Solucionar problemas de conectividade do cliente DHCP em um Cisco 9800 WLC

Contents

Introdução

Este documento descreverá vários problemas relacionados ao protocolo de configuração dinâmica de host (DHCP - Dynamic Host Configuration Protocol) encontrados por clientes sem fio quando conectados a um controlador de LAN sem fio (WLC - Wireless LAN Controller) Cisco 9800 e como solucioná-los.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Cisco WLC 9800

- Conhecimento básico do fluxo de DHCP
- Conhecimento básico de AP de modo de conexão local e flexível

Entendendo o fluxo de tráfego DHCP com clientes sem fio

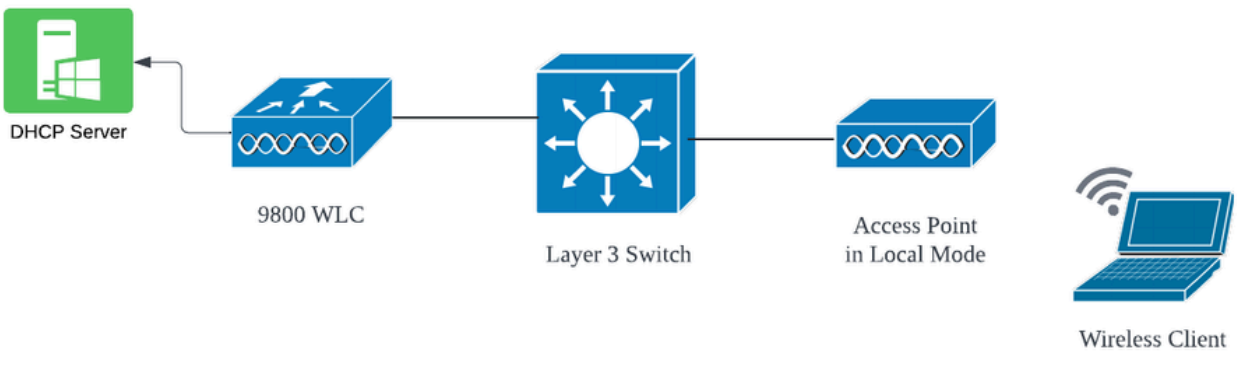
Quando o cliente sem fio se conecta, ele faz a troca DHCP normal enviando um quadro de descoberta de DHCP de broadcast para encontrar um servidor DHCP para o AP associado. Dependendo do modo de operação do AP, ele encaminhará a solicitação para a WLC através do túnel CAPWAP ou passará diretamente para o próximo salto. Se um servidor DHCP estiver disponível no domínio local da camada 2, ele responderá, facilitando uma conexão bem-sucedida. Na ausência de um servidor DHCP de sub-rede local, o roteador (configurado com o SVI do cliente) deve ser configurado para rotear a descoberta de DHCP para o servidor apropriado. Isso normalmente é feito pela configuração de um endereço IP auxiliar no roteador, que o instrui a encaminhar tráfego UDP de broadcast específico (como solicitações DHCP) para um endereço IP predeterminado.

O comportamento do tráfego DHCP do cliente depende inteiramente do modo em que seu ponto de acesso (AP) está operando. Vamos examinar cada um desses cenários separadamente:

Cenário 1. O ponto de acesso (AP) está operando no modo local

Quando um AP é configurado no modo local, o tráfego DHCP do cliente é comutado centralmente, o que significa que as solicitações DHCP dos clientes são enviadas através de um túnel CAPWAP do AP para o WLC, onde são processadas e encaminhadas de acordo. Nesse caso, há duas opções: você pode utilizar um servidor DHCP interno ou optar por um servidor DHCP externo.

Topologia (Modo Local AP)



Casos Práticos 1. Quando a WLC está configurada como um servidor DHCP interno

O controlador é capaz de oferecer um servidor DHCP interno através dos recursos integrados do software Cisco IOS XE. No entanto, é considerado uma prática recomendada usar um servidor DHCP externo. Antes de configurar a WLC como um servidor DHCP interno, vários pré-requisitos devem ser atendidos, que são os seguintes:

- Certifique-se de configurar uma interface virtual comutada (SVI) para a VLAN cliente e atribuir o endereço IP do servidor DHCP a ela.
- O endereço IP do servidor DHCP interno deve ser definido na interface voltada para o servidor, que pode ser uma interface de loopback, uma SVI ou uma interface física de Camada 3.
- Recomenda-se configurar a interface de loopback porque, ao contrário das interfaces físicas que se conectam a segmentos de rede reais, a interface de loopback não está ligada ao hardware e não corresponde a uma porta física no dispositivo. A finalidade principal de uma interface de loopback é fornecer uma interface estável e sempre ativa que não esteja sujeita a falhas de hardware ou desconexões físicas.

Configuração em funcionamento: este é um exemplo de uma configuração de servidor DHCP interno em que os clientes receberam endereços IP com êxito. Aqui estão os logs operacionais e os detalhes de configuração associados.

Configure a WLC como o servidor DHCP para a VLAN 10, com um escopo de DHCP que varia 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
```

Interface de loopback configurada no WLC:

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

VLAN cliente configurada como SVI [Interface L3] com endereço auxiliar como interface de loopback no 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, você pode definir o endereço IP do servidor DHCP dentro do perfil de política, em vez de configurar um endereço auxiliar sob o SVI. No entanto, geralmente é recomendável configurá-lo em uma base por VLAN para práticas recomendadas:

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

Rastreamentos radioativos em 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 pacotes incorporadas no 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 pacotes incorporada na WLC

Depurações de clientes 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 pacotes do lado do 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 pacote final do cliente

Nos registros operacionais fornecidos, você pode ver que a WLC está recebendo a mensagem DHCP Discover do cliente wireless e a VLAN do cliente está retransmitindo-a para o endereço auxiliar (que no exemplo fornecido é a interface de loopback interna). Em seguida, o servidor interno emite uma oferta de DHCP e, subsequentemente, o cliente envia uma solicitação de DHCP, que é confirmada pelo servidor com um DHCP ACK.

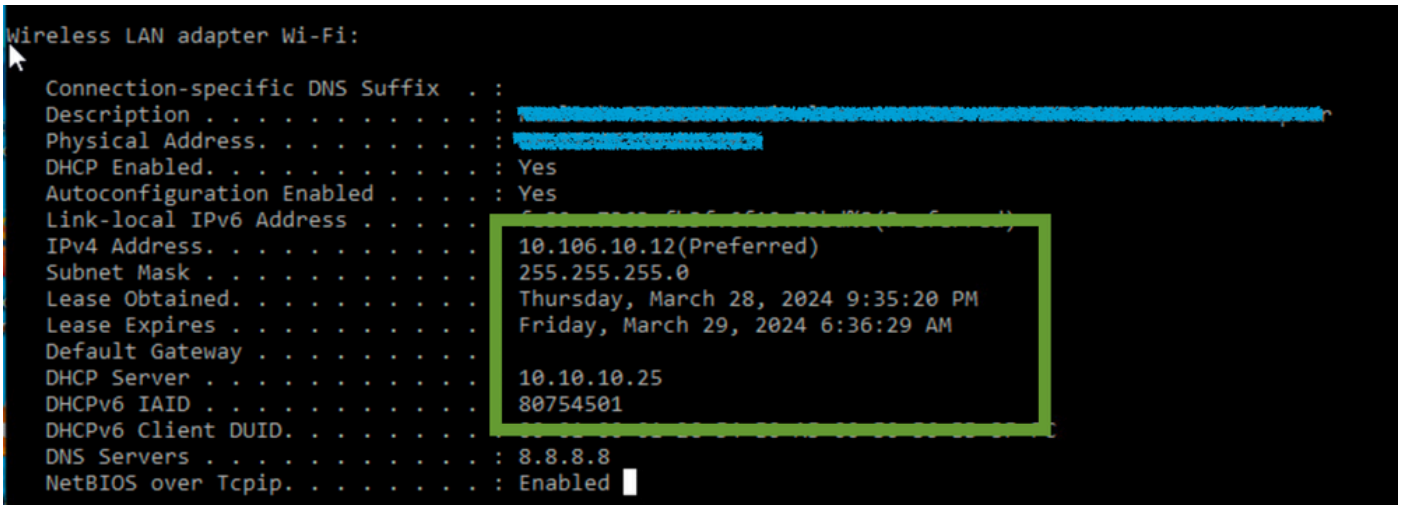
Verificação do IP do cliente sem fio:

No WLC:

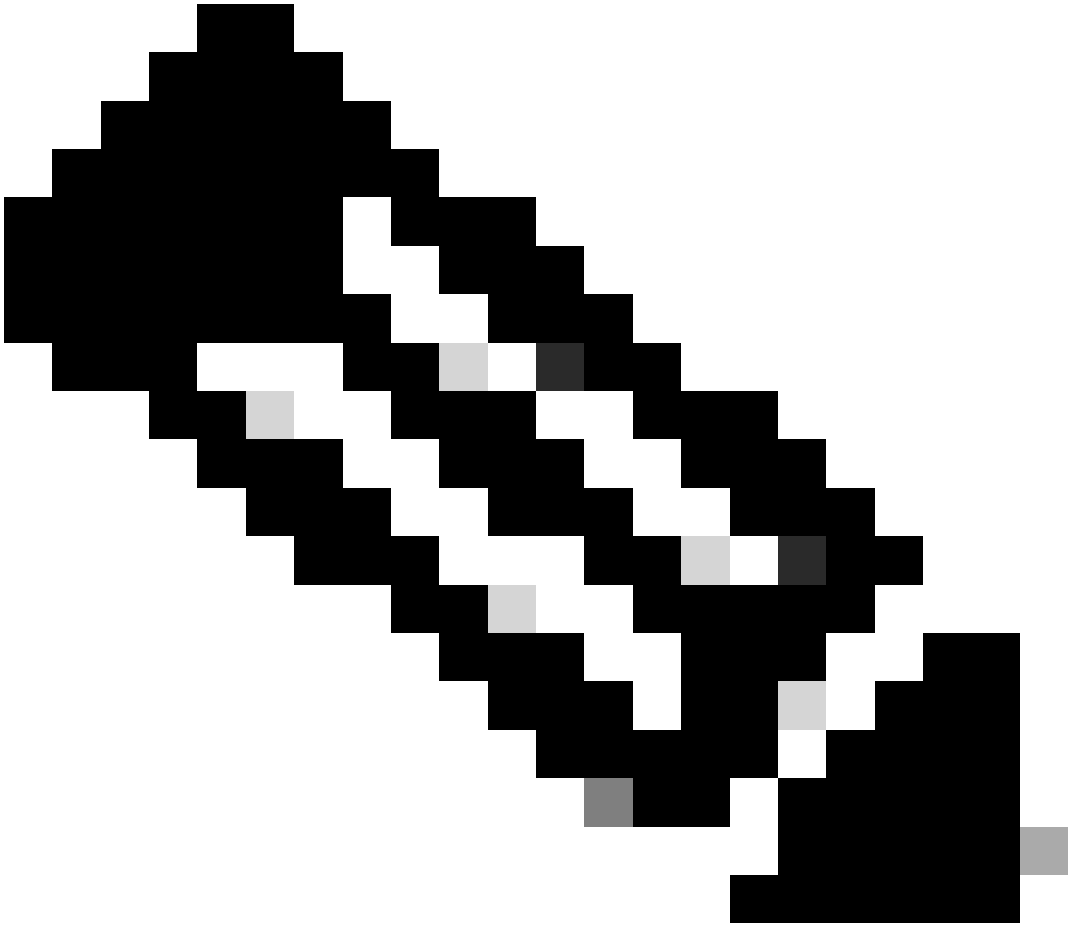
```
WLC#show ip dhcp binding
```

```
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
```

No cliente sem fio:



Verificação de IP na extremidade do Cliente



Note:
1. O VRF não é suportado nos servidores DHCP internos.
2. Não há suporte para DHCPv6 nos servidores DHCP internos.
3. No C9800, o SVI permite configurar vários endereços auxiliares, mas somente os 2 primeiros são usados.
4. Isso foi testado e, portanto, é suportado em todas as plataformas para um máximo de 20% da escala máxima de cliente da caixa. Por exemplo, para um 9800-80 que suporta 64.000 clientes, o número máximo de vinculações de DHCP suportadas é de cerca de 14.000.

Casos Práticos 2. Quando um servidor DHCP externo é usado

Um servidor DHCP externo refere-se a um servidor DHCP que não está integrado no próprio WLC, mas configurado em um dispositivo de rede diferente [Firewall, Roteadores] ou em uma entidade separada dentro da infraestrutura de rede. Esse servidor é dedicado a gerenciar a distribuição dinâmica de endereços IP e outros parâmetros de configuração de rede para clientes na rede.

Ao utilizar um servidor DHCP externo, a função da WLC é apenas receber e retransmitir o tráfego. O modo como o tráfego DHCP é roteado da WLC, seja ele de broadcast ou unicast, varia de acordo com sua preferência. Vamos considerar cada um desses métodos separadamente.

Tráfego DHCP transmitido pelo domínio da camada 2

Nessa configuração, outro dispositivo de rede, como um firewall, uplink ou switch central, atua como um agente de retransmissão. Quando um cliente envia uma solicitação de descoberta de DHCP, o único trabalho da WLC é encaminhar esse broadcast através da interface de Camada 2. Para que isso funcione corretamente, você deve garantir que a interface de Camada 2 da VLAN do cliente esteja configurada corretamente e seja permitida através da porta de dados da WLC e do dispositivo de uplink.

Configuração desejada na extremidade da WLC para a VLAN 20 do cliente para esta instância:

VLAN da camada 2 configurada no WLC:

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

Porta de dados configurada na WLC para permitir o tráfego da VLAN do 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
```

Rastreamentos radioativos em WLC 9800:

```
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 pacote incorporada realizada no 9800 WLC:

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

Captura de pacotes incorporada na WLC

Depurações de clientes 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 do lado do 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
```

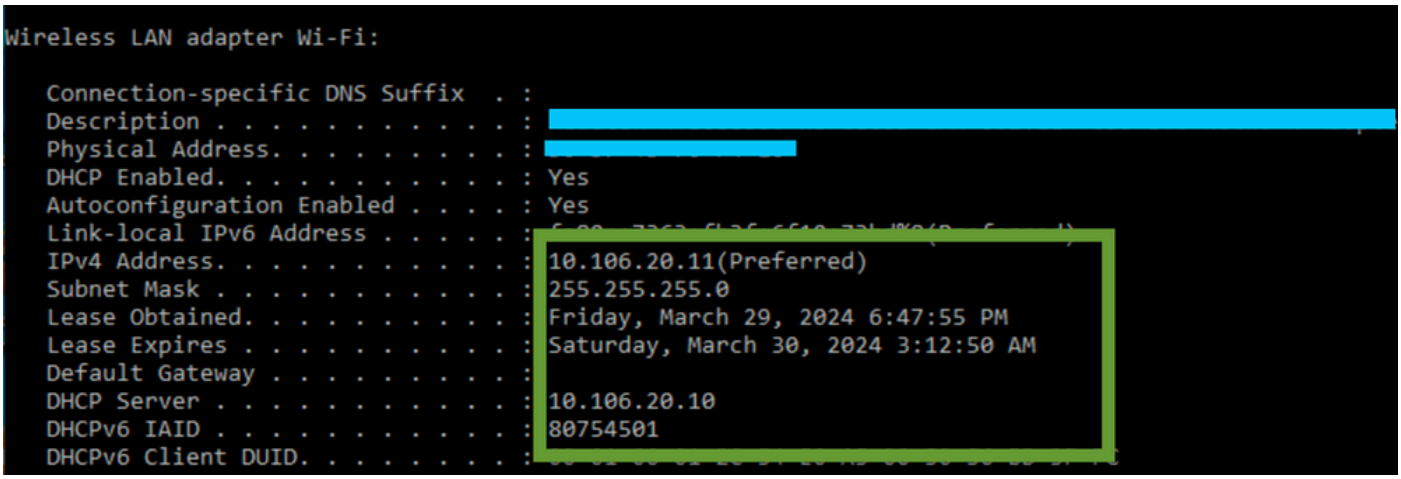
Captura de pacote final do cliente

Nos registros operacionais fornecidos, você observa nos registros que a WLC está interceptando o broadcast DHCP Discover do cliente sem fio e, em seguida, transmitindo-o adiante para o próximo salto através de sua interface L2. Assim que a WLC receber a oferta de DHCP do servidor, ela encaminhará essa mensagem ao cliente, seguida pela solicitação de DHCP e ACK.

Verificação do IP do cliente sem fio:

Você pode verificar a concessão de IP no servidor DHCP e seu status correspondente.

No cliente sem fio:



Verificação de IP na Extremidade do Cliente

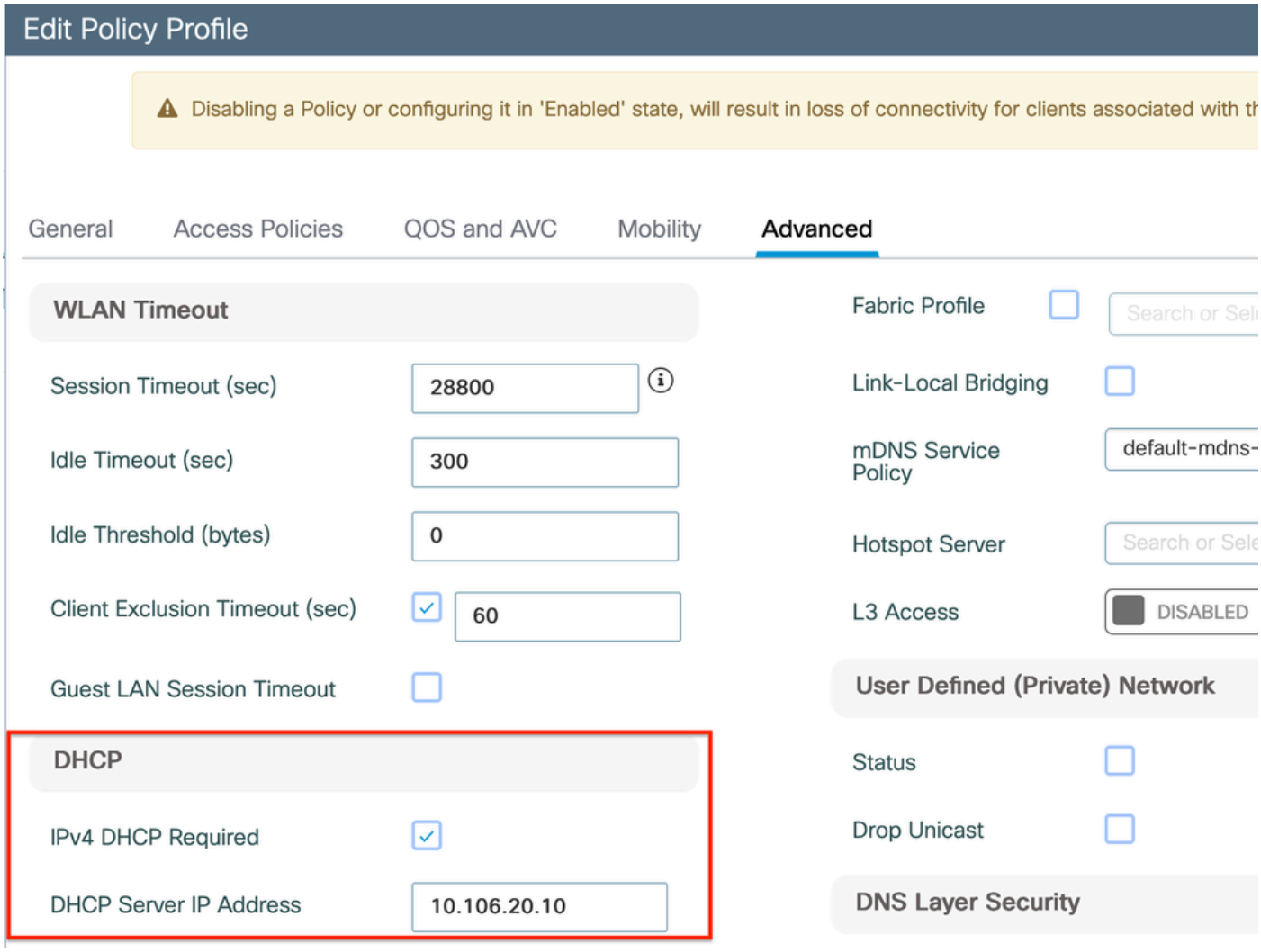
A WLC 9800 está servindo como um agente de retransmissão

Nessa configuração, a WLC encaminha diretamente os pacotes DHCP que recebe dos clientes sem fio para o servidor DHCP por unicast. Para permitir isso, certifique-se de que a SVI da VLAN para o cliente esteja configurada na WLC.

Há duas maneiras de configurar o IP do servidor DHCP no 9800 WLC:

1. Configure o IP do servidor DHCP no perfil de política em configuração avançada.

Via GUI: Navegue até Configuration > Tags & Profile > Policy > Policy_name > Advanced. Na seção DHCP você pode configurar o IP do servidor DHCP como mostrado:



Configuração do perfil de política no WLC

Via CLI:

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

2. Na configuração do SVI, você deve especificar o endereço do auxiliar. É possível configurar vários servidores DHCP na configuração do endereço auxiliar para fornecer redundância. Embora seja possível definir o endereço do servidor DHCP para cada WLAN no perfil de política, a abordagem recomendada é configurá-lo em uma base por interface. Isso pode ser feito atribuindo-se um endereço de ajuda ao SVI correspondente.

Ao empregar o recurso de retransmissão, a origem do tráfego DHCP será o endereço IP da SVI (Switched Virtual Interface) do cliente. Esse tráfego é então roteado através da interface correspondente ao destino (o endereço IP do servidor DHCP) conforme determinado pela tabela de roteamento.

Aqui está um exemplo da configuração de trabalho no 9800 que serve como um agente de retransmissão:

Interface de Camada 3 Configurada para VLAN Cliente no WLC com endereço 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
```

Porta de dados configurada na WLC para permitir o tráfego da VLAN do 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
```

Rastreamentos de RA do 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 pacotes incorporada na 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 pacotes incorporada na WLC

Tanto no RA (Radioative Traces, rastreamentos radioativos) quanto no EPC (Embedded Packet Capture, captura de pacotes incorporada) na WLC, você observará que a WLC, atuando como um agente de retransmissão, está unicast diretamente os pacotes DHCP do cliente para o

servidor DHCP.

Depurações de clientes 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 do lado do cliente:

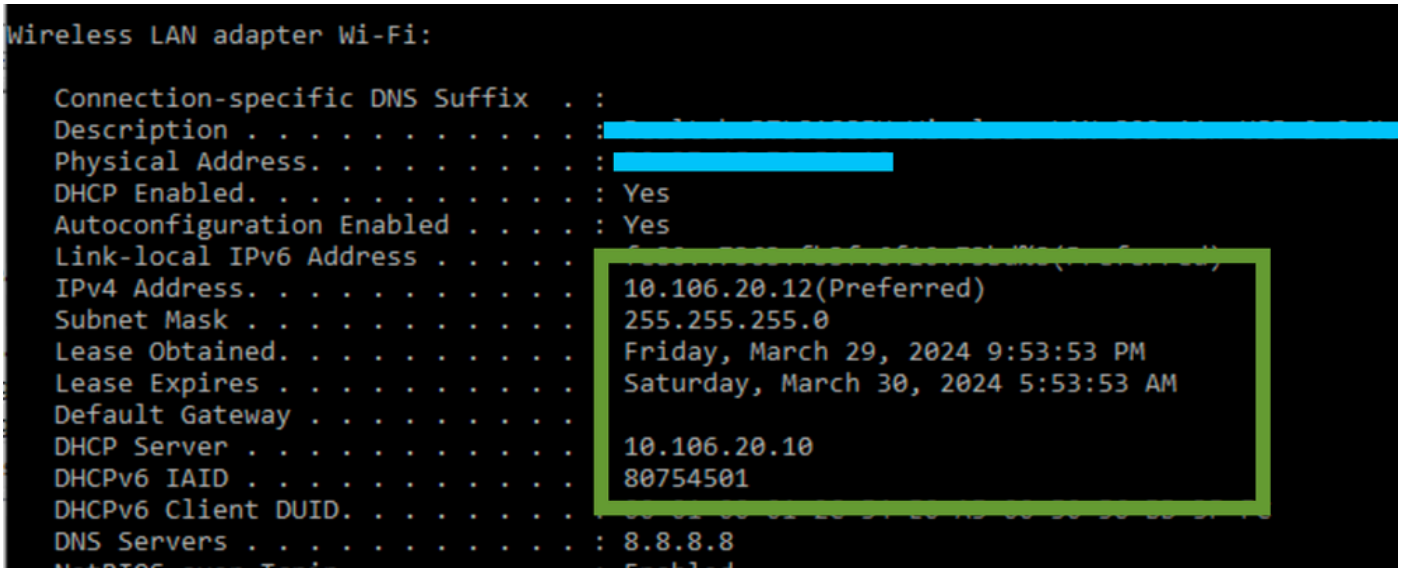
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer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

Verificação do IP do cliente sem fio:

Você pode verificar a concessão de IP no servidor DHCP e seu status correspondente.

No cliente sem fio:



Verificação de IP na Extremidade do Cliente

DHCP Opção 80 com Subopção 5/150 na WLC 9800

Em determinados cenários, talvez você prefira definir explicitamente a interface de origem para o tráfego DHCP em vez de, dependendo da tabela de roteamento, evitar possíveis complicações de rede. Isso é particularmente relevante quando o próximo dispositivo de rede ao longo do caminho, como um switch ou firewall de Camada 3, emprega verificações de Encaminhamento de Caminho Reverso (RPF). Considere, por exemplo, uma situação em que a interface de gerenciamento sem fio é definida na VLAN 50, enquanto a SVI do cliente está na VLAN 20 e está

sendo usada como uma retransmissão de DHCP para o tráfego do cliente. A rota padrão é direcionada para o gateway da VLAN/sub-rede de gerenciamento sem fio.

Começando com a versão 17.03.03 na WLC 9800, é possível escolher a interface de origem para o tráfego DHCP como a VLAN cliente ou outra VLAN, como a interface de gerenciamento sem fio (WMI), que garante a conectividade com o servidor DHCP.

Aqui está um recorte da configuração:

```
!
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
```

Neste cenário, o tráfego para o servidor DHCP 10.100.17.14 será originado da VLAN 50 (10.100.16.10), pois a interface de saída do pacote é selecionada com base em uma pesquisa na tabela de roteamento IP e, normalmente, sairia através da VLAN da Interface de Gerenciamento Sem Fio (WMI) devido à rota padrão configurada.
No entanto, se um switch de uplink implementar verificações de Encaminhamento de Caminho Reverso (RPF), ele poderá descartar um pacote que chega da VLAN 50, mas com um endereço IP de origem pertencente a uma sub-rede diferente [VLAN 20].

Para evitar isso, você deve definir uma interface de origem precisa para os pacotes DHCP com o comando IP DHCP relay source-interface. Neste caso específico, você desejaria que os pacotes DHCP se originassem da interface WMI na 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
```

Ao usarip dhcp relay source-interface o comando, a interface de origem dos pacotes DHCP e o GIADDR são definidos como a interface especificada no comando de retransmissão DHCP (VLAN50, neste caso). Isso é um problema, pois essa não é a VLAN do cliente na qual você deseja atribuir endereços DHCP.

Como o servidor DHCP sabe como atribuir o IP do pool de clientes correto?

Assim, a resposta para isso é quando ip dhcp relay source-interface o comando é usado, o C9800 adiciona automaticamente as informações de sub-rede do cliente em uma subopção proprietária 150 da opção 82 chamada seleção de link, como você pode ver na captura:

```
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
```

Opção 182, subopção 150 na Captura de Pacotes de WLC

Por padrão, ele adicionará a subopção 150 (proprietário da cisco). Certifique-se de que o servidor DHCP usado possa interpretar e agir com base nessas informações. A recomendação é alterar a configuração do C9800 para usar a opção padrão 82, subopção 5, para enviar as informações de seleção de link. Você pode fazer isso configurando o seguinte comando global:

<#root>

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

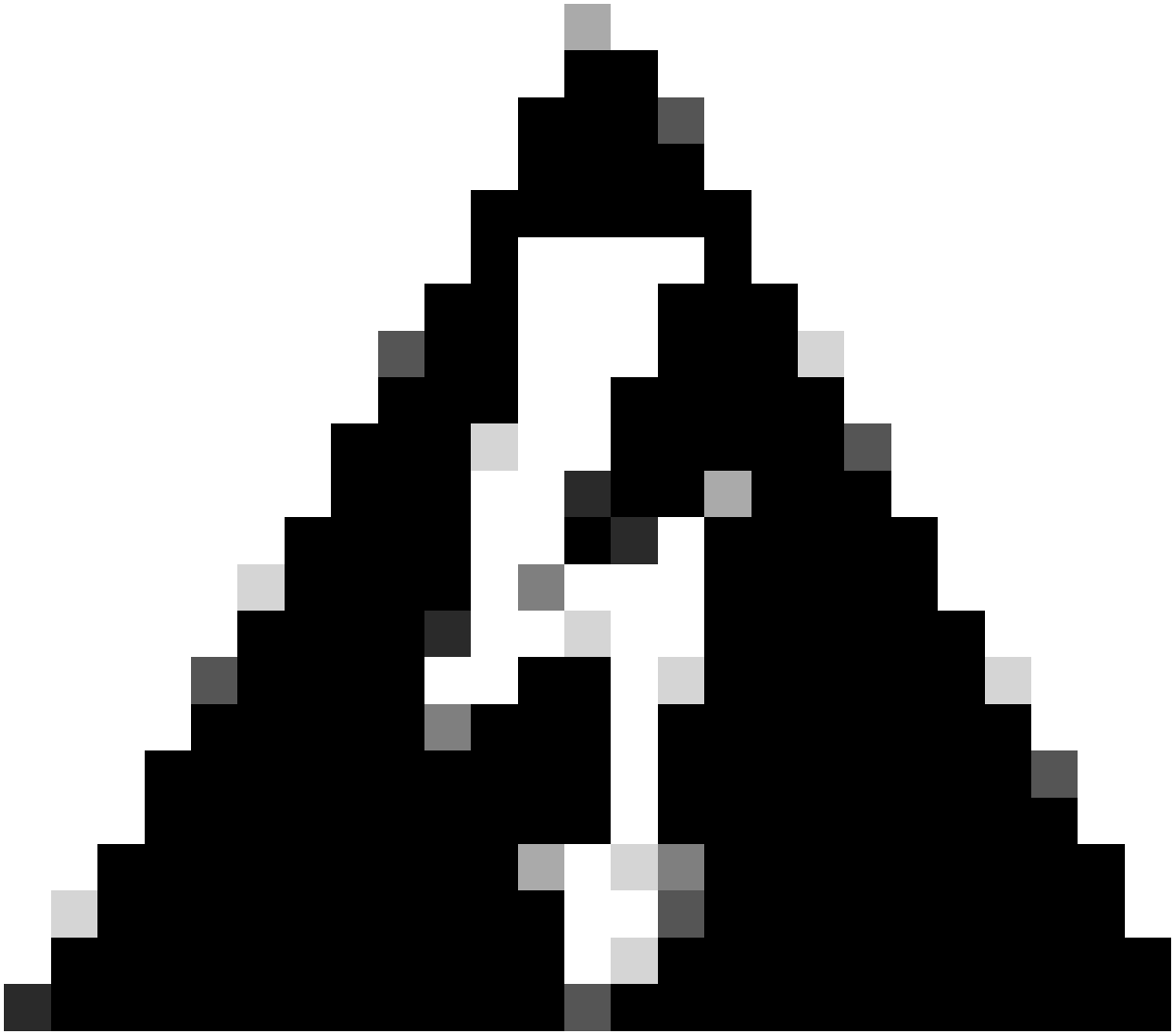
Uma vez aplicado o comando especificado, o sistema substituirá a subopção 150 pela subopção 5 nos pacotes DHCP. A subopção 5 é mais amplamente reconhecida pelos dispositivos de rede, garantindo, assim, que os pacotes sejam menos propensos a serem descartados. A aplicação dessa alteração também é evidente na captura fornecida:

```
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)
```

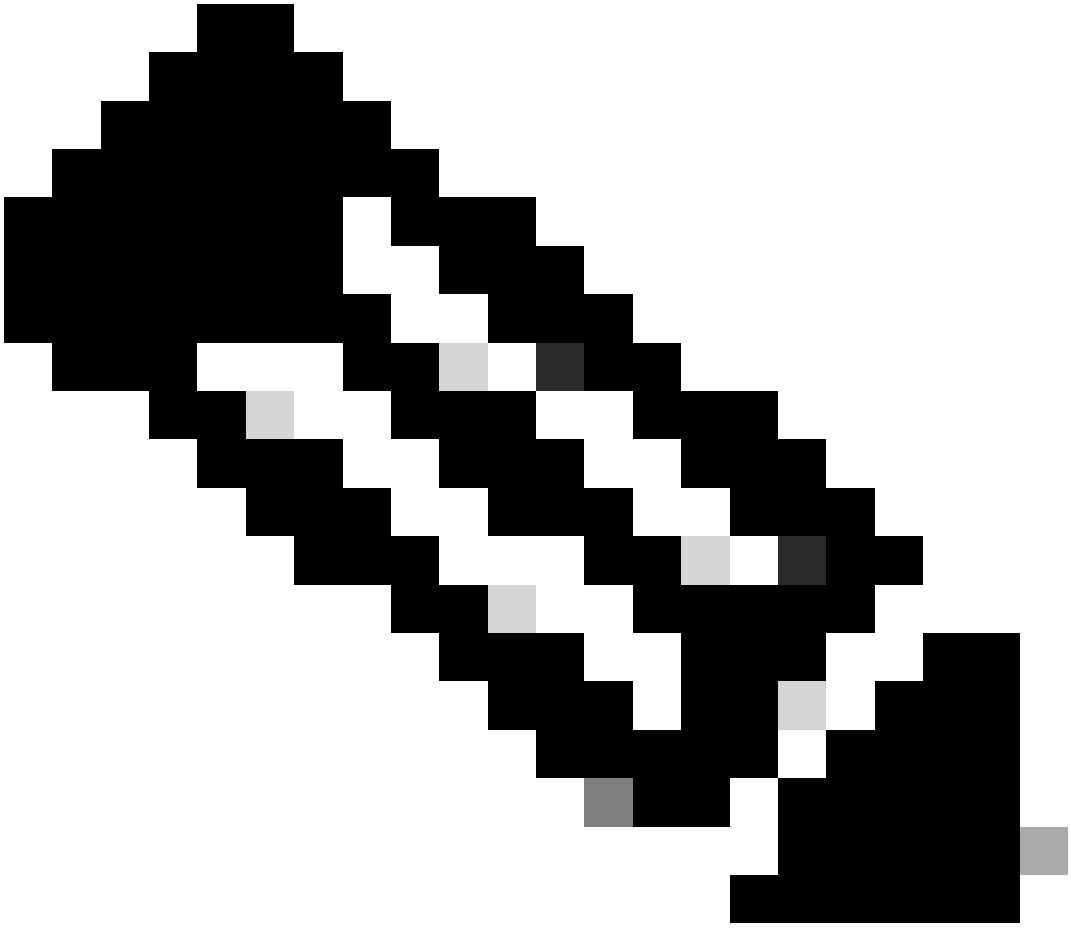
Opção 182, subopção 5, na Captura de Pacotes de WLC

Com a implementação da subopção 5, seu tráfego DHCP deve ser reconhecido por outros dispositivos de rede. No entanto, você ainda pode encontrar mensagens NAK (reconhecimento negativo), especialmente quando o servidor DHCP do Windows está em uso. Isso pode ocorrer porque o servidor DHCP não autoriza o endereço IP de origem, possivelmente porque ele não tem uma configuração correspondente para esse IP de origem.

O que você precisa fazer no servidor DHCP? Para o servidor DHCP do Windows, você precisa criar um escopo fictício para autorizar o IP do agente de retransmissão.



Aviso: todos os endereços IP de agentes de retransmissão (GIADDR) devem fazer parte de um intervalo de endereços IP de escopo de DHCP ativo. Qualquer GIADDR fora dos intervalos de endereços IP do escopo do DHCP é considerado um relay invasor e o Windows DHCP Server não confirmará as solicitações de cliente DHCP desses agentes de relay. Um escopo especial pode ser criado para autorizar agentes de retransmissão. Crie um escopo com o GIADDR (ou vários GIADDRs se forem endereços IP sequenciais), exclua o(s) endereço(s) GIADDR da distribuição e ative o escopo. Isso autorizará os agentes de retransmissão enquanto impede que os endereços GIADDR sejam atribuídos.

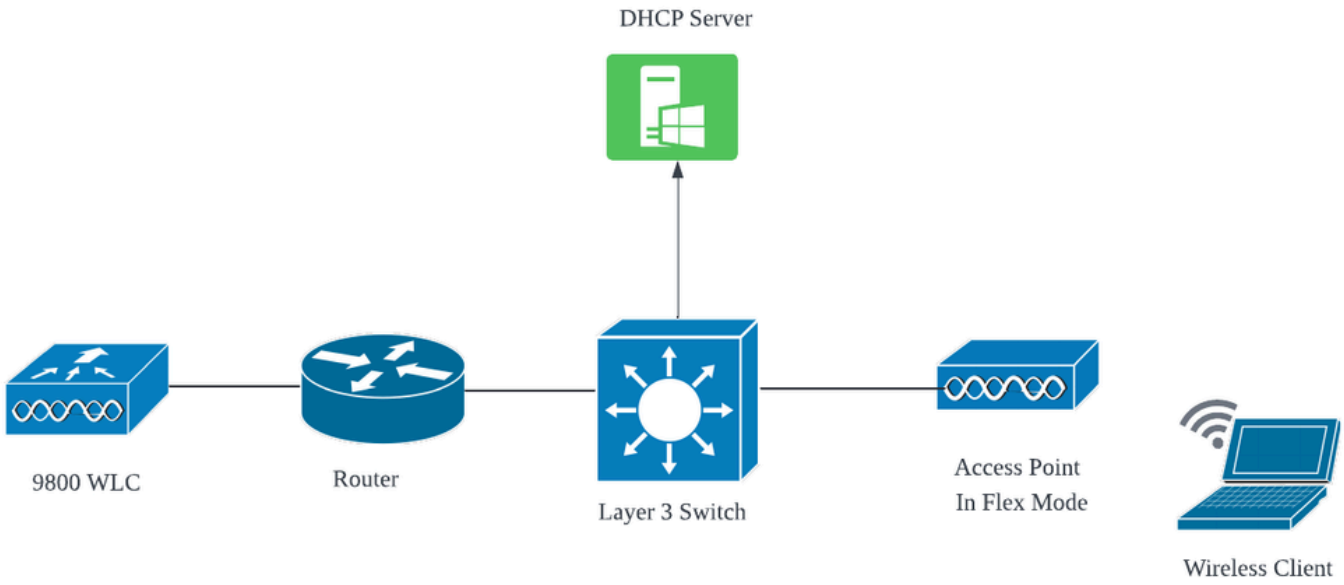


Observação: em uma configuração de âncora externa, o tráfego DHCP é processado centralmente com o modo AP definido como Local. Inicialmente, as solicitações DHCP são enviadas para a WLC estrangeira, que as encaminha para a WLC âncora por meio de um túnel de mobilidade. É a WLC âncora que manipula o tráfego de acordo com suas configurações definidas. Portanto, todas as configurações relacionadas ao DHCP devem ser implementadas na WLC âncora.

Cenário 2. O ponto de acesso (AP) está operando no modo Flex

Os APs FlexConnect são projetados para filiais e escritórios remotos, permitindo que eles operem em um modo autônomo quando perdem a conectividade com a controladora Wireless LAN (WLC) central. Os APs FlexConnect podem alternar localmente o tráfego entre um cliente e a rede sem precisar fazer backhaul do tráfego para a WLC. Isso reduz a latência e preserva a largura de banda da WAN. No AP de modo flex, o tráfego DHCP pode ser comutado centralmente ou localmente.

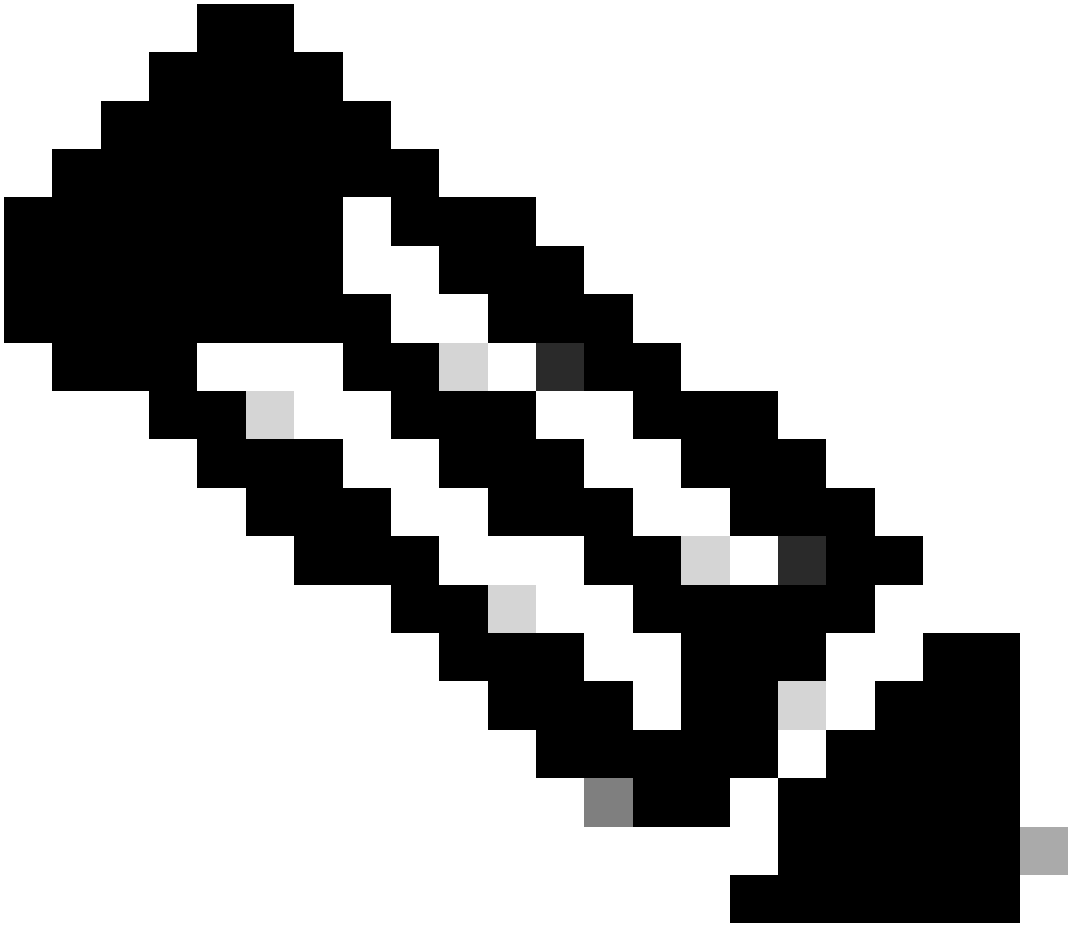
Topologia (AP de modo flexível)



Topologia de rede: AP de modo flexível

AP do modo FlexConnect com DHCP central

Independentemente do modo do AP, a configuração, o fluxo operacional e as etapas de solução de problemas permanecem consistentes ao usar um servidor DHCP central. No entanto, para APs no modo FlexConnect, geralmente é recomendável usar um servidor DHCP local, a menos que você tenha uma SVI de cliente configurada no site local.



Observação: se você não tiver uma sub-rede de cliente disponível no local remoto, poderá aproveitar o NAT-PAT do FlexConnect. O NAT/PAT do FlexConnect executa a conversão de endereço de rede (NAT) para o tráfego originado de clientes conectados ao AP, mapeando-o para o endereço IP de gerenciamento do AP. Por exemplo, se você tiver APs operando no modo FlexConnect em filiais remotas e os clientes conectados precisarem se comunicar com um servidor DHCP localizado na matriz onde os controladores residem, você poderá ativar o NAT/PAT FlexConnect em conjunto com a configuração DHCP central no perfil de política.

AP do modo FlexConnect com DHCP local

Quando um AP FlexConnect é configurado para usar DHCP local, os dispositivos clientes que se associam ao AP recebem sua configuração de endereço IP de um servidor DHCP que está disponível na mesma rede local. Esse servidor DHCP local pode ser um roteador, um servidor DHCP dedicado ou qualquer outro dispositivo de rede que forneça serviços DHCP dentro da sub-rede local. Com o DHCP local, o tráfego DHCP é comutado dentro da rede local, o que significa que o AP retransmite as solicitações DHCP dos clientes diretamente para o salto adjacente, como o switch de acesso. A partir daí, as solicitações são tratadas de acordo com a configuração de sua rede.

Pré-requisito:

1. Consulte o guia FlexConnect para garantir que sua configuração esteja alinhada com as instruções e as práticas recomendadas descritas no guia.

2. A VLAN cliente deve estar listada no perfil flex.
3. O AP precisa ser configurado no modo de tronco, com a VLAN de gerenciamento do AP designada como a VLAN nativa, e as VLANs para tráfego de cliente devem ser permitidas no tronco.

Aqui está um exemplo de configuração de porta de switch conectado a AP com VLAN de gerenciamento como 58 e 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
!
```

Configuração em funcionamento: para referência, compartilhar os logs operacionais com o servidor DHCP local quando o AP estiver configurado para o modo flex:

Depurações de clientes 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 uplink AP:

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 uplink AP

Captura do lado do cliente:

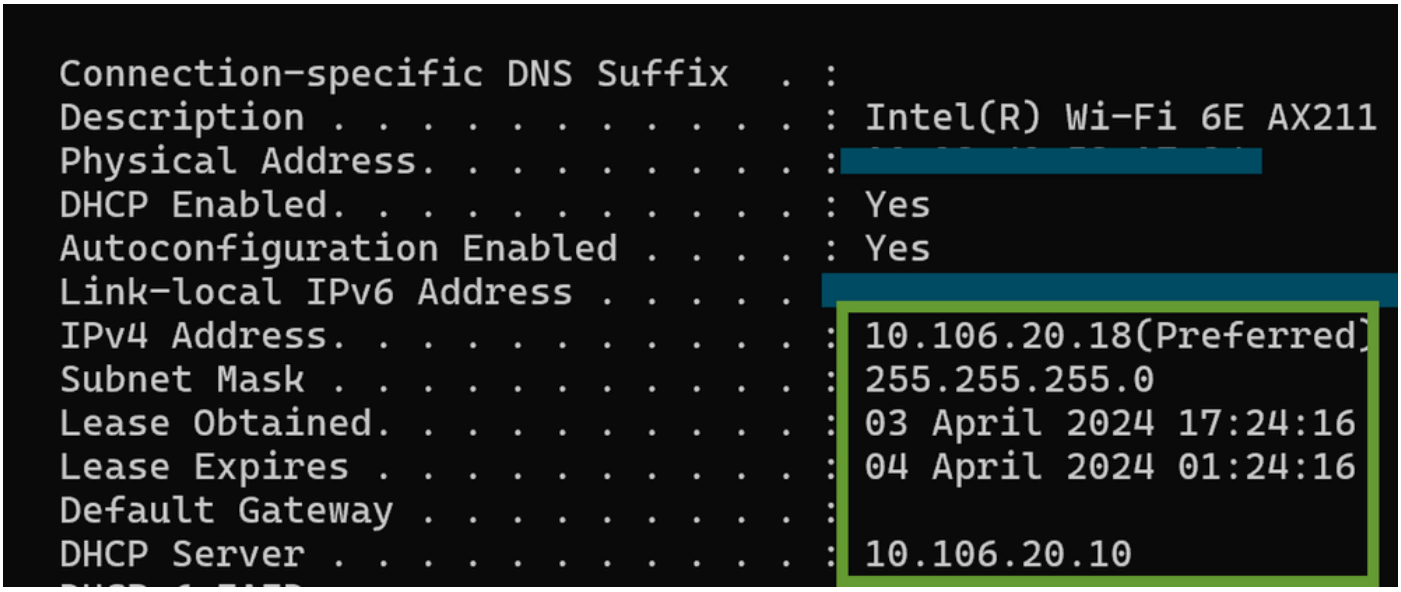
```
16540 111.905836    0.0.0.0           255.255.255.255     DHCP      343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10      10.106.20.18        DHCP      342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0           255.255.255.255     DHCP      385 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 pacote final do cliente

Verificação do IP do cliente sem fio:

Você pode verificar a concessão de IP no servidor DHCP e seu status correspondente.

No cliente sem fio:



Verificação de IP na Extremidade do Cliente

Solução de problemas de DHCP

A solução de problemas de DHCP envolve identificar e resolver problemas que impedem que os clientes obtenham um endereço IP de um servidor DHCP quando conectados à rede sem fio. Aqui estão algumas etapas e considerações comuns ao Troubleshoot problemas de DHCP:

1. Verificar a Configuração do Cliente

- Verifique se o cliente está configurado para obter um endereço IP automaticamente.
- Confirme se o adaptador de rede está ativado e funcionando corretamente.

2. Verifique o status do servidor DHCP

- Confirme se o servidor DHCP está operacional e acessível no segmento de rede do cliente.
- Verifique o endereço IP, a máscara de sub-rede e as configurações de gateway padrão do servidor DHCP.

3. Revisar a Configuração do Escopo

- Inspecione o escopo do DHCP para garantir que ele tenha um intervalo suficiente de endereços IP disponíveis para os clientes.
- Verificar a duração e as opções de concessão do escopo, como servidores DNS e gateway padrão
- Em alguns ambientes (como o Ative Diretory), verifique se o servidor DHCP está autorizado a fornecer serviços DHCP na rede.

4. Revisar a configuração na WLC 9800

- Muitos problemas foram observados devido à configuração incorreta, como a falta de uma interface de loopback, SVI do cliente ou a ausência de um endereço auxiliar configurado. Antes da coleta de logs, é recomendável verificar se a configuração foi implementada corretamente.
- Ao utilizar um servidor DHCP interno: no que se refere ao esgotamento do escopo do DHCP, é importante garantir, particularmente ao configurar o DHCP via CLI, que o temporizador de aluguel esteja configurado de acordo com seus requisitos. Por padrão, o temporizador de locação é definido como infinito na WLC 9800.
- Verifique se o tráfego de VLAN do cliente é permitido na porta de uplink da WLC ao usar um servidor DHCP central. Por outro lado, ao empregar um servidor DHCP local, assegure-se de que a VLAN relevante seja permitida na porta de uplink do AP.

5. Configurações de Firewall e Segurança

- Certifique-se de que os firewalls ou software de segurança não estejam bloqueando o tráfego DHCP (porta 67 para o servidor DHCP e porta 68 para o cliente DHCP).

Coleta de logs

Logs do WLC

1. Habilite term exec prompt timestamp para ter referência de tempo para todos os comandos.

2. Use show tech-support wireless !! para revisar a configuração

2. Você pode verificar o número de clientes, a distribuição do estado do cliente e os clientes excluídos.
show wireless summary !! Número total de APs e clientes
show wireless exclusionlist !! Caso algum cliente seja visto como excluído
show wireless exclusionlist client mac-address MAC@ !! para obter mais detalhes sobre o cliente concreto excluído e verificar se o motivo está listado como roubo de IP para qualquer cliente.

3. Verifique a atribuição de endereço IP para clientes, procure endereços incorretos ou aprendizagem de endereço estático inesperada, VLANs marcadas como sujas devido à ausência de resposta do servidor DHCP ou quedas de pacotes no SISF que está manipulando DHCP/ARP.

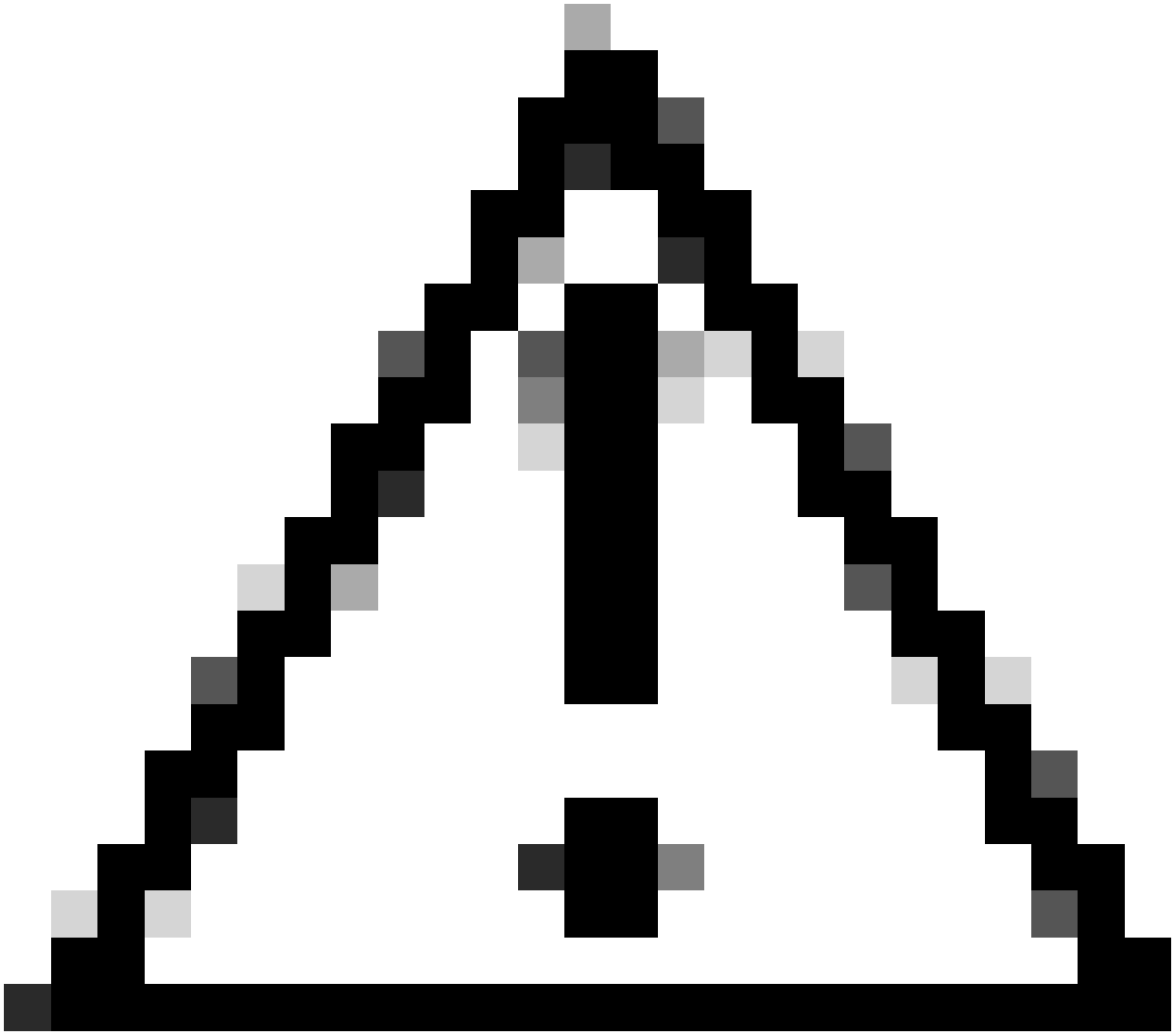
show wireless device-tracking database ip !! Verifique por IP e veja como ocorreu o aprendizado de endereço:
show wireless device-tracking database mac !! Verifique por Mac e veja qual cliente IP está atribuído.
show wireless vlan details !! Verifique se a VLAN não está marcada como suja devido a falhas de DHCP no caso de um grupo de VLANs em uso.
show wireless device-tracking feature drop !!Quedas no SISF

4. Saídas específicas da WLC para MAC@ cliente concreto show wireless device-tracking feature drop

Ative o rastreamento radioativo para o endereço MAC do cliente quando o cliente estiver tentando se conectar à rede sem fio.

Via 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



Cuidado: a depuração condicional habilita o registro em nível de depuração que, por sua vez, aumenta o volume dos logs gerados. Deixar esse item em execução reduz a distância no tempo em que você pode exibir logs. Portanto, é recomendável sempre desabilitar a depuração no final da sessão de solução de problemas.

Para desabilitar toda a depuração, execute estes comandos:

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

Via GUI:

Etapa 1. Navegue até Troubleshooting > Radioactive Trace .
Etapa 2. Clique Add e insira um endereço Mac do cliente para o qual deseja solucionar problemas. Você pode adicionar vários endereços Mac para rastrear.

Etapa 3. Quando estiver pronto para iniciar o rastreamento radioativo, clique em Iniciar. Uma vez iniciado, o registro de depuração é gravado no disco sobre qualquer processamento de plano de controle relacionado aos endereços MAC rastreados.

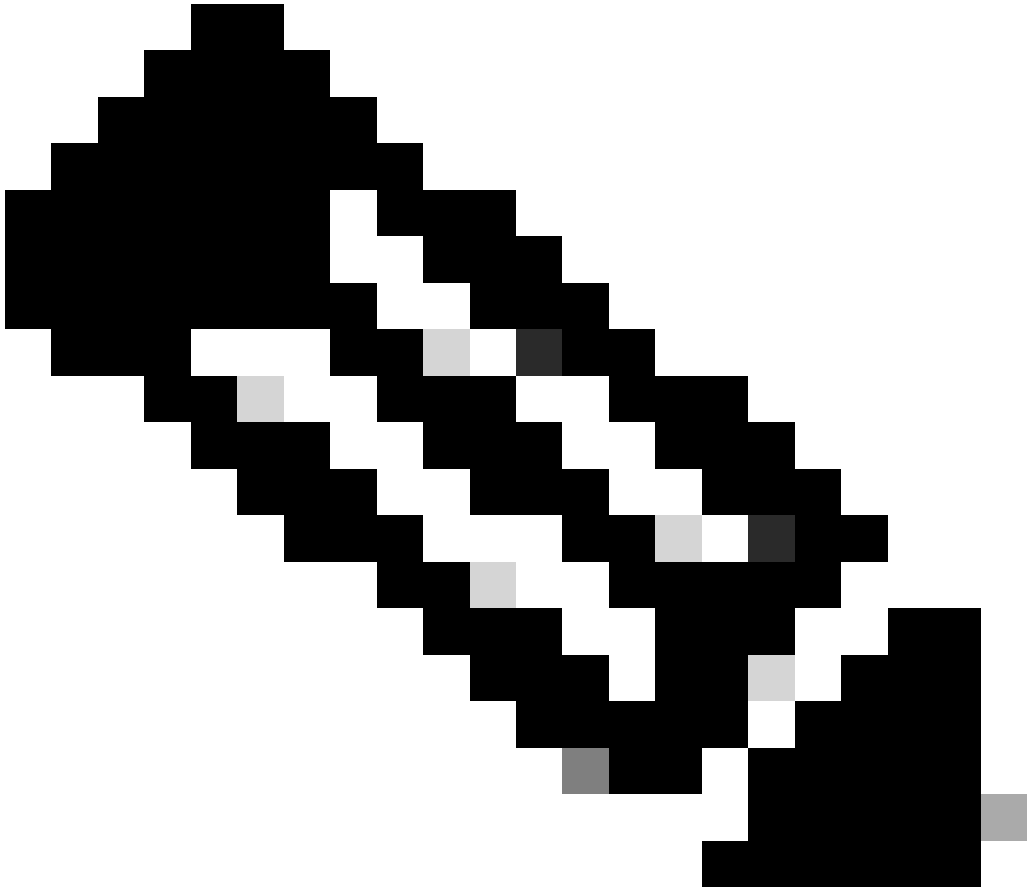
Etapa 4. Quando você reproduzir o problema que deseja solucionar, clique em Stop .

Etapa 5. Para cada endereço mac depurado, você pode gerar um arquivo de log que agrupa todos os logs referentes a esse endereço mac clicando em Generate .

Etapa 6. Escolha quanto tempo você deseja que o arquivo de log agrupado volte e clique em Aplicar ao Dispositivo.

Passo 7. Agora você pode fazer o download do arquivo clicando no pequeno ícone ao lado do nome do arquivo. Esse arquivo está presente na unidade flash de inicialização do controlador e também pode ser copiado fora da caixa através da CLI.

!!Capturas incorporadas filtradas pelo endereço MAC do cliente em ambas as direções, filtro MAC interno do cliente disponível após 17.1.



Observação: o EPC no 9800 será útil quando o DHCP central estiver ativado no 9800 WLC.

Via CLI:

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

Via GUI:
Etapa 1. Navegue até Troubleshooting > Packet Capture > +Add .

Etapa 2. Defina o nome da captura do pacote. É permitido um máximo de 8 caracteres.

Etapa 3. Defina filtros, se houver.

Etapa 4. Marque a caixa para Monitorar o tráfego de controle se quiser ver o tráfego apontado para a CPU do sistema e injetado de volta no plano de dados.

Etapa 5. Definir tamanho do buffer. É permitido um máximo de 100 MB.

Etapa 6. Defina o limite, seja pela duração, que permite um intervalo de 1 a 1000000 segundos, ou pelo número de pacotes, que permite um intervalo de 1 a 100000 pacotes, conforme desejado.

Passo 7. Escolha a interface na lista de interfaces na coluna esquerda e selecione a seta para movê-la para a coluna direita.

Etapa 8. Salvar e aplicar ao dispositivo.

Etapa 9. Para iniciar a captura, selecione Iniciar.

Etapa 10. Você pode permitir que a captura seja executada até o limite definido. Para interromper manualmente a captura, selecione Parar.

Etapa 11. Uma vez interrompido, um botão Exportar fica disponível para clicar com a opção de baixar o arquivo de captura (.pcap) na área de trabalho local via servidor HTTP ou TFTP ou servidor FTP ou disco rígido ou flash do sistema local.

Logs do lado do AP

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

Logs do servidor DHCP

Ao usar um servidor DHCP externo, é necessário coletar logs de depuração e capturas de pacotes no lado do servidor para verificar o fluxo do tráfego DHCP.

Outros Logs

Se você observar que as mensagens de descoberta de DHCP estão visíveis na WLC 9800 em uma configuração de DHCP central ou nos logs de depuração de AP em uma configuração de DHCP local, você deve continuar coletando dados de captura do uplink para confirmar que os pacotes não estão sendo descartados na porta Ethernet.Dependendo dos recursos do switch, você tem a opção de executar uma captura de pacote incorporada ou uma captura de SPAN (Switched Port Analyzer) no switch de uplink. É aconselhável rastrear passo a passo o fluxo de tráfego DHCP para determinar o ponto no qual a comunicação é interrompida, tanto do cliente DHCP para o servidor DHCP quanto na direção inversa.

Problemas conhecidos

Problema 1. O cliente está tentando obter um endereço IP de uma VLAN que reteve anteriormente. Podem surgir situações em que um cliente sem fio alterna entre dois SSIDs associados a VLANs de clientes diferentes. Nesses casos, o cliente pode persistir em solicitar um IP da VLAN à qual estava anteriormente conectado. Como esse IP não estará dentro do escopo DHCP da VLAN atual, o servidor DHCP emitirá um NAK (reconhecimento negativo) e, como resultado, o cliente não poderá adquirir um endereço IP.

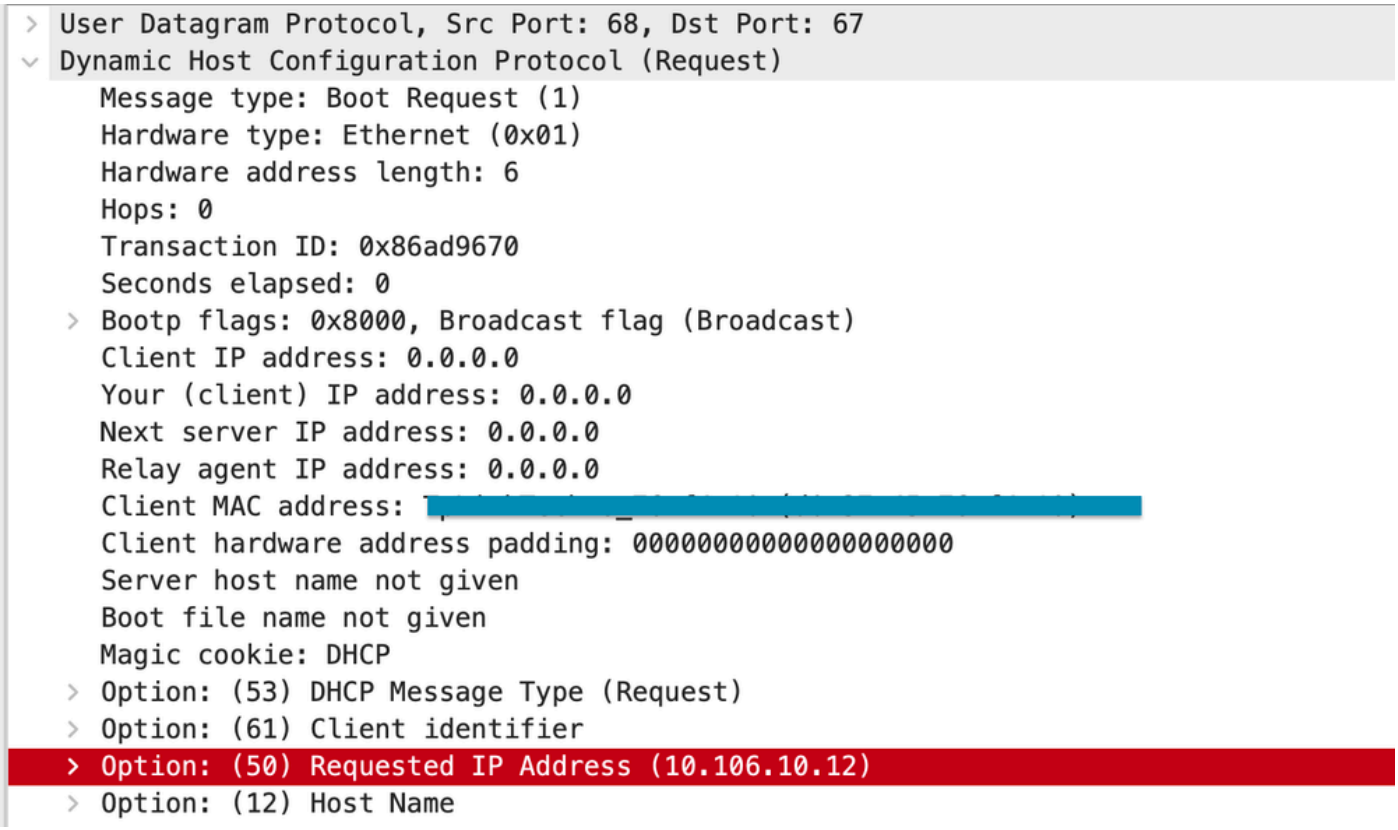
Nos logs de rastreamento radioativo, é evidente que o cliente continua a buscar um IP da VLAN à qual estava anteriormente conectado, que é a VLAN 10, apesar do fato de que a VLAN do cliente para o SSID atual é a VLAN 20.

```
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 pacotes incorporada na WLC:

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

Captura de pacotes incorporada na WLC



Opção de DHCP 50 na captura de pacotes de WLC

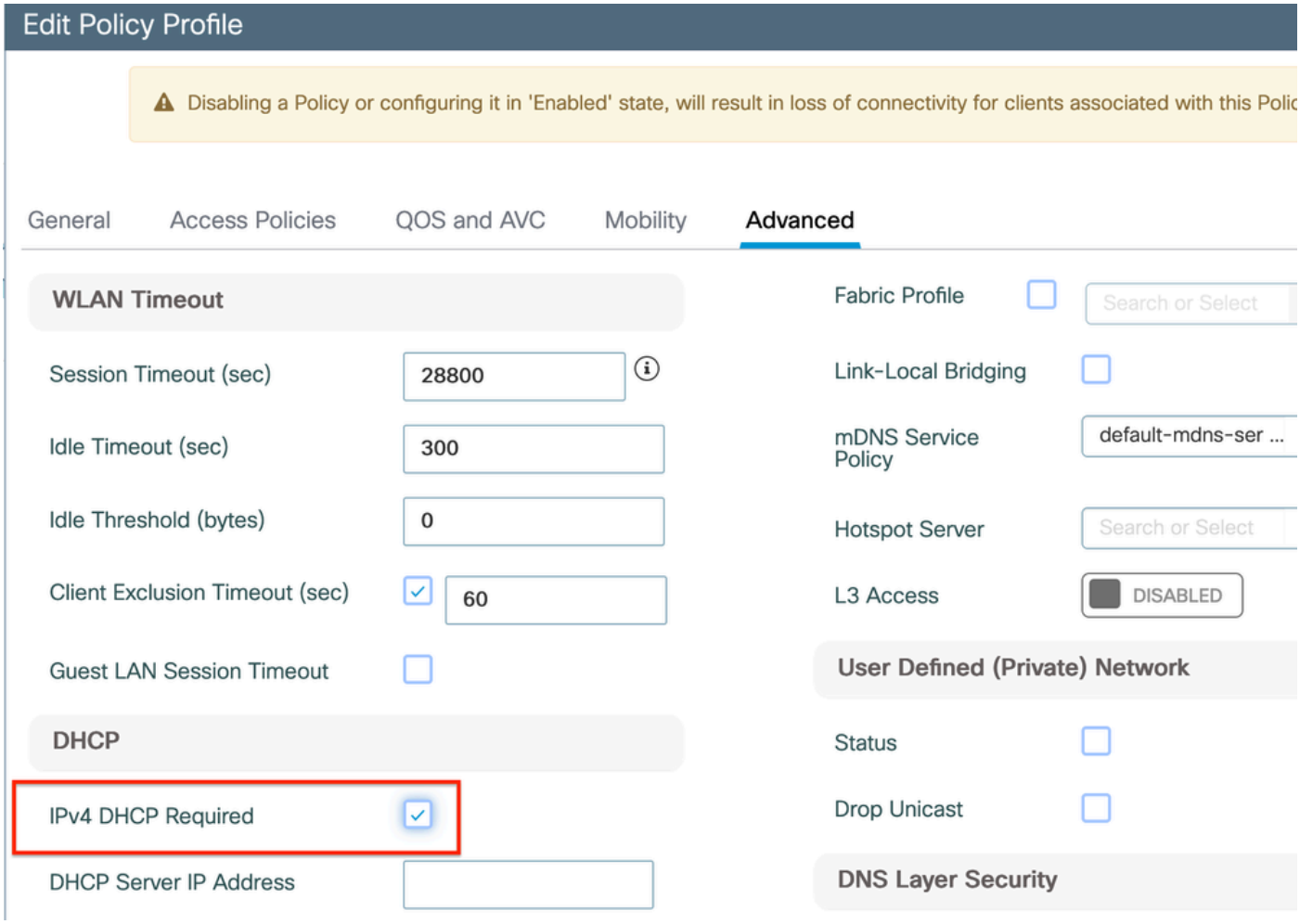
Resolução: para garantir que um cliente conclua o processo DHCP completo, você pode habilitar a opção DHCP IPv4 necessário na configuração de política. Essa configuração deve ser habilitada, especialmente quando o cliente está alternando entre SSIDs, para permitir que o servidor DHCP envie um NAK ao cliente se ele solicitar um endereço IP de uma VLAN associada ao SSID anterior. Caso contrário, o cliente pode continuar a usar ou solicitar o endereço IP que tinha anteriormente, levando a uma comunicação interrompida. Entretanto, lembre-se de que a ativação desse recurso afetará os clientes sem fio configurados com um endereço IP estático.

Aqui está o processo para ativar a opção desejada:

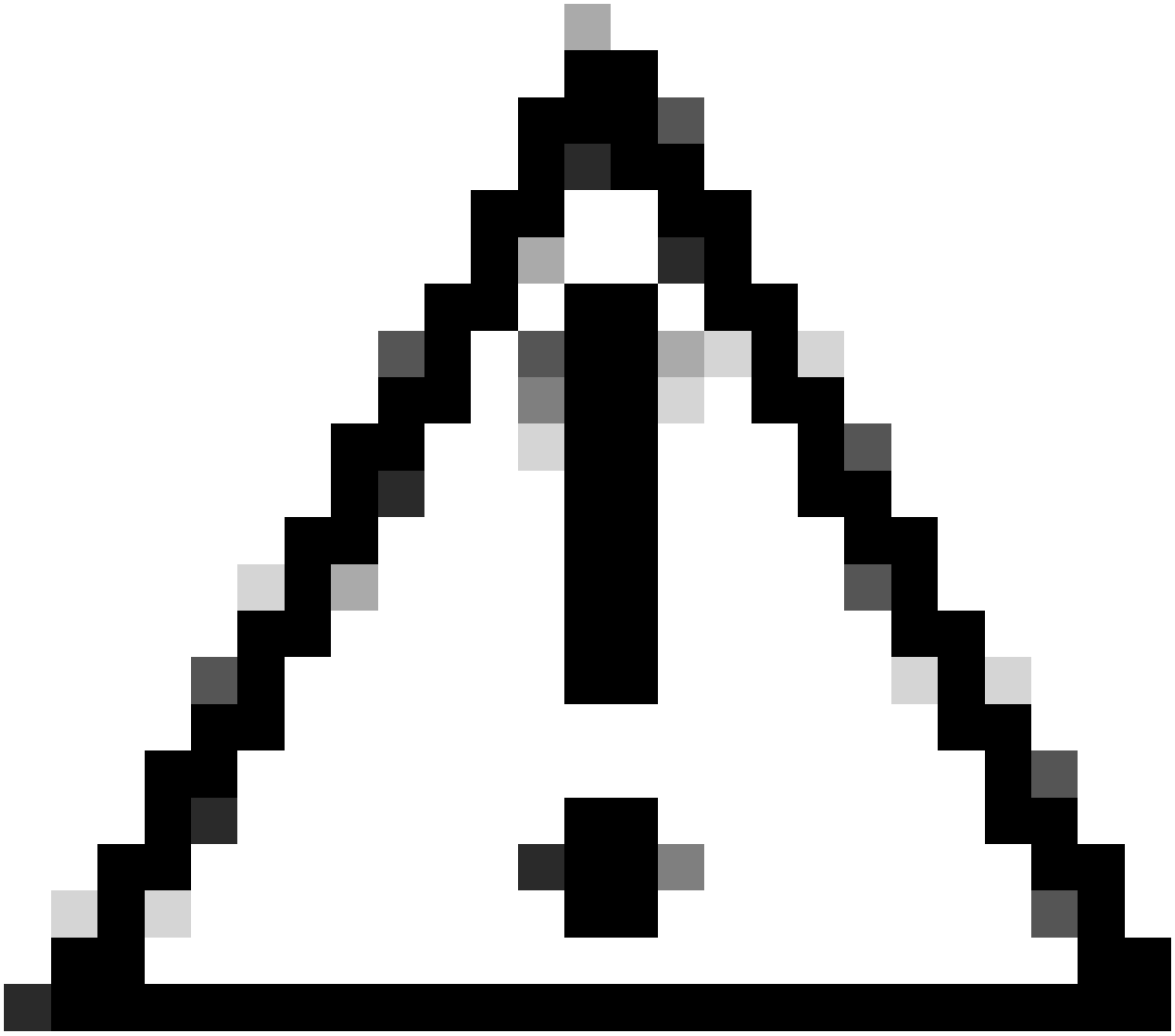
Via CLI:

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

Via GUI: Navegue até Configuration > Tags & Profile > Policy > Policy_name > Advanced. Na seção DHCP, habilite ipv4 DHCP obrigatório.



Configuração do perfil de política no WLC



Cuidado: para uma configuração de âncora externa, é importante alinhar as configurações DHCP em ambas as WLCs. Se você tiver o DHCP IPV4 obrigatório habilitado, ele precisará ser habilitado nas WLCs externa e âncora. Uma discrepância na configuração relacionada ao DHCP sob o perfil de política entre os dois pode fazer com que os clientes tenham problemas com suas funções de mobilidade.

Problema 2: O cliente está sendo excluído ou excluído devido ao problema de roubo de IP. O roubo de IP, no contexto da rede, refere-se a uma situação em que mais de um cliente sem fio está tentando usar o mesmo endereço IP. Pode ser devido a muitas razões que estão listadas abaixo:

1. Atribuição de IP Estático Não Autorizado: Quando um usuário define um endereço IP estático no dispositivo que coincide com um IP já atribuído ou atribuído na rede, isso pode resultar em um conflito de IP. Isso ocorre quando dois dispositivos tentam operar com um endereço IP idêntico, o que pode interromper as conexões de rede para um ou ambos os dispositivos envolvidos. Para evitar esses problemas, é essencial garantir que cada cliente na rede esteja configurado com um endereço IP exclusivo.

2. Servidor DHCP não autorizado: a presença de um servidor DHCP não autorizado ou não autorizado na rede pode levar à alocação de endereço IP que conflita com o plano de endereçamento IP estabelecido para a rede. Esses conflitos podem fazer com que vários dispositivos sofram

colisões de endereços IP ou obtenham configurações de rede incorretas. Para resolver esse problema, devem ser feitos esforços para identificar e eliminar o servidor DHCP invasor da rede para evitar mais conflitos de IP dentro da mesma sub-rede.

3. Entrada obsoleta de cliente no 9800 WLC: às vezes, o controlador pode reter entradas desatualizadas/obsoletas de um endereço IP que um cliente está tentando adquirir. Nesses casos, é necessário remover manualmente essas entradas obsoletas da WLC 9800. Veja como:

- Execute o rastreamento radioativo para o endereço mac que está na lista de exclusão e filtre-o com mac legítimo no rastreamento radioativo.

- Você poderá ver os logs de erros: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: MAC do cliente: Affected_Client_MAC com IP: 10.37.57.24 foi adicionado à lista de exclusão, MAC do cliente legítimo: Legit_Client_MAC, IP: 10.37.57.24, motivo: roubo de endereço IP

- Em seguida, execute estes comandos:
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(Se houver entradas obsoletas, você poderá ver mais de um IP para um endereço Mac cliente legítimo: um é o IP original, enquanto o outro é o desatualizado/obsoleto].

Resolução: Exclua manualmente as entradas obsoletas da WLC 9800 usando clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. Na implantação flexível com o servidor DHCP local usando a mesma sub-rede: nas configurações do FlexConnect, é comum que vários locais remotos utilizem um servidor DHCP local que atribua endereços IP de uma sub-rede idêntica. Esse cenário pode fazer com que clientes sem fio em locais diferentes recebam o mesmo endereço IP. Os controladores dentro dessa estrutura de rede são programados para detectar quando várias conexões de clientes estão usando um endereço IP idêntico, interpretando isso como um possível roubo de IP. Como resultado, esses clientes são geralmente colocados em uma lista bloqueada para evitar conflitos de endereço IP.

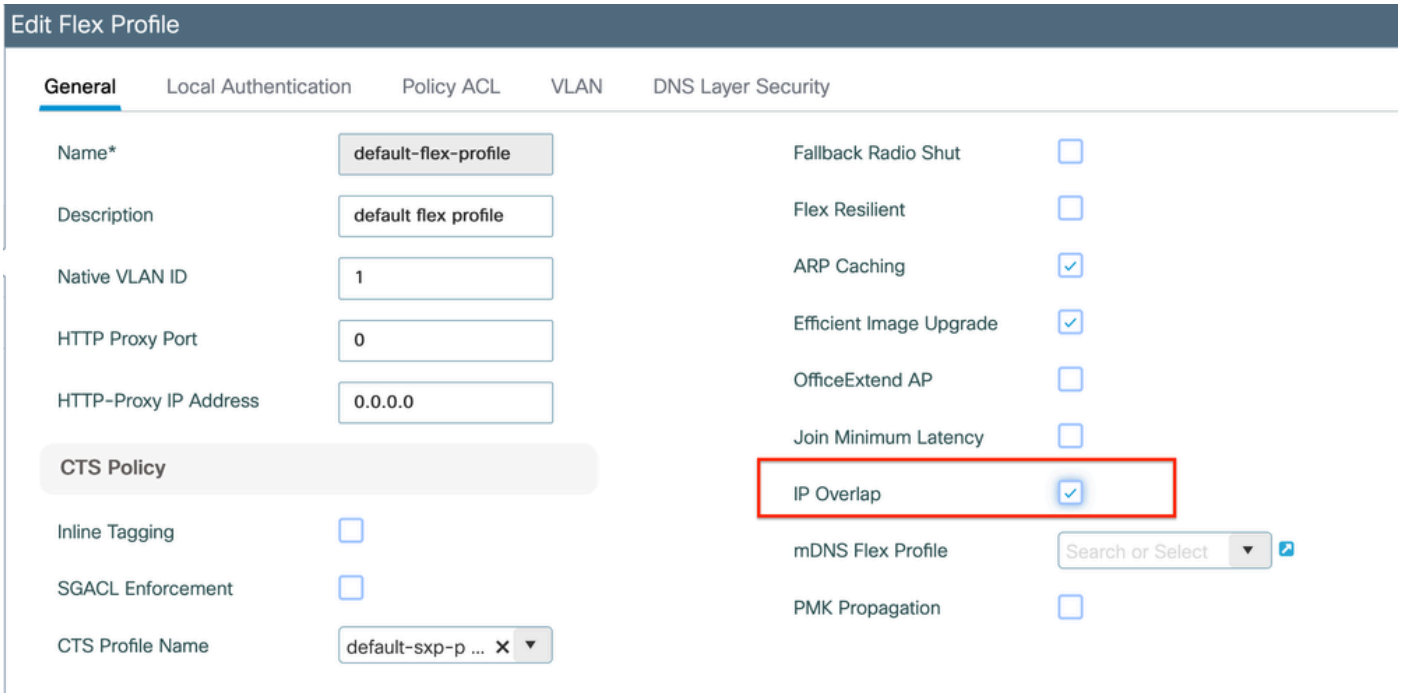
Resolução: ative o recurso de sobreposição de IP no seu perfil do FlexConnect. A funcionalidade "Sobreposição de endereço IP do cliente na implantação Flex" permite o uso dos mesmos endereços IP em vários sites FlexConnect, mantendo todos os recursos e capacidades suportados nas implantações FlexConnect.

Por padrão, esse recurso está desativado. Você pode ativá-lo através deste procedimento:

Via CLI:

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

Via GUI: Selecione Configuration > Tags & Profiles > Flex. Click on Existing Flex Profile/Add to new Flex profile e, na guia General, ative IP Overlap.



Configuração do perfil Flex no WLC

Problema 3. Os clientes sem fio não estão recebendo um endereço IP da VLAN desejada. Esse problema ocorre frequentemente quando a VLAN 1 é utilizada ou quando a VLAN atribuída aos clientes é a mesma que a VLAN usada para o gerenciamento de AP em uma implantação FlexConnect. A causa raiz desse problema geralmente são atribuições de VLAN incorretas. Para fornecer orientação, aqui estão alguns cenários a serem considerados ao configurar IDs de VLAN na série 9800:

1. Ao empregar um servidor AAA com o recurso de substituição AAA ativado, é crucial garantir que o ID de VLAN apropriado esteja sendo enviado do servidor AAA. Se um nome de VLAN for fornecido, confirme se ele corresponde ao nome de VLAN configurado na WLC 9800.

2. Quando a VLAN 1 é configurada para tráfego de cliente sem fio, o comportamento pode variar com base no modo do ponto de acesso (AP):

Para um AP no modo local/switching central:

- Especificando VLAN-name = default, o cliente é atribuído à VLAN 1
- Usando VLAN-ID 1, um cliente é atribuído à VLAN de gerenciamento sem fio

Para um AP no modo Flex/switching local:

- Especificando VLAN-name = default, o cliente é atribuído à VLAN 1
- Usando VLAN-ID 1, um cliente é atribuído à VLAN nativa FlexConnect

Aqui estão mais alguns exemplos de cenários que foram experimentados no laboratório, junto com seus resultados:

1. Por padrão, se o usuário não configurar nada no perfil de política, a WLC atribuirá VLAN-ID 1 para que os clientes usem a VLAN de gerenciamento sem fio no modo local e a VLAN nativa de AP para FlexConnect.

2. Se a VLAN Nativa sob flex-profile estiver configurada com uma ID de VLAN nativa diferente da configurada no switch, você verá o problema, o cliente obterá o IP da VLAN de gerenciamento (VLAN nativa) mesmo que o perfil de política esteja configurado com o nome de VLAN "padrão".

3. Se a VLAN Nativa sob flex-profile estiver configurada com VLAN-ID igual à VLAN nativa configurada no switch, somente o cliente poderá obter um IP da VLAN 1 com o padrão configurado no perfil de política.

4. Se você selecionou um nome de VLAN em vez de uma ID de VLAN, verifique se o nome de VLAN no perfil Flex é o mesmo.

Informações Relacionadas

- Servidor DHCP interno no 9800
- Servidor DHCP externo em uso
- DHCP opção 82 Subopção 5 no servidor DHCP do Windows
- NAT-PAT em AP flexível
- A VLAN 1 é usada para o cliente sem fio
- Suporte técnico e downloads da Cisco

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

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

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