Troubleshoot DHCP on Catalyst 9000 Switches

Contents

Introduction

This document describes how to troubleshoot DHCP on Catalyst 9000 switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Catalyst 9000 series switches architecture.
- Dynamic Host Configuration Protocol (DHCP).

Component Used

The information in this document is based on these software and hardware versions:

- C9200
- C9300
- C9500
- C9400
- C9600

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. If your network is live, ensure that you understand the potential impact of any command.

Related Products

This document can also be used with these hardware and software versions:

- Catalyst 3650/3850 series switches with Cisco IOS® XE 16.x.

Troubleshooting

When you are troubleshooting DHCP issues, there is critical information that must be confirmed in order to isolate the source of the problem. Is very important to draw a topology of the network from source to destination and identify the devices in between and their roles.

Based on these roles, there are actions that can be taken to start the troubleshooting.

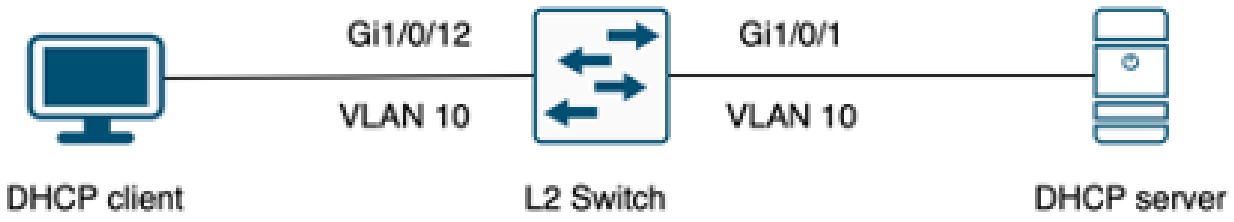
Switch Configured as Layer 2 Bridge

In this scenario, the switch is expected to receive and forward the DHCP packet without any modification.

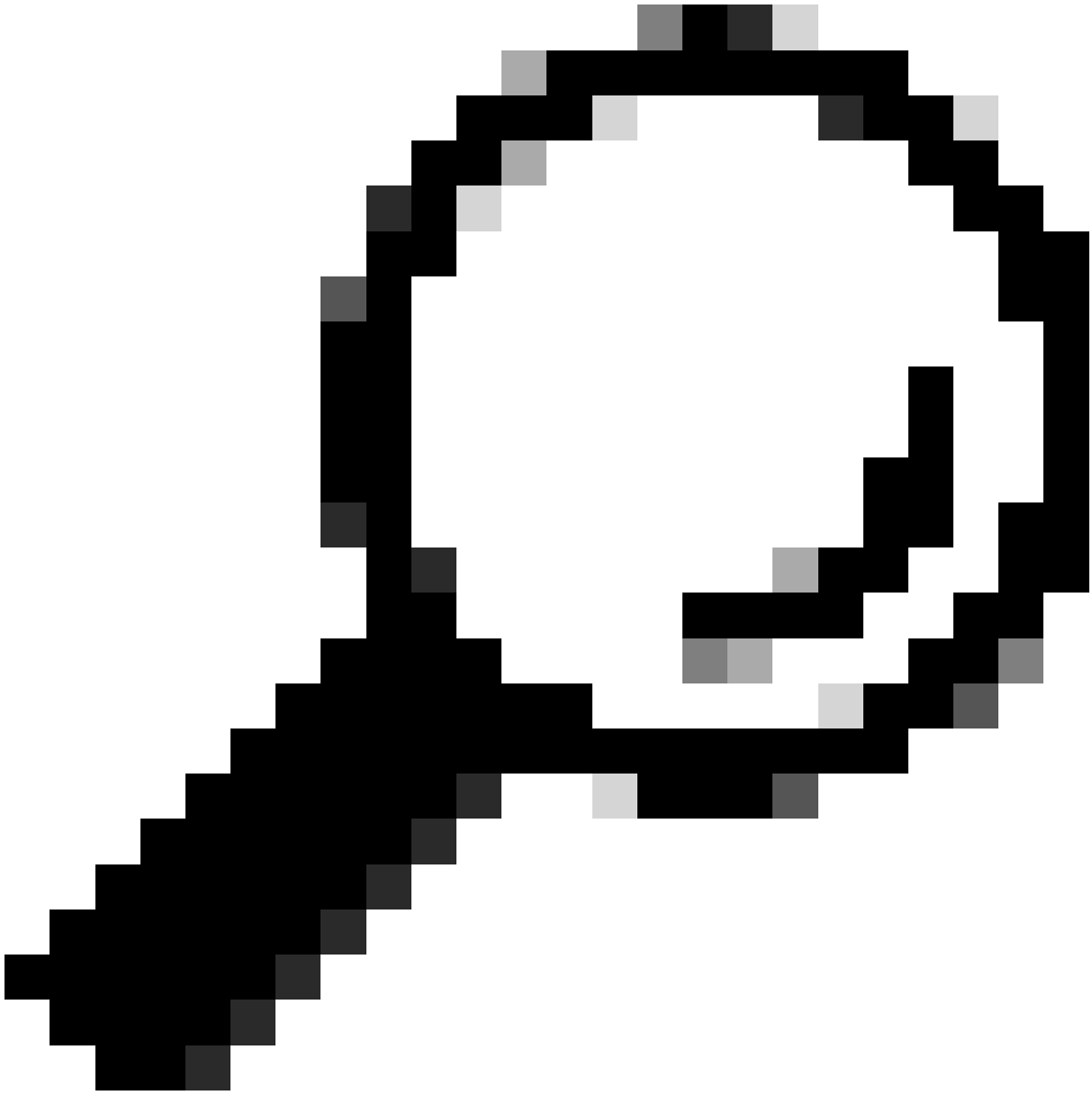
Step 1. Confirm the path of the packet.

- Identify the interfaces where the client and next hop device towards the DHCP server are connected.
- Identify the VLAN or VLANs affected.

Example: Consider the topology below, where the client connected to interface Gigabitethernet1/0/12 in VLAN 10 on a C9300 switch is unable to take an IP address via DHCP. The DHCP server is connected on interface Gigabitethernet1/0/1 also on VLAN 10.



Client connected to a Layer 2 switch.



Tip: If the issue is affecting multiple devices and VLANs, choose one client to perform the troubleshooting.

Step 2. Check the layer 2 path

- The VLAN must be created and active on the 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
```

- The VLAN must be permitted on the ingress and egress interfaces.

<#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
```

- The switch must learn the mac address of the client in the correct VLAN.

```
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
```

- If DHCP snooping is configured, make sure the trust interface is set correctly.

Step 3. Ensure the switch is receiving the DHCP discover packets on the client port.

- You can use the Embedded Packet Capture (EPC) tool.
- To filter only the DHCP packets, configure an ACL.

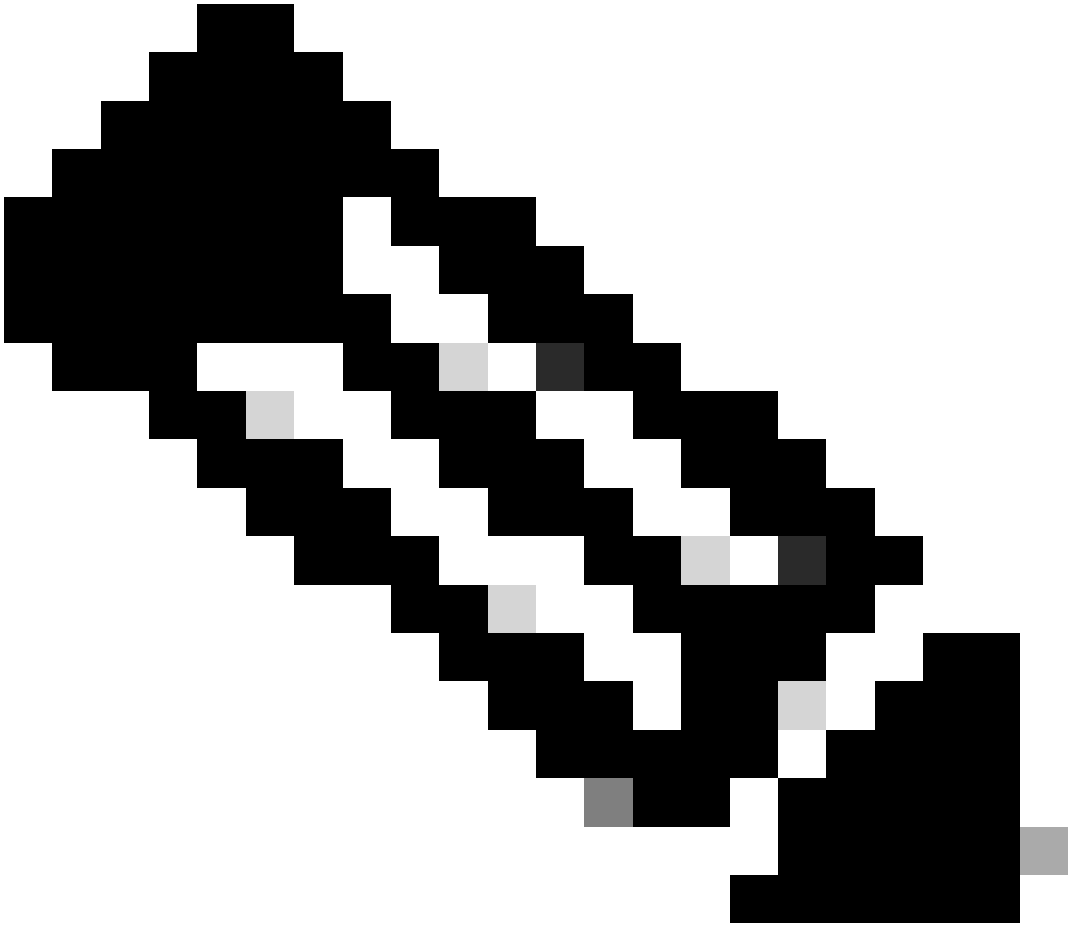
```
c9300(config)#ip access-list extended DHCP
c9300(config-ext-nacl)#permit udp any any eq 68
c9300(config-ext-nacl)#permit udp any any eq 67
c9300(config-ext-nacl)#end

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 and start the packet capture in inbound direction on the client port.

```
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
```

- Verify the content of the capture.

```
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
```

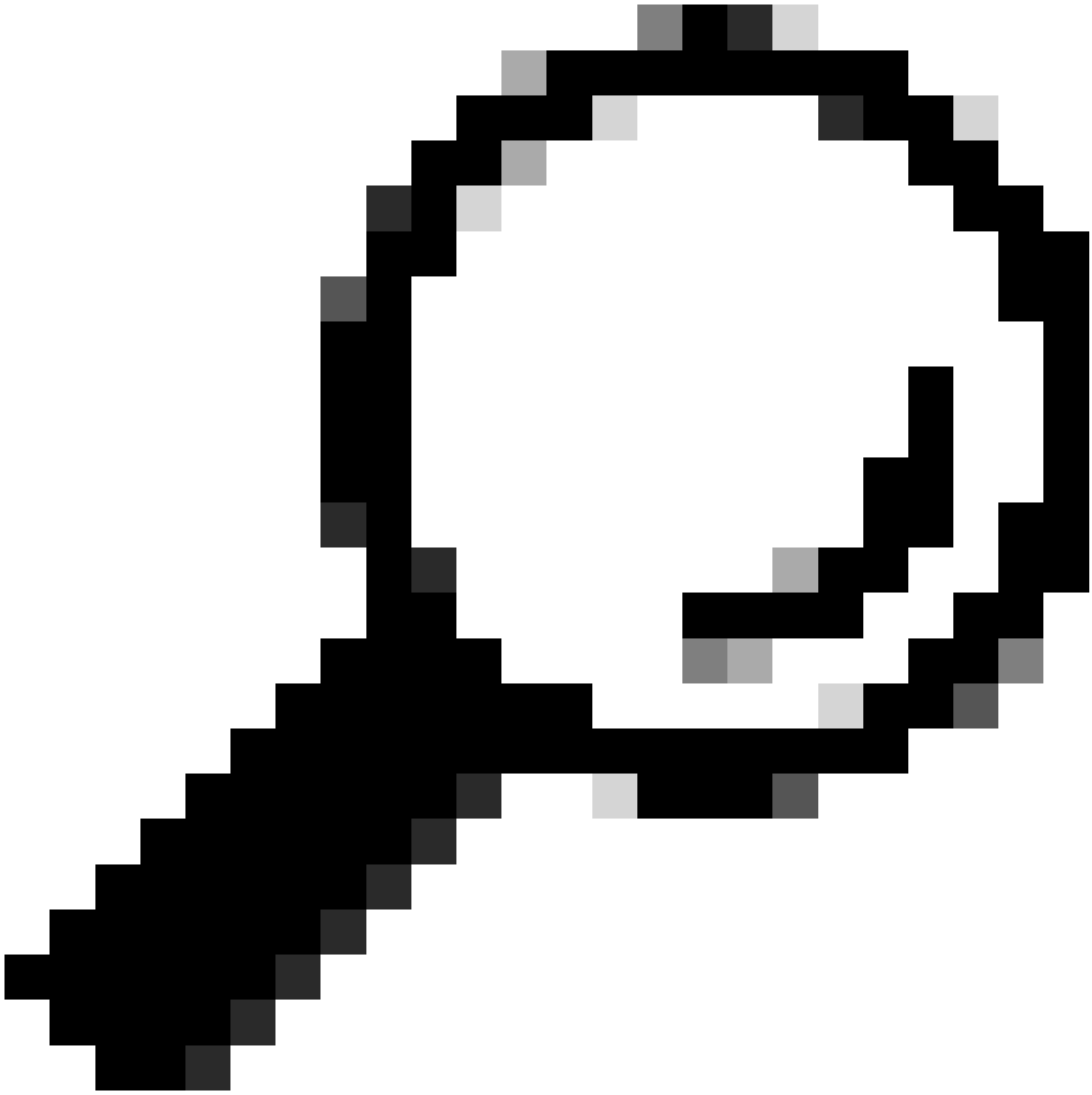


Note: Under normal circumstances if you take an EPC in BOTH direction on the client port, you can see the DORA process completed.

Step 4. Ensure the switch is forwarding the DHCP discover.

- You can take a capture on the egress port in outbound direction.

```
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
```



Tip: To confirm that the DHCP discover collected in the capture belong to the client being troubleshoot, you can apply the filter **dhcp.hw.mac_addr** to the EPC using the **display-filter** option.

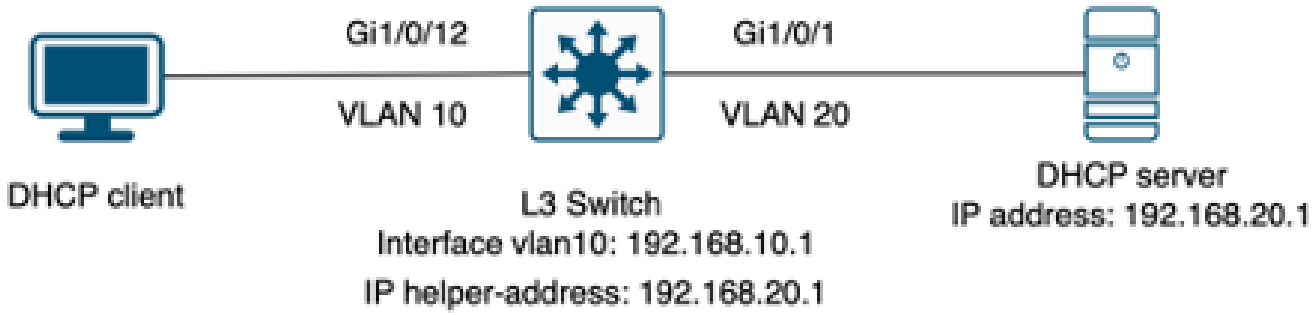
At this point we have confirmed that the switch is forwarding the DHCP packets, and the troubleshooting can be moved to the DHCP server.

Switch Configured as Relay Agent

The Relay Agent is use when the clients and the DHCP servers do not belong to the same broadcast domain.

When the switch is configured as Relay Agent, the DHCP packets are modified in the switch, for packets sent from the client the switch adds its own information (IP address and mac address) to the packet and sent it to the next hop towards the DHCP Server. The packets received from the DHCP server are pointed to the Relay Agent, and then the switch forwards those back to the client.

Continue with the example on the previous scenario, we have a client connected to interface Gigabitethernet1/0/12 on VLAN 10 unable to obtain an IP address via DHCP, now the C9000 switch is the default gateway for VLAN 10 and is configure as Relay Agent, the DHCP server is connected to interface Gigabitethernet1/0/1 on VLAN 20.



Client connected to a Layer 3 switch configured as Relay Agent.

Step 1. Confirm the switch is receiving the DHCP discover.

- Run a packet capture on the interface facing the client. Refer to the step 3 on the previous scenario.

Step 2. Check IP helper configuration.

- DHCP service must be enabled.

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

- IP helper command under the VLAN 10 SVI.

<#root>

```
interface vlan10
 ip address 192.168.10.1 255.255.255.0
```

```
ip helper-address 192.168.20.1
```

Step 3. Check connectivity to the DHCP servers.

- The switch must have unicast connectivity to the DHCP server from the client VLAN. You can test with a 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
```

Step 4. Confirm the switch is forwarding the DHCP packets to the next hop.

- You can run a **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:
```

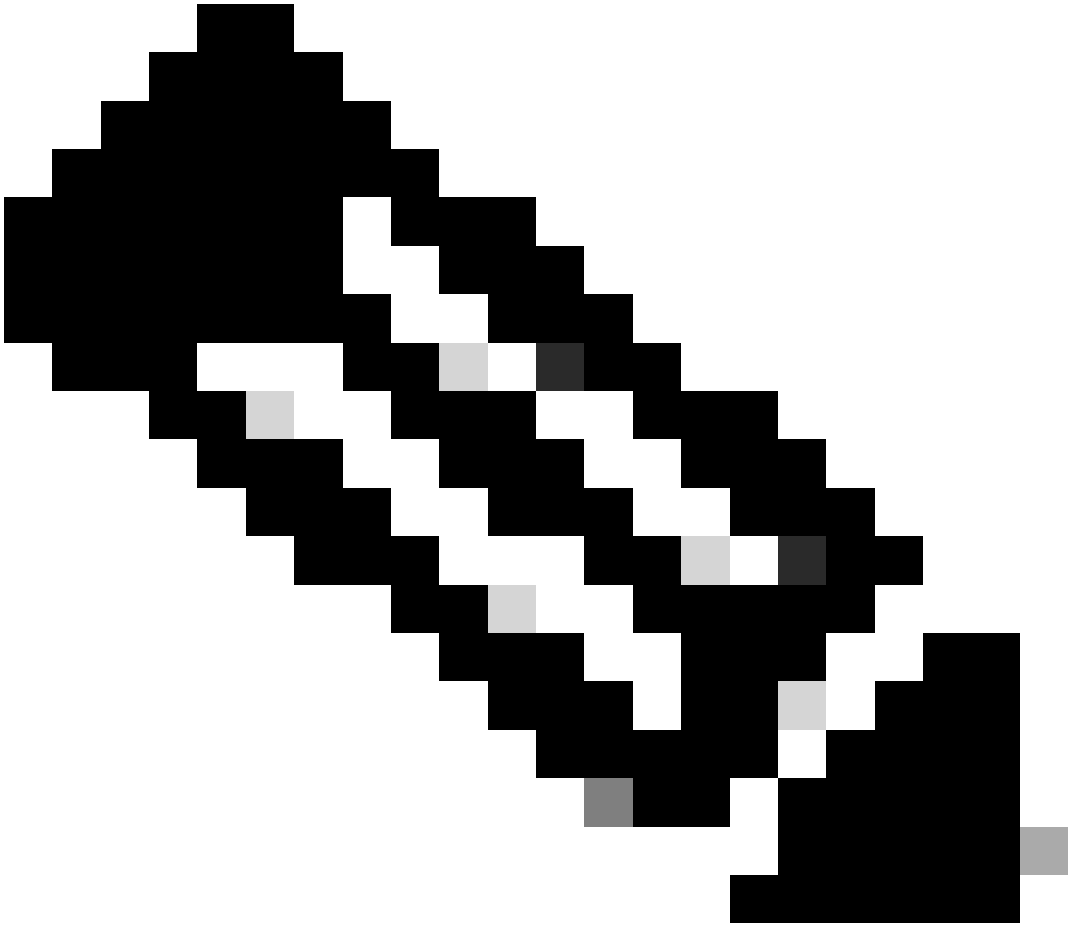
DHCPD: BOOTREQUEST from 0170.18a7.e84f.46 forwarded to 192.168.20.1.

- Take packet captures. You can use EPC on control plane.

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

- You can also take a SPAN in the egress port.

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



Note: You must configure only one Relay agent on the path.

Switch Configured as DHCP Server

In this scenario, the switch has the DHCP scope configured locally.

Step 1. Check basic configuration.

- The pool must be created and have the network, subnet mask and default router configured.

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

- DHCP services must be enable.

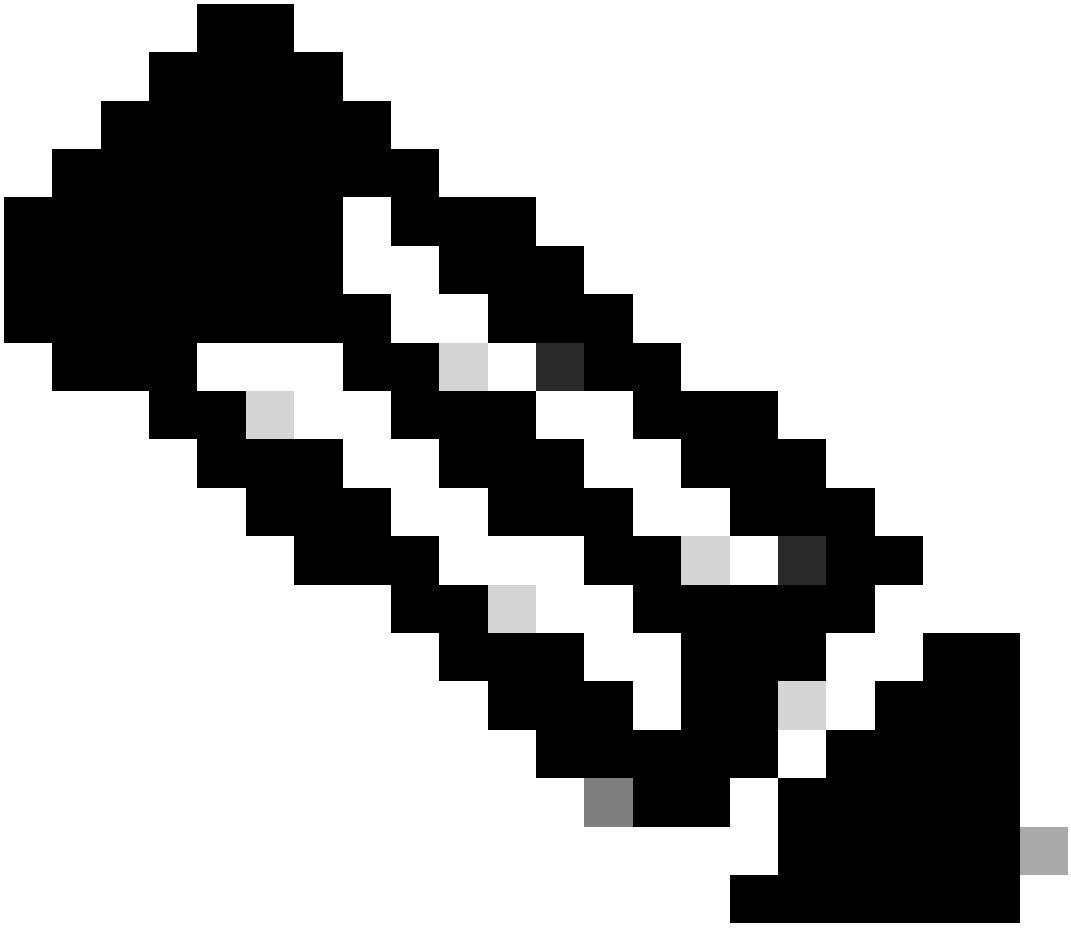
```
show run all | in dhcp
service dhcp
```

- The switch must have unicast connectivity to the networks configured in the 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
```

- All the statically configure IP addresses must be excluded from the pool range.

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

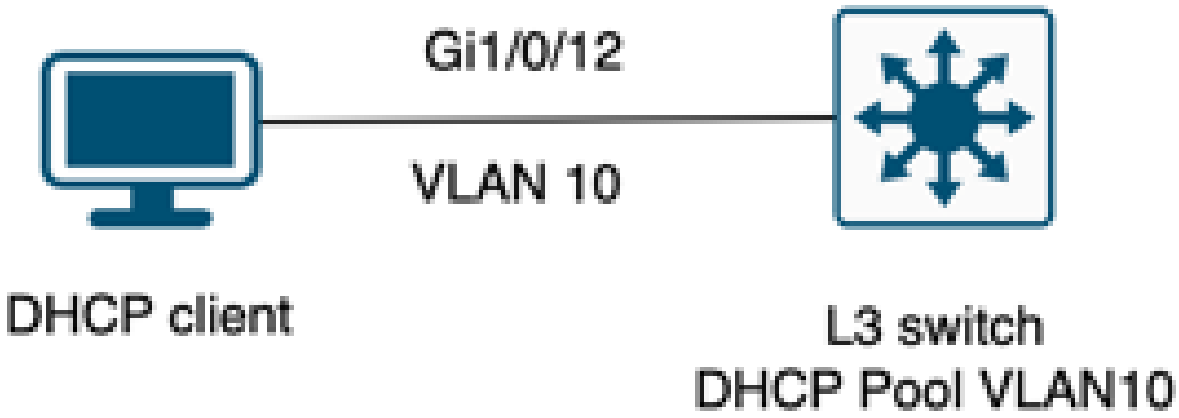


Note: Service DHCP must be enabled if the switch is configured as DHCP server or Relay agent.

Step 2. Verify the switch is leasing IP addresses.

- You can use **debug ip dhcp server packet detail**.

Example 1: The client is directly connect to the Catalyst 9000 switch configured as DHCP server on VLAN 10.



Client connected to a Layer 3 switch configured as DHCP server.

<#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

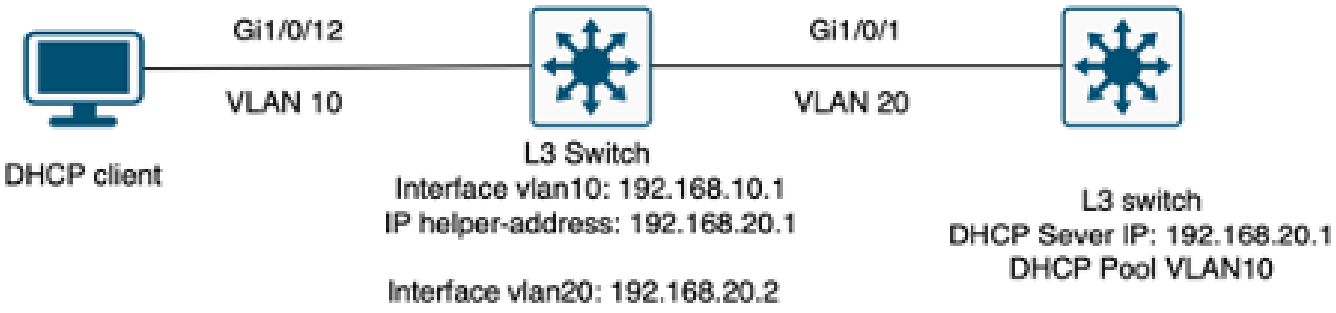
0063.6973.636f.2d39.6335.342e.3136.6237.2e37.6436.342d.5477.6531.2f30.2f31

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
```

Example 2: The client is not directly connected to the Catalyst 9000 switch configured as DHCP server.

In this scenario, the client is connected to a L3 switch that is set as default gateway and Relay agent, and the DHCP server is hosted on a neighbor Catalyst 9000 switch on VLAN 20.



Client not directly connected to the Layer 3 switch working as DHCP server.

<#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:
```

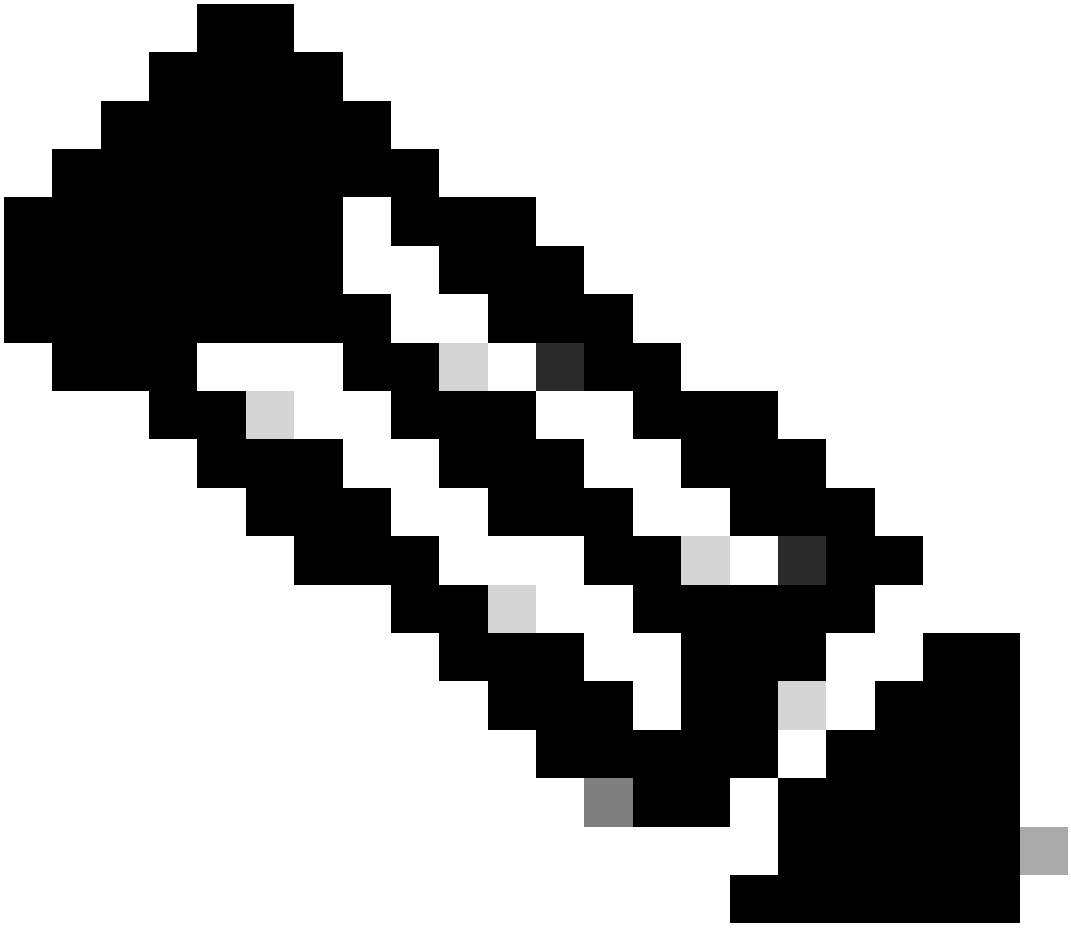
DHCPREQUEST received from client

```
 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.



Note: If the switch is configure as DHCP server and Relay agent for the same VLAN, the DHCP server takes precedence.

Related Information

- Configuring DHCP
- Configuring Embedded Packet Capture
- Configuring SPAN