Esempio di configurazione dell'accesso guest a reti cablate tramite i controller WLAN Cisco

Sommario

Introduzione

In questo documento viene descritto come configurare l'accesso guest con il nuovo supporto della funzionalità WLC (Wired Guest Access) sui controller Cisco WLAN (WLC) che usano il software Cisco Unified Wireless Software versione 4.2.61.0 e successive. Un numero crescente di aziende riconosce la necessità di fornire l'accesso a Internet a clienti, partner e consulenti quando si recano presso le loro sedi. I responsabili IT possono fornire agli utenti guest un accesso protetto e controllato a Internet tramite cavo e wireless utilizzando lo stesso controller LAN wireless.

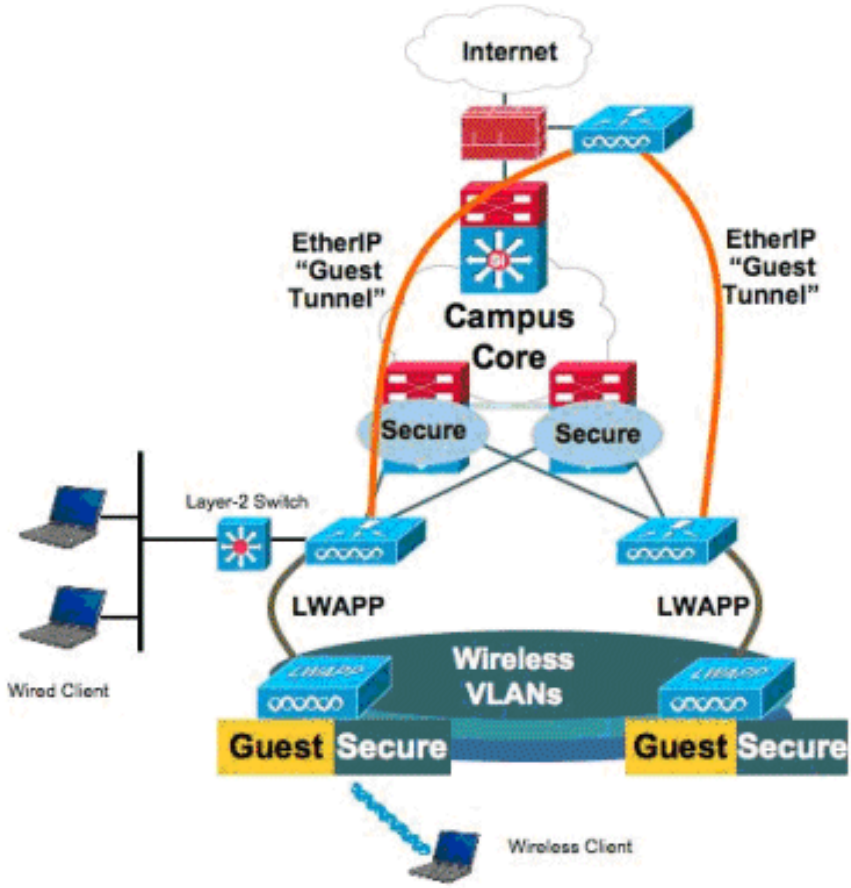
Gli utenti guest devono essere autorizzati a connettersi alle porte Ethernet designate e ad accedere alla rete guest come configurato dall'amministratore dopo aver completato i metodi di autenticazione configurati. Gli utenti guest wireless possono connettersi facilmente ai controller WLAN con le funzionalità di accesso guest correnti. Inoltre, Wireless Control System (WCS), insieme alla configurazione e alla gestione di base dei controller WLAN, offre servizi utente guest avanzati. I clienti che hanno già implementato o intendono installare controller WLAN e controller WCS nella rete possono utilizzare la stessa infrastruttura per l'accesso guest cablato. In questo modo gli utenti finali possono usufruire di un accesso wireless e cablato unificato.

Le porte guest cablate vengono fornite in una posizione designata e collegate a uno switch di accesso. La configurazione sullo switch di accesso colloca queste porte in una delle VLAN di layer 2 cablate. Sono disponibili due soluzioni separate per i clienti:

- Un controller WLAN singolo (modalità di conversione VLAN): lo switch di accesso trunk il traffico guest cablato nella VLAN guest sul controller WLAN che fornisce la soluzione di accesso guest cablato. Questo controller esegue la conversione della VLAN dalla VLAN guest

cablata in entrata alla VLAN in uscita.

- Due controller WLAN (modalità di ancoraggio automatico): lo switch di accesso trunk il traffico guest cablato su un controller WLAN locale (il controller più vicino allo switch di accesso). Questo controller WLAN locale consente di ancorare il client a un controller WLAN di ancoraggio DMZ (Demilitarized Zone) configurato per l'accesso guest cablato e wireless. Dopo il corretto trasferimento del client al controller di ancoraggio DMZ, l'assegnazione dell'indirizzo IP DHCP, l'autenticazione del client e così via vengono gestite nel WLC DMZ. Al termine dell'autenticazione, il client può inviare/ricevere
traffico.



Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il supporto della funzione Wired Guest Access sui controller Cisco WLAN è supportato dal software Cisco Unified Wireless versione 4.2.61.0 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Configurazione Access Layer Switch

Per fornire l'accesso guest cablato, l'amministratore deve configurare le porte designate nello switch del livello di accesso di layer 2 sulla VLAN guest. La VLAN guest deve essere distinta da tutte le altre VLAN configurate su questo switch. Il traffico della VLAN guest viene troncato al controller locale WLAN più vicino. Il controller locale crea un tunnel del traffico guest attraverso un tunnel Ethernet over IP (EoIP) per il controller di ancoraggio DMZ. Questa soluzione richiede almeno due controller.

In alternativa, lo switch di accesso trunk la VLAN guest su un controller singolo, converte la VLAN guest nell'interfaccia in uscita del controller WLAN.

```
cat6506# show vlan id 49

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
49   VLAN0049                         active    Gi2/1, Gi2/2, Gi2/4, Gi2/35
                                                Gi2/39, Fa4/24

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
49   enet  100049     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

cat6506#
interface FastEthernet4/24
 description Wired Guest Access
 switchport
 switchport access vlan 49
 no ip address
end
cat6506#
interface GigabitEthernet2/4
 description Trunk port to the WLC
 switchport
 switchport trunk native vlan 80
 switchport trunk allowed vlan 49,80,110
 switchport mode trunk
 no ip address
end
```

> **Nota**: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Punti importanti per l'installazione di sistemi guest cablati

- Al momento sono supportate cinque LAN guest per l'accesso guest cablato. In totale, è possibile configurare sul WLC di ancoraggio 16 WLAN per utenti wireless e 5 WLAN per l'accesso guest cablato. Non esistono tunnel separati per le WLAN. Tutte le WLAN guest, che includono le WLAN per l'accesso guest cablato, utilizzano gli stessi tunnel EoIP per il WLC di ancoraggio.
- Gli amministratori devono creare interfacce dinamiche nel controller WLAN, contrassegnarle come "LAN guest" e associarle alle WLAN create come LAN guest.
- Verificare che le configurazioni WLAN, inclusa l'autenticazione, siano identiche sui controller di ancoraggio e remoto per consentire il passaggio del traffico client.
- I WLC devono avere versioni software compatibili. Assicurarsi che eseguano la stessa versione principale.
- L'autenticazione tramite Web è il meccanismo di sicurezza predefinito disponibile su una LAN guest cablata. Le opzioni disponibili sono: Open, Web Auth e Web Passthrough.
- In caso di errore del tunnel EoIP tra il WLC remoto e il WLC di ancoraggio, il database del client viene eliminato dal WLC di ancoraggio. Il client deve essere riassociato e riautenticato.
- Non è supportata alcuna protezione di livello 2.
- Il traffico multicast/broadcast sulle LAN guest cablate viene interrotto.
- Le impostazioni del proxy DHCP devono essere identiche sui controller di ancoraggio e remoto.

Per il guest cablato, è presente un timeout di inattività nel controller. Se il client non riceve alcun pacchetto entro il periodo configurato, viene rimosso dal controller. Quando un client invia una richiesta ARP (Address Resolution Protocol) la volta successiva, viene creata una nuova voce client che viene spostata in modo appropriato nello stato di esecuzione/autenticazione Web in base alla configurazione di protezione.

Supporto piattaforma

L'accesso guest cablato è supportato sulle seguenti piattaforme:

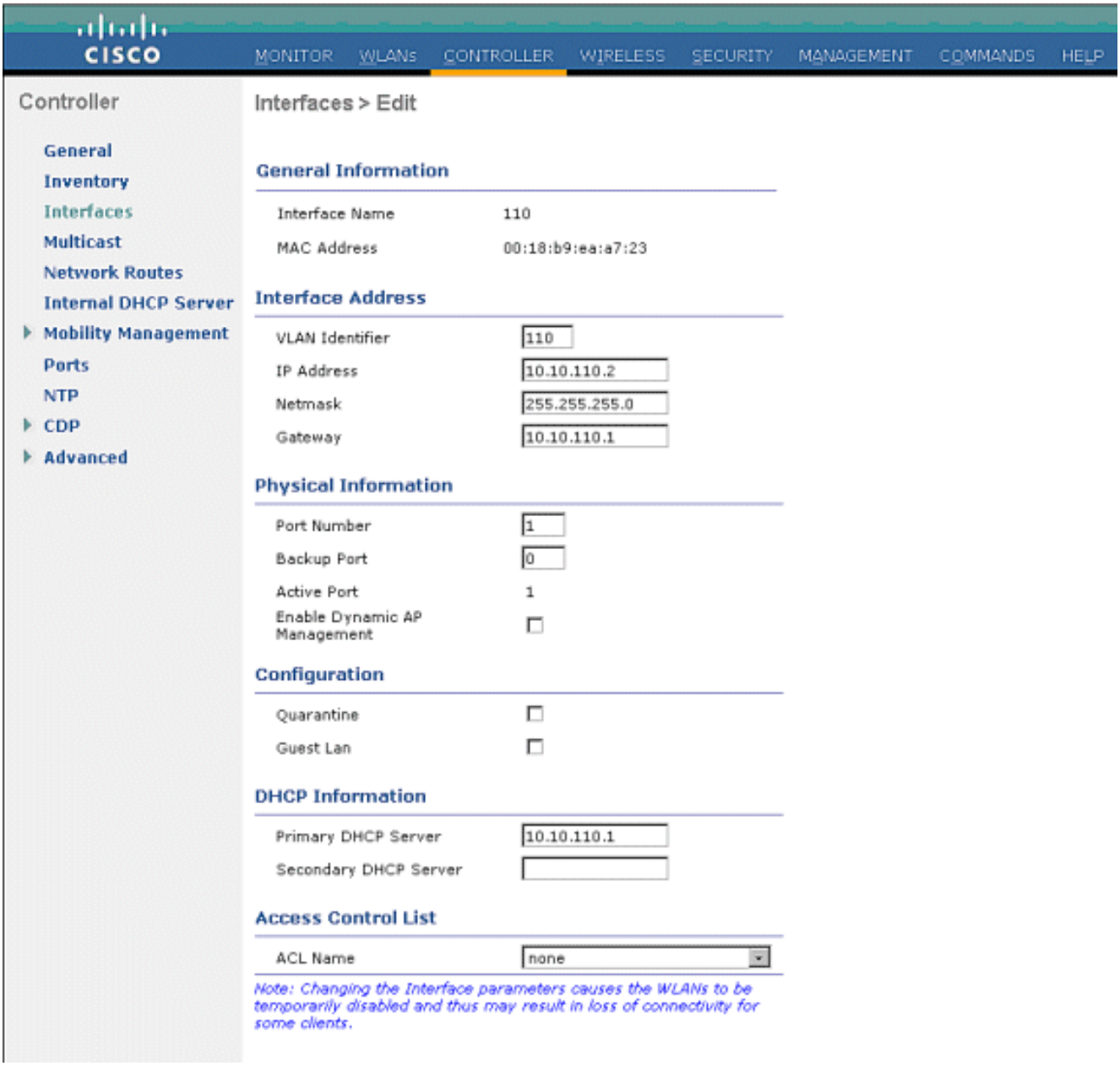
- Cisco WLC 4402, 4404, WiSM, 3750G, 5508, WiSM2, WLC virtuale

Configurazione LAN wireless

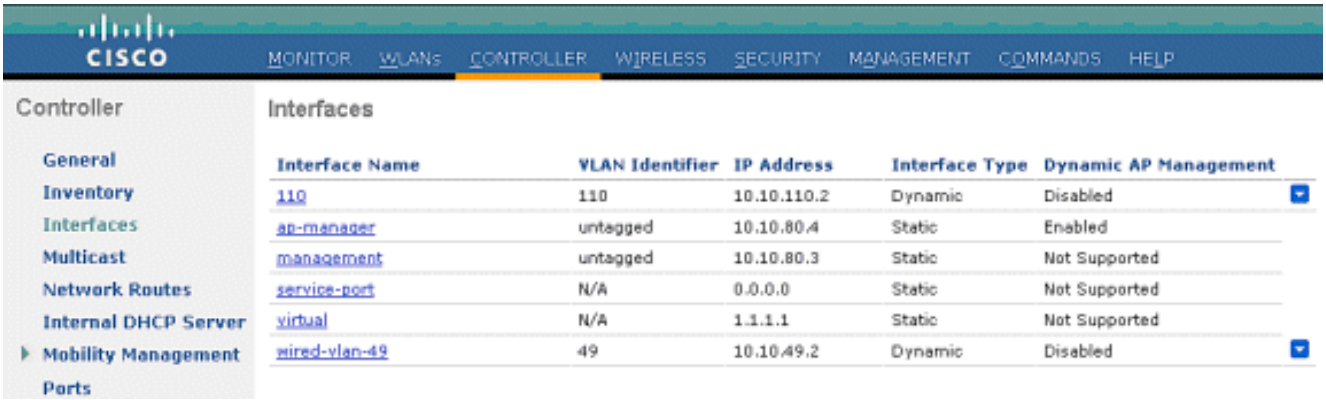
nell'esempio viene utilizzata la configurazione di base del controller LAN wireless. L'attenzione è rivolta alla configurazione aggiuntiva necessaria per completare l'implementazione dell'accesso guest cablato.

1. Creare un'interfaccia dinamica e contrassegnarla come "LAN guest". Quando si crea questa interfaccia dinamica nella versione corrente, è necessario fornire un indirizzo IP e un gateway predefinito, anche se non esiste perché è una VLAN di layer 2; non è necessario fornire alcun indirizzo DHCP. I client guest cablati sono fisicamente connessi a questa VLAN.

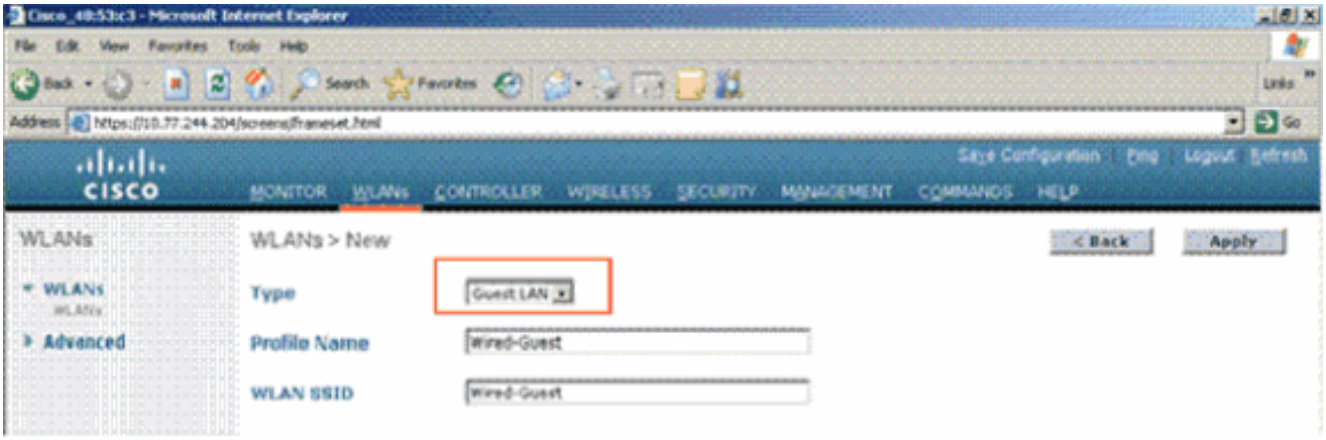
2. Creare un'altra interfaccia dinamica in cui i client guest cablati ricevono un indirizzo IP.**Nota:** Specificare un indirizzo IP, un gateway predefinito o un indirizzo del server DHCP nell'interfaccia.



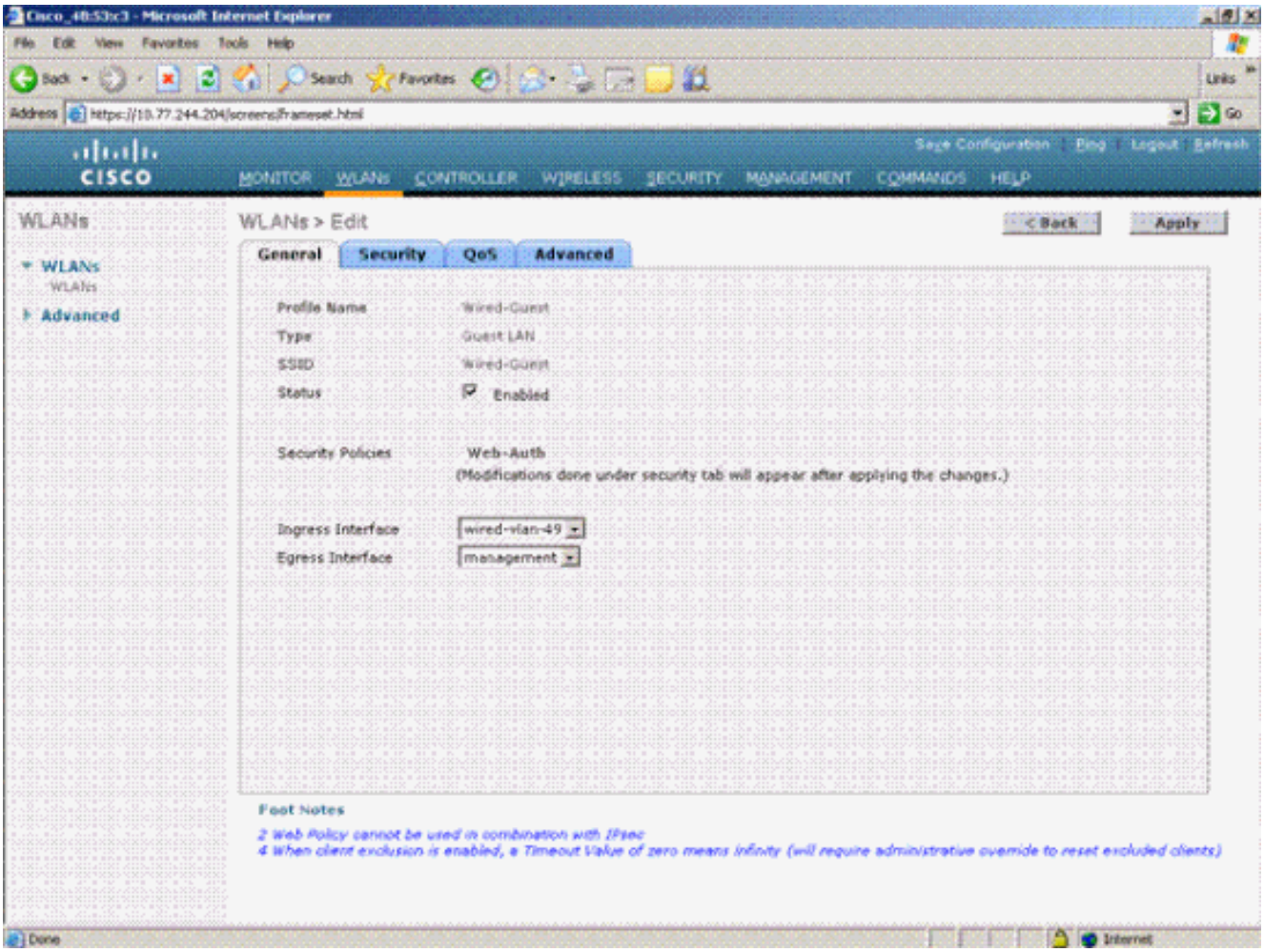
3. Queste sono le interfacce dinamiche:



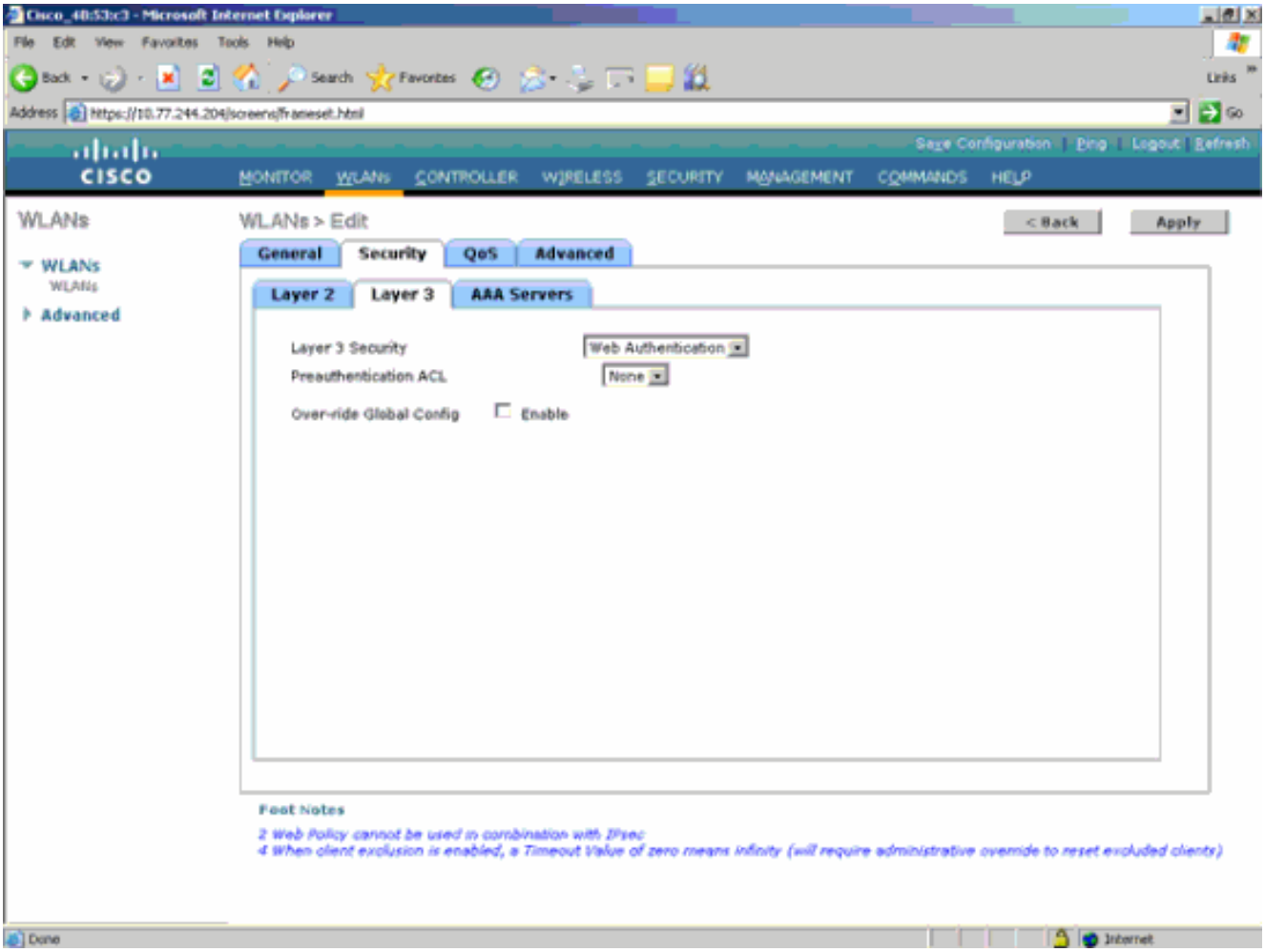
4. Aggiungi nuova WLAN: Type=LAN guest.



5. abilitare la WLAN; mappare l'interfaccia in entrata alla "LAN guest" creata nel passaggio 1 e l'interfaccia in uscita può essere un'interfaccia di gestione o qualsiasi altra interfaccia dinamica, anche se preferibilmente un'interfaccia dinamica come quella creata nel passaggio 2.

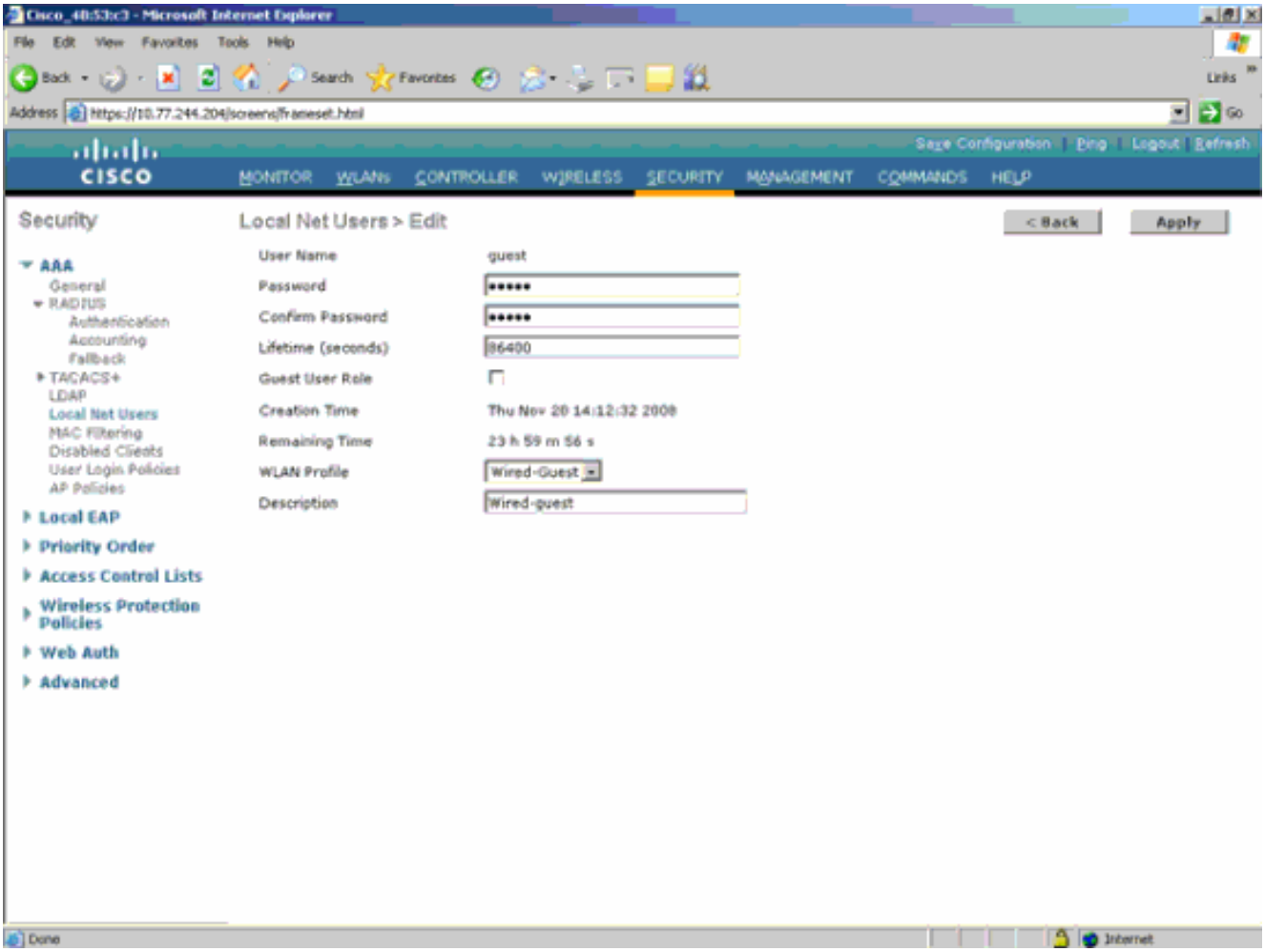


6. L'autenticazione Web è attivata per impostazione predefinita come opzione di protezione configurata sulla LAN guest. Può essere modificato in *Nessuno* o *Web Passthrough*.



7. questa è la configurazione finale della WLAN.

8. Aggiungere un utente guest nel database locale del WLC.

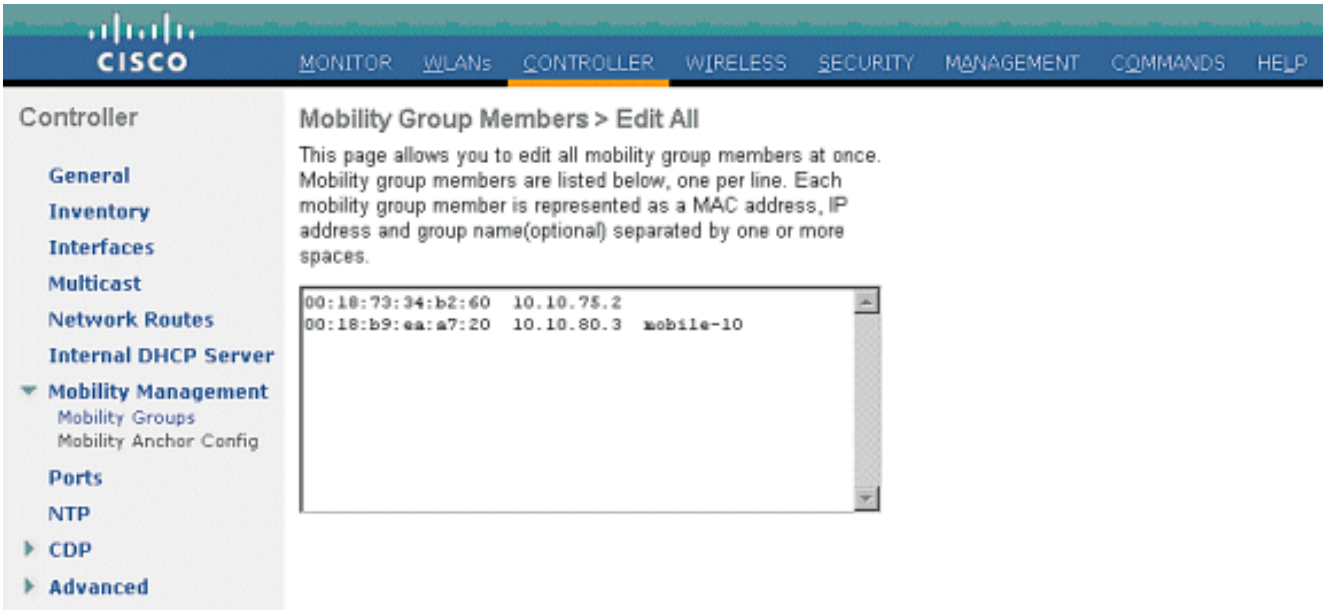


Sul collegamento esterno, è necessario impostare l'ingresso come "LAN guest" configurata. In uscita, è necessario impostarla su un'interfaccia, possibilmente l'interfaccia di gestione. Tuttavia, una volta costruito il tunnel EoIP, il traffico viene inviato automaticamente attraverso il tunnel anziché tramite l'indirizzo di gestione.

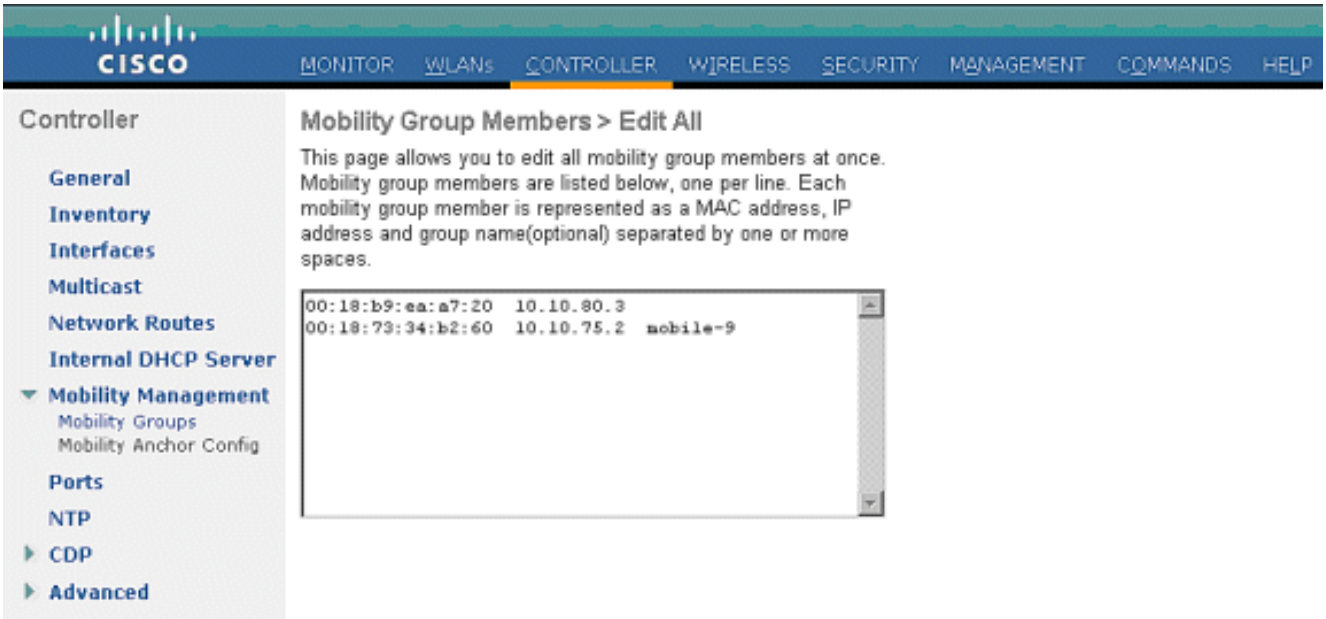
Accesso guest cablato con controller WLAN di ancoraggio

Nell'esempio, l'indirizzo IP del controller LAN wireless remoto è 10.10.80.3 e l'indirizzo IP del controller DMZ di ancoraggio è 10.10.75.2. Entrambi fanno parte di due diversi gruppi di mobilità.

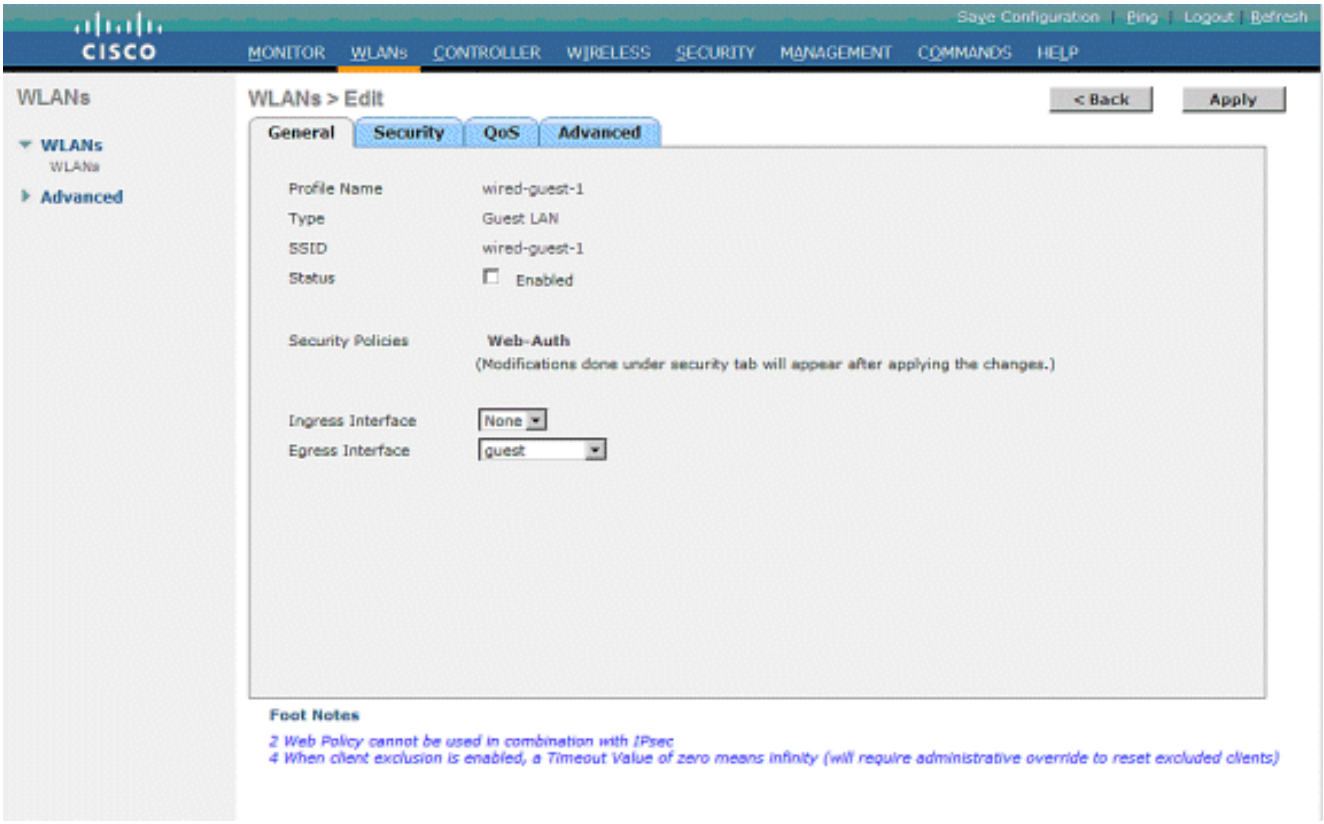
1. Configurare il gruppo di mobilità del controller Anchor DMZ quando si aggiungono l'indirizzo MAC, l'indirizzo IP e il nome del gruppo di mobilità del controller remoto.



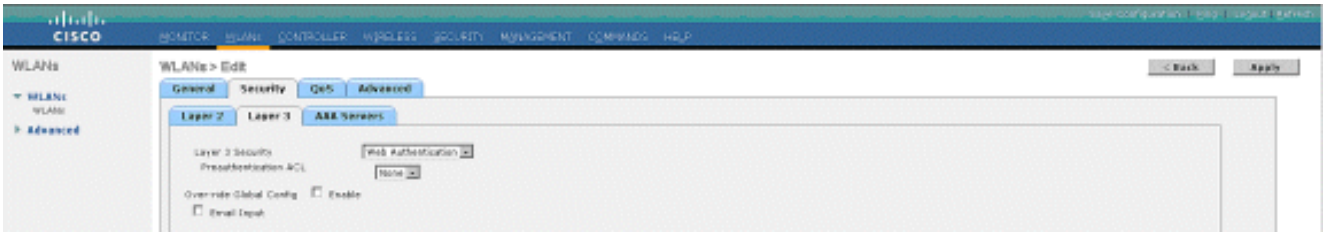
2. Analogamente, configurare il gruppo di mobilità nel telecomando.



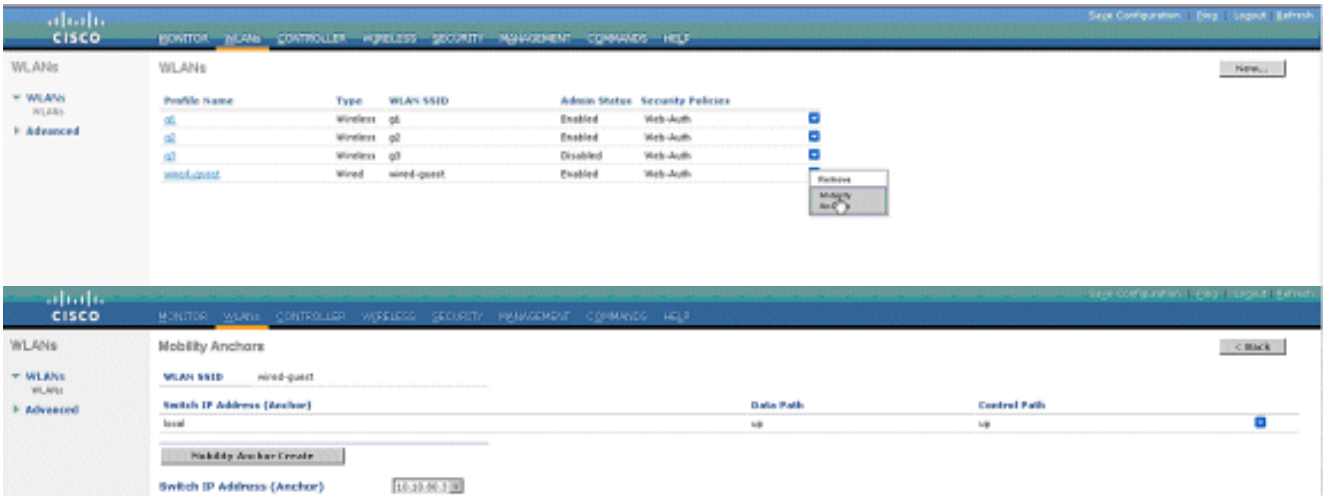
3. Creare la WLAN cablata con il nome esatto nel WLC di ancoraggio. In questo caso, l'interfaccia in entrata è "none" perché, logicamente, è il tunnel EoIP del telecomando. L'interfaccia in uscita è diversa e i client cablati ricevono l'indirizzo IP. In questo esempio viene creata un'interfaccia dinamica denominata *guest*. Tuttavia, in questa fase non è possibile abilitare la WLAN perché visualizza un messaggio di errore che indica che l'interfaccia in entrata non può essere *nessuna*.



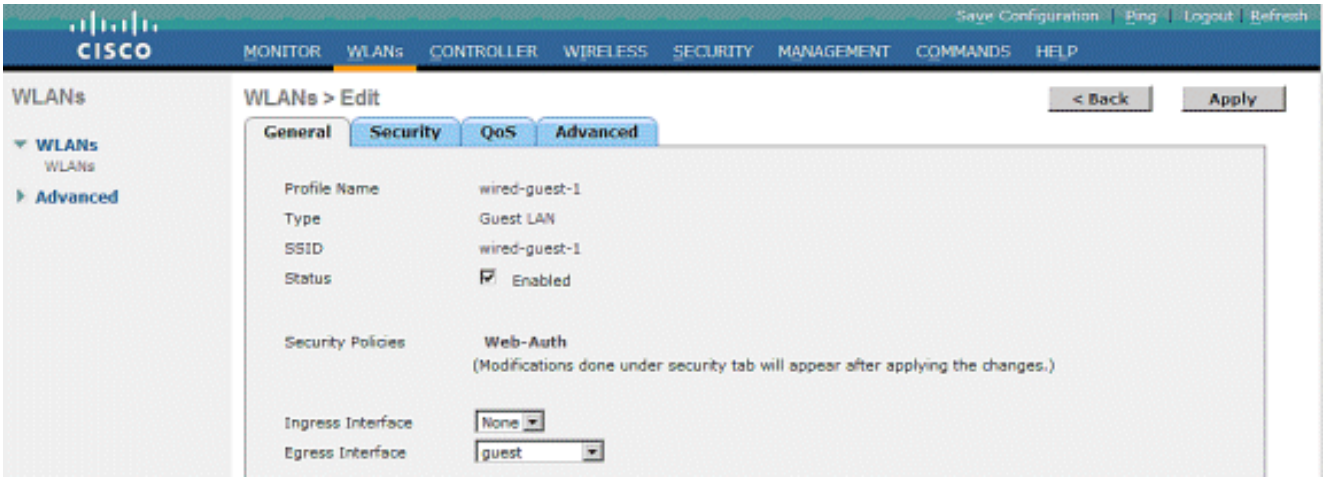
4. Configurare la sicurezza di layer 3 come *autenticazione Web*, in modo simile al controller remoto.



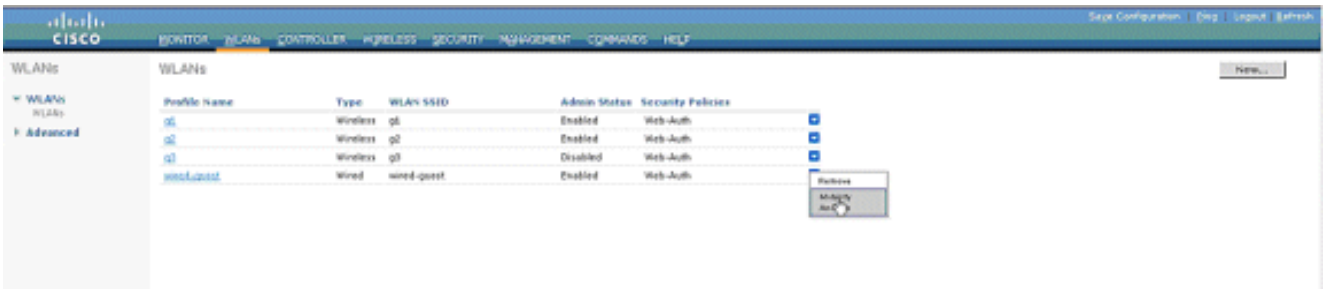
5. Creare l'ancora di mobilità sul controller di ancoraggio e mapparla a se stessa.



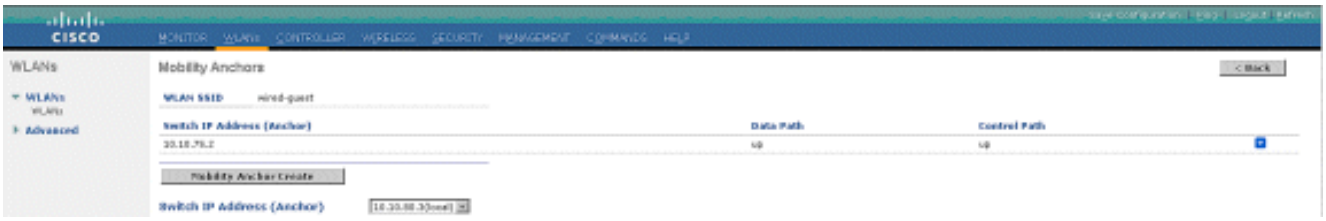
6. Dopo aver creato l'ancora per la mobilità, tornare indietro e abilitare la WLAN cablata.



7. Analogamente, creare l'ancora di mobilità sul WLC remoto per la WLAN guest cablata.



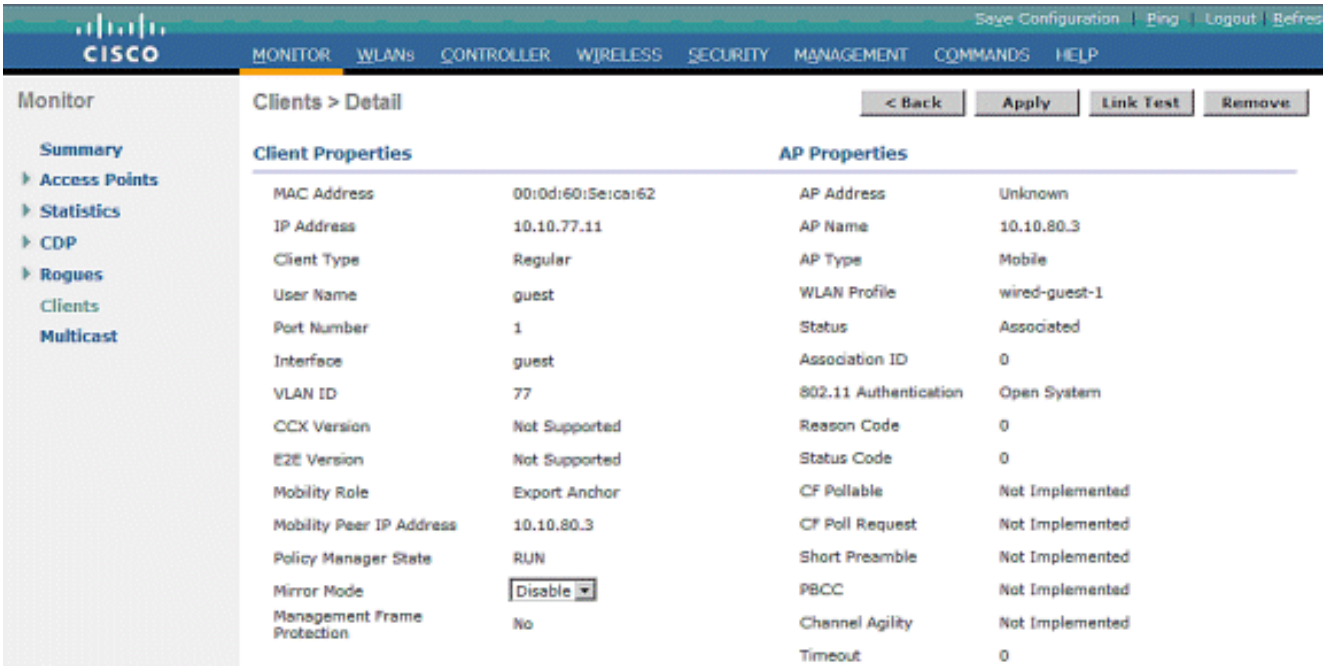
Scegliere l'indirizzo IP del WLC di ancoraggio e creare l'ancoraggio di mobilità.



Verificare che i dati e il percorso di controllo siano attivi. In caso contrario, verificare che queste porte siano aperte tra l'ancora e il controller LAN wireless remoto: UDP 1666 o IP 97.

8. Una volta che un utente guest con cavo è connesso allo switch e ha completato l'autenticazione Web, lo stato di Policy Manager deve essere ESEGUITA e il ruolo di mobilità è Esporta
esterno.

Analogamente, verificare lo stato nel WLC di ancoraggio. Lo stato di Policy Manager deve essere RUN e il ruolo di mobilità è Export
Anchor.

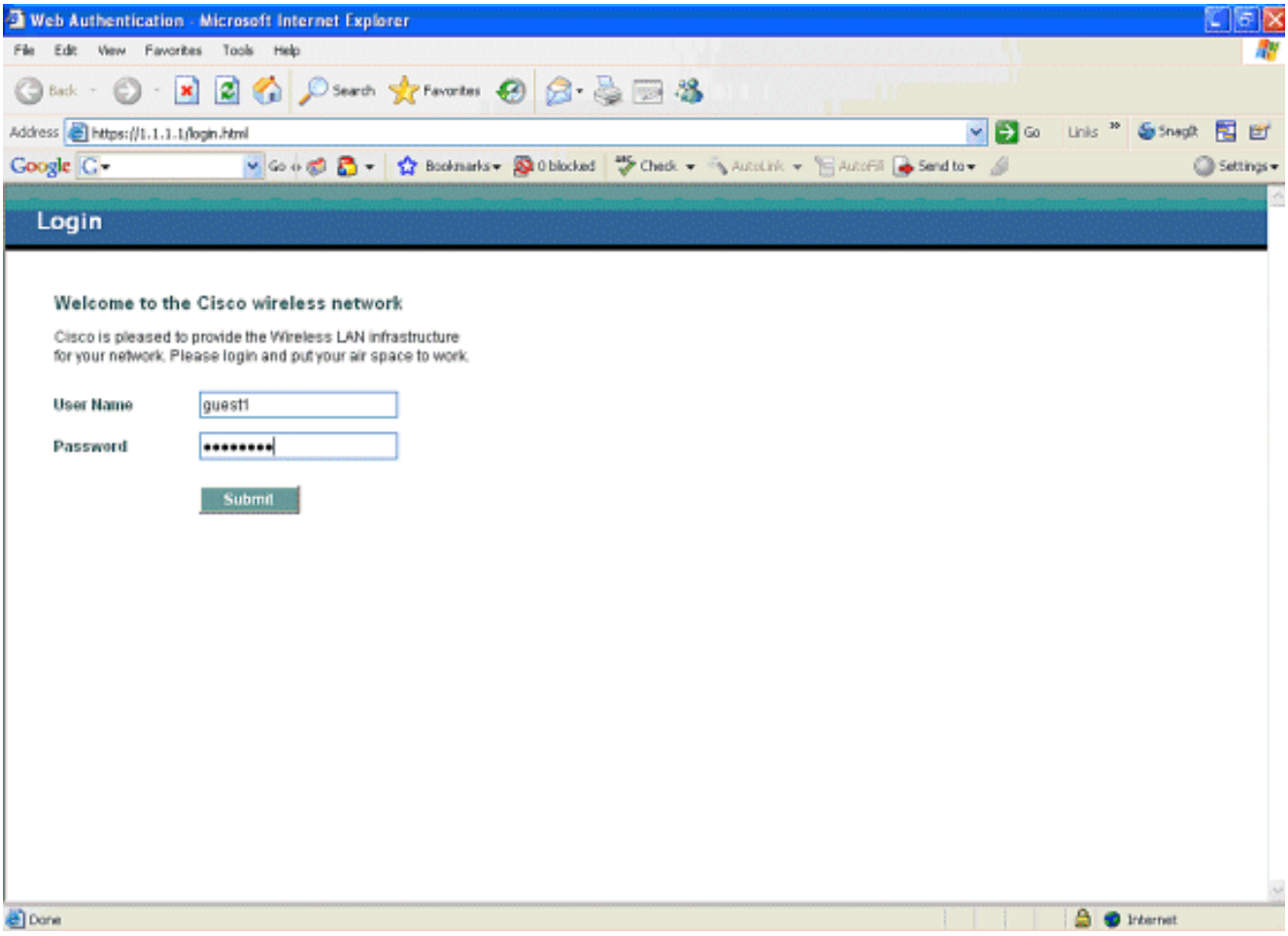


Configurazione client guest cablato

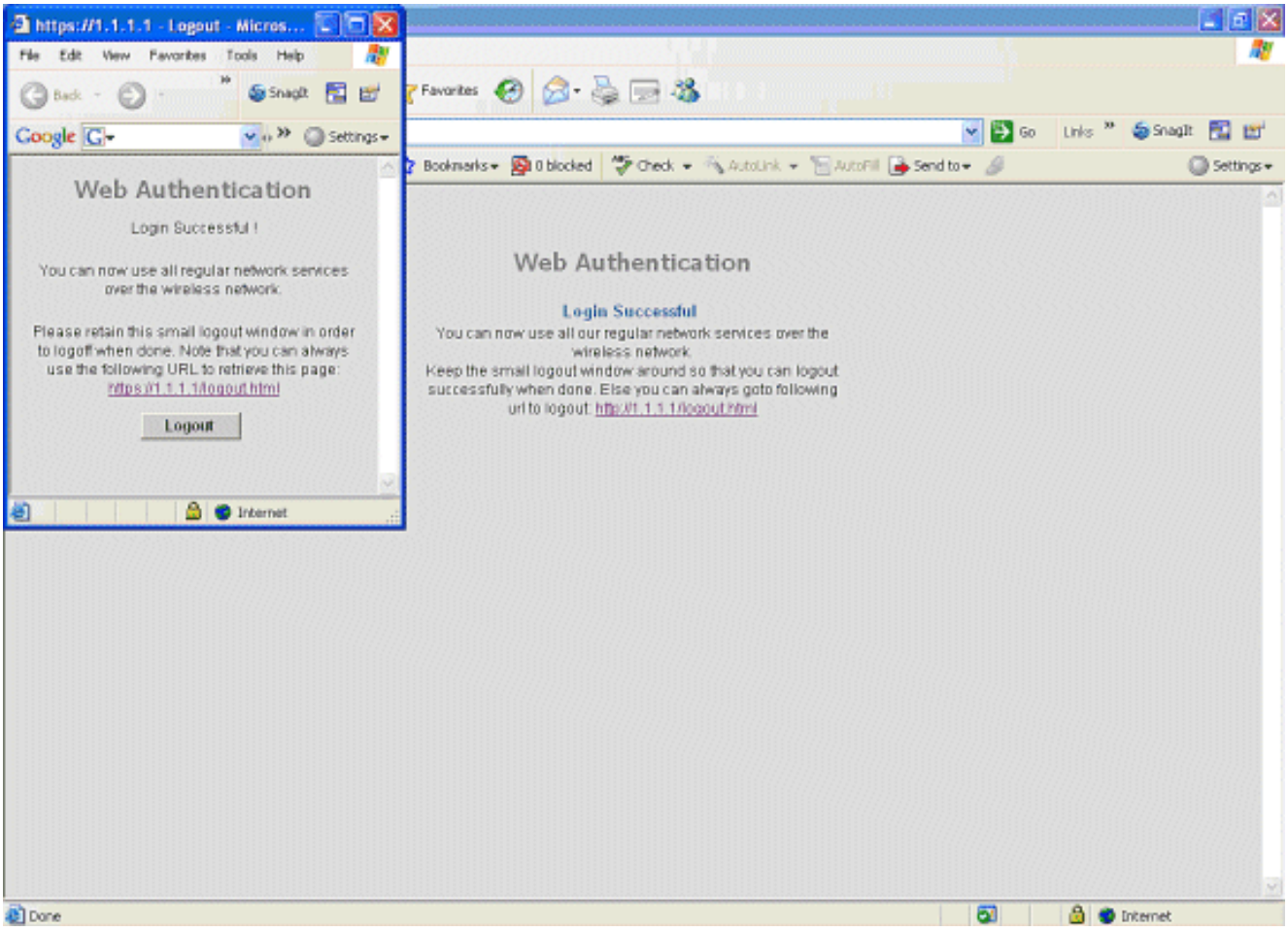
Il client guest cablato riceve un indirizzo IP dalla VLAN in uscita, ma non può passare alcun traffico finché non completa il processo di autenticazione Web.

Per accedere come utente guest, eseguire la procedura seguente:

1. Aprire una finestra del browser e immettere il nome URL desiderato (ad esempio, www.cisco.com). Il guest viene reindirizzato alla pagina Web predefinita del controller LAN wireless se l'autenticazione Web è abilitata ed è possibile completare una risoluzione DNS per l'URL immesso. In caso contrario, immettere l'URL seguente: https://1.1.1.1/login.html, dove l'indirizzo IP 1.1.1.1 è l'indirizzo IP virtuale del controller LAN
wireless.



2. Immettere il nome utente e la password forniti.
3. Se l'accesso ha esito positivo, viene visualizzata una finestra del browser.



Debug della connessione guest cablata sul WLC locale

Questo debug fornisce tutte le informazioni correlate al client guest cablato.

debug client

```
 Cisco Controller) >show debug
MAC address ............................... 00:0d:60:5e:ca:62
Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.

 (Cisco Controller) >Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Adding mobile on Wired Guest 00:00:00:00:00:00(0)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfHandleWiredGuestMobileStation
  (apf_wired_guest.c:121) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:
00:00:00 from Idle to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Initializing policy
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 START (0)
   Change state to AUTHCHECK (2) last state AUTHCHECK (2)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 AUTHCHECK (2)
   Change state to L2AUTHCOMPLETE (4) last state L2AUTHCOMPLETE (4)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 0.0.0.0 L2AUTHCOMPLETE (4)
   Change state to DHCP_REQD (7) last state DHCP_REQD (7)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   apfPemAddUser2 (apf_policy.c:209) Changing state for mobile
   00:0d:60:5e:ca:62 on AP 00:00:00:00:00:00 from Associated to Associated
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62 Session Timeout is 0 -
   not starting session timer for the mobile
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Stopping deletion of Mobile Station: (callerId: 48)
Tue Sep 11 13:27:42 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 10.10.80.252 on mobile
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Orphan Packet from 10.10.80.252
Tue Sep 11 13:27:43 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) State Update from Mobility-Incomplete
   to Mobility-Complete, mobility role=Local
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) pemAdvanceState2 3934, Adding TMP rule
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0
   DHCP_REQD (7) Adding Fast Path rule
type = Airespace AP - Learn IP address on AP 00:00:00:00:00:00,
```

```
   slot 0, interface = 1, QOS = 0 ACL Id = 255,
   Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62 0.0.0.0 DHCP_REQD
   (7) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Installing Orphan Pkt IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Unsuccessfully installed IP address 169.254.20.157 for station
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   0.0.0.0 Added NPU entry of type 9
Tue Sep 11 13:27:44 2007: 00:0d:60:5e:ca:62
   Sent an XID frame
Tue Sep 11 13:27:45 2007: 00:0d:60:5e:ca:62
   Wired Guest packet from 169.254.20.157 on mobile
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   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
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip:10.10.80.252
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP ARPing for 10.10.110.1 (SPA 10.10.110.2, vlanId 110)
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2
   VLAN: 110
Tue Sep 11 13:27:48 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 310, port 1, encap 0xec00)

Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP DISCOVER (1)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
```

```
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.80.252
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1 (len 350, port 1, vlan 110)
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:51 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 - NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP setting server from OFFER
   (server 10.10.110.1, yiaddr 10.10.110.3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP OFFER (2)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561), secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1  rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREQUEST (1) (len 334, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 1 - control block settings:
dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2  VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 1 - 10.10.110.1(local address 10.10.110.2,
   gateway 10.10.110.1, VLAN 110, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP REQUEST (3)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREQUEST, htype: Ethernet, hlen: 6, hops: 1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 36957, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0,  yiaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0,  giaddr: 10.10.110.2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   requested ip: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 10.10.110.1  rcvd server id: 1.1.1.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REQUEST to 10.10.110.1(len 374, port 1, vlan 110)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selecting relay 2 - control block settings:
```

dhcpServer: 10.10.110.1, dhcpNetmask: 0.0.0.0,
dhcpGateway: 0.0.0.0, dhcpRelay: 10.10.110.2 VLAN: 110
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP selected relay 2 -NONE
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP received op BOOTREPLY (2) (len 308, port 1, encap 0xec00)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 DHCP_REQD (7) Change state to WEBAUTH_REQD
   (8) last state WEBAUTH_REQD (8)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) pemAdvanceState2
   4598, Adding TMP rule
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Successfully
   plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Plumbing web-auth redirect rule due to user logout
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Adding Web RuleID 31 for mobile 00:0d:60:5e:ca:62
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   Assigning Address 10.10.110.3 to mobile
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP sending REPLY to Wired Client (len 350, port 1)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP transmitting DHCP ACK (5)
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   op: BOOTREPLY, htype: Ethernet, hlen: 6, hops: 0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   xid: 0x87214d01 (2267106561),secs: 0, flags: 8000
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   chaddr: 00:0d:60:5e:ca:62

Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   ciaddr: 0.0.0.0, yiaddr: 10.10.110.3
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   siaddr: 0.0.0.0, giaddr: 0.0.0.0
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   DHCP   server id: 1.1.1.1 rcvd server id: 10.10.110.1
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62
   10.10.110.3 Added NPU entry of type 2
Tue Sep 11 13:27:54 2007: 00:0d:60:5e:ca:62 Sent an XID frame
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Username entry (guest1) created for mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Setting guest session timeout for mobile
   00:0d:60:5e:ca:62 to 79953 seconds
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   Session Timeout is 79953 – starting session timer for the mobile
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_REQD (8) Change state to
   WEBAUTH_NOL3SEC (14) last state WEBAUTH_NOL3SEC (14)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62
   10.10.110.3 WEBAUTH_NOL3SEC (14) **Change state to RUN**
   (20) last state RUN (20)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Reached PLUMBFA STPATH: from line 4518
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Replacing FastPath rule
type = Airespace AP Client

```
on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
ACL Id = 255, Jumbo Frames = NO, 802.1P = 0, DSCP = 0, TokenID = 5006
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3 RUN
   (20) Successfully plumbed mobile rule (ACL ID 255)
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 10.10.110.3
   Added NPU entry of type 1
Tue Sep 11 13:28:12 2007: 00:0d:60:5e:ca:62 Sending a gratuitous
   ARP for 10.10.110.3, VLAN Id 110
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Configurazione della mobilità di ancoraggio automatico
- Esempio di configurazione di WLC, WLAN guest e WLAN interna
- Esempio di configurazione dell'autenticazione Web esterna con i controller LAN wireless
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.2
- Supporto dei prodotti wireless
- Documentazione e supporto tecnico – Cisco Systems