Esempio di configurazione di Ethernet Bridging nella rete Mesh wireless point-point

Sommario

Introduzione

Questo documento offre un semplice esempio di configurazione per configurare il bridging Ethernet su una rete mesh wireless esterna. Questo documento spiega il bridging Ethernet point-to-point tra i punti di accesso mesh wireless (AP) esterni.

Prerequisiti

- Il controller WLC è configurato per le operazioni di base.
- Il WLC è configurato nella modalità layer 3.
- Lo switch per il WLC è configurato.

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC

- Conoscenze base della soluzione di rete mesh wireless
- Conoscenze base di LWAPP (Lightweight AP Protocol)
- Conoscenze base di configurazione di switch Cisco

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2000 WLC con firmware 4.0.217.0
- Due (2) Cisco Aironet serie 1510 LAP
- Cisco Layer 2 Switch

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.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

La soluzione di rete mesh, che fa parte della soluzione di rete wireless unificata Cisco, consente a due o più punti di accesso mesh leggeri Cisco Aironet (di seguito denominati punti di accesso mesh) di comunicare tra loro su uno o più hop wireless di collegarsi a più LAN o di estendere la copertura wireless 802.11b. I punti di accesso mesh Cisco sono configurati, monitorati e gestiti da e tramite qualsiasi controller LAN wireless Cisco implementato nella soluzione di rete mesh.

Le installazioni di soluzioni di rete mesh supportate sono di tre tipi generali:

- Installazione point-to-point
- Installazione point-to-multipoint
- Distribuzione mesh

In questo documento viene illustrato come configurare in modo analogo l'implementazione di mesh point-to-point e il bridging Ethernet. Nell'implementazione delle reti mesh point-to-point, i punti di accesso mesh forniscono l'accesso wireless e il backhaul ai client wireless e possono supportare contemporaneamente il bridging tra una LAN e una terminazione a un dispositivo Ethernet remoto o a un'altra LAN Ethernet.

Per informazioni dettagliate su ciascuno di questi tipi di distribuzione, fare riferimento a Implementazioni di soluzioni di rete Mesh.

Cisco Aironet serie 1510 lightweight outdoor mesh AP è un dispositivo wireless progettato per l'accesso wireless dei client e il bridging point-to-point, il bridging point-to-multipoint e la connettività wireless mesh point-to-multipoint. Il punto di accesso esterno è un'unità indipendente che può essere montata su una parete o sporgenza, su un palo sul tetto o su un palo della luce stradale.

Èpossibile utilizzare i Cisco Aironet 1510 remote edge lightweight access point e i Cisco Aironet serie 1500 lightweight outdoor access point in uno dei seguenti ruoli:

- Access point dal tetto (RAP)
- Mesh Access Point (MAP), detto anche Pole-top Access Point (PAP)

I RAP sono dotati di una connessione cablata a un controller LAN wireless Cisco. Usano l'interfaccia wireless backhaul per comunicare con le MAP vicine. I RAP sono il nodo padre di qualsiasi rete a bridge o mesh e collegano un bridge o una rete mesh alla rete cablata, quindi può esistere un solo RAP per ogni segmento di rete a bridge o mesh.

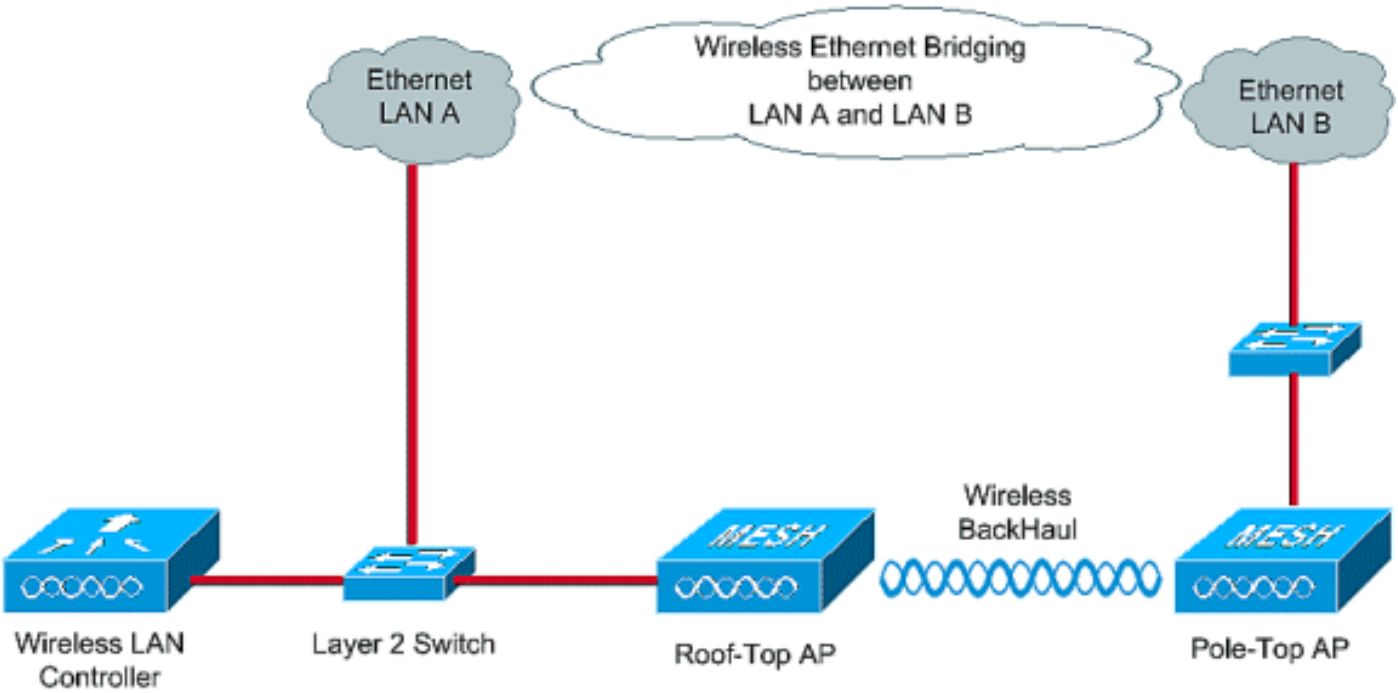
Le mappe non dispongono di connessioni cablate a un controller LAN wireless Cisco. Possono essere completamente wireless e supportare client che comunicano con altre mappe o RAP, oppure possono essere utilizzati per connettersi a periferiche o reti cablate. La porta Ethernet è disabilitata per impostazione predefinita per motivi di sicurezza, ma è possibile abilitarla per i PAP.

Configurazione

Nell'esempio di configurazione viene spiegato come configurare il bridging Ethernet tra due access point Mesh serie 1510 lightweight per ambienti esterni con un access point che funziona come RAP e l'altro come MAP.

In questa configurazione, l'access point con indirizzo MAC 00:0B:85:7F:47:00 è configurato come RAP e l'access point con indirizzo MAC 00:0B:85:71:1B:00 è configurato come MAP. Una LAN Ethernet locale A è connessa all'estremità RAP, mentre una LAN Ethernet B è connessa all'estremità MAP.

Esempio di rete



Per configurare i 1510 mesh AP integrati per il bridging Ethernet, attenersi alla seguente procedura:

1. Assegnazione dell'indirizzo IP agli access point

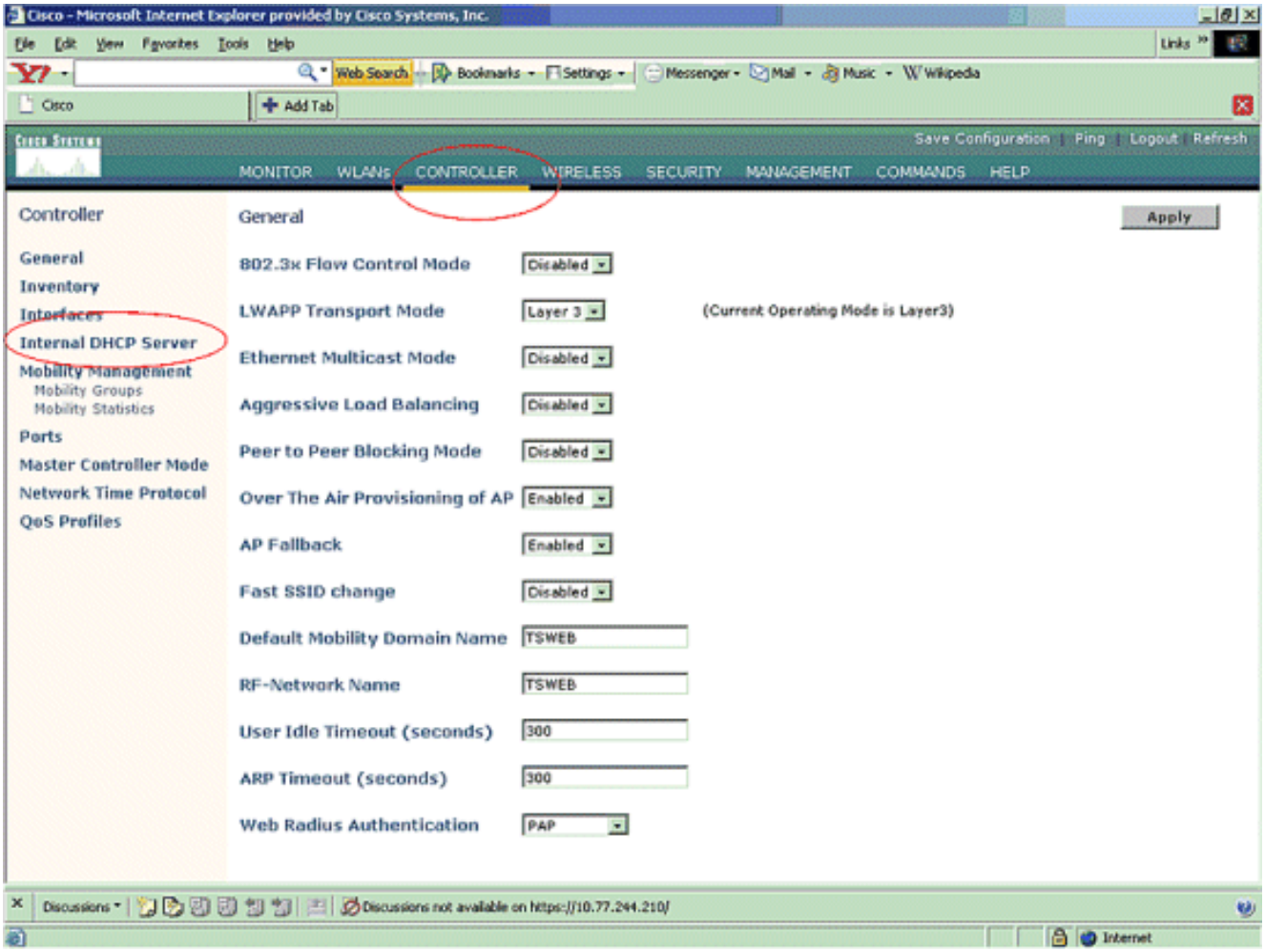
2. Aggiungere l'indirizzo MAC degli access point all'elenco dei filtri MAC del WLC
3. Registrare gli AP con il WLC
4. Configurare il ruolo PA e altri parametri di bridging
5. Abilitare Ethernet Bridging sui punti di accesso
6. Abilitare la configurazione zero-touch sul WLC

Assegnazione dell'indirizzo IP agli access point

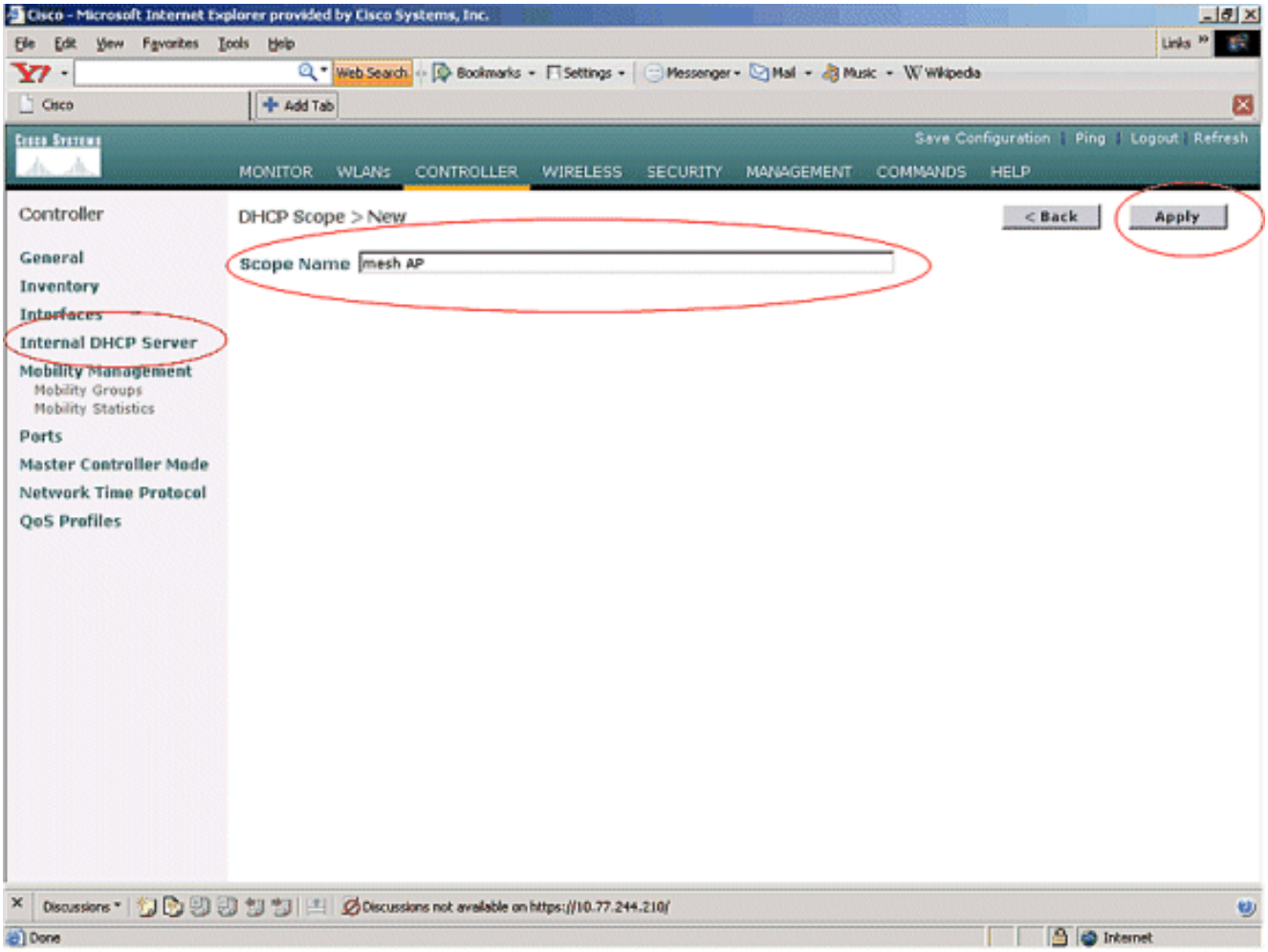
All'avvio, un access point cerca prima un indirizzo IP. Questo indirizzo IP può essere assegnato dinamicamente con un server DHCP interno esterno come Microsoft Windows®. La versione più recente del WLC (4.0 e successive) può assegnare l'indirizzo IP agli access point con il server DHCP interno sul controller stesso. In questo esempio viene utilizzato il server DHCP interno sul controller per assegnare l'indirizzo IP ai punti di accesso.

Completare questa procedura per assegnare un indirizzo IP agli access point tramite il server DHCP interno sul WLC.

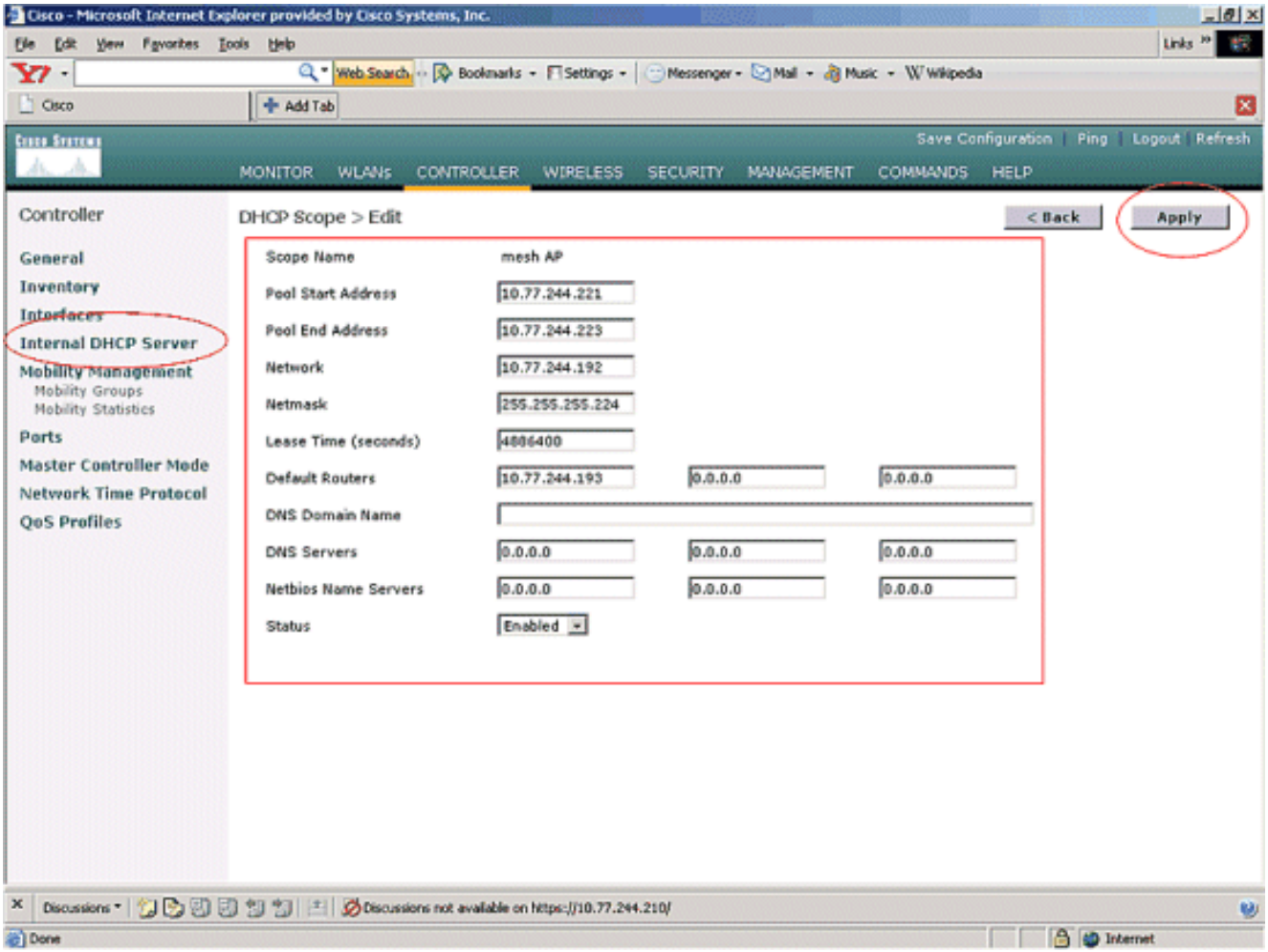
1. Fare clic su **CONTROLLER** dal menu principale dell'interfaccia utente del WLC. Selezionare **Internal DHCP Server** (Server DHCP interno) dall'angolo sinistro della pagina principale del controller.



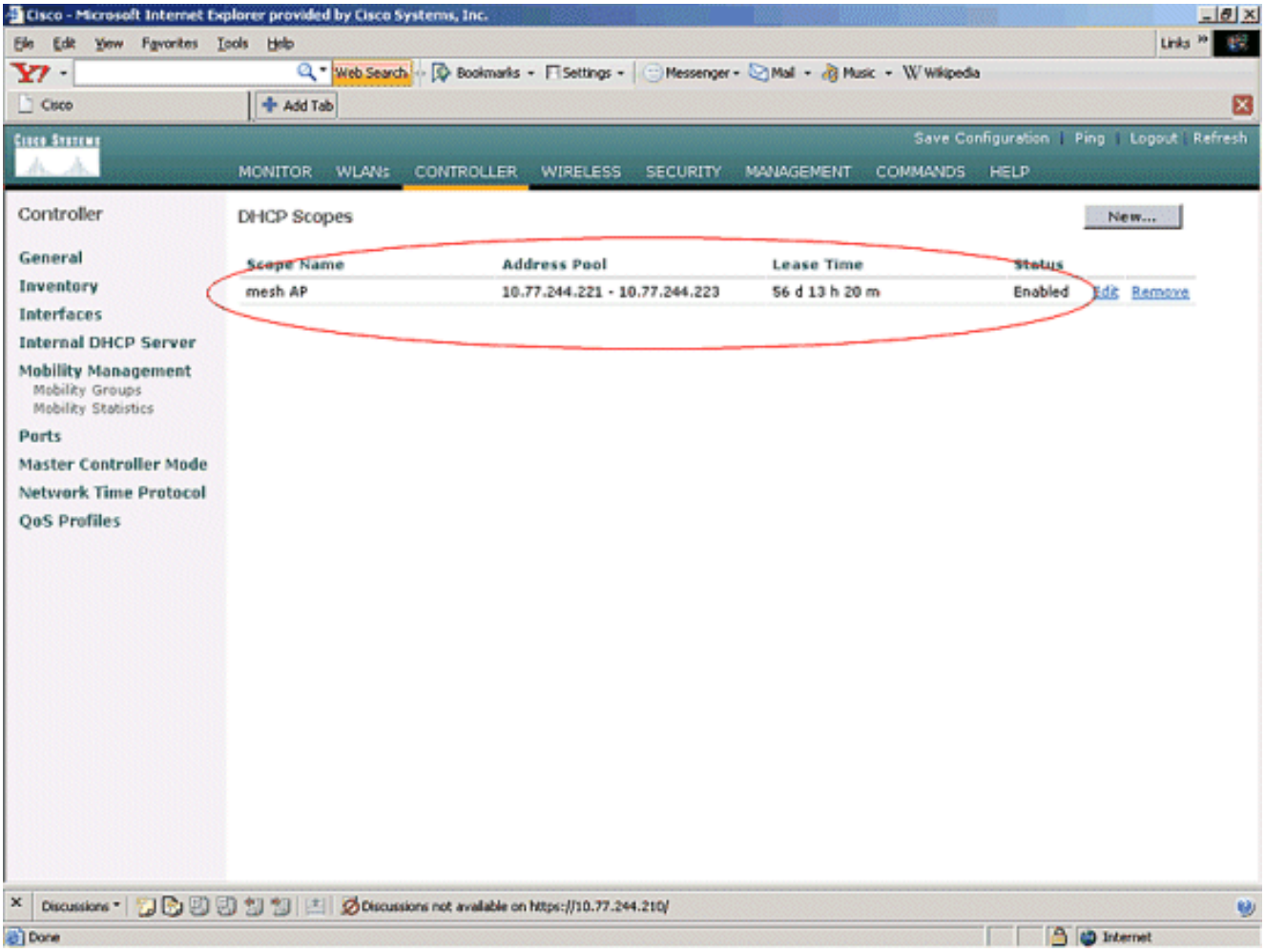
2. Nella pagina **Server DHCP interno**, **fare clic su Nuovo** per creare un nuovo ambito DHCP. In questo esempio il nome dell'ambito viene assegnato come **mesh AP**. Fare clic su **Apply** (Applica). Viene visualizzata la pagina di modifica dell'ambito DHCP del punto di accesso mesh.



3. Nella pagina **DHCP > Ambito di modifica**, configurare l'indirizzo di avvio del pool, l'indirizzo di fine del pool, la rete e la maschera di rete, i router predefiniti e tutti gli altri parametri necessari, come mostrato nell'esempio. Selezionare lo stato del server DHCP come **Abilitato** dall'elenco a discesa **Status** (Stato). Fare clic su **Apply**
(Applica).



4. A questo punto, il server DHCP interno è configurato in modo da assegnare gli indirizzi IP ai punti di accesso
   mesh.



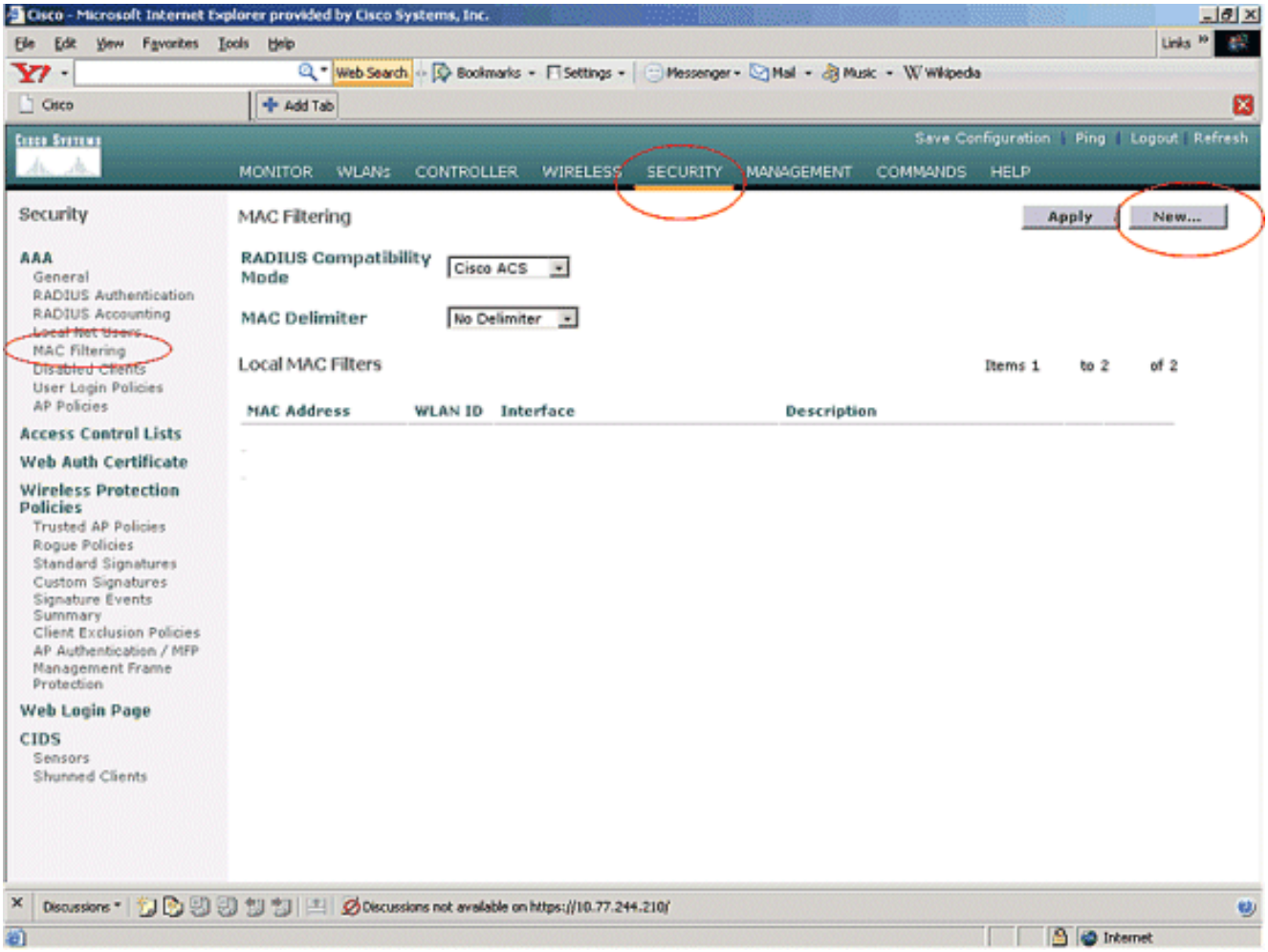
5. Una volta registrati gli access point sul controller, assegnarne l'indirizzo IP statico tramite l'interfaccia utente del controller. Se si assegnano indirizzi IP statici ai punti di accesso mesh, la convergenza dei punti di accesso risulterà più rapida alla successiva registrazione con il controller.

Aggiungere l'indirizzo MAC degli access point all'elenco dei filtri MAC del WLC

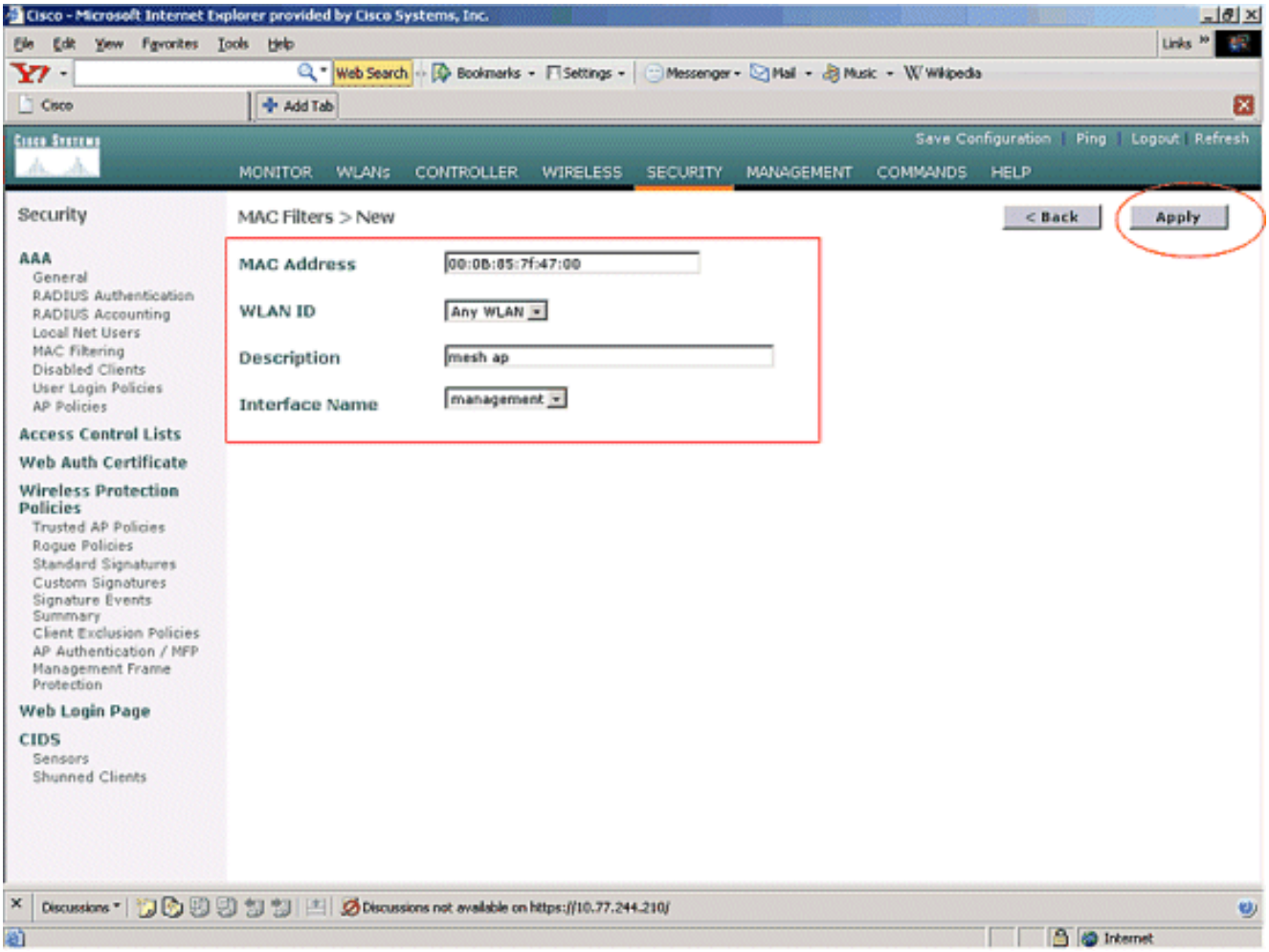
Per registrare gli AP mesh sul WLC, occorre prima aggiungere l'indirizzo MAC degli AP all'elenco dei filtri MAC sul WLC. L'indirizzo MAC è indicato sul lato superiore della mesh AP.

Completare questa procedura per aggiungere l'AP all'elenco di filtro MAC del WLC.

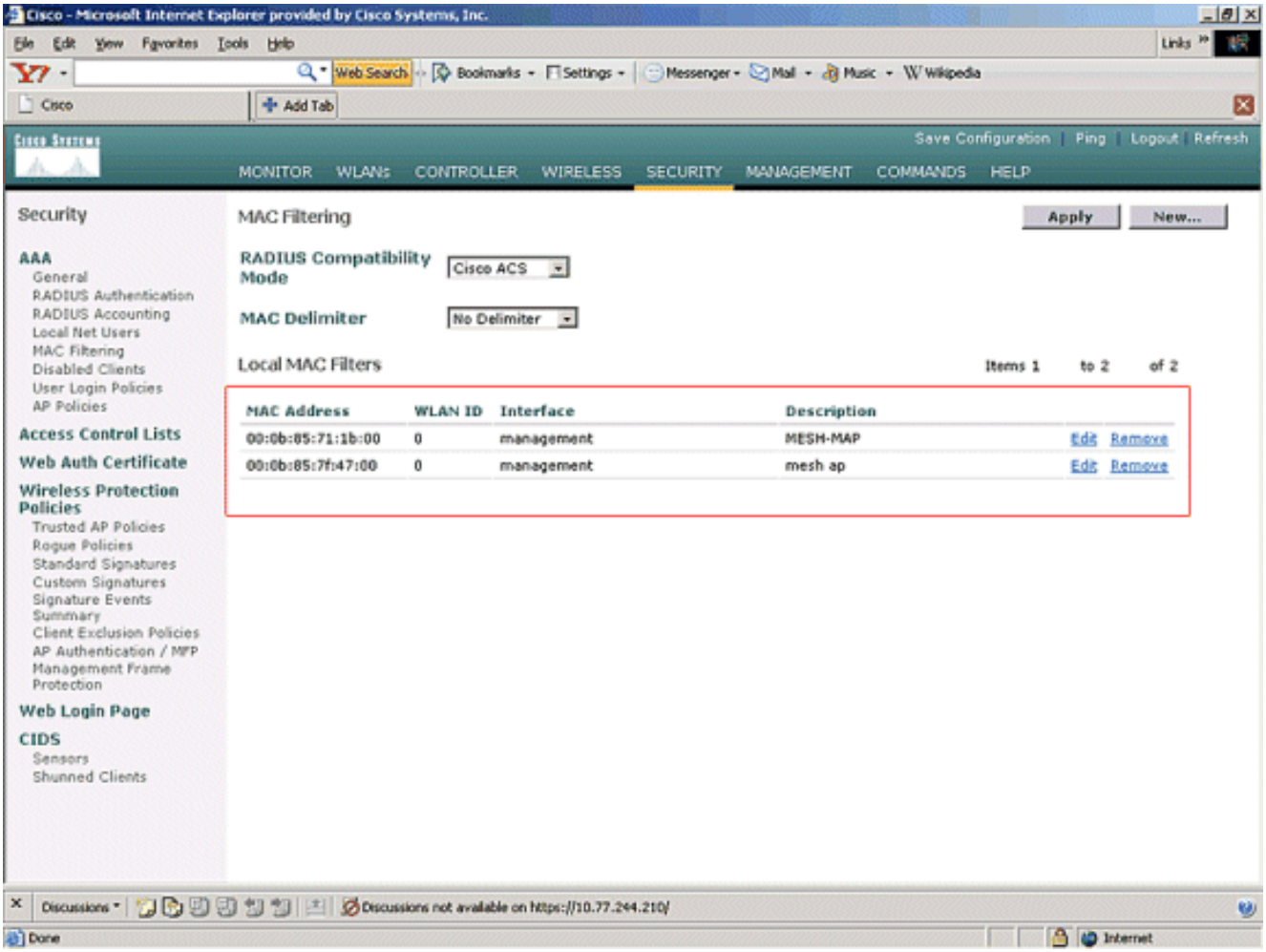
1. Fare clic su **SECURITY** (SICUREZZA) dal menu principale del controller.Nella pagina Sicurezza, scegliere **Filtro MAC** nella sezione **AAA**. Viene visualizzata la pagina Filtro MAC. Per creare i filtri MAC per gli access point con rete, fare clic su **New** (Nuovo).



2. Immettere l'**indirizzo MAC** dell'access point e la relativa **descrizione** nelle caselle di testo appropriate, come mostrato nell'esempio. Inoltre, selezionare un'interfaccia **WLAN** e un'**interfaccia dinamica** rispettivamente dai menu a discesa ID WLAN e Nome interfaccia. Fare clic su **Apply**
(Applica).



3. Ripetere i passaggi 1 e 2 per tutti gli access point coinvolti in questa rete mesh, in modo che il filtro MAC sia configurato per consentire ai access point mesh di registrarsi con il controller.



Registrare l'access point con il WLC

Il passo successivo è registrare gli access point mesh con il WLC. Un access point può registrarsi sul WLC in diversi modi. Per ulteriori informazioni su come un access point si registra sul WLC, fare riferimento alla registrazione di un Lightweight AP con il WLC.

La prima volta che si usano gli access point con mesh, registrare tutti gli access point direttamente collegati al WLC.

Se non è stato possibile aggiungere l'AP all'elenco di filtro MAC del controller, gli AP non possono unirsi al WLC al momento della registrazione al WLC. La causa è un errore di autorizzazione dall'output del comando **debug lwapp events enable** sul controller. Di seguito è riportato l'output di esempio che indica un errore di autorizzazione.

```
(Cisco Controller) >debug lwapp events enable

.Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to 00:0b:85:33:52:80 on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Received LWAPP DISCOVERY REQUEST from
AP 00:0b:85:71:1b:00 to ff:ff:ff:ff:ff:ff on port '2'
Fri Oct 26 16:04:48 2007: 00:0b:85:71:1b:00 Successful transmission of LWAPP
Discovery-Response to AP 00:0b:85:71:1b:00 on Port 2
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 Received LWAPP JOIN REQUEST from AP
00:0b:85:71:1b:00 to 00:0b:85:33:52:81 on port '2'
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 AP ap:71:1b:00: txNonce  00:0B:85:33
```

```
:52:80 rxNonce  00:0B:85:71:1B:00
Fri Oct 26 15:52:40 2007: 00:0b:85:71:1b:00 LWAPP Join-Request MTU path from AP
00:0b:85:71:1b:00 is 1500, remote debug mode is 0
Fri Oct 26 15:52:40 2007: spamRadiusProcessResponse: AP Authorization failure for
00:0b:85:71:1b:00
```

In questo output, è possibile vedere che la richiesta di join dall'access point non è accettata dal controller a causa di un errore di autorizzazione dell'access point.

Nota: nelle normali distribuzioni di rete con mesh che usano principalmente access point serie 1500, si consiglia di disabilitare l'impostazione **Consenti autenticazione dei vecchi access point** sul controller. Questa operazione può essere eseguita dalla modalità CLI del controller con il comando

Nota: (Cisco Controller) **> config network allow-old-bridge-aps disable**

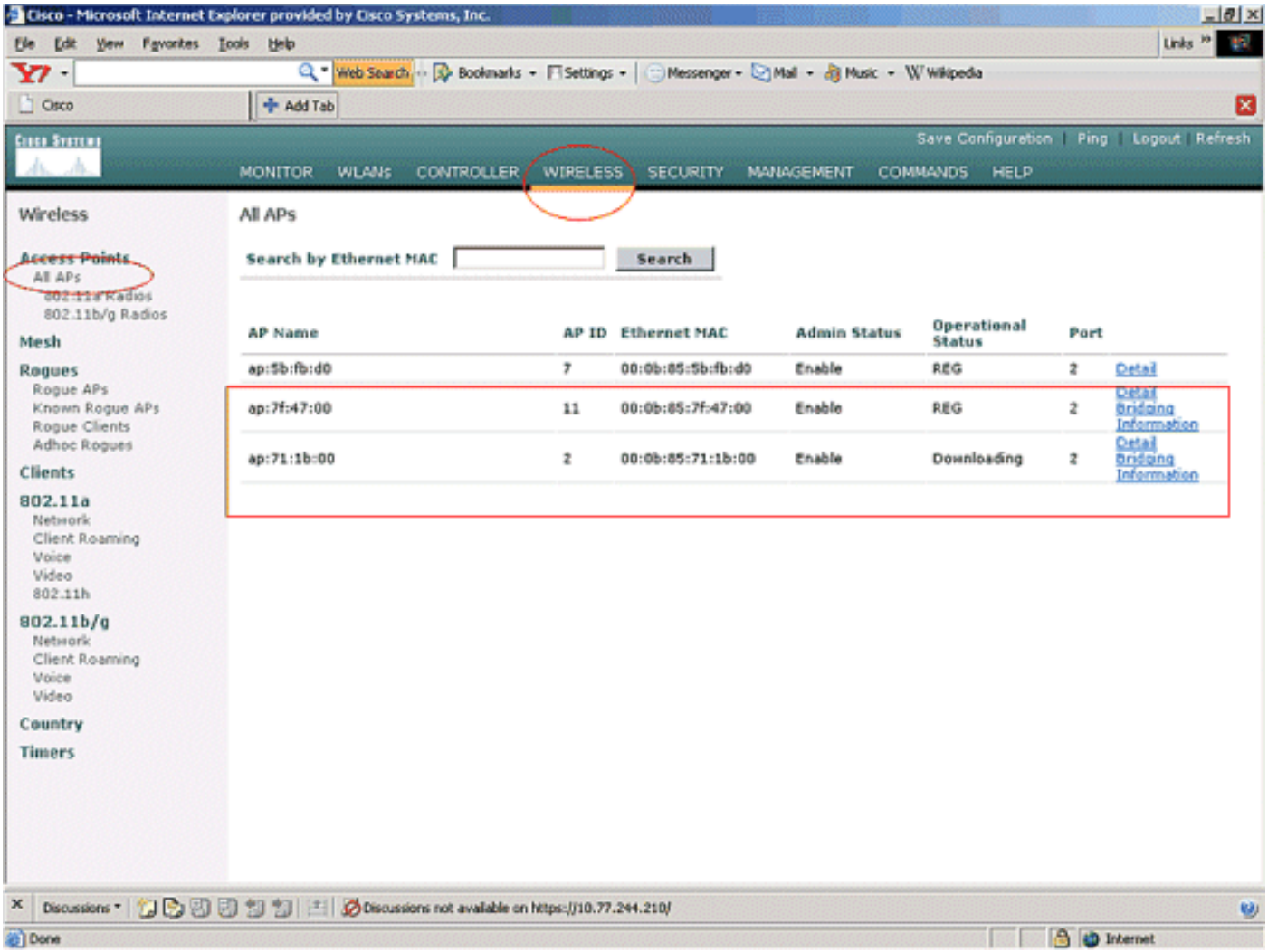
Nota: Il comando è stato rimosso nella versione 4.1 e successive, quindi non si tratta di un problema di WLC 4.1 e versioni successive.

Dalla CLI, è possibile usare il comando **show ap summary** per verificare che gli AP siano registrati sul WLC:

(Cisco Controller) **>mostra riepilogo app**

```
AP Name             Slots  AP Model             Ethernet MAC       Location
     Port
------------------  -----  -------------------  -----------------  -------------
---
ap:5b:fb:d0          2     AP1010               00:0b:85:5b:fb:d0  default_locat
ion  2
ap:7f:47:00          2     LAP1510              00:0b:85:7f:47:00  default_locat
ion  2
ap:71:1b:00          2     LAP1510              00:0b:85:71:1b:00  default_locat
ion  2
```

Èpossibile verificarlo dalla GUI nella pagina Wireless **All AP**.

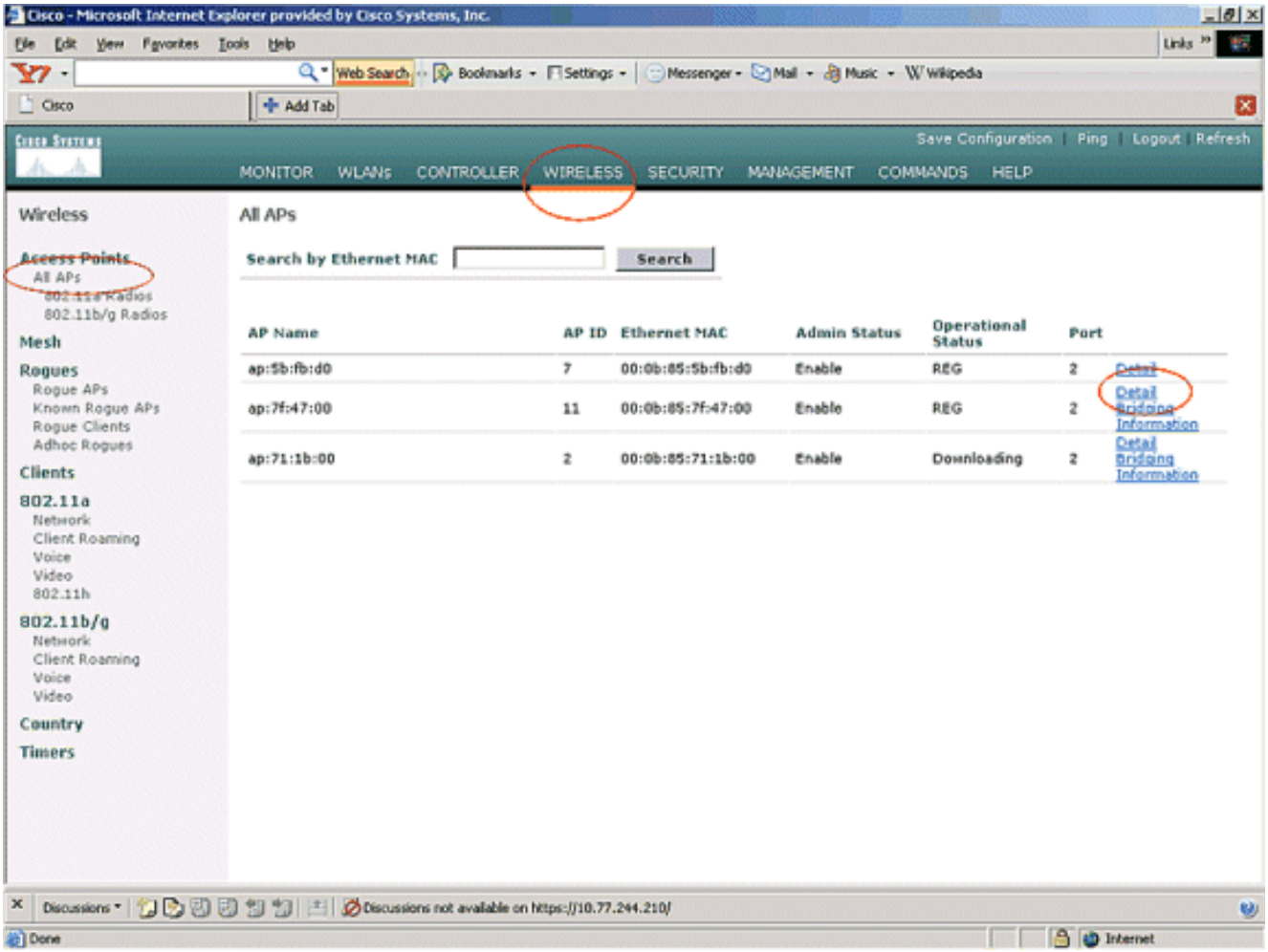


Configurare il ruolo PA e altri parametri di bridging

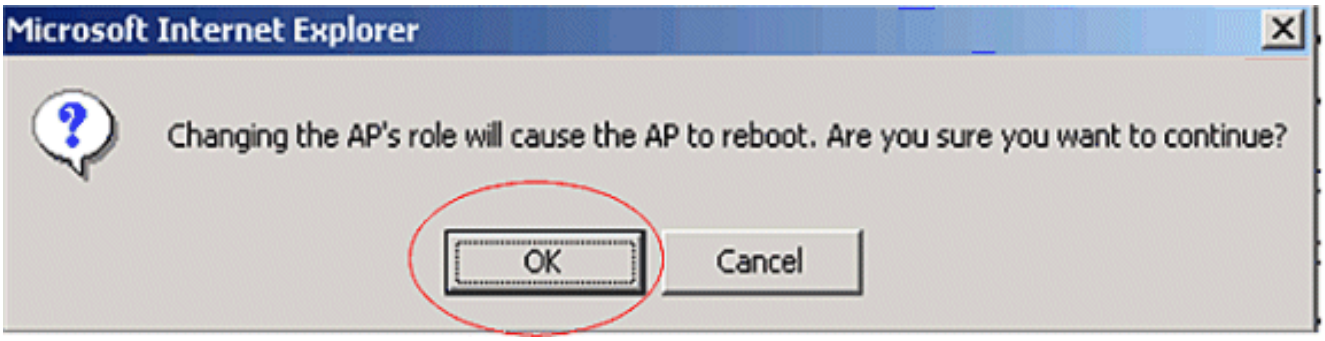
Una volta registrati gli AP sul WLC, è necessario configurare il ruolo AP e altri parametri di bridging. È necessario configurare i punti di accesso come punti di accesso e mappe, come richiesto.

Completare la procedura seguente per configurare i parametri AP:

1. Fare clic su **Wireless**, quindi su **Tutti gli access point** in **Access Point**. Viene visualizzata la pagina **Tutti gli access point**.
2. Per accedere alla pagina **Dettagli,** fare clic sul collegamento **Dettagli** del modello AP1510 in uso.



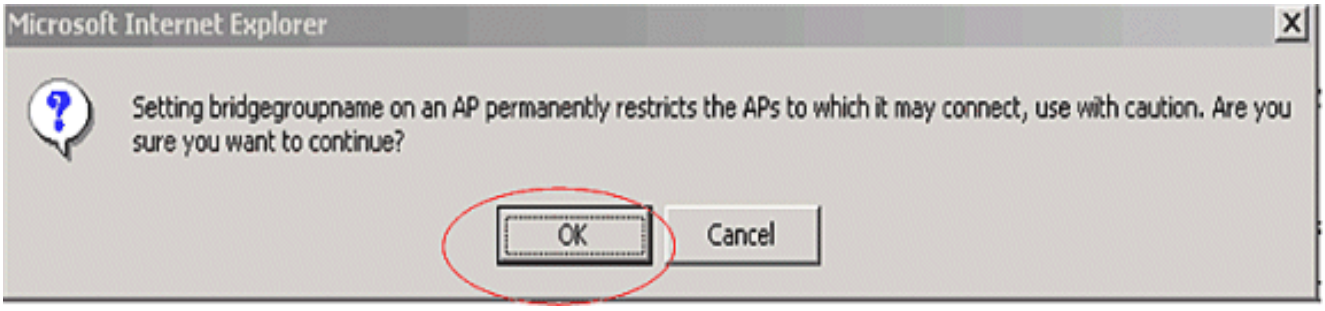
3. Nella pagina **Dettagli** del punto di accesso 1510, la **voce Modalità punto di accesso** in **Generale** viene impostata automaticamente su **Bridge** per i punti di accesso che dispongono di funzionalità di bridging, ad esempio AP1510. Questa pagina visualizza queste informazioni anche in Informazioni di bridging.In **Informazioni di bridging**, scegliere una delle seguenti opzioni per specificare il ruolo dell'access point nella rete mesh:MeshAP (MAP)RootAP (RAP)I punti di accesso configurati come RootAP devono avere una connessione cablata al WLC al momento dell'implementazione della configurazione nell'ambiente di produzione. L'access point configurato come mesh AP è connesso in modalità wireless al WLC tramite il relativo access point padre (RAP). Per impostazione predefinita, i 1510 AP assumono il ruolo di MAP quando vengono visualizzati e si registrano al WLC.Quando si configura il ruolo di bridge, viene visualizzata una finestra di avviso con questo messaggio: **AP verrà riavviato**. Fare clic su **OK** per
continuare.



Èpossibile configurare il ruolo AP con la CLI del controller e il ruolo **config ap** del comando .

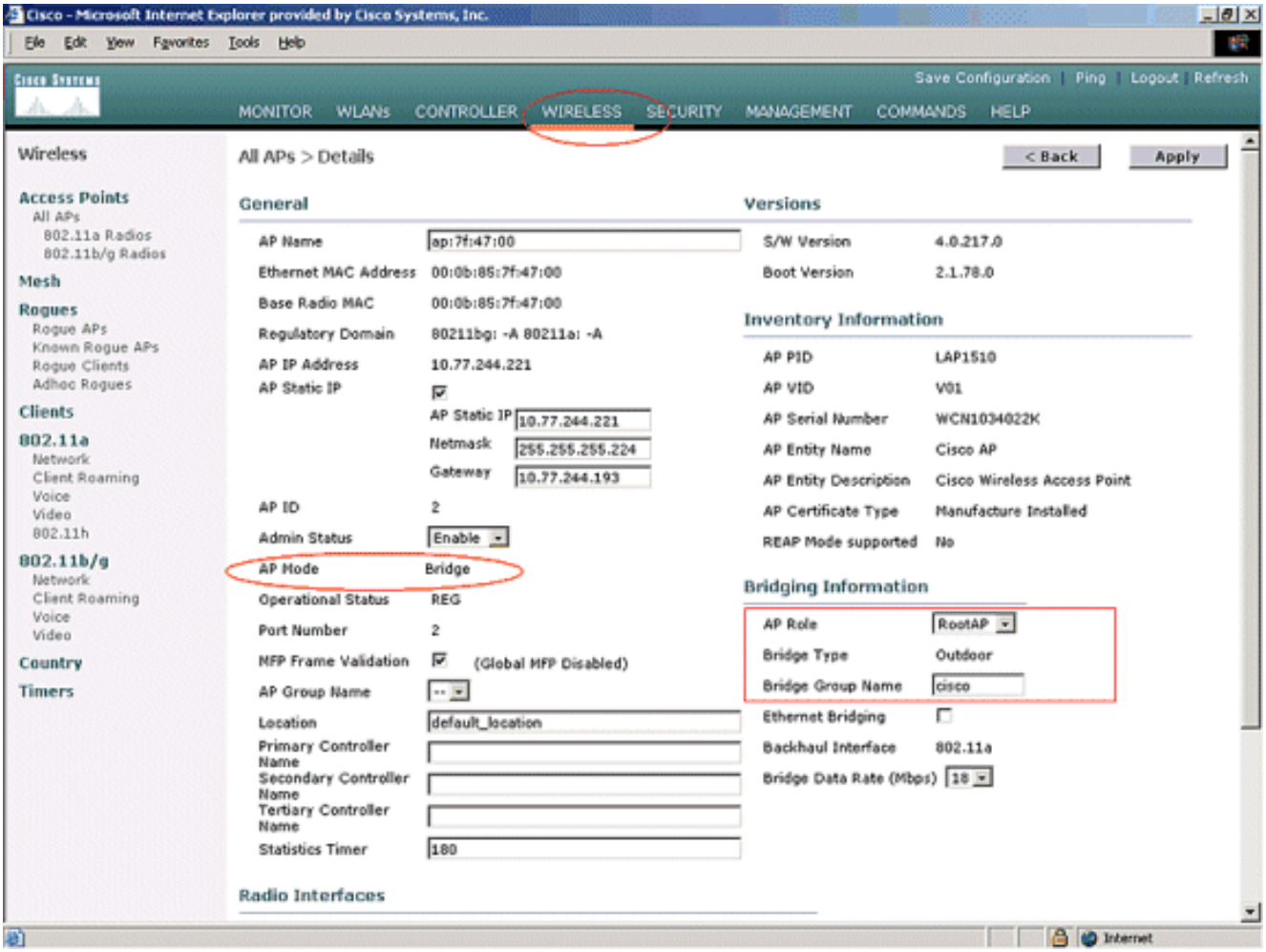
4. Configurare il parametro **Bridge Group Name**. Si tratta di una stringa di massimo 10 caratteri. Utilizzare i nomi dei gruppi di bridge per raggruppare logicamente i punti di accesso mesh in modo da evitare che due reti sullo stesso canale comunichino tra loro. **Affinché i punti di**

accesso mesh possano comunicare, devono avere lo stesso nome di gruppo di bridge. Nella fase di fabbricazione viene assegnato un nome di gruppo di bridge predefinito per i punti di accesso alla rete. Non è visibile a voi. Il campo Bridge Group Name (Nome gruppo bridge) appare vuoto nella GUI finché non viene modificato. L'access point si registra per la prima volta nel WLC con questo nome di gruppo di bridge predefinito.In questo esempio viene usato il nome del gruppo di bridge **cisco** su tutti gli access point coinvolti in questa rete mesh.Quando si configura il nome del gruppo di bridge, viene visualizzata una finestra di avviso: **L'impostazione del nome del gruppo di bridge limita in modo permanente il punto di accesso a cui può connettersi."** Fare clic su **OK** per continuare.



Èpossibile configurare il nome del gruppo bridge dalla CLI del controller con il comando **config ap nomedruppo di bridge impostato** in cisco.**Nota:** Se si desidera modificare il nome del gruppo di bridge degli access point dopo la distribuzione del criterio di autorizzazione delle risorse nel sito remoto, configurare il parametro Nome gruppo di bridge innanzitutto nel criterio di autorizzazione delle risorse e quindi nel criterio di autorizzazione delle risorse. Se il criterio di autorizzazione delle risorse viene configurato per primo, si verificheranno gravi problemi di connettività poiché il criterio di autorizzazione delle risorse viene impostato sulla modalità predefinita perché il relativo elemento padre è configurato con un nome di gruppo di bridge diverso.**Nota:** Per le configurazioni con più RAP, assicurarsi che tutti i RAP abbiano lo stesso nome di gruppo bridge per consentire il failover da un RAP all'altro. Al contrario, per le configurazioni in cui sono richiesti settori distinti, verificare che ogni punto di accesso al sistema e i punti di accesso al sistema associati abbiano nomi di gruppi di bridge distinti.

5. La **velocità di trasferimento dati** è la velocità con cui i dati vengono condivisi tra i punti di accesso mesh. Questo è fisso per un'intera rete. **La velocità dati predefinita è 18 Mbps, che è necessario utilizzare per il backhaul**. Le velocità dati valide per 802.11a sono 6, 9, 12, 18, 24, 36, 48 e 54.
6. Se si configura l'access point come RAP, il parametro **Backhaul Interface** visualizza un menu a discesa, ma se si fa clic sul pulsante a discesa viene visualizzata solo l'opzione 802.11a. **Sulla MAPPA non è disponibile un menu a discesa di questo tipo**. Fare clic su **Apply** (Applica). Ecco lo screenshot che spiega i punti da 3 a 6.



Di seguito è illustrata la configurazione di RootAP (RAP).

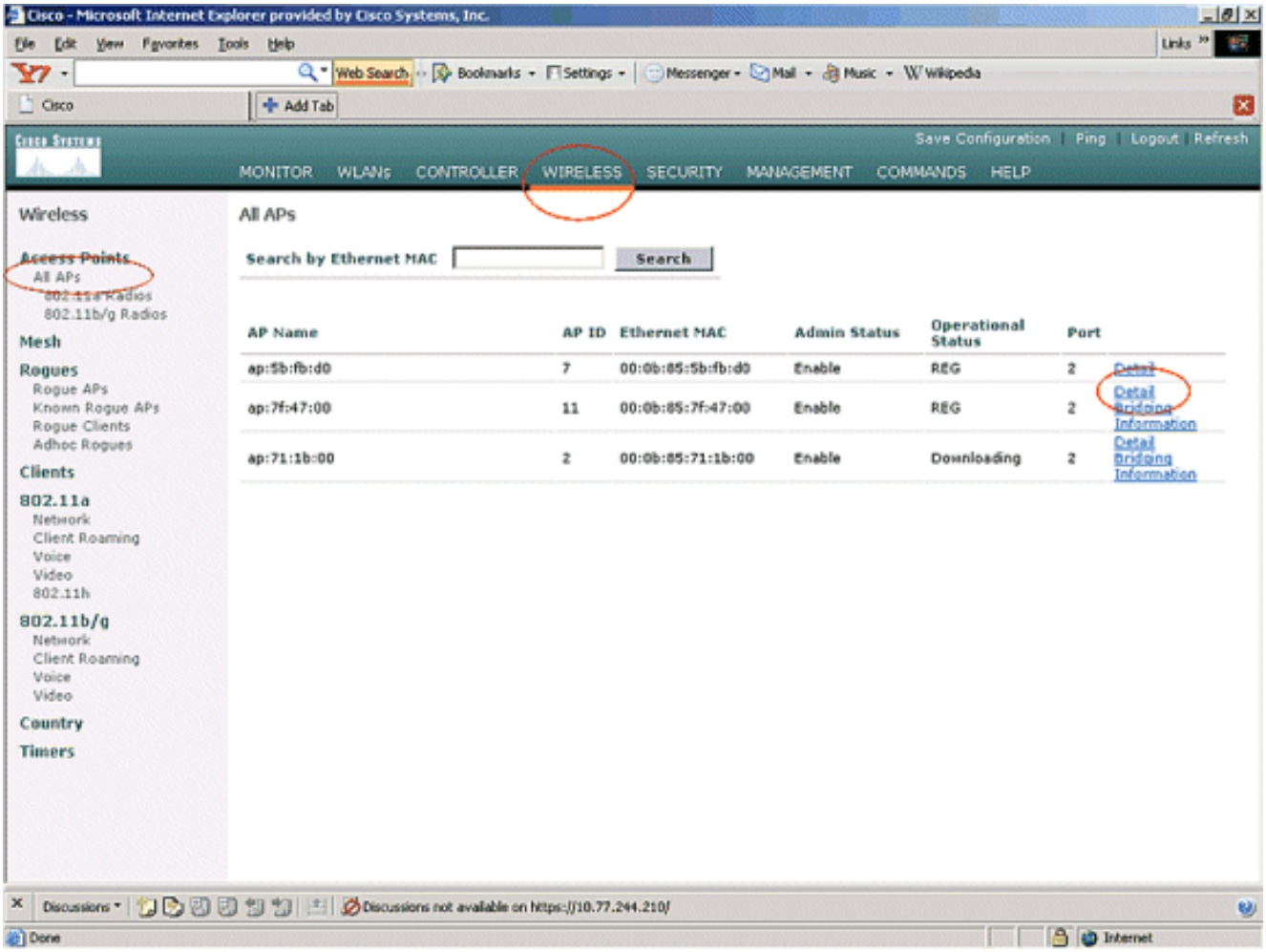
Abilitare Ethernet Bridging sui punti di accesso

Il passaggio successivo è quello di abilitare il bridging Ethernet sul RAP e su tutte le MAPPE la cui porta Ethernet è collegata a un dispositivo Ethernet. Una delle caratteristiche principali dei punti di accesso mesh è l'uso di una porta Ethernet sul MAP per collegare i dispositivi esterni e fornire il bridging Ethernet tra tutte le porte Ethernet dei punti di accesso coinvolti nella rete mesh.

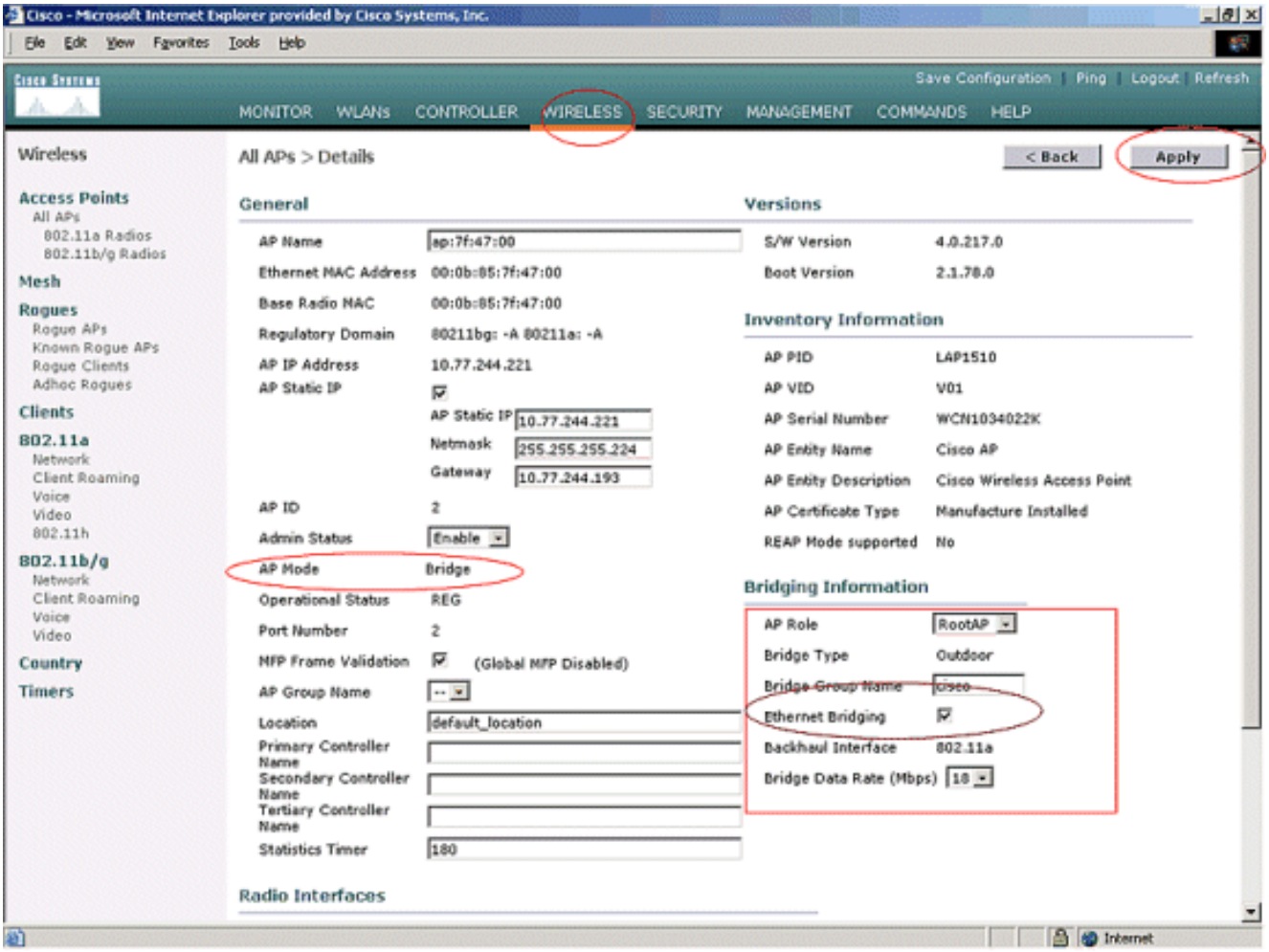
La rete mesh WLAN può trasmettere contemporaneamente due tipi di traffico diversi, il traffico dei client WLAN e il traffico del bridge MAP. Il traffico del client WLAN termina sul controller WLAN e il traffico del bridge termina sulle porte Ethernet dei 1500 mesh AP. Il traffico del bridge non raggiunge il WLC. Se un nodo mesh funziona come MAP, la porta Ethernet sul MAP viene bloccata. Questo è stato fatto per ragioni di sicurezza. Se si desidera utilizzare una porta Ethernet per l'installazione di reti P2MP o per la connessione di dispositivi esterni, è necessario attivarla sul controller per ogni MAP.

Completare questa procedura per configurare il bridging Ethernet sui punti di accesso RAP e mesh:

1. Fare clic su **Wireless**, quindi su **Tutti gli access point** in **Access Point**. Viene visualizzata la pagina **Tutti gli access point**.
2. Per accedere alla pagina **Dettagli** dell'access point, fare clic sul collegamento **Dettagli** dell'**access point** in
uso.

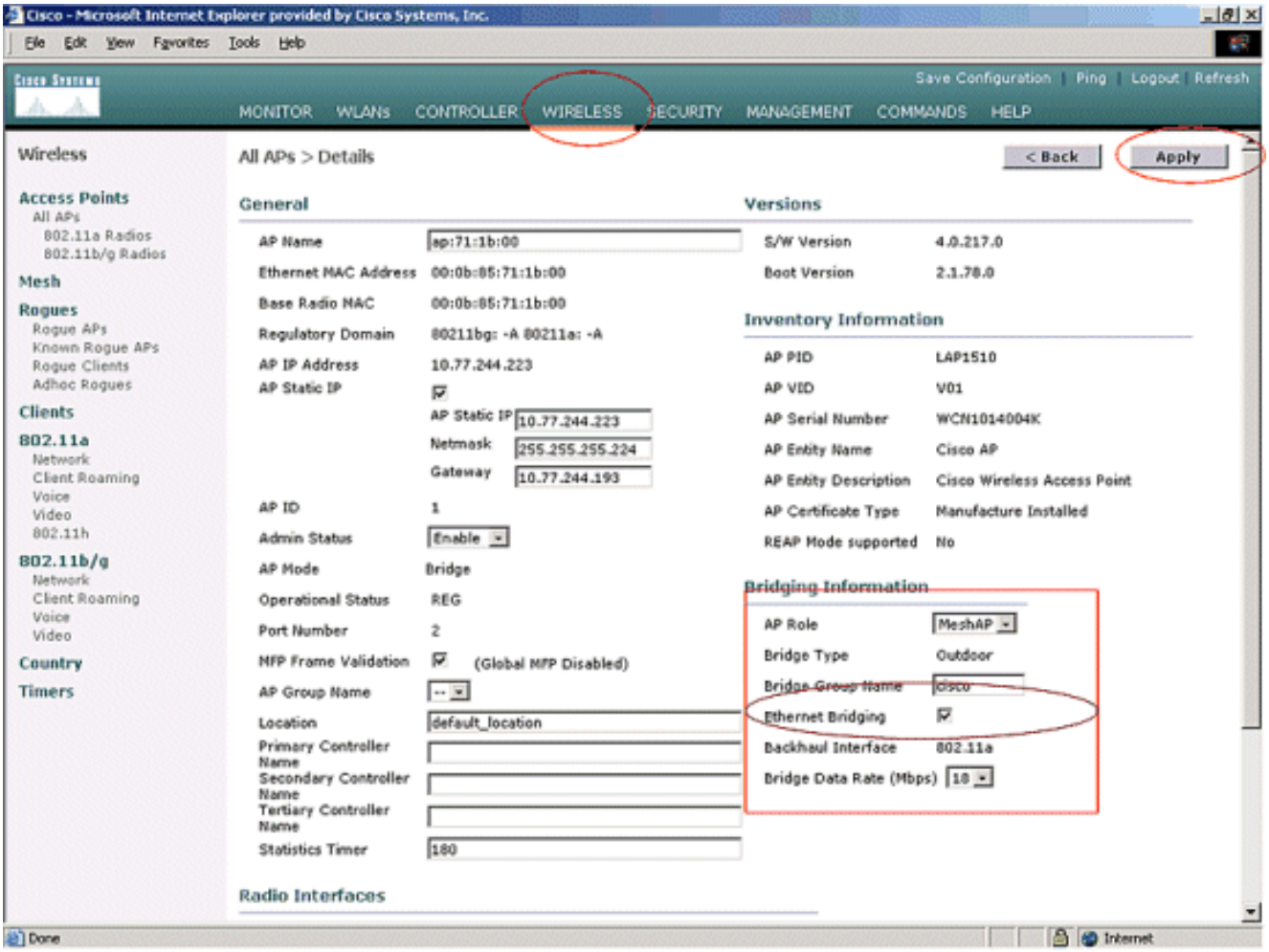


3. In **Informazioni di bridging**, selezionare la casella accanto a **Ethernet Bridging**. Ciò abilita il bridging Ethernet sull'access
point.



Se si utilizza una rete mesh punto-multipunto, abilitare il bridging Ethernet sui RAP e solo sulle MAP a cui sono collegati i dispositivi Ethernet. Non è necessario abilitare il bridging Ethernet su tutte le mappe in una rete mesh.Se è stato abilitato il bridging Ethernet per l'utilizzo della rete per il bridging (P2P o P2MP), è necessario abilitare il bridging Ethernet su tutti i nodi (MAP e RAP). Nello scenario di bridging, un RAP che funge da root bridge connette più MAP come non-root bridge alle LAN cablate associate.Èpossibile abilitare il bridging Ethernet sugli access point dalla CLI del controller con questo comando: **abilitazione del bridging dell'ap di configurazione**.**Nota:** gli switch collegati alle porte Ethernet delle mappe non devono eseguire il protocollo VLAN Trunking Protocol (VTP). Il VTP può riconfigurare la VLAN trunked sull'interfaccia mesh e causare una perdita di connessione per il RAP sul WLC primario. Se configurato in modo non corretto, può bloccare la distribuzione mesh.

4. Abilitare anche il bridging Ethernet e tutti i parametri di bridging illustrati nella sezione precedente di
MAP.



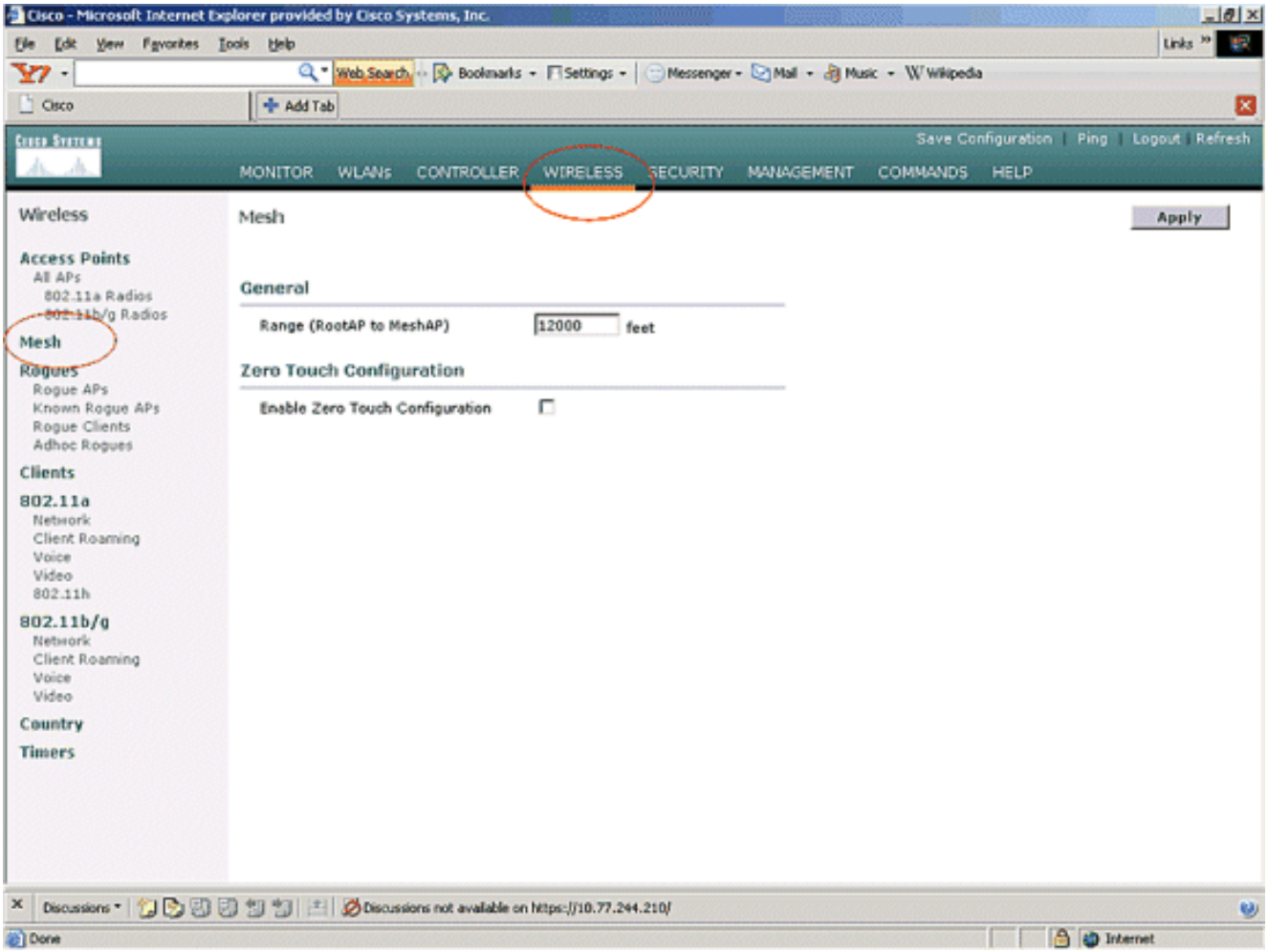
Dopo aver completato le configurazioni dei parametri bridge e dei parametri di bridging Ethernet su ciascun access point, fare clic su **Apply** (Applica) per salvare le impostazioni. In questo modo, l'AP annulla la registrazione dal WLC, viene riavviato e registrato nuovamente con il WLC.

Abilitare la configurazione zero-touch sul WLC

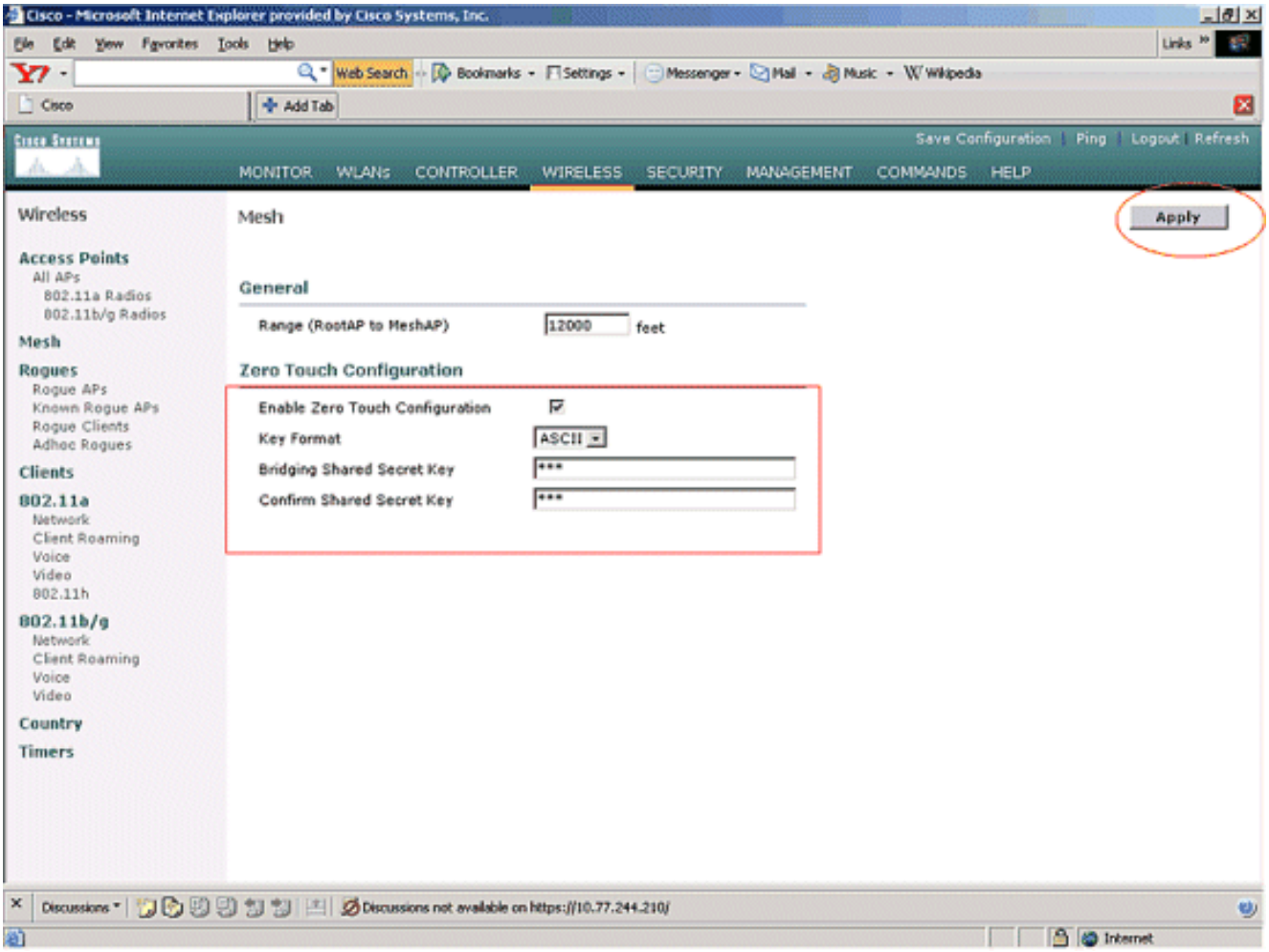
A questo punto, i punti di accesso sono stati configurati come punti di accesso e mappe, in base alle esigenze, nonché come parametri di bridging. Abilitare la **configurazione Zero-Touch sul WLC in** modo che, una volta rimossa la MAP dalla connessione cablata con il WLC e portata sulla rete di produzione (all'altra estremità della rete mesh point-to-point), la MAP sia in grado di stabilire una connessione LWAPP protetta con il WLC senza alcuna connessione cablata al WLC. Il valore predefinito per la configurazione zero-touch sul WLC è abilitato (o selezionato).

Completare questi passaggi per configurare la configurazione zero-touch sul WLC.

1. Dalla GUI del controller, selezionare **Wireless > Mesh** e fare clic su **Enable Zero Touch Configuration** (Abilita configurazione Zero Touch).



2. Scegliere il formato chiave (ASCII o Hex).
3. Immettere la chiave privata condivisa di bridging.Questo campo è abilitato solo se è abilitata l'opzione di configurazione zero-touch. Questa è la chiave che viene fornita ai punti di accesso mesh (MAP) per stabilire una connessione LWAPP sicura con il controller LAN wireless Cisco, mentre la MAP si connette in modalità wireless dall'altra estremità della rete mesh. La chiave deve avere una lunghezza di almeno 32 caratteri in formato esadecimale o ASCII. Nella fase di produzione viene assegnata una chiave segreta condivisa predefinita. Non è visibile a voi.In questo esempio viene utilizzata la chiave segreta condivisa di bridging di **cisco**.Quando si modifica la chiave segreta condivisa, il controller LAN wireless Cisco invia automaticamente la modifica a tutti i punti di accesso remoto (RAP), causando la perdita di connettività dei punti di accesso finché non saranno in grado di ottenere la nuova chiave segreta condivisa dal controller LAN wireless Cisco.
4. Immettere nuovamente la chiave privata condivisa di bridging nel campo **Conferma chiave privata condivisa**.
5. Fare clic su **Apply** (Applica). Questa schermata spiega i passaggi da 3 a 5.



Se la configurazione zero-touch è abilitata sul controller LAN wireless Cisco e la mappa viene spostata all'altra estremità della rete mesh, i punti di accesso e le mappe eseguono questa operazione per ottenere una configurazione sicura zero-touch:

1. Se si tratta di un dispositivo RAP, dispone già di una connessione LWAPP protetta al controller LAN wireless Cisco e utilizza l'interfaccia backhaul RAP configurata (impostazione predefinita: 802.11a).
2. Se si tratta di una MAP, esegue la scansione delle interfacce e dei canali backhaul per individuare i punti di accesso mesh adiacenti. Quando trova un punto di accesso mesh adiacente con lo stesso **nome di gruppo bridge** (configurato come parte dei parametri di bridging) e un percorso di ritorno al controller LAN wireless Cisco, lo rende il punto di accesso mesh padre. Se la mappa trova più di un punto di accesso mesh adiacente, utilizza un algoritmo meno costoso per determinare quale padre abbia il miglior percorso per tornare al controller LAN wireless Cisco.Per configurare una connessione LWAPP sicura con il controller LAN wireless Cisco, il MAP invia la propria chiave privata condivisa predefinita, già disponibile nella fase di produzione del punto di accesso, e l'indirizzo MAC per configurare una connessione protetta temporanea. Il controller LAN wireless Cisco convalida l'indirizzo MAC in base all'elenco di filtro MAC e, se lo trova, invia la chiave segreta condivisa, configurata come parte dell'impostazione di configurazione Zero-Touch alla mappa e disconnette. La mappa memorizza la chiave segreta condivisa e la utilizza per impostare una connessione LWAPP sicura.Se una mappa perde la connessione con il controller LAN wireless Cisco, cerca i router adiacenti validi che usano il nome del gruppo bridge di punti di accesso mesh e analizza le interfacce e i canali backhaul. Quando trova un punto di accesso mesh adiacente, lo rende il punto di accesso mesh padre. Se possiede già una chiave segreta condivisa, la utilizza e tenta di configurare una connessione LWAPP protetta al

controller LAN wireless Cisco. Se la chiave segreta condivisa non funziona, utilizza la chiave segreta predefinita condivisa e tenta di ottenere una nuova chiave segreta condivisa.

Verifica

- Dopo tutte le configurazioni, scollegare la MAP dalla rete cablata collegata al WLC e spostarla all'altra estremità della rete Mesh. Accendi la rete. Con tutte le configurazioni appropriate, il MAP è in grado di individuare il RAP come principale e di registrarsi con il controller in modalità wireless.
- Dalla CLI del WLC, è possibile usare i comandi **show mesh path** Cisco AP e **show mesh Neigh** *Cisco AP* per verificare che gli AP siano stati registrati sul WLC:Il comando **show mesh path** *AP name* viene usato per verificare il percorso dal controller verso il punto di accesso specificato. Di seguito è riportato un esempio:

```
(Cisco Controller) >show mesh path ap:71:1b:00

00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON
(86B), snrUp 10, snrDown 9, linkSnr 8
00:0B:85:7F:47:00 is RAP
```

In questo output viene indicato che per raggiungere l'access point **ap:71:1b:00(MAP)**, il controller ha nel percorso l'access point con indirizzo MAC **00:0B:85:7F:47:00** e questo access point è un **access point**.

```
(Cisco Controller) >show mesh path ap:7f:47:00

00:0B:85:7F:47:00 is RAP
```

Questo output indica che l'access point **ap:7f:47:00** è collegato direttamente al controller poiché si tratta di un access point **RAP**.Il comando **show mesh neighbors** *name* consente di visualizzare le informazioni sui router adiacenti del punto di accesso specificato. Di seguito è riportato un esempio:

```
(Cisco Controller) >show mesh neigh ap:7f:47:00

AP MAC : 00:0B:85:71:1B:00

FLAGS : 160 CHILD
worstDv 255, Ant 0, channel 0, biters 0, ppiters 10
Numroutes 0, snr 0, snrUp 0, snrDown 10, linkSnr 0
adjustedEase 0, unadjustedEase 0
txParent 0, rxParent 0
poorSnr  0
lastUpdate   1193504822 (Sat Oct 27 17:07:02 2007)
parentChange 0
Per antenna smoothed snr values: 0 0 0 0
Vector through 00:0B:85:71:1B:00
```

In questo output, il router adiacente dell'access point **ap:7f:47:00** è **MAP 00:0B:85:71:1B:00**, mentre il MAP è un **CHILD (FIGLIO)** per l'access point poiché si tratta di un access point.

```
(Cisco Controller) >show mesh neigh ap:71:1b:00


AP MAC : 00:0B:85:7F:47:00

FLAGS : 86A NEIGH PARENT BEACON
worstDv 0, Ant 0, channel 161, biters 0, ppiters 10
Numroutes 1, snr 0, snrUp 10, snrDown 10, linkSnr 8
```

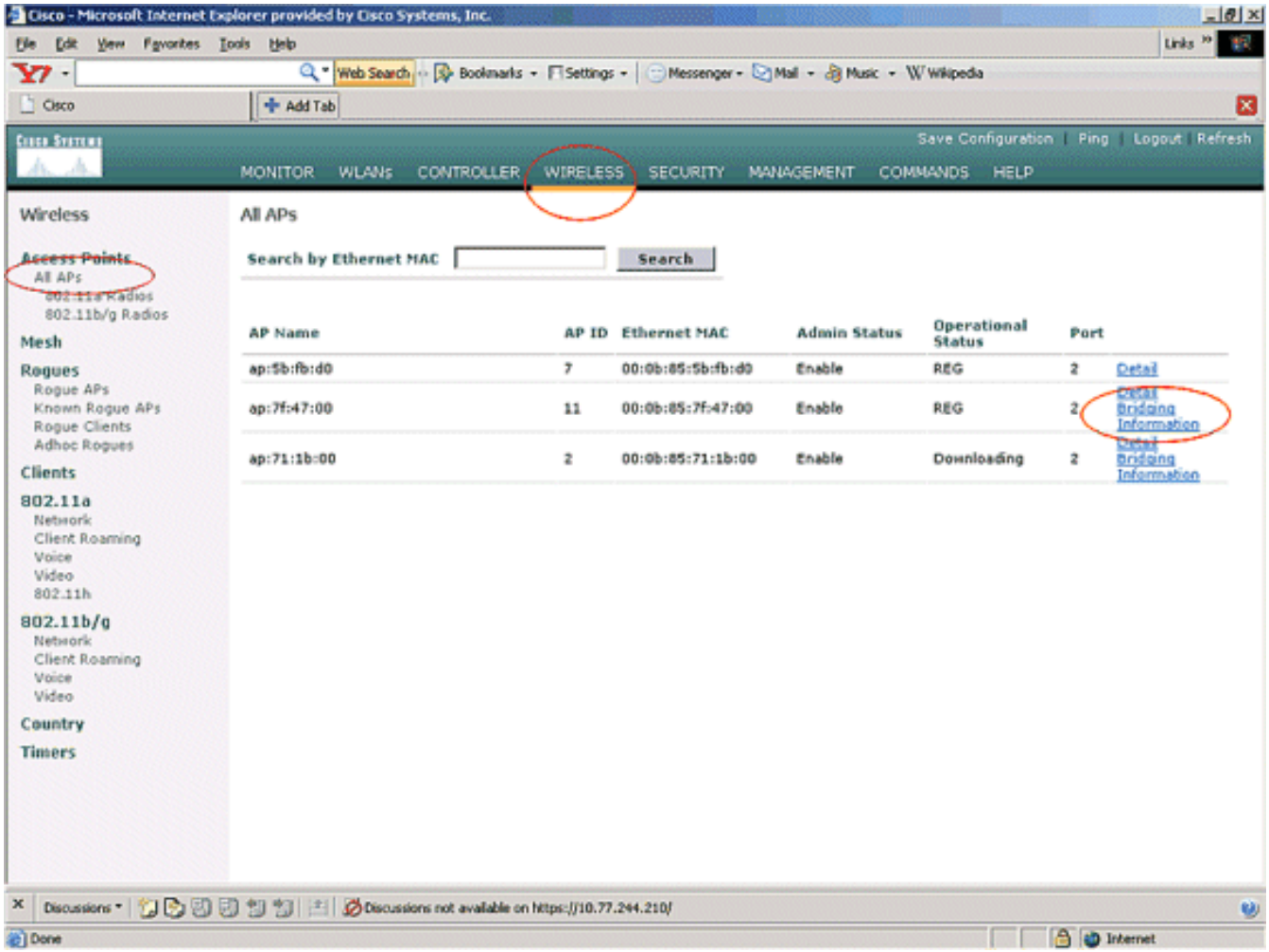
```
adjustedEase 213, unadjustedEase 256
txParent 106, rxParent 5
poorSnr  5
lastUpdate   1193504822 (Sat Oct 27 17:07:02 2007)
parentChange 1009152029 (Mon Dec 24 00:00:29 2001)
Per antenna smoothed snr values: 8 0 0 0
Vector through 00:0B:85:7F:47:00
Vector ease 1 -1,  FWD:  00:0B:85:7F:47:00
```

In questo output, il router adiacente di AP **ap:71:1b:00** è **RAP 00:0B:85:7F:47:00**, mentre il protocollo RAP è un **padre** di questo access point.

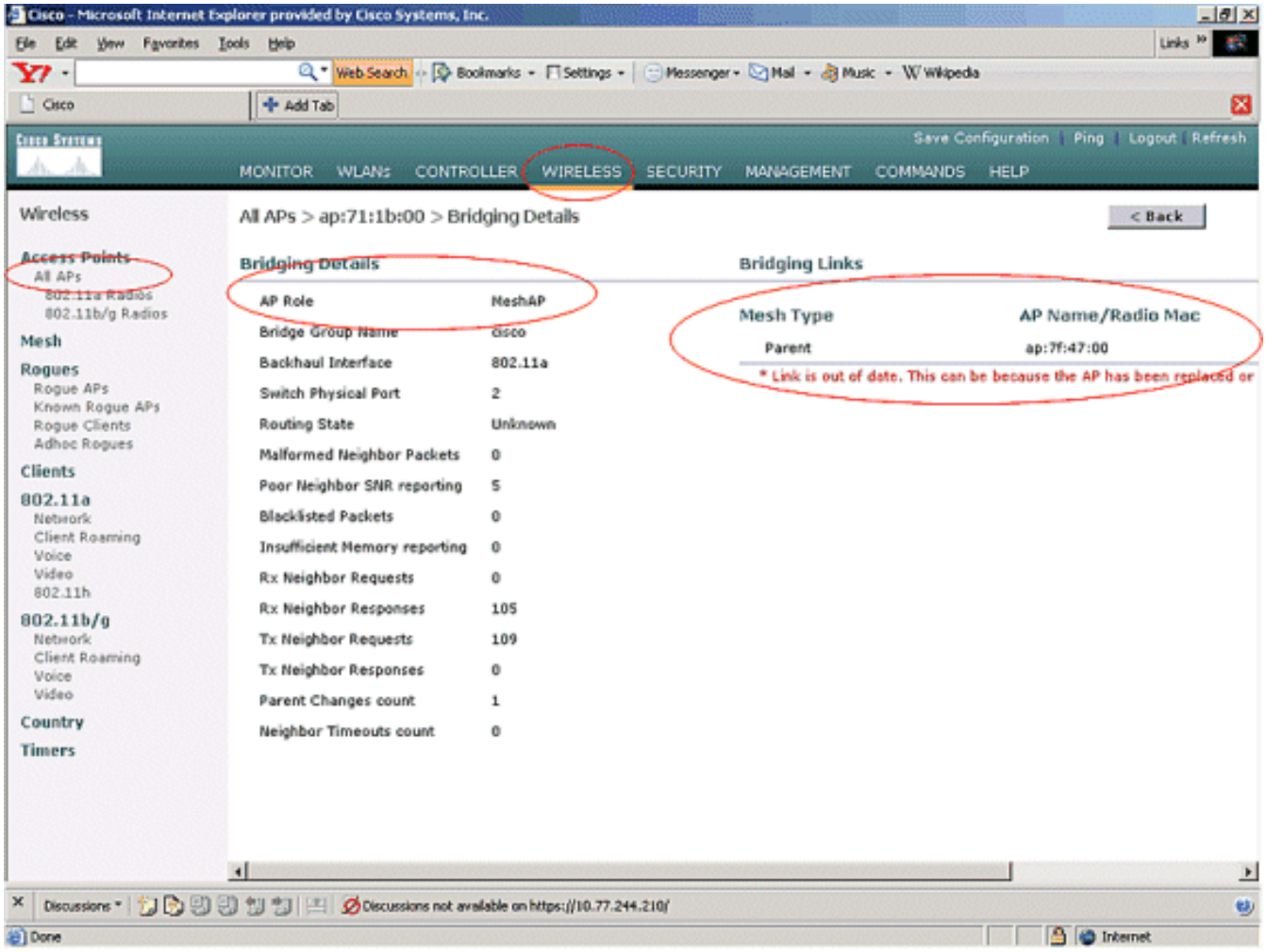
- Il comando **show mesh summary** *Nome app* visualizza i dettagli della mesh dell'access point specificato. Di seguito è riportato un esempio:

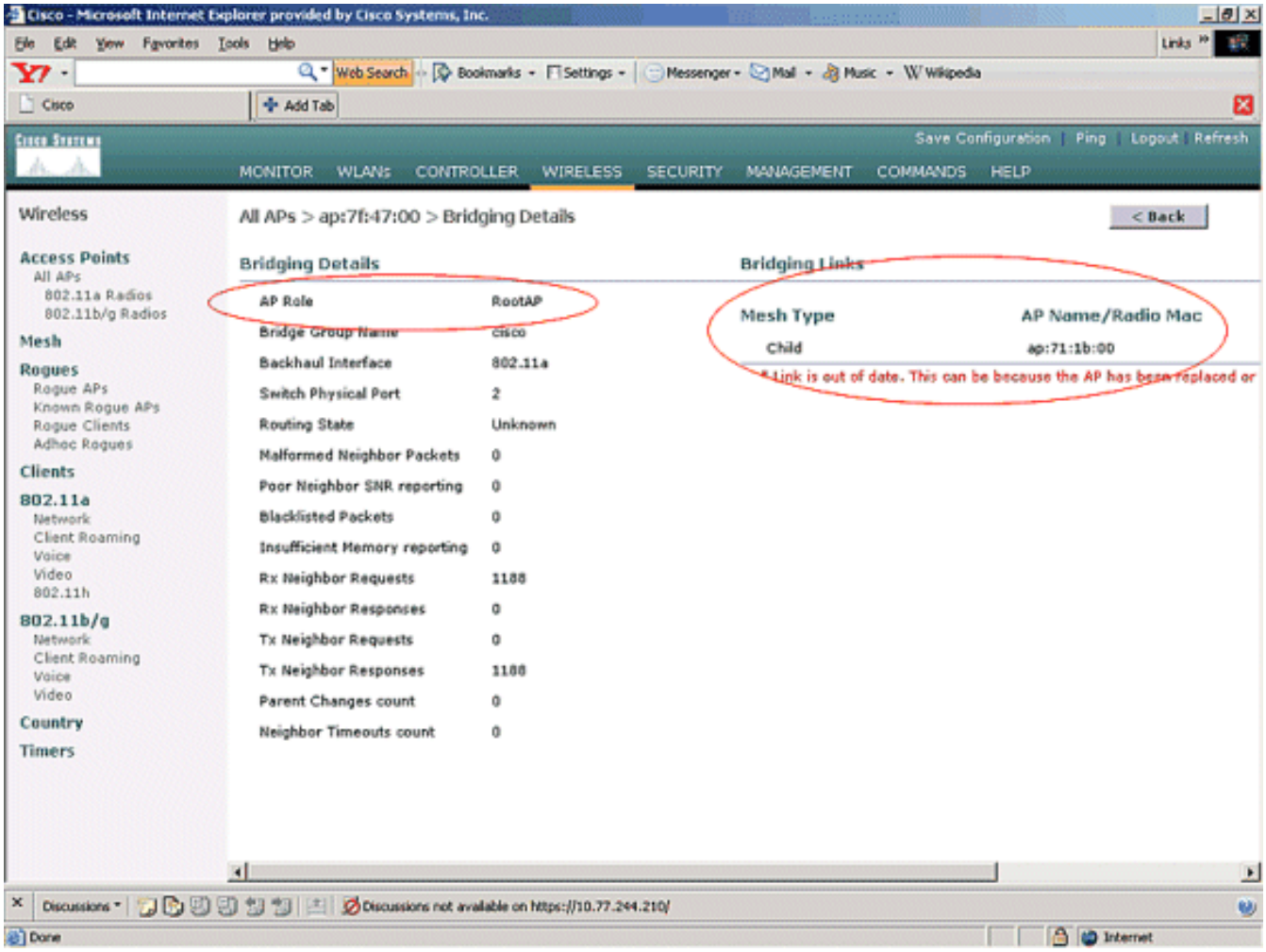
```
(Cisco Controller) >show mesh summary ap:71:1b:00

00:0B:85:7F:47:00 state UPDATED NEIGH PARENT BEACON (86B),
 snrUp 10, snrDown 10, linkSnr 8



(Cisco Controller) >show mesh summary ap:7f:47:00

00:0B:85:71:1B:00 state CHILD (160), snrUp 0, snrDown 10, linkSnr 0
```

- La stessa condizione può essere verificata dall'interfaccia del controller con questi passaggi:Dall'interfaccia utente del WLC, fare clic su **Wireless > All APs** (Wireless > Tutti gli access point).Fare clic sul collegamento **Bridging Information** (Informazioni di bridging) del modello AP1510 per accedere alla pagina **Bridging Information (Informazioni di bridging)** del modello
AP.



La pagina **Dettagli bridging** dell'access point elenca tutti i dettagli di bridging dell'access point, ad esempio il ruolo e il tipo di
mesh.





Dalla CLI del WLC, è possibile usare i comandi **show mesh path** *Cisco AP* e **show mesh Neigh** *Cisco AP* per verificare che gli AP siano registrati sul WLC:

Per verificare il corretto funzionamento del bridging Ethernet, effettuare i seguenti passaggi:

1. Collegare una rete Ethernet (LAN Ethernet B come indicato nel diagramma di rete) alla porta Ethernet del MAP tramite uno switch. Verificare che lo switch sia configurato correttamente in base alle esigenze.
2. Verificare la connettività tra la LAN Ethernet B sulla MAPPA e la rete cablata (LAN Ethernet A come indicato nel diagramma di rete) connessa al punto di accesso dietro il WLC con il comando **ping**. Se il comando **ping** ha esito positivo, il bridging Ethernet funziona correttamente.

Risoluzione dei problemi

Questi comandi di risoluzione dei problemi possono essere utili:

Comandi per la risoluzione dei problemi

- **debug lwapp errors enable**: visualizza il debug degli errori LWAPP.
- **debug pm pki enable**: visualizza il debug dei messaggi di certificato passati tra l'access point e il WLC.Questo comando mostra chiaramente se un access point non può unirsi al WLC a causa di una mancata corrispondenza del periodo di validità della certificazione.Di seguito viene riportato l'output del comando **debug pm pki enable** sul controller:

```
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: locking ca cert table
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_alloc()
   for user cert
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: calling x509_decode()
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <subject> C=US, ST=California,
                          L=San Jose, O=Cisco Systems, CN=C1200-001563e50c7e,
                          MAILTO=support@cisco.com
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: <issuer>  O=Cisco Systems,
                          CN=Cisco Manufacturing CA
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Mac Address in subject is
                          00:15:63:e5:0c:7e
Thu May 25 07:25:00 2006: sshpmGetIssuerHandles: Cert is issued by Cisco
   Systems.
.........................
.........................
.........................
.........................
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: calling x509_decode()
Fri Apr 15 07:55:03 2005: ssphmUserCertVerify: user cert verfied using
                          >cscoDefaultMfgCaCert<
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: ValidityString (current):
                          2005/04/15/07:55:03
Fri Apr 15 07:55:03 2005: sshpmGetIssuerHandles: Current time outside AP cert
                          validity interval: make sure the controller
                          time is set.
Fri Apr 15 07:55:03 2005: sshpmFreePublicKeyHandle: called with (nil)
```

In questo output, notate le informazioni evidenziate. Queste informazioni indicano chiaramente che l'ora del controller non rientra nell'intervallo di validità del certificato dell'access point, pertanto l'access point non può registrarsi con il controller. I certificati installati nel punto di accesso hanno un intervallo di validità predefinito. L'ora del controller deve essere impostata in modo da rientrare nell'intervallo di validità del certificato del punto di accesso.Fare riferimento al documento LWAPP Upgrade Tools Troubleshoot Tips per ulteriori informazioni su possibili problemi in un LAP che si registra con il controller.Per ulteriori informazioni sulla risoluzione dei problemi di una rete mesh, fare riferimento a Risoluzione dei problemi di una rete mesh.

- Di seguito sono riportati altri comandi di debug che possono essere utili:**debug pem state enable**: utilizzato per configurare le opzioni di debug di access policy manager.**debug pem events enable**: utilizzato per configurare le opzioni di debug di access policy manager.**debug dhcp message enable**: visualizza il debug dei messaggi DHCP scambiati da e verso il server DHCP.**debug dhcp packet enable**: visualizza il debug dei dettagli dei pacchetti DHCP inviati e ricevuti dal server DHCP.

Informazioni correlate

- Guida All'Implementazione Della Soluzione Cisco Mesh Networking
- Installazione e configurazione del punto di accesso Mesh
- Esempio di configurazione della rete Mesh del controller LAN wireless
- Guida introduttiva: Cisco Aironet serie 1500 Lightweight Mesh Access Point per ambienti esterni
- Guida all'installazione dell'hardware del punto di accesso Mesh per esterni di Cisco Aironet serie 1500
- Istruzioni per l'installazione di Cisco Aironet serie 1500 Access Point Power Injector
- Cisco Aironet serie 1500 AP Q e A

- Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC)
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Documentazione e supporto tecnico – Cisco Systems