Implementierung der BGP EVPN Protected Overlay-Segmentierung auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird die Implementierung einer BGP EVPN VXLAN Protected Overlay-Segmentierung auf Catalyst Switches der Serie 9000 beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- BGP EVPN VxLAN-Konzepte
- BGP EVPN Unicast-Fehlerbehebung
- BGP-EVPN-VxLAN-Routingrichtlinie

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 und neuere Versionen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Allgemeine Funktionsbeschreibung

Die Funktion für geschützte Segmente ist eine Sicherheitsmaßnahme, die verhindert, dass Ports

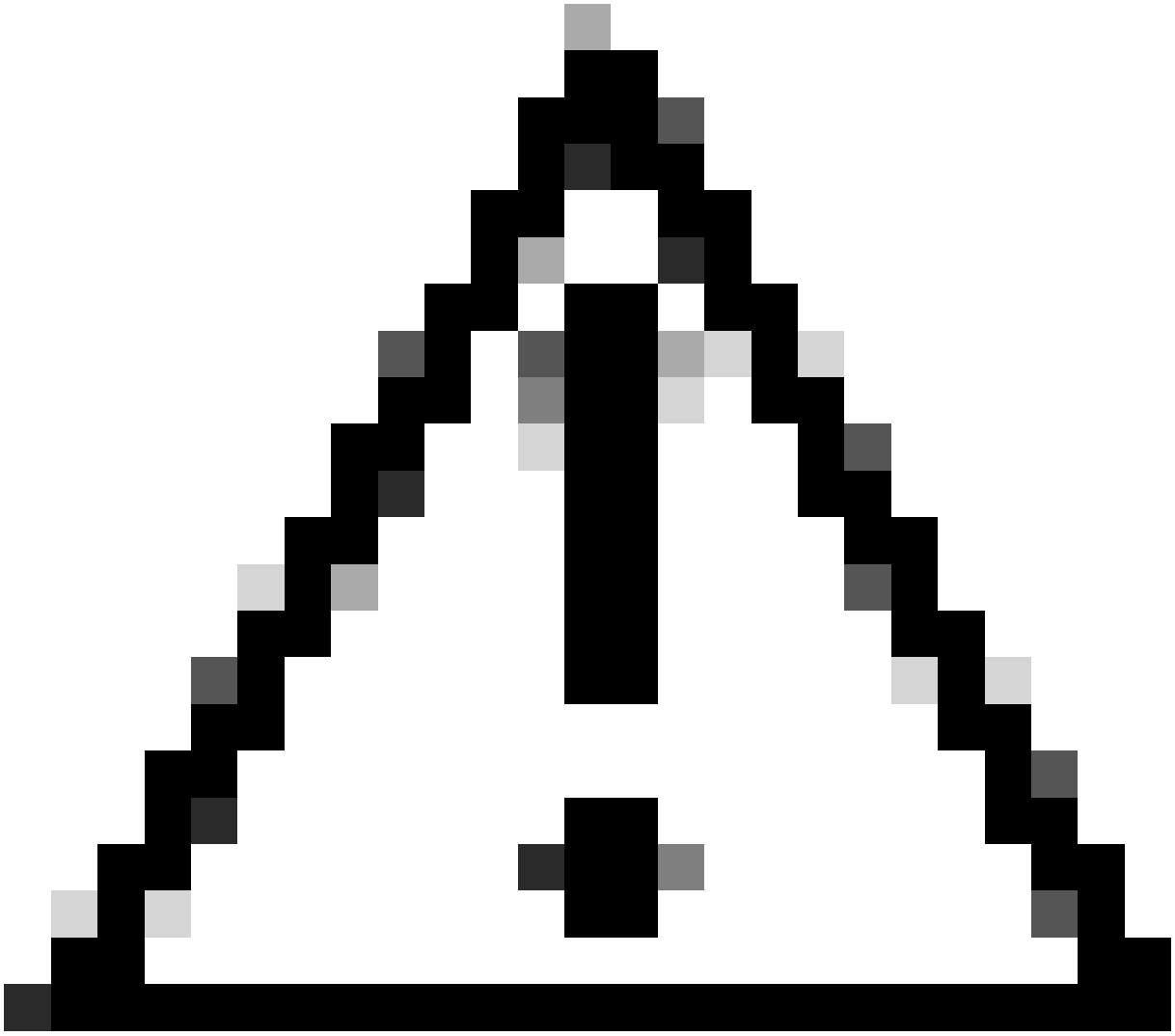
Datenverkehr untereinander weiterleiten, selbst wenn sie sich im selben VLAN und Switch befinden

- Diese Funktion ähnelt "switchport protected" oder privaten VLANs, jedoch für EVPN-Fabrics.
- Dieses Design erzwingt den gesamten Datenverkehr zum CGW, wo er von einer Firewall überprüft werden kann, bevor er an das endgültige Ziel gesendet wird.
- Der Datenverkehr wird über eine zentralisierte Sicherheits-Appliance gesteuert, ist deterministisch und lässt sich leicht überprüfen.

Dokumentdetails

Dieses Dokument umfasst Teil 2 oder 3 zusammenhängende Dokumente:

- Dokument 1: Implementierung der BGP-EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000 beschreibt die Steuerung des BGP BUM-Datenverkehrs im Overlay und muss zuerst konfiguriert werden
- Dokument 2: Dieses Dokument. Aufbauend auf dem Overlay-Design und den Richtlinien von Dokument 1 beschreibt dieses Dokument die Implementierung des Schlüsselworts "protected"
- Dokument 3: Implementierung eines BGP-EVPN-DHCP-Layer-2-Relays auf Catalyst Switches der Serie 9000 beschreibt die Funktionsweise eines DHCP-Relays auf einer VTEP nur für L2



Vorsicht: Sie müssen die Konfiguration in Dokument 1 implementieren, bevor Sie geschützte Segmentkonfigurationen implementieren können.

Geschützte Segmenttypen

Vollständig isoliert

- Ermöglicht nur die Nord-Süd-Kommunikation und
- Das Gateway wird über die CLI "default-gateway advertise" in der Fabric angekündigt.

Meist isoliert

- Ermöglicht Nord-Süd-Kommunikation (in diesem Fall sind Ost/West-Datenverkehrsflüsse basierend auf Firewall-Datenverkehrsrichtlinien zulässig)
- Ermöglicht Ost-West-Kommunikation (basierend auf Firewall-Datenverkehrsrichtlinien)
- Das Gateway befindet sich außerhalb der Fabric, und die SVI wird nicht über die CLI

"default-gateway advertise" angekündigt.

Switch-Verhalten

- Hosts können nicht direkt miteinander kommunizieren, selbst wenn sie mit demselben Switch verbunden sind (ARP-Anfrage wird nicht an andere Ports auf demselben Switch gesendet, wenn Hosts sich im selben VRF/VLAN/Segment befinden)
- Kein BUM-Datenverkehr zwischen L2 VTEPs (IMET-Präfixe werden anhand der Routing-Richtlinienkonfiguration gefiltert)
- Alle Pakete von den Hosts werden zur Weiterleitung an den Grenz-Leaf weitergeleitet. (Das bedeutet, dass Host 1 mit Host 2 auf demselben Leaf kommunizieren kann und der Datenverkehr per Fair-Pin an den CGW geleitet wird

Verarbeitung von Routentyp 2

- Access Leafs kündigen lokale RT2 mit erweiterter E-Tree-Community und festgelegter Leaf-Markierung an
- Access-Leafs installieren kein Remote-RT2, das mit einer E-Tree Extended Community und einem Leaf-Flag auf der Datenebene empfangen wurde
- Access Leafs installieren einander RT2 nicht auf Datenebene
- Access Leafs und Border Leaf (CGW) installieren sich gegenseitig RT2 auf Datenebene
- Keine Konfigurationsänderung auf Access Leaf oder Border Leaf erforderlich.

Zusammenfassung des Designs

- Für Broadcast (BUM) ist die RT3-Topologie "Hub and Spoke", um Broadcast-Datenverkehr wie ARP auf den GCW zu zwingen.
- Zur Berücksichtigung der Hostmobilität sind die RT2 auf der BGP-Kontrollebene vollständig vernetzt (wenn ein Host von einem VTEP zu einem anderen wechselt, wird die Seq-Nummer im RT2 erhöht).
- Auf der Datenebene werden MAC-Adressen selektiv installiert.
    - Ein Leaf installiert nur lokale MACs und RT2, die das DEF-GW-Attribut enthalten.
    - Der CGW verfügt nicht über den geschützten KW und installiert alle lokalen MAC und Remote-RT2 auf seiner Datenebene.

Terminologie

VRF	Virtual Routing-Weiterleitung	Definiert eine Layer-3-Routing-Domäne, die von anderen VRFs und der globalen IPv4/IPv6-Routing-Domäne getrennt wird.
AF	Adressfamilie	Legt fest, welche Typpräfixe und Routing-Informationen vom BGP verarbeitet werden.
ALS	Autonomes	Ein Satz von über das Internet routbaren IP-Präfixen, die zu einem

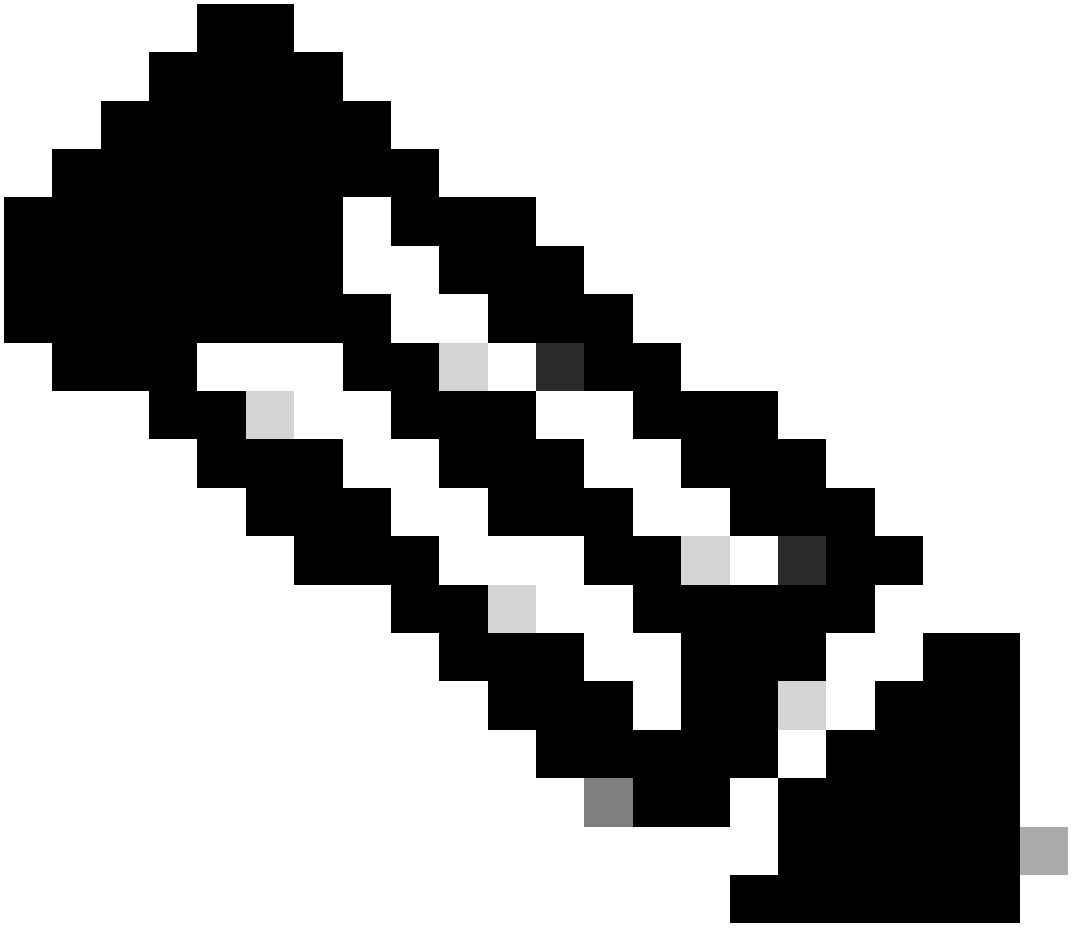
	System	Netzwerk gehören, oder eine Sammlung von Netzwerken, die alle von einer einzigen Einheit oder Organisation verwaltet, gesteuert und überwacht werden.
EVPN	Ethernet Virtual Private Network	Die Erweiterung, die es dem BGP ermöglicht, Layer-2-MAC- und Layer-3-IP-Informationen zu übertragen, ist EVPN und verwendet das Multi-Protocol Border Gateway Protocol (MP-BGP) als Protokoll zur Verteilung von Erreichbarkeitsinformationen für das VXLAN-Overlay-Netzwerk.
VXLAN	Virtuelles erweiterbares LAN (Local Area Network)	VXLAN wurde entwickelt, um die Einschränkungen von VLANs und STP zu überwinden. Es handelt sich um einen vorgeschlagenen IETF-Standard [RFC 7348], der dieselben Ethernet-Layer-2-Netzwerkdienste wie VLANs bereitstellt, jedoch mit größerer Flexibilität. Funktionell handelt es sich um ein MAC-in-UDP-Kapselungsprotokoll, das als virtuelles Overlay auf einem Layer-3-Underlay-Netzwerk ausgeführt wird.
CGW	Zentrales Gateway	Implementierung von EVPN, wobei sich die Gateway-SVI nicht auf jedem Leaf befindet Stattdessen erfolgt das gesamte Routing über ein spezielles Leaf mit asymmetrischem IRB (Integrated Routing and Bridging).
DEF GW	Standardgateway	Ein erweitertes BGP-Community-Attribut, das dem MAC/IP-Präfix über den Befehl "default-gateway advertise enable" im Konfigurationsabschnitt "l2vpn evpn" hinzugefügt wird.
IMET (RT3)	Inklusives Multicast Ethernet-Tag (Route)	Wird auch als BGP-Typ-3-Route bezeichnet. Dieser Routing-Typ wird im EVPN verwendet, um BUM-Datenverkehr (Broadcast/unbekanntes Unicast/Multicast) zwischen VTEPs zu übertragen.
RT2	Routentyp 2	BGP-MAC- oder MAC/IP-Präfix, das eine Host-MAC- oder Gateway-MAC-IP-Adresse darstellt
EVPN-Manager	EVPN-Manager	Zentrale Verwaltungskomponente für verschiedene andere Komponenten (Beispiel: lernt von SISF und signalisiert L2RIB)
SISF	Integrierte Switch-Sicherheitsfunktion	Eine unabhängige Host-Tracking-Tabelle, die von EVPN verwendet wird, um festzustellen, welche lokalen Hosts auf einem Leaf vorhanden sind.

L2RIB	Layer 2 Routing Information Base	Zwischenprodukt für das Management von Interaktionen zwischen BGP, EVPN Mgr, L2FIB
FED	Forwarding-Engine-Treiber	Programmierung der ASIC-Ebene (Hardware)
MATM	MAC-Adresstabellen-Manager	IOS MATM: Softwaretabelle, die nur lokale Adressen und FED-MATM: Hardwaretabelle, die von der Kontrollebene empfangene lokale und Remote-Adressen installiert und Teil der Hardware-Weiterleitungsebene ist

Flussdiagramme

Diagramm Route-Type 2 (RT2)

Dieses Diagramm zeigt das Full-Mesh-Design der Typ-2-MAC/MAC-IP-Host-Präfixe.



Hinweis: Zur Unterstützung von Mobilität und Roaming ist eine vollständige Vermaschung erforderlich.

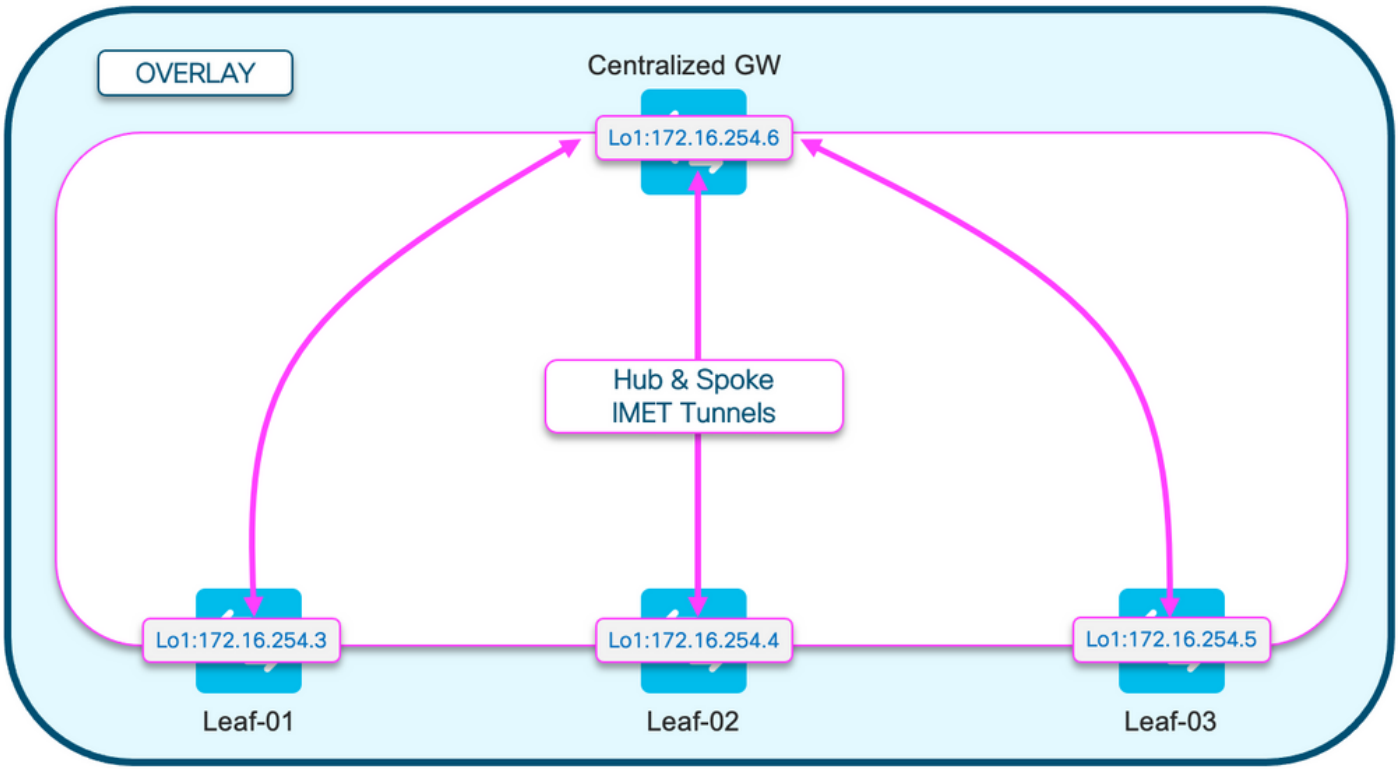
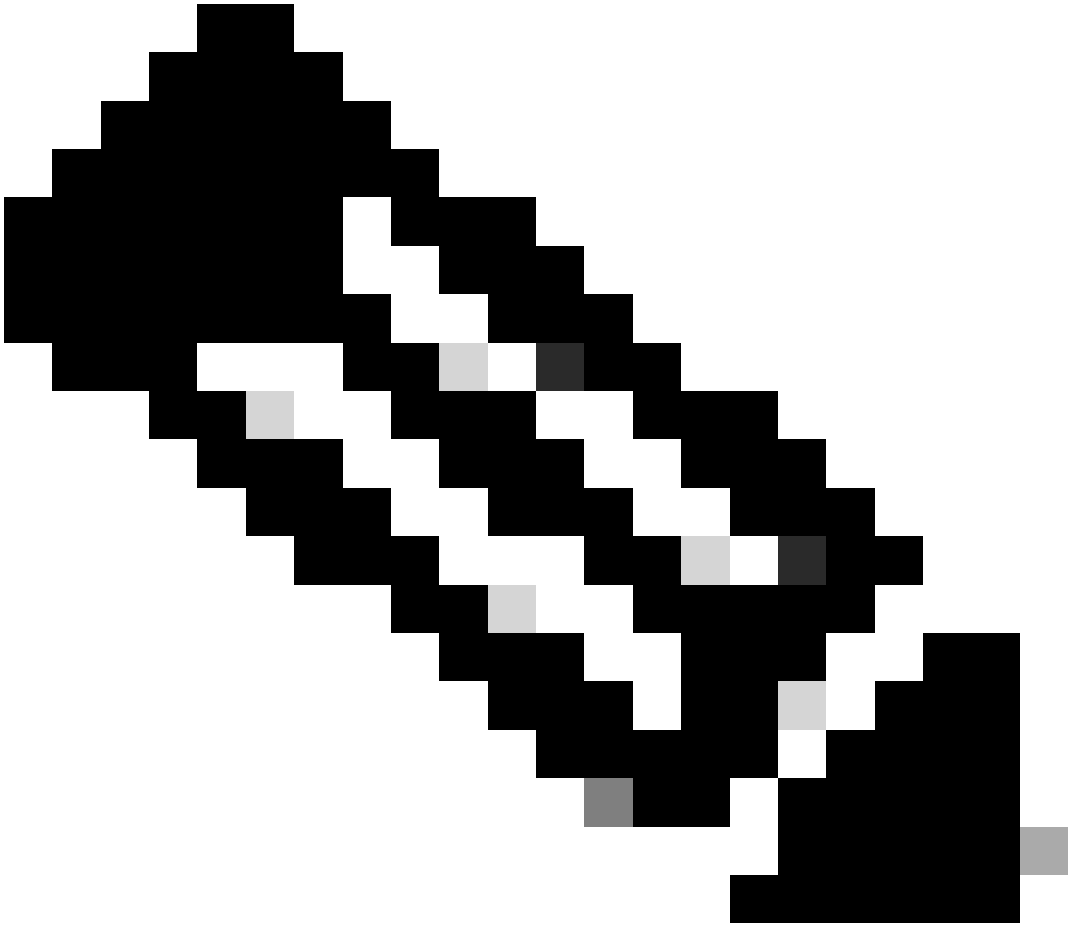
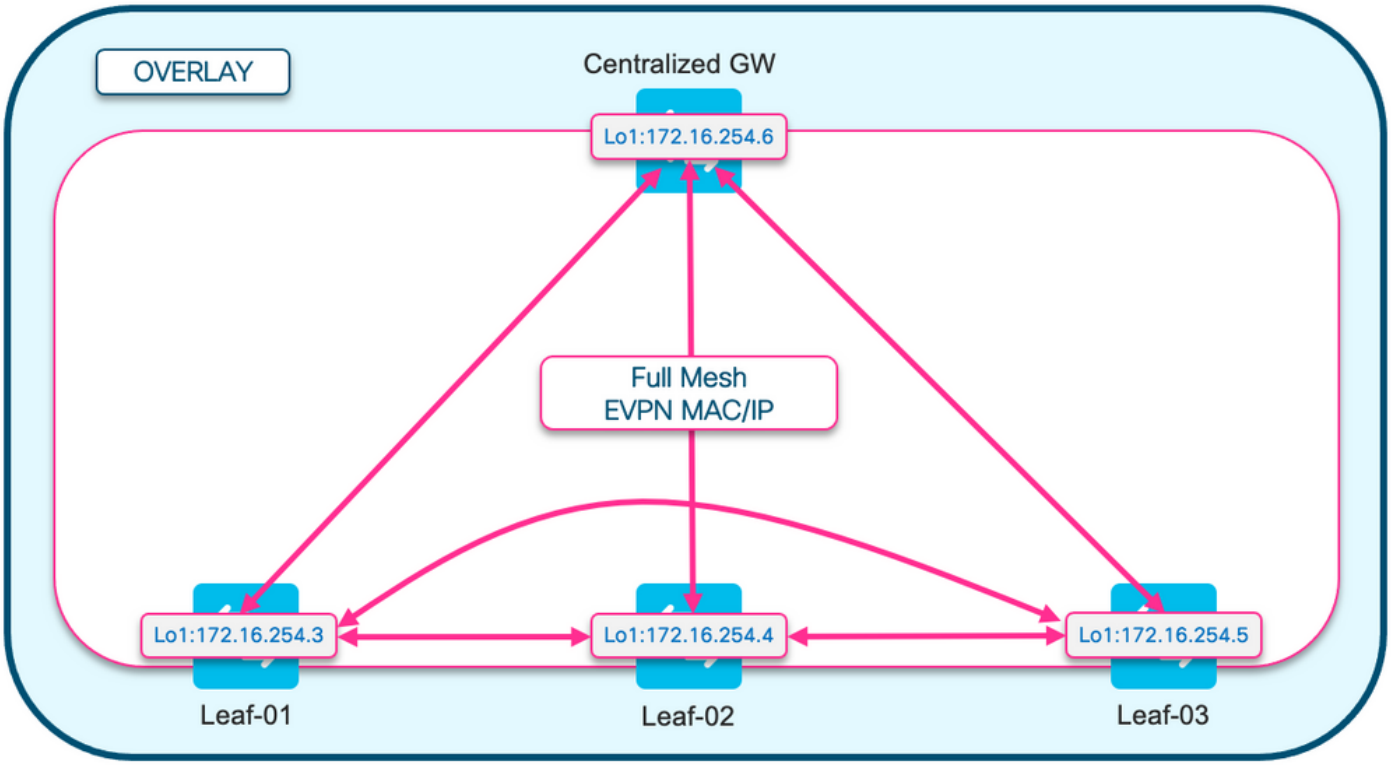


Diagramm Route-Type 3 (RT3)

Dieses Diagramm zeigt das Hub-and-Spoke-Design der Broadcast-IMET-Tunnel (RT3).

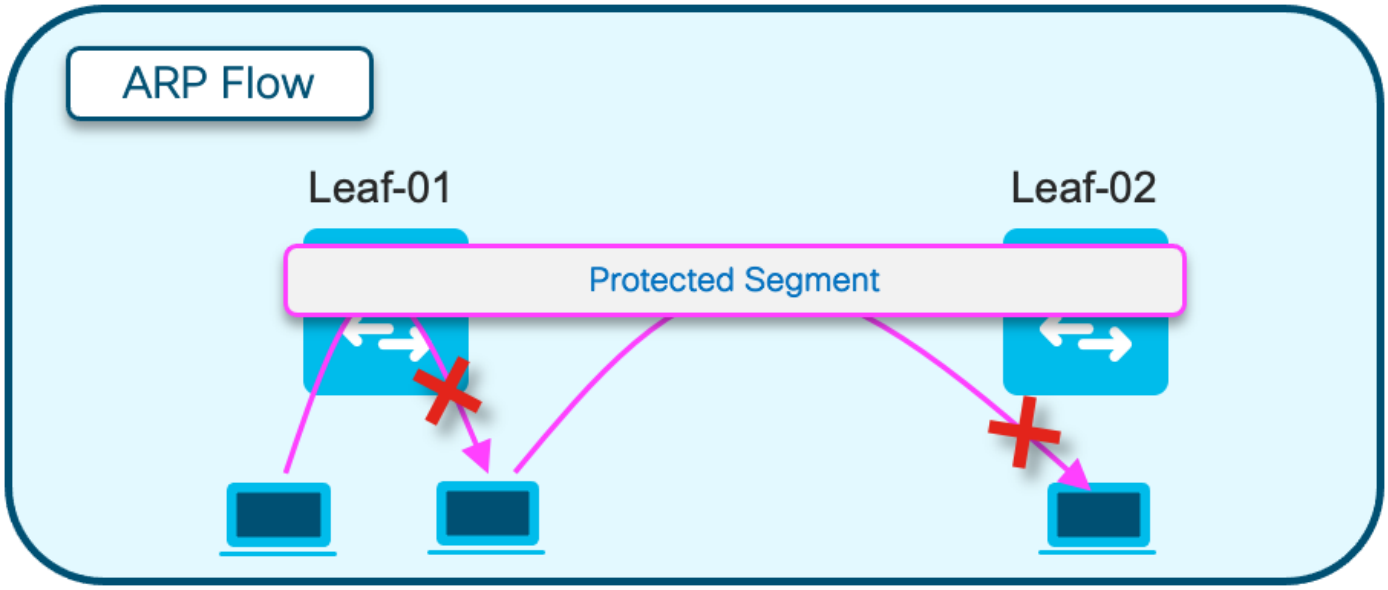


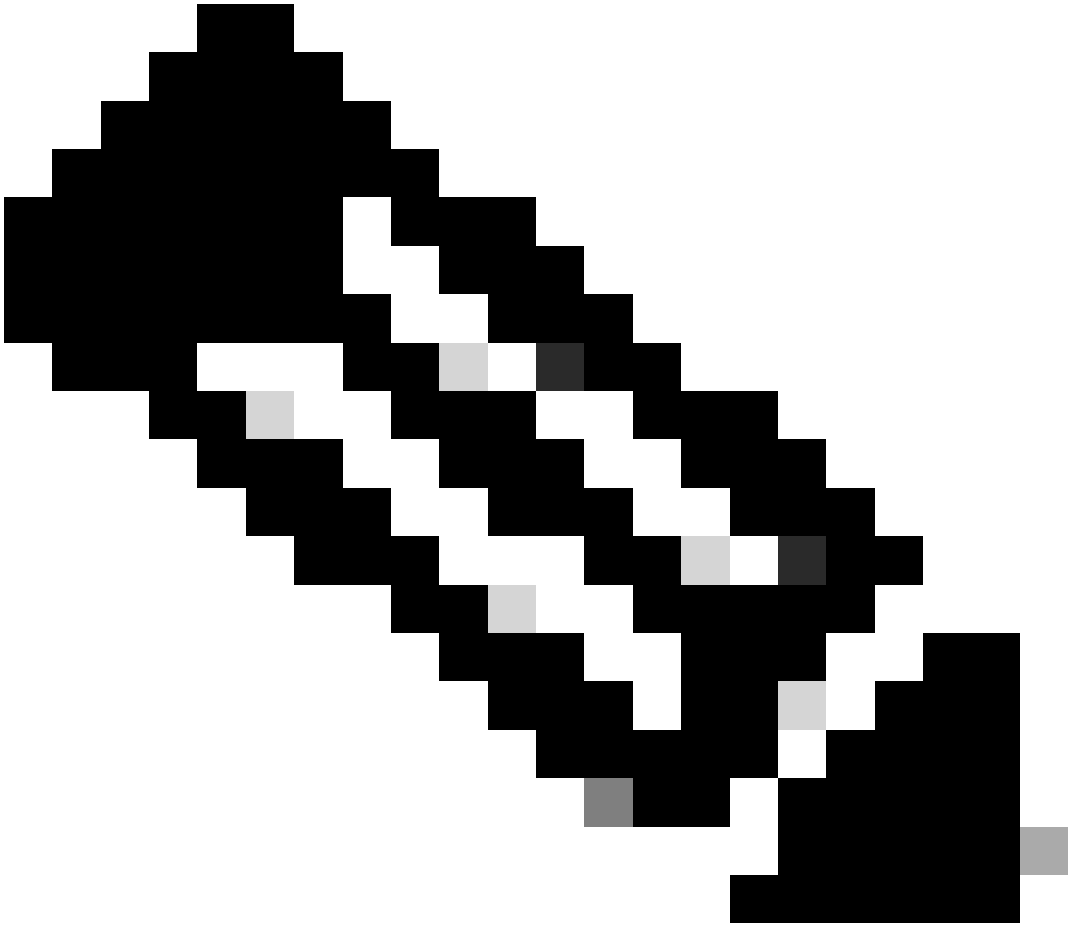
Hinweis: Hub-and-Spoke-Broadcast ist erforderlich, um zu verhindern, dass Leafs mit demselben Segment Broadcasts direkt zueinander senden.



ARP-Diagramm (Address Resolution)

Dieses Diagramm zeigt, dass ARP keinen Host im gleichen EPVN-Segment erreichen darf. Wenn Host-ARPs für einen anderen Host verwendet werden, erhält nur der CGW diesen ARP und antwortet



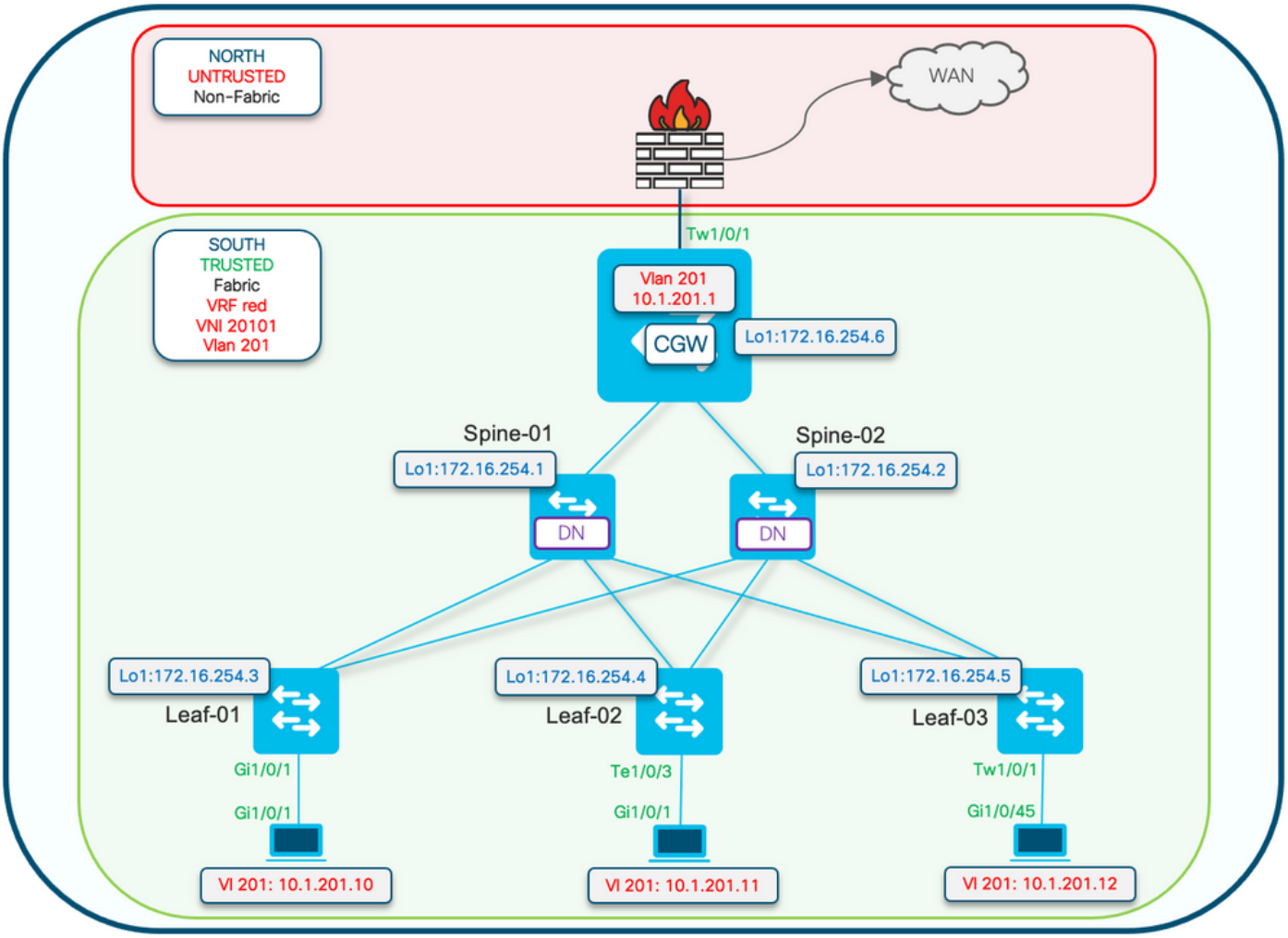


Hinweis: Diese Änderung des ARP-Verhaltens wird durch die Verwendung des Schlüsselworts "protected" instanziiert.

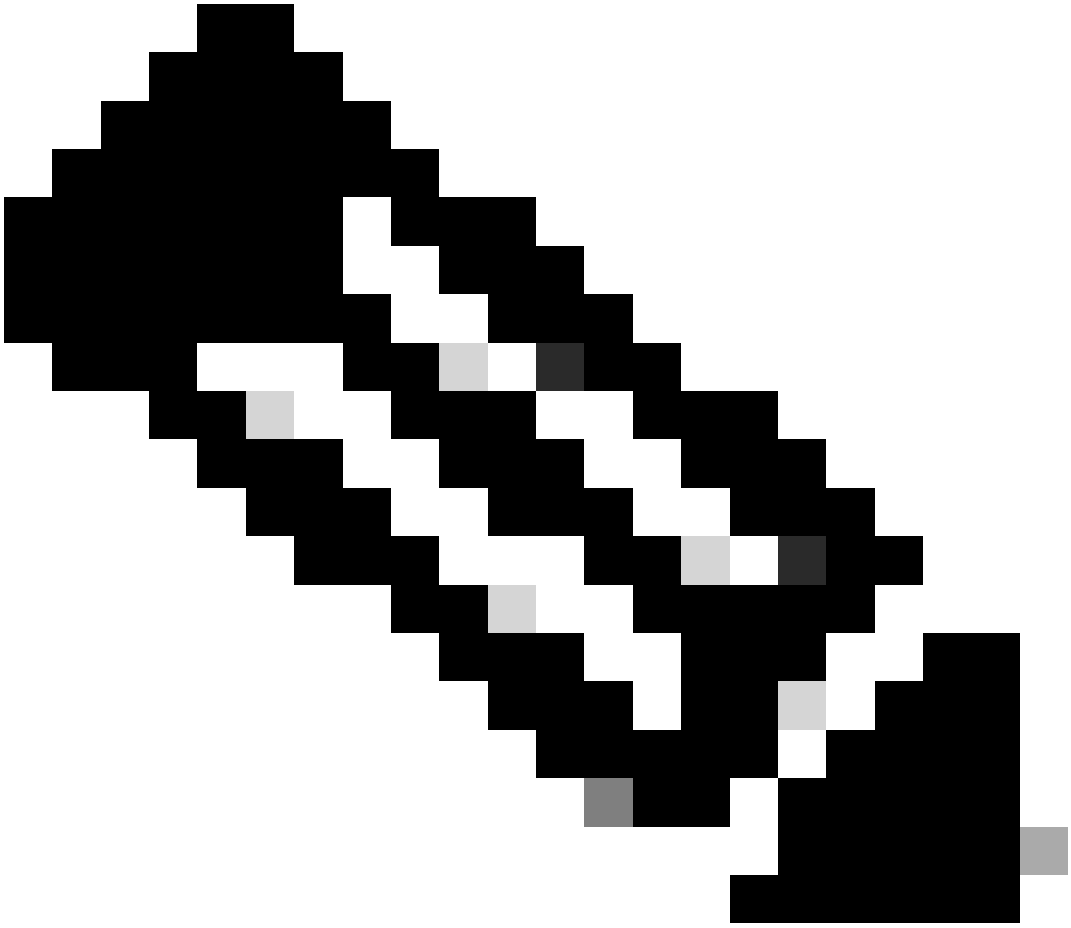
Beispiel: member evpn-instance 202 vni 20201 protected

Konfigurieren (vollständig isoliert)

Netzwerkdiagramm



Das Schlüsselwort für die geschützte Konfiguration wird auf die Leaf-Switches angewendet. Der CGW ist ein Promiscuous-Gerät und installiert alle MAC-Adressen.



Hinweis: Die Community-Liste und die Routing-Map-Konfiguration der Routing-Richtlinien, die den Import/Export von IMET-Präfixen steuert, werden unter Implementieren der BGP-EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000 angezeigt. In diesem Dokument werden nur geschützte Segmentunterschiede angezeigt.

Leaf-01 (Basis-EVPN-Konfiguration)

<#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 (Basiskonfiguration)

<#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
```

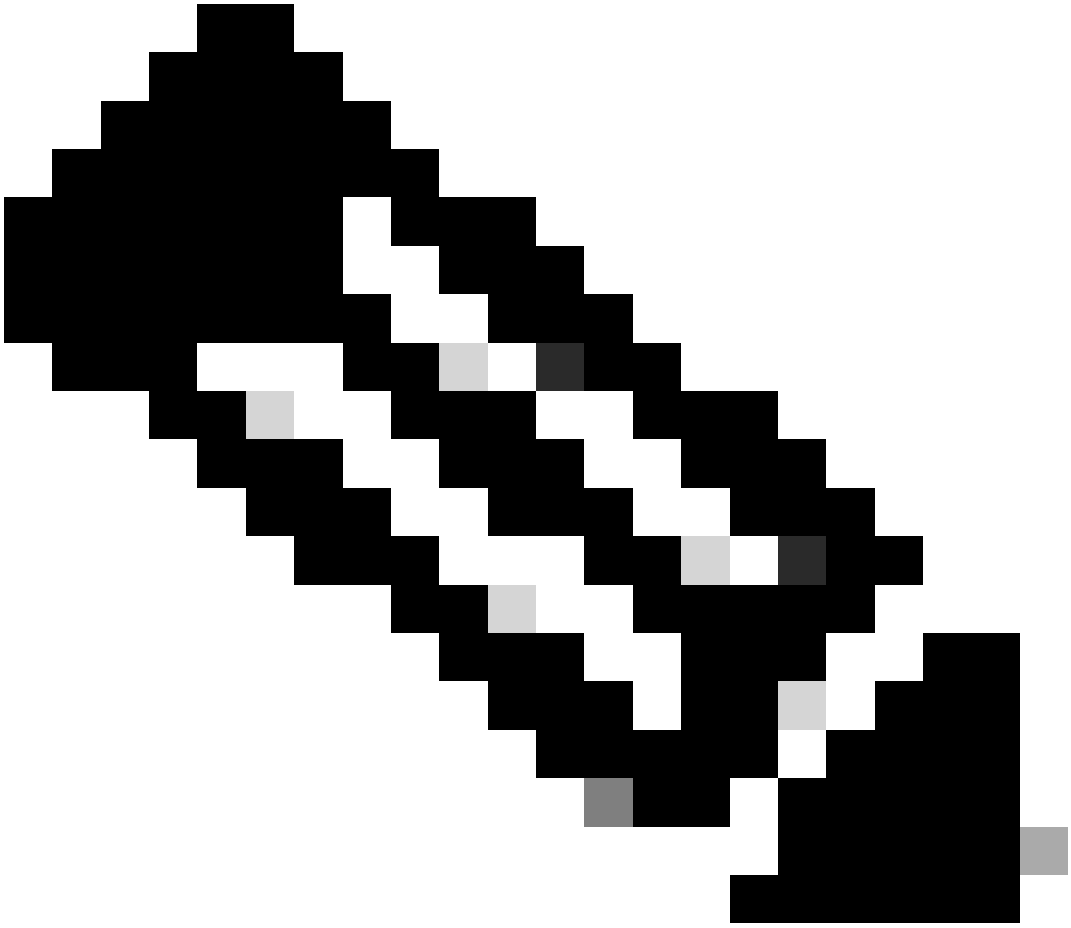
<#root>

```
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
```



Hinweis: Im CGW werden keine BGP-Richtlinien angewendet. Der CGW kann alle Präfixtypen (RT2, RT5 / RT3) empfangen und senden.

Verifizieren (vollständig isoliert)

EVI-Details

<#root>

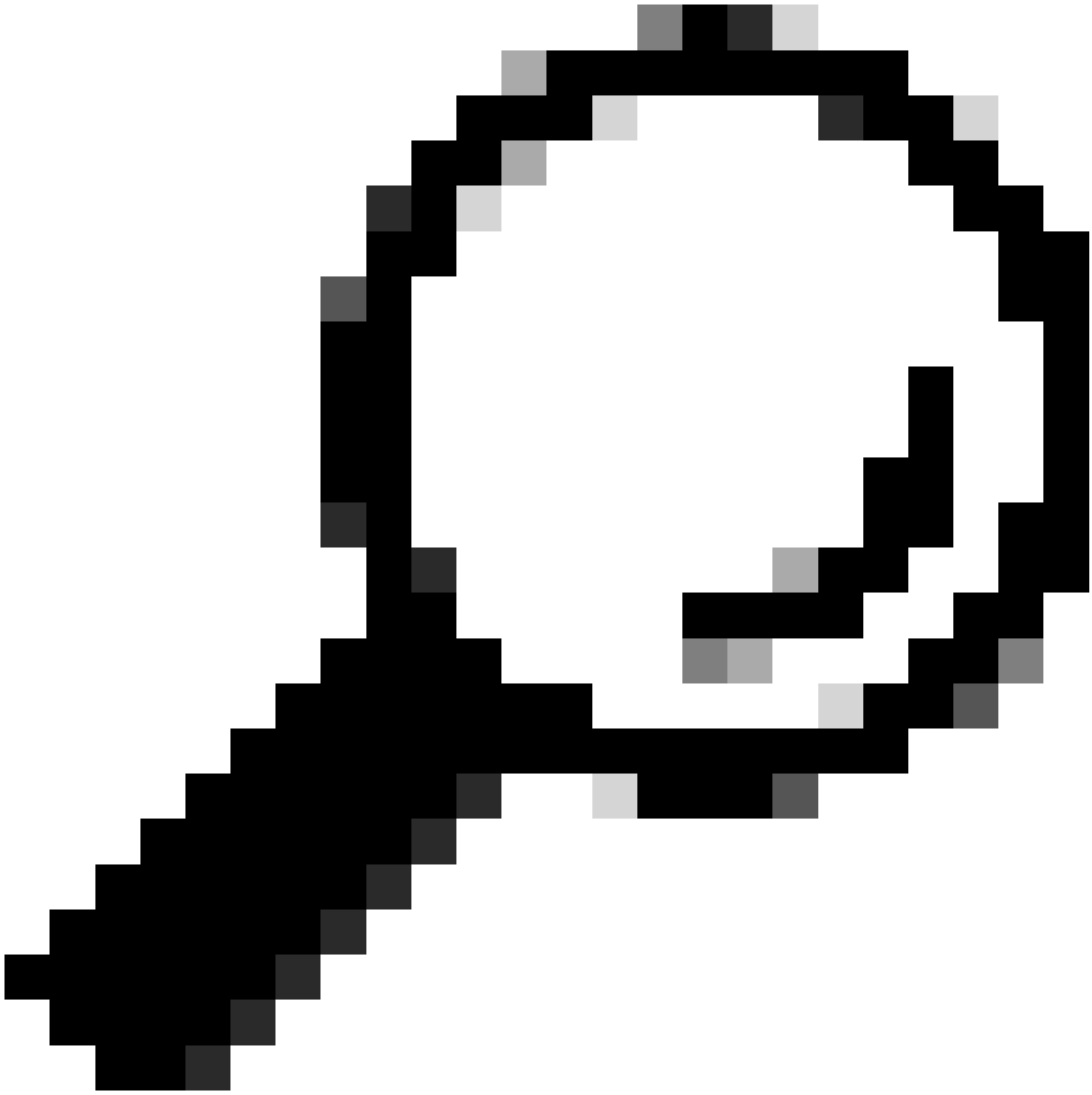
```
Leaf01#

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...>
```

Lokale RT2-Generierung (lokaler Host zu RT2)

Überprüfen Sie die Komponentenabhängigkeitskette vom lokalen Host-Learning bis zur RT2-Generierung:

- SISF (Obwohl der Leaf über keine SVI verfügt, erfasst SISF die Host-Informationen dennoch über einen ARP-Frame vom Host.)
- EVPN-Manager
- L2RIB
- BGP

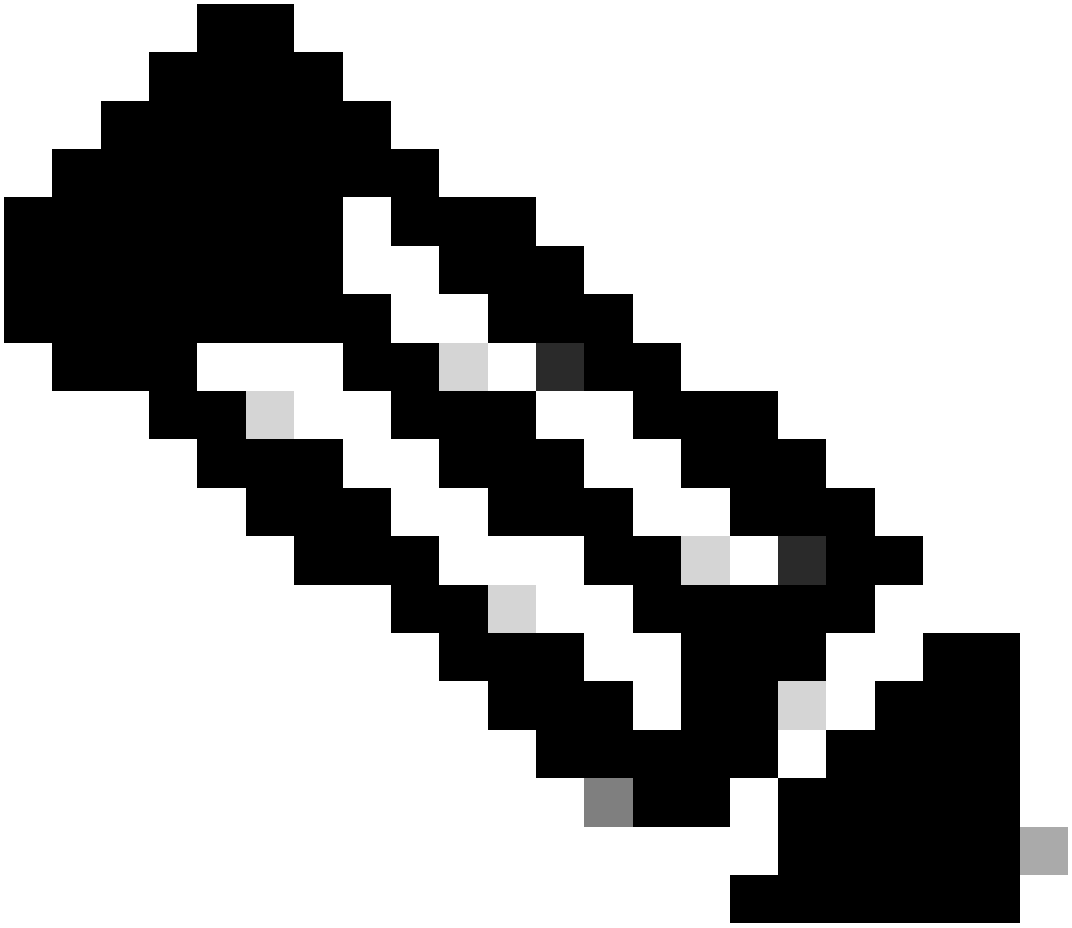


Tipp: Wenn eine vorherige Komponente nicht richtig programmiert wurde, bricht die gesamte Abhängigkeitskette (Beispiel: SISF hat keinen Eintrag, dann kann BGP kein RT2 erstellen).

SISF

Überprüfen, ob der Host vom SISF in der DB erfasst wurde (Host-Informationen wurden vom DHCP oder ARP abgerufen)

- SISF erfasst MAC-Einträge vom IOS-MATM-Learning und sendet diese dann an den EVPN Mgr (muss mit der Richtlinie "evpn-sisf-policy" MAC-ERREICHBAR sein
- SISF erfasst eine IP/MAC-Bindung an einen lokalen VTEP und verwendet den EVPN-Manager, um diese Informationen als /32-Route über BGP zu anderen Leafs zu programmieren.



Hinweis: In diesem Szenario verfügt der Host über eine statische IP, sodass SISF ARP verwendet, um die Host-Details zu ermitteln. Im Abschnitt Mostly Isolated (Meist isoliert) werden DHCP- und DHCP-Snooping angezeigt.

<#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-Manager

Der EVPN-Manager lernt die lokale MAC-Adresse und installiert sie in L2RIB. Der EVPN Mgr empfängt die Remote-MAC ebenfalls von L2RIB, der Eintrag wird jedoch nur für die Verarbeitung der MAC-Mobilität verwendet.

Bestätigen, dass der EVPN Mgrmit dem SISF-Eintrag aktualisiert wurde

```
<#root>

Leaf01#

show l2vpn evpn mac evi 201

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

0006.f601.cd43 201   201

0000.0000.0000.0000.0000 0

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

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

L2RIB

- L2RIB empfängt lokale MAC-Adressen vom EVPN Mgr und sendet sie an BGP und L2FIB
- L2RIB lernt außerdem Remote-MACs vom BGP, um den EVPN Mgr und L2FIB zu aktualisieren
- L2RIB benötigt sowohl Local als auch Remote, damit andere Komponenten ordnungsgemäß aktualisiert werden können.
- Die L2RIB-Komponente befindet sich zwischen dem lokalen und dem Remote-MAC-Learning-Bereich, je nachdem, welche Richtung/Komponente aktualisiert werden muss.

Überprüfen, ob L2RIB mit der lokalen MAC vom EVPN Mgr aktualisiert wurde

```
<#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

Überprüfung der BGP-Aktualisierung durch 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
```

Remote RT2 Learning (Standard-Gateway RT2)

BGP

Überprüfen, ob das BGP das CGW-RT2-Präfix erhalten hat

<#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

Überprüfung der BGP-aktualisierten L2RIB

- L2RIB empfängt lokale MAC vom EVPN Mgr und sendet sie an BGP und L2FIB. L2RIB lernt außerdem Remote-MACs vom BGP, um den EVPN Mgr und L2FIB zu aktualisieren
- L2RIB benötigt sowohl Local als auch Remote, damit andere Komponenten ordnungsgemäß aktualisiert werden können.
- Die L2RIB-Komponente befindet sich zwischen lokalem und Remote-MAC-Learning, je nachdem, welche Richtung und Komponente aktualisiert werden muss.

<#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

Überprüfung in L2FIB

- Komponente, die für die Aktualisierung von FED mit den MACs für die Programmierung in der Hardware verantwortlich ist.
- Remote-MAC-Einträge, die von L2FIB in FED-MATM installiert wurden, werden NICHT in IOS-MATM geschrieben. (IOS-MATM zeigt nur lokale MACs an, während FED-MATM sowohl lokale als auch Remote-MAC anzeigt)
- Die L2FIB-Ausgabe zeigt nur Remote-MACs an (sie ist nicht für das Programmieren lokaler MACs zuständig).

<#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

Überprüfen in FED-MATM

- Auf Hardwareebene der Leafs, die mit dem geschützten Schlüsselwort konfiguriert sind, sollten nur die CGW-Standard-Gateway-MACs und die lokalen Host-MACs angezeigt werden.
- Der Switch überprüft das RT2-Präfix für das DEF-GW-Attribut, um zu bestimmen, welche Remote-MAC-Adresse für die Installation infrage kommt.

<#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
```

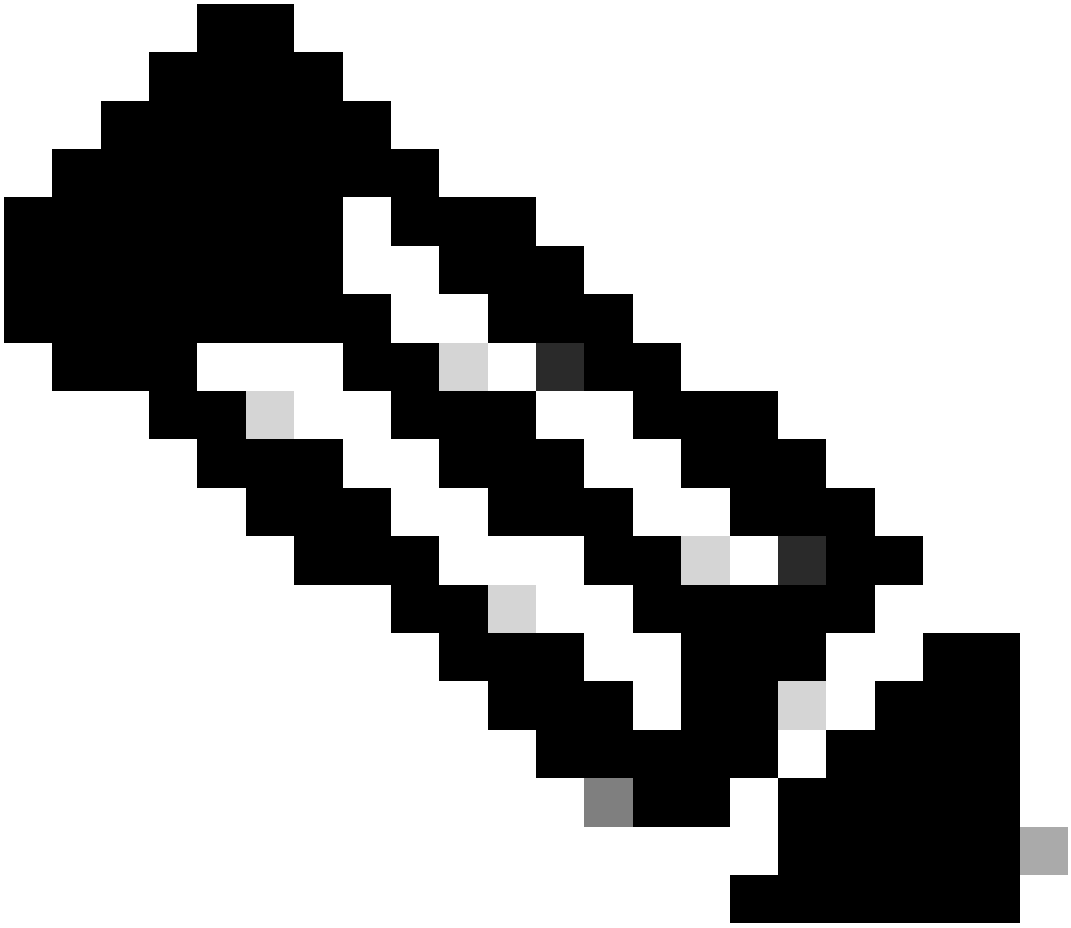
```
<-- the addition of these values = 0x5000001

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

Adjazenz der Datenebene

Als letzten Schritt nach der Bestätigung FED-Eintrag können Sie den Rewrite Index (RI) auflösen

<#root>

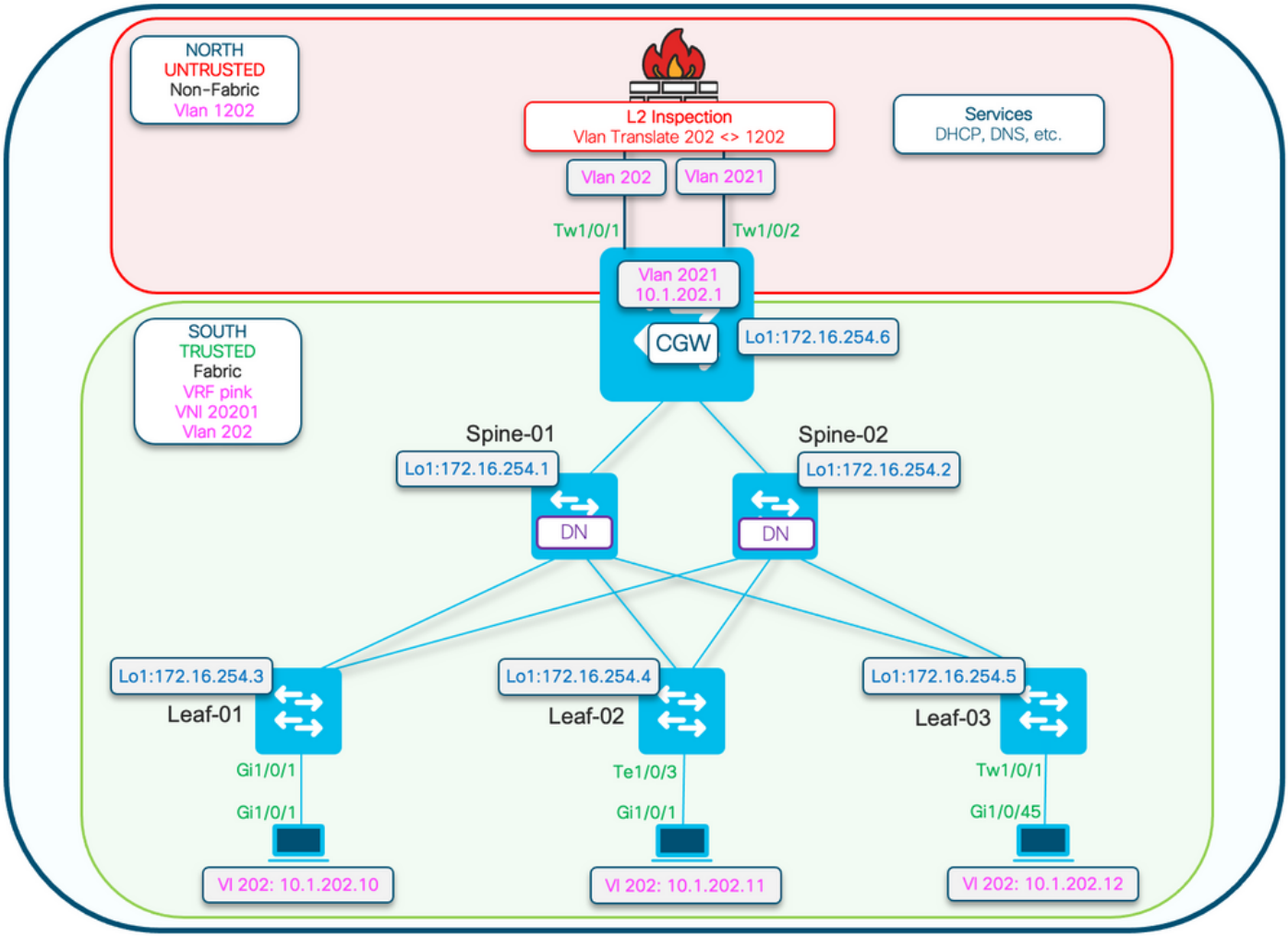
```
Leaf01#

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)
```

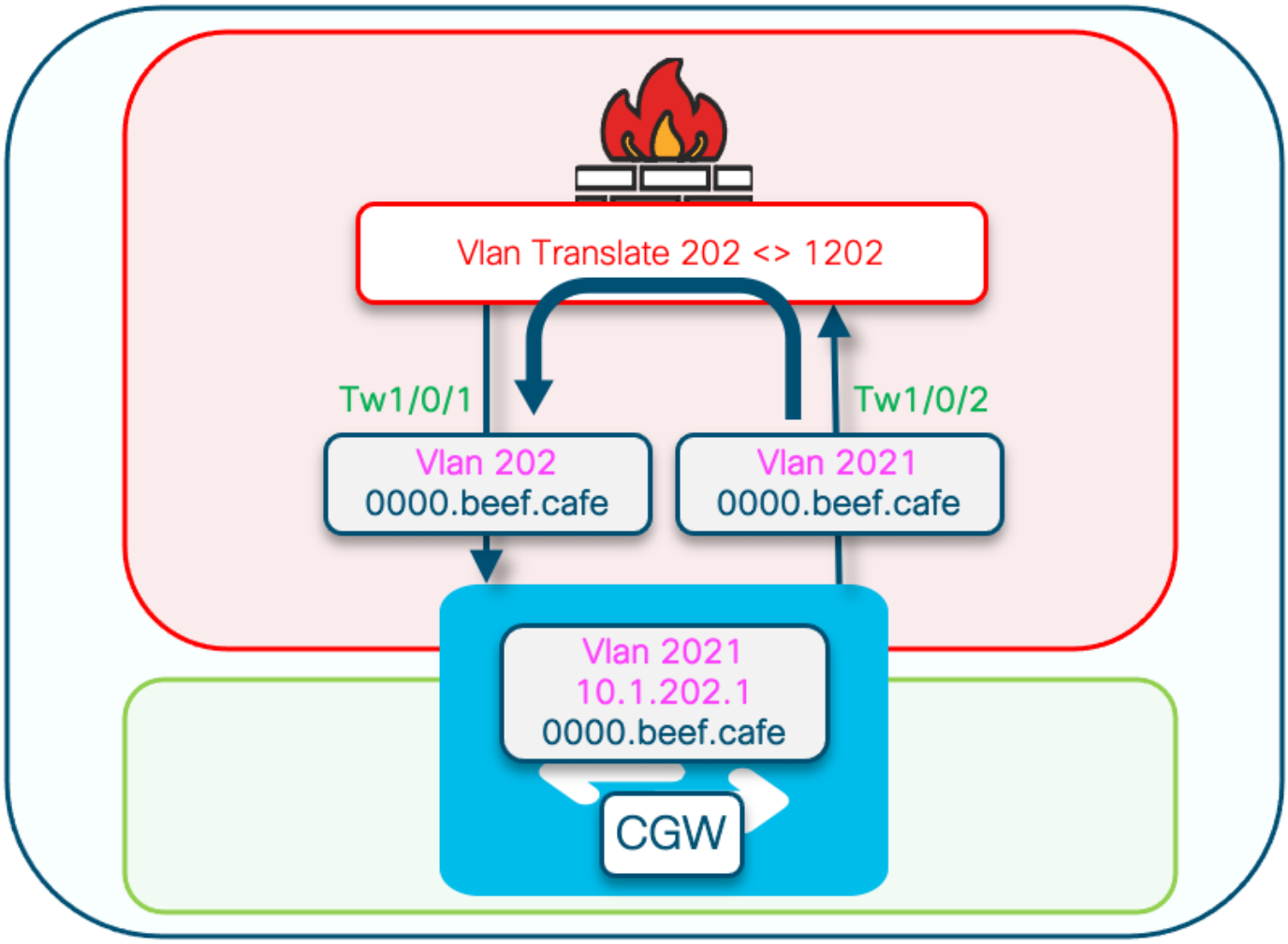


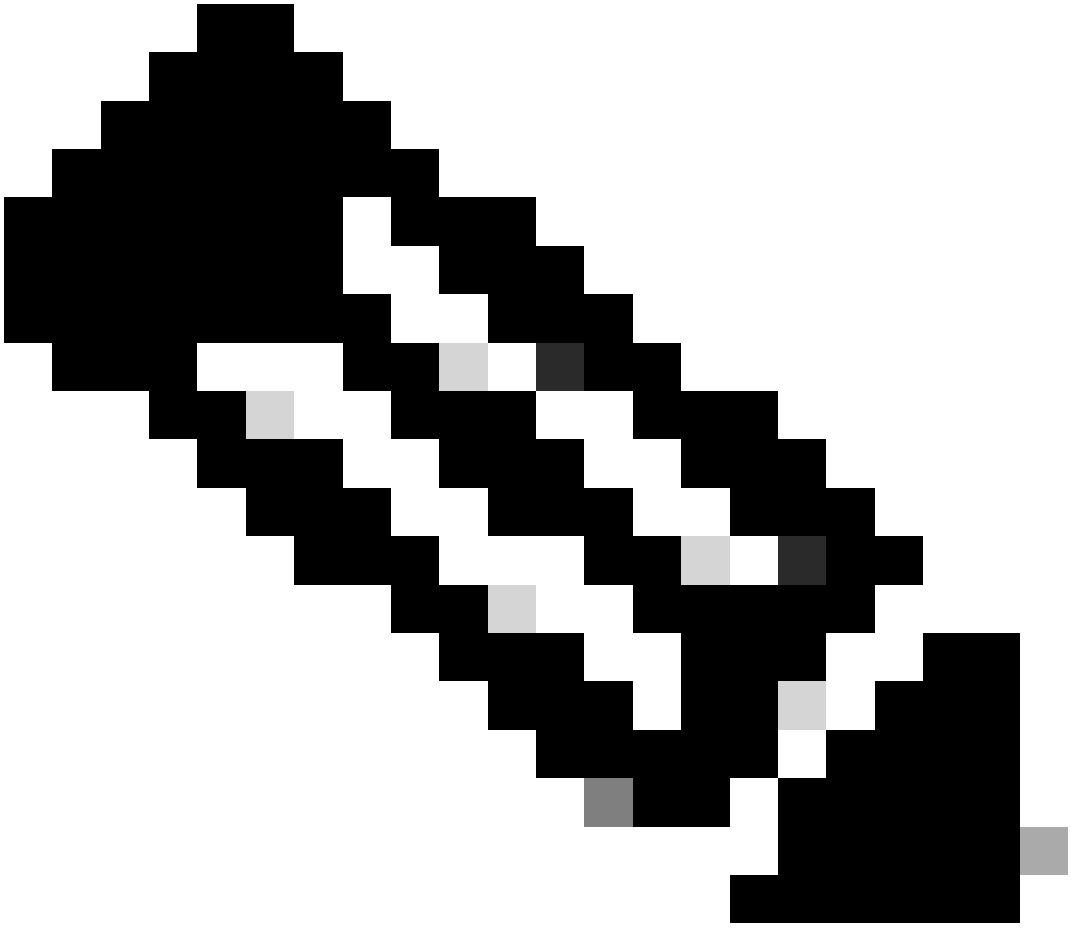
Hinweis: Sie können auch 'show platform software fed switch active matm macTable vlan 201 detail' verwenden, die diesen Befehl mit dem FED-Befehl in ein Ergebnis ketten

Konfigurieren (teilweise isoliert)

Netzwerkdiagramm


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



Hinweis: In diesem Abschnitt werden nur die Unterschiede zu vollständig isolierten Segmenten behandelt.

- Routingrichtlinie zum Markieren der MAC-IP-Adresse des GCW-Gateways mit dem DEF-GW-Attribut
- Benutzerdefinierte Richtlinie zur Geräteverfolgung erforderlich, um MAC-Flaps zu verhindern
- Statische Geräteverfolgungsbindung für GW MAC IP

Leaf-01 (Basis-EVPN-Konfiguration)

<#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 (Basiskonfiguration)

Den Replikationsmodus unter der NVE festlegen

<#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
```

Konfigurieren der externen Gateway-SVI

<#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
```

Erstellen einer Richtlinie mit deaktivierter Entschlackung

<#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
```

Anschluss an externes GatewayEvi/VLAN

<#root>

```
CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

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

Hinzufügen statischer Einträge zur Geräteverfolgungstabelle für externe Gateway-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
```

Erstellen einer BGP-Routenzuordnung für RT2-MAC-IP-Präfixe und Festlegen der erweiterten Standard-Gateway-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
```

Routing-Map auf Nachbarn des BGP-Routen-Reflektors anwenden

<#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
```

Verifizieren (teilweise isoliert)

EVI-Details

<#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...>
```

Lokale RT2-Generierung (lokaler Host zu RT2)

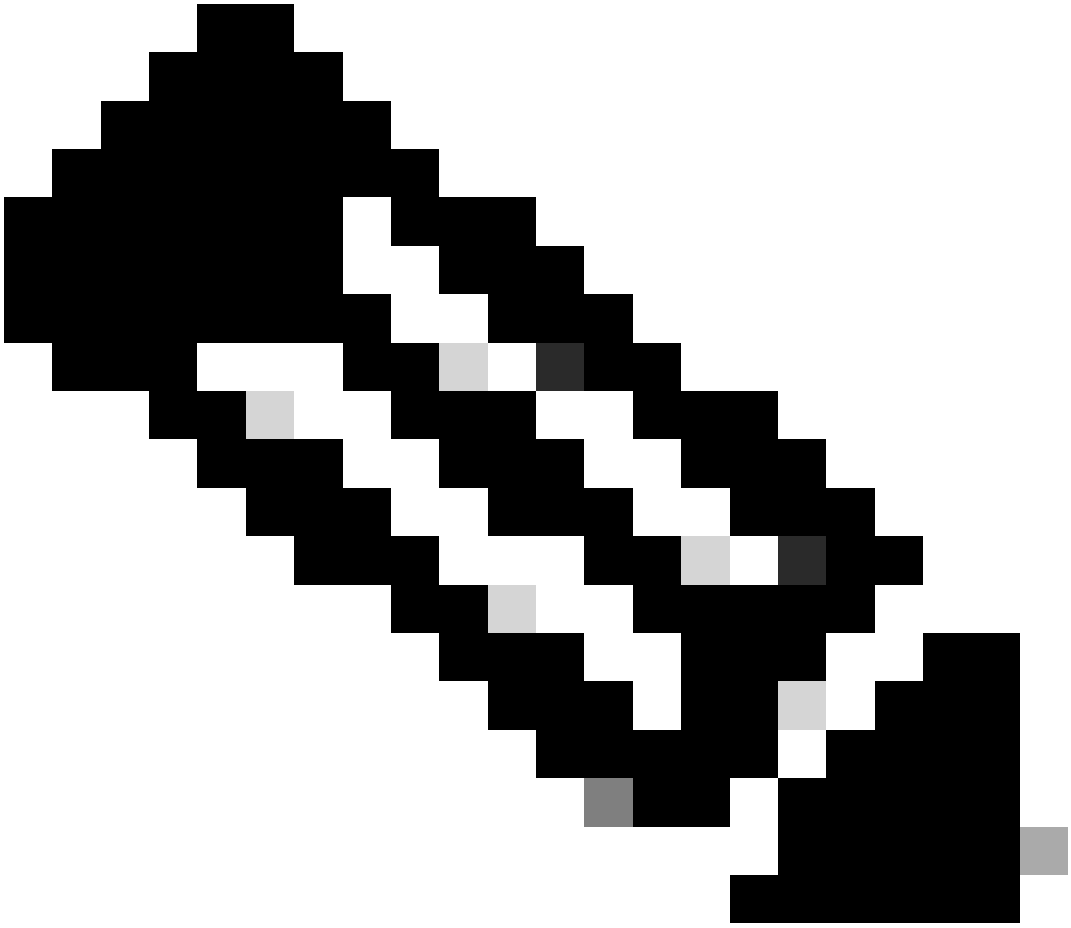
Abgedeckt im vorherigen vollständig isolierten Beispiel

Remote RT2 Learning (Standard-Gateway RT2)

Deckt die Unterschiede von Total Isolated ab.

CGW-Standard-Gateway-Präfix (Leaf)

Überprüfen Sie, ob das Präfix über das entsprechende Attribut verfügt, damit es auf der Hardware installiert werden kann.



Hinweis: Dies ist für die Funktion des DHCP-L2-Relays wichtig.

<#root>

Leaf01#

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

BGP routing table entry for [2][172.16.254.3:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24, version 1846
Paths: (1 available, best #1,

table evi_202

)

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

  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:202][0][48][0000BEEFCAFE][32][10.1.202.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best

```
      EVPN ESI: 00000000000000000000,

Label1 20201              <-- Correct Segment ID

      Extended Community: RT:65001:202 ENCAP:8

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

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

FED-MATM (Leaf)

<#root>

```
F241.03.23-9300-Leaf01#

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

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

202    0000.beef.cafe

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

VTEP 172.16.254.6

 adj_id 651

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

SISF (CGW)

<#root>

```
CGW#

sh device-tracking database vlanid 202

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


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

IOS-MATM (CGW)

<#root>

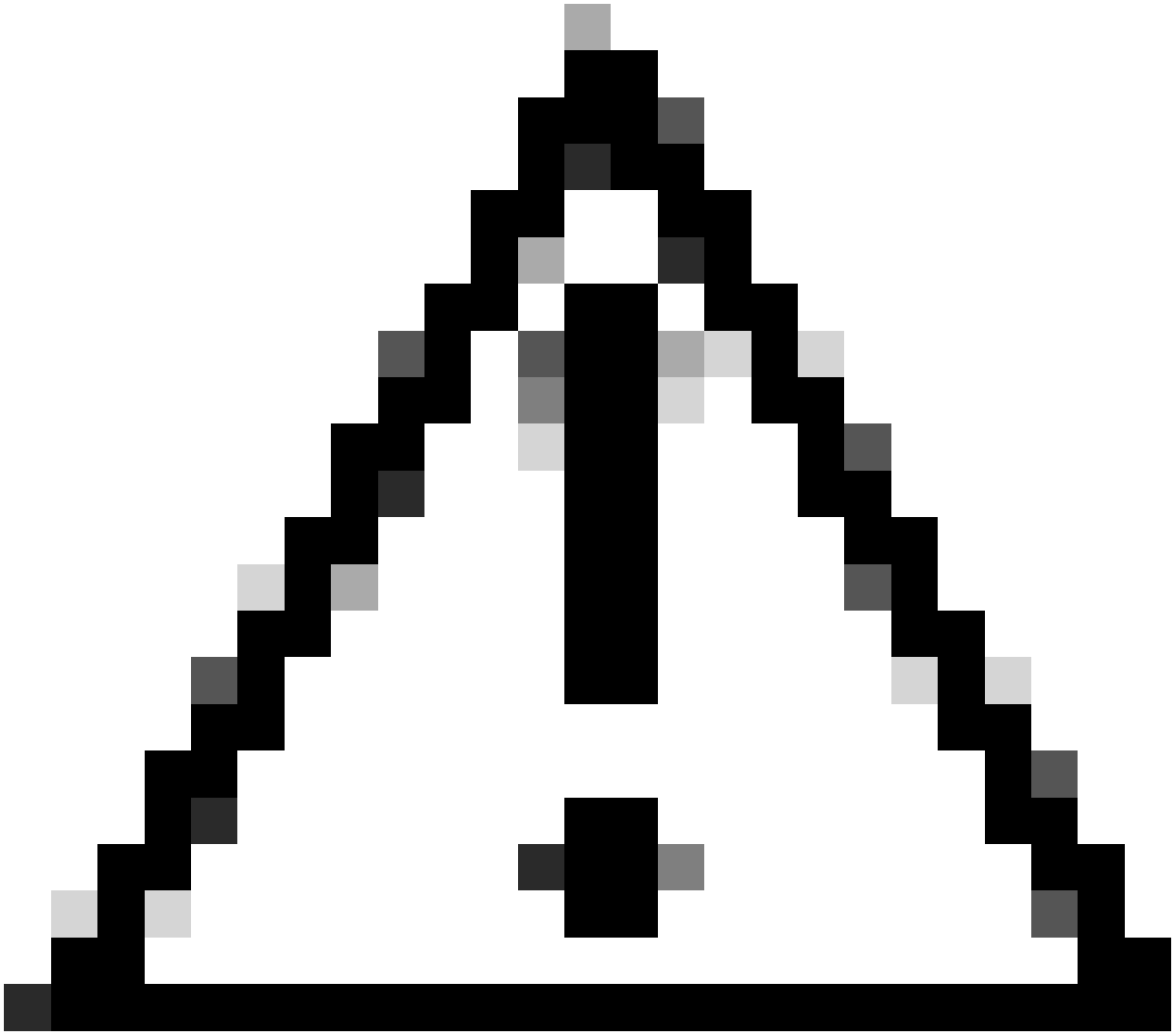
```
CGW#

show mac address-table address 0000.beef.cafe

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

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

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

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

Fehlerbehebung

Adressenauflösung (ARP)

Allgemeine Schritte zur Isolierung von ARP-Problemen

- Bestätigen, dass der IMET-Tunnel bereit ist
- Erfassung auf dem CGW-Uplink, um zu überprüfen, ob ARP vom Leaf gekapselt empfangen wurde
- Wenn kein ARP beim Uplink ankommen würde
    - Überprüfen Sie, ob der IMET-Tunnel auf Leaf und CGW bereit ist
    - Erfassung an Leaf-Uplinks zur Bestätigung, dass ARP gekapselt und gesendet wird
    - Fehlerbehebung bei Zwischenpfaden
- Wenn ARP bei der Erfassung des Border IMET-Tunnels eintrifft, aber nicht in der VRF-ARP-Tabelle programmiert ist
    - Fehlerbehebung bei CPU-/CoPP-Punt-Pfad zur Bestätigung, dass ARP auf die CPU angewendet wurde
    - Bestätigen Sie, dass die IP-Adresse/Client-Informationen richtig sind
    - Debuggen von ARP in VRF, um festzustellen, welche Auswirkungen der ARP-Prozess haben könnte
- Überprüfen Sie, ob die CGW-MAC als Next Hop-/Destest-MAC auf den Hosts installiert ist.
- Vergewissern Sie sich, dass der CGW über beide ARP-Einträge mit den echten Host-MACs verfügt.
- Überprüfung, ob die Firewall-Richtlinie diesen Datenverkehr zulässt



Vorsicht: Seien Sie vorsichtig, wenn Sie Debug-Programme aktivieren!

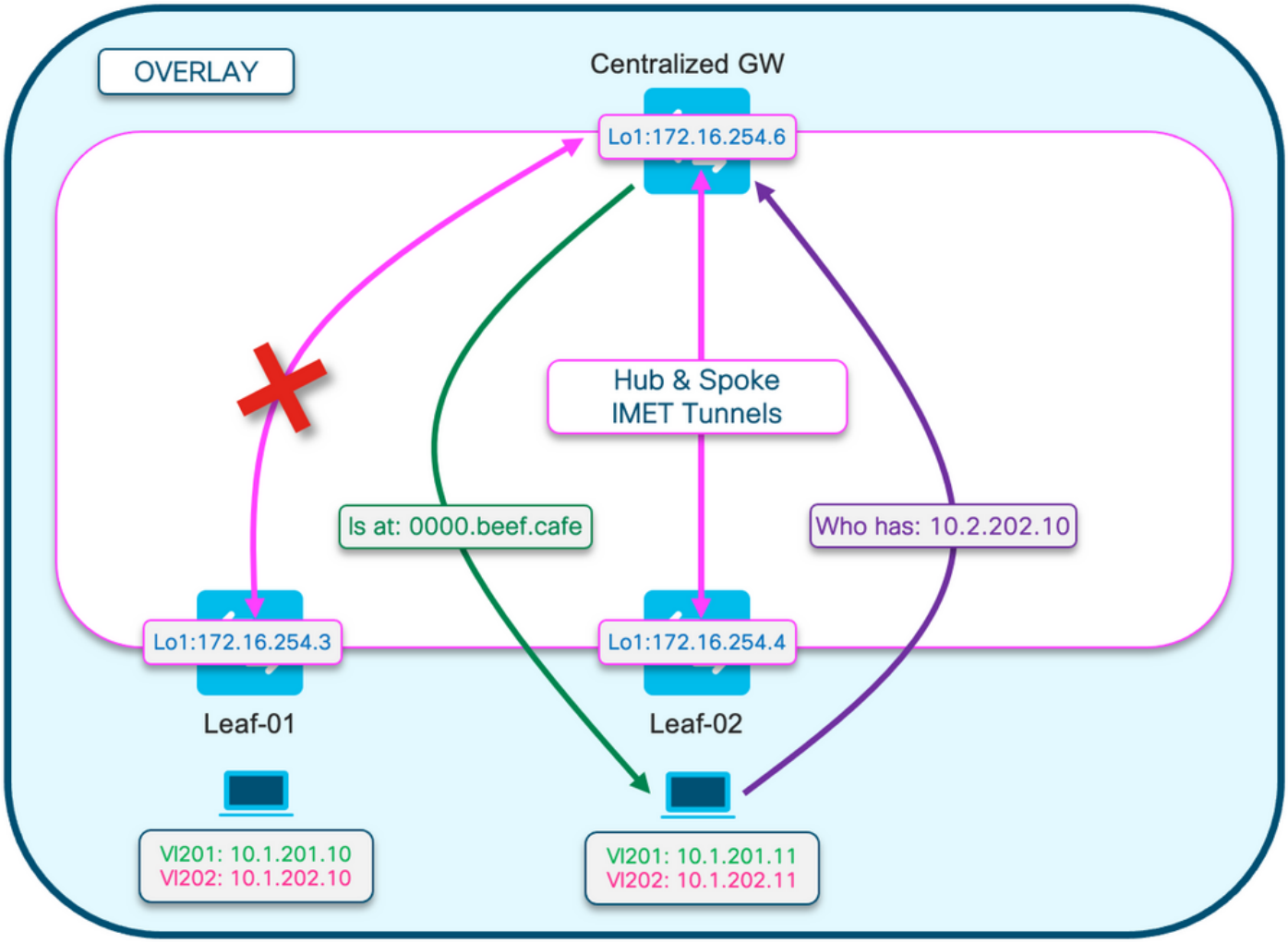
Stellen Sie sicher, dass Sie die Überflutungsunterdrückung deaktiviert haben.

<#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
```

Wenn der Host von Leaf-02 ARP für den Host von Leaf-01 auflöst, wird die ARP-Anforderung nicht direkt an Leaf-01 gesendet.

- Der ARP wird stattdessen über den einzigen BUM-Tunnel geleitet, der auf Leaf-02 in Richtung CGW programmiert wurde.
- Der CGW leitet diese Nachricht nicht an Leaf-01 weiter und antwortet stattdessen mit einer eigenen MAC-Adresse
- Dadurch wird die gesamte Kommunikation an den CGW weitergeleitet und dann zwischen den Hosts weitergeleitet.
- Der CGW leitet Pakete weiter, selbst wenn sie sich im gleichen lokalen Subnetz befinden.



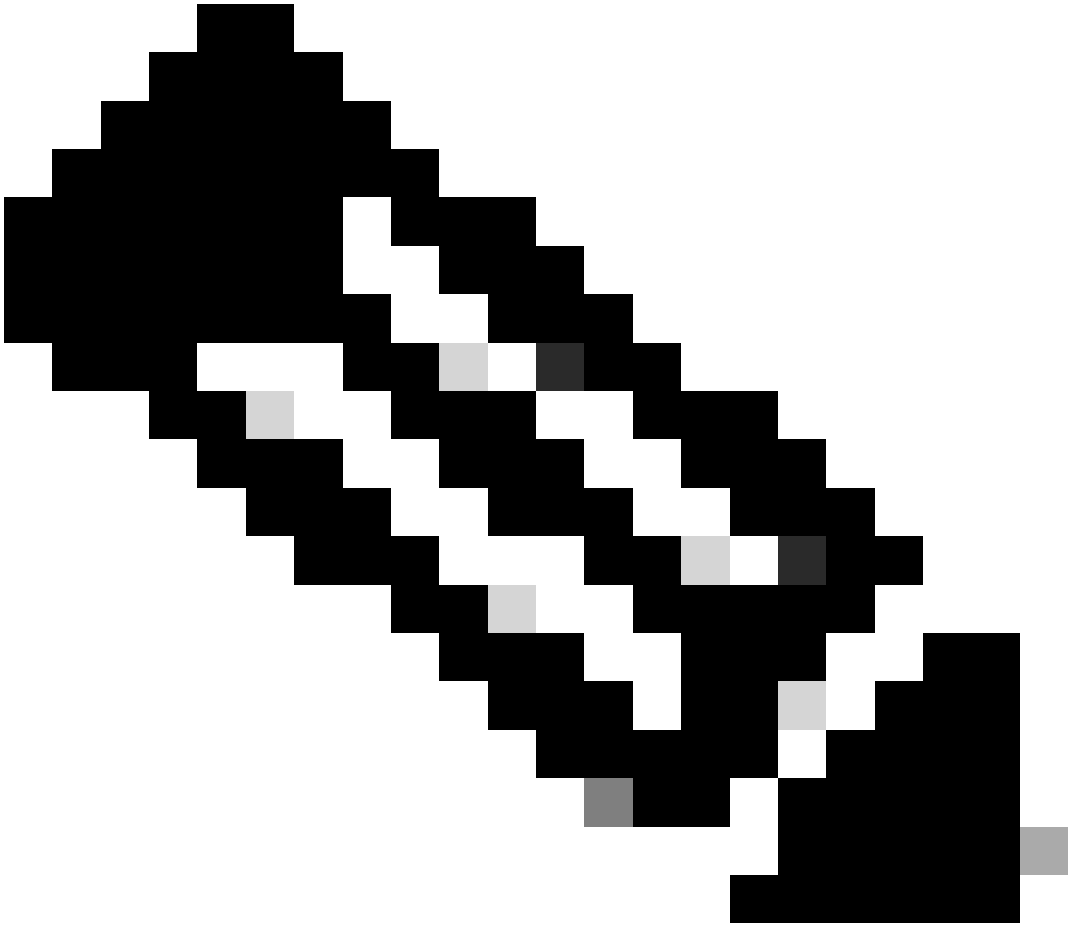
Dieses Diagramm soll Ihnen helfen, den in diesem Abschnitt beschriebenen Ablauf der ARP-Auflösung zu veranschaulichen.

Die ARP-Anforderung wird lila angezeigt.

- Diese ARP-Anforderung dient zum Auflösen der MAC-Adresse des Hosts 10.1.202.10 von Leaf-01.
- Beachten Sie, dass die violette Linie am CGW endet und nicht Leaf-01 erreicht.

Die ARP-Antwort wird grün angezeigt.

- Die Antwort enthält die MAC-Adresse der CGW SVI für VLAN 202
- Beachten Sie, dass die grüne Linie vom CGW kommt und nicht vom eigentlichen Host



Hinweis: Das rote X bedeutet, dass diese Kommunikation keinen Datenverkehr an Leaf-01 gesendet hat.

Beobachten der ARP-Einträge auf jedem Host

<#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

Beobachten Sie, dass auf dem CGW die RT2-Präfixe gelernt wurden. Dies ist erforderlich, damit der CGW Pakete routen kann.

<#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
```

Erfassen Sie den ARP-Austausch an den Uplinks, um die bidirektionale Kommunikation zu bestätigen.

- Sie können Embedded Packet Capture (EPC) auf den Fabric-Uplinks verwenden.
- Dieses Szenario zeigt EPC auf dem Leaf01-Uplink. Wiederholen Sie diesen Vorgang bei Bedarf auf dem CGW.

Konfigurieren des 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
```

Erfassung starten

```
<#root>

Leaf01#

monitor capture 1 start
```

Initiieren von Ping zum Auslösen der ARP-Anforderung (in diesem Fall erfolgt der Ping von Leaf01-Host 10.1.201.10 an Leaf02-Host 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
```

Anhalten der Erfassung und Überprüfung auf ARP-Frames

<#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

Zeigen Sie die Erfassungspakete im Detail an. Wenn Sie weitere Informationen über das Paket anzeigen möchten, verwenden Sie die Detailoption von EPC.

- Beachten Sie, dass diese Ausgabe aus Gründen der Kürze an verschiedenen Stellen abgeschnitten wird.

<#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

CGW RT2-Gateway-Präfix

Gateway-Präfix fehlt

Wie im vorherigen Abschnitt zu teilweise isolierten Segmenten erwähnt, muss die MAC-Adresse im Fabric-VLAN gelernt werden.

- Dieses Problem kann sich zeigen, wenn kein Datenverkehr für das Gateway vorhanden ist, der länger ist als der MAC-Aging-Timer.
- Wenn das CGW-Gateway-Präfix fehlt, müssen Sie die MAC-Adresse bestätigen

<#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
```

Fehlende Behebung des Gateway-Präfix

In den meisten Produktionsnetzwerken ist zu jeder Zeit ein gewisser Datenverkehr wahrscheinlich. Wenn Sie jedoch dieses Problem haben, können Sie eine der folgenden Optionen verwenden, um das Problem zu beheben:

- Fügen Sie einen statischen MAC-Eintrag hinzu, z. B. "mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1".
- Erhöhen Sie den MAC-Alterungs-Timer mit 'mac address-table aging-time <seconds>'. (Beachten Sie, dass sich dadurch die Alterungszeit für alle MAC-Adressen erhöht, daher wird die statische MAC-Option bevorzugt)

DEF GW-Attribut fehlt

Bei teilweise isolierten Segmenten gibt es eine Reihe zusätzlicher Konfigurationen, um dieses Attribut hinzuzufügen.

Fehlerbehebung für DEF-GW-Attribut fehlt

Bestätigen Sie folgende Angaben:

- Sie führen 17.12.1 oder höher aus.
- Die SISF-CLI (Device-Tracking) ist in der Konfiguration vorhanden.
- Die Befehle route-map match und set werden konfiguriert, und route-map wird auf die BGP-Nachbarn angewendet
- Sie haben die BGP-Meldungen aktualisiert (Sie müssen das BGP löschen, um das Präfix mit dem neuen Attribut erneut anzukündigen).

Wireless-Roaming

Häufiges Roaming kann dazu führen, dass das BGP zu häufig aktualisiert wird. Das Roaming pro Zeitintervall sollte erhöht werden, bevor der Switch erklärt, dass er Eigentümer der MAC ist, und RT2-Update sendet.

- Dies tritt auf, wenn sich ein Host zwischen zwei APs auf unterschiedlichen Switches bewegt.
- Der Standardgrenzwert für Roaming ist 5 pro 180 Sekunden.

<#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...>
```

Zu erfassende Befehle für TAC

Falls Ihr Problem durch diesen Leitfaden nicht behoben werden konnte, sammeln Sie die angezeigte Befehlsliste, und fügen Sie sie Ihrer TAC-Serviceanfrage bei.

Zu erfassende Mindestinformationen

(begrenzte Zeit für das Sammeln von Daten vor dem erneuten Laden/Wiederherstellen der Daten)

- Technisches EVPN- anzeigen
- Technologie anzeigen
- TechSF anzeigen

Zu erfassende detaillierte Informationen

(Wenn es Zeit gibt, vollständigere Daten zu sammeln, wird dies bevorzugt)

- technische anzeigen
- Show tech evpn
- show tech platform evpn_vxlan switch <Nummer>
- Show-Tech-Plattform
- zeigen technische Ressource
- show tech sisf
- Show Tech
- show tech bgp
- show monitor event-trace evpn event all
- show monitor event-trace evpn error all
- Anforderungsplattform Software-Ablaufverfolgungsarchiv

Zugehörige Informationen

- Implementierung einer BGP-EVPN-Routing-Richtlinie auf Catalyst Switches der Serie 9000
- DHCP Layer 2 Relay (in Kürze verfügbar)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.