Troubleshoot DHCP Client Connectivity Issue on a Cisco 9800 WLC

Contents

Introduction

This document will describe various Dynamic Host Configuration Protocol (DHCP)-related issues encountered by wireless clients when connected to a Cisco 9800 Wireless LAN Controller (WLC) and how to troubleshoot them.

Prerequisites

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Cisco WLC 9800
- Basic knowledge of DHCP Flow
- Basic knowledge of local and flex connect mode AP

Understanding the Flow of DHCP Traffic with Wireless Clients

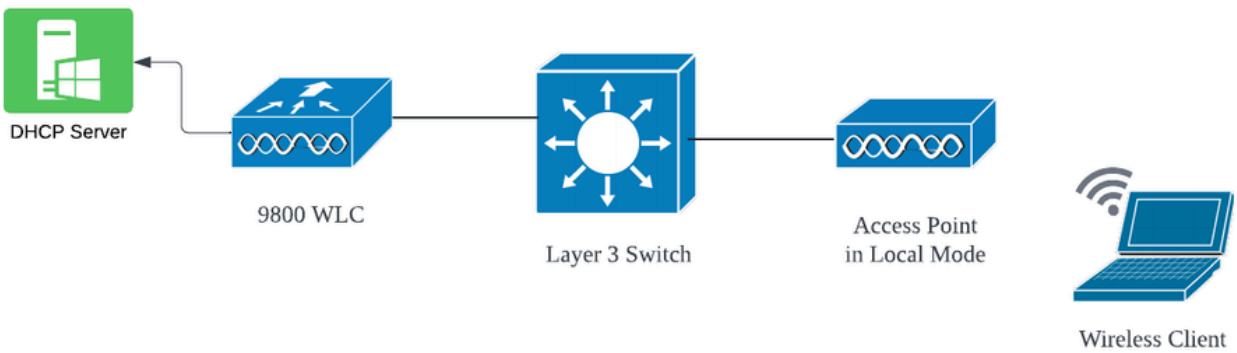
When the wireless client connects, it does the usual DHCP exchange by sending a broadcast DHCP discovery frame to find a DHCP server to the associated AP. Depending on the AP's mode of operation, it will either forward the request to the WLC via the CAPWAP tunnel or pass it directly to the next hop. If a DHCP server is available within the local Layer 2 domain, it will respond, facilitating a successful connection. In the absence of a local subnet DHCP server, the router (configured with the client's SVI) must be set up to route the DHCP discovery to the appropriate server. This is typically done by configuring an IP Helper Address on the router, which instructs it to forward specific broadcast UDP traffic (such as DHCP requests) to a predetermined IP address.

The behavior of client DHCP traffic is entirely dependent on the mode in which your access point (AP) is operating. Let's examine each of these scenarios separately:

Scenario 1. The Access Point (AP) is Operating in Local Mode

When an AP is set up in Local Mode, client DHCP traffic is centrally switched, meaning that the DHCP requests from clients are sent through a CAPWAP tunnel from the AP to the WLC, where they are then processed and forwarded accordingly. In this case, you have two choices: you can either utilize an Internal DHCP server or opt for an External DHCP server.

Topology (Local Mode AP)



Network Topology : Local Mode AP

Case Study 1. When WLC is Configured as an Internal DHCP Server

The controller is capable of offering an internal DHCP server through the integrated features of the Cisco IOS XE software. However, it is considered best practice to use an external DHCP server. Before setting up the WLC as an Internal DHCP server, several prerequisites must be addressed which are as follows:

- Ensure to configure a Switched Virtual Interface (SVI) for the client VLAN and assign the IP address of the DHCP server to it.

- The IP address of the Internal DHCP server should be set on the server-facing interface, which could be a loopback interface, an SVI, or a Layer 3 physical interface.
- Loopback interface is recommended to configure because, unlike physical interfaces that connect to actual network segments, the loopback interface is not tied to hardware and does not correspond to a physical port on the device. The primary purpose of a loopback interface is to provide a stable, always-up interface that is not subject to hardware failures or physical disconnections.

Working Setup: Here is an example of an internal DHCP server configuration where clients successfully received IP addresses. Here are the operational logs and the associated setup details.

Set up the WLC as the DHCP server for VLAN 10, with a DHCP scope ranging from 10.106.10.11/24 to 10.106.10.50/24.

```
WLC#show run | sec dhcp
ip dhcp excluded-address 10.106.10.0 10.106.10.10
ip dhcp excluded-address 10.106.10.51 10.106.10.255
ip dhcp pool vlan_10_Pool
network 10.106.10.0 255.255.255.0
lease 0 8
```

Configured Loopback interface on WLC:

```
WLC#show run interface loopback 0
interface Loopback0
ip address 10.10.10.25 255.255.255.0
end
```

Client VLAN configured as SVI [L3 Interface] with helper address as loopback interface on WLC:

<#root>

```
WLC#show run int vlan10
ip address 10.106.10.10 255.255.255.0
ip helper-address 10.10.10.25 [helper address can be loopback interface, Wireless management interface
end
```

Alternatively, you can set the DHCP server's IP address within the policy profile, rather than configuring a helper address under the SVI. However, it is generally advised to configure this on a per-VLAN basis for best practices:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
```

```
ipv4 dhcp server $WMI_IP
```

Radioactive Traces on WLC:

```
2024/03/29 13:28:06.502389611 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:06.502515811 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:06.502614149 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:06.502674118 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.505719129 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.505787349 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.505834315 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543149257 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:08.543254480 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.543334850 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543407760 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543910482 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543968250 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.544135443 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.544314185 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

Embedded Packet Captures on WLC:

```
1401 18:58:06.501972 0.0.0.0          255.255.255.255    DHCP    348 DHCP Discover - Transaction ID 0x7030bf99
1402 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1403 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1429 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1430 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1431 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    346 DHCP Offer    - Transaction ID 0x7030bf99
1432 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    416 DHCP Offer    - Transaction ID 0x7030bf99
1433 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    452 DHCP Request  - Transaction ID 0x7030bf99
1434 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    374 DHCP Request  - Transaction ID 0x7030bf99
1435 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1436 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1437 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1438 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1439 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    346 DHCP ACK      - Transaction ID 0x7030bf99
1440 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    416 DHCP ACK      - Transaction ID 0x7030bf99
```

Embedded Packet Capture on WLC

AP Client Debugs:

```
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7183] [1711718885:718317] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7184] [1711718885:718428] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7223] [1711718887:722360] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7224] chatter: dhcp_reply_nonat: 1711718887.722379604: 10
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7225] [1711718887:722524] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7591] [1711718887:759139] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7592] [1711718887:759248] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7606] [1711718887:760687] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7607] [1711718887:760780] [AP_NAME] [Client_MAC] <apr0v2>
```

Client Side Packet Capture:

```
122 07:11:56.202853  0.0.0.0          255.255.255.255      DHCP     344 DHCP Discover - Transaction ID 0x595044d4
129 07:11:58.217331  10.106.10.10     255.255.255.255      DHCP     342 DHCP Offer    - Transaction ID 0x595044d4
130 07:11:58.219406  0.0.0.0          255.255.255.255      DHCP     370 DHCP Request  - Transaction ID 0x595044d4
131 07:11:58.227525  10.106.10.10     255.255.255.255      DHCP     342 DHCP ACK      - Transaction ID 0x595044d4
```

Client End Packet Capture

In the operational logs provided, you can see that the WLC is receiving the DHCP Discover message from the wireless client, and the client's VLAN is relaying it to the helper address (which in the example provided is the internal loopback interface). Following this, the internal server issues a DHCP Offer, and subsequently, the client sends a DHCP Request, which is then acknowledged by the server with a DHCP ACK.

Verification of Wireless Client IP:

On WLC:

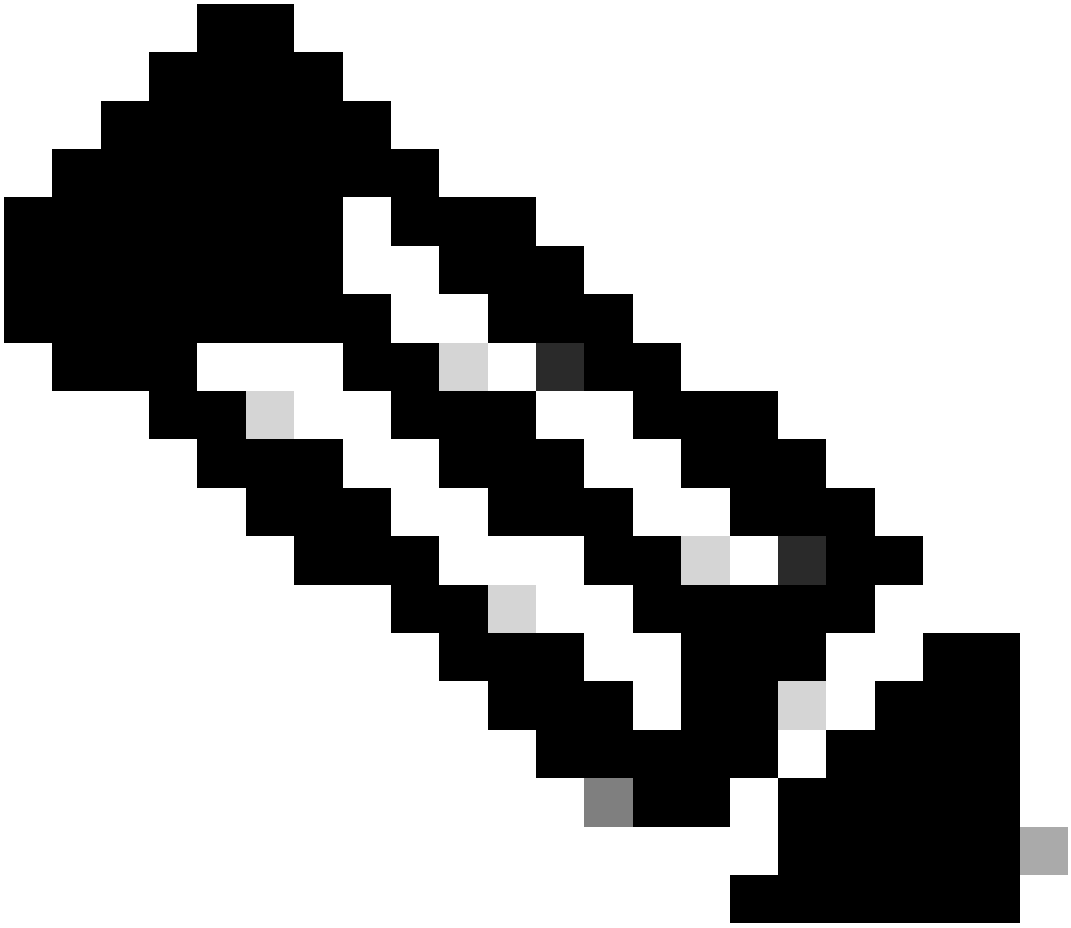
```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type          State
10.106.10.12      aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active
```

On Wireless Client:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . : [redacted]
   Physical Address. . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . [redacted]
   IPv4 Address. . . . . . . . . . . 10.106.10.12(Preferred)
   Subnet Mask . . . . . . . . . . . 255.255.255.0
   Lease Obtained. . . . . . . . . . Thursday, March 28, 2024 9:35:20 PM
   Lease Expires . . . . . . . . . . Friday, March 29, 2024 6:36:29 AM
   Default Gateway . . . . . . . . .
   DHCP Server . . . . . . . . . . . 10.10.10.25
   DHCPv6 IAID . . . . . . . . . . . 80754501
   DHCPv6 Client DUID. . . . . . . . [redacted]
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

IP verification on Client end



Note:
1. VRF is not supported in the internal DHCP servers.
2. DHCPv6 is not supported in the internal DHCP servers.
3. On C9800, SVI allows configuring multiple helper addresses but only the first 2 are used.
4. This has been tested and hence is supported across all platforms for a maximum of 20% of the box’s maximum client scale. For example, for a 9800-80 that supports 64,000 clients, the maximum DHCP bindings supported is around 14,000.

Case Study 2. When an External DHCP Server is Used

An external DHCP server refers to a DHCP server that is not integrated into WLC itself but configured on a different network device [Firewall, Routers] or a separate entity within the network infrastructure. This server is dedicated to managing the dynamic distribution of IP addresses and other network configuration parameters to clients on the network.

When utilizing an external DHCP server, the WLC's function is solely to receive and relay traffic. How the DHCP traffic is routed from the WLC, whether it's broadcast or unicast, will vary depending on your preference. Let's consider each of these methods separately.

DHCP Traffic Broadcast Across the Layer 2 Domain

In this setup, another network device, such as a firewall, uplink, or core switch, acts as a relay agent. When a client broadcasts a DHCP discovery request, the WLC's only job is to forward this broadcast via the Layer 2 interface. For this to work correctly, you must ensure that the client VLAN's Layer 2 interface is configured properly and permitted through the WLC's data port and the uplink device.

Desired configuration on the WLC end for client VLAN 20 for this instance:

Configured Layer 2 VLAN on WLC:

```
WLC#show run vlan 20
vlan 20
name Client_vlan
end
```

Configured Data port on WLC to allow the traffic of client VLAN:

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

Radioactive Traces on 9800 WLC:

```
2024/03/30 10:40:43.114800606 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.114863170 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.121515725 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.121583319 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.132967882 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: IPv6 DHCP from intf
2024/03/30 10:40:43.132999148 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: IPv6 DHCP from intf
2024/03/30 10:40:43.146521529 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 10:40:43.146605773 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.146685159 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149359205 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.149419477 {wncd_x_R0-0}{1}: [client-orch-sm] [23608]: (ERR): MAC: DHCP_Server_MAC V
2024/03/30 10:40:43.149534985 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149685174 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

Embedded Packet Capture Taken on 9800 WLC:

```
187 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     424 DHCP Discover - Transaction ID 0xa1a4f5eb
188 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
189 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
190 16:10:43.113992 0.0.0.0          255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
192 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
193 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
194 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
195 16:10:43.120980 10.106.20.10     255.255.255.255      DHCP     416 DHCP Offer    - Transaction ID 0xa1a4f5eb
201 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     452 DHCP Request  - Transaction ID 0xa1a4f5eb
202 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
203 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
204 16:10:43.145988 0.0.0.0          255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
205 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
206 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
207 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
208 16:10:43.148979 10.106.20.10     255.255.255.255      DHCP     416 DHCP ACK      - Transaction ID 0xa1a4f5eb
```

Embedded Packet Capture on WLC

AP Client Debugs:

```
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3650] [1711796737:183177] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3651] [1711796737:184281] [[AP_NAME] [Client_MAC] <wired0
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] [1711796737:185404 [[AP_NAME] [Client_MAC] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] chatter: dhcp_reply_nonat: 1711796737.459745189: 10
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3670] [1711796737:195085] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3683] [1711796737:368344] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3684] [1711796737:368439] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3931] [1711796737:393131] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3932] [1711796737:393250] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.4597] [1711796737:459726] [AP_Name] [Client_Mac] <wired0>
```

Client Side Capture:

```
  3 03:17:46.193239 0.0.0.0          255.255.255.255      DHCP     342 DHCP Discover - Transaction ID 0x56883262
 31 03:17:50.649855 0.0.0.0          255.255.255.255      DHCP     342 DHCP Discover - Transaction ID 0x56883262
 34 03:17:53.259282 10.106.20.10     255.255.255.255      DHCP     342 DHCP Offer    - Transaction ID 0x56883262
 35 03:17:53.259282 10.106.20.10     255.255.255.255      DHCP     342 DHCP Offer    - Transaction ID 0x56883262
 36 03:17:53.262280 0.0.0.0          255.255.255.255      DHCP     370 DHCP Request  - Transaction ID 0x56883262
 37 03:17:53.273130 10.106.20.10     255.255.255.255      DHCP     342 DHCP ACK      - Transaction ID 0x56883262
```

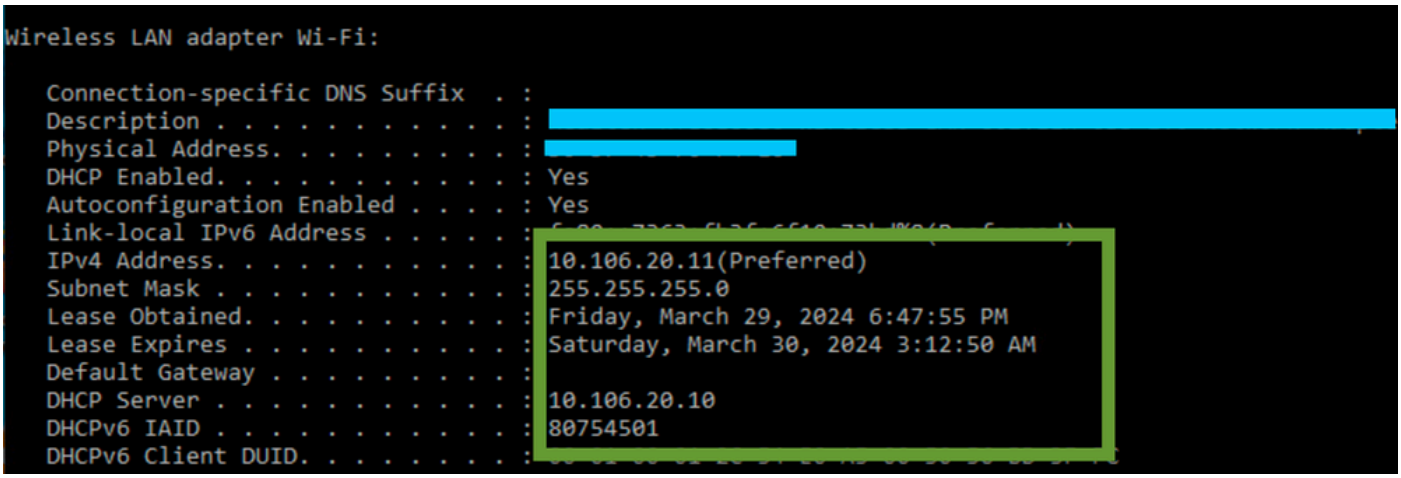
Client End Packet Capture

In the operational logs provided, you notice in the logs that the WLC is intercepting the DHCP Discover broadcast from the wireless client and then broadcasting it onward to the next hop via its L2 interface. As soon as the WLC receives the DHCP Offer from the server, it forwards this message to the client followed by DHCP Request and ACK.

Verification of Wireless Client IP:

You can check the IP lease on the DHCP server and its corresponding status.

On Wireless Client:



IP verification on Client End

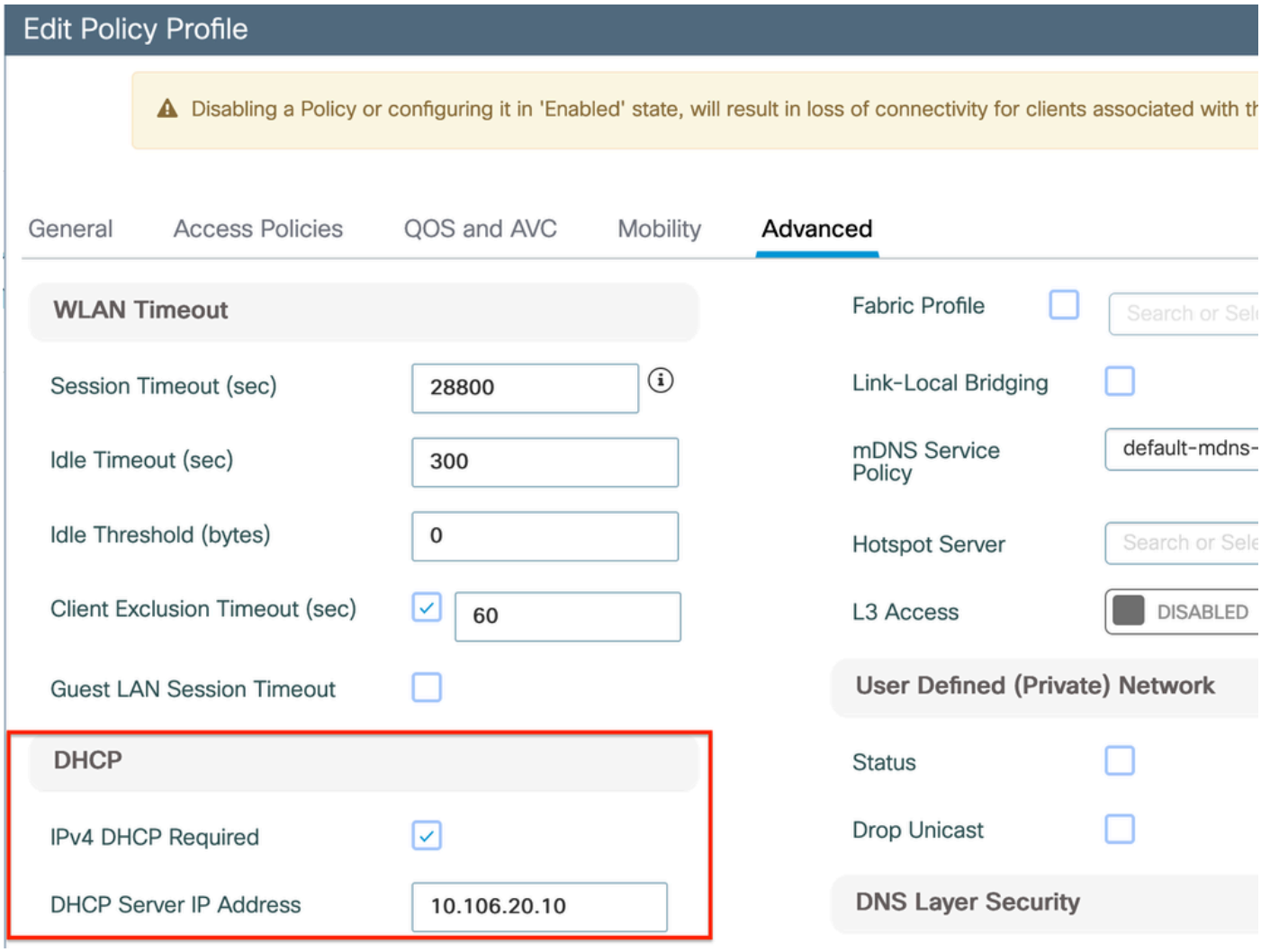
9800 WLC is Serving as a Relay Agent

In this configuration, the WLC directly forwards the DHCP packets it receives from wireless clients to the DHCP server by unicast. To enable this, ensure that the VLAN SVI for the client is configured on the WLC.

There are 2 ways to configure the DHCP server IP in 9800 WLC:

1. Configure DHCP server IP under policy profile under advanced setting.

Via GUI: Navigate to Configuration > Tags & Profile > Policy > Policy_name > Advanced. Under the DHCP section you can configure the DHCP server IP as shown:



Policy Profile Setting on WLC

Via CLI:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
ipv4 dhcp server $DHCP_Server_IP
```

2. Within the SVI configuration, you must specify the helper address. It is possible to set up multiple DHCP servers in the helper address configuration to provide redundancy. While setting the DHCP server address for each WLAN within the policy profile is possible, the recommended approach is to configure it on a per-interface basis. This can be accomplished by assigning a helper address to the corresponding SVI.

When employing the relay feature, the source of the DHCP traffic will be the IP address of the client's Switched Virtual Interface (SVI). This traffic is then routed through the interface that corresponds with the destination (the DHCP server's IP address) as determined by the routing table.

Here's a sample of the working configuration on 9800 serving as a relay agent:

Configured Layer 3 Interface for Client VLAN on WLC with helper address:

```
WLC#show run int vlan 20
interface vlan 20
ip address 10.106.20.1 255.255.255.0
ip helper-address 10.106.20.10
end
```

Configured Data port on WLC to allow the traffic of client VLAN:

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

RA Traces from WLC:

```
2024/03/30 13:46:38.549504590 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:38.549611716 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:38.549666984 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.597696305 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.597778465 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.597829829 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.598444184 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.598506350 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.598544420 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.621660873 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 13:46:41.621771405 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.621851320 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.621908730 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625257607 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.625329089 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.625490562 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625655045 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

Embedded Packet Capture on WLC:

No.	Time	Source	Destination	Protocol	Length	Info
462	19:16:34.544969	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
463	19:16:34.545961	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
594	19:16:38.548967	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
595	19:16:38.548967	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
647	19:16:41.596953	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
648	19:16:41.596953	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
649	19:16:41.597961	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
650	19:16:41.597961	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
653	19:16:41.620954	0.0.0.0	255.255.255.255	DHCP	452	DHCP Request - Transaction ID 0x137ea7ac
654	19:16:41.620954	10.106.20.1	10.106.20.10	DHCP	374	DHCP Request - Transaction ID 0x137ea7ac
655	19:16:41.624967	10.106.20.10	10.106.20.1	DHCP	346	DHCP ACK - Transaction ID 0x137ea7ac
656	19:16:41.624967	10.106.20.1	255.255.255.255	DHCP	416	DHCP ACK - Transaction ID 0x137ea7ac

Embedded Packet Capture on WLC

In both the Radioactive Traces (RA) and the Embedded Packet Capture (EPC) on the WLC, you will notice that the WLC, acting as a relay agent, is directly unicasting the DHCP packets from the client to the DHCP server.

AP Client Debugs:

```
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7476] [1711806397:747677] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7481] [1711806397:748177] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] chatter: dhcp_reply_nonat: 1711806400.797214204: 10
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] [1711806400:797362] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7978] [1711806400:797870] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7979] [1711806400:797903] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8204] [1711806400:820455] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8205] [1711806400:820550] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8248] [1711806400:824829] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8249] [1711806400:824911] [AP_Name] [Client_MAC] <apr0v1>
```

Client Side Capture:

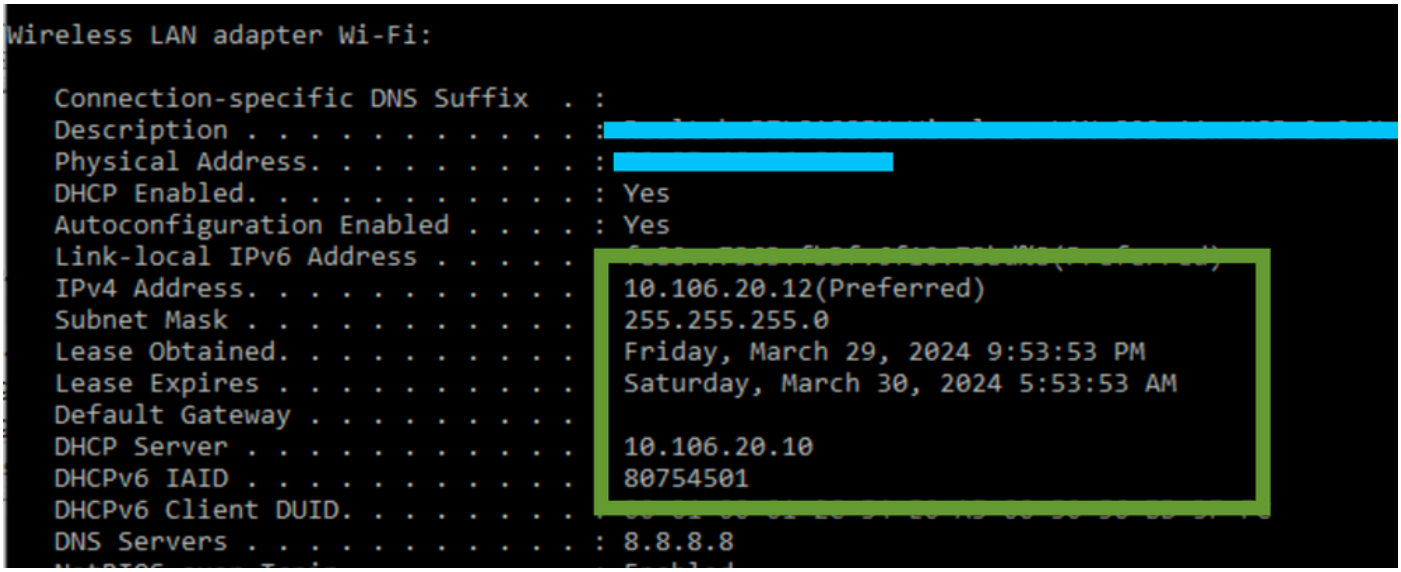
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
60	10:23:53.696530	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x137ea7ac
61	10:23:53.698634	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
62	10:23:53.737816	10.106.20.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x137ea7ac

Client End Packet Capture

Verification of Wireless Client IP:

You can check the IP lease on the DHCP server and its corresponding status.

On Wireless Client:



IP verification on Client End

DHCP Option 80 with Suboption 5/150 in 9800 WLC

In certain scenarios, you may prefer to explicitly define the source interface for DHCP traffic rather than depending on the routing table, to prevent potential network complications. This is particularly relevant when the next network device along the path, such as a Layer 3 switch or firewall, employs Reverse Path Forwarding (RPF) checks. Take, for instance, a situation where the wireless management interface is set on VLAN 50, while the client SVI is on VLAN 20 and is being used as a DHCP relay for client traffic. The default route is directed towards the gateway of the wireless management VLAN/subnet.

Starting with version 17.03.03 on the 9800 WLC, it is possible to choose the source interface for DHCP traffic to be either the client VLAN or another VLAN, such as the Wireless Management Interface (WMI), which guarantees connectivity to the DHCP server.

Here would be a snip of the config:

```
!
interface vlan 50
 description Wireless Management
 ip address 10.100.16.10 255.255.255.0
!
interface vlan 20
 description Wireless_Client_vlan
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
!
ip route 0.0.0.0 0.0.0.0 10.100.16.1
```

In this scenario, the traffic to the DHCP server 10.100.17.14 will be sourced from VLAN 50 (10.100.16.10), because the packet's exit interface is selected based on a lookup in the IP routing table, and typically, it would exit via the Wireless Management Interface (WMI) VLAN due to default route configured.
However, if an uplink switch implements Reverse Path Forwarding (RPF) checks, it may discard a packet arriving from VLAN 50 but with an IP source address belonging to a different subnet [VLAN 20].

To prevent this, you should set a precise source interface for the DHCP packets with the IP DHCP relay source-interface command. In this particular case, you'd want the DHCP packets to originate from the WMI interface on VLAN 50:

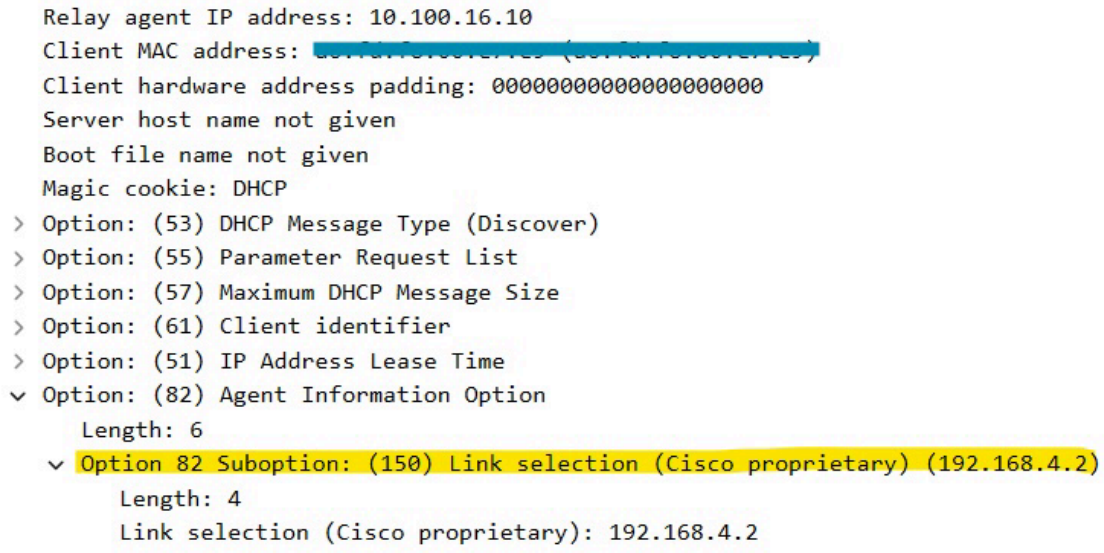
```
interface vlan 20
 description Wireless_Client_vlan=
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
 ip dhcp relay source-interface vlan 50
```

When using ip dhcp relay source-interface command, both the source interface of the DHCP packets and the GIADDR is set to the interface specified in the DHCP relay command (VLAN50, in this case). This is a

problem, as this is not the client VLAN where you want to assign DHCP addresses.

How does the DHCP server know how to assign the IP from the right client pool?

So the answer to this is when the ip dhcp relay source-interface the command is used, C9800 automatically adds the client subnet information in a proprietary sub-option 150 of option 82 called link selection, as you can see from the capture:



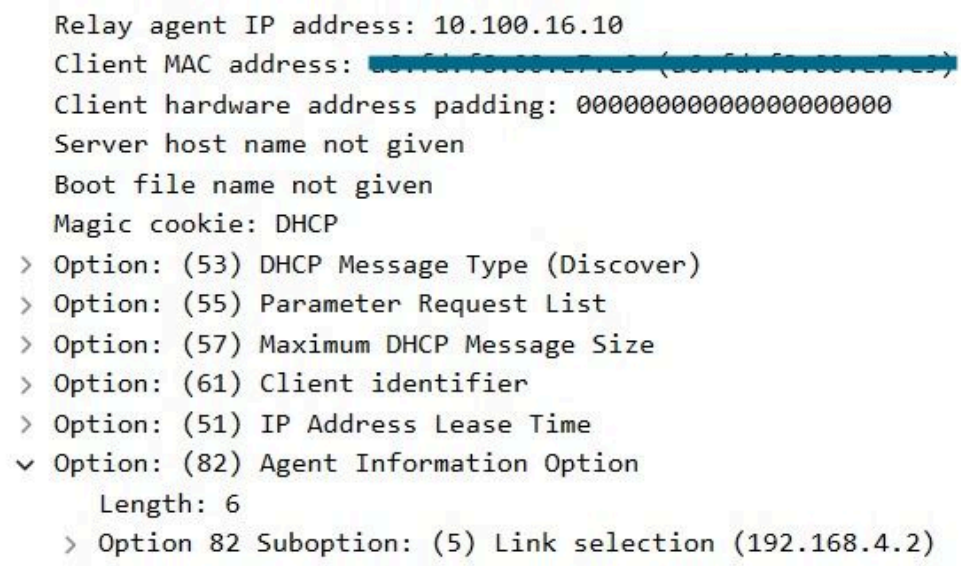
Option 182 suboption 150 on WLC Packet Capture

By default, it will add sub-option 150 (cisco proprietary). Ensure that the DHCP server used can interpret and act on this information. The recommendation is to change the C9800 configuration to use the standard option 82, sub-option 5 to send the link selection information. You can do this by configuring the following global command:

<#root>

```
C9800(config)#ip dhcp compatibility suboption link-selection standard
```

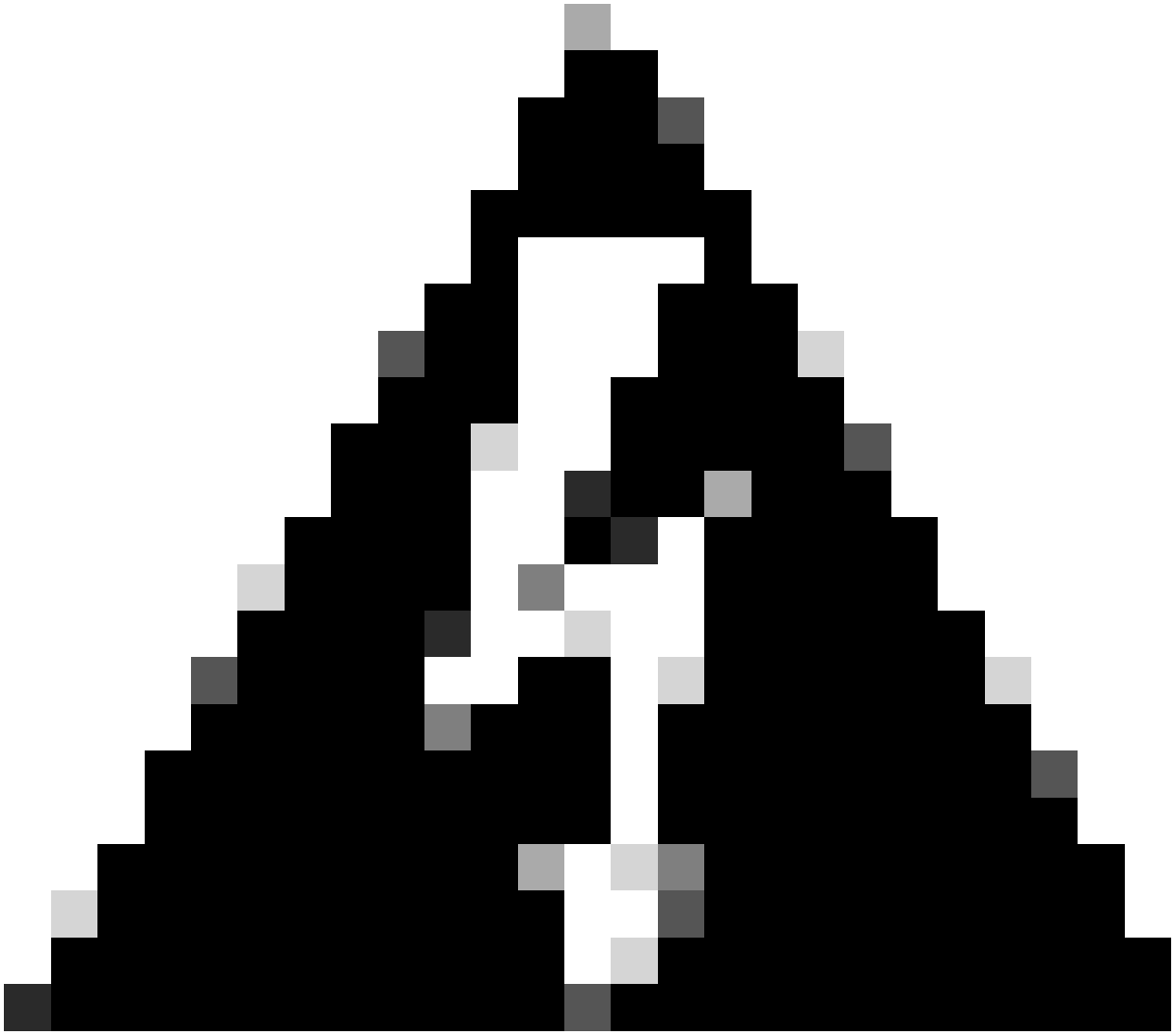
Once the specified command is applied, the system will replace suboption 150 with suboption 5 in the DHCP packets. Suboption 5 is more widely recognized by network devices, thus ensuring that the packets are less likely to be dropped. The application of this change is also evident in the capture provided:



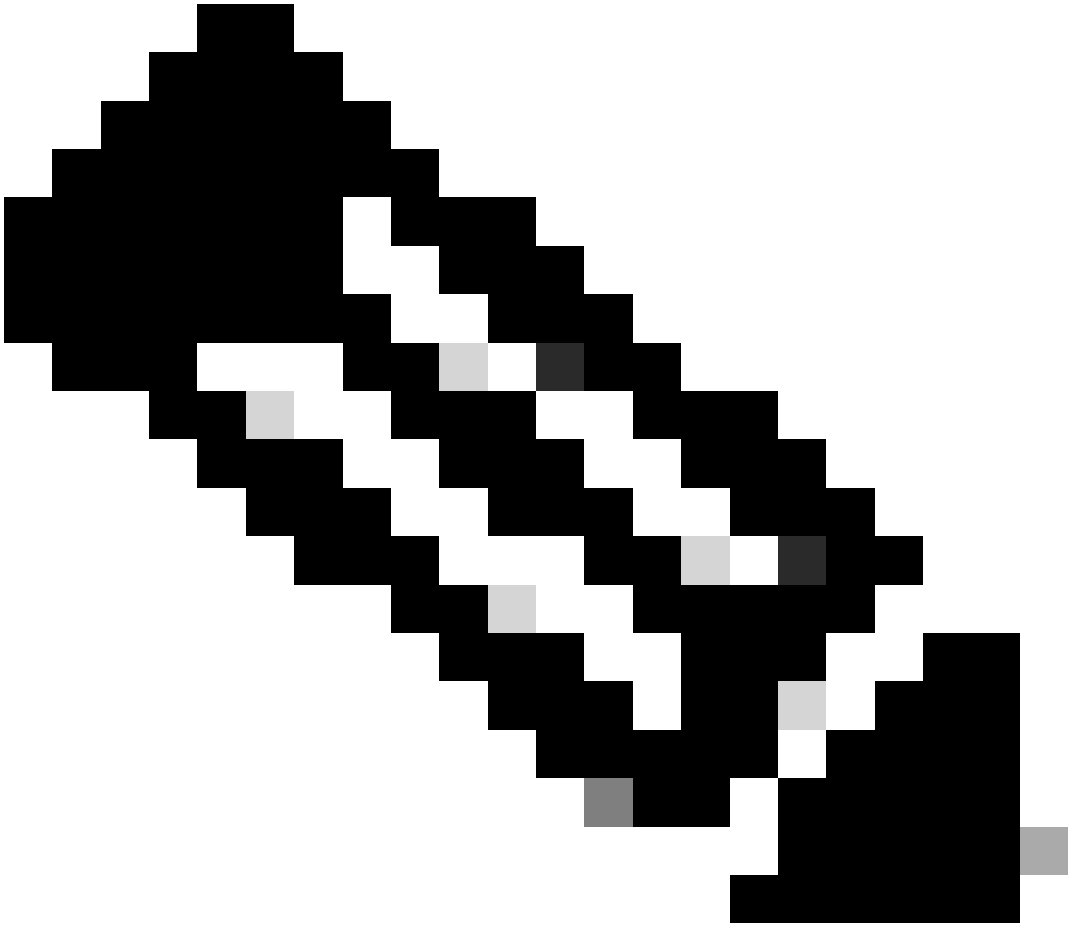
Option 182 suboption 5 on WLC Packet Capture

With the implementation of suboption 5, your DHCP traffic should be acknowledged by other network devices. However, you may still encounter NAK (negative acknowledgement) messages especially when the Windows DHCP server is in use. This could be due to the DHCP server not authorizing the source IP address, possibly because it doesn't have a corresponding configuration for that source IP.

What do you have to do on the DHCP server? For the Windows DHCP server, you have to create a dummy scope to authorize the IP of the relay agent.



Warning: All relay agent IP addresses (GIADDR) must be part of an active DHCP scope IP address range. Any GIADDR outside of the DHCP scope IP address ranges is considered a rogue relay and Windows DHCP Server will not acknowledge DHCP client requests from those relay agents. A special scope can be created to authorize relay agents. Create a scope with the GIADDR (or multiple if the GIADDRs are sequential IP addresses), exclude the GIADDR address(es) from distribution, and then activate the scope. This will authorize the relay agents while preventing the GIADDR addresses from being assigned.

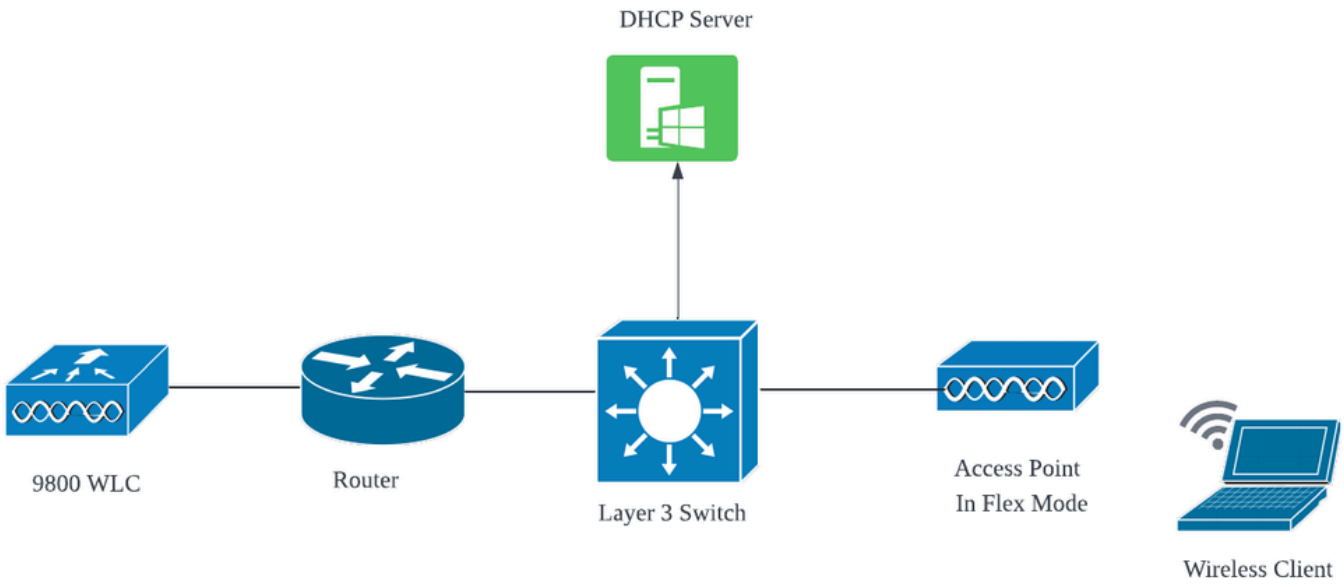


Note: In a foreign-anchor setup, DHCP traffic is centrally processed with AP mode set as Local. Initially, the DHCP requests are sent to the foreign WLC, which then forwards them to the anchor WLC via a mobility tunnel. It is the anchor WLC that handles the traffic according to its configured settings. Therefore, any configurations related to DHCP should be implemented on the anchor WLC.

Scenario 2. The Access Point (AP) is Operating in Flex Mode

FlexConnect APs are designed for branches and remote offices, allowing them to operate in a standalone mode when they lose connectivity to the central Wireless LAN Controller (WLC). FlexConnect APs can locally switch traffic between a client and the network without having to backhaul the traffic to the WLC. This reduces latency and conserves WAN bandwidth. In flex mode AP the DHCP traffic can be either centrally switched or locally switched.

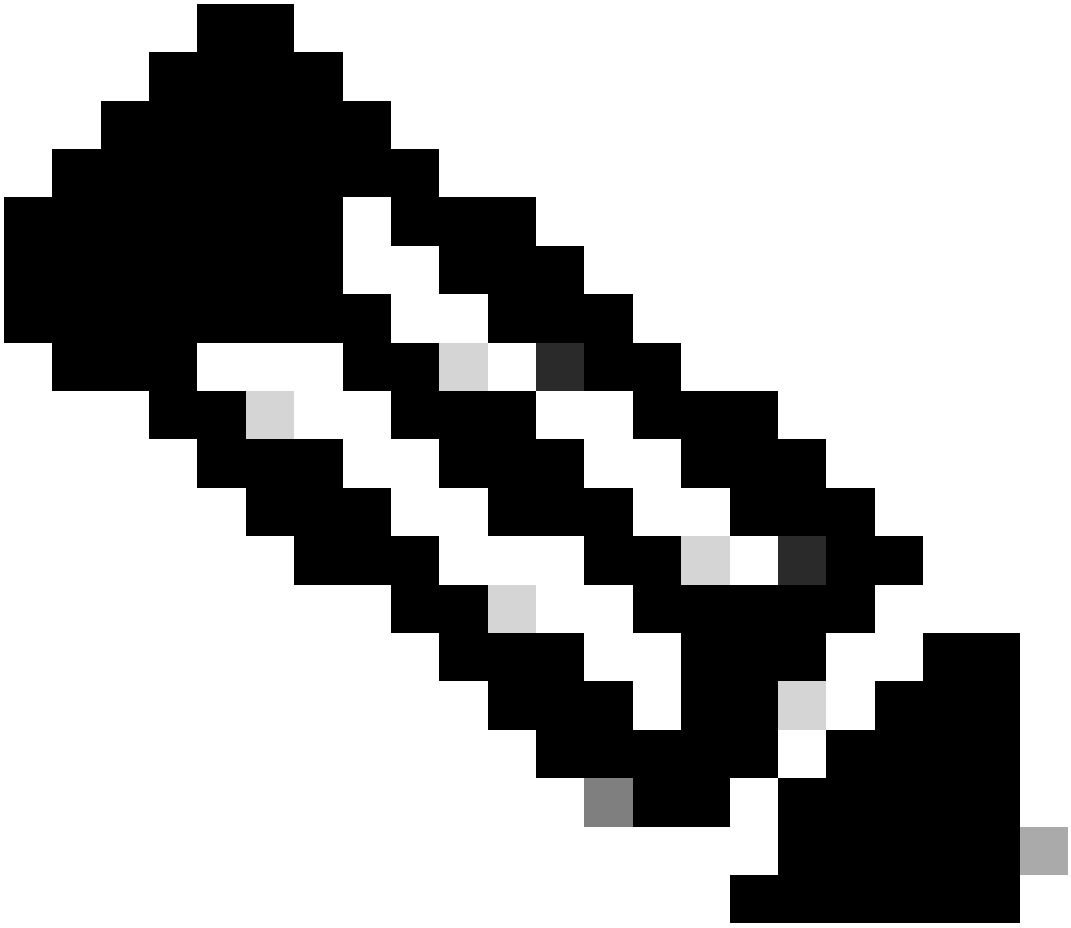
Topology (Flex Mode AP)



Network Topology: Flex Mode AP

FlexConnect Mode AP with Central DHCP

Regardless of the AP mode, the configuration, operational flow, and troubleshooting steps remain consistent when using a central DHCP server. However, for APs in FlexConnect mode, it's generally advised to use a local DHCP server unless you have a client SVI set up at the local site.



Note: If you don't have a client subnet available at the remote site, you can take advantage of FlexConnect NAT-PAT. FlexConnect NAT/PAT performs Network Address Translation (NAT) for the traffic originating from clients connected to the AP, mapping it to the AP's management IP address. For instance, if you have APs operating in FlexConnect mode at remote branches and the connected clients need to communicate with a DHCP server located at the headquarters where the controllers reside, you can activate FlexConnect NAT/PAT in conjunction with the Central DHCP setting in the Policy profile.

FlexConnect Mode AP with Local DHCP

When a FlexConnect AP is configured to use local DHCP, client devices that associate with the AP receive their IP address configuration from a DHCP server that is available within the same local network. This local DHCP server could be a router, a dedicated DHCP server, or any other network device providing DHCP services within the local subnet. With local DHCP, the DHCP traffic is switched within the local network, meaning that the AP relays DHCP requests from clients straight to the adjacent hop, such as the access switch. From there, the requests are handled according to the configuration of your network.

Prerequisite:

1. Please consult the FlexConnect guide to ensure that your configuration aligns with the instructions and best practices outlined in the guide.

2. Client VLAN should be listed under flex profile.
3. The AP needs to be set up in trunk mode, with the AP management VLAN designated as the native VLAN, and the VLANs for client traffic should be permitted on the trunk.

Here's an example of AP connected switchport configuration with management VLAN as 58 and client VLAN as 20:

```
Switch#show run int gig1/0/2
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 20,58
switchport trunk encapsulation dot1q
switchport trunk native vlan 58
switchport mode trunk
end
!
```

Working Setup: For reference sharing the operational logs with the Local DHCP server when AP is configured for flex mode:

AP Client Debugs:

```
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6056] [1712144373:605628] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6057] chatter: dhcp_req_local_sw_nonat: 1712144373.6056478
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] [1712144373:605830] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] chatter: dhcp_reply_nonat: 1712144373.605647862: 0.0
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.7462] [1712144376:746192] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9149] chatter: dhcp_from_inet: 1712144376.914892705: 10.10
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9150] chatter: dhcp_reply_nonat: 1712144376.914892705: 10.
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9151] [1712144376:915159] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9161] [1712144376:916101] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9373] [1712144376:937350] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9645] [1712144376:964530] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9646] chatter: dhcp_req_local_sw_nonat: 1712144376.9645492
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9647] [1712144376:964749] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] CLSM[client_mac]: client moved from IPLEARN_PENDING
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] [1712144376:973687] [AP_Name] [client_mac] <apr0v1>
```

AP Uplink Capture:

```
1399 18:37:…  0.0.0.0          255.255.255.255   DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1400 18:37:…  0.0.0.0          255.255.255.255   DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1499 18:37:…  0.0.0.0          255.255.255.255   DHCP    342 DHCP Discover - Transaction ID 0xb530583d
1500 18:37:…  0.0.0.0          255.255.255.255   DHCP    420 DHCP Discover - Transaction ID 0xb530583d
1545 18:38:…  10.106.20.10     255.255.255.255   DHCP    342 DHCP Offer    - Transaction ID 0xb530583d
1546 18:38:…  10.106.20.10     255.255.255.255   DHCP    420 DHCP Offer    - Transaction ID 0xb530583d
1547 18:38:…  10.106.20.10     255.255.255.255   DHCP    342 DHCP Offer    - Transaction ID 0xb530583d
1548 18:38:…  10.106.20.10     255.255.255.255   DHCP    420 DHCP Offer    - Transaction ID 0xb530583d
1553 18:38:…  0.0.0.0          255.255.255.255   DHCP    370 DHCP Request  - Transaction ID 0xb530583d
1555 18:38:…  0.0.0.0          255.255.255.255   DHCP    448 DHCP Request  - Transaction ID 0xb530583d
1556 18:38:…  10.106.20.10     255.255.255.255   DHCP    342 DHCP ACK      - Transaction ID 0xb530583d
1558 18:38:…  10.106.20.10     255.255.255.255   DHCP    420 DHCP ACK      - Transaction ID 0xb530583d
```

AP Uplink Capture

Client Side Capture:

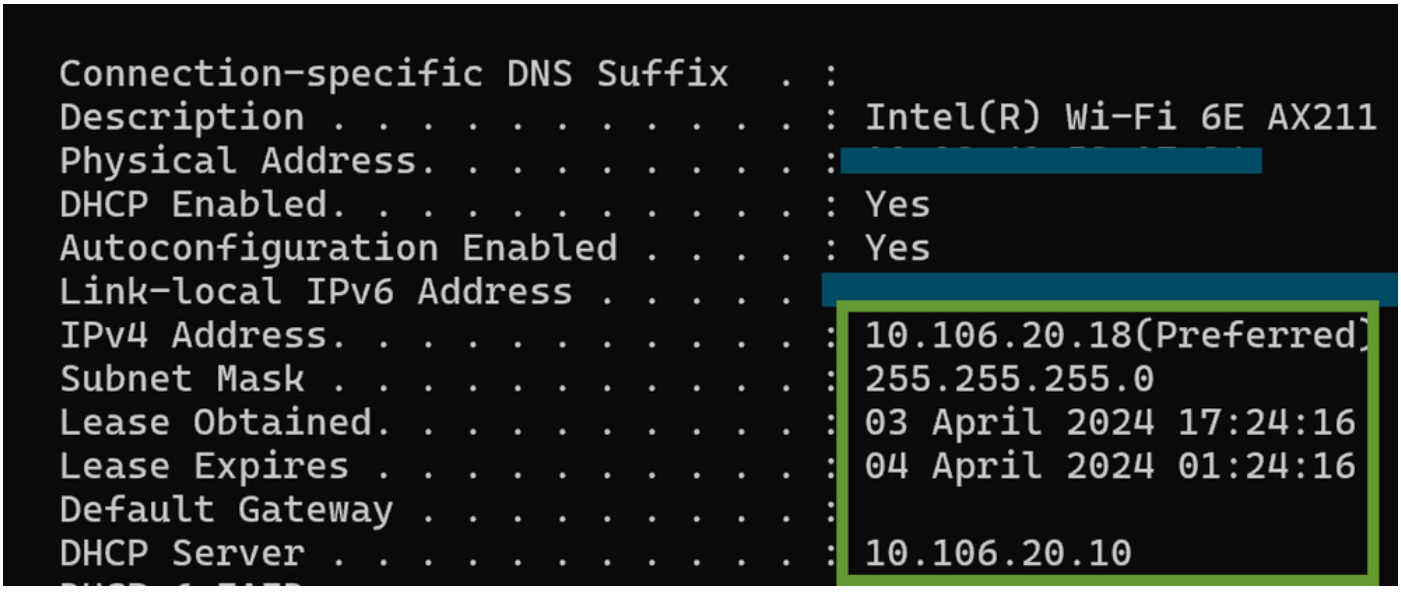
```
16540 111.905836    0.0.0.0          255.255.255.255   DHCP    343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18      DHCP    342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255   DHCP    385 DHCP Request  - Transaction ID 0x628c01b4
16543 112.304391    10.106.20.10     10.106.20.18      DHCP    342 DHCP ACK      - Transaction ID 0x628c01b4
```

Client End Packet Capture

Verification of Wireless Client IP:

You can check the IP lease on the DHCP server and its corresponding status.

On Wireless Client:



IP Verification on Client End

Troubleshooting of DHCP Issue

Troubleshooting DHCP issues involves identifying and resolving problems that prevent clients from obtaining an IP address from a DHCP server when connected to the wireless network. Here are some

common steps and considerations when troubleshooting DHCP problems:

1. Verify Client Configuration

- Ensure the client is configured to obtain an IP address automatically.
- Confirm that the network adapter is enabled and functioning properly.

2. Check DHCP Server Status

- Confirm that the DHCP server is operational and reachable from the client's network segment.
- Check the DHCP server's IP address, subnet mask, and default gateway settings.

3. Review Scope Configuration

- Inspect the DHCP scope to ensure it has a sufficient range of IP addresses available for clients.
- Verify the scope's lease duration and options, such as DNS servers and default gateway
- In some environments (like Active Directory), ensure the DHCP server is authorized to provide DHCP services within the network.

4. Review Configuration on 9800 WLC

- Many issues have been seen due to misconfiguration, such as a missing loopback interface, Client SVI or the absence of a configured helper address. Before log collection, it is recommended to verify that the configuration has been correctly implemented.
- When utilizing an internal DHCP server: Concerning the exhaustion of the DHCP scope, it's important to ensure, particularly when configuring DHCP via the CLI, that the lease timer is configured as per your requirements. By default, the lease timer is set to infinite on 9800 WLC.
- Verify that client VLAN traffic is permitted on the WLC uplink port when using a central DHCP server. Conversely, when employing a local DHCP server, ensure the relevant VLAN is allowed on the AP uplink port.

5. Firewall and Security Settings

- Ensure that firewalls or security software are not blocking DHCP traffic (port 67 for DHCP server and port 68 for DHCP client).

Log Collection

Logs from WLC

1. Enable term exec prompt timestamp to have time reference for all the commands.

2. Use show tech-support wireless !! to review the configuration

2. You can check the number of clients, client state distribution, and excluded clients.
show wireless summary !! Total number of APs and clients
show wireless exclusionlist !! In case any client is seen as excluded
show wireless exclusionlist client mac-address MAC@ !! to get more details about concrete client excluded and check if the reason is listed as IP theft for any client.

3. Check IP address assignment for clients, look for incorrect addresses or unexpected static address

learning, VLANs marked as dirty due to no response from DHCP server, or packets drops in SISF that is handling DHCP/ARP.

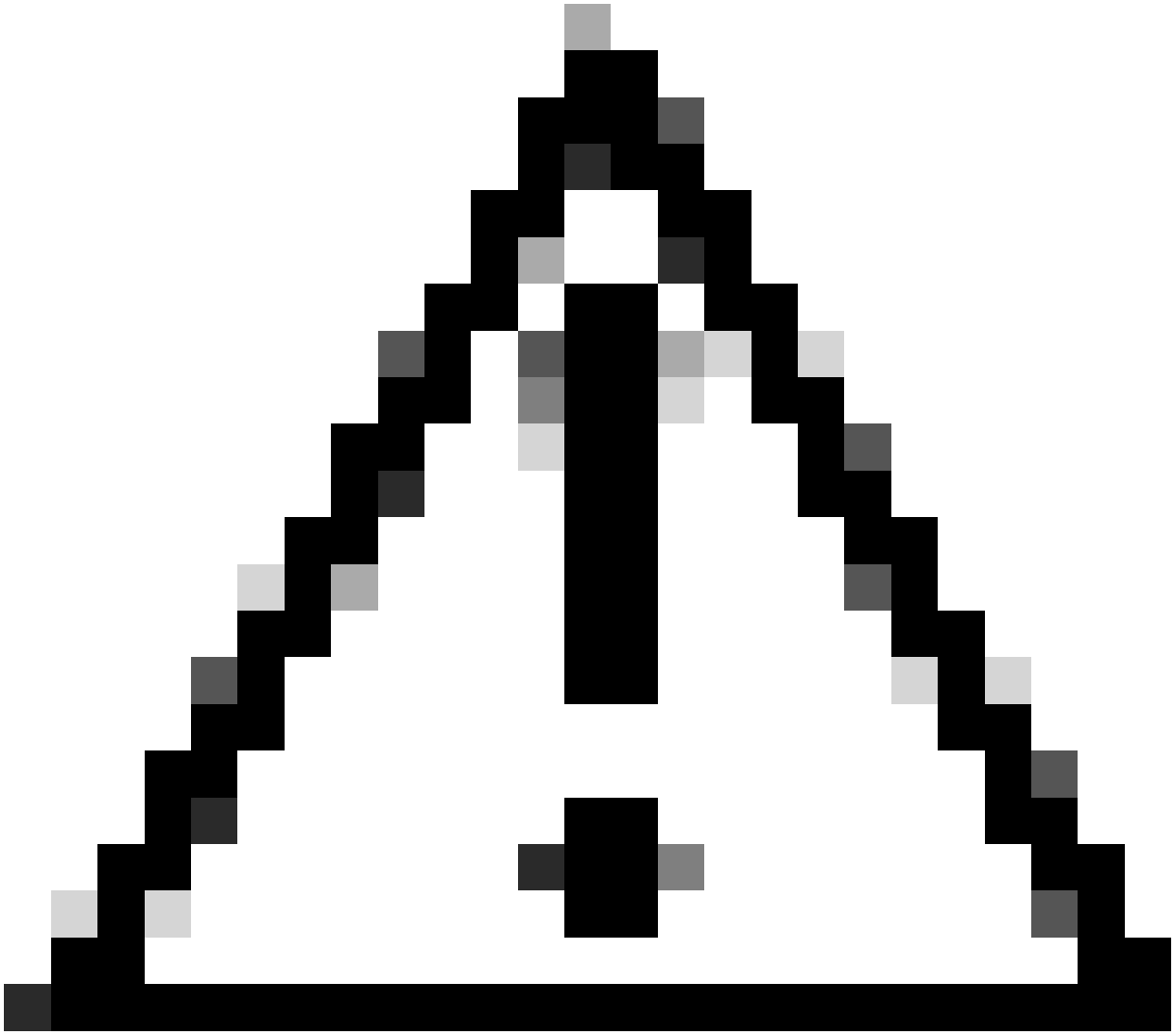
show wireless device-tracking database ip !! Check by IP and see how address learning occurred:
show wireless device-tracking database mac !! Check by Mac and see what IP client is assigned.
show wireless vlan details !! Check that VLAN is not marked as dirty due to DHCP failures in case of VLAN group in use.
show wireless device-tracking feature drop !!Drops in SISF

4. Specific outputs from WLC for concrete client MAC@ show wireless device-tracking feature drop

Enable radioactive trace for client MAC address when the client is trying to connect wireless network.

Via CLI:

```
debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting time allows
!!Reproduce [ Clients should stuck in IP learn]
no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
dir bootflash: | i debug
```



Caution: The conditional debugging enables debug-level logging which in turn increases the volume of the logs generated. Leaving this running reduces how far back in time you can view logs from. So, it is recommended to always disable debugging at the end of the troubleshooting session.

In order to disable all debugging, run these commands:

```
# clear platform condition all
# undebug all
```

Via GUI:

Step 1. Navigate to Troubleshooting > Radioactive Trace .
Step 2. Click Add and enter a client Mac address that you want to troubleshoot. You can add several Mac addresses to track.

Step 3. When you are ready to start the radioactive tracing, click start. Once started, debug logging is written to disk about any control plane processing related to the tracked MAC addresses.

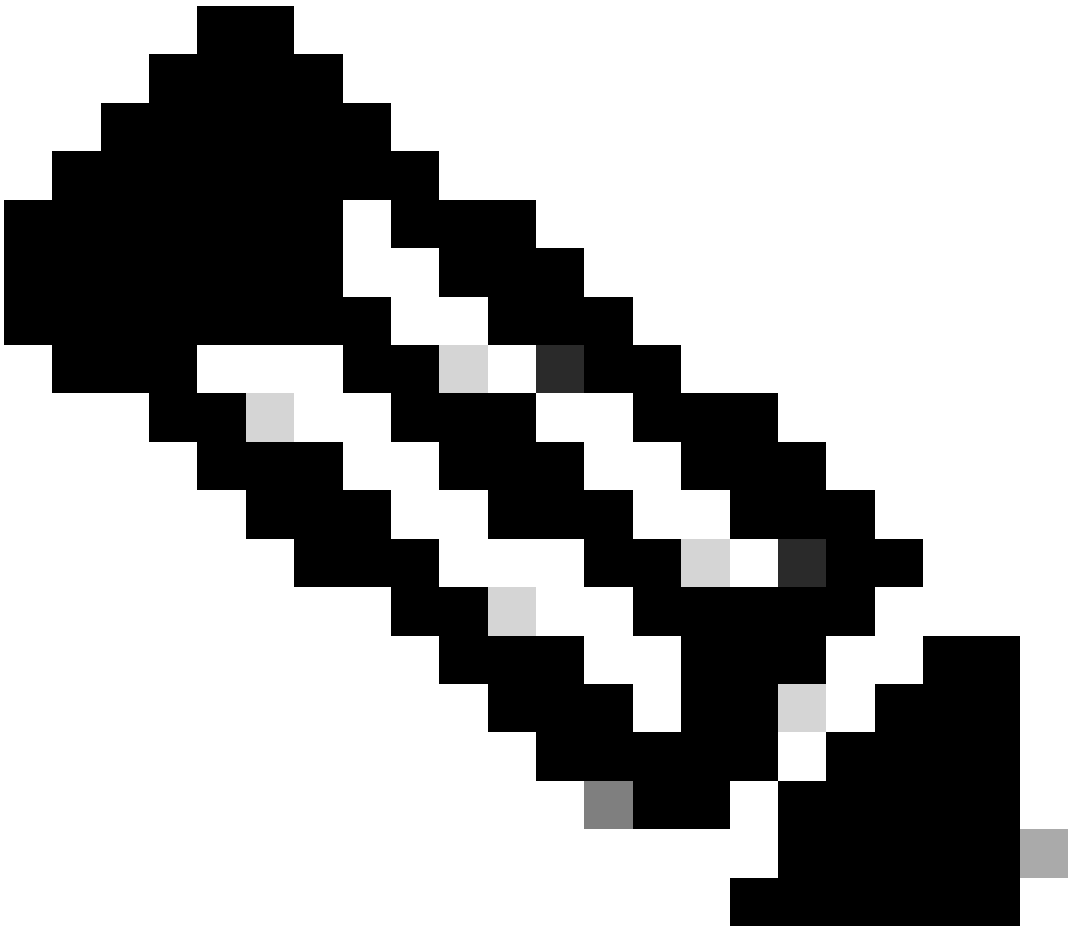
Step 4. When you reproduce the issue you want to troubleshoot, click Stop .

Step 5. For each mac address debugged, you can generate a log file collating all the logs pertaining to that mac address by clicking Generate .

Step 6. Choose how long back you want your collated log file to go and click Apply to Device.

Step 7. You can now download the file by clicking the small icon next to the file name. This file is present in the boot flash drive of the controller and can also be copied out of the box through CLI.

!!Embedded Captures filtered by client MAC address in both directions, Client inner MAC filter available after 17.1.



Note: EPC on 9800 will be useful when central DHCP is enabled on 9800 WLC.

Via CLI:

```
monitor capture MYCAP clear
monitor capture MYCAP interface Po1 both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!!Reproduce
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap
```

Via GUI:
Step 1. Navigate to Troubleshooting > Packet Capture > +Add .

Step 2. Define the name of the packet capture. A maximum of 8 characters is allowed.

Step 3. Define filters, if any.

Step 4. Check the box to Monitor Control Traffic if you want to see traffic punted to the system CPU and injected back into the data plane.

Step 5. Define buffer size. A maximum of 100 MB is allowed.

Step 6. Define limit, either by duration which allows a range of 1 - 1000000 seconds or by number of packets which allows a range of 1 - 100000 packets, as desired.

Step 7. Choose the interface from the list of interfaces in the left column and select the arrow to move it to the right column.

Step 8. Save and Apply to Device.

Step 9. To start the capture, select Start.

Step 10. You can let the capture run to the defined limit. To manually stop the capture, select Stop.

Step 11. Once stopped, an Export button becomes available to click with the option to download the capture file (.pcap) on the local desktop via HTTP or TFTP server or FTP server or local system hard disk or flash.

Logs from the AP Side

```
show tech !! Collect show tech to have all config details and client stats for the AP.
term mon
!!Basic
debug client MAC@
```

Logs from DHCP Server

When using an external DHCP server, it's necessary to gather debug logs and packet captures on the server side to verify the flow of DHCP traffic.

Other Logs

If you observe that the DHCP discover messages are visible on the 9800 WLC in a Central DHCP setup, or within AP debug logs in a Local DHCP setup, you should proceed to gather capture data from the uplink to confirm that the packets are not dropping in the Ethernet port.Depending on the switch's capabilities, you have the option to perform an embedded packet capture or a SPAN (Switched Port Analyzer) capture on the uplink switch. It is advisable to trace the DHCP traffic flow step by step to determine the point at which the communication is interrupted, both from the DHCP client to the DHCP server and in the reverse direction.

Known Issues

Issue 1. The client is attempting to obtain an IP address from a VLAN that it previously retained. Situations can arise where a wireless client switches between two SSIDs associated with different client VLANs. In such cases, the client may persist in requesting an IP from the VLAN it previously connected to. Because this IP will not be within the current VLAN's DHCP scope, the DHCP server will issue a NAK (negative acknowledgement), and as a result, the client will be unable to acquire an IP address.

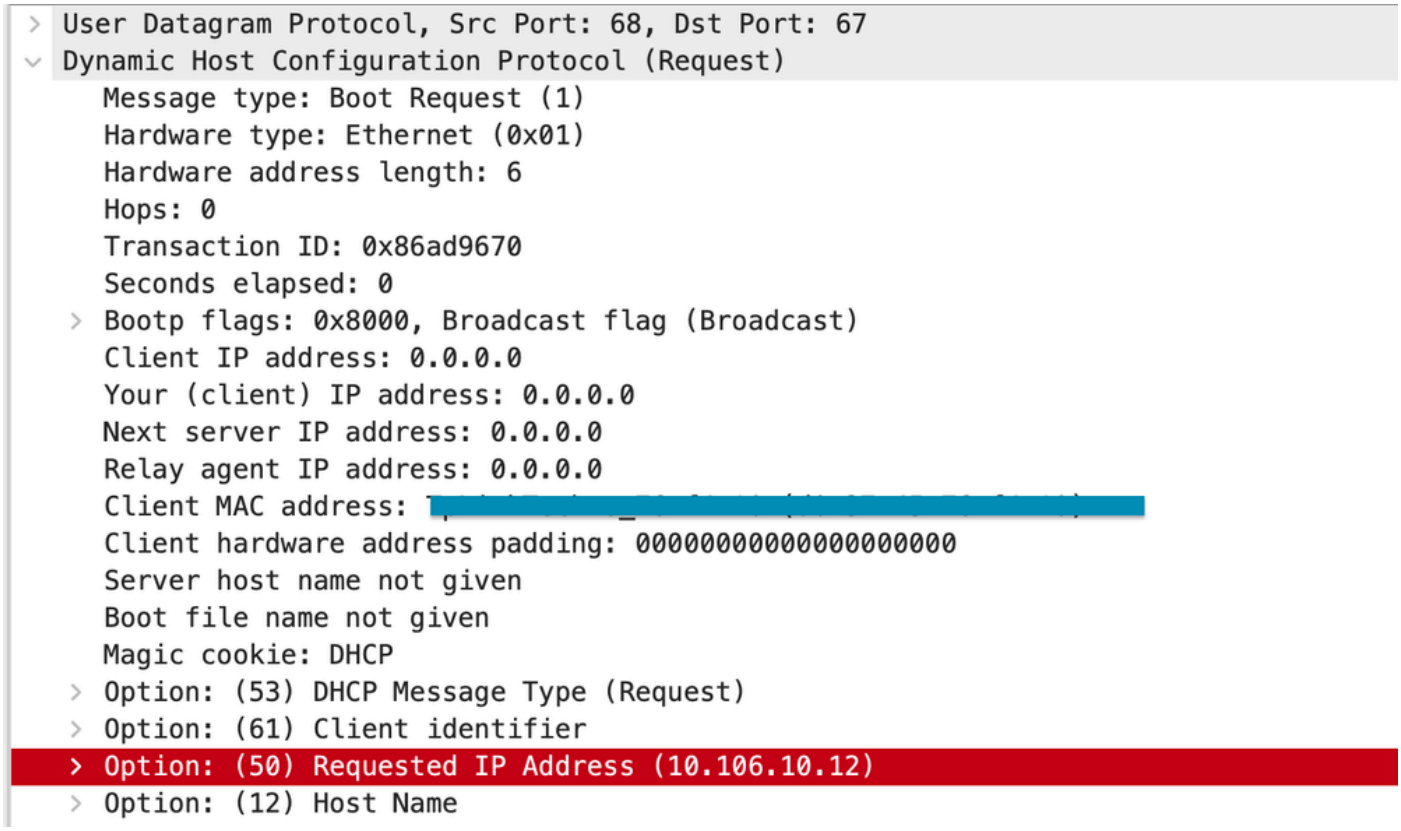
In the Radioactive trace logs, it is evident that the client continues to seek an IP from the VLAN it was formerly connected to, which is VLAN 10, despite the fact that the client VLAN for the current SSID is VLAN 20.

```
2024/03/30 10:40:43.050956833 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.051051895 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.058538643 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.058658561 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
```

Embedded Packet Capture on WLC:

```
166 16:10:…  0.0.0.0          255.255.255.255      DHCP     368 DHCP Request  - Transaction ID 0x86ad9670
167 16:10:…  0.0.0.0          255.255.255.255      DHCP     368 DHCP Request  - Transaction ID 0x86ad9670
168 16:10:…  10.106.20.10     255.255.255.255      DHCP     346 DHCP NAK      - Transaction ID 0x86ad9670
169 16:10:…  10.106.20.10     255.255.255.255      DHCP     346 DHCP NAK      - Transaction ID 0x86ad9670
```

Embedded Packet Capture on WLC



DHCP option 50 on WLC Packet capture

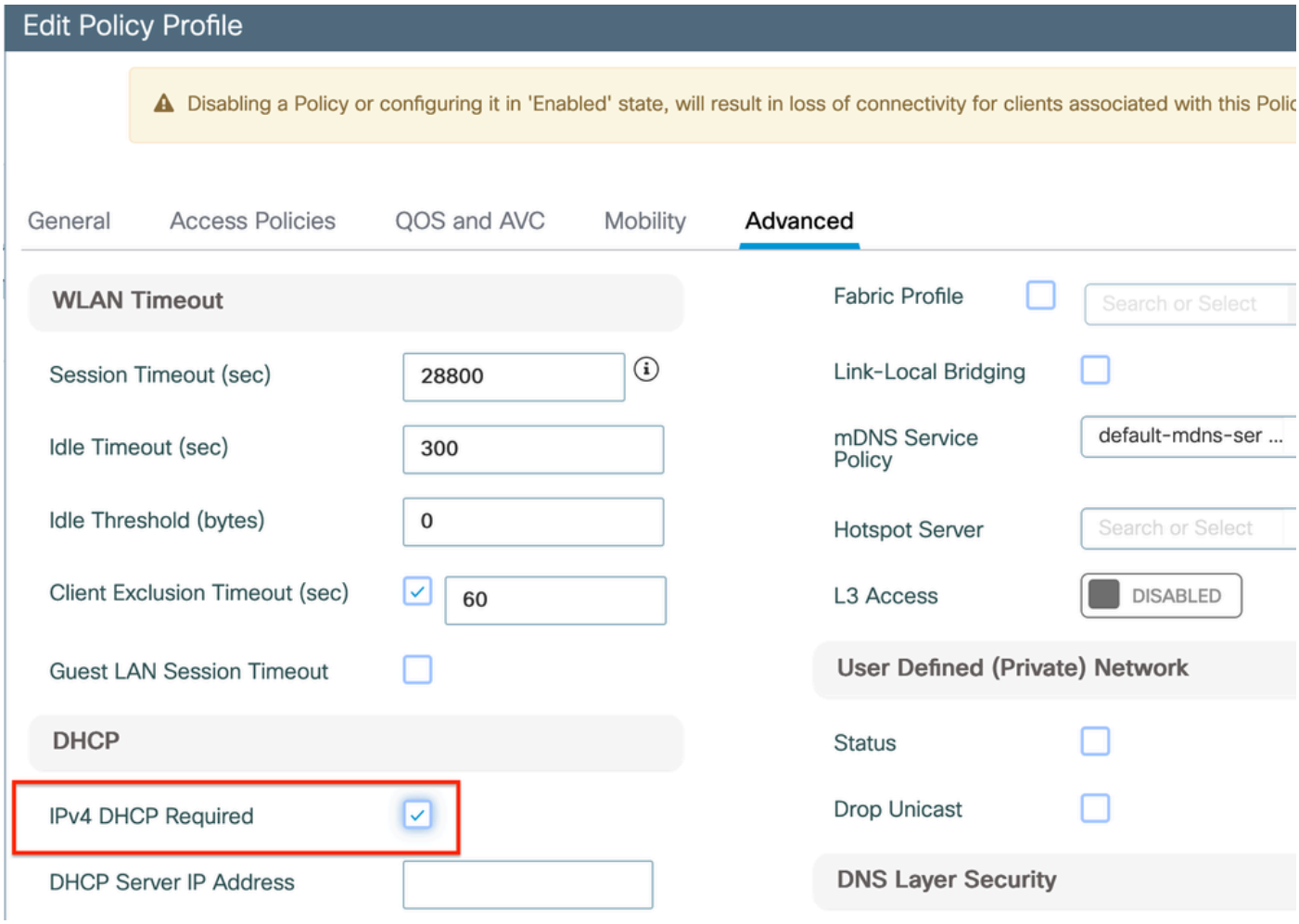
Resolution: To ensure that a client completes the full DHCP process, you can enable the IPv4 DHCP Required option within the policy configuration. This setting should be enabled, especially when the client is switching between SSIDs, to allow the DHCP server to send an NAK to the client if it requests an IP address from a VLAN associated with the previous SSID. Otherwise, the client might continue to use or request the IP address it previously held, leading to disrupted communication. However, be aware that enabling this feature will impact wireless clients that are configured with a static IP address.

Here's the process to enable the desired option:

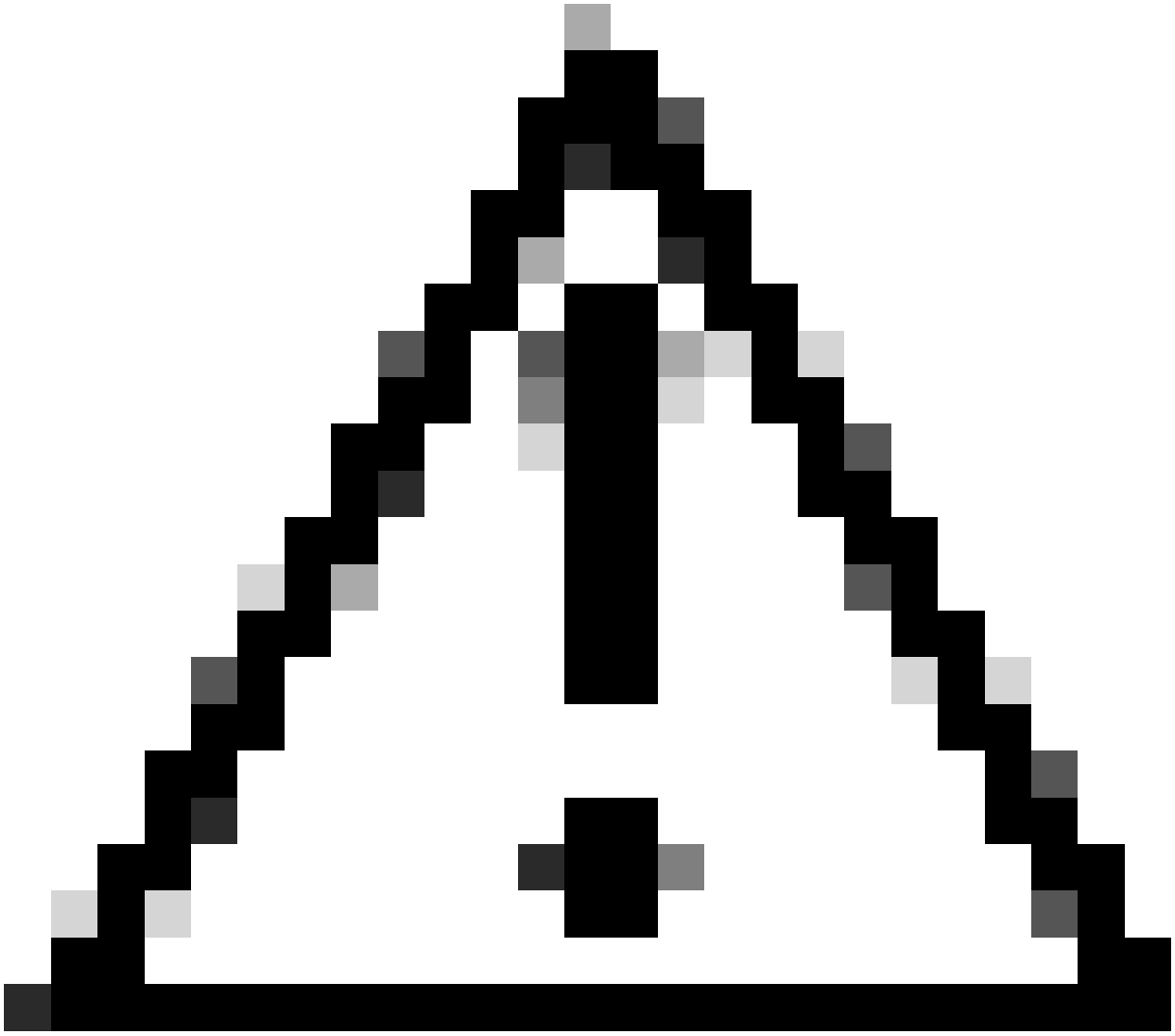
Via CLI:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
```

Via GUI: Navigate to Configuration > Tags & Profile > Policy > Policy_name > Advanced. Under the DHCP section enable ipv4 DHCP required.



Policy Profile Setting on WLC



Caution: For a foreign-anchor setup, it's important to align the DHCP settings across both WLCs. If you have IPV4 DHCP required enabled, it needs to be enabled on both the foreign and anchor WLCs. A discrepancy in the DHCP-related configuration under the policy profile between the two could cause clients to experience issues with their mobility roles.

Issue 2: Client getting deleted or excluded due to IP Theft issue. IP theft, in the context of networking, refers to a situation where more than one wireless client is trying to use the same IP address. It can be due to many reasons which are listed below:

1. Unauthorized Static IP Assignment: When a user sets a static IP address on their device that coincides with an IP already assigned or earmarked on the network, it can result in an IP conflict. This occurs when two devices attempt to operate with an identical IP address, which can disrupt network connections for either or both devices involved. To prevent such issues, it is essential to ensure that each client on the network is configured with a unique IP address.

2. Rogue DHCP Server: The presence of an unauthorized or rogue DHCP server on the network can lead to IP address allocation that clashes with the established IP addressing plan of the network. Such conflicts may result in several devices experiencing IP address collisions or obtaining incorrect network settings. To address this problem, efforts should be made to identify and eliminate the rogue DHCP server from the

network to prevent further IP conflicts within the same subnet.

3. Stale Entry of client in 9800 WLC: Sometimes, the controller may retain outdated/stale entries of an IP address that a client is attempting to acquire. In these cases, it becomes necessary to manually remove these stale entries from the 9800 WLC. Here's how to go about it:

- Run the radioactive trace for the mac address which is in the exclusion list and filter it with legit mac in the radioactive trace.
- You will be able to see the error logs: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: Client MAC: Affected_Client_MAC with IP: 10.37.57.24 was added to exclusion list, legit Client MAC: Legit_Client_MAC, IP: 10.37.57.24, reason: IP address theft
- Then run these commands:
  show wireless device-tracking database mac | sec $Legit_Client_MAC
  show wireless device-tracking database ip | sec $Legit_Client_MAC

(If there are any stale entries, you will be able to see more than one IP for a legit client Mac address: one is the original Ip while the other is the outdated/stale one].

Resolution: Delete the stale entries from 9800 WLC manually by using clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. In flex deployment with local DHCP server using the same subnet: In FlexConnect configurations, it is common for various remote locations to utilize a local DHCP server that assigns IP addresses from an identical subnet. This scenario may lead to wireless clients at different sites receiving the same IP address. Controllers within this network framework are programmed to detect when multiple client connections are using an identical IP address, interpreting this as potential IP theft. As a result, these clients are usually placed on a blocked list to prevent IP address conflicts.

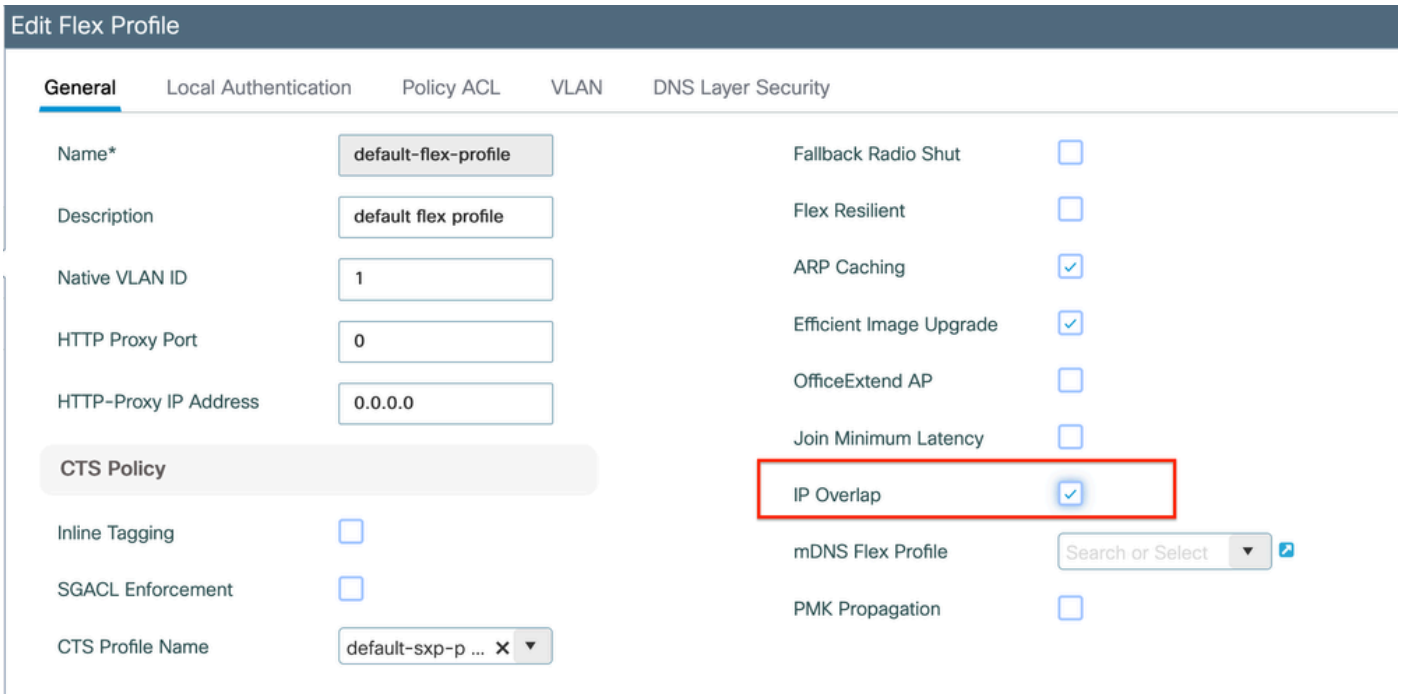
Resolution: Enable the IP overlap feature within your FlexConnect profile. The 'Overlapping Client IP Address in Flex Deployment' functionality allows for the use of the same IP addresses across multiple FlexConnect sites while maintaining all the features and capabilities supported in FlexConnect deployments.

By default this feature is disabled. You can enable it by this procedure:

Via CLI:

```
configure terminal
 wireless profile flex $Flex_Profile_name
 ip overlap
```

Via GUI: Select Configuration > Tags & Profiles > Flex. Click on Existing Flex Profile/Add to new Flex profile and under General tab enable IP Overlap.



Flex Profile Setting on WLC

Issue 3. Wireless clients are failing to receive an IP address from the intended VLAN. This problem often occurs when VLAN 1 is utilized or when the VLAN assigned to clients is the same as the VLAN used for AP management in a FlexConnect deployment. The root cause of this issue is typically incorrect VLAN assignments. To provide guidance, here are a few scenarios to consider when configuring VLAN IDs on the 9800 series:

1. When employing an AAA server with the AAA override feature activated, it is crucial to ensure that the appropriate VLAN ID is being sent from the AAA server. If a VLAN name is provided instead, confirm that it matches the VLAN name configured on the 9800 WLC.

2. When VLAN 1 is configured for wireless client traffic, the behavior may vary based on the mode of the access point (AP):

For an AP in local mode/Central switching:

- Specifying VLAN-name = default, the client is assigned to VLAN 1
- Using VLAN-ID 1, a client is assigned to wireless management VLAN

For an AP in Flex mode/Local Switching:

- Specifying VLAN-name = default, the client is assigned to VLAN 1
- Using VLAN-ID 1, a client is assigned to FlexConnect native VLAN

Here are a few more examples of scenarios that have been experimented with in the lab, along with their results:

1. By default, if the user does not configure anything under the policy profile, the WLC assigns VLAN-ID 1 so clients will use the wireless management VLAN in local mode and the AP native VLAN for FlexConnect.

2. If the Native-VLAN under flex-profile is configured with a native VLAN ID different from the one configured on the switch, you see the issue, the client gets IP from management VLAN (native VLAN) even

if the policy-profile is configured with “default” VLAN name.

3. If Native-VLAN under flex-profile is configured with VLAN-ID the same as the native VLAN configured on the switch, then only the client will be able to get an IP from VLAN 1 with default configured under policy profile.

4. If you selected a VLAN name instead of a VLAN ID, ensure the VLAN name in the Flex Profile is the same one.

Related Information

- Internal DHCP server on 9800
- External DHCP server in use
- DHCP option 82 Sub Option 5 in Windows DHCP server
- NAT-PAT in Flex AP
- VLAN 1 is used for Wireless Client
- Cisco Technical Support & Downloads