

# Configurar a malha nos controladores de LAN sem fio Catalyst 9800

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Estudo de caso 1: Modo em bridge](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Estudo de caso 2: Flex + Bridge](#)

[Configurar](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve um exemplo de configuração básica sobre como unir um Ponto de Acesso (AP) de malha ao Catalyst 9800 Wireless LAN Controller (WLC)

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração Catalyst Wireless 9800
- Configuração de LAPs
- Controle e fornecimento de access points sem fio (CAPWAP)
- Configuração de um servidor DHCP externo
- Configuração de switches Cisco

### Componentes Utilizados

Este exemplo usa o ponto de acesso lightweight (1572AP e 1542) que pode ser configurado como um Root AP (RAP) ou Mesh AP (MAP) para se unir ao Catalyst 9800 WLC. O procedimento é idêntico para 1542 ou 1562 pontos de acesso. O RAP é conectado ao Catalyst 9800 WLC através de um switch Cisco Catalyst.

As informações neste documento são baseadas nestas versões de software e hardware:

- C9800-CL v16.12.1
- Switch de Camada 2 da Cisco
- Pontos de acesso Cisco Aironet série 1572 Lightweight Outdoor para a seção Bridge
- Cisco Aironet 1542 para a seção Flex+Bridge

**The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.**

## **Configurar**

### **Estudo de caso 1: Modo em bridge**

#### **Diagrama de Rede**

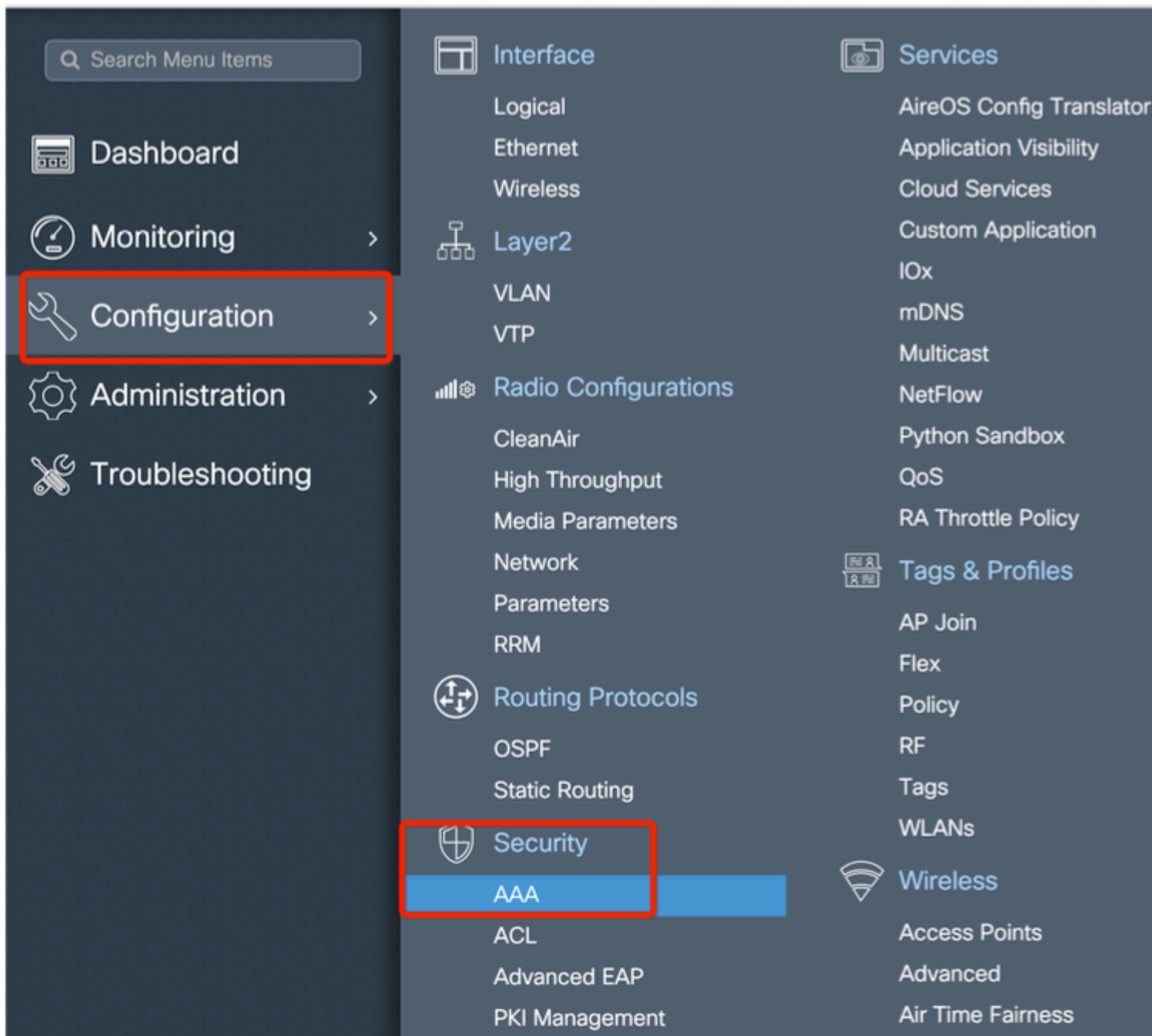
#### **Configurações**

Um AP de malha precisa ser autenticado para que ele se una ao controlador 9800. Este estudo de caso considera que você se une ao AP no modo local primeiro para o WLC e depois o converte para o modo de malha Bridge (também conhecido como).

Para evitar a atribuição de perfis de junção de AP, use este exemplo, mas configure o método default aaa authorization credential-download para que qualquer AP de malha tenha permissão para se unir à controladora.

**Etapa 1:** Configure os endereços MAC RAP/MAP em Autenticação de dispositivo.

Vá para **Configuration > AAA > AAA Advanced > Device Authentication** .

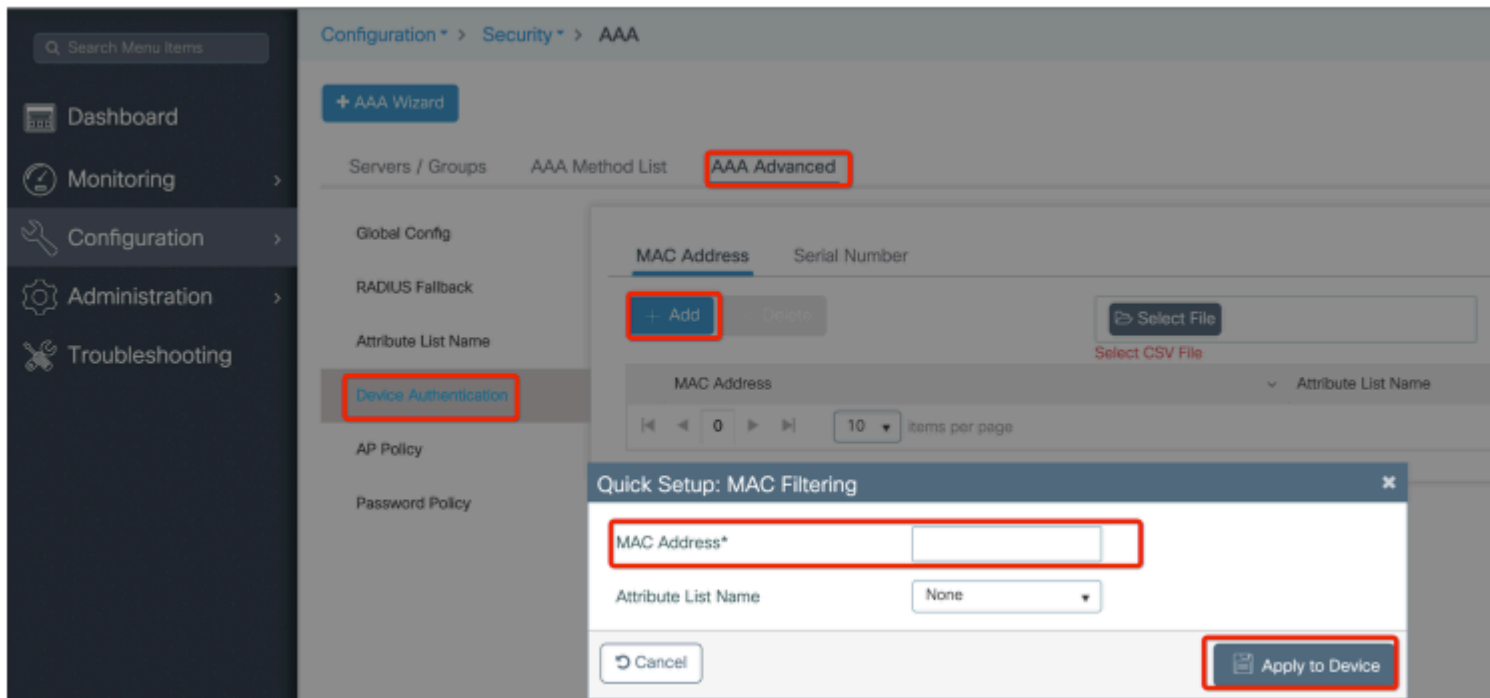


Adicione o endereço MAC Ethernet base dos pontos de acesso da malha, adicione-o sem caracteres especiais, sem '.' ou ':'

---

**Importante:** a partir da versão 17.3.1, iSe algum delimitador de endereço MAC, como '.', ':' ou '-', for adicionado, o AP não poderá se unir. No momento, há 2 aprimoramentos abertos para isso: [ID de bug Cisco CSCyv43870](#) e ID de bug Cisco [CSCvr07920](#). No futuro, o 9800 aceitará todos os formatos de endereço mac.

---



**Etapa 2:** Configurar a lista de métodos de autenticação e autorização.

Vá para **Configuration > Security > AAA > AAA Method list > Authentication** e crie a lista de métodos de autenticação e a lista de métodos de autorização.

+ 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

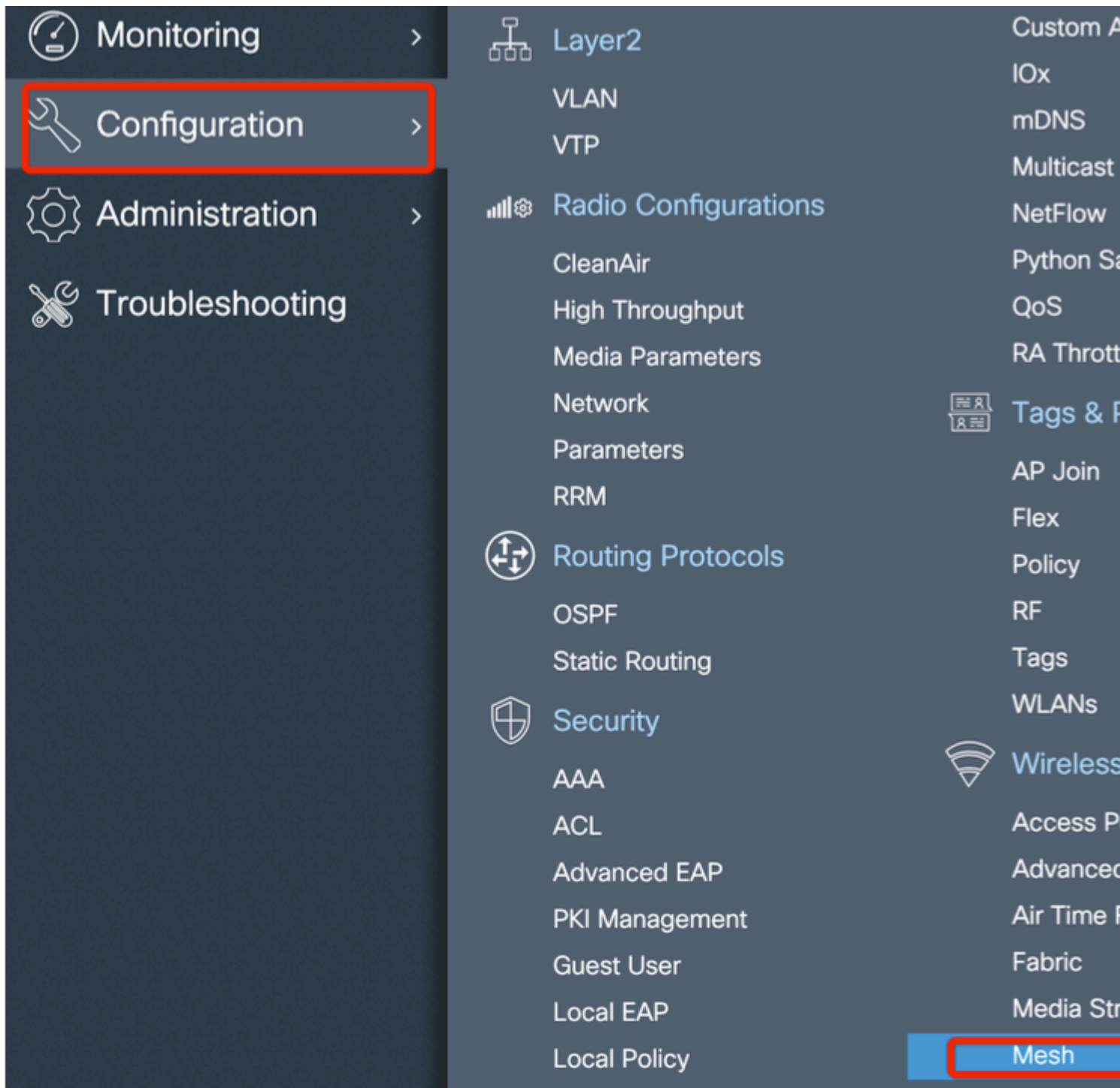
>

<

Cancel

**Etapa 3:** Configure os parâmetros globais de malha.

Vá para **Configuration > Mesh > Global** parameters. Inicialmente, podemos manter esses valores como padrão.



**Etapa 4:** Crie um novo Perfil de Malha em **Configuração > Malha > Perfil > +Adicionar**

Global Config **Profiles**

**+ Add** Delete

Number of Profiles : **1**

### Add Mesh Profile

**General** Advanced

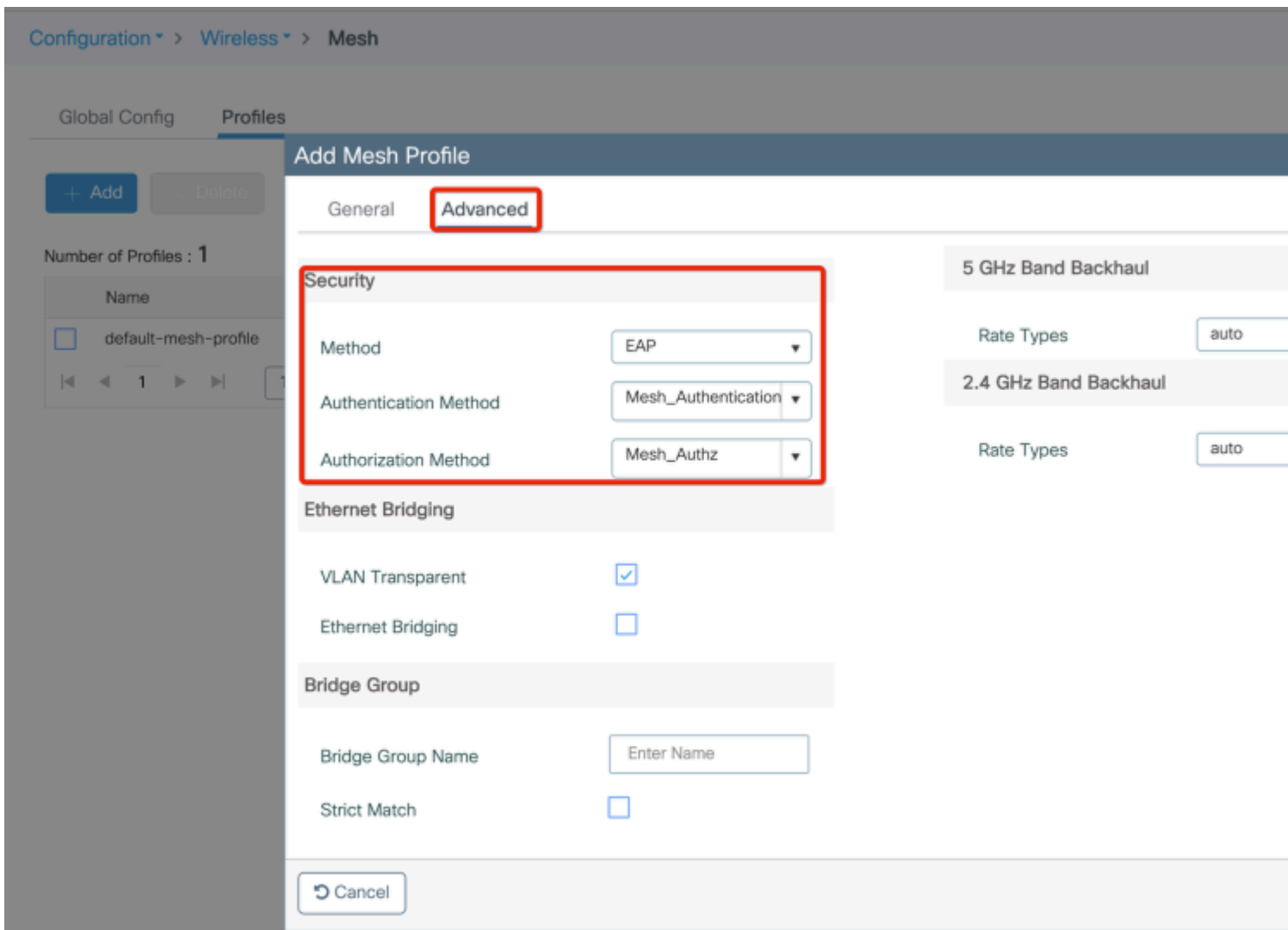
Name*	Mesh_Profile	Backhaul amsdu	<input checked="" type="checkbox"/>
Description	Enter Description	Backhaul Client Access	<input type="checkbox"/>
Range (Root AP to Mesh AP)	12000	Battery State for an AP	<input checked="" type="checkbox"/>
Multicast Mode	In-Out	Full sector DFS status	<input checked=""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

Cancel

Clique no perfil de malha criado para editar as configurações Geral e Avançado do perfil de malha.


No diagrama como mostrado, precisamos mapear o perfil de autenticação e autorização criado antes para o perfil Mesh







**Etapa 5:** Criar um novo perfil de junção AP. Vá para **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 o perfil de malha configurado anteriormente e configure a autenticação EAP AP 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)

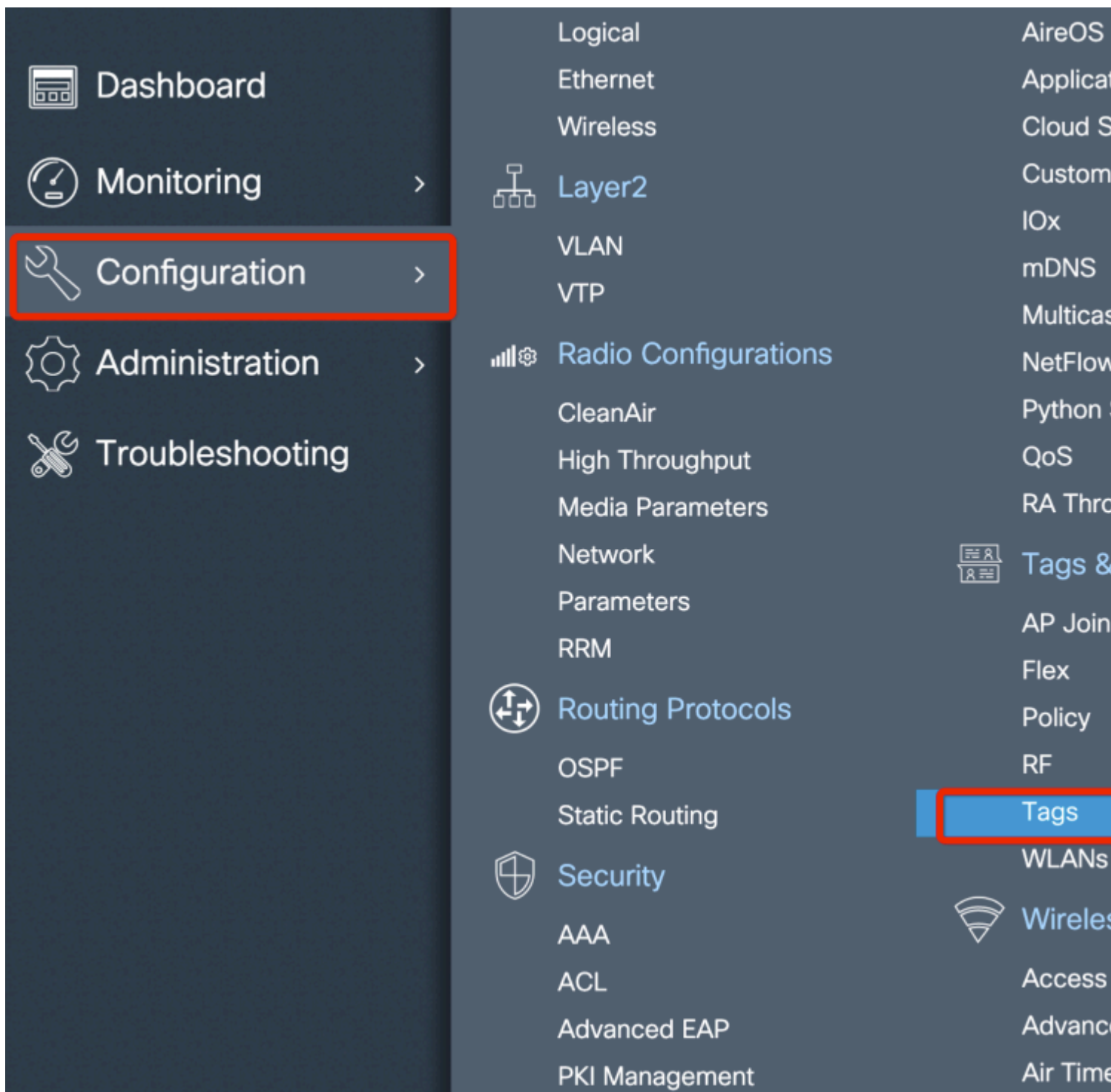
**Extended Module**

Enable

**Mesh**

Profile Name

**Etapa 6:** Crie uma tag de localização de malha como mostrado.



Configure (Configurar) Clique na TAG de localização da malha criada na Etapa 6 para configurá-la.

Chegou até a guia Site e aplique o Perfil de junção de AP do Mesh configurado anteriormente a ele:

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

**Passo 7.** Converta o AP para o 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	<span style="color: green;">✔</span>	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

via CLI, você pode usar este comando no AP:

capwap ap mode bridge

O AP é reinicializado e volta como modo de Bridge.

**Etapa 8.** Agora você pode definir a função do AP: AP raiz ou AP de malha.

O AP raiz é aquele com uma conexão com fio à WLC, enquanto o AP de malha se une à WLC através de seu rádio que tenta se conectar a um AP raiz.

Um AP de malha pode se unir à WLC através de sua interface com fio depois que ele não conseguir encontrar um AP raiz através de seu rádio, para fins de provisão.

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

Cancel

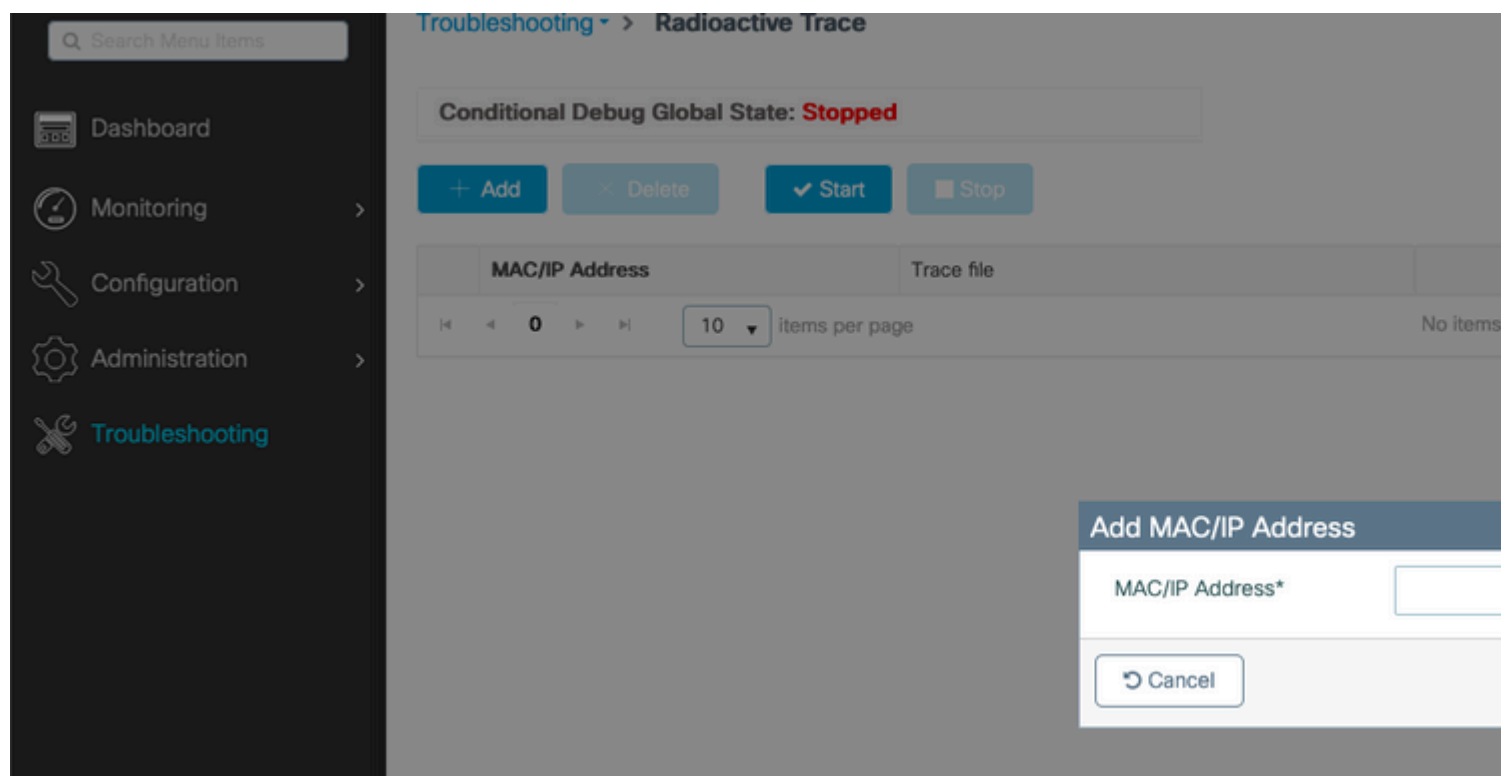
## Verificar

```
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

Na página **Troubleshooting** > **Radioactive Trace** da UI da Web, clique em **adicionar** e insira o endereço MAC do AP.



The screenshot shows the 'Radioactive Trace' configuration page in the Meraki web interface. The 'Conditional Debug Global State' is 'Stopped'. There are buttons for '+ Add', 'Delete', 'Start', and 'Stop'. Below these is a table with columns 'MAC/IP Address' and 'Trace file'. The table shows 0 items per page. A modal dialog 'Add MAC/IP Address' is open, with a text input field for 'MAC/IP Address\*' and a 'Cancel' button.

Clique em **Start** e aguarde até que o AP tente se unir ao controlador novamente.

Depois de concluído, clique em **Gerar** e escolha um período de tempo para coletar os logs (últimos 10 ou 30 minutos, por exemplo).

Clique no nome do arquivo de rastreamento para baixá-lo do seu navegador.

Aqui está um exemplo de AP não ingressado devido ao nome incorreto do método de autorização aaa definido :



```

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

```

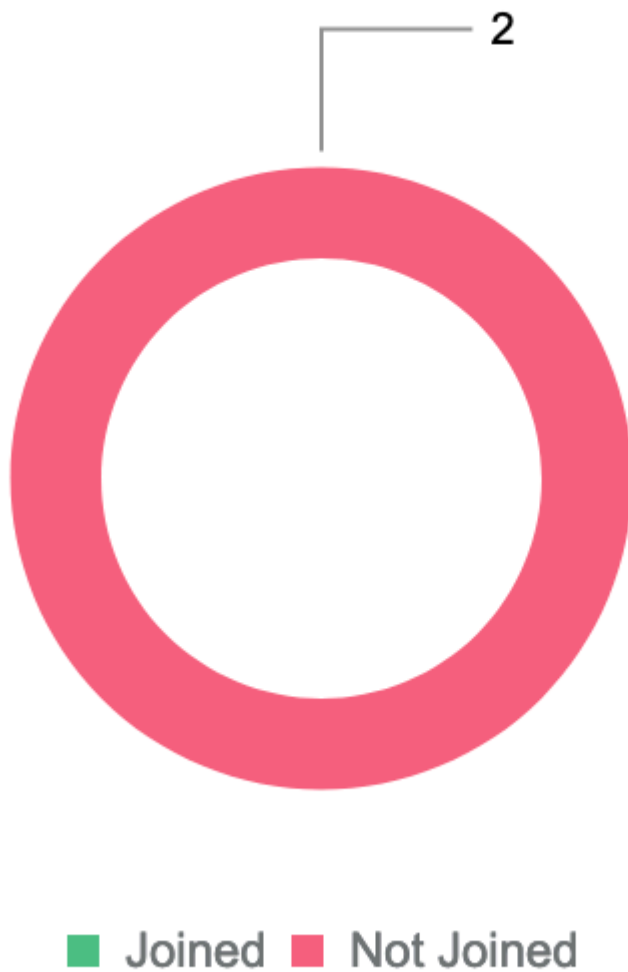
O mesmo pode ser visto mais facilmente no painel da interface do usuário da Web quando se clica em APs não ingressados. "Autenticação de AP pendente" é a dica que aponta para a autenticação do próprio AP:

The screenshot displays two panels from a network management interface:

- AP Statistics Panel:**
  - Navigation: Monitoring > Wireless > AP Statistics
  - Tabs: General, **Join Statistics**
  - Buttons: Clear, ClearAll
  - Number of AP(s): 2
  - Status filter: "Is equal to" NOT JOINED
  - Table:
| AP Name | AP Mod |
| --- | --- |
| AP2CF8-9B5F-7D70 | C9120A |
| NA |  |
  - Pagination: 1 of 10 items per page
- Join Statistics Panel:**
  - Tabs: General, **Statistics**
  - Table:
| Event | Count | Details |
| --- | --- | --- |
| 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
    - Successful join responses sent: 0
    - Unsuccessful join request processing: 0
    - Reason for last unsuccessful join attempt: Ap auth pending
    - Time at last successful join attempt: NA
    - Time at last unsuccessful join attempt: NA

---

## Access Point Join Summary



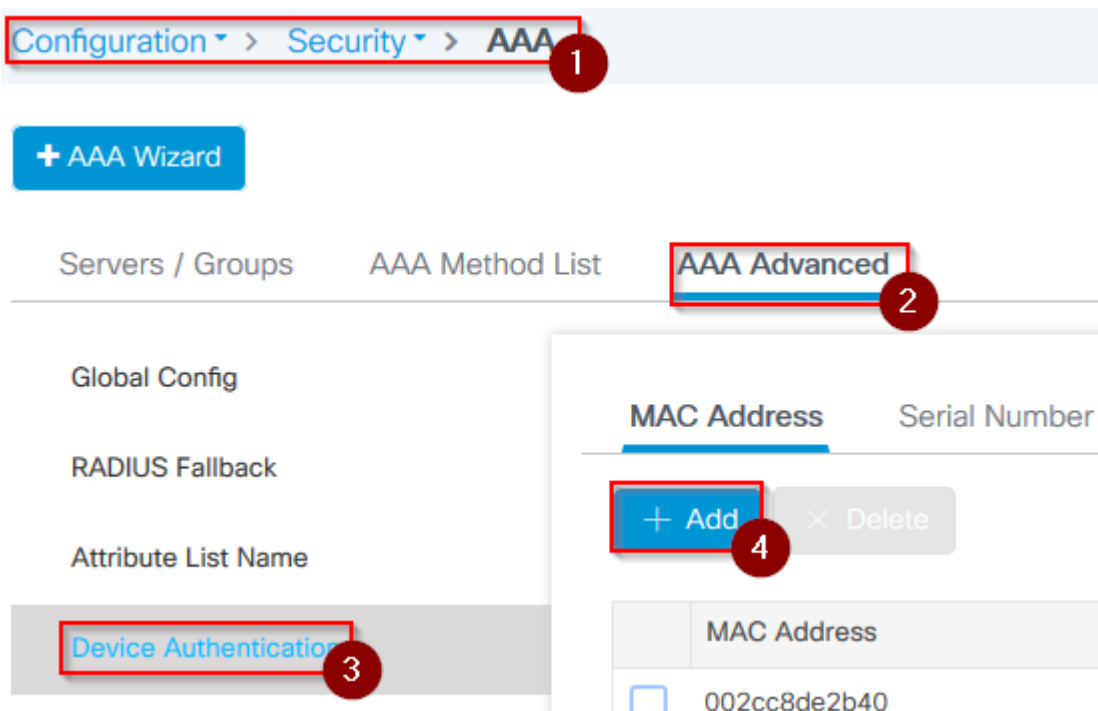
---

### Estudo de caso 2: Flex + Bridge

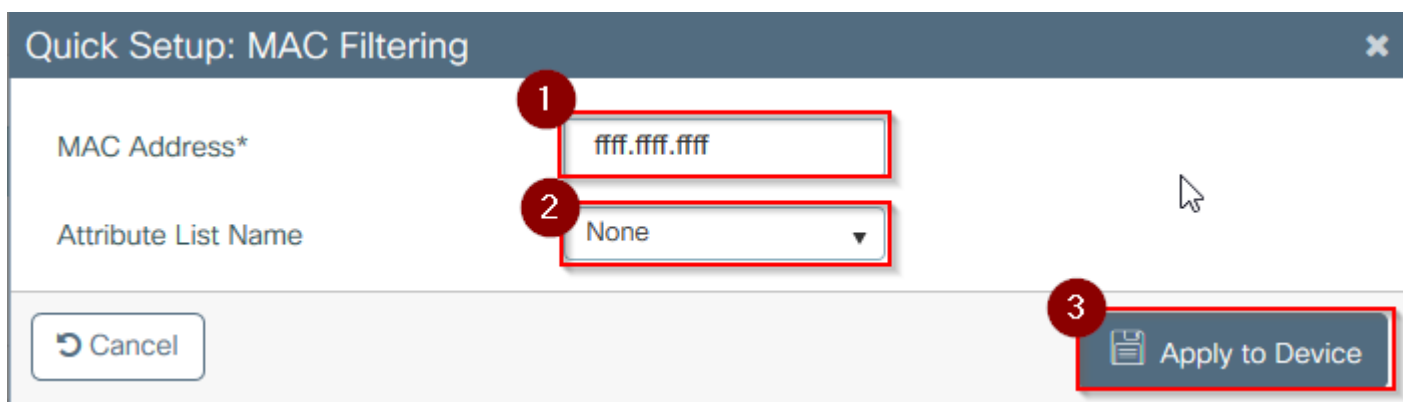
Esta seção destaca o processo de união de um AP 1542 no modo Flex+bridge com autenticação EAP feita localmente no WLC.

#### Configurar

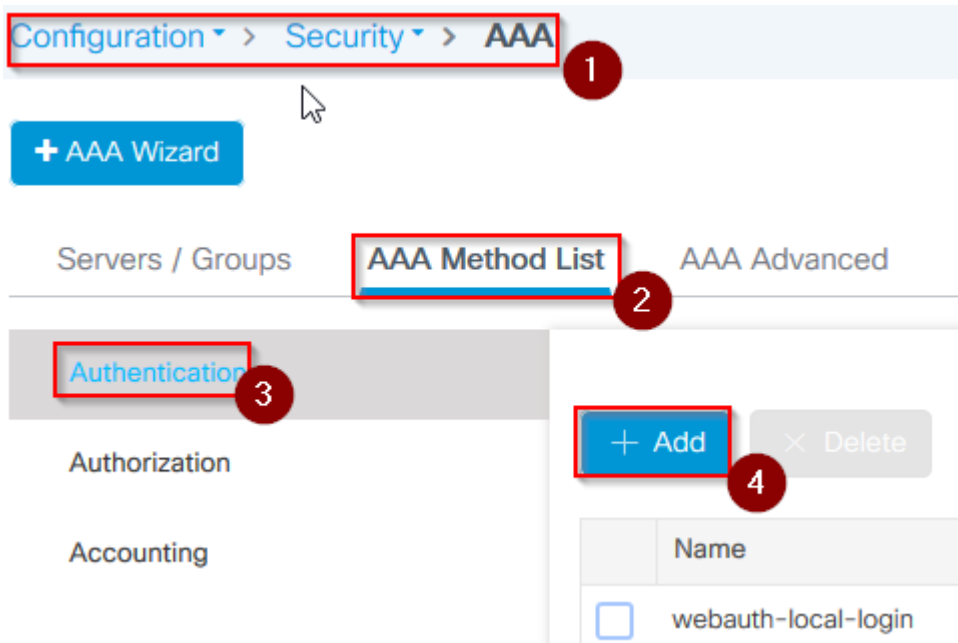
- Etapa 1. Navegue até **Configuration > Security > AAA > AAA Advanced > Device Authentication**



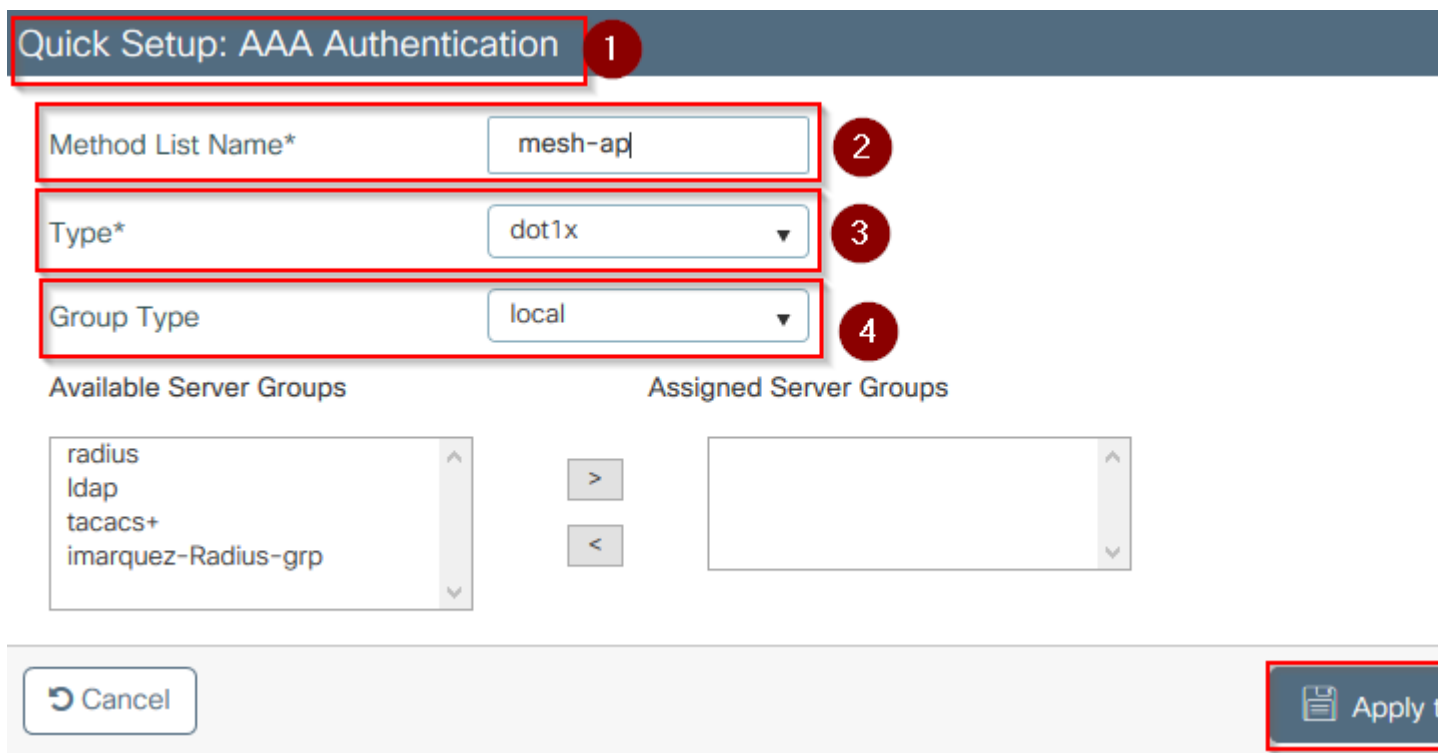
- Etapa 2. Selecione **Device Authentication** e **Add**
- Etapa 3. Digite o endereço MAC Ethernet base do AP para ingressar na WLC, deixe o **nome da lista de atributos** em branco e selecione **Apply to Device**



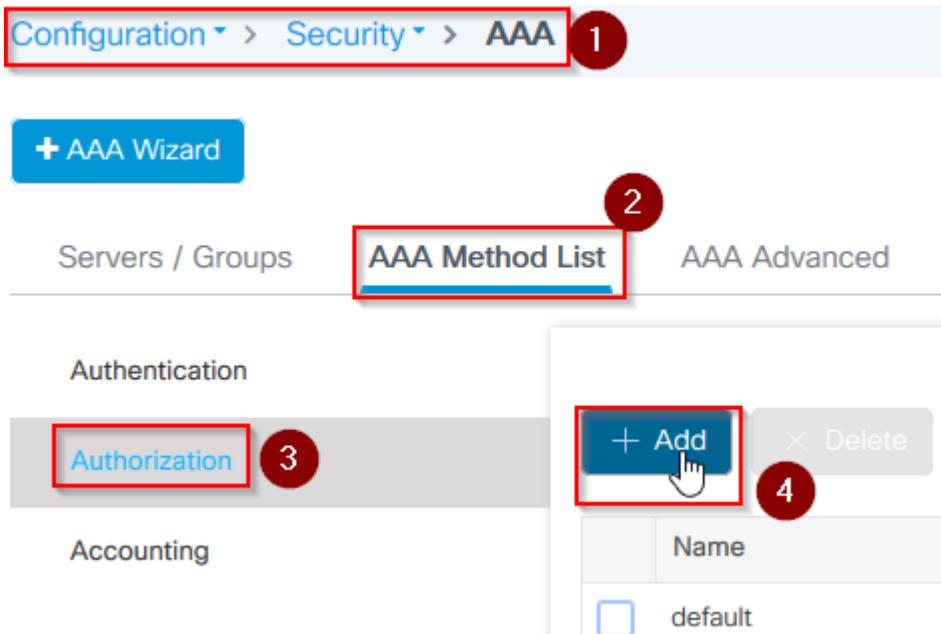
- Etapa 4. Navegue até **Configuration > Security > AAA > AAA Method List > Autenticação**
- Etapa 5. Selecione **Add**, o pop-up **AAA Authentication** será exibido



- Etapa 6. Digite um nome no Nome da lista de métodos, selecione 802.1x na lista suspensa **Tipo\*** e **local** para o **Tipo de grupo**, finalmente selecione **Aplicar ao dispositivo**



- Etapa 6b. Caso seus APs entrem diretamente como modo de Bridge e não tenham recebido uma marca de site e política antes, repita a etapa 6, mas para o método padrão.
- Configure um método de autenticação dot1x aaa que aponte para local (CLI aaa authentication dot1x default local)
- Passo 7. Navegue até **Configuration > Security > AAA > AAA Method List > Autorização**
- Etapa 8. Selecione **Add**, o pop-up **AAA Authorization** será exibido



- Etapa 9. Digite um nome no Nome da lista de métodos, selecione o download credencial na lista suspensa **Tipo\*** e **local** para o **Tipo de grupo**, finalmente selecione **Aplicar ao dispositivo**

### Quick Setup: AAA Authorization

Method List Name\*  1

Type\*  2

Group Type  3

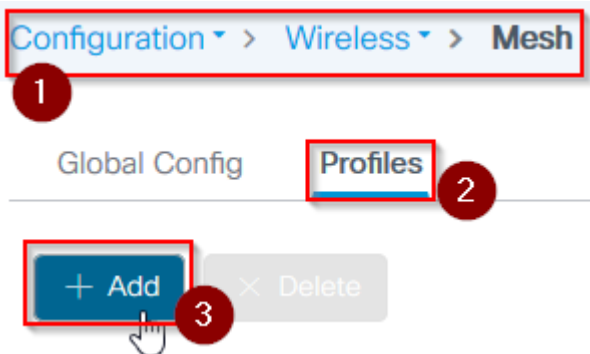
Authenticated

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

Assigned Server Groups: [Empty]

Buttons: Cancel, Apply

- Etapa 9b. Caso seu AP se una diretamente no modo Bridge (isto é, ele não se une primeiro no modo local), repita a etapa 9 para o método padrão de download de credencial (CLI aaa authorization credential-download default local)
- Etapa 10. Navegue até **Configuration > Wireless > Mesh > Profiles**
- Etapa 11. Selecione **Add**, o pop-up **Add Mesh Profile** será exibido



- Etapa 12. Na guia **Geral**, defina um nome e uma descrição para o perfil Mesh

A screenshot of the 'Add Mesh Profile' configuration page. The page has a dark blue header with the text 'Add Mesh Profile'. Below the header, there 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'.

- Etapa 13. Na guia **Advanced**, selecione **EAP** para o campo **Method**
- Etapa 14. Selecione o **perfil de Autorização** e **Autenticação** definido nas etapas 6 e 9 e selecione **Aplicar ao 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

- Etapa 15. Navegue até **Configuration > Tag & Profiles > AP Join > Profile**
- Etapa 16. Selecione **Add**, o pop-up **AP Join Profile** será exibido, defina um nome e uma descrição para o perfil de 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"/>					

- Etapa 17. Navegue até a guia **AP** e selecione o **Perfil da malha** criado na etapa 12 no menu suspenso **Nome do perfil da malha**
- Etapa 18. Certifique-se de que **EAP-FAST** e **CAPWAP DTLS** estejam definidos para os campos **Tipo de EAP** e **Tipo de autorização de AP**, respectivamente
- Etapa 19. Selecione **Aplicar ao 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

- Etapa 20. Navegue até **Configuração > Tag & Profiles > Tags > Site**
- Etapa 21. Selecione **Add**, a janela pop-up Site Tag será exibida

Configuration > Tags & Profiles > Tags

Policy **Site** RF AP

+ Add Delete

- Etapa 22. Digite um nome e uma descrição para a Marca de Site

**Add Site Tag** 1

Name\* mesh-ap-site

Description mesh-ap-site

AP Join Profile mesh-ap-join-profile 2

- Etapa 23. Selecione o **Perfil de junção AP** criado na etapa 16 no menu suspenso **Perfil de junção AP**
- Etapa 24. Na parte inferior do pop-up Marca do site, desmarque a caixa de seleção **Habilitar site local** para habilitar o menu suspenso **Perfil do Flex**.
- Etapa 35. No menu suspenso **Flex Profile**, selecione o **Flex Profile** que deseja usar para o 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

- Etapa 36. Conecte o AP à rede e verifique se o AP está no modo local.
- Etapa 37. Para garantir que o AP esteja no modo local, emita o comando **capwap ap mode local**.  
O AP deve ter uma maneira de encontrar a controladora, broadcast L2, DHCP Opção 43, resolução DNS ou configuração manual.
- Etapa 38. O AP se une à WLC, verifique se está listado na lista de APs, navegue para **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
	2	✓			Flex+Bridge
	2	✓			Local

- Etapa 39. Seleccione o AP, o pop-up **AP** será exibido.
- Etapa 40. Seleccione a guia **Site Tag** criada na Etapa 22 em **Geral > Tags > Site** no pop-up AP, seleccione **Atualizar e aplicar ao 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

- Etapa 41. O AP é reinicializado e deve se unir de volta ao WLC no modo Flex + Bridge

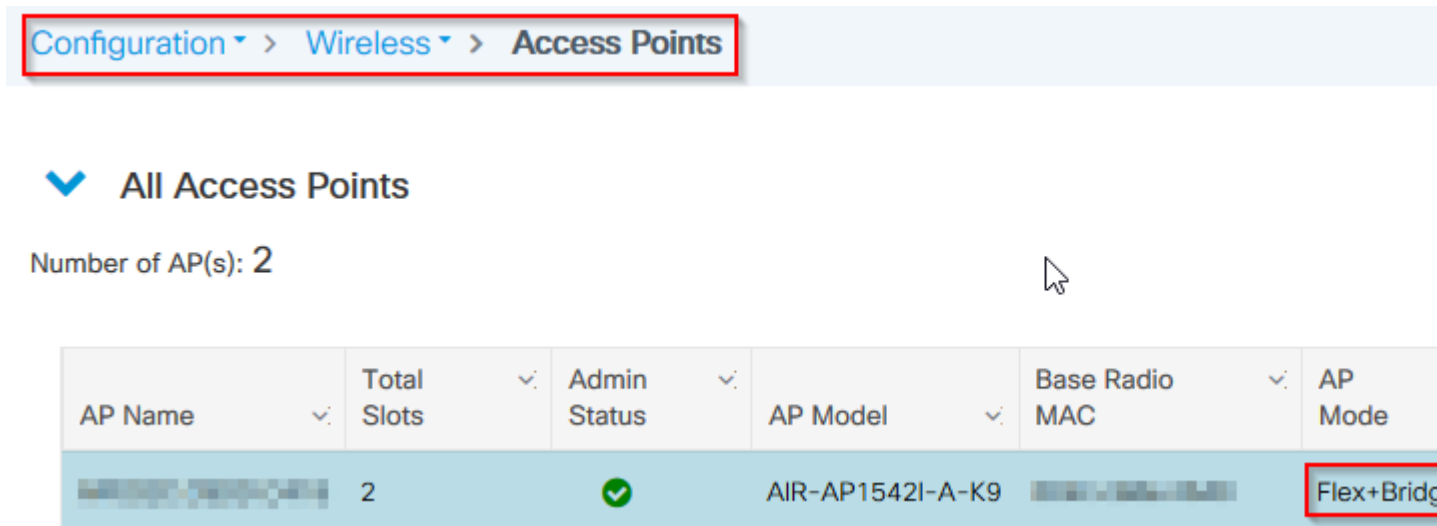
Observe que esse método junta o AP primeiro no modo local (onde não faz a autenticação dot1x) para aplicar a marca de site com o perfil de malha e, em seguida, comuta o AP para o modo de ponte.

Para unir um AP que está preso no modo Bridge (ou Flex+Bridge), configure os métodos padrão (**aaa authentication dot1x default local** e **aaa authorization cred default local**).

O AP é então capaz de autenticar e você pode atribuir as tags depois.

## Verificar

Certifique-se de que o modo AP seja exibido como Flex + Bridge, conforme mostrado nesta imagem.



Execute esses comandos da CLI do WLC 9800 e procure o atributo **AP Mode**. Ele deve estar listado como **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

Certifique-se de que os comandos **aaa authentication dot1x default local** e **aaa authorization cred default local** estejam presentes. Eles são necessários se o seu AP não tiver sido pré-ingressado no modo Local.

O painel principal do 9800 tem um widget que exibe os APs que não podem se unir. Clique nele para obter uma lista de APs que falham ao ingressar:

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

Clique no AP específico para ver o motivo pelo qual ele não ingressou. Nesse caso, vemos um problema de autenticação (autenticação de AP pendente) porque a marca do site não foi atribuída ao AP.

Portanto, o 9800 não escolheu o método de autenticação/autorização nomeado para autenticar o 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 Troubleshooting mais avançado, vá para a página **Troubleshooting > Radioactive Trace** na interface de usuário da Web.

Se você inserir o endereço MAC do AP, poderá gerar imediatamente um arquivo para obter os logs sempre ativos (no nível de aviso) do AP que tenta juntar-se.

Clique em **Iniciar** para habilitar a depuração avançada para esse endereço mac. Na próxima vez que os logs forem gerados, gere os logs, os logs de depuração para a junção do AP serão mostrados.



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 <a href="#">↓</a>

⏪ < 1 > ⏩ 10 items per page



Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.