Esempio di configurazione della rete Mesh del controller LAN wireless

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Premesse](#)
[Cisco Aironet serie 1510 Lightweight Mesh AP per ambienti esterni](#)
[Access point dal tetto (RAP)](#)
[Access point Pole-top (PAP)](#)
[Funzioni non supportate sulle reti Mesh](#)
[Sequenza di avvio del punto di accesso](#)
[Configurazione](#)
[Abilita configurazione Zero Touch (abilitata per impostazione predefinita)](#)
[Aggiungere il MIC all'elenco di autorizzazioni AP](#)
[Configurazione dei parametri di bridging per gli access point](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Comandi per la risoluzione dei problemi](#)
[Informazioni correlate](#)

Introduzione

Questo documento offre un esempio di configurazione base per stabilire un collegamento bridge point-to-point con la soluzione Mesh Network. In questo esempio vengono utilizzati due Lightweight Access Point (LAP). Un LAP funziona come punto di accesso sul tetto (RAP), l'altro LAP come punto di accesso con braccio laterale (PAP) e viene collegato a un controller WLAN (Cisco Wireless LAN). Il dispositivo RAP è collegato al WLC tramite uno switch Cisco Catalyst.

Fare riferimento all'esempio di configurazione della rete Mesh del controller LAN wireless per le versioni 5.2 e successive per WLC release 5.2 e successive

Prerequisiti

- Il WLC è configurato per il funzionamento 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 di LAP e WLC di Cisco
- Conoscenze base di LWAPP (Lightweight AP Protocol).
- Conoscenza della configurazione di un server DHCP esterno e/o di un server dei nomi di dominio (DNS)
- 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 4402 WLC con firmware 3.2.150.6
- 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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Cisco Aironet serie 1510 Lightweight Mesh AP per ambienti esterni

Cisco Aironet serie 1510 Lightweight Mesh AP è un dispositivo wireless progettato per l'accesso wireless ai 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.

AP1510 funziona con i controller per fornire gestione centralizzata e scalabile, alta sicurezza e mobilità. Progettato per supportare installazioni a configurazione zero, l'AP1510 si inserisce facilmente e in modo sicuro nella rete mesh ed è disponibile per gestire e monitorare la rete tramite la GUI o la CLI del controller.

L'AP1510 è dotato di due radio che funzionano contemporaneamente: una radio da 2,4 GHz utilizzata per l'accesso dei client e una radio da 5 GHz utilizzata per il backhaul di dati verso altri access point serie AP1510. Il traffico client LAN wireless passa attraverso la radio backhaul dell'access point o viene inoltrato attraverso altri AP1510 finché non raggiunge la connessione Ethernet del controller.

Access point dal tetto (RAP)

I RAP hanno una connessione cablata a un WLC Cisco. Usano l'interfaccia wireless backhaul per comunicare con i PAP adiacenti. I RAP sono il nodo padre di qualsiasi rete a bridging o mesh e collegano un bridge o una rete mesh alla rete cablata. Pertanto, può esistere un solo criterio di autorizzazione delle risorse per ogni segmento di rete con bridge o mesh.

Nota: quando si usa la soluzione di rete mesh per il bridging da LAN a LAN, non connettere un RAP direttamente a un Cisco WLC. È necessario uno switch o un router tra il WLC Cisco e il RAP perché i WLC Cisco non inoltrano il traffico Ethernet che proviene da una porta abilitata per LWAPP. I criteri di autorizzazione delle risorse possono funzionare in modalità LWAPP di livello 2 o 3.

Access point Pole-top (PAP)

I PAP non hanno connessioni cablate a un WLC Cisco. Possono essere completamente wireless e supportare client che comunicano con altri PAP 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 necessario abilitarla per i PAP.

Nota: i Cisco Aironet 1030 Remote Edge LAP supportano implementazioni a hop singolo, mentre i Cisco Aironet serie 1500 Lightweight Outdoor AP supportano implementazioni a hop singolo e multi-hop. Pertanto, i Cisco Aironet serie 1500 Lightweight Outdoor AP possono essere utilizzati come rooftop AP e come PAP per uno o più hop dal Cisco WLC.

Funzioni non supportate sulle reti Mesh

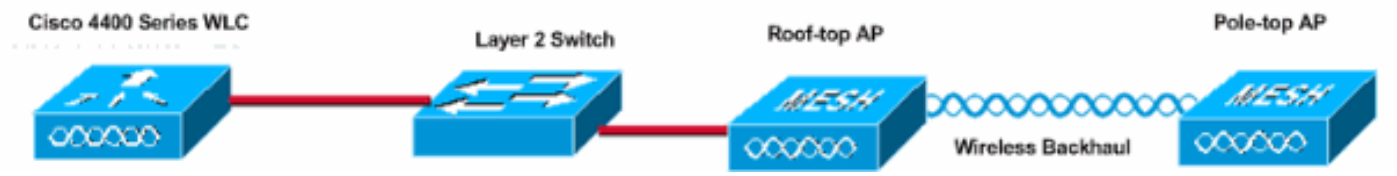
Queste funzionalità del controller non sono supportate nelle reti mesh:

- Supporto di più paesi
- CAC basato sul carico (le reti Mesh supportano solo CAC statiche o basate sulla larghezza di banda)
- Alta disponibilità (heartbeat veloce e timer di join di individuazione primaria)
- Autenticazione EAP-FASTv1 e 802.1X
- Autenticazione EAP-FASTv1 e 802.1X
- Certificato significativo locale
- Servizi basati sulla posizione

Sequenza di avvio del punto di accesso

Questo elenco descrive cosa succede all'avvio di RAP e PAP:

- Tutto il traffico attraversa il RAP e il Cisco WLC prima di essere inviato alla LAN.
- Quando viene visualizzato il file RAP, i PAP vi si connettono automaticamente.
- Il collegamento connesso utilizza un segreto condiviso per generare una chiave utilizzata per fornire AES (Advanced Encryption Standard) per il collegamento.
- Una volta che il PAP remoto si connette al RAP, i punti di accesso mesh possono passare il traffico dei dati.
- Gli utenti possono modificare il segreto condiviso o configurare i Mesh AP tramite l'interfaccia della riga di comando (CLI) Cisco, l'interfaccia utente Web Cisco del controller o Cisco Wireless Control System (Cisco WCS). Cisco consiglia di modificare il segreto condiviso.



Configurazione

Completare questa procedura per configurare il WLC e gli AP per il bridging point-to-point.

1. Abilitare la configurazione Zero Touch sul WLC.
2. Aggiungere il MIC all'elenco di autorizzazioni AP.
3. Configurare i parametri di bridging per gli access point.
4. Verificare la configurazione.

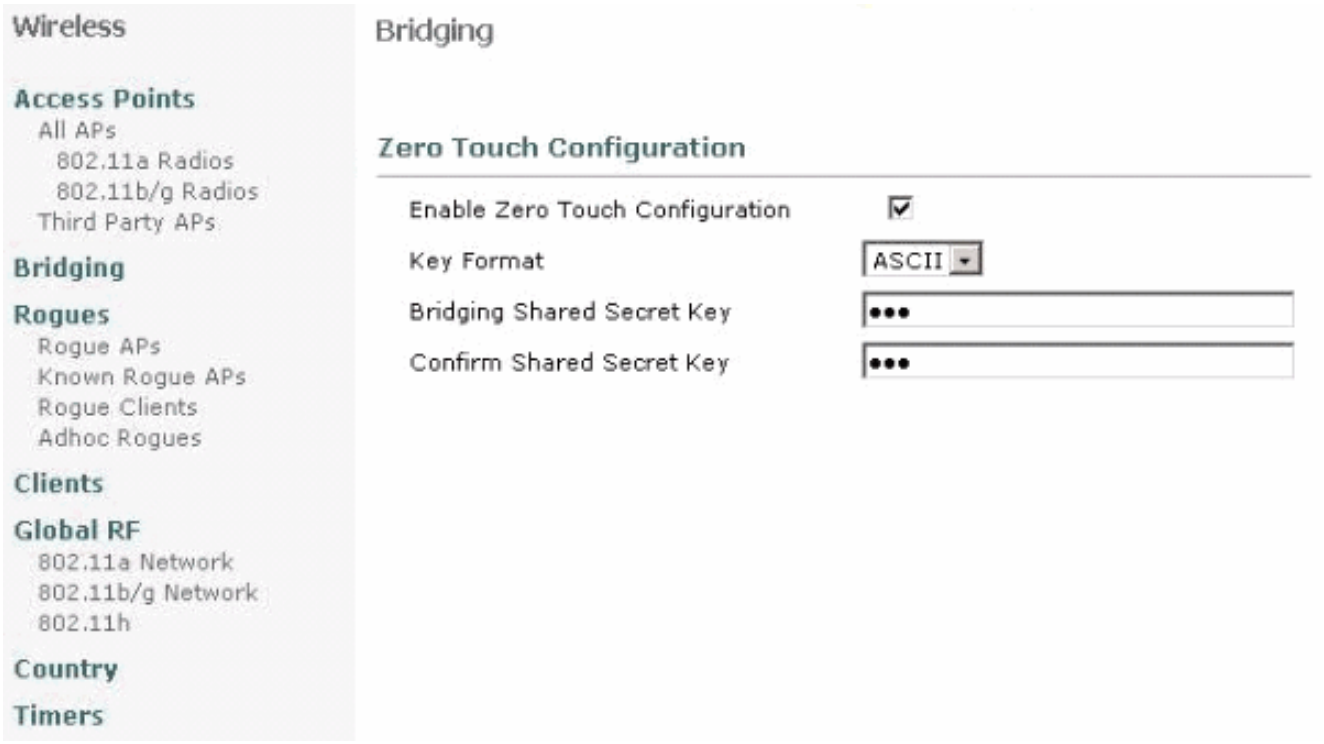
Abilita configurazione Zero Touch (abilitata per impostazione predefinita)

Configurazione GUI

Enable Zero Touch Configuration consente agli access point di ottenere la chiave privata condivisa dal controller quando si registra al WLC. Se si deseleziona questa casella, il controller non fornirà la chiave segreta condivisa e gli access point utilizzeranno una chiave precondivisa predefinita per una comunicazione sicura. Il valore predefinito è attivato (o selezionato). Completare questi passaggi dalla GUI del WLC:

Nota: non è possibile effettuare la configurazione Zero-Touch in WLC versione 4.1 e successive.

1. Scegliere **Wireless > Bridging** e fare clic su **Enable Zero Touch Configuration**.
2. Selezionare il formato della chiave.
3. Immettere la chiave privata condivisa di bridging.
4. Immettere nuovamente la chiave privata condivisa di bridging nella casella Conferma chiave privata
   condivisa.



Configurazione CLI

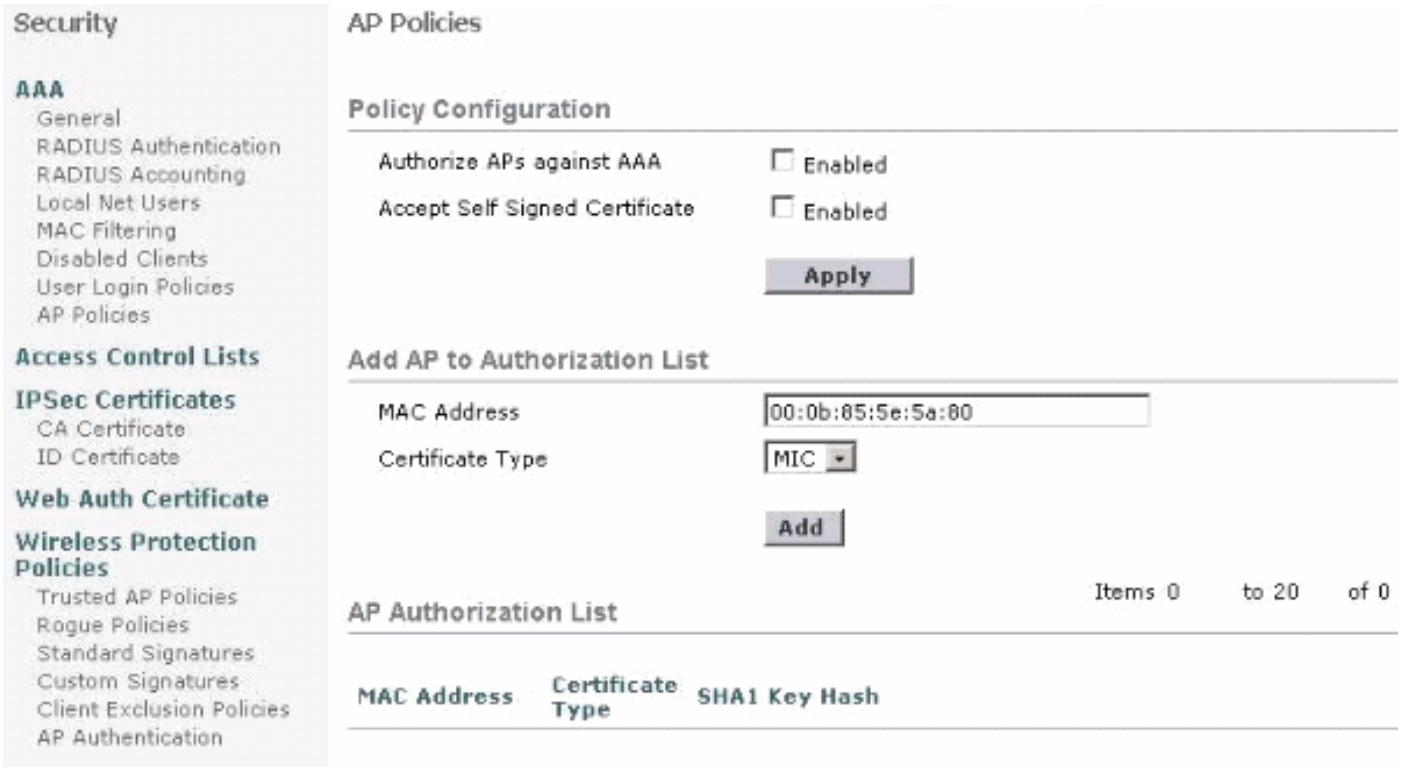
Completare questi passaggi dalla CLI:

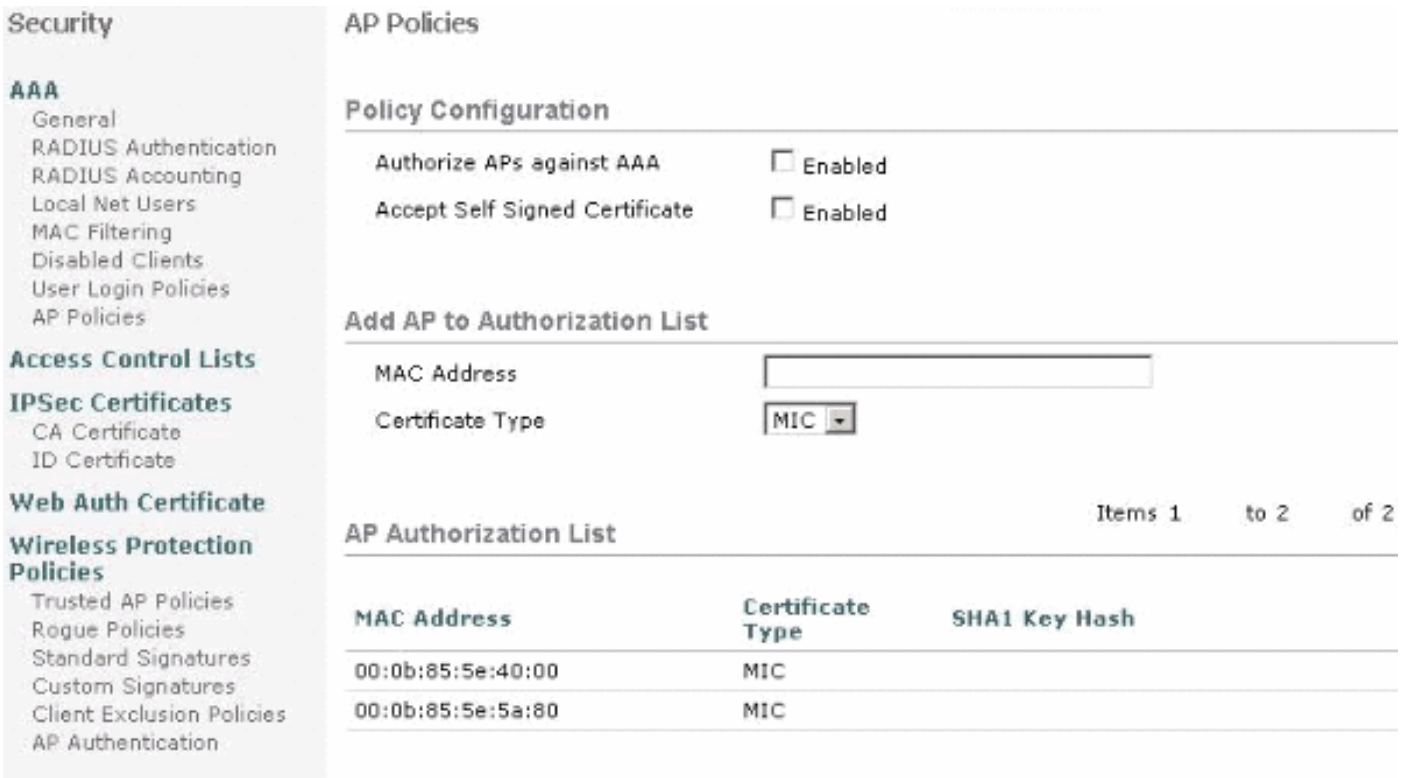
1. Usare il comando **config network zero-config enable** per abilitare la configurazione zero-touch.
   ```
   (Cisco Controller) >config network zero-config enable
   ```

2. Utilizzare il comando **config network bridging-shared-secret <string>** per aggiungere la chiave privata condivisa di bridging.
   ```
   (Cisco Controller) >config network bridging-shared-secret Cisco
   ```

Aggiungere il MIC all'elenco di autorizzazioni AP

Il passaggio successivo è aggiungere l'AP all'elenco delle autorizzazioni sul WLC. A tale scopo, scegliere **Sicurezza > Criteri PA**, immettere l'indirizzo MAC AP in Aggiungi AP all'elenco autorizzazioni e fare clic su **Aggiungi**.





Nell'esempio, entrambi gli access point (il punto di accesso e il punto di accesso) vengono aggiunti all'elenco delle autorizzazioni dell'access point sul controller.

Configurazione CLI

Usare il comando **config auth-list add mic <AP mac>** per aggiungere il MIC all'elenco di autorizzazioni.

```
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:40:00
(Cisco Controller) >config auth-list add mic 00:0b:85:5e:5a:80
```

Configurazione

Nel documento viene usata questa configurazione:

Cisco WLC 4402

```
(Cisco Controller) >show run-config

Press Enter to continue...

System Inventory
Switch Description..............................  Cisco
Controller
Machine Model.....................................
WLC4402-12
Serial Number.....................................
FLS0943H005
Burned-in MAC Address.............................
00:0B:85:40:CF:A0
Crypto Accelerator 1..............................  Absent
Crypto Accelerator 2..............................  Absent
Power Supply 1....................................  Absent
Power Supply 2....................................
Present, OK

Press Enter to continue Or <Ctl Z> to abort

System Information
Manufacturer's Name...............................  Cisco
Systems, Inc
Product Name......................................  Cisco
Controller
Product Version...................................
3.2.150.6
RTOS Version......................................
3.2.150.6
Bootloader Version................................
3.2.150.6
Build Type........................................  DATA +
WPS

System Name.......................................
lab120wlc4402ip100
System Location...................................
System Contact....................................
System ObjectID...................................
1.3.6.1.4.1.14179.1.1.4.3
IP Address........................................
192.168.120.100
System Up Time....................................  0 days
1 hrs 4 mins 6 secs

Configured Country................................  United
States
Operating Environment.............................
Commercial (0 to 40 C)
Internal Temp Alarm Limits........................  0 to
65 C
Internal Temperature..............................  +42 C
```

```
State of 802.11b Network.....................
Disabled
State of 802.11a Network.....................
Disabled
Number of WLANs.............................. 1
3rd Party Access Point Support...............
Disabled
Number of Active Clients..................... 0

Press Enter to continue Or <Ctl Z> to abort

Switch Configuration
802.3x Flow Control Mode.....................
Disable
Current LWAPP Transport Mode................... Layer
3
LWAPP Transport Mode after next switch reboot.... Layer
3
FIPS prerequisite features.....................
Disabled

Press Enter to continue Or <Ctl Z> to abort

Network Information
RF-Network Name............................. airespacerf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Shell (ssh)........................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Mode: Ucast
User Idle Timeout............................ 300 seconds
ARP Idle Timeout............................ 300 seconds
ARP Unicast Mode............................ Disabled
Cisco AP Default Master..................... Disable
Mgmt Via Wireless Interface................. Enable
Bridge AP Zero Config....................... Enable
Bridge Shared Secret.....................
youshouldsetme
Allow Old Bridging Aps To Authenticate...... Disable
Over The Air Provisioning of AP's........... Disable
Mobile Peer to Peer Blocking................ Disable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled

Press Enter to continue Or <Ctl Z> to abort

Port Summary
           STP   Admin   Physical   Physical   Link
Link    Mcast
Pr  Type   Stat   Mode     Mode      Status   Status
Trap   Appliance   POE
-- ------- ---- ------- ---------- ---------- ------ ---
---- --------- -------
1  Normal  Forw Enable  Auto       1000 Full  Up
Enable  Enable     N/A
2  Normal  Forw Enable  Auto       1000 Full  Up
Enable  Enable     N/A

Mobility Configuration
Mobility Protocol Port...................... 16666
Mobility Security Mode.....................
```

```
Disabled
Default Mobility Domain.....................
airespacerf
Mobility Group members configured.............. 3

Switches configured in the Mobility Group
 MAC Address           IP Address         Group Name
 00:0b:85:33:a8:40     192.168.5.70       <local>
 00:0b:85:40:cf:a0     192.168.120.100    <local>
 00:0b:85:43:8c:80     192.168.5.40       airespacerf

Interface Configuration
Interface Name................................. ap-
manager
IP Address.....................................
192.168.120.101
IP Netmask.....................................
255.255.255.0
IP Gateway.....................................
192.168.120.1
VLAN...........................................
untagged
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port...........................
Unconfigured
Primary DHCP Server............................
192.168.1.20
Secondary DHCP Server..........................
Unconfigured
ACL............................................
Unconfigured
AP Manager..................................... Yes

Interface Name.................................
management
MAC Address....................................
00:0b:85:40:cf:a0
IP Address.....................................
192.168.120.100
IP Netmask.....................................
255.255.255.0
IP Gateway.....................................
192.168.120.1
VLAN...........................................
untagged
Active Physical Port........................... 1
Primary Physical Port.......................... 1
Backup Physical Port...........................
Unconfigured
Primary DHCP Server............................
192.168.1.20
Secondary DHCP Server..........................
Unconfigured
ACL............................................
Unconfigured
AP Manager..................................... No

Interface Name.................................
service-port
MAC Address....................................
00:0b:85:40:cf:a1
IP Address.....................................
192.168.250.100
```

```
IP Netmask.....................................
255.255.255.0
DHCP Protocol..................................
Disabled
AP Manager..................................... No

Interface Name.................................
virtual
IP Address.....................................
1.1.1.1
Virtual DNS Host Name..........................
Disabled
AP Manager..................................... No

WLAN Configuration

WLAN Identifier................................ 1
Network Name (SSID)............................
lab120wlc4402ip100
Status.........................................
Enabled
MAC Filtering..................................
Enabled
Broadcast SSID.................................
Enabled
AAA Policy Override............................
Disabled
Number of Active Clients....................... 0
Exclusionlist Timeout.......................... 60
seconds
Session Timeout................................ 1800
seconds
Interface......................................
management
WLAN ACL.......................................
unconfigured
DHCP Server....................................
Default
Quality of Service............................. Silver
(best effort)
WMM............................................
Disabled
802.11e........................................
Disabled
Dot11-Phone Mode (7920).........................
Disabled
Wired Protocol................................. None
IPv6 Support...................................
Disabled
Radio Policy................................... All
Radius Servers
   Authentication..............................
192.168.1.20 1812
Security

   802.11 Authentication:....................... Open
System
   Static WEP Keys.............................
Enabled
        Key Index:.....................................
1
        Encryption:....................................
104-bit WEP
   802.1X.....................................
```

```
Disabled
   Wi-Fi Protected Access (WPA1).................
Disabled
   Wi-Fi Protected Access v2 (WPA2).............
Disabled
   IP Security.................................
Disabled
   IP Security Passthru........................
Disabled
   L2TP........................................
Disabled
   Web Based Authentication....................
Disabled
   Web-Passthrough.............................
Disabled
   Auto Anchor.................................
Disabled
   Cranite Passthru............................
Disabled
   Fortress Passthru...........................
Disabled

RADIUS Configuration
Vendor Id Backward Compatibility.................
Disabled
Credentials Caching.............................
Disabled
Call Station Id Type............................ IP
Address
Administrative Authentication via RADIUS.........
Enabled
Keywrap.........................................
Disabled

Load Balancing Info
Aggressive Load Balancing.......................
Enabled
Aggressive Load Balancing Window................. 0
clients

Signature Policy
  Signature Processing..........................
Enabled

Spanning Tree Switch Configuration

STP Specification..................... IEEE 802.1D
STP Base MAC Address...................
00:0B:85:40:CF:A0
Spanning Tree Algorithm................. Disable
STP Bridge Priority.................... 32768
STP Bridge Max. Age (seconds).......... 20
STP Bridge Hello Time (seconds)........ 2
STP Bridge Forward Delay (seconds)..... 15

Spanning Tree Port Configuration

STP Port ID............................... 8001
STP Port State............................ Forwarding
STP Port Administrative Mode.............. 802.1D
STP Port Priority......................... 128
STP Port Path Cost........................ 4
STP Port Path Cost Mode.................... Auto
```

```
STP Port ID..............................  8002
STP Port State...........................  Forwarding
STP Port Administrative Mode.............  802.1D
STP Port Priority........................  128
STP Port Path Cost.......................  4
STP Port Path Cost Mode..................  Auto
```

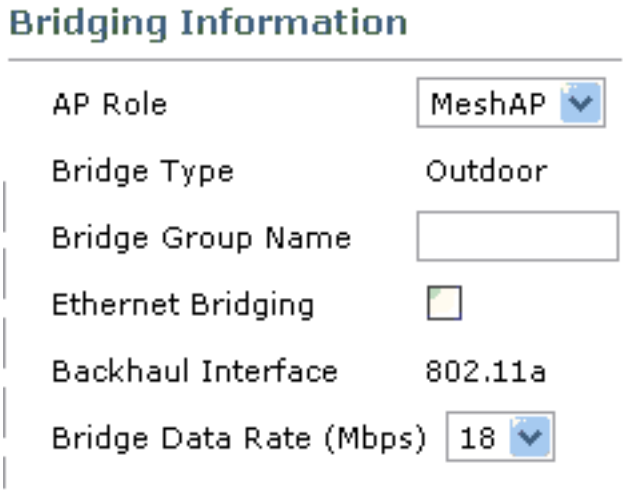
Configurazione dei parametri di bridging per gli access point

In questa sezione vengono fornite istruzioni su come configurare il ruolo dell'access point nella rete mesh e i parametri di bridging correlati. È possibile configurare questi parametri utilizzando la GUI o la CLI.

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 Tutti gli access point > Dettagli, fare clic sul collegamento **Detail** del dispositivo AP1510

In questa pagina la modalità AP in Generale viene impostata automaticamente su Bridge per gli access point con funzionalità di bridge, ad esempio AP1510. Questa pagina mostra inoltre queste informazioni in Informazioni di bridging. In Informazioni di bridging scegliere una delle opzioni seguenti per specificare il ruolo dell'access point nella rete mesh:

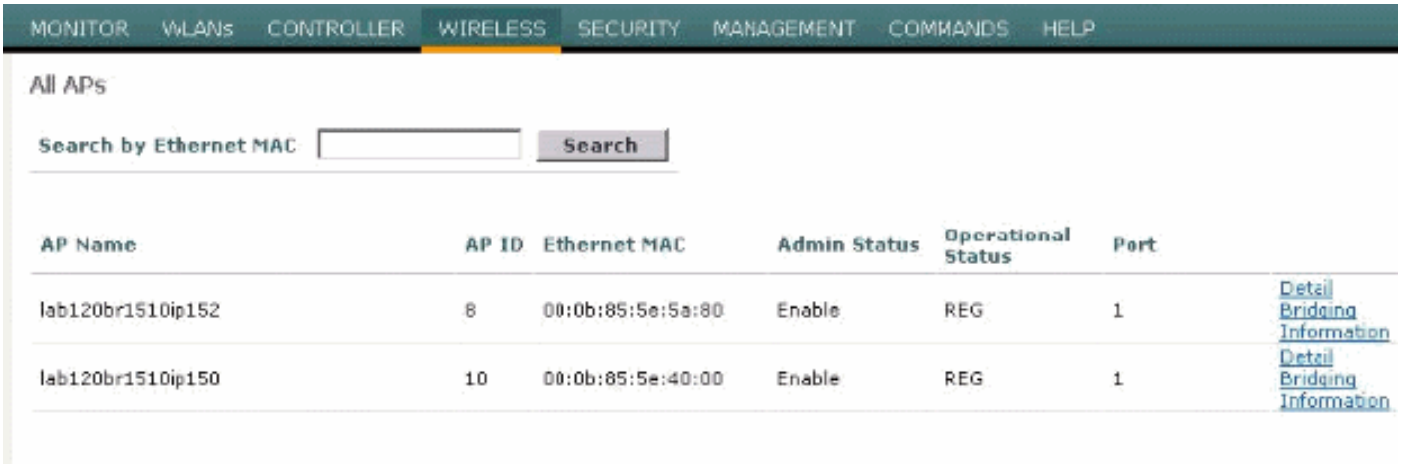
- **MeshAP**: selezionare questa opzione se l'AP1510 dispone di una connessione wireless al controller.
- **RootAP**: selezionare questa opzione se l'AP1510 ha una connessione cablata al controller.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

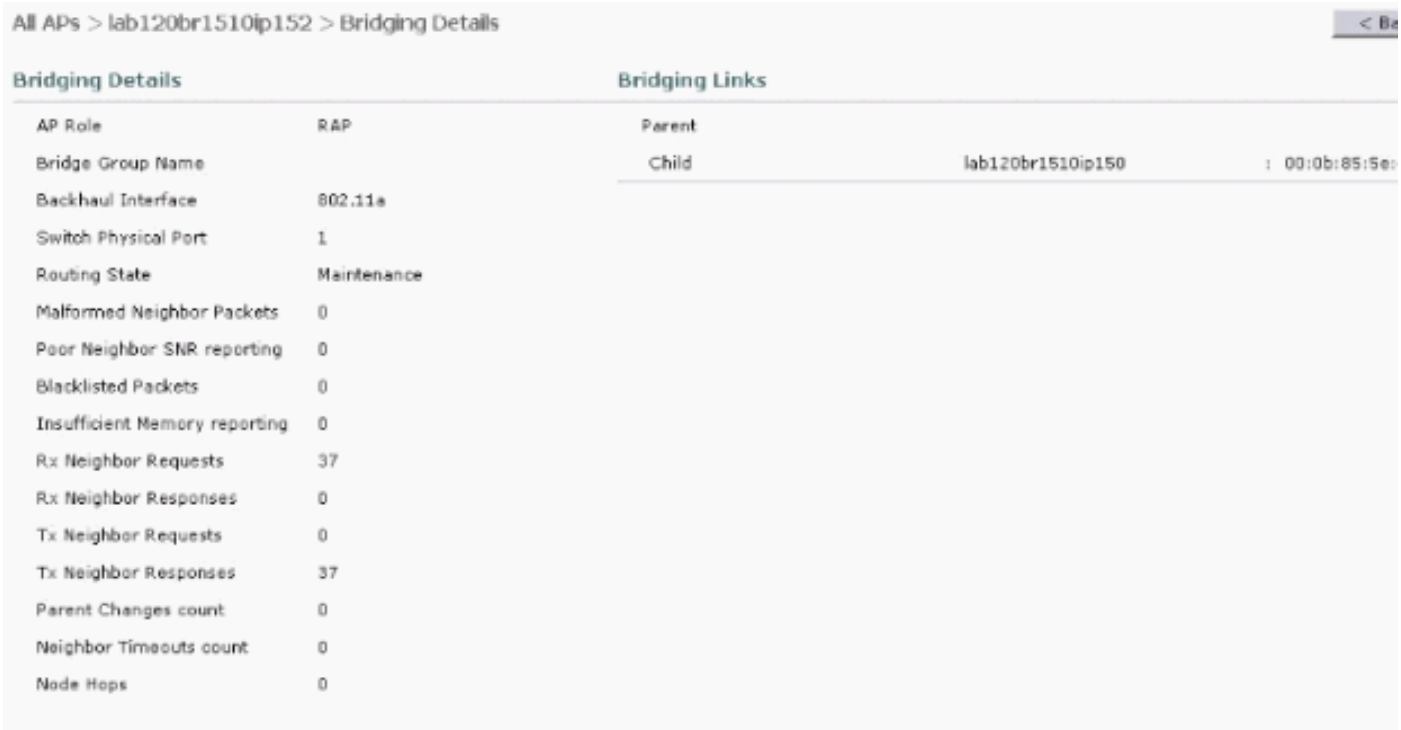
Dopo aver registrato gli AP sul WLC, è possibile visualizzarli nella scheda Wireless nella parte superiore della GUI del WLC:



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

```
(Cisco Controller) >show ap summary

AP Name             Slots  AP Model     Ethernet MAC       Location         Port

------------------  -----  ----------  -----------------  ---------------  ----

lab120br1510ip152    2     OAP1500     00:0b:85:5e:5a:80   default_location  1

lab120br1510ip150    2     OAP1500     00:0b:85:5e:40:00   default_location  1


(Cisco Controller) >
```

Fare clic su **Bridging Details** (Dettagli bridging) nella GUI per verificare il ruolo dell'access point:



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

```
(Cisco Controller) >show mesh path lab120br1510ip152
00:0B:85:5E:5A:80 is RAP

(Cisco Controller) >show mesh neigh lab120br1510ip152

AP MAC : 00:0B:85:5E:40:00

FLAGS : 160 CHILD

worstDv 255, Ant 0, channel 0, biters 0, ppiters 10

Numroutes 0, snr 0, snrUp 0, snrDown 26, linkSnr 0

adjustedEase 0, unadjustedEase 0

txParent 0, rxParent 0

poorSnr  0

lastUpdate   1150103792 (Mon Jun 12 09:16:32 2006)

parentChange 0

Per antenna smoothed snr values: 0 0 0 0

Vector through 00:0B:85:5E:40:00

(Cisco Controller) >
```

Risoluzione dei problemi

`I punti di accesso alla rete non associati al WLC` è uno dei problemi più comuni rilevati nella distribuzione della rete. Completare i seguenti controlli:

1. Verificare che l'indirizzo MAC del punto di accesso sia stato aggiunto all'elenco Mac Filter nel WLC. Questa condizione può essere rilevata in **Sicurezza > Filtro Mac**.
2. Controllare il segreto condiviso tra il RAP e il MAP. È possibile visualizzare questo messaggio nel WLC quando la chiave non corrisponde.`" LWAPP Join-Request AUTH_STRING_PAYLOAD, hash chiave BRIDGE non valido AP 00:0b:85:68:c1:d0"` **Nota:** Provare sempre a utilizzare l'opzione **Enable Zero Touch Configuration** (Abilita configurazione zero tocco), se disponibile per una versione. In questo modo la chiave per i punti di accesso mesh viene configurata automaticamente ed è possibile evitare errori di configurazione.
3. I RAP non inoltrano messaggi broadcast sulla loro interfaccia radio. Configurare quindi il server DHCP in modo che invii gli indirizzi IP tramite unicast in modo che MAP possa ottenere gli indirizzi IP inoltrati da RAP. In caso contrario, utilizzare un indirizzo IP statico per la mappa.
4. Lasciare il nome del gruppo di bridge sui valori predefiniti o accertarsi che i nomi dei gruppi di bridge siano configurati esattamente allo stesso modo nelle mappe e nei criteri di autorizzazione delle risorse corrispondenti.

Si tratta di problemi specifici dei punti di accesso Mesh. Per i problemi di connettività comuni tra il WLC e un punto di accesso, consultare il documento sulla risoluzione dei problemi di un Lightweight Access Point che non si unisce a un Wireless LAN Controller.

Comandi per la risoluzione dei problemi

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Èpossibile usare questi comandi di debug per risolvere i problemi del WLC:

- **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.

Di seguito sono riportati alcuni comandi aggiuntivi di **debug** che è possibile utilizzare per risolvere i 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 output del comando **debug lwapp events enable** WLC mostra che il LAP viene registrato sul WLC:

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

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 Received LWAPP JOIN REQUEST
from AP 00:0b:85:5e:40:00 to 06:0a:10:10:00:00 on port '1'

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 AP lab120br1510ip150: txNonce
00:0B:85:40:CF:A0 rxNonce  00:0B:85:5E:40:00

Mon Jun 12 09:04:57 2006: 00:0b:85:5e:40:00 LWAPP Join-Request MTU path from
AP 00:0b:85:5e:40:00 is 1500, remote debug mode is 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully added NPU Entry for
AP 00:0b:85:5e:40:00 (index 1) Switch IP: 192.168.120.101, Switch Port: 12223,
intIfNum 1, vlanId 0 AP IP: 192.168.120.150, AP Port: 58368, next hop
MAC: 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Successfully transmission of
LWAPP Join-Reply to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:58 2006: 00:0b:85:5e:40:00 Register LWAPP event for AP
00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE REQUEST
from AP 00:0b:85:5e:40:00 to  00:0b:85:40:cf:a3

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Updating IP info for AP 00:0b:85:5e:40:00
-- static 1, 192.168.120.150/255.255.255.0, gtw 192.168.120.1

Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 0 code 0 regstring
-A regDfromCb -A
```

```
Mon Jun 12 09:04:59 2006: spamVerifyRegDomain RegDomain set for slot 1 code 0 regstring
-A regDfromCb -A

Mon Jun 12 09:04:59 2006: spamEncodeDomainSecretPayload:Send domain secret
airespacerf<65,4d,c3,6f,88,35,cd,4d,3b,2b,bd,95,5b,42,6d,ac,b6,ab,f7,3d> to
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Config-Message to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: Running spamEncodeCreateVapPayload for SSID
'lab120wlc4402ip100'

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 AP 00:0b:85:5e:40:00 associated.
Last AP failure was due to Link Failure, reason:     STATISTICS_INFO_RES

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext:
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 0

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for
AP 00:0b:85:5e:40:00 slot 0!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CHANGE_STATE_EVENT from
AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Successfully transmission of LWAPP
Change-State-Event Response to AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 apfSpamProcessStateChangeInSpamContext:
Down LWAPP event for AP 00:0b:85:5e:40:00 slot 1

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP Down event for AP
00:0b:85:5e:40:00 slot 1!

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00

Mon Jun 12 09:04:59 2006: 00:0b:85:5e:40:00 Received LWAPP CONFIGURE COMMAND
RES from AP 00:0b:85:5e:40:00
```

Informazioni correlate

- Guida All'Implementazione Della Soluzione Cisco Mesh Networking
- Guida introduttiva: Cisco Aironet serie 1500 Lightweight Mesh Access Point per ambienti esterni
- Guida alla configurazione di Cisco Wireless LAN Controller, versione 4.0
- Pagina di supporto wireless
- Documentazione e supporto tecnico – Cisco Systems