Resolución de Problemas de Conectividad del Cliente DHCP en un Cisco 9800 WLC

Contenido

- Introducción
- Prerequisites
- Comprensión del Flujo del Tráfico DHCP con Clientes Inalámbricos
- Escenario 1. El punto de acceso (AP) funciona en modo local
  - Topología (AP de modo local)
  - Caso Práctico 1. Cuando el WLC se configura como un servidor DHCP interno
  - Caso Práctico 2. Cuando se utiliza un servidor DHCP externo
    - Tráfico DHCPTransmisión a través del dominio de capa 2
    - 9800 WLC está sirviendo como agente de retransmisión
    - Opción 80 de DHCP con subopción 5/150 en el WLC 9800
- Situación hipotética 2. El punto de acceso (AP) funciona en modo flexible
  - Topología (punto de acceso de modo flexible)
  - AP de modo FlexConnect con DHCP central
  - AP de modo FlexConnect con DHCP local
- Resolución de problemas de DHCP
  - Recopilación de registros
    - Registros de WLC
    - Registros desde el lado del AP
    - Registros del servidor DHCP
    - Otros registros
  - Problemas conocidos
- Información Relacionada

Introducción

Este documento describirá varios problemas relacionados con el protocolo de configuración dinámica de host (DHCP) que encuentran los clientes inalámbricos cuando se conectan a un controlador de LAN inalámbrica (WLC) Cisco 9800 y cómo solucionarlos.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de Cisco WLC 9800
- Conocimiento básico de DHCP Flow

- Conocimiento básico de AP de modo de conexión flexible y local

Comprensión del Flujo del Tráfico DHCP con Clientes Inalámbricos

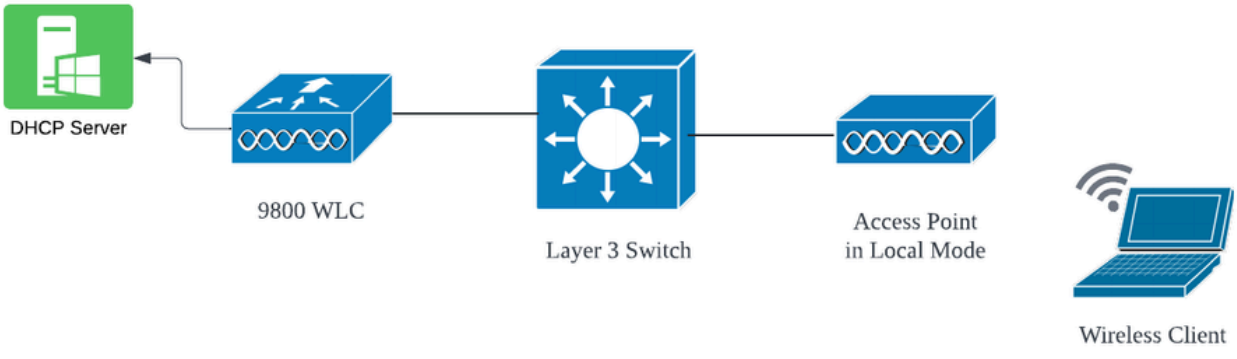
Cuando el cliente inalámbrico se conecta, realiza el intercambio DHCP habitual enviando una trama de detección DHCP de difusión para encontrar un servidor DHCP al AP asociado. Dependiendo del modo de funcionamiento del AP, reenviará la solicitud al WLC a través del túnel CAPWAP o la pasará directamente al salto siguiente. Si un servidor DHCP está disponible dentro del dominio local de Capa 2, responderá, facilitando una conexión exitosa. En ausencia de un servidor DHCP de subred local, el router (configurado con la SVI del cliente) debe configurarse para rutear la detección DHCP al servidor apropiado. Esto se realiza normalmente mediante la configuración de una dirección auxiliar IP en el router, que le indica que reenvíe el tráfico UDP de difusión específico (como las solicitudes DHCP) a una dirección IP predeterminada.

El comportamiento del tráfico DHCP del cliente depende totalmente del modo en el que funciona el punto de acceso (AP). Examinemos cada uno de estos escenarios por separado:

Escenario 1. El punto de acceso (AP) funciona en modo local

Cuando se configura un AP en el modo local, el tráfico DHCP del cliente se conmuta centralmente, lo que significa que las solicitudes DHCP de los clientes se envían a través de un túnel CAPWAP del AP al WLC, donde se procesan y se reenvían según corresponda. En este caso, tiene dos opciones: puede utilizar un servidor DHCP interno u optar por un servidor DHCP externo.

Topología (AP de modo local)



Topología de red: AP de modo local

Caso Práctico 1. Cuando el WLC se configura como un servidor DHCP interno

El controlador puede ofrecer un servidor DHCP interno a través de las funciones integradas del software Cisco IOS XE. Sin embargo, se considera una práctica recomendada utilizar un servidor DHCP externo. Antes de configurar el WLC como un servidor DHCP interno, se deben abordar varios prerrequisitos que son los siguientes:

- Asegúrese de configurar una interfaz virtual conmutada (SVI) para la VLAN del cliente y asígnele la dirección IP del servidor DHCP.
- La dirección IP del servidor DHCP interno debe configurarse en la interfaz orientada al servidor, que puede ser una interfaz de loopback, una SVI o una interfaz física de capa 3.
- Se recomienda configurar la interfaz de loopback porque, a diferencia de las interfaces físicas que se conectan a segmentos de red reales, la interfaz de loopback no está vinculada al hardware y no corresponde a un puerto físico del dispositivo. El propósito principal de una interfaz de loopback es proporcionar una interfaz estable y siempre activa que no esté sujeta a fallas de hardware o desconexiones físicas.

Configuración en funcionamiento: A continuación se muestra un ejemplo de una configuración de servidor DHCP interno en la que los clientes recibieron direcciones IP correctamente. Estos son los registros operativos y los detalles de configuración asociados.

Configure el WLC como el servidor DHCP para la VLAN 10, con un alcance DHCP que varía de 10.106.10.11/24 a 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
```

Interfaz de loopback configurada en WLC:

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

VLAN de cliente configurada como SVI [interfaz L3] con dirección de ayudante como interfaz de loopback en 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
```

Como alternativa, puede establecer la dirección IP del servidor DHCP dentro del perfil de política, en lugar de configurar una dirección de ayudante en la SVI. Sin embargo, generalmente se recomienda configurar esto en una base por VLAN para las prácticas recomendadas:

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

Rastreos radiactivos en 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
```

Capturas de paquetes incorporadas en 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
```

Captura de paquetes integrada en WLC

Depuraciones del cliente AP:

```
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>
```

Captura de paquetes del lado cliente:

```
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
```

Captura de paquetes de extremo de cliente

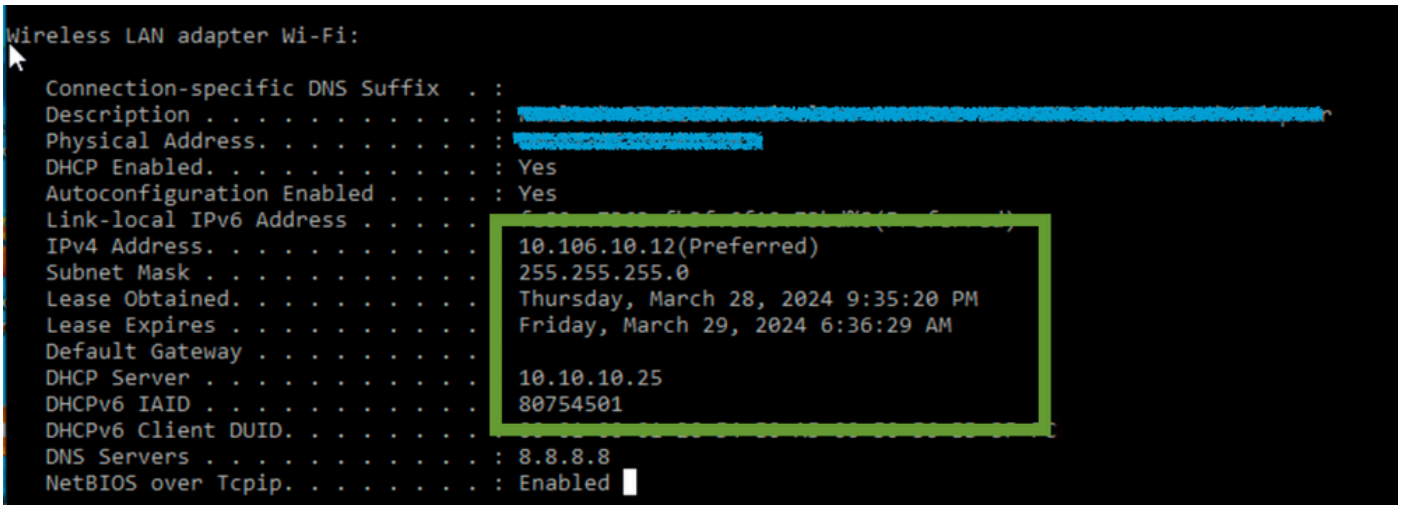
En los registros operativos proporcionados, puede ver que el WLC está recibiendo el mensaje de detección DHCP del cliente inalámbrico y que la VLAN del cliente lo está retransmitiendo a la dirección del ayudante (que en el ejemplo proporcionado es la interfaz de loopback interna). A continuación, el servidor interno emite una oferta DHCP y, posteriormente, el cliente envía una solicitud DHCP, que el servidor reconoce con un ACK DHCP.

Verificación de la IP del cliente inalámbrico:

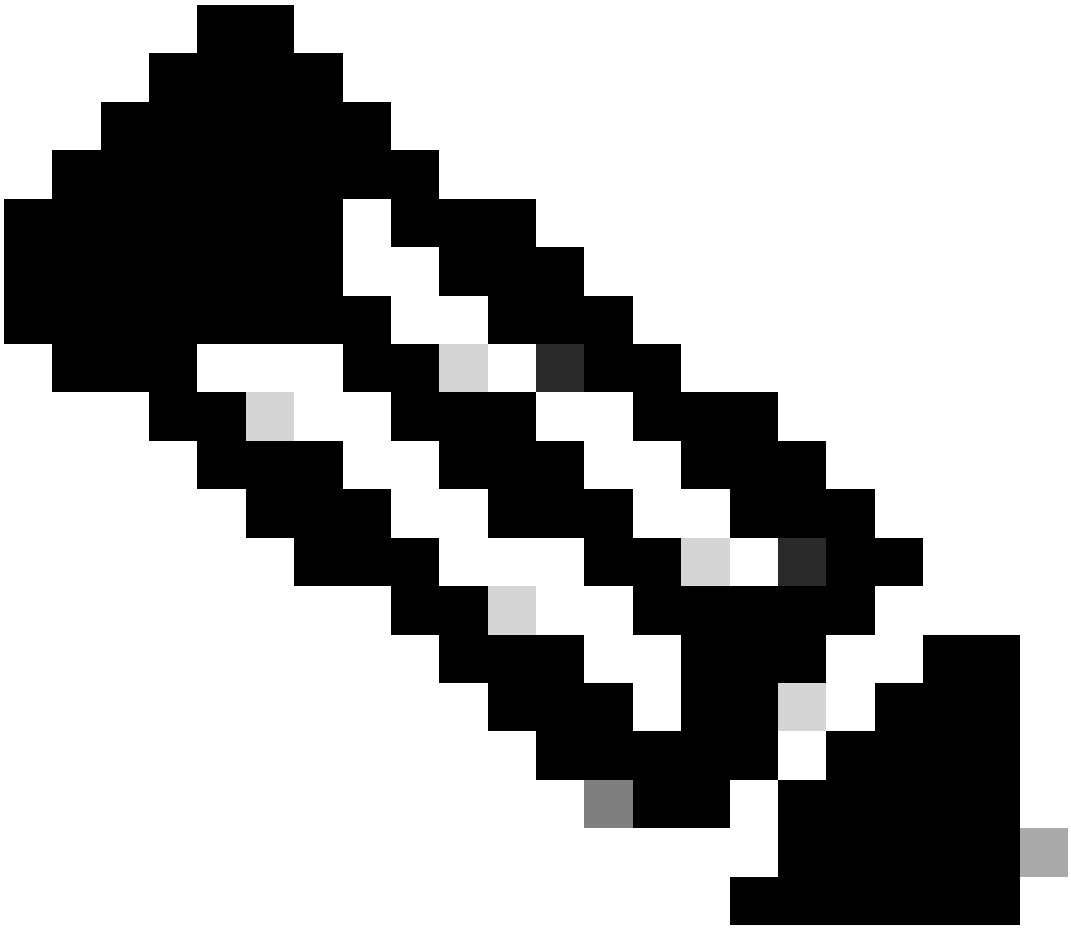
En WLC:

```
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     L
```

En cliente inalámbrico:



Verificación de IP en el extremo del cliente



Nota:

1. Los servidores DHCP internos no admiten VRF.
2. DHCPv6 no es compatible con los servidores DHCP internos.

---

3. En C9800, SVI permite configurar varias direcciones de ayudante, pero solo se utilizan las primeras 2.
4. Se ha probado y, por lo tanto, es compatible con todas las plataformas para un máximo del 20% de la escala máxima del cliente de la caja. Por ejemplo, para un 9800-80 que admite 64 000 clientes, el número máximo de enlaces DHCP admitidos es de aproximadamente 14 000.

Caso Práctico 2. Cuando se utiliza un servidor DHCP externo

Un servidor DHCP externo se refiere a un servidor DHCP que no está integrado en el WLC sí mismo pero configurado en un dispositivo de red diferente [Firewall, Routers] o una entidad separada dentro de la infraestructura de red. Este servidor está dedicado a administrar la distribución dinámica de direcciones IP y otros parámetros de configuración de red a los clientes de la red.

Cuando se utiliza un servidor DHCP externo, la función del WLC es solamente recibir y retransmitir tráfico. El modo en que el tráfico DHCP se rutea desde el WLC, si es broadcast o unicast, variará dependiendo de su preferencia. Consideremos cada uno de estos métodos por separado.

Difusión de tráfico DHCP a través del dominio de capa 2

En esta configuración, otro dispositivo de red, como un firewall, un enlace ascendente o un switch principal, actúa como agente de retransmisión. Cuando un cliente transmite una solicitud de detección DHCP, el único trabajo del WLC es reenviar esta difusión a través de la interfaz de la capa 2. Para que esto funcione correctamente, debe asegurarse de que la interfaz de Capa 2 de la VLAN del cliente esté configurada correctamente y esté permitida a través del puerto de datos del WLC y el dispositivo de link ascendente.

Configuración deseada en el extremo del WLC para la VLAN 20 del cliente para esta instancia:

VLAN de capa 2 configurada en WLC:

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

Puerto de datos configurado en el WLC para permitir el tráfico de la VLAN del cliente:

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

```
switchport mode trunk
negotiation auto
end
```

Rastreos radiactivos en 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
```

Captura de paquetes integrada tomada en el WLC 9800:

```
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
```

Captura de paquetes integrada en WLC

Depuraciones del cliente AP:

```
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>
```

Captura del lado del cliente:

```
     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
```

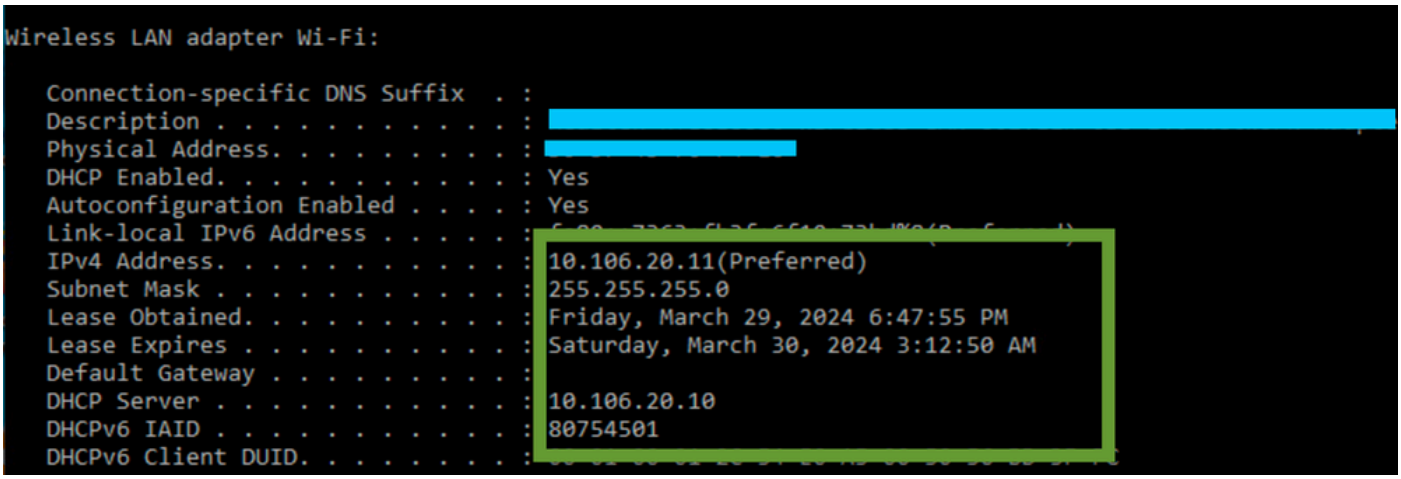
Captura de paquetes de extremo de cliente

En los registros operativos proporcionados, usted nota en los registros que el WLC está interceptando el DHCP Discover broadcast del cliente inalámbrico y luego lo transmite hacia el salto siguiente a través de su interfaz L2. Tan pronto como el WLC recibe la oferta DHCP del servidor, reenvía este mensaje al cliente seguido por la petición DHCP y el ACK.

Verificación de la IP del cliente inalámbrico:

Puede comprobar la concesión IP del servidor DHCP y su estado correspondiente.

En cliente inalámbrico:



Verificación de IP en el extremo del cliente

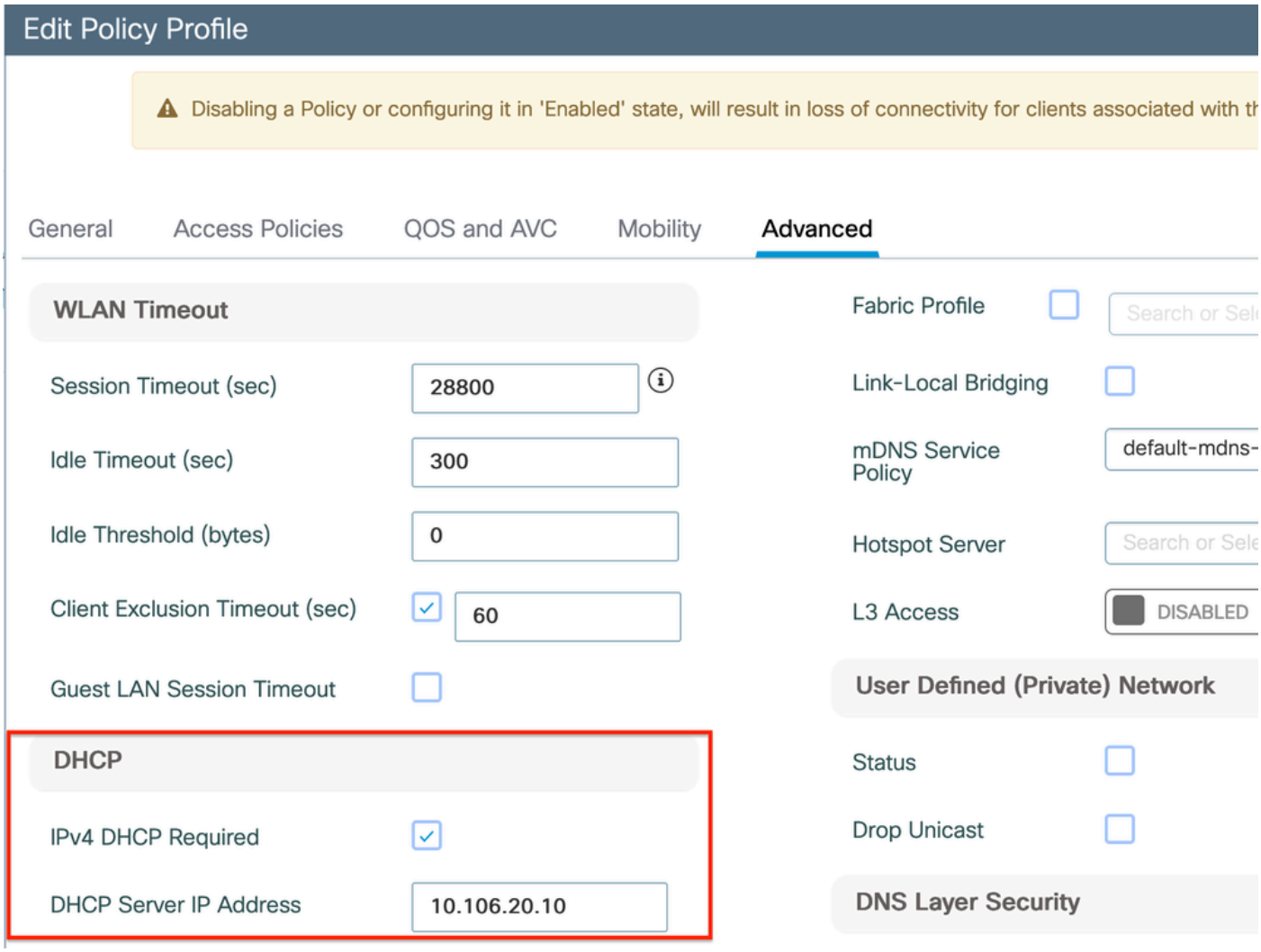
9800 WLC está sirviendo como agente de retransmisión

En esta configuración, el WLC reenvía directamente los paquetes DHCP que recibe de los clientes inalámbricos al servidor DHCP por unicast. Para habilitar esto, asegúrese de que la VLAN SVI para el cliente esté configurada en el WLC.

Hay 2 maneras de configurar la IP del servidor DHCP en el WLC 9800:

1. Configure la IP del servidor DHCP en el perfil de política en la configuración avanzada.

Via GUI: Navigate to Configuration > Tags & Profile > Policy > Policy_name > Advanced. En la sección DHCP puede configurar la IP del servidor DHCP como se muestra:



Configuración del Perfil de Política en WLC

A través de CLI:

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

2. En la configuración de SVI, debe especificar la dirección del ayudante. La configuración de varios servidores DHCP en la configuración de la dirección del ayudante es posible para proporcionar redundancia. Aunque es posible establecer la dirección del servidor DHCP para cada WLAN dentro del perfil de política, el enfoque recomendado es configurarlo por interfaz. Esto se puede lograr asignando una dirección de ayudante a la SVI correspondiente.

Al emplear la función de retransmisión, el origen del tráfico DHCP será la dirección IP de la interfaz virtual conmutada (SVI) del cliente. A continuación, este tráfico se enruta a través de la interfaz correspondiente al destino (la dirección IP del servidor DHCP) según lo determinado por la tabla de enrutamiento.

A continuación se muestra una muestra de la configuración en funcionamiento de 9800 que funciona como agente relay:

Interfaz de capa 3 configurada para VLAN de cliente en WLC con dirección auxiliar:

```
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
```

Puerto de datos configurado en el WLC para permitir el tráfico de la VLAN del cliente:

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

Rastreos de RA desde 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 Client
```

Captura de paquetes integrada en WLC:

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

Captura de paquetes integrada en WLC

Tanto en los seguimientos radiactivos (RA) como en la captura de paquetes integrada (EPC) en el WLC, observará que el WLC, que actúa como agente de retransmisión, está unidifusión directa de los paquetes DHCP del cliente al servidor DHCP.

Depuraciones del cliente AP:

```
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>
```

Captura del lado del cliente:

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

Captura de paquetes de extremo de cliente

Verificación de la IP del cliente inalámbrico:

Puede comprobar la concesión IP del servidor DHCP y su estado correspondiente.

En cliente inalámbrico:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . :
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .
   IPv4 Address. . . . . . . . . . . 10.106.20.12(Preferred)
   Subnet Mask . . . . . . . . . . . 255.255.255.0
   Lease Obtained. . . . . . . . . . Friday, March 29, 2024 9:53:53 PM
   Lease Expires . . . . . . . . . . Saturday, March 30, 2024 5:53:53 AM
   Default Gateway . . . . . . . . .
   DHCP Server . . . . . . . . . . . 10.106.20.10
   DHCPv6 IAID . . . . . . . . . . . 80754501
   DHCPv6 Client DUID. . . . . . . .
   DNS Servers . . . . . . . . . . . : 8.8.8.8
```

Verificación de IP en el extremo del cliente

Opción 80 de DHCP con subopción 5/150 en el WLC 9800

En ciertos escenarios, puede que prefiera definir explícitamente la interfaz de origen para el tráfico DHCP en lugar de depender de la tabla de ruteo, para evitar posibles complicaciones en la red. Esto es especialmente importante cuando el siguiente dispositivo de red a lo largo de la ruta, como un switch de capa 3 o un firewall, emplea comprobaciones de Reenvío de ruta inversa (RPF). Tomemos, por ejemplo, una situación en la que la interfaz de administración inalámbrica se configura en la VLAN 50, mientras que la SVI del cliente está en la VLAN 20 y se utiliza como un relé DHCP para el tráfico del cliente. La ruta predeterminada se dirige hacia el gateway de la VLAN/subred de administración inalámbrica.

A partir de la versión 17.03.03 en el WLC 9800, es posible elegir la interfaz de origen para el tráfico DHCP para que sea la VLAN del cliente u otra VLAN, como la interfaz de administración inalámbrica (WMI), que garantiza la conectividad con el servidor DHCP.

A continuación se incluye un recorte de la configuración:

```
!
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
```

En esta situación, el tráfico al servidor DHCP 10.100.17.14 se originará en la VLAN 50 (10.100.16.10), porque la interfaz de salida del paquete se selecciona en función de una búsqueda en la tabla de routing IP y, normalmente, se cerraría a través de la VLAN de la interfaz de administración inalámbrica (WMI) debido a la ruta predeterminada configurada.
Sin embargo, si un switch de link ascendente implementa las comprobaciones de Reverse Path Forwarding (RPF), puede descartar un paquete que llega de VLAN 50 pero con una dirección de origen IP que pertenece a una subred diferente [VLAN 20].

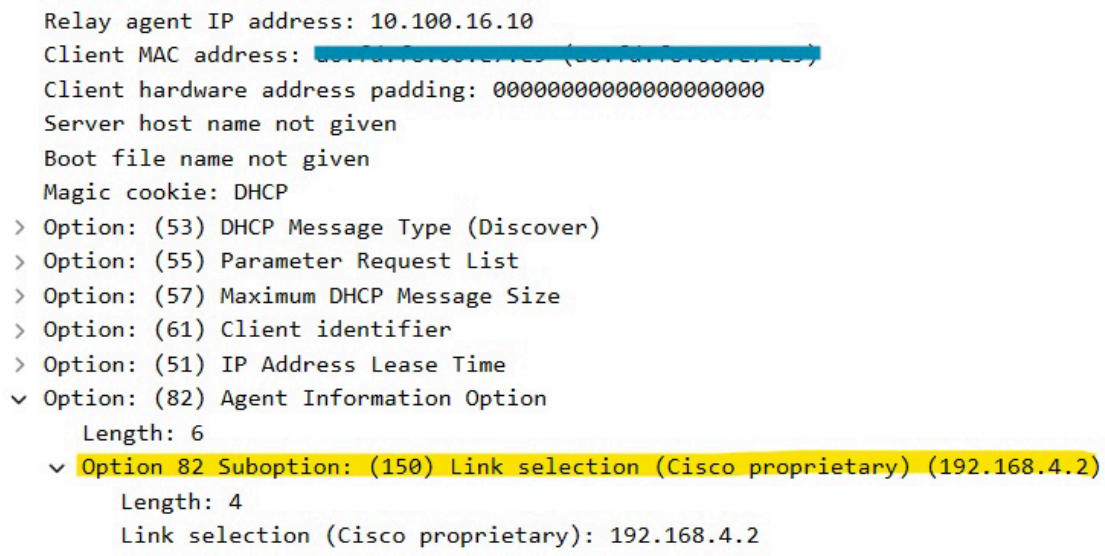
Para evitar esto, debe establecer una interfaz de origen precisa para los paquetes DHCP con el comando IP DHCP relay source-interface. En este caso en particular, querrá que los paquetes DHCP se originen desde la interfaz WMI en la VLAN 50:

```
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
```

Cuando se utiliza ip dhcp relay source-interface el comando, tanto la interfaz de origen de los paquetes DHCP como la GIADDR se configuran en la interfaz especificada en el comando de retransmisión DHCP (VLAN50, en este caso). Este es un problema, ya que no es la VLAN del cliente donde desea asignar direcciones DHCP.

¿Cómo sabe el servidor DHCP cómo asignar la IP del conjunto de clientes correcto?

La respuesta a esto es que cuando se utiliza ip dhcp relay source-interface el comando, C9800 agrega automáticamente la información de subred del cliente en una subopción propietaria 150 de la opción 82 llamada selección de link, como se puede ver en la captura:



Opción 182 subopción 150 en captura de paquetes WLC

De forma predeterminada, agregará la subopción 150 (propiedad de Cisco). Asegúrese de que el servidor DHCP utilizado puede interpretar y actuar sobre esta información. Se recomienda cambiar la configuración de C9800 para utilizar la subopción 5 de la opción 82 estándar para enviar la información de selección de enlaces. Para ello, configure el siguiente comando global:

<#root>

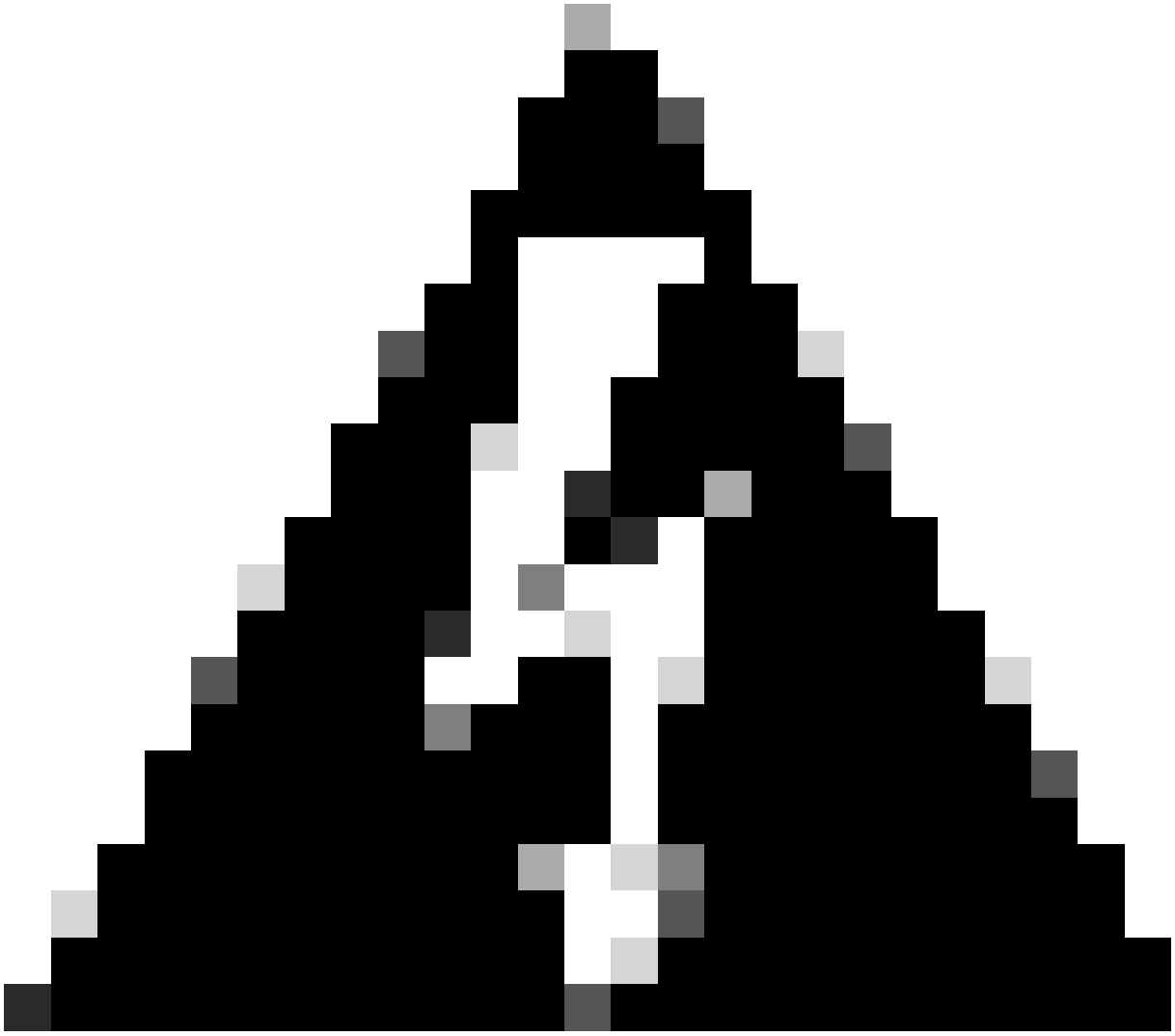
```
C9800(config)#ip dhcp compatibility suboption link-selection standard
```

Una vez que se aplica el comando especificado, el sistema reemplazará la subopción 150 con la subopción 5 en los paquetes DHCP. Los dispositivos de red reconocen más ampliamente la subopción 5, lo que garantiza que los paquetes sean menos propensos a descartarse. La aplicación de este cambio también es evidente en la captura proporcionada:

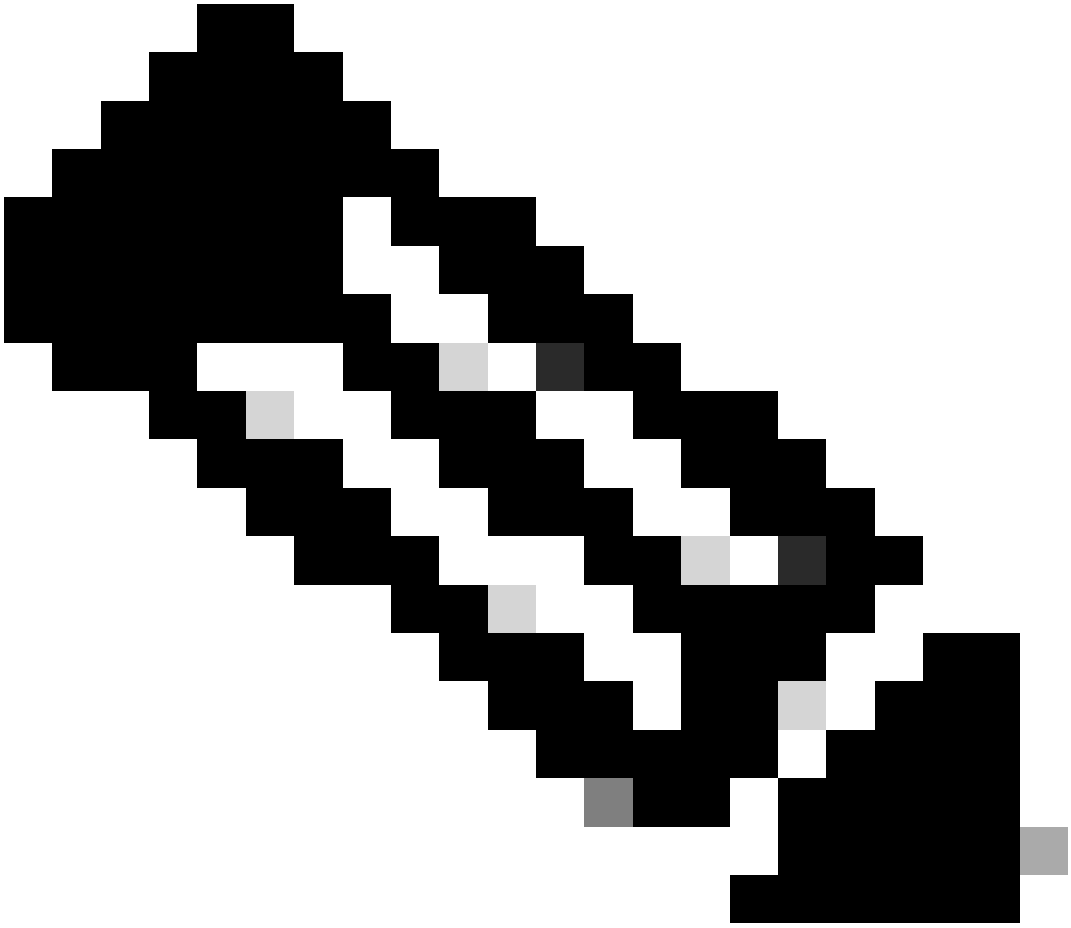
Opción 182 subopción 5 en captura de paquetes WLC

Con la implementación de la subopción 5, el tráfico DHCP debe ser reconocido por otros dispositivos de red. Sin embargo, puede que aún encuentre mensajes NAK (reconocimiento negativo), especialmente cuando el servidor DHCP de Windows está en uso. Esto podría deberse a que el servidor DHCP no autoriza la dirección IP de origen, posiblemente porque no tiene una configuración correspondiente para esa IP de origen.

¿Qué tiene que hacer en el servidor DHCP? Para el servidor DHCP de Windows, debe crear un ámbito ficticio para autorizar la IP del agente de retransmisión.



Advertencia: todas las direcciones IP (GIADDR) del agente de retransmisión deben formar parte de un intervalo de direcciones IP del ámbito DHCP activo. Cualquier GIADDR que se encuentre fuera de los intervalos de direcciones IP del ámbito DHCP se considera una retransmisión no autorizada y el servidor DHCP de Windows no aceptará las solicitudes de clientes DHCP de esos agentes de retransmisión. Se puede crear un ámbito especial para autorizar agentes de retransmisión. Cree un ámbito con la GIADDR (o varias direcciones si las GIADDR son direcciones IP secuenciales), excluya las direcciones GIADDR de la distribución y, a continuación, active el ámbito. Esto autorizará a los agentes de retransmisión mientras evita que se asignen las direcciones GIADDR.

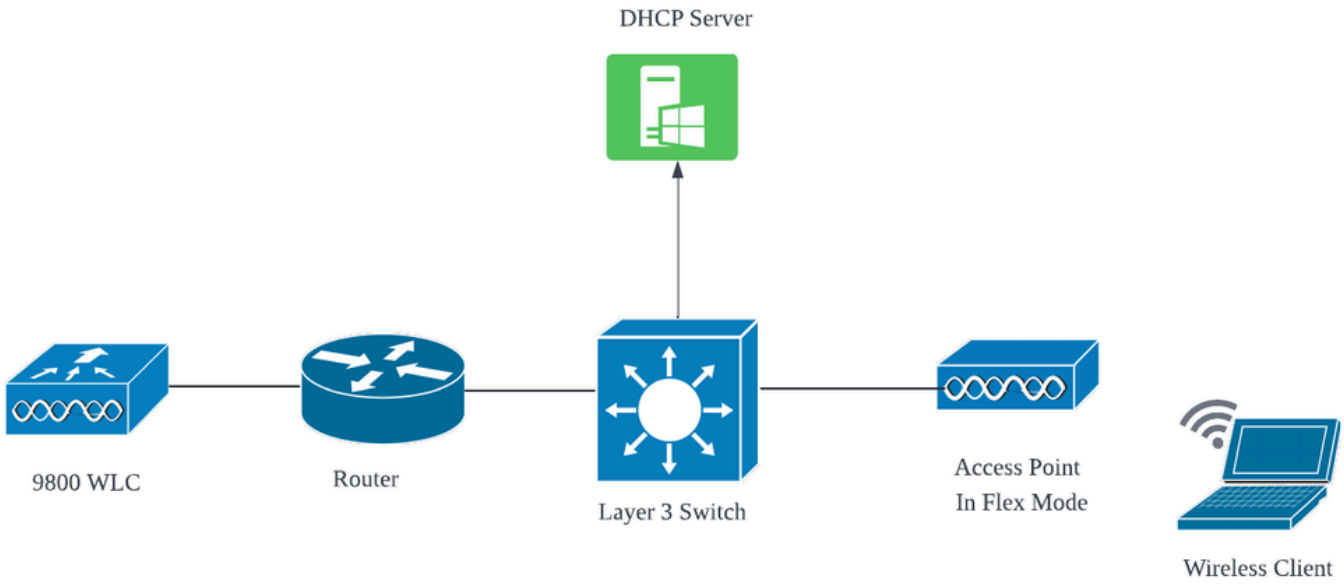


Nota: En una configuración de anclaje externo, el tráfico DHCP se procesa centralmente con el modo AP configurado como Local. Inicialmente, las solicitudes DHCP se envían al WLC externo, que luego las reenvía al WLC de anclaje a través de un túnel de movilidad. Es el WLC de anclaje que maneja el tráfico según sus configuraciones configuradas. Por lo tanto, cualquier configuración relacionada con DHCP debe ser implementada en el WLC de anclaje.

Situación hipotética 2. El punto de acceso (AP) funciona en modo flexible

Los puntos de acceso FlexConnect están diseñados para sucursales y oficinas remotas, lo que les permite funcionar en modo independiente cuando pierden la conectividad con el controlador de LAN inalámbrica (WLC) central. Los AP de FlexConnect pueden conmutar localmente el tráfico entre un cliente y la red sin tener que redirigir el tráfico al WLC. Esto reduce la latencia y ahorra ancho de banda WAN. En el modo flexible AP, el tráfico DHCP se puede conmutar centralmente o localmente conmutado.

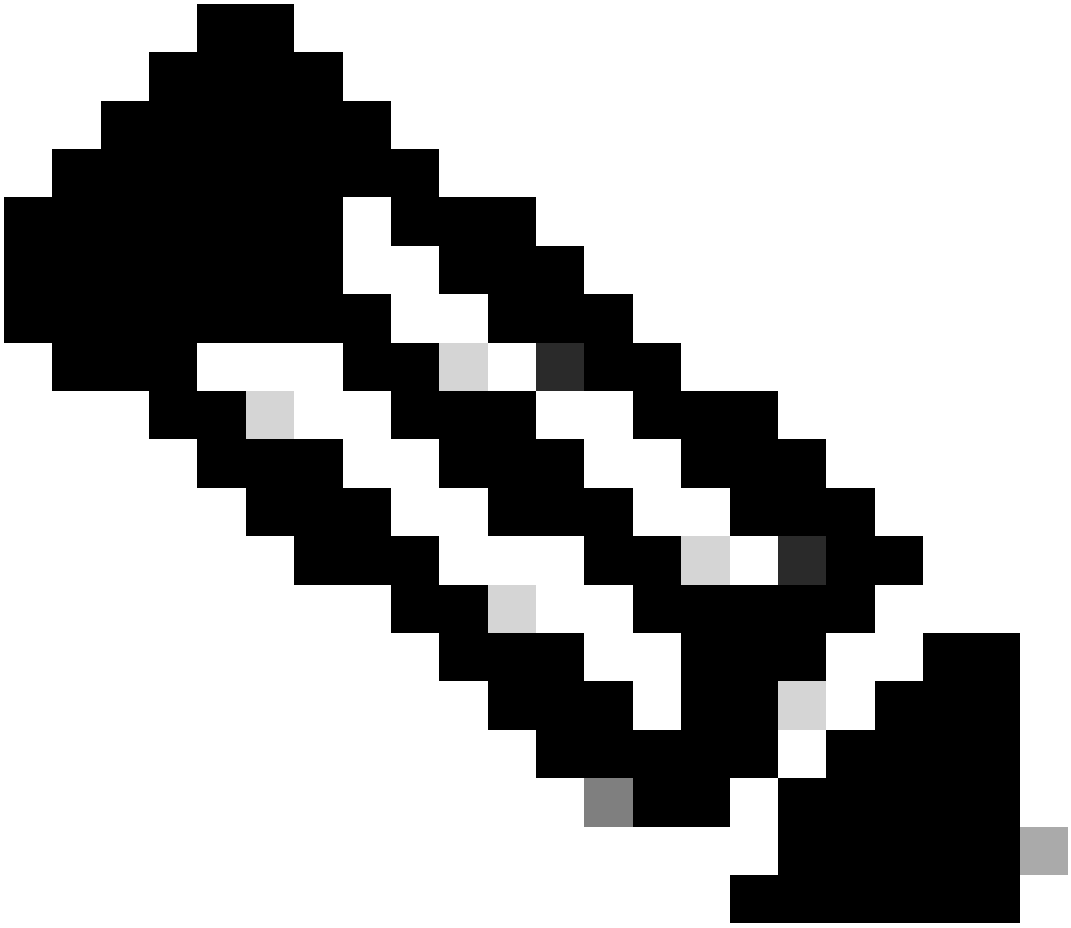
Topología (punto de acceso de modo flexible)



Topología de red: punto de acceso de modo flexible

AP de modo FlexConnect con DHCP central

Independientemente del modo AP, los pasos de configuración, flujo operativo y resolución de problemas permanecen consistentes cuando se utiliza un servidor DHCP central. Sin embargo, para los AP en el modo FlexConnect, generalmente se recomienda utilizar un servidor DHCP local a menos que tenga una SVI del cliente configurada en el sitio local.



Nota: si no tiene una subred de cliente disponible en el sitio remoto, puede aprovechar las ventajas de NAT-PAT de FlexConnect. FlexConnect NAT/PAT realiza la traducción de direcciones de red (NAT) para el tráfico que se origina en los clientes conectados al AP, asignándolo a la dirección IP de administración del AP. Por ejemplo, si tiene puntos de acceso que funcionan en el modo FlexConnect en sucursales remotas y los clientes conectados necesitan comunicarse con un servidor DHCP ubicado en la sede central donde residen los controladores, puede activar FlexConnect NAT/PAT junto con la configuración de DHCP central en el perfil de directiva.

AP de modo FlexConnect con DHCP local

Cuando un AP FlexConnect se configura para utilizar DHCP local, los dispositivos cliente que se asocian con el AP reciben su configuración de dirección IP de un servidor DHCP que está disponible dentro de la misma red local. Este servidor DHCP local puede ser un router, un servidor DHCP dedicado o cualquier otro dispositivo de red que proporcione servicios DHCP dentro de la subred local. Con DHCP local, el tráfico DHCP se conmuta dentro de la red local, lo que significa que el AP retransmite las solicitudes DHCP de los clientes directamente al salto adyacente, como el switch de acceso. A partir de ahí, las solicitudes se gestionan según la configuración de la red.

Requisito previo:

1. Consulte la guía de FlexConnect para asegurarse de que su configuración se ajusta a las instrucciones y las prácticas recomendadas descritas en la guía.

2. La VLAN del cliente debe aparecer bajo el perfil flex.
3. El AP debe configurarse en modo troncal, con la VLAN de administración del AP designada como VLAN nativa, y las VLAN para el tráfico del cliente deben estar permitidas en el troncal.

Este es un ejemplo de configuración de puerto de switch conectado a AP con VLAN de administración como 58 y VLAN de cliente como 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
!
```

Configuración en funcionamiento: para compartir de referencia los registros operativos con el servidor DHCP local cuando el AP está configurado para el modo flexible:

Depuraciones del cliente AP:

```
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>
```

Captura de enlace ascendente de PA:

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

Captura de enlace ascendente de PA

Captura del lado del cliente:

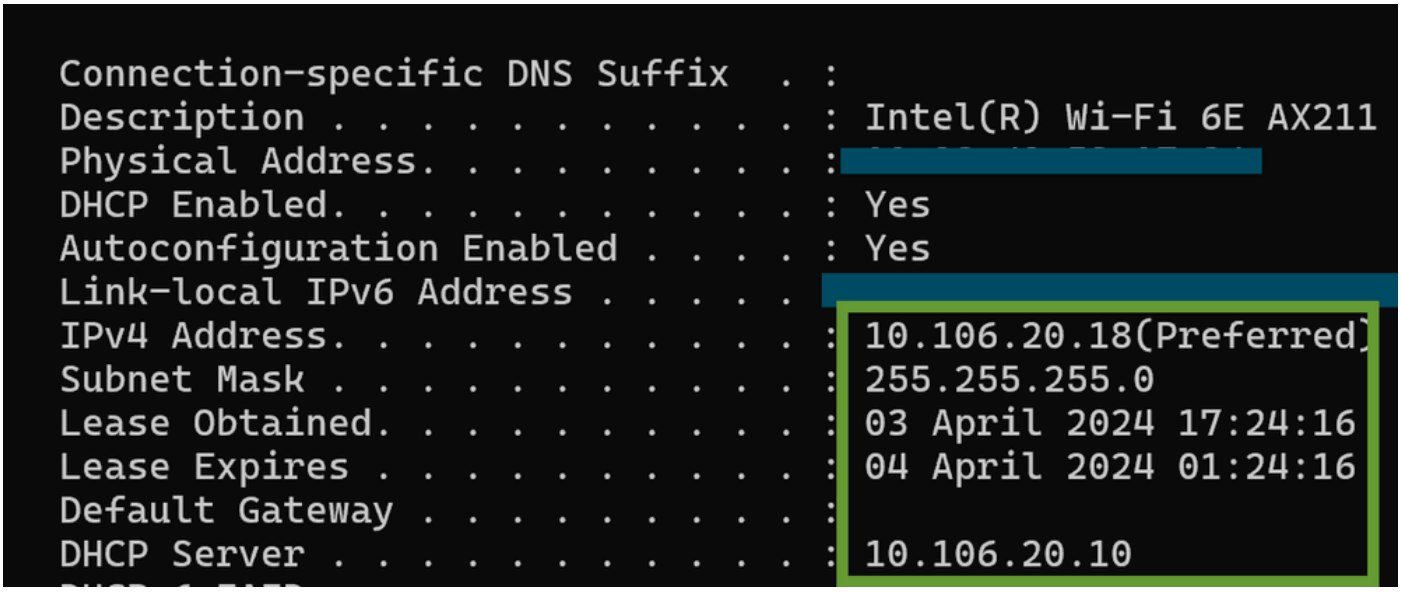
```
16540 111.905836    0.0.0.0           255.255.255.255     DHCP      343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10      10.106.20.18        DHCP      342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0           255.255.255.255     DHCP      385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

Captura de paquetes de extremo de cliente

Verificación de la IP del cliente inalámbrico:

Puede comprobar la concesión IP del servidor DHCP y su estado correspondiente.

En cliente inalámbrico:



Verificación de IP en extremo del cliente

Resolución de problemas de DHCP

La resolución de problemas de DHCP implica la identificación y resolución de problemas que impiden que los clientes obtengan una dirección IP de un servidor DHCP cuando están conectados a la red inalámbrica. Estos son algunos pasos y consideraciones comunes para la resolución de problemas de DHCP:

1. Verificar la configuración del cliente

- Asegúrese de que el cliente esté configurado para obtener una dirección IP automáticamente.
- Confirme que el adaptador de red está activado y funciona correctamente.

2. Comprobar el estado del servidor DHCP

- Confirme que el servidor DHCP está operativo y accesible desde el segmento de red del cliente.
- Compruebe la dirección IP, la máscara de subred y la configuración predeterminada de la puerta de enlace del servidor DHCP.

3. Revise la configuración del alcance

- Inspeccione el alcance DHCP para asegurarse de que tiene un rango suficiente de direcciones IP disponibles para los clientes.
- Verifique la duración y las opciones de concesión del ámbito, como los servidores DNS y la puerta de enlace predeterminada
- En algunos entornos (como Active Directory), asegúrese de que el servidor DHCP está autorizado para proporcionar servicios DHCP dentro de la red.

4. Revise la configuración en el WLC 9800

- Se han observado muchos problemas debido a una configuración incorrecta, como la falta de una interfaz de loopback, la SVI del cliente o la ausencia de una dirección de ayudante configurada. Antes de la recopilación de registros, se recomienda verificar que la configuración se ha implementado correctamente.
- Al utilizar un servidor DHCP interno: en cuanto al agotamiento del ámbito DHCP, es importante asegurarse, especialmente al configurar DHCP a través de la CLI, de que el temporizador de concesión se configura según sus requisitos. De forma predeterminada, el temporizador de arrendamiento se establece en infinito en el WLC 9800.
- Verifique que el tráfico VLAN del cliente esté permitido en el puerto de link ascendente del WLC cuando se utiliza un servidor DHCP central. Por el contrario, al emplear un servidor DHCP local, asegúrese de que la VLAN pertinente esté permitida en el puerto de enlace ascendente del AP.

5. Configuración de firewall y seguridad

- Asegúrese de que los firewalls o el software de seguridad no bloquean el tráfico DHCP (puerto 67 para el servidor DHCP y puerto 68 para el cliente DHCP).

Recopilación de registros

Registros de WLC

1. Habilite term exec prompt timestamp para tener una referencia de tiempo para todos los comandos.

2. Utilice show tech-support wireless !! para revisar la configuración

2. Puede comprobar el número de clientes, la distribución de estado del cliente y los clientes excluidos.
show wireless summary !! Número total de puntos de acceso y clientes
show wireless exclusionlist !! En caso de que cualquier cliente sea visto como excluido
show wireless exclusionlist client mac-address MAC@ !! para obtener más detalles sobre el cliente concreto excluido y comprobar si el motivo aparece como robo de IP para cualquier cliente.

3. Verifique la asignación de direcciones IP para los clientes, busque direcciones incorrectas o el aprendizaje de direcciones estáticas inesperadas, VLAN marcadas como "sucias" debido a que no hay respuesta del servidor DHCP, o paquetes descartados en SISF que está manejando DHCP/ARP.

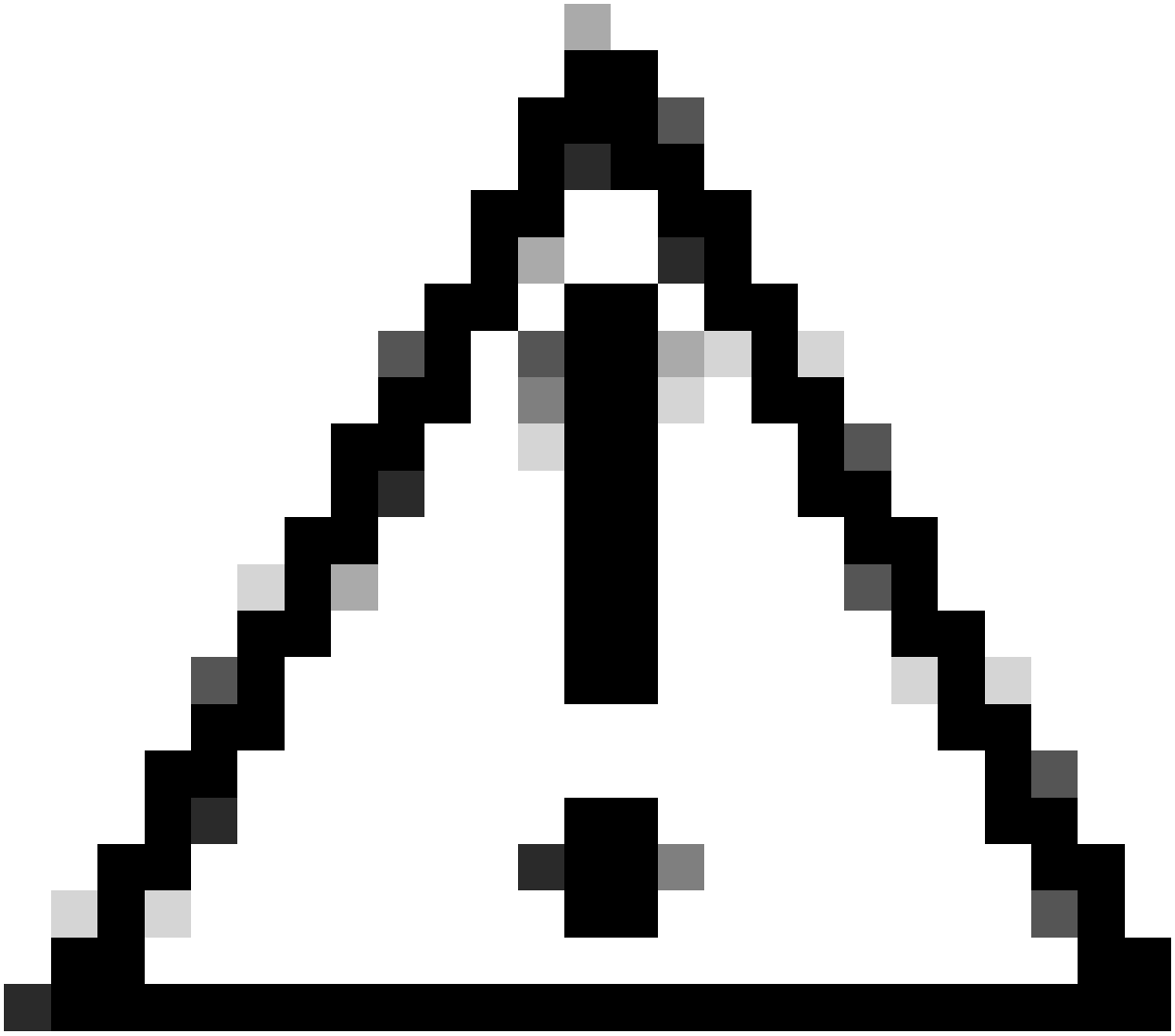
show wireless device-tracking database ip !! Verifique por IP y vea cómo ocurrió el aprendizaje de direcciones:
show wireless device-tracking database mac !! Verifique por Mac y vea qué cliente IP está asignado.
show wireless vlan details !! Verifique que la VLAN no esté marcada como "sucia" debido a fallas de DHCP en caso de que el grupo de VLAN esté en uso.
show wireless device-tracking feature drop !!Caídas en SISF

4. Salidas específicas del WLC para el cliente concreto MAC@ show wireless device-tracking feature drop

Habilite el seguimiento radioactivo para la dirección MAC del cliente cuando el cliente intenta conectar la red inalámbrica.

A través de 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



Precaución: la depuración condicional habilita el registro de nivel de depuración que, a su vez, aumenta el volumen de los registros generados. Si deja esta opción en ejecución, reducirá la cantidad de tiempo desde el que puede ver los registros. Por lo tanto, se recomienda desactivar siempre la depuración al final de la sesión de solución de problemas.

Para inhabilitar toda la depuración, ejecute estos comandos:

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

A través de GUI:

Paso 1. Desplácese hasta Troubleshooting > Radioactive Trace .
Paso 2. Haga clic Add e introduzca una dirección MAC del cliente que desee solucionar. Puede agregar varias direcciones Mac para realizar un seguimiento.

Paso 3. Cuando esté listo para iniciar el seguimiento radiactivo, haga clic en iniciar. Una vez iniciado, el registro de depuración se escribe en el disco sobre cualquier procesamiento del plano de control relacionado con las direcciones MAC objeto de seguimiento.

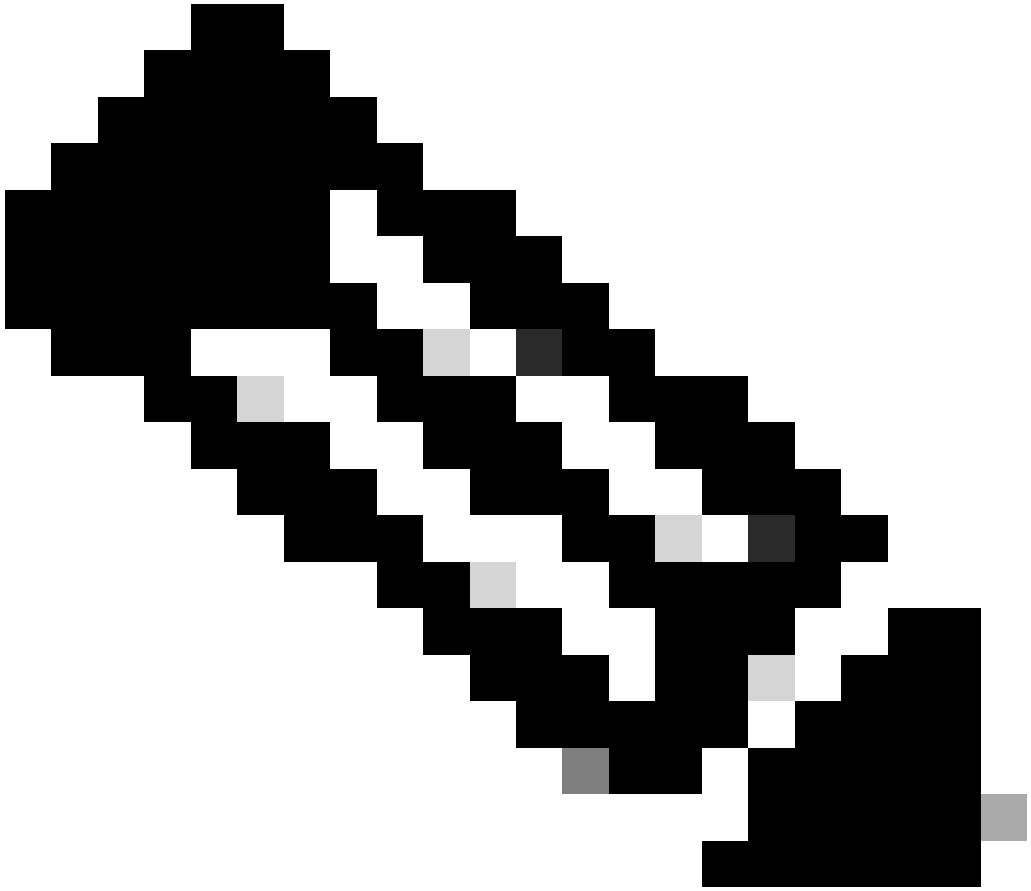
Paso 4. Cuando reproduzca el problema que desea solucionar, haga clic en Stop .

Paso 5. Para cada dirección MAC depurada, puede generar un archivo de registro que recopile todos los registros pertenecientes a esa dirección MAC haciendo clic en Generate .

Paso 6. Elija cuánto tiempo atrás desea que transcurra el archivo de registro intercalado y haga clic en Aplicar al dispositivo.

Paso 7. Ahora puede descargar el archivo haciendo clic en el pequeño icono situado junto al nombre del archivo. Este archivo está presente en la unidad flash de arranque del controlador y también se puede copiar desde el primer momento mediante CLI.

!!Capturas incrustadas filtradas por dirección MAC del cliente en ambas direcciones, filtro MAC interno del cliente disponible después de 17.1.



Nota: EPC en 9800 será útil cuando DHCP central esté habilitado en 9800 WLC.

A través de 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

A través de GUI:
Paso 1. Vaya a Troubleshooting > Packet Capture > +Add .

Paso 2. Defina el nombre de la captura de paquetes. Se permite un máximo de 8 caracteres.

Paso 3. Defina los filtros, si los hubiera.

Paso 4. Marque la casilla Monitor Control Traffic (Controlar el tráfico de control) si desea ver el tráfico dirigido a la CPU del sistema e insertado de nuevo en el plano de datos.

Paso 5. Defina el tamaño del búfer. Se permite un máximo de 100 MB.

Paso 6. Defina el límite, ya sea por la duración que permite un rango de 1 - 1000000 segundos o por el número de paquetes que permite un rango de 1 - 100000 paquetes, según lo deseado.

Paso 7. Elija la interfaz de la lista de interfaces de la columna izquierda y seleccione la flecha para moverla a la columna derecha.

Paso 8. Guardar y aplicar al dispositivo.

Paso 9. Para iniciar la captura, seleccione Iniciar.

Paso 10. Puede dejar que la captura se ejecute hasta el límite definido. Para detener manualmente la captura, seleccione Detener.

Paso 11. Una vez detenido, un botón Exportar está disponible para hacer clic con la opción de descargar el archivo de captura (.pcap) en el escritorio local a través de un servidor HTTP o TFTP o un servidor FTP o un disco duro o flash del sistema local.

Registros desde el lado del AP

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

Registros del servidor DHCP

Cuando se utiliza un servidor DHCP externo, es necesario recopilar registros de depuración y capturas de paquetes en el lado del servidor para verificar el flujo del tráfico DHCP.

Otros registros

Si observa que los mensajes de detección de DHCP son visibles en el WLC 9800 en una configuración DHCP central, o dentro de los registros de depuración de AP en una configuración DHCP local, debe proceder a recopilar datos de captura del link ascendente para confirmar que los paquetes no están cayendo en el puerto Ethernet.Dependiendo de las capacidades del switch, tiene la opción de realizar una captura de paquetes integrada o una captura SPAN (analizador de puerto conmutado) en el switch de link ascendente. Se recomienda rastrear el flujo de tráfico DHCP paso a paso para determinar el punto en el que se interrumpe la comunicación, tanto del cliente DHCP al servidor DHCP como en la dirección inversa.

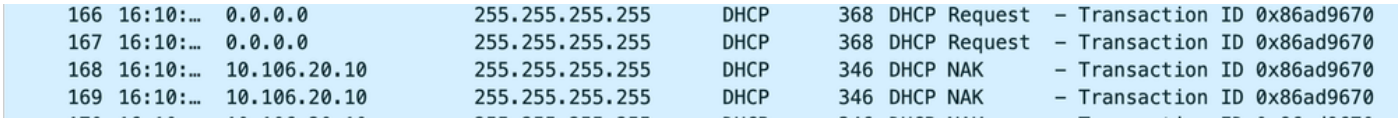
Problemas conocidos

Problema 1. El cliente está intentando obtener una dirección IP de una VLAN que previamente retuvo. Pueden surgir situaciones en las que un cliente inalámbrico cambia entre dos SSID asociados con diferentes VLAN de cliente. En estos casos, el cliente puede persistir en solicitar una IP de la VLAN a la que se conectó previamente. Debido a que esta IP no estará dentro del alcance DHCP de la VLAN actual, el servidor DHCP emitirá un NAK (reconocimiento negativo), y como resultado, el cliente no podrá adquirir una dirección IP.

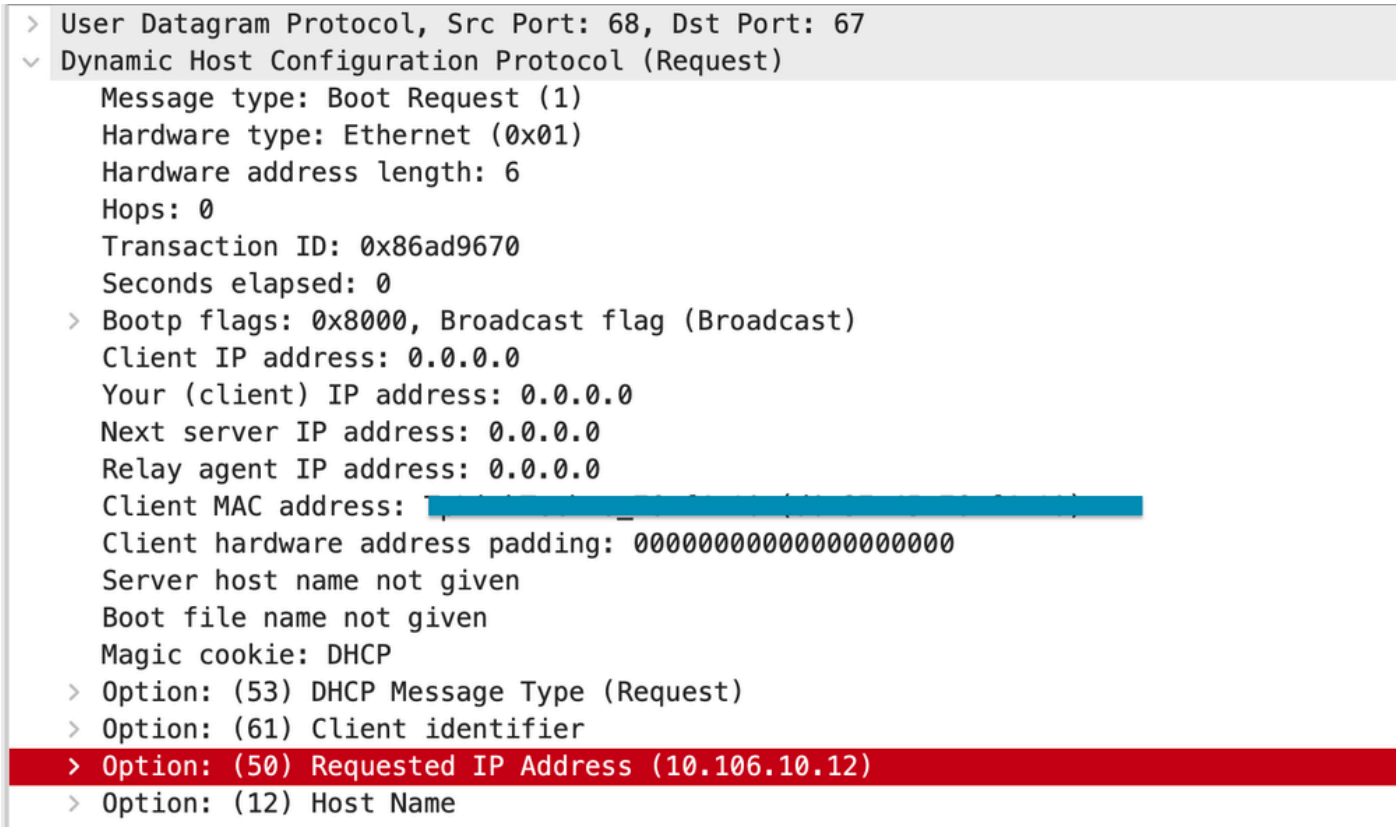
En los registros de seguimiento radiactivo, es evidente que el cliente continúa buscando una IP de la VLAN a la que estaba conectado anteriormente, que es VLAN 10, a pesar del hecho de que la VLAN del cliente para el SSID actual es VLAN 20.

```
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
```

Captura de paquetes integrada en WLC:



Captura de paquetes integrada en WLC



Opción DHCP 50 en captura de paquetes WLC

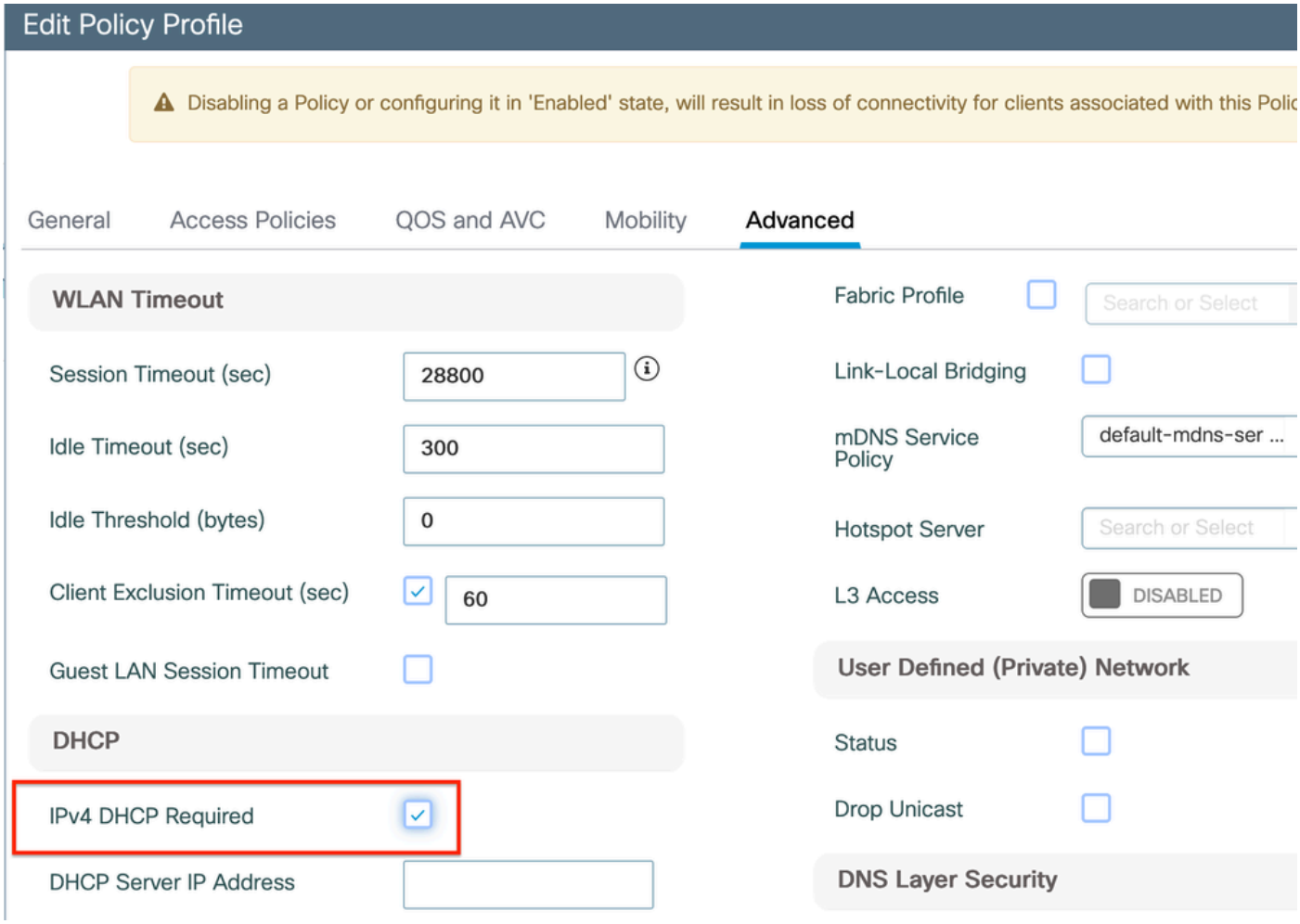
Resolución: Para asegurarse de que un cliente completa el proceso DHCP completo, puede activar la opción DHCP requerido IPv4 en la configuración de directivas. Esta configuración debe estar habilitada, especialmente cuando el cliente está conmutando entre SSID, para permitir que el servidor DHCP envíe un NAK al cliente si solicita una dirección IP de una VLAN asociada con el SSID anterior. De lo contrario, el cliente podría seguir utilizando o solicitando la dirección IP que tenía anteriormente, lo que interrumpiría la comunicación. Sin embargo, tenga en cuenta que la activación de esta función afectará a los clientes inalámbricos configurados con una dirección IP estática.

Este es el proceso para habilitar la opción deseada:

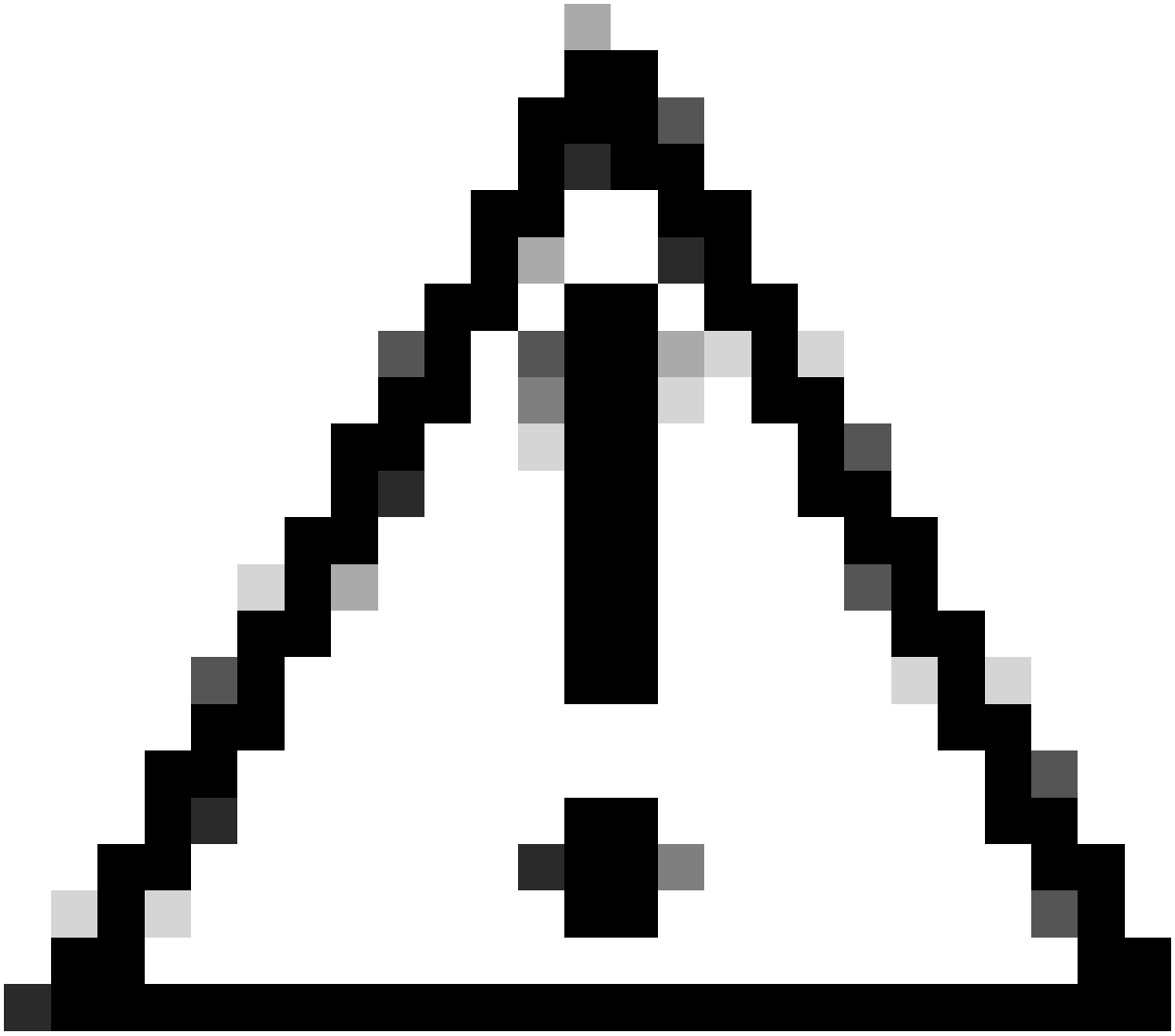
A través de CLI:

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

A través de la GUI: Navegue hasta Configuration > Tags & Profile > Policy > Policy_name > Advanced. En la sección DHCP (DHCP), active ipv4 DHCP required (DHCP obligatorio).



Configuración del Perfil de Política en WLC



Precaución: Para una configuración de anclaje externo, es importante alinear los ajustes DHCP a través de ambos WLC. Si tiene DHCP IPV4 requerido habilitado, necesita ser habilitado en los WLCs extranjeros y de anclaje. Una discrepancia en la configuración relacionada con DHCP en el perfil de política entre los dos podría hacer que los clientes experimenten problemas con sus funciones de movilidad.

Problema 2: el cliente se elimina o excluye debido a un problema de robo de IP. El robo de IP, en el contexto de la red, se refiere a una situación en la que más de un cliente inalámbrico está intentando utilizar la misma dirección IP. Puede deberse a muchas razones que se enumeran a continuación:

1. Asignación de IP estática no autorizada: cuando un usuario establece una dirección IP estática en su dispositivo que coincide con una IP ya asignada o asignada en la red, puede resultar en un conflicto de IP. Esto ocurre cuando dos dispositivos intentan funcionar con una dirección IP idéntica, lo que puede interrumpir las conexiones de red para uno o ambos dispositivos involucrados. Para evitar estos problemas, es esencial asegurarse de que cada cliente de la red esté configurado con una dirección IP única.

2. Servidor DHCP no autorizado: la presencia de un servidor DHCP no autorizado o no autorizado en la red puede llevar a la asignación de

direcciones IP que entra en conflicto con el plan de direcciones IP establecido de la red. Estos conflictos pueden dar lugar a que varios dispositivos experimenten colisiones de direcciones IP u obtengan una configuración de red incorrecta. Para solucionar este problema, se debe intentar identificar y eliminar el servidor DHCP no autorizado de la red para evitar más conflictos de IP dentro de la misma subred.

3. Entrada obsoleta del cliente en 9800 WLC: A veces, el controlador puede retener entradas obsoletas/obsoletas de una dirección IP que un cliente está intentando adquirir. En estos casos, se hace necesario eliminar manualmente estas entradas obsoletas del WLC 9800. A continuación se explica cómo hacerlo:

- Ejecute el rastro radiactivo para la dirección MAC que está en la lista de exclusión y fíltrelo con mac legítimo en el rastro radiactivo.

- Podrá ver los registros de errores: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: MAC de cliente: Affected_Client_MAC con IP: 10.37.57.24 fue agregado a la lista de exclusión, MAC de cliente legítimo: Legit_Client_MAC, IP: 10.37.57.24, razón: robo de dirección IP

- A continuación, ejecute estos comandos:
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(Si hay alguna entrada obsoleta, podrá ver más de una IP para una dirección MAC de cliente legítimo: una es la IP original mientras que la otra es la obsoleta/obsoleta].

Resolución: Elimine manualmente las entradas obsoletas del WLC 9800 mediante clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. En la implementación flexible con un servidor DHCP local que utiliza la misma subred: en las configuraciones de FlexConnect, es común que varias ubicaciones remotas utilicen un servidor DHCP local que asigna direcciones IP de una subred idéntica. Este escenario puede llevar a que los clientes inalámbricos de diferentes sitios reciban la misma dirección IP. Los controladores dentro de este marco de red se programan para detectar cuando las conexiones de varios clientes están utilizando una dirección IP idéntica, interpretando esto como un posible robo de IP. Como resultado, estos clientes se colocan normalmente en una lista de bloqueados para evitar conflictos de direcciones IP.

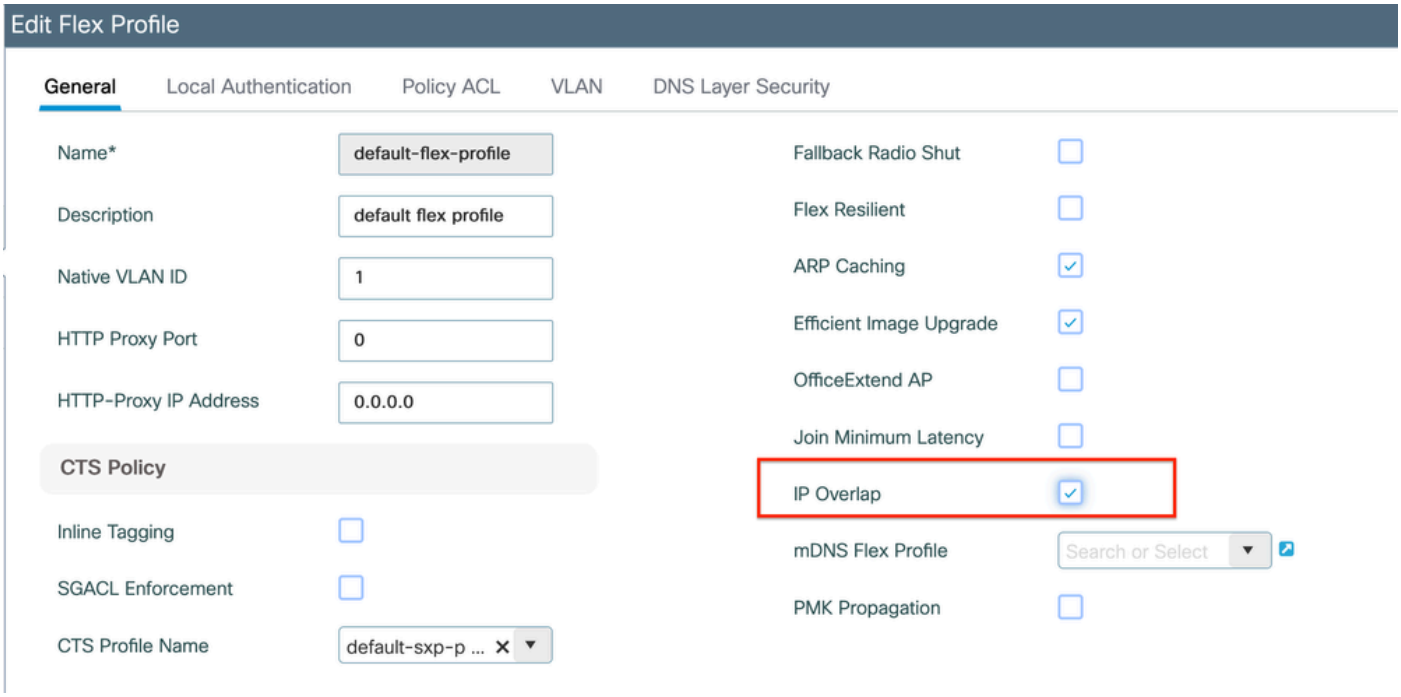
Resolución: habilite la función de superposición de IP en su perfil de FlexConnect. La funcionalidad de superposición de direcciones IP de cliente en Flex Deployment permite el uso de las mismas direcciones IP en varios sitios de FlexConnect, a la vez que se mantienen todas las funciones y capacidades admitidas en las implementaciones de FlexConnect.

De forma predeterminada, esta función está desactivada. Puede activarla mediante este procedimiento:

A través de CLI:

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

A través de la GUI: seleccione Configuration > Tags & Profiles > Flex. Haga clic en Existing Flex Profile/Add to new Flex profile y, en la ficha General, active IP Overlap.



Configuración de perfil flexible en WLC

Problema 3. Los clientes inalámbricos no reciben una dirección IP de la VLAN deseada. Este problema suele ocurrir cuando se utiliza la VLAN 1 o cuando la VLAN asignada a los clientes es la misma que la VLAN utilizada para la administración de AP en una implementación de FlexConnect. La causa raíz de este problema es generalmente asignaciones de VLAN incorrectas. A modo de guía, a continuación se detallan algunos escenarios a tener en cuenta al configurar los ID de VLAN en la serie 9800:

1. Al emplear un servidor AAA con la función de anulación AAA activada, es crucial asegurarse de que se envía el ID de VLAN apropiado desde el servidor AAA. Si se proporciona un nombre de VLAN en su lugar, confirme que coincide con el nombre de VLAN configurado en el WLC 9800.

2. Cuando la VLAN 1 se configura para el tráfico de clientes inalámbricos, el comportamiento puede variar en función del modo del punto de acceso (AP):

Para un AP en modo local/conmutación central:

- Al especificar VLAN-name = default, el cliente se asigna a VLAN 1
- Con VLAN-ID 1, se asigna un cliente a la VLAN de administración inalámbrica

Para un AP en modo Flex/Local Switching:

- Al especificar VLAN-name = default, el cliente se asigna a VLAN 1
- Con VLAN-ID 1, se asigna un cliente a la VLAN nativa de FlexConnect

Estos son algunos ejemplos más de escenarios que se han experimentado en el laboratorio, junto con sus resultados:

1. De forma predeterminada, si el usuario no configura nada bajo el perfil de política, el WLC asigna VLAN-ID 1 para que los clientes utilicen la VLAN de administración inalámbrica en modo local y la VLAN nativa AP para FlexConnect.

2. Si el Native-VLAN bajo flex-profile se configura con un ID de VLAN nativa diferente del configurado en el switch, verá el problema, el cliente obtiene la IP de la VLAN de administración (Native VLAN) incluso si el perfil de política se configura con el nombre de VLAN "predeterminado".

3. Si Native-VLAN bajo flex-profile se configura con VLAN-ID igual que la VLAN nativa configurada en el switch, entonces sólo el cliente podrá obtener una IP de VLAN 1 con el valor predeterminado configurado bajo el perfil de política.

4. Si seleccionó un nombre de VLAN en lugar de un ID de VLAN, asegúrese de que el nombre de VLAN en el perfil de Flex sea el mismo.

Información Relacionada

- Servidor DHCP interno en 9800
- Servidor DHCP externo en uso
- Opción DHCP 82 Subopción 5 en el servidor DHCP de Windows
- NAT-PAT en Flex AP
- VLAN 1 se utiliza para el cliente inalámbrico
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).