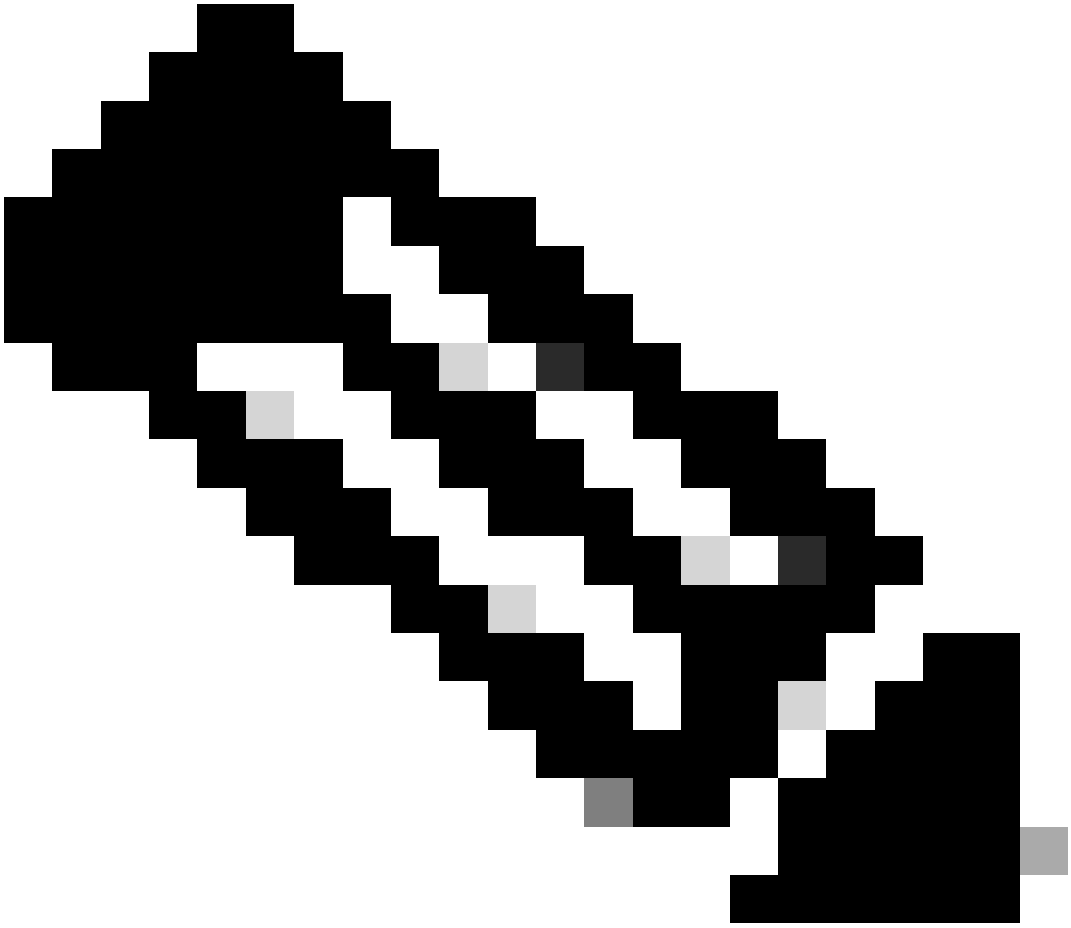
```
CGW#

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
```



注意：可在任何枝葉或CGW上使用捕獲工具來確定懷疑部分DHCP DORA交換失敗的最後一點。

驗證監聽統計資訊以查詢錯誤

<#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.
```

驗證DHCP監聽的傳送路徑

- CoPP是丟棄傳送路徑中的資料包的主要元件

<#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
```

另一個非常有用的命令，用於定位可能發生的資料包泛洪的位置，是「show platform software fed switch active punt rate interfaces」

- 這對於查詢發生泛洪的源介面非常有用，該泛洪導致傳送路徑擁塞並影響合法CPU限制流量

<#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監聽客戶端統計資訊

使用此命令觀察DHCP消息交換。可以在枝葉或CGW上運行以檢視事件跟蹤

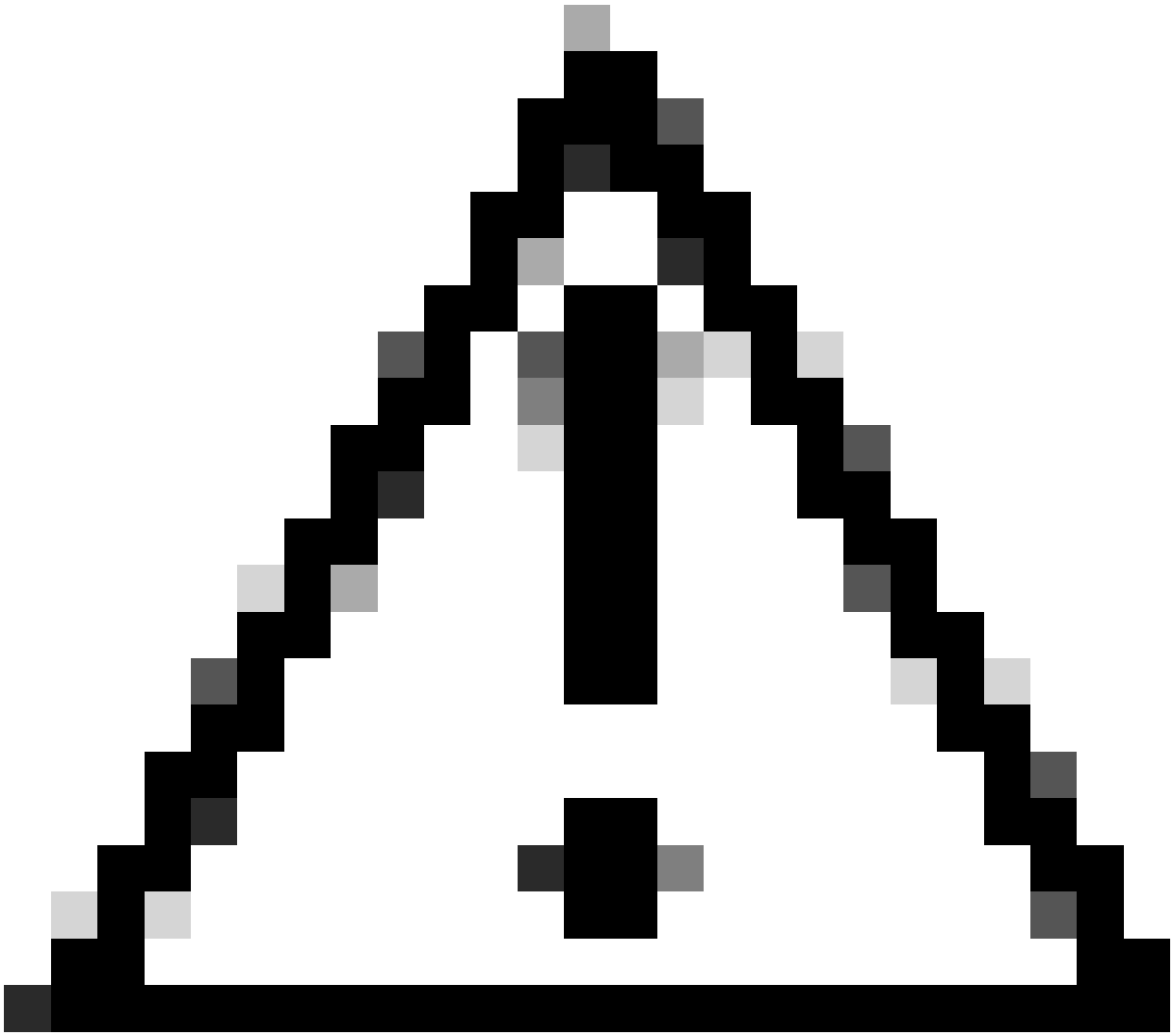
<#root>

```
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
```

其他調試

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

```
debug dhcp detail
```



注意：運行調試時請小心！

相關資訊

- 在Catalyst 9000系列交換器上實作BGP EVPN路由原則
- 在Catalyst 9000系列交換機上實施BGP EVPN保護覆蓋分段
- 操作Catalyst 9000交換機上的DHCP監聽並排除故障

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。