Identificar e Solucionar Problemas de DHCP nos Catalyst 9000 Switches

Contents

Introdução

Este documento descreve como solucionar problemas de DHCP nos switches Catalyst 9000.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Arquitetura dos switches Catalyst 9000 Series.
- DHCP (Dynamic Host Configuration Protocol).

Componente usado

As informações neste documento são baseadas nestas versões de software e hardware:

- C9200
- C9300
- C9500
- C9400
- C9600

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

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

Troubleshooting

Ao solucionar problemas de DHCP, há informações críticas que devem ser confirmadas para isolar a origem do problema. É muito importante desenhar uma topologia da rede da origem ao destino e identificar os dispositivos intermediários e suas funções.

Com base nessas funções, há ações que podem ser tomadas para iniciar a solução de problemas.

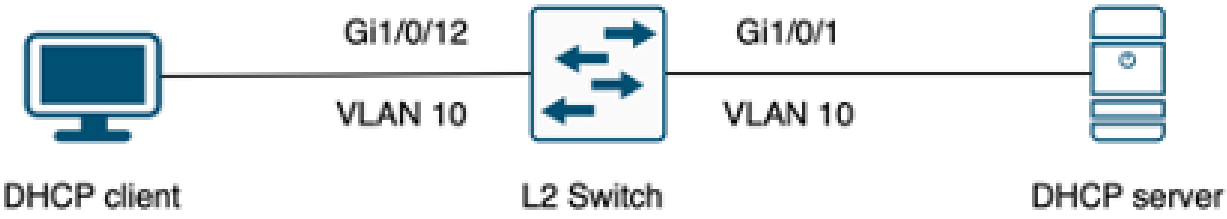
Switch configurado como bridge de camada 2

Neste cenário, espera-se que o switch receba e encaminhe o pacote DHCP sem qualquer modificação.

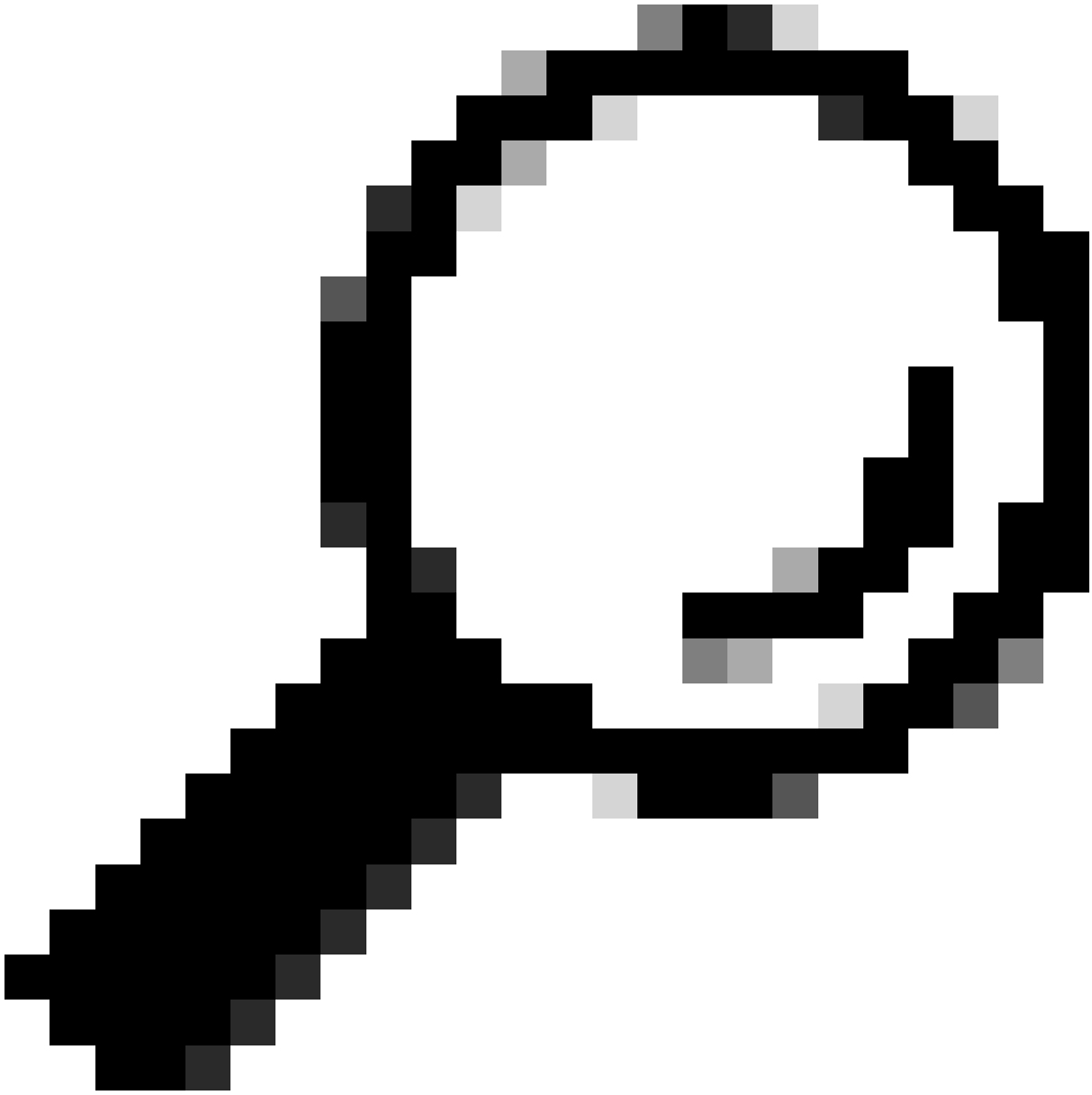
Etapa 1. Confirme o caminho do pacote.

- Identifique as interfaces onde o cliente e o dispositivo do próximo salto em direção ao servidor DHCP estão conectados.
- Identifique a VLAN ou as VLANs afetadas.

Exemplo: Considere a topologia abaixo, onde o cliente conectado à interface Gigabitethernet1/0/12 na VLAN 10 em um switch C9300 não pode obter um endereço IP via DHCP. O servidor DHCP está conectado à interface Gigabit Ethernet1/0/1 também na VLAN 10.



Cliente conectado a um switch de Camada 2.



Dica: se o problema estiver afetando vários dispositivos e VLANs, escolha um cliente para executar a solução de problemas.

Etapa 2. Verificar o caminho da camada 2

- A VLAN precisa ser criada e estar ativa no 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
```

- A VLAN deve ser permitida nas interfaces de entrada e saída.

<#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
```

- O switch deve aprender o endereço mac do cliente na VLAN correta.

```
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
```

- Se o rastreamento de DHCP estiver configurado, verifique se a interface de confiança está definida corretamente.

Etapa 3. Verifique se o switch está recebendo os pacotes de descoberta DHCP na porta do cliente.

- Você pode usar a ferramenta EPC (Embedded Packet Capture).
- Para filtrar apenas os pacotes DHCP, configure uma 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
```

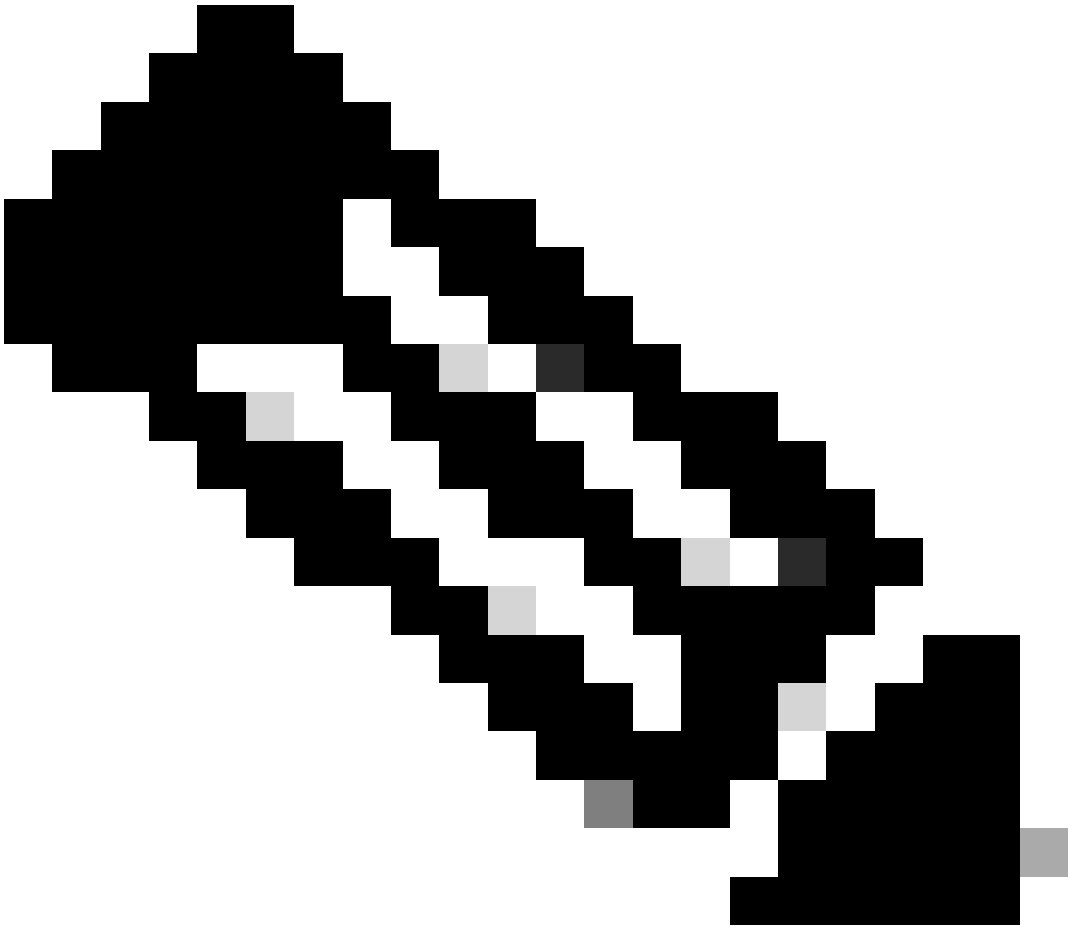
- Configure e inicie a captura de pacotes na direção de entrada na porta do cliente.

```
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 o conteúdo da 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
```

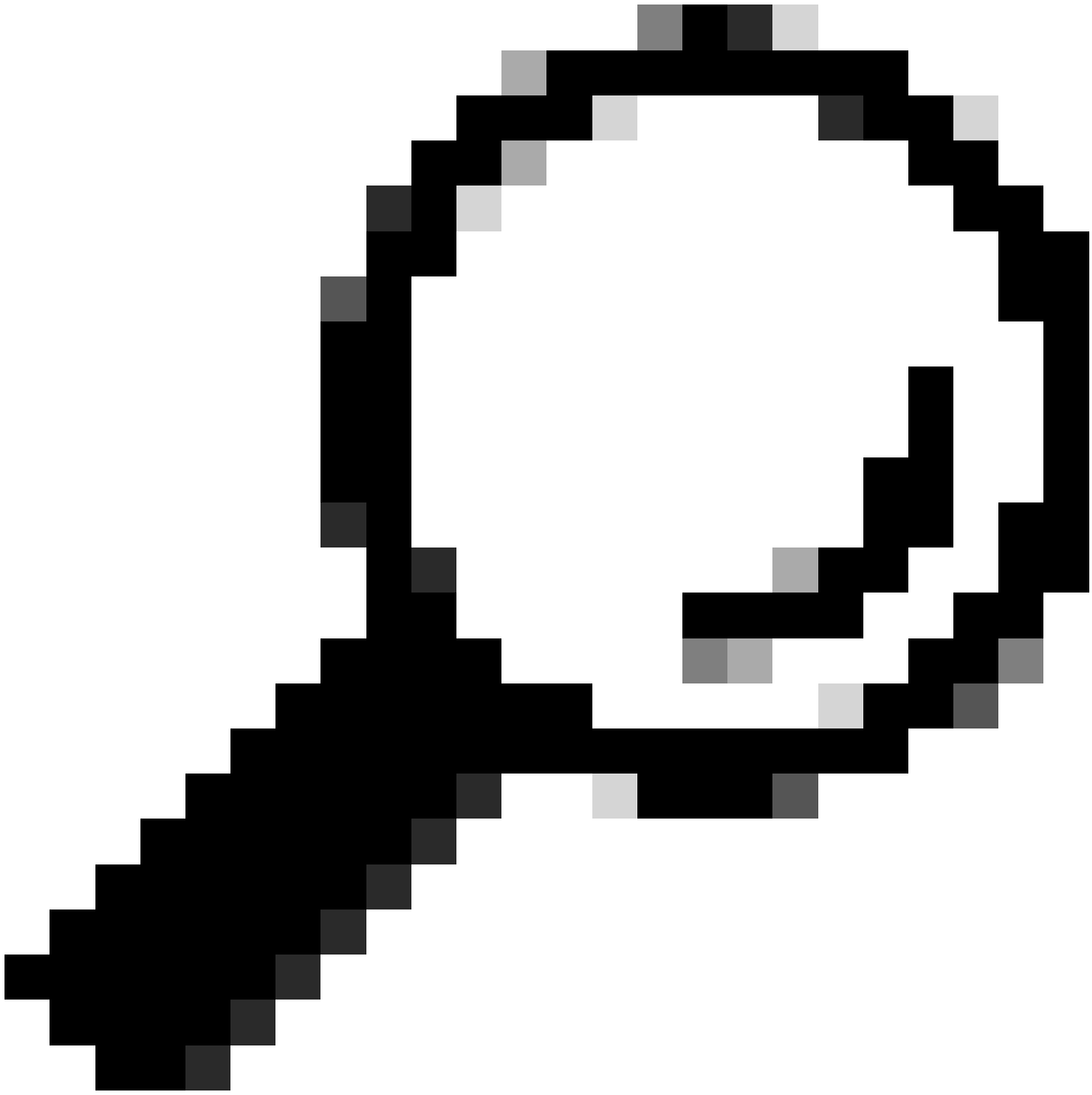


Observação: em circunstâncias normais, se você pegar um EPC em AMBAS as direções na porta do cliente, poderá ver o processo DORA concluído.

Etapa 4. Verifique se o switch está encaminhando a descoberta de DHCP.

- Você pode fazer uma captura na porta de saída na direção de saída.

```
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
```



Dica: para confirmar se a descoberta de DHCP coletada na captura pertence ao cliente que está sendo solucionado, você pode aplicar o filtro dhcp.hw.mac_addr ao EPC usando a opção display-filter.

Neste ponto, confirmamos que o switch está encaminhando os pacotes DHCP e a solução de problemas pode ser movida para o servidor DHCP.

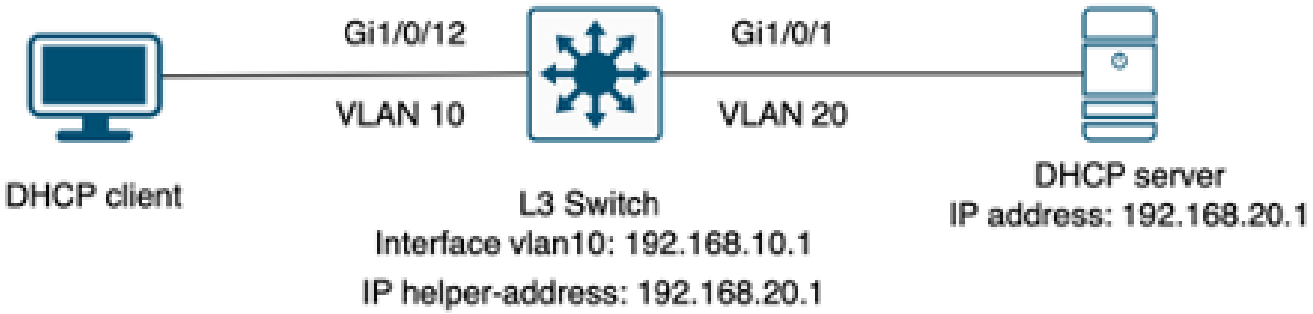
Switch configurado como agente de retransmissão

O Agente de Retransmissão é usado quando os clientes e os servidores DHCP não pertencem ao mesmo domínio de broadcast.

Quando o switch é configurado como Agente de Retransmissão, os pacotes DHCP são modificados no switch; para pacotes enviados do cliente, o switch adiciona suas próprias

informações (endereço IP e endereço MAC) ao pacote e as envia para o próximo salto em direção ao Servidor DHCP. Os pacotes recebidos do servidor DHCP são apontados para o agente de retransmissão e, em seguida, o switch os encaminha de volta para o cliente.

Continue com o exemplo no cenário anterior, temos um cliente conectado à interface Gigabitethernet1/0/12 na VLAN 10 incapaz de obter um endereço IP através de DHCP, agora o switch C9000 é o gateway padrão para a VLAN 10 e é configurado como Agente de Retransmissão, o servidor DHCP é conectado à interface Gigabitethernet1/0/1 na VLAN 20.



Cliente conectado a um switch de Camada 3 configurado como Agente de Retransmissão.

Etapa 1. Confirme se o switch está recebendo a descoberta DHCP.

- Execute uma captura de pacote na interface voltada para o cliente. Consulte a etapa 3 no cenário anterior.

Etapa 2. Verifique a configuração do auxiliar de IP.

- O serviço DHCP deve estar habilitado.

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

- Comando IP helper na VLAN 10 SVI.

<#root>

```
interface vlan10
 ip address 192.168.10.1 255.255.255.0

ip helper-address 192.168.20.1
```

Etapa 3. Verifique a conectividade com os servidores DHCP.

- O switch deve ter conectividade unicast com o servidor DHCP a partir da VLAN cliente. Você pode testar com um 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
```

Etapa 4. Confirme se o switch está encaminhando os pacotes DHCP para o próximo salto.

- Você pode executar um 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:
```

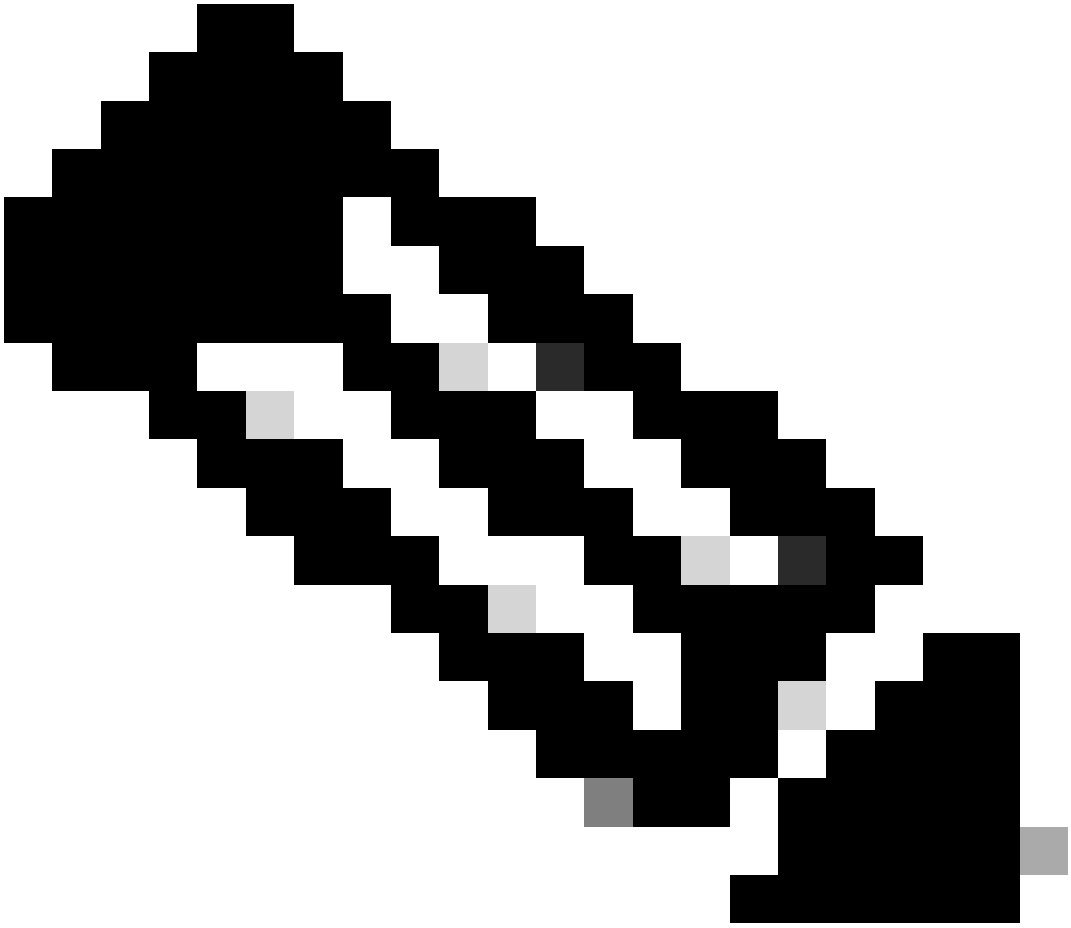
DHCPD: BOOTREQUEST from 0170.18a7.e84f.46 forwarded to 192.168.20.1.

- Faça capturas de pacotes. Você pode usar EPC no plano de controle.

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

- Você também pode obter um SPAN na porta de saída.

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



Observação: você deve configurar apenas um agente de retransmissão no caminho.

Switch configurado como servidor DHCP

Neste cenário, o switch tem o escopo DHCP configurado localmente.

Etapa 1. Verifique a configuração básica.

- O pool deve ser criado e ter a rede, a máscara de sub-rede e o roteador padrão configurados.

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

- Os serviços DHCP devem ser ativados.

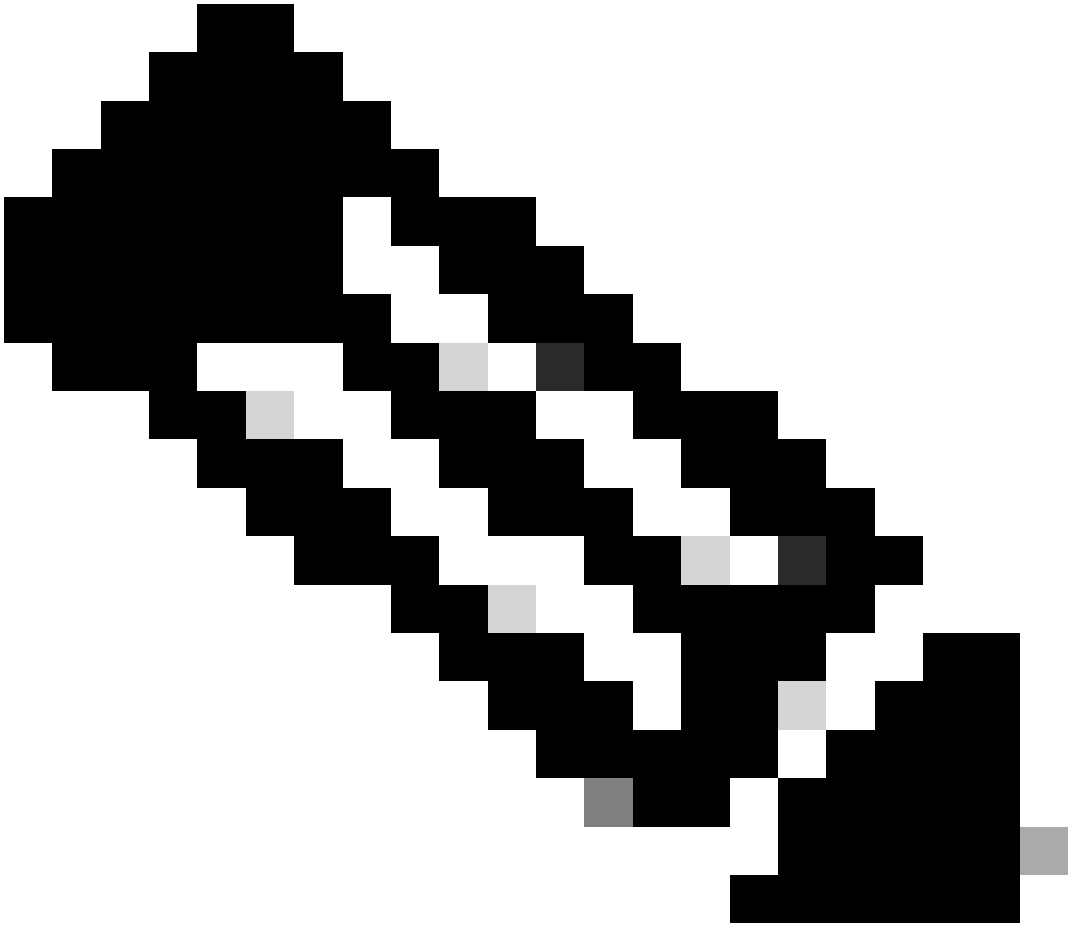
```
show run all | in dhcp
service dhcp
```

- O switch deve ter conectividade unicast com as redes configuradas nos pools.

```
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
```

- Todos os endereços IP configurados estaticamente devem ser excluídos do intervalo do pool.

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

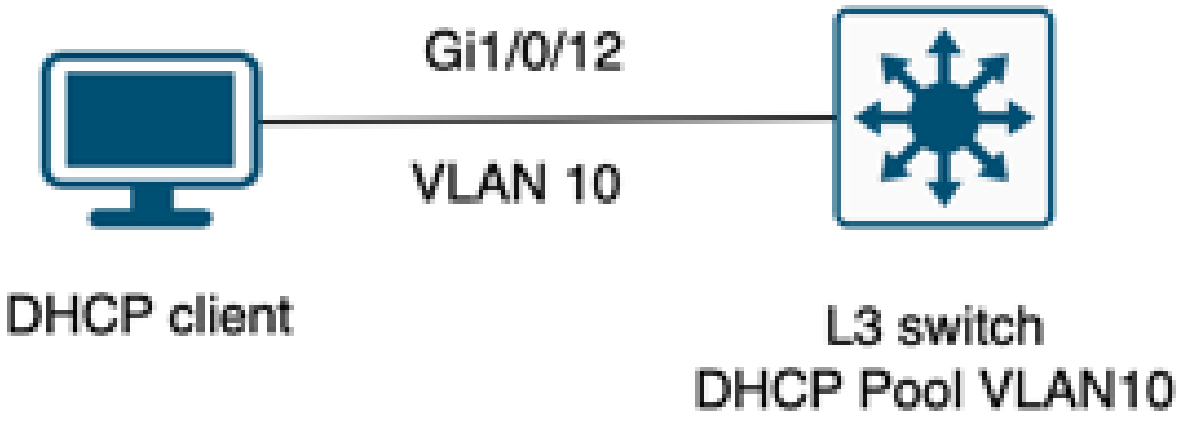


Observação: o serviço DHCP deverá ser habilitado se o switch estiver configurado como servidor DHCP ou agente de retransmissão.

Etapa 2. Verifique se o switch aluga endereços IP.

- Você pode usar debug ip dhcp server packet detail.

Exemplo 1: O cliente é conectado diretamente ao switch Catalyst 9000 configurado como servidor DHCP na VLAN 10.



Cliente conectado a um switch de Camada 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

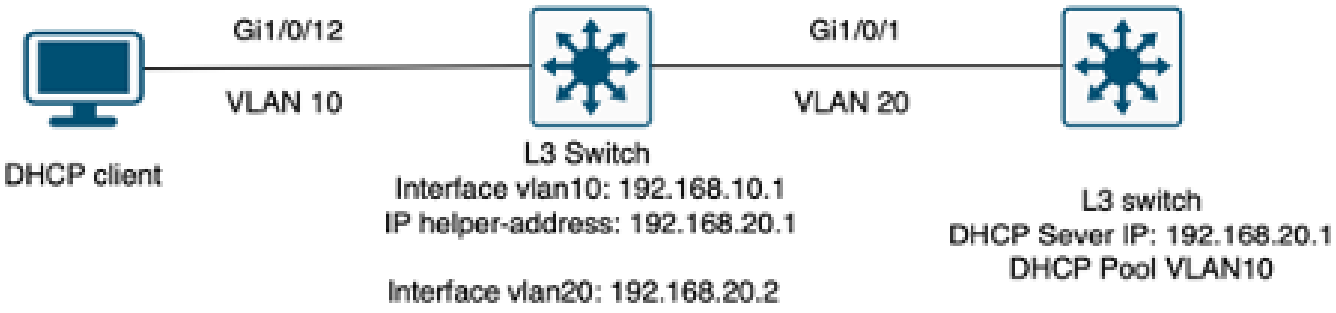
0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

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
```

Exemplo 2: O cliente não está diretamente conectado ao switch Catalyst 9000 configurado como servidor DHCP.

Neste cenário, o cliente é conectado a um switch L3 que é definido como gateway padrão e agente de retransmissão, e o servidor DHCP é hospedado em um switch Catalyst 9000 vizinho na VLAN 20.



Cliente não conectado diretamente ao switch de Camada 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:
```

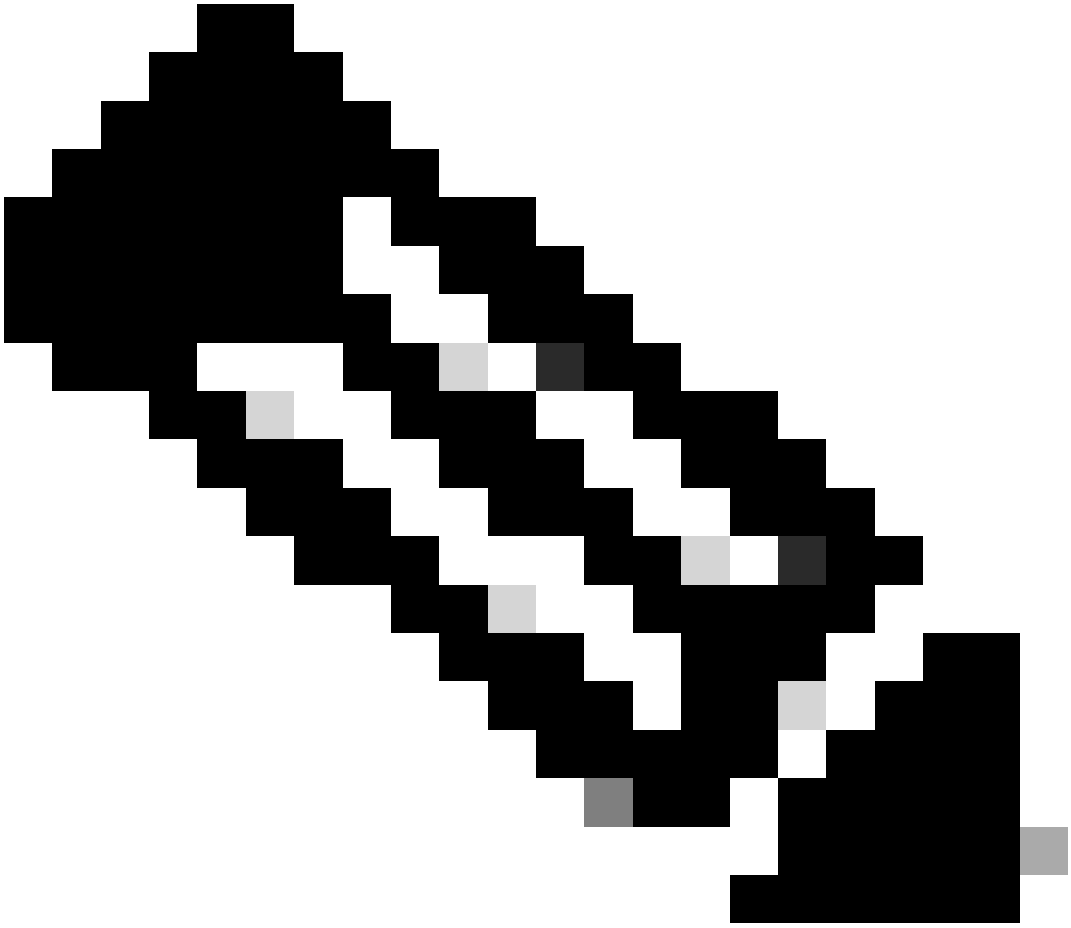
DHCPREQUEST received from client

```
 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.



Observação: se o switch for configurado como servidor DHCP e agente de retransmissão para a mesma VLAN, o servidor DHCP terá precedência.

Informações Relacionadas

- Configurando o DHCP
- Configurando a Captura de Pacotes Incorporados
- Configurando o SPAN

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.