

了解通过第3层跳的数据包的DHCP监听

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[非工作场景](#)

[远程站点交换机数据包处理](#)

[远程站点配置](#)

[远程站点交换机入口](#)

[远程站点交换机出口](#)

[边缘交换机数据包处理](#)

[边缘交换机配置](#)

[边缘交换机入口](#)

[边缘交换机出口](#)

[中央交换机数据包处理](#)

[中央交换机配置](#)

[中央交换机入口](#)

[中央交换机出口](#)

[如何解决问题？](#)

[摘要](#)

简介

本文档介绍当数据包通过任何L3设备以及数据包是否封装在L3报头中时，DHCP监听的交互和行为。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco IOS® XE在配置和操作命令方面的熟练程度。

- 熟悉Cisco Catalyst 9000系列交换机硬件和架构。
- 深入了解DHCP协议操作和DHCP监听机制。
- 对DHCP选项82和中继代理的作用的概念性理解。
- 基本的路由协议知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

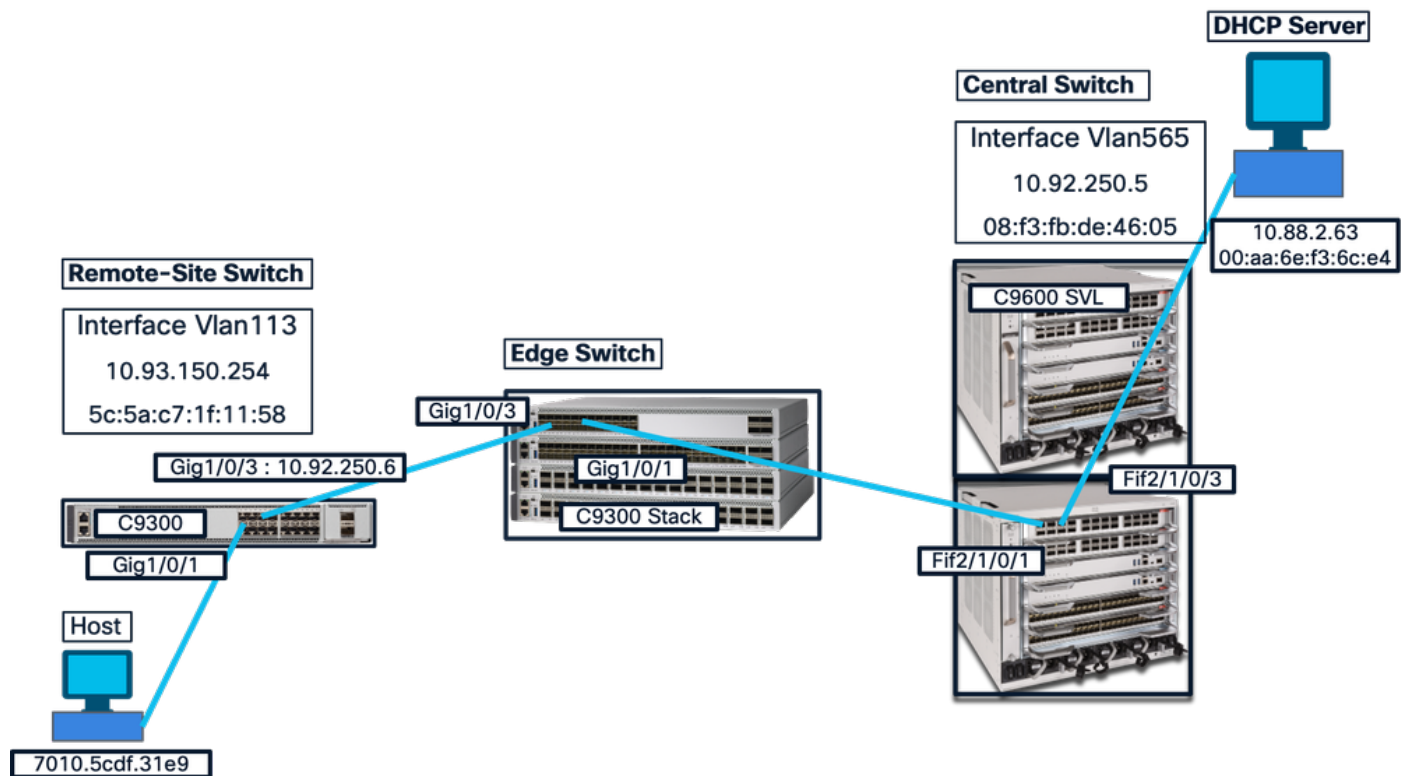
- 核心/分布层交换机：Cisco Catalyst 9600X系列
- 接入层交换机: Cisco Catalyst 9300 系列
- DHCP 客户端: 终端主机设备
- DHCP 服务器: 集中式网络服务提供商

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文检查DHCP监听如何在DHCP数据包经过第3层跳时检查并拦截它们。通过实际配置示例和相关数据包捕获的分析，它演示了DHCP监听在Cisco Catalyst 9000系列网络环境中第3层跳上的交互。

网络图



拓扑

非工作场景

首先，概述在第3层跳上丢弃DHCP发现数据包的场景，特别是在中央交换机上。现在，从DHCP客户端逐跳分析数据包传输过程。

远程站点交换机数据包处理

MAC地址为7010.5cdf.31e9的主机传输DHCP发现数据包，该数据包到达远程站点交换机上的接口GigabitEthernet1/0/1。

远程站点配置

```
<#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
!
!

远程站点交换机入口

进入远程站点交换机的广播DHCP发现数据包。

<#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
!

!

远程站点交换机出口

从远程站点交换机到边缘交换机的中继单播DHCP发现数据包。

<#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
!
!
```



注意：数据包具有“中继代理IP地址：10.93.150.254”，但由于配置了“no ip dhcp snooping information option”作为DHCP部分的一部分，因此它没有DHCP选项82。

边缘交换机数据包处理

对于DHCP流量问题，边缘交换机是一种L2交换机，仅用于将数据包分发到中央/核心交换机和远程站点交换机之间或它们之间的交换机。信任所有DHCP数据包。

边缘交换机配置

```
<#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
!					
!					

边缘交换机入口

从远程站点交换机传出的数据包按原样到达边缘交换机。

边缘交换机出口

由于这是数据包的第2层跃点，因此它会在进入下一跳时退出交换机，而交换机保持不变。边缘交换机将数据包转发到中央交换机，而不在数据包中发现任何修改。

边缘交换机出口数据包是中央交换机入口数据包。

<#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
!
!
```

中央交换机数据包处理

中央交换机配置

```
<#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

```
V1565 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
!
```

中央交换机入口

如前所述，边缘交换机出口数据包是中央交换机入口数据包。

当数据包到达接口fif 2/1/0/1时，将观察此日志。

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

接口Fif 2/1/0/1被配置为DHCP监听不可信端口。

第3层中继的DHCP发现数据包通过此端口进入。虽然数据包在第3层中继和封装，但DHCP监听仍会在第2层端口上检查数据包。由于此端口不受信任，并且数据包包含网关IP（中继代理）地址，而不使用选项82，因此DHCP监听将丢弃此不受信任端口上的数据包。此行为是预期行为，且是设计行为。



注意：在许多情况下，可以看到DHCP发现由于DHCP监听而在传输过程中被丢弃。

中央交换机出口

在这种情况下，中央交换机将丢弃DHCP发现数据包，并且不会出现任何MAC地址为70:10:5c:df:31:e9的主机发起的DHCP发现数据包从接口Fif 2/1/0/3进入。

如何解决问题？

1.在DHCP客户端的第一跳上启用选项82。

在当前示例中，请在远程交换机上配置ip dhcp snooping information option命令。

2.必须在从DHCP客户端到DHCP服务器的DHCP路径中启用DHCP监听信任。

在当前示例中，在中央交换机的接口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
```

在这些更改后，Discover数据包将开始从中央交换机发送到DHCP服务器。

<#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将到达DHCP服务器，DHCP服务器将回复DHCP Offer。

DHCP提供数据包：

<#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服务器回复的提供数据包将命中CORE/Central交换机的接口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
```

此时没有DHCP监听端的信任，并且OFFER正在进入，那么Offer为什么没有在不信任的端口上丢弃？

如您所知，在启用DHCP监听的网络中，端口被分类为可信或不可信。

可信端口连接到合法DHCP服务器或其他可信交换机。所有DHCP消息都允许在其上。

不可信端口通常连接到最终用户设备（客户端）。它们受到限制以防止“DHCP欺骗”或“非法DHCP服务器”攻击。

DHCP Offer和DHCP ACK数据包被视为“服务器端”消息。根据安全规则，这些消息只能来自合法服务器。

当DHCP中继代理或任何L3路由器/交换机在配置为不可信的L2端口上收到DHCP提供时，DHCP监听机制会将此行为标识为安全违规。它假设非法DHCP服务器尝试向网络中的客户端提供未经授权的IP地址。

即使数据包是单播（具体针对中继代理），物理或逻辑端口的信任状态优先。无论数据包是广播还是单播，都将在端口级别执行安全检查。

由于端口不受信任，系统将阻止DHCP提供，以保护网络免受来自未经授权源的潜在恶意或错误配置数据的侵害。

第3层端口（路由接口）在第3层运行。由于它是路由接口，因此它不会遵守应用于交换机端口的第2层DHCP监听信任/不信任规则。

客户端发送广播请求。中继代理（L3设备）会拦截此请求并将单播请求发送到DHCP服务器。

DHCP服务器将单播DHCP提供发送回中继代理的IP地址（特别是转发器或网关IP地址）。

当数据包到达中继代理的L3端口或到达数据包路径中的任何L3跳时，设备会接受数据包作为合法路由流量。

与早期场景（L2不受信任端口）不同，交换机正在查找来自面向客户端的端口的“服务器端”消息，L3端口充当服务器响应的预期目标或合法L3跃点。

如果L3端口丢弃了单播DHCP提供，DHCP中继机制将永远无法工作，因为服务器将永远无法与中继代理通信。

最后，Offer数据包将经过直到到达客户端。

主机/客户端将使用DHCP请求进行回复。

<#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服务器将最终确认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，主机将成功接收IP地址。

摘要

请参阅下表以了解数据包转发场景。

端口类型	信任状态	中继数据包类型	结果	原因
------	------	---------	----	----

L2端口	不受信任	单播DHCP提供/确认	已丢弃	DHCP监听可防止服务器消息出现在不可信的第2层端口上。
L3端口	不适用 (路由)	单播DHCP提供/确认	已接受	路由端口是中继代理通信的预定节点。
L2端口	可信	单播DHCP发现与选项82	已接受	可信端口允许所有DHCP信号。
L2端口	不受信任	单播DHCP发现与选项82	已接受	具有中继代理IP地址和选项82的数据包是合法的。
L2端口	可信	不带选项的单播DHCP发现82	已接受	可信端口允许所有DHCP信号。
L2端口	不受信任	不带选项的单播DHCP发现82	已丢弃	具有中继代理IP地址且没有选项82的数据包是欺诈数据包。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。