Implémenter le relais DHCP de couche 2 EVPN BGP sur les commutateurs de la gamme Catalyst 9000

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Détails du document
  - Comportement du relais L2
- Terminologie
- Configurer (déploiement CGW standard)
  - Diagramme du réseau
  - Détails de la clé L2 VTEP (Leaf)
  - Détails des clés VTEP C3 (CGW)
  - L2VTEP
  - CGW
- Vérification (déploiement CGW standard)
  - Préfixe de passerelle (Leaf)
  - FED MATM (Leaf)
  - MAC local (leaf)
  - Surveillance DHCP (leaf et CGW)
- Configuration (protection partiellement isolée)
  - Diagramme du réseau
  - Détails de la clé L2 VTEP (Leaf)
  - Détails des clés VTEP C3 (CGW)
  - CGW
- Vérification (protection partiellement isolée)
  - Préfixe de passerelle (Leaf)
  - FED MATM (Leaf)
  - MAC local (leaf)
  - Surveillance DHCP (leaf et CGW)
- Dépannage (tout type de CGW)
  - Débogages de surveillance DHCP (leaf)
  - Débogages de surveillance DHCP (CGW)
  - Capture intégrée
  - Statistiques du client de surveillance DHCP
  - Débogages supplémentaires

Informations connexes

Introduction

Ce document décrit comment configurer, vérifier et dépanner la fonctionnalité de relais L2 EVPN VxLAN DHCP.

Conditions préalables

Exigences

- Cette fonctionnalité est utilisée dans tout déploiement de type CGW où DHCP est utilisé
- Si vous implémentez la segmentation protégée, consultez ces documents
  - Implémenter la politique de routage EVPN BGP sur les commutateurs de la gamme Catalyst 9000
  - Implémenter la segmentation de recouvrement protégée EVPN BGP sur les commutateurs de la gamme Catalyst 9000

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 et versions ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Détails du document

Ce document peut être utilisé pour n'importe quel déploiement CGW où DHCP doit être relayé d'un Leaf sans SVI vers la passerelle centrale.

- Si vous n'utilisez pas la segmentation protégée, utilisez la section du document où l'interface SVI est annoncée dans le fabric

Si vous mettez en oeuvre la segmentation protégée, ce document constitue la deuxième partie des trois documents interdépendants suivants :

- Document 1 : Implémenter une politique de routage EVPN BGP sur les commutateurs de la

gamme Catalyst 9000 couvre la façon de contrôler le trafic BGP BUM dans la superposition, et doit être configuré en premier

- Document 2 : Implémenter la segmentation de recouvrement protégée EVPN BGP sur les commutateurs de la gamme Catalyst 9000 s'appuie sur la conception et la stratégie de recouvrement du document 1, décrit l'implémentation du mot clé « protected ».
- Document 3 : Ce document. Repose sur les deux derniers documents et décrit la façon dont le relais DHCP est mis en oeuvre avec les leafs et CGW de couche 2 uniquement

Comportement du relais L2

Relais	Surveillance	Inondation Du Coeur	Inondation D'Accès	IPv4
oui	oui	non	oui	• Option 82 Sous-option : (1) l'ID de circuit d'agent (vni-mod-port) est rempli avec la surveillance dhcp • Il est possible de limiter l'accès avec la configuration de confiance DHCP * MODÈLE RECOMMANDÉ
oui	non	oui	oui	• Option 82 Sous-option : (1) L'ID de circuit de l'agent (vlan-mod-port) est renseigné avec la surveillance dhcp
non	oui	non	oui	• Option 82 Sous-option : (1) l'ID de circuit d'agent (vni-mod-port) est rempli avec la surveillance dhcp • Il est possible de limiter l'accès avec la configuration de confiance DHCP
Relais	Surveillance	Inondation Du Coeur	Inondation D'Accès	IPv6
oui	oui	oui	oui	• Option 82 Sous-option : (1) l'ID de circuit d'agent (vni-mod-port) est rempli avec la surveillance dhcp • Il est possible de limiter l'accès avec la configuration de confiance DHCP
oui	non	oui	oui	• Option 82 Sous-option : (1) L'ID de circuit de l'agent (vlan-mod-port) est renseigné avec la surveillance dhcp

non	oui	oui	oui	• Option 82 Sous-option : (1) l'ID de circuit d'agent (vni-mod-port) est rempli avec la surveillance dhcp • Il est possible de limiter l'accès avec la configuration de confiance DHCP
non	non	oui	oui	

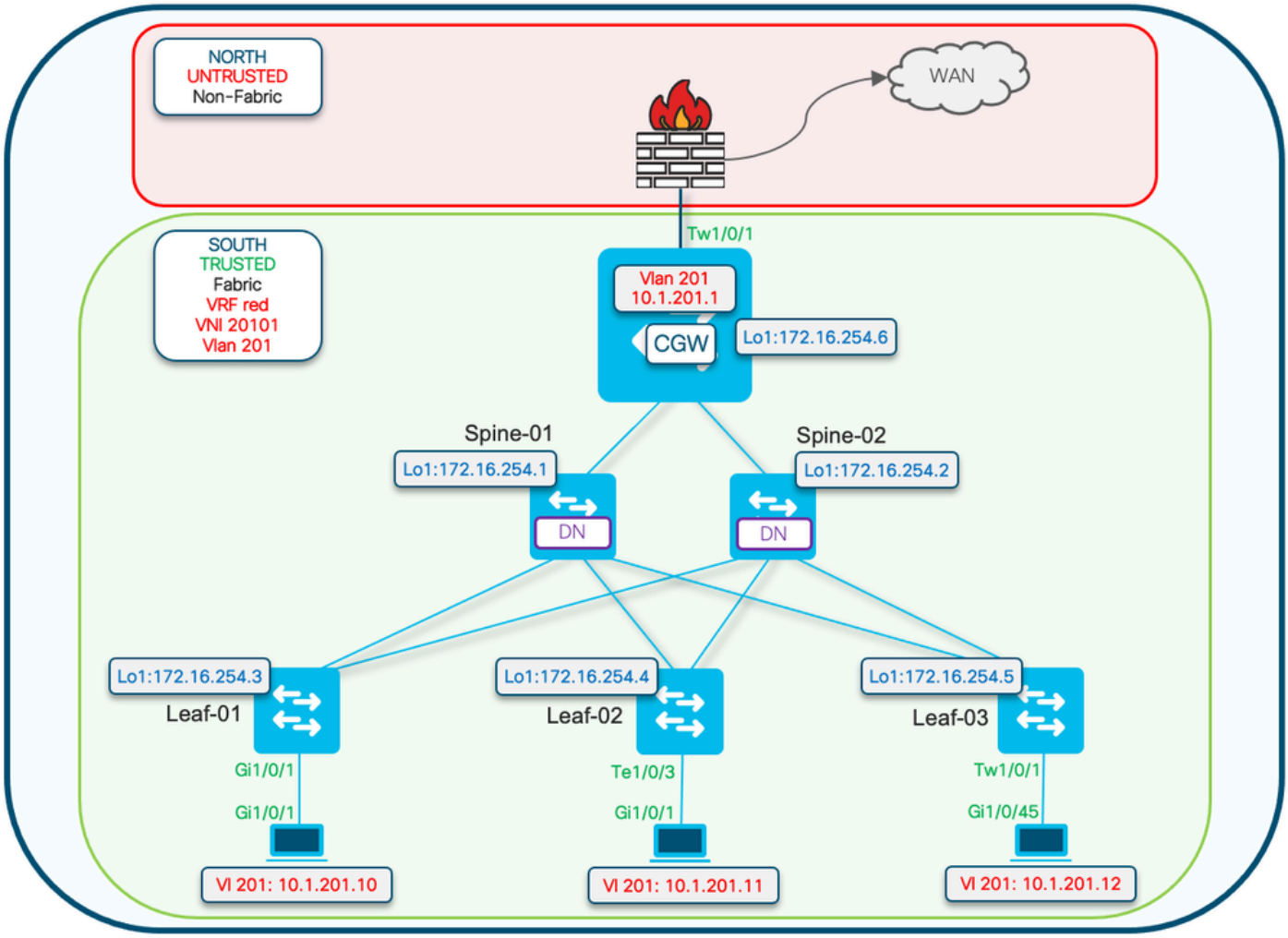
Terminologie

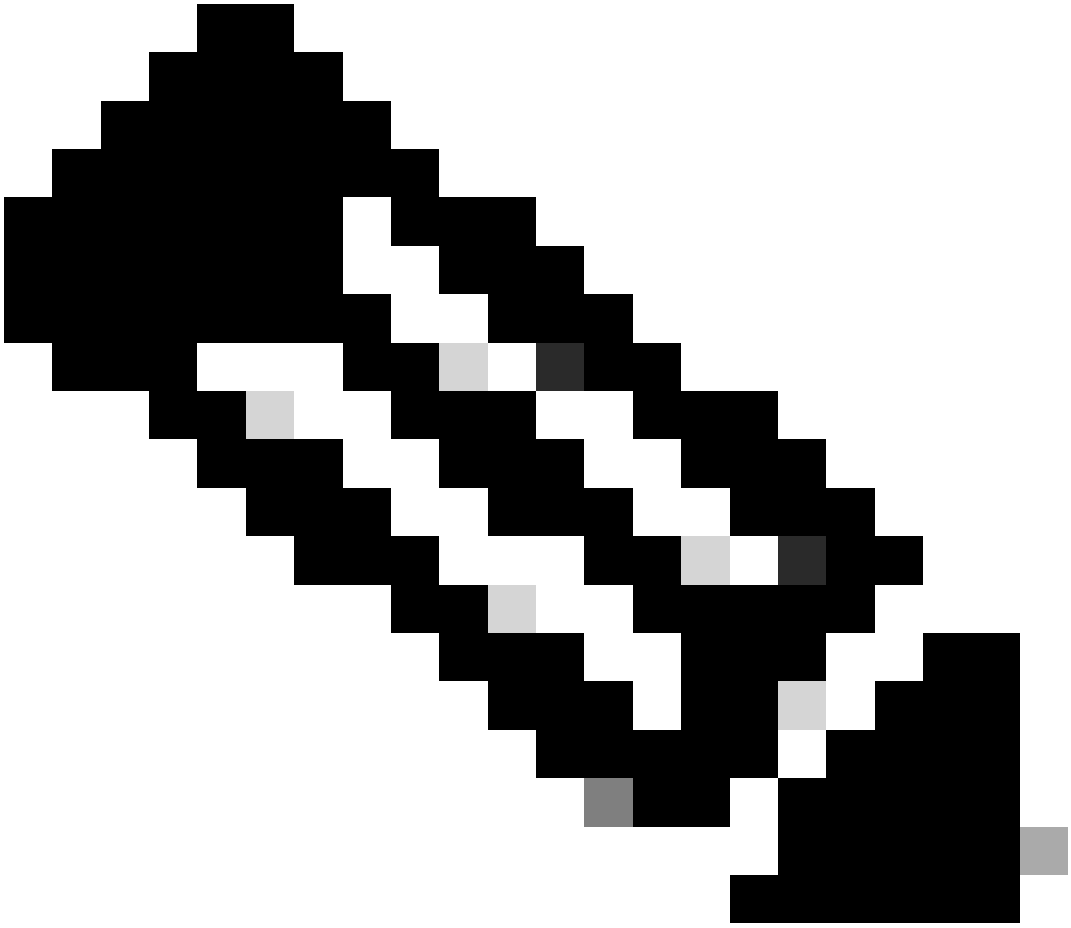
VRF	Transfert de routage virtuel	Définit un domaine de routage de couche 3 qui peut être séparé des autres domaines de routage VRF et IPv4/IPv6 global
AF	Famille d'adresses	Définit les préfixes de type et les informations de routage des handles BGP
COMME	Système Autonome	Ensemble de préfixes IP routables sur Internet qui appartiennent à un réseau ou à un ensemble de réseaux qui sont tous gérés, contrôlés et supervisés par une seule entité ou organisation
EVPN	Réseau privé virtuel Ethernet	L'extension qui permet au BGP de transporter les informations MAC de couche 2 et IP de couche 3 est EVPN et utilise le protocole MP-BGP (Multi-Protocol Border Gateway Protocol) comme protocole pour distribuer les informations d'accessibilité qui appartiennent au réseau de superposition VXLAN.
VXLAN	Réseau local (LAN) virtuel extensible	VXLAN est conçu pour surmonter les limitations inhérentes aux VLAN et au STP. Il s’agit d’une norme IETF proposée [RFC 7348] qui fournit les mêmes services réseau Ethernet de couche 2 que les VLAN, mais avec une plus grande flexibilité. Fonctionnellement, il s’agit d’un protocole d’encapsulation MAC-in-UDP qui s’exécute en tant que superposition virtuelle sur un réseau sous-jacent de couche 3.
CGW	Passerelle centralisée	Et la mise en oeuvre d'EVPN où les SVI de passerelle ne sont pas sur chaque leaf. Au lieu de cela, tout le routage est effectué par un noeud terminal spécifique à l'aide d'IRB asymétrique (Integrated Routing and Bridging)
DEF GW	Passerelle	Attribut de communauté étendue BGP ajouté au préfixe MAC/IP via la

	par défaut	commande « default-gateway advertise enable » dans la section de configuration « l2vpn evpn ».
IMET (RT3)	Balise Ethernet multidiffusion inclusive (route)	Également appelée route BGP de type 3. Ce type de route est utilisé dans EVPN pour acheminer le trafic BUM (diffusion / monodiffusion inconnue / multidiffusion) entre les VTEP.
RT2	Type de route 2	Préfixe MAC ou MAC/IP BGP qui représente un MAC hôte ou une adresse MAC de passerelle
Gestionnaire EVPN	Gestionnaire EVPN	Composant de gestion centrale pour divers autres composants (par exemple : apprend du SISF et signale au L2RIB)
ISF	Fonctionnalité de sécurité intégrée du commutateur	Table de suivi d'hôte agnostique utilisée par EVPN pour savoir quels hôtes locaux sont présents sur un leaf
NERVURE L2	Base d'informations de routage de couche 2	Dans le composant intermédiaire pour la gestion des interactions entre BGP, EVPN Mgr, L2FIB
NOURRIR	Pilote du moteur de transfert	Programmes de la couche ASIC (matériel)
MATM	Gestionnaire de table d'adresses Mac	IOS MATM : table logicielle qui installe uniquement les adresses locales et FED MATM : table matérielle qui installe les adresses locales et distantes apprises à partir du plan de contrôle et qui fait partie du plan de transfert matériel

Configurer (déploiement CGW standard)

Diagramme du réseau


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



Remarque : cette section couvre un déploiement CGW standard sans l'utilisation de la fonctionnalité protégée.

- Les débogages montrant l'échange de paquets DHCP DORA ne sont présentés que dans l'exemple de segment protégé

Détails de la clé L2 VTEP (Leaf)

Le paquet de requête provient du client

- Utilisez le mac CGW par défaut annoncé par gw.
- Si plusieurs gw existent, le premier gw mac sera utilisé.
- Convertissez l'adresse MAC de diffusion externe (initiée par le client : D et R dans DORA) en adresse MAC de monodiffusion GW et transférez-la à CGW

La surveillance DHCP ajoute : option 82 sous-options : circuit et RID

(RID est utilisé par le traitement du paquet de réponse sur CGW)

(Informe CGW qu'il n'est pas local et qu'il doit retransmettre le fabric à 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')

- Paquets de réponse reçus de CGW sur le tunnel vxlan
- Bandes de feuillets en option 82.
- Ajoute des entrées de liaison avec l'interface source du client. (vxlan-mod-port fournit l'interface source du client)
- Paquet de réponse transféré au client

Détails des clés VTEP C3 (CGW)

- Activer DHCP SNOOPING
- Activer DHCP RELAY dans SVI
- La demande est reçue de L2VTEP et est transmise au relais
- Le relais ajoute d'autres sous-options de l'option 82 (gi, server override, etc.) et envoie au serveur DHCP
- La réponse DHCP du serveur DHCP arrive d'abord au composant RELAY
- Une fois que le RELAIS a supprimé les paramètres de l'option 82 (adresse gi, remplacement du serveur, etc.), le paquet est transmis au composant de surveillance DHCP
- Le composant de surveillance vérifie le RID (ID de routeur) et si son ID n'est pas local, il ne supprime pas les sous-options 1 et 2 de l'option 82

- Le paquet de relais de matrice (puisque le RID n'est pas local) est directement transféré au client distant
- Utilise le Mac client et procède à l'injection du pont. Le matériel effectue une recherche MAC client et transfère le paquet avec vxlan encap au L2VTEP d'origine.

L2VTEP

Configurer l'instance evpn

<#root>

```
Leaf-01#
```

show run | beg l2vpn evpn instance 201

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

Activer la surveillance DHCP

<#root>

```
Leaf-01#
```

show run | sec dhcp snoop

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

201

```
ip dhcp snooping
```

CGW

Configurer l'instance evpn

<#root>

```
Border#
```

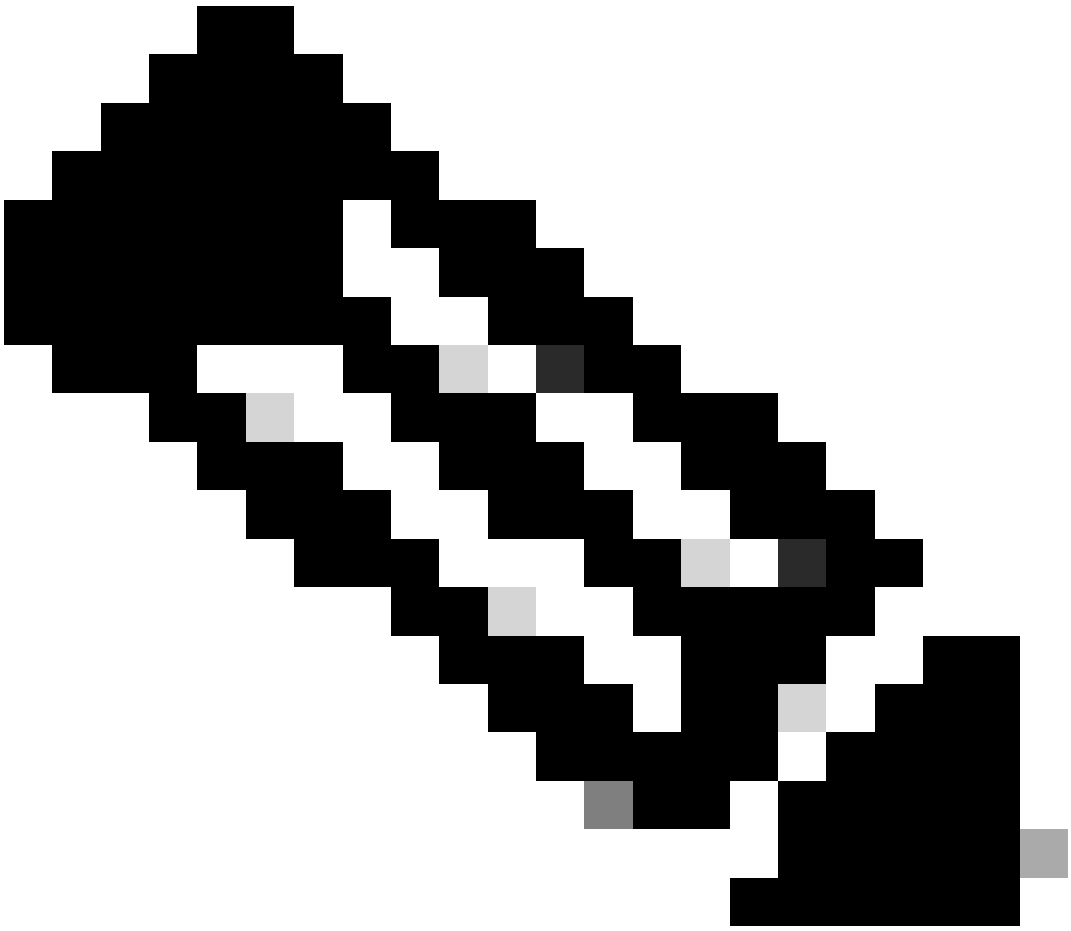
sh run | s l2vpn evpn instance 201

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

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

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

---



> Remarque : l'attribut DEF GW est essentiel pour que le relais L2 sache à qui encapsuler et à qui envoyer le paquet DHCP.

Activer la surveillance DHCP

<#root>

```
Border#
```

sh run | s dhcp snoop

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

201

ip dhcp snooping

Assurez-vous que le relais DHCP est correctement configuré pour gérer les options supplémentaires

<#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

Vérification (déploiement CGW standard)

Préfixe de passerelle (Leaf)

<#root>

Leaf-01#

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

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

table evi_201

)

<-- In the EVI context for the segment

Not advertised to any peer

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

Label1 20101 <-- Correct segment ID

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

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

Originator: 172.16.255.6

```
, Cluster list: 172.16.255.1
```

<-- Learned from the Border (CGW)

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

FED MATM (Leaf)

<#root>

```
Leaf-01#
```

show platform software fed switch active matm macTable vlan 201

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

201 0000.beef.cafe 0x5000001

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

VTEP 172.16.255.6 adj_id 1371

No

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

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

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

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

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

MAT_DYNAMIC_ADDR 0x1

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

MAT_LISP_REMOTE_ADDR 0x1000000

```
  MAT_VPLS_ADDR        0x2000000
```

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

MAC local (leaf)

<#root>

```
Leaf-01#
```

show switch

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

682c.7bf8.8700

```
     1      V01     Ready
```

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

Surveillance DHCP (leaf et CGW)

<#root>

```
Leaf-01#
```

show ip dhcp snooping

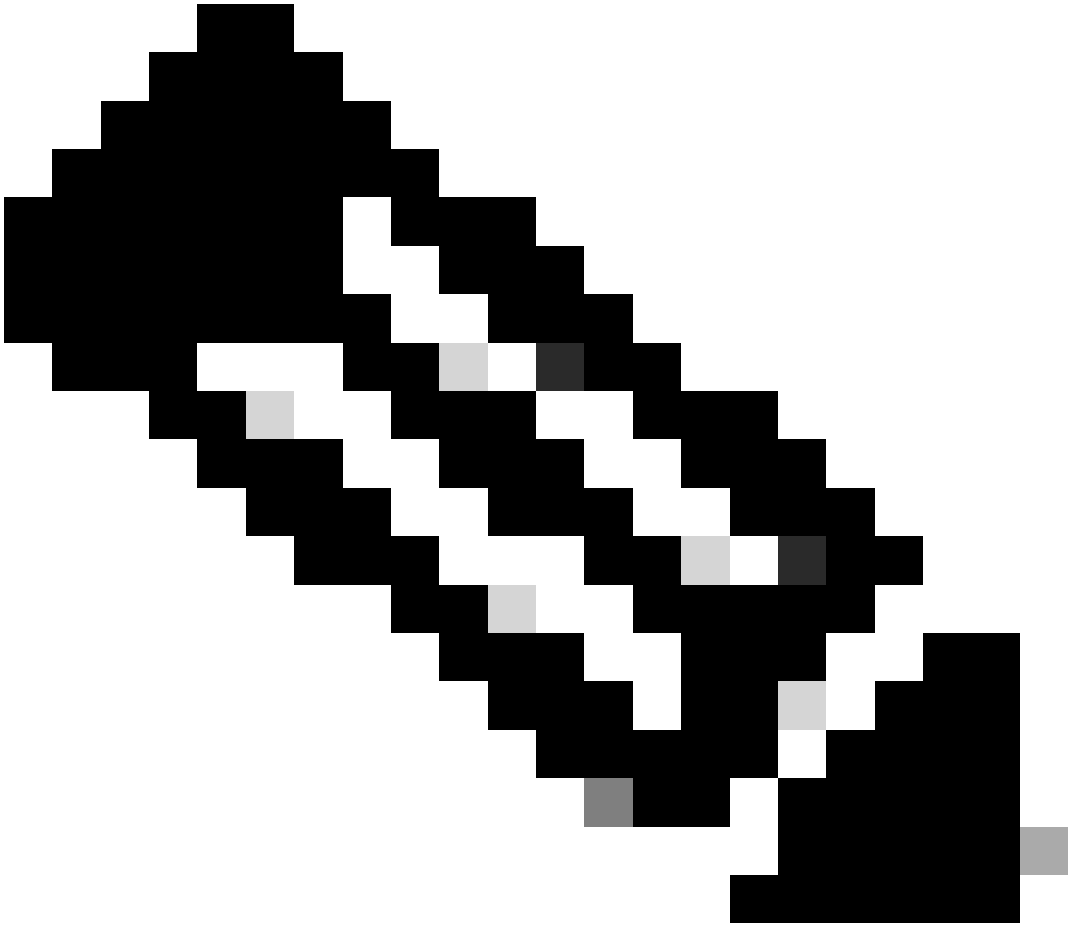
Switch DHCP snooping is enabled

```
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
```

Configuration (protection partiellement isolée)

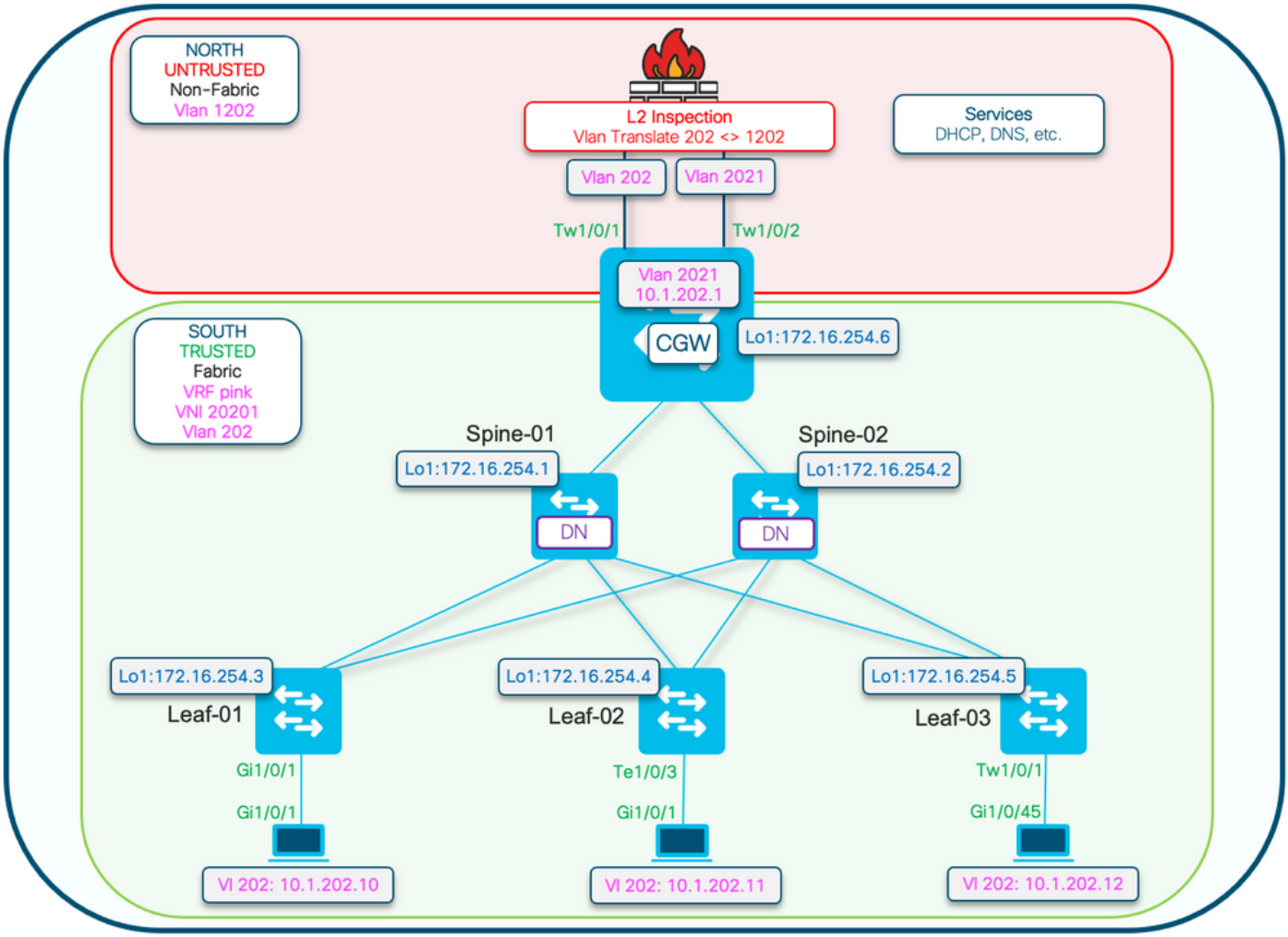
La surveillance DHCP sur la feuille d'accès s'appuie sur la route de passerelle par défaut de CGW pour apprendre l'adresse MAC de la passerelle vers laquelle transférer les paquets DHCP.

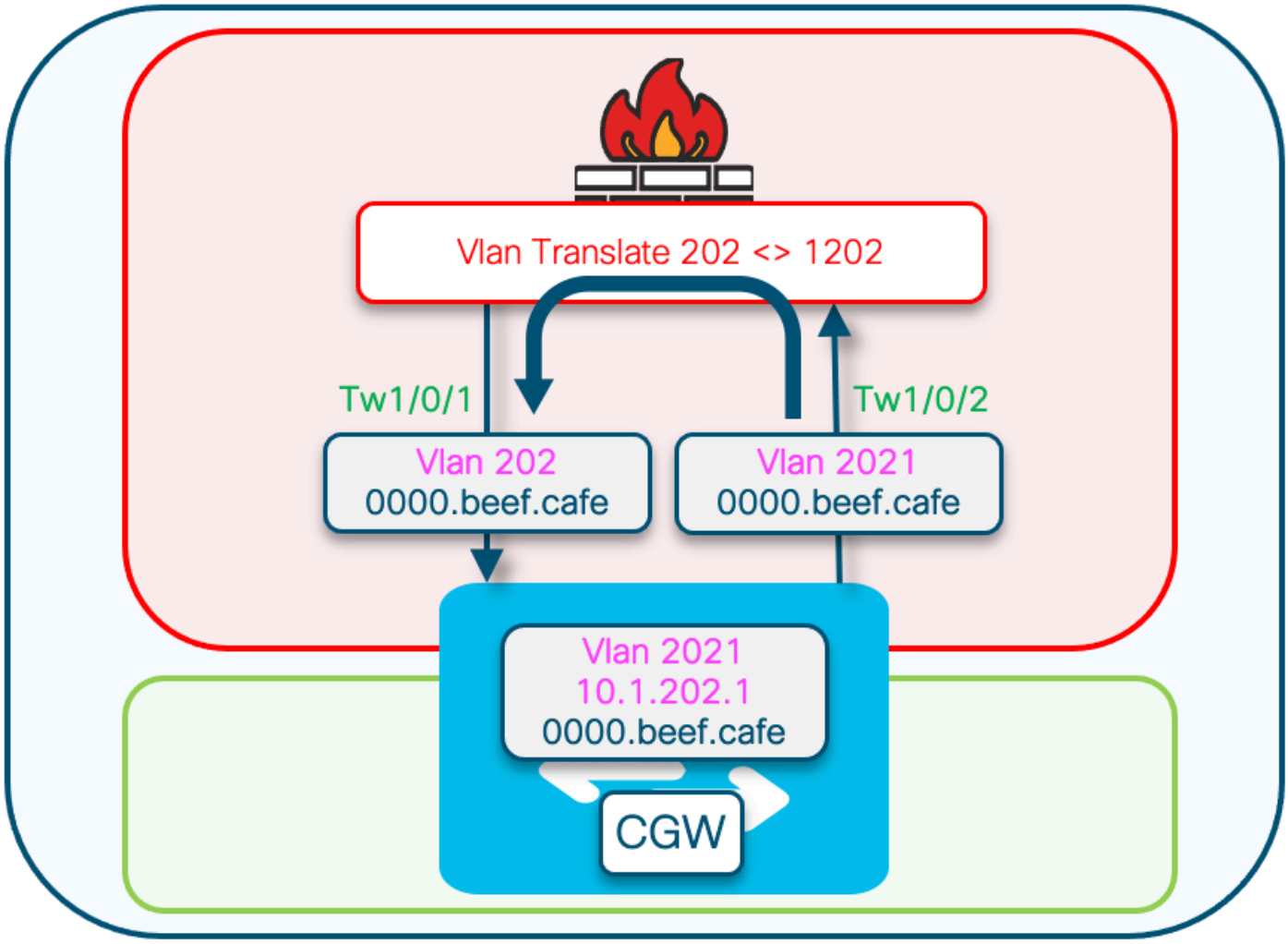
- Lors de l'utilisation de la conception partiellement isolée avec la passerelle externe, des configurations supplémentaires sont requises sur CGW pour annoncer le RT2 MAC-IP avec l'attribut de passerelle par défaut (DEF GW).



Remarque : cette section décrit également une implémentation de segment protégé totalement isolé, qui utilise également une passerelle Web annoncée dans le fabric (par rapport à une passerelle Web en dehors du fabric).

Diagramme du réseau


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



Détails de la clé L2 VTEP (Leaf)

Le paquet de requête provient du client

- Utilisez le mac CGW par défaut annoncé par gw.
- Si plusieurs gw existent, le premier gw mac sera utilisé.
- Convertissez l'adresse MAC de diffusion externe (initiée par le client : D et R dans DORA) en adresse MAC de monodiffusion GW et transférez-la à CGW

La surveillance DHCP ajoute : option 82 sous-options : circuit et RID

(RID est utilisé par le traitement du paquet de réponse sur CGW)

(Informe CGW qu'il n'est pas local et qu'il doit retransmettre le fabric à L2VTEP)

<#root>

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

        Option 82 Suboption: (2) Agent Remote ID

            Length: 8
          Agent Remote ID:
          000
```

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

- Paquets de réponse reçus de CGW sur le tunnel vxlan
- Bandes de feuillets en option 82.
- Ajoute des entrées de liaison avec l'interface source du client. (vxlan-mod-port fournit l'interface source du client)
- Paquet de réponse transféré au client

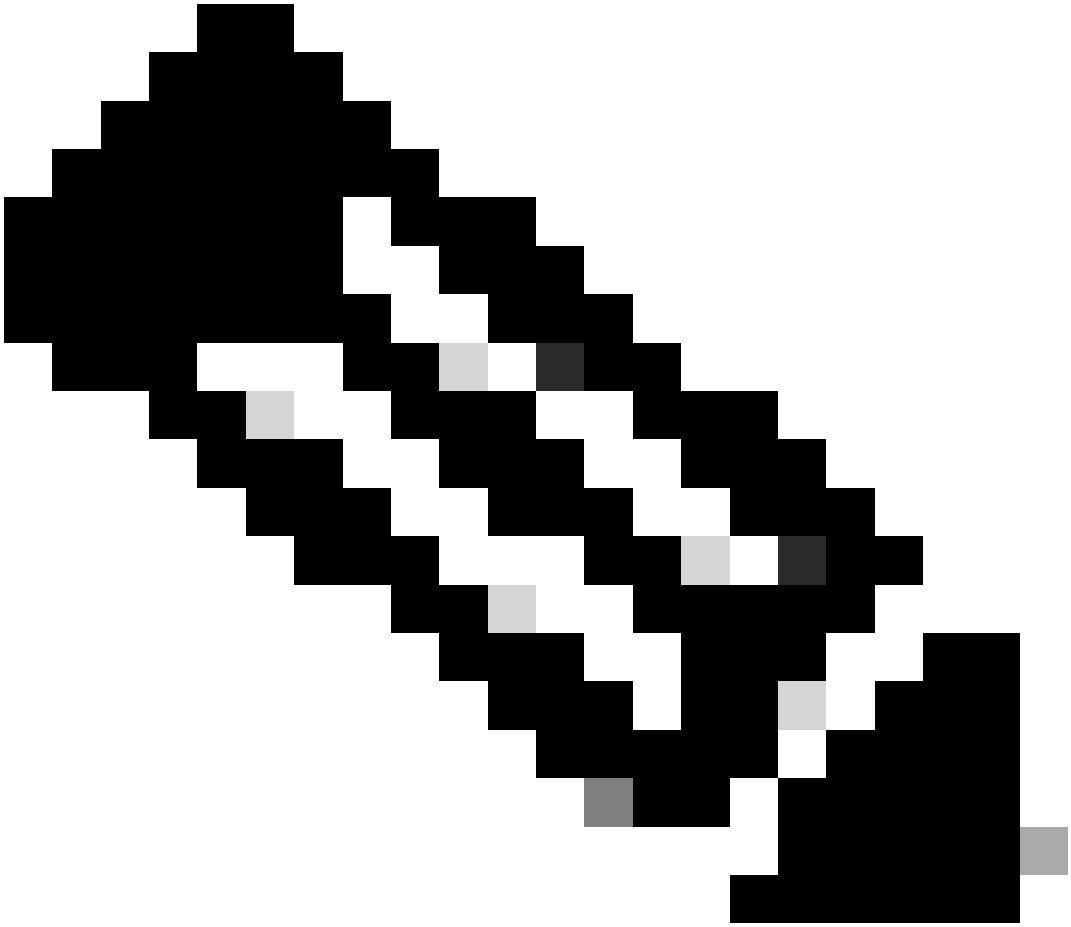
Détails des clés VTEP C3 (CGW)

- Activer DHCP SNOOPING
- Activer DHCP RELAY dans SVI
- La demande est reçue de L2VTEP et est transmise au relais
- Le relais ajoute d'autres sous-options de l'option 82 (gi, server override, etc.) et envoie au serveur DHCP
- La réponse DHCP du serveur DHCP arrive d'abord au composant RELAY
- Une fois que le RELAIS a supprimé les paramètres de l'option 82 (adresse gi, remplacement du serveur, etc.), le paquet est transmis au composant de surveillance DHCP
- Le composant de surveillance vérifie le RID (ID de routeur) et si son ID n'est pas local, il ne supprime pas les sous-options 1 et 2 de l'option 82
- Le paquet de relais de matrice (puisque le RID n'est pas local) est directement transféré au client distant
- Utilise le Mac client et procède à l'injection du pont. Le matériel effectue une recherche MAC client et transfère le paquet avec vxlan encap au L2VTEP d'origine.

Étapes requises pour prendre en charge le relais L2 DHCP :

1. Activer ip local learning
2. Créer une stratégie avec glanage désactivé
3. Connexion aux VLAN/versions de passerelle externe
4. Ajoutez des entrées statiques dans la table de suivi des périphériques pour la passerelle externe mac-ip
5. Créer une carte de route BGP pour correspondre aux préfixes MAC-IP de RT2 et définir la communauté étendue de passerelle par défaut
6. Appliquer route-map aux voisins BGP Route Reflector
7. Assurez-vous que le relais DHCP a la configuration correcte pour gérer l'option supplémentaire
8. Configurer la surveillance DHCP sur le VLAN de fabric et le VLAN GW externe

---



Remarque : aucune modification de configuration n'est requise sur les leafs d'accès pour prendre en charge le relais DHCP L2 avec la passerelle externe.

CGW

Activer 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
```

Créer une stratégie avec glanage désactivé

<#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
```

Connexion aux VLAN/versions de passerelle externe

<#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
```

Ajouter des entrées statiques dans la table de suivi des périphériques pour la passerelle externe 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

Créer une carte de route BGP pour correspondre aux préfixes MAC-IP de RT2 et définir la communauté étendue de passerelle par défaut

<#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
```

Appliquer route-map aux voisins BGP Route Reflector

<#root>

```
CGW#
```

sh run | sec router bgp

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

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

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

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

Assurez-vous que le relais DHCP est correctement configuré pour gérer les options supplémentaires

<#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
```

Configurer la surveillance DHCP sur les VLAN de fabric et le VLAN GW externe

<#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
```

Assurez-vous que la liaison ascendante vers le serveur DHCP est approuvée sur le CGW

<#root>

```
CGW#
```

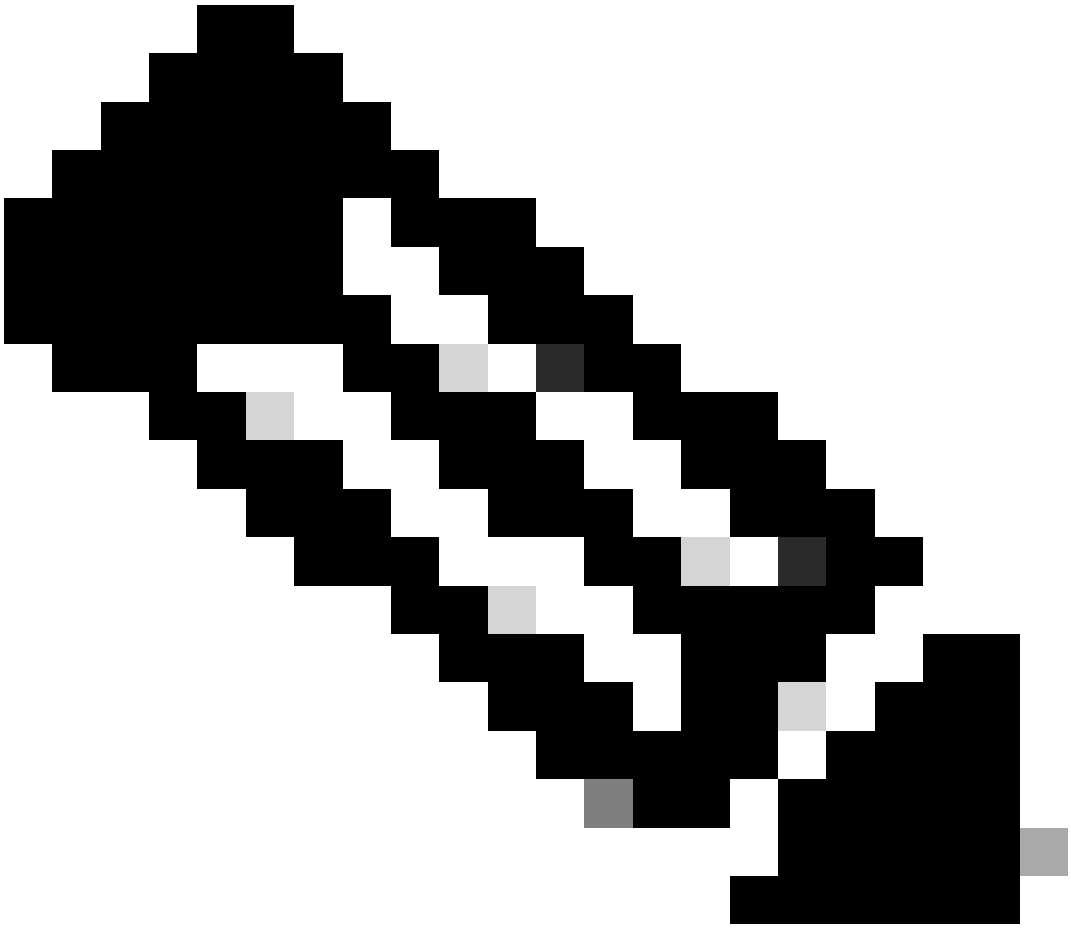
sh run int tw 1/0/1

```
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
```



Remarque : en raison de la manière dont le serveur est placé sur le pare-feu, l'approbation de périphérique a été configurée sur les deux liaisons faisant face à ce périphérique. Dans le diagramme agrandi, vous pouvez voir que l'offre arrive à la fois à Tw1/0/1 et Tw1/0/2 dans cette conception.

Vérification (protection partiellement isolée)

Préfixe de passerelle (Leaf)

<#root>

```
Leaf01#

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

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

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

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

FED MATM (Leaf)

Vérifiez que le leaf a installé l'adresse MAC distante CGW dans le matériel

<#root>

```
Leaf01#

show platform software fed switch active matm macTable vlan 202

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

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

202

 0000.beef.cafe  0x5000001
```

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

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

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

MAT_DYNAMIC_ADDR 0x1

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

MAT_LISP_REMOTE_ADDR 0x1000000

```
  MAT_VPLS_ADDR
```

0x2000000 MAT_LISP_GW_ADDR   0x4000000

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

MAC local (leaf)

<#root>

```
Leaf01#
```

show switch

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

682c.7bf8.8700

```
     1      V01     Ready
```

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

Surveillance DHCP (leaf et CGW)

Vérifiez que la surveillance DHCP est activée sur le Leaf dans le VLAN de fabric

<#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...>

Vérifiez que la surveillance DHCP est activée sur le CGW dans le fabric et les VLAN de passerelle externe

<#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

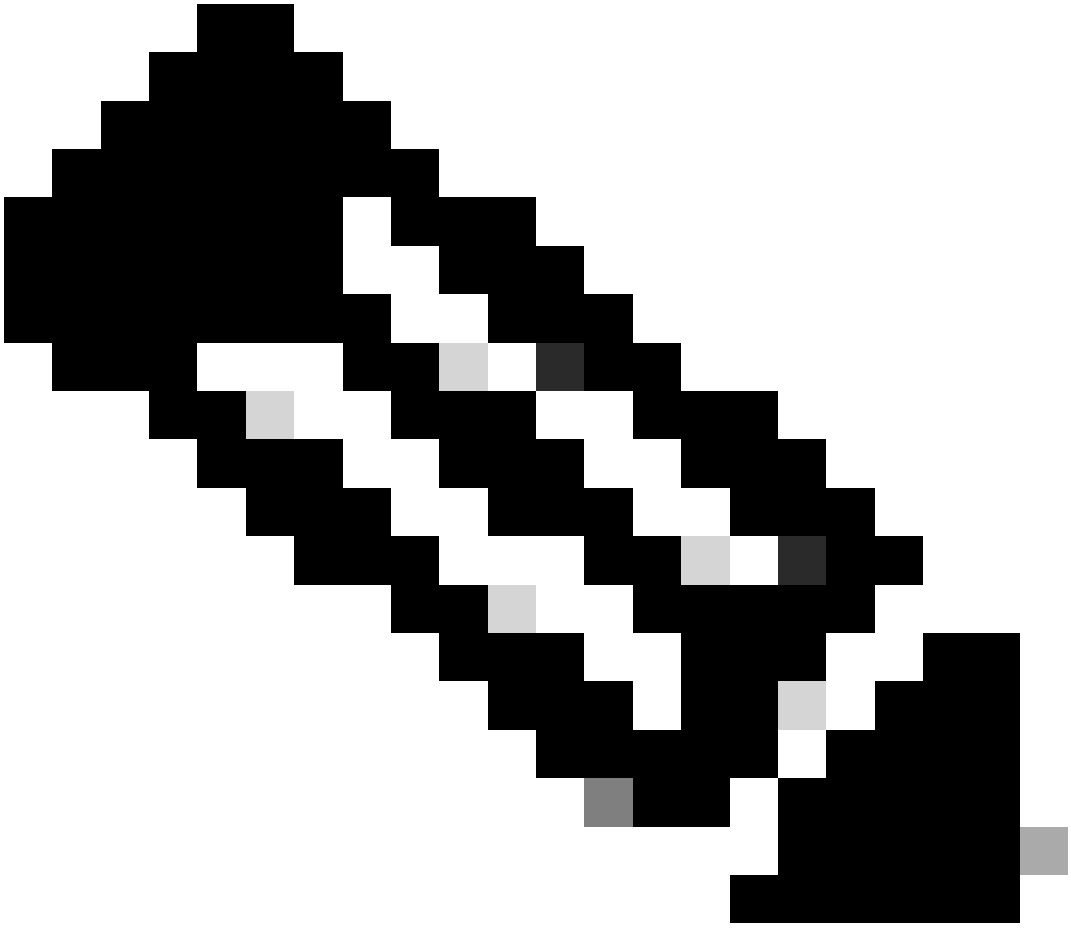
```
  Custom circuit-ids:
```

Vérifiez que la liaison de surveillance DHCP est créée

```
<#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
```

Dépannage (tout type de CGW)

Les débogages sont utiles pour montrer comment les processus de surveillance DHCP et de relais L2 traitent les paquets DHCP.



Remarque : ces débogages peuvent être utilisés pour tout type de déploiement qui utilise CGW avec DCHP L2 Relay.

Débogages de surveillance DHCP (leaf)

Debug Snooping pour confirmer le traitement des paquets

<#root>

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

Démarrer la tentative d'adresse DHCP hôte

- Pour ce document, une fermeture/aucune fermeture de l'interface SVI adressée via DHCP a été effectuée pour déclencher l'échange DORA
- Pour l'hôte Windows, vous pouvez exécuter la commande ipconfig /release **>** ipconfig /renew

Collectez les débogages à partir de show logging ou de la fenêtre du terminal

DÉTECTION DHCP

La détection provient du port faisant face à l'hôte

<#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
```

OFFRE DHCP

L'offre provient de l'interface du tunnel de fabric

<#root>

*Sep 19 20:16:33.180:

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

*Sep 19 20:16:33.194:

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

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

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

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

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

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

DHCP_SNOOPING: VxLAN vlan_id 202 VNI 20201 mod 1 port 1

*Sep 19 20:16:33.194:

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

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

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

REQUÊTE DHCP

La requête est vue depuis le port faisant face à l'hôte

<#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

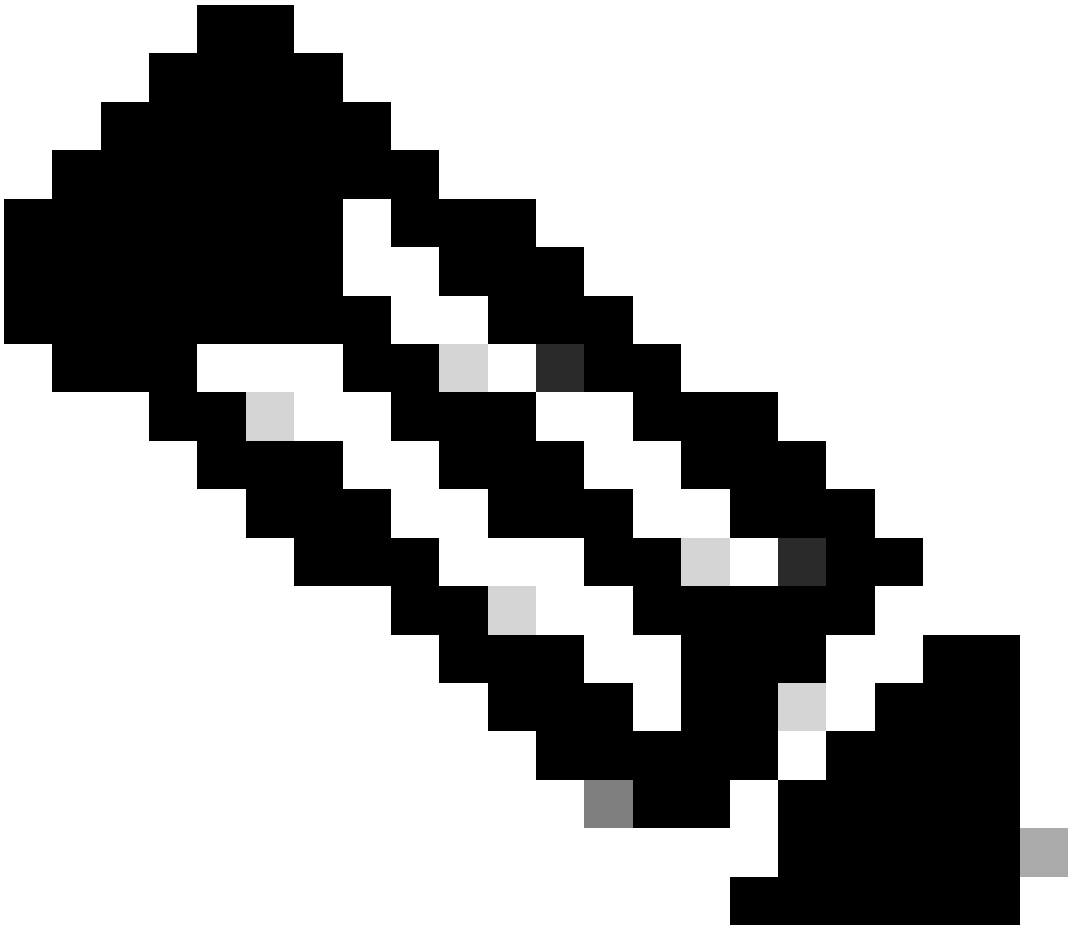
Un accusé de réception arrive de l'interface du tunnel de fabric

<#root>

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

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

*Sep 19 20:16:33.238:

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

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

DHCP_SNOOPING: opt82 data indicates local packet

*Sep 19 20:16:33.239:

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

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

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

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

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

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



> Remarque : ces débogages sont extraits. Ils produisent un vidage de mémoire du paquet, mais l'annotation de cette partie du résultat du débogage est en dehors de la portée de ce document.

Débogages de surveillance DHCP (CGW)

DÉTECTION DHCP

En raison de la manière dont le paquet est envoyé et reçu sur le CGW (épinglé au pare-feu), les débogages se déclenchent deux fois

Arrivée du fabric sur l’interface du tunnel et envoi de Tw 1/0/1 vers le pare-feu dans le VLAN de

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

Arrivée du pare-feu sur deux routeurs 1/0/2 dans le VLAN 2021 pour être envoyée à l'interface SVI et aide au serveur 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

OFFRE DHCP

Revient du serveur DHCP à l'interface SVI 2021 où l'assistant est configuré et transféré au pare-feu

<#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

Arrive du pare-feu dans le VLAN de fabric et est envoyé de CGW vers le fabric vers 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

REQUÊTE 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

Capture intégrée

Utiliser EPC pour confirmer l'échange de paquets DHCP et les paramètres corrects

- Ceci est illustré du point de vue de la CGW, mais le processus peut être répété sur Leaf pour vérifier l'échange de paquets
- Cet exemple montre la détection, car le processus et l'analyse sont identiques pour les autres paquets DHCP

Vérifier la route vers le bouclage leaf

<#root>

```
CGW#

show ip route 172.16.254.3

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

via TwentyFiveGigE1/0/48

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

via TwentyFiveGigE1/0/47

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

Configurez la capture pour qu'elle s'exécute sur les liaisons faisant face au 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
```

Démarrer la capture, déclencher votre hôte pour demander une adresse IP DHCP, arrêter la capture

<#root>

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

Affichez le résultat de la capture en commençant par la détection DHCP (attention à l'ID de transaction pour confirmer qu'il s'agit du même événement 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

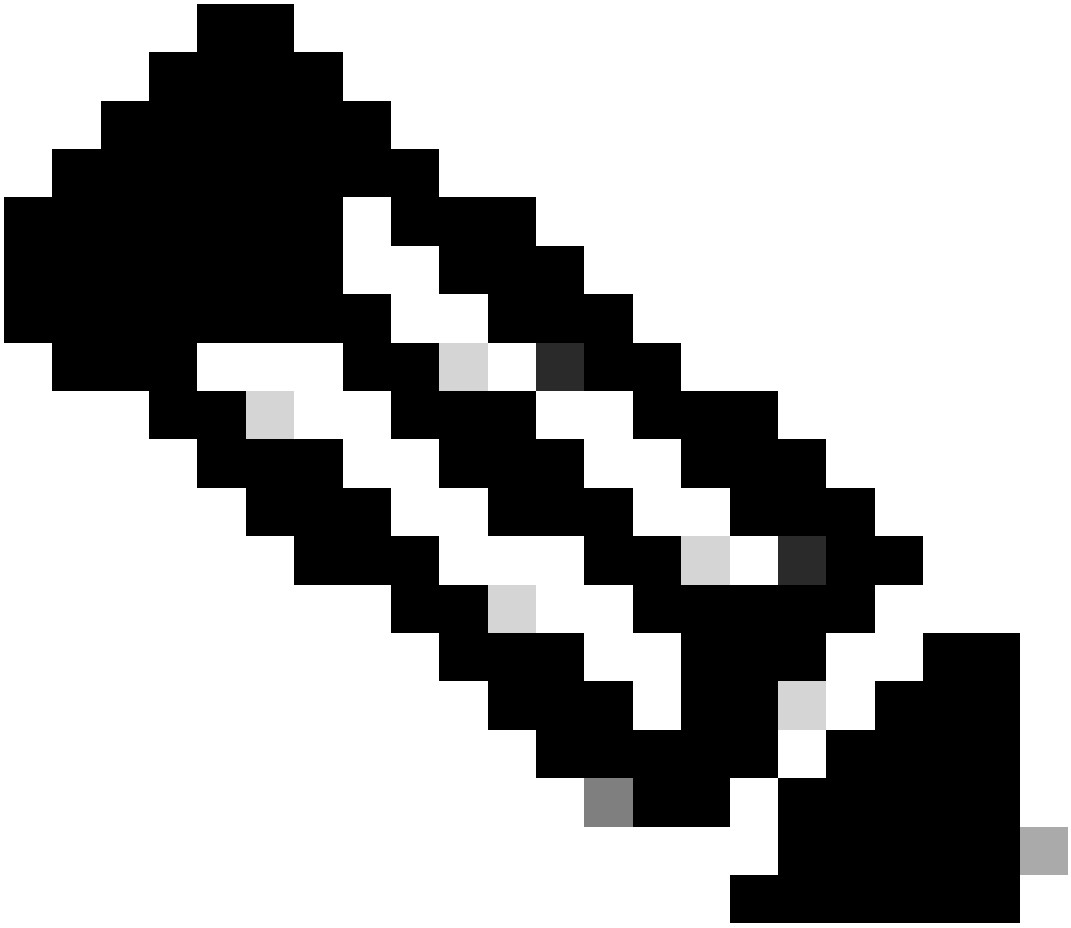
 Option: (53) DHCP Message Type (Discover)

        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
```



Remarque : l'outil de capture peut être utilisé sur n'importe quel Leafs ou CGW pour déterminer le dernier point qu'une partie de l'échange DHCP DORA est suspectée d'échouer.

Vérifier les statistiques de surveillance pour les erreurs

<#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.

Vérification du chemin de punt pour la surveillance DHCP

- CoPP est le principal composant qui abandonne les paquets dans le chemin de point

<#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
```

Une autre commande très utile pour localiser un éventuel déluge de paquets est « show platform software fed switch active punt rates interfaces »

- Ceci est très utile pour trouver une interface source où se produit une inondation qui encombre le chemin de point et affecte le trafic lié légitime au 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...>
```

Statistiques du client de surveillance DHCP

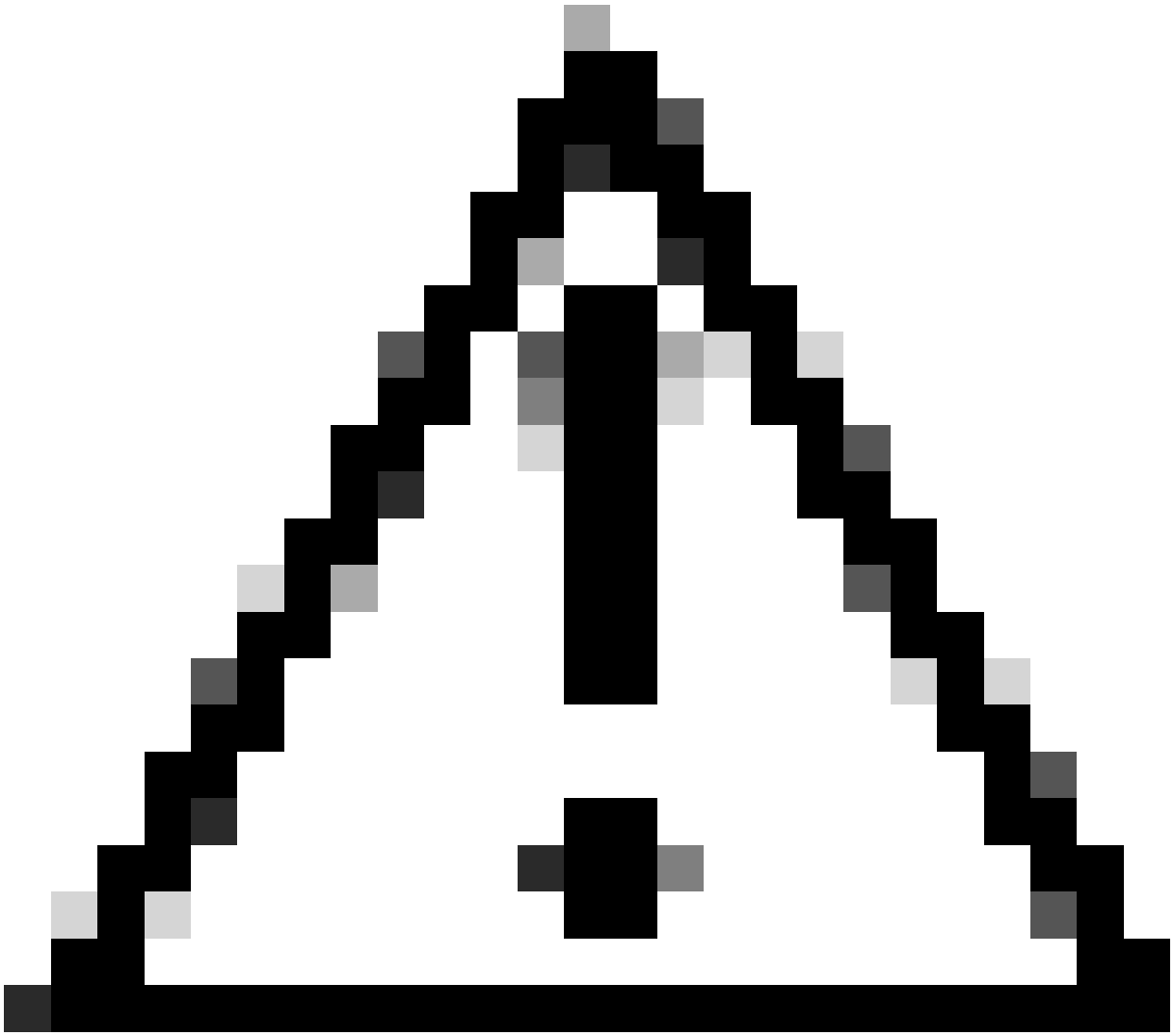
Observez l'échange de messages DHCP à l'aide de cette commande. Ceci peut être exécuté sur Leaf ou CGW pour voir la trace d'événement

<#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
```

Débogages supplémentaires

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



Attention : soyez prudent lorsque vous exécutez des débogages !

Informations connexes

- Implémenter la politique de routage EVPN BGP sur les commutateurs de la gamme Catalyst 9000
- Implémenter la segmentation de recouvrement protégée EVPN BGP sur les commutateurs de la gamme Catalyst 9000
- Fonctionnement et dépannage de la surveillance DHCP sur les commutateurs Catalyst 9000

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.