

DHCP con el WLC

Contenido

[Introducción](#)

[Servidor DHCP externo](#)

[Comparación del proxy del DHCP y de los modos del bridging](#)

[Modo de representación del DHCP](#)

[Flujo de paquetes del proxy](#)

[Captura de paquetes del proxy](#)

[Ejemplo de la configuración de representación](#)

[Troubleshooting](#)

[Advertencias](#)

[Bridging Mode del DHCP](#)

[Operaciones de bridging del DHCP - Interligar el flujo de paquetes](#)

[Interligando a la captura de paquetes - Perspectiva del cliente](#)

[Interligando a la captura de paquetes - Perspectiva del servidor](#)

[Ejemplo del configuración de Bridging](#)

[Troubleshooting](#)

[Advertencias](#)

[Servidor DHCP interno](#)

[Comparación del DHCP y de los modos internos del bridging](#)

[Servidor DHCP interno - Flujo de paquetes](#)

[Ejemplo interno de la configuración del servidor DHCP](#)

[Troubleshooting](#)

[Borre los arriendos del DHCP en el servidor DHCP interno WLC](#)

[Advertencias](#)

[Interfaz del usuario final](#)

[DHCP requerido](#)

[L2 y L3 que vagan por](#)

[Información Relacionada](#)

Introducción

Este documento describe las diversas operaciones DHCP en el regulador inalámbrico, que proporcionan constante y la información precisa a los administradores que miran para resolver problemas su red.

Servidor DHCP externo

El regulador del Wireless LAN (WLC) soporta dos modos de operaciones DHCP en caso de que utilicen a un servidor DHCP externo:

- Modo de representación del DHCP

- Bridging Mode del DHCP

El modo de representación del DHCP sirve como función del ayudante del DHCP para alcanzar una mejores Seguridad y control sobre las transacciones DHCP entre el servidor DHCP y los clientes de red inalámbrica. El Bridging Mode del DHCP proporciona una opción para hacer el papel del regulador en una transacción DHCP totalmente transparente a los clientes de red inalámbrica.

Comparación del proxy del DHCP y de los modos del bridging

Dirección del DHCP del cliente	Modo de representación del DHCP	Bridging Mode del DHCP
Modifique el giaddr	Sí	No
Modifique el siaddr	Sí	No
Modifique el contenido de paquetes Ofertas	Sí	No
redundantes no remitidas	Sí	No
Soporte de la opción 82	Sí	No
Broadcast al unicast	Sí	No
Soporte BOOTP	No	Servidor
RFC no obediente	El proxy y el Agente Relay no son exactamente el mismo concepto. El Bridging Mode del DHCP se recomienda para la conformidad completa RFC.	

Modo de representación del DHCP

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

Utilizan a la dirección IP virtual del regulador normalmente como la dirección IP de origen de todas las transacciones DHCP al cliente. Como consecuencia, el IP Address del servidor DHCP real no se expone en el aire. Esto IP virtual se visualiza en la salida de los debugs para las transacciones DHCP en el regulador. Sin embargo, el uso de una dirección IP virtual puede causar los problemas en los tipos determinados de clientes.

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

Cuando las ofertas múltiples vienen de los servidores DHCP externos, el proxy del DHCP selecciona normalmente primer que viene adentro y fija la dirección IP del servidor en la estructura de datos del cliente. Como consecuencia, todas las transacciones siguientes pasan a través del mismo servidor DHCP hasta que una transacción falle después de las recomprobaciones. En este momento, el proxy selecciona a un diverso servidor DHCP para el cliente.

El proxy del DHCP se habilita por abandono. Todos los reguladores que comunicarán deben tener la misma configuración de representación del DHCP.

Nota: El proxy del DHCP se debe habilitar para que la opción DHCP 82 de actuar correctamente.

Flujo de paquetes del proxy

Captura de paquetes del proxy

Cuando el regulador está en el modo de representación del DHCP, no sólo dirige los paquetes DHCP al servidor DHCP, él construye realmente los nuevos paquetes DHCP para remitir al servidor DHCP. Todas las opciones DHCP que están presentes en los paquetes DHCP del cliente se copian en los paquetes DHCP del regulador. Los ejemplos del tiro de siguiente pantalla muestran esto para un paquete de pedido de DHCP.

Perspectiva del cliente

Este tiro de pantalla está de una captura de paquetes tomada de la perspectiva del cliente. Muestra que un DHCP descubre, oferta de DHCP, pedido de DHCP, y un DHCP ACK. Se resalta el pedido de DHCP y se amplía el detalle del protocolo BOOTP, que muestra las opciones DHCP.

Perspectiva del servidor

Este tiro de pantalla está de una captura de paquetes tomada de la perspectiva del servidor. Similar al ejemplo anterior, muestra que un DHCP descubre, oferta de DHCP, pedido de DHCP, y un DHCP ACK. Sin embargo, éstos son los paquetes que el regulador construyó en función del proxy del DHCP. Una vez más se resalta el pedido de DHCP y se amplía el detalle del protocolo BOOTP, que muestra las opciones DHCP. Note que son lo mismo que en el paquete de pedido de DHCP de los clientes. También observe que el proxy del WLC retransmite los direccionamientos del paquete y del paquete del resaltado.

Ejemplo de la configuración de representación

Para utilizar el regulador como proxy del DHCP, la característica del proxy del DHCP se debe habilitar en el regulador. Por abandono, se habilita esta característica. Para habilitar el proxy del DHCP, este comando CLI puede ser utilizado. Lo mismo está disponible en el GUI en la página del regulador en el menú del DHCP.

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

Para que el proxy del DHCP trabaje, un servidor DHCP primario debe ser configurado en cada interfaz del regulador que requiera los servicios del DHCP. Un servidor DHCP puede ser configurado en la interfaz de administración, interfaz del ap-administrador, y en las interfaces dinámicas. Estos comandos CLI pueden ser utilizados para configurar a un servidor DHCP para cada interfaz.

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

El DHCP que interliga la característica es una configuración global, así que afecta a todas las transacciones DHCP dentro del regulador.

Troubleshooting

Ésta es la salida del **comando debug dhcp packet enable**. El debug muestra un regulador que reciba un pedido de DHCP de un cliente con la dirección MAC 00:40:96:b4:8c:e1, transmita un pedido de DHCP al servidor DHCP, reciba una contestación del servidor DHCP, y envíe una oferta de DHCP al cliente.

```
(Cisco Controller) >debug dhcp message enable Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP
received op BOOTREQUEST (1)
(len 312, port 29, encap 0xec03) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len
(including the magic cookie) 76 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message
type = DHCP REQUEST Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 61 (len 7) -
skipping Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: requested ip = 50.101.2.7 Thu
Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 12 (len 7) - skipping Thu Jun 25 21:48:55
2009: 00:40:96:b4:8c:e1 DHCP option: 81 (len 11) - skipping Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP option: vendor class id = MSFT 5.0 (len 8) Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP option: 55 (len 11) - skipping Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP options end, len 76, actual 68 Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP selecting relay 1 - control block settings: dhcpServer: 0.0.0.0,
dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0 Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP selected relay 1 - 11.0.0.11
(local address 50.101.0.11, gateway 50.101.0.1, VLAN 101, port 29) Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP transmitting DHCP REQUEST (3) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1
DHCP op: BOOTREQUEST, htype: Ethernet,
hlen: 6, hops: 1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP xid: 0xfc3c9979 (4231829881),
secs: 0,
flags: 0 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP chaddr: 00:40:96:b4:8c:e1 Thu Jun 25
21:48:55 2009: 00:40:96:b4:8c:e1 DHCP ciaddr: 0.0.0.0, yiaddr: 0.0.0.0 Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP siaddr: 0.0.0.0, giaddr: 50.101.0.11 Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP requested ip: 50.101.2.7 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP
Forwarding DHCP packet (332 octets)
-- packet received on direct-connect port requires forwarding to external DHCP
server. Next-hop is 50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REQUEST
to 50.101.0.1
(len 350, port 29, vlan 101) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selecting relay 2
- control block settings: dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0, dhcpGateway: 0.0.0.0,
dhcpRelay: 50.101.0.11 VLAN: 101 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP selected relay
2 - NONE Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP received op BOOTREPLY (2) (len 316,
port 29,
encap 0xec00) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option len (including the magic
cookie) 80 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: message type = DHCP ACK Thu
Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 58 (len 4) - skipping Thu Jun 25 21:48:55
2009: 00:40:96:b4:8c:e1 DHCP option: 59 (len 4) - skipping Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP option: lease time = 691200 seconds Thu Jun 25 21:48:55 2009:
00:40:96:b4:8c:e1 DHCP option: server id = 11.0.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1
DHCP option: netmask = 255.255.0.0 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: 15
(len 14) - skipping Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: gateway =
50.101.0.1 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: DNS server, cnt = 1, first =
11.0.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP option: WINS server, cnt = 1, first =
11.0.0.11 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP options end, len 80, actual 72 Thu
Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP setting server from ACK (server 11.0.0.11,
yiaddr 50.101.2.7) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 Assigning Address 50.101.2.7 to
mobile Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP sending REPLY to STA (len 424, port 29,
vlan 20) Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP transmitting DHCP ACK (5) Thu Jun 25
21:48:55 2009: 00:40:96:b4:8c:e1 DHCP op: BOOTREPLY, htype: Ethernet, hlen: 6,
hops: 0 Thu Jun 25 21:48:55 2009: 00:40:96:b4:8c:e1 DHCP xid: 0xfc3c9979 (4231829881), secs: 0,
flags: 0 Thu Jun 25 21:48:59 2009: 00:40:96:b4:8c:e1 DHCP chaddr: 00:40:96:b4:8c:e1 Thu Jun 25
21:48:59 2009: 00:40:96:b4:8c:e1 DHCP ciaddr: 0.0.0.0, yiaddr: 50.101.2.7 Thu Jun 25 21:48:59
```

2009: 00:40:96:b4:8c:e1 DHCP siaddr: 0.0.0.0, giaddr: 0.0.0.0 Thu Jun 25 21:48:59 2009:
00:40:96:b4:8c:e1 DHCP server id: 1.1.1.1 rcvd server id: 11.0.0.11

Advertencias

- Los problemas de interoperabilidad pueden existir entre un regulador con el proxy del DHCP habilitado y los dispositivos que actúan como un Firewall y servidor DHCP. Esto es muy probablemente debido al componente del Firewall del dispositivo pues los Firewall no responden generalmente a las peticiones del proxy. La solución alternativa para este problema es inhabilitar el proxy del DHCP en el regulador.
- Cuando un cliente está en el estado del REQ del DHCP en el regulador, el regulador cae los paquetes del DHCP inform. El cliente no entrará un estado de FUNCIONAMIENTO en el regulador (éste se requiere para que al cliente pase el tráfico) hasta que reciba un DHCP descubra el paquete del cliente. Los paquetes del DHCP inform son remitidos por el regulador cuando se inhabilita el proxy del DHCP.
- Todos los reguladores que comunicarán deben tener la misma configuración de representación del DHCP.

Bridging Mode del DHCP

El DHCP que interliga la característica se diseña para hacer el papel del regulador en la transacción DHCP totalmente transparente al cliente. A excepción del 802.11 a la conversión del Ethernet II, los paquetes del cliente se interligan sin modificar del túnel del protocolo del Lightweight Access Point (LWAPP) al VLA N del cliente (o a los Ethernetes sobre IP (EoIP) haga un túnel en el caso de itinerancia L3). Semejantemente, a excepción del Ethernet II a la conversión del 802.11, los paquetes al cliente se interligan sin modificar del VLA N del cliente (o del túnel de EoIP en el caso de itinerancia L3) al túnel del LWAPP. Piense en esto como conexión de un cliente en un switchport y después el cliente realiza una transacción DHCP tradicional.

Operaciones de bridging del DHCP - Interligar el flujo de paquetes

Interligando a la captura de paquetes - Perspectiva del cliente

En el tiro de pantalla de la captura de paquetes del lado del cliente, la diferencia principal entre el cliente que la captura en el modo de representación es el IP real del servidor DHCP se considera en los paquetes de la oferta y Ack en vez de la dirección IP virtual del regulador.

Interligando a la captura de paquetes - Perspectiva del servidor

En el tiro de pantalla atado con alambre de la captura de paquetes usted puede ver que el paquete 40 es el pedido de DHCP interligado transmitido del probar cliente 00:40:96:b6:44:51 a la red alámbrica.

Ejemplo del configuración de Bridging

Para habilitar la funcionalidad de Bridging del DHCP en el regulador, usted debe inhabilitar la característica del proxy del DHCP en el regulador. Esto se puede lograr solamente en el CLI con estos comandos:

```
(Cisco Controllor) >config dhcp proxy disable (Cisco Controllor) >show dhcp proxy DHCP Proxy
```

Behaviour: disabled

Si el servidor DHCP no existe en la misma red de la capa 2 (L2) como el cliente entonces que el broadcast necesitará ser remitido al servidor DHCP en el gateway del cliente usando ayuda IP. Esto es una muestra de esta configuración:

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

El DHCP que interliga la característica es una configuración global, así que afecta a todas las transacciones DHCP dentro del regulador. Usted necesita agregar ayuda IP las declaraciones en la infraestructura cableada para todos los VLA N necesarios en el regulador.

Troubleshooting

Los debugs enumerados aquí fueron habilitados en el regulador CLI y la porción del DHCP de la salida fue extraída para este documento.

```
(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 los debugs del DHCP, hay algunas indicaciones dominantes que el interligar del DHCP es funcionando en el regulador:

Del DHCP paquete Bridged con éxito al DS - Esto significa que el paquete DHCP original del cliente fue interligado, inalterado al sistema de distribución (DS). El DS es la infraestructura cableada.

Del DHCP paquete Bridged con éxito al STA - Este mensaje indica que el paquete DHCP fue interligado, inalterado a la estación (STA). El STA es la máquina del cliente ese DHCP de las solicitudes.

También, usted ve la dirección IP del servidor real enumerada en los debugs, que es 192.168.10.1. Si el proxy del DHCP fuera funcionando en vez del DHCP que interligaba, usted vería a la dirección IP virtual del regulador enumerada para el dirección IP del servidor.

Advertencias

- Por abandono, se habilita el proxy del DHCP.
- Todos los reguladores que comunicarán deben tener la misma configuración de representación del DHCP.
- El proxy del DHCP se debe habilitar para la opción DHCP 82 de trabajar.

Servidor DHCP interno

Presentaron al servidor DHCP interno inicialmente para las sucursales donde no está disponible un servidor DHCP externo. Se diseñó para soportar un pequeño con menos de la red inalámbrica diez (APS) de los Puntos de acceso que está en la misma subred. El servidor interno proporciona los IP Addresses a los clientes de red inalámbrica, directo-conecta los AP, dispositivo-MODE AP en la interfaz de administración, y los pedidos de DHCP que se retransmiten de los AP. No es verdadero servidor DHCP de fines generales. Soporta solamente las funciones limitadas y no las escalará en un despliegue más grande.

Comparación del DHCP y de los modos internos del bridging

Los dos modos principales del DHCP en el regulador son proxy del DHCP o el interligar del DHCP. Con el DHCP interligando el regulador actúa más bien una parte posterior del DHCP con los AP autónomos. Un paquete DHCP entra en el AP vía una asociación del cliente a un Service Set Identifier (SSID) que se conecte a un VLA N. Entonces, el paquete DHCP sale ese VLA N. Si ayuda IP se define en el gateway de la capa 3 de ese VLA N (L3), el paquete se remite a ese servidor DHCP vía el unicast dirigido. El servidor DHCP entonces responde detrás directamente a la interfaz L3 que remitió ese paquete DHCP. Con el proxy del DHCP, es la misma idea, pero toda la expedición se hace directamente en el regulador en vez de la interfaz L3 del VLA N. Por ejemplo, un pedido de DHCP viene adentro a la red inalámbrica (WLAN) del cliente, la red inalámbrica (WLAN) entonces cualquier uso que el servidor DHCP definió en el *or* de la interfaz del VLA N utilizará la función de la invalidación del DHCP de la red inalámbrica (WLAN) para

remitir un paquete DHCP del unicast al servidor DHCP con el campo GIADDR de los paquetes DHCP completado para ser la dirección IP de la interfaz VLAN.

Servidor DHCP interno - Flujo de paquetes

Ejemplo interno de la configuración del servidor DHCP

Usted debe permitir al proxy del DHCP en el regulador para permitir que el servidor DHCP interno funcione. Esto se puede hacer vía el GUI bajo esta sección:

Nota: Usted no puede fijar el proxy del DHCP vía el GUI en todas las versiones.

Controller->Advanced->DHCP

O vía el CLI:

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

Para habilitar al servidor DHCP interno, complete estos pasos:

1. Defina un alcance que usted utilice para tirar de los IP Addresses (regulador > servidor DHCP interno > alcance de DHCP). Haga clic en **New**.
2. Señale cualquier su invalidación del DHCP a la dirección IP de la interfaz de administración de su regulador. O, usted puede utilizar la opción DHCP de la configuración de la interfaz del regulador para la interfaz que usted desea utilizar al servidor DHCP interno.
3. Asegurese que el proxy del DHCP está habilitado.

Troubleshooting

Un debug del servidor DHCP interno es típicamente una cuestión de encontrar a un cliente que tenga un problema que consigue una dirección IP. Usted necesita ejecutar estos debugs.

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

El cliente del debug es una macro que habilita estos debugs para usted mientras que se centra el debug hacia fuera solamente en el MAC Address del cliente que usted 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 por problemas de DHCP es el comando **debug dhcp packet enable** que es habilitado automáticamente por el **comando client del debug**.

```
00:1b:77:2b:cf:75 dhcpd: received DISCOVER 00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet
(giaddr:192.168.100.254)to 127.0.0.1:67
from 127.0.0.1:1067 00:1b:77:2b:cf:75 sendto (548 bytes) returned 548 00:1b:77:2b:cf:75 DHCP
option len (including the magic cookie) 312 00:1b:77:2b:cf:75 DHCP option: message type = DHCP
OFFER 00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254 00:1b:77:2b:cf:75 DHCP option:
lease time = 86400 seconds 00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping 00:1b:77:2b:cf:75 DHCP option: netmask =
255.255.255.0 00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64 00:1b:77:2b:cf:75 DHCP
```



```
option len (including the magic cookie) 81 00:1b:77:2b:cf:75 DHCP option: message type = DHCP
REQUEST 00:1b:77:2b:cf:75 DHCP option: 61 (len 7) - skipping 00:1b:77:2b:cf:75 DHCP option:
requested ip = 192.168.100.100 00:1b:77:2b:cf:75 DHCP option: server id = 1.1.1.1
00:1b:77:2b:cf:75 DHCP option: 12 (len 14) - skipping 00:1b:77:2b:cf:75 DHCP option: vendor
class id = MSFT 5.0 (len 8) 00:1b:77:2b:cf:75 DHCP option: 55 (len 11) - skipping
00:1b:77:2b:cf:75 DHCP option: 43 (len 3) - skipping 00:1b:77:2b:cf:75 DHCP options end, len 81,
actual 73 00:1b:77:2b:cf:75 DHCP Forwarding packet locally (340 octets) from 192.168.100.254 to
192.168.100.254 dhcpd: Received 340 byte dhcp packet from 0xfe64a8c0 192.168.100.254:68
00:1b:77:2b:cf:75 dhcpd: packet 192.168.100.254 -> 192.168.100.254 using scope "User Scope"
00:1b:77:2b:cf:75 dhcpd: received REQUEST 00:1b:77:2b:cf:75 Checking node 192.168.100.100
Allocated 1246985143, Expires 1247071543
(now: 1246985143) 00:1b:77:2b:cf:75 dhcpd: server_id = c0a864fe 00:1b:77:2b:cf:75 dhcpd:
server_id = c0a864fe adding option 0x35 adding option 0x36
adding option 0x33 adding option 0x03 adding option 0x0f adding option 0x01 00:1b:77:2b:cf:75
dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67
from 127.0.0.1:1067 00:1b:77:2b:cf:75 sendto (548 bytes) returned 548 00:1b:77:2b:cf:75 DHCP
option len (including the magic cookie) 312 00:1b:77:2b:cf:75 DHCP option: message type = DHCP
ACK 00:1b:77:2b:cf:75 DHCP option: server id = 192.168.100.254 00:1b:77:2b:cf:75 DHCP option:
lease time = 86400 seconds 00:1b:77:2b:cf:75 DHCP option: gateway = 192.168.100.1
00:1b:77:2b:cf:75 DHCP option: 15 (len 13) - skipping 00:1b:77:2b:cf:75 DHCP option: netmask =
255.255.255.0 00:1b:77:2b:cf:75 DHCP options end, len 312, actual 64
```

Borre los arriendos del DHCP en el servidor DHCP interno WLC

Usted puede publicar este comando para borrar los arriendos del DHCP en el servidor DHCP interno del WLC:

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

Aquí tiene un ejemplo:

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

Advertencias

- El proxy del DHCP se debe habilitar para que el servidor DHCP interno funcione.
- Uso del DHCP al puerto 1067 cuando usted utiliza al servidor DHCP interno, que es afectado por el CPU ACL.
- El servidor DHCP interno escucha en el Loopback Interface del regulador vía el puerto 67 de 127.0.0.1 UDP.

Interfaz del usuario final

- El comando **disable del proxy DHCP de los config** implica el uso de la función de Bridging del DHCP. Esto es comando global (no un comando de la por-red inalámbrica (WLAN)).
- Para que los clientes experimenten el comportamiento constante con los despliegues existentes, el proxy del DHCP seguirá habilitado por abandono.
- Cuando se inhabilita el proxy del DHCP, el servidor DHCP interno no puede ser utilizado por los WLAN locales. El Bridging Operation no es constante con las operaciones requeridas para reorientar un paquete al servidor interno. El interligar realmente significa el bridging, a excepción del 802.11 a la conversión del Ethernet II. Los paquetes DHCP se pasan sin modificar del túnel del LWAPP al VLA N del cliente (y viceversa).
- Cuando se habilita el proxy, un servidor DHCP debe ser configurado en la interfaz de la red inalámbrica (WLAN) (o en la red inalámbrica (WLAN) sí mismo) para que la red inalámbrica (WLAN) sea habilitada. Ningún servidor necesita ser configurado cuando se inhabilita el proxy

pues estos servidores no se utilizan.

- Cuando un usuario intenta habilitar el proxy del DHCP, usted internamente verifica que todos los WLAN (o las interfaces asociadas) tengan un servidor DHCP configurado. Si no, la operación del permiso falla.

DHCP requerido

La configuración avanzada de la red inalámbrica (WLAN) tiene una opción que requiera a los usuarios pasar el DHCP antes de entrar el estado de FUNCIONAMIENTO (un estado donde estará capaz el cliente de pasar el tráfico a través del regulador). Esta opción requiere al cliente hacer un pedido de DHCP completo o medio. El punto principal que el regulador busca del cliente es un pedido de DHCP y un ACK que se vuelve del servidor DHCP. Mientras el cliente haga estos pasos, el cliente pasa el paso obligatorio del DHCP y se traslada al estado de FUNCIONAMIENTO.

L2 y L3 que vagan por

El L2 vaga por - Si el cliente tiene un arriendo válido del DHCP y realiza un L2 vaga por entre dos diversos reguladores en la misma red L2, el cliente no debe necesitar el reDHCP y la entrada del cliente se debe mover totalmente al nuevo regulador desde el regulador original. Entonces, si el cliente necesita el DHCP otra vez, el interligar del DHCP o el proceso del proxy en el regulador actual transparente interligaría el paquete otra vez.

El L3 vaga por - En un L3 vague por el escenario que el cliente se mueve entre dos diversos reguladores en diversas redes L3. En esta situación aseguran al regulador original y se enumeran al cliente en la tabla del cliente en el nuevo regulador no nativo. Durante asegurar el escenario el DHCP del cliente es dirigido por el regulador del ancla pues los datos del cliente son tunneled dentro de un túnel de EoIP entre los reguladores no nativos y del ancla.

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](#)