

レイヤ3ホップを通過するパケットのDHCPスヌーピングについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[バックグラウンド情報](#)

[ネットワーク図](#)

[正常に動作しないシナリオ](#)

[リモートサイトのスイッチパケット処理](#)

[リモートサイトの設定](#)

[リモートサイトスイッチの入力](#)

[リモートサイトスイッチの出力](#)

[エッジスイッチパケット処理](#)

[エッジスイッチの設定](#)

[エッジスイッチ入力](#)

[エッジスイッチ出力](#)

[中央スイッチパケット処理](#)

[中央スイッチの設定](#)

[中央のスイッチ入力](#)

[中央スイッチの出力](#)

[問題の解決方法](#)

[要約](#)

はじめに

このドキュメントでは、パケットがL3デバイスを通過する際のDHCPスヌーピングのインタラクションと動作、およびパケットがL3ヘッダーにカプセル化される場合の動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOS® XEの設定および運用コマンドに関する習熟度
- Cisco Catalyst 9000シリーズスイッチのハードウェアとアーキテクチャに精通していること
- DHCPプロトコルの動作とDHCPスヌーピングメカニズムに関する十分な理解
- DHCPオプション82とリレーエージェントの役割に関する概念の理解
- 基本的なルーティングプロトコルの知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

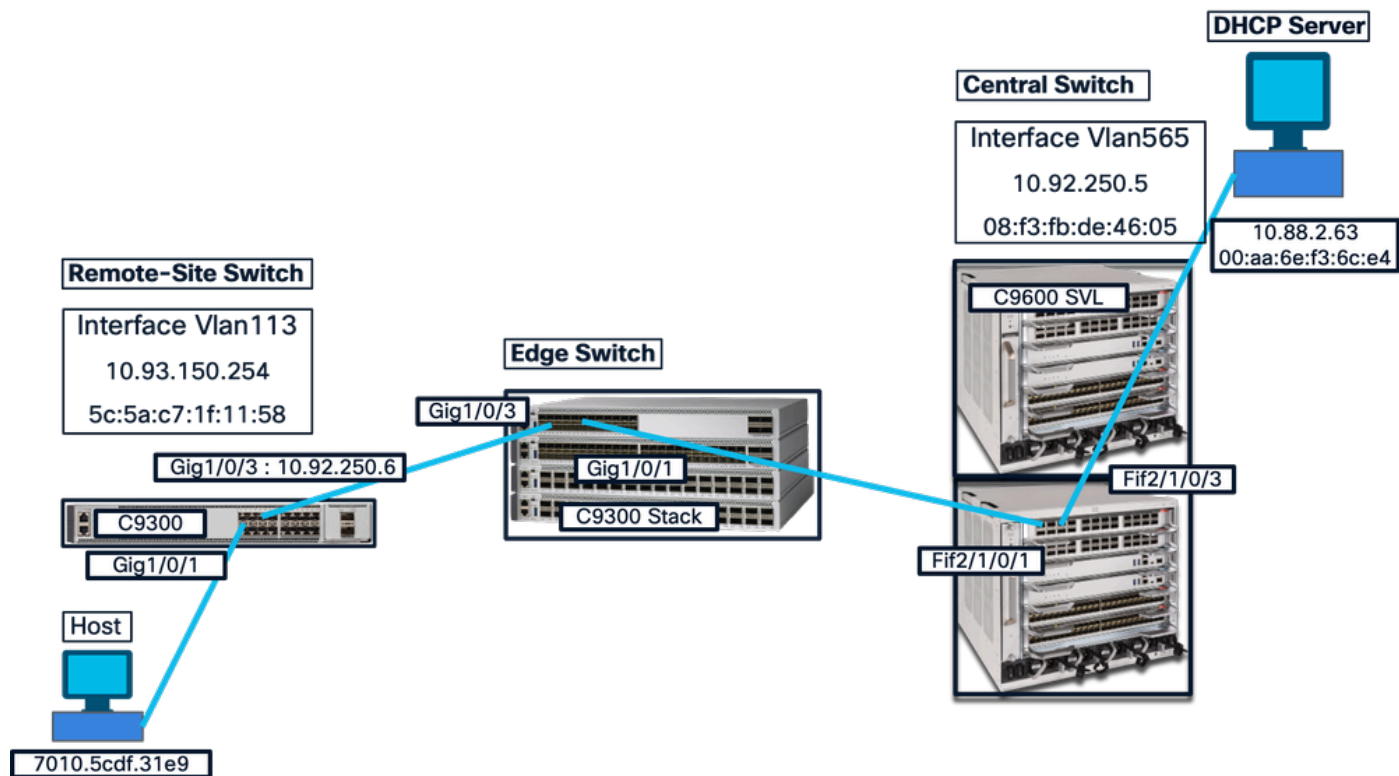
- コア/ディストリビューションスイッチ：Cisco Catalyst 9600Xシリーズ
- アクセススイッチ：Cisco Catalyst 9300シリーズ
- DHCPクライアント：エンドホストデバイス
- DHCPサーバ：集中型ネットワークサービスプロバイダー

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

バックグラウンド情報

このドキュメントでは、DHCPスヌーピングがレイヤ3ホップを通過するDHCPパケットを検査し、代行受信する方法について説明します。実際の設定例と関連するパケットキャプチャの分析を使用して、Cisco Catalyst 9000シリーズネットワーク環境内のレイヤ3ホップでのDHCPスヌーピングのインタラクションを示します。

ネットワーク図



トポロジ

正常に動作しないシナリオ

まず、DHCP Discoverパケットがレイヤ3ホップでドロップされるシナリオ、特に中央スイッチについて概説します。次に、DHCPクライアントからのパケットの移動をホップバイホップで分析します。

リモートサイトのスイッチパケット処理

MACアドレス7010.5cdf.31e9のホストからDHCP Discoverパケットが送信され、リモートサイトスイッチのインターフェイスGigabitEthernet1/0/1に到達します。

リモートサイトの設定

<#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
!
!

リモートサイトスイッチの入力

リモートサイトスイッチに入るブロードキャストDHCPディスカバリパッケージ。

<#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
!

!

リモートサイトスイッチの出力

リモートサイトスイッチからエッジスイッチに送信されるリレーされたユニキャストDHCP検出パケット。

<#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: 「Relay agent IP address:10.93.150.254」を含むパケットですが、DHCPセクションの一部として「no ip dhcp snooping information option」を設定しているため、DHCPオプション82は含まれていません。

エッジスイッチパケット処理

DHCPフローに問題がある場合、エッジスイッチは、中央/コアスイッチとリモートサイトスイッチの間でパケットを送受信するためだけに使用されるL2スイッチです。すべてのDHCPパケットを信頼しています。

エッジスイッチの設定

```
<#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

!

!

エッジスイッチ入力

リモートサイトスイッチから送信されたパケットは、そのままエッジスイッチに到達しています。

エッジスイッチ出力

これはパケットのレイヤ2ホップであるため、ネクストホップに進むにつれて、スイッチから変更されことなく出ていきます。エッジスイッチは、パケット内で確認された変更を加えることなく、パケットを中央スイッチに転送します。

エッジスイッチの出力パケットは、中央スイッチの入力パケットです。

<#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
!
!

```

中央スイッチパケット処理

中央スイッチの設定

```
<#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  
!  
!
```

中央のスイッチ入力

前述したように、エッジスイッチの出力パケットは中央スイッチの入力パケットです。

パケットがインターフェイスfif 2/1/0/1に到着すると、このログが観察されます。

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

インターフェイスFif 2/1/0/1は、DHCPスヌーピングの信頼できないポートとして設定されています。

レイヤ3リレーされたDHCP Discoverパケットがこのポートから入ります。パケットはレイヤ3でリレーおよびカプセル化されますが、DHCPスヌーピングはレイヤ2ポートでパケットを検査します。このポートは信頼できず、パケットにはオプション82のないゲートウェイIP (リレーエージェント) アドレスが含まれているため、DHCPスヌーピングはこの信頼できないポートでパケットをドロップします。この動作は予期されており、意図的なものです。



注：多くの場合、DHCP DiscoverはDHCPスヌーピングにより転送中にドロップされます。

中央スイッチの出力

この場合、Central-SwitchはDHCP Discoverパケットをドロップし、MACアドレス70:10:5c:df:31:e9のホストによって開始されたDHCP DiscoverパケットはインターフェイスFif 2/1/0/3から出力されません。

問題の解決方法

1. DHCPクライアントの最初のホップでオプション82を有効にする。
現在の例では、リモートスイッチでip dhcp snooping information optionコマンドを設定します。
2. DHCPスヌーピングの信頼は、DHCPクライアントからDHCPサーバへのDHCPパス全体で有効になっている必要があります。

現在の例では、中央スイッチのインターフェイスfif2/1/0/1でip dhcp snooping trustコマンドを設定します。

<#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
```

これらの変更の後、Discoverパケットが中央スイッチからDHCPサーバに送信され始めます。

<#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

ディスカバリはDHCPサーバに到達し、DHCPサーバはDHCPオファーに応答します。

DHCPオファーパケット :

<#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サーバが応答したOfferパケットは、CORE/Central Switchのインターフェイスfif2/1/0/3に到達します。

<#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

DHCPスヌーピング側から信頼がなく、OFFERが入力されていますが、信頼できないポートにOFFERがドロップされないのはなぜですか。

ご存知のように、DHCPスヌーピングが有効になっているネットワークでは、ポートは信頼できるポートと信頼できないポートのいずれかに分類されます。

信頼できるポートは、正当なDHCPサーバまたはその他の信頼できるスイッチに接続されます。すべてのDHCPメッセージが許可されます。

信頼できないポートは通常、エンドユーザデバイス（クライアント）に接続されます。「DHCPスプーフィング」または「不正なDHCPサーバ」攻撃を防止するように制限されています。

DHCP OfferおよびDHCP ACKパケットは、「サーバ側」のメッセージと見なされます。セキュリティルールに従って、これらのメッセージは正規のサーバからのみ発信される必要があります。DHCPリレーエージェントまたはL3ルータ/スイッチが、信頼できないとして設定されているL2ポートでDHCPオファーを受信すると、DHCPスヌーピングメカニズムは、これをセキュリティ違反として識別します。これは、不正なDHCPサーバがネットワーク上のクライアントに不正なIPアドレスを提供しようとしていることを前提としています。

パケットがユニキャスト（リレーエージェント宛てに送信）であっても、物理ポートまたは論理ポートの信頼状態が優先されます。セキュリティチェックは、パケットがブロードキャストかユニキャストかに関係なく、ポートレベルで実行されます。

ポートは信頼できないため、システムはDHCPオファーをブロックし、不正な送信元から送信された悪意のある構成データや不正な構成データからネットワークを保護します。

L3ポート（ルーテッドインターフェイス）はレイヤ3で動作します。これはルーテッドインターフェイスであるため、スイッチポートに適用されるL2 DHCPスヌーピングの信頼/非信頼ルールを順守しません。

クライアントがブロードキャスト要求を送信します。リレーエージェント（L3デバイス）はこれをインターセプトし、ユニキャスト要求をDHCPサーバに送信します。

DHCPサーバは、リレーエージェントのIPアドレス（特にgiaddrまたはゲートウェイIPアドレス）にユニキャストDHCPオファーを返信します。

パケットがリレーエージェントのL3ポートまたはパケットパス内の任意のL3ホップに到着すると、デバイスはパケットを正当なルーティングトラフィックとして受け入れます。

以前のシナリオ（L2の信頼できないポート）とは異なり、スイッチはクライアント側のポートからの「サーバ側」のメッセージを探しますが、L3ポートはサーバの応答に対して、意図された宛先または正規のL3ホップとして機能します。

L3ポートがユニキャストDHCPオファーをドロップした場合、サーバがリレーエージェントと通信できなくなるため、DHCPリレーメカニズムは機能しません。

最後に、Offerパケットは、クライアントに到達するまで通過します。

ホスト/クライアントがDHCP要求で応答します。

<#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サーバは、最終的にIPアドレスの割り当てをACKします。

<#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が完了し、ホストはIPアドレスを正常に受信します。

要約

パケット転送のシナリオについては、次の表を参照してください。

ポート タイプ	Trust state	中継パケットタイプ	結果	原因
L2ポート	Untrusted	ユニキャストDHCPオファ ー/確認応答	Dropped	DHCPスヌーピングは、信頼できない L2ポートでのサーバメッセージを防止 します。
L3ポート	該当なし (ルート)	ユニキャストDHCPオファ ー/確認応答	承諾	ルーテッドポートは、リレーエージェン ト通信用のノードです。
L2ポート	TRUSTED	オプション82を使用したユ ニキャストDHCP Discover	承諾	信頼できるポートは、すべてのDHCP信 号を許可します。
L2ポート	Untrusted	オプション82を使用したユ ニキャストDHCP Discover	承諾	リレーエージェントのIPアドレスとオプ ション82を持つパケットは正当です。
L2ポート	TRUSTED	オプション82を使用しない ユニキャストDHCP Discover	承諾	信頼できるポートは、すべてのDHCP信 号を許可します。
L2ポート	Untrusted	オプション82を使用しない ユニキャストDHCP	Dropped	リレーエージェントのIPアドレスを持ち 、オプション82を持たないパケットは

		Discover		不正です。
--	--	----------	--	-------

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。