

Mesh-APs für lokales Daten-Bridging im Flex- und Bridge-Modus konfigurieren

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdigramm](#)

[Hinzufügen des Access Points zur lokalen Controller-Datenbank](#)

[AAA-Methodenliste für die Authentifizierung](#)

[AAA-Methodenliste für Autorisierung](#)

[Mesh-Profil](#)

[AP-Teilnahmeprofil](#)

[Flex-Profil](#)

[Richtlinienprofil](#)

[WLAN-Tag](#)

[Richtlinien-Tag](#)

[Standort-Tag](#)

[Konfiguration von Access Points](#)

[Switch-Port-Konfiguration](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird die Konfiguration von MAPs im Flex- und Bridge-Modus für das lokale Client-Daten-Bridging unter Umgehung des RAP beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Catalyst Wireless 9800-Konfigurationsmodell
- Konfiguration von LAPs
- Steuerung und Bereitstellung von Wireless Access Points (CAPWAP)
- Konfiguration der Cisco Switches

Verwendete Komponenten

In diesem Beispiel werden Lightweight Access Points (9124AP-Modelle) verwendet, die entweder als Root Access Point (RAP) oder Mesh Access Point (MAP) konfiguriert werden können, um eine nahtlose Integration in den Catalyst 9800 Wireless LAN Controller (WLC) zu ermöglichen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

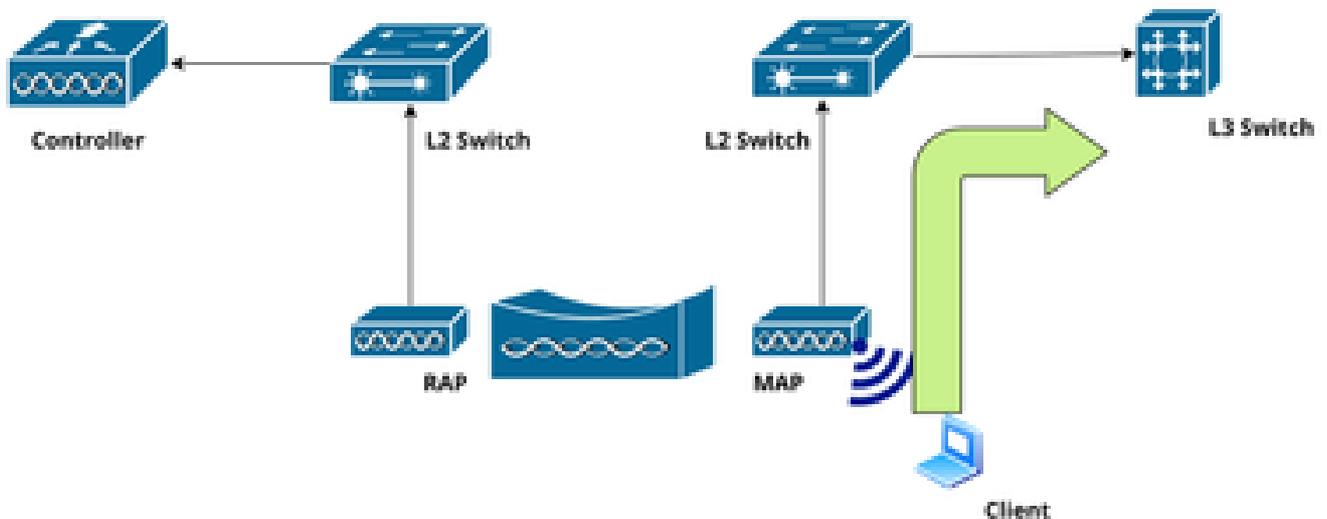
- C9800-L v17.12.5
- Cisco Catalyst 3850-Switch
- Cisco Catalyst Access Point der Serie 9124AX

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

In diesem Abschnitt wird die Konfiguration von Mesh Access Points (MAPs) beschrieben, die im Mesh + Bridge-Modus betrieben werden und es ermöglichen, lokale Client-Daten unter Umgehung des Root Access Point (RAP) direkt zum Uplink-Switch zu übertragen.

Netzwerkdiagramm



Hinzufügen des Access Points zur lokalen Controller-Datenbank

Schritt 1: Navigieren Sie zu Configuration > Security > AAA > AAA Advanced.

Cisco Catalyst 9800-L Wireless Controller
17.12.5
Welcome admin

Configuration > Security > AAA Show Me How

+ AAA Wizard

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

Global Config

RADIUS Fallback

Attribute List Name

MAC Address Serial Number

+ Add × Delete

Schritt 2: Wählen Sie Geräteauthentifizierung aus, und wählen Sie Hinzufügen aus.

Global Config

RADIUS Fallback

Attribute List Name

Device Authentication

MAC Address Serial Number

+ Add × Delete

MAC Address	Attribute Li
<input type="checkbox"/>	None

Schritt 3: Geben Sie die Base Ethernet MAC-Adresse des AP ein, der dem WLC beitreten soll. Belassen Sie die Attributlisten-Namensleiste, und wählen Sie Auf Gerät anwenden aus.

MAC Address*	<input type="text" value="3a5f1c8e729b"/>
Attribute List Name	<input type="text" value="None"/>
Description	<input type="text"/>
WLAN Profile Name	<input type="text" value="Select a value"/>

AAA-Methodenliste für die Authentifizierung

Schritt 1: Navigieren Sie zu Configuration > Security > AAA > AAA Method List > Authentication, und wählen Sie Add.

Configuration > Security > AAA

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

Authentication

Authorization

Phase 2: Definieren Sie den Namen der Methodenliste. Wählen Sie dot1x aus dem Dropdown-Menü Type* und local für den Gruppentyp aus. Wählen Sie Apply to Device (Auf Gerät anwenden), um die Konfiguration zu speichern.

Method List Name*

Type* ⓘ

Group Type ⓘ

Available Server Groups

- radius
- ldap
- tacacs+
- HTTSGROUP
- ISE_DD_Group
- ISE_HA
- Test

Assigned Server Groups

AAA-Methodenliste für Autorisierung

Schritt 1: Navigieren Sie zu Konfiguration > Sicherheit > AAA > AAA-Methodenliste > Autorisierung, und wählen Sie Hinzufügen aus.

+ AAA Wizard

Authentication

Authorization

Accounting

+ Add × Delete

	Name	Type
	default	exec

Phase 2: Definieren Sie den Namen der Methodenliste, wählen Sie Download der Anmeldeinformationen aus der Dropdown-Liste Typ* und lokal für den Gruppentyp aus. Klicken Sie auf Auf Gerät anwenden.

Method List Name*

Type* ⓘ

Group Type ⓘ

Authenticated

Available Server Groups

- radius
- ldap
- tacacs+
- HTTSGROUP
- ISE_DD_Group
- ISE_HA
- Test



Assigned Server Groups



Cancel

Update & Apply to Device

Mesh-Profil

Schritt 1: Navigieren Sie zu Configuration > Wireless > Mesh > Profiles (Konfiguration > Drahtlos > Mesh > Profile), und wählen Sie Add (Hinzufügen) aus.

Configuration ▾ > Wireless ▾ > Mesh

Global Config **Profiles**

+ Add

× Delete

Phase 2: Definieren Sie auf der Registerkarte Allgemein einen Namen und eine Beschreibung (optional) für das Mesh-Profil.

General Advanced

Name*

MESH-Profil

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▾

IDS (Rogue/Signature Detection)

Schritt 3: Legen Sie auf der Registerkarte Erweitert das Feld Methode auf EAP fest, und wählen Sie dann die zuvor erstellten Autorisierungs- und Authentifizierungsprofile aus den Dropdown-Menüs aus. Aktivieren Sie abschließend das Kontrollkästchen Ethernet Bridging, und wählen Sie Aktualisieren und anwenden aus.

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

AP-Teilnahmeprofil

Schritt 1: Navigieren Sie zu Configuration > Tag & Profiles > AP Join > Profile, und klicken Sie auf Add.

Configuration > **Tags & Profiles** > **AP Join**

+ Add

× Delete

Clone

AP Join Profile Name

Phase 2: Definieren Sie den Profilnamen und die Beschreibung (optional).

Name*

Mesh-AP-Join

Description

Enter Description

Country Code

IN



Time Zone

 Not Configured Use-Controller Delta from WLC

Schritt 3: Navigieren Sie zur Registerkarte AP, wählen Sie das Mesh Profile aus dem Dropdown-Menü Mesh Profile Name (Name des Mesh-Profiles) aus, legen Sie EAP-FAST für den EAP-Typ und CAPWAP DTLS für den AP-Autorisierungstyp fest, und klicken Sie auf Apply to Device (Auf Gerät anwenden).

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

Flex-Profil

Schritt 1: Konfiguration > Tags & Profile > Flex, und klicken Sie dann auf Hinzufügen.

Configuration > **Tags & Profiles** > **Flex**

Phase 2: Definieren Sie einen Namen für das Flex-Profil.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

Schritt 3: Navigieren Sie zur Registerkarte VLAN, und konfigurieren Sie den VLAN-Namen und die VLAN-ID für die lokale Überbrückung des Wireless-Client-Datenverkehrs, und klicken Sie auf Speichern.

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

+ Add

× Delete

VLAN Name	ID	Ingress ACL	Egress ACL
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

Richtlinienprofil

Schritt 1: Navigieren Sie zu Konfiguration > Tags und Profile > Richtlinie, und klicken Sie auf Hinzufügen.

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Clone

Admin
Status

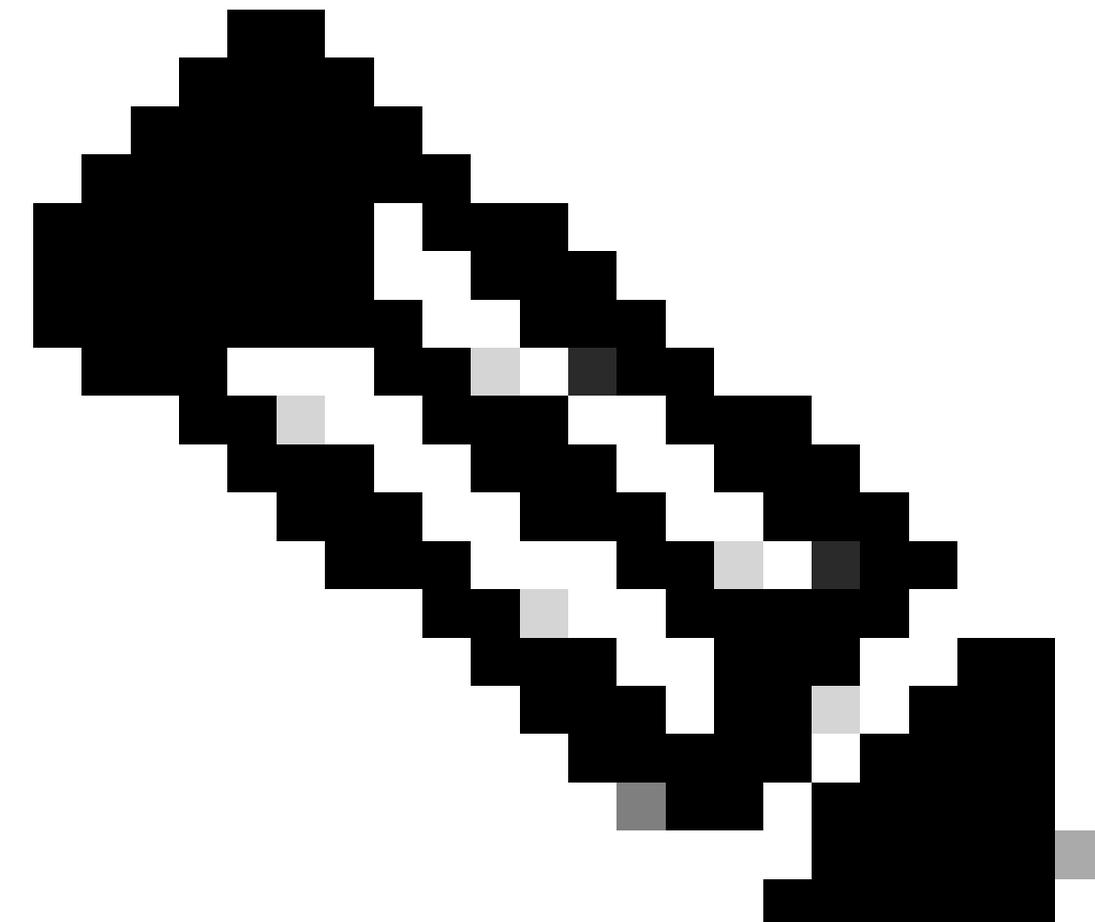


Associated
Policy Tags



Policy Profile Name

Phase 2: Definieren Sie auf der Registerkarte Allgemein den Profilnamen, setzen Sie Status auf Enabled (Aktiviert), und deaktivieren Sie die Funktion zum Umschalten über die Zentrale.



Anmerkung: Um das lokale Bridging des Client-Datenverkehrs zu aktivieren, muss die zentrale Switching-Funktion deaktiviert werden. Je nach SSID-Konfiguration können

weitere Optionen aktiviert oder deaktiviert werden.

General Access Policies QOS and AWC Mobility Advanced

Name*	<input type="text" value="Bridge-Policy"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input type="checkbox"/> DISABLED
Status	<input checked="" type="checkbox"/> ENABLED	Central Authentication	<input checked="" type="checkbox"/> ENABLED
Passive Client	<input type="checkbox"/> DISABLED	Central DHCP	<input type="checkbox"/> DISABLED
IP MAC Binding	<input checked="" type="checkbox"/> ENABLED	Flex NAT/PAT	<input type="checkbox"/> DISABLED
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED		
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SOACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

Schritt 3: Konfigurieren Sie die auf der Registerkarte "VLAN" des AP-Flex-Profiles angegebene VLAN-ID, und klicken Sie auf 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 ⓘ

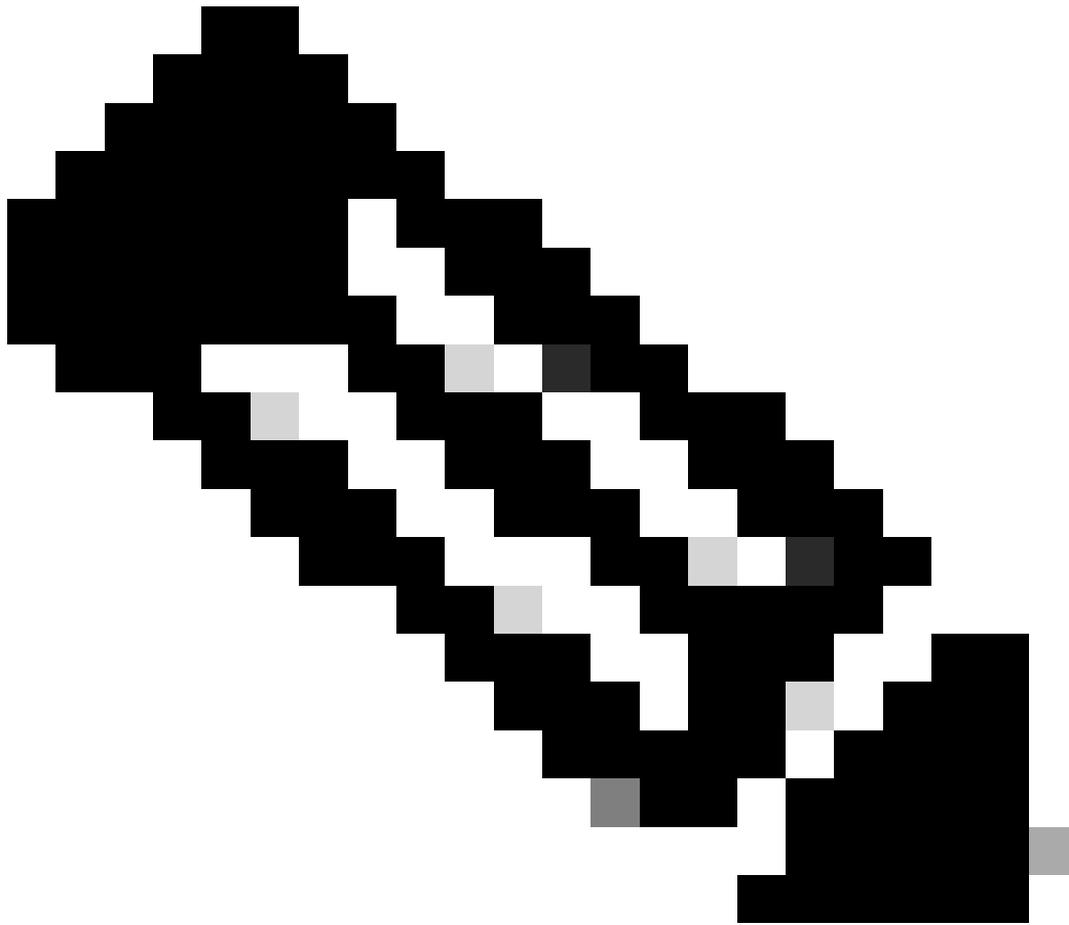
Post Auth ⓘ

WLAN-Tag

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profile > WLANs, und wählen Sie Hinzufügen aus.

Phase 2: Konfigurieren Sie auf der Registerkarte General (Allgemein) den Profilnamen, die SSID, und setzen Sie den Status auf enabled (Aktiviert).

Schritt 3: Wählen Sie die Registerkarte Sicherheit, aktivieren Sie WAP+WPA2, und konfigurieren Sie einen vorinstallierten Schlüssel.



Anmerkung: Die SSID-Konfiguration hängt vollständig von Ihren Anforderungen ab. In diesem Beispiel wird eine PSK-basierte SSID konfiguriert.

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

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

WPA2 Policy

GTK Randomize

OSCN Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Protected Management Frame

PMF

Disabled

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

Auth Key Mgmt

802.1X

PSK

Easy-PSK

CCKM

FT + 802.1X

FT + PSK

802.1X-
SHA256

PSK-SHA256

PSK Format

ASCII

PSK Type

AES

Pre-Shared Key*

Cancel

Update & Apply to Device

Richtlinien-Tag

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profiles > Tags > Policy (Registerkarte), und klicken Sie auf Add (Hinzufügen).

Schritt 2: Erstellen eines Policy Tags durch Definieren eines Namens und Zuordnen des WLAN- und Richtlinienprofils.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

➤ RLAN-POLICY Maps: 0

Standort-Tag

Schritt 1: Navigieren Sie zu Configuration > Tags & Profiles > Tags > Site, und klicken Sie auf Add (Hinzufügen).

Configuration > Tags & Profiles > Tags

Policy

Site

RF

AP

+ Add

× Delete

Clone

Schritt 2: Konfigurieren Sie den Tag-Namen, deaktivieren Sie die Option "Lokalen Standort aktivieren", und ordnen Sie dem AP-Join-Profil und dem Flex-Profil zu.

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

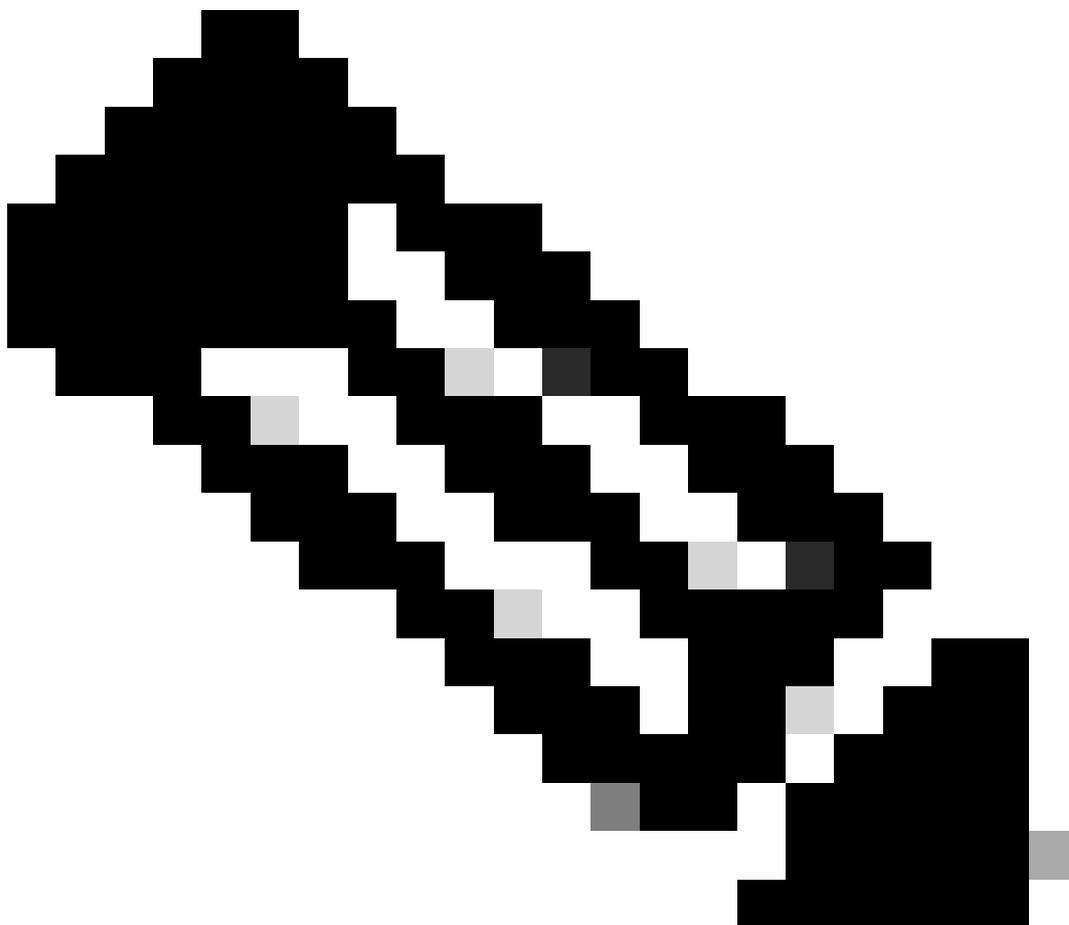
Update & Apply to Device

Konfiguration von Access Points

In dieser Fallstudie wird davon ausgegangen, dass der Access Point (AP) zuerst im lokalen Modus mit dem Wireless LAN Controller (WLC) verbunden und dann in den Flex+Bridge-Modus überführt wird.

Schritt 1: Navigieren Sie zu Configuration > Wireless > Access Points, und wählen Sie den Access Point aus.

Phase 2: Weisen Sie den Access Points (APs) die Site-Tag-Nummer und die Policy-Tag-Nummer zu.



Anmerkung: Der Access Point (AP) wird neu gestartet, im Flex+Bridge-Modus wird die Verbindung mit dem Controller hergestellt, und die Registerkarte "Mesh" ist verfügbar.

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

Schritt 3: Wählen Sie auf der Registerkarte Mesh (Netz) die Rolle aus, die verwurzelt werden soll

Edit AP

General	Interfaces	High Availability	Inventory	Geolocation	Mesh	Advanced	Support Bundle
General				Ethernet Port Configuration			
Block Child	<input type="checkbox"/>	<p>ⓘ Ethernet Bridging on the associated Mesh Profile should be enabled to configure this section successfully</p>					
Daisy Chaining	<input type="checkbox"/>						
Daisy Chaining strict-RAP	<input type="checkbox"/>						
Preferred Parent MAC	0000.0000.0000						
Role	Root <input type="text"/>						
		Port	0 <input type="text"/>				
		Mode	access <input type="text"/>				
		VLAN ID*	0 <input type="text"/>				

Schritt 4: Wiederholen Sie die Schritte 1 und 2 für den Access Point, der als Mesh-AP konfiguriert wurde, um ihn im Flex+Bridge-Modus online zu schalten. Navigieren Sie zur Registerkarte Mesh, und konfigurieren Sie die Rolle als Mesh.

Schritt 5: Der Mesh Access Point ist mit dem Switch auf Port 0 verbunden, der im Trunk-Modus konfiguriert wurde, wobei das VLAN der APs als natives VLAN festgelegt ist. Stellen Sie sicher, dass die zulässigen VLANs das im Flex-Profil angegebene Client-VLAN enthalten.

Schritt 6: Klicken Sie auf Aktualisieren und anwenden.

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

Switch-Port-Konfiguration

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

Überprüfung

Verknüpfung von Mesh-AP und Root-AP:

```
#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
```

Clientzuordnung auf dem Mesh-AP:

```
#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
```

Der Datenverkehr vom Mesh Access Point (MAP) wird unter Umgehung des Root Access Point (RAP) direkt zum Uplink-Switch geleitet:

```
<#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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.