

Présentation de la surveillance DHCP pour les paquets traversant les sauts de couche 3

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Scénario de non-fonctionnement](#)

[Traitement des paquets du commutateur de site distant](#)

[Configuration du site distant](#)

[Commutateur d'entrée de site distant](#)

[Sortie du commutateur du site distant](#)

[Traitement des paquets du commutateur de périphérie](#)

[Configuration du commutateur de périphérie](#)

[Entrée commutateur de périphérie](#)

[Sortie du commutateur de périphérie](#)

[Traitement des paquets du commutateur central](#)

[Configuration du commutateur central](#)

[Entrée du commutateur central](#)

[Sortie du commutateur central](#)

[Comment résoudre le problème ?](#)

[Résumé](#)

Introduction

Ce document décrit les interactions et le comportement de surveillance DHCP lorsque le paquet traverse un périphérique de couche 3 et si le paquet est encapsulé dans l'en-tête de couche 3.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compétence de Cisco IOS® XE en matière de configuration et de commandes opérationnelles.
- Connaissance du matériel et de l'architecture des commutateurs Cisco Catalyst 9000.
- Une bonne compréhension des opérations du protocole DHCP et des mécanismes de surveillance DHCP.
- Compréhension conceptuelle de l'option DHCP 82 et du rôle de l'agent de relais.
- Connaissances de base du protocole de routage.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

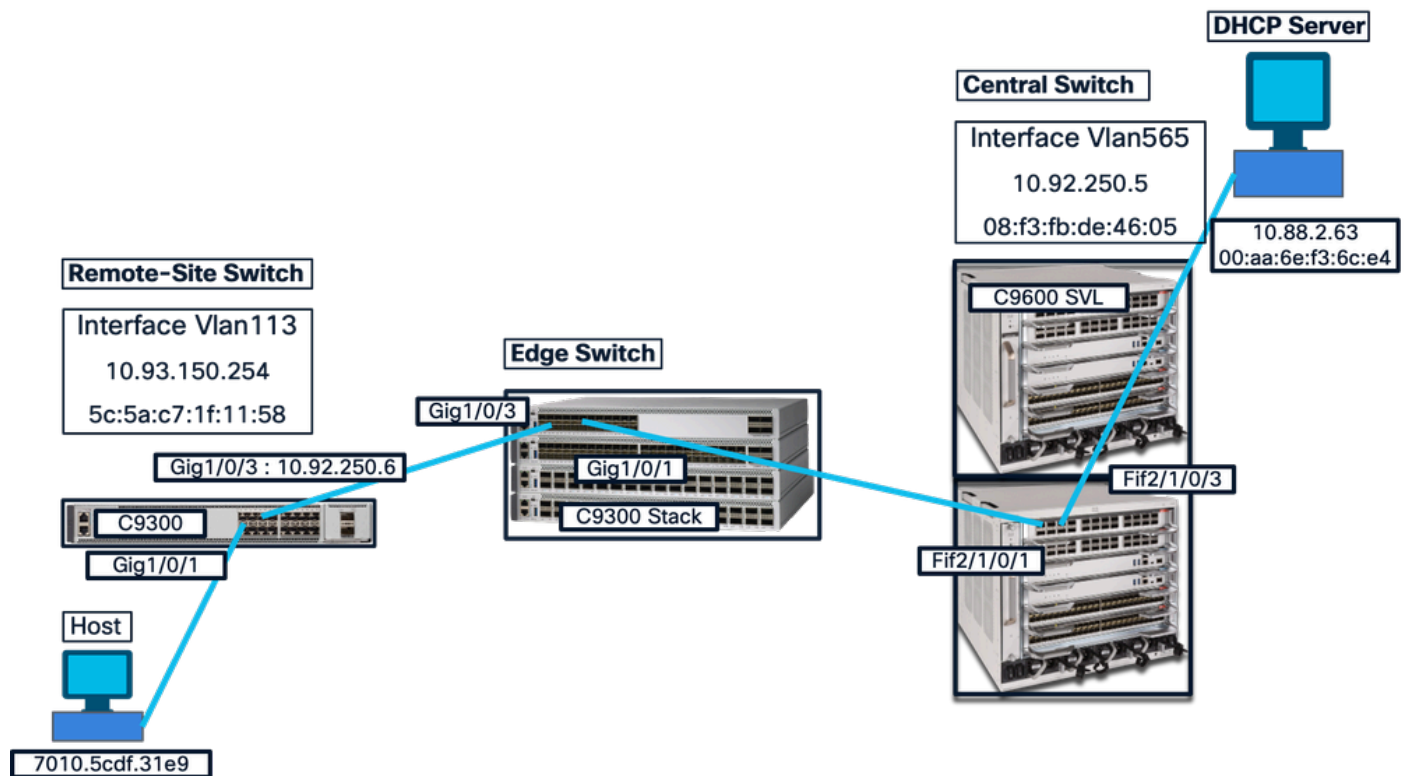
- Commutateur principal/de distribution : Gamme Cisco Catalyst 9600X
- Commutateur d'accès : Cisco Catalyst série 9300
- Client DHCP : Périphérique hôte final
- Serveur DHCP : Fournisseur de services réseau centralisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document examine comment la surveillance DHCP inspecte et intercepte les paquets DHCP lorsqu'ils traversent un saut de couche 3. À l'aide d'exemples de configuration pratiques et d'une analyse des captures de paquets associées, il illustre l'interaction de la surveillance DHCP sur les sauts de couche 3 dans un environnement réseau de la gamme Cisco Catalyst 9000.

Diagramme du réseau



Topologie

Scénario de non-fonctionnement

Tout d'abord, le scénario dans lequel le paquet de détection DHCP est abandonné au saut de couche 3 est décrit, en particulier sur le commutateur central. À présent, analysez le parcours des paquets saut par saut à partir du client DHCP.

Traitement des paquets du commutateur de site distant

L'hôte dont l'adresse MAC est 7010.5cdf.31e9 transmet le paquet de détection DHCP, qui arrive à l'interface GigabitEthernet1/0/1 sur le commutateur du site distant.

Configuration du site distant

```
<#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
!
!

Commutateur d'entrée de site distant

Paquet de détection DHCP de diffusion entrant dans le commutateur du site distant.

<#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
!

!

Sortie du commutateur du site distant

Le paquet de détection DHCP de monodiffusion relayée quitte le commutateur de site distant vers le commutateur de périphérie.

<#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
!
!
```



Remarque : Le paquet ayant « Relay agent IP address : 10.93.150.254 » mais il n'a pas DHCP Option 82 en raison de la configuration « no ip dhcp snooping information option » comme partie de la section DHCP.

Traitement des paquets du commutateur de périphérie

Pour le flux DHCP, le commutateur Edge est un commutateur de couche 2 utilisé uniquement pour distribuer les paquets entre le commutateur central/principal et les commutateurs du site distant. Il fait confiance à tous les paquets DHCP.

Configuration du commutateur de périphérie

```
<#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

!

!

Entrée commutateur de périphérie

Le paquet sortant du commutateur de site distant atteint le commutateur de périphérie tel qu'il est.

Sortie du commutateur de périphérie

Comme il s'agit d'un saut de couche 2 pour le paquet, il quitte le commutateur sans modification au fur et à mesure qu'il passe au saut suivant. Le commutateur de périphérie transfère le paquet au commutateur central sans aucune modification observée dans le paquet.

Le paquet de sortie du commutateur de périphérie est le paquet d'entrée du commutateur central.

<#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
!
!

```

Traitement des paquets du commutateur central

Configuration du commutateur central

```
<#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  
!  
!
```

Entrée du commutateur central

Comme mentionné précédemment, le paquet de sortie du commutateur de périphérie est un paquet d'entrée du commutateur central.

Lorsque le paquet arrive à l'interface fif 2/1/0/1, ce journal est observé.

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

L'interface Fif 2/1/0/1 est configurée comme port non approuvé pour la surveillance DHCP.

Un paquet de détection DHCP relayé de couche 3 entre par ce port. Bien que le paquet soit relayé et encapsulé au niveau de la couche 3, la surveillance DHCP l'inspecte toujours sur le port de couche 2. Comme ce port n'est pas fiable et que le paquet contient une adresse IP de passerelle (agent de relais) sans l'option 82, la surveillance DHCP abandonnera le paquet sur ce port non fiable. Ce comportement est attendu et prévu.



Remarque : Dans la plupart des cas, il apparaît que la détection DHCP est abandonnée en transit à cause de la surveillance DHCP.

Sortie du commutateur central

Dans ce cas, Central-Switch abandonne le paquet de détection DHCP et aucun paquet de détection DHCP initié par l'hôte avec l'adresse MAC 70:10:5c:df:31:e9 ne sort de l'interface Fif 2/1/0/3.

Comment résoudre le problème ?

1. Activez l'option 82 sur le premier saut du client DHCP.

Dans l'exemple actuel, configurez la commande `ip dhcp snooping information option` sur le Remote-Switch.

2. L'approbation de surveillance DHCP doit être activée sur tout le chemin DHCP du client DHCP au serveur DHCP.

Dans l'exemple actuel, configurez la commande ip dhcp snooping trust sur l'interface fif2/1/0/1 du commutateur central.

<#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

Une fois ces modifications effectuées, le paquet de détection commence à partir du commutateur central vers le serveur DHCP.

<#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

La détection atteint le serveur DHCP et le serveur DHCP répond à l'offre DHCP.

Paquet d'offre DHCP :

<#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

Le paquet d'offre auquel le serveur DHCP répond va atteindre l'interface fif2/1/0/3 du commutateur CORE/Central.

<#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

Ici, il n'y a pas d'approbation de l'extrémité de surveillance DHCP et l'OFFRE entre, alors pourquoi l'offre n'est pas abandonnée sur un port non approuvé ?

Comme vous le savez, dans un réseau où la surveillance DHCP est activée, les ports sont classés comme étant approuvés ou non approuvés.

Les ports approuvés sont connectés à des serveurs DHCP légitimes ou à d'autres commutateurs approuvés. Tous les messages DHCP y sont autorisés.

Les ports non approuvés sont généralement connectés aux périphériques des utilisateurs finaux (clients). Ils sont limités pour empêcher les attaques de type « usurpation DHCP » ou « serveur DHCP non autorisé ».

Les paquets DHCP Offer et DHCP ACK sont considérés comme des messages « côté serveur ». Selon les règles de sécurité, ces messages ne doivent provenir que d'un serveur légitime.

Lorsqu'un agent de relais DHCP ou un routeur/commutateur de couche 3 reçoit une offre DHCP sur un port de couche 2 configuré comme non approuvé, le mécanisme de surveillance DHCP identifie cette offre comme une violation de sécurité. Il suppose qu'un serveur DHCP non autorisé tente de fournir des adresses IP non autorisées aux clients sur le réseau.

Même si le paquet est monodiffusion (dirigé spécifiquement vers l'agent de relais), l'état de confiance du port physique ou logique est prioritaire. Le contrôle de sécurité est effectué au niveau du port, que le paquet soit diffusé ou monodiffusé.

Comme le port n'est pas approuvé, le système bloque l'offre DHCP pour protéger le réseau contre les données de configuration potentiellement malveillantes ou incorrectes provenant d'une source non autorisée.

Un port de couche 3 (une interface routée) fonctionne au niveau de la couche 3. Comme il s'agit d'une interface routée, il n'observe pas les règles d'approbation/non-approbation de surveillance DHCP de couche 2 qui s'appliquent aux ports de commutation.

Un client envoie une requête de diffusion. L'agent de relais (le périphérique L3) intercepte ce message et envoie une requête de monodiffusion au serveur DHCP.

Le serveur DHCP renvoie une offre DHCP de monodiffusion à l'adresse IP de l'agent relais (en particulier à l'adresse IP de la passerelle ou de la giaddr).

Lorsque le paquet arrive au port L3 de l'agent de relais ou sur n'importe quel saut L3 dans le chemin du paquet, le périphérique accepte le paquet comme trafic de routage légitime.

Contrairement au scénario précédent (un port non approuvé de couche 2), où le commutateur recherche des messages « côté serveur » provenant d'un port orienté client, le port de couche 3 agit comme la destination prévue ou le saut de couche 3 légitime pour la réponse du serveur.

Si les ports L3 abandonnent une offre de monodiffusion DHCP, le mécanisme de relais DHCP ne fonctionnera jamais, car le serveur ne pourra jamais communiquer de nouveau avec l'agent de relais.

Enfin, le paquet d'offre traverse jusqu'à ce qu'il atteigne le client.

L'hôte/client répondra avec la requête DHCP.

<#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

Le serveur DHCP enverra finalement un ACK pour l'attribution de l'adresse IP.

<#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 se termine et l'hôte reçoit l'adresse IP.

Résumé

Reportez-vous à ce tableau afin de comprendre les scénarios de transfert de paquets.

Type de port	État de confiance	Type de paquet relayé	Résultat	Motif
Port L2	Non Fiable	Offre/accusé de réception DHCP monodiffusion	Abandonné	La surveillance DHCP empêche les messages du serveur sur les ports L2 non approuvés.
Port L3	S/O (routé)	Offre/accusé de réception DHCP monodiffusion	Accepté	Les ports routés sont les noeuds prévus pour la communication de l'agent relais.
Port L2	Fiable	Détection DHCP monodiffusion avec option 82	Accepté	Le port sécurisé autorise tous les signaux DHCP.
Port L2	Non Fiable	Détection DHCP monodiffusion avec option 82	Accepté	Le paquet avec l'adresse IP de l'agent de relais et l'option 82 est légitime.
Port L2	Fiable	Détection DHCP monodiffusion sans option 82	Accepté	Le port sécurisé autorise tous les signaux DHCP.

Port L2	Non Fiable	Détection DHCP monodiffusion sans option 82	Abandonné	Le paquet avec l'adresse IP de l'agent de relais et aucune option 82 est non autorisé.
---------	---------------	---	-----------	--

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.