Dépannage de DHCP externe sur EVPN VxLAN Cat9000

Table des matières

Introduction

Ce document décrit comment dépanner les problèmes DHCP dans les environnements EVPN VxLAN externes sur les plates-formes Cat9000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau local virtuel extensible sur plates-formes Cat9000
- Protocoles de configuration des hôtes de découverte sur les environnements VxLAN
- Protocole BGP (Border Gateway Protocol)

Pour plus d'informations sur ces sujets, reportez-vous à :

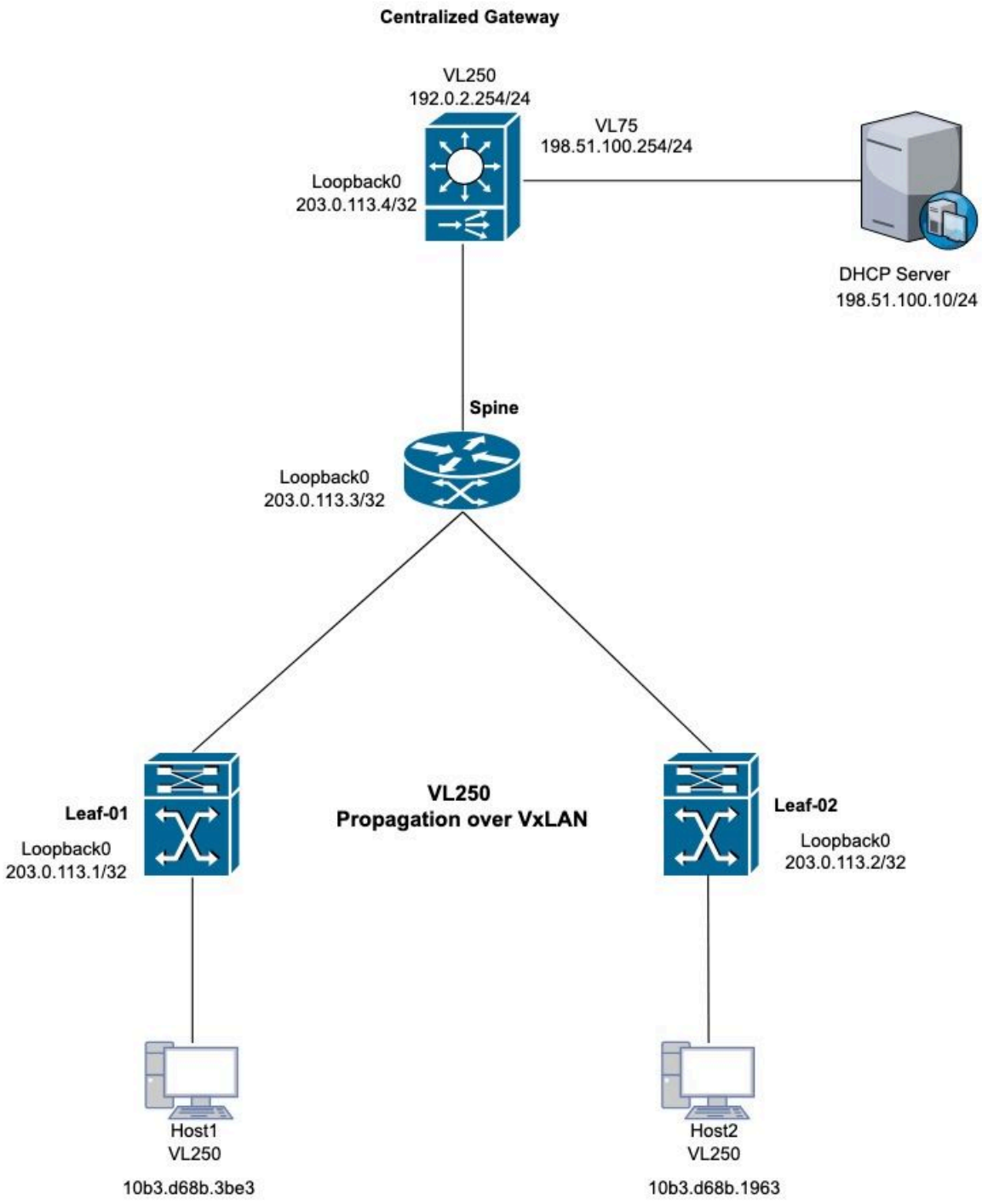
- Chapitre : Configuration du relais DHCP dans un fabric VXLAN EVPN BGP Cat9300
- Chapitre : Configuration du relais DHCP dans un fabric VXLAN EVPN BGP Cat9400
- Chapitre : Configuration du relais DHCP dans un fabric VXLAN EVPN BGP Cat9500
- Chapitre : Configuration du relais DHCP dans un fabric VXLAN EVPN BGP Cat9600

Composants utilisés

Les informations contenues dans ce document sont basées sur le logiciel Cisco IOS XE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Diagramme du réseau



Topologie DHCP VxLAN

Étude de cas 1 : Impossible d'obtenir une adresse IP du serveur externe (passerelle centralisée à l'intérieur du fabric)

Cette topologie utilise la couche 2 VxLAN pour le VLAN 250. L’hôte requiert des adresses IP du serveur DHCP externe.

Vérification Leaf-01

Étape 1. Sur Leaf-1, vérifiez l’apprentissage des adresses MAC pour les hôtes locaux.

Étape 2. Vérifiez également que l’adresse MAC de la passerelle par défaut est apprise. Assurez-vous que les adresses MAC apprises et l'adresse IP de la passerelle par défaut sont correctement installées en tant qu'entrées dans la table BGP.

<#root>

```
Leaf-1#

show mac address-table address



10b3.d68b.3be3

 (host mac address)
            Mac Address Table
------------------------------------------

Vlan    Mac Address     Type     Ports
----   -----------      -------- -----
250    10b3.d68b.3be3   DYNAMIC  Twe1/0/1

Centralized-Gateway#

show interface vlan 250 | include bia

(remote mac address)
Hardware is Ethernet SVI, address is

3473.2db8.bee3

 (bia 3473.2db8.bee3)
```

<#root>

```
Leaf-1#

show bgp l2vpn evpn



10b3.d68b.3be3

 (local mac address)
```

```
BGP routing table entry for [2][203.0.113.1:250][0][48][1OB3D68B3BE3][0][*]/20, version 3
Paths: (1 available, best #1, table evi_250)
 Advertised to update-groups:
    2
Refresh Epoch 1
Local
```

0.0.0.0 (via default) from 0.0.0.0 (203.0.113.1)

```
    Origin incomplete, localpref 100, weight 32768, valid, sourced, local,
```

best

```
    EVPN ESI: 00000000000000000000, Label1 10250
    Extended Community: RT:10:250 ENCAP:8
    Local irb vxlan vtep:
     vrf:not found, l3-vni:0
     local router mac:0000.0000.0000
     core-irb interface:(not found)
```

vtep-ip:203.0.113.1

```
   rx pathid: 0, tx pathid: 0x0
   Updated on Oct 14 2025 22:27:32 UTC

Leaf-1#
```

show bgp l2vpn evpn 3473.2db8.bee3

```
(remote mac address)
BGP routing table entry for [2][203.0.113.1:250][0][48][34732DB8BEE3][32][192.0.2.254]/24, version 9
Paths: (1 available, best #1, table evi_250)
  Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 4
  Local, imported path from [2][203.0.113.4:250][0][48][34732DB8BEE3][32][192.0.2.254]/24 (global)
    203.0.113.4 (metric 3) (via default) from 203.0.113.3 (203.0.113.3)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      EVPN ESI: 00000000000000000000, Label1 10250
      Extended Community: RT:10:250 ENCAP:8 EVPN DEF GW:0:0
      Originator: 203.0.113.4, Cluster list: 203.0.113.3
      rx pathid: 0, tx pathid: 0x0
      Updated on Oct 14 2025 14:48:35 UTC
BGP routing table entry for [2][203.0.113.4:250][0][48][34732DB8BEE3][32][192.0.2.254]/24, version 8
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Flag: 0x100
  Not advertised to any peer
  Refresh Epoch 4
  Local
    203.0.113.4 (metric 3) (via default) from 203.0.113.3 (203.0.113.3)
      Origin incomplete, metric 0, localpref 100, valid, internal,
```

best

```
      EVPN ESI: 0000000000000000000, Label1 10250
      Extended Community: RT:10:250 ENCAP:8 EVPN DEF GW:0:0
      Originator: 203.0.113.4, Cluster list: 203.0.113.3
      rx pathid: 0, tx pathid: 0x0
      Updated on Oct 14 2025 14:48:35 UTC
```

Étape 3 : validation de l'apprentissage des adresses MAC entre Leaf-1 et la passerelle par défaut Leaf-1 apprend les adresses MAC locales via le port agrégé et les adresses MAC distantes via BGP.

<#root>

```
Leaf-1#

show l2route evpn mac


EVI         ETag  Prod    Mac Address                                          Next Hop(s) Seq Number
----- ---------- ----- -------------- ---------------------------------------------------- ----------
250            0 L2VPN 10b3.d68b.3b81                                        Twe1/0/1:250          0
250            0

L2VPN 10b3.d68b.3be3

                                          Twe1/0/1:250          0 (Host local mac address)
250            0

 BGP 3473.2db8.bee3

                                   V:10250 203.0.113.4          0 (CGW SVI mac address)
```

Étape 4 : vérification de l'apprentissage de la passerelle par défaut sur le commutateur Leaf-1 au sein de l'instance EVPN L2VPN

<#root>

```
Leaf-1#

show l2vpn evpn default-gateway


Valid Default Gateway Address                  EVI  VLAN  MAC Address    Source
----- ---------------------------------- ----- ----- -------------- -----------
Y     192.0.2.254                              250   250   3473.2db8.bee3 203.0.113.4
```

Étape 5. Si la perspective VxLAN est correcte, passez au protocole DHCP pour effectuer le dépannage.

Étape 6. Confirmez le processus DORA de Leaf-1 à la passerelle DHCP. Sur Leaf-01, activez debug the ip dhcp snooping packet et vérifiez si la détection génère des entrées de journal. Si la génération du journal n'a pas lieu, activez les captures de paquets sur l'interface qui se connecte au PC.

<#root>

```
Leaf-1#

debug ip dhcp snooping packet


DHCP Snooping Packet debugging is on
Leaf-1#
*Oct 21 19:33:16.358: DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1
*Oct 21 19:33:16.358: DHCP Memory dump is printed for process packet
<snip>
*Oct 21 19:33:16.367:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Twe1/0/1, MAC da: f


, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.
*Oct 21 19:33:16.367: DHCP_SNOOPING: add relay information option.
*Oct 21 19:33:16.367: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Oct 21 19:33:16.367:

DHCP_SNOOPING:VxLAN : vlan_id 250 VNI 10250 mod 1 port 1


*Oct 21 19:33:16.367: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
*Oct 21 19:33:16.367: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB
*Oct 21 19:33:16.367: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Oct 21 19:33:16.367: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Oct 21 19:33:16.367: DHCP_SNOOPING: L2RELAY: sent unicast packet to default gw: 3473.2db8.bee3 vlan 0
*Oct 21 19:33:20.058: DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1
*Oct 21 19:33:20.058: DHCP Memory dump is printed for process packet
```

Étape 7. Si le débogage ne se déclenche pas, effectuez une capture de paquets pour validation. Utilisez la syntaxe spécifiée pour capturer les paquets de détection en entrée :

```
monitor capture <name> interface <int> in match ipv4 protocol udp any range 67 68 any range 67 68 start
monitor capture <name> stop
monitor capture export file flash:<name>.pcap
show monitor capture <name> buffer display-filter "eth.addr==[mac address]" detailed
```

Remarque : Capturez les chaînes de filtre d'affichage qui respectent la syntaxe de filtre Wireshark.

<#root>

```
Leaf-1#

monitor capture cap interface twe1/0/1 in match ipv4 protocol udp any range 67 68 any range 67 68 start


Started capture point : cap
Leaf-1#
*Oct 21 22:57:04.719: %BUFCAP-6-ENABLE: Capture Point cap enabled.
Leaf-1#
Leaf-1#

monitor capture cap stop


Capture statistics collected at software:
        Capture duration - 96 seconds


  Packets received - 10



        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Capture buffer will exists till exported or cleared

Stopped capture point : cap

*Oct 21 22:58:40.810: %BUFCAP-6-DISABLE: Capture Point cap disabled.

Leaf-1#

show monitor capture cap buffer display-filter "eth,addr==10:b3:d6:8b:3b:e3" detailed


Starting the packet display ........ Press Ctrl + Shift + 6 to exit
Frame 1: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface /tmp/epc_ws/wif_to_
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 21, 2025 22:57:07.843851000 UTC
     [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1761087427.843851000 seconds
  <snip>
    [Protocols in frame: eth:ethertype:vlan:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
```

```
   Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
       Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
       .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
       .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
   Source: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
       Address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 250
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 1111 1010 = ID: 250
Type: IPv4 (0x0800)

<snip>

User Datagram Protocol,

Src Port: 68, Dst Port: 67



    Source Port: 68
    Destination Port: 67
    Length: 333
    Checksum: 0xdf55 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x3bd7aadb
Seconds elapsed: 7

Bootp flags: 0x8000, Broadcast flag (Broadcast)



    1... .... .... .... = Broadcast flag: Broadcast
    .000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0

Client MAC address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)



Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)
```

```
<snip>
```

Étape 8 : validation de l'encapsulation de paquets VxLAN via la capture de paquets Appliquez différents filtres pour cette validation. VxLAN utilise le port UDP 4789.

```
monitor capture cap interface <outgoing interface > out match ipv4 protocol udp any any eq 4789  (Inter
```

<#root>

```
Leaf-1#
```

show ip bgp all summary

```
For address family: L2VPN E-VPN
<snip>
Neighbor       V           AS MsgRcvd MsgSent    TblVer InQ OutQ Up/Down   State/PfxRcd
```

203.0.113.3

```
     4           10    4204    4122       365    0    0 2d13h            2
Leaf-1#
```

show ip route 203.0.113.3

```
Routing entry for 203.0.113.3/32
Known via "ospf 1", distance 110, metric 2, type intra area
Last update from 172.x.x.2 on TwentyFiveGigE1/0/2, 2d13h ago
Routing Descriptor Blocks:
* 172.x.x.2, from 203.0.113.3, 2d13h ago, via
```

TwentyFiveGigE1/0/2

```
Leaf-1#
```

monitor capture cap interface twe1/0/2 out match ipv4 protocol udp any any eq 4789 start

```
*Oct 21 23:51:07.689: %BUFCAP-6-ENABLE: Capture Point cap enabled.
Leaf-1#
```

show monitor capture cap buffer display-filter "eth.addr==10:b3:d6:8b:3b:e3" detailed

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface /tmp/epc_ws/wif_to_
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 21, 2025 23:51:34.848693000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1761090694.848693000 seconds
   <snip>
   [Protocols in frame: eth:

ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]



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: 203.0.113.1, Dst: 203.0.113.4



    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
<snip>
User Datagram Protocol, Src Port: 65479, Dst Port: 4789
    Source Port: 65479
    Destination Port: 4789
    Length: 409
    [Checksum: [missing]]
    [Checksum Status: Not present]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]

Virtual eXtensible Local Area Network



Flags: 0x0800, VXLAN Network ID (VNI)
    0... .... .... .... = GBP Extension: Not defined
    .... .... .0.. .... = Don't Learn: False
    .... 1... .... .... = VXLAN Network ID (VNI): True
    .... .... .... 0... = Policy Applied: False
    .000 .000 0.00 .000 = Reserved(R): 0x0000
Group Policy ID: 0

VXLAN Network Identifier (VNI): 10250
```

```
Reserved: 0
<snip>

User Datagram Protocol, Src Port: 68, Dst Port: 67


    Source Port: 68
    Destination Port: 67
    Length: 359
    Checksum: 0x767d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    [Timestamps]
         [Time since first frame: 0.000000000 seconds]
         [Time since previous frame: 0.000000000 seconds]
Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xd4c42ec1
    Seconds elapsed: 0


 Bootp flags: 0x8000, Broadcast flag (Broadcast)


        1... .... .... .... = Broadcast flag: Broadcast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0


 Client MAC address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)


    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
```

Vérification de passerelle centralisée

Étape 1 : validation de l'adresse MAC hôte apprise sur les routes BGP et EVPN de couche 2 (cette étape reflète la procédure de vérification Leaf initiale)

<#root>

```
Centralized-Gateway#
```

show bgp l2vpn evpn 10b3.d68b.3be3

```
 (remote host mac address)
BGP routing table entry for [2][203.0.113.1:250][0][48][10B3D68B3BE3][0][*]/20, version 12
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Not advertised to any peer
  Refresh Epoch 1
  Local
```

203.0.113.1 (metric 3) (via default) from 203.0.113.3 (203.0.113.3)

```
 (learned via RR)
  Origin incomplete, metric 0, localpref 100, valid, internal,
```

best

```
  EVPN ESI: 00000000000000000000, Label1 10250
  Extended Community: RT:10:250 ENCAP:8
  Originator: 203.0.113.1, Cluster list: 203.0.113.3
  rx pathid: 0, tx pathid: 0x0
  Updated on Oct 27 2025 17:53:37 UTC
BGP routing table entry for [2][203.0.113.4:250][0][48][10B3D68B3BE3][0][*]/20, version 14
Paths: (1 available, best #1, table evi_250)
  Not advertised to any peer
  Refresh Epoch 1
  Local, imported path from [2][203.0.113.1:250][0][48][10B3D68B3BE3][0][*]/20 (global)
    203.0.113.1 (metric 3) (via default) from 203.0.113.3 (203.0.113.3)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    EVPN ESI: 00000000000000000000, Label1 10250
    Extended Community: RT:10:250 ENCAP:8
    Originator: 203.0.113.1, Cluster list: 203.0.113.3
    rx pathid: 0, tx pathid: 0x0
    Updated on Oct 27 2025 17:53:37 UTC

Centralized-Gateway#
```

show l2route evpn mac mac-address 10b3.d68b.3be3

```
EVI         ETag  Prod    Mac Address                                          Next Hop(s) Seq Number
----- ---------- ----- -------------- ---------------------------------------------------- ----------
250            0
```

BGP 10b3.d68b.3be3

V:10250 203.0.113.1

```
          0
```

Étape 2 : vérification des informations de relais DHCP et de la configuration de la surveillance DHCP sur la passerelle centralisée

<#root>

```
Centralized-Gateway#

show running-config | section dhcp


ip dhcp-relay source-interface Loopback0
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp compatibility suboption link-selection standard
ip dhcp compatibility suboption server-override standard
ip dhcp snooping vlan 250
ip dhcp snooping
```

Étape 3 : vérification de la connectivité au serveur DHCP et envoi d'une requête ping à partir de l'interface VLAN 250

<#root>

```
Centralized-Gateway#

ping 198.51.100.10 source vlan 250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.10, timeout is 2 seconds:
Packet sent with a source address of 192.0.2.254
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Étape 4. Effectuez une capture de paquets pour vérifier si les messages de détection des hôtes distants atteignent la passerelle centralisée.

<#root>

```
Centralized-Gateway#

monitor capture cap interface vlan250 in match ipv4 protocol udp any range 67 68 any range 67 68


Centralized-Gateway#monitor capture cap start
Started capture point : cap
```

<#root>

Centralized-Gateway#

show monitor capture cap buffer display-filter "eth.addr==10:b3:d6:8b:3b:e3" detailed

Starting the packet display .... Press Ctrl + Shift + 6 to exit

Frame 1: 401 bytes on wire (3208 bits), 401 bytes captured (3208 bits) on interface /tmp/epc_ws/wif_to_
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 27, 2025 20:43:30.774923000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1761597810.774923000 seconds
 <snip>
    [Protocols in frame: eth:ethertype:cmd:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3), Dst: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
    Destination: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
        Address: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
        .... ..0. .... = LG bit: Globally unique address (factory default)
        ....0 .... = IG bit: Individual address (unicast)
    Source: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
        Address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
        .... ..0. .... = LG bit: Globally unique address (factory default)
        ....0 .... = IG bit: Individual address (unicast)
   Type: CiscoMetaData (0x8909)
<snip>
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 379
    Identification: 0x0230 (560)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0xb842 [validation disabled]
    [Header checksum status: Unverified]

 Source Address: 0.0.0.0

    Destination Address: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

```
    Source Port: 68
    Destination Port: 67
    Length: 359
    Checksum: 0x8f64 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (351 bytes)

Dynamic Host Configuration Protocol (Discover)


    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xf23af863
    Seconds elapsed: 0
    Bootp flags: 0x8000, Broadcast flag (Broadcast)
        1... .... .... .... = Broadcast flag: Broadcast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0


Client MAC address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)


    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP


Option: (53) DHCP Message Type (Discover)


        Length: 1
        DHCP: Discover (1)
    Option: (57) Maximum DHCP Message Size
        Length: 2
        Maximum DHCP Message Size: 1200
    Option: (61) Client identifier
        Length: 27
        Type: 0


Client Identifier: cisco-10b3.d68b.3be3-Vl250


<snip>
```

Étape 5. Effectuez une capture de paquets suivante sur le commutateur. Vérifiez la sortie de détection et la sortie d'offre.

<#root>

```
Centralized-Gateway#

no monitor capture cap

Centralized-Gateway#

monitor capture cap interface vlan 75 both match ipv4 protocol udp any range 67 68 any range 67 68

Centralized-Gateway#

monitor capture cap start

Started capture point : cap




Centralized-Gateway#

monitor capture cap stop


Capture statistics collected at software:



        Capture duration - 78 seconds


Packets received - 0


        Packets dropped - 0
        Packets oversized - 0
Bytes dropped in asic - 0
```

Étape 6. Si la capture de paquets n’affiche aucun paquet, poursuivez le débogage DHCP et validez l’état du paquet sur la plate-forme.

<#root>

```
Centralized-Gateway#
```

debug ip dhcp snooping packet

```
<snip>
*Oct 27 22:20:24.444: DHCP_SNOOPING: process
```

new DHCP packet, message type: DHCPDISCOVER,

```
 input interface: Tu0, MAC da: 3473.2db8.bee3,
```

MAC sa: 10b3.d68b.3be3

```
, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.
*Oct 27 22:20:24.445: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Oct 27 22:20:24.445: DHCP_SNOOPING: Packet destined to SVI Mac:3473.2db8.bee3
*Oct 27 22:20:24.445: DHCP_SNOOPING: bridge packet send packet to cpu port: Vlan250.
*Oct 27 22:20:24.445: DHCP_SNOOPING: bridge packet send packet to port: GigabitEthernet1/0/2, pak_vlan
*Oct 27 22:20:27.952: DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)
*Oct 27 22:20:27.952: DHCP Memory dump is printed for process packet.

Centralized-Gateway#
```

debug ip dhcp server packet detail

```
*Oct 27 22:27:58.009: DHCPD: BOOTREQUEST from 0063.6973.636f.2d31.3062.332e.6436.3862.2e33.6265.332d.56



*Oct 27 22:28:02.008: DHCPD: tableid for 192.0.2.254 on Vlan250 is 0



*Oct 27 22:28:02.008: DHCPD: client's VPN is .
*Oct 27 22:28:02.008: DHCPD: No option 125



*Oct 27 22:28:02.008: DHCPD: Option 124: Vendor Class Information
*Oct 27 22:28:02.008: DHCPD: Enterprise ID: 9
*Oct 27 22:28:02.008: DHCPD: Vendor-class-data-len: 13



*Oct 27 22:28:02.008: DHCPD: Data: 43393330304C2D3234502D3447
*Oct 27 22:28:02.008: DHCPD: Option 125 not present in the msg.
*Oct 27 22:28:02.008: DHCPD: Option 125 not present in the msg.
*Oct 27 22:28:02.008: DHCPD: Looking up binding using address 192.0.2.254
*Oct 27 22:28:02.008: DHCPD: setting giaddr to 192.0.2.254.
```

```
*Oct 27 22:28:02.008: DHCPD: relay information option before replacing suboptions



*Oct 27 22:28:02.008: DHCPD: 5218010c010a00080000280a01010000020800064c5d3ceb4340
*Oct 27 22:28:02.008: DHCPD: replacing suboptions in relay information option.
*Oct 27 22:28:02.008: DHCPD: relay information option content (add/replace):



*Oct 27 22:28:02.008: DHCPD: 52060504c00002fe
*Oct 27 22:28:02.008: DHCPD: giaddr changed to 203.0.113.4
```

Étape 7. Vérifiez que les interfaces qui se connectent au serveur DHCP incluent la commande spécifiée (ceci empêche la suppression du paquet DHCP).

<#root>

```
Centralized-Gateway#sh running-config interface gi1/0/2
Building configuration...

Current configuration : 149 bytes
!
interface GigabitEthernet1/0/2
description to L2_switch
switchport trunk allowed vlan 75,250
switchport mode trunk

ip dhcp snooping trust


end
```

Remarque : La commande ip dhcp snooping trust s'applique uniquement aux interfaces trunk de couche 2.

Solution au problème

La configuration VxLAN fonctionne comme prévu. Cependant, le relais du serveur DHCP envoie des réponses DHCP à l'adresse IP 203.0.113.4. Le serveur DHCP n'est pas accessible à cette adresse IP. Ce manque de connectivité a entraîné des abandons de paquets de monodiffusion au niveau de la passerelle centralisée.

Pour résoudre ce problème, une nouvelle interface de bouclage 1 a été configurée et une route

pour l’adresse IP a été établie pour fournir la connectivité avec cette adresse de relais de bouclage.

Journaux DHCP :

<#root>

```
DHCP-Server#d

ebug ip dhcp server packet detail


DHCP server packet detail debugging is on.
*Oct 28 00:23:43.464:

DHCPD: DHCPDISCOVER

 received from client 0063.6973.636f.2d31.3062.332e.6436.3862.2e33.6265.332d.566c.3235.30 through relay
*Oct 28 00:23:43.464: DHCPD: Option 125 not present in the msg.
*Oct 28 00:23:43.465: DHCPD: egress Interfce GigabitEthernet0/0/4.75

*Oct 28 00:23:43.465: DHCPD: unicasting BOOTREPLY for client 10b3.d68b.3be3 to relay 203.0.113.4.


DHCP-Server#

ping 203.0.113.4

Type escape sequence to abort.



Sending 5, 100-byte ICMP Echos to 203.0.113.4, timeout is 2 seconds:



.....



Success rate is 0 percent (0/5)



DHCP-Server#
```

Passerelle centralisée : Configurez la connectivité à la nouvelle interface de bouclage pour la fonction de relais.

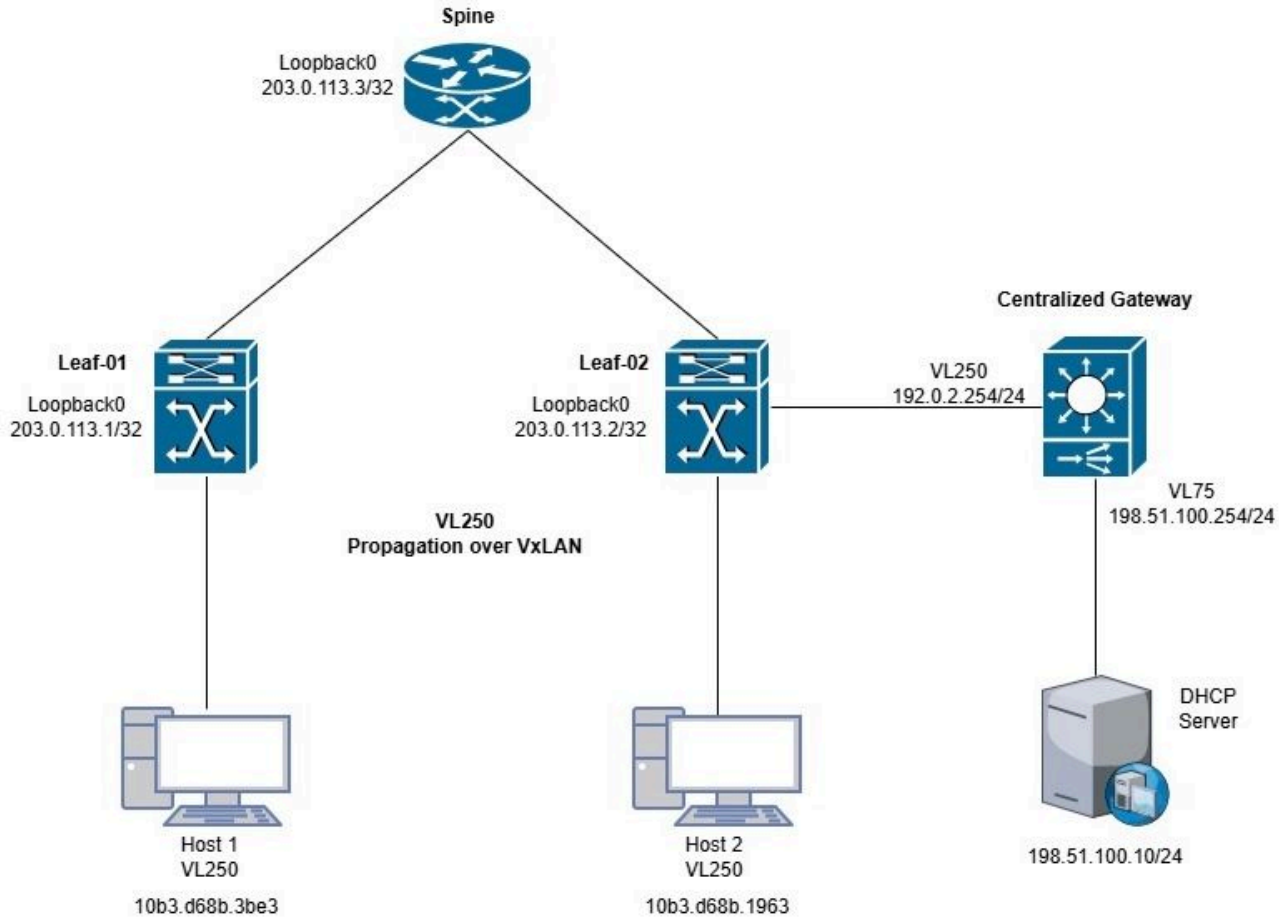
<#root>

```
Centralized-Gateway#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.



Centralized-Gateway(config)#

interface loopback 1

Centralized-Gateway(config-if)#

ip address 198.51.100.25 255.255.255.255

Centralized-Gateway(config-if)#

router eigrp 1

Centralized-Gateway(config-router)#

network 198.51.100.25 0.0.0.0

Centralized-Gateway(config-router)#exit



Centralized-Gateway(config)#

no ip dhcp-relay source-interface Loopback0

Centralized-Gateway(config)#

ip dhcp-relay source-interface Loopback1


DHCP-Server#

ping 198.51.100.25

Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 198.51.100.25, timeout is 2 seconds:
!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
DHCP-Server#
```

Étude de cas 2 : Impossible d'obtenir une adresse IP du serveur externe (passerelle centralisée en dehors du fabric)

Cette topologie utilise la couche 2 VXLAN pour le VLAN 250. L'hôte obtient son adresse IP d'un serveur DHCP externe situé à l'extérieur du fabric.



Topologie VxLAN DHCP externe

Vérification Leaf-01

Étape 1. Sur Leaf-1, vérifiez l'annonce correcte sur la passerelle par défaut. Comme le serveur DHCP est situé en dehors du fabric VxLAN, il s'agit d'une condition essentielle pour la fonctionnalité correcte de l'attribution d'adresses IP.

<#root>

```
Leaf-1#

show l2vpn evpn default-gateway


Valid Default Gateway Address EVI VLAN MAC Address Source
----- ------------------------------------ ----- ----- -------------- -----------
```

Étape 2. Si la sortie précédente est vide, poursuivez le dépannage DHCP. Vérifiez que les configurations de surveillance DHCP appropriées sont présentes sur les périphériques Leaf.

<#root>

```
Leaf-1#show running-config | section dhcp

ip dhcp relay information option vpn



ip dhcp relay information option



ip dhcp compatibility suboption link-selection standard



ip dhcp compatibility suboption server-override standard



ip dhcp snooping vlan 250



ip dhcp snooping
```

<#root>

```
Leaf-2#show running-config | section dhcp

ip dhcp relay information option vpn



ip dhcp relay information option



ip dhcp compatibility suboption link-selection standard



ip dhcp compatibility suboption server-override standard



ip dhcp snooping vlan 250



ip dhcp snooping
```

Étape 3. Si un périphérique demande activement une adresse IP via DHCP, activez la commande de débogage appropriée pour valider l'état du paquet sur la plate-forme.

<#root>

```
*Dec 6 22:42:19.568:

 DHCP_SNOOPING: received new DHCP packet from input interface (TwentyFiveGigE1/0/1)


*Dec 6 22:42:19.568: DHCP Memory dump is printed for process packet
<snip>
*Dec 6 22:42:19.578:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, input interface: Twe1/0/1


, MAC da: ffff.ffff.ffff, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa: 0.0.0.0, DHCP ciaddr:
*Dec 6 22:42:19.578: DHCP_SNOOPING: add relay information option.
*Dec 6 22:42:19.578: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Dec 6 22:42:19.578: DHCP_SNOOPING:VxLAN : vlan_id 250 VNI 10250 mod 1 port 1
*Dec 6 22:42:19.578: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
*Dec 6 22:42:19.578: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB
```

```
*Dec 6 22:42:19.579: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 6 22:42:19.579: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is floo
*Dec 6 22:42:19.579:
```

DHCP_SNOOPING: L2RELAY: cannot find default gw for bd 250: src intf TwentyFiveGigE1/0/1

Remarque : Le dernier message de débogage indique que le périphérique n'a pas pu identifier la passerelle par défaut pour le VLAN 250.

Vérification Leaf-02

Leaf-2 étant le leaf de périphérie actif à l'intérieur du fabric VxLAN, il est responsable du transfert des informations relatives à la passerelle par défaut.

Étape 1 : validation de la capacité de L2VPN EVPN à annoncer la passerelle par défaut

<#root>

```
Leaf-2#
```

show l2vpn evpn summary

```
L2VPN EVPN
EVPN Instances (excluding point-to-point): 1
VLAN Based: 1
Vlans: 1
BGP: ASN 65000, address-family l2vpn evpn configured
Router ID: 203.0.113.2
Global Replication Type: Ingress
ARP/ND Flooding Suppression: Enabled
Connectivity to Core: UP
MAC Duplication: seconds 180 limit 5
MAC Addresses: 5
Local: 3
Remote: 2
Duplicate: 0
IP Duplication: seconds 180 limit 5
IP Addresses: 2
Local: 2
Remote: 0
Duplicate: 0
```

Advertise Default Gateway: No

```
Default Gateway Addresses: 0
Local: 0
```

```
Remote: 0
Maximum number of Route Targets per EAD-ES route: 200
Multi-home aliasing: Enabled
Multi-home send proxy MAC/IP: Enabled
Multi-home device ID: 0000.5e00.0101
Global IP Local Learn: Enabled
IP local learning limits
IPv4: 4 addresses per-MAC
IPv6: 12 addresses per-MAC
IP local learning timers
Down: 10 minutes
Poll: 1 minutes
Reachable: 5 minutes
Stale: 30 minutes
Auto route-target: vni-based
Advertise Multicast: No
Global Anycast Gateway MAC: No
```

Étape 2. Le résultat précédent confirme que Leaf-2 n'annonce pas la passerelle par défaut à l'autre Leaf-1 au sein du même fabric VxLAN. Procédez à la configuration nécessaire pour effectuer l'annonce correcte.

<#root>

```
Leaf-2(config)#

l2vpn evpn


Leaf-2(config-evpn)#

default-gateway advertise
```

Étape 3. Une fois la configuration ajoutée, la fonctionnalité EVPN L2VPN doit être activée.

<#root>

```
Leaf-2#

show l2vpn evpn summary


--snip--

Advertise Default Gateway: Yes
```

Étape 4. Une fois activée, configurez l'annonce appropriée pour la passerelle par défaut vers

l’autre leaf au sein du fabric VxLAN.

Solution du problème 1

La configuration des fonctions de surveillance EVPN L2VPN et DHCP fonctionne comme prévu. Cependant, l'annonce de passerelle par défaut n'est pas exécutée. Par conséquent, les périphériques finaux connectés à Leaf-1 ne peuvent pas recevoir d'adresse IP du serveur DHCP.

Pour résoudre ce problème, l'annonce doit être configurée.

Étape 1 : configuration d’une liste de contrôle d’accès et d’une carte de routage pour annoncer la passerelle par défaut via BGP aux autres périphériques Leaf sur le réseau

<#root>

```
Leaf-2(config)#

ip access-list extended GW250


Leaf-2(config-ext-nacl)#

10 permit ip host 192.0.2.254 any

 (permit the IP address if the GW)

Leaf-2(config)#

route-map CGW


Leaf-2(config-route-map)#match ip address GW250
Leaf-2(config-route-map)#

match evpn route-type 2-mac-ip


Leaf-2(config-route-map)#

set extcommunity default-gw



Leaf-2(config)#

router bgp 65000
```

```
Leaf-2(config-router)#address-family l2vpn evpn
Leaf-2(config-router-af)#
```

neighbor 203.0.113.3 route-map CGW out

Étape 2. Une fois la configuration précédente ajoutée, vérifiez Leaf-1 pour afficher l'annonce de passerelle par défaut correcte.

<#root>

```
Leaf-1#
```

show l2vpn evpn default-gateway

```
Valid Default Gateway Address                EVI   VLAN  MAC Address    Source
----- ------------------------------------- ----- ----- -------------- -----------
  Y   192.0.2.254                           250   250   3473.2db8.bee3 203.0.113.2
```

Remarque : Sur le VTEP Border, la vérification de la passerelle par défaut affiche une valeur vide. Ce comportement est normal, car la passerelle centralisée est directement connectée au VTEP de périphérie.

<#root>

```
Leaf-2#
```

show l2vpn evpn default-gateway

```
Valid Default Gateway Address EVI VLAN MAC Address Source
----- ------------------------------------- ----- ----- -------------- -----------
```

Maintenant, les périphériques Leaf affichent correctement l'annonce de passerelle par défaut. Vérifiez que les périphériques finaux reçoivent correctement l'adresse IP du serveur DHCP.

Vérification de l'hôte 1

Étape 1. Sur l'hôte 1, demandez une adresse IP via DHCP :

<#root>

```
Host1#

show running-config interface vlan 250


Building configuration...
Current configuration : 42 bytes
!
interface Vlan250

ip address dhcp


end
```

Étape 2. Vérifier si l’adresse IP a été correctement attribuée :

```
Host1#show ip interface brief | include DHCP
Vlan250   unassigned   YES    DHCP    up    up
```

Étape 3. Si l’adresse IP n’est pas attribuée correctement après que la passerelle par défaut a été correctement annoncée par le leaf en limite, poursuivez le dépannage DHCP.

Vérification Leaf 2

Étape 1 : activation du débogage pour DHCP, en particulier pour la surveillance DHCP, pour observer comment le périphérique traite les paquets lors de leur transfert en dehors du fabric VXLAN.

<#root>

```
Leaf-2#

debug ip dhcp snooping packet


DHCP Snooping Packet debugging is on
```

Étape 2. Redémarrez le processus DHCP sur le périphérique hôte et examinez les journaux :

<#root>

```
Leaf-2#

debug ip dhcp snooping packet


*Dec 12 20:11:43.891: DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)
*Dec 12 20:11:43.891: DHCP Memory dump is printed for process packet
<snip>
*Dec 12 20:11:43.902:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER

, input interface: Tu0, MAC da: 3473.2db8.bee3, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa:
*Dec 12 20:11:43.902: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 20:11:43.902:

DHCP_SNOOPING: bridge packet output port set is null, packet is dropped.
```

Étape 3. Les journaux précédents indiquent que le paquet est abandonné. Ce message signifie que la fonctionnalité de surveillance DHCP sur le commutateur a reçu un paquet DHCP qui ne peut pas être transféré parce que le port de sortie n'est pas valide. Cela se produit généralement lorsque la surveillance DHCP ne parvient pas à déterminer le port de sortie approprié pour transférer le paquet DHCP.

Étape 4. Pour résoudre ce problème, l'interface pointant vers la passerelle centralisée doit être configurée comme étant approuvée.

<#root>

```
Leaf-2(config)#

interface fortyGigabitEthernet 2/0/1


Leaf-2(config-if)#

ip dhcp snooping trust
```

Étape 5. Vérifier si l'attribution d'adresses IP via DHCP fonctionne comme prévu.

<#root>

```
Leaf-2#
```

```
debug ip dhcp snooping packet


*Dec 12 20:33:54.156: DHCP Memory dump is printed for process packet

<snip>
*Dec 12 20:33:54.167:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER


, input interface: Tu0, MAC da: 3473.2db8.bee3, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa:
*Dec 12 20:33:54.167: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 20:33:54.167:

DHCP_SNOOPING: bridge packet send packet to port: FortyGigabitEthernet2/0/1, pak_vlan 250.
```

Étape 6. La preuve indique que le périphérique identifie désormais correctement l'interface physique via le paquet DHCPDISCOVER et qu'il doit être transféré, car l'interface est marquée comme approuvée du point de vue de la surveillance DHCP. Cependant, l'attribution de l'adresse IP ne fonctionne toujours pas comme prévu.

Vérification de passerelle centralisée

Étape 1. Le leaf en limite transférant désormais les paquets DHCP via l'interface appropriée, si l'attribution de l'adresse IP continue d'échouer, suivez les procédures de dépannage DHCP standard.

```
<#root>

Centralized-Gateway#debug ip dhcp server packet


DHCP server packet debugging is on.

*Dec 12 20:39:36.029: DHCPD: tableid for 192.0.2.254 on Vlan250 is 0
*Dec 12 20:39:36.029: DHCPD: client's VPN is .
*Dec 12 20:39:36.029: DHCPD: No option 125
*Dec 12 20:39:36.029: DHCPD: Option 124: Vendor Class Information
*Dec 12 20:39:36.029: DHCPD: Enterprise ID: 9
*Dec 12 20:39:36.029: DHCPD: Vendor-class-data-len: 13
*Dec 12 20:39:36.029: DHCPD: Data: 43393330304C2D3234502D3447
*Dec 12 20:39:36.029: DHCPD: inconsistent relay information.
*Dec 12 20:39:36.029:

DHCPD: relay information option exists, but giaddr is zero
```

Étape 2. Sur la base du résultat du débogage de la passerelle centralisée et des résultats de la capture de paquets, une configuration supplémentaire est requise pour empêcher le périphérique d'éliminer les paquets lorsque le champ giaddr est défini sur zéro.

Lorsqu'un paquet DHCP est reçu avec l'option d'informations de relais présente mais que l'adresse IP de la passerelle (giaddr) est définie sur tous les zéros, l'agent de relais DHCP, par défaut, abandonne le paquet. Pour résoudre ce problème, configurez la commande ip dhcp relay information trusted.

Étape 3. Pour vérifier que le périphérique reçoit le paquet, effectuez une capture de paquet :

<#root>

```
Configure an Access-list to filter the interested traffic.

Extended IP access list dhcp



 10 permit udp any any eq 67



 20 permit udp any eq 67 any



Configure the capture.
Centralized-Gateway#

monitor capture tac interface gigabitethernet1/0/1 both access-list dhcp buffer size 10


Centralized-Gateway#

monitor capture cap start

Started capture point : cap



Centralized-Gateway#

monitor capture cap stop


Capture statistics collected at software:
```

```
 Capture duration - 58 seconds

 Packets received - 6


 Packets dropped - 0
 Packets oversized - 0
 Bytes dropped in asic - 0

Centralized-Gateway#
```

show monitor capture cap buffer display-filter "eth.addr==10:b3:d6:8b:3b:e3" detailed

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 1: 397 bytes on wire (3176 bits), 397 bytes captured (3176 bits) on interface /tmp/epc_ws/wif_to_
    Interface id: 0 (/tmp/epc_ws/wif_to_ts_pipe)
        Interface name: /tmp/epc_ws/wif_to_ts_pipe
    Encapsulation type: Ethernet (1)
    Arrival Time: Dec 12, 2025 18:35:21.821468000 UTC
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1765564521.821468000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 397 bytes (3176 bits)
    Capture Length: 397 bytes (3176 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:vlan:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3), Dst: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
    Destination: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
        Address: 34:73:2d:b8:be:e3 (34:73:2d:b8:be:e3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
        Address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: 802.1Q Virtual LAN (0x8100)
```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 250

```
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 1111 1010 = ID: 250
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 379
```

```
    Identification: 0x4b04 (19204)
    Flags: 0x00
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 255
    Protocol: UDP (17)
    Header Checksum: 0x6f6e [validation disabled]
    [Header checksum status: Unverified]
```

Source Address: 0.0.0.0

Destination Address: 255.255.255.255

User Datagram Protocol, Src Port: 68, Dst Port: 67

```
    Source Port: 68
    Destination Port: 67
    Length: 359
    Checksum: 0x2ae5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (351 bytes)
```

Dynamic Host Configuration Protocol (Discover)

```
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe9986585
    Seconds elapsed: 0
    Bootp flags: 0x8000, Broadcast flag (Broadcast)
        1... .... .... .... = Broadcast flag: Broadcast
        .000 0000 0000 0000 = Reserved flags: 0x0000
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
```

Client MAC address: 10:b3:d6:8b:3b:e3 (10:b3:d6:8b:3b:e3)

```
    Client hardware address padding: 00000000000000000000
    Server host name not given
```

```
    Boot file name not given
    Magic cookie: DHCP


Option: (53) DHCP Message Type (Discover)


        Length: 1
        DHCP: Discover (1)
    Option: (57) Maximum DHCP Message Size
        Length: 2
        Maximum DHCP Message Size: 1200
    Option: (61) Client identifier
        Length: 27
        Type: 0


Client Identifier: cisco-10b3.d68b.3be3-Vl250
```

Étape 4. Selon la capture de paquet précédente, le paquet DHCP est correctement reçu par le périphérique.

Solution au problème 2

Étape 1. Sur la base du résultat du débogage de la passerelle centralisée et des résultats de la capture de paquets, une configuration supplémentaire est requise pour empêcher le périphérique d'éliminer les paquets lorsque le champ giaddr est défini sur zéro.

Lorsqu'un paquet DHCP est reçu avec l'option d'informations de relais présente, mais que l'adresse IP de la passerelle (giaddr) est définie sur tous les zéros, l'agent de relais DHCP abandonne généralement le paquet.

Pour résoudre ce problème, configurez la commande ip dhcp relay information trusted.

<#root>

```
Centralized-Gateway(config)#

interface vlan 250


Centralized-Gateway(config-if)

#ip dhcp relay information trusted
```

Étape 2. Procédez à la vérification en demandant une adresse IP à l'hôte 1.

<#root>

Host1#

*Dec 12 21:32:12.659: %DHCP-6-ADDRESS_ASSIGN: Interface Vlan250 assigned DHCP address 192.0.2.1, mask 2

Leaf-2#

*Dec 12 21:36:03.232: DHCP_SNOOPING: received new DHCP packet from input interface (Tunnel0)
<snip>
*Dec 12 21:36:03.243:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER

, input interface: Tu0, MAC da: 3473.2db8.bee3, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa:
*Dec 12 21:36:03.243: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 21:36:03.243:

DHCP_SNOOPING: bridge packet send packet to port: FortyGigabitEthernet2/0/1

, pak_vlan 250.
*Dec 12 21:36:03.245: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEtherne
<snip>
*Dec 12 21:36:03.255:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER

, input interface: Fo2/0/1, MAC da: ffff.ffff.ffff, MAC sa: 3473.2db8.bee3, IP da: 255.255.255.255, IP
*Dec 12 21:36:03.255: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB
*Dec 12 21:36:03.256: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0
*Dec 12 21:36:03.256: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB 0x43 0x40
*Dec 12 21:36:03.256: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Dec 12 21:36:03.256: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan
*Dec 12 21:36:03.256: DHCP_SNOOPING: opt82 data indicates not a local packet
*Dec 12 21:36:03.256: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Dec 12 21:36:03.256: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Dec 12 21:36:03.256: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10
*Dec 12 21:36:03.256:

DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 250 from Fo2/0/1

<snip>
*Dec 12 21:36:03.401:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

```
, input interface: Tu0, MAC da: 3473.2db8.bee3, MAC sa: 10b3.d68b.3be3, IP da: 255.255.255.255, IP sa:
*Dec 12 21:36:03.401: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 21:36:03.401:

DHCP_SNOOPING: bridge packet send packet to port: FortyGigabitEthernet2/0/1

, pak_vlan 250.
*Dec 12 21:36:03.402: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEtherne
<snip>
*Dec 12 21:36:03.413:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK

, input interface: Fo2/0/1, MAC da: ffff.ffff.ffff, MAC sa: 3473.2db8.bee3, IP da: 255.255.255.255, IP
*Dec 12 21:36:03.413: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0 0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB
*Dec 12 21:36:03.413: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x1 0x1 0x0 0x0
*Dec 12 21:36:03.413: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x4C 0x5D 0x3C 0xEB 0x43 0x40
*Dec 12 21:36:03.413: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Dec 12 21:36:03.413: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan
*Dec 12 21:36:03.413: DHCP_SNOOPING: opt82 data indicates not a local packet
*Dec 12 21:36:03.413: DHCP_SNOOPING: EVPN enabled Ex GW:fabric relay can't parse option 82 data of the
*Dec 12 21:36:03.413: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Dec 12 21:36:03.413: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10
*Dec 12 21:36:03.413: DHCP_SNOOPING: can't find client's destination port, packet is assumed to be not
*Dec 12 21:36:03.413: DHCP_SNOOPING: client address lookup failed to locate client interface, retry loo
*Dec 12 21:36:03.413: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10
*Dec 12 21:36:03.413:

DHCP_SNOOPING: L2RELAY: Ex GW unicast bridge packet to fabric: vlan id 250 from Fo2/0/1
```

Étape 3. L'adresse IP a été correctement attribuée et il est conseillé de valider le même comportement du point de vue de l'hôte 2.

<#root>

```
Host2#
*Dec 12 21:13:03.926:

%DHCP-6-ADDRESS_ASSIGN: Interface Vlan250 assigned DHCP address 192.0.2.2, mask 255.255.255.0, hostname
```

```
Leaf-2#
*Dec 12 22:08:15.417: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEtherne
<snip>
*Dec 12 22:08:15.428:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER

, input interface: Fo2/0/2, MAC da: ffff.ffff.ffff, MAC sa: 10b3.d68b.1963, IP da: 255.255.255.255, IP
```

```
*Dec 12 22:08:15.428: DHCP_SNOOPING: add relay information option.
*Dec 12 22:08:15.428: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Dec 12 22:08:15.428:
```

DHCP_SNOOPING:VxLAN : vlan_id 250 VNI 10250 mod 2 port 2

```
*Dec 12 22:08:15.428: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
*Dec 12 22:08:15.428: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x7D 0xB4 0xA8
*Dec 12 22:08:15.428: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 22:08:15.428: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Dec 12 22:08:15.428:
```

DHCP_SNOOPING: L2RELAY: cannot find default gw for bd 250: src intf FortyGigabitEthernet2/0/2

```
*Dec 12 22:08:15.430: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEtherne
<snip>
*Dec 12 22:08:15.440:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER

```
, input interface: Fo2/0/1, MAC da: ffff.ffff.ffff, MAC sa: 3473.2db8.bee3, IP da: 255.255.255.255, IP
*Dec 12 22:08:15.440: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x7D 0xB4 0xA8
*Dec 12 22:08:15.440: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0
*Dec 12 22:08:15.440: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x68 0x7D 0xB4 0xA8 0xAF 0x0
*Dec 12 22:08:15.440: actual_fmt_cid OPT82_FMT_CID_VXLAN_MOD_PORT_INTF global_opt82_fmt_rid OPT82_FMT_R
*Dec 12 22:08:15.440: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan
*Dec 12 22:08:15.440: DHCP_SNOOPING: opt82 data indicates local packet
*Dec 12 22:08:15.440: DHCP_SNOOPING: remove relay information option.
*Dec 12 22:08:15.440: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Dec 12 22:08:15.440: DHCP_SNOOPING: VxLAN vlan_id 250 VNI 10250 mod 2 port 2
*Dec 12 22:08:15.440:
```

DHCP_SNOOPING: mod 2 port 2 idb Fo2/0/2 found for 10b3.d68b.1963

```
*Dec 12 22:08:15.441: DHCP_SNOOPING: calling forward_dhcp_reply
*Dec 12 22:08:15.441: platform lookup dest vlan for input_if: FortyGigabitEthernet2/0/1, is NOT tunnel,
*Dec 12 22:08:15.441: DHCP_SNOOPING opt82_fmt_cid_intf OPT82_FMT_CID_VXLAN_MOD_PORT_INTF opt82_fmt_cid_
*Dec 12 22:08:15.441: DHCP_SNOOPING: VxLAN vlan_id 250 VNI 10250 mod 2 port 2
*Dec 12 22:08:15.441: DHCP_SNOOPING: mod 2 port 2 idb Fo2/0/2 found for 10b3.d68b.1963
*Dec 12 22:08:15.441: DHCP_SNOOPING: vlan 250 after pvlan check
<snip>
*Dec 12 22:08:15.930:
```

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST

```
, input interface: Fo2/0/2, MAC da: ffff.ffff.ffff, MAC sa: 10b3.d68b.1963, IP da: 255.255.255.255, IP
*Dec 12 22:08:15.930: DHCP_SNOOPING: add relay information option.
*Dec 12 22:08:15.930: DHCP_SNOOPING: Encoding opt82 CID in vlan-mod-port format
*Dec 12 22:08:15.930: DHCP_SNOOPING:VxLAN : vlan_id 250 VNI 10250 mod 2 port 2
*Dec 12 22:08:15.930: DHCP_SNOOPING: Encoding opt82 RID in MAC address format
```

```
*Dec 12 22:08:15.930: DHCP_SNOOPING: binary dump of relay info option, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x7D 0xB4 0xA8
*Dec 12 22:08:15.930: DHCPS BRIDGE PAK: vlan=250 platform_flags=1
*Dec 12 22:08:15.930: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flo
*Dec 12 22:08:15.930:

DHCP_SNOOPING: L2RELAY: cannot find default gw for bd 250: src intf FortyGigabitEthernet2/0/2


*Dec 12 22:08:15.932: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEtherne
<snip>
*Dec 12 22:08:15.940:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK


, input interface: Fo2/0/1, MAC da: ffff.ffff.ffff, MAC sa: 3473.2db8.bee3, IP da: 255.255.255.255, IP
*Dec 12 22:08:15.943: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
0x52 0x18 0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0 0x2 0x8 0x0 0x6 0x68 0x7D 0xB4 0xA8
*Dec 12 22:08:15.943: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
0x1 0xC 0x1 0xA 0x0 0x8 0x0 0x0 0x28 0xA 0x2 0x2 0x0 0x0
<snip>
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.