

Problemen oplossen met externe DHCP op EVPN VxLAN Cat9000

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Casestudy 1: IP-adres kan niet worden verkregen van de externe server \(gecentraliseerde gateway in de fabric\)](#)

[Leaf-01-verificatie](#)

[Gecentraliseerde gateway-verificatie](#)

[probleemoplossing](#)

[Casestudy 2: IP-adres kan niet worden verkregen van de externe server \(gecentraliseerde gateway buiten de verbinding\)](#)

[Leaf-01-verificatie](#)

[Leaf-02-verificatie](#)

[Probleemoplossing 1](#)

[Verificatie van host 1](#)

[Leaf 2-verificatie](#)

[Gecentraliseerde gateway-verificatie](#)

[Probleemoplossing 2](#)

Inleiding

In dit document wordt beschreven hoe u problemen met DHCP kunt oplossen in externe EVPN VxLAN-omgevingen op Cat9000-platforms.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Virtueel uitbreidbaar LAN op Cat9000-platforms
- Discovery Host Configuration Protocollen voor VxLAN-omgevingen
- Border Gateway Protocol (BGP)

Voor meer informatie over deze onderwerpen, zie:

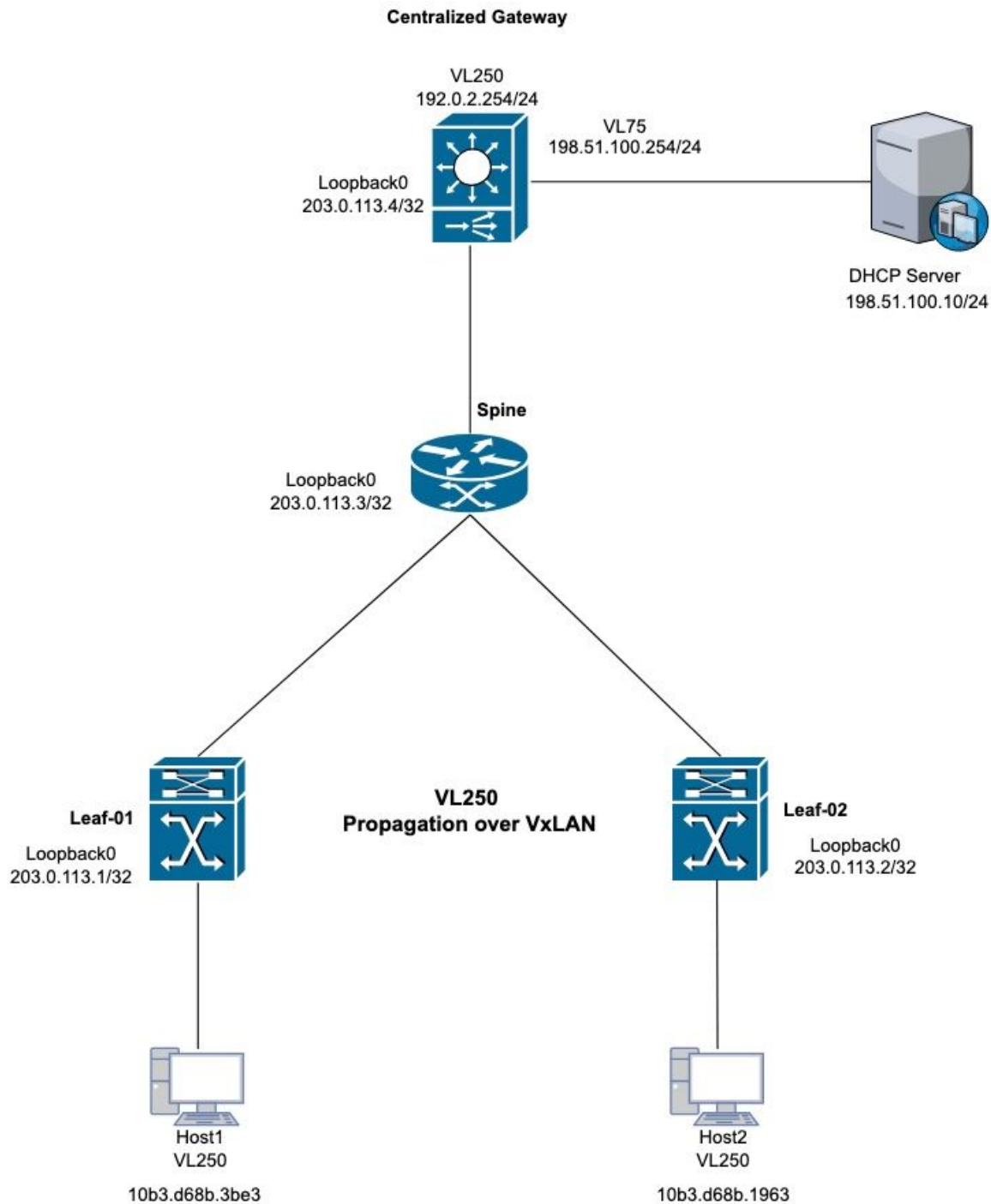
- [Hoofdstuk: DHCP-relais configureren in een BGP EVPN VXLAN Fabric Cat9300](#)
- [Hoofdstuk: DHCP-relais configureren in een BGP EVPN VXLAN Fabric Cat9400](#)
- [Hoofdstuk: DHCP-relais configureren in een BGP EVPN VXLAN Fabric Cat9500](#)
- [Hoofdstuk: DHCP-relais configureren in een BGP EVPN VXLAN Fabric Cat9600](#)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS XE-software.

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.

Netwerkdigram



DHCP VxLAN-topologie

Casestudy 1: IP-adres kan niet worden verkregen van de externe server (gecentraliseerde gateway in de fabric)

Deze topologie gebruikt de VxLAN Layer 2 voor VLAN 250. De host heeft IP-adressen nodig van de externe DHCP-server.

Leaf-01-verificatie

Stap 1. Controleer in Leaf-1 het leren van MAC-adressen voor lokale hosts.

Stap 2. Bevestig bovendien dat het standaard MAC-adres van de gateway is geleerd. Zorg ervoor dat zowel de geleerde MAC-adressen als het standaard IP-adres van de gateway correct zijn geïnstalleerd als vermeldingen in de BGP-tabel.

<#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 12vpn evpn

10b3.d68b.3be3

(local mac address)

BGP routing table entry for [2][203.0.113.1:250][0][48][10B3D68B3BE3][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, Label 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, Label 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: 00000000000000000000, Label 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
```

Stap 3. Valideer het MAC-adres tussen Leaf-1 en de standaardgateway. Leaf-1 leert lokale MAC-adressen via de trunkpoort en de externe MAC-adressen 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)
--	--	---------------------	-------------------------

Stap 4. Verifieer de standaard gateway learning op de Leaf-1-switch in de L2VPN EVPN-instantie.

<#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

Stap 5. Als het VxLAN-perspectief juist is, gaat u naar DHCP om het probleem op te lossen.

Stap 6. Bevestig het DORA-proces van Leaf-1 naar de DHCP-gateway. Schakel in Leaf-01 het foutopsporingspakket voor het IP-DHCP-snuffelpakket in en controleer of de Discovery logboekvermeldingen genereert. Als er geen logboekgeneratie plaatsvindt, schakelt u pakketopnames in op de interface die verbinding maakt met de 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: Twen1/0/1, 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: DHCP_S 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
```

Stap 7. Als foutopsporing niet wordt geactiveerd, voert u een pakketopname uit voor validatie. Gebruik de opgegeven syntaxis om ingress Discovery-pakketten vast te leggen:

```
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
```



Opmerking: leg de tekenreeksen van het weergavefilter vast die zich aan de Wireshark-filtersyntaxis houden.

<#root>

Leaf-1#

monitor capture cap interface tve1/0/1 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 exist 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>

Stap 8. VxLAN-pakketinkapseling valideren via pakketopname. Pas verschillende filters toe voor deze validatie. VxLAN gebruikt UDP-poort 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 tve1/0/2 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

Gecentraliseerde gateway-verificatie

Stap 1. Valideer het Host MAC-adres dat is geleerd op BGP en de L2 EVPN-routes (deze stap weerspiegelt de initiële Leaf-verificatieprocedure).

<#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

Stap 2. Verifieer de DHCP-relaisinformatie en de DHCP-snoopconfiguratie op de gecentraliseerde gateway.

<#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
```

Stap 3. Controleer de connectiviteit met de DHCP-server en bron een ping van de VLAN 250-interface.

<#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
```

Stap 4. Voer een pakketopname uit om te valideren of de Discovery-berichten van de externe hosts de gecentraliseerde gateway bereiken.

<#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-V1250

<snip>

Stap 5. Voer een volgende pakketopname uit op de switch. Controleer de uitgang van de ontdekking en de ingang van het voorstel.

<#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

Stap 6. Als de pakketopname geen pakketten weergeeft, gaat u verder met de DHCP-foutopsporing en valideert u de pakketstatus op het platform.

<#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: 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

Stap 7. Controleer of de interfaces die verbinding maken met de DHCP-server de opgegeven opdracht bevatten (dit voorkomt het laten vallen van het DHCP-pakket).

<#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



Opmerking: de opdracht `ip dhcp snooping trust` is alleen van toepassing op Layer 2 trunk-interfaces.

probleemoplossing

VxLAN-configuratie functioneert zoals verwacht. De DHCP-serverrelais stuurt echter DHCP-antwoorden naar IP-adres 203.0.113.4. De DHCP-server was niet bereikbaar voor dit IP-adres. Dit gebrek aan connectiviteit resulteerde in unicastpakketdalingen bij de Gecentraliseerde Gateway.

Om dit probleem op te lossen, werd een nieuwe Loopback 1-interface geconfigureerd en werd een route voor het IP-adres vastgesteld om connectiviteit te bieden met dit Loopback-relaisadres.

DHCP-logs:

<#root>

DHCP-Server#

debug 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#

Gecentraliseerde Gateway: Configureer connectiviteit met de nieuwe Loopback-interface voor relay-functie.

<#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

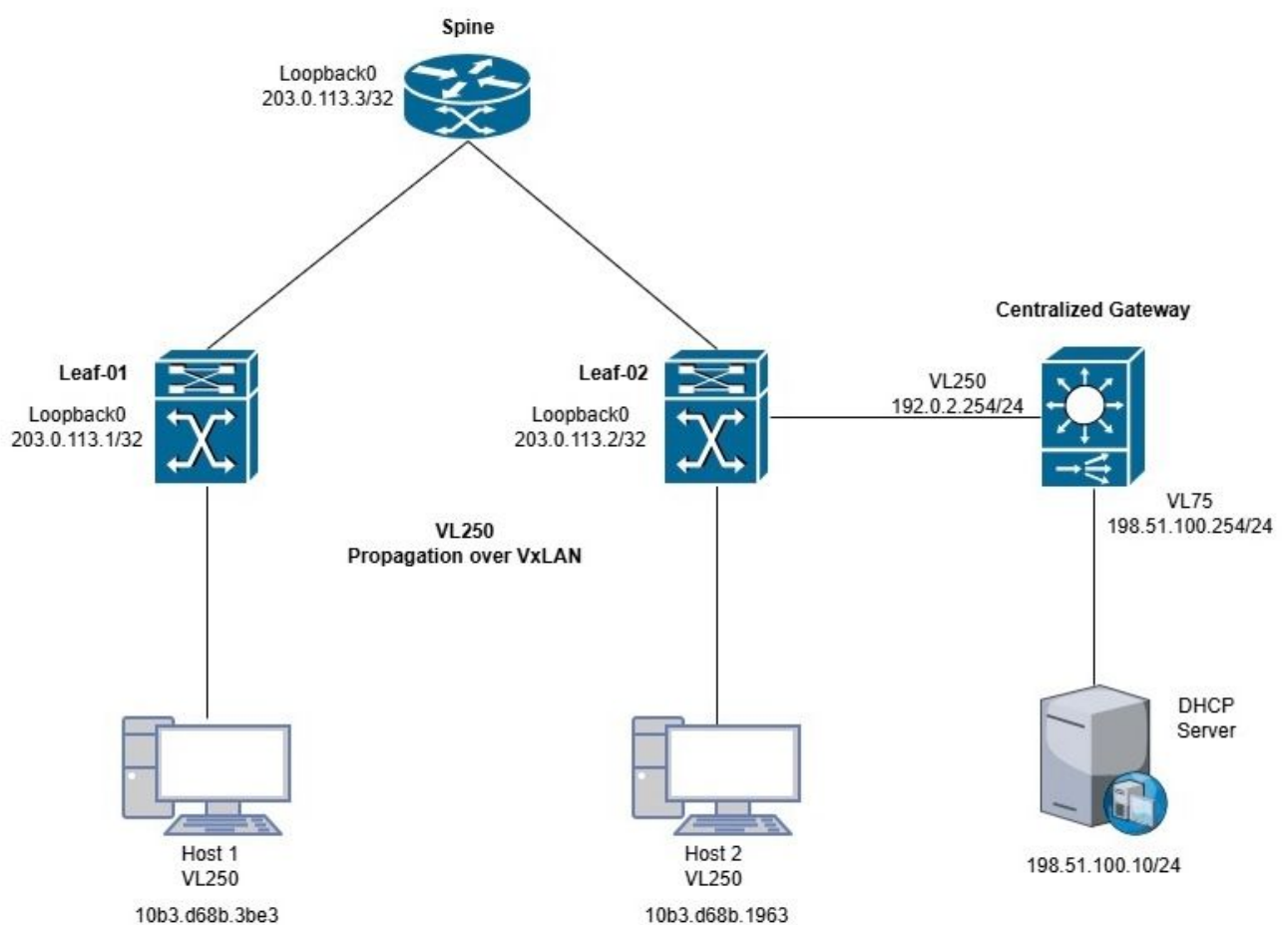
Type escape sequence to abort.

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#

Casestudy 2: IP-adres kan niet worden verkregen van de externe server (gecentraliseerde gateway buiten de verbinding)

Deze topologie gebruikt VXLAN Layer 2 voor VLAN 250. De host verkrijgt zijn IP-adres van een externe DHCP-server buiten de fabric.



Externe DHCP VxLAN-topologie

Leaf-01-verificatie

Stap 1. Controleer op Leaf-1 de juiste advertentie op de standaardgateway. Aangezien de DHCP-server zich buiten de VxLAN-verbinding bevindt, is dit een belangrijke vereiste voor de juiste

functionaliteit van de toewijzing van het IP-adres.

```
<#root>
```

```
Leaf-1#
```

```
show l2vpn evpn default-gateway
```

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

```
-----
```

Stap 2. Als de vorige uitvoer leeg is, gaat u verder met het oplossen van DHCP-problemen. Controleer of de relevante DHCP-snoopconfiguraties aanwezig zijn op de Leaf-apparaten.

```
<#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

Stap 3. Als een apparaat actief een IP-adres aanvraagt met behulp van DHCP, schakelt u de juiste foutopsporingsopdracht in om de pakketstatus op het platform te valideren.

<#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: 0.0.0.0

***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 0x0

***Dec 6 22:42:19.579: DHCP_SNOOPING: 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 flooded**

***Dec 6 22:42:19.579:**

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



Opmerking: Het laatste foutopsporingsbericht geeft aan dat het apparaat de standaardgateway voor VLAN 250 niet kon identificeren.

Leaf-02-verificatie

Aangezien Leaf-2 het actieve bladrand in de VxLAN-structuur is, is het verantwoordelijk voor het doorsturen van de informatie met betrekking tot de standaardgateway.

Stap 1. Ga verder met het valideren van de mogelijkheid van L2VPN EVPN om de standaardgateway te adverteren.

<#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
```

Stap 2. De vorige uitvoer bevestigt dat Leaf-2 geen reclame maakt voor de Default-Gateway naar de andere Leaf-1 binnen dezelfde VxLAN-structuur. Ga verder met de configuratie die nodig is om de juiste advertentie uit te voeren.

```
<#root>
```

```
Leaf-2(config)#
```

```
l2vpn evpn
```

```
Leaf-2(config-evpn)#
```

```
default-gateway advertise
```

Stap 3. Zodra de configuratie is toegevoegd, moet de EVPN-mogelijkheid van de L2VPN zijn ingeschakeld.

```
<#root>
```

```
Leaf-2#
```

```
show l2vpn evpn summary
```

```
--snip--
```

```
Advertise Default Gateway: Yes
```

Stap 4. Als deze optie is ingeschakeld, configureert u de juiste advertentie voor de standaardgateway naar de andere Leaf in de VxLAN-verbinding.

Probleemoplossing 1

L2VPN EVPN en DHCP Snooping configuratiefuncties zoals verwacht. De standaardgateway-advertentie wordt echter niet uitgevoerd. Daarom kunnen de eindapparaten die zijn aangesloten op Leaf-1 geen IP-adres ontvangen van de DHCP-server.

Om dit probleem op te lossen, moet de advertentie worden geconfigureerd.

Stap 1. Configureer een ACL, samen met een routekaart om de standaardgateway via BGP te adverteren voor de andere Leaf-apparaten op het netwerk.

```
<#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
```

Stap 2. Nadat de vorige configuratie is toegevoegd, verifieert u Leaf-1 om de juiste standaardgateway-advertentie te bekijken.

```
<#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



Opmerking: bij de VTEP-grenscontrole wordt bij het controleren van de standaardgateway een lege waarde weergegeven. Dit is te verwachten gedrag, aangezien de gecentraliseerde toegangspoort rechtstreeks is verbonden met de Border VTEP.

```
<#root>
```

```
Leaf-2#
```

```
show l2vpn evpn default-gateway
```

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

Nu tonen de Leaf-apparaten correct de standaardgateway-advertentie. Controleer of de eindapparaten het IP-adres van DHCP correct ontvangen.

Verificatie van host 1

Stap 1. Vraag op host 1 een IP-adres aan via DHCP:

```
<#root>
```

```
Host1#
```

```
show running-config interface vlan 250
```

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

```
ip address dhcp
```

```
end
```

Stap 2. Valideren of het IP-adres correct is toegewezen:

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

Stap 3. Als het IP-adres niet correct is toegewezen nadat de standaardgateway correct is geadverteerd in het Border Leaf, gaat u verder met het oplossen van DHCP-problemen.

Leaf 2-verificatie

Stap 1. Foutopsporing inschakelen voor DHCP, specifiek voor DHCP-snooping, om te observeren hoe het apparaat pakketten verwerkt wanneer deze buiten de VXLAN-structuur worden doorgestuurd.

```
<#root>
```

```
Leaf-2#
```

```
debug ip dhcp snooping packet
```

```
DHCP Snooping Packet debugging is on
```

Stap 2. Start het DHCP-proces op het hostapparaat opnieuw op en bekijk de logs:

```
<#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: DHCP_SNOOPING: bridge packet output port set is null, packet is dropped.
*Dec 12 20:11:43.902:
```

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

Stap 3. De vorige log(s) geven aan dat het pakket wordt verwijderd. Dit bericht betekent dat de DHCP-snuffelfunctie op de switch een DHCP-pakket heeft ontvangen dat niet kan worden doorgestuurd omdat de uitvoerpoort ongeldig is. Dit gebeurt meestal wanneer DHCP-snooping niet in staat is om de juiste uitgang poort voor het doorsturen van het DHCP-pakket te bepalen.

Stap 4. Om dit op te lossen, moet de interface die naar de Gateway Centralised verwijst, als vertrouwd worden geconfigureerd.

<#root>

Leaf-2(config)#

interface fortyGigabitEthernet 2/0/1

Leaf-2(config-if)#

ip dhcp snooping trust

Stap 5. Valideren of de toewijzing van het IP-adres via DHCP werkt zoals verwacht.

<#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: 0
*Dec 12 20:33:54.167: DHCP: 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.

Stap 6. Het bewijs geeft aan dat het apparaat nu de fysieke interface correct identificeert via het DHCPDISCOVER-pakket en moet worden doorgestuurd omdat de interface is gemarkeerd als vertrouwd vanuit het DHCP-snuffelperspectief. De toewijzing van het IP-adres functioneert echter nog steeds niet zoals verwacht.

Gecentraliseerde gateway-verificatie

Stap 1. Met de Border Leaf nu het doorsturen van DHCP-pakketten via de juiste interface, als de toewijzing van het IP-adres blijft mislukken, gaat u verder met de standaard DHCP-procedures voor probleemoplossing.

<#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

Stap 2. Op basis van de foutopsporingsuitvoer van de Gecentraliseerde Gateway en de resultaten van de pakketopname is extra configuratie vereist om te voorkomen dat het apparaat pakketten weggooit wanneer het veld Giaddr op nul is ingesteld.

Wanneer een DHCP-pakket wordt ontvangen met de optie Relay-informatie aanwezig, maar het IP-adres van de gateway (giaddr) is ingesteld op alle nullen, laat de DHCP-relay-agent het pakket

standaard vallen. Om dit gedrag aan te pakken, configureert u de vertrouwde opdracht ip dhcp relay information.

Stap 3. Om te controleren of het apparaat het pakket ontvangt, voert u een pakketopname uit:

```
<#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-V1250

Stap 4. Volgens de vorige pakketopname wordt het DHCP-pakket correct ontvangen door het apparaat.

Probleemoplossing 2

Stap 1. Op basis van de foutopsporingsuitvoer van de Gecentraliseerde Gateway en de resultaten van de pakketopname is extra configuratie vereist om te voorkomen dat het apparaat pakketten weggooit wanneer het veld Giaddr op nul is ingesteld.

Wanneer een DHCP-pakket wordt ontvangen met de optie Relay-informatie aanwezig, maar het IP-adres van de gateway (giaddr) is ingesteld op alle nullen, laat de DHCP-relay-agent het pakket meestal vallen.

Om dit gedrag aan te pakken, configureert u de vertrouwde opdracht voor informatie over IP-DHCP-relay.

```
<#root>
```

```
Centralized-Gateway(config)#
```

```
interface vlan 250
```

```
Centralized-Gateway(config-if)
```

```
#ip dhcp relay information trusted
```

Stap 2. Ga door met verificatie en vraag een IP-adres aan bij host 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: 0

*Dec 12 21:36:03.243: DHCP_S 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 (FortyGigabitEthernet

<snip>

*Dec 12 21:36:03.255:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPPOFFER

, 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 0

*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 r

*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: 0

*Dec 12 21:36:03.401: DHCP_S 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 (FortyGigabitEthernet2/0/1)
<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 0x0

*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_REMOTE_ID

*Dec 12 21:36:03.413: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan 250

*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 packet

*Dec 12 21:36:03.413: DHCP_SNOOPING: client address lookup failed to locate client interface, retry lookup

*Dec 12 21:36:03.413: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10b3.d68b.1963

*Dec 12 21:36:03.413: DHCP_SNOOPING: can't find client's destination port, packet is assumed to be not from local

*Dec 12 21:36:03.413: DHCP_SNOOPING: client address lookup failed to locate client interface, retry lookup

*Dec 12 21:36:03.413: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10b3.d68b.1963

*Dec 12 21:36:03.413:

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

Stap 3. Het IP-adres is correct toegewezen en er wordt voorgesteld om hetzelfde gedrag te valideren vanuit het perspectief van host 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 (FortyGigabitEthernet2/0/2)

<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: DHCP_S 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 flow
*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 (FortyGigabitEthernet2/0/1)
<snip>
*Dec 12 22:08:15.440:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPPOFFER

, 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_CID_VXLAN_MOD_PORT_INTF
*Dec 12 22:08:15.440: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan 250
*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_intf
*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_intf
*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: DHCP_S 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 flow
*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 (FortyGigabitEthernet2/0/2)
<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 0x0

*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>

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.