

FlexおよびブリッジモードでのローカルデータブリッジングのためのメッシュAPの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[コントローラのローカルデータベースへのアクセスポイントの追加](#)

[認証のAAA方式リスト](#)

[許可のためのAAA方式リスト](#)

[メッシュプロファイル](#)

[AP Join プロファイル](#)

[Flex プロファイル](#)

[ポリシー プロファイル](#)

[WLANタグ](#)

[ポリシー タグ](#)

[サイト タグ](#)

[アクセスポイントの設定](#)

[スイッチポートの設定](#)

[確認](#)

はじめに

このドキュメントでは、RAPをバイパスするローカルクライアントデータブリッジングのFlexおよびブリッジモードでのMAPの設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Catalyst Wireless 9800設定モデル
- LAPの設定
- Control And Provision of Wireless Access Points(CAPWAP)
- Ciscoスイッチの設定

使用するコンポーネント

この例では、Lightweightアクセスポイント (9124APモデル) を使用しています。このアクセスポイントは、ルートアクセスポイント(RAP)またはメッシュアクセスポイント(MAP)として設定でき、Catalyst 9800ワイヤレスLANコントローラ(WLC)とシームレスに統合できます。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

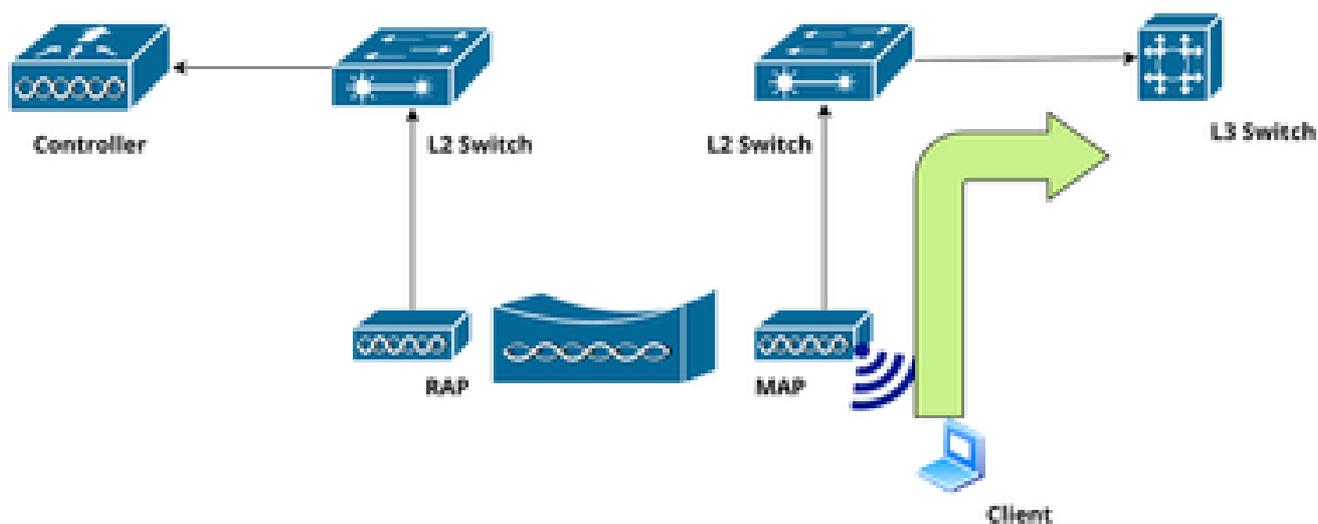
- C9800-L v17.12.5
- Cisco Catalyst 3850 スイッチ
- Cisco Catalyst 9124AXシリーズアクセスポイント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

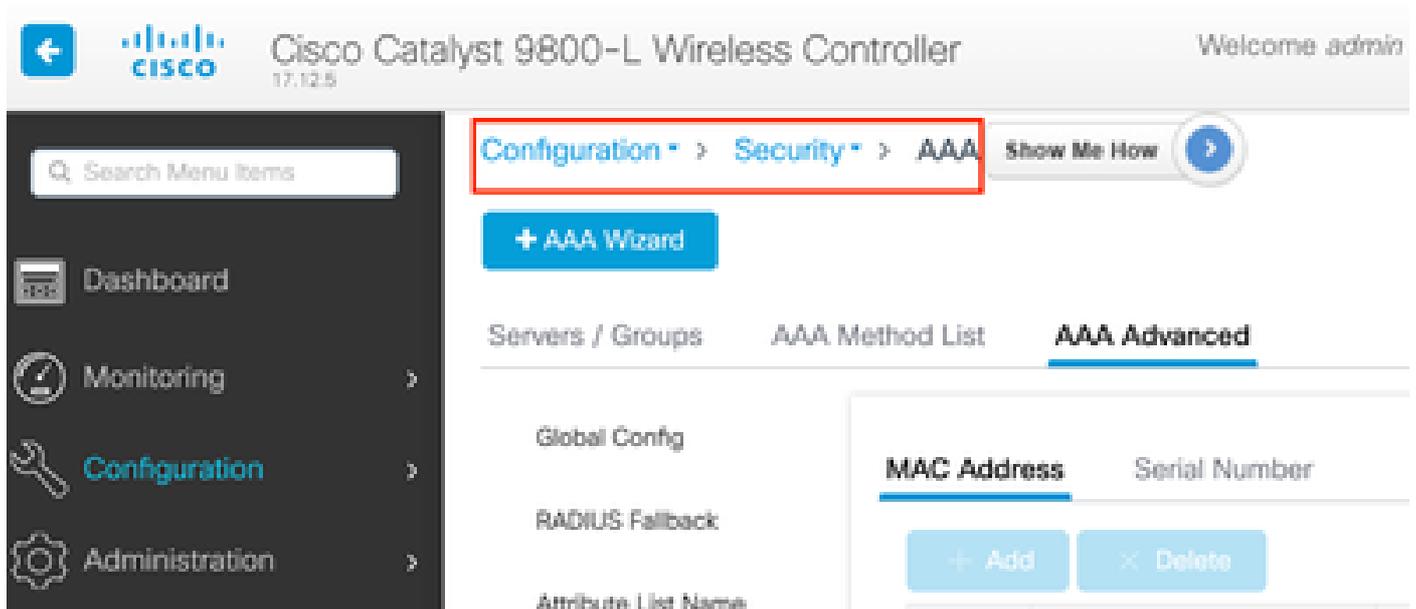
このセクションでは、メッシュ+ブリッジモードで動作するメッシュアクセスポイント(MAP)の設定の概要を説明します。これにより、ローカルクライアントデータを、ルートアクセスポイント (RAP)をバイパスして、アップリンクスイッチに直接ブリッジできます。

ネットワーク図

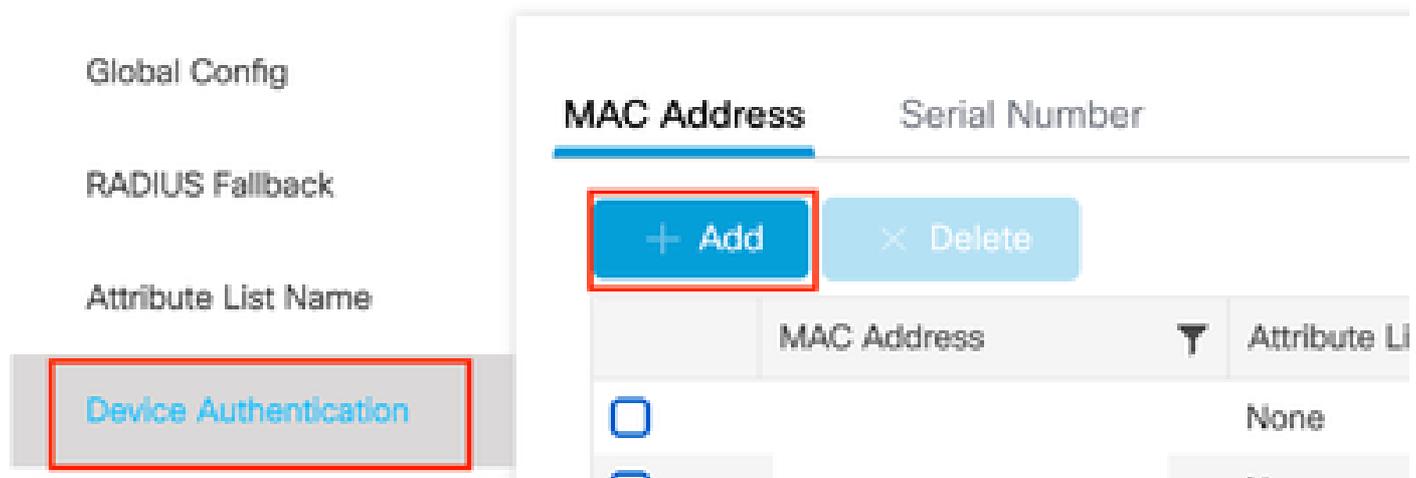


コントローラのローカルデータベースへのアクセスポイントの追加

ステップ1: Configuration > Security > AAA > AAA Advancedの順に移動します。



ステップ2: SelectDevice Authentication and selectAddを選択します。



ステップ3: WLCに加入するAPのベースイーサネットMACアドレスを入力します。属性リストの名前は空白のままにして、Apply to Deviceを選択します。

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"/>

認証のAAA方式リスト

ステップ1: Configuration > Security > AAA > AAA Method List > Authenticationの順に移動し、Addを選択します。

Configuration > Security > AAA

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

Authentication

Authorization

ステップ2: メソッドリスト名を定義します。Type* ドロップダウンからdot1xを選択し、Group Typeにはlocalを選択します。Apply to Deviceを選択して、設定を保存します。

Method List Name*

Type* ⓘ

Group Type ⓘ

Available Server Groups

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

Assigned Server Groups

許可のためのAAA方式リスト

ステップ1: Configuration > Security > AAA > AAA Method List > Authorization の順に移動し、Addを選択します。

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

	Name	Type
	default	exec

ステップ2：方式リスト名を定義し、Type*ドロップダウンからcredential downloadを選択し、Group Typeにはlocalを選択します。Apply to Deviceをクリックします。

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

メッシュプロファイル

ステップ1: Configuration > Wireless > Mesh > Profilesの順に移動し、Addを選択します。

Configuration ▾ > Wireless ▾ > Mesh

Global Config Profiles

+ Add

× Delete

ステップ2:Generalタブで、メッシュプロファイルの名前と説明（オプション）を定義します。

General Advanced

Name*

MESH-Profile

Description

Enter Description

Range (Root AP to Mesh AP)

12000

Multicast Mode

In-Out ▼

IDS (Rogue/Signature Detection)

ステップ3:Advancedタブで、MethodフィールドをEAPに設定し、ドロップダウンメニューから以前に作成したAuthorizationおよびAuthenticationプロファイルを選択します。最後に、Ethernet Bridgingチェックボックスを有効にして、Update and applyを選択します。

General

Advanced

Security

Method

EAP

Authentication Method

MESH

Authorization Method

MESH-Authorizati...

Ethernet Bridging

VLAN Transparent

Ethernet Bridging

AP Join プロファイル

ステップ1: Configuration > Tag & Profiles > AP Join > Profileの順に移動し、Addをクリックします。

Configuration > Tags & Profiles > AP Join

+ Add

× Delete

Clone

AP Join Profile Name

ステップ2: プロファイル名と説明を定義します (オプション)。

Name*

Mesh-AP-Join

Description

Enter Description

Country Code

IN



Time Zone



Not Configured



Use-Controller



Delta from WLC

ステップ3:APタブに移動し、Mesh Profile NameドロップダウンからMesh Profileを選択し、EAP TypeにEAP-FASTを、AP Authorization TypeにCAPWAP DTLSを設定して、Apply to Deviceをクリックします。

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

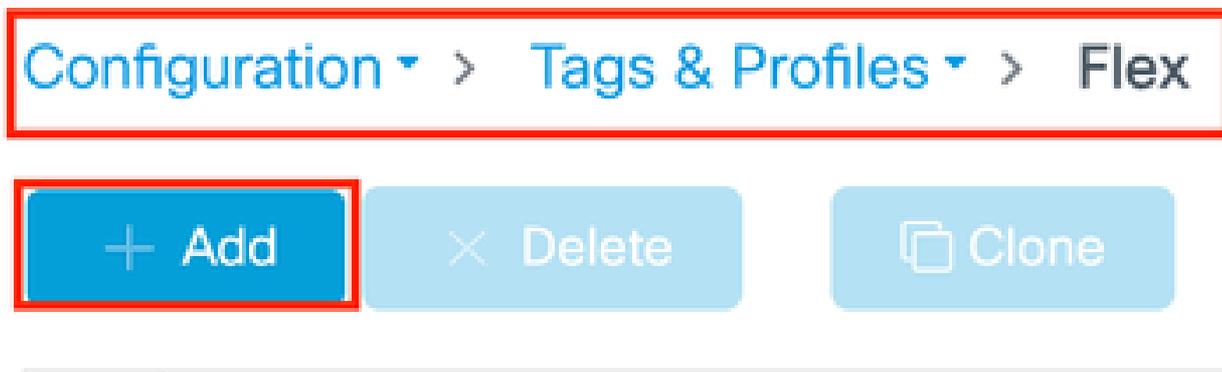
Enable

Mesh

Profile Name MESH-Profile ▾ [Cancel](#)

Flex プロファイル

ステップ1: Configuration > Tags & Profiles > Flexの順に選択し、Addをクリックします。



ステップ2: Flexプロファイルの名前を定義します。

General

Local Authentication

Policy ACL

VLAN

DNS Layer Security

Name*

Mesh-Flex

Fallback Radio Shut

Description

Enter Description

Flex Resilient

ステップ3:vlanタブに移動し、無線クライアントトラフィックのローカルブリッジのVLAN名とVLAN IDを設定し、Saveをクリックします。

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

ポリシー プロファイル

ステップ1:Configuration > Tags & Profiles > Policyの順に移動し、Addをクリックします。

Configuration > Tags & Profiles > Policy

+ Add

× Delete

Clone

Admin
Status



Associated
Policy Tags



Policy Profile Name

ステップ2:Generalタブで、プロファイル名を定義し、StatusをEnabledに設定し、Disable Central Switchingを設定します。

注：クライアントトラフィックのローカルブリッジングを有効にするには、中央スイッチングを無効にする必要があります。SSID設定に基づいて、必要に応じて他のオプション

ンを有効または無効にできません。

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"/>

ステップ3:AP Flex ProfileのVLANタブで指定されたVLANIDを設定し、Update & Applyをクリックします。

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 ⓘ

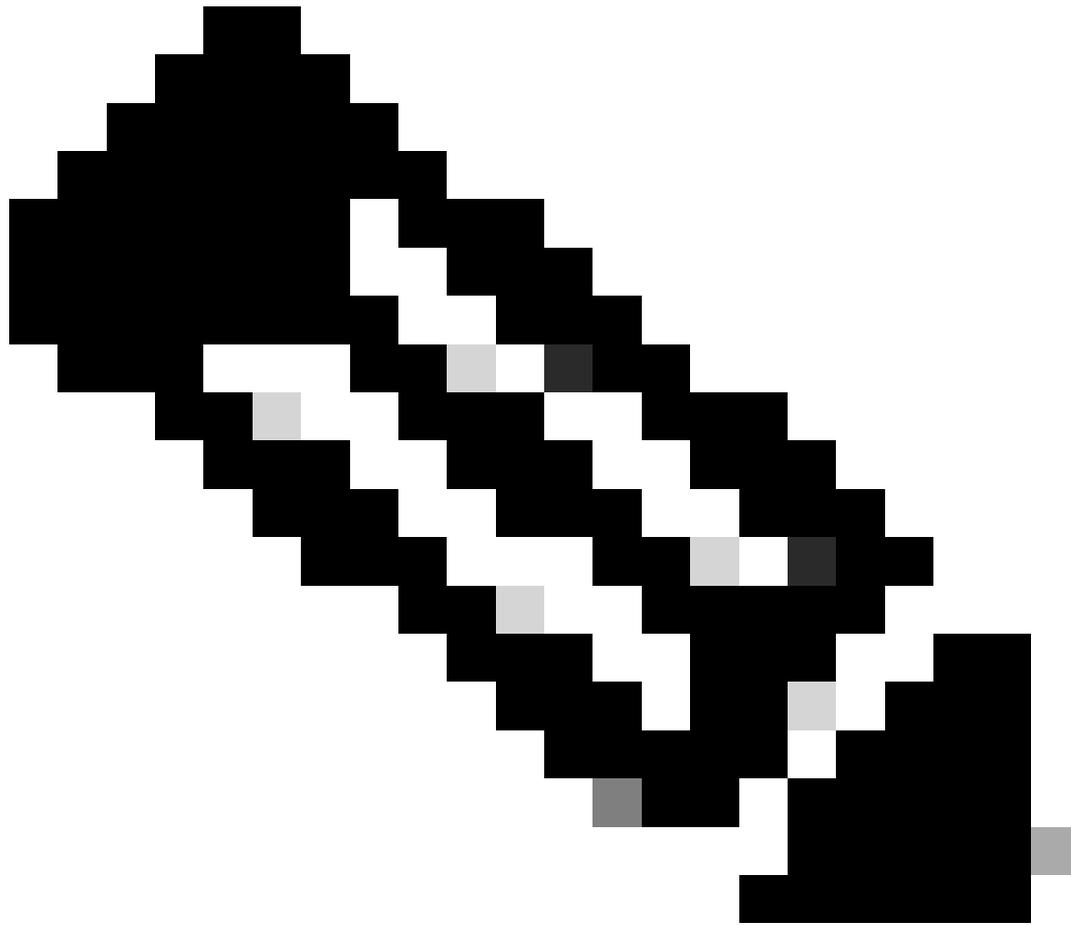
Post Auth ⓘ

WLANタグ

ステップ1: Configuration > Tags & Profiles > WLANsの順に移動し、Addを選択します。

ステップ2: Generalタブで、Profile nameとSSIDを設定し、ステータスをenabledに設定します。

ステップ3: Securityタブを選択し、WAP+WPA2を有効にして、事前共有キーを設定します。



注:SSID設定は、要件によって完全に異なります。この例では、PSKベースのSSIDが設定されます。

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 NoneMAC 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 OAKM FT + 802.1X FT + PSK 802.1X-
SHA256 PSK-SHA256

PSK Format

ASCII

PSK Type

AES

Pre-Shared Key*

.....

Cancel

Update & Apply to Device

ポリシー タグ

ステップ1: Configuration > Tags & Profiles > Tags > Policyタブの順に移動し、Addをクリックします。

ステップ2: 名前を定義し、WLANとポリシープロファイルを関連付けることによって、ポリシータグを作成します。

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*

> WLAN-POLICY Maps: 0

サイト タグ

ステップ1: Configuration > Tags & Profiles > Tags > Siteの順に移動し、Addをクリックします。

Configuration ▾ > Tags & Profiles ▾ > Tags

Policy RF AP

ステップ2：タグNameを設定し、Enable Local Siteオプションを無効にして、AP Join ProfileとFlex Profileの両方を関連付けます。

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

アクセスポイントの設定

このケーススタディでは、アクセスポイント(AP)が最初にローカルモードでワイヤレスLANコントローラ(WLC)に加入し、次にFlex+ブリッジモードに移行することを前提としています。

ステップ1: Configuration > Wireless > Access Pointsの順に移動し、APを選択します。

ステップ2: Site TagとPolicy Tagをアクセスポイント(AP)に割り当てます。

注：アクセスポイント(AP)がリブートし、Flex+Bridgeモードでコントローラとの接続を確立すると、[メッシュ]タブが使用可能になります。

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	Policy	Mesh-Policy-Tag 
Ethernet MAC	34b8.8314.a204	Site	Mesh-Site-Tag 
Admin Status	ENABLED 		

ステップ3: Meshタブで、Rootにするロールを選択します。

Edit AP

General Interfaces High Availability Inventory Geolocation **Mesh** Advanced Support Bundle

General

Block Child

Daisy Chaining

Daisy Chaining strict-RAP

Preferred Parent MAC

Role

Ethernet Port Configuration

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

Port

Mode

VLAN ID*

ステップ4：メッシュAPとして機能するように指定されたアクセスポイント(AP)でステップ1と2を繰り返し、Flex+ブリッジモードでオンラインにします。Meshタブに移動し、ロールをMeshに設定します。

ステップ5：メッシュアクセスポイントは、トランクモードに設定されているポート0のスイッチに接続されており、AP VLANはネイティブVLANとして設定されています。許可されるVLANに、Flexプロファイルで指定されたクライアントVLANが含まれていることを確認します。

ステップ6:Update and Applyをクリックします。

General Interfaces High Availability Inventory Geolocation **Mesh** Advanced Support Bundle

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

スイッチポートの設定

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

確認

ルートAPへのメッシュAPの関連付け：

```
#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
```

メッシュAPでのクライアント関連付け：

```
#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 avgrtdtds bstdtds bstrtdtds avgdtus avgrtdtus bstdtus bstrtdtus
52:95:C7:EE:B7:E5 none none none none Bridge-VLAN 0 0 0 0 0 0 0 0
```

メッシュアクセスポイント(MAP)からのトラフィックは、ルートアクセスポイント(RAP)をバイパスして、アップリンクスイッチに直接ブリッジされます。

<#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: 1748579
```

```
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 resp

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。