Comprendre comment les WLC AireOS gèrent le protocole DHCP

Table des matières

- Introduction
- Serveur DHCP externe
  - Comparaison des modes de pontage et de proxy DHCP
  - Mode proxy DHCP
  - Flux de paquets proxy
  - Capture de paquets proxy
    - Perspective du client
    - Perspective du serveur
  - Exemple de configuration du proxy
  - Dépannage
  - Mises en garde
- Mode de pontage DHCP
  - Opérations de pontage DHCP - Flux de paquets de pontage
  - Capture de paquets de pontage - Perspective client
  - Capture de paquets de pontage - Perspective serveur
  - Exemple de configuration du pontage
  - Dépannage
  - Mises en garde
- Serveur DHCP interne
  - Comparaison des modes de pontage et DHCP internes
  - Serveur DHCP interne - Flux de paquets
  - Exemple de configuration d'un serveur DHCP interne
  - Dépannage
  - Effacer les baux DHCP sur le serveur DHCP interne du WLC
  - Mises en garde
- Interface utilisateur
- DHCP requis
- Itinérance C2 et C3
- Informations connexes

Introduction

Ce document décrit les différentes opérations DHCP sur le contrôleur sans fil Cisco AireOS.

Serveur DHCP externe

Le contrôleur de réseau local sans fil (WLC) prend en charge deux modes de fonctionnement DHCP en cas d'utilisation d'un serveur DHCP externe :

- Mode proxy DHCP
- Mode de pontage DHCP

Le mode proxy DHCP sert de fonction d'assistance DHCP afin d'améliorer la sécurité et le contrôle des transactions DHCP entre le serveur DHCP et les clients sans fil. Le mode de pontage DHCP permet de rendre le rôle de contrôleur dans une transaction DHCP entièrement transparent pour les clients sans fil.

Comparaison des modes de pontage et de proxy DHCP

Gestion du DHCP client	Mode proxy DHCP	Mode de pontage DHCP
Modifier giaddr	Oui	Non
Modifier siaddr	Oui	Non
Modifier le contenu du paquet	Oui	Non
Offres redondantes non transmises	Oui	Non
Option 82 prise en charge	Oui	Non
Diffusion vers monodiffusion	Oui	Non
Support BOOTP	Non	Serveur
RFC non conforme	Les agents proxy et les agents de relais ne sont pas exactement le même concept. Le mode de pontage DHCP est recommandé pour une conformité RFC complète.	Non

Mode proxy DHCP

Le proxy DHCP n'est pas idéal pour tous les environnements réseau. Le contrôleur modifie et relaie toutes les transactions DHCP afin de fournir une fonction d'assistance et de résoudre certains problèmes de sécurité.

L'adresse IP virtuelle du contrôleur est normalement utilisée comme adresse IP source de toutes les transactions DHCP vers le client. Par conséquent, l'adresse IP réelle du serveur DHCP n'est pas exposée dans l'air. Cette adresse IP virtuelle est affichée dans la sortie de débogage pour les transactions DHCP sur le contrôleur. Cependant, l'utilisation d'une adresse IP virtuelle peut poser des problèmes pour certains types de clients.

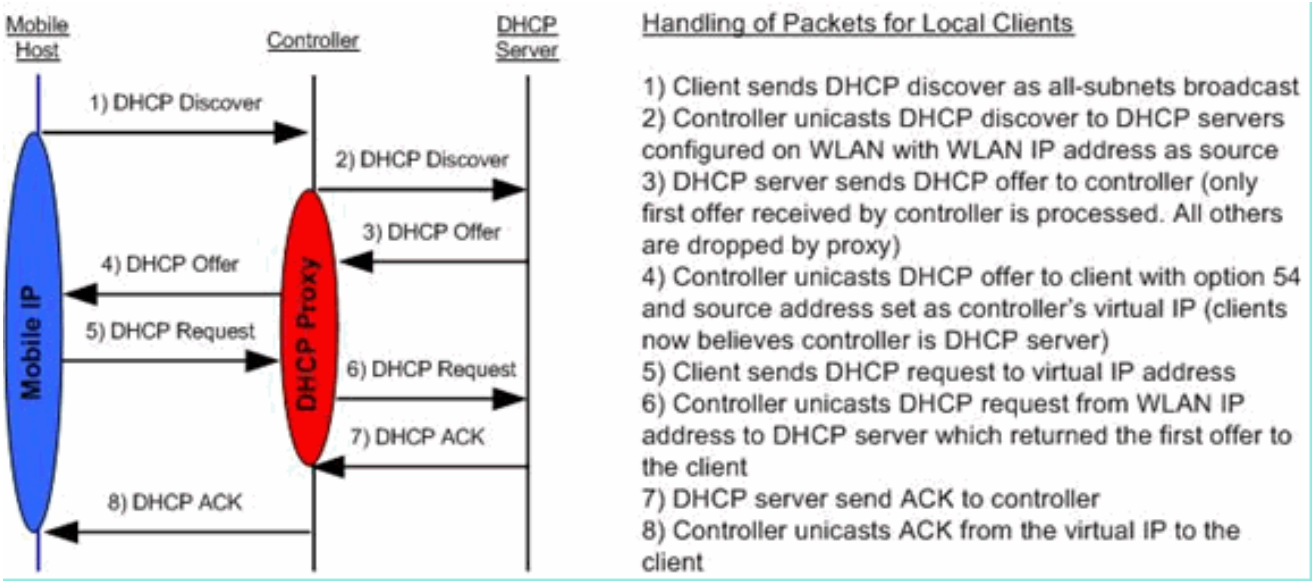
Le fonctionnement en mode proxy DHCP conserve le même comportement pour les protocoles de mobilité symétrique et asymétrique.

Lorsque plusieurs offres proviennent de serveurs DHCP externes, le proxy DHCP sélectionne normalement la première qui arrive et définit l'adresse IP du serveur dans la structure de données du client. Par conséquent, toutes les transactions suivantes s'exécutent via le même serveur DHCP jusqu'à ce qu'une transaction échoue après de nouvelles tentatives. À ce stade, le proxy sélectionne un serveur DHCP différent pour le client.

Le proxy DHCP est activé par défaut. Tous les contrôleurs qui communiquent doivent avoir le même paramètre de proxy DHCP.

Remarque : Le proxy DHCP doit être activé pour que l'option DHCP 82 fonctionne correctement.

Flux de paquets proxy

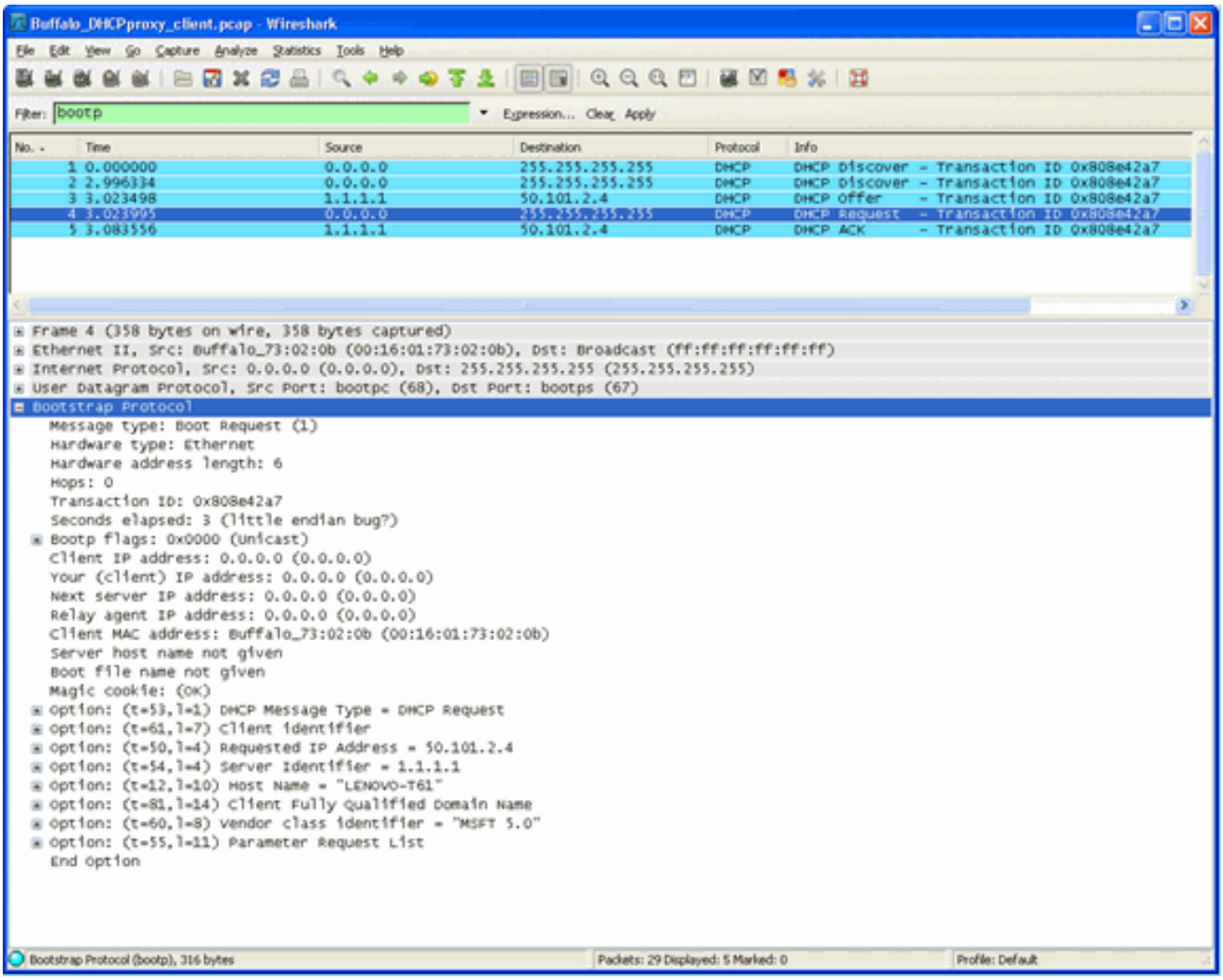


Capture de paquets proxy

Lorsque le contrôleur est en mode proxy DHCP, il dirige non seulement les paquets DHCP vers le serveur DHCP, mais il crée en fait de nouveaux paquets DHCP à transférer vers le serveur DHCP. Toutes les options DHCP présentes dans les paquets DHCP client sont copiées dans les paquets DHCP du contrôleur. Les exemples de capture d'écran suivants le montrent pour un paquet de requête DHCP.

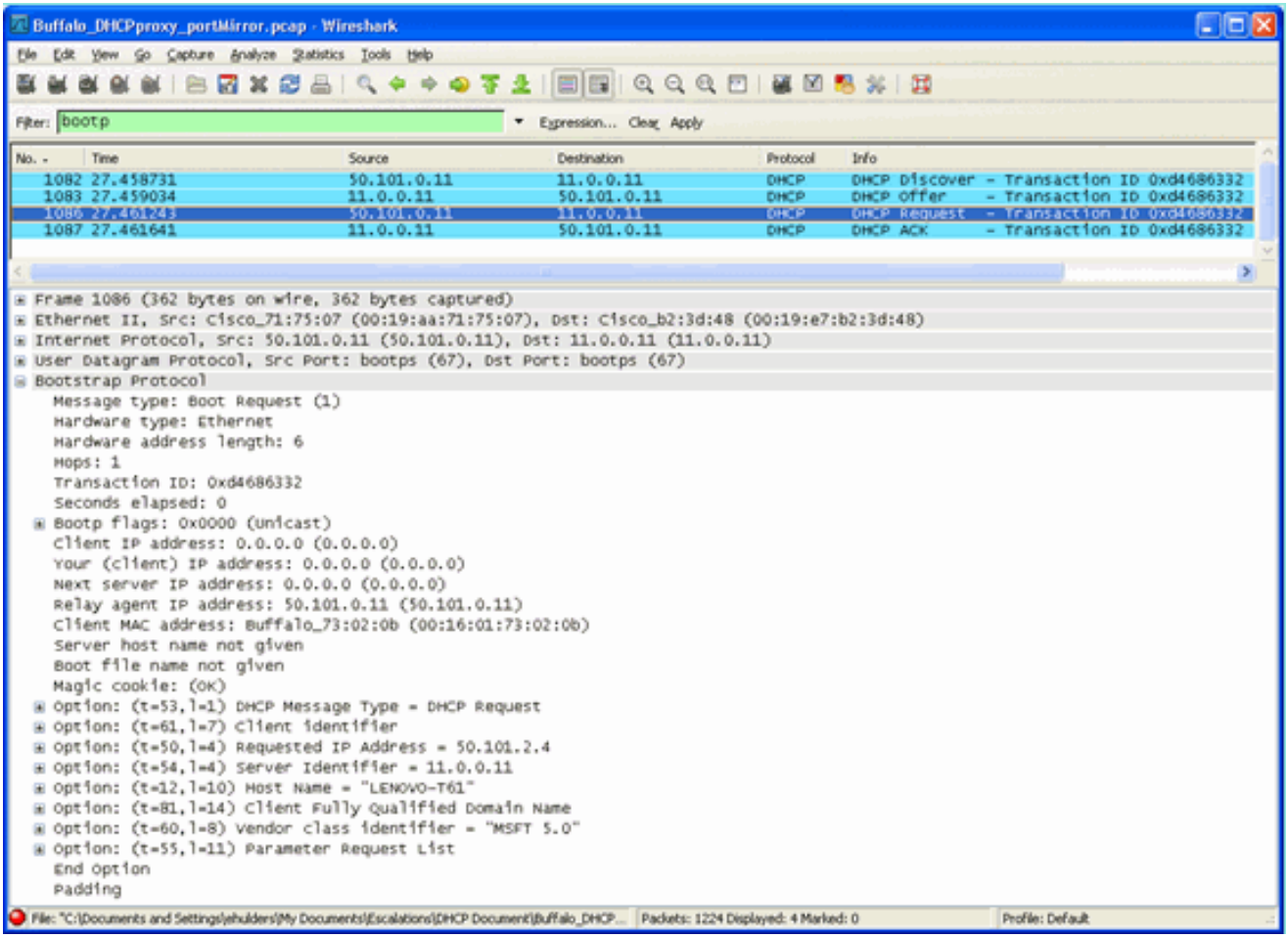
Perspective du client

Cette capture d'écran est une capture de paquets prise du point de vue du client. Elle affiche une découverte DHCP, une offre DHCP, une requête DHCP et un ACK DHCP. La requête DHCP est mise en surbrillance et le détail du protocole est développé, ce qui indique les options DHCP boot p.



Perspective du serveur

Cette capture d'écran est une capture de paquets prise du point de vue du serveur. Comme dans l'exemple précédent, il présente une découverte DHCP, une offre DHCP, une requête DHCP et un ACK DHCP. Cependant, il s'agit de paquets que le contrôleur a construits en fonction du proxy DHCP. Là encore, la requête DHCP est mise en surbrillance et le détail du protocole est développé, ce qui indique les options DHCP boot p. Notez qu'ils sont identiques à ceux du paquet de requête DHCP du client. Notez également que le proxy WLC relaie le paquet et met en surbrillance les adresses de paquet.



Exemple de configuration du proxy

Pour utiliser le contrôleur comme proxy DHCP, la fonctionnalité de proxy DHCP doit être activée sur le contrôleur. Par défaut, cette fonctionnalité est activée. Afin d'activer le proxy DHCP, cette commande CLI peut être utilisée. La même option est disponible dans l'interface utilisateur graphique de la page Controller du menu DHCP.

<#root>

```
(Cisco Controller) >
config dhcp proxy enable
(Cisco Controller) >
show dhcp proxy

DHCP Proxy Behavior: enabled
```

Pour que le proxy DHCP fonctionne, un serveur DHCP principal doit être configuré sur chaque interface de contrôleur qui nécessite des services DHCP. Un serveur DHCP peut être configuré sur l'interface de gestion, l'interface du gestionnaire d'applications et sur les interfaces dynamiques. Ces commandes CLI peuvent être utilisées afin de configurer un serveur DHCP pour

chaque interface.

<#root>

```
(Cisco Controller) >
config interface dhcp ap-manager primary <primary-server>
(Cisco Controller) >
config interface dhcp management primary <primary-server>
(Cisco Controller) >
config interface dhcp dynamic-interface <interface-name>

 primary <primary-server>
```

La fonctionnalité de pontage DHCP est un paramètre global, elle affecte donc toutes les transactions DHCP au sein du contrôleur.

Dépannage

Voici le résultat de la **debug dhcp packet enable** commande. Le débogage montre un contrôleur qui reçoit une requête DHCP d'un client avec l'adresse MAC 00:40:96:b4:8c:e1, transmet une requête DHCP au serveur DHCP, reçoit une réponse du serveur DHCP et envoie une offre DHCP au client.

<#root>

```
(Cisco Controller) >
debug dhcp message enable

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP received op BOOTREQUEST (1)
 (len 312, port 29, encap 0xec03)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len (including the magic cookie) 76
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message type = DHCP REQUEST
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 61 (len 7) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: requested ip = 192.168.4.13
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 12 (len 7) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 81 (len 11) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: vendor class id = MSFT 5.0 (len 8)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 55 (len 11) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP options end, len 76, actual 68
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selecting relay 1 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0  VLAN: 0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selected relay 1 - 192.168.3.1
 (local address 192.168.4.2, gateway 192.168.4.1, VLAN 101, port 29)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP transmitting DHCP REQUEST (3)
```

```
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   op: BOOTREQUEST, htype: Ethernet,
 hlen: 6, hops: 1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   xid: 0xfc3c9979 (4231829881), secs: 0,
 flags: 0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   chaddr: 00:40:96:b4:8c:e1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   siaddr: 0.0.0.0,  giaddr: 192.168.4.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   requested ip: 192.168.4.13

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP Forwarding DHCP packet (332 octets)
          -- packet received on direct-connect port requires forwarding to external DHCP
 server. Next-hop is 192.168.4.1

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REQUEST to 192.168.4.1
 (len 350, port 29, vlan 101)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selecting relay 2 - control block settings:
                        dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 192.168.4.1  VLAN: 101
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selected relay 2 - NONE

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP received op BOOTREPLY (2) (len 316, port 29,
 encap 0xec00)

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len (including the magic cookie) 80
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message type = DHCP ACK
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 58 (len 4) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 59 (len 4) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: lease time = 691200 seconds
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: server id = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: netmask = 255.255.0.0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 15 (len 14) - skipping
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: gateway = 192.168.4.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: DNS server, cnt = 1, first = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: WINS server, cnt = 1, first = 192.168.3.1
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP options end, len 80, actual 72
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP setting server from ACK (server 192.168.3.1,
 yiaddr 192.168.4.13)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 Assigning Address 192.168.4.13 to mobile

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REPLY to STA (len 424, port 29,
 vlan 20)
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP transmitting DHCP ACK (5)

Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6,
 hops: 0
Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP   xid: 0xfc3c9979 (4231829881), secs: 0,
 flags: 0
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   chaddr: 00:40:96:b4:8c:e1
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   ciaddr: 0.0.0.0,  yiaddr: 192.168.4.13
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP   server id: 192.0.2.10  rcvd server id: 192.168.3.1
```

Mises en garde

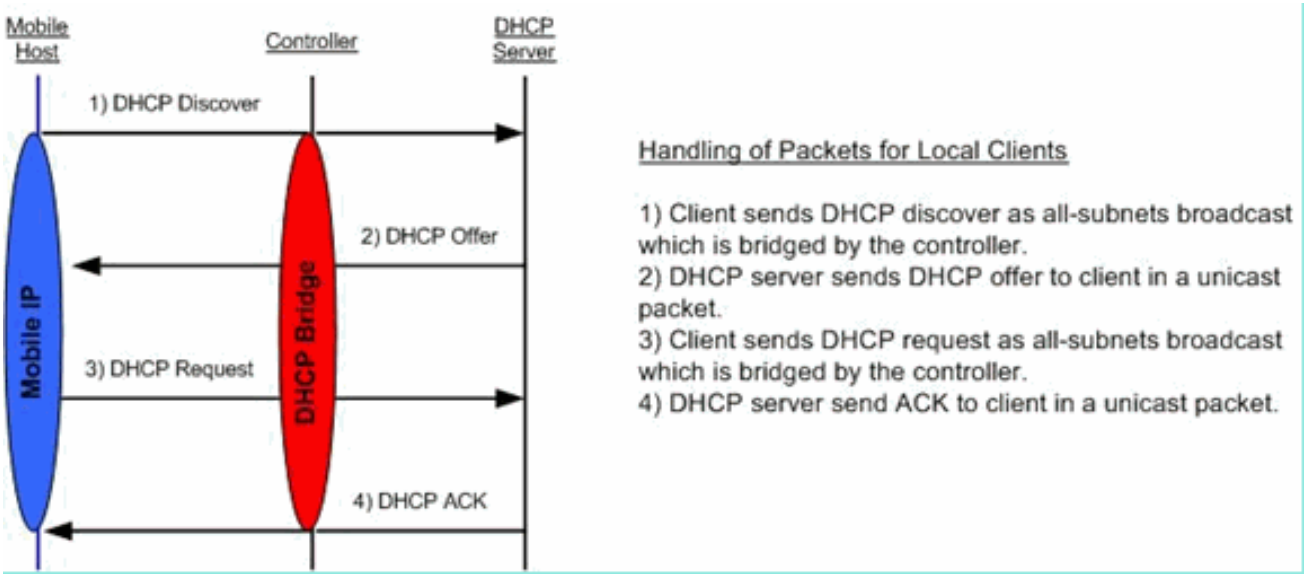
- Des problèmes d'interopérabilité peuvent exister entre un contrôleur avec proxy DHCP activé et des périphériques qui agissent à la fois comme pare-feu et comme serveur DHCP. Cela est probablement dû au composant pare-feu du périphérique, car les pare-feu ne répondent généralement pas aux requêtes proxy. La solution de contournement pour ce problème est de désactiver le proxy DHCP sur le contrôleur.

- Lorsqu'un client est à l'état DHCP REQ sur le contrôleur, le contrôleur abandonne les paquets d'information DHCP. Le client ne passe pas en état d'exécution sur le contrôleur (ceci est nécessaire pour que le client passe le trafic) jusqu'à ce qu'il reçoive un paquet de détection DHCP du client. Les paquets d'information DHCP sont transférés par le contrôleur lorsque le proxy DHCP est désactivé.
- Tous les contrôleurs qui communiquent entre eux doivent avoir le même paramètre de proxy DHCP.

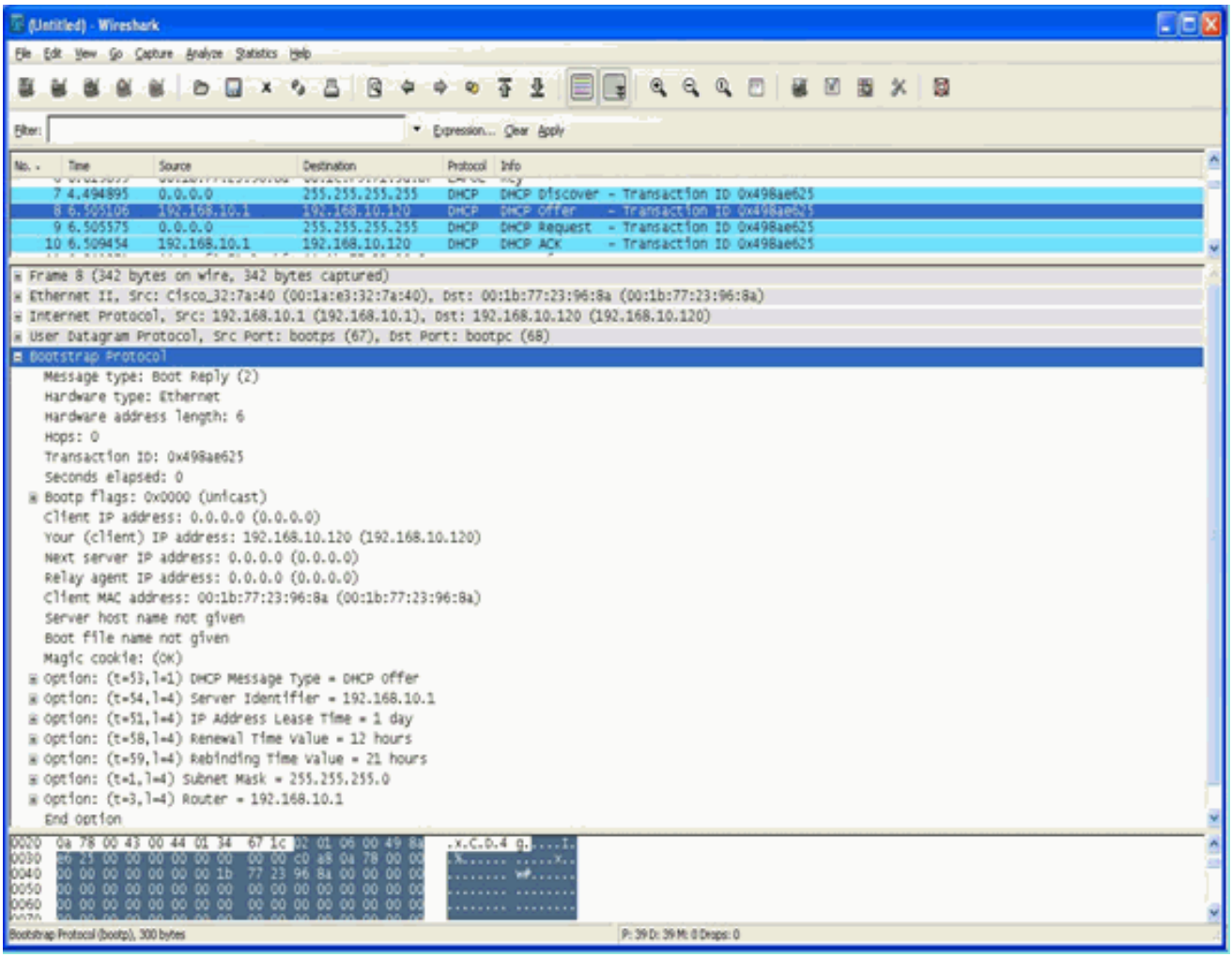
Mode de pontage DHCP

La fonctionnalité de pontage DHCP est conçue pour rendre le rôle de contrôleur dans la transaction DHCP entièrement transparent pour le client. À l'exception de la conversion 802.11 en Ethernet II, les paquets du client sont pontés sans modification du tunnel LWAPP (Light Weight Access Point Protocol) vers le VLAN client (ou du tunnel Ethernet sur IP (EoIP) dans le cas d'itinérance de couche 3). De même, à l'exception des conversions Ethernet II vers 802.11, les paquets destinés au client sont pontés sans modification depuis le VLAN client (ou tunnel EoIP dans le cas d'itinérance de couche 3) vers le tunnel LWAPP. Considérez cela comme le câblage d'un client dans un port de commutation, puis le client effectue une transaction DHCP traditionnelle.

Opérations de pontage DHCP - Flux de paquets de pontage

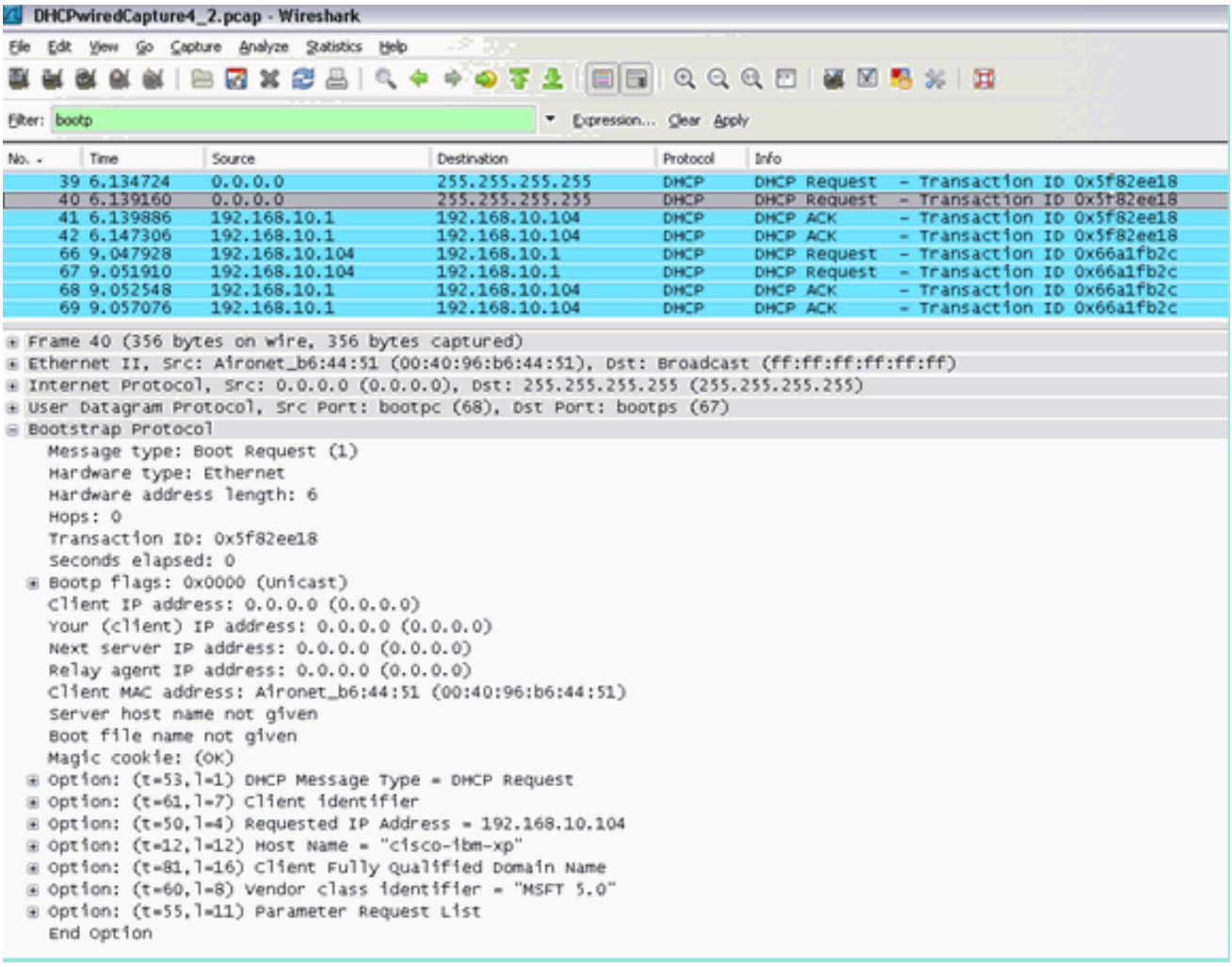


Capture de paquets de pontage - Perspective client



Dans la capture de paquets côté client, la principale différence entre la capture du client en mode Proxy est l'adresse IP réelle du serveur DHCP, qui apparaît dans les paquets Offer et Ack au lieu de l'adresse IP virtuelle du contrôleur.

Capture de paquets de pontage - Perspective serveur



Dans la capture de paquets filaire, vous pouvez voir que le paquet 40 est la diffusion de requête DHCP pontée du client test 00:40:96:b6:44:51 vers le réseau filaire.

Exemple de configuration du pontage

Afin d'activer la fonctionnalité de pontage DHCP sur le contrôleur, vous devez désactiver la fonctionnalité de proxy DHCP sur le contrôleur. Pour ce faire, vous devez utiliser les commandes suivantes dans l'interface de ligne de commande :

<#root>

```
(Cisco Controller) >
config dhcp proxy disable
(Cisco Controller) >
show dhcp proxy
DHCP Proxy Behaviour: disabled
```

Si le serveur DHCP n'existe pas sur le même réseau de couche 2 (L2) que le client, la diffusion doit être transmise au serveur DHCP au niveau de la passerelle client à l'aide d'un assistant IP.

Voici un exemple de cette configuration :

<#root>

```
Switch#
conf t
Switch(config)#
interface vlan <client vlan #>
Switch(config-if)#
ip helper-address <dhcp server IP>
```

La fonctionnalité de pontage DHCP est un paramètre global, elle affecte donc toutes les transactions DHCP au sein du contrôleur. Vous devez ajouter des instructions IP helper dans l'infrastructure filaire pour tous les VLAN nécessaires sur le contrôleur.

Dépannage

Les débogages répertoriés ici ont été activés sur l'interface de ligne de commande du contrôleur et la partie DHCP du résultat a été extraite pour ce document.

<#root>

```
(Cisco Controller) >
debug client 00:40:96:b6:44:51
(Cisco Controller) >
debug dhcp message enable

00:40:96:b6:44:51 DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 72
00:40:96:b6:44:51 DHCP option: message type = DHCP DISCOVER
00:40:96:b6:44:51 DHCP option: 116 (len 1) - skipping
00:40:96:b6:44:51 DHCP option: 61 (len 7) - skipping
00:40:96:b6:44:51 DHCP option: 12 (len 12) - skipping
00:40:96:b6:44:51 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:40:96:b6:44:51 DHCP option: 55 (len 11) - skipping
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP DISCOVER (1)
00:40:96:b6:44:51 DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP   xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP   chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP successfully bridged packet to DS
00:40:96:b6:44:51 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 72
00:40:96:b6:44:51 DHCP option: message type = DHCP OFFER
```

00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1

00:40:96:b6:44:51 DHCP option: lease time = 84263 seconds
00:40:96:b6:44:51 DHCP option: 58 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: 59 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP option: gateway = 192.168.10.1
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP OFFER (2)
00:40:96:b6:44:51 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.10.104
00:40:96:b6:44:51 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP server id: 192.168.10.1 rcvd server id: 192.168.10.1

00:40:96:b6:44:51 DHCP successfully bridged packet to STA

00:40:96:b6:44:51 DHCP received op BOOTREQUEST (1) (len 328, port 1, encap 0xec03)
00:40:96:b6:44:51 DHCP option len (including the magic cookie) 92
00:40:96:b6:44:51 DHCP option: message type = DHCP REQUEST
00:40:96:b6:44:51 DHCP option: 61 (len 7) - skipping
00:40:96:b6:44:51 DHCP option: requested ip = 192.168.10.104
00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1
00:40:96:b6:44:51 DHCP option: 12 (len 12) - skipping
00:40:96:b6:44:51 DHCP option: 81 (len 16) - skipping
00:40:96:b6:44:51 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:40:96:b6:44:51 DHCP option: 55 (len 11) - skipping
00:40:96:b6:44:51 DHCP options end, len 92, actual 84
00:40:96:b6:44:51 DHCP processing DHCP REQUEST (3)
00:40:96:b6:44:51 DHCP op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP requested ip: 192.168.10.104
00:40:96:b6:44:51 DHCP server id: 192.168.10.1 rcvd server id: 192.168.10.1

00:40:96:b6:44:51 DHCP successfully bridged packet to DS

00:40:96:b6:44:51 DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
00:40:96:b6:44:51 DHCP option len (including the magic
cookie) 72 00:40:96:b6:44:51 DHCP option: message type = DHCP ACK
00:40:96:b6:44:51 DHCP option: server id = 192.168.10.1
00:40:96:b6:44:51 DHCP option: lease time = 86400 seconds
00:40:96:b6:44:51 DHCP option: 58 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: 59 (len 4) - skipping
00:40:96:b6:44:51 DHCP option: netmask = 255.255.255.0
00:40:96:b6:44:51 DHCP option: gateway = 192.168.10.1
00:40:96:b6:44:51 DHCP options end, len 72, actual 64
00:40:96:b6:44:51 DHCP processing DHCP ACK (5)
00:40:96:b6:44:51 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
00:40:96:b6:44:51 DHCP xid: 0x224dfab6 (575535798), secs: 0, flags: 0
00:40:96:b6:44:51 DHCP chaddr: 00:40:96:b6:44:51
00:40:96:b6:44:51 DHCP ciaddr: 0.0.0.0, yiaddr: 192.168.10.104
00:40:96:b6:44:51 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0
00:40:96:b6:44:51 DHCP server id: 192.168.10.1 rcvd server id: 192.168.10.1

00:40:96:b6:44:51 Assigning Address 192.168.10.104 to mobile
00:40:96:b6:44:51 DHCP successfully bridged packet to STA
00:40:96:b6:44:51 192.168.10.104 Added NPU entry of type 1

Dans cette sortie de débogage DHCP, il y a quelques indications clés que le pontage DHCP est utilisé sur le contrôleur :

- Paquet DHCP correctement ponté vers DS : cela signifie que le paquet DHCP d'origine du client a été ponté, sans modification vers le système de distribution (DS). Le DS est l'infrastructure filaire.
- DHCP a réussi à ponter le paquet vers STA : ce message indique que le paquet DHCP a été ponté, sans modification vers la station (STA). STA est l'ordinateur client qui demande DHCP.

En outre, vous voyez l'adresse IP réelle du serveur indiquée dans les débogages, qui est 192.168.10.1. Si le proxy DHCP est utilisé au lieu du pontage DHCP, vous pouvez voir l'adresse IP virtuelle du contrôleur indiquée pour l'adresse IP du serveur.

Mises en garde

- Par défaut, le proxy DHCP est activé.
- Tous les contrôleurs qui communiquent entre eux doivent avoir le même paramètre de proxy DHCP.
- Le proxy DHCP doit être activé pour que l'option DHCP 82 fonctionne.

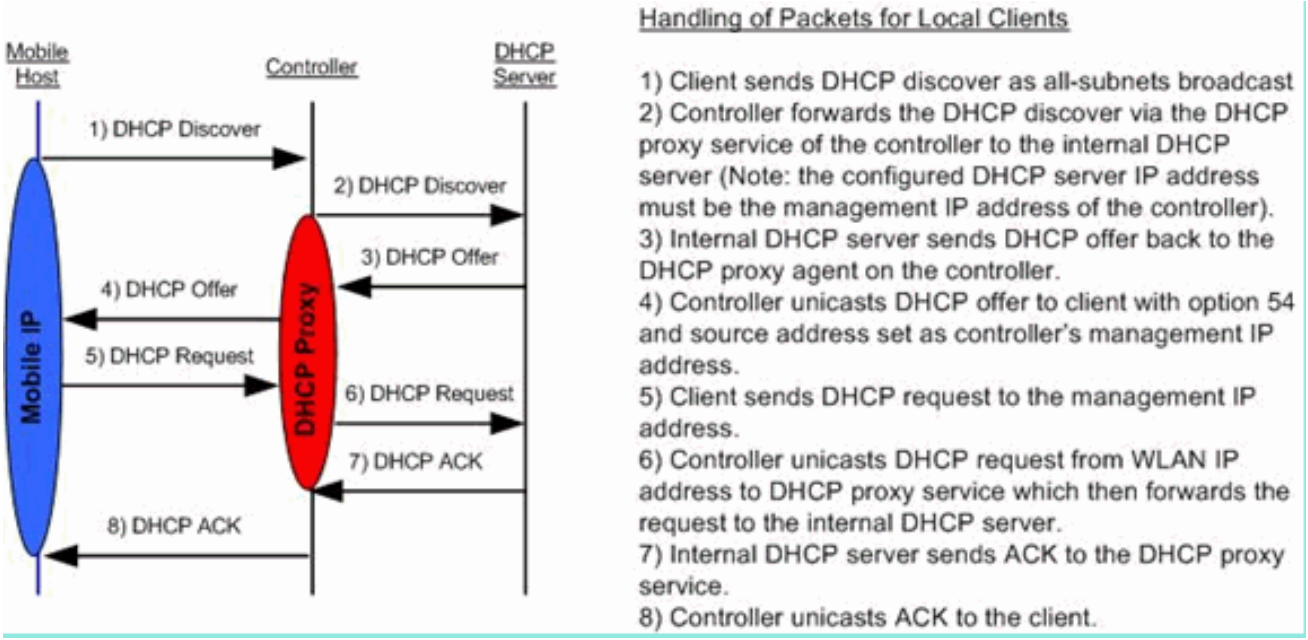
Serveur DHCP interne

Le serveur DHCP interne a été introduit initialement pour les filiales où un serveur DHCP externe n'est pas disponible. Il est conçu pour prendre en charge un petit réseau sans fil avec moins de dix points d'accès (AP) situés sur le même sous-réseau. Le serveur interne fournit des adresses IP aux clients sans fil, des points d'accès à connexion directe, des points d'accès en mode appliance sur l'interface de gestion et des requêtes DHCP qui sont relayées à partir des points d'accès. Il ne s'agit pas d'un serveur DHCP à usage général complet. Il ne prend en charge que des fonctionnalités limitées et n'évolue pas dans un déploiement plus important.

Comparaison des modes de pontage et DHCP internes

Les deux principaux modes DHCP sur le contrôleur sont le proxy DHCP ou le pontage DHCP. Avec le pontage DHCP, le contrôleur agit plus comme un retour DHCP avec des AP autonomes. Un paquet DHCP arrive dans le point d'accès via une association de client à un SSID (Service Set Identifier) qui est lié à un VLAN. Ensuite, le paquet DHCP sort de ce VLAN. Si un assistant IP est défini sur la passerelle de couche 3 (L3) de ce VLAN, le paquet est transféré à ce serveur DHCP par monodiffusion dirigée. Le serveur DHCP répond ensuite directement à l'interface L3 qui a transféré ce paquet DHCP. Avec le proxy DHCP, c'est la même idée, mais tout le transfert est fait directement au niveau du contrôleur au lieu de l'interface L3 du VLAN. Par exemple, une requête DHCP arrive dans le WLAN à partir du client, le WLAN utilise alors le serveur DHCP défini sur l'interface du VLAN *ou* utilise la fonction de remplacement DHCP du WLAN afin de transférer un paquet DHCP monodiffusion au serveur DHCP avec le champ GIADDR de paquets DHCP rempli pour être l'adresse IP de l'interface VLAN.

Serveur DHCP interne - Flux de paquets

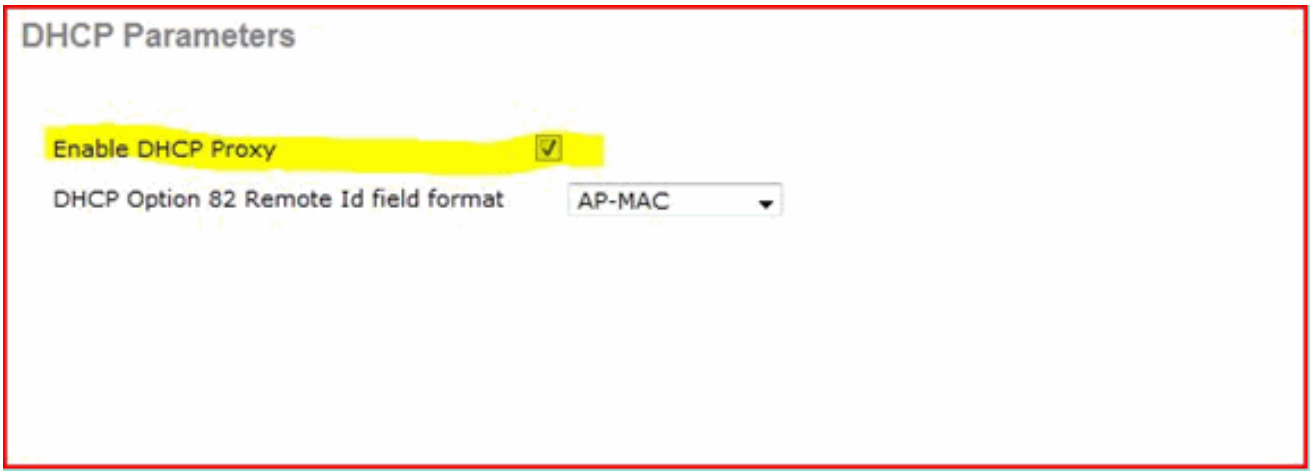


Exemple de configuration d'un serveur DHCP interne

Vous devez activer le proxy DHCP sur le contrôleur afin de permettre au serveur DHCP interne de fonctionner. Vous pouvez le faire via l'interface utilisateur graphique dans cette section :

Remarque : vous ne pouvez pas définir le proxy DHCP via l'interface utilisateur graphique dans toutes les versions.

`Controller->Advanced->DHCP`

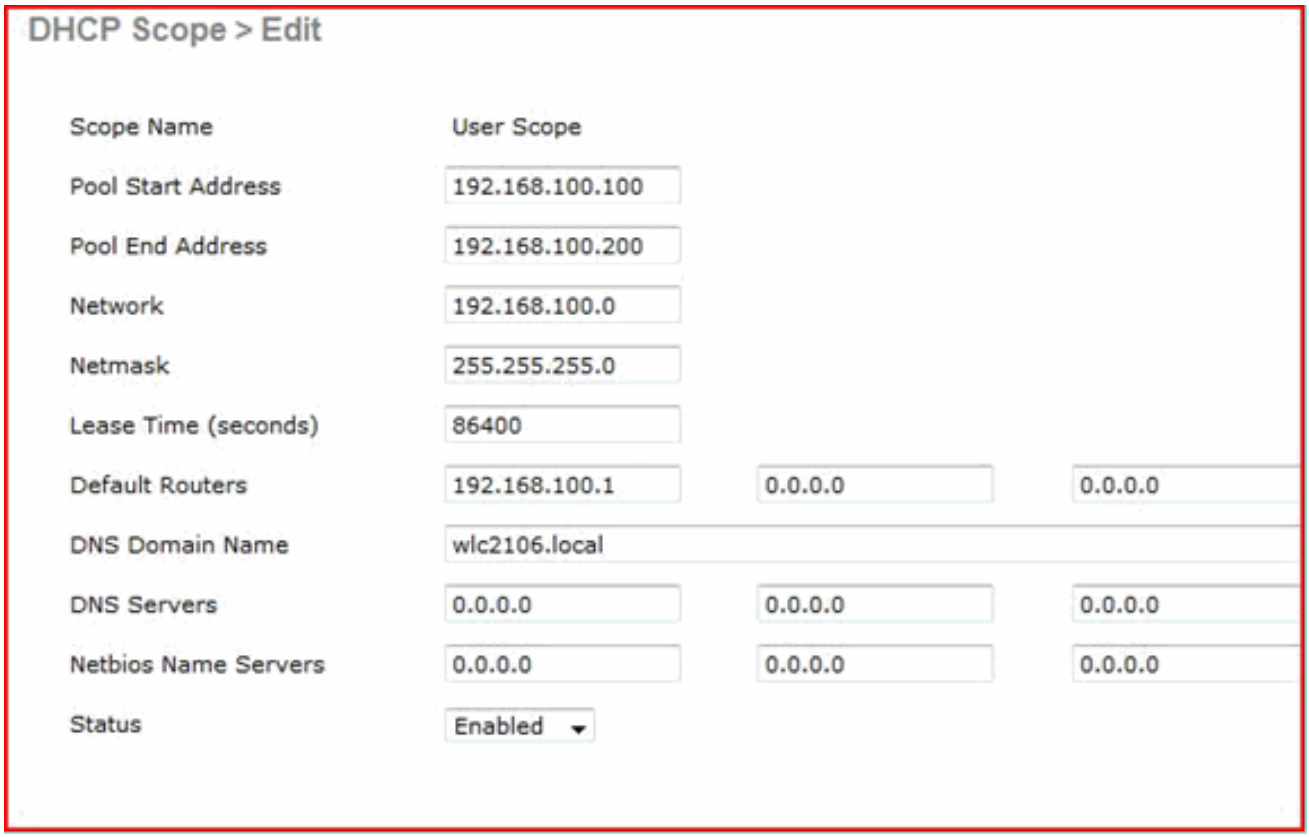


Ou via la CLI :

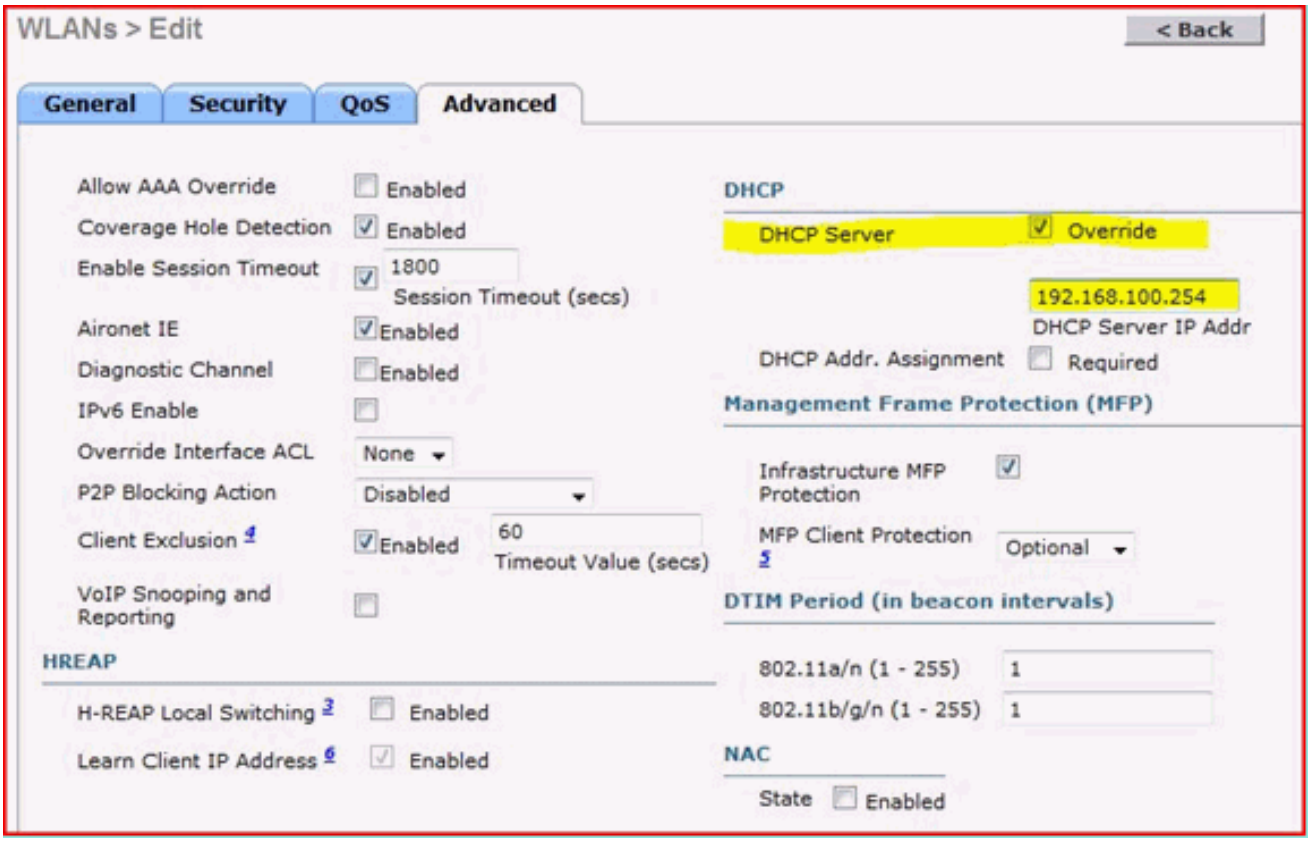
```
Config dhcp proxy enable
Save config
```

Afin d'activer le serveur DHCP interne, complétez ces étapes :

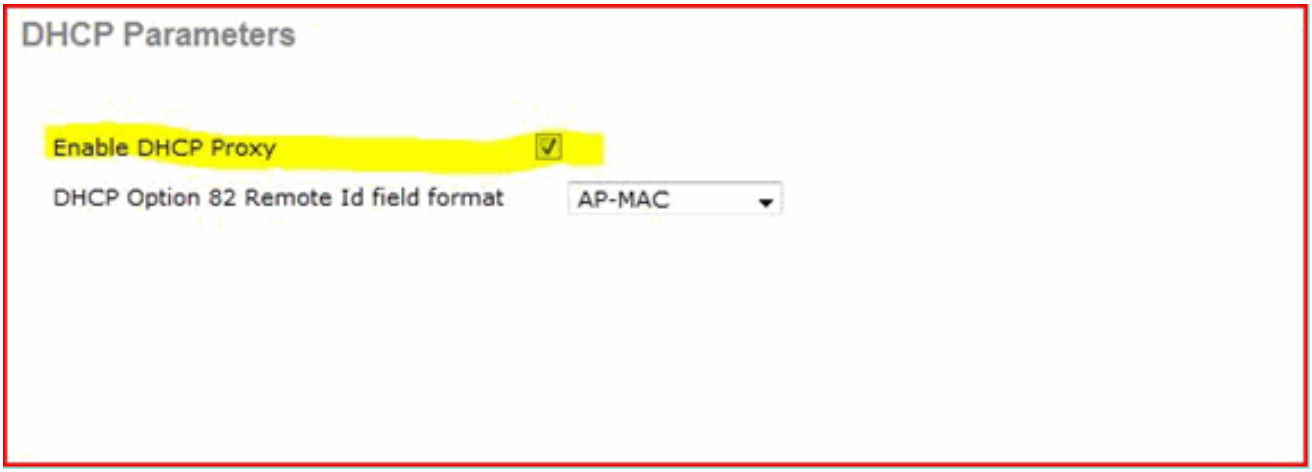
1. Définissez une étendue que vous utilisez afin d'extraire les adresses IP (Controller > Internal DHCP Server > DHCP Scope). Cliquez sur New.



2. Pointez soit votre remplacement DHCP vers l'adresse IP de l'interface de gestion de votre contrôleur.



3. Assurez-vous que le proxy DHCP est activé.



Dépannage

Un débogage du serveur DHCP interne nécessite généralement de trouver un client qui rencontre un problème pour obtenir une adresse IP. Vous devez exécuter ces débogages.

```
debug client <MAC ADDRESS OF CLIENT>
```

Le client de débogage est une macro qui active ces débogages pour vous tandis qu'il concentre le débogage uniquement sur l'adresse MAC du client que vous avez entrée.

```
debug dhcp packet enable
debug dot11 mobile enable
debug dot11 state enable
debug dot1x events enable
debug pem events enable
debug pem state enable
debug cckm client debug enable
```

La principale pour les problèmes DHCP est la commande debug dhcp packet enable qui est activée automatiquement par la commande debug client.

<#root>

```
00:1b:77:2b:cf:75 dhcpd: received DISCOVER
```

```
00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67
  from 127.0.0.1:1067

00:1b:77:2b:cf:75 sendto (548 bytes) returned 548
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 312

00:1b:77:2b:cf:75 DHCP option: message type = DHCP OFFER

00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254
00:1b:77:2b:cf:75 DHCP option: lease time = 86400 seconds
00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping
00:1b:77:2b:cf:75 DHCP option: netmask = 255.255.255.0
00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 81

00:1b:77:2b:cf:75 DHCP option: message type = DHCP REQUEST

00:1b:77:2b:cf:75 DHCP option: 61 (len 7) - skipping
00:1b:77:2b:cf:75 DHCP option: requested ip = 192.168.100.100
00:1b:77:2b:cf:75 DHCP option: server id = 192.0.2.10
00:1b:77:2b:cf:75 DHCP option: 12 (len 14) - skipping
00:1b:77:2b:cf:75 DHCP option: vendor class id = MSFT 5.0 (len 8)
00:1b:77:2b:cf:75 DHCP option: 55 (len 11) - skipping
00:1b:77:2b:cf:75 DHCP option: 43 (len 3) - skipping
00:1b:77:2b:cf:75 DHCP options end, len 81, actual 73
00:1b:77:2b:cf:75 DHCP Forwarding packet locally (340 octets) from 192.168.100.254 to
 192.168.100.254
dhcpd: Received 340 byte dhcp packet from 0xfe64a8c0 192.168.100.254:68

00:1b:77:2b:cf:75 dhcpd: packet 192.168.100.254 -> 192.168.100.254 using scope "User Scope"

00:1b:77:2b:cf:75 dhcpd: received REQUEST

00:1b:77:2b:cf:75 Checking node 192.168.100.100  Allocated 1246985143, Expires 1247071543
 (now: 1246985143)
00:1b:77:2b:cf:75 dhcpd: server_id = c0a864fe
00:1b:77:2b:cf:75 dhcpd: server_id = c0a864fe adding option 0x35 adding option 0x36
 adding option 0x33 adding option 0x03 adding option 0x0f adding option 0x01

00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67
  from 127.0.0.1:1067
```

```
00:1b:77:2b:cf:75 sendto (548 bytes) returned 548
00:1b:77:2b:cf:75 DHCP option len (including the magic cookie) 312
00:1b:77:2b:cf:75 DHCP option: message type = DHCP ACK
00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254
00:1b:77:2b:cf:75 DHCP option: lease time = 86400 seconds
00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping
00:1b:77:2b:cf:75 DHCP option: netmask = 255.255.255.0
00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64
```

Effacer les baux DHCP sur le serveur DHCP interne du WLC

Vous pouvez émettre cette commande afin d'effacer les baux DHCP sur le serveur DHCP interne du WLC :

<#root>

config dhcp clear-lease <all/IP Address>

Voici un exemple :

<#root>

config dhcp clear-lease all

Mises en garde

- Le proxy DHCP doit être activé pour que le serveur DHCP interne fonctionne
- Utilisation de DHCP sur le port 1067 lorsque vous utilisez le serveur DHCP interne, qui est affecté par la liste de contrôle d'accès du processeur
- Le serveur DHCP interne écoute l'interface de bouclage du contrôleur via le port UDP 127.0.0.1 67

Interface utilisateur

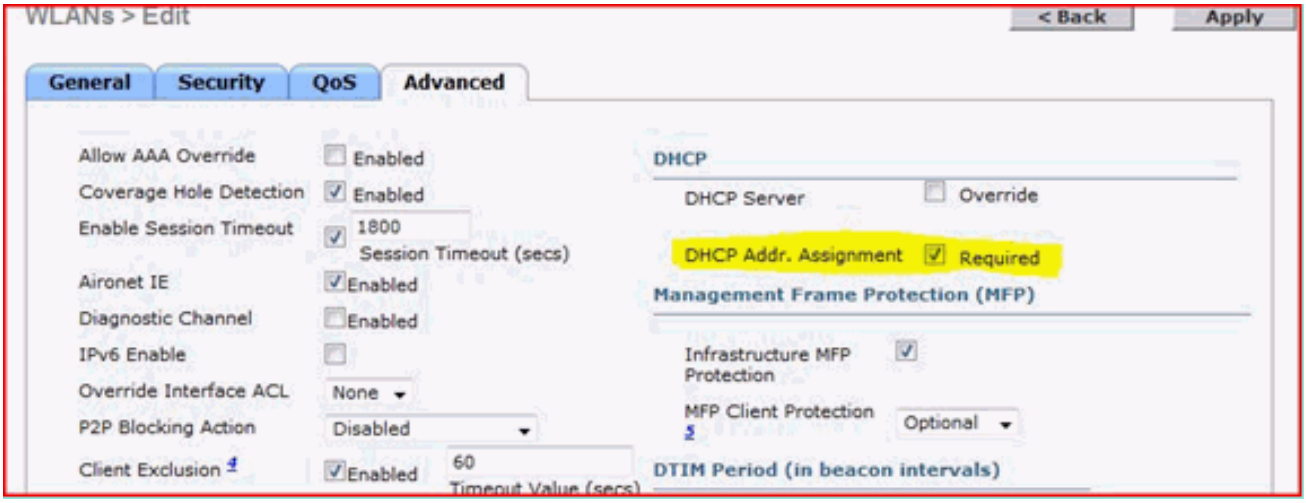
- La **config dhcp proxy disable** commande implique l'utilisation de la fonction de pontage DHCP. Il s'agit d'une commande globale (et non d'une commande par WLAN).
- Le proxy DHCP reste activé par défaut.
- Lorsque le proxy DHCP est désactivé, le serveur DHCP interne ne peut pas être utilisé par les WLAN locaux. L’opération de pontage n’est pas cohérente avec les opérations requises

pour rediriger un paquet vers le serveur interne. Le pontage signifie vraiment le pontage, à l'exception de la conversion 802.11 en Ethernet II. Les paquets DHCP sont transmis sans modification du tunnel LWAPP au VLAN client (et vice-versa).

- Lorsque le proxy est activé, un serveur DHCP doit être configuré sur l'interface du WLAN (ou dans le WLAN lui-même) pour que le WLAN soit activé. Aucun serveur ne doit être configuré lorsque le proxy est désactivé, car ces serveurs ne sont pas utilisés.
- Lorsqu'un utilisateur tente d'activer le proxy DHCP, vous vérifiez en interne qu'un serveur DHCP est configuré sur tous les WLAN (ou interfaces associées). Dans le cas contraire, l'opération d'activation échoue.

DHCP requis

La configuration WLAN avancée comporte une option qui exige que les utilisateurs passent DHCP avant de passer à l'état RUN (état dans lequel le client peut faire passer le trafic par le contrôleur). Cette option exige que le client effectue une requête DHCP complète ou partielle. La principale chose que le contrôleur recherche du client est une requête DHCP et un ACK qui revient du serveur DHCP. Tant que le client effectue ces étapes, il passe l'étape DHCP requise et passe à l'état RUN.



Itinérance C2 et C3

Itinérance de couche 2 : si le client dispose d'un bail DHCP valide et effectue une itinérance de couche 2 entre deux contrôleurs différents sur le même réseau de couche 2, le client ne doit pas avoir à renouveler le protocole DHCP et l'entrée du client doit être complètement déplacée du contrôleur d'origine vers le nouveau contrôleur. Ensuite, si le client a besoin de DHCP à nouveau, le processus de pontage ou de proxy DHCP sur le contrôleur actuel ponte de nouveau le paquet de manière transparente.

Itinérance de couche 3 : dans un scénario d'itinérance de couche 3, le client se déplace entre deux contrôleurs différents dans des réseaux de couche 3 différents. Dans cette situation, le client est ancré au contrôleur d'origine et répertorié dans la table des clients sur le nouveau contrôleur étranger. Pendant le scénario d'ancrage, le DHCP client est géré par le contrôleur d'ancrage

tandis que les données client sont tunnellisées dans un tunnel EoIP entre les contrôleurs d'ancrage et les contrôleurs étrangers.

Informations connexes

- Exemple de configuration de DHCP OPTION 43 basculement pour les points d'accès légers Cisco Aironet
- Assistance et documentation techniques - Cisco Systems

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.