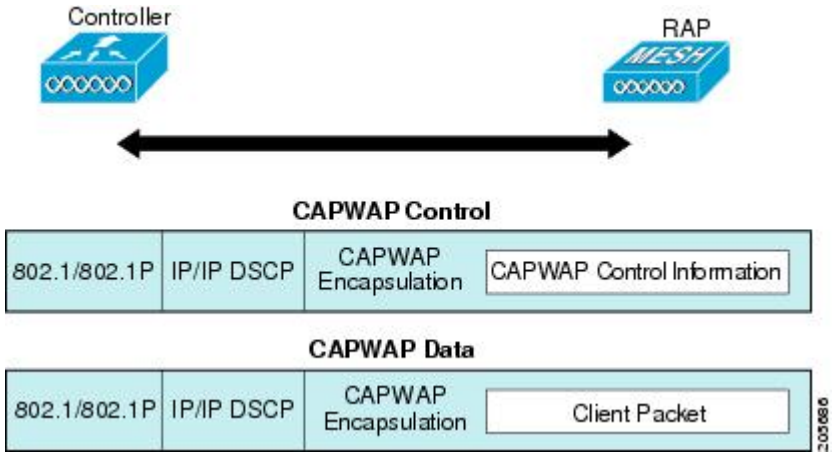
Cisco メッシュ アクセス ポイントのネットワークへの接続

この章では、ネットワークに Cisco メッシュ アクセス ポイントを接続する方法について説明します。

ワイヤレス メッシュは、有線ネットワークの 2 地点で終端します。1 つ目は、RAP が有線ネットワークに接続されているロケーションで、そこではすべてのブリッジ トラフィックが有線ネットワークに接続しています。2つ目は、CAPWAP コントローラが有線ネットワークに接続するロケーションです。そのロケーションでは、メッシュ ネットワークからの WLAN クライアント トラフィックが有線ネットワークに接続しています（図 1 : メッシュ ネットワーク トラフィックの終端 （1 ページ） を参照）。CAPWAP からの WLAN クライアント トラフィックはレイヤ 2 でトンネルされ、WLAN のマッチングは、コントローラが配置されている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、コントローラが接続されているネットワークのセキュリティ機能によって異なります。

図 *1:* メッシュ ネットワーク トラフィックの終端



（注） HSRP 設定がメッシュ ネットワークで動作中の場合は、入出力マルチキャスト モードを設定することを推奨します。マルチキャスト設定の詳細については、「Enabling Multicast on the Network (CLI)」の項を参照してください。

新しいコントローラ ソフトウェア リリースへのアップグレードの詳細については、http://www.cisco.com/en/US/products/ps10315/prod_release_notes_list.html の『*Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*』を参照してください。

メッシュとコントローラ ソフトウェアのリリースおよび互換性のあるアクセス ポイントの詳細については、http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html の『*Cisco Wireless Solutions Software Compatibility Matrix*』を参照してください。

この章の内容は、次のとおりです。

メッシュ ネットワークへのメッシュ アクセス ポイントの追加

この項では、コントローラがネットワーク内でアクティブで、レイヤ 3 モードで動作していることを前提としています。

（注） メッシュ アクセス ポイントが接続するコントローラ ポートは、タグなしでなければなりません。

メッシュ アクセス ポイントをネットワークに追加する前に、次の手順を実行します。

ステップ 1 メッシュ アクセス ポイントの MAC アドレスを、コントローラの MAC フィルタに追加します。「MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加」の項を参照してください。

ステップ 2 メッシュ アクセス ポイントのロール（RAP または MAP）を定義します。「メッシュ アクセス ポイントのロールの定義」の項を参照してください。

ステップ 3 コントローラでレイヤ 3 が設定されていることを確認します。「レイヤ 3 の設定の確認」の項を参照してください。

ステップ 4 各メッシュ アクセス ポイントに、プライマリ、セカンダリ、およびターシャリのコントローラを設定します。「DHCP 43 および DHCP 60 を使用した複数のコントローラの設定」の項を参照してください。

バックアップ コントローラを設定します。「バックアップ コントローラの設定」を参照してください。

ステップ 5 外部 RADIUS サーバを使用して、MAC アドレスの外部認証を設定します。「RADIUS サーバを使用した外部認証および許可の設定」を参照してください。

ステップ 6 グローバル メッシュ パラメータを設定します。「グローバル メッシュ パラメータの設定」の項を参照してください。

ステップ 7 バックホール クライアント アクセスを設定します。「拡張機能の設定」の項を参照してください。

ステップ 8 ローカル メッシュ パラメータを設定します。「ローカル メッシュ パラメータの設定」を参照してください。

ステップ 9 アンテナ パラメータを設定します。「アンテナ利得の設定」の項を参照してください。

ステップ 10 シリアル バックホールのチャネルを設定します。この手順は、シリアル バックホール アクセス ポイントにのみ適用できます。「シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除」の項を参照してください。

ステップ 11 メッシュ アクセス ポイントの DCA チャネルを設定します。「動的チャネル割り当ての設定」の項を参照してください。

ステップ 12 （必要に応じて）モビリティ グループを設定し、コントローラを割り当てます。『Cisco Wireless LAN Controller Configuration Guide』の「Configuring Mobility Groups」の章を参照してください。

ステップ 13 （必要に応じて）イーサネット ブリッジングを設定します。「イーサネット ブリッジングの設定」の項を参照してください。

ステップ 14 イーサネット VLAN タギング ネットワーク、ビデオ、音声などの拡張機能を設定します。「拡張機能の設定」の項を参照してください。

MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加

メッシュ ネットワーク内で使用するすべてのメッシュ アクセス ポイントのために、radio の MAC アドレスを適切なコントローラに入力する必要があります。コントローラは、許可リストに含まれる屋外無線からの discovery request にだけ応答します。コントローラでは、MAC フィルタリングがデフォルトで有効になっているため、MAC アドレスだけを設定する必要があります。アクセス ポイントが SSC を持ち、AP 認可リストに追加された場合は、AP の MAC アドレスを MAC フィルタリング リストに追加する必要はありません。

GUI と CLI のどちらを使用しても、メッシュ アクセス ポイントを追加できます。

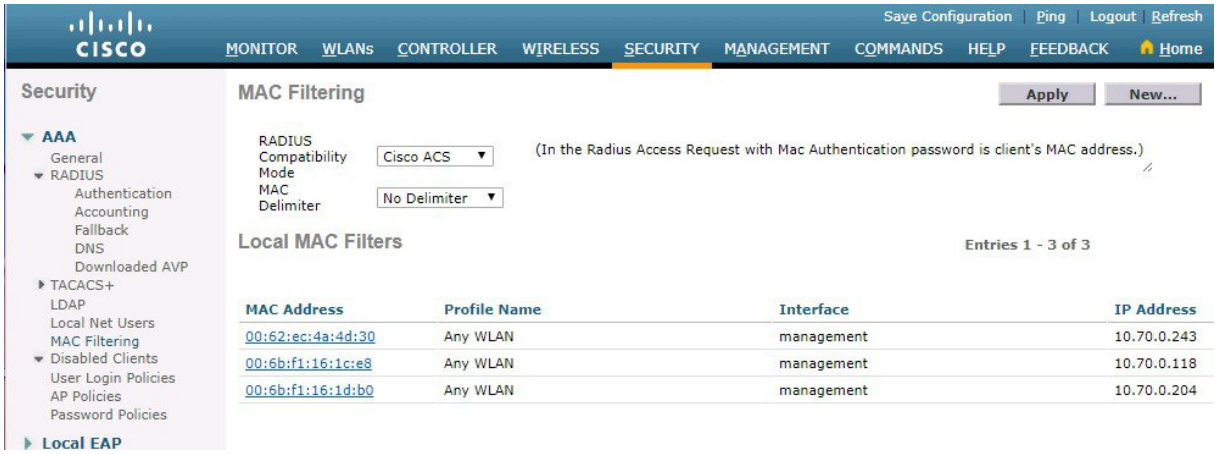
（注） メッシュ アクセス ポイントの MAC アドレスのリストをダウンロードして、Cisco Prime Infrastructure を使用してコントローラにプッシュすることもできます。

コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（GUI）

コントローラの GUI を使用してコントローラにメッシュ アクセス ポイントの MAC フィルタ エントリを追加する手順は、次のとおりです。

ステップ 1 [Security] > [AAA] > [MAC Filtering] を選択します。[MAC Filtering] ページが表示されます。

図 *2 : [MAC Filtering]* ページ



ステップ 2 [New] をクリックします。[MAC Filters > New] ページが表示されます。

ステップ 3 メッシュ アクセス ポイントの radio MAC アドレスを入力します。

（注） 1500 シリーズ屋外メッシュ アクセス ポイントの場合は、メッシュ アクセス ポイントの BVI MAC アドレスを MAC フィルタとして、コントローラで指定します。屋内メッシュ アクセス ポイントの場合は、イーサネット MAC を入力します。必要な MAC アドレスがメッシュ アクセス ポイントの外部に記載されていない場合は、アクセス ポイントのコンソールで **sh int | i** *hardware* コマンドを入力して、BVI およびイーサネット MAC アドレスを表示します。

ステップ 4 [Profile Name] ドロップダウン リストから、[Any WLAN] を選択します。

ステップ 5 [Description] フィールドで、メッシュ アクセス ポイントの説明を指定します。入力するテキストによって、コントローラでメッシュ アクセス ポイントが識別されます。

（注） たとえば、名前の略語と MAC アドレス最後の数桁（ap1522:62:39:10 など）を入力するという使い方ができます。ロケーションの詳細（屋上、ポール トップ、交差道路など）を記述することもできます。

ステップ 6 [Interface Name] ドロップダウン リストから、メッシュ アクセス ポイントを接続するコントローラ インターフェイスを選択します。

ステップ 7 [Apply] をクリックして、変更を確定します。この時点で、メッシュ アクセス ポイントが [MAC Filtering] ページの MAC フィルタのリストに表示されます。

ステップ 8 [Save Configuration] をクリックして、変更を保存します。

ステップ 9 この手順を繰り返して、追加のメッシュ アクセス ポイントの MAC アドレスを、リストに追加します。

コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（CLI）

コントローラの CLI を使用してコントローラにメッシュ アクセス ポイントの MAC フィルタ エントリを追加する手順は、次のとおりです。

ステップ 1 メッシュ アクセス ポイントの MAC アドレスをコントローラ フィルタ リストに追加するには、次のコマンドを入力します。

config macfilter add *ap_mac wlan_id interface* [*description*]

wlan_id パラメータの値をゼロ（0）にすると任意の WLAN を指定し、*interface* パラメータの値をゼロ（0）にするとなしを指定します。オプションの *description* パラメータには、最大 32 文字の英数字を入力できます。

ステップ 2 変更を保存するには、次のコマンドを入力します。

save config

メッシュ アクセス ポイントのロール定義

デフォルトでは、AP1500 は MAP に設定された radio のロールで出荷されます。RAP として動作させるには、メッシュ アクセス ポイントを再設定する必要があります。

MAP および RAP のコントローラへの接続に関する一般的な注意事項

一般的な注意事項は次のとおりです。

- MAP は常にイーサネット ポートをプライマリ バックホールとして設定し（イーサネット ポートが UP している場合）、802.11a/n/ac radio をセカンダリとして設定します。これによって、最初に、ネットワーク管理者がメッシュ アクセス ポイントを RAP として再設定する時間を取ることができます。ネットワークの高速コンバージェンスのために、メッシュ ネットワークに参加するまではイーサネット デバイスを MAP に接続しないことをお勧めします。
- UP しているイーサネット ポートでコントローラへの接続に失敗した MAP は、802.11a/n/ac radio をプライマリ バックホールとして設定します。MAP がネイバーを見つけられなかっ

た場合、またはネイバーを介してコントローラに接続できなかった場合、イーサネット ポートは再びプライマリ バックホールとして設定されます。

- イーサネット ポートを介してコントローラに接続されている MAP は、（RAP とは違って）メッシュ トポロジを構築しません。
- RAP は、常にイーサネット ポートをプライマリ バックホールとして設定します。
- イーサネット ポートが RAP で DOWN している場合、または RAP が UP しているイーサネット ポートでコントローラに接続できない場合は、802.11a/n/ac radio が 15 分間プライマリ バックホールとして設定されます。ネイバーを見つけられなかった場合、または 802.11a/n/ac radio 上でネイバーを介してコントローラに接続できない場合は、プライマリ バックホールがスキャン状態になります。プライマリ バックホールは、イーサネット ポートでスキャンを開始します。

AP ロールの設定（GUI）

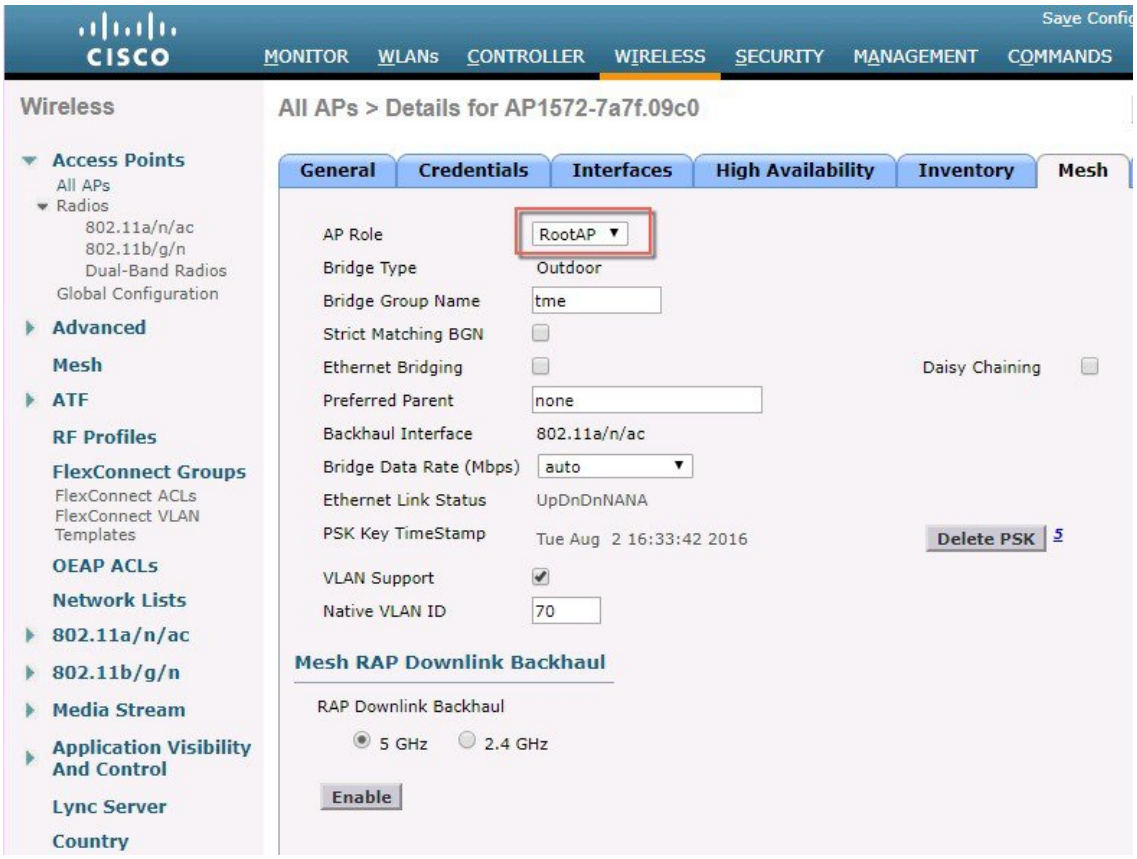
GUI を使用してメッシュ アクセス ポイントのロールを設定する手順は、次のとおりです。

ステップ 1 [Wireless] をクリックして、[All APs] ページを開きます。

ステップ 2 アクセス ポイントの名前をクリックします。[All APs > Details]（[General]）ページが表示されます。

ステップ 3 [Mesh] タブをクリックします。

図 *3 : [All APs > Details for]*（*[Mesh]*）ページ



ステップ 4 [AP Role] ドロップダウン リストから [RootAP] または [MeshAP] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

AP ロールの設定（CLI）

CLI を使用してメッシュ アクセス ポイントのロールを設定するには、次のコマンドを入力します。

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

DHCP 43 および DHCP 60 を使用した複数のコントローラの設定

組み込みの Cisco IOS DHCP サーバを使用して、メッシュ アクセス ポイント用に DHCP オプション 43 および 60 を設定する手順は、次のとおりです。

ステップ 1 Cisco IOS の CLI でコンフィギュレーション モードに切り替えます。

ステップ 2 DHCP プール（デフォルトのルータやネーム サーバなどの必要なパラメータを含む）を作成します。DHCP プールの作成に使用するコマンドは次のとおりです。

```
ip dhcp pool pool name
network IP Network Netmask
default-router Default router
dns-server DNS Server
```

値は次のとおりです。

```
pool name is the name of the DHCP pool, such as AP1520
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

ステップ 3 次の構文を使用してオプション 60 の行を追加します。

```
option 60 ascii “VCI string”
```

VCI 文字列の場合は、次のいずれかの値を使用します。引用符は必ず含める必要があります。

```
For Cisco 1570 series access points, enter “Cisco AP c1570”
For Cisco 1560 series access points, enter “Cisco AP c1560”
For Cisco 1530 series access points, enter “Cisco AP c1530”
For Cisco 1540 series access points, enter “Cisco AP c1540”
```

ステップ 4 次の構文に従って、オプション 43 の行を追加します。

```
option 43 hex hex string
```

16 進文字列には、次の TLV 値を組み合わせて指定します。

Type（型） + Length（長さ） + Value（値）

Type は、常に f1（16 進数）です。Length は、コントローラ管理 IP アドレスの個数の 4 倍の値を 16 進数で表したものです。Value は、一覧表示されるコントローラの IP アドレスを順番に 16 進数で表したものです。

たとえば、管理インターフェイスの IP アドレス 10.126.126.2 および 10.127.127.2 を持った 2 台のコントローラがあるとします。Type は、f1（16 進数）です。Length は、2 X 4 = 8 = 08（16 進数）です。IP アドレスは、0a7e7e02 および 0a7f7f02 に変換されます。文字列を組み合わせると f1080a7e7e020a7f7f02 になります。

DHCP スコープに追加された結果の Cisco IOS コマンドは、次のとおりです。

```
option 43 hex f1080a7e7e020a7f7f02
```

バックアップ コントローラ

中央の場所にあるコントローラは、ローカル地方にあるプライマリ コントローラとメッシュ アクセス ポイントとの接続が失われたときに、バックアップ コントローラとして機能できます。中央および地方のコントローラは、同じモビリティ グループに存在する必要はありません。コントローラの GUI または CLI を使用してバックアップ コントローラの IP アドレスを指定できるため、メッシュ アクセス ポイントは Mobility Group の外部にあるコントローラに対してフェール オーバーすることができます。

コントローラに接続しているすべてのアクセス ポイントに対してプライマリとセカンダリのバックアップ コントローラ（プライマリ、セカンダリ、ターシャリのコントローラが指定されていないか応答がない場合に使用される）や、ハートビート タイマーやディスカバリ要求タイマーなどの各種タイマーを設定することもできます。

（注） ファスト ハートビート タイマーはブリッジ モードのアクセス ポイントではサポートされていません。ファスト ハートビート タイマーは、ローカルおよび FlexConnect モードのアクセス ポイントでのみ設定されます。

メッシュ アクセス ポイントは、バックアップ コントローラのリストを保持し、定期的に primary discovery request をリストの各エントリに対して送信します。メッシュ アクセス ポイントがコントローラから新規の discovery response を受信すると、バックアップ コントローラのリストが更新されます。primary discovery request に 2 回連続で応答できなかったコントローラはすべて、リストから削除されます。メッシュ アクセス ポイントのローカル コントローラが応答しない場合は、バックアップ コントローラのリストから使用可能なコントローラが選択されます。選択される順序は、プライマリ コントローラ、セカンダリ コントローラ、ターシャリ コントローラ、プライマリ バックアップ、そしてセカンダリ バックアップです。メッシュ アクセス ポイントは、バックアップ コントローラのリストで最初に使用可能なコントローラからの discovery response を待ち、プライマリ ディスカバリ要求タイマーに設定された時間内に discovery response を受信した場合はそのコントローラに join します。タイマーの制限に達すると、メッシュ アクセス ポイントは、コントローラに join できなかったと見なし、バックアップ コントローラのリストで次に使用可能なコントローラからの discovery response を待ちます。

（注） メッシュ アクセス ポイントのプライマリ コントローラが復帰すると、メッシュ アクセス ポイントはバックアップ コントローラとの接続を解除し、プライマリ コントローラに再接続します。メッシュ アクセス ポイントは、設定されているセカンダリ コントローラではなく、プライマリ コントローラにフォールバックします。たとえばプライマリ、セカンダリ、およびターシャリのコントローラが設定されているメッシュ アクセス ポイントの場合、プライマリとセカンダリのコントローラが応答しなくなると、ターシャリ コントローラにフェール オーバーします。その後、プライマリ コントローラが復帰するまで待って、プライマリ コントローラにフォール バックします。セカンダリ コントローラが復帰しても、メッシュ アクセス ポイントはターシャリ コントローラからセカンダリ コントローラにフォール バックせず、プライマリ コントローラが復帰するまでターシャリ コントローラに接続したままになります。

RADIUS サーバを使用した外部認証および認可の設定

リリース 7.0 以降では、Cisco ACS（4.1 以降）や ISE などの RADIUS サーバを使用した、メッシュ アクセス ポイントの外部認証および認可がサポートされています。RADIUS サーバは、クライアント認証タイプとして、証明書を使用する EAP-FAST をサポートする必要があります。

メッシュ ネットワーク内で外部認証を使用する前に、次の変更を行う必要があります。

- AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。
- コントローラも、RADIUS サーバで設定する必要があります。
- 外部認証および認可用に設定されたメッシュ アクセス ポイントを RADIUS サーバのユーザ リストに追加します。
  - 詳細については、「RADIUS サーバへのユーザ名の追加」の項を参照してください。
- RADIUS サーバで EAP-FAST を設定し、証明書をインストールします。802.11a インターフェイスを使用してメッシュ アクセス ポイントをコントローラに接続する場合には、EAP-FAST 認証が必要です。外部 RADIUS サーバは、Cisco Root CA 2048 を信頼する必要があります。CA 証明書のインストールと信頼については、「RADIUS サーバの設定」の項を参照してください。

（注） ファスト イーサネットまたはギガビット イーサネット インターフェイスを使用してメッシュ アクセス ポイントをコントローラ接続する場合は、MAC 認可だけが必要です。

（注） また、この機能は、コントローラ上のローカル EAP および PSK 認証をサポートしています。

RADIUS サーバの設定

RADIUS サーバに CA 証明書をインストールして信頼するように設定する手順は、次のとおりです。

ステップ 1 次の場所から Cisco Root CA 2048 の CA 証明書をダウンロードします。

- https://www.cisco.com/security/pki/certs/crca2048.cer
- https://www.cisco.com/security/pki/certs/cmca.cer

ステップ 2 次のように証明書をインストールします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [ACS Certification Authority Setup] をクリックします。
b) [CA certificate file] ボックスに、CA 証明書の場所（パスと名前）を入力します（たとえば、c:\Certs\crca2048.cer）。
c) [Submit] をクリックします。`

ステップ 3 次のように外部 RADIUS サーバを設定して、CA 証明書を信頼するようにします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [Edit Certificate Trust List] の順に選択します。[Edit Certificate Trust List] が表示されます。
b) 証明書の名前（[Cisco Root CA 2048 (Cisco Systems)]）の横にあるチェックボックスを選択します。
c) [Submit] をクリックします。`
d) ACS を再起動するには、[System Configuration] > [Service Control] の順に選択してから、[Restart] をクリックします。

Cisco ACS サーバに関する追加の設定詳細については、次のドキュメントを参照してください。

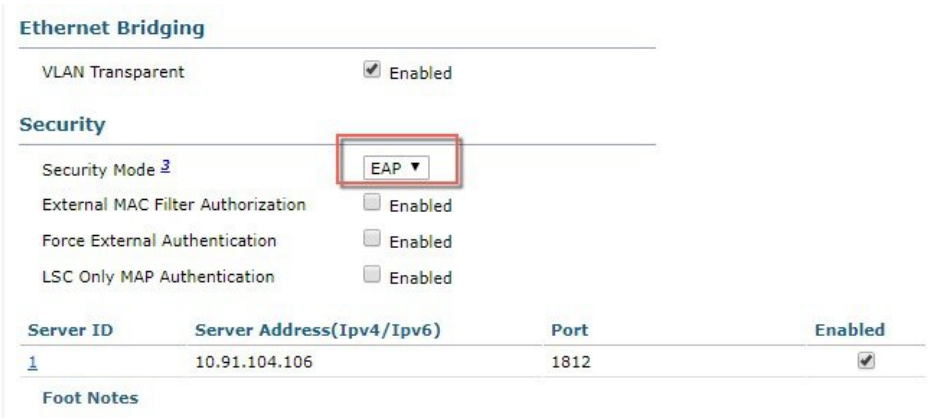
- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html（Windows）
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/（UNIX）

メッシュ アクセス ポイントの外部認証の有効化（GUI）

GUI を使用してメッシュ アクセス ポイントの外部認証を有効にする手順は、次のとおりです。

ステップ 1 [Wireless] > [Mesh] を選択します。[Mesh] ページが表示されます（図 4 : [Mesh] ページ （11 ページ） を参照）。

図 *4 : [Mesh]* ページ



ステップ 2 セキュリティ セクションで、[Security Mode] ドロップダウン リストから [EAP] オプションを選択します。

ステップ 3 [External MAC Filter Authorization] オプションと [Force External Authentication] オプションの [Enabled] チェックボックスを選択します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

RADIUS サーバへのユーザ名の追加

メッシュ アクセス ポイントの RADIUS 認証を有効にする前に、外部 RADIUS サーバによって認可および認証されるメッシュ アクセス ポイントの MAC アドレスをサーバのユーザ リストに追加します。

リモート認可および認証の場合、EAP-FAST は製造元の証明書（CERT）を使用して、子メッシュ アクセス ポイントを認証します。また、この製造元証明書に基づく ID は、ユーザの確認においてメッシュ アクセス ポイントのユーザ名として機能します。

Cisco IOS ベースのメッシュ アクセス ポイントの場合は、MAC アドレスをユーザ リストに追加するだけでなく、*platform_name_string–MAC_address* 文字列をユーザ リストに入力する必要があります（たとえば、c1240-001122334455）。コントローラは最初に MAC アドレスをユーザ名として送信します。この初回の試行が失敗すると、コントローラは *platform_name_string–MAC_address* 文字列をユーザ名として送信します。

（注） 認証 MAC アドレスは屋内と屋外の AP で異なります。屋内 AP が AP のギガビット イーサネット MAC アドレスを使用するのに対して、屋外 AP は、AP の BVI MAC アドレスを使用します。

RADIUS サーバのユーザ名エントリ

各メッシュ アクセス ポイントのために、2 つのエントリ *platform_name_string-MAC_address* 文字列と、その後にハイフンで区切られた MAC アドレスを RADIUS サーバに追加する必要があります。次に例を示します。

- platform_name_string-MAC_address

  ユーザ：c1570-aabbccddeeff

  パスワード：cisco

- ハイフンで区切られた MAC アドレス

  ユーザ：aa-bb-cc-dd-ee-ff

  パスワード：aa-bb-cc-dd-ee-ff

（注） AP1552 プラットフォームは c1550 のプラットフォーム名を使用します。AP1572 は c1570 のプラットフォーム名を使用します。

メッシュ アクセス ポイントの外部認証の有効化（CLI）

CLI を使用してメッシュ アクセス ポイントの外部認証を有効にするには、次のコマンドを入力します。

ステップ 1 **config mesh security eap**

ステップ 2 **config macfilter mac-delimiter colon**

ステップ 3 **config mesh security rad-mac-filter enable**

ステップ 4 **config mesh radius-server** *index* **enable**

ステップ 5 **config mesh security force-ext-auth enable**（任意）

セキュリティ統計情報の表示（CLI）

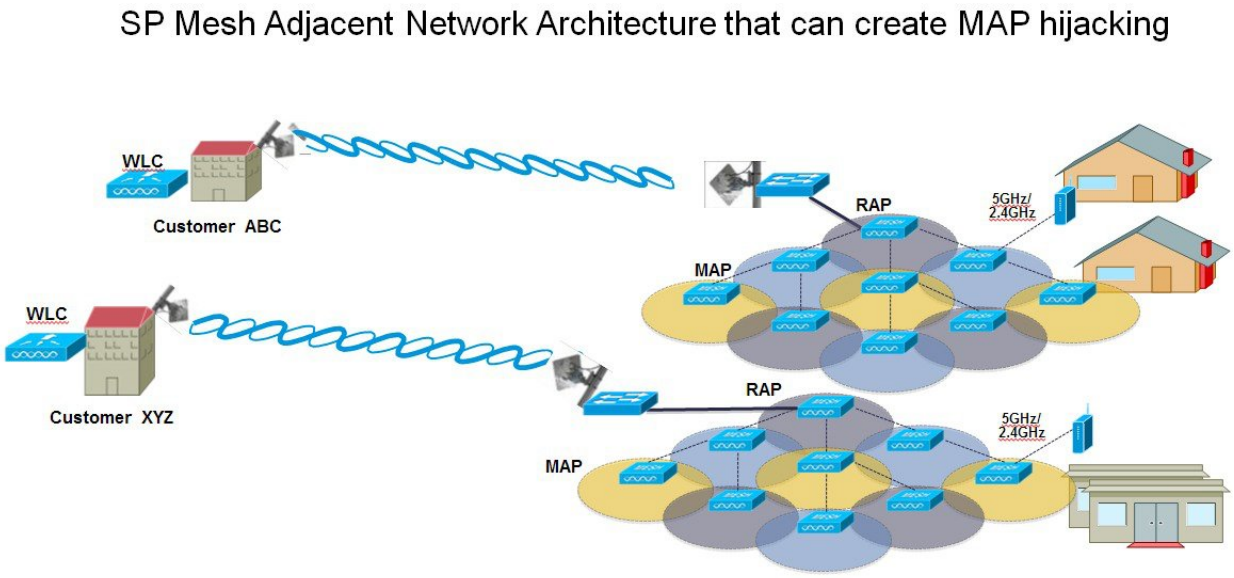
CLI を使用してメッシュ アクセス ポイントのセキュリティ統計を表示するには、次のコマンドを入力します。

show mesh security-stats *Cisco_AP*

このコマンドを使用すると、指定のアクセス ポイントとその子アクセス ポイントのパケット エラー統計、エラー数、タイムアウト数、アソシエーションと認証の成功数、再アソシエーション数、および再認証数が表示されます。

リリース8.2でのMesh PSK Keyを使ったプロビジョニング

Cisco Mesh の導入時に、ワイルドカードの MAC フィルタリングで AAA を使用し MAP 接続を許可する場合、メッシュアクセスポイント（MAP）が現在join中のネットワークから離れて、別のメッシュ ネットワークへ join することがあります。メッシュ AP のセキュリティが EAP-FAST を RADIUS 認証として使用しているため、この動作を制御できません。EAP セキュリティでは AP の MAC アドレスとタイプの組み合わせが使用されるため、制御設定を使用できないためです。PSK オプションでデフォルトのパスフレーズを使用すると、セキュリティ リスクとハイジャックの危険性が伴います。この問題は、MAP が移動車両（公共交通機関、フェリー、船など）で使用されるときに、2 つの異なる SP の重複導入で顕著に現れます。この場合、MAP は特定の SP のメッシュ ネットワークに固定される必要がなくなるため、MAP を別の SP ネットワークによって乗っ取られたり、使用されることがあります。こうした導入環境では SP の対象顧客にサービスを提供できなくなります。



8.2 リリースで導入された新しい機能は、メッシュ導入を制御し、現在使用されているデフォルトの「**cisco**」PSK を超える MAP のセキュリティの強化に役立つ（WLC からプロビジョニングできる）PSK 機能を有効にします。この新機能によって、カスタム PSK で設定した MAP は、RAP および WLC を使用して認証を行う場合に強化されたキーを使用します。コントローラ ソフトウェア リリース 8.1 以下からアップグレードするかリリース 8.2 からダウングレードする場合は、特別な注意が必要です。管理者は MAP ソフトウェアで PSK を有効化/無効化する際の影響を理解する必要があります。

サポートされるワイヤレス メッシュのコンポーネント

- 3504、WiSM-2、5508、5520、7500 および 8500 シリーズ ワイヤレス LAN コントローラ
- メッシュ AP 1550、1530、1540（リリース 8.5）、1560（リリース 8.4）、または 1570 シリーズおよび屋内メッシュ サポートの AP のすべて
- ワイヤレス クライアント（タブレット、スマートフォンなど）。

機能の設定手順

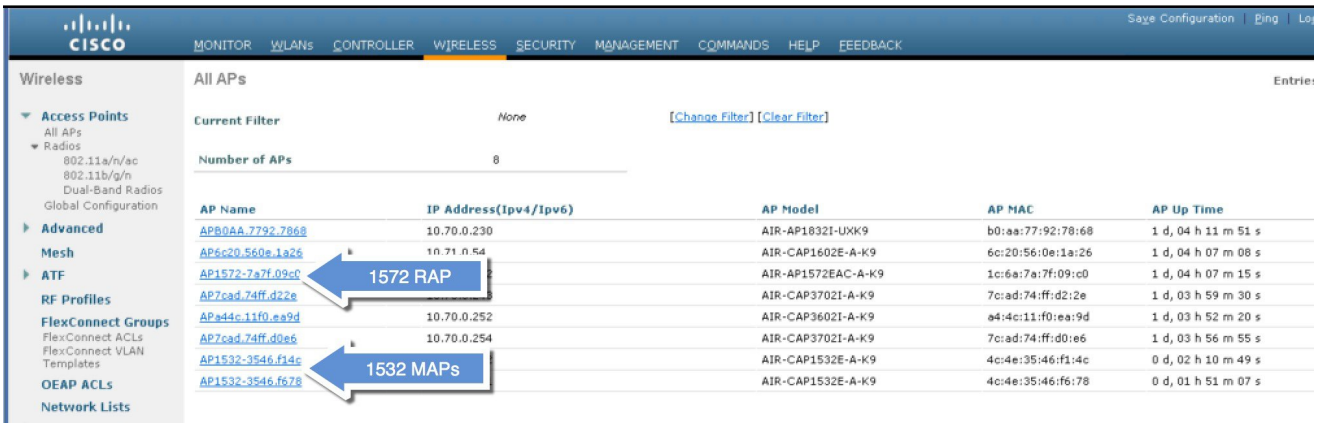
管理者はセキュリティ モードを PSK として設定する必要があります。また任意で新しい PSK を設定します。PSK が設定されていない場合、MAP はデフォルト PSK キー「**cisco**」で WLC に join することはできません。

- プロビジョニングは、各 WLC にローカルであること
- ローカル プロビジョニングを可能にするために「有効化」された状態であること
- WLC に従うキー強度（小文字、大文字の特殊文字の組み合わせを含む英数字、長さ 3 ～ 32 文字、特殊文字をサポート、冗長なパスワードはサポートされない）。

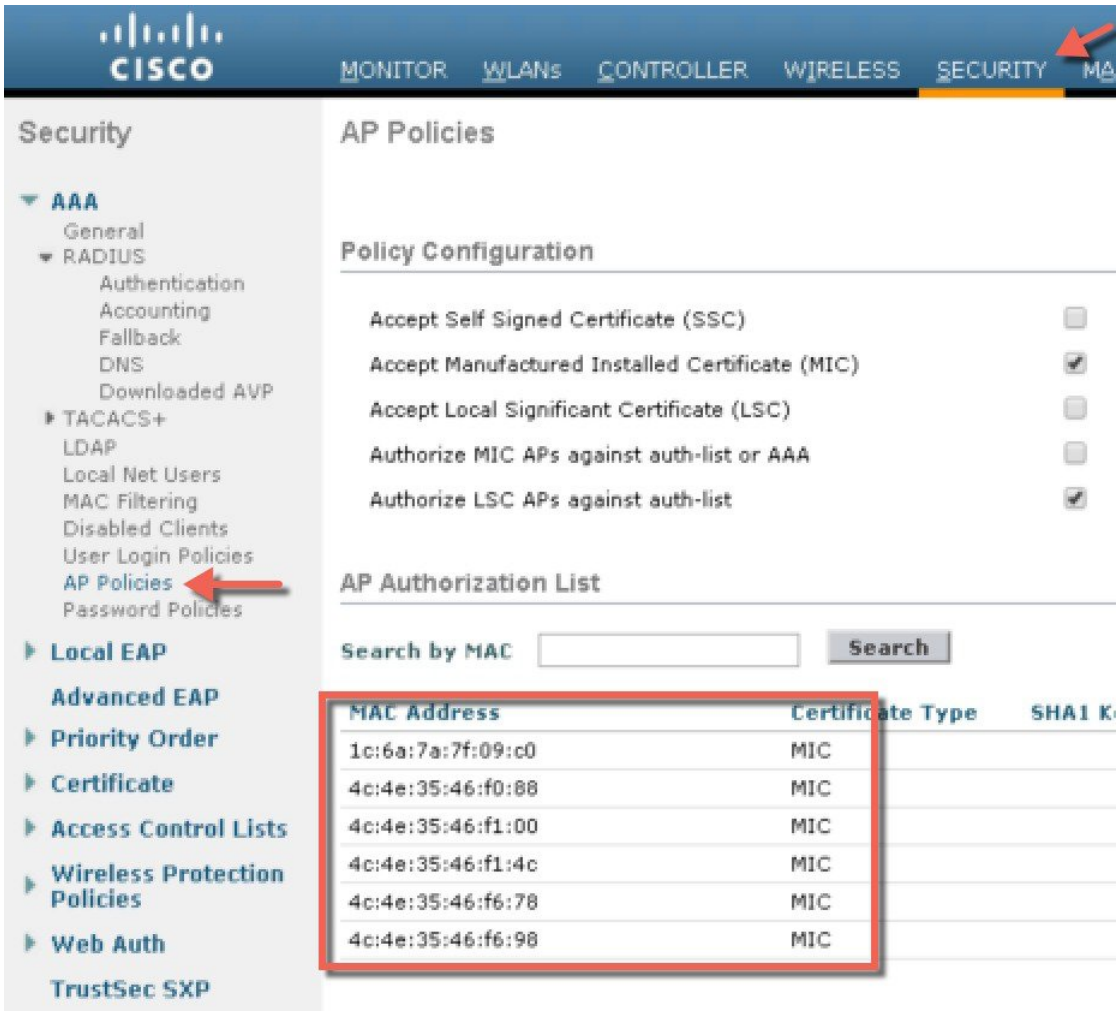
- プロビジョニングされたPSKは、WLCで暗号化され、保存され、暗号化された形式でAPに送信される。

メッシュ PSK GUI の設定

ステップ 1 本ガイドで先述したように、コントローラに RAP を接続します。下記の設定の図の例では、2 台の 1532 MAP が RAP 1572 に接続しています。

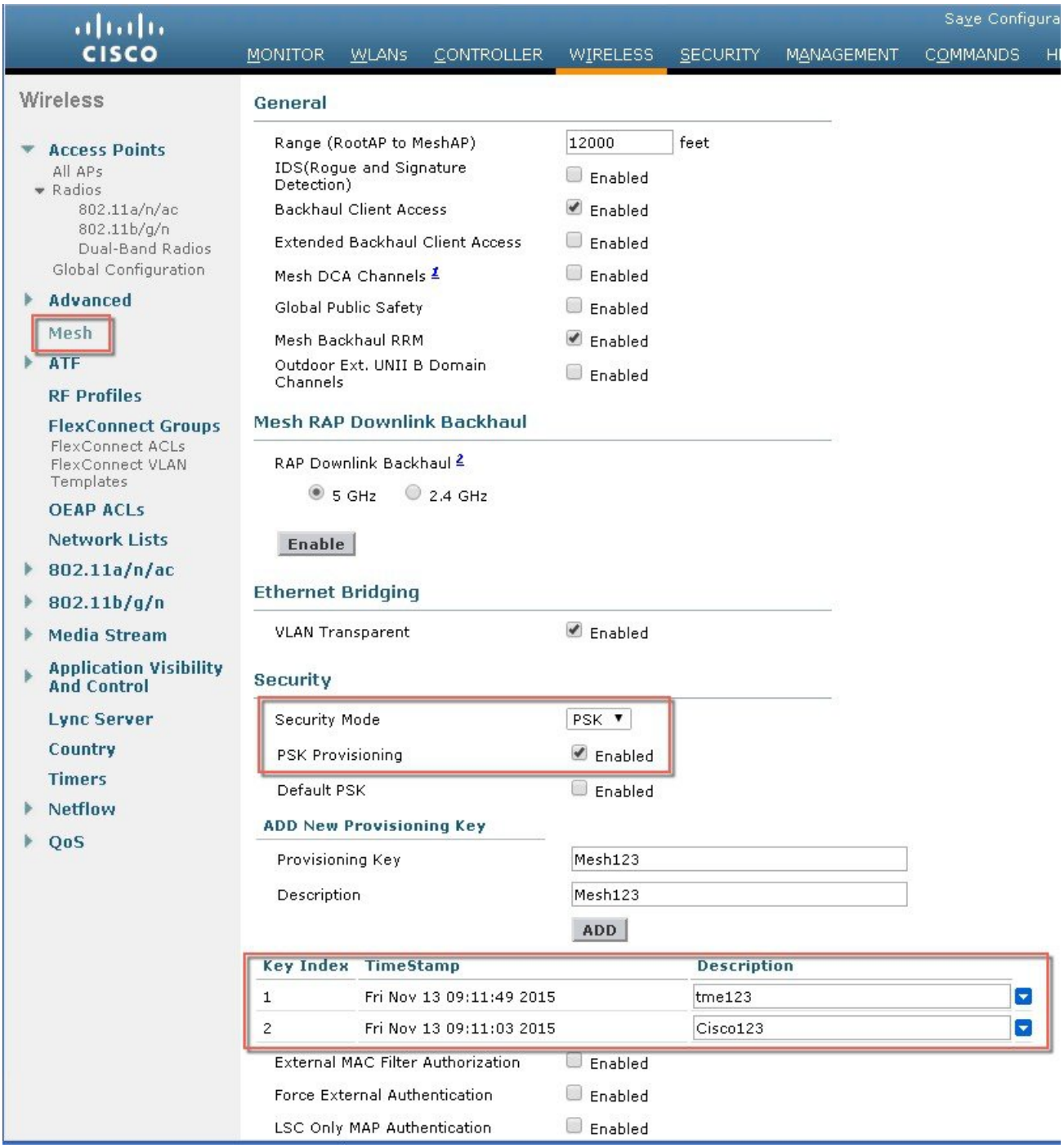


本ガイドに示すように、MAPの初期接続のオプションの1つとして、スクリーンショットのように、MAPをRAPに接続するために、コントローラにMAPのMACアドレスを入力する必要があります。



ステップ 2 [Wireless] > [Mesh] メニューから、PSK として [Security Mode] を選択し、[PSK Provisioning] を有効にします。

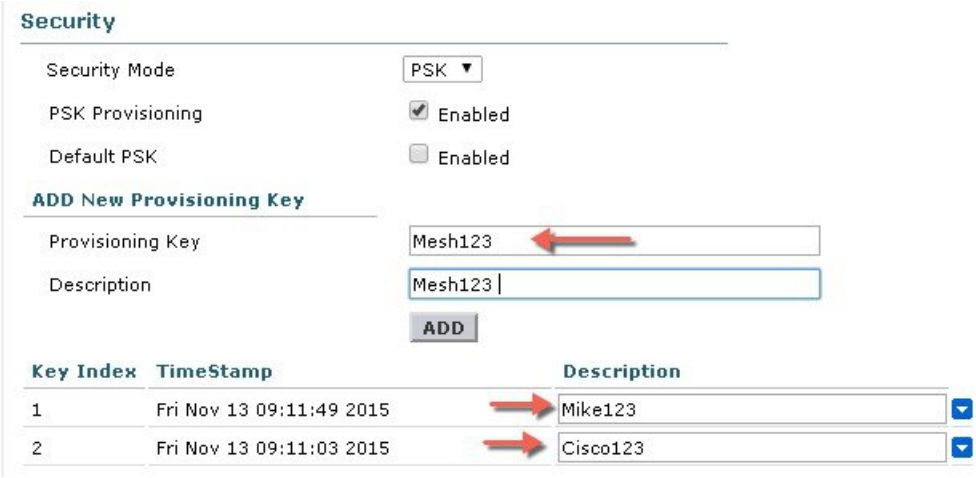
リリース 8.2 MAC 以前のワイルド カード文字を含む AAA 認証または EAP 認証には、EAP をデフォルトの内部認証と共に使用する 3 通りの方法しかありませんでした。一部の場合（特に、異なる顧客からメッシュのインストールが重複する場合）は MAC アドレス プロビジョニングが十分に信頼できず、メッシュ AP が別のメッシュ ネットワークから偶然にも乗っ取られる高い危険性がありました。これにより、メッシュ導入における多くの問題やカバレッジ ホールを生じる可能性もありました。そのため、リリース 8.2 では PSK MAP プロビジョニングが導入されました。上記のように PSK キーをワイヤレス コントローラに作成する必要があります。



ステップ 3 例に示すようにプロビジョニング キーを入力して [ADD] を押し、入力された値を適用します。

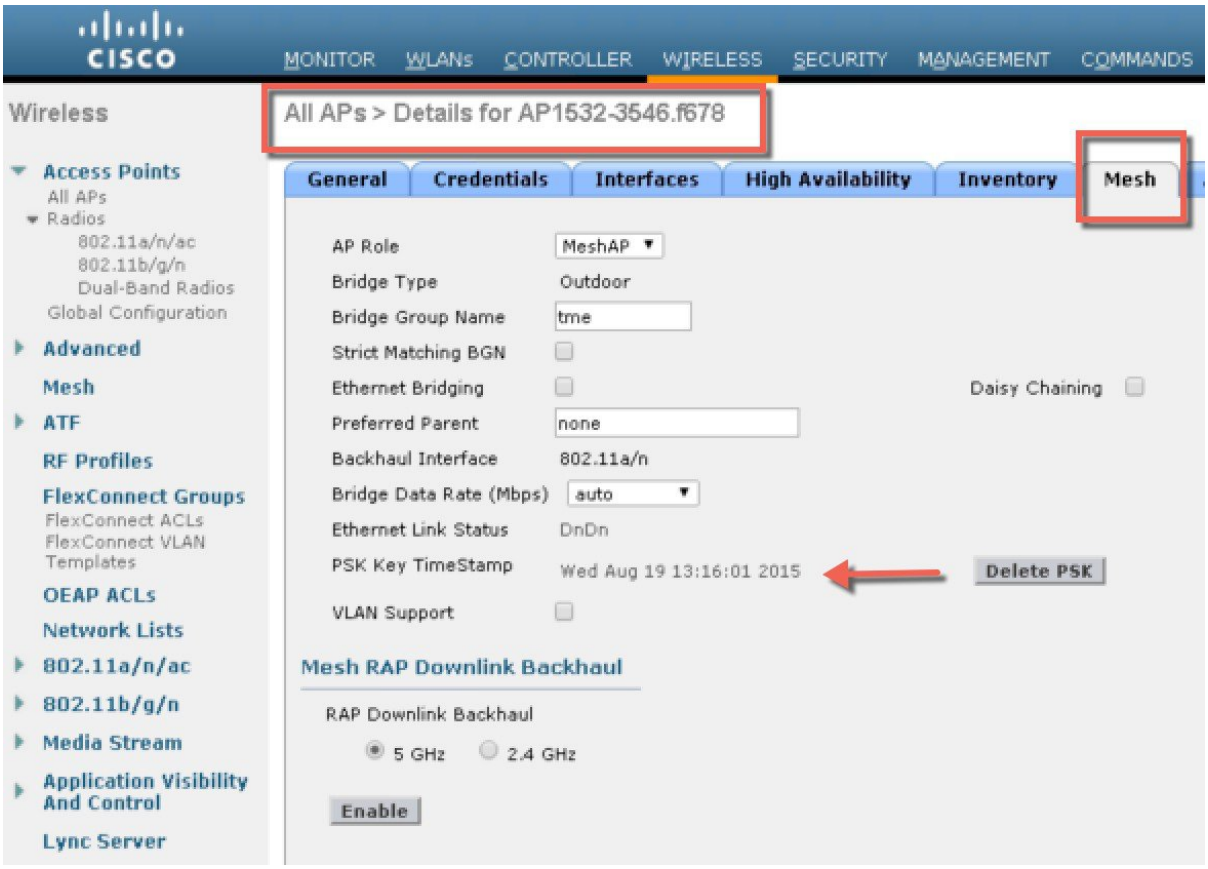
キーの値は一覧に表示されませんが、キーがコントローラにプロビジョニングされる際はタイム スタンプ付きのキーのインデックスだけが表示されます。最大 5 つのキーをプロビジョニングに使用される MAP のコントローラに入力できます。これら 5 つのキーはコントローラのフラッシュに常時保存されており、

MAP によるプロビジョニングではいずれかを使用できます。プロビジョニングされた PSK が MD5 暗号化アルゴリズム（128-bit）により暗号化され、新しいキーの設定時に AP に送信されます。

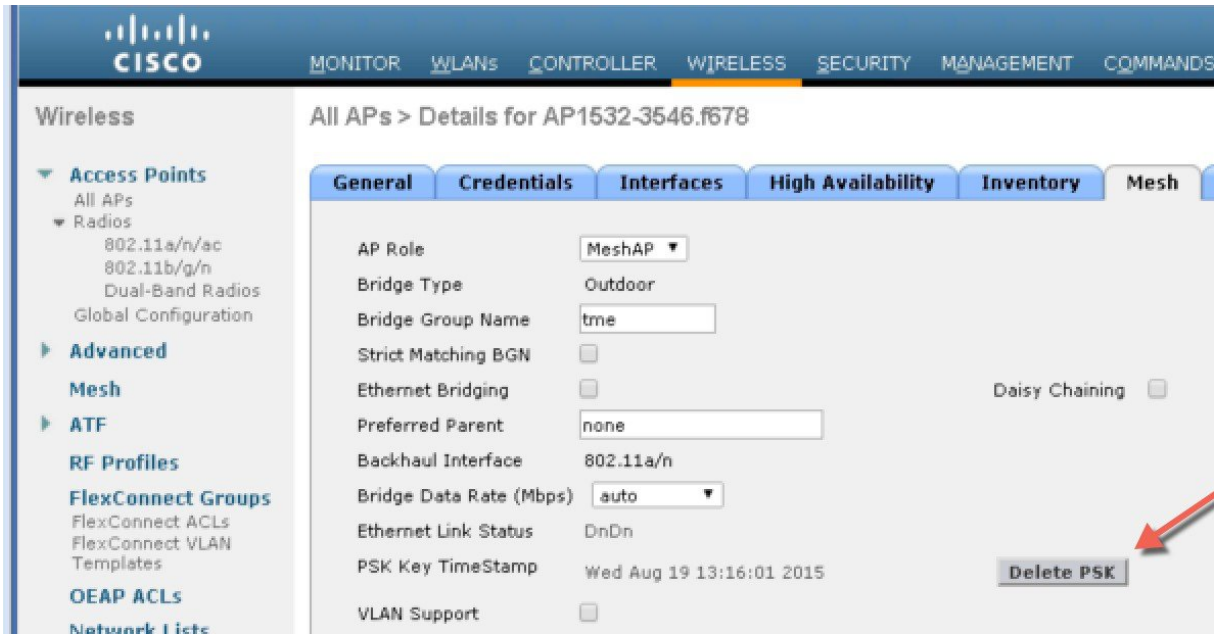


ステップ 4 設定および有効化された PSK キーがコントローラに提供されると、キーは RAP でプロビジョニングされ、その RAP に接続されたすべての MAP に伝播されます。同じキーは、メッシュ ネットワーク内の他の子 MAP すべてに伝播されます。MAP 上で PSK キーの受信と RAP/MAP ネットワークへの認証を行うのに、必要な操作はありません。

例に示すように、RAP に接続された 1 つの特定の MAP を [Mesh] タブで確認する場合、インデックス 1 および 8 月 19 日からのタイム スタンプ付きの PSK キーを使用して MAP がプロビジョニングされていることを確認できます。



ステップ 5 PSK キーがコントローラ上で失われたか、または意図的に削除された場合、プロビジョニングされた PSK キーは MAP または RAP から 削除できます。



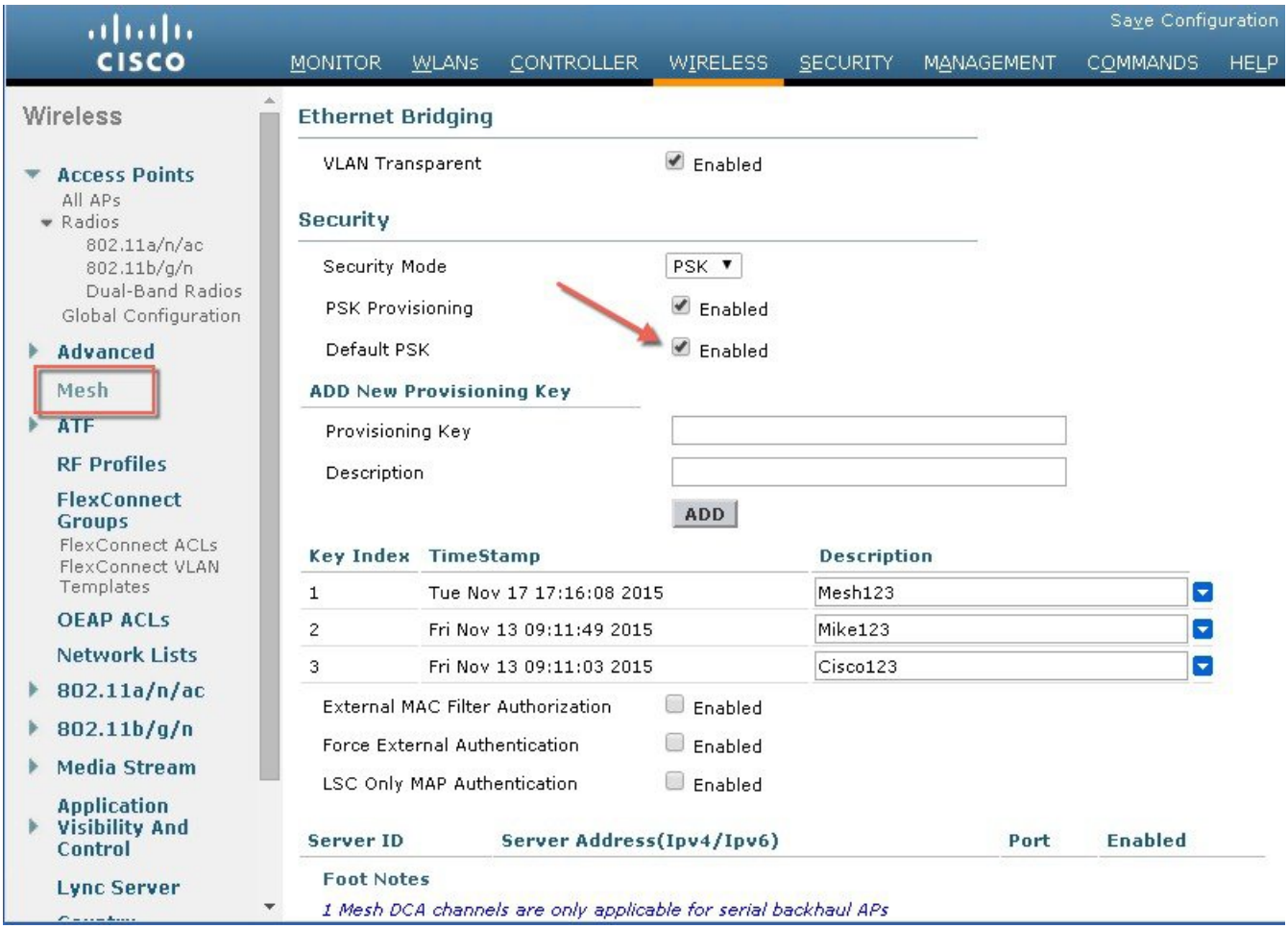
ステップ 6 このため、MAP が誤ったネットワークに接続してキーを取得した場合でも、管理者は誤った PSK キーを削除できます。さらに、EAP セキュリティで join した場合でも、WLC GUI インターフェイスで PSK タイムスタンプの [Delete PSK] を使用すれば、AP からプロビジョニング済み PSK を削除できます。このオプションは、AP が孤立状態になるか、無効な PSK/EAP セキュリティを使用して孤立状態のメッシュ AP に再 join した場合に、メッシュ AP リカバリ手段として利用できます。PSK キーが MAP から削除されると、デフォルト PSK キーが「cisco」に戻ります。

（注）

- パスフレーズ「cisco」を使用して PSK を設定しても、「シスコのデフォルト PSK」を使用しているとは限りません。プロビジョニングされた PSK は、「シスコのデフォルト PSK」とは無関係に機能します。
- RAP の PSK キーを削除すると、RAP が MAP にならない限り適用されません。

ただし、PSK キーがすでにコントローラおよび RAP/MAP で設定されている場合、一致する PSK キーが無い MAP はメッシュ ネットワークに接続できません。プロビジョニングされていない MAP を、コントローラで PSK が有効化されたメッシュ ネットワークに接続するには、[Provisioning] ウィンドウが有効化されている必要があります。

例に示すように、[Provisioning] ウィンドウを手動で有効にすると、デフォルトの「cisco」PSK キーを使用して MAP が接続可能になり、同時に新しい PSK キーを取得します。



（注） メッシュ管理者にとって重要なことは、デフォルトの PSK キーを持つ MAP がプロビジョニング済みのメッシュ ネットワークに接続しないように、デフォルトの [Provisioning] ウィンドウを無効にすることです。

次のシナリオはメッシュ AP が孤立する原因になる可能性があるため、必ずこれらの設定ミスを回避するように注意してください。

- 設定済み AP はデフォルト PSK を使用して join しようとするが、WLC でデフォルトまたは [PSK Provisioning Window] オプションが有効になっていない
- WLC でプロビジョニングされた PSK を忘れた（PSK の説明をメモしておけば、忘れたときに便利です。プロビジョニングされた PSK の保存またはリカバリは AP 上で実行する必要があります。）

モビリティ グループのコントローラを使用したメッシュ PSK のプロビジョニング

モビリティ グループで RAP が設定されている場合、モビリティ グループの全コントローラに対して同じ PSK キーを使用するか、または 5 つの認可 PSK キーのうちの 1 つを使用すること

が常に推奨されます。この方法により、異なるコントローラからの MAP でも認証できます。PSK のスタンプを見れば、MAP および PSK キーの作成元を確認できます。

マルチコントローラの設定で PSK または EAP セキュリティのメッシュ AP を設定する場合の推奨事項を次に示します。

- すべてのコントローラで同じ PSK が必要です。異なるキーを持つ WLC は、RAP および MAP がその間で移動すると予期しない動作が生じ、長時間の停止を引き起こす場合もあります。
- すべてのコントローラは、同じセキュリティ方式に設定する必要があります。（プロビジョニングを有効化および PSK を作成した）EAP と PSK の併用は推奨されません。

PSK プロビジョニング用の CLI コマンド

- config mesh security psk provisioning enable/disable
- config mesh security psk provisioning key <pre-shared-key>
- config mesh security psk provision window enable/disable
- config mesh security psk provisioning delete_psk <ap|wlc> <ap_name|psk_index>”

グローバル メッシュ パラメータの設定

この項では、メッシュ アクセス ポイントがコントローラとの接続を確立するための設定の手順について説明します。内容は次のとおりです。

- RAP と MAP 間の最大レンジの設定（屋内 MAP には非適用）
- クライアント トラフィックを伝送するバックホールの有効化
- VLAN タグが転送されるかどうかの定義
- セキュリティ設定（ローカルおよび外部認証）を含むメッシュ アクセス ポイントの認証モード（EAP または PSK）および認証方式（ローカルまたは外部）の定義

必要なメッシュ パラメータを設定するには、GUI と CLI のいずれかを使用できます。パラメータはすべてグローバルに適用されます。

グローバル メッシュ パラメータの設定（GUI）

コントローラの GUI を使用してグローバル メッシュ パラメータを設定する手順は、次のとおりです。

ステップ 1 [Wireless] > [Mesh] を選択します。

ステップ 2 必要に応じて、メッシュ パラメータを修正します。

表 *1*：グローバル メッシュ パラメータ

パラメータ	説明
Range (RootAP to MeshAP)	ルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）間に必要な最良の距離（フィート単位）です。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、このグローバル パラメータは、すべてのメッシュ アクセス ポイントに適用されます。 **範囲**：150 ～ 132,000 フィート **デフォルト**：12,000 フィート （注） この機能を有効にすると、すべてのメッシュアクセスポイントがリブートします。
IDS（Rogue and Signature Detection）	この機能を有効にすると、クライアントアクセスだけ（バックホールではなく）のすべてのトラフィックに対する IDS レポートが生成されます。 この機能を無効にすると、IDS レポートは生成されませんが、バックホール上の帯域幅が節約されます。 次のコマンドを使用して、メッシュ AP でこの機能を有効または無効にする必要があります。 **config mesh ids-state** {**enable** | **disable**} （注） 2.4GHz IDS は、コントローラのグローバル IDS 設定で有効になります。

パラメータ	説明
バックホール クライアント アクセス	（注） このパラメータは、2 つ以上の radio に対応したメッシュ アクセス ポイントに適用されます。 バックホール クライアント アクセスが有効な場合は、ワイヤレス バックホール radio を介したワイヤレス クライアント接続が許可されます。ワイヤレス バックホールは、ほとんどのメッシュ アクセス ポイントでは 5 GHz radio です。つまり、バックホール radio は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。 バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがワイヤレス バックホール radio を介して送信され、クライアント アソシエーションは 2 番目の radio のみを介して送信されます。 **デフォルト**：無効 （注） この機能を有効にすると、すべてのメッシュ アクセス ポイントがリブートします。

パラメータ	説明
VLAN トランスペアレント	この機能によって、メッシュ アクセス ポイントでイーサネット ブリッジング トラフィックの VLAN タグを処理する方法が決定されます。 （注） 概要および設定の詳細については、「拡張機能の設定」の項を参照してください。 VLAN トランスペアレントが有効な場合は、VLAN タグが処理されず、タグなしパケットとしてブリッジされます。 （注） VLAN トランスペアレントが有効な場合、イーサネット ポートの設定は必要ありません。イーサネット ポートは、タグありフレームとタグなしフレームの両方を解釈せずに渡します。 VLAN トランスペアレントが無効な場合は、すべてのパケットがポートの VLAN 設定（トランク モード、アクセス モード、またはノーマル モード）に従って処理されます。 （注） イーサネット ポートがトランク モードに設定されている場合は、イーサネット VLAN タギングを設定する必要があります。「イーサネット ブリッジングの有効化（GUI）」の項を参照してください。 （注） ノーマル、アクセス、およびトランク モードのイーサネット ポートの使用の概要については、「イーサネット ポートに関する注意」の項を参照してください。 （注） VLAN タギングを使用するには、[VLAN Transparent] チェックボックスを選択しない必要があります。 （注） デフォルトでは VLAN トランスペアレントが有効になっており、4.1.192.xxM リリースからリリース 5.2 へのソフトウェア アップグレードを円滑に実行できます。リリース 4.1.192.xxM は VLAN タギングをサポートしていません。 **デフォルト**：有効

パラメータ	説明
Security Mode	メッシュ アクセス ポイントのセキュリティ モード（Pre-Shared Key（PSK; 事前共有キー）または Extensible Authentication Protocol（EAP））を定義します。 （注） RADIUS サーバを使用する外部 MAC フィルタ認可を設定する場合、EAP を選択する必要があります。 （注） [External MAC Filter Authorization] パラメータを無効にする（チェックボックスを選択しない）と、ローカル EAP または PSK 認証はコントローラ内で実行されます。 **オプション**：PSK または EAP **デフォルト**：EAP

パラメータ	説明
External MAC Filter Authorization	

パラメータ	説明
	デフォルトでは、MAC フィルタリングは、コントローラ上のローカル MAC フィルタを使用します。 外部 MAC フィルタ認証が有効であり、MAC アドレスがローカル MAC フィルタで検出されない場合には、外部 RADIUS サーバの MAC アドレスが使用されます。 これにより、外部サーバで定義されていないメッシュ アクセス ポイントの join を防ぎ、不正なメッシュ アクセス ポイントからネットワークを保護します。 メッシュ ネットワーク内で外部認証を利用するには、次の設定が必要です。 • AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。 • コントローラも、RADIUS サーバで設定する必要があります。 • 外部認証および認証用に設定されたメッシュ アクセス ポイントは、RADIUS サーバのユーザ リストに追加する必要があります。 • リモート認可および認証の場合、EAP-FAST は製造元の証明書（CERT）を使用して、子メッシュ アクセス ポイントを認証します。また、この製造元証明書に基づく ID は、ユーザの確認においてメッシュ アクセス ポイントのユーザ名として機能します。 • IOS ベースのメッシュ アクセス ポイント（1130、1240）の場合、メッシュ アクセス ポイントのプラットフォーム名は、証明書内のイーサネット アドレスの前に位置します。つまり、外部 RADIUS サーバのユーザ名は、*platform_name_string*–イーサネット *MAC* アドレスであり、たとえば *c1520-001122334455* のようになります。 • RADIUS サーバに証明書をインストールして、EAP-FAST を設定する必要があります。 （注） この機能はデフォルトで有効ではなく、コントローラは MAC アドレス フィルタを使用してメッシュ アクセ

パラメータ	説明
	スポイントを許可および認証します。 **デフォルト**：無効
Force External Authorization	このパラメータが有効で、[EAP] および [External MAC Filter Authorization] パラメータも有効の場合、メッシュ アクセス ポイントの外部の許可および認証はデフォルトで外部 RADIUS サーバ（Cisco 4.1 以降など）が行います。RADIUS サーバによって、コントローラによるMACアドレスのローカル認証（デフォルト）が無効になります。 **デフォルト**：無効

ステップ 3 [Apply] をクリックします。

ステップ 4 [Save Configuration] をクリックします。

グローバル メッシュ パラメータの設定（CLI）

コントローラの CLI を使用して認証方式を含むグローバル メッシュ パラメータを設定する手順は、次のとおりです。

（注） CLI コマンドで使用されるパラメータの説明、有効範囲およびデフォルト値については、「グローバル メッシュ パラメータの設定（GUI）」の項を参照してください。

ステップ 1 ネットワークの全メッシュアクセスポイントの最大レンジをフィート単位で指定するには、次のコマンドを入力します。

config mesh range *feet*

現在のレンジを確認するには、**show mesh range** と入力します。

ステップ 2 バックホールのすべてのトラフィックに関して IDS レポートを有効または無効にするには、次のコマンドを入力します。

config mesh ids-state {**enable** | **disable**}

ステップ 3 バックホール インターフェイスでのアクセス ポイント間のデータが共有されるレート（Mbps 単位）を指定するには、次のコマンドを入力します。

config ap bhrate {*rate* | **auto**} *Cisco_AP*

ステップ 4 メッシュ アクセス ポイントのプライマリ バックホール（802.11a）でクライアント アソシエーションを有効または無効にするには、次のコマンドを入力します。

config mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {**add** | **delete**} **802.11a** *wlan_id Cisco_AP*

ステップ 5 VLAN トランスペアレントを有効または無効にするには、次のコマンドを入力します。

config mesh ethernet-bridging VLAN-transparent {**enable** | **disable**}

ステップ 6 メッシュ アクセス ポイントのセキュリティ モードを定義するには、次のいずれかのコマンドを入力します。

a) コントローラによるメッシュ アクセス ポイントのローカル認証を提供するには、次のコマンドを入力します。

config mesh security {**eap** | **psk**}

b) 認証用にコントローラ（ローカル）の代わりに外部 RADIUS サーバに MAC アドレス フィルタを格納するには、次のコマンドを入力します。

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

c) RADIUS サーバで外部認証を提供し、コントローラでローカル MAC フィルタを定義するには、次のコマンドを入力します。

config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

d) RADIUS サーバで MAC ユーザ名（c1520-123456 など）を使用し、RADIUS サーバで外部認証を提供するには、次のコマンドを入力します。

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server *index* **enable**

config mesh security force-ext-auth enable

ステップ 7 変更を保存するには、次のコマンドを入力します。

save config

グローバル メッシュ パラメータ設定の表示（CLI）

グローバル メッシュ設定の情報を取得するには、次のコマンドを入力します。

- **show mesh client-access**：バックホール クライアント アクセスが有効な場合は、ワイヤレス バックホール radio を介したワイヤレス クライアント接続が許可されます。ワイヤレス バックホール radio は、大部分のメッシュ アクセス ポイントで 5GHz radio が使用されます。つまり、ワイヤレス バックホール radio は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

  バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがワイヤレスバックホールradioを介して送信され、クライアント アソシエーションは 2 番目の radio のみを介して送信されます。

```
(Cisco Controller)> show mesh client-access
Backhaul with client access status: enabled
```

- **show mesh ids-state**：バックホールの IDS レポートの状態が有効か無効かを示します。

```
(Cisco Controller)> show mesh ids-state
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

- **show mesh config**：グローバル設定を表示します。

```
(Cisco Controller)> show mesh config
Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. disabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... disabled

Mesh Security
Security Mode.................................. EAP
External-Auth.................................. disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled

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

Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

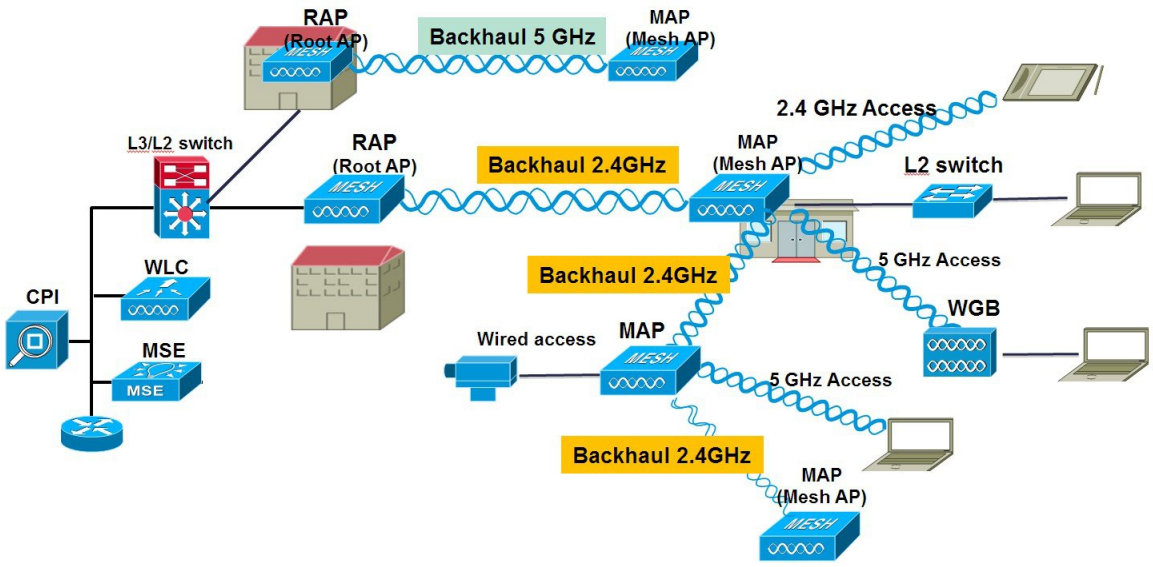
リリース 8.2 の 5 GHz および 2.4 GHz のメッシュ バックホール

リリース 8.2 以前のワイヤレス メッシュ バックホールは 5 GHz でのみサポートされていました。リリース 8.2 ではワイヤレス メッシュ バックホールは、5 GHz および 2.4 GHz でサポートされます。

特定の国では 5 GHz のバックホール ネットワークのメッシュ ネットワークを使用できません。5 GHz 帯が許可されている国でも、より大きいメッシュやブリッジの距離を達成するために 2.4 GHz 帯が優先される場合があります。

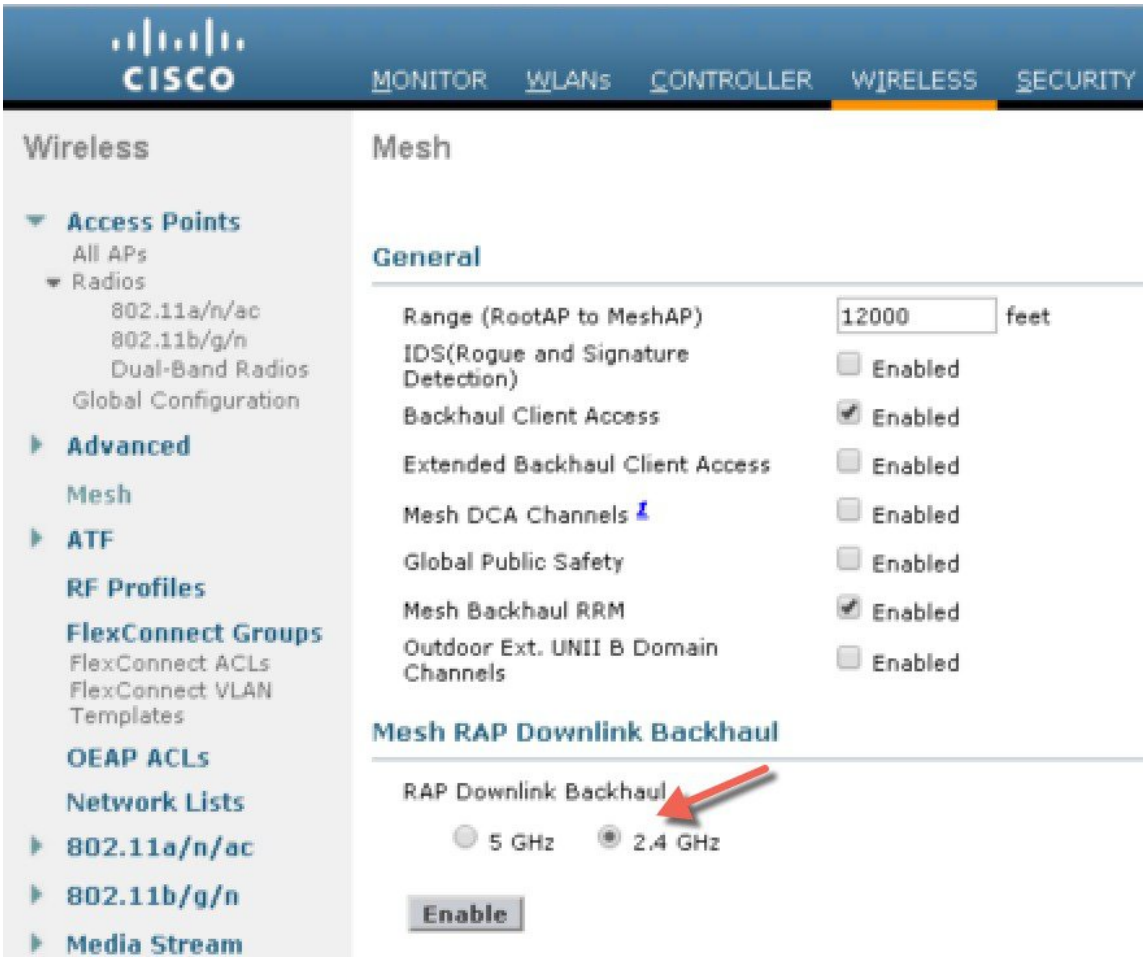
RAP が 5 GHz から 2.4 GHz へ設定を変更すると、その変更内容は RAP からすべての MAP に伝播され、5 GHz ネットワークから切り離されて 2.4 GHz 帯に再接続されます。2.4 GHz を設定する場合は、2.4 GHz のバックホールが認識されるよう、すべてのコントローラでリリース 8.2 を実行してください。

（注） RAP だけが 5 GHz または 2.4 GHz のバックホール周波数に対応します。RAP が設定されると、この周波数選択がすべての MAP に分岐して伝播します。



ステップ 1 コントローラから一回の簡単な操作でメッシュ バックホールを 2.4 GHz に設定できます。図に示すように RAP ダウンリンク バックホールを 2.4 GHz に設定して [Enable] を押します。

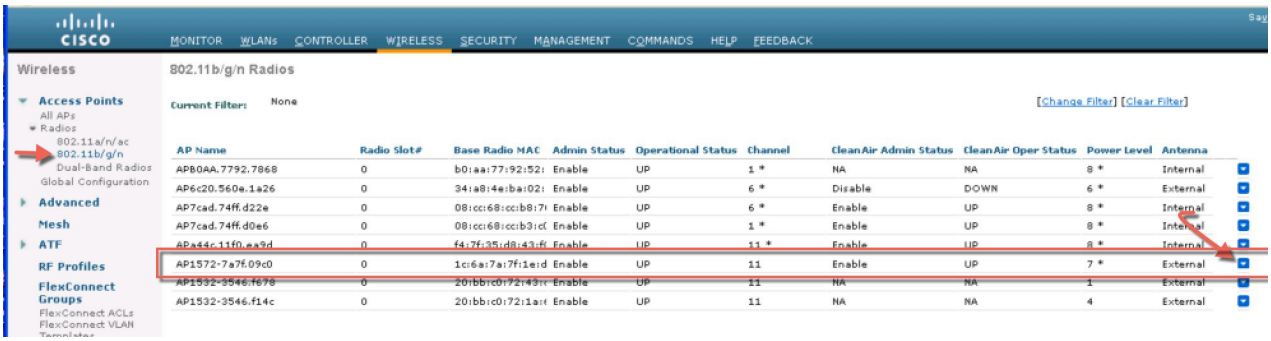
（注） 以下の例では、コントローラのグローバルの 2.4 GHz を示します。グローバル コンフィギュレーションでこれを行うと、すべてのメッシュ RAP に適用されます。チャネルのプロビジョニングは、個別の RAP でも行えます。この場合、チャネルのプロビジョニングは、親と子の特定の RAP 分岐に限り適用されます。



CLI から「show mesh ap tree」と「show mesh backhaul <ap-name>」を発行してバックホール接続を表示できます。

```
(5520-MA1) >show mesh ap tree

 ========================================================
||   AP Name [Hop Counter, Link SNR, Bridge Group Name] ||
 ========================================================

[Sector 1]
----------
AP1572-7a7f.09c0[0,0,tme]
  |-AP1532-3546.f14c[1,37,tme]
  |-AP1532-3546.f678[1,28,tme]

------------------------------------------------------
Number of Mesh APs.............................. 3
Number of RAPs.................................. 1
Number of MAPs.................................. 2
------------------------------------------------------

(5520-MA1) >show mesh backhaul ?

<Cisco AP>     Enter the name of the Cisco AP.

(5520-MA1) >show mesh backhaul AP1532-3546.f14c

Current Backhaul Slot(s)........................ 1

Basic Attributes for Slot  1
    Radio Type.................................. RADIO_TYPE_80211n-5
    Radio Subband............................... RADIO_SUBBAND_ALL
    Radio Role.................................. UPDOWNLINK ACCESS
    Administrative State ....................... ADMIN_ENABLED
    Operation State ............................ UP
      Current Tx Power Level ................... 1
      Current Channel .......................... 149
      Antenna Type.............................. EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBm units).... 0

(5520-MA1) >
```

ステップ 2 RAP でチャネルを 2.4 GHz に変更し、チャネルを自ら選択する必要があります。ここでの変更内容はすべての MAP と、RAP の分岐の「子」に伝播されます。



チャネルがカスタム オプションで選択された後、そのチャネルは RAP バックホールに使用されます。

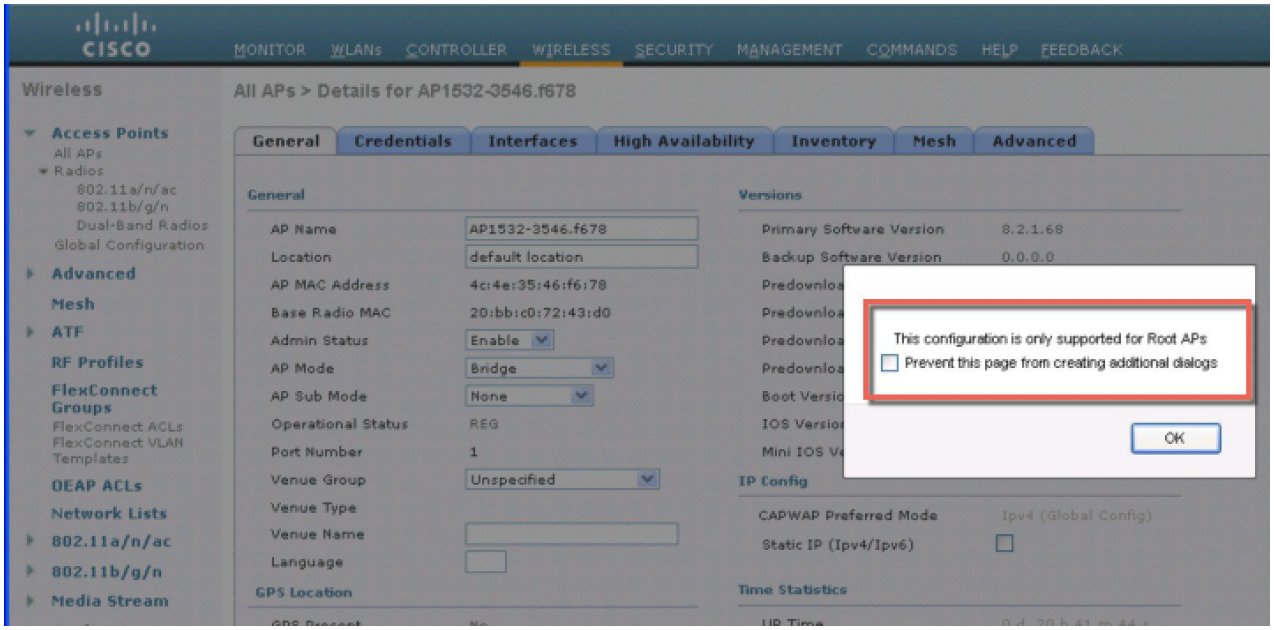
（注） RAP は同じ RF ドメインの他の RAP と共に RRM プロセスに参加できますが、MAP は RAP からの同じチャネルだけを継承して固定されます。

次の例に示すように、RAP でチャネルを変更した後は、MAP のチャネルが 2.4 GHz 帯の CH11 に 変更されています。

MAP の CLI コマンドの例：show mesh backhaul <ap-name>

```
(5520-MA1) >show mesh backhaul AP1572-7a7f.09c0

Current Backhaul Slot(s)..................... 0

Basic Attributes for Slot  0
    Radio Type.............................. RADIO_TYPE_80211n-2.4
    Radio Role.............................. DOWNLINK ACCESS
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
      Current Tx Power Level ............... 7
      Current Channel ...................... 11
      Antenna Type.......................... EXTERNAL_ANTENNA
      External Antenna Gain (in .5 dBm units).... 0
```

たとえばMAPのバックホール チャネルを変更しようとすると、この機能はMAPでサポートされていないため、エラー メッセージが表示されます。MAP および「MAP の子」はアップストリームの親 RAP からチャネルが割り当てられます。MAP からのエラー メッセージの例を示します。



バックホール クライアント アクセス

バックホール クライアント アクセスが有効な場合は、ワイヤレス バックホール radio を介したワイヤレス クライアント接続が許可されます。ワイヤレス バックホール radio では 5 GHz 帯が使用されます。つまり、ワイヤレス バックホール radio は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがワイヤレス バックホール radio を介して送信され、クライアント接続は 2 番目の radio のみを介して送信されます。

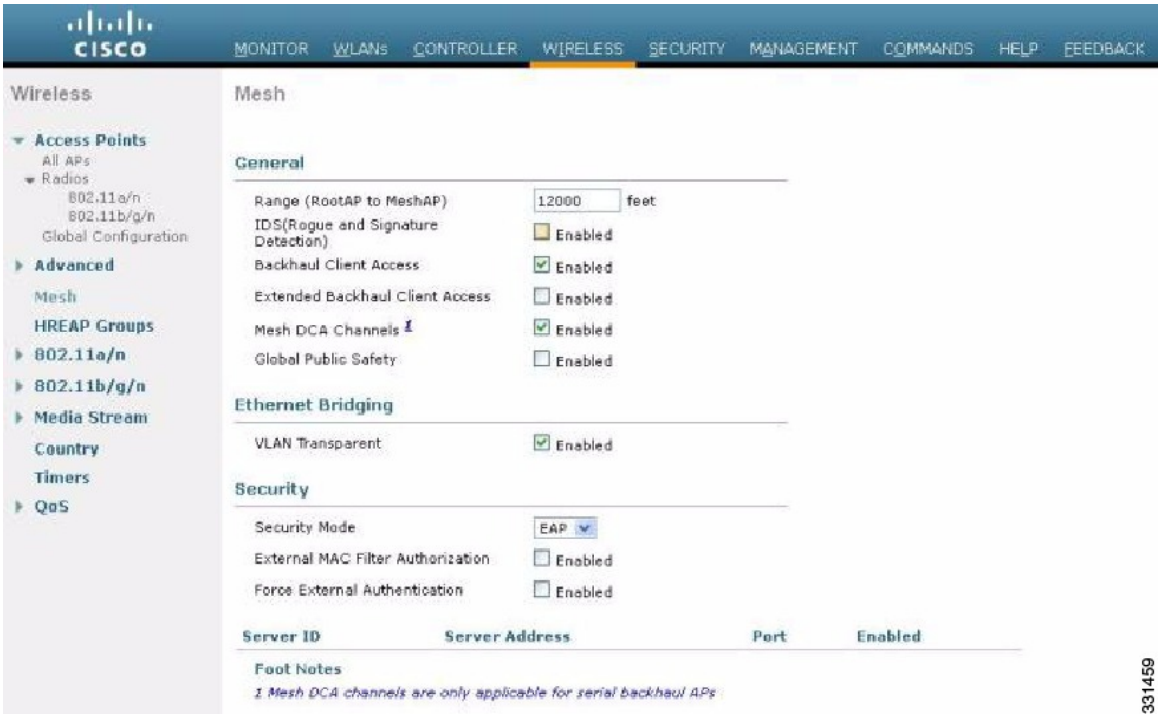
（注） バックホール クライアント アクセスはデフォルトで無効です。この機能を有効にすると、デイジーチェーン導入のスレーブ AP と子 AP を除くすべてのメッシュ アクセス ポイントは再起動します。

この機能は、2 つの radio を使用するメッシュ アクセス ポイント（1552、1532、1540、1560、1572、およびブリッジ モードの屋内 AP）に適用されます。

バックホール クライアント アクセスの設定（GUI）

この図は、GUI を使用してバックホール クライアント アクセスを有効にする方法を示しています。バックホール クライアント アクセスを有効にすると、AP をリブートするよう求められます。

図 *5: GUI* を使用したバックホール クライアント アクセスの設定



次のタスク

Flex+Bridge 導入で、バックホール クライアント アクセスをグローバルで有効にした後に 5 GHz 無線ビーコンを想定どおりに送信するためには、Flex+Bridge モードで動作するルート AP の [Install mapping on radio backhaul] オプションを有効にする必要があります。

[Install mapping on radio backhaul] オプション有効化の詳細については、以下の「Configuring Flex+Bridge Mode (GUI)」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/flexconnect.html#config-flex-bridge-gui

バックホール クライアント アクセスの設定（CLI）

次のコマンドを使用して、バックホール クライアント アクセスを有効にします。

```
(Cisco Controller)> config mesh client-access enable
```

次のメッセージが表示されます。

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

次のタスク

Flex+Bridge導入で、バックホール クライアント アクセスをグローバルで有効にした後に5 GHz無線ビーコンを想定どおりに送信するためには、Flex+Bridge モードで動作するルート AP の [Install mapping on radio backhaul] オプションを有効にする必要があります。

[Install mapping on radio backhaul] オプション有効化の詳細については、以下の「Configuring Flex+Bridge Mode (CLI)」の項を参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/flexconnect.html#config-flex-bridge-cli

ローカル メッシュ パラメータの設定

グローバル メッシュ パラメータを設定したら、ネットワークで次のような特定の機能を使っている場合次のローカル メッシュ パラメータを設定する必要があります。

- バックホール データ レート。「ワイヤレス バックホールのデータ レートの設定」の項を参照してください。
- イーサネットブリッジング。イーサネットブリッジングの設定の項を参照してください。
- ブリッジ グループ名。「イーサネット ブリッジングの設定」の項を参照してください。
- ワークグループブリッジ。「ワークグループブリッジの設定」の項を参照してください。
- 出力およびチャネル設定。
- アンテナ利得設定。「アンテナ利得の設定」の項を参照してください。
- 動的チャネル割り当て。

ワイヤレス バックホールのデータ レートの設定

バックホールは、アクセス ポイント間でワイヤレス接続のみを構築するために使用されます。バックホール インターフェイスは、アクセス ポイントによって、802.11a/n/ac レートが異なります。利用可能なRF スペクトラムを効果的に使用するにはレート選択が重要です。また、レートはクライアントデバイスのスループットにも影響を与えることがあり、スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです。

Dynamic Rate Adaptation（DRA）には、パケット伝送のために最適な伝送レートを評価するプロセスが含まれます。レートを正しく選択することが重要です。レートが高すぎると、パケット伝送が失敗し、通信障害が発生します。レートが低すぎると、利用可能なチャネル帯域幅が使用されず、品質が低下し、深刻なネットワーク輻輳および障害が発生する可能性があります。

データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。低データ レート（6 Mbps など）が、高データ レート（1300 Mbps など）よりもアクセス ポイントからの距離を伸ばします。結果として、データ レートはセル カバレッジと必要なアクセス ポイントの数に影響を与えます。異なるデータ レートは、ワイヤレス リンクで冗長度の高い信号を送信することにより（これにより、データをノイズから簡単に復元できます）、実現されます。1 Mbps のデータ レートでパケットに対して送信されるシンボル数は、11 Mbps で同じパケットに使用されたシンボル数より多くなります。したがって、低ビット レートでのデータの送信には、高ビット レートでの同じデータの送信よりも時間がかり、スループットが低下します。

コントローラ リリース 5.2 では、メッシュ 5 GHz バックホールのデフォルト データ レートは 24 Mbps です。これは、6.0 および 7.0 コントローラ リリースでも同じです。

6.0 コントローラ リリースでは、メッシュ バックホールに「Auto」データ レートを設定できます。設定後に、アクセス ポイントは、最も高いレートを選択します（次に高いレートは、すべてのレートに影響を与えることはありませんが、最も高いレートには適切でないため、使用できません）。つまり、設定後は、各リンクが、そのリンク品質に最適なレートに自動的に設定されます。

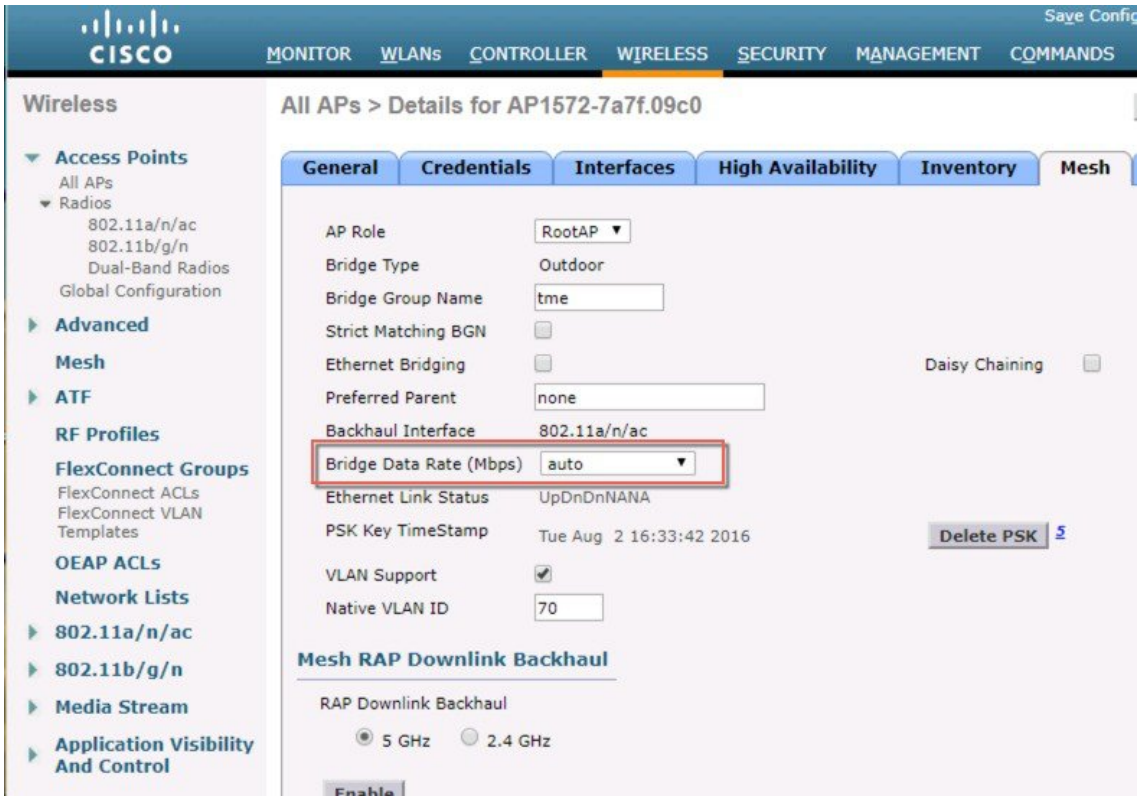
メッシュ バックホールを「Auto」に設定することをお勧めします。

たとえば、メッシュ バックホールが 48 Mbps を選択した場合、この決定は、誰かが電子レンジを使用したためではなく（これによりすべてのレートが影響を受けます）、54 Mbps に対して十分な SNR がないため、54 Mbps を使用できないことが確認された後に行われます。

低ビット レートでは、MAP 間の距離を長くすることが可能になりますが、WLAN クライアント カバレッジにギャップが生じる可能性が高く、バックホール ネットワークのキャパシティが低下します。バックホール ネットワークのビット レートを増加させる場合は、より多くの MAP が必要となるか、MAP 間の SNR が低下し、メッシュの信頼性と相互接続性が制限されます。

この図では、RAP が「Auto」バックホール データ レートを使用しており、子 MAP との間では 54 Mbps を使用していることを示しています。

図 *6:* 自動設定されたブリッジ レート



（注） データ レートは、AP ごとにバックホールで設定できます。これはグローバル コマンドではありません。

関連コマンド

以下のコマンドを使用してバックホールに関する情報を取得します。

- **config ap bhrate**：Cisco ブリッジ バックホール送信レートを設定します。

  構文は次のようになります。

```
(controller) > config ap bhrate backhaul-rate ap-name
```

（注） 各 AP に対して設定済みのデータ レート（RAP=18 Mbps、MAP1=36 Mbps）は、6.0 以降のソフトウェア リリースへのアップグレード後も保持されます。6.0 リリースにアップグレードする前に、データ レートに設定されるバックホールデータ レートがある場合は、その設定が保持されます。

次の例は、RAP でバックホール レートを 36000 Kbps に設定する方法を示しています。

```
(controller) > config ap bhrate 36000 HPRAP1
```

- **show ap bhrate**：Cisco ブリッジ バックホール レートを表示します。

  構文は次のようになります。

  ```
  (controller) > show ap bhrate ap-name
  ```

- **show mesh neigh summary**：バックホールで現在使用されているレートを含むリンク レート概要を表示します。

  例：

  ```
  (controller) > show mesh neigh summary HPRAP1

  AP Name/Radio    Channel     Rate     Link-Snr     Flags       State
  ---------------- --------   --------   -------     -----       -----
  00:0B:85:5C:B9:20 0          auto        4       0x10e8fcb8   BEACON
  00:0B:85:5F:FF:60 0          auto        4       0x10e8fcb8   BEACON DEFAULT
  00:0B:85:62:1E:00 165        auto        4       0x10e8fcb8   BEACON
  OO:0B:85:70:8C:A0 0          auto        1       0x10e8fcb8   BEACON
  HPMAP1           165         54          40      0x36         CHILD BEACON
  HJMAP2           0          auto         4       0x10e8fcb8   BEACON
  ```

バックホールのキャパシティとスループットは AP のタイプ（つまり、802.11a/n であるかや、802.11a のみであるかや、バックホール radio の数など）によって異なります。

イーサネット ブリッジングの設定

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

（注） イーサネットブリッジングが無効な場合であっても、いくつかのプロトコルで例外が許可されます。たとえば、次のプロトコルが許可されます。

- スパニング ツリー プロトコル（STP）
- アドレス解決プロトコル（ARP）
- Control and Provisioning of Wireless Access Points（CAPWAP）
- ブートストラップ プロトコル（BOOTP）パケット

レイヤ2のループの発生を防止するために、接続されているすべてのスイッチ ポート上でスパニング ツリー プロトコル（STP）を有効にします。

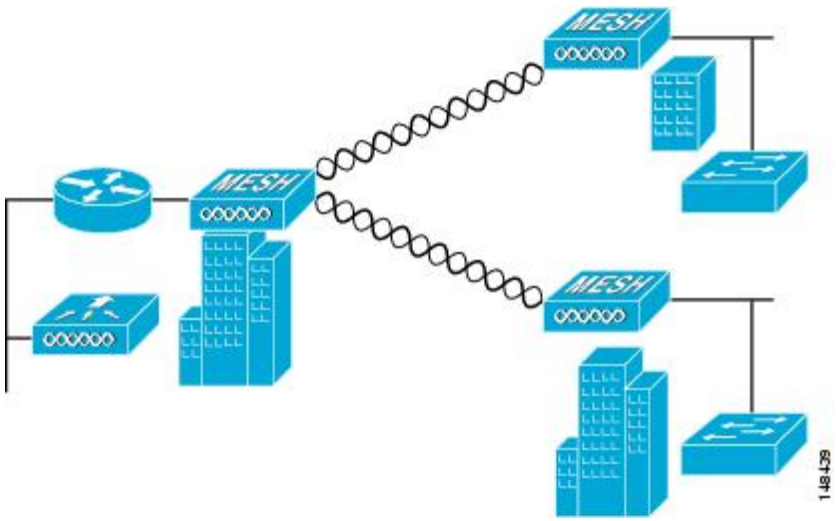
イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

1. メッシュ ノードをブリッジとして使用する場合（図 7 : ポイントツーマルチポイント ブリッジング （42 ページ） を参照）。

（注） ポイントツーポイントおよびポイントツーマルチポイント ブリッジング導入でイーサネットブリッジングを使用するのに、VLAN タギングを設定する必要はありません。

2. MAP でイーサネット ポートを使用して任意のイーサネット デバイス（ビデオ カメラなど）を接続する場合。VLAN タギングを有効にするときの最初の手順です。

図 7 : ポイントツーマルチポイント ブリッジング



イーサネット ブリッジングの有効化（GUI）

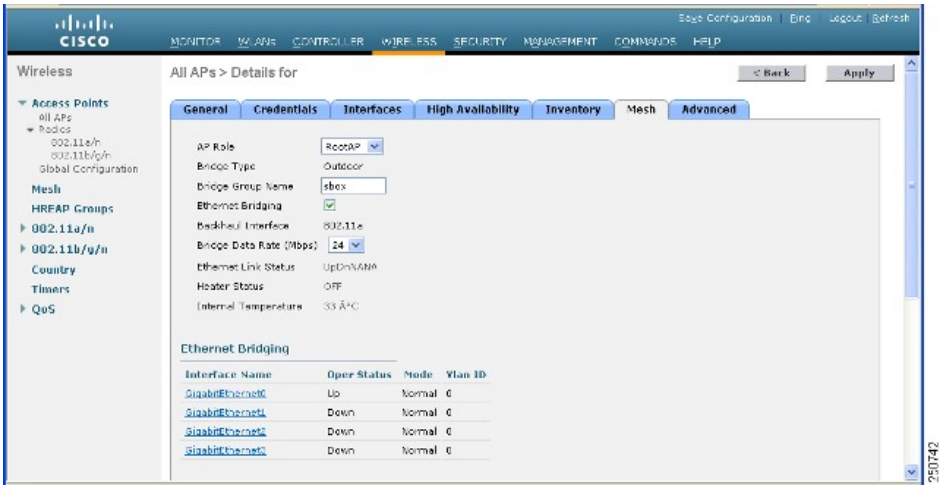
GUI を使用して RAP または MAP でイーサネット ブリッジングを有効にする手順は、次のとおりです。

ステップ 1 [Wireless] > [All APs] を選択します。

ステップ 2 イーサネット ブリッジングを有効にするメッシュ アクセス ポイントの AP 名のリンクをクリックします。

ステップ 3 詳細ページで、[Mesh] タブを選択します（図 8 : [All APs > Details for]（[Mesh]）ページ （43 ページ）を参照してください）。

図 8 : [All APs > Details for]（[Mesh]）ページ



ステップ 4 [AP Role] ドロップダウン リストから [RootAP] または [MeshAP] を選択します（すでに選択されていない場合）。

ステップ 5 イーサネット ブリッジングを有効にする場合は、[Ethernet Bridging] チェックボックスを選択します。この機能を無効にする場合は、このチェックボックスを選択しません。

ステップ 6 [Apply] をクリックして、変更を確定します。ページの最下部の [Ethernet Bridging] セクションに、メッシュ アクセス ポイントの各イーサネット ポートが一覧表示されます。

ステップ 7 該当するメッシュ AP からコントローラへのパスになる各親メッシュ AP に対してイーサネット ブリッジングを有効にします。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。

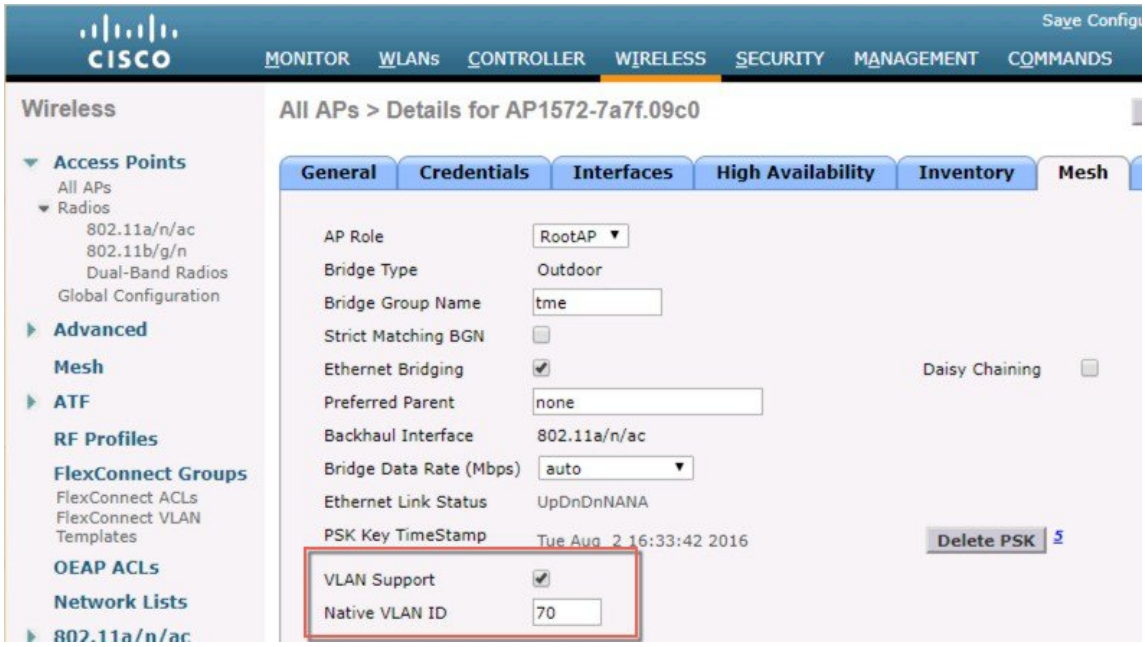
ネイティブ VLAN の設定（GUI）

（注） 8.0 以前は、有線バックホールのネイティブ VLAN は VLAN 1 に設定されていました。8.0 リリース以降では、ネイティブ VLAN を設定できます。

ステップ 1 [Wireless] > [All APs] を選択します。

ステップ 2 ネイティブ VLAN を設定したいメッシュ アクセス ポイントを選択します。

ステップ 3 AP の [VLAN Support] チェックボックスを選択します。



ステップ 4 ネイティブ VLAN を割り当てます。

（注） このネイティブ VLAN が、接続されたスイッチのスイッチ ポートに設定されたネイティブ VLAN と一致する必要があります。

ステップ 5 [Apply] をクリックして、変更を確定します。

ネイティブ VLAN の設定（CLI）

（注） 8.0 以前は、有線バックホールのネイティブ VLAN は VLAN 1 に設定されていました。8.0 リリース以降では、ネイティブ VLAN を設定できます。

1. コマンド **config ap vlan-trunking native** ***vlan-id ap-name*** を使用して有線バックホール ポートにネイティブ VLAN を設定します。

   これにより、アクセス ポイントにネイティブ VLAN 設定が適用されます。

ブリッジ グループ名の設定

ブリッジグループ名（BGN）は、メッシュアクセスポイントの接続を制御します。BGNを使用して無線を論理的にグループ分けしておくと、同じチャネルにある2つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター（領域）のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字までの文字列です。

NULL VALUE という BGN は、製造時にデフォルトで設定されています。装置自体にブリッジグループ名は表示されていませんが、このグループ名を使用することで、ネットワーク固有の BGN を割り当てる前に、メッシュ アクセス ポイントをネットワークに参加させることができます。

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

ブリッジ グループ名の設定（CLI）

ステップ 1 ブリッジ グループ名（BGN）を設定するには、次のコマンドを入力します。

config ap bridgegroupname set *group-name ap-name*

（注） BGN の設定後に、メッシュ アクセス ポイントはリブートします。

注意 稼働中のネットワークで BGN を設定する場合は、注意してください。BGN の割り当ては、必ずRAPから最も遠い距離にあるノード（メッシュツリーの一番下にある終端ノード）から開始し、RAP に向かって設定して、同じネットワーク内に混在する BGN（古い BGN と新しい BGN）のため、メッシュ アクセス ポイントがドロップしないようにします。

ステップ 2 BGN を確認するには、次のコマンドを入力します。

show ap config general *ap-name*

ブリッジ グループ名の確認（GUI）

ステップ 1 [Wireless] > [Access Points] > [AP Name] をクリックします。選択したメッシュ アクセス ポイントの詳細ページが表示されます。

ステップ 2 [Mesh] タブをクリックします。BGN を含むメッシュ アクセス ポイントの詳細が表示されます

出力およびチャネルの設定

バックホール チャネル（802.11a/n）は、RAP 上で設定できます。MAP は、RAP チャネルに合わせます。ローカル アクセスは、MAP とは無関係に設定できます。

出力およびチャネルの設定（GUI）

ステップ 1 [Wireless] > [Access Points] > [802.11a/n] を選択します。

（注） radio スロットは各 radio に対して表示されます。

ステップ 2 802.11 a/n radio の [Antenna] ドロップダウン リストで、[Configure] を選択します。[Configure] ページが表示されます。

ステップ 3 radio のチャネルを割り当てます（グローバルおよびカスタムの割り当て方式）。

ステップ 4 radio の Tx Power Level を割り当てます。

AP1500 の 802.11a バックホールでは、選択可能な 5 つの出力レベルがあります。

（注） バックホールのデフォルトの送信出力レベルは最大出力レベル（レベル 1）です。

ステップ 5 出力およびチャネルの割り当てが完了したら、[Apply] をクリックします。

ステップ 6 [802.11a/n Radios] ページで、チャネルの割り当てが正しく行われたことを確認します。

アンテナ利得の設定

コントローラの GUI または CLI を使用して、取り付けられているアンテナのアンテナ利得と一致するように、メッシュ アクセス ポイントのアンテナ利得を設定する必要があります。

アンテナ利得の設定（GUI）

コントローラの GUI を使用してアンテナ パラメータを設定する手順は、次のとおりです。

ステップ 1 [Wireless] > [Access Points] > [Radio] > [802.11a/n] の順に選択して、[802.11a/n Radios] ページを開きます。

ステップ 2 設定するメッシュ アクセス ポイントのアンテナについて、一番右の青色の矢印にマウスを移動してアンテナのオプションを表示します。[Configure] を選択します。

（注） 外部アンテナだけに設定可能な利得設定があります。

ステップ 3 [Antenna Parameters] セクションで、アンテナ利得を入力します。

利得は 0.5 dBm 単位で入力します。たとえば、2.5 dBm = 5 です。

（注） 入力する利得値は、アンテナのベンダーが指定した値と同じにする必要があります。

ステップ 4 [Apply] および [Save Configuration] をクリックして、変更を保存します。

アンテナ利得の設定（CLI）

コントローラの CLI を使用して 802.11a バックホール radio のアンテナ利得を設定するには、次のコマンドを入力します。

config 802.11a antenna extAntGain *antenna_gain AP_name*

ここで、利得は 0.5 dBm 単位で入力します（たとえば、2.5 dBm の場合は 5 になります）。

動的チャネル割り当ての設定

RRM スキャンに使用されるチャネルを選択する際に、次の手順でコントローラの GUI を使用することで、動的チャネル割り当て（DCA）アルゴリズムが使用するチャネルを指定できます。この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の規制当局による制約があるために、クライアントで特定のチャネルがサポートされないことがわかっている場合に役立ちます。

ここで説明する手順は、メッシュ ネットワークのみに関係します。

ステップ 1 802.11a/n または 802.11b/g/n ネットワークを無効にする手順は、次のとおりです。

a) [Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順に選択して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。

b) [802.11a（または 802.11b/g）Network Status] チェックボックスを選択しません。

c) [Apply] をクリックして、変更を確定します。

ステップ 2 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [DCA] の順に選択して、[802.11a（または 802.11b/g）> RRM > Dynamic Channel Assignment (DCA)] ページを開きます。

ステップ 3 [Channel Assignment Method] ドロップダウン リストから次のオプションのいずれかを選択して、コントローラの DCA モードを指定します。

- [Automatic]：コントローラは join しているすべてのメッシュ アクセス ポイントのチャネル割り当てを定期的に評価し、必要に応じて更新するようにします。これはデフォルト値です。
- [Freeze]：[Invoke Channel Update Once] をクリックしたときに限り、join しているすべてのメッシュ アクセス ポイントのチャネル割り当てを必要に応じてコントローラが評価して更新します。

（注） [Invoke Channel Update Once] をクリックしても、すぐにチャネル割り当ての評価と更新が行われるわけではありません。次の間隔が経過するまで待機します。

- [OFF]：DCA をオフにし、すべてのメッシュ アクセス ポイント radio をデフォルトで周波数帯の最初のチャネルに設定します。このオプションを選択する場合は、すべての radio のチャネルを手動で割り当てる必要があります。

ステップ 4 [Interval] ドロップダウン リストで、[10 minutes]、[1 hour]、[2 hours]、[3 hours]、[4 hours]、[6 hours]、[8 hours]、[12 hours]、または [24 hours] のいずれかのオプションを選択し、DCA アルゴリズムを実行する間隔を指定します。デフォルト値は 10 分です。

ステップ 5 [AnchorTime] ドロップダウン リストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0 ～ 23 の数値（両端の値を含む）で、午前 12 時～午後 11 時の時刻を表します。

ステップ 6 [Avoid Foreign AP Interference] チェックボックスを選択すると、コントローラの RRM アルゴリズムによって、Lightweight アクセス ポイントにチャネルを割り当てるときに、外部アクセス ポイント（ワイヤレス ネットワークに含まれないアクセス ポイント）からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、このチェックボックスを選択しません。たとえば RRM では、外部アクセス ポイントに近いチャネルをアクセス ポイントが回避するようにチャネル割り当てを調整できます。デフォルト値はオンです。

ステップ 7 [Avoid Cisco AP Load] チェックボックスを選択すると、コントローラの RRM アルゴリズムによって、チャネルを割り当てるときに、ワイヤレス ネットワーク内の Cisco Lightweight アクセス ポイントからの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、このチェックボックスを選択しません。たとえば RRM では、トラフィックの負荷が高いアクセス ポイントに適切な再利用パターンを割り当てることができます。デフォルト値はオフです。

ステップ 8 [Avoid Non-802.11a (802.11b) Noise] チェックボックスを選択すると、コントローラの RRM アルゴリズムによって、Lightweight アクセス ポイントにチャネルを割り当てるときに、チャネルのノイズ（802.11 以外のトラフィック）が考慮されます。この機能を無効にする場合は、このチェックボックスを選択しません。たとえば RRM では、電子レンジなど、アクセス ポイント以外を原因とする重大な干渉があるチャネルをアクセス ポイントに回避させることができます。デフォルト値はオンです。

ステップ 9 [DCA Channel Sensitivity] ドロップダウン リストから、次のオプションのいずれかを選択して、チャネル変更の判断材料となる環境要因（信号、負荷、ノイズ、干渉など）に対する DCA アルゴリズムの感度を指定します。

- [Low]：環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
- [Medium]：環境の変化に対する DCA アルゴリズムの感度は中程度です。
- [High]：環境の変化に対する DCA アルゴリズムの感度が高くなります。

デフォルト値は [Medium] です。

表 *2 : DCA* の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

ステップ 10 802.11a/n ネットワークの場合のみ、次のいずれかの [Channel Width] オプションを選択し、5 GHz 帯の 802.11n/a/ac すべてがサポートするチャネル幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）

（注） グローバルに設定された DCA チャネル幅設定を上書きするには、[802.11a/n Cisco APs] > [Configure] ページでアクセス ポイントの radio を 20 MHz モードに設定します。アクセス ポイント radio で静的 RF チャネルの割り当て方法を [Global] に変更すると、グローバルな DCA 設定によりアクセス ポイントが使用していたチャネル幅設定が上書きされます。

このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャネル割り当てを行う RF グループ リーダーの MAC アドレス。
- [Last Auto Channel Assignment]：RRM が現在のチャネル割り当てを最後に評価した時間。

ステップ 11 [DCA Channel List] の [DCA Channels] フィールドには、現在選択されているチャネルが表示されます。チャネルを選択するには、[Select] コラムでそのチャネルのチェックボックスを選択します。チャネルを除外するには、チャネルのチェックボックスを選択しません。

範囲：802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165、190、196、802.11b/g：1、2、3、4、5、6、7、8、9、10、11

デフォルト：802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、802.11b/g：1、6、11

（注） 802.11a 帯の拡張 UNII-2 チャネル（100、104、108、112、116、132、136、および 140）は、チャネル リストには表示されません。-E 規制区域に Cisco Aironet 1500 シリーズ メッシュ アクセス ポイントがある場合は、運用を開始する前に、DCA チャネル リストにこれらのチャネルを含める必要があります。以前のリリースからアップグレードしている場合は、これらのチャネルが DCA チャネル リストに含まれていることを確認します。チャネル リストにこれらのチャネルを含めるには、[Extended UNII-2 Channels] チェックボックスを選択します。

ステップ 12 ネットワークで AP1500 を使用している場合は、4.9 GHz チャネルが動作する 802.11a 帯で 4.9 GHz チャネルを設定する必要があります。4.9 GHz 帯域は、Public Safety に関わるクライアント アクセス トラフィック専用です。4.9 GHz チャネルを選択するには、[Select] コラムでチェックボックスを選択します。チャネルを除外するには、チャネルのチェックボックスを選択しません。

範囲：802.11a：1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26

デフォルト：802.11a：20、26

ステップ 13 [Apply] をクリックして、変更を確定します。

ステップ 14 802.11a または 802.11b/g ネットワークを再び有効にする手順は、次のとおりです。

a) [Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順にクリックして、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。
b) [802.11a（または 802.11b/g）Network Status] チェックボックスを選択します。
c) [Apply] をクリックして、変更を確定します。

ステップ 15 [Save Configuration] をクリックして、変更を保存します。

（注） DCA アルゴリズムによってチャネルが変更された理由を確認するには、[Monitor] をクリックし、次に [Most Recent Traps] の下にある [View All] をクリックします。トラップにより、チャネルが変更された radio の MAC アドレス、前のチャネルと新しいチャネル、変更された理由、変更前後のエネルギー、変更前後のノイズ、変更前後の干渉が示されます。5 GHz radio の動的チャネル割り当てはローカルまたは FlexConnect モードの屋外アクセス ポイントでのみサポートされます。

ブリッジ モードのアクセス ポイントでの RRM の設定

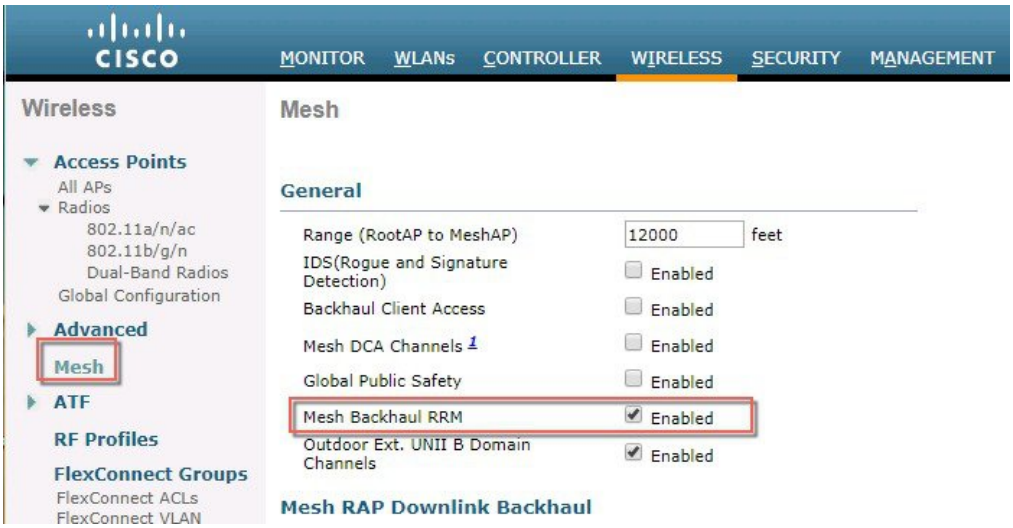
Radio Resource Management（RRM）は、次の場合に、ブリッジ モード アクセス ポイントのバックホール radio で有効にできます。

- AP がルート AP（RAP）
- RAP に WLC への有線イーサネット リンクがある
- RAP に接続された子メッシュ AP がない

これらの条件が満たされている場合、完全な RRM が確立されます。この中には、伝送出力制御（TPC）、動的チャネル割り当て（DCA）、カバレッジ ホールの検出と緩和（CHDM）が含まれます。メッシュ AP が RRM に参加する RAP に再度接続する必要がある場合、RAP は、すべての RRM 機能をただちに停止します。

次のコマンドは、RRM を有効にします。

- **config mesh backhaul rrm** ***<enable|disable>***：メッシュ バックホール radio の RRM を有効にします。
- **Config mesh backhaul rrm** ***<auto-rf global|off>***：動的チャネル割り当てのみを有効/無効にします。



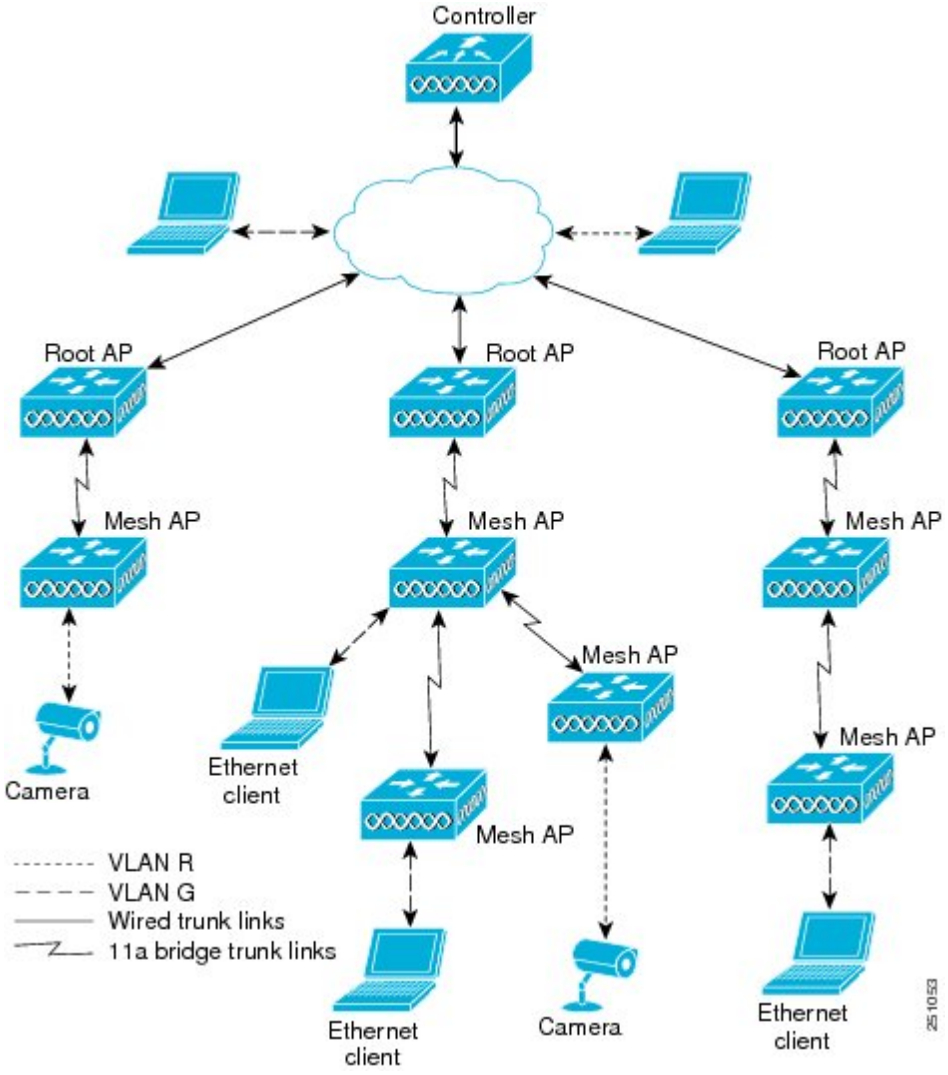
拡張機能の設定

イーサネット VLAN タギングの設定

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

イーサネット VLAN タギングを使用した一般的な Public Safety アクセス アプリケーションは、市内のさまざまな屋外の場所へのビデオ監視カメラの設置を前提にしたものです。これらのビデオ カメラはすべて MAP に有線で接続されています。また、これらのカメラのビデオはすべてワイヤレス バックホールを介して有線ネットワークにある中央の指令本部にストリーミングされます。

図 *9:* イーサネット *VLAN* タギング



イーサネット ポートに関する注意

イーサネット VLAN タギングを使用すると、屋内と屋外の両方の実装で、イーサネット ポートをノーマル、アクセス、またはトランクとして設定できます。

（注） VLAN トランスペアレントが無効な場合、デフォルトのイーサネット ポート モードはノーマルです。VLAN タギングを使用し、イーサネット ポートの設定を許可するには、VLAN トランスペアレントを無効にする必要があります。グローバル パラメータである VLAN トランスペアレント モードを無効にするには、「グローバル メッシュ パラメータの設定」の項を参照してください。

- ノーマル モード：このモードでは、イーサネット ポートが、タグ付きパケットを受信または送信しません。クライアントからのタグ付きフレームは破棄されます。

  単一VLANのみを使用している場合や、複数のVLANにわたるネットワークでトラフィックをセグメント化する必要がない場合は、アプリケーションでノーマルモードを使用します。

- アクセス モード：このモードでは、タグなしパケットだけを許可します。すべての着信パケットに、アクセス VLAN と呼ばれるユーザ設定 VLAN のタグが付けられます。

  MAP に接続され、RAP に転送される装置（カメラやPC）から情報を収集するアプリケーションでは、アクセス モードを使用します。次に、RAP はタグを適用し、トラフィックを有線ネットワーク上のスイッチに転送します。

- トランク モード：このモードでは、ユーザがネイティブ VLAN および許可された VLAN リストを設定する必要があります（デフォルトではありません）。このモードではタグ付きのパケットとタグなしパケットの両方が許可されます。タグなしパケットは許可され、ユーザ指定のネイティブ VLAN のタグが付けられます。許可された VLAN リスト内の VLAN のタグが付けられたタグ付きパケットは許可されます。

- キャンパス内の別々の建物に存在している 2 つの MAP 間でトラフィックを転送するようなブリッジング アプリケーションでは、トランク モードを使用します。

イーサネット VLAN タギングは、バックホールとして使用されていないイーサネット ポートで動作します。

（注） コントローラの7.2よりも前のリリースでは、ルート アクセス ポイント（RAP）のネイティブ VLAN は、メッシュ イーサネット ブリッジングと VLAN トランスペアレントを有効にしたメッシュ アクセス ポイント（MAP）のイーサネット ポートから転送されます。

7.2 および 7.4 リリースでは、ルート アクセス ポイント（RAP）のネイティブ VLAN は、メッシュ イーサネット ブリッジングと VLAN トランスペアレントを有効にしたメッシュ アクセス ポイント（MAP）のイーサネットポートから転送されません。この動作は7.6から変更されます。ネイティブ VLAN は、VLAN トランスペアレントが有効になると MAP により転送されます。

この動作の変更は信頼性を向上し、メッシュ バックホールの転送ループの発生を最小限に抑えます。

VLAN 登録

メッシュ アクセス ポイントで VLAN をサポートするには、すべてのアップリンク メッシュ アクセス ポイントが、異なる VLAN に属するトラフィックを分離できるよう同じ VLAN をサポートする必要があります。メッシュ アクセス ポイントが VLAN 要件を通信して親からの応答を得る処理は、VLAN 登録と呼ばれます。

（注） VLAN 登録は自動的に行われます。ユーザの操作は必要ありません。

VLAN 登録の概要は次のとおりです。

1. メッシュ アクセス ポイントのイーサネット ポートが VLAN で設定されている場合は、ポートから親へその VLAN をサポートすることを要求します。
2. 親は、要求をサポートできる場合、その VLAN のブリッジ グループを作成し、要求をさらにその親へ伝搬します。この伝搬は RAP に達するまで続きます。
3. 要求が RAP に達すると、RAP は VLAN 要求をサポートできるかどうかを確認します。サポートできる場合、RAP は VLAN 要求をサポートするために、ブリッジ グループとサブインターフェイスをアップリンク イーサネット インターフェイスで作成します。
4. メッシュ アクセス ポイントのいずれかの子で VLAN 要求をサポートできない場合、メッシュ アクセス ポイントはネガティブ応答を返します。この応答は、VLAN を要求したメッシュ アクセス ポイントに達するまでダウンストリーム メッシュ アクセス ポイントに伝搬されます。
5. 親からのネガティブ応答を受信した要求元メッシュ アクセス ポイントは、VLAN の設定を延期します。ただし、将来試みるときのために設定は保存されます。メッシュの動的な特性を考慮すると、ローミング時やCAPWAP再接続時に、別の親とそのアップリンク メッシュ アクセス ポイントがその設定をサポートできることがあります。

イーサネット VLAN タギングのガイドライン

イーサネット タギングは以下のガイドラインに従います。

- セキュリティ上の理由により、メッシュ アクセス ポイント（RAP および MAP）にあるイーサネット ポートはデフォルトで無効になっています。このイーサネット ポートは、メッシュ アクセス ポイント ポートでイーサネット ブリッジングを設定することにより、有効になります。
- イーサネット VLAN タギングが動作するには、メッシュ ネットワーク内の全メッシュ アクセス ポイントでイーサネット ブリッジングが有効である必要があります。
- VLAN モードは、非 VLAN トランスペアレントに設定する必要があります（グローバル メッシュ パラメータ）。「グローバル メッシュ パラメータの設定（CLI）」の項を参照してください。VLAN トランスペアレントは、デフォルトで有効になっています。非VLAN トランスペアレントとして設定するには、[Wireless] > [Mesh] ページで [VLAN transparent] オプションを選択しない必要があります。

- VLAN タギングは、次のようにイーサネット インターフェイスでだけ設定できます。
  - AP1500 では、4 つのポートのうちポート 0（PoE 入力）、ポート 1（PoE 出力）、およびポート 3（光ファイバ）の 3 つをセカンダリ イーサネット インターフェイスとして使用できます。ポート2（ケーブルモデム）は、セカンダリ イーサネット インターフェイスとして設定できません。
  - イーサネット VLAN タギングでは、RAP のポート 0（PoE 入力）は、有線ネットワークのスイッチのトランク ポートへの接続に使用します。MAP のポート 1（PoE 出力）は、ビデオ カメラなどの外部デバイスへの接続に使用します。
- バックホール インターフェイス（802.11a radio）は、プライマリ イーサネット インターフェイスとして機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。プライマリ イーサネット インターフェイスに必要な設定はありません。
- 屋内メッシュ ネットワークの場合、VLAN タギング機能は、屋外メッシュ ネットワークの場合と同様に機能します。バックホールとして動作しないアクセス ポートはすべてセカンダリであり、VLAN タギングに使用できます。
- RAP にはセカンダリ イーサネット ポートがないため、VLAN タギングを RAP 上で実装できず、プライマリ ポートがバックホールとして使用されます。ただし、イーサネット ポートが 1 つの MAP では VLAN タギングを有効にすることができます。これは、MAP のイーサネット ポートがバックホールとして機能せず、結果としてセカンダリ ポートになるためです。
- 設定の変更は、バックホールとして動作するイーサネットインターフェイスに適用されません。バックホールの設定を変更しようとすると警告が表示されます。設定は、インターフェイスがバックホールとして動作しなくなった後に適用されます。
- メッシュ ネットワーク内の任意の 802.11a バックホール イーサネット インターフェイスで VLAN タギングをサポートするために設定は必要ありません。
  - これには RAP アップリンク イーサネット ポートが含まれます。登録メカニズムを使用して、必要な設定が自動的に行われます。
  - バックホールとして動作する 802.11a イーサネット リンクへの設定の変更はすべて無視され、警告が表示されます。イーサネット リンクがバックホールとして動作しなくなると、変更した設定が適用されます。
- AP1500 のポート 02（ケーブル モデム ポート）では、VLAN を設定できません（該当する場合）。ポート 0（PoE 入力）、1（PoE 出力）、および 3（光ファイバ）では VLAN を設定できます。
- 各セクターでは、最大 16 個の VLAN がサポートされています。したがって、RAP の子（MAP）によってサポートされている VLAN の累積的な数は最大 16 です。
- RAP に接続されるスイッチ ポートはトランクである必要があります。
  - スイッチのトランク ポートと RAP トランク ポートは一致している必要があります。

- RAP は常にスイッチのネイティブ VLAN ID 1 に接続する必要があります。RAP のプライマリ イーサネット インターフェイスは、デフォルトではネイティブ VLAN 1 です。
- RAP に接続されている有線ネットワークのスイッチ ポート（ポート 0–PoE 入力）は、トランク ポートでタグ付きパケットを許可するように設定する必要があります。RAP は、メッシュ ネットワークから受信したすべてのタグ付きパケットを有線ネットワークに転送します。
- メッシュ セクター宛以外の VLAN をスイッチのトランク ポートに設定しないでください。

- MAP イーサネット ポートで設定した VLAN は、管理 VLAN として機能できません。
- メッシュ アクセス ポイントが CAPWAP RUN 状態であり、VLAN トランスペアレント モードが無効な場合にのみ、設定は有効です。
- ローミングする場合、または CAPWAP が再び開始される場合は、必ず設定の適用が再び試行されます。

イーサネット VLAN タギングの有効化（GUI）

VLAN タギングを設定する前に、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。

GUI を使用して RAP または MAP で VLAN タギングを有効にする手順は、次のとおりです。

ステップ 1 イーサネット ブリッジングを有効にしてから、[Wireless] > [All APs] を選択します。

ステップ 2 VLAN タギングを有効にするメッシュ アクセス ポイントの AP 名のリンクをクリックします。

ステップ 3 詳細ページで、[Mesh] タブを選択します。

ステップ 4 [Ethernet Bridging] チェックボックスを選択してこの機能を有効にし、[Apply] をクリックします。

ページの最下部の [Ethernet Bridging] セクションに、メッシュ アクセス ポイントの 4 つのイーサネット ポートそれぞれが一覧表示されます。

- MAP のアクセス ポートを設定する場合は、たとえば、[gigabitEthernet1]（ポート 1（PoE 出力））をクリックします。

  [Mode] ドロップダウン リストで [Access] を選択します。

  VLAN ID を入力します。VLAN ID には 1 ～ 4095 の任意の値を入力できます。

  [Apply] をクリックします。

  （注） VLAN ID 1 はデフォルト VLAN として予約されていません。

  （注） RAP のすべての従属 MAP 全体で最大 16 の VLAN がサポートされています。

- RAP または MAP のトランク ポートを設定する場合は、[gigabitEthernet0]（ポート 0（PoE 入力））をクリックします。

[Mode] ドロップダウン リストで [trunk] を選択します。

着信トラフィックのネイティブ VLAN ID を指定します。ネイティブ VLAN ID には 1 ～ 4095 の任意の値を入力できます。ユーザ VLAN（アクセス）に割り当てた値を割り当てないでください。

[Apply] をクリックします。

トランク VLAN ID フィールドと設定した VLAN のサマリーが、画面下部に表示されます。トランク VLAN ID フィールドは発信パケット用です。

発信パケットのトランク VLAN ID を指定します。

タグなしパケットを転送する場合、デフォルトのトランク VLAN ID 値（0）を変更しないでください（MAP-to-MAP ブリッジング、キャンパス環境）。

タグ付きパケットを転送する場合、未割り当ての VLAN ID（1 ～ 4095）を入力します（RAP から有線ネットワークのスイッチ）。

[Add] をクリックして、トランク VLAN ID を許可された VLAN リストに追加します。新しく追加した VLAN は、ページの [Configured VLANs] セクションの下に表示されます。

（注） リストから VLAN を削除するには、該当する VLAN の右にある矢印ドロップダウン リストから [Remove] オプションを選択します。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

イーサネット VLAN タギングの設定（CLI）

MAP アクセス ポートを設定するには、次のコマンドを入力します。

config ap ethernet 1 mode access enable *AP1500-MAP 50*

ここで、*AP1500-MAP* は可変の *AP* 名であり、*50* は可変のアクセス *VLAN ID* です。

RAP または MAP のトランク ポートを設定するには、次のコマンドを入力します。

config ap ethernet 0 mode trunk enable *AP1500-MAP 60*

ここで、*AP1500-MAP* は可変の *AP* 名であり、*60* は可変のネイティブ *VLAN ID* です。

VLAN をネイティブ VLAN の VLAN 許可リストに追加するには、次のコマンドを入力します。

config ap ethernet 0 mode trunk add *AP1500-MAP3 65*

ここで、*AP1500-MAP 3* は可変の *AP* 名であり、*65* は可変の *VLAN ID* です。

イーサネット VLAN タギング設定詳細の表示（CLI）

手順

- 特定のメッシュ アクセス ポイント（*AP Name*）またはすべてのメッシュ アクセス ポイント（*summary*）のイーサネットインターフェイスのVLAN設定の詳細を表示するには、次のコマンドを入力します。

  show ap config ethernet *ap-name*

- VLAN トランスペアレント モードが有効と無効のどちらであるかを確認するには、次のコマンドを入力します。

  show mesh config

ワークグループ ブリッジとメッシュ インフラストラクチャとの相互接続性

ワークグループ ブリッジ（WGB）は、イーサネット対応デバイスにワイヤレス インフラストラクチャ接続を提供できる小さいスタンドアロンユニットです。無線ネットワークに接続するためにワイヤレス クライアント アダプタを備えていないデバイスは、イーサネット ポート経由で WGB に接続できます。WGB は、ワイヤレス インターフェイスを介してルート AP に接続します。つまり、有線クライアントはワイヤレス ネットワークにアクセスできます。

WGB は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。WGB クライアントのデータ パケットでは、802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。ヘッダー内の追加 MAC は、WGB 自体のアドレスです。この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするために使用されます。

WGB アソシエーションは、各メッシュ アクセス ポイントのすべての radio でサポートされます。

現在のアーキテクチャでは、Autonomous APがワークグループブリッジとして機能しますが、1 つの radio インターフェイスだけがコントローラ接続、イーサネットインターフェースが有線クライアント接続、もう□つのradioインターフェースが無線クライアント接続に使用されます。dot11radio1（5GHz）はコントローラ（メッシュ インフラストラクチャを使用）への接続に使用でき、有線クライアントにはイーサネットインターフェースが使用できます。dot11radio 0（2.4 GHz）は無線クライアント接続に使用できます。要件に応じて、クライアント アソシエーションまたはコントローラ接続に dot11radio 1 または dot11radio 0 を使用できます。

7.0 リリースでは、ワイヤレス インフラストラクチャへのアップリンクを失ったとき、またはローミング シナリオの場合、WGB の 2 番目の radio のワイヤレス クライアントが、WGB によってアソシエート解除されません。

2 つの radio を使用する場合、1 つの radio をクライアント アクセスに使用し、もう 1 つの radio をアクセス ポイントにアクセスするために使用できます。2 つの独立した radio が 2 つの独立

した機能を実行するため、遅延の制御が向上し、遅延が低下します。また、アップリンクが失われたとき、またはローミング シナリオの場合、WGB の 2 番目の radio のワイヤレス クライアントはアソシエーション解除されません。一方の radio はルート AP（radio role）として設定し、もう一方の radio は WGB（radio role）として設定する必要があります。

（注） 一方の radio が WGB として設定された場合、もう一方の radio は WGB またはリピータとして設定できません。

次の機能を WGB と共に使用することはサポートされていません。

- アイドル タイムアウト
- Web 認証：WGB が Web 認証 WLAN にアソシエートする場合、WGB は除外リストに追加され、すべての WGB 有線クライアントが削除されます（Web 認証 WLAN はゲスト WLAN の別名です）。
- WGB 背後の有線クライアントのための MAC フィルタリング、リンク テスト、およびアイドル タイムアウト

ワークグループ ブリッジの設定

ワークグループ ブリッジ（WGB）は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。IAPP 制御メッセージの他にも、WGB クライアントのデータ パケットでは 802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。ヘッダー内の追加 MAC は、ワークグループ ブリッジ自体のアドレスです。この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするときに使用されます。

WGB アソシエーションは、すべての Cisco AP で 2.4 GHz 帯（802.11b/g）および 5 GHz 帯（802.11a）の両方でサポートされます。

サポートされているプラットフォームは、autonomous（自律型）1600、1700、2600、2700、3600、3700、1530、1550、1570 で、メッシュ アクセス ポイントに接続できる WGB として設定できます。設定手順については、『*Cisco Wireless LAN Controller Configuration Guide*』の「Cisco Workgroup Bridges」の項を参照してください。 https://www.cisco.com/c/en/us/support/wireless/8500-series-wireless-controllers/products-installation-and-configuration-guides-list.html

サポートされる WGB モードおよび機能は次のとおりです。

- WGB として設定された自律型アクセス ポイントでは Cisco IOS リリース 12.4.25d-JA 以降が動作している必要があります。

（注） メッシュ アクセス ポイントに 2 つの radio がある場合、いずれかの radio でだけワークグループ ブリッジ モードを設定できます。2 番目の radio を無効にすることをお勧めします。3 radio のアクセス ポイントは、ワークグループ ブリッジ モードをサポートしません。

- クライアント モード WGB（BSS）はサポートされていますが、インフラストラクチャ WGB はサポートされていません。クライアント モード WGB は、インフラストラクチャ WGB と同様に VLAN をトランクできません。
- ACK がクライアントから返されないため、マルチキャスト トラフィックは WGB に確実に転送されるわけではありません。マルチキャスト トラフィックがインフラストラクチャ WGB にユニキャストされると、ACK が返されます。
- Cisco IOS アクセス ポイントで一方の radio が WGB として設定された場合、もう一方の radio を WGB やリピータにすることができません。
- メッシュ アクセス ポイントでは、ワイヤレス クライアント、WGB、接続した WGB の背後の有線クライアントを含む、最大 200 のクライアントをサポートできます。
- WLAN が WPA1（TKIP）+WPA2（AES）で設定され、対応する WGB インターフェイスがこれらの暗号化の 1 つ（WPA1 または WPA2）で設定された場合、WGB はメッシュ アクセス ポイントと接続できません。

図 *10 : WGB* の *WPA* セキュリティ設定

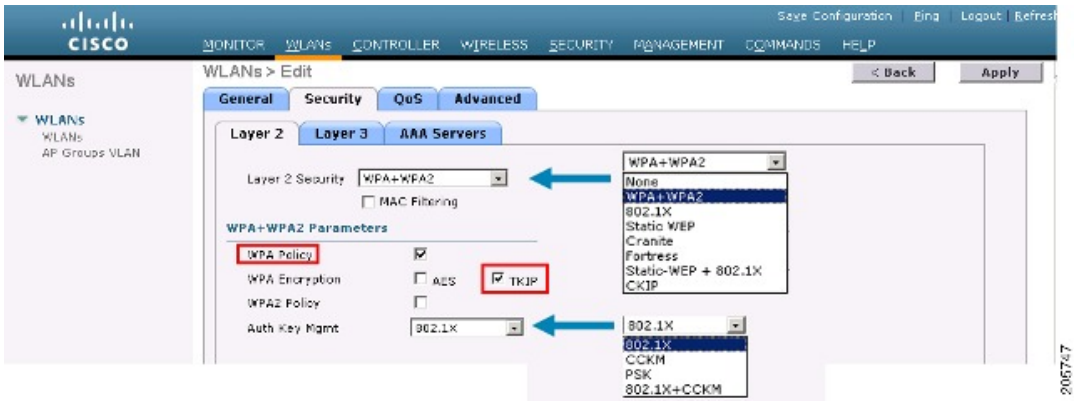
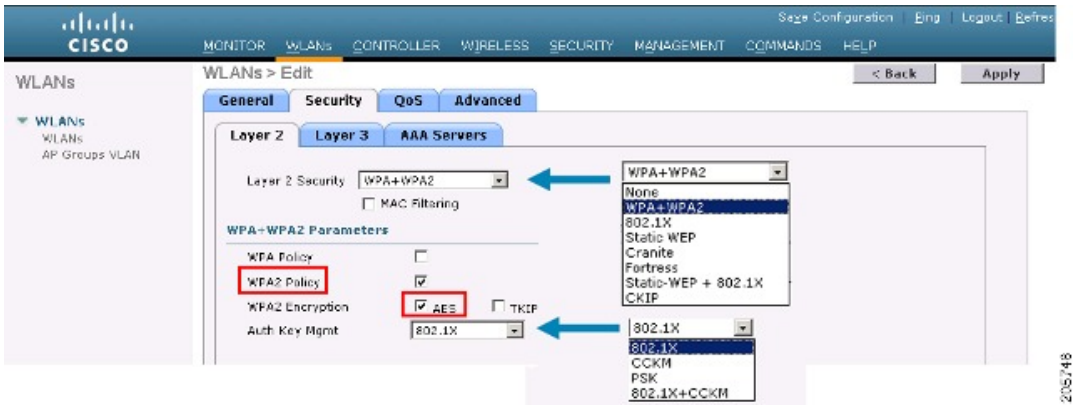


図 *11* : *WGB* の *WPA-2* セキュリティ設定



WGB クライアントのステータスを表示する手順は、次のとおりです。

ステップ 1 [Monitor] > [Clients] を選択します。

ステップ 2 クライアント サマリー ページで、クライアントの MAC アドレスをクリックするか、その MAC アドレスを使用してクライアントを検索します。

ステップ 3 表示されるページで、クライアントの種類が *WGB* として認識されていることを確認します（右端）。

図 *12* : クライアントが *WGB* であると認識されている

ステップ 4 クライアントの MAC アドレスをクリックすると、設定の詳細が表示されます。

- ワイヤレス クライアントの場合は、図 13 : [Monitor] > [Clients] > [Detail] ページ（無線 WGB クライアントの場合） （62 ページ） のようなページが表示されます。
- 有線クライアントの場合は、図 14 : [Monitor] > [Clients] > [Detail] ページ（有線 WGB クライアントの場合） （62 ページ） のようなページが表示されます。

図 *13* : *[Monitor]* > *[Clients]* > *[Detail]* ページ（無線 *WGB* クライアントの場合）

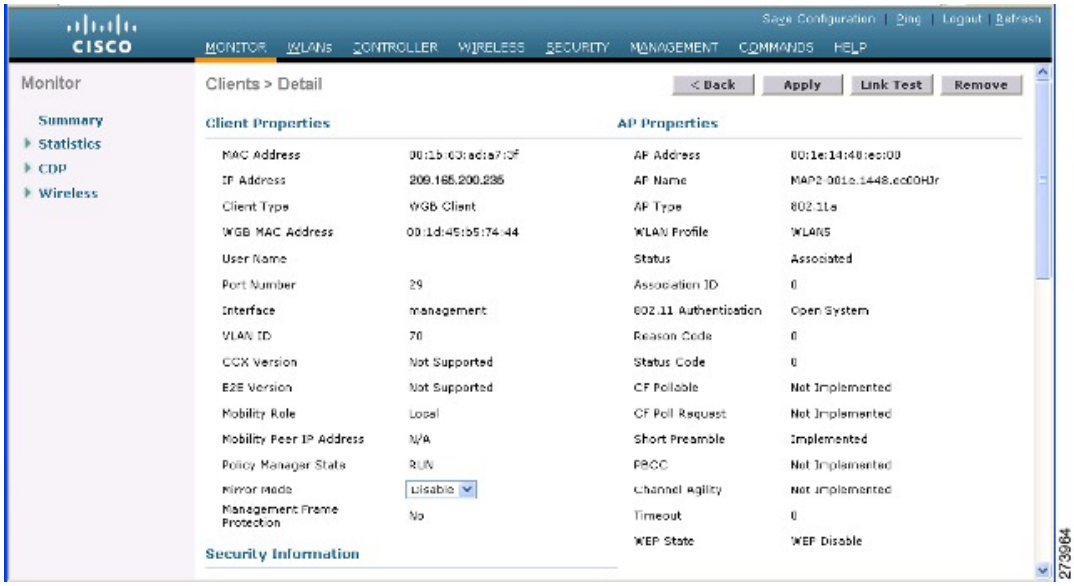
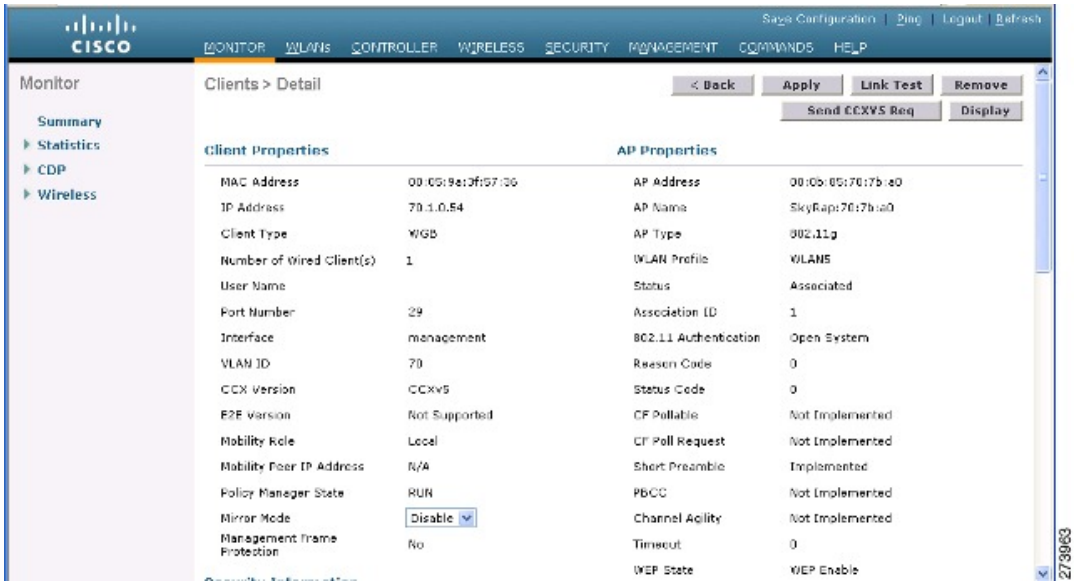


図 *14* : *[Monitor]* > *[Clients]* > *[Detail]* ページ（有線 *WGB* クライアントの場合）



設定のガイドライン

設定時は、次のガイドラインに従います。

- メッシュ アクセス ポイントで利用可能な 2 つの 5 GHz radio で強力なクライアント アクセスを利用できるよう、メッシュ AP インフラストラクチャへのアップリンクには 5 GHz radio を使用することをお勧めします。5 GHz 帯を使用すると、より大きい Effective Isotropic Radiated Power（EIRP）が許可され、品質が劣化しにくくなります。2 つの radio がある WGB では、5 GHz radio（radio 1）モードを WGB として設定します。この radio は、メッ

シュ インフラストラクチャにアクセスするために使用されます。2 番目の radio 2.4 GHz（radio 0）モードをクライアント アクセスのルート AP として設定します。

- 自律型アクセス ポイントでは、SSID を 1 つだけネイティブ VLAN に割り当てることができます。自律型アクセス ポイントでは、1 つの SSID で複数の VLAN を使用できません。SSID と VLAN のマッピングは、異なる VLAN でトラフィックを分離するために一意である必要があります。Unified アーキテクチャでは、複数の VLAN を 1 つの WLAN（SSID）に割り当てることができます。
- アクセス ポイント インフラストラクチャへの WGB のワイヤレス接続には 1 つの WLAN（SSID）だけがサポートされます。この SSID はインフラストラクチャ SSID として設定し、ネイティブ VLAN にマッピングする必要があります。
- 動的インターフェイスは、WGB で設定された各 VLAN のためにコントローラで作成する必要があります。
- アクセス ポイントの 2 番目の radio（2.4 GHz）でクライアント アクセスを設定する必要があります。両方の radio で同じ SSID を使用し、ネイティブ VLAN にマッピングする必要があります。異なる SSID を作成した場合は、一意な VLAN と SSID のマッピングの要件のため、その SSID をネイティブ VLAN にマッピングすることはできません。SSID を別の VLAN にマッピングしようとしても、ワイヤレス クライアントのための複数 VLAN サポートはありません。
- WGB でのワイヤレス クライアント接続では、WLAN（SSID）に対してすべてのレイヤ 2 セキュリティ タイプがサポートされます。
- この機能は AP プラットフォームに依存しません。コントローラ側では、メッシュ AP および非メッシュ AP の両方がサポートされます。
- WGB では、20 クライアントの制限があります。20 クライアントの制限には、有線クライアントとワイヤレス クライアントの両方が含まれます。WGB が自律型アクセス ポイントと接続する場合、クライアントの制限は非常に高くなります。
- コントローラは、ワイヤレス クライアントと WGB の背後の有線クライアントを同様に扱います。コントローラからワイヤレス WGB クライアントに対する MAC フィルタリングやリンク テストなどの機能は、サポートされません。
- 必要な場合、WGB ワイヤレス クライアントに対するリンク テストは自律型 AP から実行できます。
- WGB に接続するワイヤレス クライアントに対する複数の VLAN はサポートされません。
- 7.0 リリースから、WGB の背後の有線クライアントに対して最大 16 の複数 VLAN がサポートされます。
- ワイヤレス クライアントと WGB の背後の有線クライアントに対してローミングがサポートされます。アップリンクが失われたとき、またはローミング シナリオの場合、他の radio のワイヤレス クライアントは WGB によってアソシエート解除されません。

radio 0（2.4 GHz）をルート AP（自律型 AP の 1 つの動作モード）として設定し、radio 1（5 GHz）を WGB として設定することをお勧めします。

設定例

CLI で設定する場合に必須な項目は次のとおりです。

- dot11 SSID（WLAN のセキュリティは要件に基づいて決定できます）。
- 単一ブリッジ グループに両方の radio のサブインターフェイスをマッピングすること。

（注） ネイティブ VLAN は、デフォルトで常にブリッジ グループ 1 にマッピングされます。他の VLAN の場合、ブリッジ グループ番号は VLAN 番号に一致します。たとえば、VLAN 46 の場合、ブリッジ グループは 46 です。

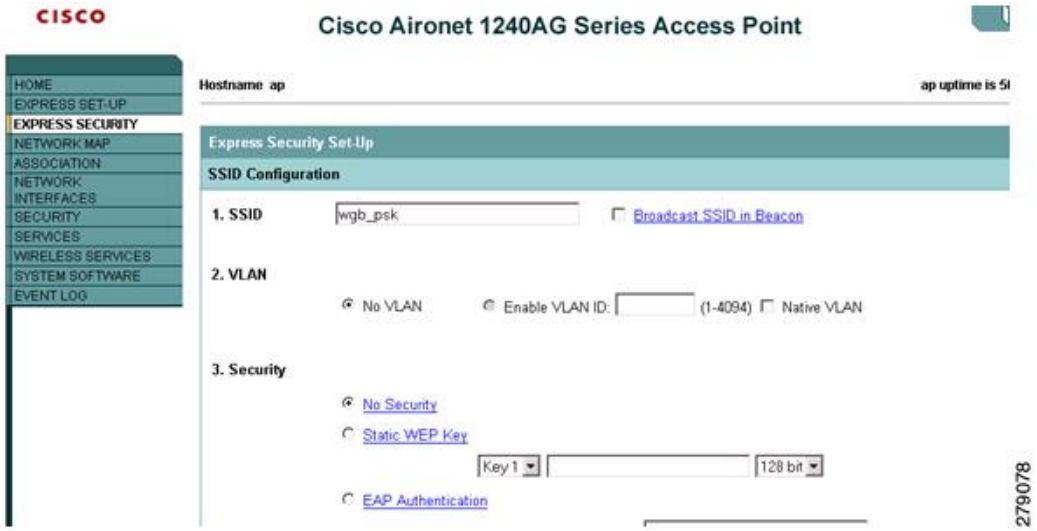
- SSID を radio インターフェイスにマッピングし、radio インターフェイスの役割を定義します。

次の例では、両方の radio で 1 つの SSID（WGBTEST）が使用され、SSID は NATIVE VLAN 51 にマッピングされたインフラストラクチャ SSID です。すべての radio インターフェイスは、ブリッジ グループ 1 にマッピングされます。

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

また、自律型 AP の GUI を使用して設定を行うこともできます。この GUI で VLAN が定義された後に、サブインターフェイスは自動的に作成されます。

図 *15 : [SSID Configuration]* ページ



WGB アソシエーションの確認

コントローラと WGB のアソシエーションおよび WGB とワイヤレス クライアントのアソシエーションの両方は、自律型 AP で **show dot11 associations client** コマンドを入力して確認できます。

```
WGB#show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :
```

MAC Address	IP Address	Device	Name	Parent	State
0024.130f.920e	209.165.200.225	LWAPP-Parent	RAPSB	-	Assoc

コントローラで、[Monitor] > [Clients] を選択します。WGB と、ワイヤレス クライアントと WGB の背後の有線クライアントは更新され、ワイヤレス/有線クライアントが WGB クライアントとして表示されます。

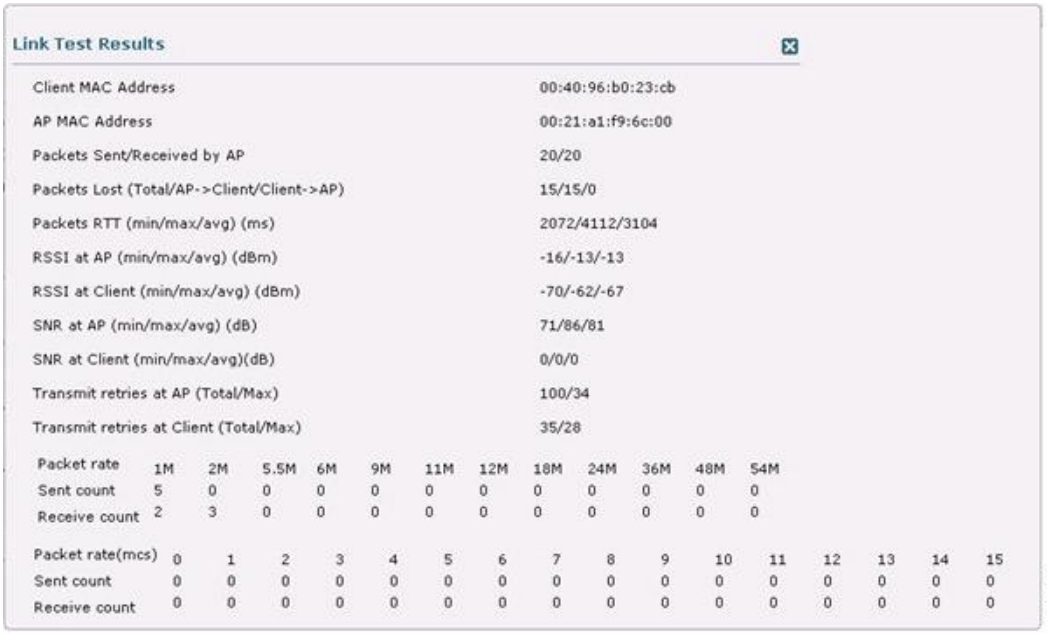
図 *16* : 更新された *WGB* クライアント

図 *17* : 更新された *WGB* クライアント

図 *18* : 更新された *WGB* クライアント

リンク テストの結果

図 *19* : リンク テストの結果



リンクテストは、コントローラのCLIから次のコマンドを使用して実行することもできます。

```
(Cisco Controller) > linktest client mac-address
```

コントローラからのリンク テストは WGB にのみ制限され、コントローラから、WGB に接続した有線クライアントやワイヤレス クライアントに対して WGB を超えて実行することはできません。WGB 自体から WGB に接続したワイヤレス クライアントのリンク テストを実行するには、次のコマンドを使用します。

```
ap#dot11 dot11Radio 0 linktest target client-mac-address
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
```

POOR (4% lost)	Time (msec)	Strength (dBm)		SNR Quality		Retries	
		In	Out	In	Out	In	Out
Sent: 100	Avg. 22	-37	-83	48	3	Tot. 34	35
Lost to Tgt: 4	Max. 112	-34	-78	61	10	Max. 10	5
Lost to Src: 4	Min. 0	-40	-87	15	3		

```
Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB 有線/ワイヤレス クライアント

また、次のコマンドを使用して、WGB と、Cisco Lightweight アクセス ポイントに接続したクライアントの概要を確認することもできます。

```
(Cisco Controller) > show wgb summary
Number of WGBs..................................... 2
```

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

```
(Cisco Controller) > show client summary

Number of Clients.................................. 7
```

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:c2	R14	Associated	1	Yes	802.11a	29	No

```
(Cisco Controller) > show wgb detail 00:1e:be:27:5f:e2

Number of wired client(s): 5
```

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth

00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No
00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes
00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

クライアント ローミング

Cisco Compatible Extension（CX）バージョン 4（v4）クライアントによる高速ローミングでは、屋外メッシュ展開において最大時速 70 マイルの速度がサポートされます。適用例としては、メッシュ パブリック ネットワーク内を移動する緊急車両の端末との通信を維持する場合があります。

3 つの Cisco CX v4 レイヤ 2 クライアント ローミング拡張機能がサポートされています。

- アクセス ポイント アシスト ローミング：クライアントのスキャン時間が短縮されます。Cisco CX v4 クライアントがアクセス ポイントに接続する際、新しいアクセス ポイントに以前のアクセス ポイントの特徴を含む情報パケットを送信します。各クライアントが接続したり、接続直後にクライアントにユニキャストを送っていたすべての以前のアクセス ポイントをまとめて作成したアクセス ポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセス ポイントのリストには、チャネル、クライアントの現在の SSID をサポートするネイバー アクセス ポイントの BSSID、およびアソシエーション解除からの経過時間が含まれます。
- 拡張ネイバー リスト：音声アプリケーションを中心に、Cisco CX v4 クライアントのローミング能力とネットワーク エッジのパフォーマンスを向上させます。アクセス ポイントは、ネイバー リストのユニキャスト更新メッセージを使用して、接続したクライアントのネイバーに関する情報を提供します。
- ローミング理由レポート：Cisco CX v4 クライアントが新しいアクセス ポイントにローミングした理由を報告できます。また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。

（注） クライアント ローミングはデフォルトでは有効です。詳細については、『Enterprise Mobility Design Guide』（http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf）を参照してください。

WGB ローミングのガイドライン

WGB ローミングのガイドラインは次のとおりです。

- WGB でのローミングの設定：WGB がモバイルである場合は、親アクセス ポイントまたはブリッジへのより良好な無線接続をスキャンするよう設定できます。ap(config-if)**mobile station period 3 threshold 50** コマンドを使用して、ワークグループ ブリッジをモバイル ステーションとして設定します。

  この設定を有効にすると、受信信号強度表示（RSSI）の数値が低いこと、電波干渉が多いこと、またはフレーム損失率が高いことが検出された場合に、WGB は新しい親への接続のためにスキャンします。これらの基準を使用して、モバイル ステーションとして設定された WGB は新しい親への接続のために検索し、現在のアソシエーションが失われる前に新しい親にローミングします。モバイル ステーションの設定が無効な場合（デフォルト設定）、WGB は現在のアソシエーションが失われるまで新しいアソシエーションを検索しません。

- WGB での限定チャネル スキャンの設定：鉄道などのモバイル環境では、WGB はすべてのチャネルをスキャンする代わりに、限定チャネルのみをスキャンするよう制限でき、WGB が 1 つのアクセス ポイントから別のアクセス ポイントにローミングするときにハンドオフによる遅延が減少します。チャネル数を制限することにより、WGB は必要なチャネルのみをスキャンします。モバイル WGB では、高速かつスムーズなローミングとともに継続的なワイヤレス LAN 接続が実現され、維持されます。この限定チャネルは、ap(config-if)#**mobile station scan** *set of channels* を使用して設定されます。

  このコマンドにより、すべてのチャネルまたは指定されたチャネルに対するスキャンが実行されます。設定できるチャネルの最大数に制限はありません。設定できるチャネルの最大数は、radio がサポートできるチャネル数に制限されます。実行時に、WGB はこの限定チャネルのみをスキャンします。この限定チャネルの機能は、WGB が現在接続しているアクセス ポイントから受け取る既知のチャネル リストにも影響します。チャネルは、そのチャネルが限定チャネルに含まれる場合にのみ、既知のチャネル リストに追加されます。

設定例

CLI で設定する場合に必須な項目は次のとおりです。

- dot11 SSID（WLAN のセキュリティは要件に基づいて決定できます）。
- 単一ブリッジ グループに両方の radio のサブインターフェイスをマッピングすること。

（注） ネイティブ VLAN は、デフォルトで常にブリッジ グループ 1 にマッピングされます。他の VLAN の場合、ブリッジ グループ番号は VLAN 番号に一致します。たとえば、VLAN 46 の場合、ブリッジ グループは 46 です。

- SSIDをradioインターフェイスにマッピングし、radioインターフェイスの役割を定義します。

次の例では、両方の radio で 1 つの SSID（WGBTEST）が使用され、SSID は NATIVE VLAN 51 にマッピングされたインフラストラクチャ SSID です。すべての radio インターフェイスは、ブリッジ グループ 1 にマッピングされます。

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

また、自律型 AP の GUI を使用して設定を行うこともできます。この GUI で VLAN が定義された後に、サブインターフェイスは自動的に作成されます。

トラブルシューティングのヒント

ワイヤレス クライアントが WGB に接続していない場合は、次の手順を実行して問題をトラブルシューティングします。

1. クライアントの設定を確認し、クライアントの設定が正しいことを確認します。
2. 自律型 AP で **show bridge** コマンドの出力を確認し、AP が適切なインターフェイスからクライアント MAC アドレスを参照していることを確認します。
3. 異なるインターフェイスの特定の VLAN に対応するサブインターフェイスが同じブリッジ グループにマッピングされていることを確認します。
4. 必要に応じて、**clear bridge** コマンドを使用してブリッジ エントリをクリアします（注：このコマンドは、WGB内の接続しているすべての有線および無線クライアントを削除し、それらのクライアントを再度接続させます）。

5. **show dot11 association** コマンドの出力を確認し、WGB がコントローラに接続していることを確認します。
6. WGB で 20 クライアントの制限を超えていないことを確認します。

通常のシナリオでは、**show bridge** コマンドの出力と **show dot11 association** コマンドの出力が期待されたものである場合、ワイヤレス クライアントの接続は成功です。

屋内メッシュ ネットワークの音声パラメータの設定

メッシュ ネットワークにおける音声およびビデオの品質を管理するために、コントローラでコール アドミッション制御（CAC）および QoS を設定できます。

屋内メッシュ アクセス ポイントは 802.11e 対応であり、QoS は、2.4 および 5 GHz のローカル AP、2.4 および 5 GHz のアクセス radio、2.4 および 5 GHz のバックホール radio でサポートされます。CAC は、バックホールおよび CCXv4 クライアントでサポートされています（メッシュ アクセス ポイントとクライアント間の CAC を提供）。

（注） 音声は、屋内メッシュ ネットワークだけでサポートされます。音声は、メッシュ ネットワークの屋外においてベストエフォート方式でサポートされます。

Call Admission Control（コール アドミッション制御）

コール アドミッション制御（CAC）を使用すると、ワイヤレス LAN で輻輳が発生した際でも、メッシュ アクセス ポイントで制御された QoS を維持できます。CCX v3 で展開される Wi-Fi Multimedia（WMM）プロトコルにより、無線 LAN に輻輳が発生しない限り十分な QoS が保証されます。ただし、さまざまなネットワーク負荷で QoS を維持するには、CCXv4 以降の CAC が必要です。

（注） CAC は Cisco Compatible Extensions（CCX）v4 以降でサポートされています。『*Cisco Wireless LAN Controller Configuration Guide, Release 7.0*』（http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html）の第 6 章を参照してください。

アクセス ポイントでは、帯域幅ベースの CAC と load-based の CAC という 2 種類の CAC が利用できます。メッシュ ネットワーク上のコールはすべて帯域幅ベースであるため、メッシュ アクセス ポイントは帯域幅ベースの CAC だけを使用します。

帯域幅ベース CAC または静的 CAC を使用すると、クライアントで新しいコールを受信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセス ポイントは、使用可能な帯域幅を確認して特定のコールに対応できるかどうかを判断し、そのコールに必要な帯域幅と比較します。品質を許容できる最大可能コール数を維持するために十分な帯域幅が使用できない場合、メッシュ アクセス ポイントはコールを拒否します。

QoS および DiffServ コード ポイントのマーキング

ローカル アクセスとバックホールでは、802.11e がサポートされています。メッシュ アクセス ポイントでは、分類に基づいて、ユーザ トラフィックの優先順位が付けられるため、すべてのユーザ トラフィックがベストエフォートの原則で処理されます。

メッシュのユーザが使用可能なリソースは、メッシュ内の位置によって異なり、ネットワークの 1 箇所に帯域幅制限を適用する設定では、ネットワークの他の部分でオーバーサブスクリプションが発生することがあります。

同様に、クライアントの RF の割合を制限することは、メッシュ クライアントに適していません。制限するリソースはクライアント WLAN ではなく、メッシュ バックホールで使用可能なリソースです。

有線イーサネット ネットワークと同様に、802.11 WLAN では、キャリア検知多重アクセス（CSMA）が導入されます。ただし、WLAN は、衝突検出（CD）を使用する代わりに衝突回避（CA）を使用します。つまり、メディアが空いたらすぐに各ステーションが伝送を行う代わりに、WLANデバイスは衝突回避メカニズムを使用して複数のステーションが同時に伝送を行うのを防ぎます。

衝突回避メカニズムでは、CWmin と CWmax という 2 つの値が使用されます。CW はコンテンション ウィンドウ（Contention Window）を表します。CW は、インターフレーム スペース（IFS）の後、パケットの転送に参加するまで、エンドポイントが待機する必要がある追加の時間を指定します。Enhanced Distributed Coordination Function（EDCF）は、遅延に影響を受けるマルチメディア トラフィックのエンド デバイスが、CWmin 値と CWmax 値を変更して、メディアに統計的に大きい（および頻繁な）アクセスを行えるようにするモデルです。

シスコのアクセス ポイントは EDCF に似た QoS をサポートします。これは最大 8 つの QoS のキューを提供します。

これらのキューは、次のようにいくつかの方法で割り当てることができます。

- パケットの TOS / DiffServ 設定に基づく
- レイヤ 2 またはレイヤ 3 アクセス リストに基づく
- VLAN に基づく
- デバイス（IP 電話）の動的登録に基づく

AP1500 は Cisco コントローラとともに、コントローラで最小の統合サービス機能（クライアント ストリームに最大帯域幅の制限がある）と、IP DSCP 値と QoS WLAN 上書きに基づいたより堅牢なディファレンシエーテッド サービス（diffServ）機能を提供します。

キュー容量に達すると、追加のフレームがドロップされます（テール ドロップ）。

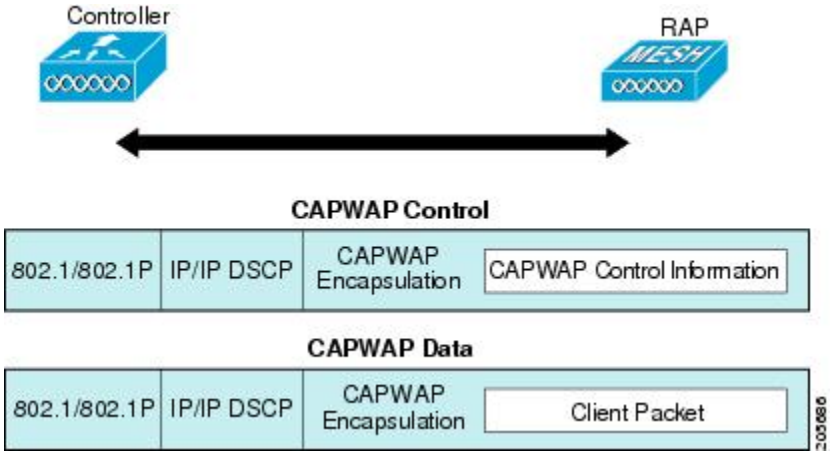
カプセル化

メッシュ システムでは複数のカプセル化が使用されます。これらのカプセル化には、コントローラと RAP 間、メッシュ バックホール経由、メッシュ アクセス ポイントとそのクライアント間の CAPWAP 制御とデータが含まれます。バックホール経由のブリッジ トラフィック（LAN

からの非コントローラ トラフィック）のカプセル化は CAPWAP データのカプセル化と同じです。

コントローラと RAP 間には 2 つのカプセル化があります。1 つは CAPWAP 制御のカプセル化であり、もう 1 つは CAPWAP データのカプセル化です。制御インスタンスでは、CAPWAP は制御情報と指示のコンテナとして使用されます。CAPWAP データのインスタンスでは、イーサネットと IP ヘッダーを含むパケット全体が CAPWAP コンテナ内で送信されます

図 *20 :* カプセル化

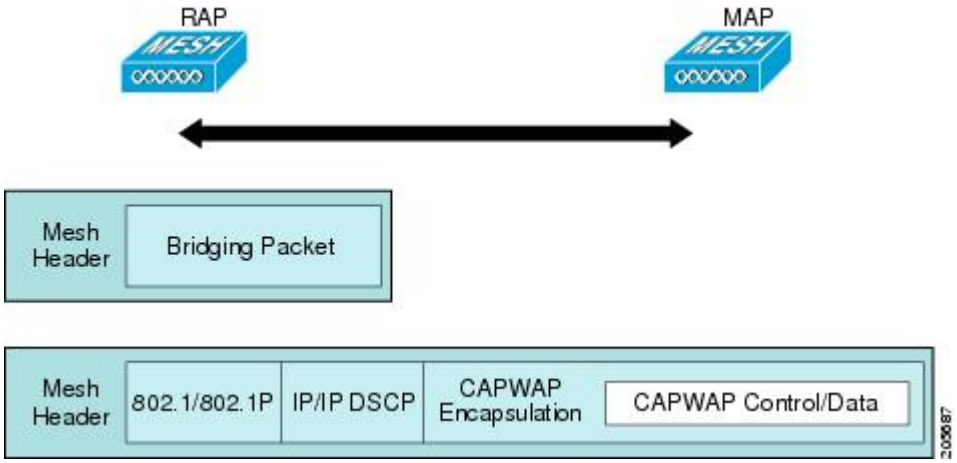


バックホールの場合、メッシュ トラフィックのカプセル化のタイプは1つだけです。ただし、2つのタイプのトラフィック（ブリッジ トラフィックとCAPWAP制御およびデータ トラフィック）がカプセル化されます。どちらのタイプのトラフィックも独自のメッシュ ヘッダーにカプセル化されます。

ブリッジ トラフィックの場合、パケットのイーサネット フレーム全体がメッシュ ヘッダーにカプセル化されます。

すべてのバックホール フレームが MAP から MAP、RAP から MAP、または MAP から RAP でも関係なく適切に処理されます。

図 *21 :* メッシュ トラフィックのカプセル化



（注） メッシュ データ DTLS 暗号化は、1540 および 1560 モデルなどの Wave 2 メッシュ AP でのみサポートされます。

メッシュ アクセス ポイントでのキューイング

メッシュ アクセス ポイントは高速の CPU を使用して、入力フレーム、イーサネット、およびワイヤレスを先着順に処理します。これらのフレームは、適切な出力デバイス（イーサネットまたはワイヤレスのいずれか）への伝送のためにキューに格納されます。出力フレームは、802.11 クライアント ネットワーク、802.11 バックホール ネットワーク、イーサネットのいずれかを宛先にすることができます。

AP1500 は、ワイヤレス クライアント伝送用に 4 つの FIFO をサポートします。これらの FIFO は 802.11e Platinum、Gold、Sliver、Bronze キューに対応し、これらのキューの 802.11e 伝送ルールに従います。FIFO では、キューの深さをユーザが設定できます。

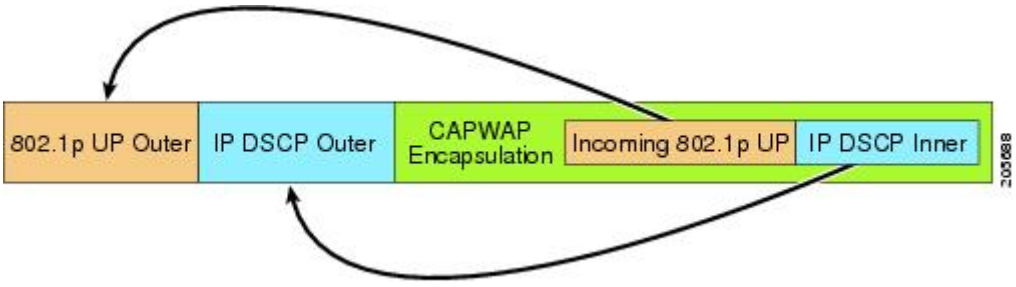
バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Siliver、および Bronze に制限されます。Platinum キューは、CAPWAP 制御トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

Gold キューの CWmin や CWmax などの 802.11e パラメータは、遅延が少なくなるように変更されています。ただし、エラー レートと積極性が若干増加します。これらの変更の目的は、ビデオ アプリケーションに使いやすいチャネルを提供することです。

イーサネット宛のフレームは FIFO として、使用可能な最大伝送バッファ プール（256 フレーム）までキューに格納されます。レイヤ 3 IP Differentiated Services Code Point（DSCP）がサポートされ、パケットのマーキングもサポートされます。

データ トラフィックのコントローラから RAP へのパスでは、外部 DSCP 値が着信 IP フレームの DSCP 値に設定されます。インターフェイスがタグ付きモードである場合、コントローラは、802.1Q VLAN ID を設定し、802.1p UP 着信と WLAN のデフォルトの優先度上限から 802.1p UP（外部）を派生させます。VLAN ID 0 のフレームはタグ付けされません。

図 *22*：コントローラから *RAP* へのパス



CAPWAP 制御トラフィックの場合、IP DSCP 値は 46 に設定され、802.1p ユーザ優先度（UP）は 7 に設定されます。バックホール経由のワイヤレス フレームの伝送の前に、ノードのペアリング（RAP/MAP）や方向に関係なく、外部ヘッダーの DSCP 値を使用して、バックホール優

先度が判断されます。次の項で、メッシュ アクセス ポイントで使用される 4 つのバックホール キューとバックホール パス QoS に示される DSCP 値のマッピングについて説明します。

表 *3:* バックホール パス *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze
26、32 ～ 63	Gold
46 ～ 56	Platinum
その他すべての値（0 を含む）	Silver

（注） Platinum バックホール キューは CAPWAP 制御トラフィック、IP 制御トラフィック、音声パケット用に予約されています。DHCP、DNS、および ARP 要求も Platinum QoS レベルで伝送されます。メッシュ ソフトウェアは、各フレームを調査し、それが CAPWAP 制御フレームであるか、IP 制御フレームであるかを判断して、Platinum キューが CAPWAP 以外のアプリケーションに使用されないようにします。

MAP からクライアントへのパスの場合、クライアントが WMM クライアントか通常のクライアントかに応じて、2 つの異なる手順が実行されます。クライアントが WMM クライアントの場合、外部フレームの DSCP 値が調査され、802.11e プライオリティ キューが使用されます。

表 *4: MAP* からクライアントへのパスの *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze
26、32 ～ 45、47	Gold
46、48 ～ 63	Platinum
その他すべての値（0 を含む）	Silver

クライアントが WMM クライアントでない場合、WLAN の上書き（コントローラで設定された）によって、パケットが伝送される 802.11e キュー（Bronze、Gold、Platinum、または Silver）が決定されます。

メッシュ アクセス ポイントのクライアントの場合、メッシュ バックホールまたはイーサネットでの伝送に備えて、着信クライアント フレームが変更されます。WMM クライアントの場合、MAP が着信 WMM クライアント フレームから外部 DSCP 値を設定する方法を示します。

図 *23 : MAP* から *RAP* へのパス

着信 802.11e ユーザ優先度および WLAN の上書き優先度の最小値が、表 5 : DSCP とバックホール キューのマッピング （77 ページ） に示された情報を使用して変換され、IP フレームの DSCP 値が決定されます。たとえば、着信フレームの優先度の値が Gold 優先度を示しているが、WLAN が Silver 優先度に設定されている場合は、最小優先度の Silver を使用して DSCP 値が決定されます。

表 *5 : DSCP* とバックホール キューのマッピング

DSCP 値	802.11e UP	バックホール キュー	パケット タイプ
2、4、6、8 ～ 23	1、2	Bronze	最小の優先度のパケット（存在する場合）
26、32 ～ 34	4、5	Gold	ビデオ パケット
46 ～ 56	6、7	Platinum	CAPWAP 制御、AWPP、DHCP/DNS、ARP パケット、音声パケット
その他すべての値（0 を含む）	0、3	Silver	ベスト エフォート、CAPWAP データ パケット

着信 WMM 優先度がない場合、デフォルトの WLAN 優先度を使用して、外部ヘッダーの DSCP 値が生成されます。フレームが（AP で）生成された CAPWAP 制御フレームの場合は、46 の DSCP 値が外部ヘッダーに配置されます。

5.2 コードでの拡張で、DSCP 情報が AWPP ヘッダーに保持されます。

Platinum キューを経由する DHCP/DNS パケットと ARP パケットを除き、すべての有線クライアント トラフィックは 5 の最大 802.1p UP 値に制限されます。

非 WMM ワイヤレス クライアントのトラフィックは、その WLAN のデフォルトの QoS 優先度を取得します。WMM ワイヤレス クライアント トラフィックには 802.11e の最大値の 6 を設定することができますが、それはその WLAN に設定された QoS プロファイル未満である必要があります。アドミッション制御を設定した場合、WMM クライアントは TSPEC シグナリングを使用し、CAC によって許可されている必要があります。

CAPWAPP データ トラフィックはワイヤレス クライアント トラフィックを伝送し、ワイヤレス クライアント トラフィックと同じ優先度を持ち、同じように扱われます。

DSCP 値が決定されたので、さらに、RAP から MAP へのバックホール パスの先述したルールを使用して、フレームを伝送するバックホール キューが決定されます。RAP からコントローラに伝送されるフレームはタグ付けされません。外部 DSCP 値は最初に作成されているため、そのままになります。

ブリッジ バックホール パケット

ブリッジサービスの処理は通常のコントローラベースのサービスと少し異なります。ブリッジパケットは、CAPWAP カプセル化されないため、外部 DSCP 値がありません。そのため、メッシュ アクセス ポイントによって受信された IP ヘッダーの DSCP 値を使用して、メッシュ アクセス ポイントからメッシュ アクセス ポイント（バックホール）までのパスに示されたようにテーブルがインデックス化されます。

LAN 間のブリッジ パケット

LAN 上のステーションから受信されたパケットは、決して変更されません。LAN 優先度の上書き値はありません。したがって、LAN は、ブリッジ モードで適切に保護されている必要があります。メッシュ バックホールに提供されている唯一の保護機能により、Platinum キューにマップされる CAPWAP 以外の制御フレームは Gold キューに降格されます。

パケットはメッシュへの着信時にイーサネット入口で受信されるため、LAN に正確に伝送されます。

AP1500 上のイーサネット ポートと 802.11a 間の QoS を統合する唯一の方法は、DSCP によってイーサネット パケットをタグ付けすることです。AP1500 は DSCP を含むイーサネット パケットを取得し、それを適切な 802.11e キューに格納します。

AP1500 では、DSCP 自体をタグ付けしません。

- AP1500 は、入力ポートで DSCP タグを確認し、イーサネット フレームをカプセル化して、対応する 802.11e 優先度を適用します。
- AP1500 は、出力ポートでイーサネット フレームのカプセル化を解除し、DSCP フィールドをそのままにして、そのフレームを回線上に配置します。

ビデオ カメラなどのイーサネット デバイスは、QoS を使用するために、DSCP 値でビットをマークする機能を持つ必要があります。

（注） QoS は、ネットワーク上で輻輳が発生したときにだけ関連します。

メッシュ ネットワークでの音声使用のガイドライン

メッシュ ネットワークで音声を使用する場合は、次のガイドラインに従います。

- 音声は、屋内メッシュ ネットワークだけでサポートされます。屋外の場合、音声は、メッシュ インフラストラクチャにおいてベストエフォート方式でサポートされます。

- 音声がメッシュ ネットワークで動作している場合、コールは3ホップ以上を通過してはいけません。音声で3ホップ以上を必要としないように、各セクターを設定する必要があります。
- 音声ネットワークの RF の考慮事項は次のとおりです。
  - 2 ～ 10 % のカバレッジ ホール
  - 15 ～ 20 % のセル カバレッジ オーバーラップ
  - 音声がデータ要件より 15 dB 以上高い RSSI 値および SNR 値を必要とする
  - すべてのデータ レートの -67 dBm の RSSI が 11b/g/n および 11a/n の目標である
  - AP に接続するクライアントにより使用されるデータ レートの SNR は 25 dB である必要がある
  - パケット エラー レートの値が 1 % 以下の値になるように設定する必要がある
  - 最小使用率のチャネル（CU）を使用する必要がある
- [802.11a/n/ac] または [802.11b/g/n] > [Global] パラメータ ページで、次のことを行う必要があります。
  - Dynamic Transmit Power Control（DTPC）を有効にする
  - 11 Mbps 未満のすべてのデータ レートを無効にする
- [802.11a/n/ac] または [802.11b/g/n] > [Voice] パラメータ ページで、次のことを行う必要があります。
  - Load-based CAC を無効にする
  - WMM が有効な CCXv4 または v5 クライアントに対してアドミッション コントロール（ACM）を有効にする。そうしない場合、帯域幅ベースの CAC は適切に動作しません。
  - 最大 RF 帯域幅を 50 % に設定する
  - 予約済みローミング帯域幅を 6 % に設定する
  - トラフィック ストリーム メトリックを有効にする
- [802.11a/n/ac] または [802.11b/g/n] > [EDCA] パラメータ ページで、次のことを行う必要があります。
  - インターフェイスの EDCA プロファイルを [Voice Optimized] に設定する
  - 低遅延 MAC を無効にする
- [QoS > *Profile*] ページで、次の手順を実行する必要があります。
  - 音声プロファイルを作成して有線 QoS プロトコル タイプとして 802.1Q を選択する

- [WLANs > *Edit* > *QoS*] ページで、次の手順を実行する必要があります。
  - バックホールの QoS として [Platinum]（音声）および [Gold]（ビデオ）を選択する
  - WMM ポリシーとして [Allowed] を選択する
- [WLANs > *Edit* > *QoS*] ページで、次の手順を実行する必要があります。
  - 高速ローミングをサポートする場合、認可（*auth*）キー管理（*mgmt*）で [CCKM] を選択します。
- [x > *y*] ページで、次の手順を実行する必要があります。
  - Voice Active Detection（VAD）を無効にする

ビデオのメッシュ マルチキャスト抑制の有効化

コントローラ CLI を使用して 3 種類のメッシュ マルチキャスト モードを設定し、すべてのメッシュ アクセス ポイントでビデオ カメラ ブロードキャストを管理できます。有効になっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは、ブリッジング対応アクセス ポイント MAP および RAP が、メッシュ ネットワーク内のイーサネット LAN 間でマルチキャストを送信する方法を決定します。メッシュ マルチキャスト モードは非 CAPWAP マルチキャスト トラフィックのみを管理します。CAPWAP マルチキャスト トラフィックは異なるメカニズムで管理されます。

次の 3 つのメッシュ マルチキャスト モードがあります。

- **regular モード**：データは、ブリッジ対応の RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにマルチキャストされます。
- **in-only モード**：MAP がイーサネットから受信するマルチキャスト パケットは RAP のイーサネット ネットワークに転送されます。追加の転送は行われず、これにより、RAP によって受信された CAPWAP 以外のマルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワーク（それらの発信ポイント）に返送されず、MAP から MAP へのマルチキャストはフィルタされるため発生しません。

（注） HSRP 設定がメッシュ ネットワークで動作中の場合は、in-out マルチキャスト モードを設定することをお勧めします。

- **in-out モード**：RAP と MAP は別々の方法でマルチキャストを行います。
  - in-out モードはデフォルトのモードです。
  - マルチキャスト パケットが、イーサネット経由で MAP で受信されると、それらは RAP に送信されますが、イーサネット経由で他の MAP に送信されず、MAP から MAP へのパケットは、マルチキャストからフィルタされます。

- マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

（注） 802.11b クライアントが CAPWAP マルチキャストを受信する必要がある場合、マルチキャストをメッシュ ネットワーク上だけでなく、コントローラ上でグローバルに有効にする必要があります（**config network multicast global enable** CLI コマンドを使用）。マルチキャストをメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない場合、グローバルなマルチキャスト パラメータを無効にする必要があります（**config network multicast global disable** CLI コマンドを使用）。

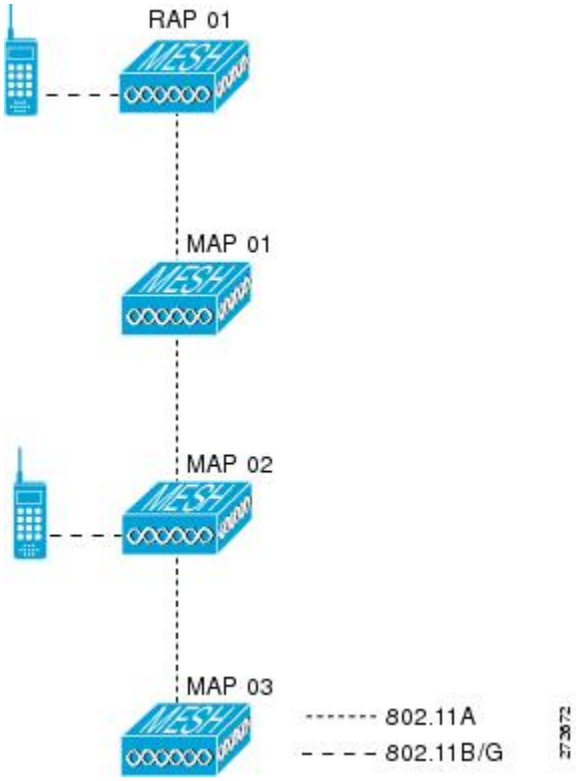
（注） AP1540/1560 は、リリース 8.5 および 8.6 で「in-out」モードのみをサポートします。その他のすべてのモードは将来のリリースでサポートされる予定です。

```
(WLAN1) >config network multicast global enable
(WLAN1) >config mesh multicast ?
 in-only        Configure Mesh Multicast In Mode.
 in-out         Configure Mesh Multicast In-Out Mode.
 regular        Configure Mesh Multicast Regular Mode.
(WLAN1) >config mesh multicast in-out
```

メッシュ ネットワークの音声詳細の表示（CLI）

この項のコマンドを使用して、メッシュ ネットワークの音声およびビデオ コールの詳細を表示します。

図 *24 :* メッシュ ネットワークの例



- 各 RAP での音声コールの合計数と音声コールに使用された帯域幅を表示するには、次のコマンドを入力します。

  show mesh cac summary

  以下に類似した情報が表示されます。

```
AP Name          Slot#   Radio  BW Used/Max  Calls
------------    -------  -----  -----------  -----
SB_RAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    2
SB_MAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP2              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP3              0   11b/g     0/23437    0
                     1   11a      0/23437    0?
```

- ネットワークのメッシュ ツリー トポロジおよび各メッシュ アクセス ポイントと radio の音声コールとビデオ リンクの帯域幅使用率（使用/最大）を表示するには、次のコマンドを入力します。

  show mesh cac bwused {**voice** | **video**} *AP_name*

  以下に類似した情報が表示されます。

```
AP Name       Slot#    Radio      BW Used/Max
```

```
------------- -------  -----      -----------
SB_RAP1         0      11b/g       1016/23437
                1      11a         3048/23437
|SB_MAP1        0      11b/g       0/23437
                1      11a         3048/23437
||  SB_MAP2     0      11b/g       2032/23437
                1      11a         3048/23437
||| SB_MAP3     0      11b/g       0/23437
                1      11a         0/23437
```

（注） [AP Name] フィールドの左側の縦棒（|）は、MAP のその RAP からのホップ数を示します。

（注） radio タイプが同じ場合、各ホップでのバックホール帯域幅使用率（bw 使用/最大）は同じです。たとえば、メッシュ アクセス ポイント *map1*、*map2*、*map3*、および *rap1* はすべて同じ radio バックホール（802.11a）上にあるので、同じ帯域幅（3048）を使用しています。コールはすべて同じ干渉ドメインにあります。そのドメインのどの場所から発信されたコールも、他のコールに影響を与えます。

- ネットワークのメッシュ ツリー トポロジを表示し、メッシュ アクセス ポイント radio によって処理中の音声コール数を表示するには、次のコマンドを入力します。

  show mesh cac access *AP_name*

```
Information similar to the following appears:

AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） メッシュ アクセス ポイント radio で受信された各コールによって、該当のコール サマリー コラムが 1 つずつ増加します。たとえば、map2 の 802.11b/g がコールを受信すると、802.11b/gの *calls* コラムにある既存の値が 1 増加します。上記の例では、map2 の 802.11b/g でアクティブなコールは、新しいコールだけです。1 つのコールがアクティブで、新しいコールが受信されると、値は 2 になります。

- ネットワークのメッシュ ツリー トポロジを表示し、動作中の音声コールを表示するには、次のコマンドを入力します。

  show mesh cac callpath *AP_name*

```
Information similar to the following appears:

AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コール パス内にある各メッシュ アクセス ポイント radio の *Calls* コラムは 1 ずつ増加します。たとえば、map2（**show mesh cac call path** *SB_MAP2*）で発信され、map1 を経由して rap1 で終端するコールの場合、1 件のコールが map2 802.11b/g と 802.11a の *calls* コラムに加わり、1 件のコールが map1 802.11a radio バックホールの *calls* コラムに加わり、1 件のコールが rap1 802.11a radio バックホールの *calls* コラムに加わります。

- ネットワークのメッシュ ツリー トポロジ、帯域幅の不足のためメッシュ アクセス ポイント無線で拒否される音声コール、拒否が発生した対応するメッシュ アクセス ポイント radio を表示するには、次のコマンドを入力します。

  show mesh cac rejected *AP_name*

  以下に類似した情報が表示されます。

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コールが map2 802.11b/g で拒否された場合、*calls* コラムは 1 ずつ増加します。

- 指定のアクセス ポイントでアクティブな Bronze、Silver、Gold、Platinum、および管理キューの数を表示するには、次のコマンドを入力します。各キューのピークおよび平均長と、オーバーフロー数が表示されます。

  show mesh queue-stats *AP_name*

  以下に類似した情報が表示されます。

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows：キュー オーバーフローによって破棄されたパケットの総数。

  Peak Length：定義された統計期間中にキューで待機していたパケットの最大数。

  Average Length：定義された統計期間中にキューで待機していたパケットの平均数。

メッシュ ネットワークにおけるマルチキャストの有効化（CLI）

（注）
- Cisco Aironet 1540 および 1560 シリーズの屋外アクセス ポイントは in-out モードのみサポートします。
- Cisco Aironet 1530、1550、および 1570 シリーズの屋外アクセス ポイントはすべてのモードをサポートします。

手順

- メッシュ ネットワークでマルチキャスト モードを有効にしてメッシュ ネットワーク外からのマルチキャストを受信するには、次のコマンドを入力します。

  config network multicast global enable

  config mesh multicast {**regular** | **in-only** | **in-out**}

- メッシュ ネットワークのみでマルチキャスト モードを有効にする（マルチキャストはメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない）には、次のコマンドを入力します。

  config network multicast global disable

  config mesh multicast {**regular** | **in-only** | **in-out**}

（注） コントローラ GUI を使用してメッシュ ネットワークのマルチキャストを有効にすることはできません。

IGMP スヌーピング

IGMP スヌーピングを使用すると、特別なマルチキャスト転送により、RF 使用率が向上し、音声およびビデオ アプリケーションでのパケット転送が最適化されます。

メッシュ アクセス ポイントは、クライアントがマルチキャスト グループに登録しているメッシュ アクセス ポイントに接続している場合にだけ、マルチキャスト パケットを伝送します。そのため、IGMP スヌーピングが有効な場合、指定したホストに関連するマルチキャスト トラフィックだけが転送されます。

コントローラ上で IGMP スヌーピングを有効にするには、次のコマンドを入力します。

configure network multicast igmp snooping enable

クライアントは、メッシュ アクセス ポイントを経由してコントローラに転送される IGMP *join* を送信します。コントローラは、*join* を傍受し、マルチキャスト グループ内のクライアントのテーブル エントリを作成します。次にコントローラはアップストリーム スイッチまたはルータを経由して、IGMP *join* をプロキシします。

次のコマンドを入力して、ルータで IGMP グループのステータスをクエリーできます。

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address    Interface   Uptime  Expires    Last Reporter
233.0.0.1        Vlan119     3w1d    00:01:52   10.1.1.130
```

レイヤ 3 ローミングの場合、IGMP クエリーはクライアントの WLAN に送信されます。コントローラはクライアントの応答を転送する前に変更し、ソース IP アドレスをコントローラの動的インターフェイス IP アドレスに変更します。

ネットワークは、コントローラのマルチキャスト グループの要求をリッスンし、マルチキャストを新しいコントローラに転送します。

音声の詳細については、次のマニュアルを参照してください。

- 『*Video Surveillance over Mesh Deployment Guide*』： http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080b02511.shtml
- 『*Cisco Unified Wireless Network Solution: VideoStream Deployment Guide*』： http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b6e11e.shtml

メッシュ AP のローカルで有効な証明書

7.0 リリースまでは、メッシュ AP は、コントローラを認証したり、コントローラに join するためにコントローラにより認証を受けたりするために、製造元がインストールした証明書（MIC）しかサポートしていませんでした。CA の制御、ポリシーの定義、有効な期間の定義、生成された証明書の制限および使用方法の定義、および AP とコントローラでインストールされたこれらの証明書の取得を行うために、独自の公開鍵インフラストラクチャ（PKI）を用意する必要がある場合がありました。これらのユーザ生成証明書またはローカルで有効な証明書

（LSC）が AP とコントローラにある場合、デバイスはこれらの LSC を使用して join、認証、およびセッション キーの派生を行います。5.2 リリース以降では通常の AP がサポートされ、7.0 リリース以降ではメッシュ AP もサポートされるようになりました。

- AP が LSC 証明書を使用してコントローラに join できない場合の MIC へのグレースフル フォールバック：ローカル AP は、コントローラで設定された回数（デフォルト値は 3）、コントローラに join しようとします。これらの試行後に、AP は LSC を削除し、MIC を使用してコントローラに join しようとします。

  メッシュ AP は、孤立タイマーが切れ、AP がリブートされるまで LSC を使用してコントローラに join しようとします。孤立タイマーは 40 分に設定されます。リブート後に、AP は MIC を使用してコントローラに join しようとします。40 分後に AP が MIC を使用して再びコントローラに join できない場合は、AP がリブートされ、LSC を使用してコントローラに join しようとします。

  （注） メッシュ AP の LSC は削除されません。LSC は、コントローラで無効な場合にのみメッシュ AP で削除され、その結果、AP がリブートされます。

- MAP の無線プロビジョニング

設定のガイドライン

メッシュ AP に LSC を使用する場合は、次のガイドラインに従います。

- この機能により、AP からどの既存の証明書も削除されません。AP では LSC 証明書と MIC 証明書の両方を使用できます。
- AP が LSC を使用してプロビジョニングされると、AP は起動時に MIC 証明書を読み取りません。LSC から MIC に変更するには、AP をリブートする必要があります。AP は、LSC を使用して join できない場合に、フォールバックのためにこの変更を行います。
- AP で LSC をプロビジョニングするために、AP で radio をオフにする必要はありません。このことは、無線でプロビジョニングを行うことができるメッシュ AP にとって重要です。
- メッシュ AP には dot1x 認証が必要なため、CA および ID 証明書をコントローラ内のサーバにインストールする必要があります。
- LSC プロビジョニングは、MAP の場合、イーサネットと OTA（無線）を介して実行できます。その場合は、イーサネットを介してコントローラにメッシュ AP を接続し、LSC 証明書をプロビジョニングする必要があります。LSC がデフォルトになると、AP は LSC 証明書を使用して無線でコントローラに接続できます。

メッシュ AP の LSC と通常の AP の LSC の違い

CAPWAP AP は、AP モードに関係なく、join 時に LSC を使用して DTLS のセットアップを行います。メッシュ AP でもメッシュ セキュリティに証明書が使用されます。これには、親 AP を介したコントローラの dot1x 認証が含まれます。LSC を使用してメッシュ AP がプロビジョニングされたら、この目的のために LSC を使用する必要があります。これは、MIC が読み込まれないためです。

メッシュ AP は、静的に設定された dot1x プロファイルを使用して認証します。

このプロファイルは、証明書の発行元として「cisco」を使用するようハードコーディングされています。このプロファイルは、メッシュ認証にベンダー証明書を使用できるよう設定可能にする必要があります（**config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** コマンドを入力します）。

メッシュ AP の LSC を有効または無効にするには、**config mesh lsc enable/disable** コマンドを入力する必要があります。このコマンドを実行すると、すべてのメッシュ AP がリブートされます。

（注） 7.0 リリースでは、メッシュの LSC は、非常に限定された石油およびガス業界のお客様向けに提供されています。これは、隠し機能です。**config mesh lsc enable/disable** は隠しコマンドです。また、**config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** コマンドは通常のコマンドですが、"prfMaP1500LlEAuth93" プロファイルは隠しプロファイルであり、コントローラに格納されず、コントローラのリブート後に失われます。

LSC AP での証明書検証プロセス

LSC でプロビジョニングされた AP には LSC 証明書と MIC 証明書の両方がありますが、LSC 証明書がデフォルトの証明書になります。検証プロセスは次の 2 つの手順から構成されます。

1. コントローラが AP に MIC デバイス証明書を送信し、AP が MIC CA を使用してその証明書を検証します。
2. AP は LSC デバイス証明書をコントローラに送信し、コントローラは LSC CA を使用してその証明書を検証します。

LSC 機能のための証明書の取得

LSC を設定するには、まず適切な証明書を収集してコントローラにインストールする必要があります。Microsoft 2003 Server を CA サーバとして使用して、この設定を行う手順を次に示します。

LSC の証明書を取得する手順は、次のとおりです。

ステップ 1 CA サーバ（http://<ip address of caserver/crtsrv）にアクセスしてログインします。

ステップ 2 次の手順で、CA 証明書を取得します。

a) [Download a CA certificate link, certificate chain, or CRF] をクリックします。
b) 暗号化方式に [DER] を選択します。
c) [Download CA certificate] リンクをクリックし、[Save] オプションを使用して、CA 証明書をローカル マシンにダウンロードします。

ステップ 3 コントローラで証明書を使用するには、ダウンロードした証明書を PEM 形式に変換します。次のコマンドを使用して、Linux マシンでこれを変換することができます。

openssl x509 -in <input.cer> -inform DER -out <output.cer> -outform PEM

ステップ 4 次の手順で、コントローラに CA 証明書を設定します。

a) [COMMANDS] > [Download File] を選択します。
b) [File Type] ドロップダウン リストから、ファイル タイプ [Vendor CA Certificate] を選択します。
c) 証明書が保存されている TFTP サーバの情報を使用して、残りのフィールドを更新します。
d) [Download] をクリックします。

ステップ 5 WLC にデバイス証明書をインストールするには、手順 1 に従い CA サーバにログインして、次の手順を実行します。

a) [Request a certificate] リンクをクリックします。
b) [advanced certificate request] リンクをクリックします。
c) [Create and submit a request to this CA] リンクをクリックします。
d) 次の画面に移動し、[Certificate Template] ドロップダウン リストから [Server Authentication Certificate] を選択します。
e) 有効な名前、電子メール、会社、部門、市、州、および国/地域を入力します。（CAP 方式を使用して、ユーザ クレデンシャルのデータベースでユーザ名を確認する場合は忘れないでください）。

（注） 電子メールは使用されません。

f) [Mark keys as exportable] を有効にします。
g) [Submit] をクリックします。`
h) ラップトップに証明書をインストールします。

ステップ 6 ステップ 5 で取得したデバイス証明書を変換します。証明書を取得するには、インターネット ブラウザのオプションを使用して、ファイルにエクスポートします。使用しているブラウザのオプションに従い、実行します。ここで設定するパスワードは覚えておく必要があります。

証明書を変換するには、Linux マシンで次のコマンドを使用します。

openssl pkcs12 -in <input.pfx> -out <output.cer>

ステップ 7 コントローラの GUI で、[Command] > [Download File] を選択します。[File Type] ドロップダウン リストから [Vendor Device Certificate] を選択します。証明書が保存されている TFTP サーバの情報および前の手順で設定したパスワードを使用して残りのフィールドを更新し、[Download] をクリックします。

ステップ 8 コントローラをリブートして、証明書が使用できるようにします。

ステップ 9 次のコマンドを使用して、コントローラに証明書が正常にインストールされていることを確認できます。

show local-auth certificates

ローカルで有効な証明書（CLI）の設定

ローカルで有効な証明書（LSC）を設定するには、次の手順に従ってください。

ステップ 1 LSC を有効にし、コントローラで LSC CA 証明書をプロビジョニングします。

ステップ 2 次のコマンドを入力します。

config local-auth eap-profile cert-issuer vendor *prfMaP1500LlEAuth93*

ステップ 3 次のコマンドを入力して、機能をオンにします。

config mesh lsc {**enable** | **disable**}

ステップ 4 イーサネットを介してメッシュ AP に接続し、LSC 証明書のためにプロビジョニングします。

ステップ 5 メッシュ AP で証明書を取得し、LSC 証明書を使用してコントローラに join します。

図 *25 :* ローカルで有効な証明書ページ

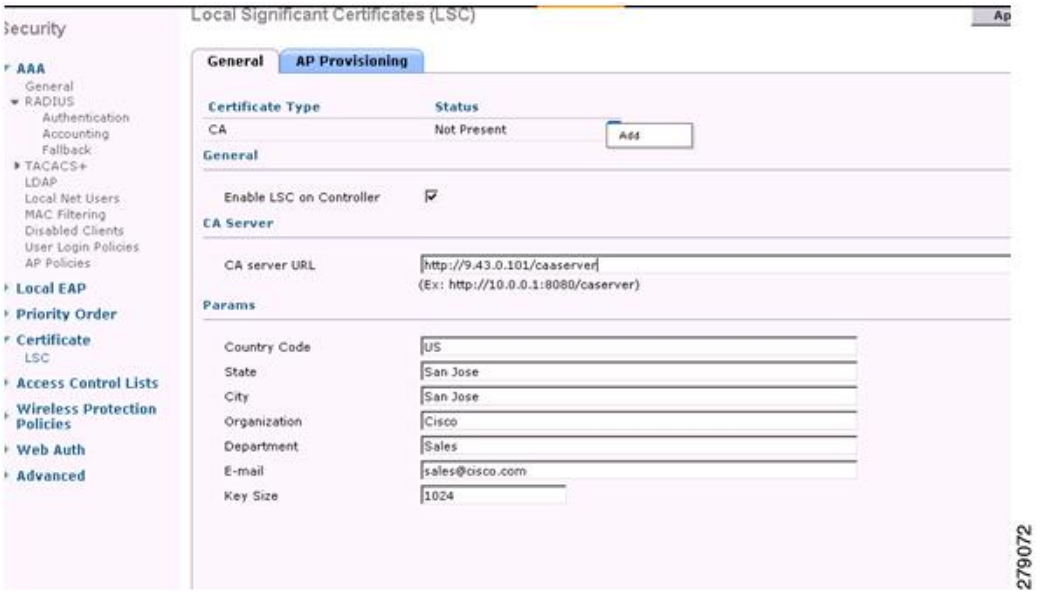


図 *26 : AP* ポリシーの設定

LSC 関連のコマンド

LSC に関連するコマンドは次のとおりです。

- **config certificate lsc** {**enable** | **disable**}
  - **enable**：システムで LSC を有効にします。
  - **disable**：システムで LSC を無効にします。LSC デバイス証明書を削除する場合や、AP にメッセージを送信して LSC デバイス証明書を削除し、LSC を無効にする場合は、このキーワードを使用します。その結果、以降の join を MIC/SSC を使用して行えるようになります。MIC/SSC に切り替わっていない AP を使用できるようにするために、WLC での LSC CA 証明書の削除は、CLI を使用して明示的に行う必要があります。

- **config certificate lsc ca-server url-path** *ip-address*

  次に、Microsoft 2003 Server 使用時の URL の例を示します。

  http:<ip address of CA>/sertsrv/mscep/mscep.dll

  このコマンドは、証明書を取得するために CA サーバへの URL を設定します。URL には、ドメイン名または IP アドレスのいずれか、ポート番号（通常は 80）、および CGI-PATH が含まれます。

  http://ipaddr:port/cgi-path

  CA サーバは 1 つだけ設定できます。CA サーバは LSC をプロビジョニングするよう設定する必要があります。

- **config certificate lsc ca-server delete**

このコマンドは、コントローラで設定された CA サーバを削除します。

- **config certificate lsc ca-cert** {**add** | **delete**}

  このコマンドは、コントローラの CA 証明書データベースに対して LSC CA 証明書を次のように追加/削除します。

  - **add**：SSCEP getca 操作を使用して、設定された CA サーバで CA 証明書を問い合わせ、WLC にログインし、WLC データベースに証明書を永久的にインストールします。インストールされたら、この CA 証明書は AP から受信された LSC デバイス証明書を検証するために使用されます。
  - **delete**：WLC データベースから LSC CA 証明書を削除します。

- **config certificate lsc subject-params** *Country State City Orgn Dept Email*

  このコマンドは、コントローラと AP で作成およびインストールされるデバイス証明書のパラメータを設定します。

  これらすべての文字列は、最大3バイトを使用する国を除き64バイトです。Common Name は、イーサネット MAC アドレスを使用して自動的に生成されます。Common Name は、コントローラ デバイス証明書要求を作成する前に提供する必要があります。

  上記のパラメータは LWAPP ペイロードとして AP に送信されるため、AP はこれらのパラメータを使用して certReq を生成できます。CN は、現在の MIC/SSC の「Cxxxx-MacAddr」形式を使用して AP で自動的に生成されます。ここで、xxxx は製品番号です。

- **config certificate lsc other-params** *keysize*

  デフォルトのキーサイズ値は 2048 ビットです。

- **config certificate lsc ap-provision** {**enable** | **disable**}

  このコマンドは、AP が SSC/MIC を使用して join した場合に、AP で LSC のプロビジョニングを有効または無効にします。有効な場合は、join し、LSC があるすべての AP がプロビジョニングされます。

  無効な場合は、自動的なプロビジョニングが行われません。このコマンドは、LSC がすでにある AP に影響を与えます。

- **config certificate lsc ra-cert** {**add** | **delete**}

  このコマンドの使用は、CA サーバが Cisco IOS CA サーバである場合にお勧めします。コントローラで RA を使用して証明書要求を暗号化すれば、通信をセキュアにできます。RA 証明書は現在、MSFT などの他の外部 CA サーバによりサポートされていません。

  - **add**：SCEP オペレーションを使用して、設定された CA サーバで RA 証明書を照会し、その証明書をコントローラ データベースにインストールします。このキーワードは、CA により署名された certReq を取得するために使用されます。
  - **delete**：WLC データベースから LSC RA 証明書を削除します。

- **config auth-list ap-policy lsc** {**enable** | **disable**}

LSC の取得後に、AP はコントローラに join を試みます。AP がコントローラに join を試みるには、その前にコントローラ コンソールで次のコマンドを入力する必要があります。デフォルトでは、**config auth-list ap-policy lsc** コマンドは無効な状態にあり、AP は LSC を使用してコントローラに join できません。

- **config auth-list ap-policy mic** {**enable** | **disable**}

  MIC の取得後に、AP はコントローラに join を試みます。AP がコントローラに join を試みるには、その前にコントローラ コンソールで次のコマンドを入力する必要があります。デフォルトでは、**config auth-list ap-policy mic** コマンドは有効な状態にあります。AP が有効なため join できない場合は、コントローラ側に「LSC/MIC AP is not allowed to join」というログ メッセージが表示されます。

- **show certificate lsc summary**

  このコマンドは、WLC にインストールされた LSC 証明書を表示します。RA 証明書もすでにインストールされている場合は、CA 証明書、デバイス証明書、および RA 証明書（オプション）を表示します。また、LSC が有効であるか有効でないかも示されます。

- **show certificate lsc ap-provision**

  このコマンドは、AP のプロビジョニングのステータス、プロビジョニングが有効であるか無効であるか、プロビジョニング リストが存在するか存在しないかを表示します。

- **show certificate lsc ap-provision details**

  このコマンドは、AP プロビジョニング リストに存在する MAC アドレスのリストを表示します。

コントローラ GUI セキュリティ設定

この設定は機能に直接関連しませんが、LSC を使用してプロビジョニングされた AP で必要な設定をするのに役立つことがあります。

- ケース 1：ローカル MAC 認可とローカル EAP 認証

  RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加します。

  例：

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- ケース 2：外部 MAC 認可とローカル EAP 認証

  WLC で次のコマンドを入力します。

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

  または

  GUI ページで外部 MAC フィルタ認可のみをオンにし、次のガイドラインに従います。

- RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加しません。
- WLC で、外部 RADIUS サーバの詳細を設定します。
- WLC で、**config macfilter mac-delimiter colon** コマンド設定を入力します。
- 外部 RADIUS サーバで、RAP/MAP の MAC アドレスを次の形式で追加します。

  User name: 11:22:33:44:55:66 Password: 11:22:33:44:55:66

展開ガイドライン

- ローカル認証を使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラにインストールされる必要があります。
- 外部 AAA サーバを使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラにインストールされる必要があります。
- メッシュ セキュリティが証明書発行元として「vendor」を使用するよう設定する必要があります。
- MAP は、バックアップ コントローラにフォール バックするときに LSC から MIC に切り替わることができません。

メッシュ AP の LSC を有効または無効にするには、**config mesh lsc** {**enable** | **disable**} コマンドを入力する必要があります。このコマンドを実行すると、すべてのメッシュ AP がリブートされます。