레이어 3 홉을 통과하는 패킷에 대한 DHCP 스누핑 이해

목차

소개

이 문서에서는 패킷이 L3 디바이스를 통과할 때 그리고 패킷이 L3 헤더에 캡슐화된 경우 DHCP 스누핑 상호 작용 및 동작에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS® XE는 구성 및 운영 명령에 대한 숙련도를 제공합니다.
- Cisco Catalyst 9000 Series 스위치 하드웨어 및 아키텍처에 대한 지식
- DHCP 프로토콜 작업 및 DHCP 스누핑 메커니즘에 대한 확실한 이해.
- DHCP 옵션 82 및 릴레이 에이전트의 역할에 대한 개념적 이해.
- 기본 라우팅 프로토콜 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

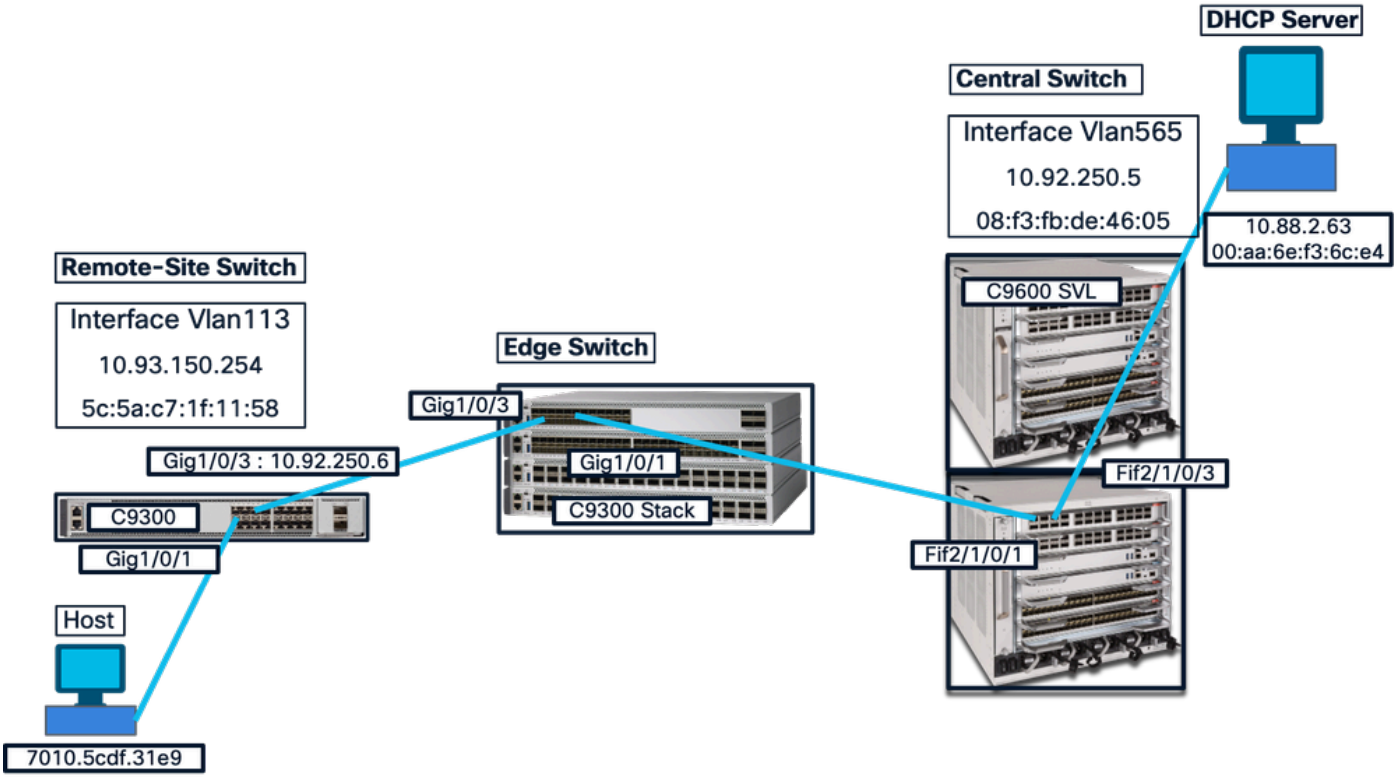
- 코어/분산 스위치: Cisco Catalyst 9600X 시리즈
- 액세스 스위치: Cisco Catalyst 9300 시리즈
- DHCP 클라이언트: 엔드-호스트 디바이스
- DHCP 서버: 중앙 집중식 네트워크 서비스 공급자

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 DHCP 스누핑이 레이어 3 홉을 통과할 때 DHCP 패킷을 검사하고 차단하는 방법을 살펴봅니다. 실제 컨피그레이션 예와 관련 패킷 캡처 분석을 사용하여 Cisco Catalyst 9000 Series 네트워크 환경 내의 레이어 3 홉에서 DHCP 스누핑의 상호 작용을 보여줍니다.

네트워크 다이어그램



토폴로지

비작업 시나리오

먼저, DHCP Discover 패킷이 레이어 3 홉에서 삭제되는 시나리오가 특히 중앙 스위치에 설명되어 있습니다. 이제 DHCP 클라이언트에서 홉별로 패킷 여정을 분석합니다.

원격 사이트 스위치 패킷 처리

MAC 주소가 7010.5cdf.31e9인 호스트는 원격 사이트 스위치의 인터페이스 GigabitEthernet1/0/1에 도착하는 DHCP Discover 패킷을 전송합니다.

원격 사이트 컨피그레이션

<#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
!
!
```

원격 사이트 스위치 인그레스

Broadcast DHCP Discover Packet(브로드캐스트 DHCP 검색 패킷)이 원격 사이트 스위치에 들어갑니다.

<#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
!

```
!
```

원격 사이트 스위치 이그레스

원격 사이트 스위치에서 에지 스위치로 나가는 릴레이된 유니캐스트 DHCP 검색 패킷입니다.

<#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
!
!
```

참고: '릴레이 에이전트 IP 주소:10.93.150.254'가 있는 패킷이지만 DHCP 옵션 82가 없습니다. DHCP 섹션의 일부로 'no ip dhcp snooping information option' 구성이 있기 때문입니다.

에지 스위치 패킷 처리

DHCP 플로우가 문제가 되는 경우 Edge 스위치는 중앙/코어 스위치와 원격 사이트 스위치 간에 패킷을 주고받는 데만 사용되는 L2 스위치입니다. 모든 DHCP 패킷을 신뢰합니다.

에지 스위치 컨피그레이션

<#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
!
!
```

에지 스위치 인그레스

원격 사이트 스위치에서 이그레스(egress)하는 패킷이 에지 스위치에 그대로 도달합니다.

에지 스위치 이그레스

이는 패킷의 레이어 2 홉이므로 다음 홉으로 진행하면서 변경되지 않은 상태로 스위치를 종료합니다. Edge-switch는 패킷에서 관찰된 수정 사항 없이 패킷을 Central-Switch로 전달합니다.

에지 스위치 이그레스 패킷은 중앙 스위치 인그레스 패킷입니다.

```
!
!
```

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
!
!
```

중앙 스위치 패킷 처리

중앙 스위치 컨피그레이션

<#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
!
!
```

중앙 스위치 인그레스

앞에서 언급한 것처럼, 에지 스위치 이그레스 패킷은 중앙 스위치 인그레스 패킷입니다.

패킷이 인터페이스 fif 2/1/0/1에 도착하면 이 로그가 관찰됩니다.

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

인터페이스 Fif 2/1/0/1은 DHCP 스누핑을 위한 신뢰할 수 없는 포트로 구성됩니다.

레이어 3 릴레이된 DHCP Discover 패킷이 이 포트를 통해 들어옵니다. 패킷이 레이어 3에서 릴레이되고 캡슐화되더라도 DHCP 스누핑은 여전히 레이어 2 포트에서 패킷을 검사합니다. 이 포트는 신뢰할 수 없고 패킷에 옵션 82 없이 게이트웨이 IP(릴레이 에이전트) 주소가 포함되어 있으므로 DHCP 스누핑은 이 신뢰할 수 없는 포트에서 패킷을 삭제합니다. 이러한 동작은 설계에 따라 필요합니다.

참고: 대부분의 경우 DHCP 스누핑으로 인해 DHCP Discover가 전송 중에 삭제되는 것으로 나타납니다.

중앙 스위치 이그레스

이 경우 Central-Switch는 DHCP Discover 패킷을 삭제하고 MAC 주소가 70:10:5c:df:31:e9인 호스트에서 시작한 DHCP Discover 패킷이 인터페이스 Fif 2/1/0/3에서 이그레스(egress)되지 않습니다.

문제를 해결하는 방법

1. DHCP 클라이언트의 첫 번째 홉에서 옵션 82를 사용하도록 설정합니다.
현재 예에서는 Remote-Switch에서 ip dhcp snooping information option 명령을 구성합니다.

2. DHCP 클라이언트에서 DHCP 서버로의 DHCP 경로 전체에서 DHCP 스누핑 트러스트를 활성화해야 합니다.

현재 예에서는 중앙 스위치의 인터페이스 fif2/1/0/1에서 ip dhcp snooping trust 명령을 구성합니다.

```
<#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
```

이러한 변경 후 Discover 패킷이 Central Switch에서 DHCP 서버로 나가기 시작합니다.

<#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(검색)가 DHCP 서버에 연결되고 DHCP 서버가 DHCP 오퍼에 응답합니다.

DHCP 제공 패킷:

<#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 서버가 다시 응답한 오퍼 패킷은 CORE/Central 스위치의 인터페이스 fif2/1/0/3에 도달합니다.

<#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
```

여기서 DHCP 스누핑 끝의 신뢰가 없고 OFFER가 들어옵니다. 그러면 Offer가 신뢰할 수 없는 포트에서 삭제되지 않는 이유는 무엇입니까?

아시다시피 DHCP Snooping이 활성화된 네트워크에서 포트는 신뢰할 수 있는 포트 또는 신뢰할 수 없는 포트로 분류됩니다.

신뢰할 수 있는 포트는 합법적인 DHCP 서버 또는 기타 신뢰할 수 있는 스위치에 연결됩니다. 모든 DHCP 메시지가 허용됩니다.
신뢰할 수 없는 포트는 일반적으로 최종 사용자 디바이스(클라이언트)에 연결됩니다. "DHCP Spoofing" 또는 "Rogue DHCP Server" 공격을 방지하기 위해 제한됩니다.
DHCP Offer 및 DHCP ACK 패킷은 '서버 측' 메시지로 간주됩니다. 보안 규칙에 따르면 이러한 메시

지는 합법적인 서버에서만 생성되어야 합니다.
DHCP 릴레이 에이전트 또는 임의의 L3 라우터/스위치가 신뢰할 수 없는 것으로 구성된 L2 포트에서 DHCP 제공을 수신하면 DHCP 스누핑 메커니즘은 이를 보안 위반으로 식별합니다. 비인가 DHCP 서버가 네트워크의 클라이언트에 권한 없는 IP 주소를 제공하려고 시도하는 것으로 가정합니다.
패킷이 유니캐스트(특히 릴레이 에이전트로 전달됨)인 경우에도 물리적 또는 논리적 포트의 신뢰 상태가 우선합니다. 보안 검사는 패킷이 브로드캐스트인지 유니캐스트인지에 관계없이 포트 레벨에서 수행됩니다.
포트를 신뢰할 수 없기 때문에 시스템은 DHCP 제공을 차단하여 무단 소스에서 오는 잠재적으로 악의적이거나 잘못된 컨피그레이션 데이터로부터 네트워크를 보호합니다.

L3 포트(라우티드 인터페이스)는 레이어 3에서 작동합니다. 라우티드 인터페이스이기 때문에 스위치 포트에 적용되는 L2 DHCP 스누핑 신뢰/신뢰 해제 규칙을 준수하지 않습니다.
클라이언트가 브로드캐스트 요청을 보냅니다. 릴레이 에이전트(L3 디바이스)는 이를 인터셉트하여 DHCP 서버에 유니캐스트 요청을 보냅니다.
DHCP 서버는 릴레이 에이전트의 IP 주소(특히, giaddr 또는 게이트웨이 IP 주소)로 유니캐스트 DHCP 제안을 다시 보냅니다.
패킷이 릴레이 에이전트의 L3 포트에 도착하거나 패킷 경로의 L3 홉에 도달하면 디바이스는 해당 패킷을 합법적인 라우팅 트래픽으로 수락합니다.
스위치가 클라이언트 연결 포트에서 오는 '서버측' 메시지를 찾는 이전 시나리오(L2 신뢰할 수 없는 포트)와 달리, L3 포트는 서버의 응답을 위해 의도한 대상 또는 올바른 L3 홉의 역할을 합니다.
L3 포트에서 유니캐스트 DHCP를 제공하면 서버가 릴레이 에이전트와 다시 통신할 수 없으므로 DHCP 릴레이 메커니즘이 작동하지 않습니다.

마지막으로 오퍼 패킷이 클라이언트에 도달할 때까지 이동합니다.

호스트/클라이언트가 DHCP 요청으로 응답합니다.

<#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 서버가 최종적으로 IP 주소 할당을 승인합니다.

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

DORA가 완료되고 호스트가 IP 주소를 수신합니다.

요약

패킷 전달 시나리오를 이해하려면 이 표를 참조하십시오.

포트 유형	트러스트 상태	릴레이된 패킷 유형	결과	이유
L2 포트	신뢰할 수 없음	유니캐스트 DHCP 오퍼/Ack	삭제됨	DHCP 스누핑은 신뢰할 수 없는 L2 포트에서 서버 메시지를 방지합니다.
L3 포트	해당 없음(라우팅됨)	유니캐스트 DHCP 오퍼/Ack	수락됨	라우티드 포트는 릴레이 에이전트 통신을 위한 노드입니다.
L2 포트	신뢰할 수 있음	옵션 82로 유니캐스트 DHCP 검색	수락됨	신뢰할 수 있는 포트는 모든 DHCP 신호를 허용합니다.
L2 포트	신뢰할 수 없음	옵션 82로 유니캐스트 DHCP 검색	수락됨	릴레이 에이전트 IP 주소와 옵션 82가 있는 패킷은 합법적입니다.
L2 포트	신뢰할 수 있음	옵션 82 없이 유니캐스트 DHCP 검색	수락됨	신뢰할 수 있는 포트는 모든 DHCP 신호를 허용합니다.
L2 포트	신뢰할 수 없음	옵션 82 없이 유니캐스트 DHCP 검색	삭제됨	릴레이 에이전트 IP 주소가 있고 옵션 82가 없는 패킷은 비인가 패킷입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.