

# Guida alla distribuzione di Mesh per ambienti interni

## Sommario

[Introduzione](#)

[Panoramica](#)

[Hardware e software supportati](#)

[Interni ed esterni](#)

[Configurazione](#)

[Modalità L3 controller](#)

[Aggiorna il controller al codice più recente](#)

[Indirizzo MAC](#)

[Registra indirizzo MAC nelle radio](#)

[Immettere l'indirizzo MAC e i nomi delle radio nel controller](#)

[Abilita filtro MAC](#)

[Installazione di Mesh L3 in ambienti interni](#)

[Definisci interfacce su controller](#)

[Ruoli radio](#)

[Nome gruppo bridge](#)

[Configurazione protezione](#)

[Installazione](#)

[Prerequisiti](#)

[Installazione](#)

[Configurazione alimentazione e canali](#)

[Controllo RF](#)

[Verifica delle interconnessioni](#)

[Sicurezza accesso console AP](#)

[Ethernet Bridging](#)

[Miglioramento nome gruppo bridge](#)

[Log - Messaggi, Sys, AP e Trap](#)

[Log messaggi](#)

[Log AP](#)

[Registri trap](#)

[Prestazioni](#)

[Test di convergenza all'avvio](#)

[Sistema colori Windows](#)

[Allarmi mesh interni](#)

[Rapporto e statistiche Mesh](#)

[Test collegamento](#)

[Test collegamento nodo-nodo](#)

[Collegamenti adiacenti punto di accesso su richiesta](#)

[Test Ping](#)

[Conclusioni](#)

[Informazioni correlate](#)

## **Introduzione**

Il Lightweight Access Point 1242/1131 è un dispositivo a due radio Wi-Fi per installazioni in interni selezionate. È un prodotto basato su LWAPP (Lightweight Access Point Protocol). Fornisce una radio a 2,4 GHz e una radio a 5,8 GHz compatibile con 802.11b/g e 802.11a. Una radio può essere utilizzata per l'accesso locale (client) per il punto di accesso (AP), mentre la seconda radio può essere configurata per il backhaul wireless. LAP1242/LAP1131 supporta architetture P2P, P2MP e mesh.

Prima di eseguire qualsiasi installazione, leggere attentamente la guida.

Questo documento descrive la distribuzione di Enterprise Wireless Mesh per reti interne. Questo documento consentirà agli utenti finali wireless di comprendere i fondamenti di Indoor Mesh, dove configurare la rete interna e come configurare la rete interna. Mesh interna è un sottoinsieme di Mesh wireless di Cisco Enterprise implementato utilizzando controller wireless e access point leggeri.

Indoor mesh è un sottoinsieme dell'architettura Enterprise mesh implementata sull'architettura Unified Wireless. La rete interna è richiesta oggi. Con la rete interna, una delle radio (generalmente 802.11b/g) e/o il collegamento Ethernet cablato viene utilizzato per il collegamento ai client, mentre la seconda radio (generalmente 802.11a) viene utilizzata per il backhaul del traffico client. Il backhaul può essere un singolo hop o su più hop. La rete interna fornisce i seguenti valori:

- Non è necessario eseguire il cablaggio Ethernet su ciascun access point.
- La porta dello switch Ethernet non è richiesta per ciascun access point.
- Connettività di rete in cui i cavi non possono fornire connettività.
- Flessibilità nell'implementazione, non limitata a 100 m da uno switch Ethernet.
- Semplice da installare in una rete wireless ad hoc.

I rivenditori di grandi dimensioni sono molto attratti dalle maglie interne per via dei risparmi sui costi del cablaggio e per le ragioni precedentemente menzionate.

Gli specialisti dell'inventario lo utilizzano per eseguire il conteggio delle scorte per rivenditori, stabilimenti di produzione e altre società. Desiderano installare rapidamente una rete Wi-Fi temporanea presso la sede del cliente per consentire la connettività in tempo reale per i dispositivi palmari. Seminari educativi, conferenze, manifattura e ospitalità sono alcuni dei luoghi in cui l'architettura a maglia interna è necessaria.

Una volta terminata la lettura di questa guida, si capirà dove usare e come configurare la rete interna. Inoltre, si capirà che la rete interna negli enclosure NEMA NON sostituisce la rete esterna. Inoltre, comprenderete la superiorità della mesh interna rispetto alla flessibilità del ruolo del collegamento (mesh single hop) utilizzata dai punti di accesso autonomi.

### **Presupposti:**

Conosci le reti wireless, l'architettura e i prodotti Cisco Unified. Conosci i prodotti Cisco Outdoor

Mesh e alcuni dei termini utilizzati per le reti mesh.

Glossario degli acronimi	
LWAPP	Lightweight Access Point Protocol: protocollo di controllo e tunneling dei dati tra i punti di accesso e il controller LAN wireless.
Controller WLAN /Controller /WLC	Controller LAN wireless: dispositivi Cisco che centralizzano e semplificano la gestione di rete di una WLAN mediante la compressione di un elevato numero di endpoint gestiti in un unico sistema unificato, consentendo un sistema di rete WLAN di informazioni intelligente unificato.
RAP	Punto di accesso principale/punto di accesso al tetto: i dispositivi wireless Cisco fungono da ponte tra il controller e gli altri punti di accesso wireless. AP collegati al controller.
MAPPA	Mesh AP (punti di accesso alla rete) - Dispositivo wireless Cisco che si connette a un dispositivo RAP o MAP via etere su una radio 802.11a e fornisce servizi ai client su una radio 802.11b/g.
Padre	Un access point (o RAP/MAP) che fornisce accesso ad altri access point via etere su una radio 802.11a.
Adiacente	Tutti i punti di accesso in una rete Mesh sono vicini e hanno vicini. Il protocollo RAP non ha un router adiacente collegato al controller.
Figlio	Un punto di accesso più lontano dal controller è sempre un elemento figlio. Un figlio avrà un padre e molti vicini in una rete

	mesh. Se il padre muore, verrà scelto il vicino successivo con il miglior valore di andamento.
SNR	Rapporto segnale/rumore
BGN	Nome gruppo bridge
EAP	Extensible Authentication Protocol
PSK	Chiave già condivisa
AWPP	Adaptive Wireless Path Protocol

## Panoramica

Il Cisco Indoor Mesh Network Access Point è un dispositivo di infrastruttura Wi-Fi a due radio per installazioni in interni selezionate. È un prodotto basato su LWAPP (Lightweight Access Point Protocol). Fornisce una radio a 2,4 GHz e una radio a 5,8 GHz compatibile con gli standard 802.11b/g e 802.11a. Una radio (802.11b/g) può essere utilizzata per l'accesso locale (client) per il punto di accesso e la seconda radio (802.11a) può essere configurata per il backhaul wireless. Fornisce un'architettura mesh interna, in cui diversi nodi (radio) comunicano tra loro tramite backhaul e forniscono anche accesso client locale. Questo punto di accesso può essere utilizzato anche per architetture di bridging point-to-point e point-to-multipoint. La soluzione Wireless Indoor Mesh Network è ideale per la copertura di grandi ambienti interni, poiché consente di ottenere velocità di trasmissione dei dati elevate e una buona affidabilità con un'infrastruttura minima. Queste sono le caratteristiche principali di base introdotte con la prima release di questo prodotto:

- Ideale in ambienti interni per un conteggio di 3 hop. Massimo 4.
- Nodo di inoltro e host per i client degli utenti finali. Una radio 802.11a è usata come interfaccia backhaul e una radio 802.11b/g per servire i client.
- Sicurezza dei punti di accesso mesh interni: supporto di EAP e PSK.
- Le MAPPE LWAPP in un ambiente mesh comunicano con i controller nello stesso modo in cui comunicano con i punti di accesso collegati a Ethernet.
- Bridging wireless point-to-point.
- Bridging wireless point-to-multipoint.
- Selezione padre ottimale. SNR, EASE e BGN
- Miglioramenti BGN. NULL e modalità predefinita.
- Accesso locale.
- Elenco nero padre. Elenco di esclusione.
- Riparazione automatica con AWPP.
- Bridging Ethernet.
- Supporto di base di Voice dalla versione 4.0.
- Selezione dinamica della frequenza.
- Anti-stranding - Failover BGN e DHCP predefinito.

**Nota:** queste funzionalità non sono supportate:

- 4.9 GHz canale di pubblica sicurezza
- Stesura intorno all'interferenza
- Scansione in background

- Accesso universale
- Supporto bridge gruppo di lavoro

## Software Mesh per interni

Il software Indoor Mesh è una versione speciale in quanto si concentra sui punti di accesso interni, in particolare sulla rete interna. In questa versione, i punti di accesso interni funzionano sia in modalità locale che in modalità bridge. Alcune delle funzioni disponibili nella release 4.1.171.0 non sono implementate in questa release. Sono stati apportati miglioramenti all'interfaccia della riga di comando (CLI), all'interfaccia grafica dell'utente (GUI - browser Web) e alla macchina a stati. L'obiettivo di questi miglioramenti è quello di ottenere informazioni preziose dal punto di vista dell'azienda relativamente a questo nuovo prodotto e alla sua fattibilità funzionale.

Miglioramenti specifici per le maglie per interni:

- **Ambiente interno** - La rete interna viene implementata utilizzando i LAP1242s e LAP1131. Questi LAP sono implementati in ambienti interni in cui il cavo Ethernet non è disponibile. L'implementazione è facile e veloce e fornisce una copertura wireless alle aree remote all'interno dell'edificio (ad esempio, centri di distribuzione al dettaglio, istruzione per seminari/conferenze, produzione, ospitalità).
- **Miglioramenti Bridge Group Name (BGN)** - Per consentire a un amministratore di rete di organizzare una rete di Indoor Mesh AP in settori specificati dall'utente, Cisco offre un meccanismo chiamato Bridge Group Name, o BGN. Il BGN, in realtà il nome del settore, determina la connessione di un access point ad altri access point con lo stesso BGN. Nel caso in cui un punto di accesso non trovi un settore adatto corrispondente al proprio BGN, opera in modalità predefinita e sceglie il miglior padre che risponde al BGN predefinito. Questa funzione ha già ricevuto un grande apprezzamento dal campo in quanto combatte contro le condizioni dell'access point isolato (se qualcuno ha mal configurato il BGN). Nella versione software 4.1.171.0, gli access point, quando si utilizza il BGN predefinito, non funzionano come nodi a rete interna e non dispongono di accesso client. È in modalità manutenzione per accedere tramite il controller e se l'amministratore non corregge il BGN, l'access point verrà riavviato dopo 30 minuti.
- **Miglioramenti della sicurezza** - Per impostazione predefinita, la sicurezza del codice Mesh interno è configurata per EAP (Extensible Authentication Protocol). Questa condizione viene definita nella RFC3748. Sebbene il protocollo EAP non sia limitato alle LAN wireless e possa essere utilizzato per l'autenticazione di LAN cablate, viene spesso utilizzato nelle LAN wireless. Quando EAP viene richiamato da un dispositivo NAS (Network Access Server) abilitato per 802.1X, ad esempio un punto di accesso wireless 802.11 a/b/g, i moderni metodi EAP possono fornire un meccanismo di autenticazione sicuro e negoziare una chiave master PMK (Pair-wise) sicura tra il client e il NAS. La chiave PMK può quindi essere utilizzata per la sessione di crittografia wireless che utilizza la crittografia TKIP o CCMP (basata su AES). Nelle versioni precedenti alla 4.1.171.0, i punti di accesso mesh esterni utilizzavano PMK/BMK per collegarsi al controller. Era un processo a tre cicli. Ora i cicli sono ridotti per una convergenza più rapida. L'obiettivo generale della sicurezza a maglia interna è fornire: Configurazione zero touch per la sicurezza del provisioning. Privacy e autenticazione dei frame di dati. Autenticazione reciproca tra la rete e i nodi. Possibilità di utilizzare i metodi EAP standard per l'autenticazione dei nodi AP mesh interni. Disaccoppiamento di LWAPP e sicurezza a maglia interna. I meccanismi di rilevamento, routing e sincronizzazione sono migliorati dall'architettura corrente per supportare gli elementi necessari per i nuovi protocolli di sicurezza. I punti di accesso mesh interni scoprono altri punti di accesso mesh eseguendo

la scansione e l'ascolto di aggiornamenti gratuiti per i vicini da altri punti di accesso mesh. I RAP o le MAPPE interne collegate alla rete pubblicizzano i parametri di sicurezza principali nei frame NEIGH\_UPD (in modo simile ai frame beacon 802.11). Al termine di questa fase, viene stabilito un collegamento logico tra un punto di accesso mesh interno e un punto di accesso radice.

- **Miglioramenti Sistema colori Windows** Sono stati aggiunti allarmi Mesh interni. È possibile generare rapporti Mesh interni che mostrano il numero di hop, il peggiore SNR, ecc. Il test di collegamento (da padre a figlio, da figlio a padre) può essere eseguito tra i nodi per fornire informazioni molto intelligenti. Le informazioni visualizzate da AP sono molto più numerose rispetto a quelle precedenti. Si ha anche la possibilità di vedere i potenziali vicini. Monitoraggio dello stato migliorato e più comodo da accedere.

## Hardware e software supportati

I requisiti hardware e software minimi per la rete interna sono:

- I Cisco LWAPP AP AIR-LAP1242AG-A-K9 e AIR-LAP1131AG-A-K9 supportano la configurazione della rete interna.
- Il software Cisco Mesh release 2 supporta Enterprise Mesh (prodotti per interni ed esterni). Può essere installato solo su Cisco Controller, Cisco 440x/210x e WISM.
- Il software Cisco Enterprise Mesh release 2 può essere scaricato dal sito Cisco.com.

## Interni ed esterni

Queste sono alcune delle differenze principali tra la rete interna ed esterna:

	<b>Rete interna</b>	<b>Mesh per esterni</b>
Ambiente	SOLO per interni, hardware classificato per interni	SOLO per esterni, hardware resistente
Hardware	AP interno con LAP1242 e LAP1131AG	AP esterno con LAP15xx e LAP152x
Livelli di potenza	2,4 Ghz:20 dbm 5,8 Ghz:17 dbm	2,4 Ghz:28dbm 5,8 Ghz:28dbm
Dimensioni celle	Circa 150 ft	Circa 300 metri
Altezza implementazione	12 piedi dal suolo	30-40 piedi dal suolo

## Configurazione

Prima di iniziare qualsiasi implementazione, soprattutto se è stato ricevuto nuovo hardware, verificare attentamente la guida.

## [Modalità L3 controller](#)

I punti di accesso mesh interni possono essere implementati come rete L3.



## [Aggiorna il controller al codice più recente](#)

Attenersi alla seguente procedura:

1. Per aggiornare Mesh Release 2 su una rete mesh interna, la rete deve essere in esecuzione sulla versione 4.1.185.0 o Mesh Release1, disponibile su Cisco.com.
2. Scaricare il codice più recente per il controller sul server TFTP. Dall'interfaccia GUI del controller, fare clic su **Comandi > Scarica file**.
3. Selezionare il tipo di file come **codice** e fornire l'indirizzo IP del server TFTP. Definite il percorso e il nome del file.



**Nota:** utilizzare il server TFTP che supporta trasferimenti di dimensioni superiori a 32 MB. Ad esempio, **ftpd32**. In Percorso file put **"/** come mostrato.

4. Al termine dell'installazione del nuovo firmware, usare il comando **show sysinfo** nella CLI per verificare che il nuovo firmware sia installato.

```
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS

System Name..... CiscoMesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs

Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit
Number of VLANs..... 2
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 3

Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
```

**Nota:** ufficialmente Cisco non supporta il downgrade ai controller.

## Indirizzo MAC

L'uso del filtro MAC è obbligatorio. Questa funzionalità ha reso la soluzione Cisco Indoor Mesh una vera e propria "Zero Touch". A differenza delle release precedenti, la schermata Mesh non dispone più dell'opzione MAC Filtering.



**Nota:** il filtro MAC è abilitato per impostazione predefinita.

## Registra indirizzo MAC nelle radio

In un file di testo, registrare gli indirizzi MAC di tutte le radio AP a rete interna distribuite nella rete. L'indirizzo MAC è disponibile sul retro degli access point. Ciò consente di eseguire test futuri, in quanto la maggior parte dei comandi CLI richiede l'immissione dell'indirizzo MAC o dei nomi degli access point con il comando. È inoltre possibile modificare il nome degli access point in un nome più facilmente memorizzabile, ad esempio "build number-pod number-AP type: ultimi quattro caratteri esadecimale dell'indirizzo MAC."

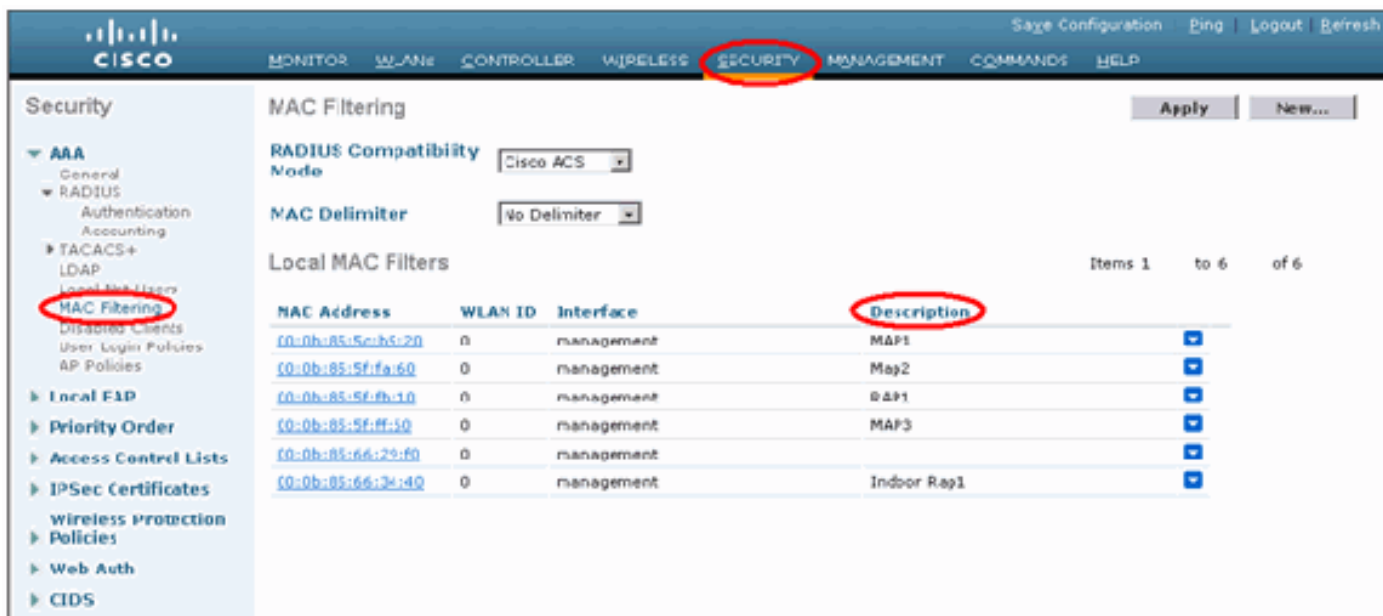
## Immettere l'indirizzo MAC e i nomi delle radio nel controller

Il controller Cisco gestisce un elenco di indirizzi MAC di autorizzazione dei punti di accesso interni. Il controller risponde solo alle richieste di rilevamento provenienti dalle radio interne visualizzate nell'elenco delle autorizzazioni. Immettere gli indirizzi MAC di tutte le radio che si tendono a utilizzare nella rete sul controller.

Sull'interfaccia GUI del controller, andare su **Security**, e fare clic sul **filtro MAC** sul lato sinistro



della schermata. Fare clic su **New** (Nuovo) per immettere gli indirizzi MAC, come mostrato di seguito:



Inoltre, immettere i nomi delle radio per maggiore comodità in **Descrizione** (ad esempio, posizione, numero AP, ecc.) La descrizione può essere utilizzata anche per indicare dove le radio sono state installate per facilitare il riferimento in qualsiasi momento.

## [Abilita filtro MAC](#)

Il filtro MAC è abilitato per impostazione predefinita.

È inoltre possibile scegliere la modalità di protezione EAP o PSK nella stessa pagina.

Dall'interfaccia GUI dello switch, usare questo percorso:

Percorso interfaccia GUI: **Wireless > Mesh interna**

La modalità di protezione può essere verificata solo nella CLI con questo comando:

(Cisco Controller) > **show network**

```
(Cisco Controller) >show network
RF-Network Name..... iMesh
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Ucast
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Disable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC Filter Config..... Enable
Bridge Security Mode..... EAP
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
Apple Talk..... Disable
AP Fallback..... Enable
--More-- or (q)uit
Web Auth Redirect Ports..... 80
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

## [Installazione di Mesh L3 in ambienti interni](#)

Per una rete Mesh L3 interna, configurare gli indirizzi IP delle radio se non si intende utilizzare il server DHCP (interno o esterno).

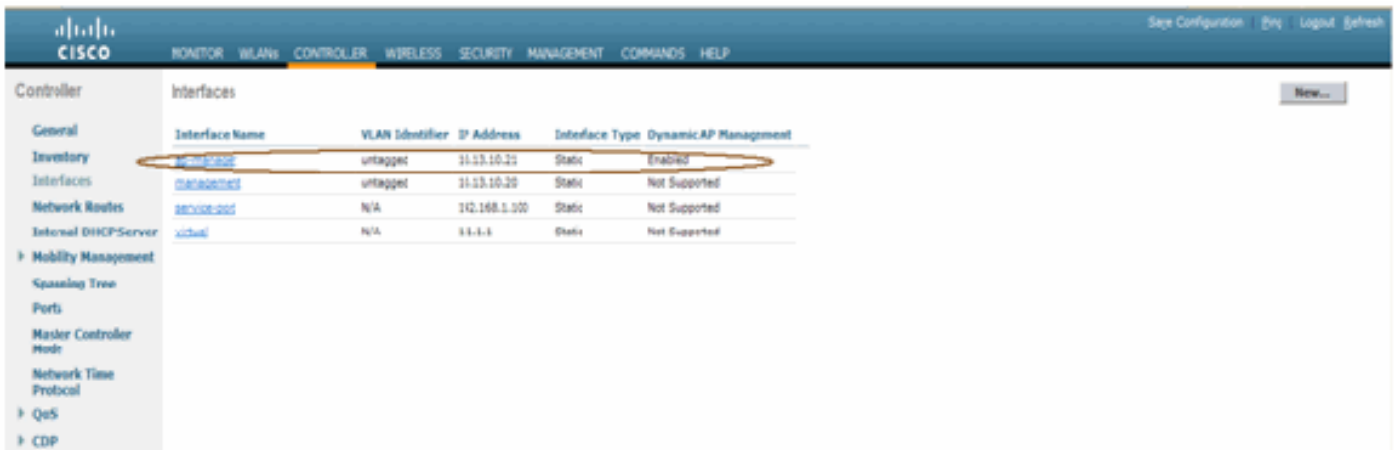
Per una rete Mesh L3 interna, se si desidera utilizzare un server DHCP, configurare il controller in modalità L3. Salvare la configurazione e riavviare il controller. Accertarsi di configurare l'opzione 43 sul server DHCP. Dopo il riavvio del controller, i nuovi access point connessi riceveranno il proprio indirizzo IP dal server DHCP.

## Definisci interfacce su controller

### AP Manager

Per una distribuzione L3, è necessario definire **AP-manager**. AP Manager funge da indirizzo IP di origine per le comunicazioni tra il controller e gli access point.

Percorso: **Controller > Interfacce > ap-manager > modifica.**



The screenshot shows the Cisco Controller web interface. The 'CONTROLLER' tab is selected. On the left, the 'Interfaces' menu item is highlighted. The main area displays a table of interfaces:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
ap-manager	untagged	10.13.10.21	Static	Enabled
management	untagged	10.13.10.20	Static	Not Supported
service-port	N/A	10.168.1.100	Static	Not Supported
vlan1	N/A	11.1.1	Static	Not Supported

All'interfaccia **AP-manager** deve essere assegnato un indirizzo IP nella stessa subnet e VLAN dell'interfaccia di gestione.



The screenshot shows the configuration page for the 'ap-manager' interface. The 'CONTROLLER' tab is selected. The left sidebar shows the 'Interfaces' menu item highlighted. The main area displays the configuration for the 'ap-manager' interface:

**General Information**

Interface Name: ap-manager  
MAC Address: 00:18:73:34:4b:63

**Interface Address**

VLAN Identifier: 0  
IP Address: 10.13.10.21  
Netmask: 255.255.255.0  
Gateway: 10.13.10.10

**Physical Information**

Port Number: 1  
Backup Port: 0  
Active Port: 1  
Enable Dynamic AP Management:

**DHCP Information**

Primary DHCP Server: 10.13.10.10  
Secondary DHCP Server:

**Access Control List**

ACL Name: none

Note: Changing the interface parameters causes the VLANs to be temporarily disabled and this may result in loss of connectivity for some clients.

## Ruoli radio

Con questa soluzione è possibile assegnare due ruoli radio principali:

- Root Access Point (RAP): la radio con cui si desidera connettersi al controller (tramite switch) assumerà il ruolo di RAP. I RAP dispongono di una connessione cablata abilitata per LWAPP al controller. Un RAP è un nodo padre di qualsiasi rete a rete con bridging o a rete interna. Un controller può disporre di uno o più RAP, ognuno associato a reti wireless uguali o diverse. Per la stessa rete mesh interna per la ridondanza, possono esistere più RAP.
- Punto di accesso Mesh interno (MAP) - La radio che non ha una connessione cablata al controller assume il ruolo di punto di accesso a rete interno. Questo punto di accesso era denominato in precedenza punto di accesso principale. Le MAPPE hanno una connessione wireless (attraverso l'interfaccia backhaul) a forse altre MAPPE e infine a un RAP e quindi al controller. Le mappe possono anche avere una connessione Ethernet cablata a una LAN e fungere da endpoint bridge per tale LAN (utilizzando una connessione P2P o P2MP). Questa condizione può verificarsi contemporaneamente, se configurato correttamente come un bridge Ethernet. I MAP servono i client sulla banda non utilizzata per l'interfaccia Backhaul.

La modalità predefinita per un punto di accesso è MAP.

**Nota:** i ruoli radio possono essere impostati tramite GUI o CLI. Gli access point verranno riavviati dopo la modifica del ruolo.

**Nota:** è possibile usare la CLI del controller per preconfigurare i ruoli radio su un access point, a condizione che l'access point sia fisicamente connesso allo switch o che l'access point sia visibile sullo switch come RAP o MAP.

```
(Cisco Controller) >config ap role ?
rootAP          RootAP role for the Cisco Bridge.
meshAP          MeshAP role for the Cisco Bridge.

(Cisco Controller) >config ap role meshAP ?
<Cisco AP>      Enter the name of the Cisco AP.

(Cisco Controller) >config ap role meshAP LAP1242-2
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

## Nome gruppo bridge

I nomi dei gruppi di bridge (BGN) controllano l'associazione dei punti di accesso. I BGN possono raggruppare logicamente le radio per evitare che due reti sullo stesso canale comunichino tra loro. Questa impostazione è utile anche se nella rete sono presenti più RAP nello stesso settore (area). Il BGN è una stringa di massimo dieci caratteri.

Un nome di gruppo di bridge impostato in fabbrica viene assegnato nella fase di produzione (VALORE NULL). Non è visibile a voi. Di conseguenza, anche senza un BGN definito, le radio possono comunque collegarsi alla rete. Se nella rete sono presenti due RAP nello stesso settore (per una maggiore capacità), è consigliabile configurare i due RAP con lo stesso BGN, ma su canali diversi.

**Nota:** il nome del gruppo di bridge può essere impostato dalla CLI e dalla GUI del controller.

```
(Cisco Controller) >config ap bridgegroupname set ?
<bridgegroupname> Set bridgegroupname on Cisco AP.
```

Dopo aver configurato il BGN, l'access point viene ripristinato.

**Nota:** il BGN deve essere configurato con molta attenzione su una rete attiva. È consigliabile iniziare sempre dal nodo più lontano (ultimo nodo) e spostarsi verso il punto di accesso. Il motivo è che se si inizia a configurare il BGN in un punto qualsiasi al centro del multihop, i nodi al di là di questo punto verranno scartati poiché questi nodi avranno un BGN diverso (vecchio BGN).

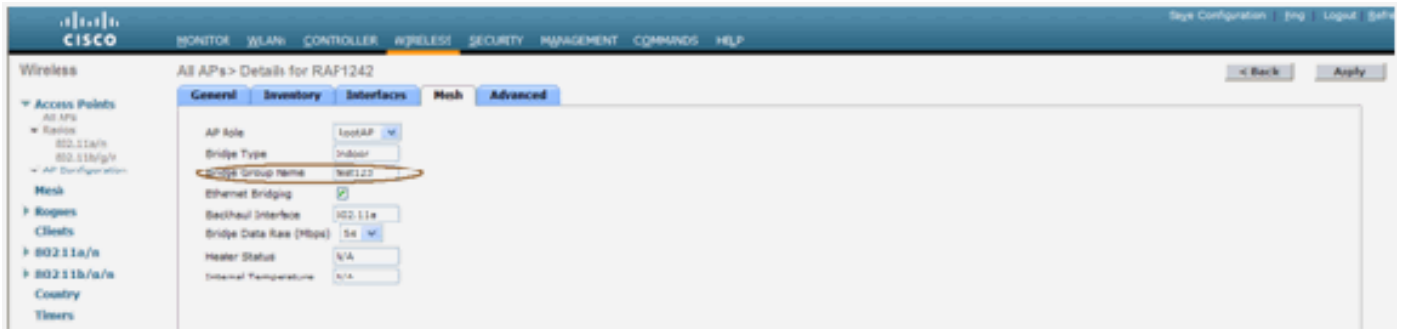
È possibile verificare il BGN usando questo comando CLI:

```
(Cisco Controller) > show ap config general
```

```
(Cisco Controller) >show ap config general RAP1242
Cisco AP Identifier..... 0
Cisco AP Name..... RAP1242
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-AB 802.11a:-A3
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 00:18:74:fa:7d:1f
IP Address Configuration..... DHCP
IP Address..... 10.13.13.11
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.13.13.10
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch..... J2106-1
Secondary Cisco Switch.....
Tertiary Cisco Switch.....
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Bridge
--More-- or (q)uit
AP Role ..... RootAP
Ethernet Bridging ..... Enabled
Bridge GroupName ..... test123
Public Safety ..... Disabled
Remote AP Debug ..... Disabled
S/W Version ..... 4.1.175.19
Boot Version ..... 12.3.7.1
Mini IOS Version ..... 3.0.51.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Disabled
PoE Power Injector MAC Addr..... Disabled
Number Of Slots..... 2
AP Model..... AIR-LAP1242AG-A-K9
IOS Version..... 12.4(20070808:082741)
Reset Button..... Enabled
AP Serial Number..... FTX1035B3RH
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Disabled
Console Login Name.....
Console Login State..... Unknown
AP Up Time..... 0 days, 02 h 43 m 38 s
AP LWAPP Up Time..... 0 days, 02 h 42 m 43 s
--More-- or (q)uit
Join Date and Time..... Sun Aug 19 11:59:07 2007
Join Taken Time..... 0 days, 00 h 00 m 24 s
Ethernet Port Duplex..... Unknown
Ethernet Port Speed..... Unknown
```

Inoltre, è possibile configurare o verificare il BGN utilizzando l'interfaccia utente del controller:

Percorso: **Wireless** > **Tutti gli access point** > **Dettagli**.



Questa nuova versione mostra anche le informazioni ambientali dell'access point.

## Configurazione protezione

La modalità di sicurezza mesh interna predefinita è EAP. Ciò significa che, a meno che non si configurino questi parametri sul controller, le mappe non verranno aggiunte:



## CLI di configurazione Mesh EAP per ambienti interni

```
(Cisco Controller) >config mesh local-auth enable
enable Local Auth

(Cisco controller) >config advanced eap ?
identity-request-timeout Configures EAP-Identity-Request Timeout in seconds.
identity-request-retries Configures EAP-Identity-Request Max Retries.
key-index Configure the key index used for dynamic WEP (802.1x) unicast key (PTK).
max-login-ignore-identity-response Configure to ignore the same username count reaching max in the E
AP identity response
request-timeout Configures EAP-Request Timeout in seconds.
request-retries Configures EAP-Request Max Retries.
```

Se è necessario rimanere in modalità PSK, utilizzare questo comando per tornare alla modalità PSK:

```
(Cisco Controller) >config mesh security psk ?
(Cisco Controller) >config mesh security psk

All Mesh AP will be rebooted
Are you sure you want to start? (y/N)n
```

## Comandi EAP mesh interni show

In modalità EAP, è possibile controllare i seguenti comandi **show** per verificare l'autenticazione MAP:



(Cisco Controller) >show network

```
RF Network Name..... jaggi123
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable Mode: Mcast 224.1.1.1
Ethernet Broadcast Mode..... Disable
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
ARP Unicast Mode..... Disabled
Cisco AP Default Master..... Disable
Mgmt Via Wireless Interface..... Enable
Mgmt Via Dynamic Interface..... Disable
Bridge MAC filter Config..... Disable
Bridge Security Mode..... EAP otherwise PSK
Mesh Multicast Mode..... 802.11b/g/n
Mesh Full Sector DFS..... Enable
Over The Air Provisioning of AP's..... Enable
Mobile Peer to Peer Blocking..... Disable
AP Fallback..... Enable
Web Auth Redirect Ports..... 80
--More-- or (q)uit
Fast SSID Change..... Disabled
802.3 Bridging..... Disable
```

(Cisco Controller) >show wlan 0

(Cisco Controller) >show wlan 0

```
WLAN Identifier..... 0
Profile Name..... Mesh_profile
Network Name (SSID)..... Mesh_ssid
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 2
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
Interface..... management
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
--More-- or (q)uit
IPv6 Support..... Disabled
Radio Policy..... All
Local EAP Authentication..... Enabled (Profile 'prfMaP1500L1EAuth93')
Security
  802.11 Authentication:..... Open System
  Static WEP Keys..... Disabled
  802.1x..... Disabled
  Wi-Fi Protected Access (WPA/WPA2)..... Enabled
    WPA (SSN IE)..... Disabled
    WPA2 (RSN IE)..... Enabled
    TKIP Cipher..... Disabled
    AES Cipher..... Enabled
    Auth Key Management
  802.1x..... Enabled
  PSK..... Disabled
  CCKM..... Disabled
  CKIP..... Disabled
  IP Security Passthru..... Disabled
  Web Based Authentication..... Disabled
  Web-Passthrough..... Disabled
  Conditional Web Redirect..... Disabled
  Auto Anchor..... Disabled
--More-- or (q)uit
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60

Mobility Anchor List
WLAN ID IP Address Status
```

(Cisco Controller) >show local-auth config

```

(Cisco Controller) >show local-auth config
User credentials database search order:
  Primary ..... Local DB
Timer:
  Active timeout ..... 300
Configured EAP profiles:
EAP Method configuration:
  EAP-FAST:
    Server key ..... <hidden>
    TTL for the PAC ..... 10
    Anonymous provision allowed ..... Yes
    Authority ID ..... 436973636f000000000000000000000000
    Authority Information ..... Cisco A-ID
(Cisco Controller) >show advanced eap
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 1
EAP-Request Max Retries..... 2

```

```
(Cisco Controller) >show advanced eap
```

## Comandi EAP Mesh debug per interni

Per eseguire il debug di eventuali problemi in modalità EAP, utilizzare questi comandi nel controller:

```

(Cisco Controller) >debug dot1x all enable
(Cisco Controller) >debug aaa all enable

```

## Installazione

### Prerequisiti

Nel controller deve essere in esecuzione la versione consigliata del codice. Fare clic su **Monitor** per verificare la versione del software. La stessa condizione può essere verificata tramite CLI.

```

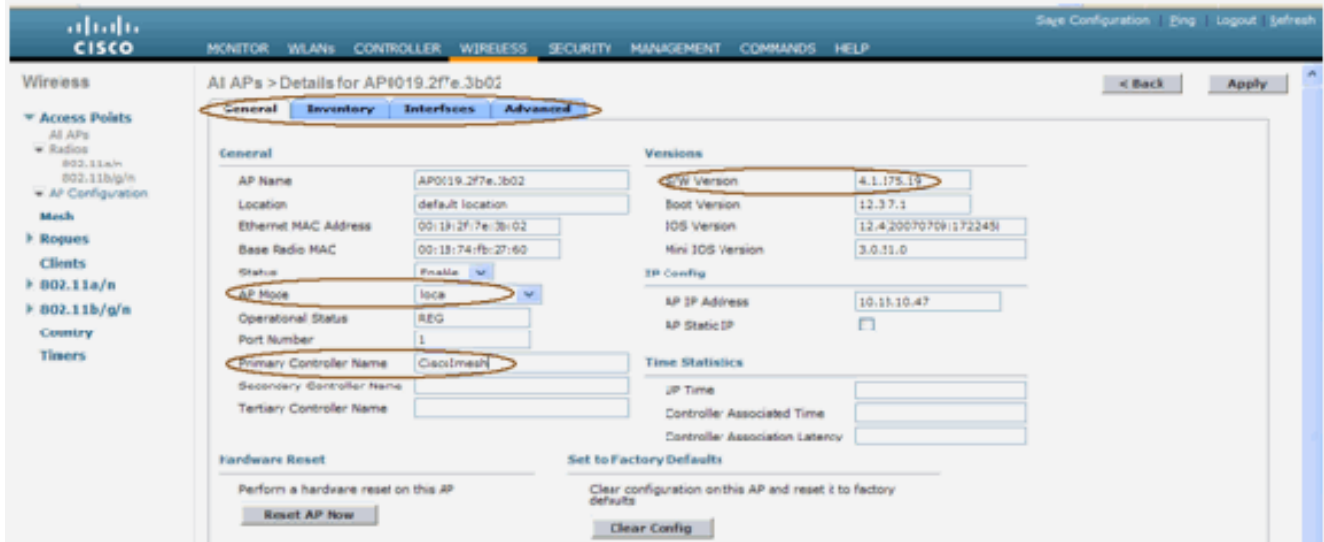
(Cisco Controller) >show sysinfo
Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 4.1.175.19
RTOS Version..... 4.1.175.19
Bootloader Version..... 4.0.206.0
Build Type..... DATA + WPS
System Name..... CiscoMesh
System Location.....
System Contact.....
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.13.10.20
System Up Time..... 1 days 22 hrs 3 mins 35 secs
Configured Country..... US - United States
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C
State of 802.11b network..... Enabled
State of 802.11a Network..... Enabled
--More-- or (q)uit.....
Number of VLANs..... 2
3rd Party Access Point Support..... Disabled
Number of Active Clients..... 3
Burned-in MAC Address..... 00:18:73:34:48:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK

```

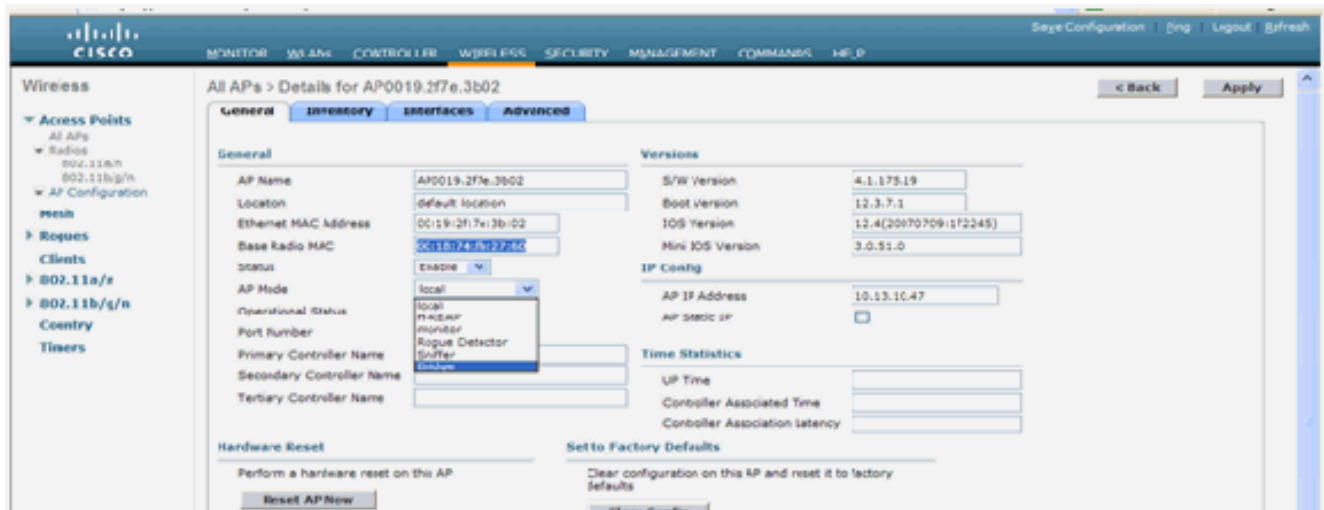
Sistemi quali il server DHCP, il server ACS e il server WCS devono essere raggiungibili.

## Installazione

1. Collegare tutti i LAP (1131AG/1242AG) a una rete di layer 3 sulla stessa subnet dell'indirizzo IP di gestione. Tutti gli access point verranno collegati al controller come access point in modalità locale. In questa modalità, assegnare ai punti di accesso il nome del controller primario, il nome del controller secondario e il nome del controller terziario.

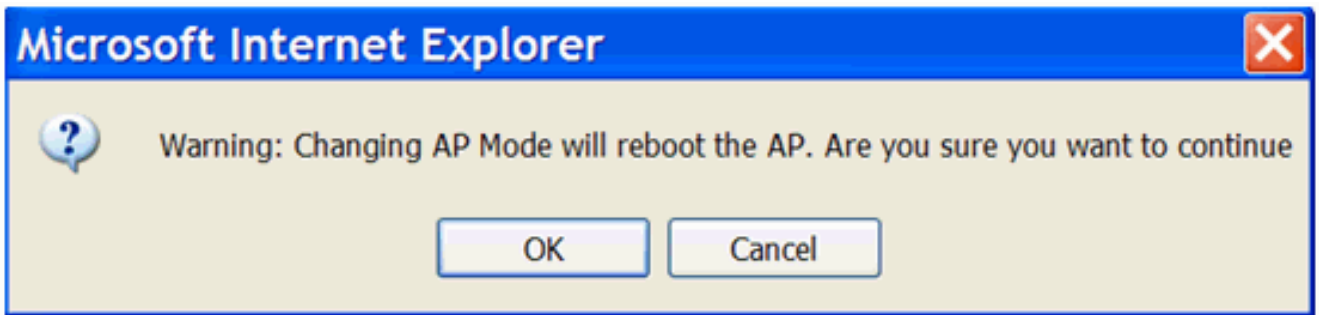


2. Acquisire l'indirizzo MAC della radio base dell'access point (ad esempio, 00:18:74: fb 27:60).
3. Aggiungere l'indirizzo MAC dell'access point per il join dell'access point in modalità bridge.
4. Fare clic su **Security > MAC-filtering > New** (Sicurezza > Filtro MAC > Nuovo).
5. Aggiungere l'indirizzo MAC copiato e assegnare un nome agli access point nell'elenco dei filtri MAC e nell'elenco degli access point.
6. Selezionare **Bridge** dall'elenco **Modalità AP**.



7. Verrà richiesto di confermare il riavvio dell'access point.





8. L'access point si riavvierà e si unirà al controller in modalità bridge. La nuova finestra PA avrà una scheda aggiuntiva: MESH. Fare clic sulla scheda **MESH** per verificare il ruolo, il tipo di bridge, il nome del gruppo di bridge, il bridging Ethernet, l'interfaccia backhaul, la velocità dati bridge e così via.



9. In questa finestra, accedere all'elenco dei ruoli PA e scegliere il ruolo appropriato. In questo caso, il ruolo predefinito è MAP. Il nome del gruppo di bridge è vuoto per impostazione predefinita. L'interfaccia di backhaul è 802.11a. La velocità dei dati di ponte (ossia, la velocità dei dati di backhaul) è di 24 Mbps.
10. Collegare al controller l'access point che si desidera utilizzare come dispositivo RAP. Distribuire le radio (MAP) nelle posizioni desiderate. Accendere le radio. Dovrebbe essere possibile vedere tutte le radio sul controller.

```
(Cisco Controller) >show ap summ
Number of APs..... 3
AP Name           Slots  AP Model          Ethernet MAC      Location          Port  Country
-----
RAP1242           2      AIR-LAP1242AG-A-K9  00:18:74:fa:7d:1f default location  1     US
LAP1242-1         2      AIR-LAP1242AG-A-K9  00:1b:2b:a7:ad:bf default location  1     US
LAP1242-2         2      AIR-LAP1242AG-A-K9  00:14:1b:59:07:af default location  1     US
```

11. Cercare di avere condizioni di visibilità tra i nodi. Se non esistono condizioni di visibilità, creare isolamenti di zona di Fresnel per ottenere condizioni di prossimità del sito.
12. Se più controller sono connessi alla stessa rete mesh interna, è necessario specificare il nome del controller primario in ogni nodo. In caso contrario, il controller visualizzato per primo verrà considerato come principale.

## Configurazione alimentazione e canali

Il canale backhaul può essere configurato su un RAP. Le mappe si sintonizzeranno sul canale RAP. L'accesso locale può essere configurato in modo indipendente per le mappe.

Dall'interfaccia dello switch, seguire il percorso: **Wireless > radio 802.11a > configurare**.



**Nota:** il livello di potenza Tx predefinito sul backhaul è il livello di potenza più alto (Livello 1) e Radio Resource Management (RRM) è OFF per impostazione predefinita.

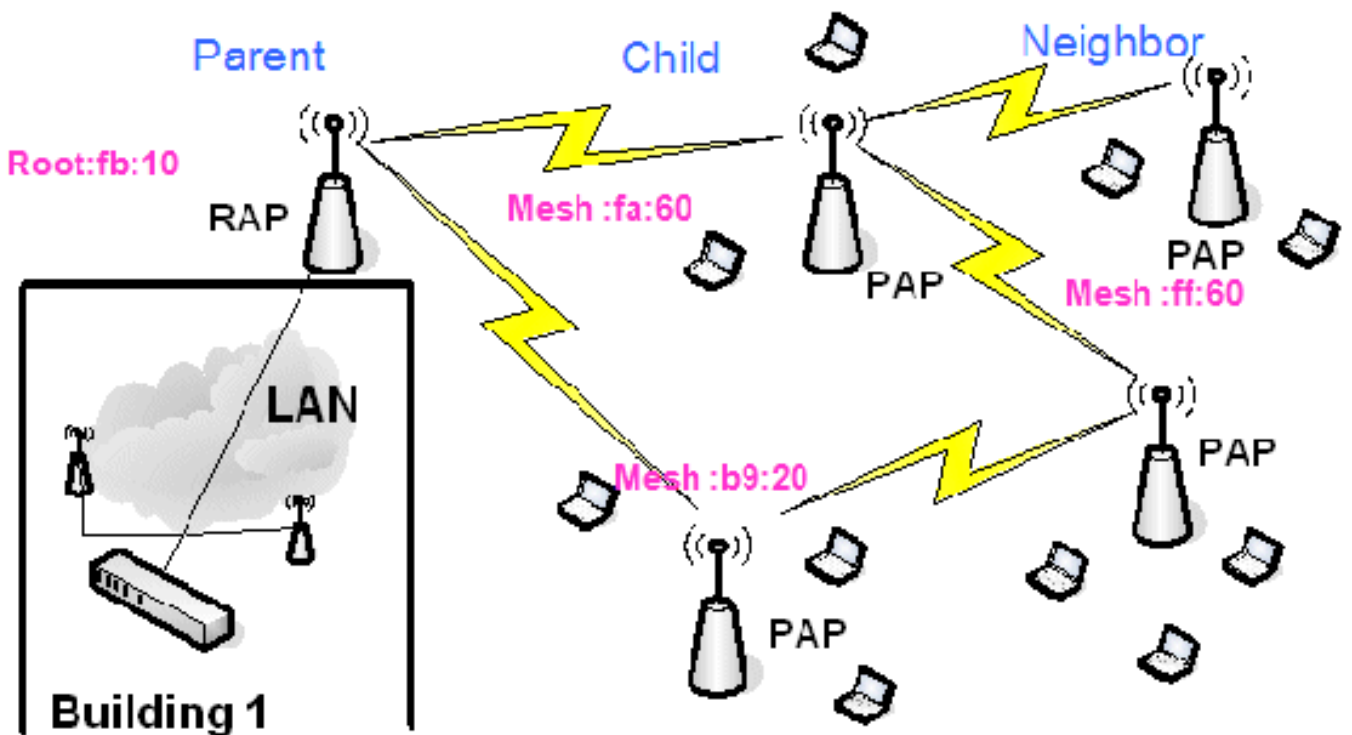
Se si collocano i RAP, è consigliabile utilizzare canali adiacenti alternativi in ogni RAP. Ciò riduce le interferenze tra i canali.

## Controllo RF

In una rete mesh interna è necessario verificare la relazione padre-figlio tra i nodi. **Hop** è un collegamento wireless tra le due radio. La relazione padre-figlio cambia quando si attraversa la rete. Dipende da dove ti trovi nella rete a maglia interna.

La radio più vicina al controller in una connessione wireless (hop) è la **principale** della radio sull'altro lato dell'hop. In un sistema con più hop è presente una struttura ad albero in cui il nodo connesso al controller è un RAP (**padre**). Il nodo immediato sull'altro lato del primo hop è un nodo **Child**, mentre i nodi successivi nel secondo hop successivo sono i **nodi adiacenti** per quel particolare nodo padre.

**Figura 1: Rete a due hop**



Nella Figura 1, i nomi dei punti di accesso sono menzionati per comodità. Nella schermata successiva, si sta indagando sul **RAP(fb:10)**. Questo nodo può vedere (nell'implementazione effettiva) i punti di accesso Mesh interni (**fa:60 & b9:20**) come figli e **MAP ff:60** come adiacenti.

Dall'interfaccia GUI dello switch, seguire il percorso: **Wireless > Tutti gli access point > Rap1 > Informazioni router adiacente.**

Mesh Type	AP Name/Radio Mac	Base Radio Mac
Child	Map1	00:06:85:5C:B9:20
Child	Map2	00:06:85:5F:FA:60
Default Neighbor	Map3	00:06:85:5F:FF:60

Assicuratevi che le relazioni padre-figlio siano stabilite e mantenute correttamente per la rete mesh interna.

### Verifica delle interconnessioni

**show Mesh** è un comando informativo per verificare l'interconnettività nella rete.

È necessario fornire questi comandi in ogni nodo (AP) utilizzando la CLI di Controller e caricare i risultati in un file di Word o di testo nel sito di caricamento.

```
(Cisco Controller) >show mesh ?
env          Show mesh environment.
neigh       Show AP neigh list.
path        Show AP path.
stats       Show AP stats.
secbh-stats Show Mesh AP secondary backhaul stats.
per-stats   Show AP Neighbor Packet Error Rate stats.
queue-stats Show AP local queue stats.
security-stats Show AP security stats.
config      Show mesh configurations.
secondary-backhaul Show mesh secondary-backhaul
client-access Show mesh backhaul with client access.
public-safety Show mesh public safety.
background-scanning Show mesh background-scanning state.
cac         Show mesh cac.
```

Nella rete mesh interna, scegliere un collegamento con più hop ed eseguire questi comandi a partire dal RAP. Carica il risultato dei comandi nel sito di caricamento.

Nella sezione successiva, tutti questi comandi sono stati emessi per la rete a rete mesh interna a due hop mostrata nella Figura 1.

### [Mostra percorso mesh interno](#)

Questo comando mostra gli indirizzi MAC, i ruoli radio dei nodi, il rapporto segnale/rumore in dB per Uplink/Downlink (SNRUp, SNRDown) e il rapporto SNR collegamento in dB per un particolare percorso.

```
(Cisco Controller) >show mesh path RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
RAP1242 is a Root AP.
(Cisco Controller) >show mesh path LAP1242-2
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-1 56 29 29 27 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 56 41 32 34 0x86b UPDATED NEIGH PARENT BEACON
RAP1242 is a Root AP.
```

### [Mostra riepilogo router adiacenti mesh interni](#)

Questo comando mostra gli indirizzi MAC, le relazioni padre-figlio e gli SNR Uplink/Downlink in dB.

```
(Cisco Controller) >show mesh neigh ?
detail      Show Link rate neigh detail.
summary     Show Link rate neigh summary.
(Cisco Controller) >show mesh neigh summary RAP1242
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 0 0 0 0x860 BEACON
LAP1242-1 56 0 33 0 0x960 CHILD BEACON

(Cisco Controller) >show mesh neigh summary LAP1242-1
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
-----
LAP1242-2 56 30 29 28 0x961 UPDATED CHILD BEACON
RAP1242 56 43 46 31 0x86b UPDATED NEIGH PARENT BEACON
```

A questo punto, dovrebbe essere possibile visualizzare le relazioni tra i nodi della rete e verificare la connettività RF visualizzando i valori SNR per ogni collegamento.

## Sicurezza accesso console AP

Questa funzione fornisce una protezione avanzata per l'accesso alla console dell'access point. Per utilizzare questa funzione è necessario un cavo console per l'access point.

Sono supportati:

- Una CLI per eseguire il push della combinazione ID utente/password nell'access point specificato:

```
(Cisco Controller) >config ap username Cisco password Cisco ?
all           Configures the Username/Password for all connected APs.
<Cisco AP>   Enter the name of the Cisco AP.
```

- Un comando CLI per inviare la combinazione nome utente/password a tutti gli access point registrati sul controller:

```
(Cisco Controller) >config ap username Cisco password Cisco all
```

Con questi comandi, la combinazione di ID utente e password inviata dal controller viene mantenuta durante il ricaricamento sugli access point. Se un access point viene cancellato dal controller, non è disponibile alcuna modalità di accesso di protezione. L'access point genera una trap SNMP con esito positivo. L'access point genererà anche una trap SNMP in caso di errore di accesso alla console per tre volte consecutive.

## Ethernet Bridging

Per motivi di sicurezza, la porta Ethernet sulle mappe è disabilitata per impostazione predefinita. Può essere abilitato solo configurando Ethernet Bridging sul RAP e le rispettive MAP.

Di conseguenza, Ethernet Bridging deve essere abilitato per due scenari:

- Quando si desidera utilizzare i nodi mesh interni come ponti.
- Quando si desidera collegare qualsiasi dispositivo Ethernet (come PC/laptop, videocamera, ecc.) sulla MAPPA utilizzando la porta Ethernet.

Percorso: **Wireless** > Fare clic su un punto di accesso > **Mesh**.



È disponibile un comando CLI che può essere utilizzato per configurare la distanza tra i nodi che eseguono il bridging. Provare a collegare un dispositivo Ethernet come una videocamera ad ogni hop e verificare le prestazioni.

## Miglioramento nome gruppo bridge

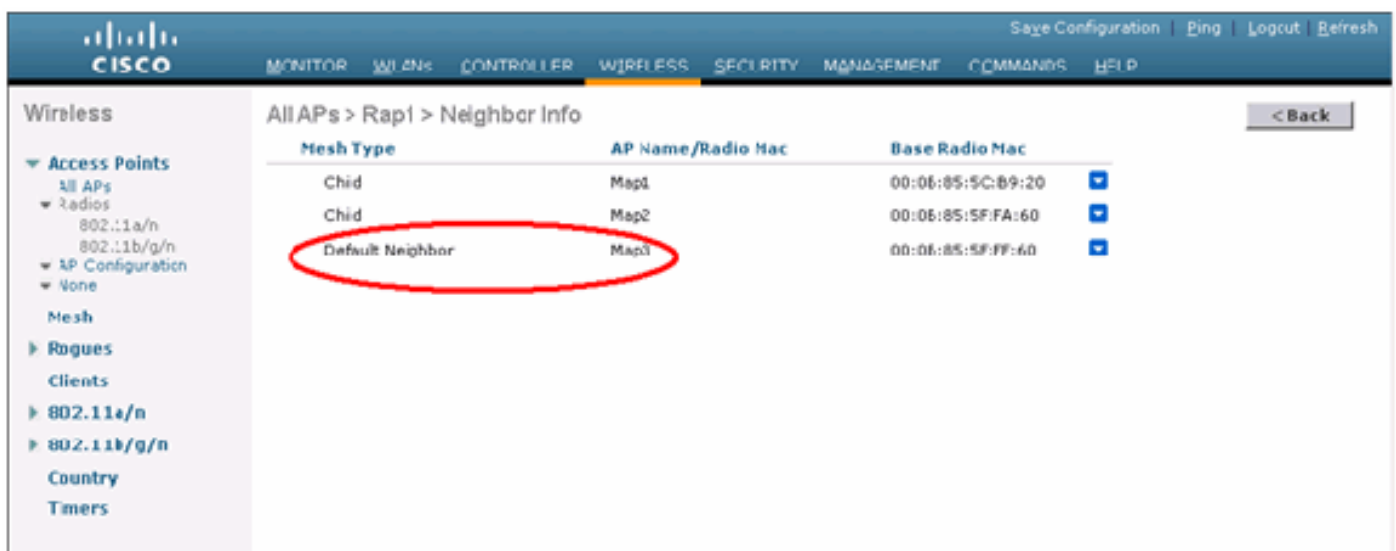
È possibile che un access point sia stato configurato in modo errato con un "nomegruppoponte" per il quale non era previsto. A seconda della struttura della rete, questo punto di accesso può essere o non essere in grado di raggiungere e trovare il settore o la struttura corretta. Se non riesce a raggiungere un settore compatibile, può diventare isolato.

Per ripristinare un punto di accesso bloccato, il concetto di nome del gruppo di bridge predefinito è stato introdotto con il codice 3.2.xx.x. L'idea di base è che un access point che non è in grado di connettersi a nessun altro access point con il nome del gruppo di bridge configurato, tenti di connettersi con "default" (la parola) come nome del gruppo di bridge. Tutti i nodi che eseguono la versione 3.2.xx.x e versioni successive del software accettano altri nodi con questo nome di gruppo di bridge.

Questa funzionalità consente inoltre di aggiungere un nuovo nodo o un nodo configurato in modo errato a una rete in esecuzione.

Se si dispone di una rete in esecuzione, selezionare un access point preconfigurato con un BGN diverso e collegarlo alla rete. Il punto di accesso verrà visualizzato nel controller utilizzando il valore BGN "predefinito" dopo aver aggiunto l'indirizzo MAC nel controller.

```
(CiscoController) >show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 4
8, linkSnr 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B), snrUp 72, snrDown 63,
linkSnr 57
00:0B:85:5F:FB:10 is RAP
```



The screenshot shows the Cisco Wireless Controller GUI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The left sidebar shows a tree view with 'Wireless' expanded, containing 'Access Points', 'Radios', 'AP Configuration', 'Mesh', 'Rogues', 'Clients', '802.11a/n', '802.11b/g/n', 'Country', and 'Timers'. The main content area is titled 'All APs > Rapi > Neighbor Info' and contains a table with the following data:

Mesh Type	AP Name/Radio Mac	Base Radio Mac
Child	Map1	00:0B:85:5C:89:20
Child	Map2	00:0B:85:5F:FA:60
<b>Default Neighbor</b>	<b>Map3</b>	00:0B:85:5F:FF:60

L'access point che utilizza il valore predefinito BGN può agire come un normale access point Mesh interno che associa i client e forma relazioni padre-figlio Mesh interna.

Nel momento in cui l'access point che utilizza il valore BGN predefinito trova un altro elemento padre con il valore BGN corretto, passa a tale elemento.

## Log - Messaggi, Sys, AP e Trap



## [Log messaggi](#)

Abilita il livello di reporting per i log dei messaggi. Dalla CLI del controller, usare questo comando:

```
(Cisco Controller) >config msglog level ?
critical      Critical hardware or software Failure.
error        Non-Critical software error.
security     Authentication or security related error.
warning      Unexpected software events.
verbose      Significant system events.

(Cisco Controller) >config msglog level verbose
```

Per visualizzare i log dei messaggi, eseguire questo comando dalla CLI del controller:

```
(Cisco Controller) >show msglog

Message Log Severity Level ..... VERBOSE
Mon Jul 11 01:42:08 2005 [SECURITY] apf_foreignap.c 765: Received a packet for
which no AP was configured from 00:0F:B5:93:71:E7 on port 0.
Fri Jul 8 06:12:02 2005 [ERROR] spam_radius.c 93: spamRadiusProcessResponse: A
P Authorization failure for 00:0b:85:0e:04:80
Fri Jul 8 05:40:15 2005 [ERROR] spam_twr.c 501: Did not receive heartbeat reply
from AP 00:0b:85:0e:05:80
Fri Jul 8 05:38:45 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:05:80
Fri Jul 8 05:38:40 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:14:00
Fri Jul 8 05:38:40 2005 Previous message occurred 5 times
Fri Jul 8 05:33:54 2005 [ERROR] spam_lrad.c 1310: Validation of Config Request
failed from AP 00:0b:85:0e:05:80
Fri Jul 8 05:32:23 2005 [ERROR] poe.c 449: poeInitPowerSupply : poePortResync
returned FAILURE.
Fri Jul 8 05:32:17 2005 [ERROR] dhcpd.c 78: dhcp server: binding to 0.0.0.0
Fri Jul 8 05:32:17 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11a swi
tch group reset
Fri Jul 8 05:32:16 2005 [ERROR] rrmgroup.c 733: Airewave Director: 802.11bg sw
itch group reset
Fri Jul 8 05:32:16 2005 Previous message occurred 2 times
Fri Jul 8 05:31:19 2005 [CRITICAL] osapi_sem.c 794: Error! osapiMutexTake cal
```

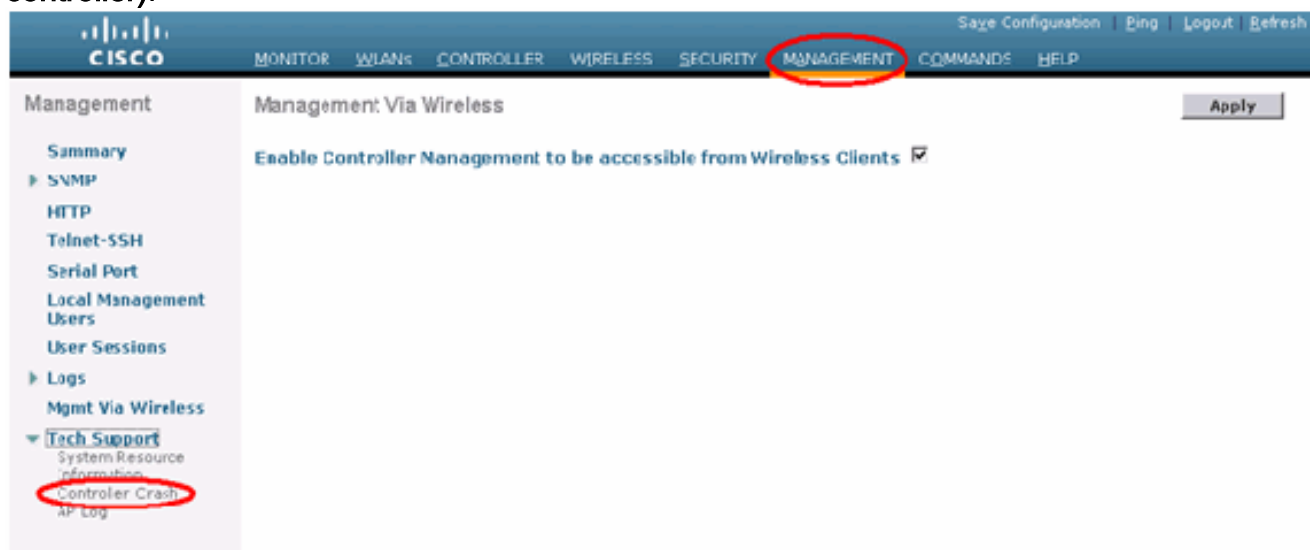
Per caricare i log dei messaggi, usare l'interfaccia GUI del controller:

1. Fare clic su **Commands > Upload**.



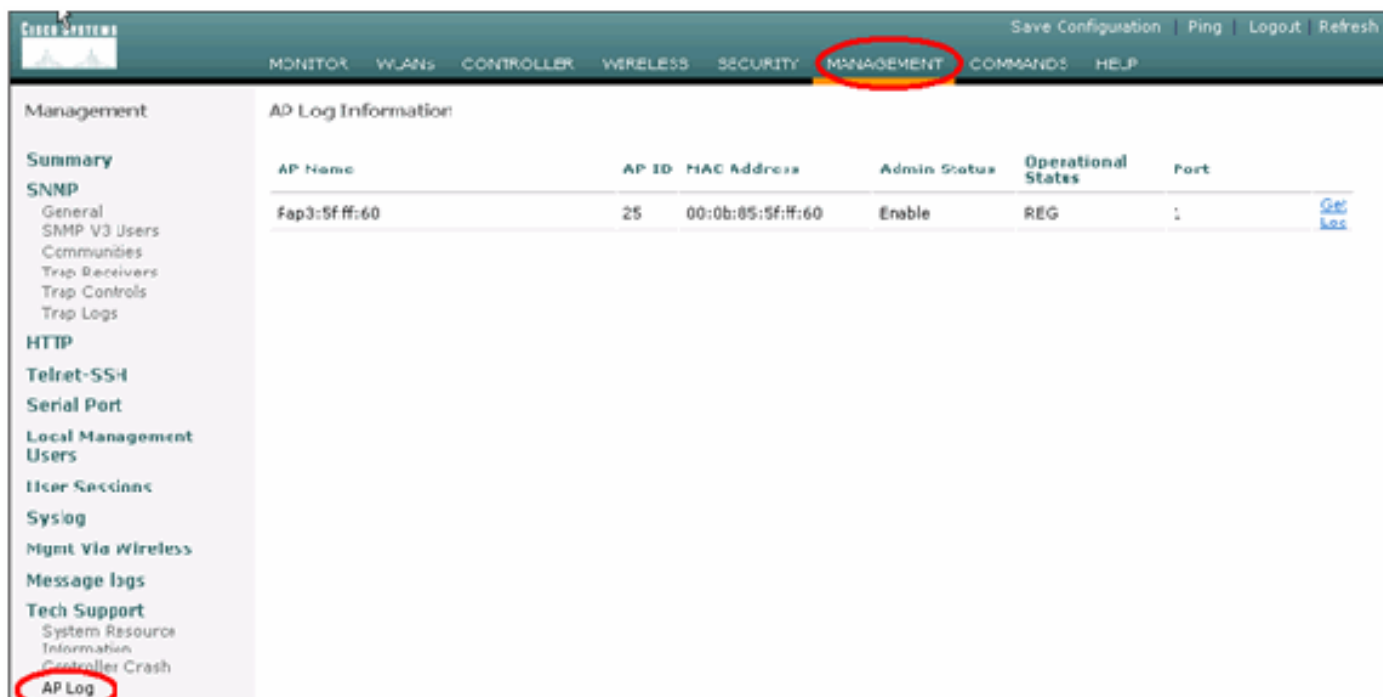
2. Immettere le informazioni sul server TFTP. In questa pagina sono disponibili diverse opzioni

per il caricamento e si desidera inviare i file seguenti: Log messaggi Registro eventi Registro trap File di arresto anomalo (se presente) Per controllare i file di arresto anomalo (Crash), fare clic su **Management (Gestione) > Controller Crash (Arresto anomalo controller)**.



## [Log AP](#)

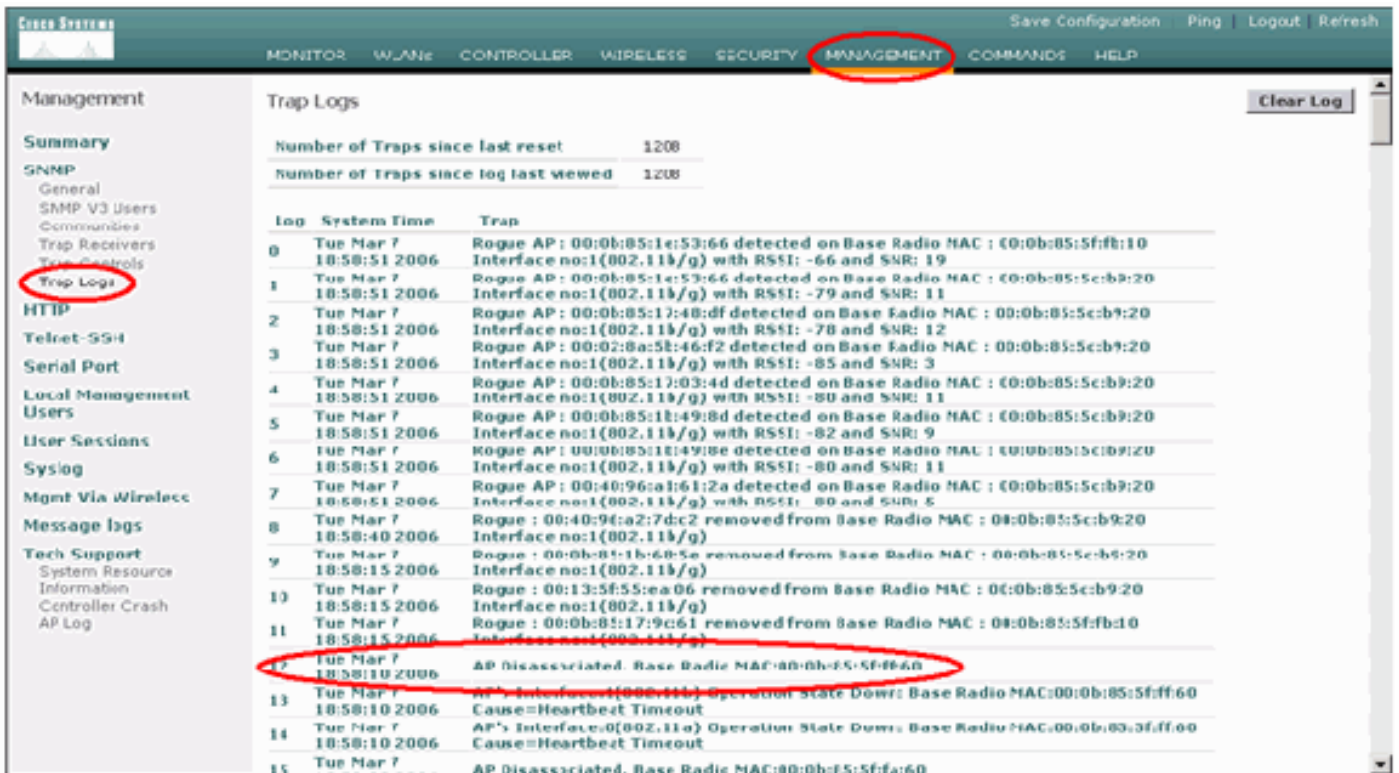
Andare a questa pagina dell'interfaccia utente sul controller per controllare i log dell'access point per l'eventuale access point locale:



## [Registri trap](#)

Andare a questa pagina dell'interfaccia utente del controller e controllare i log delle trap:





## Prestazioni

### Test di convergenza all'avvio

La convergenza è il tempo impiegato da un RAP/MAP per stabilire una connessione LWAPP stabile con un controller WLAN a partire dal momento del primo avvio, come indicato di seguito:

Test di convergenza	Tempo di convergenza (min:sec)			
	RAP	MAP1	MAP2	MAP3
Aggiornamento immagine	2:34	3:50	5:11	6:38
Riavvio controller	0:38	0:57	1:12	1:32
Accensione rete mesh interna	2:44	3:57	5:04	6:09
Riavvio RAP	2:43	3:57	5:04	6:09
MAP re-join		3:58	5:14	6:25
Modifica MAP dell'elemento padre (stesso canale)		0:38		

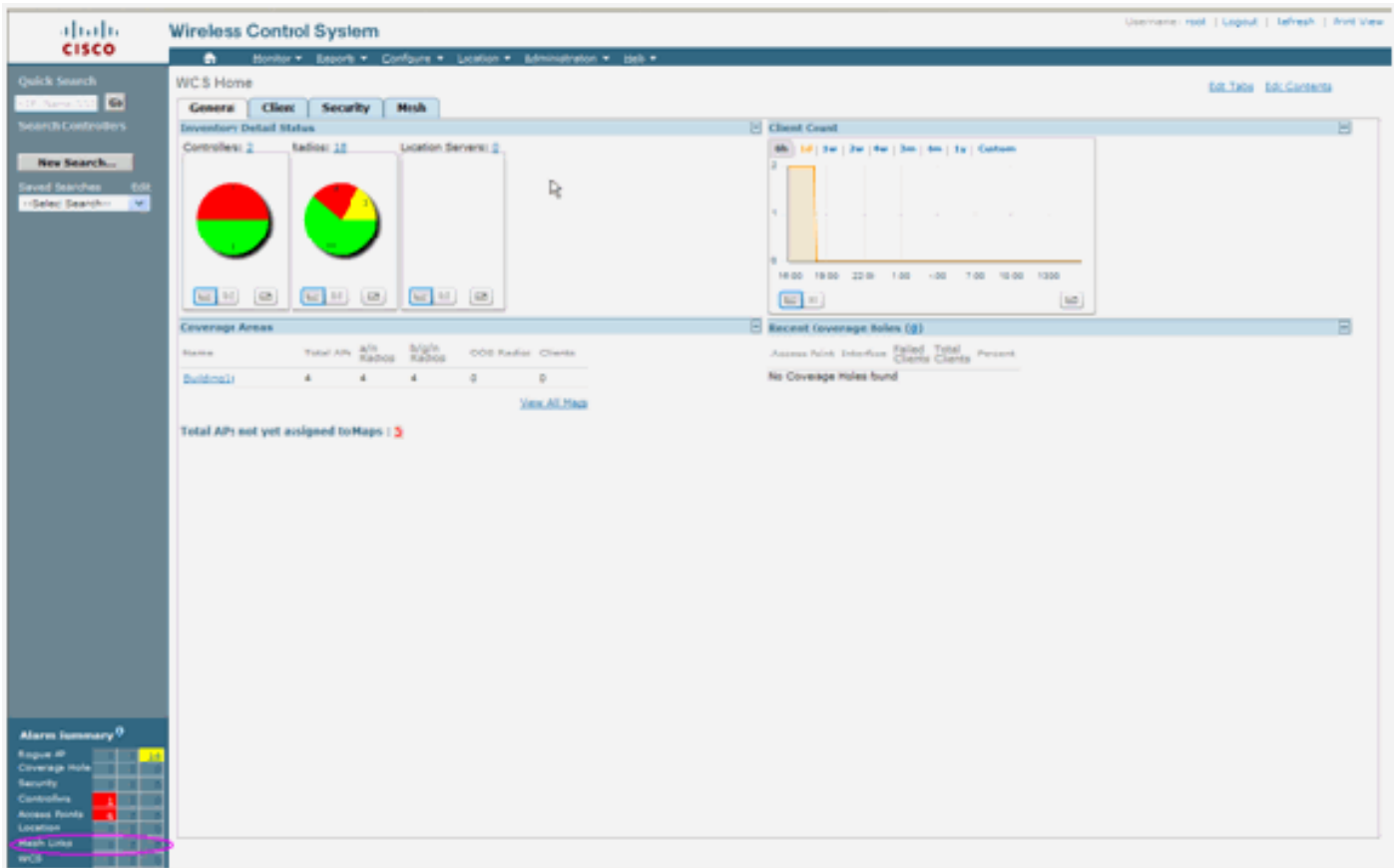
## Sistema colori Windows

### Allarmi mesh interni

Il sistema WCS genererà questi allarmi ed eventi relativi alla rete mesh interna in base alle trap provenienti dal controller:

- SNR collegamento insufficiente
- Elemento padre modificato
- Figlio spostato
- MAPPE spesso le modifiche principali
- Evento porta console
- Errore di autorizzazione MAC
- Errori di autenticazione
- Padre figlio escluso

Fare clic su **Collegamenti mesh**. Mostrerà tutti gli allarmi relativi ai collegamenti a rete interna.



I seguenti allarmi si applicano ai collegamenti mesh interni:

- Link SNR insufficiente - Questo allarme viene generato se il link SNR scende al di sotto di 12 db. L'utente non può modificare questa soglia. Se viene rilevato un SNR insufficiente sul collegamento backhaul per figlio/padre, viene generata la trap. La trap conterrà il valore SNR e gli indirizzi MAC. La gravità dell'allarme è maggiore. Il rapporto SNR (segnale-rumore) è importante perché un'elevata forza del segnale non è sufficiente a garantire buone prestazioni del ricevitore. Il segnale in ingresso deve essere più forte di qualsiasi rumore o interferenza presente. Ad esempio, è possibile che il segnale sia molto forte e che le prestazioni wireless siano ancora scarse in presenza di forti interferenze o di un elevato livello di rumore.
- Padre modificato: questo allarme viene generato quando il figlio viene spostato in un altro padre. Quando il padre viene perso, il figlio si unisce a un altro padre e invia a WCS una trap contenente gli indirizzi MAC del padre precedente e del nuovo padre. Gravità allarme: Informativo.
- Bambino spostato: questo allarme viene generato quando il sistema WCS riceve una trappola per bambini perduti. Quando l'access point padre rileva la perdita di un elemento figlio e non è in grado di comunicare con tale elemento figlio, invia a WCS una trap perduta per l'elemento

figlio. La trap conterrà l'indirizzo MAC figlio. Gravità allarme: Informativo.

- Il padre MAP viene modificato frequentemente. Questo allarme viene generato se il punto di accesso Mesh interno cambia frequentemente il padre. Quando MAP parent-change-counter supera la soglia entro una determinata durata, invia una trap a WCS. La trap conterrà il numero di volte in cui le modifiche MAP verranno apportate e la durata dell'ora. Se ad esempio sono state apportate 5 modifiche entro 2 minuti, la trap verrà inviata. Gravità allarme: Informativo.
- Padre escluso figlio: questo allarme viene generato quando un figlio viene inserito in una blacklist di un padre. Un figlio può inserire in una lista nera un padre quando non è riuscito ad autenticarsi nel controller dopo un numero fisso di tentativi. Il figlio ricorda il padre in blacklist e, quando si unisce alla rete, invia la trap che contiene l'indirizzo MAC padre in blacklist e la durata del periodo della blacklist.

Allarmi diversi dai collegamenti a rete interna:

- Accesso alla porta della console: la porta della console consente al cliente di modificare il nome utente e la password per ripristinare il punto di accesso esterno bloccato. Tuttavia, per impedire a qualsiasi utente autorizzato l'accesso all'access point, il servizio WCS deve inviare un allarme quando qualcuno tenta di accedere. Questo allarme è richiesto per fornire protezione in quanto il punto di accesso è fisicamente vulnerabile quando è situato all'esterno. Questo avviso viene generato se l'utente ha eseguito correttamente il login alla porta della console AP o se ha avuto un errore per tre volte consecutive.
- Errore di autorizzazione MAC - Questo allarme viene generato quando l'access point tenta di unirsi alla rete interna ma non esegue l'autenticazione perché non è presente nell'elenco dei filtri MAC. Il sistema WCS riceverà una trap dal controller. La trap conterrà l'indirizzo MAC dell'access point che non ha superato l'autorizzazione.

## Rapporto e statistiche Mesh

Riportiamo la relazione migliorata e il quadro statistico dal 4.1.185.0:

- Nessun percorso alternativo
- Hop nodo mesh
- Statistiche errori pacchetti
- Statistiche pacchetti
- Hop nodo peggiore
- Collegamenti SNR peggiori

Wireless Control System

Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Help

Mesh Reports

Mesh No Alternate Parent

Mesh Node Hops

Mesh Packet Error Stats

Mesh Packet Stats

Mesh Worst Node Hops

Mesh Worst SNR Links

Alarm Summary

Rogue AP	0	191
Coverage Hole	0	0
Security	0	0
Controllers	0	0
Access Points	0	2
Mesh Links	0	0
Location	0	0

Mesh No Alternate Parent

-- Select a command -- GO

Report Title	Schedule	Last Run Time	Next Scheduled Run
<input type="checkbox"/> test	Disabled		<a href="#">Run Now</a>

### [Nessun percorso alternativo](#)

Il punto di accesso mesh interno in genere ha più di un router adiacente. Nel caso in cui un punto di accesso con rete interna perda il collegamento padre, l'accesso deve essere in grado di trovare l'elemento padre alternativo. In alcuni casi, se non ci sono vicini mostrati, l'AP non potrà andare da nessun altro genitore se perde i suoi genitori. È fondamentale per l'utente sapere quali punti di accesso non dispongono di padri alternativi. In questo report vengono elencati tutti gli access point che non dispongono di altri access point adiacenti oltre al padre corrente.

### [Hop per nodi mesh interni](#)

Questo report mostra il numero di hop lontani dal punto di accesso radice (RAP). È possibile creare il report in base ai seguenti criteri:

- AP per controller
- AP per piano

### [Frequenze errori pacchetti](#)

Gli errori dei pacchetti possono essere causati da interferenze e perdite di pacchetti. Il calcolo della frequenza degli errori dei pacchetti si basa sui pacchetti inviati e su quelli inviati correttamente. La frequenza degli errori del pacchetto viene misurata sul collegamento backhaul e viene raccolta sia per i router adiacenti che per quelli padre. L'access point invia periodicamente le informazioni sul pacchetto al controller. Non appena il padre cambia, l'access point invia le informazioni sull'errore del pacchetto raccolto al controller. Per impostazione predefinita, WCS esegue il polling delle informazioni sugli errori del pacchetto dal controller ogni 10 minuti e le memorizza nel database per un massimo di 7 giorni. In Sistema colori Windows la frequenza degli errori del pacchetto viene visualizzata sotto forma di grafico. Il grafico degli errori dei pacchetti si

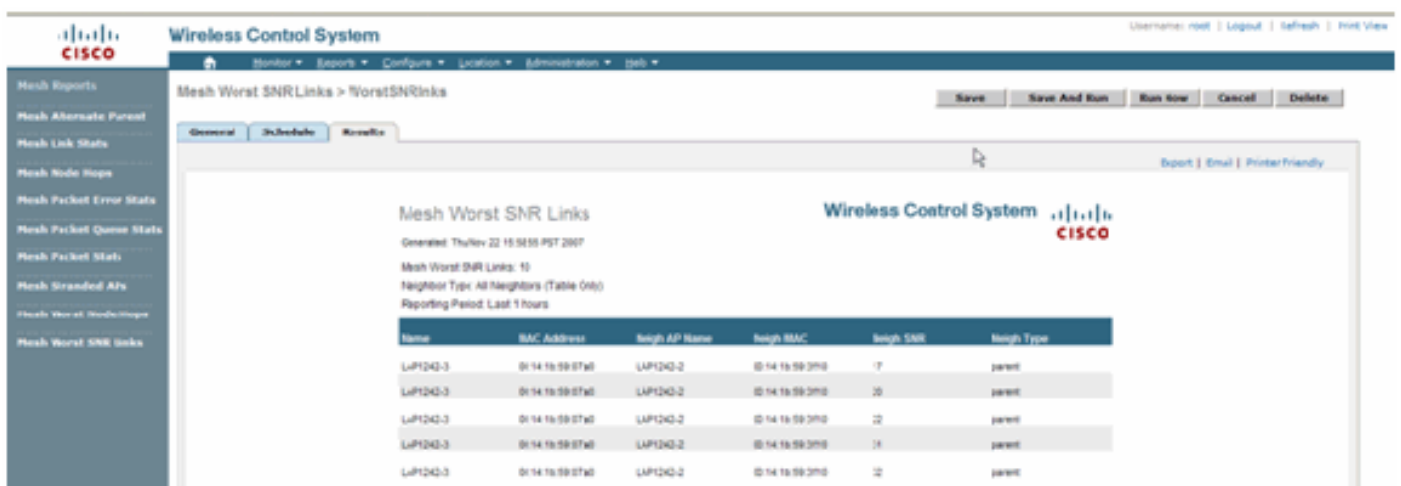
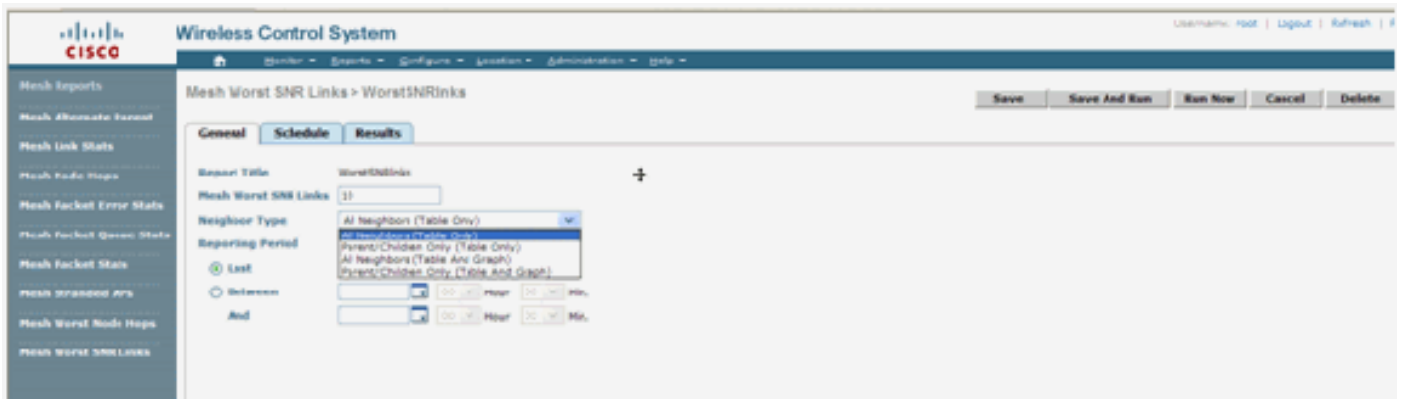
basa sui dati cronologici memorizzati nel database.

## [Statistiche pacchetti](#)

Questo report mostra i valori dei contatori dei pacchetti di trasmissione totali dei router adiacenti e dei pacchetti totali dei router adiacenti trasmessi correttamente. È possibile creare il report in base a determinati criteri.

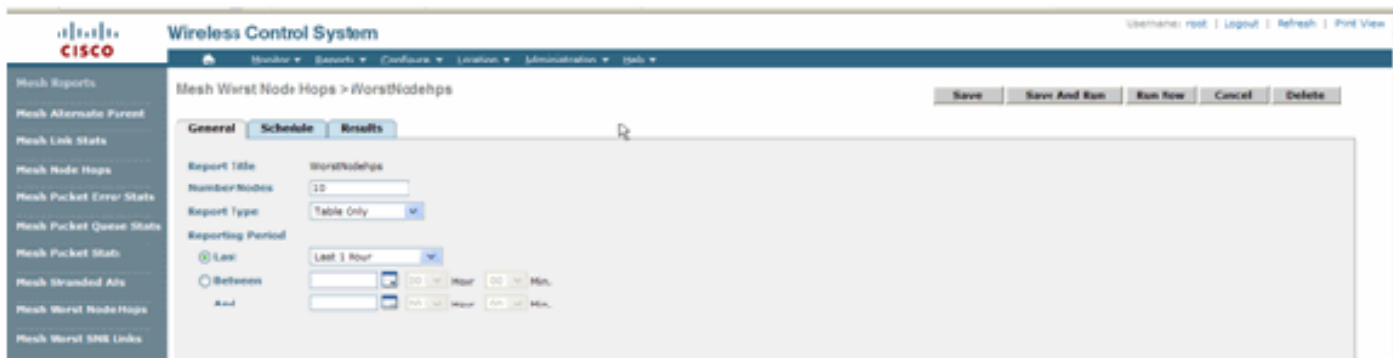
## [I collegamenti SNR peggiori](#)

I problemi di rumore possono verificarsi in momenti diversi e il rumore può aumentare a velocità diverse o durare per periodi di tempo diversi. Nella figura seguente viene illustrato come creare un report sia per Radio a che per b/g, nonché per interfacce selettive. Per impostazione predefinita, nel report vengono elencati i 10 collegamenti SNR peggiori. È possibile scegliere tra 5 e 50 collegamenti peggiori. Il report può essere generato per l'ultima ora, le ultime 6 ore, l'ultimo giorno, gli ultimi 2 giorni e fino a 7 giorni. Per impostazione predefinita, il polling dei dati viene eseguito ogni 10 minuti. I dati vengono conservati nel database per un massimo di sette giorni. Il criterio di selezione Tipo router adiacente può essere Tutti i vicini, Solo padre/figli.

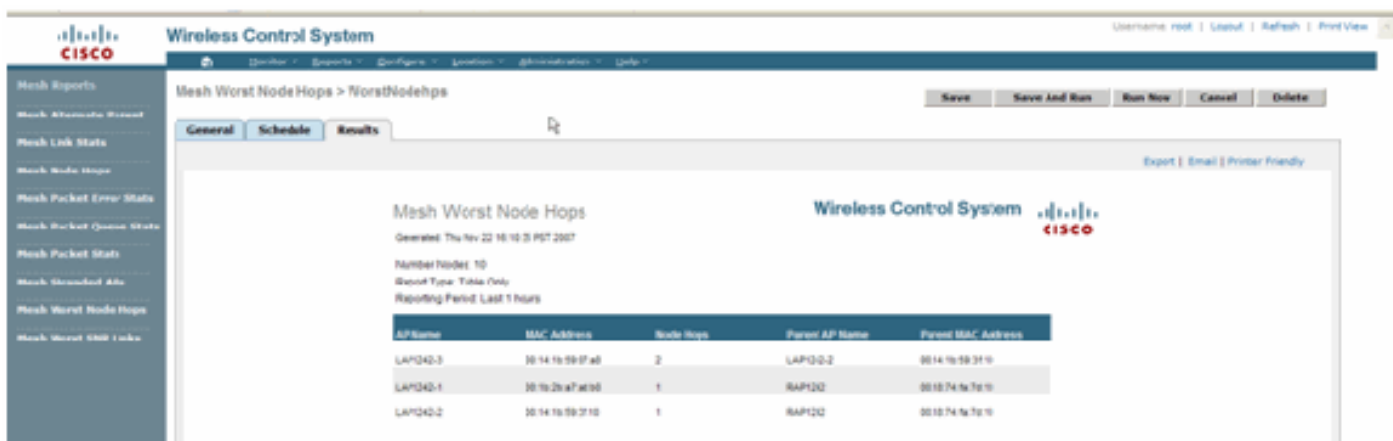


## [Hop del nodo peggiori](#)

In questo report vengono elencati per impostazione predefinita i 10 punti di accesso peggiori. Se gli access point sono troppo lontani, i collegamenti potrebbero essere molto deboli. L'utente può isolare i punti di accesso che hanno molti hop lontani dal punto di accesso principale e adottare le misure appropriate. È possibile scegliere di modificare il criterio **Numero di nodi** tra 5 e 50. I criteri di filtro **Tipo di rapporto** riportati in questa figura possono essere Solo tabella o Tabella e grafico.



Nella figura seguente viene illustrato il risultato dell'ultimo report:



## [Statistiche protezione](#)

Le statistiche di Indoor Mesh Security vengono visualizzate nella pagina dei dettagli dell'access point sotto la sezione Bridging info. Una voce nella tabella Statistiche di sicurezza MeshNodeInterno viene creata quando un nodo mesh interno figlio si associa o esegue l'autenticazione a un nodo Mesh interno padre. Le voci vengono rimosse quando il nodo Mesh interna viene dissociato dal controller.

## [Test collegamento](#)

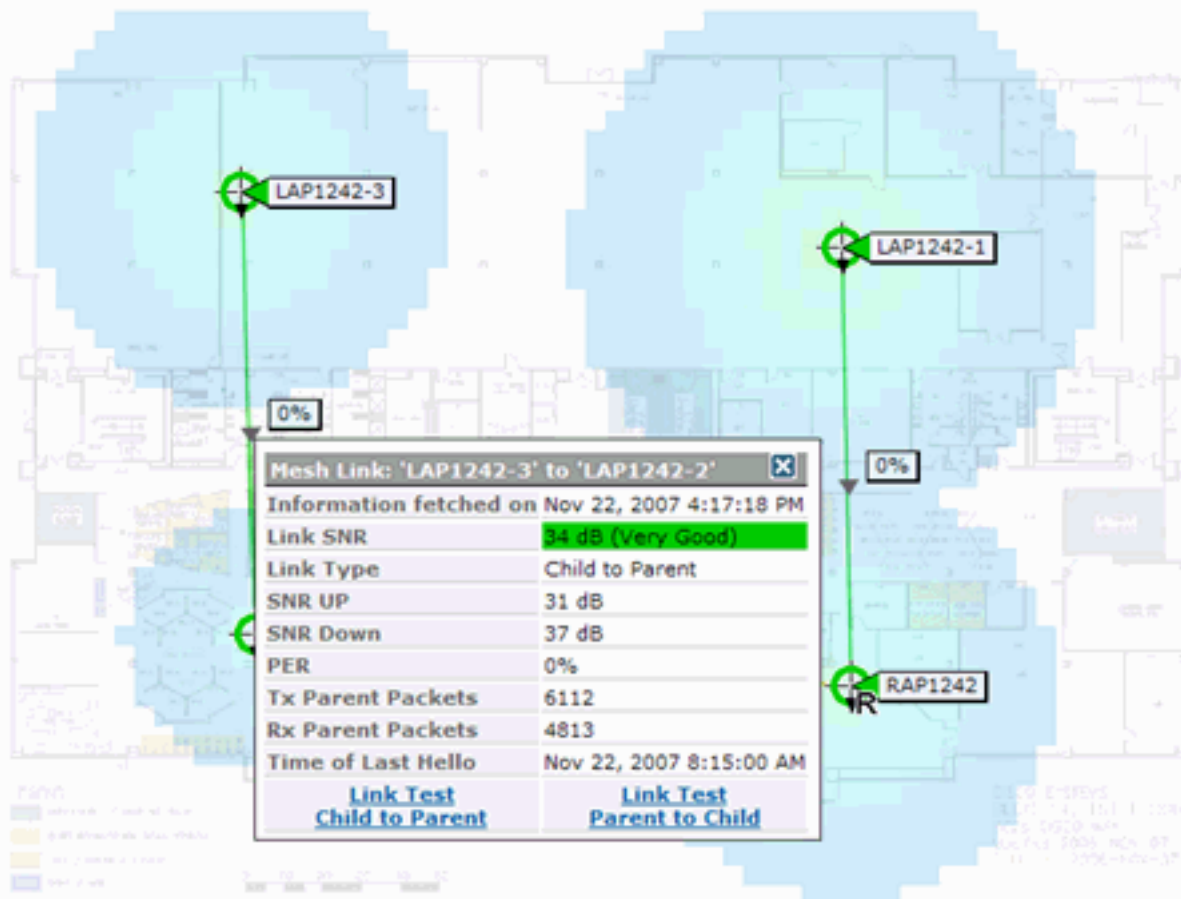
Il test del collegamento da punto di accesso a punto di accesso è supportato nel sistema WCS. È possibile selezionare due access point qualsiasi e richiamare un test di collegamento tra i due.

Se questi access point sono vicini di RF, il test del collegamento potrebbe avere un risultato. Il risultato viene visualizzato in una finestra di dialogo sulla mappa stessa senza un aggiornamento completo della pagina. Il dialogo può essere eliminato facilmente.

Tuttavia, se questi due access point non sono vicini di RF, il servizio WCS non tenta di individuare un percorso tra i due access point per eseguire un test di combinazione di più collegamenti.

Quando il mouse viene spostato sulla freccia sul collegamento tra i due nodi, viene visualizzata questa finestra:





## Test collegamento nodo-nodo

Lo strumento test collegamento è uno strumento su richiesta per verificare la qualità del collegamento tra due punti di accesso. In Sistema colori Windows questa funzionalità viene aggiunta alla pagina di dettaglio AP.

Nella pagina dei dettagli dell'access point, sotto la scheda **Collegamento Mesh Interno** dove sono elencati i link accanto ad essa, c'è un link per eseguire il test del link.

Lo strumento Controller CLI Link Test ha i parametri di input opzionali: Dimensioni dei pacchetti, totale dei pacchetti di test del collegamento, durata del test e velocità di collegamento dati. Il test di collegamento dispone di valori predefiniti per questi parametri facoltativi. Gli indirizzi MAC per i nodi sono gli unici parametri di input obbligatori.

Lo strumento test collegamento verifica l'intensità, il pacchetto inviato e il pacchetto ricevuto tra i nodi. Il collegamento per il test del collegamento viene visualizzato nel report dettagliato AP. Quando si fa clic sul collegamento, viene visualizzata una schermata popup con i risultati del test del collegamento. Il test Collegamento sarà applicabile solo al padre-figlio e ai vicini.

L'output del test di collegamento genera pacchetti inviati, pacchetti ricevuti, pacchetti di errore (bucket per motivi di diff), SNR, Noise Floor e RSSI.

Il test Link fornisce almeno questi dettagli sulla GUI:

- Pacchetti di test di collegamento inviati
- Pacchetti test di collegamento ricevuti

- Potenza del segnale in dBm
- Rapporto S/N

## [Collegamenti adiacenti punto di accesso su richiesta](#)

Si tratta di una nuova funzionalità della mappa di Sistema colori Windows. È possibile fare clic su un punto di accesso Mesh e viene visualizzata una finestra popup con informazioni dettagliate. È quindi possibile fare clic su **Visualizza vicini rete** per recuperare le informazioni sui vicini per l'access point selezionato e visualizzare una tabella con tutti i vicini per l'access point rete interna selezionato.

Il link Adiacente alla rete visualizza tutti i vicini dell'access point evidenziato. Questa istantanea mostra tutti i vicini, il tipo dei vicini e il valore SNR.

## [Test Ping](#)

Il test Ping è uno strumento su richiesta utilizzato per eseguire il ping tra il controller e l'access point. Lo strumento Test ping è disponibile sia nella pagina dei dettagli dell'access point che in MAP. Fare clic sul collegamento **Esegui test ping** nella pagina dei dettagli dell'access point o nelle informazioni sull'access point per avviare il ping tra il controller e l'access point corrente.

## [Conclusioni](#)

Enterprise Mesh (ovvero, una rete interna) è un'estensione della copertura wireless di Cisco ai luoghi in cui l'Ethernet cablata non è in grado di fornire connettività. La flessibilità e la gestibilità di una rete wireless vengono realizzate con mesh aziendali.

La maggior parte delle funzionalità degli access point cablati è fornita dalla topologia della rete interna. La rete aziendale può inoltre coesistere con gli access point cablati sullo stesso controller.

## [Informazioni correlate](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)