Cisco Catalyst 9800 Series Configuration Best Practices

マニュアルの変更履歴

2025 年 12 月 19 日

- 新しいセクション
  - 「RADIUS ネットワークデバイス設定」セクションを追加

2025 年 11 月 27 日

- 新しいセクション
  - 「AP 負荷分散の概要」セクションを追加
  - 「ジャンボフレームのサポートと「ip mtu」インターフェイスコマンド」セクションを追加
  - 「グローバル ユース アクセス ポイント」セクションを追加
  - 「プライマリへの AP フォールバック」セクションを追加
  - 「アクセスポイント向けの Cisco Discovery Protocol（CDP）」セクションを追加
  - 「DHCP スコープおよびリース設計に関する考慮事項」セクションを追加
  - 「802.11v」セクションを追加
  - 「WPA3」セクションを追加
  - 「Web 認証」セクションを追加
  - 「RADIUS 中間アカウンティング」セクションを追加
  - 「6 GHz 設計」セクションを追加
  - 「高スループット」セクションを追加
- 更新されたセクション
  - 「RF ベースの自動 AP 負荷分散による設計の強化」セクションを更新
  - 異なるタイマーについて説明する「プライマリ/セカンダリ/ターシャリとバックアッププライマリ/バックアップセカンダリの違い」セクションを更新
  - 正しいコマンドと更新されたスクリーンショットによって「トラストポイントの取り扱い」セクションを更新
  - 帯域ごとの SSID の推奨最大数を明確にするために「SSID の数の削減」セクションを更新
  - RF グループ名に関する注を含めるために「RF グループ」セクションを更新
- その他の変更
  - 新しい CW9800 コントローラの仕様を追加

2024 年 5 月 3 日

- 新しいセクション
  - 「大規模展開向けの設計」：AP から WNCd へのマッピング、サイトタグの設計、機能、および推奨事項
  - 「アクセスポイントのコンソールボーレート」：17.12.1 以降の変更と変更にともなう推奨事項

- 更新されたセクション
  - 「サービスポートの使用」：サポートされているプロトコルのリストを更新
  - 「ワイヤレス クライアント インターフェイス」：クライアント SVI 上のアクセス制御リスト（ACL）に関する推奨事項
  - 「クライアントタイマー」：セッションおよび除外タイムアウトに関する推奨事項を改訂
  - 「802.11r 高速移行の有効化」：適応型 802.11r の代わりに 802.11r 混合モードを設定するための推奨事項を更新

はじめに

Cisco® Catalyst® 9800 シリーズ（C9800）は、シスコの次世代ワイヤレス LAN コントローラです。25 年間にわたってワイヤレス業界をリードして培った RF の卓越性と、モジュール化され、拡張に優れた、セキュアな最新のオペレーティングシステムである Cisco IOS® XE ソフトウェアが統合されています。Catalyst ワイヤレスソリューションは、ネットワークの卓越性に関する 3 つの主要な柱であるレジリエンシ、セキュリティ、インテリジェンスに基づいて構築されています。

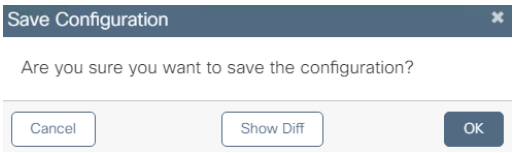
AireOS WLC と比較して、C9800 ソフトウェアは、Cisco IOS XE の利点を活用するためにゼロから書き直されており、設定モデルもよりモジュール化され、柔軟性が向上しています。つまり、ほとんどの AireOS 機能は維持されていますが、特定の機能の設定方法が変更されている場合があります。

このガイドでは、一般的な Cisco Catalyst 9800 シリーズ ワイヤレス インフラストラクチャの設定に推奨されるベストプラクティスについて説明します。この章の目的は、大部分のワイヤレスネットワークの実装に適用できる共通設定を示すことにあります。ただし、すべてのネットワークが同じであるわけではありません。一部のヒントはインストール時に適用できない場合があります。適用できない内容については、稼働中のネットワークに変更を加える前に必ず確認してください。

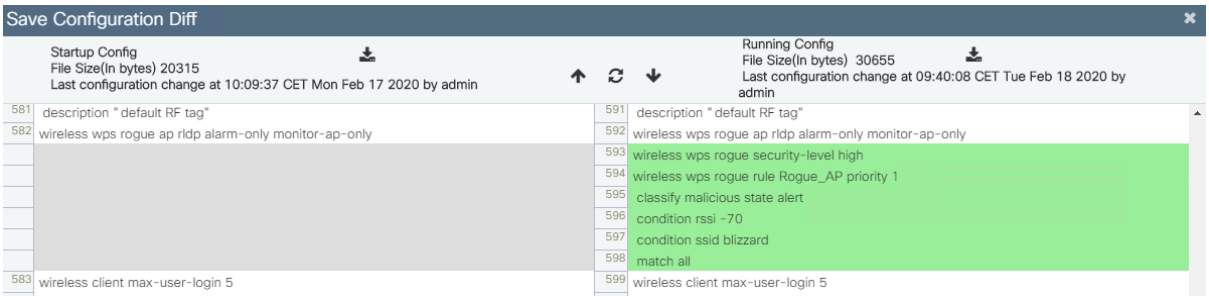
このガイドに関する注意事項

ガイドの最初の部分では、Catalyst 9800 ワイヤレスコントローラのいくつかの重要な設定および設計コンセプトに焦点を当てています。これらは、ガイドの残りの部分に示されているベストプラクティスを理解するために役立ちます。このガイドは、一般設定、ネットワーク設定、無線周波数（RF）設定、セキュリティ設定などに関するセクションに編成された推奨設定のリストになっています。

利用可能な場合、これらの設定は Catalyst 9800 の新しいグラフィカル ユーザー インターフェイス（GUI）を使用して表示されます。これは、GUI が大幅に改善されており、容易に操作できるためです。特定の GUI 設定に対応するコマンド ライン インターフェイス（CLI）コマンドを確認する場合、C9800 には非常に便利で簡単な方法があります。GUI を使用して目的の設定を適用し、右上隅にある [保存（Save）] アイコン をクリックします。次のポップアップウィンドウで、[差分の表示（Show Diff）] を選択してください。



これにより、既存の設定と新しい設定を比較できる別のウィンドウが開きます。異なるコマンドが強調表示されます。緑色は新しいコマンド、オレンジ色は変更されたコマンド、赤色は削除されたコマンドを示します。次は、新しい不正管理設定の例です。



各推奨設定は、既知の制限事項がある場合、または特定のリリースのコードに適用される場合に強調表示されます。また、AireOS との相違点には下線が付けられます。

このガイドの情報は、特定のラボ環境でのデバイスのテストに基づいています。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

前提条件

次の項目に関する知識が推奨されます。

- シスコのワイヤレス互換性マトリックスに記載された、サポートされている互換リリースに関する最新情報：https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html、およびアクセスポイントでサポートされている機能に関する最新情報：https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html
- シスコは、IOS XE の推奨リリースのリストをこちらで公開しています：https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214749-tac-recommended-ios-xe-builds-for-wirele.html
- 実装を計画している特定のソフトウェアのリリースノートを必ず確認してください：https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html
- 新しい Cisco Catalyst 9800 ワイヤレスコントローラの設定モデル。詳細をこちらで確認してください：https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213911-understand-catalyst-9800-wireless-contro.html

- このガイドで説明している機能のほとんどは、次のいずれかのドキュメントに記載されています。設定ガイド：https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html

  または、テクニカルリファレンス：

  https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-configuration-examples-list.html

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。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォーム（明示的に指定されていない限り、すべてのプラットフォーム）。これには、CW9800 プラットフォームも含まれます。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア（明示的に指定されていない限り、推奨事項はすべてのリリースで有効）。
- Cisco 802.11be（Wi-Fi 7）、802.11ax（Wi-Fi 6 および 6E）、802.11ac（Wi-Fi 5）アクセスポイント。

Cisco Catalyst 9800 シリーズの新しい設定モデル

まず、簡単に総括します。Cisco Catalyst 9800 シリーズの新しい設定モデルは、プロファイルとタグの 2 つの構成要素に基づいています。プロファイルは一連の機能をグループ化し、タグを使用すると、それらの機能を AP に割り当てることができます。プロファイルには次の 5 つのタイプがあります。

- **AP 参加プロファイルまたは AP プロファイル**：Control And Provisioning of Wireless Access Points（CAPWAP）タイマー、802.1X サプリカント、SSH/Telnet 設定などの一般的な AP 設定が含まれます。AireOS におけるこれらの設定は、通常、すべての AP に対するグローバル設定です。
- **WLAN プロファイル**：SSID 名およびプロファイルと、すべてのセキュリティ設定を定義します。
- **ポリシープロファイル**：WLAN に関連付けられるポリシー機能が含まれます。クライアント VLAN、認証、認可、アカウンティング（AAA）、アクセス制御リスト（ACL）、セッション、アイドルタイムアウトなどの設定を指定します。
- **Flex プロファイル**：Flex AP に割り当てられるすべての設定（ネイティブ VLAN、ACL マッピングなど）をグループ化します。
- **RF プロファイル**：AireOS と同様に、各帯域の RF 特性を定義します。

タグを使用すると、プロファイルの設定をアクセスポイントにバインドできます。タグには次の 3 つのタイプがあります。

- **ポリシータグ**：ポリシープロファイルと WLAN を結び付けます。
- **サイトタグ**：AP に AP 参加プロファイル設定を割り当て、サイトがローカルサイトであるかどうかを決定します。ローカルサイトである場合、AP はローカルモードになり、ローカルサイトでない場合、AP は Cisco FlexConnect® モードになります。
- **RF タグ**：6-GHz、5-GHz、および 2.4-GHz プロファイルを AP にバインドします。

アクセスポイントには、常に 3 つのタグ（タイプごとに 1 つ）が割り当てられます。タグが明示的に定義されていない場合、AP はデフォルトのポリシー、サイト、または RF タグを取得します。

C9800 設定モデルにより、特定のワイヤレス展開に合わせて設定を調整する際の柔軟性が大幅に向上します。TCP MSS 調整の設定を例に説明します。AireOS では、これがグローバル設定であるため、各ロケーションのすべての AP に同じ値が適用されるか、デフォルトのままにされます。新しい設定モデルでは、TCP MSS 調整値が AP 参加プロファイルレベルで設定されるため、各サイトの転送ネットワークを評価し、特定の AP グループに最適な値を決定することができます。このことはすべての設定に当てはまり、大きな付加価値となっています。

Cisco Catalyst 9800 シリーズのプロファイルとタグに関する考慮事項

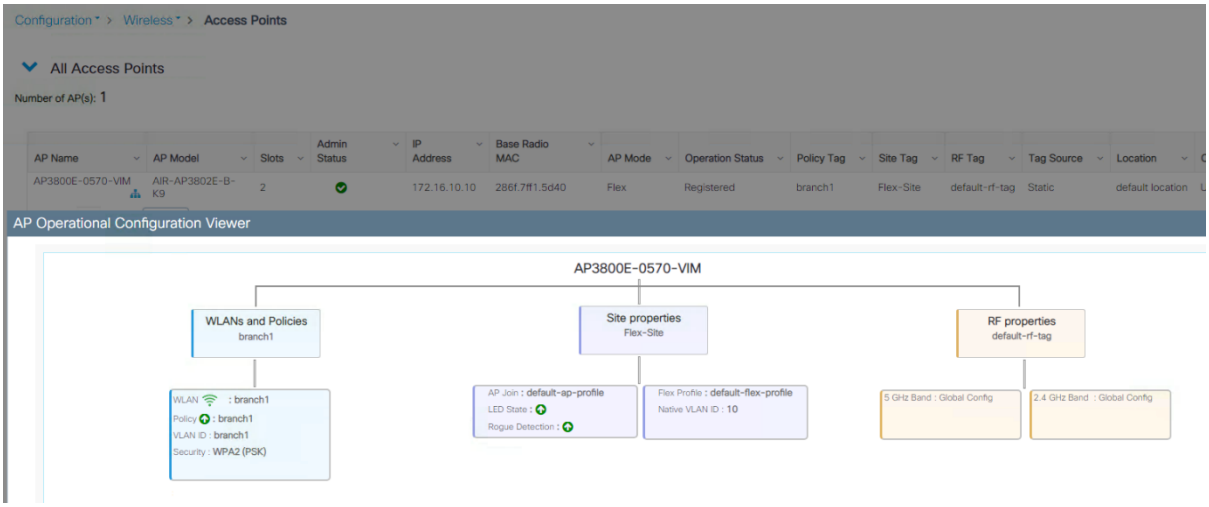
前述したように、C9800 では、一部の設定の方法が AireOS と異なっています。これは、設定をより柔軟に、より簡単に使用できるようにするためです。AireOS ワイヤレスコントローラで慣れている機能は C9800 でもサポートされていますが、それらを利用するには設定モデルに習熟する必要があります。さらに、新しい設定モデルは、C9800 でサポートされる独自の新たな機能に拡張できるように作成されています。

次のセクションでは、プロファイルとタグのベストプラクティスについて説明し、それらを最大限に活用する方法に関するヒントを提供します。

タグの割り当て

各アクセスポイントには、ポリシータグ、サイトタグ、および RF タグの 3 つの固有タグを割り当てる必要があります。デフォルトでは、AP は、C9800 ワイヤレスコントローラに参加するとデフォルトのタグ（デフォルトポリシータグ、デフォルトサイトタグ、およびデフォルト RF タグ）を取得します。ユーザーは、デフォルトのタグを変更したり、カスタムタグを作成することができます。各 AP で設定されているタグを確認するには、GUI に移動します。

また、AP の横にある アイコンをクリックしてポップアップウィンドウを開き、詳細を確認することもできます。



これにより、SSID がブロードキャストされているかどうかを確認できます（ブロードキャストされていないと緑色ではなく灰色になる）。タグに関する設定ミスがあると、 アイコンが赤色になります。

CLI で、`show ap tag summary` コマンドを使用します。

```
LabW-9800M1#show ap tag summary
Number of APs: 3

AP Name                          AP Mac          Site Tag Name                 Policy Tag Name               RF Tag Name                   Misconfigured  Tag Source
-------------------------------------------------------------------------------------------------------------------------------------------------------
C9130-SJ-1                       0c75.bdb5.fab8  default-site-tag              default-policy-tag            default-rf-tag                No             Static
C9120-SJ-1                       6c41.0e16.5184  default-site-tag              default-policy-tag            default-rf-tag                No             Static
APCC6E.2ACA.F590                 cc6e.2aca.f590  default-site-tag              default-policy-tag            default-rf-tag                No             Default
```

このコマンドにより、タグおよびプロファイルに関する設定ミスがあるかどうかが明確に示されます。タグに関する設定ミスの典型的な例は、AVC（Application Visibility and Control）設定が異なる 2 つの異なるポリシープロファイルに同じ WLAN を割り当てることです。この場合、`show avc status <WLAN name>` コマンドにより、エラーとしてフラグが付けられ、関連する説明も示されます。

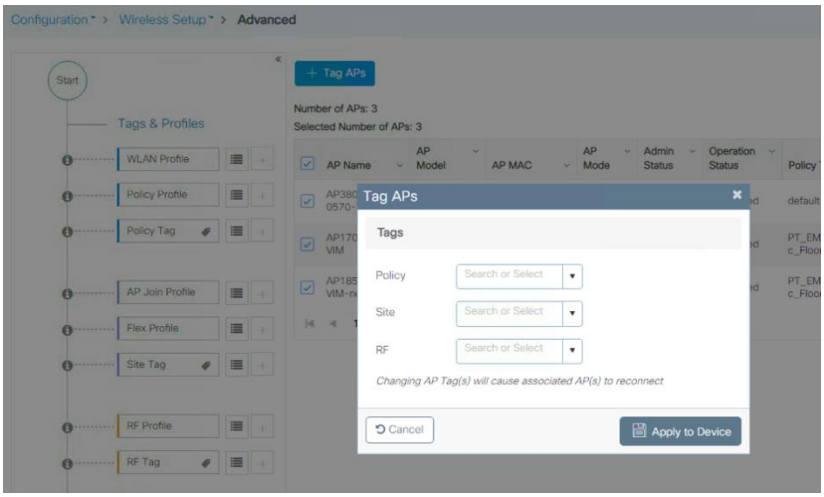
上記のコマンドの出力にある [タグソース（Tag Source）] フィールドを確認してください。これは、AP がタグを取得した方法を示しています。考えられるソースは、優先順位の順に次のとおりです。

- **静的**：AP を選択し、特定のタグを割り当てます。この設定は、AP のイーサネット MAC アドレスに基づいてコントローラに保存されます。AP がその特定のコントローラに参加すると、指定されたタグが常に割り当てられます。
- **ロケーション**：これは C9800 の内部設定構造であり（各 AP で設定できる AP ロケーションではなく）、主に基本セットアップフローで使用されます。ロケーションにより、3 つのタグ（ポリシー、サイト、および RF）のグループを作成し、それに AP を割り当てることができます。
- **フィルタ**：正規表現を使用して、コントローラに参加する AP にタグを割り当てることができます。現時点では、AP 名に基づいてのみフィルタを設定できるため、この方法は初期状態の AP には使用できません。また、同じフィルタで AP プライミングプロファイル（後にある「予測参加の設定：プライマリ/セカンダリ/ターシャリコントローラ」セクションを参照）を利用して、プライマリ、セカンダリ、およびターシャリコントローラを割り当てることもできます。
- **AP**：AP 自体は、プラグアンドプレイ（PnP）を介して学習した、またはコントローラからプッシュされたタグ情報を保持します。
- **デフォルト**：これはデフォルトのタグソースです。

最初の 2 つのソース（静的およびロケーション）は、AP をタグに割り当てるための静的マッピング設定であるため、優先順位が最も高くなります。フィルタを使用すると、正規表現に基づいて、AP からタグへの動的なマッピングを定義できます。ソースが AP である場合は、この情報が AP 自体に保存されており、AP が参加したときにそれがコントローラに提示されることを意味します。最後に、C9800 にタグマッピング設定がなく、AP がタグ情報を保持していない場合、AP にはデフォルトのタグが割り当てられます。

一連のタグに複数の AP を割り当てる簡単な方法は、GUI で詳細セットアップ（[設定（Configuration）] > [ワイヤレスのセットアップ（Wireless Setup）] > [詳細（Advanced）]）を使用することです。メインページで [今すぐ開始（Start Now）] をクリックしてから、[適用（Apply）] セクションに移動し、アイコンをクリックして AP リストを表示させます。

次のページで、目的の AP を選択し、[+ AP のタグを付け（+ Tag APs）] をクリックして、ポップアップウィンドウでタグを割り当てます。



ソフトウェアリリース 17.6 以降では、「AP タグ永続化」機能を利用して、タグを AP に自動的に保存できます。これは、CLI コマンドを使用してコントローラでグローバルに有効化されます。

```
C9800(config)#ap tag persistency enable
```

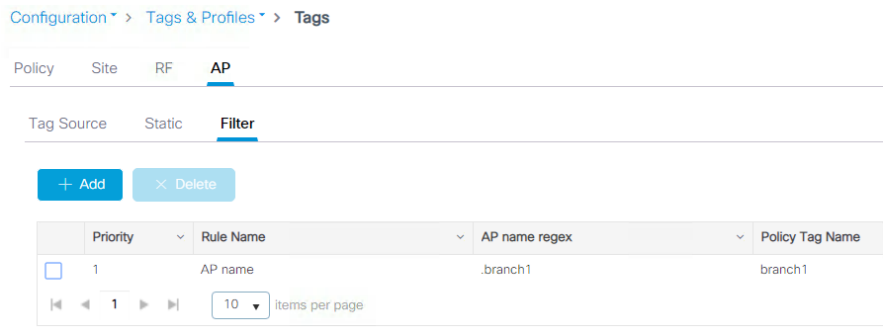
17.6 以降では、以前のリリースとの後方互換性のために、この機能はデフォルトで無効になっていますが、シスコでは有効にすることをお勧めします。タグ永続化機能が有効になっている場合、AP が C9800 ワイヤレスコントローラに参加すると、設定されたタグが自動的に AP に保存されます。

AP タグ永続化が導入される前は、AP にタグをプッシュして保存するために、単一の AP ごとに EXEC モードで CLI コマンドを使用する必要がありました。

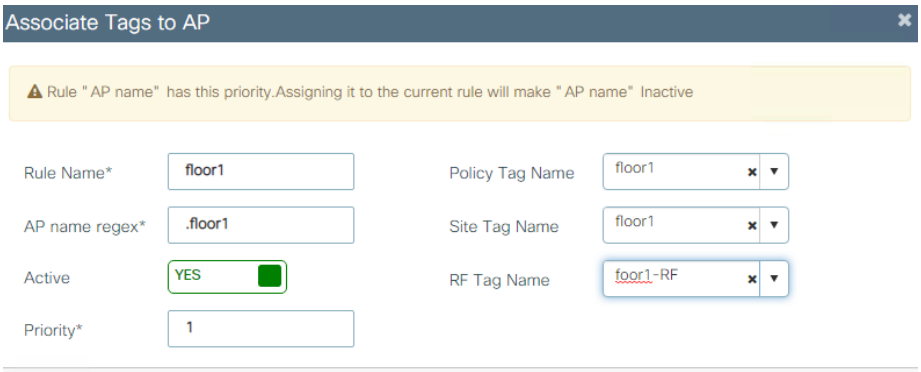
```
C9800#ap name <APname> write tag-config
```

AP タグ永続化機能の運用上の利点は、ワイヤレスコントローラ間で AP を移動する必要がある場合に明確になります。これは、AP 移行のコンテキストにおいて、またはプライマリ/セカンダリ（N+1）高可用性展開において発生する可能性があります。タグは AP に保存されているため、AP がセカンダリ WLC に参加するとタグが提示され、それらがコントローラに存在している場合、そのマッピングが適用されます。当然のことながら、タグソースの優先順位は依然として適用され、AP タグソースは、その AP に対して静的マッピングまたはフィルタベースのマッピングがない場合にのみ考慮されます。

あるコントローラから別のコントローラに AP を移動するときにタグを維持する別の方法は、AP タグフィルタを使用することです。フロア 1 にある AP を WLC1 から WLC2 に移動するとします。また、AP には、「APx_floor1」（「x」は AP 番号）という命名方法で名前が付けられているとします。両方のコントローラで必要なタグを設定し、その後に WLC2 で、「floor1」で終わる任意の AP 名と一致するフィルタルールを設定して、それを目的のタグに割り当てる必要があります。[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [タグ（Tags）] に移動し、[フィルタ（Filter）] をクリックします。

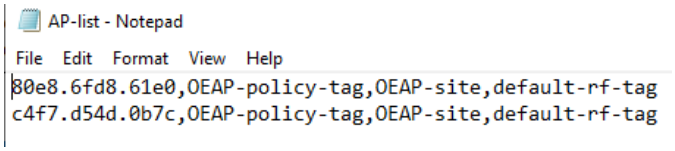


上のページで [+ 追加（+ Add）] をクリックすることにより、新しいルールを追加できます。次に、「floor1」で終わる任意の AP 名と一致するルールの例を示します。

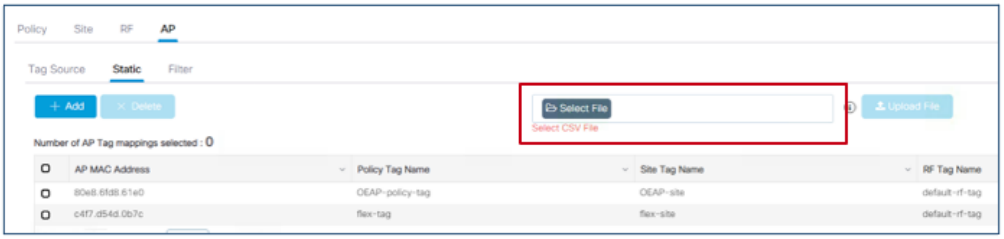


最後に、CSV ファイルを使用して AP とタグのマッピングを事前に設定することで、別のコントローラに参加するときに AP に正しいタグが割り当てられるようにすることができます。これは、次の 2 つの手順で簡単に実行できます。

- まず、CSV ファイルを作成します。これは、「AP のイーサネット MAC, ポリシータグ名, サイトタグ名, RF タグ名」という特定の形式である必要があります。次に例を示します。



- 次のスクリーンショットに示すように、[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [タグ（Tags）] に移動して、CSV ファイルをロードします。



既存のタグを変更したり、新しいタグを作成したり、さまざまな方法でそれらを AP に付加することができるので、不整合を検出するために、EXEC モードで次のコマンドを使用してタグ設定を検証することが推奨されます。

```
C9800#wireless config validate
```

コントローラ間での AP の移動とタグの維持

前の段落で、C9800 が AP へのタグのマッピングを処理する方法について説明しました。この情報を踏まえて、2 つの C9800 ワイヤレスコントローラ（C9800-1 と C9800-2）の間で AP を移動する場合は、次の点を考慮する必要があります。

- C9800-1 上の AP がタグ情報を保持しておらず（AP タグ永続化機能または `ap name <APname> write tag-config` コマンドのいずれによっても）、C9800-2 でその AP に対してマッピングが設定されていない場合、その AP が C9800-2 に移動するとデフォルトのタグが割り当てられます。
- AP がコントローラ間を移動する際、両方のコントローラが AP とタグのマッピングに関して同じ情報を持っている場合、AP はタグ情報を保持します。これは、静的設定を介して、AP をロケーションに割り当てることによって、またはタグフィルタを使用して実行できます。
- また、タグが AP 自体に保存されており（AP タグ永続化機能または `ap name <APname> write tag-config` コマンドのいずれかによる）、そのタグが両方のコントローラで定義されており、より優先順位の高いマッピングが定義されていない（たとえば、静的設定によって C9800-2 で AP に別のタグセットが割り当てられることによって）場合にも、AP は、2 つのコントローラ間で移動してもタグを保持します。
- AP が、タグを保存しており、それらのタグが定義されていないコントローラに参加する場合、その AP にはデフォルトのタグに割り当てられます（AP が参加しているコントローラで他のマッピングが設定されていない限り）。
- どの場合でも、AP がタグ名の割り当てを保持しており、タグ内の設定が 2 つのコントローラで異なるときは、現在参加しているコントローラに存在する設定に基づいて AP が設定されます。

注： 上記の情報は、N+1 冗長化にも適用されます。

AireOS コントローラから C9800 コントローラに AP を移動する場合は、AP が AireOS からのタグ情報を引き継がないため、デフォルトのタグにマッピングされます。ただし、前述したように、C9800 コントローラで静的または動的タグの事前割り当てが行われている場合は、この限りではありません。

ポリシータグ間のローミング

ポリシータグは、どの SSID がどの AP によってどのポリシーでブロードキャストされるかを決定するために使用されます。つまり、ポリシータグにより、AP のグループのブロードキャストドメインが定義されます。この点において、ポリシータグは、AireOS における AP グループの概念に非常によく似ています。

デフォルトでは、同じ SSID で設定されているにもかかわらず関連するポリシーが異なる 2 つの AP 間でクライアントをローミングする場合、スローローミングになります。言い換えると、2 つの異なるポリシータグ（SSID は同じであるがポリシープロファイル名が異なる）間でローミングすると、クライアントは、完全な認証と DHCP プロセスによる IP アドレスの更新を強制されます。これは、コントローラ内ローミングを実行する場合にも適用されます。これは、クライアントが完全な再認証なしでポリシー間を移動するのを防ぐためです。

注： SSID に関連付けられているポリシープロファイルが、異なるポリシータグで同じ（名前も内容も同じ）である場合、その SSID のローミングはシームレスになります。SSID に関連付けられているポリシープロファイルに変更があると、スローローミングになります。

C9800 を使用してワイヤレスネットワークを設計する際は、この点を考慮する必要があります。たとえば、大学においてキャンパス全体で /22 サブネットを使用するルールがある顧客ユースケースがあるとします。さらに、ネットワーク全体で 1 つの教職員用 SSID を使用しており、ユーザー数が 1022 人を超えるために SSID に複数のクライアントサブネットを割り当てる必要があるとします。

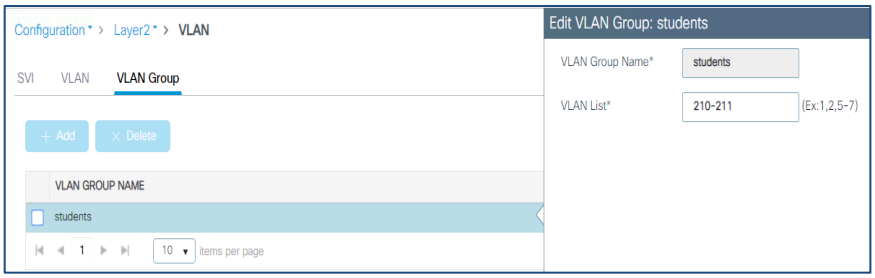
AireOS では、これを実装する一般的な方法が 3 つあります。

1. AAA サーバーからの VLAN オーバーライドを使用して、異なるユーザーグループを異なるサブネット /VLAN に割り当てます。
2. VLAN Select（別名、インターフェイスグループ機能）を使用して、複数のクライアントサブネットを同じ SSID にマッピングし、グループ内の利用可能な VLAN にラウンドロビン方式でクライアントを割り当てます。
3. AP グループを使用して、AP のグループごとに特定の VLAN を SSID にマッピングします。これにより、クライアントがそのロケーション（AP のグループ）に参加する際に、そのクライアントが属する IP サブネットをユーザーが確実に把握できるようにもなります。

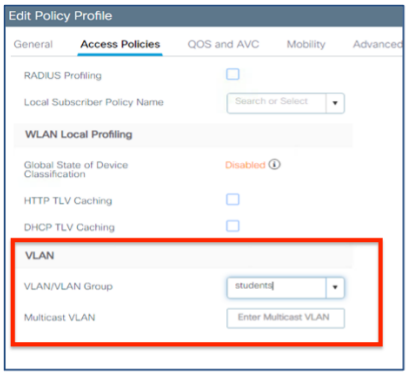
オプション 1 は、C9800 で完全にサポートされています。VLAN グループと呼ばれる、AireOS の VLAN Select に似た機能を利用することでオプション 2 を使用することもできます。Cisco Catalyst ワイヤレスコントローラでは、クライアント VLAN に関連付けられたレイヤ 3 インターフェイスは必要ないため、レイヤ 2 VLAN をグループ化できることを思い出してください。

注： クライアントに静的 IP があり、VLAN グループを使用している場合は、VLAN グループ内の各 VLAN に SVI を設定する必要があります。設定しないと、そのクライアントは除外されます。詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_conf_vlan_grp_vewlc.html#vlan-grp-supp-dhcp-stat-ip-cl を参照してください。

最初に VLAN グループを設定し、VLAN（この例では VLAN 210 および 211）を割り当てます。



その後に、SSID を定義済みの VLAN グループにマッピングするようにポリシープロファイルを設定します。



さらに、SSID がこのポリシーにマッピングされている同一のポリシータグに、すべての AP を割り当てます。

オプション 3 の場合は、2 つのポリシープロファイル（VLAN 210 を使用するものと VLAN 211 を使用するもの）を定義し、それらを、異なるポリシータグを使用して同じ SSID にマッピングする必要があります。その後に、異なるポリシータグを異なる AP グループに適用します。この場合は、前述したポリシータグ間でのスローローミングの制限を考慮する必要があります。2 つのロケーションが離れており、エアギャップがある場合は、いずれにしてもクライアントが切断される必要があるため、問題はありません。ただし、ロケーションが同じローミングドメイン内にある場合は、異なる VLAN を持つ 2 つのポリシータグ間でクライアントがローミングするときに完全な再認証が行

われることを考慮する必要があります。これは AireOS の動作とは異なります。AireOS WLC では、異なる VLAN にマッピングされた 2 つの AP グループ間でもシームレスなローミングが可能です。

Cisco IOS XE リリース 17.3 以降、ポリシープロファイルの違いが特定のパラメータ（VLAN と ACL が最も重要）のみである場合、ポリシープロファイル（および関連するポリシータグ）間でシームレスなローミングが可能になります。機能を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
C9800(config)#wireless client vlan-persistant
```

このコマンドには「VLAN」としか書かれていませんが、実際には、2 つのポリシープロファイル間で異なっていてもシームレスなローミングになる他のパラメータが多数あります。これらの属性の完全なリストについては、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_client_roaming_policy_profile.html を参照してください。

ポリシータグの割り当てを設計する際には、「同じローミングドメイン内のすべての AP は同じポリシープロファイルを持つ必要があり、異なるポリシーを割り当てる必要がある場合は、リリース 17.3 以降を展開して *wireless client vlan-persistant* 機能を使用することが推奨される」という動作について考慮することをお勧めします。

大規模展開向けの設計

ハイエンドモデルの Catalyst 9800 ワイヤレス LAN コントローラは、単一のプラットフォームで最大 6,000 の AP と 64,000 のクライアントをサポートしています。これは非常に多くの AP とクライアントです。大規模で高密度の展開を処理する場合は、WLC の負荷を継続的に制御する必要があります。

注： 高密度クライアント向けの設計方法の詳細については、『Wireless High Client Density Design Guide』（https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/b_wireless_high_client_density_design_guide.html）および https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/222000-design-guide-cx-wireless-for-large-pub.html を参照してください。

ほとんどの場合、「負荷」という言葉は CPU 負荷を指します。Catalyst 9800 物理アプライアンスは、ハードウェアでデータプレーンを高速化しているため、マルチ CPU ソフトウェアアーキテクチャに負荷がかかる可能性のあるのは、ほとんどがコントロールプレーン関連のアクティビティ（AP の CAPWAP メッセージの処理、クライアントのオンボーディング、クライアントのローミング、不正管理、干渉検出、mDNS のような CPU 負荷の高いクライアント アプリケーションなど）です。

システム負荷は、特定のタイプの展開およびスケーリング要因（AP 数、クライアントの密度、クライアントの認証およびローミングレート、クライアントのローミングタイプ、キーキャッシングメカニズム、使用されているアプリケーションなど）に完全に依存します。これらのすべてがシステムキャパシティに影響を与える要因であるため、特定の展開に対して推奨される規模の数値を事前に提示することは困難です。

ネットワークの負荷を事前に予測することが困難であるとしても、システム設計では、単一のボックスを最大キャパシティまで利用するのではなく、「予期せぬ事態」や利用のピークに対応できるようにある程度の余裕を残しておくことが推奨されます。

C9800 の設計も例外ではなく、一般的にシスコでは、AP およびクライアントの規模の 80% 程度に負荷を制限することをお勧めします。

「80% の規模」は、テストおよび検証済みの数値であるため、Catalyst ワイヤレスネットワークの設計および展開のプランニングを開始する上で適した推奨値となります。

たとえば、C9800-80/CW9800H1/H2 の場合、これは 4,800 の AP または約 50,000 のクライアントを意味します。これは、1 台の C9800-80 に 6,000 の AP を設定できないことを意味するのでしょうか。いいえ、決してそう

ではありません。シスコでは、最大規模での展開に成功した事例が多数あります。80% の規模は、Catalyst ワイヤレスネットワークの設計および展開のプランニングを開始するための推奨値にすぎません。

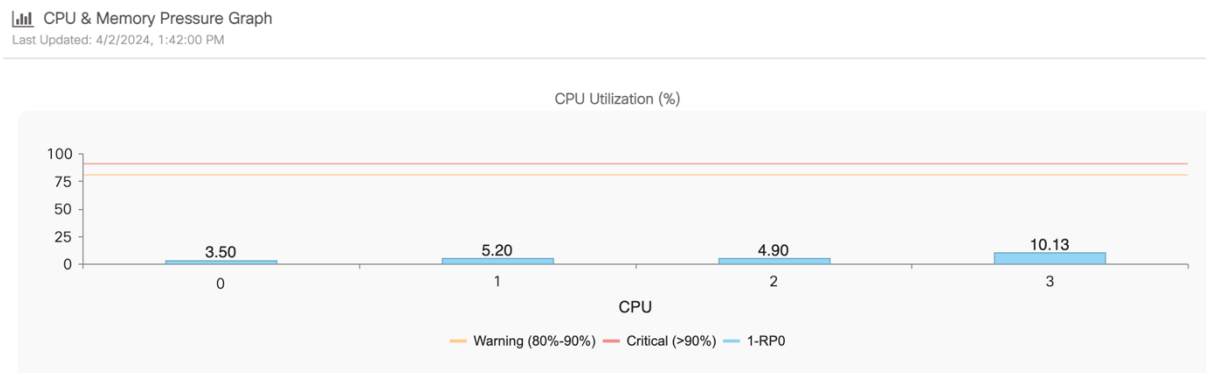
逆もまた真ではありません。特定の状況では、AP とクライアントの数が大幅に少なくても、C9800 のマルチ CPU システムに大きな負荷がかかることがあります。高 CPU 負荷の問題は、必ずしも製品の規模やパフォーマンスの限界が原因ではなく、クライアントのプローブおよびローミング動作、クライアント アプリケーションの動作、クライアントトラフィックの性質といった考慮すべき要因が複数あります。Wi-Fi は進化と成長を続けているテクノロジーであり、クライアントトラフィックは垂直方向と水平方向に拡張されています。予測される変化に備えて、システムキャパシティを最適化し、使用率が急増した場合にも対応できるように余裕を持たせておくことが、常に最善の策になります。

そのため、プロセスの CPU 負荷をモニターし、システムが推奨負荷の範囲で動作していることを確認することが重要になります。CPU 使用率が 5 分間で 70% 未満であれば問題ありません。CPU スパイク（1 分未満）で 80/90% になることは、まったく正常な状態です。

次の CLI コマンドを使用して内部プロセスをモニターできます。

```
show processes cpu platform sorted | inc Name|---|wncd
```

または、メインダッシュボードページの [CPU/メモリ負荷グラフ（CPU & Memory Pressure Graph）] ダッシュレットで直接モニターできます。



CPU 負荷が常に 70% を超えている場合は、詳細な調査を開始し、ボックスのリソースの使用状況を最適化する方法を確認することができます。最初に、次のセクションで説明するように、サイトタグの設計を確認することをお勧めします。次の 2 つのドキュメントに、詳細な障害対応手順が記載されています。

- 『Troubleshoot Wireless LAN Controller CPU Load』（https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/221965-troubleshoot-wireless-lan-controller-cpu.html）
- 『Understand High CPU Usage Reported for the Dataplane on Catalyst 9800』（ https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-cl-wireless-controller-cloud/221058-understand-high-cpu-usage-reported-for-t.html）

サイトタグを考慮した設計：ローカルモードの AP

Catalyst 9800 ワイヤレス LAN コントローラは、IOS XE マルチプロセス アーキテクチャに基づいています。

モビリティとローミング、無線リソース管理（RRM）、不正管理といった最重要の機能には専用のプロセスがあります。AP およびクライアントセッションを担当するメインプロセスは、「ワイヤレス ネットワーク コントローラ プロセス」（WNCd）と呼ばれます。次の表に示すように、内部 WNCd プロセスの数はプラットフォームによって異なります。

表 1. プラットフォームごとの WNCd プロセス数

プラットフォーム	WNCd インスタンス
EWC（AP および Catalyst 9000 スイッチ上）	1
C9800-L	1
C9800-CL（小規模）	1
C9800-CL（中規模）	3
C9800-40、CW9800M	5
C9800-CL（大規模）	7
C9800-80、CW9800H1、CW9800H2	8

次の CLI コマンドを使用して、プラットフォームの WNCd の数を確認できます。

```
C9800#sh processes platform | inc wncd
```

これは、AireOS ベースの WLC とは異なります。AireOS ベースの WLC では、単一のマルチスレッドプロセスのみで、AP やクライアントのセッションだけでなく WLC のすべての機能を処理していました。C9800 マルチプロセス ソフトウェア アーキテクチャには、次のような複数の利点があります。

- 各プロセスはシングルスレッドであり、ノンブロッキングです。
- 単一の障害ドメイン（メモリ分離など）は存在しません。
- プロセスごとのデータ分離とデータ外部化が実現されます。
- 複数の WNCd を追加することにより、水平方向への拡張が容易になります。
- プロセスの問題を容易に修正できます。

このソフトウェアアーキテクチャにより、シスコは、In Service Software Upgrade（ISSU）、ソフトウェアメンテナンス更新（SMU）などの多数の重要なイノベーションを Catalyst Wireless に導入できました。

ソフトウェアアーキテクチャがマルチプロセスである場合、プラットフォームを最大限に活用するには、すべてのプロセスが均等に利用されていることを確認する必要があります。WNCd はすべての AP および関連クライアント セッションを処理するため、明らかに開始点として適切であり、AP の負荷がさまざまな内部プロセス間で均等に分散されていることを確認する必要があります。

AP は、C9800 に参加すると、使用可能な WNCd に分散されます（もちろん、これは複数のプロセスが存在するプラットフォームに適用されます）。当然のことながら、使用可能な WNCd プロセス間で AP（および関連クライアント）の負荷を分散することで、C9800 で使用可能なリソースがより有効に活用されるため、拡張性とパフォーマンスが向上します。

内部プロセス間の AP の分散は、サイトタグに基づきます。同じサイトタグに関連付けられた AP は同じプロセスに参加するため、そのプロセスによって管理されます。AP のマッピングは、特定のサイトタグから参加した最初の AP で行われます。

最適なパフォーマンスを実現できるように Cisco Catalyst ワイヤレスネットワークを設計する際には、AP をサイトタグにどのように割り当てるか、つまり内部プロセスにどのように割り当てるかを理解することが重要になります。

そこで最初に、ローカルモード AP を使用して Catalyst 9800 ワイヤレスコントローラを展開する際に注意する必要があるいくつかの一般的な推奨事項について説明します（FlexConnect に関するいくつかの特定の推奨事項については、後のセクションで詳しく説明します）。

1. 特にローミングや高速ローミングが要件である場合は、デフォルトサイトタグではなく、カスタムサイトタグを使用します。
2. 同じローミングドメイン内のすべての AP に同じサイトタグを割り当てます。「ローミングドメイン」は、同じ RF ドメインを共有し、同じ SSID をブロードキャストする AP の論理グループとして定義されます。
3. 単一のサイトタグに割り当てる AP の数を制限します（サイトタグあたり 500 AP の値を推奨）。
4. 可能な場合は、次の表に示す単一サイトタグあたりの最大アクセスポイント数を超えないようにしてください。

表 2. 単一サイトタグあたりのアクセスポイント数

プラットフォーム	サイトタグあたりの最大 AP 数*
C9800-80 、 CW9800H1 、 CW9800H2 、 C9800-CL（中規模と大規模）	1600
C9800-40、CW9800M	800
その他の C9800 プラットフォーム	サポートされる最大 AP 数

*これらはローカルモード AP の場合の数値です。FlexConnect AP および関連するリモートサイトタグの場合、シームレスローミングが必要であれば、サイトタグあたりの上限は 100 AP です。リリース 17.8.1 で、「ペアワイズマスターキー（PMK）伝達」機能（「FlexConnect ハイスケールモード」とも呼ばれる）を利用して、サイトタグあたり 300 AP に制限が引き上げられました。

5. 大規模展開、高密度シナリオを扱う場合は、その特定のプラットフォームの WNCd プロセス数と等しい数のサイトタグを使用し、それらの間に AP を均等に分散させることが推奨されます。何らかの理由でサイトタグが多い場合は、その数を WNCd 数の倍数として保持し（たとえば、9800-40 ではサイトタグ = 5、10、15 など）、やはり AP を均等に分散させることが推奨されます。

   注： 上記の推奨事項も、あくまで推奨事項にすぎません。たとえば、同じサイトタグに 500 を超える AP がある場合でもシステムは動作しますが、ネットワークのパフォーマンスを最適化できない可能性があります。

最初の推奨事項である「デフォルトサイトタグを使用しない」は、C9800 内部でのリソースの使用方法を改善し、プロセス間通信ではなくプロセス内通信に最適化するために役立ちます。カスタムサイトタグを使用することにより、同じサイトタグに属するすべての AP が同じ内部プロセスに割り当てられます。

2 つ目の推奨事項である「ローミングドメインをサイトタグと一致させる」ことにより、確実に、ほとんどのローミングが同じプロセス内で発生するようになります。デフォルトサイトタグを使用すると、AP は使用可能なプロセス間にラウンドロビン方式で分散され、ある AP から別の AP にクライアントがローミングする際に、プロセス間通信が発生する可能性が高くなります。

リリース 17.6 より前のリリースでは、WLAN（ワイヤレス LAN）を介した音声通信のような遅延に敏感なアプリケーション向けに最適化された高速ローミングが必要な場合、同じローミングドメイン内のすべての AP に同じサイトタグを割り当てることも特に重要です。ここで「最適化された」は、C9800 が 80211k/v などのプロトコルを活用してクライアントに追加情報を渡し、ローミングプロセスを支援することを意味します。たとえば、クライアント

がローミングできるネイバー AP のリストは、802.11k ネイバーリストを介して提供されます。異なるサイトタグに属する 2 つの AP 間、つまり WNCd プロセス間でローミングする場合は、AP ネイバー情報が失われるため、この情報に依存する 802.11v や 802.11k などのプロトコルは最適化されません。これが、同じローミングドメイン内のすべての AP（シームレスで高速なローミングが必要）を同じサイトタグに割り当てるもうひとつの理由です。これは、802.11k/v にのみ影響し、サイトタグをまたいでサポートされる高速かつシームレスなローミングには影響しません。

重要：リリース 17.6.1 以降ではこの制限が解消されているため、サイトタグ間でローミングするクライアントは 802.11k/v のメリットを享受できます。このリリースでは、ユーザーは、SSID がポリシータグに含まれていることを確認することにより、ネイバー AP で SSID が有効になっているかどうかを手動で調べる必要があります。リリース 17.7.1 以降では、このチェックは自動的に行われます。

注： ローミングのサポートについては、ローカルモードの AP（つまり、中央アソシエーションの SSID）の場合、802.11r および便宜的キーキャッシング（OKC）を使用したシームレスなローミングがサイトタグをまたいで機能します。制限はありません。

なぜ、単一のサイトタグにすべての AP を割り当てて、作業を終わらせないのでしょうか。ここで、3 つ目の推奨事項が登場します。パフォーマンスを最適化するには、サイトタグごと、つまり WNCd ごとの AP 数を制限する必要があります。複数のサイトタグを設定し、サイトタグごとの AP 数を制限することで、単一のプロセスが過負荷状態になる可能性が減少します。シスコが推奨する数は、サイトタグごとに約 500 の AP です。これは、すべての異なる Catalyst 9800 プラットフォームに利用できる単なる参照値です。

明確に説明すると、サイトタグごとに 500 を超える AP を割り当てても、上記の表に示す、テスト済みであるために公式にサポートされている制限内にとどまる場合、何かが壊れることはありません。

注： 500 AP は、Cisco Catalyst Center が単一のサイトタグに配置する AP のデフォルトの最大数でもあります。リリース 2.2.2 以降では、ユーザーは、Cisco Catalyst Center でカスタムサイトタグを設定でき、それによって特定の展開に応じた設計が可能です。

これらの上限を超えること（たとえば、9800-40 でサイトタグあたり 800 AP）は推奨されません。上限を超えると、パフォーマンスへの悪影響が発生しはじめます。つまり、1 秒あたりのクライアントローミング数が減少する可能性があり、同様に 1 秒あたりの認証数も減少する可能性があります。WNCd プロセスの過負荷状態を示す syslog イベントが発生する場合もあります。これらはすべて、単一の WNCd プロセスの過負荷状態による影響です。C9800 が自動車のエンジンであり、WNCd がそのシリンダーであると考えてみてください。1 つの シリンダーだけで自動車を走らせると、よい結果は得られず、最適化されたものともなりません。

1 つの大きなローミングドメインである大規模展開（大規模な病院、会議センター、スタジアム、大企業のキャンパスなど）がある場合はどうでしょうか。サイトタグをどのように設計しますか。AP を複数のカスタムサイトタグに分散させるには、どうすればよいですか。

最初に、1 つの重要な概念を明確にしておきます。名前から連想されるとしても、サイトタグを地理的な物理サイトと一致させる必要はありません。サイトタグは、特定の共通設定（AP 参加プロファイルに含まれる設定）を割り当てることを可能にするアクセスポイントの論理グループです。また、AP グループに関連する AP およびクライアントイベントの処理を最適化するために、内部的にも使用されます。

多数のクライアントがあり、それらのクライアントがあらゆる場所でシームレスにローミングできる高密度（HD）展開では、C9800 のパフォーマンスを最適化するために、次の表に示すように、特定のプラットフォームに応じてサイトタグの数を選択することが推奨されます。

表 3. 高密度の単一サイトの展開におけるサイトタグの推奨数

プラットフォーム	サイトタグの推奨数
C9800-80、CW9800H1、CW9800H2	8
C9800-CL（大規模）	7
C9800-40、CW9800M	5
C9800-CL（中規模）	3

カスタムタグの数を選択したら、これらのサイトタグに AP を均等に分散させる必要もあります。繰り返しになりますが、サイトタグを物理サイトに対応させる必要はありません。ただし、AP をグループ化するための仮想エリアを作成する必要があります。

以下に、これらの推奨事項を実装する方法を理解するための例を示します。

- 3,000 の AP と数万のクライアントが存在する大規模な会場（スタジアムなど）を設計する必要があります。あらゆる場所でローミングが必要であるため、実際には大規模なローミングドメインとなります。この展開を管理するために、C9800-80 を選択しました。推奨される方法は、ほとんどのローミングが発生することがわかっている 8 つの仮想ローミングエリア（たとえば、スタジアムの各セクターをグループ化したもの）を特定し、それぞれにサイトタグを定義することです。この場合、8 つのサイトタグで 3000 の AP になり、サイトタグごとに 375 の AP になります。もちろん、正確に切り分ける必要はありませんが、物理的な場所/サイトの観点からは妥当であってもいくつかのサイトタグが過負荷状態になるようなことは避けて、AP を均等に分散させることが推奨されます。一方で、AP がほとんどない小さなエリア（チケットエリアなど）がある場合は、それらを他の AP と統合して、サイトタグの規模が推奨される規模（この場合は 375 の AP）に近くなるようにします。
- 3 つの建物がある小さなキャンパスにおいて、C9800-40 で 600 の AP を管理しています。ほとんどの場合、建物間に Wi-Fi カバレッジ外の場所（エアギャップ）があり、建物間でのローミングは発生しません。このような場合、建物ごとに 1 つずつ、3 つのサイトタグを設定できます。これは、サイトタグごとに 200 の AP を意味し、推奨設定の範囲内に十分収まっています。
- 複数の建物がある大きなキャンパスにおいて、C9800-40 で 1200 の AP を管理しており、今回は、キャンパス全体にわたるローミングが必要です（病院のキャンパスなど）。1200 の AP がサイトタグごとの最大数を超えていることに加えて、これは大規模なローミングドメインであるため、5 つのサイトタグ（建物を 5 つの仮想エリアにグループ化）を使用することが推奨されます。この場合、サイトタグごとに 240 の AP となり、非常にバランスのとれたシステムになります。なお、シームレスなローミングがサイトタグ間で完全にサポートされており、17.7 以降では 802.11k/v もサイトタグ間で機能することに注意してください。

サイトタグを考慮した設計：FlexConnect モードの AP

FlexConnect 展開の場合、クライアントのキーキャッシングおよびキー配布が単一の Flex サイトタグ内でのみ行われるため、サイトタグが高速ローミングドメインを識別します。通常、また当然のことながら、高速ローミングが必要なリモートロケーションごとに 1 つのサイトタグが存在するため、FlexConnect 展開で単一の内部プロセスが過負荷状態になる可能性は、ローカルモードの場合よりもはるかに低くなります。

サイトタグを設計する際の FlexConnect 固有の推奨事項は次のとおりです。

- デフォルトサイトタグは、高速ローミングが要件となる Flex 展開では使用できないため、カスタムサイトタグの使用が常に推奨されます。その理由は、デフォルトサイトタグでは FlexConnect AP 間でクライアン

トキーが配布されていないためです。Flex サイトごとに少なくとも 1 つのサイトタグを設定する必要があります。

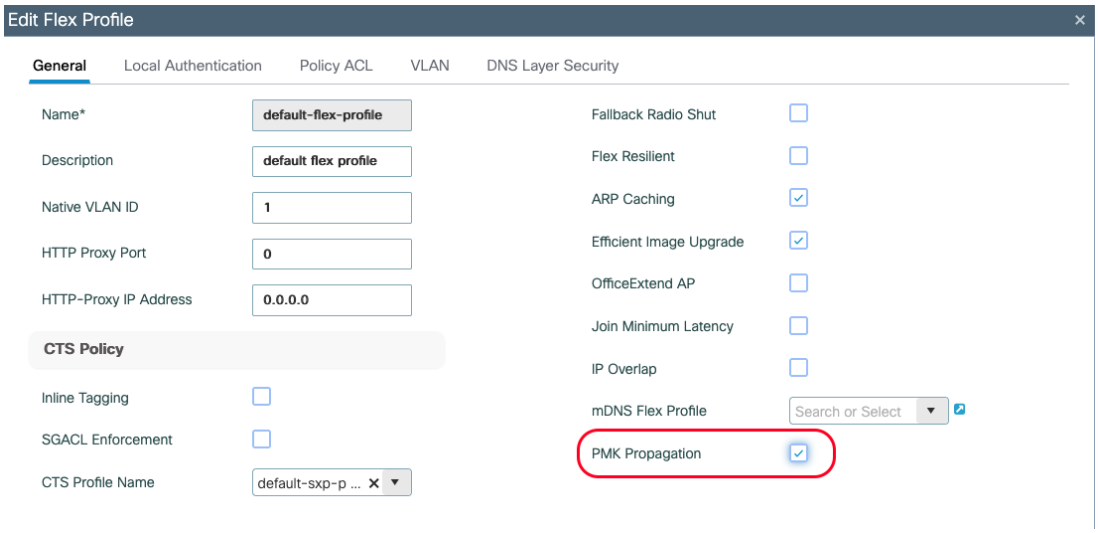
- 高速シームレスローミング（802.11r、CCKM、OKC）のサポートが必要な場合、Flex サイトのサイトタグあたりの最大 AP 数は 100 です（AireOS の場合と同じ）。リリース 17.8.1 で、「ペアワイズマスターキー（PMK）伝達」機能（デフォルトでは無効）を利用して、サイトタグあたり 300 AP に制限が引き上げられました。

  これは、次のコマンドを使用して FlexConnect プロファイルで設定できます。

```
C9800(config)#wireless profile flex NAME
C9800(config-wireless-flex-profile)#pmk propagate
```

  または、GUI で次のように設定します。

図 1：GUI で PMK 伝達を有効にする方法



- 複数の FlexConnect サイトで同じサイトタグ名を使用しないでください（これにはデフォルトサイトタグが含まれます）。C9800 は物理的な場所を認識しません。加えて、異なる物理的な場所にある AP にクライアントキーを配布しても、ローミングが発生しないため、意味がありません。また、ローカルスイッチング SSID において Flex 接続サイト間でのクライアントの IP アドレスの重複をサポートするには、異なるサイトタグ名を使用する必要があります。
- WAN 帯域幅を節約し、リモートサイトにある AP へのソフトウェアダウンロードをより効率的にするために、FlexConnect プロファイルでは効率的なアップグレードがデフォルトでオンになっています。FlexConnect AP を持つ各サイトタグに、モデルごとに 1 つの AP がマスター AP として選択され、その AP が WAN リンクを介して WLC からイメージをダウンロードします。マスター AP にイメージがダウンロードされると、そのサイトダグに含まれる AP がマスター AP からのイメージのダウンロードを開始します。サイトタグの割り当てには注意してください。1 つのサイトタグが複数のブランチにまたがる場合、AP は、WLC ではなく別のブランチからイメージをダウンロードする可能性があります。

サイトタグの設計に関する最後の、しかし重要な考慮事項が 1 つあります。大規模のサイトタグと小規模のサイトタグの混在を回避できず、推奨されているように AP を均等に分散させることができない場合は、どうすればよいでしょうか。これは、キャンパス（ローカルモード AP を使用）と多数の小さなリモートサイト（FlexConnect AP を使用）を含む展開がある場合です。前述したように、FlexConnect では、各サイトが高速セキュアローミングドメインを定義するため、それらのサイトが独自のサイトタグである必要があり、タグの数については多くの選択肢があり

ません。この場合、負荷が最適に分散されたシステムを構築するとともに、ローカルモード AP の推奨事項に従うためには、おそらく WLC を 2 つ用意し、一方をキャンパス AP 管理用、もう一方をブランチ専用とすることが最善です。コストを最適化するために、9800-CL を使用することも考えられます。

サイトタグの「load」コマンドを使用した設計の強化

前のセクションでは、Catalyst 9800 のリソースを最適化するためのサイトタグ設計に関するベストプラクティスについて説明しました。これは、IT チームにとって運用上の負担となる場合があります。その理由は、サイトタグの数を定義し、どの AP をどのタグにマッピングする必要があるかを特定し、その設定を実装する作業が、多くのプランニングと時間を要する可能性があるからです。

17.9.2 以降、サイト タグ コンフィギュレーションに新しい「load」コマンドが導入されました。これにより、サイトタグベースの設計をさらに最適化し、IT 運用を簡素化することができます。このコマンドは、負荷の想定値をコントローラに示します。AP 数を負荷として使用することもできますし、クライアント数や使用率を表すこともできます。これはユーザーに依存します。

この機能拡張が導入されるまでは、C9800 がサイトタグのサイズに関する情報を持たず、内部プロセスへの AP 負荷分散の決定はサイトタグ数のみを考慮して行われており、実際の AP 数やそれによって生成される可能性のある負荷は考慮されていませんでした。前のセクションで推奨されているように、AP がサイトタグ全体に均等に分散されている場合、システムは引き続き正常に機能します。

ただし、さまざまなサイズのサイトタグがあり、サイトタグの数が WNCd プロセスの数より多い場合、一部のプロセスに負荷が集中し、他のプロセスが十分に活用されないという、アンバランスなシステム構成になる可能性があります。

強化されたサイトタグベースの負荷分散機能を使用すると、サイトの負荷を設定できるため、システムはより適切に負荷分散を決定できるようになります。負荷は、サイト タグ コンフィギュレーション モードで次の CLI を使用して設定されます。

```
C9800(config)#wireless tag site <name>
C9800(config-site-tag)#load <1-1000>
```

負荷を設定した後に、すべてのサイトタグがアクティブになったら（つまり、1 つ以上の AP が参加したら）、WLC を再起動することが推奨されます。コントローラが再起動した場合の負荷分散機能の動作は次のとおりです。

- 機能を設定し、コントローラを再起動すると、AP が参加する前であっても、負荷分散機能は、永続メモリでアクティブに使用されているサイトタグを保持し、起動時にそれらの負荷を分散させます。起動時の負荷分散は、設定されたサイト負荷の降順で行われます。
- AP がすでに参加しているサイトタグでこの負荷分散機能を設定すると、そのサイトタグ内にないものを含む、すべての AP が切断されるか、コントローラが再起動しない限り、負荷分散は変更されません。

負荷パラメータの値は、どのように選択すればよいでしょうか。負荷は、そのサイトタグ（したがって、AP グループと関連クライアント）用に予約される相対的な WNCd キャパシティの推定値です。

クライアントプローブ、クライアント参加、クライアント認証、ローミングなどに加え、CPU 時間を必要とする mDNS のような機能も含め、コントロールプレーンのすべてのアクティビティが、内部プロセスの「負荷」の原因となります。AP が忙しいほど、「負荷」は大きくなります。最も一般的な選択肢は、負荷を、サイトタグに含まれる AP の数と同じに設定することです。これは、各 AP のクライアント数がほぼ同じであり、そのためにアクティビティもほぼ同じであると推定されるオフィス建物では、優れた選択肢となります。

会議/トレーニングセンターやカフェテリアのように、より頻繁なアクティビティ（クライアントの参加、離脱、ローミングが頻繁に発生）が予想される建物/エリア/フロアがある場合は、その特定のサイトタグに対してより高い

重み付けをした「負荷」を設定します。たとえば、会議センターエリアに 10 の AP が存在する場合、負荷を 20 に設定します。

要件と推奨事項：

- 負荷を使用することは、設定されたサイトタグの数が WNCd プロセスの数より多い場合にのみ有益です。
- すべてのサイトタグに負荷を設定する必要があります。
- 負荷の設定は、ローカルモード展開と FlexConnect モード展開の両方で推奨されます。
- 設定する負荷はあくまでも推定値です。これは、サイトタグの負荷分散にのみ使用されます。具体的には、AP またはクライアントの参加や関連付けを妨げることはありません。
- 負荷は、どのように選択すればよいでしょうか。一般的なクライアント密度のサイトの場合、AP 数をサイト負荷の適切な概算値として使用できます。このようなサイトの例としては、オフィスのフロアや建物が挙げられます。クライアント密度が高く、ローミング負荷が大きいサイトの場合は、AP 数よりも高い負荷設定を使用できます。たとえば、そのようなサイトの AP 数が 200 である場合、300 または 400 の負荷係数を使用して、より高いクライアント負荷を補うことができます。このようなサイトの例としては、カフェテリア、講堂、会議センターのフロアなどが挙げられます。
- AP 分散アルゴリズムに負荷を考慮させるとともに、AP 参加の順序に依存しないようにするには、サイトタグの下で負荷パラメータを設定し、C9800 を再起動します。

サイトタグが負荷分散の対象として考慮されるには、少なくとも 1 つの AP が参加している必要があります。この情報は、次回以降の実行のためにシステムによって保存および記憶されます。

新規導入の場合、AP 参加のタイミングが異なる可能性があるため、システムは、最後の起動から 1 時間待機して（AP の起動を待って）から、アクティブなタグを保存し、それらを計算の対象として考慮します。これが、少なくとも 1 時間の稼働時間後に WLC の再起動をトリガーする必要がある理由です。

C9800 が再起動しない場合でも、設定された負荷パラメータによってサイトの負荷が考慮されるため、負荷分散アルゴリズムは改善されます。ただし、その場合は、WLC に参加する AP の順序に依存することになります。

RF ベースの自動 AP 負荷分散による設計の強化

リリース 17.12 以降では、RF ベースの自動 AP 負荷分散機能により、前のセクションで説明した既存のサイトタグベースの負荷分散が改善される可能性があります。適切に計画されていない場合、サイトタグベースの方法により、内部インスタンス間で AP が不均等に分散され、メモリと CPU の使用率が高くなる可能性があります。サイトタグベースの方式は、load コマンドによって強化されましたが、AP 負荷制限が正しく設定されていない場合や、お客様がほとんどの AP を 1 つの大きなサイトタグにまとめると決定した場合、パフォーマンスが最適化されない可能性があります。

RF ベースの自動 AP 負荷分散機能は、無線リソース管理（RRM）を使用して、AP を自動的にグループ化し、WNCd インスタンス間で負荷を分散させます。この機能を有効にすると、AP ネイバーレポートから受信した RSSI に基づいて AP クラスタが形成されます。これらの AP クラスタまたはネイバーフッドは、サブネイバーフッドや、より小さなエリアにさらに分割されます。生成された AP のグループは、その後、内部プロセス間で均等に分散されます。

RF ベースの自動 AP 負荷分散は、アルゴリズムを実行（「学習」とも呼ばれます）してからアルゴリズムを適用するという 2 段階のプロセスです。アルゴリズムの実行は、オンデマンドまたはスケジュール設定で行うことができます。アルゴリズムは、コントローラの再起動後に自動的に適用されるか、`ap neighborhood load-balance apply` コマンドでトリガーされる AP の CAPWAP リセットによって手動で適用されます。RF ベースの自動 AP 負荷分散機能がアクティブになっている場合、他のサイトタグベースの負荷分散は無効になります。

RF ベースの自動 AP 負荷分散の有効化および設定については、次の設定ガイドを参照してください：
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_auto-wncd-lb.html

要件と推奨事項：

- この機能は、サイトタグ数が特定のプラットフォームの WNCD 数より多い場合、またはサイトタグに 100 を超える AP がある場合に、より優れた負荷分散を実現するために推奨されます。
- この機能は、ローカルモード、ファブリックモード、および FlexConnect モードの AP でのみサポートされています。
- 新しい展開の場合でも、サイトタグベースの方式を使用し、その推奨事項に従って AP を均等に分散させる（サイトタグの load コマンドも併用）ことが推奨されます。なぜでしょうか。サイトタグを使用すると、同じサイトタグのすべての AP が同じ WNCd に接続されるようになります。これは、トラブルシューティングに役立つとともに、WNCd 内でのローミングが最適化されます。
- 新規の展開でも既存の展開でも、AP をグループ化できないためにサイトタグを中心に設計できない場合（たとえば、AP に識別しやすい名前がない場合や、AP の場所がわからない場合など）、またはサイトタグの設計に時間をかけたくない場合は、デフォルトサイトタグまたは名前付きサイトタグを使用して、RF ベースの自動 AP ロードバランシング機能をオンにすることができます。サイトタグと load コマンドを使用して負荷が均等に分散されたシステムと比較すると、パフォーマンスに影響が出る可能性があることに注意してください。
- 既存の展開で、アンバランスなシステムが原因で CPU 使用率が高くなる問題が発生した場合は、サイトタグを再設計する代わりに自動 RRM ロードバランシングシステムを使用します。
- アンバランスなシステムでも CPU 負荷の問題が発生していない場合は何も変更しない、という最重要のルールを忘れないようにしてください。
- RF ベースの自動負荷分散は、サイトあたり 100 以上の AP がある場合に最もよく機能します。小さなサイトタグを持つ展開では、前のセクションで説明したように、代わりに load コマンドを使用することをお勧めします。
- この機能の使用は、学習と適用の 2 段階のプロセスであることに注意してください（設定ガイドを参照）。
- システムの全体的な負荷が高い場合は、この機能をオンにすることは推奨されません。

AP 負荷分散の概要

前のセクションでは、Cisco Catalyst 9800 ワイヤレス LAN コントローラでサポートされているさまざまなタイプの AP 負荷分散について説明しました。ここでは、これまで説明した負荷分散のメカニズムの概要を示します。

表 4. AP 負荷分散の概要

負荷分散モード	推奨設定	備考
なし	WNCd が常に低いのであれば、何もする必要はありません。	
負荷ベースのサイトタグ	さまざまなサイズのサイトタグがあり、サイトタグの数が WNCd プロセスの数より多い場合に使用されます。	負荷ベースのサイトタグ設定を有効にしたら、コントローラを再起動する必要があります。
RF ベースの自動 AP 負荷分散	小さなサイトタグが多数あり、サイトタグあたりの AP が 100 未満の場合に推奨されます。	管理者がサイトタグの設計に時間をかけたくない展開に適しています。

負荷分散モード	推奨設定	備考
		このアプローチでは、RRM がサイトタグの所有権を引き受けるため、詳細さが低くなります。 これは学習と適用の 2 段階のプロセスであることに注意してください。

C9800 ワイヤレスコントローラの一般設定

これらの設定は、ボックスレベルで C9800 ワイヤレスコントローラに適用されます。

インストールモードとバンドルモード

C9800 WLC で Cisco IOS XE イメージを実行するには、次の 2 つの方法があります。

- *インストールモード*：インストールモードでは、コントローラを起動するために、バイナリファイルからフラッシュに事前抽出されたファイルが使用されます。コントローラは、抽出中に作成された ***packages.conf*** ファイルをブート変数として使用します。インストールモードはデフォルトのモードです。
- *バンドルモード*：コントローラがブート変数としてバイナリイメージ（.bin）を使用して起動する場合、システムはバンドルモードで動作します。このモードでは、コントローラは .bin ファイルを RAM に抽出し、そこから実行します。起動時に抽出されたパッケージが RAM にコピーされるため、このモードではインストールモードよりも多くのメモリを使用します。

次の show コマンドを使用して、現在のモードを確認できます。

```
9800#show version | i Installation mode
Installation mode is INSTALL
```

注： インストールモードには、In Service Software Upgrade（ISSU）などの高可用性機能のサポート、ソフトウェア メンテナンス アップグレード（SMU）/パッチ適用（ホットおよびコールド）、起動時間の短縮、メモリ消費の削減、Cisco Catalyst Center によるアップグレードのサポートといった利点があるため、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを実行する場合に推奨されるモードはインストールモードです。

何らかの理由でボックスがバンドルモードになっている場合、インストールモードで起動するには次の手順を実行します。

1. イメージをダウンロードするための十分な容量がフラッシュにあるかどうかを確認します。
   ```
   C9800#dir flash:
   ```
2. 使用していない古いインストールファイルをクリーンアップして、空き容量を確保します。
   ```
   C9800#install remove inactive
   ```
3. イメージをフラッシュにコピーします（TFTP 転送などを使用）。
   ```
   C9800#copy tftp://<path> flash:
   ```
4. 現在のブート変数を削除し、packages.conf を指すように設定します。次のコマンドを使用します。
   ```
   C9800(config)#no boot system
   C9800(config)#do write
   C9800(config)#boot system bootflash:packages.conf
   C9800(config)#do write
   ```

5. イメージをフラッシュにインストールしてから、コードをアクティブ化してコミットします。これにより、C9800 がバンドルモードからインストールモードに移行します。これは、次の 1 つのコマンドで実行できます。

```
C9800#install add file bootflash:<image.bin> activate commit
```

ワイヤレス管理インターフェイス

C9800 にはワイヤレス管理インターフェイス（WMI）が 1 つだけあります。これは、レイヤ 3 インターフェイスです。WMI は、AP からのすべての CAPWAP トラフィックを終端します。また、ボックスから生成されるすべてのコントロール プレーン トラフィックのデフォルトの送信元インターフェイスとなります。ゲストトラフィック用のフォーリン/アンカーを含むすべての展開で、スイッチド VLAN インターフェイス（SVI）を WMI として使用することが推奨されます。唯一の例外は、パブリッククラウドの C9800-CL であり、ワイヤレス管理にレイヤ 3 ポートを使用することが必須です。また、Cisco Catalyst 9000 スイッチの組み込みワイヤレスでは、ループバック インターフェイスが推奨されます。

注： C9800 には、AireOS のような複数の AP マネージャインターフェイスがありません。CAPWAP の終端には 1 つのインターフェイスだけが使用されます。これが WMI です。

ジャンボフレームのサポートと「ip mtu」インターフェイスコマンド

ジャンボフレームは、標準的な 1,500 バイトの制限を超える（通常は 9,000 バイトまで）ペイロードを持つイーサネットフレームです。C9800/CW9800 によって送信されるパケットの最大伝送ユニット（MTU）を変更するには、レイヤ 3 インターフェイス（SVI）で「mtu」コマンドおよび「ip mtu」コマンドを使用できます。

```
C9800(config)#interface vlan 105
C9800(config-if)#mtu ?
<1500-9216>  MTU size in bytes
C9800(config-if)#mtu 9100
C9800(config-if)#ip mtu 9000
```

ip mtu コマンドは IP パケットのペイロードサイズを変更し、mtu コマンドはイーサネットフレームのペイロードを変更します。デフォルト値はどちらも 1,500 バイトです。IP MTU を 1,500 バイトより大きいものに変更するには、最初に L2 ペイロードを増やす必要があります。

C9800/CW9800 には次の 2 タイプのトラフィックが存在します。

1) ボックス自体から発信されるトラフィック（RADIUS、syslog、SNMP など）：サポートされている
2) CAPWAP 経由のクライアントトラフィック：サポートされていない

ボックスから発信されるトラフィック（上記のタイプ 1）については、シスコは 17.11 以降でパケットの MTU の変更をサポートしています。特に RADIUS パケットの場合は、`aaa group server` 設定セクションで、IP MTU 変更を適用する RADIUS 送信元インターフェイスを指定する必要もあります。詳細については、次を参照してください：https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/222920-understand-radius-mtu-and-fragmentation.html。

このガイドの作成時点では、クライアントトラフィック（したがって、CAPWAP パケット）の MTU の変更はサポートされていません。これは、クライアントトラフィックおよび CAPWAP のジャンボフレームがサポートされていないことを意味します。

もちろん、AP は WLC に参加するときに動的パス MTU 検出（PMTU）を実行して、パケット送信時に使用する最適な MTU を見つけます。IP MTU は、1,500 バイトを超えることはできませんが、それより小さくすることは可能です。この小さな MTU は、通常、CAPWAP トラフィックが WAN ネットワークを通過する必要があり、複数のカプセル化のために MTU が 1,500 未満である必要がある場合に役立ちます。

コントローラのリロードまたはネットワークのダウンをともなう設定

C9800 のソフトウェアアーキテクチャにより、有効にするためにボックスをリロードする必要がある機能はありません。これは、ワイヤレスネットワーク全体の稼働時間を増やすために重要です。これの唯一の例外は、ボックスでライセンスレベルを変更する場合と、ステートフル スイッチオーバー（SSO）冗長化を設定する場合です。

ワイヤレスネットワーク（2.4 GHz、5 GHz、および 6 GHz の 3 つの帯域によるネットワークのすべてにおいて）のシャットダウンが必要な唯一の機能は、主に無線リソース管理（RRM）の設定です。

NTP の有効化

Network Time Protocol（NTP）を有効にすることは、一部の機能にとって非常に重要です。コントローラでの NTP 同期は、ロケーション、Simple Network Management Protocol（SNMP）v3、アクセスポイント認証、または 802.11w 保護管理フレーム（PMF）のいずれかの機能を使用する場合に必須です。NTP は、保守性にとっても非常に重要です。

イベントに異なるタイムスタンプが付かないように、AP のタイムゾーンを設定することもできます。これは、AP 参加プロファイルの全般設定で実行するか、次のコマンドを使用して実行することができます。

timezone {use-controller | delta hour offset-hour minute offset-minute} CLI で NTP サーバーを有効にするには、次のコマンドを使用します。

```
C9800(config)#ntp server <IP or dns name>
```

GUI で、次のように設定します。

NTP トラフィックの送信元インターフェイスを指定できます。物理アプライアンスでは、これは、アウトオブバンド管理ポートであるサービスポート（SP）から送信するように NTP を設定する場合に役立ちます。9800 シリーズの物理アプライアンスでは、SP は、別の管理 Virtual Route Forwarding（VRF）インスタンス（Mgmt-intf）にマッピングされています。これを設定するには、次の CLI コマンドを使用します。

```
ntp server vrf Mgmt-intf <ip or dns name>
```

C9800 は、認証を使用した NTP との同期もサポートしています。NTP 認証を有効にするには、次のコマンドを使用します。

```
C9800(config)#ntp authentication-key 1 hmac-sha2-256 <key value>
C9800(config)#ntp authenticate
C9800(config)#ntp trusted-key 1
```

NTP サーバーのステータスが同期していることを確認するには、次のコマンドを使用します。

```
C9800#sh ntp status
Clock is synchronized, stratum 9, reference is 172.16.254.254
[…]
```

設定ファイルの管理

C9800 の場合、すべての異なるフォームファクタで、ベースソフトウェアコードが共通です。これは重要であり、物理アプライアンスと仮想アプライアンスが混在する場合のお客様の展開作業が簡素化されます。これは、ユーザーインターフェイスが同じであり、機能も同じであることを意味します。

これには、スイッチに組み込まれたコントローラと 9800-CL Ultra-Low という 2 つの「例外」があります。Cisco Catalyst 9000 スイッチに組み込まれているコントローラは、Software-Defined Access（SD-Access）アーキテクチャのみをサポートしているため、ファブリック展開モードに関連する機能のみがサポートされます。クラウド向けの Ultra-Low バージョンの Cisco Catalyst 9800-CL ワイヤレスコントローラは、ローカルスイッチングモードでのみ FlexConnect をサポートします。

お客様は、WLC1 から設定を取得して WLC2 で使用するために、「バックアップと復元」手順の実行を希望する場合があります。推奨される手順は、次のとおりです。

- 設定を WLC1 からテキストファイルにコピーし、TFTP/FTP サーバーにアップロードします。
- 次の CLI コマンドを使用して、設定ファイルを WLC2 のスタートアップ コンフィギュレーション ファイルにコピーします：`copy tftp://<server>/config.txt startup-config.`
- WLC2 ボックスをリロードします（保存しない）。
- 元の設定でパスワード暗号化が有効になっていた場合、ユーザーは、バックアップされた設定をインポートする前に、新しい WLC でパスワード暗号化を設定する必要があります。この作業が完了したら、バックアップされた設定をインポートできます。すべてのキーとパスワードは、そのまま保持されます。次に、パスワード暗号化を設定するコマンドを示します。

  `key config-key password-encrypt <private-key> password encryption aes”`
- SNMP v3 ユーザーは、設定ファイルに含まれていないため、コピーされません。次のコマンドを使用して、SNMPv3 ユーザーを再度追加します。

  `snmp-server user <username>  <group> v3 auth sha <password>  priv aes 128 <password>`
- ベストプラクティスとして、管理インターフェイスの MAC アドレスをワイヤレスモビリティ MAC アドレスとして追加します。これは新しいインスタンス/ハードウェアであるため、SVI の MAC アドレスが変更されます。使用するコマンドは、次のとおりです。

  `wireless mobility mac-address <new MAC>`
- （`show wireless interface summary` コマンドで MAC を取得します）
- スマートライセンスのトークンを追加します：`license smart register idtoken <TOKENID>`

9800-CL では、製造元でインストールされる証明書が仮想アプライアンスに付属していないため、追加の考慮事項が必要になります。AP から CAPWAP トンネルを終端させるには、自己署名証明書（SSC）が必要です。9800-CL 用の SSC を生成するには、次の手順を実行します。

- 設定とともにコピーされた証明書を削除します。これを実行するには、まず `show crypto pki trustpoint` コマンドを使用して既存の証明書を確認します。
- 既存の認証局「WLC_CA」を削除します：`no crypto pki server WLC_CA`
- 既存のデバイス証明書を削除します：

  `no crypto pki trustpoint "<hostname>_WLC_TP"`
- 次の EXEC コマンドを使用して管理インターフェイス用の新しい SSC を作成します：

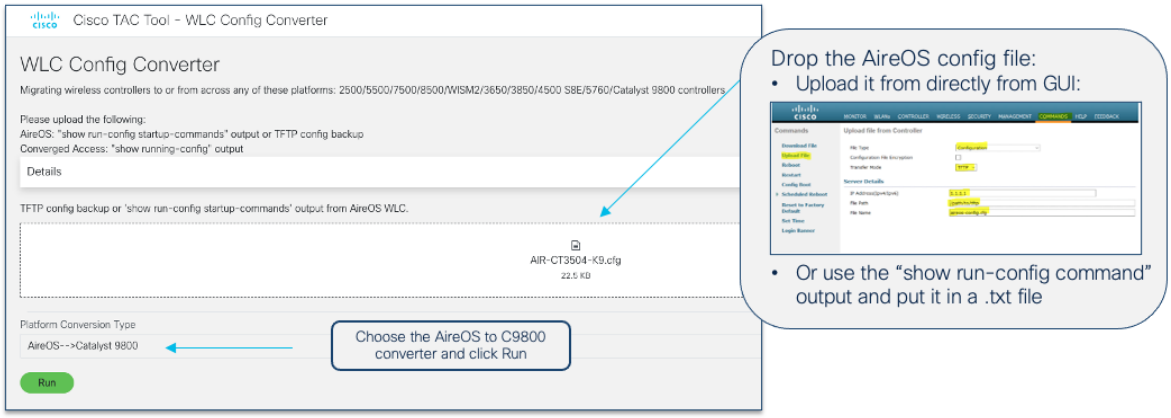
  `wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <password>`

注： お客様が Catalyst 9800 にサードパーティの証明書をインポートした場合は、重要な点として、設定をコピーしただけでは秘密キーがコピーされないことに注意してください。そのため、お客様は新しい WLC に証明書を再度インポートする必要があります。お客様の Web 認証ページについても同様です。これらも、この方法ではコピーされません。

AireOS WLC から Catalyst 9800 に移行する場合は、オペレーティングシステムが異なるため、設定ファイルを変換する必要があります。これを実行するには、設定移行ツールを使用することが推奨されます。Web ベースのバージョンは、次の場所にあります。

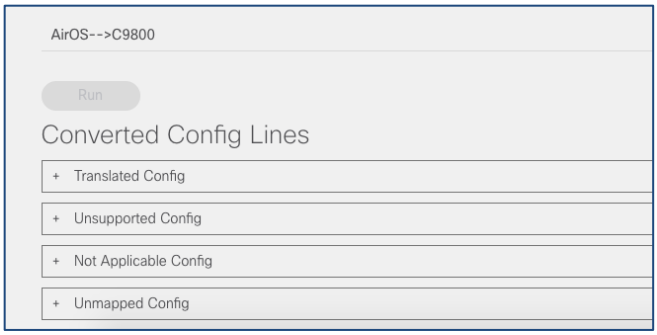
https://cway.cisco.com/wlc-config-converter/

注： 設定ツールにアクセスするには、Cisco.com のログイン情報が必要です。



次のステップを実行します。

1. AireOS の設定ファイルを取得し（TFTP 経由で、または `show run-config commands` CLI コマンドを使用してアップロード）、テキストファイルに保存します。
2. AireOS の設定ファイルをツールにアップロードします。
3. AireOS から 9800 への変換を選択します。
4. [実行（Run）] をクリックします。
   ツールの出力には、次の 4 つの異なるセクションがあります。



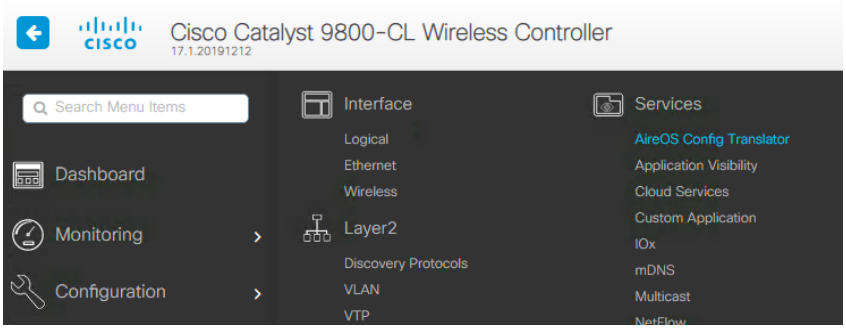
各設定ファイルの説明は、次のとおりです。

- [変換済み（Translated）] : AireOS CLI から Cisco IOS XE CLI に変換された、サポートされている CLI コマンドが含まれています。9800 シリーズで同じ設定がどのように行われるのかを確認するためにも役立ちます。
- [サポートされていない（Unsupported）] : サポートされていない機能に関連する CLI コマンドが含まれています（サポートされていない機能についてはシスコ担当者にご確認ください）。

- [該当しない（Not Applicable）]：Catalyst 9800 では仕組みが異なるか、コマンドが廃止されているため、Cisco IOS XE に適用されない CLI コマンドのリストが含まれています。
- [マッピングされていない（Unmapped）]：サポートされているがツールでまだ変換されない機能に関連するコマンドが含まれています。

5. 変換済みの設定をダウンロードし、必要に応じて編集します。SSID や RADIUS 設定用のパスワードを再入力する必要がある場合や、SVI などの必要性を評価する必要がある場合があります。このファイルは、Catalyst 9800 にそのままコピーするためのものではありません。
6. 設定を Catalyst 9800 の実行コンフィギュレーションにコピーします。CLI で直接コピーして貼り付けることをお勧めします。または、WebUI の [管理（Administration）] > [コマンド ライン インターフェイス（Command Line Interface）] で CLI ツールを使用できます。

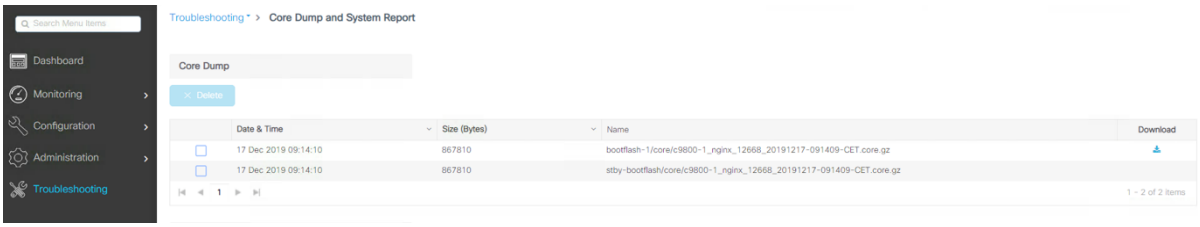
C9800 の GUI に組み込まれたバージョンのツールもあります。



常に最新の修正が反映されるため、https://cway.cisco.com/wlc-config-converter/ にあるオンラインバージョンを使用することをお勧めします。

コアダンプのエクスポート

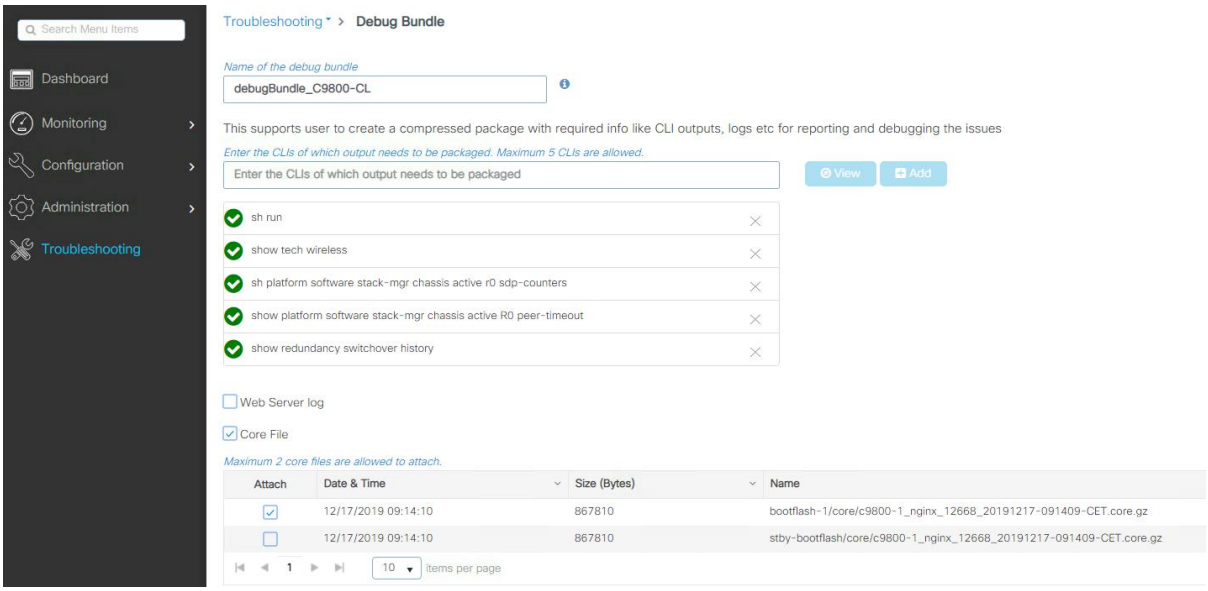
コントローラがクラッシュした場合でも 9800 シリーズ コントローラにはファイルをローカルに保存するための十分なローカルストレージがあるため、ボックス外の場所に自動的にアップロードする必要はありません。C9800 GUI の [トラブルシューティング（Troubleshooting）] セクションには、システムレポートファイル（コアダンプ）を簡単にダウンロードできるセクションがあります。



デバッグバンドル

9800 シリーズは、最も重要なサポートデータを簡素化された方法で簡単に収集できる単一ファイル ダウンロード オプションをサポートしています。これにより、クラッシュ情報、コアファイル、設定、特定の CLI コマンドの出力などを含むバンドルが提供されます。TAC ケースを開く際には、良い出発点となるデータセットを用意するために、常にこのファイルを含めることをお勧めします。

GUI からのサポートバンドルへのアクセスは非常に簡単です。



Web ユーザーインターフェイス（WebUI）

WebUI は、HTTP 要求の処理に VTY 回線を使用します。複数の接続が開いていると、デバイスによって設定されたデフォルトの VTY 回線数である 15 が使い果たされることがあります。そのため、VTY 回線の数を 50 に増やすことを強くお勧めします。これを実行するには、次の設定コマンドを使用します。

```
C9800#config t
C9800(config)#line vty 5-50
```

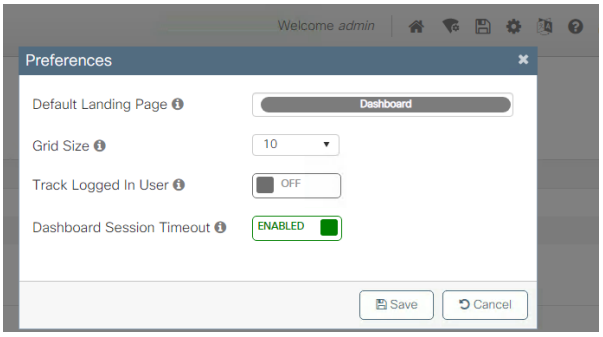
もう 1 つのベストプラクティスは、service tcp-keepalives を設定して、ボックスへの TCP 接続を監視することです。

```
C9800(config)#service tcp-keepalives in
C9800(config)#service tcp-keepalives out
```

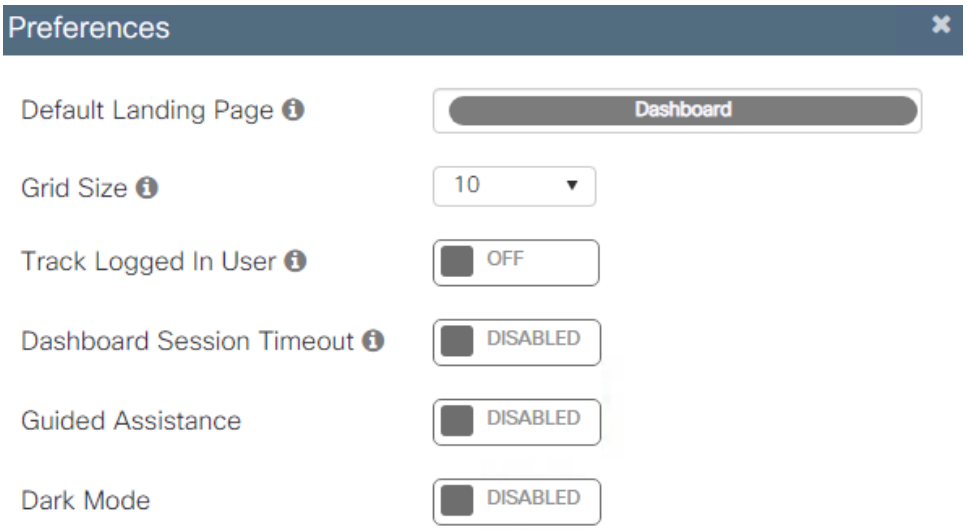
リリース 17.3 以降では、WebUI アクセス用と Web 認証 SSID のリダイレクト用に HTTP/HTTPS を個別に設定できます。ボックスへのアクセスを保護するために、WebUI アクセスの HTTP を無効にすることをお勧めします。設定オプションの詳細については、設定ガイドの「Web-Based Authentication」の章にある「Configuring HTTP and HTTPS Requests for Web Authentication」を参照してください。

[ダッシュボード（Dashboard）] ページは動的なページであり、情報が自動的に更新されます。これにより、セッション アイドル タイムアウトがトリガーされてユーザーがログアウトされる（これは、他のすべてのページで発生する）ことがありません。これを防ぐために、ダッシュボード セッション タイムアウトを有効にすることをお勧めします。ダッシュボードのタイムアウトをオンにすると、[管理（Administration）] > [管理（Management）] > [HTTP/HTTPS/Netconf/VTY] ページで設定されたセッション アイドル タイムアウトが有効になります。ダッシュボードのタイムアウトがオフになっている場合、セッションは 4 時間後に期限切れになります。

ダッシュボード セッション タイムアウトを有効にするには、任意のページの右上隅にある設定（歯車）アイコンをクリックして、次の設定を切り替えます。



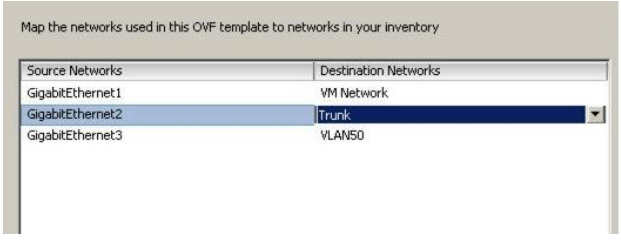
最新のリリースには、GUI 設定に関してお客様を支援するためのインライン ガイド アシスタンスが含まれています。この機能は、すべてのページで、画面の右下隅に組み込まれています。[ガイドアシスタンス（Guided Assistance）] と表示されている水色の垂直タブを探して、クリックしてください。オフにする必要がある場合は、ダッシュボード設定（歯車アイコン）から直接切り替えることができます。



C9800-CL の考慮事項

Cisco Catalyst 9800-CL（CL は「クラウド」を表す）は、プライベートクラウドまたはパブリッククラウドに展開できる仮想マシンフォームファクタです。9800-CL を扱う場合は、展開に関する考慮事項がいくつかあります。

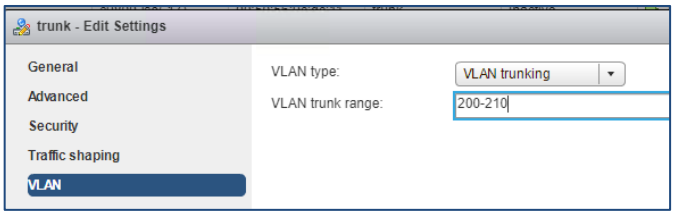
サポートされているハイパーバイザのいずれかを使用して、プライベートクラウド上で 9800-CL をセットアップする際は、複数のインターフェイスを使用する場合、それらが仮想スイッチ側で異なる仮想ネットワーク/VLAN にマッピングされることが重要です。



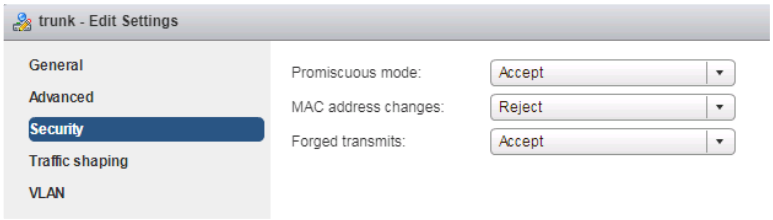
上記の例では、GigabitEthernet1 がアウトオブバンド ネットワークにマッピングされています。GigabitEthernet2 は、ワイヤレス管理およびクライアント VLAN 用のメインインターフェイスであるため、トランクとして設定され

ています。GigbitEthernet3 は冗長化ポート（RP）に使用され、専用のレイヤ 2 VLAN を持っています。ポートは、使用していない場合でも、専用ネットワークにマッピングする必要があります。

トランクを設定する場合は、使用中の VLAN のみを許可するようにすることがベストプラクティスです。



最後はセキュリティ設定です。9800-CL が接続されているポートグループで、[無差別モード（Promiscuous mode）] と [偽装送信（Forged Transmits）] の両方を [承認（Accept）] に設定する必要があります。これは、トランク接続と非トランク接続の両方に必要です。



これらのセキュリティ設定は、9800-CL が接続されている単一ポートグループに制限でき、このポートグループでのみ VLAN を使用できるようになっている限り、これらの設定は他のポートグループに接続されている他の VM には影響しません。ポートグループ内で [無差別モード（Promiscuous mode）] を [承認（Accept）] に設定すると、同じ VLAN 上にある他のすべての VM にトラフィックがフラッディングされることに注意してください。このため、ポートグループあたりの VM の数を制限することをお勧めします。

注： 上記の例は ESXi 用ですが、他のハイパーバイザでも同様の設定と推奨事項があります。詳細については、展開ガイドを参照してください。

9800-CL の場合は、シリアルコンソールではなく、VGA 統合コンソール（デフォルト）を使用することをお勧めします。

9800-CL をシャットダウンする場合は、次の簡単な手順に従って正常にシャットダウンすることをお勧めします。

- ハイパーバイザから VM の電源をオフにする前に、EXEC コマンド `reload pause` を実行します。このコマンドにより、ボックスがリロードされた後に一時停止し、ユーザー入力の開始を待機します。
- この時点で、VM の電源をオフにします。

設定エラーの確認

CLI または GUI を介して設定をプッシュする場合、いずれかの設定が正しく適用されていなくても、ユーザーにエラーが表示されないことがあります。ボックスによって生成されるログを表示してエラーを確認することが、常に推奨されます。これは、CLI で `show logging` を使用するか、Web インターフェイスで [トラブルシューティング（Troubleshooting）] > [Syslog] セクションを確認することによって実行できます。

設定：特殊文字

ユーザーがオープン文字列を設定する必要がある設定項目（AP 名、SSID 名、プロファイル、タグなど）について、Catalyst 9800 は特定の文字リストをサポートしています。これらは、先頭または末尾に空白がない印刷可能な ASCII 文字（ASCII 32 ～ 126）です。唯一の例外は、SSID 名の先頭にあるスペース（ASCII 文字 32）のみです。

また、SSID および AP 名が 32 文字を超えないようにしてください。印刷可能な ASCII 文字のリストについては、次を参照してください：https://en.wikipedia.org/wiki/ASCII。

簡単なヒント：CLI で「?」という文字を入力する必要がある場合は、どうすればよいでしょうか。たとえば、この特殊文字が、パラメータマップで設定する URL に含まれている場合があります。CLI で直接この文字を入力しようとすると、表示されません（そのときのモードに応じて使用可能なキーワードまたは引数が一覧表示されます）。この場合、CLI で「?」を入力するには、Ctrl + v キーを押してから「?」を入力してください。

注： 常に、SSID と AP 名が 32 文字を超えないようにしてください。

SNMP の推奨設定：

Catalyst 9800 ワイヤレス LAN コントローラでは、テレメトリに重点が置かれています。テレメトリは「プッシュ」モデルで機能し、WLC はクエリを必要とせずに関連情報をサーバーに送信します。Catalyst 9800 は、レガシー用として SNMP を引き続き提供しています。一部の情報はテレメトリ専用である場合があります。また、以前 AireOS で利用できていた SNMP オブジェクト識別子（OID）の一部が、9800 ではまだ利用できない場合もあります。

C9800 の SNMP の詳細については、次のリンクを参照してください：
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217460-monitor-catalyst-9800-wlc-via-snmp-with.html。

SNMP を使用して異なる OID をポーリングする場合は、C9800 の CPU への影響を最小限に抑えるためのベストプラクティスとして、次の CLI を設定する必要があります。

```
C9800config)#snmp-server subagent cache
```

このコマンドを使用すると、キャッシュは 60 秒後にクリアされます。この間隔を変更するには、次の CLI を使用します。

```
C9800(config)#snmp-server subagent cache timeout ? <1-100>  cache timeout interval (default 60 seconds)
```

デフォルトは、ほとんどの展開に適しています。

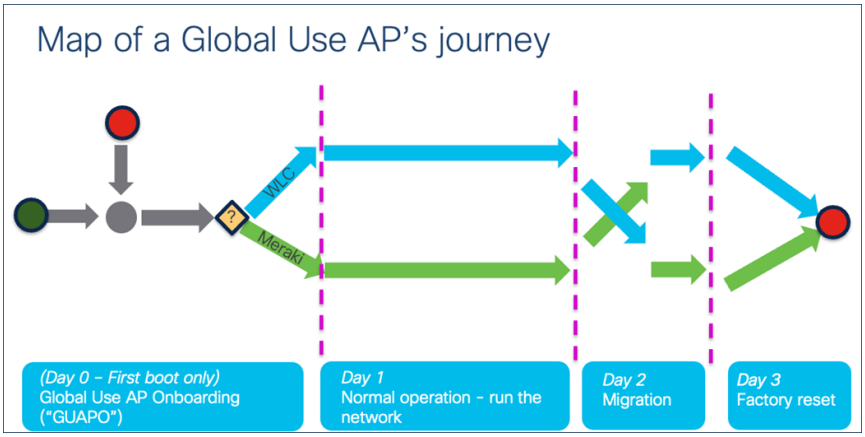
アクセスポイントの一般設定

Cisco Catalyst 9800 シリーズの設定モデルの利点は、AireOS ではグローバルである推奨設定のほとんどを、Cisco IOS XE においてプロファイルとタグを使用して AP グループで設定できることです。これにより、設定を取得する AP を柔軟に決定し、適切な値を選択できます。推奨設定を確認しましょう。

グローバル ユース アクセス ポイント

Wi-Fi 7 アクセスポイント以降では、地域または国に合わせて特定の製品を購入する必要はなくなり、1 つのだけの製品 ID をグローバルに使用できようになりました。また、何らかの理由でクラウド展開に移行する必要がある場合やその逆の場合も、これらのアクセスポイントは外部からの介入なしで移行できます。

図 2 : グローバルユース AP：プロセス



最初のステップは、AP が、Catalyst 9800 LAN コントローラに参加するか Cisco Meraki ダッシュボードに参加するかを決定することです。このガイドでは Catalyst 9800 コントローラについて説明しているため、このコントローラに焦点を当てて説明します。AP は、いくつかの方法で WLC に参加させることができます。

- **オプション 1 :** CW917x シリーズ AP からのインターネット接続があり、お客様が Cisco Meraki ダッシュボードのアカウントを持っている場合。AP を Cisco Meraki ダッシュボードに追加して、WLC に移行させます。
- **オプション 2 :** CW917x シリーズ AP からのインターネット接続がない場合。Catalyst 9800 WLC への到達のために、DHCP、DNS、ローカルステータスページ（LSP）、ブロードキャスト（IPv4）、マルチキャスト（IPv6）、または PnP などの検出メカニズムを活用します。

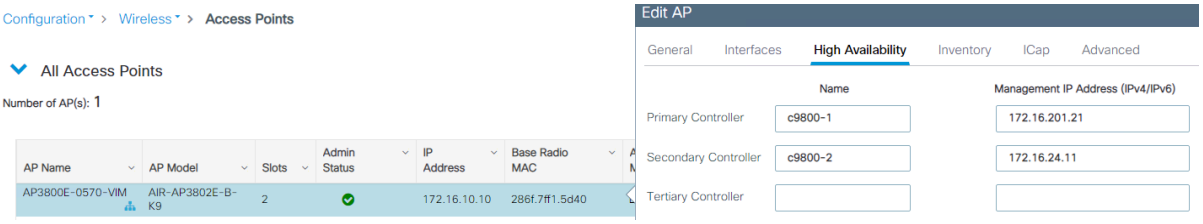
両方のオプションの詳細については、『Cisco Wireless Global Use Access Points Deployment Guide』（https://www.cisco.com/c/en/us/td/docs/wireless/access_point/technical-reference/global-use-ap-dg.html）を参照してください。

グローバルユース AP を Catalyst 9800 ワイヤレス LAN コントローラ に接続する場合、現地の RF 規制を遵守するために、AP を使用する国を決定する必要があります。グローバルユース AP は、稼働する国を複数の方法で把握できます。これについても『Cisco Wireless Global Use Access Points Deployment Guide』（https://www.cisco.com/c/en/us/td/docs/wireless/access_point/technical-reference/global-use-ap-dg.html）を参照してください。

注 : エアギャップ展開などの複雑なシナリオにおいて、GPS/GNSS 信号を取得する方法がなく、ネットワークにレガシー AP が存在せず、組織によるポリシー制限のために AP がクラウドに到達できない場合、Cisco Meraki ダッシュボードから規制アクティベーションファイル（RAF）を使用して、国コードを手動で取得できます。RAF ファイルはダッシュボードから取得されますが、AP がクラウドに到達する必要はありません。詳細については、「Country Code and Regulatory Domain」のセクション（特に「6. Regulatory Activation File」）を参照してください。

予測参加の設定：プライマリ/セカンダリ/ターシャリコントローラ

アクセスポイントを設定する場合は、CAPWAP 参加プロセス中の AP の選択を制御するために、必ず、プライマリおよびセカンダリ（およびオプションでターシャリ）コントローラの名前と IP アドレスを設定してください。これにより、ローミング時間に影響を与える可能性のある、近接している AP が異なるコントローラに参加する状態（いわゆる「ソルトアンドペッパー」シナリオ）を防止できます。プライマリ WLC とセカンダリ WLC を確定的に割り当てることにより、トラブルシューティングが容易になり、より予測可能なネットワーク運用が実現されます。AP レベルで設定するには、次の手順を実行します。



CLI で、次のコマンドを使用します。

```
C9800#ap name <APname> controller primary/secondary <WLCname> <WLC_IP>
```

また、AP プライミングプロファイルを使用してプライマリ/セカンダリおよびターシャリを割り当てることもできます。AP プライミングプロファイルは、次のためのコントローラ設定です。

- AP のプライマリ、セカンダリ、ターシャリコントローラ割り当てを定義します。
- AP グループまたは個々のデバイスに対するコントローラの一元化された割り当てを可能にします。
- AP が割り当てられたコントローラとの接続を失ったときのフォールバックおよび再接続の動作を自動化します。

詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_set_ap_priority.html?bookSearch=true#conf-ap-prime-profile を参照してください。

プライマリへの AP フォールバック

デフォルトでは、プライマリコントローラが到達不能であり、AP がセカンダリ（またはターシャリ）コントローラに参加する場合、その APは、セカンダリ/ターシャリコントローラに参加した状態を維持しつつ、プライマリコントローラに探索要求を送信しつづけます。言い換えると、AP には「プライマリコントローラ優先設定」があり、プライマリが到達可能になるとすぐに参加しようとします。

このデフォルト動作は、[AP 参加プロファイル（AP Join Profile）] > [CAPWAP] > [高可用性（High Availability）] > [プライマリへの AP フォールバック（AP Fallback to Primary）] で変更できます。

プライマリ/セカンダリ/ターシャリとバックアッププライマリ/バックアップセカンダリの違い

プライマリ/セカンダリ/ターシャリとバックアッププライマリ/バックアップセカンダリには重要な違いがあります。

- **プライマリ/セカンダリ/ターシャリ WLC** は AP レベルで設定され、保存されます（WLC にも AP 参加プロファイルにもグローバルに保存されない）。プライマリが設定または変更されると、AP は CAPWAP のリセットを実行し、新しく設定されたコントローラに参加します。
- **バックアッププライマリ/バックアップセカンダリ**の設定は、AP 参加プロファイルの WLC レベルで設定され、AP にプッシュされます。これらは、プライマリ、セカンダリ、およびターシャリが応答しない場合にのみ使用されます。

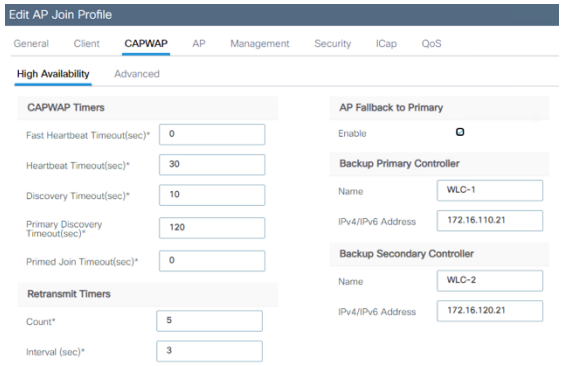
2 つのタイプの冗長化コントローラ間にある動作の違いを理解することは重要です。

- AP は、現在参加しているコントローラに到達できない場合、すべての探索応答を収集し、リストから使用可能なコントローラをプライマリ、セカンダリ、ターシャリ、プライマリバックアップ、セカンダリバックアップの順に選択します。
- AP フォールバック（前のセクションを参照）は、プライマリコントローラにのみ適用され、他のコントローラには適用されません。

また、コントローラ障害検出時間を調整するために、さまざまなタイマー（ハートビートタイマー、探索要求タイマーなど）を設定できます。

- **ハートビート**タイムアウト（秒）：このタイマーは、デバイス障害を検出して CAPWAP を再起動するために使用されます。CAPWAP を再起動すると、AP は探索メカニズムを開始し、セカンダリ/ターシャリ/バックアッププライマリ/バックアップ セカンダリ コントローラを選択します（使用可能な場合）。
- **高速ハートビートタイムアウト**（秒）：このタイマーは、「通常の」ハートビートタイムアウトよりも迅速に障害を検出するためにオプションで使用できます。デフォルトでは、無効を意味する 0 になっています。一部のシナリオ（たとえば、N+1 を使用し、HA SSO を使用しない）では、高速ハートビートを有効にしたい場合があります。高速ハートビートでは「通常の」ハートビートタイムアウトよりも頻繁にハートビートが送信されるため、確実に、プライマリコントローラに到達できない場合のセカンダリコントローラへのスイッチオーバーが迅速になります。信頼性の高い接続が必要であるため、このメカニズムを使用する場合は注意が必要です。一般に、遅延が小さく、損失がほとんどない LAN シナリオでのみ使用することが推奨されます。
- **探索タイムアウト**（秒）：応答があったコントローラの中から参加するコントローラを決定する前に、AP がコントローラからの応答を収集する時間を決定します。AP がコントローラに参加するには、少なくとも 1 つの探索応答が必要です。コントローラからの応答がない場合は、プロセスが再起動します。
- **プライマリ探索タイムアウト**（秒）：AP が、設定されたプライマリ以外のコントローラに参加している場合に、プライマリ探索要求を送信する間隔。プライマリ探索タイムアウトは、有効になっている場合、AP がプライマリへのフォールバックを開始するまでの時間を決定します。
- **準備参加タイムアウト**（秒）：AP がコントローラ探索プロセス中であり、参加するコントローラを決定するためにコントローラからの探索応答を待機している場合、この準備参加タイムアウトが適用されます。準備参加タイムアウトの間、AP はプライマリ/セカンダリ/ターシャリコントローラへの参加のみを試み、他のコントローラから受信した探索応答を無視します。準備参加タイムアウトは、デフォルトでは無効になっています。

AireOS とは異なり、Catalyst 9800 では AP 参加プロファイルレベルでバックアップ WLC を設定できるため、AP グループに対して設定できますが、AireOS ではグローバルレベルでのみ可能です。WebUI で、[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [AP 参加（AP Join）] に移動します。



CLI では、AP プロファイルにあります。

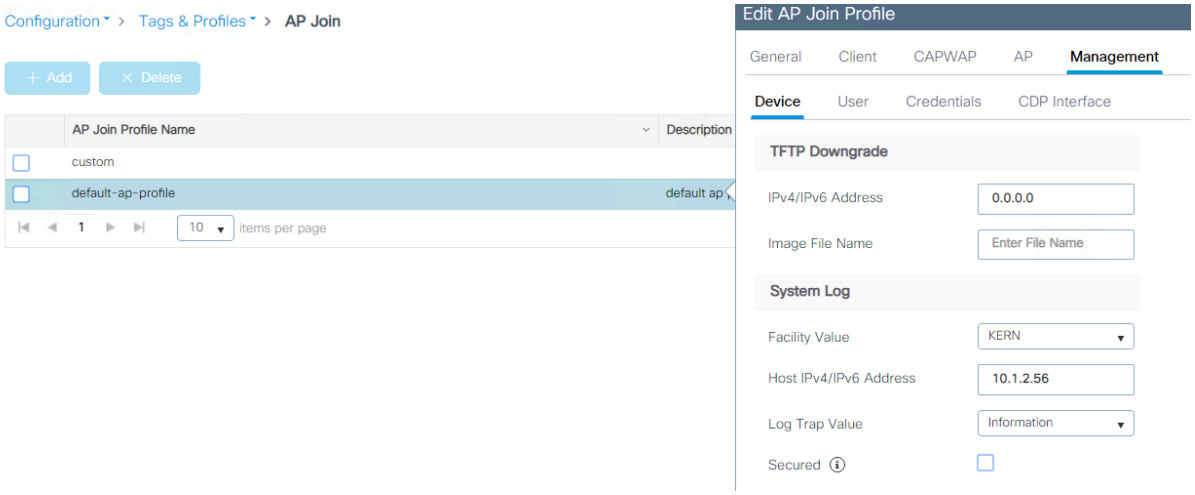
```
C9800(config)#ap profile <name>
C9800(config-ap-profile)#capwap backup primary <name> <IP>
```

AP syslog の宛先の設定

アクセスポイントは、トラブルシューティングと保守性のために重要なイベントに関する syslog を生成します。デフォルトでは、ローカルブロードキャスト接続先（255.255.255.255）を使用するため、AP が出荷時状態であって

も、ローカルキャプチャを実行することによって、発生する可能性がある問題に関する情報を取得できます。パフォーマンス、セキュリティ、およびトラブルシューティングの容易さのために、ユニキャスト接続先を設定し、問題が発生した場合に後で分析するための AP ログを保存することをお勧めします。

コントローラに参加するすべてのアクセスポイントに対して設定するには、デフォルト AP プロファイルで syslog サーバーの IP アドレスを設定します。



CLI では、デフォルト AP プロファイルにあります。

```
C9800(config)#ap profile default-ap-profile
C9800(config-ap-profile)# syslog host <IP>
```

ユーザーは、カスタム AP プロファイルとタグを使用して、AP グループの syslog サーバー（たとえば、ロケーションごとに異なる syslog サーバー）を設定することもできます。

注： 何らかの理由で AP からの syslog メッセージを無効にする場合は、AP 参加プロファイルで IP アドレスを 0.0.0.0 に設定します。

アクセスポイントのコンソールボーレート

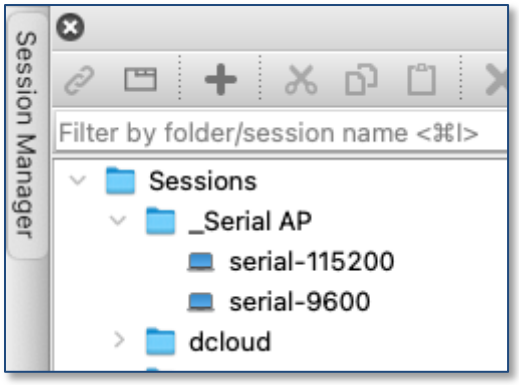
従来、AP のコンソールポートではすべての接続に対してデフォルトのボーレートである 9600 bps が使用されており、17.12.1 より前のすべての C9800 IOS XE リリースでも同様でした。IOS XE 17.12.1 以降、すべての新しい AP および工場出荷時状態にリセットされた AP のデフォルトのボーレートが 115200 bps になりました。

これは、AP の起動時間を短縮するために行われました。これにより、AP のリロードが必要な場合（新しい AP の起動、ソフトウェアのアップグレードなど）の待機時間を短縮することが可能になります。17.12.1 より前でコントローラに参加した AP は、デフォルトのボーレートを維持します。

これにより、展開に 2 つのボーレートのいずれかを持つ AP が含まれる状況が発生します。

1. 9600 bps：アップグレード前に C9800 に参加したすべての既存の AP
2. 115200 bps：17.12.1 にアップグレードした後に C9800 に参加するすべての新しい AP および工場出荷時状態にリセットされた AP

このため、ネットワーク管理者は、AP コンソールに接続するための個別の設定を用意することが推奨されます。あるボーレートの設定が機能しない場合は、他のボーレートに簡単に切り替えることができます。



単一のボーレートにする必要がある場合は、起動時間が短縮されるメリットを得るために、すべての AP を 115200 bps に移行させることをお勧めします。現在、2 つの方法でこれを実行できます。

1. 既存の AP の設定をクリアしてボーレートを変更し、すべての AP に対して 1 つの方法でコンソール接続できるようにします。ただし、この場合は、AP に設定された名前とロケーションが失われ、MAC アドレスが唯一の永続的な情報となるため、AP に MAC アドレスとの静的なタグマッピングが必要です。
2. 各 AP に接続し（コンソール、Telnet、または SSH を介して）、ボーレートを 115200 bps に設定します。

   ```
   AP# config boot baudrate 115200
   ```

   これは、手動で実行することも、Cisco DevNet サイトにある自動化ツールの WLAN Poller（https://developer.cisco.com/docs/wireless-troubleshooting-tools/#!wlan-poller-wlan-poller）を使用して自動化することもできます。

アクセスポイント向けの Cisco Discovery Protocol（CDP）

デフォルトでは、アクセスポイントは、AP 参加プロファイルで CDP が有効になっています（[AP 参加プロファイル（AP Join Profile）] > [管理（Management）] > [CDP インターフェイス（CDP Interface）] > [CDP の状態（CDP State）]）。

AP が Cisco スイッチに接続されていない場合は、CDP を無効にすることをお勧めします。これにより、CDP のフラッディングや、AP が大量の CDP ネイバーリストを報告することを回避できます。

ネットワークコントローラ設定

ここでは、ネットワークデバイスとしてコントローラの推奨設定について説明します。

アップリンクポートでのスパニングツリープロトコル（STP）設定

C9800 ワイヤレスコントローラは、AireOS WLC と同様に、ネットワークの観点からはレイヤ 2 ホストとして動作するように設計されています。これは、たとえば、スパニングツリーに参加しないことを意味します。ネットワークのコンバージェンスを高速化するために、C9800 が接続されているスイッチのアップリンクに対して PortFast または PortFast トランク設定を有効にすることをお勧めします。

コントローラのアップリンクポートでの VLAN プルーニング

コントローラのデータプレーンでの不要な作業をなくし、ネットワークループを防ぐために、必要な VLAN のみを許可するように WLC とアップリンクスイッチ間のトランクリンクを設定することをお勧めします。具体的には、ワイヤレス管理インターフェイス VLAN と中央でスイッチされるクライアント VLAN のみにします。他のすべての VLANは、トランクリンクからプルーニングする必要があります。

サービスポートの使用

C9800 物理アプライアンスでは、サービスポート（SP）はアウトオブバンド管理ポートです。これは GigabitEthernet0 インターフェイスであり、Mgmt-intf VRF にマッピングされています。このことは、このインターフェイスからトラフィックをルーティングするには、この VRF でルートを設定する必要があることを意味します。これは、ネットワークに応じて、デフォルトルートの場合もあれば特定のルートの場合もあります。次に、デフォルトルートの例を示します。

```
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 <gateway>
```

WebUI および SSH アクセスに加えて、SP からコントロールプレーンのトラフィックを送信することも可能ですが、送信元インターフェイスを設定して C9800 に Mgmt-intf またはその VRF のインターフェイスを使用させる必要があります。

以下に、TACACS+ の設定例を示します。これは、次のようにグローバルに設定するか、

```
ip tacacs source-interface GigabitEthernet0/0 vrf Mgmt-intf
```

特定のグループサーバーの下で設定することができます。

```
aaa group server tacacs+ demo
 server name ISE
 ip vrf forwarding Mgmt-int
 exit
```

他のプロトコルについては、Cisco IOS XE の設定ガイドを参照してください。

注： リリース 17.6 以降では、サービスポート（SP）を介して次のプロトコルと機能がサポートされています：Cisco Catalyst Center、Cisco Smart Services Manager、Cisco Prime Infrastructure、Telnet、コントローラ GUI、DNS、ファイル転送、GNMI、HTTP/HTTPS、LDAP、CSSM と通信するためのスマートライセンス機能のライセンス、Netconf、NetFlow、NTP、RADIUS（CoA を含む）、RESTCONF、SNMP、SSH、SYSLOG、TACACS+。

Address Resolution Protocol（ARP）プロキシ

デフォルトでは、Catalyst 9800 は、宛先 MAC をブロードキャストからユニキャストに変更することによって ARP トラフィックを転送します。たとえば、ワイヤレスクライアント A が別のワイヤレスクライアント B に ARP パケットを送信する場合、Catalyst 9800 は、ユニキャスト宛先 MAC B を使用して ARP パケットを転送します。クライアント B は、応答するとともに、クライアント A の MAC アドレスも学習します。このデフォルトの動作により、2 つのクライアント間での ARP パケットの交換が最適化されます。

リリース 17.3 では、Catalyst 9800 は、ARP トラフィックのプロキシとして機能し、登録済みクライアントの代わりに応答するように設定できます。設定は、ポリシープロファイルにあります。

```
C9800(config)#wireless profile policy <name>
C9800(config-wireless-policy)#ipv4 arp-proxy
```

WLC がデバイスの代わりに ARP に応答するため、ワイヤレスデバイスのバッテリ寿命を節約できるので、この設定が推奨されます。

注： これは FlexConnect モードでもサポートされていますが、Flex プロファイルで明示的に設定する必要があります。設定ガイド（https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m-sniffer-cg.html?bookSearch=true#proxy-arp-for-flex-wireless）を参照してください。

DHCP プロキシ

AireOS では、ワイヤレスクライアントに対して DHCP プロキシを有効にすることがベストプラクティスです。C9800 の場合、DHCP プロキシは必要ありません。これは、Cisco IOS XE に、Dynamic Host Configuration Protocol（DHCP）スヌーピング、Address Resolution Protocol（ARP）インスペクションなどの組み込みセキュリティ機能があり、DHCP トラフィックのプロキシになる必要がないからです。そのため、9800 シリーズ ワイヤレス コントローラには同等の設定がありません。

DHCP ブリッジングと DHCP リレー

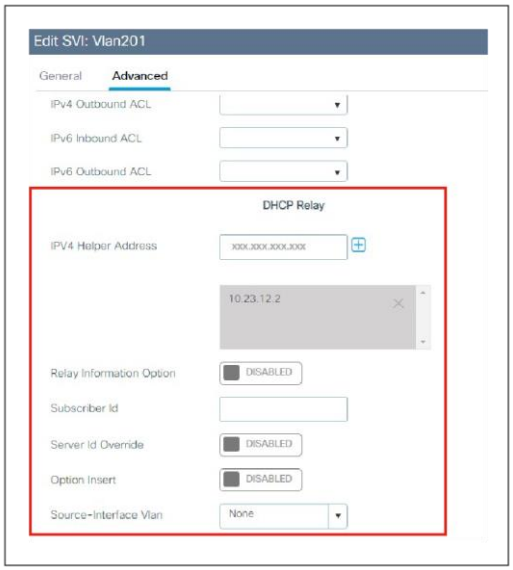
DHCP ブリッジングは、C9800 のデフォルトの動作モードであり、推奨されます。これは、クライアントの DHCP トラフィックが、SSID にマッピングされたクライアント VLAN、または AAA オーバーライドを介してクライアントに割り当てられた VLAN において、コントローラでブリッジングされることを意味します。DHCP サーバーがクライアント VLAN に存在しない場合（通常、存在しない）、上流に位置するスイッチで DHCP リレー機能を有効にすることをお勧めします。次に、VLAN 210 のワイヤレス クライアント トラフィックのデフォルトゲートウェイおよび DHCP リレーとして機能する Cisco Catalyst 9500 シリーズ スイッチの設定例を示します。

```
interface Vlan210
 description c9800-guest-vlan
 ip address 172.16.210.254 255.255.255.0
 ip helper-address 172.16.3.10
```

C9800 では DHCP リレーも設定できますが、その場合は、そのトラフィックの送信元となるレイヤ 3 VLAN インターフェイス（SVI）を設定する必要があります。複数の理由により、C9800 で DHCP リレーを設定する場合があります。次に例を示します。

- ワイヤレスチームにネクストホップスイッチ設定へのアクセス権がない。
- DHCP サーバーにオプション 82 情報を追加したい。

Catalyst 9800 で DHCP リレーを設定する場合は、SVI 設定の [詳細（Advanced）] タブ（[設定（Configuration）] > [レイヤ 2（Layer2）] > [VLAN]）で行うことをお勧めします。複数の DHCP サーバーやオプション 82 のリレー設定を定義することもできます。



リレー機能を使用すると、DHCP トラフィックはクライアント SVI の IP アドレスから送信され、ルーティングテーブル内の宛先（DHCP サーバーの IP アドレス）と一致するインターフェイスからルーティングされます。言い換えると、送信元 IP と発信インターフェイスの IP が異なる場合があります。

ネットワークで発生する可能性のある問題を回避するために、ルーティングテーブルに依存するのではなく、DHCP トラフィックの送信元インターフェイスを指定したい場合があります。これは、ネクストホップのネットワークデバイス（レイヤ 3 スイッチまたはファイアウォール）でリバース パス フォワーディング（RPF）チェックが設定されている場合です。たとえば、VLAN 201 にワイヤレス管理インターフェイスが設定されており、VLAN 210 にクライアント SVI が設定されてクライアント DHCP トラフィック用の DHCP リレーとして機能しているとします。デフォルトルートは、ワイヤレス管理 VLAN/サブネット上のゲートウェイを指しています。次に、設定の一部を示します。

```
!
interface Vlan201
 description Wireless Management
 ip address 172.16.201.5 255.255.255.0
!
interface Vlan210
 description Employee-SVI
 ip address 172.16.210.21 255.255.255.0
 ip helper-address 172.16.3.10
!
ip route 0.0.0.0 0.0.0.0 172.16.201.1
```

ip helper-address コマンドの結果として、DHCP サーバー 172.16.3.10 へのトラフィックは、VLAN 210（172.16.201.5）から送信されます。DHCP パケットの GIADDR にも同じ IP が設定されます。その後、発信インターフェイスが IP ルーティングテーブルのルックアップに従って選択されます。今回の場合は、ワイヤレス管理インターフェイス（WMI）VLAN になります。

RFP チェックが設定されたアップリンクスイッチは、VLAN 201 から着信したにもかかわらず別のサブネット（VLAN 210）の IP から送信されたパケットを認識し、そのパケットをドロップします。

これを回避するための最初の手順は、`ip dhcp relay source-interface` コマンドを使用して DHCP パケットの特定の送信元インターフェイスを設定することです。今回の場合は、DHCP パケットが WMI インターフェイス（VLAN 201）から送信されるようにします。

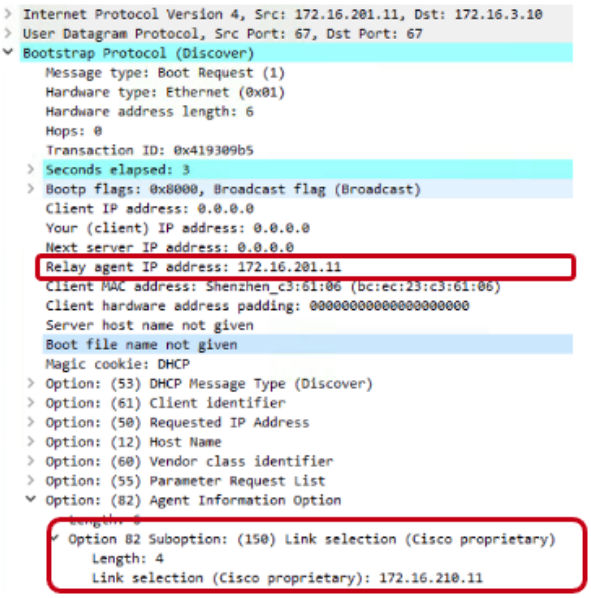
```
interface Vlan210
 description Employee-SVI
 ip address 172.16.210.21 255.255.255.0
 ip helper-address 172.16.3.10
 ip dhcp relay source-interface vlan 201
```

注： 「ip dhcp relay source-interface」コマンドをオプション 82 パラメータと組み合わせて使用するには、リリース 17.3.3 以降を使用している必要があります。

このコマンドを使用すると、DHCP パケットの送信元インターフェイスと GIADDR の両方が、DHCP リレーコマンドで指定されたインターフェイス（今回の場合は VLAN 201）に設定されます。これは DHCP アドレスを割り当て

たいクライアント VLAN ではないため、問題があります。DHCP サーバーは、どのようにして、正しいクライアントプールから IP を割り当てる方法を認識するのでしょうか。

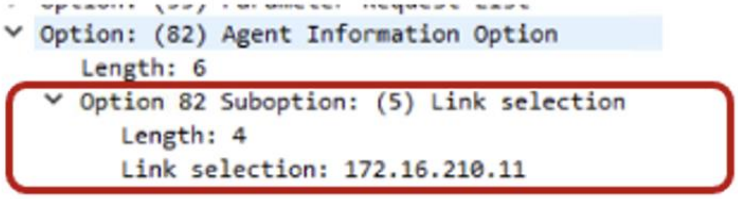
次のキャプチャに示されているように、「ip dhcp relay source-interface」コマンドを使用すると、C9800 は、オプション 82 の独自サブオプション 150（「リンク選択」と呼ばれる）にクライアントのサブネット情報を自動的に追加します。



使用している DHCP サーバーがこの情報を解釈し、機能することを確認する必要があります。標準のオプション 82 のサブオプション 5 を使用してリンク選択情報を送信するように C9800 の設定を変更することをお勧めします。これは、次のグローバルコマンドを設定することで実行できます。

```
C9800(config)#ip dhcp compatibility suboption link-selection standard
```

次の新しいキャプチャに示されているように、リンク選択のオプションが変更されています。



DHCP サーバーでは何をする必要があるでしょうか。Windows 2016 サーバーの場合は、リレーエージェントの IP を「承認」するために、ダミーの範囲を作成する必要があります。この例では、VLAN 201 つまり WMI のIP（172.16.201.11）です。IP を範囲に追加してから、配布から除外する必要があります。詳細な手順については、次のドキュメントを参照してください。

https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-subnet-options

内部 DHCP サーバー

このコントローラには、Cisco IOS XE ソフトウェアの組み込み機能を使用して内部 DHCP サーバーを提供する機能があります。ベストプラクティスは、この機能専用のボックスとなる外部 DHCP サーバーを使用することです。それでも、内部 DHCP サーバーを使用したい場合、このサーバーはテスト済みであるため、すべてのプラットフォームで、ボックスの最大クライアント数の 20% まではサポートされます。たとえば、64,000 のクライアントをサポートする 9800-80 の場合、サポートされる最大 DHCP バインディングは約 14,000 です。内部 DHCP のステータスを確認するには、次のコマンドを実行します。

```
C9800#show ip dhcp server stat
Memory usage         6840697
Address pools        11
Database agents      0
Automatic bindings   14780
```

内部 DHCP サーバーに関するその他の重要なガイドライン：

- 内部サーバーは、ワイヤレスクライアント、間接的に接続された AP（C9800 はどのモデルでも AP の直接接続をサポートしていない）、および AP からリレーされた DHCP 要求に対して DHCP アドレスを提供します。内部 DHCP サーバーを使用する場合は、クライアント VLAN に対して SVI を設定し、IP アドレスを DHCP サーバーの IP アドレスとして設定していることを確認してください。
- クライアントがデバイスの内部 DHCP サーバーを使用する場合、IP アドレスは、再起動後には保持されません。その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあります。IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。

関連資料：

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_dhcp_wlan_9800.html

DHCP タイムアウト

C9800 には、各クライアント状態（認証、DHCP アドレスネゴシエーション、Web 認証待ちなど）に対するタイムアウトがあります。DHCP については、クライアントが正常にアドレスネゴシエーションを完了できるように、コントローラにデフォルトのタイマーで設定されています。このタイムアウトは「IP-Learn タイムアウト」と呼ばれ、固定値で 120 秒です。

DHCP スコープおよびリース設計に関する考慮事項

DHCP スコープの枯渇を防ぐために、そのエリアに参加する可能性のあるすべてのデバイス（固定されたデバイスだけでなく、他のエリアからローミングしてくるデバイスも含める）を考慮して、DHCP スコープのサイズを決定します。

DHCP リースは、DHCP サーバーの負荷を軽減し、枯渇やセキュリティの問題を防ぐために非常に重要です。

DHCP リースに関する推奨事項：その環境での平均滞在時間に合わせて調整します。次に例を示します。

- 通常のオフィス展開の場合は、12 時間以上に設定します。
- 大学の場合は、8 時間に設定します。
- 小売業の場合は、1 時間に設定します。
- セキュリティ上の理由（不正利用時間の削減）から、非常に短く設定します（30 分など）。これにより、DHCP サーバーとコントローラの両方で負荷が高くなります。一部のクライアント実装ではトラフィックの

中断が発生する可能性もあります。また、ランダム MAC も考慮し、枯渇を回避するために DHCP リースを短めに維持してください。

ワイヤレス管理 IP アドレス設定

C9800 ワイヤレスコントローラに必要な IP アドレスは、ワイヤレス管理インターフェイス（WMI）に割り当てられる IP アドレスだけです。これは、AP への CAPWAP トラフィックの終端と、他の管理トラフィックの送信に使用されるインターフェイスです。

サービスポート（SP）への IP アドレスの割り当ては任意ですが、物理アプライアン上の SP は管理 VRF に属するため、それに応じた IP アドレスを割り当てる必要があることに注意してください。次に、アウトオブバンド ネットワークに接続するためのルートを含む SP の設定例を示します。

```
interface GigabitEthernet0/0
 description SP_out_of_band
 vrf forwarding Mgmt-intf
 ip address 10.58.55.246 255.255.255.0
 negotiation auto
!
ip route vrf Mgmt-intf 10.58.0.0 255.255.0.0 10.58.55.254
```

WMI への IP アドレス設定に関する推奨事項：

- 9800 物理アプライアンスおよびプライベートクラウドの 9800-CL の WMI に SVI を使用します。
- パブリッククラウドの 9800-CL の場合は、レイヤ 3 ポートを使用する必要があります（ブートストラップ時に自動設定される）。これは、スニファモードの AP および Hyperlocation がサポートされないことを意味します。
- Cisco Catalyst 9000 スイッチファミリ上の Cisco Catalyst 9800 組み込みワイヤレスコントローラでは、ループバック インターフェイスが使用されます。
- ループバック インターフェイスは、内部 DHCP サーバー（使用する場合）によって使用されます（この機能を使用する前に、「内部 DHCP サーバー」のセクションを参照してください）。

ワイヤレス管理インターフェイスの VLAN タグ

シスコでは、WLC のワイヤレス管理インターフェイスに VLAN タギングを使用することをお勧めします。ワイヤレス管理トラフィックがタグ付けされるように設定するには、ポート/LAG のトランク設定にネイティブ VLAN コマンドがないことを確認してください。次に例を示します。

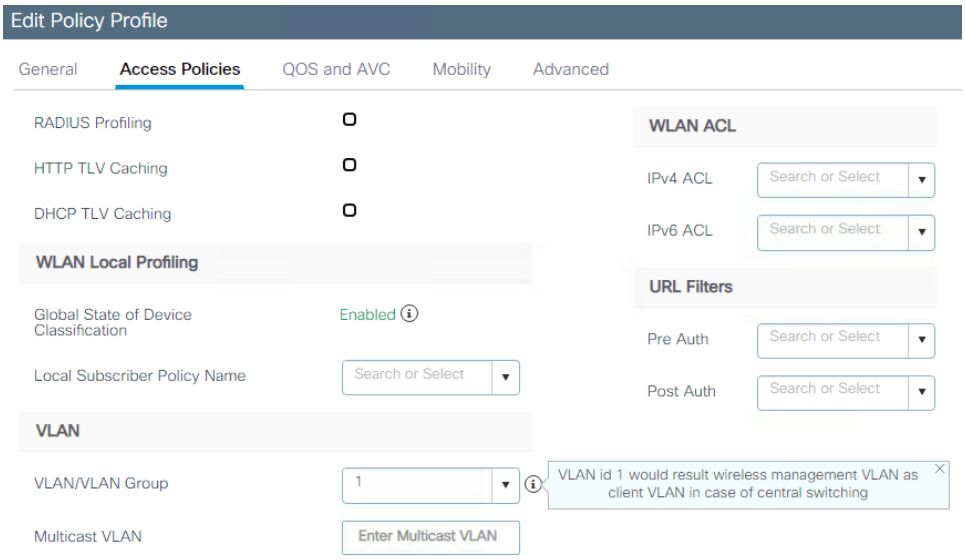
```
interface GigabitEthernet2
 switchport trunk allowed vlan 201,210,211
 switchport mode trunk
```

VLAN 201 はワイヤレス管理インターフェイス VLAN であり、210 と 211 はクライアント VLAN です。対応する VLAN がスイッチポートでも許可されており、トランクによってタグ付けされている（ネイティブ VLAN ではない）ことを確認してください。この設定例では、ネイティブ VLAN（デフォルトでは VLAN 1）がトラフィックの伝送に使用されないことが前提となっています。

注： これは、すべてのデバイス（AP、WLC、クライアント）が同じ VLAN 上にある可能性がある小規模の組み込みワイヤレスコントローラ（EWC）ベースのネットワーク展開を除くほとんどのシナリオで実行する必要があります。これはシンプルなネットワークですが、セキュリティも低くなります。

ポリシープロファイルでの VLAN 1 の使用

クライアントトラフィック用の VLAN を設定するには、[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [ポリシー（Policy）] に移動します。[アクセスポリシー（Access Policies）] で、[VLAN] フィールドを設定できます。これは、Catalyst 9800 のポリシープロファイルで VLAN ID = 1（および VLAN 名「default」）の使用に関連する重要な補足説明です。



動作は、AP のモードによって異なります。ローカルモード/Flex 中央スイッチングの AP の場合は、次のようになります。

- vlan-name = default を指定すると、クライアントは VLAN 1 に割り当てられます。
- vlan-id 1 を使用すると、クライアントがワイヤレス管理 VLAN に割り当てられます。

ユーザーにこのことを通知する警告が表示されます。

FlexConnect ローカルスイッチングモードの AP の場合は、次のようになります。

- vlan-name = default を指定すると、クライアントは VLAN 1 に割り当てられます。
- vlan-id 1 を使用すると、クライアントはネイティブ VLAN に割り当てられます。

デフォルトでは、ユーザーがポリシープロファイルで何も設定しない場合、WLC は vlan-id 1 を割り当てます。そのため、クライアントは、ローカルモードではワイヤレス管理 VLAN を使用し、FlexConnect モードでは AP のネイティブ VLAN を使用します。

ワイヤレス クライアント インターフェイス

中央スイッチングされるトラフィックの場合、SSID にマッピングされるレイヤ 2 VLAN（または VLAN のプール）を設定することは必須ですが、対応するレイヤ 3 インターフェイス（SVI）は必要ありません。これは、ダイナミック インターフェイス（レイヤ 3 インターフェイスおよび関連する IP アドレス）が必要な AireOS とは異なります。C9800 では、以下の場合を除き、クライアント VLAN に SVI を設定しないことをお勧めします。

- C9800 で DHCP リレーを実行する必要がある場合：これは、ネクストホップのレイヤ 3 スイッチ（その VLAN のデフォルトゲートウェイ）でこの機能を設定できないか、DHCP リレーされるパケットにオプション 82 情報（AP のロケーション、AP の MAC など）を追加するためです。
- 17.9.1 より前のコードを実行しており、mDNS ゲートウェイを有効にしたい場合：17.9.1 以降では、mDNS ゲートウェイ機能にクライアント SVI インターフェイスは必要なくなりました。
- 静的 IP のクライアントがあり、VLAN グループを使用している場合：これには SVI が必要です。詳細については、設定ガイド（https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_conf_vlan_grp_vewlc.html#vlan-grp-supp-dhcp-stat-ip-cl）を参照してください。

注： C9800 で複数の SVI を設定する場合は、特定の VLAN 間での不正な通信を防止するために、アクセス制御リスト（ACL）を設定することをお勧めします。たとえば、クライアント VLAN が設定されている場合は、対応するサブネットからのクライアントトラフィックのみを許可する必要があります。また、有線クライアントは、クライアント SVI インターフェイスを使用してボックスに接続できないようにする必要があります。

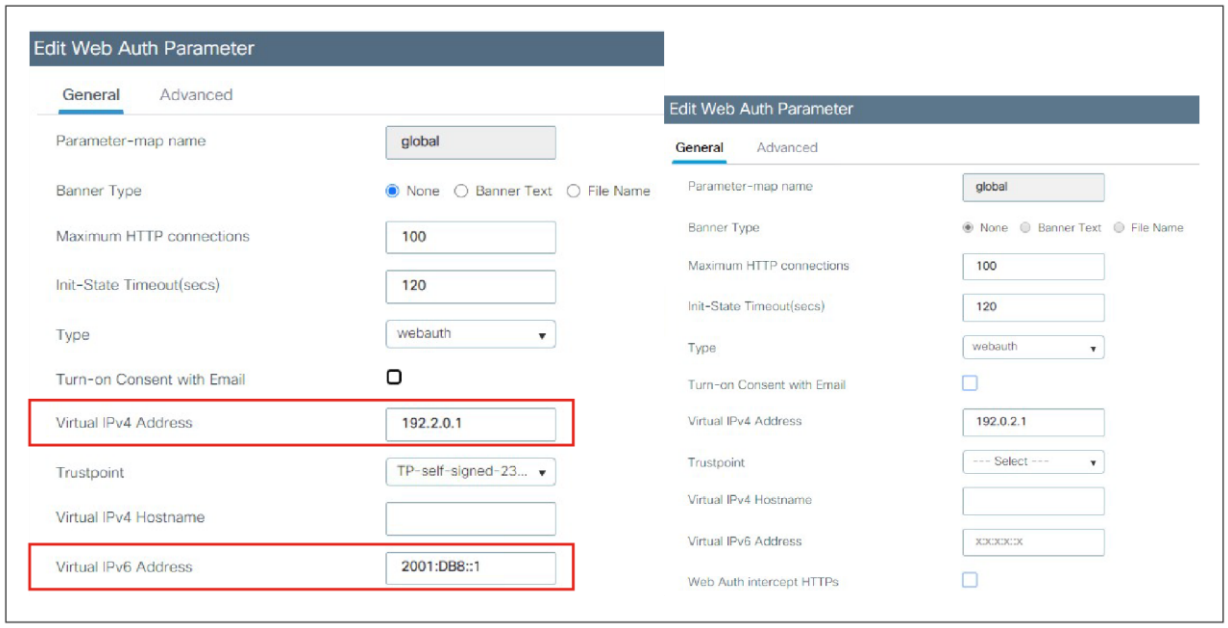
仮想 IP アドレス

AireOS と比較して、C9800 では仮想 IP アドレス（IPv4 および IPv6）の使用は Web 認証に限定されています。具体的には、リダイレクト機能のためや、Web 認証証明書をインストールして信頼させるために必要です。仮想インターフェイスには、ルーティング不可能な IP アドレスを設定することをお勧めします。ネットワーク インフラストラクチャ アドレスとオーバーラップしていないアドレスが理想的です。IPv4 と IPv6 の両方の仮想 IP を設定することをお勧めします。IPv4 については、RFC 5737 で提示されているオプション（たとえば、192.0.2.0/24、198.51.100.0/24、および 203.0.113.0/24 ネットワーク）のいずれかを使用できます。IPv6 については、RFC 3849 で規定されているプレフィックス 2001:DB8::/32 を使用できます。

注： IPv6 のみのクライアントネットワークでは、IPv6 リダイレクト アドレス オプションを設定することが重要です。

仮想 IP が設定されていないと、クライアントは、設定された外部ポータルではなく内部ポータルにリダイレクトされることがあります。

仮想 IP アドレスはグローバルパラメータマップで設定でき、初期セットアップ用の Day 0 GUI を使用する場合、IPv4 についてはデフォルトで 192.0.2.1 に設定されます。



リンク集約モード

リンク集約（LAG）モードは、冗長化と追加のネットワーク帯域幅を提供するため、推奨される動作モードです。同じアップリンクスイッチへの複数の物理リンクが使用可能な場合は、これを常に使用する必要があります。LAG モードは C9800 のポートチャネル機能を使用して設定され、これを有効にするためにボックスをリロードする必要はありません。次に、いくつかの重要な推奨事項を示します。

- LAG を使用する場合は、コントローラのすべてのポートで、スイッチ側と同じレイヤ 2 設定になっていることを確認してください。たとえば、あるポートで VLAN をフィルタし、それ以外のポートではフィルタしない、ということは避ける必要があります。
- ポートチャネルの物理ポート間で最適な負荷分散を実現するには、`src-dst-mixed-ip-port` オプションを使用します。C9800 コントローラとネイバースイッチで同じオプションを設定することが重要です。

```
C9800(config)#port-channel load-balance src-dst-mixed-ip-port
```

- スタンドアロンの C9800 では、静的（モード ON）と動的（Link Aggregation Control Protocol（LACP）/Port Aggregation Protocol（PagP））の両方のポート チャネル ネゴシエーションがサポートされています。モードは、ポートチャネルグループに参加しているすべてのインターフェイスで選択する必要があります。

```
C9800(config-if)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PagP only if a PagP device is detected
  desirable  Enable PagP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
```

- SSO ペアでは、初期リリース以降、ポートチャネルは静的モード（モード ON）をサポートしています。リリース 17.1 以降では LACP もサポートされています。

ゲストまたは AAA オーバーライドのシナリオにおけるトラフィックリークの防止

「ブラックホール」VLAN は、コントローラ上で設定されたクライアント VLAN が、スイッチへのトランクで転送されない、スイッチ上に存在しない、またはデフォルトゲートウェイを欠いている特定の設定シナリオです。この

VLAN に割り当てられているクライアントは、トラフィックを渡したり、ネットワークの接続先に到達することができません。これの目的は、人間による設定エラーを防止し、トラフィックリークの可能性を減らすことです。

このシナリオの対象は、次のとおりです。

- ゲストアクセスまたはモビリティ自動アンカー：フォーリンレベルでブラックホール VLAN を設定して、フォーリンレベルでのトラフィックリークがないことと、アンカーで割り当てられた VLAN を経由した接続のみが可能であることを確認します。
- AAA オーバーライド：これには、すべてのクライアントが RADIUS サーバーから割り当てられた VLAN を取得する必要があります。取得しない場合、どのネットワーク接続先にも到達できません。

ネットワーク アクセス ポイントの設定

ここでは、APの 推奨ネットワーク設定について説明します。

AP とワイヤレス管理インターフェイス VLAN

ワイヤレス管理インターフェイス（WMI）VLAN とは異なる VLAN にアクセスポイントを配置することがベストプラクティスであり、通常、どの実稼働展開でもそのようにされます。ステージングやテスト目的で、WMI と同じ VLAN に AP を設定する必要がある場合は、AP の数を 100 未満に制限することをお勧めします。

AP とコントローラの間のラウンドトリップ遅延

ローカルモードとファブリックモードの AP については、アクセスポイントとコントローラの間のラウンドトリップ遅延が 20 ミリ秒（ms）を超えないようにします。これは AireOS の場合と同じです。

AP スイッチポートでの PortFast の使用

ローカルモード、ファブリックモード、または中央でスイッチされる WLAN のみを扱う FlexConnect モードの AP のスイッチポートでは PortFast を使用します。PortFast のスイッチポートを設定するには、switch port host コマンドを使用するか、PortFast コマンドを直接使用して、ポートをホストポートとして接続するように設定します。これにより、AP の参加プロセスが高速になります。ローカルモードの AP では VLAN 間でトラフィックが直接ブリッジされないため、ループが発生するリスクはありません。ポートはアクセスモードで直接設定できます。

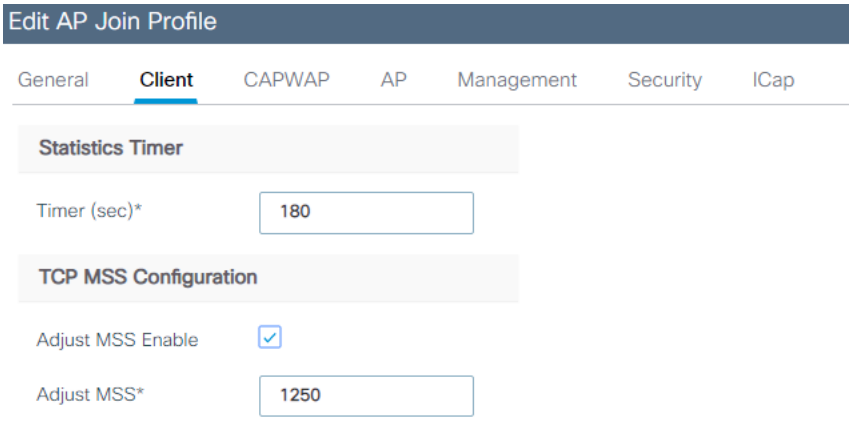
注： Flex モードおよびローカルスイッチングの AP の場合、ほとんどのシナリオでスイッチポートをトランクモードにする必要があります。これらの場合は、スイッチポートで `spanning-tree portfast trunk` を使用します。

FlexConnect モード AP スイッチポートの VLAN のプルーニング

FlexConnect モードの AP で、異なる VLAN にマッピングされたローカルにスイッチされる WLAN を使用する場合（AP スイッチポートはトランクモード）、ポートに存在する VLAN をプルーニングまたは制限して、AP が設定された VLAN と一致させます。

すべての AP での TCP MSS の有効化

CAPWAP での TCP クライアントトラフィックのカプセル化を最適化するために、TCP 最大セグメントサイズ（MSS）機能を常に有効にすることをお勧めします。これにより、CAPWAP フラグメンテーションの全体的な量を削減し、ワイヤレスネットワーク全体のパフォーマンスを向上させることができます。MSS 値は、トラフィックタイプと、WLC から AP へのパスの最大伝送ユニット（MTU）に応じて調整する必要があります。C9800 では、TCP MSS 調整がデフォルトで有効になっており、値は 1250 バイトです。これはほとんどの展開において適切な値と考えられますが、セットアップによってはさらに最適化できます。



CLI では、AP プロファイル（カスタムまたはデフォルト）にあります。

```
C9800(config)#ap profile custom
C9800(config-ap-profile)# tcp-adjust-mss ?
  enable  Enable TCP MSS for all Cisco APs
  size    TCP MSS configuration size
```

これは、C9800 の AP 参加プロファイルでの設定であるため、AP グループまたはロケーションごとに異なる値を設定できます。

SSID/WLAN の設定

ここでは、SSID/WLAN に関する推奨事項について説明します。C9800 では、これらの設定が WLAN 設定自体に常に適用されるわけではありません。ほとんどの場合、ポリシープロファイルが使用されます。一般に、WLAN の変更できない部分であるセキュリティは、WLAN プロファイルで設定されます。その他の WLAN プロパティ（QoS、VLAN など）は、ポリシープロファイルで設定されます。このアプローチにより、ユーザーは、ポリシーを毎回再設定することなく、共通ポリシーを定義して複数の SSID に適用することができます。

ブロードキャスト SSID の使用

WLAN は、SSID 名を「隠して」にして、プローブ要求に明示的な SSID が含まれている（つまり、クライアントがその名前を認識している）場合にのみ応答することによって動作できます。デフォルトでは、SSID はビーコンに含まれており、AP は、Null プローブ要求に応答して、クライアントに事前に設定されていない場合でも SSID 名情報を提供します。SSID を隠しても、セキュリティは向上しません。単純な攻撃を実行して SSID 名を取得することは常に可能であり、一部のクライアントタイプ（Apple iOS など）で関連付けが遅くなるといった副作用もあります。一部のクライアントは、このモードでまったく安定して動作しません。唯一の利点は、接続を試行するデバイスからのランダムな関連付け要求を防止できることです。クライアントの相互運用性を最適化するために、ブロードキャスト SSID オプションを有効にすることをお勧めします。

ブロードキャスト SSID は、C9800 コントローラではデフォルトで有効になっています。

音声用の Cisco Centralized Key Management のタイムスタンプ検証

注： Cisco Centralized Key Management は非推奨になりました。このセクションは、今後の更新で削除される予定です。

Cisco Centralized Key Management を引き続き使用しているデバイスがある場合、Cisco ベースのクライアント（8821 IP 電話、Cisco ワークグループブリッジなど）を使用する際のローミングの問題を回避するために、CCKM 検証を 5 秒に変更することを強くお勧めします。このパラメータを設定するには、WLAN 設定の下で次のコマンドを使用します。

```
C9800(config-wlan)#security wpa akm cckm timestamp-tolerance 5000
```

5000 は 5 秒に相当します。

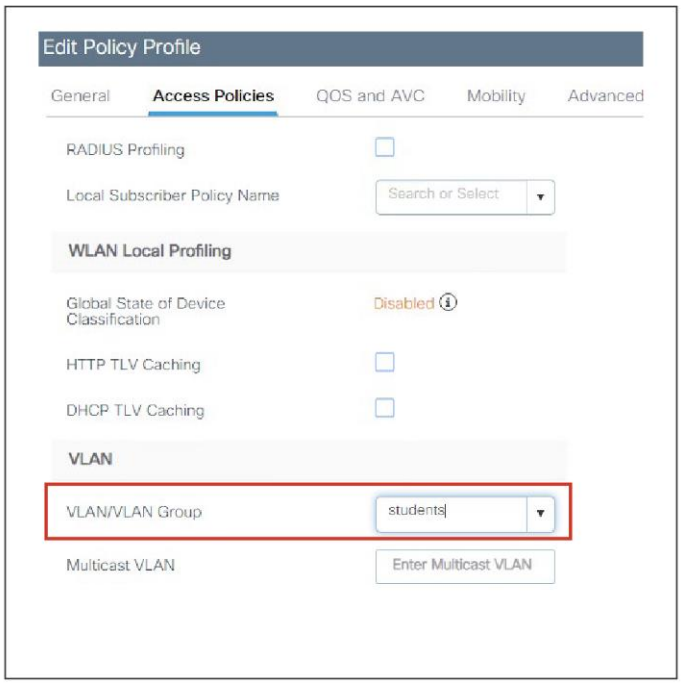
VLAN グループ

VLAN グループは、AireOS のインターフェイスグループ/VLAN 選択機能に相当します。この機能により、負荷分散のために、異なる DHCP プールに対応する複数の VLAN を動的にサポートできる単一の WLAN を使用できます。クライアントは、MAC アドレスのハッシュを使用して、設定済みの VLAN のいずれかに割り当てられるため、VLAN グループの設定に変更がないかぎり、その割り当ては長期間にわたって保持されます。VLAN グループプール機能は、DHCP サーバーの応答をモニターし、DHCP アドレスの割り当てを取得できなかったクライアントがいる VLAN の使用を自動的に停止します。

この機能を有効にするには、次の手順を実行します。

1. VLAN グループを作成し、クライアント VLAN を追加します。

2. ポリシープロファイルに VLAN グループを追加します。



マルチキャスト VLAN

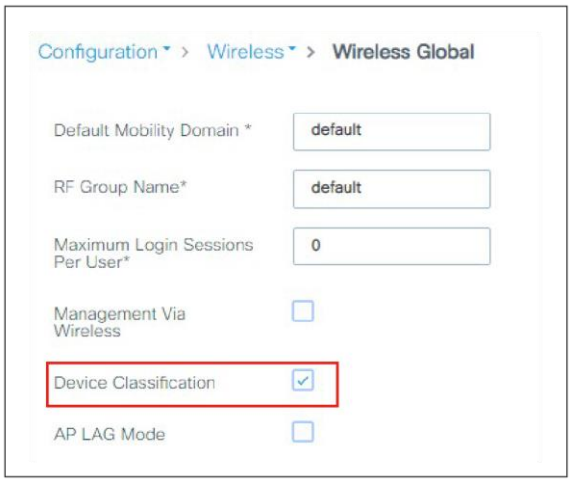
VLAN グループが使用されている場合は、マルチキャスト VLAN を有効にして、無線上のマルチキャストを事前定義されたマルチキャスト VLAN 上の単一のコピーに制限することをお勧めします。

マルチキャスト VLAN はポリシープロファイルで有効にします。

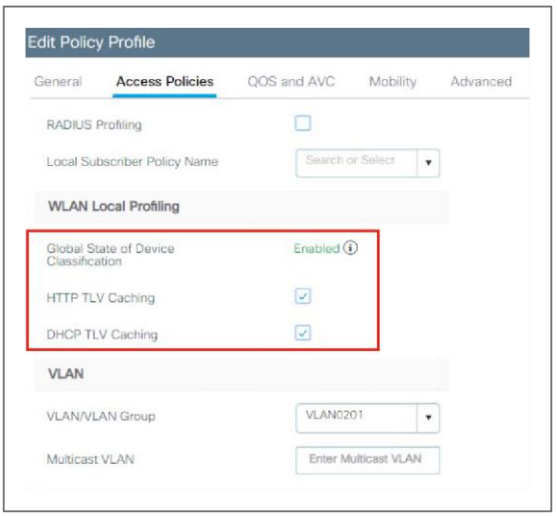
クライアント プロファイリングの有効化

クライアントのタイプを把握することは、トラブルシューティングのシナリオ、デバイスタイプごとのポリシーの割り当て、またはそれらに適応させるための設定の最適化において非常に役立ちます。ローカルプロファイリングにより、外部サーバーに依存することなく、コントローラに接続されているクライアントのタイプを簡単に検出できるようになります。コントローラは、クライアントからの DHCP または HTTP 要求を解析して、既知の一連のクライアントタイプルールと照合し、デバイスタイプの最適な評価を行います。この情報は、WLC GUI で、または CLI を介して利用できます。

WLAN でローカルプロファイリングを有効にするには、関連付けられているポリシープロファイルを変更する必要があります。それを実行する前に、コントローラでデバイス分類をグローバルに有効にする必要があります。



その後に、ポリシープロファイルでクライアント プロファイリングを有効にすることができます。

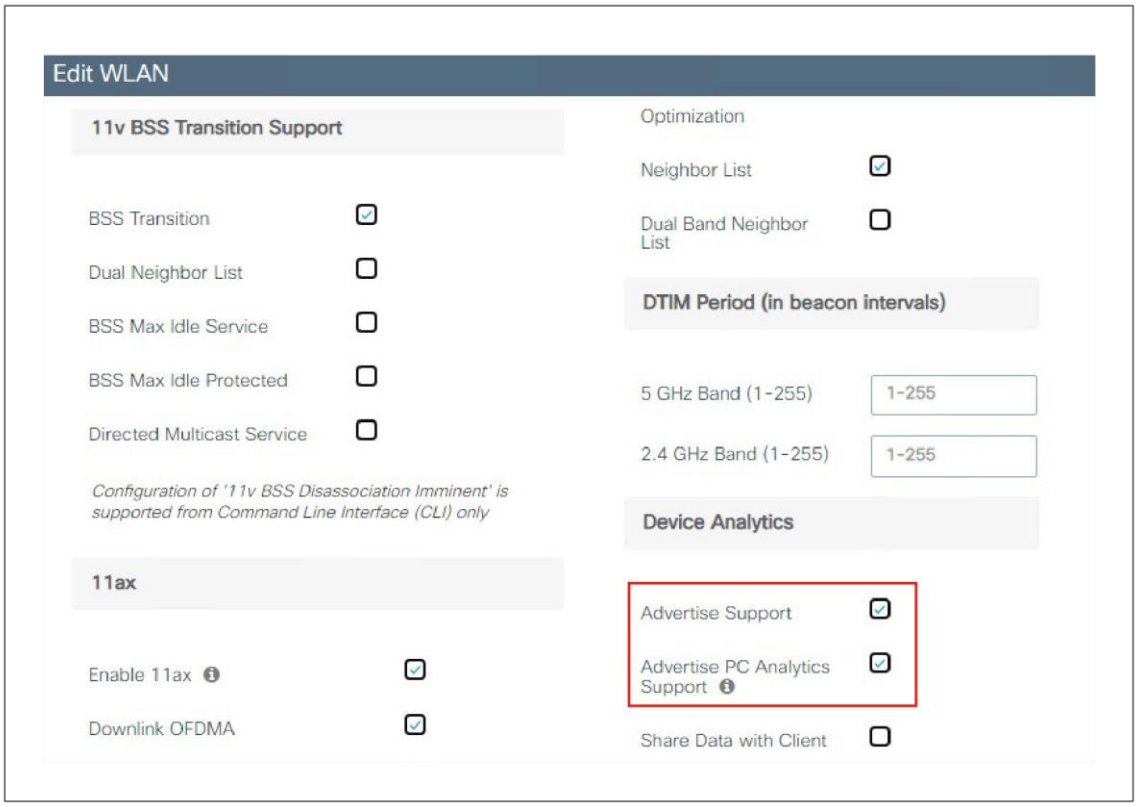


このポリシープロファイルに関連付けられているすべての WLAN で、ローカルプロファイリングが有効になります。

17.1 以降、C9800 は、エンタープライズ Wi-Fi エクスペリエンスを向上させるデバイス分析機能をサポートしています。この機能により、とりわけ、ワイヤレス クライアント デバイスの動作を分析するための一連のデータが提供されます。コントローラでデバイスプロファイリングを有効にすると、クライアントデバイスとコントローラおよび AP の間で情報が交換されます。当初、この機能は Apple および Samsung デバイスに適用されましたが、リリース 17.6 以降では、Intel チップセット（AC9560、AC8561、AX201、AX200、AX1650、AX210、AX211、および AX1675 チップセット）を搭載したデバイスに拡張されました。C9800 は、これらのデバイスから追加のクライアント情報を受信し、それを使用して、ボックスでのデバイスプロファイリングを強化できます。同じ情報が Cisco Catalyst Center とも共有され、アシュアランスに表示されます。

注： Intel の分析には PMF が必要です。PMF をオプションまたは必須として設定することを検討してください。

この機能を有効にするには、WLAN 設定の [詳細（Advanced）] タブに移動し、[アドバタイズのサポート（Advertise Support）] と [アドバタイズ PC 分析のサポート（Advertise PC Analytics Support）] を有効にします。後者が Intel デバイス向けの設定です。



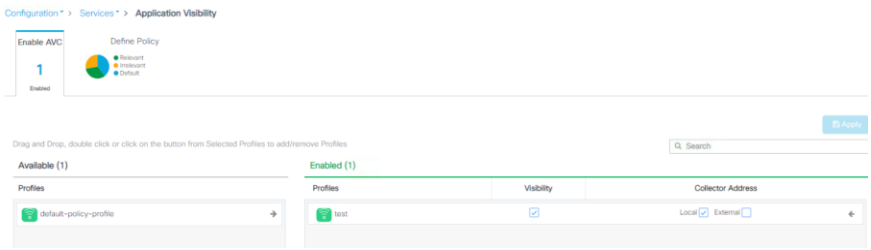
Application Visibility and Control

Application Visibility and Control（AVC）は、Network Based Application Recognition（NBAR）エンジンによるシスコのディープ パケット インスペクション（DPI）技法でアプリケーションを分類し、Wi-Fi ネットワークのアプリケーションレベルの可視性と制御を提供します。アプリケーションの認識後は、AVC 機能によってトラフィックをドロップまたはマークできます。AVC を使用することで、コントローラは、1400 を超えるアプリケーションを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストのかかるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成できます。AVC は、すべての C9800 ワイヤレス コントローラ プラットフォームでサポートされています。

注： AVC 検査は、クライアントのトラフィックスループットが最大 30% 低下するという形で、パフォーマンスに影響を与える可能性があります。プラットフォームの最大転送キャパシティに近い状態で動作しているワイヤレス コントローラ セットアップでは、使用を避ける必要があります。

Cisco Catalyst 9800 ワイヤレスコントローラでは、AVC（基本的なアプリケーション使用状況のため）がポリシープロファイルレベルで有効になっています。その後に、ポリシープロファイルを WLAN にマッピング（ポリシータグを使用）でき、その結果、AVC が SSID に適用されます。GUI から、左側の列にある使用可能なプロファイルの矢印をクリックするだけで有効になり、AVC が適用されたプロファイルが右側の列に表示されます。

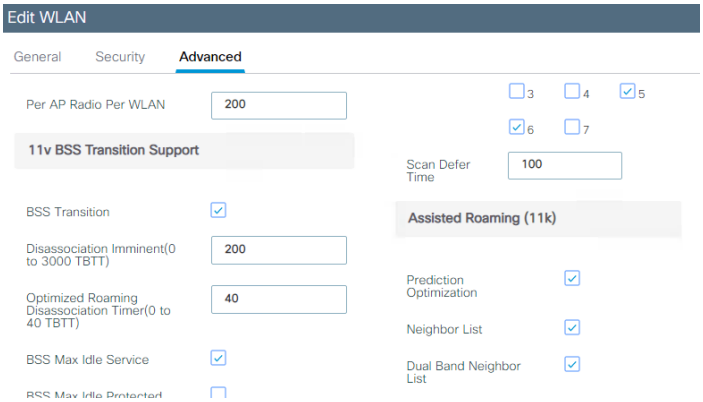
注： FlexConnect モードでは、AP ごとに 1 つの AVC プロファイルのみがサポートされます。



最適なローミングのための 802.11k の有効化

802.11k 標準では、クライアントが、ローミングの候補となる既知のネイバー AP に関する情報を示すネイバーレポートを要求することができます。802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンを軽減できます。802.11k が解決に役立つ一般的な問題は、「固定」クライアントです。これは、通常、特定の AP に関連付けられ、より近くの AP ではるかに優れたオプションが利用可能になった場合でも、その AP に強く固執するクライアントです。

802.11k 機能は、WLAN の詳細設定で直接設定できます。



デュアルバンド レポーティングでは、802.11k を有効にすることをお勧めします。デュアルバンド レポーティングを有効にすると、クライアントは、クライアントが直接要求したベストの 2.4 GHz/5 GHz/6 GHz AP のリストを受け取ります。クライアントは、ほとんどの場合、同じチャネル、次にクライアントが現在稼働している帯域の順序で、AP のリストを上から検索します。このロジックにより、スキャン時間が短縮され、バッテリーの電力が節約されます。

注： シングルバンドのクライアントを使用する場合、または主に 5 GHz 用に設定されたデバイスを使用する展開シナリオでは、デュアルリストオプションを有効にしないでください。

注： 802.11k により、不明な情報要素に誤って応答する一部のレガシーデバイスで問題が発生する可能性があります。ほとんどのデバイスでは 802.11k 情報は（サポートしていない場合でも）無視されますが、一部のデバイスでは切断や関連付けの失敗が発生する可能性があります。これらはまれなケースですが、このオプションを有効にする前にテストすることをお勧めします。

802.11v

802.11k と同様に、802.11v は、クライアントのローミングおよびバッテリ節約を支援するために後から導入されました。802.11k との主な違いは、802.11v では、AP の接続先となるクライアントがプロアクティブに提案されることです。802.11v でできる主なことを以下に示します。

Directed Multicast Service：Directed Multicast Service（DMS）を使用して、クライアントは、必要なマルチキャストパケットをユニキャストフレームとして送信するようにアクセスポイントに要求します。これにより、クライアントは、スリープ モードでは無視していたマルチキャスト パケットを受信でき、レイヤ 2 の信頼性も保証されます。

BSS 移行管理：AP が、ローミング先としてより適切な AP をプロアクティブに提案できます。これは、次の 3 つのシナリオに適用されます。

- 要請された要求：クライアントは、ローミングする前に、再度関連付ける AP のより適切なオプションを得るために、802.11v 基本サービスセット（BSS）移行管理クエリを AP に送信できます。

- 要請されない負荷分散要求：AP は、負荷が高い場合、関連付けられたクライアントに 802.11v BSS 移行管理要求を送信して、別の AP へのローミングを促します。
- 要請されない最適化ローミング要求：クライアントの RSSI とレートが要件を満たしていない場合、対応する AP は、このクライアントに 802.11v BSS 移行管理要求を送信します。

デフォルトでは、次のオプションが有効になっており、これらを有効のままにすることをお勧めします。

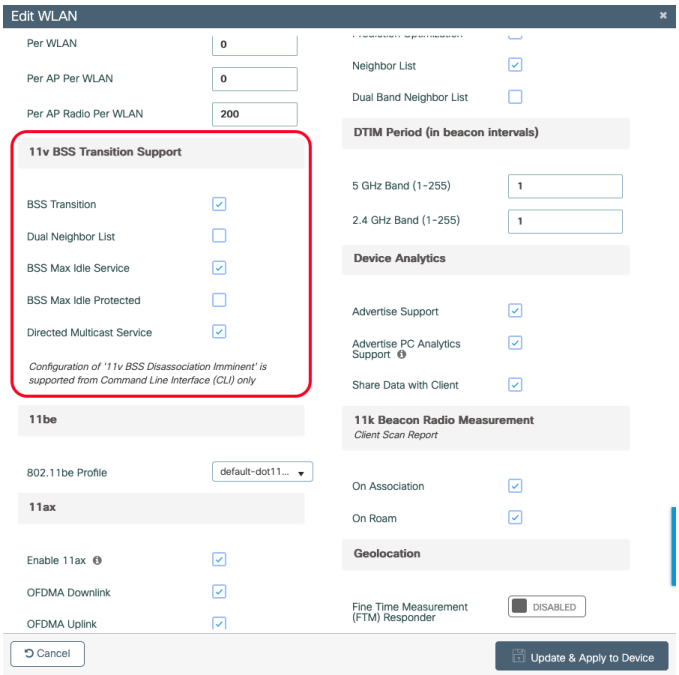
- BSS 移行
- BSS 最大アイドル
- Directed Mulicast Service

802.11k と 802.11v（BSS 移行、BSS 最大アイドルサービス、および Directed Multicast Service）の両方を有効にすることをお勧めします。

「要請されない移行要求」（CLI のみ）と「最適化ローミング」（後にある「最適化ローミング」のセクションを参照）を有効にすることはお勧めできません。

802.11v 設定を変更するには、[設定（Configuration）] > [タグとプロファイル（Tags & Profiles）] > [WLAN（WLANs）] > [WLAN の編集（Edit WLAN）] > [詳細（Advanced）] タブ > [11v BSS 移行のサポート（11v BSS Transition Support）] セクションに移動します。

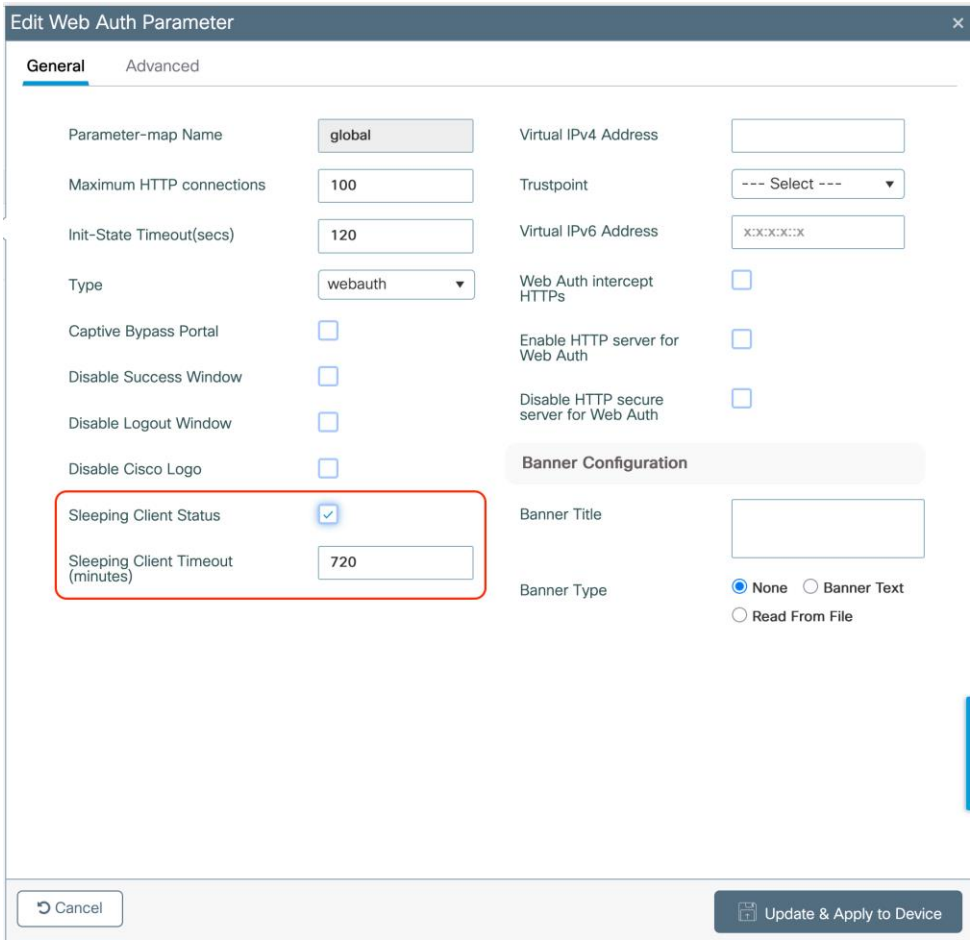
図 3：802.11v BSS 移行の設定



スリープクライアント機能

C9800 では、Web 認証パラメータはパラメータマップにあるため、スリープクライアント機能やそのタイムアウトの有効化もそこで行います。[設定（Configuration）] > [セキュリティ（Security）] > [Web 認証（Web Auth）] に移動し、デフォルトのパラメータマップを編集するか、新しいパラメータマップを作成してスリープクライアントのステータスとタイムアウトを設定します。

図 4 : Web 認証パラメータの設定

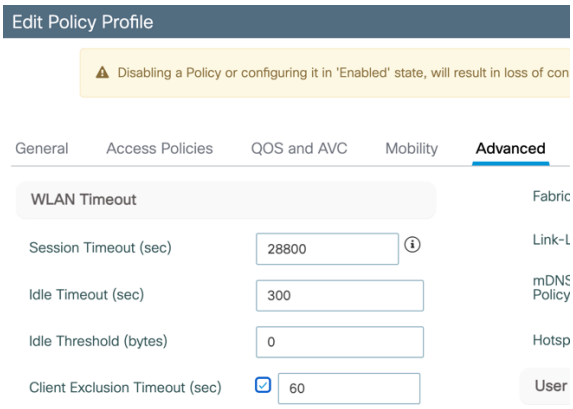


その後、パラメータマップは、[セキュリティ（Security）] > [レイヤ 3（Layer 3）] タブで WLAN プロファイルに関連付けられます。

スリープ タイマーは、アイドル タイムアウト後に有効になります。Web 認証でスリープクライアント機能を使用する場合は、クライアントが誤って削除されることを防ぐために、アイドルタイムアウトがセッションタイムアウトよりも短いことを確認してください。

クライアントタイマー

考慮する必要があるクライアントタイマーがいくつかあります。C9800 では、ポリシープロファイルでこれらのタイマーを設定することによる柔軟性が得られます。そのため、展開要件に応じて、同じ SSID であっても異なる値を適用できます。クライアントタイマーは、[ポリシープロファイル（Policy Profile）] > [詳細（Advanced）] タブにあります。



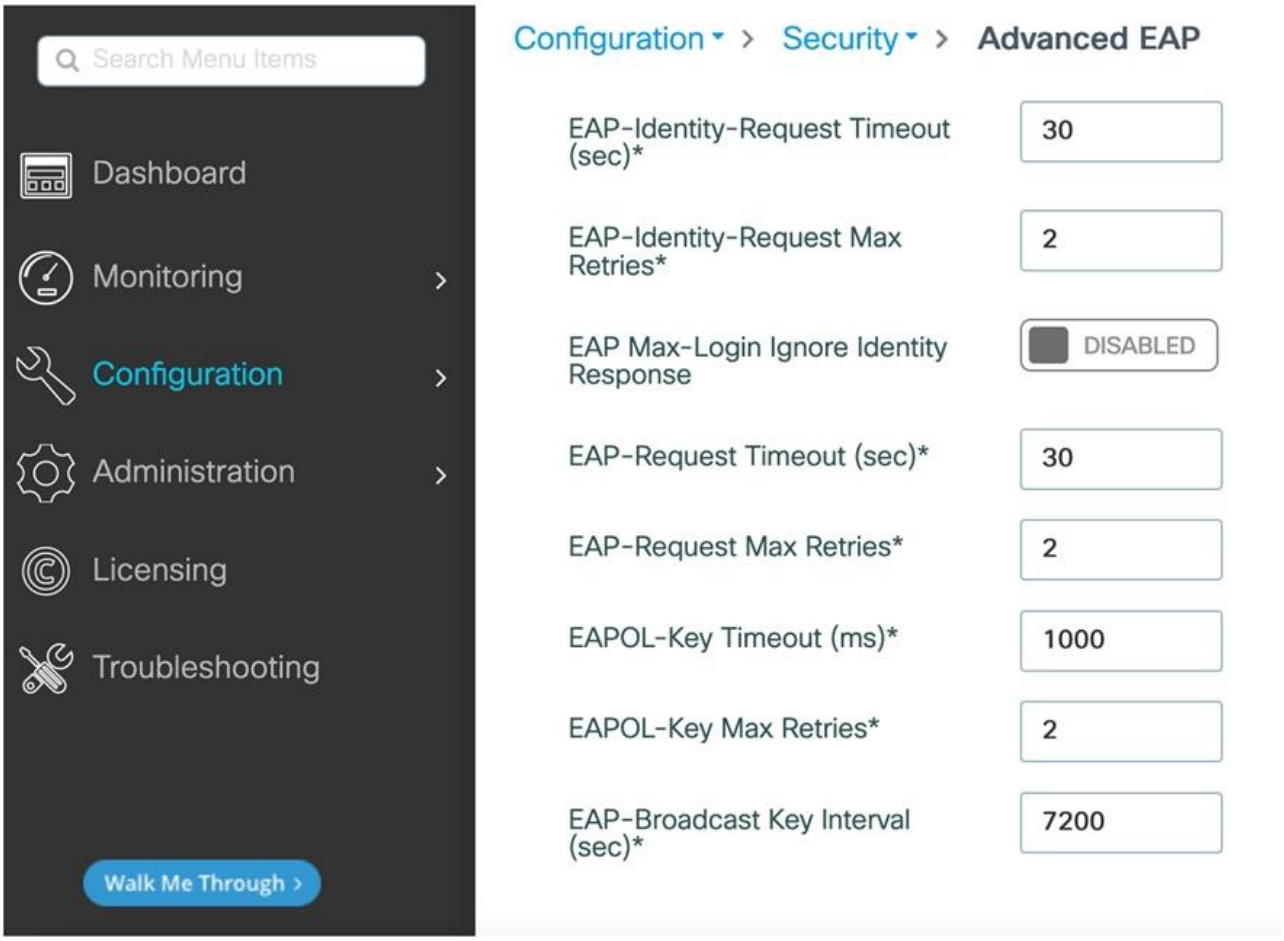
推奨値は次のとおりです。

- セッションタイムアウト = 28800 秒（8 時間）が、すべての SSID およびポリシープロファイルの推奨値です。

注： AireOS では、0（ゼロ）に設定されたセッションタイムアウトは、可能な最大のタイムアウトを意味します。17.4.1 より前のリリースの C9800 では、実際には「セッションタイムアウトなし」を意味するため、AireOS と同じ設定を使用すると、C9800 ネットワーク上のすべてのローミングがスローローミングになり、完全な再認証が必要になります。

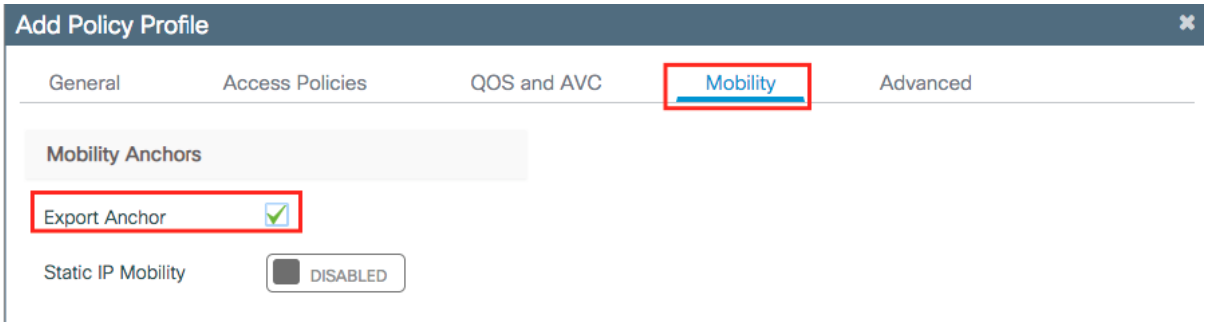
- リリース 17.4.1 以降では、802.1x 認証用に設定された WLAN において、ユーザーが 0（含む）～ 300 秒の任意の値を設定すると、セッションタイムアウトは自動的に 86400 秒（24 時間）に設定されます。これは、サポートされる最大値です。
- WLAN ごとのユーザー アイドル タイムアウトは 300 秒（5 分）に設定してください。これは、多数のクライアントが存在する高密度展開（スタジアム、会議場、大学など）で特に重要です。ランダム MAC アドレス（「ローカル管理アドレス」とも呼ばれる）を使用するデバイスがますます増えているため、アイドル時間が長いと、AP がこれらのランダム MAC エントリを保持し、最大ステーション数に達したことが原因で AP が新しいクライアント関連付けを拒否する可能性があります。また、アイドルタイムアウトを短くすることで、大規模なアカウンティング更新が AAA サーバーに送信されることを回避できます。

注： クライアントがカバレッジエリアを出入りするシナリオや、クライアントがバッテリ駆動で頻繁にスリープ状態になる可能性がある場合は、クライアントが削除される可能性を減らすために、アイドルタイムアウトを 3,600 秒（60 分）に増やすことを検討できます。除外タイムアウトは有効にする必要があり、通常、除外時間は 60 秒に設定されます。アイドルタイムアウトの変更が必要な場合は、EAP ブロードキャストキー間隔がアイドルタイムアウトよりも長いことを確認してください。これは、AAA サーバーが過負荷状態になる可能性がある「一括」クライアント削除を回避するためです。ブロードキャスト ローテーション タイマーは、[設定（Configuration）] > [セキュリティ（Security）] > [高度な EAP（Advanced EAP）] セクションで変更できます。



SSID のアンカーリングとローカル AP へのブロードキャスト

（ゲスト）SSID をフォーリン WLC からアンカー WLC にトンネリングさせるには、ポリシープロファイルを適切に設定する必要があります。フォーリンでは [ポリシープロファイル（Policy Profile）] > [モビリティ（Mobility）] タブでアンカー IP を選択し、アンカー WLC では同じタブで [エクスポートアンカー（Export Anchor）] 機能を有効にします（次の図を参照）。



上記の設定を有効にした時点で、同じプロファイルを、アンカーコントローラに参加している AP でブロードキャストする必要がある WLAN/SSID に関連付けることができなくなります。アンカー WLC は、通常、DMZ 内にあって、トンネルトラフィック専用であり、ローカルに登録されたアクセスポイントを持たないため、このシナリオが発生することはほとんどありません。ただし、そのような状況において、フォーリンで定義されているものと同じ SSID をアンカーでもブロードキャストしたい場合は、アンカー WLC で別のポリシープロファイルを定義する必要があります。その場合は、[エクスポートアンカー（Export Anchor）] が有効になっているものとは異なる名前を使用し、そのポリシープロファイルをポリシータグ内の SSID にマッピングして、ローカル AP に割り当てます。

パッシブ クライアント

パッシブクライアントとは、認証の完了後に DHCP パケットも ARP パケットも送信しないクライアントです。言い換えると、話しかけられないかぎり対話しない（まさに受動な）クライアントです。典型的な使用例は、静的 IP アドレスが設定され、アイドル状態になっているプリンタです。

このタイプのクライアントを稼働状態にして、トラフィックを受信し、その後に送信できるようにするには、次のように Catalyst 9800 を設定する必要があります：ポリシープロファイルで、パッシブクライアント機能を有効にします。これは、基本的に、クライアントが RUN 状態に移行することを妨げる IP 学習タイムアウトを無効にするように WLC に指示します。

```
wireless profile policy <policy-name>
  passive-client
```

トラフィックが中央スイッチング（ローカルモードまたは FlexConnect 中央スイッチング展開）される場合は、クライアント VLAN で ARP ブロードキャストも有効にする必要があります。

```
vlan configuration <vlan-id>
  arp broadcast
```

トラフィックが FlexConnect モードの AP でローカルスイッチングされる場合は、ARP トラフィックがパッシブクライアントに到達できるように、Flex プロファイルで ARP プロキシを無効にする必要があります。

```
Wireless profile flex <flex-policy-name>
  no arp-caching
```

Flex 展開において Flex サイト（サイトタグ）間で IP アドレスを重複させる必要もある場合は、次の設定ガイドで説明されているように、Flex プロファイルで追加のコマンドが必要になります：
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m-sniffer-cg.html#d5718e15126a1635

```
wireless profile flex <flex-profile-name>
  ip overlap
```

サードパーティ製 WGB

サードパーティ製ワークグループブリッジ（WGB）は、有線クライアントをその背後に接続し、それらをワイヤレスネットワークにブリッジングできるネットワークデバイスです。Cisco WGB とは異なり、サードパーティ製 WGB は、クライアントの MAC/IP アドレスの WLC への登録を実行しません。これは、異なる IP アドレスを持つ複数の有線デバイスが、WGB 自体と同じ MAC アドレスで登録されることを意味します。通常、これは ARP/DHCP ドロップと見なされ、クライアントは接続を許可されません。C9800 でサードパーティ製 WGB およびその背後にある有線デバイスをサポートするには、ポリシープロファイル設定で次のコマンドを追加する必要があります。

```
wireless profile policy <policy-name>
  no ip mac-binding
```

注： このコマンドにより、コントローラでの IP デバイストラッキングが無効になります。このコマンドは、17.7.1 以降のすべてのモード（ローカル、FlexConnect、ファブリック）でサポートされています。IP MAC バインディングを無効にすると、ARP プロキシ、Web 認証、NAC、および DHCP プロファイリングが影響を受け、それらが機能しなくなります。

古いバージョンの場合は、どうでしょうか。17.3.x トレインの 17.3.4 以降のバージョンを実行している場合は、サードパーティ製 WGB をサポートするために、代わりにポリシープロファイルで `passive-client` コマンドを設定する必要があります。これは、`no ip mac-binding` コマンドが 17.3.x トレインでサポートされていないためです。17.4.1、17.5.1、または 17.6.x トレインを実行している場合、ローカル/中央モードでサードパーティ製 WGB をサポートするには、ポリシープロファイルで `no ip mac-binding` と `passive-client` の両方を追加する必要があります。

上記の設定により、クライアント デバイス トラッキング機能が無効になり、WGB の背後にある IP アドレスの異なる複数のクライアントが同じ MAC アドレスを使用して接続できるようになります。クライアントトラフィックが WLC を通過する場合（つまり、ローカルモードまたは FlexConnect 中央スイッチング展開の場合）には、クライアント VLAN で ARP ブロードキャストも有効にする必要があります。これは、次のコマンドを使用して実行します。

```
C9800(config)#vlan configuration <vlan ID>
C9800(config-vlan-config)#arp broadcast
```

セキュリティ設定

以下のセクションでは、セキュリティに関するベストプラクティスについて説明します。

WPA3

Wi-Fi 6E および Wi-Fi 7 の導入により、新しい周波数帯および Wi-Fi 7 の機能を活用するために WPA3 が必須になりました。

Wi-Fi 7 は Wi-Fi 6E よりも制限が厳しく、WPA3 を必須とするだけでなく、許可される認証キー管理（AKM）や暗号も制限されています。Wi-Fi 7 の要件の一部を次に示します。

- すべての周波数帯で WPA3 が必須です。
- ビーコン保護が必須です。
- 暗号として GCMP-256 が必須です。
- 保護された管理フレームが必須です。

次の表に、サポートされている組み合わせの一部と、それらの Wi-Fi 6E および Wi-Fi 7 との互換性の概要を示します。

各 WPA タイプでは、1 つの組み合わせが「互換性重視」でハイライトされています。これは、ほとんどのお客様による使用が想定される設定ですが、シナリオごとに専用の分析が必要です。

この件について詳しく説明している専用の展開ガイドもあります：
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html。

表で使用されている略語：

- **AKM**：認証キー管理
- **SAE**：Simultaneous Authentication of Equals
- **PMF**：保護された管理フレーム
- **H2E**：Hash to Element

- **HPN**： Hunting and Pecking

エンタープライズ

表 5. エンタープライズ WPA3 の組み合わせと互換性

WPA のタイプ*	AKM	高速移行	PMF	AES-128	GCMP-256***	互換性	注意
WPA3 Enterp.	802.1X-SHA256	すべて	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	将来的に GCMP-256
WPA3 Enterp.	FT + 802.1X**	有効	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	将来的に GCMP-256
WPA3 Enterp.	802.1X-SHA256 FT + 802.1X**	有効	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	将来的に GCMP-256
WPA3 Enterp.	SUITEB192-1X	無効	✓	×	✓	Wi-Fi 6E Wi-Fi 7	
WPA2 Enterp. WPA3 Enterp.	802.1X 802.1X-SHA256	すべて	オプション	✓	✓	Wi-Fi 6E^ Wi-Fi 7^	将来的に GCMP-256 2.4/5 GHz のレガシークライアントを許可 ^^ 6GHz では PMF が必須としてブロードキャストされる 🏆 互換性重視
WPA2 Enterp.	802.1X	適応型 無効	×	✓	×	レガシー （6E および 7 なし）	802.11be なし、6GHz なし

* ビーコン保護を有効にします。
** 名前に明示されていなくても、依然として SHA256 を使用します。
*** GCMP256 は C9105、C9115、C9120 ではサポートされていません。

パーソナル

表 6. パーソナル WPA3 の組み合わせと互換性

WPA のタイプ*	AKM	高速移行	PMF	AES-128	GCMP-256***	互換性	注意
WPA3 Pers.	SAE-EXT-KEY	無効	✓	✓	✓	レガシーなし Wi-Fi 7	17.15 で AES-128 を許可 17.18 では GCMP-256 が必須

WPA のタイプ*	AKM	高速移行	PMF	AES-128	GCMP-256***	互換性	注意
WPA3 Pers.	SAE-EXT-KEY FT + SAE-EXT-KEY	有効	✓	✓	✓	レガシーなし Wi-Fi 7	17.15 で AES-128 を許可 17.18 では GCMP-256 が必須
WPA3 Pers.	SAE SAE-EXT-KEY	無効	✓	✓	✓	Wi-Fi 6 Wi-Fi 6E Wi-Fi 7	SAE「移行」、「移行」に H2E/HPN が必要な場合がある SAE-EXT-KEY のないクライアントをサポート
WPA2 Pers. WPA3 Pers.	PSK SAE SAE-EXT-KEY	無効	任意	✓	✓	レガシー Wi-Fi 6E Wi-Fi 7	移行に H2E/HPN が必要な場合がある 17.15 で AES-128 を許可 17.18 では GCMP-256 が必須 互換性重視
WPA2 Pers. WPA3 Pers.	PSK SAE SAE-EXT-KEY FT-SAE-EXT-KEY FT-SAE	有効	オプション	✓	✓	レガシー Wi-Fi 6E Wi-Fi 7	FT をサポート 移行に H2E/HPN が必要な場合がある 17.15 で AES-128 を許可 17.18 では GCMP-256 が必須 互換性重視
WPA2 Pers. WPA3 Pers.	PSK SAE	無効	✓	✓	✗	レガシー Wi-Fi 6E Wi-Fi 7 なし	802.11be なし、ただし 6GHz をサポート
WPA2 Pers.	PSK	無効	✗	✓	✗	レガシー （6E および 7 なし）	802.11be なし、6GHz なし

* ビーコン保護を有効にします。

** Wi-Fi 6E および 7 には SAE Hash to Element（H2E）が必要です。

*** GCMP256 は C9105、C9115、C9120 ではサポートされていません。

拡張オープン（ゲスト）

表 7. 拡張オープンの組み合わせと互換性

WPA のタイプ*	AKM	高速移行	PMF	AES-128	GCMP-256***	互換性	注意
拡張オープン	OWE	無効	✓	✓	✓	Wi-Fi 6E Wi-Fi 7	17.15 で AES-128 を許可

WPA のタイプ*	AKM	高速移行	PMF	AES-128	GCMP-256***	互換性	注意
							17.18 では GCMP-256 が必須
拡張オープン	OWE	無効	✓	✓	×	Wi-Fi 6E Wi-Fi 7 なし	802.11be なし、ただし 6GHz をサポート
拡張オープン	OWE	無効	該当なし	✓	×	レガシー Wi-Fi 6E なし Wi-Fi 7 なし	802.11be なし、6GHz はサポートされない 2 つの SSID が必要**

* GCMP256 は C9105、C9115、C9120 ではサポートされていません。

** 次を参照してください：https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217737-configure-enhanced-open-ssid-with-transi.html

トラストポイントの取り扱い

トラストポイントとは信頼できる認証局（CA）のことであり、暗黙的に信頼される認証局であるため、「トラストポイント」と呼ばれています。Public Key Infrastructure（PKI）は、C9800 で証明書管理を提供します。特定の自己署名証明書（SSC）を信頼すると、PKI システムは、その信頼できる証明書で署名されている他のすべての証明書を自動的に信頼します。これは、Datagram Transport Layer Security（DTLS）、HTTPS、セキュアシェル（SSH）、セキュアソケットレイヤ（SSL）などのさまざまな機能およびプロトコルに対して証明書管理を提供するために使用されます。C9800 では、トラストポイントは次の複数の機能で使用されます。

- AP 参加（DTLS トンネル）
- HTTPS 接続（GUI）
- Web 認証リダイレクト
- モビリティトンネル

これらについて個別に説明します。AP 参加用のトラストポイントは、WLC と AP 間の接続を保護します。これは、CLI で次のコマンドを使用して表示できます。

```
C9800#show wireless management trustpoint
```

すべての物理アプライアンスは、デフォルトで、製造元でインストールされる証明書（MIC）を使用します。すべての仮想アプライアンスは、自己署名証明書（SSC）を使用します。

物理アプライアンス

```
LabW-9800M1#show wireless management trustpoint
Trustpoint Name  : CISCO_IDEVID_CMCA3_SUDI
Certificate Info : Available
Certificate Type : MIC
Certificate Hash : d34d9a6a71e799077b36242081ca0e3bc49a92fe
Private key Info : Available
FIPS suitability : Not Applicable
```

仮想アプライアンス

```
LabW-9800CL1#show wireless management trustpoint
Trustpoint Name  : LabW-9800CL1_WLC_TP
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : dcf8998004c500a1d3e0655b8f6af135e4b430b1
Private key Info : Available
FIPS suitability : Not Applicable
```

AP 参加に問題があるときは、多くの場合、それがトラブルシューティングを開始する出発点となり、次の手順に実行することをお勧めします。

- 次のコマンドを発行して、トラストポイントが設定されているかどうかを確認します。

  `show wireless management trustpoint`

- トラストポイント設定がないときは、多くの場合、それが原因の一つです。設定するには、次の手順を実行します。
  - 物理アプライアンスでは、次のコマンドを使用して CAPWAP 証明書チェーンを単純に再割り当てします。

    `C9800(config)#default wireless management trustpoint`

  - 仮想アプライアンスでは、EXEC モードで内部スクリプトを使用してワイヤレストラストポイントを生成できます。

    `C9800#wireless config vwlc-ssc key-size 2048 signature-algo sha256 password 0 <password>`

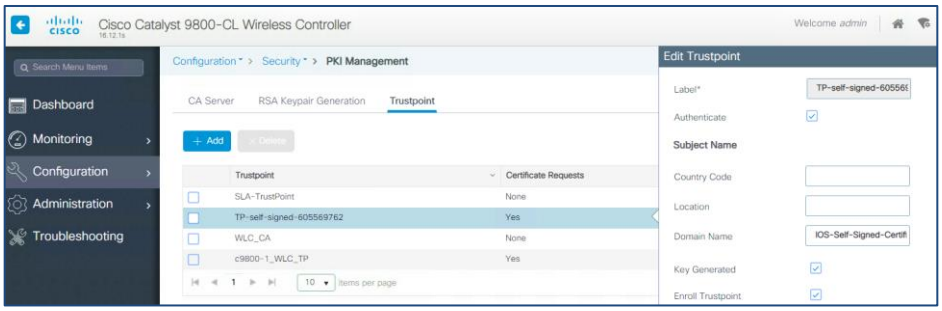
注： このコマンドは、exec プロンプトで（コンフィギュレーション モードではなく）実行する必要があります。

  - 次のコマンドを使用してワイヤレス設定を検証します。

    `C9800#wireless config validate`

HTTPS GUI アクセスに使用されるトラストポイントを静的に割り当てることをお勧めします。

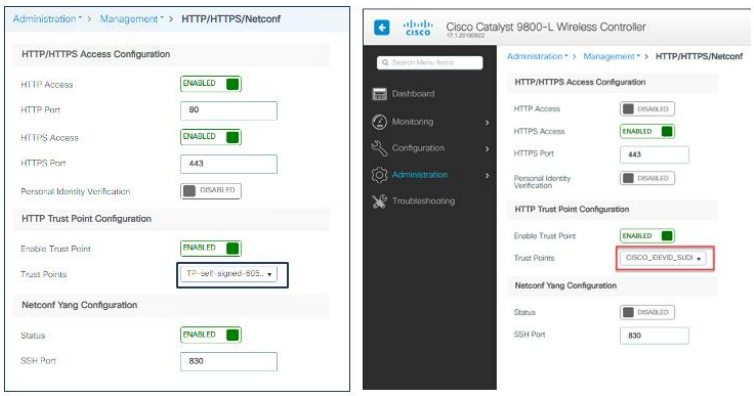
1. 9800-CL の場合は、`show crypto pki trustpoint` コマンドまたは GUI を使用して IOS 自己署名証明書を特定します。



この証明書が存在しない場合や、破損している場合などは、設定コマンドの `no ip http secure-server` を実行し、続けて `ip http secure-server` を実行して HTTPS プロセスを再起動することで、証明書を再生成できます。

2. 証明書を HTTPS に割り当てます（次の図は VM とアプライアンスの両方）。

C9800-CL　　物理アプライアンス



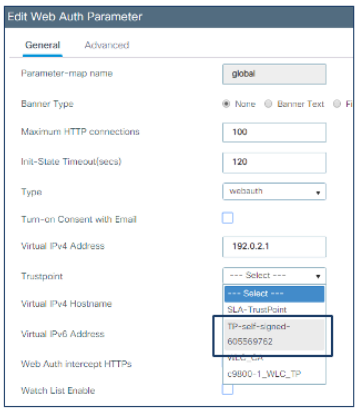
また、対応する CLI コマンドは次のとおりです。

```
C9800(config)#ip http secure-trustpoint <name>
```

3. 正しく割り当てられていることを確認します（次の例は 9800-CL の場合）。

```
C9800#sh ip http server secure status
HTTP secure server status: Enabled
[snip]
HTTP secure server trustpoint: TP-self-signed-605569762
```

Web 認証の場合は、HTTPS リダイレクト用のトラストポイントが必要です。この場合も、ベストプラクティスはプロセスに静的に割り当てることです。これは、グローバルパラメータマップで実行できます（次の図は 9800-CL の場合）。



注： SUDI 証明書は Web 認証/HTTP に使用しないでください。また、その証明書が Catalyst Center によってプッシュされる可能性があることに注意してください。

CLI では同じ設定を次のように行います。

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 virtual-ip ipv6 FD00::0:2:1
 trustpoint TP-self-signed605569762
```

モビリティトンネルでは CAPWAP が使用され、デフォルトでは DTLS を使用してコントロールプレーンのメッセージが暗号化されます。WLC ではワイヤレス管理トラストポイント（AP トラストポイント）を使用してこのトンネルが確立されるため、特別な操作は必要ありません。

トラストポイントと Cisco Catalyst Center

Catalyst Center は、Catalyst Center 独自の自己署名証明書を管理対象デバイスにプッシュします。デフォルトの証明書は「sdn-network-infra-iwan」です。Catalyst 9800 のボックスで複数の証明書（自己生成のトラストポイントや Catalyst Center によってプッシュされた証明書など）が設定されている場合は、デバイスへの HTTPS アクセスに使用する証明書を指定することを強くお勧めします。これを行わないと、Catalyst 9800 が誤った証明書を選択し、グラフィカル インターフェイスにアクセスできなくなる可能性があります。前の段落で説明したように、これを実行するには次の CLI コマンドを使用します。

```
C9800(config)#ip http secure-trustpoint <truspoint-name>
```

または、GUI で [管理（Administration）] > [管理（Management）] > [HTTP/HTTPS/Netconf] ページに移動し、[HTTP トラストポイント設定（HTTP Trust Point Configuration）] セクションで特定の証明書を選択します。

ローカル管理パスワードポリシー

強力なパスワードを適用する必要があります。パスワードポリシーを使用すると、コントローラおよびアクセスポイントの管理ユーザーを強化するために、新しく作成されるパスワードに対して、強力なパスワードチェックを適用することができます。新規パスワードには次の要件が適用されます。

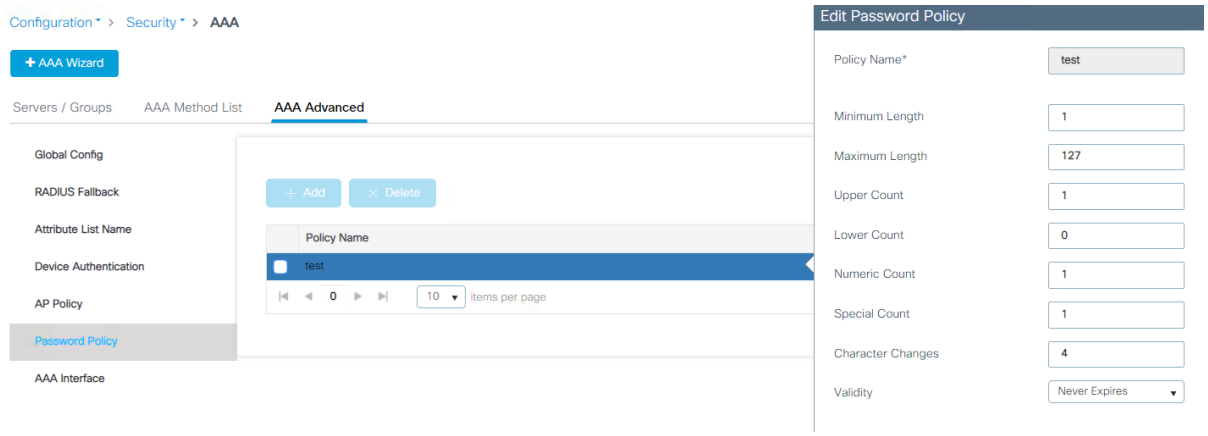
- コントローラが旧バージョンからアップグレードされた場合、古いパスワードはすべて、それらが弱いものであっても維持されます。システムをアップグレードすると、強力なパスワードチェックが有効になっている場合、その時点からそれが適用されます。以前に追加されたパスワードの強度はチェックされず、変更もされません。
- [パスワードポリシー（Password Policy）] ページで設定された内容によっては、ローカル管理ユーザーおよびアクセスポイントユーザーの設定が影響を受けます。

C9800 ワイヤレスコントローラでは、コモンクライテリアに準拠したパスワードの強度と管理機能が、ユーザーパスワードを指定するルールの保存、検索、提供のためのパスワードポリシーおよびセキュリティメカニズムを指定するために使用されます。

ローカル ユーザについては、ユーザのプロファイルとパスワード情報が重要なパラメータとともにシスコ デバイスに保存され、このプロファイルを使用して、ユーザのローカル認証が行われます。このユーザーになり得るのは、管理者（ターミナルアクセス）またはネットワークユーザー（たとえば、ネットワークアクセスのために認証された PPP（Point-to-Point Protocol）ユーザー）です。

リモートユーザーについては、ユーザープロファイル情報がリモートサーバーに保存されている場合、管理アクセスとネットワークアクセスの双方にサードパーティの AAA サーバーを使用して AAA サービスが提供される可能性があります。

パスワードポリシーを設定するには、[設定（Configuration）] > [セキュリティ（Security）] > [AAA] に移動し、パスワードのポリシーを定義します。



ユーザーログインポリシー

ユーザーログインポリシーを使用すると、同じユーザーログイン情報を使用する異なるデバイスによる同時ログインの数を制限できます。セキュリティ上の理由でこの制御を行う場合は、デフォルトの 0（無制限ログイン）より大きい値を設定する必要があります。ただし、これは、同じユーザー名とパスワードを共有している可能性のあるネットワークデバイス（ワイヤレス接続に同じユーザープロファイルを使用するワイヤレス電話など）に影響を与える可能性があることに注意してください。

次のコマンドを入力して、ユーザー ログイン ポリシーを設定します。

```
C9800(config)# wireless client max-user-login ?
<0-8> Maximum number of login sessions for a single user, 0-8 (0=Unlimited)
```

ユーザーログインポリシーを確認するには、次のコマンドを入力します。

```
C9800# show run | I max-user-login
```

パスワード暗号化

Cisco IOS XE では、機器で使用されるすべてのパスワードを暗号化できます。これには、ユーザーパスワードだけでなく、たとえば SSID パスワードも含まれます。暗号化を使用するには、まず暗号化キーを定義します。

```
C9800(config)#key config-key password-encrypt <key>
```

その後、次のコマンドを使用します。

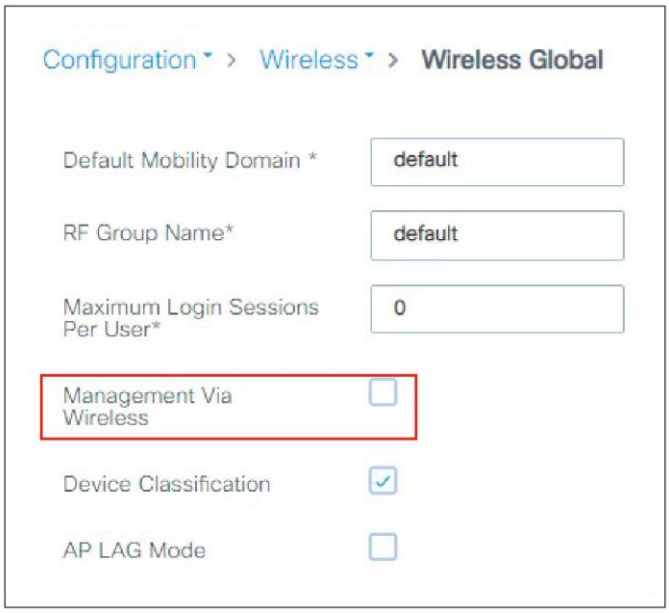
```
C9800(config)#password encryption aes
```

これはパスワード情報を保護するために推奨されます。

注： C9800 では、パスワードが暗号化されると、セキュリティ上のベストプラクティスとして、それらを復号するメカニズムが存在しません。唯一の回復方法は、パスワードを再設定することです。

ワイヤレス経由での管理の無効化

ワイヤレス経由で管理する機能により、オペレータは、ワイヤレス コントローラ ネットワークに接続されたワイヤレスクライアントを使用して WLC をモニターおよび設定することができます。ワイヤレス経由の管理は、デフォルトでは無効になっています。セキュリティが懸念される場合は無効のままにしておく必要があります。GUI で設定を確認するには、[設定（Configuration）] > [ワイヤレス（Wireless）] > [ワイヤレスグローバル（Wireless Global）] に移動します。



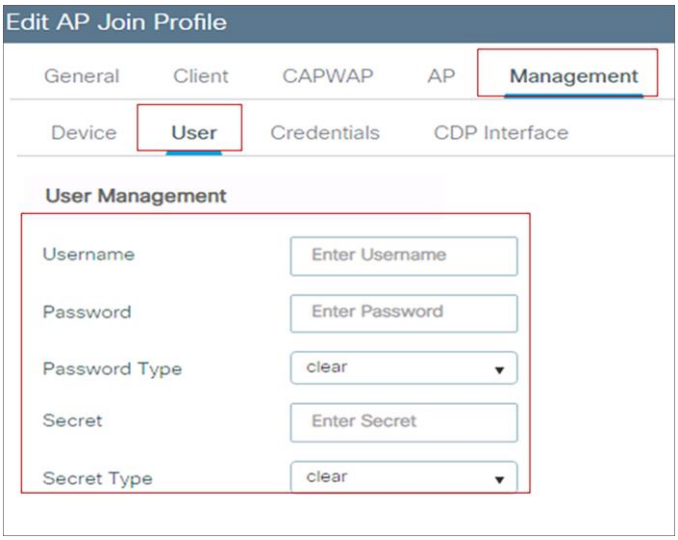
CLI では、次のように入力します。

```
C9800(config)#no wireless mgmt-via-wireless
```

AP コンソールのデフォルトのユーザー名とパスワード

シスコ セキュア開発ライフサイクル（SDL）は、シスコ製品の復元力と信頼性を高めるために設計された、反復可能かつ測定可能なプロセスです。SDL において、シスコ製品セキュリティベースライン（PSB）により、デフォルトのユーザー名とパスワード（Cisco/Cisco）を使用したアクセスポイントへのコンソールアクセスを無効にすることが義務付けられました。リリース 16.12.2s 以降、ユーザーは、アクセスポイントのログイン情報を設定してからでないと、コンソール、Telnet、または SSH の使用が許可されません。これは、セキュリティ上の理由により適用されるベストプラクティスです。

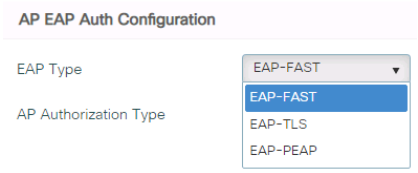
カスタムログイン情報を定義するには、AP 参加プロファイルに移動します。



デフォルトの参加プロファイルでユーザー名とパスワードを変更すると、それらがすべての AP に自動的に割り当てられます。その後、カスタム参加プロファイルを使用して、AP グループごとに異なるログイン情報を設定することもできます。

AP ポートの 802.1X 認証

セキュリティを向上させるために、AP と Cisco スイッチの間で 802.1X 認証を設定してください。AP は、802.1X サプリカントとして機能し、EAP-FAST、EAP-PEAP、または EAP-TLS（拡張可能認証プロトコル（EAP）の Flexible Authentication via Secure Tunneling（FAST）、Protected EAP（PEAP）、または Transport Layer Security（TLS））を使用してスイッチによって認証されます。これは、AP 参加プロファイル設定で設定できます。



新しい設定モデルでは、この機能が非常に柔軟になりました。AP 802.1X 設定はグローバルではなくなっており、特定の AP グループ（特定の AP プロファイルおよびサイトタグに割り当てられたグループ）に対してのみ設定できます。802.1X AP 機能は、サポートされているすべての AP で利用できます。

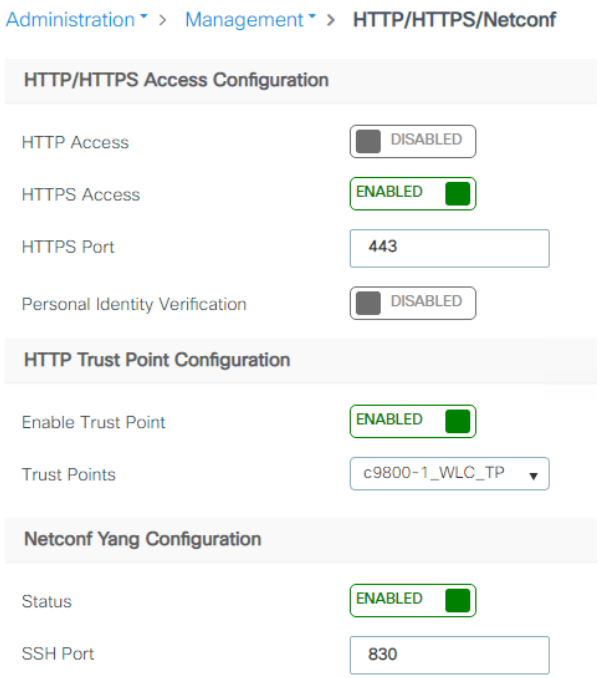
次に、スイッチポートで 802.1X 認証を有効にするための設定例を示します。

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(config)#
Switch(config)# interface gigabitethernet2/1
Switch(config-if)# switchport mode access
```

```
Switch(config-if)# dot1x pae authenticator
Switch(config-if)# dot1x port-control auto
Switch(config-if)# end
```

セキュア Web アクセスの有効化

セキュリティを強化するために、管理アクセスに対して HTTPS が有効で、HTTP が無効であることを確認します（これらがデフォルト設定）。



システムがセキュア Web サーバープロセスを有効にすると、起動時に HTTPS 用の SSC トラストポイントが自動的に作成されますが、HTTPS 用にとして明示的に割り当てられるわけではありません。GUI を使用して（上の図を参照）、または CLI で次のコマンドを使用して、明示的に割り当てることをお勧めします。

```
C9800(config)#ip http secure-trustpoint <trustpointname>
```

割り当てると、設定に表示されます。

```
C9800#sh ip http server status
[snip]
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite:  aes-128-cbc-sha dhe-aes-128-cbc-sha
        ecdhe-rsa-aes-128-cbc-sha rsa-aes-cbc-sha2 rsa-aes-gcm-sha2
        dhe-aes-cbc-sha2 dhe-aes-gcm-sha2 ecdhe-rsa-aes-cbc-sha2
        ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2
```

```
HTTP secure server TLS version:  TLSv1.2 TLSv1.1
[snip]
HTTP secure server trustpoint: c9800-1_WLC_TP
HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL
```

CLI を使用して、独自の TLS バージョンを定義することもできます。

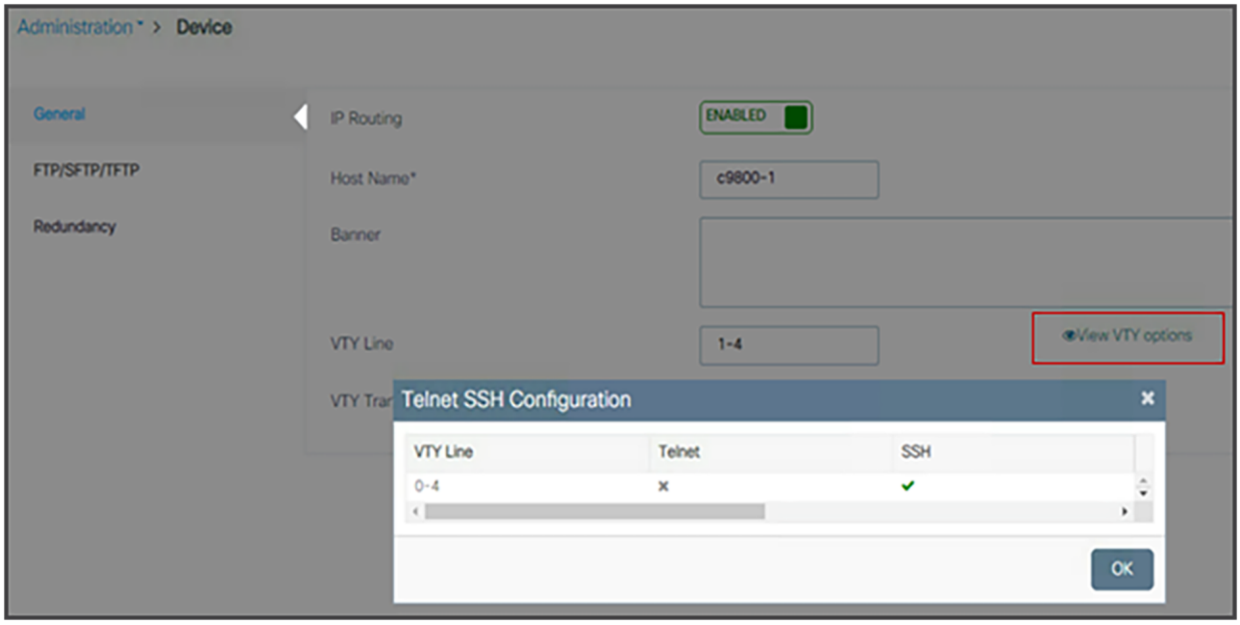
```
C9800(config)#ip http  tls-version ?
  TLSv1.0  Set TLSv1.0 version Only
  TLSv1.1  Set TLSv1.1 version Only
  TLSv1.2  Set TLSv1.2 version Only
```

また、暗号スイートも定義できます。

```
C9800(config)#ip http secure-ciphersuite ?
  3des-ede-cbc-sha            Encryption type tls_rsa_with_3des_ede_cbc_sha ciphersuite
  aes-128-cbc-sha             Encryption type tls_rsa_with_aes_cbc_128_sha ciphersuite
  aes-256-cbc-sha             Encryption type tls_rsa_with_aes_cbc_256_sha ciphersuite
  dhe-aes-128-cbc-sha         Encryption type tls_dhe_rsa_with_aes_128_cbc_sha ciphersuite
  dhe-aes-cbc-sha2            Encryption type tls_dhe_rsa_with_aes_cbc_sha2(TLS1.2 & above)
ciphersuite
  dhe-aes-gcm-sha2            Encryption type tls_dhe_rsa_with_aes_gcm_sha2(TLS1.2 & above)
ciphersuite
  ecdhe-ecdsa-aes-gcm-sha2    Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 & above)
ciphersuite
  ecdhe-rsa-3des-ede-cbc-sha  Encryption type tls_ecdhe_rsa_3des_ede_cbc_sha ciphersuite
  ecdhe-rsa-aes-128-cbc-sha   Encryption type tls_ecdhe_rsa_with_aes_128_cbc_sha ciphersuite
  ecdhe-rsa-aes-cbc-sha2      Encryption type tls_ecdhe_rsa_aes_cbc_sha2(TLS1.2 & above)
ciphersuite
  ecdhe-rsa-aes-gcm-sha2      Encryption type tls_ecdhe_rsa_aes_gcm_sha2(TLS1.2 & above)
ciphersuite
  rsa-aes-cbc-sha2            Encryption type tls_rsa_with_aes_cbc_sha2(TLS1.2 & above)
ciphersuite
  rsa-aes-gcm-sha2            Encryption type tls_rsa_with_aes_gcm_sha2(TLS1.2 & above)
ciphersuite
```

セキュア SSH/Telnet

セキュア Web アクセスと同様に、セキュリティを強化するために、コントローラに対して SSH が有効で、Telnet が無効であることを確認します。[管理（Administration）] > [デバイス（Device）] に移動して [VTY オプションの表示（View VTY Options）] をクリックすることで確認できます。



他の Cisco IOS XE ボックスの場合と同様の設定で、Telnet と SSH を有効または無効にします。これは、GUI で簡単に実行できます。

関連資料：

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_config_secure_shell_ewlc.html

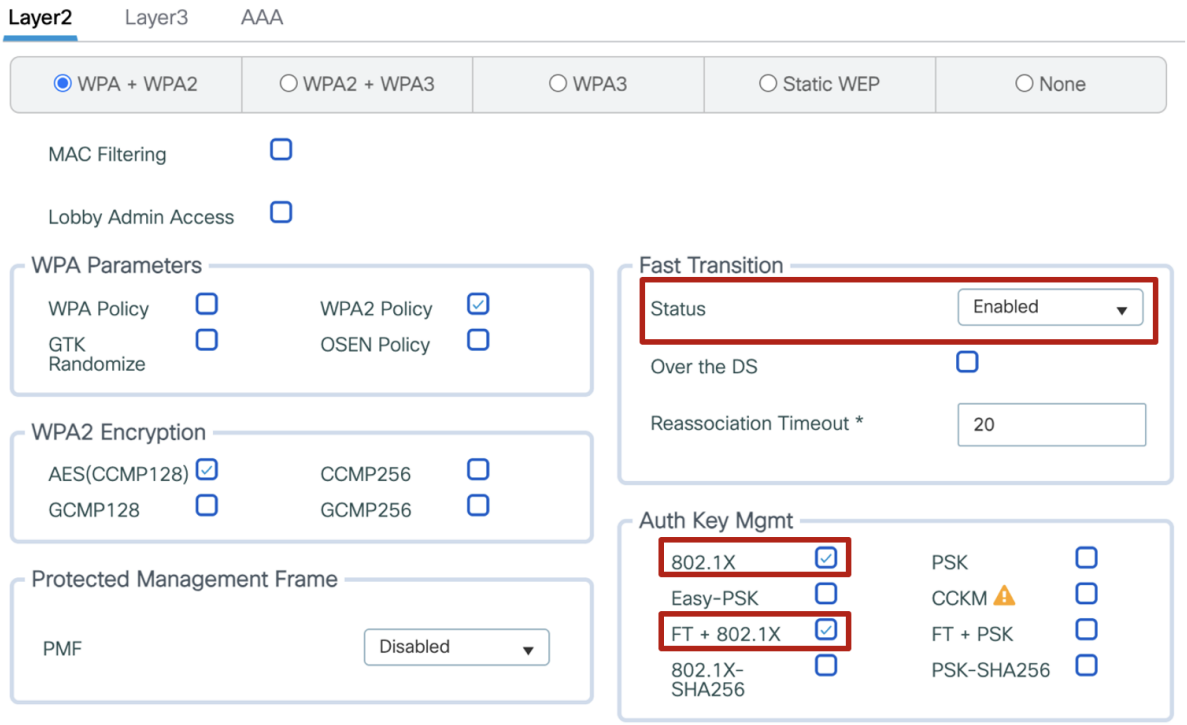
802.11r 高速移行の有効化

802.11r は高速ローミングのための IEEE 標準規格であり、この規格では、クライアントがターゲット AP（つまり、クライアントが接続を試みる次の AP）に関連付けられる前であっても、ターゲット AP との最初の認証ハンドシェイクが実行されます。この手法は、高速移行（FT）と呼ばれます。

11r をサポートしていないデバイスは、「FT のみ」が設定されている SSID に参加できないことに注意してください。

適応型 802.11r の導入前は、異なるタイプのデバイスが混在するワイヤレスネットワークで 802.11r を活用するために、FT が有効な WLAN と FT が無効な WLAN を別々に作成して、非 11r デバイスがネットワークに参加できるようにする必要がありました。これはあまり実用的ではありませんでした。そこで、シスコは、Apple 社や Samsung 社などのデバイスエコシステムパートナーと協力して、FT 対応デバイスと非 FT 対応デバイスを同じ SSID で混在させることができる設定できる適応型 FT をサポートしました。C9800 では、適応型 FT がデフォルトで有効になっています。これは、ネットワークに Apple デバイスや Samsung デバイスがある場合に役立ちます。

実際には、ネットワークでは通常さまざまなタイプおよび機能のクライアントが混在しており、一部の非 FT 対応クライアントでは、適応型 FT が有効になっている WLAN に接続する際に問題が発生することがあります。シスコでは、802.11r クライアントと非 802.11r クライアントの互換性を確保するために、単一の WLAN を 802.11r 混合モードで設定することをお勧めします。これには、高速移行を有効に設定し、FT と非 FT の両方の認証キー管理（AKM）モードを選択します。これは、クライアントがその機能に応じて「802.11r あり」または「802.11r なし」の AKM を選択できるため、「802.11r 混合モード」と呼ばれます。次に、WPA/WPA2 セキュリティと 802.1x AKM の設定例を示します。



クライアントの相互運用性を最適化するために、「DS 経由」（Over the DS）設定は無効のままにすることをお勧めします。

802.11r を使用することは、ローミングの高速化以外でも重要です。クライアントは、AP を切り替えるたびに完全な認証を受けずにセキュアなローミングを実行できるため、認証サービスの合計使用量を減らすことができます。つまり、ローミング速度が向上することと AAA サーバーで全体的な認証負荷が軽減することの両方の利点が得られます。

注： WPA3 と組み合わせた高速移行の詳細については、「WPA3」のセクションを参照してください。

[DHCP 必須（DHCP Required）] オプション

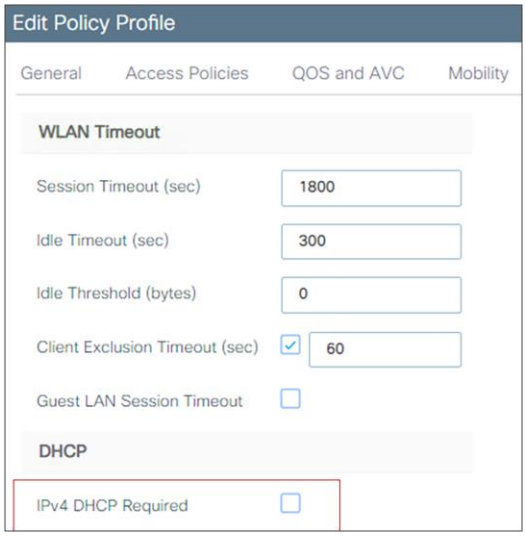
セキュリティを強化するために、シスコでは、すべてのクライアントが DHCP サーバーから IP アドレスを取得するように設定することをお勧めします。ポリシープロファイル設定の [DHCP 必須（DHCP Required）] オプションを使用すると、クライアントが WLAN に関連付けられるたびに、ネットワークでの他のトラフィックの送受信が許可

される前に、DHCP アドレスの要求または更新を強制することができます。セキュリティの観点からは、これにより、使用中の IP アドレスをより厳格に制御できるようになります。

ただし、この設定は慎重に分析する必要があります。それは、この設定により、ローミング中にトラフィック通信が再度許可されるまでの合計時間に影響を与える可能性があるからです。さらに、リース期間が終了するまで DHCP アドレスを更新しない一部のクライアント実装にも影響を与える可能性があります。これは、クライアントのタイプによって異なります。たとえば、Cisco 8821 IP 電話の場合、コントローラは DHCP フェーズが完了するまで音声またはシグナリングトラフィックを通過させないため、このオプションを有効にすると、ローミング中に音声の問題が発生する可能性があります。別の例として、Android および一部の Linux ディストリビューションがあります。それらでは、DHCP アドレスがリース期間の半分が経過した時点でのみ更新され、ローミング時には更新されません。これは、クライアントエントリの期限が切れた場合に問題になる可能性があります。一部のサードパーティ製プリンタサーバーも影響を受ける可能性があります。

一般的に、WLAN に Windows 以外のクライアントがある場合は、このオプションを使用しないことをお勧めします。これは、DHCP クライアント側の実装方法によっては、より厳格な制御によって接続の問題が発生する可能性があるためです。

このオプションはポリシープロファイルにあるため、やはり、同じ SSID/WLAN をブロードキャストする場合でも特定の AP グループにこの設定を使用できるという柔軟性があります。



注： 音声サービスまたはビデオサービスをサポートする WLAN の場合や、ワイヤレスデバイスがローミング時に DHCP 更新を控えめに行う場合は、[DHCP 必須（DHCP Required）] を決して有効にしないでください。

WebAuth

最大許容 HTTP 接続数を制限すると、さまざまなシナリオで Web 認証が失敗する可能性があるため、次のコマンドは使用しないことをお勧めします。

```
ip http max-connections
```

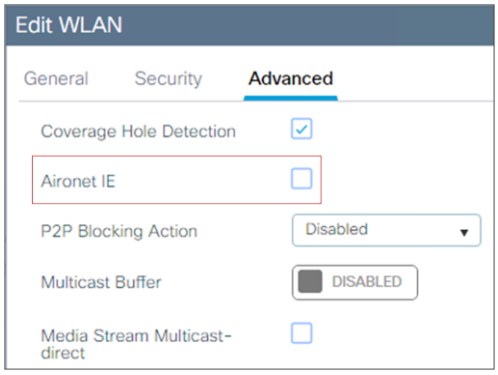
Aironet IE

Aironet IE とは、接続性の向上とトラブルシューティングのためにシスコのデバイスで使用されるシスコ独自の属性です。この属性には、AP によって送信される WLAN のビーコンやプローブ応答にある、アクセスポイント名、負荷、関連付けられたクライアントの数などの情報が含まれています。これは、一部のサイトサーベイツールでネット

ワークから詳細情報を取得するために使用され、また Cisco Client Extensions クライアントで関連付けに使用する最適な AP を選択するために使用されます。

この設定は、これを活用できる Cisco 音声デバイス（8821 または 7925 IP 電話など）や Cisco ワークグループ ブリッジ デバイスを使用する場合にのみ推奨されます。たとえば、Cisco Centralized Key Management では、Aironet IE を有効にする必要があります。

また、サーベイツールで追加情報をキャプチャできるため、サイトサーベイを実行する場合にも役立ちます。ただし、この設定は Cisco 以外のクライアントで問題を引き起こす可能性があるため、最初はご自身の環境内でテストし、使用しているクライアントデバイスに基づいて決定することをお勧めします。デフォルトでは、これはオフになっています。



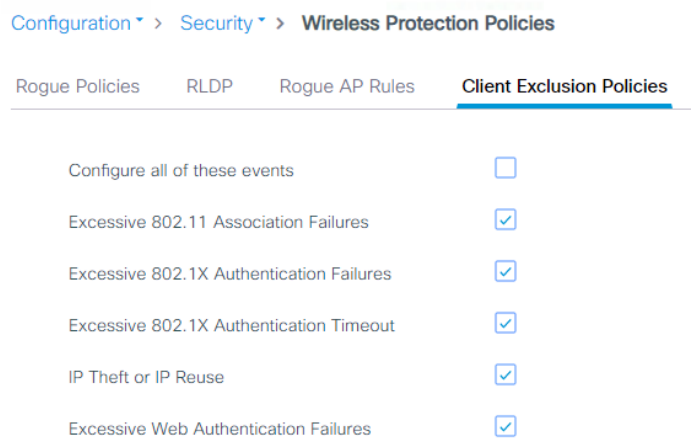

```
Device# conf t
Device(config)# wlan <profile-name> <wlan-id> <ssid>
Device(config-wlan)# no ccx aironet-iesupport
```

クライアント除外

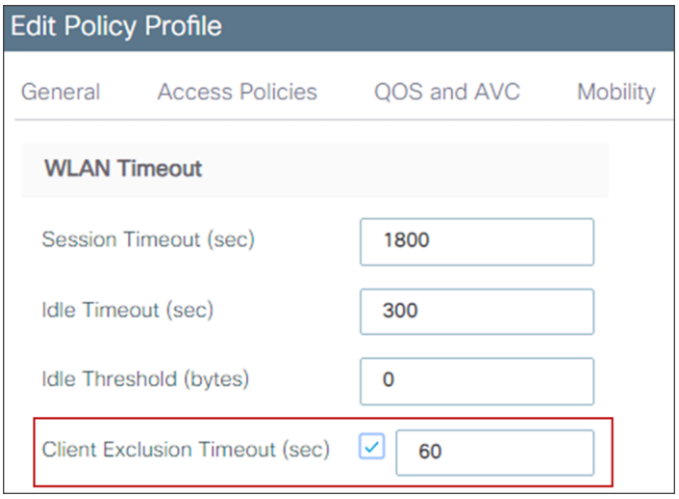
ユーザーが認証に失敗した場合、コントローラは、そのクライアントを除外することができます。そのクライアントは、除外タイマーが期限切れになるか、または管理者によって除外タイマーが手動でオーバーライドされるまで、そのネットワークに接続できません。この機能により、クライアントセキュリティの意図的な、または不注意による設定ミスによって引き起こされる、高負荷による認証サーバーの問題を防ぐことができます。非常にまれな場合や特殊な場合を除き、すべての WLAN で常にクライアント除外を設定しておくことを強くお勧めします。クライアント除外は AAA サーバーの保護メカニズムとして機能し、誤って設定されたクライアントによって引き起こされる可能性のある認証要求の大量発生を防止します。クライアント除外では、単一のデバイスによる認証試行が検出されます。そのデバイスが最大失敗回数を超えると、その MAC アドレスの関連付けはそれ以上許可されなくなります。C9800 ワイヤレスコントローラは、次のいずれかの条件が満たされた場合にクライアントを除外します。

- 802.11 関連付けに 5 回連続して失敗した
- 802.1X 認証に 3 回連続して失敗した
- IP 盗用または IP 再使用が発生した（クライアントが取得した IP アドレスが他のデバイスにすでに割り当てられている）
- Web 認証に 3 回連続して失敗した

これらは、グローバル保護ポリシーレベルで設定できます。



クライアントを除外しておく期間を設定できます。また、ポリシープロファイルレベルで除外を有効または無効にすることができます。

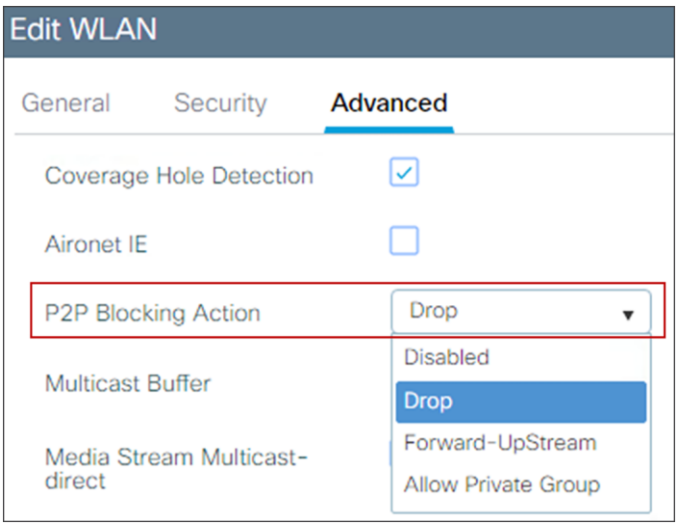


ピアツーピア ブロック

ピアツーピア（P2P）ブロッキングは WLAN ごとの設定であり、各クライアントは、関連付けられている WLAN の P2P ブロッキング設定を継承します。これにより、トラフィックをリダイレクトする方法をより細かく制御できるようになります。たとえば、トラフィックを、コントローラ内でローカルにブリッジしたり、コントローラによってドロップしたり、クライアント VLAN の上流に位置するスイッチに転送したりすることを選択できます。

この設定により、クライアントが同じ WLAN に接続されている別のクライアントに攻撃することを阻止できますが、重要な点として、ドロップオプションを使用すると、チャットや音声サービスといったクライアント間で直接通信できるあらゆるアプリケーションが妨げられることに注意してください。ゲスト SSID で P2P ブロッキングを使用することは、クライアントがインターネットとだけ通信できればよいため、理にかなっています。

この設定は、WLAN プロファイルで有効にされています。



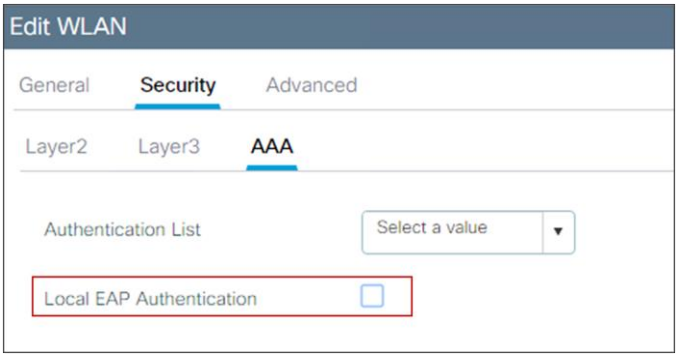
音声またはビデオサービスをサポートする WLAN や、クライアント間での直接通信が必要なシナリオでは、この機能を無効にしてください。

注： ローカルスイッチングを使用する FlexConnect モードの場合は、トラフィックがコントローラを通過しないため、P2P ブロッキングは同じ AP に接続されたクライアントからのトラフィックにのみ適用されます。AP 間のトラフィックには適用されません。同様に、SD-Access モードでは、クライアントトラフィックが、ポリシーを適用するために常にファブリックエッジスイッチに送信されるため、この設定は実際には影響しません。P2P ブロッキングでは、モビリティグループ内の別の WLC からのトラフィックもブロックされません。

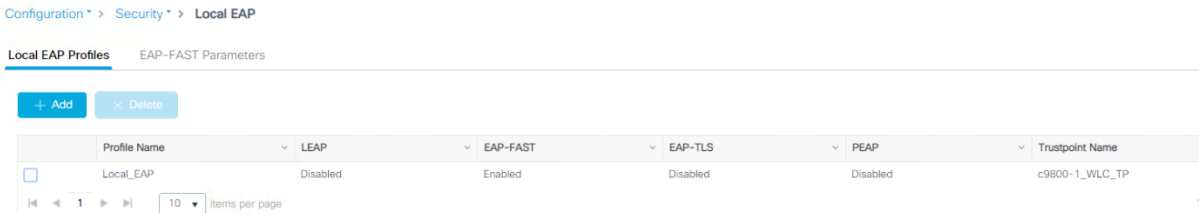
ローカル EAP

ローカル EAP は、RADIUS サーバーを使用する代わりに、ユーザーおよびワイヤレスクライアントをコントローラでローカルに認証することを可能にする認証方式です。拡張性の理由から、企業の実稼働環境でローカル EAP を使用することは推奨されません。

WLAN がローカル EAP を使用するように設定されているかどうかを確認するには、AAA 設定を調べます。



有効にする場合はチェックボックスをクリックしますが、まず、どの EAP プロトコルを使用するのかを決める ローカル EAP プロファイルを作成する必要があります。次の例では、EAP-FAST 用に設定されています。



ワイヤレス管理 VLAN の WLAN へのマッピング（ポリシープロファイル経由）

クライアントが WLC のワイヤレス管理 VLAN に割り当てられる可能性のあるエラーを回避するために、どのポリシープロファイルもワイヤレス管理 VLAN を使用するように設定しないことをお勧めします。これにより、関連する SSID で管理サブネットにトラフィックが転送されることがなくなります。

フォーリンコントローラがすべてのトラフィックをアンカーに転送する自動アンカー型 WLAN のシナリオでは、フォーリンコントローラのポリシープロファイルを「ダミー」 VLAN に設定することが引き続き推奨されます。これにより、アンカーコントローラに到達しないトラフィックがブラックホール処理されます。このことは、ワイヤレス管理インターフェイスをレイヤ 3 ポートとして定義している場合、つまり、次のような設定を使用している場合にも重要です。

```
interface GigabitEthernet2
description L3 WMI
no switchport
ip address <ip_address> <mask>
end

wireless management interface GigabitEthernet2
```

パブリッククラウドで C9800-CL を使用している場合を除き、L3 ポートでの WMI は推奨されません。ただし、WMI を L3 ポートとして使用しており、C9800 がフォーリン WLC として機能している場合は、ポリシープロファイルの VLAN を VLAN 1 以外に設定してください。

また、C9800 では、中央スイッチング WLAN の場合、ポリシープロファイルの WLAN に VLAN をマッピングするときには、VLAN 1 およびデフォルト VLAN に対して特別な処理が行われていることに注意してください。

- vlan-name = default を指定すると、クライアントは VLAN 1 に割り当てられます。
- vlan-id が明示的に 1 に設定されていると、クライアントはワイヤレス管理 VLAN に割り当てられます。

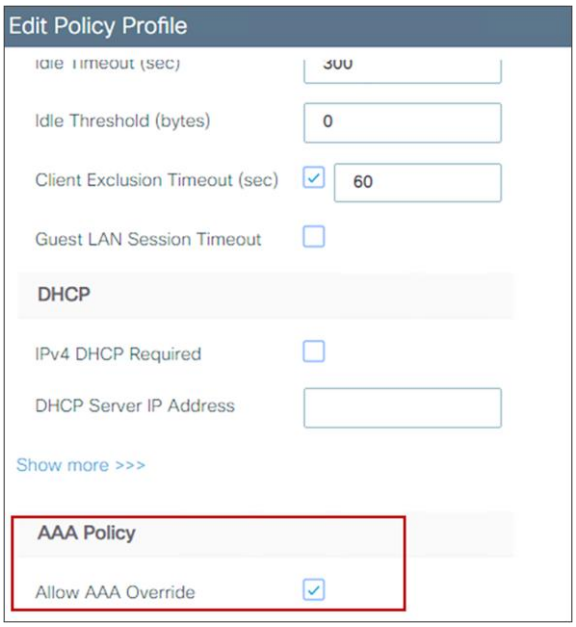
このことを通知する警告が表示されます。

AAA Override

ワイヤレスクライアントが、セキュリティ上の理由で異なるグループに分割され、たとえば、異なる VLAN、異なる拡張可能グループタグ（SGT）、またはその他のセキュリティポリシーを取得する必要がある、アイデンティティベースのネットワークサービスを設計する場合は、AAA オーバーライド機能を使用して WLAN を統合します。

この機能により、1 つの共通 SSID を使用しながら、ユーザーごとの設定または属性を割り当てることができます。可能なセキュリティの向上に加えて、AAA オーバーライドは、異なる WLAN/SSID を 1 つに統合することもできます。これにより、全体的な RF 利用効率が大幅に改善されます（ビーコンが減り、プローブアクティビティも少なくなります）。

C9800 では、AAA オーバーライド設定はポリシープロファイルの [詳細（Advanced）] タブで定義されます。これにより、必要に応じて、ある場所（AP グループ = ポリシータグ）では AAA オーバーライドを使用し、別の場所は使用しない設定を同じ 802.1X SSID に対して行うことができます。ただし、通常は、AAA 設定がすべての AP で共通になります。



また、AAA オーバーライドを機能させるには、サーバーから RADIUS を介して受信した設定を承認するように Catalyst 9800 を設定する必要があることに注意してください。設定内に、承認リストとサーバーグループ名を指している「`aaa authorization network`」行があることを確認してください。

AAA VLAN およびファブリック VNID オーバーライド

VLAN オーバーライドは、ワイヤレスで一般的に使用される、よく知られた機能です。これにより、1 つの共通 SSID を使用し、ユーザーが属するグループに基づいて異なる VLAN/サブネットを返すことにより、基本的なユーザー グループ セグメンテーション ポリシーを適用できます。

SD-Access では、セグメンテーションは階層型であり、VRF レベル（マクロセグメンテーション）と SGT レベル（マイクロセグメンテーション）で行うことができます。レイヤ 2 ボックスである WLC（AireOS または Cisco IOS XE ベース）は、VRF を理解せず、代わりにレイヤ 2 の仮想ネットワーク識別子（VNID）の概念を使用します。そのため、SD-Access ワイヤレスでの AAA オーバーライドでは、ユーザーグループに基づいて異なるレイヤ 2 VNID を返すことができ、その VNID はスイッチで VLAN インターフェイス（SVI）にマッピングされ、結果としてサブネットや VRF にマッピングされます。

C9800 を使用した AAA オーバーライドについて把握しておく必要がある重要な事項は、次のとおりです。

- 非ファブリック展開の場合、VLAN AAA オーバーライドは、Tunnel-Private-Group-ID または Airespace-Interface-Name を使用して実装できます。C9800 は両方の属性を同時に取得でき、適切な属性を使用し、もう一方の属性を破棄するため、どちらでも機能します。
- ファブリック展開の場合、現時点では、C9800 は、レイヤ 2 VNID 情報を受け渡すために Airespace-Interface-Name のみをサポートしています。

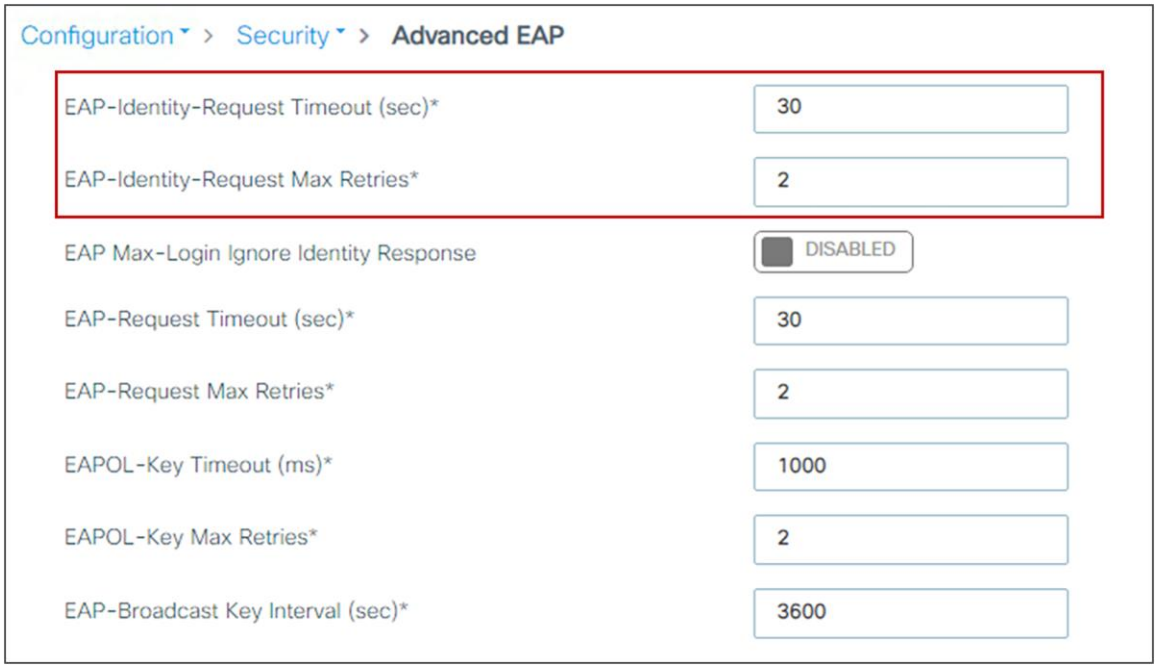
注： AireOS は、ファブリック展開および非ファブリック展開において Airespace-Interface-Name でのみ動作します。

EAP アイデンティティ要求タイムアウトおよび最大再試行回数

EAP アイデンティティ要求のデフォルトのタイムアウトおよび最大再試行回数は、ほとんどのユースケースに対応できるように設定されています。一部のクライアント認証シナリオでは、これらのパラメータを増やす必要がある場合があります。たとえば、スマートカードでワンタイムパスワードを実装する場合や、一般的に最初のアイデンティティ要求に応答するためにユーザーの操作が必要になる場合は、それらを増やす必要がある可能性があります。ま

た、障害時の回復時間を短くすることにより、クライアントエクスペリエンスを向上させるために、これらのパラメータを減らす必要がある場合もあります。

デフォルトの EAP アイデンティティ タイムアウトを確認し、必要に応じて値を変更するには、[設定（Configuration）] > [セキュリティ（Security）] > [高度な EAP（Advanced EAP）] に移動します。



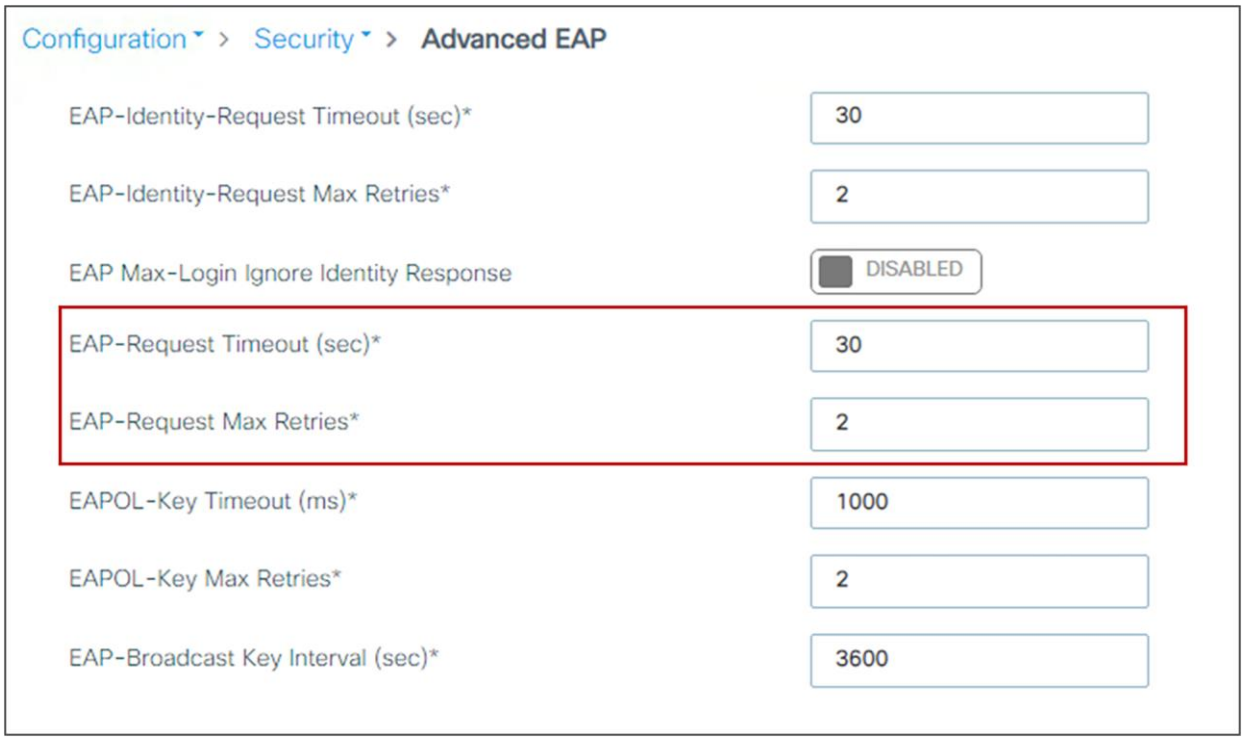
CLI では、次のコマンドを使用します。

```
C9800(config)#wireless security dot1x identity-request ?
  retries  Maximum number of EAP ID request retries
  timeout  no description
```

EAP 要求タイムアウトおよび最大再試行回数

802.1X 認証フェーズ中に、パケット損失やクライアントからの応答の欠如によって EAP 再試行が発生した場合、WLC は EAP 要求を再試行することがあります。一部のクライアントは高速の再試行タイマーを適切に処理できない場合があるため、クライアントのタイプに応じてこの設定の調整が必要になることがあります。これは、RF 環境の状態が悪い場合に迅速に回復するために重要です。

一般的な推奨値を示すことは困難ですが、ほとんどの場合、許容値は 2 秒前後であり、低速なクライアント（電話）の場合は最大 30 秒であるため、通常、このタイムアウトは最悪のシナリオを考慮して 30 秒に設定されます。デフォルトのタイムアウトを表示し、必要に応じて変更するには、次の図を参照してください。



CLI では、次のコマンドを使用します。

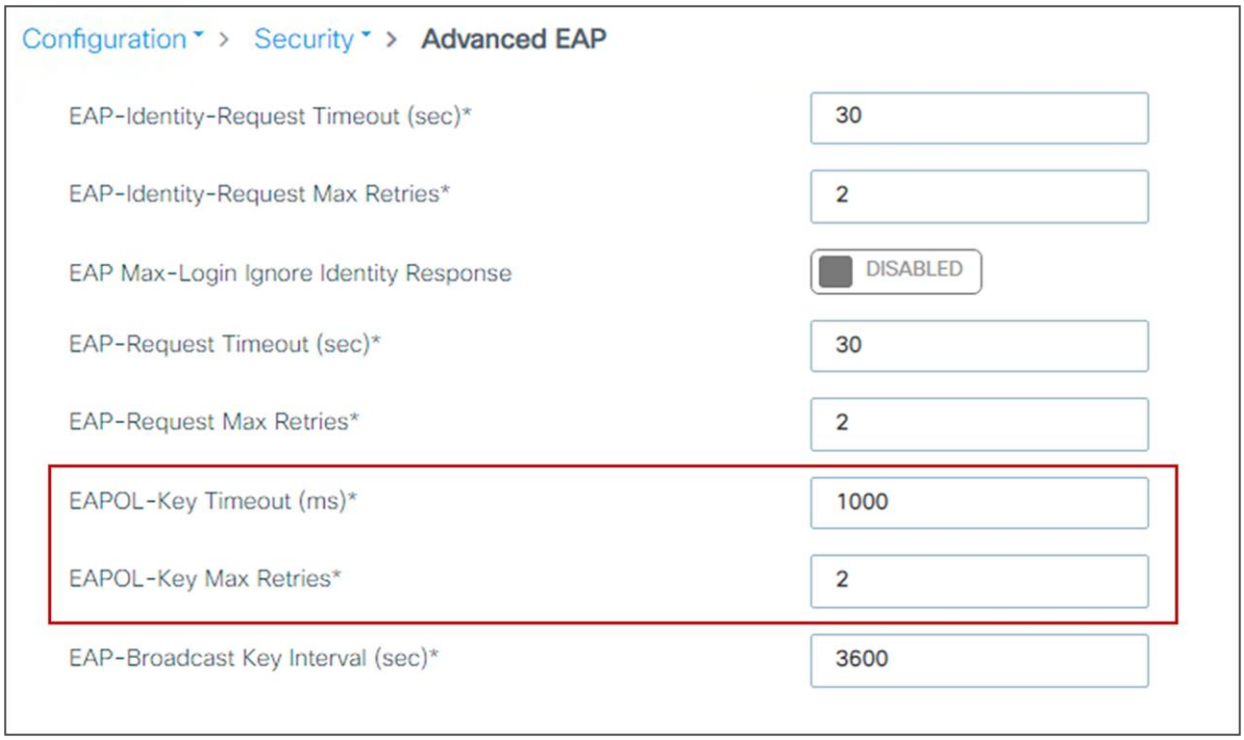
```
C9800(config)#wireless security dot1x request ?
  retries  Maximum number of EAP ID request retries
  timeout  no description
```

EAPoL キータイムアウトおよび最大再試行回数

7925 または 8821 IP 電話などの音声クライアントでは、EAP over LAN（EAPoL）タイムアウトをできるだけ短くする必要があります。通常、ほとんどのシナリオでは、400 ～ 1000 ミリ秒の範囲であれば正常に機能します。

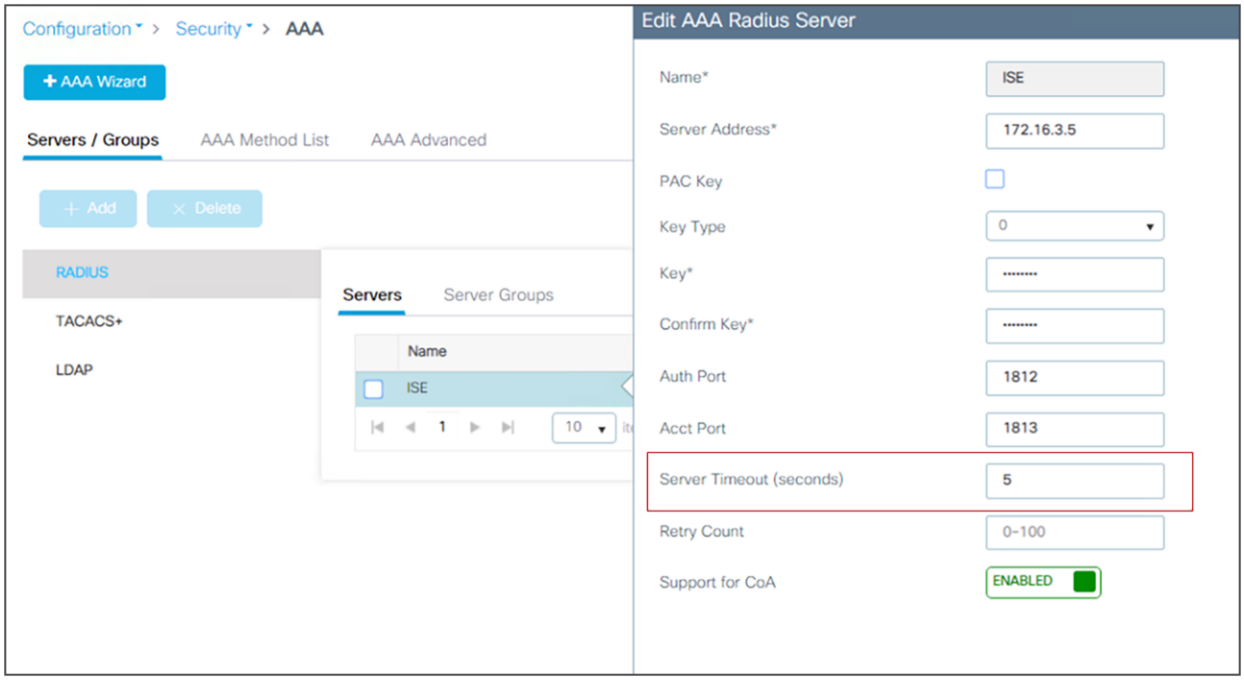
最大再試行カウンタは、2017 年に報告された、WPA および WPA2 を使用するワイヤレスクライアントに対するいくつかの KRACK 攻撃に直接影響します。このカウンタをゼロに設定すると、この脆弱性に対するパッチがまだ適用されていないクライアントに対するほとんどの攻撃を防ぐことができます。ただし、この設定は、RF の状態が悪いシナリオにおいて、またはパケット損失が発生する可能性のある WAN ネットワーク経由で実行される認証に影響を及ぼします。これは、ゼロを使用すると、元のパケットが失われた場合に認証プロセスが失敗する可能性があるためです。

デフォルト値を表示し、EAPoL パラメータを変更するには、次の GUI 設定を使用します。



RADIUS サーバーのタイムアウト

高い負荷がかかっているときにクライアント認証プロセスが早期に期限切れになることを防ぐために、RADIUS 認証およびアカウンティングサーバーで、サーバータイムアウトの最小値を 5 秒に設定する必要があります。次の設定を入力して、RADIUS 認証およびアカウンティングサーバーのタイムアウトを設定してください。



Catalyst 9800 では、特に複数の AAA サーバーを使用しており、負荷分散を適用している場合、dead-criteria（ダウン基準）および deadtime（ダウン時間）タイマーを設定することが重要です。これらのコマンドを使用すると、Catalyst 9800 は、応答のないサーバーを「dead」（ダウン）とマークし、バックアップサーバーに切り替えます。これらのタイマーを設定するには、次の CLI コマンドを使用します。

```
radius-server dead-criteria time 5 tries 3
radius-server deadtime 5
```

「deadtime」は、dead-criteria によって dead とマークされた後にそのサーバーが dead ステータスのままである時間を指定します。deadtime が経過した後に AAA サーバーが実際に「alive」（稼働中）であることを確認し、まだ到達不能な AAA サーバーへの要求の送信を回避するために、サーバー定義でアクティブプローブを設定できます。

```
C9800(config)#radius server <name>
C9800(config-radius-server)#automate-tester username <username> probe-on
```

このコマンドのユーザー名はダミーにできます。AAA サーバーのデータベースに存在している必要はありません。サーバーが到達可能であれば、バックエンドのデータベース（Active Directory など）またはその他のサービスが動作していない場合でも、WLC はサーバーを稼働していると見なすことに注意してください。

RADIUS ネットワークデバイス設定

HA SSO を使用している場合、コントローラの RADIUS サーバーにエントリを作成するときは、次の 3 つの IP アドレスを設定する必要があります。

- ワイヤレス管理インターフェイス（WMI）
- アクティブコントローラの冗長化管理インターフェイス（RMI）
- スタンバイコントローラの冗長化管理インターフェイス（RMI）

スタンバイコントローラは、常にその RMI IP を使用して SSH セッションを認証します。アクティブコントローラは、RMI と WMI の両方を使用して AAA サーバーにアクセスします。

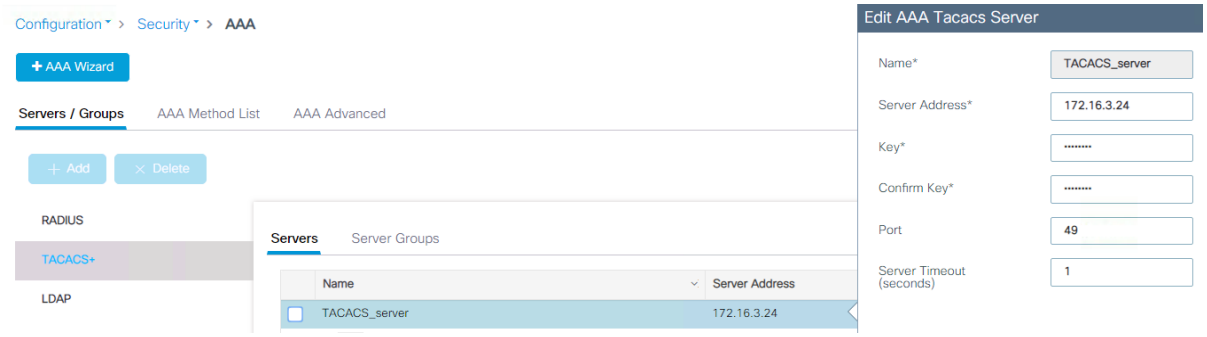
RADIUS 中間アカウンティング

RADIUS 中間アカウンティングは、アカウンティング更新を含むアカウンティング要求パケットを、ネットワークアクセス サーバー（NAS）から RADIUS サーバーに送信します。RADIUS アカウンティング要求は、VLAN ID、認証方式などのデータを送信し、NAC を最新の状態に保ちます。

大規模なシナリオでは、NAC のサーバー負荷を軽減するために、RADIUS 中間アカウンティングを無効にすることが望ましい場合があります。詳細については、設定ガイド（https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_interim-accounting.html）を参照してください。

TACACS+ 管理タイムアウト

再認証試行が繰り返される場合や、プライマリサーバーがアクティブで到達可能であるにもかかわらずコントローラがバックアップサーバーにフォールバックする場合は、TACACS+ AAA サーバーの再送信タイムアウト値を長くすることがベストプラクティスになります。これは、ワンタイムパスワードを実装している場合に特に当てはまります。サーバータイムアウトは TACACS+ サーバーエントリの作成時に設定でき、通常、1 秒の値が推奨されます。

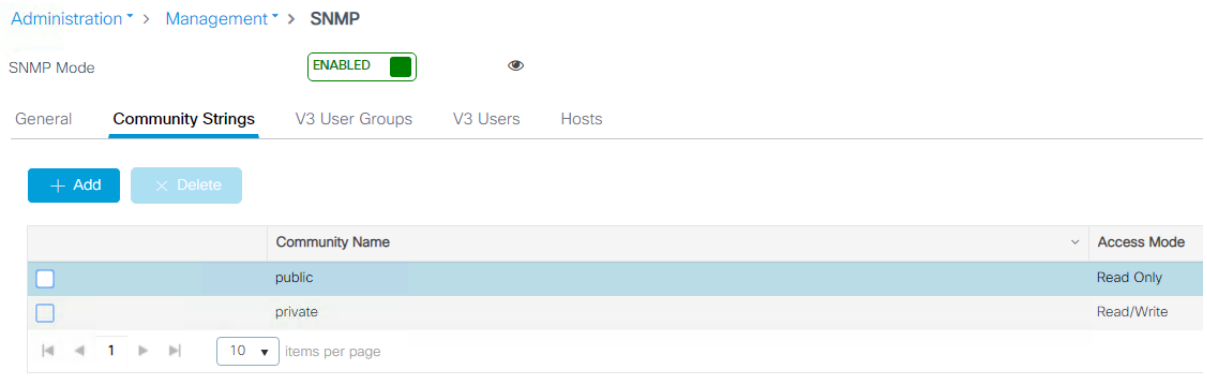


SNMP コミュニティ

注： SNMP コミュニティは将来的に廃止される予定であるため、ユーザー名/パスワードを使用した SNMPv3 が今後の推奨方法となります。

SNMP コミュニティを調べて、デフォルトや非常によく知られたもの（「private」、「public」など）を使用していないことを確認してください。それらは、ほとんどの展開でセキュリティリスクをもたらす可能性があります。

それらのデフォルトが設定されている場合は、削除し、新しいものを再作成することをお勧めします。

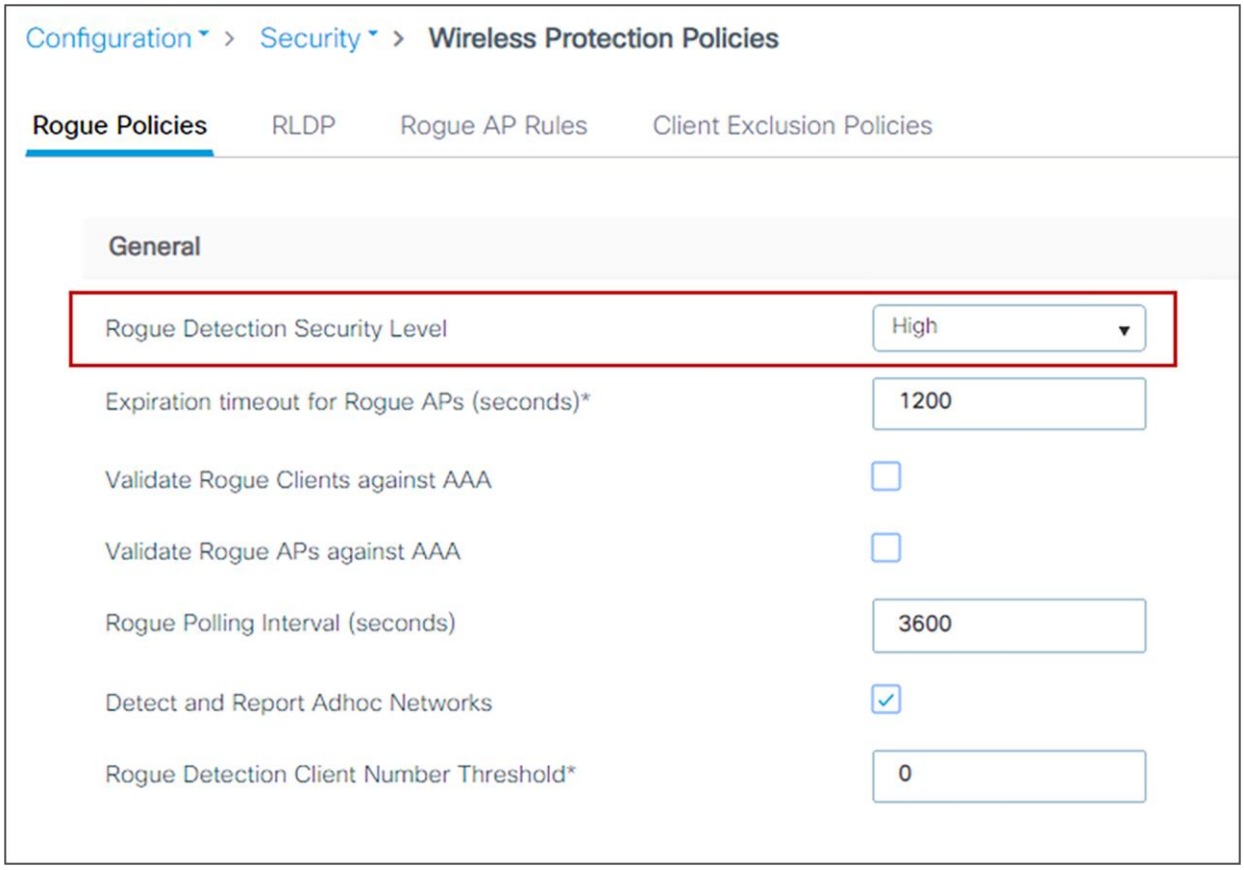


不正の管理と検知

不正なワイヤレスデバイスは、企業のワイヤレスネットワークにとって常に脅威となっています。ネットワークの所有者は、不明なデバイスをスキャンするだけでなく、それ以上のことを実施する必要があります。ネットワークの所有者は、不正 AP や侵入者の脅威の検出、無効化、位置の特定、および管理をリアルタイムで自動的に実行できる必要があります。不正 AP は、正規のクライアントをハイジャックし、プレーン テキスト攻撃、DoS 攻撃、または中間者攻撃を使用することによって、無線 LAN の運用を妨害します。つまり、ハッカーは不正 AP を使用して、パスワードやユーザー名などの機密情報を取得できます。これに成功すると、ハッカーは一連の Clear To Send（CTS）フレームを送信できるようになります。このフレームでは AP を模倣して、特定のワイヤレス LAN クライアントアダプタに送信を通知し、他のすべてのアダプタには待機を通知します。その結果、正規のクライアントは、無線 LAN リソースに接続できなくなります。このため、ワイヤレス LAN のサービスプロバイダーは、その無線空間で不正 AP を禁止する方法を探し求めています。ベストプラクティスは、企業環境などで、不正 AP 検知を使用してセキュリティリスクを最小限に抑えることです。しかしながら、OfficeExtend アクセスポイント（OEAP）展開、市全域、屋外など、不正 AP 検知が不要な特定のシナリオがあります。屋外のメッシュ AP を使用して不正 AP を検出しても、分析を実行するリソースが増えるばかりでメリットはほとんどありません。さらに、不正 AP の自動封じ込めを評価する（または完全に止める）ことがきわめて重要です。これは、不正 AP の自動封じ込めを動作させておくと法的な問題や責任が生じる可能性があるためです。以下のセクションに示されているいくつかのベストプラクティスにより、不正 AP のリストを維持する際の効率が向上し、リストが管理しやすいものになります。

不正ポリシー

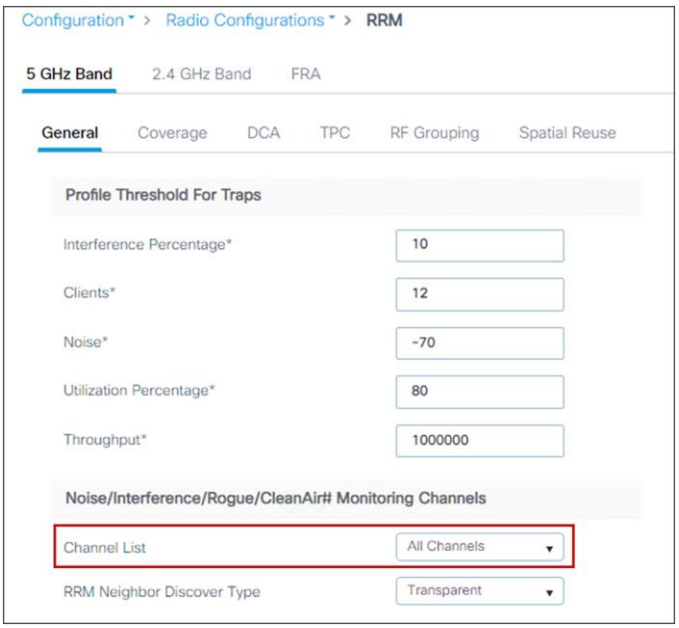
少なくとも、セキュリティレベルを [高（High）] に設定する必要があります。GUI で、次のように操作します。



不正モニタリングチャネル

「すべてのチャネルをモニター」するように設定して、不正検知を強化します。コントローラは、RRM メトリック（ノイズ、干渉）と不正検知モニタリングのために、単一のチャネルスキャンリストを維持します。このリストは、動的チャネル割り当て（DCA）チャネル（AP に自動的に割り当てられるチャネル）または国別のチャネル（設定済みの国でのみ有効）に焦点を当てるか、可能なすべてのチャネルをスキャンするように設定できます。後者は、一般的でないチャネルを使用するあらゆる不正の適切な検知を確実に行うための最適なオプションとなります。欠点は、チャネルリストが長いと、設定されたチャネルスキャン間隔内で AP がより頻繁にオフチャネルになる必要があることです。これらのトレードオフを考慮して、以下にいくつかの推奨事項を示します。

- セキュリティを強化するには、すべてのチャネルをスキャンすることを選択します。
- パフォーマンスを向上させるには、DCA チャネルを選択します。これにより、システムがスキャンするチャネルの数が最も少なくなります。
- パフォーマンスとセキュリティのバランスをとるには、国別のチャネルのオプションを選択します。

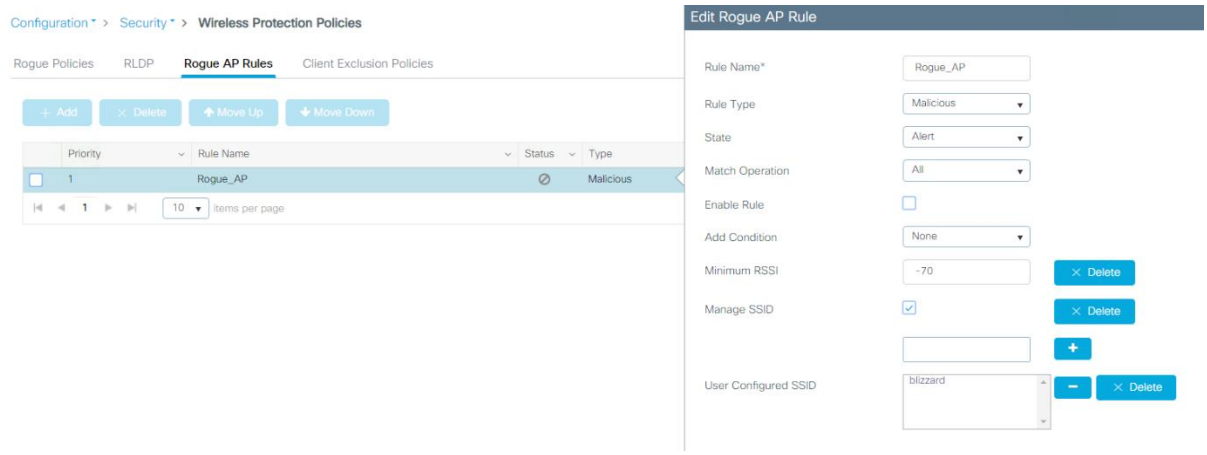


適切な悪意のある不正 AP ルールの定義

即時の対応や緩和策を必要とする「メジャー」および「クリティカル」不正 AP アラームに優先的に処理するために、悪意のある不正 AP ルールを定義してください。クリティカルまたはメジャー不正 AP アラームが、悪意のあるものとして分類され、ネットワークで検出されます。各不正 AP ルールは、単一または複数の条件で構成され、そのルールと照合するために、AND（すべてに一致）または OR（いずれかに一致）のロジックを設定します。推奨される悪意のある不正 AP ルールは、次のとおりです。

- 管理対象 SSID：使用しているワイヤレス インフラストラクチャと同じ管理対象 SSID を使用するすべての不正 AP は、悪意のある AP としてマークされる必要があります。管理者は、この脅威を調査して軽減する必要があります。
- 最小 RSSI が -70 dBm 超：この基準は、通常、未知の不正 AP が施設内に存在し、ワイヤレスネットワークに対する干渉の原因となる可能性があることを示しています。このルールは、独自の隔離された建物とセキュリティ保護された境界を持つ企業の展開でのみ推奨されます。このルールは、小売業の店舗や、さまざまなテナントによって共有される施設には推奨されません。このような場所では、通常、各当事者からの Wi-Fi 信号が混在しているためです。
- ユーザー設定 SSID または部分文字列 SSID：実稼働 SSID の文字の異なるバリエーションや組み合わせを使用している SSID をモニターします。

ルールに対して、[アラート（Alert）]、[封じ込め（Contain）]、または [削除（Delete）] のいずれかの状態を設定する必要があります。[アラート（Alert）] を使用することが推奨されます。次に、不正 AP ルールの設定方法を示します。



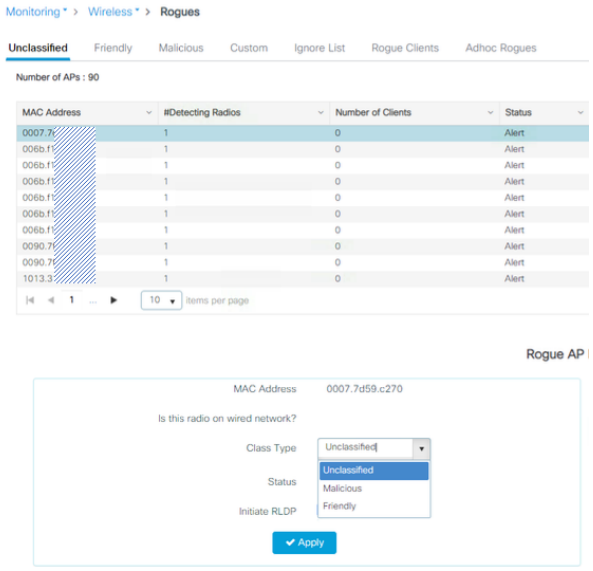
注： 不正 AP を封じ込めることには法的影響があります。さらに、専用 AP が封じ込めアクティビティに使用されていないかぎり、インフラストラクチャ AP を使用して不正 AP を封じ込めると、運用中のワイヤレスサービスに大きな悪影響を及ぼします。

危険性のない不正 AP のリストの特定と更新

定期的にリサーチと調査を行い、「未分類」の不正 AP のリストから危険性のない不正 AP を定期的に（毎週または毎月）削除します。危険性のない不正 AP の例は、次のとおりです。

- 危険性のない既知の内部不正 AP（施設内に存在する不正 APなど）や、危険性のない不正 AP のリストにインポートされている既知の AP MAC アドレス。
- 危険性のない既知の外部不正 AP（ベンダー共有の場所や近隣の小売店に見られるような不正 AP）。

[モニター（Monitor）] > [ワイヤレス（Wireless）] > [不正（Rouges）] に移動して、次の操作を実行します。



AP 不正検知設定

AP ごとに不正検知機能を設定できます。たとえば、公共エリアにある AP では、不正検知を無効することが有用である場合があります。デフォルトでは、不正検知が有効になっています。WLC で不正検知設定を確認するには、次のコマンドを使用します。

```
show ap config general
```

また、アクセスポイントでは、次のコマンドを使用します。

```
AP-D6-122#sh rrm rogue detection config
Rogue Detection Configuration for Slot 0:
Rogue Detection Mode : Enabled
Rogue Detection Report Interval : 30
Rogue Detection Minimum Rssi : -90
Rogue Detection Transient Interval : 0
```

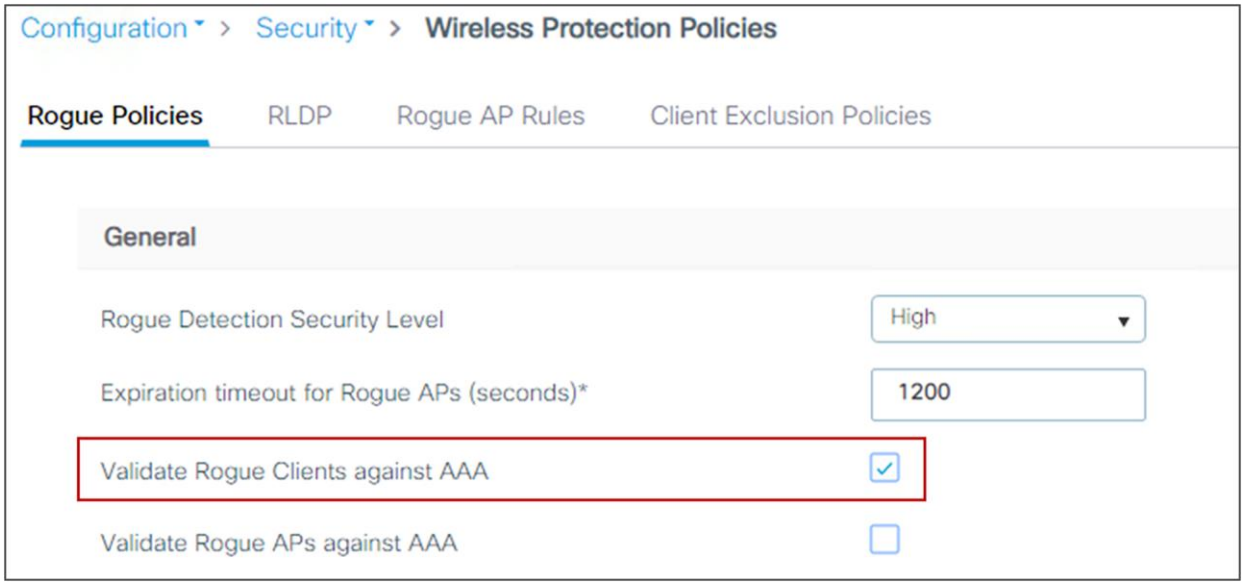
アドホック不正検知の有効化

一般的な不正検知と同様に、アドホック不正検知は、セキュリティが正当化される特定のシナリオに最適です。ただし、オープンな会場/スタジアム、市街地、および公共の屋外スペースなどのシナリオでは推奨されません。アドホック不正検知および報告を有効にするには、次のコマンドを使用します。

```
C9800(config)#wireless wps rogue adhoc
```

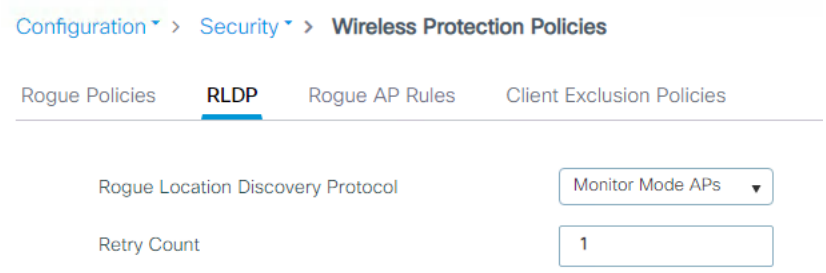
不正クライアントの AAA 検証の有効化

不正クライアントの AAA 検証を有効にする理由は、WLC が AAA サーバー上のクライアントの存在を確実かつ継続的にチェックし、正当なものまたは悪意のあるものとしてマークすることです。これを GUI で設定する方法は、次のとおりです。



Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）機能が必要な場合は、ワイヤレスネットワークのパフォーマンスおよびサービスへの影響を防ぐために、モニターモードの AP でのみ使用してください。



CLI で、次のコマンドを使用します。

```
C9800(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only
```

注： RLDP は、802.11ac Wave 1 AP でのみサポートされています。最新情報については、AP 機能マトリックスを参照してください。

不正通知およびテレメトリ

Catalyst 9800 には、デフォルトで、積極的な不正通知しきい値が設定されています。RF が頻繁に変更される特定の展開では、通知受信者（Cisco Catalyst Center など）が過剰なメッセージによって過負荷状態になる可能性があります。

不正 AP およびクライアントの RSSI 変動通知のしきい値をゼロ（デフォルト）より大きい値に変更することをお勧めします。次のコマンドを使用します。

```
C9800(config)#wireless wps rogue ap notify-rssi-deviation 5
C9800(config)#wireless wps rogue clients notify-rssi-deviation 5
```

推奨値は 5 以上です。

展開タイプ、AP モデル、および RF 環境によっては、不正の封じ込めにより、深刻なネットワークの中断が発生する可能性があります。十分に注意して使用してください。国によっては法的影響が発生する可能性があるため、地域の規制を確認してください。

高可用性

ここでは、高可用性のための推奨設定について説明します。

ステートフル スイッチオーバー（SSO）

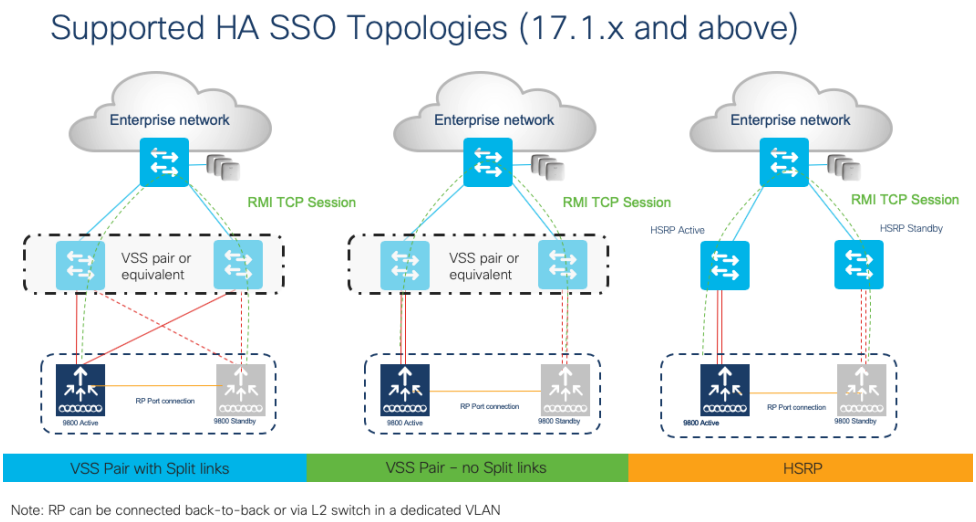
ステートフル スイッチオーバー（SSO）をともなう高可用性（HA）は、すべてのバージョンの Cisco Catalyst 9800 シリーズ ソフトウェアおよびすべてのフォームファクタ（C9800-CL を含む）でサポートされている機能です。SSO 機能を使用すると、ペアのコントローラが単一のネットワークエンティティとして機能し、アクティブ/スタンバイシナリオで動作できます。すべての設定と AP およびクライアントの状態が、アクティブとスタンバイの間で同期されます。HA SSO により、現在のアクティブコントローラで障害が発生してもワイヤレスクライアントが再接続や再認証を行う必要がない状態が確保されます。使用中のコントローラのハードウェアタイプによって許可されている場合には常に、HA SSO 機能を活用して、障害時に発生する可能性のあるダウンタイムを削減することをお勧めします。

Cisco IOS XE リリース 17.1 以降では、C9800 は、冗長化マネージャインターフェイス（RMI）の使用をサポートしています。これにより、以下の機能をサポートできます。

- ゲートウェイチェック
- デュアルアクティブ検出

このため、C9800 HA SSO の推奨リリースは 17.1 以降です。図 5 は、サポートされているトポロジを示しています。

図 5 : サポートされている HA SSO トポロジ



詳細については、『High Availability SSO Deployment Guide』（https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller_ha_sso_dg.html）を参照してください。

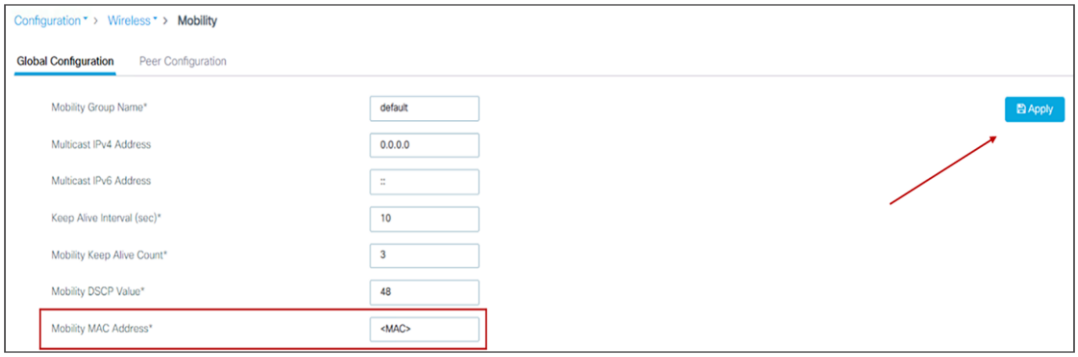
注： Cisco Embedded Wireless Controller（EWC）on Catalyst Access Points では、HA の実装が少し異なります。アクティブコントローラとスタンバイコントローラが 2 つの Cisco Catalyst 9100 アクセスポイント上で同時に動作するため、アクティブ WLC で障害が発生すると、スタンバイが、ユーザーの操作なしで自動的に引き継ぎます。スイッチオーバー時間は 10 秒未満ですが、ステートフルではないため、コントローラサービスの復旧にはこの時間がかかります。EWC は、AireOS の Mobility Express と同じように FlexConnect ローカルスイッチングモードで動作するため、スイッチオーバー中にクライアントトラフィックは影響を受けません。

モビリティ MAC

ワイヤレスモビリティ MAC は、モビリティ通信に使用される MAC アドレスです。SSO シナリオでは、ワイヤレスモビリティ MAC アドレスを明示的に設定してください。設定しないと、SSO 後にモビリティトンネルがダウンします。SSO ペアのモビリティ MAC アドレスは、次のいずれかで設定できます。

- 各スタンドアロンコントローラで SSO ペアを形成する前に設定します。ソフトウェアリリース 16.12.3 より前ではこの方法をお勧めします。
- SSO ペアが形成された後のアクティブコントローラで設定します。

モビリティ MAC アドレスを設定する場合、GUI を使用できます。



アドレスを入力したら、[Apply] をクリックします。

注： GUI の MAC アドレスは、ワイヤレス管理インターフェイスから自動的に取得されますが、他の有効な MAC アドレスも使用できます。

CLI では、次のコマンドを使用します。

```
C9800#wireless mobility mac-address <MAC>
```

C9800-CL による SSO HA と vMware vMotion

VMware vSphere vMotion は、サーバー間でのワークロードのダウンタイムなしのライブ移行を実現します。この機能は、C9800-CL にも利用できます。

SSO ペアで設定された C9800-CL で vMotion を使用する場合は、次の点に注意する必要があります。

- 仮想ゲストタギング（VGT モード）に関する ESXi スイッチの現在の制限により、vMotion 中のデータ障害時間が長くなる可能性があります。回避策として、サーバーに接続された物理スイッチ上のテーブル内の MAC アドレスを更新するために、9800-CL からトラフィック（継続的な ping など）を開始する必要があります。この制限については、次のドキュメントを参照してください：https://kb.vmware.com/s/article/2113783?lang=en_US。
- ローカルストレージを使用する場合は、SSD または RAID 0 構成の HDD にする必要があります。
- リモートストレージ（ネットワーク ファイル システム（NFS）やストレージ エリア ネットワーク（SAN）など）を使用する場合は、遅延を最小限に抑える（10 ミリ秒未満）必要があり、10 Gbps 以上のリンクで接続することをお勧めします。
- vMotion およびスナップショットは、SR-IOV インターフェイスではサポートされていません。
- アクティブとスタンバイの両方で vMotion を同時に実行することは推奨されません。

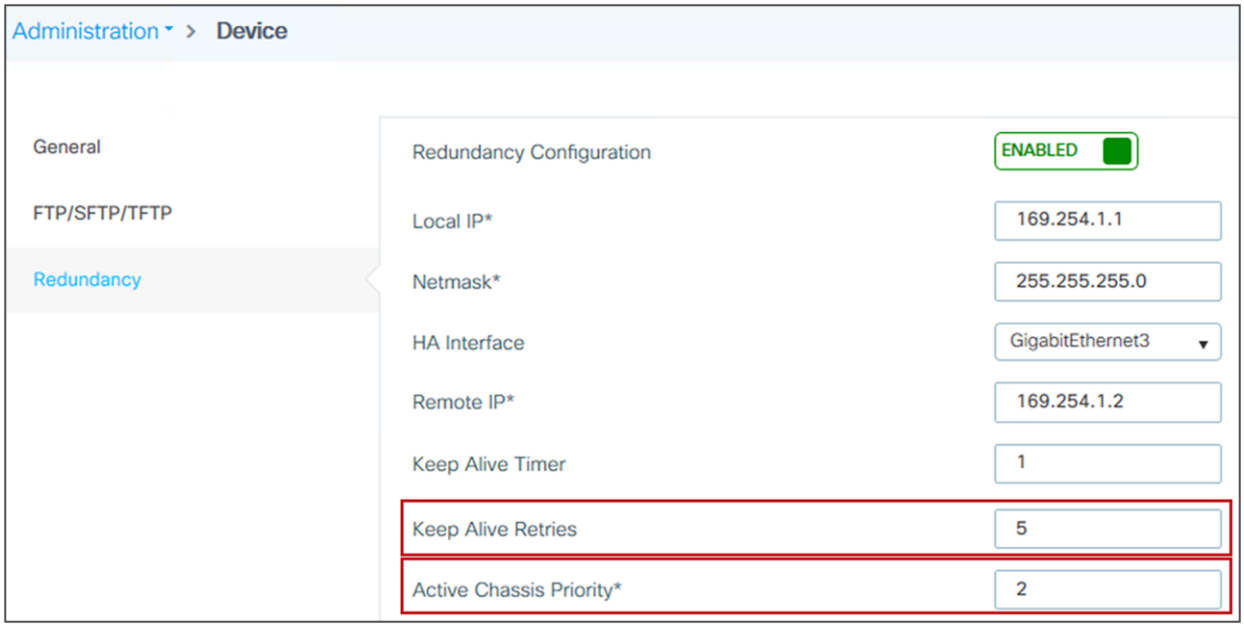
注： リリース 17.6 の時点では、HyperV および KVM における vMotion に相当する機能は検証されていません。

その他の SSO のベストプラクティス

SSO ペアを形成する前に、次のことを確認してください。

- HA SSO を有効にする前に、RP ポートが直接、または専用 L2 ネットワークを介して、接続されている必要があります。光ファイバ SFP またはイーサネット RJ-45 ポートのいずれかに接続できます。光ファイバ SFP HA 接続は、RJ-45 よりも優先されます。RJ-45 HA の稼働中に SFP が接続されると、HA ペアがリロードされます。
- RP ポートを直接（バックツーバックで）接続する場合、シスコでは、長さが 30 m（100 フィート）未満の銅線ケーブルを使用することをお勧めします。30 m（100 フィート）を超える距離で接続する必要がある場合は、光ファイバケーブルを使用して RP ポートを接続することをお勧めします。
- 両方のボックスで同じソフトウェアが動作しており、同じ起動モード（推奨起動モードはインストールモード）になっている必要があります。
- 物理アプライアンスの場合は、まったく同じタイプのハードウェアを使用する必要があります（たとえば、C9800-LC と C9800-LF はペアリングできない）。
- Catalyst 9800-CL の場合は、両方の仮想マシンで同じスケールテンプレート（大規模、中規模、または小規模）を選択する必要もあります。
- HA ペアを形成する前に、以前にスタンドアロンとして展開されていた各 C9800 内の既存の証明書とキーを削除することをお勧めします。これは、両方の WLC に同じトラストポイントが存在するにもかかわらずキーが異なるリスクを回避するためです。これにより、スイッチオーバー後に問題が発生する可能性があります。
- キープアライブ再試行回数を 5 回（リリース 17.1 以降のデフォルト）に設定する必要があります。
- アクティブ WLC にするシャーシに高い優先順位（2）を設定する必要があります。

次に、アクティブコントローラとなるボックスの設定例を示します。



SSO ペアの返品および交換（RMA）での交換手順

SSO ペアのいずれかのボックスに障害が発生し、交換する必要がある場合、シスコでは、ワイヤレスネットワークの中断を回避しながらデバイスをクラスタに戻すために、次の手順を実行することをお勧めします。

1. 障害が発生したボックスを物理的に切り離し、RMA のために発送します。
2. アクティブ WLC に高いシャーシ優先順位（2）が設定されていることを確認します。
3. 新しいボックスを受け取ったら、ネットワークおよび既存の C9800 に接続する前に、基本パラメータ（ログイン情報、IP 接続、および RMI（適用されている場合）を含む冗長化設定）をオフラインで設定します。シャーシの優先順位は必ず 1 に設定してください。これにより、SSO ペアが形成されると、このボックスがスタンバイになり、既存のアクティブ WLC の動作が中断されません。
4. 新しいボックスに設定を保存し、電源をオフにします。
5. 新しい C9800 をネットワーク（アップリンクポートと RP ポート）に物理的に接続します。
6. 新しいボックスの電源をオンにします。
7. ボックスが起動し、SSO ペアが再形成され、新しいボックスがスタンバイホット状態になります。

ワイヤレスおよび RF 設定

ここでは、安定したワイヤレスネットワークの基盤となる、安定した高品質の RF 設計を構築するための一般的な推奨事項について説明します。

サイトサーベイ

どのワイヤレス展開でも、常に適切なサイトサーベイを実施して、ワイヤレスクライアントおよびアプリケーションに適切なサービスレベルを確保してください。各アプリケーションには、異なる要件があることに注意してください。たとえば、音声展開には、遅延やジッターに関してデータサービスよりも厳しい要件があります。ロケーションベースの展開では、各クライアントの位置を三角測量できるように、AP をより高密度で展開する必要があります。新しい IoT アプリケーションでは、遅延に関する厳しい要件が課される場合があります。

RRM は優れたツールであり、動的チャネル割り当て（DCA）や送信電力制御（TPC）などの機能が、最適なチャネルや電力プランを自動的に設定するために役立ちますが、RRM では不適切な RF 設計を修正できないことに注意してください。サイトサーベイは、実際のネットワークで使用するデバイスの送信電力および伝搬動作と一致するデバイスを使用して実施する必要があります。理想的には、実際のデバイスモデルおよびオペレーティングシステム/ファームウェアバージョンを、実稼働ネットワークで使用される場合と同じ状態および設置方向で使用する必要があります。たとえば、最終的なネットワークで 802.11a/b/g/n や 802.11ac/ax/be のデータレートに対応した最新のデュアル無線を使用する場合は、カバレッジの調査で無指向性アンテナを備えた古い 802.11b/g 無線を使用しないでください。サイトサーベイは、設置する AP のモデルに一致させて実施する必要があります。AP は、最終的な設置状態で典型的となる設置方向および高さにする必要があります。AP のデータレートは、アプリケーション、帯域幅、およびカバレッジの要件に応じたレートに設定する必要があります。ネットワーク設計の主な目的が、各カバレッジエリアにおいて 30 人のユーザーが 5GHz で 9Mbps のデータレートを利用できることである場合は、5GHz および 9Mbps のデータレートのみが有効になっている主要なネットワークデバイスを使用してカバレッジテストを実施します。その後、AP とクライアントの間にアクティブなデータトラフィックがあるときに、テスト用のネットワーククライアントについて、受信信号強度表示（RSSI）が -67 dBm であることを AP で測定します。高品質の RF リンクは、25 以上の良好な信号対雑音比（SNR）と、低いチャネル使用率（CU）パーセンテージを持ちます。RSSI、SNR、および CU の値は、WLC のクライアントおよび AP 情報ページで確認できます。

低データレート

データレートを有効または無効にするプロセスは、慎重に計画する必要があります。カバレッジが十分である場合は、低いデータレートを 1 つずつ段階的に無効化することをお勧めします。ACK やビーコンなどの管理フレームは、最小必須レート（通常、1Mbps）で送信されます。この最小必須レートが最も多くの通信時間を消費するため、全体のスループットが低下します。クライアントが再送信時にレートをより迅速に下げられるように、サポートされるデータレートを増やしすぎないようにしてください。通常、クライアントは、最も高速なデータレートでの送信を試みます。フレームの送信に失敗する場合、クライアントは、フレームが正常に送信されるまで、段階的にデータレートを下げて再送信します。サポートされるレートの数を減らすことで、フレームを再送信するクライアントが、複数のデータレートを一度に下げることができ、結果として、フレームが 2 回目の試行で正常に送信される可能性が高くなります。

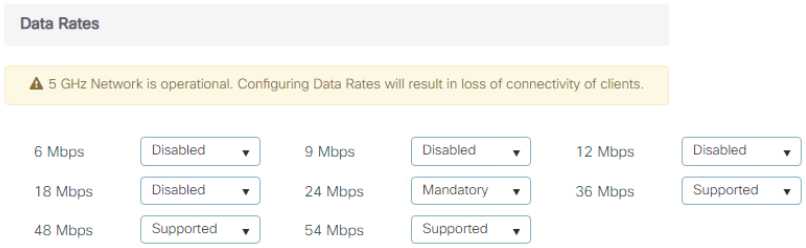
データレート設定を検討する際の注意事項：

- ビーコンは最も低い必須レートで送信されます。これによって、おおよそのセルサイズが決定されます。
- マルチキャストは、選択されている最も低い必須データレートで送信されます。
- ネットワークに 802.11b クライアントが実際に存在しているでしょうか。存在しない場合は、802.11b のデータレート（1、2、5.5、および 11Mbps）を無効にして、その他は有効のままにすることを検討してください。
- ホットスポット向けに設計する場合、目的は速度よりもカバレッジの広さであるため、最も低いデータレートを有効にします。
- 逆に、高速ネットワークやキャパシティを目的に設計しており、すでに RF カバレッジが良好である場合は、最も低いデータレートを無効にします。
- 通信仕様（TSPEC）とコールアドミッション制御（CAC）を使用する場合は、12Mbps を有効にする必要があります。

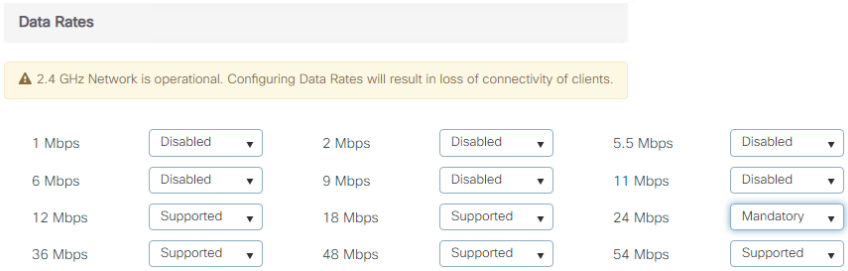
以下に、データレートに関する一般的な推奨事項を示します。ただし、これらは一般的なものであるため、注意が必要です。上記のリストを参照して、実際のネットワークに適用されるかどうかを判断してください。

- 必要でないかぎり、すべての 11b レートを無効にします。
- スループットよりも範囲が優先される場合（屋外など）は、6Mbps を必須レートとして使用します。
- ほとんどのネットワークでは、デフォルトの開始点として、12Mbps を必須レートとして使用します。
- 適切に設計された高密度ネットワークでは、24Mbps を必須レートとして使用します。
- 必須レートを下回るすべてのレートを無効にします。

以下の設定はあくまで一例であり、すべての設計の厳密なガイドラインと見なさないでください。これらの変更は慎重に行う必要があり、RF カバレッジ設計に大きく依存します。データレートを変更するには、[設定（Configuration）] > [無線設定（Radio Configuration）] > [ネットワーク（Network）] に移動し、[5 GHz] タブをクリックします。



次に、[2.4 GHz] タブをクリックします。



[6 GHz] タブについても同様です。

SSID 数の削減

シスコでは、コントローラに設定するサービスセット識別子（SSID）の数を制限することをお勧めします。WLAN/SSID は（各 AP の無線ごとに）同時に 16 個まで設定できますが、それぞれの WLAN または SSID で個別のプローブ応答とビーコンが必要となり、それらが最も低い必須レートで送信されるため、SSID が追加されるにつれて RF 汚染が増大します。また、PDA、Wi-Fi 電話機、バーコードスキャナなどの小型ワイヤレスステーションの一部では、多数の基本 SSID（BSSID）を無線で処理できません。この結果、ロックアップ（動作停止）、リロード、または関連付けの失敗が発生します。企業の場合は無線帯域ごとに 1 ～ 3 つの SSID を設定し、高密度設計の場合は無線帯域ごとに 1 つの SSID を設定することをお勧めします。これらは、すべての周波数帯（2.4 GHz、5 GHz、および 6 GHz）に適用されます。AAA オーバーライド機能を使用すると、単一の SSID シナリオでユーザーごとに個別の VLAN/設定を割り当てながら、WLAN/SSID の数を減らすことができます。SSID を確認するには、次のコマンドを入力します。

```
C9800#sh wlan summary

Number of WLANs: 3

ID   Profile Name            SSID             Status              Security
-------------------------------------------------------------------------------1    employee
employee             UP          [WPA2][802.1x][AES]
2    guest                   guest                UP    [open],[Web Auth]
3    voice                voice               UP    [WPA2][802.1x][AES]
```

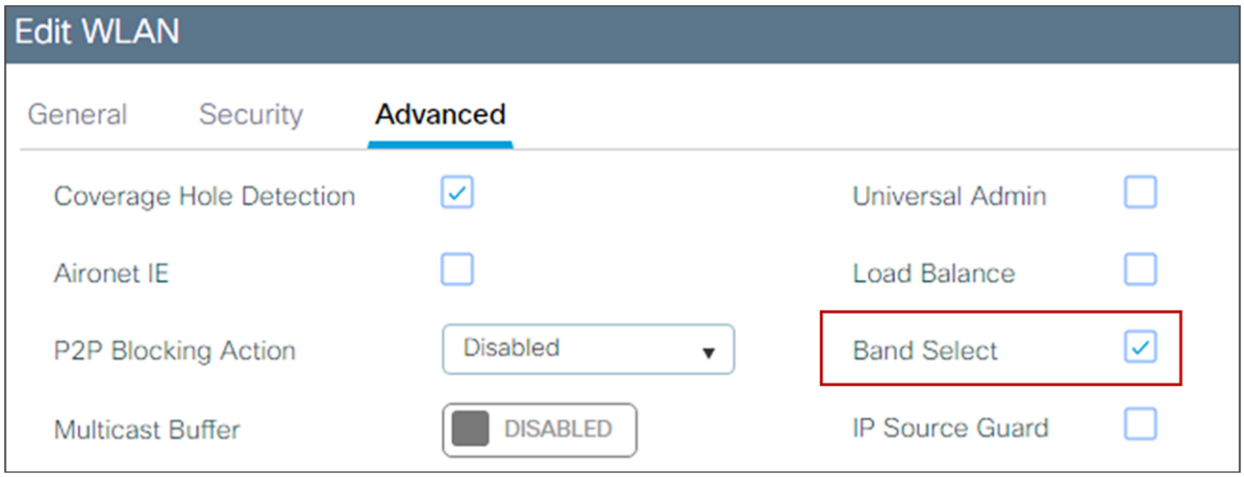
帯域選択

2.4 GHz 帯域は頻繁に利用率が高くなり、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受ける可能性があるだけでなく、他の AP からの同一チャネル干渉も発生します。802.11b/g では、重複しないチャ

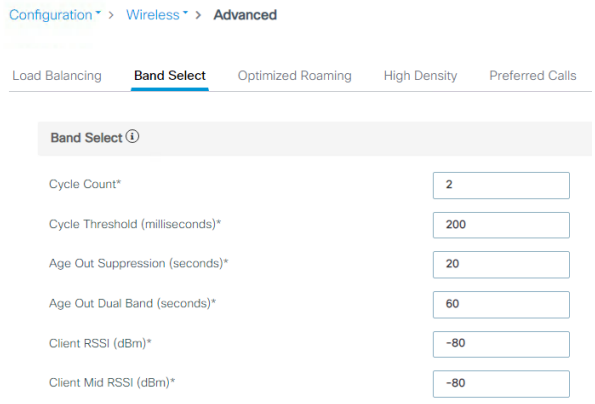
ネルが 3 つしかないからです。これらの干渉の原因を防止して、ネットワーク全体のパフォーマンスを向上させるために、コントローラで帯域選択を設定できます。以下の点に注意してください。

- 帯域選択は WLAN ごとに設定でき、デフォルトでは無効になっています。
- 帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。
- 音声またはビデオサービス（あらゆるインタラクティブなトラフィック）を展開する場合は、帯域選択を使用しないでください。一部のクライアントタイプでは、ローミングパフォーマンスが低下する可能性があります。

AP の 5 GHz 信号が 2.4 GHz 信号と同等かそれ以上に強い場合、ほとんどの最新クライアントではデフォルトで 5 GHz が優先されます。これは、新しいクライアントタイプを使用した展開において、帯域選択が必要ない可能性があることを意味します。一般的に、デュアルバンドクライアントは、最初に関連付けられたのと同じ帯域でスキャンを開始します。帯域選択は初回スキャンに影響を与え、クライアントを 5 GHz に誘導します。そのため、クライアントが最初に 5 GHz 帯域に参加した場合、5 GHz の送信電力レベルが良好であれば、その帯域に留まる可能性が高くなります。この機能を有効にするには、WLAN 設定の [詳細（Advanced）] タブに移動します。



デフォルト設定を変更する一般的な理由はありませんが、特定の環境に合わせて帯域選択動作を調整する必要がある場合は、ここで行ってください。



6 GHz 設計

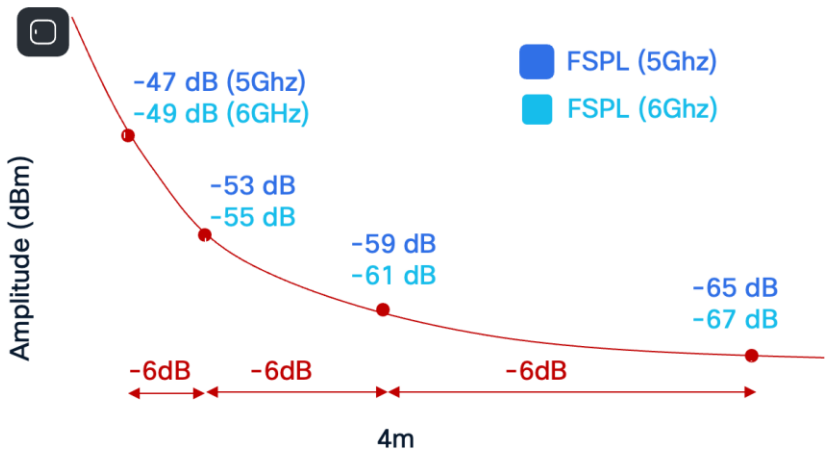
Wi-Fi 6E の導入により、新しい周波数が使用可能になりました。この新しい周波数は 6 GHz であり、利用可能な帯域幅は国によって異なります。以下に、この新しい周波数向けに設計する方法に関する考慮事項を示します。

Cisco ワイヤレスを使用して 6 GHz および Wi-Fi 7 に移行する方法については、専用のガイド（https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/223061-migrate-to-wi-fi-7-and-6ghz.html）を参照してください。

自由空間パス損失（FPSL）：これは、電磁波が空間を伝搬するときの電力密度の減少です。自由空間とは、送信者と受信者の間に障害物がなく、視線が通っている状態を指します。最初の 1 メートルにおけるパス損失は、5 GHz よりも **6 GHz の方が平均 2dB 高く**なります。その後は 6 dB のルールが適用されます。つまり、周波数に関係なく、距離が 2 倍になると 6 dB の損失が発生します。

セルサイズに関する考慮事項：6 GHz では、同じ送信電力レベルの場合、6 GHz のセルは 5 GHz のセルよりも小さくなります。電磁気学の物理法則により、6 GHz でのパス損失は 5 GHz よりも大きくなります。次のグラフは、これを示しています。

図 6 : 5 GHz と 6 GHz のパス損失



吸収/反射：6 GHz は、壁やその他の表面を通過するときに、より大きく減衰します。

6 GHz でのノイズフロアは、5 GHz よりも大幅に低くなります（少なくとも当面の間、6 GHz には多くの干渉がないため）。

ダウンストリーム（AP からクライアントへ）**/アップストリーム**（クライアントから AP へ）：2.4 GHz および 5 GHz と同様に、6 GHz でも、アップストリームがセルの制限要因になることが予想されます。

カバレッジタイプ：現在、6 GHz は、屋内でのみ使用できます。ただし、米国/カナダでは、自動周波数調整（AFC）を利用することで屋外でも使用できます。これは変わりつつあり、最終的に、規制当局が承認すると、より多くの国がサポートされるようになります。

6 GHz での AP アンテナパターンは、5 GHz と似ていますが、前述したように、パス損失のために少し「短く」なります。5 GHz と 6 GHz の間の AP カバレッジは、特に開けた空間では似ています。ただし、6 GHz では 3dB 以上高い送信電力で補正する必要があります。

図 7 : 5 GHz セルと 6 GHz セルの比較

展開に関する考慮事項

更新時期を迎えた**既存の展開**では、AP を 1 対 1 で置き換えることを検討できます。セルサイズが 140 ～ 190 m^2 で、天井の高さが 3 ～ 4 m の場合のガイダンスは、次のとおりです。

- 平均送信電力レベルが 3 ～ 4 である場合は、1 対 1 の AP の交換が可能です。5 GHz と 6 GHz の間で同等のカバレッジレベルが得られます。
- 平均送信電力レベルが 1 ～ 2 である場合は、追加の AP が必要になります（約 10 ～ 20% の追加 AP）。

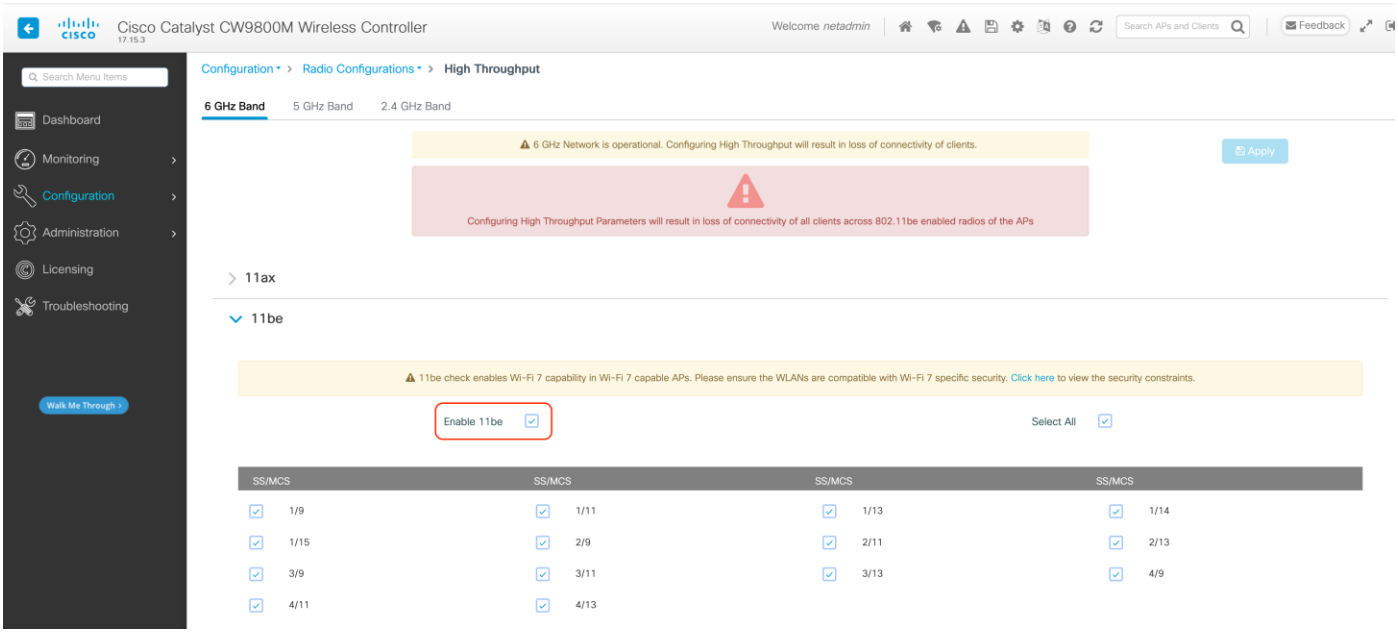
新しい展開の場合は、サイトサーベイを実施することをお勧めします。Cisco Wi-Fi 6E/7 AP では、サイトサーベイモードを活用してください。

同じエリアに Wi-Fi 6E AP、Wi-Fi 7 AP と古い世代の AP を混在させることは推奨されません。これまでと同様に、「ソルトアンドペパー」設計はできるだけ避けることが推奨されています。

高スループット

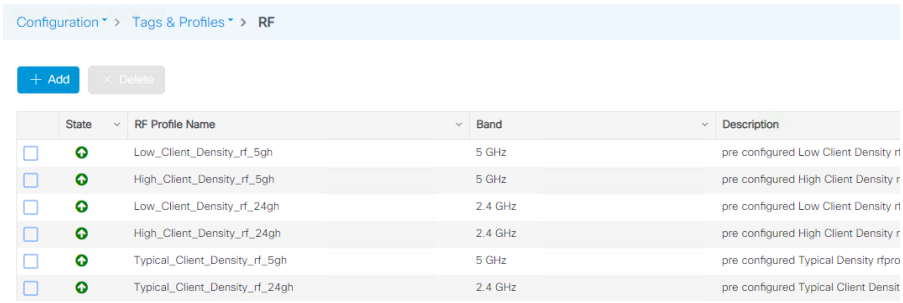
高スループットは、無線ネットワークを介してデータが正常に配信されるレートを向上させるために設計されたパラメータで構成されます。

ネットワークで Wi-Fi 7（802.11be）を有効にする場合は、[11be の有効化（Enable 11be）] チェックボックスをオンにする必要があります。



RF プロファイル

RF プロファイルは、特定の一連のアクセスポイントに対して RRM および RF パラメータをカスタマイズするための主要なメカニズムです。C9800 には 2 つの RF プロファイル（帯域ごとに 1 つ）があり、これらは RF タグを介して AP に割り当てられます。C9800 には 6 つのデフォルト RF プロファイル（帯域ごとに 3 つ）があり、「Typical」（標準）プロファイルがデフォルトになっています。



デフォルトのいずれかを変更するか、カスタムパラメータを作成することができます。RF プロファイル内にはカスタマイズできる多数の RF パラメータ（チャネル選択、データレート、RRM 設定（DCA、TPC、CHD）、RX-SOP しきい値など）があります。いくつかの一般的な推奨事項を以下に示します。

- AP 密度と設置高さに基づいて、RF グループに必要な TPC しきい値を設定します。大規模な展開では RF 環境が大幅に変化する可能性があるため、TPC を適切に調整して、各場所で最適なカバレッジを確保することが重要です。
- データレートは、送信電力とともに、クライアントのローミング動作に影響を与える主要なメカニズムです。最も低い必須レートを変更すると、クライアントが新しいローミングをトリガーするタイミングが変更されることがあります。この点は、スティッキークライアントの問題が発生する大規模なオープンスペースでは特に重要です。

RF プロファイルを設定する場合は、DCA の計算に悪影響を与える可能性があるため、隣接する AP グループと RF プロファイルを異なる DCA チャネルセットで設定しないでください。

ユーザーは、チャネルが設定された規制ドメインでサポートされていない場合でも、サポートされていないチャネルを RF プロファイル DCA リストに追加できます。設定されたチャネルが使用国のドメインで許可されているか、常に確認することを推奨します。DCA はサポートされていないチャネルを AP に割り当てないため、ネットワーク運用に影響を与えることはありませんが、リリース 17.5 以降、C9800 では、追加されたチャネルが許可されているかどうかを確認するための検証機能が追加されています。

集約プローブ応答の最適化

大規模な高密度展開の場合は、アクセスポイントによって送信される集約プローブの間隔のデフォルト値を変更することをお勧めします。デフォルトでは、AP は、クライアントによって送信されたプローブに関する情報を 500 ミリ秒ごとに更新します。この情報は、負荷分散、帯域選択、ロケーション、および 802.11k 機能で使用されます。多数のクライアントとアクセスポイントがある場合、WLC でコントロールプレーンのパフォーマンスの問題が発生しないように、更新間隔を変更することをお勧めします。

この設定を変更するには、次のコマンドを使用します。

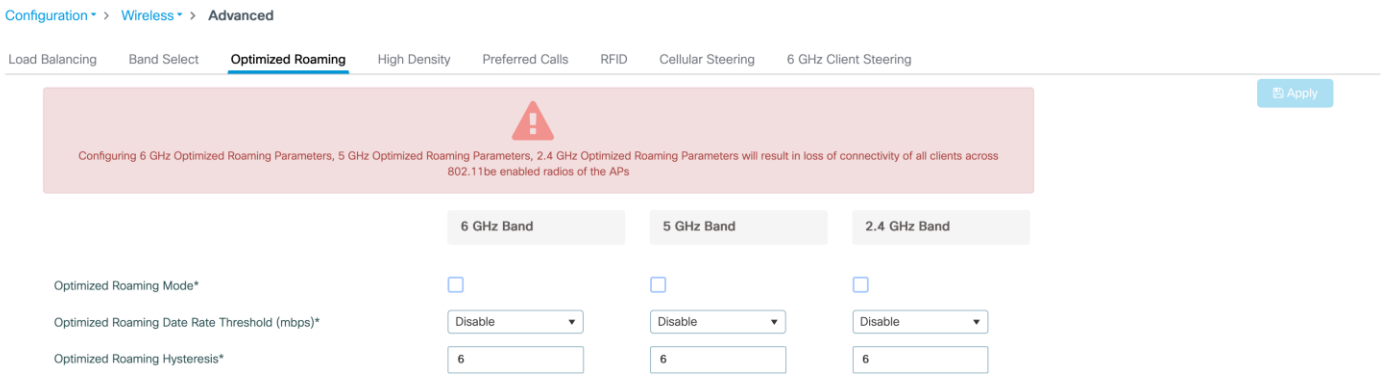
```
C9800(config)# wireless probe limit 50 64000
```

これにより、64 秒ごとに 50 件の集約プローブ応答に設定されます。これが推奨設定です。

最適化ローミング

Apple、Samsung、およびその他の最新デバイスが新しい 802.11r、802.11k、および 802.11v ローミングの改善を使用するため、最適化ローミングは無効にする必要があります。この設定はデフォルトで無効になっており、GUI で確認できます。

図 8 : 最適化ローミングの設定

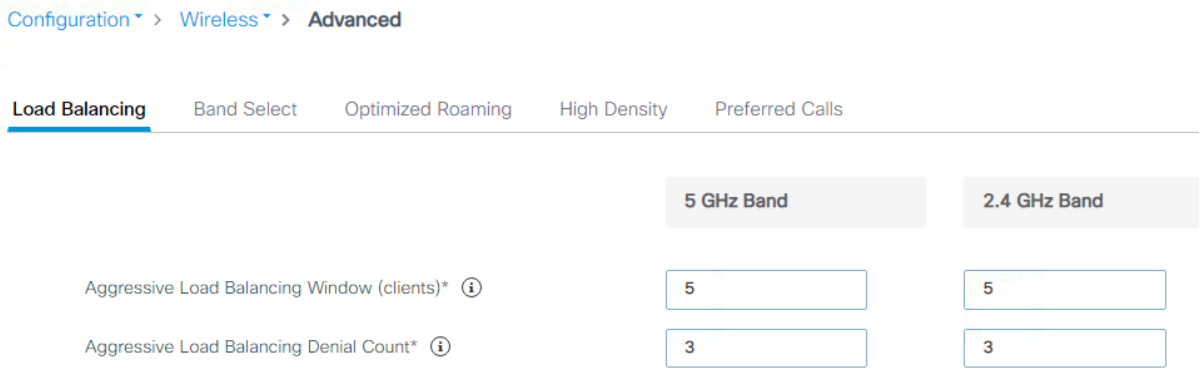


CLI で設定するには、次のコマンドを使用します。

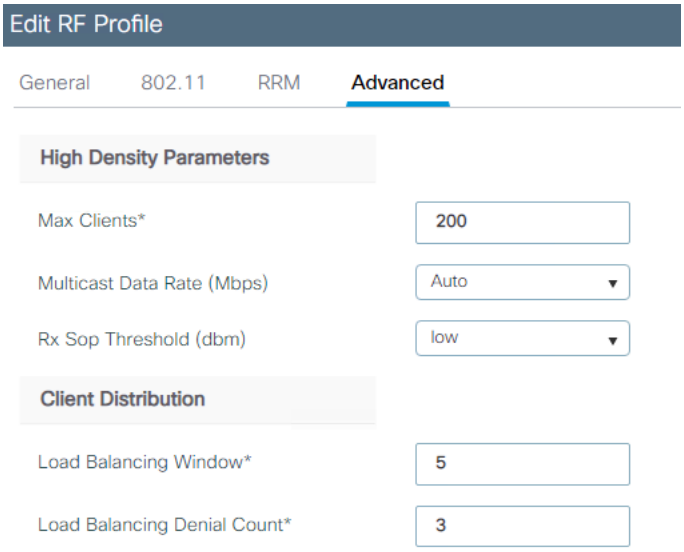
```
Device(config)# ap dot11 [6ghz | 5ghz | 24ghz] rrm optimized-roam
```

アグレッシブ負荷分散

負荷分散が必要な場合は、WLAN で有効にできます。関連付けエラーを防ぐため、コントローラのグローバルウィンドウが 5 クライアント以上に設定されていることを確認してください。これは、5 GHz 帯域と 2.4 GHz 帯域の両方に適用されます。



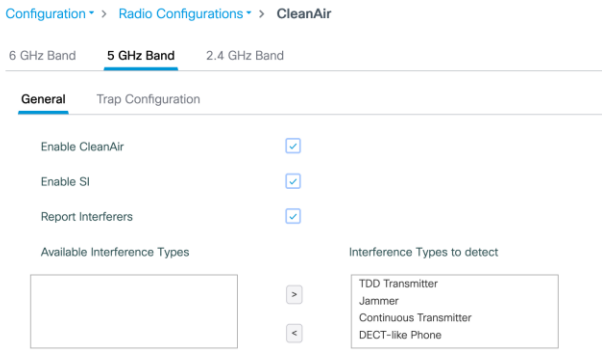
C9800 では、これらの設定を RF プロファイルごとに設定することもできます。これにより、特定の AP グループを固有の RF プロファイルおよびタグに割り当てることで、負荷分散ウィンドウを特定の AP グループのみに割り当てることができる柔軟性が得られます。



音声またはインタラクティブなビデオトラフィックに悪影響を与える可能性があるため、良好なカバレッジ環境でのみこの機能を使用することをお勧めします。

CleanAir の有効化

RF 干渉を効果的に検出し軽減するため、可能な限り Cisco CleanAir® を有効にします。新しい 6 GHz 帯域の追加により、CleanAir は、17.13 以降で CleanAir Pro に進化しています。汎用の DECT 電話、電波妨害装置など、セキュリティアラートを起動する各干渉源に対しては推奨対策があります。異なる帯域での CleanAir の設定を確認するには、次の操作を実行します。



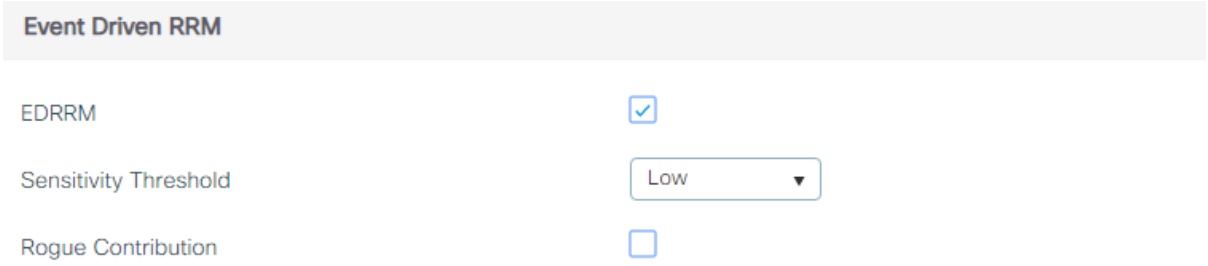
一般的に、CleanAir はネットワークパフォーマンスに影響を与えないため、オンのままにておいてください。お客様のいくつかの導入事例において、多数の Bluetooth ビーコンデバイスが存在するためにパフォーマンスが多少低下したことがありました。このような場合、これらのタイプのデバイスに対する CleanAir 検出を無効にすることをお勧めします。これを実行するには、次のコマンドを使用します。

```
C9800(config)#no ap dot11 24ghz cleanair device ble-beacon
```

イベント駆動型 RRM

この機能により、AP の現在の動作チャネルにおいて突発的で重大な RF 干渉が検出された場合、通常の DCA プロセスによる RF メトリックに基づいた変更の実行を待つことなく、WLC がチャネル変更を行うことができます。この機能は、CleanAir の情報を活用し、クライアントがスループットの低下や接続の問題を抱えている可能性が高い状況で、迅速な対応を強制的に実行させることができます。

イベント駆動型 RRM（ED-RRM）はデフォルトでは有効になっていませんが、有効にすることをお勧めします。これは、[設定（Configuration）] > [無線設定（Radio Configuration）] > [RRM 設定（RRM settings）] で行います。



スペクトル インテリジェンス

スペクトルインテリジェンス（SI）は、2.4 GHz 帯域および 5 GHz 帯域における非 Wi-Fi 無線干渉を AP がスキャンできるようにする機能です。スペクトルインテリジェンスは、マイクロ波、連続波（ビデオブリッジやベビーモニターなど）、Wi-Fi および周波数ホッピング（Bluetooth および周波数ホッピングスペクトラム拡散（FHSS）コードレス電話）の 3 種類の干渉を検出する基本的な機能を提供します。これは、専用無線によるハードウェア アクセラレーション ソリューションがない AP でサポートされています。

SI は、ソフトウェアで実行され、クライアントにサービスを提供する無線を活用するため、シスコでは、この機能を無効にすることをお勧めします（リリース 17.6.1 以降ではデフォルトで無効になっている）。有効にする場合は、いつ、どこで行うかを慎重に検討してください。

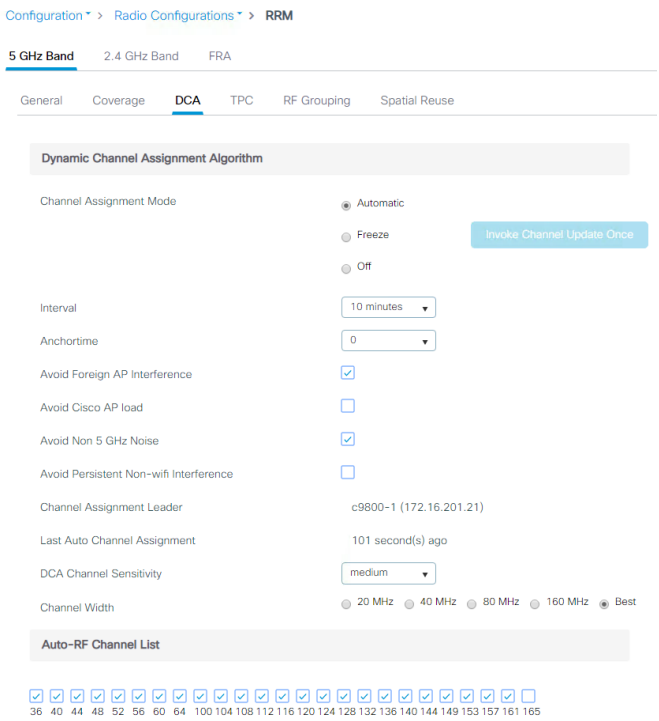
チャネルの動的割り当て

ワイヤレスネットワークが初めて初期化される際、参加するすべての無線で、干渉なしで動作するためにチャネルの割り当てが必要になります。動的チャネル割り当て（DCA）は、干渉なしの動作を可能にするチャネル割り当てを最適化します。C9800 ワイヤレスコントローラは、検出された全チャネルについて各無線から報告された電波メトリックを使用して、チャネル帯域幅を最大化し、RF 干渉を最小化する解決策を提供します。この干渉は、当該ネットワーク（シグナル）、他のネットワーク（外部干渉）、ノイズ（その他すべて）といったあらゆる干渉源からのものです。

DCA はデフォルトで有効になっており、社内のネットワークのためにチャネルプランニングのグローバルな解決策として機能します。RRM に、可用性と干渉に基づいてすべての 802.11a または 802.11b/g チャネルを自動的に設定させます。これはデフォルトですが、CLI コマンドを次に示します。

```
C9800(config)#ap dot11 5ghz rrm channel dca global auto
C9800(config)#ap dot11 24ghz rrm channel dca global auto
```

すべての設定は GUI でも利用できます（次の例は 5 GHz ネットワークの場合）。



DCA 間隔

この間隔は、デフォルトで 10 分に設定されています。ネットワークが起動して安定した後は、時間単位で長い間隔（4 ～ 6 時間など）を選択することをお勧めします。

チャネル幅

802.11n は、2 つの 20 MHz チャネルを結合することで、40 MHz チャネルで動作できます。これにより、スループットが大幅に向上します。すべての 802.11n デバイスが 40 MHz の結合チャネルをサポートしているわけではないため、確認することが重要です。802.11ac/ax/be では、20 MHz チャネルを 80 MHz 幅のチャネルに結合して、802.11ac/ax/be で利用できます。また、すべてのクライアントが 80 MHz をサポートしている必要があります。2.4 GHz では、使用可能な重複しない 20 MHz チャネルの数が非常に限られているため、これは実用的ではありません。ただし、5 GHz および 6 GHz では、使用可能な 20 MHz チャネルが十分にある場合、スループットと速度が大幅に向上する可能性があります。

次に、チャネル幅の概要を示します。

- [20 MHz]：20 MHz チャネルだけを使用する無線の通信を許可します。20 MHz チャネルだけを使用して通信するレガシー 802.11a 無線、20 MHz 802.11n 無線、または 40 MHz 802.11n 無線の場合にこのオプションを選択します。
- [40 MHz]：隣接する 2 つの 20 MHz チャネルを結合して使用する 40 MHz 802.11n/ac/ax/be 無線の通信を許可します。無線では、ユーザーが選択するプライマリチャネルをアンカーチャネル（ビーコン用）として使用すると同時に、データスループット向上のために、その拡張チャネルも使用します。各チャネルには、1 つの拡張チャネルがあります（36 と 40 のペア、44 と 48 のペアなど）。たとえば、プライマリ チャネルとして 44 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 48 が使用されます。プライマリ チャネルとして 48 を選択すると、Cisco WLC では拡張チャネルとしてチャネル 44 が使用されます。Apple iOS に焦点を合わせた展開では、40 MHz が推奨されるチャネル幅です。
- [80 MHz]：802.11ac/ax/be 無線のチャネル幅を 80 MHz に設定します。
- [160 MHz]：802.11ac/ax/be 無線のチャネル幅を 160 MHz に設定します。

- [320 MHz]：6 GHz にのみ適用され、802.11ax/be 無線のチャンネル幅を 320 MHz に設定します。6 Ghz スペクトラムをどれくらい利用できるかは国によって異なるため、これの有効性は国によって変わる可能性があります。
- [最適（Best）]：環境条件に応じてチャネル幅を変更できる動的帯域幅選択を有効にします。これがデフォルト設定です。

可能な場合は、AI-RRM の最大限の活用を試みることをお勧めします。これにより、チャネル幅も自動管理されます。一部のデバイスでは、より大きなチャネル幅を優先する（20MHz よりも 80MHz）傾向があることが知られています。隣接する AP のチャネル幅が異なる場合、一部のクライアントが特定の AP を優先する可能性があります。設計時には、同じエリア内のチャネル幅を非常に近いものにする（同じではなくても）ことを試みてください。

他のワイヤレスネットワークが同じ RF 空間で動作するために、チャネル結合の重複が発生する可能性があるマルチテナントビルディングの場合は、[最適（Best）] オプションでチャネル結合を強制的に 40 MHz に制限することができます。

```
C9800(config)#ap dot11 5ghz rrm channel dca chan-width width-max WIDTH_40Mhz
```

企業シナリオでは、40 MHz チャネル幅が安全であり、重複しないチャネルの可用性とパフォーマンスのバランスが最もよく取れた妥協点となります。高密度展開または産業用展開では、20 MHz にする必要がある場合があります。重複するネットワークがない場合にのみ、80、160、または 320 MHz を使用してください。一部のクライアントデバイスは、80、160、または 320 MHz で正常に動作しない可能性があるため、実際の環境で検証する必要があります。高いスループットにはより高い SNR が必要であることと、2.4 GHz や 5 GHz でチャネル幅を広げると SNR が低下することに注意してください。

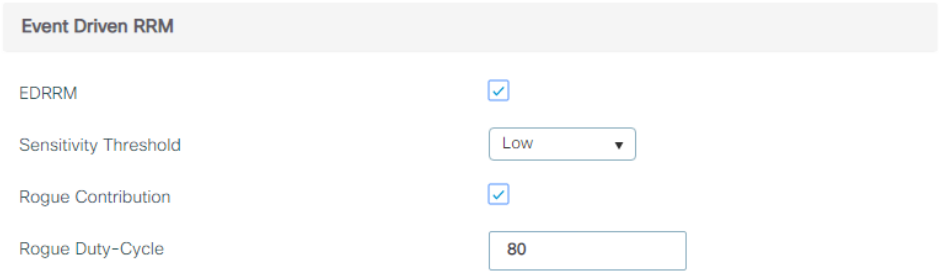
注： 初めて [最適（Best）] を有効にする場合は、`C9800#ap dot11 5ghz/24ghz rrm dca restart` コマンドを使用して DCA を完全に再起動することをお勧めします。

Wi-Fi 干渉認識

RRM は CleanAir およびスペクトル解析と連携して動作します。また、ED-RRM は干渉に対して迅速に対応できるようにする重要な機能です。Wi-Fi 干渉への対応を改善するために、Wi-Fi 干渉認識と呼ばれる機能により、不正のシビラティ（重大度）が ED-RRM メトリックに追加されました。不正アクセスポイントによって指定のしきい値を超える干渉が生じている場合は、この機能によって、次の DCA サイクルまで待つことなく、すぐにチャネルが変更されます。

注： ED-RRM が有効になっている場合は、Wi-Fi 干渉認識を使用してください。非常に多数のコロケーション Wi-Fi ネットワークがある建物（マルチテナントビルディング）で、それらが 100% 重複している場合は、こうした干渉を回避する必要があります。

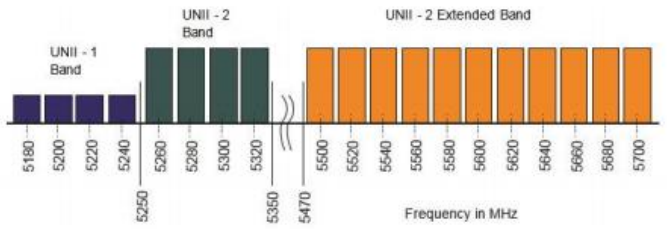
Wi-Fi 干渉認識を有効にして、デューティサイクルを 80% に設定するには、[設定（Configuration）] > [無線設定（Radio Configuration）] > [RRM] で [DCA] タブに移動し、[イベント駆動型 RRM（Event-Driven-RRM）] セクションに移動します。



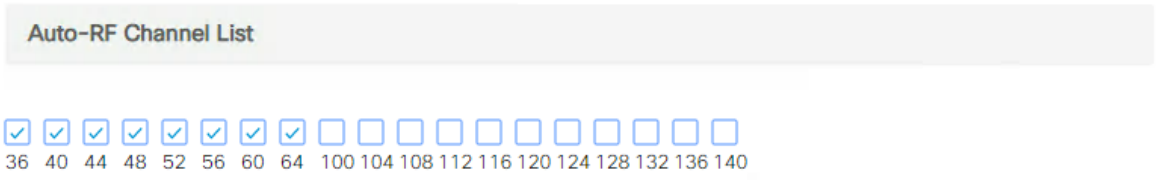
DCA と動的周波数選択

動的周波数選択（DFS）は、5 Ghz スペクトラムのチャネルの可用性を増やすために作成されました。規制ドメインに応じて、これは 4 ～ 12 の追加チャネルになります。チャネルが多いほど、キャパシティが大きくなります。DFS は、レーダー信号を検出し、その周波数で動作している可能性のある気象レーダーとの干渉がないことを確認します。5 GHz 帯域はより多くのチャネルを提供しますが、5 GHz チャネルでは送信電力および屋内/屋外展開に関するさまざまな制限があるため、全体的な設計には注意が必要です。たとえば、北米では、U-NII-1 チャネルは屋内でのみ使用でき、最大送信電力が 50 mW に制限されています。また、U-NII-2 と U-NII-2e の両方が DFS の対象になります。

図 9 : U-NII チャネル



デフォルトでは、U-NII-2e チャネルは DCA チャネルリストで無効になっています。使用中のチャネルを確認したり、チャネルを追加するには、[チャネルリスト（Channel List）] セクションに移動します。



DCA の再起動

チャネルとチャネル幅を選択すると、DCA は、そのチャネルを動的に管理し、時間の経過や条件の変化に応じて必要な調整を行います。ただし、新規の導入の場合や、DCA に大きな変更（チャネル幅の変更や新しい AP の追加など）を加えた場合は、DCA プロセスを再起動できます。これにより、アグレッシブ検索モード（スタートアップ）が初期化され、最適化された初期チャネル計画が提供されます。どの WLC が現在グループリーダーであるかを確認するには、次のコマンドを使用します。

```
C9800#sh ap dot11 5ghz group
C9800#sh ap dot11 24ghz group
```

特定されたグループリーダーから DCA を再初期化するには、次のコマンドを使用します。

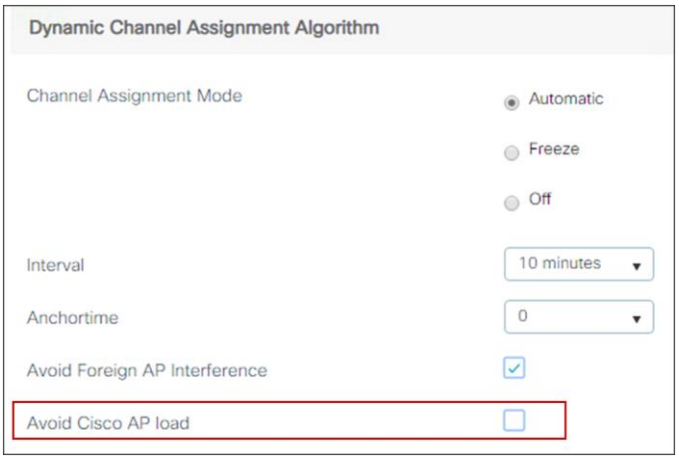
```
C9800# ap dot11 5ghz rrm dca restart
C9800# ap dot11 2.4ghz rrm dca restart
```

スタートアップモードは 100 分間実行され、通常、30 ～ 40 分以内にソリューションに到達します。チャネル幅、AP 数などに大幅な変更が加えられた場合、多数のチャネル変更が原因でクライアント接続が中断する可能性があります。

注： DCA の再起動は、特に医療分野で多く見られるリアルタイムベースのアプリケーションを含むワイヤレスネットワークにおいては、変更管理の承認なしに実行しないでください。

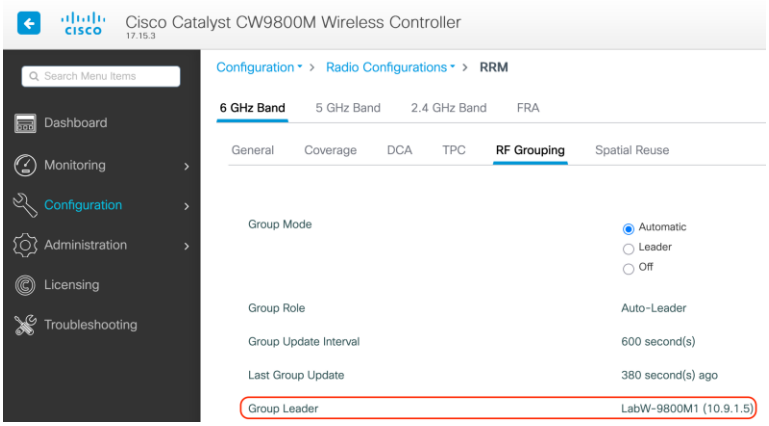
DCA Cisco AP Load

負荷条件の変動により、DCA での変更が過剰にトリガーされる可能性があるため、このオプションは使用しないでください。この機能はデフォルトではディセーブルになっています。



DCA とフレキシブル ラジオ アサインメント

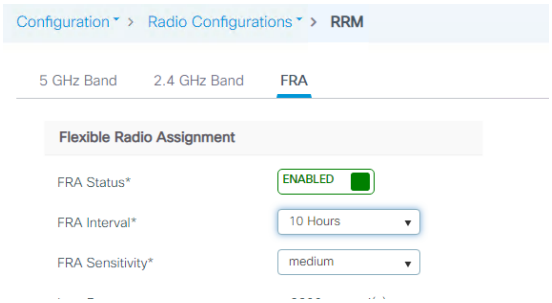
フレキシブル ラジオ アサインメント（FRA）を適切に機能させるには、チャネル変更リーダー（RF グループリーダー）が 2.4 GHz、5 GHz、および 6 GHz 帯域で同じである必要があります。同じかどうかを確認するには、次の場所に移動します。



3 つのタブ（2.4 GHz、5 GHz、および 6 GHz のタブ）を調べて、すべての周波数のグループリーダーを確認してください。

DCA 間隔と FRA 間隔

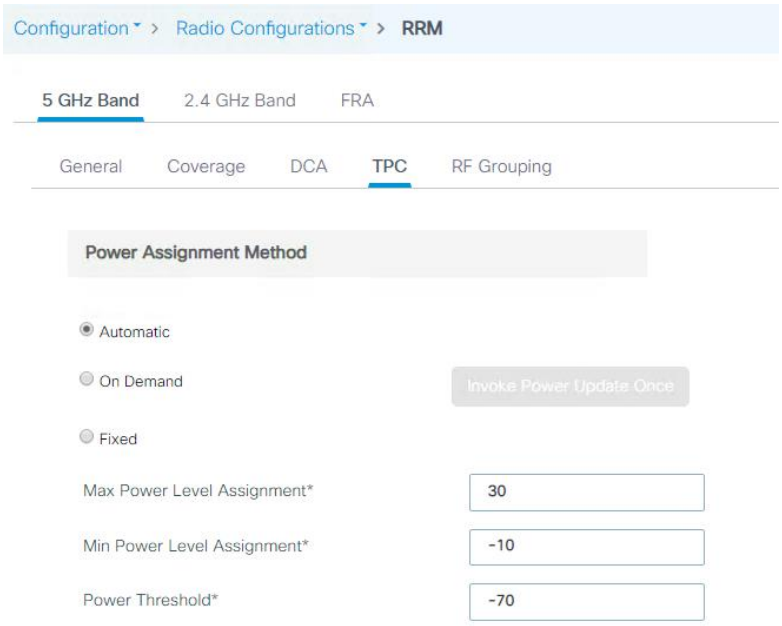
FRA が使用されていない場合でも、FRA 間隔は DCA 間隔以上である必要があります。変更するには、FRA 間隔を目的の値に設定してから、DCA 間隔を変更するだけです。次の例では、DCA を 8 時間ごとに実行すると設定されていると想定されており、FRA を 10 時間ごとに実行するように設定できます。



送信電力の制御

Catalyst 9800 ワイヤレスコントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセスポイントの送信電力を動的に制御します。

送信電力制御（TPC）アルゴリズムでは、RF 環境での変化に応じて AP の送信電力を増減させます。ほとんどの場合、TPC では干渉を低減するために AP の送信電力を減らそうとします。しかしながら、RF カバレッジに急激な変化が生じた場合（たとえば、AP で障害が発生したり、AP が無効になったりした場合）、TPC が周囲の AP の送信電力を増やす可能性もあります。この機能は、主にクライアントと関係があるカバレッジホールの検出とは異なります。TPC では AP 間のチャネルの干渉を防止しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を供給します。6 GHz、5 GHz、または 2.4 GHz 帯域で自動 TPC を設定するには、[設定（Configuration）] > [無線設定（Radio Configuration）] > [RRM] に移動してから、[6 GHz 帯域（6-GHz Band）]、[5 GHz 帯域（5-GHz Band）]、または [2.4 GHz 帯域（2.4-GHz Band）] タブを選択します。



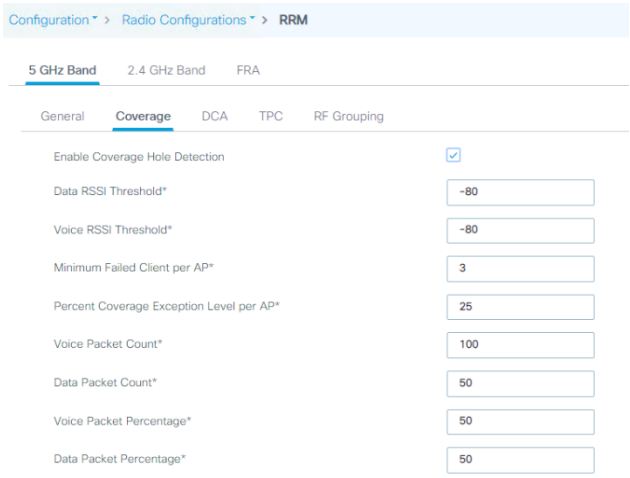
最適なパフォーマンスを得るには、無線ごとに最適な送信電力を許可するための [自動（Automatic）] 設定を使用します。ほとんどの環境ではデフォルト値が機能しますが、RF 展開の特性に適切に適応させるために、TPC しきい値を調整することをお勧めします。

カバレッジホール検出

コントローラは、AP から報告されたクライアントのシグナルの品質情報を基に、AP の送信電力を増やす必要があるかどうかを判断します。カバレッジホール検出（CHD）は単一のコントローラで実行されるため、RF グループ リーダーはこれらの計算に関与しません。コントローラは、特定の AP に関連付けられているクライアントの数と、

クライアントごとの信号対雑音比（SNR）を把握しています。クライアントの SNR がコントローラに設定されたしきい値を下回った場合、AP はクライアントを補うために自身の送信電力レベルを増やします。SNR のしきい値は、AP の送信電力とコントローラのカバレッジ プロファイル設定に基づいて設定されます。

CHD 設定は、[設定（Configuration）] > [無線設定（Radio Configuration）] > [RRM] に移動し、[6 GHz 帯域（6 GHz Band）]、[5 GHz 帯域（5 GHz Band）]、または [2.4 GHz 帯域（2.4 GHz Band）] タブを選択して確認できます。



ほとんどの展開ではデフォルト値が推奨されます。

モビリティ

ここでは、モビリティグループ設定に関するベストプラクティスについて説明します。

モビリティグループ接続

すべてのコントローラの管理インターフェイス間に IP 接続が存在することを確認してください。モビリティグループ内のコントローラが永続的にダウン（交換、テストなどで）している場合は、そのコントローラをすべてのピアのモビリティ設定から削除することをお勧めします。

シームレスで高速なローミング

モビリティグループ名は、高速ローミング情報（Cisco Centralized Key Management、802.11r、プロアクティブキーキャッシング（PKC）、または OKC）のための共通キャッシュを共有するコントローラを示す識別子として機能します。コントローラ間で高速ローミングが必要な場合は、コントローラ間で同じモビリティグループ名が共有されていることを確認することが重要です。

モビリティグループのサイズ

不必要に大きなモビリティグループを作成しないでください。モビリティグループには、クライアントが物理的にローミングできるエリアに AP を持つコントローラ（1 つの建物内に AP を持つすべてのコントローラなど）のみを含める必要があります。複数の建物が離れているシナリオがある場合は、それらを複数のモビリティグループに分割する必要があります。これにより、コントローラが、グループ内の、実際には相互にやり取りしない有効なクライアント、不正デバイス、および AP の大きなリストを保持する必要がなくなり、メモリと CPU を節約できます。C9800 ワイヤレスコントローラは、AireOS と同様に、単一のモビリティグループで最大 24 のメンバーをサポートします。

注： モビリティグループとモビリティドメインを混同しないでください。C9800 は、モビリティドメインまたはリストで最大 72 台のワイヤレスコントローラをサポートします。これは、複数のモビリティグループ間のモビリティに使用されます（同じモビリティグループ内でのみ使用可能であるため、高速ローミング「ではな

い」）。また、ゲストトンネリングのためのフォーリン アンカー ピアリングをセットアップするためにも使用されます。

コントローラ間のレイヤ 2 ローミングとレイヤ 3 ローミング

Catalyst 9800 では、SSID に関連付けられたクライアント VLAN が両方のコントローラで同じである場合に、コントローラ間レイヤ 2 ローミングが発生します。クライアントが新たなコントローラに join されたアクセス ポイントへアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

SSID に関連付けられたクライアント VLAN が各コントローラで異なる場合は、コントローラ間レイヤ 3 ローミングが発生します。レイヤ 3 ローミングは、コントローラがクライアントのローミングに関するモビリティメッセージを交換する点でレイヤ 2 ローミングと似ています。ただし、クライアントのデータベース エントリを新しいコントローラに移動するのではなく、元のコントローラのクライアント データベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングはワイヤレスクライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

Catalyst 9800 ワイヤレスコントローラでは、レイヤ 2 ローミングかレイヤ 3 ローミングかの決定は、クライアント VLAN にマッピングされているクライアントサブネットには依存しません。ローミングのタイプを決定する際に重要なのは VLAN のみです。これは、Catalyst 9800 では、クライアント VLAN ごとに L3 インターフェイスを設定する必要がないためです。コントローラ間レイヤ 2 ローミングが必要な場合、両方のワイヤレスコントローラで同じ IP サブネットが同じ VLAN に関連付けられるようにネットワークを設定することは、ユーザーの責任となります。

注： これは AireOS とは異なります。AireOS では、クライアント VLAN とそれに関連付けられたサブネットが両方のワイヤレスコントローラで同じである場合に、レイヤ 2 ローミングが発生します。

コントローラ間ローミングの必要性の削減

同じモビリティグループ内のコントローラ間で AP を分散させる場合は、同じ RF 空間内のすべてのアクセスポイントが単一のコントローラに属している状態の確保を試みてください。これにより、必要なコントローラ間ローミングの数が削減されます。「ソルトアンドペッパー」シナリオ（異なるコントローラに属する AP が同じ RF 空間をカバーする）はサポートされていますが、RF 空間ごとに単一のコントローラを使用する場合に比べて、CPU およびプロトコル交換の観点で、よりコストのかかるプロセスとなります。

リリース間コントローラローミング

シスコでは、異なる Cisco IOS XE ソフトウェアバージョンを実行しているコントローラ間でのローミングをサポートしていますが、一般的に、デバイス間での動作の一貫性を確保するために、同じモビリティグループ内のコントローラ間で同じバージョンを使用することをお勧めします。相互運用性をサポートするソフトウェアバージョンの詳細については、次のドキュメントを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html#pgfId-550562

シスコでは、Catalyst 9800 と AireOS ワイヤレスコントローラ間のリリース間コントローラローミング（IRCM）をサポートしています。これは、ブラウンフィールドおよび移行シナリオにおいてシームレスなモビリティを確保するために重要です。詳細については、『Cisco Catalyst 9800 Wireless Controller–AireOS IRCM Deployment Guide』を参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_c9800_wireless_controller-aireos_ircm_dg.html

AireOS WLC から C9800 への移行

AireOS 展開と新しい C9800 ワイヤレスネットワークの間での移行を設計する場合、考慮すべきベストプラクティスがいくつかあります。IRCM のガイドラインについては、「モビリティ」セクションで前述したとおりです。

シームレスなレイヤ 3 ローミング

C9800 と AireOS コントローラの間でのローミングはすべて、レイヤ 3 ローミングです。これは、各 WLC で SSID がどの VLAN にマッピングされていても、クライアントは常に最初に参加した WLC にアンカーリングされることを意味します。言い換えると、有線ネットワーク側の VLAN が両方の WLC で同じであっても、有線ネットワークへの接続点はローミングで変更されません。問題を回避するため、AireOS と C9800 の間で異なる VLAN ID を使用することをお勧めします。

移行設計フェーズで、ローミング用に共通の SSID を定義する際は、Catalyst 9800 と AireOS WLC で異なる VLAN ID およびサブネットを使用してください。

その結果、クライアントは、最初に Catalyst 9800 に参加するか AireOS に参加するかによって、異なる IP を取得します。クライアントは、最初に参加した VLAN/サブネット上の IP アドレスを常に保持するため、いずれの場合でもシームレスなローミングが保証されます。

これは、次の場合に（次の理由で）不可能であることがあります。

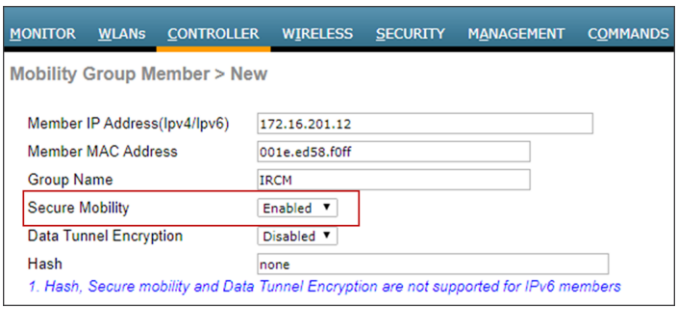
- お客様は、新しく追加された Catalyst 9800 に参加するクライアント用に別の VLAN/サブネットを追加するようなサブネット設計の変更を希望していません。これには、AAA とファイアウォールの設定の変更も含まれる場合があります。
- お客様は、パブリック IP サブネットを利用しているため、同じ SSID 上のクライアントに割り当てる別の余分なサブネットがありません。
- お客様は、ワイヤレスデバイスに静的 IP を使用しています。

Catalyst 9800 と AireOS の両方で同じ VLAN/サブネットを使用する必要がある場合は、次のリリースを使用することをお勧めします。

- Cisco IOS XE のコード：リリース 16.12.4a または 17.3.2 以降
- AireOS のコード：リリース 8.5.17x（2021 年 1 月に予定された 7 回目のメンテナンスリリース）またはリリース 8.10.142 以降

モビリティグループと Secure Mobility

C9800 ワイヤレスコントローラは、Secure Mobility プロトコルを使用して、モビリティピアへのセキュアなモビリティトンネルを構築します。セキュアモビリティは、CAPWAP をベースとしており、デフォルトでは DTLS を介してすべてのコントロールプレーン通信を暗号化します。C9800 と AireOS の間にトンネルをセットアップするには、適切な AireOS IRCM イメージが必要です。さらに、次の図のように、AireOS 側で Secure Mobility を設定する必要があります。



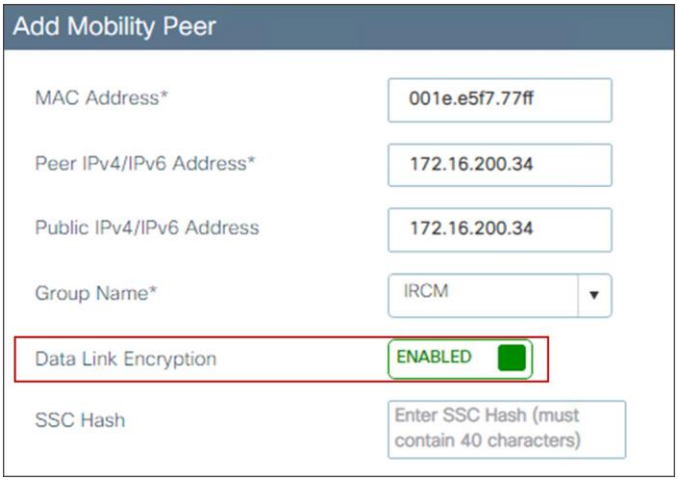
ハッシュは、C9800-CL とピアリングする場合にのみ必要です。その場合は、次のコマンドを使用してハッシュを取得する必要があります。

```
C9800#sh wireless management trustpoint
Trustpoint Name  : ewlc-tp1
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : 555c83c89d8fefab2d3601602117566b4e734e8e
[snip]
```

証明書ハッシュをコピーして、AireOS のモビリティピア設定に貼り付けます。

データリンク暗号化（コントローラ間のクライアント データ トラフィックの暗号化）はオプションであり、トンネルが信頼できないネットワーク上に構築される場合に推奨されます。これはデフォルトで無効になっており、有効にする場合は両側で設定する必要があります。AireOS では、次のように設定します。

また、C9800 では、次のように設定します。



2 つの AireOS コントローラまたは 2 つの C9800 コントローラの場合と同様に、シームレスなモビリティをサポートするためにモビリティグループを作成する場合は、グループ名が一致している必要があります。ゲストアンカーリング用のモビリティトンネルを構築する場合は、グループ名が同じである必要はありません。また、2 つのコントローラ間でローミングがない場合は、異なっている必要があります。C9800 は、ゲストアンカー上のローカル AP に対して、アンカーリングされた SSID をアドバタイズしません。そのため、フォーリンからアンカーにはローミングできません。

RF グループ

RF グループは、グローバルに最適化された方法で無線ネットワークごとに RRM の実行を調整するワイヤレスコントローラの論理的な集合です。2.4 GHz、5 GHz、および 6 GHz ネットワークには個別の RF グループが存在します。複数の WLC を単一の RF グループにまとめるには、同じ RF グループ名を設定する必要があります。この場合、RF リーダーが選出され、RRM アルゴリズムが単一の WLC の機能を超えて拡張されます。

注： RF グループ名は必ず変更し、デフォルトのままにしないでください。これは、将来のバージョンでは必須になる予定です。

共通の RF ドメインを管理する AireOS および IOS XE ベースのワイヤレスコントローラがある移行シナリオでは、次のガイドラインに従ってください。

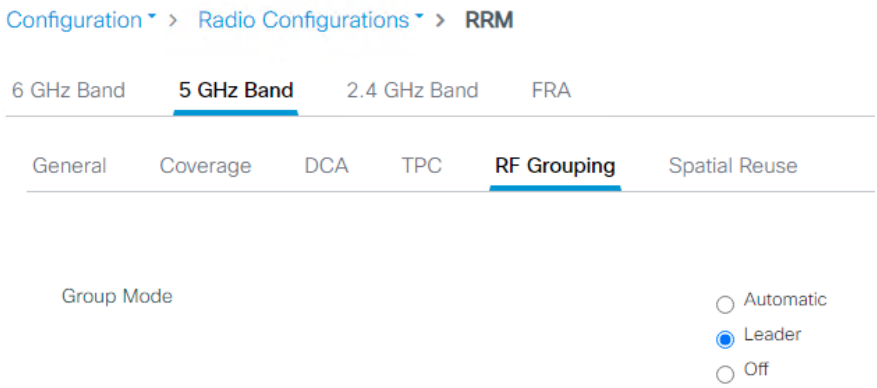
- 単一 RF グループを形成する場合は、デフォルトの自動選択に依存せずに、RF リーダーを静的に設定することをお勧めします。これは、最も能力の高いコントローラをリーダーに静的に設定する必要があることを意味します。優先順位順のリストを次に示します。

表 8. RF グループの拡張性

グループリーダーの順序	最大 AP 数	最大 AP/RF グループ数
3504	150	500
C9800-L	250	500
C9800-CL（小規模）	1000	2000
5520	1500	3000
C9800-40 / CW9800M	2000	4000
C9800-CL（中規模）	3000	6000

グループリーダーの順序	最大 AP 数	最大 AP/RF グループ数
8540	6000	6000
C9800-CL（大規模）	6000	12000
C9800-80 / CW9800H1 / CW9800H2	6000	12000

- 既存の 5520 展開があり、C9800-40 を追加する場合は、IOS XE ベースのコントローラをリーダーにする必要があります。これは、GUI で C9800-40 を RF リーダーとして設定することにより実現できます。[設定（Configuration）] > [無線設定（Radio Configuration）] > [RRM] に移動して、各バンド（6 GHz、5 GHz、および 2.4 GHz）を選択し、[RF グループ（RF Grouping）] に移動して [リーダー（Leader）] をクリックしてから適用します。



- AP およびクライアントの数がプラットフォームの最大スケール数に近い、非常に高密度な展開では、ユーザーは、各 WLC を独自の RF グループとして設定することを検討してください。これの利点は、新しい機能をより有効に活用できることと、Catalyst 9800 にのみ展開される可能性が非常に高い、新しい Catalyst AP をより適切に管理できることです。また、各ワイヤレスコントローラの負荷を軽減するためにも役立ちます。

注： 2 つの個別の RF グループを設定する場合は、AireOS WLC 上の AP が C9800 で不正 AP として検知されないように、2 つの WLC を同じモビリティグループに設定してください。

AireOS WLC と C9800 の間での AP の移動

AP を AireOS ベースのワイヤレスコントローラから Cisco IOS XE ベースのワイヤレスコントローラに移動する場合、注意が必要な考慮事項がいくつかあります。

AP が、異なる OS を搭載したコントローラに初めて参加すると、イメージをダウンロードしてリロードする必要があるため、ダウンタイムが発生することを考慮してください。初回参加後は、AP のメモリに両方のイメージ（アクティブイメージとバックアップイメージ）が保持されるため、追加のダウンロードなしで、2 つのコントローラ間で AP を移動したり戻したりすることができます。

特定の AP グループおよび特定の RF プロファイルに割り当てられている AP を AireOS から C9800 に移動すると、その情報が失われます。必ず、C9800 が正しいプロファイル、タグ、および AP マッピングを使用して設定されていることを確認してください。これにより、AP が参加したときに適切な設定が取得されます。

AP を AireOS ベースのアプライアンスから C9800-CL に移動する場合は、特に注意してください。アプライアンスでは、AP は、製造元でインストールされる証明書（MIC）を使用してコントローラに安全に参加します。C9800-CL では、VM であるために MIC がなく、自己署名証明書（SSC）が使用されます。AP を C9800-CL に参加させるには、次の 2 つの選択肢があります。

1. AP を移動する前に、AireOS アプライアンスで SSC 検証を無効にします。

   これにより、AP が任意の仮想 WLC に確実に参加できるようになります。

2. AP を移動する前に、両方のコントローラでトークンを設定します。

```
config certificate ssc auth-token <token> - on AireOS WLC
wireless management certificate ssc auth-token 0 <token> - on the C9800
```

   トークンはただの文字列であり、両方のワイヤレスコントローラで一致している必要があります。

注： AP が Cisco AireOS コントローラから Cisco Catalyst 9800 コントローラに移動すると、802.1X のログイン情報と設定が失われます。それらを復元するには、AP が新しい Catalyst 9800 コントローラに参加する必要があります。これにより、スイッチポートでの認証に必要なログイン情報と設定がプッシュされます。スイッチポートで 802.1X 認証を一時的に無効にして、AP が接続して設定を受信できるようにするか、MAC 認証バイパス（MAB）を使用して、ステージング用のネットワークアクセスを AP に提供することができます。ステージング後に、AP をリロードするか、スイッチで 802.1X 認証を再開して、セットアップを完了させてください。

FlexConnect のベストプラクティス

FlexConnect 展開は、分散型企業のリモートサイトまたはブランチ向けに最適化されています。いくつかの重要な考慮事項を次に示します。

- FlexConnect は、ブランチのハードウェアフットプリントの削減を支援し、設備投資と運用コストを削減し、ローカルコントローラを不要にして消費電力を削減します。
- ワイヤレスコントローラ機能はデータセンターサイトに統合され、一元化された容易な IT サポートが実現されます。FlexConnect は、複数のロケーションに対して「クッキーの型抜き」のように定型的に設定できる場合に最適です。これは、すべてを一元的に管理できるためです。
- FlexConnect は、WAN 全体で動作するように設計されており、WAN 障害に対する存続可能性を提供し、中央サイトとリモートサイトの間での WAN の使用率を減少させます。

- FlexConnect AP の場合、コントロールプレーンは常に中央 WLC で集中管理されますが、データプレーンは柔軟です。つまり、クライアントトラフィックは、AP でローカルにスイッチングすることも、コントローラで集中的にスイッチングすることもできます。

分散ブランチオフィスを展開する場合は、最小 WAN 帯域幅、最大ラウンドトリップ時間（RTT）、最小 MTU、フラグメンテーションなど、特定の構成要件を考慮する必要があります。これらのガイドラインは、次のガイドにまとめられています。

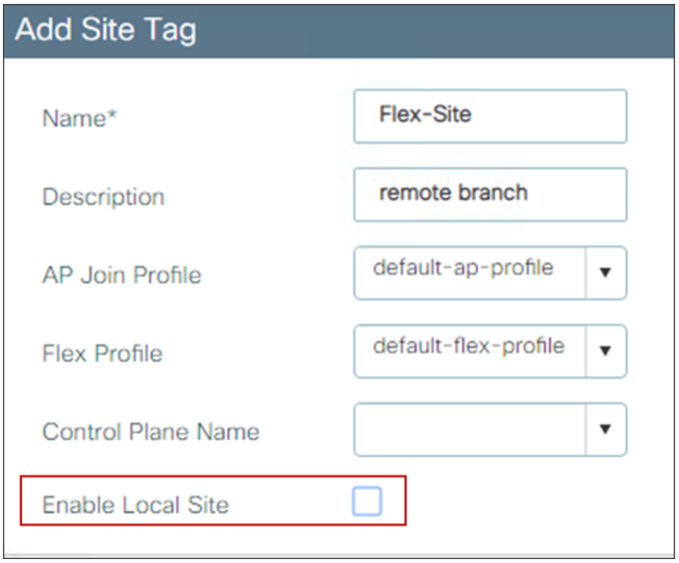
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-8/b_flex_connect_catalyst_wirelss_branch_controller_dg.html#id_93580

注： AP と WLC の間の CAPWAP 制御トラフィックが WAN を通過するため、有線インフラストラクチャでサービス品質（QoS）を設定して、UDP ポート 5246 で CAPWAP 制御チャネルのトラフィックを優先させることをお勧めします。

C9800 での FlexConnect モード

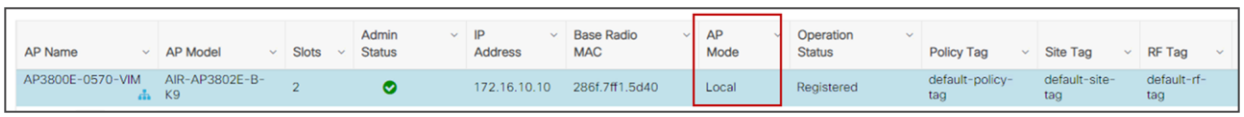
C9800 では、AP を FlexConnect モードで動作するように設定する場合、その AP に割り当てたサイトタグを適切に設定する必要があります。つまり、AireOS で行っていたように AP 自体でモードを FlexConnect に設定する必要はなく、リモートサイトとして設定されたサイトタグに AP を割り当てるだけで、C9800 が変換を自動的に実行します。AP は再起動「しません」が、単に CAPWAP が再起動され、30 秒未満で再び参加します。

次に、FlexConnect 用に設定されたサイトタグの例を示します。



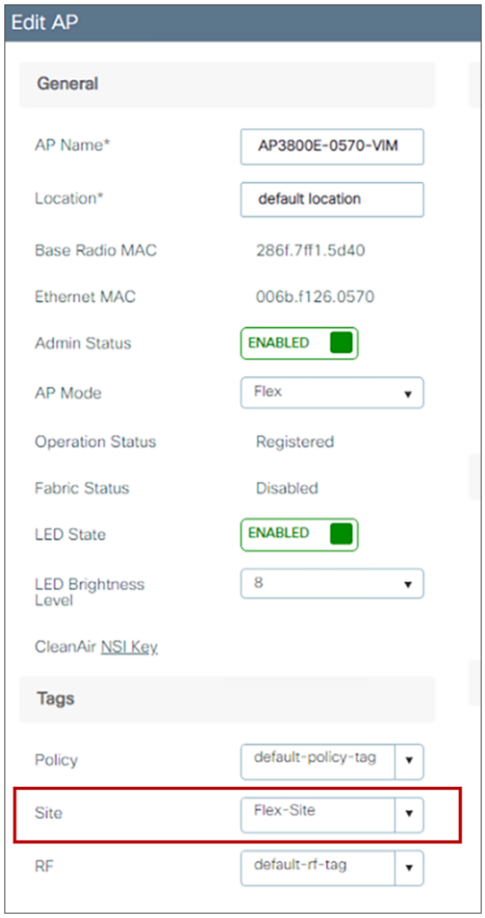
上のスクリーンショットで強調表示されているように、[ローカルサイトの有効化（Enable Local Site）] をオフ（デフォルト）にする必要があります。これにより、AP の Flex モードへの変換がトリガーされるようになります。また、デフォルトの Flex プロファイルも選択されることに注意してください。ここで、すべての Flex 設定を指定します。ブランチごとに設定が異なる場合は、デフォルトまたはカスタムの設定を使用できます。

次の例を参照してください。AP は最初、デフォルトサイトタグで参加しており、このタグはデフォルトでローカルサイトになっているため、予想どおり、AP がローカルモードになっていることがわかります。



AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Policy Tag	Site Tag	RF Tag
AP3800E-0570-VIM	AIR-AP3802E-B-K9	2	✔	172.16.10.10	286f.7ff1.5d40	Local	Registered	default-policy-tag	default-site-tag	default-rf-tag

ここで、作成したサイトタグ（Flex サイトタグ）に AP を割り当てます。これは、AP 自体でタグ割り当てを編集することにより実行できます。



AP が切断され、予想どおり、Flex モードに戻ります。

FlexConnect を使用する場合は、「Flex プロファイル」と呼ばれる専用の設定要素があります。これには、リモートサイト固有のパラメータが含まれています。たとえば、マスターおよびスレーブの AP リスト、AP が認証サーバーとして機能する場合に使用できる EAP プロファイル、ローカル RADIUS サーバー情報、VLAN-ACL のマッピングなどです。

注： FlexConnect モードの設定時に、VLAN がポリシープロファイルで設定されている場合は、Flex プロファイルでも設定する必要があります。これが行われていないと、WLAN がブロードキャストされません。

FlexConnect に関する推奨事項/注意事項は、次のとおりです。

- デフォルトの Flex プロファイルは、[DHCP 必須（DHCP Required）]（このオプションの意味の詳細については、「[DHCP 必須（DHCP Required）] オプション」のセクションを参照）をサポートしていません。
- シスコでは、デフォルト以外の Flex プロファイルを常に設定することをお勧めします。デフォルト以外の Flex プロファイルを使用することで、OKC、高速移行などのキーキャッシング機能が有効になります。

ローカル スイッチング

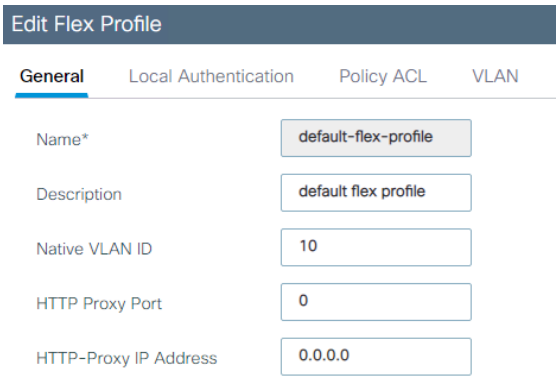
WLAN でローカルスイッチングを有効にすると、WAN 障害に対する復元力が提供されます。また、WAN を通過するデータの量が減少するため、WAN 帯域幅の使用量が削減されます。ローカルスイッチングは、リソースがブランチサイトにローカルに存在し、データトラフィックを WAN リンク経由でコントローラに送り返す必要がない展開で役立ちます。ローカルスイッチングに関する推奨事項は、次のとおりです。

- FlexConnect AP を、スイッチの 802.1Q トランクポートに接続します。
- AP でネイティブ VLAN を使用して接続する場合、レイヤ 2 のネイティブ VLAN 設定は、AP の設定と一致する必要があります。
- ネイティブ VLAN が、同じロケーションおよびサイトタグ内のすべての AP で同じであることを確認してください。

ローカルスイッチングモードでは、AP が接続モード（WLC に登録されている）かスタンドアロンモード（AP が WLC への接続を失っている）かによって、一部の機能が使用できなくなります。Flex マトリックスを参照して、機能が使用可能かどうかを確認してください。

https://www.cisco.com/c/en/us/td/docs/wireless/access_point/feature-matrix/ap-feature-matrix.html

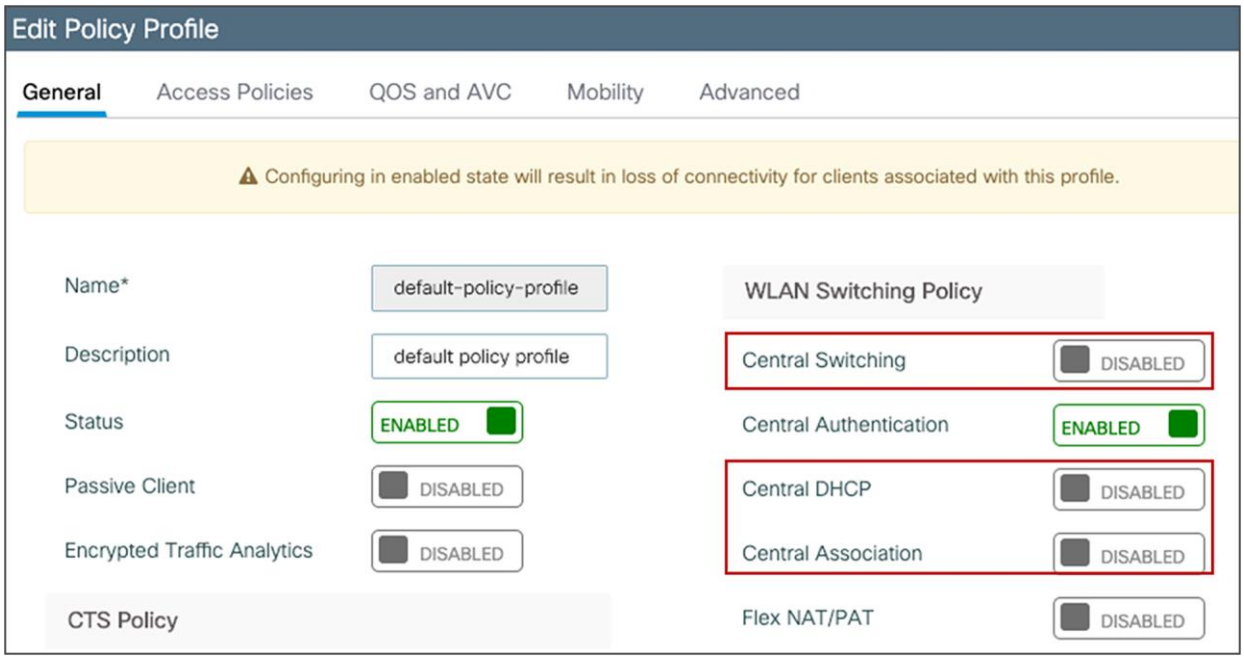
C9800 では、ネイティブ VLAN は、その Flex サイトに関する設定であるため、Flex プロファイルで定義されます。次の例では、ネイティブ VLAN は VLAN 10 です。



また、スイッチでの設定と一致しています。

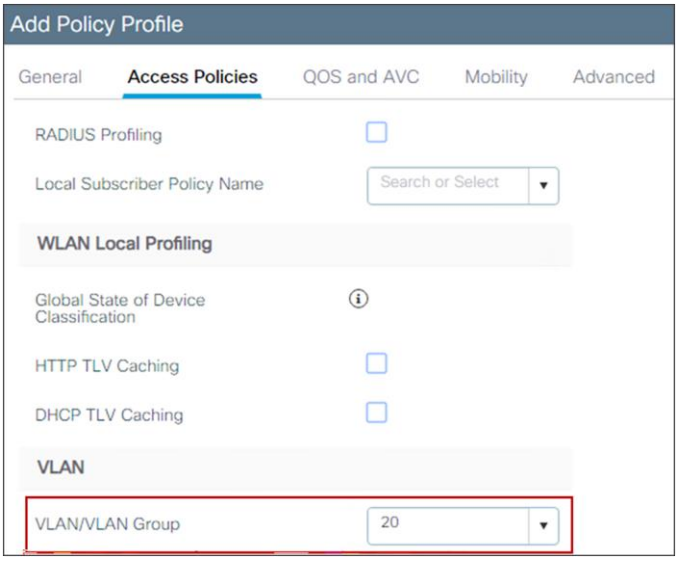
```
interface TenGigabitEthernet1/0/3
 description to_Flex_AP
 switchport trunk native vlan 10
 switchport mode trunk
 spanning-tree portfast trunk
```

ローカルスイッチング属性と、クライアントが使用する VLAN は、ポリシープロファイルで定義されます。これは、それらが WLAN に関連付けられたポリシーであるためです。ローカルにスイッチングされる WLAN の場合は、ポリシープロファイルで、中央スイッチングと中央関連付けを無効にします。DHCP サーバーをローカルサイトで使用できる場合は、中央 DHCP も無効にします。



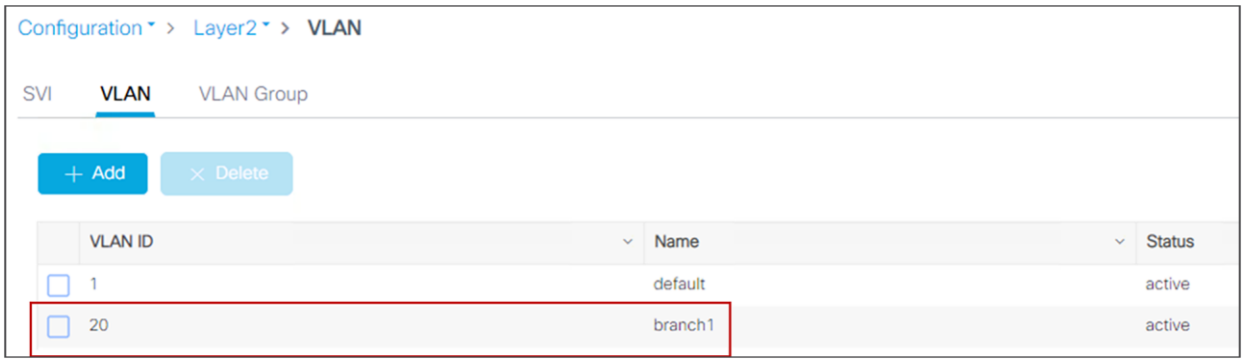
ローカルにスイッチングされるトラフィック用の AP 上の VLAN は、次の 2 つの方法で設定できます。

- VLAN ID（番号）を使用：ポリシープロファイルに VLAN 番号を直接入力します。ローカルにスイッチングされるトラフィック専用であるため、コントローラ自体でこの VLAN を定義する必要はありません。この VLAN は AP にプッシュされます。

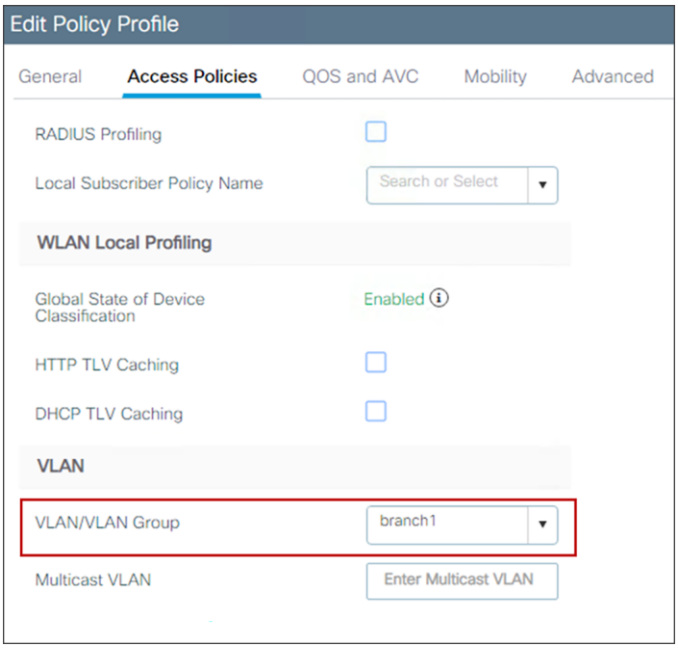


- VLAN 名を使用：この場合は、最初に WLC で VLAN 名をグローバルに作成します。その後、特定のサイトでその VLAN 名に対して使用する VLAN ID を AP に指示する必要があります。VLAN 名と VLAN 番号のマッピングは、Flex プロファイルで設定する必要があります。これにより、正しい VLAN ID が AP にプッシュされます。

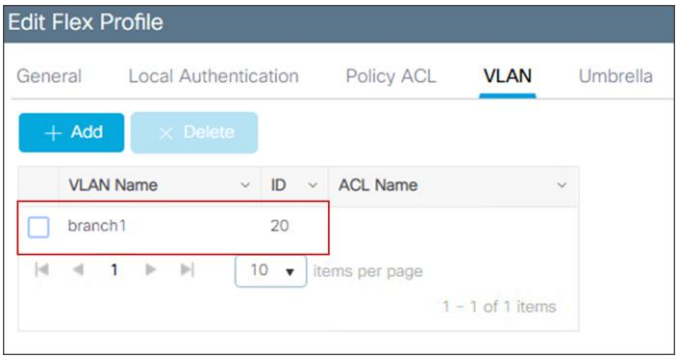
  次の例を参照してください。VLAN「branch1」は、まず、コントローラでレイヤ 2 VLAN として定義されます。



その後に、ポリシープロファイルで、その VLAN 名を選択します。



Flex プロファイルの [VLAN] タブで、同じ VLAN 名が目的の VLAN ID にマッピングされています（この例では、20 という同じ番号になっている）。



複数のブランチがあり、各ブランチで異なる VLAN ID（番号）を同じ VLAN 名とともに使用する場合は、各ブランチに割り当てられるカスタム Flex プロファイルで、目的の VLAN ID へのマッピングを設定することによって実現できます。

注： 最大 16 のローカルにスイッチングされる VLAN を Flex プロファイルにマッピングできます。

注：　ローカルにスイッチングされる VLAN が AAA サーバー経由で返される場合に AAA VLAN オーバーライドも使用するためにも、VLAN 名から VLAN ID へのマッピングを Flex プロファイルで設定する必要があります。

FlexConnect サイトタグ

サイトタグは、Flex 用に設定されている場合（つまりローカルサイトとしては無効になっている場合）、AireOS FlexGroup と同等のものになります。C9800 については、次の点に注意することが重要です。

- シームレスでセキュアな高速ローミングが必要である場合でも、Flex サイトタグごとに AP の数は 100 に制限されています（AireOS と同じ）。リリース 17.8.1 以降、この制限は 300 の AP と 3000 のクライアントに増加しています。これには、デフォルトでは有効になっていない「ペアワイズマスターキー（PMK）伝達」機能を活用します。設定ガイドを参照してください。
- クライアントのペアマスターキー（PMK）は、同じ Flex サイトタグに属する AP 間で配布されます。2 つの Flex サイトタグ間をローミングする場合、クライアントは、完全な再認証を強制されます（AireOS で、Flex グループ間でローミングする場合と同じ）。
- Flex サイトタグにおける AP に関するすべての設定は、Flex プロファイルレベルで行われ、サイトタグに割り当てられます。

設計の観点から、FlexConnect サイトタグを扱う際に考慮する必要があるベストプラクティスは、次のとおりです。

- FlexConnect では、サイトタグによって、セキュアな高速ローミングがサポートされる境界が定義されます。そのため、クライアントがローミングする可能性が高いローミングドメインと一致するサイトタグを割り当てる必要があります。これは、2 つのフロア間で RF リークが発生している場合、両方のフロアの AP を同じサイトタグの一部として設定することが推奨されることを意味します。当然のことながら、前述した 100 の AP の制限には注意してください。
- FlexConnect を使用する場合は、常にカスタムサイトタグを使用する必要があります。デフォルトサイトタグでは、セキュアな高速ローミングはサポートされません。
- FlexConnect のロケーションごとに少なくとも 1 つのカスタムサイトタグを設定する必要があります（100/300 の AP の制限を超える予定がある場合は、複数のタグが必要になる可能性がある）。また、複数の Flex ロケーションで同じサイトタグ（デフォルトサイトタグを含む）を再使用しないことも重要です。
- リリース 17.3.3 以降、C9800 では、異なるサイトタグ間で IP アドレスが重複するクライアントがサポートされています。C9800 では、サイトタグと IP アドレスの組み合わせをクライアントの一意の ID（「ゾーン ID」と呼ばれる）として使用するため、各サイトのサイトタグは一意である必要があります。

最大 300 の AP と 3000 のクライアントをサポートする FlexConnect ハイスケールモードを利用する場合は、次の点に注意してください。

- シームレスなローミングをサポートするには、単一の共通レイヤ 2 クライアント VLAN も必要になります。これは、スパニングツリーの問題や大きな ARP テーブルが発生する可能性があるため、注意が必要です。マルチレイヤスイッチングの設計が必要になる場合があります。
- この規模に近づいている場合は、専用 WLC を検討してください。

注：　クライアントの IP アドレス重複は、ローカルスイッチングでの Flex 展開で、ローカル DHCP サーバーを使用する場合にのみ利用できます。他のすべての展開（ローカルモード、中央スイッチング、中央 DHCP など）では、重複する IP は引き続きサポートされません。

FlexConnect プロファイルとサイトタグの概念を活用する機能がいくつかあります。

- 音声展開向けの 802.11r 高速移行（FT）、Cisco Centralized Key Management、または OKC 高速ローミング
- ローカルバックアップ RADIUS サーバー
- ローカル EAP
- WLAN から VLAN へのマッピングおよび VLAN から ACL へのマッピング
- Cisco Umbrella®
- Cisco TrustSec®

Split Tunneling

ほとんどのリソースが中央サイトに配置されており、クライアントのデータは中央でスイッチングされる必要がある一方で、リモートオフィスにローカルに存在する特定のデバイスについては WAN 帯域幅の使用率を低下させるためにローカルでスイッチングする必要があるシナリオでは、スプリットトンネリング機能を設定します。これの典型的なユースケースは OEAP テレワーカーのセットアップです。この場合、企業の SSID 上のクライアントが、CAPWAP 経由でパケットを送信して WAN 帯域幅を消費することなく、ローカルネットワーク上のデバイス（プリンタ、リモート LAN ポート上の有線マシン、またはパーソナル SSID 上のワイヤレスデバイス）と直接通信できます。中央 DHCP およびスプリットトンネリングでは、AP のルーティング機能が使用されます。

C9800 でのスプリットトンネリングは、ポリシープロファイルで設定されます。設定ガイドの参考資料（https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m-sniffer-cg.html?bookSearch=true#spilt-tunneling-for-flex）を参照してください。

スプリットトンネリングを展開する場合には、次の制約事項が適用されます。

- スプリットトンネリングは、リリース 17.3 以降、802.11ac Wave 2 および 802.11ax の AP でサポートされています。
- 静的 IP クライアントは、中央 DHCP およびローカルスプリット WLAN ではサポートされていません。そのため、ポリシープロファイルで [DHCP 必須（DHCP Required）] を設定する必要があります。

VLAN ベースの中央スイッチング

AAA サーバーから返される VLAN と、ブランチサイトに存在する VLAN に基づいて、データトラフィックをローカルにスイッチングするか中央でスイッチングするかを動的に決定する必要があるシナリオでは、VLAN ベースの中央スイッチングを使用します。AAA サーバーから返された VLAN が、ブランチサイトに存在しない場合、つまり Flex プロファイルを介して AP にマッピングされていない場合、トラフィックは中央でスイッチングされます。C9800 では、VLAN ベースの中央スイッチングはポリシープロファイルレベルで設定されます。

Quality Of Service（ QoS ）

ここでは、Catalyst 9800 ワイヤレス QoS の概要と、いくつかの重要なベストプラクティスについて説明します。

Catalyst 9800 ワイヤレスコントローラのワイヤレス QoS

ワイヤレス QoS とは、ワイヤレスメディアにおいて、選択されたネットワークトラフィックにより良いサービスを提供するネットワークの機能です。QoS の主要な目的は、専用の帯域幅の確保、ジッターおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

Catalyst ワイヤレスで QoS を考慮する場合、次の重要な点を知っておく必要があります。

- 他のすべての Cisco IOS XE デバイスと同様に、Catalyst 9800 の QoS 機能は、**モジュラ QoS コマンド ライン インターフェイス（MQC）**を使用して有効にされます。MQC は、トラフィックポリシーを作成し、それらのポリシーをターゲット（クラスマップ、ポリシーマップなど）にアタッチすることを可能にするコマンド ライン インターフェイス（CLI）構造です。
- 「**ターゲット**」とは、ポリシーが適用されるエンティティです。Catalyst 9800 は、**SSID** と **クライアント**の 2 つのターゲットをサポートしています。
- Catalyst 9800 のワイヤレス QoS ポリシーに関しては、次のガイドラインを考慮する必要があります。
  - ワイヤレスターゲットには、マーキングおよびポリシングポリシーのみを設定できます。
  - 方向ごとに、ターゲットあたり 1 つのポリシーがサポートされています。
  - 1 つのマーキングアクション（set DSCP）のみがサポートされています。
  - クラスごとに 1 つの set アクションのみがサポートされています。
- SSID およびクライアントに対するワイヤレス QoS ポリシーは、**アップストリーム**方向および**ダウンストリーム**方向で適用できます。**有線**ソースからワイヤレスターゲットへのトラフィックフローは、ダウンストリーム（または**出力**）トラフィックと呼ばれます。ワイヤレスソースから有線ターゲットへのトラフィックフローは、アップストリーム（または**入力**）トラフィックと呼ばれます。
- **SSID ポリシー**：入力および出力方向で SSID の QoS ポリシーを作成できます。設定されていない場合は、SSID ポリシーは適用されません。このポリシーは、SSID ごと、AP ごとに適用されます。
- **クライアントポリシー**：クライアントポリシーは、入力および出力方向に適用できます。AAA オーバーライドもサポートされます。
- ワイヤレス QoS ポリシーは、**ポリシープロファイル**で設定されます。

メタル QoS プロファイル

メタル QoS プロファイルの主な目的は、ネットワークで許可される最大 DSCP 値を制限することです。Catalyst 9800 は、4 つの異なる QoS レベル/プロファイルをサポートしています。

- Platinum/音声：無線を介して転送される音声のために高品質のサービスを保証します。
- Gold/ビデオ：高品質のビデオアプリケーションをサポートします。
- Silver/ベストエフォート：クライアント向けに通常の帯域幅をサポートします。これがデフォルト設定です。
- Bronze/バックグラウンド：ゲストサービス用の最も低い帯域幅を提供します。

一般的に、メタル QoS プロファイルは、AireOS の場合と同じように機能します。ただし、Catalyst 9800 には、考慮が必要ないくつかの違いがあります。

- メタルプロファイルは、出力と入力の両方で個別に適用できます。
- GUI では、SSID 単位でのみ メタル QoS を設定できます。CLI では、クライアントターゲットで設定することもできます。
- Catalyst 9800 では、メタル QoS プロファイルは、ユーザーが設定できません。

- Catalyst 9800 では、一致しないトラフィックはデフォルトクラスに入り、ベストエフォートとしてマークされます。
- ユーザー単位および SSID 単位の帯域幅コントラクトは、MQC QoS ポリシーを使用して設定できます。

ワイヤレス QoS に関する推奨事項

「DSCP Trust」は、Catalyst 9800 でサポートされている QoS モデルです。これは、AP および WLC 内でワイヤレストラフィックに適用されるすべての QoS 処理（キューイングおよびポリシー）が、802.11 ユーザー優先順位（UP）ではなく、クライアント DSCP 値に基づくことを意味します。

たとえば、ダウンストリーム方向（有線からワイヤレスへのトラフィック）での中央スイッチング SSID の場合、AP は、受信した CAPWAP ヘッダーから DSCP 値を取得し、それを内部 QoS 処理およびマッピング（受信した DSCP > UP > アクセスカテゴリ）に使用します。DSCP 値は、RFC 8325 に従い、表 9 のデータを使用してワイヤレスクライアントへのフレーム内の UP 値にマッピングされます。

表 9. QoS サービスクラス

IETF DiffServ サービスクラス	DSCP	802.11 ユーザー優先順位（UP）	801.11 アクセスカテゴリ
ネットワーク制御	CS6（CS7）	0	AC_BE
IP テレフォニー	EF（46）	6	AC_VO
VOICE-ADMIT	VA（44）	6	AC_VO
シグナリング	CS5（40）	5	AC_VI
マルチメディア会議	AF4x	4	AV_VI
リアルタイム インタラクティブ	CS4（32）	5	AC_VI
マルチメディア ストリーミング	AF3x	4	AC_VI
ブロードキャストビデオ	CS3（24）	4	AC_VI
低遅延データ（トランザクション）	AF2x	3	AC_BE
OAM	CS2（16）	0	AC_BE
高スループットデータ（バルクデータ）	AF1x	0	AC_BE
ベスト エフォート	DF	0	AC_BE
優先順位の低いデータ（スカベンジャー）	CS1（8）	1	AC_BK
残り	残り	0	AC_BE

注： テーブル 9 のエントリにマッピングされていない DSCP 値の場合、Catalyst 9800 は UP = 0 を使用するため、トラフィックはベストエフォートとして送信されます。

アップストリーム方向では、内部 DSCP クライアント値を外部 CAPWAP ヘッダーにマッピングするように AP を設定することをお勧めします。これは、AP 参加プロファイルで次のコマンドを使用して実行されます。

```
ap profile <name>
    qos-map trust-dscp-upstream
```

設定されていない場合、AP は、UP 値を使用し、それを表 9 に記載されている DSCP 値にマッピングします。リリース 17.4 以降では、`qos-map trust-dscp-upstream` がデフォルト設定であるため、クライアントの DSCP はデフォルトでエンドツーエンドで維持されます。

QoS に関する設定の詳細なガイドについては、次の設定ガイドを参照してください：
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html。

以下に、その他のいくつかの重要な考慮事項と推奨事項を示します。

- SSID レベルのポリシー：AP 単位で、その SSID 上のすべてのクライアントの集約トラフィックに適用されます。
- クライアントレベルのポリシー：これはクライアント単位のポリシーです。メタルポリシー（Platinum、Gold、Silver、Bronze）は、WebUI ではクライアント単位で設定できませんが、CLI では設定できます。
- SSID ポリシーとクライアントポリシーの両方が適用される場合は、最初にクライアントポリシーが適用され、次に SSID ポリシーが適用されます。
- QoS ポリシーの AAA オーバーライドは、SSID 単位ではなく、クライアント単位で利用できます。これは、ローカルモードと FlexConnect モードの AP でサポートされています。RADIUS サーバーから、ポリシー名を cisco av-pair として返す必要があります。
- cisco-av-pair = ip:sub-qos-policy-in=MyPolicy
- cisco-av-pair = ip:sub-qos-policy-out=MyPolicy
- QoS ポリシーは、AutoQoS を介して適用することもできます。これは、事前定義された一連のプロファイルであり、お客様は、これを変更してさまざまなトラフィックフローに優先順位を付けることができます。さまざまな AutoQoS プロファイルとその機能については、次の設定ガイドを参照してください：
  https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_wireless_autoqos_cg_vewlc.html。
- 音声 SSID の場合は、「Fastlane」AutoQoS プロファイル（音声プロファイルではなく）を使用することをお勧めします。Fastlane は、次の設定をトリガーします。
  - クライアント QoS ポリシーを Platinum に設定します。
  - [無線設定（Radio Configuration）] > [パラメータ（Parameters）] > [5 および 2.4 GHz 帯域幅（5 and 2.4 GHz bands）] で EDCA パラメータを Fastlane に設定します。
  - Catalyst 9800 の出力優先順位キューイングは、AutoQos-4.0-wlan-Port-Output-Policy サービスポリシーを適用することで、音声および CAPWAP トラフィックを優先するように設定されています。
  - EDCA 設定を確認するには、AP の CLI で次のコマンドを使用します。

    ```
    sh controllers dot11Radio 1 | begin EDCA
    ```
- ゲスト SSID の場合は、メタル QoS ポリシーを Bronze に設定することをお勧めします。
- EDCA 設定については、これらの設定は、SSID ごとではなく、無線ごとのグローバルであることに注意してください。すべてのネットワークに適用される単一の推奨値はないため、さまざまな値をテストすることが

重要です。音声トラフィックとビデオトラフィックがあるネットワークの場合は、EDCA を「optimized-video-voice」に設定することをお勧めします。

- AAA オーバーライドをともなう QoS 双方向レート制限（BDRL）ポリシーは、ローカルモードと FlexConnect モードの両方でサポートされています。詳細については、『QoS BDRL with AAA override on Catalyst 9800 Series Wireless Controllers』ガイドを参照してください：http://cs.co/BDRL-QoS-example

Catalyst 9800 での QoS 設定の確認

設定済みの QoS ポリシーを確認するために使用するメインコマンドは、次のとおりです。

```
C9800#sh policy-map interface wireless <ssid/client> profile-name <WLAN> radio type <2.4/5GHz> ap name <name> input/output
```

クライアントポリシーを確認するには、次のコマンドを使用します。

```
C9800#show wireless client mac <> service-policy input/output
```

AP で EDCA パラメータを確認するには、次のコマンドを使用します。

```
AP#sh controllers dot11Radio 1 | begin EDCA
```

注： AireOS と同様に、QoS ポリシーは、FlexConnect ローカルスイッチング SSID の場合は AP で適用され、中央でスイッチングされるトラフィックの場合はコントローラで適用されます。アップストリーム方向とダウンストリーム方向で同じです。

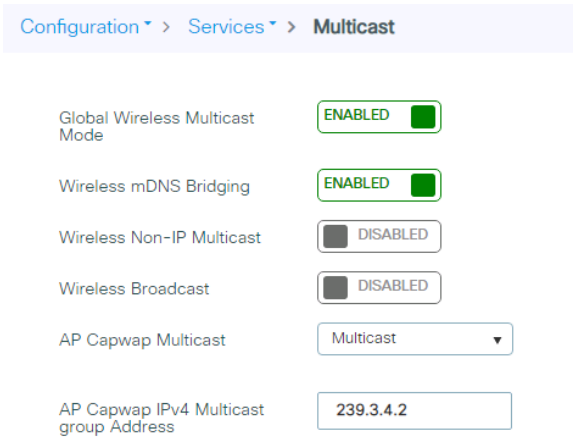
マルチキャスト

ここでは、ワイヤレスネットワーク上でマルチキャスト アプリケーションを有効にするためのベストプラクティスについて説明します。

マルチキャスト転送モード

基盤となるスイッチング インフラストラクチャがマルチキャストをサポートしている場合は、マルチキャスト アプリケーションの帯域幅使用率を抑えてパフォーマンスを最適化するために、マルチキャスト転送モードを使用してください。多数の IPV6 クライアントが存在するネットワーク、マルチキャストによるビデオストリーミングを行うネットワーク、および mDNS プロキシなしで Bonjour を利用するネットワークでは、マルチキャストモードを使用すると大きなメリットがあります。AP が WLC の管理インターフェイスで使用されているサブネットとは異なるサブネット上にあり、AP マルチキャストモードが有効になっている場合、ネットワーク インフラストラクチャは、管理インターフェイスサブネットとすべての AP サブネットの間でマルチキャストルーティングを提供する必要があります。そうでない場合、すべてのマルチキャストトラフィックが失われます。

WLC Web UI でマルチキャスト - マルチキャスト動作を設定するには、[設定（Configuration）] > [サービス（Services）] > [マルチキャスト（Multicast）] に移動します。



CLI でコントローラのマルチキャストモードを確認するには、次のコマンドを使用します。

```
C9800#sh wireless multicast
Multicast                                   : Enabled
AP Capwap Multicast                         : Multicast
AP Capwap iPv4 Multicast group Address      : 239.3.4.2
AP Capwap iPv6 Multicast group Address      : FF08::3:4:2
Wireless Broadcast                          : Disabled
Wireless Multicast non-ip-mcast             : Disabled
```

AP CAPWAP IPv6 マルチキャスト グループ アドレスは、IPv6 アドレスが設定された AP がある場合にのみ必要です。すべてのアクセスポイントが IPv4 アドレス上にある場合は、IPv4 マルチキャスト CAPWAP オーバーレイによって、クライアントの IPv4 と IPv6 の両方のマルチキャストトラフィックを伝送できるため、IPv6 マルチキャストアドレスは必要ありません。

リリース 17.2 以降では、次の CLI コマンドを使用して、AP の CAPWAP マルチキャストトンネルのステータスを確認できます。

```
C9800#sh ap multicast mom
AP Name     MOM-IP TYPE           MOM-STATUS
AP1                   iPv4                            UP
AP2                   iPv4                            UP
```

「MOM」は、マルチキャスト オーバー マルチキャストを表します。

マルチキャスト転送モードが推奨設定です。ユニキャスト転送は、小規模な展開や、ネットワーク インフラストラクチャでマルチキャストルーティングのサポートが不可能な場合にのみ使用してください。ユニキャスト転送は、C9800-80、C9800-40、および C9800-CL 中規模/大規模テンプレート プラットフォームではサポートされていません。

CAPWAP のマルチキャストアドレス

マルチキャストアドレスは、コントローラが、AP にトラフィックを転送するために使用します。マルチキャストアドレスが、他のプロトコルによってネットワーク上で使用されている別のアドレスと一致していないことを確認して

ください。たとえば、224.0.0.251 を使用すると、一部のサードパーティ製アプリケーションで使用されている mDNS が動作しなくなります。

シスコでは、アドレスをプライベート範囲（239.0.0.0 ～ 239.255.255.255）内に設定することをお勧めします（ただし、239.0.0.x および 239.128.0.x はレイヤ 2 フラッディングの原因となるため、これらの範囲は含まれない）。また、マルチキャストパケットの重複を避けるために、マルチキャスト IP アドレスが各 WLC で異なる値に設定されていることを確認してください。

ネイティブ iPv6 ワイヤレス インフラストラクチャ（iPv6 アドレスで設定された AP）を使用している場合、または IPv4 と IPv6 が混在している場合は、マルチキャスト グループ アドレスも IPv6 アドレスで設定する必要があります。

IGMP スヌーピングと MLD スヌーピング

Internet Group Management Protocol（IGMP）スヌーピングおよびマルチキャストリスナー検出（MLD）スヌーピングを使用すると、それぞれのマルチキャストグループに参加しているクライアントを持つ AP のみがマルチキャストトラフィックを無線で送信するようになるため、マルチキャスト転送のさらなる最適化が可能になります。そのため、ほとんどのシナリオにおいて、これは推奨される設定です。クライアントおよびマルチキャスト アプリケーションの動作を常に確認してください。一部の実装では、IGMP グループに参加しなかったり、適切に更新されなかったりする場合があり、そのためにマルチキャストストリームが期限切れになる可能性があるためです。

マルチキャスト DNS（mDNS）

mDNS（Bonjour プロトコル）は、ローカルネームサーバーを含まない小規模ネットワーク内でホスト名を IP アドレスに解決するためのプロトコルです。これは、AirPlay、AirPrint、Googlecast などのサービスを検出するためにクライアントによって使用されます。このプロトコルは、UDP IP マルチキャストを利用しており、レイヤ 2 ブロードキャストドメインに限定されます。

C9800 アーキテクチャには、mDNS トラフィック転送に関して、ブリッジングと mDNS ゲートウェイという 2 つの動作モードがあります。

mDNS ブリッジングとは、同じ L2 ブロードキャストのプロトコルパケット転送を指します。C9800 では、デフォルトで、各 WLAN の有線ポートおよびワイヤレスインターフェイスで受信されたパケットに対して mDNS ブリッジング機能が有効になっています。ただし、WLAN 設定で mDNS モードを変更するだけで、必要に応じて WLAN ごとに無効にすることができます。マルチキャスト - マルチキャストモードが有効になっている場合、C9800 は、各 mDNS パケットを、コントローラで設定された AP マルチキャストグループにブリッジングするため、ワイヤレスクライアントがそれを受信できるようになります。有効になっていない場合は、受信した各 mDNS パケットのコピーが作成され、CAPWAP ユニキャストトンネル経由で、個々の単一の AP に個別にブリッジングされます。どちらのシナリオでも、C9800 は、mDNS パケットを発信したクライアントの VLAN の有線ネットワークにも、その mDNS パケットをブリッジングします。そのため、mDNS は、デバイスが同じサブネット上にある場合、特別な設定を行わなくても C9800 で動作します。理想的には、mDNS ゲートウェイを使用して mDNS トラフィックをフィルタ処理することをお勧めします。

C9800 の mDNS ゲートウェイサービスは、有線インターフェイスおよびワイヤレスインターフェイス上の Bonjour サービス（mDNS アドバタイズメントおよびクエリ）をリッスンし、これらの Bonjour サービスを内部データベースにキャッシュして、不要なサービスをフィルタ処理しながら、異なるブロードキャストドメイン/VLAN 間でこれらの mDNS パケットを転送します。この方法では、そのようなサービスの送信元とクライアントを異なるサブネットに存在させることができ、ネットワーク内の mDNS トラフィックを制御できます。

mDNS ゲートウェイとして機能する C9800 は、クライアントからの mDNS クエリ（キャッシュされたサービスに関する）に応答します。その際、これらの mDNS 応答の送信元アドレスに、サービスを要求したクライアントに割り当てられている VLAN の、C9800 自身の IP アドレスが使用されます。このため、mDNS/Bonjour サービスを必要とするクライアントが存在する C9800 コントローラ上のすべての VLAN には、スイッチ仮想インターフェイス（SVI）で設定された有効な IP アドレスがある必要があります。

この要件は、mDNS トラフィックが WMI インターフェイスから送信されるようになるリリース 17.9.1 以降では適用されません。

mDNS パケットの処理は、特に mDNS ゲートウェイが有効になっている場合に、非常に多くのリソースを消費する可能性があります。具体的には、Apple の Continuity サービスが、非常に多くの通信を行う可能性があります。多数のクライアントが存在し、多数のサービスがアドバタイズされているネットワークでは、次のベストプラクティスを考慮することをお勧めします。

- 独自の mDNS サービスリストを作成し、デフォルトのプロファイルは使用しないでください。これにより、本当に必要なサービスを決定できるようになります。

```
mdns-sd service-list <service list name> OUT
 no match <service name>
mdns-sd service-list <service list name> IN
no match <service name>
```

- クライアントへの mDNS 応答を最適化するために、ロケーション特定サービス（LSS）を使用するように mDNS サービスポリシーを設定します。これには、次のコマンドを使用します。

```
mdns-sd service-policy <name>
 location lss
```

- mDNS トランスポートを IPv4 または IPv6（両方ではなく）に設定します。IPv4 が推奨されます。

```
mdns-sd gateway
       transport ipv4
```

- 非常に密度の高い環境では、前述したように、Apple の Continuity サービスを無効にすることもお勧めします。

```
mdns-sd service-list <service list name> OUT
 no match apple-continuity
mdns-sd service-list <service list name> IN
 no match apple-continuity
```

屋外展開

ここでは、屋外の設計、展開、およびセキュリティに関するベストプラクティスについて説明します。

RF アクティブサイトサーベイの実施とカバレッジの推定

屋外環境は、困難な RF 環境です。回避できない障害物や干渉源が多数存在します。ネットワークを設計する前に、RF 環境を把握するために RF アクティブサイトサーベイを実施することが最初のステップになります。

RF アクティブサイトサーベイを実施したら、ネットワークの設計要件を満たすために必要な屋外アクセスポイントの数を推定する必要があります。これを行うための専門的なツールが市場にいくつか存在します。常にそれらを活用して、必要な AP の数を把握することをお勧めします。

屋外 AP の展開

屋外アクセスポイントは、複数の展開モードで動作でき、各展開モードは異なるユースケースに対応しています。

- ローカルモード：これは、メッシュが不要な場合の、屋外展開に最適な選択肢です。すべての機能のサポートと RRM が提供され、2.4 GHz および 5 GHz 無線をクライアントアクセス専用として使用できます。この展開モードは、各アクセスポイントに専用イーサネット接続がある場合に使用する必要があります。

- ブリッジモード：すべての AP に対してケーブル接続を確保できないためにメッシュ展開が必要な場合の、屋外展開での一般的な選択肢です。AP は、有線バックホールが使用可能な場合はルートアクセスポイント（RAP）モードで動作し、無線バックホールを使用する場合はメッシュアクセスポイント（MAP）モードで動作します。ワイヤレスクライアントのトラフィックは、CAPWAP トンネルによって WLC に送られます。
- ブリッジ Flex モード：メッシュと Flex 間で柔軟なハイブリッド動作を提供します。これは、AP が WAN リンクによって WLC から離れた場所にあるシナリオで推奨されます。また、このモードは、トラフィックを AP レベルでローカルにスイッチングする必要があり、中央のコントローラには送信しない場合にも役立ちます。

注： 屋外 AP をファブリックモードで使用する場合、つまりファブリック SSID をブロードキャストする場合、サポートされるモードはローカルモードのみです。

バックホール用に DFS チャネルを選択することの回避

規制ドメインチャネル計画で許可される場合は、メッシュツリーのバックホールチャネルを選択するときに、レーダーに使用できるチャネル（DFS チャネル）を避けてください。

各 BGN への複数の RAP の展開

メッシュネットワークを展開する場合は、各アクセスポイントから WLC に戻る複数のパスが存在する必要があります。メッシュツリーごとに複数の RAP を配置することで、複数のパスを追加できます。RAP に障害が発生してオフラインになると、他のメッシュアクセスポイントが同じブリッジグループ名（BGN）を持つ別の RAP に参加し、WLC に戻るパスを維持します。

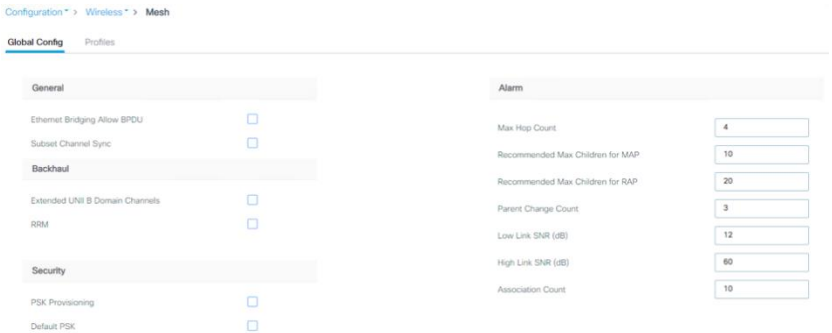
最善の結果を得るために、次の簡単な推奨事項に従ってください。

- 同一チャネル干渉を軽減または回避するために、RAP が異なるチャネルで設定されていることを確認してください。MAP は、バックグラウンドスキャンを使用して各 RAP を識別します。
- 親の変更時にメッシュ AP アドレスが再ネゴシエートされ、メッシュ全体のコンバージェンス時間が遅延することを防ぐために、RAP を同じ VLAN/サブネット上に配置する必要があります。
- 新しい親の検出を容易にするために、MAP でバックグラウンドスキャンが有効になっていることを確認してください。

推奨メッシュ設定

C9800 ワイヤレスコントローラでは、メッシュの設定は、グローバルレベル、メッシュプロファイルレベル、および AP レベルでも実行できます。メッシュプロファイルを使用すると、必要なすべての設定を 1 つの場所にまとめておき、メッシュプロファイルを AP 参加プロファイルに割り当てることで、それらを AP グループに適用できるため、便利です。

グローバル設定は、[設定（Configuration）] > [ワイヤレス（Wireless）] > [メッシュ（Mesh）] にあります。



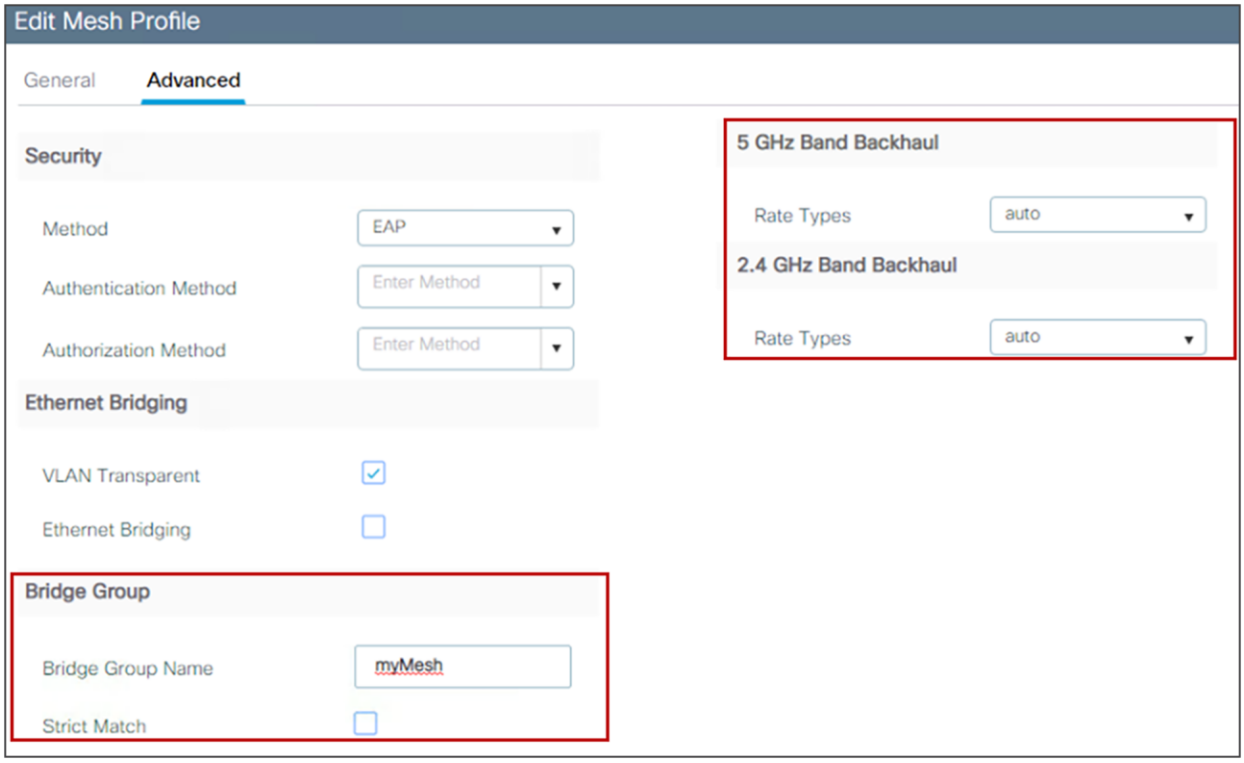
同じページで、[プロファイル（Profiles）] タブをクリックして、カスタムメッシュプロファイルを定義したり、デフォルトのメッシュプロファイルを変更することができます。

別の AP 固有の設定は、`ap exec` コマンドを使用して実行できます。

```
C9800#ap name <NAME>  mesh ?
  backhaul         Configure mesh backhaul
  block-child      Set mesh block child state
  daisy-chaining   Set mesh daisy chaining
  ethernet         Configures Ethernet Port of the AP
  linktest         Perform a linktest between two APs
  parent           Set mesh preferred parent mac address
  security         PSK provisioned key deletion from AP
  vlan-trunking    Enables vlan trunking for bridge mode AP
```

いくつかの推奨設定について説明します。ブリッジモードで動作させる場合は、各アクセスポイントにブリッジグループ名と優先親を割り当てる必要があります。これにより、メッシュネットワークが常に同じ順序でコンバージェンスするようになり、ネットワークを初期設計と一致させることができます。

ブリッジグループは、メッシュプロファイルレベルで設定できます。



メッシュネットワークを展開する場合は、各メッシュノードが可能な限り高いバックホールデータレートで通信する必要があります。これを確認するには、[自動（Auto）] バックホールデータレートを選択して、動的レート調整（DRA）を有効にすることをお勧めします。上に示されているように、メッシュプロファイルで有効にして、すべてのメッシュリンクで DRA を有効にする必要があります。

優先親の設定は、AP ごとの設定です。

```
C9800#ap name ap-name mesh parent preferred mac-address
```

確認するには、次のコマンドを使用します。

```
C9800#show ap name ap-name mesh neighbor detail
```

メッシュネットワークの場合、バックホール速度を 40 MHz にすると、パフォーマンスの向上と RF 輻輳の回避との間で最適なバランスを実現できます。AP ごとにチャネル幅を設定するには、次のコマンドを使用します。

```
C9800# ap name <AP-name> dot11 5ghz channel width 40
```

メッシュネットワークで最適なパフォーマンスを確保するために、バックホールリンクの品質が良好であることを確認してください。最適なリンク品質は 40 dBm を超えますが、非視認の展開や長距離のブリッジでは、常にこれを達成できるとはかぎりません。シスコでは、リンク SNR を 25 dBm 以上にすることをお勧めします。リンク SNR を確認するには、次のコマンドを使用します。

```
C9800#sh wireless mesh neighbor
```

メッシュネットワークに参加する AP を認証する場合は、MAC 認証用に外部 RADIUS サーバーを設定する必要があります。これにより、すべてのブリッジモードのアクセスポイントを単一の場所で認証できるようになるため、ネットワーク管理が簡素化されます。認証のセットアップ方法については、次の設定ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_mesh_ewlc.htmlメッシュのセキュリティと展開のしやすさの間で最適なバランスを実現するために、メッシュキープロビジョニング機能を有効にすることをお勧めします。詳細については、次の設定ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-15/config-guide/b_wl_17_15_cg/m_mesh_ewlc.html#preshd-key-provsn

テレメトリ

Catalyst 9800 ワイヤレスコントローラは、ストリーミングテレメトリをサポートしており、外部コレクタにデータを効率的にストリーミングできます。コレクタは、そのデータをさらに分析し、モニタリングやトラブルシューティングのための関連情報を抽出します。C9800 は、ダイヤルインテレメトリとダイヤルアウトテレメトリをサポートしています。ダイヤルアウトまたは「設定済み」テレメトリ サブスクリプションでは、ユーザーによって設定がセットアップされると、C9800 がサブスクリプション設定を維持してサブスクライバにテレメトリを送信します。コレクタへのアクティブなセッションは必要ありません。次に、テレメトリ サブスクリプションの設定例を示します。

```
telemetry ietf subscription 1011
 encoding encode-tdl
 filter tdl-uri /services;serviceName=ewlc/wlan_config
 source-address <source IP on the C9800>
 stream native
 update-policy on-change
 receiver ip address <collector/subscriber IP>  protocol tls-native profile <profile name>
```

17.6 以降、C9800 は最大 128 の同時テレメトリ サブスクリプションをサポートしており、17.15 ではこの制限が 150 に増加しました。Catalyst 9800 は、Cisco Catalyst Center および Cisco Prime Infrastructure（PI）の 1 つインスタンス（1 つのインスタンスのみ）へのストリーミングテレメトリをサポートしています。両方のコレクタを同時にアクティブにすることはできますが、たとえば、C9800 ストリーミングテレメトリを 2 つの異なる Cisco Catalyst Center コレクタに送信することはできません。外部のサードパーティ製コレクタを使用する場合は、セッション数がサポートされる最大数を超えないことを確認してください。

既存のサブスクリプションを表示するには、次のコマンドを使用できます。

```
show telemetry ietf subscription all
```

```
Telemetry subscription brief
ID                Type         State       Filter type
-----------------------------------------------------
1011              Configured   Valid       tdl-uri
1012              Configured   Valid       tdl-uri
1013              Configured   Valid       tdl-uri
1014              Configured   Valid       nested-uri
1016              Configured   Valid       tdl-uri
1051              Configured   Valid       tdl-uri
```

[状態（State）] 列では、サブスクリプションが有効かどうかも確認できます。

詳細については、『Catalyst 9800 Programmability and Telemetry Deployment Guide』（https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/catalyst-9800-programmability-telemetry-deployment-guide.html）を参照してください。

Prime および Catalyst Center によって管理される C9800

Catalyst 9800 ワイヤレス LAN コントローラは、Cisco Prime Infrastructure（PI）と Catalyst Center の両方によって読み書き可能な方式で同時に管理することはできません。ただし、設定やレポート作成のために Prime で C9800 を管理し、アシュアランスに Catalyst Center を使用することは可能です。要するに、ボックスを設定することができ、書き込みアクセス権限を持てる管理プラットフォームは 1 つだけです。

注： Prime はすでに販売終了となっています。置き換えを検討してください。サポートされる最新の IOS-XE バージョンは 17.17 です。最新の物理アプライアンスである CW9800 はサポートされていません。

Prime を設定して C9800 を管理する方法の詳細については、次のリンク先を参照してください：
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/214286-managing-catalyst-9800-wireless-controll.html。

ここで理解する必要がある重要な点があります。ネットワーク管理ソリューションとして Cisco Catalyst Center に移行する予定がある場合は、最初に C9800 を Prime Infrastructure から削除する必要があります。C9800 が PI から削除/削除されても、インベントリ登録時に PI によって C9800 にプッシュされたすべての設定がロールバックされないため、システムから手動で削除する必要があります。具体的には、ストリーミング テレメトリ データをパブリッシュするために C9800 WLC 用に確立されたサブスクリプションチャネルは削除されません。

この特定の設定を確認するには、次のコマンドを使用します。

```
C9800#show run | sec telemetry
```

この設定を削除するには、このコマンドの no 形式を実行します。

```
C9800(config) # no telemetry ietf subscription <Subscription-Id>
```

この CLI を繰り返して、各サブスクリプション識別子を削除します。この別の CLI を繰り返して、各トランスフォーム名を削除します

```
C9800(config) # no telemetry transform <Transform-Name>
```

トラブルシューティングのヒント

トラブルシューティングに関する最新情報については、次のドキュメントを参照してください。

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-tech-notes-list.html

https://logadvisor.cisco.com/logadvisor/wireless/9800/

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。