# メッシュ導入モード

この章では、メッシュ導入モードについて説明します。内容は次のとおりです。



# ワイヤレス メッシュ ネットワーク

Ciscoのワイヤレス屋外メッシュ ネットワークでは、複数のメッシュ アクセス ポイントによって、安全でスケーラブルな屋外ワイヤレス LAN を提供するネットワークが構成されます。

それぞれの場所で、3つのRAPが有線ネットワークに接続され、建物の屋根に配置されています。すべてのダウンストリーム アクセス ポイントは、MAP として動作し、ワイヤレス リンク（表示されていません）を使用して通信します。

MAP と RAP の両方共、WLAN クライアント アクセスを提供できますが、RAP の場所がクライアント アクセスの提供には向いていないことがよくあります。3 台の AP はすべて建物の屋根に設置され、RAP として機能しています。これらの RAP は、それぞれの場所でネットワークに接続します。

メッシュ アクセス ポイントから CAPWAP セッションを終端させるオンサイト コントローラがある建物もありますが、CAPWAP セッションはワイドエリア ネットワーク（WAN）を介してコントローラにバックホールできるため、それは必須要件ではありません

（注） CAPWAP 経由での CAPWAP はサポートされません。RAP または MAP イーサネット ポートで接続されているローカル モードの AP は、サポートされる構成ではありません。

# ワイヤレス バックホール

Cisco ワイヤレス バックホール ネットワークでは、トラフィックを MAP と RAP の間でブリッジできます。このトラフィックは、ワイヤレス メッシュによってブリッジされている有線デバイスからのトラフィックか、メッシュ アクセス ポイントからの CAPWAP トラフィックになります。このトラフィックは、ワイヤレス バックホールなどのワイヤレス メッシュ リンクを通過する際に必ず AES 暗号化されます。

AES 暗号化は、他のメッシュ アクセス ポイントと共に、メッシュ アクセス ポイントにおけるネイバー同士の関係として確立されます。メッシュ アクセス ポイント間で使用される暗号鍵は、EAP 認証プロセス中に生成されます。

## ユニバーサル アクセス

802.11a 無線を介してクライアント トラフィックを受け入れるようメッシュ アクセス ポイントでバックホールを設定できます。この機能は、コントローラの GUI の Backhaul Client Access（[Monitor] > [Wireless]）で識別できます。この機能が無効な場合、バックホール トラフィックは 802.11a または 802.11a/n 無線を介してのみ伝送され、クライアント アソシエーションは 802.11b/g または 802.11b/g/n 無線を介してのみ許可されます。設定の詳細については、159 ページの「拡張機能の設定」の項を参照してください。

（注） リリース 8.2 以降では、2.4 GHz でもバックホールがサポートされます。

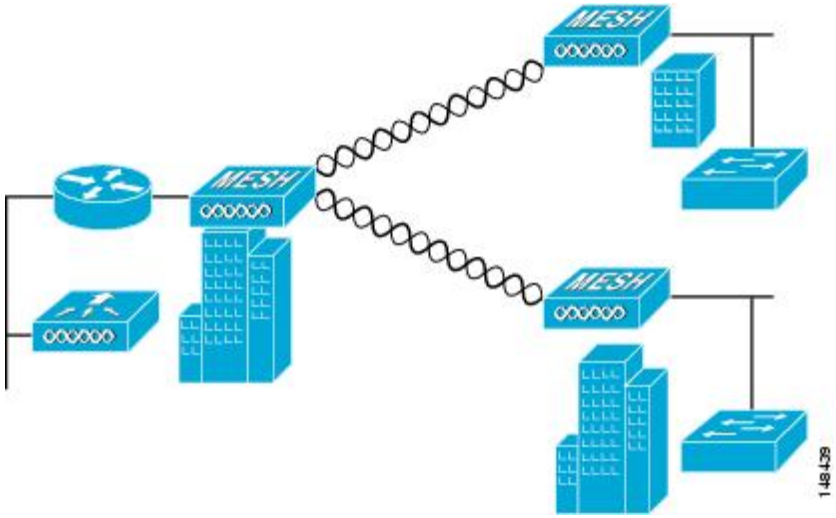
# ポイントツーマルチポイント無線ブリッジング

ポイントツーマルチポイント ブリッジング シナリオでは、ルート ブリッジとして機能する RAP が、有線 LAN に接続した非ルートブリッジとしての複数の MAP と接続します。デフォルトでは、この機能はすべての MAP に対して無効になっています。イーサネット ブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネット ブリッジングを有効にする必要があります。

**図 *1:* ポイントツーマルチポイント ブリッジングの例**

次の図は、1 つの RAP と 2 つの MAP のシンプルな導入を示していますが、この構成は基本的に WLAN クライアントがないワイヤレス メッシュです。イーサネット ブリッジングを有効にすることでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上

からの MAP カバレッジはクライアント アクセスに適していないことがあります。

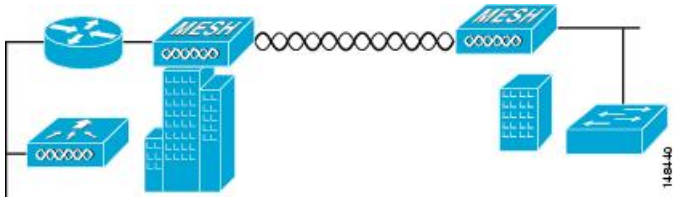



# ポイントツーポイント無線ブリッジング

ポイントツーポイントブリッジング シナリオでは、ワイヤレス バックホールを使用してスイッチ ネットワークの2つのセグメントをブリッジ接続することにより、1500 シリーズのメッシュ AP を使用してリモート ネットワークを拡張できます。これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイント ネットワークと同様に、イーサネット ブリッジングを有効にすることでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

イーサネット ブリッジド アプリケーションを使用する場合は、RAP およびそのセグメント内のすべての MAP でブリッジング機能を有効にすることをお勧めします。MAP のイーサネット ポートに接続されたすべてのスイッチで VLAN Trunking Protocol（VTP）を使用していないことを確認する必要があります。VTP によってメッシュ全体のトランキングされた VLAN が再設定されることがあるため、プライマリ WLC と RAP 間の接続が失われることがあります。設定が正しくないと、メッシュ導入がダウンすることがあります。

**図 *2:* ポイントツーポイント ブリッジングの例**




セキュリティ上の理由により、デフォルトでは MAP のイーサネット ポートは無効になっています。有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定する必要があります。コントローラの GUI を使用してイーサネット ブリッジングを有効にするには、

[Wireless] > [All APs] > [Details for the AP] ページの順に選択し、[Mesh]タブをクリックして、[Ethernet Bridging] チェックボックスを選択します。

（注） ワイヤレスバックホールの全体的なスループットはメッシュ ツリーの各ホップの半分になります。イーサネット ブリッジング対象のクライアントが MAP で使用され、大量のトラフィックが通過する際、スループット消費が高くなり、ダウンリンク MAP がスループットの枯渇によってネットワークに接続できなくなる可能性があります。

イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

メッシュ ノードをブリッジとして使用する場合。

MAP でイーサネット ポートを使用してイーサネット デバイス（ビデオ カメラなど）を接続する場合。

該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP でもイーサネット ブリッジングを有効にします。たとえば、Hop 2 の MAP2 でイーサネット ブリッジングを有効にする場合は、MAP1（親 MAP）と、コントローラに接続している RAP でもイーサネット ブリッジングを有効にする必要があります。

長距離リンクのレンジ パラメータを設定するには、 [Wireless] > [Mesh] の順に選択します。ルート アクセス ポイント（RAP）と最遠のメッシュ アクセス ポイント（MAP）間に最適な距離（フィート単位）が存在します。RAP ブリッジから MAP ブリッジまでのレンジは、フィート単位で記述する必要があります。

ネットワーク内のコントローラと既存のすべてのメッシュ アクセス ポイントに join する場合は、次のグローバル パラメータがすべてのメッシュ アクセス ポイントに適用されます。

レンジ：150 ～ 132,000 フィート

# メッシュ レンジの設定（CLI）

**手順**

- ブリッジングを実行するノード間の距離を設定するには、**config mesh range** コマンドを入力します。

  レンジの指定後に、AP はリブートされます。

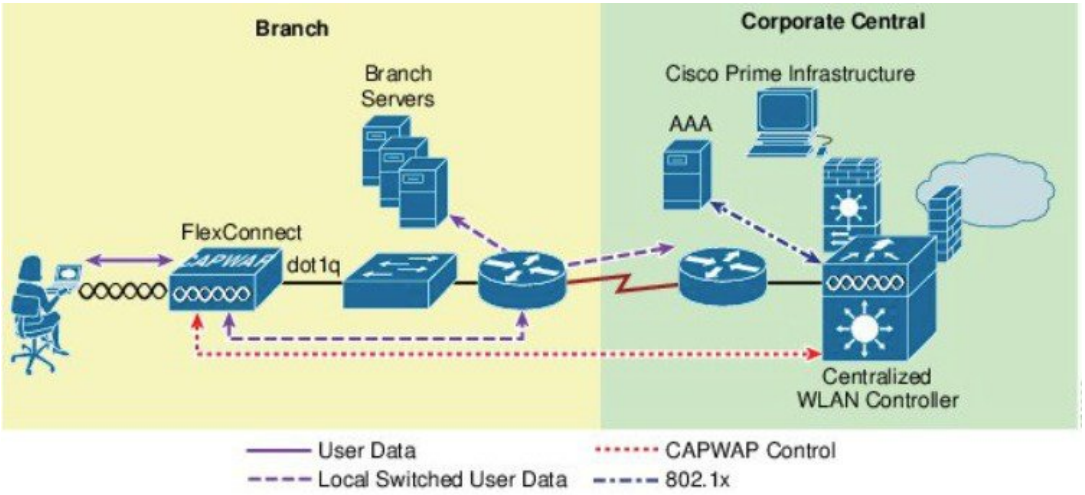
（注） 範囲と AP の密度を見積もる場合、次の URL にある範囲カルキュレータを使用できます。

すべてのアクセス ポイントのレンジ カルキュレータ： http://173.37.206.125/aspnet_client/system_web/2_0_50727/wng_coverage_capacity_calculator_v2.0_html/wng_coverage_capacity_calculator_v2.0.htm

- メッシュ レンジを表示するには、**show mesh config** と入力します。

# リリース 8.8 の Flex+Mesh の概要

以下は、一般的な FlexMesh アーキテクチャです。CAPWAP AP は FlexConnect + ブリッジ モードで、「ルート」AP または RAP モードのコア ネットワークに有線アップリンクで接続されています。この状況でも AP は、CAPWAP 経由で中央コントローラによって管理されます。ただし、AP は AP に設定されている WLAN のデータ スイッチング方式に基づいて、802.11 クライアントへのサービスの提供を継続できるスタンドアロン モードに移行することができます。データは中央、またはローカルでスイッチングできます。データを中央でスイッチングする場合、すべてのデータは WLC に送信され、そこでさらにスイッチングされます。ローカル スイッチ ネットワークでは、データは RAP に送信され、RAP が有線アップリンク上でローカルにスイッチングします。FlexConnect と Flex+Mesh モード AP の間に、中央およびローカルにスイッチされた WLAN の設定および機能での違いはありません。




# 新しい 8.8 の機能をサポートする Mesh COS AP

1562 は、8.4 リリースでメッシュをサポートしました。1542 AP（1542D および 1542I）モデルは、8.5 リリースでメッシュをサポートしました。Flex Mesh はプラットフォームに依存しない機能であり、1542 に基づいて設計された Flex Mesh は 1562 にも適用できるため、これらすべての AP は Flex Mesh をサポートできます。

Flex Mesh 機能は、リリース 8.8 以前でも IOS ベースのメッシュ AP でサポートされていますが、リリース 8.8 では、この機能が COS ベースのメッシュ AP で公式サポートされ、リリース 8.8 以降で TAC のサポート対象になりました。また、IPv6 も COS ベースのメッシュ AP でサポートされるようになりました。

1542 には、2 つの新しい SKU が開発されています。8.5 でリリースされた AP1540 シリーズは、ほとんどの技術要件を満たしていますが、外部アンテナはありません。AP1542E2 および AP1542E4 は 1541D/I AP のハードウェア異型です。1542E2 はデュアル バンド モード AP で、2.4 GHz（802.11b/g/n、20 MHz）と 5 GHz（802.11a/n/acW2、20/40/80 MHz）のデュアル無線、デュアルバンドです。1542E4 はシングル バンド モード AP で、2.4 G をサポートするアンテナ

A と B、5 G をサポートするアンテナ C と D を備えています。これら AP は、少なくとも 2 TX & 2 RX チェーン、2 つの空間ストリームをサポートします。AP は、TX あたり、最小 22 dBm（2.4 GHz）および 24 dBm（5 GHz）の伝導送信送出電力をサポートすることが求められています。この新しいプラットフォーム用の新しい基本 PID の追加とパワー テーブルの変更は、AP と WLC の両方で実行されます。外部アンテナを備えた -D（INDIA）のパワー テーブルが新しくなっています。

## フレキシブル アンテナ ポート設定

上記の HW の変更により、SW にも変更が必要です。AP は、フレキシブル アンテナ ポート設定をサポートする必要があります。アンテナがサポートするモードをシングル バンドまたはデュアル バンドのいずれかにユーザが設定できるように SW が変更されています。シングル バンドまたはデュアル バンド モードは、ソフトウェアで設定できます。これは、1532 AP の設定と同様です。ユーザは、WLC CLI または GUI を使用して、アンテナ バンド モードを設定できます。

## Flex Mesh AP の実行モード

Flex Mesh COS AP は、接続モードまたはスタンドアロン モードで実行できます。FlexConnect のスタンドアロン モードには、メッシュ ネットワークのスタンドアロン機能を継承するために変更が行われます。また、本ガイドのこのセクションの下で説明する「放棄」モードと呼ばれる別のモードもあります。

## 接続モード

COS Flex Mesh AP（ルート AP または子のメッシュ AP）は、WLC にアクセスして接続し、WLC とキープアライブ メッセージを定期的に交換できる場合、接続モードであると見なされます。このモードでは、Flex Mesh AP はローカルおよび中央でスイッチされる WLAN をサポートできます。これによって、通常のクライアントと子のメッシュ AP に接続を許可します。

## スタンドアロン モード

COS Flex Mesh AP は、コントローラへの接続が失われてもローカル ゲートウェイにアクセスできる場合は、スタンドアロン モードにあると見なされます。このモードの COS Flex+Mesh AP は、中央でスイッチされるすべての WLAN を無効にし、ローカルにスイッチされた WLAN を起動および実行された状態に維持します。また、認証サーバがローカル ネットワークで到達可能である限り、ローカル認証を使用して、新しいクライアントがローカルにスイッチされた WLAN に接続するのを許可します。子のメッシュ AP は、このモードでの接続を許可されません。

# 放棄モードまたは永続 SSID モード

COS Flex+Mesh AP は、ゲートウェイ IP にアクセスできなくなり、ローカル ネットワークに接続していない状態になると、放棄モードになります。考えられるシナリオは次のとおりです。

- AP がいずれの有線またはワイヤレスのアップリンクにも接続されていない。
- ワイヤレス アップリンクは確立されているが、認証されていない。
- アップリンクは確立および認証されており、IP アドレスは設定されているがゲートウェイ IP は設定されていない。
- アップリンクは確立および認証されており、IP アドレスとゲートウェイ IP も設定されているが、1 分以上たってもゲートウェイに到達できない。

子のメッシュ AP とクライアントのどちらも、このモードでの接続は許可されません。ローカルおよび中央でスイッチされる WLAN は無効になります。AP はこのモードでもアップリングをスキャニングする可能性があり、この間にビーコンは送信されません。

（注） Flex Mesh COS AP では、放棄モードで再起動タイマーが有効になるため、スタンドアロン モードと接続モードのいずれにも移行しなければ、AP は 40 分後に再起動します。

# Flex Mesh COS AP のモード/状態の遷移

- Flex Mesh モードの COS AP は常に放棄モードで起動します。このモードでは、アップリンク（有線または無線）をスキャンする必要があります。
- 初期段階またはゲートウェイ ローミングのシナリオ時のいずれかで新しいアップリンクが選択されると、認証に合格することが期待されるため、CAPWAP 接続を 2 分以内に確立する必要があり、そうでない場合、選択した親はブラックリストに記載されます。この機能は、通常の Mesh モード COS AP と同じです。
- Flex Mesh AP に有効な CAPWAP 接続があり、CAPWAP 接続が失われると、スタンドアロン モードに移行し、ゲートウェイが到達可能である限りスタンドアロン モードのままになります。Flex Mesh AP は、最後に成功した CAPWAP 接続に使用した IP モード（IPV6 または IPV4）およびその IP モードの GW の到達可能性を追跡します。
- スタンドアロン モードの Flex Mesh AP では、Mesh コントロールがタイマー（20 秒）を開始し、GW IP（IPV4 または IPV6）の ARP エントリを定期的に更新するほか、GW の到達可能性ステータスを Path Control Protocol（パス制御プロトコル）に問い合わせます。PCP は、対象の AP から得られたゲートウェイの到達可能性ステータスを保持しますが、これは PCP メッセージ経由でルート AP によって報告されたステータス、または対象 AP がルート AP 自身の場合はゲートウェイ IP アドレスの ARP ルックアップを実行して報告されたステータスです。GW が 1 分以上到達不能の場合、Flex Mesh AP は親をブラック リストに記載し、放棄モードに移行して新しいアップリンクを再スキャンします。

- 放棄モードを終了するには、AP は WLC に接続し、接続モードに移行する必要があります。放棄モードからスタンドアロンモードへの直接の移行はサポートされていません。今後の設計上の機能強化で検討する必要があります。

# スタンドアロン モードの Flex AP に関する設計上の考慮事項

- Flex AP はスタンドアロン モードの場合、同じ親を継続し、より適切なネイバー（それが優先される親であっても）を検出することも、ローミングすることもありません。これは、セキュリティが新しい親に引き継がれることやローミングの成功が保証されていないことが理由です。セキュリティに失敗すると、候補の親が不必要にブラックリストに記載される可能性があります。スタンドアロンのローミングは、今後の設計の機能強化でスタンドアロン時のセキュリティがメッシュ AP でサポートされるようになってから検討する方がよいでしょう。
- BGN タイマーは、スタンドアロンモードでは停止します。したがって、子のメッシュ AP がスタンドアロン モードの状態で、異なる BGN の親に接続し、その後またスタンドアロンモードに戻る場合は、BGN タイマーが停止するため、子のメッシュ AP は 15 分後（BGN タイマーの有効期限）に再スキャン モードになりません。
- スタンドアロン モードでは再起動タイマーが停止するため、AP は CAPWAP 接続がない場合、40 分後に再起動しません。
- スタンドアロンモードから接続モードに戻った後は、最適なネイバー選択タイマーと BGN タイマーが再起動するため、子のメッシュ AP は最適なネイバーにローミングできます。

# COS Flex RAP の特別なスタンドアロン モード

このモードでは、SSID が常にブロードキャストされます（永続的な SSID）。さらに、リブート後、この特殊な永続モードを有効にすると、Flex Mesh RAP はゲートウェイが到達不能の場合でも、SSID のブロードキャストを開始できる必要があります。

# 既存の FlexConnect AP モードの設計

- ローカルにスイッチされた WLAN は config.flex ファイルに保存され、FlexConnect AP はスタンドアロン モードである限り、ローカルの WLAN SSID をブロードキャストします。
- 起動時、FlexConnect AP はゲートウェイがプロビジョニングされている場合、ローカルにスイッチされた WLAN のブロードキャストのみを開始します。
- COS FlexConnect AP は、ゲートウェイ情報がある時点で削除されると、スタンドアロンモードから移行し、ローカルにスイッチされた SSID のブロードキャストを停止し、ゲートウェイが再度プロビジョニングされるのを待機します。
- ゲートウェイがプロビジョニングされると、FlexConnect AP は再度スタンドアロンモードに移行し、ローカルにスイッチされた SSID のブロードキャストを再度開始します。

- 有効なゲートウェイがない場合、ローカルネットワークに到達できずクライアントに接続する理由がないため、FlexConnect APは最終的にSSIDのブロードキャストを停止します。

既存の FlexConnect AP モードには、リブート時に WLAN 設定を保持したり、ローカル SSID のブロードキャストを開始できるようにしたりするための設計が含まれています。ただし、Flex RAP については、以下で説明するように NBN 導入に関する特別なスタンドアロン モード要件があります。

- Flex RAPは、ゲートウェイに到達できない場合も、直接スタンドアロンモードで起動し、SSID のブロードキャストを開始できること。
- Flex RAPは、最初に到達可能だったゲートウェイがある時点で到達不能になった場合、スタンドアロン モードを継続し、SSID をブロードキャストし続ける。
- Flex RAP は、実際のクライアントをサポートできない場合でも、AP が起動して実行中かどうかをオペレータが確認できるように SSID をブロードキャストする必要がある。

# 新しい要件をサポートするための設計上の考慮事項

- Flex RAP は、WLAN 設定をダウンロードして config.flex に保存するために、少なくとも一度はコントローラに接続します。この WLAN は、ローカルにスイッチされた WLAN です。
- 設定は、config.flex ファイルに保存されるとリブートしても残るため、設定が消去されない限り、AP が WLC に再度接続する必要はありません。
- RAP で有線リンクを維持するために必要な新しい設定がサポートされています。この設定は、メッシュ設定ファイル、つまり「strict_wired_uplink」に保存されます。
- 次の条件が true の場合、Flex Mesh AP は、ゲートウェイに到達できない場合でも、フレックス設定ファイルに保存されているローカル WLAN をブロードキャストします。
  - AP が Flex Mesh Root AP である
  - AP の strict_wired_uplink が true に設定されている
- Flex Mesh AP を strict wired AP として設定するための新しい AP CLI コマンドがサポートされる予定です。

  **# CAPWAP ap mesh strict-wired-uplink <true/false>**
- 新しい設定パラメータの「strict_wired_uplink」は、ストレージディレクトリの config.mesh ファイルに保存されるため、リブートに関係なく永続的になります。このパラメータのデフォルト値は false になります。
- strict_wired_uplink 設定は、AP が Flex-Mesh Root AP として設定されている場合のみ有効です。その他のすべての AP モードおよびメッシュ AP ロールでは、strict_wired_uplink を設定しても有効になりません。
- strict_wired_uplink が Flex Mesh Root AP に対して true の場合：

- メッシュの再起動時に、有線アップリンクが直ちに選択される。
- 有線アップリンクがブラックリストに記載されることがない。
- CAPWAP 稼動タイマーが実行されない。
- Mesh Reboot タイマーが実行されない。
- 有線の隣接関係の探索は、インターフェイスがダウンしていても常に true を返す。
- ワイヤレス バックホールをアップリンクとして選択することはできない。
- ワイヤレスバックホールをダウンリンクとして使用し、メッシュの子ノードへの接続を提供できる。

- ゲートウェイの設定チェックによる問題を避けるためには、スタティック IP およびゲートウェイを Flex RAP に設定する必要があります（単なるダミーの IP またはゲートウェイであっても）。
  - スタティック IP とゲートウェイの設定により、Flex RAP はローカル ネットワークへの接続がない場合（つまり、IP とゲートウェイをプロビジョニングする DHCP サーバがない）でも、リブート後にスタンドアロンモードに移行できます。Flex RAP は、ネットワークへの接続が何もない場合であっても、ローカルにスイッチされた SSID をブロードキャストし続けます。
  - IP とゲートウェイが有効でない場合、AP が DHCP サーバに接続されると、DHCP IP がスタティック IP 設定を上書きし、DHCP IP とゲートウェイ設定が使われます。
- 「永続的な SSID」機能を有効/無効にするシンプルな WLC CLI を提供する予定です。WLC と AP は、この設定を有効にするために通信が必要です。
- AP の「show mesh config」も、この機能の現在のステータスを表示します。

# メッシュの機能強化の設定

**ステップ 1** 上記の説明で示したように、RAP は SSI を永続的に送信するモードに設定する必要があります。この設定オプションは、CLI モードでのみ使用できます。

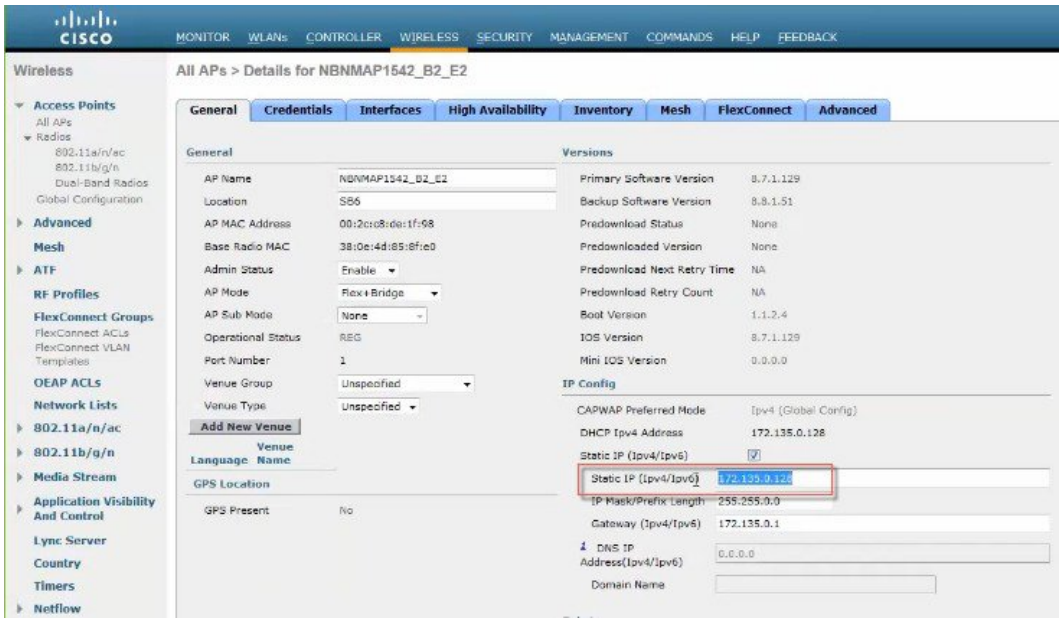
```
NBNMAP1542_B2_E2#capwap ap mesh strict-wired-uplink
  disable  disable strict wired uplink
  enable   enable strict wired uplink
NBNMAP1542_B2_E2#capwap ap mesh strict-wired-uplink
```

**ステップ 2** このモードは、「show mesh config」コマンドを実行して「strict wired uplink」が Enabled と表示されていれば有効です。

```
NBNMAP1542_B2_E2#show mesh conf
AP Specific Configuration:
AP Role: Flex Root AP
Backhaul Mode: 802.11a
Strict Wired Uplink: Enabled
Ethernet Bridging: Disabled
Public Safety: Disabled
Slot Bias: Disabled
LSC Authentication: Disabled
Background Scanning: Disabled
Strict Matching BGN: Disabled
Convergence Method: Standard Convergence, CCN mode: Disabled
Ethernet Bridging BPDU Allow: Disabled
Daisy Chain Mode: Disabled
VLAN Transparent Bridging: Disabled
Trunk VLAN Id: 0
Backhaul Rate: Auto
Preferred Parent: 0C:75:BD:0C:A1:F1
CAPWAP Join Mode: IPv4
Bridge Group Name:
Mesh Statistics Push Interval(min): 3
Range(feet): 12000
Mesh Security Mode: EAP (PSK Provisioned:Tue Nov 21 15:37:59 2017)
Background Scanning: Disabled
Universal Client Access: Enabled
Universal Client Access Ext: Enabled
Global Public Safety: Disabled
Battery Backup: Enabled
Full Sector DFS: Enabled
IDS(Rogue/Signature Reporting): Disabled
Backhaul A-MSDU: Enabled
Backhaul DCA Status: Disabled
Configured Parent: 0C:75:BD:0C:A1:F1
Multicast Mode:In-Out
```

**ステップ 3** 上記で示したように、永続的な SSID が機能し、ゲートウェイの設定チェックによる問題を避けるためには、スタティック IP およびゲートウェイを Flex RAP に設定する必要があります（単なるダミーの IP またはゲートウェイであっても）。スタティック IP とゲートウェイの設定により、Flex RAP はローカル ネットワークへの接続がない場合（つまり、IP とゲートウェイをプロビジョニングする DHCP サーバがない）でも、リブート後にスタンドアロンモードに移行できます。Flex RAP は、ネットワークへの接続が何もない場合であっても、ローカルにスイッチされた SSID をブロードキャストし続けます。

IP とゲートウェイが有効でない場合、AP が DHCP サーバに接続されると、DHCP IP がスタティック IP 設定を上書きし、DHCP IP とゲートウェイ設定が使われます。




# リリース 8.8 で RAP 永続モードをテストする手順

最適な環境でテストするために、永続的な SSID が設定されている、または放棄モードの RAP と通常の RAP モードの RAP を 1 つずつ用意します。クライアントを両方の RAP に接続し、RAP とコントローラの接続が失われたときの動作を確認します。

- 永続モードが有効な RAP に接続されているクライアントは SSID の送信が継続されるため、RAP への接続を維持します。
- 通常モードの RAP に接続されているクライアントは、SSID の送信が停止されるため接続を失います。

# リリース 8.8 での追加メッシュ機能の概要

導入ガイドのこの項では、リリース 8.8 の新しいメッシュ機能または屋外 AP 機能について説明します。

このドキュメントの目的は、次の機能について設定ガイド情報を提供することです。

1. 「合法的傍受（LI）」とモニタリング
2. 特定の URL のホワイトリスト作成
3. キャプティブ ポータル設定
4. ポリシーの適用と割当量の管理

# リリース 8.8 での「合法的傍受」（LI）とモニタリング

シスコの一部のお客様は、Flex+Mesh（ローカル スイッチングを使用）ツリーによって、非常に大規模な地理的領域に Cisco Wi-Fi メッシュ ソリューションを導入することを計画しています。中央集中型の WLC への有線バックホールを持つ RAP（ルート アクセス ポイント）は、ワイヤレス クライアントに対応するメッシュ ツリーを形成します。合法的傍受の機能は、管理者が集中型モニタリング システム（CMS）を設定した場合に行われる、携帯電話、固定電話、およびワイヤレス インターネット トラフィックの合法的傍受とモニタリングのプロセスです。

Flex+Mesh モードのセットアップにはメッシュ ネットワークが存在し、LI の一部として各フローのクライアント フロー情報をエクスポートできます。

RAP は NAT/PAT および LI レコードの生成を実行し、WLC 経由で LI サーバに送信します。NAT/PAT ですべてのフローのレコードが作成されます。この時点で、RAP はそのフローの Syslog レコードを作成します。RAP は、これらの Syslog パケットを CAPWAP-DATA を介して WLC に送信します。

（注） RAP を経由しないメッシュ ツリー内のすべてのピア ツー ピア クライアント トラフィック（MAP のみがローカルに処理する）は、LI サーバへの報告対象とは見なされません。

WLC は自身の MAC および IP を含む Syslog パケットを更新し、ネットワーク内の Syslog サーバに Syslog パケットを転送します。これらのパケットは暗号化されません。

一般的なワークフローは次のとおりです。

1. 管理者は、Syslog サーバの設定を行う必要があります。

   IPv4 または IPv6 のいずれかのみがサポートされます。

   IPv6 を設定する場合は、WLC が IPv6 対応である必要があります。

   既存の「config ap syslog global」コマンドが機能します。

2. LI は、グローバルにのみ有効または無効になります。

   これに関する前提条件は、Syslog サーバの設定になります。

3. AP は、RAP で WLC から受信した syslog サーバの設定（IP アドレスおよび有効/無効）を保存します。

4. IPv4 パケットに対して NAT/PAT 交換が実行されます（内部 DHCP の場合）。

   IPv6 パケットおよび IPv4 パケットについては次のとおりです（外部 DHCP の場合）。

   1. パケットの送信元/宛先 IP/ポートに基づいてフローを特定します。
   2. FlowTable エントリにフローを保存します。

5. LI レポータ要素が以下を実行します。

1. NAT 要素または FlowTable 要素によってプッシュされた新しいフロー レコードを受信および保存します。
2. 定期的なタイマー（通常は 1 分）を実行します。
3. このタイマーが期限切れになると、テーブル内のすべてのフロー レコードがフラッシュされ、v4 と v6 の両方のフローを含む syslog レコードに変換されます。次のセクションで syslog 形式が指定されます。

6. フロー作成の開始時にのみ、そのレコードが送信されます。その後、他のフロー レコードが送信されることはありません。
7. AP が syslog パケットを形成します。
8. WLC は、LI パケットかどうかを特定します。

   内容を更新します。

   IP：**Dst IP**：LI IP（v4 または v6）

   **Source IP**：Mgmt IP

   **Dst Mac**：GW Mac

   **Source Mac**：Mgmt Mac

   **UDP** Source Port：514

   **UDP Dest Port**：514
9. WLC は、内部 IP パケットに基づいて Mgmt IP を更新します。

   IPv4 の場合は、Mgmt IP が更新されます。

   IPv6 の場合は、Mgmt IPv6 が更新されます。
10. WLC は レコードを**保存しません**。
11. AP からの着信メッセージに関する**統計情報**は**記録されます**。

    統計情報は、WLC から syslog サーバへの送信メッセージについても記録されます。

    また、パケットが廃棄された場合はその他の統計情報も記録されます。
12. show コマンドを実行すると、常にログが表示されます。

# Netflow コレクタの syslog 形式

その後、syslog レコードは WLC から受信した設定に基づいて、AP から LI サーバへの UDP/IP ヘッダー内にカプセル化されます。

syslog レコードの形式は次のとおりです。

***“syslog header+’:’+ LI Header +’:’+ LI Record 1+’|’+ LI Record 2 +’|’+….”***

**syslog ヘッダー**

- Facility：Syslog ファシリティ コード。
- Severity：Syslog 重大度。
- Timestamp：AP が Syslog メッセージを送信した時刻。これは、可読日付形式（mmm dd yyyy hh:mm:ss）で送信されます。
- Hostname：AP の名前（RAP 名）
- Tag：Tag フィールドはペイロードで送信されるメッセージのタイプを示す文字列です（AP_LI_V4_FLOW/ AP_LI_V6_FLOW）。

**LI ヘッダー**：

“VVTTTTTTTTMMMMMMMMMMMM”

- VV：バージョン（現在は常に「01」です）
- TTTTTTTT：このロギングが作成された秒単位の時間（16 進数値）
- MMMMMMMMMMMM：AP の MAC アドレス（RAP の MAC アドレス）

**LI レコード（IPv4）**：

“MMMMMMMMMMM
AAAAA’A’A’A’BBBBCCCCCCCCCC’C’C’C’C’C’C’C’DDDDDDDDTTTTTTTTHHHHHHHH”

- MMMMMMMMMMM：クライアントの MAC アドレス（6 バイト）
- AAAA：16 進数（2 バイト）の送信元ポート
- A’A’A’A’：16 進数（2 バイト）の NAT 送信元ポート（上記の非 NAT の場合と同じです）
- BBBB：16 進数（2 バイト）の宛先ポート
- CCCCCCCC：16 進数（4 バイト）の送信元 IP アドレス
- C’C’C’C’C’C’C’C’：16 進数（4 バイト）の NAT 送信元 IP アドレス（上記の非 NAT の場合と同じです）
- DDDDDDDD：16 進数（4 バイト）の宛先 IP アドレス
- TTTTTTTT：フローが作成された秒単位の時間（4 バイト）
- HHHHHHHH：16 進数（4 バイトまたは 16 バイト）の RAP IP

**LI レコード（IPv6）（NAT IP およびポートは含まれません）**：

“MMMMMMMMMMM AAAABBBB
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDTTTTTTTTHHHHHHHH”

- F：IPv4 の場合は 0、IPv6 の場合は 1
- MMMMMMMMMMM：クライアントの MAC アドレス（6 バイト）
- AAAA：16 進数（2 バイト）の送信元ポート

- BBBB：16 進数（2 バイト）の宛先ポート
- CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC：16 進数（16 バイト）の送信元 IPv6 アドレス
- DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD：16 進数（16 バイト）の宛先 IPv6 アドレス
- TTTTTTTT：フローが作成された秒単位の時間（4 バイト）
- HHHHHHHH：16 進数（4 バイトまたは 16 バイト）の RAP IP

# CLI 設定と show コマンド

LI の有効化および無効化のための新しいコマンドが追加されます。

```
(Cisco Controller) >config flexconnect lawful-interception ?
disable        Disable Lawful-Interception.
enable         Enable Lawful-Interception.
syslog         Configure Lawful-Interception syslog.
timer          Configure Lawful-Interception timer value. Timer is periodic interval
[60sec - 600sec]
```

**前提条件**：Ap Syslog を使用するには、設定する必要があります。

1. 既存のコマンドを変更して、LI 変更を反映します。

   ```
   # config ap syslog host global <ipv4/ipv6>
   ```

   **前提条件**：IPv6 を設定するには、IPv6 が有効になっていて、IPv6 アドレスで管理が設定されているかどうかを確認する必要があります。

2. 統計情報を表示する新しい show コマンドがあります。

   ```
   (Cisco Controller) >show flexconnect lawful-interception ?
   summary        Display Lawful-Interception summary.
   Example of the LI show command on the controller:
   (Cisco Controller) >show flexconnect lawful-interception sum
   Lawful Interception Status: Disabled
   Lawful Interception Timer: 60
   Lawful Interception IPv4 Addr: 192.201.1.1
   Lawful Interception IPv6 Addr: Not Configured
   ```

（注） AP に設定されている LI サーバの IP とステータスを表示する show コマンドが追加されます。

AP 上の show LI コマンドの例。

```
AP-2802#show lawful-intercept
Enable: false
Interval(sec): 60
AP IPv4 Address: 1.5.39.108
AP IPv6 Address: ::
Max records: 15
syslog src ip: 192.201.1.2
syslog src ipv6: ::syslog
```

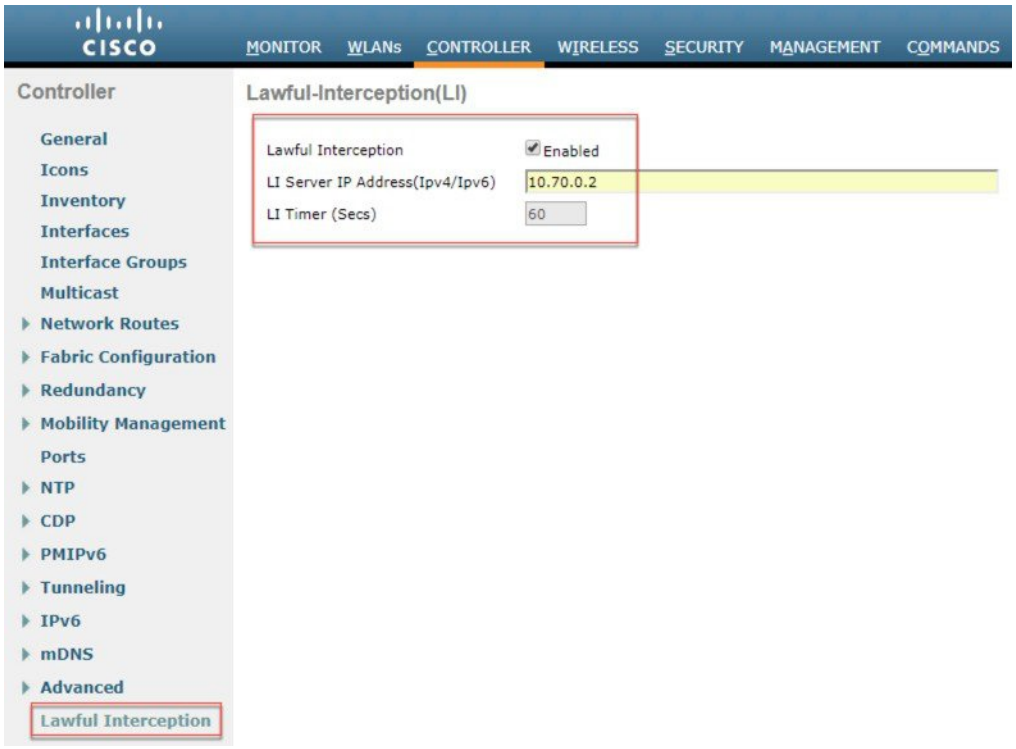
```
src mac: 00:01:02:03:04:09
extlog server ip: 0.0.0.0
extlog server ipv6: ::
extlog server mac: 00:8E:73:56:24:C7
ap name: AP-2802
```

# LI の GUI 設定

コントローラ GUI インターフェイスから合法的傍受を設定するには、次の手順を実行します。

**ステップ 1** コントローラの [Management] タブの [Logs] > [Config] でログ サーバの IP アドレスを設定します。


**ステップ 2** [Controller] タブで [Lawful Intercept] を選択し、設定したログ サーバの IP アドレスで有効化します。[Apply] をクリックします。




# リリース 8.8 での特定の URL のホワイトリスト作成

コントローラまたはAPで特定のURLのホワイトリスト機能を使用すると、ユーザはインターネットに接続せずに特定のサイトにアクセスできます。ホワイトリストに含まれている URL にアクセスする際に認証は必須ではありません。

- 顧客デバイスを「XXXX」SSID に関連付ける
- クライアントがIPアドレスを取得して、HTTPおよびHTTPSサイトの「**webauth**」required 状態に移行する
- クライアントは、認証なしでもホワイトリストの Web サイトにアクセスできる（たとえば、ユーザにロケーション固有の情報やその他の詳細情報を提供することができます）
- 特定の GP の（flex グループに基づく）一意のホワイトリスト URL はローカルの地域ポリシーに基づく
- ユーザがホワイトリスト ウォールド ガーデン プロファイルに設定されていない他の Web サイトに移動しようとすると、ログイン ページにリダイレクトされる
- ユーザは、認証された後はインターネット（ホワイトリストに含まれていない Web サイト）にアクセスできる

上記の機能は、8.7 リリース（DNS ACL）で実装された DNS-PreAuth ACL 機能で対処されていました。最大 20 のドメイン名を設定できます。スヌーピングされた IP アドレス（最大 64 個）は WLC に送信され、webauth_reqd 状態の AP 間でのクライアント ローミングに利用されます。クライアントは認証なしでこれらの URL を使用するため、事前設定済み URL のスヌーピングされた IP 間で送受信されるデータ トラフィックが AP で許可されます。

暗号化された HTTPS パケットは、クライアントが webauth_reqd 状態の場合にアクセスを許可または拒否するクリアテキスト URL 名を提供しないので、この要件に対応するには IP アドレス スヌーピングが必要です。

管理者は、ホワイトリストに含まれる URL のリストを使って preAuth ACL を設定し、特定の場所またはユーザに割り当てられている FlexConnect グループにマッピングする必要があります。

上記の機能の設定については、次のリンクにある 8.7 および 8.8 の FlexConnect 導入ガイドに記載されています。 https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-7/Flex_7500_DG.html#pgfId-167660

# リリース 8.8 でのキャプティブ ポータル設定

この機能は、ユーザが SSID（Flex グループ/VLAN ベース）ごとに複数のスプラッシュ ページを使用できるようにします。特定の場所にいるユーザが VLAN に基づいて分けられていても、同じ SSID（XXXX）が WLAN によってブロードキャストされるため、1 つの SSID で複数のスプラッシュ ページをサポートできる機能が必要です。

使用例：

- 顧客デバイスを「XXXX」SSID に関連付ける
- クライアントが IP アドレスを取得して、HTTP および HTTPS サイトの「**webauth**」required 状態に移行する
- 外部 Web 認証を介してカスタマイズされたキャプティブ ポータルを AP グループ設定に基づいてユーザに表示する

このシナリオでは、スケーリングに注意する必要があります。1 台の WLC に多くのリモート ロケーションが接続されている場合は、それぞれの場所に独自のキャプティブ ポータルが必要になります。たとえば、WLC 8540 は 6000 の AP をサポートできます。1 つのリモート ロケーションは 5 ～ 6 の AP を持つことができ、1 台の WLC8540 に最大 1000 のロケーションを接続できるため、WLC がリモート ロケーションごとに 1 つのスプラッシュ ページをサポートするには、1000 スプラッシュ ページをサポートすることになります。

WLC は現在、SSID ごとの外部リダイレクト URL 設定をサポートしています。この新しい機能では、1 つの SSID に複数の外部リダイレクト URL を使用できます。FlexConnect グループまたは AP グループは外部リダイレクト URL の設定入力を受け取り、グループにマッピングされた AP の背後にあるクライアントに適用する必要があります。

# CLI 設定と show

```
(WLC)config wlan apgroup custom-web global enable/disable <apgroup_name>

(WLC)config wlan apgroup custom-web ext-webauth-url add <ext-webauth-url> <apgroup_name>

 (WLC)config wlan apgroup custom-web ext-webauth-url delete <apgroup_name>
```

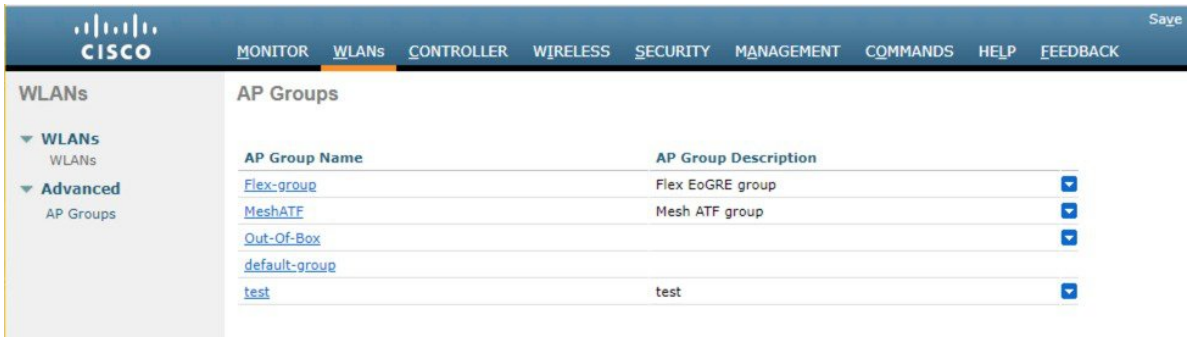
設定されているリダイレクト URL が既存の show ダンプに表示されます。

```
(WLC)show wlan apgroups
```

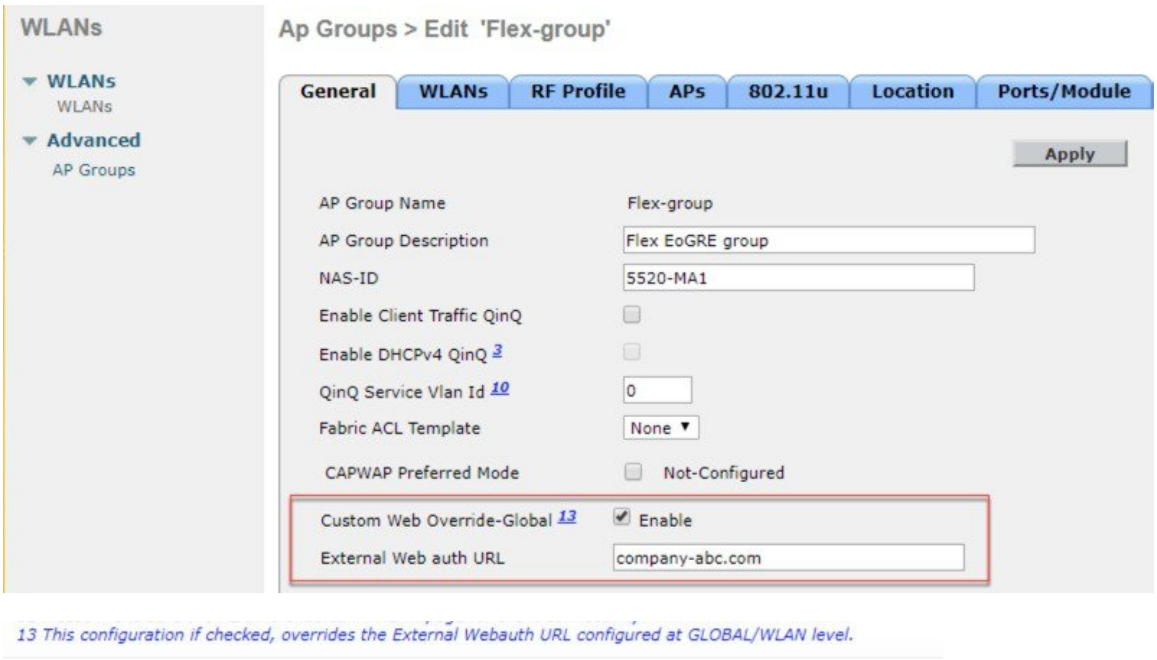
# キャプティブ ポータルの GUI 設定

コントローラ GUI からキャプティブ ポータルを設定するには、次の手順を実行します。

**ステップ 1** [WLAN] タブから [Advanced] > [AP Groups] を選択し、Flex グループを作成してから、キャプティブ ポータルを適用する FlexConnect グループを選択します。




**ステップ 2** 「カスタム web オーバーライド」を有効にして、「外部 WebAuth URL」を入力します。




（注） この機能では、同じ WLAN で異なるキャプティブ ポータルを使用して複数のグループを作成し、グローバル WLAN レベルで設定した外部 Webauth URL を上書きできます。

# リリース 8.8 でのポリシーの適用と割当量の管理

割当量の管理の場合：WLC は RADIUS ユーザ認証の変更要求を受け入れて、ユーザの接続を解除せずに同じユーザに異なる割当量を割り当てる必要があります。

この機能は以下でサポートされます。

- ローカル、ブリッジ（中央スイッチング）
- Flexconnect、Flex + ブリッジ（ローカル スイッチング）

**機能の使用例**：

- クライアントには、インターネットにアクセスするための 2 GB プランがあります
- AP が帯域幅の使用状況をモニタリングしてコントローラに統計情報をレポートします（帯域幅のモニタリング）
- コントローラは、IPv4 および（または）IPv6（デュアル スタック クライアント）の暫定アップデートを Radius サーバに送信します
- 特定の割当量が使い果たされるとすぐに、Radius は CoA を送信してポリシーを別のデフォルト プランに変更します（CoA オーバーライド）

- クライアントは、実際にネットワークから接続解除することなく新しいプランに移行します（即座に新しいポリシーを適用する）

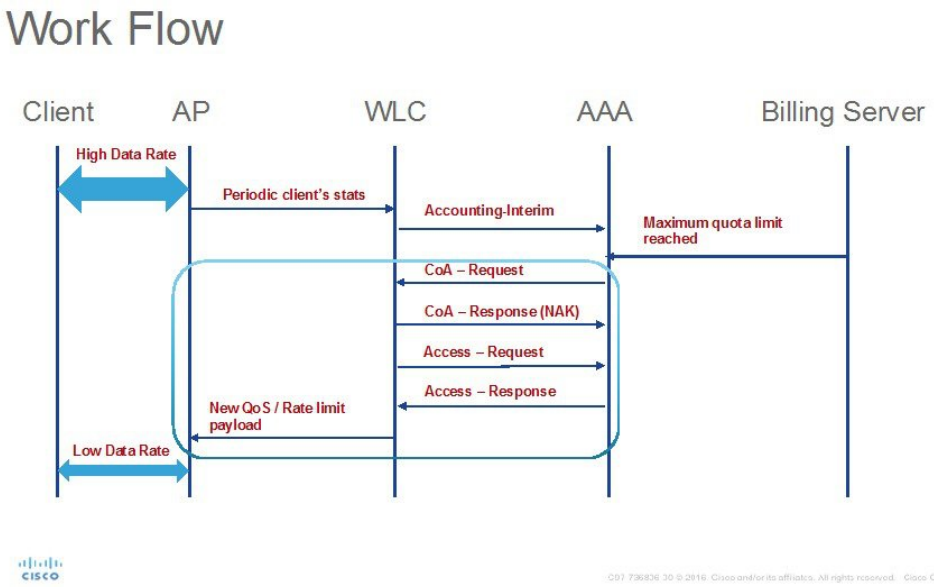
### AAA からのダイナミック ポリシー

- 802.11 クライアントには、AAA サーバでの認証時に QoS ポリシーとデータ レート制限が割り当てられます。
- WLC は「実行時」のポリシーの適用をサポートしていないため、クライアントは完全な認証時に新しいポリシーを取得します
- RFC 5176 により、Change-of-Authorization（CoA）要求/応答を使用したダイナミック レート制限が許可されています
- エンド クライアントは、プリペイドまたはポストペイドのデータ プランに基づいてサービス プロバイダーによって割り当てられた最大割当量でプロビジョニングされます
- 外部の課金サーバは、クライアントごとの最大データ制限に達すると AAA に通知します

### WLC での機能の実装

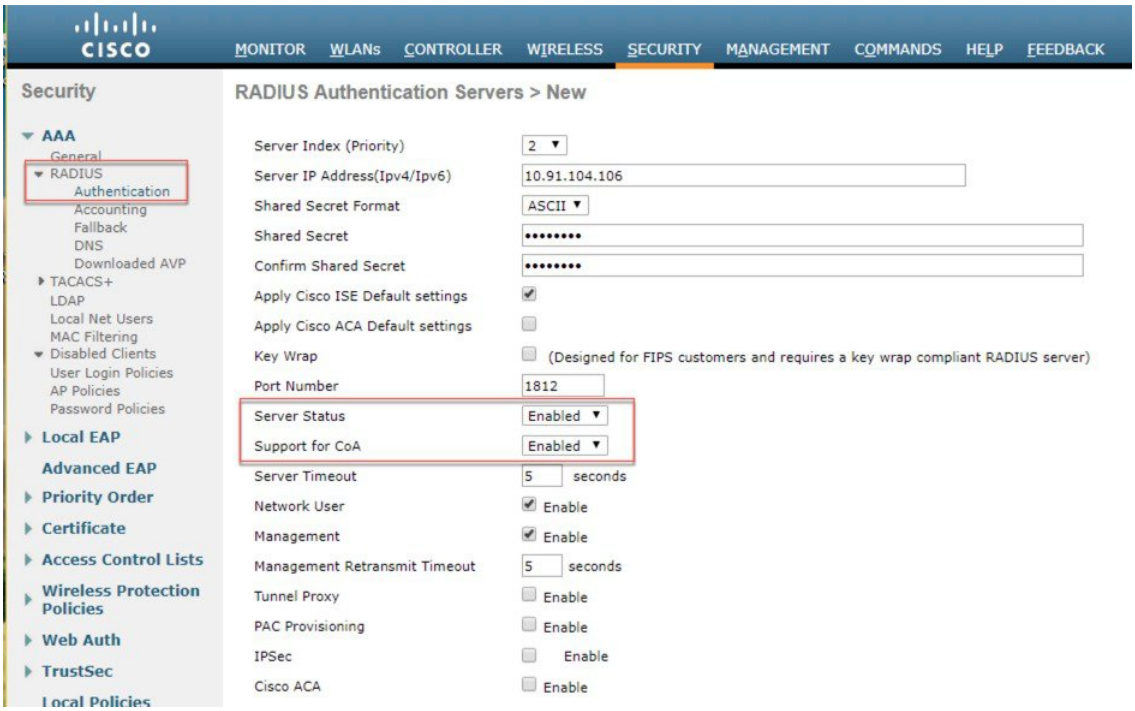
新しいポリシー/割当量を適用できるように、次の拡張機能が WLC で実装されています。

1. WLC は、クライアントの統計情報を使用して中間アカウンティングを定期的に AAA に送信します。
2. クライアントごとに割り当てられている最大割当量に達すると、AAA は service-type を「Authorize Only」に設定して state パラメータを指定した CoA-Request を送信します。
3. WLC は、CoA-NAK で service-type を「Authorize-Only」に設定して state パラメータを変更せずに応答します。
4. WLC は、service-type を「Authorize-Only」に設定して CoA-Request で受信した state パラメータを指定した Access-Request も AAA に送信します。
5. Access-Request では、CoA-Request で受信した他のセッションの属性/NAS を保持する同じ形式を使用します。
6. AAA は、レート/帯域幅の適用に関する新しいポリシーを使用した Access-Accept で応答します。
7. WLC は既存 の AP_AAA_QOS_PARAMS_PAYLOAD を使用して、これらの新しい QoS パラメータを AP に転送します。
8. AP は、新しい QoS 値を Flex ローカル スイッチド クライアントに適用します。
9. WLC または AP から、Disassociation/De-Authentication のメッセージがエンド クライアントに送信されることはありません。




# GUI からの設定

**ステップ 1** 次の例に示すように、[Security] > [Radius] > [Authentication] で [Support for CoA] を選択して認証サーバを設定します。



**ステップ 2** 以下に示すように、WLAN で AAA オーバーライドのオプションを選択します。