Catalyst 9000シリーズスイッチでのBGP EVPN保護オーバーレイセグメンテーションの実装

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

- 機能の概要
- ドキュメントの詳細
- 保護されたセグメントの種類
  - 完全に隔離
  - ほとんど隔離
- スイッチの動作
- ルートタイプ2の処理
- 設計の概要

用語

フロー図

- ルートタイプ2(RT2)の図
- ルートタイプ3(RT3)の図
- アドレス解決(ARP)ダイアグラム

設定（完全に分離）

- ネットワーク図
- Leaf-01（ベースEVPN設定）
- CGW（基本設定）

確認（完全に分離）

- EVIの詳細
- ローカルRT2生成（ローカルホストからRT2）
- リモートRT2ラーニング（デフォルトゲートウェイRT2）

構成（部分的に分離）

- ネットワーク図
- Leaf-01（ベースEVPN設定）
- CGW（基本設定）

検証（部分的に分離）

- EVIの詳細
- ローカルRT2生成（ローカルホストからRT2）
- リモートRT2ラーニング（デフォルトゲートウェイRT2）
  - CGWデフォルトゲートウェイプレフィクス（リーフ）

FED MATM (リーフ)
SISF(CGW)
IOS MATM(CGW)
トラブルシュート
アドレス解決(ARP)
CGW RT2ゲートウェイプレフィックス
ワイヤレスローミング
TAC用に収集すべきコマンド
関連情報

はじめに

このドキュメントでは、Catalyst 9000シリーズスイッチにBGP EVPN VXLAN Protected Overlay Segmentation(PPTP)を実装する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- BGP EVPN VxLANの概念
- BGP EVPNユニキャストのトラブルシューティング
- BGP EVPN VxLANルーティングポリシー

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1以降のバージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

機能の概要

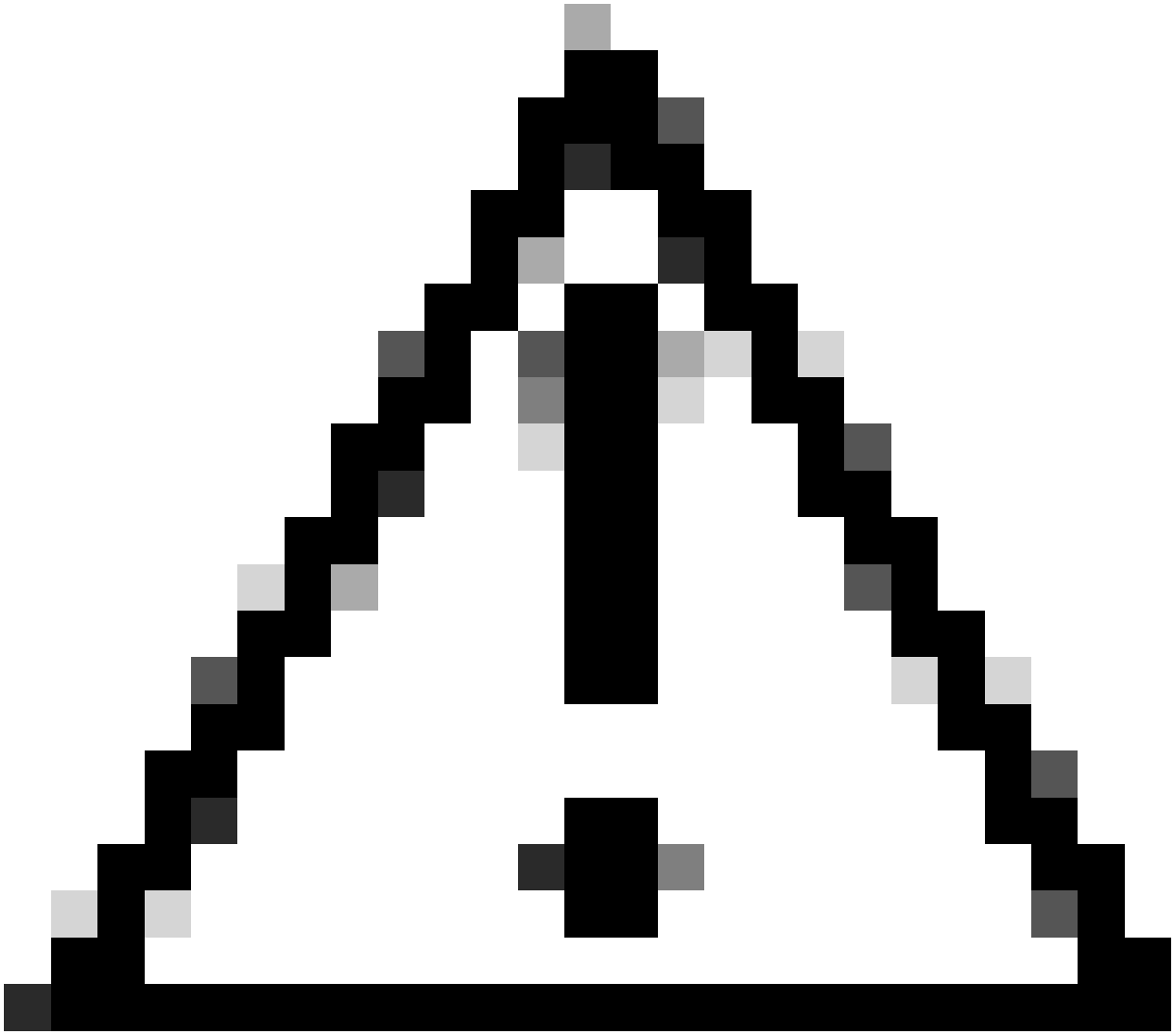
保護セグメント機能は、ポートが同じVLANおよび同じスイッチ上にある場合でも、ポート間でのトラフィックの転送を防止するセキュリティ対策です

- この機能は、「switchport protected」またはプライベートVLANに似ていますが、EVPNファブリック用です。
- この設計では、最終的な宛先に送信される前に、ファイアウォールによる検査が可能なCGWへのすべてのトラフィックが強制されます。
- トラフィックフローは、制御され、決定論的で、中央集中型セキュリティアプライアンスを使用して検査が容易です。

ドキュメントの詳細

このドキュメントは、第2部または第3部の相互に関連するドキュメントです。

- ドキュメント1:Catalyst 9000シリーズスイッチでのBGP EVPNルーティングポリシーの実装」には、オーバーレイでのBGP BUMトラフィックの制御方法が記載されており、最初に設定する必要があります
- ドキュメント2:このドキュメント。このドキュメントでは、ドキュメント1のオーバーレイ設計とポリシーに基づいて、「protected」キーワードの実装について説明します
- ドキュメント3:Catalyst 9000シリーズスイッチでのBGP EVPN DHCPレイヤ2リレーの実装」には、L2専用VTEPでDHCPリレーがどのように動作するかが記載されています



注意：保護セグメント設定を実装する前に、ドキュメント1の設定を実装する必要があります。

保護されたセグメントの種類

完全に隔離

- 北から南への通信のみを許可
- ゲートウェイは、「default-gateway advertise」CLIを使用してファブリックにアドバタイズされます

ほとんど隔離

- 北から南への通信を許可します（この使用例では、ファイアウォールトラフィックポリシーに基づいて東/西のトラフィックフローが許可されます）
- 水平方向の通信を許可（ファイアウォールトラフィックポリシーに基づく）

- ゲートウェイがファブリックの外部にあり、「default-gateway advertise」CLIを使用してSVIがアドバタイズされない

スイッチの動作

- ホストは、同じスイッチに接続されていても相互に直接通信できません（ホストが同じVRF/Vlan/セグメント内にある場合、ARP要求は同じスイッチ上の他のポートに送信されません）
- L2 VTEP(ルーティングポリシー設定を使用してフィルタリングされたIMETプレフィクス)間のBUMトラフィックなし
- ホストからのすべてのパケットは、転送されるボーダーリーフにリレーされます。（これは、ホスト1が同じリーフ上のホスト2と通信することを意味します。トラフィックはCGWにヘアピニングされます）

ルートタイプ2の処理

- アクセスリーフは、E-Tree Extended Communityとリーフフラグが設定されたローカルRT2をアドバタイズます。
- アクセスリーフは、データプレーンでE-Tree Extended Communityとリーフフラグが設定されたリモートRT2をインストールしません
- アクセスリーフは、データプレーンに互いにRT2をインストールしません
- アクセスリーフとボーダーリーフ(CGW)は、データプレーンで互いにRT2をインストールします
- アクセスリーフまたはボーダーリーフでは、設定変更は必要ありません。

設計の概要

- ブロードキャスト(BUM)の場合、ARPなどのブロードキャストトラフィックをGCWまで強制するために、RT3トポロジはハブアンドスポークです。
- ホストのモビリティを考慮すると、RT2はBGPコントロールプレーンでフルメッシュ構造になっています（ホストがあるVTEPから別のVTEPに移動すると、RT2のシーケンス番号が増分されます）
- データプレーンは選択的にMACアドレスをインストールします。
    - リーフは、DEF GW属性を含むローカルMAC & RT2のみをインストールします
    - CGWには保護されたKWがなく、すべてのローカルMACとリモートRT2をデータプレーンにインストールします。

用語

VRF	仮想ルーティング転送	他のVRFおよびグローバルIPv4/IPv6ルーティングドメインから分離されたレイヤ3ルーティングドメインを定義する
AF	アドレスファミリ	BGPが処理するプレフィックスとルーティング情報のタイプを定義します。

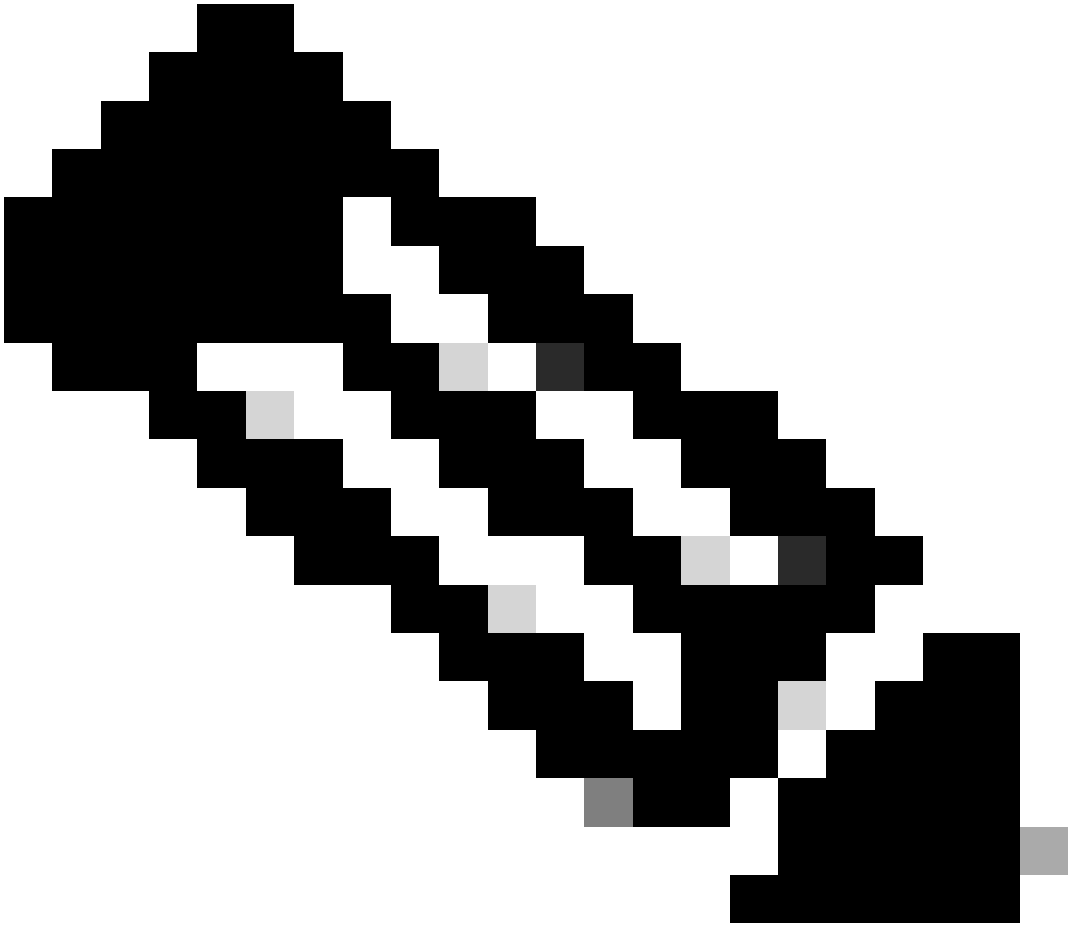
AS	自律システム	ネットワークまたはネットワークの集合に属し、単一のエンティティまたは組織によってすべて管理、制御、および監視される一連のインターネットルーティング可能なIPプレフィクス
EVPN	イーサネット仮想プライベートネットワーク	BGPにレイヤ2 MACおよびレイヤ3 IP情報の転送を許可する拡張はEVPNであり、VXLANオーバーレイネットワークに関連する到達可能性情報を配布するプロトコルとしてマルチプロトコルボーダーゲートウェイプロトコル(MP-BGP)を使用します。
VXLAN	仮想拡張LAN（ローカルエリアネットワーク）	VXLANは、VLANとSTPに固有の制限を克服するように設計されています。VLANと同じイーサネットレイヤ2ネットワークサービスを提供するIETF標準[RFC 7348]として提案されていますが、柔軟性に優れています。機能的には、レイヤ3アンダーレイネットワーク上で仮想オーバーレイとして動作するMAC-in-UDPカプセル化プロトコルです。
CGW	中央集中型ゲートウェイ	ゲートウェイSVIが各リーフ上にない場合のEVPNの実装。その代わり、すべてのルーティングは非対称IRB(Integrated Routing and Bridging)を使用して特定のリーフによって実行されます
DEF GW	[Default Gateway]	BGP拡張コミュニティアトリビュートが、「l2vpn evpn」設定セクションで「default-gateway advertise enable」コマンドを使用してMAC/IPプレフィクスに追加された。
IMET(RT3)	包括マルチキャストイーサネットタグ（ルート）	BGPタイプ3ルートとも呼ばれます。このルートタイプは、VTEP間でBUM（ブロードキャスト/不明ユニキャスト/マルチキャスト）トラフィックを配信するためにEVPNで使用されます。
RT2	ルートタイプ2	ホストMACまたはゲートウェイMAC-IPを表すBGP MACまたはMAC/IPプレフィクス
EVPNマネージャ	EVPNマネージャ	その他のさまざまなコンポーネントの中央管理コンポーネント（例：SISFから学習し、L2RIBに信号を送信）
SISF	スイッチ統合セキュリティ機能	リーフ上に存在するローカルホストを学習するためにEVPNによって使用される非依存のホストトラッキングテーブル
L2リブ	レイヤ2ルーティング情報	BGP間のインタラクションを管理するための中間コンポーネント、EVPN Mgr、L2FIB

	ベース	
FED	転送エンジンドライバ	ASIC（ハードウェア）層をプログラムする
マトム	Macアドレステーブルマネージャ	IOS MATM：ローカルアドレスと FED MATM：コントロールプレーンから学習したローカルアドレスとリモートアドレスをインストールするハードウェアテーブル。ハードウェアフォワーディングプレーンの一部です。

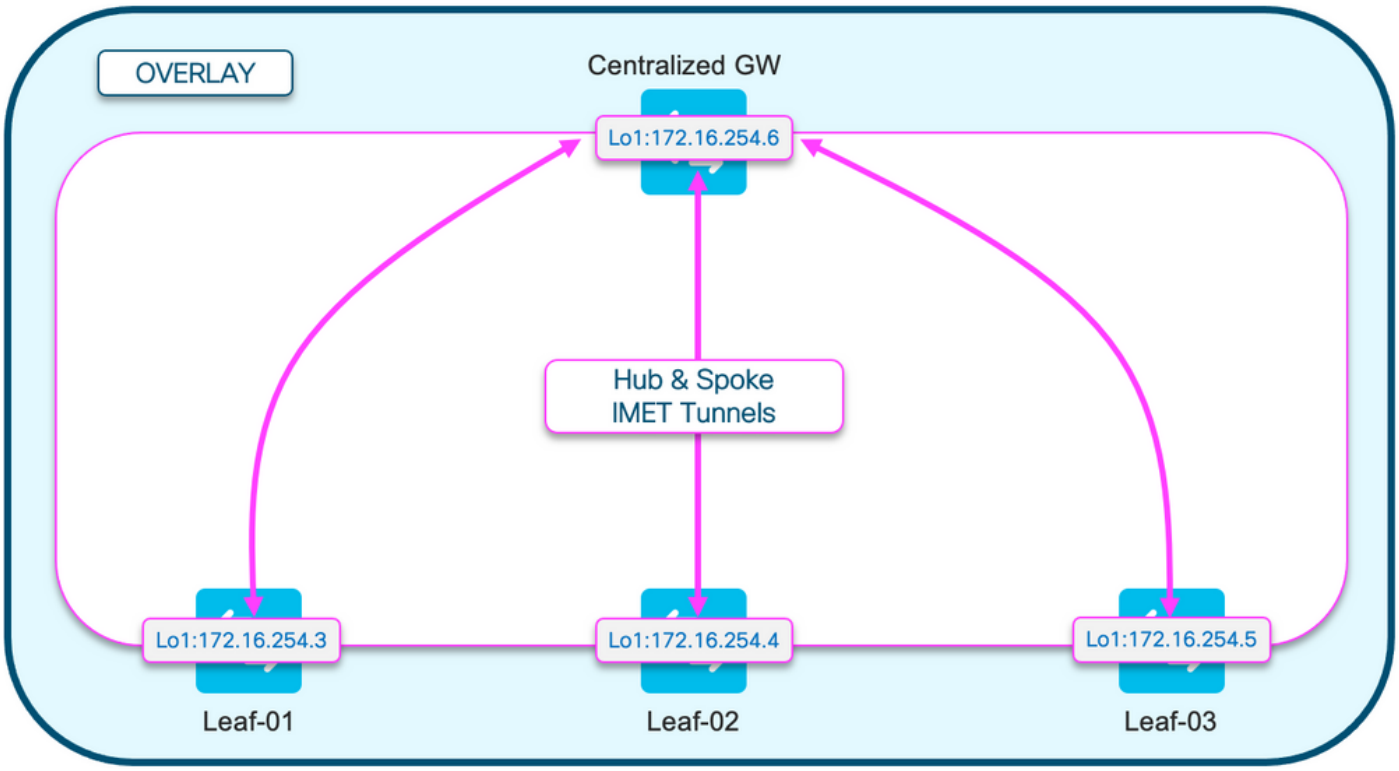
フロー図

ルートタイプ2(RT2)の図

次の図は、タイプ2 MAC/MAC-IPホストプレフィクスのフルメッシュ設計を示しています。

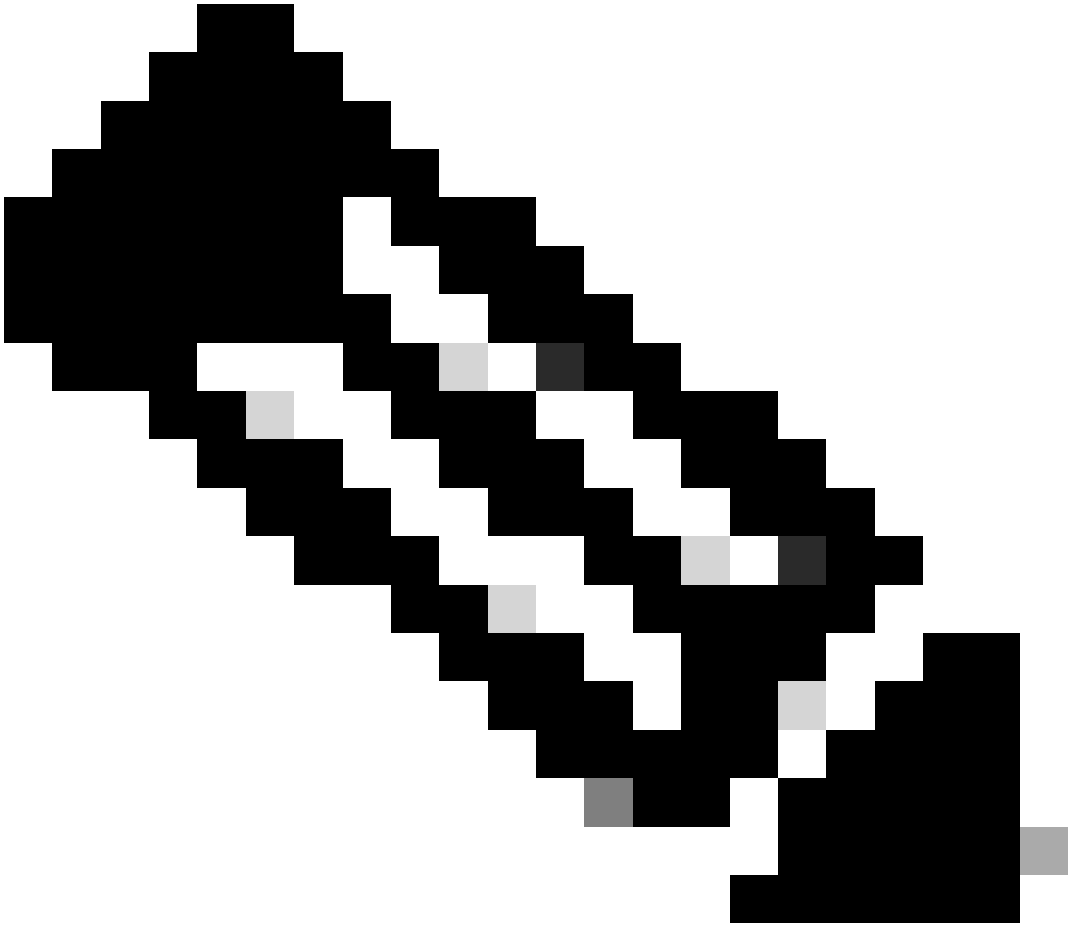


注：モビリティとローミングをサポートするにはフルメッシュが必要です

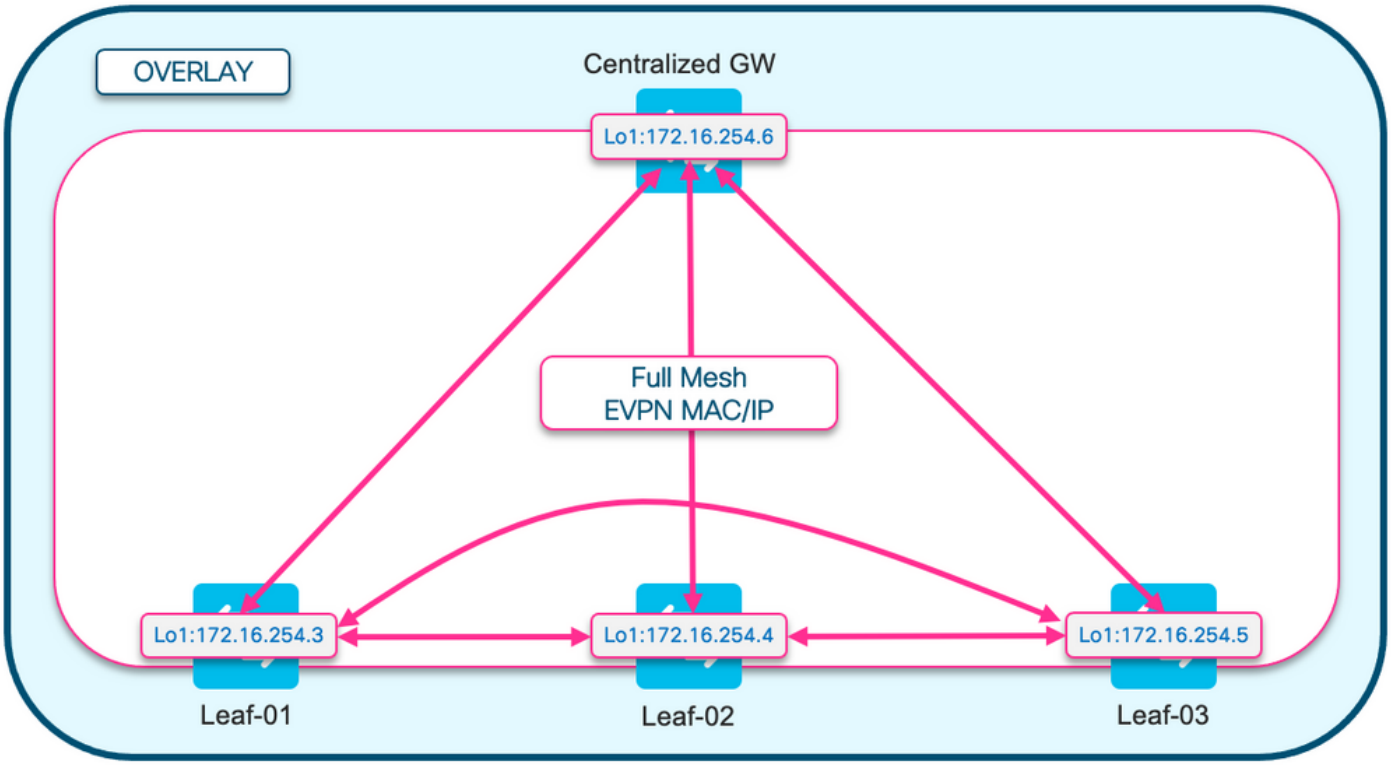


ルートタイプ3(RT3)の図

次の図は、ブロードキャストIMET(RT3)トンネルのハブアンドスポーク設計を示しています

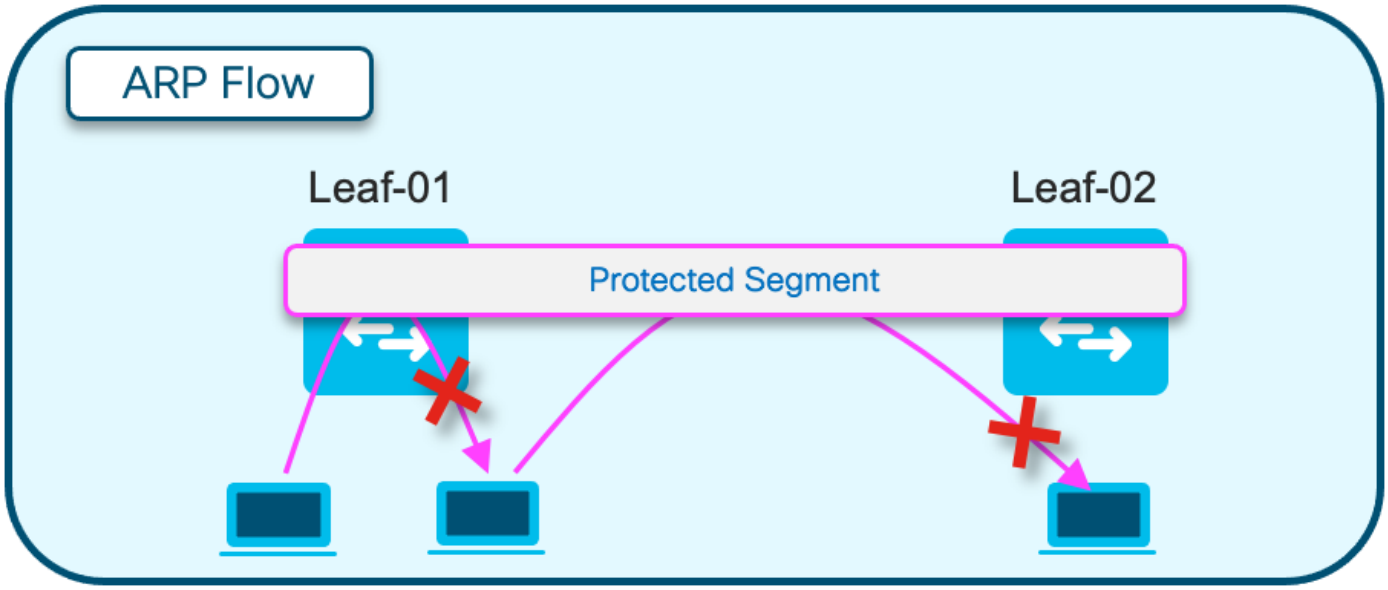


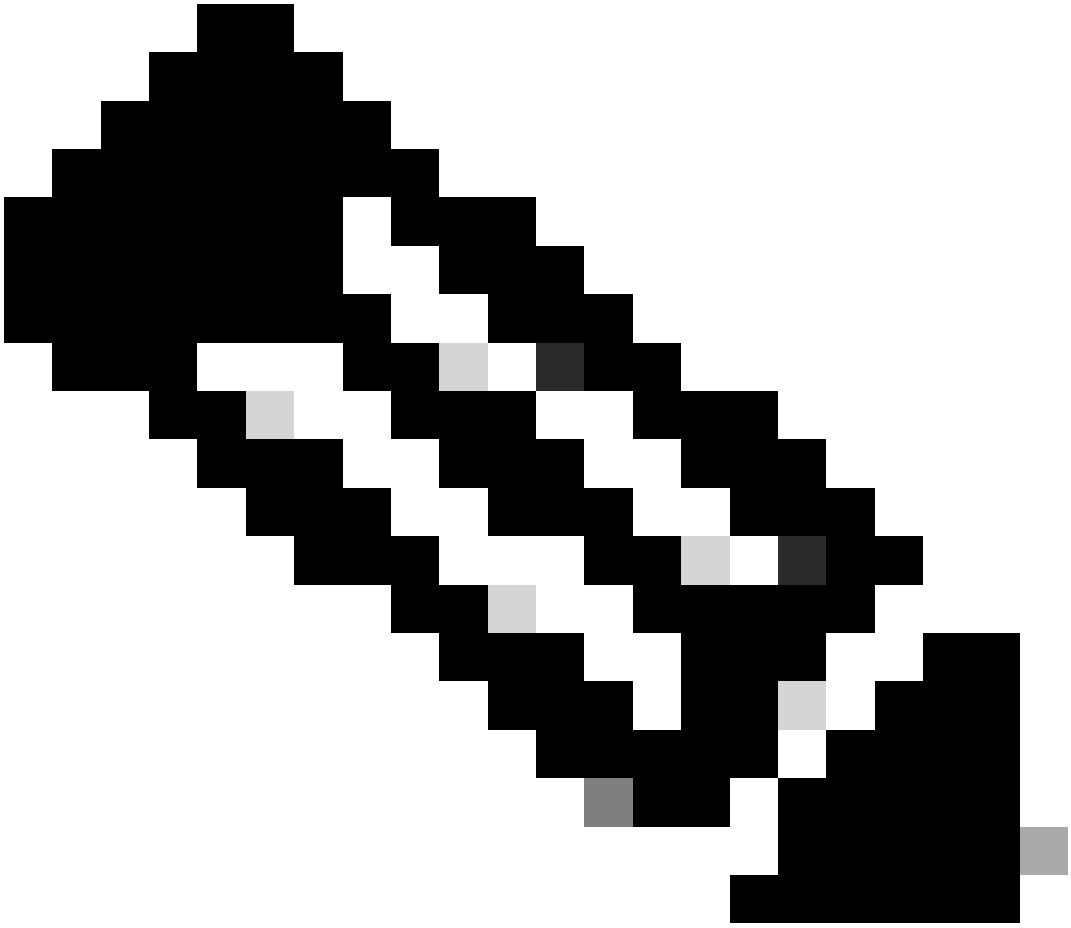
注：ハブアンドスポークブロードキャストは、同じセグメントを持つリーフが相互にブロードキャストを直接送信するのを防ぐために必要です。



アドレス解決(ARP)ダイアグラム

次の図は、ARPが同じEPVNセグメント内のどのホストにも到達できないことを示しています。別のホストのホストARPでは、CGWだけがこのARPを取得して応答します



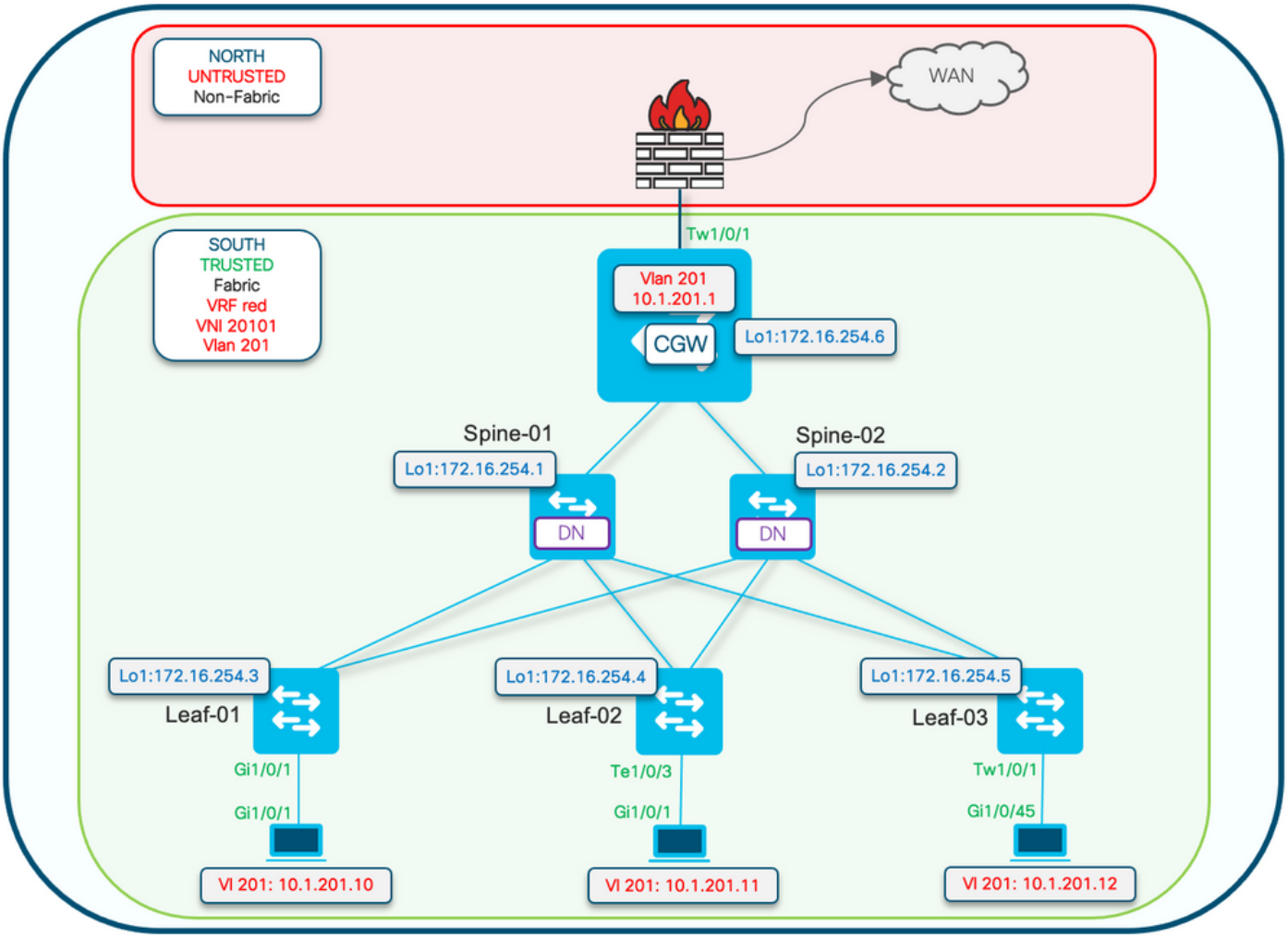


注：このARP動作の変更は、「protected」キーワードを使用してインスタンス化されます。

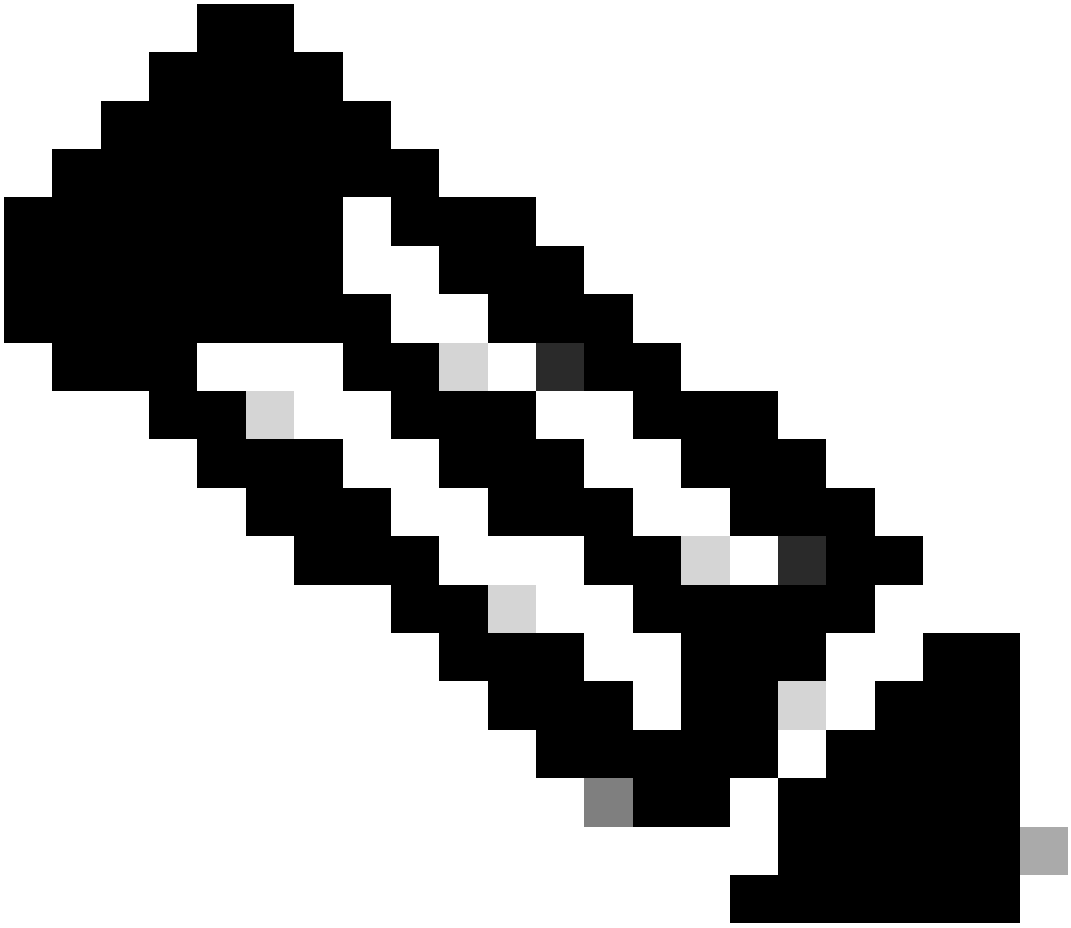
例：member evpn-instance 202 vni 20201 protected

設定（完全に分離）

ネットワーク図



保護された設定キーワードがリーフスイッチに適用されている。CGWは混合デバイスで、すべてのMACアドレスをインストールします。



注：IMETプレフィクスのインポート/エクスポートを制御するルーティングポリシーコミュニティリストおよびルートマップの設定については、『Catalyst 9000シリーズスイッチでのBGP EVPNルーティングポリシーの実装』を参照してください。 このドキュメントでは、保護されたセグメントの違いのみを示します。

Leaf-01（ベースEVPN設定）

<#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（基本設定）

<#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
```

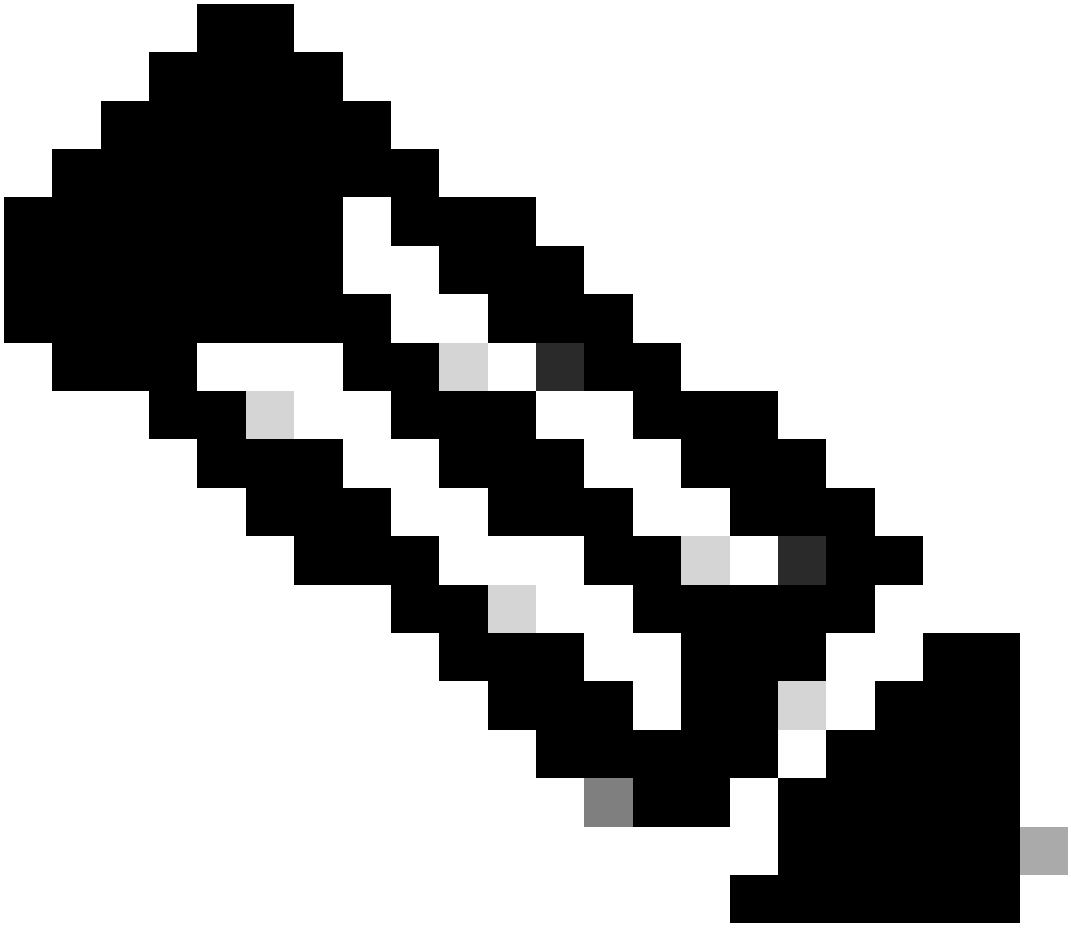
<#root>

```
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
```



注:CGWでは、適用されるBGPポリシーはありません。CGWは、すべてのプレフィックスタイプ(RT2、RT5/RT3)の送受信を許可されています。

確認（完全に分離）

EVIの詳細

<#root>

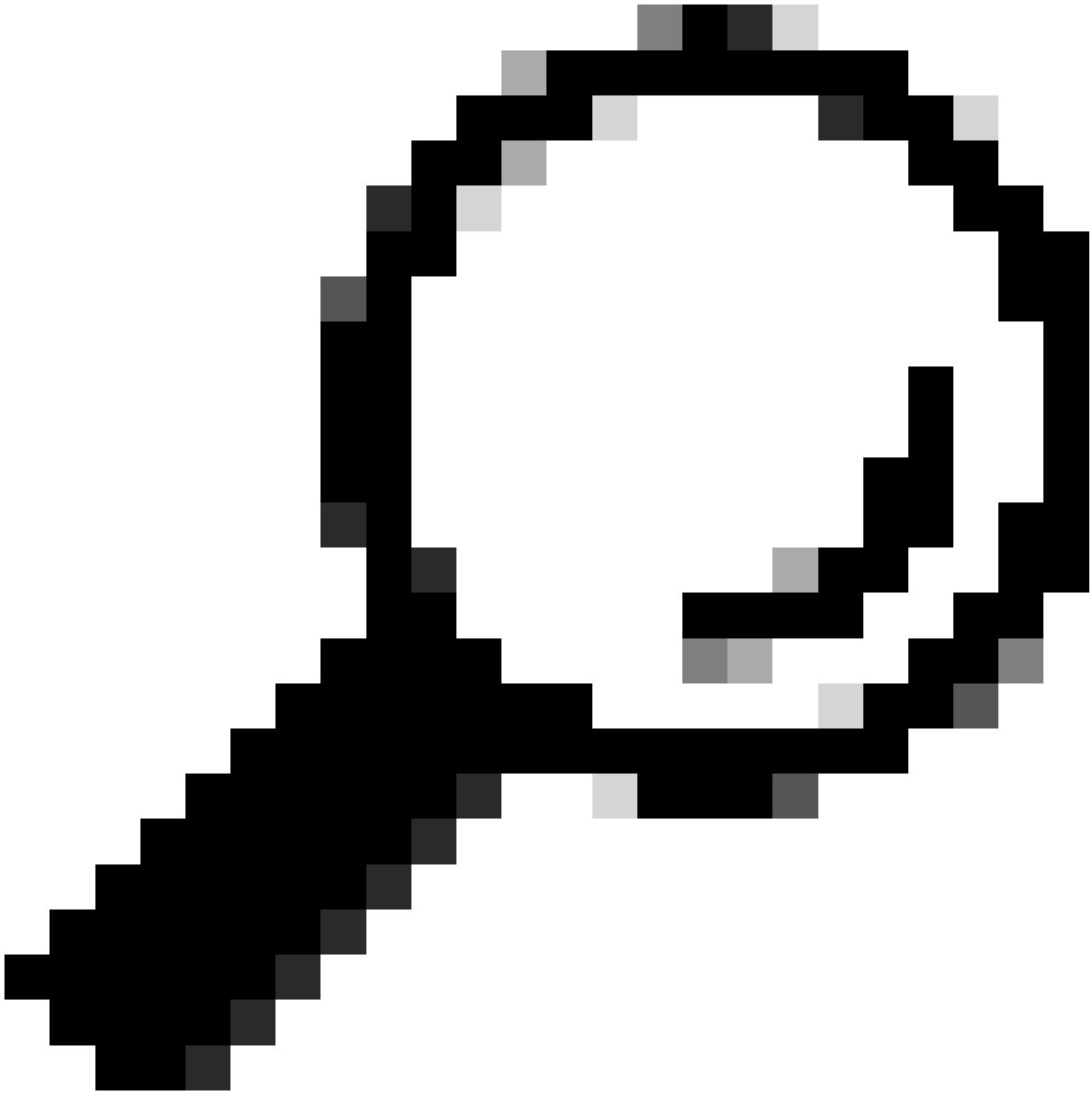
```
Leaf01#

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...>
```

ローカルRT2生成（ローカルホストからRT2）

ローカルホストの学習からRT2の生成までのコンポーネントの依存関係チェーンを確認します。

- SISF（リーフにはSVIがありませんが、SISFは引き続きホストからのARPフレームを介してホスト情報を収集します）
- EVPNマネージャ
- L2リブ
- BGP

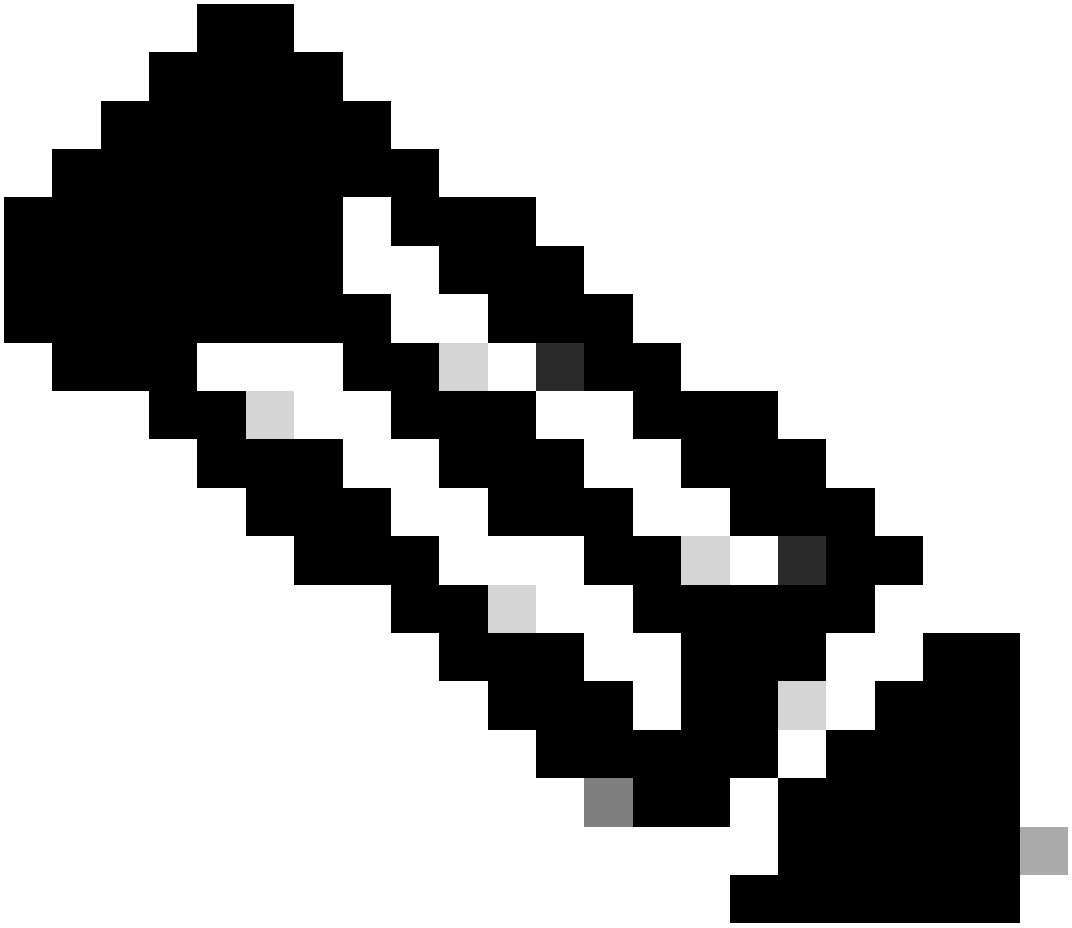


ヒント：前のコンポーネントが適切にプログラムされていない場合、依存関係チェーン全体が壊れます（例：SISFにenエントリがない場合、BGPはRT2を作成できません）。

SISF

SISFがホストをDBで学習したことを確認します（ホスト情報はDHCPまたはARPから学習しました）。

- SISFはIOS-MATMラーニングからMACエントリを学習し、EVPN Mgrに送信します（ポリシー「evpn-sisf-policy」でMAC到達可能である必要があります）
- SISFは、ローカルVTEP上のIP/MACバインディングを収集し、EVPNマネージャを使用して、その情報が他のリーフへのBGPを介した/32ルートとしてプログラムされることが想定されます。



注：このシナリオでは、ホストにスタティックIPがあるため、SISFはARPを使用してホストの詳細を収集します。「最も隔離された」セクションに、DHCPとDHCPスヌーピングが示されています。

<#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
```

EVPNマネージャ

EVPN MgrはローカルMACを学習し、L2RIBにインストールします。EVPN MgrもL2RIBからリモートMACを学習しますが、エントリはMACモビリティの処理にのみ使用されます

EVPN MgrがSISFエントリで更新されていることを確認します。

```
<#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...>
```

L2リブ

- L2RIBはEVPN MgrからローカルMACを学習し、BGPとL2FIBに送信する
- L2RIBは、EVPN MgrとL2FIBを更新するために、BGPからリモートMACを学習する役割も担います。
- L2RIBでは、他のコンポーネントを正しくアップデートするために、ローカルとリモートの両方が必要です。 0.
- L2RIBコンポーネントは、更新が必要な方向/コンポーネントに応じて、ローカルとリモートのMACラーニングの間に配置されます

0.

L2RIBがEVPN MgrからのローカルMACで更新されていることを確認します。

```
<#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

L2RIBによるBGPの更新の確認

<#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
```

リモートRT2ラーニング（デフォルトゲートウェイRT2）

BGP

BGPがCGW RT2プレフィックスを学習したことを確認します

<#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 11411
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
```

L2リブ

BGPで更新されたL2RIBの確認

- L2RIBはEVPNマネージャからローカルMACを学習し、BGPとL2FIBに送信します。 L2RIBは、EVPN MgrとL2FIBを更新するために、BGPからリモートMACを学習する役割も担います。
- L2RIBでは、他のコンポーネントを正しくアップデートするために、ローカルとリモートの両方が必要です。 0.
- L2RIBコンポーネントは、どの方向とコンポーネントを更新する必要があるかによって、ローカルMACラーニングとリモートMACラーニングの間に位置します。

<#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

L2FIBでの確認

- FEDをMACで更新してハードウェアでプログラムするコンポーネント。
- L2FIBによってFED-MATMにインストールされたリモートMACエントリは、IOS-MATMにパントされません（IOS-MATMはローカルMACのみを表示し、FED-MATMはローカルとリモートの両方のMACを表示します）
- L2FIB出力はリモートMACのみを示します（ローカルMACをプログラミングする責任はありません）。

<#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

FED MATMでの確認

- 「protected keyword」で設定されたリーフのハードウェアレベルでは、CGWのデフォルトゲートウェイのMACとローカルホストのMACのみが表示されます。
- スイッチは、DEF GW属性のRT2プレフィックスを参照して、インストールに適格なリモートMACを判別します。

<#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
```

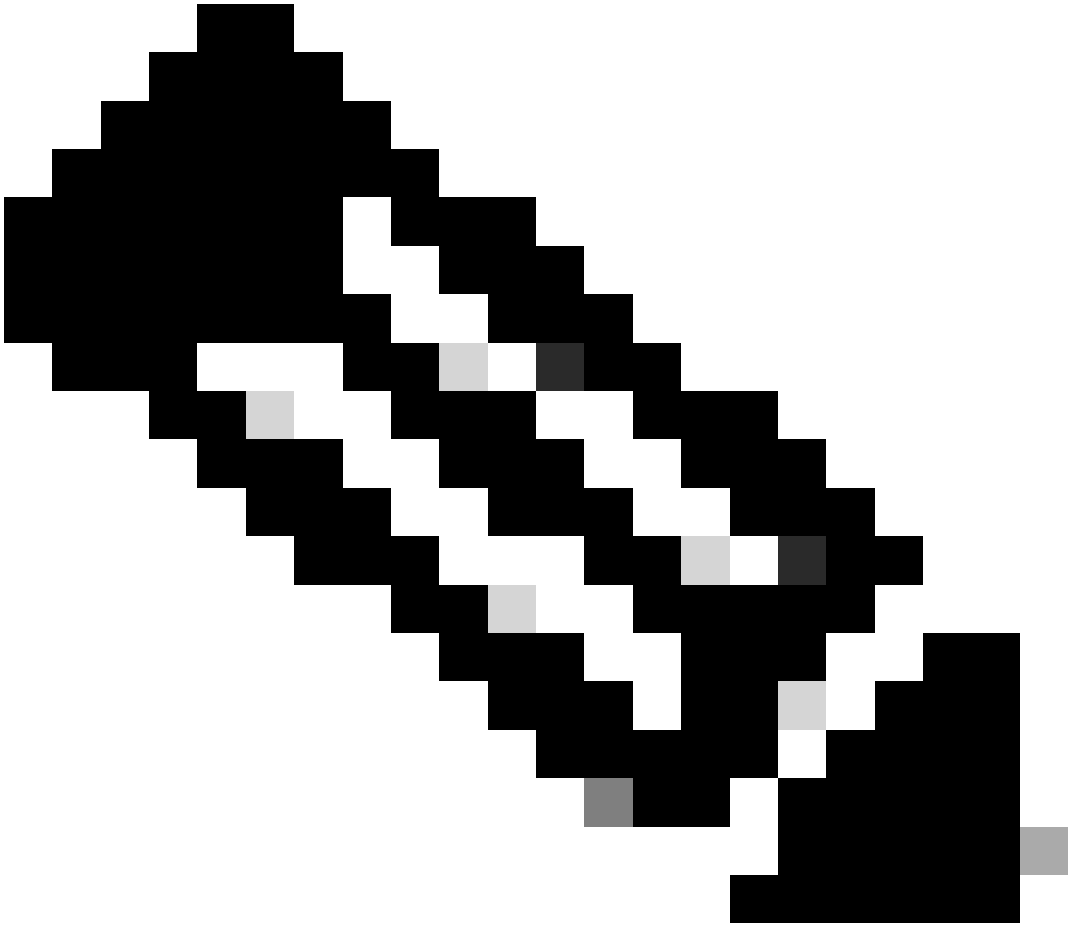
```
MAT_LISP_GW_ADDR 0x4000000
MAT_DYNAMIC_ADDR 0x1
```

データプレーン隣接関係

FEDエントリを確認した後の最後のステップとして、書き換えインデックス(RI)を解決できます

<#root>

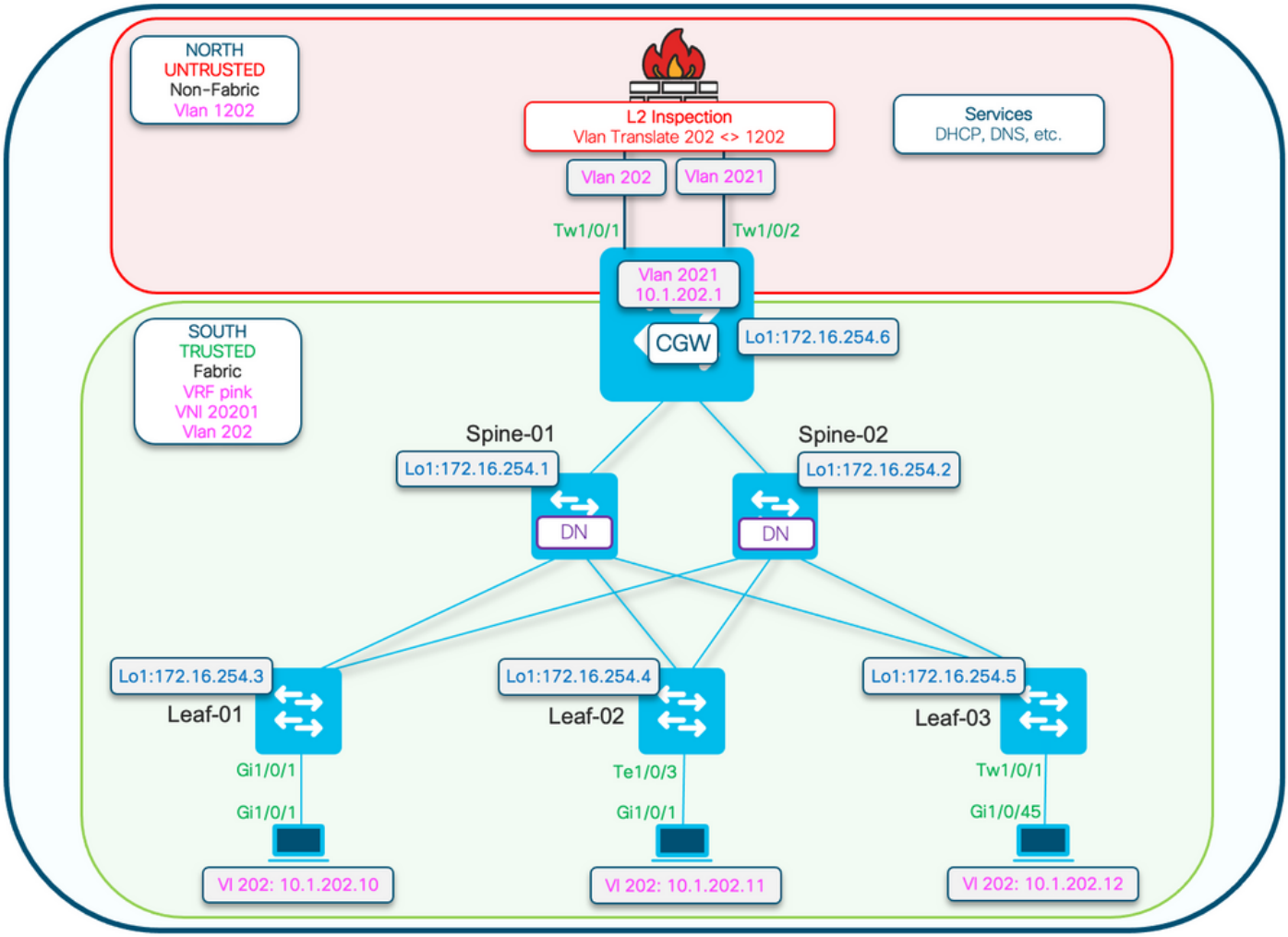
```
Leaf01#

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)
```

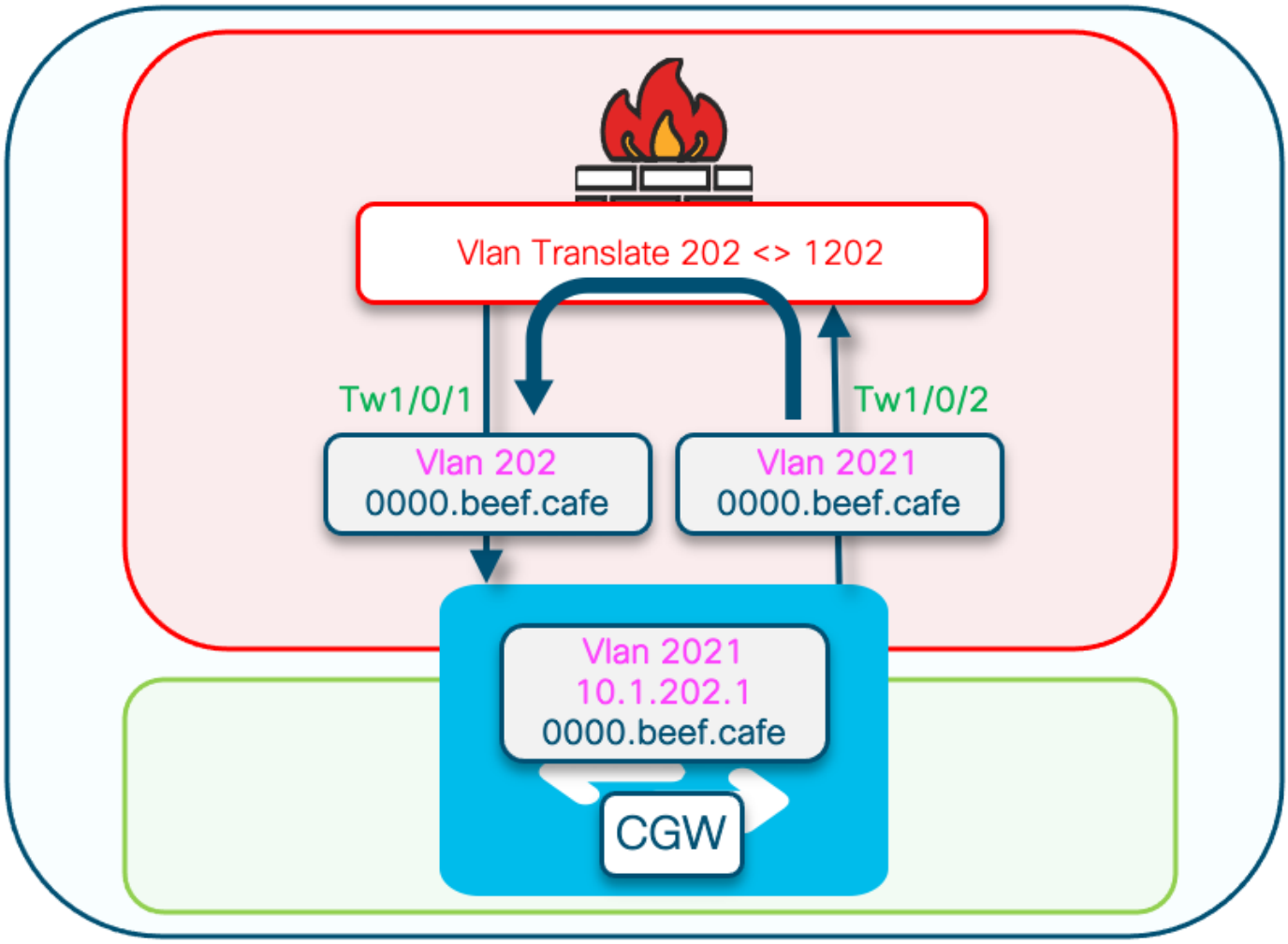


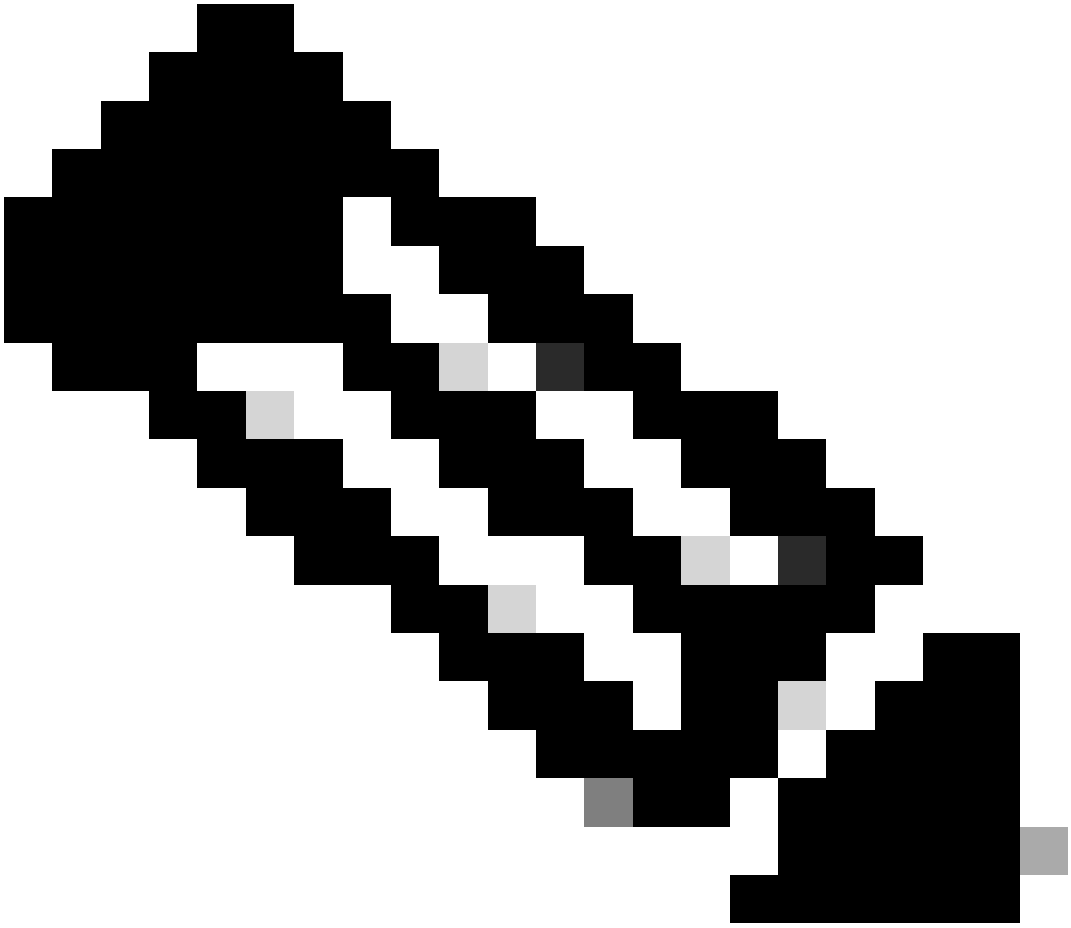
注：このコマンドとFEDコマンドを1つの結果にまとめる「show platform software fed switch active matm macTable vlan 201 detail」を使用することもできます

構成（部分的に分離）

ネットワーク図


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



注：このセクションでは、完全に隔離されたセグメントとの違いのみを取り上げます。

- GCWゲートウェイMAC IPにDEF GW属性をマーキングするルーティングポリシー
- MACフラップを防ぐためにカスタムデバイストラッキングポリシーが必要
- GW MAC IPのスタティックデバイストラッキングバインディング

Leaf-01（ベースEVPN設定）

<#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（基本設定）

nveでレプリケーションモードを設定します

<#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
```

外部ゲートウェイSVIの設定

<#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
```

収集を無効にしてポリシーを作成します

<#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
```

Attach to 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
```

externalgateway mac-ipのデバイストラッキングテーブルにスタティックエントリを追加します

<#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
```

RT2 MAC-IPプレフィクスに一致するBGPルートマップを作成し、デフォルトゲートウェイのextendedcommunityを設定します。

<#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
```

BGPルートリフレクタネイバーへのルートマップの適用

<#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
```

検証（部分的に分離）

EVIの詳細

<#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...>
```

ローカルRT2生成（ローカルホストからRT2）

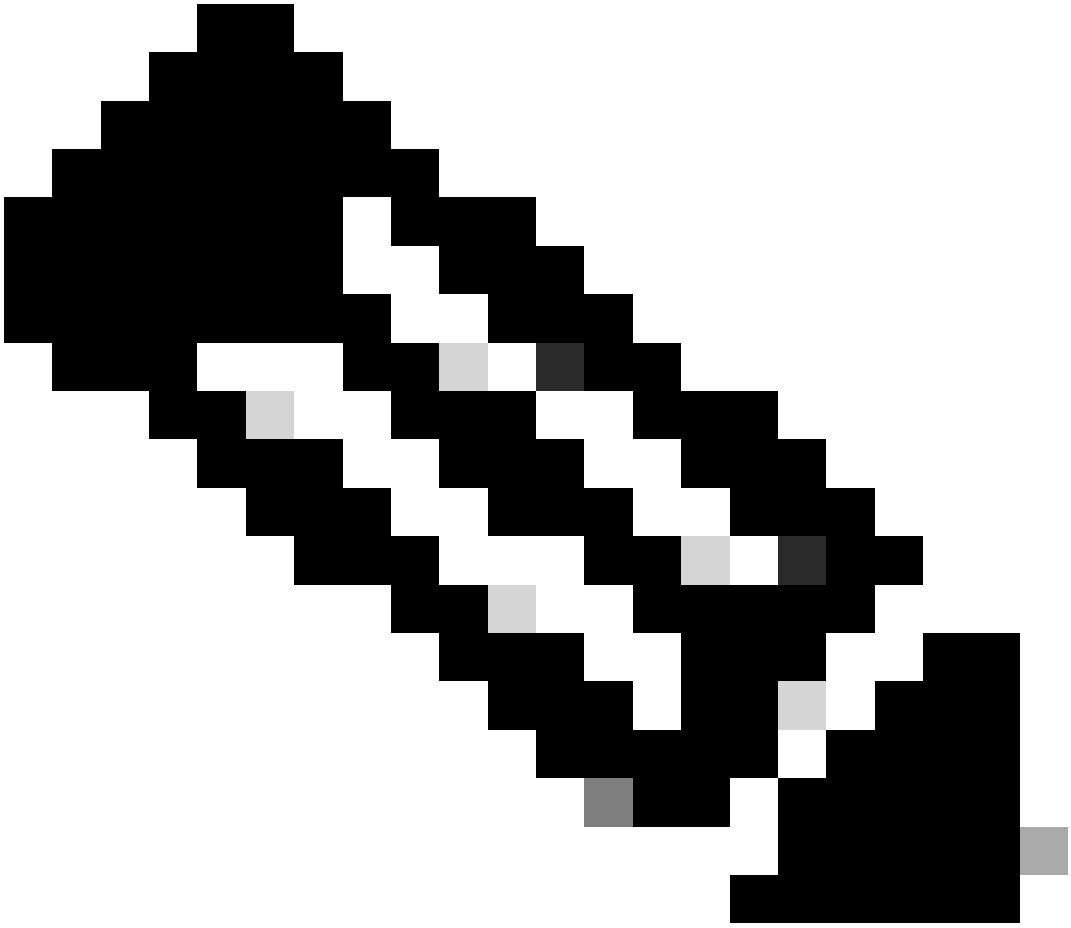
前の完全に分離された例で説明

リモートRT2ラーニング（デフォルトゲートウェイRT2）

完全に隔離された状態との違いをカバー

CGWデフォルトゲートウェイプレフィクス（リーフ）

ハードウェアにインストールする資格を得るために、プレフィクスに適切な属性があることを確認します



注：これはDHCP L2リレーを機能させるために重要です

<#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 (リーフ)

<#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>

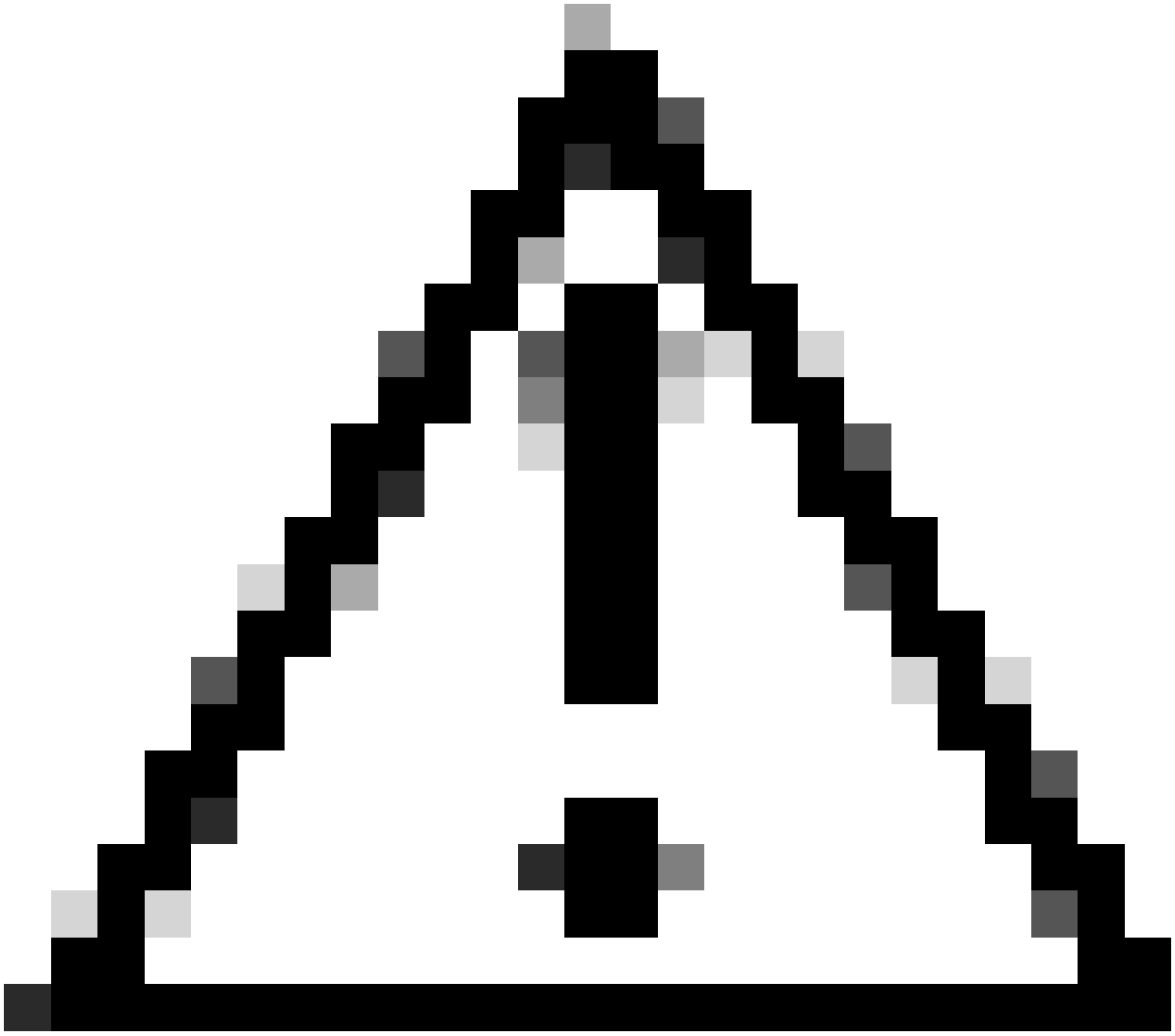
```
CGW#

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
```

トラブルシュート

アドレス解決(ARP)

ARPの問題を切り分けるための一般的な手順

- IMETトンネルの準備が整っていることを確認します。
- リーフからカプセル化されて受信されたARPを確認するためのCGWアップリンクでのキャプチャ
- ARPがアップリンクにカプセル化されない場合
  - リーフとCGWの両方でIMETトンネルの準備が整っていることを確認する
  - リーフアップリンクでキャプチャし、ARPがカプセル化されて送信されていることを確認する
  - 中間パスのトラブルシューティング
- ARPが境界IMETトンネルに到着したが、VRF ARPテーブルにプログラムされていない場合
  - CPU/CoPPパントパスのトラブルシューティングを行い、ARPがCPUにパントされたことを確認する
  - IPアドレス/クライアント情報が正しいことを確認する
  - VRFでのARPのデバッグによるARPプロセスへの影響の確認
- ホストにネクストホップ/宛先MACとしてインストールされているCGW MACを確認します。
- CGWに実ホストMACの両方のARPエントリがあることを確認します。
- ファイアウォールポリシーでこのタイプのトラフィックが許可されていることを確認します



注意：デバッグを有効にする際には注意が必要です。

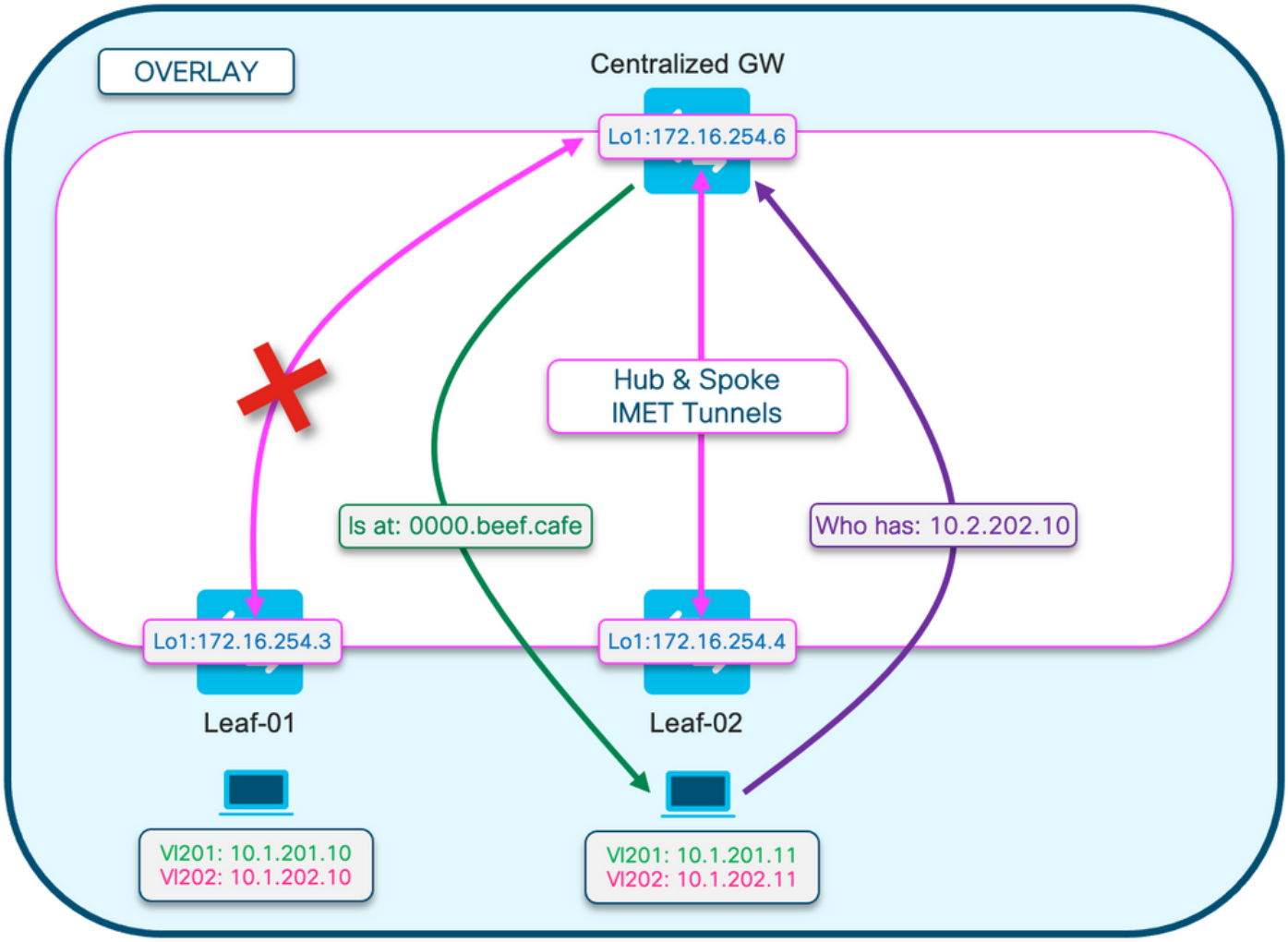
フラッディング抑制を無効にしたことを確認します

<#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
```

Leaf-02のホストがLeaf-01のホストのARPを解決すると、ARP要求はLeaf-01に直接ブロードキャストされません

- その代わり、ARPは、Leaf-02でプログラムされたCGWへの唯一のBUMトンネルとして渡されます
- CGWはこれをLeaf-01に転送せず、代わりに自身のMACで応答します
- これにより、すべての通信がCGWに渡され、ホスト間にルーティングされます
- CGWは、同じローカルサブネット上にある場合でも、パケットをルーティングします



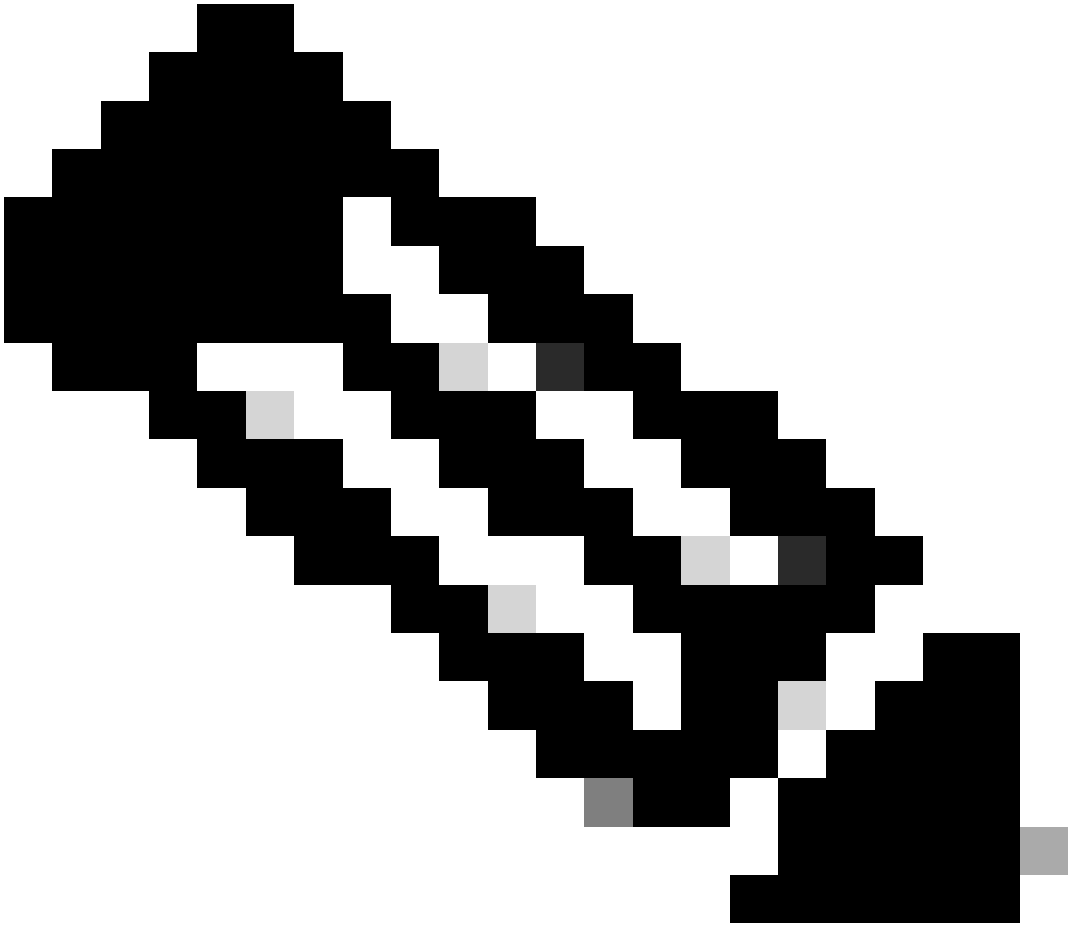
次の図は、このセクションで説明するARP解決プロセスのフローを視覚化するために役立ちます。

ARP要求は紫色で表示されます

- このARP要求は、ホスト10.1.202.10のMACアドレスをLeaf-01から解決することです
- 紫色の回線はCGWで終端し、Leaf-01には到達していないことに注意してください

ARP応答は緑色で表示されます

- 応答には、Vlan 202のCGW SVIのMACが含まれています
- 緑色の回線は、実際のホストからではなく、CGWから発信されていることに注意してください



注：赤いXは、この通信にリーフ–01へのトラフィックの送信が含まれていないことを示します。

各ホストのARPエントリを確認します

<#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

CGWでRT2プレフィックスが学習されることを確認します。これは、CGWがパケットをルーティングするために必要です

<#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
```

アップリンクでのARP交換をキャプチャして、双方向通信であることを確認します

- ファブリックアップリンクで組み込みパケットキャプチャ(EPC)を使用できます
- このシナリオでは、Leaf01アップリンクのEPCを示します。必要に応じて、CGWでこの同じプロセスを繰り返します

EPCの設定

```
<#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
```

キャプチャの開始

```
<#root>

Leaf01#

monitor capture 1 start
```

ARP要求をトリガーするためにpingを開始します（この例では、pingはLeaf01ホスト10.1.201.10からLeaf02ホスト10.1.201.11に対して実行されます）

```
<#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
```

キャプチャの停止とARPフレームのチェック

<#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
```

キャプチャパケットの詳細を表示します。パッケージに関する詳細情報を表示するには、EPCのdetailオプションを使用します

- この出力は、簡略化するためにさまざまな場所でクリップされていることに注意してください

<#root>

```
Leaf01#
show mon cap 1 buffer detailed | beg Frame 11   <-- begin detail result from Frame 11 (ARP Request)
Frame 11: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface /tmp/epc_ws/wif_to_t
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Destination: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
        Address: 00:00:00:00:00:00 (00:00:00:00:00:00)
```

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

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

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

Dst Port: 4789  <-- VXLAN Dest port


Virtual eXtensible Local Area Network
    VXLAN Network Identifier

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

    Reserved: 0

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



  Type: ARP (0x0806)

    Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (

request

)

 <-- is an ARP request


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


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



Frame 12:

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

<-- ARP reply


Ethernet II,

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

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

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

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

<-- Underlay MACs
```

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

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

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

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

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

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

 <-- Start of payload



 Type: ARP

 (0x0806)
    Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (

reply

)

<-- is an ARP reply


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


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

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

CGW RT2ゲートウェイプレフィックス

ゲートウェイプレフィックスがありません

前の「部分的に隔離されたセグメント」の項で説明したように、MACはファブリックVlanで学習する必要があります

- この問題は、MACエージングタイマーよりも長くゲートウェイを宛先とするトラフィックがない場合に発生する可能性があります。
- CGWゲートウェイプレフィックスがない場合、MACが存在することを確認する必要があります

<#root>

```
CGW#

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

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


CGW#

show mac address-table address 0000.beef.cafe

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

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

<-- MAC is not learned in Fabric Vlan 202

Total Mac Addresses for this criterion: 2
```

修復が見つからないゲートウェイプレフィックス

ほとんどの実稼働ネットワークでは、常に何らかのトラフィックが存在する可能性があります。ただし、この問題が発生している場合は、次のいずれかの方法で問題を修復できます。

- 「mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1」などのスタティックMACエントリを追加します。
- 「mac address-table aging-time <seconds>」を使用して、MACエージングタイマーの値を増やします。（これにより、すべてのMACアドレスのエージングタイムが長くなるので、スタティックMACオプションが優先されます）

DEF GW属性がありません

部分的に分離されたセグメントでは、この属性を追加する設定が多数追加されます。

DEF GW属性の修復がありません

次の詳細を確認します。

- 17.12.1以降を実行している
- 設定にはSISF(Device-Tracking)CLIが存在します
- route-map matchおよびsetコマンドが設定され、BGPネイバーにルートマップが適用されます
- BGPアドバタイズメントを更新しました（新しい属性でプレフィックスを再アドバタイズするには、BGPをクリアする必要があります）

ワイヤレスローミング

頻繁なローミングはBGPのアップデートを頻繁に発生させる可能性があり、スイッチがMACの所

有を宣言してRT2アップデートを送信する前に、時間間隔あたりのローミングを増加させる必要があります

- これは、ホストが異なるスイッチにある2つのAP間を移動するときに発生します。
- ローミングのデフォルトの制限は180秒あたり5です

<#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 section
 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...>
```

TAC用に収集すべきコマンド

このガイドで問題が解決しない場合は、表示されているコマンドリストを収集して、TACサービスリクエストに添付してください。

収集する最小限の情報

（リロード/リカバリアクションの前にデータを収集する時間が限られている）

0.

- Show tech evpn
- show tech
- show techの問題

0.

収集すべき詳細情報

（より完全なデータを収集する時間がある場合は、これが推奨されます）

0.

- show tech
- show tech evpn（隠しコマンド）
- show tech platform evpn_vxlan switch <数値>
- show tech platform
- show tech resource
- show tech sisf
- show tech isis
- show tech bgp
- show monitor event-trace evpn event all（隠しコマンド）
- show monitor event-trace evpn error all（隠しコマンド）
- 要求プラットフォームソフトウェアトレースアーカイブ

関連情報

- Catalyst 9000シリーズスイッチでのBGP EVPNルーティングポリシーの実装
- DHCPレイヤ2リレー（準備中）

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。