

DHCP com o WLC

Índice

[Introdução](#)

[Servidor de DHCP externo](#)

[Comparação do proxy e dos modos de Bridging DHCP](#)

[Modo de proxy DHCP](#)

[Fluxo de pacote de informação do proxy](#)

[Captura de pacote de informação do proxy](#)

[Exemplo da configuração de proxy](#)

[Troubleshooting](#)

[Caveats](#)

[Modo de Bridging DHCP](#)

[Operações de Bridging DHCP - Construindo uma ponte sobre o fluxo de pacote de informação](#)

[Construindo uma ponte sobre a captura de pacote de informação - Perspectiva do cliente](#)

[Construindo uma ponte sobre a captura de pacote de informação - Perspectiva do server](#)

[Exemplo da configuração de Bridging](#)

[Troubleshooting](#)

[Caveats](#)

[Servidor DHCP interno](#)

[Comparação do DHCP interno e dos modos de Bridging](#)

[Servidor DHCP interno - Fluxo de pacote de informação](#)

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

[Troubleshooting](#)

[Cancele os aluguéis de DHCP no servidor DHCP interno do WLC](#)

[Caveats](#)

[Interface de usuário final](#)

[DHCP exigido](#)

[L2 e L3 que vagueiam](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as operações de DHCP diferentes no controlador wireless, que fornecem consistente e a informação precisa aos administradores que olham para pesquisar defeitos sua rede.

Servidor de DHCP externo

O controlador do Wireless LAN (WLC) apoia dois modos de operações de DHCP caso que um servidor de DHCP externo é usado:

- Modo de proxy DHCP

- Modo de Bridging DHCP

Saques do modo de proxy DHCP como uma função do ajudante DHCP a fim conseguir a melhores Segurança e controle sobre transações de DHCP entre o servidor DHCP e os clientes Wireless. O modo de Bridging DHCP fornece uma opção para fazer o papel do controlador em uma transação de DHCP inteiramente transparente aos clientes Wireless.

Comparação do proxy e dos modos de Bridging DHCP

Tratando o cliente DHCP	Modo de proxy DHCP	Modo de Bridging DHCP
Altere o giaddr	Sim	Não
Altere o siaddr	Sim	Não
Altere o conteúdo de pacote de informação	Sim	Não
Ofertas redundantes não enviadas	Sim	Não
Apoio da opção 82	Sim	Não
Transmissão ao unicast	Sim	Não
Apoio BOOTP	Não	Serviço
RFC NON-complacente	O proxy e o agente de transmissão não são exatamente o mesmo conceito. O modo de Bridging DHCP é recomendado para a conformidade completa RFC.	Não

Modo de proxy DHCP

O proxy DHCP não é ideal para todos os ambientes de rede. O controlador altera e retransmite todas as transações de DHCP para fornecer a função do ajudante e para endereçar determinadas questões de segurança.

O endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador é usado normalmente como o endereço IP de origem de todas as transações de DHCP ao cliente. Em consequência, o endereço IP de servidor DHCP real não é exposto no ar. Este IP virtual é indicado no resultado do debug para transações de DHCP no controlador. Contudo, o uso de um endereço IP de Um ou Mais Servidores Cisco ICM NT virtual pode causar edições em determinados tipos de clientes.

A operação do modo de proxy DHCP mantém o mesmo comportamento para protocolos simétricos e assimétricos da mobilidade.

Quando as ofertas múltiplas vêm dos servidores de DHCP externos, o proxy DHCP seleciona normalmente primeiro que entra e ajusta o endereço IP de Um ou Mais Servidores Cisco ICM NT do server na estrutura de dados do cliente. Em consequência, todas as seguintes transações atravessam o mesmo servidor DHCP até que uma transação falhe após novas tentativas. Neste momento, o proxy seleciona um servidor DHCP diferente para o cliente.

O proxy DHCP é permitido à revelia. Todos os controladores que se comunicarão devem ter o mesmo ajustes do proxy DHCP.

Nota: O proxy DHCP deve ser permitido para que a opção de DHCP 82 operar-se corretamente.

Fluxo de pacote de informação do proxy

Captura de pacote de informação do proxy

Quando o controlador reage do modo de proxy DHCP, dirige não somente pacotes DHCP ao servidor DHCP, ele constrói realmente pacotes DHCP novos para enviar ao servidor DHCP. Todas as opções de DHCP que estão presente nos pacotes DHCP do cliente são copiadas nos pacotes DHCP do controlador. Os exemplos do tiro de tela seguinte mostram este para um pacote de requisição DHCP.

Perspectiva do cliente

Este tiro de tela é de uma captura de pacote de informação tomada da perspectiva do cliente. Mostra que um DHCP descobre, oferta de DHCP, requisição DHCP, e um DHCP ACK. A requisição DHCP é destacada e o detalhe de protocolo BOOTP é expandido, que mostra as opções de DHCP.

Perspectiva do server

Este tiro de tela é de uma captura de pacote de informação tomada da perspectiva do server. Similar ao exemplo anterior, mostra que um DHCP descobre, oferta de DHCP, requisição DHCP, e um DHCP ACK. Contudo, estes são os pacotes que o controlador construiu em função do proxy DHCP. Além disso, a requisição DHCP é destacada e o detalhe de protocolo BOOTP é expandido, que mostra as opções de DHCP. Observe que são os mesmos que no pacote de requisição DHCP dos clientes. Igualmente note que o proxy WLC retransmite endereços do pacote e do pacote do destaque.

Exemplo da configuração de proxy

A fim usar o controlador como um proxy DHCP, a característica do proxy DHCP deve ser permitida no controlador. À revelia, esta característica é permitida. A fim permitir o proxy DHCP, este comando CLI pode ser usado. O mesmo está disponível no GUI na página do controlador no menu DHCP.

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

Para que o proxy DHCP trabalhe, um servidor DHCP preliminar deve ser configurado em cada relação do controlador que exige serviços DHCP. Um servidor DHCP pode ser configurado na interface de gerenciamento, relação do ap-gerente, e em interfaces dinâmica. Estes comandos CLI podem ser usados a fim configurar um servidor DHCP para cada relação.

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

O DHCP que constrói uma ponte sobre a característica é uma configuração global, assim que afeta todas as transações de DHCP dentro do controlador.

Troubleshooting

Esta é a saída do comando **debug dhcp packet enable**. Debugar mostra um controlador que receba uma requisição DHCP de um cliente com MAC address 00:40:96:b4:8c:e1, transmita uma requisição DHCP ao servidor DHCP, receba uma resposta do servidor DHCP, e envie uma oferta de DHCP ao 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
```

Caveats

- As questões de interoperabilidade podem existir entre um controlador com o proxy DHCP

permitido e os dispositivos que atuam como um Firewall e o servidor DHCP. Isto é muito provavelmente devido ao componente do Firewall do dispositivo porque os Firewall geralmente não respondem às solicitações de proxy. A ação alternativa para esta edição é desabilitar o proxy DHCP no controlador.

- Quando um cliente está no estado do REQ DHCP no controlador, o controlador deixa cair pacotes do DHCP inform. O cliente não entrará em um estado de CORRIDA no controlador (este está exigido para que o cliente passe o tráfego) até que receba um DHCP descobrir o pacote do cliente. Os pacotes do DHCP inform estão enviados pelo controlador quando o proxy DHCP é desabilitado.
- Todos os controladores que se comunicarão devem ter o mesmo ajustes do proxy DHCP.

Modo de Bridging DHCP

O DHCP que constrói uma ponte sobre a característica é projetado fazer o papel do controlador na transação de DHCP inteiramente transparente ao cliente. À exceção do 802.11 à conversão do Ethernet II, os pacotes do cliente são construídos uma ponte sobre unmodified do túnel de pouco peso do protocolo do Access point (LWAPP) ao VLAN do cliente (ou dos Ethernet sobre IP (EoIP) escave um túnel no caso L3 vagueando). Similarmente, à exceção do Ethernet II à conversão do 802.11, os pacotes ao cliente são construídos uma ponte sobre unmodified do VLAN do cliente (ou do túnel de EoIP no caso L3 vagueando) ao túnel LWAPP. Pense disto como prender um cliente em um switchport e então o cliente execute uma transação de DHCP tradicional.

Operações de Bridging DHCP - Construindo uma ponte sobre o fluxo de pacote de informação

Construindo uma ponte sobre a captura de pacote de informação - Perspectiva do cliente

No tiro de tela da captura de pacote de informação do lado do cliente, o principal diferença entre o cliente que a captação do modo de proxy reage o IP real do servidor DHCP é considerado nos pacotes da oferta e Ack em vez do endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador.

Construindo uma ponte sobre a captura de pacote de informação - Perspectiva do server

No tiro de tela prendido da captura de pacote de informação você pode ver que o pacote 40 é a transmissão construída uma ponte sobre da requisição DHCP do cliente de teste 00:40:96:b6:44:51 à rede ligada com fio.

Exemplo da configuração de Bridging

A fim permitir a funcionalidade bridging DHCP no controlador, você deve desabilitar a característica do proxy DHCP no controlador. Isto pode somente ser realizado no CLI com estes comandos:

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

Se o servidor DHCP não existe na mesma rede da camada 2 (L2) como o cliente então que a transmissão deverá ser enviada ao servidor DHCP no gateway do cliente usando um ajudante de IP. Esta é uma amostra desta configuração:

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

O DHCP que constrói uma ponte sobre a característica é uma configuração global, assim que afeta todas as transações de DHCP dentro do controlador. Você precisa de adicionar indicações do ajudante de IP na infraestrutura ligada com fio para todos os VLAN necessários no controlador.

Troubleshooting

Debuga alistado aqui foram permitidos no controlador CLI e a parcela DHCP da saída foi 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
```

Neste resultado do debug DHCP, há algumas indicações chaves que a construção de uma ponte sobre DHCP está no uso no controlador:

DHCP pacote interligado com sucesso ao DS - Isto significa que o pacote DHCP original do cliente esteve construído uma ponte sobre, inalterado ao sistema de distribuição (DS). O DS é a infraestrutura ligada com fio.

DHCP pacote interligado com sucesso ao STA - Esta mensagem indica que o pacote DHCP esteve construído uma ponte sobre, inalterado à estação (STA). O STA é a máquina cliente que pede o DHCP.

Também, você vê que o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor real alistado no debuga, que é 192.168.10.1. Se o proxy DHCP estava no uso em vez do DHCP que constrói uma ponte sobre, você veria o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual do controlador alistado para o endereço IP do servidor.

Caveats

- À revelia, o proxy DHCP é permitido.
- Todos os controladores que se comunicarão devem ter o mesmo ajustes do proxy DHCP.
- O proxy DHCP deve ser permitido para a opção de DHCP 82 trabalhar.

Servidor DHCP interno

O servidor DHCP interno foi introduzido inicialmente para os escritórios filiais onde um servidor de DHCP externo não está disponível. É projetado apoiar com menos do que uma rede Wireless pequena dez Access point (AP) que esteja na mesma sub-rede. O servidor interno fornece endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes Wireless, direto-conecta AP, dispositivo-MODE AP na interface de gerenciamento, e requisições DHCP que são retransmitidas dos AP. Não é um servidor DHCP de uso geral desenvolvido. Apoia somente funcionalidade limitada e não a escalará em um desenvolvimento maior.

Comparação do DHCP interno e dos modos de Bridging

Os dois modos principais DHCP no controlador são proxy DHCP ou construção de uma ponte sobre DHCP. Com o DHCP que constrói uma ponte sobre o controlador atua mais como um DHCP para trás com AP autônomos. Um pacote DHCP entra o AP através de uma associação de cliente a um Service Set Identifier (SSID) que seja ligada a um VLAN. Então, o pacote DHCP sai esse VLAN. Se um ajudante de IP está definido no gateway da camada 3 desse VLAN (L3), o pacote está enviado a esse servidor DHCP através do unicast dirigido. O servidor DHCP responde então para trás diretamente à relação L3 que enviou esse pacote DHCP. Com proxy DHCP, é a mesma ideia, mas toda a transmissão é feita diretamente no controlador em vez da relação L3 do VLAN. Por exemplo, uma requisição DHCP entra ao WLAN do cliente, o WLAN então um ou outro uso que o servidor DHCP definida no *or* da relação do VLAN usará a função da ultrapassagem DHCP do WLAN para enviar um pacote DHCP do unicast ao servidor DHCP com o campo GIADDR dos pacotes DHCP completado para ser o endereço IP de Um ou Mais

Servidores Cisco ICM NT da interface de VLAN.

Servidor DHCP interno - Fluxo de pacote de informação

Exemplo interno da configuração do servidor de DHCP

Você deve permitir o proxy DHCP no controlador a fim permitir que o servidor DHCP interno funcione. Isto pode ser feito através do GUI sob esta seção:

Nota: Você não pode ajustar o proxy DHCP através do GUI em todas as versões.

Controller->Advanced->DHCP

Ou através do CLI:

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

A fim permitir o servidor DHCP interno, termine estas etapas:

1. Defina um espaço que você se use para puxar endereços IP de Um ou Mais Servidores Cisco ICM NT (controlador > servidor DHCP interno > escopo de DHCP). Clique em **New**.
2. Aponte uma ou outra sua ultrapassagem DHCP ao endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento de seu controlador. Ou, você pode usar a opção de DHCP da configuração da interface do controlador para a relação que você deseja usar o servidor DHCP interno.
3. Certifique-se de que o proxy DHCP está permitido.

Troubleshooting

Debugar do servidor DHCP interno é tipicamente uma matéria de encontrar um cliente que tenha um problema que obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT. Você precisa de executar estes debuga.

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

O cliente debugar é um macro que permita estes debugue para você quando se centrar debugar para fora somente sobre o endereço MAC de cliente que você incorporou.

```
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
```

Principal para questões de DHCP é o **comando debug dhcp packet enable** que é permitido automaticamente pelo **comando client debugar**.

```
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
```

Cancele os aluguéis de DHCP no servidor DHCP interno do WLC

Você pode emitir este comando a fim cancelar os aluguéis de DHCP no servidor DHCP interno do WLC:

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

Aqui está um exemplo:

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

Caveats

- O proxy DHCP deve ser permitido para que o servidor DHCP interno funcione.
- Uso do DHCP à porta 1067 quando você usar o servidor DHCP interno, que está afetado pelo CPU ACL.
- O servidor DHCP interno escuta na interface de loopback do controlador através da porta 67 de 127.0.0.1 UDP.

Interface de usuário final

- O comando `disable` do proxy DHCP da configuração implica o uso da função de Bridging DHCP. Este é um comando global (não um comando por-WLAN).
- Para que os clientes experimentem o comportamento consistente com distribuições existentes, o proxy DHCP permanecerá permitido à revelia.
- Quando o proxy DHCP é desabilitado, o servidor DHCP interno não pode ser usado por WLAN locais. A operação de Bridging não é consistente com as operações exigidas para reorientar um pacote ao servidor interno. Construir uma ponte sobre realmente significa a construção de uma ponte sobre, à exceção do 802.11 à conversão do Ethernet II. Os pacotes DHCP são passados unmodified do túnel LWAPP ao VLAN do cliente (e vice-versa).
- Quando o proxy é permitido, um servidor DHCP deve ser configurado na relação do WLAN (ou no WLAN próprio) para que o WLAN esteja permitido. Nenhum server precisa de ser configurado quando o proxy é desabilitado porque estes server não estão usados.

- Quando um usuário tenta permitir o proxy DHCP, você verifica internamente que todos os WLAN (ou as relações associadas) têm um servidor DHCP configurado. Se não, a operação da possibilidade falha.

DHCP exigido

A configuração avançada WLAN tem uma opção que exija usuários passar o DHCP antes de entrar no estado de CORRIDA (um estado onde o cliente poderá passar o tráfego através do controlador). Esta opção exige o cliente fazer uma requisição DHCP completa ou meia. A coisa mais importante que o controlador procura do cliente é uma requisição DHCP e um ACK que volte do servidor DHCP. Enquanto o cliente executa estas etapas, o cliente passa o passo requerido DHCP e transporta-se ao estado de CORRIDA.

L2 e L3 que vagueiam

O L2 vagueia - Se o cliente tem um aluguel de DHCP válido e executa um L2 vagueia entre dois controladores diferentes na mesma rede L2, o cliente não deve precisar o reDHCP e a entrada de cliente deve completamente ser movida para o controlador novo do controlador original. Então, se o cliente precisa o DHCP outra vez, a construção de uma ponte sobre DHCP ou o processo do proxy no controlador atual construiriam uma ponte sobre transparentemente o pacote outra vez.

O L3 vagueia - Em um L3 vagueie a encenação que o cliente se move entre dois controladores diferentes nas redes L3 diferentes. Nesta situação o cliente é ancorado ao controlador original e alistado na tabela do cliente no controlador estrangeiro novo. Durante a ancoragem da encenação o DHCP do cliente está segurado pelo controlador da âncora enquanto os dados do cliente são escavados um túnel dentro de um túnel de EoIP entre os controladores estrangeiros e da 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](#)