

Understanding DHCP Snooping for Packets Crossing Layer 3 Hops

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Non-Working Scenario](#)

[Remote-site Switch Packet Processing](#)

[Remote Site Configuration](#)

[Remote-site Switch Ingress](#)

[Remote-site Switch Egress](#)

[Edge Switch Packet Processing](#)

[Edge Switch Configuration](#)

[Edge Switch Ingress](#)

[Edge Switch Egress](#)

[Central Switch Packet Processing](#)

[Central Switch Configuration](#)

[Central Switch Ingress](#)

[Central Switch Egress](#)

[How to fix the problem?](#)

[Summary](#)

Introduction

This document describes the DHCP snooping interactions and behaviour when the packet is crossing any L3 device and if the packet is encapsulated in L3 header.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS® XE proficiency in configuration and operational commands.
- Familiarity with the Cisco Catalyst 9000 series switch hardware and architecture.
- A solid understanding of DHCP protocol operations and DHCP snooping mechanisms.
- A conceptual understanding of DHCP option 82 and the role of the relay agent.
- Basic Routing protocol knowledge.

Components Used

The information in this document is based on these software and hardware versions:

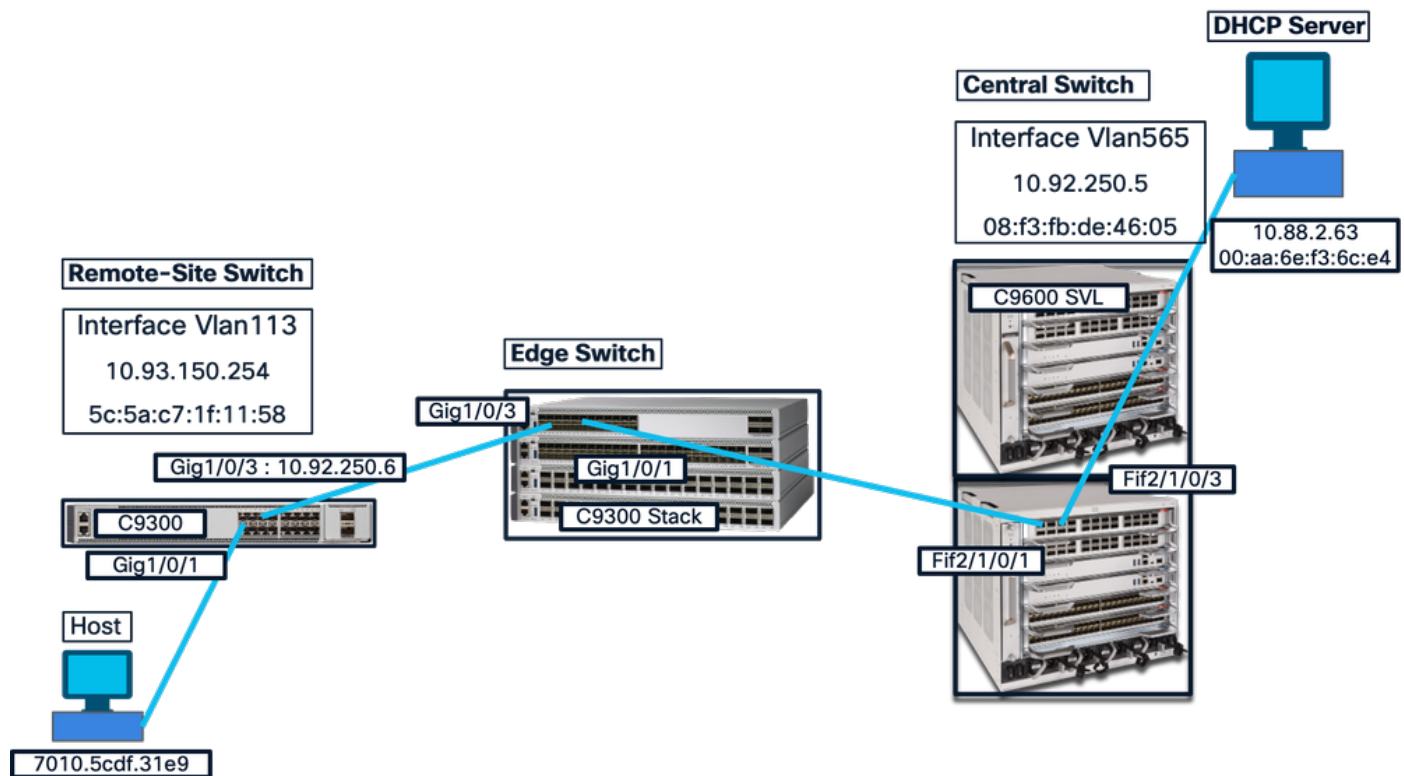
- Core/Distribution switch: Cisco Catalyst 9600X series
- Access switch: Cisco Catalyst 9300 series
- DHCP client: End-host device
- DHCP server: Centralised network service provider

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document examines how DHCP snooping inspects and intercepts DHCP packets as they traverse a Layer 3 hop. Using practical configuration examples and analysis of related packet captures, it demonstrates the interaction of DHCP snooping on Layer 3 hops within a Cisco Catalyst 9000 series network environment.

Network Diagram



Topology

Non-Working Scenario

First, the scenario where the DHCP Discover packet is dropped at the Layer 3 hop is outlined, specifically on the Central Switch. Now, analyse the packet journey hop by hop from the DHCP client.

Remote-site Switch Packet Processing

The Host with MAC address 7010.5cdf.31e9 transmits the DHCP Discover packet, which arrives at interface GigabitEthernet1/0/1 on the remote-site switch.

Remote Site Configuration

```
<#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
!
!

Remote-site Switch Ingress

The Broadcast DHCP Discover Packet entering the Remote-site switch.

<#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
!
!

Remote-site Switch Egress

The Relayed Unicast DHCP Discover Packet exiting from Remote-site switch to Edge Switch.

<#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
!
!
```



Note: The packet having 'Relay agent IP address:10.93.150.254' but it does not have DHCP Option 82 because of configuration 'no ip dhcp snooping information option' as the part of DHCP section.

Edge Switch Packet Processing

For the DHCP flow is concern, Edge switch is a L2 switch used just to distribute the packets to and fro between central/core switch and the Remote Site switches. Its trusting all the DHCP packets.

Edge Switch Configuration

```
<#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
!					
!					

Edge Switch Ingress

The packet egressing from the Remote-site Switch is hitting the Edge Switch as it is.

Edge Switch Egress

Since this is a Layer 2 hop for the packet, it exits the switch unchanged as it proceeds to the next hop. The Edge-switch forwards the packet to the Central-Switch without any modification observed in the packet.

Edge Switch Egress Packet is Central Switch Ingress packet.

<#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

!
!

Central Switch Packet Processing

Central Switch Configuration

<#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  
!  
!
```

Central Switch Ingress

As mentioned earlier, Edge Switch Egress Packet is Central Switch Ingress packet.

When the packet arrives at interface fif 2/1/0/1, this log will be observed.

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

Interface Fif 2/1/0/1 is configured as an untrusted port for DHCP snooping.

A Layer 3 relayed DHCP Discover packet enters through this port. Although the packet is relayed and encapsulated at Layer 3, DHCP snooping still inspects it on the Layer 2 port. Since this port is untrusted and the packet contains a Gateway IP (Relay Agent) address without option 82, DHCP snooping will drop the packet on this untrusted port. This behavior is expected and by design.



Note: In many of the cases it is seen that DHCP Discover getting dropped in transit because of DHCP snooping.

Central Switch Egress

In this case, Central-Switch will drop the DHCP Discover packet and there will not be any DHCP Discover packet initiated by Host with MAC address 70:10:5c:df:31:e9 egressing from interface Fif 2/1/0/3.

How to fix the problem?

1. Have Option 82 enabled on the first hop of the DHCP client.

In the current example, configure **ip dhcp snooping information option** command on the Remote-Switch.

2. DHCP snooping trust must be enabled throughout the DHCP path from DHCP client to DHCP server.

In the current example, configure **ip dhcp snooping trust** command on interface fif2/1/0/1 of Central Switch.

<#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
```

After these changes, the Discover packet will start leaving from Central Switch to DHCP server.

<#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

The Discover will reach the DHCP server and DHCP server will reply back the DHCP Offer.

DHCP Offer Packet:

<#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

The Offer packet replied back by DHCP server will hit the interface fif2/1/0/3 of CORE/Central Switch.

<#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
```

Here there is no trust from DHCP snooping end and OFFER is entering, then why is the Offer not getting dropped on an untrusted port?

As you know, in a network where DHCP Snooping is enabled, ports are categorised as either trusted or untrusted.

Trusted Ports are connected to legitimate DHCP servers or other trusted switches. All DHCP messages are allowed on it.

Untrusted Ports are typically connected to end-user devices (clients). They are restricted to prevent "DHCP Spoofing" or "Rogue DHCP Server" attacks.

DHCP Offer and DHCP ACK packets are considered 'server-side' messages. According to security rules, these messages must only ever originate from a legitimate server.

When a DHCP relay agent or any L3 Router/Switch receives a DHCP Offer on a L2 port configured as untrusted, the DHCP Snooping mechanism identifies this as a security violation. It assumes that a rogue DHCP server is attempting to provide unauthorised IP addresses to clients on the network.

Even though the packet is unicast (directed specifically to the relay agent), the trust state of the physical or logical port takes precedence. The security check is performed on the port level regardless of whether the packet is broadcast or unicast.

Because the port is untrusted, the system will block the DHCP Offer to protect the network from potentially malicious or incorrect configuration data coming from an unauthorised source.

An L3 port (a routed interface) operates at Layer 3. Because it is a routed interface, it does not observe the L2 DHCP Snooping trust/untrust rules that apply to switchports.

A client sends a broadcast request. The Relay Agent (the L3 device) intercepts this and sends an unicast request to the DHCP server.

The DHCP server sends an unicast DHCP Offer back to the IP address of the Relay Agent (specifically to the giaddr or Gateway IP address).

When the packet arrives at the L3 port of the Relay Agent or on any L3 hop in the packet path, the device

accepts the packet as legitimate routing traffic.

Unlike the earlier scenario (an L2 untrusted port), where the switch is looking for 'server-side' messages coming from a client-facing port, the L3 port is acting as the intended destination or legitimate L3 hop for the response of the server.

If L3 ports dropped unicast DHCP offers, DHCP relaying mechanism will never work, as the server will never be able to communicate back to the relay agent.

Finally the Offer packet will traverse till it reaches the client.

Host/Client will reply back with DHCP Request.

<#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 server will finally ACK the IP address assignment.

<#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 completes and host will receive IP address successfully.

Summary

Refer to this table in order to understand the packet forwarding scenarios.

Port Type	Trust State	Relayed Packet Type	Result	Reason
L2 Port	Untrusted	Unicast DHCP Offer/Ack	Dropped	DHCP Snooping prevents server messages on untrusted L2 ports.
L3 Port	N/A (Routed)	Unicast DHCP Offer/Ack	Accepted	Routed ports are the intended nodes for Relay Agent communication.
L2 Port	Trusted	Unicast DHCP Discover with option 82	Accepted	Trusted port allows all DHCP signals.

L2 Port	Untrusted	Unicast DHCP Discover with option 82	Accepted	The packet with relay agent IP address and Option 82 is legitimate.
L2 Port	Trusted	Unicast DHCP Discover without option 82	Accepted	Trusted port allows all DHCP signals.
L2 Port	Untrusted	Unicast DHCP Discover without option 82	Dropped	The packet with relay agent IP address and no option 82 is rogue.