Grundlegendes zum DHCP-Snooping für Pakete, die Layer-3-Hops passieren

Inhalt

Einleitung

Dieses Dokument beschreibt die DHCP-Snooping-Interaktionen und das Verhalten, wenn das Paket ein L3-Gerät durchläuft und das Paket in den L3-Header gekapselt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS® XE Kenntnisse in Konfiguration und Betriebsbefehlen.
- Vertrautheit mit der Hardware und Architektur von Cisco Catalyst Switches der Serie 9000
- Grundlegendes Verständnis der DHCP-Protokollvorgänge und DHCP-Snooping-Mechanismen
- Grundlegendes Verständnis der DHCP-Option 82 und der Rolle des Relay-Agenten
- Grundlegende Kenntnisse über Routing-Protokolle

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

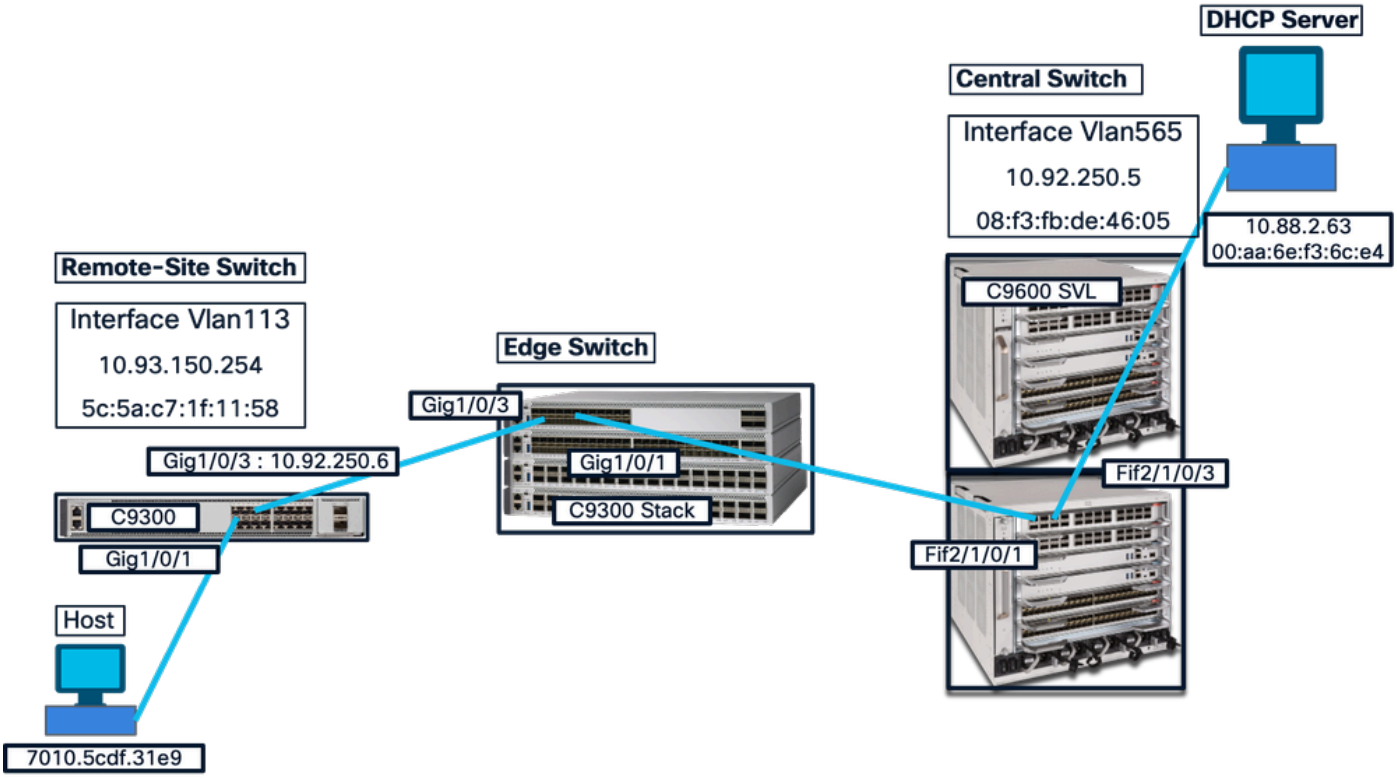
- Core/Distribution Switch: Cisco Catalyst Serie 9600X
- Access Switch: Switches der Cisco Catalyst 9300-Serie
- DHCP-Client: End-Host-Gerät
- DHCP-Server: Zentraler Netzwerkservice-Provider

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird untersucht, wie DHCP-Snooping DHCP-Pakete während der Übertragung durch einen Layer-3-Hop prüft und abfängt. Anhand praktischer Konfigurationsbeispiele und Analysen der zugehörigen Paketerfassung wird die Interaktion von DHCP-Snooping auf Layer-3-Hops in einer Netzwerkumgebung mit Cisco Catalyst Switches der Serie 9000 demonstriert.

Netzwerkdiagramm



Topologie

Nicht-Arbeitsszenario

Zunächst wird das Szenario beschrieben, in dem das DHCP Discover-Paket im Layer-3-Hop verworfen wird, insbesondere auf dem zentralen Switch. Analysieren Sie nun den Paketverlauf für jeden Hop vom DHCP-Client.

Paketverarbeitung am Remote-Standort-Switch

Der Host mit der MAC-Adresse 7010.5cdf.31e9 überträgt das DHCP Discover-Paket, das an der Schnittstelle GigabitEthernet1/0/1 am Remote-Standort-Switch eingeht.

Konfiguration des Remote-Standorts

<#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
!
!
```

Switch-Eingang am Remote-Standort

Das Broadcast-DHCP-Discover-Paket, das auf den Remote-Standort-Switch zugreift.

<#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
!

```
!
```

Switch-Ausgang am Remote-Standort

Das vom Remote-Standort-Switch zum Edge-Switch gesendete Unicast-DHCP-Ermittlungspaket.

<#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
!
!
```

Anmerkung: Das Paket hat die 'Relay agent IP address:10.93.150.254', verfügt aber aufgrund der Konfiguration 'no ip dhcp snooping information option' als Teil des DHCP-Abschnitts nicht über die DHCP-Option 82.

Edge Switch-Paketverarbeitung

Beim DHCP-Fluss handelt es sich um einen L2-Switch, der nur zur Verteilung der Pakete zwischen dem zentralen/Kern-Switch und den Switches am Remote-Standort verwendet wird. Alle DHCP-Pakete werden als vertrauenswürdig eingestuft.

Edge-Switch-Konfiguration

<#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-Eingang

Das vom Remote-Standort-Switch ausgehende Paket trifft den Edge-Switch in der vorliegenden Form an.

Edge-Switch-Ausgang

Da es sich um einen Layer-2-Hop für das Paket handelt, verlässt es den Switch unverändert, während er zum nächsten Hop wechselt. Der Edge-Switch leitet das Paket an den Central-Switch weiter, ohne dass Änderungen am Paket festgestellt werden.

Edge-Switch-Ausgangspaket ist zentrales Switch-Eingangspaket.

<#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
!
!
```

Zentrale Switch-Paketverarbeitung

Konfiguration des zentralen Switches

<#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
!
!
```

Zentraler Switch-Eingang

Wie bereits erwähnt, handelt es sich beim Edge Switch-Ausgangspaket um ein zentrales Switch-Eingangspaket.

Wenn das Paket an Schnittstelle fünf 1/2/0/1 ankommt, wird dieses Protokoll beobachtet.

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

Schnittstelle FIF 2/1/0/1 ist als nicht vertrauenswürdiger Port für DHCP-Snooping konfiguriert.

Über diesen Port geht ein Layer-3-weitergeleitetes DHCP-Discover-Paket ein. Obwohl das Paket auf Layer 3 weitergeleitet und gekapselt wird, wird es durch DHCP-Snooping immer noch auf dem Layer-2-Port geprüft. Da dieser Port nicht vertrauenswürdig ist und das Paket eine Gateway-IP-Adresse (Relay Agent) ohne Option 82 enthält, verwirft DHCP-Snooping das Paket auf diesem nicht vertrauenswürdigen Port. Dieses Verhalten wird erwartet und ist geplant.

Anmerkung: In vielen Fällen wird DHCP Discover bei der Übertragung aufgrund von DHCP-Snooping verworfen.

Zentraler Switch-Ausgang

In diesem Fall verwirft der Central-Switch das DHCP Discover-Paket und es wird kein DHCP Discover-Paket vom Host mit der MAC-Adresse 70:10:5c:df:31:e9 initiiert, das von der Schnittstelle Fif 2/1/0/3 ausgeht.

Wie das Problem zu beheben?

1. Lassen Sie Option 82 im ersten Hop des DHCP-Clients aktiviert.
Im aktuellen Beispiel konfigurieren Sie den Befehl ip dhcp snooping information option auf dem Remote-Switch.

2. DHCP-Snooping-Vertrauensstellung muss im gesamten DHCP-Pfad vom DHCP-Client zum DHCP-Server aktiviert sein.

Im aktuellen Beispiel konfigurieren Sie den Befehl ip dhcp snooping trust auf der Schnittstelle fif2/1/0/1 des 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
```

Nach diesen Änderungen verlässt das Ermittlungspaket den zentralen Switch zum 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
```

Die Erkennung erreicht den DHCP-Server, und der DHCP-Server antwortet auf das DHCP-Angebot.

DHCP-Angebotspaket:

<#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
```

Das vom DHCP-Server zurückgesendete Angebotspaket erreicht die Schnittstelle fif2/1/0/3 des 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
```

Hier besteht keine Vertrauensstellung vom DHCP-Snooping-Ende, und OFFER wird eingegeben. Warum wird das Angebot dann nicht an einem nicht vertrauenswürdigen Port verworfen?

Wie Sie wissen, werden Ports in einem Netzwerk, in dem DHCP Snooping aktiviert ist, entweder als vertrauenswürdig oder nicht vertrauenswürdig kategorisiert.

Vertrauenswürdige Ports sind mit legitimen DHCP-Servern oder anderen vertrauenswürdigen Switches verbunden. Alle DHCP-Meldungen sind darauf zulässig.
Nicht vertrauenswürdige Ports werden normalerweise mit Endbenutzergeräten (Clients) verbunden. Sie sind eingeschränkt, um "DHCP Spoofing"- oder "Rogue DHCP Server"-Angriffe zu verhindern.
DHCP Offer- und DHCP ACK-Pakete werden als 'serverseitige' Nachrichten betrachtet. Gemäß den Sicherheitsregeln dürfen diese Nachrichten niemals von einem legitimen Server stammen.
Wenn ein DHCP-Relay-Agent oder ein L3-Router/Switch ein DHCP-Angebot an einem L2-Port erhält, der als nicht vertrauenswürdig konfiguriert ist, identifiziert der DHCP-Snooping-Mechanismus dies als Sicherheitsverletzung. Es wird davon ausgegangen, dass ein nicht autorisierter DHCP-Server versucht, Clients im Netzwerk nicht autorisierte IP-Adressen bereitzustellen.
Obwohl es sich um ein Unicast-Paket handelt (das speziell an den Relay-Agenten gerichtet ist), hat der Vertrauensstatus des physischen oder logischen Ports Vorrang. Die Sicherheitsprüfung wird auf Portebene durchgeführt, unabhängig davon, ob es sich um Broadcast- oder Unicast-Pakete handelt.
Da der Port nicht vertrauenswürdig ist, blockiert das System das DHCP-Angebot, um das Netzwerk vor potenziell schädlichen oder falschen Konfigurationsdaten zu schützen, die von einer nicht autorisierten Quelle stammen.

Ein L3-Port (eine geroutete Schnittstelle) wird auf Layer 3 ausgeführt. Da es sich um eine geroutete Schnittstelle handelt, werden die L2-Regeln für "DHCP Snooping trust/untrust", die für Switch-Ports gelten, nicht beachtet.
Ein Client sendet eine Broadcast-Anforderung. Der Relay Agent (das L3-Gerät) fängt dies ab und sendet eine Unicast-Anforderung an den DHCP-Server.
Der DHCP-Server sendet ein Unicast-DHCP-Angebot zurück an die IP-Adresse des Relay-Agenten (insbesondere an die IP-Adresse von giaddr oder Gateway).
Wenn das Paket am L3-Port des Relay Agents oder an einem beliebigen L3-Hop im Paketpfad ankommt, akzeptiert das Gerät das Paket als legitimen Routingverkehr.
Im Gegensatz zum vorherigen Szenario (ein nicht vertrauenswürdiger L2-Port), bei dem der Switch nach "serverseitigen" Nachrichten sucht, die von einem Client-seitigen Port kommen, agiert der L3-Port als beabsichtigtes Ziel oder legitimer L3-Hop für die Antwort des Servers.
Wenn L3-Ports Unicast-DHCP-Angebote verwerfen, funktioniert der DHCP-Weiterleitungsmechanismus nicht, da der Server nie wieder mit dem Relay-Agent kommunizieren kann.

Schließlich wird das Angebotspaket durchlaufen, bis es den Kunden erreicht.

Host/Client antwortet mit DHCP-Anfrage.

<#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
```

Der DHCP-Server AKTIVIERT schließlich die IP-Adresszuweisung.

<#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 wird abgeschlossen und Host erhält erfolgreich die IP-Adresse.

Zusammenfassung

In dieser Tabelle finden Sie Informationen zu den Paketweiterleitungsszenarien.

Port-Typ	Vertrauenswürdiger Status	Weitergeleiteter Pakettyp	Ergebnis	Grund
L2-Port	Nicht vertrauenswürdig	Unicast-DHCP-Angebot/-Bestätigung	Verworfen	DHCP-Snooping verhindert Servermeldungen an nicht vertrauenswürdigen L2-Ports.
L3-Port	K/A (geroutet)	Unicast-DHCP-Angebot/-Bestätigung	Akzeptiert	Geroutete Ports sind die für die Relay Agent-Kommunikation vorgesehenen Knoten.
L2-Port	Vertrauenswürdig	Unicast DHCP Discover mit Option 82	Akzeptiert	Der vertrauenswürdige Port lässt alle DHCP-Signale zu.
L2-Port	Nicht vertrauenswürdig	Unicast DHCP Discover mit Option 82	Akzeptiert	Das Paket mit der IP-Adresse des Relay-Agents und Option 82 ist legitim.
L2-	Vertrauenswürdig	Unicast DHCP Discover	Akzeptiert	Der vertrauenswürdige Port lässt

Port		ohne Option 82		alle DHCP-Signale zu.
L2-Port	Nicht vertrauenswürdig	Unicast DHCP Discover ohne Option 82	Verworfen	Das Paket mit der IP-Adresse des Relay-Agents und ohne Option 82 ist nicht autorisiert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.