Resolución de problemas de DHCP en switches Catalyst 9000

Contenido

Introducción

Este documento describe cómo resolver problemas de DHCP en switches Catalyst 9000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Arquitectura de los switches Catalyst serie 9000.
- Protocolo de configuración dinámica de host (DHCP).

Componente utilizado

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

- C9200
- C9300
- C9500
- C9400
- C9600

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

- Catalyst 3650/3850 Series Switches con Cisco IOS® XE 16.x.

Resolución de problemas

Cuando está resolviendo problemas de DHCP, hay información crítica que debe ser confirmada para aislar el origen del problema. Es muy importante dibujar una topología de la red desde el origen hasta el destino e identificar los dispositivos intermedios y sus funciones.

En función de estas funciones, hay acciones que se pueden llevar a cabo para iniciar la solución de problemas.

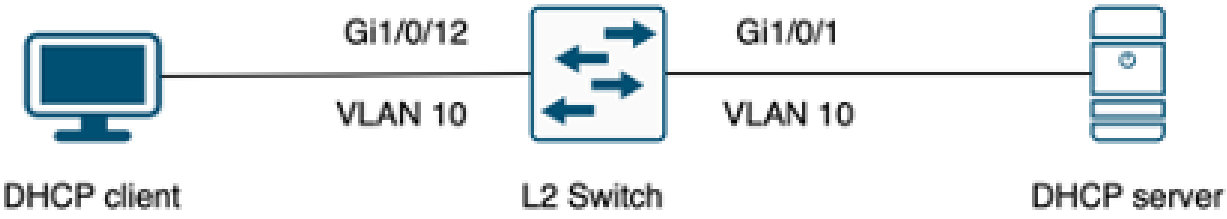
Switch configurado como puente de capa 2

En este escenario, se espera que el switch reciba y reenvíe el paquete DHCP sin ninguna modificación.

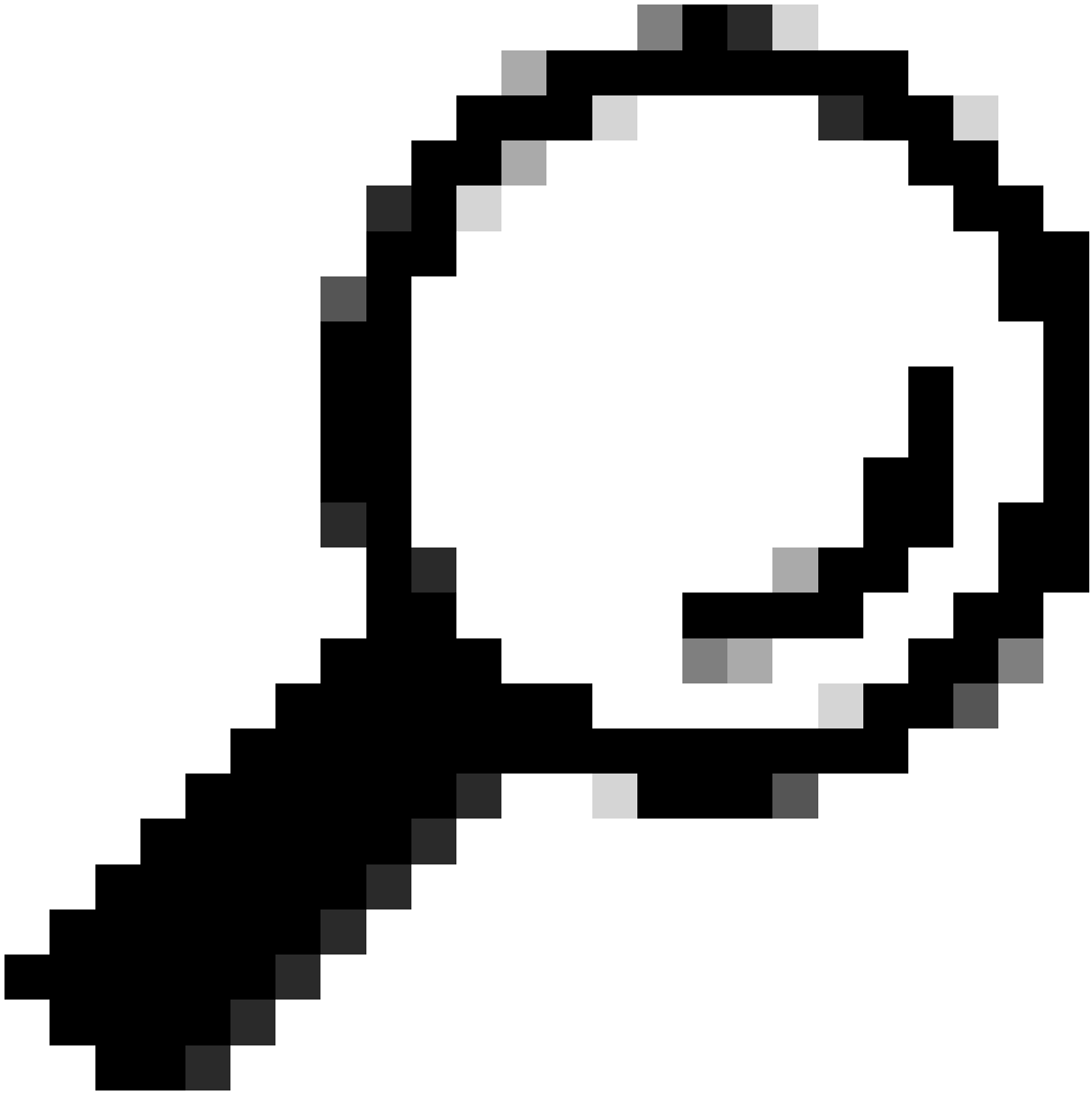
Paso 1. Confirme la trayectoria del paquete.

- Identifique las interfaces a las que están conectados el cliente y el dispositivo de salto siguiente hacia el servidor DHCP.
- Identifique la VLAN o VLAN afectadas.

Ejemplo: considere la topología siguiente, donde el cliente conectado a la interfaz Gigabit Ethernet1/0/12 en VLAN 10 en un switch C9300 no puede tomar una dirección IP a través de DHCP. El servidor DHCP está conectado en la interfaz Gigabit Ethernet1/0/1 también en la VLAN 10.



Cliente conectado a un switch de Capa 2.



Sugerencia: si el problema afecta a varios dispositivos y VLAN, elija un cliente para llevar a cabo la resolución de problemas.

Paso 2. Verifique el trayecto de la capa 2

- La VLAN debe crearse y estar activa en el switch.

<#root>

```
c9300#show vlan brief

VLAN Name                             Status    Ports

---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24

10   users                            active    Gi1/0/12


1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- La VLAN debe estar permitida en las interfaces de ingreso y egreso.

<#root>

```
interface GigabitEthernet1/0/12
 description Client Port

 switchport access vlan 10


 switchport mode access

interface GigabitEthernet1/0/1
 description DHCP SERVER

 switchport mode trunk
```

<#root>

```
c9300#show interfaces trunk

Port          Mode             Encapsulation  Status        Native vlan
Gi1/0/1       on               802.1q         trunking      1

Port          Vlans allowed on trunk
Gi1/0/1       1-4094

Port          Vlans allowed and active in management domain
Gi1/0/1       1,
```

```
10


Port            Vlans in spanning tree forwarding state and not pruned


Gi1/0/1         1,10
```

- El switch debe aprender la dirección MAC del cliente en la VLAN correcta.

```
c9300-01#show mac address interface gi1/0/12
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    7018.a7e8.4f46    DYNAMIC     Gi1/0/12
```

- Si se configura la indagación DHCP, asegúrese de que la interfaz de confianza esté configurada correctamente.

Paso 3. Asegúrese de que el switch esté recibiendo los paquetes de detección DHCP en el puerto del cliente.

- Puede utilizar la herramienta Embedded Packet Capture (EPC).
- Para filtrar sólo los paquetes DHCP, configure una ACL.

```
c9300(config)#ip access-list extended DHCP
c9300(config-ext-nacl)#permit udp any any eq 68
c9300(config-ext-nacl)#permit udp any any eq 67
c9300(config-ext-nacl)#end

c9300#show access-lists DHCP
Extended IP access list DHCP
    10 permit udp any any eq bootpc
    20 permit udp any any eq bootps
```

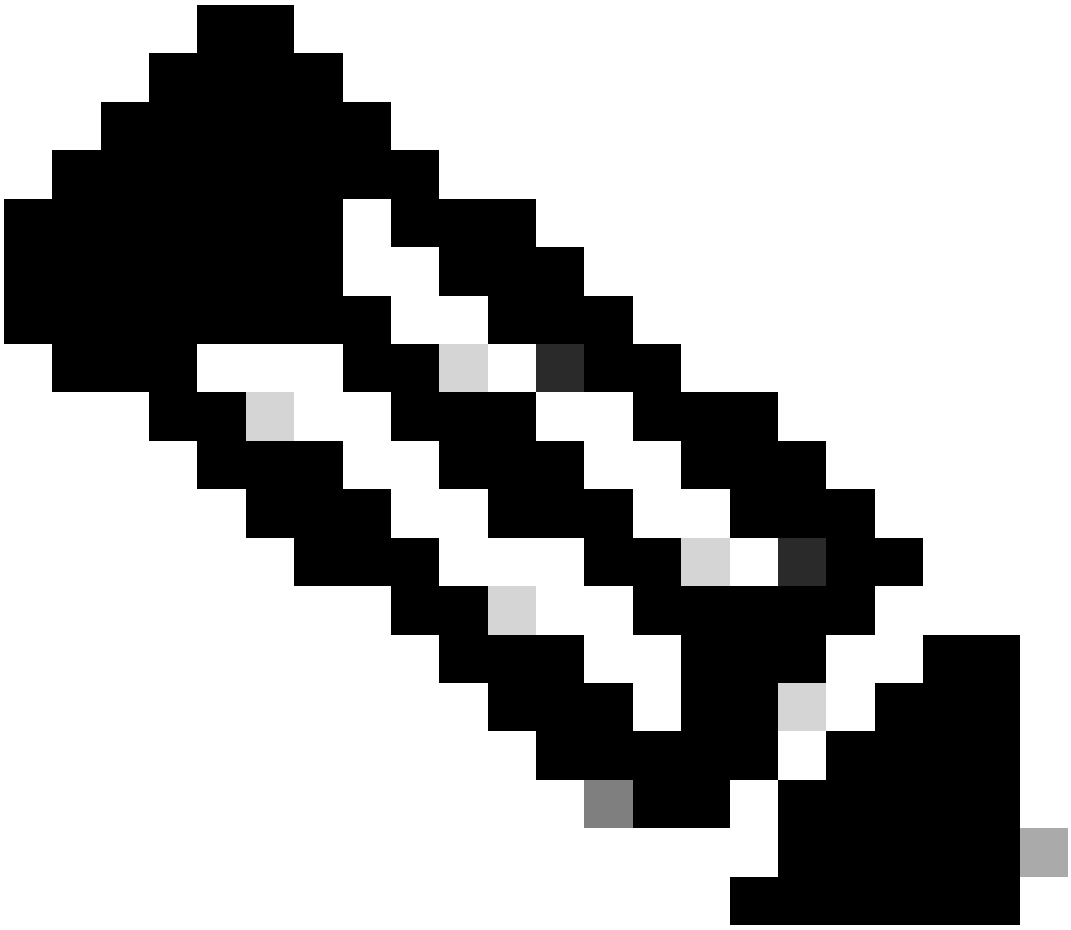
- Configure e inicie la captura de paquetes en dirección entrante en el puerto del cliente.

```
c9300#monitor capture cap interface GigabitEthernet1/0/12 in access-list DHCP
c9300#monitor capture cap start
Started capture point : cap

c9300#monitor capture cap stop
Capture statistics collected at software:
```

```
        Capture duration - 66 seconds
        Packets received - 5
        Packets dropped - 0
        Packets oversized - 0

Bytes dropped in asic - 0

Stopped capture point : cap
```

- Verifique el contenido de la captura.

```
c9300#show monitor capture cap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x9358003
2   3.653608      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x935800
```

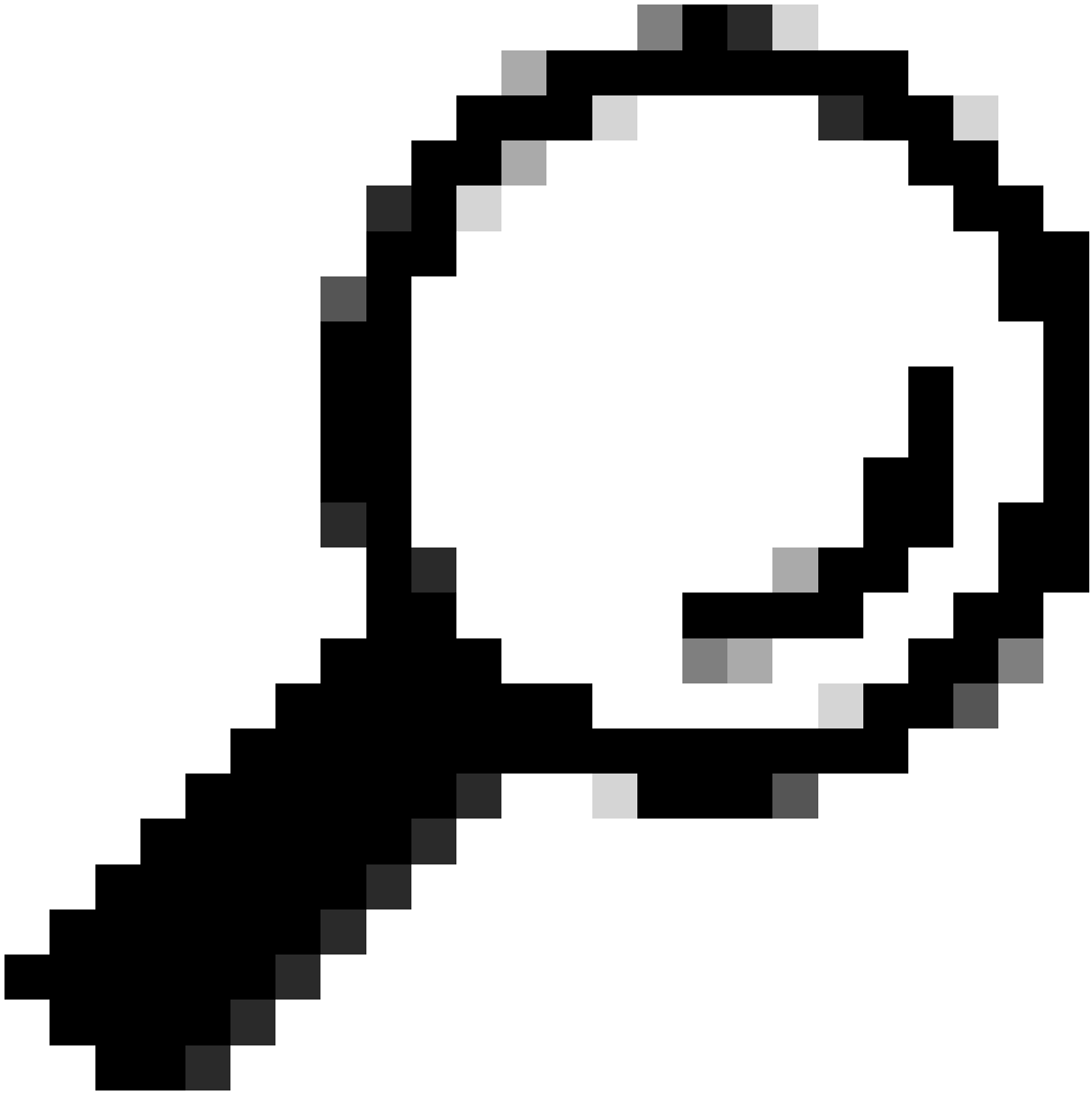


Nota: En circunstancias normales, si toma un EPC en AMBAS direcciones en el puerto del cliente, puede ver el proceso DORA completado.

Paso 4. Asegúrese de que el switch esté reenviando la detección DHCP.

- Puede realizar una captura en el puerto de salida en dirección saliente.

```
c9300#monitor capture cap interface GigabitEthernet1/0/1 out access-list DHCP
c9300#show monitor capture cap buffer brief
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

1   0.000000      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x4bf2a30e
2   0.020893      0.0.0.0 -> 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xe4331741
```



Sugerencia: Para confirmar que la detección DHCP recopilada en la captura pertenece al cliente que está resolviendo problemas, puede aplicar el filtro dhcp.hw.mac_addr al EPC usando la opción display-filter.

Llegados a este punto, hemos confirmado que el switch está reenviando los paquetes DHCP y que la resolución de problemas se puede trasladar al servidor DHCP.

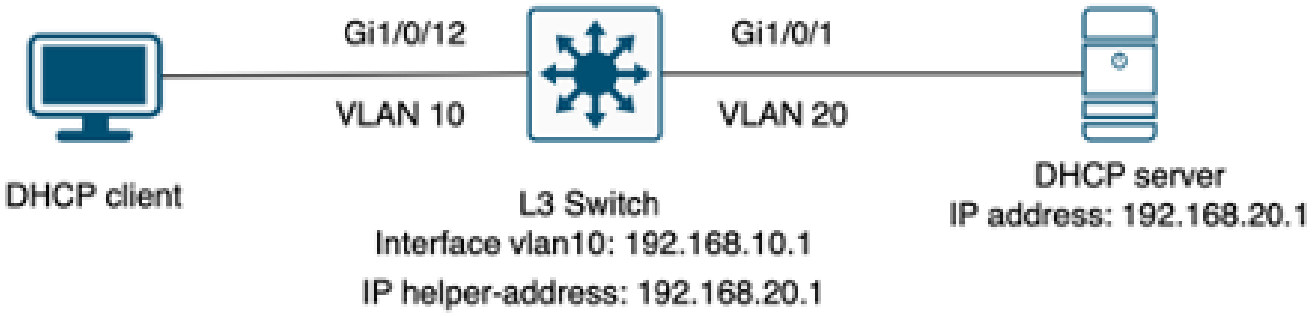
Switch configurado como agente de retransmisión

El agente de retransmisión se utiliza cuando los clientes y los servidores DHCP no pertenecen al mismo dominio de difusión.

Cuando el switch se configura como agente de retransmisión, los paquetes DHCP se modifican en el switch; para los paquetes enviados desde el cliente, el switch agrega su propia información

(dirección IP y dirección MAC) al paquete y lo envía al siguiente salto hacia el servidor DHCP. Los paquetes recibidos del servidor DHCP se dirigen al Agente Relay y luego el switch los reenvía al cliente.

Continúe con el ejemplo en el escenario anterior, tenemos un cliente conectado a la interfaz Gigabitethernet1/0/12 en la VLAN 10 que no puede obtener una dirección IP a través de DHCP, ahora el switch C9000 es el gateway predeterminado para la VLAN 10 y está configurado como agente de retransmisión, el servidor DHCP está conectado a la interfaz Gigabitethernet1/0/1 en la VLAN 20.



Cliente conectado a un switch de Capa 3 configurado como agente de retransmisión.

Paso 1. Confirme que el switch está recibiendo la detección de DHCP.

- Ejecute una captura de paquetes en la interfaz de cara al cliente. Consulte el paso 3 del escenario anterior.

Paso 2. Verifique la configuración del ayudante IP.

- El servicio DHCP debe estar activado.

```
show run all | in dhcp
service dhcp
```

- Comando IP helper bajo la VLAN 10 SVI.

<#root>

```
interface vlan10
 ip address 192.168.10.1 255.255.255.0

ip helper-address 192.168.20.1
```

Paso 3. Compruebe la conectividad con los servidores DHCP.

- El switch debe tener conectividad de unidifusión al servidor DHCP desde la VLAN del cliente. Puede probar con un ping.

```
c9300-01#ping 192.168.20.1 source vlan 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Paso 4. Confirme que el switch esté reenviando los paquetes DHCP al salto siguiente.

- Puede ejecutar un comando debug ip dhcp server packet detail.

<#root>

```
*Feb  2 23:14:20.435: DHCPD: tableid for 192.168.10.1 on Vlan10 is 0
*Feb  2 23:14:20.435: DHCPD: client's VPN is .
*Feb  2 23:14:20.435: DHCPD: No option 125
*Feb  2 23:14:20.435: DHCPD: No option 124
*Feb  2 23:14:20.435: DHCPD: Option 125 not present in the msg.
*Feb  2 23:14:20.435: DHCPD: using received relay info.
*Feb  2 23:14:20.435: DHCPD: Looking up binding using address 192.168.10.1
*Feb  2 23:14:20.435:
```

DHCPD: setting giaddr to 192.168.10.1.

```
*Feb  2 23:14:20.435:
```

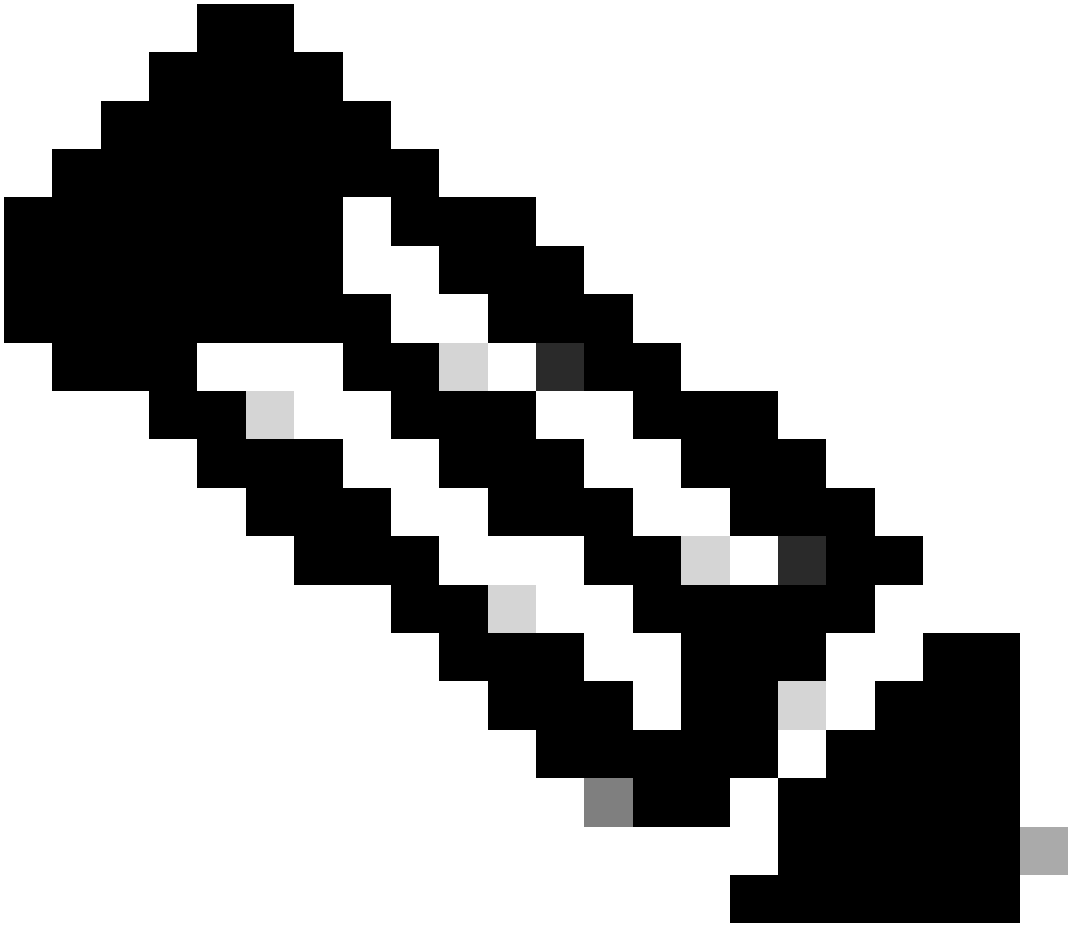
DHCPD: BOOTREQUEST from 0170.18a7.e84f.46 forwarded to 192.168.20.1.

- Tome capturas de paquetes. Puede utilizar EPC en el plano de control.

```
monitor capture cap control-plane both access-list DHCP
monitor capture cap [start | stop]
```

- También puede tomar un SPAN en el puerto de salida.

```
Monitor session 1 source interface Gi1/0/1 tx
Monitor session 1 destination interface [interface ID] encapsulation replicate
```



Nota: Debe configurar sólo un agente de retransmisión en la ruta.

Switch configurado como servidor DHCP

En este escenario, el switch tiene el alcance DHCP configurado localmente.

Paso 1. Compruebe la configuración básica.

- Se debe crear el conjunto y configurar la red, la máscara de subred y el router predeterminado.

```
ip dhcp pool VLAN10
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
```

- Los servicios DHCP deben estar activados.

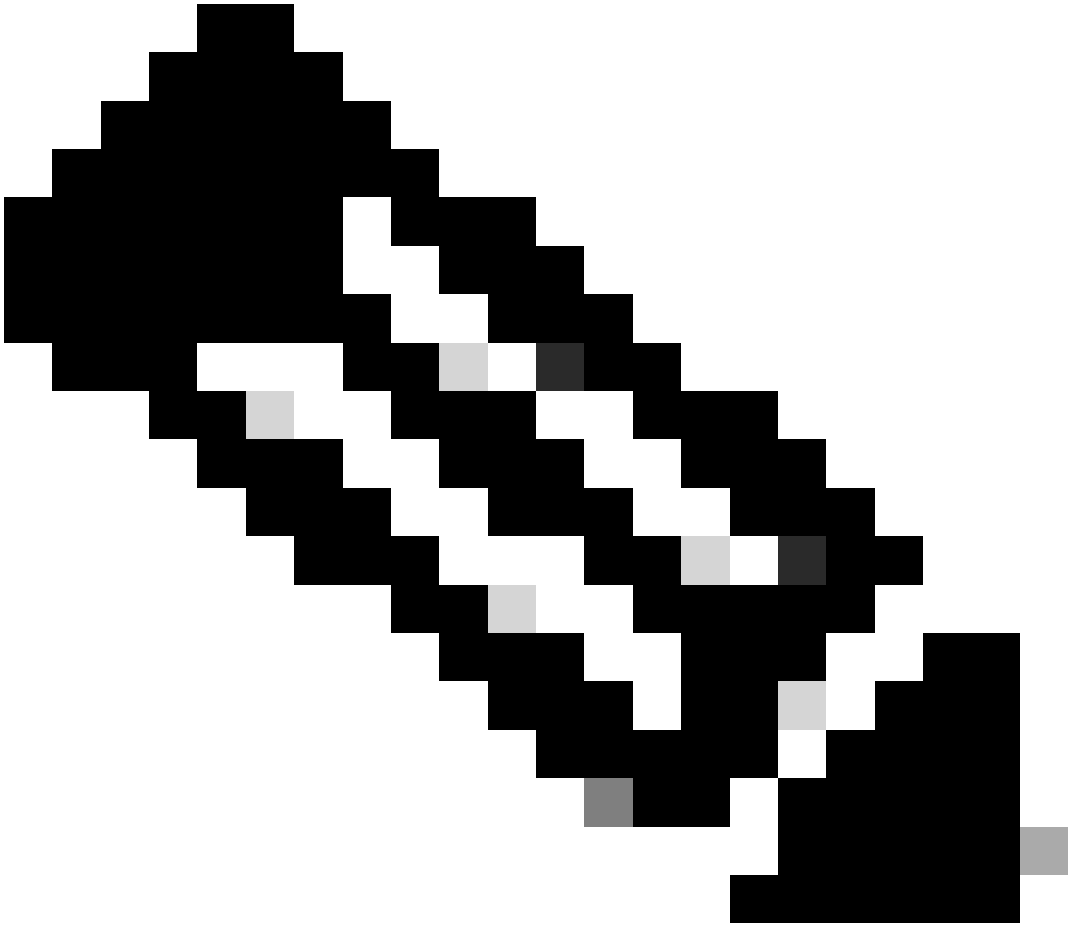
```
show run all | in dhcp
service dhcp
```

- El switch debe tener conectividad de unidifusión a las redes configuradas en los grupos.

```
ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- Todas las direcciones IP configuradas estáticamente deben excluirse del rango del conjunto.

```
ip dhcp excluded-address 192.168.10.1
```

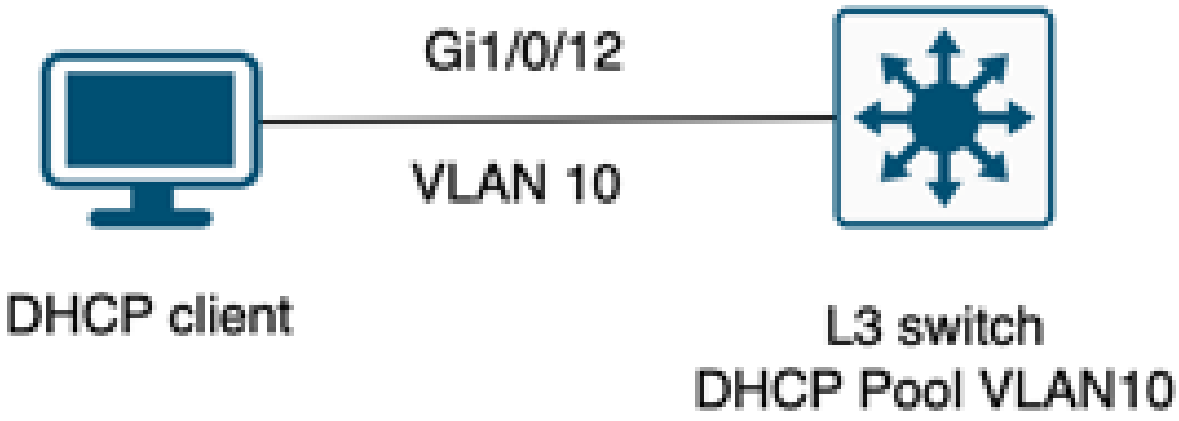


Nota: El servicio DHCP debe estar habilitado si el switch está configurado como servidor DHCP o agente de retransmisión.

Paso 2. Verifique que el switch arriende direcciones IP.

- Puede utilizar debug ip dhcp server packet detail.

Ejemplo 1: El cliente se conecta directamente al switch Catalyst 9000 configurado como servidor DHCP en la VLAN 10.



Cliente conectado a un switch de Capa 3 configurado como servidor DHCP.

<#root>

Feb 16 19:03:33.828:

DHCPD: DHCPDISCOVER received from client

0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

on interface Vlan10.DHCPD: Setting only requested parameters

*Feb 16 19:03:33.828: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.828:

DHCPD: egress Interfce Vlan10

*Feb 16 19:03:33.828:

DHCPD: broadcasting BOOTREPLY to client 9c54.16b7.7d64.

*Feb 16 19:03:33.828: Option 82 not present
*Feb 16 19:03:33.828: DHCPD: tableid for 192.168.10.1 on Vlan10 is 0
*Feb 16 19:03:33.828: DHCPD: client's VPN is .
*Feb 16 19:03:33.828: DHCPD: No option 125
*Feb 16 19:03:33.828: DHCPD: Option 124: Vendor Class Information
*Feb 16 19:03:33.828: DHCPD: Enterprise ID: 9
*Feb 16 19:03:33.829: DHCPD: Vendor-class-data-len: 10
*Feb 16 19:03:33.829: DHCPD: Data: 4339333030582D313259
*Feb 16 19:03:33.829:

DHCPD: DHCPREQUEST received from client

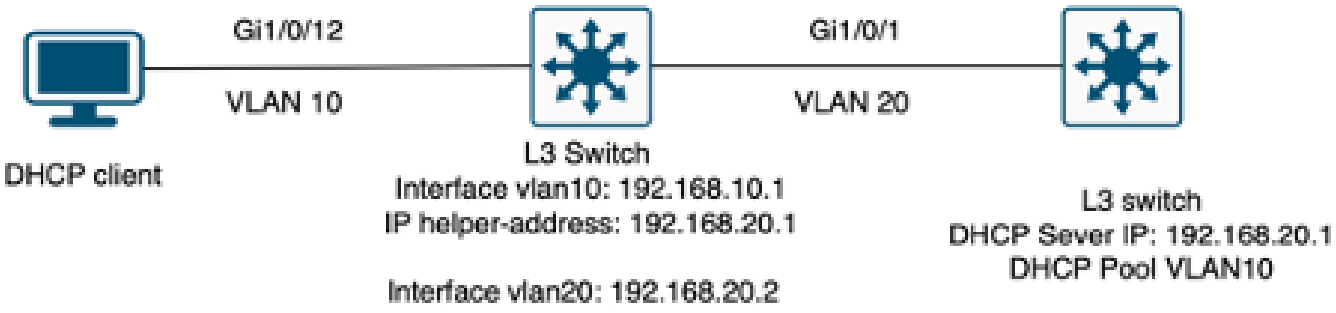
0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

on interface Vlan10

```
*Feb 16 19:03:33.829: DHCPD: Client is Selecting (

DHCP Request with Requested IP = 192.168.10.2

,

Server ID = 192.168.10.1

)
*Feb 16 19:03:33.829: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.829: DHCPD: No default domain to append - abort updateDHCPD: Setting only requested pa
*Feb 16 19:03:33.829: DHCPD: Option 125 not present in the msg.
*Feb 16 19:03:33.829: DHCPD: egress Interfce Vlan10
*Feb 16 19:03:33.829:

DHCPD: broadcasting BOOTREPLY to client 9c54.16b7.7d64
```

Ejemplo 2: el cliente no está conectado directamente al switch Catalyst 9000 configurado como servidor DHCP.

En este escenario, el cliente está conectado a un switch L3 que está configurado como gateway predeterminado y agente de retransmisión, y el servidor DHCP está alojado en un switch Catalyst 9000 vecino en VLAN 20.



El cliente no está conectado directamente al switch de capa 3 que funciona como servidor DHCP.

<#root>

```
*Feb 16 19:56:35.783: DHCPD:

DHCPDISCOVER received from client

 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

through relay 192.168.10.1.


*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.783: Option 82 not present
*Feb 16 19:56:35.783: Option 82 not present
*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.DHCPD: Setting only requested parameters
*Feb 16 19:56:35.783: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.783: DHCPD:

egress Interfce Vlan20
```

```
*Feb 16 19:56:35.783: DHCPD:
```

unicasting BOOTREPLY for client 9c54.16b7.7d64 to relay 192.168.10.1.

```
*Feb 16 19:56:35.785: Option 82 not present
*Feb 16 19:56:35.785: DHCPD: tableid for 192.168.20.1 on Vlan20 is 0
*Feb 16 19:56:35.785: DHCPD: client's VPN is .
*Feb 16 19:56:35.785: DHCPD: No option 125
*Feb 16 19:56:35.785: DHCPD: Option 124: Vendor Class Information
*Feb 16 19:56:35.785:   DHCPD: Enterprise ID: 9
*Feb 16 19:56:35.785:   DHCPD: Vendor-class-data-len: 10
*Feb 16 19:56:35.785:   DHCPD: Data: 4339333030582D313259
*Feb 16 19:56:35.785: DHCPD:
```

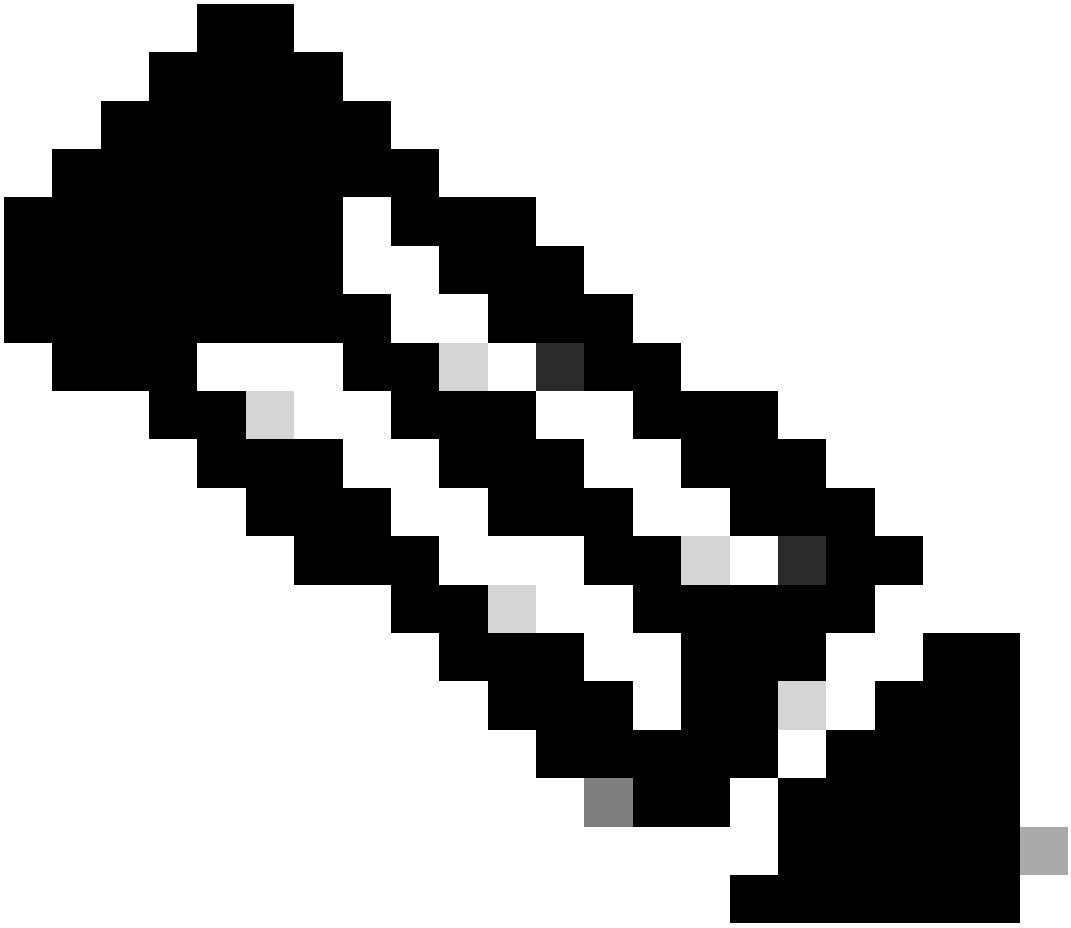
DHCPREQUEST received from client

```
 0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31 on interface Vlan20
*Feb 16 19:56:35.785: DHCPD: Client is Selecting (
```

DHCP Request with Requested IP = 192.168.10.2, Server ID = 192.168.20.1

```
)
*Feb 16 19:56:35.785: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.785: DHCPD: No default domain to append - abort updateDHCPD: Setting only requested pa
*Feb 16 19:56:35.785: DHCPD: Option 125 not present in the msg.
*Feb 16 19:56:35.785: DHCPD: egress Interfce Vlan20
*Feb 16 19:56:35.785:
```

DHCPD: unicasting BOOTREPLY for client 9c54.16b7.7d64 to relay 192.168.10.1.



Nota: Si el switch está configurado como servidor DHCP y agente de retransmisión para la misma VLAN, el servidor DHCP tiene prioridad.

Información Relacionada

- Configuración de DHCP
- Configuración de Captura de Paquetes Integrada
- Configuración de SPAN

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).