排除Cisco 9800 WLC上的DHCP客户端连接问题

目录

简介

本文档将介绍无线客户端在连接到Cisco 9800无线LAN控制器(WLC)时遇到的各种动态主机配置协议(DHCP)相关问题以及如何解决这些问题。

先决条件

Cisco 建议您了解以下主题：

- Cisco WLC 9800的基础知识
- DHCP流基础知识
- 本地和Flex连接模式AP的基础知识

了解无线客户端的DHCP流量流

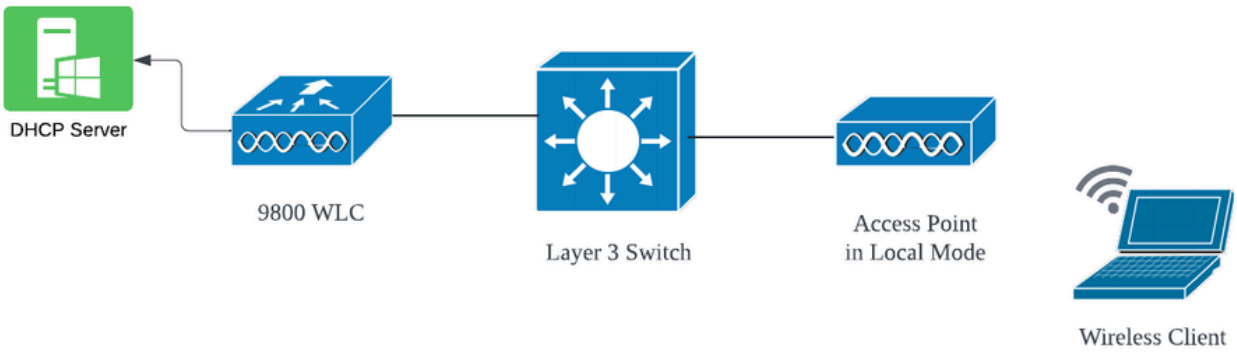
当无线客户端连接时，它通过发送广播DHCP发现帧执行常规的DHCP交换，以向关联的AP查找DHCP服务器。根据AP的操作模式，它将通过CAPWAP隧道将请求转发到WLC，或者直接将其传递到下一跳。如果DHCP服务器在本地第2层域中可用，它将做出响应，促进连接成功。如果没有本地子网DHCP服务器，则必须设置路由器（使用客户端的SVI配置）以将DHCP发现路由到相应的服务器。这通常通过在路由器上配置IP帮助地址来完成，该地址指示路由器将特定广播UDP流量（例如DHCP请求）转发到预先确定的IP地址。

客户端DHCP流量的行为完全取决于接入点(AP)的运行模式。让我们分别了解一下这些场景：

场景 1.接入点(AP)在本地模式下运行

在Local Mode下设置AP时，客户端DHCP流量会集中交换，这意味着客户端的DHCP请求会通过CAPWAP隧道从AP发送到WLC，然后在其中进行相应的处理和转发。在这种情况下，您有两种选择：可以使用内部DHCP服务器或选择外部DHCP服务器。

拓扑（本地模式AP）



网络拓扑：本地模式*AP*

案例研究1.当WLC配置为内部DHCP服务器时

控制器能够通过Cisco IOS XE软件的集成功能提供内部DHCP服务器。但是，最佳做法是使用外部DHCP服务器。在将WLC设置为内部DHCP服务器之前，必须满足以下几个先决条件：

- 确保为客户端VLAN配置交换虚拟接口(SVI)，并为其分配DHCP服务器的IP地址。
- 应在面向服务器的接口上设置内部DHCP服务器的IP地址，该接口可以是环回接口、SVI或第

3层物理接口。

- 建议配置环回接口，因为环回接口与连接到实际网段的物理接口不同，它不与硬件绑定，也不与设备上的物理端口对应。环回接口的主要用途是提供稳定、始终开启的接口，不受硬件故障或物理断开的影响。

工作设置：以下是客户端成功接收IP地址的内部DHCP服务器配置示例。以下是运行日志和相关设置详细信息。

将WLC设置为VLAN 10的DHCP服务器，DHCP范围从10.106.10.11/24到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
```

WLC上配置的环回接口：

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

将客户端VLAN配置为SVI [L3接口]，并将帮助程序地址用作WLC上的环回接口：

<#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
```

或者，您可以在策略配置文件中设置DHCP服务器的IP地址，而不是在SVI下配置帮助地址。但是，为了获得最佳实践，通常建议为每个VLAN配置此功能：

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

WLC上的放射性痕迹：

```
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
```

WLC上的嵌入式数据包捕获：

```
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
```

WLC上的嵌入式数据包捕获

AP客户端调试：

```
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>
```

客户端数据包捕获：

```
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
```

客户端数据包捕获

在提供的操作日志中，您可以看到WLC正在从无线客户端接收DHCP发现消息，并且客户端的VLAN正在将其中继到帮助地址（在提供的示例中，该地址是内部环回接口）。之后，内部服务器发出DHCP Offer，随后，客户端发送DHCP请求，然后服务器使用DHCP ACK确认该请求。

无线客户端IP验证：

在WLC上：

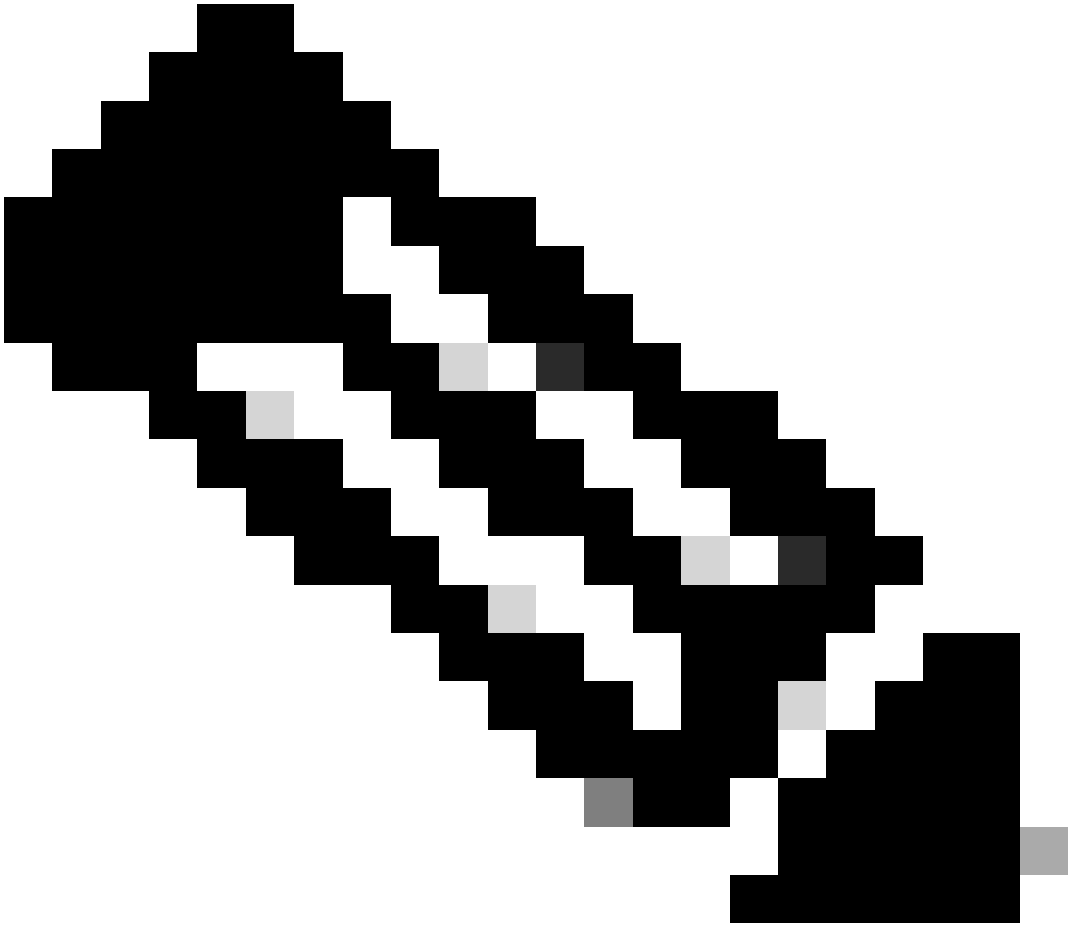
```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type          State
10.106.10.12      aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active     L
```

在无线客户端上：

```
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
```

客户端上的*IP*验证



注意：
1. 内部DHCP服务器不支持VRF。
2. 内部DHCP服务器不支持DHCPv6。
3. 在C9800上，SVI允许配置多个帮助地址，但仅使用前2个。
4. 这已经过测试，因此在所有平台上都受支持，最多占机箱最大客户端规模的20%。例如，对于支持64,000个客户端的9800-80，支持的最大DHCP绑定约为14,000个。

案例分析2.使用外部DHCP服务器时

外部DHCP服务器是指未集成到WLC本身中，但配置在不同的网络设备[防火墙、路由器]或网络基础设施中的独立实体上的DHCP服务器。此服务器专用于管理IP地址和其他网络配置参数动态分配到网络上的客户端。

当使用外部DHCP服务器时，WLC的功能仅仅是接收和中继流量。从WLC路由DHCP流量的方式（无论是广播流量还是单播流量）因您的首选项而异。让我们分别考虑这些方法。

第2层域中的DHCP流量广播

在此设置中，其他网络设备（例如防火墙、上行链路或核心交换机）充当中继代理。当客户端广播DHCP发现请求时，WLC的唯一工作是通过第2层接口转发此广播。要正常工作，您必须确保客户端VLAN的第2层接口配置正确并允许其通过WLC的数据端口和上行链路设备。

WLC端上此实例的客户端VLAN 20的所需配置：

在WLC上配置的第2层VLAN：

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

在WLC上配置数据端口，以允许客户端VLAN的流量：

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

9800 WLC上的放射性痕迹：

```
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
```

9800 WLC上的嵌入式数据包捕获：

```
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
```

WLC上的嵌入式数据包捕获

AP客户端调试：

```
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>
```

客户端捕获：

```
  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
```

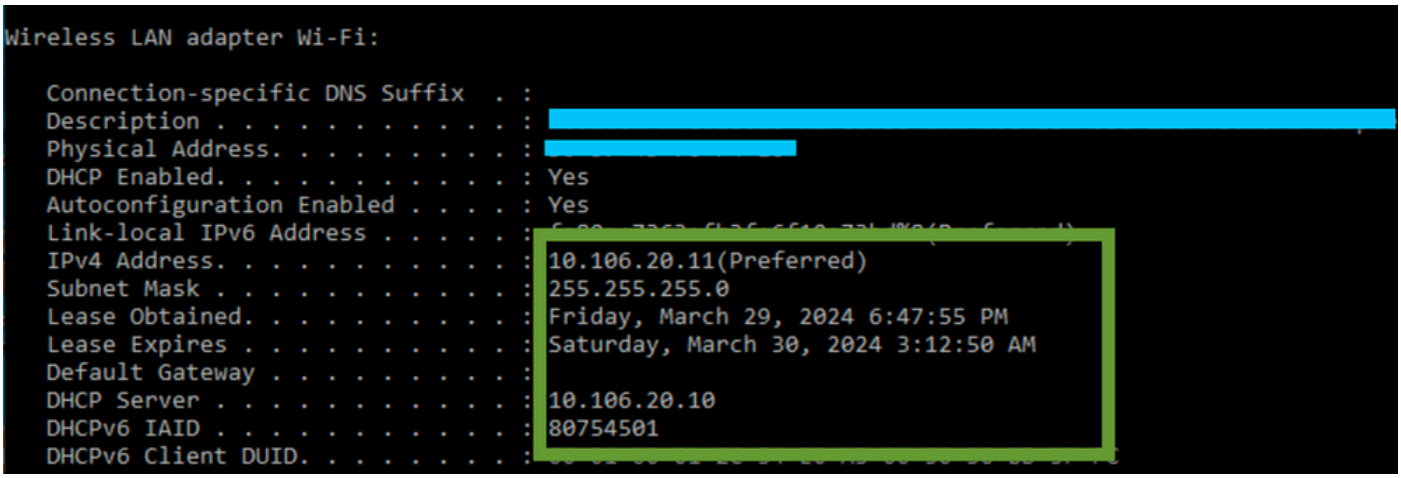
客户端数据包捕获

在提供的操作日志中，您注意到WLC拦截来自无线客户端的DHCP发现广播，然后通过其第2层接口将其广播到下一跳。当WLC收到来自服务器的DHCP Offer时，它就会将该消息转发到客户端，然后是DHCP Request和ACK。

无线客户端IP验证：

您可以检查DHCP服务器上的IP租用及其相应的状态。

在无线客户端上：



客户端上的*IP*验证

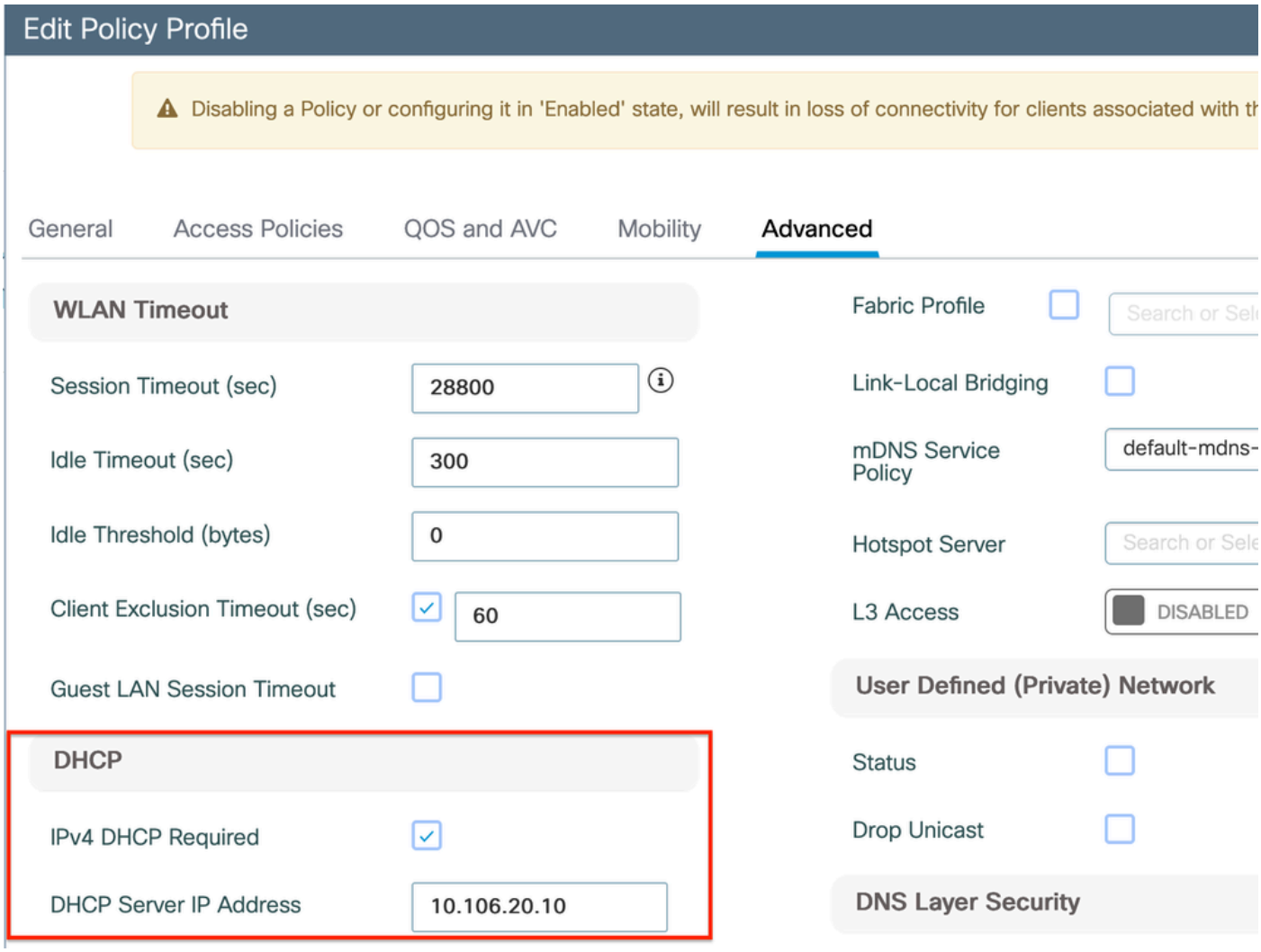
9800 WLC充当中继代理

在此配置中，WLC通过单播直接将从无线客户端收到的DHCP数据包转发到DHCP服务器。要启用此功能，请确保在WLC上配置客户端的VLAN SVI。

在9800 WLC中配置DHCP服务器IP的方法有两种：

1. 在“高级设置”下的“策略配置文件”下配置DHCP服务器IP。

通过GUI：导航至DHCP部分下的Configuration > Tags & Profile > Policy > Policy_name > Advanced. ，您可以配置DHCP服务器IP，如下所示：



WLC上的策略配置文件设置

通过CLI：

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

2. 在SVI配置中，您必须指定帮助地址。可以在帮助地址配置中设置多个DHCP服务器以提供冗余。虽然可以为策略配置文件中的每个WLAN设置DHCP服务器地址，但建议的方法是按接口逐一进行配置。这可以通过为相应的SVI分配帮助地址来实现。

当采用中继功能时，DHCP流量的源将是客户端的交换虚拟接口(SVI)的IP地址。然后，该流量通过与路由表确定的目标（DHCP服务器的IP地址）对应的接口进行路由。

以下是9800作为中继代理的工作配置示例：

使用帮助地址为WLC上的客户端VLAN配置的第3层接口：

```
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
```

在WLC上配置数据端口，以允许客户端VLAN的流量：

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

来自WLC的RA跟踪：

```
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
```

WLC上的嵌入式数据包捕获：

No.	Time	Source	Destination	Protocol	Lengtr	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

WLC上的嵌入式数据包捕获

在WLC上的放射性跟踪(RA)和嵌入式数据包捕获(EPC)中，您会注意到，作为中继代理的WLC直接将DHCP数据包从客户端单播到DHCP服务器。

AP客户端调试：

```
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>
```

客户端捕获：

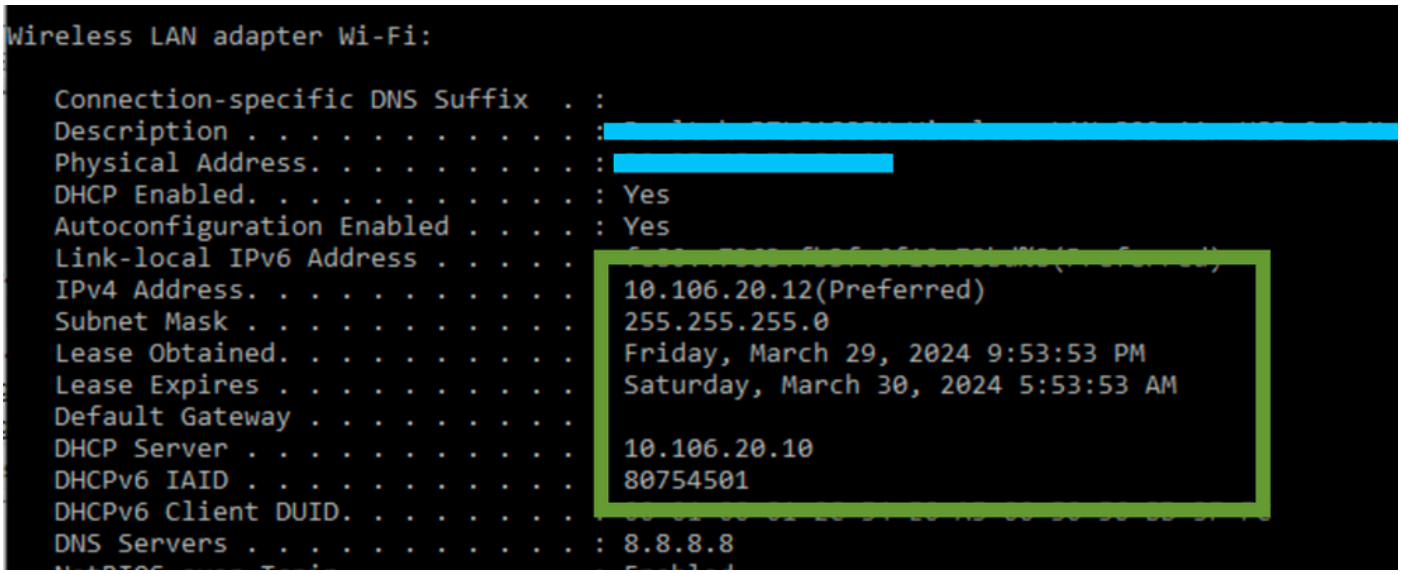
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - 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

客户端数据包捕获

无线客户端IP验证：

您可以检查DHCP服务器上的IP租用及其相应的状态。

在无线客户端上：



客户端上的*IP*验证

9800 WLC中带有子选项5/150的DHCP选项80

在某些情况下，您可能更愿意明确定义DHCP流量的源接口，而不是根据路由表来定义，以防止潜在的网络复杂性。当路径沿途的下一台网络设备（例如第3层交换机或防火墙）采用反向路径转发(RPF)检查时，这一点尤其重要。例如，无线管理接口设置在VLAN 50上，而客户端SVI设置在VLAN 20上并用作客户端流量的DHCP中继。默认路由指向无线管理VLAN/子网的网关。

从9800 WLC上的版本17.03.03开始，可以为DHCP流量选择源接口，使其成为客户端VLAN或另一个VLAN（例如无线管理接口

[WMI]），从而保证与DHCP服务器的连接。

下面是配置片段：

```
!
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
```

在此场景中，到DHCP服务器10.100.17.14的流量将来自VLAN 50 (10.100.16.10)，因为数据包的送出接口是基于IP路由表中的查找选择的，并且由于配置了默认路由，通常它将通过无线管理接口(WMI) VLAN送出。
但是，如果上行链路交换机实施反向路径转发(RPF)检查，它可能会丢弃来自VLAN 50但其IP源地址属于其他子网[VLAN 20]的数据包。

要防止出现这种情况，您应该使用IP DHCP relay source-interface命令为DHCP数据包设置一个精确的源接口。在这种情况下，您希望从VLAN 50上的WMI接口发出DHCP数据包：

```
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
```

使用ip dhcp relay source-interface命令时，DHCP数据包的源接口和GIADDR都设置为在DHCP中继命令中指定的接口（本例中为VLAN50）。这是一个问题，因为这不是您要分配DHCP地址的客户端VLAN。

DHCP服务器如何知道如何从正确的客户端池分配IP？

因此，当使用ip dhcp relay source-interface 命令时，C9800会自动将客户端子网信息添加到选项82的专有子选项150（称为链路选择）中，正如您在捕获图中所看到的：

```
Relay agent IP address: 10.100.16.10
Client MAC address: [redacted]
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
v Option: (82) Agent Information Option
    Length: 6
  v Option 82 Suboption: (150) Link selection (Cisco proprietary) (192.168.4.2)
      Length: 4
      Link selection (Cisco proprietary): 192.168.4.2
```

Option 182 WLC数据包捕获上的子选项150

默认情况下，它将添加子选项150（思科专有）。确保使用的DHCP服务器可以解释此信息并根据此信息执行操作。建议将C9800配置更改为使用标准选项82子选项5发送链路选择信息。您可以通过配置以下全局命令执行此操作：

<#root>

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

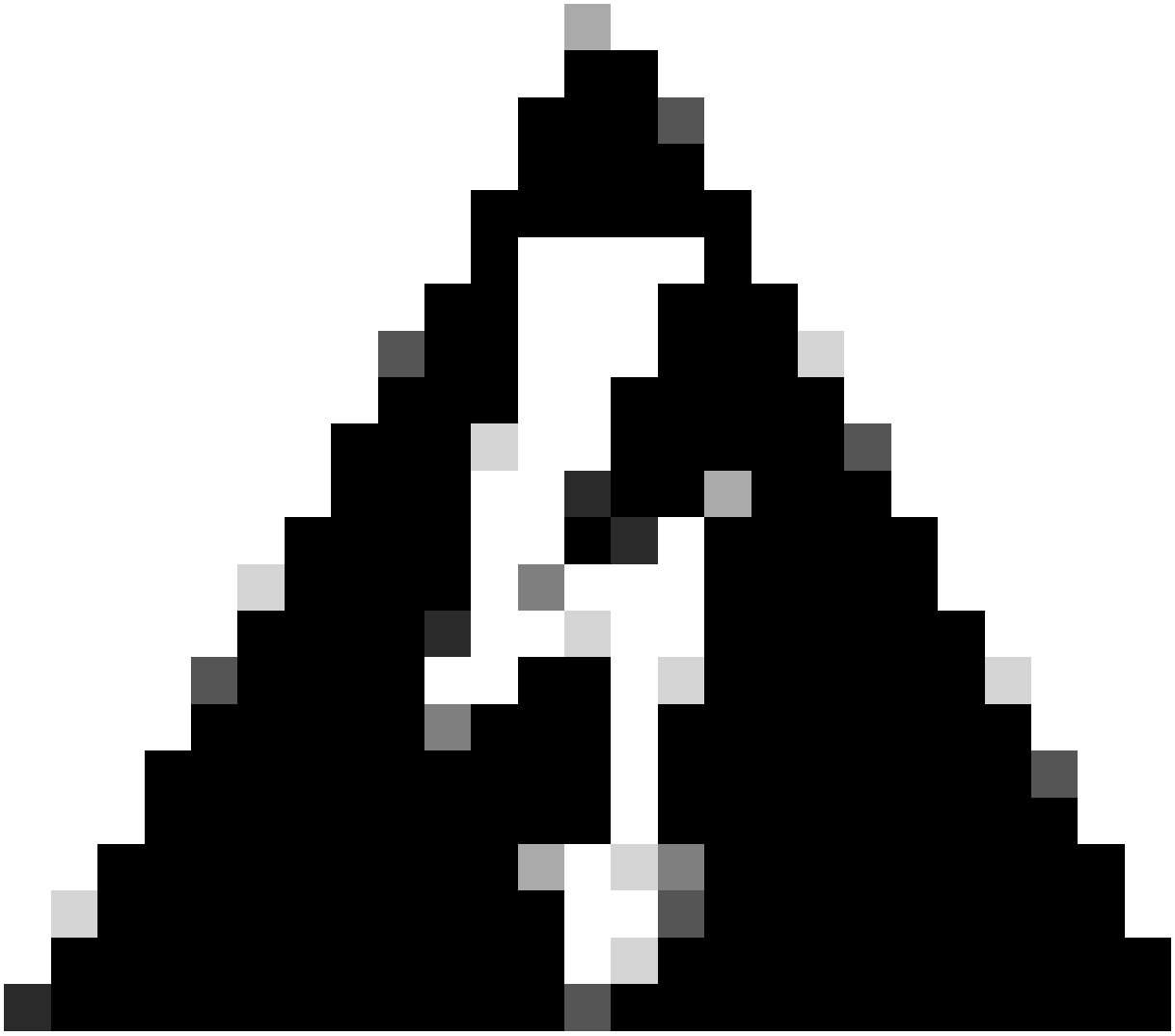
应用指定的命令后，系统将使用DHCP数据包中的子选项5替换子选项150。子选项5被网络设备更广泛地识别，因此可以确保数据包不易被丢弃。此更改的应用在所提供的捕获中也很明显：

```
Relay agent IP address: 10.100.16.10
Client MAC address: [redacted]
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
v Option: (82) Agent Information Option
    Length: 6
  > Option 82 Suboption: (5) Link selection (192.168.4.2)
```

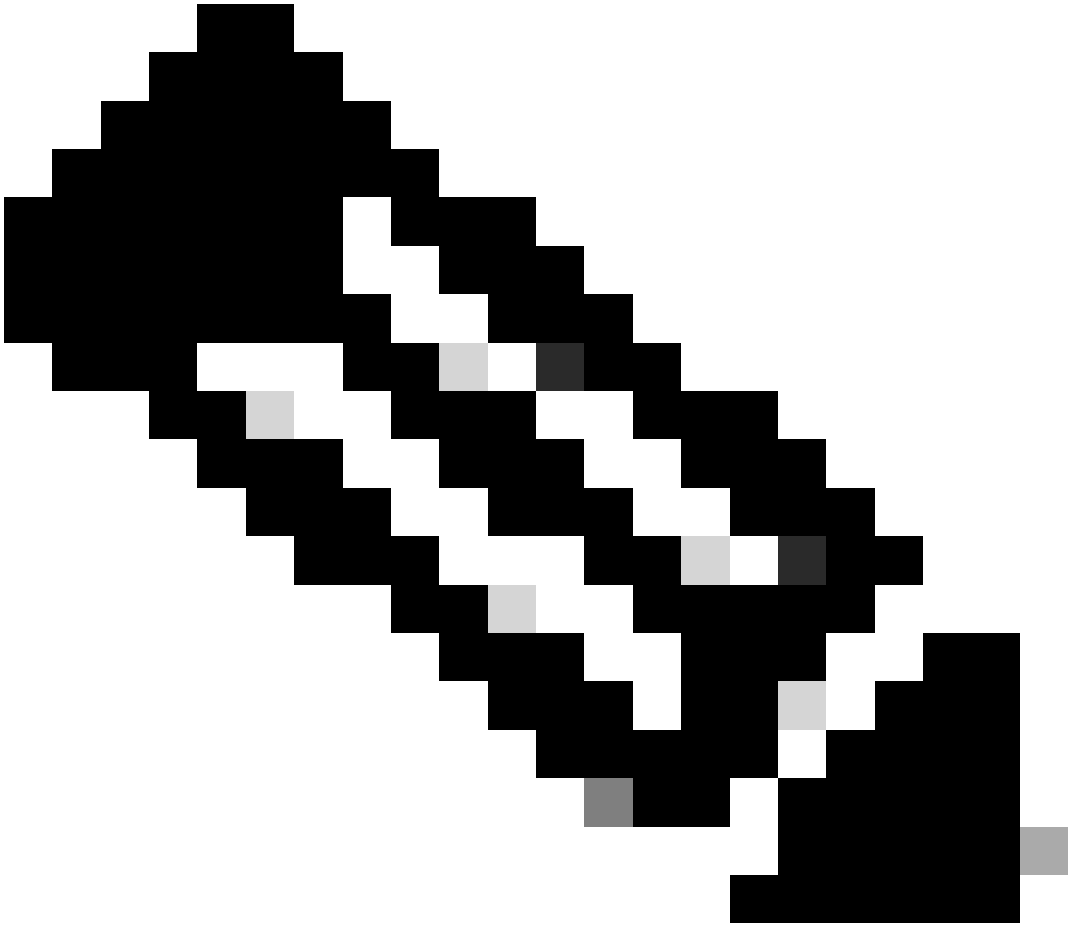
选项182 *WLC*数据包捕获上的子选项5

实施子选项5后，您的DHCP流量应由其他网络设备确认。但是，您仍可能会遇到NAK（否定确认）消息，特别是在使用Windows DHCP服务器时。这可能是因为DHCP服务器未授权源IP地址，可能是因为它没有该源IP的相应配置。

您必须在DHCP服务器上执行什么操作？对于Windows DHCP服务器，必须创建虚拟作用域以授权中继代理的IP。



警告：所有中继代理IP地址(GIADDR)必须是活动DHCP范围IP地址范围的一部分。DHCP范围IP地址范围之外的任何GIADDR都被视为恶意中继，Windows DHCP服务器不会确认来自这些中继代理的DHCP客户端请求。可以创建特殊范围以授权中继代理。使用GIADDR创建范围（如果GIADDR是连续的IP地址，则创建多个），从分发中排除GIADDR地址，然后激活范围。这将授权中继代理，同时阻止分配GIADDR地址。

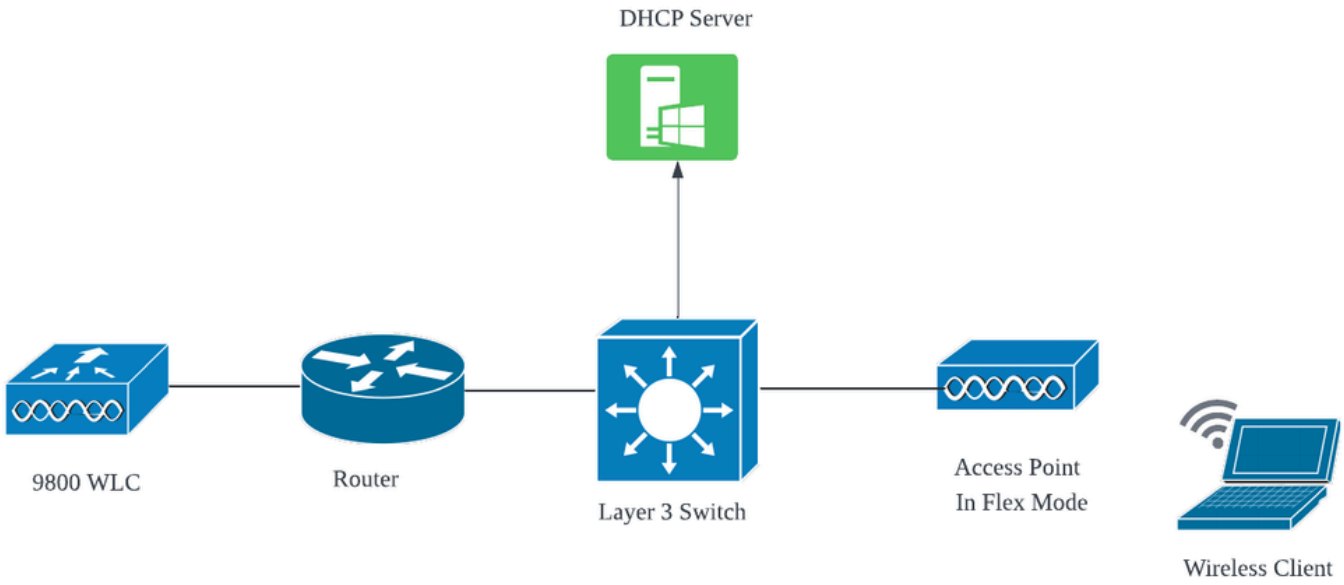


注意：在外锚点设置中，DHCP流量在将AP模式设置为“本地”的情况下进行集中处理。最初，DHCP请求发送到外部WLC，然后外部WLC通过移动隧道将其转发到锚点WLC。它是根据已配置的设置处理流量的锚点WLC。因此，应在锚点WLC上实施与DHCP相关的所有配置。

场景 2：接入点(AP)在Flex模式下运行

FlexConnect AP专为分支机构和远程办公室设计，允许他们在与中央无线局域网控制器(WLC)失去连接时在单机模式下运行。FlexConnect AP可以在本地交换客户端与网络之间的流量，而无需将流量回传到WLC。这样可以降低延迟并节约广域网带宽。在Flex模式AP中，DHCP流量可集中交换或本地交换。

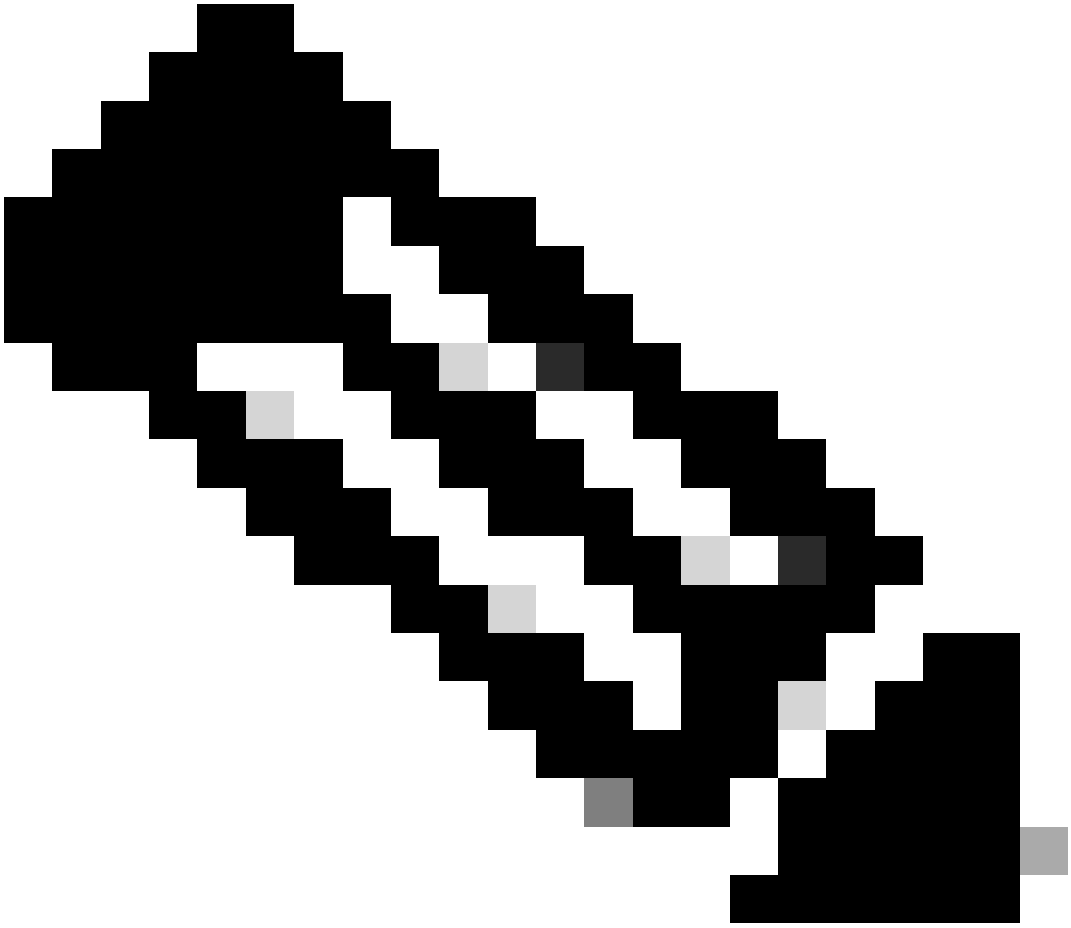
拓扑（Flex模式AP）



网络拓扑：*Flex*模式*AP*

具有中央DHCP的FlexConnect模式AP

使用中央DHCP服务器时，无论AP模式如何，配置、操作流程和故障排除步骤都是一致的。但是，对于FlexConnect模式下的AP，通常建议使用本地DHCP服务器，除非您在本地站点设置了客户端SVI。



注意：如果远程站点没有可用的客户端子网，则可以使用FlexConnect NAT-PAT。FlexConnect NAT/PAT为源自连接到AP的客户端的流量执行网络地址转换(NAT)，将其映射到AP的管理IP地址。例如，如果您的AP在远程分支机构以FlexConnect模式运行，并且连接的客户端需要与位于控制器所在总部的DHCP服务器通信，则可以结合策略配置文件中的中心DHCP设置来激活FlexConnect NAT/PAT。

具有本地DHCP的FlexConnect模式AP

当FlexConnect AP配置为使用本地DHCP时，与AP关联的客户端设备会从同一本地网络中可用的DHCP服务器接收其IP地址配置。此本地DHCP服务器可以是路由器、专用DHCP服务器，或者任何在本地子网内提供DHCP服务的其他网络设备。使用本地DHCP时，DHCP流量在本地网络内交换，这意味着AP会直接将DHCP请求从客户端中继到相邻跳（例如接入交换机）。然后，将根据您的网络配置处理请求。

前提条件:

1. 请查阅FlexConnect指南，确保您的配置与指南中概述的说明和最佳实践保持一致。

2. 客户端VLAN应在flex profile下列出。
3. 需要将AP设置为中继模式，将AP管理VLAN指定为本征VLAN，并且中继上应允许用于客户端流量的VLAN。

以下是AP连接的交换机端口配置示例，其中管理VLAN为58，客户端VLAN为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
!
```

工作设置：有关在AP配置为flex模式时与本地DHCP服务器共享操作日志的参考：

AP客户端调试：

```
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上行链路捕获：

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上行链路捕获

客户端捕获：

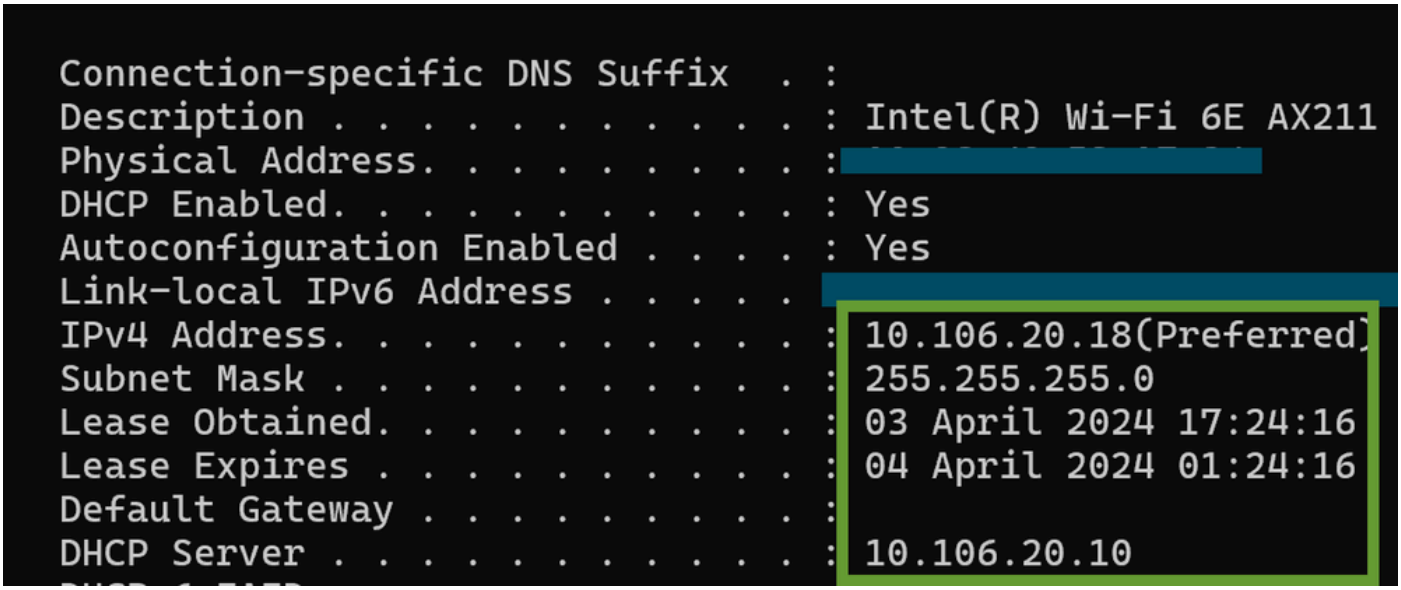
```
16540 111.905836    0.0.0.0          255.255.255.255    DHCP     343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18       DHCP     342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255    DHCP     385 DHCP Request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

客户端数据包捕获

无线客户端IP验证：

您可以检查DHCP服务器上的IP租用及其相应的状态。

在无线客户端上：



客户端上的*IP*验证

DHCP问题的故障排除

排除DHCP故障涉及确定并解决阻止客户端在连接到无线网络时从DHCP服务器获取IP地址的问题。以下是排除DHCP故障时的一些常见步骤和注意事项：

1. 验证客户端配置

- 确保将客户端配置为自动获取IP地址。
- 确认网络适配器已启用且工作正常。

2. 检查DHCP服务器状态

- 确认DHCP服务器运行正常且可从客户端网段访问。
- 检查DHCP服务器的IP地址、子网掩码和默认网关设置。

3. 查看范围配置

- 检查DHCP作用域，确保其有足够的IP地址范围可供客户端使用。
- 验证作用域的租用期限和选项，例如DNS服务器和默认网关
- 在某些环境（如Active Directory）中，请确保DHCP服务器有权在网络中提供DHCP服务。

4. 查看9800 WLC上的配置

- 由于配置错误（例如缺少环回接口、客户端SVI或缺少已配置的帮助地址）已发现许多问题。在收集日志之前，建议验证配置是否已正确实施。
- 使用内部DHCP服务器时：关于DHCP范围的耗尽，必须确保根据您的要求配置租用计时器，特别是在通过CLI配置DHCP时。默认情况下，9800 WLC上的租用计时器设置为无限。
- 验证在使用中央DHCP服务器时，WLC上行链路端口上是否允许客户端VLAN流量。相反，当采用本地DHCP服务器时，请确保在AP上行链路端口上允许相关VLAN。

5. 防火墙和安全设置

- 确保防火墙或安全软件未阻止DHCP流量（DHCP服务器的端口67和DHCP客户端的端口68）。

日志收集

来自WLC的日志

1. 启用术语exec提示符时间戳，使所有命令都有时间参考。

2. 使用show tech-support wireless !! 检查配置

2. 您可以检查客户端数量、客户端状态分布和排除的客户端。
show wireless summary !! AP和客户端总数
show wireless exclusionlist !! 如果任何客户端被视为已排除
show wireless exclusionlist client mac-address MAC@ !! 获取有关排除具体客户端的更多详细信息，并检查原因是否被列为任何客户端的IP盗窃。

3. 检查客户端的IP地址分配，查找不正确的地址或意外的静态地址学习，VLAN标记为脏（因为没有来自DHCP服务器的响应），或正在处理DHCP/ARP的SISF中的数据包丢弃。

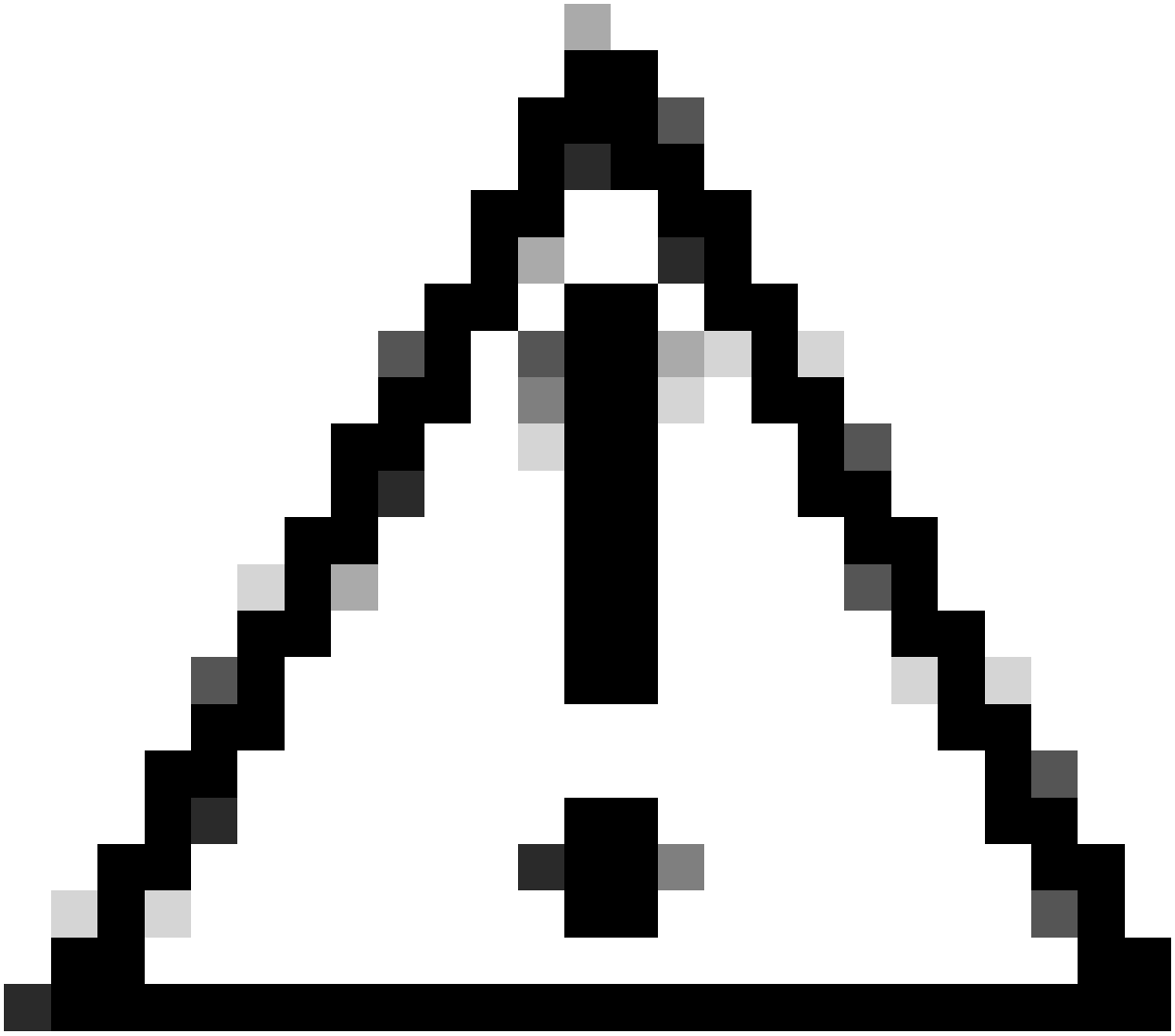
show wireless device-tracking database ip !! 按IP进行检查并查看地址学习的方式：
show wireless device-tracking database mac !! 按Mac进行检查，查看分配的IP客户端。
show wireless vlan details !! 检查在使用VLAN组的情况下，由于DHCP故障，VLAN未标记为脏。
show wireless device-tracking feature drop !!SISF中的丢包

4. 来自WLC的具体客户端MAC@的特定输出 show wireless device-tracking feature drop

当客户端尝试连接无线网络时，启用客户端MAC地址的放射性跟踪。

通过CLI：

debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting time allows us to enable traces for up to 24 days
!!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



注意：条件调试会启用调试级别日志记录，从而增加生成的日志量。保持此运行状态可缩短查看日志的时间间隔。因此，建议始终在故障排除会话结束时禁用调试。

要禁用所有调试，请运行以下命令：

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

通过GUI：

步骤1:导航至 Troubleshooting > Radioactive Trace .

第二步：单击Add并输入要排除故障的客户端Mac地址。您可以添加多个要跟踪的Mac地址。

第三步：准备好开始放射性示踪后，单击“开始”。启动后，调试日志记录会写入磁盘，记录与被跟踪的MAC地址相关的任何控制平面处理。

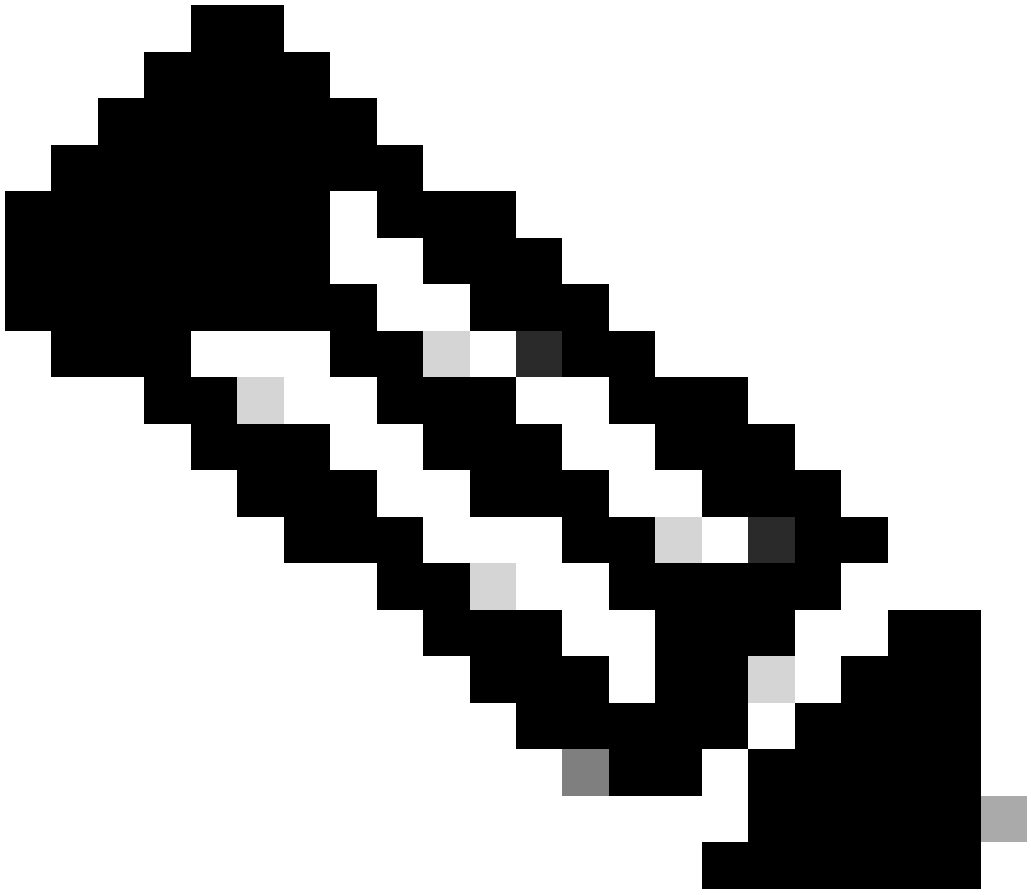
第四步：重现要排除故障的问题时，单击Stop。

第五步：对于所调试的每个mac地址，您可以通过点击 Generate 来生成一个日志文件，整理与该mac地址相关的所有日志。

第六步：选择希望经过整理的日志文件回溯多长时间，然后点击Apply to Device。

步骤 7.现在，您可以通过点击文件名旁边的小图标下载文件。此文件存在于控制器的引导闪存驱动器中，也可以通过CLI从机箱中复制出来。

!!按客户端MAC地址双向过滤的嵌入式捕获，客户端内部MAC过滤器在17.1之后可用。



注意：在9800 WLC上启用中央DHCP后，9800上的EPC将非常有用。

通过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
```

通过GUI：
步骤1:导航到Troubleshooting > Packet Capture > +Add。

第二步：定义数据包捕获的名称。最多允许 8 个字符。

第三步：定义过滤器（如果有）。

第四步：如果想要查看传送至系统CPU并注入数据平面的流量，请选中监控控制流量的复选框。

第五步：定义缓冲区大小。最多允许100 MB。

第六步：定义限制，可根据需要按持续时间或1至1000000秒的数据包数量来定义允许范围1至100000的数据包。

步骤 7.从左侧列中的接口列表中选择接口，并选择箭头将其移动到右侧列。

步骤 8保存并应用到设备。

步骤 9要开始捕获，请选择Start。

步骤 10您可以让捕获运行到定义的限制。要手动停止捕获，请选择停止。

步骤 11停止后，可使用Export按钮单击选项，通过HTTP或TFTP服务器、FTP服务器、本地系统硬盘或闪存将捕获文件(.pcap)下载到本地桌面。

从AP端登录

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

来自DHCP服务器的日志

使用外部DHCP服务器时，需要在服务器端收集调试日志和数据包捕获信息，以检验DHCP流量的流动。

其他日志

如果您发现DHCP发现消息在9800 WLC上的中央DHCP设置中可见，或者在本地DHCP设置中的AP调试日志中可见，则您应该继续从上行链路收集捕获数据，以确认数据包未在以太网端口中丢弃。根据交换机的功能，您可以选择对上行链路交换机执行嵌入式数据包捕获或SPAN（交换端口分析器）捕获。建议逐步跟踪DHCP流量，以确定从DHCP客户端到DHCP服务器以及反向通信的中断点。

已知问题

问题 1.客户端正在尝试从之前保留的VLAN获取IP地址。当无线客户端在与不同客户端VLAN关联的两个SSID之间切换时，可能会出现这种情况。在这种情况下，客户端可能会一直从其之前连接的VLAN请求IP。由于此IP不在当前VLAN的DHCP范围内，因此DHCP服务器将发出NAK（否定确认），因此，客户端将无法获取IP地址。

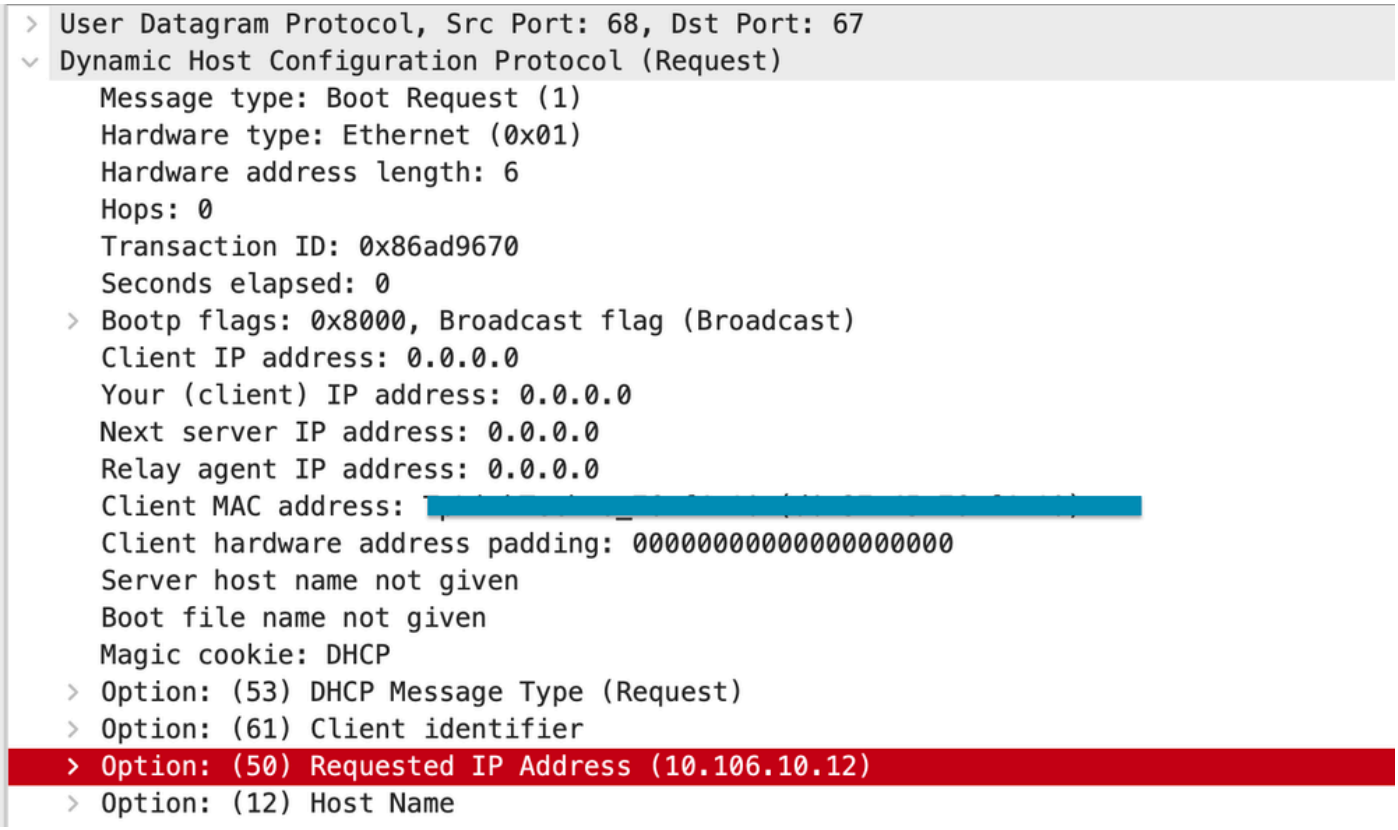
在放射性跟踪日志中，很明显客户端继续从其以前连接的VLAN （即VLAN 10）中寻找IP，尽管当前SSID的客户端VLAN是VLAN 20。

```
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
```

WLC上的嵌入式数据包捕获：

```
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
```

WLC上的嵌入式数据包捕获



WLC数据包捕获上的DHCP选项50

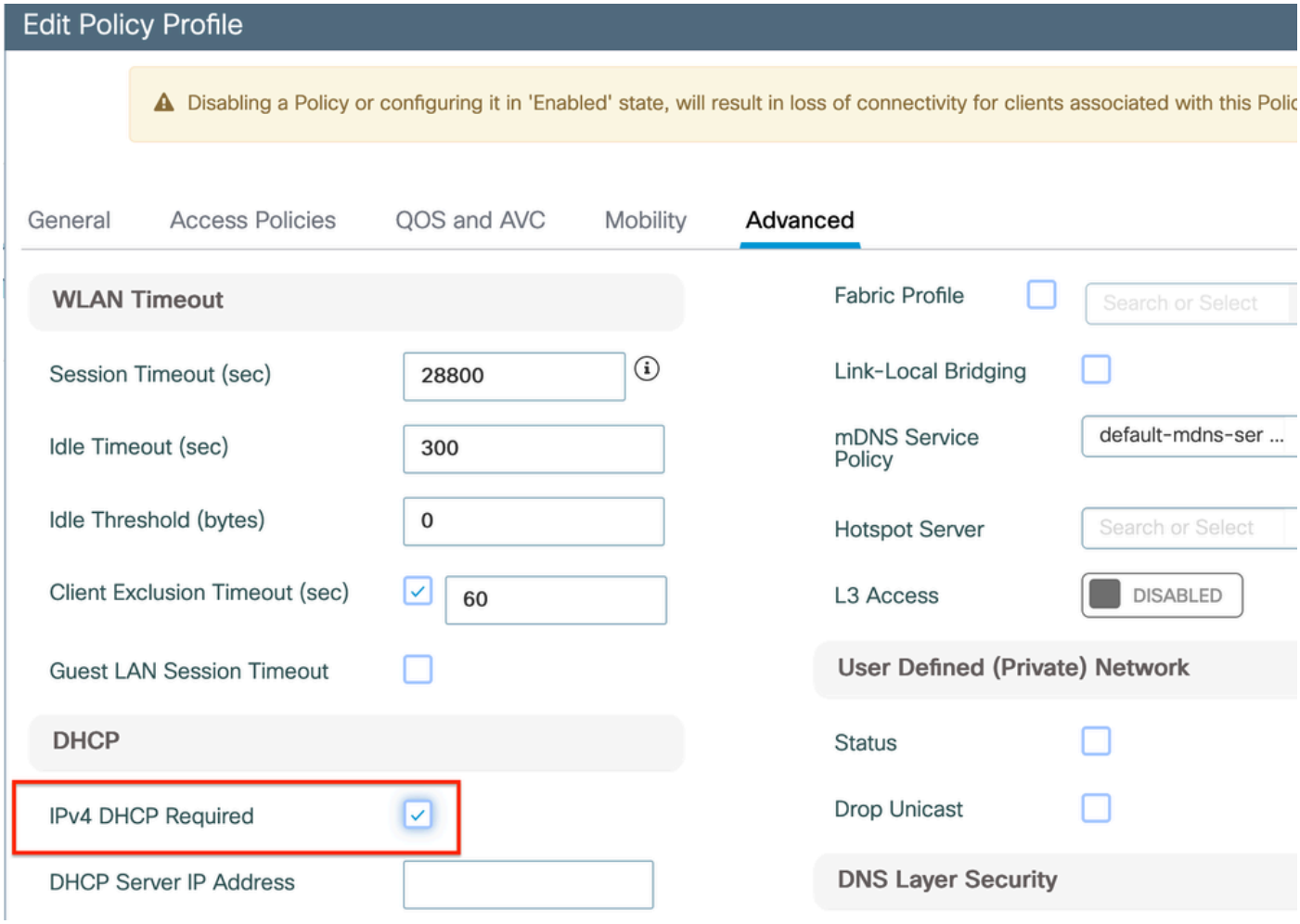
解决方法：要确保客户端完成完整的DHCP过程，可以在策略配置中启用IPv4 DHCP Required选项。应启用此设置，尤其是当客户端在SSID之间切换时，以允许DHCP服务器向客户端发送NAK（如果它请求来自与之前的SSID相关联的VLAN的IP地址）。否则，客户端可能会继续使用或请求其先前拥有的IP地址，从而导致通信中断。但是，请注意，启用此功能会影响配置了静态IP地址的无线客户端。

下面是启用所需选项的流程：

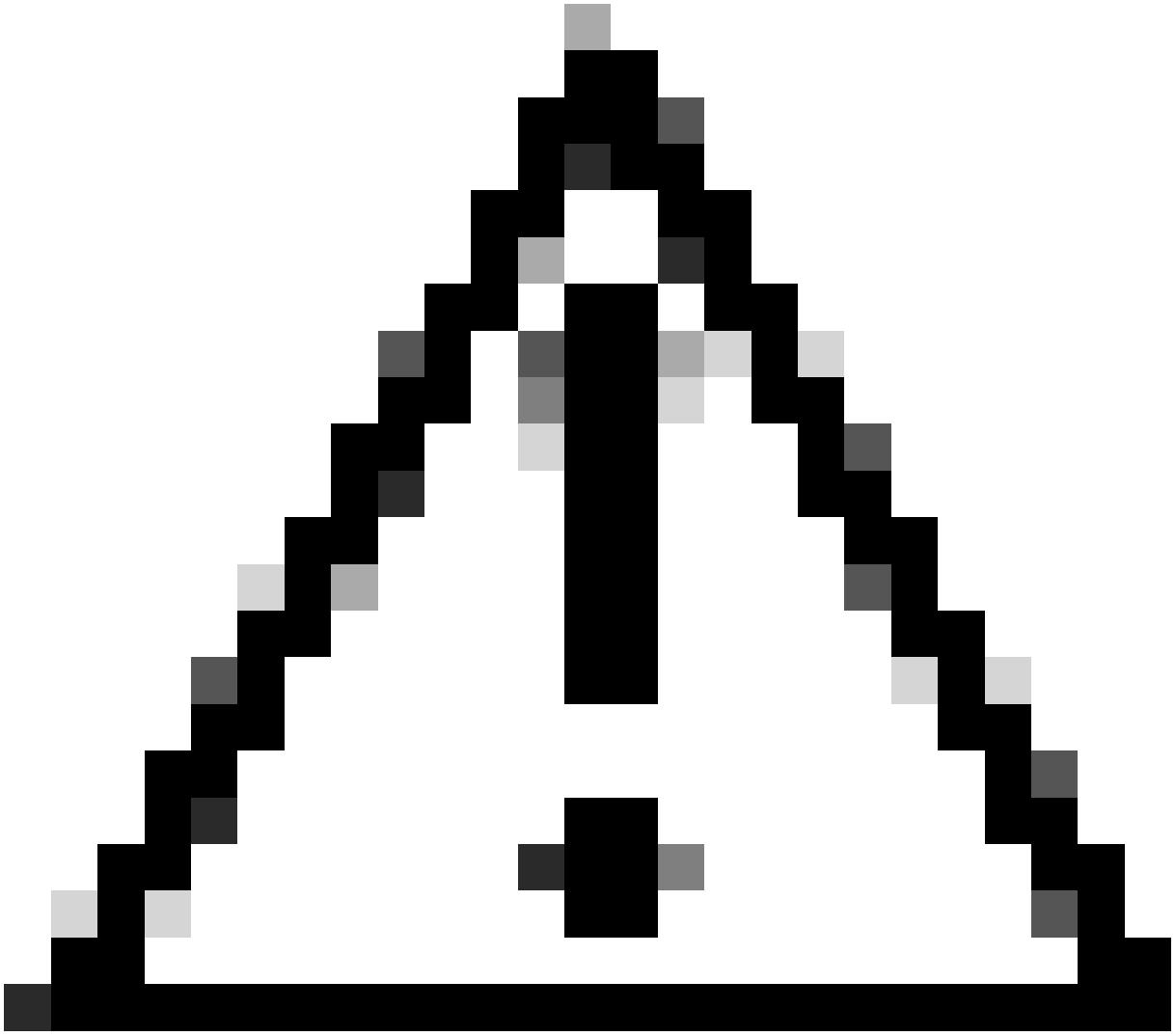
通过CLI：

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

通过GUI：导航至DHCP部分下的Configuration > Tags & Profile > Policy > Policy_name > Advanced. enable ipv4 DHCP required。



WLC上的策略配置文件设置



注意：对于外部锚点设置，务必跨两个WLC调整DHCP设置。如果已启用所需的IPV4 DHCP，则需要在外部和锚点WLC上同时启用它。两者之间的策略配置文件下DHCP相关配置存在差异可能导致客户端遇到其移动角色的问题。

问题2：由于IP窃取问题，客户端被删除或排除。在网络环境中，IP窃取是指多个无线客户端尝试使用同一IP地址的情况。其原因有很多，如下所示：

1. 未经授权的静态IP分配：当用户在其设备上设置的静态IP地址与网络中已分配或指定用途的IP地址相符时，可能会导致IP冲突。当两台设备尝试使用同一IP地址运行时，就会发生这种情况，这可能中断所涉及的任一设备或两个设备的网络连接。要避免此类问题，必须确保网络中的每个客户端都配置有唯一的IP地址。

2. 非法DHCP服务器：网络上存在未授权或非法DHCP服务器可能会导致IP地址分配与已建立的网络IP编址计划冲突。此类冲突可能导致多台设备发生IP地址冲突或获得不正确的网络设置。要解决此问题，应努力从网络中识别并消除非法DHCP服务器，以防止同一子网内出现进一步的IP冲突。

3. 9800 WLC中客户端的过时条目：有时，控制器可能会保留客户端尝试获取的IP地址的过时/过时条目。在这些情况下，需要从9800 WLC中手动删除这些过时的条目。具体操作如下：

- 对排除列表中的mac地址运行放射性跟踪，并使用放射性跟踪中的合法mac过滤该地址。
- 您将能够看到错误日志： %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON：Client MAC：Affected_Client_MAC with IP： 10.37.57.24已添加到排除列表中，合法客户端MAC： Legit_Client_MAC， IP：10.37.57.24，原因： IP地址盗窃
- 然后运行以下命令：
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(如果存在任何过时条目，您将能够看到合法客户端Mac地址的多个IP：一个是原始IP，而另一个是过时/过时的IP]。

解决方法：使用 clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. 在使用相同子网的本地DHCP服务器的Flex部署中：在FlexConnect配置中，不同远程位置通常使用从相同子网分配IP地址的本地DHCP服务器。这种情况可能导致位于不同站点的无线客户端收到相同的IP地址。此网络框架中的控制器经过编程，可检测多个客户端连接何时使用相同的IP地址，将此解释为潜在的IP盗窃。因此，这些客户端通常会被放在阻止列表中，以防止IP地址冲突。

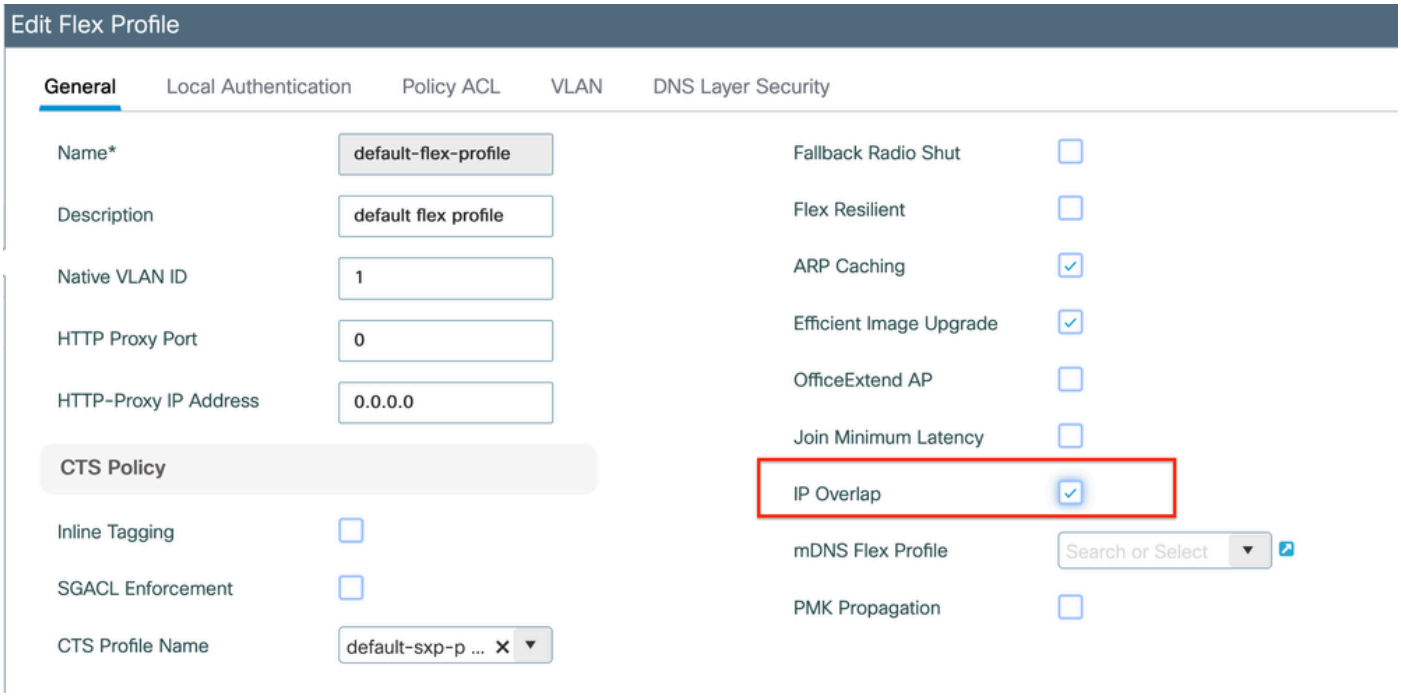
解决方法：在FlexConnect配置文件中启用IP重叠功能。“Flex Deployment中的重叠客户端IP地址”功能允许在多个FlexConnect站点中使用相同的IP地址，同时保持FlexConnect部署中支持的所有特性和功能。

默认情况下，此功能处于禁用状态。您可以通过以下过程启用它：

通过CLI：

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

通过GUI：选择Configuration > Tags & Profiles > Flex. 点击现有Flex配置文件/添加到新Flex配置文件，并在“常规”选项卡下启用IP重叠。



WLC上的Flex配置文件设置

问题 3.无线客户端无法从预期的VLAN接收IP地址。当使用VLAN 1或分配给客户端的VLAN与FlexConnect部署中用于AP管理的VLAN相同时，通常会发生此问题。此问题的根源通常是VLAN分配不正确。为了提供指导，以下是在9800系列上配置VLAN ID时要考虑的几个方案：

1. 当采用已激活AAA覆盖功能的AAA服务器时，确保从AAA服务器发送适当的VLAN ID至关重要。如果提供了VLAN名称，请确认其与9800 WLC上配置的VLAN名称匹配。

2. 当为无线客户端流量配置VLAN 1时，行为可能因接入点(AP)的模式而异：

对于处于本地模式/集中交换模式的AP：

- 指定VLAN-name =默认值，将客户端分配给VLAN 1
- 使用VLAN-ID 1可将客户端分配给无线管理VLAN

对于Flex模式/本地交换中的AP：

- 指定VLAN-name =默认值，将客户端分配给VLAN 1
- 使用VLAN-ID 1可将客户端分配给FlexConnect本地VLAN

下面是一些在实验室中试验过的场景示例，以及它们的结果：

1. 默认情况下，如果用户未在策略配置文件下配置任何内容，则WLC会分配VLAN-ID 1，以便客户端在本地模式下使用无线管理VLAN，并在FlexConnect中使用AP本地VLAN。

2. 如果flex-profile下的本地VLAN配置的本地VLAN ID与交换机上配置的本地VLAN ID不同，您会看到问题，即使策略配置文件配置了“默认”VLAN名称，客户端也会从管理VLAN（本地VLAN）获取IP。

3. 如果flex-profile下的Native-VLAN配置的VLAN-ID与交换机上配置的本地VLAN相同，则只有客户端才能从策略配置文件下配置了默认值的VLAN 1获取IP。

4. 如果选择VLAN名称而不是VLAN ID，请确保Flex Profile中的VLAN名称相同。

相关信息

- 9800上的内部DHCP服务器
- 外部DHCP服务器正在使用中
- Windows DHCP服务器中的DHCP选项82子选项5
- Flex AP中的NAT-PAT
- VLAN 1用于无线客户端
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。