



メッシュ アクセス ポイント

-
- [メッシュの概要 \(2 ページ\)](#)
- [制約事項と制限 \(3 ページ\)](#)
- [メッシュ展開 \(3 ページ\)](#)
- [MAC 認証 \(4 ページ\)](#)
- [事前共有キーのプロビジョニング \(7 ページ\)](#)
- [EAP 認証 \(9 ページ\)](#)
- [ブリッジグループ名 \(10 ページ\)](#)
- [2.4 GHz および 5 GHz のメッシュバックホール \(12 ページ\)](#)
- [Dynamic Frequency Selection \(動的周波数選択\) \(13 ページ\)](#)
- [国コード \(14 ページ\)](#)
- [侵入検知システム \(15 ページ\)](#)
- [コントローラ間のメッシュ相互運用性 \(16 ページ\)](#)
- [メッシュ コンバージェンス \(16 ページ\)](#)
- [イーサネットブリッジング \(17 ページ\)](#)
- [メッシュ デイジー チェーン接続 \(20 ページ\)](#)
- [メッシュ イーサネットブリッジング ネットワーク経由のマルチキャスト \(22 ページ\)](#)
- [メッシュでの無線リソース管理 \(24 ページ\)](#)
- [メッシュ リーフ ノード \(25 ページ\)](#)
- [フレックス+ブリッジモード \(26 ページ\)](#)
- [バックホールクライアントアクセス \(27 ページ\)](#)
- [アクセスポイントごとのメッシュバックホールでの Dot11ax レートの設定 \(GUI\) \(28 ページ\)](#)
- [メッシュプロファイルのメッシュバックホールでの Dot11ax レートの設定 \(GUI\) \(29 ページ\)](#)
- [AP ごとのデータレートの設定 \(CLI\) \(30 ページ\)](#)
- [メッシュプロファイルを使用したデータレートの設定 \(CLI\) \(30 ページ\)](#)
- [ルート AP のバックホールスロットの指定 \(GUI\) \(31 ページ\)](#)
- [ルート AP のバックホールスロットの指定 \(CLI\) \(31 ページ\)](#)

- [ワイヤレスバックホールのデータレートの設定 \(CLI\) \(31 ページ\)](#)
- [メッシュバックホールでのリンクテストの使用 \(GUI\) \(32 ページ\)](#)
- [メッシュバックホールでのリンクテストの使用 \(33 ページ\)](#)
- [メッシュ CAC \(33 ページ\)](#)
- [アップリンクゲートウェイの到達可能性障害の高速検出によるメッシュネットワークの回復の高速化 \(34 ページ\)](#)
- [サブセットチャネル同期の設定 \(35 ページ\)](#)
- [優先される親の選択 \(GUI\) \(36 ページ\)](#)
- [優先される親の選択 \(CLI\) \(36 ページ\)](#)
- [AP のロールの変更 \(GUI\) \(37 ページ\)](#)
- [AP のロールの変更 \(CLI\) \(38 ページ\)](#)
- [メッシュ AP のバッテリー状態の設定 \(GUI\) \(38 ページ\)](#)
- [メッシュ AP のバッテリー状態の設定 \(38 ページ\)](#)
- [組み込みワイヤレスコントローラでのメッシュ設定の確認 \(39 ページ\)](#)

メッシュの概要

Cisco IOS XE 17.6.1 リリースでは、Cisco 組み込みワイヤレスコントローラ (EWC) は Cisco Catalyst 9124AX シリーズの屋外アクセスポイントで実行され、メッシュ展開でルートアクセスポイント (RAP) として機能します。メッシュネットワークでは、Cisco Aironet の屋外メッシュアクセスポイントと Cisco 組み込みワイヤレスコントローラを組み合わせ、拡張性、集中管理、および展開間のモビリティが提供されます。Control and Provisioning of Wireless Access Points (CAPWAP) プロトコルは、ネットワークへのメッシュアクセスポイントの接続を管理します。

メッシュネットワーク内のアクセスポイントは、次のいずれかの方法で動作します。

- ルートアクセスポイント (RAP)
- メッシュアクセスポイント (MAP)

EWC は RAP で機能します。RAP はコントローラに有線接続され、MAP はコントローラにワイヤレス接続されます。メッシュ AP は、802.11a/n 無線バックホール経由のワイヤレス接続を使用して、親メッシュ AP および子メッシュ AP と通信します。MAP では Cisco Adaptive Wireless Path Protocol (AWPP) を使用して、他のメッシュアクセスポイントを介したコントローラへの最適なパスを決定します。メッシュアクセスポイントでは、CAPWAP ディスカバリを開始する前にすでにコントローラに接続されている親メッシュ AP との AWPP リンクが確立されません。

ワイヤレスメッシュは、有線ネットワークの 2 地点で終了します。1 つ目はルートアクセスポイント (RAP) が有線ネットワークに接続される場所です。すべてのブリッジトラフィックがその場所で有線ネットワークに接続されます。2 つ目は CAPWAP コントローラが有線ネットワークに接続する場所です。ここでは、メッシュネットワークからの WLAN クライアントトラフィックが有線ネットワークに接続されます。CAPWAP からの WLAN クライアントトラフィックは、レイヤ 2 にトンネリングされます。一致する WLAN は、ワイヤレスコントローラ

ラが同じ場所に設置されている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、ワイヤレス コントローラが接続されているネットワークのセキュリティ機能によって異なります。

メッシュ ネットワーク内のエンドツーエンドのセキュリティは、ワイヤレス メッシュ アクセスポイントと Wi-Fi Protected Access 2 (WPA2) クライアントの間で Advanced Encryption Standard (AES) の暗号化を採用することでサポートされています。メッシュアクセスポイント (MAP) ワイヤレス クライアントへの接続 (MAP 同士や MAP とルート アクセス ポイントなど) では、WPA2 が適用されます。

新しい設定モデルでは、コントローラにデフォルトのメッシュプロファイルがあります。このプロファイルは、デフォルトの AP 接続プロファイルにマッピングされた後、デフォルトのサイトタグにマッピングされます。名前付きメッシュプロファイルを作成する場合は、これらのマッピングが行われていること、および該当する AP が対応するサイトタグに追加されていることを確認します。



(注) メッシュプロファイルのセキュリティモード、BGN、クライアントアクセス、および範囲の変更に関する設定を変更すると、メッシュ AP がリロードされます。EWC では、内部 AP をアクティブな EWC に自動的にリロードすることはできません。リロード後にスタンバイ EWC ノードが動作し始めてから、内部 AP を手動でリロードする必要があります。

スケール番号

Cisco Catalyst 9124 シリーズ屋外アクセスポイントは、100 の AP と 2000 のクライアントの規模をサポートします。

制約事項と制限

- メッシュ機能は、Cisco 組み込みワイヤレスコントローラの Cisco Catalyst 9124 シリーズアクセスポイントでのみサポートされています。
- EWC は、同じコントローラ内の親メッシュ AP 間の AP ローミングのみをサポートしません。
- EWC メッシュトポロジでは、ワイヤレスネットワークを拡張するために MAP の子として展開する場合、すべての FlexConnect EWC 対応 AP を CAPWAP モードにする必要があります。AP が CAPWAP モードではない場合、コントローラが生成されます。

メッシュ展開

メッシュ展開は次のとおりです。

- **[Wireless Bridging]** : ワイヤレスブリッジングは、ポイントツーポイントまたはポイントツーマルチポイントにすることができます。ワイヤレスブリッジにより、ケーブルが利用できない場合にネットワークが無線で拡張されます。RAP と MAP 間の無線リンクは、パンプとして扱われます。このタイプの展開では、通常、RAP と 1 レベルの MAP を使用します。MAP の第 1 レベルの下に子 MAP はありません。SSID は展開されません。
 - **[Point-to-Point Wireless Bridging]** : ポイントツーポイントブリッジングシナリオでは、バックホール無線を使用してスイッチドネットワークの 2 つのセグメントをブリッジ接続することにより、Cisco Catalyst 9124 シリーズ メッシュ AP を使用してリモートネットワークを拡張できます。これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイントネットワークと同様に、イーサネットブリッジングを有効にすることでクライアントアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。
 - **[Point-to-Multipoint]** : ポイントツーマルチポイントブリッジングシナリオでは、ルートブリッジとして機能する RAP が、アソシエートされた有線 LAN を使用して複数の MAP を非ルートブリッジとして接続します。デフォルトでは、この機能はすべての MAP に対して無効になっています。イーサネットブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネットブリッジングをイネーブルにする必要があります。
- **[Mesh with Wi-Fi Clients]** : Wi-Fi ネットワークを拡張するための、マルチレベル MAP とワイヤレスクライアントを使用したメッシュ展開。Cisco のワイヤレス屋外メッシュ ネットワークでは、複数のメッシュ アクセス ポイントによって、安全でスケーラブルな屋外ワイヤレス LAN を提供するネットワークが構成されます。

MAC 認証

MAP をコントローラに接続させるには、AP の MAC アドレスをコントローラに入力する必要があります。コントローラは、認証リストで使用可能な MAP からの CAPWAP 要求にのみ応答します。AP の背面に記載されている MAC アドレスを必ず使用してください。

イーサネット経由でコントローラに接続された MAP の MAC 認証は、CAPWAP 接続プロセス中に行われます。無線でコントローラに接続する MAP の場合、対応する AP が親 MAP との Adaptive Wireless Path Protocol (AWPP) リンクを保護しようとする、MAC 認証が行われます。AWPP は、Cisco メッシュネットワークで使用されるプロトコルです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、内部での MAC 認証と、外部 AAA サーバーを使用した認証をサポートしています。

MAC 認証の設定 (GUI)

手順

-
- ステップ 1 [Configuration] > [Security] > [AAA] > [AAA Advanced] > [Device Authentication] を選択します。
- ステップ 2 [Add] をクリックします。
[Quick Step: MAC Filtering] ウィンドウが表示されます。
- ステップ 3 [Quick Step: MAC Filtering] ウィンドウで、次の手順を実行します。
- [MAC Address] を入力します。MAC アドレスは、xx:xx:xx:xx:xx:xx、xx-xx-xx-xx-xx-xx、または xxxx.xxxx.xxxx のいずれかの形式で指定できます。
 - ドロップダウンリストから [Attribute List Name] を選択します。
 - ドロップダウンリストから [WLAN Profile Name] を選択します。
 - [Apply to Device] をクリックします。
- ステップ 4 [Configuration] > [Security] > [AAA] > [AAA Method List] > [Authorization] を選択します。
- ステップ 5 [Add] をクリックします。
[Quick Step: AAA Authorization] ウィンドウが表示されます。
- ステップ 6 [Quick Step: AAA Authorization] ウィンドウで、次の手順を実行します。
- [Method List Name] を入力します。
 - ドロップダウンリストから [Type] を選択します。
 - ドロップダウンリストから [Group Type] を選択します。
 - [Fallback to Local] チェックボックスをオンにします。
 - [Authenticated] チェックボックスをオンにします。
 - 必要なサーバーを [Available Server Groups] から [Assigned Server Groups] に移動します。
 - [Apply to Device] をクリックします。
- ステップ 7 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
- ステップ 8 メッシュプロファイルをクリックします。
[Edit Mesh Profile] ウィンドウが表示されます。
- ステップ 9 [Advanced] タブをクリックします。
- ステップ 10 [Security] 設定の [Method] ドロップダウンリストから、[EAP] を選択します。
- ステップ 11 ドロップダウンリストから [Authentication Method] を選択します。
- ステップ 12 ドロップダウンリストから [Authorization Method] を選択します。
- ステップ 13 [Update & Apply to Device] をクリックします。
-

MAC 認証の設定 (CLI)

ブリッジモード AP の MAC アドレスをコントローラに追加するには、次の手順に従います。

始める前に

- コントローラでは、ブリッジモード AP の MAC フィルタリングがデフォルトで有効になっています。したがって、設定する必要があるのは MAC アドレスだけです。使用する MAC アドレスは、該当する AP の背面に記載されています。
- MAC 認証は内部での認証と、外部 AAA サーバーを使用した認証がサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	username user-name 例： Device(config)# username username1	ユーザー名が MAC アドレスである MAC フィルタリングのユーザー名認証を設定します。
ステップ 3	aaa authorization credential-download method-name local 例： Device(config)# aaa authorization credential-download list1 local	ローカルログイン情報を使用するための認可方式リストを設定します。
ステップ 4	aaa authorization credential-download method-name radius group server-group-name 例： Device(config)# aaa authorization credential-download auth1 radius group radius-server-1	RADIUS サーバーグループを使用するための認可方式リストを設定します。
ステップ 5	wireless profile mesh profile-name 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 6	method authorization method-name 例： Device(config-wireless-mesh-profile)# method authorization auth1	メッシュ AP 認証の認証方式を設定します。

事前共有キーのプロビジョニング

メッシュ展開では、MAPがネットワークから移動して別のメッシュネットワークに接続することがあります。これは、両方のメッシュ展開がワイルドカードのMACフィルタリングでAAAを使用してMAPのアソシエーションを許可する場合に発生します。MAPはEAP-FASTを使用する可能性があるため、この動作を制御することはできません。EAPセキュリティにAPのMACアドレスとタイプの組み合わせが使用されて、制御設定を使用できないためです。デフォルトのパスフレーズを使用した事前共有キー（PSK）オプションには、セキュリティリスクも存在します。

この問題は、MAPが移動車両（公共交通機関、フェリー、船など）で使用される場合に、2つのサービスプロバイダのオーバーラップ導入環境で顕著に現れます。この場合、サービスプロバイダのメッシュネットワークに残るMAPに制限はなく、MAPがハイジャックされたり、別のサービスプロバイダのネットワークで使用されたりして、導入環境で本来のサービスプロバイダの対象顧客にサービスを提供できなくなる可能性があります。

PSKキープロビジョニング機能を使用すると、コントローラからプロビジョニング可能なPSK機能が有効になります。これにより、メッシュ展開の制御が容易になり、デフォルトよりもMAPセキュリティが強化されます。この機能によってカスタムPSKが設定されたMAPは、PSKキーを使用してRAPおよびコントローラで認証を行います。

PSK プロビジョニングの設定（GUI）

PSK プロビジョニングを設定するには、次の手順に従います。

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] を選択します。

ステップ 2 [Global Config] タブをクリックします。

ステップ 3 [Security] の設定で、[PSK Provisioning] チェックボックスをオンにして、次の手順を実行します。

- a) ドロップダウンリストの番号から [PSK Inuse Index] を選択します。
- b) [Keys Configuration] の設定で、追加アイコン [+] をクリックしてキーを設定します。
- c) ドロップダウンリストから [Key] を選択します。
- d) 設定するキーの [Name] と [Description] を入力します。
- e) [Password Type] として [UNENCRYPTED] または [AES Encrypted] を選択します。
- f) [Apply] をクリックします。キーは、設定されたキーのリストに表示されます。

ステップ 4 [Default PSK] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックします。

PSK プロビジョニングの設定 (CLI)

PSK プロビジョニングが有効になっている場合、AP は最初にデフォルト PSK を使用して接続します。PSK プロビジョニング キーが設定された後は、新しく接続した AP に設定済みのキーがプッシュされます。

PSK を設定するには、以下の手順に従います。

始める前に

プロビジョニングされた PSK は、メッシュセキュリティとして PSK が設定されているすべての AP にプッシュされている必要があります。



- (注)
- PSK は、コントローラおよび対応するメッシュ AP のリブート後も保存されます。
 - コントローラは、合計 5 つの PSK と 1 つのデフォルト PSK を保持できます。
 - メッシュ AP は、初期設定へのリセット時にのみプロビジョニング済み PSK を削除します。
 - メッシュ AP は、最初のプロビジョニング済み PSK を受信した後はデフォルトの PSK を使用しません。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless mesh security psk provisioning 例： Device(config)# wireless mesh security psk provisioning	ワイヤレスのセキュリティ方式を PSK として設定します。 (注) プロビジョニングされた PSK は、メッシュセキュリティ方式として PSK が設定されている AP にのみプッシュされます。
ステップ 3	wireless mesh security psk provisioning key index {0 8} pre-shared-key description 例： Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key	メッシュ AP の新しい PSK を設定します。

	コマンドまたはアクション	目的
ステップ 4	wireless mesh security psk provisioning default-psk 例 : <pre>Device(config)# wireless mesh security psk provisioning default-psk</pre>	デフォルトの PSK ベースの認証を有効にします。
ステップ 5	wireless mesh security psk provisioning inuse index 例 : <pre>Device(config)# wireless mesh security psk provisioning inuse 1</pre>	アクティブに使用する PSK を指定します。 (注) PSK インデックスを指すグローバル設定で、使用中のキー インデックスを明示的に設定する必要があります。

EAP 認証

ローカル EAP は、ユーザーおよびワイヤレス クライアントのローカル認証をコントローラで可能にする認証方式です。バックエンドシステムが妨害されたり、外部認証サーバーがダウンした場合でも、ワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使用を目的として設計されています。ローカル EAP を有効にすると、コントローラは認証サーバーおよびローカル ユーザー データベースとして機能するため、外部認証サーバーに依存する必要がなくなります。ローカル EAP は、ローカル ユーザー データベースまたは LDAP バックエンドデータベースからユーザーの資格情報を取得して、ユーザーを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間の MAP 認証で、EAP-FAST 認証方式のみがサポートされます。

ローカル EAP はバックエンド データベースとして LDAP サーバーを使用し、コントローラとワイヤレス クライアント間の MAP 認証のユーザー ログイン情報を取得します。LDAP バックエンドデータベースを使用すると、コントローラで、特定のユーザーの資格情報（ユーザー名およびパスワード）を LDAP サーバーから検索できるようになります。これらの資格情報は、ユーザーの認証に使用されます。



- (注) コントローラ上で RADIUS サーバーが設定されている場合、コントローラはまず RADIUS サーバーを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバーが見つからない、タイムアウトになっている、または設定されていない場合にのみ試行されます。

LSC による EAP 認証

ローカルで有効な証明書ベース（LSC ベース）の EAP 認証も MAP でサポートされています。この機能を使用するには、認証局の制御、生成された証明書のポリシー、有効期間、制限、お

よび使用方法の定義、AP とコントローラでインストールされたこれらの証明書の取得を行うために、公開キー インフラストラクチャ (PKI) が必要です。

これらのユーザー生成証明書または LSC が AP とコントローラで使用可能になると、デバイスはこれらの LSC を使用して接続、認証、およびセッション キーの取得を開始できます。

LSC によって AP から既存の証明書が削除されることはありません。AP は LSC と製造元でインストールされる証明書 (MIC) の両方を保持できます。ただし、AP が LSC でプロビジョニングされた後は、起動時に MIC 証明書が使用されなくなります。LSC から MIC に変更する場合は、該当する AP をリブートする必要があります。

次の目的で、コントローラは指定サーバーに対する EAP 認証を使用したメッシュセキュリティもサポートしています。

- メッシュ子 AP の認証
- パケット暗号化のためのマスター セッション キー (MSK) の生成

ブリッジグループ名

ブリッジグループ名 (BGN) は、親メッシュ AP への MAP のアソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておく、同じチャネルにある2つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター (領域) のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字から成る文字列です。

NULL VALUE という BGN が製造時にデフォルトで割り当てられます。このグループ名は表示されませんが、これにより、ネットワーク固有の BGN を割り当てる前に MAP をネットワークに参加させることができます。

同一セクターのネットワーク内に (より大きなキャパシティを得るために) RAP が2つある場合は、別々のチャネルで2つの RAP に同じ BGN を設定することをお勧めします。

完全一致 BGN を MAP で有効にすると、一致する BGN 親を見つけるためにスキャンが 10 回行われます。10 回スキャンしても一致する BGN 親を見つけられない場合、AP は一致しない BGN に接続して 15 分間接続を維持します。15 分後に AP は再び 10 回スキャンを行い、このサイクルが繰り返されます。デフォルトの BGN の機能は完全一致 BGN が有効な場合も同じです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、メッシュ プロファイルに BGN が設定されています。MAP がコントローラに参加するたびに、コントローラはメッシュ プロファイルに設定されている BGN を AP にプッシュします。



(注) EWC HA ペアでは、BGN 設定を変更するとスイッチオーバーが発生します。設定された BGN をメッシュ プロファイルから削除すると、スイッチオーバーがトリガーされます。

優先される親 (Preferred Parent) の選択

MAP の優先される親を使用すると、メッシュ環境で線形トポロジを適用できます。この機能を使用すると、Adaptive Wireless Path Protocol で定義された (AWPP 定義) 親選択メカニズムをオーバーライドして、優先される親に MAP を強制的に移動できます。

Cisco Wave 1 AP の場合、優先される親を設定する際には、目的の親に対して実際のメッシュネイバーの MAC アドレスを指定してください。この MAC アドレスは base radio MAC アドレスで、最後の文字が「f」になります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f
```

Cisco Wave 2 AP の場合、優先される親を設定すると、MAC アドレスは、最後の 2 文字に「0x11」が追加された base radio MAC アドレスになります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:11 を指定する必要があります。

```
Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11
```

ブリッジグループ名の設定 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
- ステップ 2 [Add] をクリックします。
- ステップ 3 [Advanced] タブの [Bridge Group] の設定で、[Bridge Group Name] を入力します。
- ステップ 4 [Bridge Group] の設定で、[Strict Match] チェックボックスをオンにして機能を有効にします。完全一致 BGN を MAP で有効にすると、一致する BGN 親を見つけるためにスキャンが 10 回行われます。
- ステップ 5 [Apply to Device] をクリックします。

ブリッジグループ名の設定 (CLI)

- ブリッジグループ名 (BGN) がメッシュプロファイルに設定されている場合、MAP がコントローラに接続するたびに、メッシュプロファイルに設定されている BGN が AP にプッシュされます。
- メッシュ AP が AireOS コントローラから Cisco Catalyst 9800 シリーズワイヤレスコントローラに移動するたびに、メッシュプロファイルに設定されている BGN がその AP にプッシュされて保存されます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	bridge-group name <i>bridge-grp-name</i> 例： Device(config-wireless-mesh-profile)# bridge-group name bgn1	ブリッジ グループ名を設定します。
ステップ 4	bridge-group strict-match 例： Device(config-wireless-mesh-profile)# bridge-group strict-match	ブリッジ グループの厳密な照合を設定します。

2.4 GHz および 5 GHz のメッシュバックホール

バックホールは、MAP 間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは 802.11a/n/ac/g です (AP によって異なります)。デフォルトのバックホール インターフェイスは 5 GHz です。利用可能な無線周波数スペクトラムを効果的に使用するには、レート選択が重要です。このレートは、クライアントデバイスのスループットにも影響を与える可能性があります (スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです)。

メッシュバックホールは、2.4 GHz および 5 GHz でサポートされています。ただし特定の国では、5 GHz のバックホール ネットワークでメッシュ ネットワークを使用することは許可されていません。2.4 GHz の無線周波数を使用すると、より大きなメッシュまたはブリッジ距離を実現できます。RAP はスロット変更設定を取得すると、すべての子 MAP に伝達します。すべての MAP は接続を解除し、新たに設定されたバックホール スロットに接続します。

メッシュバックホールの設定 (CLI)

ここでは、2.4 GHz でメッシュバックホールを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	ap name <i>ap_name</i> mesh backhaul radio dot11 24ghz 例 : Device # ap name test-ap mesh backhaul radio dot11 24ghz	メッシュバックホールを 2.4GHz に変更します。

Dynamic Frequency Selection (動的周波数選択)

既存のレーダーサービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要があるデバイスに対して、動的周波数選択 (DFS) プロトコルに従って動作することを求めています。DFS に準拠するために、無線デバイスがレーダー信号の存在を検出できることが義務付けられています。無線でレーダー信号が検出された場合、最低 30 分間は伝送を停止してそのサービスを保護する必要があります。その後、無線は別のチャンネルを選択しますが、伝送する前にこのチャンネルをモニターリングする必要があります。使用する予定のチャンネルで 1 分間以上レーダーが検出されなかった場合は、新しい無線サービス デバイスがそのチャンネルで伝送を開始できます。DFS 機能により、メッシュ AP はセクター内のいずれかのメッシュ AP でレーダーイベントが検出されたときに、ただちにチャンネルを切り替えることができます。

動的周波数選択の設定 (GUI)

手順

-
- ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
 - ステップ 2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。
 - ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。
 - ステップ 4 プロファイル名を入力します。
 - ステップ 5 [Full sector DFS status] チェックボックスをオンにして、動的周波数選択を有効にします。
 - ステップ 6 [Apply to Device] をクリックします。
-

動的周波数選択の設定 (CLI)

DFS は、DFS チャンネルでライセンスを必要としない操作の特定のタイマーとともに検出されるレーダー波形のタイプを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	full-sector-dfs 例： Device(config-wireless-mesh-profile)# full-sector-dfs	DFS を有効にします。 (注) DFS 機能により、レーダー信号を検出した MAP はそれを RAP まで伝送することができ、RAP はレーダーを経験したことがあるかのように動作し、セクターを移動します。このプロセスは、コーディネイテッドチャンネル変更と呼ばれます。コントローラで、この機能はオンまたはオフにできます。コーディネイテッドチャンネル変更は、デフォルトでイネーブルになっています。

国コード

コントローラおよび AP は、法的な規制基準の異なるさまざまな国で使用できるように設計されています。AP 内の無線は、製造時に特定の規制ドメイン（ヨーロッパの場合には E など）に割り当てられていますが、国コードを使用すると、稼働する特定の国を指定できます（フランスの場合には FR、スペインの場合には ES など）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャンネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

国によっては、屋内と屋外の AP に次のような違いがあります。

- 規制ドメイン コード
- サポートされるチャンネルセット
- 送信電力レベル

侵入検知システム

Cisco 侵入検知システム/侵入防御システム (CIDS/CIPS) は、特定のクライアントに関わる攻撃がレイヤ3～レイヤ7で検出されたとき、これらのクライアントによるワイヤレスネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーション不正使用などの脅威を検出、分類、阻止することで、強力なネットワーク保護を提供します。

侵入検知システムの設定 (GUI)

手順

- ステップ1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
- ステップ2 [Add] をクリックします。
[Add Mesh Profile] ウィンドウが表示されます。
- ステップ3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。
- ステップ4 プロファイル名を入力します。
- ステップ5 [IDS (Rogue/Signature Detection)] チェックボックスをオンにして、侵入検知システムを有効にします。
- ステップ6 [Apply to Device] をクリックします。

侵入検知システムの設定 (CLI)

侵入検知システムを有効にすると、クライアントアクセスのすべてのトラフィックに関するレポートが生成されます。ただし、バックホールトラフィックは対象になりません。

手順

	コマンドまたはアクション	目的
ステップ1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ2	wireless profile mesh profile-name 例： Device(config)# wireless profile mesh mesh1	メッシュプロファイルを設定し、メッシュプロファイル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 3	ids 例 : Device (config-wireless-mesh-profile) # ids	メッシュ AP の侵入検知システムレポートを設定します。

コントローラ間のメッシュ相互運用性

AireOS と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の間の相互運用性が維持され、次のサポートが提供されます。

- MAP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に接続された AP によって形成されたメッシュ ネットワーク を介して AireOS コントローラ に接続できます。
- MAP は、AireOS コントローラ に接続された AP によって形成されたメッシュ ネットワーク を介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に接続できます。
- AireOS に接続されている親メッシュ AP と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の間で、PMK キャッシュを使用した MAP ローミングがサポートされます。



- (注) シームレスな相互運用性を実現するためには、AireOS コントローラ と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ が同じモビリティ グループ に属し、IRCM をサポートするイメージバージョンを使用する必要があります。

メッシュ コンバージョン

メッシュ コンバージョン により、MAP は現在の親とのバックホール接続が失われた場合に、コントローラ との接続を再確立できます。コンバージョン時間を短縮するために、各メッシュ AP はチャンネルのサブセットを維持して将来のスキャン/シークに使用し、ネイバー リストのサブセットで親を識別します。

次のコンバージョン方式がサポートされています。

表 1: メッシュ コンバージョン

メッシュ コンバージョン	親の損失検出/キープアライブタイマー
規格	21 / 3 秒
速い	7 / 3 秒
Very Fast	4 / 2 秒

メッシュコンバージェンス	親の損失検出/キープアライブタイマー
ノイズトレラント高速	21 / 3 秒

ノイズトレラント高速

ノイズトレラント高速検出は、現在の親を 21 秒ごとに標準方式で評価する AWPP ネイバー要求に対する応答を取得できないことが前提になります。親への要求とともに、各ネイバーに 3 秒ごとにユニキャスト要求が送信されます。親からの応答を取得できないときは、ローミング（ネイバーが同じチャンネルで使用可能な場合）または新しい親のフルスキャンが開始されます。

メッシュコンバージェンスの設定（CLI）

ここでは、メッシュコンバージェンスを設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュプロファイルを作成します。
ステップ 3	convergence {fast noise-tolerant-fast standard very-fast} 例： Device(config-wireless-mesh-profile)# convergence fast	メッシュプロファイルのメッシュコンバージェンス方式を設定します。

イーサネットブリッジング

セキュリティ上の理由により、デフォルトではすべての MAP でイーサネットポートが無効になっています。有効にするには、ルートおよび各 MAP でイーサネットブリッジングを設定します。

タグ付きパケットとタグなしパケットの両方が、セカンダリイーサネットインターフェイスでサポートされています。

ポイントツーポイントブリッジングシナリオでは、バックホール無線を使用してスイッチドネットワークの複数のセグメントをブリッジ接続することにより、Cisco Aironet 1500 シリーズ MAP を使用してリモートネットワークを拡張できます。これは基本的には、1つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイント ネットワークと同様に、イーサネットブリッジングを有効にすることでクライアントアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。イーサネットブリッジドアプリケーションを使用するには、RAP およびそのセクター内のすべての MAP でブリッジング機能を有効にする必要があります。

イーサネットブリッジングは、次の場合に有効にする必要があります。

- メッシュ ノードをブリッジとして使用する。
- MAP でイーサネットポートを使用してイーサネットデバイス（ビデオカメラなど）を接続する。



(注) メッシュ AP からコントローラへのパスを取るすべての親メッシュ AP に対してイーサネットブリッジングを有効にしてください。

イーサネットブリッジング用の VLAN がサポートされたメッシュ環境では、MAP 上のセカンダリイーサネットインターフェイスにコントローラから VLAN を個別に割り当てます。すべてのバックホールブリッジリンク（有線とワイヤレスの両方）は、すべての VLAN が有効になっているトランクリンクです。非イーサネットブリッジドトラフィック、およびタグなしイーサネットブリッジドトラフィックは、メッシュ内の AP のネイティブ VLAN を使用してメッシュに沿って伝送されます。これは、AP がサービスを提供しているワイヤレスクライアントで送受信されるすべてのトラフィックと同様です。VLAN タグ付きパケットは、ワイヤレスバックホールリンクを介して AWPP でトンネリングされます。

MAP イーサネットクライアントの VLAN タギング

メッシュ AP のバックホールインターフェイスはプライマリ インターフェイスと呼ばれ、他のインターフェイスはセカンダリ インターフェイスと呼ばれます。

イーサネット VLAN タギングを使用すると、無線メッシュネットワーク内で特定のアプリケーショントラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセスモード）、別の無線メッシュネットワークにブリッジングすることができます（トランクモード）。

イーサネットブリッジングの設定 (GUI)

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ2 [Add] をクリックします。

ステップ3 [General] タブで、メッシュプロファイルの [Name] を入力します。

ステップ4 [Advanced] タブで、[VLAN Transparent] チェックボックスをオンにして、VLAN 透過性を有効にします。

ステップ5 [Advanced] タブで、[Ethernet Bridging] チェックボックスをオンにします。

ステップ6 [Apply to Device] をクリックします。

イーサネットブリッジングの設定 (CLI)

MAPのイーサネットポートはデフォルトで無効になっています。有効にするには、ルートAPと他の各MAPでイーサネットブリッジングを設定する必要があります。

イーサネットブリッジングは、次の場合に有効にできます。

- メッシュノードをブリッジとして使用する。
- MAPのイーサネットポートを使用してイーサネットデバイス（ビデオカメラなど）を接続する。

始める前に

- イーサネットブリッジングを有効にするには、メッシュプロファイル設定で次のコマンドを設定してください。
 - `ethernet-bridging` : APでイーサネットブリッジング機能を有効にします。
 - `no ethernet-vlan-transparent` : ワイヤレスメッシュブリッジVLANを認識させます。次のAPコマンドを使用してVLANフィルタリングを許可します。[no] `mesh ethernet {0|1|2|3} mode trunk vlan allowed`



注 すべてのVLANをブリッジする場合（ブリッジが有線の一部として機能する場合）、VLAN透過性を有効にして、すべてのVLANが通過できるようにする必要があります。VLANトランスペアレントモードを使用する場合は、ネットワークの有線側でVLANをフィルタリングして、不要なトラフィックによってネットワークがフラグディングしないようにすることをお勧めします。

- イーサネットブリッジングが機能するように、ルートAPが接続されているスイッチポートをトランクポートとして設定する必要があります。

- ブリッジモード AP の場合は、**ap name name-of-rap mesh vlan-trunking native vlan-id** コマンドを使用して対応する RAP でトランク VLAN を設定します。イーサネットブリッジ機能は、このコマンドが設定されていない AP では有効になりません。
- フレックス+ブリッジ AP の場合は、対応する flex プロファイルでネイティブ VLAN ID を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device# enable	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	ap name ap-name mesh ethernet {0 1 2 3} mode access vlan-id 例： Device# ap name ap1 mesh ethernet 1 mode access 21	AP のイーサネットポートを設定し、モードをトランクとして設定します。
ステップ 3	ap name ap-name mesh ethernet {0 1 2 3} mode trunk vlan vlan-id 例： Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21	ネイティブ VLAN をトランク ポート用に設定します。
ステップ 4	ap name ap-name mesh ethernet {0 1 2 3} mode trunk vlan allowed vlan-id 例： Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21	トランク ポートの許可 VLAN を設定します。 メッシュまたはルートアクセスポイントのイーサネットポートで VLAN フィルタリングを許可します。メッシュプロファイルで VLAN 透過性が無効になっている場合にのみアクティブです。

メッシュ デイジー チェーン 接続

メッシュ AP には、MAP として機能する AP をデイジーチェーン接続する機能があります。デイジーチェーン接続された MAP では、AP をシリアルバックホールとして運用する（アップリンクアクセスとダウンリンクアクセスに別々のチャンネルを使用できるためバックホール帯域幅が向上する）ことも、ユニバーサルアクセスを拡張することもできます。ユニバーサルアクセスの拡張により、ローカルモードまたは FlexConnect モードのメッシュ AP を MAP のイーサネットポートに接続できるため、ネットワークが拡張され、より良いクライアントアクセスを提供できます。

デイジーチェーン接続された AP は、AP の電源供給方法に応じて異なる方法でケーブル接続する必要があります。DC 電源を使用して AP に電力が供給されている場合は、プライマリ AP の LAN ポートから下位 AP の PoE 入力ポートにイーサネットケーブルを直接接続する必要があります。

デイジーチェーン接続モードに関するガイドラインは次のとおりです。

- プライマリ MAP は、メッシュ AP として設定する必要があります。
- 下位 MAP は、ルート AP として設定する必要があります。
- デイジーチェーン接続は、プライマリ MAP と下位 MAP の両方で有効にする必要があります。
- ブリッジモードのすべての AP でイーサネットブリッジングを有効にする必要があります。メッシュプロファイルでイーサネットブリッジングを有効にして、セクター内のすべてのブリッジモード AP を同じメッシュプロファイルにマッピングします。
- VLAN サポートは、ネイティブ VLAN を適切に設定して、有線ルート AP、下位 MAP、およびプライマリ MAP で有効にする必要があります。

メッシュイーサネット デイジーチェーン接続の制約事項

- この機能は、Cisco Industrial Wireless 3702 AP にのみ適用されます。
- この機能は、ブリッジモードおよび Flex+ブリッジモードでのみ動作する AP に適用されます。
- Flex+ブリッジモードでは、ローカルスイッチング WLAN が有効になっている場合、ワークグループブリッジ (WGB) マルチ VLAN はサポートされません。
- イーサネット デイジーチェーン トポロジをサポートするには、Cisco Industrial Wireless 3702 PoE 出力ポートをポート内の他の Cisco Industrial Wireless 3702 PoE に接続しないで、パワーインジェクタを AP の電源として使用する必要があります。
- チェーン内の AP の数が増えると、ネットワーク コンバージェンス時間が長くなります。
- デイジーチェーンの一部であり、RAP ロールが割り当てられている EWC 対応 AP は、CAPWAP モード (ap-type capwap) である必要があります。

メッシュイーサネット デイジーチェーン接続の前提条件

- AP ロールがルート AP として設定されていることを確認します。
- 対応する AP でイーサネットブリッジングと厳密な有線アップリンクが有効になっていることを確認します。
- VLAN 透過性が無効になっていることを確認します。

- ブリッジモード AP の各ルート AP における VLAN サポートを有効にするには、**ap name name-of-rap mesh vlan-trunking [native] vlan-id** コマンドを使用して対応する RAP でトランク VLAN を設定します。
- Flex + ブリッジ AP の各ルート AP における VLAN サポートを有効にするには、対応する Flex プロファイルでネイティブ VLAN ID を設定する必要があります。
- 1000 Mbps をサポートする 4 ペアケーブルを使用してください。この機能は、100 Mbps をサポートする 2 ペアケーブルでは正しく動作しません。

メッシュイーサネット デイジー チェーン接続の設定 (CLI)

ここでは、メッシュ AP でメッシュイーサネット デイジー チェーン接続機能を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	ap profile default-ap-profile 例： Device(config)# ap profile default-ap-profile	AP プロファイルを指定します。
ステップ 3	ssid broadcast persistent 例： Device(config-ap-profile)# ssid broadcast persistent	永続的 SSID ブロードキャストを設定し、厳密な有線アップリンクを確保します。このコマンドを設定すると、RAP はワイヤレスバックホールに切り替わりません。

メッシュイーサネット ブリッジング ネットワーク経由のマルチキャスト

メッシュマルチキャストモードによって、ブリッジング対応 AP (MAP や RAP など) がメッシュネットワーク内のイーサネット LAN 間でマルチキャストパケットを送信する方法が決まります。メッシュマルチキャストモードは非 CAPWAP マルチキャストトラフィックのみを管理します。CAPWAP マルチキャストトラフィックは異なるメカニズムで管理されます。

異なるメッシュマルチキャストモードを使用して、すべての MAP でマルチキャストおよびブロードキャストパケットを管理できます。イネーブルになっている場合、これらのモードは、

メッシュネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは次のとおりです。

- **regular** モード：マルチキャストの通常モードは、EWC 上の Cisco Catalyst 9124 シリーズ屋外アクセスポイントではサポートされていません。
- **in-only** モード：MAP がイーサネットから受信するマルチキャストパケットは、対応する RAP のイーサネットネットワークに転送されます。他の転送は行われないので、RAP が受信した非 CAPWAP マルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワーク（発信元）に返送されず、MAP から MAP へのマルチキャストはフィルタで除去されるため発生しません。
- **in-out** モード：RAP と MAP は別々の方法でマルチキャストを実行します。
 - イーサネット経由で MAP が受信したマルチキャスト パケットは RAP に送信されますが、イーサネット経由で他の MAP に送信されることはありません。MAP から MAP へのパケットはマルチキャストからフィルタで除去されます。
 - マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

メッシュを介したマルチキャストモードの設定 (GUI)

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ 2 [Add] をクリックします。

[Add Mesh Profile] ウィンドウが表示されます。

ステップ 3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ 4 プロファイル名を入力します。

ステップ 5 ドロップダウンリストから、次のいずれかの [Multicast Modes] を選択します。

- a) [Regular]：このモードでは、データは、ブリッジ対応の RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにマルチキャストされます。
- b) [In]：このモードでは、MAP がイーサネットから受信するマルチキャストパケットは、対応する RAP のイーサネットネットワークに転送されます。
- c) [In-Out]：このモードでは、RAP と MAP は別々の方法でマルチキャストを実行します。

ステップ 6 [Apply to Device] をクリックします。

メッシュを介したマルチキャストモードの設定

- マルチキャストパケットがイーサネット経由で MAP で受信された場合は、RAP に送信されます。ただし、他の MAP には送信されません。MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。
- マルチキャストパケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。
- in-out モードがデフォルトのモードです。in-out モードで動作中の場合、1 台の RAP によって送信されたマルチキャストを同じイーサネットセグメント上の別の RAP が受信してネットワークに戻さないよう、ネットワークを適切に分割する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	multicast {in-only in-out regular} 例： Device(config-wireless-mesh-profile)# multicast regular	メッシュ マルチキャスト モードを設定します。

メッシュでの無線リソース管理

Radio Resource Management (RRM) ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは関連する Lightweight AP を継続的にモニターリングして、トラフィック負荷、干渉、ノイズ、カバレッジ、およびその他の隣接 AP に関する情報を取得できます。

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネットリンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

メッシュバックホールの RRM の設定 (GUI)

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Global Config] を選択します。

ステップ 2 [Backhaul] セクションで、[RRM] チェックボックスをオンにして、メッシュでの無線リソース管理を有効にします。

ステップ 3 [Apply] をクリックします。

メッシュバックホールの RRM の設定 (CLI)

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネット リンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

メッシュ バックホールで RRM を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless mesh backhaul rrm 例： Device(config)# wireless mesh backhaul rrm	メッシュバックホールの RRM を設定します。

メッシュ リーフ ノード

リーフ ノードとしてのみ動作するパフォーマンスの低い MAP を設定できます。メッシュ ネットワークが形成および統合されると、リーフ ノードは子 MAP としてのみ動作でき、他の MAP が親 MAP として選択することはできなくなります。したがって、ワイヤレスバックホールパフォーマンスはダウングレードされません。

メッシュリーフノードの設定 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
- ステップ 2 [Access Point] をクリックします。
- ステップ 3 [Mesh] タブで、[Block Child] チェックボックスをオンにします。
- ステップ 4 [Update & Apply to Device] をクリックします。

メッシュリーフノードの設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name ap-namemesh block-child 例： Device# #ap name ap1 mesh block-child	リーフ ノードとしてのみ動作するように AP を設定します。他の MAP がこの AP を親 MAP として選択することはできません。 (注) 通常の AP に変更するには、このコマンドの no 形式を使用します。

フレックス + ブリッジ モード

フレックス + ブリッジ モードは、メッシュ (ブリッジ モード) AP 上で FlexConnect の機能を有効にするために使用されます。メッシュ AP は接続先のルート AP から VLAN を継承します。

MAP に接続されている Flex モードの EWC 対応 AP は、CAPWAP モード (AP-type CAPWAP) である必要があります。

次のいずれかのモードの各 AP で、VLAN トランッキングを有効または無効にしたり、ネイティブ VLAN ID を設定したりできます。

- FlexConnect

- Flex + ブリッジ (FlexConnect + メッシュ)

バックホールクライアントアクセス

バックホールクライアントアクセスが有効な場合は、無線バックホールを介したワイヤレスクライアントアソシエーションが許可されます。バックホール無線は2.4または5 GHz 無線です。つまり、バックホール無線は、バックホールトラフィックとクライアントトラフィックの両方を伝送できます。

バックホールクライアントアクセスが無効な場合は、バックホールトラフィックのみがバックホール無線を介して送信され、クライアント関連付けはアクセス無線でのみ実行されます。



- (注) バックホールクライアントアクセスはデフォルトで無効になっています。バックホールクライアントアクセスを有効にすると、ダイジーチェーン接続展開の下位 AP と子 AP を除くすべての MAP が再起動します。

バックホールクライアントアクセスの設定 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
- ステップ 2 プロファイルを選択します。
- ステップ 3 [General] タブで、[Backhaul Client Access] チェックボックスをオンにします。
- ステップ 4 [Update & Apply to Device] をクリックします。

バックホールクライアントアクセスの設定 (CLI)



- (注) バックホールクライアントアクセスはデフォルトで無効になっています。有効にすると、ダイジーチェーン接続展開の下位 AP と子 AP を除くすべての MAP が再起動します。

メッシュプロファイルでバックホールクライアントアクセスを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	client-access 例： Device(config-wireless-mesh-profile)# client-access	クライアント アクセス AP を使用してバックホールを設定します。

アクセスポイントごとのメッシュバックホールでの Dot11ax レートの設定 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Access Points] を選択します。
ネットワーク内のすべての設定済み AP が一覧表示される [All Access Points] セクションが、対応する詳細とともに表示されます。
- ステップ 2 設定されたメッシュ AP をクリックします。
[Edit AP] ウィンドウが表示されます。
- ステップ 3 [Mesh] タブを選択します。
- ステップ 4 [General] セクションの [Backhaul] セクションに、デフォルトの [Backhaul Radio Type]、[Backhaul Slot ID]、および [Rate Types] フィールドの詳細が表示されます。[Backhaul Radio Type] と [Backhaul Slot ID] の値は、ルート AP に対してのみ変更できることに注意してください。
- ステップ 5 [Rate Types] ドロップダウンリストから、バックホールレートタイプを選択します。
選択内容に基づいて、表示される対応するフィールドに詳細を入力します。バックホールインターフェイスは、AP によって、自動レートおよび 802.11a/b/g/n/ac/ax レートが異なります。Cisco Catalyst 9124AX 屋外アクセスポイントは、メッシュバックホールで 11ax バックホールレートをサポートする唯一の AP です。
- ステップ 6 [Backhaul MCS Index] フィールドに、AP 間で送信できる変調符号化方式 (MCS) レートを入力します。有効な範囲は、両方の帯域で 0 ~ 11 です。

ステップ7 [Spatial Stream] フィールドに、サポートされている空間ストリームの数を入力します。5 GHz 無線帯域の1つの無線でサポートされる空間ストリームの最大数は8ですが、2.4 GHz 無線帯域では4つの空間ストリームがサポートされます。

ステップ8 [Update and Apply to Device] をクリックします。

メッシュプロファイルのメッシュバックホールでの Dot11ax レートの設定 (GUI)

手順

ステップ1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ2 [Add] をクリックします。

[Add Mesh Profile] ウィンドウが表示されます。

ステップ3 [Add Mesh Profile] ウィンドウで [General] タブをクリックします。

ステップ4 [Name] フィールドに、メッシュプロファイルの名前を入力します。

ステップ5 [Advanced] タブをクリックします。

ステップ6 [5 GHz Band Backhaul] セクションと [2.4 GHz Band Backhaul] セクションで、[Rate Types] ドロップダウンリストから [dot11ax] バックホールレートタイプを選択します。

(注) Cisco Catalyst 9124AXI/D シリーズ屋外アクセスポイントは、メッシュバックホールで 11ax バックホールレートをサポートする唯一の AP です。

ステップ7 [Dot11ax MCS index] フィールドで、AP 間でデータを送信可能な MCS レートを指定します。値の範囲は、両方の無線帯域で 0 ~ 11 です。

ステップ8 [Spatial Stream] フィールドに値を入力します。5 GHz 無線帯域の1つの無線でサポートされる空間ストリームの最大数は8ですが、2.4 GHz 無線帯域では4つの空間ストリームがサポートされます。

ステップ9 [Update and Apply to Device] をクリックします。

AP ごとのデータレートの設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name ap-name mesh backhaul rate dot11ax mcs <0-11> ss <1-8> 例： Device# ap name ap1 mesh backhaul rate dot11ax 5 ss 4	2.4 GHz および 5 GHz 帯域のメッシュバックホール 11ax レートを設定します。

メッシュプロファイルを使用したデータレートの設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	wireless profile mesh profile-name 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュプロファイル コンフィギュレーションモードを開始します。
ステップ 3	backhaul rate dot11 {24ghz 5ghz} dot11ax mcs <0-11> spatial-stream <1-8> 例： Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11ax mcs 5 spatial-stream 6 Device(config-wireless-mesh-profile)# backhaul rate dot11 24ghz dot11ax mcs 5 spatial-stream 4	2.4 GHz 帯域および 5 GHz 帯域のバックホール転送速度を設定します。2.4 GHz 帯域の 802.11ax 空間ストリーム値は 1 ~ 4、5 GHz 帯域の空間ストリーム値は 1 ~ 8 です。

ルート AP のバックホールスロットの指定 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。
- ステップ 2 [Add] をクリックします。
- ステップ 3 [General] タブで、メッシュプロファイルの [Name] を入力します。
- ステップ 4 [Advanced] タブで、[5 GHz Band Backhaul] および [2.4 GHz Band Backhaul] の [Rate Types] ドロップダウンリストからレートタイプを選択します。
- ステップ 5 [Apply to Device] をクリックします。

ルート AP のバックホールスロットの指定 (CLI)

メッシュバックホールレートを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name rap-name mesh backhaul radio dot11 {24ghz 5ghz} [slot slot-id] 例： Device# ap name rap1 mesh backhaul radio dot11 24ghz slot 2	メッシュバックホール無線スロットを設定します。

ワイヤレスバックホールのデータレートの設定 (CLI)

バックホールは、AP 間のワイヤレス接続を作成するために使用されます。AP に応じて 802.11bg/a/n/ac のバックホールインターフェイスを使用できます。レート選択によって、利用可能な RF スペクトラムを効果的に使用できます。データレートは、RF カバレッジとネットワークパフォーマンスにも影響を与えます。低データレート (6 Mbps など) のほうが、高データレート (1300 Mbps など) よりも AP からの距離を延長できます。結果として、データレートはセルカバレッジ、および必要な AP の数に影響を与えます。



- (注) バックホールデータレートは設定できます（可能な場合は、メッシュプロファイルを使用）。特定のデータレートが必要な場合は、コマンドを使用して AP ごとのデータレートを設定します。

特権 EXEC モードまたはメッシュプロファイル コンフィギュレーション モードでワイヤレスバックホール データ レートを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name <i>ap-name</i> mesh backhaul rate {auto dot11abg dot11ac dot11n} 例： Device# #ap name ap1 mesh backhaul rate auto	バックホール転送速度を設定します。
ステップ 3	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュプロファイルを設定し、メッシュプロファイル コンフィギュレーション モードを開始します。
ステップ 4	backhaul rate dot11 {24ghz 5ghz} dot11n RATE_6M 例： Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n mcs 31	バックホール転送速度を設定します。 (注) AP に設定されたレート（ステップ 2）は、メッシュプロファイルに設定されたレート（ステップ 4）と一致する必要があります。ご注意ください。

メッシュバックホールでのリンクテストの使用 (GUI)

手順

ステップ 1 [Monitoring] > [Wireless] > [AP Statistics] > [General] を選択します。

ステップ 2 [Access Point] をクリックします。

- ステップ3 [Mesh] > [Neighbor] > [Linktest] を選択します。
- ステップ4 [Data Rates]、[Packets to be sent (per second)]、[Packet Size (bytes)]、および[Test Duration (seconds)] ドロップダウンリストから目的の値を選択します。
- ステップ5 [Start] をクリックします。

メッシュバックホールでのリンクテストの使用

ネイバーメッシュ AP 間のリンクテストをトリガーするには、次の手順に従います。



- (注) AP からリンクテストを実行するには、**test mesh linktest mac-address neighbor-ap-mac rate data-rate fps frames-per-second frame-size frame-size** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ2	ap name ap-name mesh linktest dest-ap-mac data-rate packet-per-sec packet-size test-duration 例： Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200	リンクテストパラメータを設定します。

メッシュ CAC

コールアドミッション制御 (CAC) を使用すると、メッシュアクセスポイントはコントローラで制御されている Quality of Service (QoS) を維持して、メッシュネットワークの音声品質を管理できます。帯域幅に基づく、静的な CAC を使用すると、クライアントで新しいコールを受信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセスポイントは、使用可能な帯域幅を確認して特定のコールに対応できるかどうかを判断し、そのコールに必要な帯域幅と比較します。品質を許容できる最大可能コール数を維持するために十分な帯域幅が使用できない場合、メッシュアクセスポイントはコールを拒否します。

- クライアントが同じサイト内にある MAP 間でローミングすると、アクティブコールの新しいツリーで帯域幅の可用性が再度チェックされます。

- MAP が新しい親にローミングしても、アクティブ コールが終了することではなく、サブツリー内の他のアクティブ コールで引き続きアクティブのままになります。
- MAP のハイ アベイラビリティ (HA) はサポートされていません。MAP のアクセス無線に接続されたコールは HA スイッチオーバー時に終了します。
- RAP の HA はサポートされているため、RAP のアクセス無線に接続されたコールは、スイッチオーバー後も新しいコントローラでアクティブのままになります。
- メッシュ CAC アルゴリズムは、音声コールにのみ適用されます。
- メッシュ バックホール無線帯域幅の計算では、スタティック CAC が適用されます。AP でメッシュ バックホールの負荷ベース CAC がサポートされていないため、負荷ベース CAC は使用されません。
- 無線で使用可能な帯域幅に基づいてコールが許可されます。コール アドミッションでは Air Time Fairness (ATF) が考慮されず、ATF ポリシーが適用されるコールには ATF ウェイトに従って帯域幅が割り当てられます。

メッシュ CAC は、次のシナリオではサポートされていません。

- メッシュ ツリー内の AP に異なるサイト タグが割り当てられている場合。
- メッシュ ツリー内の AP にデフォルトのサイト タグが割り当てられている場合。

メッシュ CAC の設定 (CLI)

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless mesh cac 例： Device(config)# <code>wireless mesh cac</code>	メッシュ CAC モードを有効にします。

アップリンクゲートウェイの到達可能性障害の高速検出によるメッシュネットワークの回復の高速化

すべての 802.11ac Wave 2 AP では、アップリンクゲートウェイの到達可能性障害を迅速に検出することにより、メッシュネットワークの回復メカニズムの速度が向上します。メッシュ AP

のアップリンクゲートウェイの到達可能性は、IPv4 または IPv6 のデフォルトゲートウェイへの ICMP ping を使用してチェックされます。

メッシュ AP は、次の 2 つのシナリオで到達可能性チェックをトリガーします。

- 新しいアップリンクが選択された後、メッシュ AP がコントローラに接続するまで
 新しいアップリンクが選択された後、メッシュ AP には、選択したアップリンクを介して（静的 IP または DHCP 経由で）ゲートウェイに到達するための 45 秒の時間帯があります。45 秒経過してもメッシュ AP がゲートウェイに到達できない場合、現在のアップリンクはブロックリストにあるため、アップリンクの選択プロセスが再開されます。AP がこの 45 秒の時間帯内にコントローラに接続すると、到達可能性チェックは停止します。その後、通常動作中はゲートウェイの到達可能性チェックは実行されません。
- メッシュ AP がコントローラとの接続をタイムアウトした直後
 メッシュ AP がコントローラとの接続をタイムアウトし、AP が 5 秒以内にゲートウェイに到達できないと、現在のアップリンクがブロックリストにすぐに追加されて、アップリンクの選択プロセスが再開されます。

サブセットチャンネル同期の設定

コントローラ内のすべての RAP で使用されるすべてのチャンネルが、以降の検索とコンバージェンスのためにすべての MAP に送信されます。コントローラは、各ブリッジグループ名 (BGN) のサブセットチャンネルのリストを保持します。また、サブセットチャンネルのリストはモビリティグループ内のすべてのコントローラで共有されます。

サブセットチャンネルリストは、特定の BGN の RAP が動作しているチャンネルのリストです。このリストは、コントローラ内およびコントローラ間のすべての MAP に伝達されます。サブセットチャンネルリストは、メッシュ AP のより高速なコンバージェンスのためのリストです。コンバージェンス方式はメッシュプロファイルで選択できます。コンバージェンス方式が標準的な方式でない場合、サブセットチャンネルリストが MAP にプッシュされます。

モビリティグループのサブセットチャンネルの同期を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーションモードを開始します。
ステップ 2	wireless mesh subset-channel-sync mac 例： Device(config)# wireless mesh subset-channel-sync	モビリティグループのサブセットチャンネルの同期を設定します。

優先される親の選択 (GUI)

手順

-
- ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
- ステップ 2 [Access Point] をクリックします。
- ステップ 3 [Mesh] タブで、[Preferred Parent MAC] を入力します。
- ステップ 4 [Update & Apply to Device] をクリックします。
-

優先される親の選択 (CLI)

MAP の優先される親を設定するには、次の手順に従います。

このメカニズムを使用すると、AWPP で定義された親選択メカニズムをオーバーライドして、優先される親にメッシュ AP を強制的に移動できます。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name ap-name mesh parent preferred mac-address 例：	AP のメッシュ パラメータを設定し、メッシュで優先される親の MAC アドレスを設定します。

	コマンドまたはアクション	目的
	<pre>Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:8F</pre>	<p>(注) 優先される親の無線 MAC アドレスを使用してください。</p> <p>Cisco Wave 1 AP の場合、優先される親を設定する際には、目的の親に対して実際のメッシュネイバーの MAC アドレスを指定してください。この MAC アドレスは base radio MAC アドレスで、最後の文字が「f」になります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。</p> <pre>Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:0f</pre> <p>Cisco Wave 2 AP の場合、優先される親を設定すると、MAC アドレスは、最後の 2 文字に「0x11」が追加された base radio MAC アドレスになります。たとえば、base radio MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:11 を指定する必要があります。</p> <pre>Device# ap name ap1 mesh parent preferred 00:24:13:0f:92:11</pre>

AP のロールの変更 (GUI)

手順

- ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
- ステップ 2 [Access Point] をクリックします。
- ステップ 3 [Mesh] タブで、[Role] ドロップダウンリストから [Root] または [Mesh] を選択します。

ステップ 4 [Update & Apply to Device] をクリックします。

ロールの変更がトリガーされると、AP が再起動します。

AP のロールの変更 (CLI)

AP を MAP から RAP (またはその逆) に変更するには、次の手順に従います。

デフォルトでは、AP はメッシュ AP ロールでコントローラに参加します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを開始します。
ステップ 2	ap name ap-name role {mesh-ap root-ap} 例： Device# #ap name ap1 root-ap	ブリッジモードの Cisco AP のロールを変更します。ロールの変更がトリガーされると、AP が再起動します。

メッシュ AP のバッテリー状態の設定 (GUI)

手順

ステップ 1 [Configuration] > [Wireless] > [Mesh] > [Profiles] を選択します。

ステップ 2 プロファイルを選択します。

ステップ 3 [General] タブで、[Battery State for an AP] チェックボックスをオンにします。

ステップ 4 [Update & Apply to Device] をクリックします。

メッシュ AP のバッテリー状態の設定

一部のシスコ屋外 AP には、バッテリー バックアップのオプションが付属しています。ビデオ監視カメラに電力を供給できる PoE 出力も用意されています。外部電源が使用できないとき、内部バッテリーを一時的にバックアップ電源として使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	wireless profile mesh <i>profile-name</i> 例： Device(config)# wireless profile mesh mesh1	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	battery-state 例： Device(config-wireless-mesh-profile)# battery-state	AP のバッテリー状態を設定します。

組み込みワイヤレスコントローラでのメッシュ設定の確認

メッシュ設定の確認

次の **show** コマンドを使用して、メッシュ設定のさまざまな要素を確認します。

- **show wireless mesh stats *ap-name***
- **show wireless mesh security-stats {*all* | *ap-name*}**
- **show wireless mesh queue-stats {*all* | *ap-name*}**
- **show wireless mesh per-stats summary {*all* | *ap-name*}**
- **show wireless mesh neighbor summary {*all* | *ap-name*}**
- **show wireless mesh neighbor detail *ap-name***
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail *bridge-group-name***
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**

- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*
- **show ap environment**
- **show ap gps location**

これらのコマンドの詳細については、『[Cisco Catalyst 9800 Series Wireless Controller Command Reference](#)』ドキュメントを参照してください。

MAC 認証

次の show コマンドを使用して、MAC 認証の設定を確認します。

```
Device# show run aaa
aaa authentication dot1x CENTRAL_LOCAL local
aaa authorization credential-download CENTRAL_AUTHOR local
username 002cc8de4f31 mac
username 00425a0a53b1 mac

ewlc_eft#sh wireless profile mesh detailed madhu-mesh-profile

Mesh Profile Name           : abc-mesh-profile
-----
Description                  :
Bridge Group Name           : bgn-abbc
Strict match BGN            : ENABLED
```



```

Amsdu : ENABLED
...
Battery State : ENABLED
Authorization Method : CENTRAL_AUTHOR
Authentication Method : CENTRAL_LOCAL
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : 802.11n mcs15

```

PSK プロビジョニング

次の show コマンドを使用して、PSK プロビジョニングの設定を確認します。

```

Device# show wireless mesh config
Mesh Config
  Backhaul RRM : ENABLED
  Mesh CAC : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH) : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed : ENABLED
  Rap Channel Sync : ENABLED

Mesh Alarm Criteria
  Max Hop Count : 4
  Recommended Max Children for MAP : 10
  Recommended Max Children for RAP : 20
  Low Link SNR : 12
  High Link SNR : 60
  Max Association Number : 10
  Parent Change Number : 3

Mesh PSK Config
  PSK Provisioning : ENABLED
  Default PSK : ENABLED
  PSK In-use key number : 1
  Provisioned PSKs(Maximum 5)

  Index Description
  -----
  1 key1

```

Bridge Group Name

次の show コマンドを使用して、ブリッジグループ名の設定を確認します。

```

Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name : abc-mesh-profile
-----
Description :
  Bridge Group Name : bgn-abc
  Strict match BGN : ENABLED
  Amsdu : ENABLED
  Background Scan : ENABLED
  Channel Change Notification : DISABLED
  Backhaul client access : ENABLED
  Ethernet Bridging : ENABLED
  Ethernet Vlan Transparent : DISABLED
  Full Sector DFS : ENABLED
  IDS : ENABLED
  Multicast Mode : In-Out
  Range in feet : 12000
  Security Mode : EAP
  Convergence Method : Fast
  LSC only Authentication : DISABLED
  Battery State : ENABLED

```

```

Authorization Method      : CENTRAL_AUTHOR
Authentication Method     : CENTRAL_LOCAL
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : 802.11n mcs15

```

バックホールクライアントアクセス

次の show コマンドを使用して、バックホールクライアントアクセスの設定を確認します。

```

Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
Amsdu                 : ENABLED
Background Scan       : ENABLED
Channel Change Notification : DISABLED
Backhaul client access : ENABLED
Ethernet Bridging     : ENABLED
Ethernet Vlan Transparent : DISABLED
...
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : 802.11n mcs15

```

無線バックホールのデータレート

次の show コマンドを使用して、ワイヤレスバックホールのデータレートの設定を確認します。

```

Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
...
Authorization Method : CENTRAL_AUTHOR
Authentication Method : CENTRAL_LOCAL
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : 802.11n mcs15

```

Dynamic Frequency Selection (動的周波数選択)

次の show コマンドを使用して、動的周波数選択の設定を確認します。

```

Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
Amsdu                 : ENABLED
Background Scan       : ENABLED
Channel Change Notification : DISABLED
Backhaul client access : ENABLED
Ethernet Bridging     : ENABLED
Ethernet Vlan Transparent : DISABLED
Full Sector DFS       : ENABLED
...
Backhaul tx rate(802.11a) : 802.11n mcs15

```

侵入検知システム

次の show コマンドを使用して、ワイヤレスバックホールのデータレートの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
Amsdu                  : ENABLED
Background Scan       : ENABLED
Channel Change Notification : DISABLED
Backhaul client access : ENABLED
Ethernet Bridging     : ENABLED
Ethernet Vlan Transparent : DISABLED
Full Sector DFS       : ENABLED
IDS                  : ENABLED
Multicast Mode        : In-Out
...
Backhaul tx rate(802.11a) : 802.11n mcs15
```

イーサネットブリッジング

次の show コマンドを使用して、イーサネットブリッジングの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
Amsdu                  : ENABLED
Background Scan       : ENABLED
Channel Change Notification : DISABLED
Backhaul client access : ENABLED
Ethernet Bridging     : ENABLED
Ethernet Vlan Transparent : DISABLED
Full Sector DFS       : ENABLED
IDS                   : ENABLED
Multicast Mode        : In-Out
...
Backhaul tx rate(802.11a) : 802.11n mcs15
```

メッシュを介したマルチキャスト

次の show コマンドを使用して、メッシュを介したマルチキャストの設定を確認します。

```
Device# show wireless profile mesh detailed abc-mesh-profile
Mesh Profile Name      : abc-mesh-profile
-----
Description           :
Bridge Group Name     : bgn-abc
Strict match BGN      : ENABLED
Amsdu                  : ENABLED
Background Scan       : ENABLED
Channel Change Notification : DISABLED
Backhaul client access : ENABLED
Ethernet Bridging     : ENABLED
Ethernet Vlan Transparent : DISABLED
Full Sector DFS       : ENABLED
IDS                   : ENABLED
Multicast Mode       : In-Out
```

```
...
Backhaul tx rate(802.11a)      : 802.11n mcs15
```

メッシュバックホールの RRM

次の show コマンドを使用して、メッシュバックホールの RRM の設定を確認します。

```
Device# show wireless mesh config
Mesh Config
  Backhaul RRM                : ENABLED
  Mesh CAC                    : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH) : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed    : ENABLED
  Rap Channel Sync                : ENABLED

Mesh Alarm Criteria
  Max Hop Count                : 4
  Recommended Max Children for MAP : 10
  Recommended Max Children for RAP : 20
  Low Link SNR                 : 12
  High Link SNR                : 60
  Max Association Number       : 10
  Parent Change Number        : 3

Mesh PSK Config
  PSK Provisioning             : ENABLED
  Default PSK                  : ENABLED
  PSK In-use key number        : 1
  Provisioned PSKs(Maximum 5)

  Index   Description
  -----
  1       key1
```

優先される親 (Preferred Parent) の選択

次の show コマンドを使用して、優先される親の設定を確認します。

```
Device# show wireless mesh ap tree
=====
AP Name [Hop Ctr,Link SNR,BG Name,Channel,Pref Parent,Chan Util,Clients]
=====

[Sector 1]
-----
1542-RAP [0, 0, bgn-madhu, (165), 0000.0000.0000, 1%, 0]
  |-MAP-2700 [1, 67, bgn-madhu, (165), 7070.8b7a.6fb8, 0%, 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
```

AP ロールの変更

次の show コマンドを使用して、AP ロールの変更の設定を確認します。

```
Device# show wireless mesh ap summary
AP Name                AP Model BVI MAC                BGN                AP Role
-----                -
-----                -
-----                -
-----                -
```

```

1542-RAP                1542D    002c.c8de.1338 bgn-abc  Root AP
MAP-2700                2702I    500f.8095.01e4 bgn-abc  Mesh AP

Number of Bridge APs      : 2
Number of RAPs            : 1
Number of MAPs            : 1
Number of Flex+Bridge APs : 0
Number of Flex+Bridge RAPs : 0
Number of Flex+Bridge MAPs : 0

```

メッシュリーフノード

次の show コマンドを使用して、メッシュリーフノードの設定を確認します。

```

Device# show ap name MAP-2700 config general
Cisco AP Name      : MAP-2700
=====

Cisco AP Identifier      : 7070.8bbc.d3e0
Country Code            : Multiple Countries : IN,US,IO,J4
Regulatory Domain Allowed by Country : 802.11bg:-AEJPQU 802.11a:-ABDJNPQU
AP Country Code         : IN - India
AP Regulatory Domain
  Slot 0                 : -A
  Slot 1                 : -D
MAC Address             : 500f.8095.01e4
...
AP Mode                : Bridge
Mesh profile name      : abc-mesh-profile
AP Role                : Mesh AP
Backhaul radio type    : 802.11a
Backhaul slot id       : 1
Backhaul tx rate      : auto
Ethernet Bridging     : Enabled
Daisy Chaining          : Disabled
Strict Daisy Rap        : Disabled
Bridge Group Name     : bgn-abc
Strict-Matching BGN    : Enabled
Preferred Parent Address : 7070.8b7a.6fb8
Block child state     : Disabled
PSK Key Timestamp       : Not Configured
...
FIPS status             : Disabled
WLANCC status           : Disabled
GAS rate limit Admin status : Disabled
WPA3 Capability         : Disabled
EWC-AP Capability       : Disabled
AWIPS Capability        : Disabled
Proxy Hostname          : Not Configured
Proxy Port               : Not Configured
Proxy NO_PROXY list     : Not Configured
GRPC server status      : Disabled

```

サブセットチャネルの同期

次の show コマンドを使用して、サブセットチャネルの同期の設定を確認します。

```

Device# show wireless mesh config
Mesh Config
  Backhaul RRM           : ENABLED
  Mesh CAC                : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH) : ENABLED
  Mesh Ethernet Bridging STP BFDU Allowed : ENABLED

```

```
Rap Channel Sync : ENABLED
```

```
Mesh Alarm Criteria
```

```
Max Hop Count : 4
Recommended Max Children for MAP : 10
Recommended Max Children for RAP : 20
Low Link SNR : 12
High Link SNR : 60
Max Association Number : 10
Parent Change Number : 3
```

```
Mesh PSK Config
```

```
PSK Provisioning : ENABLED
Default PSK : ENABLED
PSK In-use key number : 1
Provisioned PSKs(Maximum 5)
```

```
Index Description
-----
1 key1
```

ブリッジモードおよびメッシュ AP 用の LSC のプロビジョニング

次の show コマンドを使用して、ブリッジモードおよびメッシュ AP 用の LSC のプロビジョニングに関する設定を確認します。

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name : default-mesh-profile
-----
Description : default mesh profile
Bridge Group Name : bgn-abc
Strict match BGN : DISABLED
Amsdu : ENABLED
Background Scan : ENABLED
Channel Change Notification : ENABLED
Backhaul client access : ENABLED
Ethernet Bridging : DISABLED
Ethernet Vlan Transparent : ENABLED
Full Sector DFS : ENABLED
IDS : DISABLED
Multicast Mode : In-Out
Range in feet : 12000
Security Mode : EAP
Convergence Method : Fast
LSC only Authentication : DISABLED
Battery State : ENABLED
Authorization Method : default
Authentication Method : default
Backhaul tx rate(802.11bg) : auto
Backhaul tx rate(802.11a) : auto
```

ルート AP のバックホールスロットの指定

次の show コマンドを使用して、ルート AP のバックホールスロットの設定を確認します。

```
Device# show ap name 1542-RAP mesh backhaul
MAC Address : 380e.4d85.5e60
Current Backhaul Slot: 1
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
```

```

Operation State: Up
Current Tx Power Level:
Current Channel: (165)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 18

```

メッシュバックホールでのリンクテストの使用

次の show コマンドを使用して、メッシュバックホールでのリンクテストの使用の設定を確認します。

```

Device# show ap name 1542-RAP mesh linktest data 7070.8bbc.d3ef
380e.4d85.5e60 ==> 7070.8bbc.d3ef

```

```

Started at : 05/11/2020 20:56:28
Status: In progress

```

```

Configuration:
=====
Data rate: Mbps
Packets per sec: : 234
Packet Size: : 1200
Duration: : 200

```

メッシュ CAC

次の show コマンドを使用して、メッシュ CAC の設定を確認します。

```

Device# show wireless mesh config
Mesh Config
  Backhaul RRM : ENABLED
  Mesh CAC : DISABLED
  Outdoor Ext. UNII B Domain channels(for BH) : ENABLED
  Mesh Ethernet Bridging STP BPDU Allowed : ENABLED
  Rap Channel Sync : ENABLED

Mesh Alarm Criteria
  Max Hop Count : 4
  Recommended Max Children for MAP : 10
  Recommended Max Children for RAP : 20
  Low Link SNR : 12
  High Link SNR : 60
  Max Association Number : 10
  Parent Change Number : 3

Mesh PSK Config
  PSK Provisioning : ENABLED
  Default PSK : ENABLED
  PSK In-use key number : 1
  Provisioned PSKs(Maximum 5)

  Index Description
  -----
  1 key1

```

メッシュコンバージョンの確認

次に、使用されたメッシュコンバージョン方式を表示する show wireless profile mesh detailed コマンドの出力例を示します。

```
Device# show wireless profile mesh detailed default-mesh-profile

Mesh Profile Name          : default-mesh-profile
-----
Description                : default mesh profile
Convergence Method        : Fast
```

次に、選択されたブリッジグループ名のサブセットチャンネルを表示する `show wireless mesh convergence subset-channels` コマンドの出力例を示します。

```
Device# show wireless mesh convergence subset-channels

Bridge group name          Channel
-----
Default                    132
```

メッシュバックホールの確認

次に、2.4 GHz でのメッシュバックホールの詳細を表示する `show ap name mesh backhaul` コマンドの出力例を示します。

```
Device# show ap name test-ap mesh backhaul

MAC Address : xxxx.xxxx.xxxx
Current Backhaul Slot: 0
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
Operation State: Up
Current Tx Power Level:
Current Channel: (11)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 0
```

次に、メッシュバックホールの詳細を表示する `show wireless mesh ap backhaul` コマンドの出力例を示します。

```
Device# show wireless mesh ap backhaul

MAC Address : xxxx.xxxx.xxxx
Current Backhaul Slot: 0
Radio Type: 0
Radio Subband: All
Mesh Radio Role: DOWNLINK
Administrative State: Enabled
Operation State: Up
Current Tx Power Level:
Current Channel: (11)
Antenna Type: N/A
Internal Antenna Gain (in .5 dBm units): 0
```

メッシュ イーサネット デイジー チェーン接続の確認

- 次に、永続的 SSID が AP に設定されているかどうかを表示する `show ap config general` コマンドの出力例を示します。

```
Device# show ap 3702-RAP config general

Persistent SSID Broadcast          Enabled/Disabled
```


- 次に、すべてのブリッジRAPの永続的SSIDブロードキャストステータスを表示する `show wireless mesh persistent-ssid-broadcast summary` コマンドの出力例を示します。

```
Device# show wireless mesh persistent-ssid-broadcast summary

  AP Name      AP Model BVI MAC          BGN          AP Role          Persistent
  SSID state
  -----
  3702-RAP     3702    5c71.0d07.db50  ap_name     Root AP          Enabled
  1560-RAP     1562E   380e.4dbf.c6b0  ap_name     Root AP          Disabled
```

メッシュバックホールでの Dot11ax レートの確認

メッシュプロファイルのメッシュバックホールの 802.11ax レートを確認するには、次のコマンドを使用します。

```
Device# show wireless profile mesh detailed default-mesh-profile
Mesh Profile Name          : default-mesh-profile
-----
Description                : default mesh profile
.
.
Backhaul tx rate(802.11bg) : 802.11ax mcs7 ss1
Backhaul tx rate(802.11a)  : 802.11ax mcs9 ss2
```

AP の一般的な設定でメッシュバックホールの 802.11ax レートを確認するには、次のコマンドを使用します。

```
Device# show ap config general
Cisco AP Identifier        : 5c71.0d17.49e0
.
.
Backhaul slot id          : 1
Backhaul tx rate          : 802.11ax mcs7 ss1
```

