

Configurar APs em malha para Bridging de Dados Local no Modo Flex e Bridge

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Adicionar Ponto de Acesso ao Banco de Dados Local do Controlador](#)

[Lista de métodos AAA para autenticação](#)

[Lista de Método AAA para Autorização](#)

[Perfil de malha](#)

[Perfil de ingresso no AP](#)

[Perfil Flex](#)

[Perfil da política](#)

[Marca WLAN](#)

[Marca de política](#)

[Marca Site](#)

[Configuração de pontos de acesso](#)

[Configuração da porta do switch](#)

[Verificar](#)

Introdução

Este documento descreve a configuração de MAPs no modo Flex e Bridge para bridging de dados de cliente local, ignorando o RAP.

Pré-requisitos

Requisitos

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 switches Cisco

Componentes Utilizados

Este exemplo utiliza pontos de acesso lightweight (modelos 9124AP), que podem ser configurados como um Root Access Point (RAP) ou um Mesh Access Point (MAP) para integração transparente com o Catalyst 9800 Wireless LAN Controller (WLC).

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

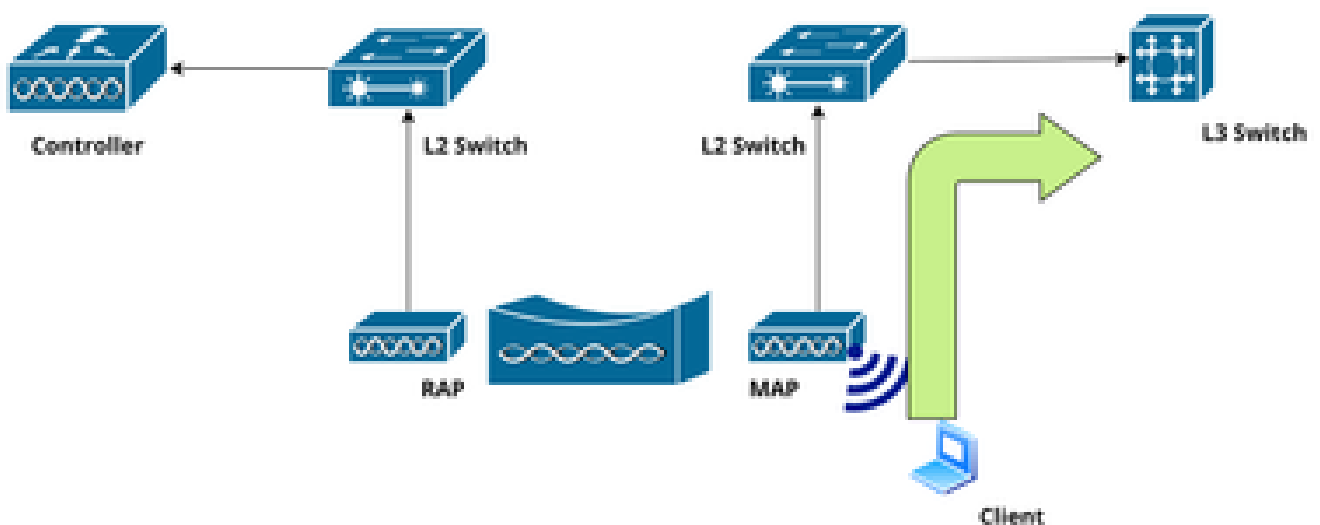
- C9800-L v17.12.5
- Cisco Catalyst 3850 Switch
- Access point Cisco Catalyst 9124AX Series

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.

Configurar

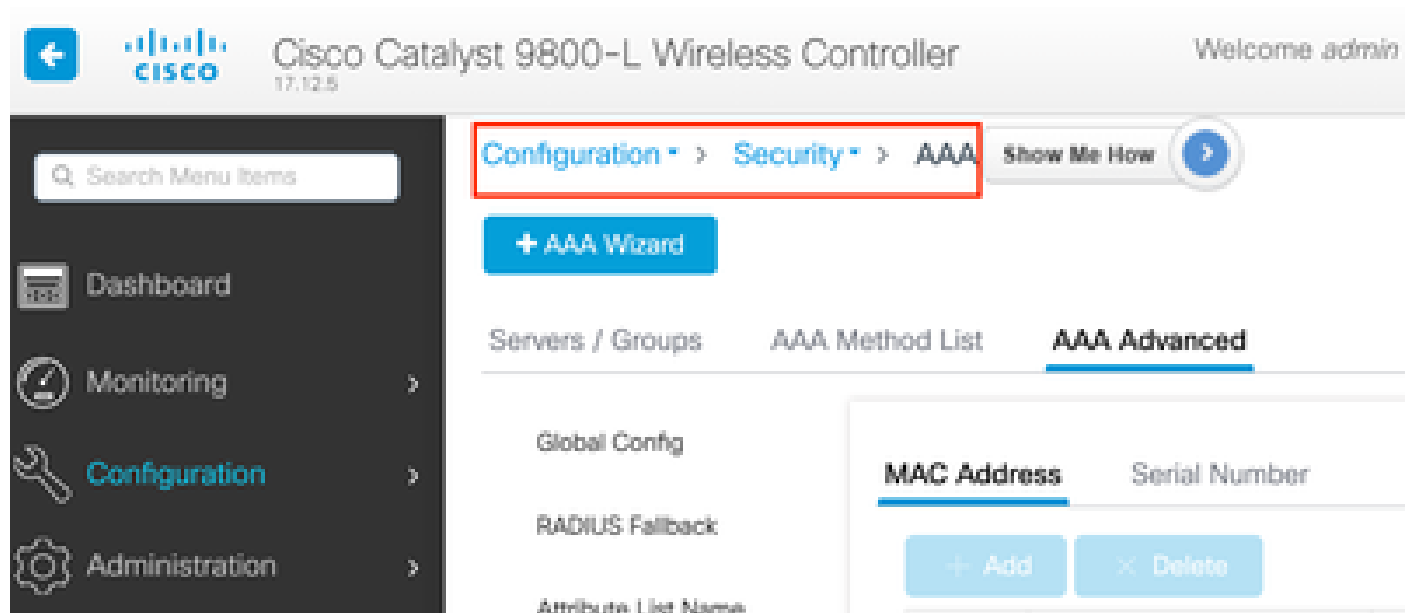
Esta seção descreve a configuração dos Pontos de Acesso em Malha (MAPs) que operam no modo Malha + Bridge, permitindo que os dados do cliente local sejam conectados diretamente ao switch de uplink, ignorando o Ponto de Acesso Raiz (RAP).

Diagrama de Rede

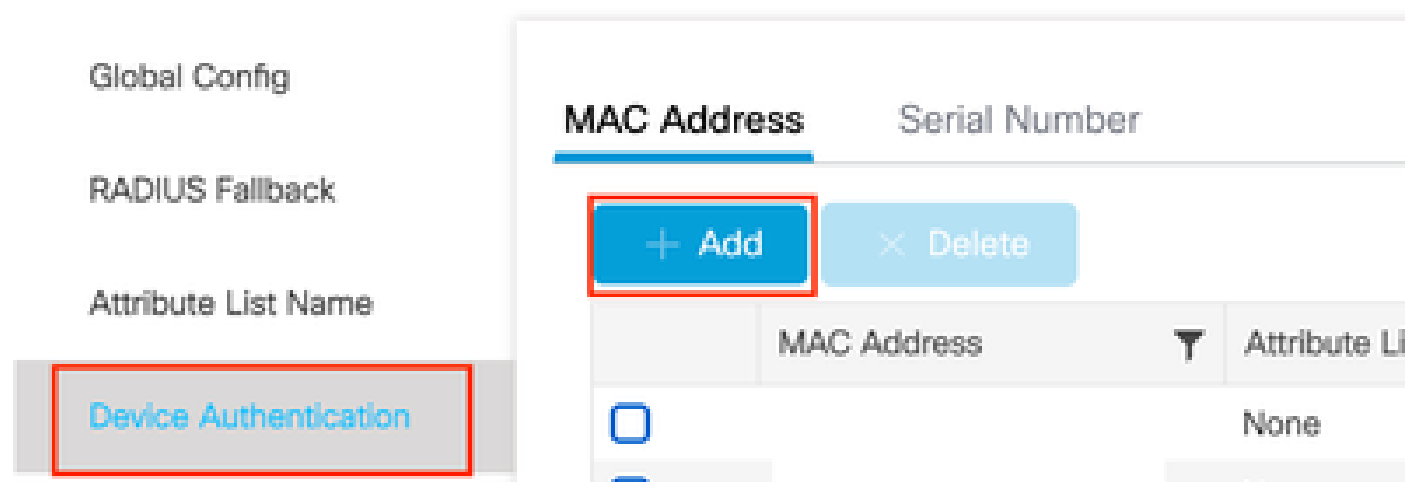


Adicionar Ponto de Acesso ao Banco de Dados Local do Controlador

Etapa 1: Navegue até Configuration > Security > AAA > AAA Advanced.



Etapa 2. SelectDevice Authentication e selectAdd.



Etapa 3. Digite o endereço MAC Ethernet base do AP para se unir à WLC. Deixe o nome da lista de atributos em branco e selecione Aplicar ao dispositivo.

MAC Address*	3a5f1c8e729b
Attribute List Name	None
Description	
WLAN Profile Name	Select a value

Lista de métodos AAA para autenticação

Etapa 1: Navegue até Configuration > Security > AAA > AAA Method List > Authentication e selecione Add.

Configuration > Security > AAA

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Passo 2: Definir nome da lista de métodos. Selecione dot1x na lista Type* e local para o Group Type. Selecione Apply to Device para salvar a configuração.

Method List Name*	MESH		
Type*	dot1x		
Group Type	local		
Available Server Groups	Assigned Server Groups		
radius ldap tacacs+ HTTSGROUP ISE_DD_Group ISE_HA Test	> < > <		+ + + +

Cancel

Update & Apply to Device

Lista de Método AAA para Autorização

Etapa 1: Navegue até Configuration > Security > AAA > AAA Method List > Authorization e selecione Add.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

	Name		Type
	default		EXEC

Passo 2: Defina o nome da lista de métodos, selecione download de credenciais no menu suspenso Tipo* e local para o Tipo de grupo. Clique em Apply to Device.

Method List Name*	MESH-Authorization
Type*	credential-downlo... ⓘ
Group Type	local ⓘ
Authenticated	☐
Available Server Groups	Assigned Server Groups
radius ldap tacacs+ HTTSGROUP ISE_DD_Group ISE_HA Trust	><><>< <><><><

Cancel

Update & Apply to Device

Perfil de malha

Etapa 1: Navegue até Configuration > Wireless > Mesh >Profiles e selecione Add.

Configuration ▾ > Wireless ▾ > Mesh

Global Config

Profiles

+ Add

× Delete

Passo 2: Na guia Geral, defina um nome e uma descrição (opcional) para o perfil Mesh.

General

Advanced

Name*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▼

IDS (Rogue/Signature Detection)

☐

Etapa 3: na guia Avançado, defina o campo Método como EAP e selecione os perfis Autorização e Autenticação criados anteriormente nos menus suspensos. Por fim, marque a caixa de seleção Ethernet Bridging e selecione Update and apply.

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

☐

Ethernet Bridging

☒

Perfil de ingresso no AP

Passo 1: Navegue até Configuration > Tag & Profiles > AP Join > Profile e clique em Add.

Configuration > Tags & Profiles > AP Join

+ Add

× Delete

Clone

AP Join Profile Name

Passo 2: Defina o nome do perfil e a descrição (opcional).

General

Client

CAPWAP

AP

Management

S

Name*

Mesh-AP-Join

Description

Enter Description

Country Code

IN

Time Zone

☒ Not Configured

☐ Use-Controller

☐ Delta from WLC

Etapa 3: Navegue até a guia AP, selecione o Perfil de malha no menu suspenso Nome do perfil de malha, defina EAP-FAST para o Tipo de EAP e CAPWAP DTLS para o Tipo de autorização de AP e clique em Aplicar ao dispositivo.

Edit AP Join Profile

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

Geolocation

General

Power Management

Hyperlocation

AP Statistics

Power Over Ethernet

Switch Flag

☐

Power Injector State

☐

Power Injector Type

Unknown

Injector Switch MAC

0000.0000.0000

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-Profile

Cancel

Update & Apply to Device

Perfil Flex

Etapa 1: Configuração > Marcas e perfis > Flex, depois clique em Adicionar.

Configuration > Tags & Profiles > Flex

+ Add

× Delete

Clone

Passo 2: Defina um nome para o perfil do Flex.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

Passo 3: Navegue até a guia vlan e Configure o Nome da VLAN e a ID da VLAN para Local Bridging of Wireless Client Traffic, clique em Save.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

+ Add

< Delete

VLAN Name

T

ID

T

Ingress ACL

T

Egress ACL

T

0

10

No items to display

VLAN Name*

Bridge-VLAN

VLAN ID*

100

ACL

☒ Unidirectional☐ Bidirectional

Ingress ACL

Select ACL

Egress ACL

Select ACL

✓ Save

Cancel

Cancel

Update & Apply to Device

Perfil da política

Passo 1: Navegue até Configuration > Tags & Profiles > Policy e clique em Add.

Configuration ▾ > Tags & Profiles ▾ > Policy

+ Add

× Delete

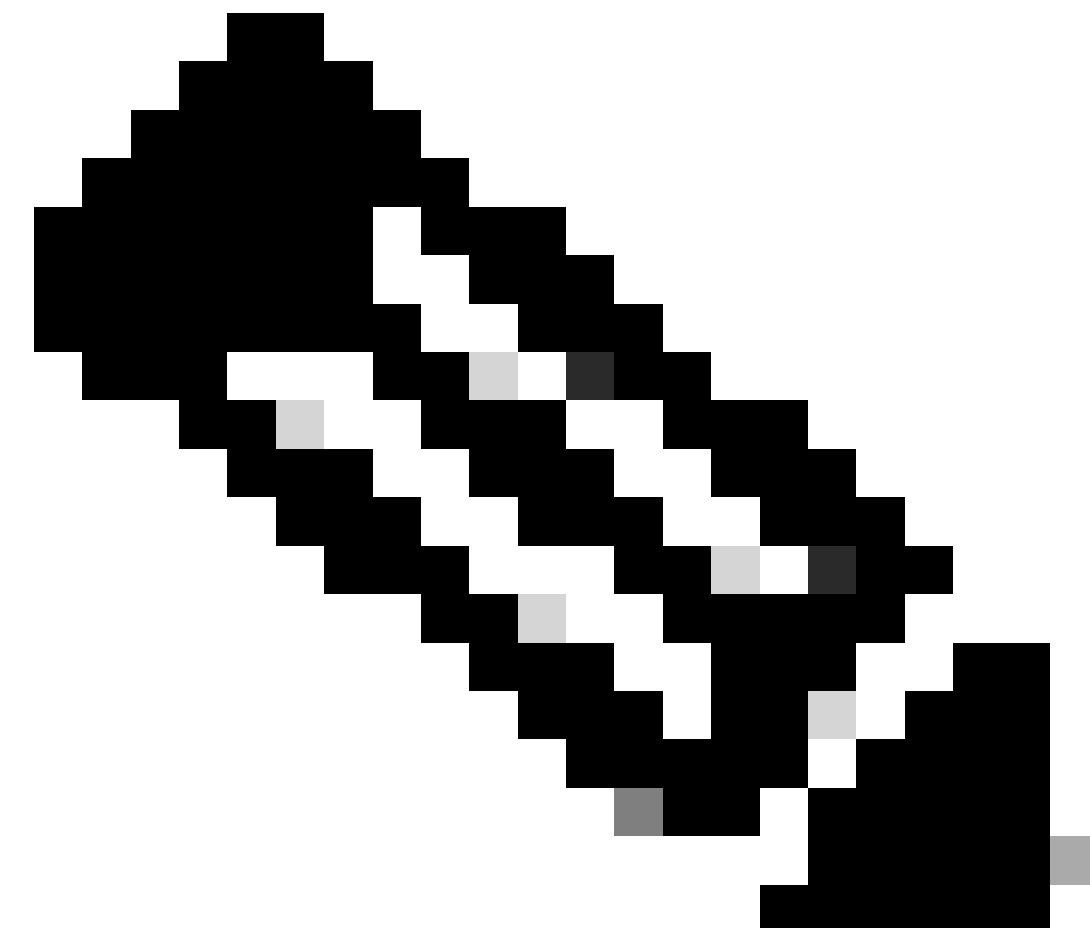
Clone

Admin
Status ▾

Associated
Policy Tags ⓘ ▾

Policy Profile Name

Passo 2: Na guia Geral, defina o nome do perfil, defina Status como Ativado e Desative a Comutação Central.



Note: Para habilitar o Bridging local do tráfego do cliente, a Central Switching deve ser desabilitada. Com base na configuração do SSID, outras opções podem ser ativadas ou

desativadas conforme necessário.

General

Access Policies

QoS and AWC

Mobility

Advanced

Name*	Bridge-Policy	WLAN Switching Policy	
Description	Enter Description	Central Switching	☐ DISABLED
Status	ENABLED ☒	Central Authentication	ENABLED ☒
Passive Client	☐ DISABLED	Central DHCP	☐ DISABLED
IP MAC Binding	ENABLED ☒	Flex NAT/PAT	☐ DISABLED
Encrypted Traffic Analytics	☐ DISABLED		
CTS Policy			
Inline Tagging	☐		
SGACL Enforcement	☐		
Default SGT	2-65519		

Cancel

Update & Apply to Device

Etapa 3: Configure o VLANID especificado na guia VLAN do AP Flex Profile e clique em Update & Apply.

General
Access Policies
QoS and AVC
Mobility
Advanced

RADIUS Profiling
☐

HTTP TLV Caching
☐

DHCP TLV Caching
☐

WLAN Local Profiling

Global State of Device Classification
Enabled ⓘ

Local Subscriber Policy Name
 ⓘ

VLAN

VLAN/VLAN Group
 ⓘ

Multicast VLAN

WLAN ACL

IPv4 ACL
 ⓘ

IPv6 ACL
 ⓘ

URL Filters ⓘ

Pre Auth
 ⓘ

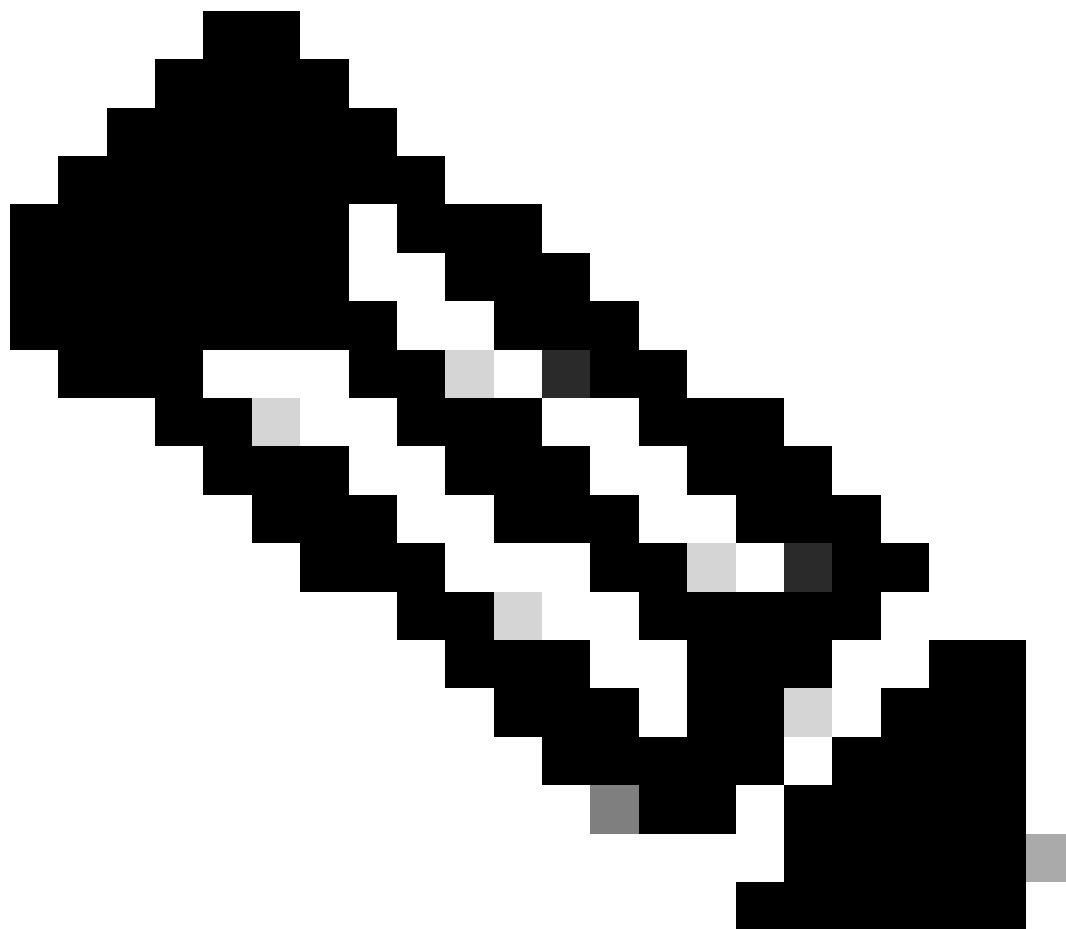
Post Auth
 ⓘ

Marca WLAN

Passo 1: Navegue até Configuration > Tags & Profiles > WLANs e selecione Add.

Passo 2: Na guia General, configure o Profile name, SSID e defina o status como enabled.

Passo 3: Selecione a guia Security, Enable WAP+WPA2 e configure uma chave pré-compartilhada.



Note: A configuração do SSID depende inteiramente de seus requisitos. Para este exemplo, um SSID baseado em PSK é configurado.

General

Security

Advanced

Add To Policy Tags

Profile Name*

Bridge

R

SSID*

Bridge-SSID

WLAN ID*

6

6

St

Status

ENABLED



Broadcast SSID

ENABLED



5

St

Edit WLAN

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☒ WPA + WPA2
 ☐ WPA2 + WPA3
 ☐ WPA3
 ☐ Static WEP
 ☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

GTK Randomize

☐

WPA2 Policy

☒

OSN Policy

☐

Fast Transition

Status

Disabled

Over the DS

☐

Reassociation Timeout *

20

WPA2 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Disabled

Auth Key Mgmt

802.1X

☐

Easy-PSK

☐

FT + 802.1X

☐

802.1X-SHA256

☐

PSK

☒

CKM

☐

FT + PSK

☐

PSK-SHA256

☐

PSK Format

ASCII

PSK Type

AES

Pre-Shared Key*

Cancel

Update & Apply to Device

Marca de política

Passo 1: Navegue até Configuration > Tags & Profiles > Tags > Policy Tab, clique em Add.

Etapa 2: Crie uma tag de política definindo um nome e associando a WLAN e o perfil de política.

Add Policy Tag

Name*

Mesh-Policy-Tag

Description

Enter Description

WLAN-POLICY Maps: 0

+ Add

× Delete

WLAN Profile

Policy Profile

10

No items to display

Map WLAN and Policy

WLAN Profile*

Bridge

Policy Profile*

Bridge-Policy

×

✓

> WLAN-POLICY Maps: 0

Cancel

Apply to Device

Marca Site

Passo 1: Navegue até Configuração > Tags e perfis > Tags > Site e clique em Adicionar.

Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Etapa 2: Configure o Nome da tag, desative a opção Ativar site local e associe o Perfil de junção AP e o Perfil Flex.

Edit Site Tag

Name*

Mesh-Site-Tag

Description

Enter Description

AP Join Profile

Mesh-AP-Join

Flex Profile

Mesh-Flex

Fabric Control Plane Name

Enable Local Site

☐

Load* ⓘ

0

Cancel

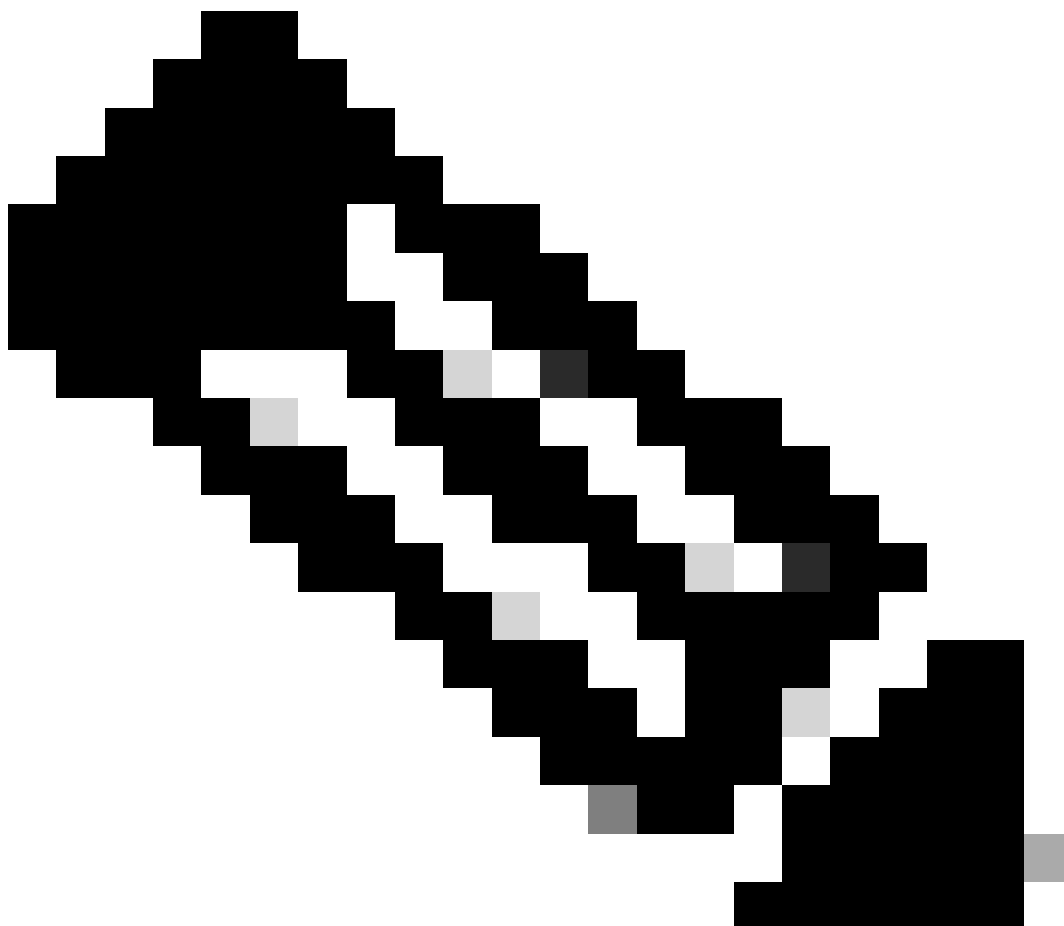
Update & Apply to Device

Configuração de pontos de acesso

Este estudo de caso pressupõe que o ponto de acesso (AP) foi unido primeiro ao controlador de LAN sem fio (WLC) no modo local e depois foi transferido para o modo Flex+Bridge.

Passo 1: Navegue até Configuration > Wireless > Access Points e selecione o AP.

Passo 2: Atribua a marca de site e a marca de política aos access points (APs).



Note: O ponto de acesso (AP) é reinicializado, estabelece conexão com o controlador no modo Flex+Bridge e a guia Mesh está disponível.

General		Tags	
AP Name*	AP34B8.8314.A204	 Changing Tags will cause the AP to momentarily lose association with the Controller. Writing Tag Config to AP is not allowed while changing Tags.	
Location*	default location		
Base Radio MAC	34b8.831d.05a0		
Ethernet MAC	34b8.8314.a204	Policy	Mesh-Policy-Tag 
Admin Status	ENABLED 	Site	Mesh-Site-Tag 

Passo 3: Na guia Mesh, selecione a função para raiz

Edit AP

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Ethernet Port Configuration

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

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

Port

Mode

VLAN ID*

Passo 4: Repita as etapas 1 e 2 para o ponto de acesso (AP) designado para funcionar como um AP em malha para colocá-lo on-line no modo Flex+Bridge. Navegue até a guia Mesh e configure a função como Mesh.

Passo 5: O Ponto de Acesso em Malha é conectado ao switch na Porta 0, configurado no Modo de Tronco, com a VLAN dos APs definida como VLAN Nativa. Certifique-se de que as VLANs permitidas incluam a VLAN cliente especificada no perfil Flex.

Passo 6: Clique em Update and Apply.

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General

Ethernet Port Configuration

Block Child
☐

Daisy Chaining
☐

Daisy Chaining strict-RAP
☐

Preferred Parent MAC

Role

Remove PSK

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

Port

Mode

Native VLAN ID*

Allowed VLAN IDs

Configuração da porta do switch

```
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 100
switchport mode trunk
end
```

Verificar

Associação de AP em malha ao AP raiz:

```
#show wireless mesh ap summary
AP Name AP Model BVI MAC BGN AP Role
-----
AP34B8.8314.A204 C9124AXI-ROW 34b8.8314.a204 Default Root AP
APC828.E536.D47C C9124AXI-ROW c828.e536.d47c Default Mesh AP
Number of Flex+Bridge APs : 2
Number of Flex+Bridge RAPs : 1
Number of Flex+Bridge MAPs : 1
```

```
#show wireless mesh ap tree
=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=====
[Sector 1]
-----
AP34B8.8314.A204 [0, 0, Default, (36,40), 0000.0000.0000, 5%, 0]
|-APC828.E536.D47C [1, 68, Default, (36,40), 0000.0000.0000, 6%, 0]

Number of Bridge APs : 2
Number of RAPs : 1
Number of MAPs : 1
```

Associação de cliente no AP da Malha:

```
#show flexconnect client
Flexconnect Clients:
mac radio vap aid state encr aaa-vlan aaa-ac1 aaa-ipv6-ac1 assoc auth switching key-method roam key-pro
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 none none none Local Central Local Other regular No Yes No 0

#show controllers dot11Radio 0 client
mac radio vap aid state encr Maxrate Assoc Cap is_wgb_wired wgb_mac_addr
52:95:C7:EE:B7:E5 0 0 1 FWD AES_CCM128 MCS92SS HE HE false 00:00:00:00:00:00
```

```
#show flexconnect client aaa-override
Flexconnect Clients:
mac vlan qos acl ipv6-acl vlan-name avgdtids avgrtdtids bstdtids bstrtdtids avgdtus avgrtdtus bstdtus bstrtdtus
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

O tráfego do Ponto de Acesso da Malha (MAP) é diretamente ligado ao switch de uplink, ignorando o Ponto de Acesso Raiz (RAP):

<#root>

DHCP:

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2883] [ 62081:607119] [APC828.E536.D47C]
```

[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2884] chatter: dhcp_req_local_sw_nonat: 1
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] [ 62081:607245] [APC828.E536.D47C]
```

[U:C] DHCP_REQUEST : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2885] chatter: dhcp_reply_nonat: 17485791
```

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613080] [APC828.E536.D47C]
```

[D:C] DHCP_ACK : TransId 0x3bcb0a7b

```
May 30 04:25:21 APC828.E536.D47C kernel: [*05/30/2025 04:25:21.2943] [ 62081:613123] [APC828.E536.D47C]
```

[D:W] DHCP_ACK : TransId 0x3bcb0a7b

ARP:

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [62464:537183] [APC828.E536.D47C]

[U:W] ARP_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0572] [62464:537219] [APC828.E536.D47C]

[U:C] ARP_QUERY : Sender 100.0.0.2 TargIp 100.0.0.1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0573] chatter: ethertype_cl1: 1748579504

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0628] [62464:542842] [APC828.E536.D47C]

[D:C] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] chatter: fromdevs_arp_resp: arp rep

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0629] [62464:542971] [APC828.E536.D47C]

[D:C] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:44 APC828.E536.D47C kernel: [*05/30/2025 04:31:44.0630] [62464:543018] [APC828.E536.D47C]

[D:W] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

May 30 04:31:45 APC828.E536.D47C kernel: [*05/30/2025 04:31:45.4301] [62465:910100] [APC828.E536.D47C]

[D:A] ARP_REPLY : Sender 100.0.0.1 HwAddr c4:44:a0:a2:61:d1

ICMP:

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [62489:785903] [APC828.E536.D47C]

[U:W] ICMP_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3059] [62489:785938] [APC828.E536.D47C]

[U:C] ICMP_ECHO : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3104] [62489:790444] [APC828.E536.D47C]

[D:C] ICMP_ECHO_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [62489:790534] [APC828.E536.D47C]

[D:C] ICMP_ECHO_REPLY : Id 39016 Seq 0

May 30 04:32:09 APC828.E536.D47C kernel: [*05/30/2025 04:32:09.3105] [62489:790583] [APC828.E536.D47C]

[D:W] ICMP_ECHO_REPLY : Id 39016 Seq 0

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.