

# Informazioni sulla gestione del protocollo DHCP da parte dei WLC di AireOS

## Sommario

---

[Introduzione](#)

[Server DHCP esterno](#)

[Confronto tra modalità proxy e bridging DHCP](#)

[Modalità proxy DHCP](#)

[Flusso di pacchetti proxy](#)

[Acquisizione di pacchetti proxy](#)

[Prospettiva client](#)

[Prospettiva server](#)

[Esempio di configurazione del proxy](#)

[Risoluzione dei problemi](#)

[Avvertenze](#)

[Modalità bridging DHCP](#)

[Funzionamento bridging DHCP - Flusso di pacchetti bridging](#)

[Acquisizione di pacchetti bridging - Prospettiva client](#)

[Acquisizione di pacchetti bridging - Prospettiva server](#)

[Esempio di configurazione bridging](#)

[Risoluzione dei problemi](#)

[Avvertenze](#)

[Server DHCP interno](#)

[Confronto tra modalità DHCP e bridging interno](#)

[Server DHCP interno - Flusso di pacchetti](#)

[Esempio di configurazione del server DHCP interno](#)

[Risoluzione dei problemi](#)

[Cancella i lease DHCP sul server DHCP interno del WLC](#)

[Avvertenze](#)

[Interfaccia utente finale](#)

[DHCP richiesto](#)

[Roaming L2 e L3](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento vengono descritte le diverse operazioni DHCP sul controller wireless Cisco AireOS.

## Server DHCP esterno

Quando viene utilizzato un server DHCP esterno, il WLC (Wireless LAN Controller) supporta due modalità di funzionamento DHCP:

- Modalità proxy DHCP
- Modalità bridging DHCP

La modalità proxy DHCP funge da funzione di supporto DHCP per migliorare la sicurezza e il controllo delle transazioni DHCP tra il server DHCP e i client wireless. La modalità di bridging DHCP consente di rendere il ruolo di controller in una transazione DHCP completamente trasparente per i client wireless.

### Confronto tra modalità proxy e bridging DHCP

Gestione client DHCP	Modalità proxy DHCP	Modalità bridging DHCP
Modificare giaddr	Sì	No
Modificare siaddr	Sì	No
Modificare il contenuto dei pacchetti	Sì	No
Offerte ridondanti non inoltrate	Sì	No
Supporto dell'opzione 82	Sì	No
Conversione da broadcast a unicast	Sì	No
Supporto BOOTP	No	Server
Non conformità RFC	Gli agenti proxy e relay non hanno esattamente lo stesso concetto. Per la piena conformità RFC, si raccomanda la modalità bridging DHCP.	No

### Modalità proxy DHCP


Il proxy DHCP non è ideale per tutti gli ambienti di rete. Il controller modifica e inoltra tutte le transazioni DHCP per fornire una funzione di supporto e risolvere alcuni problemi di sicurezza.

L'indirizzo IP virtuale del controller viene in genere utilizzato come indirizzo IP di origine di tutte le transazioni DHCP per il client. Di conseguenza, il vero indirizzo IP del server DHCP non è visibile. Questo IP virtuale viene visualizzato nell'output di debug per le transazioni DHCP sul controller. Tuttavia, l'utilizzo di un indirizzo IP virtuale può causare problemi per alcuni tipi di client.

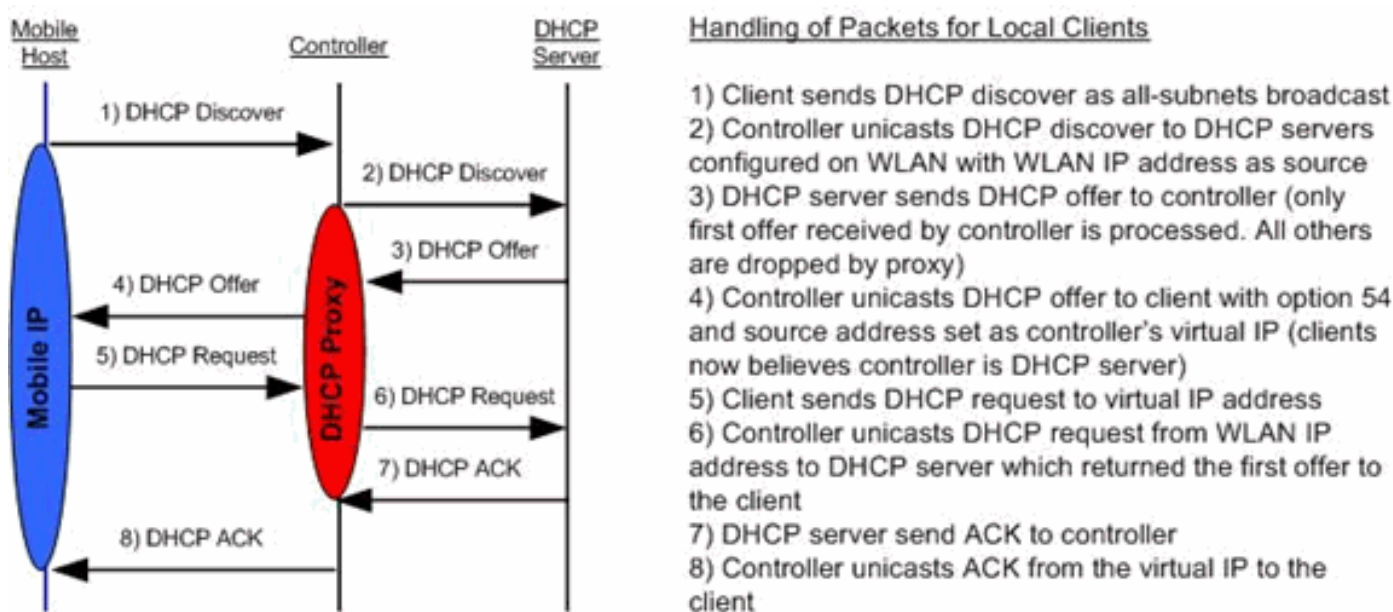
L'operazione in modalità proxy DHCP mantiene lo stesso comportamento sia per i protocolli di mobilità simmetrica che asimmetrica.

Quando più offerte provengono da server DHCP esterni, il proxy DHCP normalmente seleziona la prima in ordine di arrivo e imposta l'indirizzo IP del server nella struttura dati del client. Di conseguenza, tutte le transazioni successive vengono eseguite attraverso lo stesso server DHCP fino a quando una transazione non riesce dopo i nuovi tentativi. A questo punto, il proxy seleziona un altro server DHCP per il client.

Il proxy DHCP è abilitato per impostazione predefinita. Tutti i controller che comunicano devono avere la stessa impostazione del proxy DHCP.

 Nota: per il corretto funzionamento dell'opzione DHCP 82, il proxy DHCP deve essere abilitato.

## Flusso di pacchetti proxy

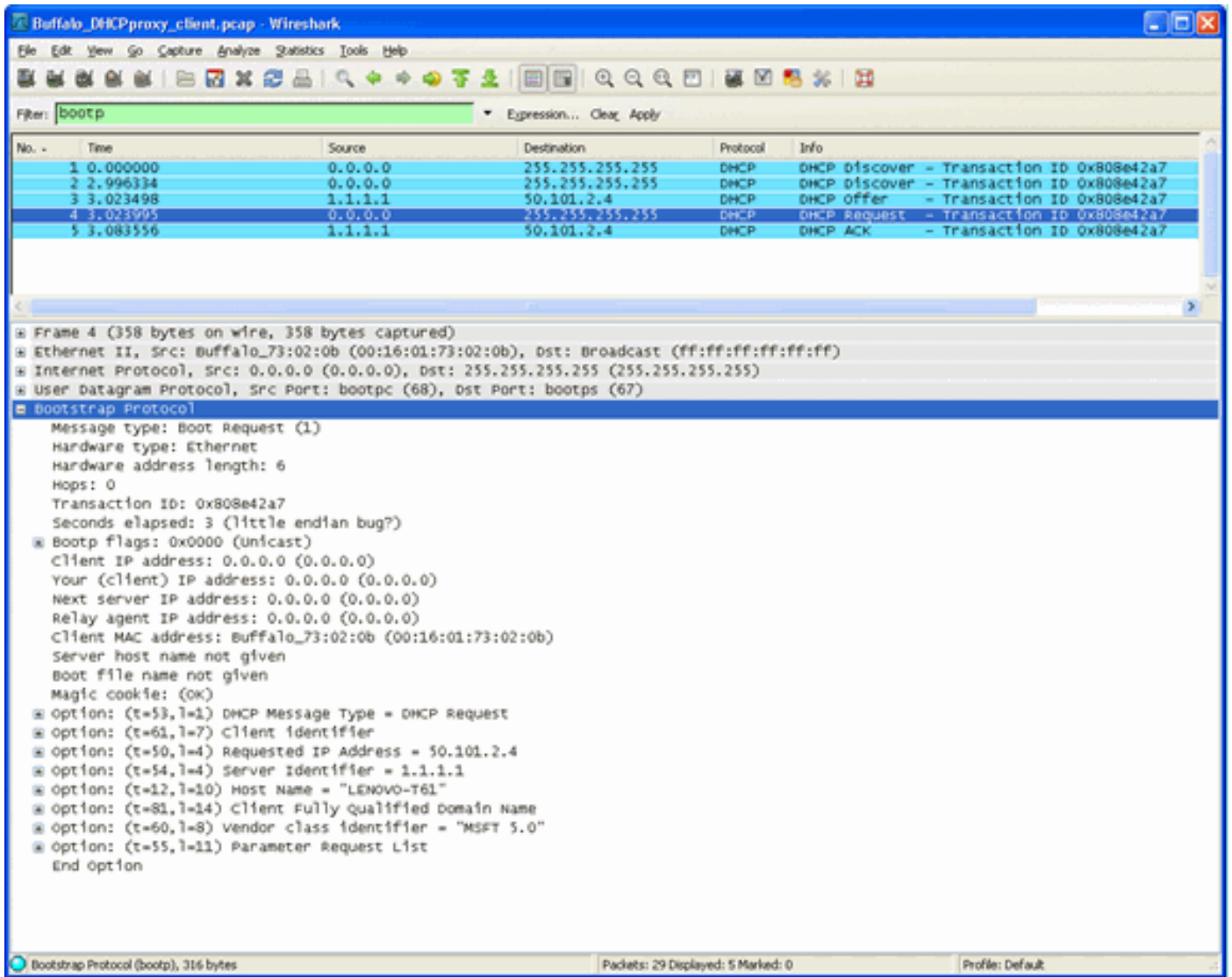


## Acquisizione di pacchetti proxy

Quando il controller è in modalità proxy DHCP, non solo indirizza i pacchetti DHCP al server DHCP, ma in realtà crea nuovi pacchetti DHCP da inoltrare al server DHCP. Tutte le opzioni DHCP presenti nei pacchetti DHCP client vengono copiate nei pacchetti DHCP del controller. Gli esempi seguenti mostrano questa condizione per un pacchetto richiesta DHCP.

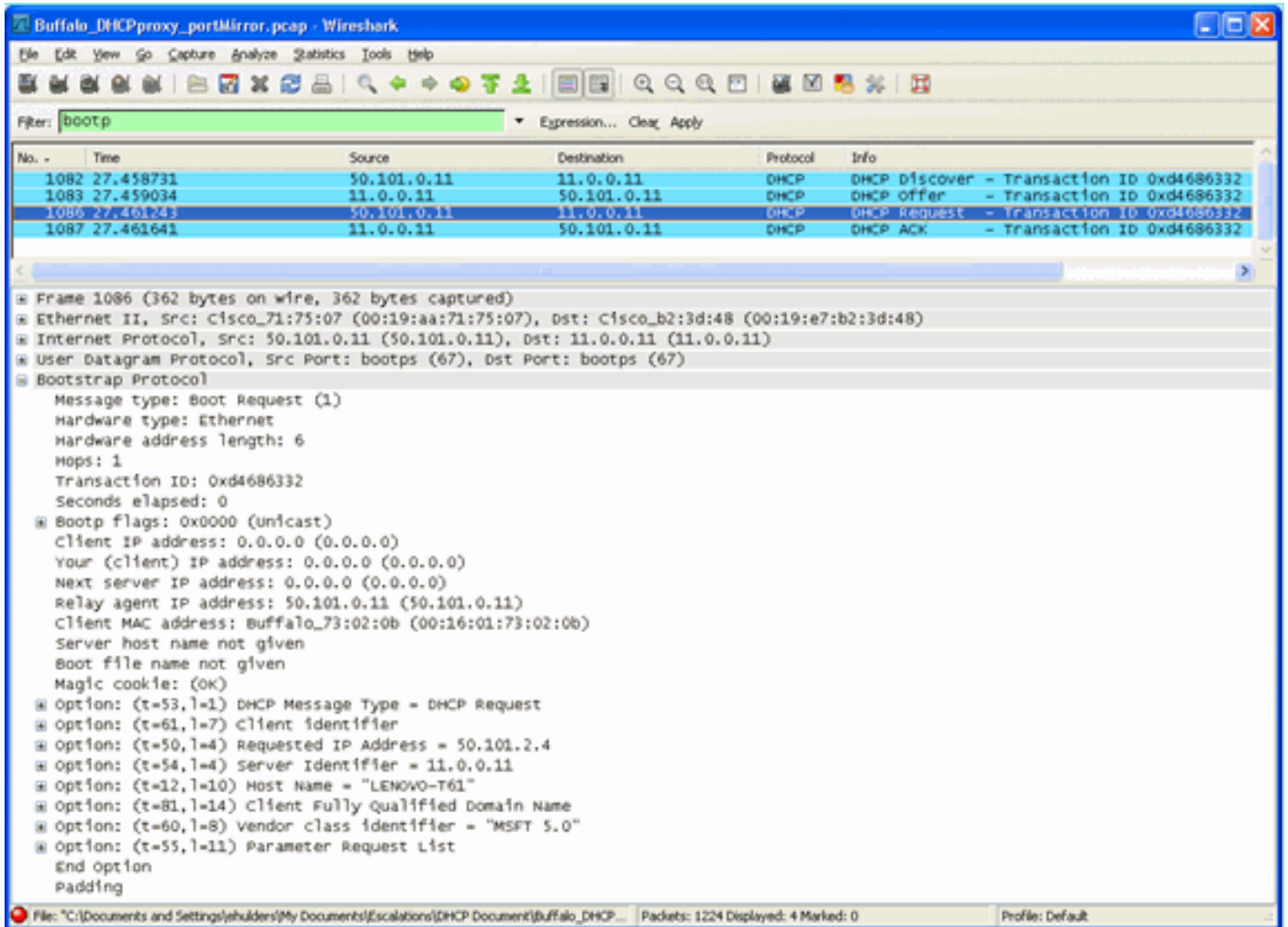
### Prospettiva client

In questa schermata viene mostrata un'acquisizione dei pacchetti dal punto di vista del client. Mostra un rilevamento DHCP, un'offerta DHCP, una richiesta DHCP e un ACK DHCP. La richiesta DHCP viene evidenziata e i dettagli del boot p protocollo vengono espansi, per visualizzare le opzioni DHCP.



### Prospettiva server

In questa schermata viene mostrata un'acquisizione dei pacchetti dal punto di vista del server. Analogamente all'esempio precedente, mostra un rilevamento DHCP, un'offerta DHCP, una richiesta DHCP e un ACK DHCP. Si tratta tuttavia di pacchetti generati dal controller in funzione del proxy DHCP. La richiesta DHCP viene evidenziata e i dettagli del bootp protocollo vengono espansi, per visualizzare le opzioni DHCP. Si noti che sono gli stessi del pacchetto di richiesta DHCP del client. Inoltre, il proxy WLC inoltra il pacchetto ed evidenzia gli indirizzi del pacchetto.



Esempio di configurazione del proxy

Per utilizzare il controller come proxy DHCP, è necessario abilitare la funzione proxy DHCP sul controller. Per impostazione predefinita, questa funzionalità è abilitata. Per abilitare il proxy DHCP, è possibile usare questo comando CLI. Lo stesso comando è disponibile nella GUI della pagina Controller nel menu DHCP.

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy enable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behavior: enabled
```

Affinché il proxy DHCP funzioni, è necessario configurare un server DHCP primario in ogni interfaccia del controller che richiede servizi DHCP. Un server DHCP può essere configurato sull'interfaccia di gestione, sull'interfaccia ap-manager e sulle interfacce dinamiche. Per configurare un server DHCP su ciascuna interfaccia, è possibile utilizzare questi comandi CLI.

```
<#root>
```

```
(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>
```

La funzione di bridging DHCP è un'impostazione globale, quindi influisce su tutte le transazioni DHCP all'interno del controller.

Risoluzione dei problemi

Questo è l'output del **debug dhcp packet enable** comando. Il debug mostra un controller che riceve una richiesta DHCP da un client con indirizzo MAC 00:40:96:b4:8c:e1, trasmette una richiesta DHCP al server DHCP, riceve una risposta dal server DHCP e invia un'offerta DHCP al client.

```
<#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
```

```
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
```

```
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
```

```
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 - cont
```

```
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  
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 mob
```

```
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 21:48:5

## Avvertenze

- 

Tra un controller con proxy DHCP abilitato e dispositivi che fungono sia da firewall che da server DHCP, possono verificarsi problemi di interoperabilità. Ciò è probabilmente dovuto al componente firewall del dispositivo, in quanto i firewall generalmente non rispondono alle richieste proxy. Per risolvere il problema, disabilitare il proxy DHCP sul controller.

- 

Quando un client si trova nello stato DHCP REQ sul controller, il controller scarta i pacchetti DHCP INFORM. Il client non passa in stato RUN sul controller (necessario per il passaggio del traffico da parte del client) fino a quando non riceve un pacchetto di individuazione DHCP dal client. I pacchetti informativi DHCP vengono inoltrati dal controller quando il proxy DHCP è disabilitato.

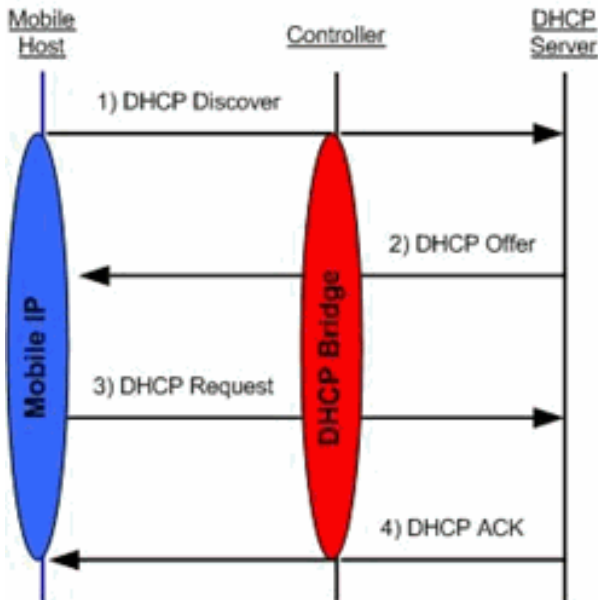
- 

Tutti i controller che comunicano tra loro devono avere la stessa impostazione del proxy DHCP.

## Modalità bridging DHCP

La funzionalità di bridging DHCP è progettata per rendere il ruolo di controller nella transazione DHCP completamente trasparente per il client. Ad eccezione della conversione da 802.11 a Ethernet II, i pacchetti del client vengono sottoposti a bridging senza modifiche dal tunnel LWAPP (Light Weight Access Point Protocol) al tunnel VLAN client (o Ethernet over IP (EoIP) nel caso di roaming L3. Analogamente, ad eccezione delle conversioni da Ethernet II a 802.11, i pacchetti al client vengono collegati senza modifiche dalla VLAN client (o dal tunnel EoIP nel caso di roaming L3) al tunnel LWAPP. Si pensi a questo come al cablaggio di un client in una switchport e quindi considerando che il client esegue una transazione DHCP tradizionale.

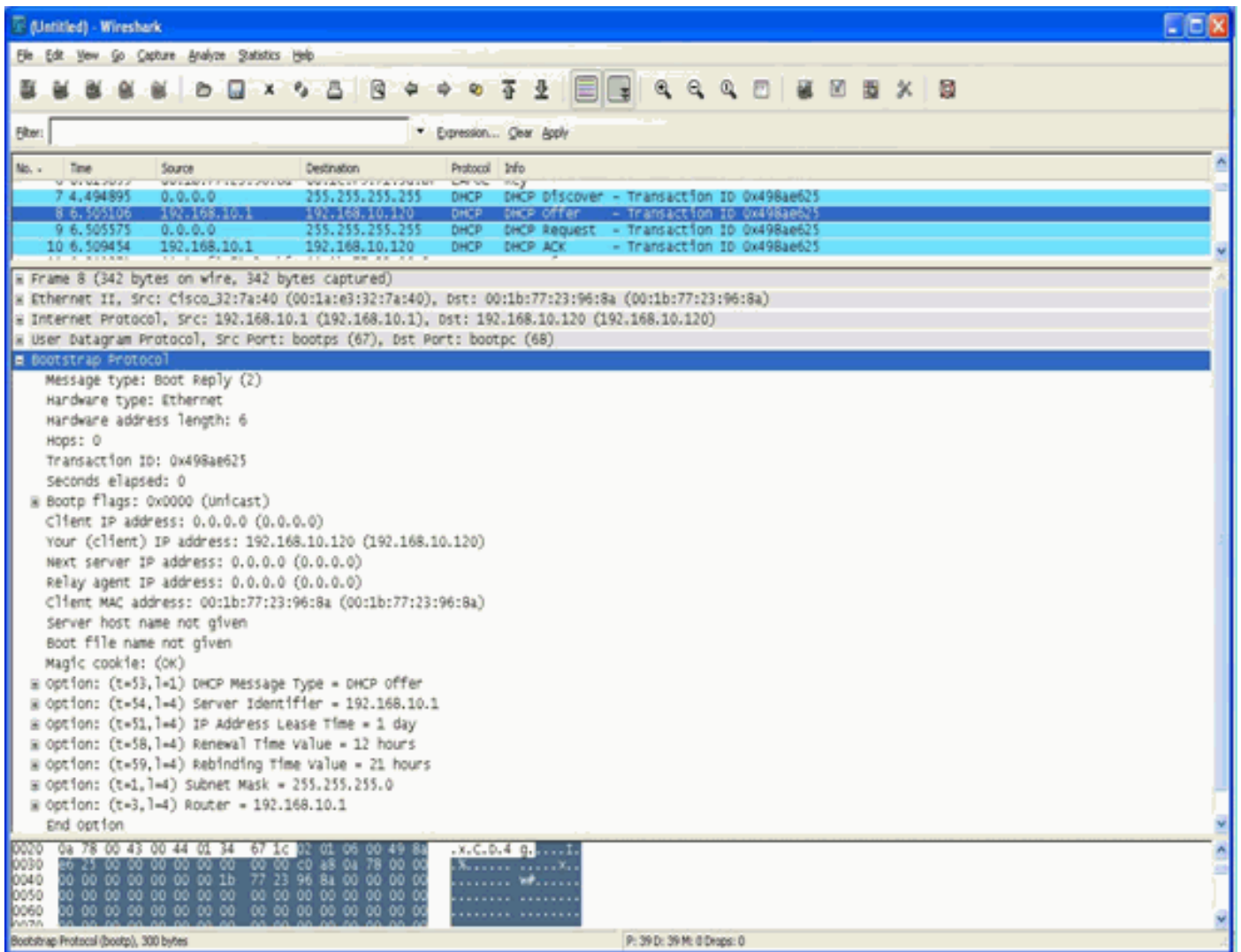
## Funzionamento bridging DHCP - Flusso di pacchetti bridging



### Handling of Packets for Local Clients

- 1) Client sends DHCP discover as all-subnets broadcast which is bridged by the controller.
- 2) DHCP server sends DHCP offer to client in a unicast packet.
- 3) Client sends DHCP request as all-subnets broadcast which is bridged by the controller.
- 4) DHCP server send ACK to client in a unicast packet.

Acquisizione di pacchetti bridging - Prospettiva client



Nella schermata di acquisizione dei pacchetti sul lato client, la differenza principale tra l'acquisizione del client in modalità proxy è l'IP reale del server DHCP visualizzato nei pacchetti Offerta e Ack invece dell'indirizzo IP virtuale del controller.



## Acquisizione di pacchetti bridging - Prospettiva server

DHCPwiredCapture4\_2.pcap - Wireshark

Filter: bootp

No.	Time	Source	Destination	Protocol	Info
39	6.134724	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x5f82ee18
40	6.139160	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x5f82ee18
41	6.139886	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x5f82ee18
42	6.147306	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x5f82ee18
66	9.047928	192.168.10.104	192.168.10.1	DHCP	DHCP Request - Transaction ID 0x66a1fb2c
67	9.051910	192.168.10.104	192.168.10.1	DHCP	DHCP Request - Transaction ID 0x66a1fb2c
68	9.052548	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x66a1fb2c
69	9.057076	192.168.10.1	192.168.10.104	DHCP	DHCP ACK - Transaction ID 0x66a1fb2c

Frame 40 (356 bytes on wire, 356 bytes captured)

Ethernet II, Src: Aironet\_b6:44:51 (00:40:96:b6:44:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)

User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)

Bootstrap Protocol

- Message type: Boot Request (1)
- Hardware type: Ethernet
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0x5f82ee18
- Seconds elapsed: 0
- Bootp flags: 0x0000 (unicast)
- Client IP address: 0.0.0.0 (0.0.0.0)
- Your (client) IP address: 0.0.0.0 (0.0.0.0)
- Next server IP address: 0.0.0.0 (0.0.0.0)
- Relay agent IP address: 0.0.0.0 (0.0.0.0)
- Client MAC address: Aironet\_b6:44:51 (00:40:96:b6:44:51)
- Server host name not given
- Boot file name not given
- Magic cookie: (OK)
- Option: (t=53,l=1) DHCP Message Type = DHCP Request
- Option: (t=61,l=7) Client identifier
- Option: (t=50,l=4) Requested IP Address = 192.168.10.104
- Option: (t=12,l=12) Host Name = "cisco-ibm-xp"
- Option: (t=81,l=16) Client Fully Qualified Domain Name
- Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
- Option: (t=55,l=11) Parameter Request List
- End Option

Nella schermata di acquisizione dei pacchetti cablati si può vedere che il pacchetto 40 è la richiesta DHCP con bridge trasmessa dal client di prova 00:40:96:b6:44:51 alla rete cablata.

## Esempio di configurazione bridging

Per abilitare la funzionalità di bridging DHCP sul controller, è necessario disabilitare la funzione proxy DHCP sul controller. Questo è possibile solo nella CLI con questi comandi:

```
<#root>
```

```
(Cisco Controller) >
```

```
config dhcp proxy disable
```

```
(Cisco Controller) >
```

```
show dhcp proxy
```

```
DHCP Proxy Behaviour: disabled
```

Se il server DHCP non si trova sulla stessa rete di layer 2 (L2) del client, la trasmissione deve essere inoltrata al server DHCP sul gateway del client tramite un helper IP. Segue un esempio di questa configurazione:

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

La funzione di bridging DHCP è un'impostazione globale, quindi influisce su tutte le transazioni DHCP all'interno del controller. È necessario aggiungere istruzioni helper IP nell'infrastruttura cablata per tutte le VLAN necessarie sul controller.

Risoluzione dei problemi

I debug elencati qui sono stati abilitati sulla CLI del controller e la parte DHCP dell'output è stata estratta per questo documento.

```
<#root>
```

```
(Cisco Controller) >
```

```
debug client 00:40:96:b6:44:51
```

```
(Cisco Controller) >
```

```
debug dhcp message enable
```

```
00:40:96:b6:44:51 DHCP received op BOOTREQUEST (1) (len 308, port 1, encap 0xec03) 00:40:96:b6:44:51 DHCP
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
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) -
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
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
00:40:96:b6:44:51 Assigning Address 192.168.10.104 to mobile 00:40:96:b6:44:51 DHCP successfully bridged
```

Questo output di debug DHCP contiene alcune indicazioni chiave che il bridging DHCP è in uso sul controller:

- Il DHCP ha eseguito il bridging del pacchetto verso DS: questo significa che il pacchetto DHCP originale dal client è stato sottoposto a bridging, inalterato, verso il sistema di distribuzione (DS). Il DS è l'infrastruttura cablata.
- Il DHCP ha eseguito il bridging del pacchetto verso STA: questo messaggio indica che il pacchetto DHCP è stato sottoposto a bridging, inalterato, verso la stazione (STA). L'STA è il computer client che richiede il DHCP.

Inoltre, viene visualizzato l'indirizzo IP effettivo del server elencato nei debug, ossia 192.168.10.1. Se il proxy DHCP è in uso anziché il bridging DHCP, è possibile visualizzare l'indirizzo IP virtuale del controller elencato per l'indirizzo IP del server.

#### Avvertenze

- 

Per impostazione predefinita, il proxy DHCP è abilitato.

- 

Tutti i controller che comunicano tra loro devono avere la stessa impostazione del proxy DHCP.

- 

Il proxy DHCP deve essere abilitato affinché l'opzione DHCP 82 funzioni.

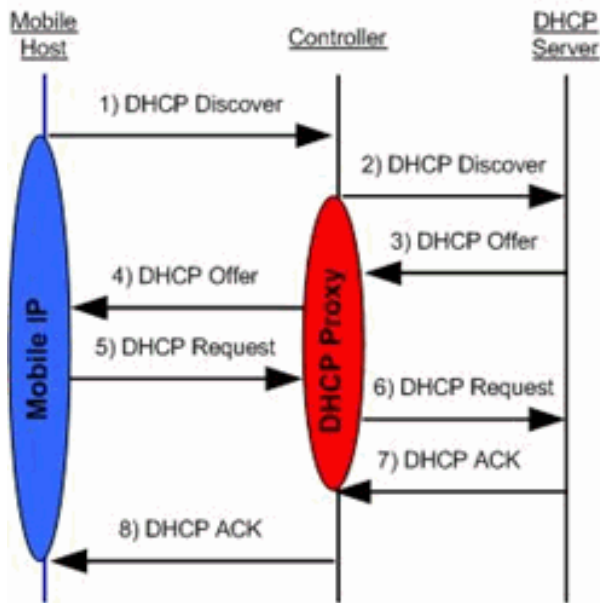
#### Server DHCP interno

Il server DHCP interno è stato introdotto inizialmente per le filiali in cui non è disponibile un server DHCP esterno. È progettato per supportare una piccola rete wireless con meno di dieci punti di accesso (AP) che si trovano sulla stessa subnet. Il server interno fornisce gli indirizzi IP ai client wireless, agli AP a connessione diretta, agli AP in modalità appliance sull'interfaccia di gestione e alle richieste DHCP inoltrate dagli AP. Non è un server DHCP generico completo. Supporta solo funzionalità limitate e non è scalabile in un'installazione di maggiori dimensioni.

#### Confronto tra modalità DHCP e bridging interno

Le due modalità DHCP principali sul controller sono proxy DHCP o bridging DHCP. Con la modalità bridging DHCP il controller agisce più come supporto DHCP con AP autonomi. Un pacchetto DHCP entra nell'AP tramite un'associazione client a un Service Set Identifier (SSID) collegato a una VLAN. Quindi, il pacchetto DHCP esce dalla VLAN. Se sul gateway di layer 3 (L3) della VLAN è definito un helper IP, il pacchetto viene inoltrato al server DHCP tramite unicast diretto. Il server DHCP risponde quindi direttamente all'interfaccia L3 che ha inoltrato il pacchetto DHCP. Con il proxy DHCP, si tratta della stessa idea, ma tutto l'inoltro viene eseguito direttamente sul controller anziché sull'interfaccia L3 della VLAN. Ad esempio, se il client invia una richiesta DHCP alla WLAN, la WLAN usa il server DHCP definito sull'interfaccia della VLAN \*oppure\* usa la funzione di override DHCP della WLAN per inoltrare un pacchetto DHCP unicast al server DHCP con il campo DHCP GIADDR compilato come indirizzo IP dell'interfaccia VLAN.

#### Server DHCP interno - Flusso di pacchetti




### Handling of Packets for Local Clients

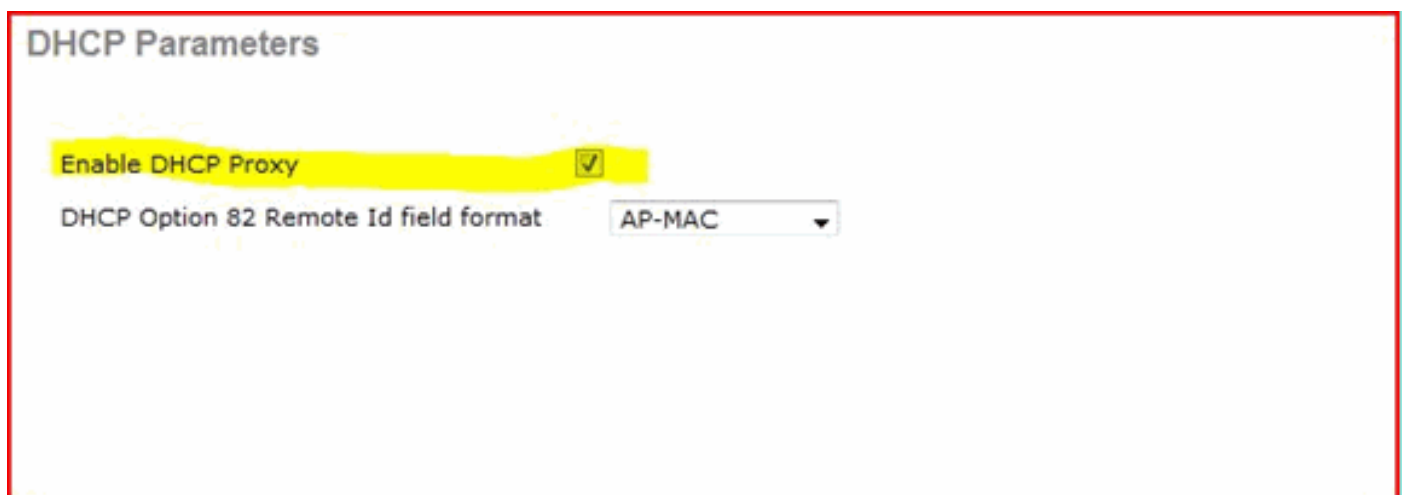
- 1) Client sends DHCP discover as all-subnets broadcast
- 2) Controller forwards the DHCP discover via the DHCP proxy service of the controller to the internal DHCP server (Note: the configured DHCP server IP address must be the management IP address of the controller).
- 3) Internal DHCP server sends DHCP offer back to the DHCP proxy agent on the controller.
- 4) Controller unicasts DHCP offer to client with option 54 and source address set as controller's management IP address.
- 5) Client sends DHCP request to the management IP address.
- 6) Controller unicasts DHCP request from WLAN IP address to DHCP proxy service which then forwards the request to the internal DHCP server.
- 7) Internal DHCP server sends ACK to the DHCP proxy service.
- 8) Controller unicasts ACK to the client.

Esempio di configurazione del server DHCP interno

È necessario abilitare il proxy DHCP sul controller per consentire il funzionamento del server DHCP interno. A questo scopo è possibile usare la GUI in questa sezione:

 **Nota:** in alcune versioni non è possibile impostare il proxy DHCP tramite la GUI.

Controller->Advanced->DHCP



Oppure tramite la CLI:

Config dhcp proxy enable Save config

Per abilitare il server DHCP interno, attenersi alla seguente procedura:

1. Definire un ambito da utilizzare per il pull degli indirizzi IP (Controller > Internal DHCP Server > DHCP Scope). Fare clic su .New

### DHCP Scope > Edit

Scope Name	User Scope		
Pool Start Address	<input type="text" value="192.168.100.100"/>		
Pool End Address	<input type="text" value="192.168.100.200"/>		
Network	<input type="text" value="192.168.100.0"/>		
Netmask	<input type="text" value="255.255.255.0"/>		
Lease Time (seconds)	<input type="text" value="86400"/>		
Default Routers	<input type="text" value="192.168.100.1"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
DNS Domain Name	<input type="text" value="wlc2106.local"/>		
DNS Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Netbios Name Servers	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Status	<input type="text" value="Enabled"/>		

2. Puntare l'override DHCP all'indirizzo IP dell'interfaccia di gestione del controller.

WLANs > Edit < Back

**General** **Security** **QoS** **Advanced**

Allow AAA Override  Enabled  
 Coverage Hole Detection  Enabled  
 Enable Session Timeout  1800  
     Session Timeout (secs)  
 Aironet IE  Enabled  
 Diagnostic Channel  Enabled  
 IPv6 Enable   
 Override Interface ACL   
 P2P Blocking Action   
 Client Exclusion  Enabled 60  
     Timeout Value (secs)  
 VoIP Snooping and Reporting

**DHCP**

DHCP Server  Override  
 192.168.100.254  
 DHCP Server IP Addr  
 DHCP Addr. Assignment  Required

**Management Frame Protection (MFP)**

Infrastructure MFP Protection   
 MFP Client Protection

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255)   
 802.11b/g/n (1 - 255)

**HREAP**

H-REAP Local Switching  Enabled  
 Learn Client IP Address  Enabled

**NAC**

State  Enabled

3. Verificare che il proxy DHCP sia abilitato.

**DHCP Parameters**

Enable DHCP Proxy

DHCP Option 82 Remote Id field format

Risoluzione dei problemi

Per eseguire il debug del server DHCP interno, in genere è necessario individuare un client che non riesce a ottenere un indirizzo IP. Eseguire il debug.

debug client <MAC ADDRESS OF CLIENT>

Il client di debug è una macro che abilita questi debug e concentra il debug solo sull'indirizzo MAC del client immesso.

```
debug dhcp packet enable debug dot11 mobile enable debug dot11 state enable debug dot1x events enable debug pem events enable debug pem state enable
```

Il comando principale per i problemi DHCP è il comando `debug dhcp packet enable` abilitato automaticamente dal debug client comando.

<#root>

```
00:1b:77:2b:cf:75 dhcpd: received DISCOVER
```

```
00:1b:77:2b:cf:75 dhcpd: Sending DHCP packet (giaddr:192.168.100.254)to 127.0.0.1:67
from 127.0.0.1:1067
```

```
00:1b:77:2b:cf:75 sendto (548 bytes) returned 548 00:1b:77:2b:cf:75 DHCP option len (including the mag
```

```
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 =
```

```
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
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 = c
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 mag
```

```
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 =
```

Cancella i lease DHCP sul server DHCP interno del WLC

È possibile utilizzare questo comando per azzerare i lease DHCP sul server DHCP interno del WLC:

<#root>

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

Di seguito è riportato un esempio:

```
<#root>
```

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

Avvertenze

- 

Per il funzionamento del server DHCP interno, il proxy DHCP deve essere abilitato

- 

Utilizzo di DHCP per la porta 1067 quando si utilizza il server DHCP interno, interessato dall'ACL della CPU

- 

Il server DHCP interno è in ascolto sull'interfaccia loopback del controller tramite la porta 67 dell'UDP 127.0.0.1

Interfaccia utente finale

- 

Il **config dhcp proxy disable** comando implica l'uso della funzione di bridging DHCP. Questo è un comando globale (non un comando per WLAN).

- 

Il proxy DHCP rimane abilitato per impostazione predefinita.

- 

Quando il proxy DHCP è disabilitato, il server DHCP interno non può essere utilizzato dalle WLAN locali. Il bridging non è coerente



con le operazioni necessarie per reindirizzare un pacchetto al server interno. Bridging è tale a tutti gli effetti, ad eccezione della conversione da 802.11 a Ethernet II. I pacchetti DHCP vengono passati senza modifiche dal tunnel LWAPP alla VLAN client (e viceversa).

•

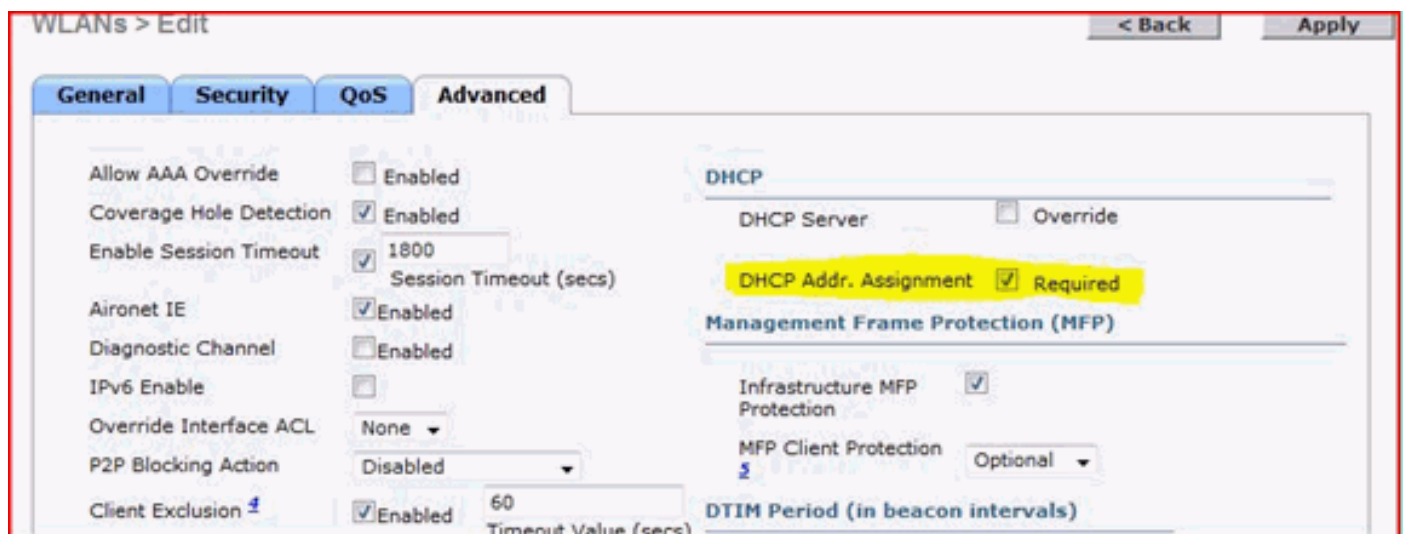
Quando il proxy è abilitato, per abilitare la WLAN è necessario configurare un server DHCP sull'interfaccia della WLAN (o nella WLAN stessa). Non occorre configurare nessun server quando il proxy è disabilitato, in quanto questi server non vengono utilizzati.

•

Quando un utente tenta di abilitare il proxy DHCP, si verifica internamente che per tutte le WLAN (o le interfacce associate) sia stato configurato almeno un server DHCP. In caso contrario, l'operazione di abilitazione non riesce.

## DHCP richiesto

La configurazione avanzata della WLAN dispone di un'opzione che richiede il passaggio del protocollo DHCP prima che gli utenti passino allo stato RUN (uno stato in cui il client può passare il traffico attraverso il controller). Questa opzione richiede al client di eseguire una richiesta DHCP full o half. Il controller cerca una richiesta DHCP dal client e un ACK che ritorna dal server DHCP. Finché il client esegue questi passaggi, passa il passaggio DHCP richiesto e passa allo stato RUN.



## Roaming L2 e L3

Roam L2: se il client ha un lease DHCP valido ed esegue un roaming L2 tra due controller diversi sulla stessa rete L2, il client non deve essere riconnesso a DHCP e la voce del client deve essere spostata completamente nel nuovo controller dal controller originale. Quindi, se il client deve nuovamente DHCP, il processo di bridging o proxy DHCP sul controller corrente esegue di nuovo il bridging del pacchetto in modo trasparente.

L3 Roam - In uno scenario L3 roam, il client si sposta tra due controller diversi in reti L3 diverse. In questo caso, il client è ancorato al controller originale ed elencato nella tabella client del nuovo controller esterno. Durante lo scenario di ancoraggio, il DHCP client viene gestito dal controller di ancoraggio come i dati client vengono tunneling all'interno di un tunnel EoIP tra i controller di ancoraggio e i controller esterni.

## Informazioni correlate

- [Esempio di configurazione dell'opzione DHCP 43 sui Cisco Aironet Lightweight Access Point](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).