Implemente a segmentação BGP EVPN Protected Overlay em switches Catalyst 9000 Series

Contents

Introdução

Este documento descreve como implementar a segmentação de sobreposição protegida BGP EVPN VXLAN em Catalyst 9000 Series Switches.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos de BGP EVPN VxLAN
- Troubleshooting de Unicast BGP EVPN
- Política de roteamento BGP EVPN VxLAN

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 e versões posteriores

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Descrição do recurso de alto nível

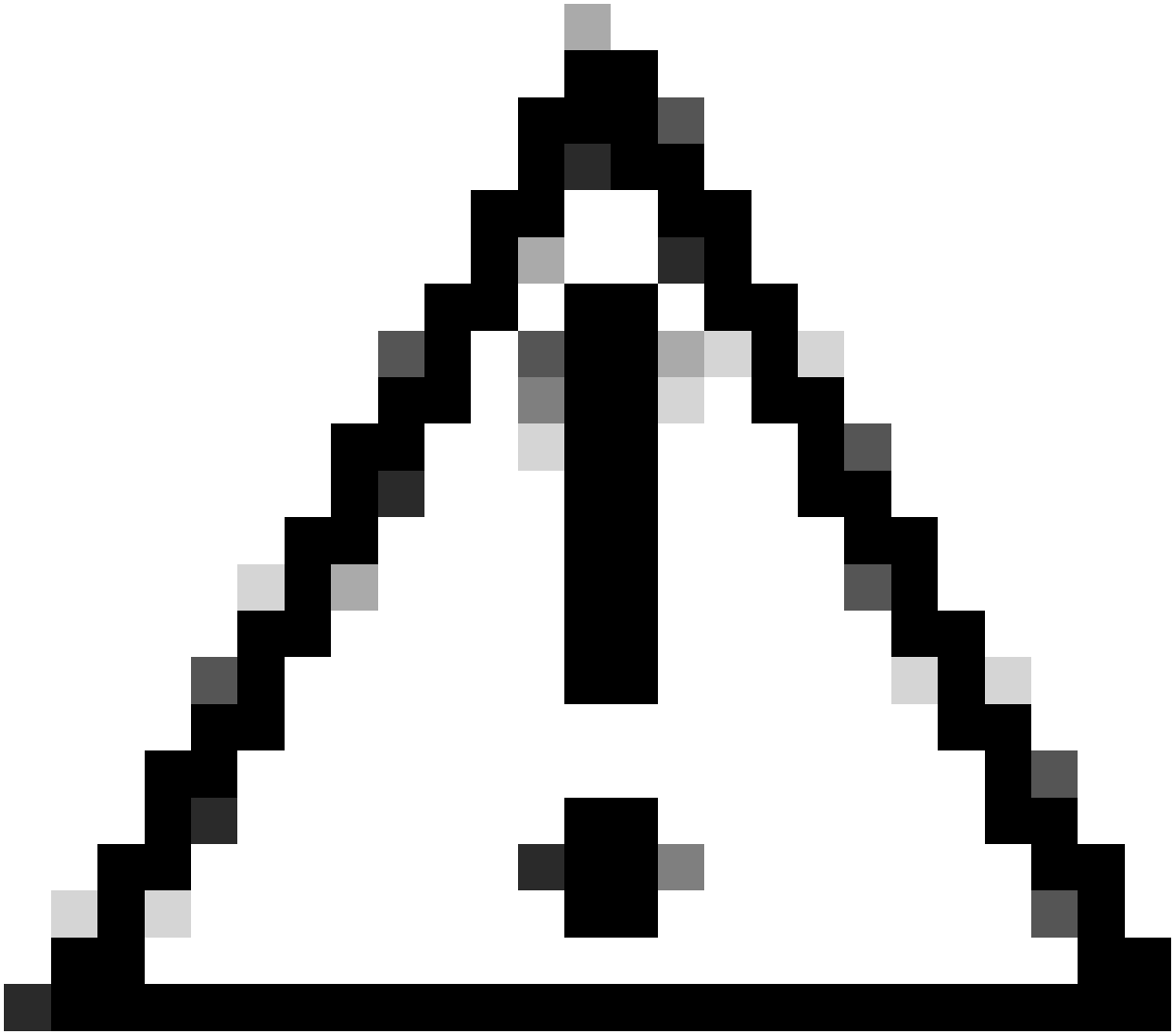
O recurso de segmento protegido é uma medida de segurança que impede que as portas encaminhem o tráfego entre si, mesmo que estejam na mesma VLAN e no mesmo switch

- Esse recurso é semelhante a 'switchport protected' ou a Vlans privadas, mas para estruturas EVPN.
- Esse design força todo o tráfego para o CGW, onde ele pode ser inspecionado por um firewall antes de ser enviado ao seu destino final.
- Os fluxos de tráfego são controlados, determinísticos e fáceis de inspecionar usando um dispositivo de segurança centralizado.

Detalhes do documento

Este documento é parte 2 ou 3 documentos inter-relacionados:

- Documento 1: Implementar a política de roteamento BGP EVPN nos switches Catalyst 9000 Series aborda como controlar o tráfego BGP BUM na sobreposição e deve ser configurado primeiro
- Documento 2: Este documento. Com base no design e na política de sobreposição do documento 1, este documento descreve a implementação da palavra-chave 'protected'
- Documento 3:Implement BGP EVPN DHCP Layer 2 Relay on Catalyst 9000 Series Switches aborda como a retransmissão de DHCP funciona em um VTEP somente de L2



Cuidado: você deve implementar a configuração no documento 1 antes de implementar configurações de segmentos protegidos.

Tipos de Segmento Protegidos

Totalmente isolado

- Permite somente comunicação Norte-Sul e
- O gateway é anunciado na estrutura com a CLI 'default-gateway advertise'

Isolado na maioria

- Permite comunicação Norte-Sul (neste caso de uso, os fluxos de tráfego Leste/Oeste são permitidos com base nas políticas de tráfego de firewall)
- Permite comunicação de leste para oeste (com base em políticas de tráfego de firewall)
- O gateway é externo à estrutura e o SVI não é anunciado usando a CLI 'default-gateway

advertise'

Comportamento do Switch

- Os hosts não podem se comunicar diretamente, mesmo que estejam conectados ao mesmo switch (solicitação ARP não enviada a outras portas no mesmo switch quando os hosts estão no mesmo VRF/Vlan/Segment)
- Nenhum tráfego BUM entre VTEPs L2 (prefixos IMET filtrados usando a configuração de política de roteamento)
- Todos os pacotes dos hosts são retransmitidos para a folha de borda para serem encaminhados. (Isso significa que, para que o Host 1 se comunique com o Host 2 na mesma folha, o tráfego é direcionado para o CGW)

Manuseio de rota tipo 2

- Os Access Leafs anunciam o RT2 local com a comunidade estendida E-Tree e o conjunto de sinalizadores Leaf.
- Os Access Leafs não instalam nenhum RT2 remoto recebido com a E-Tree Extended Community e o flag Leaf definido no plano de dados
- Os Access Leafs não instalam RT2 um no outro no plano de dados
- Os Access Leafs e o Border Leaf (CGW) instalam RT2 um no plano de dados.
- Nenhuma alteração de configuração é necessária na Folha de Acesso ou Folha de Borda.

Resumo do design

- Para broadcast (BUM), a topologia RT3 é hub and spoke para forçar o tráfego de broadcast, como ARP, até o GCW.
- Para considerar a mobilidade do host, o RT2 é full mesh no plano de controle do BGP (quando um host se move de um VTEP para outro, o número Seq é incrementado no RT2)
- O plano de dados instala seletivamente endereços MAC.
    - Uma folha instala somente MACs e RT2 locais que contêm o atributo DEF GW
    - O CGW não tem o KW protegido e instala todo o MAC local e RT2 remoto em seu plano de dados.

Terminologia

VRF	Encaminhamento de roteamento virtual	Define um domínio de roteamento de camada 3 que deve ser separado de outros domínios de roteamento VRF e IPv4/IPv6 global
AF	Família de Endereços	Define quais prefixos de tipo e informações de roteamento o BGP trata
COMO	Sistema	Um conjunto de prefixos IP roteáveis da Internet que pertencem a uma

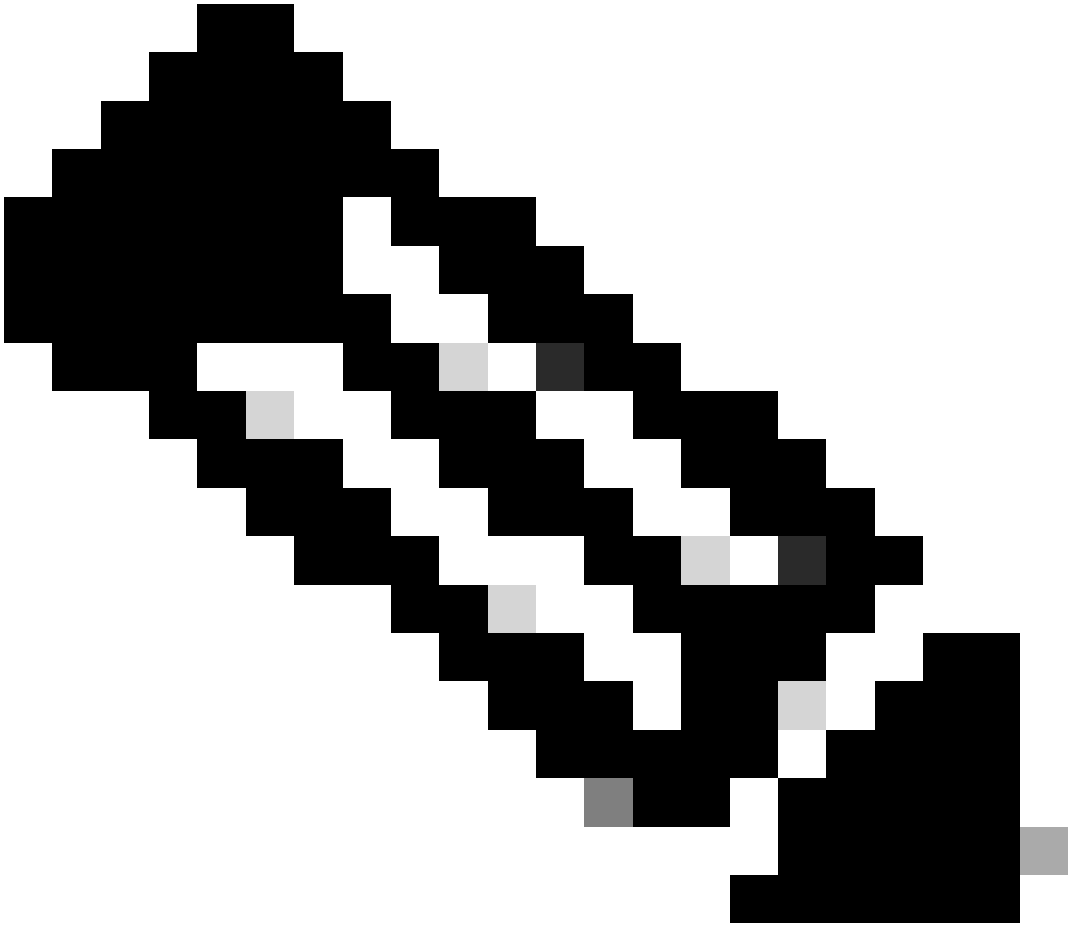
	autônomo	rede ou a um conjunto de redes gerenciadas, controladas e supervisionadas por uma única entidade ou organização
EVPN	Rede Privada Virtual Ethernet	A extensão que permite que o BGP transporte informações de MAC de Camada 2 e IP de Camada 3 é o EVPN e usa o Protocolo de Gateway de Borda Multiprotocolo (MP-BGP - Multi-Protocol Border Gateway Protocol) como o protocolo para distribuir informações de alcance que pertencem à rede de sobreposição de VXLAN.
VXLAN	LAN virtual extensível (rede local)	A VXLAN foi projetada para superar as limitações inerentes de VLANs e STP. É um padrão IETF proposto [RFC 7348] para fornecer os mesmos serviços de rede Ethernet de Camada 2 que as VLANs, mas com maior flexibilidade. Funcionalmente, é um protocolo de encapsulamento MAC-em-UDP executado como uma sobreposição virtual em uma rede de camada 3 subjacente.
CGW	Gateway centralizado	E a implementação do EVPN onde o SVI do gateway não está em cada folha. Em vez disso, todo o roteamento é feito por uma folha específica usando IRB assimétrico (Integrated Routing and Bridging)
DEF GW	Gateway padrão	Um atributo de comunidade estendida de BGP adicionado ao prefixo MAC/IP através do comando "default-gateway advertise enable" na seção de configuração 'l2vpn evpn'.
IMET (RT3)	Tag Ethernet Multicast Inclusiva (Rota)	Também chamada de rota BGP tipo 3. Esse tipo de rota é usado no EVPN para fornecer tráfego BUM (broadcast / unicast desconhecido / multicast) entre VTEPs.
RT2	Tipo de rota 2	Prefixo MAC ou MAC/IP de BGP que representa um MAC de host ou MAC-IP de gateway
Gerente de EVPN	Gerenciador EVPN	Componente de gerenciamento central para vários outros componentes (exemplo: aprende do SISF e envia sinais para o L2RIB)
SISF	Recurso de segurança integrada do switch	Uma tabela de rastreamento de host independente usada pelo EVPN para saber quais hosts locais estão presentes em uma folha

L2RIB	Base de informações de roteamento da camada 2	Em componente intermediário para gerenciar interações entre BGP, EVPN Mgr, L2FIB
FED	Driver do mecanismo de encaminhamento	Programa da camada ASIC (hardware)
MATM	Gerenciador de Tabelas de Endereços Mac	IOS MATM: tabela de software que instala somente endereços locais e FED MATM: tabela de hardware que instala endereços locais e remotos aprendidos do plano de controle e faz parte do plano de encaminhamento de hardware

Diagramas de fluxo

Diagrama de tipo de rota 2 (RT2)

Este diagrama mostra o design de malha completa dos prefixos de host MAC/MAC-IP tipo 2.



Observação: é necessária a malha completa para oferecer suporte à mobilidade e ao roaming

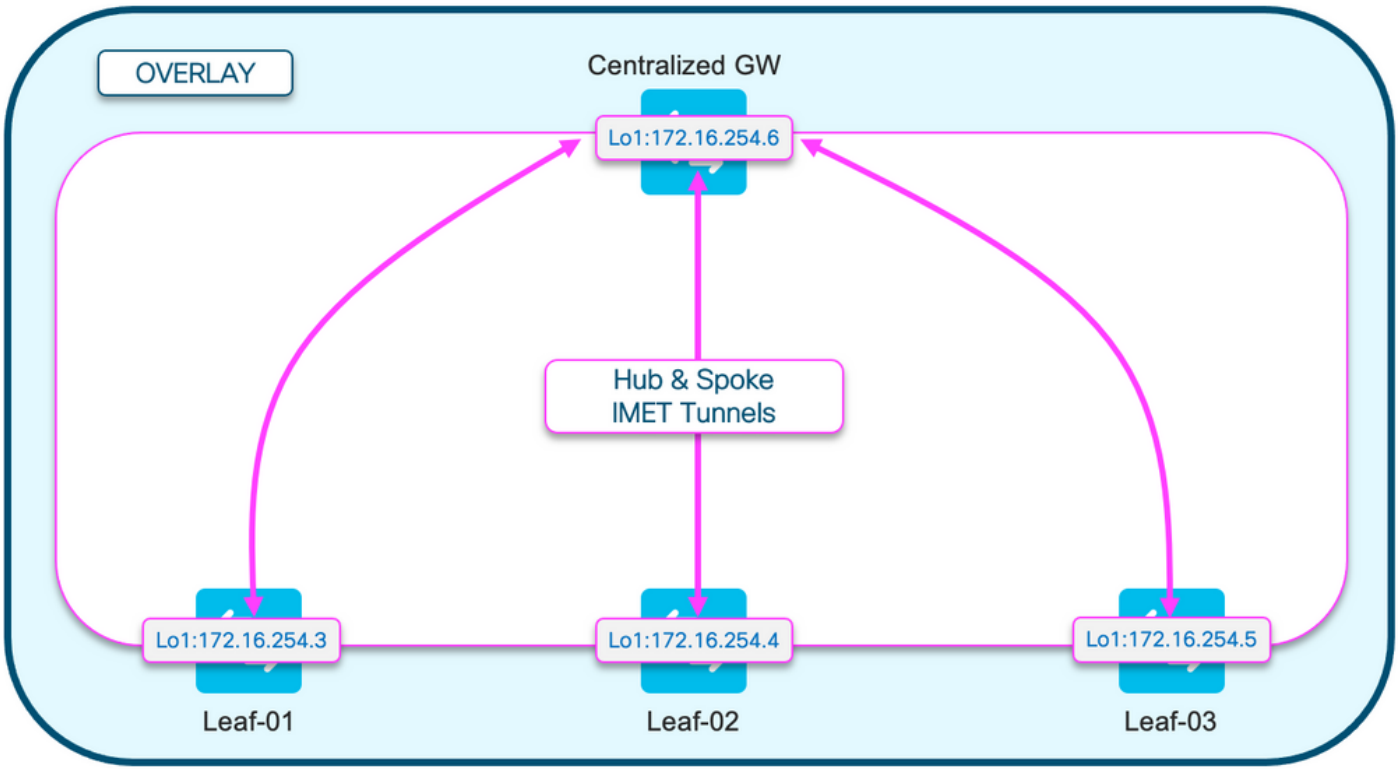
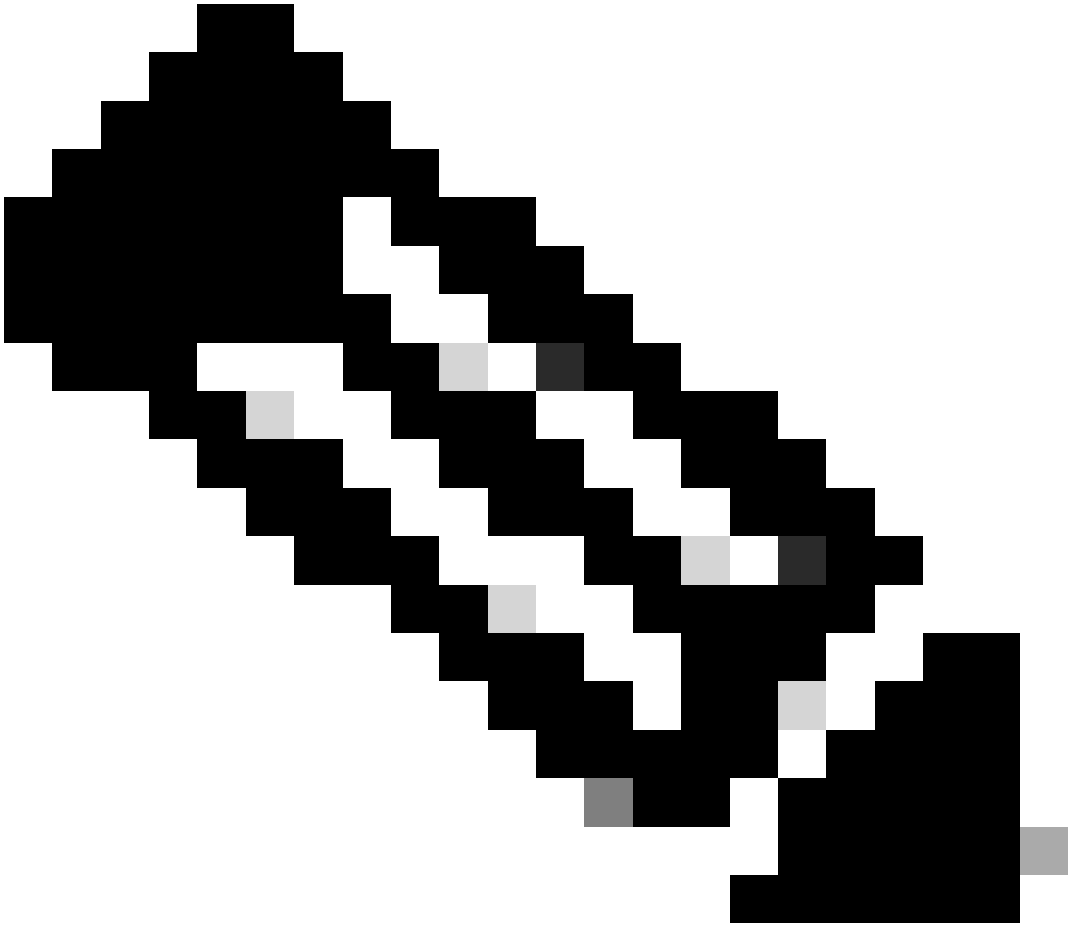


Diagrama de Tipo de Rota 3 (RT3)

Este diagrama mostra o projeto de hub e spoke dos túneis IMET de broadcast (RT3)



Observação: o broadcast hub e spoke é necessário para impedir que leafs com o mesmo segmento enviem broadcast diretamente entre si.

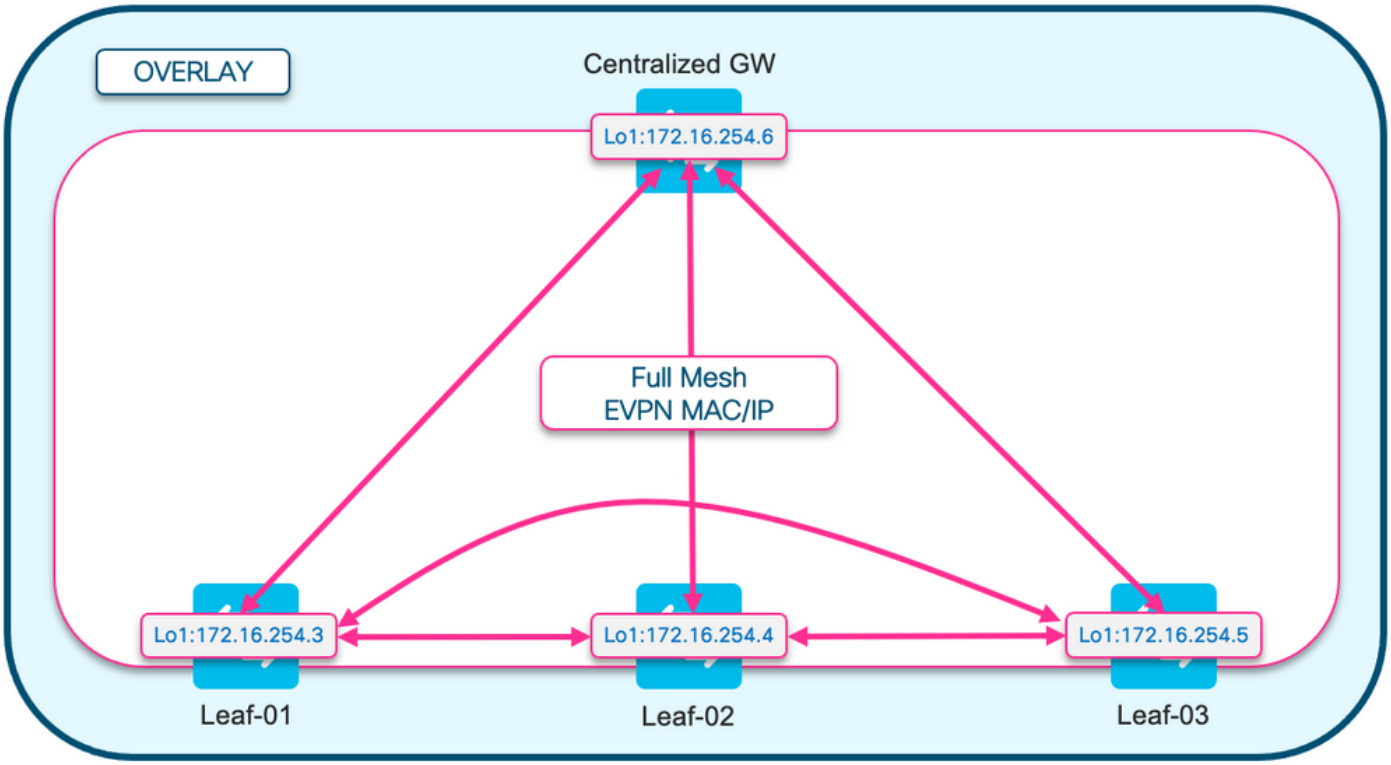
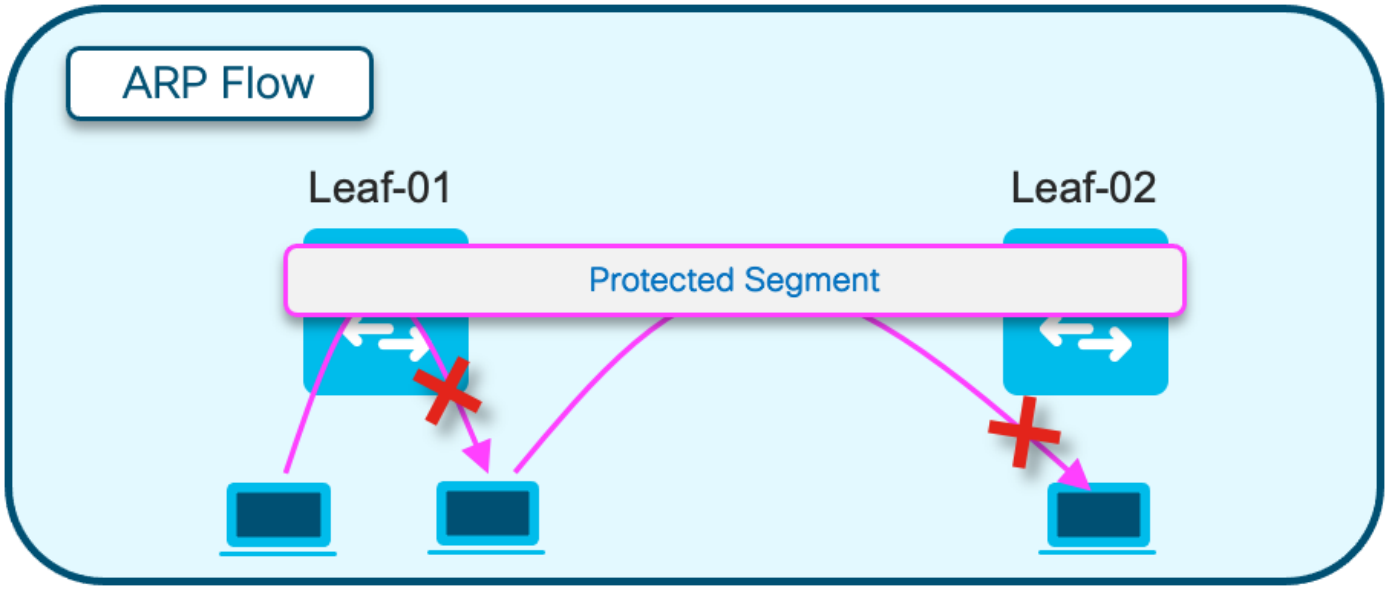
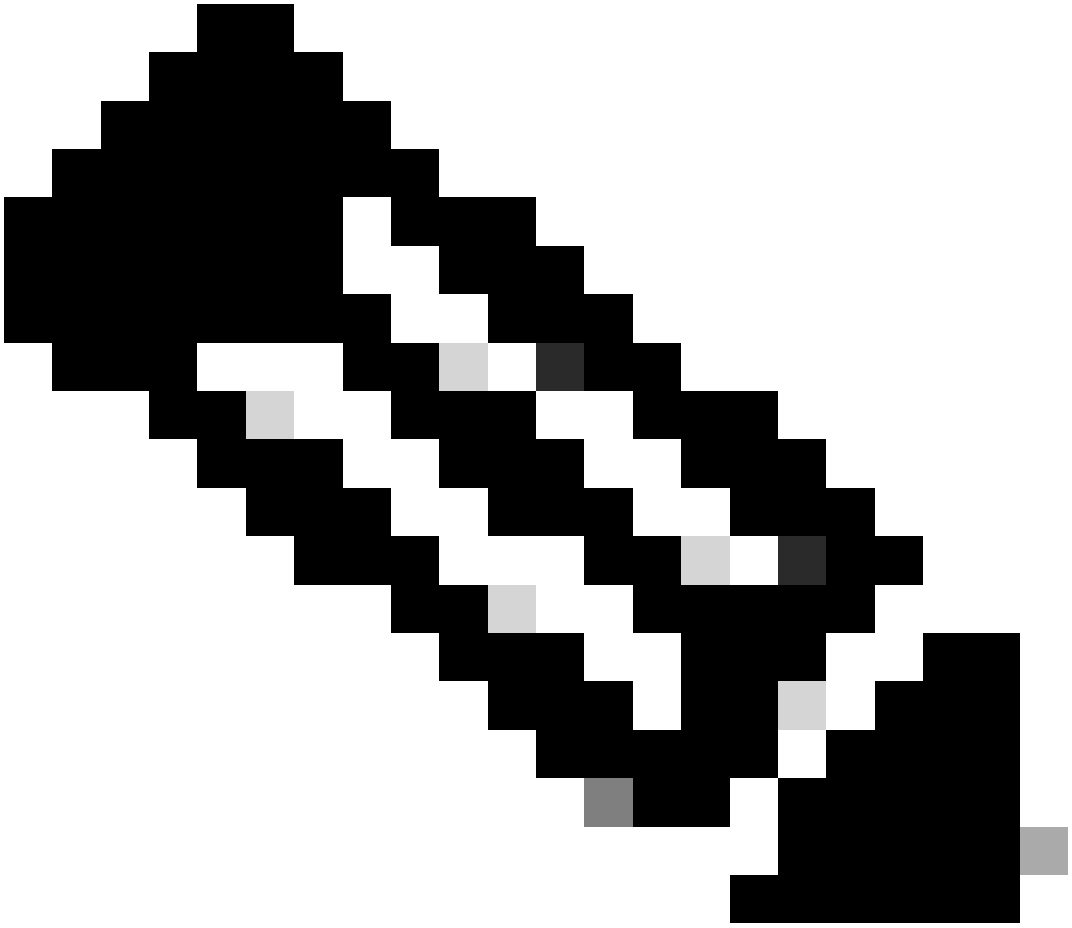


Diagrama de resolução de endereço (ARP)

Este diagrama demonstra que o ARP não tem permissão para acessar nenhum host no mesmo segmento EPVN. Quando ARPs de host de outro host, somente o CGW obtém esse ARP e responde



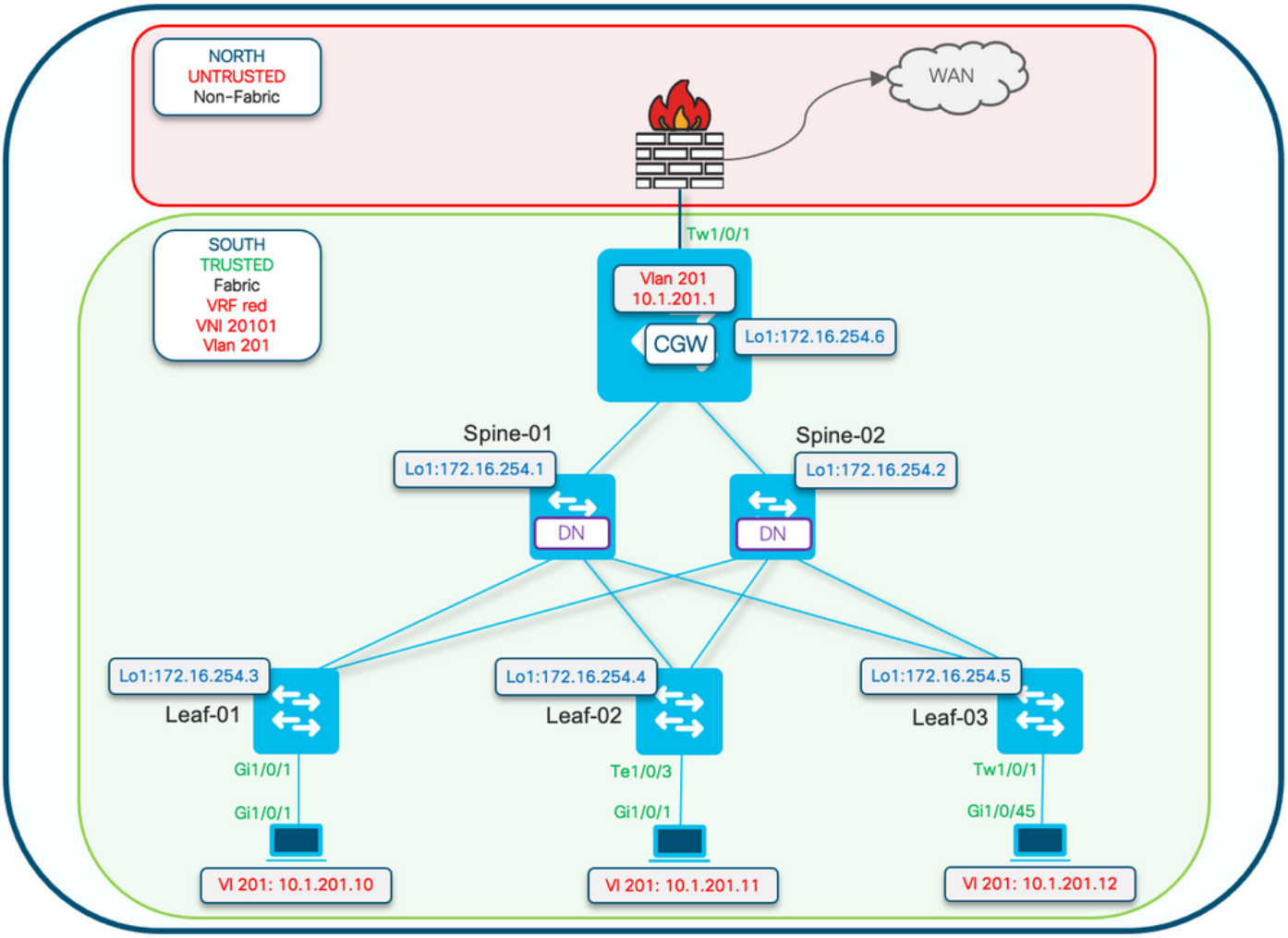


Observação: esta alteração de comportamento ARP é instanciada pelo uso da palavra-chave 'protected'.

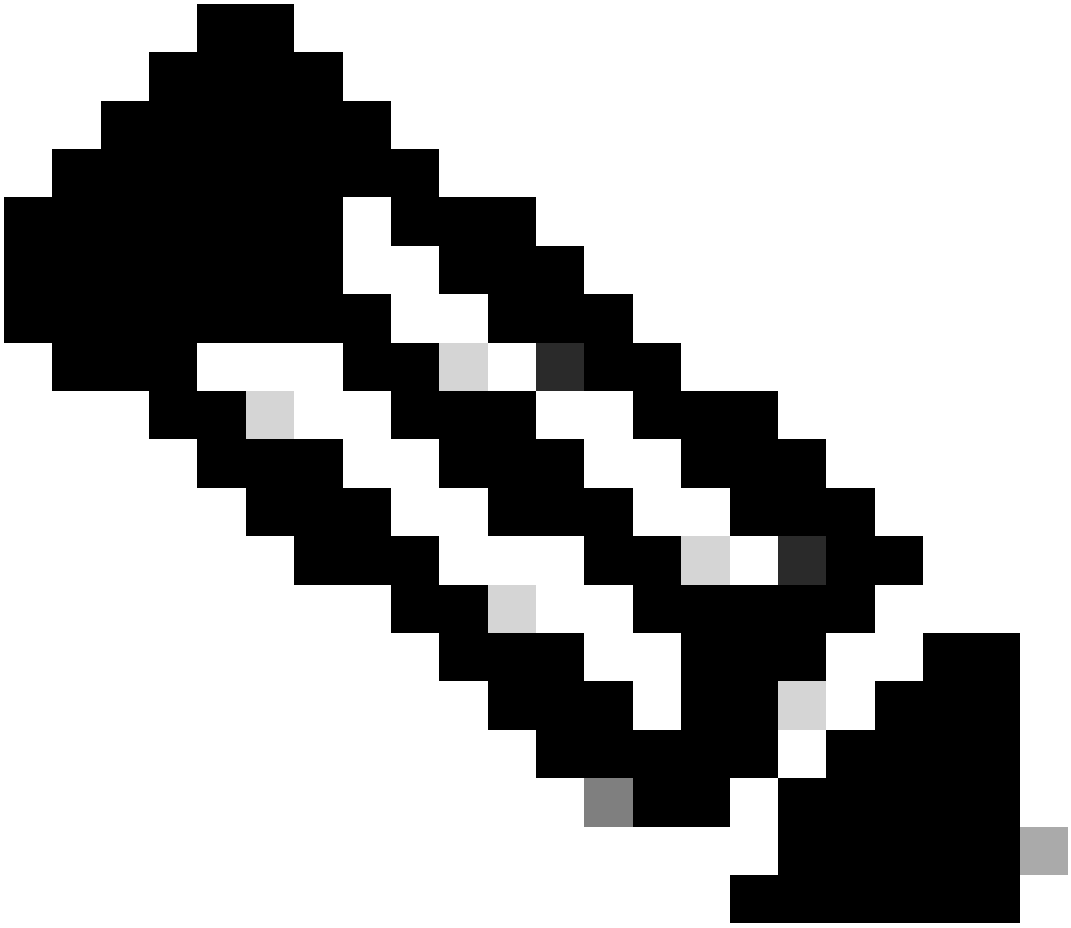
Exemplo: membro evpn-instance 202 vni 20201 protected

Configurar (Totalmente Isolado)

Diagrama de Rede



A palavra-chave de configuração protegida é aplicada aos switches Leaf. O CGW é um dispositivo promíscuo e instala todos os endereços mac.



Observação: a lista de comunidade da política de roteamento e a configuração do mapa de rota que controla a importação/exportação de prefixos IMET é mostrada em Implementar política de roteamento BGP EVPN nos Catalyst 9000 Series Switches. Apenas as diferenças de segmentos protegidos são mostradas neste documento.

Leaf-01 (configuração EVPN básica)

<#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 (configuração 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
```

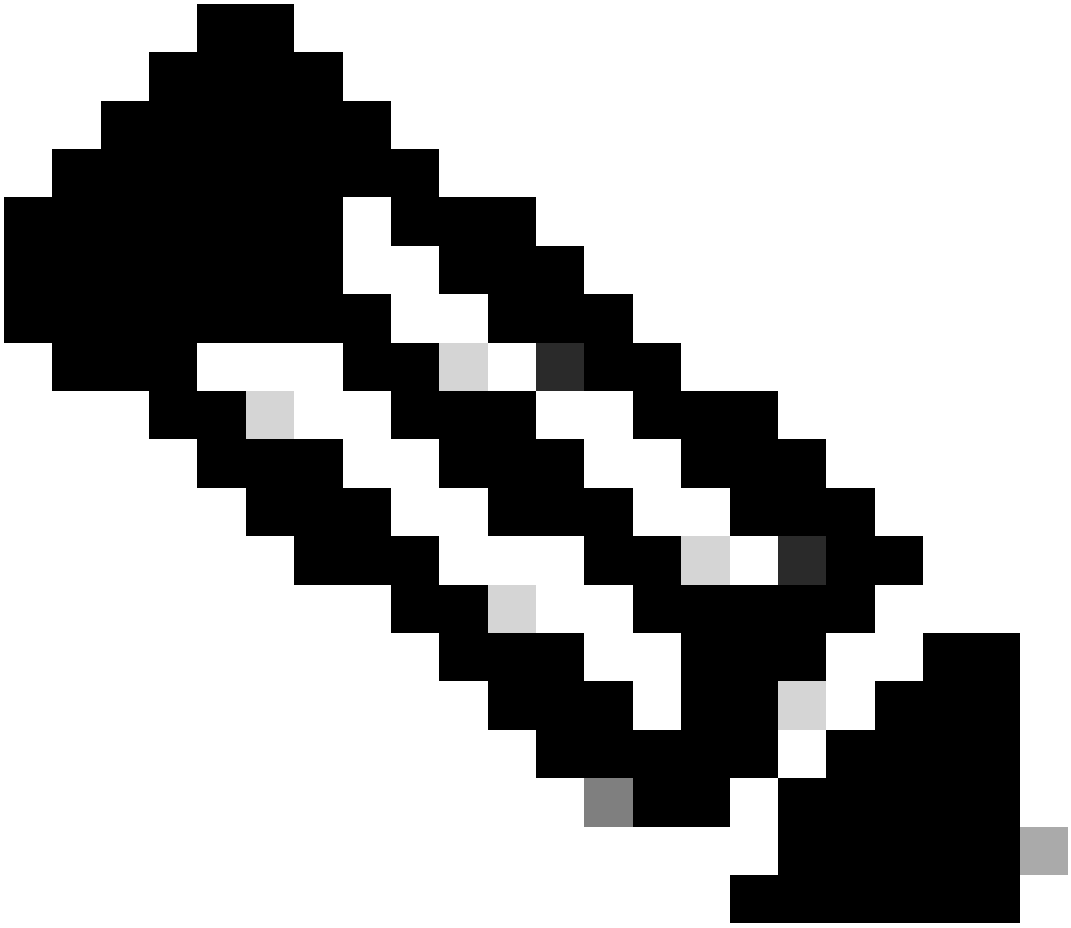
<#root>

```
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
```



Observação: no CGW não há política de BGP aplicada. O CGW tem permissão para receber e enviar todos os tipos de prefixo (RT2, RT5 / RT3).

Verificar (Totalmente Isolado)

Detalhes de EVI

<#root>

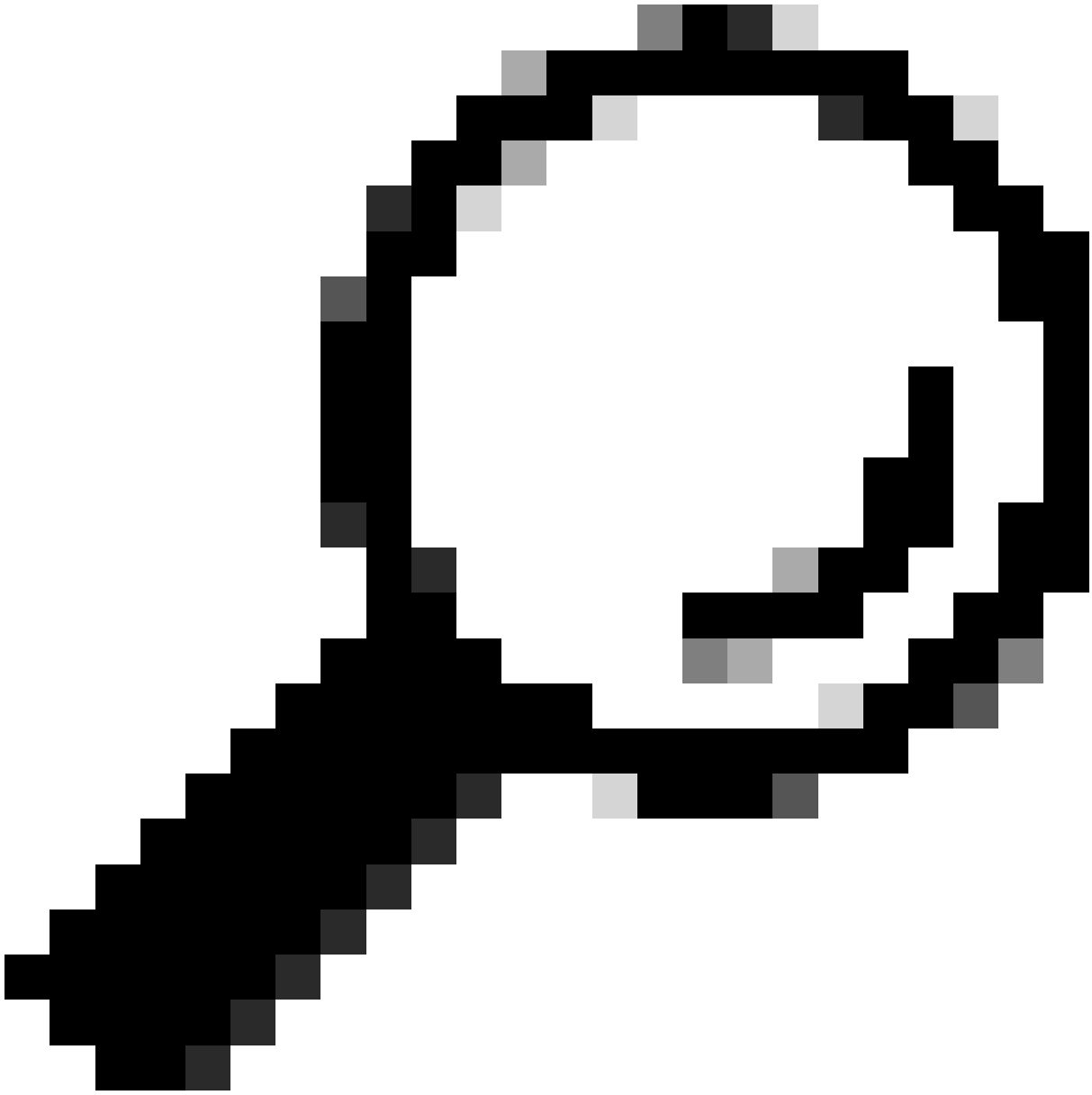
```
Leaf01#

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...>
```

Geração de RT2 Local (Host Local para RT2)

Verifique a cadeia de dependência do componente desde o aprendizado do host local até a geração de RT2:

- SISF (Embora a folha não tenha um SVI, o SISF ainda obtém do host as informações do host através do quadro ARP)
- Gerente de EVPN
- L2RIB
- BGP

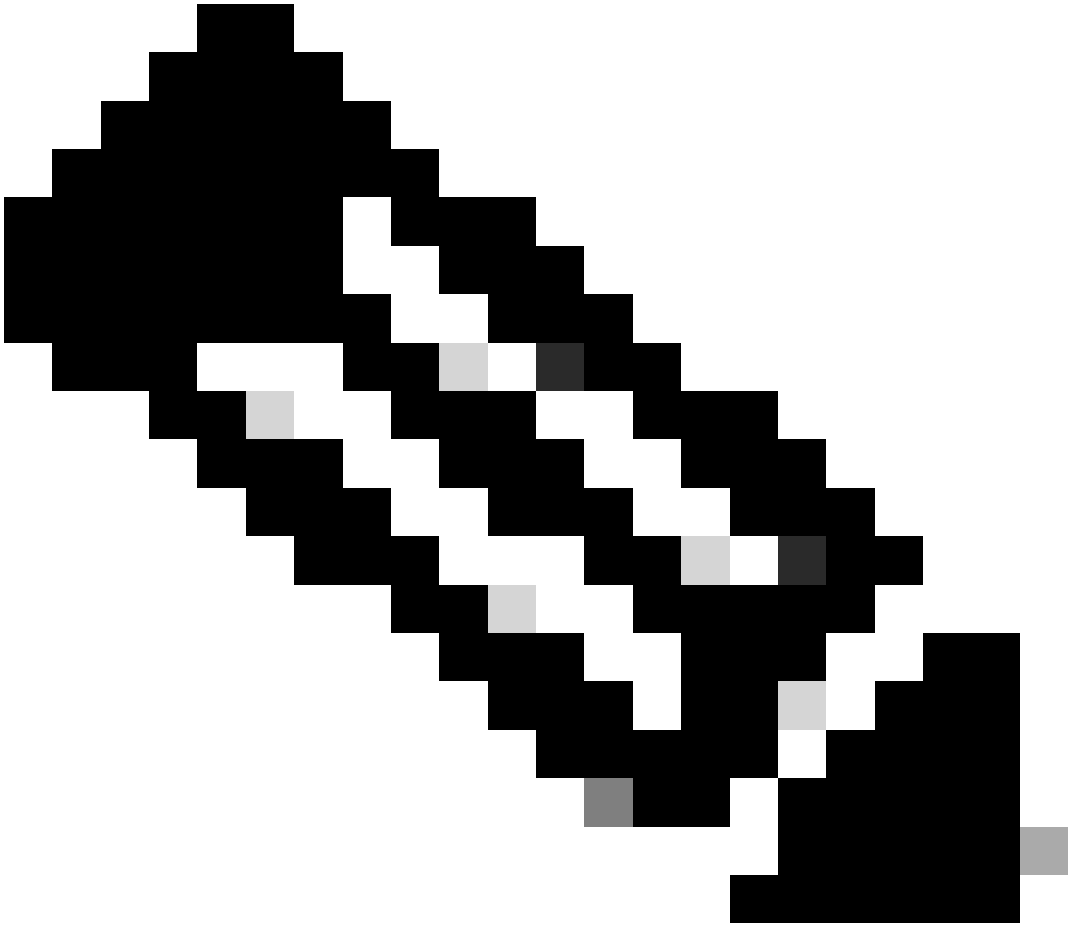


Dica: se um componente anterior não for programado corretamente, toda a cadeia de dependência é interrompida (exemplo: o SISF não tem uma entrada en, o BGP não pode criar um RT2).

SISF

Verifique se o SISF tem o host aprendido no BD (Informações do host aprendidas do DHCP ou ARP)

- O SISF aprende as entradas MAC do aprendizado do IOS-MATM e depois envia para o EVPN Mgr (deve ser MAC-REACHABLE com a política "evpn-sisf-policy").
- O SISF obtém uma ligação IP/MAC em um VTEP local e usa o gerenciador EVPN para que as informações sejam programadas como uma rota /32 via BGP para outros leafs.



Observação: neste cenário, o host tem um IP estático, de modo que o SISF usa o ARP para obter os detalhes do host. Na seção Principalmente Isolada, DHCP e rastreamento de DHCP são mostrados.

<#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
```

Gerenciador EVPN

O EVPN Mgr aprende o MAC local e é instalado no L2RIB. O EVPN Mgr também aprende o MAC remoto de L2RIB, mas a entrada é usada somente para processar a mobilidade MAC

Confirme se o EVPN Mgr está atualizado com a 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

- O L2RIB aprende o MAC local do EVPN Mgr e envia para o BGP e o L2FIB
- O L2RIB também é responsável por aprender MACs remotos do BGP para atualizar o EVPN Mgr e o L2FIB.
- O L2RIB precisa ser local e remoto para que outros componentes sejam atualizados corretamente.
- O componente L2RIB fica entre o aprendizado de MAC local e remoto, dependendo de qual direção/componente precisa ser atualizado

Verifique se o L2RIB está atualizado com o MAC local do 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 se o BGP é atualizado por 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
```

Aprendizado Remoto RT2 (Gateway Padrão RT2)

BGP

Verifique se o BGP aprendeu o prefixo 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

Verifique se o BGP atualizou L2RIB

- O L2RIB aprende o MAC local do EVPN Mgr e envia para o BGP e o L2FIB. O L2RIB também é responsável por aprender MACs remotos do BGP para atualizar o EVPN Mgr e o L2FIB.
- O L2RIB precisa ser local e remoto para que outros componentes sejam atualizados corretamente.
- O componente L2RIB fica entre o aprendizado de MAC local e remoto, dependendo da direção e do componente que precisa ser atualizado.

<#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 em L2FIB

- Componente responsável pela atualização do FED com os MACs para programar no hardware.
- As entradas MAC remotas instaladas por L2FIB no FED-MATM NÃO são direcionadas para o IOS-MATM. (O IOS-MATM mostra apenas MACs locais, enquanto o FED-MATM exibe MAC locais e remotos).
- A saída L2FIB mostra apenas MACs remotos (não é responsável pela programação de MACs locais).

<#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 no FED MATM

- No nível de hardware dos Leafs configurados com a 'palavra-chave protected', você só deve ver o MAC do gateway padrão do CGW e os MACs do host local.
- O switch examina o prefixo RT2 do atributo DEF GW para determinar qual MAC remoto está qualificado para instalação.

<#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
```

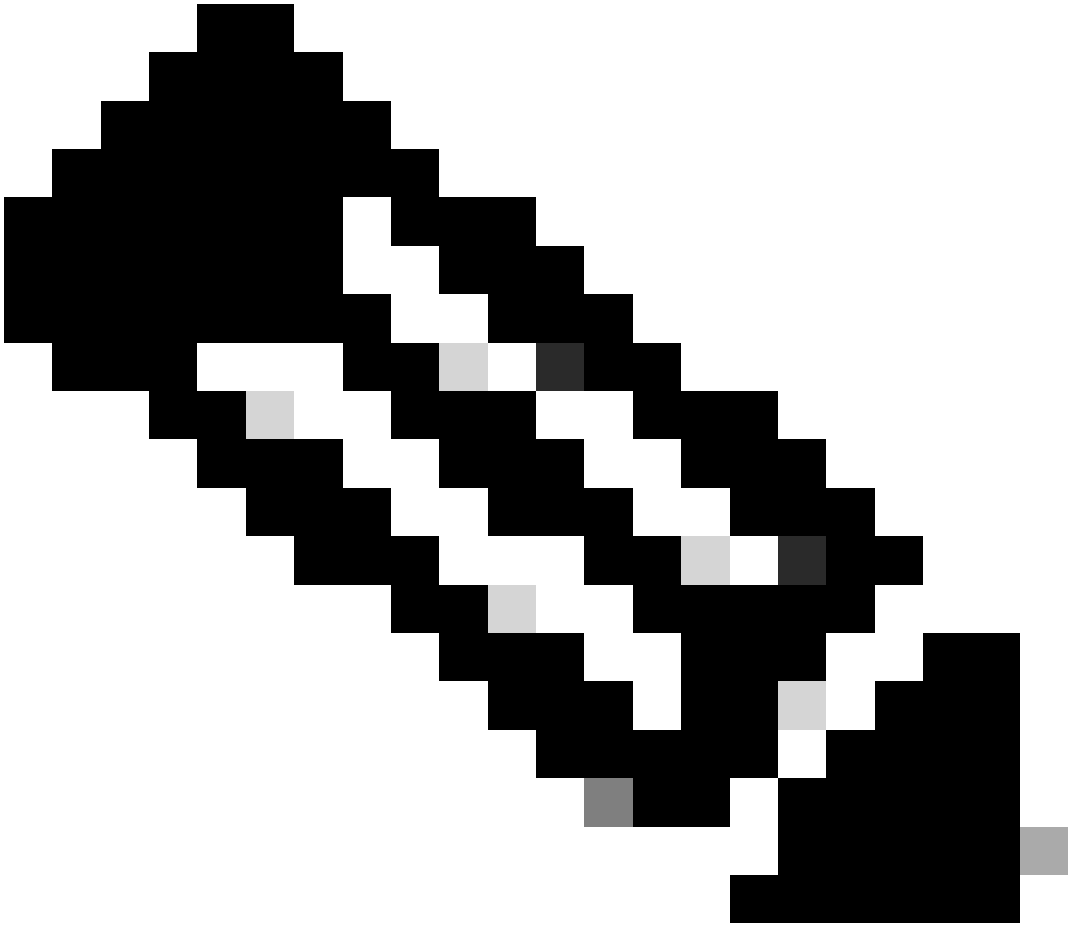
```
MAT_LISP_REMOTE_ADDR 0x1000000
MAT_LISP_GW_ADDR 0x4000000
MAT_DYNAMIC_ADDR 0x1
```

Adjacência do Plano de Dados

Como etapa final após confirmar a entrada de FED, você pode resolver o índice de regravação (RI)

<#root>

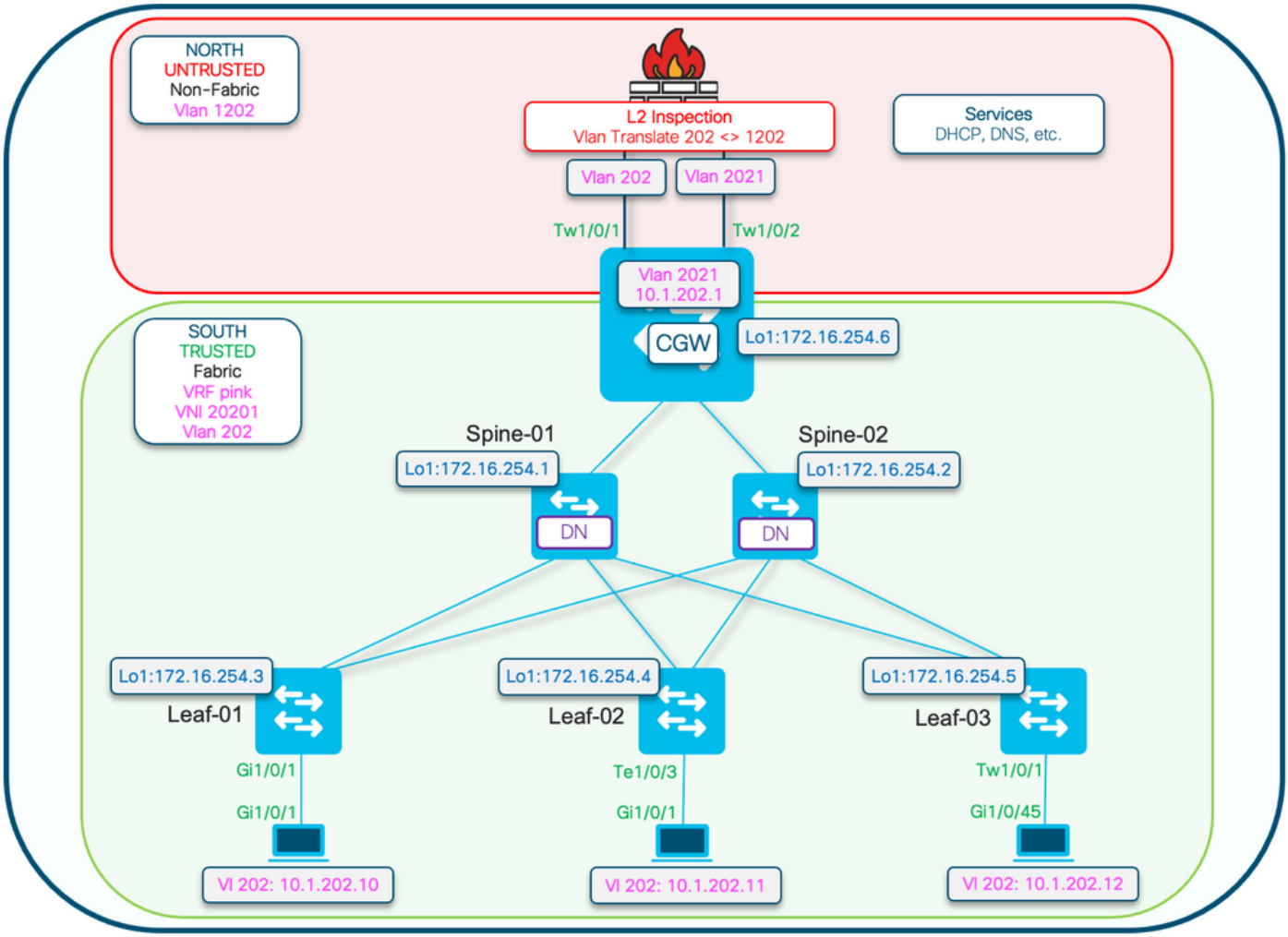
```
Leaf01#

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)
```

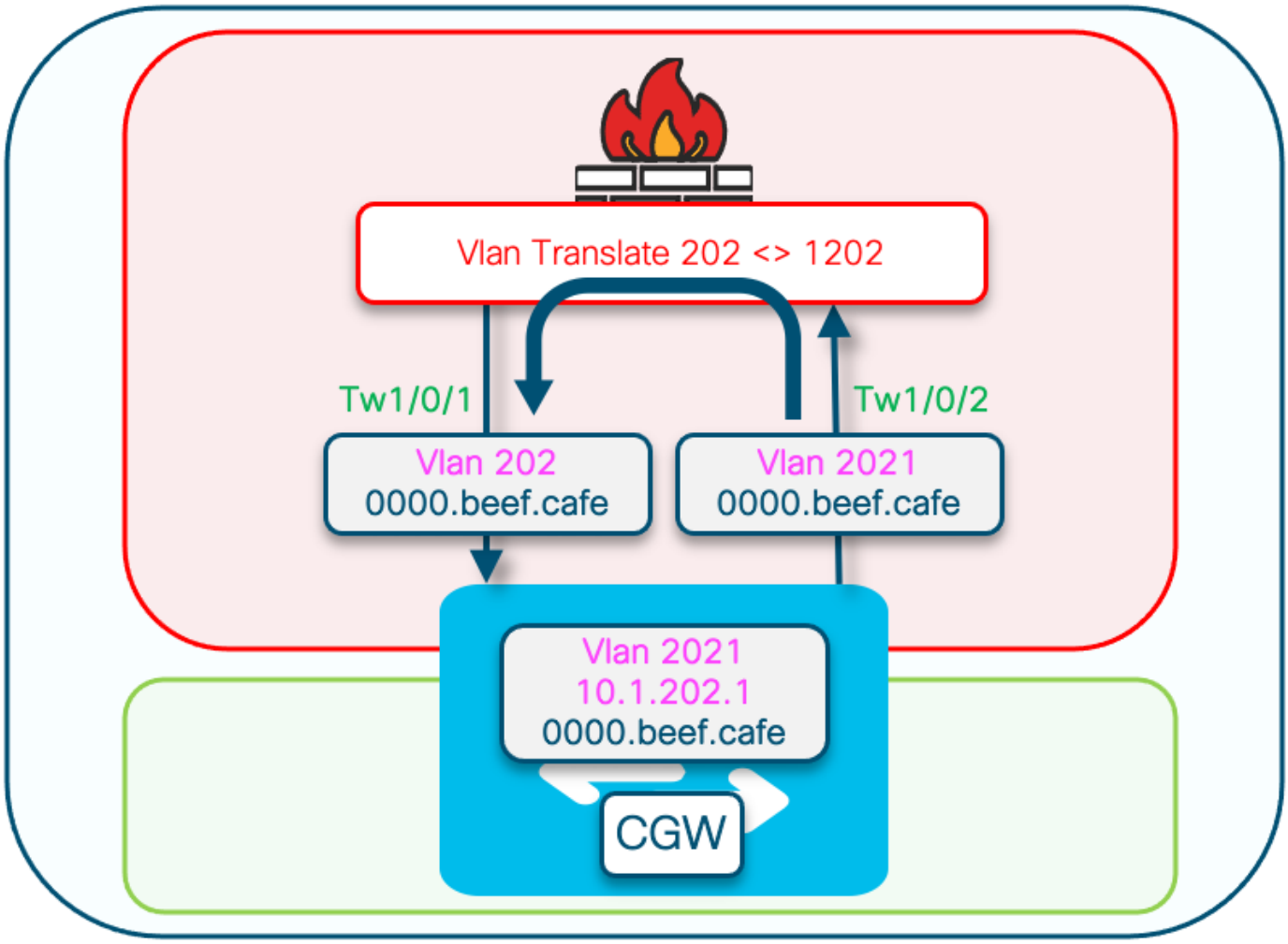


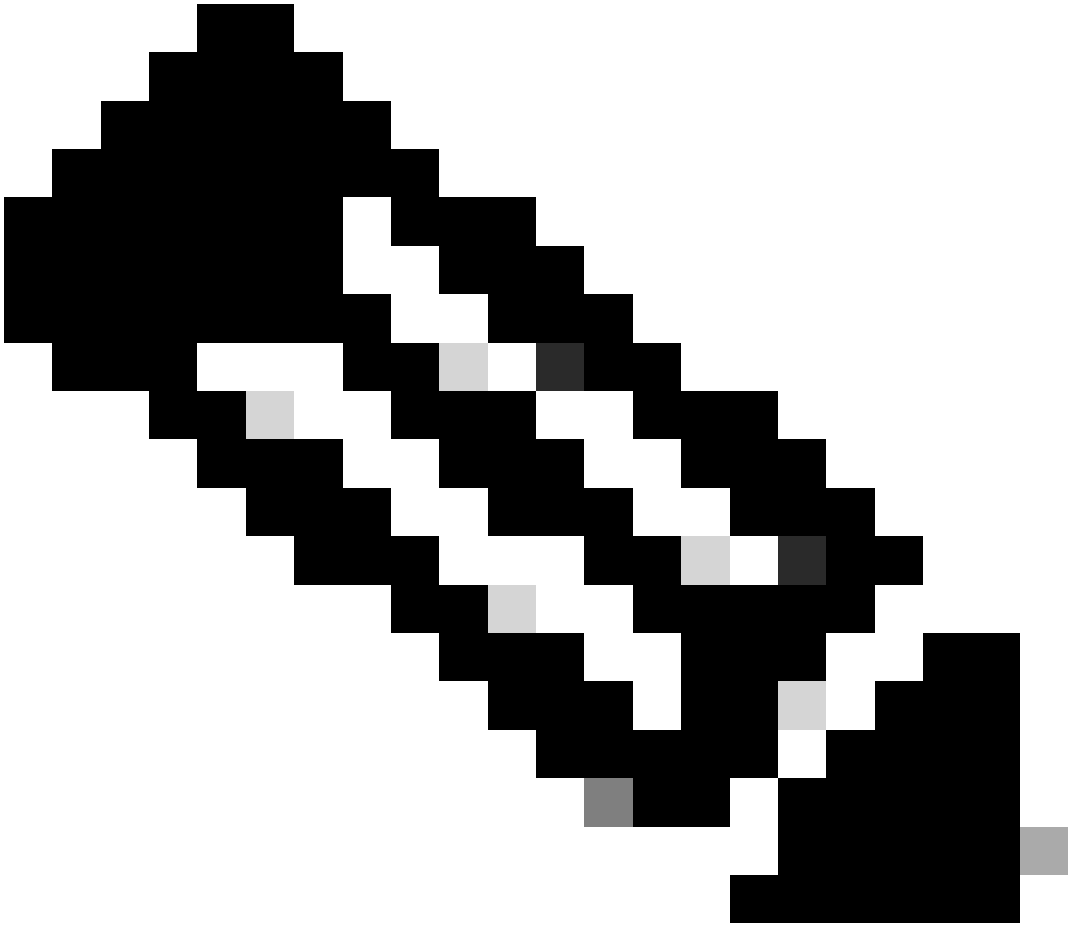
Observação: você também pode usar 'show platform software fed switch ative matm macTable vlan 201 detail' que encadeia esse comando com o comando FED em um resultado

Configurar (Parcialmente isolado)

Diagrama de Rede


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



Observação: esta seção aborda apenas as diferenças dos Segmentos Totalmente Isolados.

- Política de roteamento para marcar o IP MAC do gateway GCW com o atributo DEF GW
- Política de rastreamento de dispositivo personalizado necessária para evitar falhas de MAC
- Ligação estática de rastreamento de dispositivo para o IP MAC GW

Leaf-01 (configuração EVPN básica)

<#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 (configuração básica)

Defina o modo de replicação no 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
```

Configurar o SVI de 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
```

Criar uma política com a limpeza desabilitada

<#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
```

Anexar a externalgatewayevi/vlans

<#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
```

Adicione entradas estáticas na tabela de controle de dispositivos para 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
```

Crie o mapa de rotas BGP para corresponder aos prefixos MAC-IP de RT2 e defina o gateway padrão extended community

<#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
```

Aplicar mapa de rota aos vizinhos do refletor de rota BGP

<#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 Isolado)

Detalhes 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...>
```

Geração de RT2 Local (Host Local para RT2)

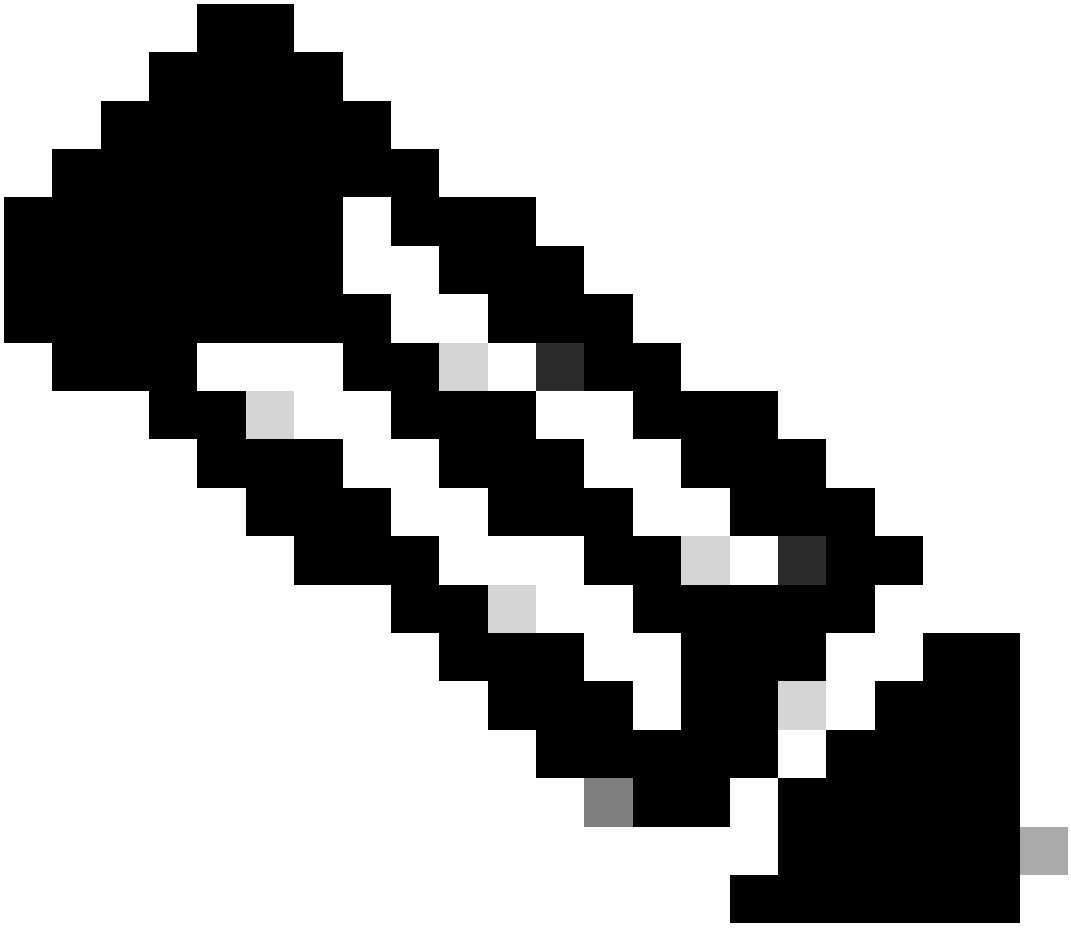
Abrangido no exemplo anterior totalmente isolado

Aprendizado Remoto RT2 (Gateway Padrão RT2)

Abrange as diferenças de Totalmente Isolado

Prefixo de gateway padrão do CGW (folha)

Verifique se o prefixo tem o atributo apropriado para estar qualificado para ser instalado no hardware



Observação: isso é crítico para que o DHCP L2 Relay 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 (Folha)

<#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>

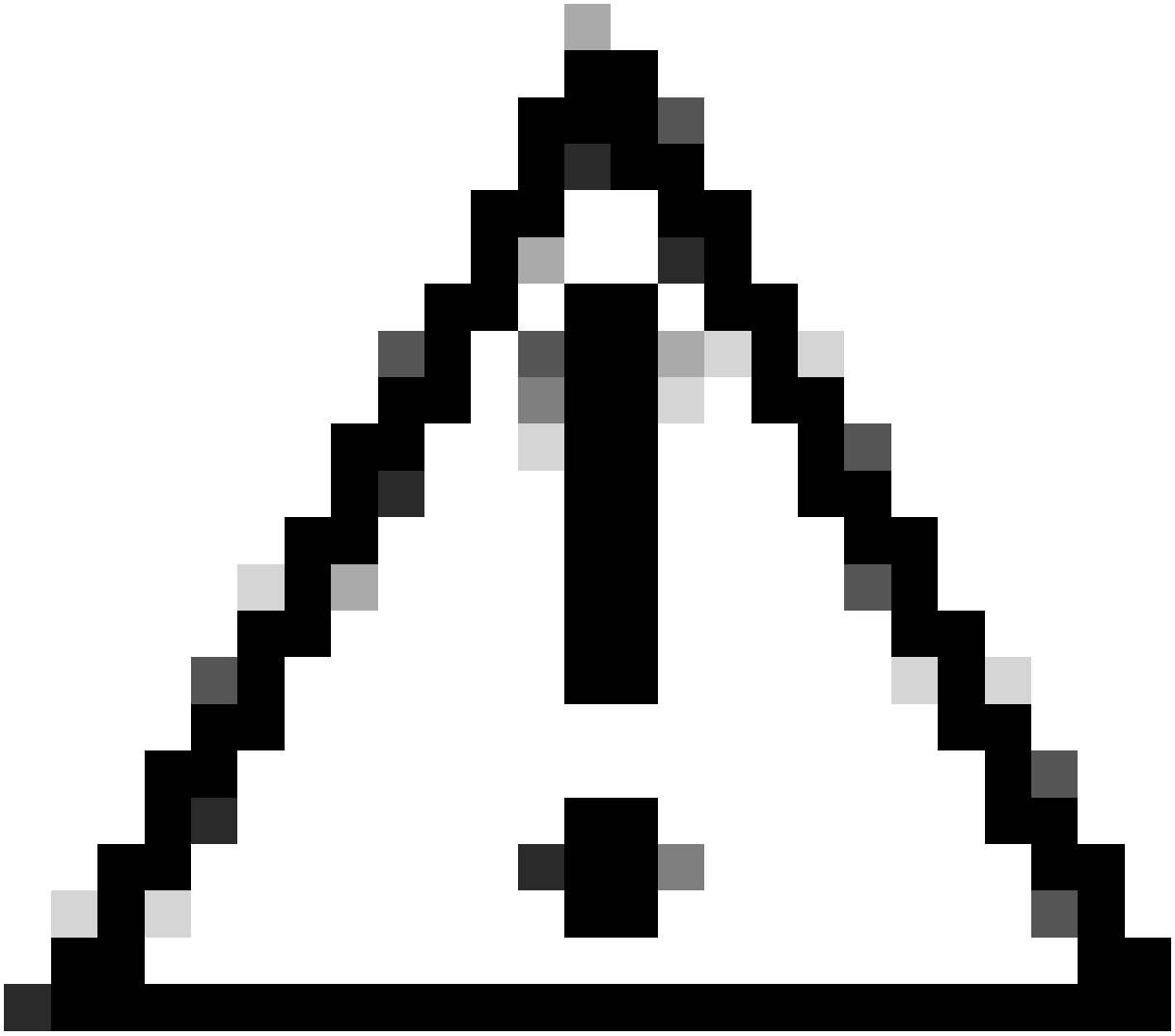
```
CGW#

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
```

Troubleshooting

Resolução de Endereços (ARP)

Etapas gerais para isolar problemas do ARP

- Confirme se o túnel IMET está pronto
- Capturar no Uplink do CGW para verificar o ARP recebido Encapsulado da Folha
- Se não for visto nenhum ARP chegando ao encap no uplink
  - Verifique se o túnel IMET está pronto em Leaf e CGW
  - Capturar em uplinks leaf para confirmar se o ARP foi encapsulado e enviado
  - Solucionar problemas de caminho intermediário
- Se o ARP chegar na captura de túnel Border IMET, mas não for programado na tabela ARP VRF
  - Solucionar problemas de caminho de punt CPU/CoPP para confirmar o ARP apontado para a CPU
  - Confirme se as informações de endereço IP/cliente estão corretas
  - Depurar o ARP no VRF para ver o que pode estar afetando o processo ARP
- Verificar o CGW MAC instalado como o próximo salto/destino MAC nos hosts
- Confirme se o CGW tem ambas as entradas ARP com os MACs de host reais
- Verificar se a política de firewall permite esse tipo de tráfego



Cuidado: tenha cuidado ao habilitar depurações!

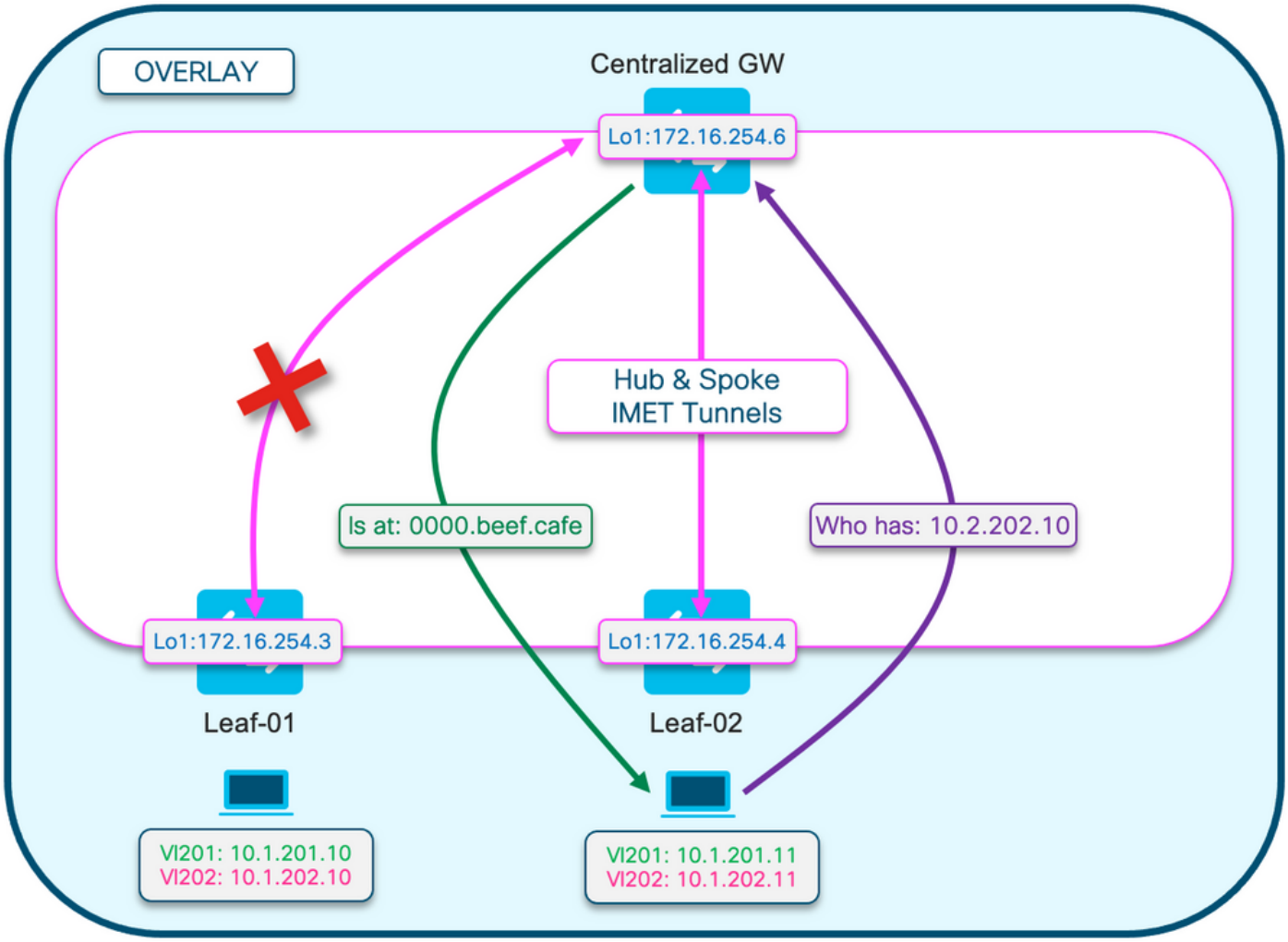
Verifique se você desabilitou a supressão de inundação

<#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
```

Quando o host da Folha-02 resolve o ARP para o host da Folha-01, a solicitação ARP não é transmitida diretamente para a Folha-01

- O ARP é passado pelo único túnel BUM programado na Leaf-02 em direção ao CGW
- O CGW não encaminha isso para Leaf-01 e, em vez disso, responde com seu próprio MAC
- Isso faz com que toda a comunicação seja passada para o CGW e, em seguida, roteada entre os hosts
- O CGW roteia pacotes, mesmo quando eles estão na mesma sub-rede local



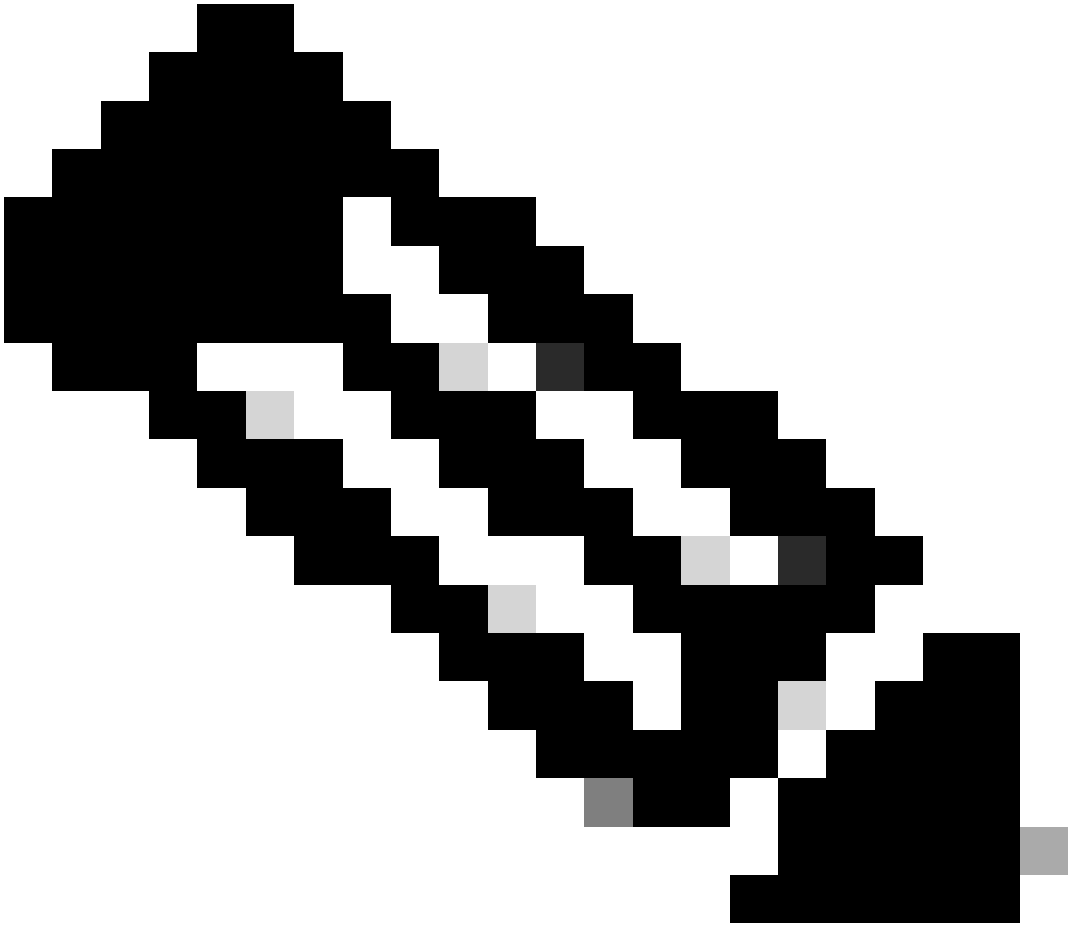
Este diagrama serve para ajudar a visualizar o fluxo do processo de resolução ARP descrito nesta seção.

A Solicitação ARP é exibida em roxo

- Essa solicitação ARP é para resolver o endereço MAC do host 10.1.202.10 fora da Leaf-01
- Observe que a linha roxa termina no CGW e não atinge Leaf-01

A Resposta ARP é mostrada em verde

- A resposta contém o MAC do SVI do CGW para a VLAN 202
- Observe que a linha verde vem do CGW, não do host real



Observação: o X vermelho indica que essa comunicação não envolveu o envio de tráfego para a Folha-01.

Observar as entradas ARP em 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 no CGW que os prefixos RT2 são aprendidos. Isso é necessário para que o CGW roteie pacotes

<#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
```

Capturar a troca ARP nos uplinks para confirmar a comunicação bidirecional

- Você pode usar o EPC (Embedded Packet Capture) nos uplinks de estrutura
- Este cenário mostra o EPC no uplink Leaf01. Repita esse mesmo processo no CGW, se necessário

Configurar o 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 a captura

```
<#root>

Leaf01#

monitor capture 1 start
```

Inicie o ping para disparar a solicitação ARP (Nesse caso, o ping é do host Leaf01 10.1.201.10 para o 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
```

Stop Capture & Check for the ARP frames (Parar captura e verificação dos quadros 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

Exiba os pacotes de captura em detalhes. Se você quiser ver mais informações sobre os pacotes, use a opção de detalhes do EPC

- Esteja ciente de que essa saída é cortada em vários lugares para ser breve

<#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

Prefixo do gateway CGW RT2

Prefixo de Gateway Ausente

Como mencionado na seção anterior sobre segmentos parcialmente isolados, o MAC deve ser aprendido na Vlan da estrutura

- Esse problema pode se manifestar se não houver tráfego destinado para o gateway por mais tempo do que o temporizador de envelhecimento MAC.
- Se o prefixo CGW Gateway estiver ausente, você precisará confirmar se o 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
```

Prefixo de Gateway Sem Correção

Na maioria das redes de produção, é provável que haja tráfego o tempo todo. No entanto, se você tiver esse problema, poderá usar uma destas opções para corrigi-lo:

- Adicione a entrada MAC estática como 'mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1'
- Aumente o temporizador de envelhecimento MAC com 'mac address-table aging-time <seconds>'. (Lembre-se de que isso aumenta o tempo de envelhecimento de todos os endereços MAC, portanto, a opção MAC estático é a preferida)

Atributo DEF GW ausente

Com os Segmentos Parcialmente Isolados, há várias configurações adicionais para adicionar esse atributo.

Falta correção do atributo DEF GW

Confirme estes detalhes:

- Você está executando 17.12.1 ou posterior
- A CLI do SISF (rastreamento de dispositivo) está presente na configuração
- Os comandos route-map match & set são configurados e route-map é aplicado aos vizinhos BGP
- Você atualizou os anúncios de BGP (você deve limpar o BGP para anunciar novamente o prefixo com o novo atributo

Roaming sem fio

O roaming frequente pode fazer com que o BGP atualize com muita frequência e o roaming por intervalo de tempo deve ser aumentado antes que o switch declare que é proprietário do MAC e

envie a Atualização RT2

- Isso ocorre quando um host se move entre dois APs que estão em switches diferentes.
- O limite padrão para roaming é de 5 a cada 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 a serem coletados para TAC

Caso este guia não resolva o problema, colete a lista de comandos mostrada e anexe-a à sua solicitação de serviço do TAC.

Informações mínimas para coletar

(tempo limitado para coletar dados antes da ação de recarregamento/recuperação)

- Mostrar de vpn técnico
- Show tech
- Mostrar sisf técnico

Informações detalhadas para coletar

(Se houver tempo para coletar dados mais completos, esta é a opção preferida)

- show tech
- show tech evpn
- show tech platform evpn_vxlan switch <número>
- 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
- solicitar arquivo de rastreamento de software de plataforma

Informações Relacionadas

- Implemente a política de roteamento BGP EVPN nos switches Catalyst 9000 Series
- Retransmissão de camada 2 do DHCP (em breve)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.