

Interacciones de snooping DHCP con GIADDR y opción 82 en CAT9000

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Diagrama de la red](#)

[Casos de prueba](#)

[Snooping DHCP del switch principal habilitado](#)

[Opción de switch de acceso 82 desactivada](#)

[Switch de acceso activado 82](#)

[Detección DHCP del switch principal desactivada](#)

[Switch de acceso activado 82](#)

[Opción de switch de acceso 82 desactivada](#)

[Summary](#)

Introducción

Este documento describe las interacciones de snooping DHCP con GIADDR y la opción 82 en CAT9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Competencia de Cisco IOS® XE en comandos de configuración y operativos.
- Familiaridad con la arquitectura y el hardware de los switches Catalyst de Cisco serie 9000.
- Una sólida comprensión de las operaciones del protocolo DHCP y los mecanismos de detección DHCP.
- Comprensión conceptual de la opción 82 de DHCP y la función del agente de retransmisión.

Componentes Utilizados

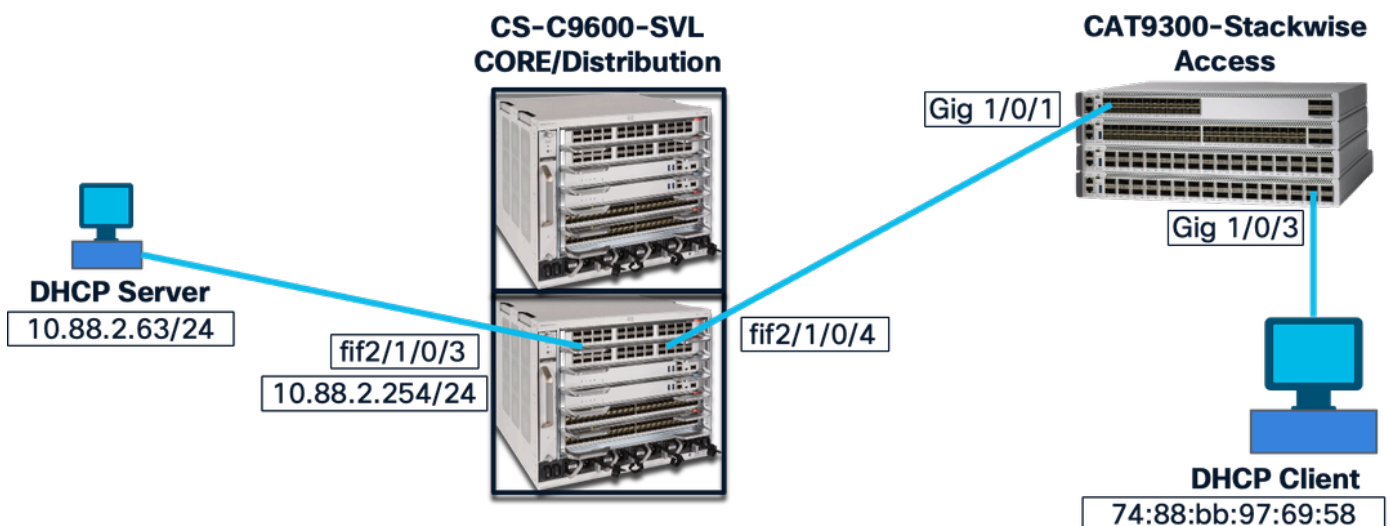
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch de núcleo/distribución: Cisco Catalyst serie 9600X
- Switch de acceso: Cisco Catalyst serie 9300
- cliente DHCP: dispositivo host final
- servidor DHCP: proveedor de servicios de red centralizada

Antecedentes

Este documento explora varias configuraciones de snooping DHCP en switches de núcleo/distribución, integradas con implementaciones de la opción DHCP 82 en switches de acceso. A través de ejemplos prácticos de configuración y análisis de las capturas de paquetes correspondientes, esta guía ilustra la interacción entre estas funciones dentro de un entorno Cisco Catalyst serie 9000.

Diagrama de la red



Casos de prueba

Snooping DHCP del switch principal habilitado

Opción de switch de acceso 82 desactivada

Switch principal:

```
<#root>
!
int f1f2/1/0/4 --> Downlink to Access Switch
ip dhcp snooping trust
!
ip dhcp snooping vlan 1-2048

ip dhcp snooping

!
```

Switch de acceso:

```
<#root>
!
int gig1/0/1 -> uplink to Core
ip dhcp snooping trust
switchport mode trunk
!
ip dhcp snooping vlan 1-1400

no ip dhcp snooping information option

ip dhcp snooping
!
int gig1/0/3 ----> End device connected port
switchport mode access
switchport access vlan 287
!
```

Resultado:

Exitoso.

El dispositivo final obtiene la dirección IP sin problemas.

Explicación:

La opción 82 del switch de acceso está inhabilitada y envía el paquete al núcleo sin la opción 82. La opción 82 del switch de núcleo está habilitada de forma predeterminada y agrega la opción 82 con la dirección IP del agente de retransmisión en el paquete y la envía al servidor DHCP.

Paquete en enlace entre el cliente y el switch de acceso:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1604
2	0.000156	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1604
3	2.002663	10.88.39.254	255.255.255.255	DHCP	363	DHCP Offer - Transaction ID 0x1604
4	2.002977	10.88.39.254	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x1604
5	2.004966	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1604
6	2.005228	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1604
7	2.007080	10.88.39.254	255.255.255.255	DHCP	363	DHCP ACK - Transaction ID 0x1604


```
> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_v
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001604
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End
```



Nota: Las capturas de paquetes se realizan varias veces y en varios puntos de captura para el mismo cliente; ignorar el id de transacción.

Paquete en enlace entre el switch de acceso y el switch de distribución/núcleo:

El switch de acceso no tiene inserción de opciones de información de indagación, por lo que el mismo paquete que proviene del cliente se reenvía al switch de distribución.

No.	Time	Source	Destination	Protocol	Length	Info
5	11.360258	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID 0x1147
6	12.858224	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8478fad8
7	12.858519	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x8478fad8
8	13.362861	10.88.39.254	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x1147
9	13.364854	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID 0x1147
10	13.469795	10.88.39.254	255.255.255.255	DHCP	359	DHCP ACK - Transaction ID 0x1147


```

> Frame 5: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_ws.
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001147
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paquete entre el switch CORE y el servidor DHCP:

A medida que se habilita la indagación DHCP y se configura la retransmisión, el switch CORE unidifusión del paquete al servidor DHCP 10.88.2.63 con IP del agente de retransmisión se inserta como su propia IP.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.88.39.254	10.88.2.63	DHCP	379	DHCP Discover - Transaction ID 0x5df
2	0.000069	10.88.2.63	10.88.39.254	DHCP	359	DHCP Offer - Transaction ID 0x5df
3	0.128743	10.88.39.254	10.88.2.63	DHCP	397	DHCP Request - Transaction ID 0x5df
4	0.128997	10.88.2.63	10.88.39.254	DHCP	359	DHCP ACK - Transaction ID 0x5df


```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmp/epc_
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000005df
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Switch de acceso activado 82

Switch principal:

<#root>

```

!
int fif2/1/0/4 --> Downlink to Access Switch
ip dhcp snooping trust
!
ip dhcp snooping vlan 1-2048

ip dhcp snooping
!

```

Switch de acceso:

<#root>

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400  
  
ip dhcp snooping information option
```

```
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Resultado:

Exitoso.

El dispositivo final obtiene la dirección IP sin problemas.

Explicación:

La opción 82 del switch de acceso está habilitada, pero este switch no tiene la SVI creada y envía el paquete al núcleo sin la opción 82. La opción 82 del switch de núcleo está habilitada de forma predeterminada y agrega la opción 82 con la dirección IP del agente de retransmisión en el paquete y la envía al servidor DHCP.

Paquete del cliente al switch de acceso:

Time	Source	Destination	Protocol	Length	Info
1 0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID
2 0.000161	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
3 1.110008	Cisco_9e:c8:c6	Broadcast	ARP	64	Who has 10.88.0.254? Tell 10.88
4 2.002486	10.88.39.254	255.255.255.255	DHCP	383	DHCP Offer - Transaction ID
5 2.002871	10.88.39.254	255.255.255.255	DHCP	379	DHCP Offer - Transaction ID
6 2.004750	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID
7 2.004994	0.0.0.0	255.255.255.255	DHCP	417	DHCP Request - Transaction ID
8 2.006887	10.88.39.254	255.255.255.255	DHCP	383	DHCP ACK - Transaction ID
9 2.108976	10.88.39.254	255.255.255.255	DHCP	379	DHCP ACK - Transaction ID

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00000121
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

El paquete del switch de acceso al switch de núcleo/distribución:

Como 'ip dhcp snooping information option' está habilitado de forma predeterminada en el switch de acceso, el switch de acceso inserta la opción 82 con relay IP como 0.0.0.0.

Según el mundo de la indagación DHCP, este es un paquete no autorizado y debe ser descartado por el switch CORE. Pero como el switch CORE tiene la interfaz confiable, el paquete será procesado para retransmitir hacia el servidor DHCP.

Time	Source	Destination	Protocol	Length	Info
2 0.000129	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction I
3 0.002398	10.88.39.254	255.255.255.255	DHCP	379	DHCP Offer - Transaction I
4 0.005010	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction I

```

> Frame 2: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000026a5
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  v Option: (82) Agent Information Option
    Length: 18
    v Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    v Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
  v Option: (255) End
    Option End: 255

```

Paquete entre el switch CORE y el servidor DHCP:

Como la interfaz de link descendente es confiable, el switch CORE reemplaza al agente relay de 0.0.0.0 a 10.88.39.254 y lo envía al link ascendente.

Además, el proceso DORA completa legítimo y el cliente obtiene la dirección IP.

Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.88.39.254	10.88.2.63	DHCP	399 DHCP Discover - Transaction ID 0x9fc
2	2.000064	10.88.2.63	10.88.39.254	DHCP	379 DHCP Offer - Transaction ID 0x9fc
3	2.003716	10.88.39.254	10.88.2.63	DHCP	417 DHCP Request - Transaction ID 0x9fc
4	2.003963	10.88.2.63	10.88.39.254	DHCP	379 DHCP ACK - Transaction ID 0x9fc

```

> Frame 1: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface /t
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000009fc
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  < Option: (82) Agent Information Option
    Length: 18
    < Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    < Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
  > Option: (255) End

```

Detección DHCP del switch principal desactivada

Switch de acceso activado 82

Switch principal:

```
<#root>
```

```
!
Int fif2/1/0/4 --> Downlink to Access Switch
no Ip dhcp snooping trust
!
```

```
no ip dhcp snooping vlan 1-2048
```

```
no ip dhcp snooping
```

```
!
```

Switch de acceso:

```
<#root>
```

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400
```

```
ip dhcp snooping information option
```

```
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Resultado:

Falla.

El dispositivo final no obtiene la dirección IP.

Explicación:

La opción de switch de acceso 82 está habilitada, pero este switch no tiene SVI ni agente de retransmisión. Por lo tanto, envía el paquete al NÚCLEO con la opción 82 y la IP de retransmisión como 0.0.0.0. A medida que se inhabilita la indagación DHCP en el switch NÚCLEO; la verificación, edición e inserción de la opción 82 está deshabilitada allí. Por lo tanto, el switch CORE no puede agregar el relé y descarta el paquete.

DHCP del cliente detecta el paquete que viene del cliente y va al switch de acceso:

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID
2	0.000187	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
3	3.223897	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID
4	7.224730	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00001617
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 000000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Flujo de paquetes desde el switch de acceso al switch de núcleo/distribución:

- El switch de acceso tiene el comando `ip dhcp snooping information option` habilitado, lo que hace que inserte la opción 82 en los paquetes DHCP. En este caso, la dirección IP del agente de retransmisión en la opción 82 se establece en 0.0.0.0.
- El switch de acceso funciona únicamente en la capa 2 para vLAN 287.
- Desde la perspectiva del switch CORE, el paquete con la opción 82 insertada por el switch de acceso se considera ilegítimo. Sin embargo, dado que la interfaz de enlace descendente en el switch CORE se configura como de confianza, el switch CORE procesa el paquete en lugar de descartarlo en el nivel de interfaz.
- El switch CORE tiene la función DHCP snooping inhabilitada, por lo que no reenvía paquetes que contengan la opción 82.

Comportamiento del switch CORE con paquetes de detección DHCP:

- El switch CORE intenta unidifusión del paquete de detección DHCP a la dirección de ayudante configurada 10.88.2.63.
- Para hacer esto, el switch CORE debe establecer la dirección IP de retransmisión (GIADDR) en el paquete DHCP.
- Dado que la opción 82 ya está presente con los datos insertados por el switch de acceso, el switch CORE debe verificar la opción 82 antes de establecer la IP de retransmisión.
- Dado que la indagación DHCP está inhabilitada en el switch CORE, no puede verificar la opción 82.
- Debido a esta incapacidad para verificar y modificar la opción 82, el switch CORE no tiene más opción que descartar el paquete de detección DHCP.

Time	Source	Destination	Protocol	Length	Info
1 0.000000	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0
2 3.974135	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0
3 7.075625	0.0.0.0	255.255.255.255	DHCP	399	DHCP Discover - Transaction ID 0

```

> Frame 1: Packet, 399 bytes on wire (3192 bits), 399 bytes captured (3192 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
√ Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000018b1
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 0000000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  √ Option: (82) Agent Information Option
    Length: 18
    √ Option 82 Suboption: (1) Agent Circuit ID
      Length: 6
      Agent Circuit ID: 0004011f0103
    √ Option 82 Suboption: (2) Agent Remote ID
      Length: 8
      Agent Remote ID: 000690eb5000eb80
  > Option: (255) End

```

El paquete de detección no se retransmitirá desde el switch CORE hacia el servidor DHCP.

Depuraciones en el switch CORE para un escenario que no funciona:

```
DHCPD: Reload workspace interface Vlan287 tableid 0.  
DHCPD: tableid for 10.88.39.254 on Vlan287 is 0  
DHCPD: client's VPN is .  
DHCPD: No option 125  
DHCPD: Option 124: Vendor Class Information  
DHCPD: Enterprise ID: 9  
DHCPD: Vendor-class-data-len: 13  
DHCPD: Data: 43~~~~~58  
DHCPD: inconsistent relay information.  
DHCPD: relay information option exists, but giaddr is zero.
```

Opción de switch de acceso 82 desactivada

Switch principal:

```
<#root>  
  
!  
int fif2/1/0/4 --> Downlink to Access Switch  
no ip dhcp snooping trust  
!  
no ip dhcp snooping vlan 1-2048  
  
no ip dhcp snooping  
  
!
```

Switch de acceso:

```
!  
int gig1/0/1 -> uplink to Core  
ip dhcp snooping trust  
switchport mode trunk  
!  
ip dhcp snooping vlan 1-1400  
no ip dhcp snooping information option  
ip dhcp snooping  
!  
int gig1/0/3  
switchport mode access  
switchport access vlan 287  
!
```

Resultado:

Exitoso.

El dispositivo final obtiene la dirección IP.

Observación:

La opción 82 del switch de acceso está inhabilitada y envía el paquete al núcleo sin la opción 82 y el switch CORE tiene la SVI presente con la retransmisión configurada. El switch CORE agrega la dirección IP de los agentes de retransmisión al paquete y lo envía al servidor DHCP.

DHCP del cliente detecta paquetes que llegan al switch de acceso:

Time	Source	Destination	Protocol	Length	Info
6	11.127914	0.0.0.0	255.255.255.255	DHCP	379 DHCP Discover - Transaction ID
7	12.467192	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
8	12.467511	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID
9	13.130633	10.88.39.254	255.255.255.255	DHCP	359 DHCP Offer - Transaction ID
10	13.132841	0.0.0.0	255.255.255.255	DHCP	397 DHCP Request - Transaction ID
11	13.236938	10.88.39.254	255.255.255.255	DHCP	359 DHCP ACK - Transaction ID

```

> Frame 6: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x00002336
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Switch de paquete a NÚCLEO desde switch de acceso:

Como la opción 82 está inhabilitada en el switch de acceso, el switch de acceso reenviará el paquete de difusión tal como está en el trunk de link ascendente.

	Time	Source	Destination	Protocol	Length	Info
6	10.652455	0.0.0.0	255.255.255.255	DHCP	379	DHCP Discover - Transaction ID
7	11.292839	Cisco_9e:c8:c6	Broadcast	ARP	64	Who has 10.88.0.254? Tell 10.8
8	12.653654	10.88.39.254	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID
9	12.655561	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID
10	12.655730	0.0.0.0	255.255.255.255	DHCP	397	DHCP Request - Transaction ID
11	12.760079	10.88.39.254	255.255.255.255	DHCP	359	DHCP ACK - Transaction ID

```

> Frame 6: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface
> Ethernet II, Src: Cisco_97:69:58 (74:88:bb:97:69:58), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
< Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x000003fd
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Paquete transmitido por el switch CORE hacia el servidor DHCP:

Time	Source	Destination	Protocol	Length	Info
1 0.000000	10.88.39.254	10.88.2.63	DHCP	379	DHCP Discover - Transaction ID 0x271
2 0.000139	10.88.2.63	10.88.39.254	DHCP	359	DHCP Offer - Transaction ID 0x271
3 0.463381	10.88.39.254	10.88.2.63	DHCP	397	DHCP Request - Transaction ID 0x271
4 0.463628	10.88.2.63	10.88.39.254	DHCP	359	DHCP ACK - Transaction ID 0x271

```

> Frame 1: Packet, 379 bytes on wire (3032 bits), 379 bytes captured (3032 bits) on interface /tmj
> Ethernet II, Src: Cisco_de:46:05 (08:f3:fb:de:46:05), Dst: Cisco_f3:6c:e4 (00:aa:6e:f3:6c:e4)
> Internet Protocol Version 4, Src: 10.88.39.254, Dst: 10.88.2.63
> User Datagram Protocol, Src Port: 67, Dst Port: 67
√ Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x00000271
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  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: 10.88.39.254
  Client MAC address: Cisco_97:69:58 (74:88:bb:97:69:58)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (57) Maximum DHCP Message Size
  > Option: (61) Client identifier
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  > Option: (60) Vendor class identifier
  > Option: (124) V-I Vendor Class
  > Option: (255) End

```

Depuraciones en el switch CORE:

```

Option 82 not present
DHCPD: Reload workspace interface Vlan287 tableid 0.
DHCPD: tableid for 10.88.39.254 on Vlan287 is 0
DHCPD: client's VPN is .
DHCPD: No option 125
DHCPD: No option 124
DHCPD: FSM state change INVALID
DHCPD: Workspace state changed from INIT to INVALID
DHCPD: Finding a relay for client ~~~~ on interface Vlan287.
DHCPD : Locating relay for Subnet 10.88.39.254
DHCPD: there is no pool for 10.88.39.254.
DHCPD: Looking up binding using address 10.88.39.254
DHCPD: setting giaddr to 10.88.39.254

```

En este caso, el cliente recibe la dirección IP.

Summary

- El snooping DHCP debe estar habilitado para que el switch inserte, quite o valide la información de la opción DHCP 82.
- Cuando se inhabilita la indagación DHCP, el switch no realiza las funciones de inserción o extracción de la opción 82.
- El procesamiento de la opción 82, que incluye descartar o permitir paquetes con la opción 82, depende de que se habilite y configure la indagación DHCP.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).