Implémenter la segmentation de recouvrement protégée EVPN BGP sur les commutateurs de la gamme Catalyst 9000

Table des matières

Introduction

Ce document décrit comment implémenter la segmentation de recouvrement protégée par VXLAN EVPN BGP sur les commutateurs de la gamme Catalyst 9000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Concepts de VxLAN EVPN BGP
- Dépannage de la monodiffusion EVPN BGP
- Stratégie de routage BGP EVPN VxLAN

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

Description des fonctionnalités de haut niveau

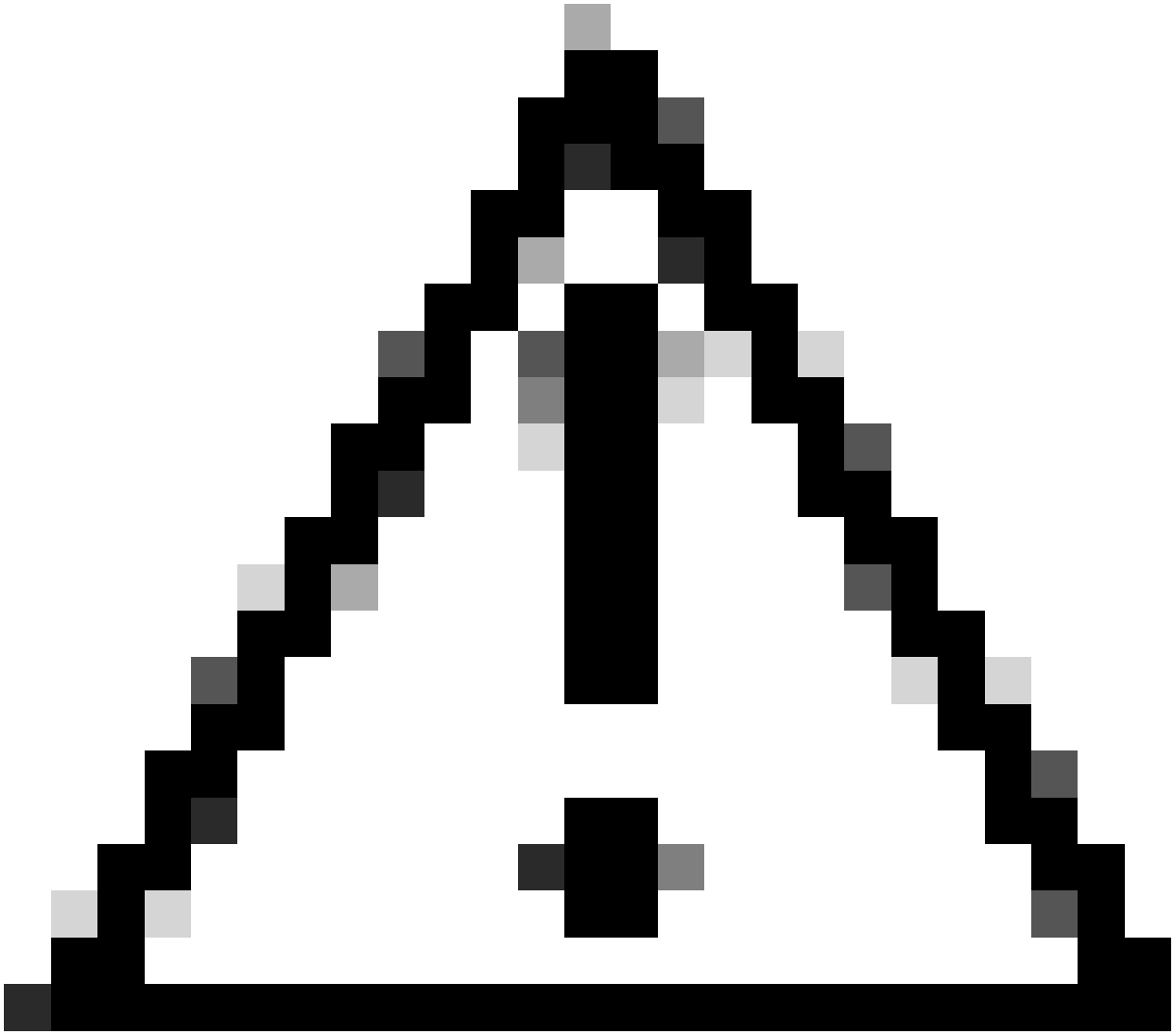
La fonctionnalité de segment protégé est une mesure de sécurité qui empêche les ports de transférer du trafic entre eux, même s'ils se trouvent sur le même VLAN et le même commutateur

- Cette fonctionnalité est similaire à « switchport protected » ou aux VLAN privés, mais pour les fabrics EVPN.
- Cette conception force tout le trafic vers le CGW où il peut être inspecté par un pare-feu avant d'être envoyé à sa destination finale.
- Les flux de trafic sont contrôlés, déterministes et faciles à inspecter à l'aide d'une appliance de sécurité centralisée.

Détails du document

Ce document est une partie 2 ou 3 documents interdépendants :

- Le document 1 : Implémenter la 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 : Ce document. S'appuyant sur la conception et la stratégie de superposition du document 1, ce document décrit la mise en oeuvre du mot clé « protected »
- Document 3 : Implémentation du relais DHCP de couche 2 EVPN BGP sur les commutateurs de la gamme Catalyst 9000 couvre le fonctionnement du relais DHCP sur un VTEP de couche 2 uniquement



Attention : vous devez implémenter la configuration du document 1 avant d'implémenter des configurations de segments protégés.

Types de segments protégés

Totalement isolé

- Permet uniquement la communication Nord-Sud, et
- La passerelle est annoncée dans le fabric avec l'interface de ligne de commande « default-gateway advertise »

La plupart du temps isolé

- Permet la communication Nord-Sud (dans ce cas, les flux de trafic Est/Ouest sont autorisés en fonction des politiques de trafic du pare-feu)
- Permet la communication Est-Ouest (en fonction des politiques de trafic du pare-feu)

- La passerelle est externe au fabric et l'interface SVI n'est pas annoncée à l'aide de la CLI « default-gateway advertise »

Comportement du commutateur

- Les hôtes ne peuvent pas communiquer directement entre eux même s'ils sont connectés au même commutateur (requête ARP non envoyée aux autres ports du même commutateur lorsque les hôtes se trouvent dans le même VRF/Vlan/segment)
- Aucun trafic BUM entre les VTEP de couche 2 (préfixes IMET filtrés à l'aide de la configuration de stratégie de routage)
- Tous les paquets provenant des hôtes sont relayés vers le leaf en limite pour être transférés. (Cela signifie que pour que l'hôte 1 communique avec l'hôte 2 sur le même noeud leaf, le trafic est épinglé au CGW)

Traitement de route de type 2

- Les leafs d'accès annoncent le RT2 local avec la communauté étendue E-Tree et l'indicateur Leaf défini
- Les leafs d'accès n'installent aucun RT2 distant reçu avec la communauté étendue E-Tree et l'indicateur Leaf défini dans le plan de données
- Les leafs d'accès ne s'installent pas entre eux RT2 dans le plan de données
- Les leafs d'accès et les leafs en limite (CGW) s'installent mutuellement RT2 dans le plan de données
- Aucune modification de configuration n'est requise sur le leaf d'accès ou le leaf en limite.

Résumé de la conception

- Pour la diffusion (BUM), la topologie RT3 est Hub and Spoke afin de forcer le trafic de diffusion tel que ARP jusqu'au GCW.
- Pour prendre en compte la mobilité de l'hôte, les RT2 sont à maillage global au niveau du plan de contrôle BGP (lorsqu'un hôte passe d'un VTEP à un autre, le numéro de séquence est incrémenté dans le RT2)
- Le plan de données installe les adresses MAC de manière sélective.
  - Un noeud terminal installe uniquement les adresses MAC et RT2 locales qui contiennent l'attribut DEF GW
  - Le CGW ne dispose pas du KW protégé et installe tous les adresses MAC locales et les RT2 distants dans son plan de données.

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

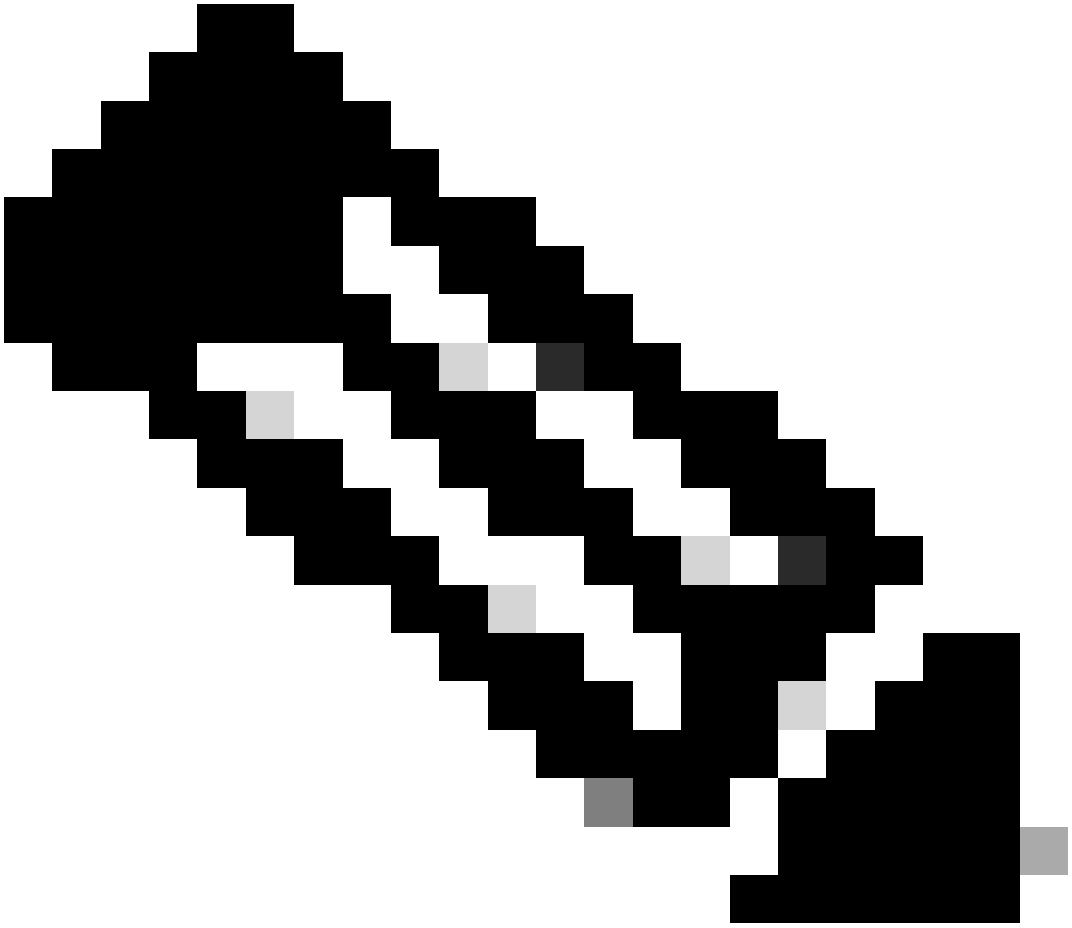
AF	Famille d'adresses	Définit les préfixes de type et les informations de routage des handles BGP
COMME	Système Autonome	Ensemble de préfixes IP routables sur Internet qui appartiennent à un réseau ou à un ensemble de réseaux qui sont tous gérés, contrôlés et supervisés par une seule entité ou organisation
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 par défaut	Attribut de communauté étendue BGP ajouté au préfixe MAC/IP via la 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

Diagrammes de flux

Diagramme de type de route 2 (RT2)

Ce schéma montre la conception de maillage global des préfixes d'hôte MAC/MAC-IP de type 2.



Remarque : le maillage global est nécessaire pour prendre en charge la mobilité et l'itinérance

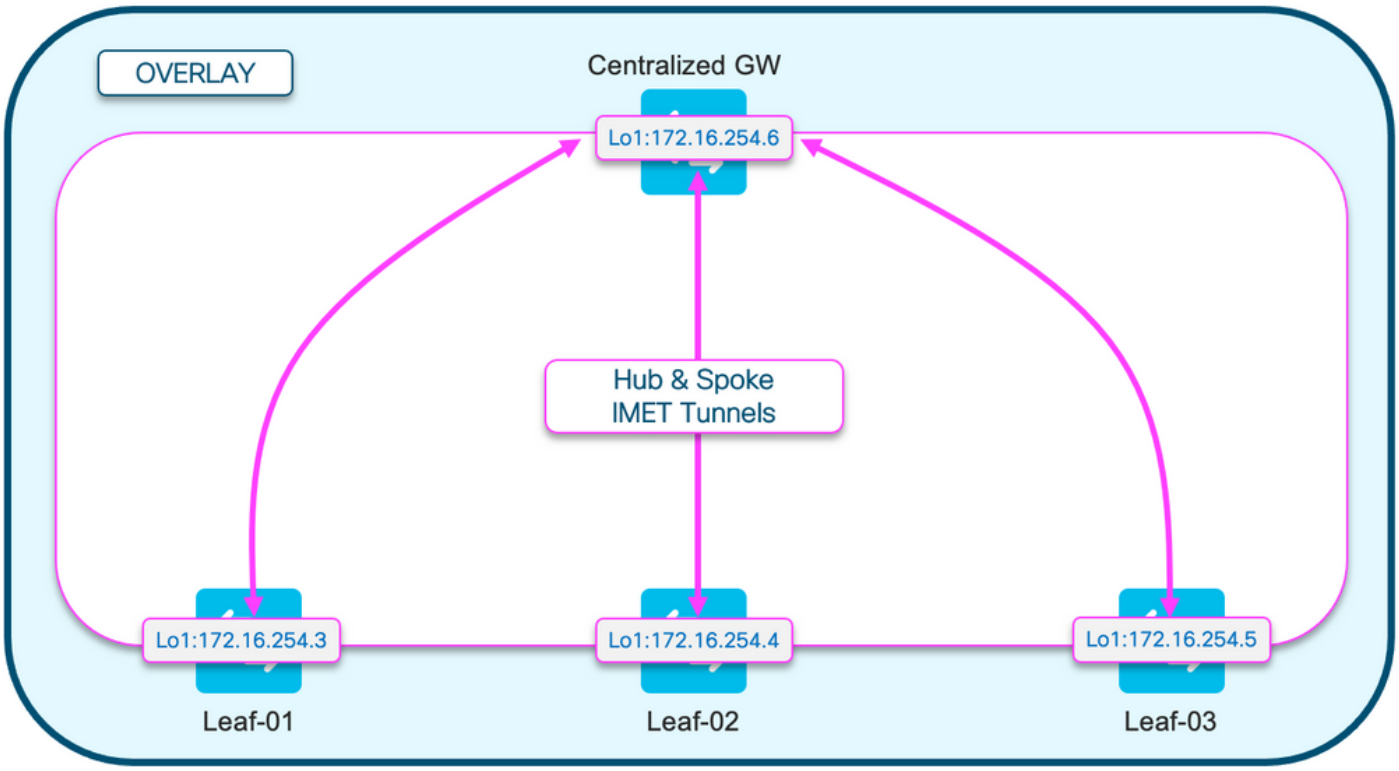
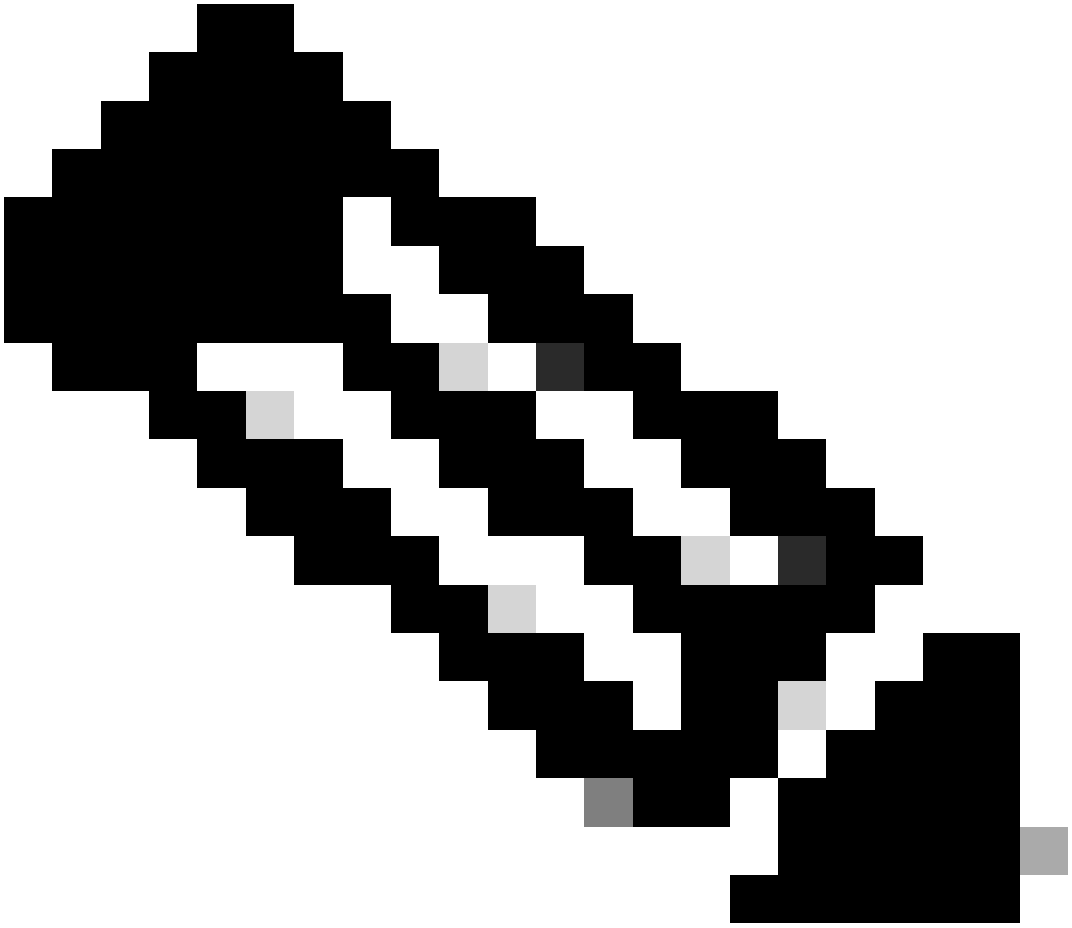


Diagramme de type de route 3 (RT3)

Ce schéma montre la conception Hub and Spoke des tunnels de diffusion IMET (RT3)



Remarque : la diffusion Hub and Spoke est requise pour empêcher les leafs avec le même segment de s'envoyer directement des messages de diffusion.

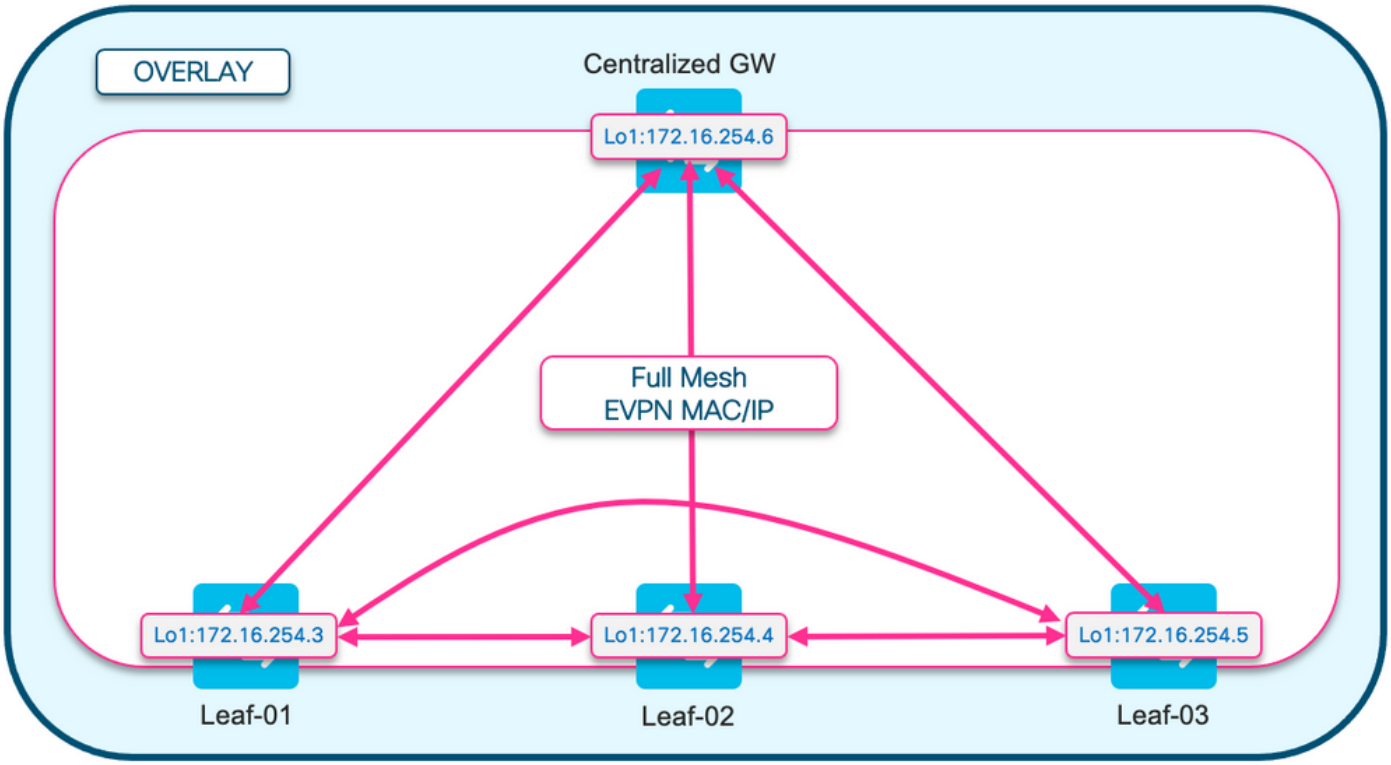
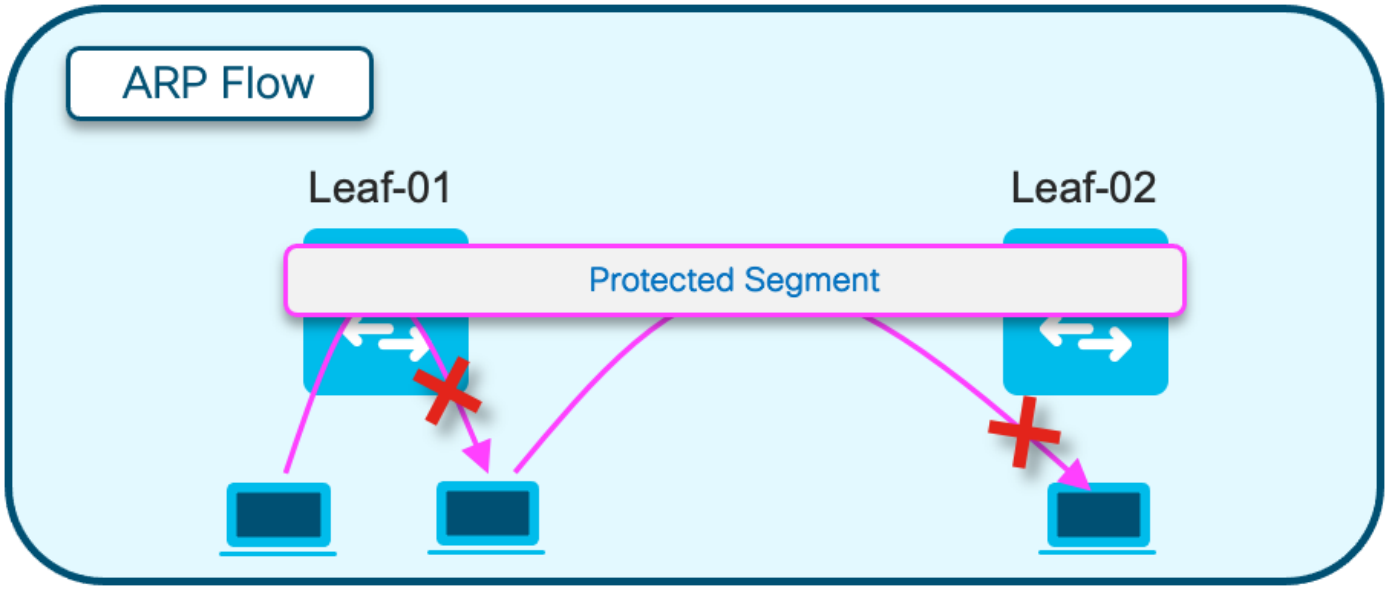
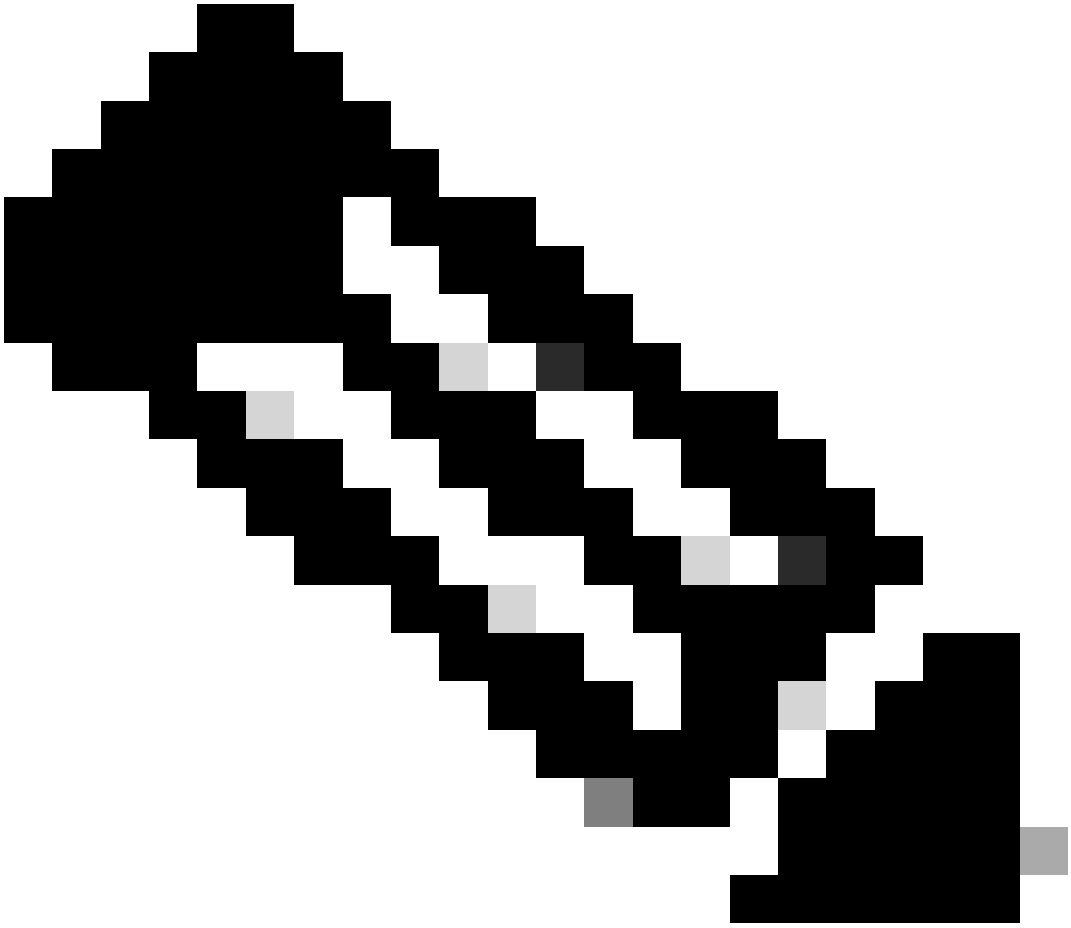


Schéma de résolution d'adresse (ARP)

Ce schéma montre que le protocole ARP n'est pas autorisé à atteindre un hôte dans le même segment EPVN. Lorsque les ARP d'hôte d'un autre hôte, seul le CGW obtient cet ARP et répond



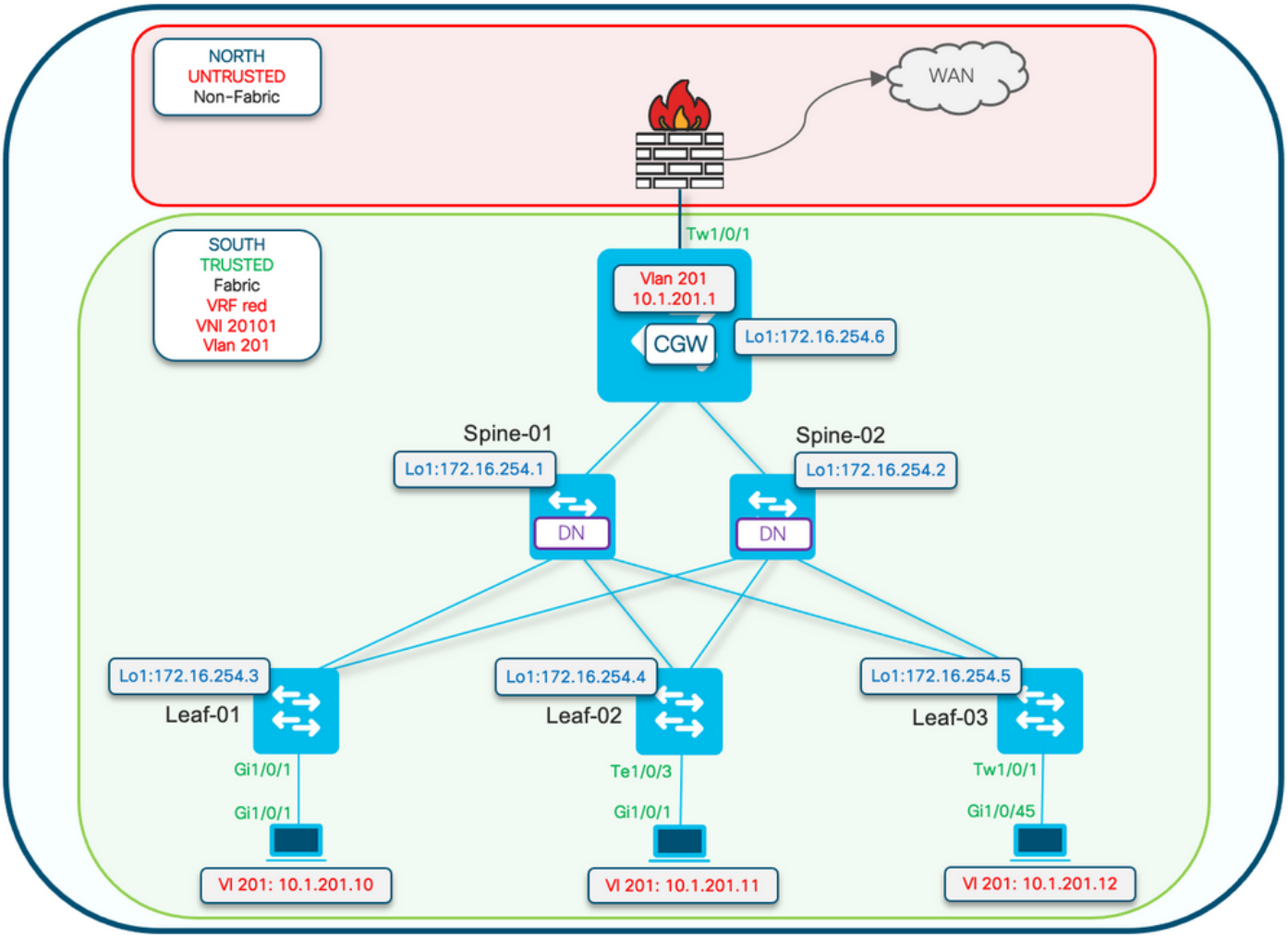


Remarque : ce changement de comportement ARP est instancié par l'utilisation du mot clé « protected ».

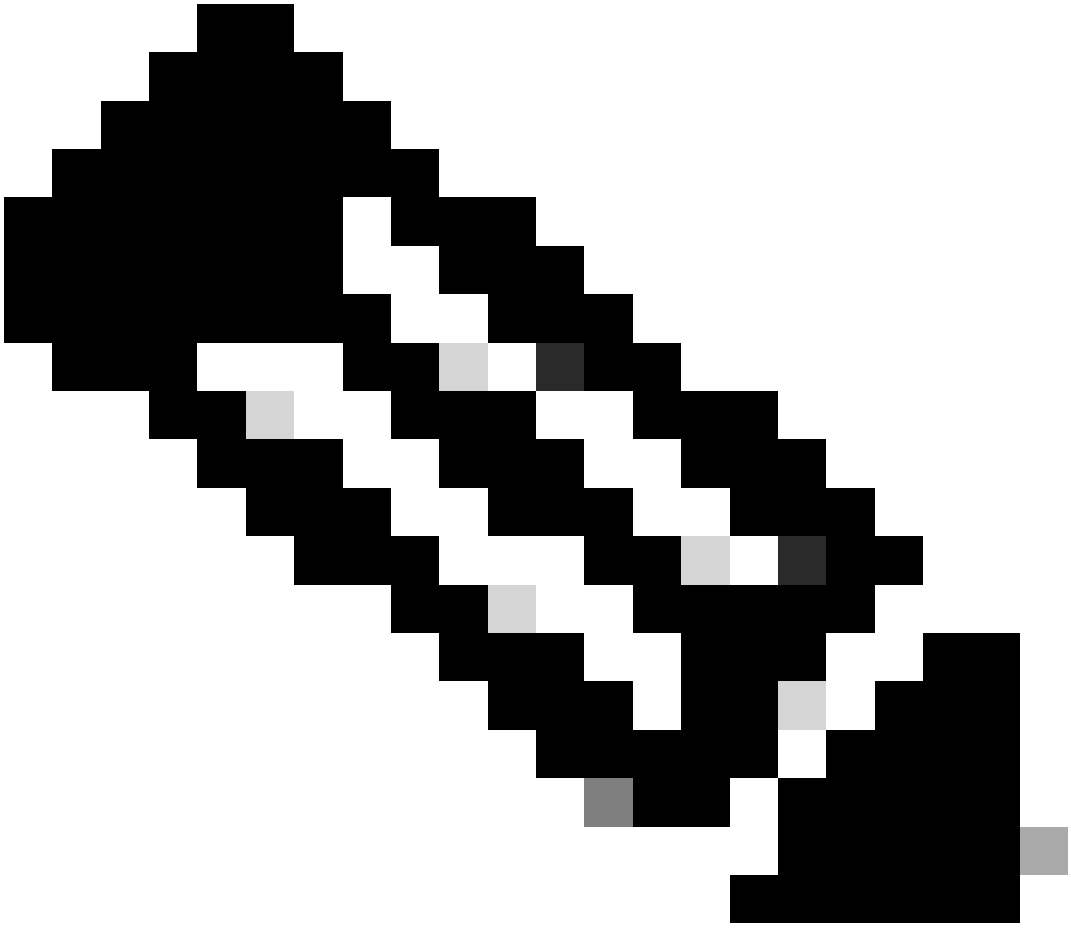
Exemple : member evpn-instance 202 vni 20201 protected

Configurer (totalement isolé)

Diagramme du réseau



Le mot-clé de configuration protégée est appliqué aux commutateurs Leaf. Le CGW est un périphérique proche qui installe toutes les adresses MAC.



Remarque : la configuration de la liste de la communauté de stratégie de routage et de la carte de routage qui contrôle l'importation/exportation des préfixes IMET est présentée dans Implémenter la stratégie de routage EVPN BGP sur les commutateurs de la gamme Catalyst 9000. Seules les différences de segments protégés sont affichées dans ce document.

Leaf-01 (configuration EVPN de base)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

 flooding-suppression address-resolution disable  <-- Disables ARP caching so ARP is always sent up to t

 router-id Loopback1
```

```
l2vpn evpn
instance 201
 vlan-based
 encapsulation vxlan
replication-type ingress                          <-- Sets segment to use Unicast replication of BUM traff
 multicast advertise enable
```

<#root>

```
Leaf01#
show run | sec vlan config
vlan configuration 201
 member evpn-instance 201 vni 20101
protected  <-- protected keyword added
```

CGW (configuration de base)

<#root>

```
CGW#
show running-config | beg l2vpn evpn instance 201
l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress
 default-gateway advertise enable    <-- adds the BGP attribute EVPN DEF GW:0:0 to the MAC/IP prefix
 multicast advertise enable
```

<#root>

```
CGW#
show running-config | sec vlan config
vlan configuration 201
 member evpn-instance 201 vni 20101
```

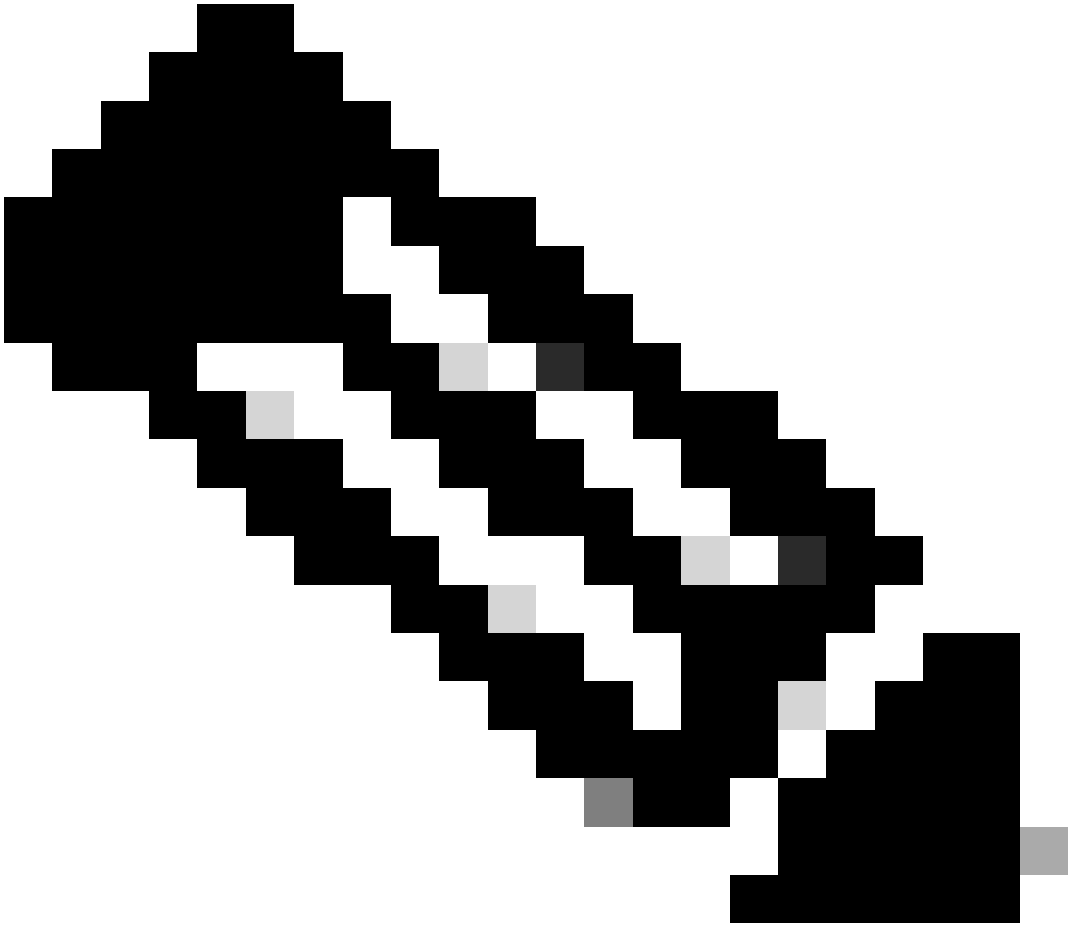
<#root>

```
CGW#
show run int nve 1
```

```
Building configuration...

Current configuration : 313 bytes
!
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 20101 ingress-replication local-routing  <-- 'ingress-replication' (Unicast all BUM traffic)
```

<#root>

```
CGW#
show run interface vlan 201

Building configuration...

Current configuration : 231 bytes
!
interface Vlan201

mac-address 0000.beef.cafe          <-- MAC is static in this example for viewing simplicity. This is no
 vrf forwarding red                  <-- SVI is in VRF red
 ip address 10.1.201.1 255.255.255.0
 no ip redirects
 ip local-proxy-arp                 <-- Sets CGW to Proxy reply even for local subnet ARP requests
 ip pim sparse-mode
 ip route-cache same-interface      <-- This is auto added when local-proxy-arp is configured. However,
 ip igmp version 3
 no autostate
```



Remarque : aucune stratégie BGP n'est appliquée au CGW. Le CGW est autorisé à recevoir et à envoyer tous les types de préfixe (RT2, RT5 / RT3).

Vérifier (Totalement isolé)

Détails EVI

<#root>

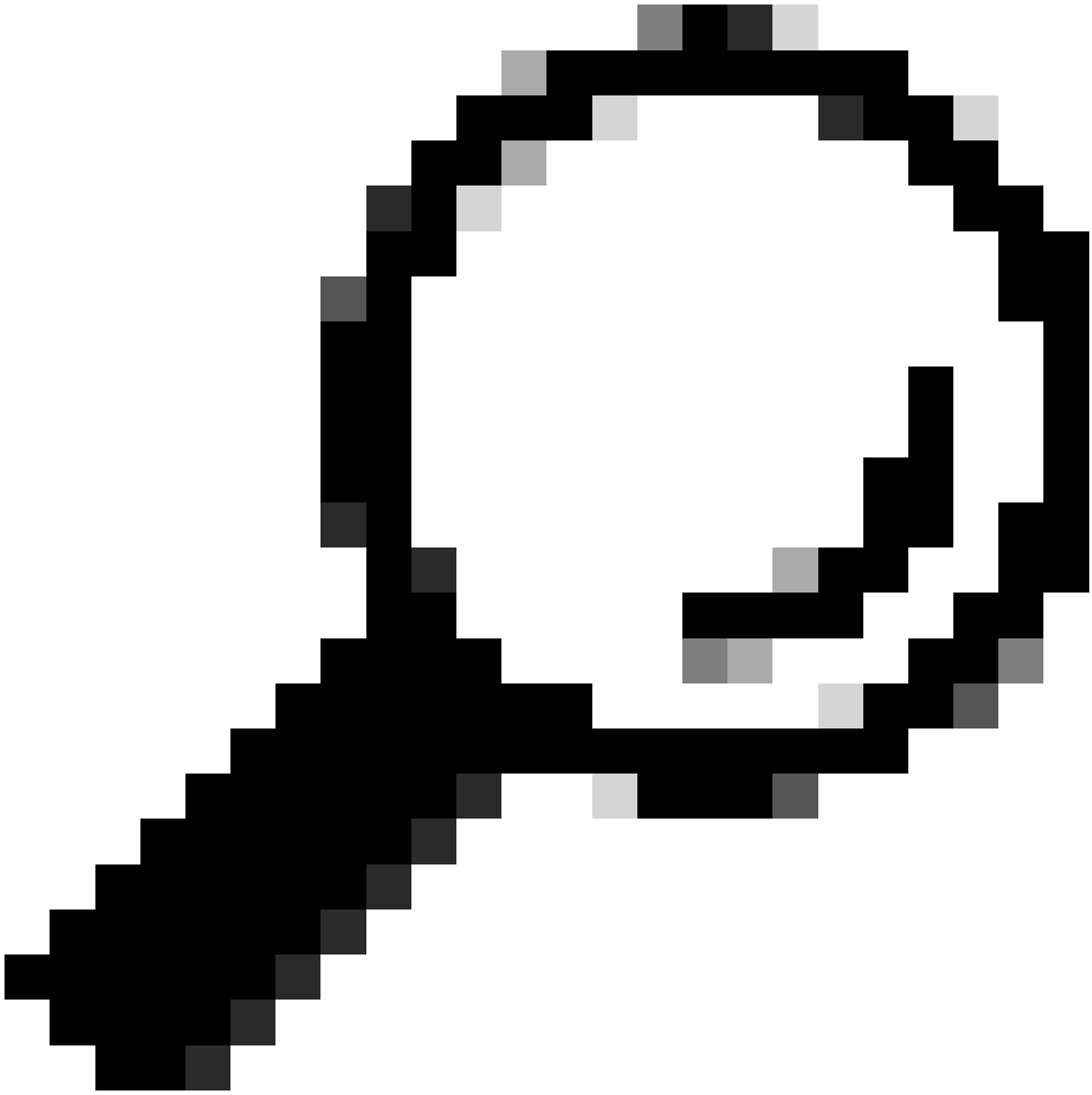
```
Leaf01#

sh l2vpn evpn evi 201 detail

EVPN instance:       201 (VLAN Based)
  RD:                172.16.254.3:201 (auto)
  Import-RTs:        65001:201
  Export-RTs:        65001:201
  Per-EVI Label:     none
  State:             Established
```

```
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Enabled
  AR Flood Suppress: Disabled (global)


Vlan:              201
    Protected:       True (local access p2p blocked)  <-- Vlan 201 is in protected mode

<...snip...>
```

Génération locale RT2 (hôte local vers RT2)

Vérifiez la chaîne de dépendance des composants de l’apprentissage local de l’hôte à la génération RT2 :

- SISF (bien que le Leaf ne dispose pas d'interface SVI, SISF collecte toujours les informations d'hôte via la trame ARP à partir de l'hôte)
- Gestionnaire EVPN
- NERVURE L2
- BGP

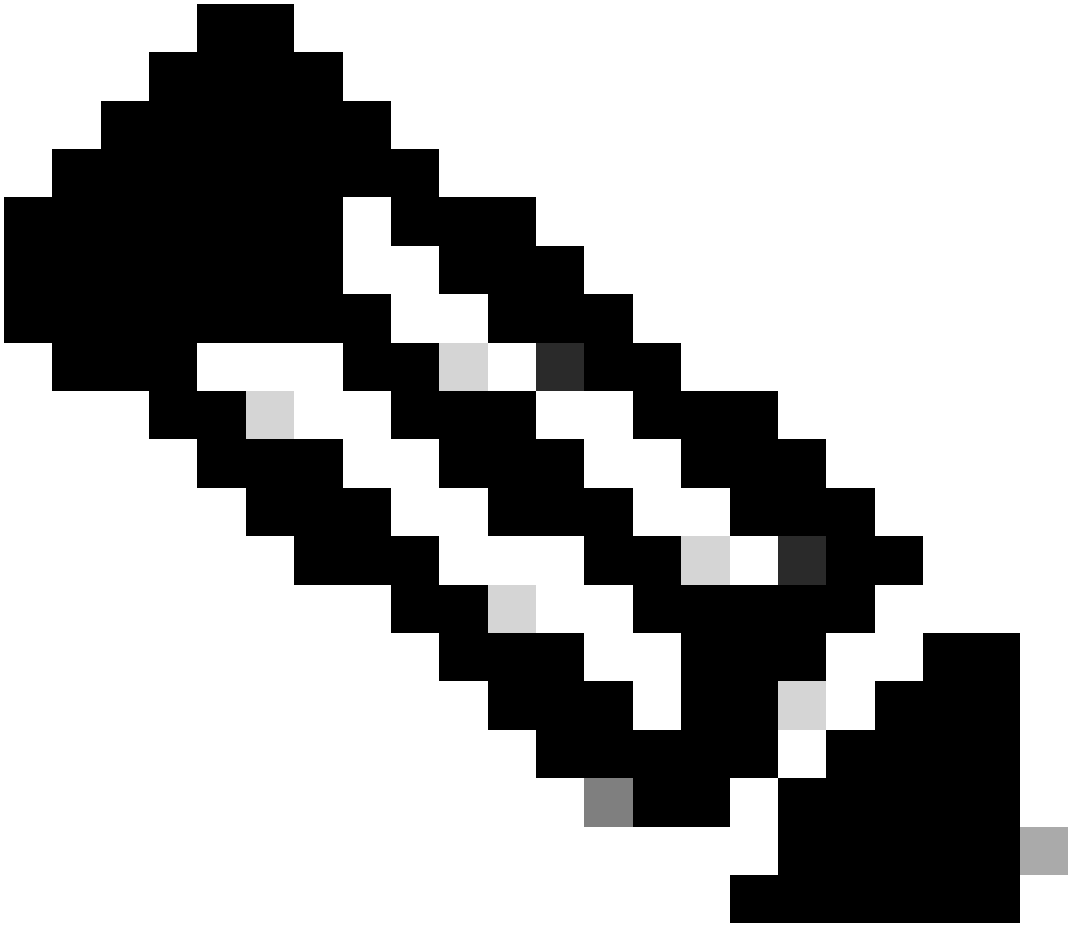


Conseil : si un composant précédent n'est pas correctement programmé, toute la chaîne de dépendances se rompt (exemple : SISF n'a pas d'entrée, alors BGP ne peut pas créer de RT2).

ISF

Vérifiez que le SISF a acquis l'hôte dans la base de données (informations sur l'hôte acquises à partir du DHCP ou du protocole ARP)

- SISF apprend les entrées MAC à partir de l'apprentissage IOS-MATM, puis les envoie à EVPN Mgr (doit être MAC-REACHABLE avec la stratégie « evpn-sisf-policy »)
- SISF glane une liaison IP/MAC sur un VTEP local et en utilisant le gestionnaire EVPN que les informations sont censées être programmées comme une route /32 via BGP vers d'autres leafs.



Remarque : dans ce scénario, l'hôte a une adresse IP statique, de sorte que SISF utilise ARP pour glaner les détails de l'hôte. La section Principalement isolé présente la surveillance DHCP et DHCP.

<#root>

```
Leaf01#

show device-tracking database vlanid 201

vlanDB has 1 entries for vlan 201, 1 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DHC
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      age

ARP
```

```
 10.1.201.10

0006.f601.cd43


Gi1/0/1

    201        0005       3mn        REACHABLE  86 s

<-- Gleaned from local host ARP Request
```

Gestionnaire EVPN

EVPN Mgr apprend l'adresse MAC locale et s'installe dans L2RIB. EVPN Mgr apprend également l'adresse MAC distante de L2RIB, mais l'entrée est utilisée uniquement pour traiter la mobilité MAC

Confirmer que le gestionnaire EVPN est mis à jour avec l'entrée SISF

<#root>

```
Leaf01#

show l2vpn evpn mac evi 201

MAC Address    EVI   VLAN  ESI                       Ether Tag  Next Hop(s)
-------------- ----- ----- ------------------------- ---------- ---------------

0006.f601.cd43 201   201

0000.0000.0000.0000.0000 0

         Gi1/0/1:201    <-- MAC in VLan 201 local interface Gi1/0/1:service instance 201

<...snip...>
```

NERVURE L2

- L2RIB apprend l'adresse MAC locale à partir d'EVPN Mgr et l'envoie à BGP et L2FIB
- L2RIB est également responsable de l'apprentissage des MAC distants à partir de BGP pour mettre à jour EVPN Mgr et L2FIB.
- L2RIB a besoin de Local et de Remote pour que les autres composants soient correctement mis à jour.
- Le composant L2RIB se situe entre l'apprentissage MAC local et distant, selon la direction/le composant à mettre à jour

Vérifiez que L2RIB est mis à jour avec l'adresse MAC locale du gestionnaire EVPN

<#root>

```
Leaf01#
show l2route evpn mac topology 201      <-- View the overall topology for this segment
  EVI       ETag
Prod
    Mac Address                                    Next Hop(s) Seq Number
----- ---------- ----- -------------- ------------------------------------------------- ----------
  201          0
BGP
 0000.beef.cafe                                V:20101 172.16.254.6          0
<-- produced by BGP who updated L2RIB (remote learn)
  201          0
L2VPN
 0006.f601.cd43                                Gi1/0/1:201          0
<-- produced by EVPN Mgr who updated L2RIB (local learn)


Leaf01#
show l2route evpn mac mac-address 0006.f601.cd43 detail
EVPN Instance:            201
Ethernet Tag:             0
Producer Name:            L2VPN                <-- Produced by local
MAC Address:              0006.f601.cd43       <-- Host MAC Address
Num of MAC IP Route(s):   1
Sequence Number:          0
ESI:                      0000.0000.0000.0000.0000
Flags:                    B()
Next Hop(s):              Gi1/0/1:201 (E-LEAF) <-- Port:Instance and info about the Role (Leaf)
```

BGP

Vérifiez que BGP est mis à jour par L2RIB

<#root>

```
Leaf01#
show bgp l2vpn evpn route-type 2 0 0006.f601.cd43 *
BGP routing table entry for [2][172.16.254.3:201][0][48][0006F601CD43][0][*]/20, version 268232
Paths: (1 available, best #1,
table evi_201
)
```

<-- In the totally isolated evi context

  Advertised to update-groups:
     2
  Refresh Epoch 1
  Local

 0.0.0.0 (via default) from 0.0.0.0

 (172.16.255.3)

<-- from 0.0.0.0 indicates local

      Origin incomplete, localpref 100, weight 32768, valid, sourced,

local

, best

<-- also indicates local

      EVPN ESI: 00000000000000000000, Label1 20101
      Extended Community: RT:65001:201 ENCAP:8

EVPN E-Tree:flag:1

,label:0

<-- EVPN e-Tree attribute with Leaf flag = 1 (added to indicate this is a host address)

      Local irb vxlan vtep:
        vrf:not found, l3-vni:0
        local router mac:0000.0000.0000
        core-irb interface:(not found)

 vtep-ip:172.16.254.3 **<-- Local VTEP Loopback**

      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 14 2023 20:16:17 UTC

Apprentissage RT2 à distance (passerelle par défaut RT2)

BGP

Vérifiez que BGP a appris le préfixe CGW RT2

<#root>

Leaf01#

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

BGP routing table entry for [2][172.16.254.3:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24, version 1141
Paths: (1 available, best #1,

table evi_201

)

```
<-- EVI context is 201

  Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:201][0][48][0000BEEFCAFE][32][10.1.201.1]/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 20101               <-- Correct segment identifier

      Extended Community: RT:65001:201 ENCAP:8

EVPN DEF GW:0:0    <-- Default gateway attribute is added via the 'default gateway advertise CLI'

      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 1 2023 15:27:45 UTC
```

NERVURE L2

Vérifier la mise à jour de BGP L2RIB

- L2RIB apprend l'adresse MAC locale à partir du gestionnaire EVPN et l'envoie à BGP et L2FIB. L2RIB est également responsable de l'apprentissage des MAC distants à partir de BGP pour mettre à jour EVPN Mgr et L2FIB.
- L2RIB a besoin de Local et de Remote pour que les autres composants soient correctement mis à jour.
- Le composant L2RIB se situe entre l'apprentissage MAC local et distant, selon la direction et le composant à mettre à jour.

<#root>

```
Leaf01#

show l2route evpn default-gateway host-ip 10.1.201.1

  EVI       ETag  Prod    Mac Address                                Host IP
----- ---------- ----- -------------- ---------------------------------------- ------------------------


201

          0

BGP


0000.beef.cafe


10.1.201.1

                              V:20101 172.16.254.6

<-- L2RIB has the MAC-IP of the Gateway programmed
```

FIB2L

Vérification dans L2FIB

- Composant chargé de mettre à jour FED avec les MAC pour programmer dans le matériel.
- Les entrées MAC distantes installées par L2FIB dans FED-MATM ne sont PAS envoyées à IOS-MATM (IOS-MATM affiche uniquement les adresses MAC locales, tandis que FED-MATM affiche les adresses MAC locales et distantes)
- La sortie L2FIB affiche uniquement les adresses MAC distantes (il n'est pas responsable de la programmation des adresses MAC locales).

<#root>

```
Leaf01#

show l2fib bridge-domain 201 address unicast 0000.beef.cafe


MAC Address                  :

0000.beef.cafe                                        <-- CGW MAC

Reference Count              : 1
Epoch                        : 0

Producer                     : BGP                                                    <-- Learned fro

Flags                        : Static
Adjacency                    :

VXLAN_UC

  PL:2973(1) T:VXLAN_UC [MAC]20101:

172.16.254.6  <-- CGW Loopback IP

PD Adjacency                 : VXLAN_UC  PL:2973(1) T:VXLAN_UC [MAC]20101:172.16.254.6
Packets                      : 6979
Bytes                        : 0
```

NOURRIR

Vérifier dans FED MATM

- Au niveau matériel des leafs configurés avec le mot clé protected, vous ne devriez voir que l'adresse MAC de la passerelle par défaut CGW et les adresses MAC de l'hôte local.
- Le commutateur recherche le préfixe RT2 pour l'attribut DEF GW afin de déterminer quel MAC distant est éligible à l'installation.

<#root>

```
Leaf01#
show platform software fed switch active matm macTable vlan 201
VLAN   MAC
Type
  Seq#    EC_Bi  Flags  machandle           siHandle            riHandle            diHandle
Con
--------------------------------------------------------------------------------------------------
201    0000.beef.cafe


0x5000001
       0      0     64  0x7a199d182498      0x7a199d183578
0x71e059173e08
      0x0                          0       82
VTEP 172.16.254.6
 adj_id 9
No
<-- Only remote MAC installed in Fed is the Default Gateway (0x5000001 type) Conn = No (meaning not dire
201    0006.f601.cd01
0x1
    2458      0      0  0x7a199d1a2248      0x7a199d19eef8      0x0                 0x7a199c6f7cd8
201    0006.f601.cd43        0x1    8131      0      0  0x7a199d195a98      0x7a199d19eef8      0x0
<-- Two local MAC addresses (0x1 type) Conn = Yes (directly connected)


Total Mac number of addresses:: 5
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:: 3
*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_RESV
MAT_DO_NOT_AGE           0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT              0x400  MAT_DROP
MAT_DUP_ADDR            0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR          0x4000  MAT_ROUT
MAT_WIRELESS_ADDR      0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT   0x40000  MAT_WIRE
MAT_DLR_ADDR          0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR         0x400000  MAT_LISP
MAT_LISP_REMOTE_ADDR 0x1000000
  MAT_VPLS_ADDR        0x2000000
MAT_LISP_GW_ADDR     0x4000000
```

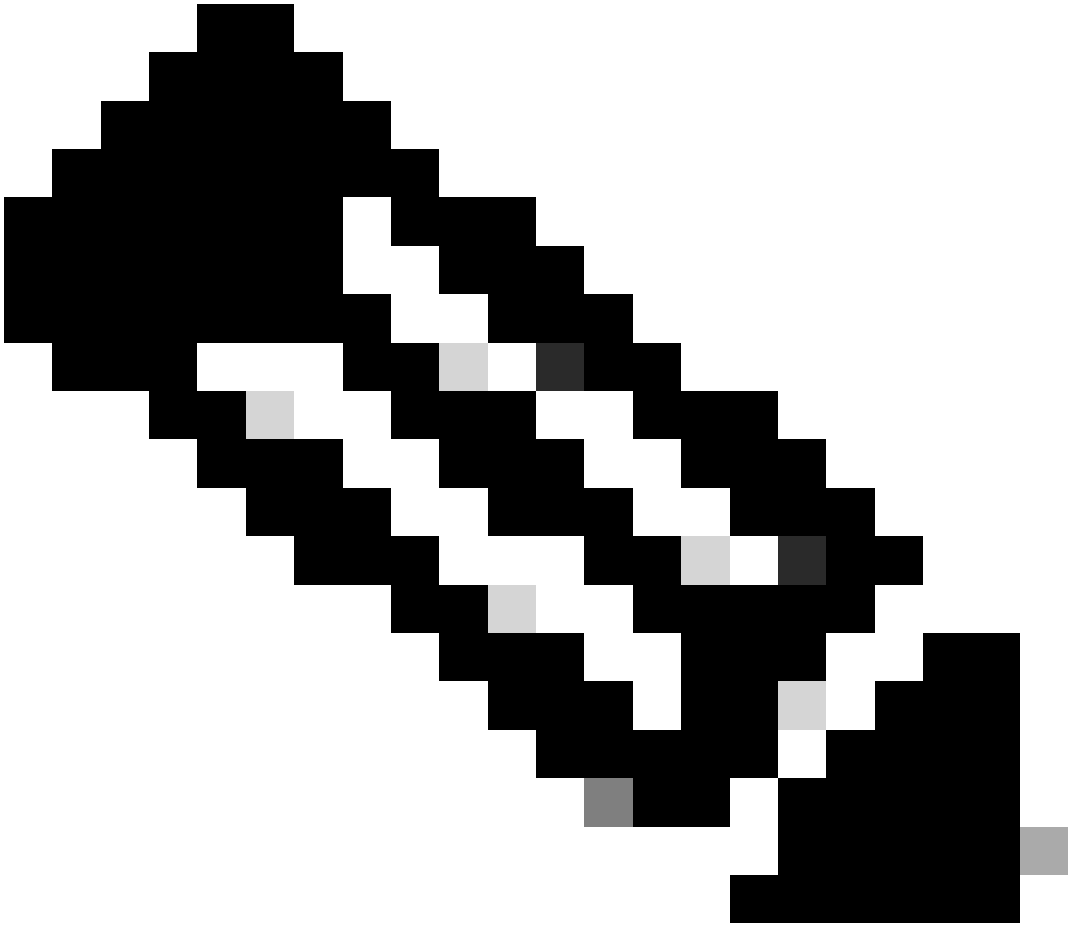
```
<-- the addition of these values = 0x5000001

MAT_LISP_REMOTE_ADDR 0x1000000
MAT_LISP_GW_ADDR 0x4000000
MAT_DYNAMIC_ADDR 0x1
```

Contiguïté du plan de données

Comme dernière étape après avoir confirmé l'entrée FED, vous pouvez résoudre l'index de réécriture (RI)

<#root>

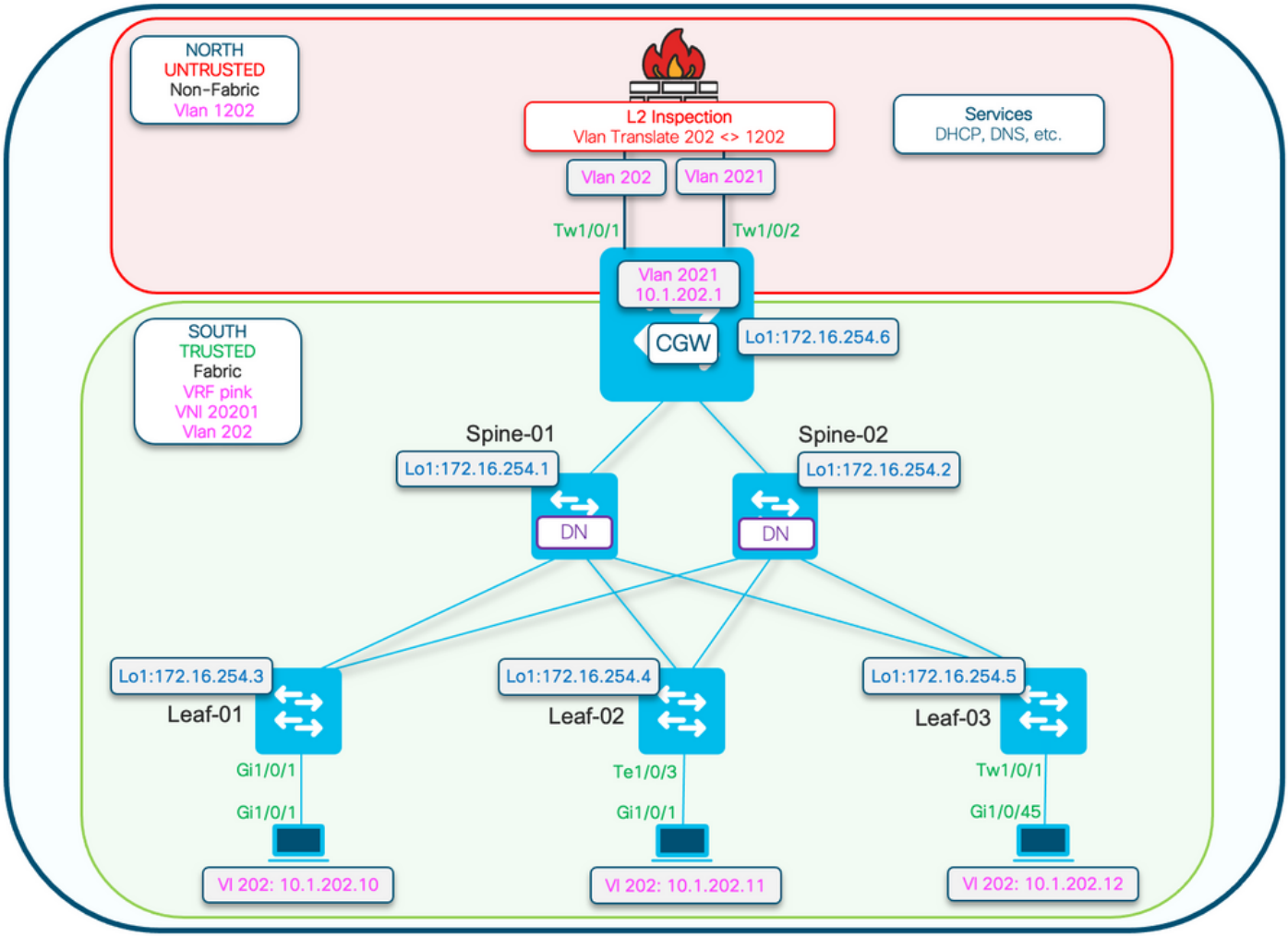
```
Leaf01#

sh platform hardware fed switch active fwd-asic abstraction print-resource-handle 0x71e059173e08 0
<-- 0x71e059173e08 is taken from previous FED command riHandle for the CGW MAC

Handle:0x71e059173e08 Res-Type:ASIC_RSC_RI Res-Switch-Num:255 Asic-Num:255 Feature-ID:AL_FID_L2_WIRELESS
priv_ri/priv_si Handle: 0x71e05917b8d8Hardware Indices/Handles: index0:0x38  mtu_index/l3u_ri_index0:0x0
Features sharing this resource:58 (1)]


Brief Resource Information (ASIC_INSTANCE# 0)
---------------------------------------
ASIC#:0 RI:56 Rewrite_type:AL_RRM_REWRITE_LVX_IPV4_L2_PAYLOAD_ENCAP_EPG(116) Mapped_rii:LVX_L3_ENCAP_L2_

 Src IP:     172.16.254.3      <-- source tunnel IP
 Dst IP:     172.16.254.6      <-- dest tunnel IP

 iVxlan dstMac:     0x9db:0x00:0x00
 iVxlan srcMac:     0x00:0x00:0x00
 IPv4 TTL:     0
 iid present:     0

 lisp iid:     20101            <-- Segment 20101

 lisp flags:     0

 dst Port:     4789             <-- VxLAN

 update only l3if:     0
 is Sgt:     0
 is TTL Prop:     0
 L3if LE:     53 (0)
 Port LE:     281 (0)
 Vlan LE:     8 (0)
```

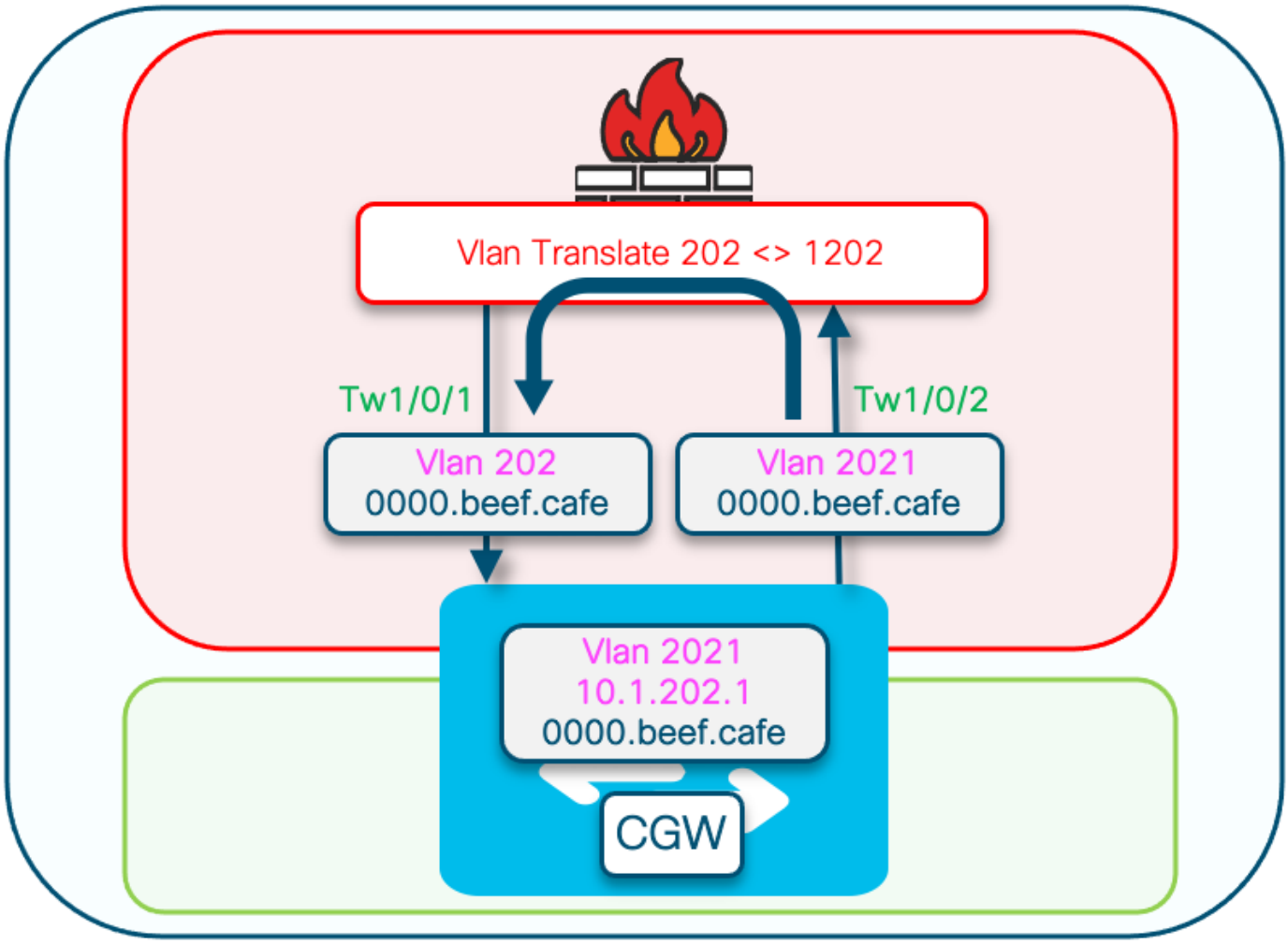


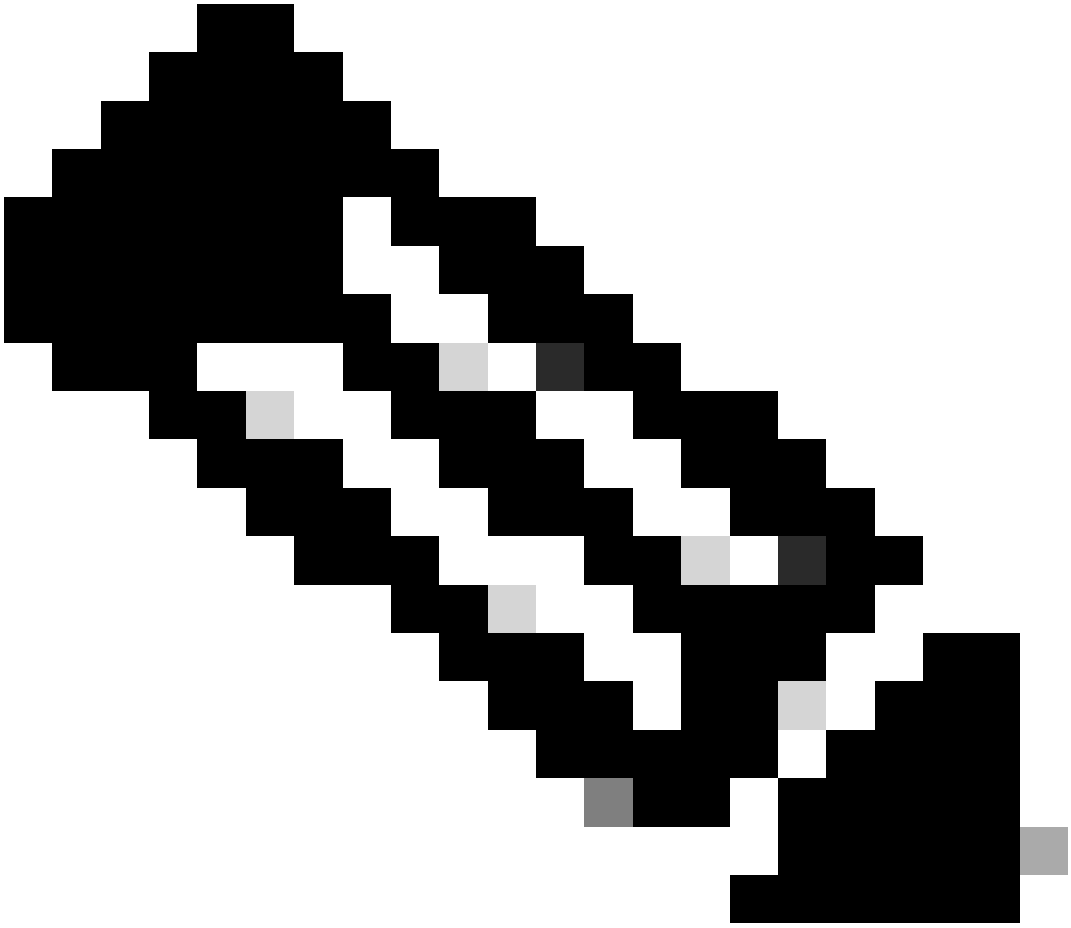
Remarque : vous pouvez également utiliser « show platform software fed switch active matm macTable vlan 201 detail » qui enchaîne cette commande avec la commande FED en un seul résultat

Configurer (partiellement isolé)

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


Vlan Translate 202 <> 1202
Tw1/0/1
Tw1/0/2
Vlan 202
0000.beef.cafe
Vlan 2021
0000.beef.cafe
Vlan 2021
10.1.202.1
0000.beef.cafe
CGW



Remarque : cette section traite uniquement des différences par rapport aux segments totalement isolés.

- Stratégie de routage pour marquer l'adresse MAC IP de la passerelle GCW avec l'attribut DEF GW
- Stratégie de suivi de périphérique personnalisée requise pour empêcher les défaillances MAC
- Liaison de suivi de périphérique statique pour l'adresse IP MAC GW

Leaf-01 (configuration EVPN de base)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn
```

```
 replication-type static
 flooding-suppression address-resolution disable  <-- Disables ARP caching so ARP is always sent up to t
 router-id Loopback1
l2vpn evpn
instance 202
 vlan-based
 encapsulation vxlan
replication-type ingress
 multicast advertise enable
```

<#root>

```
Leaf01#
show run | sec vlan config
vlan configuration 202
 member evpn-instance 202 vni 20201
protected <-- protected keyword added
```

CGW (configuration de base)

Définissez le mode de réplication sous l'onglet

<#root>

```
CGW#
show run int nve 1
Building configuration...

Current configuration : 313 bytes
!
interface nve1
 no ip address
 source-interface Loopback1
 host-reachability protocol bgp
 member vni 20201 ingress-replication local-routing <-- 'ingress-replication' (Unicast all BUM traffic)
end
```

Configurer l'interface SVI de passerelle externe

<#root>

```
CGW#
show run interface vlan 2021

Building configuration...

Current configuration : 231 bytes
!
interface Vlan2021

mac-address 0000.beef.cafe          <-- MAC is static in this example for viewing simplicity. This is no
 vrf forwarding pink                  <-- SVI is in VRF pink
 ip address 10.1.202.1 255.255.255.0
 no ip redirects
 ip local-proxy-arp                 <-- Sets CGW to Proxy reply even for local subnet ARP requests
 ip pim sparse-mode
 ip route-cache same-interface      <-- This is auto added when local-proxy-arp is configured. However,
 ip igmp version 3
 no autostate
end
```

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 à des réseaux locaux virtuels/externes

<#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 externalgateway 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 map
```

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

<#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 | s r 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
```

Vérification (partiellement isolée)

Détails EVI

<#root>

```
Leaf01#

show l2vpn evpn evi 202 detail

EVPN instance:       202 (VLAN Based)
  RD:                172.16.254.3:202 (auto)
  Import-RTs:        65001:202
  Export-RTs:        65001:202
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Enabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Enabled

  Vlan:              202
    Protected:       True (local access p2p blocked)  <-- Vlan 202 is in protected mode

<...snip...>
```

Génération locale RT2 (hôte local vers RT2)

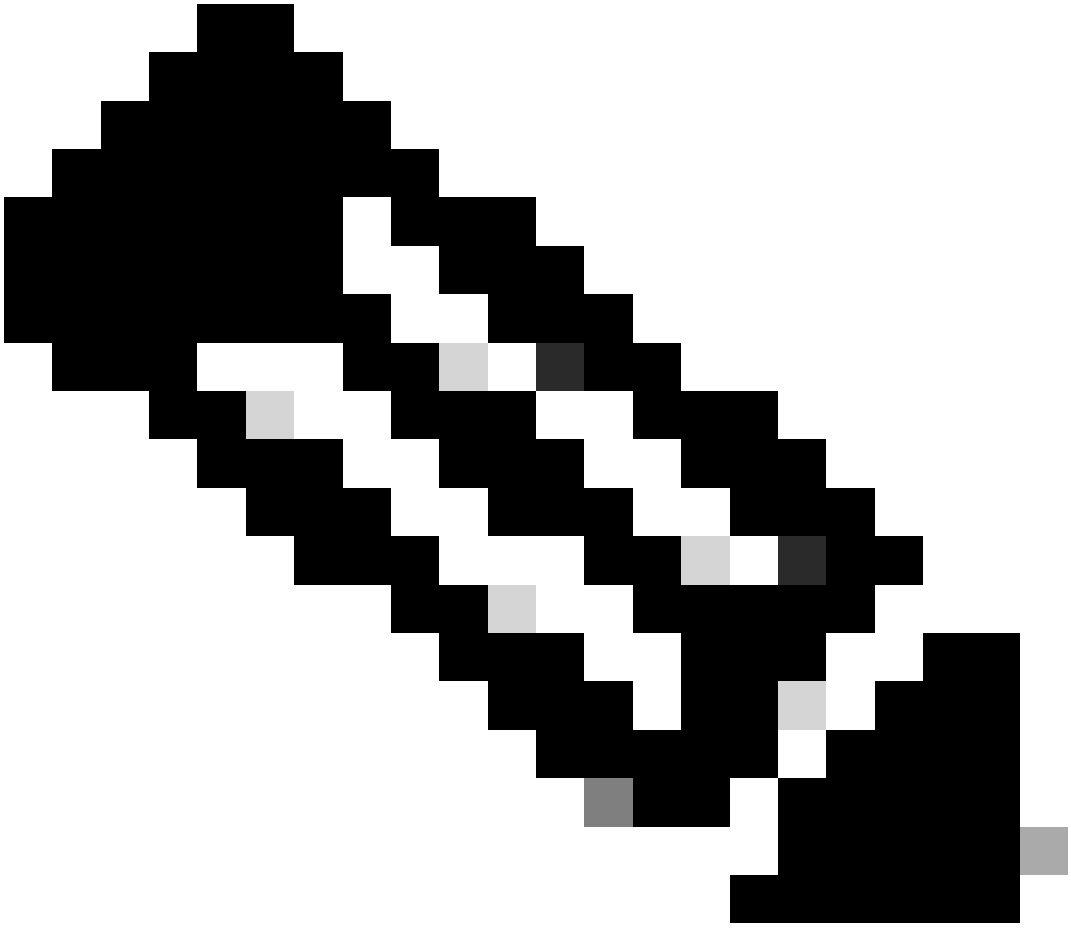
Couvert dans l'exemple précédent Totally Isolated

Apprentissage RT2 à distance (passerelle par défaut RT2)

Couvre les différences par rapport à Totally Isolated

Préfixe de passerelle par défaut CGW (leaf)

Vérifiez que le préfixe possède l'attribut approprié afin de pouvoir être installé dans le matériel



Remarque : ceci est essentiel au fonctionnement du relais L2 DHCP

<#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 1846
Paths: (1 available, best #1,

table evi_202

)

<-- the EVI context of 202 which matches the Vlan/EVI we are concerned about

  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              <-- Correct Segment ID

      Extended Community: RT:65001:202 ENCAP:8

EVPN DEF GW:0:0  <-- prefix has the Default GW attribute added

      Originator: 172.16.255.6, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Sep 7 2023 19:56:43 UTC
```

FED MATM (Leaf)

<#root>

```
F241.03.23-9300-Leaf01#

show platform software fed active matm macTable vlan 202 mac 0000.beef.cafe

VLAN   MAC                  Type  Seq#    EC_Bi  Flags  machandle           siHandle            riHandl
-------------------------------------------------------------------------------------------------------

202    0000.beef.cafe

  0x5000001       0      0     64  0x71e058da7858      0x71e05916c0d8      0x71e059171678      0x0

VTEP 172.16.254.6

 adj_id 651

No
<-- MAC of Default GW is installed in FED
```

SISF (CGW)

<#root>

```
CGW#

sh device-tracking database vlanid 202

vlanDB has 1 entries for vlan 202, 0 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol, DH4 - IPv4 DH
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                  Link Layer Address     Interface  vlan       prlvl      ag
S   10.1.202.1                             0000.beef.cafe         Twe1/0/1   202        0100       13
```

IOS MATM (CGW)

<#root>

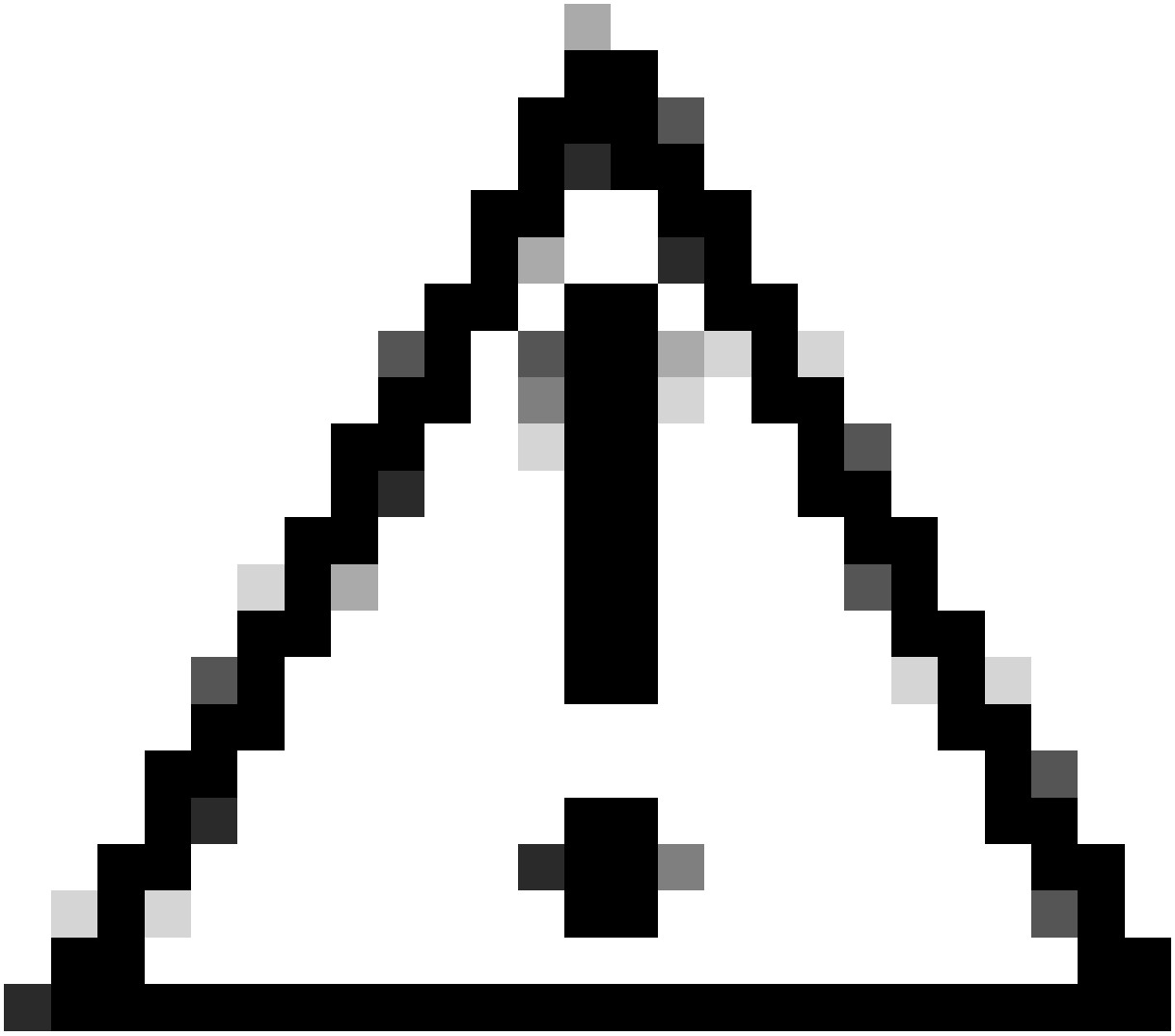
```
CGW#

show mac address-table address 0000.beef.cafe

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0000.beef.cafe    STATIC      Vl201

2021    0000.beef.cafe    STATIC      Vl2021   <-- The Vlan 2021 SVI MAC advertised out Tw1/0/1

 202    0000.beef.cafe    DYNAMIC     Twe1/0/1 <-- The Vlan 2021 SVI MAC learned dynamically after passi
```

Dépannage

Résolution d'adresse (ARP)

Étapes générales pour isoler les problèmes ARP

- Confirmer que le tunnel IMET est prêt
- Capture sur la liaison ascendante CGW pour vérifier le protocole ARP reçu encapsulé à partir du leaf
- Si aucun ARP n'est détecté, encapsulation sur la liaison ascendante
  - Vérifier que le tunnel IMET est prêt sur Leaf et CGW
  - Capture sur les liaisons ascendantes Leaf pour confirmer que le protocole ARP est encapsulé et envoyé
  - Dépannage du chemin intermédiaire
- Si ARP arrive sur la capture de tunnel IMET en limite mais n'est pas programmé dans la table ARP VRF
  - Dépanner le chemin de pontage CPU/CoPP pour confirmer le pontage ARP vers le CPU
  - Confirmez que l'adresse IP/les informations du client sont correctes
  - Déboguer ARP dans VRF pour voir ce qui pourrait avoir un impact sur le processus ARP
- Vérifiez que l'adresse MAC CGW est installée comme adresse MAC de tronçon suivant/dest sur les hôtes
- Confirmez que CGW possède les deux entrées ARP avec les adresses MAC réelles de l'hôte
- Vérifier que la stratégie de pare-feu autorise ce type de trafic



Attention : soyez prudent lorsque vous activez les débogages !

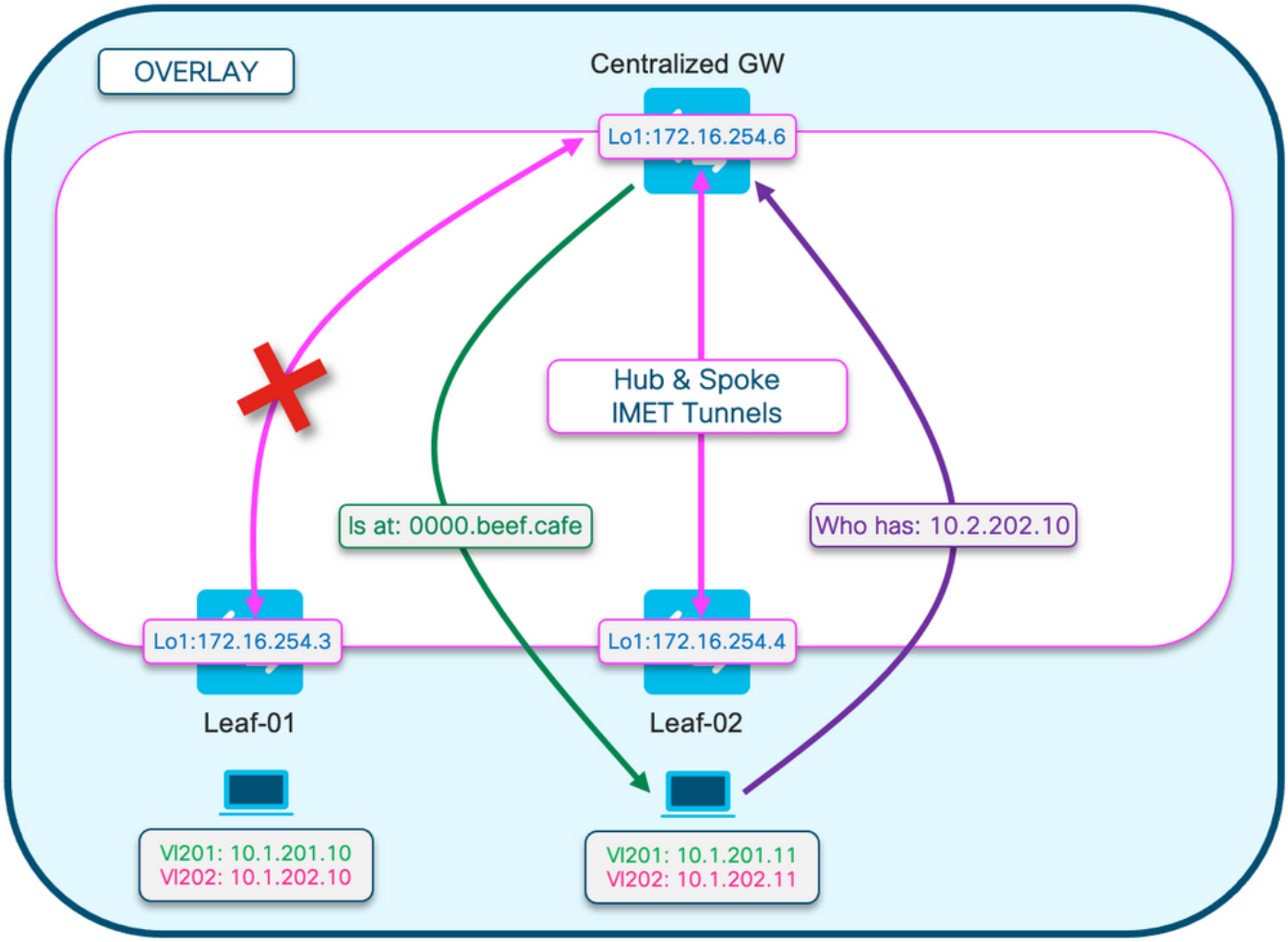
Assurez-vous d'avoir désactivé la suppression des inondations

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

 flooding-suppression address-resolution disable <-- This CLI prevents a VTEP from trying to unicast oth
```

Lorsque l’hôte de la couche Leaf-02 résout le protocole ARP pour l’hôte de la couche Leaf-01, la requête ARP n’est pas diffusée directement à la couche Leaf-01

- Le protocole ARP est transmis au seul tunnel BUM programmé sur Leaf-02 vers le CGW
- La CGW ne transmet pas ce message à Leaf-01, mais répond avec son propre MAC
- Toutes les communications sont alors transmises au CGW, puis acheminées vers entre les hôtes
- CGW achemine les paquets, même s'ils se trouvent sur le même sous-réseau local



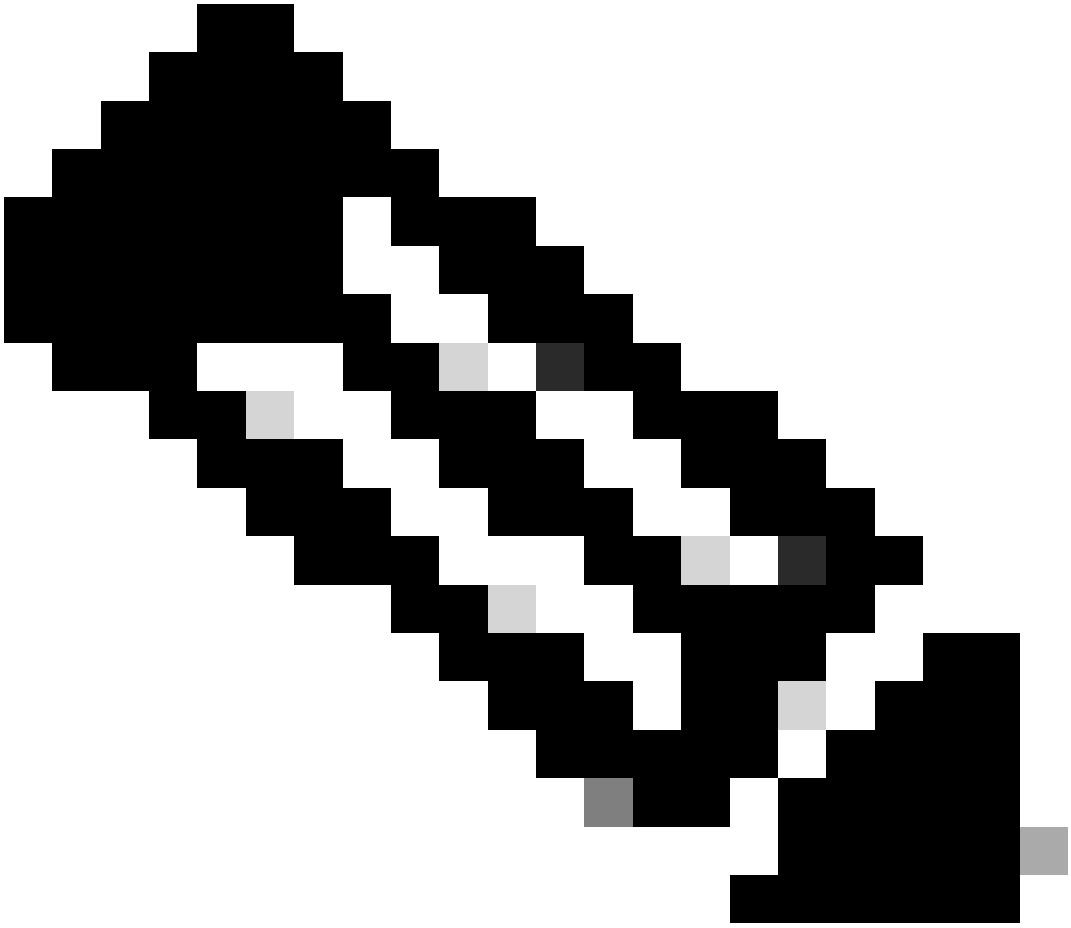
Ce schéma permet de visualiser le flux du processus de résolution ARP décrit dans cette section.

La requête ARP est affichée en violet

- Cette requête ARP a pour but de résoudre l'adresse MAC de l'hôte 10.1.202.10 de Leaf-01
- Notez que la ligne violette se termine à la CGW et n'atteint pas Leaf-01

La réponse ARP s'affiche en vert

- La réponse contient l'adresse MAC de la SVI CGW pour VLAN 202
- Notez que la ligne verte provient du CGW et non de l'hôte réel



Remarque : le X rouge indique que cette communication n'impliquait pas l'envoi de trafic vers Leaf-01.

Observez les entrées ARP sur chaque hôte respectif

<#root>

```
Leaf02-HOST#

sh ip arp 10.1.202.10

Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.202.10             1

0000.beef.cafe

  ARPA   Vlan202

<-- MAC address for Leaf01 host is CGW MAC


Leaf01-HOST#
```

sh ip arp 10.1.202.11

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.1.202.11             7
```

0000.beef.cafe

```
  ARPA   Vlan202
```

<-- MAC address for Leaf02 host is CGW MAC

Observez sur CGW que les préfixes RT2 sont appris. Cela est nécessaire pour que le CGW achemine les paquets

<#root>

CGW#

sh bgp l2vpn evpn route-type 2 0 0006.f617.eec4 * <-- Leaf02 actual MAC

BGP routing table entry for [2][172.16.254.6:202][0][48][0006F617EEC4][0][*]/20, version 235458
Paths: (1 available, best #1,

table evi_202

)
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.4:202][0][48][0006F617EEC4][0][*]/20 (global)
    172.16.254.4 (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 <-- correct segment identifier

      Extended Community: RT:65001:202 ENCAP:8

EVPN E-Tree:flag:1

,label:0

<-- prefix contains the Leaf flag indicating this is a normal host

      Originator: 172.16.255.4, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 9 2025 17:11:22 UTC

CGW#

sh bgp l2vpn evpn route-type 2 0 0006.f601.cd44 * <-- Leaf01 actual MAC

BGP routing table entry for [2][172.16.254.6:202][0][48][0006F601CD44][0][*]/20, version 235521
Paths: (1 available, best #1,

table evi_202)

  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.3:202][0][48][0006F601CD44][0][*]/20 (global)
    172.16.254.3 (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                          <-- correct segment identifier

      Extended Community: RT:65001:202 ENCAP:8

EVPN E-Tree:flag:1

,label:0

<-- prefix contains the Leaf flag indicating this is a normal host


      Originator: 172.16.255.3, Cluster list: 172.16.255.1
      rx pathid: 0, tx pathid: 0x0
      Updated on Apr 9 2025 17:17:06 UTC
```

Capturez l'échange ARP sur les liaisons ascendantes pour confirmer la communication bidirectionnelle

- Vous pouvez utiliser Embedded Packet Capture (EPC) sur les liaisons ascendantes du fabric
- Ce scénario montre EPC sur la liaison ascendante Leaf01. Répétez cette procédure sur CGW si nécessaire

Configuration de l'EPC

```
<#root>

Leaf01#

monitor capture 1 interface range te 1/1/2 , te 1/1/4 both match any buffer size 100


<-- both Uplinks toward fabric included
```

Démarrer la capture

```
<#root>

Leaf01#

monitor capture 1 start
```

Lancez la commande ping pour déclencher la requête ARP (dans ce cas, la commande ping va de l’hôte Leaf01 10.1.201.10 à l’hôte Leaf02 10.1.201.11)

```
<#root>

Leaf01-HOST#
```

```
ping vrf red 10.1.201.11


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.201.11, timeout is 2 seconds:
...!!
Success rate is 40 percent (2/5), round-trip min/avg/max = 1/1/1 ms
```

Arrêter la capture et vérifier la présence des trames ARP

```
<#root>

Leaf01#

mon cap 1 stop


F241.03.23-9300-Leaf01#

show mon cap 1 buff br | i ARP


11

 8.153510 00:06:f6:01:cd:42 -> ff:ff:ff:ff:ff:ff ARP 110

Who has 10.1.201.11? Tell 10.1.201.10  <-- .10 requests .11 MAC (this is Frame 11)


12 8.154030 00:00:be:ef:ca:fe -> 00:06:f6:01:cd:42 ARP 110 10.1.201.11

is at 00:00:be:ef:ca:fe    <-- CGW replies with its MAC
```

Affichez les paquets de capture en détail. Pour plus d'informations sur les paquets, utilisez l'option detail de EPC

- Sachez que cette sortie est découpée à différents endroits pour plus de concision

```
<#root>

Leaf01#

show mon cap 1 buffer detailed | beg Frame 11   <-- begin detail result from Frame 11 (ARP Request)

Frame 11: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_t

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

    Destination: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
```

```
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.16.254.3, Dst: 172.16.254.6     <--- Outer tunnel IP header

    Source: 172.16.254.3
    Destination: 172.16.254.6
User Datagram Protocol, Src Port: 65483,

Dst Port: 4789  <-- VXLAN Dest port


Virtual eXtensible Local Area Network
    VXLAN Network Identifier

(VNI): 20101               <-- Verify the VNI for the segment you are investigating

    Reserved: 0

Ethernet II, Src: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)  <--



  Type: ARP (0x0806)

    Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (

request

)

 <-- is an ARP request


    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)


Sender MAC address: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42)   <-- Sending host
    Sender IP address: 10.1.201.10
    Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)   <-- Trying to resolve MAC for host
    Target IP address: 10.1.201.11



Frame 12:

 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, i

<-- ARP reply


Ethernet II,

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

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

Dst: 68:2c:7b:f8:87:48

 (68:2c:7b:f8:87:48)

<-- Underlay MACs
```

```
Internet Protocol Version 4, Src: 172.16.254.6, Dst: 172.16.254.3

User Datagram Protocol, Src Port: 65410, Dst Port: 4789
Virtual eXtensible Local Area Network
    VXLAN Network Identifier (VNI): 20101
    Reserved: 0
Ethernet II,

Src: 00:00:be:ef:ca:fe

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

Dst: 00:06:f6:01:cd:42

 (00:06:f6:01:cd:42)

 <-- Start of payload



 Type: ARP

 (0x0806)
    Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (

reply

)

<-- is an ARP reply


    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)


 Sender MAC address: 00:00:be:ef:ca:fe (00:00:be:ef:ca:fe)   <-- Reply is that of the CGW MAC due to loc

    Sender IP address: 10.1.201.11
    Target MAC address: 00:06:f6:01:cd:42 (00:06:f6:01:cd:42)
    Target IP address: 10.1.201.10
```

Préfixe de passerelle CGW RT2

Préfixe de passerelle manquant

Comme indiqué dans la section précédente sur les segments partiellement isolés, l'adresse MAC doit être apprise dans le VLAN de fabric

- Ce problème peut se manifester s'il n'y a aucun trafic destiné à la passerelle pendant plus longtemps que le compteur d'obsolescence MAC.
- Si le préfixe de passerelle CGW est manquant, vous devez confirmer la présence de l'adresse MAC

<#root>

```
CGW#

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

% Network not in table <-- RT2 not generated on CGW


CGW#

show mac address-table address 0000.beef.cafe

          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0000.beef.cafe    STATIC      Vl201
2021    0000.beef.cafe    STATIC      Vl2021

<-- MAC is not learned in Fabric Vlan 202

Total Mac Addresses for this criterion: 2
```

Correction manquante du préfixe de passerelle

Dans la plupart des réseaux de production, il y a probablement du trafic en permanence. Toutefois, si vous rencontrez ce problème, vous pouvez utiliser l'une des options suivantes pour le résoudre :

- Ajoutez une entrée MAC statique telle que « mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1 »
- Augmentez le compteur d'obsolescence MAC avec « mac address-table aging-time <seconds> ». (Gardez à l'esprit que cela augmente le temps de vieillissement pour toutes les adresses MAC, de sorte que l'option MAC statique est préférée)

Attribut DEF GW manquant

Avec les segments partiellement isolés, il existe un certain nombre de configurations supplémentaires pour ajouter cet attribut.

Correction d'attribut DEF GW manquant

Confirmez ces détails :

- Vous exécutez 17.12.1 ou une version ultérieure
- L'interface de ligne de commande SISF (Device-Tracking) est présente dans la configuration
- Les commandes route-map match & set sont configurées et route-map est appliquée aux voisins BGP
- Vous avez actualisé les annonces BGP (vous devez effacer BGP pour annoncer à nouveau le préfixe avec le nouvel attribut

Itinérance sans fil

L'itinérance fréquente peut entraîner une mise à jour trop fréquente de BGP et l'itinérance par intervalle de temps doit être augmentée avant que le commutateur ne déclare qu'il possède l'adresse MAC et envoie la mise à jour RT2

- Cela se produit lorsqu'un hôte se déplace entre deux points d'accès situés sur des commutateurs différents.
- La limite par défaut pour l'itinérance est de 5 par 180 secondes

<#root>

```
Leaf01#

sh run | sec l2vpn

l2vpn evpn
 replication-type static
 flooding-suppression address-resolution disable

 ip duplication limit 10 time 180          <--- You can adjust this default in the global l2vpn sectior
 mac duplication limit 10 time 180


Leaf01#

sh l2vpn evpn summary

L2VPN EVPN
  EVPN Instances (excluding point-to-point): 4
    VLAN Based:   4
  Vlans: 4
  BGP: ASN 65001, address-family l2vpn evpn configured
  Router ID: 172.16.254.3
  Global Replication Type: Static
  ARP/ND Flooding Suppression: Disabled
  Connectivity to Core: UP

  MAC Duplication: seconds 180 limit 10

  MAC Addresses: 13
    Local:     6
    Remote:    7

    Duplicate: 0
  IP Duplication: seconds 180 limit 10

  IP Addresses: 7
    Local:     4
    Remote:    3

    Duplicate: 0

<...snip...>
```

Commandes à collecter pour le TAC

Si ce guide n'a pas résolu votre problème, collectez la liste de commandes affichée et joignez-la à votre demande de service TAC.

Informations minimales à collecter

(temps limité de collecte des données avant l'action de rechargement/récupération)

- Afficher les evpn techniques
- Montrez la technologie
- Show tech sisf

Informations détaillées à collecter

(Si vous avez le temps de recueillir des données plus complètes, il est préférable de le faire)

- show tech
- show tech evpn
- show tech platform evpn_vxlan switch <numéro>
- show tech platform
- show tech resource
- show tech sisf
- show tech isis
- show tech bgp
- show monitor event-trace evpn event all
- show monitor event-trace evpn error all
- request platform software trace archive

Informations connexes

- Implémenter la politique de routage EVPN BGP sur les commutateurs de la gamme Catalyst 9000
- Relais DHCP de couche 2 (disponible prochainement)

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.