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

Sommario

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	Proxy e agente relay non sono esattamente la stessa cosa. 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 la 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'uso di un indirizzo IP virtuale può causare problemi su alcuni tipi di client.

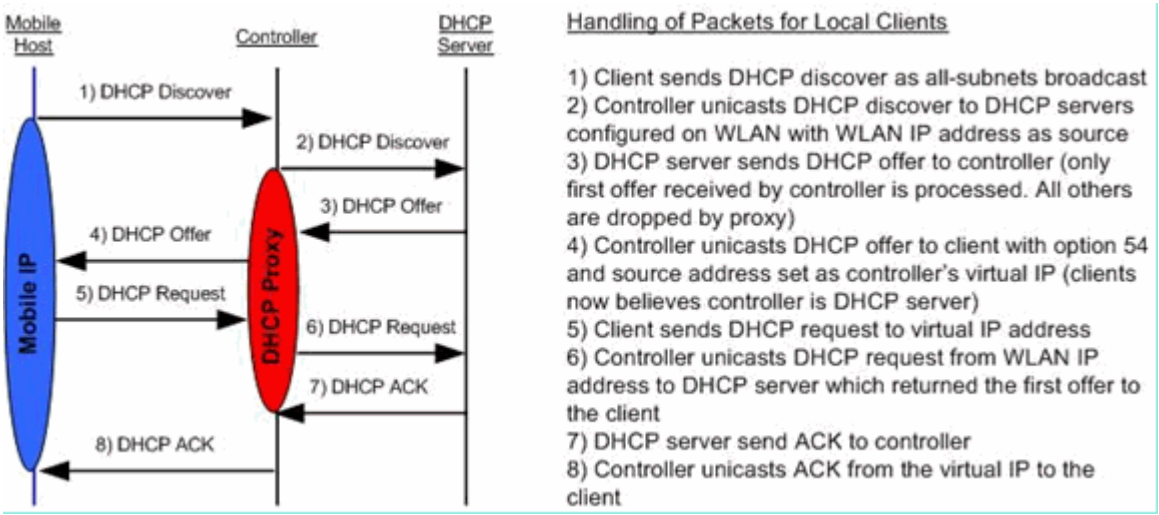
Il funzionamento in modalità proxy DHCP mantiene lo stesso comportamento sia per i protocolli di mobilità simmetrici che asimmetrici.

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 passano attraverso lo stesso server DHCP fino a quando una transazione non riesce dopo i 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

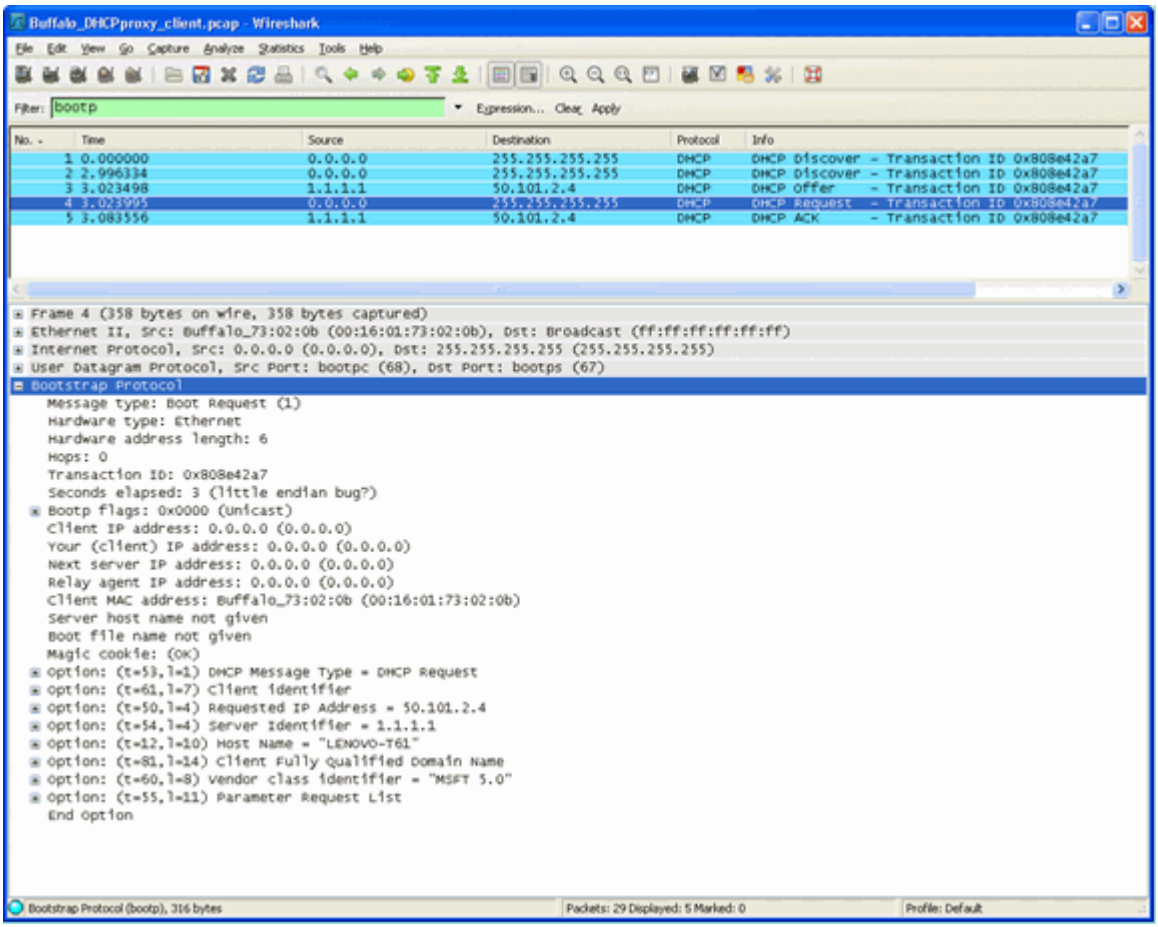


Acquisizione di pacchetti proxy

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.

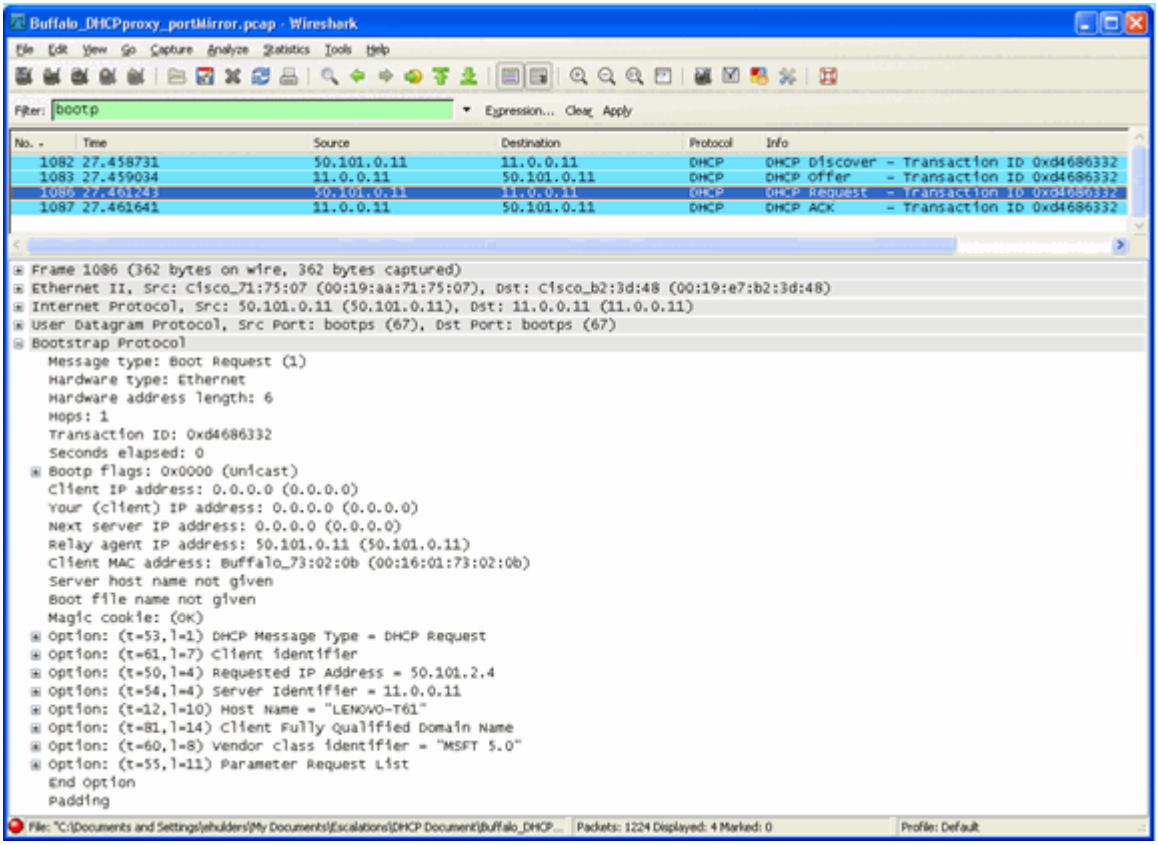
Prospettiva client

Questa schermata mostra 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 è evidenziata e i dettagli del protocollo di avvio sono espansi per mostrare le opzioni DHCP.



Prospettiva server

Questa schermata mostra un'acquisizione di 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. Tuttavia, si tratta di pacchetti creati dal controller come funzione del proxy DHCP. Anche in questo caso, la richiesta DHCP è evidenziata e i dettagli del protocollo di avvio sono espansi per mostrare le opzioni DHCP. Si noti che sono uguali a quelle del pacchetto richiesta DHCP dei client. Si noti inoltre che il proxy del WLC ritrasmette gli indirizzi dei pacchetti e li evidenzia.



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 utilizzare questo comando CLI, disponibile anche nella GUI, nella pagina Controller del 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 su 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

(Cisco Controller) >

config interface dhcp management primary

(Cisco Controller) >

config interface dhcp dynamic-interface

primary

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** 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 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
```

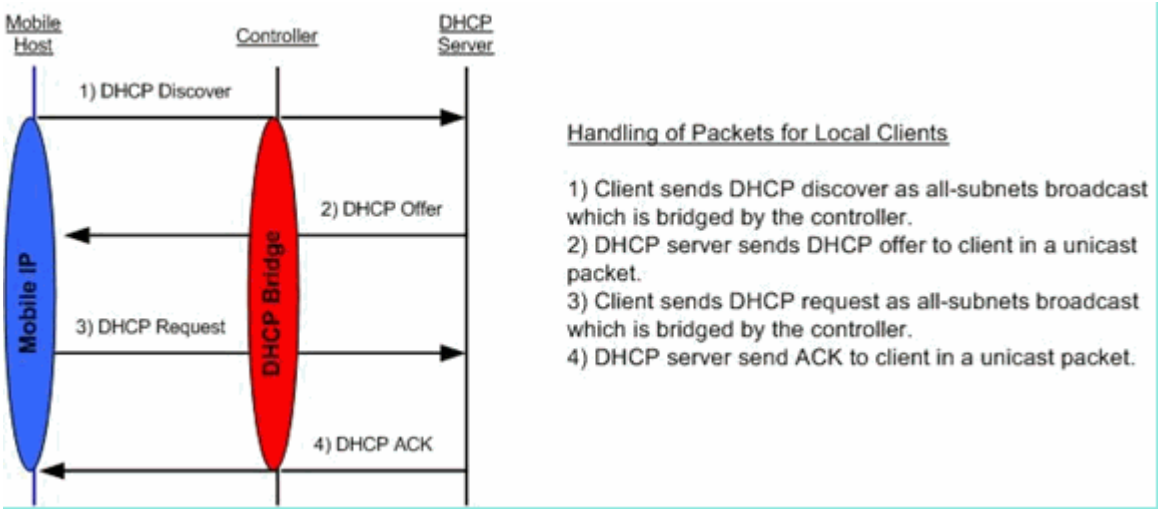
Avvertenze

- 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. La soluzione a questo problema consiste nel disabilitare il proxy DHCP sul controller.
- Quando un client si trova nello stato DHCP REQ sul controller, il controller rilascia i pacchetti di informazioni DHCP. 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. Quando il proxy DHCP è disabilitato, i pacchetti di informazioni DHCP vengono inoltrati dal controller.
- Tutti i controller che comunicano tra loro devono avere la stessa impostazione del proxy DHCP.

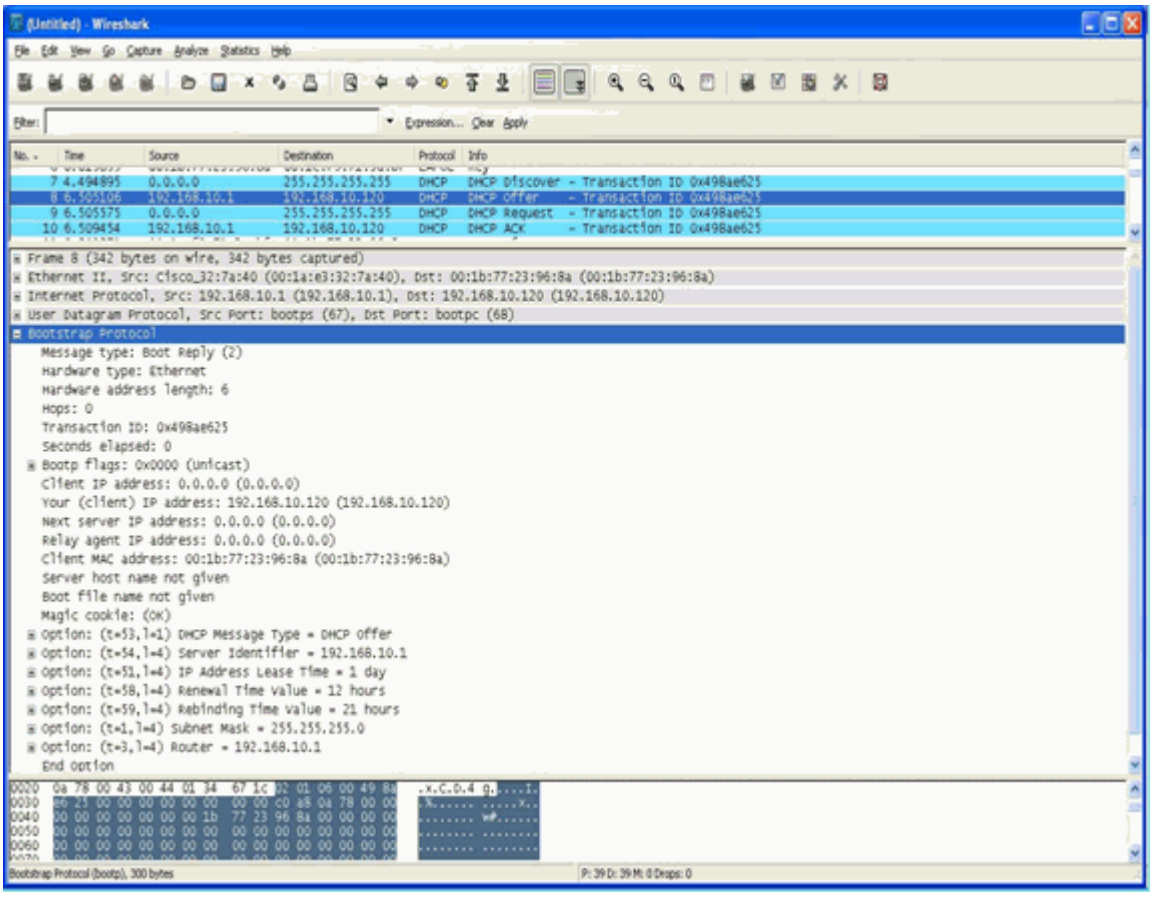
Modalità bridging DHCP

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 della conversione da Ethernet II a 802.11, i pacchetti al client vengono collegati senza modifiche dalla VLAN client (o 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

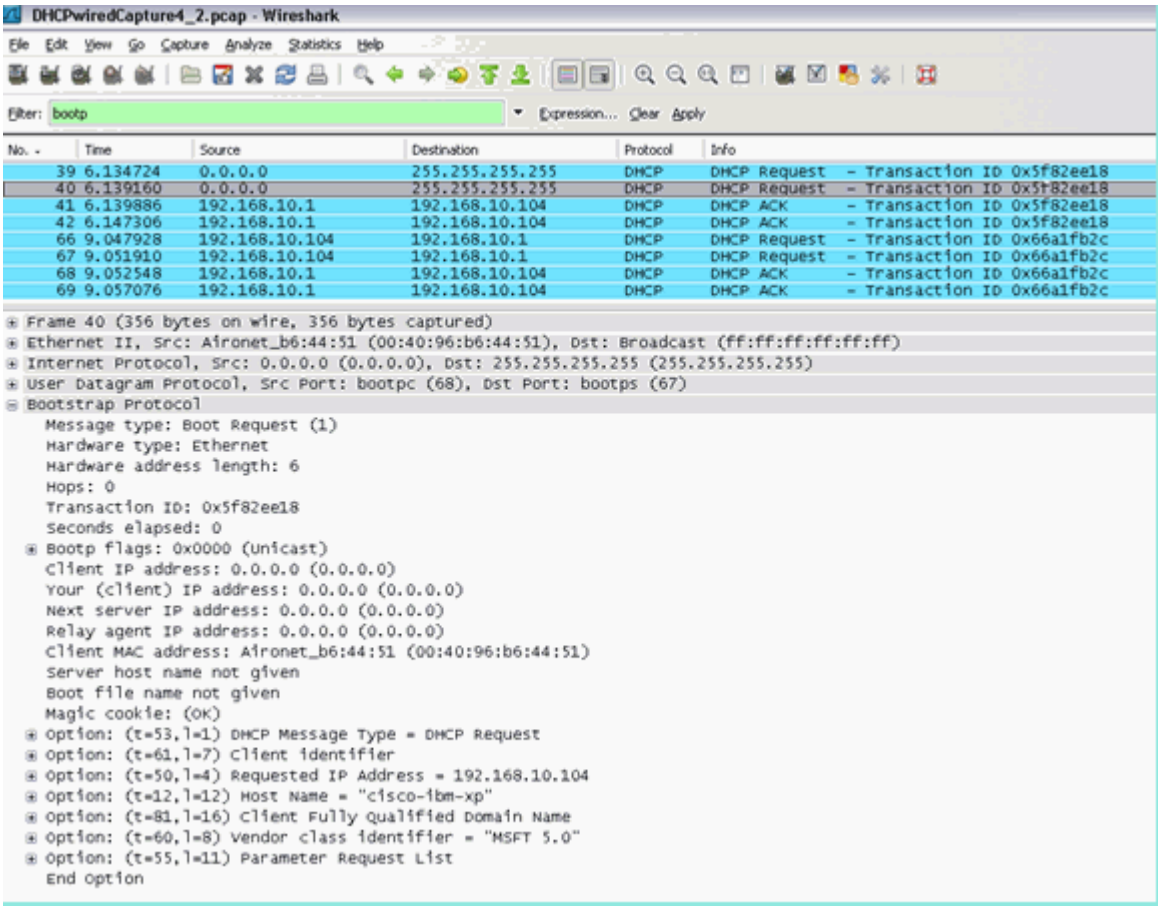


Acquisizione di pacchetti bridging - Prospettiva client



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

Acquisizione di pacchetti bridging - Prospettiva server



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




Switch(config-if)#

ip helper-address
```

La funzione di bridging DHCP è un'impostazione globale, quindi influisce su tutte le transazioni DHCP all'interno del controller. È necessario aggiungere le istruzioni di supporto 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 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
```

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 era in uso anziché il bridging DHCP, l'indirizzo IP virtuale del controller verrà 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.

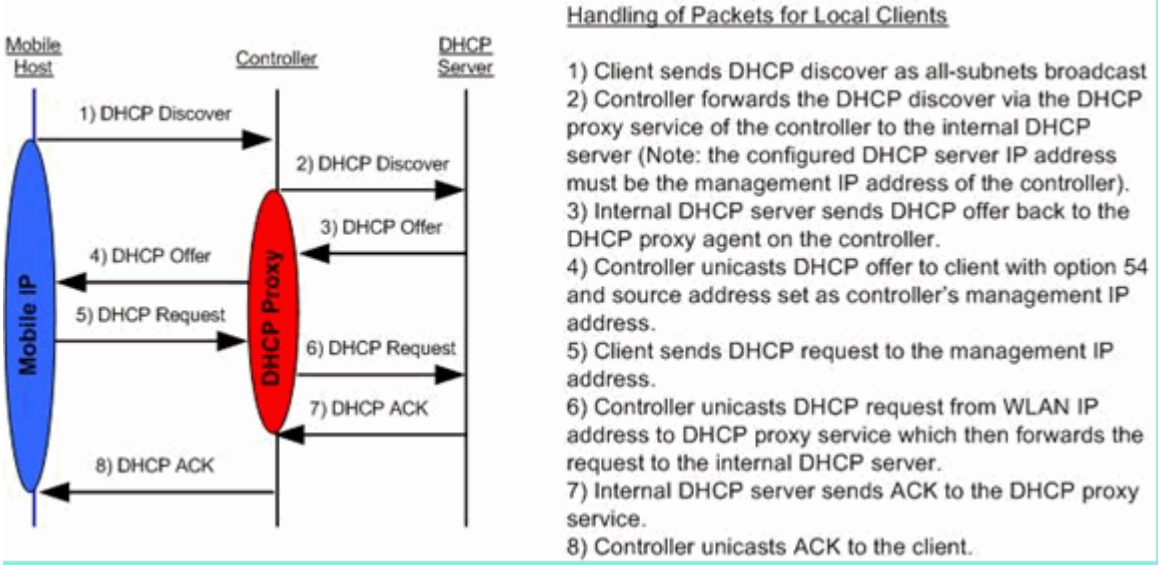
Server DHCP interno

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 access point (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 si tratta di un server DHCP per scopi generici. 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 viene definito un supporto IP sul gateway di livello 3 (L3) della VLAN, 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, l'idea è la stessa, ma 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* utilizza 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

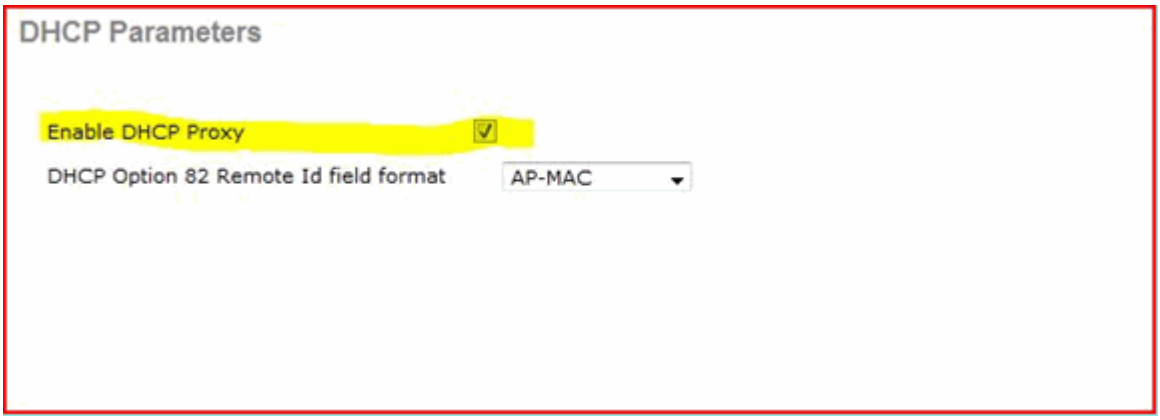


Esempio di configurazione del server DHCP interno

Per consentire il funzionamento del server DHCP interno è necessario abilitare il proxy DHCP sul controller. 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
```

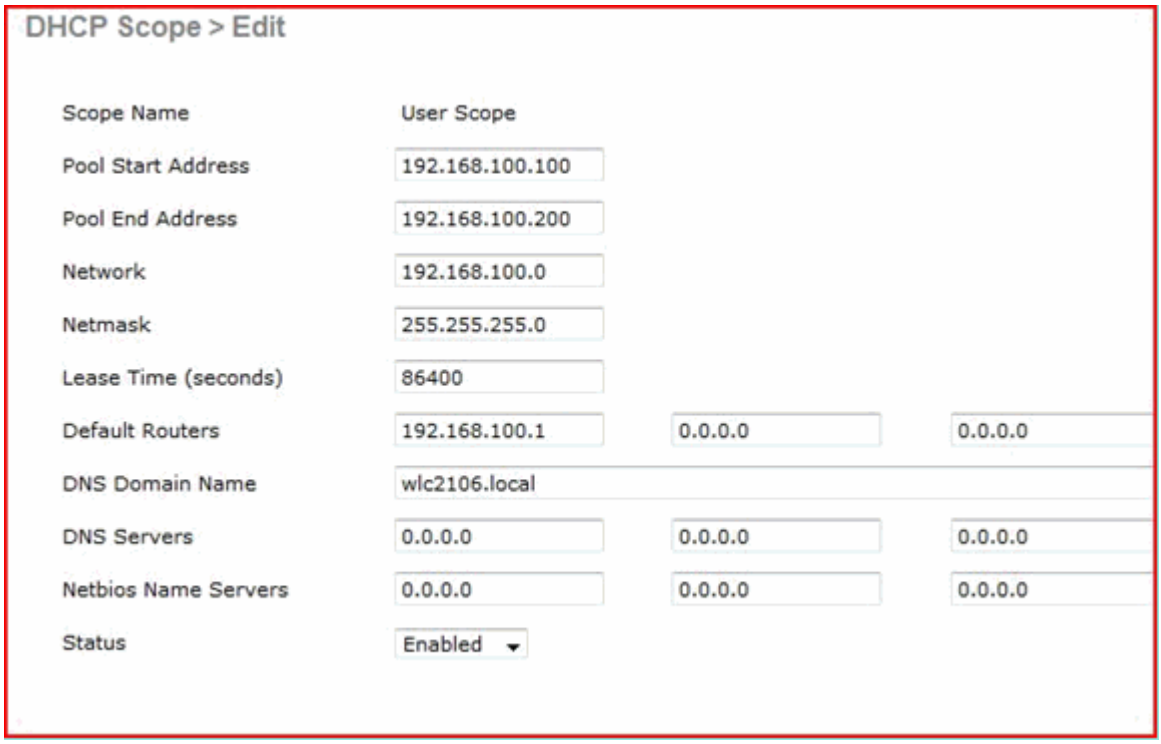


Oppure tramite la CLI:

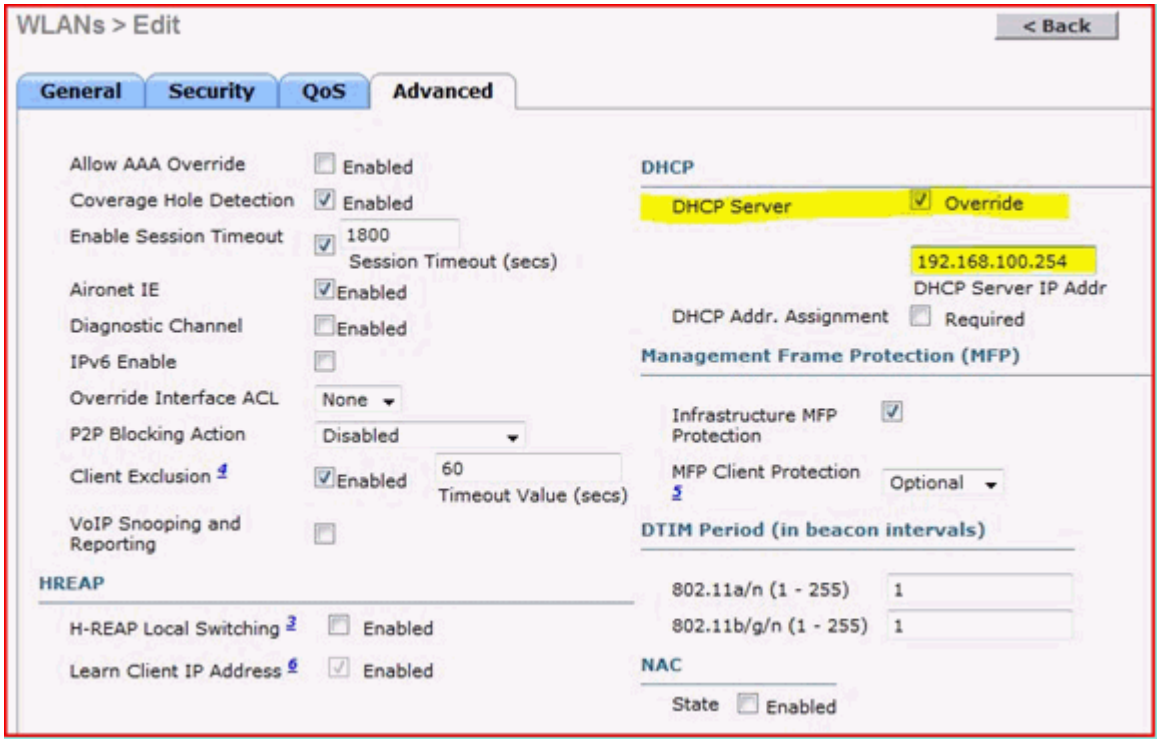
```
Config dhcp proxy enable
Save config
```

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

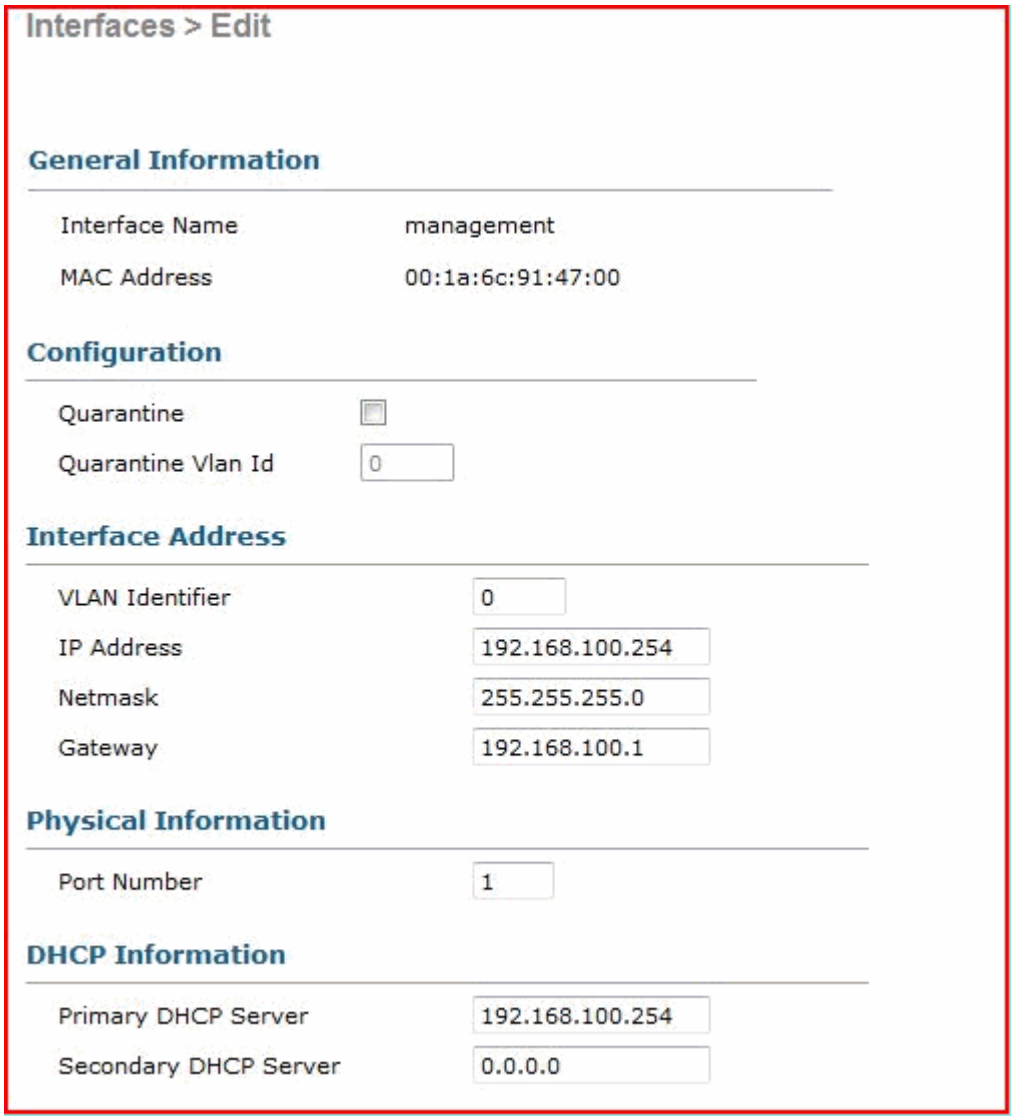
1. Definire un ambito da utilizzare per il pull degli indirizzi IP (Controller > Server DHCP interno > Ambito DHCP). Fare clic su **New**.



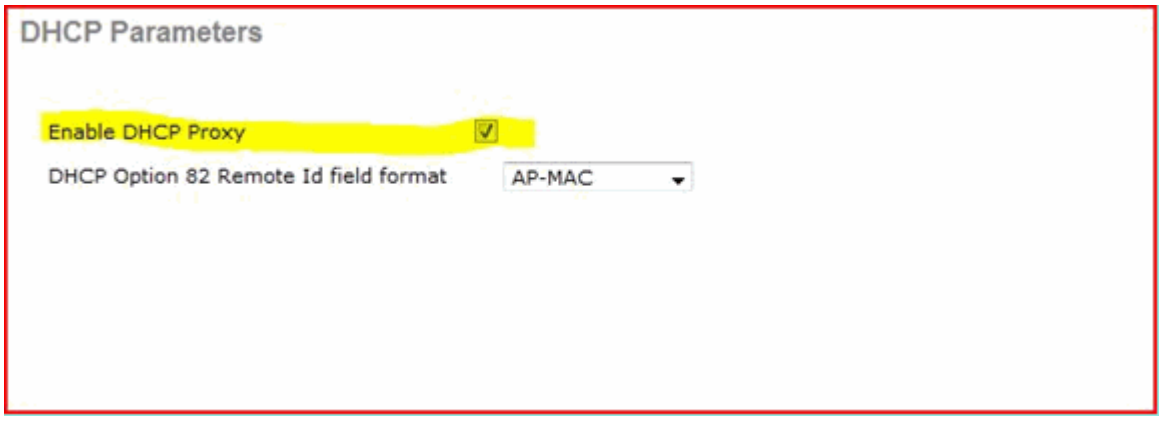
2. Puntare l'override DHCP sull'indirizzo IP dell'interfaccia di gestione del controller.



In alternativa, è possibile utilizzare l'opzione DHCP della configurazione dell'interfaccia del controller per l'interfaccia con cui si desidera utilizzare il server DHCP interno.



3. Assicurarsi che il proxy DHCP sia abilitato.



Risoluzione dei problemi

Il debug del server DHCP interno in genere richiede l'individuazione di un client con problemi per ottenere un indirizzo IP. È necessario eseguire questi 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
debug cckm client debug enable
```

La principale per i problemi DHCP è la **debug dhcp packet enable** che viene attivato automaticamente dal **debug client**

<#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
```

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
```

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

- OSPF (Open Shortest Path First) **config dhcp proxy disable** 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.

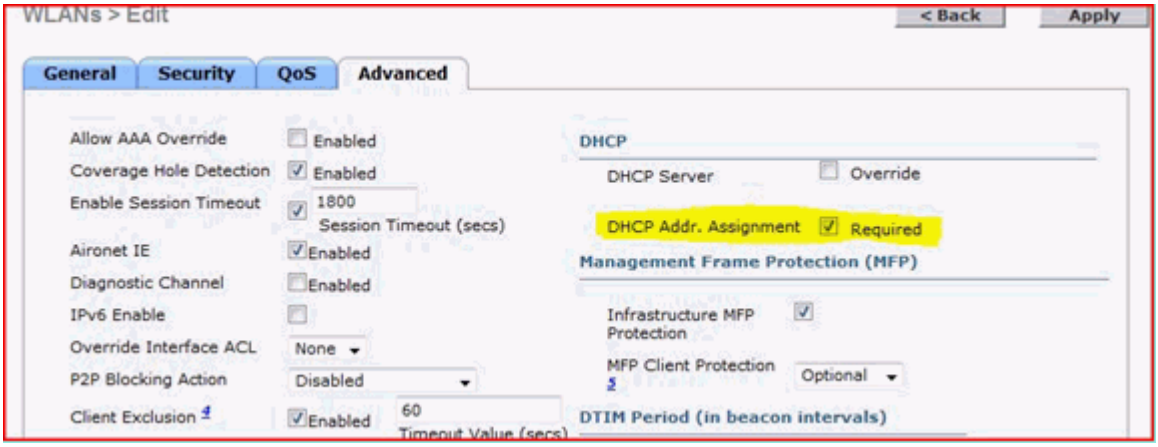
- Quando il proxy DHCP è disabilitato, il server DHCP interno non può essere utilizzato dalle WLAN locali. Il bridging non è coerente con le operazioni necessarie per reindirizzare un pacchetto al server interno. Bridging è tale a tutti gli effetti, ad eccezione della conversione da 802.11 a Ethernet 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 abbiano 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. Fintanto che il client esegue questi passaggi, il client supera 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 eseguire nuovamente il DHCP, il bridging DHCP o il processo proxy sul controller corrente eseguirà nuovamente il bridging 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 â€“ 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).