Implemente la segmentación de superposición protegida BGP EVPN en los switches Catalyst serie 9000

Contenido

Introducción

Este documento describe cómo implementar BGP EVPN VXLAN Protected Overlay Segmentation en Catalyst 9000 Series Switches.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conceptos de BGP EVPN VxLAN
- Troubleshooting de BGP EVPN Unicast
- política de ruteo BGP EVPN VxLAN

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 y versiones posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Descripción de características de alto nivel

La función de segmento protegido es una medida de seguridad que impide que los puertos se

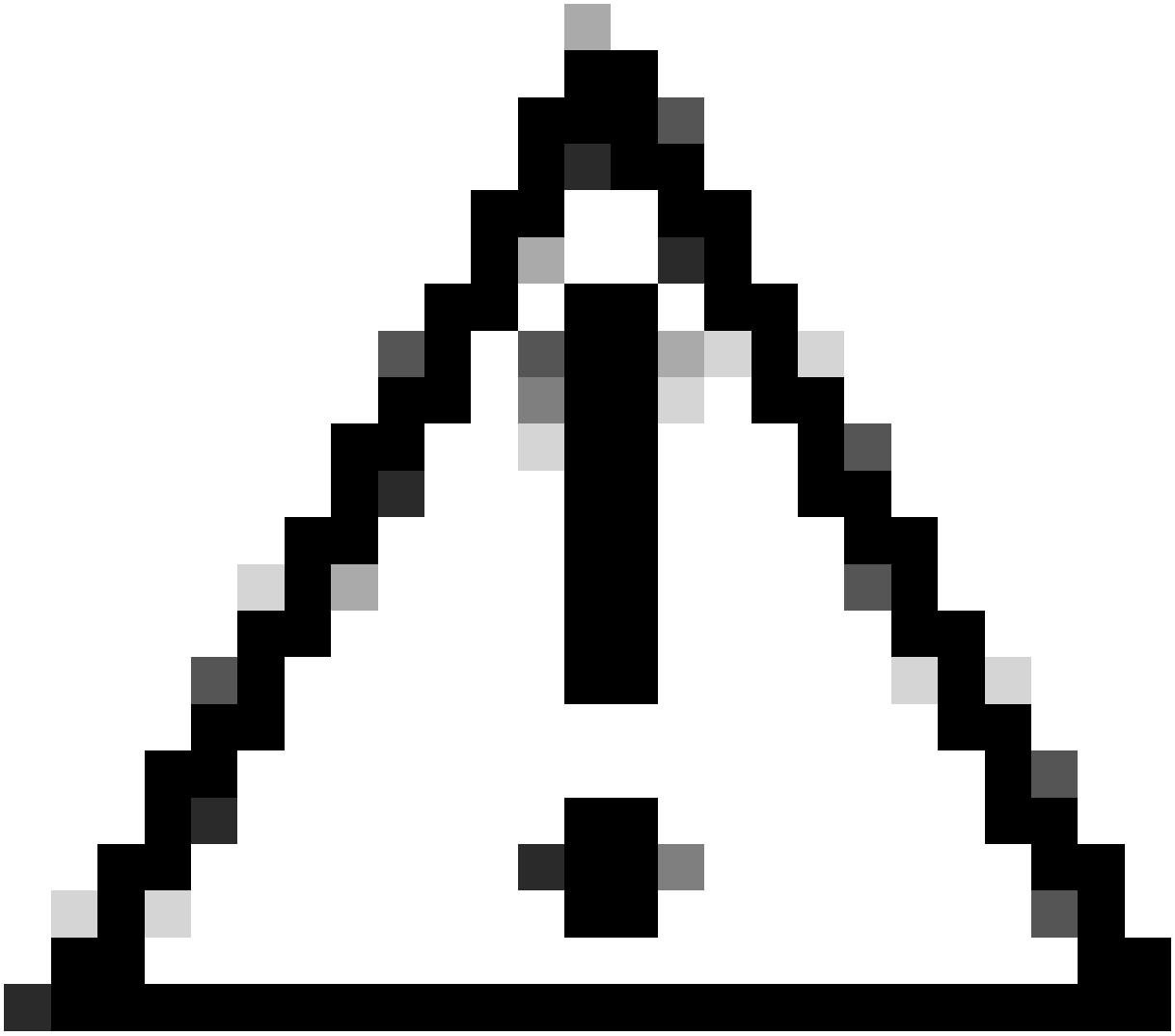
reenvíen tráfico entre sí, incluso si se encuentran en la misma VLAN y el mismo switch

- Esta función es similar a las VLAN 'switchport protected' o privadas, pero para fabrics EVPN.
- Este diseño fuerza todo el tráfico al CGW, donde un firewall puede inspeccionarlo antes de enviarlo a su destino final.
- Los flujos de tráfico son controlados, previsibles y fáciles de inspeccionar mediante un dispositivo de seguridad centralizado.

Detalles del documento

Este documento es parte 2 o 3 documentos interrelacionados:

- Documento 1: Implementación de la Política de Ruteo BGP EVPN en los Catalyst 9000 Series Switches cubre cómo controlar el tráfico BGP BUM en la superposición, y debe configurarse primero
- Documento 2: Este documento. A partir del diseño y la política de superposición del documento 1, este documento describe la implementación de la palabra clave 'protected'
- Documento 3:Implementación de Retransmisión DHCP de Capa 2 de BGP EVPN en Switches Catalyst de la Serie 9000 cubre cómo funciona el relé DHCP en un VTEP solo de L2



Precaución: debe implementar la configuración del documento 1 antes de implementar configuraciones de segmentos protegidos.

Tipos de segmentos protegidos

Totalmente aislado

- Permite únicamente la comunicación de norte a sur y
- La puerta de enlace se anuncia en el fabric con la CLI 'default-gateway advertise'

Principalmente aislado

- Permite la comunicación de norte a sur (en este caso de uso, se permiten los flujos de tráfico de este y oeste en función de las políticas de tráfico del firewall).
- Permite la comunicación de Este a Oeste (basada en las políticas de tráfico del firewall)
- La puerta de enlace es externa al fabric y la SVI no se anuncia mediante la CLI 'default-

gateway advertise'

Comportamiento del switch

- Los hosts no pueden comunicarse entre sí directamente aunque estén conectados al mismo switch (solicitud ARP no enviada a otros puertos en el mismo switch cuando los hosts están en el mismo VRF/Vlan/Segmento)
- Sin tráfico BUM entre VTEP L2 (prefijos IMET filtrados mediante la configuración de política de routing)
- Todos los paquetes de los hosts se retransmiten a Border Leaf para ser reenviados. (Esto significa que para que el Host 1 se comunique con el Host 2 en la misma hoja, el tráfico está anclado al CGW)

Manejo de Tipo de Ruta 2

- Las hojas de acceso anuncian RT2 local con la Comunidad ampliada del árbol E y el indicador de hoja configurado
- Los Hojas de acceso no instalan ningún RT2 remoto recibido con la Comunidad ampliada de árbol E y el indicador de hoja establecidos en el plano de datos
- Las hojas de acceso no se instalan mutuamente RT2 en el plano de datos
- Access Leafs y Border Leaf (CGW) se instalan mutuamente RT2 en el plano de datos
- No se requiere ningún cambio de configuración en Access Leaf o Border Leaf.

Resumen del diseño

- Para broadcast (BUM) la topología RT3 es hub y spoke para forzar el tráfico de broadcast como ARP hasta el GCW.
- Para tener en cuenta la movilidad del host, los RT2 son de malla completa en el plano de control BGP (cuando un host se mueve de un VTEP a otro, el número de secuencia aumenta en el RT2)
- El plano de datos instala direcciones MAC de forma selectiva.
  - Una hoja instala solamente MACs locales y RT2 que contienen el atributo DEF GW
  - El CGW no tiene el KW protegido e instala todos los MAC locales y RT2 remotos en su plano de datos.

Terminology

VRF	Reenvío de routing virtual	Define un dominio de routing de capa 3 que se puede separar de otro VRF y de un dominio de routing IPv4/IPv6 global
AF	Familia de direcciones	Define qué prefijos de tipo y manejos BGP de información de ruteo
AS	Sistema	Conjunto de prefijos IP enrutables de Internet que pertenecen a una red o

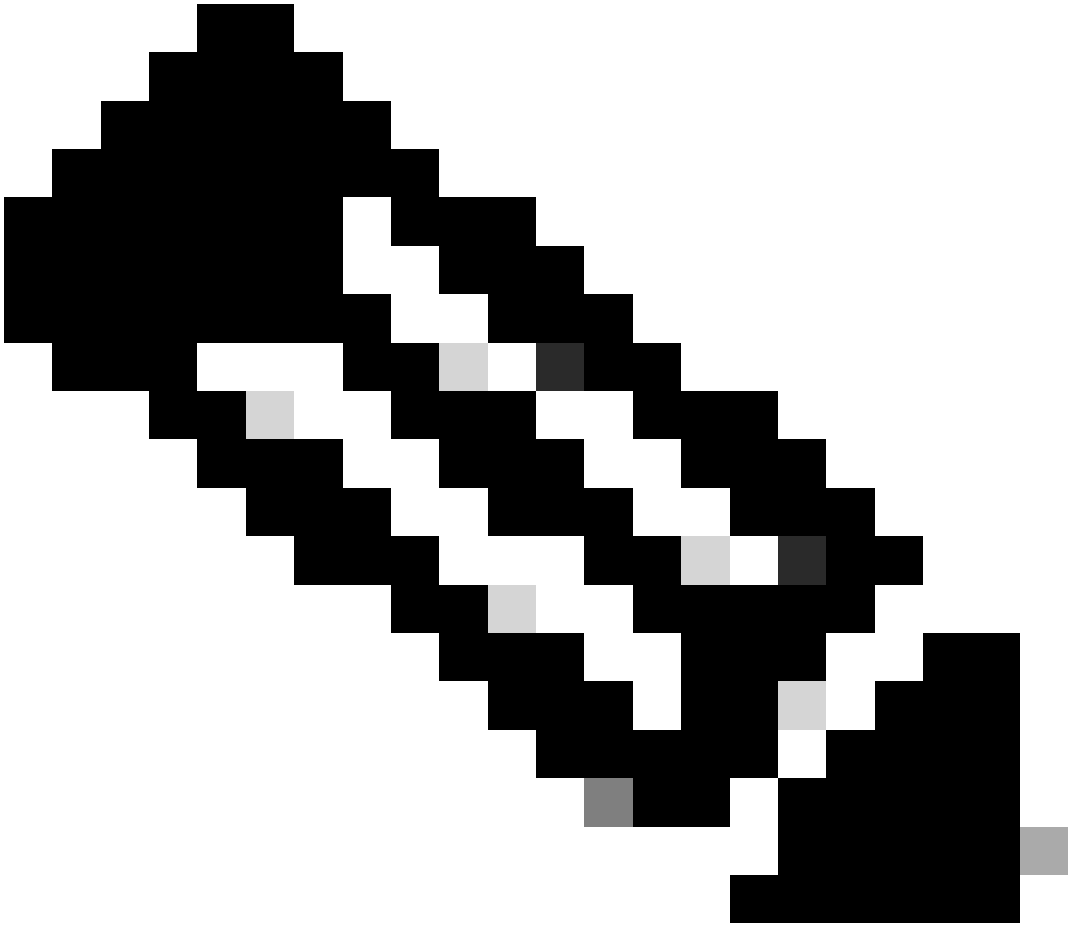
	autónomo	a un conjunto de redes administradas, controladas y supervisadas por una sola entidad u organización
EVPN	Red privada virtual Ethernet	La extensión que permite que BGP transporte la información de IP de Capa 2 MAC y Capa 3 es EVPN y utiliza Multi-Protocol Border Gateway Protocol (MP-BGP) como protocolo para distribuir la información de alcance que pertenece a la red superpuesta VXLAN.
VXLAN	LAN extensible virtual (red de área local)	VXLAN está diseñado para superar las limitaciones inherentes de las VLAN y el STP. Se propone un estándar IETF [RFC 7348] para proporcionar los mismos servicios de red Ethernet de capa 2 que las VLAN, pero con mayor flexibilidad. Funcionalmente, es un protocolo de encapsulación MAC-in-UDP que se ejecuta como una superposición virtual en una red subyacente de Capa 3.
CGW	Gateway centralizado	Implementación de EVPN donde la SVI del gateway no está en cada hoja. En su lugar, todo el ruteo se realiza mediante una hoja específica que utiliza IRB asimétrico (Ruteo y Bridging Integrados)
GW DEF	Gateway predeterminado	Atributo de comunidad ampliada BGP agregado al prefijo MAC/IP mediante el comando "default-gateway advertise enable" en la sección de configuración 'l2vpn evpn'.
IMET (RT3)	Etiqueta Ethernet Multicast Inclusiva (Route)	También se denomina ruta BGP de tipo 3. Este tipo de ruta se utiliza en EVPN para entregar el tráfico BUM (difusión/unidifusión desconocida/multidifusión) entre VTEP.
RT2	Tipo de ruta 2	Prefijo BGP MAC o MAC/IP que representa un MAC de host o MAC-IP de gateway
Gestor de EVPN	Administrador de EVPN	Componente de administración central para varios otros componentes (ejemplo: aprende de SISF y envía señales a L2RIB)
SISF	Función de seguridad integrada en el switch	Una tabla de seguimiento de host agnóstico que es utilizada por EVPN para aprender qué hosts locales están presentes en una hoja

L2RIB	Base de información de routing de capa 2	En componente intermedio para la administración de interacciones entre BGP, EVPN Mgr y L2FIB
FED	Controlador de motor de reenvío	Programas para la capa ASIC (hardware)
MATM	Administrador de tabla de direcciones MAC	IOS MATM: tabla de software que instala sólo direcciones locales y FED MATM: tabla de hardware que instala las direcciones locales y remotas aprendidas del plano de control, y es parte del plano de reenvío de hardware

Diagramas de flujo

Diagrama Route-Type 2 (RT2)

Este diagrama muestra el diseño de malla completo de los prefijos de host MAC/MAC-IP de tipo 2.



Nota: se requiere una malla completa para admitir movilidad y roaming

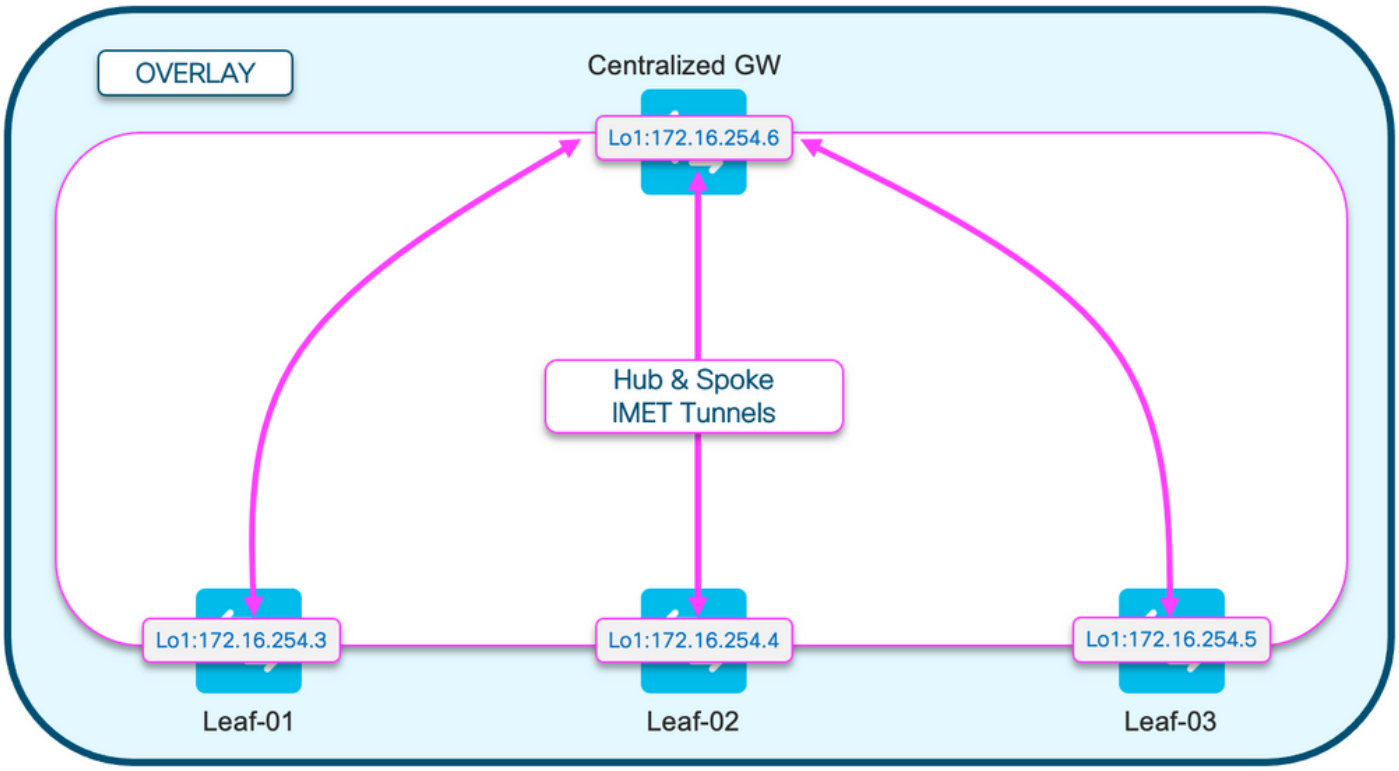
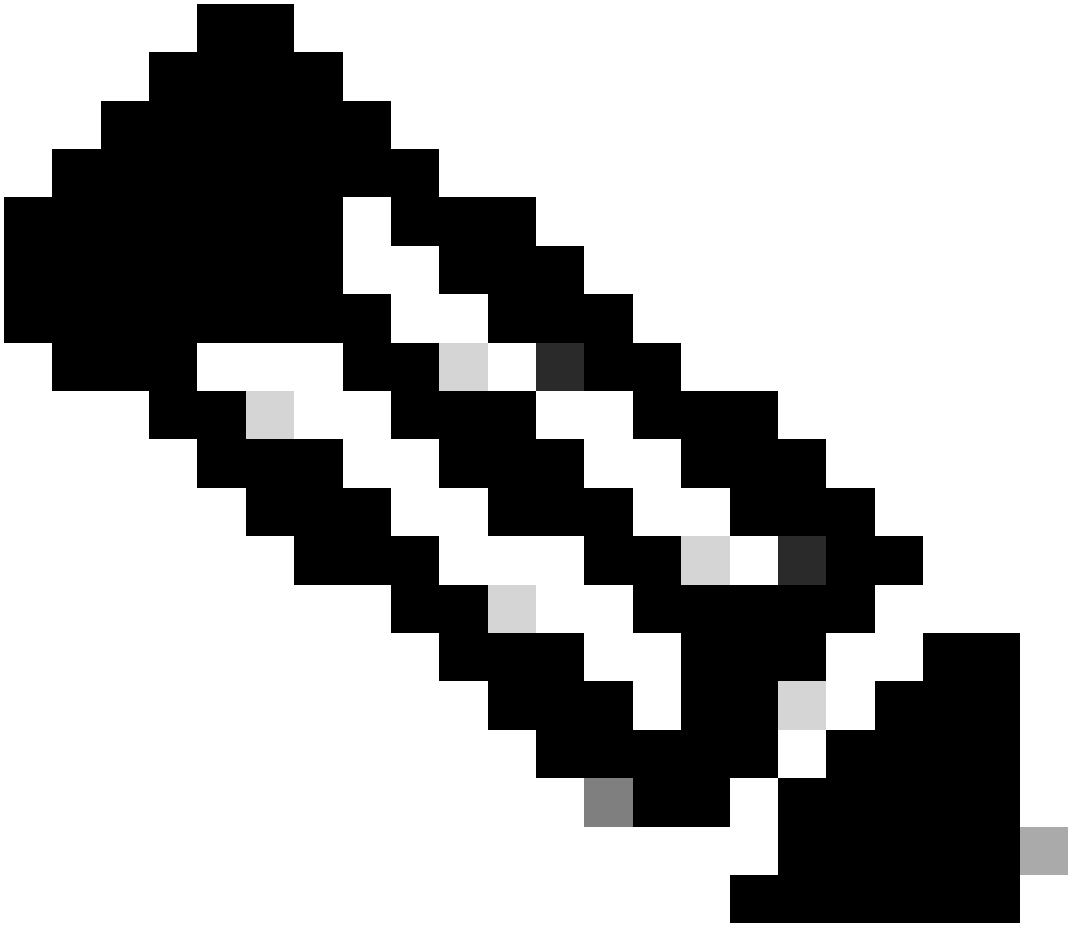


Diagrama Route-Type 3 (RT3)

Este diagrama muestra el diseño radial de los túneles de difusión IMET (RT3)



Nota: se requiere la difusión radial para evitar que los folletos con el mismo segmento se envíen difusión entre sí directamente.

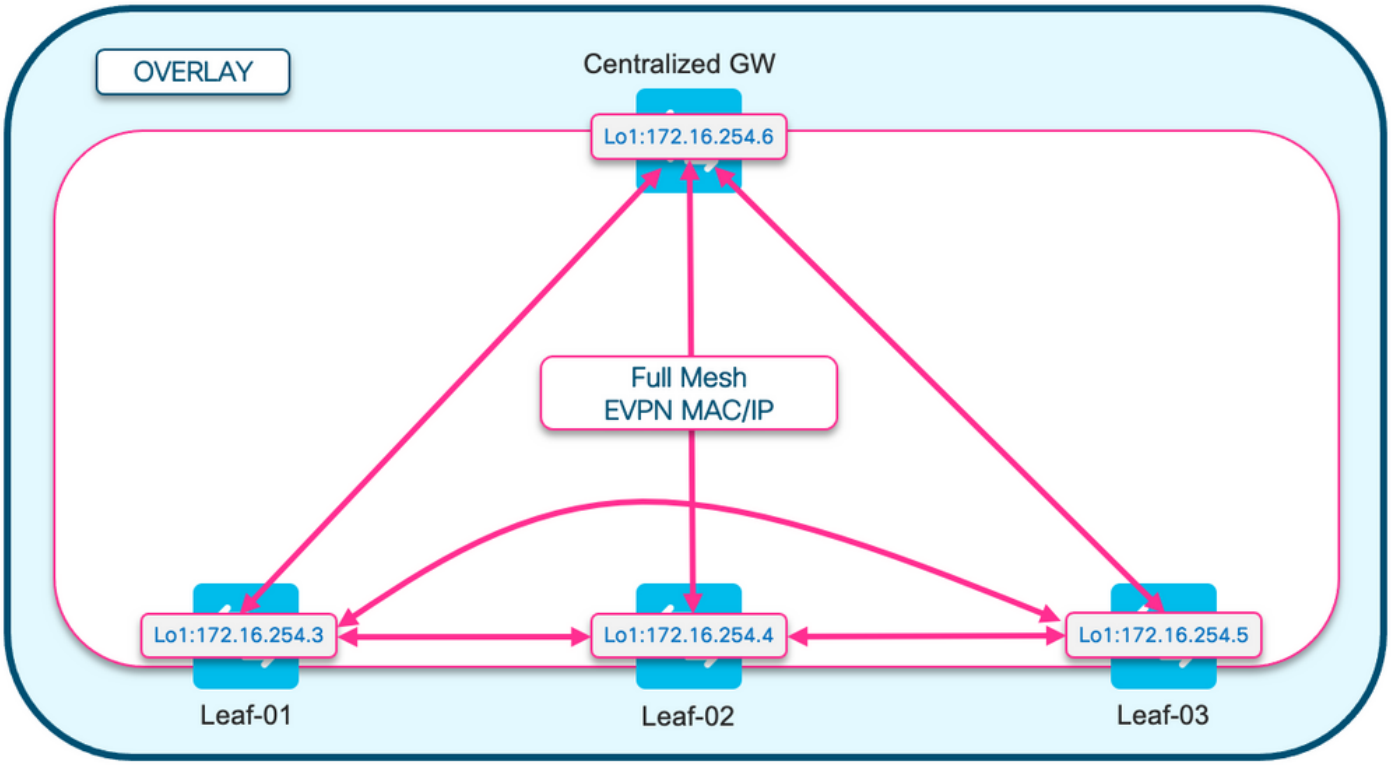
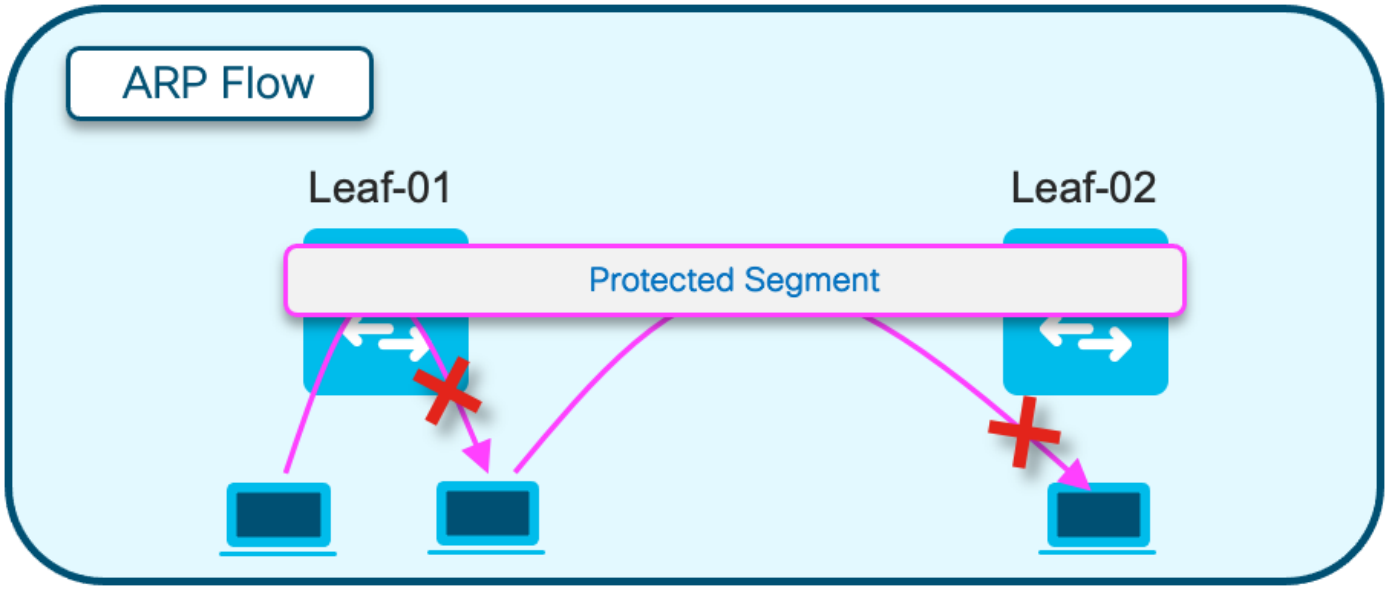
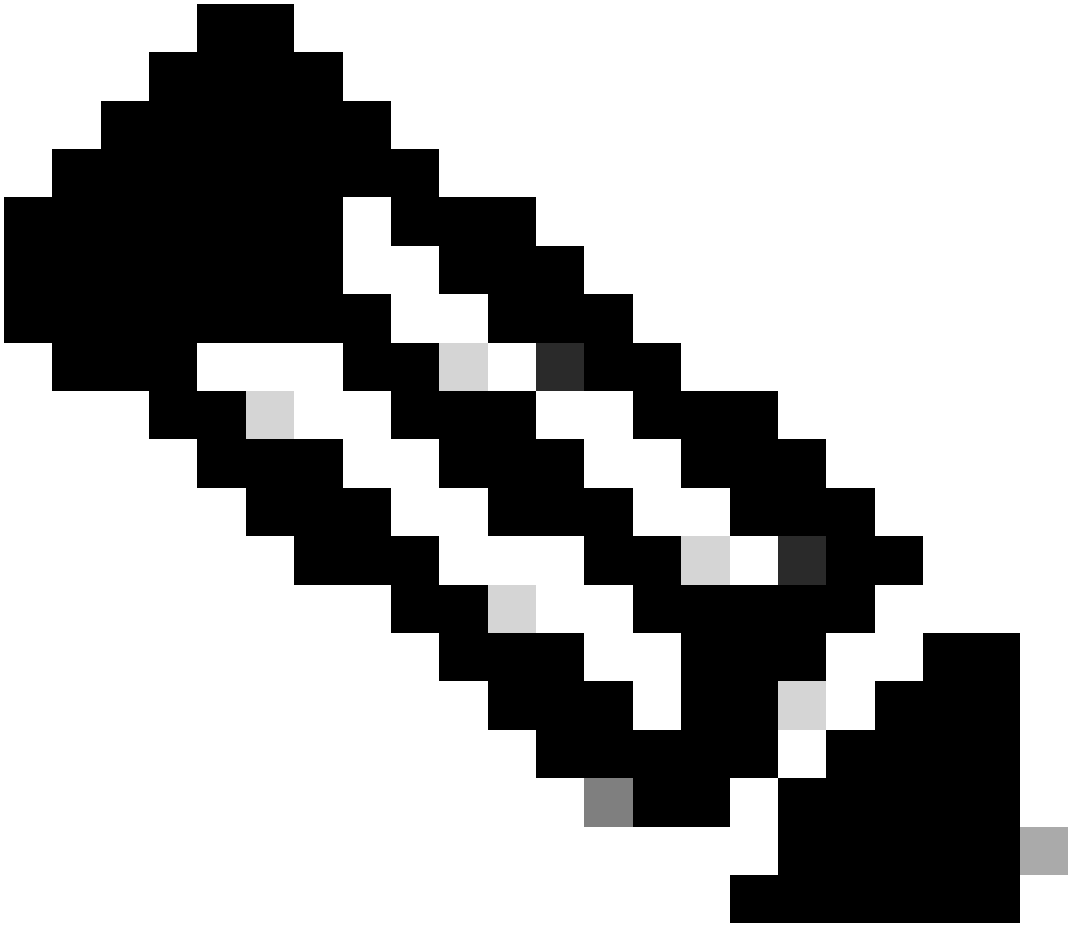


Diagrama de resolución de direcciones (ARP)

Este diagrama demuestra que ARP no puede alcanzar ningún host en el mismo segmento EPVN. Cuando el host ARPs para otro host, sólo el CGW obtiene este ARP y responde



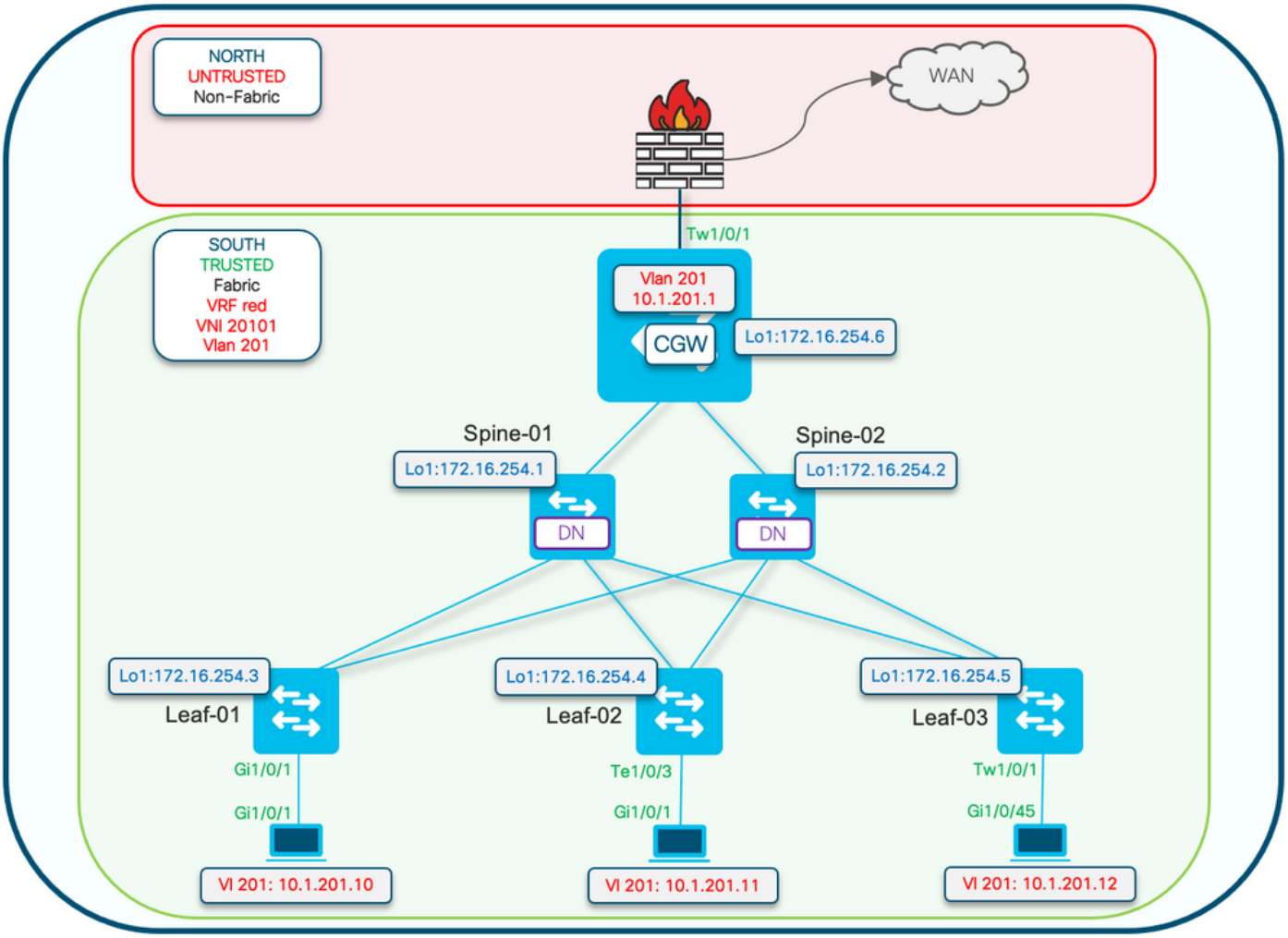


Nota: Este cambio de comportamiento ARP es instanciado por el uso de la palabra clave 'protected'.

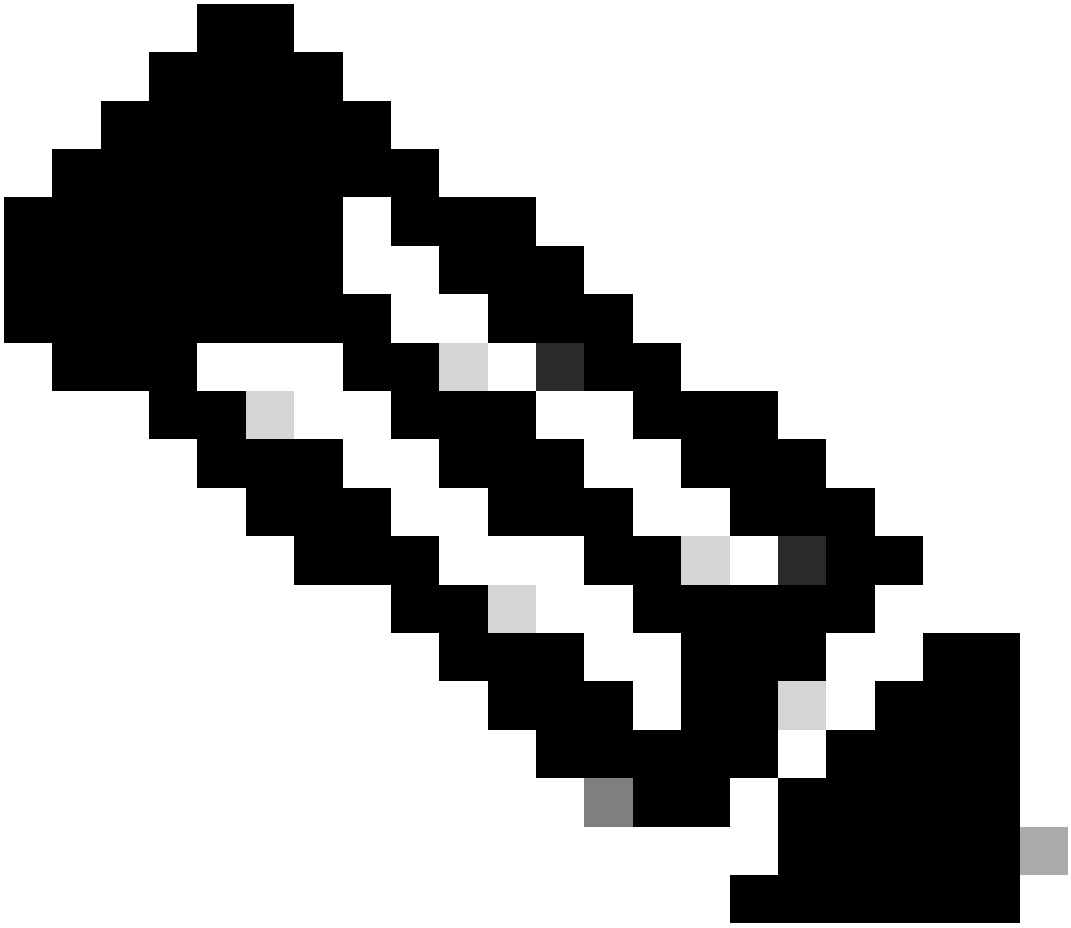
Ejemplo: miembro evpn-instance 202 vni 20201 protected

Configurar (Totalmente aislado)

Diagrama de la red



La palabra clave Protected configuration se aplica en los switches Leaf. El CGW es un dispositivo promiscuo e instala todas las direcciones MAC.



Nota: La lista de comunidad de política de ruteo y la configuración de route-map que controla la importación/exportación de prefijos IMET se muestra en Implementación de la Política de Ruteo EVPN BGP en los Catalyst 9000 Series Switches. En este documento sólo se muestran las diferencias de segmentos protegidos.

Leaf-01 (configuración de EVPN 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 (configuración básica)

<#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
```

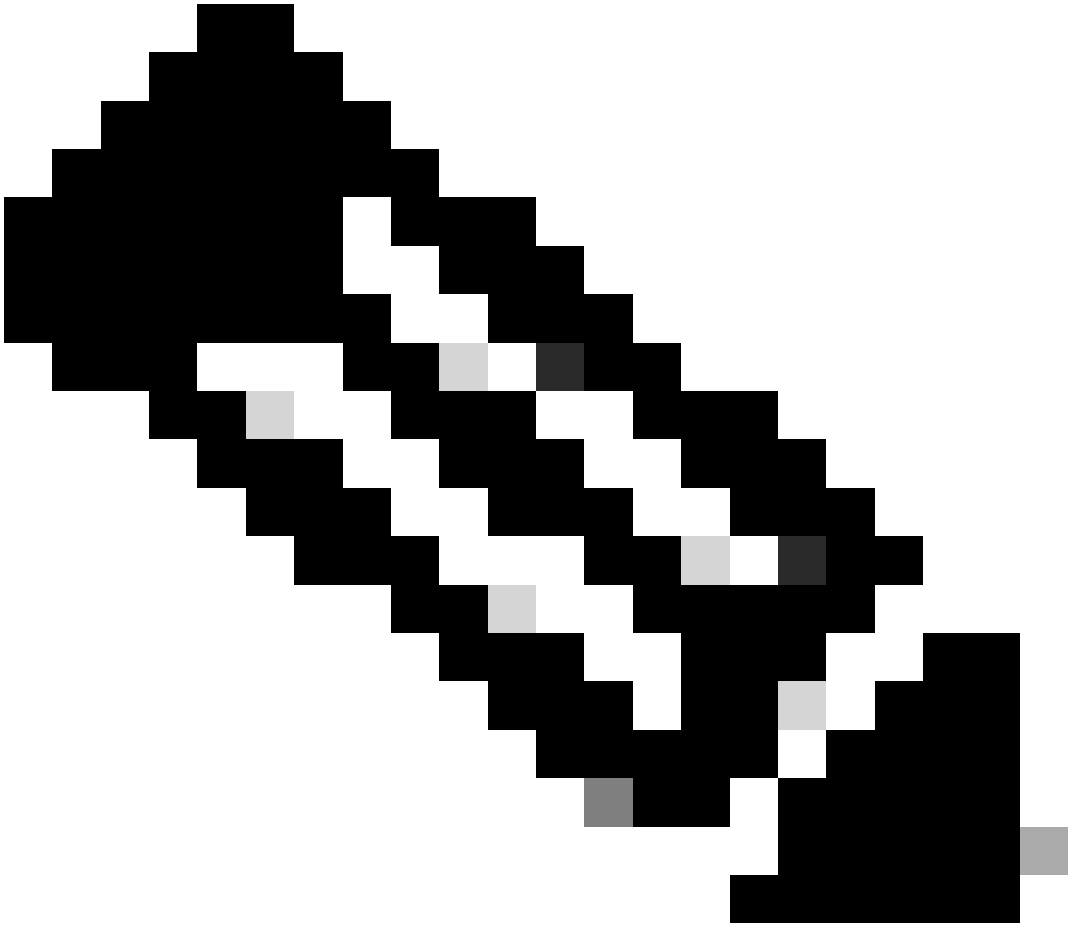
<#root>

```
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
```



Nota: En el CGW no se aplica ninguna política BGP. El CGW puede recibir y enviar todos los tipos de prefijo (RT2, RT5 / RT3).

Verificar (totalmente aislado)

Detalles de EVI

<#root>

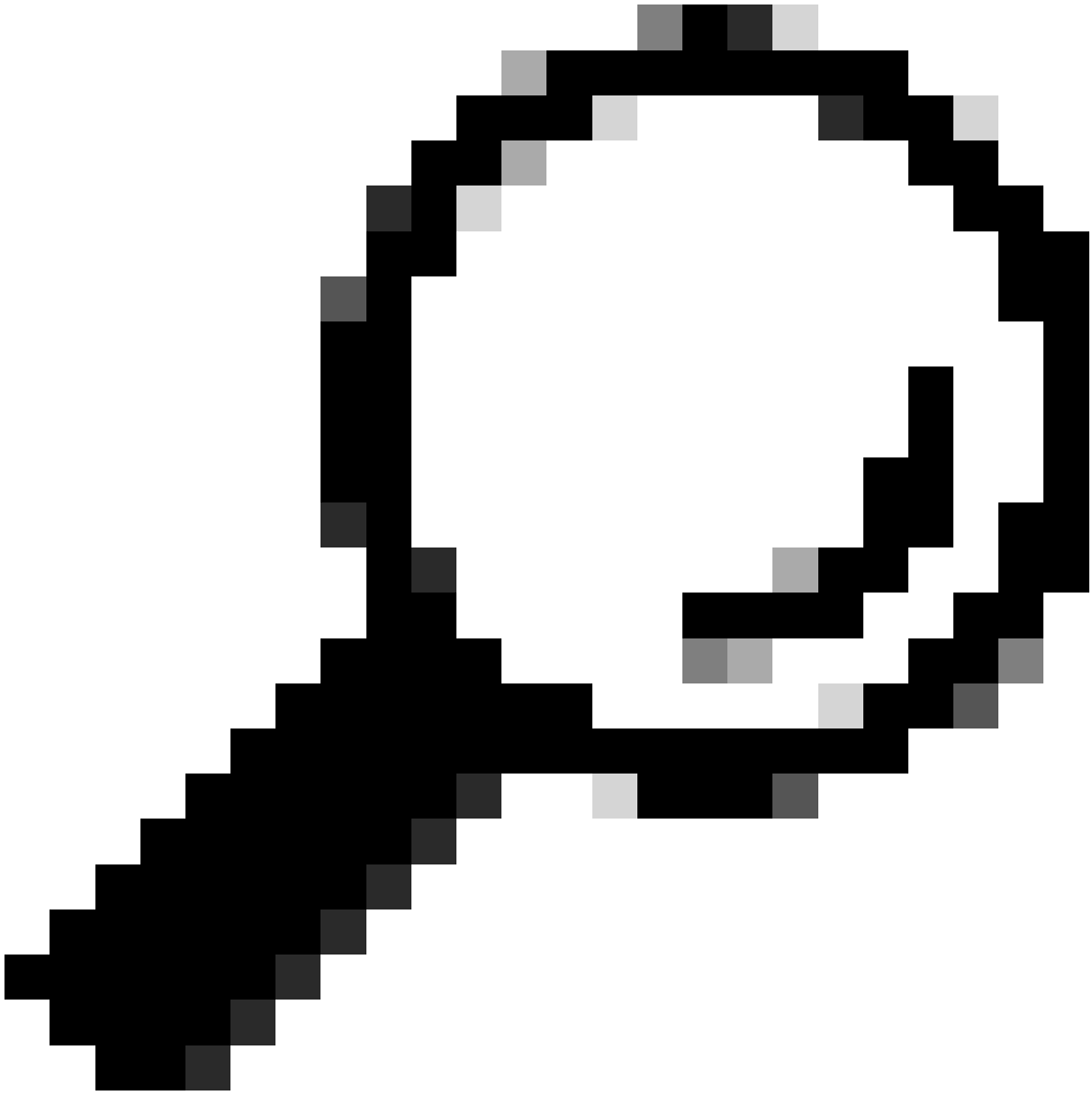
```
Leaf01#

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...>
```

Generación de RT2 local (host local a RT2)

Verifique la cadena de dependencia de componentes desde el aprendizaje del host local hasta la generación RT2:

- SISF (Mientras que la hoja no tiene una SVI, SISF todavía obtiene la información del host a través de la trama ARP del host)
- Gestor de EVPN
- L2RIB
- BGP

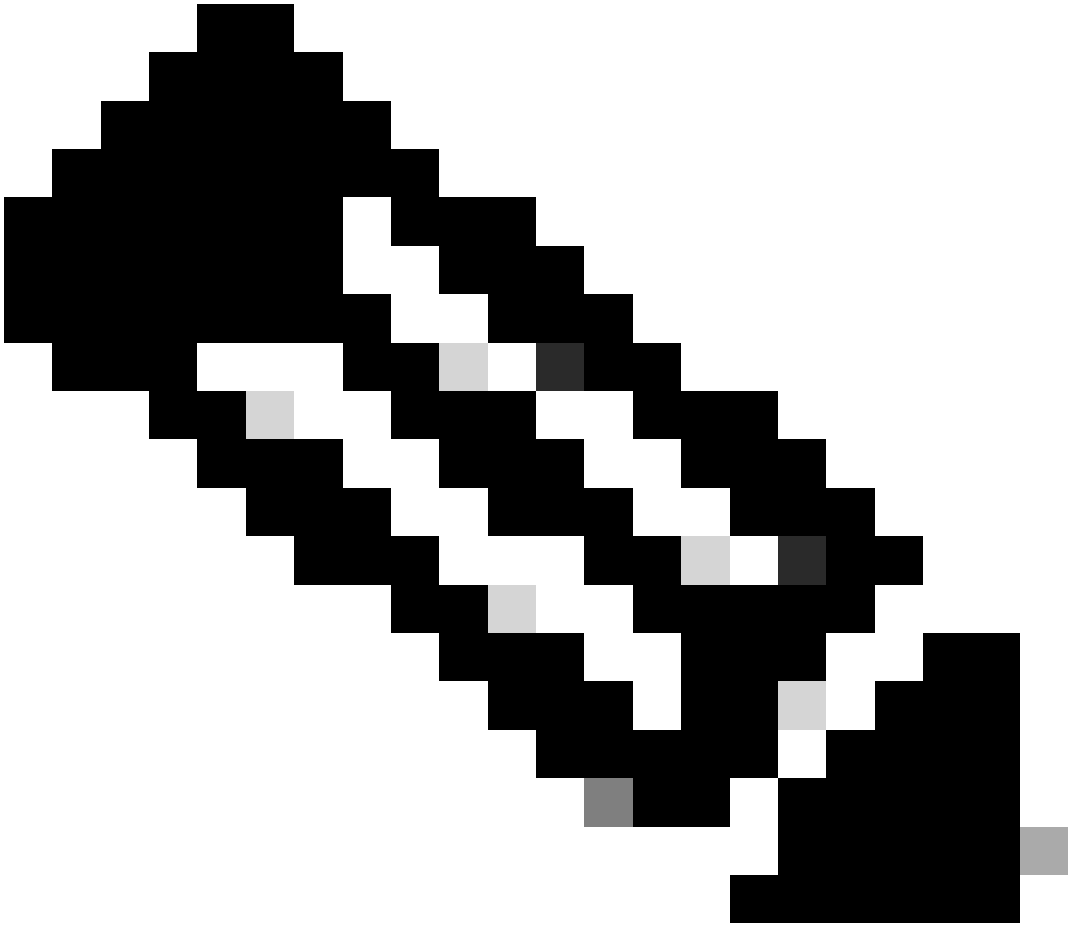


Sugerencia: Si un componente anterior no está correctamente programado, toda la cadena de dependencias se rompe (ejemplo: SISF no tiene una entrada final, BGP no puede crear una RT2).

SISF

Verifique que SISF tenga el host aprendido en la base de datos (la información del host aprendida de DHCP o ARP)

- El SISF aprende las entradas MAC del aprendizaje IOS-MATM y luego las envía al EVPN Mgr (debe ser MAC-REACHABLE con la política "evpn-sisf-policy")
- SISF obtiene un enlace IP/MAC en un VTEP local y usando el administrador EVPN esa información se espera que sea programada como una ruta /32 vía BGP a otras hojas.



Nota: En este escenario, el host tiene una IP estática, por lo que SISF utiliza ARP para obtener los detalles del host. En la sección Mayormente aislado se muestra la indagación DHCP y 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
```

Administrador de EVPN

EVPN Mgr aprende la MAC local y se instala en L2RIB. EVPN Mgr también aprende el MAC remoto de L2RIB, pero la entrada se utiliza solamente para procesar la movilidad MAC

Confirmar que el EVPN Mgr se actualiza con la entrada 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...>
```

L2RIB

- L2RIB aprende el MAC local de EVPN Mgr y lo envía a BGP y L2FIB
- L2RIB también es responsable de aprender MAC remotos de BGP para actualizar EVPN Mgr y L2FIB.
- L2RIB necesita tanto local como remoto para que otros componentes se actualicen correctamente. conservado
- El componente L2RIB se sitúa entre el aprendizaje MAC local y remoto en función de la dirección/componente que se debe actualizar

conservado

Verifique que L2RIB esté actualizado con el MAC local del EVPN Mgr

```
<#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

Verificar que L2RIB actualice BGP

<#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
```

Aprendizaje de RT2 remoto (gateway predeterminado RT2)

BGP

Verifique que BGP haya aprendido el prefijo 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
```

L2RIB

Verificar L2RIB actualizado de BGP

- L2RIB aprende el MAC local de EVPN Mgr y lo envía a BGP y L2FIB. L2RIB también es responsable de aprender MAC remotos de BGP para actualizar EVPN Mgr y L2FIB.
- L2RIB necesita tanto local como remoto para que otros componentes se actualicen correctamente. conservado
- El componente L2RIB se sitúa entre el aprendizaje MAC local y remoto dependiendo de la dirección y el componente que se debe actualizar.

<#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
```

L2FIB

Verificar en L2FIB

- Componente responsable de actualizar FED con los MAC para programar en hardware.
- Las entradas MAC remotas instaladas por L2FIB en FED-MATM NO se puntean en IOS-MATM. (IOS-MATM muestra sólo MAC locales, mientras que FED-MATM muestra tanto MAC local como remoto)
- La salida L2FIB solo muestra los MAC remotos (no es responsable de programar los 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
```

FED

Verificar en FED MATM

- En el nivel de hardware de las Hojas configuradas con la 'palabra clave protected' sólo debería ver la MAC de gateway predeterminada CGW y las MAC de host local.
- El switch observa el prefijo RT2 para el atributo DEF GW para determinar qué MAC remoto es elegible para instalar.

<#root>

```
Leaf01#

show platform software fed switch active matm macTable vlan 201

VLAN   MAC
```

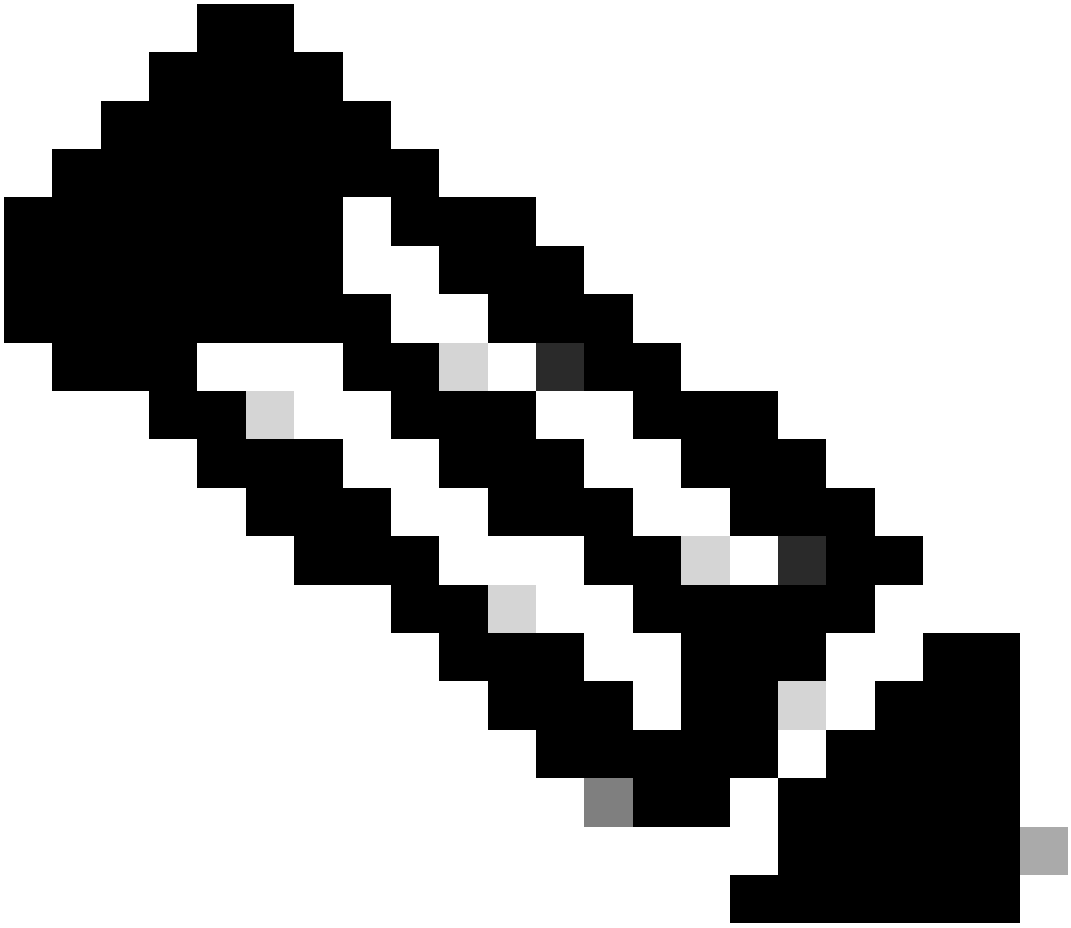
```
Type
  Seq#    EC_Bi  Flags  machandle           siHandle            riHandle            diHandle
Con
-------------------------------------------------------------------------------------------------
201    0000.beef.cafe


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
```

Adyacencia del plano de datos

Como paso final después de confirmar la entrada FED, puede resolver el índice de reescritura (RI)

<#root>

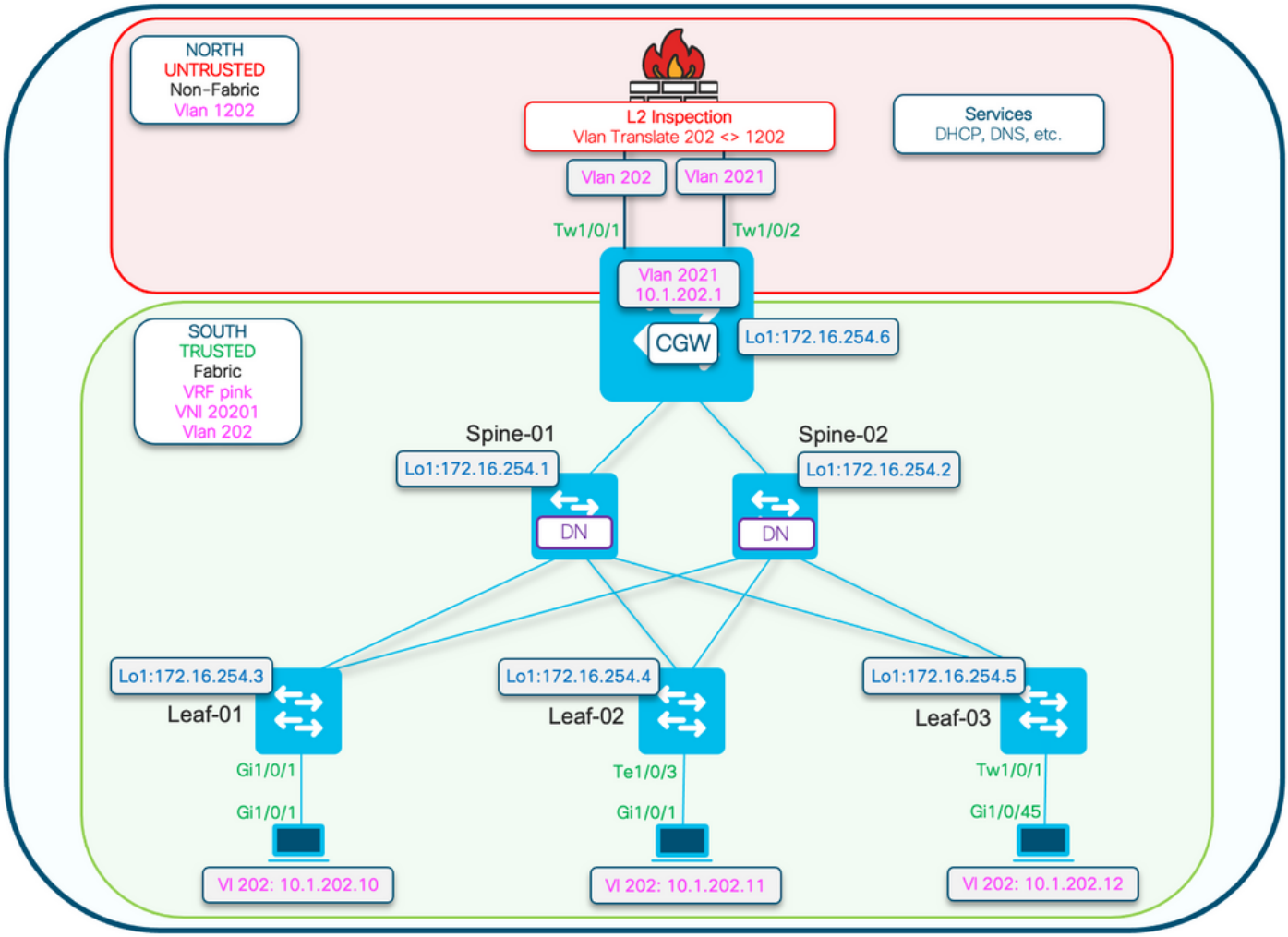
```
Leaf01#

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)
```

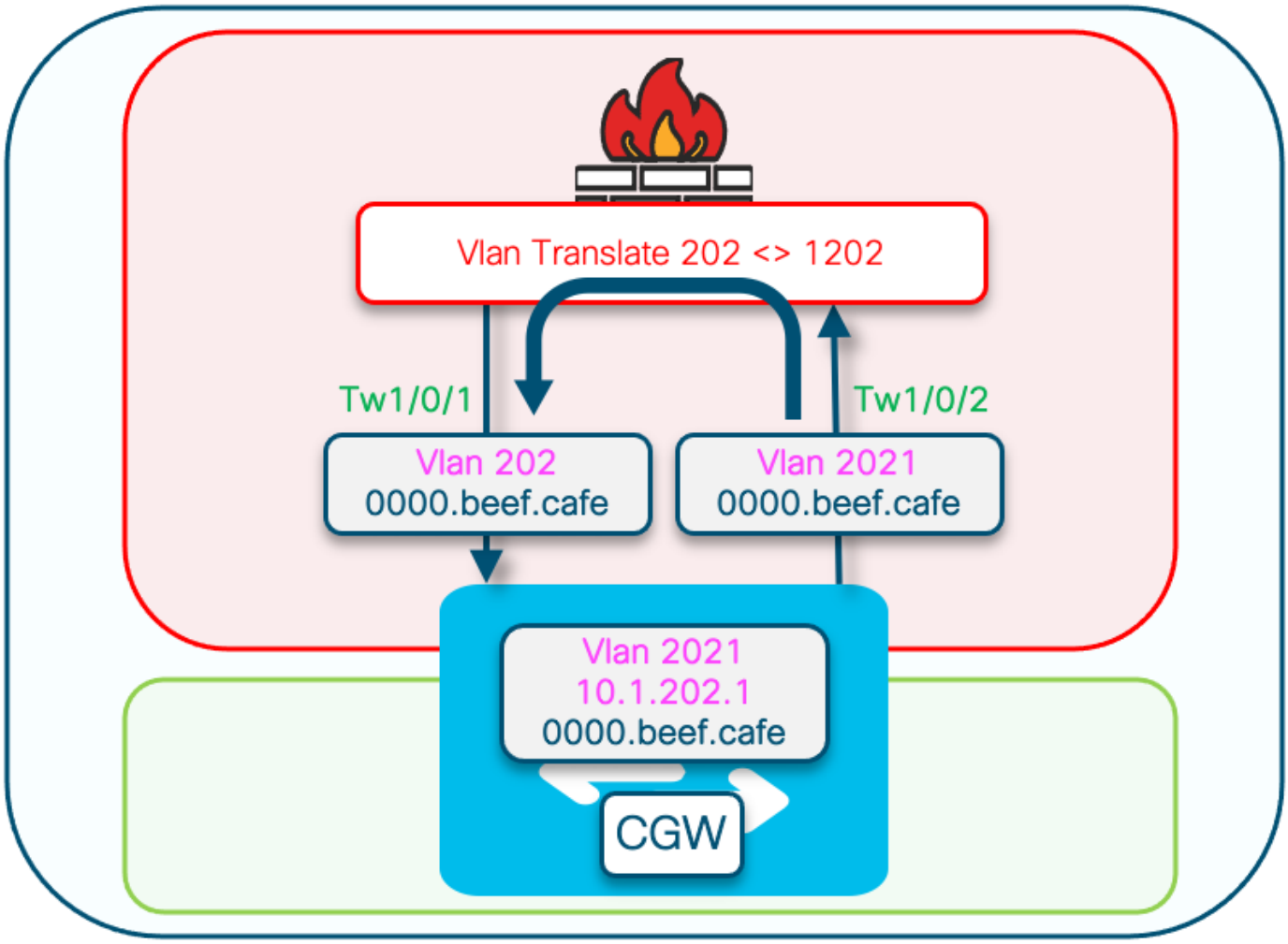


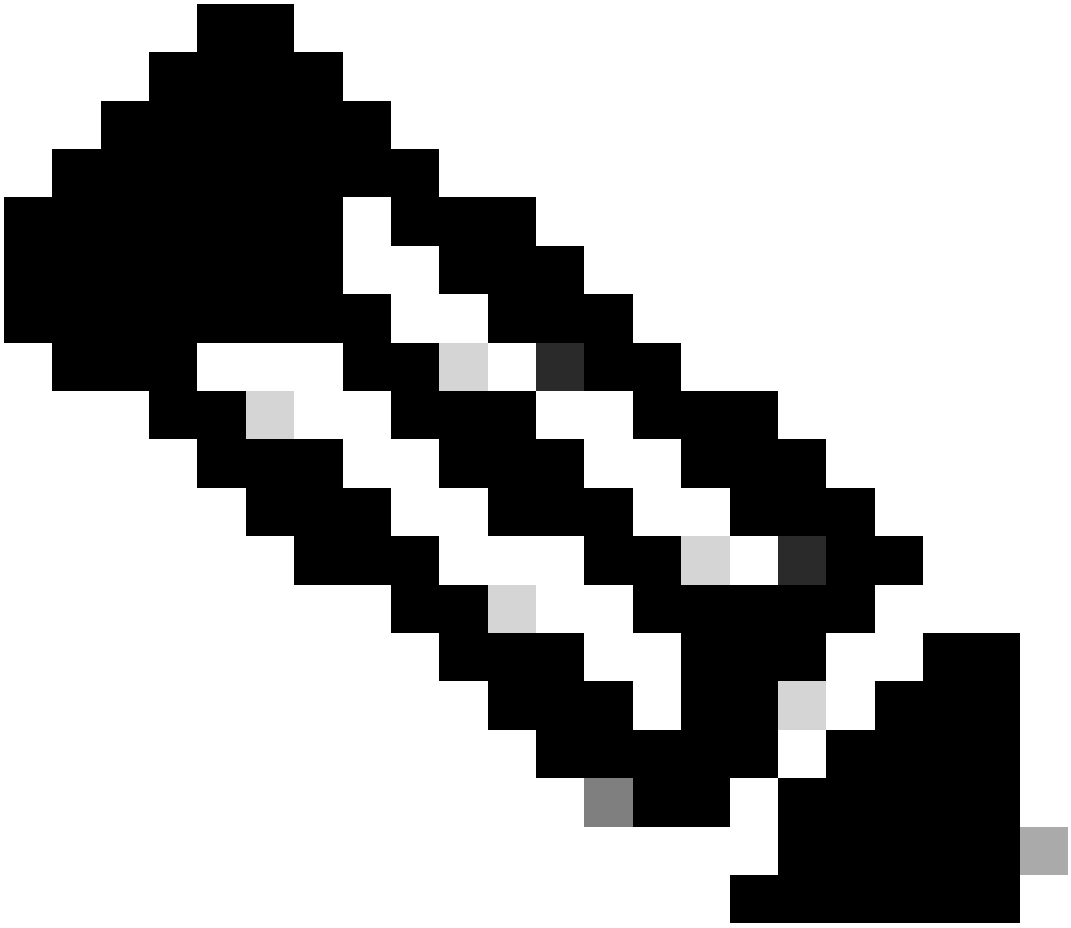
Nota: También puede utilizar 'show platform software fed switch active matm macTable vlan 201 detail' que encadena este comando con el comando FED en un resultado

Configurar (parcialmente aislado)

Diagrama de la red


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



Nota: Esta sección sólo trata las diferencias de los segmentos totalmente aislados.

- Routing-policy para marcar la dirección IP MAC del gateway GCW con el atributo DEF GW
- Política de seguimiento de dispositivos personalizados necesaria para evitar los flaps de MAC
- Enlace estático de seguimiento de dispositivos para IP MAC GW

Leaf-01 (configuración de EVPN 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 (configuración básica)

Establezca el modo de replicación en nve

<#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
```

Configuración de la SVI del gateway externo

<#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
```

Crear una política con la limpieza desactivada

```
<#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
```

Adjuntar a externalgatewayevi/vlan

```
<#root>

CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

 device-tracking attach-policy dt-no-glean <-- apply the new device tracking policy to the vlan configur
```

Agregar entradas estáticas a la tabla de seguimiento de dispositivos para mac-ip de gateway externo

<#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

Cree el route map BGP para que coincida con los prefijos RT2 MAC-IP y establezca la comunidad ampliada del gateway predeterminado

<#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
```

Aplique route-map a los vecinos 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

Verificar (parcialmente aislado)

Detalles de 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...>
```

Generación de RT2 local (host local a RT2)

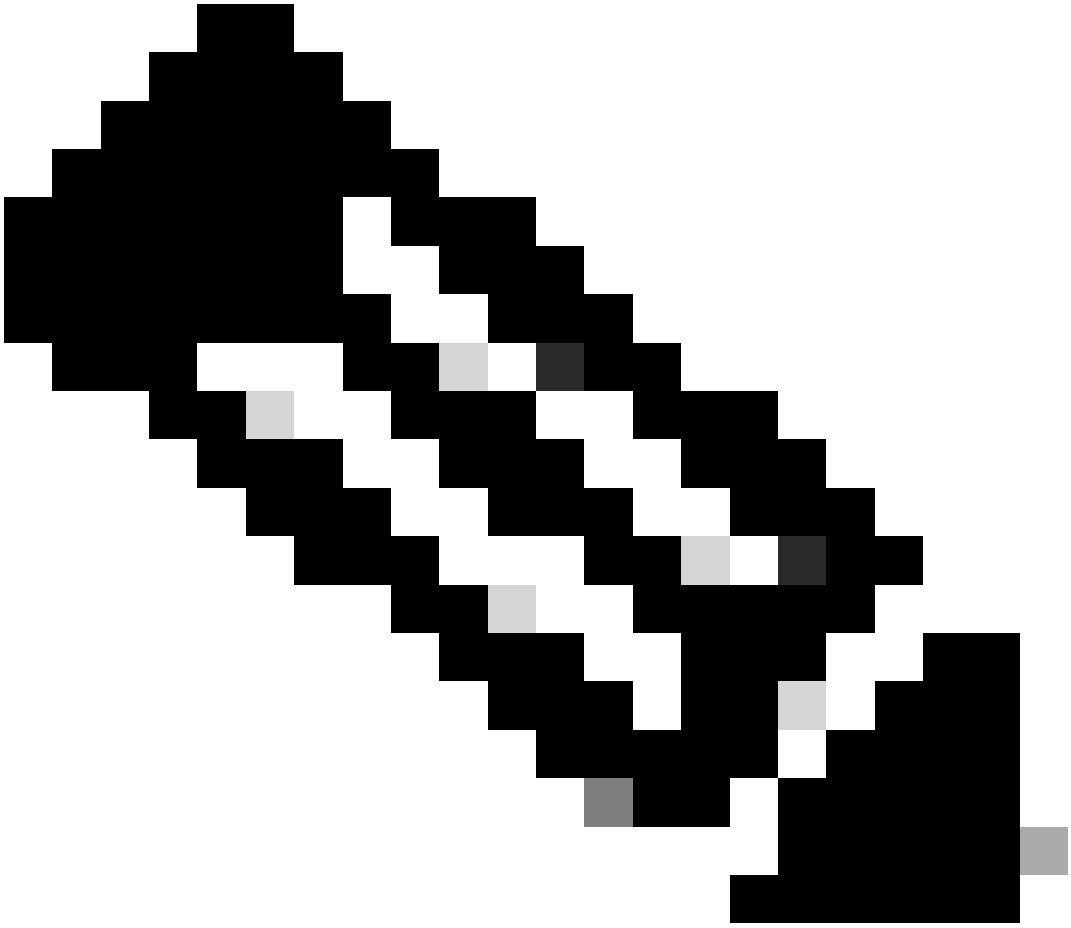
Cubierto en el anterior ejemplo Totalmente aislado

Aprendizaje de RT2 remoto (gateway predeterminado RT2)

Describe las diferencias de Totally Isolated

Prefijo de gateway predeterminado CGW (hoja)

Verifique que el prefijo tenga el atributo apropiado para ser elegible para ser instalado en el hardware



Nota: Esto es crítico para que la retransmisión DHCP L2 funcione

---

<#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 (hoja)

<#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>

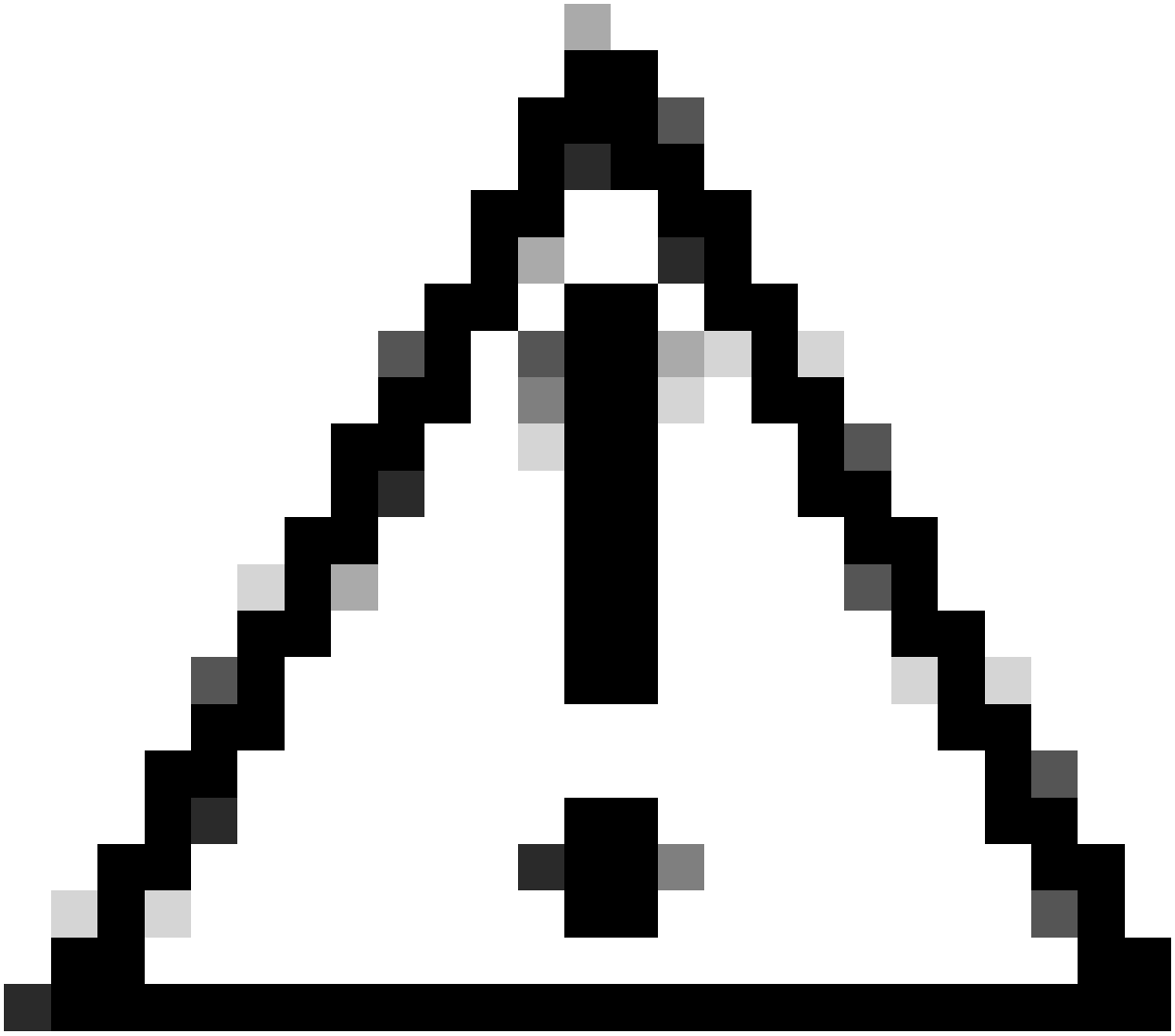
```
CGW#

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
```

Troubleshoot

Resolución de direcciones (ARP)

Pasos generales para aislar los problemas ARP

- Confirmar que el túnel IMET está listo
- Captura en enlace ascendente CGW para verificar que ARP recibido encapsulado desde hoja
- Si no se ve que ARP llega, encap en uplink
  - Verifique que el túnel IMET esté listo tanto en la hoja como en CGW
  - Captura en enlaces ascendentes de hoja para confirmar que el ARP se encapsula y envía
  - Solucionar problemas de ruta intermedia
- Si ARP llega a la captura de túnel IMET de borde pero no está programado en la tabla VRF ARP
  - Solucione los problemas de ruta de punt CPU/CoPP para confirmar ARP punted a CPU
  - Confirme que la dirección IP/información del cliente es correcta
  - Debug ARP en VRF para ver qué podría estar impactando el proceso ARP
- Verifique que CGW MAC esté instalado como next hop/dest mac en los hosts
- Confirmar CGW tiene ambas entradas ARP con los MACs host reales
- Verificar que la política de firewall permita este tipo de tráfico



Precaución: ¡Tenga cuidado al habilitar los debugs!

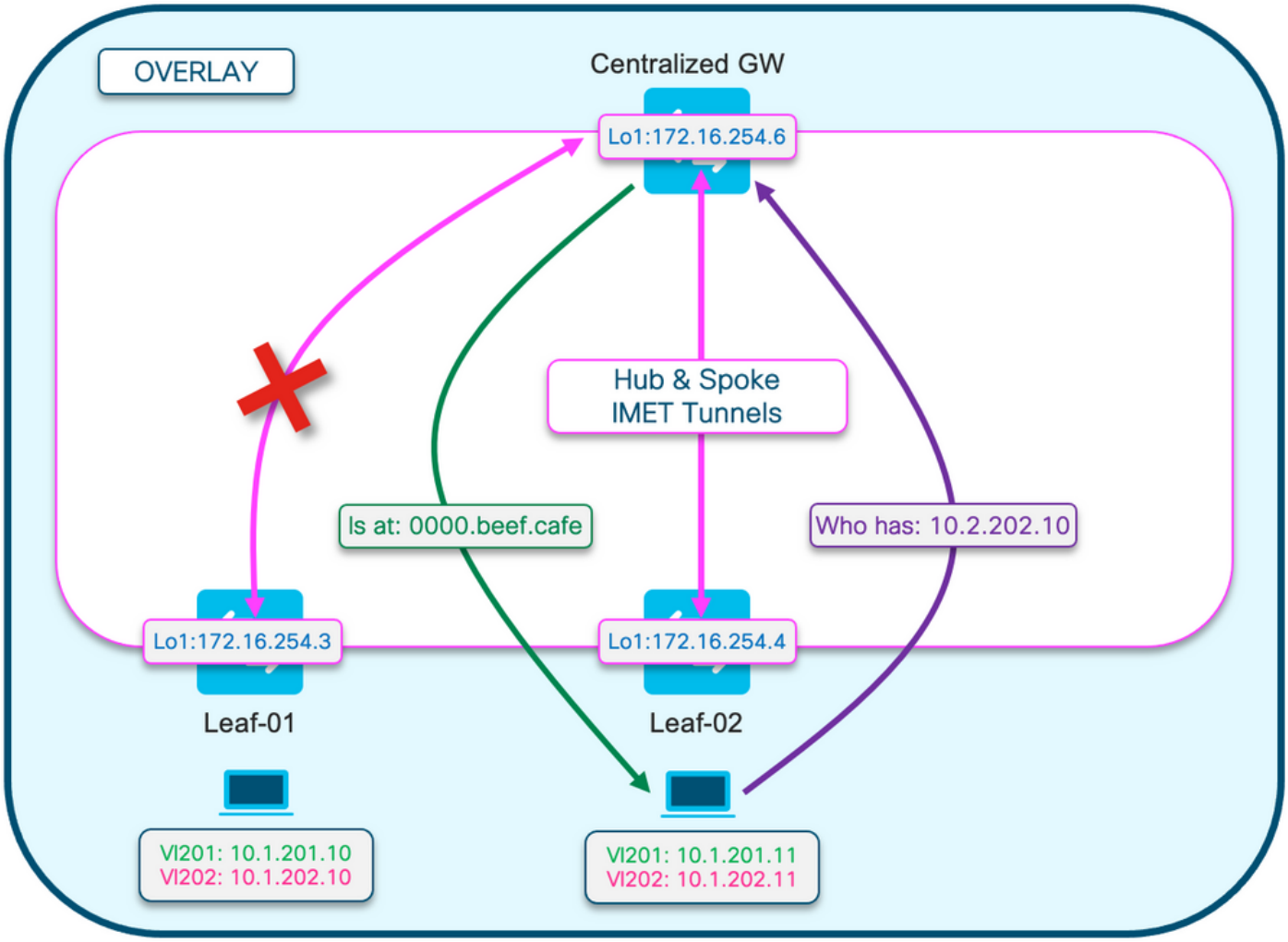
Asegúrese de que ha desactivado la supresión de inundaciones

<#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
```

Cuando el host de Leaf-02 resuelve ARP para el host de Leaf-01, la solicitud ARP no se transmite directamente a Leaf-01

- El ARP en cambio pasa por el único túnel BUM programado en Leaf-02 hacia el CGW
- El CGW no reenvía esto a Leaf-01, y en cambio responde con su propio MAC
- Esto hace que todas las comunicaciones pasen al CGW y luego se enruten entre los hosts
- CGW enruta los paquetes, incluso cuando están en la misma subred local



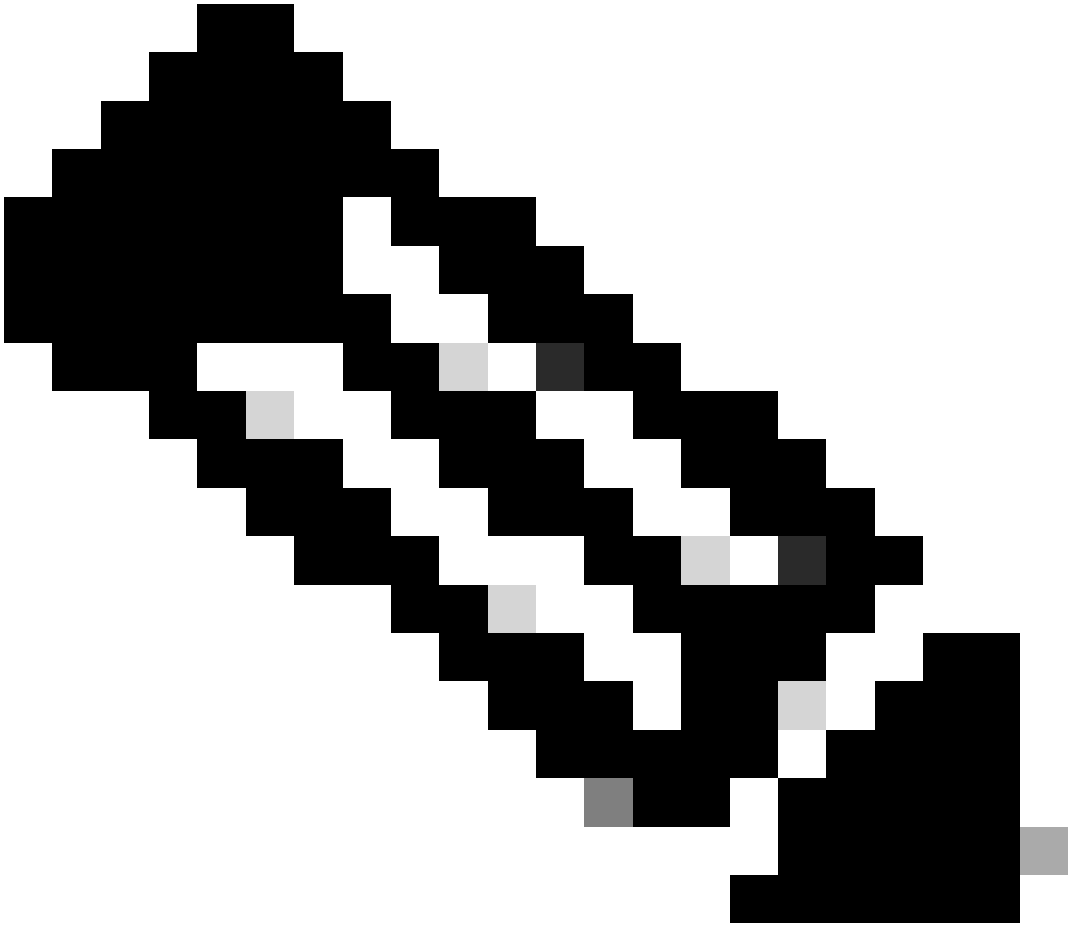
Este diagrama es para ayudar a visualizar el flujo del proceso de resolución ARP descrito en esta sección.

La solicitud ARP se muestra en color morado

- Esta solicitud ARP es para resolver la dirección MAC del host 10.1.202.10 fuera de Leaf-01
- Observe que la línea púrpura termina en CGW y no llega a Leaf-01

La respuesta ARP se muestra en verde

- La respuesta contiene el MAC de CGW SVI para Vlan 202
- Observe que la línea verde proviene del CGW, no del host real



Nota: La X roja indica que esta comunicación no implicó el envío de tráfico a Leaf-01.

Observe las entradas ARP en cada host respectivo

<#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

Observe en CGW que se aprenden los prefijos RT2. Esto es necesario para que CGW rutee los paquetes

<#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
```

Capture el intercambio ARP en los links ascendentes para confirmar la comunicación bidireccional

- Puede utilizar Embedded Packet Capture (EPC) en los enlaces ascendentes de fabric
- Este escenario muestra EPC en el link ascendente Leaf01. Repita este mismo proceso en CGW si es necesario

Configuración del 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
```

Iniciar la captura

<#root>

```
Leaf01#

monitor capture 1 start
```

Inicie el ping para activar la solicitud ARP (en este caso, el ping es desde el host Leaf01 10.1.201.10 al host 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
```

Detenga Capture & Check para las tramas 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
```

Vea los paquetes de captura en detalle. Si desea ver más información sobre los paquetes, utilice la opción de detalle de EPC

- Tenga en cuenta que esta salida se recorta en varios lugares para obtener mayor brevedad

<#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: 000000000000000000000000000000000000
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

Prefijo de gateway CGW RT2

Falta el prefijo de gateway

Como se mencionó en la sección anterior sobre segmentos parcialmente aislados, es necesario aprender el MAC en la VLAN de fabric

- Este problema puede manifestarse si no hay tráfico destinado al gateway durante más tiempo que el temporizador de envejecimiento de MAC.
- Si falta el prefijo de la puerta de enlace CGW, debe confirmar que la dirección MAC está presente

```
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
```

Remediación de prefijo de gateway faltante

En la mayoría de las redes de producción es probable que haya algo de tráfico en todo momento. Sin embargo, si tiene este problema, puede utilizar una de estas opciones para solucionarlo:

- Agregue entradas MAC estáticas como 'mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1'
- Aumente el temporizador de envejecimiento de MAC con 'mac address-table aging-time <seconds>'. (Tenga en cuenta que esto aumenta el tiempo de caducidad de todas las direcciones MAC, por lo que se prefiere la opción de MAC estático)

Falta el atributo DEF GW

Con los segmentos parcialmente aislados, existen varias configuraciones adicionales para añadir este atributo.

Falta la remediación del atributo DEF GW

Confirme estos datos:

- Está ejecutando 17.12.1 o posterior
- La CLI SISF (seguimiento de dispositivos) está presente en la configuración
- Los comandos route-map match & set se configuran y route-map se aplica a los vecinos BGP
- Ha actualizado los anuncios de BGP (debe borrar BGP para volver a anunciar el prefijo con el nuevo atributo

Roaming inalámbrico

El roaming frecuente puede hacer que BGP se actualice con demasiada frecuencia y el roaming por intervalo de tiempo debe incrementarse antes de que el switch declare que posee el MAC y

envíe la actualización de RT2

- Esto ocurre cuando un host se mueve entre dos AP que están en switches diferentes.
- El límite predeterminado para la itinerancia es de 5 por 180 segundos

<#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...>
```

Comandos que se deben recopilar para TAC

En caso de que esta guía no haya resuelto su problema, recopile la lista de comandos mostrada y adjúntela a su solicitud de servicio del TAC.

Información mínima que se debe recopilar

(tiempo limitado para recopilar datos antes de la acción de recarga/recuperación)

conservado

- Show tech evpn
- Show tech
- Show tech sisf

conservado

Información detallada para recopilar

(Si hay tiempo para recopilar datos más completos, es preferible hacerlo)

conservado

- show tech
- show tech evpn
- show tech platform evpn_vxlan switch <number>
- 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

Información Relacionada

- Implemente la Política de Ruteo BGP EVPN en los Catalyst 9000 Series Switches
- Retransmisión de capa 2 de DHCP (próximamente)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).