Comprender cómo los WLCs de AireOS manejan el protocolo DHCP

Contenido

Introducción

Este documento describe las diferentes operaciones DHCP en el controlador inalámbrico Cisco AireOS.

Servidor DHCP externo

El controlador de LAN inalámbrica (WLC) admite dos modos de operaciones DHCP en caso de que se utilice un servidor DHCP externo:

- modo de proxy DHCP
- modo de conexión en puente DHCP

El modo proxy DHCP sirve como función auxiliar de DHCP para lograr una mayor seguridad y control sobre las transacciones DHCP entre el servidor DHCP y los clientes inalámbricos. El modo de puente DHCP

ofrece una opción para hacer totalmente transparente para los clientes inalámbricos la función de controlador en una transacción DHCP.

Comparación de los modos proxy DHCP y puente

Manejo de DHCP del cliente	Modo proxy DHCP	Modo de Bridging DHCP
Modificar giaddr	Yes	No
Modificar siaddr	Yes	No
Modificar el contenido del paquete	Yes	No
Ofertas redundantes no reenviadas	Yes	No
Compatibilidad con la opción 82	Yes	No
Transmisión a unidifusión	Yes	No
Compatibilidad con BOOTP	No	Servidor
RFC no conforme	Proxy y relay agent no son exactamente el mismo concepto. Se recomienda el modo de conexión en puente DHCP para el cumplimiento de RFC completo.	No

Modo proxy DHCP

El proxy DHCP no es ideal para todos los entornos de red. El controlador modifica y retransmite todas las transacciones DHCP para proporcionar la función de ayudante y abordar ciertos problemas de seguridad.

La dirección IP virtual del controlador se utiliza normalmente como la dirección IP de origen de todas las transacciones DHCP al cliente. Como resultado, la dirección IP real del servidor DHCP no se expone en el aire. Esta IP virtual se muestra en la salida de depuración para las transacciones DHCP en el controlador. Sin embargo, el uso de una dirección IP virtual puede causar problemas en ciertos tipos de clientes.

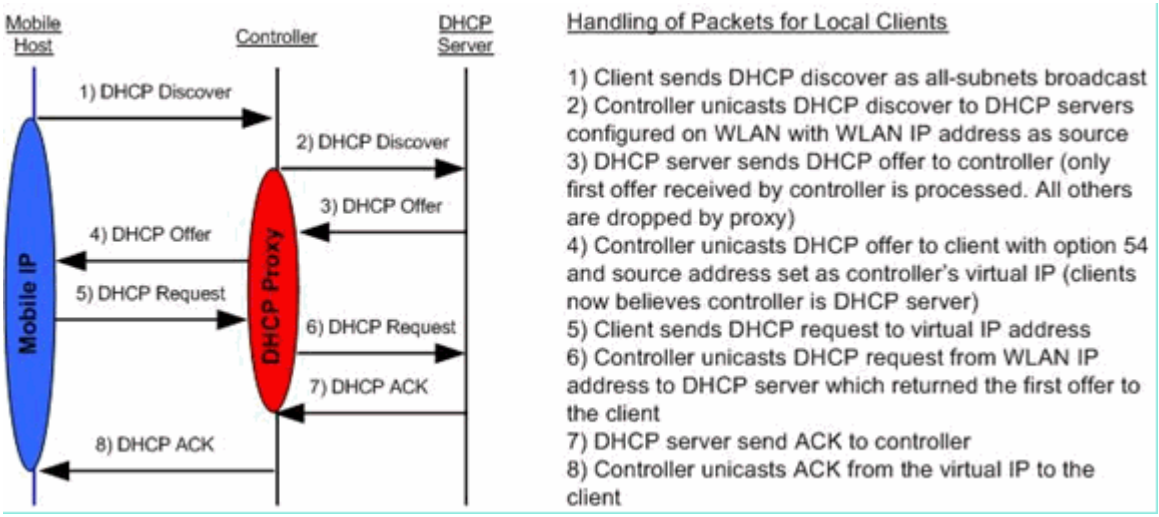
La operación del modo proxy DHCP mantiene el mismo comportamiento para los protocolos de movilidad simétricos y asimétricos.

Cuando varias ofertas proceden de servidores DHCP externos, el proxy DHCP normalmente selecciona el primero que entra y establece la dirección IP del servidor en la estructura de datos del cliente. Como resultado, todas las transacciones subsiguientes pasan a través del mismo servidor DHCP hasta que una transacción falla después de los reintentos. En este punto, el proxy selecciona un servidor DHCP diferente para el cliente.

El proxy DHCP está activado de forma predeterminada. Todos los controladores que se comunican deben tener la misma configuración de proxy DHCP.

Nota: El proxy DHCP debe estar activado para que la opción DHCP 82 funcione correctamente.

Flujo de paquetes proxy

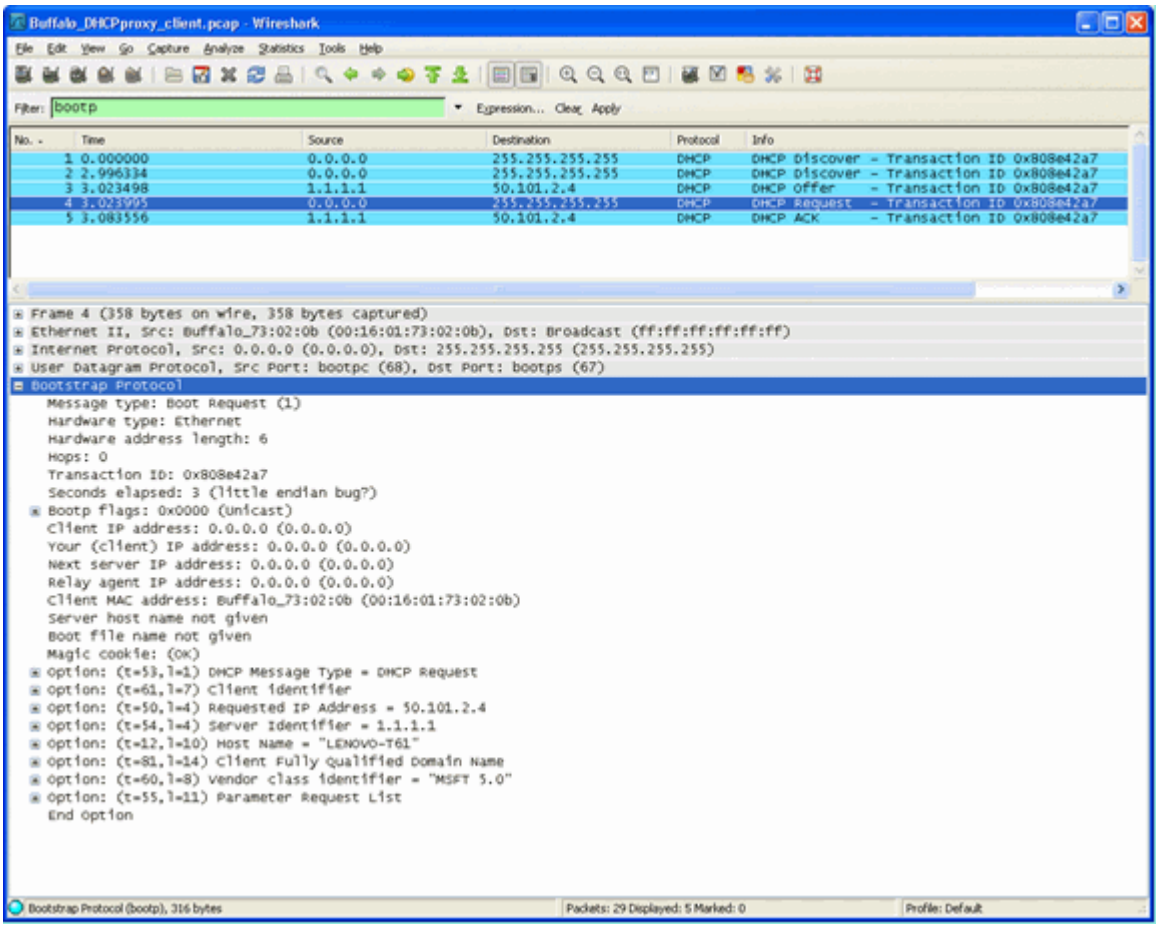


Captura de paquetes proxy

Cuando el controlador está en modo proxy DHCP, no sólo dirige los paquetes DHCP al servidor DHCP, sino que en realidad crea nuevos paquetes DHCP para reenviarlos al servidor DHCP. Todas las opciones DHCP presentes en los paquetes DHCP del cliente se copian en los paquetes DHCP del controlador. Los siguientes ejemplos de capturas de pantalla muestran esto para un paquete de solicitud DHCP.

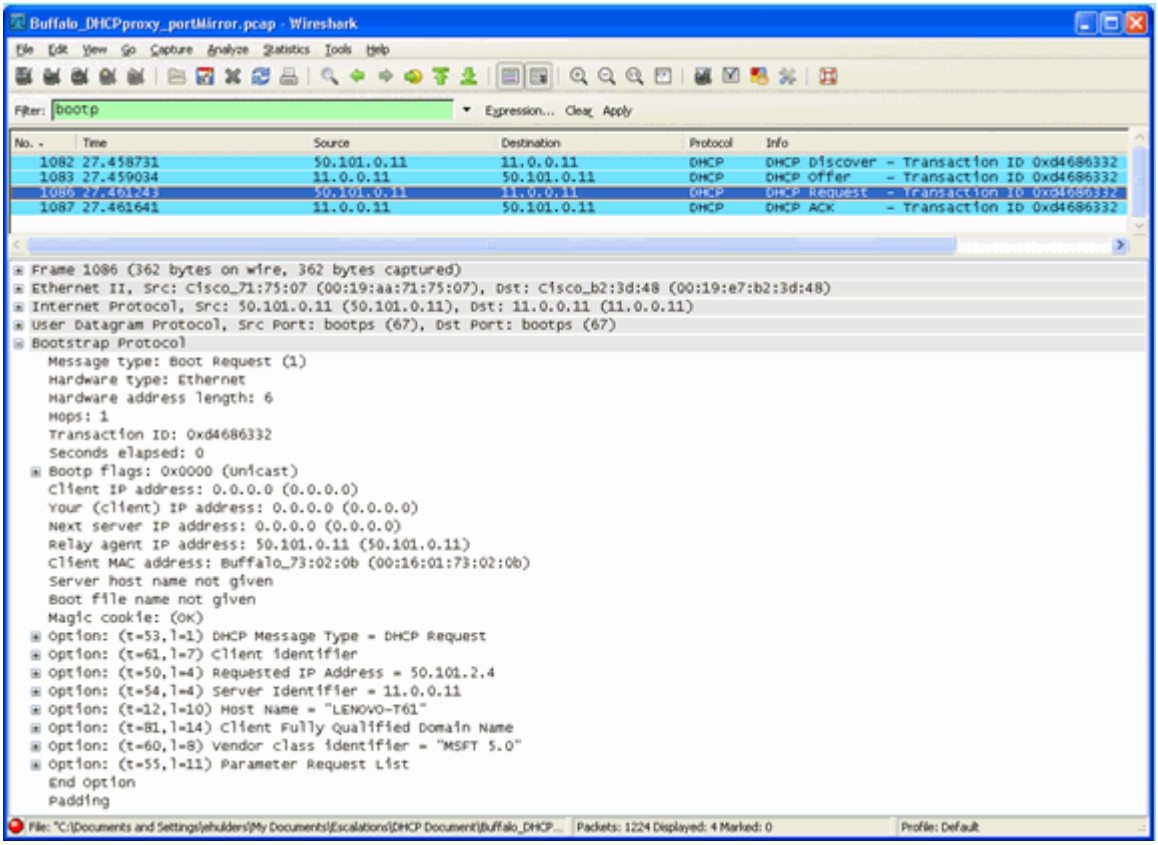
Perspectiva del cliente

Esta captura de pantalla es de una captura de paquetes tomada desde la perspectiva del cliente. Muestra una detección DHCP, una oferta DHCP, una solicitud DHCP y un ACK DHCP. Se resalta la solicitud DHCP y se expande el detalle del protocolo bootp, que muestra las opciones DHCP.



Perspectiva del servidor

Esta captura de pantalla es de una captura de paquetes tomada desde la perspectiva del servidor. Similar al ejemplo anterior, muestra una detección de DHCP, una oferta de DHCP, una solicitud de DHCP y un ACK de DHCP. Sin embargo, estos son paquetes que el controlador construyó como una función del proxy DHCP. Una vez más, se resalta la solicitud DHCP y se expande el detalle del protocolo bootp, que muestra las opciones DHCP. Observe que son los mismos que en el paquete de solicitud DHCP del cliente. También tenga en cuenta que el proxy WLC retransmite el paquete y resalta las direcciones del paquete.



Ejemplo de Configuración de Proxy

Para utilizar el controlador como proxy DHCP, la función de proxy DHCP debe estar habilitada en el controlador. Esta función está activada de forma predeterminada. Para habilitar el proxy DHCP, se puede utilizar este comando CLI. Lo mismo está disponible en la GUI en la página Controlador del menú DHCP.

<#root>

```
(Cisco Controller) >
```

config dhcp proxy enable

```
(Cisco Controller) >
```

show dhcp proxy

```
DHCP Proxy Behavior: enabled
```

Para que el proxy DHCP funcione, se debe configurar un servidor DHCP principal en cada interfaz de

controlador que requiera servicios DHCP. Se puede configurar un servidor DHCP en la interfaz de administración, en la interfaz de administrador de aplicaciones y en las interfaces dinámicas. Estos comandos CLI se pueden utilizar para configurar un servidor DHCP para cada interfaz.

<#root>

(Cisco Controller) >

config interface dhcp ap-manager primary

(Cisco Controller) >

config interface dhcp management primary

(Cisco Controller) >

config interface dhcp dynamic-interface

primary

La función de conexión en puente DHCP es un parámetro global, por lo que afecta a todas las transacciones DHCP dentro del controlador.

Troubleshoot

Este es el resultado de la **debug dhcp packet enable** comando. La depuración muestra un controlador que recibe una solicitud DHCP de un cliente con dirección MAC 00:40:96:b4:8c:e1, transmite una solicitud DHCP al servidor DHCP, recibe una respuesta del servidor DHCP y envía una oferta DHCP al 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
```

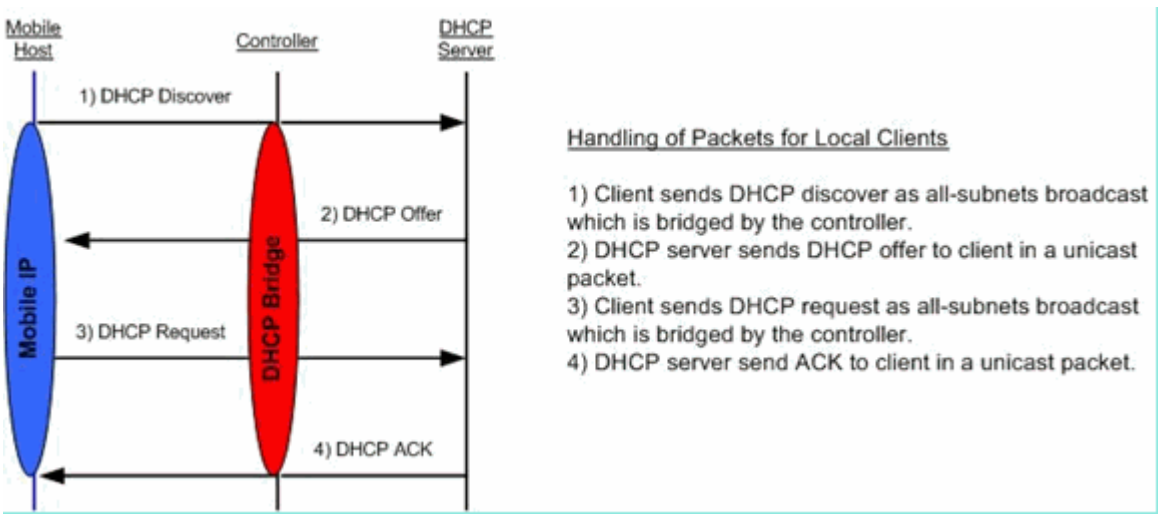
Advertencias

- Pueden existir problemas de interoperabilidad entre un controlador con el proxy DHCP habilitado y los dispositivos que actúan como firewall y servidor DHCP. Esto se debe probablemente al componente de firewall del dispositivo, ya que los firewalls generalmente no responden a las solicitudes de proxy. La solución alternativa para este problema es inhabilitar el proxy DHCP en el controlador.
- Cuando un cliente se encuentra en el estado DHCP REQ en el controlador, el controlador descarta los paquetes de información DHCP. El cliente no entra en un estado RUN en el controlador (esto es necesario para que el cliente pase el tráfico) hasta que recibe un paquete de detección DHCP del cliente. El controlador reenvía los paquetes de información DHCP cuando el proxy DHCP está desactivado.
- Todos los controladores que se comunican entre sí deben tener la misma configuración de proxy DHCP.

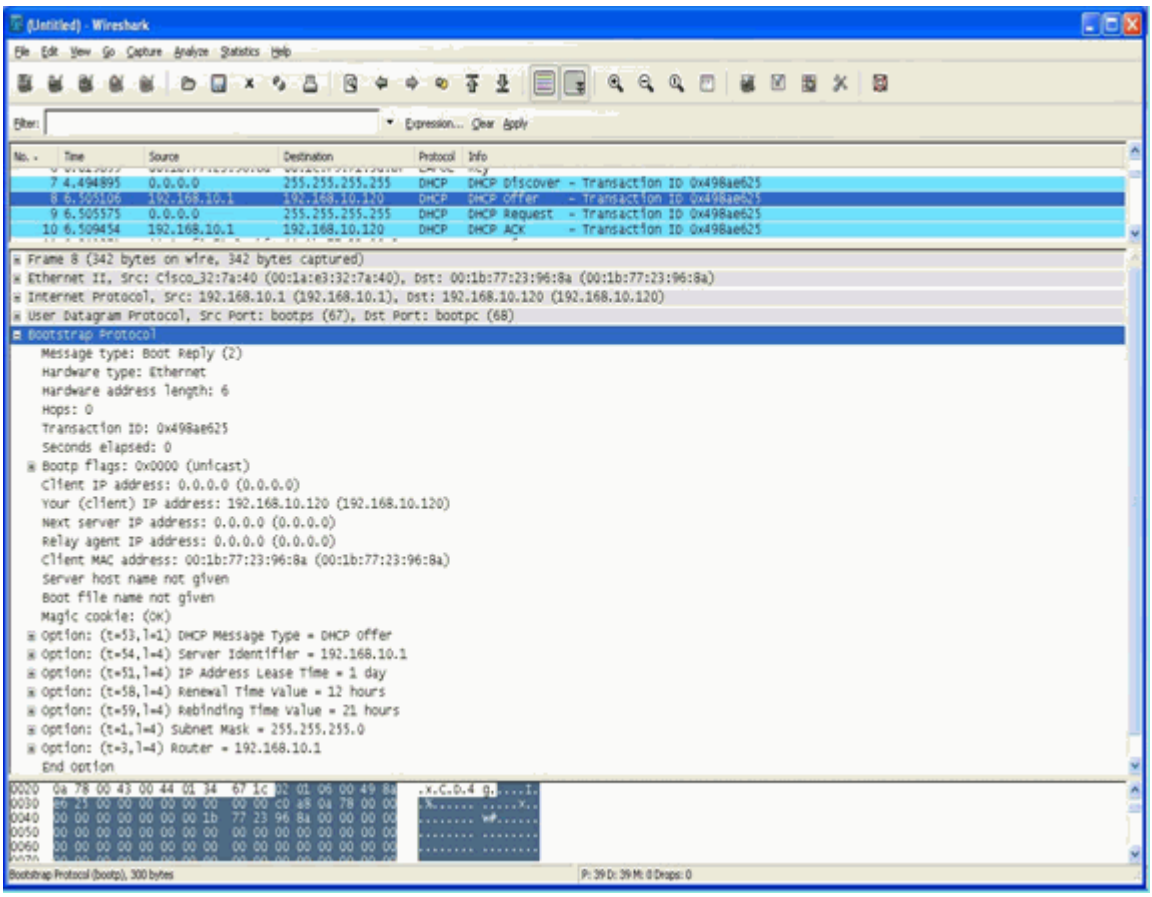
Modo de Bridging DHCP

La función de conexión en puente DHCP está diseñada para hacer que la función de controlador en la transacción DHCP sea totalmente transparente para el cliente. Con la excepción de la conversión de 802.11 a Ethernet II, los paquetes del cliente se puentean sin modificaciones desde el túnel del protocolo de punto de acceso ligero (LWAPP) a la VLAN del cliente (o túnel Ethernet sobre IP (EoIP) en el caso de itinerancia L3). De manera similar, con la excepción de la conversión de Ethernet II a 802.11, los paquetes al cliente se puentean sin modificar desde la VLAN del cliente (o túnel EoIP en el caso de itinerancia L3) al túnel LWAPP. Piense en esto como conectar un cliente a un puerto de switch y luego el cliente realiza una transacción DHCP tradicional.

Operaciones de Bridging DHCP - Bridging Packet Flow

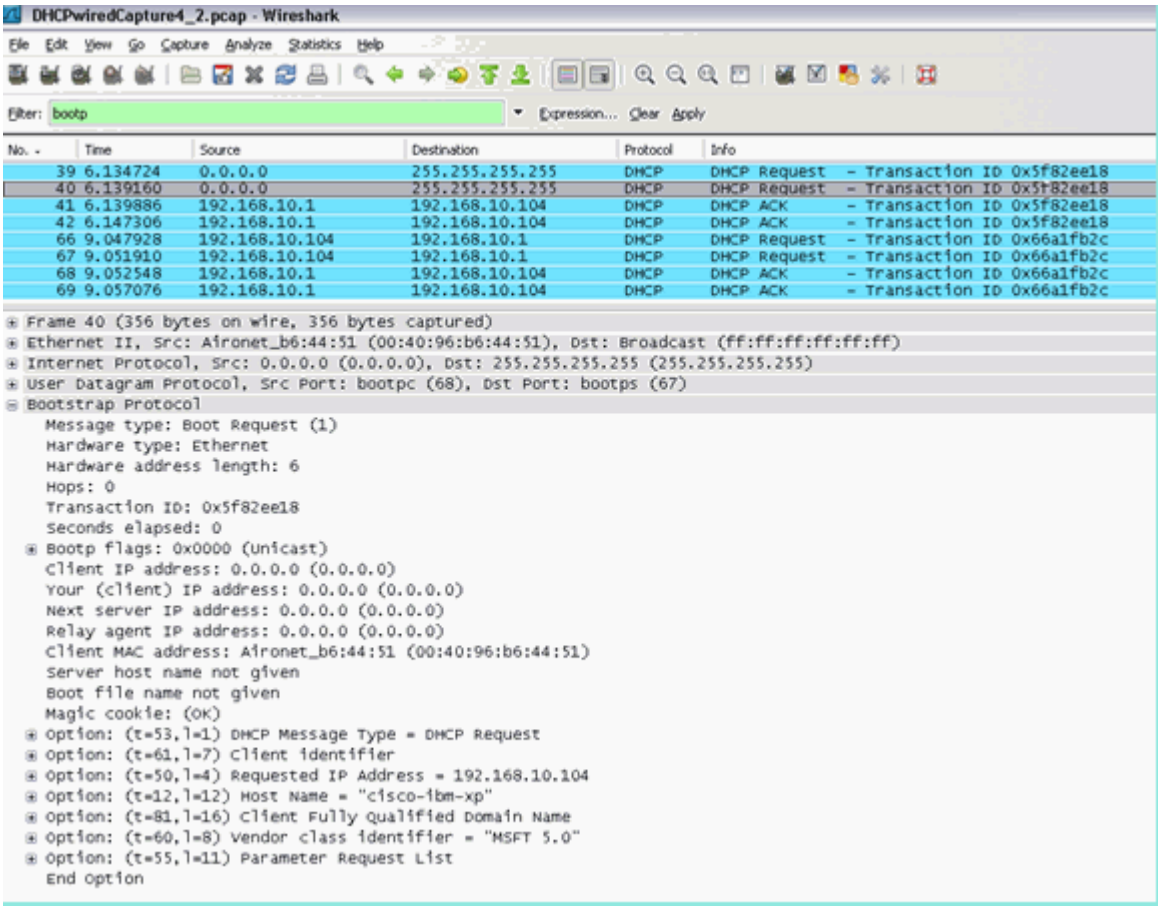


Bridging Packet Capture - Perspectiva del cliente



En la captura de pantalla de captura de paquetes del lado del cliente , la diferencia principal entre la captura del cliente en el modo Proxy es que la IP real del servidor DHCP se ve en los paquetes Offer y Ack en lugar de la dirección IP virtual del controlador.

Captura de paquetes en puente: perspectiva del servidor



En la captura de pantalla de captura de paquetes cableados puede ver que el paquete 40 es la transmisión de la solicitud DHCP puenteada desde el cliente de prueba 00:40:96:b6:44:51 a la red cableada.

Ejemplo de Configuración de Bridging

Para habilitar la funcionalidad de conexión en puente DHCP en el controlador, debe inhabilitar la función de proxy DHCP en el controlador. Esto solo se puede lograr en la CLI con estos comandos:

```
<#root>

(Cisco Controller) >

config dhcp proxy disable

(Cisco Controller) >

show dhcp proxy

DHCP Proxy Behaviour: disabled
```

Si el servidor DHCP no existe en la misma red de capa 2 (L2) que el cliente, la difusión debe reenviarse al servidor DHCP en la puerta de enlace del cliente mediante un ayudante IP. Este es un ejemplo de esta configuración:

```
<#root>

Switch#
```

```
conf t

Switch(config)#

interface vlan




Switch(config-if)#

ip helper-address
```

La función de conexión en puente DHCP es un parámetro global, por lo que afecta a todas las transacciones DHCP dentro del controlador. Debe agregar sentencias de ayudante IP en la infraestructura cableada para todas las VLAN necesarias en el controlador.

Troubleshoot

Las depuraciones enumeradas aquí se habilitaron en la CLI del controlador y la parte DHCP del resultado se extrajo 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
```

En esta salida de depuración DHCP, hay algunas indicaciones clave de que el puente DHCP está en uso en el controlador:

DHCP puenteó correctamente el paquete a DS - Esto significa que el paquete DHCP original del cliente se puenteó, sin alteraciones al sistema de distribución (DS). La DS es la infraestructura por cable.

DHCP puenteó correctamente el paquete a STA: este mensaje indica que el paquete DHCP se puenteó, sin alteraciones a la estación (STA). El STA es la máquina cliente que solicita DHCP.

Además, puede ver la dirección IP real del servidor que aparece en las depuraciones, que es 192.168.10.1. Si el proxy DHCP estaba en uso en lugar de la conexión en puente DHCP, verá la dirección IP virtual del controlador enumerada para la dirección IP del servidor.

Advertencias

- De forma predeterminada, el proxy DHCP está activado.
- Todos los controladores que se comunican entre sí deben tener la misma configuración de proxy DHCP.
- El proxy DHCP debe estar activado para que funcione la opción 82 de DHCP.

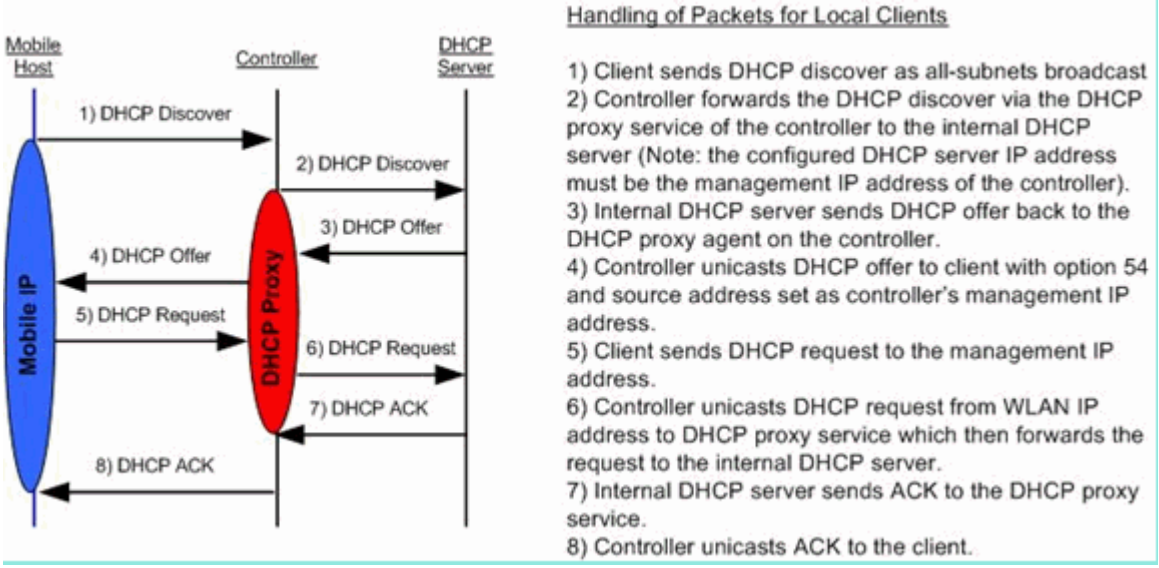
Servidor DHCP interno

El servidor DHCP interno se introdujo inicialmente para las sucursales en las que no hay un servidor DHCP externo disponible. Está diseñado para admitir una red inalámbrica pequeña con menos de diez puntos de acceso (AP) que se encuentren en la misma subred. El servidor interno proporciona direcciones IP a clientes inalámbricos, puntos de acceso de conexión directa, puntos de acceso en modo de dispositivo en la interfaz de administración y solicitudes DHCP que se transmiten desde puntos de acceso. No es un servidor DHCP de uso general completo. Solo admite funcionalidad limitada y no se puede ampliar en una implementación más grande.

Comparación de los modos de conexión en puente y DHCP interno

Los dos modos DHCP principales en el controlador son proxy DHCP o conexión en puente DHCP. Con el bridging DHCP, el controlador actúa más como un back DHCP con los AP autónomos. Un paquete DHCP entra en el AP a través de una asociación de cliente a un identificador de conjunto de servicios (SSID) que se enlaza a una VLAN. Luego, el paquete DHCP sale de esa VLAN. Si se define un ayudante IP en el gateway de capa 3 (L3) de esa VLAN, el paquete se reenvía a ese servidor DHCP a través de unidifusión dirigida. El servidor DHCP entonces responde directamente a la interfaz L3 que reenvió ese paquete DHCP. Con el proxy DHCP, es la misma idea, pero todo el reenvío se realiza directamente en el controlador en lugar de en la interfaz L3 de la VLAN. Por ejemplo, una solicitud DHCP llega a la WLAN desde el cliente, la WLAN luego utiliza el servidor DHCP definido en la interfaz de la VLAN *o* utiliza la función de reemplazo DHCP de la WLAN para reenviar un paquete DHCP de unidifusión al servidor DHCP con el campo GIADDR de paquetes DHCP completado para ser la dirección IP de la interfaz VLAN.

Servidor DHCP interno: flujo de paquetes

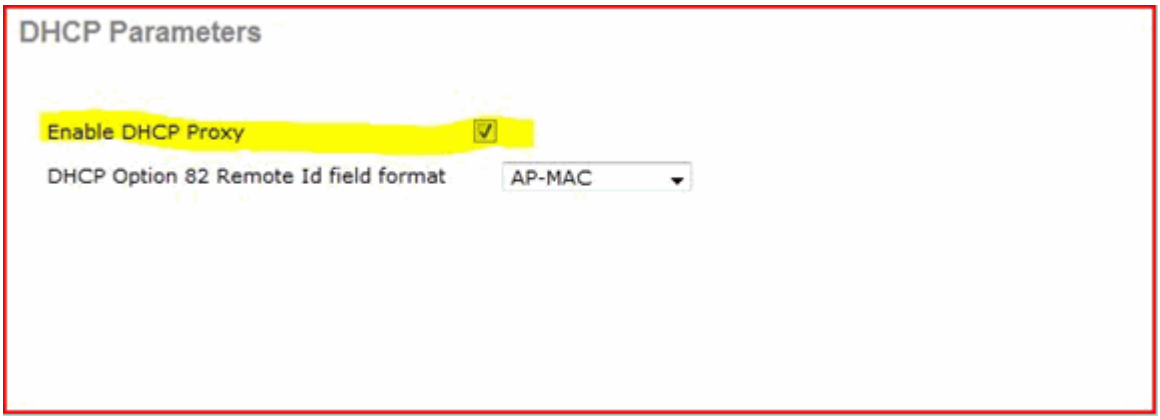


Ejemplo de Configuración del Servidor DHCP Interno

Debe habilitar el proxy DHCP en el controlador para permitir que el servidor DHCP interno funcione. Esto se puede hacer a través de la GUI en esta sección:

Nota: No puede establecer el proxy DHCP a través de la GUI en todas las versiones.

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

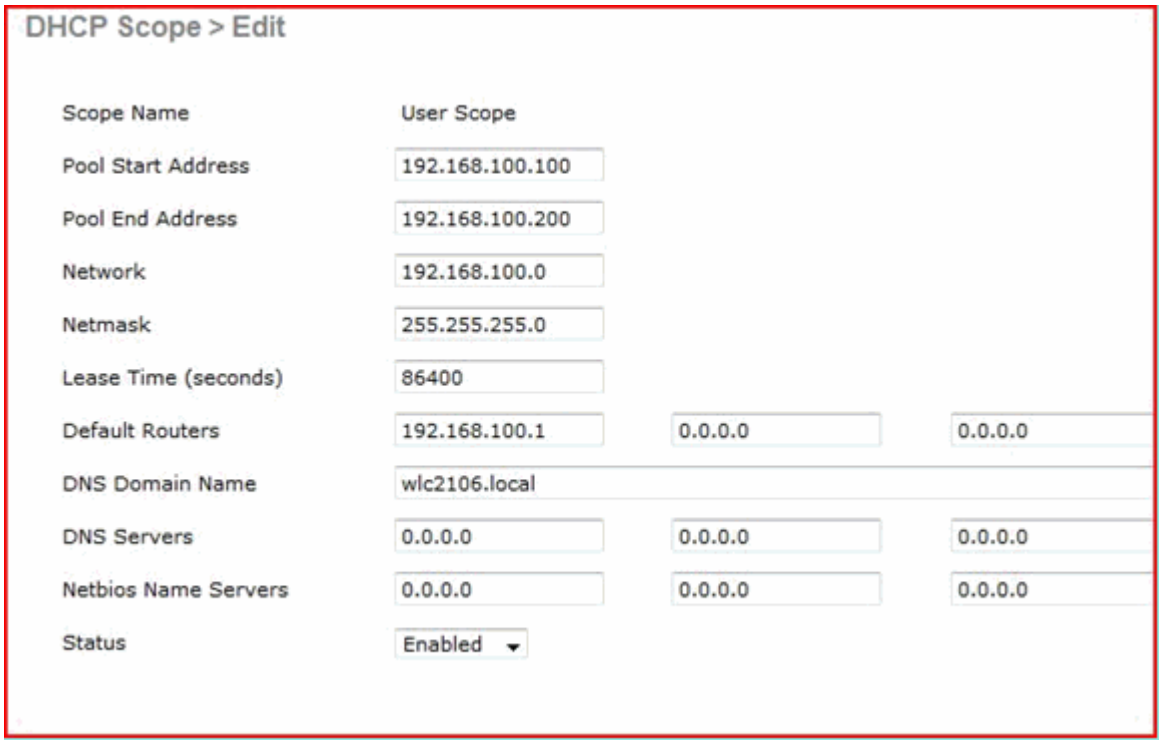


O a través de la CLI:

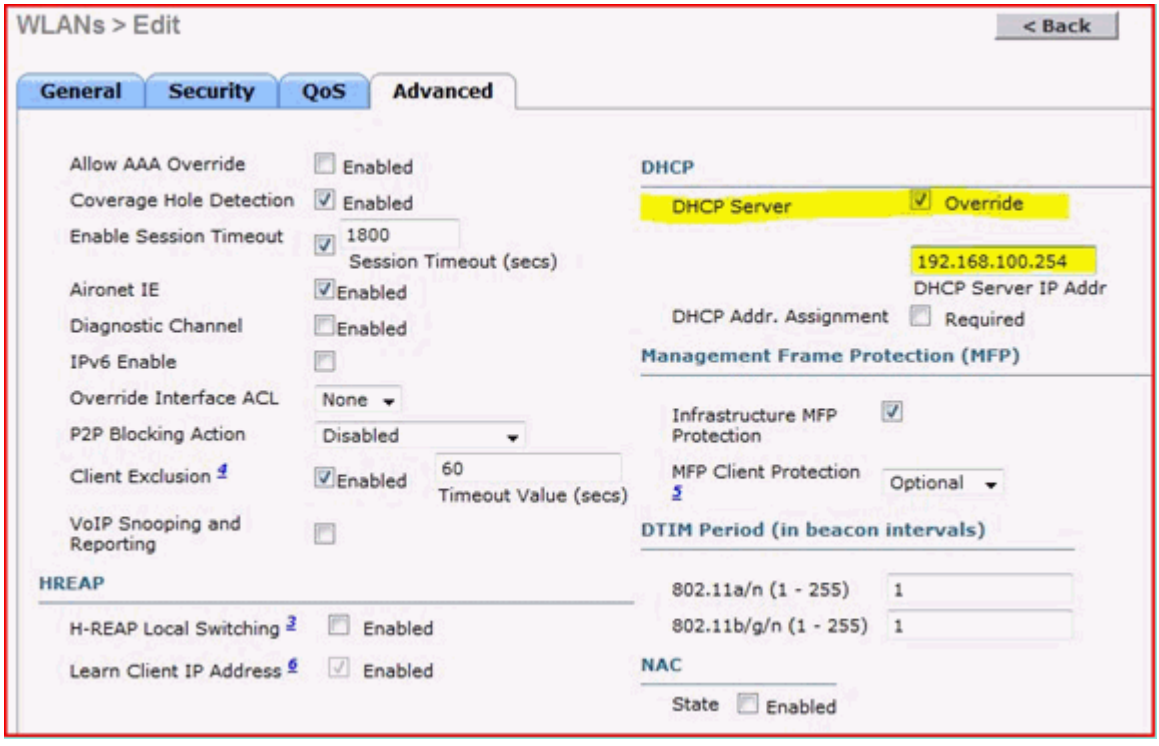
```
Config dhcp proxy enable
Save config
```

Para habilitar el servidor DHCP interno, complete estos pasos:

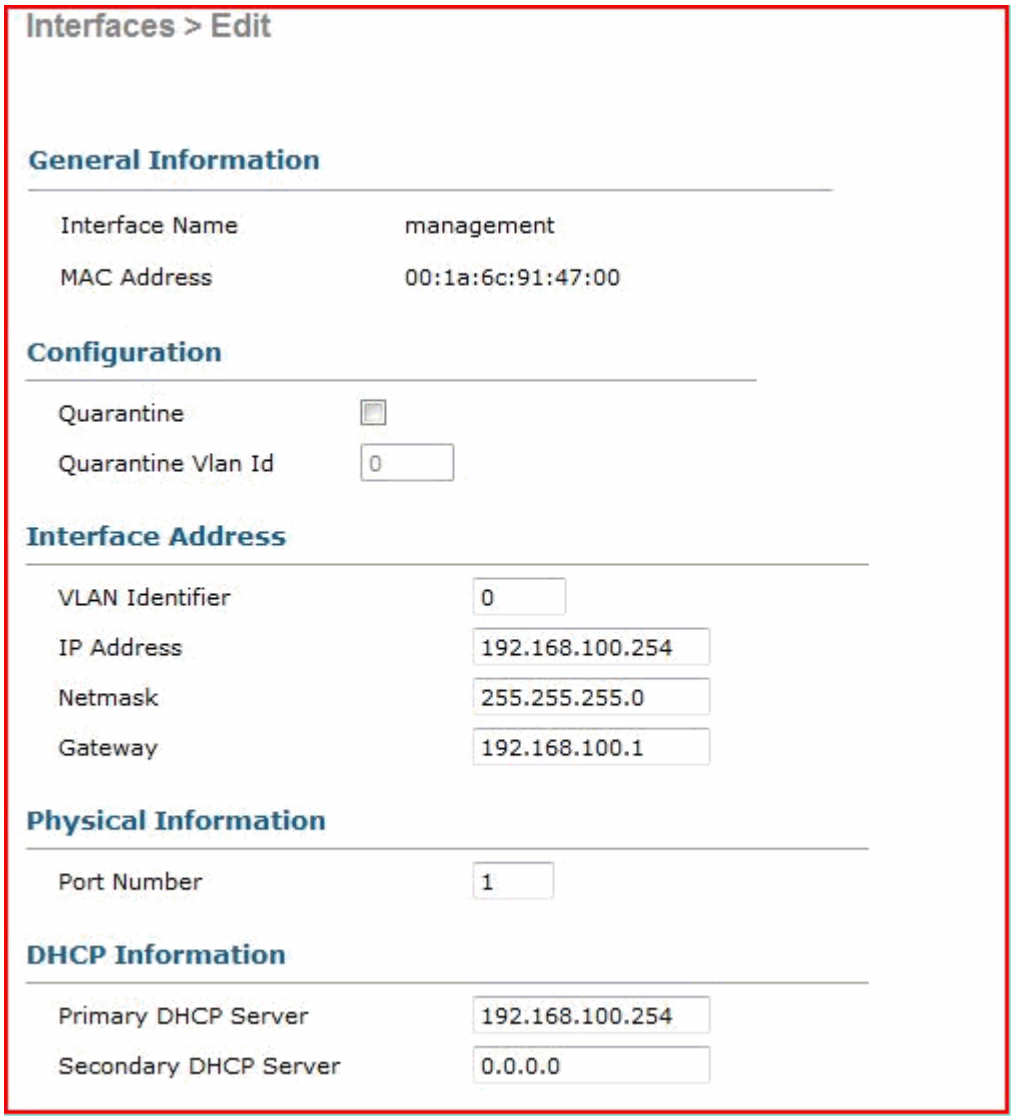
1. Defina un ámbito que utilice para extraer direcciones IP (Controlador > Servidor DHCP interno > Ámbito DHCP). Haga clic en **New**.



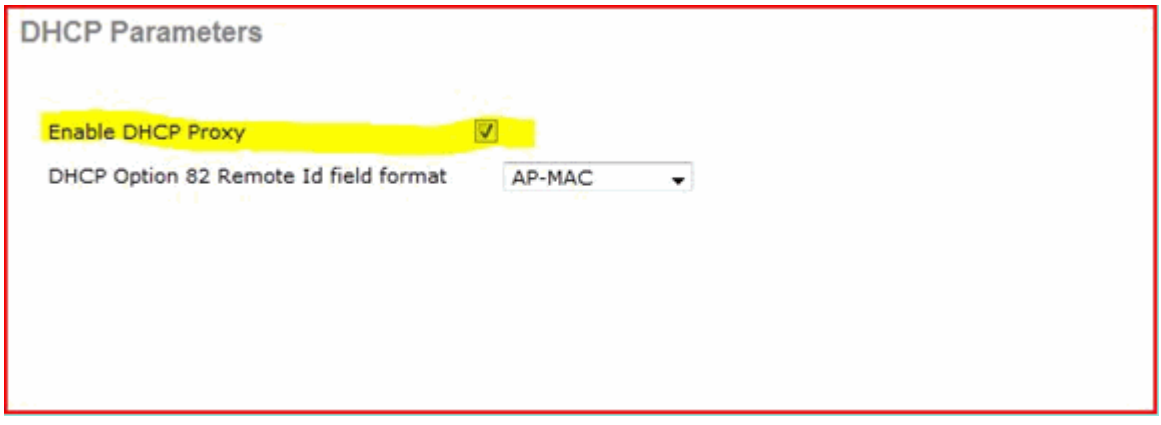
2. Señale la anulación de DHCP a la dirección IP de la interfaz de gestión del controlador.



O bien, puede utilizar la opción DHCP de la configuración de la interfaz del controlador para la interfaz que desea utilizar el servidor DHCP interno.



3. Asegúrese de que el proxy DHCP está activado.



Troubleshoot

Una depuración del servidor DHCP interno requiere generalmente encontrar un cliente que tiene un problema para obtener una dirección IP. Necesita ejecutar estos debugs.

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

El cliente de depuración es una macro que habilita estas depuraciones mientras centra la depuración sólo en la dirección MAC del cliente que ha ingresado.

```
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
```

El principal para problemas de DHCP es el **debug dhcp packet enable** que se habilita automáticamente mediante el comando **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
```

Borre las concesiones DHCP en el servidor DHCP interno del WLC

Puede ejecutar este comando para borrar las concesiones DHCP en el servidor DHCP interno del WLC:

<#root>

```
config dhcp clear-lease
```

Aquí tiene un ejemplo:

<#root>

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

Advertencias

- El proxy DHCP debe estar activado para que funcione el servidor DHCP interno.
- Uso de DHCP al puerto 1067 cuando utiliza el servidor DHCP interno, que se ve afectado por la ACL de la CPU.
- El servidor DHCP interno escucha en la interfaz de loopback del controlador a través del puerto 67 UDP 127.0.0.1.

Interfaz del usuario final

- **config dhcp proxy disable** implica el uso de la función de conexión en puente DHCP. Este es un comando global (no un comando por WLAN).
- El proxy DHCP permanece activado de forma predeterminada.

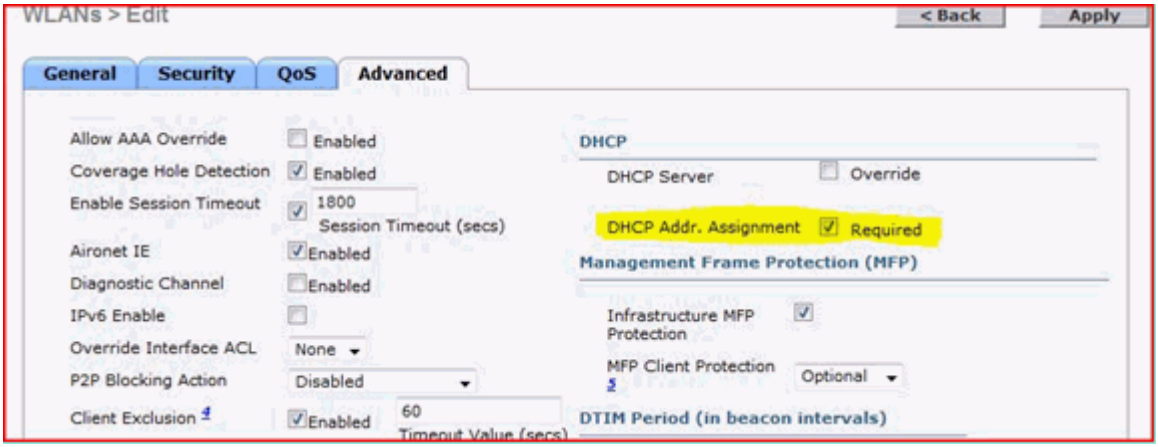
- Cuando el proxy DHCP está desactivado, las WLAN locales no pueden utilizar el servidor DHCP interno. La operación de conexión en puente no es coherente con las operaciones necesarias para redirigir un paquete al servidor interno. En realidad, el bridging significa bridging, con la excepción de la conversión de 802.11 a Ethernet II. Los paquetes DHCP se pasan sin modificar desde el túnel LWAPP a la VLAN del cliente (y viceversa).

- Cuando el proxy está activado, se debe configurar un servidor DHCP en la interfaz WLAN (o en la propia WLAN) para que la WLAN esté activada. No es necesario configurar ningún servidor cuando el proxy está deshabilitado, ya que estos servidores no se utilizan.

- Cuando un usuario intenta habilitar el proxy DHCP, usted verifica internamente que todas las WLANs (o las interfaces asociadas) tienen un servidor DHCP configurado. Si no es así, la operación de habilitación falla.

Se requiere DHCP

La configuración avanzada de WLAN tiene una opción que requiere que los usuarios pasen DHCP antes de pasar al estado RUN (un estado donde el cliente puede pasar el tráfico a través del controlador). Esta opción requiere que el cliente realice una solicitud DHCP completa o media. Lo principal que el controlador busca del cliente es una solicitud DHCP y un ACK que regresa del servidor DHCP. Mientras el cliente realiza estos pasos, el cliente pasa el paso DHCP requerido y pasa al estado RUN.



Roaming L2 y L3

L2 Roam - Si el cliente tiene una concesión DHCP válida y realiza una itinerancia L2 entre dos controladores diferentes en la misma red L2, el cliente no debe necesitar reDHCP y la entrada del cliente debe moverse completamente al nuevo controlador desde el controlador original. Luego, si el cliente necesita volver a DHCP, el proceso de conexión en puente DHCP o proxy en el controlador actual conectaría nuevamente el paquete de forma transparente.

L3 Roam - En un escenario de roaming L3, el cliente se mueve entre dos controladores diferentes en redes L3 diferentes. En esta situación, el cliente se ancla al controlador original y se enumera en la tabla de clientes en el nuevo controlador externo. Durante el escenario de anclaje, el DHCP del cliente es manejado por el controlador de anclaje como los datos del cliente se tunelizan dentro de un túnel EoIP entre los controladores de anclaje y externos.

Información Relacionada

- **Ejemplo de Opción 43 de DHCP para la Configuración de Puntos de Acceso Cisco Aironet en**

Modo Ligero

- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).