

Configuración de AP de malla para el Bridging de datos locales en el Modo Flex y Bridge

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Agregar punto de acceso a base de datos local del controlador](#)

[Lista de métodos AAA para la autenticación](#)

[Lista de métodos AAA para la autorización](#)

[Perfil de malla](#)

[Perfil de unión a PA](#)

[Perfil de Flex](#)

[Perfil de política](#)

[Etiqueta WLAN](#)

[Etiqueta de política](#)

[Etiqueta del sitio](#)

[Configuración de puntos de acceso](#)

[Configuración del puerto del switch](#)

[Verificación](#)

Introducción

Este documento describe la configuración de los MAP en el modo Flex y Bridge para el bridging de datos del cliente local, omitiendo el RAP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

Este ejemplo utiliza puntos de acceso ligeros (modelos 9124AP), que se pueden configurar como un punto de acceso raíz (RAP) o un punto de acceso de malla (MAP) para integrarse sin problemas con el controlador de LAN inalámbrica (WLC) Catalyst 9800.

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

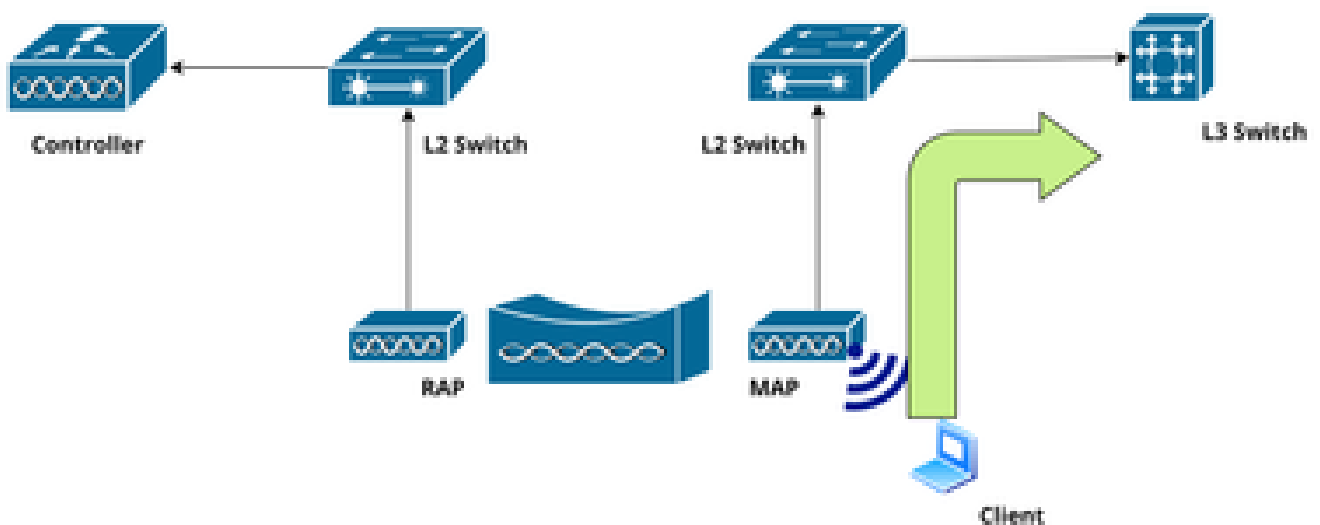
- C9800-L v17.12.5
- Cisco Catalyst 3850 Switch
- Punto de acceso Cisco Catalyst serie 9124AX

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

Configurar

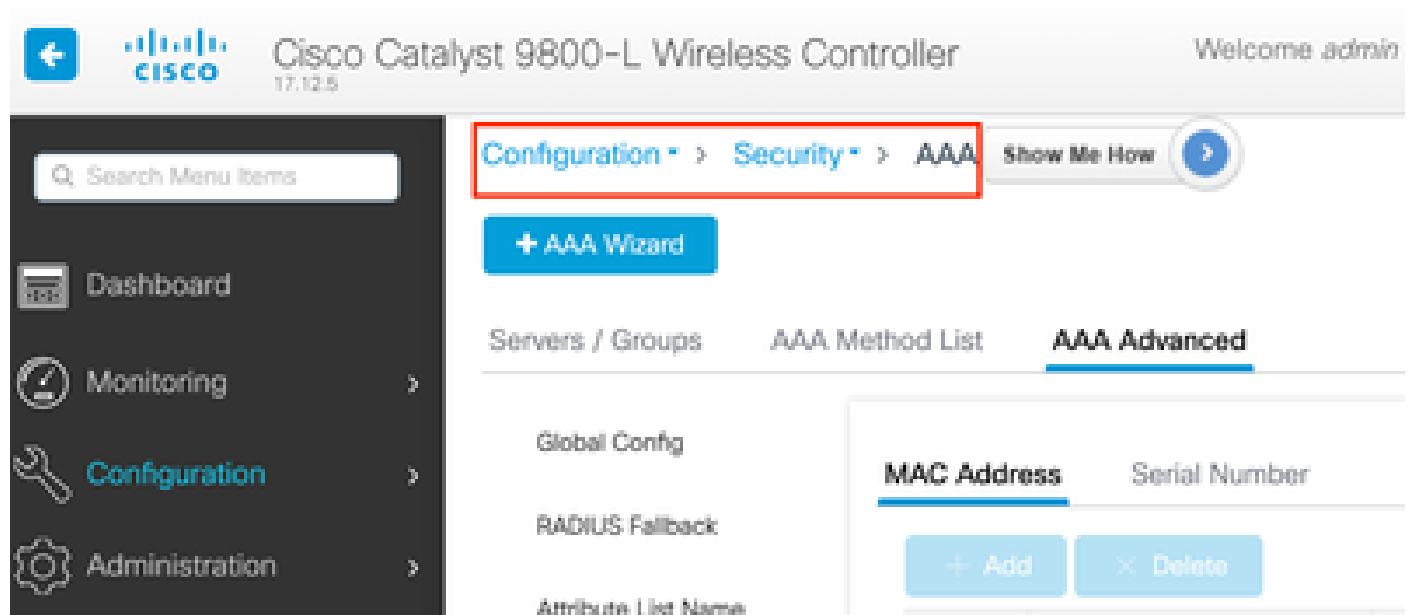
En esta sección se describe la configuración de los puntos de acceso de malla (MAP) que funcionan en el modo de malla + puente, lo que permite que los datos del cliente local se conecten en puente directamente al switch de enlace ascendente, omitiendo el punto de acceso raíz (RAP).

Diagrama de la red

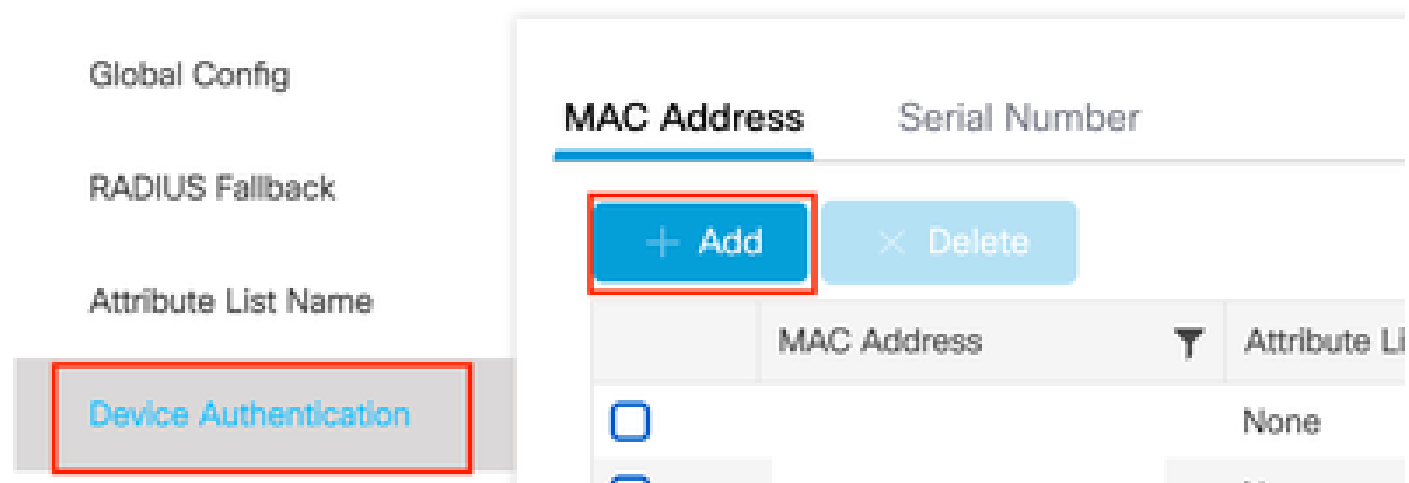


Agregar punto de acceso a base de datos local del controlador

Paso 1: Vaya a Configuration > Security > AAA > AAA Advanced.



Paso 2. Seleccione Autenticación de dispositivo y seleccione Agregar.



Paso 3. Ingrese la dirección MAC de Ethernet base del AP para unirse al WLC. Deje en blanco Attribute List Name y seleccione Apply to Device.

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

Lista de métodos AAA para la autenticación

Paso 1: Vaya a Configuration > Security > AAA > AAA Method List > Authentication y seleccione Add.

Configuration > Security > AAA

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Paso 2: Defina el nombre de la lista de métodos. Seleccione dot1x en el menú desplegable Type* y local para el Group Type. Seleccione Apply to Device para guardar la configuración.

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 métodos AAA para la autorización

Paso 1: Vaya a Configuration > Security > AAA > AAA Method List > Authorization y seleccione Add.

+ AAA Wizard

Servers / Groups

AAA Method List

AAA Advanced

Authentication

Authorization

Accounting

+ Add

× Delete

	Name		Type
	default		EXEC

Paso 2: Defina el nombre de la lista de métodos, seleccione la descarga de credenciales en el menú desplegable Type* y local para el tipo de grupo. Haga clic en Aplicar al dispositivo.

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 Test	> < > <		^ ^ v v

Cancel

Update & Apply to Device

Perfil de malla

Paso 1: Vaya a Configuration > Wireless > Mesh >Profiles y seleccione Add.

Configuration ▾ > Wireless ▾ > Mesh

Global Config

Profiles

+ Add

× Delete

Paso 2: En la pestaña General, defina un nombre y una descripción (opcional) para el perfil de malla.

General

Advanced

Name*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▼

IDS (Rogue/Signature Detection)

☐

Paso 3: en la ficha Avanzadas, establezca el campo Método en EAP y, a continuación, seleccione los perfiles Authorization y Authentication creados anteriormente en los menús desplegables. Por último, active la casilla de verificación Ethernet Bridging y seleccione Update and apply.

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

☐

Ethernet Bridging

☒

Perfil de unión a PA

Paso 1: Vaya a Configuration > Tag & Profiles > AP Join > Profile, haga clic en Add.

Configuration > Tags & Profiles > AP Join

+ Add

× Delete

Clone

AP Join Profile Name

Paso 2: Defina el nombre y la descripción del perfil (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

Paso 3: Navegue hasta la pestaña AP, seleccione el perfil de malla del menú desplegable Nombre del perfil de malla, establezca EAP-FAST para el tipo EAP y CAPWAP DTLS para el tipo de autorización AP, y haga clic en Aplicar al 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

Injector Switch MAC

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

Cancel

Update & Apply to Device

Perfil de Flex

Paso 1: Configuration > Tags & Profiles > Flex, luego haga clic en Add.

Configuration > Tags & Profiles > Flex

+ Add

× Delete

Clone

Paso 2: Defina un nombre para el perfil Flex.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

Paso 3: Navegue hasta la pestaña vlan y configure el Nombre de VLAN y el ID de VLAN para el puente local del tráfico de cliente inalámbrico, haga clic en Guardar.

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 de política

Paso 1: Navegue hasta Configuration > Tags & Profiles > Policy y haga clic en Add.

Configuration ▾ > Tags & Profiles ▾ > Policy

+ Add

× Delete

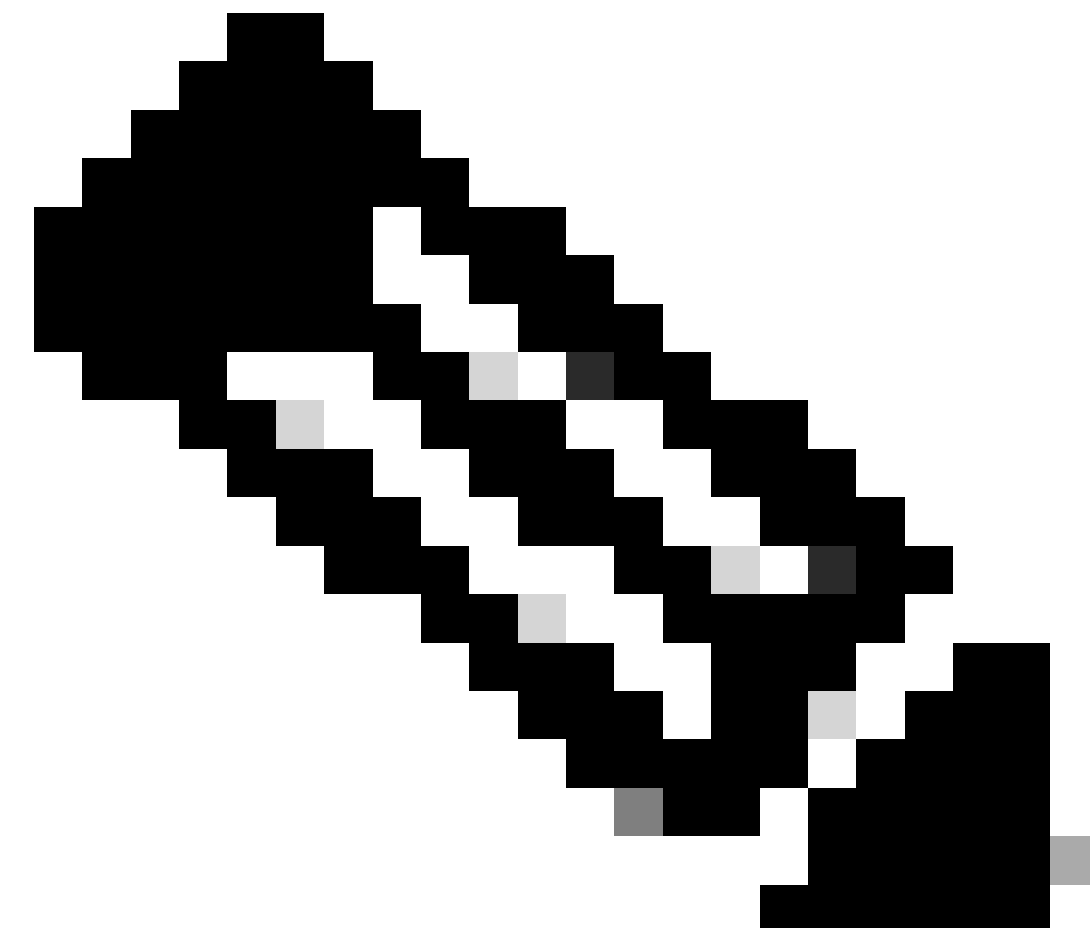
Clone

Admin
Status ▾

Associated
Policy Tags ⓘ ▾

Policy Profile Name

Paso 2: En la ficha General, defina el nombre del perfil, establezca Status en Enabled y Disable Central Switching.



Nota: Para habilitar el bridging local del tráfico del cliente, se debe inhabilitar el Switching central. Según la configuración de SSID, se pueden activar o desactivar otras opciones

según sea necesario.

General

Access Policies

QoS and AWC

Mobility

Advanced

Name*

Bridge-Policy

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

DISABLED

Central Authentication

ENABLED

Central DHCP

DISABLED

Flex NAT/PAT

DISABLED

Cancel

Update & Apply to Device

Paso 3: Configure el VLANID especificado en la pestaña VLAN del perfil flexible de AP y haga clic en Update & Apply.

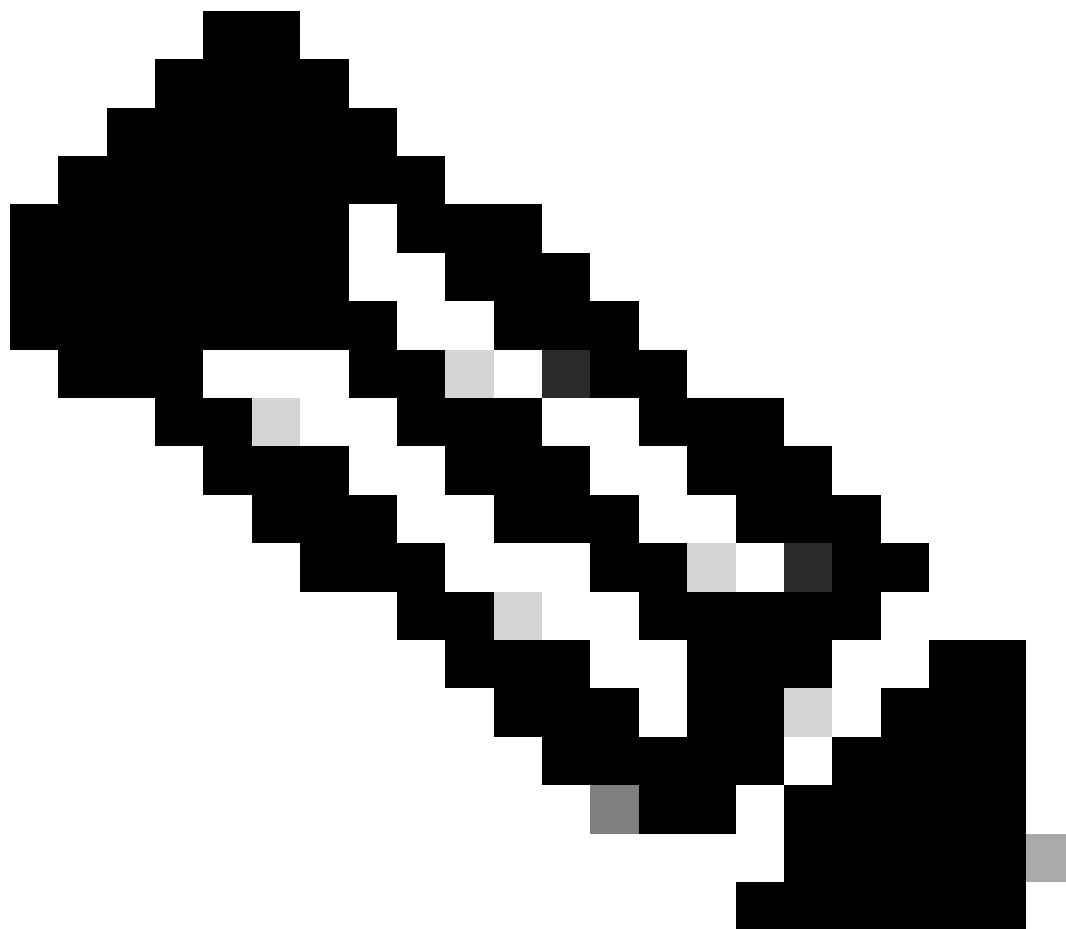
General	Access Policies	QoS and AVC	Mobility	Advanced
RADIUS Profiling ☐ HTTP TLV Caching ☐ DHCP TLV Caching ☐		WLAN ACL IPv4 ACL Search or Select IPv6 ACL Search or Select URL Filters Pre Auth Search or Select Post Auth Search or Select		
WLAN Local Profiling Global State of Device Classification Enabled Local Subscriber Policy Name Search or Select				
VLAN VLAN/VLAN Group 100 Multicast VLAN Enter Multicast VLAN				
Cancel		Update & Apply to Device		

Etiqueta WLAN

Paso 1: Vaya a Configuration > Tags & Profiles > WLANs y seleccione Add.

Paso 2: En la ficha General, configure el nombre del perfil, SSID, y establezca el estado en enabled.

Paso 3: Seleccione la ficha Security (Seguridad), Enable WAP+WPA2 (Activar WAP+WPA2) y configure una clave previamente compartida.



Nota: La configuración de SSID depende completamente de sus requisitos. En este ejemplo, se configura un SSID basado en PSK.

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

Etiqueta de política

Paso 1: Vaya a Configuración > Etiquetas y perfiles > Etiquetas > Ficha Directiva, haga clic en Agregar.

Paso 2: Cree una etiqueta de política definiendo un nombre y asociando el perfil de WLAN y el 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

Etiqueta del sitio

Paso 1: Navegue hasta Configuración > Etiquetas y perfiles > Etiquetas > Sitio y haga clic en Agregar.

Configuration ▾ > Tags & Profiles ▾ > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Paso 2: Configure el Nombre de Etiqueta, inhabilite la opción Enable Local Site y asocie tanto el AP Join Profile como el Flex Profile.

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

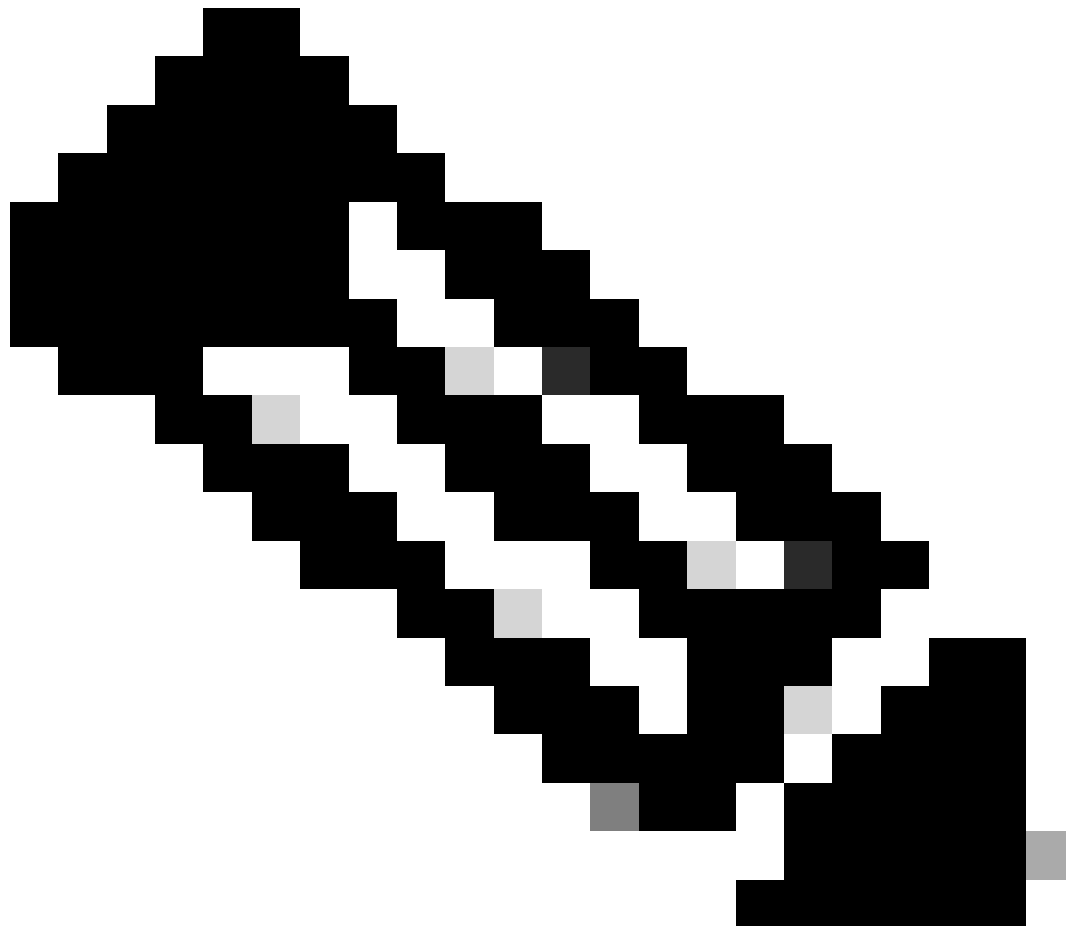
Update & Apply to Device

Configuración de puntos de acceso

En este caso práctico se supone que el punto de acceso (AP) se une primero al controlador de LAN inalámbrica (WLC) en modo local y, a continuación, se cambia al modo Flex+Bridge.

Paso 1: Navegue hasta Configuration > Wireless > Access Points y seleccione el AP.

Paso 2: Asigne las etiquetas Site Tag y Policy Tag a los puntos de acceso (AP).



Nota: El punto de acceso (AP) se reinicia, establece la conexión con el controlador en el modo Flex+Bridge y la ficha Mesh (Malla) está disponible.

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

Paso 3: En la pestaña Malla, seleccione el rol al que desea enraizar

Edit AP

General
Interfaces
High Availability
Inventory
Geolocation
Mesh
Advanced
Support Bundle

General		Ethernet Port Configuration	
Block Child	☐	ⓘ Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully	
Daisy Chaining	☐		
Daisy Chaining strict-RAP	☐		
Preferred Parent MAC	0000.0000.0000	Port	0
Role	Root	Mode	access
		VLAN ID*	0

Paso 4: Repita los pasos 1 y 2 para el punto de acceso (AP) designado para que funcione como un AP de malla para conectarlo en línea en el modo Flex+Bridge. Vaya a la pestaña Mesh y configure el rol como Mesh.

Paso 5: El punto de acceso de malla está conectado al switch en el puerto 0, configurado en el modo troncal, con la VLAN de AP establecida como VLAN nativa. Asegúrese de que las VLAN permitidas incluyan la VLAN del cliente especificada en el perfil Flex.

Paso 6: Haga clic en 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

Configuración del puerto del switch

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

Verificación

Asociación de AP de malla al AP raíz:

```
#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
```

Asociación del cliente en el AP de malla:

```
#show flexconnect client  
Flexconnect Clients:  
mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl 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 bstrt  
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

El tráfico del punto de acceso de malla (MAP) se enlaza directamente al switch de enlace ascendente, omitiendo el punto de acceso raíz (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

Acerca de esta traducción

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

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

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