# Résolution des problèmes de connectivité du client DHCP sur un WLC Cisco 9800

## Table des matières



## Introduction

Ce document décrit divers problèmes liés au protocole DHCP (Dynamic Host Configuration Protocol) rencontrés par les clients sans fil lorsqu'ils sont connectés à un contrôleur LAN sans fil (WLC) Cisco 9800 et explique comment les résoudre.

## Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du contrôleur Cisco WLC 9800
- Connaissances de base du flux DHCP

- Connaissance de base du point d’accès en mode de connexion local et flexible

## Présentation du flux du trafic DHCP avec les clients sans fil

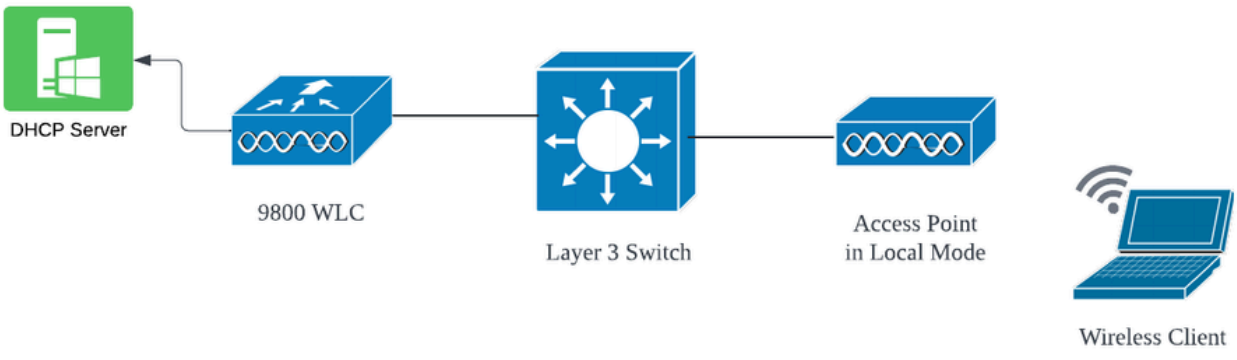
Lorsque le client sans fil se connecte, il effectue l'échange DHCP habituel en envoyant une trame de découverte DHCP de diffusion pour trouver un serveur DHCP au point d'accès associé. Selon le mode de fonctionnement de l'AP, il transmettra la requête au WLC via le tunnel CAPWAP ou la passera directement au saut suivant. Si un serveur DHCP est disponible dans le domaine local de couche 2, il répond, facilitant ainsi une connexion réussie. En l'absence d'un serveur DHCP de sous-réseau local, le routeur (configuré avec l'interface SVI du client) doit être configuré pour acheminer la détection DHCP vers le serveur approprié. Pour ce faire, il configure généralement une adresse IP d’assistance sur le routeur, qui lui indique de transférer un trafic UDP de diffusion spécifique (comme les requêtes DHCP) vers une adresse IP prédéterminée.

Le comportement du trafic DHCP client dépend entièrement du mode dans lequel votre point d'accès (AP) fonctionne. Examinons chacun de ces scénarios séparément :

## Scénario 1. Le point d'accès fonctionne en mode local

Lorsqu'un AP est configuré en mode local, le trafic DHCP client est commuté de manière centralisée, ce qui signifie que les requêtes DHCP des clients sont envoyées via un tunnel CAPWAP de l'AP au WLC, où elles sont ensuite traitées et transmises en conséquence. Dans ce cas, vous avez deux choix : vous pouvez utiliser un serveur DHCP interne ou opter pour un serveur DHCP externe.

### Topologie (point d'accès en mode local)




*Topologie du réseau : point d'accès en mode local*

## Étude de cas 1. Lorsque le WLC est configuré en tant que serveur DHCP interne

Le contrôleur est capable de proposer un serveur DHCP interne grâce aux fonctionnalités intégrées du logiciel Cisco IOS XE. Cependant, il est recommandé d'utiliser un serveur DHCP externe. Avant de configurer le WLC en tant que serveur DHCP interne, plusieurs conditions préalables doivent être remplies, notamment :

- Assurez-vous de configurer une interface virtuelle commutée (SVI) pour le VLAN client et attribuez-lui l'adresse IP du serveur DHCP.
- L'adresse IP du serveur DHCP interne doit être définie sur l'interface orientée serveur, qui peut être une interface de bouclage, une interface SVI ou une interface physique de couche 3.
- Il est recommandé de configurer l’interface de bouclage car, contrairement aux interfaces physiques qui se connectent à des segments de réseau réels, l’interface de bouclage n’est pas liée au matériel et ne correspond pas à un port physique sur le périphérique. L’objectif principal d’une interface de bouclage est de fournir une interface stable, toujours active, qui n’est pas sujette à des pannes matérielles ou à des déconnexions physiques.

Fonctionnement de la configuration : voici un exemple de configuration de serveur DHCP interne dans lequel les clients ont reçu des adresses IP. Voici les journaux d'exploitation et les détails de configuration associés.

Configurez le WLC en tant que serveur DHCP pour VLAN 10, avec une étendue DHCP allant de 10.106.10.11/24 à 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 bouclage configurée sur le WLC :

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

VLAN client configuré comme SVI [interface L3] avec l'adresse d'assistance comme interface de bouclage sur le 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
```

Vous pouvez également définir l'adresse IP du serveur DHCP dans le profil de stratégie, plutôt que de configurer une adresse d'assistance sous l'interface SVI. Cependant, il est généralement conseillé de configurer cette option pour chaque VLAN afin d'appliquer les meilleures pratiques :

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

Radioactive Traces sur 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
```

Captures de paquets intégrées sur 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 |

*Capture de paquets intégrée sur WLC*

Débogages du client 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>
```

Capture de paquets côté client :

```
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
```

*Capture de paquets client final*

Dans les journaux d'exploitation fournis, vous pouvez voir que le WLC reçoit le message DHCP Discover du client sans fil, et que le VLAN du client le relaie à l'adresse d'assistance (qui dans l'exemple fourni est l'interface de bouclage interne). Ensuite, le serveur interne émet une offre DHCP, puis le client envoie une requête DHCP, qui est ensuite confirmée par le serveur avec un accusé de réception DHCP.

Vérification de l'adresse IP du client sans fil :

Sur 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
```

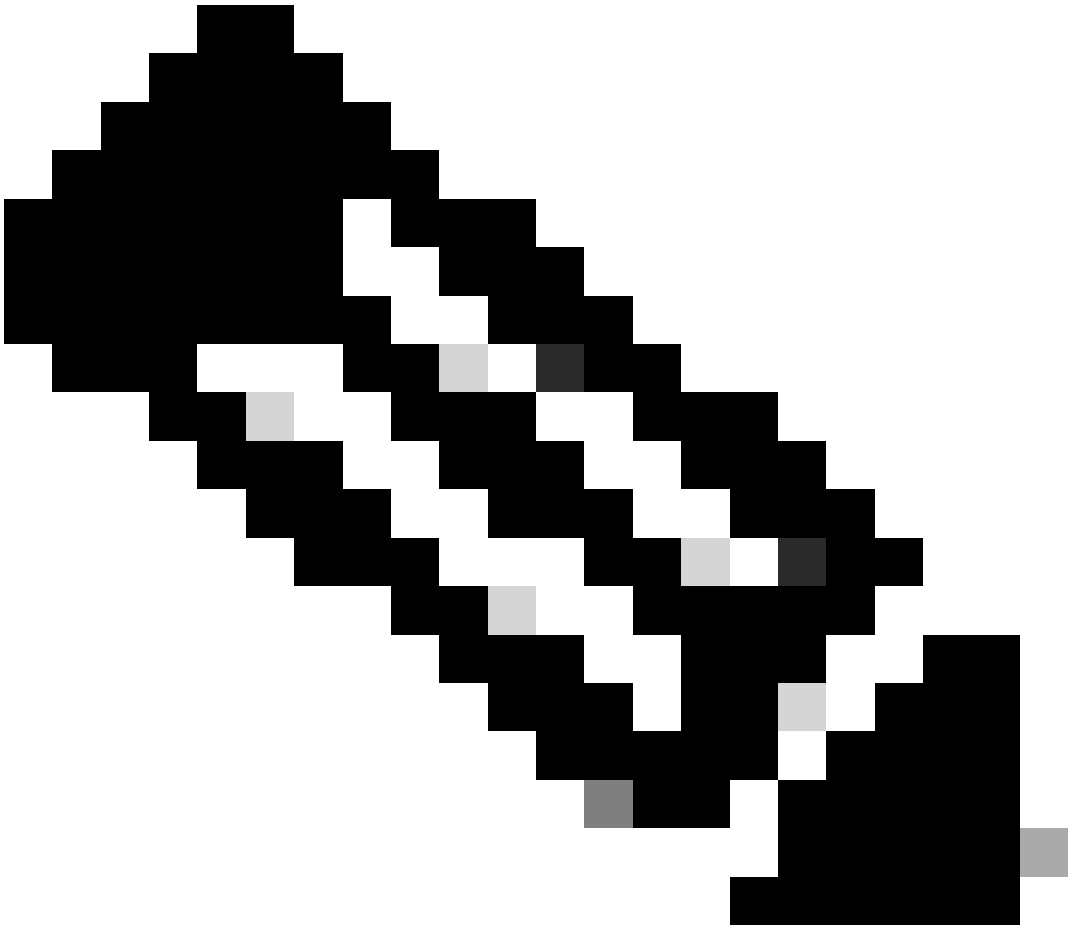
Sur le client sans fil :

```
Wireless LAN adapter Wi-Fi:

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

*Vérification IP côté client*

---



Remarque :

1. VRF n'est pas pris en charge dans les serveurs DHCP internes.
2. DHCPv6 n'est pas pris en charge dans les serveurs DHCP internes.

---

3. Sur C9800, l'interface SVI permet de configurer plusieurs adresses d'assistance, mais seules les 2 premières sont utilisées.
4. Cette fonctionnalité a été testée et est donc prise en charge sur toutes les plates-formes pour un maximum de 20 % de l'échelle client maximale du boîtier. Par exemple, pour un 9800-80 qui prend en charge 64 000 clients, le nombre maximal de liaisons DHCP prises en charge est d'environ 14 000.

## Étude de cas 2. Lorsqu'un serveur DHCP externe est utilisé

Un serveur DHCP externe fait référence à un serveur DHCP qui n'est pas intégré dans le WLC lui-même, mais configuré sur un périphérique réseau différent [pare-feu, routeurs] ou une entité distincte au sein de l'infrastructure réseau. Ce serveur est dédié à la gestion de la distribution dynamique des adresses IP et autres paramètres de configuration réseau aux clients du réseau.

Lors de l'utilisation d'un serveur DHCP externe, la fonction du WLC est uniquement de recevoir et de relayer le trafic. La façon dont le trafic DHCP est routé à partir du WLC, qu'il s'agisse de diffusion ou de monodiffusion, varie selon votre préférence. Examinons chacune de ces méthodes séparément.

Diffusion du trafic DHCP sur le domaine de couche 2

Dans cette configuration, un autre périphérique réseau, tel qu'un pare-feu, une liaison ascendante ou un commutateur principal, agit en tant qu'agent de relais. Quand un client diffuse une requête de détection DHCP, la seule tâche du WLC est de transférer cette diffusion via l'interface de couche 2. Pour que cela fonctionne correctement, vous devez vous assurer que l'interface de couche 2 du VLAN client est configurée correctement et autorisée via le port de données du WLC et le périphérique de liaison ascendante.

Configuration souhaitée sur l'extrémité WLC pour le VLAN client 20 pour cette instance :

VLAN de couche 2 configuré sur WLC :

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

Port de données configuré sur le WLC pour autoriser le trafic du VLAN client :

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

```
negotiation auto
end
```

Traces radioactives sur le 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
```

Capture de paquets intégrée sur le 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
```

*Capture de paquets intégrée sur WLC*

Débogages du client 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>
```

Capture côté client :

```
     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
```

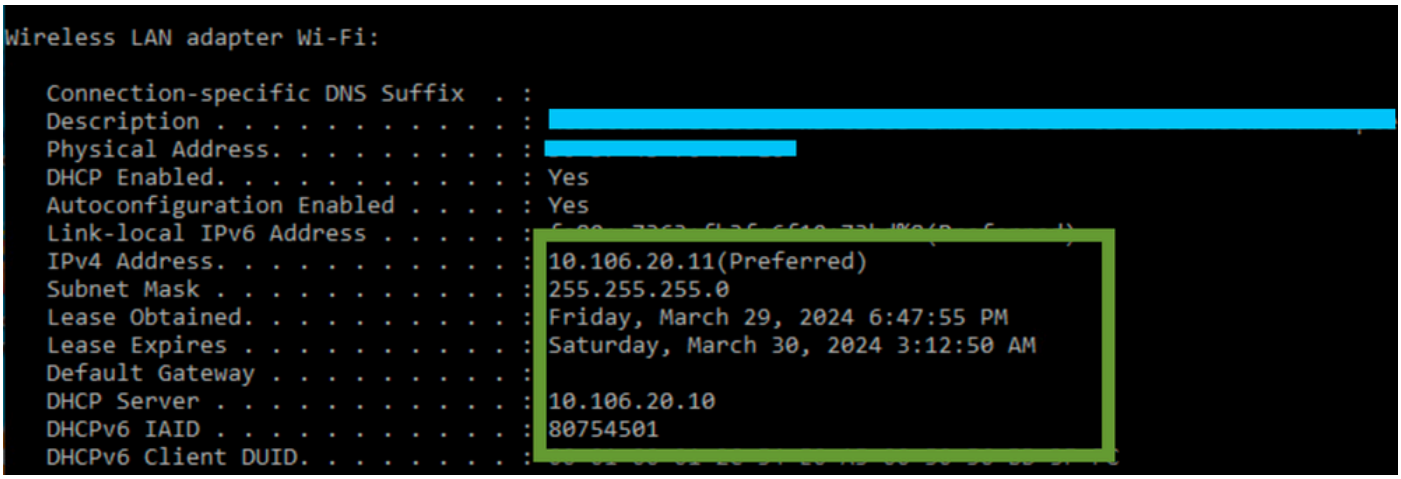
*Capture de paquets client final*

Dans les journaux d'exploitation fournis, vous remarquez dans les journaux que le WLC intercepte la diffusion de détection DHCP à partir du client sans fil, puis la diffuse vers le tronçon suivant via son interface L2. Dès que le WLC reçoit l'offre DHCP du serveur, il transfère ce message au client, suivi de la requête DHCP et de l'ACK.

Vérification de l'adresse IP du client sans fil :

Vous pouvez vérifier le bail IP sur le serveur DHCP et son état correspondant.

Sur le client sans fil :




*Vérification IP côté client*

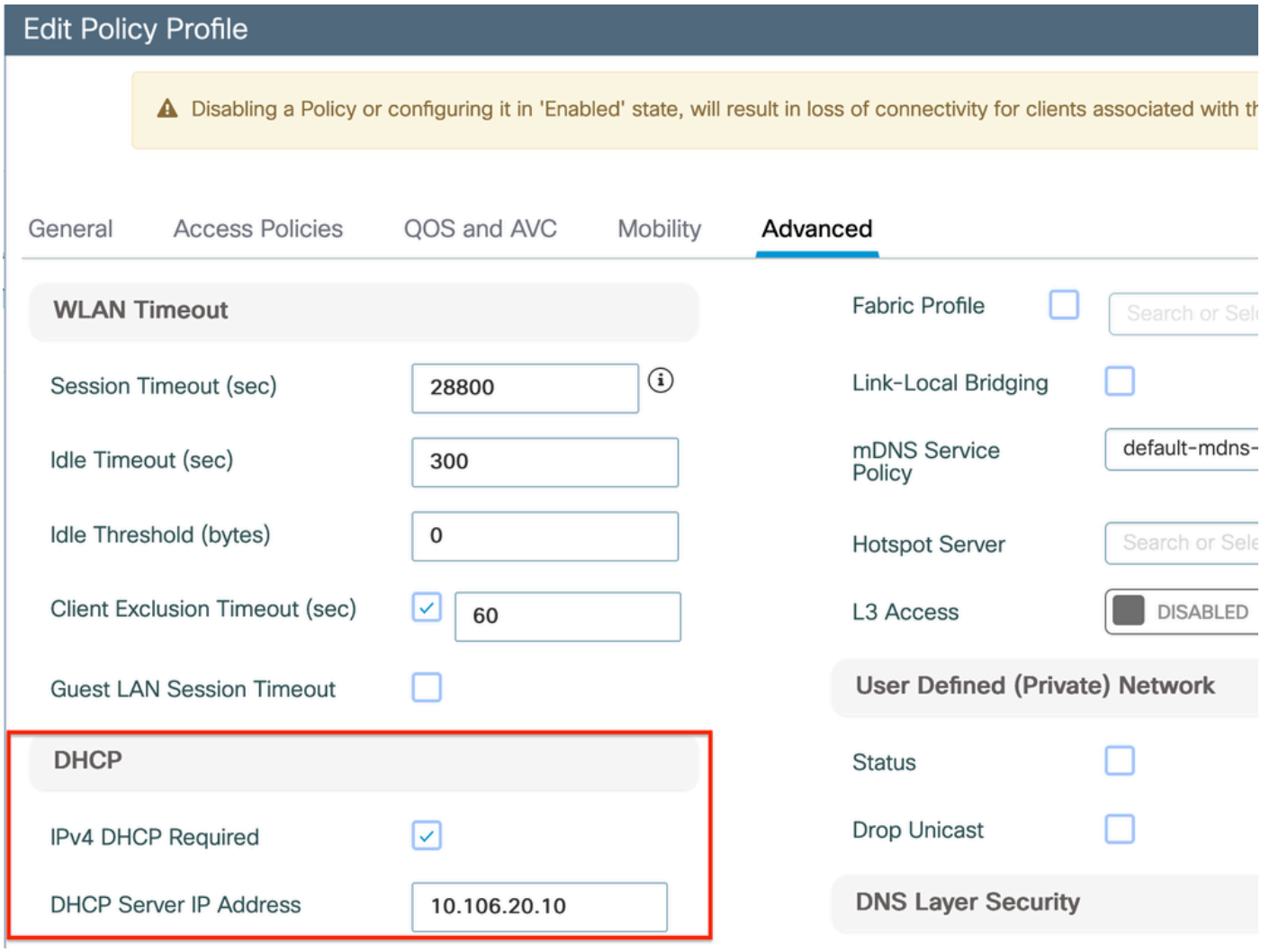
9800 WLC sert d'agent de relais

Dans cette configuration, le WLC transfère directement les paquets DHCP qu'il reçoit des clients sans fil au serveur DHCP par monodiffusion. Pour l'activer, assurez-vous que l'interface SVI VLAN du client est configurée sur le WLC.

Il y a 2 façons de configurer l'IP du serveur DHCP dans le WLC 9800 :

1. Configurez l'adresse IP du serveur DHCP sous le profil de stratégie sous le paramètre avancé.

Via l'interface GUI : accédez à Configuration > Tags & Profile > Policy > Policy_name > Advanced. Dans la section DHCP, vous pouvez configurer l'adresse IP du serveur DHCP comme indiqué :




*Paramètre de profil de stratégie sur WLC*

Via CLI :

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

2. Dans la configuration SVI, vous devez spécifier l'adresse de l'assistant. Il est possible de configurer plusieurs serveurs DHCP dans la configuration d'adresse d'assistance pour assurer la redondance. Bien qu'il soit possible de définir l'adresse du serveur DHCP pour chaque réseau local sans fil dans le profil de stratégie, l'approche recommandée consiste à la configurer par interface. Pour ce faire, attribuez une adresse d'assistance à l'interface SVI correspondante.

Lors de l'utilisation de la fonctionnalité de relais, la source du trafic DHCP sera l'adresse IP de l'interface virtuelle commutée (SVI) du client. Ce trafic est ensuite acheminé via l'interface qui correspond à la destination (l'adresse IP du serveur DHCP), comme déterminé par la table de routage.

Voici un exemple de la configuration de travail du 9800 servant d'agent de relais :

Interface de couche 3 configurée pour le VLAN client sur le WLC avec l'adresse d'assistance :

```
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
```

Port de données configuré sur le WLC pour autoriser le trafic du VLAN client :

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

Traces RA du WLC :

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

Capture de paquets intégrée sur 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 |

*Capture de paquets intégrée sur WLC*

Dans les traçages radioactifs (RA) et la capture de paquets intégrée (EPC) sur le WLC, vous remarquerez que le WLC, agissant en tant qu'agent de relais, effectue une monodiffusion directe des paquets DHCP du client vers le serveur DHCP.

Débogages du client 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>
```

Capture côté client :

| 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 |

*Capture de paquets client final*

Vérification de l'adresse IP du client sans fil :

Vous pouvez vérifier le bail IP sur le serveur DHCP et son état correspondant.

Sur le client sans fil :

```
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
```

*Vérification IP côté client*

**DHCP Option 80 avec sous-option 5/150 dans WLC 9800**

Dans certains scénarios, vous pouvez définir explicitement l'interface source pour le trafic DHCP plutôt que de dépendre de la table de routage, afin d'éviter des complications potentielles sur le réseau. Ceci est particulièrement pertinent lorsque le périphérique réseau suivant sur le chemin, tel qu'un commutateur de couche 3 ou un pare-feu, utilise des contrôles RPF (Reverse Path Forwarding). Prenons, par exemple, une situation où l'interface de gestion sans fil est définie sur le VLAN 50, alors que l'interface SVI du client est sur le VLAN 20 et est utilisée comme relais DHCP pour le trafic du client. La route par défaut est dirigée vers la passerelle du sous-réseau/VLAN de gestion sans fil.

À partir de la version 17.03.03 sur le WLC 9800, il est possible de choisir l'interface source pour le trafic DHCP comme VLAN client ou un autre VLAN, tel que l'interface de gestion sans fil (WMI), qui garantit la connectivité au serveur DHCP.

Voici un extrait de la configuration :

```
!
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
```

Dans ce scénario, le trafic vers le serveur DHCP 10.100.17.14 proviendra du VLAN 50 (10.100.16.10), car l'interface de sortie du paquet est sélectionnée en fonction d'une recherche dans la table de routage IP et, en général, il s'arrête via le VLAN WMI (Wireless Management Interface) en raison de la route par défaut configurée.
Cependant, si un commutateur de liaison ascendante implémente des contrôles RPF (Reverse Path Forwarding), il peut rejeter un paquet arrivant du VLAN 50 mais avec une adresse IP source appartenant à un sous-réseau différent [VLAN 20].

Pour éviter cela, vous devez définir une interface source précise pour les paquets DHCP à l'aide de la commande IP DHCP relay source-interface. Dans ce cas particulier, vous souhaiteriez que les paquets DHCP proviennent de l'interface WMI sur le 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
```

Lors de l'utilisation de cette ip dhcp relay source-interface commande, l'interface source des paquets DHCP et le GIADDR sont définis sur l'interface spécifiée dans la commande de relais DHCP (VLAN50, dans ce cas). Il s’agit d’un problème, car il ne s’agit pas du VLAN client auquel vous souhaitez attribuer des adresses DHCP.

Comment le serveur DHCP sait-il attribuer l'adresse IP à partir du pool de clients approprié ?

La réponse à cette question est que lorsque ip dhcp relay source-interface la commande est utilisée, C9800 ajoute automatiquement les informations de sous-réseau client dans une sous-option propriétaire 150 de l'option 82 appelée sélection de lien, comme vous pouvez le voir à partir de la capture :

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

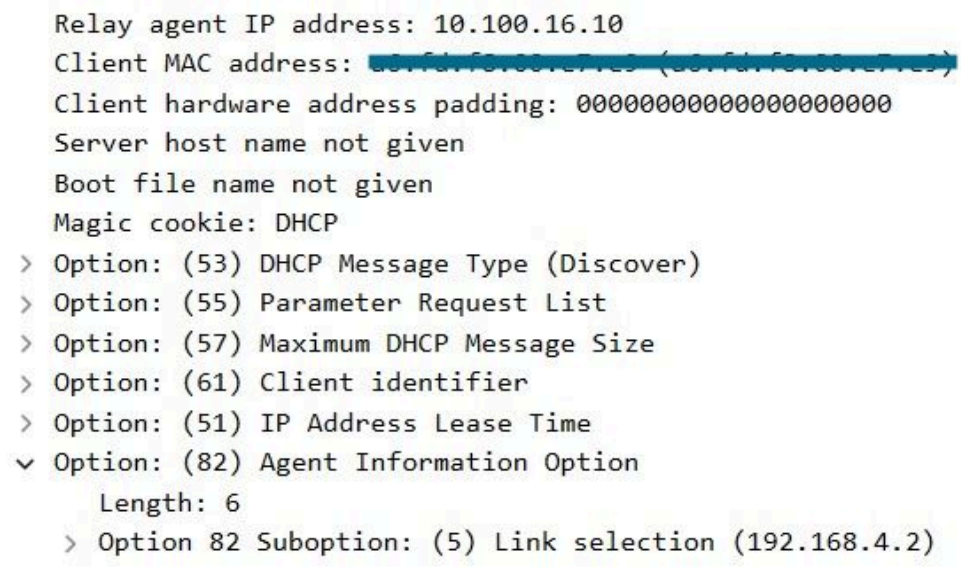
*Option 182 sous-option 150 sur la capture de paquets WLC*

Par défaut, il ajoute la sous-option 150 (propriétaire de cisco). Assurez-vous que le serveur DHCP utilisé peut interpréter et agir sur ces informations. Il est recommandé de modifier la configuration du C9800 pour utiliser l'option standard 82, sous-option 5, afin d'envoyer les informations de sélection de liaison. Pour ce faire, vous pouvez configurer la commande globale suivante :

<#root>

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

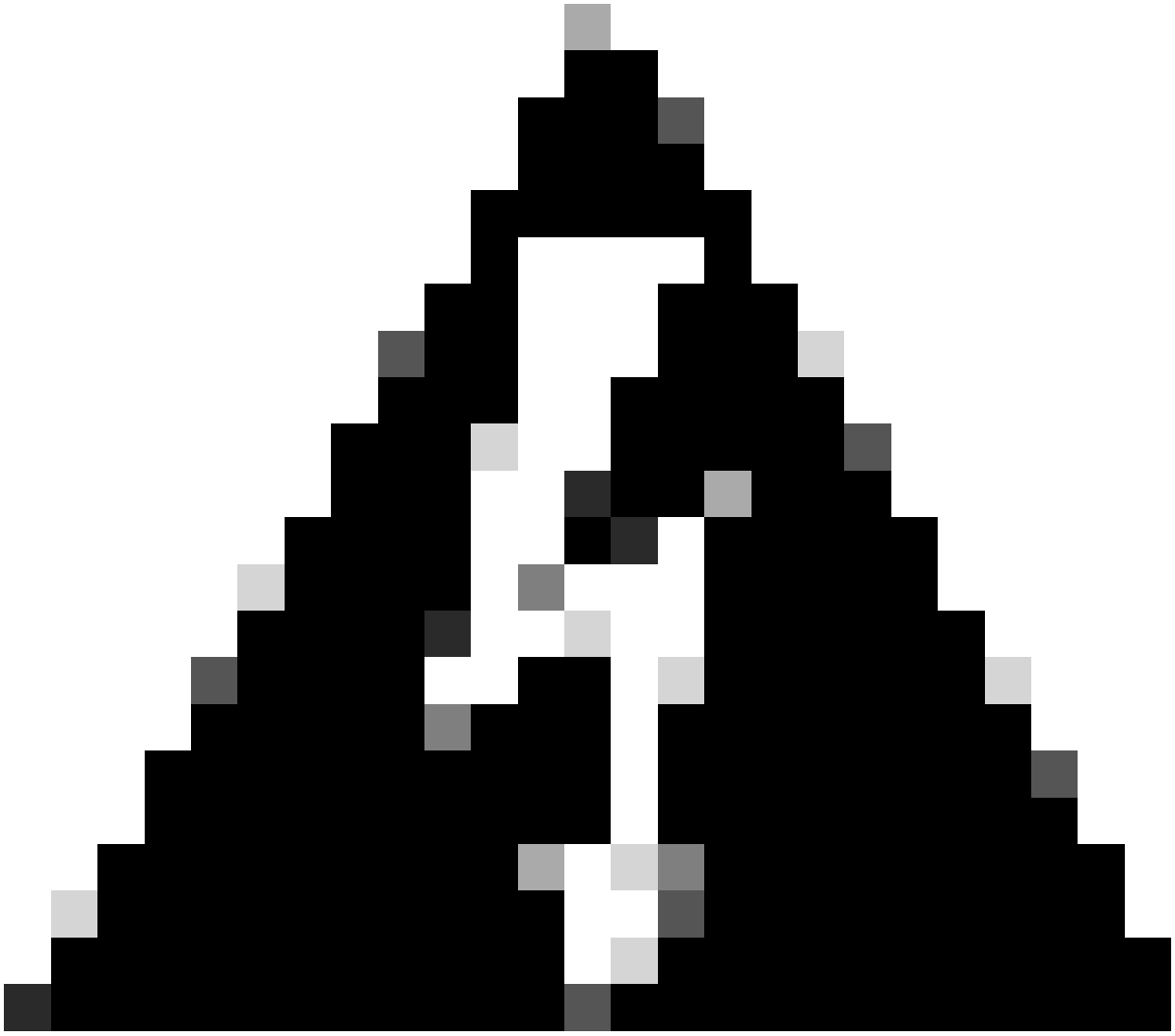
Une fois la commande spécifiée appliquée, le système remplace la sous-option 150 par la sous-option 5 dans les paquets DHCP. La sous-option 5 est plus largement reconnue par les périphériques réseau, ce qui garantit que les paquets sont moins susceptibles d'être abandonnés. L'application de ce changement est également évidente dans la capture fournie :



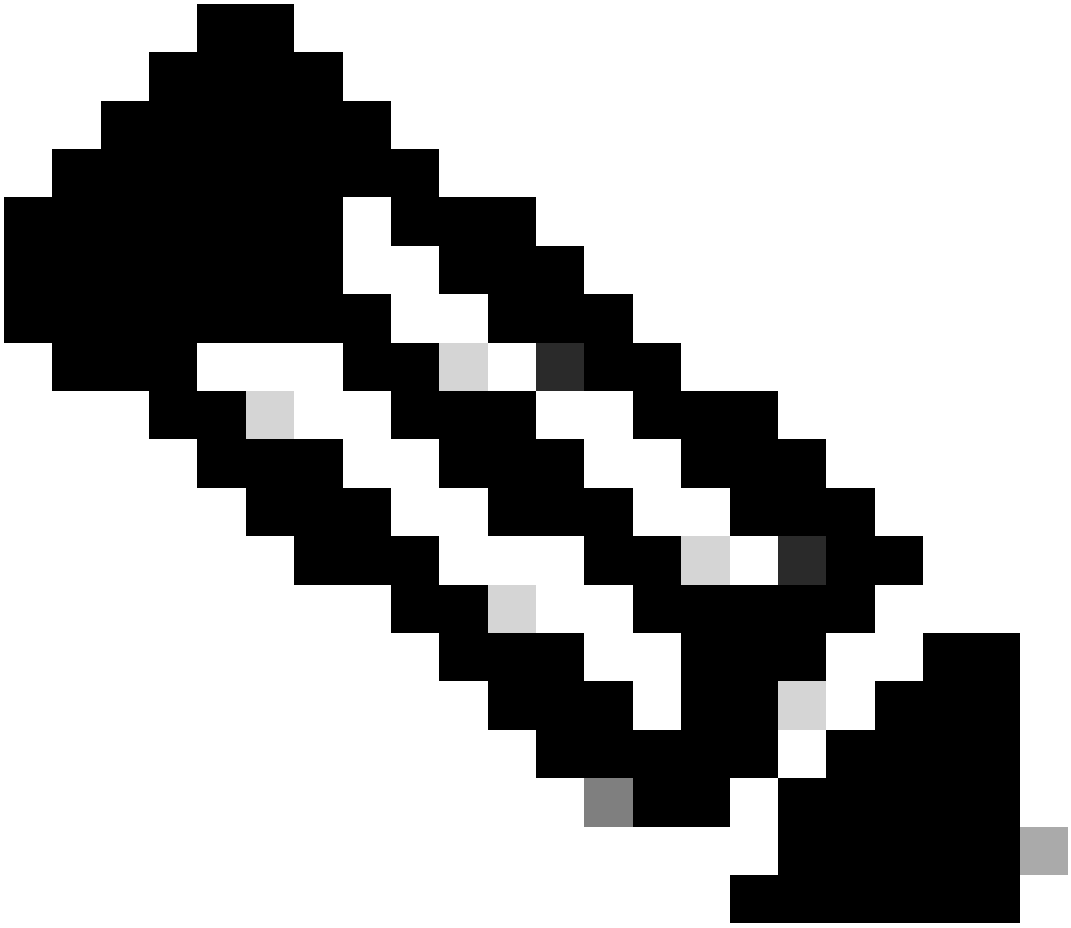

*Option 182 sous-option 5 sur la capture de paquets WLC*

Avec la mise en oeuvre de la sous-option 5, votre trafic DHCP doit être reconnu par les autres périphériques réseau. Cependant, vous pouvez toujours rencontrer des messages NAK (accusé de réception négatif), en particulier lorsque le serveur DHCP Windows est en cours d'utilisation. Cela peut être dû au fait que le serveur DHCP n'autorise pas l'adresse IP source, probablement parce qu'il n'a pas de configuration correspondante pour cette adresse IP source.

Que devez-vous faire sur le serveur DHCP ? Pour le serveur DHCP Windows, vous devez créer une portée factice pour autoriser l'adresse IP de l'agent de relais.



**Avertissement** : toutes les adresses IP de l'agent relais (GIADDR) doivent faire partie d'une plage d'adresses IP d'étendue DHCP active. Tout GIADDR en dehors des plages d'adresses IP de l'étendue DHCP est considéré comme un relais non autorisé et le serveur DHCP Windows n'accuse pas réception des requêtes des clients DHCP de ces agents de relais. Une étendue spéciale peut être créée pour autoriser les agents de relais. Créez une étendue avec le GIADDR (ou plusieurs si les GIADDR sont des adresses IP séquentielles), excluez la ou les adresses GIADDR de la distribution, puis activez l'étendue. Les agents de relais seront ainsi autorisés tout en empêchant l'attribution des adresses GIADDR.



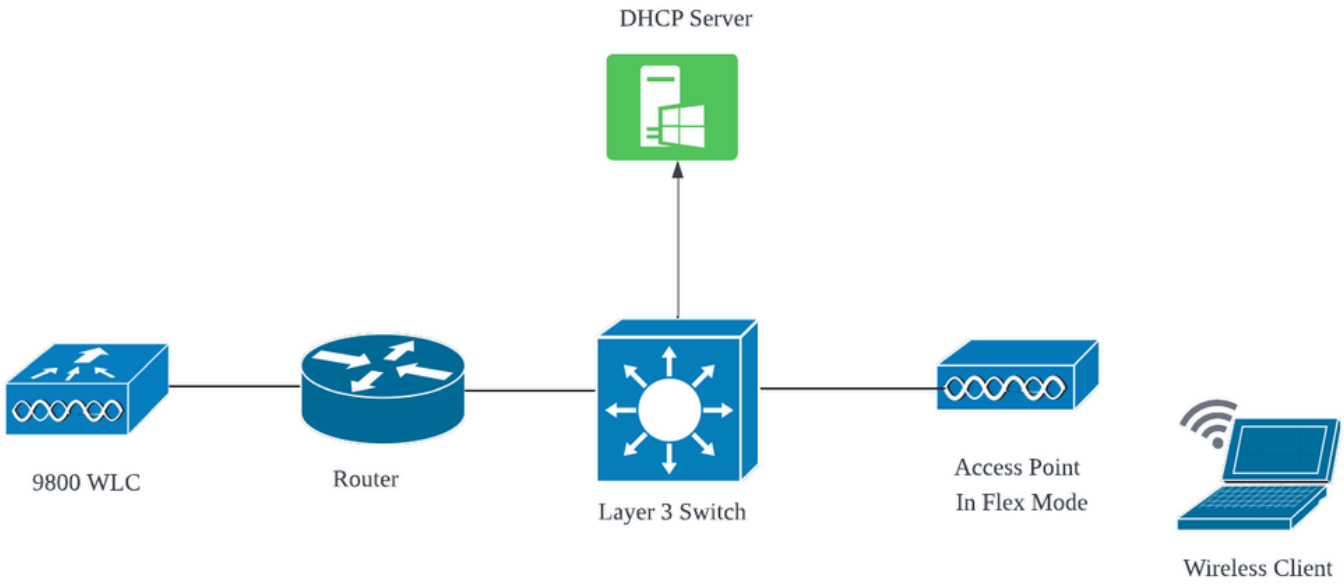
**Remarque** : dans une configuration d'ancrage étranger, le trafic DHCP est traité de manière centralisée avec le mode AP défini sur Local. Initialement, les requêtes DHCP sont envoyées au WLC étranger, qui les transfère ensuite au WLC d'ancrage via un tunnel de mobilité. C'est le WLC d'ancrage qui gère le trafic selon ses paramètres configurés. Par conséquent, toutes les configurations liées à DHCP doivent être implémentées sur le WLC d'ancrage.

---

Scénario 2. Le point d'accès fonctionne en mode flexible

Les points d'accès FlexConnect sont conçus pour les succursales et les bureaux distants, ce qui leur permet de fonctionner en mode autonome lorsqu'ils perdent la connectivité au contrôleur LAN sans fil (WLC) central. Les points d'accès FlexConnect peuvent commuter localement le trafic entre un client et le réseau sans avoir à fédérer le trafic vers le WLC. Cela réduit la latence et économise la bande passante WAN. En mode flexible AP, le trafic DHCP peut être commuté soit de manière centrale, soit de manière locale.

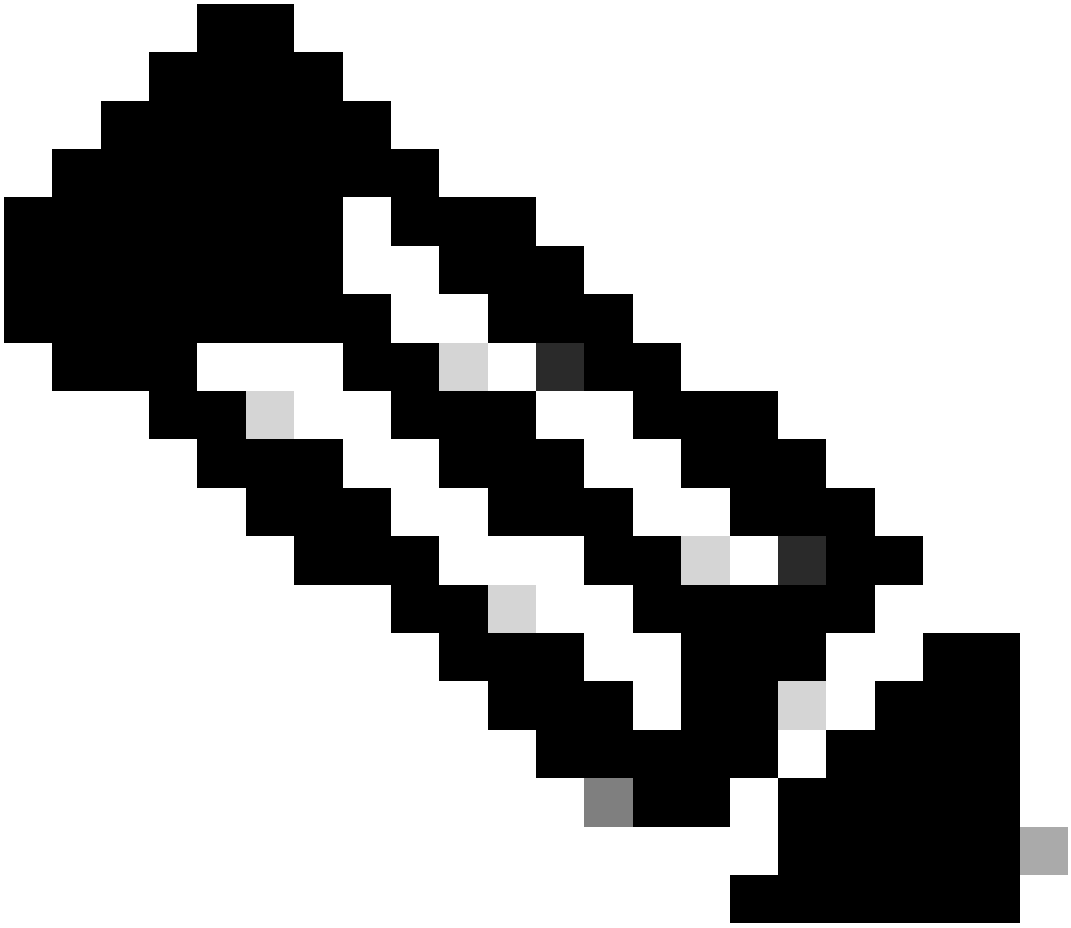
Topologie (point d'accès en mode flexible)




*Topologie réseau : point d'accès en mode flexible*

Point d'accès en mode FlexConnect avec DHCP central

Quel que soit le mode du point d’accès, les étapes de configuration, de flux opérationnel et de dépannage restent cohérentes lors de l’utilisation d’un serveur DHCP central. Cependant, pour les AP en mode FlexConnect, il est généralement conseillé d'utiliser un serveur DHCP local à moins qu'une interface SVI client ne soit configurée sur le site local.



**Remarque** : si aucun sous-réseau client n'est disponible sur le site distant, vous pouvez tirer parti de la fonction NAT-PAT de FlexConnect. FlexConnect NAT/PAT effectue la traduction d'adresses de réseau (NAT) pour le trafic provenant des clients connectés au point d'accès, en le mappant à l'adresse IP de gestion du point d'accès. Par exemple, si vous avez des AP fonctionnant en mode FlexConnect dans des filiales distantes et que les clients connectés doivent communiquer avec un serveur DHCP situé au siège où les contrôleurs résident, vous pouvez activer la NAT/PAT FlexConnect en conjonction avec le paramètre DHCP Central dans le profil de stratégie.

Point d'accès en mode FlexConnect avec DHCP local

Lorsqu'un point d'accès FlexConnect est configuré pour utiliser le protocole DHCP local, les périphériques clients qui s'associent au point d'accès reçoivent leur configuration d'adresse IP d'un serveur DHCP qui est disponible dans le même réseau local. Ce serveur DHCP local peut être un routeur, un serveur DHCP dédié ou tout autre périphérique réseau fournissant des services DHCP au sein du sous-réseau local. Avec le protocole DHCP local, le trafic DHCP est commuté au sein du réseau local, ce qui signifie que le point d'accès relaie les requêtes DHCP des clients directement au saut adjacent, tel que le commutateur d'accès. De là, les requêtes sont traitées en fonction de la configuration de votre réseau.

Prérequis:

1. Veuillez consulter le guide FlexConnect pour vous assurer que votre configuration est conforme aux instructions et aux meilleures pratiques décrites dans le guide.

2. Le VLAN client doit être répertorié sous Flex Profile.
3. Le point d'accès doit être configuré en mode d'agrégation, avec le VLAN de gestion du point d'accès désigné comme VLAN natif, et les VLAN pour le trafic client doivent être autorisés sur l'agrégation.

Voici un exemple de configuration de port de commutation connecté AP avec le VLAN de gestion comme 58 et le VLAN client comme 20 :

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

Working Setup : pour référence, partage des journaux opérationnels avec le serveur DHCP local lorsque le point d'accès est configuré pour le mode flexible :

Débogages du client 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>
```

Capture de liaison ascendante 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
```

*Capture de liaison ascendante AP*

Capture côté client :

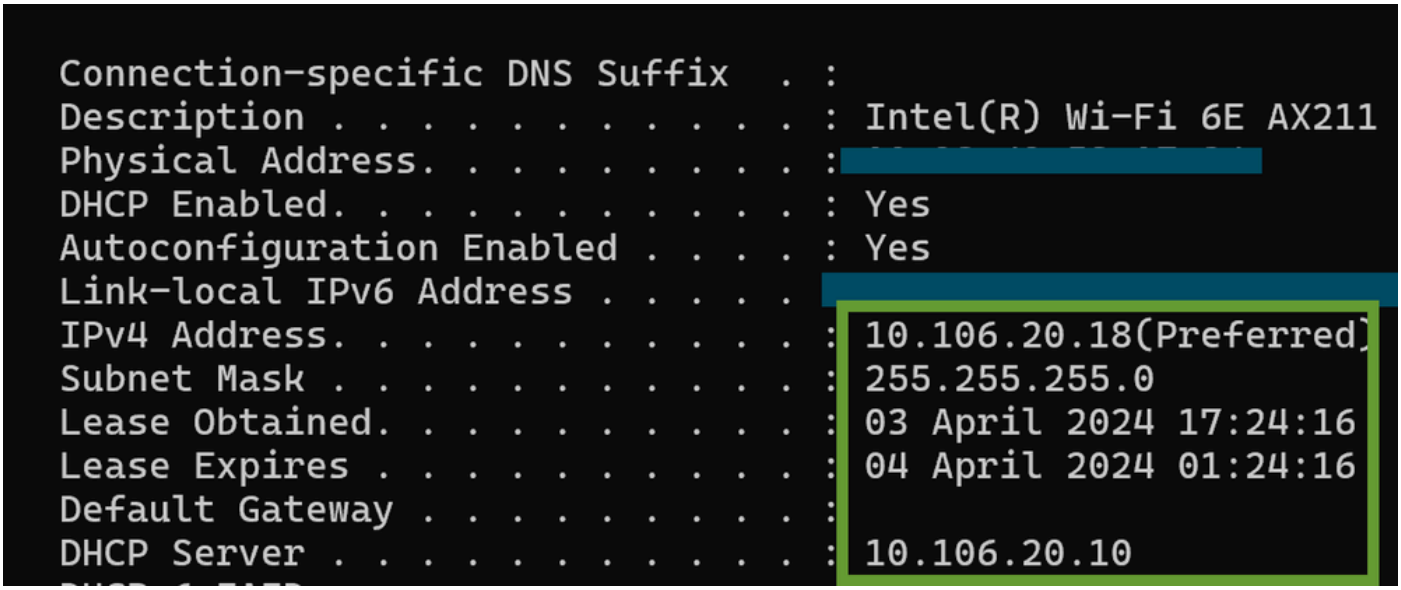
```
16540 111.905836    0.0.0.0          255.255.255.255   DHCP    343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18      DHCP    342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255   DHCP    385 DHCP Request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

*Capture de paquets client final*

Vérification de l'adresse IP du client sans fil :

Vous pouvez vérifier le bail IP sur le serveur DHCP et son état correspondant.

Sur le client sans fil :




*Vérification IP côté client*

## Dépannage du problème DHCP

Le dépannage des problèmes DHCP implique l'identification et la résolution des problèmes qui empêchent les clients d'obtenir une adresse IP d'un serveur DHCP lorsqu'ils sont connectés au réseau sans fil. Voici quelques étapes et considérations courantes lors du dépannage de problèmes DHCP :

1. Vérifier la configuration du client

- Assurez-vous que le client est configuré pour obtenir automatiquement une adresse IP.
- Vérifiez que la carte réseau est activée et qu'elle fonctionne correctement.

2. Vérifiez l'état du serveur DHCP

- Vérifiez que le serveur DHCP est opérationnel et accessible à partir du segment de réseau du client.
- Vérifiez l'adresse IP, le masque de sous-réseau et les paramètres de passerelle par défaut du serveur DHCP.

3. Revoir la configuration du périmètre

- Inspectez l'étendue DHCP pour vous assurer qu'elle dispose d'une plage suffisante d'adresses IP disponibles pour les clients.
- Vérifiez la durée du bail de l'étendue et les options, telles que les serveurs DNS et la passerelle par défaut
- Dans certains environnements (comme Active Directory), assurez-vous que le serveur DHCP est autorisé à fournir des services DHCP au sein du réseau.

4. Révisez la configuration sur le WLC 9800

- De nombreux problèmes ont été constatés en raison d'une mauvaise configuration, comme une interface de bouclage manquante, l'interface SVI du client ou l'absence d'une adresse d'assistance configurée. Avant la collecte des journaux, il est recommandé de vérifier que la configuration a été correctement implémentée.
- Lors de l'utilisation d'un serveur DHCP interne : en ce qui concerne l'épuisement de l'étendue DHCP, il est important de s'assurer, en particulier lors de la configuration de DHCP via l'interface de ligne de commande, que le minuteur de bail est configuré selon vos besoins. Par défaut, le temporisateur de bail est défini à l'infini sur le WLC 9800.
- Vérifiez que le trafic VLAN client est autorisé sur le port de liaison ascendante WLC lors de l'utilisation d'un serveur DHCP central. Inversement, lorsque vous utilisez un serveur DHCP local, assurez-vous que le VLAN approprié est autorisé sur le port de liaison

ascendante AP.

5. Paramètres de pare-feu et de sécurité

- Assurez-vous que les pare-feu ou le logiciel de sécurité ne bloquent pas le trafic DHCP (port 67 pour le serveur DHCP et port 68 pour le client DHCP).

## Collecte des journaux

**Journaux du WLC**

1. Activez l'horodatage de l'invite term exec pour avoir une référence temporelle pour toutes les commandes.

2. Utilisez pourshow tech-support wireless !! vérifier la configuration

2. Vous pouvez vérifier le nombre de clients, la répartition de l'état du client et les clients exclus.
**show wireless summary !!** Nombre total de points d'accès et de clients
**show wireless exclusionlist !!** Si un client est considéré comme exclu
show wireless exclusionlist client mac-address MAC@ !! pour obtenir plus de détails sur les clients exclus et vérifier si la raison est indiquée comme vol d'IP pour un client.

3. Vérifiez l'attribution d'adresses IP pour les clients, recherchez les adresses incorrectes ou l'apprentissage d'adresses statiques inattendu, les VLAN marqués comme sales en raison de l'absence de réponse du serveur DHCP ou les abandons de paquets dans le SISF qui gère DHCP/ARP.

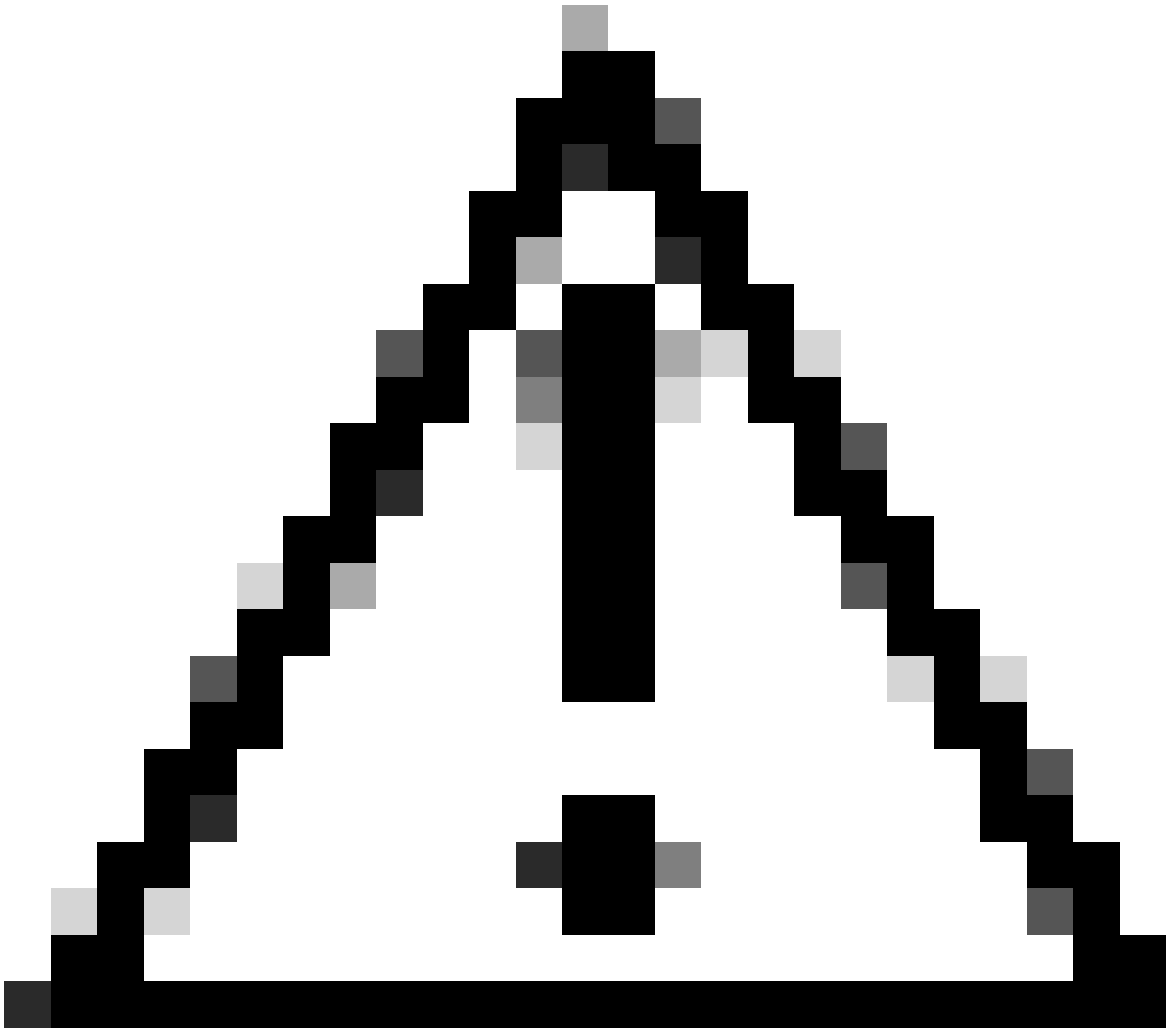
**show wireless device-tracking database ip !!** Vérifiez par IP et voyez comment l'apprentissage d'adresses a eu lieu :
**show wireless device-tracking database mac !!** Vérifiez par Mac et voyez quel client IP est attribué.
**show wireless vlan details !!** Vérifiez que le VLAN n'est pas marqué comme sale en raison de pannes DHCP en cas de groupe de VLAN utilisé.
**show wireless device-tracking feature drop !!**Baisses dans SISF

4. Sorties spécifiques du WLC pour MAC client concret@ show wireless device-tracking feature drop

Activez le suivi radioactif pour l'adresse MAC du client lorsque ce dernier tente de se connecter au réseau sans fil.

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



**Attention** : le débogage conditionnel active la journalisation au niveau du débogage qui à son tour augmente le volume des journaux générés. Laisser cette opération en cours réduit le retard dans le temps à partir duquel vous pouvez afficher les journaux. Il est donc recommandé de toujours désactiver le débogage à la fin de la session de dépannage.

---

Afin de désactiver tous les débogages, exécutez ces commandes :

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

Via l'interface utilisateur :

Étape 1. Naviguez jusqu'à  Troubleshooting > Radioactive Trace .
Étape 2. Cliquez sur Add et saisissez l'adresse Mac du client à dépanner. Vous pouvez ajouter plusieurs adresses Mac à suivre.

Étape 3. Lorsque vous êtes prêt à démarrer le suivi radioactif, cliquez sur Démarrer. Une fois démarré, la journalisation de débogage est écrite sur le disque à propos de tout traitement du plan de contrôle lié aux adresses MAC suivies.

Étape 4. Lorsque vous reproduisez le problème que vous souhaitez résoudre, cliquez sur Stop .

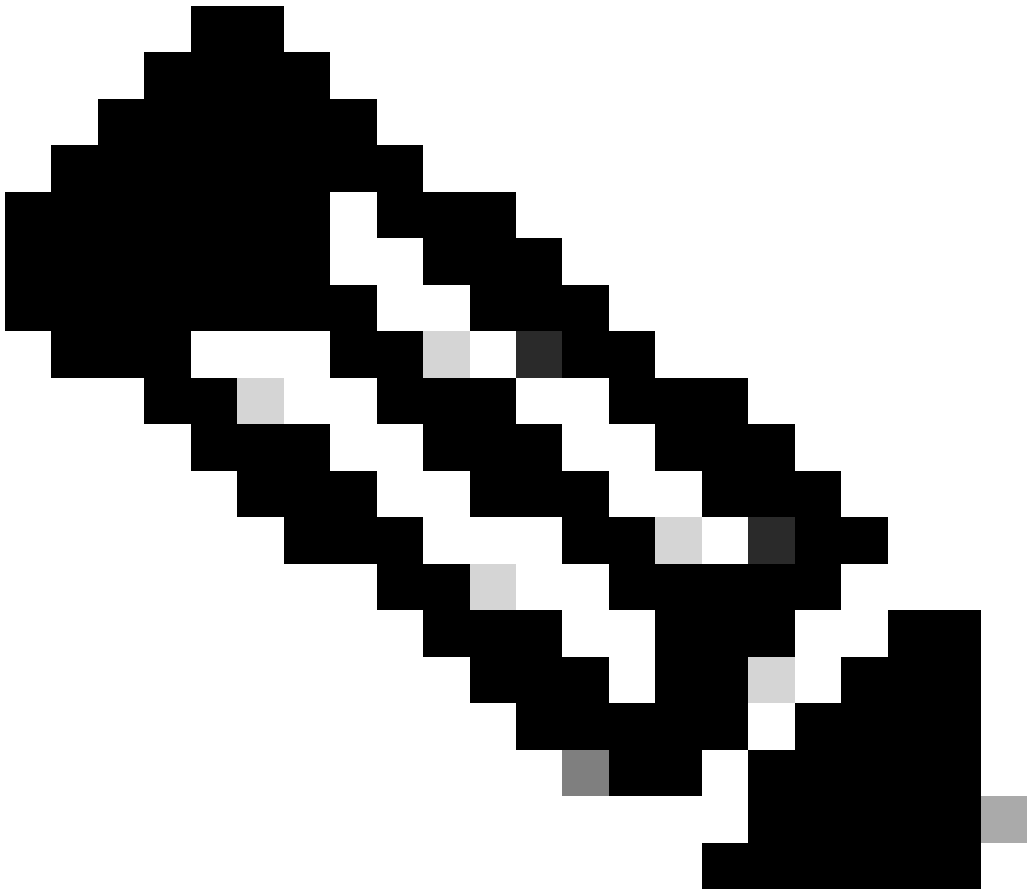
Étape 5. Pour chaque adresse mac déboguée, vous pouvez générer un fichier journal rassemblant tous les journaux relatifs à cette adresse mac en cliquant sur Generate .

Étape 6. Choisissez le délai de retour du fichier journal que vous souhaitez conserver et cliquez sur Apply to Device (Appliquer au périphérique).

Étape 7. Vous pouvez maintenant télécharger le fichier en cliquant sur la petite icône située à côté du nom du fichier. Ce fichier est présent dans le lecteur flash d'amorçage du contrôleur et peut également être copié à partir de la boîte via CLI.

!!Captures intégrées filtrées par l’adresse MAC du client dans les deux directions, filtre MAC interne du client disponible après 17.1.

---



**Remarque** : EPC sur 9800 sera utile lorsque le DHCP central est activé sur le WLC 9800.

---

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 l'interface utilisateur :
Étape 1. Accédez à Troubleshooting > Packet Capture > +Add .

Étape 2. Définissez le nom de la capture de paquets. Un maximum de 8 caractères est autorisé.

Étape 3. Définissez les filtres, le cas échéant.

Étape 4. Cochez cette case pour surveiller le trafic de contrôle si vous voulez voir le trafic envoyé au processeur du système et réinjecté dans le plan de données.

Étape 5. Définissez la taille du tampon. Un maximum de 100 Mo est autorisé.

Étape 6. Définissez la limite, soit par la durée qui permet une plage de 1 à 1000000 secondes, soit par le nombre de paquets qui permet une plage de 1 à 100000 paquets, selon vos besoins.

Étape 7. Choisissez l'interface dans la liste des interfaces de la colonne de gauche et sélectionnez la flèche pour la déplacer vers la colonne de droite.

Étape 8. Enregistrer et appliquer au périphérique.

Étape 9. Pour démarrer la capture, sélectionnez Start (Démarrer).

Étape 10. Vous pouvez laisser la capture s'exécuter jusqu'à la limite définie. Pour arrêter manuellement la capture, sélectionnez Arrêter.

Étape 11. Une fois arrêté, un bouton Export (Exporter) permet de cliquer sur l'option permettant de télécharger le fichier de capture (.pcap) sur le bureau local via le serveur HTTP ou TFTP, le serveur FTP ou le disque dur ou la mémoire flash du système local.

Journaux côté point d'accès

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

**Journaux du serveur DHCP**

Lors de l'utilisation d'un serveur DHCP externe, il est nécessaire de collecter des journaux de débogage et des captures de paquets côté serveur

pour vérifier le flux du trafic DHCP.

**Autres journaux**

Si vous constatez que les messages de détection DHCP sont visibles sur le WLC 9800 dans une configuration DHCP centrale, ou dans les journaux de débogage AP dans une configuration DHCP locale, vous devez continuer à collecter des données de capture à partir de la liaison ascendante pour confirmer que les paquets ne sont pas déposés dans le port Ethernet.Selon les capacités du commutateur, vous avez la possibilité d'effectuer une capture de paquet intégrée ou une capture SPAN (Switched Port Analyzer) sur le commutateur de liaison ascendante. Il est conseillé de suivre le flux de trafic DHCP étape par étape pour déterminer le point auquel la communication est interrompue, à la fois du client DHCP au serveur DHCP et dans le sens inverse.

## Problèmes identifiés

Problème 1. Le client tente d'obtenir une adresse IP d'un VLAN qu'il a précédemment conservé. Il peut arriver qu'un client sans fil commute entre deux SSID associés à des VLAN clients différents. Dans ce cas, le client peut persister à demander une adresse IP au VLAN auquel il était précédemment connecté. Comme cette adresse IP ne fait pas partie de l'étendue DHCP du VLAN actuel, le serveur DHCP émet un NAK (accusé de réception négatif) et, par conséquent, le client ne peut pas acquérir d'adresse IP.

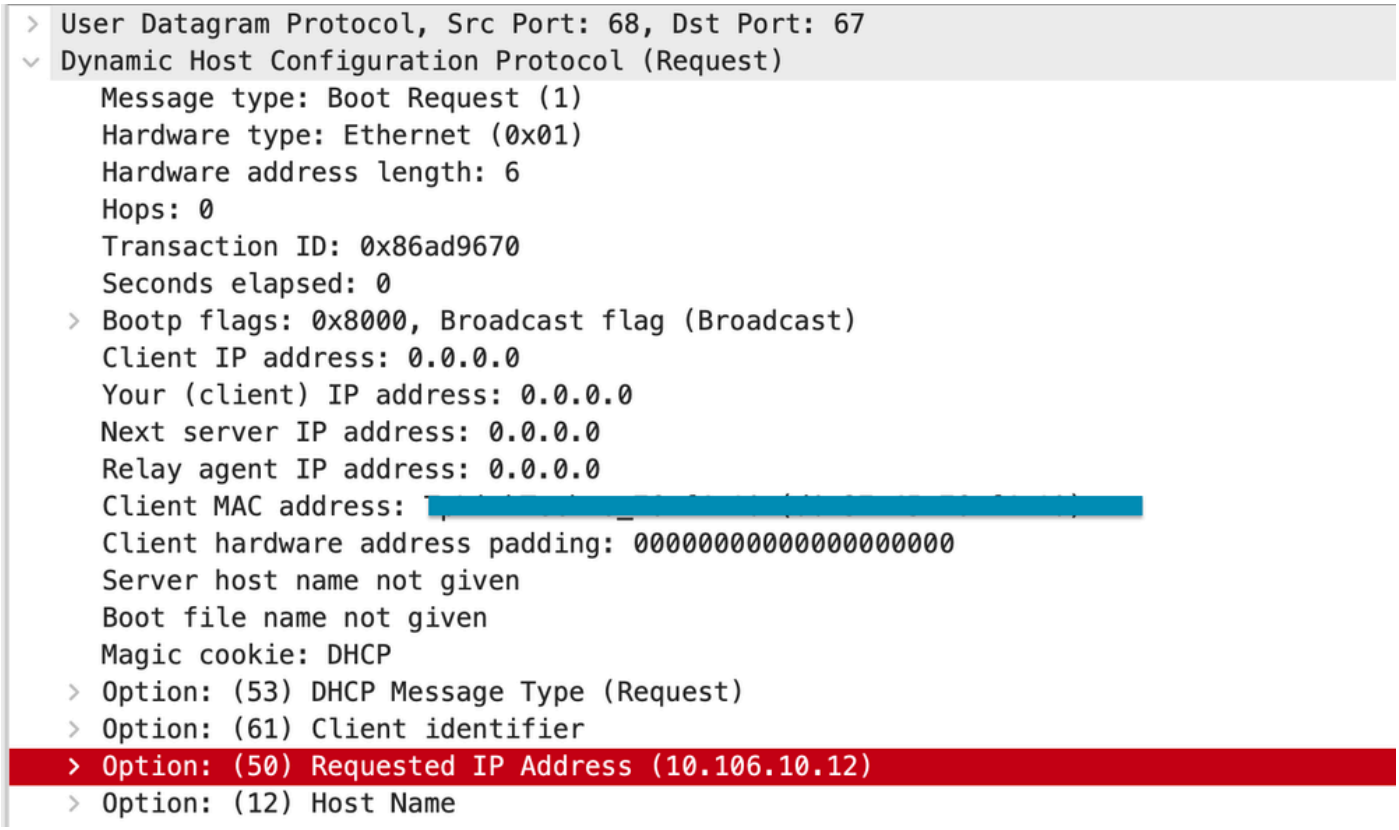
Dans les journaux de suivi radioactif, il est évident que le client continue à rechercher une adresse IP à partir du VLAN auquel il était précédemment connecté, à savoir le VLAN 10, bien que le VLAN client pour le SSID actuel soit le VLAN 20.

```
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
```

Capture de paquets intégrée sur 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
```

*Capture de paquets intégrée sur WLC*




*Option DHCP 50 sur capture de paquets WLC*

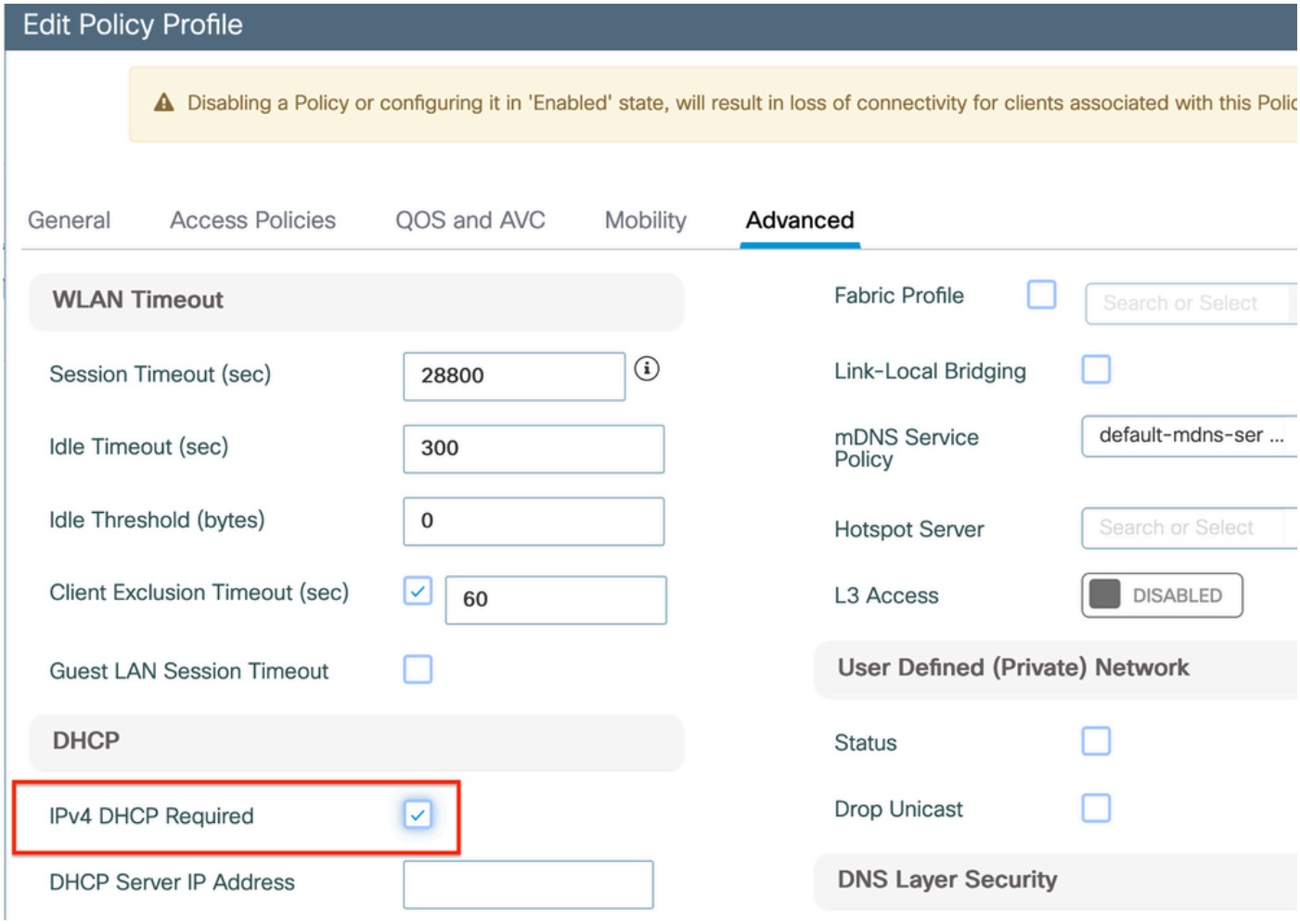
Résolution : pour vous assurer qu'un client termine le processus DHCP complet, vous pouvez activer l'option IPv4 DHCP Required dans la configuration de la stratégie. Ce paramètre doit être activé, en particulier lorsque le client commute entre des SSID, pour permettre au serveur DHCP d'envoyer un NAK au client s'il demande une adresse IP à partir d'un VLAN associé au SSID précédent. Dans le cas contraire, le client peut continuer à utiliser ou à demander l'adresse IP qu'il détenait précédemment, ce qui entraîne une interruption de la communication. Cependant, sachez que l'activation de cette fonctionnalité aura un impact sur les clients sans fil configurés avec une adresse IP statique.

Voici le processus permettant d'activer l'option souhaitée :

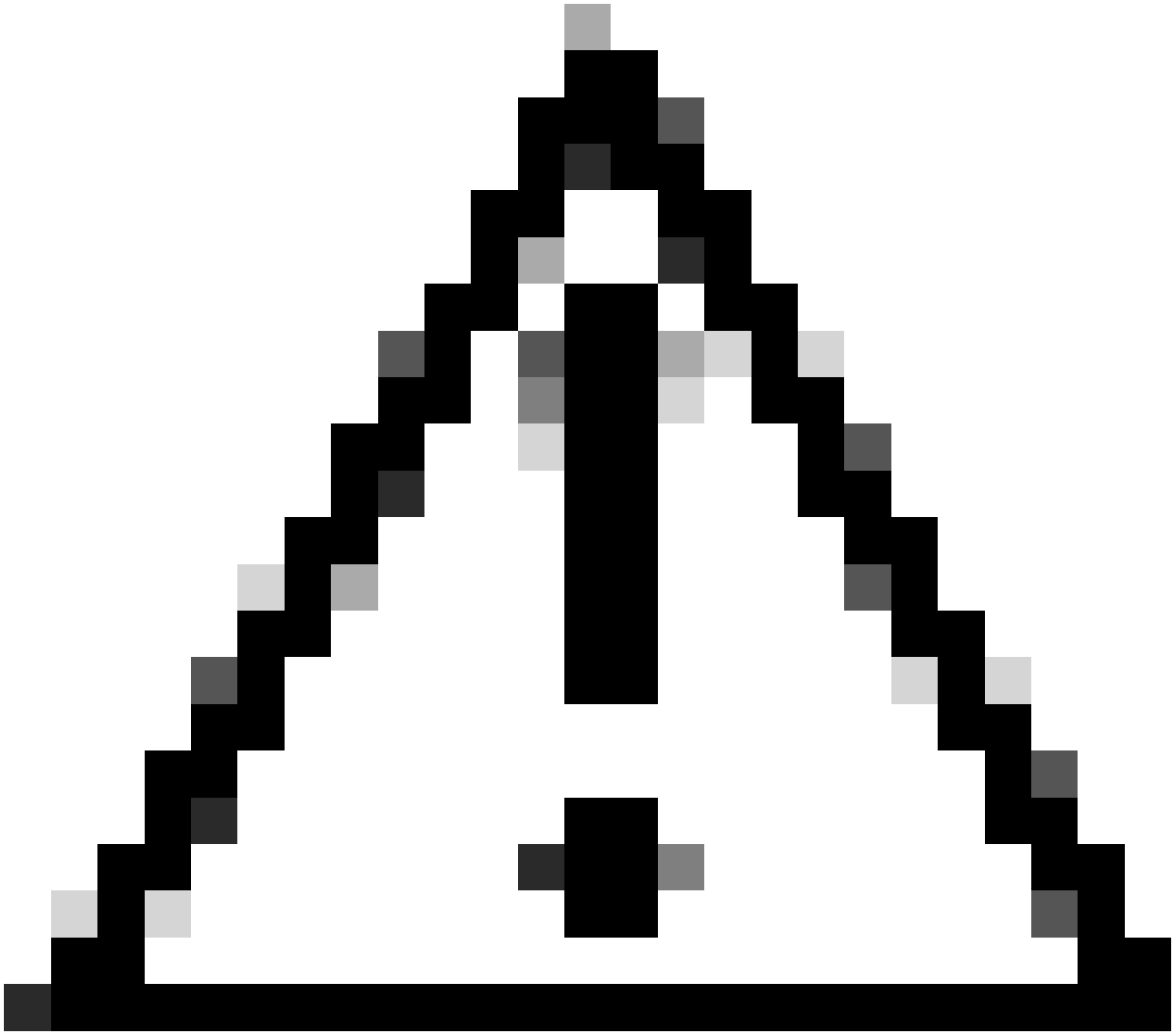
Via CLI :

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

Via l'interface GUI : accédez à Configuration > Tags & Profile > Policy > Policy_name > Advanced. Sous la section DHCP, activez ipv4 DHCP requis.




*Paramètre de profil de stratégie sur WLC*



**Attention** : pour une configuration d'ancrage étranger, il est important d'aligner les paramètres DHCP sur les deux WLC. Si le DHCP IPV4 est requis, il doit être activé sur les WLC étrangers et d'ancrage. Une différence dans la configuration relative au protocole DHCP sous le profil de stratégie entre les deux peut entraîner des problèmes pour les clients avec leurs rôles de mobilité.

---

Problème 2 : le client est supprimé ou exclu en raison d'un problème de vol d'IP. Le vol d’adresses IP, dans le contexte d’un réseau, fait référence à une situation dans laquelle plusieurs clients sans fil tentent d’utiliser la même adresse IP. Il peut être dû à de nombreuses raisons qui sont énumérées ci-dessous :

1. Unauthorized Static IP Assignment : lorsqu'un utilisateur définit une adresse IP statique sur son périphérique qui coïncide avec une adresse IP déjà attribuée ou affectée sur le réseau, cela peut entraîner un conflit d'adresses IP. Cela se produit lorsque deux périphériques tentent de fonctionner avec une adresse IP identique, ce qui peut interrompre les connexions réseau pour l'un ou les deux périphériques impliqués. Pour éviter de tels problèmes, il est essentiel de s’assurer que chaque client du réseau est configuré avec une adresse IP unique.

2. Serveur DHCP non autorisé : la présence d'un serveur DHCP non autorisé ou non autorisé sur le réseau peut entraîner l'attribution d'adresses IP en conflit avec le plan d'adressage IP établi du réseau. De tels conflits peuvent entraîner des collisions d’adresses IP ou l’obtention de

paramètres réseau incorrects pour plusieurs périphériques. Pour résoudre ce problème, des efforts doivent être faits pour identifier et éliminer le serveur DHCP non autorisé du réseau afin d'éviter d'autres conflits d'adresses IP au sein du même sous-réseau.

3. Stale Entry of client in 9800 WLC : parfois, le contrôleur peut conserver les entrées obsolètes/obsolètes d'une adresse IP qu'un client tente d'acquérir. Dans ces cas, il devient nécessaire de supprimer manuellement ces entrées périmées du WLC 9800. Voici comment s'y prendre :

- Exécutez la trace radioactive pour l'adresse MAC qui figure dans la liste d'exclusion et filtrez-la avec la trace radioactive légitime.

- Vous pourrez voir les journaux d'erreurs : %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON : Client MAC : Affected_Client_MAC avec IP : 10.37.57.24 a été ajouté à la liste d'exclusion, Legit Client MAC : Legit_Client_MAC, IP : 10.37.57.24, raison : vol d'adresse IP

- Exécutez ensuite ces commandes :
show wireless device-tracking database mac | sec $Legit_Client_MAC
**show wireless device-tracking database ip | sec $Legit_Client_MAC**

(S'il y a des entrées périmées, vous pourrez voir plus d'une adresse IP pour une adresse Mac client légitime : l'une est l'adresse IP d'origine tandis que l'autre est l'adresse obsolète/périmée.)

Résolution : supprimez manuellement les entrées obsolètes du WLC 9800 à l'aide de clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. Dans un déploiement flexible avec un serveur DHCP local utilisant le même sous-réseau : dans les configurations FlexConnect, il est courant pour divers emplacements distants d'utiliser un serveur DHCP local qui attribue des adresses IP à partir d'un sous-réseau identique. Dans ce scénario, les clients sans fil de sites différents peuvent recevoir la même adresse IP. Les contrôleurs de cette infrastructure réseau sont programmés pour détecter lorsque plusieurs connexions client utilisent une adresse IP identique, ce qui les interprète comme un vol potentiel d'IP. Par conséquent, ces clients sont généralement placés sur une liste bloquée pour éviter les conflits d'adresses IP.

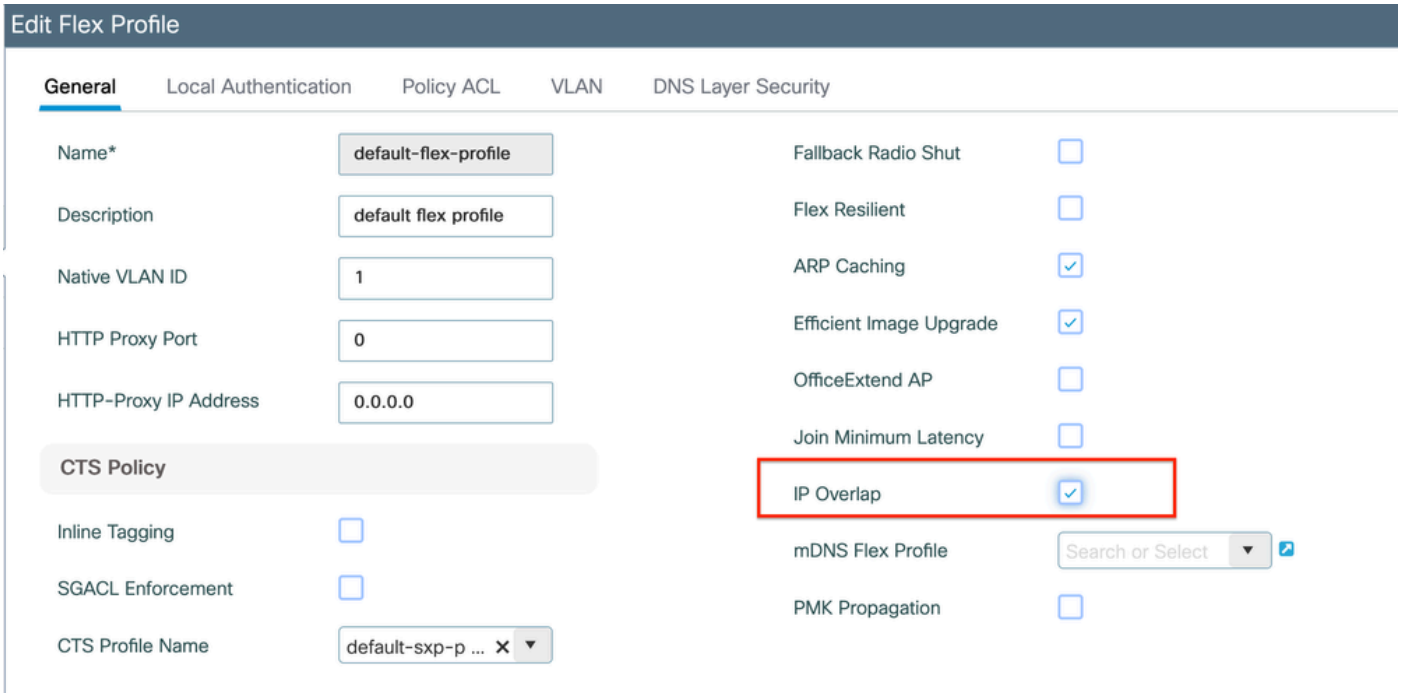
Résolution : activez la fonction de chevauchement IP dans votre profil FlexConnect. La fonctionnalité « Chevauchement d'adresses IP client dans le déploiement Flex » permet d'utiliser les mêmes adresses IP sur plusieurs sites FlexConnect tout en conservant toutes les fonctionnalités prises en charge dans les déploiements FlexConnect.

Par défaut, cette fonctionnalité est désactivée. Vous pouvez l'activer en procédant comme suit :

Via CLI :

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

Via GUI : sélectionnez Configuration > Tags & Profiles > Flex. Cliquez sur Existing Flex Profile/Add to new Flex profile et sous l'onglet General, activez IP Overlap.




*Paramètre de profil flexible sur WLC*

Problème 3. Les clients sans fil ne parviennent pas à recevoir une adresse IP du VLAN prévu. Ce problème se produit souvent lorsque le VLAN 1 est utilisé ou lorsque le VLAN attribué aux clients est le même que le VLAN utilisé pour la gestion des points d'accès dans un déploiement FlexConnect. La cause principale de ce problème est généralement des attributions de VLAN incorrectes. Pour vous guider, voici quelques scénarios à prendre en compte lors de la configuration des ID de VLAN sur la gamme 9800 :

1. Lors de l'utilisation d'un serveur AAA avec la fonction de remplacement AAA activée, il est essentiel de s'assurer que l'ID de VLAN approprié est envoyé à partir du serveur AAA. Si un nom de VLAN est fourni à la place, vérifiez qu'il correspond au nom de VLAN configuré sur le WLC 9800.

2. Lorsque le VLAN 1 est configuré pour le trafic client sans fil, le comportement peut varier en fonction du mode du point d'accès :

Pour un point d'accès en mode local/commutation centrale :

- En spécifiant VLAN-name = default, le client est affecté au VLAN 1
- À l'aide de VLAN-ID 1, un client est affecté au VLAN de gestion sans fil

Pour un point d'accès en mode flexible/commutation locale :

- En spécifiant VLAN-name = default, le client est affecté au VLAN 1
- Avec l'ID de VLAN 1, un client est affecté au VLAN natif FlexConnect

Voici quelques autres exemples de scénarios qui ont été expérimentés en laboratoire, ainsi que leurs résultats :

1. Par défaut, si l'utilisateur ne configure rien sous le profil de stratégie, le WLC attribue VLAN-ID 1 afin que les clients utilisent le VLAN de gestion sans fil en mode local et le VLAN natif AP pour FlexConnect.

2. Si le VLAN natif sous flex-profile est configuré avec un ID de VLAN natif différent de celui configuré sur le commutateur, vous voyez le problème, le client obtient l'IP du VLAN de gestion (VLAN natif) même si le profil de stratégie est configuré avec le nom de VLAN « par défaut ».

3. Si le VLAN natif sous flex-profile est configuré avec l'ID de VLAN identique au VLAN natif configuré sur le commutateur, alors seul le client pourra obtenir une adresse IP du VLAN 1 avec la valeur par défaut configurée sous le profil de stratégie.

4. Si vous avez sélectionné un nom de VLAN au lieu d'un ID de VLAN, assurez-vous que le nom de VLAN dans le profil flexible est le même.

Informations connexes

- Serveur DHCP interne sur le 9800
- Serveur DHCP externe utilisé
- Option DHCP 82 Sub Option 5 dans le serveur DHCP Windows
- NAT-PAT dans Flex AP
- VLAN 1 est utilisé pour le client sans fil
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.