

Entender como as WLCs AireOS lidam com o protocolo DHCP

Contents

[Introdução](#)

[Servidor DHCP externo](#)

[Comparação entre os modos de proxy e de bridging DHCP](#)

[Modo de proxy DHCP](#)

[Fluxo de pacote de proxy](#)

[Captura de pacote de proxy](#)

[Perspectiva do cliente](#)

[Perspectiva do servidor](#)

[Exemplo de configuração de proxy](#)

[Troubleshooting](#)

[Caveats](#)

[Modo de ponte DHCP](#)

[Operações de ponte DHCP - Bridging Packet Flow](#)

[Captura de pacotes de Bridging - Perspectiva do cliente](#)

[Captura de pacote de ponte - Perspectiva do servidor](#)

[Exemplo de configuração de Bridging](#)

[Troubleshooting](#)

[Caveats](#)

[Servidor DHCP interno](#)

[Comparação dos Modos DHCP e Bridging Internos](#)

[Servidor DHCP interno - Fluxo de pacotes](#)

[Exemplo de configuração de servidor DHCP interno](#)

[Troubleshooting](#)

[Limpe as concessões de DHCP no servidor DHCP interno da WLC](#)

[Caveats](#)

[Interface de usuário final](#)

[DHCP necessário](#)

[Roaming de L2 e L3](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as diferentes operações DHCP no controlador sem fio Cisco AireOS.

Servidor DHCP externo

A controladora Wireless LAN (WLC) oferece suporte a dois modos de operações DHCP, caso um servidor DHCP externo seja usado:

- modo de proxy DHCP
- modo de DHCP Bridging

O modo proxy DHCP serve como uma função de ajuda DHCP para obter melhor segurança e controle sobre as transações DHCP entre o servidor DHCP e os clientes sem fio. O modo de ponte DHCP fornece uma

opção para tornar a função de controlador em uma transação DHCP totalmente transparente para os clientes sem fio.

Comparação entre os modos de proxy e de bridging DHCP

Lidando com o DHCP do cliente	Modo de proxy DHCP	Modo de ponte DHCP
Modificar giaddr	Yes	No
Modificar siaddr	Yes	No
Modificar o conteúdo do pacote	Yes	No
Ofertas redundantes não encaminhadas	Yes	No
Suporte à opção 82	Yes	No
Transmissão para unicast	Yes	No
Suporte a BOOTP	No	Servidor
RFC não compatível	O proxy e o agente de retransmissão não são exatamente o mesmo conceito. O modo de ponte DHCP é recomendado para conformidade total com RFC.	No

Modo de proxy DHCP

O proxy DHCP não é ideal para todos os ambientes de rede. O controlador modifica e retransmite todas as transações DHCP para fornecer uma função auxiliar e resolver determinados problemas de segurança.

O endereço IP virtual do controlador é normalmente usado como o endereço IP origem de todas as transações DHCP para o cliente. Como resultado, o endereço IP real do servidor DHCP não é exposto no ar. Esse IP virtual é exibido na saída de depuração para transações DHCP no controlador. No entanto, o uso de um endereço IP virtual pode causar problemas em determinados tipos de clientes.

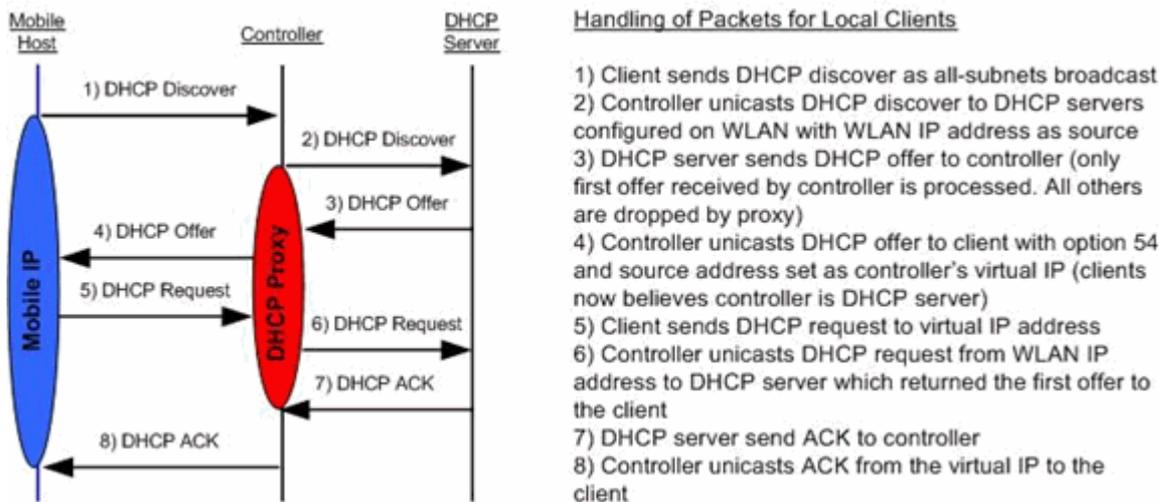
A operação do modo proxy DHCP mantém o mesmo comportamento para os protocolos de mobilidade simétrica e assimétrica.

Quando várias ofertas vêm de servidores DHCP externos, o proxy DHCP normalmente seleciona o primeiro que chega e define o endereço IP do servidor na estrutura de dados do cliente. Como resultado, todas as transações subsequentes passam pelo mesmo servidor DHCP até que uma transação falhe após novas tentativas. Neste ponto, o proxy seleciona um servidor DHCP diferente para o cliente.

O proxy DHCP é ativado por padrão. Todos os controladores que se comunicam devem ter a mesma configuração de proxy DHCP.

Observação: o proxy DHCP deve estar habilitado para que a opção de DHCP 82 funcione corretamente.

Fluxo de pacote de proxy



Captura de pacote de proxy

Quando o controlador está no modo proxy DHCP, ele não apenas direciona os pacotes DHCP para o servidor DHCP, mas também cria novos pacotes DHCP para encaminhá-los ao servidor DHCP. Todas as opções DHCP presentes nos pacotes DHCP do cliente são copiadas nos pacotes DHCP do controlador. Os próximos exemplos de captura de tela mostram isso para um pacote de solicitação DHCP.

Perspectiva do cliente

Esta captura de tela é de uma captura de pacote tomada da perspectiva do cliente. Ele mostra uma descoberta DHCP, uma oferta DHCP, uma solicitação DHCP e um DHCP ACK. A solicitação DHCP é realçada e os detalhes do protocolo bootp são expandidos, o que mostra as opções DHCP.

Buffalo_DHCPproxy_client.pcap - Wireshark

Filter: bootp

No.	Time	Source	Destination	Protocol	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x808e42a7
2	2.996334	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x808e42a7
3	3.023498	1.1.1.1	50.101.2.4	DHCP	DHCP Offer - Transaction ID 0x808e42a7
4	3.023995	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x808e42a7
5	3.083556	1.1.1.1	50.101.2.4	DHCP	DHCP ACK - Transaction ID 0x808e42a7

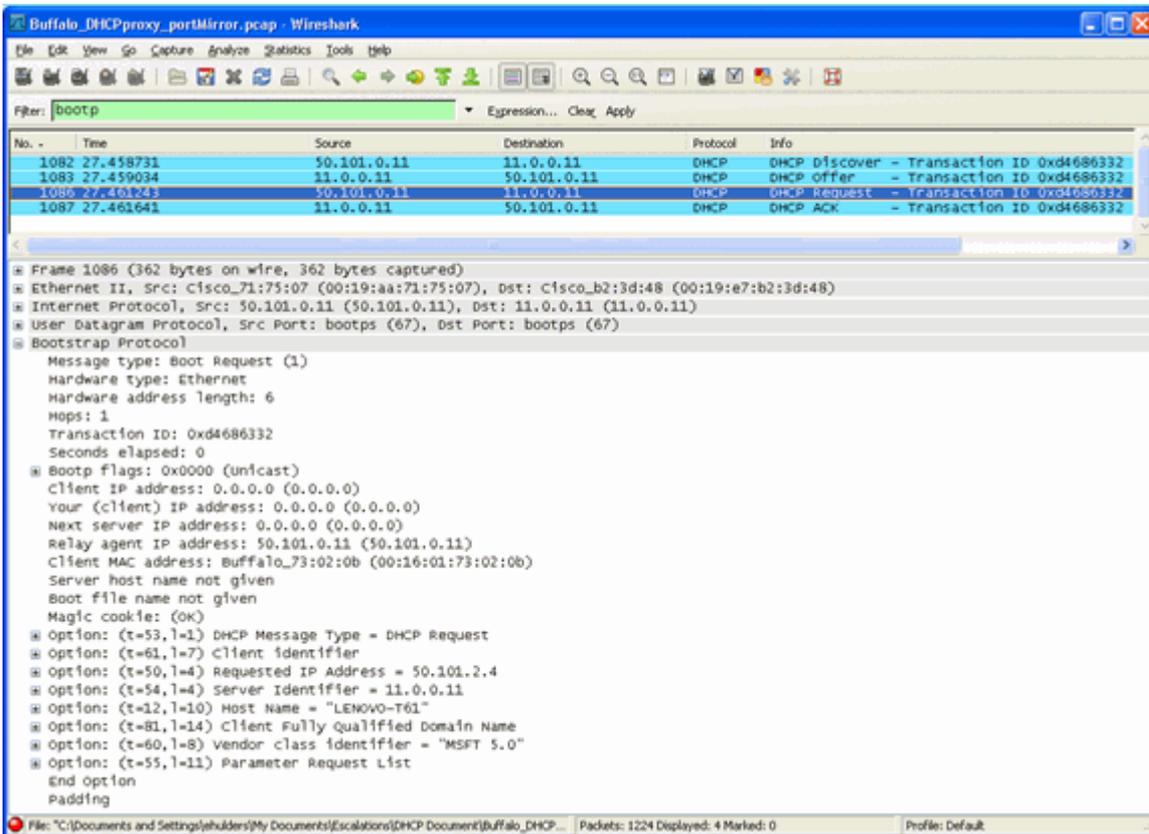
Frame 4 (358 bytes on wire, 358 bytes captured)

- Ethernet II, Src: Buffalo_73:02:0b (00:16:01:73:02:0b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
- User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
- Bootstrap Protocol
 - Message type: Boot Request (1)
 - Hardware type: ethernet
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0x808e42a7
 - Seconds elapsed: 3 (little endian bug?)
 - Bootp flags: 0x0000 (unicast)
 - Client IP address: 0.0.0.0 (0.0.0.0)
 - Your (client) IP address: 0.0.0.0 (0.0.0.0)
 - Next server IP address: 0.0.0.0 (0.0.0.0)
 - Relay agent IP address: 0.0.0.0 (0.0.0.0)
 - Client MAC address: Buffalo_73:02:0b (00:16:01:73:02:0b)
 - Server host name not given
 - Boot file name not given
 - Magic cookie: (OK)
 - option: (t=53,l=1) DHCP Message Type = DHCP Request
 - option: (t=61,l=7) Client identifier
 - option: (t=50,l=4) Requested IP Address = 50.101.2.4
 - option: (t=54,l=4) Server Identifier = 1.1.1.1
 - option: (t=12,l=10) Host Name = "LEXOVO-T61"
 - option: (t=81,l=14) Client Fully Qualified Domain Name
 - option: (t=60,l=8) vendor class identifier = "MSFT 5.0"
 - option: (t=55,l=11) Parameter Request List
 - End option

Bootstrap Protocol (bootp), 316 bytes | Packets: 29 Displayed: 5 Marked: 0 | Profile: Default

Perspectiva do servidor

Esta captura de tela é de uma captura de pacote tomada da perspectiva do servidor. Semelhante ao exemplo anterior, ele mostra uma descoberta DHCP, uma oferta DHCP, uma solicitação DHCP e um DHCP ACK. No entanto, esses são pacotes que o controlador construiu como uma função do proxy DHCP. Novamente, a solicitação DHCP é realçada e os detalhes do protocolo bootp são expandidos, o que mostra as opções DHCP. Observe que eles são os mesmos que no pacote de solicitação DHCP dos clientes. Observe também que o proxy de WLC retransmite o pacote e destaca os endereços de pacote.



Exemplo de configuração de proxy

Para usar o controlador como um proxy DHCP, o recurso de proxy DHCP deve ser habilitado no controlador. Por padrão, esse recurso está habilitado. Para habilitar o proxy DHCP, este comando CLI pode ser usado. O mesmo está disponível na GUI na página Controller no menu DHCP.

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy enable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

Para que o proxy DHCP funcione, um servidor DHCP primário deve ser configurado em cada interface do

controlador que requer serviços DHCP. Um servidor DHCP pode ser configurado na interface de gerenciamento, na interface do gerenciador de aplicativos e nas interfaces dinâmicas. Esses comandos CLI podem ser usados para configurar um servidor DHCP para cada interface.

```
<#root>
```

```
(Cisco Controller) >
```

```
config interface dhcp ap-manager primary
```

```
(Cisco Controller) >
```

```
config interface dhcp management primary
```

```
(Cisco Controller) >
```

```
config interface dhcp dynamic-interface
```

```
primary
```

O recurso de DHCP Bridging é uma configuração global, portanto afeta todas as transações DHCP dentro do controlador.

Troubleshooting

Esta é a saída do comando `debug dhcp packet enable` comando. A depuração mostra um controlador que recebe uma solicitação DHCP de um cliente com endereço MAC 00:40:96:b4:8c:e1, transmite uma solicitação DHCP ao servidor DHCP, recebe uma resposta do servidor DHCP e envia uma oferta DHCP ao cliente.

```
<#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

```

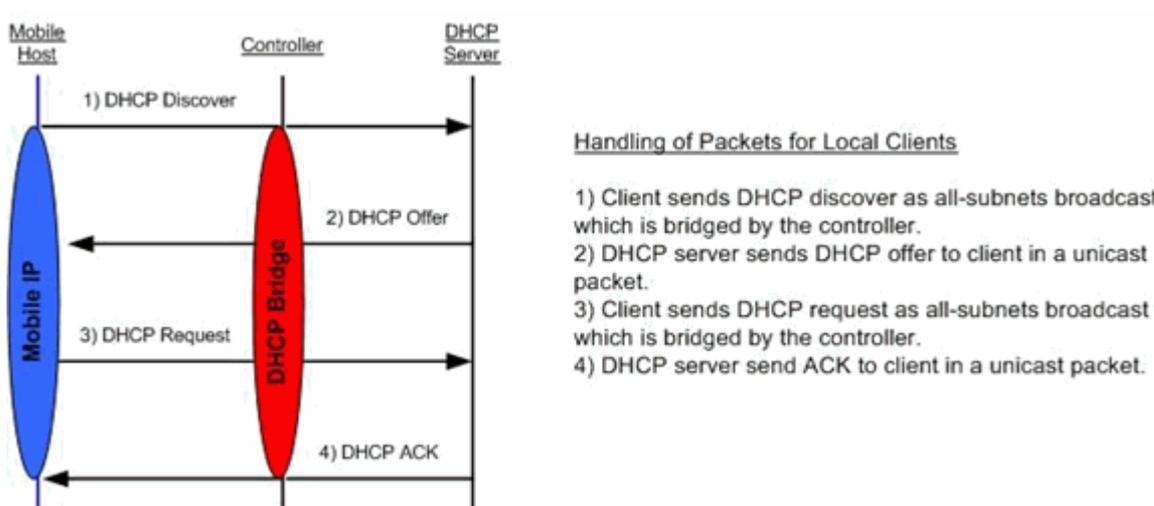
Caveats

- Podem existir problemas de interoperabilidade entre um controlador com proxy DHCP ativado e dispositivos que atuam como firewall e servidor DHCP. Isso ocorre provavelmente devido ao componente de firewall do dispositivo, pois os firewalls geralmente não respondem às solicitações de proxy. A solução alternativa para esse problema é desabilitar o proxy DHCP no controlador.
- Quando um cliente está no estado DHCP REQ no controlador, o controlador descarta os pacotes de informação DHCP. O cliente não entra em um estado RUN no controlador (isso é necessário para que o cliente passe o tráfego) até receber um pacote de descoberta DHCP do cliente. Os pacotes de informação DHCP são encaminhados pelo controlador quando o proxy DHCP está desativado.
- Todos os controladores que se comunicam entre si devem ter a mesma configuração de proxy DHCP.

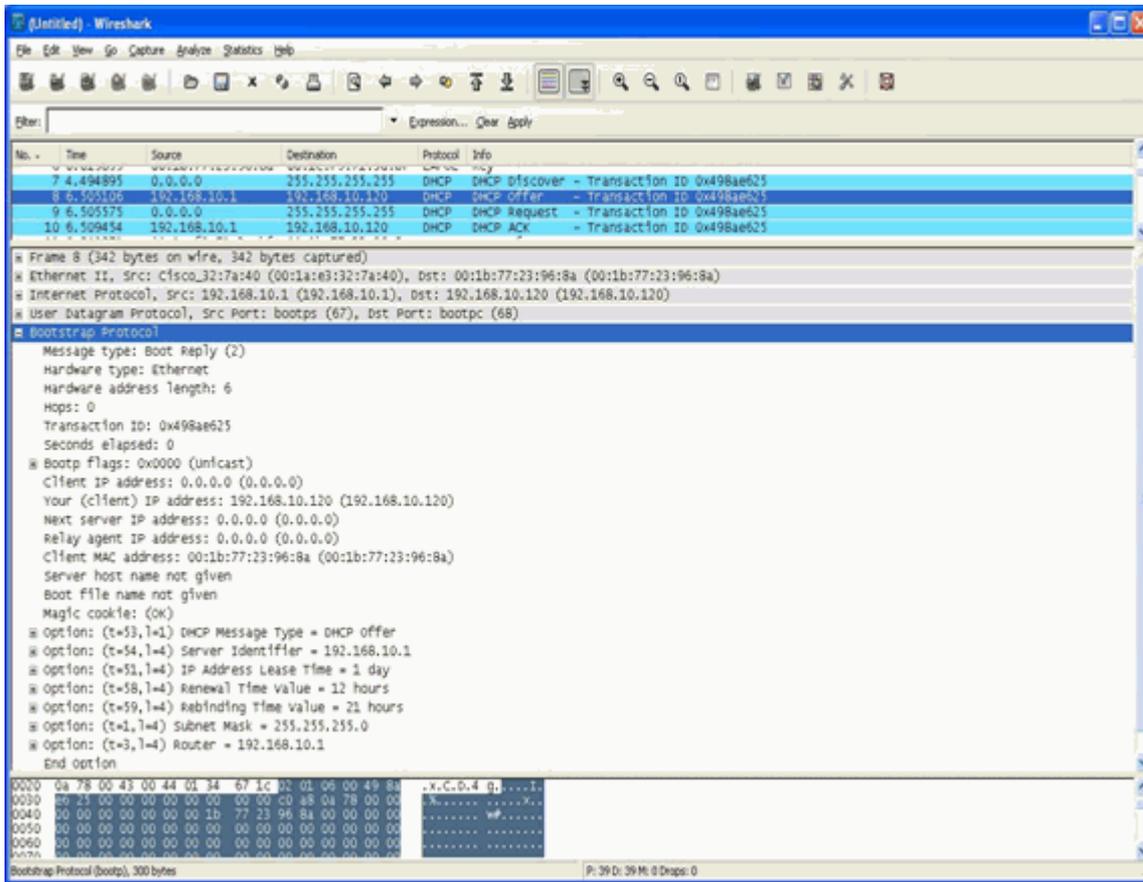
Modo de ponte DHCP

O recurso de ponte DHCP foi projetado para tornar a função de controlador na transação DHCP totalmente transparente para o cliente. Com exceção da conversão de 802.11 para Ethernet II, os pacotes do cliente são ligados sem modificação do túnel Light Weight Access Point Protocol (LWAPP) para a VLAN do cliente (ou túnel Ethernet over IP (EoIP) no caso de roaming de L3). Da mesma forma, com exceção da conversão de Ethernet II para 802.11, os pacotes para o cliente são ligados sem modificação da VLAN do cliente (ou túnel EoIP no caso de roaming de L3) para o túnel LWAPP. Pense nisso como cabear um cliente em uma porta de switch e, em seguida, o cliente executa uma transação DHCP tradicional.

Operações de ponte DHCP - Bridging Packet Flow

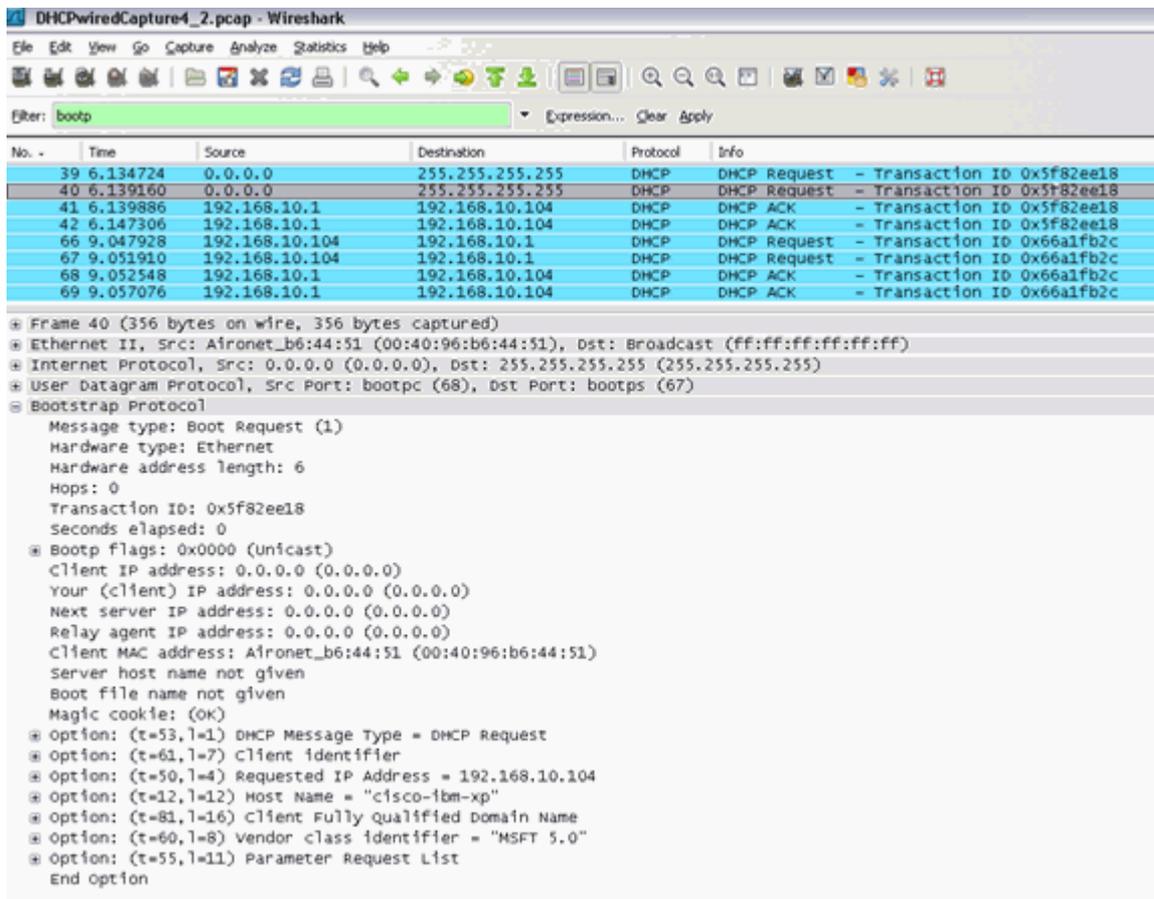


Captura de pacotes de Bridging - Perspectiva do cliente



Na captura de tela do pacote do lado do cliente, a principal diferença entre a captura do cliente no modo Proxy é que o IP real do servidor DHCP é visto nos pacotes Offer e Ack em vez do endereço IP virtual do controlador.

Captura de pacote de ponte - Perspectiva do servidor



Na captura de tela do pacote com fio, você pode ver que o pacote 40 é o broadcast de solicitação DHCP interligado do cliente de teste 00:40:96:b6:44:51 para a rede com fio.

Exemplo de configuração de Bridging

Para habilitar a funcionalidade de ponte DHCP no controlador, você deve desabilitar o recurso de proxy DHCP no controlador. Isso só pode ser realizado no CLI com estes comandos:

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy disable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behaviour: disabled
```

Se o servidor DHCP não existir na mesma rede de Camada 2 (L2) que o cliente, o broadcast precisará ser encaminhado ao servidor DHCP no gateway cliente através do uso de um IP helper. Este é um exemplo desta configuração:

```
<#root>
```

```
Switch#
```

```
conf t
```

```
Switch(config)#
```

```
interface vlan
```

```
Switch(config-if)#
```

```
ip helper-address
```

O recurso de DHCP Bridging é uma configuração global, portanto afeta todas as transações DHCP dentro do controlador. Você precisa adicionar instruções IP helper na infraestrutura com fio para todas as VLANs necessárias no controlador.

Troubleshooting

As depurações listadas aqui foram ativadas na CLI da controladora e a parte DHCP da saída foi extraída para este documento.

```
<#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
```

Nesta saída de depuração de DHCP, há algumas indicações importantes de que o DHCP Bridging está em uso no controlador:

O DHCP fez a ponte do pacote com êxito para o DS - Isso significa que o pacote DHCP original do cliente foi colocado em ponte, sem alterações para o sistema de distribuição (DS). O DS é a infraestrutura com fio.

O DHCP fez a ponte do pacote com êxito para o STA - Essa mensagem indica que o pacote DHCP foi colocado em ponte, sem alterações para a estação (STA). O STA é a máquina cliente que solicita DHCP.

Além disso, você vê o endereço IP do servidor real listado nas depurações, que é 192.168.10.1. Se o proxy DHCP estivesse em uso em vez do DHCP Bridging, você veria o endereço IP virtual do controlador listado para o endereço IP do servidor.

Caveats

- Por padrão, o proxy DHCP está habilitado.
- Todos os controladores que se comunicam entre si devem ter a mesma configuração de proxy DHCP.
- O proxy DHCP deve ser ativado para que a opção 82 do DHCP funcione.

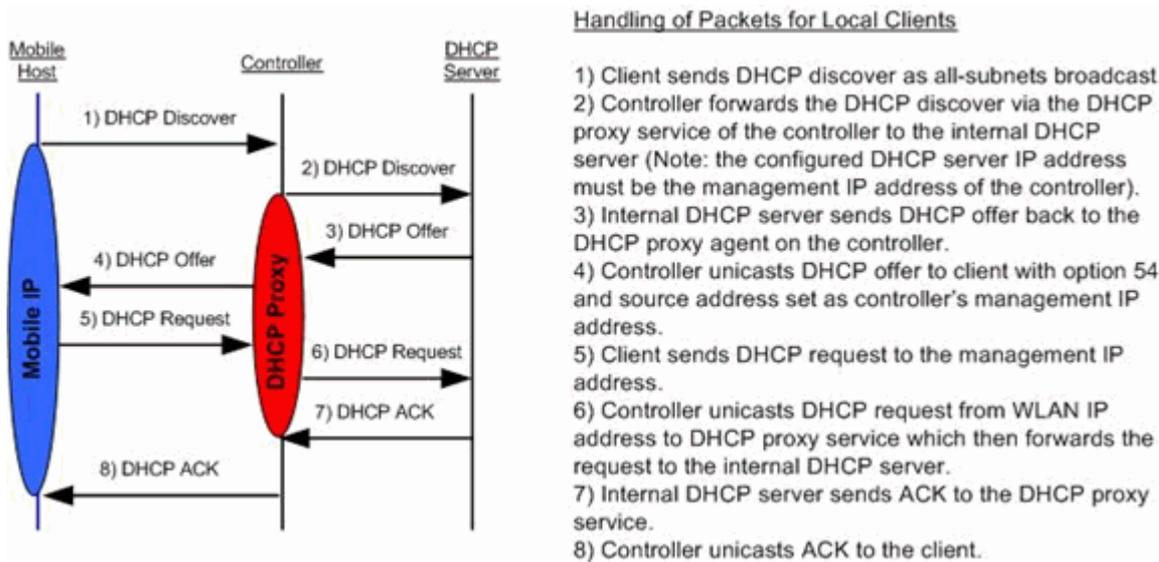
Servidor DHCP interno

O servidor DHCP interno foi introduzido inicialmente para filiais onde um servidor DHCP externo não está disponível. Ele foi projetado para suportar uma pequena rede sem fio com menos de dez pontos de acesso (APs) que estejam na mesma sub-rede. O servidor interno fornece endereços IP para clientes sem fio, APs de conexão direta, APs de modo de dispositivo na interface de gerenciamento e solicitações DHCP que são retransmitidas de APs. Não é um servidor DHCP de finalidade geral completo. Ele suporta apenas funcionalidade limitada e não é escalável em uma implantação maior.

Comparação dos Modos DHCP e Bridging Internos

Os dois modos principais do DHCP no controlador são proxy DHCP ou DHCP Bridging. Com o DHCP Bridging, a controladora age mais como um DHCP de volta com APs autônomos. Um pacote DHCP entra no AP por meio de uma associação de cliente a um SSID (Service Set Identifier) vinculado a uma VLAN. Em seguida, o pacote DHCP sai dessa VLAN. Se um auxiliar de IP for definido no gateway da Camada 3 (L3) dessa VLAN, o pacote será encaminhado para esse servidor DHCP via unicast direcionado. Em seguida, o servidor DHCP responde diretamente à interface L3 que encaminhou esse pacote DHCP. Com o proxy DHCP, a ideia é a mesma, mas todo o encaminhamento é feito diretamente no controlador, em vez da interface L3 da VLAN. Por exemplo, uma solicitação DHCP chega à WLAN do cliente, a WLAN usa o servidor DHCP definido na interface da VLAN *ou* usa a função de substituição DHCP da WLAN para encaminhar um pacote DHCP unicast ao servidor DHCP com o campo DHCP packets GIADDR preenchido para ser o endereço IP da interface da VLAN.

Servidor DHCP interno - Fluxo de pacotes

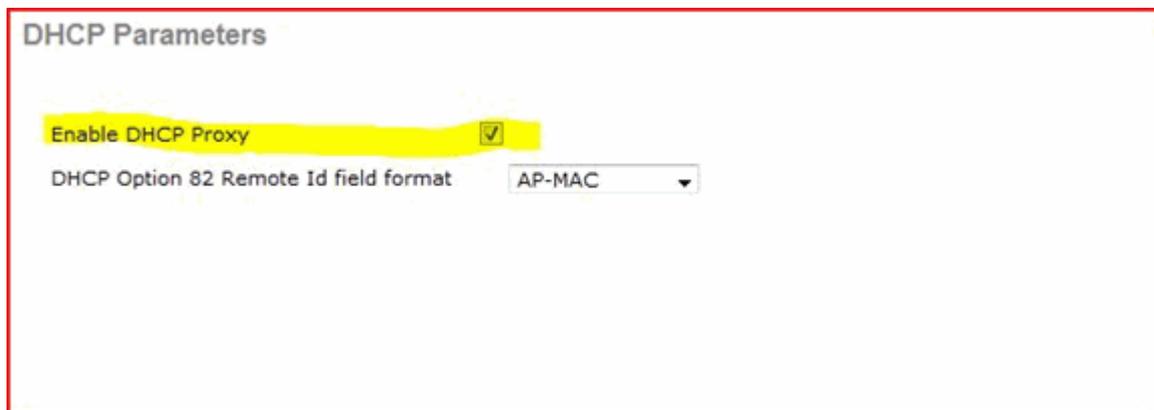


Exemplo de configuração de servidor DHCP interno

Você deve habilitar o proxy DHCP no controlador para permitir que o servidor DHCP interno funcione. Isso pode ser feito por meio da GUI nesta seção:

Observação: você não pode definir o proxy DHCP através da GUI em todas as versões.

Controller->Advanced->DHCP



Ou pelo CLI:

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

Para habilitar o servidor DHCP interno, execute estas etapas:

1. Defina um escopo que você usa para receber endereços IP (Controlador > Servidor DHCP interno > Escopo DHCP). Clique em **New**.

DHCP Scope > Edit

Scope Name	User Scope		
Pool Start Address	192.168.100.100		
Pool End Address	192.168.100.200		
Network	192.168.100.0		
Netmask	255.255.255.0		
Lease Time (seconds)	86400		
Default Routers	192.168.100.1	0.0.0.0	0.0.0.0
DNS Domain Name	wlc2106.local		
DNS Servers	0.0.0.0	0.0.0.0	0.0.0.0
Netbios Name Servers	0.0.0.0	0.0.0.0	0.0.0.0
Status	Enabled ▾		

2. Aponte a substituição de DHCP para o endereço IP da interface de gerenciamento do controlador.

WLANs > Edit

[< Back](#)

General | **Security** | **QoS** | **Advanced**

<p>Allow AAA Override <input type="checkbox"/> Enabled</p> <p>Coverage Hole Detection <input checked="" type="checkbox"/> Enabled</p> <p>Enable Session Timeout <input checked="" type="checkbox"/> 1800 Session Timeout (secs)</p> <p>Aironet IE <input checked="" type="checkbox"/> Enabled</p> <p>Diagnostic Channel <input type="checkbox"/> Enabled</p> <p>IPv6 Enable <input type="checkbox"/></p> <p>Override Interface ACL <input type="checkbox"/> None ▾</p> <p>P2P Blocking Action <input type="checkbox"/> Disabled ▾</p> <p>Client Exclusion <input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)</p> <p>VoIP Snooping and Reporting <input type="checkbox"/></p> <hr/> <p>HREAP</p> <p>H-REAP Local Switching <input type="checkbox"/> Enabled</p> <p>Learn Client IP Address <input checked="" type="checkbox"/> Enabled</p>	<p>DHCP</p> <p>DHCP Server <input checked="" type="checkbox"/> Override</p> <p>192.168.100.254 DHCP Server IP Addr</p> <p>DHCP Addr. Assignment <input type="checkbox"/> Required</p> <hr/> <p>Management Frame Protection (MFP)</p> <p>Infrastructure MFP Protection <input checked="" type="checkbox"/></p> <p>MFP Client Protection <input type="checkbox"/> Optional ▾</p> <hr/> <p>DTIM Period (in beacon intervals)</p> <p>802.11a/n (1 - 255) 1</p> <p>802.11b/g/n (1 - 255) 1</p> <hr/> <p>NAC</p> <p>State <input type="checkbox"/> Enabled</p>
---	--

Ou você pode usar a opção DHCP da configuração de interface do controlador para a interface que deseja usar no servidor DHCP interno.

Interfaces > Edit

General Information

Interface Name	management
MAC Address	00:1a:6c:91:47:00

Configuration

Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	<input type="text" value="0"/>

Interface Address

VLAN Identifier	<input type="text" value="0"/>
IP Address	<input type="text" value="192.168.100.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.100.1"/>

Physical Information

Port Number	<input type="text" value="1"/>
-------------	--------------------------------

DHCP Information

Primary DHCP Server	<input type="text" value="192.168.100.254"/>
Secondary DHCP Server	<input type="text" value="0.0.0.0"/>

3. Verifique se o proxy DHCP está habilitado.

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

Troubleshooting

Uma depuração do servidor DHCP interno geralmente requer a localização de um cliente que tenha um problema para obter um endereço IP. Você precisa executar essas depurações.

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

O cliente de depuração é uma macro que ativa essas depurações para você enquanto focaliza a depuração somente no endereço MAC do cliente que você inseriu.

```
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
```

O principal problema do DHCP é o `debug dhcp packet enable` que é ativado automaticamente pelo `debug client` comando.

```
<#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
```

Limpe as concessões de DHCP no servidor DHCP interno da WLC

Você pode executar este comando para limpar as concessões de DHCP no servidor DHCP interno da WLC:

```
<#root>

config dhcp clear-lease
```

Aqui está um exemplo:

```
<#root>

config dhcp clear-lease all
```

Caveats

- O proxy DHCP deve ser habilitado para que o servidor DHCP interno funcione.
- O uso do DHCP para a porta 1067 quando você usa o servidor DHCP interno, que é afetado pela ACL da CPU.
- O servidor DHCP interno ouve a interface de loopback do controlador através da porta 67 UDP 127.0.0.1.

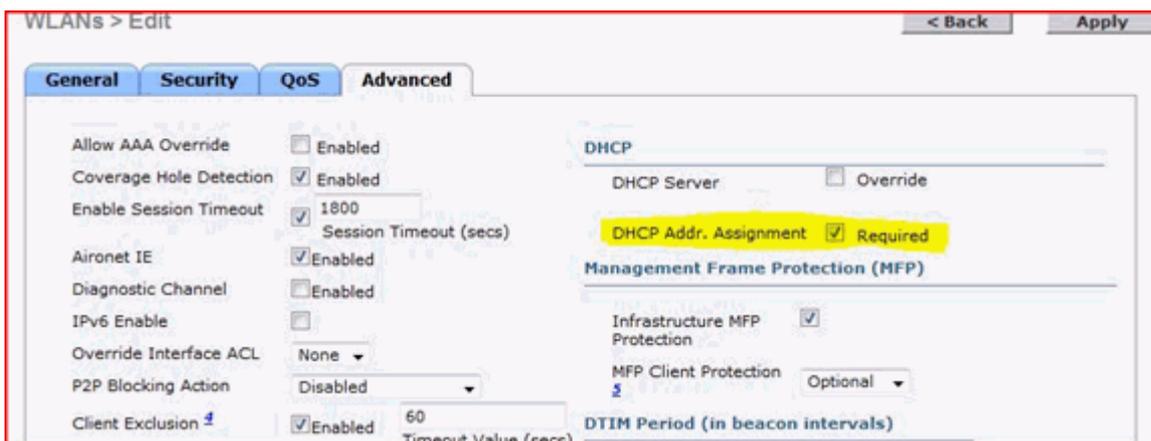
Interface de usuário final

- O `config dhcp proxy disable` implica o uso da função de ponte DHCP. Esse é um comando global (não um comando por WLAN).
- O proxy DHCP permanece habilitado por padrão.

- Quando o proxy DHCP é desativado, o servidor DHCP interno não pode ser usado por WLANs locais. A operação de bridging não é consistente com as operações necessárias para redirecionar um pacote para o servidor interno. Bridging realmente significa bridging, com exceção de 802.11 para conversão Ethernet II. Os pacotes DHCP são passados sem modificação do túnel LWAPP para a VLAN cliente (e vice-versa).
- Quando o proxy estiver habilitado, um servidor DHCP deverá ser configurado na interface da WLAN (ou na própria WLAN) para que a WLAN seja habilitada. Nenhum servidor precisa ser configurado quando o proxy está desabilitado, pois esses servidores não são usados.
- Quando um usuário tenta habilitar o proxy DHCP, você verifica internamente se todas as WLANs (ou interfaces associadas) têm um servidor DHCP configurado. Caso contrário, a operação de ativação falhará.

DHCP necessário

A configuração avançada da WLAN tem uma opção que exige que os usuários passem o DHCP antes de entrarem no estado RUN (um estado onde o cliente pode passar o tráfego através da controladora). Esta opção exige que o cliente faça uma solicitação DHCP completa ou metade. A principal coisa que o controlador procura do cliente é uma solicitação DHCP e um ACK que volta do servidor DHCP. Enquanto o cliente executar essas etapas, ele passará a etapa necessária do DHCP e passará para o estado RUN.



Roaming de L2 e L3

L2 Roam - Se o cliente tiver um aluguel de DHCP válido e executar um roam de L2 entre dois controladores diferentes na mesma rede L2, o cliente não precisará reDHCP e a entrada do cliente deverá ser completamente movida do controlador original para o novo controlador. Em seguida, se o cliente precisar executar o DHCP novamente, a ponte DHCP ou o processo proxy no controlador atual fará novamente a ponte transparente do pacote.

L3 em roaming - Em um cenário de roaming L3, o cliente se move entre dois controladores diferentes em redes L3 diferentes. Nessa situação, o cliente é ancorado na controladora original e listado na tabela de clientes na nova controladora estrangeira. Durante o cenário de âncora, o DHCP do cliente é tratado pelo controlador de âncora à medida que os dados do cliente são encapsulados em um túnel EoIP entre os controladores externo e de âncora.

Informações Relacionadas

- [Exemplo de configuração da OPÇÃO 43 do DHCP para os Pontos de Acesso Leves do Cisco](#)

Aironet.

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução

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

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

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