

# Configuración del enlace de malla punto a punto con puente Ethernet en el controlador inalámbrico integrado con puntos de acceso C9124

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Puente Ethernet](#)

[Controlador inalámbrico incorporado en el punto de acceso Catalyst](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuraciones de switch](#)

[Configuración de EWC y RAP](#)

[Configurar MAP](#)

[Verificación](#)

[Troubleshoot](#)

[Comandos útiles](#)

[Ejemplo 1: RAP recibe adyacencia de MAP y realiza la autenticación correctamente](#)

[Ejemplo 2: la dirección MAC de MAP no se agregó al WLC o se agregó incorrectamente](#)

[Ejemplo 3: el RAP pierde el MAP](#)

[Consejos, trucos y recomendaciones](#)

[Referencias](#)

---

## Introducción

Este documento describe cómo configurar P2P Mesh Link con Ethernet Bridging en Embedded Wireless Controller (eWC) con puntos de acceso C9124.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controladores de LAN inalámbrica de Cisco (WLC) 9800.

- Puntos de acceso Cisco Catalyst (AP).
- Controlador inalámbrico incorporado en los puntos de acceso Catalyst.
- Tecnología de malla.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- EWC IOS® XE 17.12.2.
- 2 AP C9124.
- 2 inyectores de alimentación AIR-PWRINJ-60RGD1.
- 2 switches;
- 2 portátiles;
- 1 AP C9115.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

### Puente Ethernet

La solución de red de malla, que forma parte de la solución de red inalámbrica unificada de Cisco, permite que dos o más puntos de acceso de malla de Cisco (en lo sucesivo denominados puntos de acceso de malla) se comuniquen entre sí a través de uno o más saltos inalámbricos para unirse a varias LAN o ampliar la cobertura WiFi.

Los puntos de acceso de malla de Cisco se configuran, supervisan y utilizan desde y a través de cualquier controlador de LAN inalámbrica de Cisco que se implemente en la solución de red de malla.

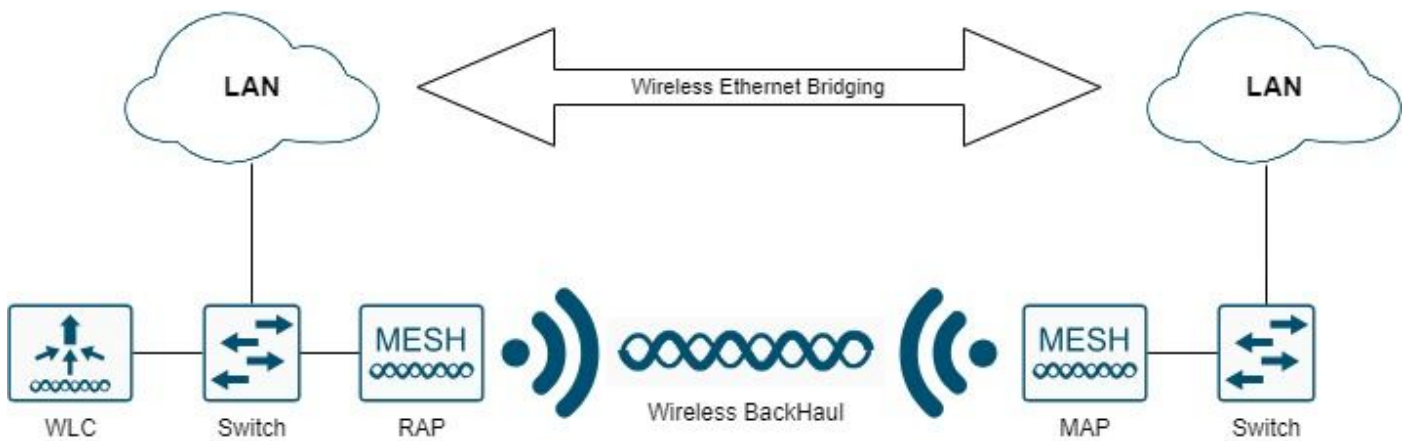
Las implementaciones de soluciones de red de malla compatibles son de uno de estos tres tipos generales:

- Implementación de punto a punto
- Implementación de punto a multipunto
- Implementación de malla

Este documento se centra en cómo configurar la implementación de malla punto a punto y la conexión en puente Ethernet en la misma red.

En la implementación de malla punto a punto, los puntos de acceso de malla proporcionan acceso inalámbrico y red de retorno a los clientes inalámbricos, y pueden admitir simultáneamente la

conexión en puente entre una LAN y una terminación a un dispositivo Ethernet remoto u otra LAN Ethernet.



Puente Ethernet inalámbrico

Consulte [Guía de implementación de malla para los controladores inalámbricos Cisco Catalyst serie 9800](#) para obtener información detallada sobre cada uno de estos tipos de implementación.

El punto de acceso de malla exterior Cisco Catalyst serie 9124 es un dispositivo inalámbrico diseñado para el acceso inalámbrico de clientes y el puente punto a punto, el puente punto a multipunto y la conectividad inalámbrica de malla punto a multipunto.

El punto de acceso exterior es una unidad independiente que se puede montar en una pared o saliente, en un poste de techo o en un poste de farola.

Puede utilizar el C9124 en una de estas funciones de malla:

- Punto de acceso en la parte superior del techo (RAP)
- Punto de acceso de malla (MAP)

Los RAP tienen una conexión por cable a un controlador de LAN inalámbrica de Cisco. Utilizan la interfaz inalámbrica de red de retorno para comunicarse con los MAP cercanos. Los RAP son el nodo principal de cualquier red de puente o malla y conectan un puente o una red de malla a la red cableada, por lo que solo puede haber un RAP para cualquier segmento de red de puente o malla.

Los MAP no tienen conexión con cable a un controlador de LAN inalámbrica de Cisco. Pueden ser completamente inalámbricas y admitir clientes que se comuniquen con otros MAP o RAP, o pueden utilizarse para conectarse a dispositivos periféricos o a una red con cables.

## Controlador inalámbrico incorporado en el punto de acceso Catalyst

El controlador inalámbrico integrado (EWC) de Cisco en los puntos de acceso Catalyst es un controlador basado en software integrado en los puntos de acceso Cisco Catalyst 9100.

En una red Cisco EWC, un punto de acceso (AP) que ejecuta la función de controlador inalámbrico se designa como el AP activo.

Los otros puntos de acceso, que son administrados por este AP activo, se conocen como AP subordinados.

El EWC activo tiene dos funciones:

- Funciona y funciona como un controlador de LAN inalámbrica (WLC) para administrar y controlar los AP subordinados. Los AP subordinados funcionan como puntos de acceso ligeros para servir a los clientes.
- Funciona como un punto de acceso para atender a los clientes.

Para obtener una descripción general del producto sobre EWC en los AP, visite la [hoja de datos del controlador inalámbrico integrado de Cisco en los puntos de acceso Catalyst](#).

Para saber cómo implementar EWC en su red, visite el informe técnico [Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\)](#).

Este documento se centra en C9124 como EWC y asume que ya existe un AP 9124 en modo EWC.

## Configurar

### Diagrama de la red


Todos los dispositivos de esta red se encuentran dentro de la subred 192.168.100.0/24, excepto los portátiles que se encuentran en la VLAN 101 con la subred 192.168.101.0/25.

El EWC AP (WLC) tiene su interfaz de administración sin etiquetar, y la VLAN nativa en los puertos de switch se establece en VLAN 100.

AP AP9124\_RAP tiene la función de un eWC y punto de acceso raíz (RAP), mientras que AP9124\_MAP tiene la función de punto de acceso de malla (MAP).

En este laboratorio, un AP C9115 también se coloca detrás del MAP para mostrar que podemos tener AP para unirse a un WLC sobre un link de malla.

Esta tabla contiene las direcciones IP de todos los dispositivos de la red:

 Nota: Etiquetar la interfaz de administración puede causar problemas con el AP que se une al proceso interno del WLC. Si decide etiquetar la interfaz de administración, asegúrese de que la parte de la infraestructura cableada esté configurada en consecuencia.

Dispositivo	IP Address
Gateway predeterminado	Estático en VLAN 100: 192.168.100.1
Portátil1	DHCP en VLAN 101
Portátil2	DHCP en VLAN 101
Switch1 (servidor DHCP)	VLAN 100 SVI: estática en VLAN 100: 192.168.100.1 (servidor DHCP)

Switch1 (servidor DHCP)	VLAN 101 SVI: estática en VLAN 101: 192.168.101.1 (servidor DHCP)
Switch2	VLAN 100 SVI: DHCP en VLAN 100
Switch2	VLAN 101 SVI: DHCP en VLAN 101
9124EWC	Estático en VLAN 100: 192.168.100.40
AP9124_RAP	DHCP en VLAN 100
AP9124_MAP	DHCP en VLAN 100
AP9115	DHCP en VLAN 100

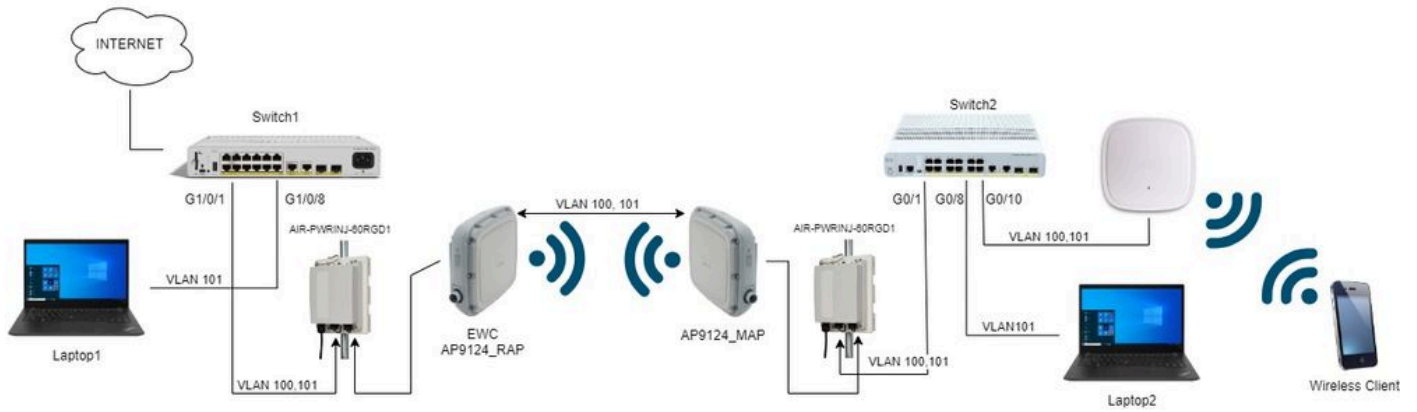


Diagrama de la red



Nota: Los AP C9124 se alimentan mediante AIR-PWRINJ-60RGD1 con las pautas de la [Guía de Instalación de Hardware de Punto de Acceso para Exteriores Cisco Catalyst 9124AX Series](#).

---

## Configuraciones

Este documento asume que ya existe un AP 9124 que ejecuta EWC con la implementación inicial realizada según el [informe técnico Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\)](#).

Para ver otros consejos y trucos relacionados con el proceso de conversión, consulte el documento [Convertir puntos de acceso Catalyst 9100 en controlador inalámbrico incorporado](#).

### Configuraciones de switch

Estas son las configuraciones relevantes de los switches.

Los puertos del switch donde se conectan los AP están en modo trunk con la VLAN nativa configurada en 100 y que permite la VLAN 101.

Durante el desarrollo de los AP, debe configurar el MAP como MAP, por lo tanto, debe hacer que el AP se una al eWC vía ethernet. Aquí utilizamos el puerto G1/0/2 del Switch1 para el desarrollo del MAP. Después de realizar el montaje, el MAP se mueve al Switch 2.

Los puertos de switch a los que se conectan los portátiles se configuran como puertos de acceso en la VLAN 101.

Switch1:

```
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
```

Switch2:

```
interface GigabitEthernet0/1
description AP9124_MAP
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end
interface GigabitEthernet0/8
```

```

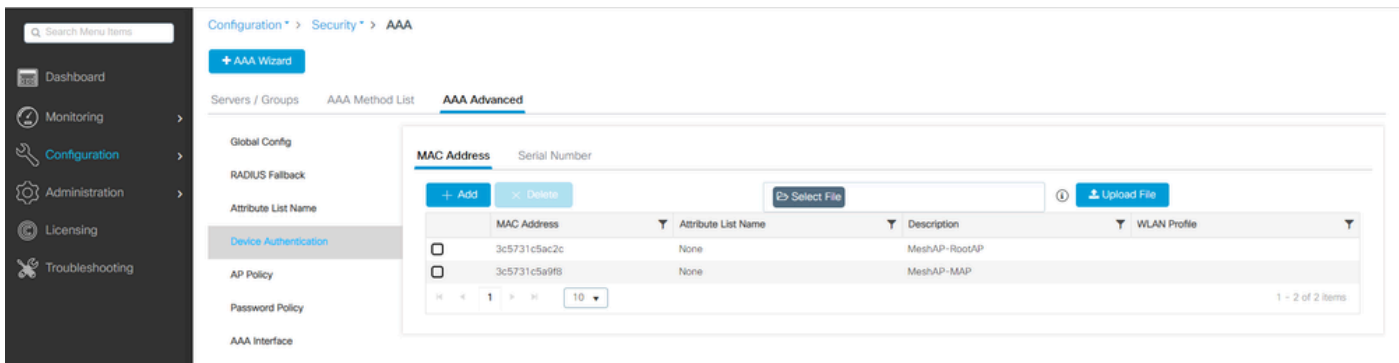
description laptop2
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
interface GigabitEthernet0/1
description AP9115
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end

```

## Configuración de EWC y RAP

Después de la configuración Day0 del EWC AP, el AP embebido necesita unirse a sí mismo.

1. Agregue las direcciones MAC de Ethernet del AP raíz y del AP de malla a la autenticación del dispositivo. Vaya a Configuration > Security > AAA > AAA Advanced > Device Authentication, haga clic en el botón Agregar:



Direcciones MAC en la autenticación de dispositivos

## Comandos CLI:

```

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

```

La dirección MAC de Ethernet se puede confirmar ejecutando "show controllers wired 0" desde la CLI del AP. Ejemplo de AP raíz:

```

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

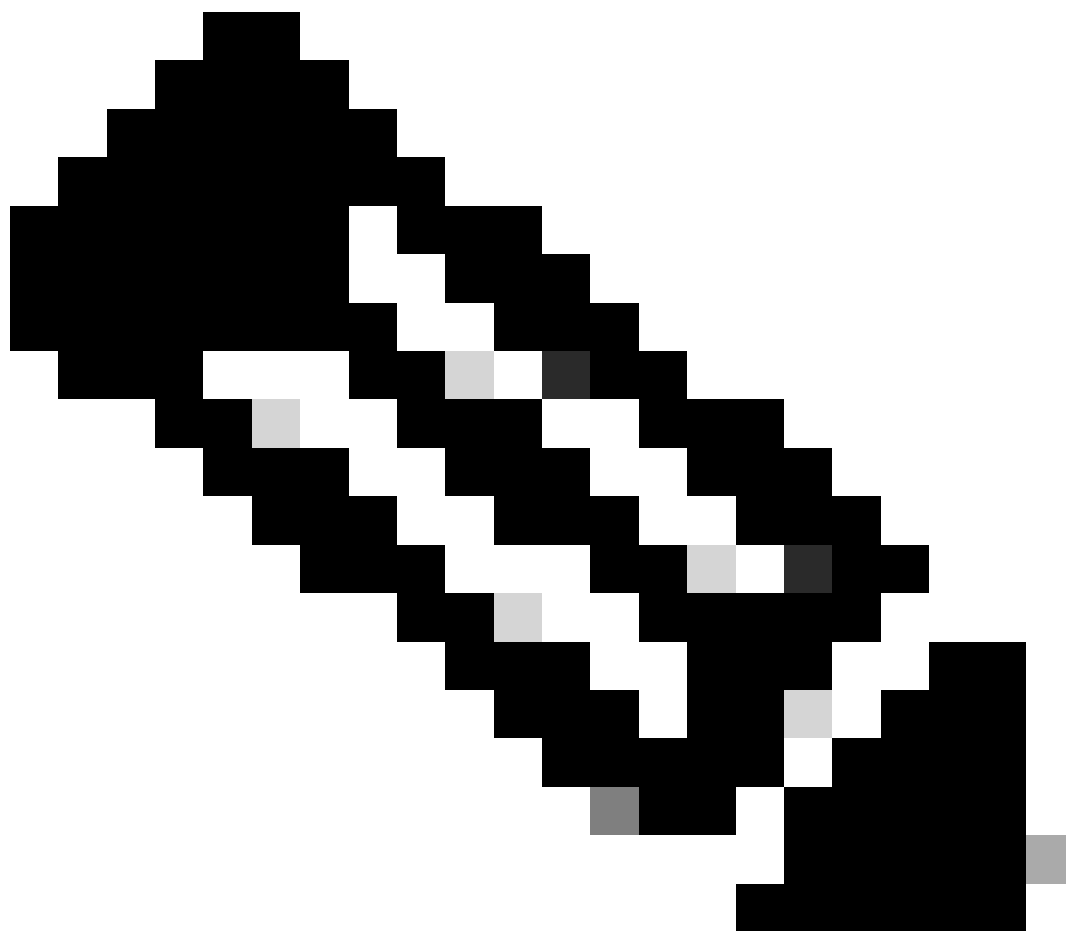
```



El acceso al shell AP subyacente se puede completar con el comando "wireless ewc-ap ap shell username x" como se ejemplifica:

```
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#
```

---



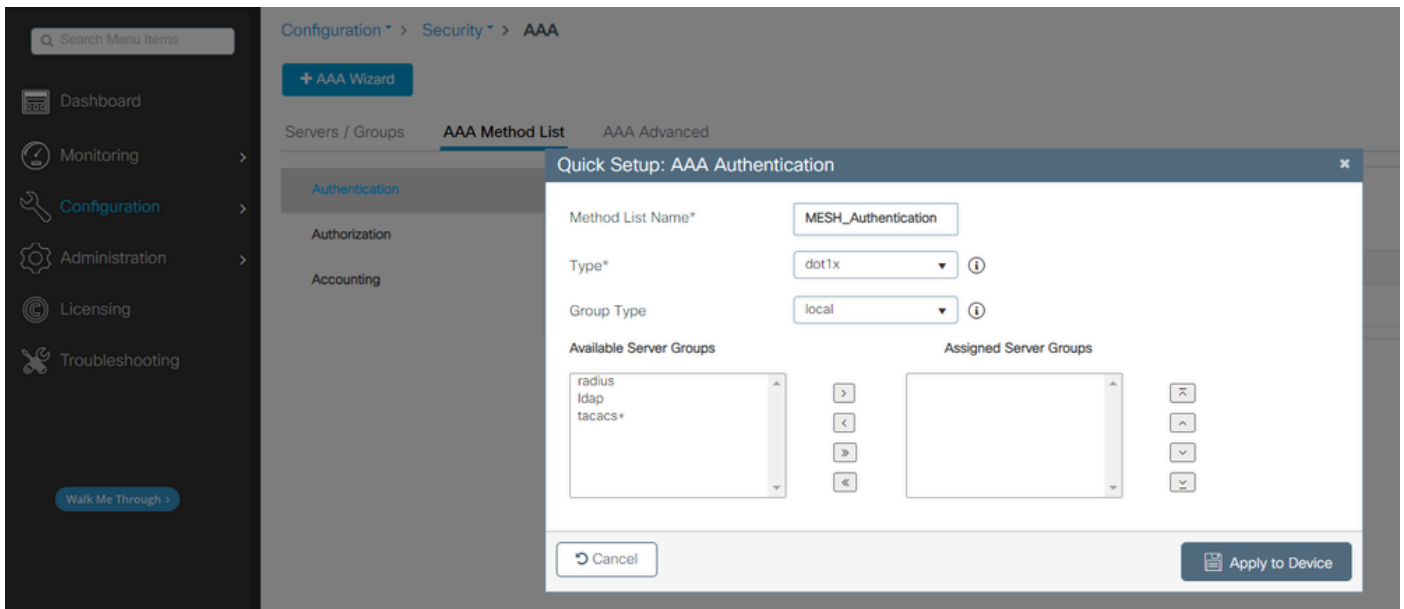
Nota: Este comando es equivalente a apciscoshell que antes estaba disponible en los controladores de Mobility Express.

Si el nombre de usuario y la contraseña de administración de AP no se especifican en el

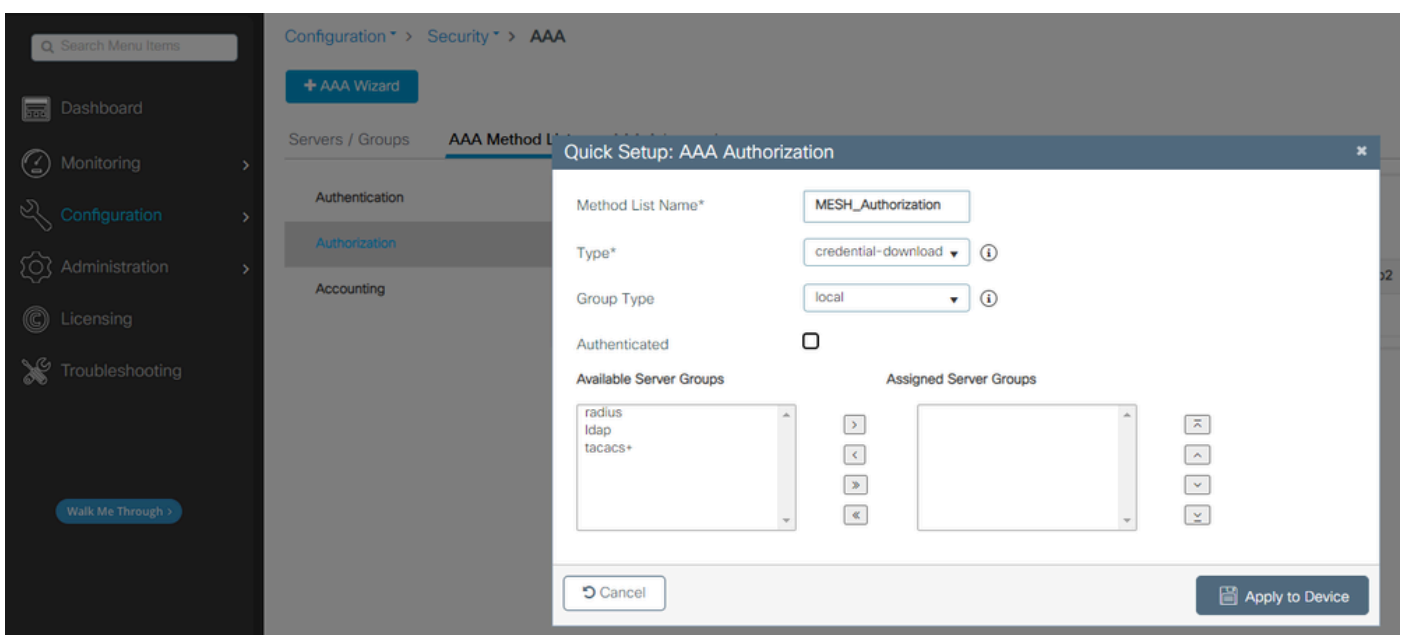
---

perfil de AP, utilice el nombre de usuario predeterminado Cisco y la contraseña Cisco en su lugar.

## 2. Agregar métodos de autenticación y autorización:



Lista de métodos de autenticación



Lista de métodos de autorización

## Comandos CLI:

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

3. Vaya a Configuration > Wireless > Mesh. Como la configuración en este documento requiere conexión en puente Ethernet, habilite Ethernet Bridging Allow BPDUs:

The screenshot shows the configuration page for Wireless Mesh. The breadcrumb navigation is Configuration > Wireless > Mesh. The page is divided into sections: Global Config, Profiles, General, Backhaul, Security, and Alarm. The 'Ethernet Bridging Allow BPDUs' checkbox is checked. Other settings include Subset Channel Sync, Extended UNII B Domain Channels, RRM, Auto-DCA, PSK Provisioning, Default PSK, 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 visible in the top right corner.

Section	Setting	Value
General	Ethernet Bridging Allow BPDUs	<input checked="" type="checkbox"/>
	Subset Channel Sync	<input type="checkbox"/>
Backhaul	Extended UNII B Domain Channels	<input type="checkbox"/>
	RRM	<input type="checkbox"/>
	Auto-DCA	<input type="checkbox"/>
	Security	
Security	PSK Provisioning	<input type="checkbox"/>
	Default PSK	<input type="checkbox"/>
Alarm	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
	Association Count	10

Ethernet Bridging Allow BPDUs

Comandos CLI:

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



Nota: Por defecto, los AP de malla no están reenviando BPDU sobre el link de malla.

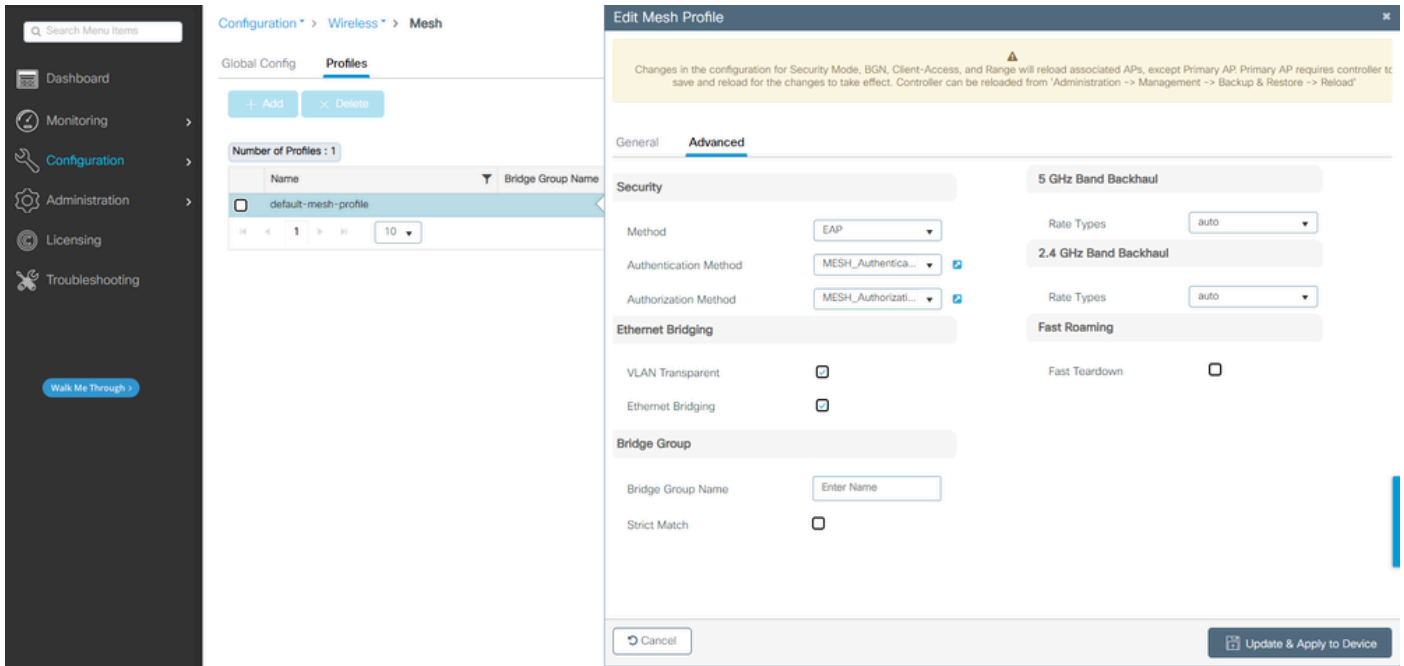
Si no tiene ningún enlace redundante entre los 2 sitios, no es necesario.

Si hay links redundantes, debe permitir las BPDU. Si esto no se hace, se arriesga a crear un loop STP en la red.

---

4. Configure el perfil de malla por defecto donde selecciona los métodos de Autenticación y Autorización AAA previamente configurados. Haga clic y edite el perfil de malla predeterminado.

Vaya a la pestaña Advanced y seleccione los métodos Authentication y Authorization. Active la opción Ethernet Bridging.



Editor default-mesh-profile

## Comandos CLI:

```

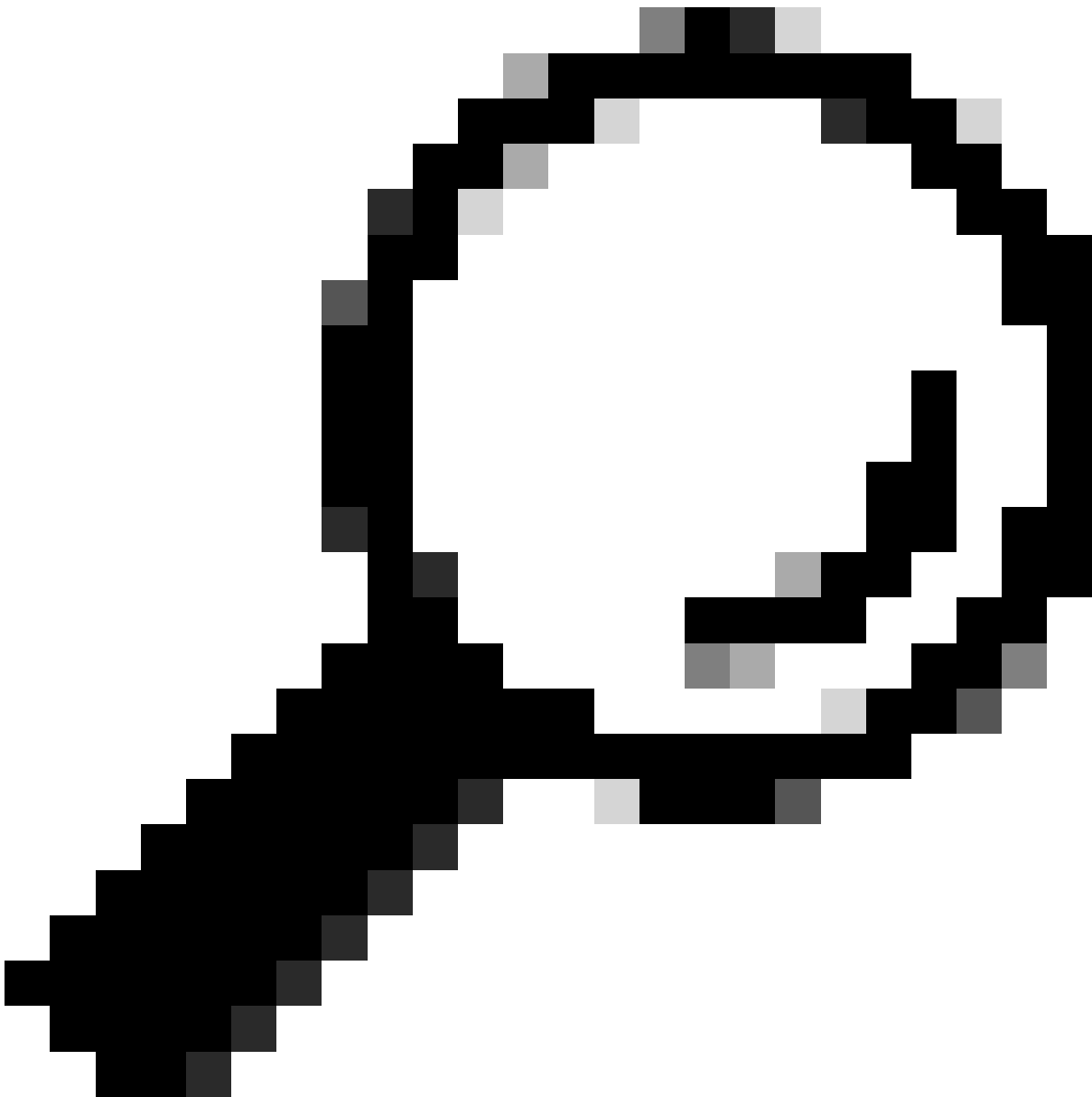
9124EWC(config)#wireless profile mesh default-mesh-profile
9124EWC(config-wireless-mesh-profile)#description "default mesh profile"
9124EWC(config-wireless-mesh-profile)#ethernet-bridging
9124EWC(config-wireless-mesh-profile)#ethernet-vlan-transparent
9124EWC(config-wireless-mesh-profile)#method authentication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

```

Llamada especial a la opción VLAN Transparente:

Esta función determina cómo un punto de acceso de malla maneja las etiquetas VLAN para el tráfico puenteado Ethernet:

- Si VLAN Transparent está habilitado, las etiquetas VLAN no se manejan y los paquetes se puentean como paquetes sin etiqueta.
  - No se requiere ninguna configuración de puertos Ethernet cuando se habilita la VLAN transparente. El puerto Ethernet pasa las tramas etiquetadas y no etiquetadas sin interpretar las tramas.
- Si VLAN Transparent está inhabilitado, todos los paquetes se gestionan de acuerdo con la configuración de VLAN en el puerto (troncal, acceso o modo normal).
  - Si el puerto Ethernet está configurado en el modo Trunk, se debe configurar el etiquetado de VLAN Ethernet.



Sugerencia: para utilizar el etiquetado de VLAN de punto de acceso, debe desactivar la casilla de verificación VLAN Transparente.

Si no utiliza etiquetado VLAN, significa que el RAP y el MAP están en la VLAN nativa configurada en los puertos troncales. En esta condición, si desea que otros dispositivos detrás de MAP estén en la VLAN nativa (aquí VLAN 100), debe habilitar VLAN Transparente.

---

5. El AP interno se une al EWC y puede verificar el estado de unión del AP usando el comando "show ap summary":

```

9124EWC#show ap summary
Number of APs: 1

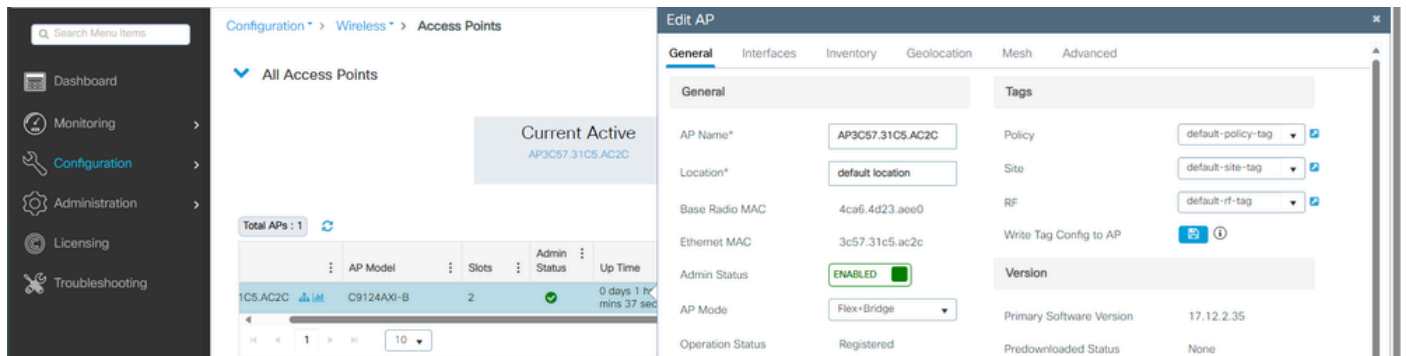
CC = Country Code
RD = Regulatory Domain

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

```

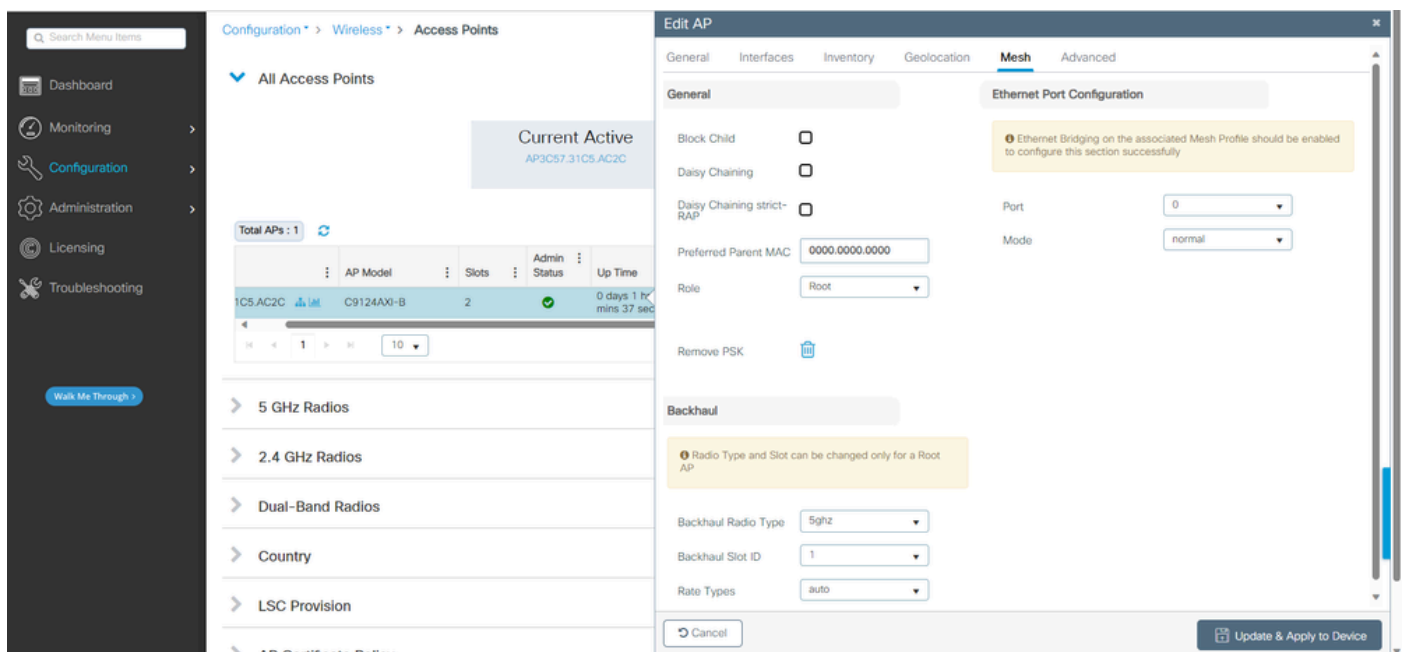
show ap summary

También puede ver el AP unido a través de la GUI donde el AP se muestra como modo Flex+Bridge. Para mayor comodidad, puede cambiar el nombre del AP ahora. En esta configuración se utiliza el nombre AP9124\_RAP:



Detalles generales de AP

Puede editar la geolocalización y, a continuación, en la ficha Mesh, asegúrese de que su función está configurada como Root AP y de que Ethernet Port Configuration está configurada como trunk con los ID de VLAN correspondientes:



Raíz de rol de malla

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

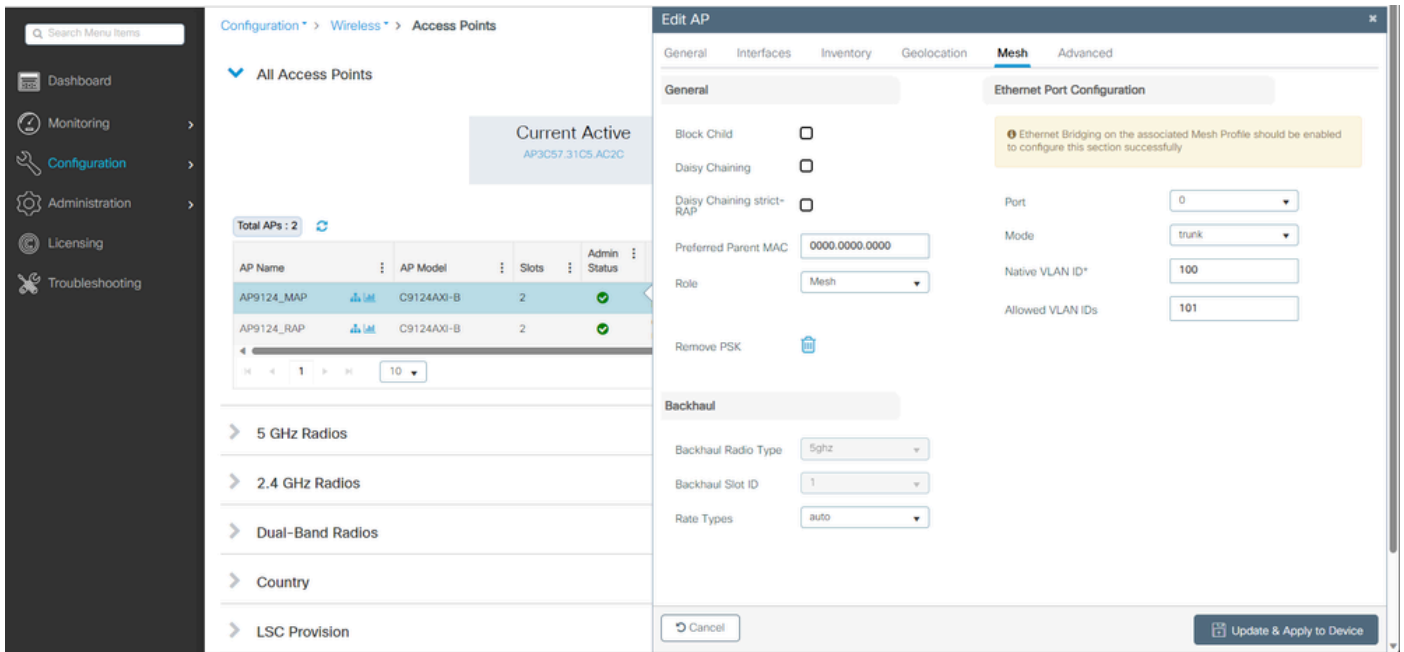
Configuración de puerto Ethernet

## Configurar MAP

Es hora de unirse al 9124 MAP.

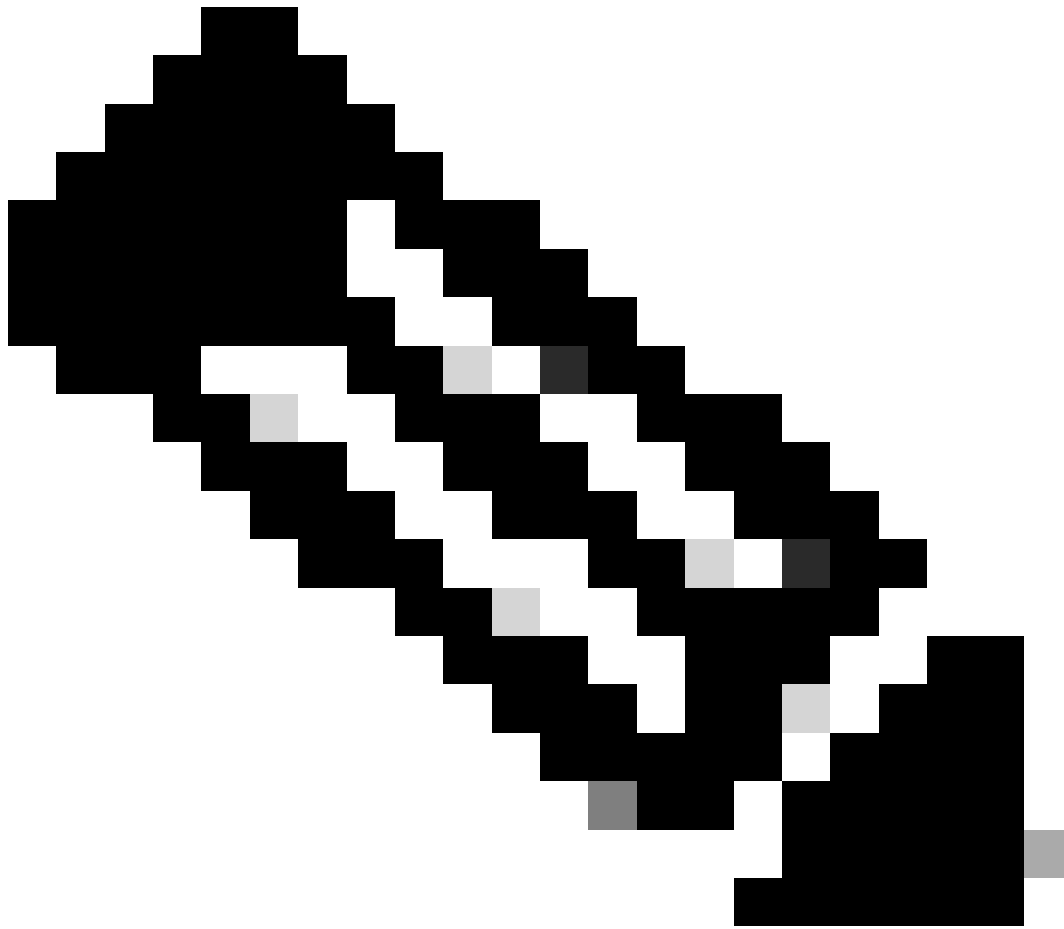
1. Conecte el AP MAP al Switch1 para el desarrollo. El AP se une al EWC y se muestra en la lista de AP. Cambie su nombre a algo como AP9124\_MAP y configúrelo como Mesh Role en la pestaña Mesh. Haga clic en Update & Apply to Device:





## Configuración de MAP

2. Desconecte el AP del Switch1 y conéctelo al Switch2 según el Diagrama de red. El MAP se une al EWC a través de la interfaz inalámbrica a través del RAP.



Nota: Como los AP se alimentan a través del inyector de energía, el AP no se apaga, y como la configuración está en un entorno controlado, el Switch2 está físicamente cerca y podemos simplemente mover el cable de un switch al otro.

---

Puede conectar un cable de consola al AP y ver qué sucede a través de la consola. Aquí se ven algunos mensajes importantes.

---

Nota: a partir de la versión 17.12.1, la velocidad en baudios de la consola predeterminada de los AP 802.11AX cambia de 9600 bps a 115200 bps.

---

MAP pierde conectividad con 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 pasa al modo de detección vía inalámbrica y encuentra el RAP vía Radio Backhaul en el canal 36, encuentra el EWC y se une a él:

```
[*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 se une ahora a EWC a través de RAP.

El AP C9115 ahora puede obtener una dirección IP en la VLAN 100 y luego unirse al EWC:



Advertencia: Tenga en cuenta que la VLAN 100 es la VLAN nativa troncal de los puertos de switch. Para que el tráfico del AP en la VLAN 100 llegue al WLC en la VLAN 100, el link de malla debe tener VLAN Transparent habilitada. Esto se realiza en la sección de conexión en puente Ethernet del perfil de malla.

```
[*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]
[*01/19/2024 11:40:58.2070] CAPWAP State: Init
[*01/19/2024 11:40:58.2150]
[*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]
[*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]
[*01/19/2024 15:13:56.0070] CAPWAP State: DTLS Setup
```

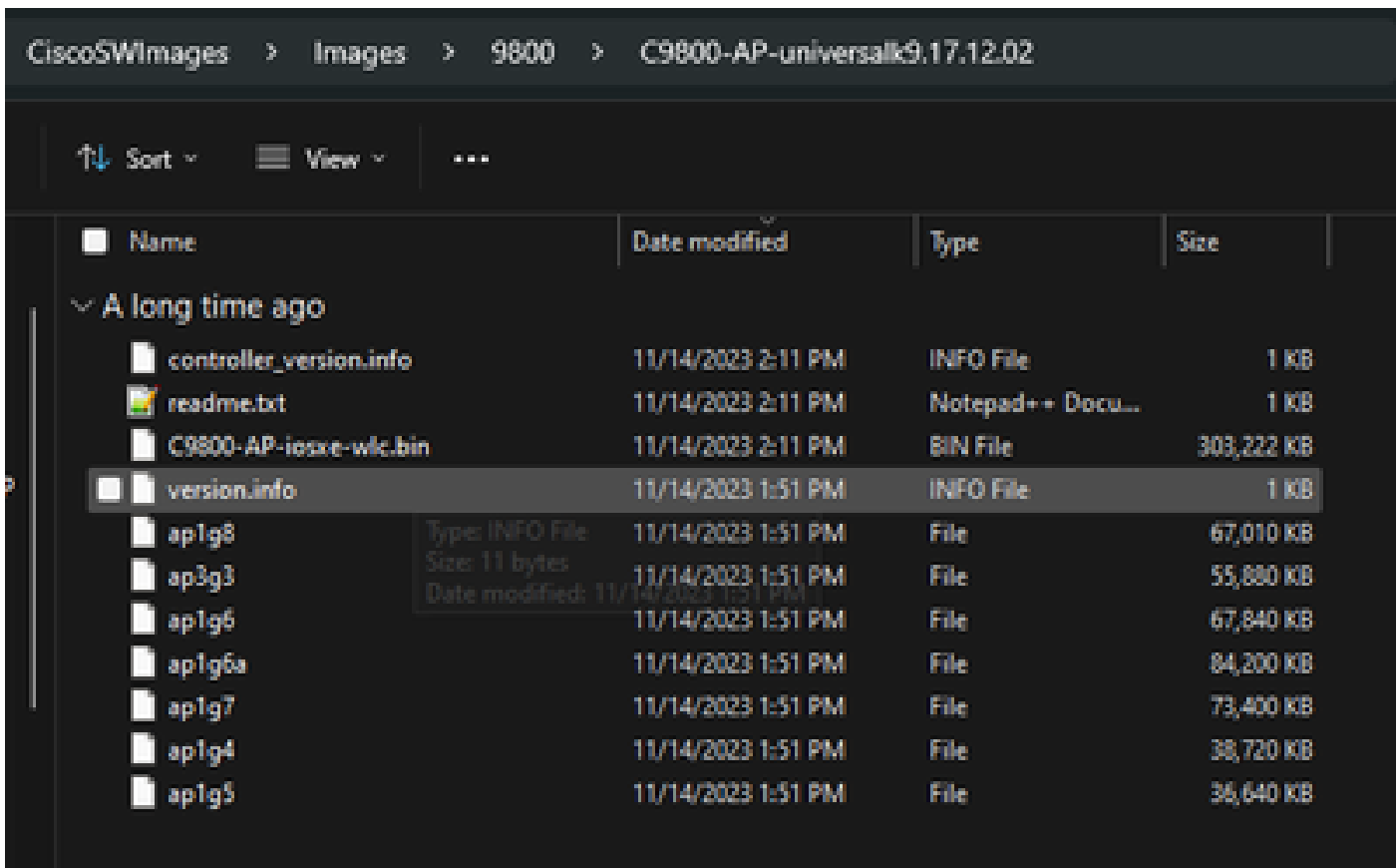
```

[...]
[*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!

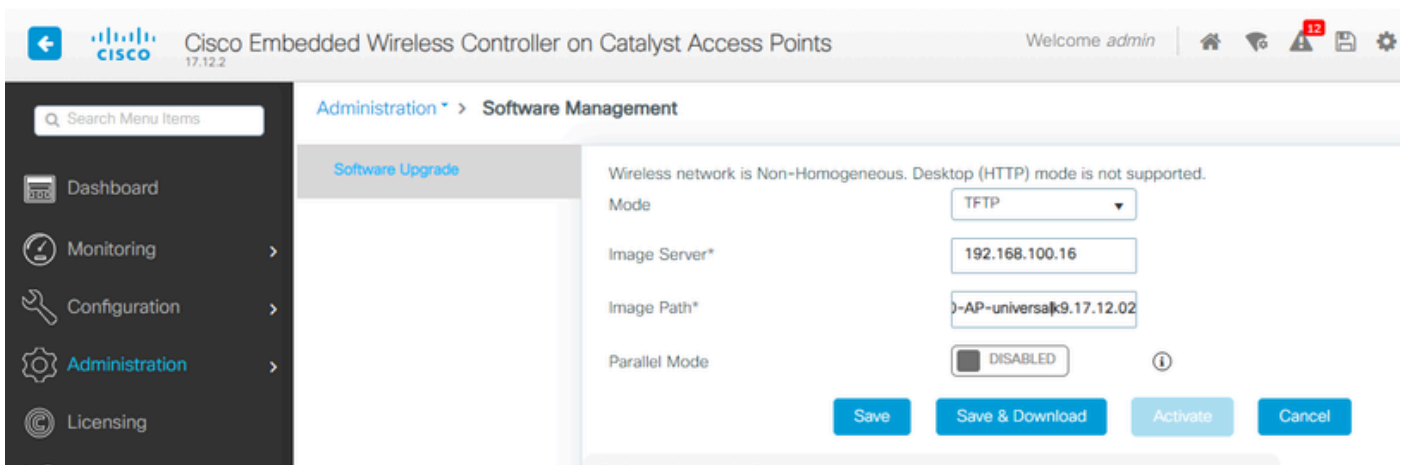
```

Como se trata de un EWC AP, solo contiene la imagen de AP que corresponde a su propio modelo (aquí un C9124 ejecuta ap1g6a). Cuando se une a un modelo diferente de AP, tiene una red no homogénea.

En estas condiciones, si el AP no está en la misma versión, necesita descargar la misma versión, por lo tanto, asegúrese de que tiene un servidor TFTP/SFTP válido y una ubicación, con las imágenes del AP, configuradas en EWC > Administration > Software Management:



Servidor TFTP con carpeta de imágenes AP

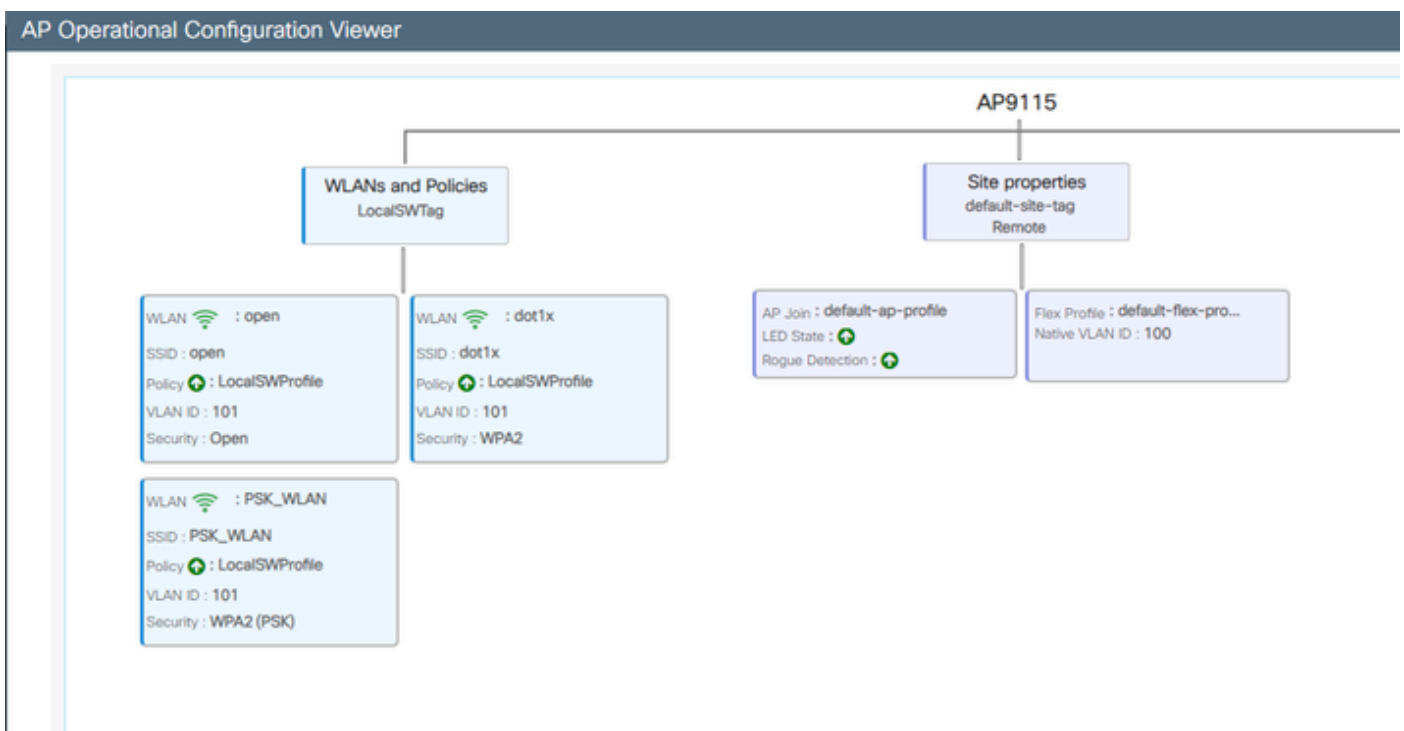


Imágenes de PA

El AP se muestra en la lista AP y puede asignar una PolicyTag:

The screenshot shows the Cisco Embedded Wireless Controller interface. On the left is a navigation sidebar with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area is titled 'Configuration > Wireless > Access Points'. It displays a table of 'All Access Points' with columns for AP Name, AP Model, Slots, Admin Status, and Up Time. A 'Current Active' box highlights AP9124\_RAP. Below the table, there are '5 GHz Radios' and a 'Total APs : 3' indicator. On the right, the 'Edit AP' configuration page for AP9115 is shown, with tabs for General, Interfaces, Inventory, Geolocation, ICap, and Advanced. The General tab is active, showing fields for AP Name (AP9115), Location (default location), Base Radio MAC, Ethernet MAC, Admin Status (ENABLED), AP Mode (Flex), Operation Status (Registered), Fabric Status (Disabled), CleanAir (NSI Key), LED Settings (ENABLED), and Tags (LocalSWTag, default-site-tag, default-rf-tag). A Version section shows Primary Software Version 17.12.2.35 and Predownloaded Status as Predownloading.

Lista de puntos de acceso con detalles del 9115



Vista operativa del PA

## Verificación

Puede ver el árbol de malla a través de la GUI, que también proporciona el resultado de CLI si utiliza el comando "show wireless mesh ap tree". En la GUI, vaya a 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

```

Árbol AP de malla

En el RAP y el MAP, puede verificar la red de retorno de malla mediante el 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 show mesh backhaul

```

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

Puede verificar la configuración de Trunking VLAN de malla en el lado del AP:

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:

El portátil 2 conectado en el switch 2 recibió la dirección IP de la 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
```

El Laptop1 ubicado en el Switch1 recibió una IP de 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: Tenga en cuenta que para probar el ICMP entre los dispositivos de Windows debe permitir el ICMP en el firewall del sistema. De forma predeterminada, los dispositivos de Windows bloquean el ICMP en el firewall del sistema.

---

Otra prueba sencilla para verificar el puente Ethernet es tener SVI para VLAN 101 en ambos switches y configurar Switch2 SVI para DHCP. El Switch2 SVI para VLAN 101 obtiene la IP de VLAN 101 y puede hacer ping al Switch 1 VLAN 101 SVI para verificar la conectividad de 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#
```

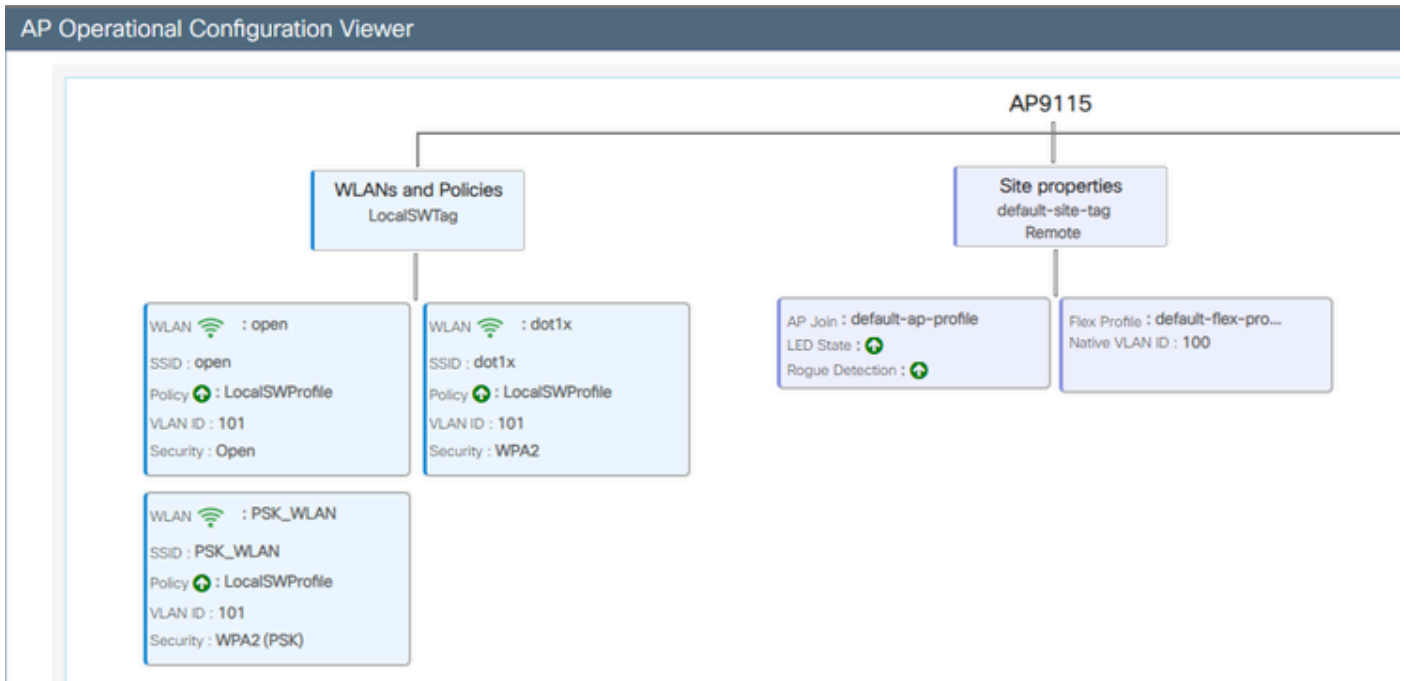
El AP C9115 de modo local también se unió al EWC:

The screenshot shows the Meraki dashboard interface. On the left is a navigation sidebar with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area is titled 'Configuration > Wireless > Access Points' and shows 'All Access Points'. At the top, there are three summary boxes: 'Current Active' (AP9124\_RAP), 'Current Standby' (Not Applicable), and 'Preferred Active' (AP9124\_RAP). Below this is a table with 3 total APs.

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 Se unió al EWC

Se crearon 3 WLAN, abiertas, PSK y dot1x asignadas a un perfil de política con VLAN 101 definida en las políticas de acceso:



Configuración operativa de AP9115

Los clientes inalámbricos pueden conectarse a las WLAN:

Monitoring > Wireless > Clients

Selected 2 out of 2 Clients

Client MAC Address	IP Address	IPv6 Address	AP Name	Site ID	SSID	WLAN ID	Client Type	Status
9294-809a-e572	192.168.101.14	fe80:9294-809a-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

## Troubleshoot

En esta sección, se presentan comandos útiles y algunos consejos, trucos y recomendaciones.

Comandos útiles

En 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
```

show 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
```

Opciones de malla de depuración RAP/MAP

En 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

Para depurar en el WLC, el mejor punto de inicio es utilizar el seguimiento de RadioActive con la dirección MAC del MAP/RAP.

Ejemplo 1: RAP recibe adyacencia de MAP y realiza la autenticación correctamente

<#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-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

```

Ejemplo 2: la dirección MAC de MAP no se agregó al WLC o se agregó incorrectamente

<#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

```

Ejemplo 3: el RAP pierde el 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
```

## Consejos, trucos y recomendaciones

- Al actualizar el MAP y el RAP a la misma versión de imagen a través del cable, evitamos que la descarga de imágenes se realice por el aire (lo que puede resultar problemático en entornos de RF "sucios").
- Se recomienda encarecidamente probar la configuración en un entorno controlado antes de implementarla in situ.
- Si está probando el puente Ethernet con ordenadores portátiles con Windows en cada lado, tenga en cuenta que para probar el ICMP entre los dispositivos de Windows debe permitir el ICMP en el firewall del sistema. De forma predeterminada, los dispositivos de Windows bloquean el ICMP en el firewall del sistema.
- Si se utilizan AP con antenas externas, asegúrese de consultar la guía de implementación para verificar qué antenas son compatibles y qué puerto se supone que deben estar conectadas.
- Para unir el tráfico de diferentes VLAN sobre el link de malla, la función VLAN Transparent

debe ser inhabilitada.

- Considere la posibilidad de tener un servidor syslog local para los AP, ya que puede proporcionar información de depuración que, de lo contrario, sólo está disponible con una conexión de consola.

## Referencias

[Hoja de datos del controlador inalámbrico integrado de Cisco en puntos de acceso Catalyst](#)

[Informe técnico sobre el controlador inalámbrico integrado de Cisco en puntos de acceso Catalyst \(EWC\)](#)

[Configuración del Link de Malla Punto a Punto con Puente Ethernet en los AP de Mobility Express](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).