DHCP avec contrôleur de réseau local sans fil

Contenu

Introduction

Ce document décrit les différents fonctionnements de DHCP sur le contrôleur sans-fil, qui fournissent cohérent et les informations précises aux administrateurs qui regardent pour dépanner leur réseau.

Serveur DHCP externe

Le contrôleur LAN Sans fil (WLC) prend en charge deux modes des fonctionnements de DHCP au cas où un serveur DHCP externe serait utilisé :

- Mode proxy DHCP

- DHCP jetant un pont sur le mode

Le mode proxy DHCP sert de fonction d'aide DHCP afin de réaliser une meilleurs Sécurité et contrôle des transactions DHCP entre le serveur DHCP et les clients sans fil. Le DHCP jetant un pont sur le mode fournit une option de rendre le rôle du contrôleur dans une transaction DHCP entièrement transparent aux clients sans fil.

Comparaison de proxy DHCP et de modes de transition

Manipulation du DHCP de client	Mode proxy DHCP	DHCP jeta pont sur le mode
Modifiez le giaddr	Oui	Non
Modifiez le siaddr	Oui	Non
Modifiez le contenu de paquet	Oui	Non
Offres redondantes non expédiées	Oui	Non
Support de l'option 82	Oui	Non
Émission à l'unicast	Oui	Non
Support de Protocole BOOTP	Non	Serveur
RFC non-conforme	Le proxy et l'agent de relais ne sont pas exactement le même concept. Le DHCP jetant un pont sur le mode est recommandé pour la totale conformité RFC.	Non

Mode proxy DHCP

Le proxy DHCP n'est pas idéal pour tous les environnements de réseau. Le contrôleur modifie et transmet par relais toutes les transactions DHCP pour fournir la fonction d'aide et pour aborder certains problèmes de sécurité.

L'adresse IP virtuelle du contrôleur est normalement utilisée comme adresse IP source de toutes les transactions DHCP au client. En conséquence, la vraie adresse IP de serveur DHCP n'est pas exposée dans le ciel. Cet IP virtuel est affiché dans la sortie de débogage pour des transactions DHCP sur le contrôleur. Cependant, l'utilisation d'une adresse IP virtuelle peut entraîner des questions sur certains types de clients.

L'exécution de mode proxy DHCP met à jour le même comportement pour des protocoles symétriques et asymétriques de mobilité.

Quand le multiple offre les serveurs DHCP externes provenus, le proxy DHCP sélectionne normalement le premier qui entre et place l'adresse IP du serveur dans la structure de données de client. En conséquence, toutes les transactions suivantes passent par le même serveur DHCP jusqu'à ce qu'une transaction échoue après des relances. En ce moment, le proxy sélectionne un serveur DHCP différent pour le client.

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

> Remarque: Le proxy DHCP doit être activé afin de l'option 82 DHCP de fonctionner correctement.

Écoulement de paquet de proxy

Capture de paquet de proxy

Quand le contrôleur est dans le mode proxy DHCP, il dirige non seulement des paquets DHCP vers le serveur DHCP, il construit réellement de nouveaux paquets DHCP pour expédier au serveur DHCP. Toutes les options DHCP qui sont présentes dans des paquets DHCP du client sont copiées dans des paquets DHCP du contrôleur. Les exemples de tir d'écran suivant affichent ceci pour un paquet de requête DHCP.

Point de vue de client

Ce tir d'écran est d'une capture de paquet prise du point de vue du client. Il affiche qu'un DHCP les découvrent, offre DHCP, requête DHCP, et un DHCP ACK. La requête DHCP est mise en valeur et le détail de protocole de BOOTP est développé, qui affiche les options DHCP.

Point de vue de serveur

Ce tir d'écran est d'une capture de paquet prise du point de vue du serveur. Semblable à l'exemple précédent, il affiche qu'un DHCP les découvrent, offre DHCP, requête DHCP, et un DHCP ACK. Cependant, ce sont des paquets que le contrôleur a construits en fonction du proxy DHCP. De nouveau, la requête DHCP est mise en valeur et le détail de protocole de BOOTP est développé, qui affiche les options DHCP. Notez qu'ils sont identiques que dans le paquet de requête DHCP de clients. Notez également que le proxy WLC transmet par relais des adresses de paquet et de paquet de point culminant.

Exemple de configuration de proxy

Afin d'utiliser le contrôleur comme proxy DHCP, la caractéristique de proxy DHCP doit être activée sur le contrôleur. Par défaut, cette caractéristique est activée. Afin d'activer le proxy DHCP, cette commande CLI peut être utilisée. Le même est disponible dans le GUI dans la page de contrôleur dans le menu DHCP.

```
(Cisco Controller) >config dhcp proxy enable (Cisco Controller) >show dhcp proxy DHCP Proxy
Behavior: enabled
```

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

```
(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>
```

Le DHCP jetant un pont sur la caractéristique est un paramètre général, ainsi il affecte toutes les transactions DHCP dans le contrôleur.

Dépannez

C'est la sortie de la commande d'**enable de paquet de debug dhcp**. Le débogage affiche 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.

```
(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 = 50.101.2.7 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 - 11.0.0.11
(local address 50.101.0.11, gateway 50.101.0.1, 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: 50.101.0.11 Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP requested ip: 50.101.2.7 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 50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REQUEST
to 50.101.0.1
(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: 50.101.0.11 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 = 11.0.0.11 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 =
50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: DNS server, cnt = 1, first =
11.0.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: WINS server, cnt = 1, first =
11.0.0.11 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 11.0.0.11,
yiaddr 50.101.2.7) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 Assigning Address 50.101.2.7 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: 50.101.2.7 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: 1.1.1.1 rcvd server id: 11.0.0.11
```

Mises en garde

- Les problèmes d'interopérabilité peuvent exister entre un contrôleur avec le proxy DHCP activé et les périphériques qui agissent en tant que Pare-feu et serveur DHCP. C'est très probablement dû au composant de Pare-feu du périphérique car les Pare-feu généralement ne répondent pas aux demandes de proxy. Le contournement pour cette question est de désactiver le proxy DHCP sur le contrôleur.
- Quand un client est dans l'état DHCP REQ sur le contrôleur, le DHCP de baisses de contrôleur informent des paquets. Le client n'entrera pas dans un état de PASSAGE sur le contrôleur (ceci est exigé pour que le client passe le trafic) jusqu'à ce qu'il reçoive un DHCP découvrent le paquet du client. Le DHCP informent des paquets sont expédiés par le contrôleur quand le proxy DHCP est désactivé.
- Tous les contrôleurs qui communiqueront doivent avoir le même paramètre de proxy DHCP.

DHCP jetant un pont sur le mode

Le DHCP jetant un pont sur la caractéristique est conçu pour rendre le rôle du contrôleur dans la transaction DHCP entièrement transparent au client. Excepté le 802.11 à la conversion d'Ethernet II, des paquets du client pont non modifiés du tunnel de Protocol de point d'accès léger (LWAPP) au VLAN du client (ou des Ethernets au-dessus de tunnel IP (EoIP) dans le cas d'itinérance L3). De même, excepté Ethernet II à la conversion de 802.11, des paquets en client pont non modifiés du VLAN du client (ou du tunnel d'EoIP dans le cas d'itinérance L3) au tunnel LWAPP. Pensez à ceci en tant que câblage d'un client dans un switchport et le client puis exécutez une transaction traditionnelle DHCP.

Exécutions de transition DHCP - Transition de l'écoulement de paquet

Jetant un pont sur la capture de paquet - Point de vue de client

Dans le tir d'écran de capture de paquet de côté client, la principale différence entre le client que la capture dans le mode proxy est le vrai IP du serveur DHCP est vue dans les paquets d'offre et ACK au lieu de l'adresse IP virtuelle du contrôleur.

Jetant un pont sur la capture de paquet - Point de vue de serveur

Dans le tir d'écran de câble de capture de paquet vous pouvez voir que le paquet 40 est l'émission traversière de requête DHCP du client 00:40:96:b6:44:51 de test au réseau câblé.

Transition de l'exemple de configuration

Afin d'activer le DHCP jetant un pont sur la fonctionnalité sur le contrôleur, vous devez désactiver la configuration de proxy DHCP sur le contrôleur. Ceci peut seulement être accompli dans le CLI avec ces commandes :

```
(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 la couche 2 (L2) comme le client alors

que l'émission devra être expédiée au serveur DHCP à la passerelle de client utilisant une aide IP. C'est un échantillon de cette configuration :

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

Le DHCP jetant un pont sur la caractéristique est un paramètre général, ainsi il affecte toutes les transactions DHCP dans le contrôleur. Vous devez ajouter des déclarations d'aide IP dans l'infrastructure câblée pour tous les VLAN nécessaires sur le contrôleur.

Dépannez

Met au point répertorié ici ont été activés sur le contrôleur CLI et la partie DHCP de la sortie a été extraite pour ce document.

```
(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 principales que la transition DHCP est en service sur le contrôleur :

Le DHCP a avec succès jeté un pont sur le paquet au DS - Ceci signifie que le paquet DHCP d'origine du client pont, inchangé au système de distribution (DS). Le DS est l'infrastructure câblée.

Le DHCP a avec succès jeté un pont sur le paquet à STA - Ce message indique que le paquet DHCP pont, inchangé à la station (STA). Le STA est la machine cliente qui demande le DHCP.

En outre, vous voyez que l'adresse IP du serveur réelle répertoriée dans met au point, qui est 192.168.10.1. Si le proxy DHCP était en service au lieu du DHCP jetant un pont sur, vous verriez l'adresse IP virtuelle du contrôleur répertoriée pour l'adresse IP du serveur.

Mises en garde

- Par défaut, le proxy DHCP est activé.
- Tous les contrôleurs qui communiqueront doivent avoir le même paramètre de proxy DHCP.
- Le proxy DHCP doit être activé pour l'option 82 DHCP de fonctionner.

Serveur DHCP interne

Le serveur DHCP interne a été introduit au commencement pour des succursales où un serveur DHCP externe n'est pas disponible. Il est conçu pour prendre en charge un petit réseau Sans fil à moins de dix Points d'accès (aps) que soyez sur le même sous-réseau. Le serveur interne fournit des adresses IP aux clients sans fil, les aps liés directement, l'appliance-mode aps sur l'interface de gestion, et les requêtes DHCP qui sont transmises par relais des aps. Ce n'est pas un véritable serveur DHCP d'usage universel. Il prend en charge seulement la fonctionnalité limitée et ne la mesurera pas dans un plus grand déploiement.

Comparaison des modes internes DHCP et de transition

Les deux modes principaux DHCP sur le contrôleur sont proxy DHCP ou transition DHCP. Avec le DHCP jetant un pont sur le contrôleur agit plutôt un DHCP de retour avec des aps autonomes. Un paquet DHCP entre dans AP par l'intermédiaire d'une association de client à un Identifiant SSID (Service Set Identifier) qui est liée à un VLAN. Puis, le paquet DHCP sort ce VLAN. Si une aide IP est définie sur la passerelle de la couche 3 de ce VLAN (L3), le paquet est expédié à ce serveur DHCP par l'intermédiaire de l'unicast dirigé. Le serveur DHCP répond alors de retour directement à l'interface L3 qui a expédié ce paquet DHCP. Avec le proxy DHCP, c'est la même idée, mais tout les expédition est fait directement au contrôleur au lieu de l'interface L3 du VLAN. Par exemple, une requête DHCP entre au WLAN du client, le WLAN alors l'un ou l'autre d'utilisation que le serveur DHCP défini sur le *or* de l'interface du VLAN emploiera la fonction de priorité DHCP du WLAN pour expédier un paquet DHCP d'unicast au serveur DHCP avec le champ GIADDR de paquets DHCP complété pour être l'adresse IP de l'interface VLAN.

Serveur DHCP interne - Écoulement de paquet

Exemple interne de configuration du serveur DHCP

Vous devez permettre au proxy DHCP sur le contrôleur afin de permettre au serveur DHCP interne pour fonctionner. Ceci peut être fait par l'intermédiaire du GUI sous cette section :

> Remarque: Vous ne pouvez pas placer le proxy DHCP par l'intermédiaire du GUI dans toutes les versions.

```
Controller->Advanced->DHCP
```

Ou par l'intermédiaire du CLI :

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

Afin d'activer le serveur DHCP interne, terminez-vous ces étapes :

1. Définissez une portée que vous utiliserez pour tirer des adresses IP (contrôleur > serveur DHCP interne > portée de DHCP). Cliquez sur **New**.
2. Indiquez l'un ou l'autre de votre dépassement DHCP l'adresse IP d'interface de gestion de votre contrôleur.Ou, vous pouvez utiliser l'option DHCP de la configuration d'interface de contrôleur pour l'interface que vous souhaitez utiliser le serveur DHCP interne.
3. Assurez-vous que le proxy DHCP est activé.

Dépannez

Un débogage du serveur DHCP interne est typiquement une question de trouver un client qui a un problème obtenant une adresse IP. Vous devez exécuter ces derniers met au point.

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

Le client de débogage est une macro-instruction qui active ces derniers met au point pour vous tandis qu'elle concentre le débogage seulement sur l'adresse MAC de client que vous avez écrite.

```
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
```

Le principal pour des problèmes de DHCP est la commande d'**enable de paquet de debug dhcp** qui est activée automatiquement par l'ordre de **client de débogage**.

```
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 = 1.1.1.1
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

Effacez 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 :

config dhcp clear-lease *<all/IP Address>*

Voici un exemple :

config dhcp clear-lease *all*

Mises en garde

- Le proxy DHCP doit être activé pour que le serveur DHCP interne fonctionne.
- Utilisation de DHCP au port 1067 quand vous utilisez le serveur DHCP interne, qui est affecté par l'ACL CPU.
- Le serveur DHCP interne écoute sur l'interface de bouclage de contrôleur par l'intermédiaire du port UDP 67 de 127.0.0.1.

Interface d'utilisateur final

- La commande de **débronchement de config dhcp proxy** implique l'utilisation du DHCP jetant un pont sur la fonction. C'est une commande globale (pas une commande par-WLAN).
- Pour que les clients éprouvent à comportement cohérent avec des déploiements existants, le proxy DHCP demeurera activé par défaut.
- Quand le proxy DHCP est désactivé, le serveur DHCP interne ne peut pas être utilisé par les gens du pays WLAN. L'exécution de transition n'est pas compatible aux exécutions exigées pour réorienter un paquet au serveur interne. La transition vraiment signifie la transition, excepté le 802.11 à la conversion d'Ethernet II. Des paquets DHCP sont passés non modifiés du tunnel LWAPP au VLAN du client (et vice-versa).
- Quand 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 quand le proxy est désactivé car ces serveurs ne sont pas utilisés.
- Quand les tentatives d'un utilisateur d'activer le proxy DHCP, vous vérifient intérieurement que tous les WLAN (ou interfaces associées) ont un serveur DHCP configuré. Sinon, l'exécution d'enable échoue.

DHCP requis

La configuration avancée WLAN a une option qui exige des utilisateurs de passer le DHCP avant d'aller dans l'état de PASSAGE (un état où le client pourra passer le trafic par le contrôleur). Cette option exige du client de faire une pleine ou demi requête DHCP. 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 fait ces étapes, le client passe l'étape priée par DHCP et se déplace à l'état de PASSAGE.

Itinérance L2 et L3

L2 errent - Si le client a un bail valide DHCP et exécute un L2 errent entre deux contrôleurs différents sur le même réseau L2, le client ne devrait pas avoir besoin de reDHCP et l'entrée de client devrait être complètement déplacée au nouveau contrôleur du contrôleur d'origine. Puis, si le client a besoin de DHCP de nouveau, le processus de transition DHCP ou de proxy sur le contrôleur en cours jetterait un pont sur d'une manière transparente le paquet de nouveau.

L3 errent - Dans un L3 errez le scénario que le client se déplace entre deux contrôleurs différents dans différents réseaux L3. Dans cette situation le client est ancré au contrôleur d'origine et répertorié dans la table de client sur le nouveau contrôleur étranger. Pendant l'ancrage du scénario le DHCP du client est manipulé par le contrôleur d'ancre pendant que les données de client sont percées un tunnel dans un tunnel d'EoIP entre les contrôleurs étrangers et d'ancre.

Informations connexes

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