

Configuración de malla en los controladores de LAN inalámbrica de Catalyst 9800

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Caso práctico 1: Modo puente](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Caso práctico 2: Flex + Bridge](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe un ejemplo de configuración básica sobre cómo unir un punto de acceso (AP) de malla al controlador de LAN inalámbrica (WLC) Catalyst 9800

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Modelo de configuración de Catalyst Wireless 9800
- Configuración de LAPs
- Control y suministro de puntos de acceso inalámbricos (CAPWAP)
- Configuración de un servidor DHCP externo
- Configuración de los switches Cisco

Componentes Utilizados

Este ejemplo utiliza un punto de acceso ligero (1572AP y 1542) que se puede configurar como un punto de acceso raíz (RAP) o un punto de acceso de malla (MAP) para unirse al WLC de Catalyst 9800. El procedimiento es idéntico para los puntos de acceso 1542 o 1562. El RAP está conectado al WLC Catalyst 9800 a través de un switch Cisco Catalyst.

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

- C9800-CL v16.12.1
- Switch de capa 2 de Cisco
- Sección Lightweight Outdoor Access Points de Cisco Aironet serie 1572 para el puente

- Cisco Aironet 1542 para la sección Flex+Bridge

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.

Configurar

Caso práctico 1: Modo puente

Diagrama de la red

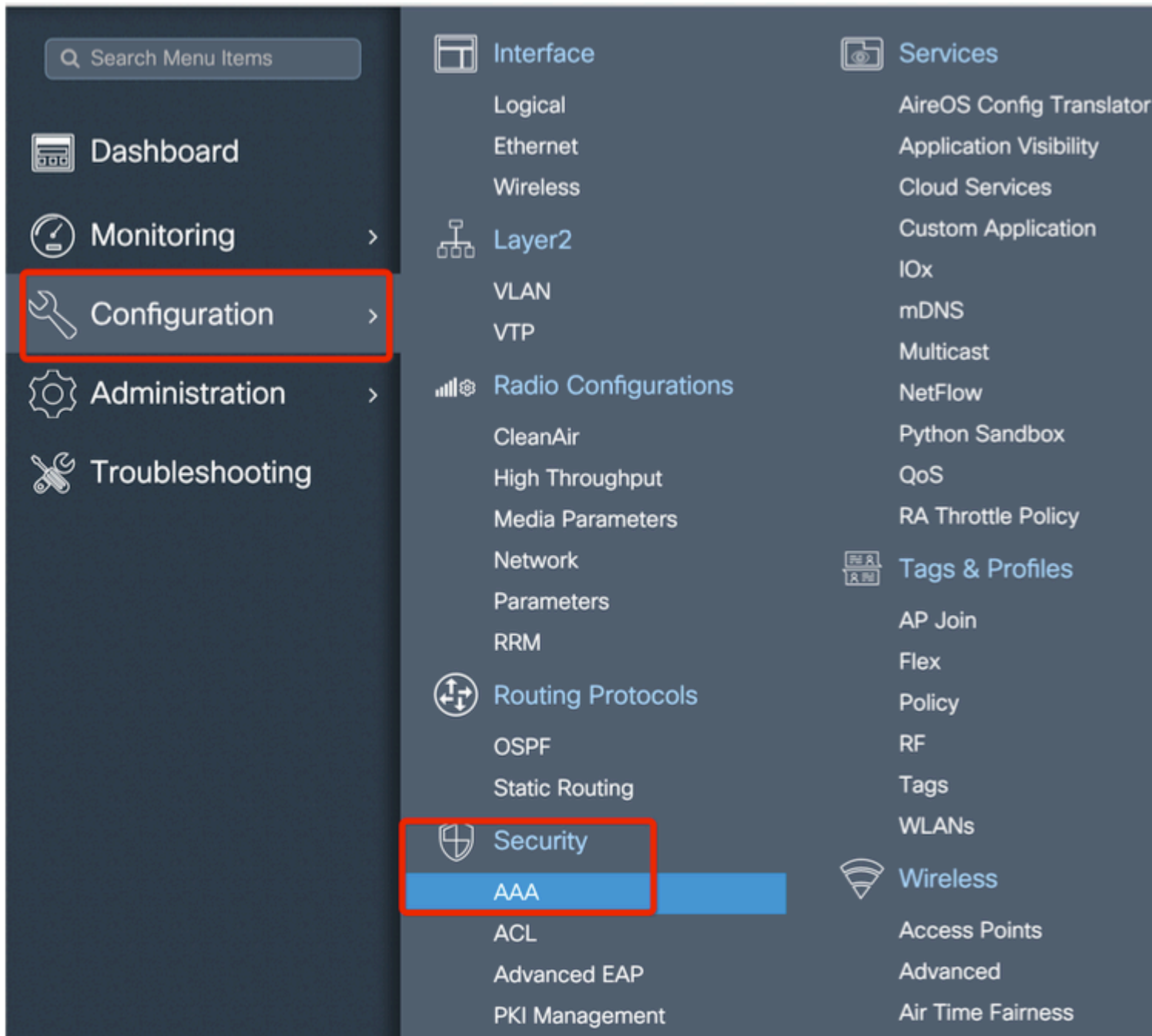
Configuraciones

Un AP de malla necesita ser autenticado para que se una al controlador 9800. Este caso práctico considera que usted se une al AP en el modo local primero al WLC y después lo convierte al modo de malla del puente (también conocido como).

Para evitar la asignación de perfiles de unión de AP, utilice este ejemplo pero configure el método de descarga de credenciales de autorización de aaa predeterminado de modo que cualquier AP de malla pueda unirse al controlador.

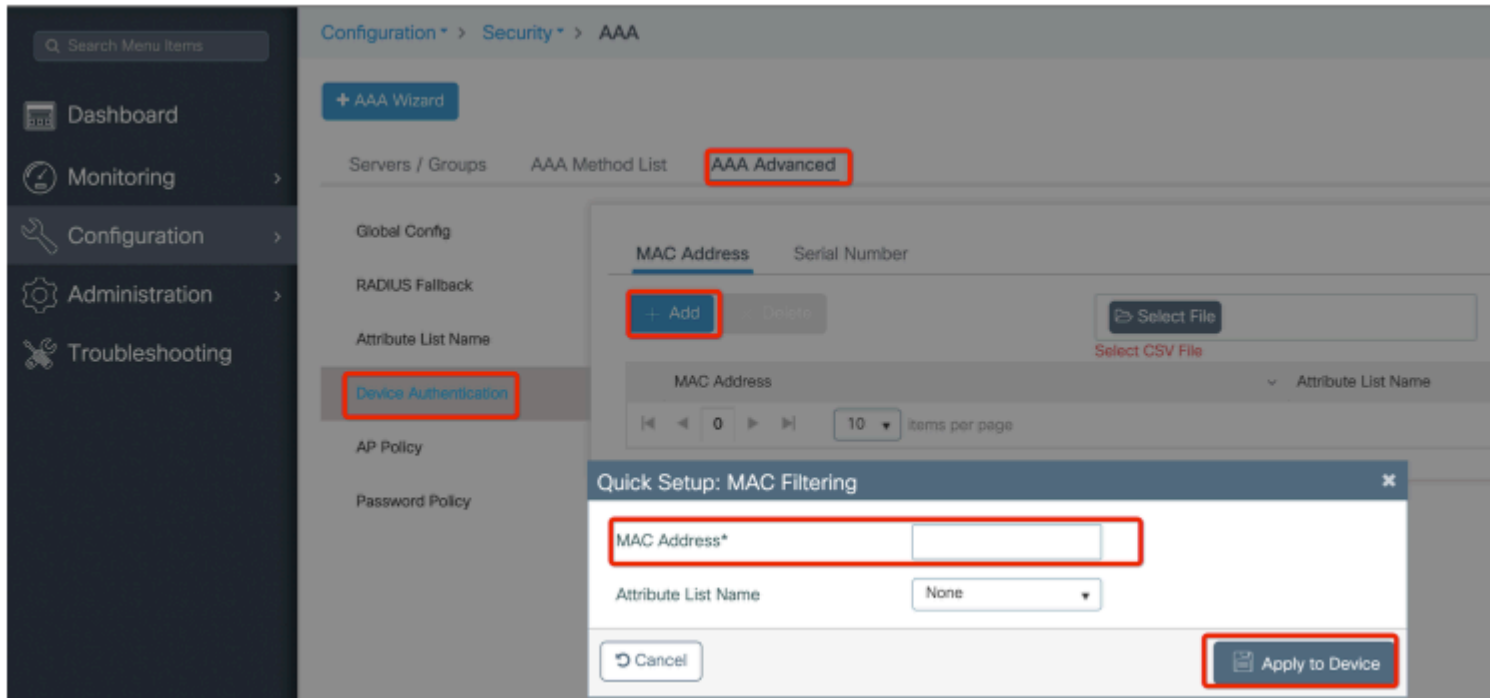
Paso 1: Configure las direcciones MAC de RAP/MAP en Autenticación del Dispositivo.

Vaya a **Configuration > AAA > AAA Advanced > Device Authentication** .



Agregue la dirección MAC de Ethernet base de los puntos de acceso de malla, agréguela sin caracteres especiales, sin '.' o ':'

Importante: a partir de la versión 17.3.1, iSi se agrega cualquier delimitador de dirección mac como '.', ':' o '-', el AP no puede unirse. Actualmente hay 2 mejoras abiertas para esto: [ID de bug de Cisco CSCyv43870](#) e ID de bug de Cisco [CSCvr07920](#). En el futuro, 9800 aceptará todos los formatos de direcciones MAC.



Paso 2: Configure la lista de métodos de autenticación y autorización.

Vaya a **Configuration > Security > AAA > AAA Method list > Authentication** y cree la lista de métodos de autenticación y la lista de métodos de autorización.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

Delete

Quick Setup: AAA Authorization

Method List Name*

Mesh_Authz

Type*

credential-download

Group Type

local

Authenticated

Available Server Groups

radius
ldap
tacacs+
ISE-Group
ISE_grp_I2

Assigned Server Groups

>

<

Cancel

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add Delete

Quick Setup: AAA Authentication

Method List Name*	Mesh_Authentication
Type*	dot1x
Group Type	local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-Group
- ISE_grp_I2

Assigned Server Groups

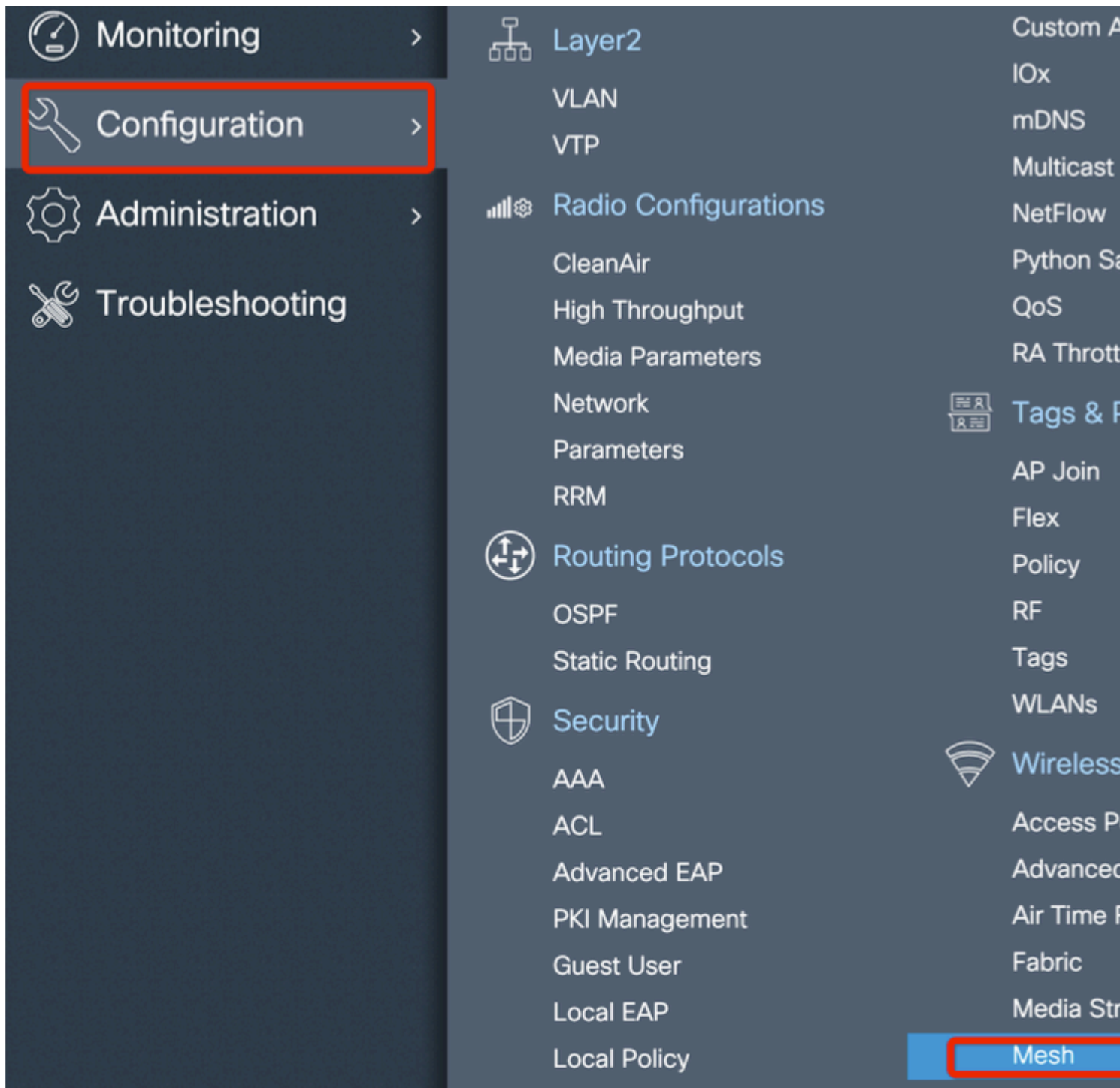
>

<

Cancel

Paso 3: Configure los parámetros de malla global.

Vaya a **Configuration > Mesh > Global** parameters. Inicialmente, podemos mantener estos valores predeterminados.



Paso 4: Cree un nuevo perfil de malla en **Configuration > Mesh > Profile > +Add**

Global Config **Profiles**

+ Add Delete

Number of Profiles : **1**

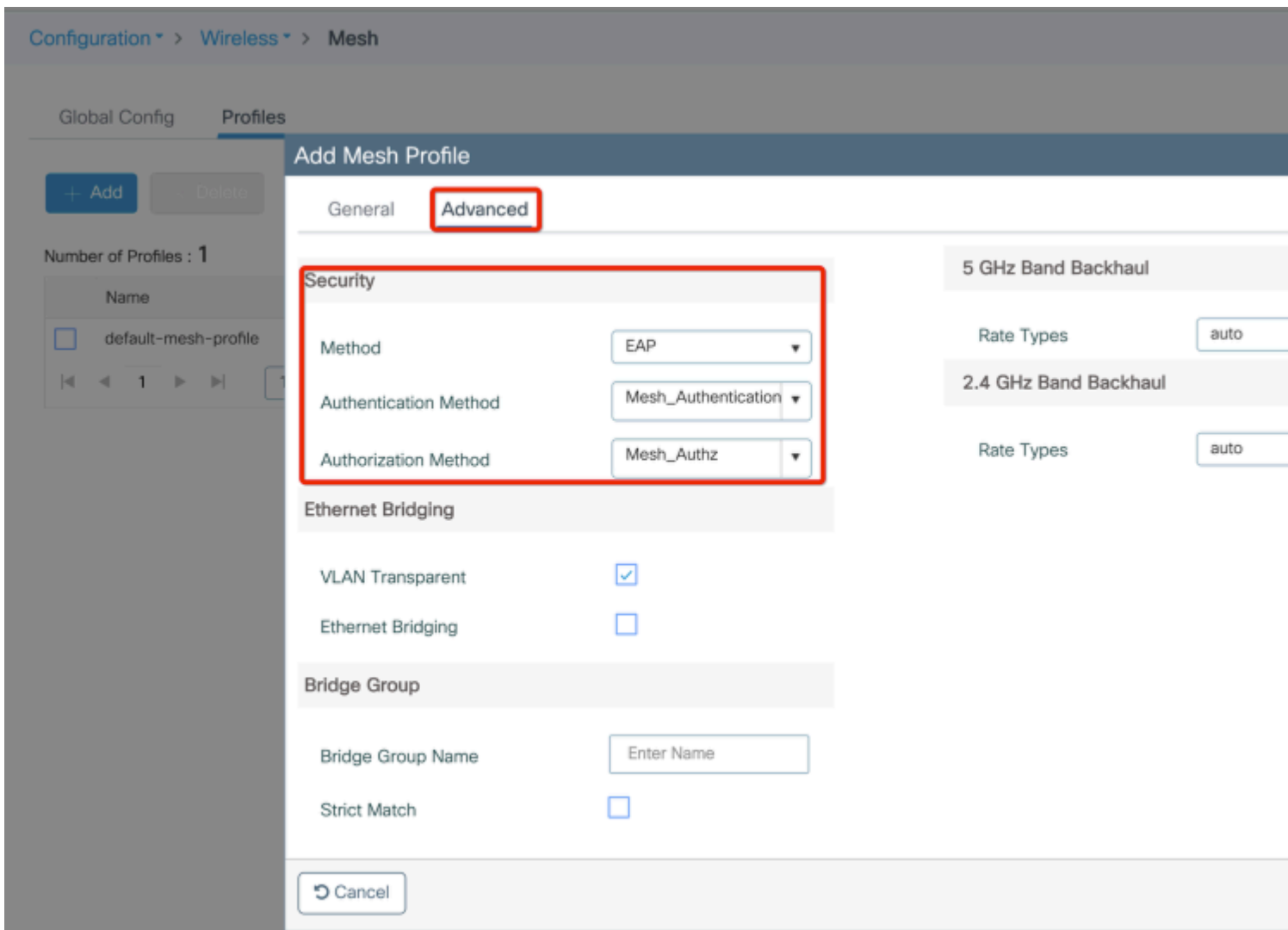
Add Mesh Profile

General Advanced

Name*	<input type="text" value="Mesh_Profile"/>	Backhaul amsdu	<input checked="" type="checkbox"/>
Description	<input type="text" value="Enter Description"/>	Backhaul Client Access	<input type="checkbox"/>
Range (Root AP to Mesh AP)	<input type="text" value="12000"/>	Battery State for an AP	<input checked="" type="checkbox"/>
Multicast Mode	<input type="text" value="In-Out"/>	Full sector DFS status	<input checked="" type="checkbox"/>
IDS (Rogue/Signature Detection)	<input type="checkbox"/>		
Convergence Method	<input type="text" value="Standard"/>		
Background Scanning	<input type="checkbox"/>		
Channel Change Notification	<input type="checkbox"/>		
LSC	<input type="checkbox"/>		


Haga clic en el perfil de malla creado para editar la configuración general y avanzada del perfil de malla.


En el diagrama que se muestra, necesitamos asignar el perfil de autenticación y autorización creado antes al perfil de malla




Paso 5: Crear un nuevo perfil de unión a AP. Vaya a **Configure > Tags and Profiles: AP Join.**


Search Menu Items

 Dashboard

 Monitoring >

 Configuration >

 Administration >

 Troubleshooting

 Interface

Logical
Ethernet
Wireless

 Layer2

VLAN
VTP

 Radio Configurations

CleanAir
High Throughput
Media Parameters

Network
Parameters
RRM

 Routing Protocols

OSPF
Static Routing

 Security

AAA
ACL

 Services

AireOS C
Applicatio
Cloud Se
Custom A
IOx
mDNS
Multicast
NetFlow
Python S
QoS
RA Throt

 Tags & Profiles

AP Join
Flex
Policy
RF
Tags
WLANs

 Wireless

Access P

Configuration > Tags & Profiles > AP Join

+ Add - Delete

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile

General Client CAPWAP AP Management Rogue AP ICap

Name* Mesh_AP_Join_Profile

Description Enter Description

LED State

LAG Mode

NTP Server 0.0.0.0

Cancel

Aplique el perfil de malla previamente configurado y configure la autenticación EAP AP:

AP Join Profile Name	Description
<input type="checkbox"/> default-ap-profile	default ap profile

Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Code

AP EAP Auth Configuration

EAP Type

AP Authorization Type

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

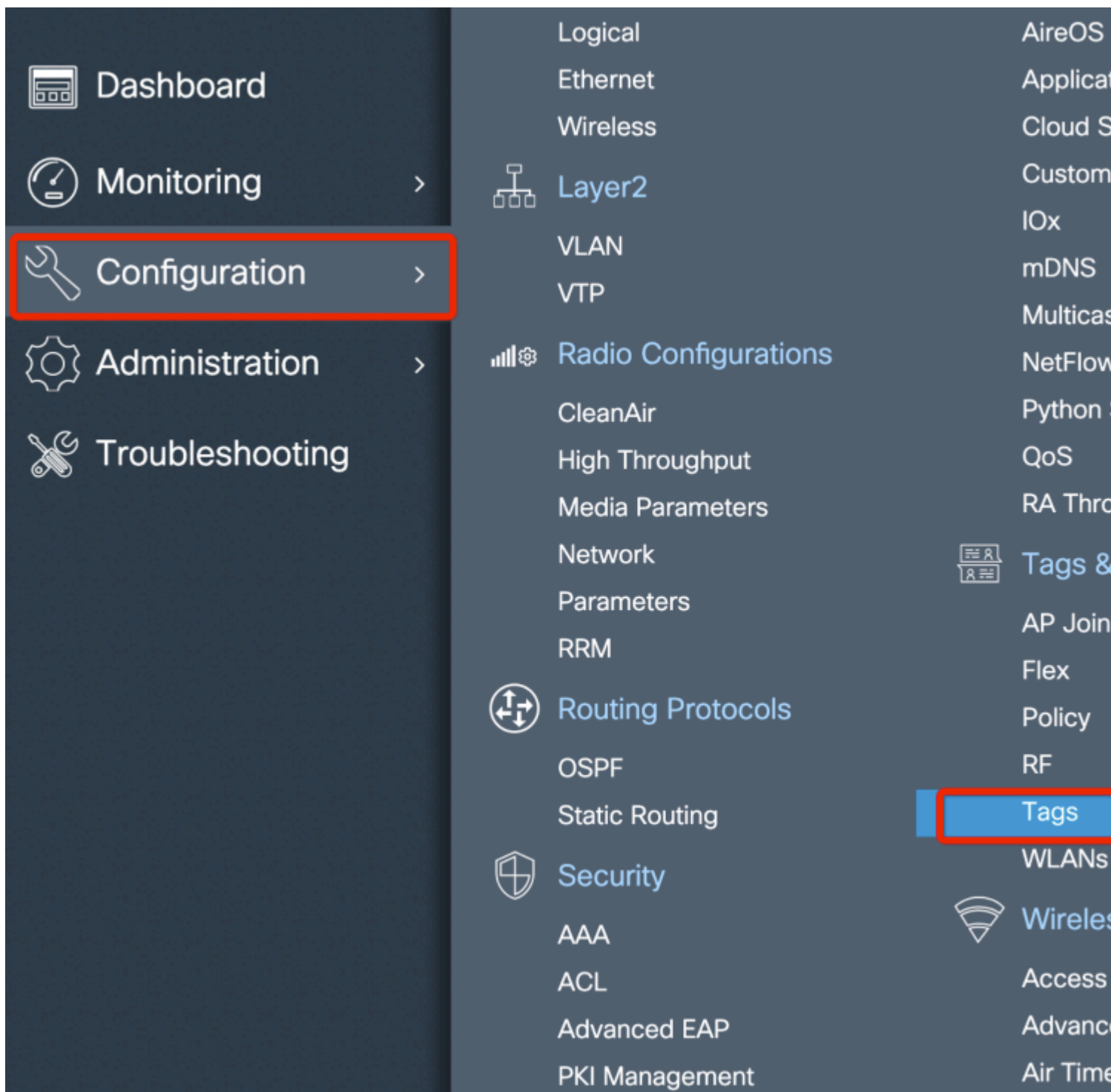
Extended Module

Enable

Mesh

Profile Name

Paso 6: Cree una etiqueta de ubicación de malla como se muestra.



Configure (Configurar) Haga clic en la ETIQUETA de ubicación de malla creada en el paso 6 para configurarla.

Acceder a la ficha Sitio y aplicarle el perfil de unión de Mesh AP previamente configurado:

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add - Delete

Add Site Tag

Name* Mesh_AP_tag

Description Enter Description

AP Join Profile Mesh_AP_Join_Profi

Control Plane Name

Enable Local Site

Cancel

Paso 7. Convierta el AP al modo Bridge.

Configuration > Wireless > Access Points

▼ All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2	✔	109.129.49.9

1 10 items per page

> 5 GHz Radios

> 2.4 GHz Radios

> Dual-Band Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* AP2C33-110E-6B66

Location* default location

Base Radio MAC 7070.8bb4.9200

Ethernet MAC 2c33.110e.6b66

Admin Status **ENABLED**

AP Mode Bridge

Operation Status

Fabric Status

LED State

a través de la CLI, puede utilizar este comando en el AP:

capwap ap mode bridge

El AP se reinicia y vuelve a unirse como modo Bridge.

Paso 8. Ahora puede definir el rol del AP: AP raíz o AP de malla.

El AP raíz es el que tiene una conexión cableada al WLC mientras que el AP de la malla se une al WLC vía su radio que intenta conectar a un AP raíz.

Un AP de malla puede unirse al WLC a través de su interfaz cableada una vez que no ha podido encontrar un AP raíz a través de su radio, para propósitos de provisión.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address
AP2C33-110E-6B66	AIR-AP1562E-E-K9	2		109.129.49.9

5 GHz Radios

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provision

Edit AP

General Interfaces High Availability Inventory **Mesh**

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

VLAN Trunking Native

Role
Mesh
Root
Mesh

Remove PSK

Backhaul

Backhaul Radio Type

Backhaul Slot ID

Rate Types

Verificación

```
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default local
aaa authentication dot1x Mesh_Authentication local
```

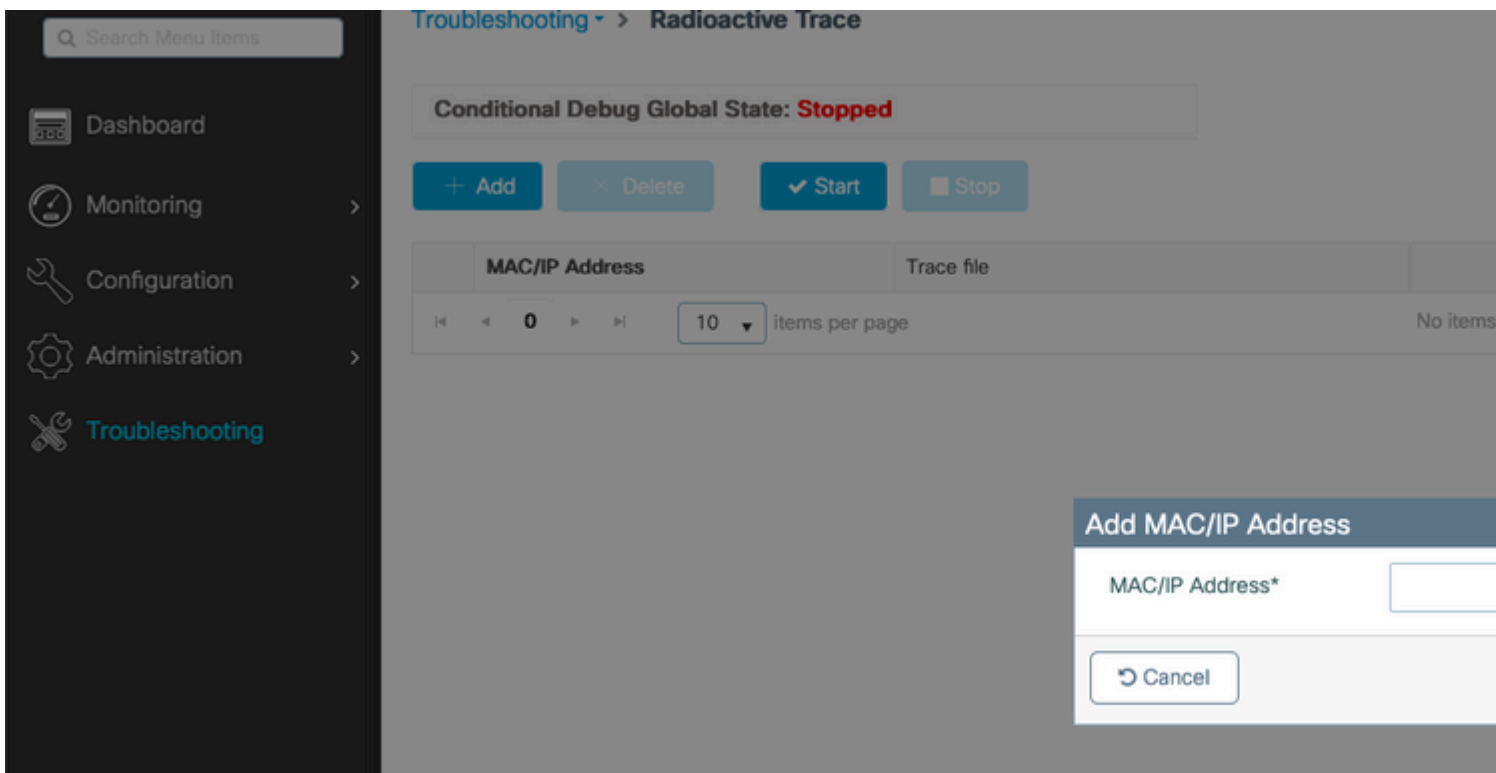
```

aaa authorization network default local
aaa authorization credential-download default local
aaa authorization credential-download Mesh_Authz local
username 111122223333 mac
wireless profile mesh Mesh_Profile
  method authentication Mesh_Authentication
  method authorization Mesh_Authz
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site Mesh_AP_Tag
  ap-profile Mesh_AP_Join_Profile
ap profile Mesh_AP_Join_Profile
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
  mesh-profile Mesh_Profile

```

Troubleshoot

En la página **Troubleshooting** > **Radioactive Trace** Web UI, haga clic en **add** e ingrese la dirección MAC del AP.



Haga clic en **Inicio** y espere a que el AP intente unirse al controlador otra vez.

Una vez hecho esto, haga clic en **Generar** y elija un período de tiempo para recopilar los registros (por ejemplo, los últimos 10 o 30 minutos).

Haga clic en el nombre del archivo de seguimiento para descargarlo del explorador.

Aquí hay un ejemplo de AP no unido debido a que se definió el nombre incorrecto del método de autorización aaa :


```

019/11/28 13:08:38.269 {wncd_x_R0-0}{1}: [capwapac-smgr-srvr] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [23388]: (info): DTLS record type: 23, applic
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess] [23388]: (info): Session-IP: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [mesh-config] [23388]: (ERR): Failed to get ap PMK cache rec s
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (info): 00a3.8e95.6c40 Ap auth pe
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): Failed to initialize autho
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-capwap-join] [23388]: (ERR): 00a3.8e95.6c40 Auth reques
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get wtp re
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [apmgr-db] [23388]: (ERR): 00a3.8e95.6c40 Failed to get ap tag
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (ERR): Session-IP: 192.168.8
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (info): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [capwapac-smgr-sess-fsm] [23388]: (note): Session-IP: 192.168
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.4
2019/11/28 13:08:38.288 {wncd_x_R0-0}{1}: [ewlc-dtls-sessmgr] [23388]: (info): Remote Host: 192.168.88.4
2019/11/28 13:08:38.289 {wncmgrd_R0-0}{1}: [ewlc-infra-evq] [23038]: (debug): instance :0 port:38932MAC

```

Lo mismo se puede ver más fácilmente en el panel de interfaz de usuario web cuando se hace clic en AP no unidos. "Ap auth pending" es el indicio que apunta hacia la autenticación del propio AP:

The screenshot displays two panels from a network management interface:

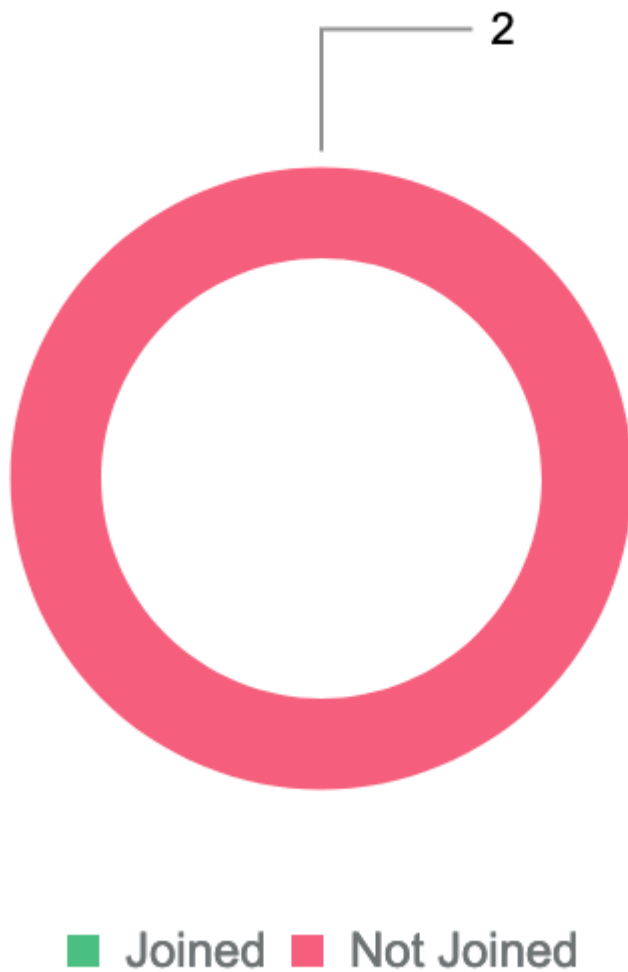
- AP Statistics Panel:**
 - Navigation: Monitoring > Wireless > AP Statistics
 - Sub-panels: General, **Join Statistics**
 - Buttons: Clear, ClearAll
 - Number of AP(s): 2
 - Status filter: "Is equal to" NOT JOINED
 - Table of APs:

AP Name	AP Model
AP2CF8-9B5F-7D70	C9120A
NA	
 - Page controls: 1 of 10 items per page
- Join Statistics Panel:**
 - Sub-panels: General, **Statistics**
 - DTLS Session Statistics:

DTLS Session request received	1	Configuration
Established DTLS session	1	Successful co responses se
Unsuccessful DTLS session	0	Unsuccessful request proce
Reason for last unsuccessful DTLS session	DTLS Handshake Success	Reason for las configuration
Time at last successful DTLS session	Mon, 17 Feb 2020 09:15:41 GMT	Time at last s configuration
Time at last unsuccessful DTLS session	NA	Time at last u configuration
 - Join phase statistics:

Join requests received	1	Data DTLS S
Successful join responses sent	0	DTLS Session
Unsuccessful join request processing	0	Established D
Reason for last unsuccessful join attempt	Ap auth pending	Unsuccessful
Time at last successful join attempt	NA	Reason for las DTLS session
Time at last unsuccessful join attempt	NA	Time at last s session
		Time at last u session

Access Point Join Summary

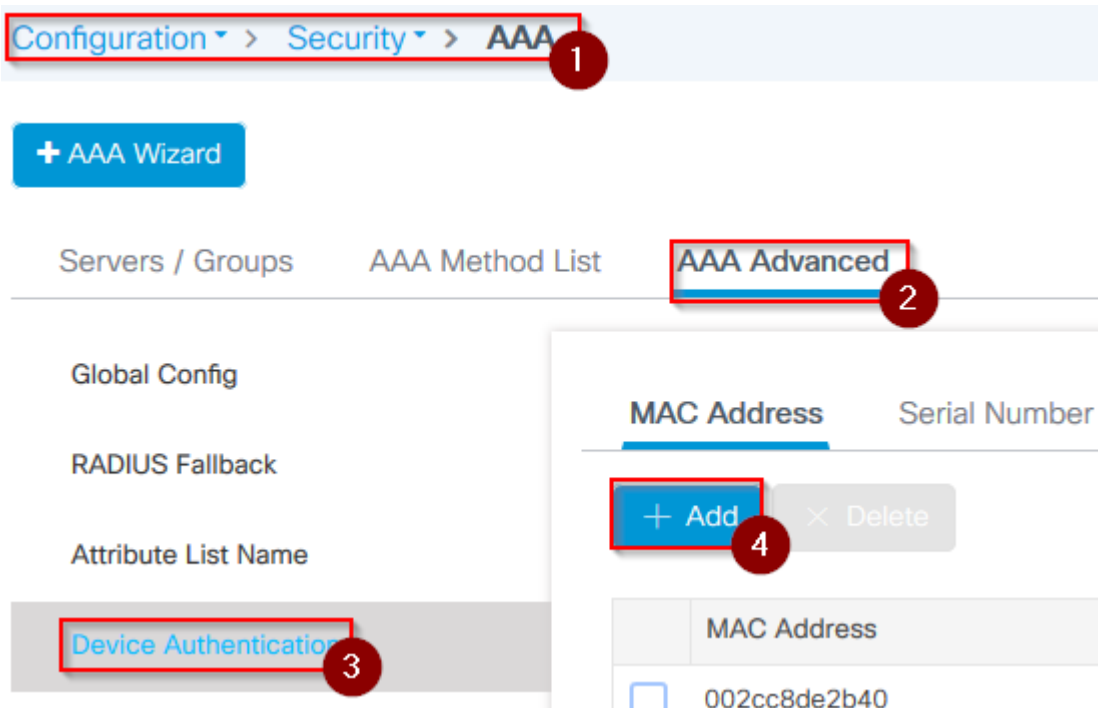


Caso práctico 2: Flex + Bridge

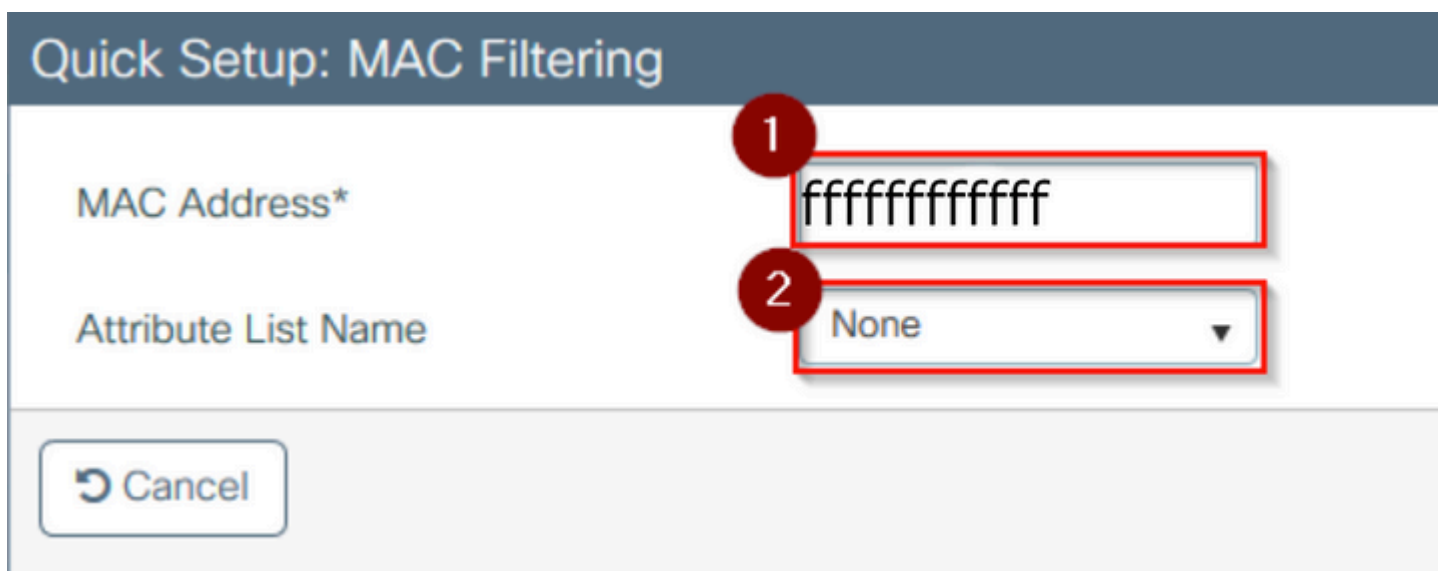
Esta sección resalta el proceso de unión de un AP 1542 en el modo Flex+Bridge con la autenticación EAP hecha localmente en el WLC.

Configurar

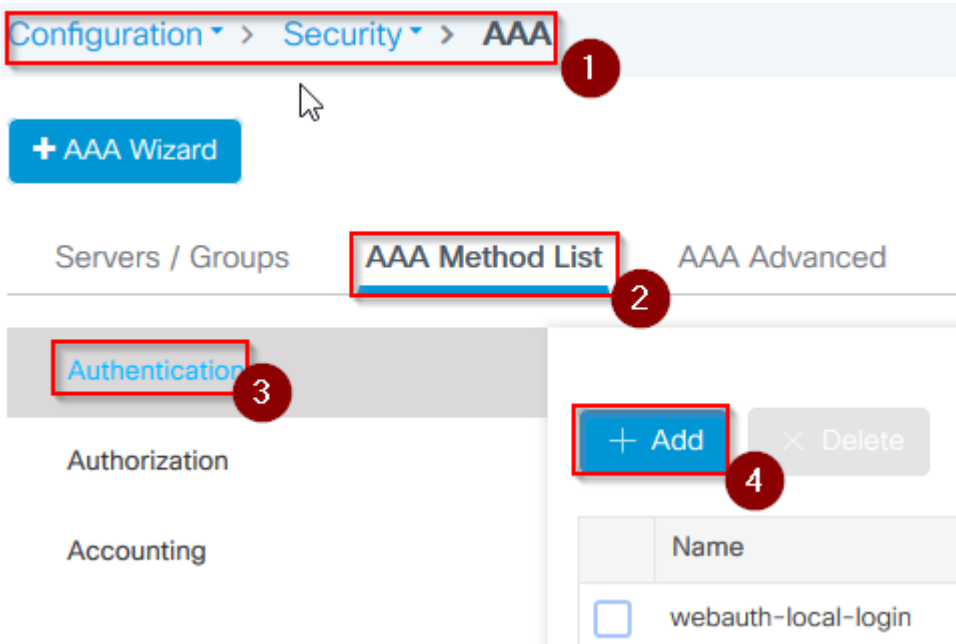
- Paso 1. Vaya a **Configuration > Security > AAA > AAA Advanced > Autenticación de dispositivo**



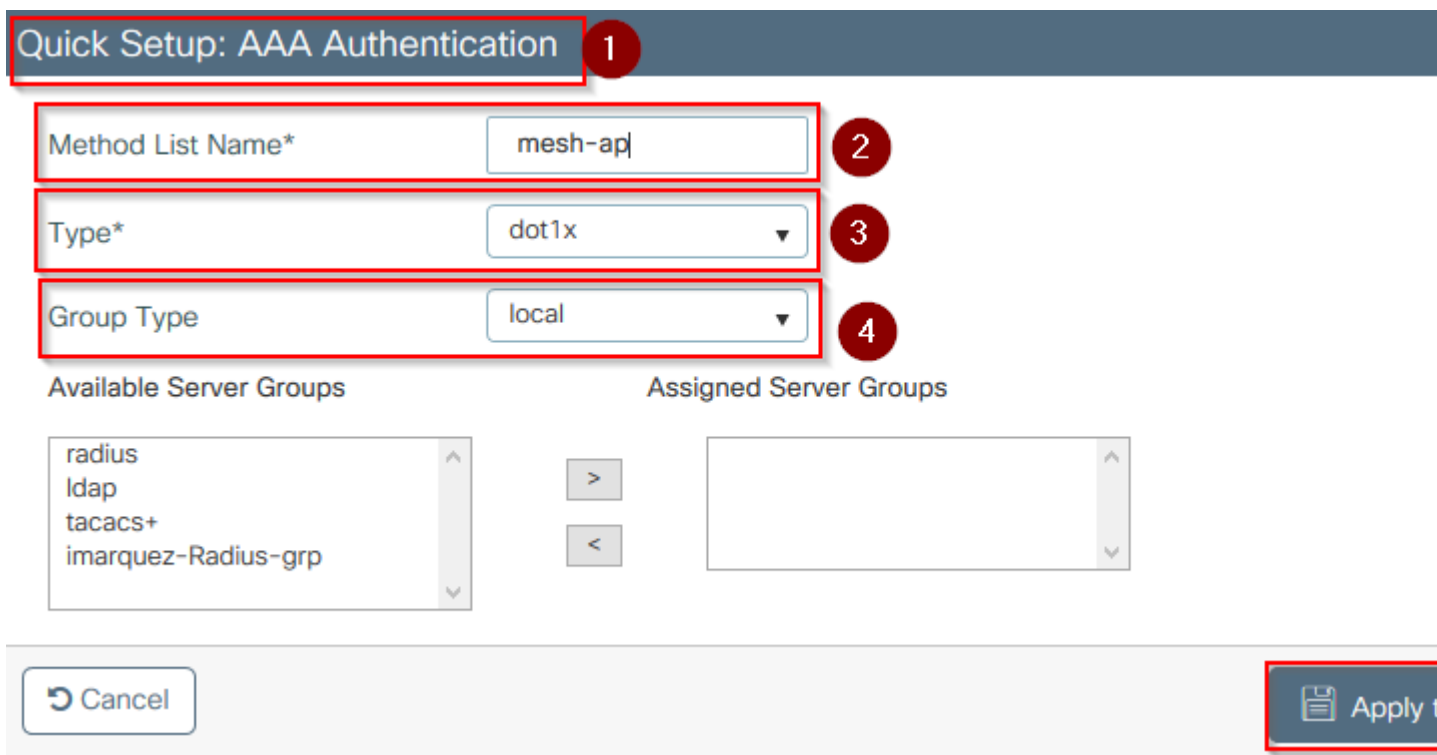
- Paso 2. Seleccione **Autenticación de dispositivo** y seleccione **Agregar**
- Paso 3. Escriba la dirección MAC Ethernet básica del AP para unirse al WLC, deje el **Nombre de la lista de atributos** en blanco y seleccione **Aplicar al dispositivo**



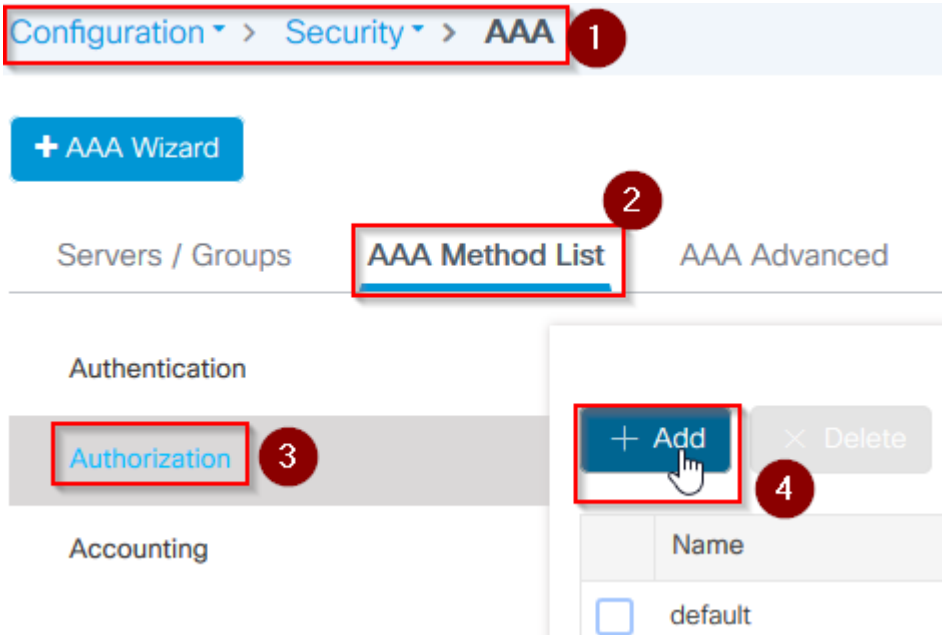
- Paso 4. Vaya a **Configuration > Security > AAA > AAA Method List > Autenticación**
- Paso 5. Seleccione **Add**, aparecerá el mensaje emergente **AAA Authentication**



- Paso 6. Escriba un nombre en Nombre de lista de métodos, seleccione 802.1x en el menú desplegable **Type*** y **local** para el **Tipo de grupo**, y finalmente seleccione **Apply to Device**.



- Paso 6b. En caso de que sus AP se unan directamente como modo Bridge y no se les haya asignado un sitio y una etiqueta de política antes, repita el paso 6 pero para el método predeterminado.
- Configure un método de autenticación dot1x aaa que apunte a local (CLI aaa authentication dot1x default local)
- Paso 7. Vaya a **Configuration > Security > AAA > AAA Method List > Autorización**
- Paso 8. Seleccione **Add**, aparecerá el mensaje emergente **AAA Authorization**



- Paso 9. Escriba un nombre en Nombre de la lista de métodos, seleccione descarga de credenciales en el menú desplegable **Tipo*** y **local** para el **Tipo de grupo**, y finalmente seleccione **Aplicar al dispositivo**

Quick Setup: AAA Authorization

Method List Name* 1

Type* 2

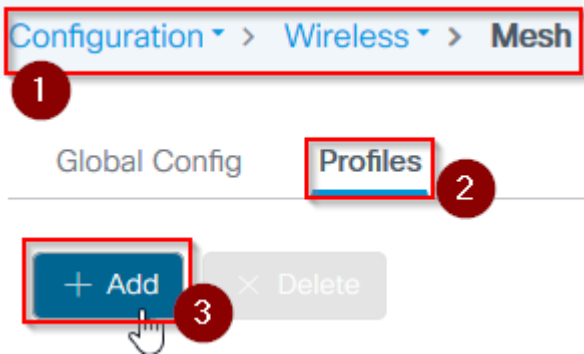
Group Type 3

Authenticated

Available Server Groups: radius, ldap, tacacs+, imarquez-Radius-grp

Assigned Server Groups: [Empty]

- Paso 9b. En caso de que su AP se una directamente en el modo Bridge (es decir, no se une primero en el modo local), repita el paso 9 para el método predeterminado de descarga de credenciales (CLI `aaa authorization credential-download default local`)
- Paso 10. Vaya a **Configuration > Wireless > Mesh > Profiles**.
- Paso 11. Seleccione **Add**, aparecerá la ventana emergente **Add Mesh Profile**.



- Paso 12. En la ficha **General**, defina un nombre y una descripción para el perfil de malla

A screenshot of the 'Add Mesh Profile' form. The title 'Add Mesh Profile' is at the top in a dark blue header. Below the title are two tabs: 'General' and 'Advanced'. The 'General' tab is selected and highlighted with a blue underline. The form contains two input fields. The first field is labeled 'Name*' and contains the text 'mesh-profile|'. The second field is labeled 'Description' and contains the text 'mesh-profile'.

- Paso 13. En la pestaña **Advanced**, seleccione **EAP** para el campo **Method**.
- Paso 14. Seleccione el perfil de **autorización** y **autenticación** definido en los pasos 6 y 9, y seleccione **Aplicar al dispositivo**

Add Mesh Profile

General

Advanced

1

Security

Method

EAP

2

Authentication Method

mesh-ap

3

Authorization Method

mesh-ap|

4

5 GHz Band Backhaul

Rate Types

2.4 GHz Band Backhaul

Rate Types

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

Bridge Group

Bridge Group Name

Enter Name

Strict Match

Cancel

- Paso 15. Navegue hasta **Configuración > Etiqueta y perfiles > Unión de AP > Perfil**
- Paso 16. Seleccione **Add**, aparecerá el **emergente AP Join Profile**, establezca un nombre y una descripción para el perfil AP Join

Configuration > Tags & Profiles > AP Join

1

+ Add

× Delete

2

AP Join Profile Name

Add AP Join Profile

General	Client	CAPWAP	AP	Management	Rogue AP	ICap
Name*	<input type="text" value="mes-ap-join"/>					
Description	<input type="text" value="mesh-ap-join"/>					
LED State	<input checked="" type="checkbox"/>					
LAG Mode	<input type="checkbox"/>					
NTP Server	<input type="text" value="0.0.0.0"/>					

- Paso 17. Navegue hasta la pestaña **AP** y seleccione el **perfil de malla** creado en el paso 12 del menú desplegable **Nombre del perfil de malla**
- Paso 18. Asegúrese de que **EAP-FAST** y **CAPWAP DTLS** estén configurados para los campos **EAP Type** y **AP Authorization Type** respectivamente
- Paso 19. Seleccione **Aplicar al dispositivo**

Add AP Join Profile

General Client CAPWAP **AP** Management Rogue AP ICap

General Hyperlocation BLE Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

Code

AP EAP Auth Configuration

EAP Type EAP-FAST ▾

AP Authorization Type CAPWAP DTLS ▾

Client Statistics Reporting Interval

5 GHz (sec) 90

2.4 GHz (sec) 90

Extended Module

Enable

Mesh

Profile Name mesh-p

Cancel

- Paso 20. Vaya a **Configuración > Etiqueta y perfiles > Etiquetas > Sitio**
- Paso 21. Seleccione **Agregar**, aparecerá el elemento emergente Etiqueta del sitio

Configuration ▾ > Tags & Profiles ▾ > **Tags**

Policy **Site** RF AP

+ Add Delete

- Paso 22. Escriba un nombre y una descripción para la etiqueta del sitio

Add Site Tag 1

Name* mesh-ap-site

Description mesh-ap-site

AP Join Profile mesh-ap-join-profile 2

- Paso 23. Seleccione el **AP Join Profile** creado en el paso 16 del menú desplegable **AP Join Profile**
- Paso 24. En la parte inferior de la ventana emergente Site Tag (Etiqueta del sitio), desactive la casilla de verificación **Enable Local Site** para activar el menú desplegable **Flex Profile**.
- Paso 35. En el menú desplegable **Flex Profile**, seleccione el **Flex Profile** que desea utilizar para el AP

Add Site Tag

Name* mesh-ap-site

Description mesh-ap-site

AP Join Profile mesh-ap-join-profile

Flex Profile imarquez-FlexLocal 2

Control Plane Name

Enable Local Site 1

Cancel

- Paso 36. Conecte el AP a la red y asegúrese de que el AP esté en el modo local.
- Paso 37. Para asegurarse de que el AP esté en el modo local, ejecute el comando **capwap ap mode local**.

El AP debe tener una manera de encontrar el controlador, ya sea broadcast L2, opción DHCP 43, resolución DNS o configuración manual.

- Paso 38. El AP se une al WLC, asegúrese de que aparezca en la lista AP, navegue hasta **Configuration > Wireless > Access Points > All Access Points**

▼ All Access Points

Number of AP(s): 2

AP Name	Total Slots	Admin Status	AP Model	Base Radio MAC	AP Mode
[REDACTED]	2	✓	[REDACTED]	[REDACTED]	Flex+Bridge
[REDACTED]	2	✓	[REDACTED]	[REDACTED]	Local

- Paso 39. Seleccione el AP, aparecerá la ventana emergente AP.
- Paso 40. Seleccione la **etiqueta del sitio** creada en el paso 22 en la ficha **General > Etiquetas > Sitio** dentro de la ventana emergente AP, seleccione **Actualizar y aplicar al dispositivo**

Edit AP

General

1

Interfaces

High Availability

Inventory

Mesh

Advanced

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status Registered

Fabric Status Disabled

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Tags

Policy

Site

RF

Version

Primary Software Version 16.12.1.13

Predownloaded Status N/A

Predownloaded Version N/A

Next Retry Time N/A

Boot Version 1.1.2.4

IOS Version 16.12.1.13

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address

Static IP (IPv4/IPv6)

Time Statistics

Up Time 4 da mins

Controller Association Latency 20 s

- Paso 41. El AP se reinicia y debe unirse nuevamente al WLC en el modo Flex + Bridge

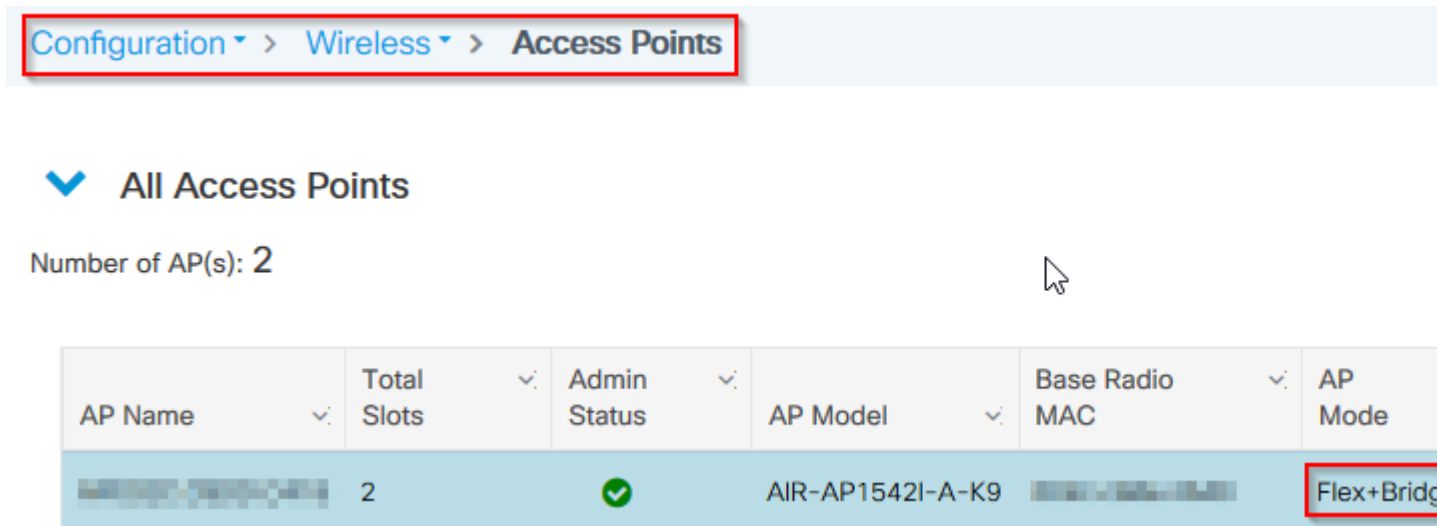
Observe que este método se une al AP primero en modo local (donde no realiza la autenticación dot1x) para aplicar la etiqueta de sitio con el perfil de malla y luego cambiar el AP al modo bridge.

Para unirse a un AP atascado en el modo Bridge (o Flex+Bridge), configure los métodos predeterminados (**aaa authentication dot1x default local** y **aaa authorization cred default local**).

El AP puede entonces autenticarse y puede asignar las etiquetas después.

Verificación

Asegúrese de que el modo AP se muestre como Flex + Bridge, como se muestra en esta imagen.



Ejecute estos comandos desde WLC 9800 CLI y busque el atributo **AP Mode**. Debe aparecer como **Flex+Bridge (Flex+Bridge)**

```
aaa authorization credential-download mesh-ap local
aaa authentication dot1x mesh-ap local
wireless profile mesh default-mesh-profile
  description "default mesh profile"
wireless tag site meshsite
  ap-profile meshapjoin
  no local-site
ap profile meshapjoin
  hyperlocation ble-beacon 0
  hyperlocation ble-beacon 1
  hyperlocation ble-beacon 2
  hyperlocation ble-beacon 3
  hyperlocation ble-beacon 4
mesh-profile mesh-profile
```

Troubleshoot

Asegúrese de que los comandos **aaa authentication dot1x default local** y **aaa authorization cred default local** estén presentes. Son necesarios si su AP no fue pre-unido en el modo local.

El panel principal del 9800 tiene un widget que muestra los AP que no pueden unirse. Haga clic en él para obtener una lista de AP que no pueden unirse :

General **Join Statistics**[Clear](#) [ClearAll](#)

Number of AP(s): 2

Status *is equal to* NOT JOINED x

	Status	Base Radio MAC	Ethernet MAC	AP Name
<input type="checkbox"/>		10b3.c622.5d80	2cf8.9b21.18b0	AP2CF8.9B21.18B0
<input type="checkbox"/>		7070.8bb4.9200	2c33.110e.6b66	AP2C33.110E.6B66

1 10 items per page

Haga clic en el AP específico para ver la razón por la que no está unido. En este caso, vemos un problema de autenticación (autenticación de AP pendiente) porque la etiqueta del sitio no fue asignada al AP.

Por lo tanto, el 9800 no eligió el método de autenticación/autorización designado para autenticar el AP :

Join Statistics

General

Statistics

Control DTLS Statistics

DTLS Session request received	179
Established DTLS session	179
Unsuccessful DTLS session	0
Reason for last unsuccessful DTLS session	DTLS Handshake Success
Time at last successful DTLS session	Thu, 19 Dec 2019 13:03:19 GMT
Time at last unsuccessful DTLS session	NA

Join phase statistics

Join requests received	179
Successful join responses sent	173
Unsuccessful join request processing	0
Reason for last unsuccessful join attempt	Ap auth pending
Time at last successful join attempt	Thu, 19 Dec 2019 12:36:10 GMT
Time at last unsuccessful join attempt	NA

Configuration phase statistics

Configuration requests received
Successful configuration responses sent
Unsuccessful configuration request processing
Reason for last unsuccessful configuration attempt
Time at last successful configuration attempt
Time at last unsuccessful configuration attempt

Data DTLS Statistics

DTLS Session request received
Established DTLS session
Unsuccessful DTLS session
Reason for last unsuccessful DTLS session
Time at last successful DTLS session
Time at last unsuccessful DTLS session

Para una resolución de problemas más avanzada, vaya a la página **Troubleshooting > Radioactive Trace** en la interfaz de usuario web.

Si ingresa la dirección MAC del AP, puede generar inmediatamente un archivo para obtener los registros siempre activos (en el nivel de aviso) del AP que intenta unirse.

Haga clic en **Start** para habilitar la depuración avanzada para esa dirección MAC. La próxima vez que se generen los registros, se mostrarán los registros de nivel de depuración para la unión de AP.



Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Troubleshooting

Troubleshooting > Radioactive Trace

[← Back to Troubleshooting Menu](#)

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file
<input type="checkbox"/>	2c33.110e.6b66	debugTrace_2c33.110e.6b66.txt ↓

⏪ < 1 > ⏩ 10 items per page

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).