

Configurazione di un collegamento Mesh point-to-point con Bridging Ethernet su controller wireless integrato con access point C9124

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Ethernet Bridging](#)

[Controller wireless integrato nel punto di accesso Catalyst](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazioni switch](#)

[Configurazione EWC e RAP](#)

[Configura MAP](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi utili](#)

[Esempio 1: il protocollo RAP riceve l'adiacenza dal protocollo MAP e riesce l'autenticazione](#)

[Esempio 2: indirizzo MAC MAP non aggiunto al WLC o aggiunto in modo non corretto](#)

[Esempio 3: il formato RAP perde il formato MAP](#)

[Suggerimenti, consigli e suggerimenti](#)

[Riferimenti](#)

Introduzione

In questo documento viene descritto come configurare P2P Mesh Link con Ethernet Bridging su Embedded Wireless Controller (eWC) con access point C9124.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Wireless Lan Controller (WLC) 9800.
- Access Point (AP) Cisco Catalyst.
- Controller wireless incorporato sui punti di accesso Catalyst.

- Tecnologia Mesh.

Componenti usati

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

- EWC IOS® XE 17.12.2
- 2 AP C9124.
- 2 iniettori di alimentazione AIR-PWRINJ-60RGD1.
- switch 2x;
- 2 notebook;
- 1x AP C9115.

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.

Premesse

Ethernet Bridging

La soluzione di rete mesh, che fa parte della soluzione di rete wireless unificata Cisco, consente a due o più punti di accesso Mesh Cisco (di seguito denominati punti di accesso mesh) di comunicare tra loro su uno o più hop wireless per collegarsi a più LAN o estendere la copertura WiFi.

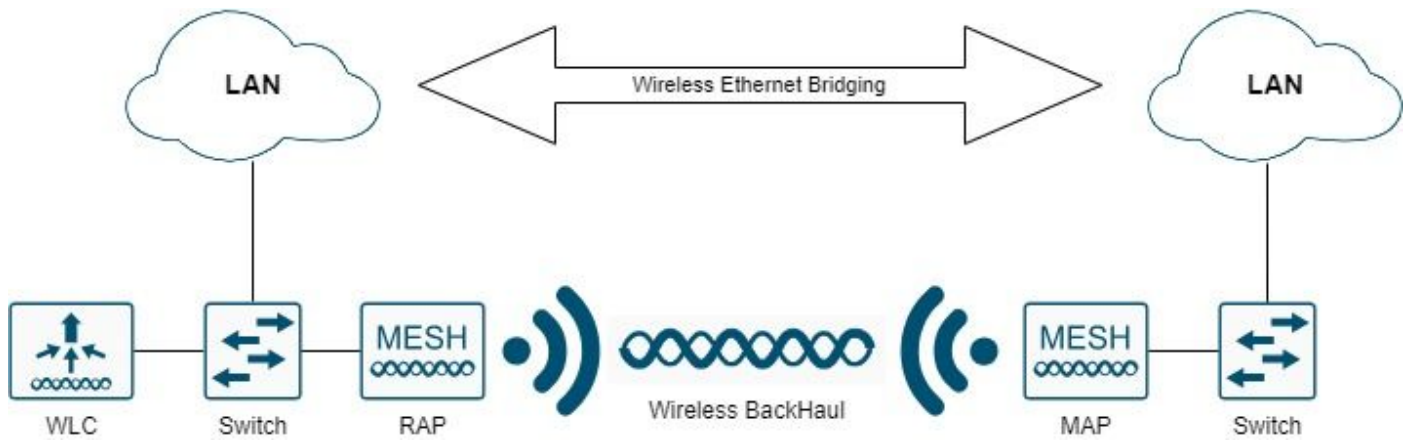
I punti di accesso mesh Cisco sono configurati, monitorati e gestiti da e tramite qualsiasi controller LAN wireless Cisco implementato nella soluzione di rete mesh.

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

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

In questo documento viene illustrato come configurare in modo analogo la distribuzione mesh point-to-point e il bridging Ethernet.

Nell'implementazione delle reti mesh point-to-point, i punti di accesso mesh forniscono l'accesso wireless e il backhaul ai client wireless e possono supportare contemporaneamente il bridging tra una LAN e una terminazione a un dispositivo Ethernet remoto o a un'altra LAN Ethernet.



Bridging Ethernet wireless

Per informazioni dettagliate su ciascuno di questi tipi di implementazione, consultare [la guida alla distribuzione di Mesh per Cisco Catalyst serie 9800 Wireless Controller](#).

Cisco Catalyst serie 9124 outdoor 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.

È possibile utilizzare C9124 in uno dei seguenti ruoli mesh:

- Access point dal tetto (RAP)
- Mesh Access Point (MAP)

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

Le mappe non dispongono di connessioni cablate a un controller LAN wireless Cisco. Possono essere completamente wireless e supportare client che comunicano con altre mappe o RAP, oppure possono essere utilizzati per collegarsi a periferiche o reti cablate.

Controller wireless integrato nel punto di accesso Catalyst

Il Cisco Embedded Wireless Controller (EWC) sui punti di accesso Catalyst è un controller basato su software integrato nei punti di accesso Cisco Catalyst 9100.

In una rete Cisco EWC, un access point (AP) con la funzione di controller wireless è designato come access point attivo.

Gli altri punti di accesso, gestiti da questo access point attivo, sono definiti punti di accesso subordinati.

Il CAE attivo ha due ruoli:

- Funziona e funziona come un controller WLC (Wireless LAN Controller) per gestire e controllare gli access point subordinati. I punti di accesso subordinati fungono da punti di accesso lightweight per servire i client.
- Funziona come punto di accesso per servire i client.

Per una panoramica del prodotto EWC sui punti di accesso, consultare il [data sheet](#) sul [controller wireless integrato Cisco sui punti di accesso Catalyst](#).

Per informazioni su come distribuire EWC sulla rete, consultare il [white paper Cisco Embedded Wireless Controller on Catalyst Access Point \(EWC\)](#).

Il presente documento si concentra su C9124 come EWC e presume che esista già un AP 9124 in modalità EWC.

Configurazione

Esempio di rete


Tutti i dispositivi della rete si trovano nella subnet 192.168.100.0/24, ad eccezione dei notebook con subnet 192.168.101.0/25 nella VLAN 101.

L'interfaccia di gestione del WLC non è codificata e la VLAN nativa sulle porte dello switch è impostata sulla VLAN 100.

AP9124_RAP ha il ruolo di eWC e di punto di accesso principale (RAP), mentre AP9124_MAP ha il ruolo di punto di accesso mesh (MAP).

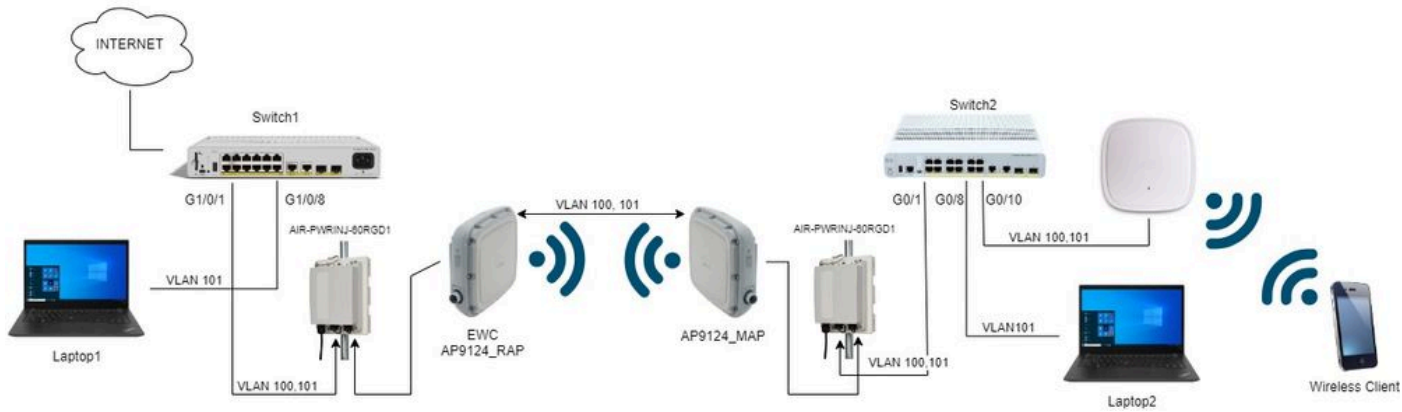
In questa esercitazione, dietro la MAPPa viene posizionato anche un AP C9115 per mostrare che possiamo avere AP che si uniscono a un WLC su un collegamento Mesh.

Questa tabella contiene gli indirizzi IP di tutti i dispositivi della rete:

 Nota: l'aggiunta di tag all'interfaccia di gestione può causare problemi all'access point che si unisce al processo WLC interno. Se si decide di contrassegnare l'interfaccia di gestione, verificare che la parte dell'infrastruttura cablata sia configurata di conseguenza.

Sul dispositivo bootflash o slot0:	Indirizzo IP
Gateway predefinito	Statica sulla VLAN 100: 192.168.100.1
Notebook1	DHCP su VLAN 101
Notebook2	DHCP su VLAN 101
Switch1 (server DHCP)	VLAN 100 SVI: statica sulla VLAN 100: 192.168.100.1 (server DHCP)
Switch1 (server DHCP)	VLAN 101 SVI: statica sulla VLAN 101: 192.168.101.1 (server DHCP)

Interruttore2	VLAN 100 SVI: DHCP su VLAN 100
Interruttore2	VLAN 101 SVI: DHCP su VLAN 101
9124EWC	Statica sulla VLAN 100: 192.168.100.40
AP9124_RAP	DHCP su VLAN 100
AP9124_MAP	DHCP su VLAN 100
AP9115	DHCP su VLAN 100



Esempio di rete



Nota: i punti di accesso C9124 sono alimentati tramite AIR-PWRINJ-60RGD1 in base alle linee guida contenute nella [guida all'installazione dell'hardware per access point esterni Cisco Catalyst serie 9124AX](#).

Configurazioni

In questo documento si presume che esista già un access point serie 9124 con EWC con distribuzione iniziale eseguita come da [white paper di Cisco Embedded Wireless Controller on Catalyst Access Point \(EWC\)](#).

Per altri suggerimenti e suggerimenti sul processo di conversione, consultare il documento [Convert Catalyst 9100 Access Point to Embedded Wireless Controller](#) (Converti punti di accesso Catalyst 9100 in controller wireless integrato).

Configurazioni switch

Ecco le configurazioni degli switch.

Le porte degli switch a cui sono connessi i punti di accesso sono in modalità trunk con la VLAN nativa impostata su 100 e consente la VLAN 101.

Durante la gestione temporanea degli access point, è necessario configurare la mappa come MAP, quindi è necessario collegare l'access point all'eWC tramite Ethernet. Qui si utilizza la porta dello switch 1 G1/0/2 per il posizionamento nell'area intermedia del MAP. Dopo aver posizionato la mappa nell'area intermedia, questa viene spostata sullo switch 2.

Le porte degli switch a cui sono collegati i notebook sono configurate come porte di accesso sulla VLAN 101.

Interruttore1:

```
ip dhcp excluded-address 192.168.101.1 192.168.101.10
ip dhcp excluded-address 192.168.100.1 192.168.100.10
!
ip dhcp pool AP_VLAN100
network 192.168.100.0 255.255.255.0
default-router 192.168.100.1
dns-server 192.168.1.254
!
ip dhcp pool VLAN101
network 192.168.101.0 255.255.255.0
default-router 192.168.101.1
dns-server 192.168.1.254
!
interface GigabitEthernet1/0/1
description AP9124_RAP (EWC)
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet1/0/2
description AP9124_MAP_Staging
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet1/0/8
description laptop1
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
```

Interruttore 2:

```
interface GigabitEthernet0/1
description AP9124_MAP
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
```

```

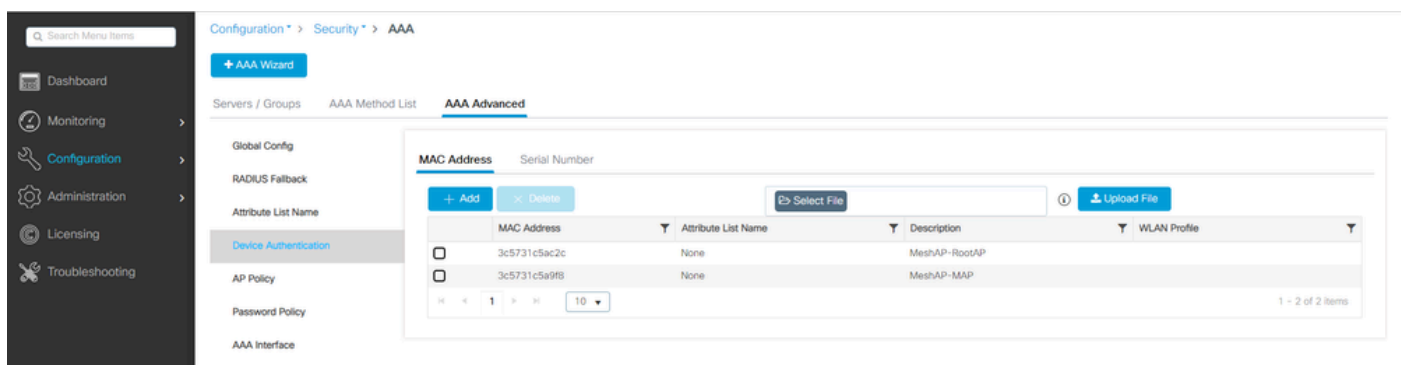
end
interface GigabitEthernet0/8
description laptop2
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
interface GigabitEthernet0/1
description AP9115
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end

```

Configurazione EWC e RAP

Dopo la configurazione Day0 del punto di accesso EWC, il punto di accesso integrato deve unirsi a se stesso.

1. Aggiungere gli indirizzi MAC Ethernet dei punti di accesso radice e mesh all'autenticazione del dispositivo. Selezionare Configuration > Security > AAA > AAA Advanced > Device Authentication, fare clic sul pulsante +Add:



The screenshot shows the Cisco configuration interface for AAA Advanced Device Authentication. The left sidebar contains navigation options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Security > AAA' and includes a '+ AAA Wizard' button. Under 'AAA Advanced', there is a table for MAC addresses:

MAC Address	Serial Number	Attribute List Name	Description	WLAN Profile
<input type="checkbox"/> 3c5731c5ac2c		None	MeshAP-RootAP	
<input type="checkbox"/> 3c5731c5a9f8		None	MeshAP-MAP	

At the bottom of the table, it indicates '1 - 2 of 2 items'.

Indirizzi MAC in autenticazione dispositivo

Comandi CLI:

```

9124EWC(config)#username 3c5731c5ac2c mac description MeshAP-RootAP
9124EWC(config)#username 3c5731c5a9f8 mac description MeshAP-MAP

```

L'indirizzo mac Ethernet può essere confermato eseguendo il comando "show controller wired 0" dalla CLI dell'access point. Esempio dal punto di accesso radice:

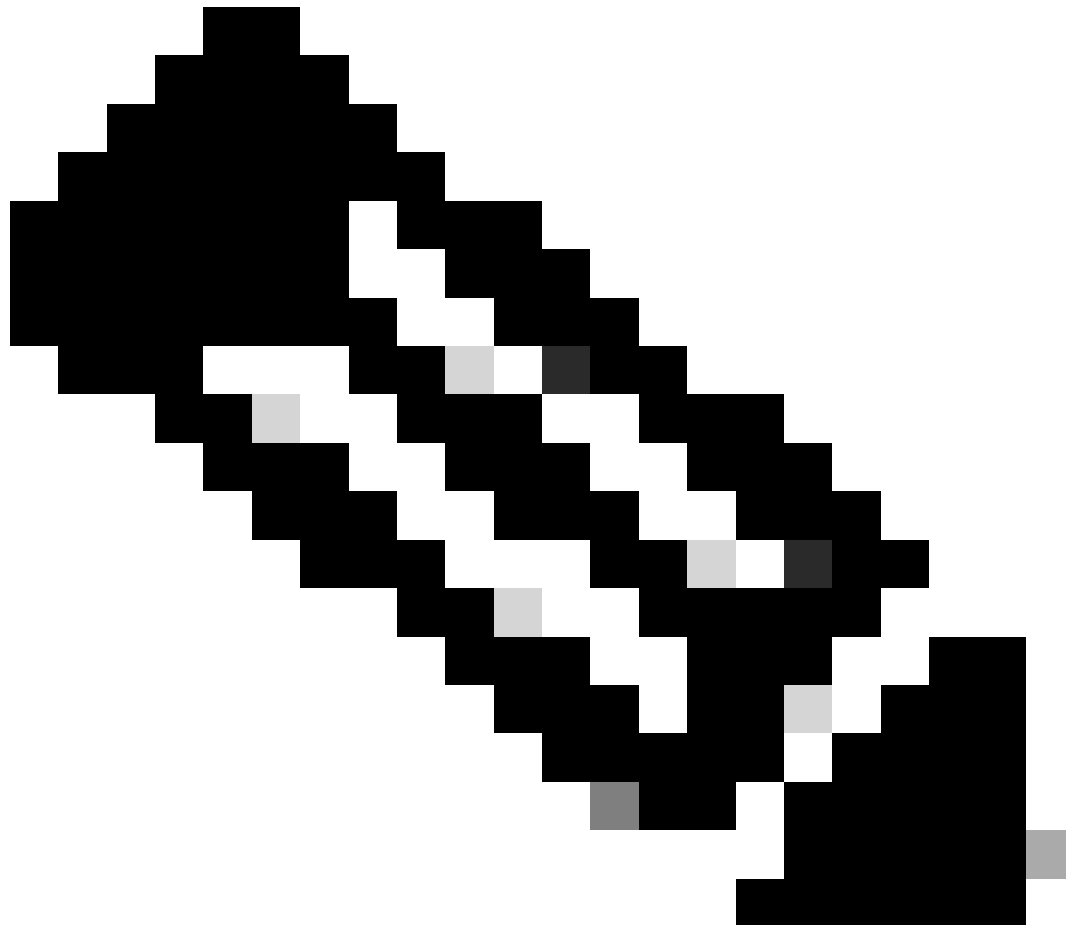
```

AP3C57.31C5.AC2C#show controllers wired 0
wired0 Link encap:Ethernet HWaddr 3C:57:31:C5:AC:2C

```


L'accesso alla shell dell'access point sottostante può essere completato con il comando "wireless ewc-ap ap shell username x", come mostrato di seguito:

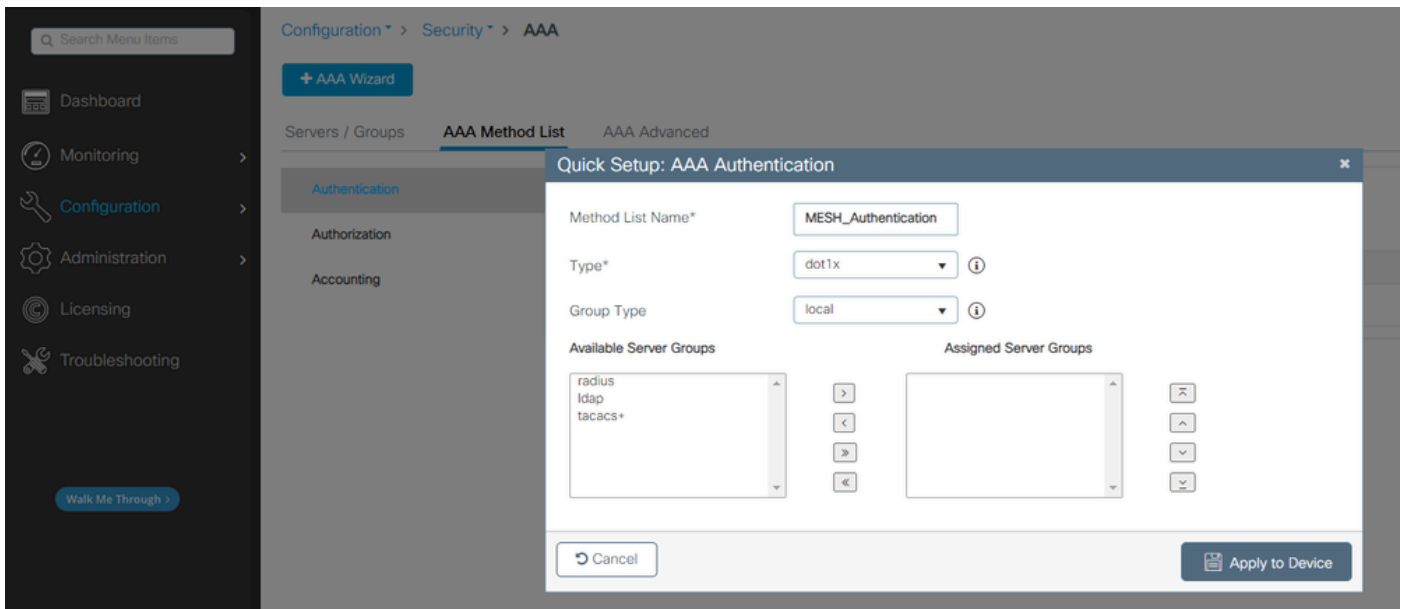
```
9124EWC#wireless ewc-ap ap shell username admin
[...]
admin@192.168.255.253's password:
AP3C57.31C5.AC2C>en
Password:
AP3C57.31C5.AC2C#
AP3C57.31C5.AC2C#logout
Connection to 192.168.255.253 closed.
9124EWC#
```



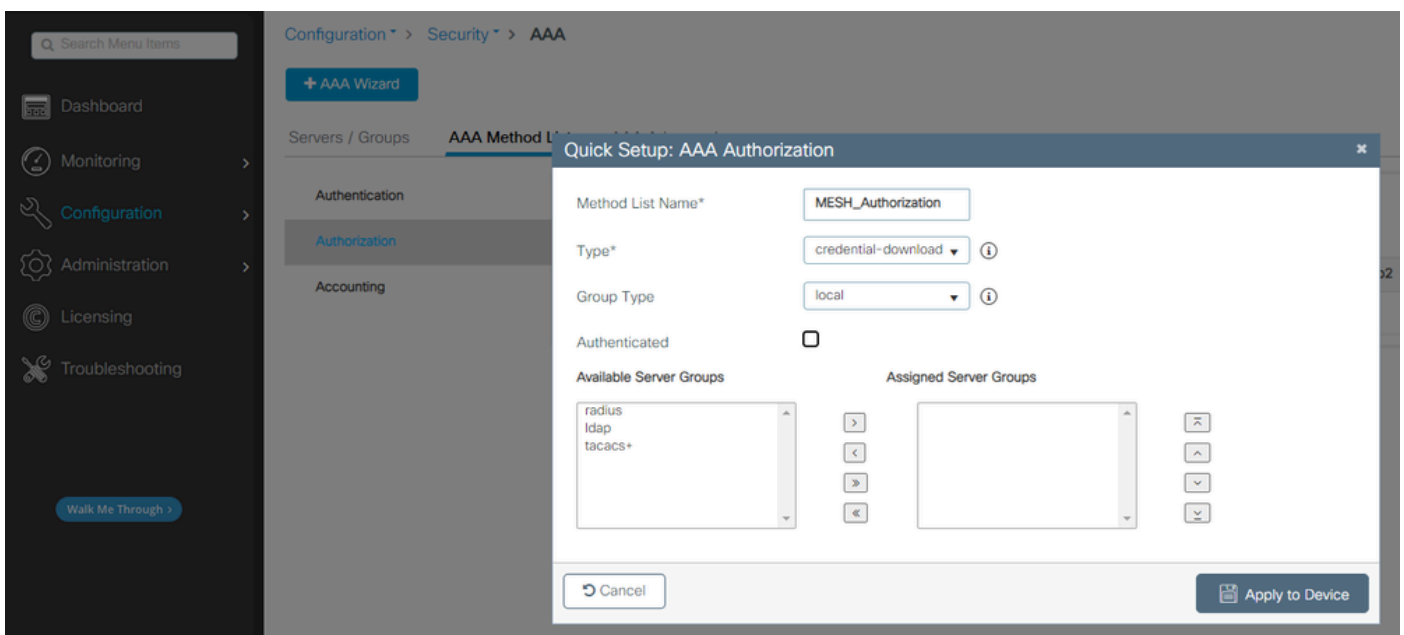
Nota: questo comando equivale al comando apciscoshell disponibile precedentemente sui controller Mobility Express.

Se il nome utente e la password per la gestione dell'access point non sono specificati nel profilo, usare invece il nome utente predefinito Cisco e la password Cisco.

2. Aggiungere i metodi di autenticazione e autorizzazione:



Elenco metodi di autenticazione

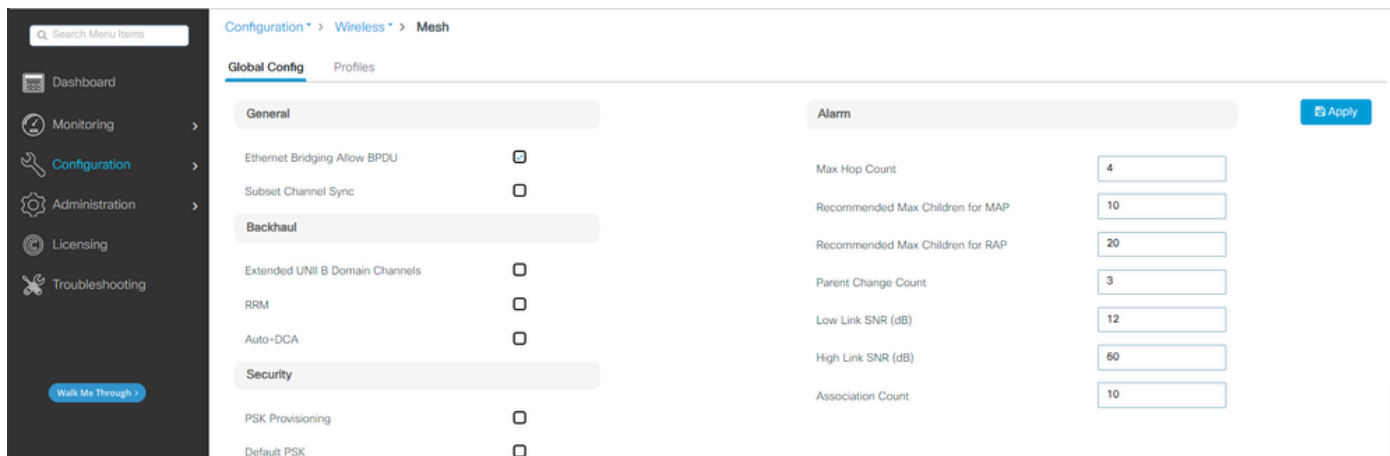


Elenco metodi di autorizzazione

Comandi CLI:

```
9124EWC(config)#aaa authentication dot1x MESH_Authentication local  
9124EWC(config)#aaa authorization credential-download MESH_Authentication local
```

3. Selezionare Configuration > Wireless > Mesh (Configurazione > Wireless > Mesh). Poiché l'impostazione di questo documento richiede il bridging Ethernet, abilitare Ethernet Bridging per consentire i BPDU:



The screenshot shows the configuration page for Wireless Mesh. The breadcrumb navigation is Configuration > Wireless > Mesh. The page is divided into two main sections: Global Config and Profiles. Under Global Config, there are three sub-sections: General, Backhaul, and Security. In the General section, the 'Ethernet Bridging Allow BPDU' option is checked, while 'Subset Channel Sync' is unchecked. In the Backhaul section, 'Extended UNII B Domain Channels', 'RRM', and 'Auto-DCA' are all unchecked. In the Security section, 'PSK Provisioning' and 'Default PSK' are both unchecked. On the right side, there is an 'Alarm' section with several numeric input fields: Max Hop Count (4), Recommended Max Children for MAP (10), Recommended Max Children for RAP (20), Parent Change Count (3), Low Link SNR (dB) (12), High Link SNR (dB) (60), and Association Count (10). An 'Apply' button is located at the top right of the configuration area.

Bridging Ethernet per consentire BPDU

Comandi CLI:

```
9124EWC(config)#wireless mesh ethernet-bridging allow-bdpu
```



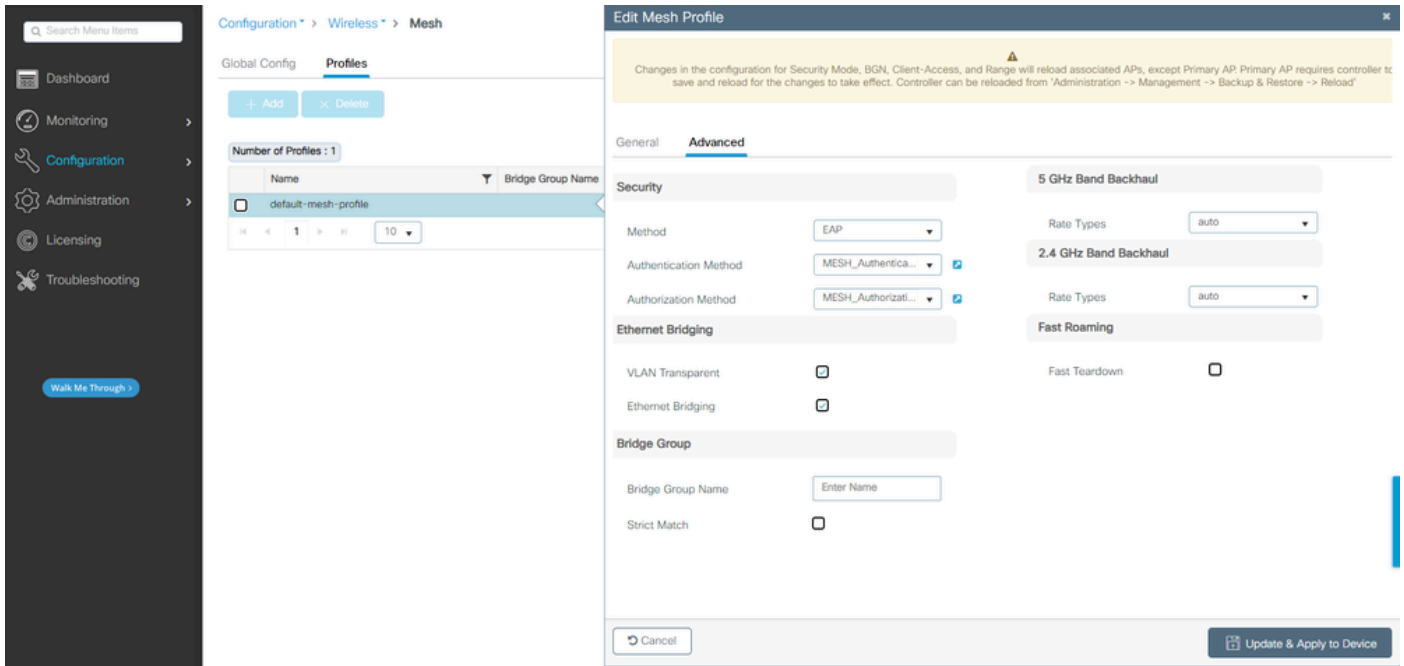
Nota: per impostazione predefinita, gli access point mesh non inoltrano i BPDU sul collegamento mesh.

Se non si dispone di un collegamento ridondante tra i due siti, non è necessario.

Se sono presenti collegamenti ridondanti, è necessario consentire le BPDU. In caso contrario, si rischia di creare un loop STP nella rete.

4. Configurare il profilo mesh predefinito selezionando i metodi di autenticazione e autorizzazione AAA configurati in precedenza. Fate clic su e modificate il profilo mesh di default.

Andare alla scheda Advanced e selezionare i metodi Authentication (Autenticazione) e Authorization (Autorizzazione). Abilitare l'opzione Ethernet Bridging.



Modifica profilo mesh di default

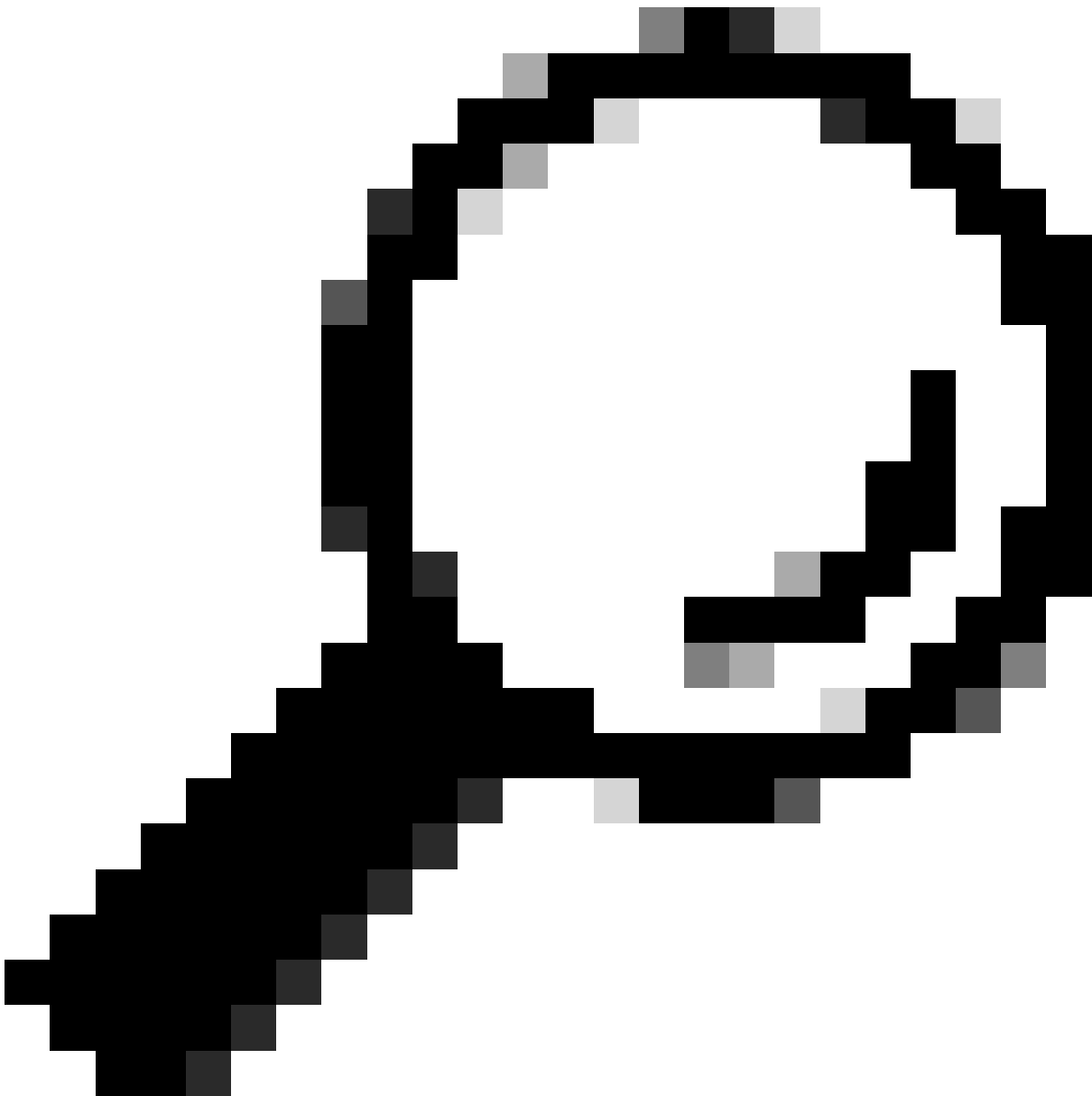
Comandi CLI:

```
9124EWC(config)#wireless profile mesh default-mesh-profile
9124EWC(config-wireless-mesh-profile)#description "default mesh profile"
9124EWC(config-wireless-mesh-profile)#ethernet-bridging
9124EWC(config-wireless-mesh-profile)#ethernet-vlan-transparent
9124EWC(config-wireless-mesh-profile)#method authentication MESH_Authentication
9124EWC(config-wireless-mesh-profile)#method authorization MESH_Authorization
```

Callout speciale all'opzione VLAN Transparent:

Questa funzione determina il modo in cui un punto di accesso mesh gestisce i tag VLAN per il traffico Ethernet con bridging:

- Se la funzione VLAN Transparent è abilitata, i tag VLAN non vengono gestiti e i pacchetti vengono raggruppati come pacchetti senza tag.
 - Quando la funzione VLAN transparent è abilitata, non è richiesta alcuna configurazione delle porte Ethernet. La porta Ethernet trasmette i frame con e senza tag senza interpretarli.
- Se VLAN Transparent è disabilitato, tutti i pacchetti vengono gestiti in base alla configurazione VLAN sulla porta (trunk, accesso o modalità normale).
 - Se la porta Ethernet è impostata sulla modalità trunk, è necessario configurare il tagging VLAN Ethernet.



Suggerimento: per utilizzare il tagging VLAN AP, è necessario deselezionare la casella di controllo VLAN trasparente.

Se non si utilizza il tagging VLAN, significa che il RAP e il MAP si trovano sulla VLAN nativa configurata sulle porte del trunk. In questa condizione, se si desidera che altri dispositivi dietro a MAP si trovino sulla VLAN nativa (qui VLAN 100), è necessario abilitare VLAN Transparent.

5. L'access point interno si unisce all'EWC ed è possibile verificare lo stato di join dell'AP utilizzando il comando "show ap summary":

```

9124EWc#show ap summary
Number of APs: 1

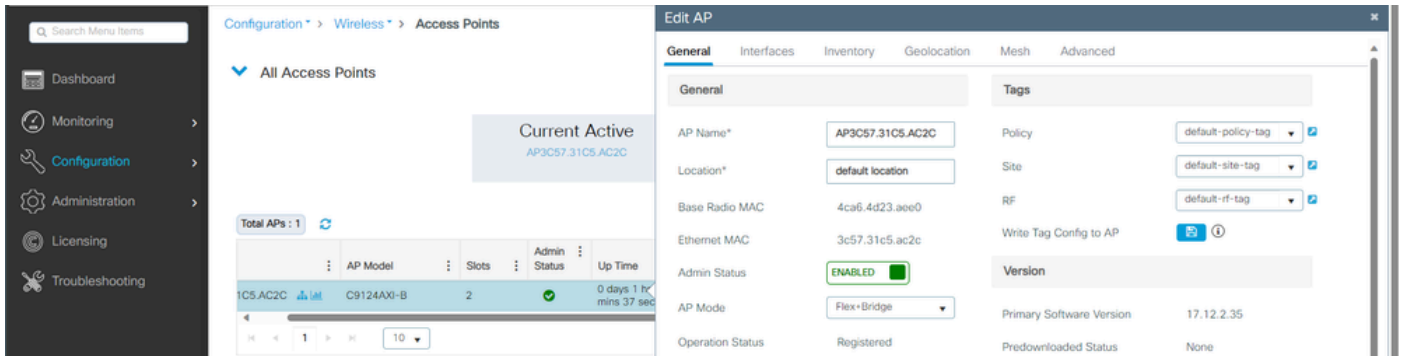
CC = Country Code
RD = Regulatory Domain

AP Name           Slots AP Model           Ethernet MAC   Radio MAC      CC  RD  IP Address           State      Location
-----
AP3C57.31C5.AC2C  2     C9124AXI-B     3c57.31c5.ac2c 4ca6.4d23.aee0 US  -8  192.168.100.11     Registered default location

```

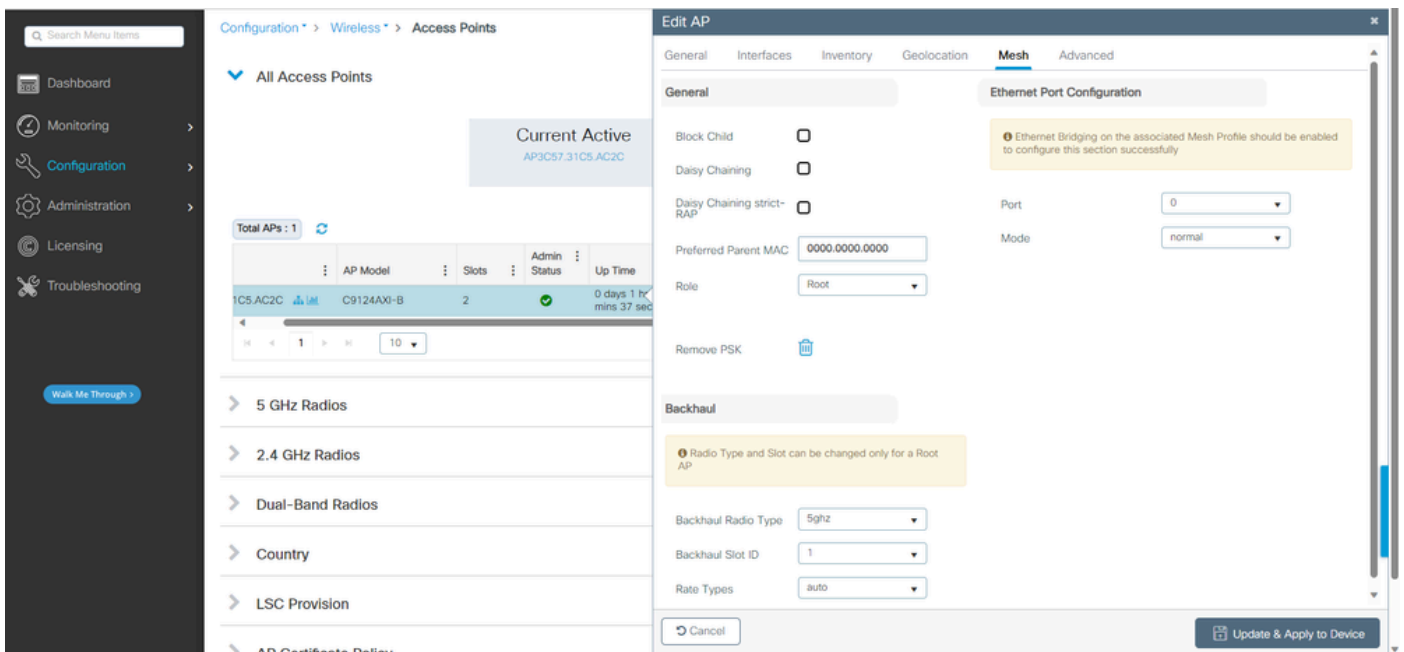
mostra riepilogo app

È inoltre possibile visualizzare l'access point collegato tramite la GUI, in cui l'access point viene visualizzato come modalità Flex+Bridge. Per comodità è possibile modificare il nome dell'access point adesso. In questa configurazione viene utilizzato il nome AP9124_RAP:



Dettagli generali contabilità fornitori

È possibile modificare la georilevazione e quindi verificare che nella scheda Mesh il ruolo sia configurato come Root AP e che Ethernet Port Configuration sia impostato su trunk con gli ID VLAN corrispondenti:



Radice ruolo mesh

Edit AP ✕

General
Interfaces
Inventory
Geolocation
Mesh
Advanced

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Remove PSK

Ethernet Port Configuration

ⓘ Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully

Port

Mode

Native VLAN ID*

Allowed VLAN IDs

Backhaul

ⓘ Radio Type and Slot can be changed only for a Root AP

Backhaul Radio Type

Backhaul Slot ID

Rate Types

↶ Cancel

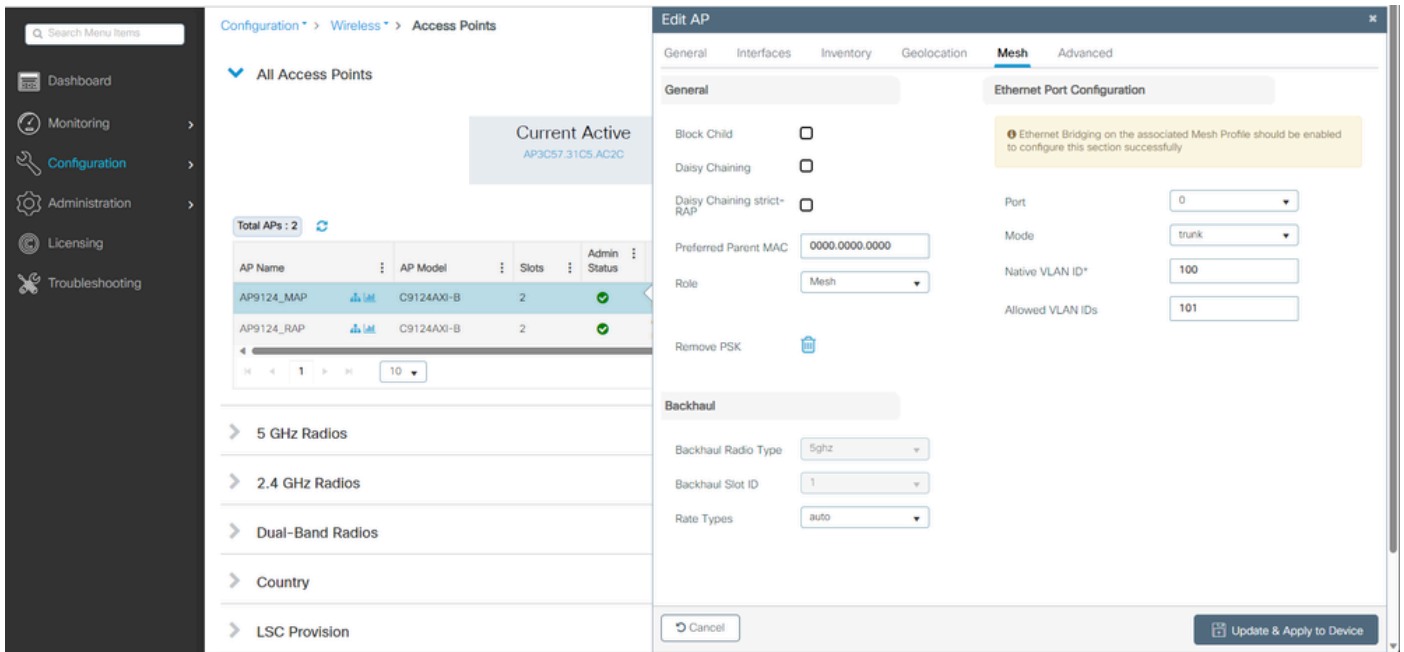
Update & Apply to Device

Ethernet Port Configuration

Configura MAP

Ora è il momento di unirsi al 9124 MAP.

1. Collegare l'access point MAP allo switch 1 per la gestione temporanea. L'access point si unisce all'EWC e viene visualizzato nell'elenco AP. Modificate il nome in un nome simile a AP9124_MAP e configuratelo come Ruolo mesh (Mesh Role) nella scheda Mesh (Mesh). Fare clic su Aggiorna e applica al dispositivo:



Configurazione MAP

2. Scollegare il punto di accesso dallo switch 1 e collegarlo allo switch 2 come indicato nel diagramma reticolare. Il MAP si unisce all'EWC tramite l'interfaccia wireless attraverso il RAP.



Nota: poiché i punti di accesso sono alimentati tramite un iniettore di alimentazione, il punto di accesso non si spegne e, poiché la configurazione si trova in un ambiente controllato, lo switch 2 è fisicamente vicino e possiamo semplicemente spostare il cavo da uno switch all'altro.

È possibile collegare un cavo console all'access point e vedere cosa succede tramite la console. Di seguito sono riportati alcuni messaggi importanti.

Nota: dalla versione 17.12.1, la velocità in baud predefinita della console degli access point 802.11AX viene modificata da 9600 bps a 115200 bps.

MAP perde la connettività a EWC:

AP9124_MAP#

```
[*01/11/2024 14:08:23.0214] chatter: Device wired0 notify state change link DOWN
[*01/11/2024 14:08:28.1474] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:28.1474]
[*01/11/2024 14:08:31.1485] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:31.1486]
[*01/11/2024 14:08:33.4214] chatter: Device wired0 notify state change link UP
[*01/11/2024 14:08:34.1495] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=83, M
[*01/11/2024 14:08:34.1495]
[*01/11/2024 14:08:37.1505] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=84, M
[*01/11/2024 14:08:37.1505]
[*01/11/2024 14:08:40.1515] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=84, M
[*01/11/2024 14:08:40.1515]
```

```
[*01/11/2024 14:08:43.1524] Max retransmission count exceeded, going back to D
[...]
```

MAP passa alla modalità di rilevamento via wireless e trova il RAP via Radio Backhaul sul canale 36, trova EWC e si unisce ad esso:

```
[*01/11/2024 14:08:51.3893] CRIT-MeshRadioBackhaul[1]: Set as uplink
[*01/11/2024 14:08:51.3894] CRIT-MeshAwppAdj[1][4C:A6:4D:23:AE:F1]: Set as Par
[*01/11/2024 14:08:51.3915] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (mon0)
[*01/11/2024 14:08:51.3926] wlan: [0:I:CMN_MLME] mlme_ext_vap_down: VAP (apbhr0)
[*01/11/2024 14:08:51.4045] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (apbhr0)
[*01/11/2024 14:08:51.4053] wlan: [0:I:CMN_MLME] mlme_ext_vap_up: VAP (mon0)
[*01/11/2024 14:08:53.3898] CRIT-MeshLink: Set Root port Mac: 4C:A6:4D:23:AE:F1
[*01/11/2024 14:08:53.3904] Mesh Reconfiguring DHCP.
[*01/11/2024 14:08:53.8680] DOT11_UPLINK_EV: wgb_uplink_set_port_authorized: c
[*01/11/2024 14:08:53.9232] CRIT-MeshSecurity: Mesh Security successful auther
[...]
```

MAP è ora unito a EWC tramite RAP.

AP C9115: è possibile ottenere un indirizzo IP sulla VLAN 100 e quindi unirsi all'EWC:



Avviso: tenere presente che la VLAN 100 è la VLAN nativa trunk delle porte switch. Affinché il traffico proveniente dall'access point sulla VLAN 100 raggiunga il WLC sulla VLAN 100, il collegamento mesh deve avere la VLAN trasparente abilitata. Questa operazione viene eseguita nella sezione Bridging Ethernet del profilo mesh.

```
[*01/19/2024 11:40:55.0710] ethernet_port wired0, ip 192.168.100.14, netmask 255.255.255.255
[*01/19/2024 11:40:58.2070] CAPWAP State: Init
[*01/19/2024 11:40:58.2150] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2150] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2400] Discovery Request sent to 192.168.100.40, discovered
[*01/19/2024 11:40:58.2530] Discovery Request sent to 255.255.255.255, discovered
[*01/19/2024 11:40:58.2600] CAPWAP State: Discovery
[*01/19/2024 11:40:58.2670] Discovery Response from 192.168.100.40
[*01/19/2024 11:40:58.2670] Found Configured MWAR '9124EWC' (respIdx 1).
[*01/19/2024 15:13:56.0000] Started wait dtls timer (60 sec)
[*01/19/2024 15:13:56.0070] CAPWAP State: DTLS Setup
```

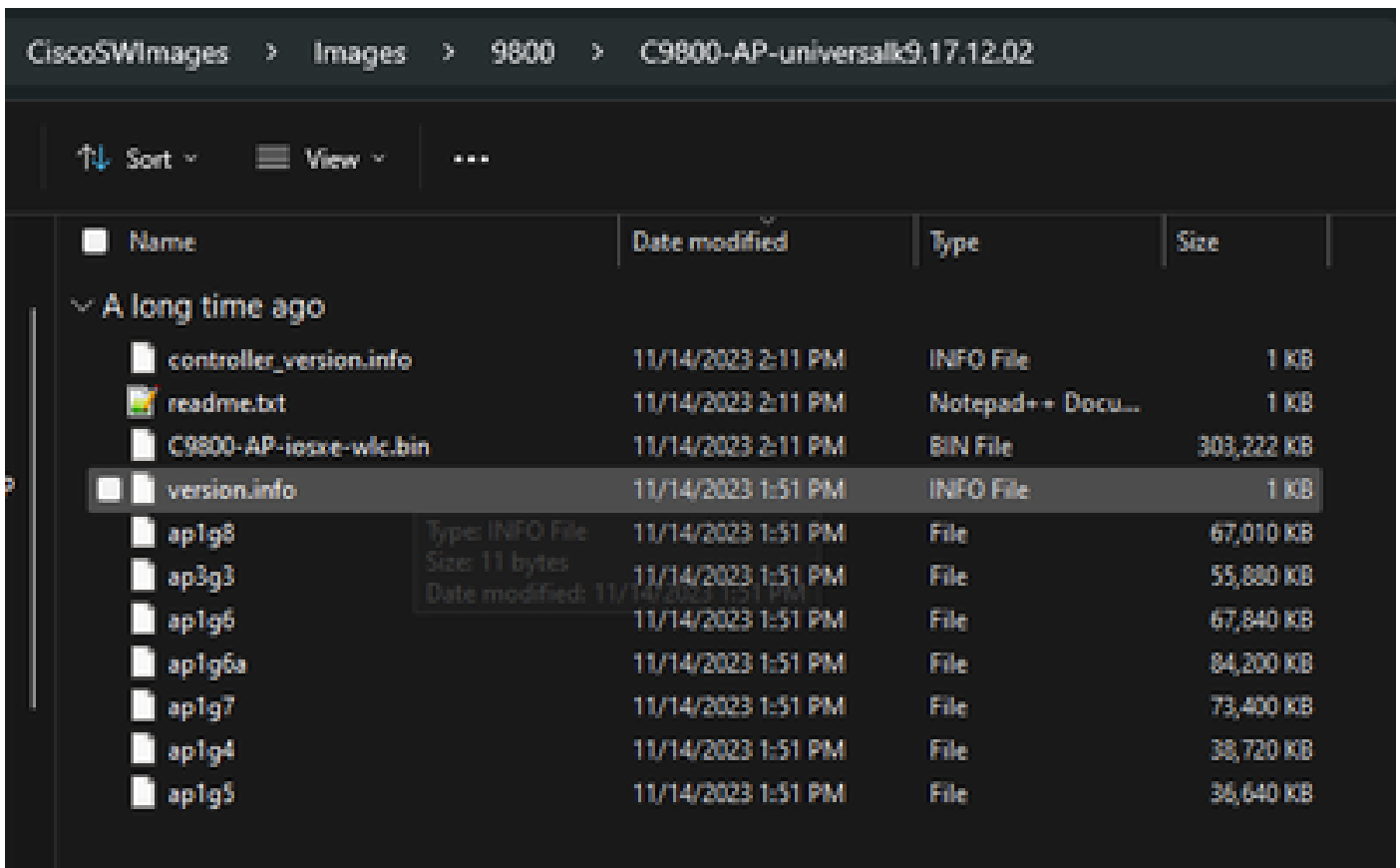
```

[...]
[*01/19/2024 15:13:56.1660] dtls_verify_server_cert: Controller certificate ve
[*01/19/2024 15:13:56.9000] sudi99_request_check_and_load: Use HARSA SUDI cert
[*01/19/2024 15:13:57.2980]
[*01/19/2024 15:13:57.2980] CAPWAP State: Join
[*01/19/2024 15:13:57.3170] shared_setenv PART_BOOTCNT 0 &> /dev/null
[*01/19/2024 15:13:57.8620] Sending Join request to 192.168.100.40 through po
[*01/19/2024 15:14:02.8070] Sending Join request to 192.168.100.40 through po
[*01/19/2024 15:14:02.8200] Join Response from 192.168.100.40, packet size 139
[*01/19/2024 15:14:02.8200] AC accepted previous sent request with result code
[*01/19/2024 15:14:03.3700] Received wlcType 2, timer 30
[*01/19/2024 15:14:03.4440]
[*01/19/2024 15:14:03.4440] CAPWAP State: Image Data
[*01/19/2024 15:14:03.4440] AP image version 17.12.2.35 backup 17.9.4.27, Cont
[*01/19/2024 15:14:03.4440] Version is the same, do not need update.
[*01/19/2024 15:14:03.4880] status 'upgrade.sh: Script called with args:[NO_UP
[*01/19/2024 15:14:03.5330] do NO_UPGRADE, part2 is active part
[*01/19/2024 15:14:03.5520]
[*01/19/2024 15:14:03.5520] CAPWAP State: Configure
[*01/19/2024 15:14:03.5600] Telnet is not supported by AP, should not encode t
[*01/19/2024 15:14:03.6880] Radio [1] Administrative state DISABLED change to
[*01/19/2024 15:14:03.6890] Radio [0] Administrative state DISABLED change to
[*01/19/2024 15:14:03.8670]
[*01/19/2024 15:14:03.8670] CAPWAP State: Run
[*01/19/2024 15:14:03.9290] AP has joined controller 9124EWC
[*01/19/2024 15:14:03.9310] Flexconnect Switching to Connected Mode!

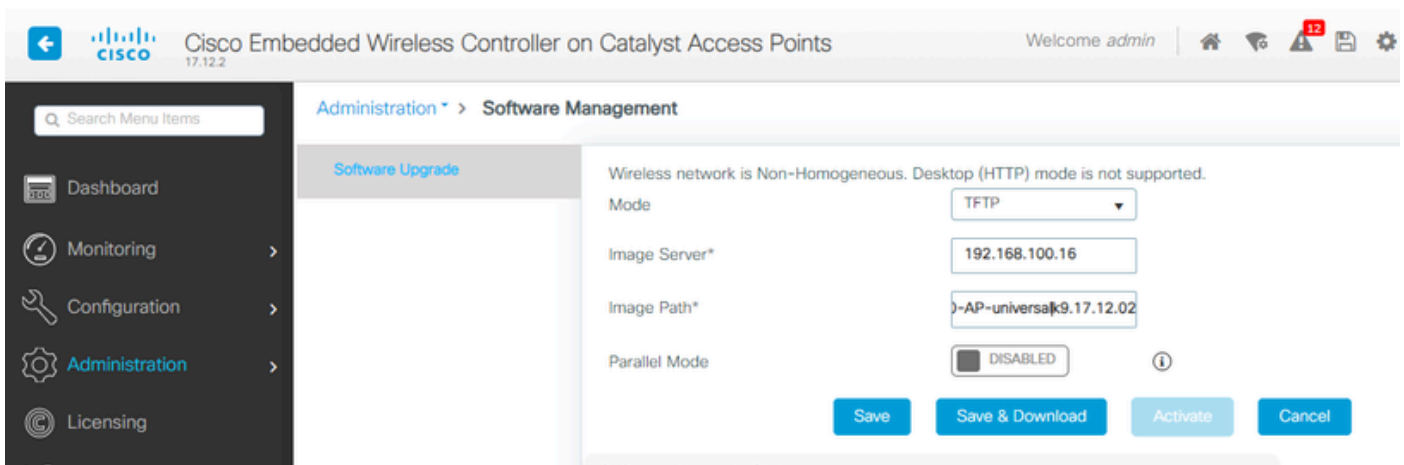
```

Poiché si tratta di un punto di accesso EWC, contiene solo l'immagine AP corrispondente al proprio modello (in questo caso, un C9124 esegue ap1g6a). Quando si partecipa a un modello diverso di punto di accesso, la rete è non omogenea.

In queste condizioni, se l'access point non è nella stessa versione, deve scaricare la stessa versione, quindi assicurarsi di avere un server TFTP/SFTP valido e una posizione, con le immagini AP, configurate in EWC > Amministrazione > Gestione software:



Server TFTP con cartella immagini AP



Immagini PA

Il punto di accesso viene visualizzato nell'elenco dei punti di accesso ed è possibile assegnare un tag di criterio:

Cisco Embedded Wireless Controller on Catalyst Access Points

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Current Active
AP9124_RAP

Total APs : 3

AP Name	AP Model	Slots	Admin Status	Up Time
AP9115	C9115AXE-B	2	✓	0 days 0 hrs mins 36 secs
AP9124_MAP	C9124AXI-B	2	✓	8 days 6 hrs mins 37 secs
AP9124_RAP	C9124AXI-B	2	✓	8 days 6 hrs mins 40 secs

5 GHz Radios

Edit AP

General Interfaces Inventory Geolocation ICap Advanced

General

AP Name* AP9115

Location* default location

Base Radio MAC 1cd1.e079.66e0

Ethernet MAC 84f1.47b3.2cdc

Admin Status ENABLED

AP Mode Flex

Operation Status Registered

Fabric Status Disabled

CleanAir NSI Key

LED Settings

LED State ENABLED

Tags

Policy LocalSWTag

Site default-site-tag

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.12.2.35

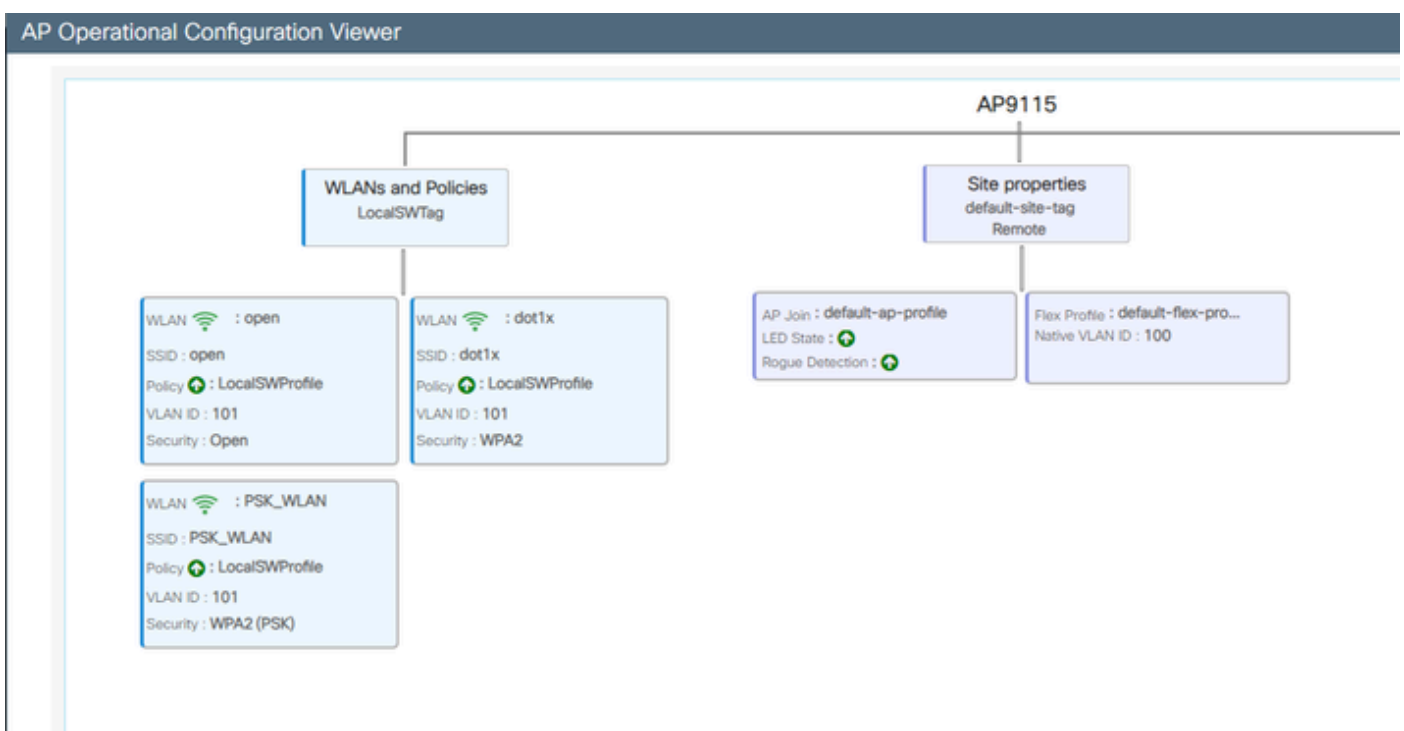
Predownloaded Status Predownloading

Predownloaded Version 0.0.0.0

Next Retry Time 0

Boot Version 1.1.2.4

Elenco AP con dettagli su 9115



Vista operativa AP

Verifica

è possibile vedere la struttura della rete tramite la GUI che fornisce anche l'output dalla CLI se si usa il comando "show wireless mesh ap tree". Dalla GUI, selezionare Monitoring > Wireless > Mesh:

Monitoring > Wireless > Mesh

AP Convergence

Global Stats

Number of Bridge APs	0	Number of Flex+Bridge APs	2
Number of RAPs	0	Number of Flex+Bridge RAPs	1
Number of MAPs	0	Number of Flex+Bridge MAPs	1

Tree

```

AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
-----
[Sector 1]
-----
AP9124_RAP [0, 0, Default, (36), 0000.0000.0000, 3%, 0]
|-AP9124_MAP [1, 73, Default, (36), 0000.0000.0000, 3%, 0]
Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
(*) Wait for 3 minutes to update or Ethernet Connected Mesh AP.
(**) Not in this Controller

```

Albero Mesh AP

Sulla RAP e sulla MAP potete verificare il backhaul mesh usando il comando "show mesh backhaul":

```

AP9124_RAP#show mesh backhaul
Wired Backhaul: 0 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
0 16 TRUE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16 0 T/F: T F T T F T Filtered

-----

Wired Backhaul: 1 [3C:57:31:C5:AC:2C]
idx Cost Uplink InterfaceType
1 Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address Cost RawCost BlistCount Flags: P C R W B A Reject reason
3C:57:31:C5:AC:2C 16 16 0 T/F: F F F F F F Filtered

-----

Radio Backhaul: 0 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
2 INITIAL ACCESS UP Invalid FALSE FALSE TRUE FALSE FALSE ALLOWED RADIO

No Radio Adjacency Exists

-----

Radio Backhaul: 1 [4C:A6:4D:23:AE:F1]
idx State Role RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
3 MAINT DOWNLINK UP Invalid FALSE TRUE FALSE FALSE TRUE ALLOWED RADIO
Mesh AMPP Radio adjacency info
Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W),
BlockListed(B), Authenticated(A), HTC capable(H), VHTCapable(V)
OldParent(O), BGScan(S)
Address Cost RawCost LinkCost ReportedCost Snr BCount Ch Width Bgn Flags: P O C N R W B A H V S Reject reason
4C:A6:4D:23:9D:51 Invalid Invalid 0 0 76 0 36 20 MHz - (T/F): F F T F T F F T T T F -

```

RAP - mostra backhaul mesh

```

AP9124_MAP#show mesh backhaul
Wired Backhaul: 0 [3C:57:31:C5:A9:F8]
idx Cost    Uplink InterfaceType
0  Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address      Cost RawCost BlistCount Flags: P C R W B A  Reject reason
3C:57:31:C5:A9:F8 16  16    32          T/F: F F T F T T  Blocklisted: GW UNREACHABLE

-----

Wired Backhaul: 1 [3C:57:31:C5:A9:F8]
idx Cost    Uplink InterfaceType
1  Invalid FALSE WIRED
Mesh Wired Adjacency Info
Flags: Parent(P), Child(C), Reachable(R), CapwapUp(W), BlockListed(B) Authenticated(A)
Address      Cost RawCost BlistCount Flags: P C R W B A  Reject reason
3C:57:31:C5:A9:F8 16  16    0          T/F: F F F F F F  Filtered

-----

Radio Backhaul: 0 [4C:A6:4D:23:9D:51]
idx State  Role  RadioState Cost    Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
2  INITIAL ACCESS UP          Invalid FALSE  FALSE  TRUE  FALSE  FALSE          ALLOWED          RADIO

No Radio Adjacency Exists

-----

Radio Backhaul: 1 [4C:A6:4D:23:9D:51]
Hops to Root: 1
idx State Role  RadioState Cost Uplink Downlink Access ShutDown ChildrenAllowed BlockChildState InterfaceType
3  MAINT UPLINK UP          217 TRUE  TRUE  FALSE  FALSE  TRUE          ALLOWED          RADIO
Mesh AWPP Radio adjacency info
Flags: Parent(P), Child(C), Neighbor(N), Reachable(R), CapwapUp(W),
      BlockListed(B), Authenticated(A), HTC capable(H), VHTCapable(V)
      OldParent(O), BGScan(S)
Address      Cost RawCost LinkCost ReportedCost Snr BCount Ch Width  Bgn Flags: P O C N R W B A H V S Reject reason
4C:A6:4D:23:AE:F1 217 272    256    16          70 0    36 20 MHz - (T/F): T F F T T T F T T T F -

-----

AP9124_MAP#

```

MAP show mesh backhaul

È possibile verificare la configurazione del trunking VLAN della rete sull'access point:

```

AP9124_RAP#show mesh ethernet vlan config static
Static (Stored) ethernet VLAN Configuration

```

```

Ethernet Interface: 0
Interface Mode: TRUNK
Native Vlan: 100
Allowed Vlan: 101,

```

```

Ethernet Interface: 1
Interface Mode: ACCESS
Native Vlan: 0
Allowed Vlan:

```

Ethernet Interface: 2
Interface Mode: ACCESS
Native Vlan: 0
Allowed Vlan:

Il notebook 2 connesso allo switch 2 ha ricevuto l'indirizzo IP dalla VLAN 101:

```
C:\Users\luke>ipconfig

Windows IP Configuration

Ethernet adapter usb_xhci:

    Connection-specific DNS Suffix . : 
    IPv4 Address. . . . . : 192.168.101.12
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.101.1
```

Il notebook 1 posizionato sullo switch 1 ha ricevuto un indirizzo IP dalla VLAN 101:

Ethernet adapter Ethernet 6_White:

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::d1d6:f607:ff02:4217%18
IPv4 Address. . . . . : 192.168.101.13
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.101.1
```

```
C:\Users\tantunes>ping 192.168.101.12 -i 192.168.101.13
```

```
Pinging 192.168.101.12 with 32 bytes of data:
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
Reply from 192.168.101.12: bytes=32 time=7ms TTL=128
Reply from 192.168.101.12: bytes=32 time=5ms TTL=128
```

```
Ping statistics for 192.168.101.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 5ms, Maximum = 7ms, Average = 5ms
```



Nota: per testare il protocollo ICMP tra i dispositivi Windows, è necessario autorizzare il protocollo ICMP sul firewall del sistema. Per impostazione predefinita, i dispositivi Windows bloccano l'ICMP nel firewall di sistema.

Un altro semplice test per verificare il bridging Ethernet è la presenza di SVI per VLAN 101 su entrambi gli switch e l'impostazione dello switch 2 SVI su DHCP. Lo switch 2 SVI per VLAN 101 riceve l'indirizzo IP dalla VLAN 101 ed è possibile eseguire il ping tra lo switch 1 VLAN 101 e la SVI per verificare la connettività della vlan 101:

```
<#root>
```

```
Switch2#show ip int br
Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned YES NVRAM up down
Vlan100 192.168.100.61 YES DHCP up up
```

```
Vlan101 192.168.101.11 YES DHCP up up
```

```
GigabitEthernet0/1 unassigned YES unset up up
[...]
Switch2#
Switch2#ping 192.168.101.1 source 192.168.101.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.101.11
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7 ms
Switch2#
```

<#root>

```
Switch1#sh ip int br
Interface IP-Address OK? Method Status Protocol
Vlan1 192.168.1.11 YES NVRAM up up
Vlan100 192.168.100.1 YES NVRAM up up
```

```
Vlan101 192.168.101.1 YES NVRAM up up
```

```
GigabitEthernet1/0/1 unassigned YES unset up up
[...]
Switch1#ping 192.168.101.11 source 192.168.101.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.101.11, timeout is 2 seconds:
Packet sent with a source address of 192.168.101.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms
Switch1#
```

Anche l'access point in modalità locale C9115 è entrato a far parte dell'EWC:

Configuration > Wireless > Access Points

▼ All Access Points

Current Active
AP9124_RAP

Current Standby
Not Applicable

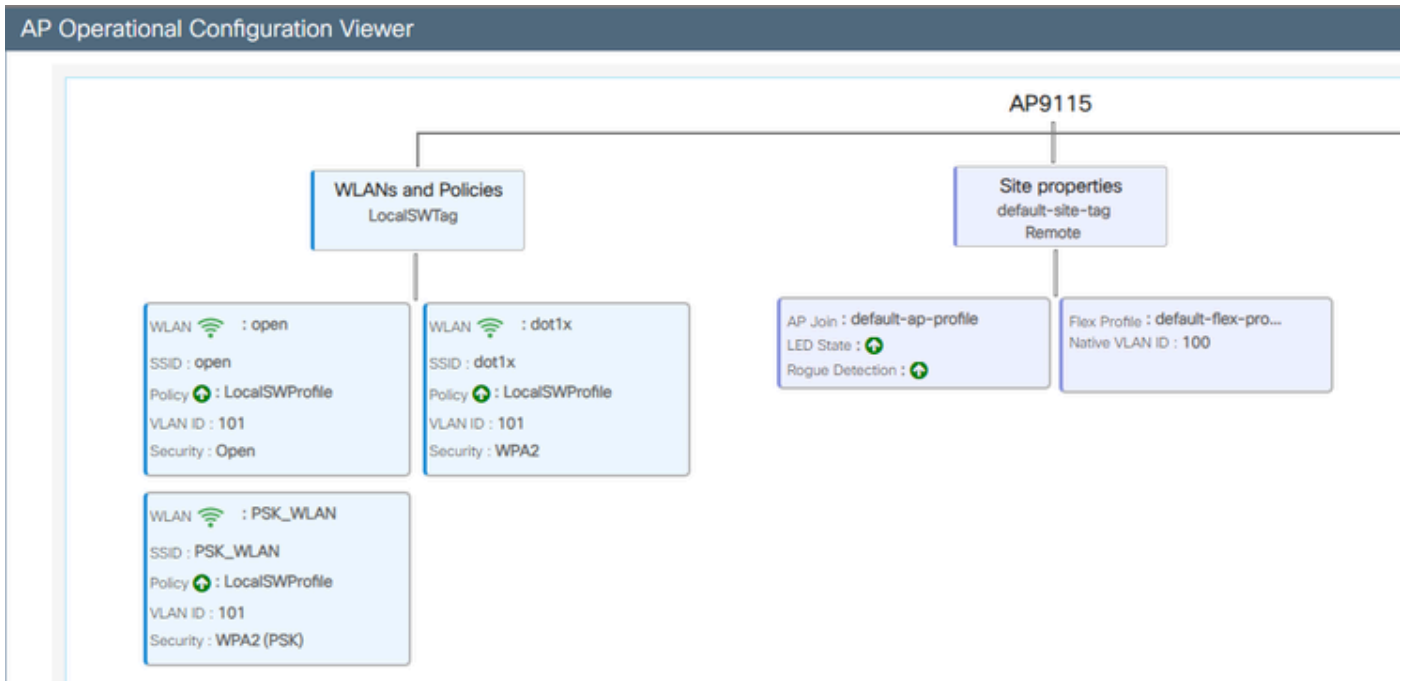
Preferred Active
AP9124_RAP

Total APs : 3

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode
AP9115	C9115AXE-B	2	✓	0 days 0 hrs 35 mins 30 secs	192.168.100.14	1cd1.e079.66e0	84f1.47b3.2cdc	Flex
AP9124_MAP	C9124AXI-B	2	✓	0 days 0 hrs 52 mins 59 secs	192.168.100.12	4ca6.4d23.9d40	3c57.31c5.a9f8	Flex+Bridge
AP9124_RAP	C9124AXI-B	2	✓	0 days 2 hrs 46 mins 57 secs	192.168.100.11	4ca6.4d23.aee0	3c57.31c5.ac2c	Flex+Bridge

AP 9115 aggiunto al CAE

Sono state create 3 WLAN, open, PSK e dot1x mappati a un profilo criteri con VLAN 101 definita in Criteri di accesso:



Configurazione operativa di AP9115

I client wireless sono in grado di connettersi alle WLAN:

The screenshot shows the 'Monitoring > Wireless > Clients' page. The table displays the following data:

Client MAC Address	IP Address	IPV6 Address	AP Name	Site ID	SSID	WLAN ID	Client Type	State
9294-808a-e572	192.168.101.14	fe80::9294-808a-e572	AP9115	1	open	4	WLAN	Run
wc0a-3434-216c	192.168.101.15	fe80::wc0a-3434-216c	AP9115	1	PSK_WLAN	5	WLAN	Run

Risoluzione dei problemi

In questa sezione vengono presentati comandi utili e alcuni suggerimenti, suggerimenti e consigli.

Comandi utili

Su RAP/MAP:

```
AP9124_RAP#show mesh
```

```
adjacency      MESH Adjacency
backhaul       MESH backhaul
bgscan         MESH Background Scanning
channel        MESH channels
client-debug-filter MESH client debugging filter set
config         MESH config parameter
convergence    MESH convergence info
dfs            MESH dfs information
dhcp           Flex-mesh Internal DHCP Server
ethernet       show mesh ethernet bridging
forwarding     MESH Forwarding
history        MESH history of events
least-congested-scan Mesh least congested channel scan
linktest       MESH linktest stats
nat            Flex-mesh NAT/PAT
res            MESH RES info
security       MESH Security Show
stats          MESH stats
status         MESH status
stp            MESH daisychain STP info
timers         MESH Adjacency timers
```

mostra mesh

```

AP9124_RAP#debug mesh
  adjacency      MESH adjacency debugs
  ap-link        MESH link debugs
  bg-scan        Mesh background scanning debugs
  channel        MESH channel debugs
  clear          RESET all MESH debugs
  client         Debug mesh clients
  convergence    MESH convergence debugs
  dhcp          MESH Internal DHCP debugs
  dump-pkts     Dump mesh packets
  events         MESH events
  filter         MESH debug filter
  forward-mcast  Mesh forwarding mcast debugs
  forward-table  Mesh forwarding table debugs
  history        MESH history of events
  level          Enable different mesh debug levels
  linktest      Mesh linktest debugs
  nat           Mesh NAT debugs
  path-control   MESH path-control debugs
  port-control   MESH port-control debugs
  security       MESH security debugs
  stp           MESH daisychain STP debugs
  wpa_suplicant Mesh WPA_SUPPLICANT debugs
  wstp          MESH WSTP debugs

```

Opzioni mesh di debug RAP/MAP

Sul WLC:


```

9124ENC#show wireless mesh ?
airtime-fairness    Shows Mesh AP Airtime Fairness information
ap                  Shows mesh AP related information
cac                 Shows Mesh AP cac related information
config              Show mesh configurations
convergence          Show mesh convergence details.
ethernet            Show wireless mesh ethernet
neighbor            Show neighbors of all connected mesh Aps
persistent-ssid-broadcast Shows Mesh AP persistent ssid broadcast
information
rrm                 Show wireless mesh rrm information

```

show wireless mesh

Per eseguire il debug sul WLC, il miglior punto di inizio è usare RadioActive trace con l'indirizzo MAC del MAP/RAP.

Esempio 1: il protocollo RAP riceve l'adiacenza dal protocollo MAP e riesce l'autenticazione

<#root>

AP9124_RAP#show debug

mesh:

adjacent packet debugging is enabled

event debugging is enabled

mesh linktest debug debugging is enabled

```

Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshRadio
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9559] EVENT-MeshAwppA
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9560] EVENT-MeshAwppA
Jan 16 14:47:01 AP9124_RAP kernel: [*01/16/2024 14:47:01.9570] CLSM[4C:A6:4D:2
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9588] EVENT-MeshRadio
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9592] EVENT-MeshLink
Jan 16 14:47:04 AP9124_RAP kernel: [*01/16/2024 14:47:04.9600] EVENT-MeshSecur
Jan 16 14:47:05 AP9124_RAP kernel: [*01/16/2024 14:47:05.1008] EVENT-MeshSecur
Jan 16 14:47:05 AP9124_RAP kernel: [*01/16/2024 14:47:05.1011] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1172] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.1173] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2033] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2139] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshSecur
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2143] EVENT-MeshLink:

```

```

Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2144] EVENT-MeshLink
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2146] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2147] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwppA
Jan 16 14:47:06 AP9124_RAP kernel: [*01/16/2024 14:47:06.2151] EVENT-MeshAwppA
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3576] EVENT-MeshRadio
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadio
Jan 16 14:47:19 AP9124_RAP kernel: [*01/16/2024 14:47:19.3577] EVENT-MeshRadio

```

Esempio 2: indirizzo MAC MAP non aggiunto al WLC o aggiunto in modo non corretto

<#root>

```

Jan 16 14:52:13 AP9124_RAP kernel: [*01/16/2024 14:52:13.6402] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7407] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7408] EVENT-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7409] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7411] EVENT-MeshLink
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7419] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7583] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7586] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7586] EVENT-MeshSecur
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7620] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7620] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] 0x3c 0x57 0x31
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7621] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] 0xff 0xff 0xff
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] 0xaa 0xff 0x00
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7622] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] INFO-MeshAwppAc
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] 0xaa 0xff 0xaa
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7623] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7636] EVENT-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7637] INFO-MeshRadio
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7642] EVENT-MeshLink
Jan 16 14:52:15 AP9124_RAP kernel: [*01/16/2024 14:52:15.7642] EVENT-MeshSecur

```

Esempio 3: il formato RAP perde il formato MAP

<#root>

```
Jan 16 14:48:58 AP9124_RAP kernel: [*01/16/2024 14:48:58.9929] INFO-MeshRadio
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.2889] INFO-MeshAwppAc
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.7894] INFO-MeshAwppAc
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.9931] INFO-MeshRadio
Jan 16 14:48:59 AP9124_RAP kernel: [*01/16/2024 14:48:59.9932] INFO-MeshRadio
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.2891] INFO-MeshAwppAc
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.7891] INFO-MeshAwppAc
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.9937] INFO-MeshRadio
Jan 16 14:49:00 AP9124_RAP kernel: [*01/16/2024 14:49:00.9938] INFO-MeshRadio
Jan 16 14:49:01 AP9124_RAP kernel: [*01/16/2024 14:49:01.2891] INFO-MeshAwppAc

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5480] EVENT-MeshAwppAc

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5481] EVENT-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5481] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5488] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5489] INFO-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5501] EVENT-MeshRadio

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5501] EVENT-MeshAdj[1

Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5502] EVENT-MeshRadio
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5511] EVENT-MeshLink
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5512] EVENT-MeshSecur
Jan 16 14:49:25 AP9124_RAP kernel: [*01/16/2024 14:49:25.5513] EVENT-MeshLink
```

Suggerimenti, consigli e suggerimenti

- Aggiornando MAP e RAP alla stessa versione dell'immagine via cavo, si evita che il download dell'immagine avvenga via etere (cosa che può essere problematica in ambienti RF "sporchi").
- Si consiglia vivamente di testare l'installazione in un ambiente controllato prima di distribuirla in loco.
- Se si prova il bridging Ethernet con i notebook Windows su entrambi i lati, notare che per testare l'ICMP tra i dispositivi Windows è necessario consentire l'ICMP sul firewall del sistema. Per impostazione predefinita, i dispositivi Windows bloccano l'ICMP nel firewall di sistema.
- Se vengono utilizzati access point con antenne esterne, consultare la guida alla distribuzione per verificare quali antenne sono compatibili e quale porta devono essere collegate.
- Per creare un ponte tra il traffico di diverse VLAN sul collegamento mesh, è necessario disabilitare la funzione VLAN Transparent.

- Prendere in considerazione la presenza di un server syslog locale per gli access point, in quanto può fornire informazioni di debug altrimenti disponibili solo con una connessione alla console.

Riferimenti

[Scheda tecnica di Cisco Embedded Wireless Controller sui punti di accesso Catalyst](#)

[White paper su Cisco Embedded Wireless Controller sui punti di accesso Catalyst \(EWC\)](#)

[Configurazione del collegamento Mesh point-to-point con Ethernet Bridging sui Mobility Express AP](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).