

Implementatie van BGP EVPN beschermde overlay segmentatie op Catalyst 9000 Series Switches

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beschrijving functie op hoog niveau](#)

[Documentgegevens](#)

[Beschermde segmenttypen](#)

[Volledig geïsoleerd](#)

[Meestal geïsoleerd](#)

[Switch](#)

[Routetype 2 Behandeling](#)

[Ontwerpoverzicht](#)

[Terminologie](#)

[Flow-diagrammen](#)

[Routetype 2 \(RT2\)](#)

[Routetype 3 \(RT3\)](#)

[Diagram van Adresresolutie \(ARP\)](#)

[Configureren \(volledig geïsoleerd\)](#)

[Netwerkdigram](#)

[Leaf-01 \(basis-EVPN-configuratie\)](#)

[CGW \(basisconfiguratie\)](#)

[Verifiëren \(volledig geïsoleerd\)](#)

[EVI-gegevens](#)

[Lokale RT2-generatie \(lokale host voor RT2\)](#)

[Remote RT2 Learning \(standaardgateway RT2\)](#)

[Configureren \(gedeeltelijk geïsoleerd\)](#)

[Netwerkdigram](#)

[Leaf-01 \(basis-EVPN-configuratie\)](#)

[CGW \(basisconfiguratie\)](#)

[Verifiëren \(gedeeltelijk geïsoleerd\)](#)

[EVI-gegevens](#)

[Lokale RT2-generatie \(lokale host voor RT2\)](#)

[Remote RT2 Learning \(standaardgateway RT2\)](#)

[CGW standaardgatewayprefix \(blad\)](#)

[FED MATM \(blad\)](#)

[SISF \(CGW\)](#)

[IOS MATM \(CGW\)](#)

[Problemen oplossen](#)

[Adresoplossing \(ARP\)](#)

[CGW RT2-gatewayprefix](#)

[Draadloos roaming](#)

[Te verzamelen opdrachten voor TAC](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u BGP EVN VPN Protected Overlay Segmentatie op Catalyst 9000 Series Switches kunt implementeren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- BGP EVPN VLAN-concepten
- [BGP EVN Unicast-probleemoplossing](#)
- [BGP EVN VXLAN-routeringsbeleid](#)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.12.1 en latere versies

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Beschrijving functie op hoog niveau

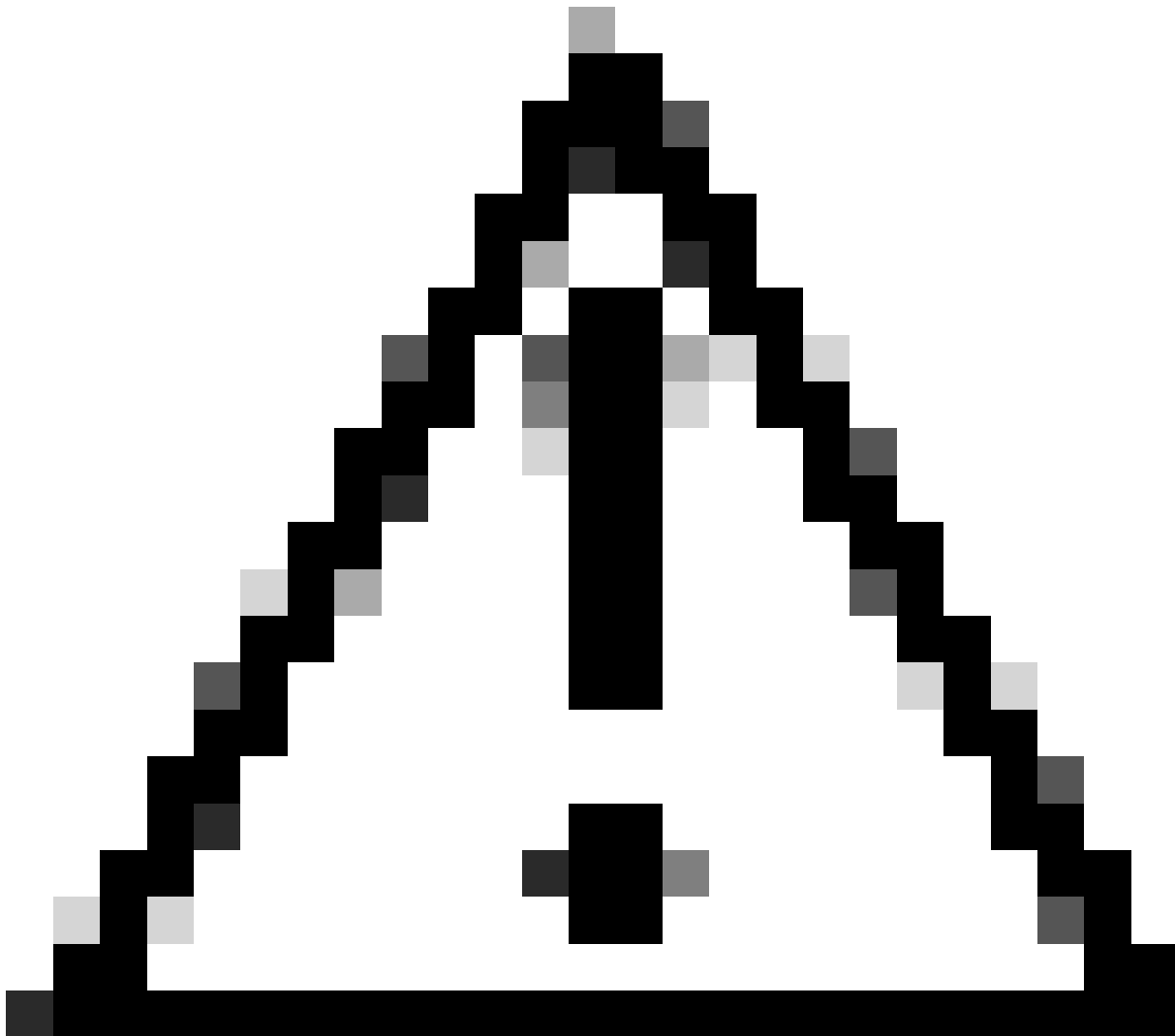
De beveiligde segmentfunctie is een beveiligingsmaatregel die voorkomt dat poorten verkeer naar elkaar doorsturen, zelfs als ze op hetzelfde VLAN en dezelfde switch staan

- Deze functie is vergelijkbaar met 'switchport protected' of private VLAN's, maar voor EVPN-stoffen.
- Dit ontwerp dwingt al verkeer naar de CGW waar het kan worden geïnspecteerd door een Firewall alvorens naar zijn eindbestemming te worden verzonden.
- Verkeersstromen worden gecontroleerd, deterministisch en gemakkelijk te inspecteren met een gecentraliseerd security apparaat.

Documentgegevens

Dit document maakt deel 2 of 3 uit van onderling verband houdende documenten:

- Document 1: [Voer het BGP EVP-routingbeleid op Catalyst 9000 Series Switches uit](#) om te bepalen hoe het BGP BUM-verkeer in de Overlay wordt bestuurd en moet eerst worden geconfigureerd
- Document 2: Dit document. Voortbouwend op het Overlay-ontwerp en het beleid van document 1, beschrijft dit document de implementatie van het 'beschermd' sleutelwoord
- Document 3: [Implementeer BGP EVPN DHCP Layer 2 Relay op Catalyst 9000 Series Switches](#) en bespreekt hoe DHCP Relay werkt op een L2 alleen VPN



Waarschuwing: u moet de configuratie in document 1 implementeren voordat u beveiligde segmentconfiguraties implementeert.

Beschermde segmenttypen

Volledig geïsoleerd

- uitsluitend noord-zuidcommunicatie mogelijk maakt, en
- De gateway wordt geadverteerd in de stof met de 'standaard-gateway adverteren' CLI

Meestal geïsoleerd

- Maakt communicatie tussen het noorden en het zuiden mogelijk (in dit geval zijn verkeer tussen het oosten en het westen toegestaan op basis van beleid voor firewallverkeer)
- Maakt Oost-naar-West communicatie mogelijk (gebaseerd op beleid voor firewallverkeer)
- De gateway is extern aan de stof en de SVI wordt niet geadverteerd met behulp van de

'standaard-gateway adverteren' CLI

Switch

- Hosts kunnen niet rechtstreeks met elkaar communiceren, zelfs als ze verbonden zijn met dezelfde switch (ARP-verzoek niet naar andere poorten op dezelfde switch verzonden als hosts zich in hetzelfde VRF/VLAN/segment bevinden)
- Geen BUM-verkeer tussen L2 VTEP's (IMET-prefixes gefilterd met behulp van de [routerbeleidsconfiguratie](#))
- Alle pakketten van de hosts worden doorgestuurd naar Border Leaf om doorgestuurd te worden. (Dit betekent voor host 1 om te communiceren met host 2 op hetzelfde blad, verkeer is vastgepind tot aan de CGW)

Routetype 2 Behandeling

- Access Leafs adverteren met lokale RT2 met E-Tree Extended Community en Leaf-vlagset.
- Access Leafs installeert geen enkel afgelegen RT2 dat is ontvangen met de E-Tree Extended Community en Leaf-vlag die is ingesteld in dataplane.
- Access Leafs installeren elkaar niet RT2 in dataplane.
- Access Leafs and Border Leaf (CGW) installeert elkaar RT2 in dataplaat.
- Geen configuratiewijziging vereist op toegangsblad of grensblad.

Ontwerpoverzicht

- Voor uitzending (BUM) is de RT3-topologie hub en spaak om uitzendverkeer zoals ARP naar de GCW te dwingen.
- Om rekening te houden met de gastmobiliteit is RT2 volledig mesh op het BGP-besturingsplane (wanneer een host van de ene VTEP naar de andere beweegt, wordt het volgnummer in de RT2 verhoogd)
- De gegevensvlak installeert selectief de adressen van MAC.
 - Een blad installeert alleen lokale MAC's & RT2 die de DEF GW attributen bevatten
 - De CGW heeft niet de beschermde KW en installeert alle lokale MAC & Remote RT2 in zijn dataplatform.

Terminologie

VRF	Doorsturen van virtuele routing	Bepaalt een Layer 3-routeringsdomein dat moet worden gescheiden van andere VRF- en wereldwijde IPv4/IPv6-routeringsdomein
AF	Adresfamilie	Bepaalt welk type prefixes en routing info BGP handvatten
AS	Autonoom systeem	Een reeks routeerbare IP-prefixes voor internet die behoren tot een netwerk of een verzameling netwerken die allemaal worden beheerd, gecontroleerd en gecontroleerd door één entiteit of organisatie

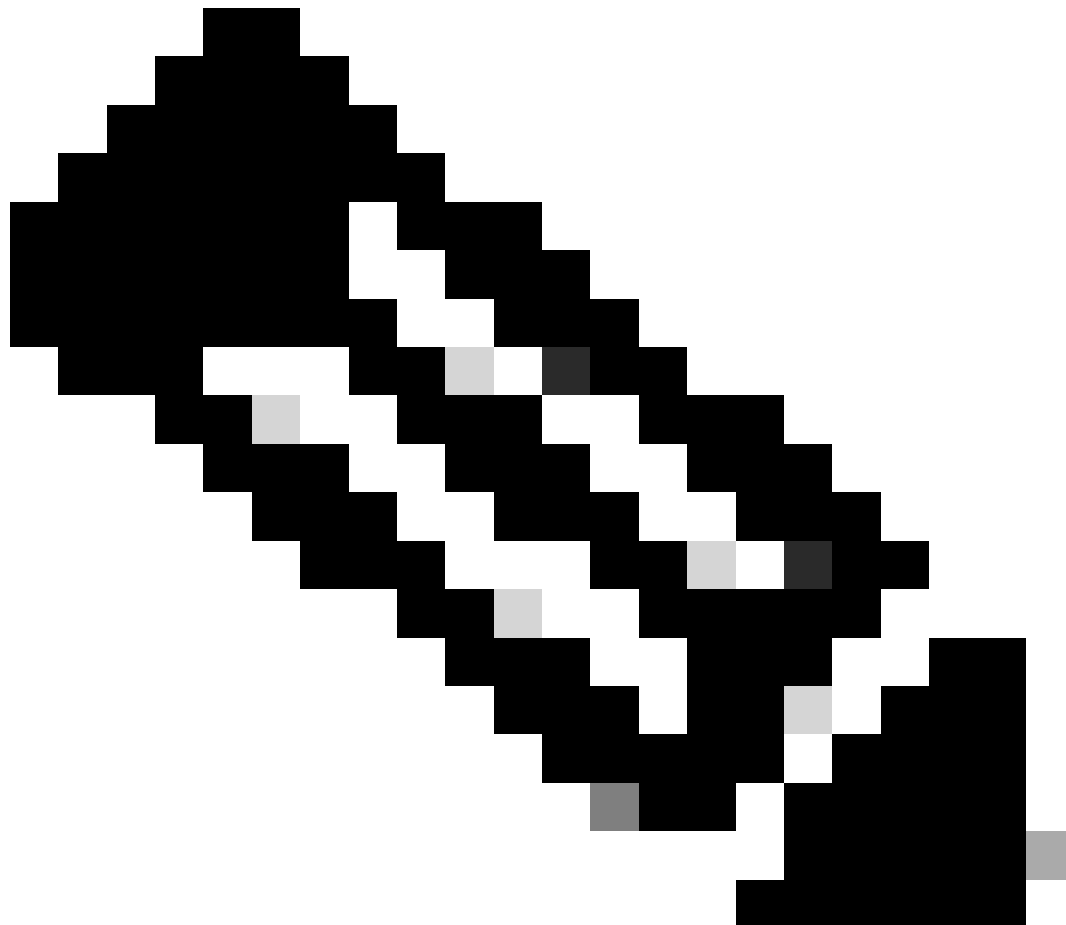
EVPN	Ethernet Virtual Private Network	De uitbreiding die BGP in staat stelt Layer 2 MAC- en Layer 3 IP-informatie te transporteren, is EVPN en gebruikt Multi-Protocol Border Gateway Protocol (MP-BGP) als het protocol om bereikbaarheidsinformatie te distribueren die betrekking heeft op het VXLAN-overlay-netwerk.
VXLAN	Virtual Extensible LAN (Local Area Network)	VXLAN is ontworpen om de inherente beperkingen van VLAN's en STP te overwinnen. Het is een voorgestelde IETF-standaard [RFC 7348] om dezelfde Ethernet Layer 2-netwerkservices te bieden als VLAN's, maar met grotere flexibiliteit. Functioneel is het een MAC-in-UDP inkapselingsprotocol dat als virtuele overlay op een Layer 3 underlay-netwerk wordt uitgevoerd.
CGW	Gecentraliseerde gateway	En implementatie van EVPN waar de toegangspoort SVI niet op elk blad staat. In plaats daarvan wordt alle routing uitgevoerd door een specifiek blad met behulp van asymmetrische IRB (geïntegreerde routing en bridging)
DEF GW	Standaardgateway	Een BGP uitgebreid community attribuut toegevoegd aan de MAC/IP prefix via het commando "standaard-gateway adverteren inschakelen" onder de 'l2vpn evpn' configuratie sectie.
IMET (RT3)	Inclusief multicast Ethernet-tag (router)	Wordt ook BGP type-3 route genoemd. Dit routetype wordt in EVPN gebruikt om BUM-verkeer (broadcast / onbekende unicast / multicast) tussen VTEP's te leveren.
RT2	Routetype 2	BGP MAC- of MAC/IP-prefix die een MAC-host of MAC-IP-gateway vertegenwoordigt
EVPN Mgr	EVPN Manager	Central management component voor verschillende andere componenten (bijvoorbeeld: leert van SISF en signalen naar L2RIB)
SISF	Switch-geïntegreerde beveiligingsfunctie	Een agnostische host tracking tabel die wordt gebruikt door EVPN om te leren wat lokale hosts aanwezig zijn op een blad
L2RIB	Layer 2 Routing-informatiebasis	In tussencomponent voor het beheer van interacties tussen BGP, EVPN Mgr, L2FIB
FED	Forwarding	Programma's op de ASIC (hardware) laag

	Engine Driver	
MATM	Mac-adrestabelbeheer	IOS MATM: software tabel die alleen lokale adressen en FED MATM: hardwaretabel die lokale en externe adressen installeert die geleerd zijn vanuit het besturingsplane, en die deel uitmaakt van het hardware-doorsturen vlak

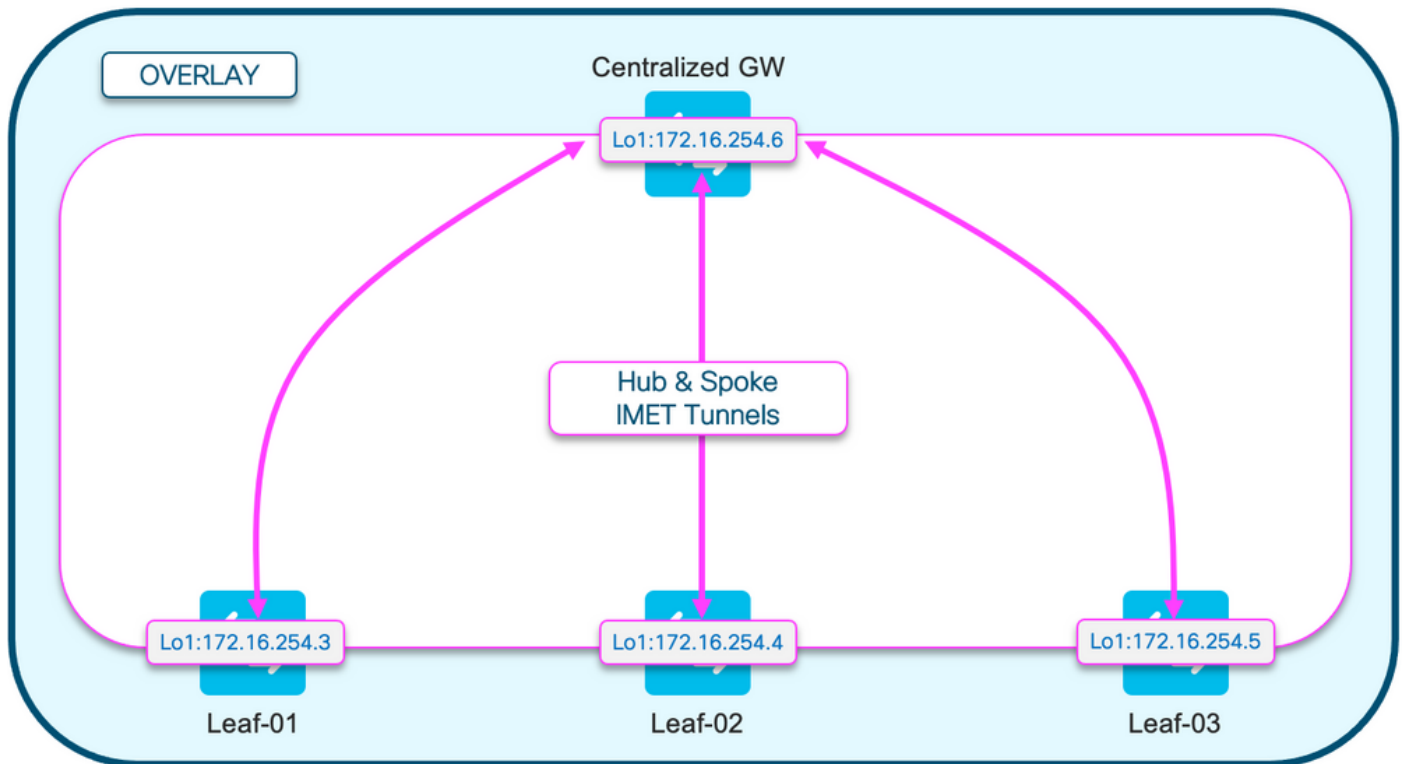
Flow-diagrammen

Routetype 2 (RT2)

Dit diagram toont het volledige netwerkontwerp van de type 2 MAC/MAC-IP-hostprefixes.

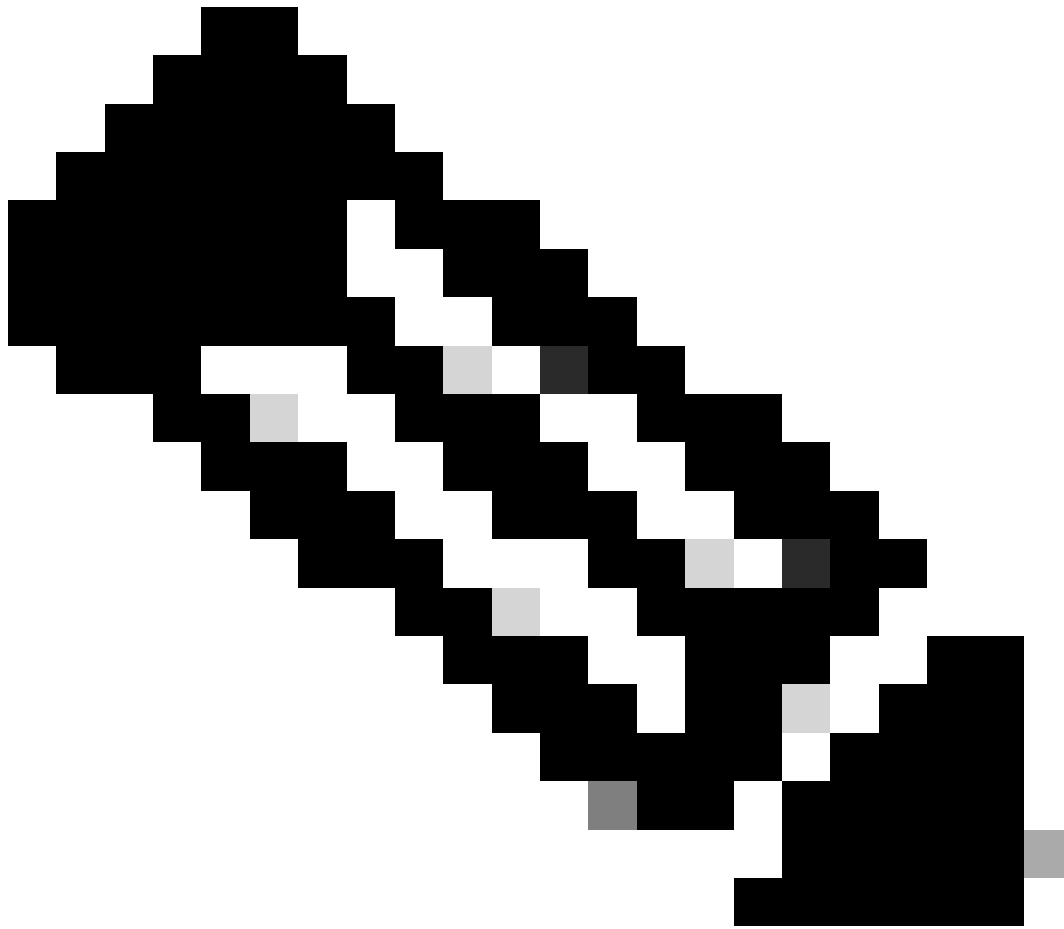


Opmerking: volledige mesh is vereist om mobiliteit en roaming te ondersteunen



Routetype 3 (RT3)

Dit diagram toont het hub and spoke-ontwerp van de uitzending IMET (RT3) tunnels



Opmerking: Hub and spoke uitzending is vereist om te voorkomen dat bladeren met hetzelfde segment rechtstreeks uitzending naar elkaar verzenden.

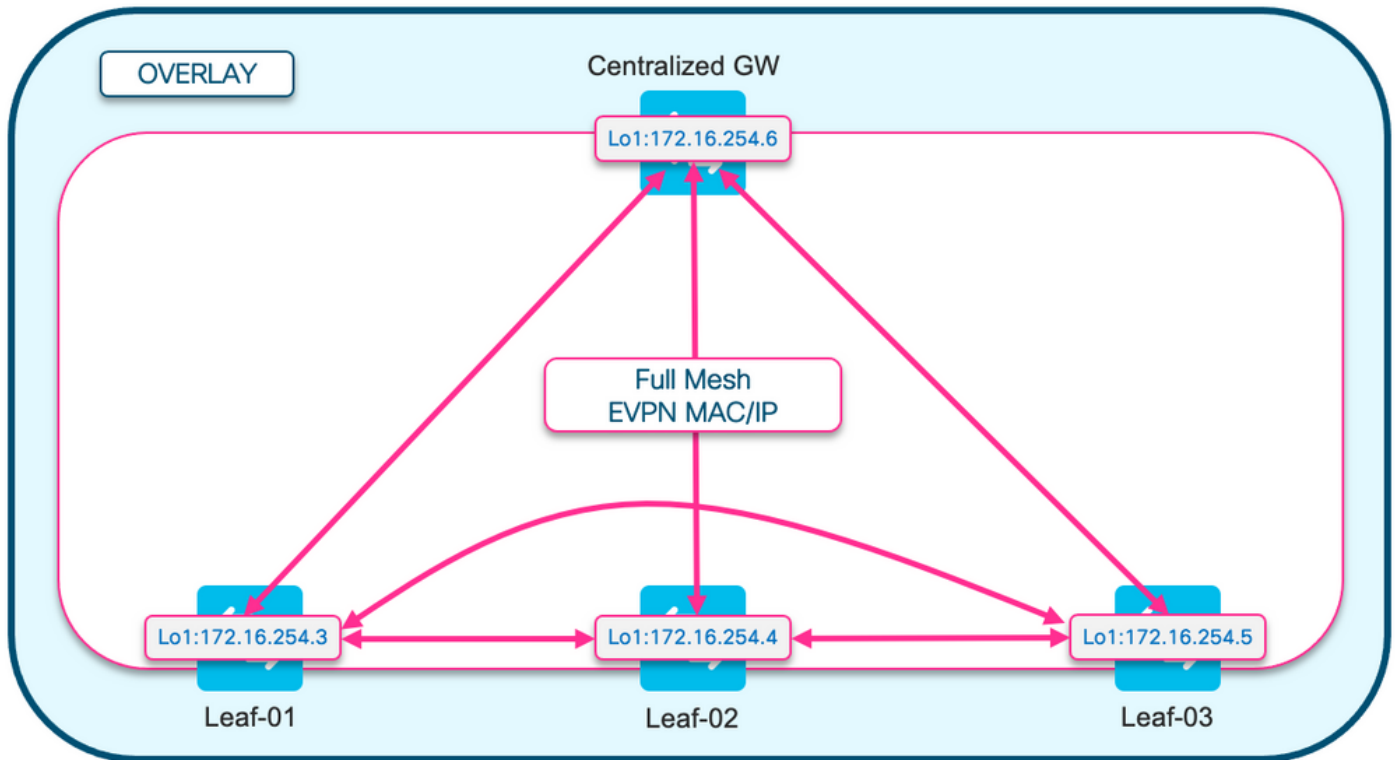
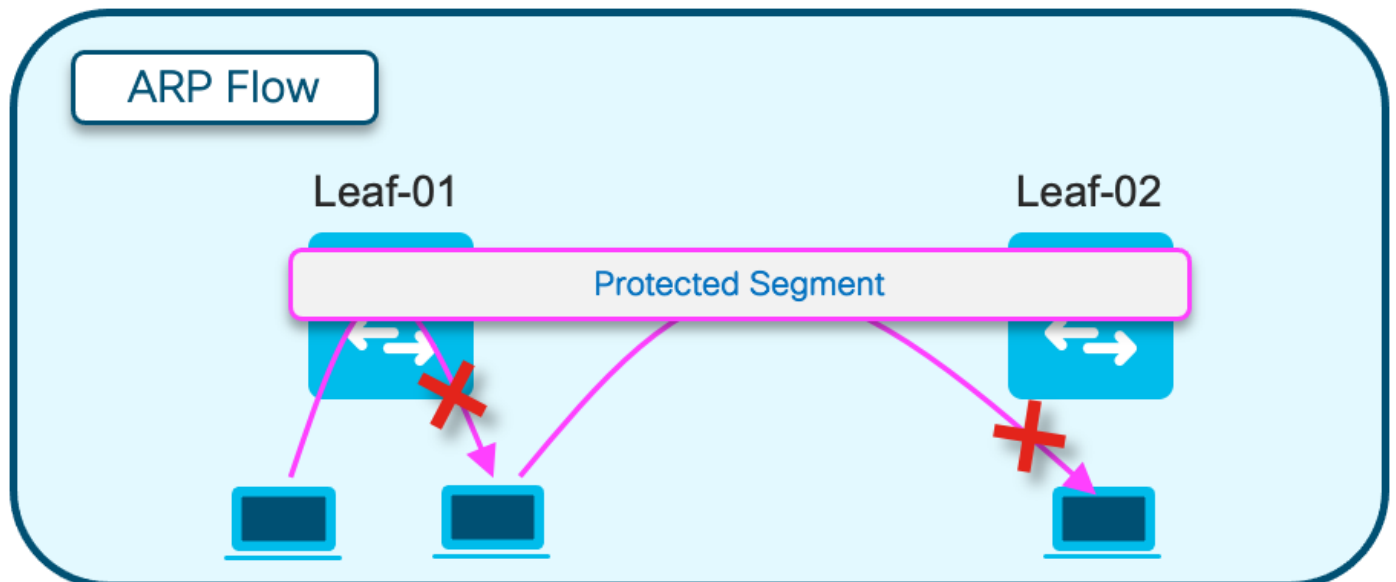


Diagram van Adresresolutie (ARP)

Dit diagram toont aan dat ARP geen gastheer in het zelfde segment EPVN mag bereiken. Wanneer gastheer ARPs voor een andere gastheer, slechts CGW deze ARP krijgt en antwoordt



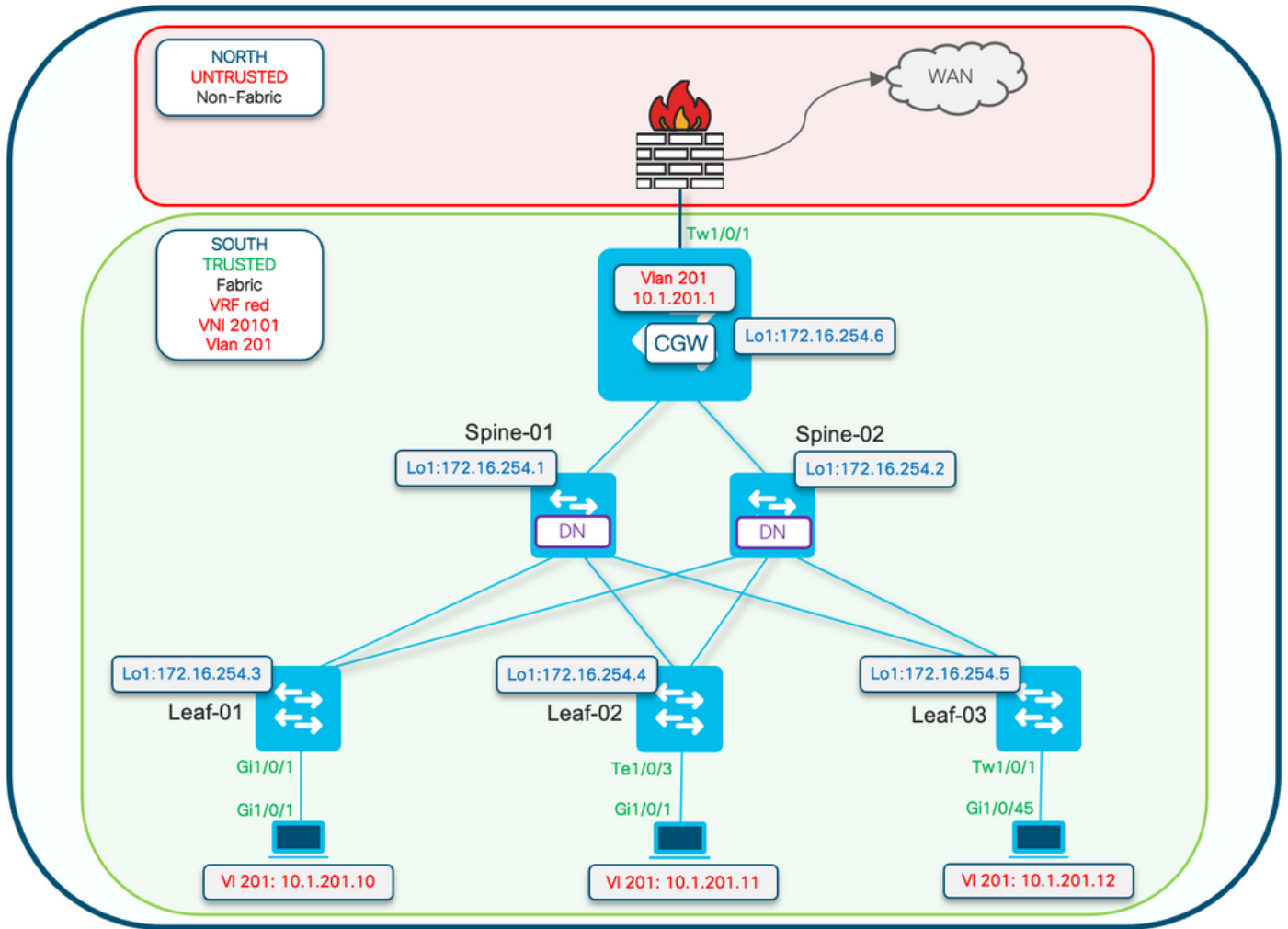


Opmerking: deze wijziging in ARP-gedrag wordt geconcretiseerd door het gebruik van het 'afgeschermd' sleutelwoord.

Voorbeeld: `member evpn-instance 202 vni 20201 protected`

Configureren (volledig geïsoleerd)

Netwerkdigram



Het beschermde configuratiesleutelwoord wordt toegepast op de switches van het Blad. CGW is een promiscuous device en installeert alle mac-adressen.



Opmerking: de configuratie van de routebeleidscommunity list en routekaart die de import/export van IMET-prefixes controleert, wordt weergegeven in [Importeren BGP EVP-routingbeleid op Catalyst 9000 Series Switches](#) . In dit document worden alleen beschermde segmentverschillen weergegeven.

Leaf-01 (basis-EVPN-configuratie)

```
<#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 traffic
  multicast advertise enable
```

<#root>

Leaf01#

```
show run | sec vlan config

vlan configuration 201
  member evpn-instance 201 vni 20101

protected <-- protected keyword added
```

CGW (basisconfiguratie)

<#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
```

Opmerking: bij de CGW wordt geen BGP-beleid toegepast. De CGW mag alle prefixtypes (RT2, RT5 / RT3) ontvangen en verzenden.

Verifiëren (volledig geïsoleerd)

EVI-gegevens

<#root>

Leaf01#

```
sh 12vpn 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)
```

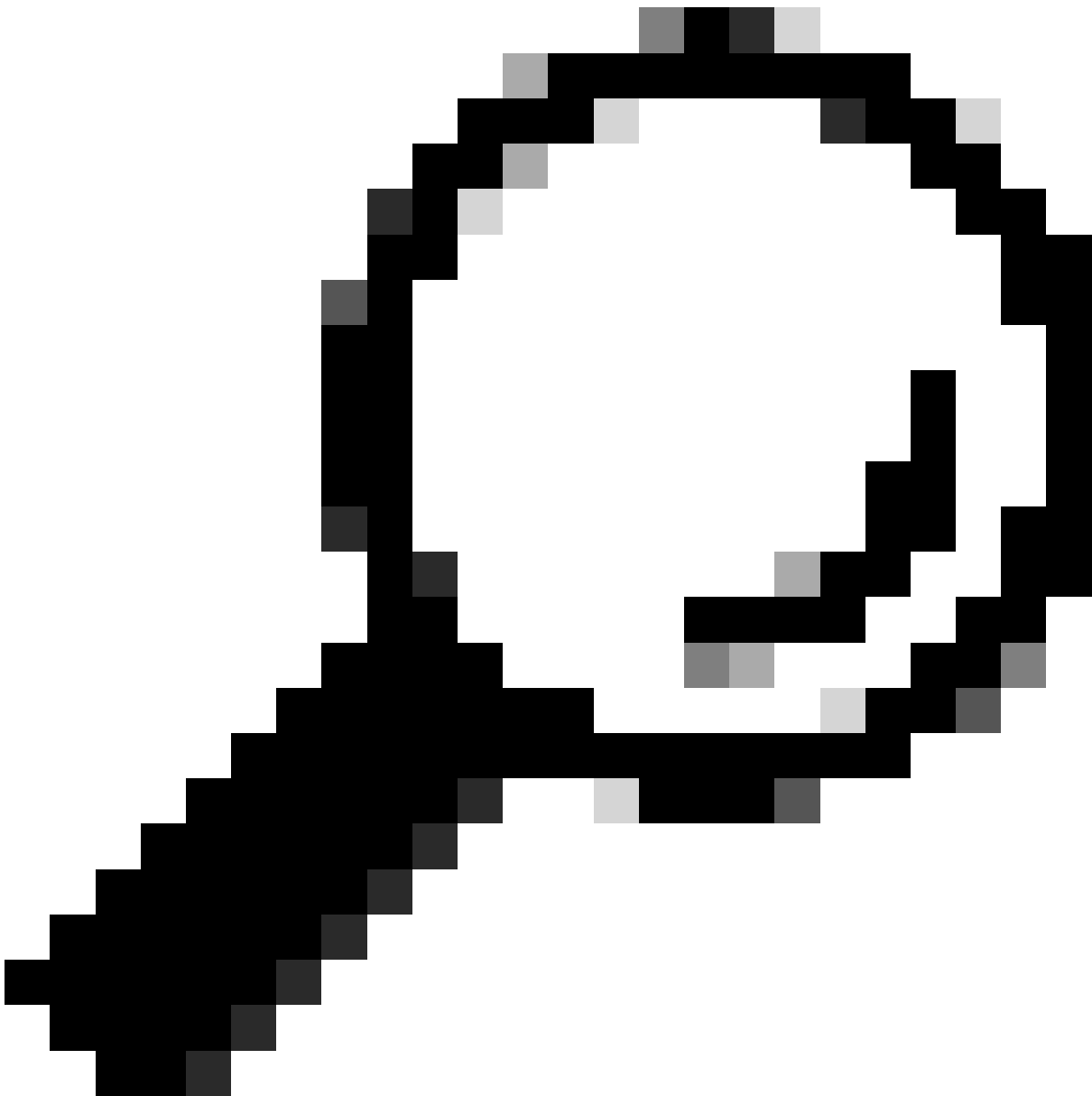
```
Vlan: 201
Protected: True (local access p2p blocked) <-- Vlan 201 is in protected mode
```

<...snip...>

Lokale RT2-generatie (lokale host voor RT2)

Verifieer de component afhankelijkheidsketen van lokale host learning tot RT2 generatie:

- SISF (Terwijl het blad geen SVI heeft, gleent SISF nog steeds de hostinformatie via ARP frame van de host)
- EVPN Mgr
- L2RIB
- BGP



Tip: Als een vorige component niet goed is geprogrammeerd, kan de hele afhankelijkheidsketen worden onderbroken (bijvoorbeeld: SISF heeft geen ingang dan kan BGP geen RT2 maken).

SISF

Controleer of SISF de host heeft geleerd in DB (hostinformatie van DHCP of ARP)

- SISF leert MAC-vermeldingen van IOS-MATM leren en stuurt vervolgens naar EVPN Mgr (moet MAC-BEREIKBAAR zijn met beleid "evpn-sisf-policy").
- SISF zorgt voor een IP/MAC-binding op een lokale VTEP en maakt gebruik van de EVPN-beheerder om informatie te programmeren als een /32-route via BGP naar andere pagina's.

Opmerking: in dit scenario heeft de host een statisch IP, dus SIFS gebruikt ARP om de hostgegevens te verzamelen. In het gedeelte over het algemeen geïsoleerde DHCP- en DHCP-snuffelen wordt weergegeven.

```
<#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 DHCP
```

```
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

EVPN Mgr leert Local MAC en installeert in L2RIB. EVPN Mgr leert ook de Remote MAC van L2RIB, maar entry wordt alleen gebruikt voor het verwerken van MAC-mobiliteit

Bevestig dat EVPN Mgr wordt bijgewerkt met de SISF-vermelding

```
<#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 leert lokale MAC van EVPN Mgr en stuurt deze naar BGP en L2FIB.
- L2RIB is ook verantwoordelijk voor het leren van externe MAC's van BGP om EVPN Mgr en L2FIB bij te werken.
- L2RIB heeft zowel Local als Remote nodig om andere onderdelen goed te kunnen updaten.
- L2RIB-component ligt tussen lokaal en extern MAC-leren afhankelijk van welke richting / component moet worden bijgewerkt

Controleer of L2RIB is bijgewerkt met de lokale MAC van 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

Controleer of BGP is bijgewerkt door 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, Label 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 (standaardgateway RT2)

BGP

Controleer of BGP de CGW RT2-prefix heeft geleerd

```
<#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

Controleer BGP-update L2RIB

- L2RIB leert lokale MAC van EVPN Mgr en stuurt deze naar BGP en L2FIB. L2RIB is ook verantwoordelijk voor het leren van externe MAC's van BGP om EVPN Mgr en L2FIB bij te werken.
- L2RIB heeft zowel Local als Remote nodig om andere onderdelen goed te kunnen updaten.
- L2RIB-component ligt tussen lokale en externe MAC-learning, afhankelijk van welke richting en component moet worden bijgewerkt.

```
<#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

Verifiëren in L2FIB

- Component verantwoordelijk voor het updaten van de FED met de MAC's voor het programmeren in hardware.
- De externe MAC-ingangen die door L2FIB in FED-MATM zijn geïnstalleerd, worden NIET gekopieerd naar IOS-MATM. (IOS-MATM toont alleen lokale MAC's, terwijl FED-MATM zowel lokale als externe MAC toont).
- L2FIB-uitvoer toont alleen externe MAC's (het is niet verantwoordelijk voor de programmering van lokale MAC's).

<#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 from
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

Verifiëren via FED MATM

- Op het hardwareniveau van de bladeren die met het 'beveiligde trefwoord' zijn geconfigureerd, moet u alleen de CGW standaard gateway MAC en de lokale host MACs zien.
- De switch bekijkt het prefix RT2 voor het kenmerk DEF GW om te bepalen welke afstandsbediening in aanmerking komt voor installatie.

<#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_DO_NOT_AGE	0x100	MAT_SECURE_ADDR	0x200	MAT_NO_PORT	0x400
MAT_DUP_ADDR	0x1000	MAT_NULL_DESTINATION	0x2000	MAT_DOT1X_ADDR	0x4000
MAT_WIRELESS_ADDR	0x10000	MAT_SECURE_CFG_ADDR	0x20000	MAT_OPQ_DATA_PRESENT	0x40000
MAT_DLR_ADDR	0x100000	MAT_MRP_ADDR	0x200000	MAT_MSRRP_ADDR	0x400000

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

Adjacency voor gegevensplane

Als laatste stap na bevestiging van FED-vermelding kunt u de herschrijvingsindex (RI) oplossen

<#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)
```

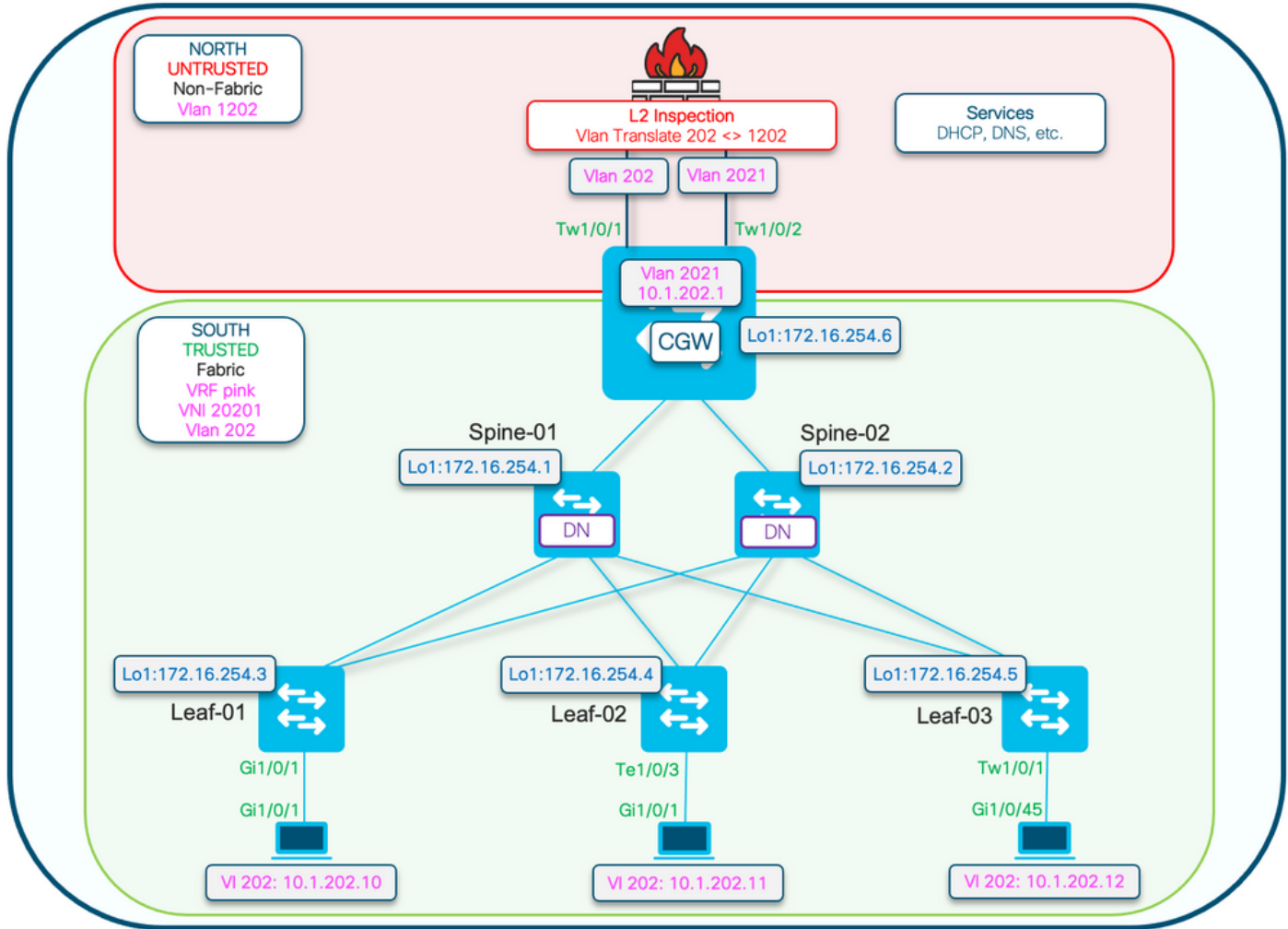
```
Vlan LE:        8 (0)
```

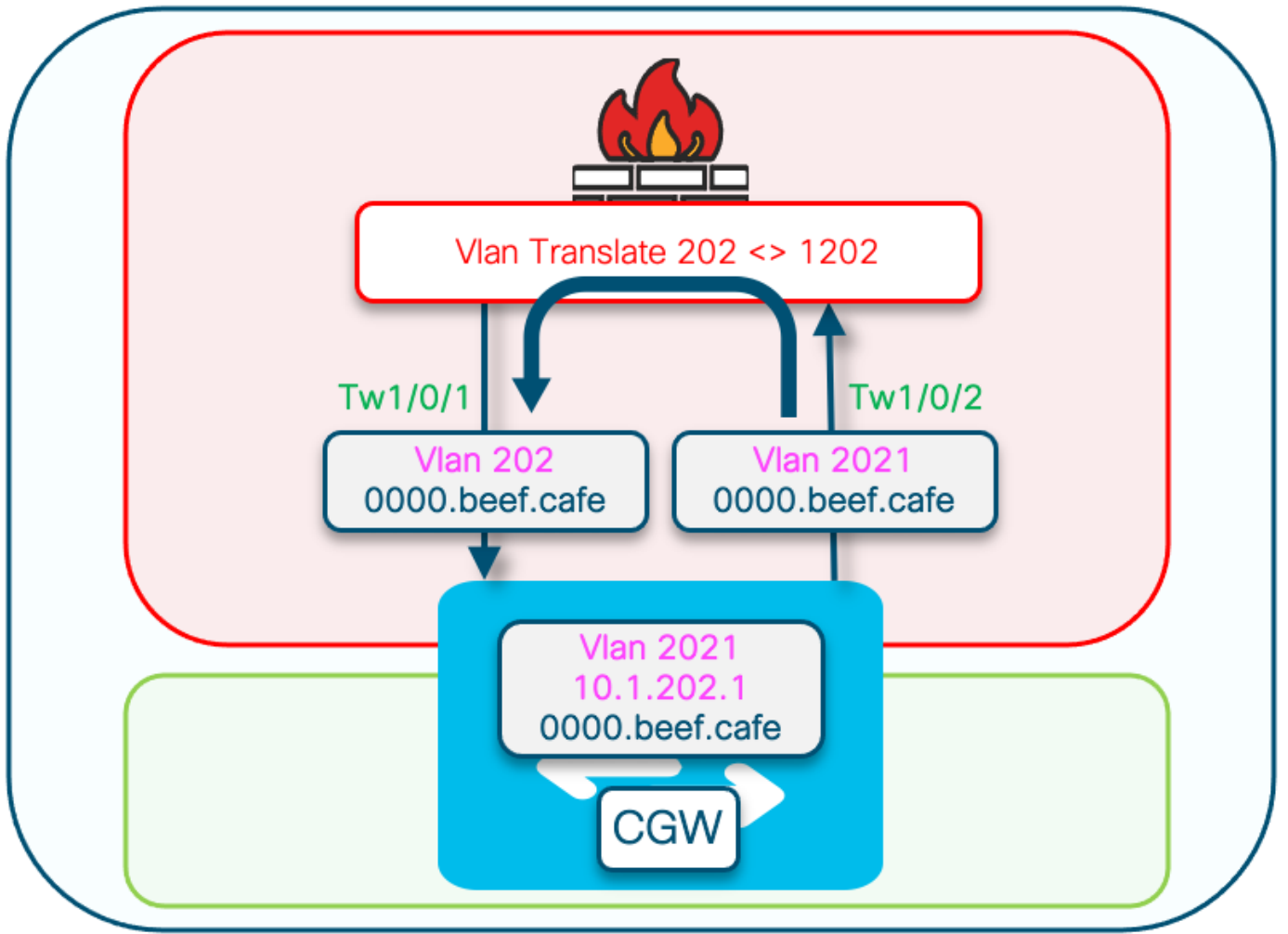


Opmerking: U kunt ook 'show platform software fed switch active matm macTable vlan 201 detail' gebruiken die deze opdracht met de opdracht FED in één resultaat verbindt

Configureren (gedeeltelijk geïsoleerd)

Netwerkdigram







Toelichting: Deze paragraaf behandelt alleen verschillen van volledig geïsoleerde segmenten.

- Routing-beleid om de GCW gateway MAC IP te markeren met het kenmerk DEF GW
- Aangepast apparaattraceringsbeleid vereist om MAC-flaps te voorkomen
- Statische apparaat-tracking binding voor de GW MAC IP

Leaf-01 (basis-EVPN-configuratie)

```
<#root>
```

```
Leaf-01#
```

```
show run | sec 12vpn  
12vpn 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 (basisconfiguratie)

Stel de replicatiemodus in onder het menu

<#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
```

Configureer de externe 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
```

Maak een beleid met glimmen gehandicapten

```
<#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
```

Bevestigen aan externe gatewayevi/VLAN's

```
<#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
```

Voeg statische ingangen in apparaat het volgen lijst voor externe gateway mac-ip toe


```
<#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
```

Maak BGP-routekaart om RT2 MAC-IP-prefixes aan te passen en stel de standaardgateway extendedcommunity in

```
<#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
```

Route-map toepassen op BGP-routereflectorburen

```
<#root>
```

```
CGW#
```

```
sh run | s r bgp
```

```
address-family 12vpn 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
```

Verifiëren (gedeeltelijk geïsoleerd)

EVI-gegevens

<#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-generatie (lokale host voor RT2)

Gedekt in vorig volledig geïsoleerd voorbeeld

Remote RT2 Learning (standaardgateway RT2)

Dekt de verschillen van volledig geïsoleerd

CGW standaardgatewayprefix (blad)

Controleer of het prefix de juiste eigenschap heeft om in aanmerking te komen voor installatie in de hardware

Opmerking: dit is essentieel voor het functioneren van DHCP L2 Relay

```
<#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 (blad)

<#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	riHandle
------	-----	------	------	-------	-------	-----------	----------	----------

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 DHCP

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

S	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>

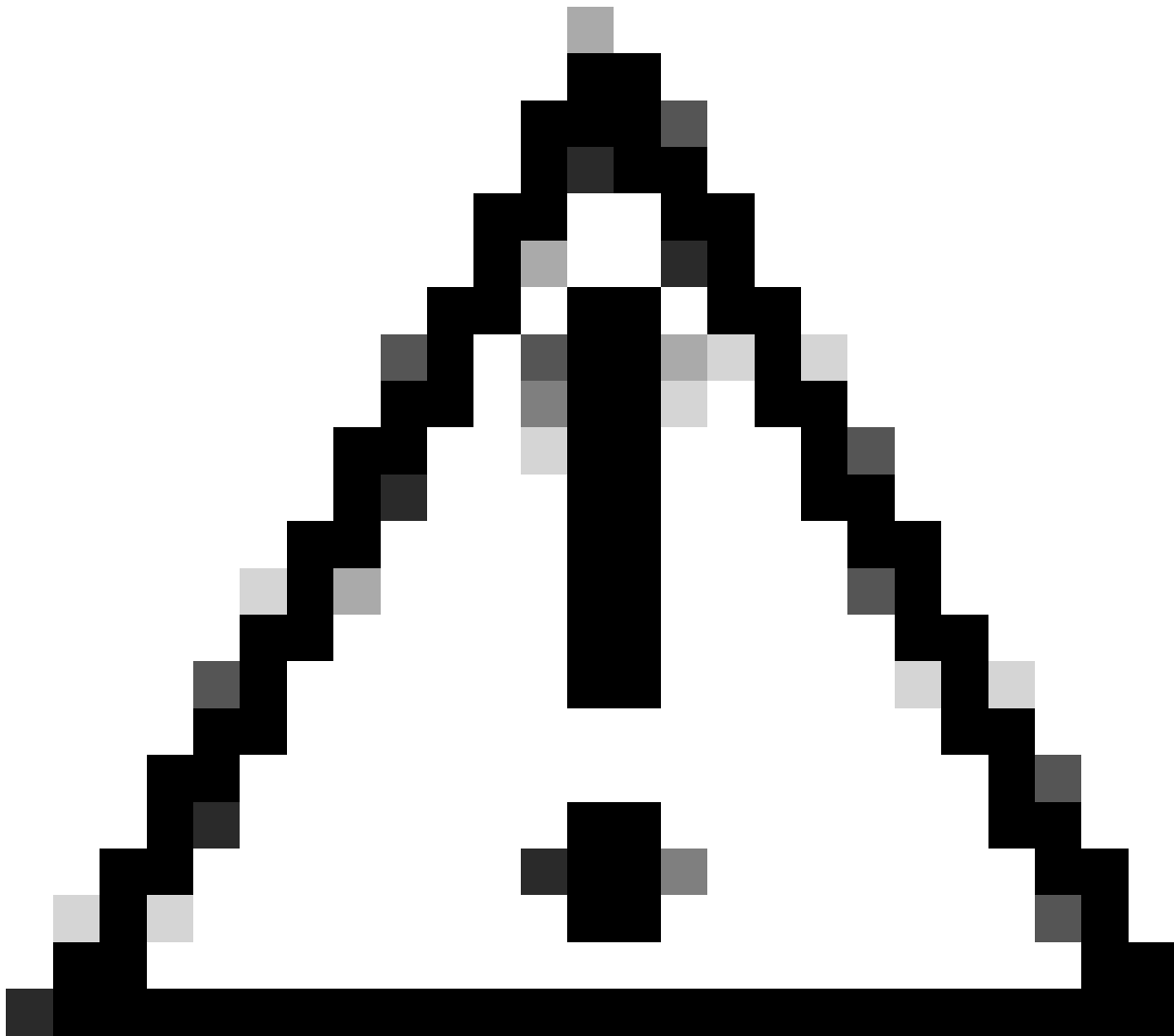
```
CGW#  
show mac address-table address 0000.beef.cafe  
  
Mac Address Table  
-----  
Vlan    Mac Address      Type      Ports  
----    -  
201     0000.beef.cafe  STATIC   Vl201  
2021    0000.beef.cafe  STATIC   Vl2021  <-- The Vlan 2021 SVI MAC advertised out Tw1/0/1  
202     0000.beef.cafe  DYNAMIC  Twel/0/1 <-- The Vlan 2021 SVI MAC learned dynamically after pass
```

Problemen oplossen

Adresoplossing (ARP)

Algemene stappen voor het isoleren van ARP kwesties

- Bevestig dat de IMET-tunnel klaar is
- Leg vast op CGW uplink om te controleren of ARP is ontvangen via bladopname
- Als er geen ARP te zien aankomende encaps op uplink
 - Controleer of de IMET-tunnel op zowel Leaf als CGW klaar is
 - Leg op bladuplinks vast om te bevestigen dat ARP is ingekapseld en verzonden
 - Probleemoplossing voor tussenliggende pad
- Als ARP op border IMET-tunnelopname arriveert maar niet geprogrammeerd in VRF ARP-tabel, moeten we de volgende stap zetten
 - Probleemoplossing voor CPU/CoPP puntpad om ARP gestraft te bevestigen voor CPU-
 - Bevestig dat IP-adres / clientgegevens juist zijn.
 - Zuig ARP in VRF om te zien wat ARP proces zou kunnen beïnvloeden
- Controleer CGW MAC geïnstalleerd als volgende hop / dest mac op de hosts
- Bevestig dat CGW beide ARP-vermeldingen heeft met de echte host-MAC's
- Controleer of het firewallbeleid dit type verkeer toestaat



Waarschuwing: Wees voorzichtig wanneer het inschakelen van debugs!

Zorg ervoor dat u de onderdrukking van overstromingen hebt uitgeschakeld

```
<#root>
```

```
Leaf-01#
```

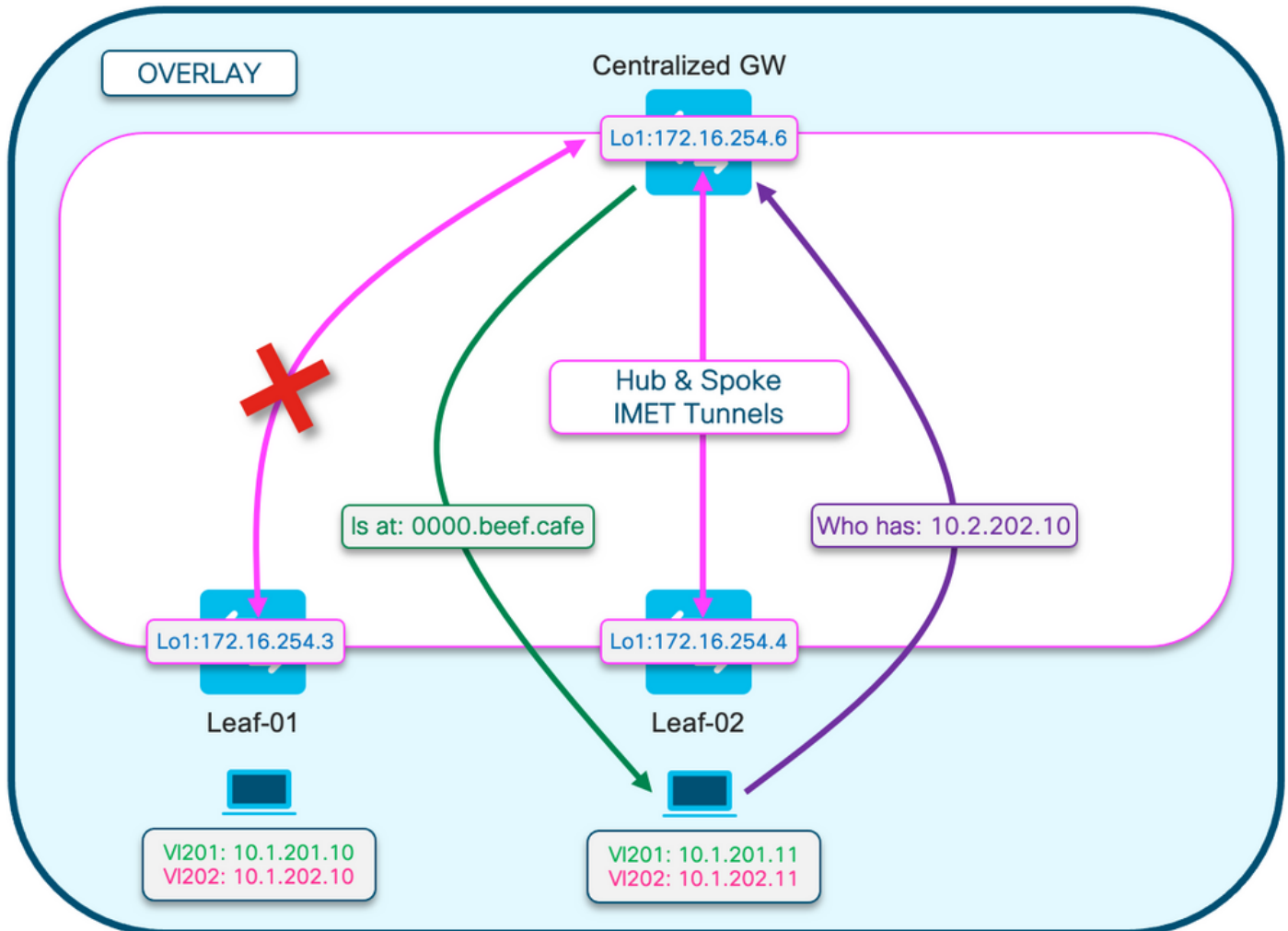
```
show run | sec 12vpn  
12vpn evpn
```

```
replication-type static
```

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

Wanneer host van Leaf-02 ARP oplost voor host van Leaf-01 wordt het ARP-verzoek niet direct naar Leaf-01 uitgezonden

- De ARP wordt in plaats daarvan doorgegeven de enige BUM-tunnel geprogrammeerd op Leaf-02 naar de CGW
- De CGW stuurt dit niet door naar Leaf-01, maar antwoordt met zijn eigen MAC
- Dit zorgt ervoor dat alle communicatie wordt doorgegeven aan de CGW en vervolgens wordt gerouteerd naar tussen de hosts
- CGW routeert pakketten, zelfs wanneer ze op hetzelfde lokale subsysteem staan



Dit diagram helpt bij het visualiseren van de stroom van het ARP-resolutieproces dat in deze sectie wordt beschreven.

Het ARP Verzoek wordt getoond in paars

- Dit ARP verzoek is om het MAC-adres van de host 10.1.202.10 van Leaf-01 op te lossen
- Merk op dat de paarse lijn eindigt bij de CGW en niet Leaf-01 bereikt

Het ARP antwoord wordt weergegeven in groen

- Het antwoord bevat de MAC van CGW SVI voor VLAN 2012
- Merk op dat de groene lijn van CGW, niet van de daadwerkelijke gastheer komt

Opmerking: De rode X is om aan te geven dat deze communicatie niet het verzenden van verkeer naar Leaf-01 betrof.

Neem de ARP vermeldingen op elke respectievelijke host waar

```
<#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
```

```
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
```

Let op CGW de RT2 prefixes worden aangeleerd. Dit is vereist voor de CGW om pakketten te routeren

```
<#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: 000000000000000000000000,
```

```
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: 000000000000000000000000,
```

```
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
```

Leg de ARP-uitwisseling op de uplinks vast om bidirectionele communicatie te bevestigen

- U kunt Embedded Packet Capture (EPC) gebruiken op de Fabric uplinks
- Dit scenario toont EPC op de Leaf01 uplink. Herhaal indien nodig dit zelfde proces op CGW

De EPC configureren

```
<#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
```

Start de vastlegging

```
<#root>
Leaf01#
monitor capture 1 start
```

Initiate ping om het ARP verzoek teweeg te brengen (In dit geval ping is van Leaf01 host 10.1.201.10 tot 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

Opname en controle van ARP-frames stoppen

```
<#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
```

Bekijk de opnamepakketten in detail. Als u meer informatie wilt zien over het pakket, gebruik dan de detailoptie van EPC

- Houd in acht dat deze uitvoer op verschillende plaatsen wordt geknipt zodat u het kort houdt

```
<#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: 00000000000000000000000000000000
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: 00000000000000000000000000000000

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 lo

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-gatewayprefix

Gatewayprefix ontbreekt

Zoals vermeld in de vorige sectie over gedeeltelijk geïsoleerde segmenten moet de MAC worden geleerd in de stof VLAN

- Deze kwestie kan zich voordoen als er geen verkeer is bestemd voor de gateway voor langer dan de verouderende tijdopnemer van MAC.
- Als het voorvoegsel CGW Gateway ontbreekt, moet u bevestigen dat de MAC aanwezig is

<#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   V1201  
2021    0000.beef.cafe  STATIC   V12021  
  
<-- MAC is not learned in Fabric Vlan 202  
Total Mac Addresses for this criterion: 2
```

Gatewayprefix voor ontbrekende oplossing

In de meeste productienetwerken zal er waarschijnlijk altijd wel wat verkeer zijn. Als u echter dit probleem hebt, kunt u een van deze opties gebruiken om het probleem op te lossen:

- Voeg statische MAC-vermeldingen toe zoals 'mac-adrestabel statisch 000.beef.café VLAN 202 interface TwentyFiveGigE1/0/1'
- Verhoog de MAC aging timer met 'mac address-table aging-time <seconden>'. (Houd in gedachten dat dit de verouderingstijd voor alle MAC-adressen verhoogt, zodat de statische MAC-optie de voorkeur heeft)

Ontbrekende DEF GW-kenmerk

Met gedeeltelijk geïsoleerde segmenten zijn er een aantal extra configuraties om deze eigenschap toe te voegen.

Ontbrekende correctie van DEF GW-kenmerken

Bevestig deze gegevens:

- U draait op 17.12.1 of hoger
- De SISF (Device-Tracking) CLI is aanwezig in de configuratie
- De route-kaart gelijke & vastgestelde bevelen worden gevormd en de route-kaart wordt toegepast op de burens BGP
- U hebt de BGP-advertenties ververs (u moet BGP wissen om het prefix opnieuw te adverteren met het nieuwe attribuut)

Draadloos roaming

Frequent roaming kan ertoe leiden dat BGP te vaak werkt en roaming per tijdsinterval moet worden verhoogd voordat switch verklaart eigenaar te zijn van de MAC en verstuurt RT2 Update

- Dit gebeurt wanneer een host beweegt tussen twee AP's die op verschillende switches zijn.
- Standaardlimiet voor zwerven is 5 per 180 seconden

<#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...>

Te verzamelen opdrachten voor TAC

In het geval dat deze handleiding uw probleem niet heeft opgelost, verzamelt u de getoonde opdrachtlijst en voegt u deze toe aan uw TAC-serviceverzoek.

Minimale te verzamelen informatie

(beperkte tijd voor het verzamelen van gegevens voorafgaand aan herladen/herstelactie)

- Toon tech evpn

- Toon tech-
- Toon tech sisf

Gedetailleerde informatie die moet worden verzameld

(Als er tijd is om meer volledige gegevens te verzamelen, verdient dit de voorkeur)

- Toon tech
- show tech-evenement
- show tech platform evpn_vxlan switch <number>
- Toon tech platform
- Toon tech resource
- show tech sisf
- show tech isis
- show tech bgp
- toon monitor gebeurtenis-spoor evpn gebeurtenis allen
- toon monitor gebeurtenis-spoor evpn fout allen
- archiefbestand voor opsporingssoftware voor aanvraagplatform

Gerelateerde informatie

- [Voer het BGP EVPN-routingbeleid op Catalyst 9000 Series Switches uit](#)
- DHCP Layer 2 Relay (binnenkort beschikbaar)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.