Implementazione della segmentazione della sovrimpressione protetta da BGP VPN sugli switch Catalyst serie 9000

Sommario

Introduzione

Questo documento descrive come implementare la segmentazione della sovrimpressione protetta VXLAN BGP sugli switch Catalyst serie 9000.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti della VxLAN BGP VPN
- Risoluzione dei problemi unicast VPN BGP
- Politica di routing BGP VPN VxLAN

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Descrizione funzionalità di alto livello

La funzione di protezione del segmento impedisce alle porte di inoltrare il traffico tra loro, anche se

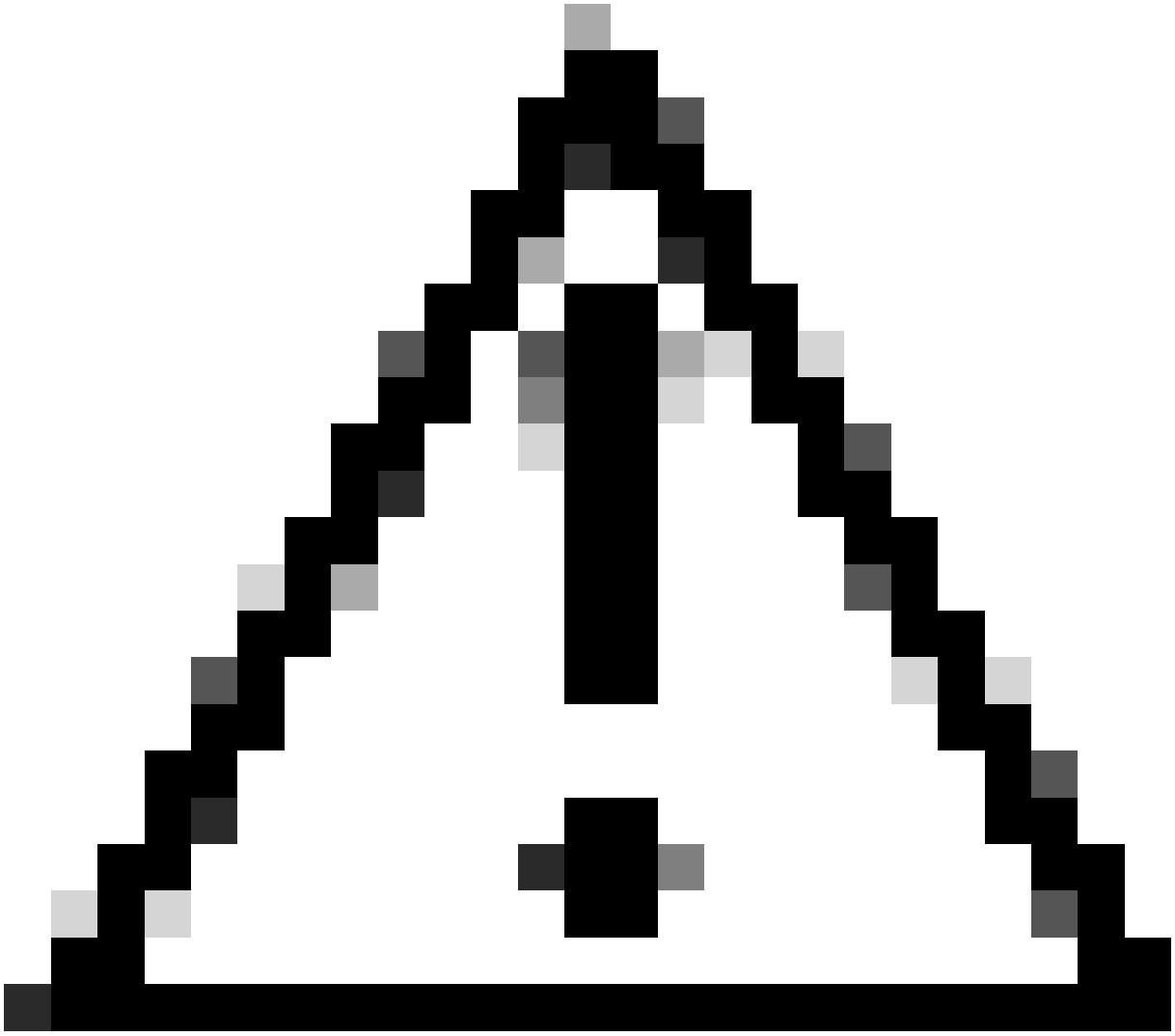
si trovano sulla stessa VLAN e sullo stesso switch

- Questa funzione è simile alla funzione 'switchport protected' o alle VLAN private, ma per i fabric EVPN.
- Questo progetto forza tutto il traffico diretto al CGW dove può essere ispezionato da un firewall prima di essere inviato alla destinazione finale.
- Grazie a un'appliance di sicurezza centralizzata, i flussi di traffico sono controllati, deterministici e facilmente ispezionabili.

Dettagli documento

Questo documento è la parte 2 o 3 di documenti correlati:

- Documento 1: Implementazione della policy di routing BGP VPN sugli switch Catalyst serie 9000 descrive come controllare il traffico BGP BUM nell'overlay e deve essere configurato per primo
- Documento 2: Questo documento. Basato sulla progettazione e la policy di overlay del documento 1, questo documento descrive l'implementazione della parola chiave 'protected'
- Documento 3: Implementazione del relay DHCP BGP EVP sul layer 2 sugli switch Catalyst serie 9000 illustra il funzionamento del relay DHCP su un VTEP solo L2



Attenzione: prima di implementare le configurazioni dei segmenti protetti, è necessario implementare la configurazione descritta nel documento 1.

Tipi di segmento protetti

Totalmente isolato

- Consente solo le comunicazioni da Nord a Sud e
- Il gateway viene annunciato nell'infrastruttura con la CLI 'default-gateway annuncio'

Per lo più isolato

- Consente le comunicazioni da Nord a Sud (in questo caso i flussi di traffico da Est a Ovest sono consentiti in base alle policy di traffico del firewall)
- Consente le comunicazioni da est a ovest (in base ai criteri di traffico del firewall)
- Il gateway è esterno alla struttura e la SVI non viene pubblicizzata utilizzando la CLI 'default-

gateway advertising'

Comportamento switch

- Gli host non possono comunicare direttamente tra loro anche se sono collegati allo stesso switch (la richiesta ARP non viene inviata alle altre porte dello stesso switch quando gli host si trovano nello stesso VRF/Vlan/Segment)
- Nessun traffico BUM tra VTEP L2 (prefissi IMET filtrati utilizzando la configurazione dei criteri di routing)
- Tutti i pacchetti provenienti dagli host vengono inoltrati a Border Leaf per essere inoltrati. (Questo significa che l'host 1 deve comunicare con l'host 2 sulla stessa foglia, il traffico è bloccato fino al CGW)

Gestione tipo di ciclo di lavorazione 2

- I fogli di accesso pubblicizzano l'RT2 locale con la comunità estesa E-Tree e il flag Foglia impostato
- Access Leafs non installa alcun RT2 remoto ricevuto con E-Tree Extended Community e Flag Foglia impostato nel piano dati
- I fogli di Access non installano l'uno l'altro RT2 nel piano dati.
- Access Leafs e Border Leaf (CGW) installano l'un l'altro RT2 nel piano dati.
- Non è richiesta alcuna modifica alla configurazione su Access Leaf o Border Leaf.

Riepilogo della progettazione

- Per il broadcast (BUM), la topologia RT3 è hub e spoke per forzare il traffico broadcast come ARP fino alla GCW.
- Per tenere conto della mobilità dell'host, l'RT2 è una mesh completa sul control plane BGP (quando un host si sposta da un VTEP all'altro, il numero Seq viene incrementato nell'RT2)
- Il piano dati installa in modo selettivo gli indirizzi MAC.
    - Una foglia installa solo MAC locali e RT2 che contengono l'attributo DEF GW
    - Il CGW non ha il KW protetto e installa tutti gli indirizzi MAC locali e gli RT2 remoti nel suo piano dati.

Terminologia

VRF	Inoltro routing virtuale	Definisce un dominio di routing di livello 3 che deve essere separato da altri VRF e da un dominio di routing IPv4/IPv6 globale
AF	Famiglia indirizzi	Definisce quali prefissi di tipo e informazioni di routing sono handle BGP
AS	Sistema autonomo	Set di prefissi IP instradabili Internet appartenenti a una rete o a un insieme di reti gestite, controllate e supervisionate da una singola entità o

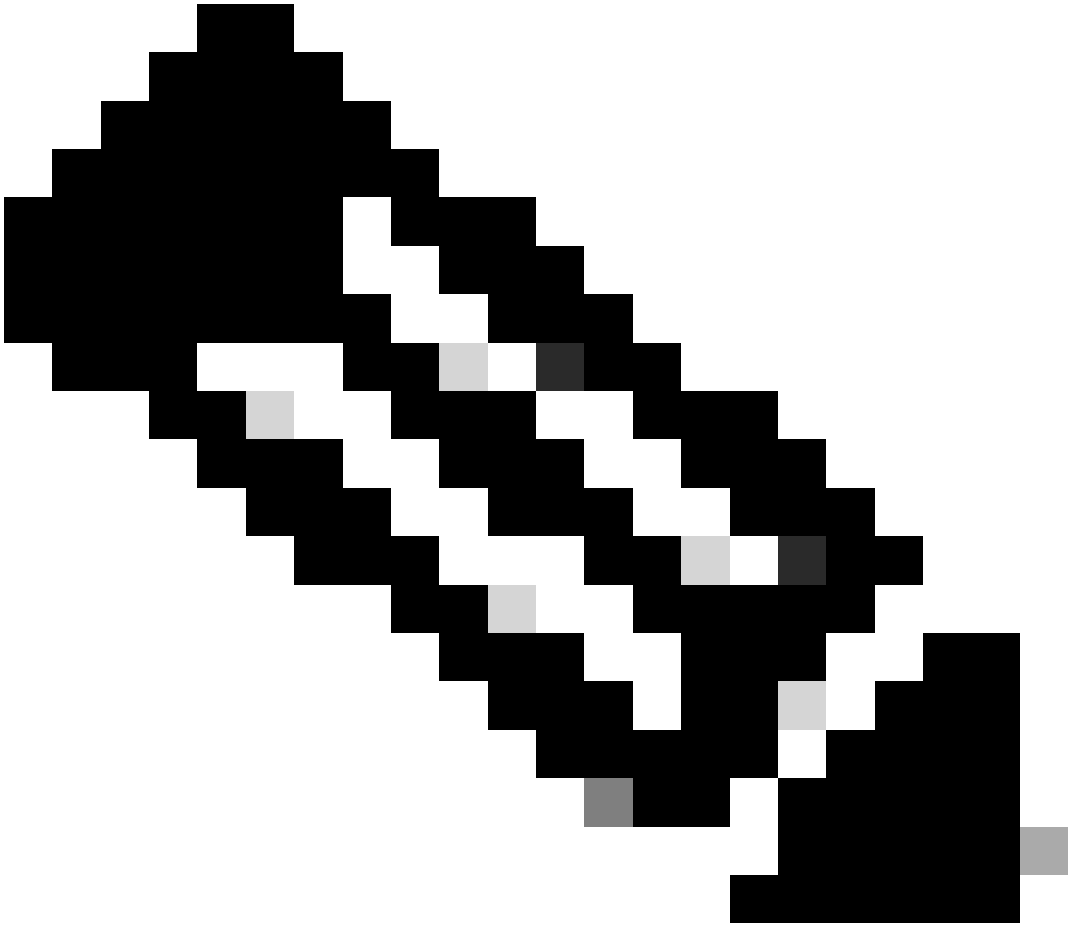
		organizzazione
EVPN	Ethernet Virtual Private Network	L'estensione che consente a BGP di trasportare le informazioni MAC di layer 2 e IP di layer 3 è EVPN e utilizza il protocollo MP-BGP (Multi-Protocol Border Gateway Protocol) come protocollo per distribuire le informazioni sulla raggiungibilità relative alla rete di sovrapposizione VXLAN.
VXLAN	LAN virtuale estendibile (LAN)	La VXLAN è progettata per superare i limiti intrinseci delle VLAN e dell'STP. Si tratta di uno standard IETF [RFC 7348] proposto per fornire gli stessi servizi di rete Ethernet di layer 2 delle VLAN, ma con una maggiore flessibilità. A livello funzionale, è un protocollo di incapsulamento MAC-in-UDP che viene eseguito come sovrimpressione virtuale su una rete sottostante di layer 3.
CGW	Gateway centralizzato	E implementazione di EVPN in cui la SVI del gateway non è su ciascuna foglia. Tutto il routing viene invece eseguito da una foglia specifica utilizzando il protocollo IRB (Integrated Routing and Bridging) asimmetrico
DEF GW	Gateway predefinito	Un attributo della community estesa BGP aggiunto al prefisso MAC/IP tramite il comando "default-gateway annuncio enable" nella sezione di configurazione 'l2vpn evpn'.
IMET (RT3)	Tag Inclusive Multicast Ethernet (Route)	Chiamata anche route BGP di tipo 3. Questo tipo di route viene utilizzato nell'EVPN per consegnare il traffico BUM (broadcast / unicast sconosciuto / multicast) tra i VTEP.
RT2	Tipo di route 2	Prefisso BGP MAC o MAC/IP che rappresenta un MAC host o un MAC-IP gateway
EVPN Mgr	Responsabile EVPN	Componente di gestione centrale per vari altri componenti (ad esempio, apprende da SISF e segnala a L2RIB)
SISF	Funzionalità di sicurezza integrata dello switch	Tabella di rilevamento host agnostica utilizzata da EVPN per individuare gli host locali presenti in una foglia
L2RIB	Base	In un componente intermedio per la gestione delle interazioni tra BGP,

	informazioni routing Layer 2	EVPN Mgr, L2FIB
FED	Driver motore di inoltro	Programmazione del livello ASIC (hardware)
MATM	Mac Address Table Manager	IOS MATM: tabella software che installa solo indirizzi locali e FED MATM: tabella hardware che installa gli indirizzi locali e remoti appresi dal control plane e fa parte del piano di inoltro hardware

Diagrammi di flusso

Diagramma Route-Type 2 (RT2)

Il diagramma mostra la struttura a maglia completa dei prefissi host MAC/MAC-IP di tipo 2.



Nota: per il supporto della mobilità e del roaming è richiesta la rete completa

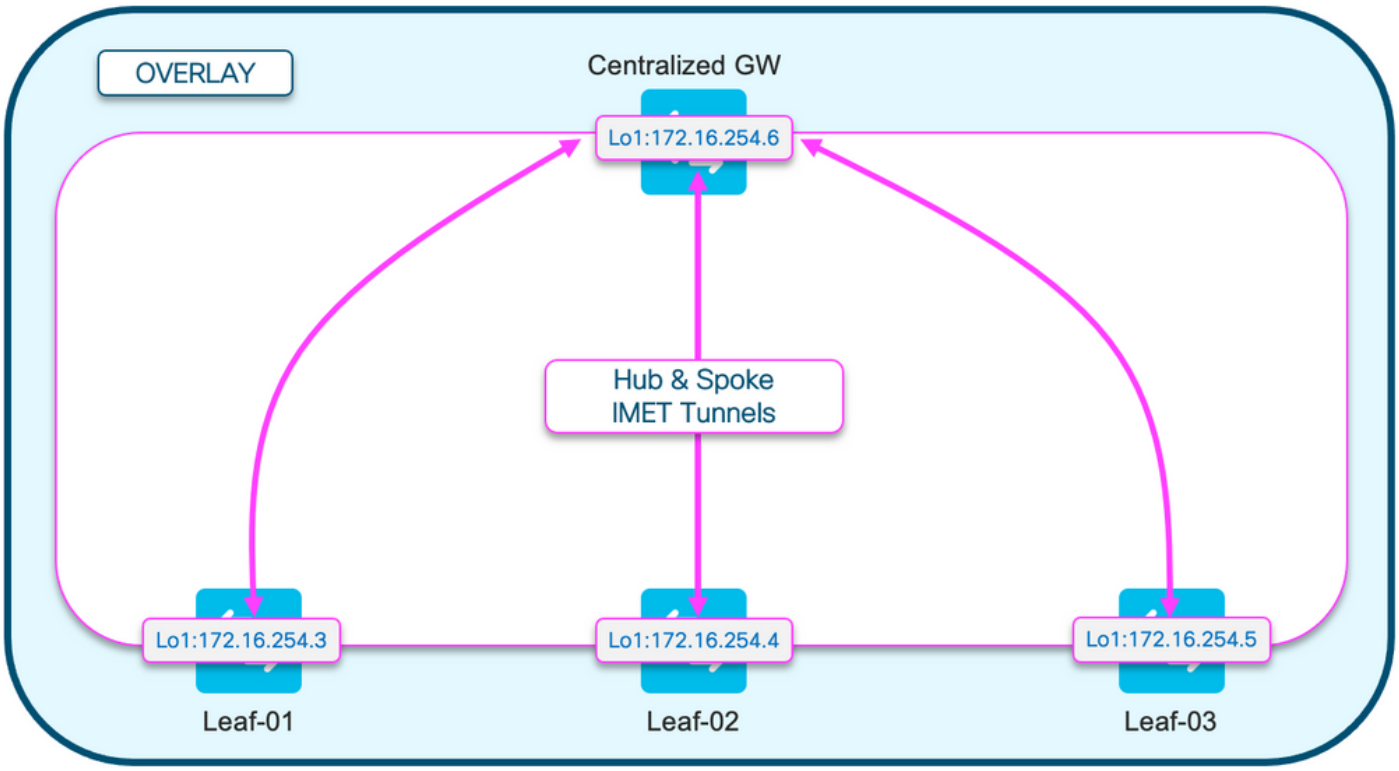
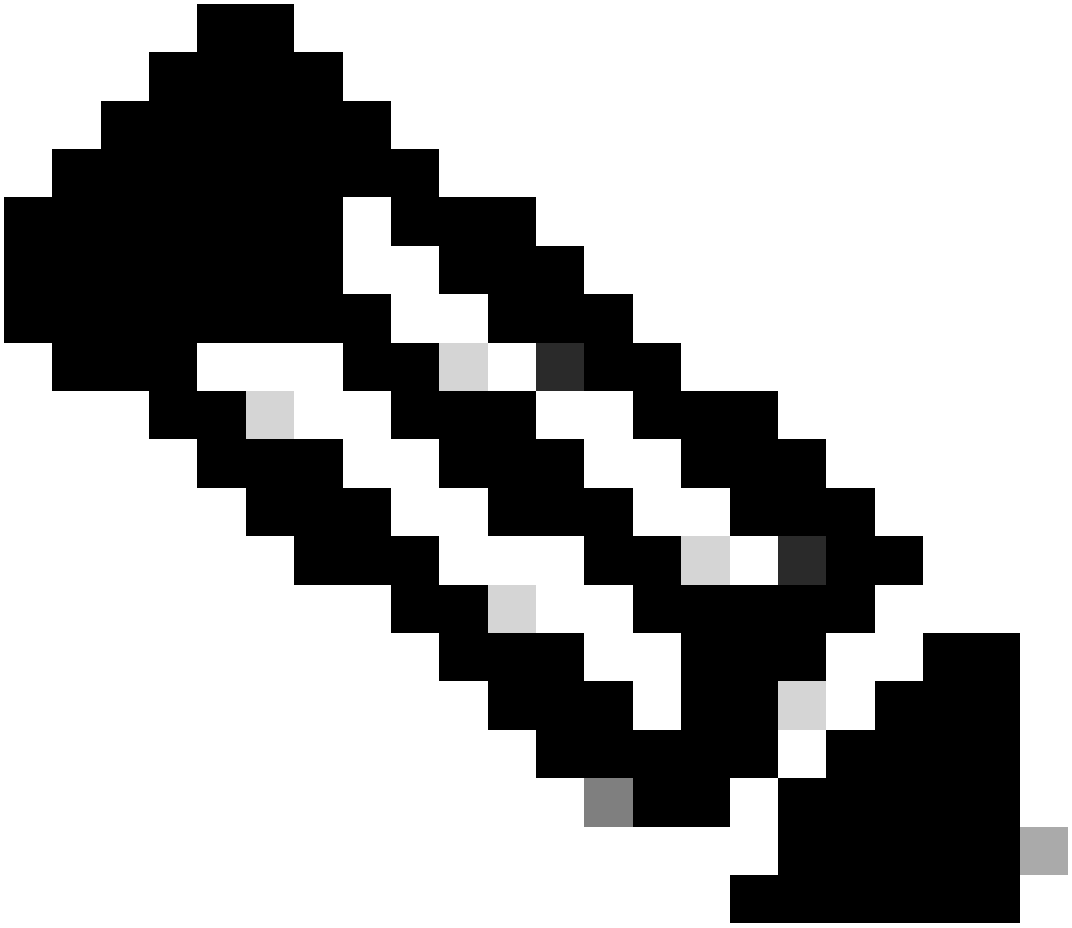


Diagramma RT3 (Route-Type 3)

Il diagramma mostra il design hub and spoke dei tunnel IMET (RT3) broadcast



Nota: la trasmissione Hub and Spoke è necessaria per impedire che foglie con lo stesso segmento inviino trasmissioni l'una all'altra direttamente.

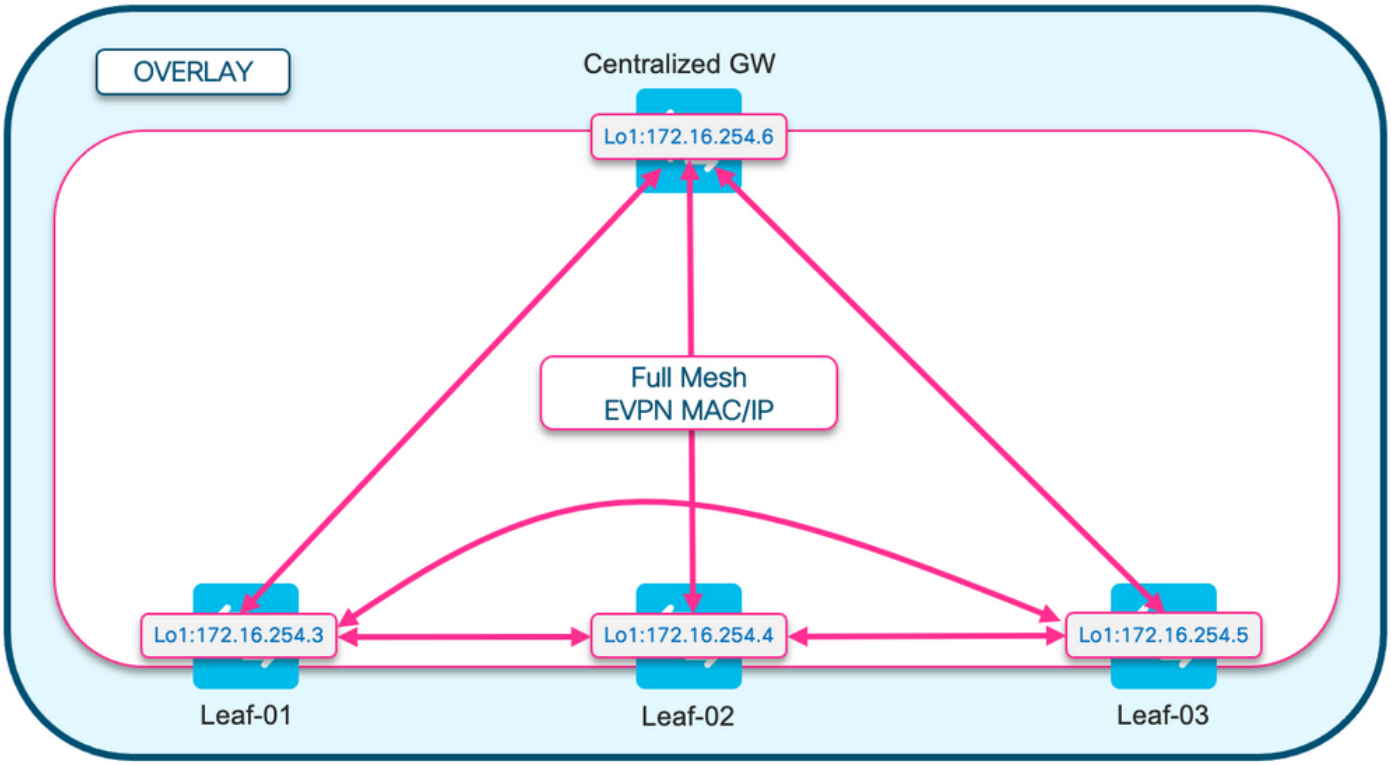
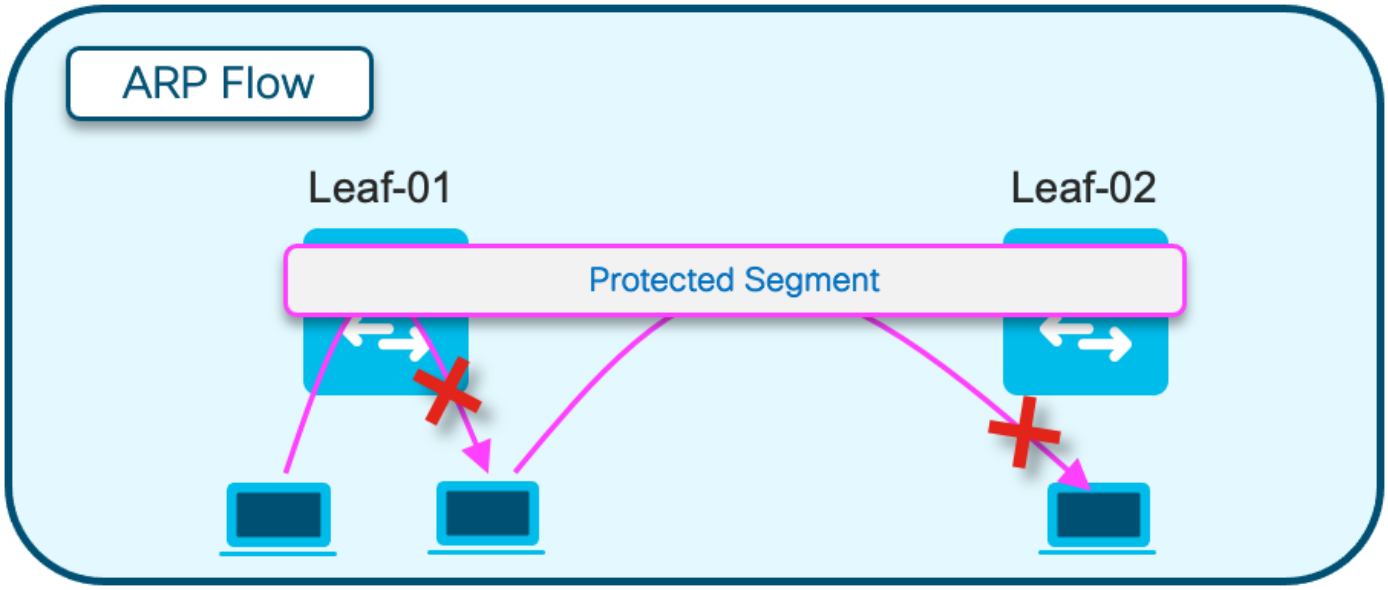
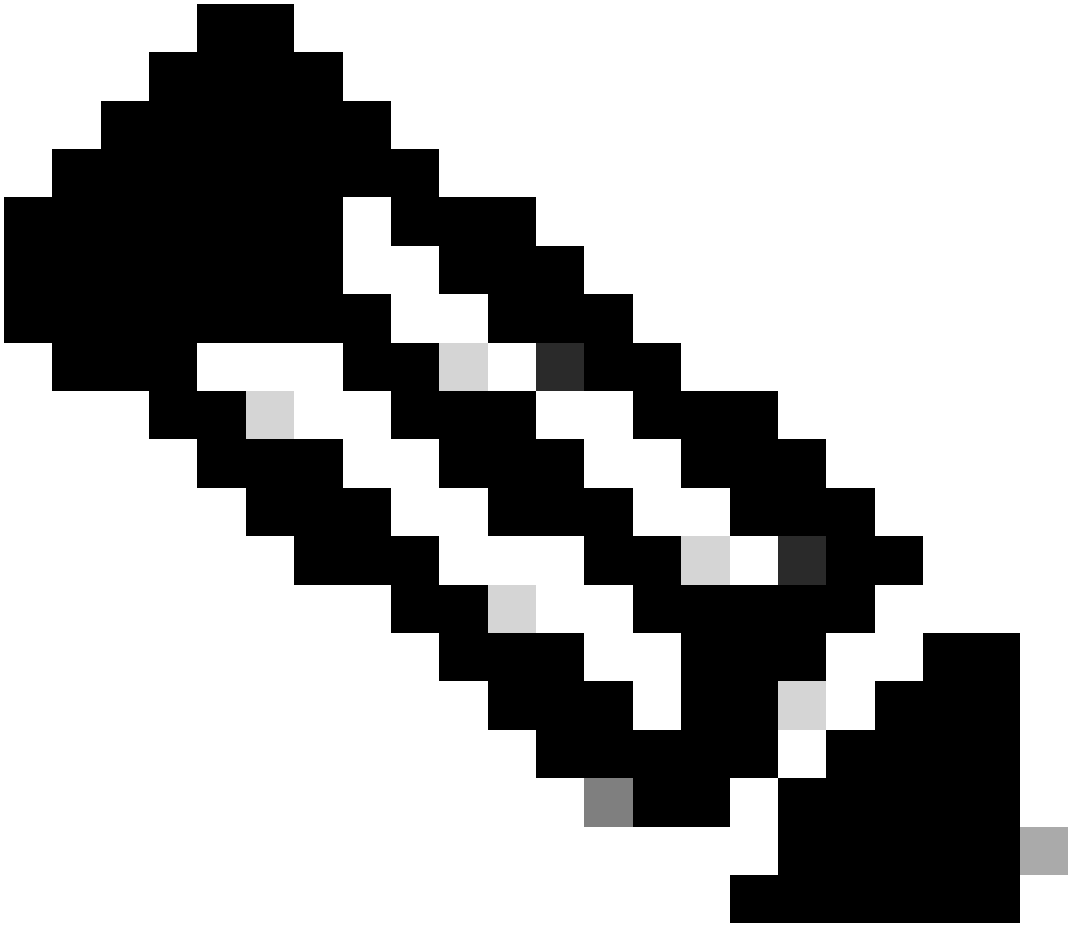


Diagramma Address Resolution (ARP)

Questo diagramma mostra che ARP non può raggiungere alcun host nello stesso segmento EPVN. Quando gli ARP host sono per un altro host, solo CGW ottiene questo ARP e risponde



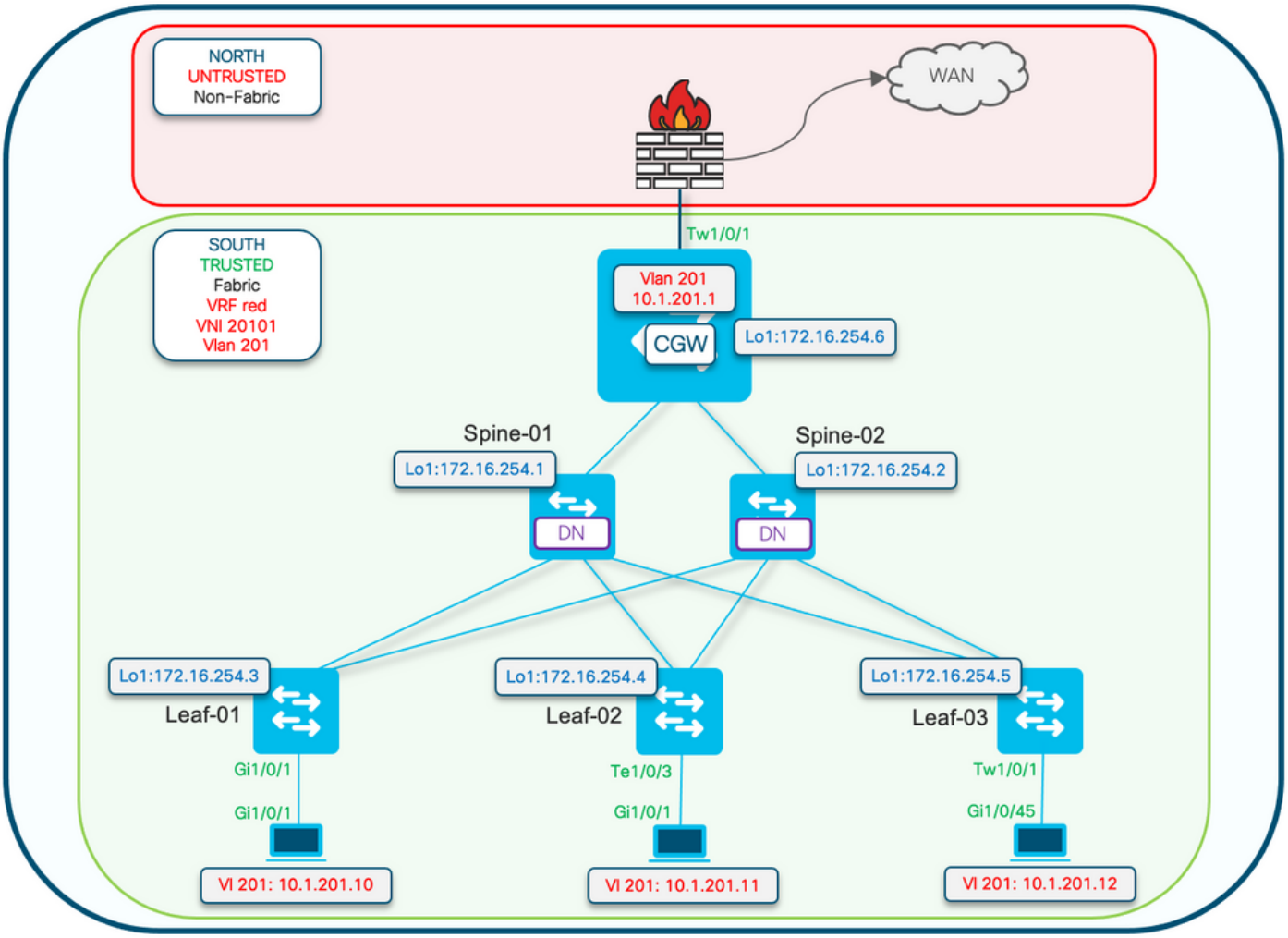


Nota: l'istanza di questa modifica del comportamento ARP viene creata utilizzando la parola chiave 'protected'.

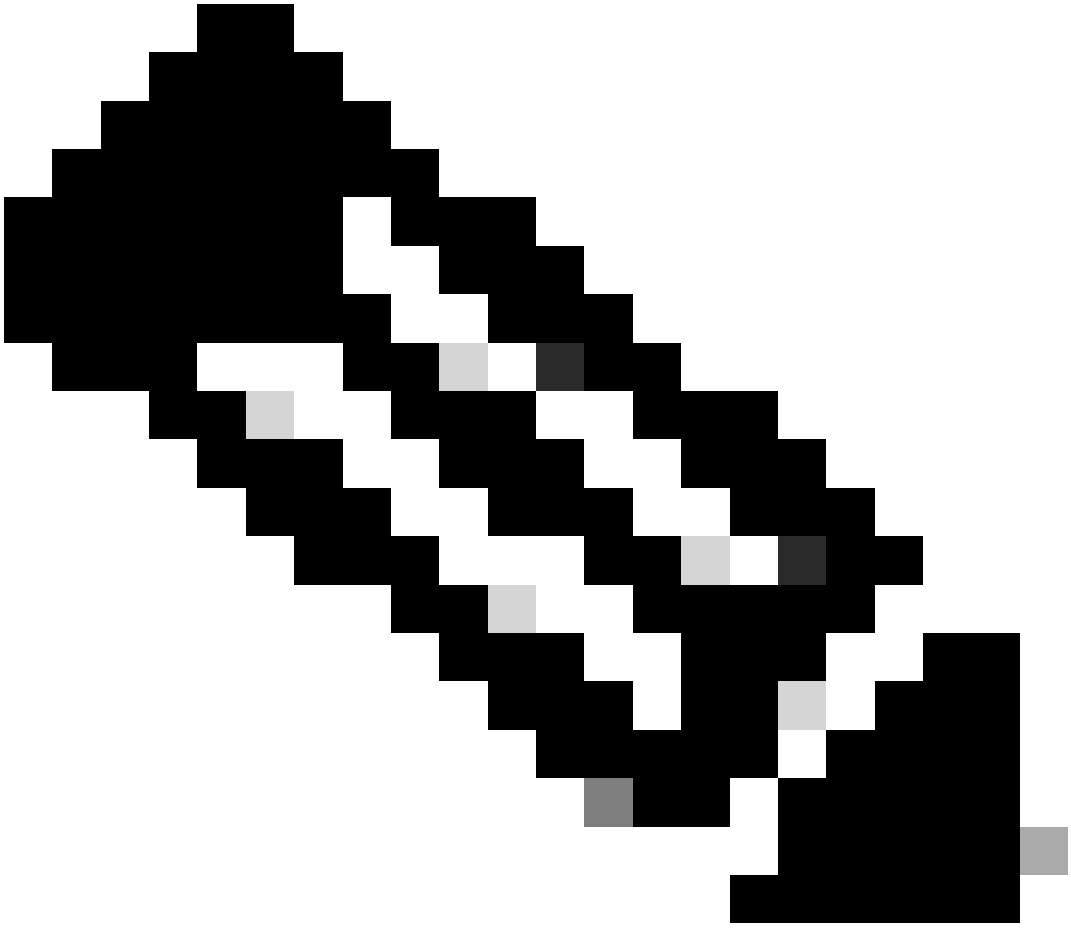
Esempio: membro evpn-instance 202 vni 20201 protected

Configura (completamente isolato)

Esempio di rete



Sugli switch foglia viene applicata la parola chiave Protected configuration. Il CGW è un dispositivo promiscuo e installa tutti gli indirizzi MAC.



Nota: l'elenco delle community dei criteri di routing e la configurazione della route-map che controlla l'importazione/esportazione dei prefissi IMET sono visualizzati in Implementazione della policy di routing BGP VPN sugli switch Catalyst serie 9000. In questo documento vengono mostrate solo le differenze dei segmenti protetti.

Leaf-01 (configurazione EVPN di base)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

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

 router-id Loopback1
l2vpn evpn
```

```
instance 201

 vlan-based
 encapsulation vxlan


replication-type ingress                          <-- Sets segment to use Unicast replication of BUM traff

 multicast advertise enable
```

<#root>

```
Leaf01#

show run | sec vlan config

vlan configuration 201
 member evpn-instance 201 vni 20101

protected  <-- protected keyword added
```

CGW (configurazione base)

<#root>

```
CGW#

show running-config | beg l2vpn evpn instance 201

l2vpn evpn instance 201 vlan-based
 encapsulation vxlan
 replication-type ingress

 default-gateway advertise enable    <-- adds the BGP attribute EVPN DEF GW:0:0 to the MAC/IP prefix

 multicast advertise enable
```

<#root>

```
CGW#

show running-config | sec vlan config

vlan configuration 201
 member evpn-instance 201 vni 20101
```

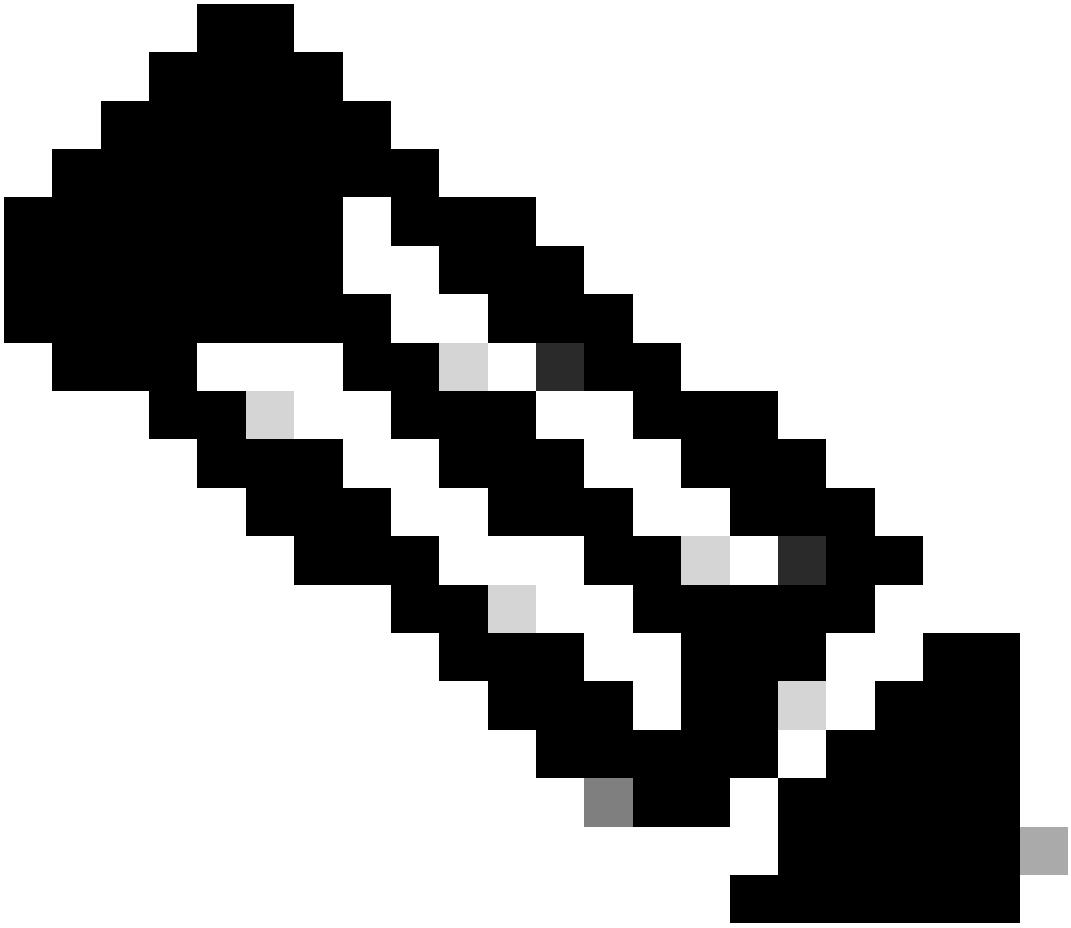
<#root>

```
CGW#

show run int nve 1

Building configuration...
```

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

<#root>

```
CGW#
show run interface vlan 201

Building configuration...

Current configuration : 231 bytes
!
interface Vlan201

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



Nota: in CGW non è applicata alcuna policy BGP. Il CGW può ricevere e inviare tutti i tipi di prefisso (RT2, RT5 / RT3).

Verifica (completamente isolato)

Dettagli EVI

<#root>

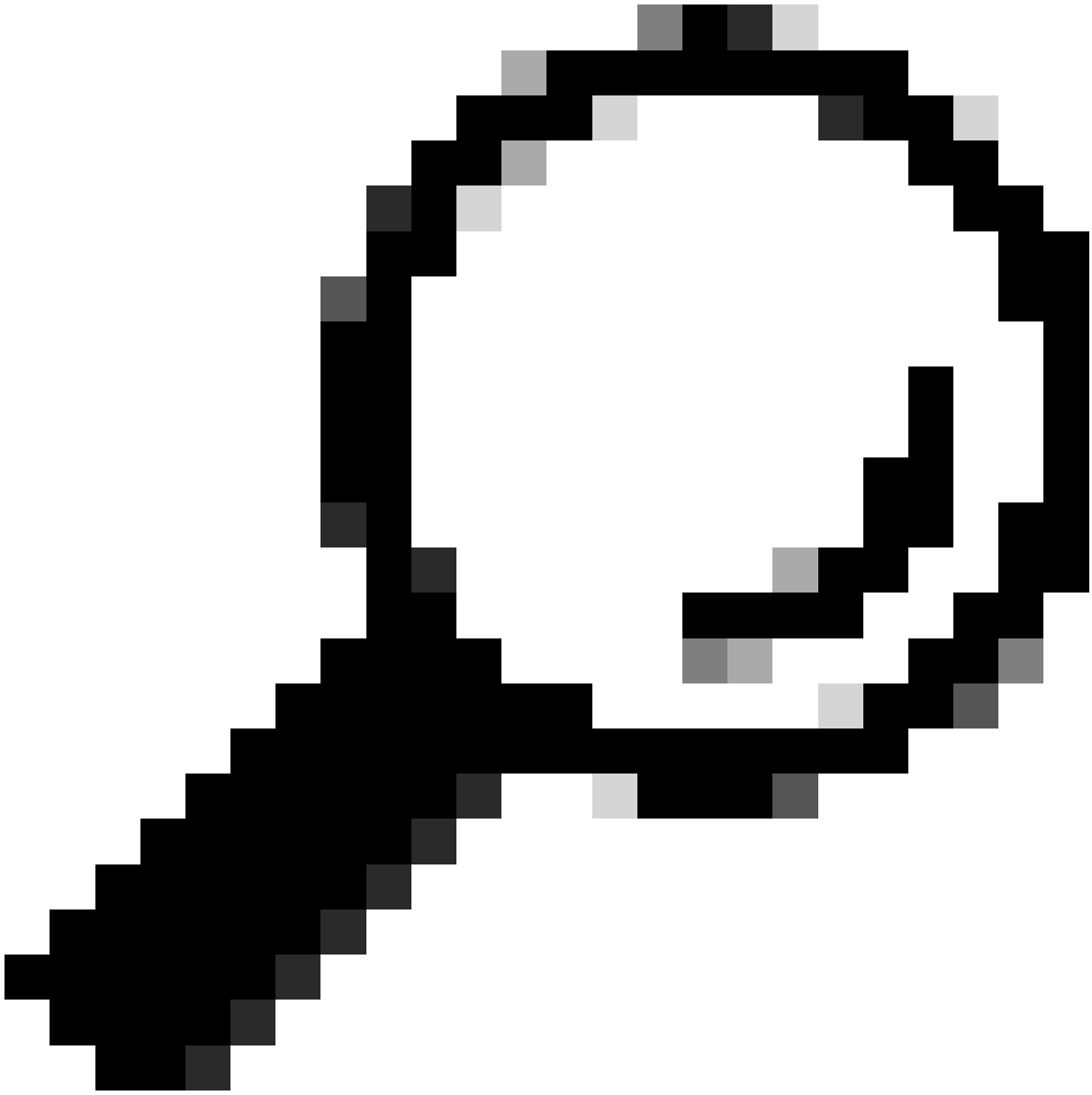
```
Leaf01#

sh l2vpn evpn evi 201 detail

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

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


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

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

Generazione RT2 locale (da host locale a RT2)

Verificare la catena di dipendenze dei componenti dall'apprendimento dell'host locale alla generazione RT2:

- SISF (mentre il Leaf non ha una SVI, il SISF fornisce ancora le informazioni sull'host tramite il frame ARP dall'host)
- EVPN Mgr
- L2RIB
- BGP

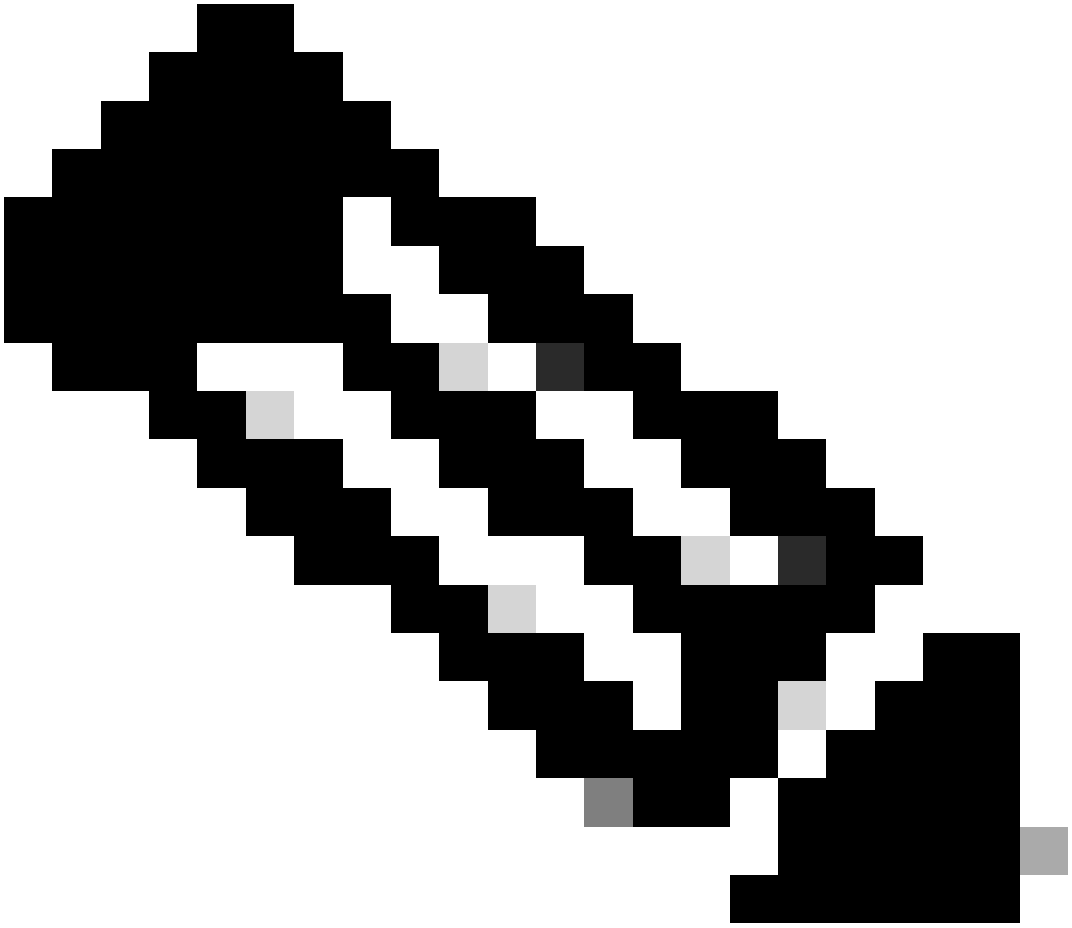


Suggerimento: se un componente precedente non è programmato correttamente, l'intera catena delle dipendenze si interrompe (ad esempio, SISF non dispone di una voce end, BGP non è in grado di creare un RT2).

SISF

Verificare che l'host sia stato appreso nel database da SISF (informazioni host apprese da DHCP o ARP)

- Il SISF apprende le voci MAC dall'apprendimento IOS-MATM e quindi le invia a EVPN Mgr (deve essere raggiungibile tramite MAC con il criterio "evpn-sisf-policy").
- SISF fornisce un binding IP/MAC su un VTEP locale e, utilizzando EVPN manager, prevede che le informazioni vengano programmate come route /32 tramite BGP ad altri leafs.



Nota: poiché l'host dispone di un indirizzo IP statico, SISF utilizza ARP per ottenere i dettagli dell'host. Nella sezione Principalmente isolati, è visualizzato DHCP e DHCP snooping.

<#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
```

Responsabile EVPN

EVPN Mgr apprende l'indirizzo MAC locale e lo installa in L2RIB. EVPN Mgr apprende anche l'indirizzo MAC remoto da L2RIB, ma la voce viene utilizzata solo per l'elaborazione della mobilità MAC

Conferma EVPN Mgr viene aggiornato con la voce SISF

```
<#root>

Leaf01#

show l2vpn evpn mac evi 201

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

0006.f601.cd43 201   201

0000.0000.0000.0000.0000 0

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

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

L2RIB

- L2RIB apprende l'indirizzo MAC locale da EVPN Mgr e lo invia a BGP e L2FIB
- L2RIB è anche responsabile dell'apprendimento di MAC remoti da BGP per aggiornare EVPN Mgr e L2FIB.
- L2RIB richiede sia locale che remoto per il corretto aggiornamento degli altri componenti.
- Il componente L2RIB si colloca tra l'apprendimento MAC locale e remoto a seconda della direzione/componente da aggiornare

Verificare che L2RIB sia aggiornato con l'indirizzo MAC locale da EVPN Mgr

```
<#root>

Leaf01#
```

show l2route evpn mac topology 201 <-- View the overall topology for this segment

EVI ETag

Prod

Mac Address Next Hop(s) Seq Number

----- ---------- ----- -------------- ---------- ----------

201 0

BGP

0000.beef.cafe V:20101 172.16.254.6 0

<-- produced by BGP who updated L2RIB (remote learn)

201 0

L2VPN

0006.f601.cd43 Gi1/0/1:201 0

<-- produced by EVPN Mgr who updated L2RIB (local learn)

Leaf01#

show l2route evpn mac mac-address 0006.f601.cd43 detail

EVPN Instance: 201

Ethernet Tag: 0

Producer Name: L2VPN <-- Produced by local

MAC Address: 0006.f601.cd43 <-- Host MAC Address

Num of MAC IP Route(s): 1
Sequence Number: 0
ESI: 0000.0000.0000.0000.0000
Flags: B()

Next Hop(s): Gi1/0/1:201 (E-LEAF) <-- Port:Instance and info about the Role (Leaf)

BGP

Verificare che BGP sia aggiornato da 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
```

Apprendimento remoto RT2 (gateway predefinito RT2)

BGP

Verificare che BGP abbia imparato il prefisso CGW RT2

<#root>

```
Leaf01#
```

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

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

table evi_201

```
)
```

<-- EVI context is 201

```
  Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 2
  Local, imported path from [2][172.16.254.6:201][0][48][0000BEEFCAFE][32][10.1.201.1]/24 (global)
    172.16.254.6 (metric 3) (via default) from 172.16.255.1 (172.16.255.1)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000,

Label1 20101                <-- Correct segment identifier

      Extended Community: RT:65001:201 ENCAP:8

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

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

L2RIB

Verifica aggiornamento BGP di L2RIB

- L2RIB apprende l'indirizzo MAC locale da EVPN Mgr e lo invia a BGP e L2FIB. L2RIB è anche responsabile dell'apprendimento di MAC remoti da BGP per aggiornare EVPN Mgr e L2FIB.
- L2RIB richiede sia locale che remoto per il corretto aggiornamento degli altri componenti.
- Il componente L2RIB si trova tra l'apprendimento MAC locale e remoto a seconda della direzione e del componente da aggiornare.

<#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

Verifica in L2FIB

- Componente responsabile dell'aggiornamento di FED con gli indirizzi MAC per la programmazione nell'hardware.
- Le voci MAC remote installate da L2FIB in FED-MATM NON sono collegate a IOS-MATM. (IOS-MATM mostra solo i MAC locali, mentre FED-MATM mostra sia i MAC locali che quelli remoti).
- L'output L2FIB mostra solo MAC remoti (non è responsabile della programmazione di MAC locali).

<#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

Verifica in FED MATM

- A livello di hardware dei fogli configurati con la parola chiave protected, dovrebbero essere visualizzati solo il MAC gateway predefinito CGW e i MAC host locali.
- Lo switch cerca il prefisso RT2 per l'attributo DEF GW per determinare quale MAC remoto è idoneo per l'installazione.

<#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
```

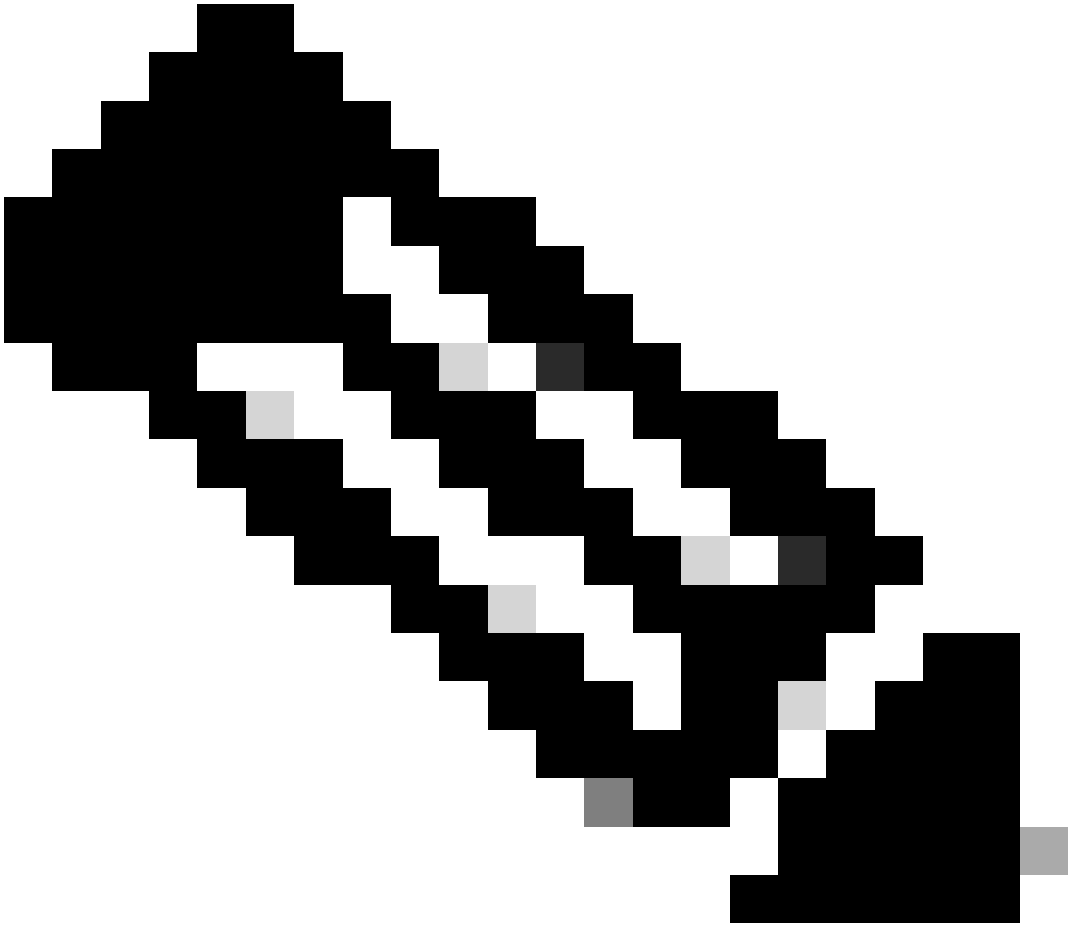
```
MAT_LISP_GW_ADDR 0x4000000
MAT_DYNAMIC_ADDR 0x1
```

Adiacenza piano dati

Come ultimo passo dopo la conferma dell'ingresso FED, potete risolvere l'indice di riscrittura (RI)

<#root>

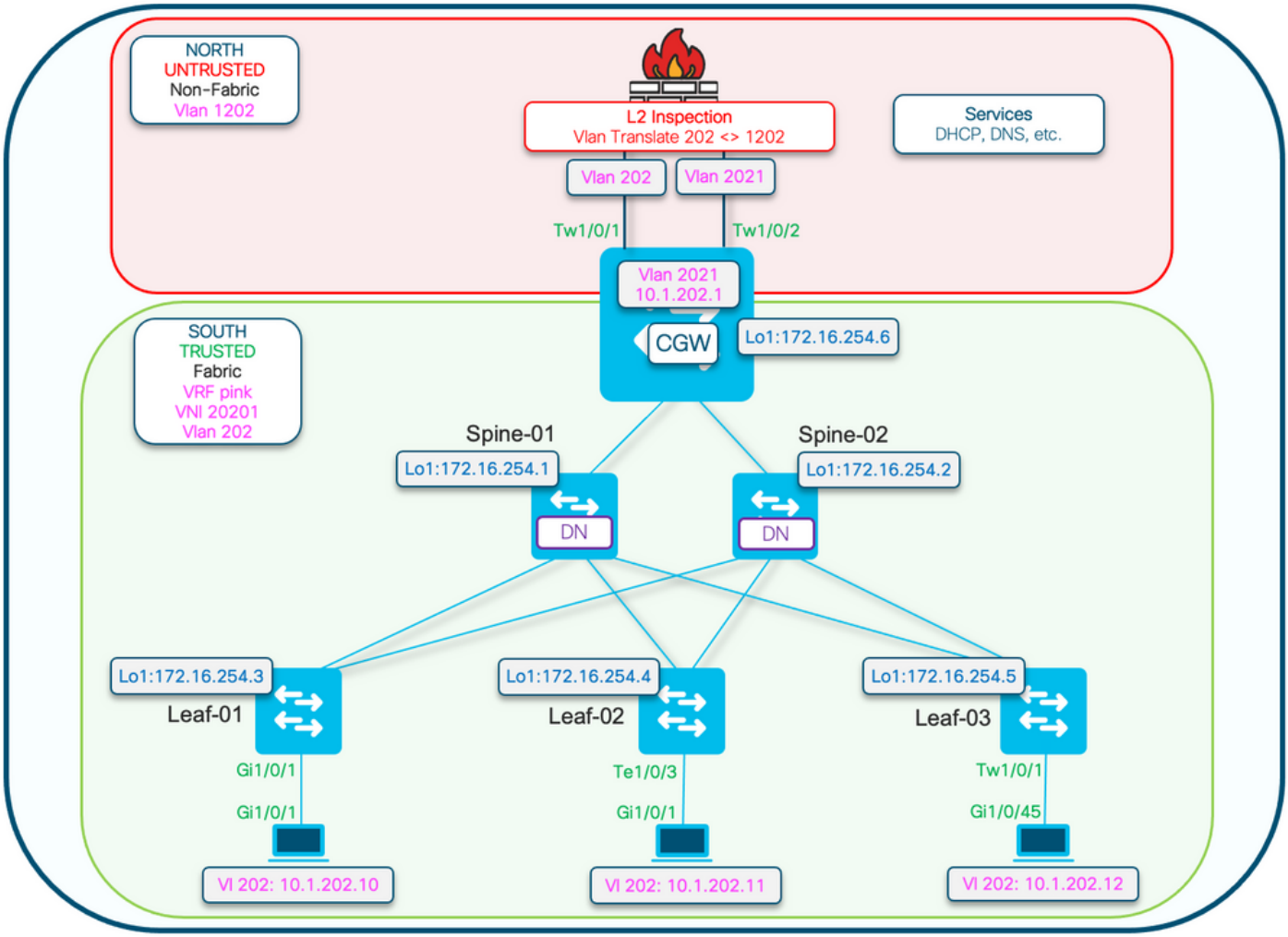
```
Leaf01#

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

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


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

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

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

 lisp iid:     20101            <-- Segment 20101

 lisp flags:     0

 dst Port:     4789             <-- VxLAN

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

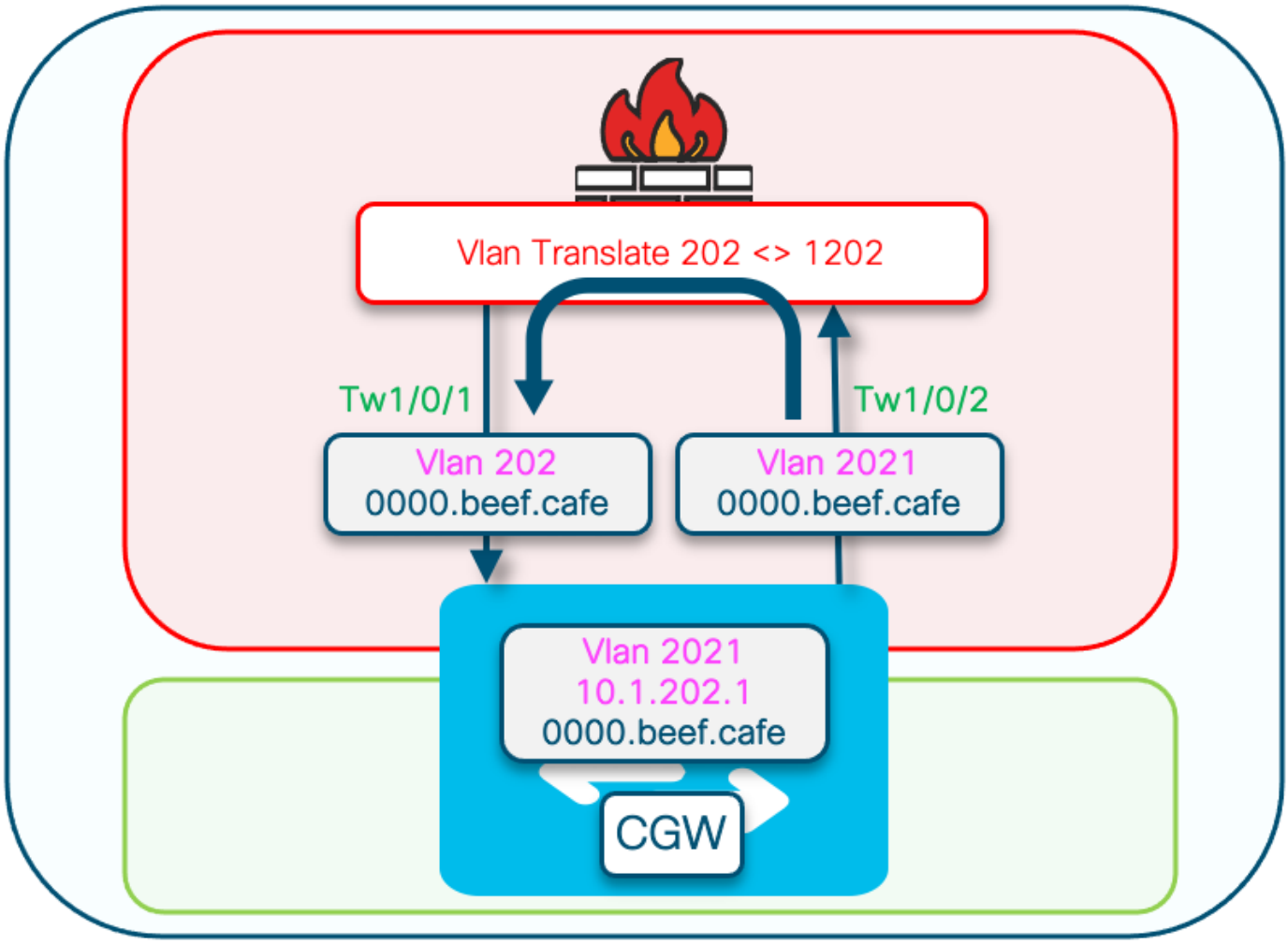


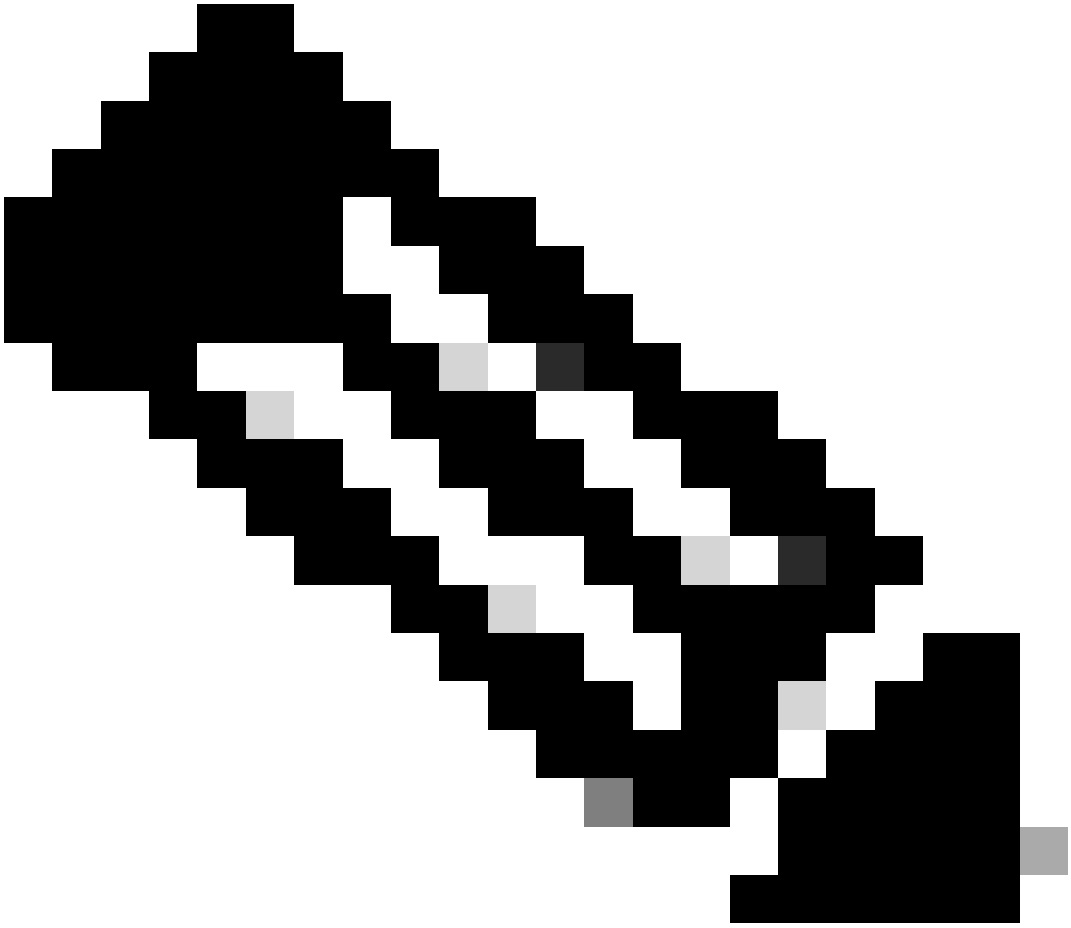
Nota: è anche possibile usare 'show platform software fed switch active matm macTable vlan 201 detail' che concatena questo comando con il comando FED in un unico risultato

Configura (parzialmente isolato)

Esempio di rete


NORTH
UNTRUSTED
Non-Fabric
Vlan 1202
L2 Inspection
Vlan Translate 202 <> 1202
Services
DHCP, DNS, etc.
Vlan 202
Vlan 2021
Tw1/0/1
Tw1/0/2
Vlan 2021
10.1.202.1
CGW
Lo1:172.16.254.6
SOUTH
TRUSTED
Fabric
VRF pink
VNI 20201
Vlan 202
Spine-01
Lo1:172.16.254.1
DN
Spine-02
Lo1:172.16.254.2
DN
Lo1:172.16.254.3
Leaf-01
Lo1:172.16.254.4
Leaf-02
Lo1:172.16.254.5
Leaf-03
Gi1/0/1
Gi1/0/1
Te1/0/3
Gi1/0/1
Tw1/0/1
Gi1/0/45
Vl 202: 10.1.202.10
Vl 202: 10.1.202.11
Vl 202: 10.1.202.12


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



Nota: in questa sezione vengono descritte solo le differenze rispetto ai segmenti completamente isolati.

- Routing-policy per contrassegnare l'IP MAC del gateway GCW con l'attributo DEF GW
- Criterio di rilevamento dispositivi personalizzato necessario per impedire flap MAC
- Binding di tracciamento del dispositivo statico per IP MAC GW

Leaf-01 (configurazione EVPN di base)

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static
```

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

 router-id Loopback1
l2vpn evpn

instance 202

 vlan-based
 encapsulation vxlan


replication-type ingress

 multicast advertise enable
```

<#root>

```
Leaf01#

show run | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

protected <-- protected keyword added
```

CGW (configurazione base)

Impostare la modalità di replica nella finestra di dialogo

<#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
```

Configurare la SVI del gateway esterno

<#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
```

Creare un criterio con la spaziatura disabilitata

```
<#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
```

Collegamento a externalgatewayevi/vlan

```
<#root>

CGW#

show running-config | sec vlan config

vlan configuration 202
 member evpn-instance 202 vni 20201

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

Aggiungi voci statiche nella tabella di rilevamento dispositivi per externalgateway mac-ip

<#root>

```
device-tracking binding vlan 202 10.1.202.1 interface TwentyFiveGigE1/0/1 0000.beef.cafe
```

<-- All static entries in device tracking table should be for external gateway mac-ip’s.
If there is any other static entry in device tracking table, match ip/ipv6 configurations in route map

Creare la mappa della route BGP in modo che corrisponda ai prefissi RT2 MAC-IP e impostare la community estesa del gateway predefinita

<#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
```

Applica route-map ai router adiacenti del reflector di route BGP

<#root>

```
CGW#
```

sh run | s r bgp

```
address-family l2vpn evpn
 neighbor 172.16.255.1 activate
 neighbor 172.16.255.1 send-community both
 neighbor 172.16.255.1
```

route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR

```
 neighbor 172.16.255.2 activate
 neighbor 172.16.255.2 send-community both
 neighbor 172.16.255.2
```

route-map CGW_DEF_GW out <-- Sets the DEF GW Community when it advertises MAC-IP type RT2 to the RR

Verifica (parzialmente isolata)

Dettagli EVI

<#root>

```
Leaf01#

show l2vpn evpn evi 202 detail

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

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

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

Generazione RT2 locale (da host locale a RT2)

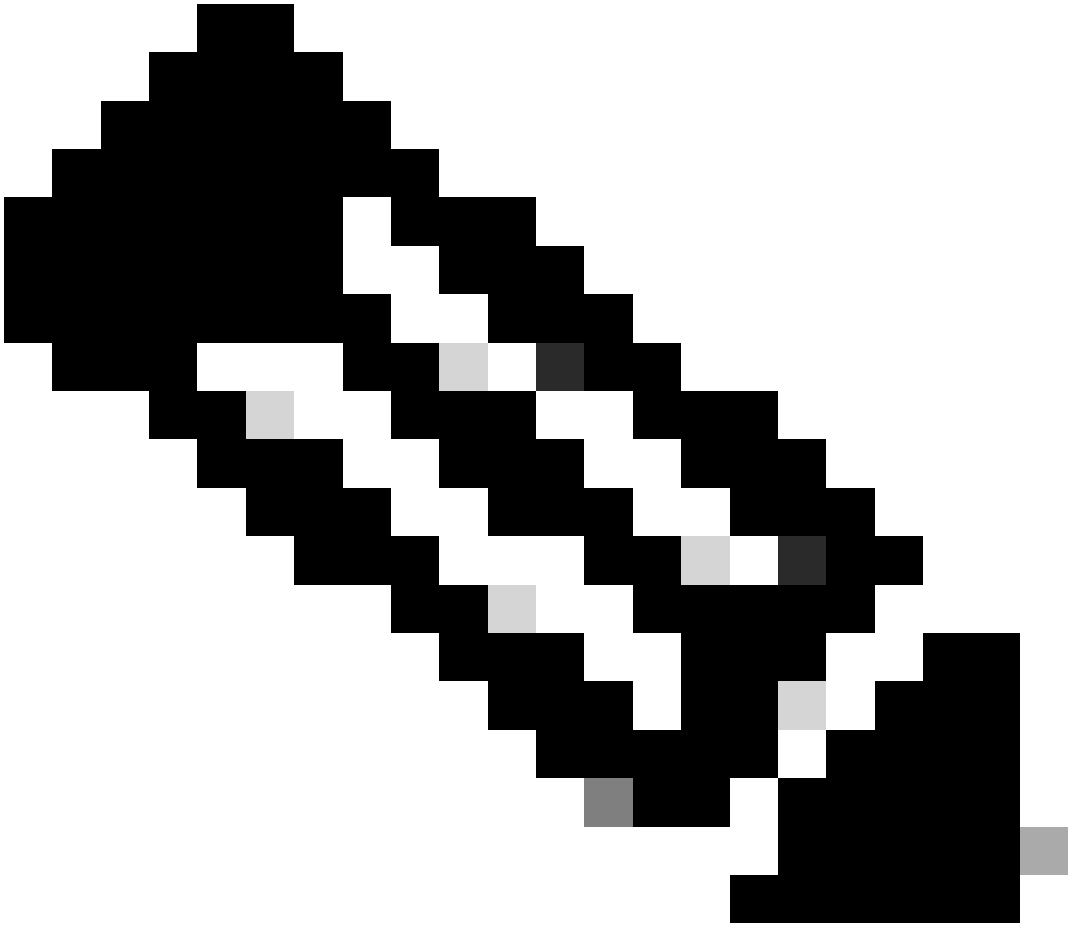
Coperto in un precedente esempio di totale isolamento

Apprendimento remoto RT2 (gateway predefinito RT2)

Copertura delle differenze rispetto a Totalmente Isolato

Prefisso gateway predefinito CGW (foglia)

Verificare che il prefisso disponga dell'attributo appropriato per poter essere installato nell'hardware



Nota: si tratta di un fattore critico per il funzionamento del relay L2 DHCP

<#root>

```
Leaf01#

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

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

table evi_202

)

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


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

```
      EVPN ESI: 00000000000000000000,

Label1 20201              <-- Correct Segment ID

      Extended Community: RT:65001:202 ENCAP:8

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

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

MATM FED (Foglia)

<#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>

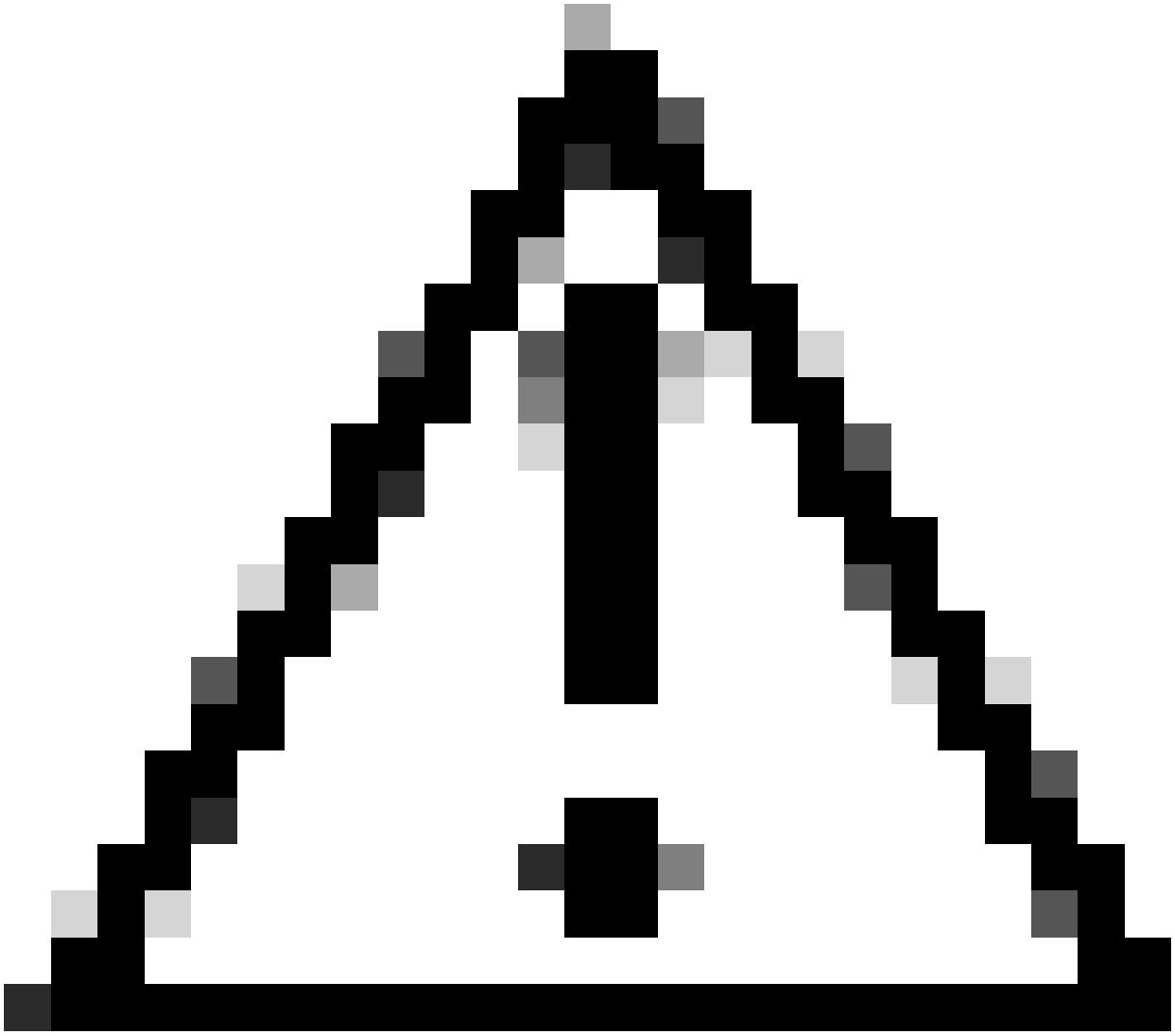
```
CGW#

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
```

Risoluzione dei problemi

Risoluzione indirizzi (ARP)

Fasi generali per l'isolamento dei problemi ARP

- Conferma che il tunnel IMET è pronto
- Cattura su uplink CGW per verificare che ARP sia stato ricevuto e incapsulato da Leaf
- Se non si rileva ARP in arrivo su uplink
  - Verificare che il tunnel IMET sia pronto sia su Leaf che su CGW
  - Cattura su uplink foglia per confermare che ARP è incapsulato e inviato
  - Risolvere i problemi relativi al percorso intermedio
- Se ARP arriva sull'acquisizione del tunnel IMET del bordo ma non è programmato nella tabella ARP VRF
  - Risolvere i problemi relativi al percorso del punt CPU/CoPP per confermare che il punt ARP sia stato eseguito sulla CPU
  - Confermare che le informazioni sull'indirizzo IP/client siano corrette
  - Eseguire il debug di ARP in VRF per verificare l'impatto sul processo ARP
- Verificare che l'indirizzo MAC CGW sia installato come mac hop successivo/destinazione sugli host
- Conferma che CGW ha entrambe le voci ARP con i MAC host reali
- Verificare che i criteri firewall consentano questo tipo di traffico



Attenzione: prestare attenzione quando si attivano i debug.

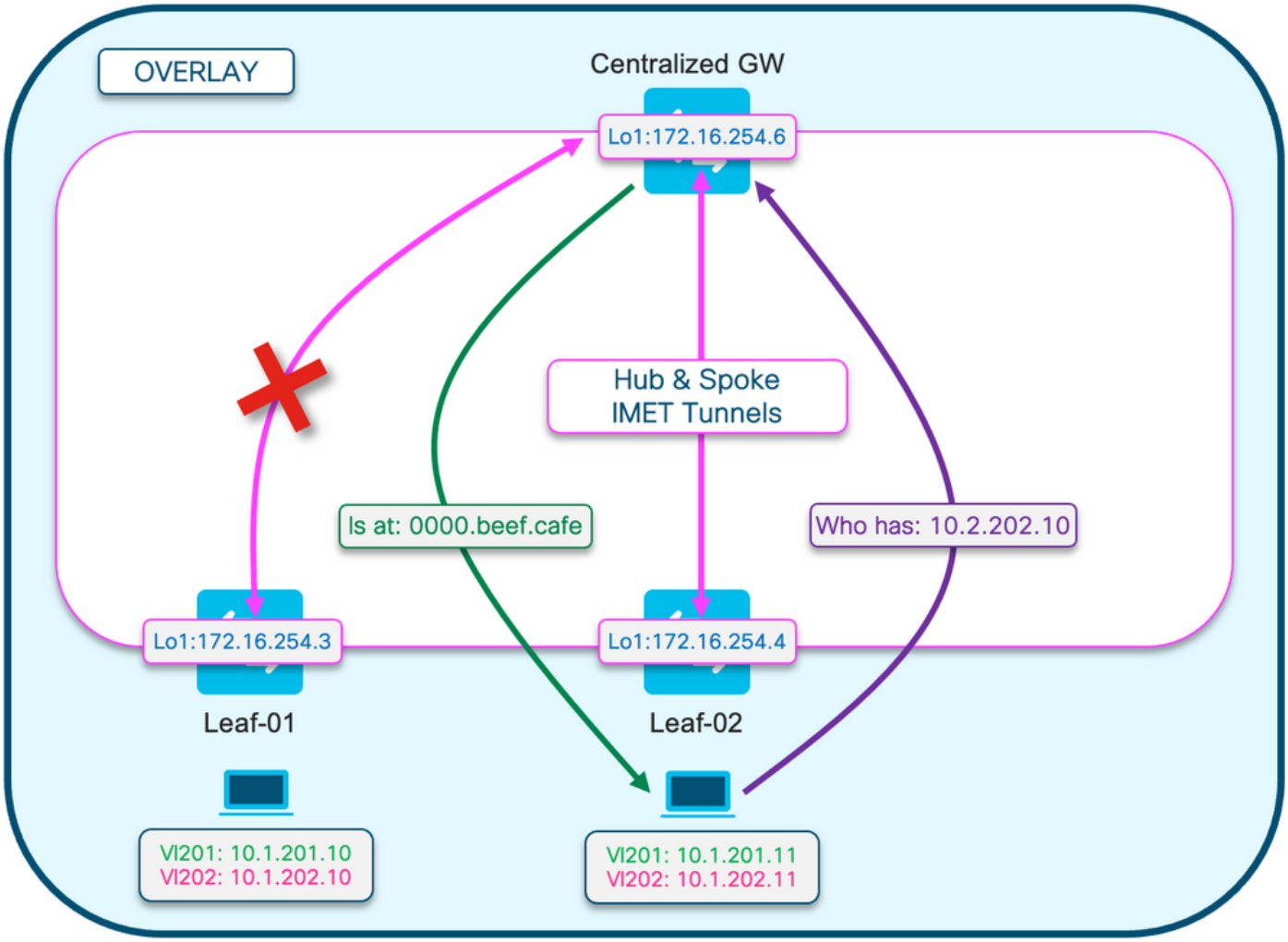
Assicurarsi di aver disattivato la soppressione di flooding

<#root>

```
Leaf-01#

show run | sec l2vpn
l2vpn evpn

 replication-type static

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

Quando l'host di Leaf-02 risolve l'ARP per l'host di Leaf-01, la richiesta ARP non viene trasmessa direttamente a Leaf-01

- L'ARP viene invece trasmesso all'unico tunnel BUM programmato su Leaf-02 verso il CGW
- Il CGW non lo inoltra a Leaf-01, ma risponde con il proprio MAC
- In questo modo, tutte le comunicazioni vengono trasmesse al CGW e quindi instradate a tra gli host
- CGW instrada i pacchetti, anche quando si trovano sulla stessa subnet locale



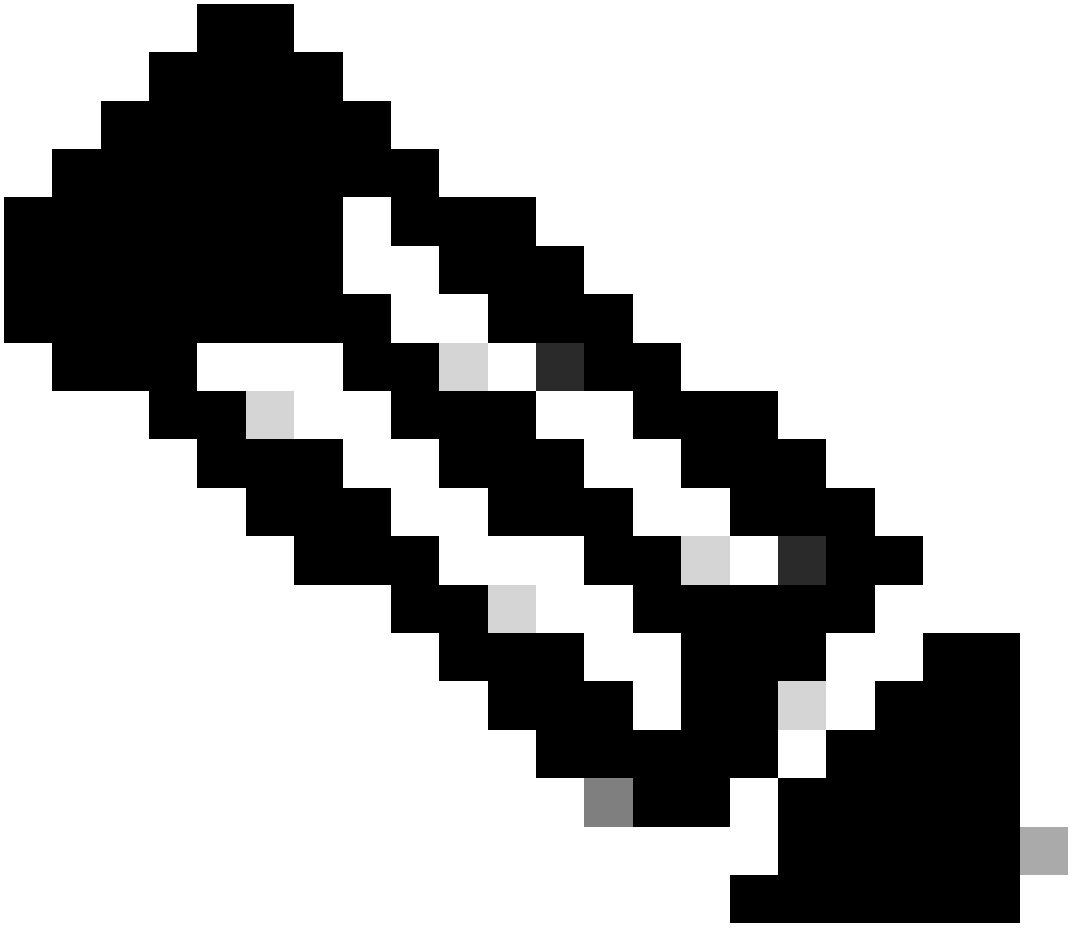
Questo diagramma consente di visualizzare il flusso del processo di risoluzione ARP descritto in questa sezione.

La richiesta ARP è visualizzata in viola

- Questa richiesta ARP deve risolvere l'indirizzo MAC dell'host 10.1.202.10 off Leaf-01
- La linea viola termina in corrispondenza del CGW e non raggiunge Leaf-01

La risposta ARP viene visualizzata in verde

- La risposta contiene l'indirizzo MAC della CGW SVI per Vlan 202
- Si noti che la linea verde proviene dal CGW e non dall'host effettivo



Nota: la X rossa indica che la comunicazione non ha comportato l'invio del traffico a Leaf-01.

Osservare le voci ARP su ciascun 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

Osservate che su CGW vengono appresi i prefissi RT2. Questa operazione è richiesta da CGW per inoltrare i pacchetti

<#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
```

Acquisire lo scambio ARP sugli uplink per confermare la comunicazione bidirezionale

- È possibile utilizzare Embedded Packet Capture (EPC) sugli uplink del fabric
- In questo scenario viene visualizzato EPC nell'uplink Leaf01. Se necessario, ripetere la stessa procedura su CGW

Configurazione di 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
```

Avvia l'acquisizione

```
<#root>

Leaf01#

monitor capture 1 start
```

Inizializzare il ping per attivare la richiesta ARP (in questo caso il ping va da host Leaf01 10.1.201.10 a host Leaf02 10.1.201.11)

```
<#root>

Leaf01-HOST#

ping vrf red 10.1.201.11
```

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

Interrompi cattura e verifica fotogrammi ARP

<#root>

```
Leaf01#
```

mon cap 1 stop

```
F241.03.23-9300-Leaf01#
```

show mon cap 1 buff br | i ARP

11

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

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

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

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

Visualizzare i pacchetti di acquisizione in dettaglio. Per visualizzare ulteriori informazioni sui pacchetti, usare l'opzione detail di EPC

- Tenere presente che questo output viene ritagliato in varie posizioni per brevità

<#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 Prefix

Prefisso gateway mancante

Come accennato nella sezione precedente sui segmenti parzialmente isolati, è necessario apprendere l'indirizzo MAC nella VLAN della struttura

- Questo problema può verificarsi se non è presente traffico destinato al gateway per un periodo di tempo superiore a quello del timer di aging MAC.
- Se manca il prefisso del gateway CGW, è necessario confermare che l'indirizzo MAC sia presente

```
CGW#

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

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


CGW#

show mac address-table address 0000.beef.cafe

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

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

<-- MAC is not learned in Fabric Vlan 202

Total Mac Addresses for this criterion: 2
```

Correzione mancante del prefisso del gateway

Nella maggior parte delle reti di produzione è probabile che ci sia sempre del traffico. Tuttavia, se il problema si verifica, è possibile utilizzare una delle seguenti opzioni per risolverlo:

- Aggiungere una voce MAC statica, ad esempio 'mac address-table static 0000.beef.cafe vlan 202 interface TwentyFiveGigE1/0/1'
- Aumentare il timer di aging MAC con 'mac address-table aging-time <seconds>'. Tenere presente che in questo modo si aumenta il tempo di permanenza per tutti gli indirizzi MAC, pertanto si preferisce l'opzione MAC statico.

Attributo DEF GW mancante

Con i segmenti parzialmente isolati esistono diverse configurazioni aggiuntive per aggiungere questo attributo.

Correzione attributo DEF GW mancante

Confermare i seguenti dettagli:

- È in esecuzione la versione 17.12.1 o successive
- La CLI SISF (Device-Tracking) è presente nella configurazione
- I comandi route-map match & set vengono configurati e route-map viene applicata ai router BGP adiacenti
- Gli annunci BGP sono stati aggiornati (è necessario cancellare BGP per pubblicizzare nuovamente il prefisso con il nuovo attributo)

Roaming wireless

Il roaming frequente può causare aggiornamenti troppo frequenti di BGP e il roaming per intervallo di tempo deve essere aumentato prima che lo switch dichiari di essere il proprietario dell'MAC e

invii l'aggiornamento RT2

- Questo si verifica quando un host si sposta tra due access point che si trovano su switch diversi.
- Il limite predefinito per il roaming è 5 per 180 secondi

<#root>

```
Leaf01#

sh run | sec l2vpn

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

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


Leaf01#

sh l2vpn evpn summary

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

  MAC Duplication: seconds 180 limit 10

  MAC Addresses: 13
    Local:     6
    Remote:    7

    Duplicate: 0
  IP Duplication: seconds 180 limit 10

  IP Addresses: 7
    Local:     4
    Remote:    3

    Duplicate: 0

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

Comandi da raccogliere per TAC

Se il problema non è stato risolto, raccogliere l'elenco dei comandi visualizzato e allegarlo alla richiesta di assistenza TAC.

Informazioni minime da raccogliere

(tempo limitato per la raccolta dei dati prima di un'operazione di ricaricamento/ripristino)

- Mostra tecnico evpn
- Mostra tecnologia
- Mostra se tecnico

Informazioni dettagliate da raccogliere

Se si dispone del tempo necessario per raccogliere dati più completi, è preferibile procedere in questo modo

- show tech
- show tech evpn
- show tech platform evpn_vxlan switch <numero>
- show tech platform
- mostra risorsa tecnica
- show tech sisf
- mostra isis tech
- show tech bgp
- show monitor event-trace evpn event all
- show monitor event-trace evpn error all
- richiedi archivio di traccia software piattaforma

Informazioni correlate

- Implementazione della policy di routing BGP VPN sugli switch Catalyst serie 9000
- Relay layer 2 DHCP (presto disponibile)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).