

# Configure o link de malha ponto a ponto com ponte Ethernet no controlador sem fio incorporado com pontos de acesso C9124

## Contents

---

### [Introdução](#)

### [Pré-requisitos](#)

#### [Requisitos](#)

#### [Componentes Utilizados](#)

### [Informações de Apoio](#)

#### [Bridging Ethernet](#)

#### [Controlador sem fio integrado no ponto de acesso Catalyst](#)

### [Configurar](#)

#### [Diagrama de Rede](#)

#### [Configurações](#)

##### [Configurações do switch](#)

##### [Configuração EWC e RAP](#)

##### [Configurar MAP](#)

#### [Verificar](#)

### [Troubleshooting](#)

#### [Comandos úteis](#)

#### [Exemplo 1: RAP recebe adjacência de MAP e obtém autenticação](#)

#### [Exemplo 2: endereço MAC do MAP não adicionado ao WLC ou adicionado incorretamente](#)

#### [Exemplo 3: RAP perde MAP](#)

#### [Dicas, truques e recomendações](#)

### [Referências](#)

---

## Introdução

Este documento descreve como configurar o Enlace de Malha P2P com Bridging Ethernet em Controlador Sem Fio Embutido (eWC) com Pontos de Acesso C9124.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controladores de LAN sem fio (WLC) 9800 da Cisco.
- Pontos de acesso (APs) Cisco Catalyst.
- Controlador sem fio integrado nos pontos de acesso Catalyst.

- Tecnologia de malha.

## Componentes Utilizados

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

- EWC IOS® XE 17.12.2
- 2x APs C9124.
- 2x injetores de energia AIR-PWRINJ-60RGD1.
- 2x switches;
- 2x notebooks;
- 1 AP C9115.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

### Bridging Ethernet

A solução de rede em malha, que faz parte da solução de rede sem fio unificada da Cisco, permite que dois ou mais pontos de acesso em malha da Cisco (doravante denominados pontos de acesso em malha) se comuniquem entre si em um ou mais saltos sem fio para ingressar em várias LANs ou estender a cobertura WiFi.

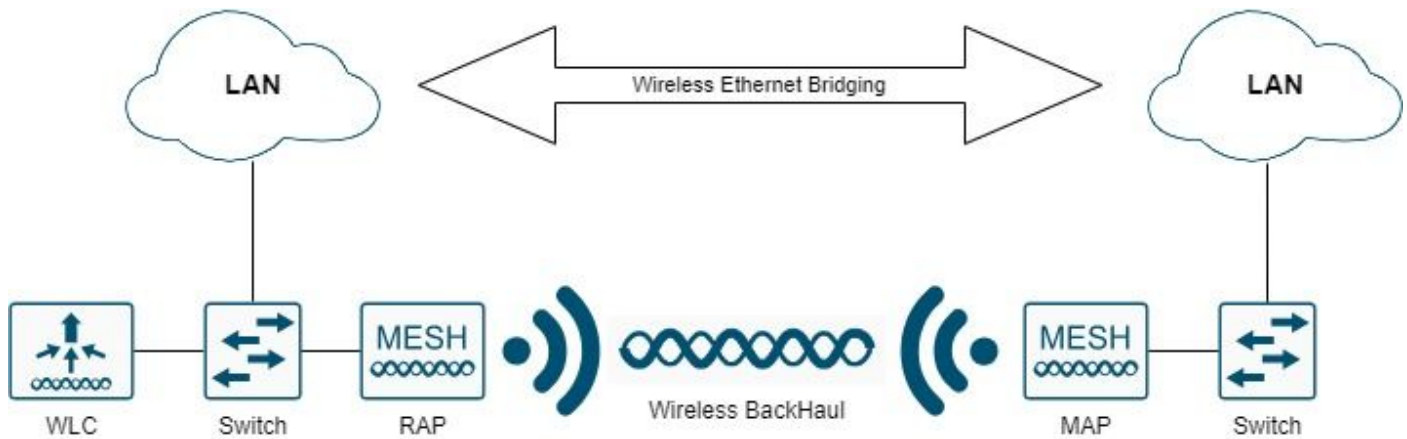
Os pontos de acesso em malha da Cisco são configurados, monitorados e operados de e através de qualquer controlador de LAN sem fio da Cisco que é implantado na solução de rede em malha.

As implantações de soluções de rede em malha suportadas são de um dos três tipos gerais:

- Implantação ponto a ponto
- Implantação ponto a multiponto
- Implantação de malha

Este documento concentra-se em como configurar a distribuição de malha ponto-a-ponto e o bridging Ethernet no mesmo ponto.

Na distribuição de malha ponto-a-ponto, os pontos de acesso de malha fornecem acesso sem fio e backhaul para clientes sem fio e podem simultaneamente suportar bridging entre uma LAN e uma terminação para um dispositivo Ethernet remoto ou outra LAN Ethernet.



Bridging Ethernet Sem Fio

Consulte [Guia de Implantação em Malha para Controladores Wireless Cisco Catalyst 9800 Series](#) para obter informações detalhadas sobre cada um desses tipos de implantação.

O AP de malha externa Cisco Catalyst 9124 Series é um dispositivo sem fio projetado para acesso de cliente sem fio e ponte ponto a ponto, ponte ponto a multiponto e conectividade sem fio de malha ponto a multiponto.

O ponto de acesso externo é uma unidade autônoma que pode ser montada em uma parede ou em um forro, em um poste no telhado ou em um poste de iluminação pública.

Você pode operar o C9124 em uma destas funções de malha:

- Ponto de acesso (RAP) no último piso
- Ponto de Acesso em Malha (MAP)

Os RAPs têm uma conexão com fio a um controlador de LAN sem fio da Cisco. Eles usam a interface sem fio de backhaul para se comunicar com MAPs próximos. Os RAPs são o nó pai de qualquer bridging ou rede em malha e conectam uma bridge ou rede em malha à rede com fio, portanto pode haver apenas um RAP para qualquer segmento de rede em bridge ou em malha.

Os MAPs não têm conexão com fio com um controlador de LAN sem fio da Cisco. Eles podem ser completamente sem fio e suportar clientes que se comunicam com outros MAPs ou RAPs, ou podem ser usados para se conectar a dispositivos periféricos ou a uma rede com fio.

## Controlador sem fio integrado no ponto de acesso Catalyst

O Cisco Embedded Wireless Controller (EWC) em pontos de acesso Catalyst é um controlador baseado em software integrado aos pontos de acesso Cisco Catalyst 9100.

Em uma rede Cisco EWC, um ponto de acesso (AP) que executa a função de controlador sem fio é designado como o AP ativo.

Os outros pontos de acesso, que são gerenciados por esse AP ativo, são chamados de APs subordinados.

O conselho de empresa europeu ativo tem duas funções:

- Funciona e opera como um Wireless LAN Controller (WLC) para gerenciar e controlar os APs subordinados. Os APs subordinados operam como pontos de acesso lightweight para atender clientes.
- Ele opera como um ponto de acesso para atender clientes.

Para ter uma visão geral do produto sobre EWC em APs, visite a [Folha de Dados do Cisco Embedded Wireless Controller em Pontos de Acesso Catalyst](#).

Para saber como implantar o EWC na sua rede, visite o [White Paper Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\)](#).

Este documento se concentra no C9124 como EWC e supõe que já existe um AP 9124 no modo EWC.

## Configurar

### Diagrama de Rede


Todos os dispositivos nessa rede estão localizados dentro da sub-rede 192.168.100.0/24, exceto os laptops que estão na VLAN 101 com a sub-rede 192.168.101.0/25.

O AP EWC (WLC) tem sua interface de gerenciamento não marcada e a VLAN nativa nas portas de switch está definida como VLAN 100.

AP9124\_RAP tem a função de um eWLC e de um ponto de acesso raiz (RAP), enquanto AP9124\_MAP assume a função de ponto de acesso em malha (MAP).

Neste laboratório, um AP C9115 também é colocado atrás do MAP para mostrar que podemos ter APs para se unir a uma WLC em um link de malha.

Esta tabela contém os endereços IP de todos os dispositivos na rede:

 Observação: marcar a interface de gerenciamento pode causar problemas com o AP que ingressa no processo interno da WLC. Se você decidir marcar a interface de gerenciamento, certifique-se de que a parte da infraestrutura com fio esteja configurada de acordo.

Dispositivo	IP Address
Gateway padrão	Estático na VLAN 100: 192.168.100.1
Notebook1	DHCP na VLAN 101
Notebook2	DHCP na VLAN 101
Switch 1 (servidor DHCP)	VLAN 100 SVI: estática na VLAN 100: 192.168.100.1 (servidor DHCP)
Switch 1 (servidor DHCP)	VLAN 101 SVI: estática na VLAN 101: 192.168.101.1 (servidor DHCP)

Switch2	SVI da VLAN 100: DHCP na VLAN 100
Switch2	SVI da VLAN 101: DHCP na VLAN 101
9124CEE	Estático na VLAN 100: 192.168.100.40
AP9124_RAP	DHCP na VLAN 100
AP9124_MAP	DHCP na VLAN 100
AP9115	DHCP na VLAN 100

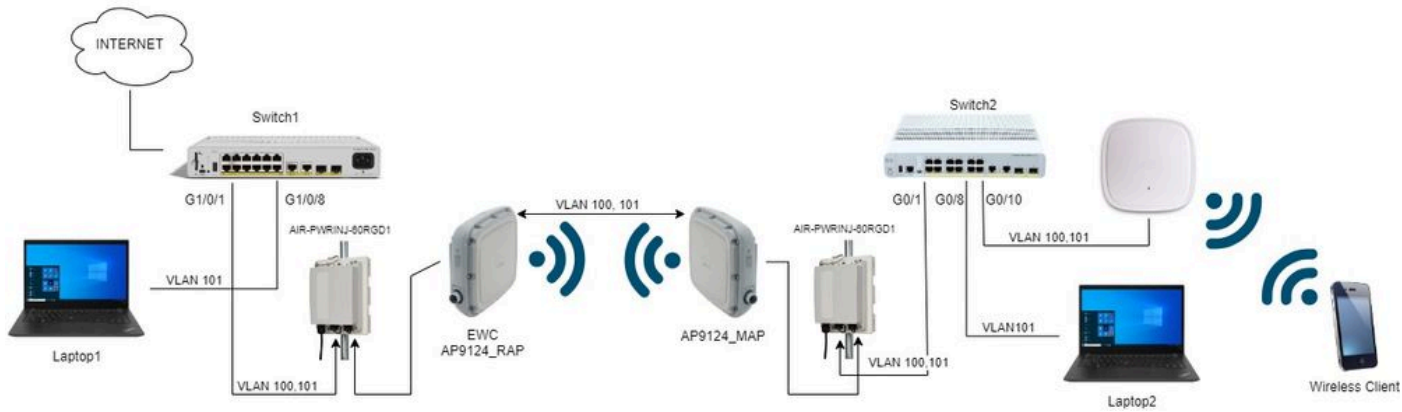


Diagrama de Rede



Observação: os APs C9124 são alimentados usando AIR-PWRINJ-60RGD1 com as diretrizes do [Guia de Instalação de Hardware de Ponto de Acesso Externo do Cisco Catalyst 9124AX Series](#).

---

## Configurações

Este documento supõe que já existe um AP 9124 executando EWC com implantação inicial feita de acordo com o [white paper Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\)](#).

Para obter outras dicas e truques sobre o processo de conversão, consulte o documento [Converter pontos de acesso Catalyst 9100 em controlador sem fio integrado](#).

### Configurações do switch

Aqui estão as configurações relevantes dos switches.

As portas de switch onde os APs estão conectados estão no modo trunk com a VLAN nativa definida como 100 e permitindo a VLAN 101.

Durante a preparação dos APs, você precisa configurar o MAP como MAP, portanto, você precisa fazer o AP se unir ao eWC via ethernet. Aqui, usamos a porta G1/0/2 do Switch 1 para preparar o MAP. Após a preparação, o MAP é movido para o Switch2.

As portas de switch onde os laptops estão conectados são configuradas como portas de acesso na VLAN 101.

Switch 1:

```
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
```

Switch 2:

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

```

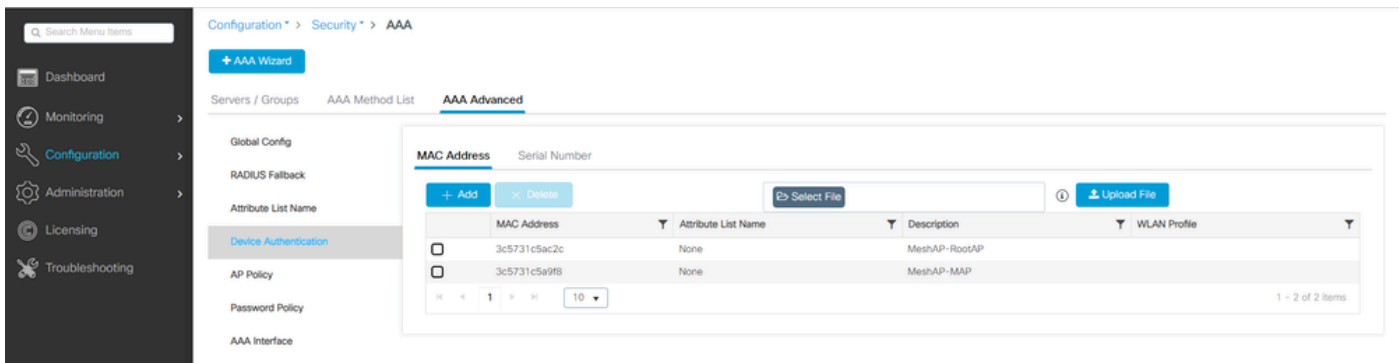
description laptop2
switchport access vlan 101
switchport mode access
spanning-tree portfast edge
end
interface GigabitEthernet0/1
description AP9115
switchport trunk native vlan 100
switchport trunk allowed vlan 100,101
switchport mode trunk
end

```

## Configuração EWC e RAP

Após a configuração Day0 do AP EWC, o AP incorporado precisa unir-se a si mesmo.

1. Adicione os endereços MAC Ethernet do ponto de acesso raiz e do ponto de acesso em malha à autenticação do dispositivo. Vá para Configuration > Security > AAA > AAA Advanced > Device Authentication, clique no botão +Add:



Endereços MAC na Autenticação do Dispositivo

## Comandos CLI:

```

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

```

O endereço MAC Ethernet pode ser confirmado executando-se o "show controllers wired 0" a partir do CLI do AP. Exemplo do AP raiz:

```

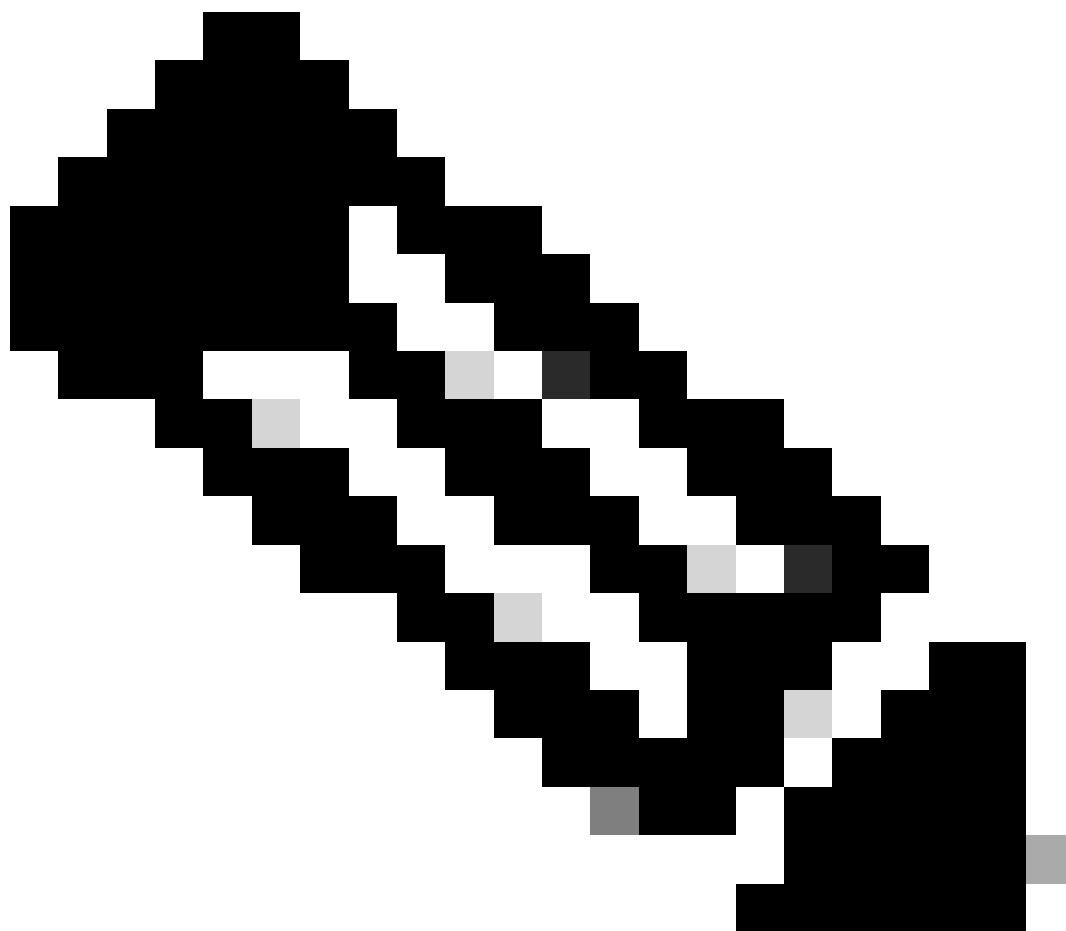
AP3C57.31C5.AC2C#show controllers wired 0
wired0 Link encap:Ethernet HWaddr 3C:57:31:C5:AC:2C

```



O acesso ao shell do AP subjacente pode ser concluído com o comando "wireless ewc-ap ap shell username x", como exemplificado:

```
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#
```



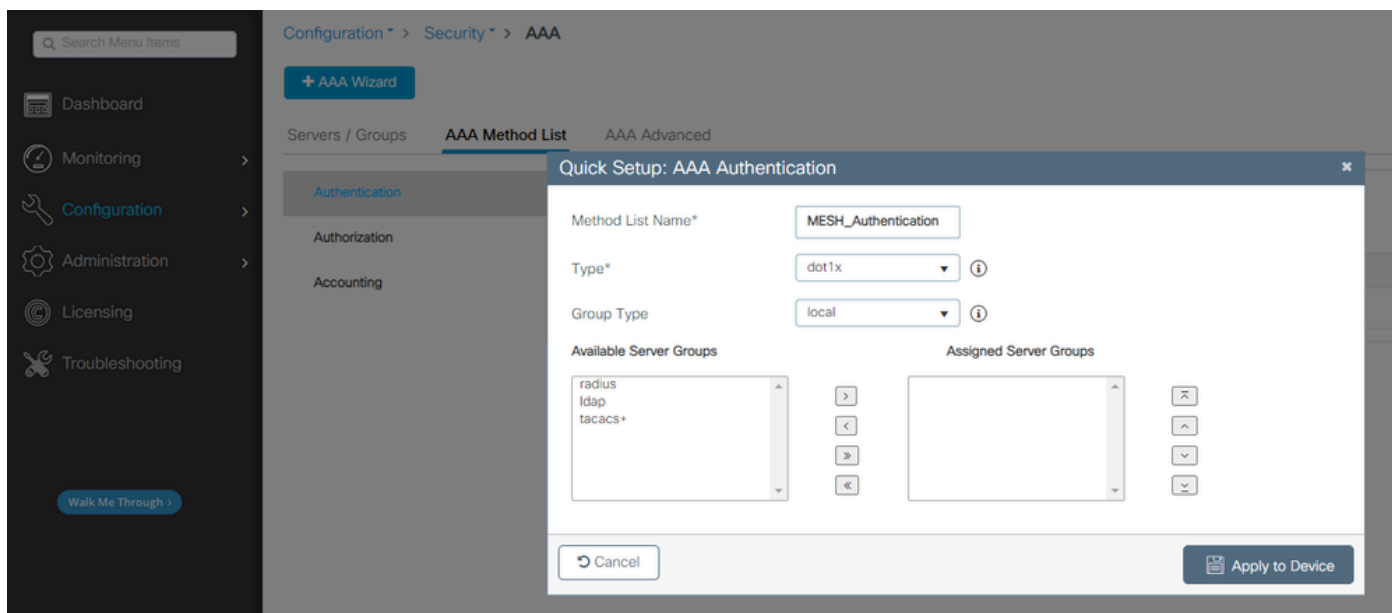
Observação: esse comando é equivalente ao apciscoshell que estava disponível anteriormente nos controladores Mobility Express.

Se o nome de usuário e a senha de gerenciamento do AP não forem especificados no

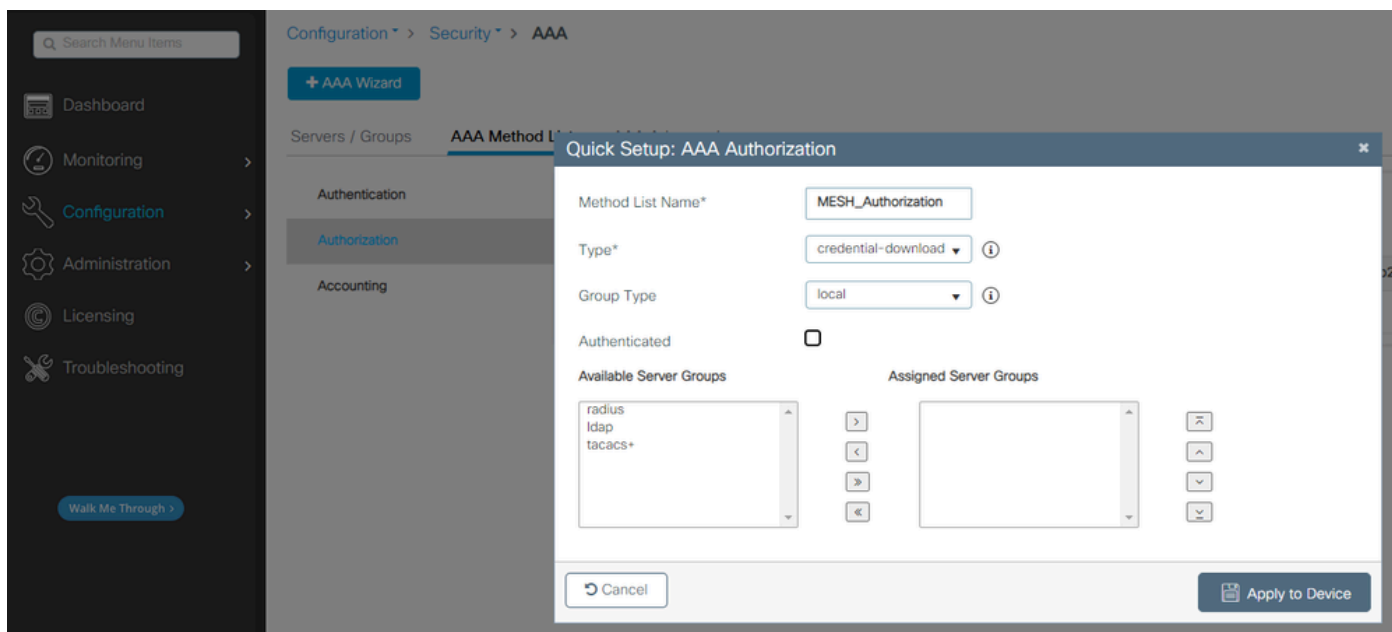
---

perfil do AP, use o nome de usuário padrão Cisco e a senha Cisco.

## 2. Adicionar Métodos de Autenticação e Autorização:



Lista de métodos de autenticação



Lista de métodos de autorização

## Comandos CLI:

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

3. Vá para Configuration > Wireless > Mesh. Como a configuração neste documento requer Ethernet Bridging, habilite Ethernet Bridging Permitir BPDUs:

The screenshot shows the configuration page for Mesh. The breadcrumb navigation is Configuration > Wireless > Mesh. The 'Global Config' section is active, showing various settings. The 'Ethernet Bridging Allow BDPUs' checkbox is checked. Other settings include 'Subset Channel Sync', 'Extended UNII B Domain Channels', 'RRM', 'Auto-DCA', 'PSK Provisioning', and 'Default PSK'. The 'Alarm' section on the right has an 'Apply' button and several input fields for 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).

Ethernet Bridging Permitir BPDUs

Comandos CLI:

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



Observação: por padrão, os APs de malha não estão encaminhando BPDUs pelo link de malha.

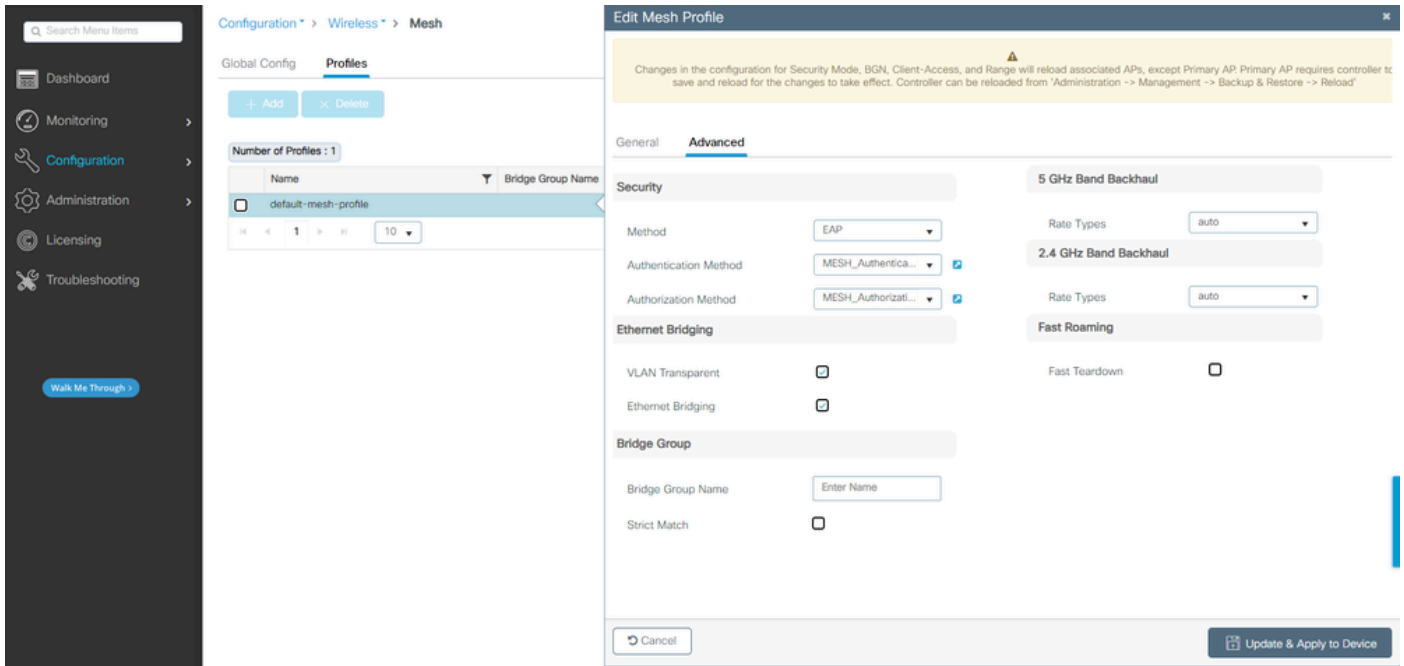
Se você não tiver nenhum link redundante entre os dois locais, ele não será necessário.

Se houver links redundantes, você precisará permitir BPDUs. Se isso não for feito, você corre o risco de criar um loop STP na rede.

---

4. Configure o default-mesh-profile onde você seleciona os métodos de Autenticação e Autorização AAA configurados anteriormente. Clique e edite o default-mesh-profile.

Vá até a guia Avançado e selecione os métodos Autenticação e Autorização. Ative a opção Ethernet Bridging.



Editor default-mesh-profile

## Comandos CLI:

```

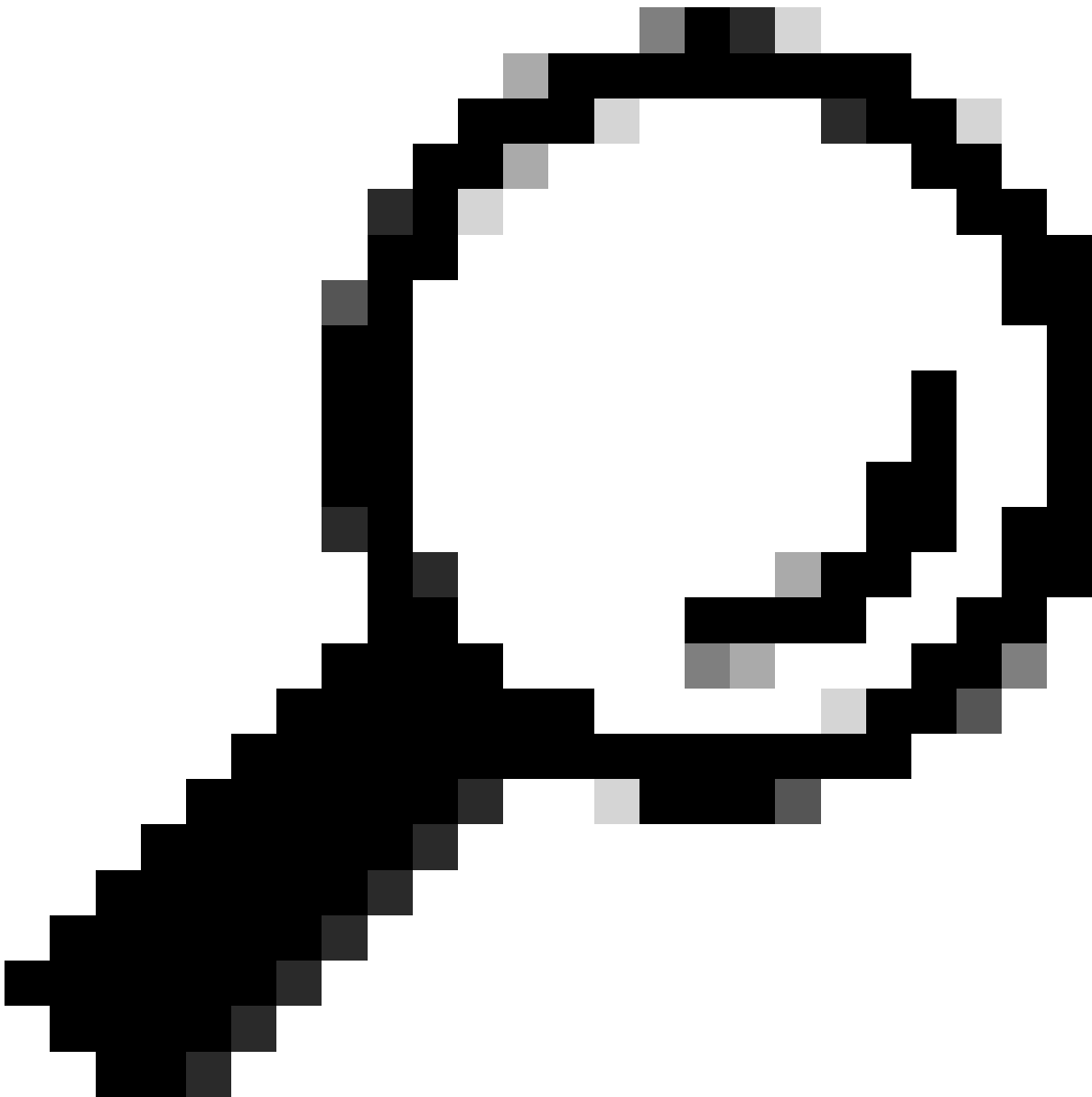
9124EWC(config)#wireless profile mesh default-mesh-profile
9124EWC(config-wireless-mesh-profile)#description "default mesh profile"
9124EWC(config-wireless-mesh-profile)#ethernet-bridging
9124EWC(config-wireless-mesh-profile)#ethernet-vlan-transparent
9124EWC(config-wireless-mesh-profile)#method authentication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

```

Texto explicativo especial para a opção VLAN Transparente:

Esse recurso determina como um ponto de acesso de malha trata as marcas de VLAN para o tráfego de Ethernet com bridge:

- Se VLAN Transparent estiver habilitado, as marcas de VLAN não serão manipuladas e os pacotes serão interligados como pacotes não marcados.
  - Nenhuma configuração de portas Ethernet é necessária quando VLAN transparent está habilitado. A porta Ethernet passa quadros marcados e não marcados sem interpretar os quadros.
- Se VLAN Transparente estiver desabilitado, todos os pacotes serão tratados de acordo com a configuração da VLAN na porta (tronco, acesso ou modo normal).
  - Se a porta Ethernet estiver definida para o modo Tronco, a marcação de VLAN Ethernet deverá ser configurada.



Dica: para usar a marcação de VLAN de AP, você deve desmarcar a caixa de seleção VLAN Transparent.

Se você não usar a marcação de VLAN, significa que o RAP e o MAP estão na VLAN nativa configurada nas portas de tronco. Nessa condição, se desejar que outros dispositivos atrás do MAP estejam na VLAN Nativa (aqui VLAN 100), você precisará habilitar a VLAN Transparente.

---

5. O AP interno entra no EWC e você pode verificar o estado de junção do AP usando o comando "show ap summary":

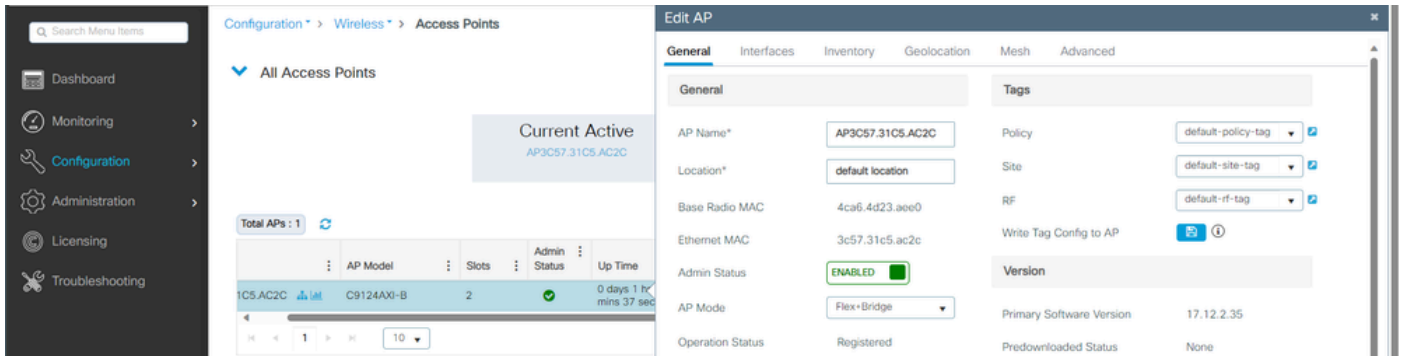
```
9124EwC#show ap summary
Number of APs: 1

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
```

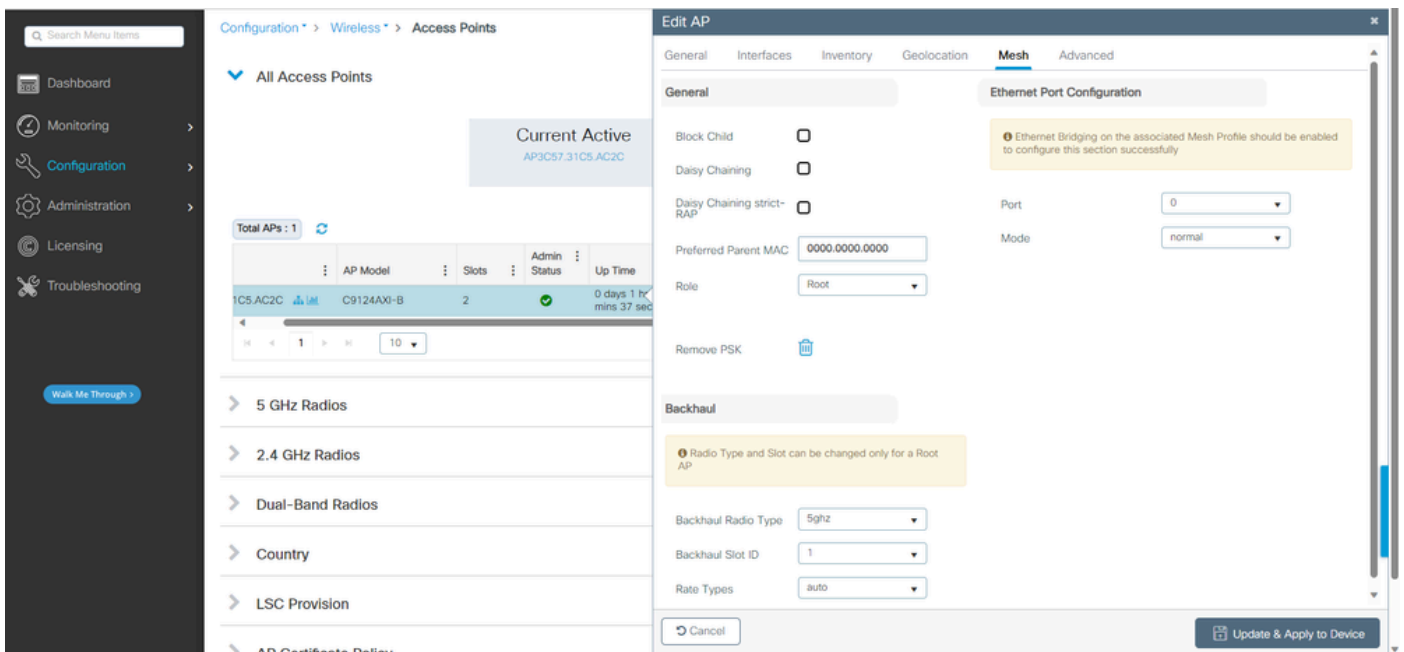
show ap summary

Você também pode ver o AP unido através da GUI, onde o AP aparece como modo Flex+Bridge. Por conveniência, você pode alterar o nome do AP agora. Nessa configuração, é usado o nome AP9124\_RAP:



Detalhes gerais do AP

Você pode editar a localização geográfica e, em seguida, na guia Mesh, certifique-se de que sua função esteja configurada como Root AP e que a configuração da porta Ethernet esteja definida como trunk com as IDs de VLAN correspondentes:



Raiz da Função Mesh

Edit AP
✕

---

General
Interfaces
Inventory
Geolocation
Mesh
Advanced

**General**

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Remove PSK

**Ethernet Port Configuration**

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

Port

Mode

Native VLAN ID\*

Allowed VLAN IDs

**Backhaul**

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

Backhaul Radio Type

Backhaul Slot ID

Rate Types

↶ Cancel

Update & Apply to Device

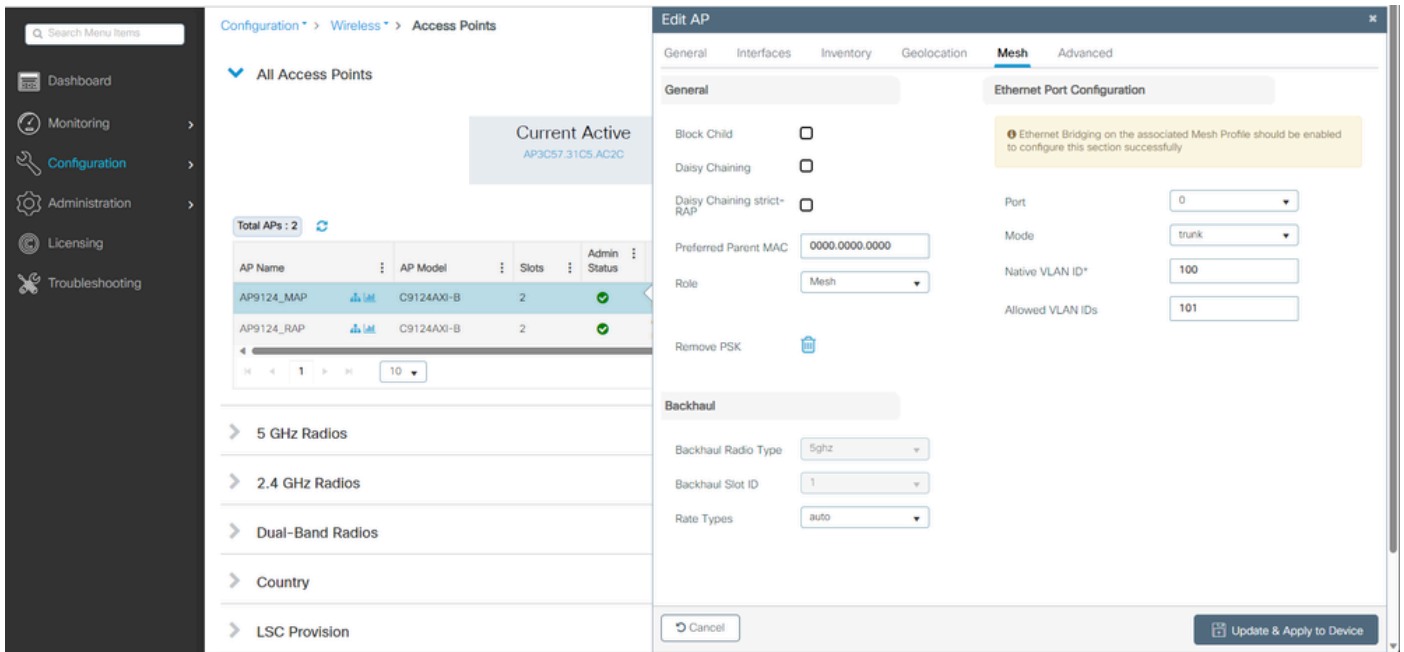
Configuração da porta Ethernet

## Configurar MAP

Agora é hora de se juntar ao MAP 9124.

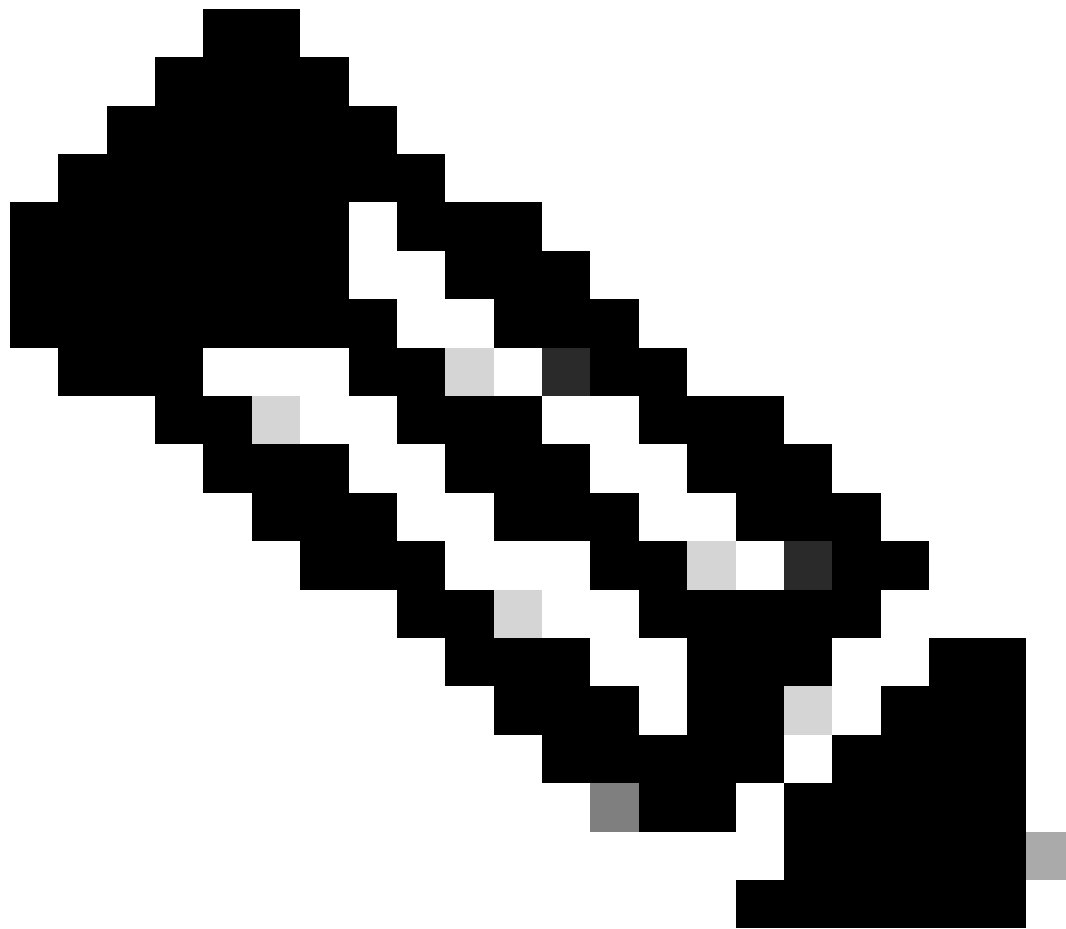
1. Conecte o AP MAP ao Switch 1 para preparação. O AP entra no EWC e aparece na lista de APs. Altere seu nome para algo como AP9124\_MAP e configure-o como Mesh Role na guia Mesh. Clique em Update & Apply to Device:





configuração de MAP

2. Desconecte o AP do Switch 1 e conecte-se ao Switch 2 de acordo com o Diagrama de Rede. O MAP adere ao conselho de empresa europeu através da interface sem fios através do RAP.



Observação: como os APs são alimentados através de injetor de energia, o AP não fica inativo e, como a configuração está em um ambiente controlado, o Switch2 está fisicamente próximo e podemos simplesmente mover o cabo de um switch para o outro.

---

Você pode conectar um cabo de console ao AP e ver o que acontece através do console. Aqui estão algumas mensagens importantes vistas.

---

Observação: da versão 17.12.1, a taxa de baud de console padrão dos APs 802.11AX é alterada de 9600 bps para 115200 bps.

---

O MAP perde conectividade com o 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
[...]
```

O MAP vai para o modo de descoberta via rede sem fio e encontra o RAP via Radio Backhaul no canal 36, encontra o EWC e junta-se a ele:

```
[*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
[...]
```

A MAP está agora associada à CER através da RAP.

O AP C9115 agora pode obter um endereço IP na VLAN 100 e depois ingressar no EWC:



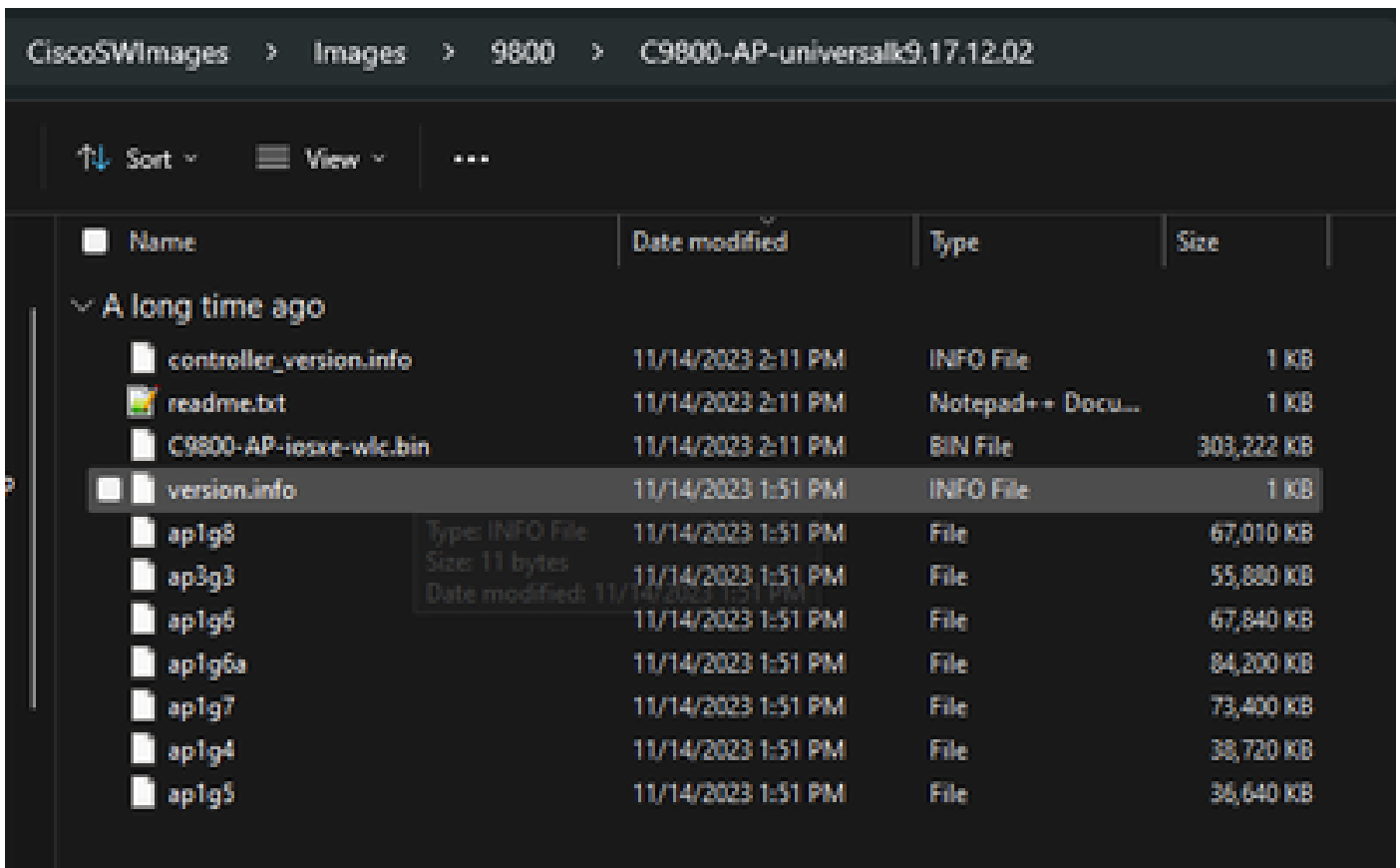
Aviso: lembre-se de que a VLAN 100 é a VLAN nativa do tronco das portas de switch. Para que o tráfego do AP na VLAN 100 acesse a WLC na VLAN 100, o link de malha deve ter VLAN Transparent habilitado. Isso é feito na seção Ponte Ethernet do perfil de malha.

```
[*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
```

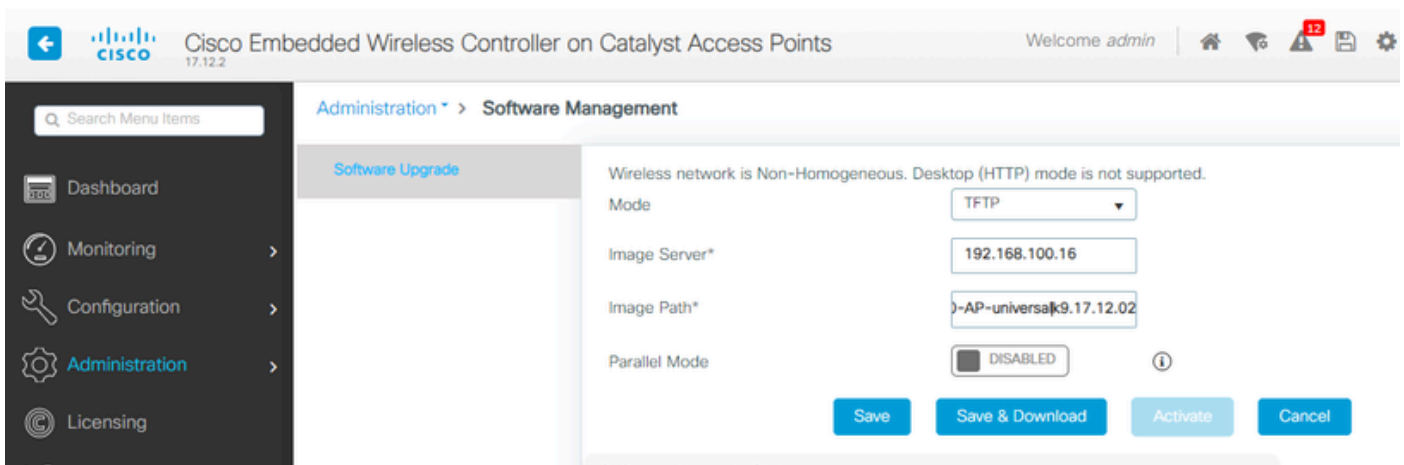
```
[...]
[*01/19/2024 15:13:56.1660] dtls_verify_server_cert: Controller certificate ve
[*01/19/2024 15:13:56.9000] sudi99_request_check_and_load: Use HARSA SUDI cert
[*01/19/2024 15:13:57.2980]
[*01/19/2024 15:13:57.2980] CAPWAP State: Join
[*01/19/2024 15:13:57.3170] shared_setenv PART_BOOTCNT 0 &> /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 este é um AP EWC, ele contém apenas a imagem do AP que corresponde ao seu próprio modelo (aqui um C9124 executa ap1g6a). Quando você se une a um modelo diferente de AP, você tem uma rede não-homogênea.

Nessas condições, se o AP não estiver na mesma versão, ele precisará fazer o download da mesma versão, portanto, certifique-se de que você tenha um servidor e um local TFTP/SFTP válidos, com as imagens do AP, configuradas no EWC > Administração > Gerenciamento de software:



Servidor TFTP com pasta de imagens AP



Imagens AP

O AP é mostrado na lista de APs e você pode atribuir um PolicyTag:

Cisco Embedded Wireless Controller on Catalyst Access Points

Welcome admin

Search APs and Clients

Feedback

Configuration > Wireless > Access Points

All Access Points

Current Active  
AP9124\_RAP

Total APs : 3

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

5 GHz Radios

Edit AP

General Interfaces Inventory Geolocation ICap Advanced

General

AP Name\* AP9115

Location\* default location

Base Radio MAC 1cd1.e079.66e0

Ethernet MAC 84f1.47b3.2cdc

Admin Status ENABLED

AP Mode Flex

Operation Status Registered

Fabric Status Disabled

CleanAir NSI Key

LED Settings

LED State ENABLED

Tags

Policy LocalSWTag

Site default-site-tag

RF default-rf-tag

Write Tag Config to AP

Version

Primary Software Version 17.12.2.35

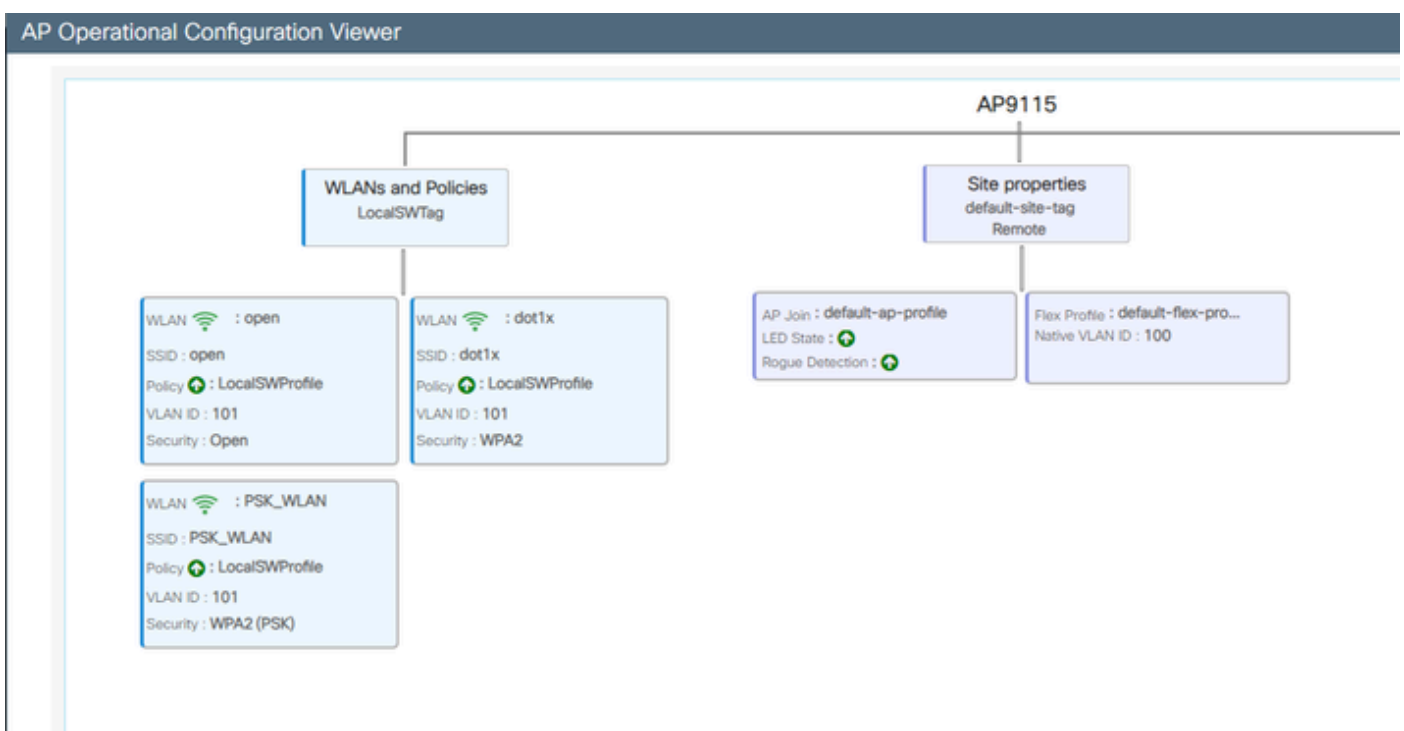
Predownloaded Status Predownloading

Predownloaded Version 0.0.0.0

Next Retry Time 0

Boot Version 1.1.2.4

Lista AP com detalhes do 9115



Visualização operacional do AP

## Verificar

Você pode ver a árvore de malha via GUI que também fornece a saída do CLI se você usar o comando "show wireless mesh ap tree". Na GUI, vá para 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

```

Árvore AP de malha

No RAP e no MAP, você pode verificar o backhaul de malha usando o 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

Você pode verificar a configuração de entroncamento de VLAN de malha no lado do 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:

Laptop2 conectado ao Switch 2 recebeu o endereço IP da 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
```

O Laptop1 colocado no Switch1 recebeu um IP da 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
```



Observação: observe que para testar o ICMP entre dispositivos Windows é necessário permitir o ICMP no firewall do sistema. Por padrão, os dispositivos Windows bloqueiam o ICMP no firewall do sistema.

---

Outro teste simples para verificar o Ethernet Bridging é ter SVI para VLAN 101 em ambos os switches e configurar o Switch 2 SVI para DHCP. O SVI do Switch 2 para a VLAN 101 obtém o IP da VLAN 101 e você pode fazer ping no SVI da VLAN 101 do Switch 1 para verificação de conectividade da 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#
```

O modo local AP C9115 também aderiu ao CER:

Configuration > Wireless > Access Points

▼ All Access Points

Current Active  
AP9124\_RAP

Current Standby  
Not Applicable

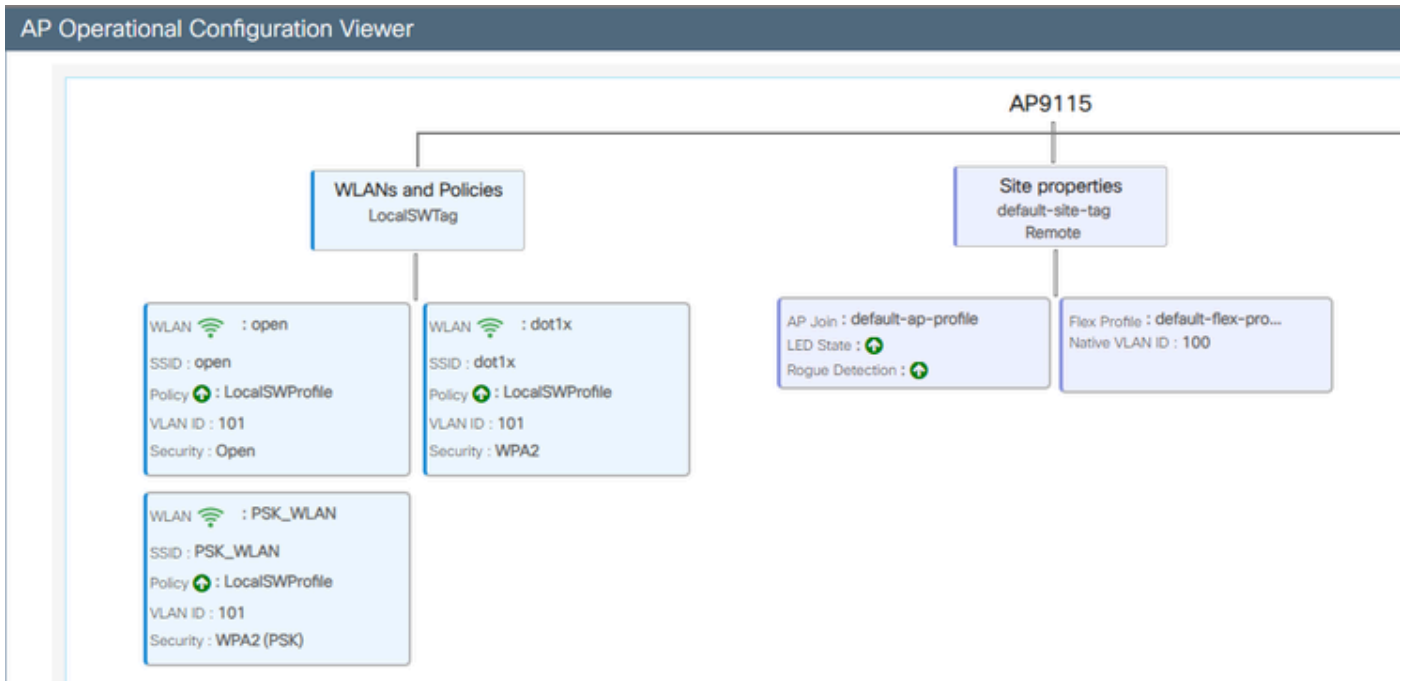
Preferred Active  
AP9124\_RAP

Total APs: 3

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

AP 9115 Participação no Conselho de Empresa Europeu

Criadas 3 WLANs, abertas, PSK e dot1x mapeadas para um Perfil de Política com VLAN 101 definido nas Políticas de Acesso:



Configuração operacional do AP9115

Os clientes sem fio podem se conectar às WLANs:

Client MAC Address	IP Address	IPV6 Address	AP Name	Site ID	SSID	WLAN ID	Client Type	State
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

## Troubleshooting

Nesta seção, comandos úteis e algumas dicas, truques e recomendações são apresentados.

Comandos úteis

Em 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

```

Opções de malha de depuração RAP/MAP

No 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 no WLC, o melhor ponto de início é usar o rastreamento RadioActive com o endereço MAC do MAP/RAP.

Exemplo 1: RAP recebe adjacência de MAP e obtém autenticação

<#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

```

Exemplo 2: endereço MAC do MAP não adicionado ao WLC ou adicionado incorretamente

<#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

```

Exemplo 3: RAP perde 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
```

## Dicas, truques e recomendações

- Ao atualizar o MAP e o RAP para a mesma versão de imagem pelo fio, evitamos o download de imagens pelo ar (o que pode ser problemático em ambientes de RF "sujos").
- É altamente recomendável testar a instalação em um ambiente controlado antes de implantá-la no local.
- Se estiver testando o Bridging Ethernet com laptops Windows em cada lado, observe que para testar o ICMP entre dispositivos Windows é necessário permitir o ICMP no firewall do sistema. Por padrão, os dispositivos Windows bloqueiam o ICMP no firewall do sistema.
- Se APs com antenas externas estiverem sendo usados, certifique-se de consultar o guia de implantação para verificar quais antenas são compatíveis e em que porta eles devem estar conectados.
- Para fazer a ponte do tráfego de VLANs diferentes sobre o link de malha, o recurso VLAN Transparente precisa ser desabilitado.
- Considere ter um servidor syslog local para os APs, pois ele pode fornecer informações de

depuração, caso contrário, só estará disponível com uma conexão de console.

## Referências

[Dados técnicos do Cisco Embedded Wireless Controller em Pontos de Acesso Catalyst](#)

[White Paper sobre Cisco Embedded Wireless Controller em Catalyst Access Points \(EWC\)](#)

[Configurando o link de malha ponto a ponto com ponte Ethernet em APs Mobility Express](#)

## 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.