

DHCP с WLC

Содержание

[Введение](#)

[Внешний сервер DHCP](#)

[Сравнение прокси DHCP и режимов моста](#)

[Режим проху DHCP](#)

[Поток пакетов прокси](#)

[Захват пакета прокси](#)

[Пример настройки прокси](#)

[Устранение неполадок](#)

[Предупреждения](#)

[Режим моста DHCP](#)

[Операции объединения с помощью моста DHCP - мостовое соединение потока пакетов](#)

[Мостовое соединение захвата пакета - клиентская перспектива](#)

[Мостовое соединение захвата пакета - перспектива сервера](#)

[Пример конфигурации мостов](#)

[Устранение неполадок](#)

[Предупреждения](#)

[Внутренний сервер DHCP](#)

[Сравнение внутреннего DHCP и режимов моста](#)

[Внутренний сервер DHCP - Поток пакетов](#)

[Пример конфигурирования внутреннего сервера DHCP](#)

[Устранение неполадок](#)

[Очистите аренду DHCP на внутреннем сервере DHCP WLC](#)

[Предупреждения](#)

[Интерфейс конечного пользователя](#)

[Требуемый DHCP](#)

[L2 и роуминг L3](#)

[Дополнительные сведения](#)

Введение

Этот документ описывает другие операции DHCP на контроллере беспроводной локальной сети, которые предоставляют последовательные и точные сведения администраторам, которые надеются устранять неполадки их сети.

Внешний сервер DHCP

Контроллер беспроводной локальной сети (WLC) поддерживает два режима операций DHCP в случае, если используется внешний сервер DHCP:

- Режим проху DHCP

- Режим моста DHCP

Режим проху DHCP служит функцией помощника DHCP для достижения лучшей безопасности и контроля над транзакциями DHCP между сервером DHCP и беспроводными клиентами. Режим моста DHCP предоставляет возможность делать роль контроллера в транзакции DHCP совершенно очевидной для беспроводных клиентов.

Сравнение прокси DHCP и режимов моста

Обработка клиентского DHCP	Режим проху DHCP	Режим моста DHCP
Модифицируйте giaddr	Да	Нет
Модифицируйте siaddr	Да	Нет
Модифицируйте содержимое пакета	Да	Нет
Избыточные предложения, не переданные	Да	Нет
Поддержка опции 82	Да	Нет
Широковещание для одноадресной передачи	Да	Нет
Поддержка BOOTP	Нет	Серв
Не соответствующий стандарту RFC	Прокси и агент ретрансляции не являются точно тем же понятием. Режим моста DHCP рекомендуется для полного соответствия RFC.	

Режим проху DHCP

Прокси DHCP не идеален для всех сетевых сред. Контроллер модифицирует и реле, все транзакции DHCP для обеспечения помощника функционируют и обращаются к определенным проблемам безопасности.

Виртуальный IP - адрес контроллера обычно используется в качестве IP - адреса источника всех транзакций DHCP клиенту. В результате реальный IP - адрес сервера DHCP не представлен в воздухе. Это виртуальное IP отображено в выходных данных отладки для транзакций DHCP на контроллере. Однако использование виртуального IP - адреса может вызвать проблемы на определенных типах клиентов.

Операция режима проху DHCP поддерживает то же поведение и для симметричных и для асимметричных протоколов мобильности.

Когда множественные предложения прибывают из внешних серверов DHCP, прокси DHCP обычно выбирает первый, который входит и устанавливает IP-адрес сервера в структуре данных клиента. В результате весь после транзакций проходит тот же сервер DHCP, пока транзакция не отказывает после повторных попыток. На этом этапе прокси выбирает другой сервер DHCP для клиента.

Прокси DHCP включен по умолчанию. Все контроллеры, которые свяжутся, должны иметь тот же параметр прокси DHCP.

Примечание: Прокси DHCP должен быть включен для параметра DHCP 82 для работы

правильно.

Поток пакетов прокси

Захват пакета прокси

Когда контроллер находится в режиме прокси DHCP, он не только направляет пакеты DHCP к серверу DHCP, он фактически создает новые пакеты DHCP для передачи серверу DHCP. Все параметры DHCP, которые присутствуют в пакетах DHCP клиента, скопированы в пакетах DHCP контроллера. Следующие примеры снимка экрана показывают это для пакета запроса DHCP.

Клиентская перспектива

Этот снимок экрана имеет захват пакета, взятый с точки зрения клиента. Это показывает, что DHCP обнаруживает, предложение DHCP, запрос DHCP и ACK DHCP. Запрос DHCP выделен, и сведения о протоколе протокола BOOTP расширены, который показывает параметры DHCP.

Перспектива сервера

Этот снимок экрана имеет захват пакета, взятый с точки зрения сервера. Подобный предыдущему примеру, это показывает, что DHCP обнаруживает, предложение DHCP, запрос DHCP и ACK DHCP. Однако это пакеты, которые контроллер создал как функция прокси DHCP. Снова, запрос DHCP выделен, и сведения о протоколе протокола BOOTP расширены, который показывает параметры DHCP. Заметьте, что они совпадают с в пакете запроса DHCP клиентов. Также обратите внимание, что пакет реле прокси WLC и выделяет пакетные адреса.

Пример настройки прокси

Для использования контроллера в качестве прокси DHCP опция прокси DHCP должна быть активирована на контроллере. По умолчанию эта опция активирована. Для включения прокси DHCP эта команда CLI может использоваться. То же доступно в GUI на странице Controller в меню DHCP.

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

Для прокси DHCP для работы основной сервер DHCP должен быть настроен в каждом интерфейсе контроллера, который требует сервисов DHCP. Сервер DHCP может быть настроен на интерфейсе управления, интерфейсе диспетчера точки доступа, и на динамических интерфейсах. Эти команды CLI могут использоваться для настройки сервера DHCP для каждого интерфейса.

```
(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>
```

Функцией мостового соединения DHCP является глобальный параметр, таким образом, она влияет на все транзакции DHCP в контроллере.

Устранение неполадок

Это - выходные данные команды `debug dhcp packet enable`. Отладка показывает контроллер, который получает запрос DHCP от клиента с MAC-адресом 00:40:96:b4:8c:e1, передает запрос DHCP к серверу DHCP, получает ответ от сервера DHCP и передает предложение DHCP клиенту.

```
(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, encaps 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,
encaps 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
```

Предупреждения

- Проблемы совместимости могут существовать между контроллером с включенным

прокси DHCP и устройствами, которые действуют и как межсетевой экран и как сервер DHCP. Это происходит, скорее всего, из-за компонента межсетевого экрана устройства, поскольку межсетевые экраны обычно не отвечают на запросы прокси. Обходной путь для этой проблемы должен отключить прокси DHCP на контроллере.

- Когда клиент находится в состоянии REQ DHCP на контроллере, отбрасывания контроллера DHCP inform пакеты. Клиент не войдет в состояние ВЫПОЛНЕНИЯ на контроллере (это требуется для клиента передать трафик), пока это не получает DHCP, обнаруживают пакет от клиента. DHCP inform, что пакеты переданы контроллером, когда отключен прокси DHCP.
- Все контроллеры, которые свяжутся, должны иметь тот же параметр прокси DHCP.

Режим моста DHCP

Функция мостового соединения DHCP разработана для создания роли контроллера в транзакции DHCP совершенно очевидной для клиента. За исключением 802.11 к преобразованию Ethernet II, пакеты от клиента соединены немодифицированные от туннеля Протокола точки доступа легкого веса (LWAPP) до VLAN клиента (или Ethernet по IP (EoIP) туннель в случае роуминга L3). Точно так же за исключением Ethernet II к преобразованию 802.11, пакеты клиенту соединены немодифицированные от VLAN клиента (или туннель EoIP в случае роуминга L3) в туннель LWAPP. Думайте об этом как о проводном соединении клиента в порт коммутатора, и затем клиент выполняет традиционную транзакцию DHCP.

Операции объединения с помощью моста DHCP - мостовое соединение потока пакетов

Мостовое соединение захвата пакета - клиентская перспектива

В снимке экрана захвата пакета клиентской стороны основное различие между клиентским перехватом в Режиме проху является реальным IP сервера DHCP, замечен в Предложении и пакетах Ask вместо виртуального IP - адреса контроллера.

Мостовое соединение захвата пакета - перспектива сервера

В проводном снимке экрана захвата пакета вы видите, что пакет 40 является соединённым мостом ширококестанием Запроса DHCP от тестового клиента 00:40:96:b6:44:51 к проводной сети.

Пример конфигурации мостов

Для включения функциональных возможностей моста DHCP на контроллере необходимо отключить опцию прокси DHCP на контроллере. Это может только быть выполнено в CLI с этими командами:

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

Если сервер DHCP не будет существовать в той же сети (L2) Уровня 2 как клиент тогда, то ширококестание должно будет быть передано серверу DHCP в клиентском шлюзе с помощью IP - помощника. Это - выборка этой конфигурации:

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

Функцией мостового соединения DHCP является глобальный параметр, таким образом, она влияет на все транзакции DHCP в контроллере. Необходимо добавить операторы IP - помощника в проводной инфраструктуре для всех необходимых VLAN на контроллере.

Устранение неполадок

Отладки, перечисленные здесь, были включены на CLI контроллера, и часть DHCP выходных данных была извлечена для этого документа.

```
(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
```

В этих выходных данных отладки DHCP существует несколько ключевых индикаций, что мостовое соединение DHCP используется на контроллере:

DHCP успешно пакет моста к DS - Это означает, что исходный пакет DHCP от клиента был соединен, неизменен к системе распределения (DS). DS является проводной инфраструктурой.

DHCP успешно пакет моста к STA - Это сообщение указывает, что пакет DHCP был соединен, неизменен к станции (STA). STA является клиентским компьютером, который запрашивает DHCP.

Кроме того, вы видите IP-адрес реального сервера, перечисленный в отладках, который является 192.168.10.1. Если бы прокси DHCP использовался вместо мостового соединения DHCP, то вы видели бы виртуальный IP - адрес контроллера, перечисленный для IP-адреса сервера.

Предупреждения

- По умолчанию прокси DHCP включен.
- Все контроллеры, которые свяжутся, должны иметь тот же параметр прокси DHCP.
- Прокси DHCP должен быть включен для параметра DHCP 82 для работы.

Внутренний сервер DHCP

Внутренний сервер DHCP был представлен первоначально для филиалов компании, где внешний сервер DHCP не доступен. Это разработано для поддержки маленькой беспроводной сети меньше десять точек доступа (AP), которые находятся в той же подсети. Внутренний сервер предоставляет IP-адреса беспроводным клиентам, AP directconnect, AP режима устройства на интерфейсе управления и запросам DHCP, которые переданы от AP. Это не полноценный сервер DHCP общего назначения. Это только поддерживает ограниченную функциональность и не будет масштабироваться в больших развертываниях.

Сравнение внутреннего DHCP и режимов моста

Два основных режима DHCP на контроллере являются или прокси DHCP или мостовым соединением DHCP. С DHCP, соединяющим контроллер, действует больше как DHCP назад с автономными AP. Пакет DHCP входит в AP через связывание клиента к идентификаторам наборов сервисов (SSID), которые связаны с VLAN. Затем пакет DHCP выходит та VLAN. Если IP - помощник определен на Уровне 3 той VLAN (L3) шлюз, пакет передан к тому серверу DHCP через направленную индивидуальную рассылку. Сервер DHCP тогда назад непосредственно отвечает на L3 интерфейс, который передал тот пакет DHCP. С прокси DHCP это - та же идея, но вся передача сделана непосредственно в контроллере вместо L3 интерфейса VLAN. Например, запрос DHCP входит к WLAN от клиента, WLAN тогда будет или использовать сервер DHCP, определенный на интерфейсе VLAN *или*, будет использовать функцию замены DHCP WLAN для передачи пакета DHCP индивидуальной рассылки серверу DHCP с Полем GIADDR пакетов DHCP, заполненным, чтобы быть IP-адресом интерфейса виртуальной локальной сети (VLAN).

Внутренний сервер DHCP - Поток пакетов

Пример конфигурирования внутреннего сервера DHCP

Необходимо включить прокси DHCP на контроллере, чтобы позволить внутреннему серверу DHCP функционировать. Это может быть сделано через GUI под этим разделом:

Примечание: Вы не в состоянии установить прокси DHCP через GUI во всех версиях.

Controller->Advanced->DHCP

Или через CLI:

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

Для включения внутреннего сервера DHCP выполните эти шаги:

1. Определите область, которую вы будете использовать для получения по запросу IP-адресов (Контроллер> Внутренний сервер DHCP> Область DHCP). **Щелкните New.**
2. Укажите любую свою замену DHCP к IP-адресу интерфейса управления вашего контроллера. Или, можно использовать параметр DHCP конфигурации интерфейса контроллера для интерфейса, вы хотите использовать внутренний сервер DHCP.
3. Удостоверьтесь, что включен прокси DHCP.

Устранение неполадок

Отладка внутреннего сервера DHCP, как правило, является вопросом обнаружения клиента, который имеет проблему при получении IP-адреса. Необходимо выполнить эти отладки.

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

Клиент отладки является макросом, который включает эти отладки для вас, в то время как он фокусирует отладку только на MAC - адресе клиента, который вы ввели.

```
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
```

Основной для проблем DHCP является командой **debug dhcp packet enable**, которая включена автоматически командой **debug client**.

```
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
```

Очистите аренду DHCP на внутреннем сервере DHCP WLC

Можно выполнить эту команду для очистки аренды DHCP на Внутреннем сервере DHCP WLC:

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

Например:

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

Предупреждения

- Прокси DHCP должен быть позволен для Внутреннего сервера DHCP функционировать.
- Использование DHCP к порту 1067, когда вы используете Внутренний сервер DHCP, на который влияет ACL ЦП.
- Внутренний сервер DHCP слушает на интерфейсе обратной связи контроллера через 127.0.0.1 порта 67 UDP.

Интерфейс конечного пользователя

- Команда `config dhcp proxy disable` подразумевает использование функции мостовой передачи DHCP. Это - команда global (не команда на WLAN).
- Для клиентов для испытания последовательного поведения с существующими развертываниями прокси DHCP останется включенным по умолчанию.
- Когда прокси DHCP отключен, Внутренний сервер DHCP не может использоваться локальными WLAN. Операции объединения с помощью моста не совместимы с операциями, требуемыми перенаправить пакет к внутреннему серверу. Мостовое соединение действительно означает соединять, за исключением 802.11 к преобразованию Ethernet II. Пакеты DHCP передают немодифицированные от туннеля LWAPP до VLAN клиента (и наоборот).
- Когда прокси включен, сервер DHCP должен быть настроен на интерфейсе WLAN (или в самом WLAN) для WLAN, который будет включен. Никакой сервер не должен быть настроен, когда прокси отключен, поскольку не используются эти серверы.
- Когда пользователь пытается включить прокси DHCP, вы внутренне проверяете, что всем WLAN (или связанные интерфейсы) настроили сервер DHCP. В противном случае разрешать сбои операции.

Требуемый DHCP

Усовершенствованная конфигурация WLAN имеет опцию, которая требует, чтобы пользователи передали DHCP перед входом в состояние ВЫПОЛНЕНИЯ (состояние, где клиент будет в состоянии передать трафик через контроллер). Эта опция требует, чтобы клиент сделал полный запрос DHCP или половину запроса DHCP. Главное, которое контроллер ищет от клиента, является запросом DHCP и ACK, который возвращается из сервера DHCP. Пока клиент выполняет эти шаги, клиент передает обязательный шаг DHCP и переходит в состояние ВЫПОЛНЕНИЯ.

L2 и роуминг L3

L2 Перемещаются - Если клиент имеет допустимую аренду DHCP и выполняет, L2 перемещаются между двумя другими контроллерами в той же сети L2, клиенту не должно быть нужно к reDHCP, и запись клиента должна быть полностью перемещена в новый контроллер от исходного контроллера. Затем если бы клиент действительно нуждается к DHCP снова, мостовому соединению DHCP или проксирует процесс на текущем контроллере, прозрачно соединил бы пакет снова.

L3 Перемещается - В L3, перемещаются сценарий клиентские шаги между двумя другими контроллерами в других сетях L3. В этой ситуации клиент привязан на исходном контроллере и перечислен в клиентской таблице на новом внешнем контроллере. Во время сценария связывания DHCP клиента обрабатывается якорным контроллером, поскольку данные клиента туннелированы в туннеле EoIP между внешними и якорными контроллерами.

Дополнительные сведения

- [Пример конфигурации DHCP OPTION 43 для облегченных точек доступа Cisco](#)
- [Cisco Systems – техническая поддержка и документация](#)