

Verständnis für den Umgang von AireOS WLCs mit DHCP-Protokollen

Inhalt

[Einleitung](#)
[Externer DHCP-Server](#)
[Vergleich von DHCP-Proxy- und Bridging-Modi](#)
[DHCP-Proxy-Modus](#)
[Proxy-Paketfluss](#)
[Proxy-Paketerfassung](#)
[Kundenperspektive](#)
[Server-Perspektive](#)
[Beispiel für Proxy-Konfiguration](#)
[Fehlerbehebung](#)
[Hinweise](#)
[DHCP-Bridge-Modus](#)
[DHCP-Bridging-Vorgänge - Bridging-Paketfluss](#)
[Bridging-Paketerfassung - Client-Perspektive](#)
[Bridging-Paketerfassung - Server-Perspektive](#)
[Beispiel einer Bridge-Konfiguration](#)
[Fehlerbehebung](#)
[Hinweise](#)
[Interner DHCP-Server](#)
[Vergleich von internem DHCP und Bridging-Modus](#)
[Interner DHCP-Server - Paketfluss](#)
[Konfigurationsbeispiel für internen DHCP-Server](#)
[Fehlerbehebung](#)
[Löschen Sie die DHCP-Leases auf dem internen DHCP-Server des WLC.](#)
[Hinweise](#)
[Endbenutzeroberfläche](#)
[DHCP erforderlich](#)
[L2- und L3-Roaming](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die verschiedenen DHCP-Vorgänge auf dem Cisco AireOS Wireless Controller beschrieben.

Externer DHCP-Server

Der Wireless LAN Controller (WLC) unterstützt bei Verwendung eines externen DHCP-Servers zwei DHCP-Betriebsmodi:

- DHCP-Proxy-Modus
- DHCP-Bridging-Modus

Der DHCP-Proxy-Modus dient als DHCP-Helper-Funktion, um die Sicherheit und Kontrolle von DHCP-

Transaktionen zwischen dem DHCP-Server und den Wireless-Clients zu verbessern. Der DHCP-Bridging-Modus bietet eine Option, um die Controller-Rolle in einer DHCP-Transaktion für die Wireless-Clients vollständig transparent zu machen.

Vergleich von DHCP-Proxy- und Bridging-Modi

Umgang mit Client-DHCP	DHCP-Proxy-Modus	DHCP-Bridge-Modus
Leitfaden ändern	Ja	Nein
Siadr ändern	Ja	Nein
Paketinhalt ändern	Ja	Nein
Nicht weitergeleitete redundante Angebote	Ja	Nein
Unterstützung für Option 82	Ja	Nein
Broadcast an Unicast	Ja	Nein
BOOTP-Unterstützung	Nein	Server
RFC nicht konform	Proxy- und Relay-Agent sind nicht identisch. Für eine vollständige RFC-Konformität wird der DHCP-Bridging-Modus empfohlen.	Nein

DHCP-Proxy-Modus

Der DHCP-Proxy ist nicht für alle Netzwerkkumgebungen geeignet. Der Controller ändert alle DHCP-Transaktionen und leitet sie weiter, um Hilfsfunktionen bereitzustellen und bestimmte Sicherheitsprobleme zu beheben.

Die virtuelle IP-Adresse des Controllers wird normalerweise als Quell-IP-Adresse aller DHCP-Transaktionen mit dem Client verwendet. Dadurch wird die tatsächliche IP-Adresse des DHCP-Servers nicht übertragen. Diese virtuelle IP wird in der Debug-Ausgabe für DHCP-Transaktionen auf dem Controller angezeigt. Die Verwendung einer virtuellen IP-Adresse kann jedoch bei bestimmten Clienttypen zu Problemen führen.

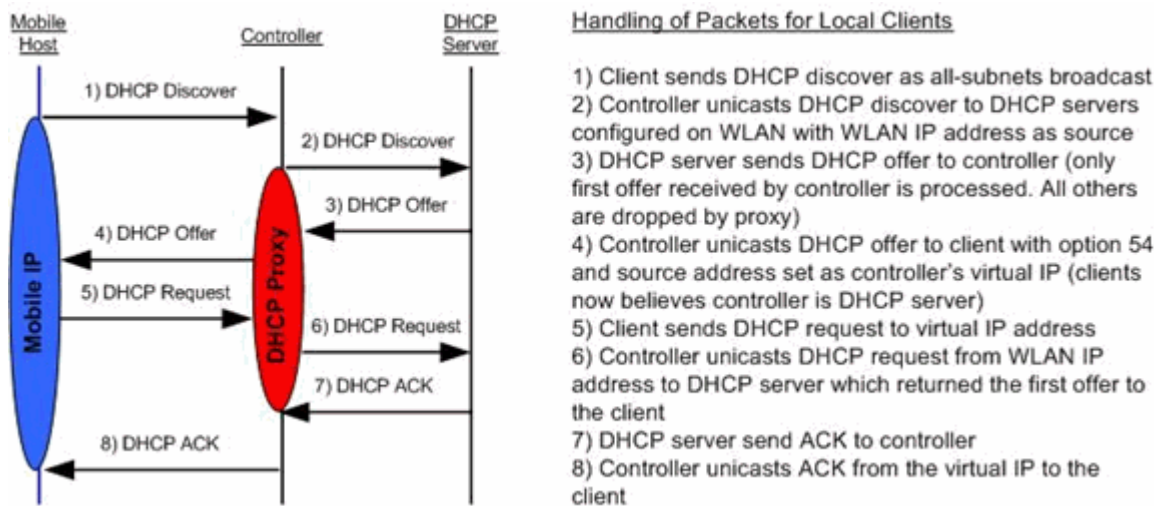
Der DHCP-Proxy-Modus behält das gleiche Verhalten für symmetrische und asymmetrische Mobilitätsprotokolle bei.

Wenn mehrere Angebote von externen DHCP-Servern stammen, wählt der DHCP-Proxy normalerweise den ersten eingehenden aus und legt die IP-Adresse des Servers in der Client-Datenstruktur fest. Daher durchlaufen alle nachfolgenden Transaktionen denselben DHCP-Server, bis eine Transaktion nach einem erneuten Versuch fehlschlägt. An diesem Punkt wählt der Proxy einen anderen DHCP-Server für den Client aus.

Der DHCP-Proxy ist standardmäßig aktiviert. Alle Controller, die miteinander kommunizieren, müssen die gleiche DHCP-Proxysteuerung haben.

Hinweis: Der DHCP-Proxy muss aktiviert sein, damit die DHCP-Option 82 ordnungsgemäß funktioniert.

Proxy-Paketfluss

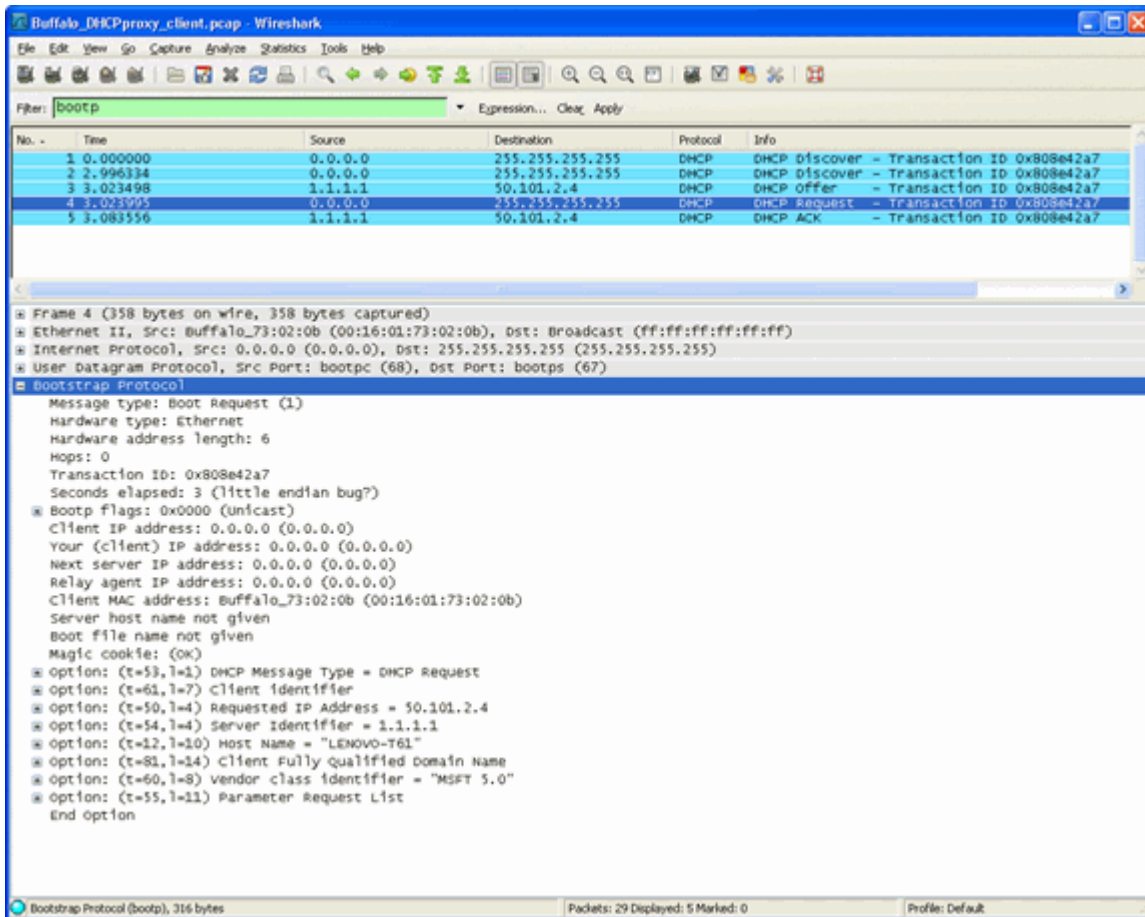


Proxy-Paketerfassung

Wenn sich der Controller im DHCP-Proxy-Modus befindet, leitet er nicht nur DHCP-Pakete an den DHCP-Server weiter, sondern erstellt auch neue DHCP-Pakete für die Weiterleitung an den DHCP-Server. Alle DHCP-Optionen, die in den DHCP-Paketen des Clients vorhanden sind, werden in die DHCP-Pakete des Controllers kopiert. Die nächsten Screenshot-Beispiele zeigen dies für ein DHCP-Anforderungspaket.

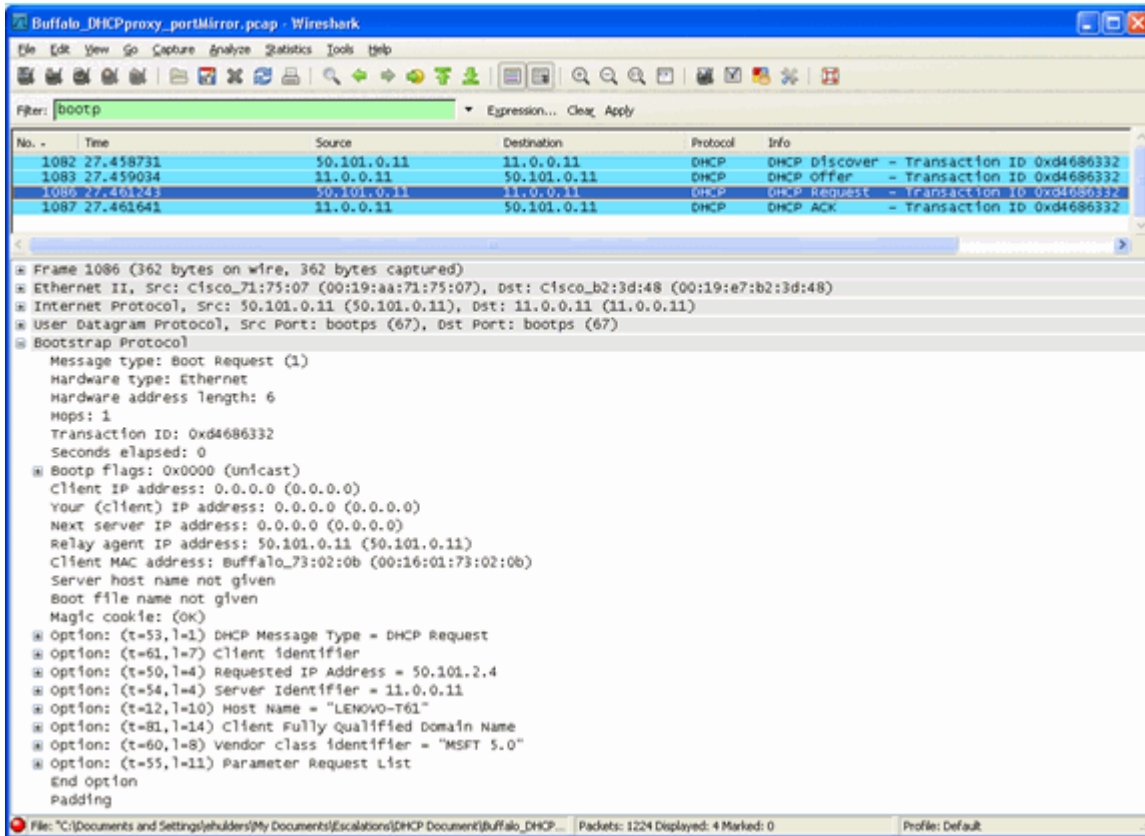
Kundenperspektive

Dieser Screenshot zeigt eine Paketerfassung aus Client-Sicht. Es zeigt eine DHCP-Erkennung, ein DHCP-Angebot, eine DHCP-Anfrage und ein DHCP ACK. Die DHCP-Anfrage ist hervorgehoben, und die Details des Bootprotokolls werden erweitert. Darin werden die DHCP-Optionen angezeigt.



Server-Perspektive

Dieser Screenshot zeigt eine Paketerfassung aus Sicht des Servers. Ähnlich wie im vorherigen Beispiel werden hier eine DHCP-Erkennung, ein DHCP-Angebot, eine DHCP-Anfrage und ein DHCP ACK angezeigt. Hierbei handelt es sich jedoch um Pakete, die der Controller als Funktion des DHCP-Proxys erstellt hat. Die DHCP-Anfrage wird hervorgehoben, und die Details des Bootprotokolls werden erweitert. Darin werden die DHCP-Optionen angezeigt. Beachten Sie, dass sie mit dem DHCP-Anforderungspaket des Clients übereinstimmen. Beachten Sie außerdem, dass der WLC-Proxy ein Paket weiterleitet und Paketadressen hervorhebt.



Beispiel für Proxy-Konfiguration

Damit der Controller als DHCP-Proxy verwendet werden kann, muss die DHCP-Proxy-Funktion auf dem Controller aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Um den DHCP-Proxy zu aktivieren, kann dieser CLI-Befehl verwendet werden. Entsprechendes steht in der GUI auf der Seite Controller im DHCP-Menü zur Verfügung.

```
</root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy enable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

Damit der DHCP-Proxy funktioniert, muss an jeder Controller-Schnittstelle, die DHCP-Dienste benötigt, ein primärer DHCP-Server konfiguriert werden. Ein DHCP-Server kann auf der Management-Schnittstelle, der AP-Manager-Schnittstelle und auf dynamischen Schnittstellen konfiguriert werden. Diese CLI-Befehle können verwendet werden, um einen DHCP-Server für jede Schnittstelle zu konfigurieren.

```
</root>
```

```
(Cisco Controller) >
```

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

```
(Cisco Controller) >
```

```
config interface dhcp management primary
```

```
(Cisco Controller) >
```

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

```
primary
```

Bei der DHCP-Bridging-Funktion handelt es sich um eine globale Einstellung, die alle DHCP-Transaktionen innerhalb des Controllers beeinflusst.

Fehlerbehebung

Dies ist die Ausgabe des `debug dhcp packet enable` aus. Das Debugging zeigt einen Controller, der eine DHCP-Anfrage von einem Client mit der MAC-Adresse 00:40:96:b4:8c:e1 empfängt, eine DHCP-Anfrage an den DHCP-Server sendet, eine Antwort vom DHCP-Server erhält und ein DHCP-Angebot an den Client sendet.

```
<#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
```

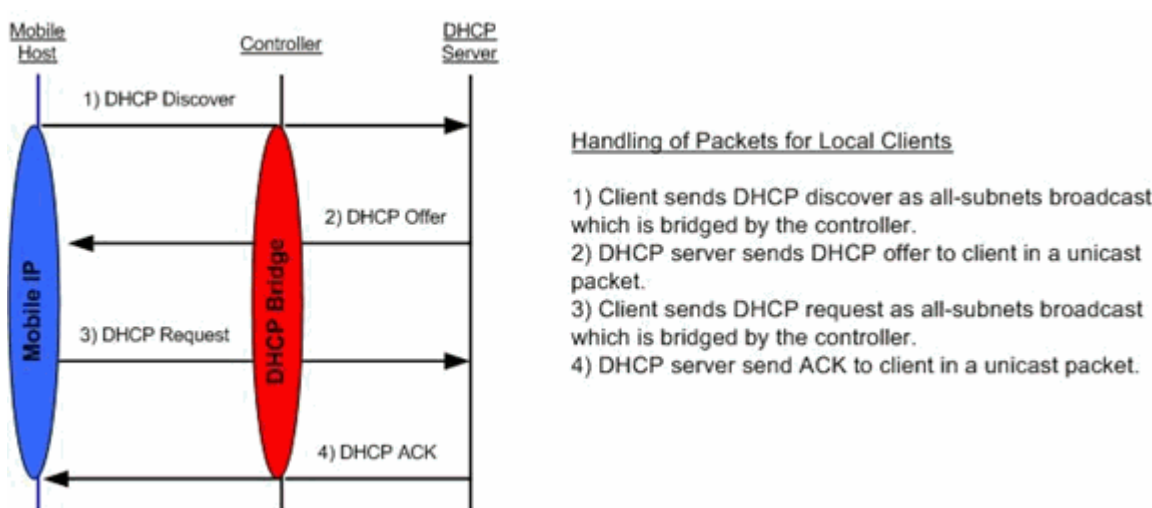
Hinweise

- Interoperabilitätsprobleme können zwischen einem Controller mit aktiviertem DHCP-Proxy und Geräten auftreten, die sowohl als Firewall als auch als DHCP-Server fungieren. Dies ist höchstwahrscheinlich auf die Firewall-Komponente des Geräts zurückzuführen, da Firewalls im Allgemeinen nicht auf Proxy-Anfragen reagieren. Die Problemumgehung für dieses Problem besteht darin, den DHCP-Proxy auf dem Controller zu deaktivieren.
- Wenn sich ein Client im DHCP REQ-Status des Controllers befindet, verwirft der Controller die DHCP-Inform-Pakete. Der Client wechselt erst dann in den Status "RUN" auf dem Controller (dies ist erforderlich, damit der Client Datenverkehr weiterleiten kann), wenn er ein DHCP-Ermittlungspaket vom Client empfängt. DHCP Inform-Pakete werden vom Controller weitergeleitet, wenn der DHCP-Proxy deaktiviert ist.
- Alle Controller, die miteinander kommunizieren, müssen über dieselbe DHCP-Proxyeinstellung verfügen.

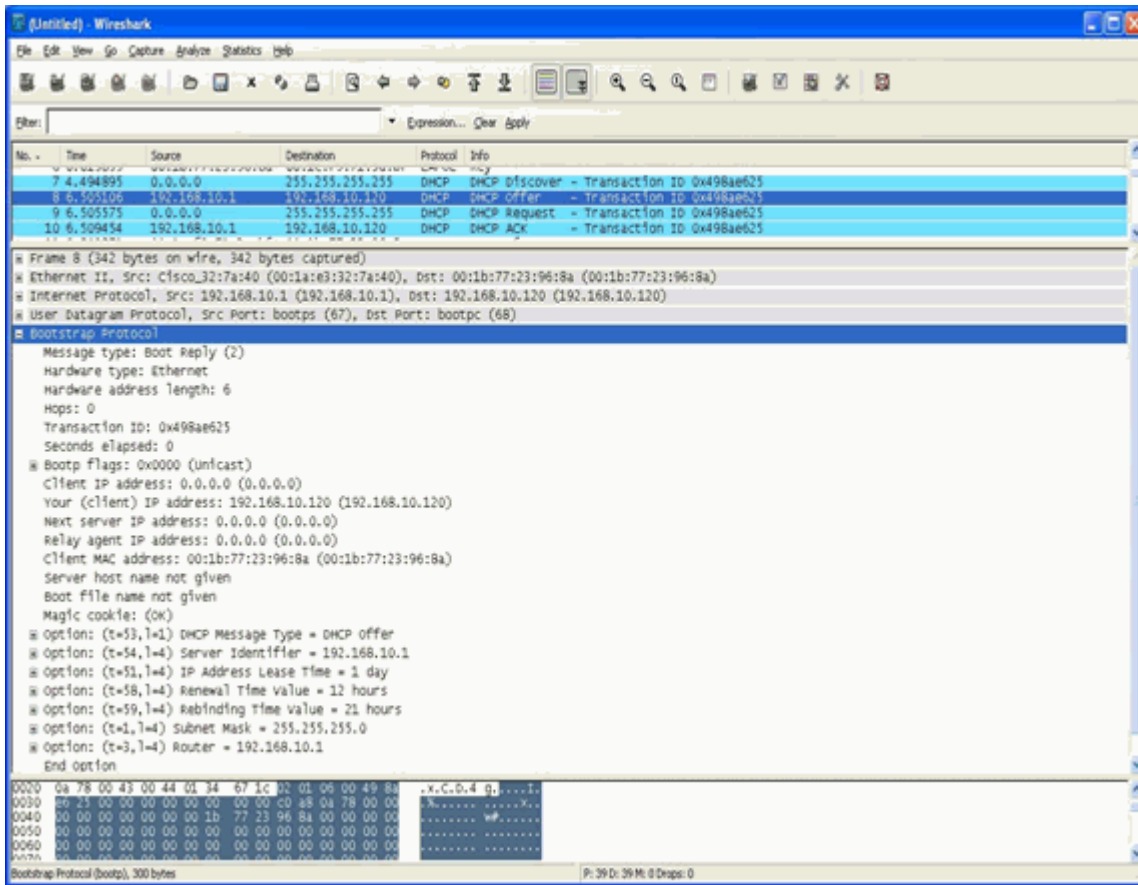
DHCP-Bridge-Modus

Die DHCP-Bridging-Funktion wurde entwickelt, um die Controller-Rolle in der DHCP-Transaktion für den Client vollständig transparent zu machen. Mit Ausnahme der Umwandlung von 802.11 in Ethernet II werden Pakete vom Client unverändert vom LWAPP-Tunnel (Light Weight Access Point Protocol) zum Client-VLAN (oder im L3-Roaming-Fall zum EoIP-Tunnel (Ethernet over IP)) überbrückt. Mit Ausnahme der Umwandlung von Ethernet II in 802.11 werden Pakete an den Client unverändert vom Client-VLAN (oder im L3-Roaming-Fall vom EoIP-Tunnel) zum LWAPP-Tunnel überbrückt. Stellen Sie sich vor, Sie verkabeln einen Client mit einem Switch-Port und dann führt der Client eine herkömmliche DHCP-Transaktion durch.

DHCP-Bridging-Vorgänge - Bridging-Paketfluss

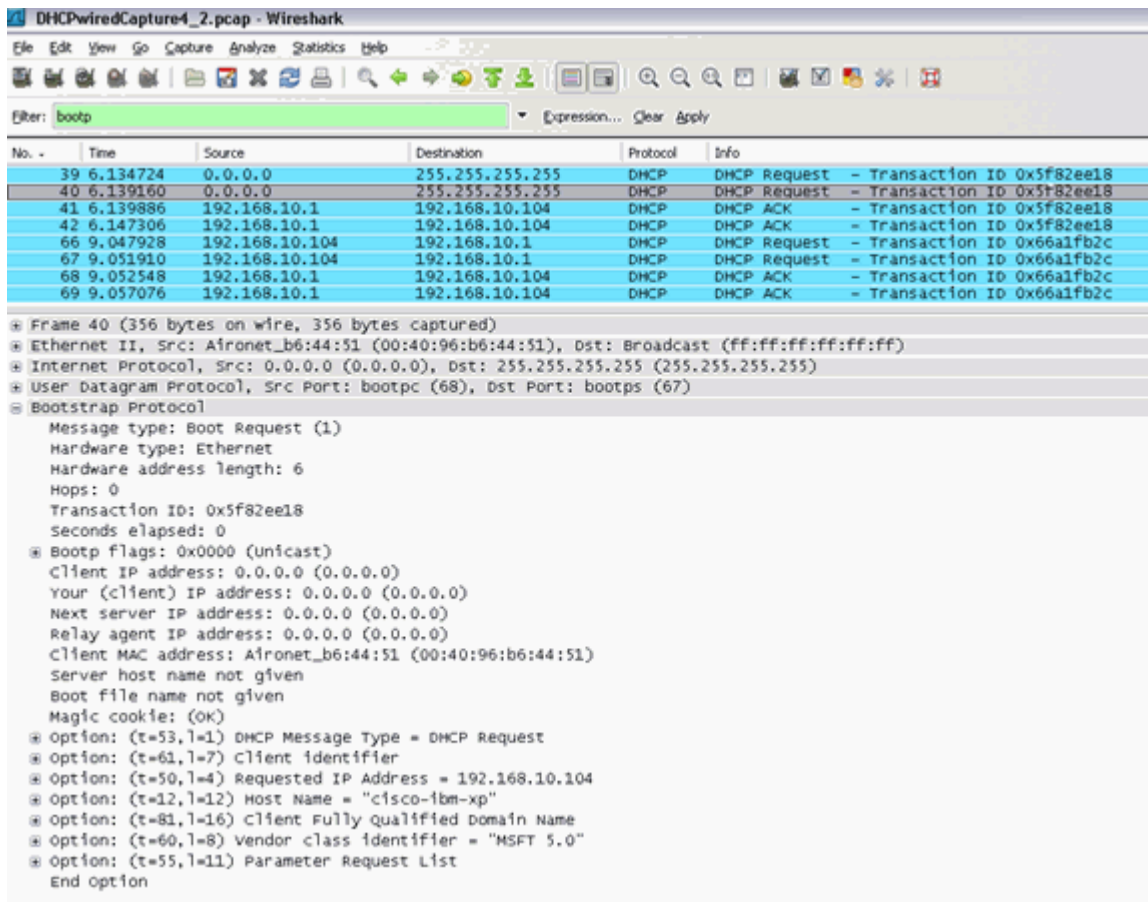


Bridging-Paketerfassung - Client-Perspektive



Im clientseitigen Paketerfassungs-Screenshot besteht der Hauptunterschied zwischen der Client-Erfassung im Proxy-Modus darin, dass die tatsächliche IP-Adresse des DHCP-Servers in den Paketen Offer und Ack angezeigt wird, und nicht in der virtuellen IP-Adresse des Controllers.

Bridging-Paketerfassung - Server-Perspektive



Im Wired Packet Capture-Screenshot können Sie sehen, dass Paket 40 die überbrückte DHCP-Anfrage ist, die vom Test-Client 00:40:96:b6:44:51 an das Wired-Netzwerk gesendet wird.

Beispiel einer Bridge-Konfiguration

Um die DHCP-Bridging-Funktion auf dem Controller zu aktivieren, müssen Sie die DHCP-Proxy-Funktion auf dem Controller deaktivieren. Dies kann in der CLI nur mit den folgenden Befehlen erreicht werden:

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy disable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behaviour: disabled
```

Wenn der DHCP-Server nicht im selben Layer-2-Netzwerk (L2) wie der Client vorhanden ist, muss der Broadcast mithilfe eines IP-Helpers an den DHCP-Server am Client-Gateway weitergeleitet werden. Dies ist ein Beispiel für diese Konfiguration:

```
<#root>
```

```
Switch#
```

```
conf t
```

```
Switch(config)#
```

```
interface vlan
```

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

```
ip helper-address
```

Bei der DHCP-Bridging-Funktion handelt es sich um eine globale Einstellung, die alle DHCP-Transaktionen innerhalb des Controllers beeinflusst. Sie müssen der kabelgebundenen Infrastruktur IP-Helper-Statements für alle erforderlichen VLANs auf dem Controller hinzufügen.

Fehlerbehebung

Die hier aufgeführten Debugging-Funktionen wurden in der CLI des Controllers aktiviert, und der DHCP-Teil der Ausgabe wurde für dieses Dokument extrahiert.

```
<#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
```

In dieser DHCP-Debug-Ausgabe gibt es einige Schlüsselhinweise dafür, dass DHCP-Bridging auf dem Controller verwendet wird:

DHCP erfolgreich Bridge-Paket an DS - Dies bedeutet, dass das ursprüngliche DHCP-Paket vom Client überbrückt wurde, unverändert am Distribution System (DS). Der DS ist die kabelgebundene Infrastruktur.

DHCP erfolgreich Bridge-Paket an STA - Diese Nachricht gibt an, dass das DHCP-Paket an die Station (STA) überbrückt wurde, unverändert. Der STA ist der Client-Computer, der DHCP anfordert.

Außerdem wird die tatsächliche Server-IP-Adresse in den Debugs aufgeführt, nämlich 192.168.10.1. Wenn der DHCP-Proxy anstelle des DHCP-Bridging-Diensts verwendet wurde, würde die virtuelle IP-Adresse des Controllers als IP-Adresse des Servers aufgeführt.

Hinweise

- Der DHCP-Proxy ist standardmäßig aktiviert.
- Alle Controller, die miteinander kommunizieren, müssen über dieselbe DHCP-Proxyeinstellung verfügen.
- Der DHCP-Proxy muss aktiviert sein, damit die DHCP-Option 82 funktioniert.

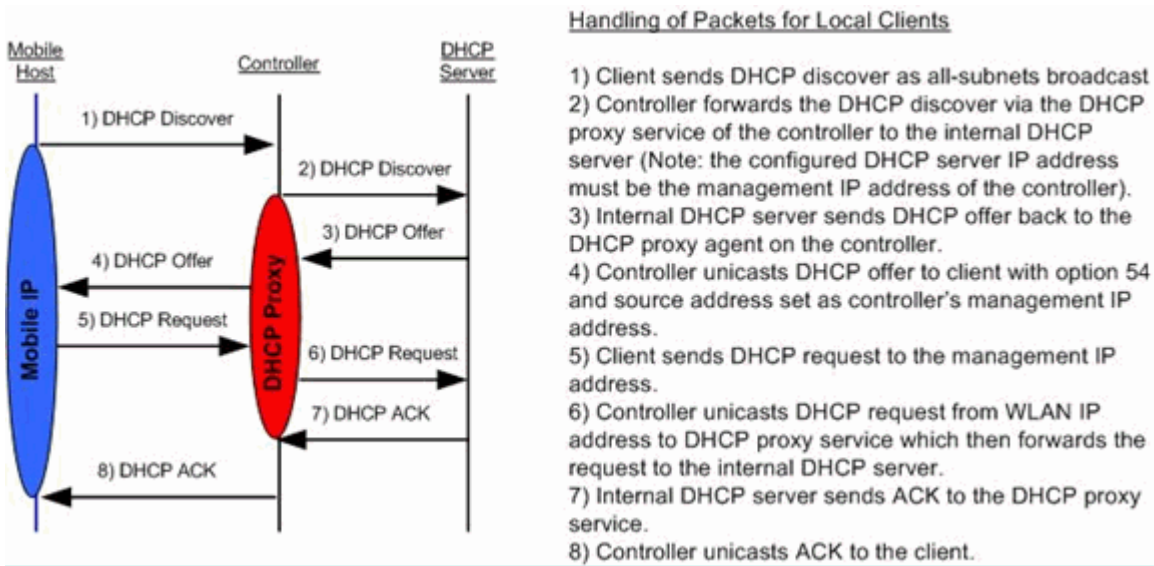
Interner DHCP-Server

Der interne DHCP-Server wurde ursprünglich für Zweigstellen eingeführt, in denen kein externer DHCP-Server verfügbar ist. Es unterstützt ein kleines Wireless-Netzwerk mit weniger als zehn Access Points (APs), die sich im gleichen Subnetz befinden. Der interne Server stellt Wireless-Clients IP-Adressen, Direktverbindungs-APs, Appliance-Mode-APs an der Management-Schnittstelle und DHCP-Anfragen bereit, die von APs weitergeleitet werden. Es handelt sich nicht um einen ausgereiften DHCP-Server für allgemeine Dienste. Sie unterstützt nur einen eingeschränkten Funktionsumfang und lässt sich nicht in einer größeren Bereitstellung skalieren.

Vergleich von internem DHCP und Bridging-Modus

Die beiden DHCP-Hauptmodi auf dem Controller sind entweder DHCP-Proxy oder DHCP-Bridging. Beim DHCP-Bridging agiert der Controller wie ein DHCP-Back mit autonomen APs. Ein DHCP-Paket gelangt über eine Client-Zuordnung zu einem mit einem VLAN verbundenen Service Set Identifier (SSID) in den AP. Anschließend wird das DHCP-Paket über das VLAN übertragen. Wenn auf dem Layer-3 (L3)-Gateway dieses VLAN ein IP-Helper definiert ist, wird das Paket über gerichtetes Unicast an diesen DHCP-Server weitergeleitet. Der DHCP-Server antwortet dann direkt auf die L3-Schnittstelle, die das DHCP-Paket weitergeleitet hat. Beim DHCP-Proxy ist dies der gleiche Ansatz, aber die gesamte Weiterleitung erfolgt direkt am Controller und nicht an der L3-Schnittstelle des VLAN. Wenn beispielsweise eine DHCP-Anfrage vom Client in das WLAN eingeht, verwendet das WLAN entweder den DHCP-Server, der auf der VLAN-Schnittstelle definiert ist, *oder* verwendet die DHCP-Überschreibungsfunktion des WLAN, um ein Unicast-DHCP-Paket an den DHCP-Server weiterzuleiten, wobei das Feld DHCP Packets GIADDR als IP-Adresse der VLAN-Schnittstelle ausgefüllt ist.

Interner DHCP-Server - Paketfluss

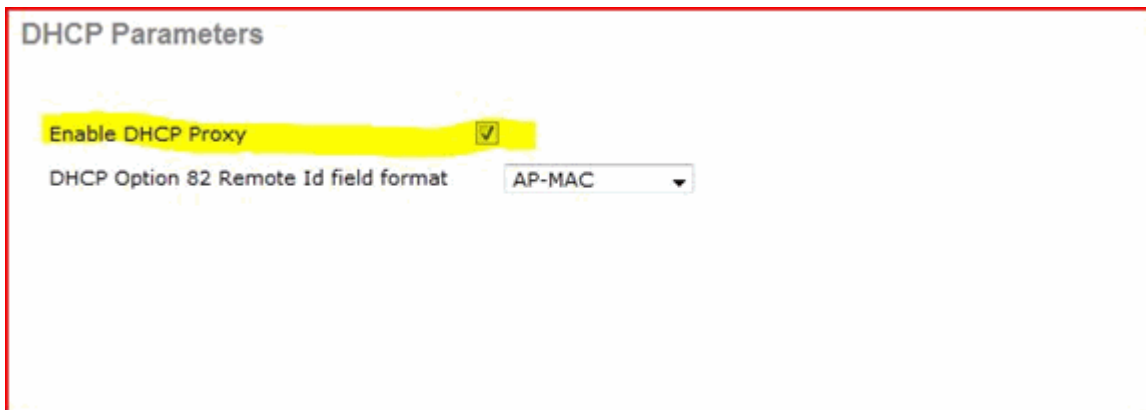


Konfigurationsbeispiel für internen DHCP-Server

Sie müssen den DHCP-Proxy auf dem Controller aktivieren, damit der interne DHCP-Server funktioniert. Dies kann über die grafische Benutzeroberfläche in diesem Abschnitt durchgeführt werden:

Hinweis: Sie können den DHCP-Proxy nicht in allen Versionen über die grafische Benutzeroberfläche einrichten.

Controller->Advanced->DHCP



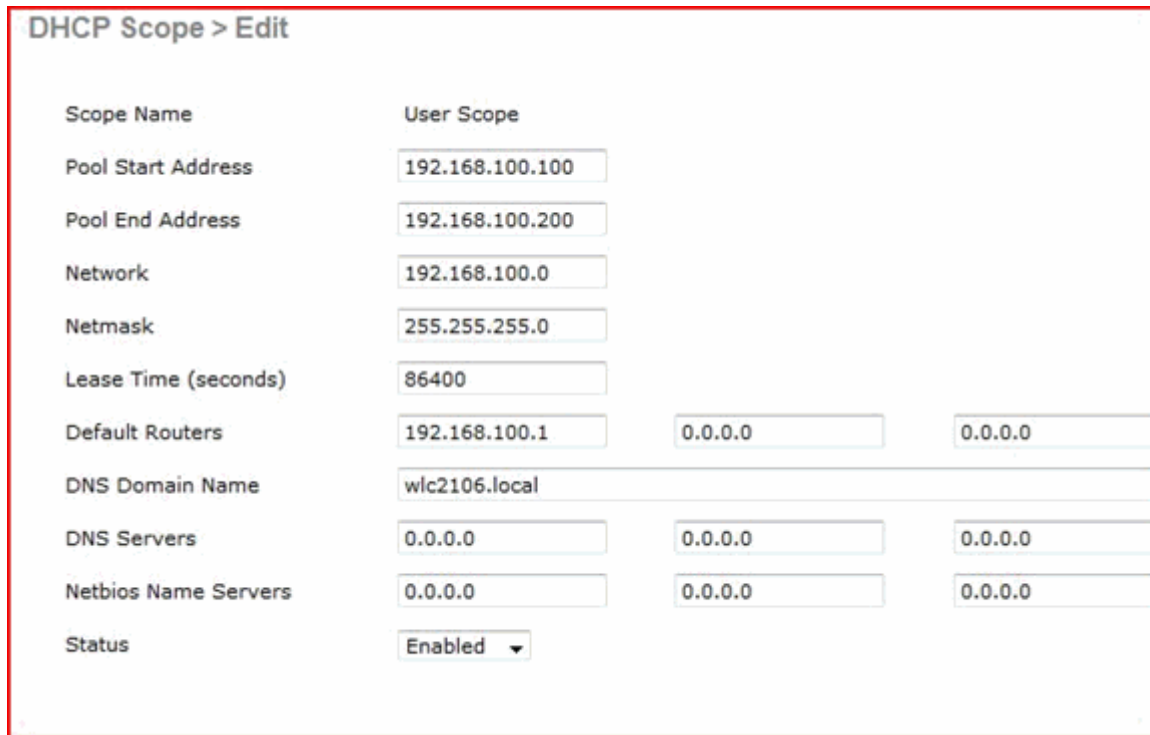
oder über die Kommandozeile:

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

Führen Sie die folgenden Schritte aus, um den internen DHCP-Server zu aktivieren:

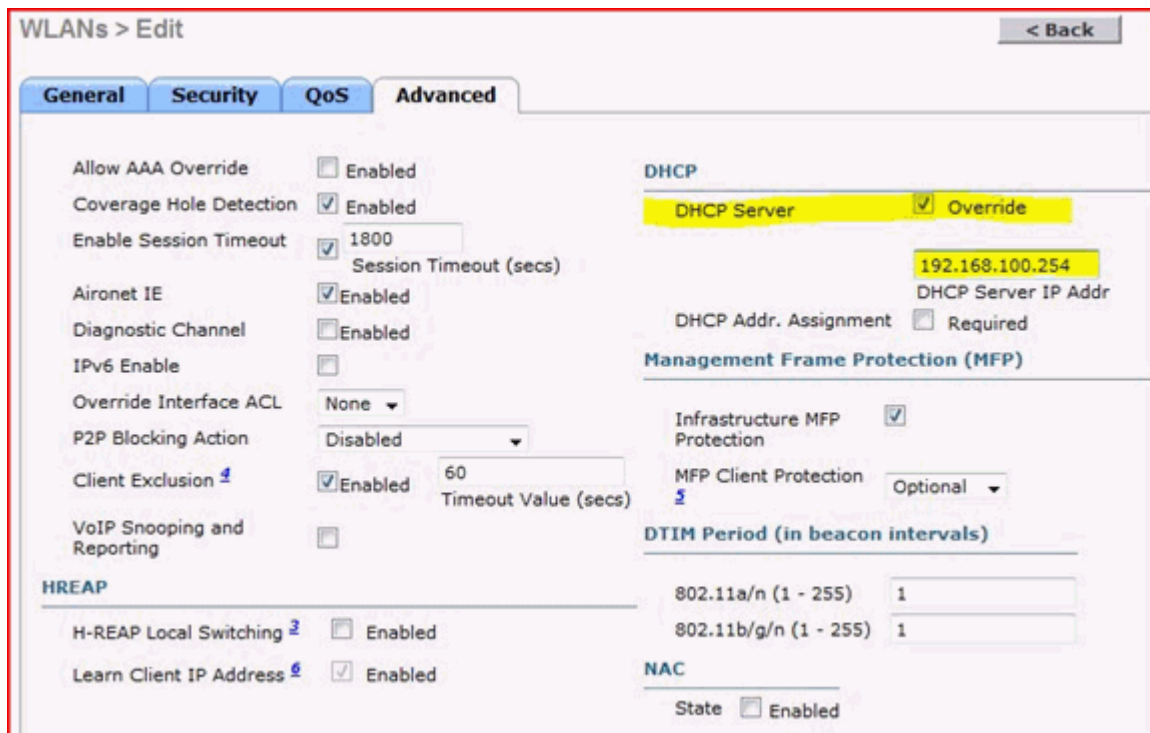
1. Definieren Sie einen Bereich, den Sie zum Abrufen von IP-Adressen verwenden (Controller > Internal

DHCP Server > DHCP Scope). Klicken Sie auf **Neu**.



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

2. Zeigen Sie entweder die DHCP-Überschreibung auf die IP-Adresse der Verwaltungsschnittstelle Ihres Controllers.



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

Alternativ können Sie die DHCP-Option der Controller-Schnittstellenkonfiguration für die Schnittstelle verwenden, die Sie für den internen DHCP-Server verwenden möchten.

Interfaces > Edit

General Information

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

Configuration

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

Interface Address

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

Physical Information

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

DHCP Information

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

3. Stellen Sie sicher, dass der DHCP-Proxy aktiviert ist.

DHCP Parameters

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

Fehlerbehebung

Bei einem Debugging des internen DHCP-Servers muss in der Regel ein Client gefunden werden, der Probleme beim Abrufen einer IP-Adresse hat. Sie müssen diese Debugs ausführen.

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


Der Debug-Client ist ein Makro, das diese Debug-Vorgänge für Sie aktiviert, während er das Debuggen nur auf die eingegebene Client-MAC-Adresse fokussiert.

```
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
```

Die wichtigste Ursache für DHCP-Probleme ist `debug dhcp packet enable` Befehl, der automatisch vom `debug client` aus.

```
<#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
```

Löschen Sie die DHCP-Leases auf dem internen DHCP-Server des WLC.

Mit diesem Befehl können Sie die DHCP-Leases auf dem internen DHCP-Server des WLC löschen:

```
<#root>

config dhcp clear-lease
```

Hier ein Beispiel:

```
<#root>

config dhcp clear-lease all
```

Hinweise

- Der DHCP-Proxy muss aktiviert sein, damit der interne DHCP-Server funktioniert.
- Verwendung von DHCP für den Port 1067, wenn Sie den internen DHCP-Server verwenden, der von der CPU-ACL betroffen ist.
- Der interne DHCP-Server hört die Loopback-Schnittstelle des Controllers über den UDP-Port 67 (127.0.0.1) ab.

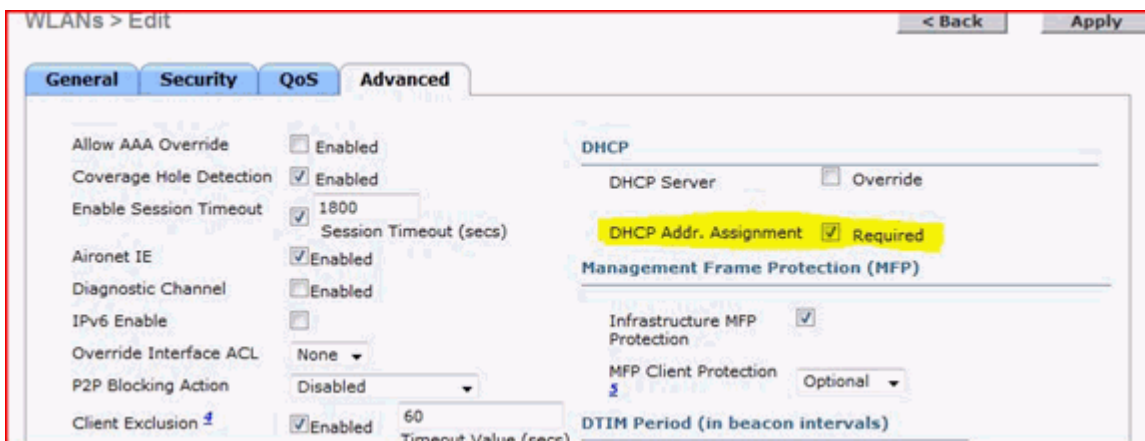
Endbenutzeroberfläche

- Die Fehlermeldung `config dhcp proxy disable` impliziert die Verwendung der DHCP-Bridging-Funktion. Hierbei handelt es sich um einen globalen Befehl (und nicht um einen Befehl pro WLAN).
- Der DHCP-Proxy bleibt standardmäßig aktiviert.

- Wenn der DHCP-Proxy deaktiviert ist, kann der interne DHCP-Server nicht von lokalen WLANs verwendet werden. Der Bridging-Vorgang stimmt nicht mit den Vorgängen überein, die zum Umleiten eines Pakets an den internen Server erforderlich sind. Bridging bedeutet in der Tat Bridging, mit Ausnahme der Umwandlung von 802.11 in Ethernet II. DHCP-Pakete werden unverändert vom LWAPP-Tunnel an das Client-VLAN weitergeleitet (und umgekehrt).
- Wenn der Proxy aktiviert ist, muss ein DHCP-Server an der Schnittstelle des WLAN (oder im WLAN selbst) konfiguriert werden, damit das WLAN aktiviert werden kann. Wenn der Proxy deaktiviert ist, muss kein Server konfiguriert werden, da diese Server nicht verwendet werden.
- Wenn ein Benutzer versucht, den DHCP-Proxy zu aktivieren, überprüfen Sie intern, ob für alle WLANs (oder die zugehörigen Schnittstellen) ein DHCP-Server konfiguriert ist. Andernfalls schlägt der Aktivierungsvorgang fehl.

DHCP erforderlich

Die erweiterte WLAN-Konfiguration verfügt über eine Option, bei der Benutzer DHCP weiterleiten müssen, bevor sie in den RUN-Status wechseln (einen Status, bei dem der Client Datenverkehr über den Controller weiterleiten kann). Für diese Option muss der Client eine vollständige oder eine halbe DHCP-Anfrage durchführen. Der Controller sucht vom Client hauptsächlich nach einer DHCP-Anfrage und einer ACK, die vom DHCP-Server zurückgesendet werden. Solange der Client diese Schritte ausführt, leitet der Client den erforderlichen DHCP-Schritt weiter und wechselt in den Status "RUN".



L2- und L3-Roaming

L2-Roam - Wenn der Client über eine gültige DHCP-Lease verfügt und ein L2-Roaming zwischen zwei verschiedenen Controllern im gleichen L2-Netzwerk durchführt, muss der Client kein erneutes DHCP durchführen, und der Client-Eintrag muss vollständig vom ursprünglichen Controller auf den neuen Controller verschoben werden. Wenn der Client dann erneut DHCP ausführen muss, überbrückt der DHCP-Bridging- oder Proxy-Prozess auf dem aktuellen Controller das Paket auf transparente Weise erneut.

L3-Roam - In einem L3-Roam-Szenario bewegt sich der Client zwischen zwei verschiedenen Controllern in verschiedenen L3-Netzwerken. In diesem Fall wird der Client am ursprünglichen Controller verankert und in der Client-Tabelle auf dem neuen ausländischen Controller aufgeführt. Während des Ankerszenarios wird der Client-DHCP-Server vom Anker-Controller verwaltet, da die Client-Daten in einem EoIP-Tunnel zwischen dem Fremd- und dem Anker-Controller getunnelt werden.

Zugehörige Informationen

- [Konfigurationsbeispiel zu DHCP-Option 43 für Cisco Aironet Lightweight Access Points](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.