CHAPTER 8

メッシュ アクセス ポイントの制御

この章では、屋内および屋外用のメッシュ アクセス ポイントについて説明し、コントローラに接続してアクセス ポイント設定を管理する方法についても説明します。この章の内容は、次のとおりです。

Cisco Aironet メッシュ アクセス ポイント

コントローラ ソフトウェア リリース 6.0 では、次の Cisco Aironet メッシュ アクセス ポイントがサポートされます。

- Cisco Aironet 1520 シリーズ屋外メッシュ アクセス ポイント：1522 二重無線メッシュ アクセス ポイントおよび 1524PS/1524SB 多重無線メッシュ アクセス ポイントがあります。

（注）　メッシュ アクセス ポイントの物理的なインストレーションおよび初期設定に関する詳細については、次の URL にある『*Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html

- Cisco Aironet 1130AG および 1240AG シリーズ屋内メッシュ アクセス ポイント

（注）　AP1130 および AP1240 は、屋内メッシュ アクセス ポイントとして動作するよう変換する必要があります。「屋内アクセス ポイントのメッシュ アクセス ポイントへの変換（1130AG、1240AG）」（P.8-55）を参照してください。

（注）　この章で説明されているすべての機能は、特に記載のない限り、屋内（1130、1240）および屋外メッシュ アクセス ポイント（1522、1524PS/1524SB）に該当します。*メッシュ アクセス ポイント*または *MAP* は以降は、屋内メッシュ アクセス ポイントと屋外メッシュ アクセス ポイントの両方について言及する場合に使用されます。

（注）　Cisco Aironet 1505 および 1510 アクセス ポイントはこのリリースではサポートされていません。

（注）　メッシュ機能の概要、操作に関する注意事項、および 4.1.19x.xx メッシュ リリースからコントローラ リリース 6.0 への移行に関するソフトウェア アップグレード手順については、次の URL にある『*Release Notes for Cisco Wireless LAN Controllers and Mesh Access Points for Release 6.0*』を参照してください。

http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

5500 シリーズ コントローラでの屋内メッシュ アクセス ポイントのライセンス

5500 シリーズ コントローラで屋内メッシュ アクセス ポイントを使用するには、コントローラで WPLUS ライセンスを使用する必要があります。屋内メッシュ アクセス ポイントが基本ライセンス（WPLUS ライセンスではない）のみを使用しているコントローラに接続しようとすると、コントローラのトラップ ログに「License Not Available for feature: IndoorMeshAP」というメッセージが表示されます。コントローラのトラップ ログを表示するには、コントローラの GUI で [Monitor] を選択し、[Most Recent Traps] の下にある [View All] をクリックします。

ライセンスの入手およびインストールに関する情報は、第 4 章を参照してください。

（注）　屋外メッシュ アクセス ポイントには、WPLUS ライセンスは必要ありません。

（注）　他のコントローラ プラットフォーム（2100 および 4400 シリーズ コントローラなど）にも、屋内メッシュ アクセス ポイントを使用するためのライセンスが必要です。詳細は、次の URL にある『*Cisco Enterprise Wireless Mesh Licensing and Ordering Guide*』を参照してください。
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/ordering_guide_c07-482365.html

アクセス ポイントのロール

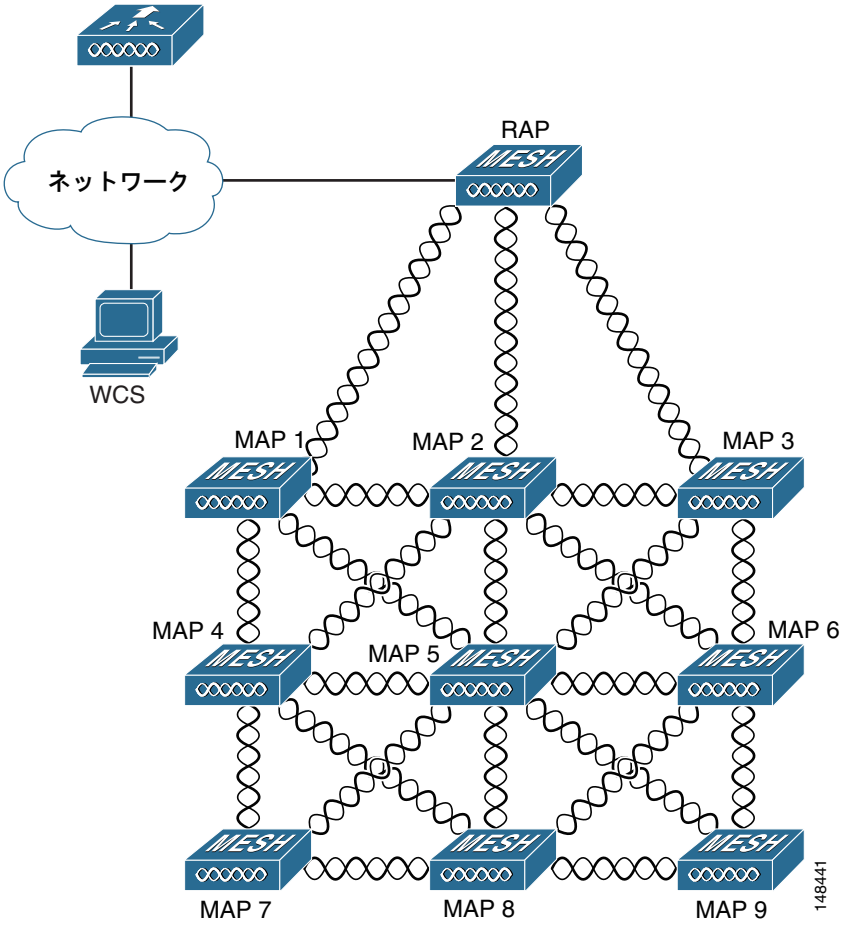
メッシュ ネットワーク内のアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）のいずれかとして動作します。

RAP はコントローラへ有線で接続され、MAP はコントローラへ無線で接続されます。

MAP は MAP 間および RAP への通信に 802.11a 無線バックホールを使用して無線接続を行います。MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。

MAP と RAP との間にある考えられるすべてのパスが無線メッシュ ネットワークを形成します。図 8-1 は、メッシュ ネットワーク内の MAP と RAP の間にある関係を示しています。

図 8-1　単純なメッシュ ネットワーク階層



ネットワーク アクセス

無線メッシュ ネットワークでは同時に 2 つの異なるトラフィック タイプ（無線 LAN クライアント トラフィックおよび MAP イーサネット ポート トラフィック）が伝送されます。

無線 LAN クライアント トラフィックはコントローラで終端し、イーサネット トラフィックはメッシュ アクセス ポイントのイーサネット ポートで終端します。

メッシュ アクセス ポイントによる無線 LAN メッシュへのアクセスは次で管理されます。

- MAC 認証：メッシュ アクセス ポイントが参照可能なデータベースに追加され、指定のコントローラおよびメッシュ ネットワークへのアクセスが可能になります。「メッシュ アクセス ポイントのメッシュ ネットワークへの追加」（P.8-11）を参照してください。
- 外部 RADIUS 認証：メッシュ アクセス ポイントは外部認証が可能で、証明書を使用する EAP-FAST クライアント認証タイプをサポートする Cisco ACS（4.1 以降）などの RADIUS サーバを使用することができます。「RADIUS サーバの設定」（P.8-14）を参照してください。

ネットワークのセグメント化

メッシュ アクセス ポイントの無線 LAN メッシュ ネットワークのメンバシップは次で制御されます。

- ブリッジ グループ名：メッシュ アクセス ポイントは、メンバシップの管理やネットワーク セグメント化のため、ブリッジ グループに配置できます。「GUI を使用したアンテナ ゲインの設定」（P.8-29）を参照してください。

展開モード

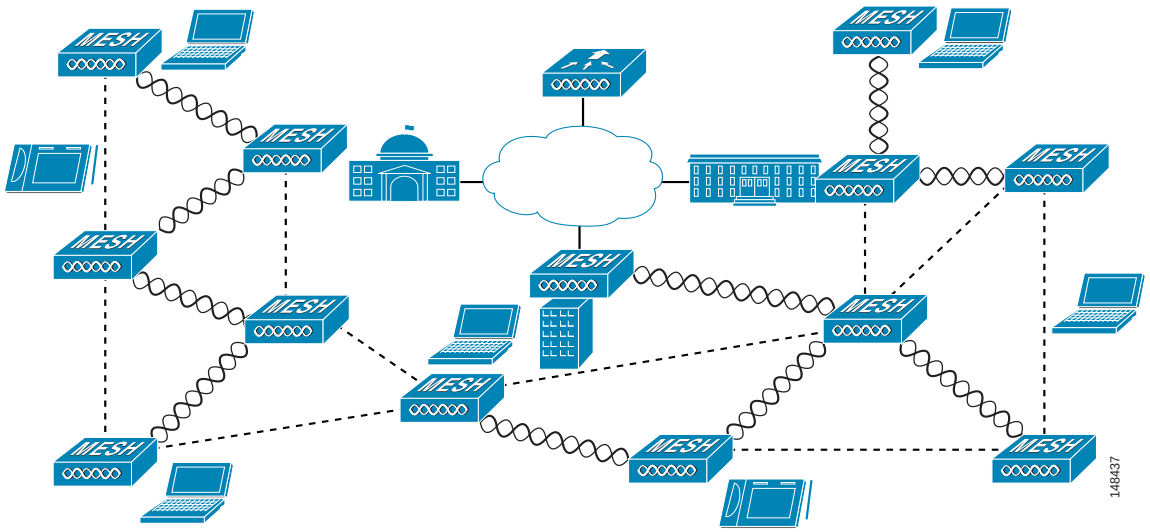
メッシュ アクセス ポイントは次のような複数の展開モードをサポートしています。

- 無線メッシュ
- WLAN バックホール
- ポイントツーマルチポイント無線ブリッジング
- ポイントツーポイント無線ブリッジング

Cisco 無線メッシュ ネットワーク

Cisco 無線屋外メッシュ ネットワークでは、複数のメッシュ アクセス ポイントによって、安全でスケーラブルな屋外無線 LAN を提供するネットワークが構成されています。図 8-2 は、メッシュ展開の一例です。

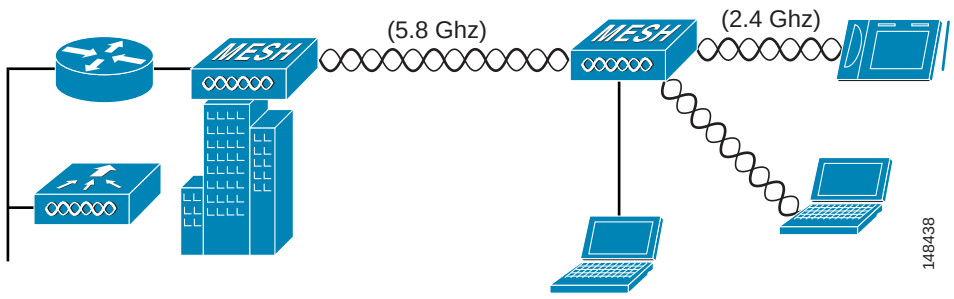
図 8-2　　無線メッシュ展開



無線バックホール

メッシュ アクセス ポイントでは、802.11b/g サービスを無線 LAN および有線クライアントに提供する、シンプルな無線バックホール ソリューションを実現できます。この構成は基本的には、1 台の MAP を備えた無線メッシュです。図 8-3 は、この展開タイプの一例です。

図 8-3　無線バックホール展開



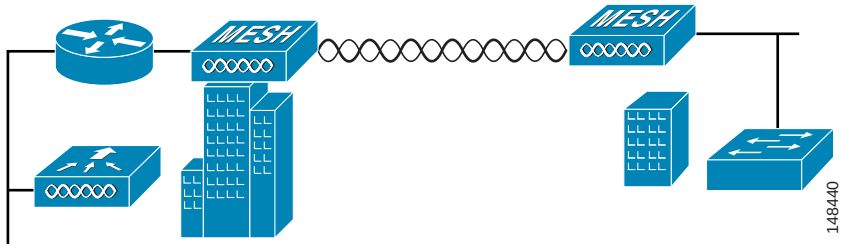
ポイントツーポイント無線ブリッジング

メッシュ アクセス ポイントは、ポイントツーポイント ブリッジングでの使用に対応しています。この展開に含まれるメッシュ アクセス ポイントは、スイッチド ネットワークの 2 つのセグメントのブリッジ処理にバックホール無線を使用して、レイヤ 2 ネットワークを拡張します（図 8-4 を参照）。これは基本的には、1 台の MAP を含み、WLAN クライアントのない無線メッシュ ネットワークです。

イーサネット ブリッジングを有効にすることでクライアントにアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

イーサネット ブリッジッド アプリケーションを使用する場合、RAP およびそのセグメント内のすべての MAP でブリッジング機能を有効にする必要があります。また、MAP のイーサネット ポートに接続されたすべてのスイッチで VLAN Trunking Protocol（VTP）を使用していないことを確認してください。VTP でによってメッシュ全体のトランキングされた VLAN が再設定される場合があるので、プライマリ WLC と RAP 間の接続が失われることがあります。設定が不適切な場合、メッシュ展開が動作しなくなることがあります。

図 8-4　無線ポイントツーポイント ブリッジ展開

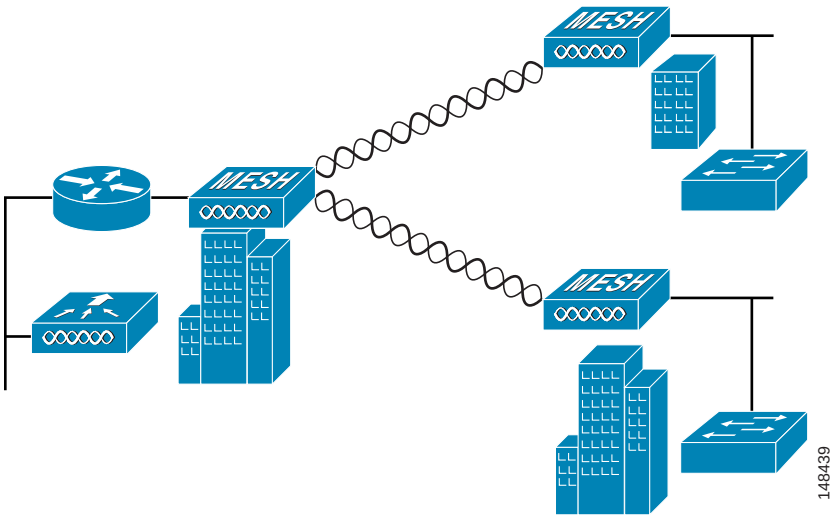


ポイントツーマルチポイント無線ブリッジング

メッシュ アクセス ポイントは、ポイントツーマルチポイント ブリッジングでの使用に対応しています。特にルート ブリッジとして動作する RAP は、複数の MAP をそれらに関連付けられた有線 LAN に非ルート ブリッジとして接続します。デフォルトでは、ブリッジングはすべての MAP で無効です。イーサネット ブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネット ブリッジングを有効にする必要があります。設定の詳細については、「イーサネット ブリッジングおよびイーサネット VLAN タギングの設定」（P.8-32）を参照してください。

図 8-5 は、1 台の RAP と 2 台の MAP を含むシンプルなポイントツーマルチポイント展開を示しています。これは基本的には、WLAN クライアントのない無線メッシュ ネットワークです。イーサネット ブリッジングを有効にすることでクライアントにアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

図 8-5　無線ポイントツーマルチポイント ブリッジ展開



アーキテクチャの概要

CAPWAP

CAPWAP は、ネットワーク内のアクセス ポイント（メッシュおよび非メッシュ）を管理するため、コントローラで使用されるプロビジョニングおよび制御プロトコルです。コントローラのソフトウェア リリース 5.2 以降では、LWAPP の代わりにこのプロトコルを使用します。

Cisco Adaptive Wireless Path Protocol 無線メッシュ ルーティング

Cisco Adaptive Wireless Path Protocol（AWPP）は、無線メッシュ ネットワーキング専用に設計されています。AWPP では、リンクの品質とホップ数に基づいてパスが決定されます。

また、AWPP の重要な要素として、展開の容易さ、高速コンバージェンス、最低限のリソース消費があります。

AWPP の目的は、RAP のブリッジ グループの一部である各 MAP から RAP への最適なパスを検出することです。これを実行するため、MAP はネイバー MAP をアクティブに要請メッセージを送信します。要請メッセージのやり取りの際に、MAP は RAP への接続に使用可能なネイバーをすべて学習し、最適なパスを提供するネイバーを決定して、そのネイバーと同期します。

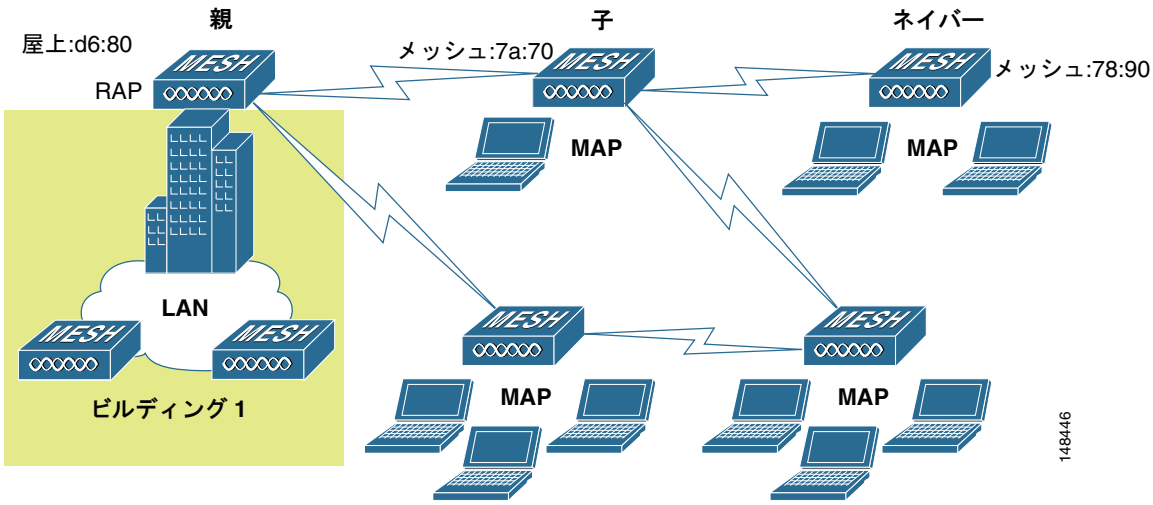
メッシュ ネイバー、親、および子

メッシュ ネットワークにおけるアクセス ポイント間の関係は、親、子、またはネイバーとして分類されます（図 8-6 を参照）。

- 親アクセス ポイントは、緩和値に基づいて RAP への最適なルートを提供します。親は RAP 自身または別の MAP のいずれかです。
  - 緩和値は各ネイバーの SNR およびリンク ホップ値を用いて計算されます。複数の選択肢がある場合、通常は緩和値の高いアクセス ポイントが選択されます。

- 子アクセス ポイントは、RAP に戻る最適なルートとして親アクセス ポイントを選択します。
- ネイバー アクセス ポイントは、別のアクセス ポイントの無線周波数（RF）の範囲内にありますが、*緩和*値が親よりも低いため、親または子として選択されません。

図 8-6　　親、子、およびネイバー アクセス ポイント



無線メッシュの制約

無線メッシュ ネットワークを設計および構築する場合に考慮する必要のあるシステムの特性は、次のとおりです。一部はバックホール ネットワーク設計、残りは CAPWAP コントローラの設計に当てはまります。

- バックホール レートは **auto** に設定することをお勧めします。

  ブリッジ データ レートを **auto** に設定すると、メッシュ バックホールでは、（すべてのレートに影響を与える条件が原因ではなく）特定のレートに対する不適切な条件のためにそのレートを使用できない場合、次善のレートが選択されます。

  - 通常は、MAP のクライアント WLAN に対する WLAN 部分の最大カバレッジに対応しているので、最適なバックホール レートとして 24 Mbp が選択されます。つまり、24 Mbp のバックホールを使用する MAP 間の距離の場合、MAP 間での WLAN クライアントのシームレスなカバレッジが可能になります。
  - 低ビット レートでは、メッシュ アクセス ポイント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、バックホール ネットワークのキャパシティが縮小される可能性があります。
  - バックホール ネットワークのビット レートを大きくすると、多数のメッシュ アクセス ポイントが必要になるか、メッシュ アクセス ポイント間の SNR が低下するため、メッシュの信頼性および相互接続が制限されます。
  - 無線メッシュ バックホールのビット レートはアクセス ポイントで設定されます。

  （注）　各アクセス ポイントのバックホールのビット レートを設定するには、[WIRELESS] > [Access Points] > [All APs] の順に選択し、AP 名をクリックして、[Mesh] タブをクリックします。

  - 各データ レートのバックホール リンクに必要な最小 LinkSNR を 表 8-1 に示します。

表 8-1　バックホールのデータ レートと LinkSNR の最小要件

データ レート	必要な最小 LinkSNR（dB）
54 Mbps	31
48 Mbps	29
36 Mbps	26
24 Mbps	22
18 Mbps	18
12 Mbps	16
9 Mbps	15
6 Mbps	14

- 必要な最小 LinkSNR はデータ レートおよび数式（最小 SNR + フェード マージン）によって決定されます。表 8-2 に、データ レート別の計算をまとめています。
  - 最小 SNR は、干渉とノイズのなく、システムのパケット エラー レート（PER）が 10% 未満の理想的な状態を表します。
  - 一般的なフェード マージンは約 9 ～ 10 dB です。
  - SNR の要件による距離は現実的ではないので、自治体のメッシュ展開で 24 Mbps を上回るデータ レートを使用することはお勧めしません。

表 8-2　データ レート別の必要最小 LinkSNR の計算

データ レート	最小 SNR（dB）+	フェード マージン =	必要な最小 LinkSNR（dB）
6	5	9	14
9	6	9	15
12	7	9	16
18	9	9	18
24	13	9	22
36	17	9	26

- バックホールのホップ数は最大 8 個ですが、3 ～ 4 個にすることをお勧めします。

  すべてのメッシュ AP はバックホール トラフィックの伝送および受信に同じ無線を使用するので、十分なバックホール スループットを維持することを主な目的として、ホップ数は 3 ～ 4 に制限することをお勧めします。これは、スループットがホップごとに約半分になることを意味しています。たとえば、24 Mbps の最大スループットは、最初のホップで約 14 Mbps、2 番目のホップで 9 Mbps、3 番目のホップで 4Mbps になります。
- RAP ごとの MAP 数

  RAP ごとに設定できる MAP 数については、今のところソフトウェアによる制限はありません。ただし、1 台の RAP につき 20 台の MAP に制限することをお勧めします。
- コントローラ数

  モビリティ グループごとのコントローラ数は 72 に制限されます。
- コントローラごとにサポートされているメッシュ アクセス ポイント数（表 8-3 を参照）

表 8-3　コントローラ モデル別にサポートされるメッシュ アクセス ポイント

コントローラ モデル	ローカル AP サポート（非メッシュ）[1]	サポート可能なメッシュ AP の最大数	RAP	MAP	サポートするメッシュ AP の合計（RAP + MAP）
5508[2]	250	250	1	249	250
			100	150	250
			150	100	250
			250	0	250
4404[3]	100	150	1	149	150
			50	100	150
			75	50	125
			100	0	100
2106[3]	6	11	1	10	11
			2	8	10
			3	6	9
			4	4	8
			5	2	7
			6	0	6
2112[2]	12	12	1	11	12
			3	9	12
			6	6	12
			9	3	12
			12	0	12
2125[2]	25	25	1	24	25
			5	20	25
			10	15	25
			15	10	25
			20	5	25
			25	0	25
WiSM[3]	300	375	1	374	375
			100	275	375
			250	100	350
			300	0	300

1. ローカル AP サポートは、コントローラ モデルでサポートされている非メッシュ AP の合計数です。
2. 5508、2112、および 2125 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。
3. 4404、2106、および WiSM コントローラの場合、MAP の数は（(ローカル AP サポート - RAP 数）x 2）になりますが、サポート可能なメッシュ AP の最大数は超えてはいけません。

メッシュ アクセス ポイントのメッシュ ネットワークへの追加

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。大規模な展開には、レイヤ 3 モードをお勧めします。

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、次の作業を行います。

1. MAP 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。「コントローラのフィルタリストに対するメッシュ アクセス ポイントの MAC アドレスの追加」（P.8-12）を参照してください。
   - 外部 RADIUS サーバを使用する MAC アドレスの外部認証を設定するには、「RADIUS サーバを使用した外部認証および認可の設定」（P.8-14）を参照してください。
2. メッシュ アクセス ポイントの DCA チャネルを設定します。詳細は、「GUI を使用したチャネルの動的割り当ての設定」（P.11-13）を参照してください。
3. メッシュ アクセス ポイントの AP モードを設定します。「AP モードの設定」（P.8-16）を参照してください。

（注）　この手順は、1520 シリーズ アクセス ポイントには必要ありません。1520 シリーズ アクセス ポイントのデフォルト モードは Bridge です。

4. 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」（P.8-17）を参照してください。
5. （必要に応じて）シリアル バックホールの RAP のチャネル割り当てを設定します。「AP1524SB のアンテナおよびチャネルの割り当て」（P.8-18）を参照してください。
6. 各 MAP のプライマリ、セカンダリ、およびターシャリ コントローラを設定します。第 7 章の「アクセス ポイントのコントローラへの接続の確認」および「バックアップ コントローラの設定」の項を参照してください。
7. 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」（P.8-23）を参照してください。
8. ブリッジリング パラメータを設定します。「イーサネット ブリッジングおよびイーサネット VLAN タギングの設定」（P.8-32）を参照してください。
   a. ブリッジ グループ名を設定します。
   b. DHCP を使用しない場合は、IP アドレスを MAP に割り当てます。

      DHCP を使用する場合は、オプション 43 およびオプション 60 を設定します。『*Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*』を参照してください。
9. （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。第 12 章「モビリティ グループの設定」を参照してください。
10. ネットワーク内での音声およびビデオの使用など、高度な機能を設定します。「拡張機能の設定」（P.8-39）を参照してください。

コントローラのフィルタ リストに対するメッシュ 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 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検出要求にだけ応答します。コントローラ上の MAC フィルタはデフォルトでは有効なので、MAC アドレスだけを設定する必要があります。

GUI または CLI のいずれかを使用してアクセス ポイントを追加できます。

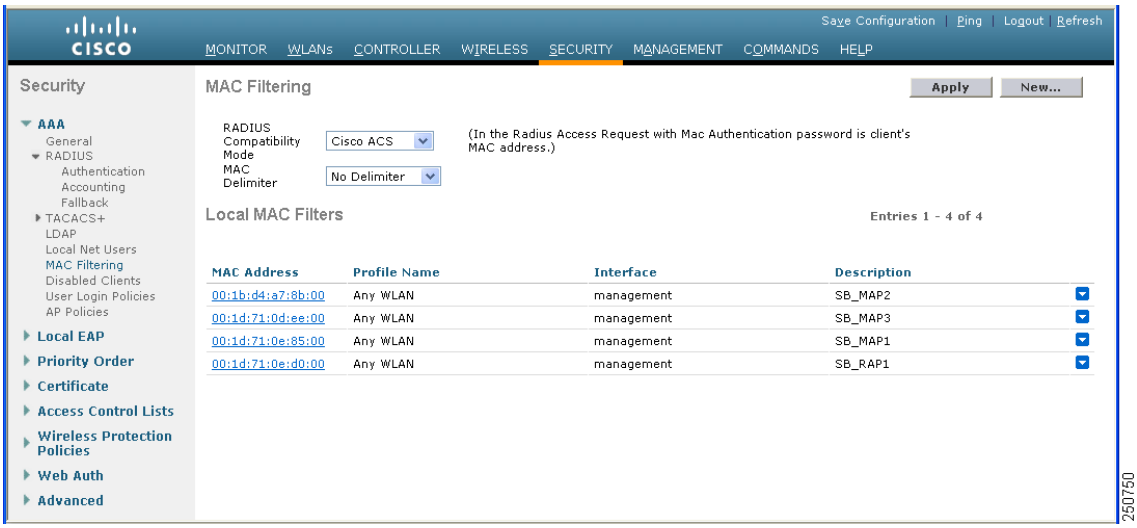
（注）　また、アクセス ポイントの MAC アドレスのリストをダウンロードし、Cisco Wireless Control System（WCS）を使用してコントローラにプッシュすることができます。手順については、『*Cisco Wireless Control System Configuration Guide, Release 6.0*』を参照してください。

GUI を使用したコントローラのフィルタ リストに対するメッシュ アクセス ポイントの MAC アドレスの追加

コントローラの GUI を使用して、コントローラでアクセス 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。

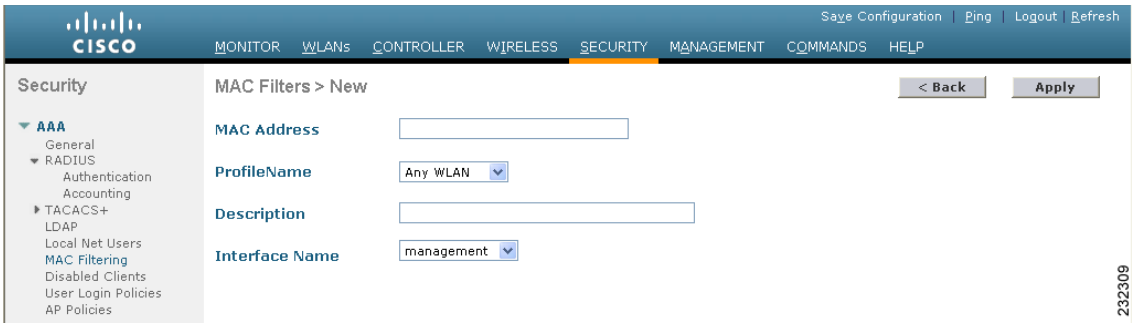
ステップ 1　[Security] > [AAA] > [MAC Filtering] の順にクリックして、[MAC Filtering] ページを開きます（図 8-7 を参照）。

図 8-7　[MAC Filtering] ページ



ステップ 2　[New] をクリックして [MAC Filters > New] ページを開きます（図 8-8 を参照）。

図 8-8　[MAC Filters > New] ページ



ステップ 3　[MAC Address] フィールドに、メッシュ アクセス ポイントの MAC アドレスを入力します。

（注）　1522 および 1524PS/1524SB 屋外メッシュ アクセス ポイントの場合、MAC フィルタとしてメッシュ アクセス ポイントの BVI MAC アドレスをコントローラに入力します。1130 および 1240 屋内メッシュ アクセス ポイントの場合、イーサネット MAC アドレスを入力します。必要な MAC アドレスがメッシュ アクセス ポイントの外部には記載されていない場合、アクセス ポイントのコンソールから **sh int | i Hardware** コマンドを入力して、BVI およびイーサネット MAC アドレスを判別します。

ステップ 4　[Profile Name] ドロップダウン ボックスから、[Any WLAN] を選択します。

ステップ 5　[Description] フィールドに、アクセス ポイントの説明を入力します。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）　*ap1522:62:39:10* などのように、省略名と最後の数桁の MAC アドレスを含めることができます。また、*屋上*、*柱上*、または交差点などの場所の詳細を入力することもできます。

ステップ 6　[Interface Name] ドロップダウン ボックスから、アクセス ポイントが接続されるコントローラ 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、変更を適用します。アクセス ポイントは [MAC Filtering] ページの MAC フィルタのリストに表示されるようになりました。

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、追加のアクセス ポイントの MAC アドレスをリストに追加します。

CLI を使用したコントローラのフィルタ リストに対するメッシュ アクセス ポイントの MAC アドレスの追加

コントローラの CLI を使用して、コントローラでアクセス 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　アクセス ポイントの MAC アドレスをコントローラのフィルタ 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

RADIUS サーバを使用した外部認証および認可の設定

コントローラ ソフトウェア リリース 5.2 以降では、Cisco ACS（4.1 以降）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。

- コントローラの AAA サーバとして使用する RADIUS サーバを設定します。
- RADIUS サーバでコントローラを設定します。
- 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」（P.8-15）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および信頼に関する情報については、「RADIUS サーバの設定」（P.8-14）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、MAC 認可だけが必要になります。

（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　Internet Explorer を使用して、Cisco Root CA 2048 の CA 証明書をダウンロードします。

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

ステップ 2　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] の順にクリックします。

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　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オンにします。

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。

（注） Cisco ACS サーバのその他の設定の詳細については、次のリンク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/tsd_products_support_series_home.html（UNIX）

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。

IOS ベースのメッシュ アクセス ポイント（1130、1240、1522、1524）の場合、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–Ethernet_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–Ethernet_MAC_address* 文字列をユーザ名として送信します。

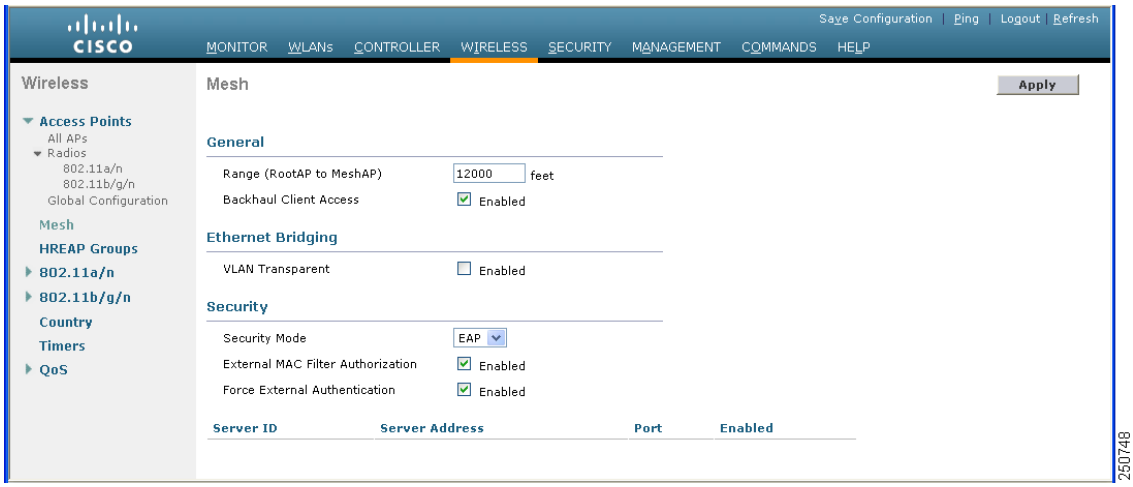
（注） *platform_name_string–Ethernet_MAC_address* 文字列だけをユーザ リストに入力する場合、AAA サーバに初回試行失敗のログが表示されます。ただし、IOS ベースのメッシュ アクセス ポイントは、*platform_name_string–Ethernet_MAC_address* 文字列をユーザ名として使用して 2 回目の試行で認証されます。

GUI を使用したメッシュ アクセス ポイントの外部認証の有効化

コントローラの 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] の順にクリックして、[Mesh] ページを開きます（図 8-9 を参照）。

図 8-9　[Mesh] ページ



ステップ 2　[Security Mode] ドロップダウン ボックスから [EAP] を選択します。

ステップ 3　[External MAC Filter Authorization] および [Force External Authentication] オプションの [Enabled] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックして、変更を適用します。

ステップ 5　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したメッシュ アクセス ポイントの外部認証の有効化

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。

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（オプション）

CLI を使用したセキュリティ統計の表示

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*

コマンドを入力すると、指定のアクセス ポイントおよびその子アクセス ポイントのパケット エラーの統計、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と再認証数が表示されます。

AP モードの設定

（注）　この手順は、1520 シリーズ アクセス ポイントには必要ありません。1520 シリーズ アクセス ポイントのデフォルト モードは Bridge です。

デフォルトではアクセス ポイントは Local として設定されます。メッシュ アクセス ポイントを設定するには、最初に GUI または CLI を使用してアクセス ポイント モードを Bridge に変更する必要があります。

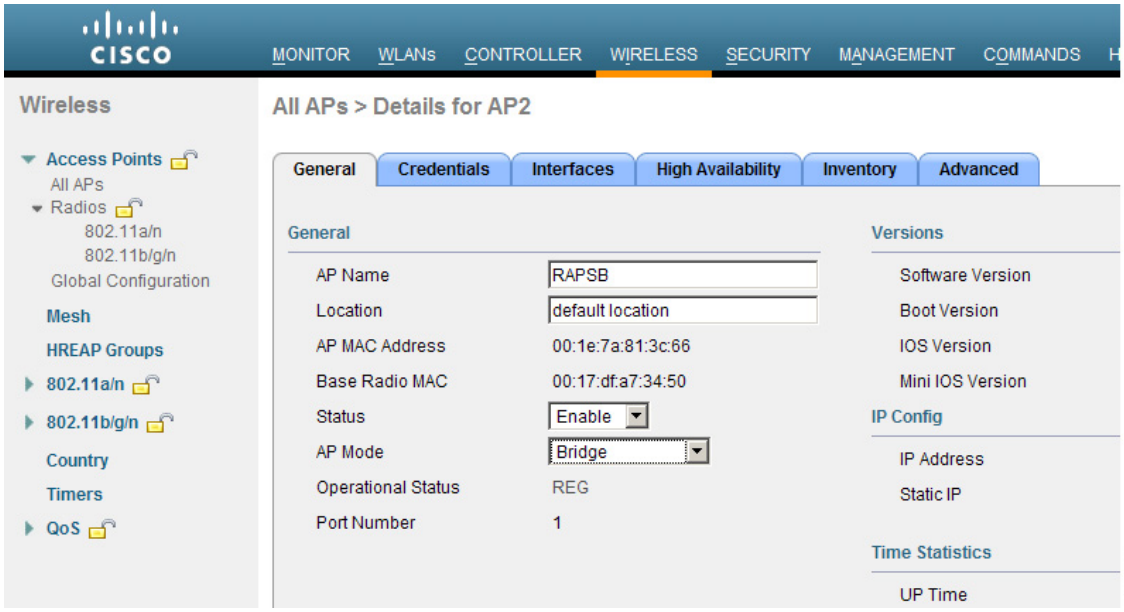
GUI を使用した AP モードの設定

GUI を使用して AP モードを設定する手順は、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（図 8-10 を参照）。

図 8-10　[[All APs > Details]（[General]）ページ



ステップ 3　[AP Mode] ドロップダウン ボックスから [Bridge] を選択します。

ステップ 4　[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。

CLI を使用した AP モードの設定

CLI を使用して AP モードを設定するには、次のコマンドを入力します。

config ap mode bridge *Cisco_AP*

メッシュ アクセス ポイントのロールの定義

152x メッシュ アクセス ポイントは、出荷時にデフォルトで無線ロールが MAP に設定されています。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。

（注）　5500 シリーズ コントローラで AP1130 および AP1240 屋内メッシュ アクセス ポイントを使用するには、コントローラで WPLUS ライセンスを使用する必要があります。

GUI を使用した AP ロールの設定

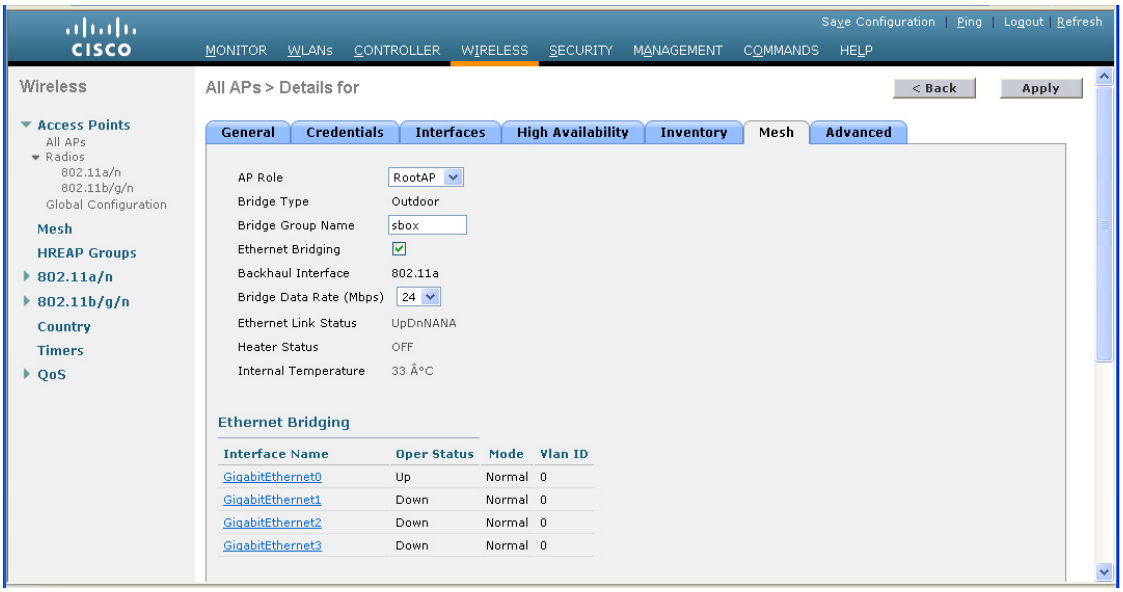
GUI を使用してメッシュ アクセス ポイントのロールを設定する手順は、次のとおりです。

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 8-11 を参照）。

図 8-11　[All APs > Details for]（[Mesh]）ページ



ステップ 4　[AP Role] ドロップダウン ボックスから [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。

CLI を使用した AP ロールの設定

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*

AP1524SB のアンテナおよびチャネルの割り当て

AP1524SB（シリアル バックホール）アクセス ポイントはコントローラ ソフトウェア リリース 6.0 で導入されました。AP1524SB にはアップリンクとダウンリンク用の 2 つのバックホール無線があります。AP1524SB は線型の展開に適しています。

AP1524SB メッシュ アクセス ポイントは RAP または MAP として動作します。AP1524SB のアンテナ ポートにはラベルが付いていて、各スロットの無線に内部的に接続されます。AP1524SB には、表 8-4 で説明するように、3 つの無線スロット（0、1、2）を備えた 6 つのポートがあります。

表 8-4　AP1524SB のアンテナ ポート

アンテナ ポート	無線スロット	説明
1	1	5 GHz バックホールおよびユニバーサル クライアント アクセスで使用
2	0	2.4 GHz クライアント アクセスで使用
3	0	2.4 GHz クライアント アクセスで使用
4	0	2.4 GHz クライアント アクセスで使用
5	–	接続なし
6	2	5 GHz バックホールで使用 **（注）** MAP のアップリンクの場合、スロット 2 無線に指向性アンテナを使用することをお勧めします。

（注） 製品モデルに応じて、AP1524SB には、5.0 GHz 無線または 5.8 GHz サブバンド無線のいずれかがスロット 1 およびスロット 2 に搭載されています。搭載されている無線に関係なく、コントローラ ソフトウェア リリース 6.0 を実行している AP1524SB では、スロット 1 およびスロット 2 は UNII-3 チャネル（149、153、157、161、および 165）に制限されます。

シリアル バックホールでは 2 つの 5.8 GHz 無線が使用されており、アップリンクおよびダウンリンクのアクセスが提供されます。各 5.8 GHz 無線バックホールには別々のバックホール チャネルが設定されるので、メッシュ ツリーベース ネットワークのノースバンドとサウスバンドのトラフィック間で同じ共有無線メディアを使用する必要はありません。

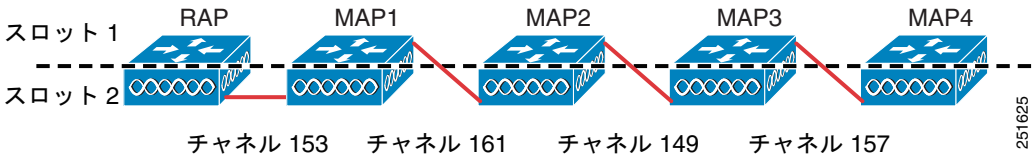
RAP の場合、スロット 2 の無線はダウンリンク方向へのバックホールの拡張に使用され、スロット 1 の無線はクライアント アクセスに使用されます。

MAP の場合、スロット 2 の無線はアップリンク方向へのバックホールに使用され、スロット 1 の無線はダウンロード方向のバックホールおよびクライアント アクセスに使用されます。

RAP ダウンリンク（スロット 2）チャネルだけを設定する必要があります。MAP では自動的に、チャネル サブセットからチャネルが選択されます。5.8 GHz 帯域で使用可能なチャネルは、149、153、157、161、および 165 です。

図 8-12 に、RAP ダウンリンク チャネルが 153 である場合のチャネル選択の一例を示します。

図 8-12　　チャネル選択の例

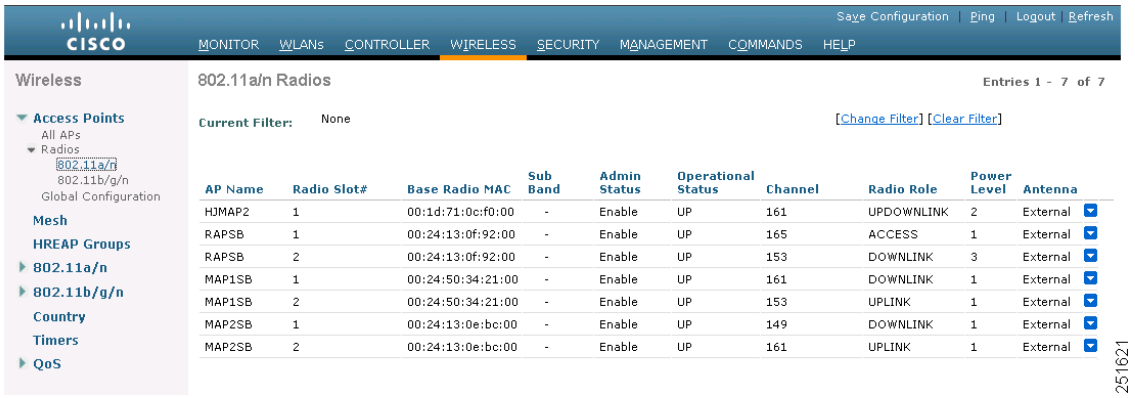


GUI を使用したシリアル バックホールでのチャネル設定

コントローラの GUI を使用して、RAP のシリアル バックホールのチャネルを設定する手順は、次のとおりです。

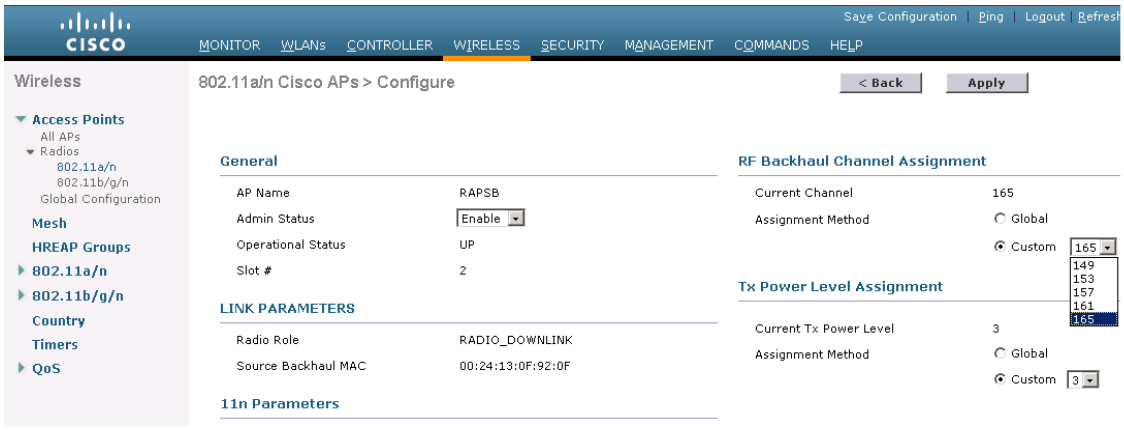
ステップ 1　[Wireless] > [Access Points] > [Radios] > [802.11a/n] の順にクリックして、[802.11a/n Radios] ページを開きます（図 8-13 を参照）。

図 8-13　　[802.11a/n Radios] ページ



ステップ 2　カーソルをスロット 2 にある RAP アンテナ（バックホール ダウンリンク）の青いドロップダウン矢印の上に置いて、[Configure] を選択します。[802.11a/n Cisco APs > Configure] ページが表示されます（図 8-14 を参照）。

図 8-14　[802.11a/n Cisco APs > Configure] ページ



ステップ 3　[RF Backhaul Channel Assignment] で割り当て方式として [Custom] を選択し、ドロップダウン リストからチャネルを選択します。5.8 GHz 帯域で使用可能なチャネルは、149、153、157、161、および 165 です。

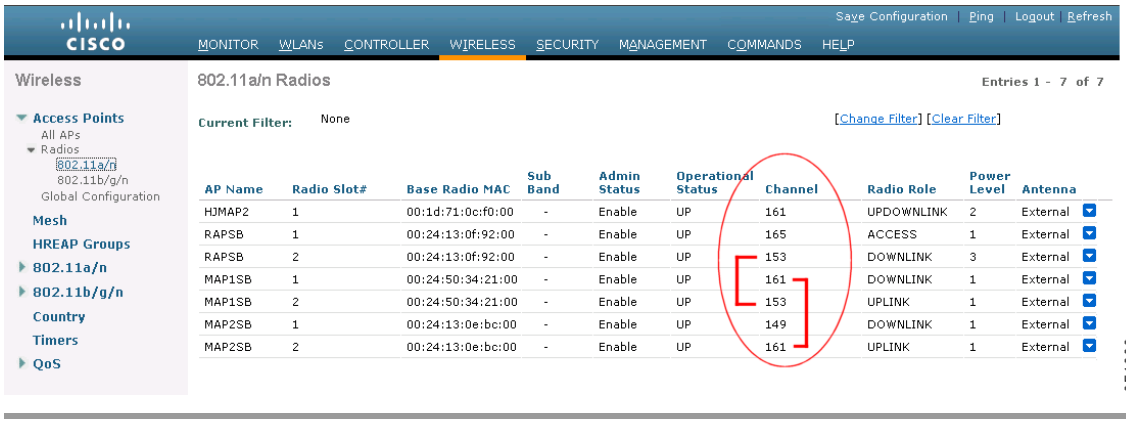
ステップ 4　[Tx Power Level Assignment] で割り当て方式として [Custom] を選択し、パワー レベルを選択します。有効な値は 1 ～ 5 で、デフォルト値は 1 です。

（注）　Radio Resource Management（RRM）はデフォルトでは無効です。バックホールで RRM は有効にすることはできません。

ステップ 5　[Apply] をクリックして、変更を適用します。

ステップ 6　[802.11a/n Radios] ページで、アップリンクおよびダウンリンク チャネルが割り当てられたことを確認します（図 8-15 を参照）。

図 8-15　チャネルの割り当て



CLI を使用したシリアル バックホールでのチャネル設定

コントローラの CLI を使用して、RAP のシリアル バックホールのチャネルを設定する手順は、次のとおりです。

ステップ 1　RAP のスロット 2 にある無線のバックホール チャネルを設定するには、次のコマンドを入力します。

config slot 2 channel ap *Cisco_RAPSB channel*

5.8 GHz 帯域で使用可能なチャネルは、149、153、157、161、および 165 です。

ステップ 2　RAP のスロット 2 にある無線の伝送パワー レベルを設定するには、次のコマンドを入力します。

config slot 2 txPower ap *Cisco_RAPSB power*

有効な値は 1 ～ 5 で、デフォルト値は 1 です。

ステップ 3　メッシュ アクセス ポイントの設定を表示するには、次のコマンドを入力します。

- **show mesh path** *MAP*

  次のような情報が表示されます。

```
AP Name/Radio      Channel Rate Link-Snr Flags    State
-----------------  ------- ---- -------- -------  -----

MAP1SB             161     auto 60       0x10ea9d54 UPDATED NEIGH PARENT BEACON
RAPSB              153     auto 51       0x10ea9d54 UPDATED NEIGH PARENT BEACON
RAPSB             is a Root AP.
```

- **show mesh backhaul** *RAPSB*

  次のような情報が表示されます。

```
Current Backhaul Slot(s)......................... 1, 2,

Basic Attributes for Slot  1
    Radio Type.................................... RADIO_TYPE_80211a
    Radio Role.................................... ACCESS
    Administrative State ......................... ADMIN_ENABLED
    Operation State .............................. UP
    Current Tx Power Level ....................... 1
    Current Channel .............................. 165
    Antenna Type.................................. EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0

Basic Attributes for Slot  2
    Radio Type.................................... RADIO_TYPE_80211a
    Radio Role.................................... RADIO_DOWNLINK
    Administrative State ......................... ADMIN_ENABLED
    Operation State .............................. UP
    Current Tx Power Level ....................... 3
    Current Channel .............................. 153
    Antenna Type.................................. EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0
```

- **show ap channel** *MAP1SB*

  次のような情報が表示されます。

```
802.11b/g Current Channel ................. 11
Slot Id ................................... 0
Allowed Channel List....................... 1,2,3,4,5,6,7,8,9,10,11
802.11a(5.8Ghz) Current Channel ........... 161
Slot Id ................................... 1
Allowed Channel List....................... 149,153,157,161,165
802.11a(5.8Ghz) Current Channel ........... 153
Slot Id ................................... 2
Allowed Channel List....................... 149,153,157,161,165
```

グローバル メッシュ パラメータの設定

この項では、アクセス ポイントを設定してコントローラとの接続を確立する方法について、次の手順も含めて説明します。

- RAP と MAP 間の最大範囲の設定（1130 および 1240 屋内メッシュ アクセス ポイントは該当しません）
- 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 タグを転送するかどうかの定義
- 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

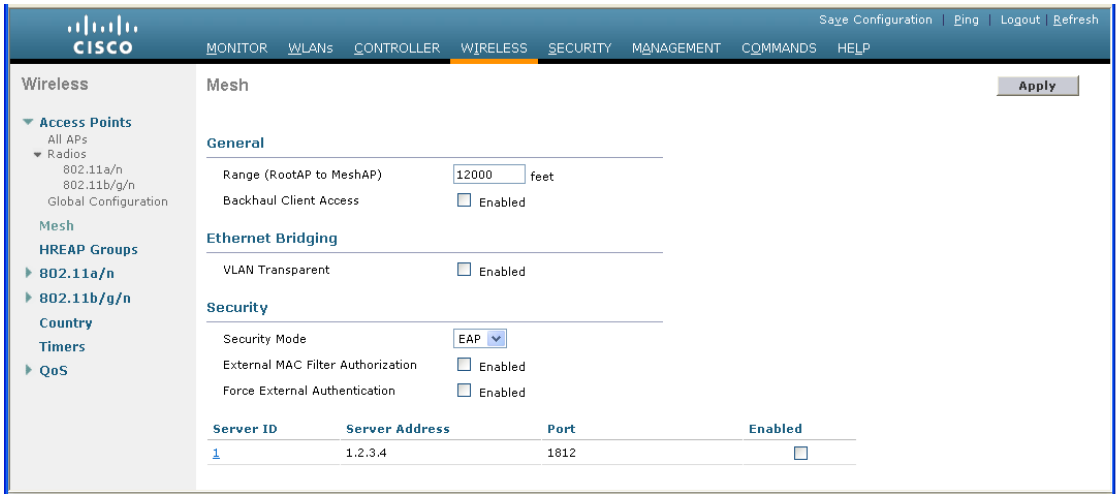
コントローラ GUI または CLI を使用して、必要なメッシュ パラメータを設定できます。パラメータはすべてグローバルに適用されます。

GUI を使用したグローバル メッシュ パラメータの設定

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] の順にクリックして、[Mesh] ページを開きます（図 8-16 を参照）。

図 8-16　[Mesh] ページ



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 8-5 に、各パラメータについての説明を示します。

表 8-5　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)	**（注）**　このパラメータは屋外メッシュ アクセス ポイントに適用されます。 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。このグローバル パラメータは、コントローラにアクセス ポイントが接続されるたびにアクセス ポイントに適用され、ネットワーク内に存在する既存のアクセス ポイントにも適用されます。 **範囲**：150 ～ 132,000 フィート **デフォルト**：12,000 フィート **（注）**　この機能を有効にした後、すべての屋外メッシュ アクセス ポイントがリブートされます。
IDS (Rogue and Signature Detection)	**（注）**　このパラメータは屋外メッシュ アクセス ポイントに適用されます。 この機能を有効にすると、バックホールのすべてのトラフィックに関して IDS レポートが生成されます。これらのレポートは、大学や企業の屋外キャンパス領域、または 4.9 GHz を利用しているユーザを検出する公共安全に携わるユーザにとって便利な場合があります。 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。 **（注）**　IDS レポートは、すべての屋内メッシュ アクセス ポイントで有効になっており、無効にすることはできません。 **デフォルト**：無効
Backhaul Client Access	**（注）**　このパラメータは、1524PS を*除く*、2 つ以上の無線を備えたメッシュ アクセス ポイントに適用されます（1524SB、1522、1240、および 1130）。 この機能を有効にすると、メッシュ アクセス ポイントで 802.11a 無線での無線クライアント アソシエーションが可能になります。したがって、メッシュ アクセス ポイントは、同じ 802.11a 無線でバックホール トラフィックおよび 802.11a クライアント トラフィックの両方を伝送できます。 この機能を無効にすると、メッシュ アクセス ポイントでは、802.11a 無線でバックホール トラフィックが伝送され、クライアント アソシエーションは 802.11b/g 無線のみで行われます。 **デフォルト**：無効 **（注）**　この機能を有効にした後、すべてのメッシュ アクセス ポイントがリブートされます。

表 8-5　グローバル メッシュ パラメータ （続き）

パラメータ	説明
VLAN Transparent	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 ブリッジド 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、「イーサネット ブリッジングおよびイーサネット VLAN タギングの設定」（P.8-32）を参照してください。 このパラメータが有効だと、VLAN タグは処理されず、タグが付いていないものとしてパケットはブリッジ処理されます。 このパラメータが無効だと、すべてのパケットには非 VLAN 透過または VLAN 不透明のタグが付けられ、すべてのタグ付きパケットがドロップされます。 VLAN タギング機能を有効にするには、チェックボックスをオフにします。 **（注）** [VLAN Transparent] は、4.1.192.xxM リリースからリリース 5.2 以降へのソフトウェア アップグレードが円滑になるよう、デフォルトで有効です。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。 **（注）** 詳細については、「イーサネット ブリッジングおよびイーサネット VLAN タギングの設定」（P.8-32）を参照してください。 **デフォルト：**有効
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オフにする）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

表 8-5　グローバル メッシュ パラメータ （続き）

パラメータ	説明
External MAC Filter Authorization	デフォルトでは、MAC フィルタリングにコントローラのローカル MAC フィルタを使用します。 外部 MAC フィルタ認可が有効なときに、ローカル MAC フィルタで MAC アドレスが検出されない場合は、外部 RADIUS サーバ内の 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アクセス ポイントの接続が防止され、不正メッシュ アクセス ポイントからネットワークが保護されます。 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。 • また、コントローラを RADIUS サーバに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、1522、1524）の場合、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-Ethernet_MAC_address* 文字列を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-Ethernet_MAC_address* 文字列をユーザ名として送信します。 **（注）** *platform_name_string-Ethernet_MAC_address* 文字列だけをユーザ リストに入力する場合、AAA サーバに初回試行失敗のログが表示されます。ただし、IOS ベースのメッシュ アクセス ポイントは、*platform_name_string–Ethernet_MAC_address* 文字列をユーザ名として使用して 2 回目の試行で認証されます。 • 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。証明書のインストールについては、「RADIUS サーバの設定」（P.8-14）の項を参照してください。 **（注）** この機能が有効でない場合、コントローラで MAC アドレス フィルタが使用され、メッシュ アクセス ポイントが認可および認証されます。 **デフォルト：**無効
Force External Authorization	[EAP] および [External MAC Filter Authorization] パラメータと一緒に有効にすると、デフォルトで外部 RADIUS サーバ（Cisco 4.1 以降など）によってメッシュ アクセス ポイントの外部認可および認証が処理されます。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] をクリックして、変更を適用します。

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

CLI を使用したグローバル メッシュ パラメータの設定

コントローラの CLI 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。

（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、「GUI を使用したグローバル メッシュ パラメータの設定」（P.8-23）を参照してください。

ステップ 1　ネットワーク内にあるすべてのアクセス ポイントの最大範囲（フィート単位）を指定するには、次のコマンドを入力します。

config mesh range *feet*

現在の範囲を確認するには、**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共有レート（Mb/s）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　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 透過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.　コントローラによってメッシュ アクセス ポイントのローカル認証を提供するには、**config mesh security {eap | psk}** コマンドを入力します。

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

CLI を使用したグローバル メッシュ パラメータ設定の表示

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** *:* クライアント アクセス バックホールの状態が有効か無効かを示します。このオプションが有効の場合、メッシュ アクセス ポイントは 802.11a バックホールで 802.11a 無線クライアントとのアソシエートが可能になります。802.11a バックホールでは、ルートとメッシュ アクセス ポイント間の既存の通信に加えて、クライアント アソシエーションが行われます。

```
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。

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

- **show mesh env** {**summary** | ***Cisco_AP***} *:* すべてのアクセス ポイント（概要）か特定のアクセス ポイント（***Cisco_AP***）のいずれかについて温度、ヒータ ステータス、およびイーサネット ステータスを示します。アクセス ポイント名、ロール（RootAP または MeshAP）、およびモデルも示されます。
  - 温度は華氏と摂氏の両方で示されます。
  - ヒータ ステータスは ON または OFF です。
  - イーサネット ステータスは UP または DOWN です。

（注）　バッテリ ステータスは、**show mesh env** *Cisco_AP* によるステータスの表示では N/A（適用されない）と記載されます（アクセス ポイントは非対応のため）。

```
controller >show mesh env summary

AP Name             Temperature(C/F)  Heater  Ethernet  Battery
------------------  ----------------  ------  --------  -------
SB_RAP1              39/102           OFF     UpDnNANA  N/A
SB_MAP1              37/98            OFF     DnDnNANA  N/A
SB_MAP2              42/107           OFF     DnDnNANA  N/A
SB_MAP3              36/96            OFF     DnDnNANA  N/A

controller >show mesh env SB_RAP1
```

```
AP Name..................................... SB_RAP1
AP Model.................................... AIR-LAP1522AG-A-K9
AP Role..................................... RootAP

Temperature................................. 39 C, 102 F
Heater...................................... OFF
Backhaul.................................... GigabitEthernet0

GigabitEthernet0 Status..................... UP
    Duplex.................................. FULL
    Speed................................... 100
    Rx Unicast Packets...................... 988175
    Rx Non-Unicast Packets.................. 8563
    Tx Unicast Packets...................... 106420
    Tx Non-Unicast Packets.................. 17122
GigabitEthernet1 Status..................... DOWN
  POE Out................................... OFF

Battery..................................... N/A
```

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、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。

- アンテナ ゲイン：「アンテナ ゲインの設定」（P.8-29）を参照してください。
- ワークグループ ブリッジ グループ：「メッシュ アクセス ポイントのワークグループ ブリッジ グループ」（P.8-31）を参照してください。

アンテナ ゲインの設定

コントローラの GUI またはコントローラの CLI を使用して、設置されたアンテナと一致するようにアクセス ポイントのアンテナ ゲインを設定します。

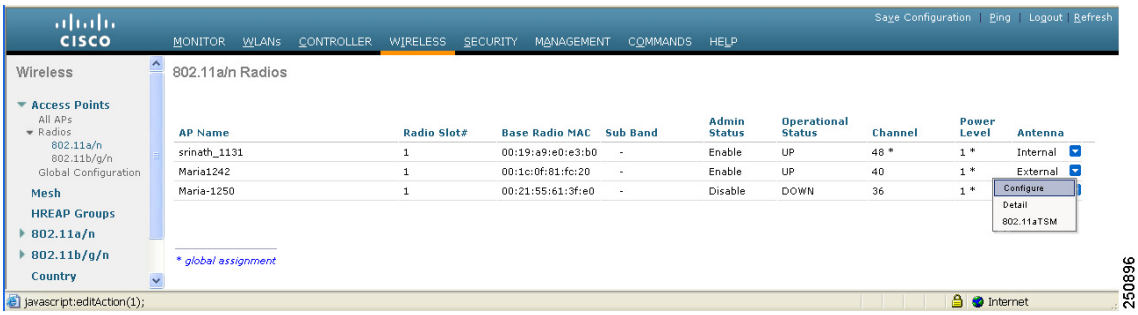
（注）　サポートされているアンテナおよびアンテナ ゲインの概要については、『*Cisco Aironet 1520 Series Outdoor Mesh Access Points Getting Started Guide*』の「External Antennas」の項を参照してください（http://www.cisco.com/en/US/docs/wireless/access_point/1520/quick/guide/ap1520qsg.html）。

GUI を使用したアンテナ ゲインの設定

コントローラの GUI を使用してアンテナ ゲインを設定する手順は、次のとおりです。

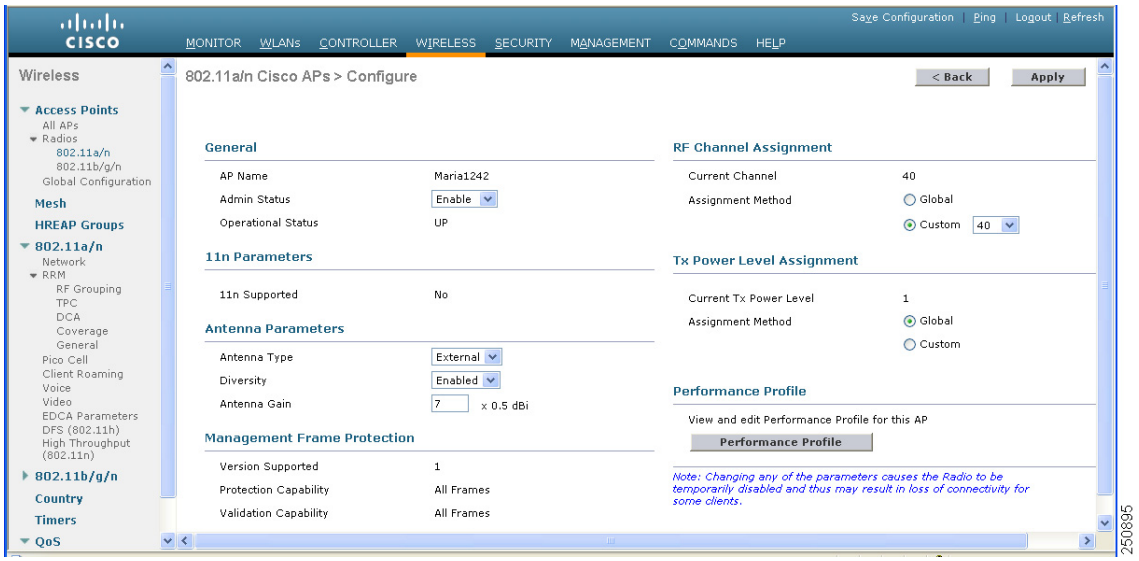
ステップ 1　[Wireless] > [Access Points] > [Radios] > [802.11a/n] の順にクリックして、[802.11a/n Radios] ページを開きます（図 8-17 を参照）。

図 8-17　[802.11a/n Radios] ページ



ステップ 2　設定するメッシュ アクセス ポイント アンテナの青いドロップダウン矢印の上にカーソルを置いて、[Configure] を選択します。[802.11a/n Cisco APs > Configure] ページが表示されます（図 8-18 を参照）。

図 8-18　[802.11a/n Cisco APs > Configure] ページ



ステップ 3　[Antenna Parameters] の [Antenna Gain] フィールドに、0.5 dBm 単位でアンテナ ゲインを入力します。たとえば、2.5 dBm = 5 です。

（注）　外部アンテナのみでゲイン設定を設定できます。アンテナのベンダーが指定した値に一致している値を入力する必要があります。

ステップ 4　[Apply] をクリックして、変更を適用します。

ステップ 5　[Save Configuration] をクリックして、変更を保存します。

CLI を使用したアンテナ ゲインの設定

コントローラの CLI を使用してアンテナ ゲインを設定する手順は、次のとおりです。

ステップ 1　802.11a バックホール無線のアンテナ ゲインを設定するには、次のコマンドを入力します。

config 802.11a antenna extAntGain *antenna_gain Cisco_AP*

ここで、*antenna_gain* は 0.5 dBm 単位の値です（たとえば、2.5 dBm = 5）。

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 ポイントのワークグループ ブリッジ グループ

イーサネット インターフェイスで有線クライアントの MAC アドレスを学習し、それらを Internet Access Point Protocol（IAPP）メッセージングを使用してメッシュ アクセス ポイントに報告することで、ワークグループ ブリッジ（WGB）は単一の無線セグメントを介して有線ネットワークを接続します。メッシュ アクセス ポイントは、WGB を無線クライアントとして処理します。

WGB として設定する場合、1130、1240、および 1310 Autonomous アクセス ポイントに加えて、3200 シリーズ モバイル アクセス ルータ（MAR）は、メッシュ アクセス ポイントとアソシエートすることができます。メッシュ アクセス ポイントは RAP または MAP として設定できます。WGB アソシエーションは、1522 では 2.4 GHz（802.11b）および 5 GHz（802.11a）無線、1524PS では 2.4 GHz（802.11b）および 4.9 GHz（公共安全無線）の両方でサポートされています。

（注）　設定の詳細については、「Cisco ワークグループ ブリッジ」（P.7-57）を参照してください。

サポートされているワークグループ モードおよびキャパシティ

- 1130、1240、1310 Autonomous アクセス ポイントでは、Cisco IOS リリース 12.4（3g）JA 以降（32 MB アクセス ポイント）または Cisco IOS リリース 12.3（8）JEB 以降（16 MB アクセス ポイント）が稼動している必要があります。12.4（3g）JA および 12.3（8）JEB より前の Cisco IOS リリースは、サポートされていません。

  （注）　メッシュ アクセス ポイントに 2 つの無線がある場合、いずれかの無線でだけワークグループ ブリッジ モードを設定できます。もう一方の無線を無効にしておくことをお勧めします。1524 などの 3 つの無線を備えたアクセス ポイントでは、ワークグループ ブリッジ モードはサポートされていません。

- 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。
- メッシュ アクセス ポイントでは、無線クライアント、WGB、アソシエートされた WGB 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。
- Cisco IOS リリース 12.4(3g)JA で動作する WGB は、WLAN が WPA1（TKIP）+ WPA2（AES）で設定されていて、対応する WGB インターフェイスがいずれかの暗号化だけ（WPA1 または WPA2）で設定されている場合、メッシュ アクセス ポイントとアソシエートすることができません。

クライアント ローミング

Cisco Compatible Extension（CX）バージョン 4（v4）クライアントの高速ローミングは、1522 および 1524 メッシュ アクセス ポイントの屋外メッシュ展開では最高 70 mph の速度でサポートされています。使用例としては、メッシュ パブリック ネットワーク内を移動する際に緊急車両の端末で通信を維持する場合が考えられます。

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 ポイント経由ローミング**：この機能により、クライアントはスキャン時間を節約できます。Cisco CX v4 クライアントがアクセス ポイントにアソシエートする際、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。各クライアントがアソシエートされていた以前のアクセス ポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセス ポイントをすべて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 をサポートしているネイバー アクセス ポイントの BSSID、およびアソシエーション解除以来の経過時間が含まれています。
- **拡張ネイバー リスト**：この機能は、特に音声アプリケーションを提供する際に、Cisco CX v4 クライアントのローミング性能とネットワーク エッジのパフォーマンスの向上に重点をおいています。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、アソシエートされ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**：この機能により、Cisco CX v4 クライアントは新しいアクセス 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監視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。

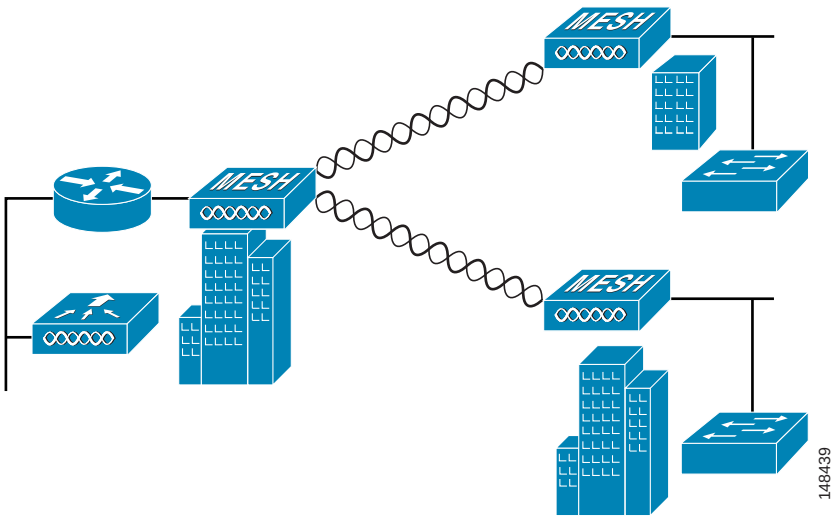
イーサネット ブリッジングおよびイーサネット VLAN タギングの設定

イーサネット ブリッジングは、2 つのメッシュ ネットワークのシナリオで使用されます。

- MAP 間の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（タグなしパケット）。一般的なトランク アプリケーションではキャンパス内の建物間のトラフィックをブリッジングすることがあります（図 8-19）。

（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 ブリッジング展開でイーサネット 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。

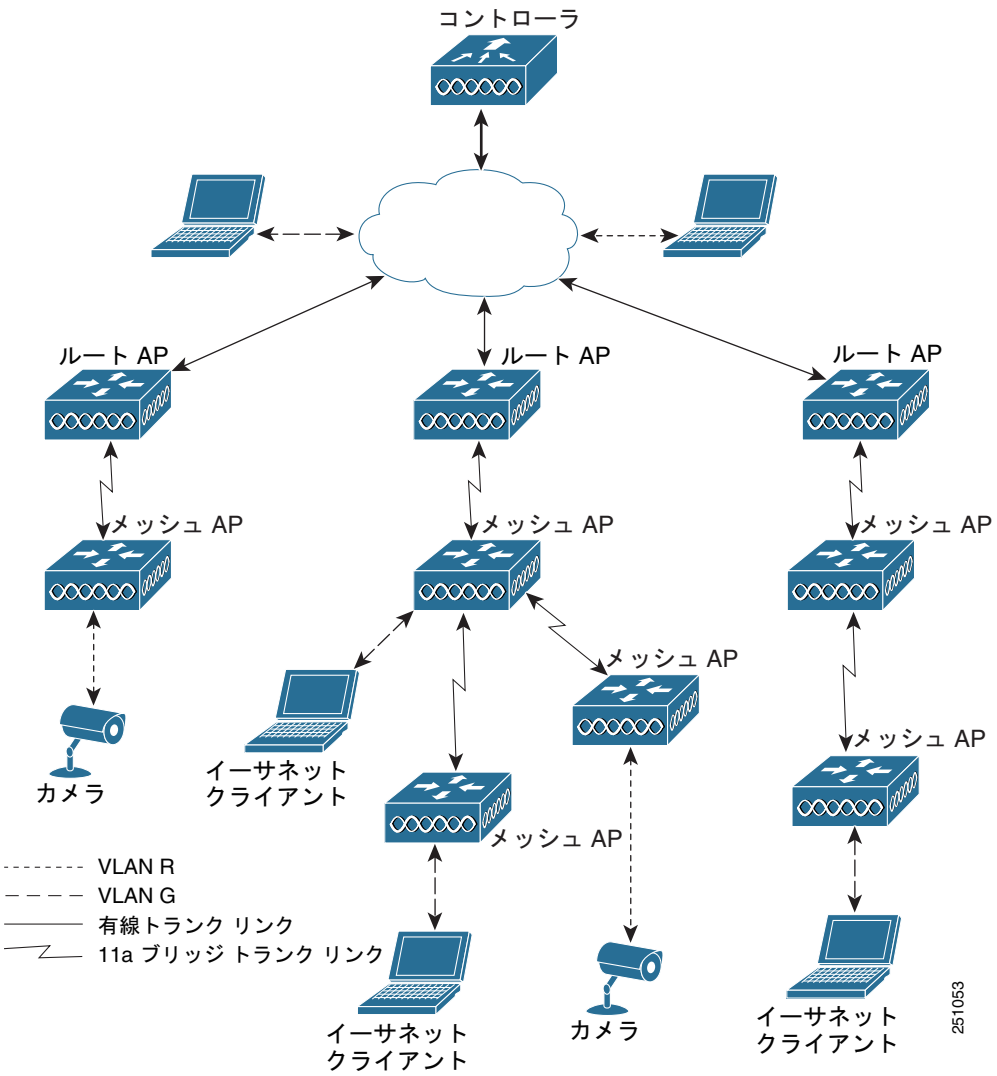
図 8-19　ポイントツーマルチポイント ブリッジング



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

  イーサネット VLAN タギングを使用した一般的な公共安全アクセス アプリケーションには、市内のさまざまな屋外の場所へのビデオ監視カメラの配置があります。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。さらに、これらのカメラのビデオはすべて無線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 8-20 を参照）。

図 8-20　　イーサネット VLAN タギング



イーサネット VLAN タギングのガイドライン

- 安全上の理由で、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は無効です。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と、有効になります。
- イーサネット VLAN タギングが動作するためには、メッシュ ネットワークのすべてのアクセス ポイントでイーサネット ブリッジングを有効にする必要があります。

- VLAN モードは、非 VLAN 透過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」（P.8-23）を参照してください。
  - VLAN 透過は、デフォルトで有効になっています。非 VLAN 透過として設定するには、グローバル メッシュ パラメータのウィンドウで VLAN 透過のオプションをオフにする必要があります。
- メッシュ アクセス ポイントの VLAN 設定が適用されるのは、すべてのアップリンク メッシュ アクセス ポイントがその VLAN をサポートできる場合だけです。
  - アップリンク アクセス ポインがその VLAN をサポートできない場合は、その設定は適用されるのではなく、格納されます。
- VLAN タギングはイーサネット インタフェースでだけ設定できます。
  - 152x メッシュ アクセス ポイントでは、4 つのうち 3 つのポート（*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*）*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* は、セカンダリ イーサネット インタフェー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 無線）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 インターフェイスの設定は必要ありません。
- 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 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 タギングのサポートを設定する必要はありません。
  - 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いときは、変更した設定は適用されます。
- 152x アクセス ポイントの 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。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。
- 2 つの MAP 間でブリッジングする場合、ブリッジングする 2 つのアクセス ポイント間の距離（メッシュ範囲）を入力します。MAP に接続されているトラフィックを RAP に転送しているアプリケーションは該当しません（アクセス モード）。
- 各セクタでは、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。
- アクセス ポイントのイーサネット ポートは、イーサネット タギング展開内の*アクセス*または*トランク* ポートのいずれかとして機能します。
- アクセス モード：このモードではタグなしパケットだけが許可されます。すべてのパケットに、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。このモードが有効になるには、グローバル VLAN モードが非 VLAN 透過である必要があります。
  - このオプションは、カメラや PC などの MAP に接続されているデバイスから情報を収集し、RAP に転送するアプリケーションで使用されます。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常に許可されて、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。このモードが有効になるには、グローバル VLAN モードが非 VLAN 透過である必要があります。
  - このオプションは、ブリッジング アプリケーションに使用されます。たとえば、キャンパス内の別々の建物にある 2 つの MAP 間でトラフィックを転送する場合です。
- 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。
- 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。
- 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。

GUI を使用したイーサネット ブリッジングおよび VLAN タギングの有効化

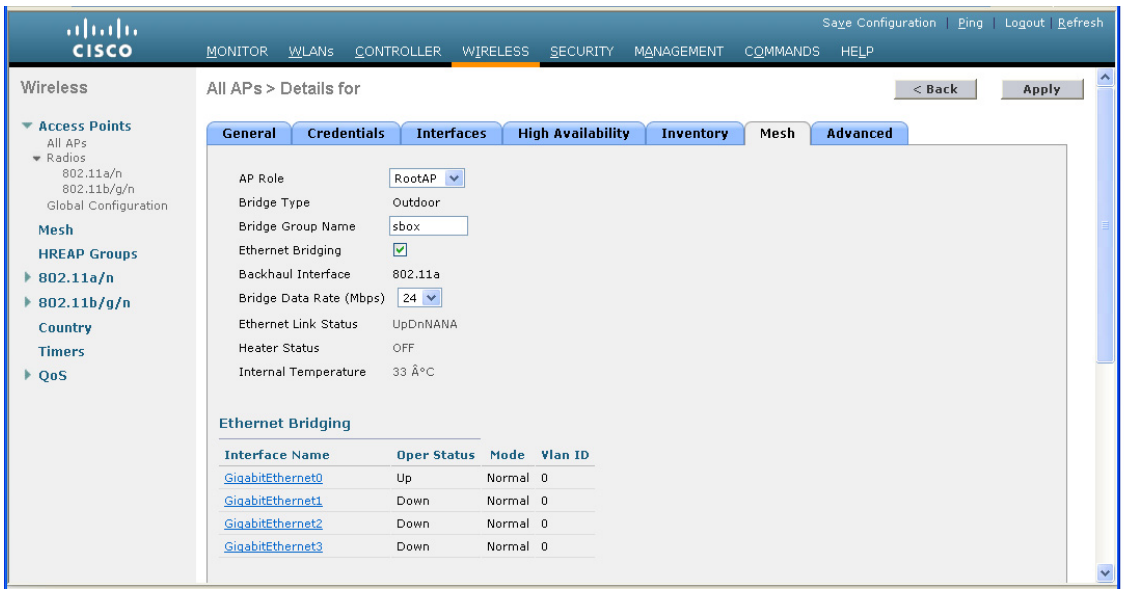
コントローラの GUI を使用して RAP または MAP のイーサネット ブリッジングを有効にする手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順にクリックして、[All APs] ページを開きます。

ステップ 2　イーサネット ブリッジングを有効にするアクセス ポイントの名前をクリックします。

ステップ 3　[Mesh] タブをクリックして、[All APs > Details for]（[Mesh)]）ページを開きます（図 8-21 を参照）。

図 8-21　[All APs > Details for]（[Mesh]）ページ



ステップ 4　[AP Role] ドロップダウン ボックスから、次のオプションのいずれかを選択します。

- [MeshAP] : 1520 シリーズ アクセス ポイントにコントローラに対する無線接続がある場合にこのオプションを選択します。これはデフォルト設定です。

- [RootAP] : 1520 シリーズ アクセス ポイントにコントローラに対する有線接続がある場合にこのオプションを選択します。

（注）　少なくとも 1 台のメッシュ アクセス ポイントをメッシュ ネットワークで RootAP に設定する必要があります。

ステップ 5　このアクセス ポイントをブリッジ グループに割り当てるには、[Bridge Group Name] フィールドのグループ名を入力します。

ステップ 6　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オンにします。この機能を無効にする場合は、オフにします。

ステップ 7　[Bridge Data Rate] ドロップダウン メニューから、802.11a バックホール インターフェイスの適切なバックホール レートを選択します。バックホール レートは **auto** に設定することをお勧めします。

ブリッジ データ レートを **auto** に設定すると、メッシュ バックホールでは、（すべてのレートに影響を与える条件が原因ではなく）特定のレートに対する不適切な条件のためにそのレートを使用できない場合、次善のレートが選択されます。

ステップ 8　[Apply] をクリックして、変更を適用します。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 9　イーサネット ポートを設定するには、次のいずれかの操作を行います。

- MAP アクセス ポートを設定する場合、次の手順に従います。
  - **a.** [gigabitEthernet1]（ポート 1-PoE 出力）をクリックします。
  - **b.** [Mode] ドロップダウン メニューで [access] を選択します。
  - **c.** 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。
  - **d.** 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。

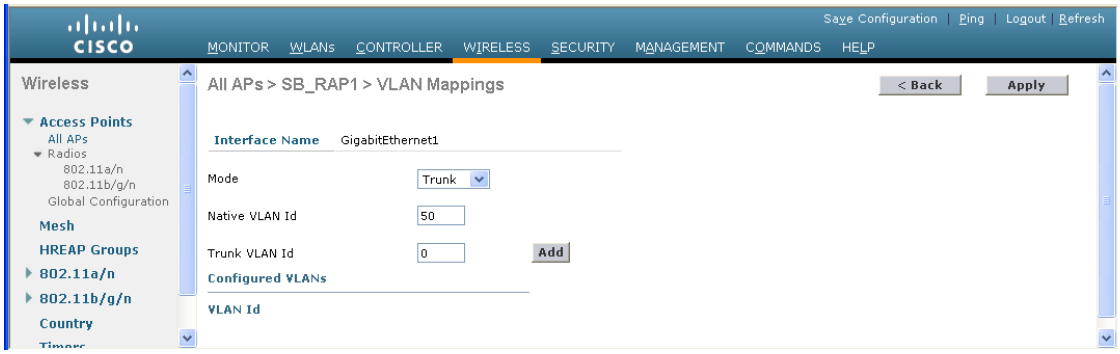
（注）　VLAN ID 1 はデフォルト VLAN として予約されていません。

（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 トランク ポートを設定する場合は、次の手順に従います。
  - **a.** [gigabitEthernet0]（ポート 0-PoE 入力）をクリックします。
  - **b.** [Mode] ドロップダウン メニューで [trunk] を選択します。
  - **c.** *着信*トラフィックのネイティブ VLAN ID を入力します。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。
  - **d.** *発信*パケットのトランク VLAN ID を入力します。
  - **e.** *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）。
  - **f.** *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）。
  - **g.** [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 はウィンドウの [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、目的の VLAN の右にある矢印ドロップダウンから [Remove] オプションを選択します。

図 8-22　[All APs > AP > VLAN Mappings] ページ



ステップ 10　[Apply] をクリックして、変更を適用します。

ステップ 11　[Save Configuration] をクリックして、変更を保存します。

表 8-6 に、メッシュ ページに表示される設定できないパラメータの説明を示します。

表 8-6　アクセス ポイントの表示パラメータ

パラメータ	説明
Bridge Type	屋外（152x アクセス ポイント）または屋内（1130 または 1240 アクセス ポイント）かを表示します。
Backhaul Interface	この MAP で他の MAP へのデータ転送に使用する無線帯域を表示します。表示される値は 802.11a だけです。
Ethernet Link Status	AP152x のイーサネット リンクのアップまたはダウンのステータスを表示します。4 つのイーサネット ポートのアップ（Up）またはダウン（Dn）のステータスが、port0:port1:port2:port3 の形式で報告されます。たとえば、[UpDnDnDn] はポート 0 が Up、ポート 1、2、および 3 がダウン（Dn）であることを示しています。 （注）　ステータスの文字列に *NA* と表示される場合、ポートへの有線接続はありません。
Heater Status	[ON] または [OFF] のいずれかのステータスを表示します。
Internal Temperature	1522 および 1524PS/1524SB の内部温度を表示します。

CLI を使用したイーサネット ブリッジング パラメータの設定

コントローラの CLI を使用して RAP または MAP のイーサネット ブリッジングを設定する手順は、次のとおりです。

ステップ 1　AP152x にブリッジ機能を指定するには、次のコマンドを入力します。

config ap mode bridge *Cisco_AP*

ステップ 2　メッシュ ネットワーク内でのこのアクセス ポイントのロールを指定するには、次のコマンドを入力します。

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

アクセス ポイントにコントローラへの無線接続がある場合は **meshAP** パラメータ、アクセス ポイントにコントローラへの有線接続がある場合は **rootAP** パラメータを使用します。

（注）　デフォルトのアクセス ポイント ロールは **meshAP** です。

ステップ 3　アクセス ポイントをブリッジ グループに割り当てるには、次のコマンドを入力します。

config ap bridgegroupname set *groupname Cisco_AP*

ステップ 4　アクセス ポイントでイーサネット ブリッジングを有効にするには、次のコマンドを入力します。

config mesh ethernet-bridging vlan transparent *disable*

ステップ 5　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共有レート（Mb/s）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*

ブリッジ データ レートを **auto** に設定すると、メッシュ バックホールでは、（すべてのレートに影響を与える条件が原因ではなく）特定のレートに対する不適切な条件のためにそのレートを使用できない場合、次善のレートが選択されます。

ステップ 6　設定を保存するには、次のコマンドを入力します。

save config

CLI を使用したイーサネット VLAN タギングの設定

VLAN ID 1 はデフォルト VLAN として予約されていません。

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。

VLAN ID には 1 ～ 4095 の任意の値を入力できます。別の VLAN に割り当てられた値を割り当てないでください。

- 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 *AP1520-MAP 50*

  ここで、*AP1520-MAP* は変数 *Cisco_AP* で、*50* は変数 *access_vlan ID*

- 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 *AP1520-MAP 60*

  ここで、*AP1520-MAP* は変数 *Cisco_AP*、*60* は変数 *native_vlan ID*

  - 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 *AP1522-MAP3 65*

ここで、*AP1522-MAP 3* は変数 *Cisco_AP*、*65* は変数 *vlan ID*

拡張機能の設定

メッシュ ネットワークでの音声パラメータの設定

コントローラで Call Admission Control（CAC; コール アドミッション制御）および QoS を設定し、メッシュ ネットワークの音声の品質を管理できます。

（注）　音声は屋内メッシュ ネットワークでだけサポートされています（1130 および 1240 アクセス ポイント）。

CAC

CAC を使用すると、無線 LAN で輻輳が発生した際に、アクセス ポイントで制御された QoS（Quality of Service）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、異なるネットワーク負荷で QoS を維持するには、CCX v4 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。CCX の詳細については、「Cisco Client Extensions の設定」（P.6-46）を参照してください。

メッシュ アクセス ポイントのすべてのコールでは、帯域幅に基づく CAC を使用します。負荷に基づく CAC はサポートされていません。

帯域幅に基づく、静的な CAC を使用すると、クライアントで新しいコールを受信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセス ポイントでは、使用可能な帯域幅を調べてコールに必要な帯域幅と比較し、特定のコールに対応できるかどうかを判断します。許容される品質のコールを最大数維持するために使用できる帯域幅が不十分な場合、アクセス ポイントによってコールが拒否されます。

QoS および DSCP マーキング

QoS 802.11e はメッシュ アクセス ポイントのアクセスおよびバックホール無線でサポートされています。MAP はコントローラで定義された QoS 設定に基づいてクライアント トラフィックを優先できます。CAC はバックホールで実装されます。

メッシュ アクセス ポイントはデバイスからの DSCP マーキングを認識します。DSCP は起点の Cisco 7920 音声受話器（クライアント）および終点の音声受話器または端末で実行されます。DSCP マーキングはコントローラ、MAP、または CAC で実行されません。

（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。

コントローラの GUI または CLI を使用してメッシュ ネットワークで帯域幅に基づく CAC および QoS を設定できます。これらの機能を設定する手順は、QoS 設定を除くと、メッシュおよび非メッシュ ネットワークで同じです。

- 音声および音声パラメータを設定するには、「音声パラメータとビデオ パラメータの設定」（P.4-74）の手順に従います。
  - QoS などの音声に関するメッシュ固有の設定のガイドラインについては、「メッシュ ネットワークにおける音声使用のガイドライン」（P.8-40）を参照してください。

CLI を使用して音声およびビデオの詳細を表示する手順は、メッシュおよび非メッシュ ネットワークで異なります。

- メッシュ アクセス ポイントの詳細を表示するには、「CLI を使用したメッシュ ネットワークの音声の詳細の表示」（P.8-41）の手順に従います。

メッシュ ネットワークにおける音声使用のガイドライン

- 音声は屋内メッシュ アクセス ポイント（1130、および 1240）でだけサポートされています。
- 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、各セクタを設定する必要があります。
- [802.11a（または 802.11b/g/n）Global Parameters] ウィンドウで次を行います。
  - DTPC（Dynamic Target Power Control）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（または 802.11b/g/n）> Voice Parameters] ウィンドウで次を行います。
  - 負荷に基づく CAC を無効にする
  - WMM が有効化されている 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（または 802.11b/g/n）> EDCA Parameters] ウィンドウで次を行います。
  - 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] ウィンドウで次を行います。
  - 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）ウィンドウで次を行います。
  - 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）ウィンドウで次を行います。
  - 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。「クライアント ローミング」（P.8-31）を参照してください。
- [x > y] ウィンドウで次を行います。
  - VAD（Voice Active Detection）を無効にする

メッシュ ネットワークでの音声コールのサポート

表 8-7 に、計画に活用できるよう、無線のタイプおよびメッシュ アクセス ポイントのロール（RAP または MAP）別にサポートされている予想最少および最大音声コール数の一覧を示します。

表 8-7　メッシュ ネットワークで予想される音声コールのサポート

メッシュ アクセス ポイントのロール	無線	サポートされている最少コール数[1]	サポートされている最大コール数[2]
RAP	802.11a	14	18
	802.11b/g/n	14	18
MAP1	802.11a	6	9
	802.11b/g/n	11	18
MAP2	802.11a	4	7
	802.11b/g/n	5	9

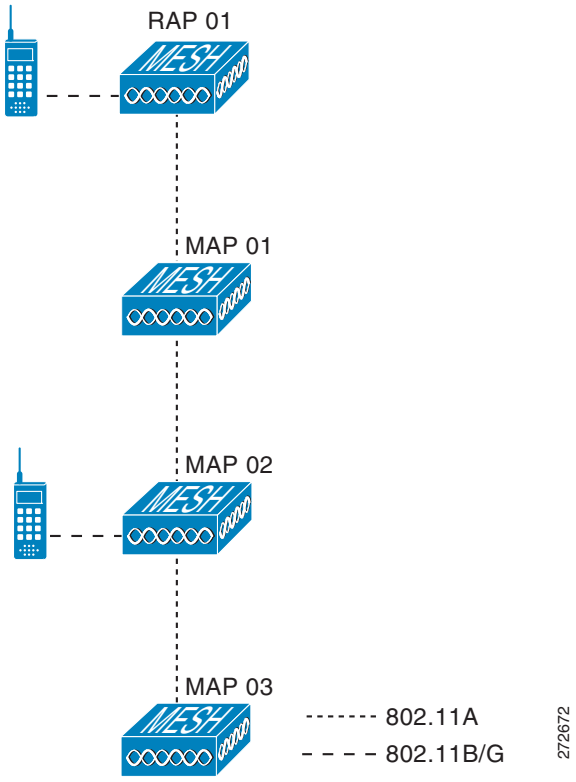
1. 855 伝送単位（TU）の帯域幅（50% の帯域幅は音声コール用に予約）。
2. 1076 TU の帯域幅（50% の帯域幅は音声コール用に予約）。

CLI を使用したメッシュ ネットワークの音声の詳細の表示

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コールの詳細を表示します。

CLI コマンドを使用して出力を表示する場合は、図 8-23 を参照してください。

図 8-23　メッシュ ネットワークの例



- 各ルート アクセス ポイントの音声コールの総数および音声コールで使用する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

  次のような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 トポロジおよび各アクセス ポイントおよび無線の音声コールとビデオ リンクの帯域幅利用率（使用量/使用可能な最大量）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**} *Cisco_AP*

  次のような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 フィールドの左にある縦棒（|）は、メッシュ アクセス ポイントがルート アクセス ポイント（RAP）から何ホップ離れているかを示しています。

（注） 無線のタイプが同じ場合、各ホップで使用するバックホールの帯域幅は同じです（Bw Used/Max）。たとえば、メッシュ アクセス ポイント *map1*、*map2*、*map3*、および *rap1* はすべて同じ無線バックホール（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、アクセス ポイント無線で動作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 *Cisco_AP*

  次のような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）　アクセス ポイント無線でコールが受信されるたびに、適切な Calls サマリー カラムが 1 つずつ増加します。たとえば、*map2* の 802.11b/g 無線でコールが受信されると、その無線の Calls カラムにある既存の値に 1 が加えられます。上記の例の場合、*map2* の 802.11b/g 無線でアクティブなコールは、新しいコールだけです。新しいコールが受信されるときに 1 つのコールがアクティブである場合、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 *Cisco_AP*

  次のような情報が表示されます。

```
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 ポイント無線の *Calls* カラムは 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 つのコールが *map2* 802.11b/g および 802.11a 無線の *Calls* カラム、1 つのコールが *map1* 802.11a バックホール無線の *Calls* カラム、1 つのコールが *rap1* 802.11a バックホール無線の *Calls* カラムに加わります。

- ネットワークのメッシュ ツリー トポロジ、不十分な帯域幅が原因でアクセス ポイント無線で拒否された音声コール、および拒否が発生した該当するアクセス ポイント無線を表示するには、次のコマンドを入力します。

  show mesh cac rejected *Cisco_AP*

  次のような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 無線で拒否された場合、*Calls* カラムは 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ブロンズ、シルバー、ゴールド、プラチナ、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 {*Cisco_AP* | **all**}

  次のような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：キューのオーバーフローのためにドロップしたパケットの総数。

  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。

ビデオのメッシュ マルチキャストの抑制の有効化

コントローラの CLI を使用して、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する 3 つのメッシュ マルチキャスト モードを設定できます。これらのモードを有効にすると、メッシュ ネットワーク内の不要なマルチキャスト転送が減り、バックホール帯域幅が節約されます。

メッシュ マルチキャスト モードによって、ブリッジングを有効にしたアクセス ポイント（メッシュ アクセス ポイント（MAP）およびルート アクセス ポイント（RAP））がメッシュ ネットワーク内のイーサネット LAN にマルチキャストを送信する方法が決定されます。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。

3 つのツリー メッシュ マルチキャスト モードは次のとおりです。

- **regular** モード：データは、ブリッジングが有効な 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** 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。それ以上の転送は実行されず、RAP が受信する非 CAPWAP マルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワークには送り戻されません。また、フィルタが適用されるため、MAP-to-MAP マルチキャストは発生しません。in モードはデフォルトのモードです。
- **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。
  - マルチキャスト パケットがイーサネットを介して MAP で受信されると、RAP に送信されます。ただし、これらのパケットは他の MAP イーサネットには送信されません。また、MAP-to-MAP パケットはマルチキャストからフィルタ処理されます。
  - マルチキャスト パケットがイーサネットを介して RAP で受信されると、すべての MAP およびそれらのイーサネット ネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

（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）。

CLI を使用したメッシュ ネットワークでのマルチキャストの有効化

- 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** | **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** | **in-out**}

（注）　コントローラの GUI を使用してメッシュ ネットワークのマルチキャストは有効にできません。

屋内および屋外メッシュ アクセス ポイントのバックホール クライアントアクセス（ユニバーサル アクセス）

メッシュ アクセス ポイント（1524SB、1522、1240、および 1130）のバックホールでクライアント トラフィックを許可するよう設定できます。この機能を有効にすると、メッシュ アクセス ポイントで 802.11a 無線での無線クライアント アソシエーションが可能になります。このユニバーサル アクセスを使用すると、アクセス ポイントは、同じ 802.11a 無線でバックホール トラフィックと 802.11a クライアント トラフィックの両方を伝送できます。この機能を無効にすると、802.11a 無線でバックホール トラフィックだけが伝送され、クライアント アソシエーションは 802.11b/g 無線だけで行われます。

この機能を有効にした後、すべてのメッシュ アクセス ポイントがリブートされます。

デフォルト：無効

（注）　このパラメータは、1524PS を*除く*、2 つ以上の無線を備えたメッシュ アクセス ポイントに適用されます（1524SB、1522、1240、および 1130）。

コントローラ上でこの機能を有効にするには、[Wireless] > [Mesh] ウィンドウの [Backhaul Client Access] チェックボックスをオンにします。「グローバル メッシュ パラメータの設定」（P.8-23）を参照してください。

メッシュの統計情報およびレポートの表示

アクセス ポイントのメッシュに関する統計情報の表示

この項では、コントローラの GUI または CLI を使用して特定のアクセス ポイントのメッシュに関する統計情報を表示する方法について説明します。

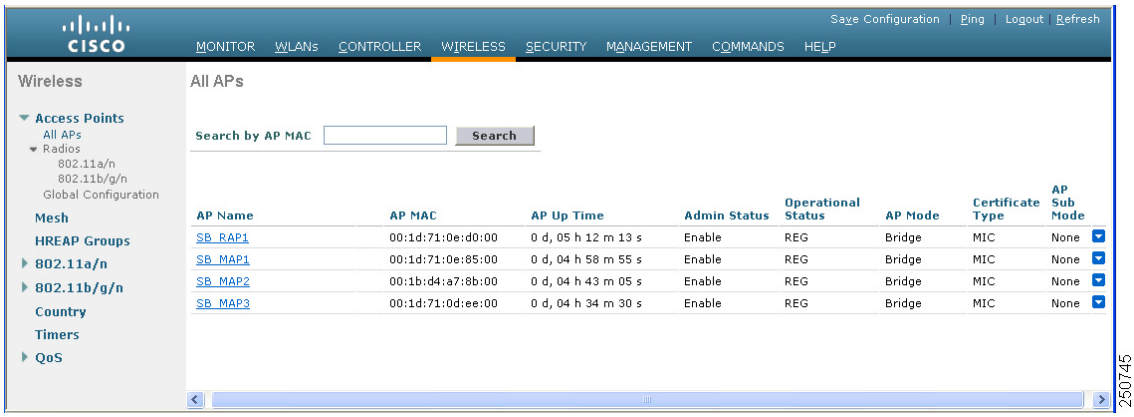
（注）　コントローラの GUI の [All APs > Details] ページでは、統計情報タイマー間隔の設定を変更できます。

GUI を使用したアクセス ポイントのメッシュに関する統計情報の表示

コントローラの GUI を使用して特定のアクセス ポイントのメッシュに関する統計情報を表示する手順は、次のとおりです。

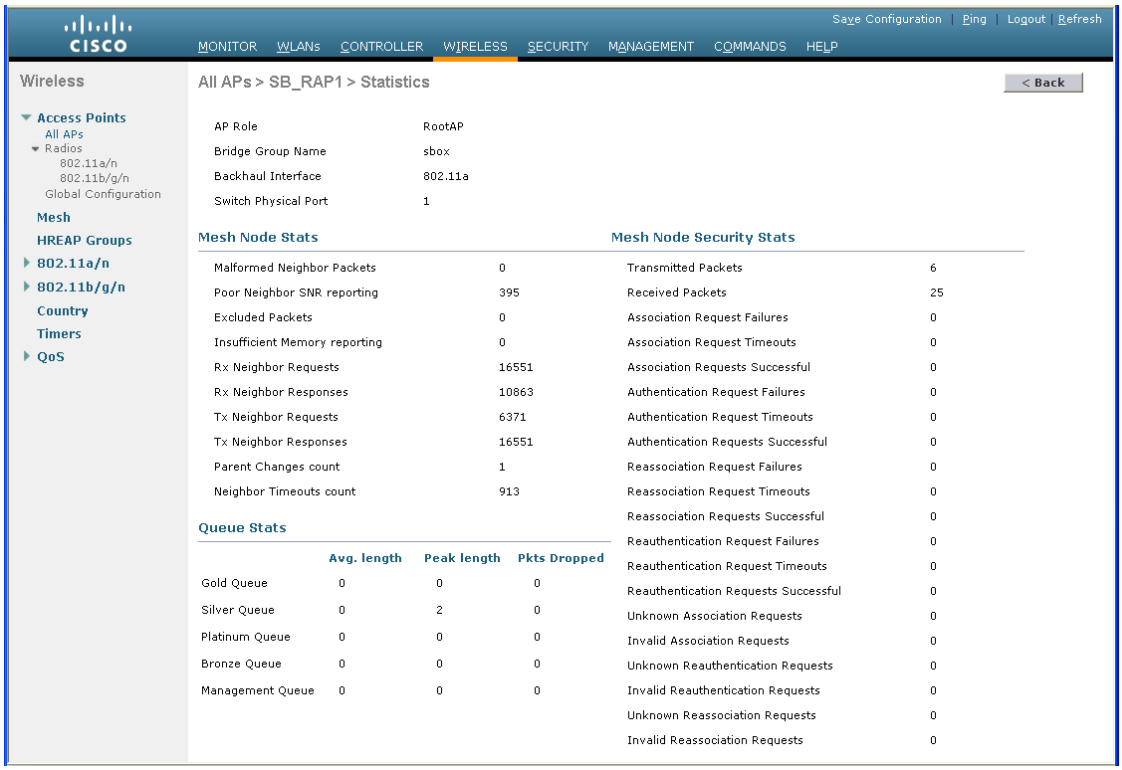
ステップ 1　[Wireless] > [Access Points] > [All APs] の順にクリックして、[All APs] ページを開きます（図 8-24 を参照）。

図 8-24　[All APs] ページ



ステップ 2　特定のアクセス ポイントの統計情報を表示するには、カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて、[Statistics] を選択します。アクセス ポイントの [All APs > *アクセス ポイント名* > Statistics] ページが表示されます（図 8-25 を参照）。

図 8-25　[All APs > アクセス ポイント名 > Statistics] ページ



このページには、メッシュ ネットワーク内のアクセス ポイントのロール、アクセス ポイントが属しているブリッジ グループの名前、アクセス ポイントが動作しているバックホール インターフェイス、物理スイッチ ポートの数が表示されます。また、このアクセス ポイントに関してメッシュのさまざまな統計情報も表示されます。表 8-8 に、各統計情報についての説明を示します。

表 8-8　メッシュ アクセス ポイントの統計情報

統計情報	パラメータ	説明
Mesh Node Stats	Malformed Neighbor Packets	ネイバーから受信した不正な形式のパケットの数。不正な形式のパケットの例には、不正な形式のショート DNS パケットや不正な形式の DNS 応答といったトラフィックの悪意のあるフラッドがあります。
	Poor Neighbor SNR Reporting	信号対雑音比がバックホール リンクで 12 dB 未満になった回数。
	Excluded Packets	除外したネイバー メッシュ アクセス ポイントから受信したパケットの数。
	Insufficient Memory Reporting	メモリ不足になった状態の数。
	Rx Neighbor Requests	ネイバー メッシュ アクセス ポイントから受信したブロードキャストおよびユニキャストの要求数。
	Rx Neighbor Responses	ネイバー メッシュ アクセス ポイントから受信した応答数。
	Tx Neighbor Requests	ネイバー メッシュ アクセス ポイントに送信したブロードキャストおよびユニキャストの要求数。
	Tx Neighbor Responses	ネイバー メッシュ アクセス ポイントに送信した応答数。
	Parent Changes Count	メッシュ アクセス ポイント（子）が別の親に移動した回数。
	Neighbor Timeouts Count	ネイバー タイムアウト回数。
Queue Stats	Gold Queue	定義された統計期間中にゴールド（ビデオ）キューで待機していたパケットの平均および最大数。
	Silver Queue	定義された統計期間中にシルバー（ベスト エフォート）キューで待機していたパケットの平均および最大数。
	Platinum Queue	定義された統計期間中にプラチナ（音声）キューで待機していたパケットの平均および最大数。
	Bronze Queue	定義された統計期間中にブロンズ（バックグラウンド）キューで待機していたパケットの平均および最大数。
	Management Queue	定義された統計期間中に管理キューで待機していたパケットの平均および最大数。

表 8-8　メッシュ アクセス ポイントの統計情報 （続き）

統計情報	パラメータ	説明
Mesh Node Security Stats	Transmitted Packets	選択したメッシュ アクセス ポイントによってセキュリティ ネゴシエーション中に伝送されたパケット数。
	Received Packets	選択したメッシュ アクセス ポイントによってセキュリティ ネゴシエーション中に受信されたパケット数。
	Association Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求の失敗数。
	Association Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求のタイムアウト回数。
	Association Requests Successful	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求の成功数。
	Authentication Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生した認証要求の失敗数。
	Authentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生した認証要求のタイムアウト回数。
	Authentication Requests Successful	選択したメッシュ アクセス ポイントとその親の間の認証要求の成功数。
	Reassociation Request Failures	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求の失敗数。
	Reassociation Request Timeouts	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求のタイムアウト回数。
	Reassociation Requests Successful	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求の成功数。
	Reauthentication Request Failures	選択したメッシュ アクセス ポイントとその親の間の再認証要求の失敗数。
	Reauthentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生した再認証要求のタイムアウト回数。
	Reauthentication Requests Successful	選択したメッシュ アクセス ポイントとその親の間で発生した再認証要求の成功数。
	Unknown Association Requests	親メッシュ アクセス ポイントが子から受信した不明なアソシエーション要求の数。不明なアソシエーション要求は、子が不明なネイバー メッシュ アクセス ポイントの場合によくみられます。
	Invalid Association Requests	親メッシュ アクセス ポイントが選択した子メッシュ アクセス ポイントから受信した無効なアソシエーション要求の数。この状況は、選択した子が有効なネイバーであるが、アソシエーションが許可される状態ではないときに発生することがあります。

表 8-8　メッシュ アクセス ポイントの統計情報 （続き）

統計情報	パラメータ	説明
Mesh Node Security Stats （続き）	Unknown Reauthentication Requests	親メッシュ アクセス ポイントが子から受信した不明な再認証要求の数。この状況は、子メッシュ アクセス ポイントが不明なネイバーであるときに発生することがあります。
	Invalid Reauthentication Requests	親メッシュ アクセス ポイントが子から受信した無効な再認証要求の数。この状況は、子が有効なネイバーであるが、再認証に適した状態でないときに発生することがあります。
	Unknown Reassociation Requests	親メッシュ アクセス ポイントが子から受信した不明な再アソシエーション要求の数。この状況は、子メッシュ アクセス ポイントが不明なネイバーであるときに発生することがあります。
	Invalid Reassociation Requests	親メッシュ アクセス ポイントが子から受信した無効な再アソシエーション要求の数。この状況は、子が有効なネイバーであるが、再アソシエーションに適した状態でないときに発生することがあります。

CLI を使用したアクセス ポイントのメッシュに関する統計情報の表示

コントローラの CLI を使用して特定のアクセス ポイントのメッシュに関する統計情報を表示するには、次のコマンドを使用します。

- 特定のアクセス ポイントのパケット エラーの統計、失敗数、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と再認証の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* | **all**}

  次のような情報が表示されます。

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
```

```
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- キュー内のパケット数をキューのタイプ別に表示するには、次のコマンドを入力します。

  show mesh queue-stats *Cisco_AP*

  次のような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：キューのオーバーフローのためにドロップしたパケットの総数。

  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。

アクセス ポイントのネイバーに関する統計情報の表示

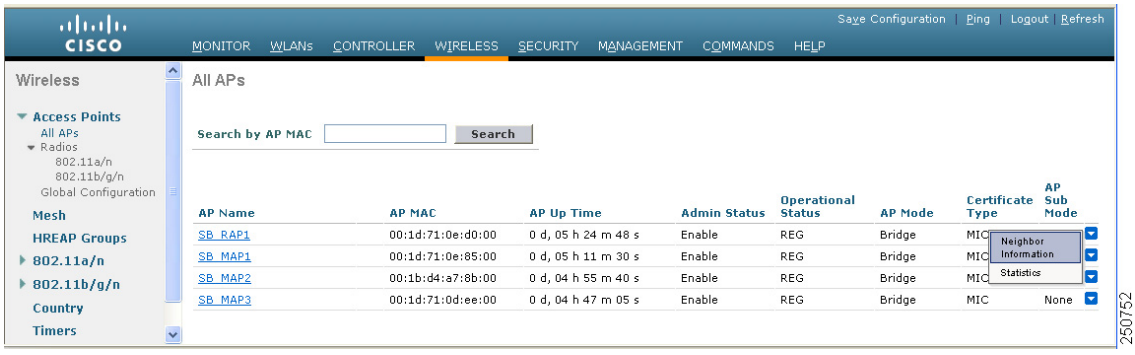
この項では、コントローラの GUI または CLI を使用して選択したアクセス ポイントのネイバーに関する統計情報を表示する方法について説明します。また、選択したアクセス ポイントとその親の間でリンク テストを実行する方法についても説明します。

GUI を使用したアクセス ポイントのネイバーに関する統計情報の表示

コントローラの GUI を使用して、アクセス ポイントのネイバーに関する統計情報を表示する手順は、次のとおりです。

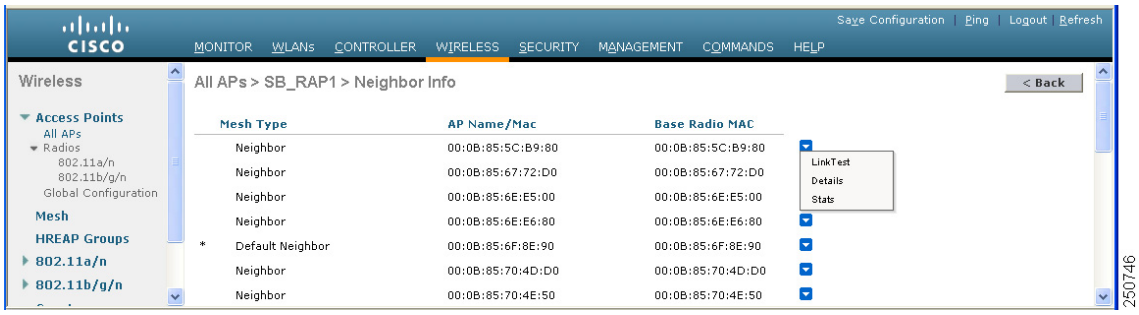
ステップ 1　[Wireless] > [Access Points] > [All APs] の順にクリックして、[All APs] ページを開きます（図 8-26 を参照）。

図 8-26　[All APs] ページ



ステップ 2　特定のアクセス ポイントのネイバーに関する統計情報を表示するには、カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて、[Neighbor Information] を選択します。アクセス ポイントの [All APs > *アクセス ポイント名* > Neighbor Info] のページが表示されます（図 8-27 を参照）。

図 8-27　[All APs > アクセス ポイント名 > Neighbor Info] ページ

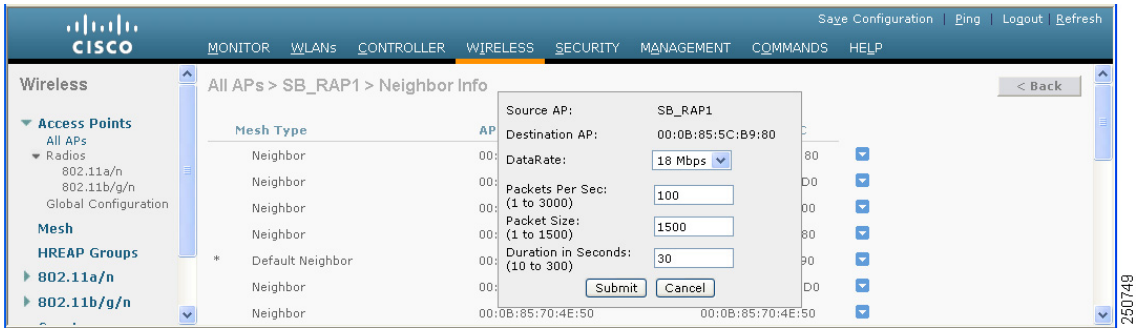


このページには、アクセス ポイントの親、子、およびネイバーの一覧が表示されます。各アクセス ポイントの名前と無線 MAC アドレスが示されます。

ステップ 3　アクセス ポイントとその親または子の間でリンク テストを実行する手順は、次のとおりです。

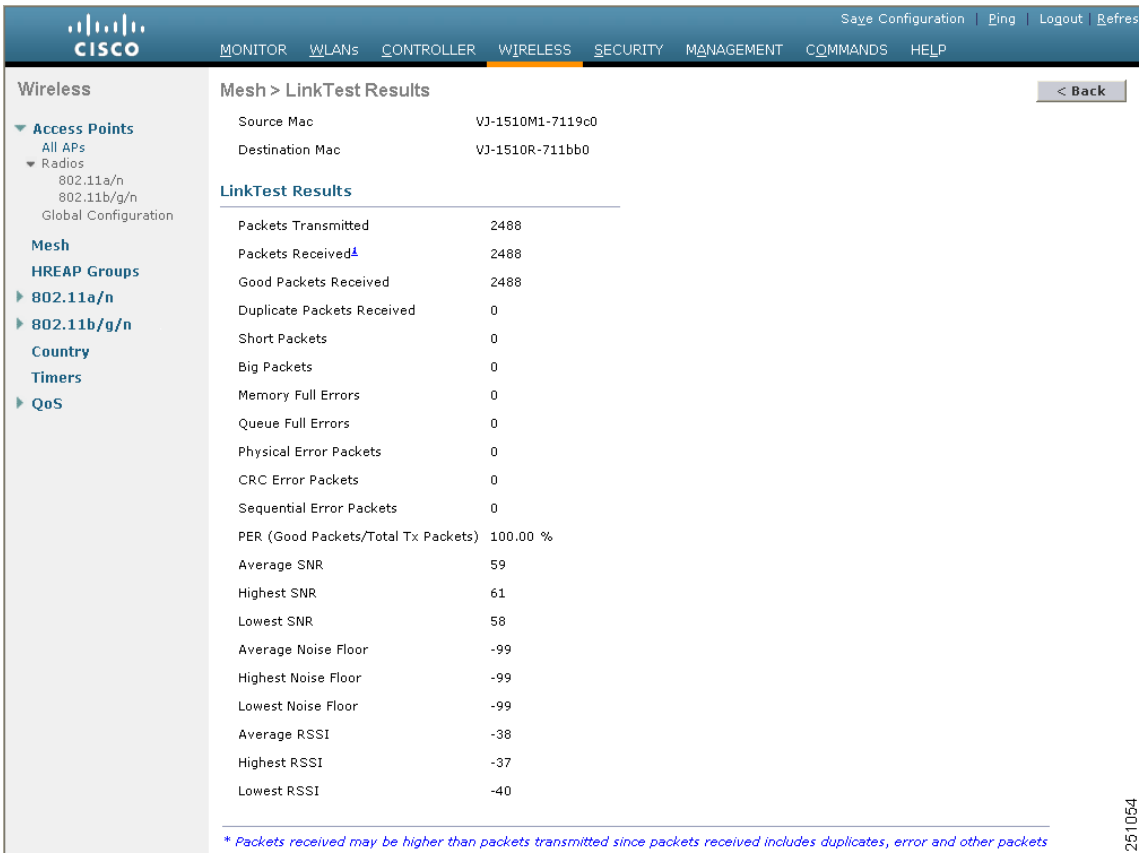
a.　カーソルを親または子の青いドロップダウン矢印の上に置いて [LinkTest] を選択します。ポップアップ ウィンドウが表示されます（図 8-28 を参照）。

図 8-28　リンク テスト ウィンドウ



b.　[Submit] をクリックしてリンク テストを開始します。リンク テストの結果が [Mesh > LinkTest Results] ページに表示されます（図 8-29 を参照）。

図 8-29　[Mesh > LinkTest Results] ページ

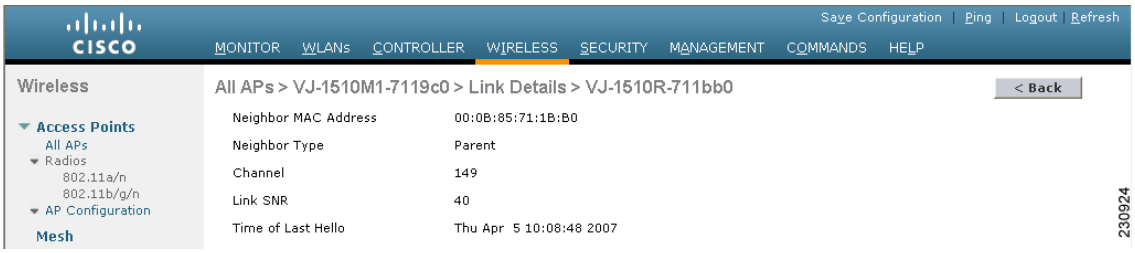


c. [Back] をクリックして、[All APs > *アクセス ポイント名* > Neighbor Info] ページに戻ります。

ステップ 4　このページの任意のアクセス ポイントに関する詳細を表示する手順は、次のとおりです。

a. カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて、[Details] を選択します。[All APs > *アクセス ポイント名* > Link Details > *ネイバー名*] ページが表示されます（図 8-30 を参照）。

図 8-30　[All APs > アクセス ポイント名 > Link Details > ネイバー名] ページ

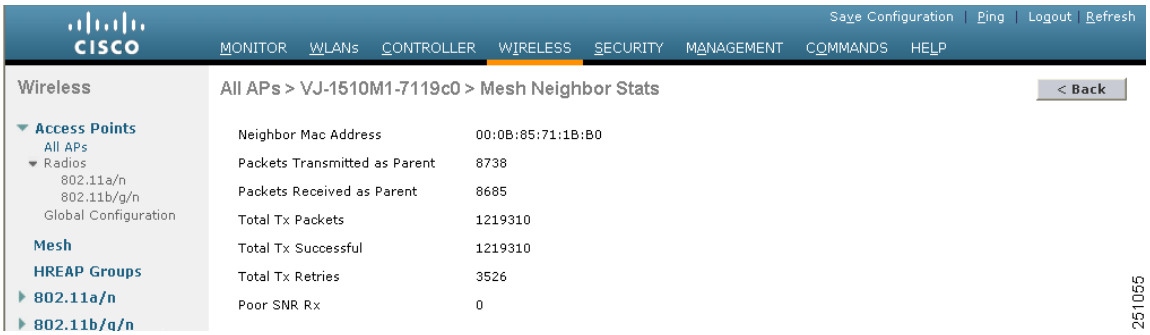


b. [Back] をクリックして、[All APs > *アクセス ポイント名* > Neighbor Info] ページに戻ります。

ステップ 5　このページの任意のアクセス ポイントに関する統計情報を表示する手順は、次のとおりです。

a. カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて、[Stats] を選択します。[All APs > *アクセス ポイント名* > Mesh Neighbor Stats] ページが表示されます。（図 8-31 を参照）。

図 8-31　[All APs > アクセス ポイント名 > Mesh Neighbor Stats] ページ



b. [Back] をクリックして、[All APs > *アクセス ポイント名* > Neighbor Info] ページに戻ります。

CLI を使用したアクセス ポイントのネイバーに関する統計情報の表示

特定のアクセス ポイントのネイバーに関する統計情報を表示するには、次のコマンドを使用します。

- 特定のアクセス ポイントのメッシュ ネイバーを表示するには、次のコマンドを入力します。

  show mesh neigh {detail | summary} {*Cisco_AP* **| all}**

  概要の表示を指定すると、次のような情報が表示されます。

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0  149      5      6        5       0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F  149      7      0       0        0x860     BEACON
```

- アクセス ポイントとそのネイバーとの間のリンクに関するチャネルおよび Signal-to-Noise Ratio（SNR; 信号対雑音比）の詳細を表示するには、次のコマンドを入力します。

  show mesh path *Cisco_AP*

  次のような情報が表示されます。

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags State
-----------------  ------- ------ -------- -------- ------ -------
mesh-45-rap1       165     15     18       16       0x86b UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- ネイバー メッシュ アクセス ポイントによって伝送されるパケットのパケット エラーの割合を表示するには、次のコマンドを入力します。

  show mesh per-stats {*Cisco_AP* | **all**}

  次のような情報が表示されます。

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028
Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

```
Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

（注）　パケット エラー レートの割合 = 1 –（伝送に成功したパケット数/伝送したパケットの総数）

屋内アクセス ポイントのメッシュ アクセス ポイントへの変換（1130AG、1240AG）

1130AG または 1240AG 屋内アクセス ポイントを屋内メッシュ展開に導入する前に、次の手順を実行する必要があります。

1. Autonomous アクセス ポイント（k9w7 イメージ）を Lightweight アクセス ポイントに変換します。

   このプロセスの詳細な説明については、次の URL を参照してください。

   http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

2. Lightweight アクセス ポイントをメッシュ アクセス ポイント（MAP）またはルート アクセス ポイント（RAP）のいずれかに変換します。

   屋内メッシュ アクセス ポイント（1130 および 1240）は RAP または MAP のいずれかとして機能できます。デフォルトではすべて MAP として設定されます。

   メッシュ ネットワーク内では少なくとも 1 台のアクセス ポイントを RAP として機能するように設定する必要があります。

   - CLI を使用してアクセス ポイントをメッシュ アクセス ポイントに変換するには、次のいずれかの手順を実行します。
     - Lightweight アクセス ポイントをメッシュ アクセス ポイントに変換するには、次の CLI コマンドを入力します。

       config ap mode bridge *Cisco_AP*

       メッシュ アクセス ポイントはリロードされます。
     - Lightweight アクセス ポイントを RAP に変換するには、次の CLI コマンドを入力します。

       config ap mode bridge *Cisco_AP*

       config ap role rootAP *Cisco_AP*

       メッシュ アクセス ポイントはリロードされ、RAP として動作するように設定されます。
   - GUI を使用してアクセス ポイントをメッシュ アクセス ポイントに変換するには、次の手順を実行します。
     a. [Wireless] を選択し、変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。
     b. [General Properties] パネルの [AP Mode] ドロップダウン メニューから [Bridge] を選択します。

        アクセス ポイントがリブートされます。
     c. [Mesh] パネルの [AP Role] ドロップダウン メニューから [RootAP] または [MeshAP] のいずれかを選択します。
     d. [Apply] および [Save Configuration] をクリックします。

屋内メッシュ アクセス ポイント（1130AG、1240AG）の MAP および RAP ロールの変更

Cisco 1130 および 1240 シリーズ屋内メッシュ アクセス ポイントは RAP または MAP のいずれかとして機能できます。

GUI を使用した屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更

コントローラの GUI を使用して、屋内メッシュ アクセス ポイントをあるロールから別のロールに変更する手順は、次のとおりです。

ステップ 1　[Wireless] > [Access Points] > [All APs] の順にクリックして、[All APs] ページを開きます。

ステップ 2　変更する 1130 または 1240 シリーズ アクセス ポイントの名前をクリックします。

ステップ 3　[Mesh] タブをクリックします。

ステップ 4　[AP Role] ドロップダウン ボックスから [MeshAP] または [RootAP] を選択し、アクセス ポイントをそれぞれ MAP または RAP として指定します。

ステップ 5　[Apply] をクリックして、変更を適用します。アクセス ポイントがリブートされます。

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

（注）　MAP から RAP に変更する場合、MAP とコントローラ間でファスト イーサネット接続を使用することをお勧めします。

（注）　RAP から MAP への変換の後、コントローラへの MAP の接続は、ファスト イーサネット接続ではなく、無線バックホールになります。MAP が無線で接続できるように MAP を起動する前に、変換する RAP のファスト イーサネット接続が切断されていることを確認する必要があります。

（注）　MAP の電源は、電源装置またはパワー インジェクタのいずれかにすることをお勧めします。PoE は、MAP の電源としてはお勧めしません。

CLI を使用した屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更

コントローラの CLI を使用して、屋内メッシュ アクセス ポイントをあるロールから別のロールに変更する手順は、次のとおりです。

ステップ 1　屋内アクセス ポイントのロールを MAP から RAP または RAP から MAP に変更するには、次のコマンドを入力します。

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

ロールの変更後に、アクセス ポイントはリブートされます。

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

屋内メッシュ アクセス ポイントの非メッシュ Lightweight アクセス ポイントへの変換（1130AG、1240AG）

変換コマンドの入力後に、アクセス ポイントはリブートされます（下記参照）。

（注）　メッシュ（ブリッジ）から非メッシュ（ローカル）アクセス ポイントに変換する場合、コントローラへの接続にファスト イーサネットを使用することをお勧めします。バックホールが無線である場合、変換後にイーサネットを有効にして、アクセス イメージをリロードする必要があります。リロードおよびリブート後、バックホールはファスト イーサネットになります。

（注）　ルート アクセス ポイントを Lightweight アクセス ポイントに変換すると、すべての従属メッシュ アクセス ポイントでコントローラに対する接続が失われます。そのため、メッシュ アクセス ポイントは隣接する別のルート アクセス ポイントに接続できるまでは、クライアントを処理できません。同様に、ネットワークに対する接続を維持するため、クライアントは隣接する別のメッシュ アクセス ポイントに接続されることがあります。

- CLI を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次のコマンドを入力します。

  config ap mode local *Cisco_AP*

  アクセス ポイントはリロードされます。

- GUI を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次の手順を実行します。

  a. [Wireless] をクリックし、変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。

  b. [General Properties] パネルの [AP Mode] ドロップダウン メニューから [Local] を選択します。

  c. [Apply] および [Save Configuration] をクリックします。

- Cisco WCS を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次の手順を実行します。

  a. [Configure] > [Access Points] の順にクリックし､変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。

  b. [General Properties] パネルで、AP モードとして [Local] を選択します（左側）。

  c. [Save] をクリックします。

Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定

屋外アクセス ポイント（1522、1524PS）は、2.4 GHz アクセスおよび 5.8 GHz バックホールだけでなく、公共安全用のチャネル（4.9 GHz）で Cisco 3200 シリーズ モバイル アクセス ルータ（MAR）と相互運用することができます。

Cisco 3200 は*車載ネットワーク*を構築します。ここでは、PC、監視カメラ、デジタル ビデオ レコーダ、プリンタ、PDA、スキャナなどのデバイスは、主要インフラストラクチャへの接続に携帯電話や WLAN ベースのサービスなどの無線ネットワークを共有できます。これにより、警察車両などの車載展開から収集されたデータは無線インフラストラクチャ全体に統合できます。1130、1240、および 1520 シリーズ メッシュ アクセス ポイントと 3200 シリーズ モバイル アクセス ルータの間の具体的な相互運用性の詳細については、表 8-9 を参照してください。

表 8-9　メッシュ アクセス ポイントおよび MAR 3200 の相互運用性

メッシュ アクセス ポイントのモデル	MAR のモデル
1522[1]	c3201[2]、c3202[3]、c3205[4]
1524PS	c3201、c3202
1130、1240（ユニバーサル アクセスが有効な屋内メッシュ アクセス ポイントとして設定）	c3201、c3205

1. 802.11a 無線または 4.9 GHz 帯域で MAR に接続する場合、1522 でユニバーサル アクセスを有効にする必要があります。
2. モデル c3201 は、802.11b/g 無線（2.4 GHz）を搭載した MAR です。
3. モデル c3202 は、4.9 GHz サブ帯域無線を搭載した MAR です。
4. モデル c3205 は、802.11a 無線（5.8GHz サブ帯域）を搭載した MAR です。

設定のガイドライン

1522 または 1524PS メッシュ アクセス ポイントおよび Cisco MAR 3200 を公共安全ネットワークで相互運用するには、設定に関する次のガイドラインに従う必要があります。

- バックホールでクライアント アクセスを有効にする必要があります（メッシュ グローバル パラメータ）。
- メッシュ ネットワーク内のすべてのメッシュ アクセス ポイント（MAP）でグローバルに公共安全への対応を有効にする必要があります。
- 1522 または 1524PS のチャネル番号の割り当ては、Cisco 3200 の無線インターフェイスの番号と一致する必要があります。
  - チャネル 20（4950 GHz）～ 26（4980 GHz）およびサブ帯域チャネル 1 ～ 19（5 および 10 MHz）は MAR の相互運用に使用します。この設定の変更はコントローラで行います。アクセス ポイントの設定は変更されません。
  - チャネル割り当ては RAP のみに対して行います。MAP へのアップデートは、RAP によって伝搬されます。

MAR 3200 のデフォルトのチャネル幅は、5 MHz です。次のいずれかを実行する必要があります。

- チャネル幅を 10 または 20 MHz に変更し、WGB が 1520 シリーズ メッシュ アクセス ポイントとアソシエートできるようにします。

- 1522 または 1524PS のチャネルを 5 MHz（チャネル 1 ～ 10）または 10 MHz 帯域（チャネル 11 ～ 19）のチャネルに変更します。
  - CLI を使用する場合、チャネルを設定する前に、802.11a 無線を無効にする必要があります。チャネルの設定後、無線を再度有効にします。
  - GUI を使用する場合、チャネルの設定時に 802.11a 無線を有効および無効にする必要はありません。
  - Cisco MAR 3200 は 5、10、または 20 MHz 帯域内でチャネルをスキャンできますが、複数の帯域にわたってスキャンすることはできません。

GUI を使用した Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定

コントローラの GUI を使用して、1522 および 1524PS メッシュ アクセス ポイントが Cisco 3200 シリーズ MAR とアソシエートできるようにする手順は、次のとおりです。

ステップ 1　バックホールでのクライアント アクセスを有効にするには、[Wireless] > [Mesh] の順にクリックして、[Mesh] ページを開きます。

ステップ 2　[Backhaul Client Access] チェックボックスをオンにして、802.11a 無線での無線クライアント アソシエーションを許可します。

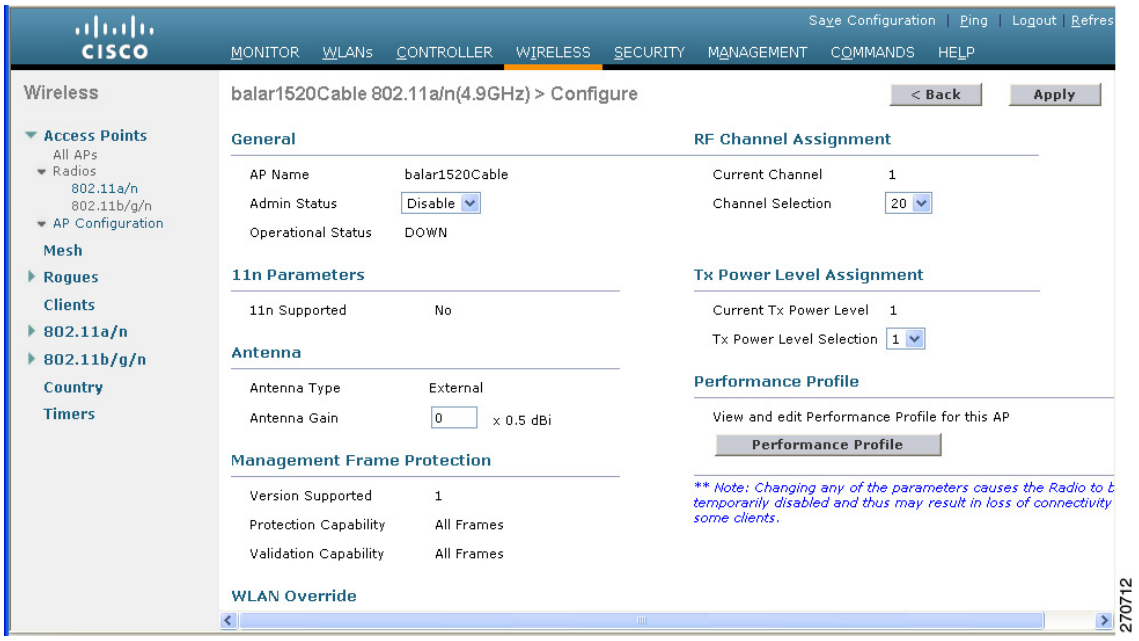
ステップ 3　[Apply] をクリックして、変更を適用します。

ステップ 4　ネットワーク上のすべてのメッシュ アクセス ポイントがリブートされることを確認するプロンプトが表示されたら、[OK] をクリックします。

ステップ 5　[Wireless] > [Access Points] > [Radios] > [802.11a/n] の順にクリックして、[802.11a/n Radios] ページを開きます。

ステップ 6　カーソルを適切な RAP の青いドロップダウン矢印の上に置いて、[Configure] を選択します。[802.11a/n (4.9 GHz) > Configure] ページが表示されます（図 8-32 を参照）。

図 8-32　[802.11 a/n (4.9GHz) > Configure] ページ



ステップ 7　[RF Channel Assignment] の [Assignment Method] で [Custom] オプションを選択し、1 ～ 26 のチャネルを選択します。

ステップ 8　[Apply] をクリックして、変更を適用します。

ステップ 9　[Save Configuration] をクリックして、変更を保存します。

CLI を使用した Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定

コントローラの CLI を使用して、1522 および 1524PS メッシュ アクセス ポイントが Cisco 3200 シリーズ MAR とアソシエートできるようにする手順は、次のとおりです。

ステップ 1　1522 および 1524PS メッシュ アクセス ポイントでクライアント アクセス モードを有効にするには、次のコマンドを入力します。

config mesh client-access enable

ステップ 2　公共安全への対応をグローバルに有効にするには、次のコマンドを入力します。

config mesh public-safety enable *all*

ステップ 3　公共安全チャネルを有効にするには、次のコマンドを入力します。

- 1522 アクセス ポイントの場合、次のコマンドを入力します。

  config 802.11a disable *Cisco_MAP*

  config 802.11a channel ap *Cisco_MAP channel_number*

  config 802.11a enable *Cisco_MAP*

- 1524PS の場合、次のコマンドを入力します。

config 802.11–a49 disable *Cisco_MAP*

config 802.11–a49 channel ap *Cisco_MAP channel_number*

config 802.11–a49 enable *Cisco_MAP*

（注）　5.8 GHz 無線を有効にするには、**config 802.11–a58 enable** *Cisco_MAP* と入力します。

（注）　1522 および 1524PS メッシュ アクセス ポイントの両方で、有効なチャネル番号の値は 1 ～ 26 です。

ステップ 4　変更を保存するには、次のコマンドを入力します。

save config

ステップ 5　設定を確認するには、次のコマンドを入力します。

show mesh public-safety

show mesh client-access

show ap config 802.11a summary（1522 アクセス ポイントの場合）

show ap config 802.11–a49 summary（1524PS アクセス ポイントの場合）

（注）　5.8 GHz 無線の設定の詳細を表示するには、**show config 802.11-a58 summary** と入力します。