Implementazione del relay BGP VPN DHCP Layer 2 sugli switch Catalyst serie 9000

Sommario

Introduzione

In questo documento viene descritto come configurare, verificare e risolvere i problemi relativi alla funzionalità di inoltro DHCP L2 della VLAN VPN.

Prerequisiti

Requisiti

- Questa funzionalità viene utilizzata in qualsiasi distribuzione di tipo CGW in cui viene utilizzato DHCP
- Se si implementa la segmentazione protetta, rivedere i seguenti documenti
  - Implementazione della policy di routing BGP VPN sugli switch Catalyst serie 9000
  - Implementazione della segmentazione della sovrimpressione protetta da BGP VPN sugli switch Catalyst serie 9000

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Dettagli documento

Questo documento può essere usato per qualsiasi implementazione di CGW in cui il protocollo DHCP deve essere inoltrato da una foglia senza SVI verso il gateway centrale.

- Se non si utilizza la segmentazione protetta, utilizzare la sezione del documento in cui l'SVI è pubblicizzato nel fabric

Se si sta implementando la segmentazione protetta, questo documento è la parte 2 di 3 documenti correlati:

- Documento 1: Implementazione della policy di routing BGP VPN sugli switch Catalyst serie

9000 descrive come controllare il traffico BGP BUM nell'overlay e deve essere configurato per primo

- Il documento 2:Implementazione della segmentazione della sovrimpressione protetta da BGP VPN sugli switch Catalyst serie 9000 si basa sul progetto e sulla policy di sovrapposizione di cui al documento 1, descrive l'implementazione della parola chiave 'protected'.
- Documento 3: Questo documento. Si basa sugli ultimi due documenti e descrive il modo in cui l'inoltro DHCP viene implementato solo con fogli di layer 2 e CGW

Comportamento relay L2

Relè	Bagno	Core Flood	Access Flood	IPv4
sì	sì	no	sì	• Opzione 82: (1) L'ID del circuito agente (porta vni-mod) viene popolato con lo snooping dhcp • È possibile limitare il lato accesso con la configurazione dell'attendibilità dhcp * MODELLO CONSIGLIATO
sì	no	sì	sì	• Opzione 82: (1) L'ID del circuito agente (vlan-mod-port) viene popolato con lo snooping dhcp
no	sì	no	sì	• Opzione 82: (1) L'ID del circuito agente (porta vni-mod) viene popolato con lo snooping dhcp • È possibile limitare il lato accesso con la configurazione dell'attendibilità dhcp
Relè	Bagno	Core Flood	Access Flood	IPv6
sì	sì	sì	sì	• Opzione 82: (1) L'ID del circuito agente (porta vni-mod) viene popolato con lo snooping dhcp • È possibile limitare il lato accesso con la configurazione dell'attendibilità dhcp
sì	no	sì	sì	• Opzione 82: (1) L'ID del circuito agente (vlan-mod-port) viene popolato con lo snooping dhcp
no	sì	sì	sì	• Opzione 82: (1) L'ID del circuito agente (porta vni-mod)

				viene popolato con lo snooping dhcp • È possibile limitare il lato accesso con la configurazione dell'attendibilità dhcp
no	no	sì	sì	

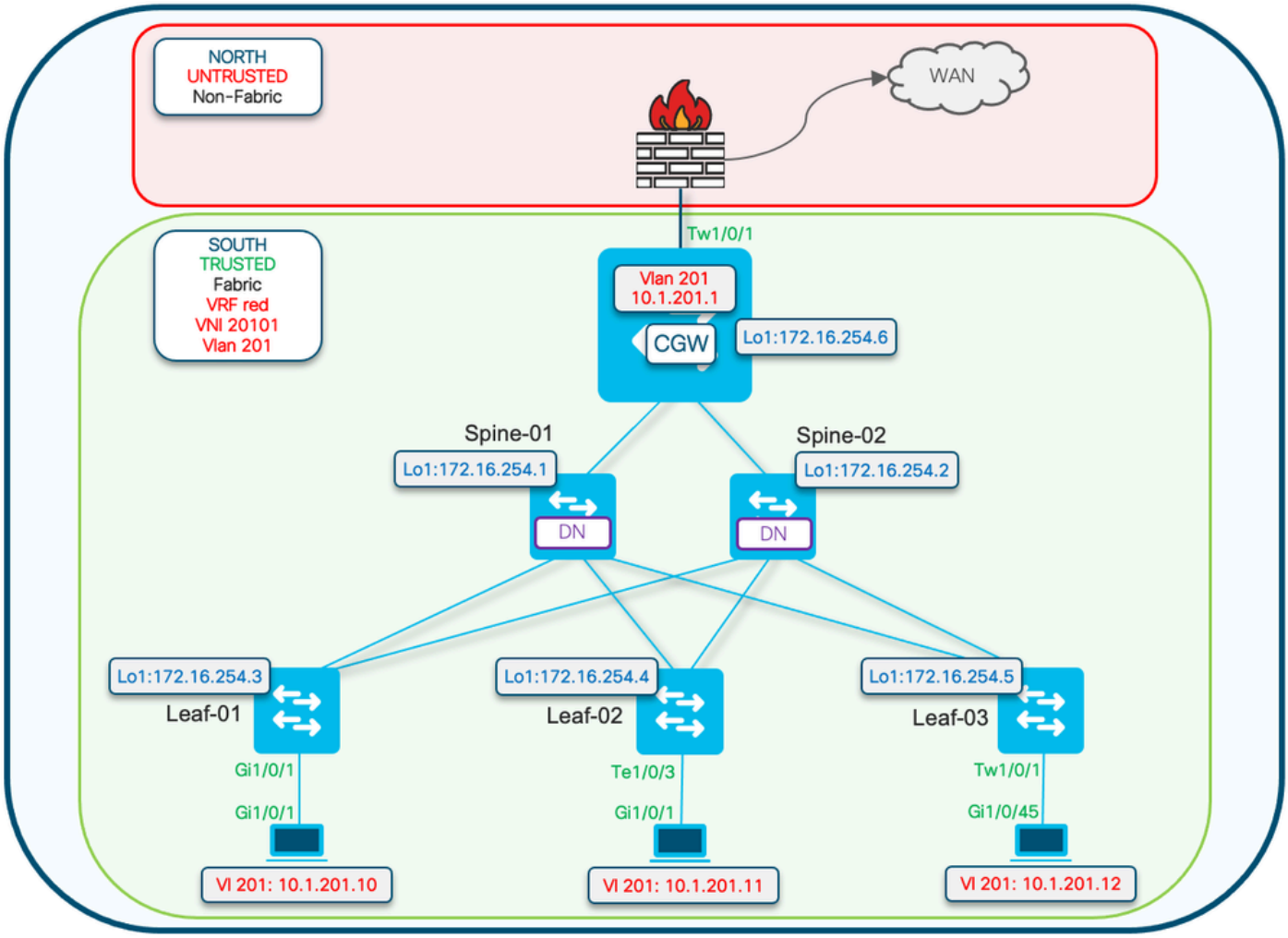
Terminologia

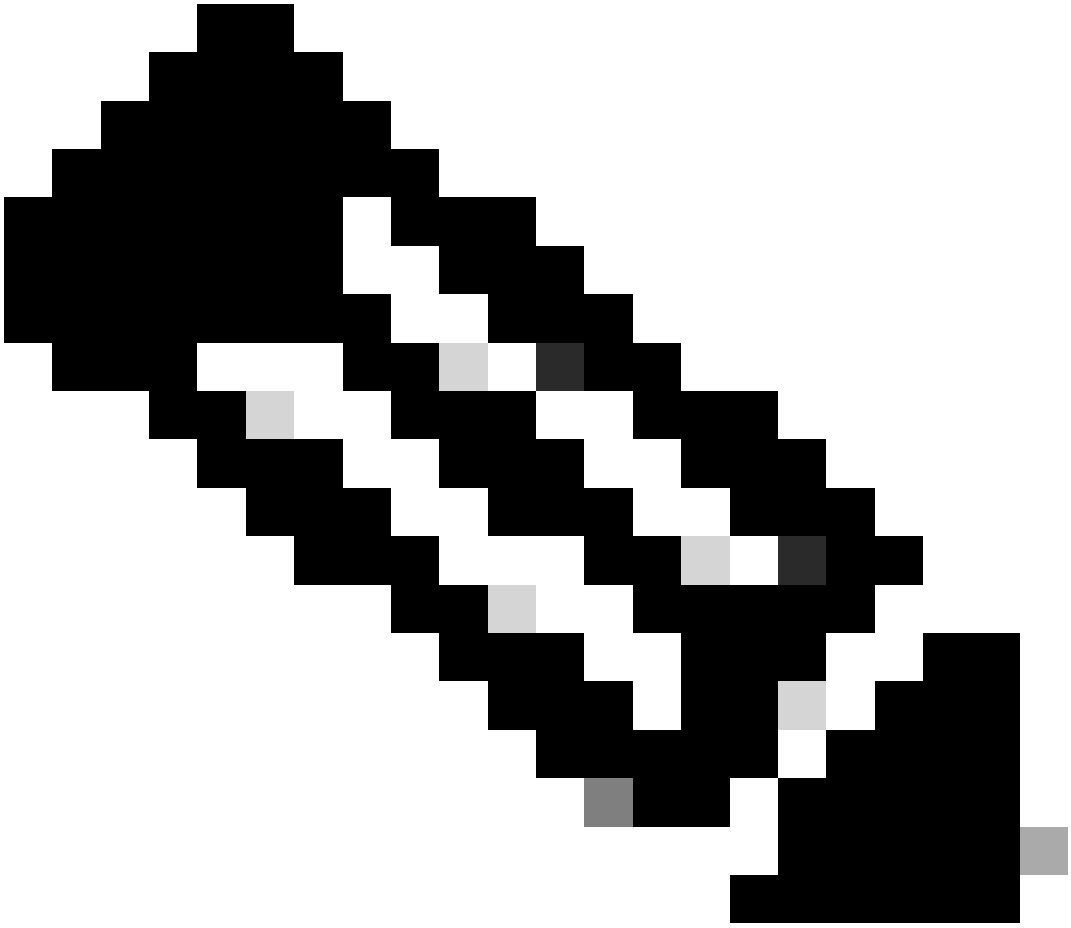
VRF	Inoltro routing virtuale	Definisce un dominio di routing di livello 3 che deve essere separato da altri VRF e da un dominio di routing IPv4/IPv6 globale
AF	Famiglia indirizzi	Definisce quali prefissi di tipo e informazioni di routing sono handle BGP
AS	Sistema autonomo	Set di prefissi IP instradabili Internet appartenenti a una rete o a un insieme di reti gestite, controllate e supervisionate da una singola entità o organizzazione
EVPN	Ethernet Virtual Private Network	L'estensione che consente a BGP di trasportare le informazioni MAC di layer 2 e IP di layer 3 è EVPN e utilizza il protocollo MP-BGP (Multi-Protocol Border Gateway Protocol) come protocollo per distribuire le informazioni sulla raggiungibilità relative alla rete di sovrapposizione VXLAN.
VXLAN	LAN virtuale estendibile (LAN)	La VXLAN è progettata per superare i limiti intrinseci delle VLAN e dell'STP. Si tratta di uno standard IETF [RFC 7348] proposto per fornire gli stessi servizi di rete Ethernet di layer 2 delle VLAN, ma con una maggiore flessibilità. A livello funzionale, è un protocollo di incapsulamento MAC-in-UDP che viene eseguito come sovrimpressione virtuale su una rete sottostante di layer 3.
CGW	Gateway centralizzato	E implementazione di EVPN in cui la SVI del gateway non è su ciascuna foglia. Tutto il routing viene invece eseguito da una foglia specifica utilizzando il protocollo IRB (Integrated Routing and Bridging) asimmetrico
DEF GW	Gateway predefinito	Un attributo della community estesa BGP aggiunto al prefisso MAC/IP tramite il comando "default-gateway annuncio enable" nella sezione di configurazione 'l2vpn evpn'.

IMET (RT3)	Tag Inclusive Multicast Ethernet (Route)	Chiamata anche route BGP di tipo 3. Questo tipo di route viene utilizzato nell'EVPN per consegnare il traffico BUM (broadcast / unicast sconosciuto / multicast) tra i VTEP.
RT2	Tipo di route 2	Prefisso BGP MAC o MAC/IP che rappresenta un MAC host o un MAC-IP gateway
EVPN Mgr	Responsabile EVPN	Componente di gestione centrale per vari altri componenti (ad esempio, apprende da SISF e segnala a L2RIB)
SISF	Funzionalità di sicurezza integrata dello switch	Tabella di rilevamento host agnostica utilizzata da EVPN per individuare gli host locali presenti in una foglia
L2RIB	Base informazioni routing Layer 2	In un componente intermedio per la gestione delle interazioni tra BGP, EVPN Mgr, L2FIB
FED	Driver motore di inoltro	Programmazione del livello ASIC (hardware)
MATM	Mac Address Table Manager	IOS MATM: tabella software che installa solo indirizzi locali e FED MATM: tabella hardware che installa gli indirizzi locali e remoti appresi dal control plane e fa parte del piano di inoltro hardware

Configura (distribuzione CGW standard)

Esempio di rete


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



Nota: questa sezione descrive un'implementazione CGW standard senza l'utilizzo della funzionalità protetta.

- I debug che mostrano lo scambio di pacchetti DORA DHCP vengono mostrati solo nell'esempio del segmento protetto

---

Dettagli chiave VTEP (foglia) L2

Pacchetto di richiesta proveniente dal client

- Utilizzare il mac CGW annunciato predefinito gw.
- Se esiste più di un gw, viene utilizzato il primo gw mac.
- Converte MAC broadcast esterno (avviato dal client: D e R in DORA) in mac GW unicast e inoltra a CGW

Aggiunge lo snooping DHCP: opzione 82 opzioni secondarie: circuito e RID

(RID viene utilizzato dall'elaborazione dei pacchetti di risposta su CGW)

(informa CGW che non è locale e che il relay fabric torna a L2VTEP)

<#root>

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

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000

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

- Pacchetti di risposta ricevuti da CGW su tunnel VXLAN.
- Strisce foglia, opzione 82.
- Aggiunge voci di binding con l'interfaccia dell'origine client. (vxlan-mod-port fornisce l'interfaccia di origine del client).
- Pacchetto di risposta inoltrato al client

Dettagli principali sul VTEP (CGW) L3

- Abilita SNOOPING DHCP
- Abilitare l'inoltro DHCP in SVI
- Richiesta ricevuta da L2VTEP e inviata al relay.
- Relay aggiunge altre opzioni secondarie dell'opzione 82 (gi, override del server e così via) e le invia al server DHCP
- La risposta DHCP del server dhcp arriva prima al componente RELAY
- Dopo che l'opzione 82 è stata rimossa da RELAY (indirizzo gi, override del server e così via), il pacchetto viene passato al componente di snooping dhcp
- Il componente di snooping controlla il RID (ID router) e, se non è locale, non rimuove l'opzione 82, sottotitoli 1 e 2.

- Il pacchetto RID (Fabric Relay, poiché non è locale) viene inoltrato direttamente al client remoto
- Utilizza il Mac client e esegue l'input bridge. L'hardware esegue la ricerca del mac del client e inoltra il pacchetto con crittografia vxlan all'L2VTEP di origine.

L2VTEP

Configurare l'istanza evpn

<#root>

```
Leaf-01#
```

show run | beg l2vpn evpn instance 201

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

Abilita snooping DHCP

<#root>

```
Leaf-01#
```

show run | sec dhcp snoop

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

201

```
ip dhcp snooping
```

CGW

Configurare l'istanza evpn

<#root>

```
Border#
```

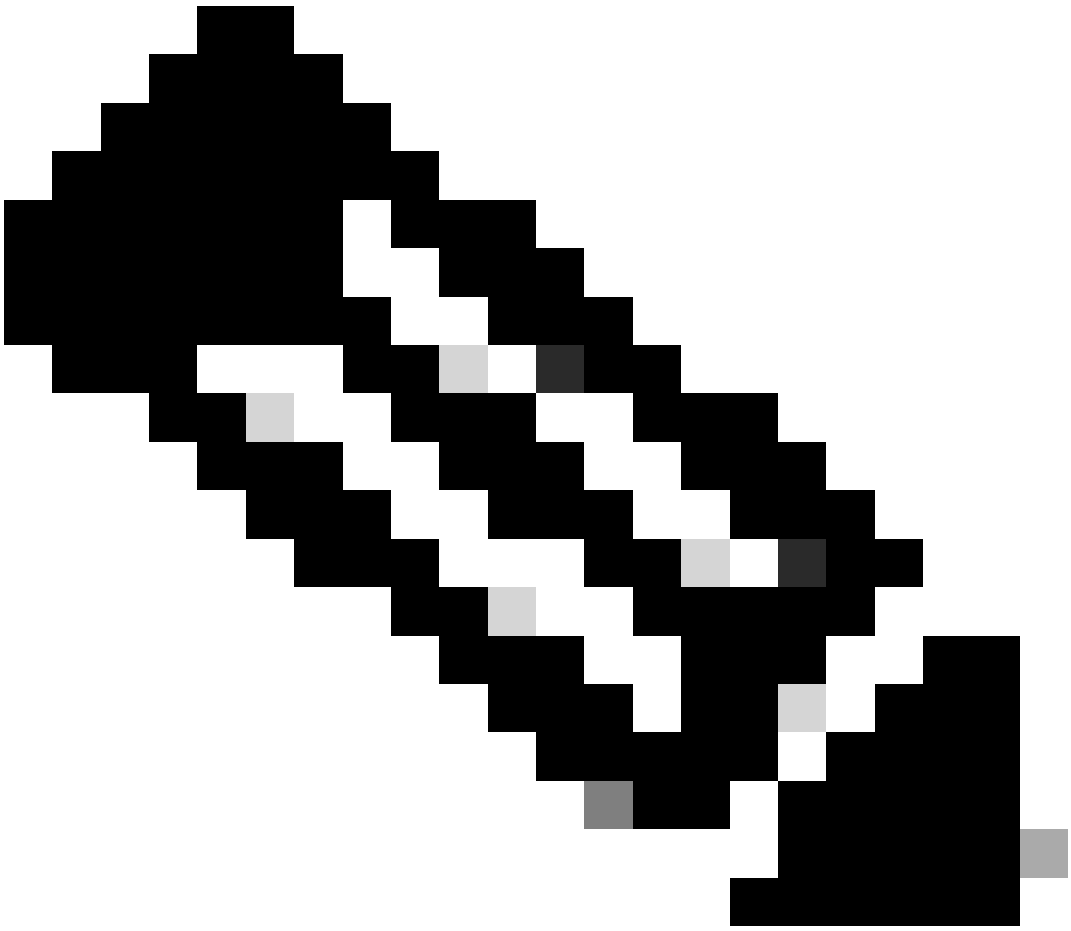
sh run | s l2vpn evpn instance 201

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

```
 encapsulation vxlan
 replication-type ingress
```

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

---



> Nota: l'attributo DEF GW è fondamentale per il relay L2 per sapere a chi incapsulare e inviare il pacchetto DHCP.

Abilita snooping DHCP

<#root>

```
Border#
```

sh run | s dhcp snoop

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

```
201

ip dhcp snooping
```

Verificare che il relay DHCP abbia la configurazione corretta per gestire le opzioni aggiuntive

<#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
```

Verifica (distribuzione CGW standard)

Prefisso gateway (foglia)

<#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
```

MATM FED (Foglia)

<#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 locale (foglia)

<#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
```

Snooping DHCP (Leaf e CGW)

<#root>

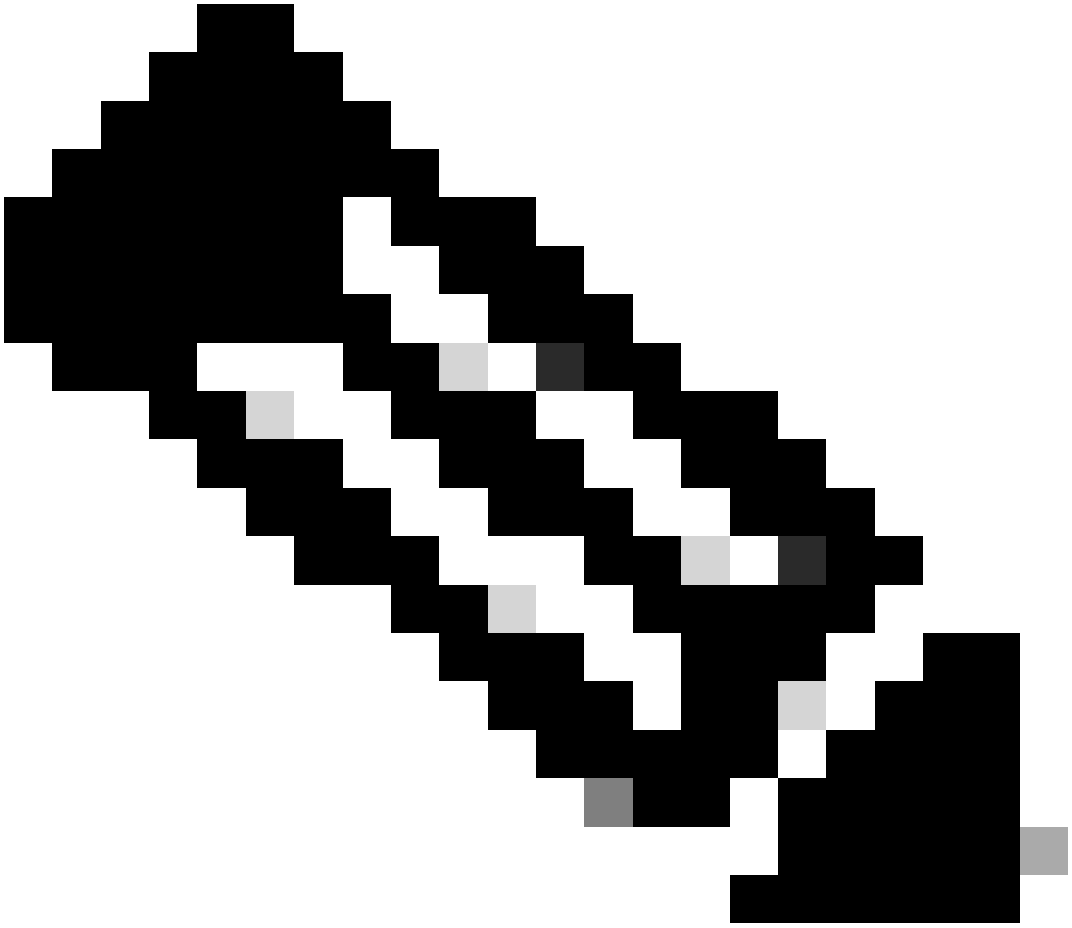
```
Leaf-01#

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
```

Configura (protezione parzialmente isolata)

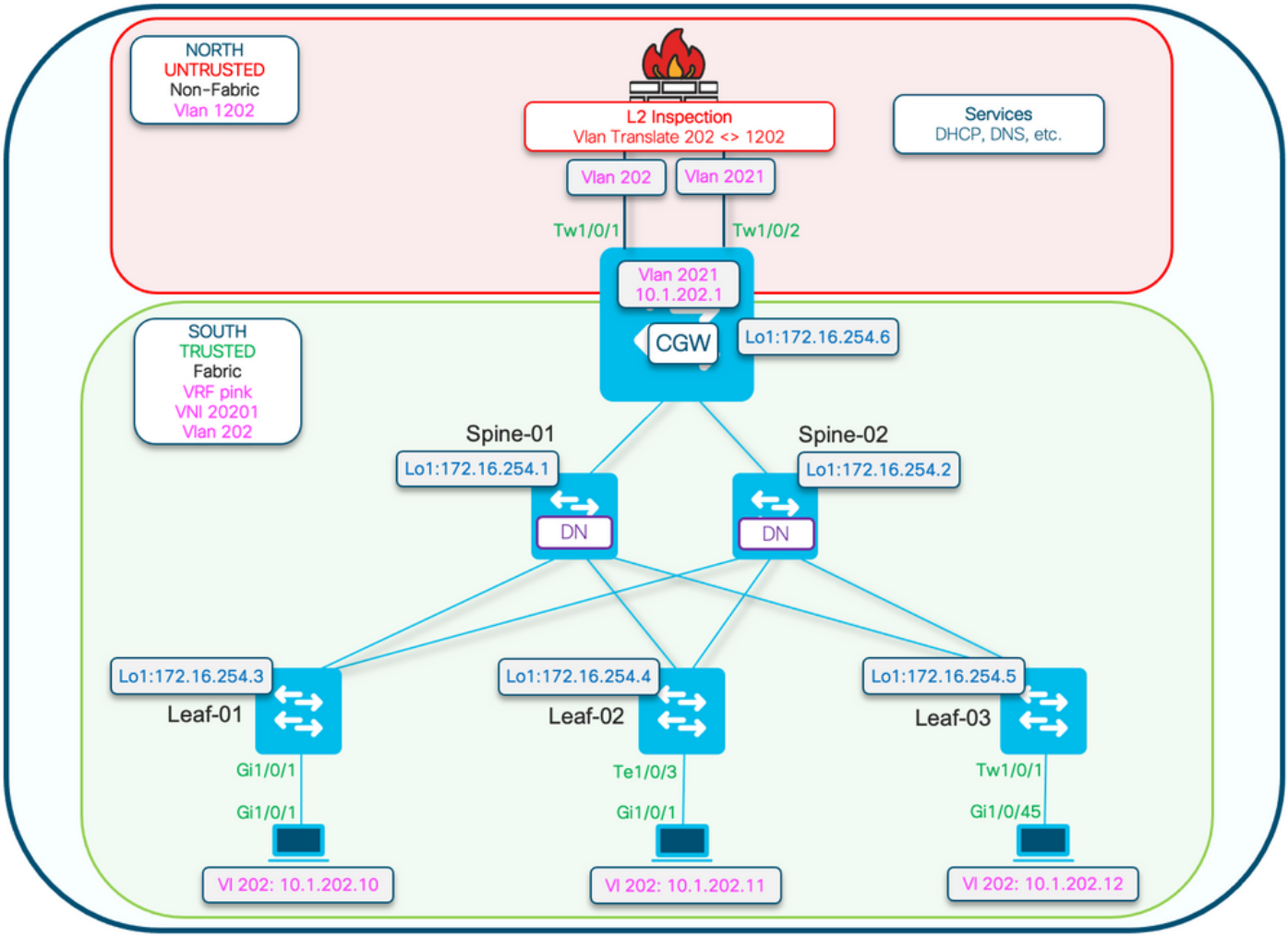
Lo snooping DHCP su Access Leaf si basa sulla route del gateway predefinito da CGW per imparare l'indirizzo MAC del gateway a cui inoltrare i pacchetti DHCP.

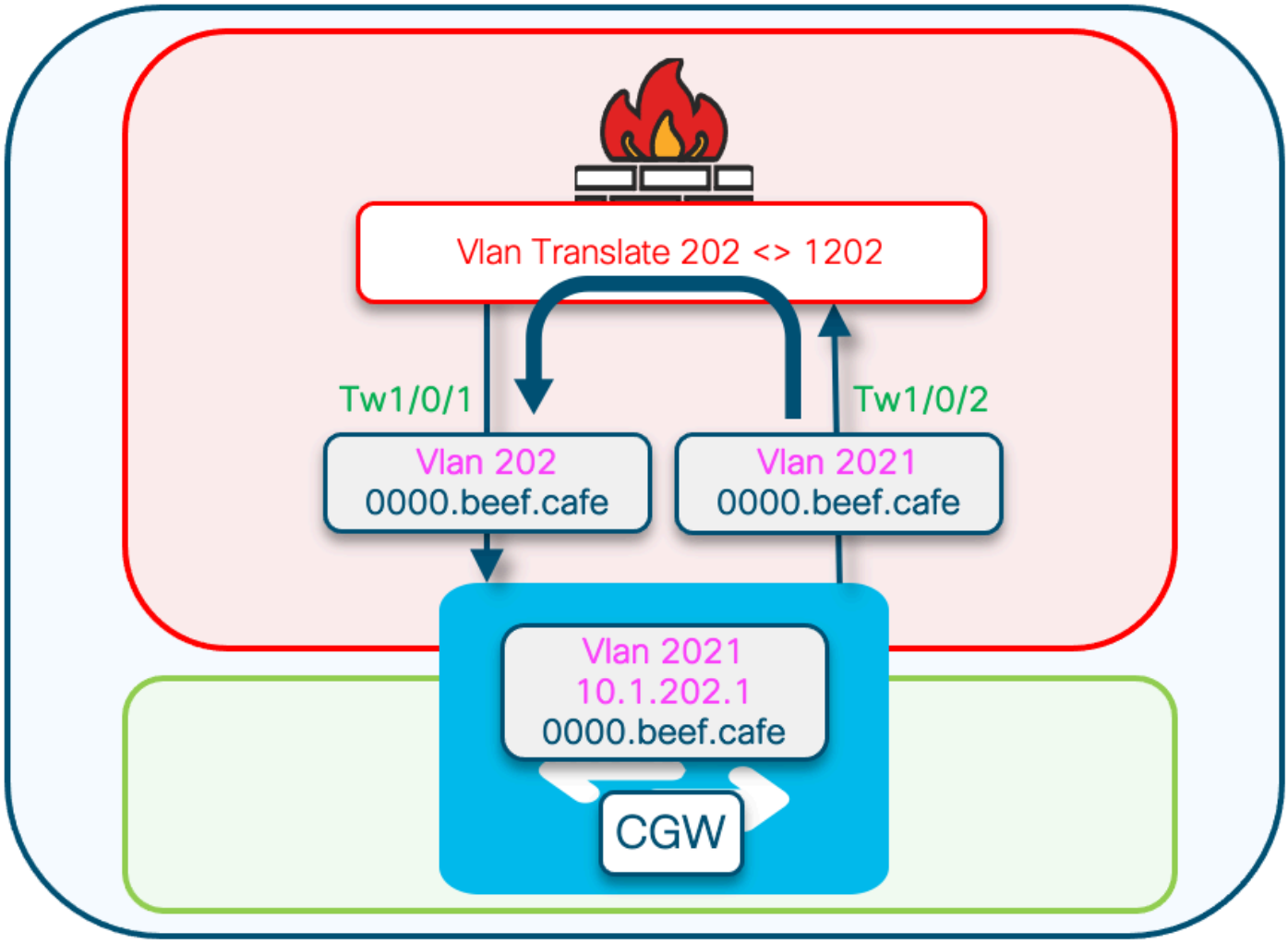
- Quando si utilizza il progetto Partially Isolated con gateway esterno, sono necessarie ulteriori configurazioni su CGW per annunciare MAC-IP RT2 con l'attributo default gateway (DEF GW).



Nota: questa sezione descrive anche un'implementazione di un segmento protetto completamente isolato, che utilizza anche un GW pubblicizzato nel fabric (rispetto al GW esterno al fabric).

Esempio di rete


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



Dettagli chiave VTEP (foglia) L2

Pacchetto di richiesta proveniente dal client

- Utilizzare il mac CGW annunciato predefinito gw.
- Se esiste più di un gw, viene utilizzato il primo gw mac.
- Converte MAC broadcast esterno (avviato dal client: D e R in DORA) in mac GW unicast e inoltra a CGW

Aggiunge lo snooping DHCP: opzione 82 opzioni secondarie: circuito e RID

(RID viene utilizzato dall'elaborazione dei pacchetti di risposta su CGW)

(informa CGW che non è locale e che il relay fabric torna a L2VTEP)

<#root>

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

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000
```

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

- Pacchetti di risposta ricevuti da CGW su tunnel VXLAN.
- Strisce foglia, opzione 82.
- Aggiunge voci di binding con l'interfaccia dell'origine client. (vxlan-mod-port fornisce l'interfaccia di origine del client).
- Pacchetto di risposta inoltrato al client

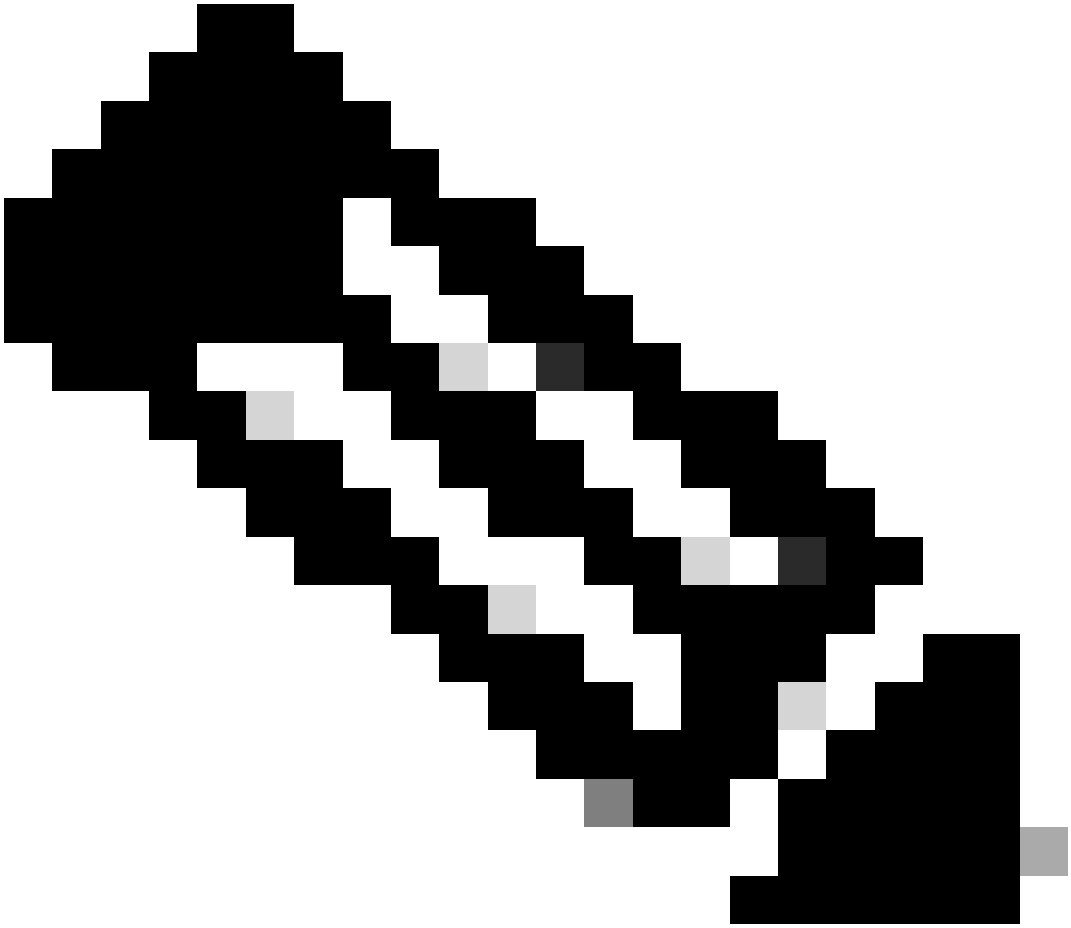
Dettagli principali sul VTEP (CGW) L3

- Abilita SNOOPING DHCP
- Abilitare l'inoltro DHCP in SVI
- Richiesta ricevuta da L2VTEP e inviata al relay.
- Relay aggiunge altre opzioni secondarie dell'opzione 82 (gi, override del server e così via) e le invia al server DHCP
- La risposta DHCP del server dhcp arriva prima al componente RELAY
- Dopo che l'opzione 82 è stata rimossa da RELAY (indirizzo gi, override del server e così via), il pacchetto viene passato al componente di snooping dhcp
- Il componente di snooping controlla il RID (ID router) e, se non è locale, non rimuove l'opzione 82, sottotitoli 1 e 2.
- Il pacchetto RID (Fabric Relay, poiché non è locale) viene inoltrato direttamente al client remoto
- Utilizza il Mac client e esegue l'input bridge. L'hardware esegue la ricerca del mac del client e inoltra il pacchetto con crittografia vxlan all'L2VTEP di origine.

Passaggi necessari per supportare il inoltro DHCP L2:

1. Abilita apprendimento locale IP
2. Creare un criterio con la spaziatura disabilitata
3. Collegamento a evi/vlan gateway esterno
4. Aggiungere voci statiche nella tabella di rilevamento dei dispositivi per il gateway esterno mac-ip
5. Creare la mappa della route BGP in modo che corrisponda ai prefissi RT2 MAC-IP e impostare la community estesa del gateway predefinita
6. Applica route-map ai router adiacenti del reflector di route BGP
7. Verificare che il relay DHCP abbia la configurazione corretta per gestire l'opzione aggiuntiva
8. Configurazione dello snooping DHCP sulla vlan dell'infrastruttura e sulla vlan GW esterna

---



> Nota: per il supporto del relay DHCP L2 con gateway esterno, sui fogli di accesso non sono necessarie modifiche alla configurazione.

CGW

Abilita apprendimento locale 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
```

Creare un criterio con la spaziatura disabilitata

<#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
```

Collegamento a evi/vlan gateway esterno

<#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
```

Aggiungi voci statiche nella tabella di rilevamento dispositivi per il gateway esterno 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

Creare la mappa della route BGP in modo che corrisponda ai prefissi RT2 MAC-IP e impostare la community estesa del gateway predefinita

<#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
```

Applica route-map ai router adiacenti del reflector di route 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

Verificare che il relay DHCP abbia la configurazione corretta per gestire le opzioni aggiuntive

<#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
```

Configurazione dello snooping DHCP sulle vlan dell'infrastruttura e sulla vlan GW esterna

<#root>

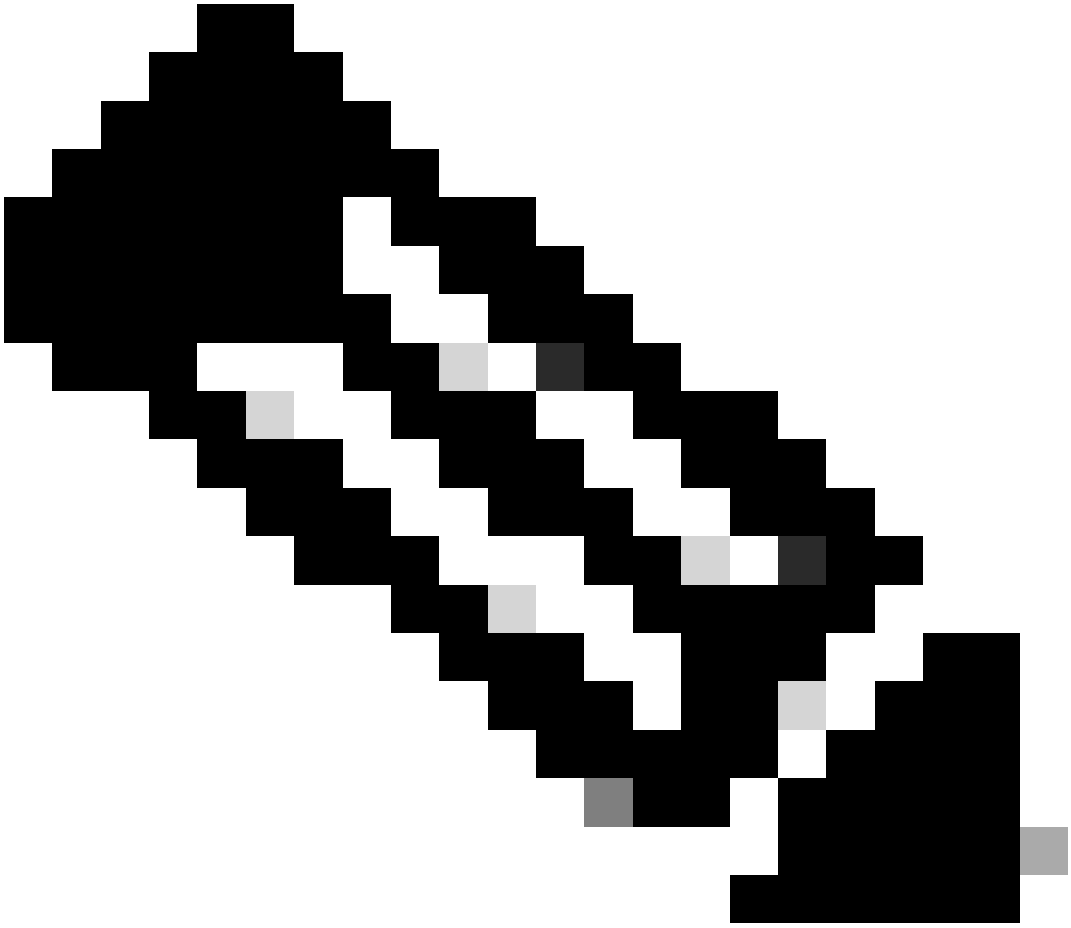
```
Leaf01#

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
```

Verificare che l'uplink al server DHCP sia attendibile sul CGW

<#root>

```
CGW#

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

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

 ip dhcp snooping trust

end

CGW#

sh run int tw 1/0/2


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

 ip dhcp snooping trust

end
```



Nota: a causa del modo in cui il server è posizionato sul dispositivo firewall, l'attendibilità

---

del dispositivo è stata configurata su entrambi i collegamenti rivolti a questo dispositivo. Nel diagramma ingrandito potete vedere che in questo progetto l'offerta arriva sia a Tw1/0/1 che a Tw1/0/2.

Verifica (parzialmente isolato protetto)

Prefisso gateway (foglia)

<#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
```

MATM FED (Foglia)

Confermare che Leaf abbia installato il MAC remoto CGW nell'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 locale (foglia)

<#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

Snooping DHCP (Leaf e CGW)

Confermare che lo snooping DHCP sia abilitato sulla foglia nella vlan dell'infrastruttura

<#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...>

Confermare che lo snooping DHCP sia abilitato su CGW nella struttura e nelle vlan gateway esterne

<#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

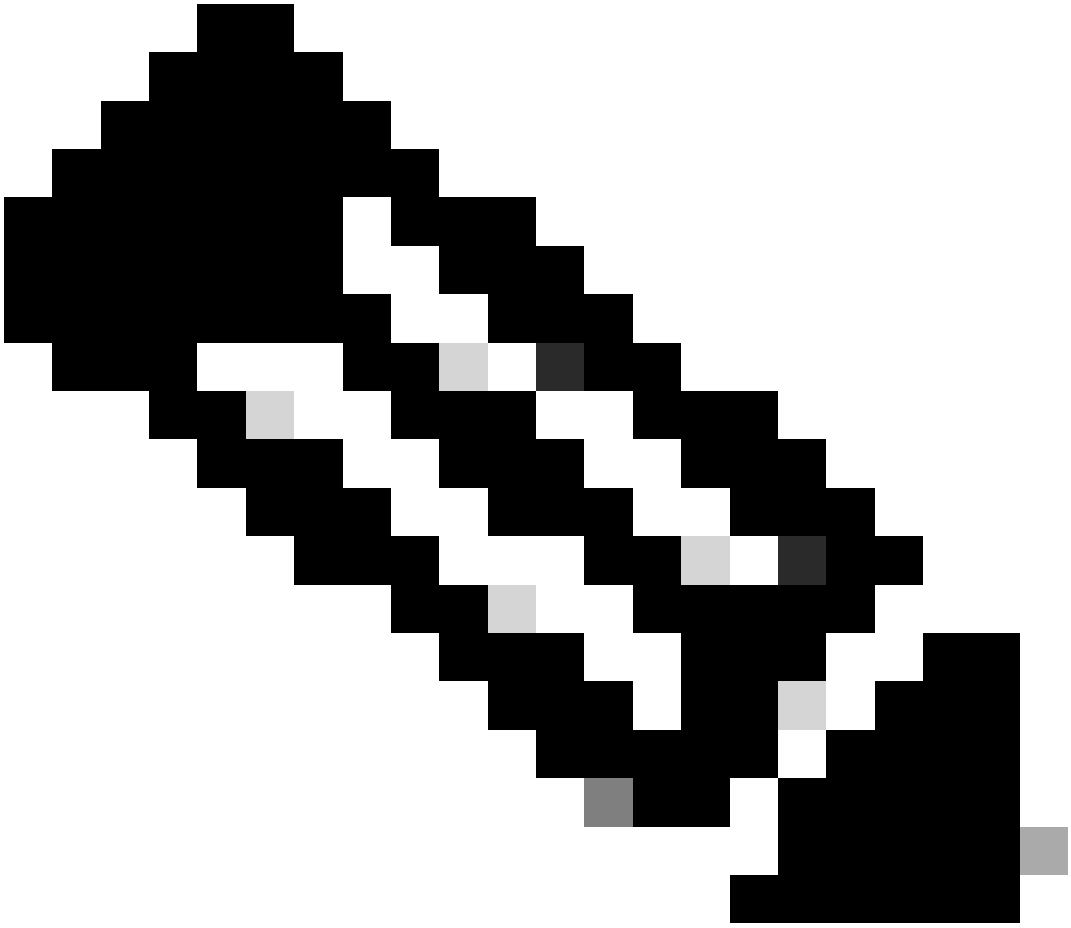
```
  Custom circuit-ids:
```

Confermare la creazione del binding dello snooping DHCP

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


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

Risoluzione dei problemi (qualsiasi tipo CGW)

I debug sono utili per mostrare come lo snooping DHCP e i processi di inoltro L2 gestiscono i pacchetti DHCP.



Nota: questi debug possono essere utilizzati per qualsiasi tipo di distribuzione che utilizza CGW con DCHP L2 Relay.

Debug dello snooping DHCP (foglia)

Debug Snooping per confermare l'elaborazione dei pacchetti

<#root>

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

Avvia tentativo di impostazione dell'indirizzo DHCP host

- Per questo documento è stata eseguita una chiusura/non chiusura dell'SVI indirizzata tramite DHCP per attivare lo scambio DORA
- Per l'host Windows è possibile eseguire un comando ipconfig /release > ipconfig /renew

Raccogliere i debug da show logging o dalla finestra del terminale

INDIVIDUAZIONE DHCP

Il comando Discover viene visualizzato dalla porta rivolta verso l'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
```

OFFERTA DHCP

L'offerta arriva dall'interfaccia del tunnel fabric

<#root>

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

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

*Sep 19 20:16:33.194:

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

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

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

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

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


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

DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1

*Sep 19 20:16:33.194:

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

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

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

RICHIESTA DHCP

La richiesta viene visualizzata dalla porta rivolta verso l'host

<#root>

```
*Sep 19 20:16:33.209:

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


*Sep 19 20:16:33.222:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

, input interface: Gi1/0/1, MAC da: ffff.ffff.ffff, MAC sa: 0006.f601.cd43, IP da: 255.255.255.255, IP
```

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

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

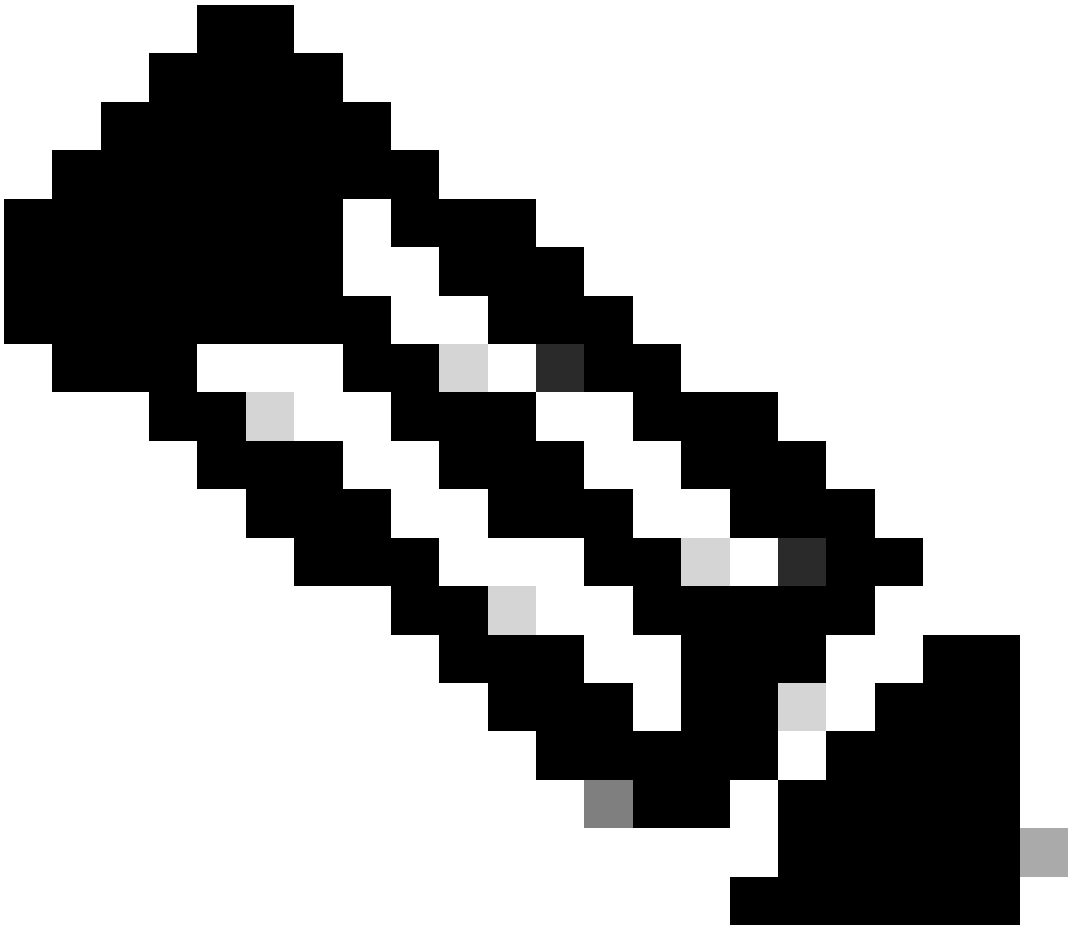
ACK DHCP

Ack in arrivo dall'interfaccia del tunnel fabric

<#root>

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

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

*Sep 19 20:16:33.238:

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

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

DHCP_SNOOPING: opt82 data indicates local packet

*Sep 19 20:16:33.239:

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

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

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

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

```
*Sep 19 20:16:33.252:
DHCP_SNOOPING: direct forward dhcp replyto output port: GigabitEthernet1/0/1.
```



> Nota: questi debug vengono ignorati. Producono un dump della memoria del pacchetto, ma l'annotazione di questa parte del risultato del debug non è inclusa nell'ambito di questo documento.

Debug dello snooping DHCP (CGW)

INDIVIDUAZIONE DHCP

A causa di come il pacchetto viene inviato e ricevuto sul CGW (hairpinning sul firewall), i debug si attivano due volte

In arrivo dal fabric sull'interfaccia tunnel e inviato due 1/0/1 al firewall nella VLAN fabric 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

In arrivo dal firewall il due 1/0/2 nella Vlan 2021 per l'invio alla SVI e all'helper al server 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

OFFERTA DHCP

Torna dal server DHCP all'interfaccia SVI 2021 in cui è configurato l'helper e lo inoltra al firewall

<#root>

*Apr 16 14:37:45.913:

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

*Apr 16 14:37:45.923:

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

, MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciadd
*Apr 16 14:37:45.923: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0

```
*Apr 16 14:37:45.924: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:45.924: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:45.924: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:45.924:
```

DHCP_SNOOPING: opt82 data indicates not a local packet

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

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

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

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

Arriva dal firewall nella vlan del fabric e viene inviato da CGW nel fabric verso 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

RICHIESTA DHCP

<#root>

*Apr 16 14:37:45.967:

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

*Apr 16 14:37:45.978:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

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

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

<#root>

*Apr 16 14:37:45.978:

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

*Apr 16 14:37:45.989:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

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

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

ACK DHCP

<#root>

*Apr 16 14:37:45.990:

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

*Apr 16 14:37:46.000:

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

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

```
*Apr 16 14:37:46.001:
DHCP_SNOOPING: opt82 data indicates not a local packet   <-- found this is coming from Leaf01 RID


*Apr 16 14:37:46.001: DHCP_SNOOPING: can't parse option 82 data of the message,it is either in wrong fo
*Apr 16 14:37:46.001: DHCP_SNOOPING: calling forward_dhcp_reply
*Apr 16 14:37:46.001: platform lookup dest vlan for input_if: Vlan2021, is NOT tunnel, if_output: Vlan2
*Apr 16 14:37:46.001: DHCP_SNOOPING: vlan 2021 after pvlan check
*Apr 16 14:37:46.011:
DHCP_SNOOPING: direct forward dhcp replyto output port: TwentyFiveGigE1/0/2.  <-- Send to Firewall
```

<#root>

```
*Apr 16 14:37:46.011:
DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1)  <-- Coming back in f


*Apr 16 14:37:46.022:
DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input interface: Twe1/0/1,

 MAC da: ffff.ffff.ffff, MAC sa: 0000.beef.cafe, IP da: 255.255.255.255, IP sa: 10.1.202.1, DHCP ciaddr
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x4E 0xE9 0x1 0x1 0x0 0x0
*Apr 16 14:37:46.022: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x2C 0x7B 0xF8 0x87 0x0
*Apr 16 14:37:46.022: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Apr 16 14:37:46.022: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 20201, vlan
*Apr 16 14:37:46.022:
DHCP_SNOOPING: opt82 data indicates not a local packet


*Apr 16 14:37:46.022: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022: DHCP_SNOOPING: can't find client's destination port, packet is assumed to be not
*Apr 16 14:37:46.022: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Apr 16 14:37:46.022: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 00
*Apr 16 14:37:46.022:
DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 202 from Twe1/0/1  <-- Send packe
```

Acquisizione integrata

Utilizzare EPC per verificare che lo scambio di pacchetti DHCP e i parametri siano corretti

- Questo viene mostrato dalla prospettiva del CGW, ma il processo può essere ripetuto su Leaf per verificare lo scambio del pacchetto

- Nell'esempio viene mostrato come eseguire il rilevamento, in quanto il processo e l'analisi sono gli stessi per gli altri pacchetti DHCP.

Controllare il percorso per il loopback foglia

<#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
```

Configurare l'acquisizione in modo che venga eseguita sui collegamenti con interfaccia Leaf01

```
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
```

Avviare la cattura, avviare l'host per richiedere un indirizzo IP DHCP, interrompere la cattura

<#root>

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

Visualizzare il risultato dell'acquisizione a partire dal comando DHCP Discover (prestare attenzione all'ID transazione per confermare che si tratta dello stesso evento DORA)

<#root>

```
CGW#
```

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


 16

  12.737135      0.0.0.0 -> 255.255.255.255 DHCP 434

DHCP Discover

 -

Transaction ID 0x78b <-- Discover starts at Frame 16 with all same transaction ID

   18  14.740041   10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP

Offer

    - Transaction ID

0x78b

   19  14.742741      0.0.0.0 -> 255.255.255.255 DHCP 452 DHCP

Request

  - Transaction ID

0x78b

   20  14.745646   10.1.202.1 -> 255.255.255.255 DHCP 438 DHCP

ACK

      - Transaction ID

0x78b
```

<#root>

```
CGW#

sh mon cap 1 buff detailed | b Frame 16

Frame 16:

 434 bytes on wire (3472 bits), 434 bytes captured (3472 bits) on interface /tmp/epc_ws/wif_to_ts_pipe,
    [Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]
Ethernet II,

Src: dc:77:4c:8a:6d:7f

 (dc:77:4c:8a:6d:7f),

Dst: 10:f9:20:2e:9f:82

 (10:f9:20:2e:9f:82)

<-- Underlay Interface MACs

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

Src: 172.16.254.3, Dst: 172.16.254.6

User Datagram Protocol, Src Port: 65281,
```

Dst Port: 4789 <-- VXLAN Port

Virtual eXtensible Local Area Network
VXLAN Network Identifier

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

Reserved: 0
Ethernet II,

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

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

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

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

<-- Inner Packet destined to CGW MAC

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

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

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

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

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

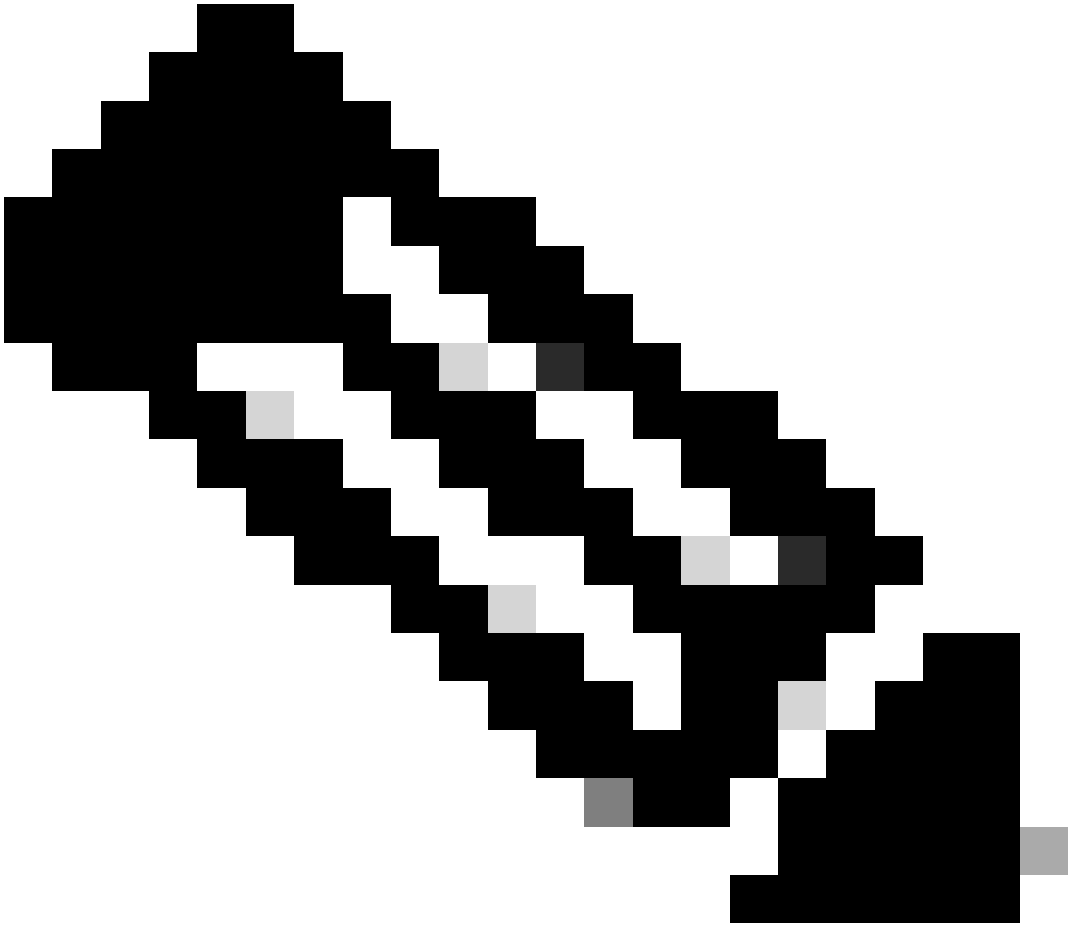
Option: (53) DHCP Message Type (Discover)

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

Host Name: 9300-HOST-3750X-2

Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address

```
        Parameter Request List Item: (43) Vendor-Specific Information
    Option: (60) Vendor class identifier
        Length: 8
        Vendor class identifier: ciscopnp


Option: (82) Agent Information Option

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


Option 82 Suboption: (2) Agent Remote ID

            Length: 8


Agent Remote ID:

000

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

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



Nota: lo strumento Capture può essere usato su qualsiasi foglia o CGW per determinare l'ultimo punto in cui si sospetta che una parte dello scambio DORA DHCP non funzioni.

Verificare le statistiche di snooping per gli errori

<#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.
```

Verifica percorso puntato per lo snooping DHCP

- CoPP è il componente principale che scarta i pacchetti nel percorso 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
```

Un altro comando molto utile per individuare dove si sta verificando un possibile flusso di pacchetti è 'show platform software fed switch active punt rates interfaces"

- Questo è molto utile per trovare un'interfaccia di origine in cui si verifica un flooding che congestiona il percorso punt e influisce sul traffico legittimo collegato alla 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...>
```

Statistiche client snooping DHCP

Osservare lo scambio di messaggi DHCP utilizzando questo comando. Può essere eseguito sia su Leaf che su CGW per visualizzare la traccia degli eventi

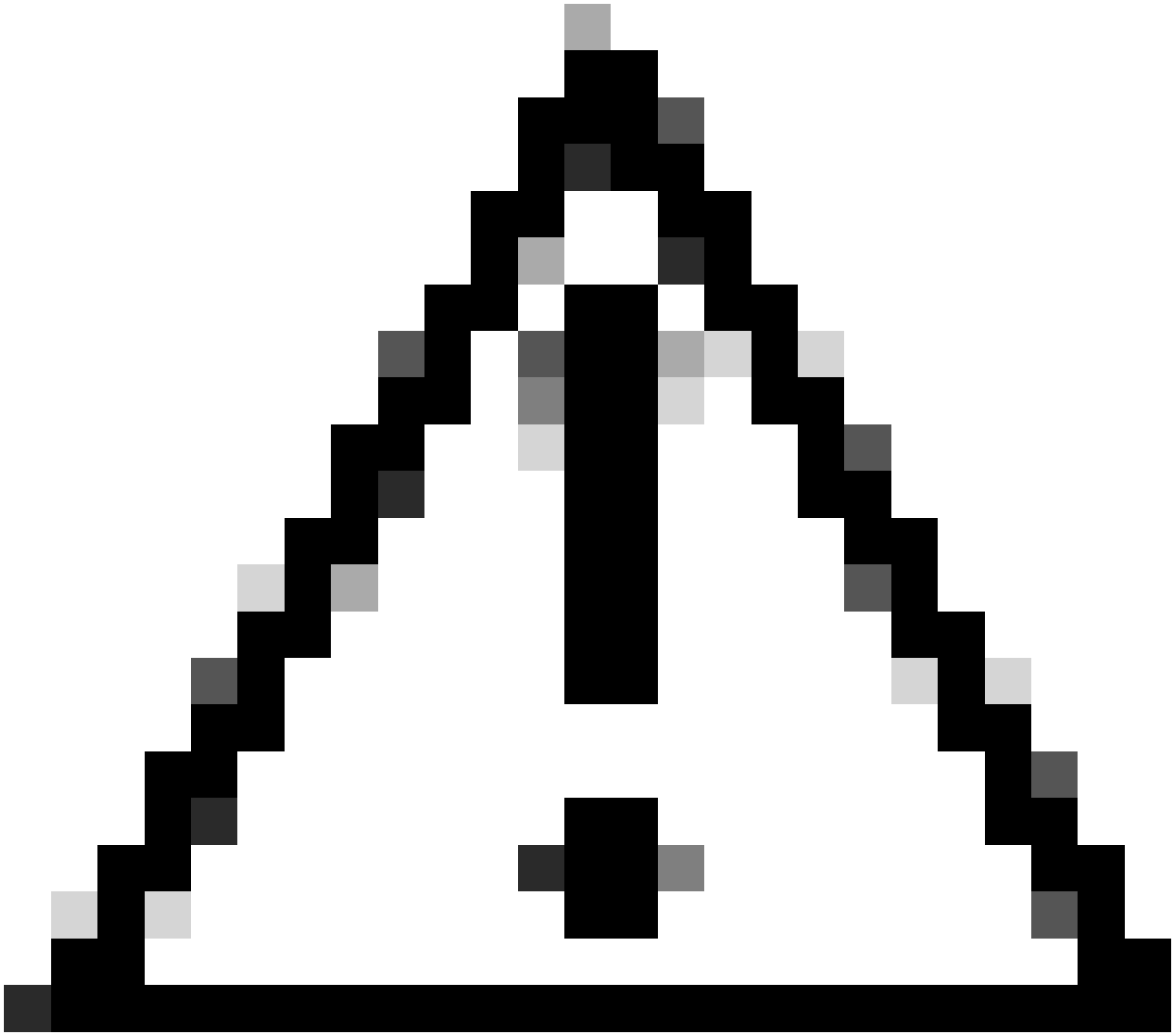
<#root>

```
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
```

Debug aggiuntivi

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

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



Attenzione: prestare attenzione quando si eseguono i debug.

Informazioni correlate

- Implementazione della policy di routing BGP VPN sugli switch Catalyst serie 9000
- Implementazione della segmentazione della sovrimpressione protetta da BGP VPN sugli switch Catalyst serie 9000
- Funzionamento e risoluzione dei problemi di snooping DHCP sugli switch Catalyst 9000

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).