瞭解通過第3層跳的資料包的DHCP監聽

目錄

簡介

本文檔介紹當資料包通過任何L3裝置並且資料包是否封裝在L3報頭中時，DHCP監聽的互動和行為。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS® XE在配置和操作命令方面的熟練程度。

- 熟悉Cisco Catalyst 9000系列交換機硬體和架構。
- 深入瞭解DHCP協定操作和DHCP監聽機制。
- 對DHCP選項82和中繼代理角色的概念性理解。
- 基本的路由協定知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

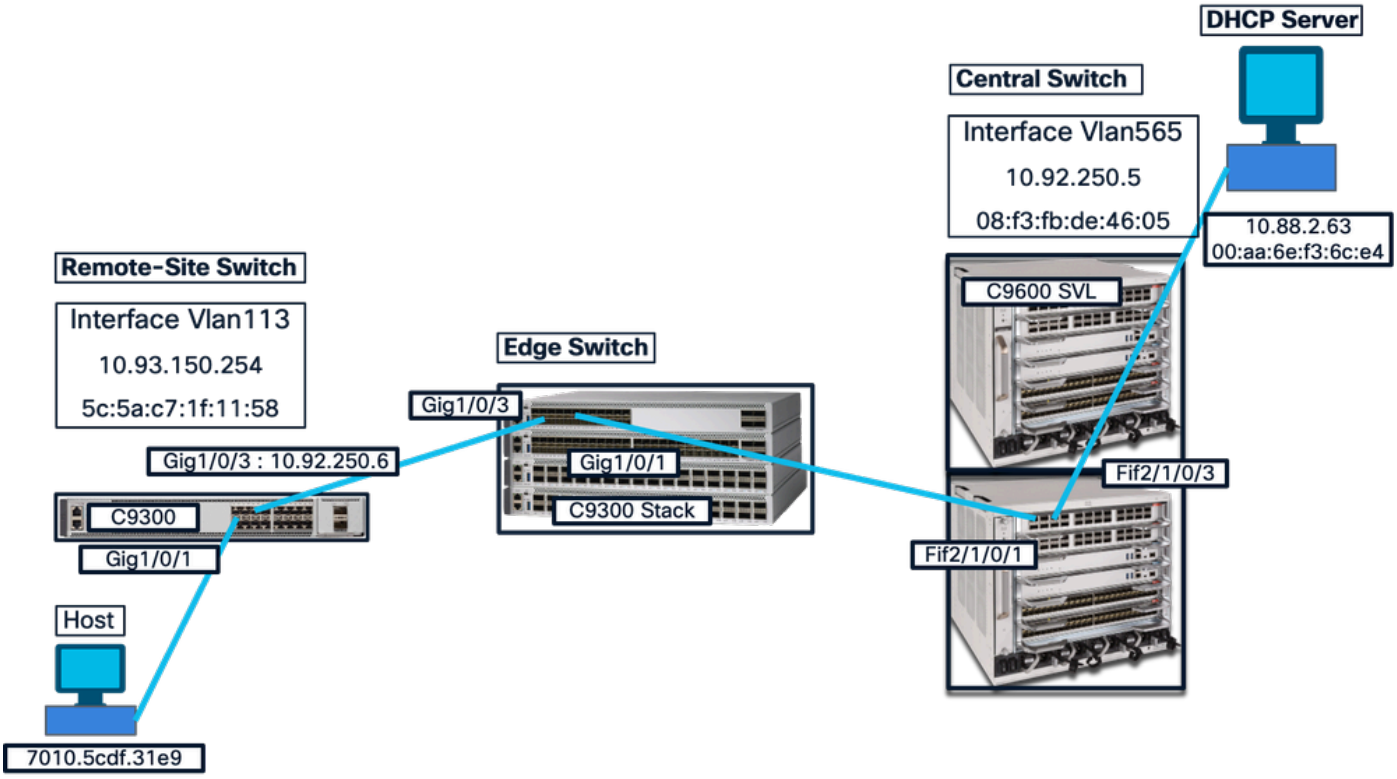
- 核心/分佈層交換機：Cisco Catalyst 9600X系列
- 接入交換機：Cisco Catalyst 9300 系列
- DHCP客戶端：終端主機裝置
- DHCP伺服器：集中式網路服務提供商

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。

背景資訊

本檔案將研究DHCP窺探如何在DHCP封包經過第3層躍點時檢查並擷取這些封包。通過實際配置示例和相關資料包捕獲的分析，它演示了Cisco Catalyst 9000系列網路環境中第3層跳上的DHCP監聽的互動。

網路圖表



拓撲

無效情境

首先，概述在第3層跳上丟棄DHCP發現資料包的場景，尤其是在中央交換機上。現在，從DHCP客戶端逐跳分析資料包旅程。

遠端站點交換器封包處理

MAC地址為7010.5cdf.31e9的主機傳輸DHCP發現資料包，該資料包到達遠端站點交換機上的介面GigabitEthernet1/0/1。

遠端站點配置

<#root>

!
!

Remote-Site#show run int vlan 113

```
Building configuration...

Current configuration : 170 bytes
!
interface Vlan113
ip address 10.93.150.254 255.255.255.0
ip helper-address 10.88.2.63
no ip redirects
no ip proxy-arp
end
!
!
!
```

Host Access Port

Remote-Site#show run int gig1/0/1

```
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet1/0/1
switchport access vlan 113
switchport mode access
end
!
!
!
```

Uplink Port

Remote-Site#show run int gig1/0/3

```
Building configuration...

Current configuration : 121 bytes
!
interface GigabitEthernet1/0/3
no switchport
ip address 10.92.250.6 255.255.255.252
end
!
!
```

Remote-Site#show run | sec dhcp

```
ip dhcp snooping vlan 1-999
no ip dhcp snooping information option
ip dhcp snooping
```

```
!
!
```

Remote-Site#show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID     Local Intrfce    Holdtme      Capability    Platform       Port ID

Edge-Switch   Gig 1/0/3        153          R S I         C9300-48H      Gig 1/0/3
!
!
```

Remote-Site#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.92.250.5 Gi1/0/3 14 00:04:40 1 100 0 20
!
!
```

Remote-Site#show ip route 10.88.2.63

```
Routing entry for 10.88.2.0/24
 Known via "eigrp 100", distance 90, metric 3072, precedence routine (0), type internal
 Redistributing via eigrp 100
 Last update from 10.92.250.5 on GigabitEthernet1/0/3, 00:05:15 ago
 Routing Descriptor Blocks:
 * 10.92.250.5, from 10.92.250.5, 00:05:15 ago, via GigabitEthernet1/0/3
     Route metric is 3072, traffic share count is 1
     Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
     Reliability 255/255, minimum MTU 1500 bytes
     Loading 1/255, Hops 1
!
!
```

遠端站點交換器輸入

進入遠端站點交換機的廣播DHCP發現資料包。

<#root>

```
!
!
```

Remote-Site#show monitor capture tac parameter

```
     monitor capture tac control-plane BOTH
     monitor capture tac interface GigabitEthernet1/0/1 BOTH
     monitor capture tac match any
     monitor capture tac file location flash:pcport.pcap
!
!
```

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 667 detailed

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

Frame 667: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), 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: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
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: 331
Identification: 0x0405 (1029)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
```

Protocol: UDP (17)

```
Header checksum: 0xb69d [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
```

Source Port: 68
Destination Port: 67
Length: 311
Checksum: 0x33de [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x000026ee
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: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

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: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!

```
!
```

遠端站點交換器輸出

從遠端站點交換機到邊緣交換機的中繼單播DHCP發現資料包。

<#root>

```
!
!

Remote-Site#show monitor capture tac1 parameter


 monitor capture tac1 control-plane BOTH
 monitor capture tac1 interface GigabitEthernet1/0/3 BOTH
 monitor capture tac1 match any
 monitor capture tac1 file location flash:remote_edge.pcap
!
!

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 669 detailed


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

Frame 669: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)


Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63


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: 331
Identification: 0x001c (28)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 4]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x000026ee
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: 10.93.150.254


Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
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: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
```

```
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

附註：資料包具有「Relay agent IP address:10.93.150.254」，但由於配置了「no ip dhcp snooping information option」作為DHCP部分的一部分，因此它沒有DHCP選項82。

邊緣交換器封包處理

對於DHCP流量而言，邊緣交換機是一種L2交換機，僅用於在中央/核心交換機和遠端站點交換機之間分發資料包。信任所有DHCP資料包。

邊緣交換機配置

<#root>

```
!
!
```

Edge-Switch#show run int gig1/0/3

```
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/0/3
switchport access vlan 565
ip flow monitor IPv4_NETFLOW input
ip dhcp snooping trust
end
!
!
```

Edge-Switch#show run int gig1/0/1

```
Building configuration...

Current configuration : 119 bytes
!
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
switchport mode trunk
ip dhcp snooping trust
end
!
!
```

Edge-Switch#show run | sec dhcp

```
ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!
```

Edge-Switch#show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce   Holdtme   Capability   Platform     Port ID
Remote-Site      Gig 1/0/3       153       R S I        C9300L-48    Gig 1/0/3
Central-Switch   Gig 1/0/1       170       R S I        C9606R       Fif 2/1/0/1
!
!
```

邊緣交換器輸入

從遠端站點交換機傳出的資料包正按原樣到達邊緣交換機。

邊緣交換器輸出

由於這是封包的第2層躍點，因此它會在進入下一個躍點時退出交換器，但不會發生任何變化。邊緣交換器將封包轉送到中央交換器，而沒有在封包中看到任何修改。

Edge Switch Egress Packet是中央交換機入口資料包。

<#root>

```
!
!
```

Edge-Switch#show monitor capture tac parameters

```
 monitor capture tac control-plane BOTH
 monitor capture tac interface GigabitEthernet1/0/1 BOTH
 monitor capture tac match any
 monitor capture tac file location flash:edge_central.pcap
!
!
```

Edge-Switch#show monitor capture file flash:edge_central.pcap packet-number 25597 detail

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

Frame 25597: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface /tmp/epc_ws/wif
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]
```

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)

```
Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63

```
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: 331
Identification: 0x001c (28)
Flags: 0x0000
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: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
```

Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[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: 1
Transaction ID: 0x000026ee
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: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
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: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier

```
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

中央交換器封包處理

中央交換機配置

<#root>

```
!
!

Central-Switch#show cdp neighbors



Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce   Holdtme   Capability   Platform    Port ID

Edge-Switch    Fif 2/1/0/1     177       R S I        C9300-48H   Gig 1/0/1
!
!

Central-Switch#show run int fif2/1/0/1



Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
switchport mode trunk
end
!
!

Central-Switch#show run int fif2/1/0/3



Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
```

```
ip address 10.88.2.254 255.255.255.0
end
!
!

interface Vlan565



ip address 10.92.250.5 255.255.255.252
!
!
!

Central-Switch#show run | sec dhcp



ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!

Central-Switch#show ip eigrp neighbors



EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0

10.92.250.6

 Vl565 11 00:10:32 3 100 0 19
~
~
!
!

router eigrp 100



  network 10.0.0.0
  network 10.88.0.0 0.0.255.255
  passive-interface default
  no passive-interface Vlan565
  eigrp router-id 10.255.255.254
!
!
```

中央交換器輸入

如前所述，邊緣交換機出口資料包是中央交換機入口資料包。

當封包到達介面fif 2/1/0/1時，將觀察此記錄。

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or optio
```

介面Fif 2/1/0/1被配置為DHCP監聽的不可信埠。

第3層中繼DHCP發現資料包通過此埠進入。雖然封包是在第3層進行中繼和封裝，但DHCP窺探仍會在第2層連線埠上檢查該封包。由於此埠不受信任，並且資料包包含不帶選項82的網關IP（中繼代理）地址，因此DHCP監聽將丟棄此不受信任埠上的資料包。這是預期行為，也是設計行為。

附註：在許多情況下，可以看到DHCP發現由於DHCP監聽而在傳輸過程中被丟棄。

中央交換器輸出

在這種情況下，中央交換機將丟棄DHCP發現資料包，並且不會出現任何MAC地址為70:10:5c:df:31:e9的主機從介面Fif 2/1/0/3發起的DHCP發現資料包。

如何解決問題？

1.在DHCP客戶端的第一跳上啟用選項82。
在當前示例中，在遠端交換機上配置ip dhcp snooping information option命令。

2.必須在從DHCP客戶端到DHCP伺服器的整個DHCP路徑中啟用DHCP監聽信任。

在當前示例中，在中央交換機的介面fif2/1/0/1上配置ip dhcp snooping trust命令。

<#root>

```
Central-Switch#show run int fif2/1/0/1

Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
```

```
switchport mode trunk

ip dhcp snooping trust


end
```

在這些更改之後，Discover資料包將從中央交換機開始離開，到DHCP伺服器。

<#root>

```
Frame 9: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0



~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)



Destination: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63



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: 331
Identification: 0x02ff (767)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 254
Protocol: UDP (17)
Header checksum: 0x0ab1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
```

User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0x061b [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: 1
Transaction ID: 0x00000563
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: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

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: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8

```
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

Discover將到達DHCP伺服器，DHCP伺服器將回覆DHCP提供。

DHCP提供資料包：

<#root>

Frame 128: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)

```
Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

```
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: 339
Identification: 0x0006 (6)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa2 [validation disabled]
[Header checksum status: Unverified]
```

Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x9c4c [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
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: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

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

Option: (53) DHCP Message Type (Offer)

Length: 1
DHCP: Offer (2)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (58) Renewal Time Value

```
Length: 4
Renewal Time Value: (36559s) 10 hours, 9 minutes, 19 seconds
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (63973s) 17 hours, 46 minutes, 13 seconds
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255
```

DHCP伺服器回覆的提供資料包將命中CORE/Central交換機的介面fif2/1/0/3。

<#root>

Central-Switch#show run int fif2/1/0/3

```
Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
ip address 10.88.2.254 255.255.255.0
end
```

在這裡，沒有來自DHCP監聽端的信任，並且OFFER正在進入，那麼Offer為什麼沒有丟棄到不受信任的埠上？

如您所知，在啟用DHCP監聽的網路中，埠被分類為可信或不可信。

受信任的埠連線到合法的DHCP伺服器或其他受信任的交換機。所有DHCP消息都允許在其上。
不可信埠通常連線到終端使用者裝置（客戶端）。 它們受到限制以防止「DHCP欺騙」或「惡意DHCP伺服器」攻擊。
DHCP提供和DHCP ACK資料包被視為「伺服器端」消息。根據安全規則，這些消息只能來自合法伺服器。
當DHCP中繼代理或任何L3路由器/交換機在配置為不可信的L2埠上收到DHCP提供時，DHCP監聽機制會將此行為標識為安全違規。它假設欺詐DHCP伺服器嘗試向網路上的客戶端提供未經授權的IP地址。
雖然封包是單點傳播（特別針對中繼代理），但實體或邏輯連線埠的信任狀態優先。無論封包是廣播還是單點傳播，都會在連線埠層級執行安全檢查。

由於埠不受信任，系統將阻止DHCP提供，以保護網路免受來自未授權源的潛在惡意或錯誤配置資料的侵害。

第3層埠（路由介面）在第3層運行。因為它是路由介面，所以它不遵循應用於交換機埠的第2層DHCP監聽信任/不信任規則。
客戶端傳送廣播請求。中繼代理（L3裝置）會攔截該請求並將單播請求傳送到DHCP伺服器。
DHCP伺服器將單播DHCP提供傳送回中繼代理的IP地址（特別是轉發器或網關IP地址）。
當資料包到達中繼代理的L3埠或資料包路徑中的任何L3跳時，裝置會接受資料包作為合法路由流量。
與先前的場景（L2不受信任埠）不同（交換機正在查詢來自面向客戶端的埠的「伺服器端」消息），L3埠充當伺服器響應的預定目標或合法L3躍點。
如果L3埠丟棄了單播DHCP提供，DHCP中繼機制將永遠無法工作，因為伺服器將永遠無法與中繼代理通訊。

最後， Offer資料包將經過直到到達客戶端。

主機/客戶端將使用DHCP請求進行回覆。

<#root>

Frame 20: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0

~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), 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: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
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: 349
Identification: 0x3be5 (15333)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x7eab [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 329
Checksum: 0xed98 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
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: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

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

Option: (53) DHCP Message Type (Request)

Length: 1
DHCP: Request (3)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0

```
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63



Option: (50) Requested IP Address
Length: 4

Requested IP Address: 10.93.150.11



Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

DHCP伺服器將最終確認IP地址分配。

<#root>

```
Frame 25: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0



~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)



Destination: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
```

Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

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: 339
Identification: 0x0007 (7)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x1e0f [unverified]
[Checksum Status: Unverified]
[Stream index: 2]

Bootstrap Protocol (ACK)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
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: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

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

Option: (53) DHCP Message Type (ACK)

Length: 1
DHCP: ACK (5)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (86400s) 1 day
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (43200s) 12 hours
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (75600s) 21 hours
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255

DORA完成，主機將成功接收IP地址。

摘要

請參閱下表以了解封包轉送案例。

連接埠類型	信任狀態	中繼資料包型別	結果	原因

L2埠	不受信任	單播DHCP提供/確認	Dropped	DHCP監聽防止伺服器消息出現在不可信的L2埠上。
L3埠	不適用（路由）	單播DHCP提供/確認	已接受	路由埠是中繼代理通訊的預定節點。
L2埠	受信任	使用選項82的單播DHCP發現	已接受	受信任埠允許所有DHCP訊號。
L2埠	不受信任	使用選項82的單播DHCP發現	已接受	具有中繼代理IP地址和選項82的資料包是合法的。
L2埠	受信任	不帶選項的單播DHCP發現82	已接受	受信任埠允許所有DHCP訊號。
L2埠	不受信任	不帶選項的單播DHCP發現82	Dropped	具有中繼代理IP地址且沒有選項82的資料包是欺詐資料包。

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）。