Begrijp hoe AireOS WLCs DHCP-protocol verwerkt

Inhoud

Inleiding

Dit document beschrijft de verschillende DHCP-bewerkingen op de Cisco AireOS draadloze controller.

Externe DHCP-server

De wireless LAN-controller (WLC) ondersteunt twee modi van DHCP-bewerkingen wanneer een externe DHCP-server wordt gebruikt:

- DHCP-proxymodus
- DHCP-overbruggingsmodus

De DHCP-proxymodus fungeert als een DHCP-helper voor betere security en controle van DHCP-transacties tussen de DHCP-server en de wireless clients. DHCP-overbruggingsmodus biedt een optie om de

controllerrol in een DHCP-transactie volledig transparant te maken voor de draadloze clients.

Vergelijking van proxymodus en overbruggingsmodus van DHCP

Verwerking van client-DHCP	DHCP-proxymodus	DHCP-overbruggingsmodus
giaddr wijzigen	Ja	Nee
siaddr wijzigen	Ja	Nee
Pakketinhoud wijzigen	Ja	Nee
Redundante aanbiedingen: niet doorgestuurd	Ja	Nee
Ondersteuning voor optie 82	Ja	Nee
Broadcast naar unicast	Ja	Nee
BOOTP-ondersteuning	Nee	Server
Niet-compliant RFC	Proxy en relay agent zijn niet gelijk. De DHCP-overbruggingsmodus wordt aanbevolen voor volledige RFC-compliance.	Nee

DHCP-proxymodus

DHCP-proxy is niet ideaal voor alle netwerkomgevingen. De controller wijzigt alle DHCP-transacties en geeft deze door om de helperfunctie te bieden en bepaalde security problemen aan te pakken.

Het virtuele IP-adres van de controller wordt normaal gebruikt als het IP-adres van alle DHCP-transacties naar de client. Hierdoor wordt het echte IP-adres van de DHCP-server niet vrijgegeven. Deze virtuele IP wordt getoond in output van foutopsporing voor DHCP-transacties op de controller. Het gebruik van een virtueel IP-adres kan echter problemen veroorzaken op bepaalde typen clients.

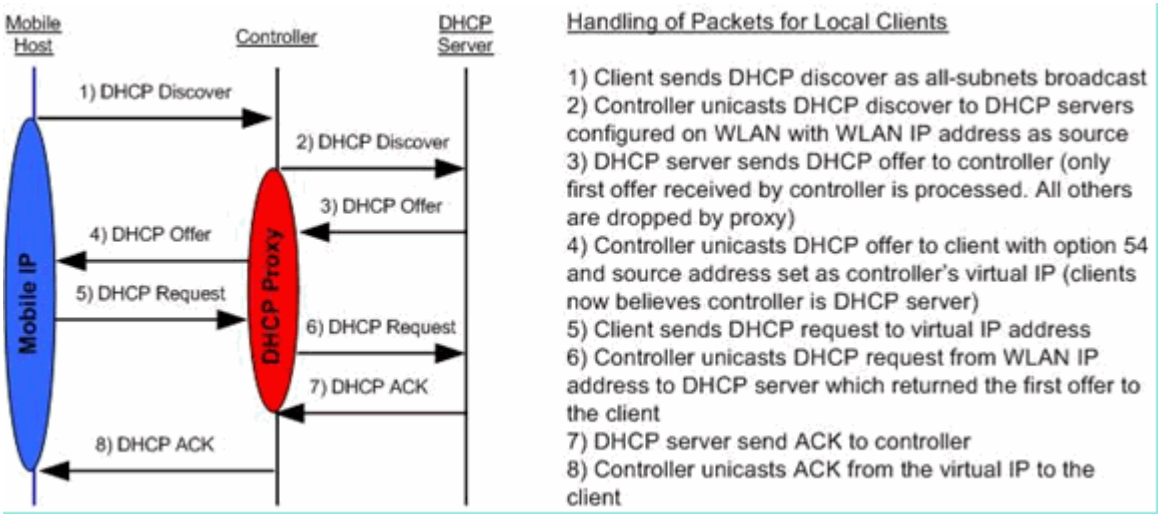
Bij gebruik van de DHCP-proxymodus wordt hetzelfde gedrag getoond bij zowel symmetrische als asymmetrische mobiliteitsprotocollen.

Wanneer meerdere aanbiedingen afkomstig zijn van externe DHCP-servers, selecteert de DHCP-proxy doorgaans de eerste die wordt ontvangen en stelt het IP-adres van de server in de clientdatastructuur in. Dientengevolge, gaan alle verdere transacties door de zelfde server van DHCP tot een transactie ontbreekt nadat opnieuw probeert. De proxy selecteert dan een andere DHCP-server voor de client.

DHCP-proxy is standaard ingeschakeld. Alle controllers die communiceren moeten dezelfde DHCP-proxyinstelling hebben.

Opmerking: DHCP-proxy moet zijn ingeschakeld zodat DHCP-optie 82 correct kan werken.

Proxy-pakketstroom

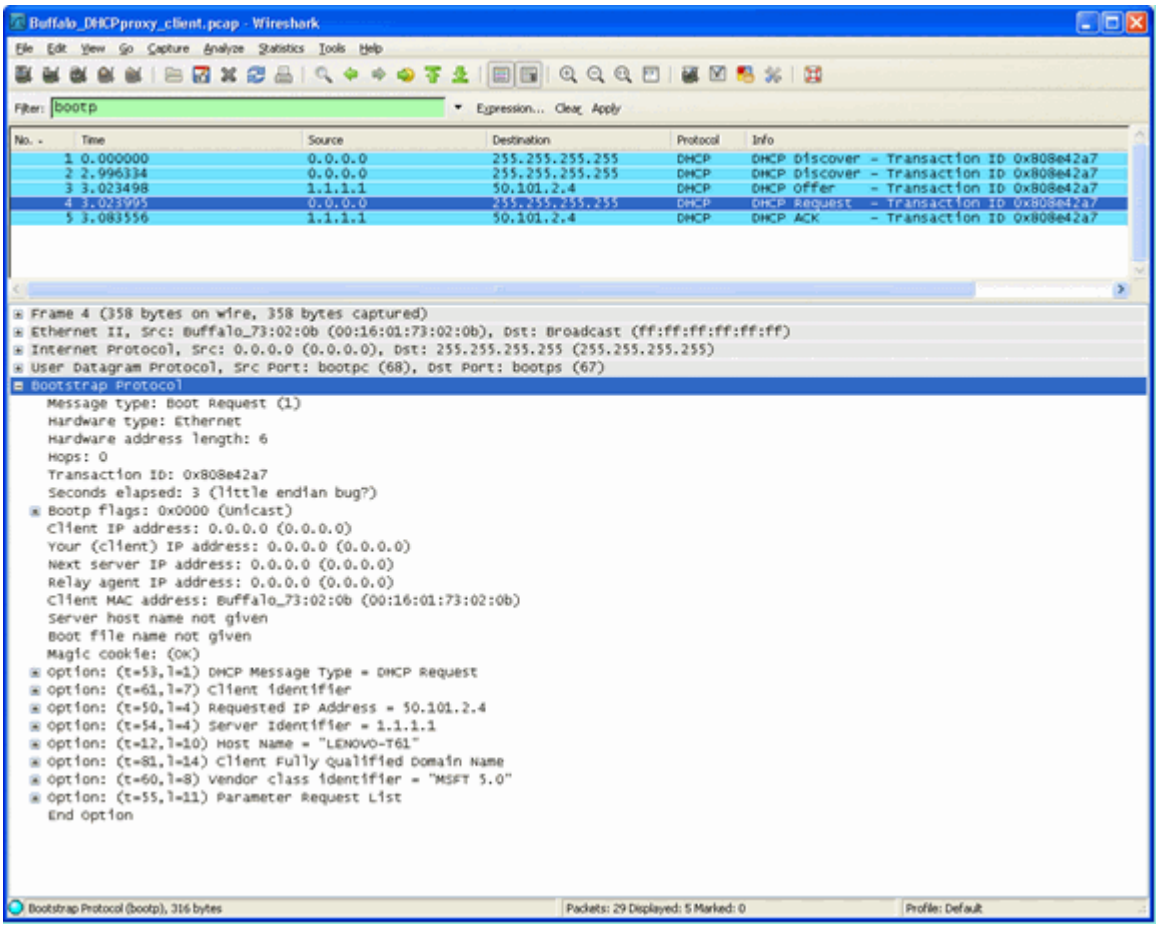


Proxy-pakketvastlegging

Wanneer de controller in DHCP-proxymodus staat, worden niet alleen DHCP-pakketten naar de DHCP-server geleid, maar worden ook nieuwe DHCP-pakketten gemaakt om door te sturen naar de DHCP-server. Alle DHCP-opties die aanwezig zijn in de client-DHCP-pakketten worden gekopieerd in de controller-DHCP-pakketten. In de volgende schermopnamevoorbeelden wordt dit getoond voor een DHCP-aanvraagpakket.

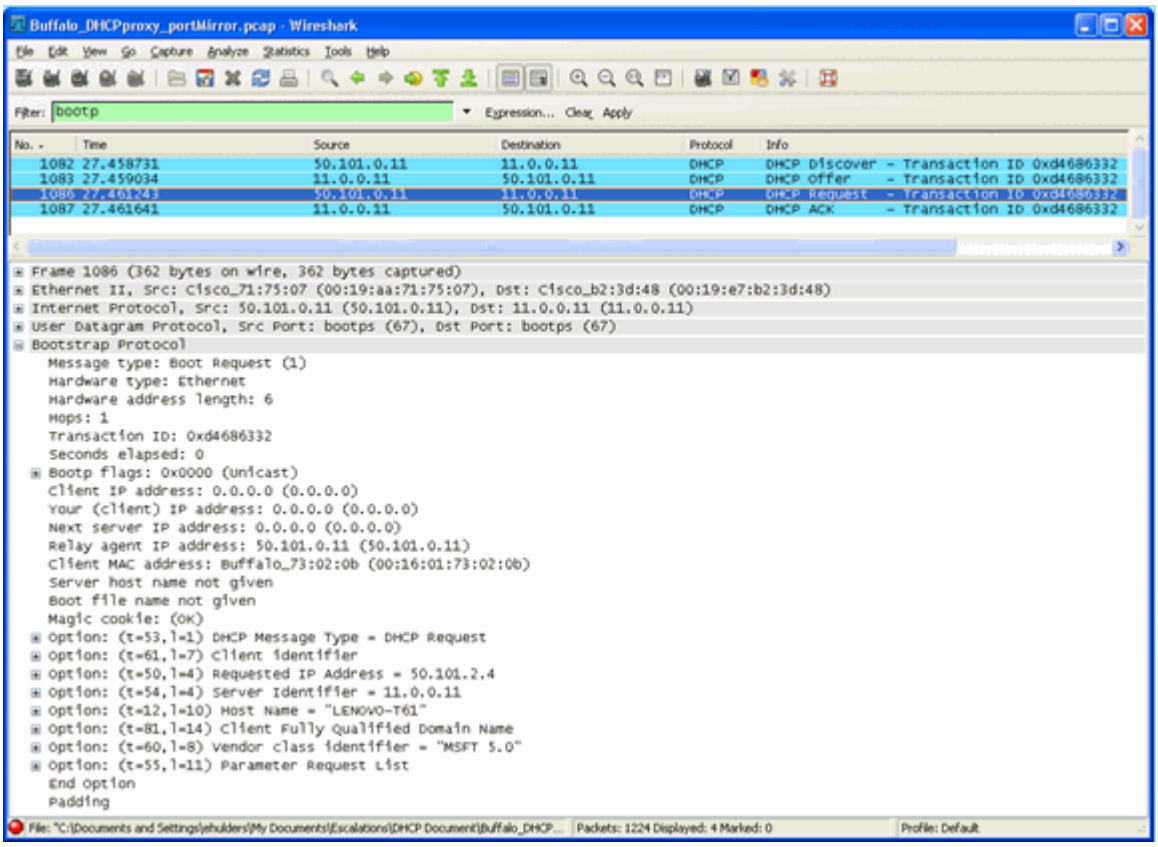
Clientperspectief

Deze screenshot is van een pakketopname die vanuit het clientperspectief is genomen. U ziet een DHCP-detectie, DHCP-aanbieding, DHCP-aanvraag en een DHCP ACK. De DHCP-aanvraag is gemarkeerd en de informatie van het bootstrap-protocol (bootp) is uitgevouwen om de DHCP-opties te tonen.



Serverperspectief

Deze schermopname toont een pakketvastlegging gezien van het perspectief van de server. Net als in het vorige voorbeeld zie u een DHCP-detectie, DHCP-aanbieding, DHCP-aanvraag en een DHCP ACK. Dit zijn echter pakketten die de controller als een functie van DHCP-proxy heeft gemaakt. Net als eerder is de DHCP-aanvraag gemarkeerd en de informatie van het bootstrap-protocol (bootp) uitgevouwen om de DHCP-opties te tonen. Deze zijn gelijk aan die in het DHCP-aanvraagpakket van de client. De WLC-proxy geeft het pakket door en markeert pakketadressen.



Configuratievoorbeeld van proxy

Om de controller als DHCP-proxy te gebruiken, moet de functie DHCP-proxy op de controller zijn ingeschakeld. Deze functie is standaard ingeschakeld. Om DHCP-proxy in te schakelen kan de volgende CLI-opdracht worden gebruikt. Deze opdracht is ook beschikbaar via de grafische gebruikersinterface (GUI) op de pagina Controller in het menu DHCP.

<#root>

```
(Cisco Controller) >
```

config dhcp proxy enable

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behavior: enabled
```

Voor goede werking van DHCP-proxy moet een primaire DHCP-server worden geconfigureerd op elke controller-interface die DHCP-services vereist. Een DHCP-server kan worden geconfigureerd via de beheerinterface, de interface van de AP-manager en dynamische interfaces. Deze CLI-opdrachten kunnen worden gebruikt om voor elke interface een DHCP-server te configureren.

<#root>

```
(Cisco Controller) >
```

config interface dhcp ap-manager primary

```
(Cisco Controller) >
config interface dhcp management primary
```

```
(Cisco Controller) >
config interface dhcp dynamic-interface
```

```
 primary
```

De DHCP-overbruggingsmodus is een algemene instelling en is van toepassing op alle DHCP-transacties op de controller.

Problemen oplossen

Dit is de output van **debug dhcp packet enable** uit. De output toont een controller die een DHCP-aanvraag van een client met MAC-adres 00:40:96:b4:8c:e1 ontvangt, een DHCP-aanvraag doorgeeft aan de DHCP-server, een antwoord van de DHCP-server ontvangt en een DHCP-aanbieding naar de client stuurt.

<#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
```

Voorbehouden

- Er kunnen interoperabiliteitsproblemen bestaan tussen een controller met DHCP-proxy en apparaten die als firewall en als DHCP-server fungeren. Dit is waarschijnlijk te wijten aan de firewallcomponent van het apparaat, aangezien firewalls over het algemeen niet reageren op proxy-aanvragen. De tijdelijke oplossing voor dit probleem is om DHCP-proxy op de controller uit te schakelen.

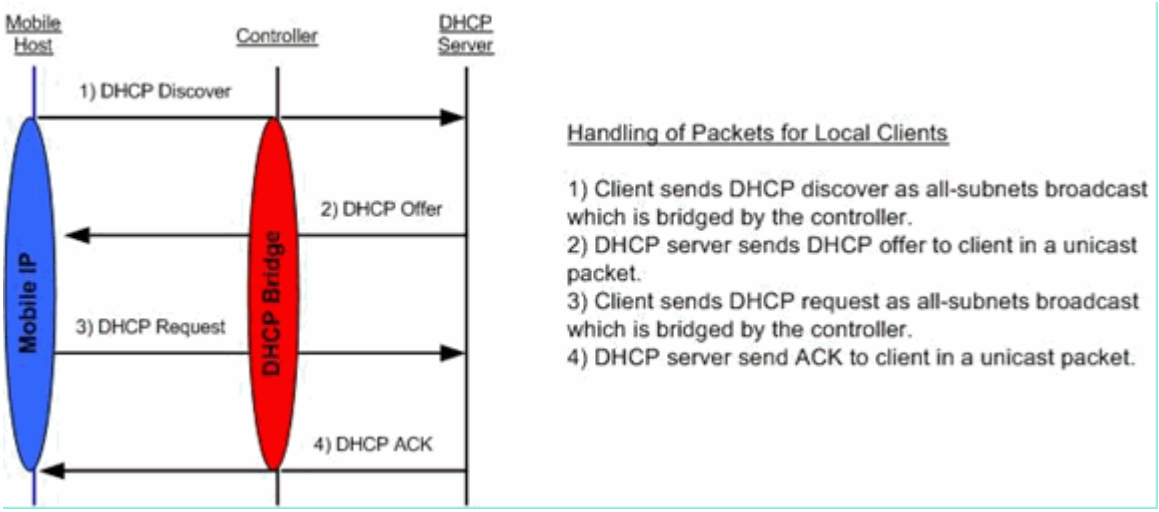
- Wanneer een client op de controller de toestand DHCP REQ heeft, wijst de controller DHCP-informatiepakketten af. De client gaat niet naar een RUN-status op de controller (dit is nodig om de client verkeer door te geven) tot het een DHCP-detectiepakket van de client ontvangt. DHCP-informatiepakketten worden door de controller doorgestuurd wanneer DHCP-proxy is uitgeschakeld.

- Alle controllers die met elkaar communiceren, moeten dezelfde DHCP-proxyinstelling hebben.

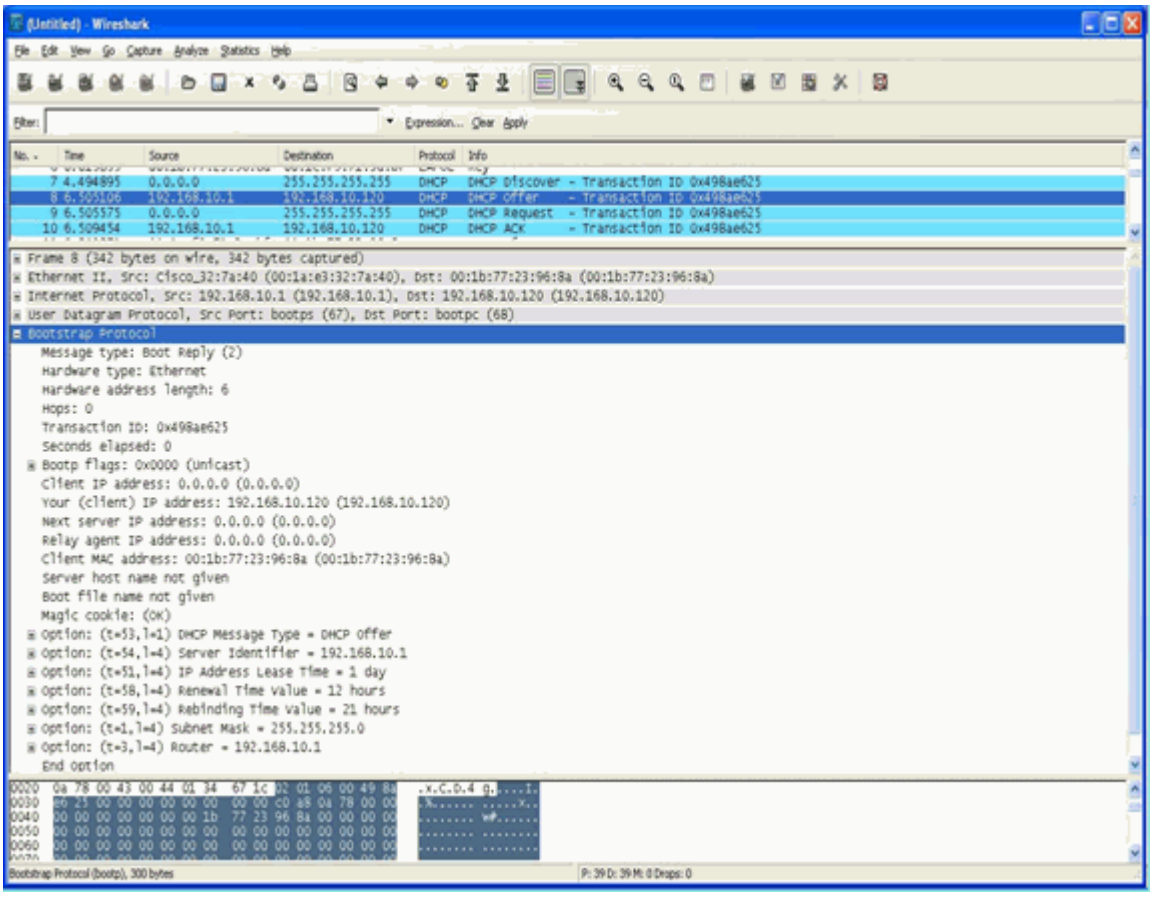
DHCP-overbruggingsmodus

De DHCP-overbruggingsfunctie is ontworpen om de controllerrol in de DHCP-transactie volledig transparant te maken voor de client. Met uitzondering van 802.11 naar Ethernet II-conversie, worden pakketten van de client ongewijzigd overbrugd van de LWAP-tunnel (Light Weight Access Point Protocol) naar de client-VLAN (of Ethernet over IP (EoIP)-tunnel in de L3-roamingcase). Op dezelfde manier, met uitzondering van Ethernet II naar 802.11 conversie, worden pakketten naar de client overbrugd zonder wijzigingen van de client-VLAN (of EoIP-tunnel in de L3 roaming-case) naar de LWAP-tunnel. Een client wordt als het ware via een kabel verbonden met een switchpoort waarna de client een traditionele DHCP-transactie uitvoert.

DHCP-overbruggingsprocessen â€“ overbruggingspakketstroom

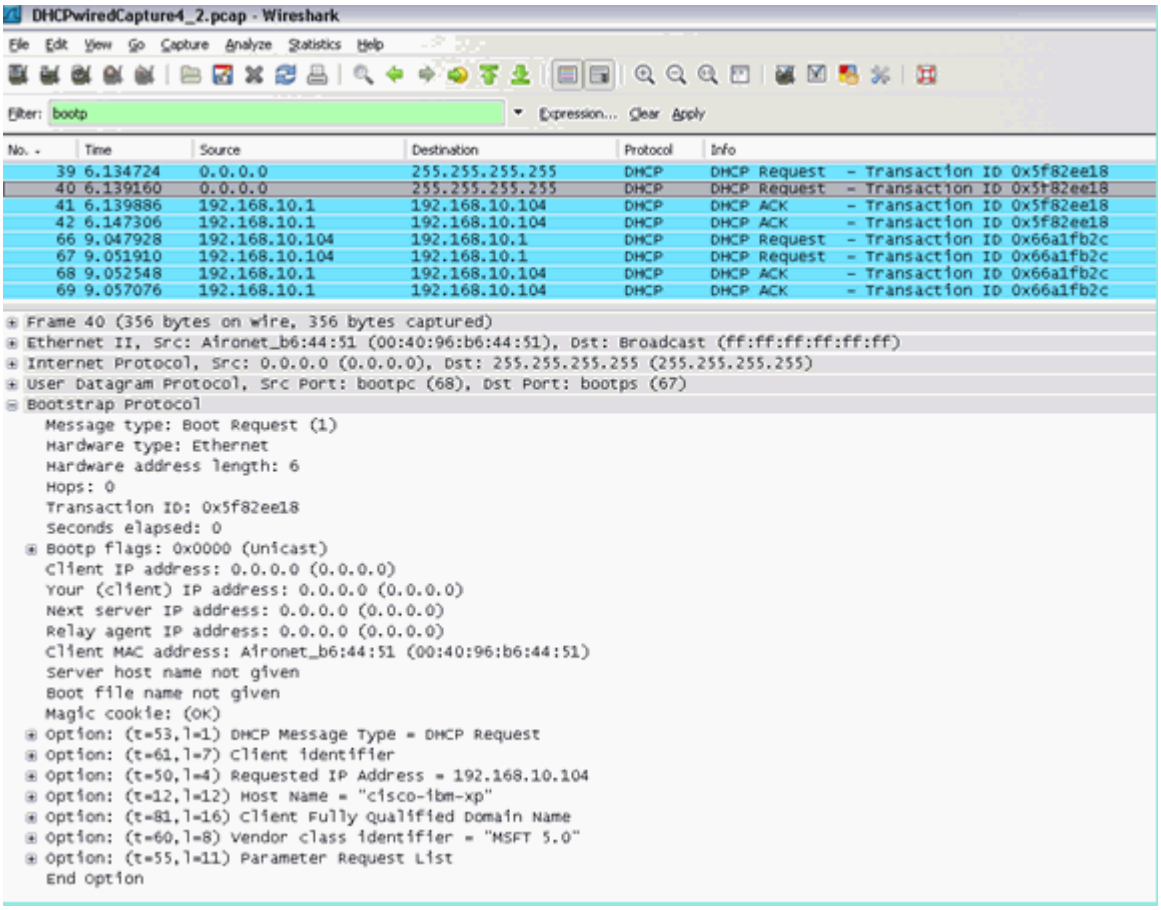


Pakketvastlegging bij overbrugging â€“ clientperspectief



In de screenshot van de pakketopname aan de clientzijde wordt het belangrijkste verschil tussen de clientopname in de proxymodus weergegeven in het echte IP van de DHCP-server in de pakketten Aanbieding en Ack in plaats van het virtuele IP-adres van de controller.

Pakketvastlegging bij overbrugging â€“ serverperspectief



In de schermopname van bekabelde pakketvastlegging kunt u zien dat pakket 40 de overbrugde broadcast is van de DHCP-aanvraag van testclient 00:40:96:b6:44:51 naar het bekabelde netwerk.

Configuratievoorbeeld van overbrugging

Om de DHCP-overbruggingsmodus op de controller te activeren, moet de functie DHCP-proxy op de controller worden uitgeschakeld. Dat kan alleen via de opdrachtregelinterface (CLI) met de volgende opdrachten:

<#root>

```
(Cisco Controller) >
```

config dhcp proxy disable

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behaviour: disabled
```

Als de DHCP-server niet op hetzelfde Layer 2 (L2) netwerk als de client bestaat, moet de uitzending via een IP-helper worden doorgestuurd naar de DHCP-server bij de clientgateway. Hieronder volgt een voorbeeld van deze configuratie:

<#root>

```
Switch#
```

```
conf t

Switch(config)#

interface vlan




Switch(config-if)#

ip helper-address
```

De DHCP-overbruggingsmodus is een algemene instelling en is van toepassing op alle DHCP-transacties op de controller. U moet instructies voor een IP-helper toevoegen in de bekabelde infrastructuur voor alle benodigde VLANâ€™s op de controller.

Problemen oplossen

De hier genoemde debug-opdrachten waren ingeschakeld op de CLI van de controller en het DHCP-gedeelte van de uitvoer werd voor dit document geëxtraheerd.

<#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
```

Deze output van DHCP-foutopsporing bevat enkele belangrijke indicaties dat de DHCP-overbruggingsmodus in gebruik is op de controller:

DHCP successfully bridged packet to DS â€“ geeft aan dat het oorspronkelijke DHCP-pakket van de client via overbrugging ongewijzigd is doorgegegeven aan het distributiesysteem (DS). Het DS is de bekabelde infrastructuur.

DHCP successfully bridged packet to STA â€“ geeft aan dat het DHCP-pakket via overbrugging ongewijzigd is doorgegeven aan het station (STA). Het STA is de clientcomputer die DHCP aanvraagt.

Ook, ziet u het daadwerkelijke server IP adres dat in wordt vermeld debugs, die 192.168.10.1 is. Als DHCP-proxy in gebruik was in plaats van DHCP-overbrugging, ziet u het virtuele IP-adres van de controller dat wordt vermeld voor het IP-adres van de server.

Voorbehouden

- DHCP-proxy is standaard ingeschakeld.
- Alle controllers die met elkaar communiceren, moeten dezelfde DHCP-proxyinstelling hebben.
- DHCP-proxy moet zijn ingeschakeld voor correcte werking van DHCP-optie 82.

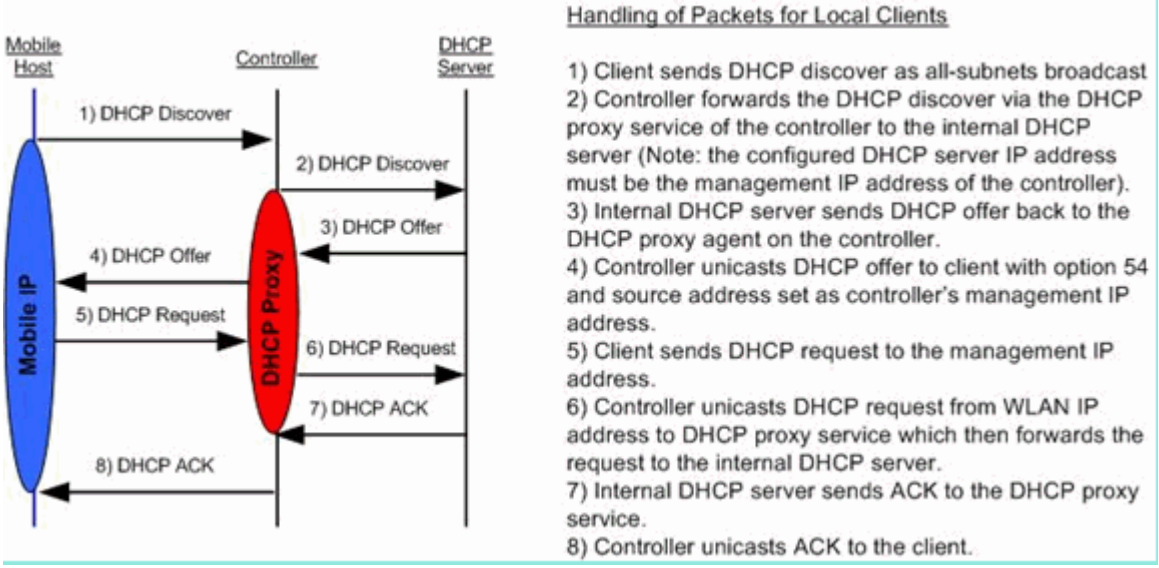
Interne DHCP-server

De interne DHCP-server werd oorspronkelijk ingezet voor nevenvestigingen die geen externe DHCP-server hebben. Deze is ontwikkeld om een klein wireless netwerk met minder dan tien access points (APâ€™s) op hetzelfde subnet. De interne server biedt IP-adressen voor wireless clients, rechtstreeks aangesloten APâ€™s, APâ€™s in applicatiemodus op de beheerinterface en DHCP-aanvragen die via APâ€™s worden doorgegeven. Dit is geen volledige DHCP-server voor algemeen gebruik. Het ondersteunt slechts beperkte functionaliteit en is niet schaalbaar in een grotere inzet.

Vergelijking van proxymodus en overbruggingsmodus van interne DHCP

De twee belangrijkste DHCP-modi op de controller zijn DHCP-proxy en DHCP-overbrugging. In de DHCP-overbruggingsmodus fungeert de controller meer als een DHCP-back-up met autonome APâ€™s. Een DHCP-pakket komt bij een AP via een clientkoppeling met een Service Set Identifier (SSID) die is gekoppeld aan een VLAN. Vervolgens wordt het DHCP-pakket naar dat VLAN gestuurd. Als een IP-helper is gedefinieerd op de L3-gateway (Layer 3) van dat VLAN, wordt het pakket doorgestuurd naar die DHCP-server via gerichte unicast. De DHCP-server reageert dan rechtstreeks naar de L3-interface die door dat DHCP-pakket is doorgestuurd. In de DHCP-proxymodus vindt het doorsturen altijd rechtstreeks via de controller plaats en niet via de L3-interface van het VLAN. Een DHCP-verzoek wordt bijvoorbeeld via het WLAN ingediend vanaf de client. Het WLAN gebruikt vervolgens de DHCP-server die is gedefinieerd op de VLAN-interface *of* gebruikt de DHCP-overschrijvingsfunctie van het WLAN om een unicast DHCP-pakket te verzenden naar de DHCP-server met het veld DHCP-pakketten GIADR., dat is ingevuld als IP-adres van de VLAN-interface.

Interne DHCP-server â€“ pakketstroom

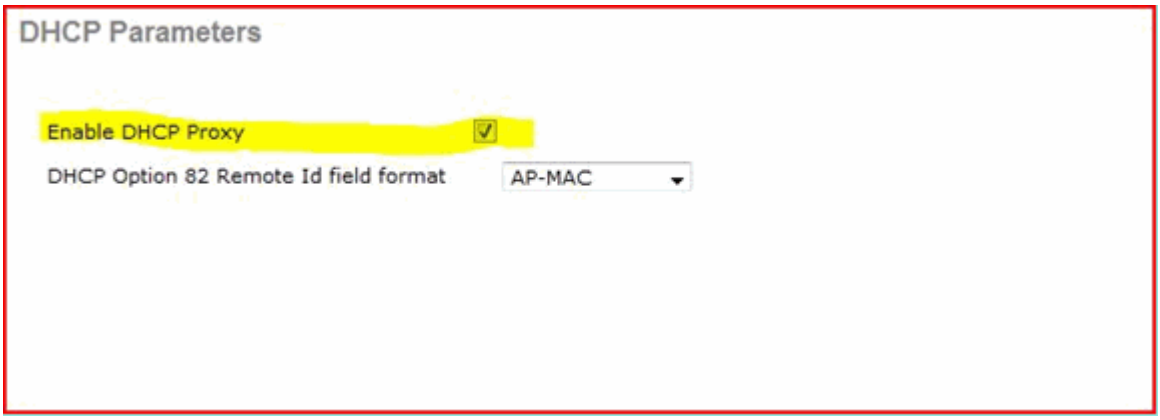


Configuratievoorbeeld van interne DHCP-server

U moet DHCP-proxy op de controller inschakelen om de interne DHCP-server goed te laten functioneren. Dit kan worden gedaan via de GUI:

Opmerking: Het is niet in alle versies mogelijk om DHCP-proxy via de GUI in te schakelen.

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

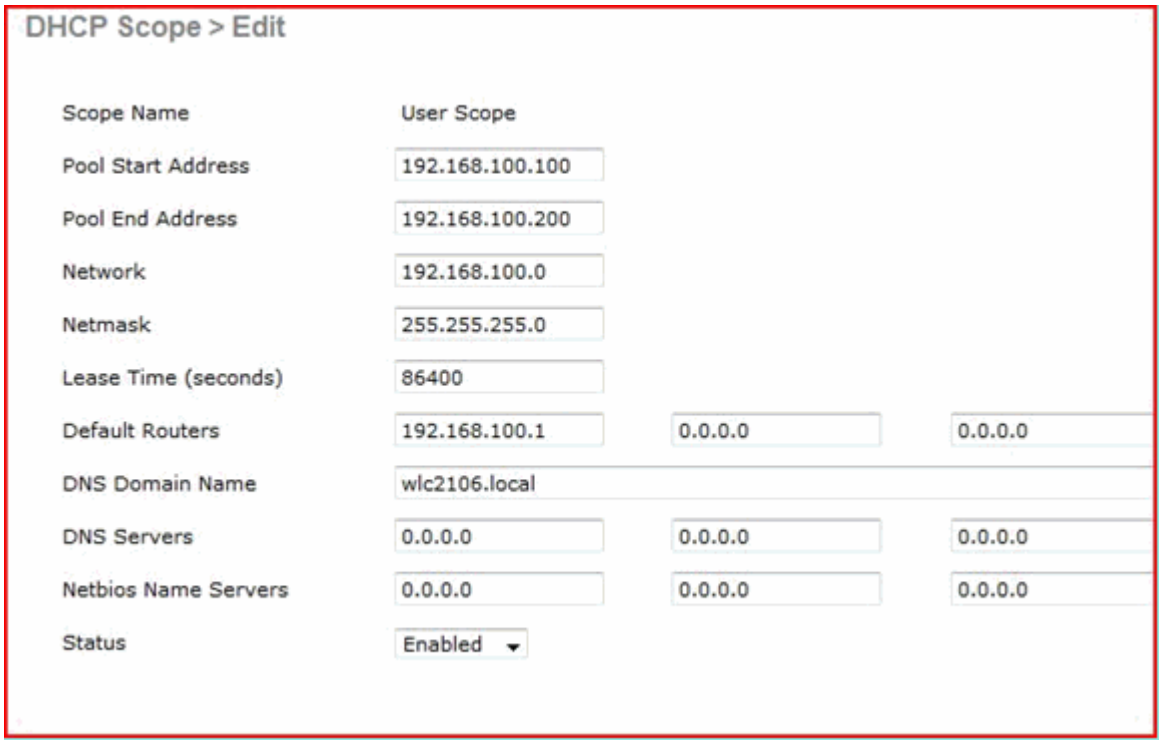


Of via de CLI:

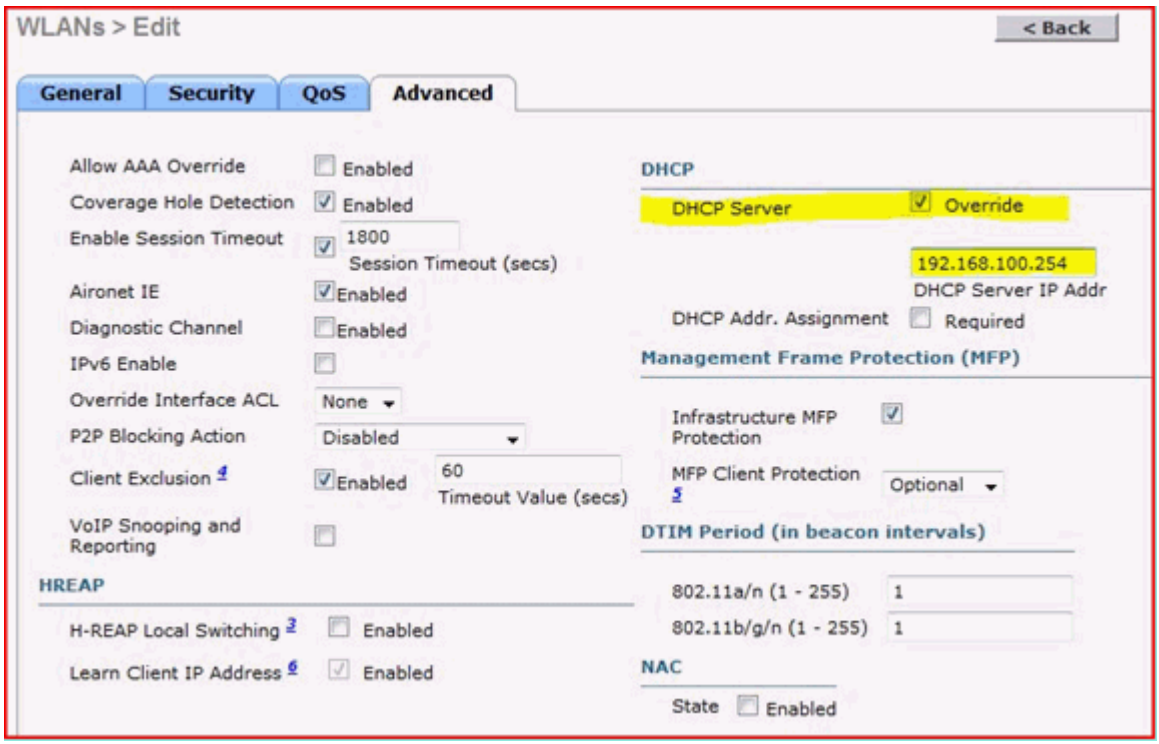
```
Config dhcp proxy enable
Save config
```

Voer de volgende stappen uit om de interne DHCP-server in te schakelen:

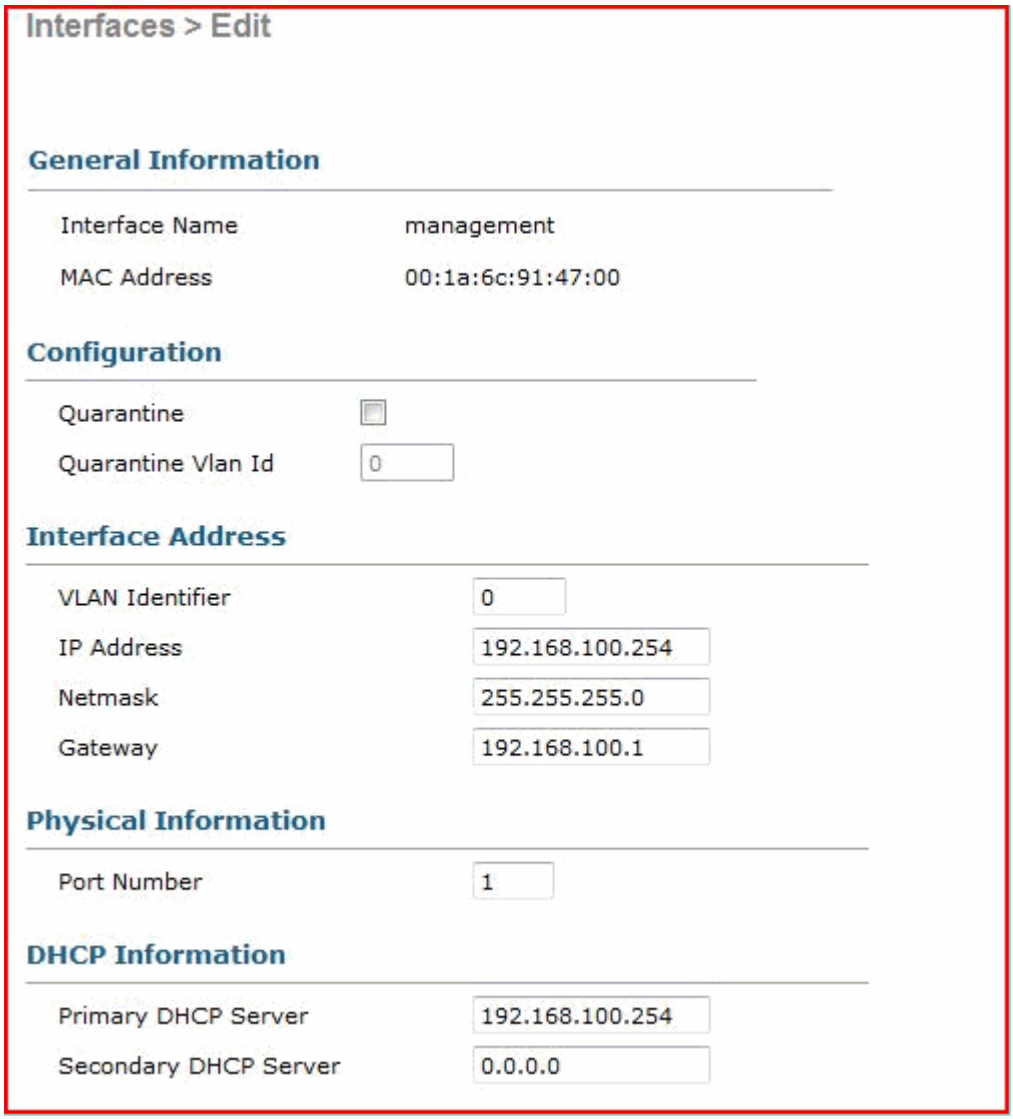
1. Definieer een scope die u gebruikt om IP-adressen (Controller > Interne DHCP-server > DHCP-bereik) op te halen. Klik op **New** (Nieuw).



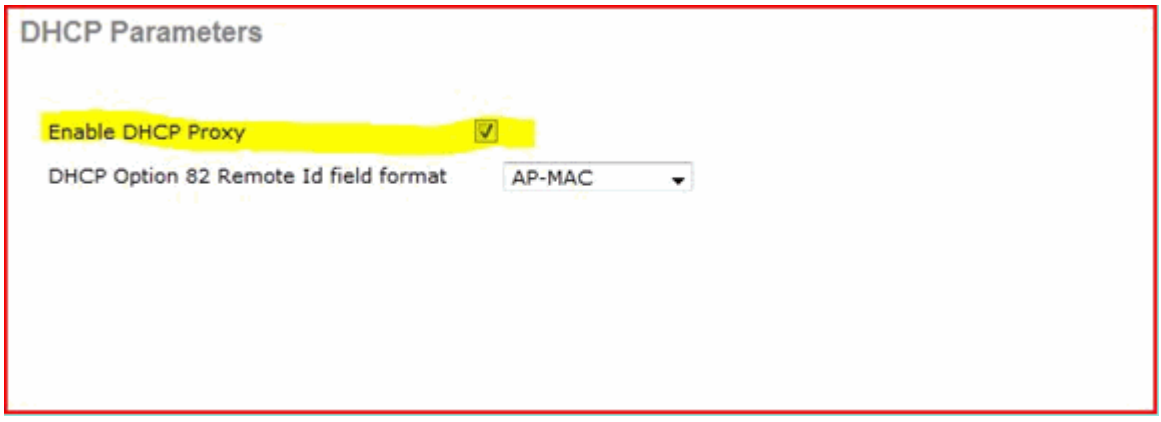
2. Overschrijf ofwel de DHCP-instelling om te verwijzen naar het IP-adres van de beheerinterface van uw controller.



Of gebruik de DHCP-optie van de configuratie van de controller-interface voor de interface die van de interne DHCP-server moet gebruikmaken.



3. Zorg dat DHCP-proxy is ingeschakeld.



Problemen oplossen

Debug van de interne DHCP-server vereist doorgaans om een client te vinden die een probleem heeft om een IP-adres te verkrijgen. Voer de volgende debug-opdrachten uit.

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

De opdracht â€˜debug clientâ€™ is een macro die deze debug-opdrachten mogelijk maakt, waarbij alleen wordt gelet op het MAC-adres van de client dat u heeft ingevoerd.

```
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
```

De belangrijkste voor DHCP-problemen is de **debug dhcp packet enable** bevel dat automatisch door de **debug client** uit.

<#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
```

De DHCP-leases op de WLC Internal DHCP Server wissen

U kunt de volgende opdracht uitvoeren om de DHCP-leases op de interne DHCP-server van de WLC te wissen:

<#root>

```
config dhcp clear-lease
```

Hierna volgt een voorbeeld:

<#root>

```
config dhcp clear-lease all
```

Voorbehouden

- DHCP-proxy moet zijn ingeschakeld om de interne DHCP-server te laten functioneren.
- Gebruik van DHCP naar poort 1067 wanneer u de interne DHCP-server gebruikt, waarop de CPU-ACL invloed heeft.
- De interne DHCP-server luistert naar de loopback-interface van de controller via 127.0.0.1, UDP-poort 67.

Eindgebruikersinterface

- Het **config dhcp proxy disable** Het bevel impliceert het gebruik van de het overbruggen van DHCP functie. Dit is een algemene opdracht (geen opdracht per WLAN).
- DHCP-proxy blijft standaard ingeschakeld.

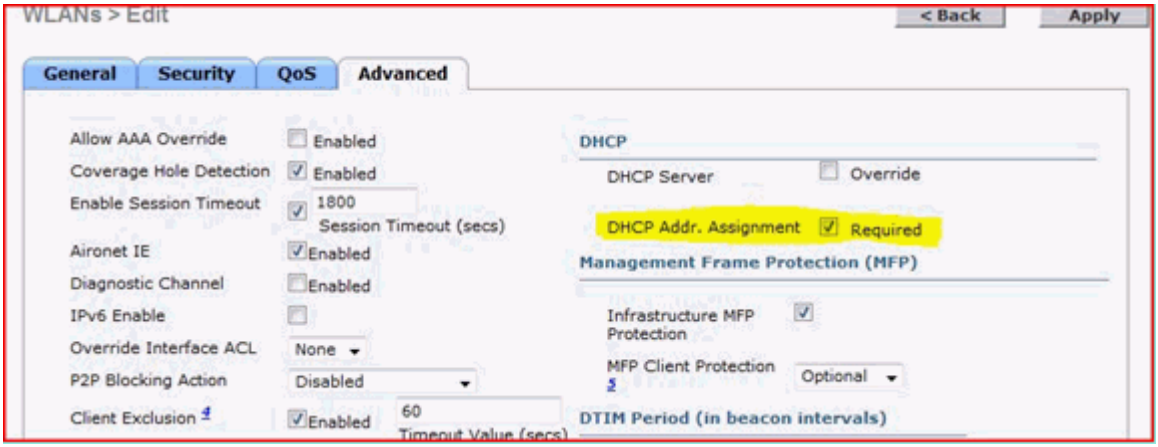
- Wanneer DHCP-proxy is uitgeschakeld, kan de interne DHCP-server niet worden gebruikt door lokale WLANâ€™s. Overbrugging vindt niet consistent plaats bij de benodigde bewerkingen om een pakket om te leiden naar de interne server. Overbrugging houdt werkelijk overbrugging in, met uitzondering van de conversie van 802.11 naar Ethernet II. DHCP-pakketten worden ongewijzigd via de LWAP-tunnel doorgegeven aan de client-VLAN (en vice versa).

- Wanneer de proxy is ingeschakeld, moet een DHCP-server worden geconfigureerd in de interface van het WLAN (of in het WLAN zelf) om het WLAN in te schakelen. Er hoeft geen server te worden geconfigureerd wanneer de proxy is uitgeschakeld omdat deze servers dan niet worden gebruikt.

- Wanneer een gebruiker probeert de DHCP-proxy in te schakelen, moet u intern controleren of voor alle WLANâ€™s (of bijbehorende interfaces) een DHCP-server is geconfigureerd. Als dat niet het geval is, zal het proces mislukken.

DHCP vereist

De WLAN geavanceerde configuratie heeft een optie die vereist dat gebruikers DHCP doorgeven voordat ze naar de RUN-staat gaan (een staat waar de client verkeer door de controller kan doorgeven). Deze optie vereist dat de client een volledige of halve DHCP-aanvraag doet. De controller wil een DHCP-aanvraag van de controller en een ACK die wordt teruggestuurd vanaf de DHCP-server. Wanneer de client deze stappen uitvoert, wordt DHCP doorgegeven en wordt de toestand RUN geactiveerd.



L2- en L3-roaming

L2 Roam - Als de client een geldige DHCP-lease heeft en een L2-roam uitvoert tussen twee verschillende controllers op hetzelfde L2-netwerk, hoeft de client niet opnieuw DHCP te gebruiken en moet de client-ingang volledig worden verplaatst naar de nieuwe controller van de oorspronkelijke controller. Als de client vervolgens opnieuw DHCP moet uitvoeren, zal via het proces voor DHCP-overbrugging of DHCP-proxy op de huidige controller het pakket op transparante wijze opnieuw worden doorgegeven.

L3 Roam - In een L3 roam scenario, beweegt de client zich tussen twee verschillende controllers in verschillende L3 netwerken. In deze situatie, wordt de cliënt verankerd aan de originele controlemechanisme en vermeld in de cliëntlijst op de nieuwe buitenlandse controller. Tijdens het ankerscenario wordt de client-DHCP behandeld door de ankercontroller als de clientgegevens worden getunneld in een EoIP-tunnel tussen de buitenlandse en ankercontrollers.

Gerelateerde informatie

- **Configuratievoorbeeld van DHCP-optie 43 voor lichtgewicht Cisco Aironet access points**

- **Technische ondersteuning en documentatie â€“ Cisco Systems**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.