

排除EVPN VxLAN Cat9000上的外部DHCP故障

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[案例研究 1：無法從外部伺服器（交換矩陣內的集中網關）獲取IP地址](#)

[Leaf-01驗證](#)

[集中式網關驗證](#)

[問題解決方案](#)

[案例研究 2：無法從外部伺服器（交換矩陣外部的集中網關）獲取IP地址](#)

[Leaf-01驗證](#)

[Leaf-02驗證](#)

[問題解決方案1](#)

[主機1驗證](#)

[枝葉2驗證](#)

[集中式網關驗證](#)

[問題解決方案2](#)

簡介

本文描述如何在Cat9000平台上的外部EVPN VxLAN環境中排除DHCP問題。

必要條件

需求

思科建議您瞭解以下主題：

- Cat9000平台上的虛擬可擴充LAN
- VxLAN環境中的發現主機配置協定
- 邊界閘道通訊協定(BGP)

有關這些主題的詳細資訊，請參閱：

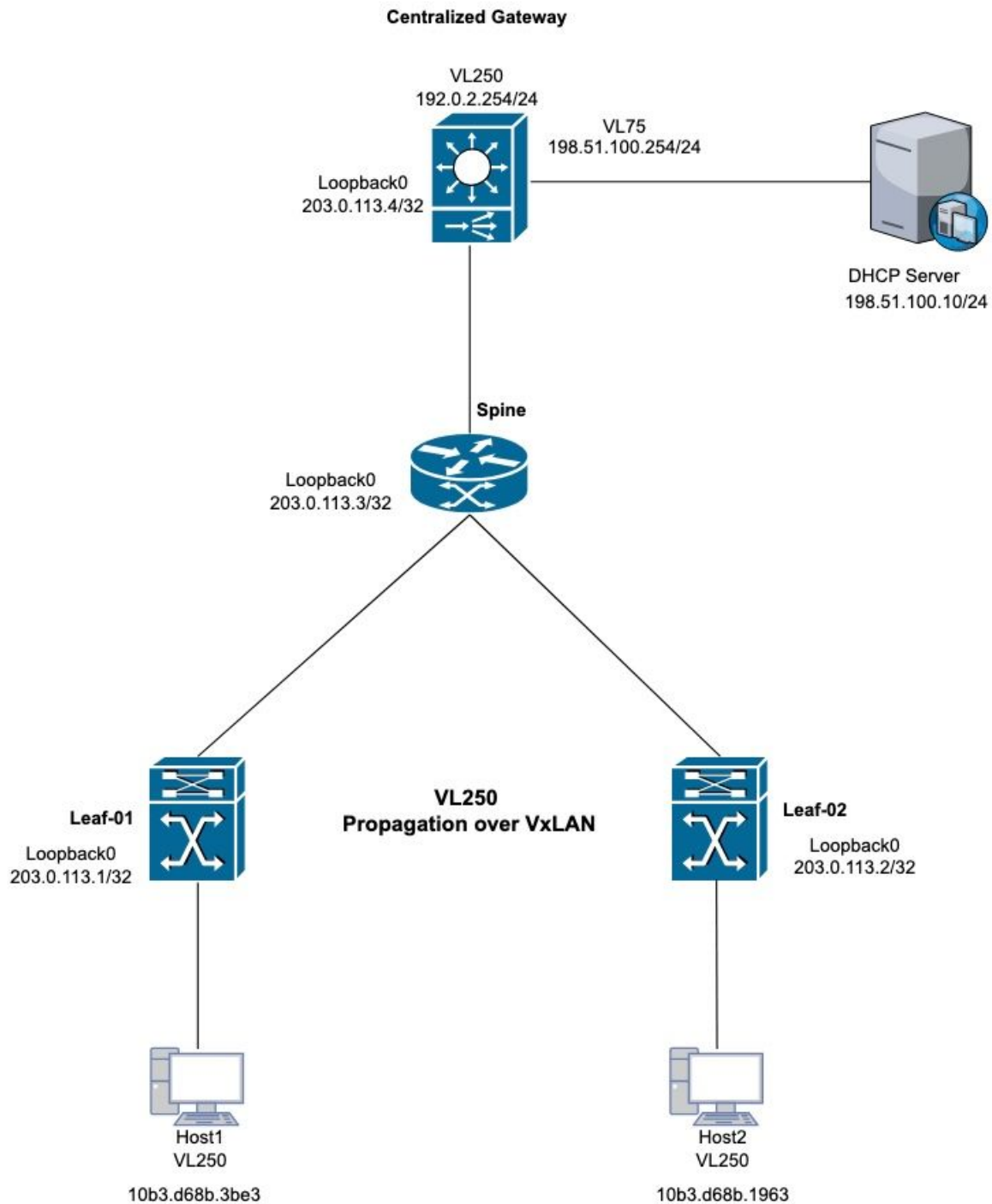
- [章節：在BGP EVPN VXLAN光纖Cat9300中配置DHCP中繼](#)
- [章節：在BGP EVPN VXLAN光纖Cat9400中配置DHCP中繼](#)
- [章節：在BGP EVPN VXLAN光纖Cat9500中配置DHCP中繼](#)
- [章節：在BGP EVPN VXLAN光纖Cat9600中配置DHCP中繼](#)

採用元件

本檔案中的資訊是根據Cisco IOS XE軟體。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

網路圖表



DHCP VxLAN拓撲

案例研究 1：無法從外部伺服器（交換矩陣內的集中網關）獲取 IP 地址

此拓撲將VxLAN第2層用於VLAN 250。主機需要來自外部DHCP伺服器的IP地址。

Leaf-01驗證

步驟1.在Leaf-1上，驗證本地主機的MAC地址學習。

步驟2.此外，確認已獲取預設網關MAC地址。確保已獲取的MAC地址和預設網關IP地址都正確安裝為BGP表中的條目。

```
<#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
```

步驟3.驗證枝葉1和預設網關之間的MAC地址學習。枝葉1通過中繼埠獲取本地MAC地址，通過BGP獲取遠端MAC地址。

<#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)
--	---------	-------------	-------------------------

步驟4.檢驗L2VPN EVPN例項中枝葉-1交換機上的預設網關學習情況。

<#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

步驟5.如果VxLAN視角正確，請繼續到DHCP進行故障排除。

步驟6.確認從Leaf-1到DHCP網關的DORA進程。在Leaf-01上，啟用debug ip dhcp snooping packet並驗證Discovery是否生成日誌條目。如果未生成日誌，請在連線到PC的介面上啟用資料包捕獲。

```
<#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 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
```

步驟7.如果未觸發調試，請執行資料包捕獲以進行驗證。使用指定的語法捕獲入口發現資料包：

```
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
```



附註：捕獲遵循Wireshark過濾器語法的顯示過濾器字串。

<#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 default)

.... ..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>

步驟8.通過資料包捕獲驗證VxLAN資料包封裝。為此驗證應用各種篩選器。VxLAN使用UDP埠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
```

集中式網關驗證

步驟1.驗證在BGP和L2 EVPN路由上獲知的主機MAC地址 (此步驟映象初始枝葉驗證過程)。

<#root>

Centralized-Gateway#

show bgp 12vpn 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

步驟2.檢驗集中網關上的DHCP中繼資訊和DHCP監聽配置。

<#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
```

步驟3.檢驗與DHCP伺服器的連通性並從VLAN 250介面發出ping命令。

<#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
```

步驟4.執行資料包捕獲，以驗證來自遠端主機的發現消息是否到達集中網關。

<#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>

步驟5.在交換器上執行後續封包擷取。驗證Discovery egress和Offer ingress。

<#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

步驟6.如果資料包捕獲未顯示資料包，請繼續DHCP調試並驗證平台上的資料包狀態。

<#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 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

步驟7.檢驗連線到DHCP伺服器的介面是否包含指定的命令（這可防止DHCP資料包丟棄）。

```
<#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
```



附註：ip dhcp snooping trust命令僅適用於第2層中繼介面。

問題解決方案

VxLAN配置按預期運行。但是，DHCP伺服器中繼會向IP地址203.0.113.4傳送DHCP應答。DHCP伺服器無法訪問此IP地址。缺乏連線導致集中網關上的單播資料包丟棄。

為了解決此問題，配置了一個新的Loopback 1介面，並為IP地址建立了路由以提供與此環回中繼地址的連線。

DHCP日誌：

```
<#root>
```

```
DHCP-Server#d
```

```
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 Interface 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#

集中網關：為中繼功能配置到新環回介面的連線。

<#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
```

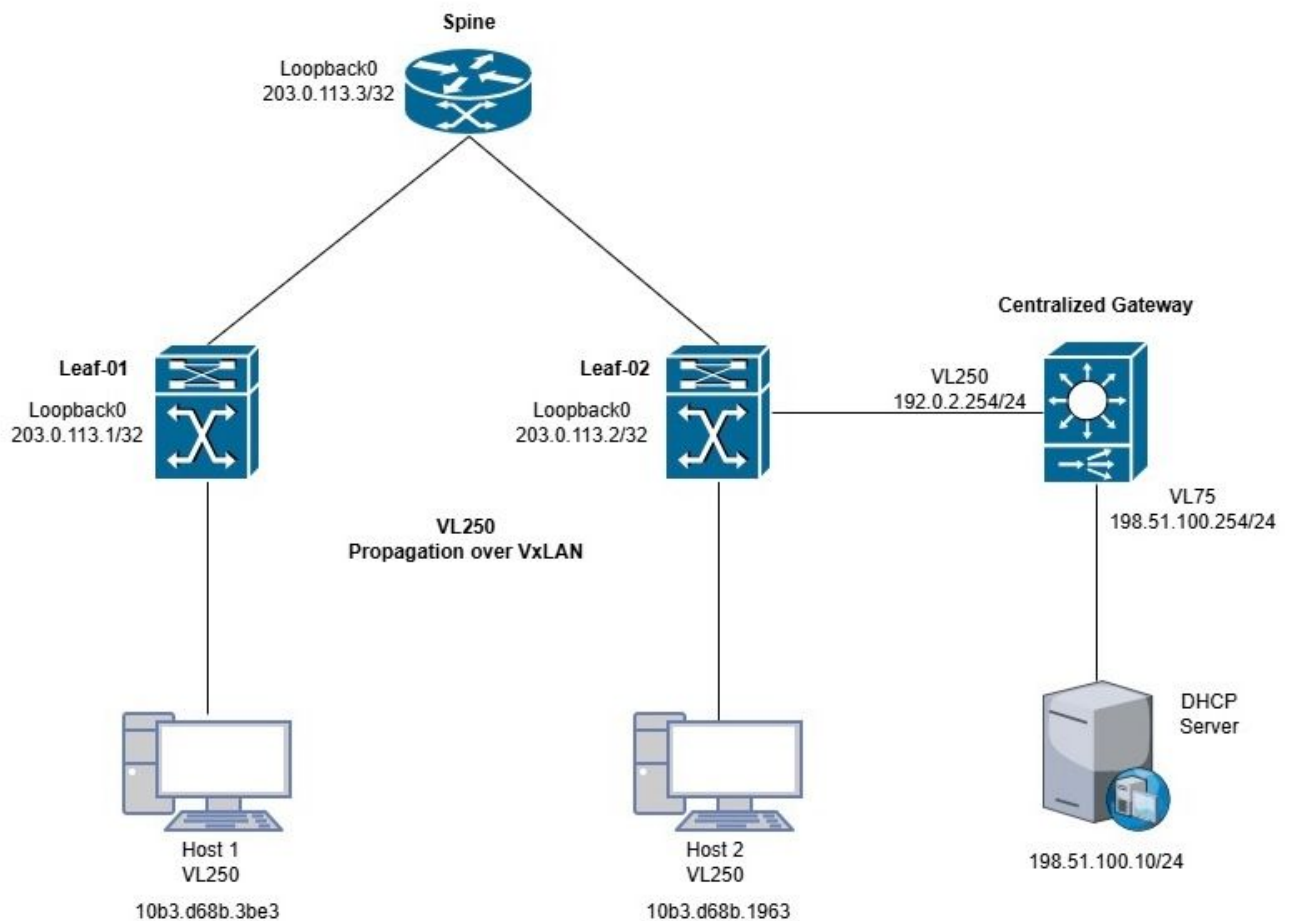
```
Type escape sequence to abort.
```

```
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#
```

案例研究 2：無法從外部伺服器（交換矩陣外部的集中網關）獲取 IP 地址

此拓撲將 VXLAN 第 2 層用於 VLAN 250。主機從位於交換矩陣外部的內部 DHCP 伺服器獲取其 IP 地址。



外部DHCP VxLAN拓撲

Leaf-01驗證

步驟1.在Leaf-1上，驗證預設網關上的正確通告。由於DHCP伺服器位於VxLAN交換矩陣之外，因此這是IP地址分配功能正常的關鍵要求。

```
<#root>
```

```
Leaf-1#
```

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

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

```
-----
```

步驟2.如果前面的輸出為空，請繼續DHCP故障排除。驗證枝葉裝置上是否存在相關的DHCP監聽配

置。

<#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
```

步驟3.如果裝置正在使用DHCP主動請求IP地址，請啟用適當的調試命令以驗證平台上的資料包狀態。

```
<#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: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flood
```

```
*Dec 6 22:42:19.579: DHCP_SNOOPING: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flood
```

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

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



附註：最終調試消息表明裝置無法識別VLAN 250的預設網關。

Leaf-02驗證

由於Leaf-2是VxLAN交換矩陣內的活動邊界枝葉，因此它負責轉發與預設網關相關的資訊。

步驟1.繼續驗證L2VPN EVPN通告預設網關的功能。

<#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

步驟2.上一個輸出驗證Leaf-2未向同一VxLAN交換矩陣中的其他Leaf-1通告預設網關。繼續執行執行正確通告所需的配置。

<#root>

Leaf-2(config)#

```
l2vpn evpn
```

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

```
default-gateway advertise
```

步驟3.新增配置後，必須啟用L2VPN EVPN功能。

```
<#root>
```

```
Leaf-2#
```

```
show l2vpn evpn summary
```

```
--snip--
```

```
Advertise Default Gateway: Yes
```

步驟4.啟用後，為到VxLAN交換矩陣內其他枝葉的預設網關配置足夠的通告。

問題解決方案1

L2VPN EVPN和DHCP監聽配置按預期運行。但是，未執行預設網關通告。因此，連線到枝葉1的終端裝置無法從DHCP伺服器接收IP地址。

要解決此問題，必須配置通告。

步驟1.配置ACL和路由對映，以便通過BGP將預設網關通告給網路上的其他枝葉裝置。

```
<#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
```

步驟2.新增先前的配置後，驗證Leaf-1以檢視正確的預設網關通告。

```
<#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



附註：在邊界VTEP上，驗證預設網關顯示空值。這是預期行為，因為集中網關直接連線到邊界VTEP。

```
<#root>
```

```
Leaf-2#
```

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

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

```
-----
```

現在，枝葉裝置正確顯示了預設網關通告。驗證終端裝置是否正確從DHCP接收IP地址。

主機1驗證

步驟1.在Host 1上，通過DHCP請求IP地址：

```
<#root>
```

```
Host1#
```

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

```
Building configuration...
```

```
Current configuration : 42 bytes
```

```
!
```

```
interface Vlan250
```

```
ip address dhcp
```

```
end
```

步驟2.驗證是否已正確分配IP地址：

```
Host1#show ip interface brief | include DHCP
```

```
Vlan250    unassigned    YES        DHCP        up        up
```

步驟3.如果在邊界枝葉正確通告預設網關後未正確分配IP地址，請繼續DHCP故障排除。

枝葉2驗證

步驟1.為DHCP啟用調試，特別是為DHCP監聽啟用調試，以觀察裝置在VXLAN交換矩陣外部轉發資料包時如何處理資料包。

```
<#root>
```

```
Leaf-2#
```

```
debug ip dhcp snooping packet
```

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

步驟2.在主機裝置上重新啟動DHCP進程並檢視日誌：

```
<#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: 0.0.0.0
```

```
*Dec 12 20:11:43.902: DHCP 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.
```

步驟3.上一個日誌指示資料包被丟棄。此消息表示交換機上的DHCP監聽功能收到的DHCP資料包因輸出埠無效而無法轉發。當DHCP監聽無法確定用於轉發DHCP資料包的適當出口埠時，通常會發生這種情況。

步驟4.要解決此問題，必須將指向集中式網關的介面配置為受信任。

```
<#root>
```

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

```
interface fortyGigabitEthernet 2/0/1
```

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

```
ip dhcp snooping trust
```

步驟5.驗證通過DHCP分配的IP地址現在是否按預期工作。

```
<#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: DHCP PS 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.
```

步驟6.證據顯示裝置現在通過DHCPDISCOVER資料包正確識別物理介面，並且必須轉發，因為從DHCP監聽的角度該介面已標籤為可信。但是，IP地址分配仍無法按預期運行。

集中式網關驗證

步驟1.現在，Border Leaf通過適當的介面轉發DHCP資料包，如果IP地址分配繼續失敗，請繼續執行標準DHCP故障排除過程。

```
<#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

步驟2.根據集中式網關的調試輸出和資料包捕獲結果，需要額外的配置來防止裝置在giaddr欄位設定為零時丟棄資料包。

當接收到帶有中繼資訊選項的DHCP資料包時，但網關IP地址(giaddr)設定為全零，預設情況下，DHCP中繼代理會丟棄該資料包。要解決此行為，請配置ip dhcp relay information trusted命令。

步驟3.要驗證裝置是否收到資料包，請執行資料包捕獲：

<#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

步驟4.根據前面捕獲的資料包，裝置正確接收了DHCP資料包。

問題解決方案2

步驟1.根據集中式網關的調試輸出和資料包捕獲結果，需要額外的配置以防止裝置在將giaddr欄位設定為零時丟棄資料包。

當接收到帶有中繼資訊選項的DHCP資料包，但網關IP地址(giaddr)設定為全零時，DHCP中繼代理通常會丟棄該資料包。

要解決此行為，請配置ip dhcp relay information trusted命令。

<#root>

Centralized-Gateway(config)#

interface vlan 250

Centralized-Gateway(config-if)

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

步驟2.繼續從主機1請求IP地址的驗證。

```
<#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_SNOOPING: bridge packet send packet to port: FortyGigabitEthernet2/0/1
```

```
*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 (FortyGigabitEthernet2/0/1)
```

```
<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 sa: 0
```

```
*Dec 12 21:36:03.255: DHCP_SNOOPING: binary dump of option 82, length: 26 data:
```

```
0x52 0x18 0x01 0xC 0x01 0xA 0x00 0x8 0x00 0x0 0x28 0xA 0x01 0x01 0x00 0x0 0x2 0x8 0x00 0x6 0x4C 0x3C 0xEB 0x00
```

```
*Dec 12 21:36:03.256: DHCP_SNOOPING: binary dump of extracted circuit id, length: 14 data:
```

```
0x01 0xC 0x01 0xA 0x00 0x8 0x00 0x0 0x28 0xA 0x01 0x01 0x00 0x0
```

```
*Dec 12 21:36:03.256: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
```

```
0x02 0x8 0x00 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_RID_VXLAN_MOD_PORT_INTF
```

```
*Dec 12 21:36:03.256: dhcp_snooping_platform_is_local_dhcp_packet: VXLAN-MOD-PORT opt82 vni 10250, vlan 250
```

```
*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 packet
```

```
*Dec 12 21:36:03.256: DHCP_SNOOPING: client address lookup failed to locate client interface, retry lookup
```

```
*Dec 12 21:36:03.256: DHCP_SNOOPING: lookup packet destination port failed to get mat entry for mac: 10b3.d68b.3be3
```

```
*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: DHCP_SNOOPING: received new DHCP packet from input interface (FortyGigabitEthernet

<snip>
*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 (FortyGigabitEthernet

<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

步驟3.已正確分配IP地址，建議從主機2的角度驗證相同行為。

<#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 (FortyGigabitEthernet

<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 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 (FortyGigabitEthernet
<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: 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 (FortyGigabitEthernet
<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>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。