シスコ ワイヤレス メッシュ アクセス ポイント リリース 8.1 ～ 8.4 設計および展開ガイド

初版：2017 年 03 月 06 日

最終更新：2015 年 11 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

本書では、Cisco Unified Wireless Network（CUWN）のコンポーネントである Cisco Wireless Mesh Networking ソリューションを使用したセキュアな企業、キャンパス、メトロポリタンの Wi-Fi ネットワークの設計および展開のガイドラインについて説明しています。

メッシュ ネットワーキングでは、シスコ ワイヤレス LAN コントローラと共に、Cisco Aironet 1500 シリーズの屋外メッシュ アクセス ポイントおよび屋内メッシュ アクセス ポイント（Cisco Aironet 1130, 1240、1250、2600、2700、3500、3600、および 3700 シリーズ アクセス ポイント）、さらに Cisco Prime Infrastructure を採用してスケーラブルな集中管理および屋内外の展開のモビリティを提供しています。Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、ネットワークへのメッシュ アクセス ポイントの接続を管理します。

メッシュ ネットワーク内のエンドツーエンドのセキュリティは、ワイヤレス メッシュ アクセス ポイントと Wi-Fi Protected Access 2（WPA2）クライアントの間で高度な暗号化標準（AES）の暗号化を採用することでサポートされています。本書では、屋外ネットワークの設計時に考慮しなければならない無線周波数（RF）コンポーネントの概略についても説明しています。

このマニュアルで説明する機能は、次の製品に該当します。

- Cisco Aironet 1570（1572）シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1560（1562）シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1550（1552）シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1530 シリーズ屋外メッシュ アクセス ポイント
- Cisco Aironet 2600、2700、3500、3600、および 3700 シリーズの屋内メッシュ アクセス ポイント
- Cisco ワイヤレス LAN コントローラのメッシュ機能
- Cisco Prime Infrastructure のメッシュ機能

この章の内容は、次のとおりです。

- 表記法，xv ページ
- 関連資料，xvii ページ
- マニュアルの入手方法およびテクニカル サポート，xvii ページ

対象読者

このドキュメントは、メッシュ ネットワークの設計および導入、シスコのメッシュ アクセス ポイントとシスコ ワイヤレス LAN コントローラの設定および維持を行う経験豊富なネットワーク管理者向けです。

マニュアルの構成

このガイドは次の章にわかれています。

章タイトル	説明
メッシュ ネットワーク コンポーネント	この章では、メッシュ ネットワークのコンポーネントについて説明します。
メッシュ導入モード	この章では、メッシュ アクセス ポイントのさまざまな導入モードについて説明します。
デザインの考慮事項	この章では、メッシュ ネットワークに関連する設計上の考慮事項について説明します。
メッシュ導入リリース 8.4 の Air Time Fairness	この章では、メッシュ導入における Air Time Fairness について説明します。
サイトの準備と計画	この章では、実装の詳細と設定例について説明します。
Cisco 1500 シリーズ 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、ネットワークへのメッシュ アクセス ポイントの接続およびメッシュ アクセス ポイントの設定に関連する手順について説明します。
ネットワークの状態の確認	この章では、メッシュ ネットワークの状態を確認するために入力するコマンドについて説明します。
トラブルシューティング	この章では、トラブルシューティング情報について説明します。
Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理	この章では、Cisco Prime Infrastructure でのアクセス ポイント管理に関する情報について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.（このマニュアルに記載されている警告の翻訳を参照するには、付録の「翻訳版の安全上の警告」を参照してください）。

警告タイトル	説明
Waarschuwing	Dit waarschuwingssymbool betekent gevaar.U verkeert in een situatie die lichamelijk letsel kan veroorzaken.Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.(Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa.Olet tilanteessa, joka voi johtaa ruumiinvammaan.Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.(Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger.Vous vous trouvez dans une situation pouvant entraîner des blessures.Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents.Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr.Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte.Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.(Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo.Si è in una situazione che può causare infortuni.Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare.Du befinner deg i en situasjon som kan føre til personskade.Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.(Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)

警告タイトル	説明
Aviso	Este símbolo de aviso indica perigo.Encontra-se numa situação que lhe poderá causar danos fisicos.Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.(Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro.Existe riesgo para su integridad física.Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.(Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara.Du befinner dig i en situation som kan leda till personskada.Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.(Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

関連資料

Cisco Unified Wireless Network ソリューションについては、併せて次のマニュアルも参照してください。

- *Cisco* ワイヤレス *LAN* コントローラ コンフィギュレーション ガイド
- 『*Cisco Wireless LAN Controller Command Reference*』
- 『*Cisco Prime Infrastructure Configuration Guide*』
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

メッシュ ネットワーク コンポーネント

この章では、メッシュ ネットワーク コンポーネントについて説明します。

Cisco ワイヤレス メッシュ ネットワークには、次の 4 つのコア コンポーネントがあります。

- Cisco Aironet シリーズ アクセス ポイント

（注） Cisco Aironet 1520 シリーズのメッシュ アクセス ポイントは、生産終了のためサポートされていません。

- シスコ ワイヤレス LAN コントローラ（以下、**コントローラ**）
- Cisco Prime Infrastructure
- メッシュ ソフトウェア アーキテクチャ

この章の内容は、次のとおりです。

メッシュ アクセス ポイント

5508、5520、および8540シリーズCiscoコントローラにおけるメッシュ アクセス ポイントのライセンス

Cisco 5500 および 8500 シリーズ コントローラでメッシュ アクセス ポイントと非メッシュ アクセス ポイントの両方を使用する場合、7.0 リリース以降、必要なライセンスは基本ライセンスだけになりました。ライセンスの取得とインストールの詳細については、http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html の『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

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、次の 2 つの方法のいずれかで動作します。

1. ルート アクセス ポイント（RAP）
2. メッシュ アクセス ポイント（MAP）

（注） すべてのアクセス ポイントは、メッシュ アクセス ポイントとして設定され、出荷されます。アクセス ポイントをルート アクセス ポイントとして使用するには、メッシュ アクセス ポイントをルート アクセス ポイントに再設定する必要があります。すべてのメッシュ ネットワークで、少なくとも 1 つのルート アクセス ポイントがあることを確認します。

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

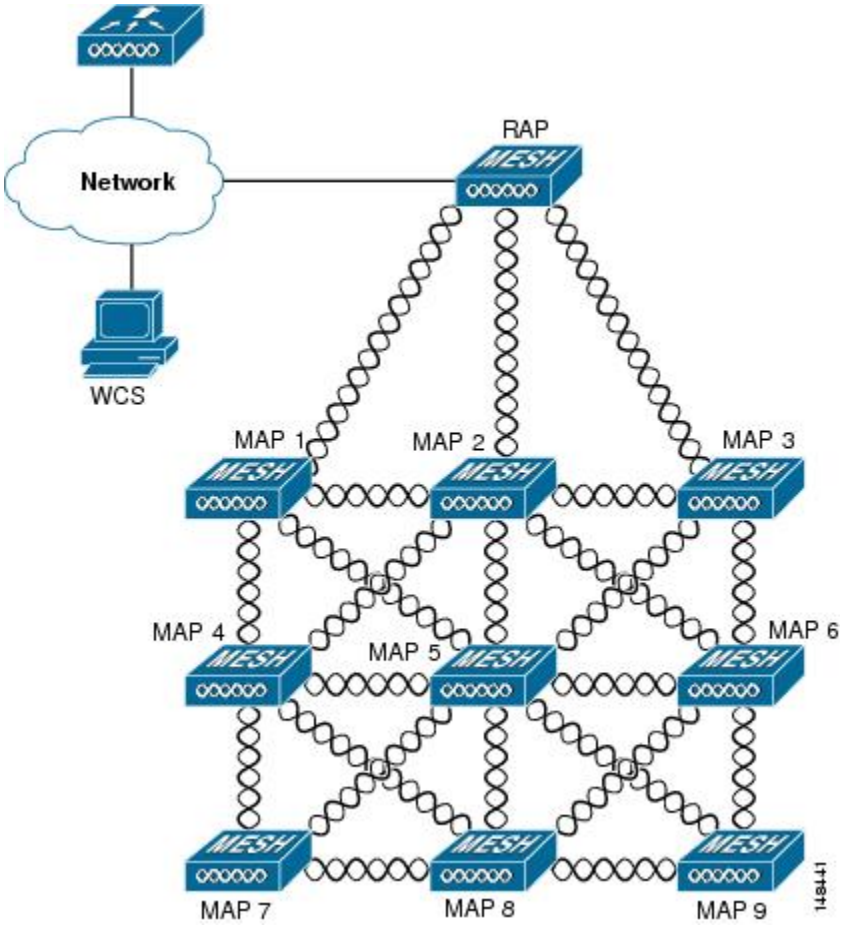
MAP は MAP 間および RAP への通信に 802.11a/n/g 無線バックホールを使用して無線接続を行います。MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。

ブリッジモードのアクセスポイントでは、CleanAirによってメッシュバックホールがサポートされ、干渉デバイス レポート（IDR）および電波品質の指標（AQI）レポートのみが生成されます。

（注） RAP または MAP は、ブリッジ プロトコル データ ユニット（BPDU）自体は生成しません。ただし、RAP または MAP がネットワーク全体で接続された有線またはワイヤレスのインターフェイスから BPDU を受信した場合、RAP または MAP はアップストリーム デバイスに BPDU を転送します。

この図は、メッシュ ネットワーク内の RAP と MAP の間にある関係を示しています。

図 *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

ワイヤレス メッシュ ネットワークでは、異なる 2 つのトラフィック タイプを同時に伝送できます。伝送できるトラフィック タイプは次のとおりです。

- 無線 LAN クライアント トラフィック
- MAP イーサネット ポート トラフィック

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の認証方式で管理されます。

- MAC 認証：メッシュ アクセス ポイントが参照可能データベースに追加され、特定のコントローラおよびメッシュ ネットワークに確実にアクセスできるようにします。

- 外部 RADIUS 認証：メッシュ アクセス ポイントは、証明書付きの拡張認証プロトコル（EAP-FAST）のクライアント認証タイプをサポートする Cisco ACS（4.1 以上）などの RADIUS サーバを使用して、外部から認証できます。

ネットワークのセグメント化

メッシュ アクセス ポイント用のワイヤレス LAN メッシュ ネットワークへのメンバーシップは、ブリッジ グループ名（BGN）によって制御されます。メッシュ アクセス ポイントは、類似のブリッジグループに配置して、メンバーシップを管理したり、ネットワーク セグメンテーションを提供したりすることができます。

Cisco 屋内メッシュ アクセス ポイント

このリリースでサポートされているアクセス ポイント プラットフォームは以下のとおりです。

- Cisco Aironet 1600 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 2600 シリーズ アクセス ポイント
- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 3500 シリーズ アクセス ポイント
- Cisco Aironet 3600 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Aironet 1530 シリーズ アクセス ポイント
- Cisco Aironet 1550 シリーズ アクセス ポイント
- Cisco Aironet 1560 シリーズ アクセス ポイント
- Cisco Aironet 1570 シリーズ アクセス ポイント
- Cisco Industrial Wireless 3700 シリーズ アクセス ポイント

（注） 8.4 リリースでは次の AP がサポートされます。

（注） アクセス ポイントのコントローラ ソフトウェアのサポートの詳細については、『*Cisco Wireless Solutions Software Compatibility Matrix*』を参照してください。URL は次のとおりです。http://www.cisco.com/en/US/docs/wireless/controller/5500/tech_notes/Wireless_Software_Compatibility_Matrix.html

エンタープライズ 11n/ac メッシュは、802.11n/ac アクセス ポイントで動作するために CUWN 機能に追加される拡張機能です。エンタープライズ 11ac メッシュ機能は 802.11ac 以外のメッシュと互換性がありますが、バックホールとクライアントのアクセス速度が向上します。802.11ac 屋内アクセス ポイントは、特定の屋内展開用のデュアル無線 Wi-Fi インフラストラクチャ デバイスです。一方の無線をアクセス ポイントのローカル（クライアント）アクセスに使用でき、もう一方の無線をワイヤレス バックホールに対して設定できます。ユニバーサル バックホール アクセスが有効な場合、リリース 8.2 の 5 GHz および 2.4 GHz 無線はローカル（クライアント）アクセス、バックホールの両方に使用できます。エンタープライズ 11ac メッシュは、P2P、P2MP、およびアーキテクチャのメッシュ タイプをサポートします。

屋内アクセス ポイントをブリッジモードに直接設定して、これらのアクセス ポイントをメッシュ アクセス ポイントとして直接使用できます。これらのアクセス ポイントがローカル モード（非メッシュ）である場合は、これらのアクセス ポイントをコントローラに接続し、AP モードをブリッジ モード（メッシュ）に変更する必要があります。このシナリオは、特に、展開されるアクセス ポイント量が大きく、アクセス ポイントが従来の非メッシュ ワイヤレス カバレッジに対してローカル モードですでに展開されている場合に、煩雑になります。

Cisco 屋内メッシュ アクセス ポイントでは、次の 2 つの無線が同時に動作します。

- リリース 8.2 以降、UBA が有効な場合に 2.4 GHz 無線はデータ バックホールとクライアント アクセスに使用されてきました。
- ユニバーサル バックホール アクセスが有効である場合、データ バックホールおよびクライアント アクセスに使用される 5 GHz の無線

5 GHz の無線は、5.15 GHz、5.25 GHz、5.47 GHz、および 5.8 GHz の帯域をサポートします。

Cisco 屋外メッシュ アクセス ポイント

Cisco 屋外メッシュ アクセス ポイントは、Cisco Aironet 1500 シリーズ アクセス ポイントから構成されます。1500 シリーズには、1572 11ac 屋外アクセス ポイント、1552 および 1532 11n 屋外メッシュ アクセス ポイント、および 1560 11ac Wave 2 シリーズが含まれます。

Cisco 1500 シリーズ メッシュ アクセス ポイントは、ワイヤレス メッシュ展開の中核的なコンポーネントです。AP1500 は、コントローラ（GUI および CLI）と Cisco Prime Infrastructure の両方により設定されます。屋外メッシュ アクセス ポイント（MAP および RAP）間の通信は、802.11a/n/ac 無線バックホールを介します。クライアント トラフィックは、一般に 802.11b/g/n 無線を介して送信されます（クライアント トラフィックを受け入れるように 802.11a/n/ac も設定できます）。

メッシュ アクセス ポイントは、有線ネットワークに直接接続されていない他のアクセス ポイントの中継ノードとしても動作します。インテリジェントな無線ルーティングは Adaptive Wireless Path Protocol（AWPP）によって提供されます。このシスコのプロトコルを使用することで、各メッシュ アクセス ポイントはネイバー アクセス ポイントを識別し、パスごとに信号の強度とコントローラへのアクセスに必要なホップ カウントについてコストを計算して、有線ネットワークまでの最適なパスをインテリジェントに選択できるようになります。

アップリンク サポートには、ギガビット イーサネット（1000BASE-T）と、ファイバまたはケーブル モデム インターフェイスに接続できる小型フォーム ファクタ（SFP）スロットが含まれます。1000BASE-BX までのシングルモード SFP とマルチモード SFP の両方がサポートされます。

メッシュ アクセス ポイントのタイプに基づき、ケーブル モデムは DOCSIS 2.0 または DOCSIS/EuroDOCSIS 3.0 になります。

AP1550 は、厳しい環境向けハードウェア格納ラックに設置します。危険場所対応の AP1500 は、Class I、Division 2、Zone 2 の危険場所での安全基準を満たしています。

メッシュ アクセス ポイントは、メッシュ モード以外では、以下のモードで動作できます。

- ローカル モード：このモードでは、AP は割り当てられたチャネル上のクライアントを処理できます。180 秒周期で帯域上のすべてのチャネルをモニタ中にも、クライアントの処理が可能です。この間に、AP は 50 ミリ秒周期で各チャネルをリッスンし、不正なクライアントのビーコン、ノイズ フロアの測定値、干渉、および IDS イベントを検出します。また AP は、チャネル上の CleanAir 干渉もスキャンします。
- FlexConnect モード：FlexConnect は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。FlexConnect モードを使用すると、各オフィスにコントローラを展開しなくても、会社のオフィスから WAN リンクを介して支社や離れた場所にあるオフィスのアクセス ポイントを設定および制御できます。コントローラとの接続が失われたときは、FlexConnect AP でクライアント データ トラフィックをローカルでスイッチして、クライアント認証をローカルで実行することができます。コントローラに接続されている場合、FlexConnect モードではコントローラにトラフィックをトンネリングで戻すこともできます。
- Flex+Bridge モード：このモードでは、FlexConnect とブリッジ モードの設定オプションの両方をアクセス ポイントで使用できます。
- モニタ モード：このモードでは、AP 無線は受信状態にあります。AP は、12 秒ごとにすべてのチャネルをスキャンし、不正なクライアントのビーコン、ノイズ フロアの測定値、干渉、IDS イベント、および CleanAir 侵入者を検出します。
- Rogue Detector モード：このモードでは、AP 無線がオフになり、AP は有線トラフィックのみをリッスンします。コントローラは Rogue Detector として設定されている AP と、疑わしい不正クライアントおよび AP の MAC アドレスのリストを渡します。Rogue Detector は ARP パケットを監視します。Rogue Detector はトランク リンクを介して、すべてのブロードキャスト ドメインに接続できます。
- スニファ モード：AP はチャネル上のすべてのパケットをキャプチャし、Wireshark などのパケット アナライザ ソフトウェアを使用してパケットを復号するリモート デバイスに転送します。
- ブリッジ モード：このモードでは、有線ネットワークのケーブル接続が利用できない無線メッシュ ネットワークを作成するために、AP が設定されます。

（注） GUI および CLI の両方を使用してこれらのモードを設定できます。手順については、『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

（注） MAP は、有線と無線のバックホールに関係なく、ブリッジ/Flex+Bridge モードでだけ設定できます。有線バックホールを持つ MAP の場合は、AP モードを変更する前に、AP ロールを RAP に変更する必要があります。

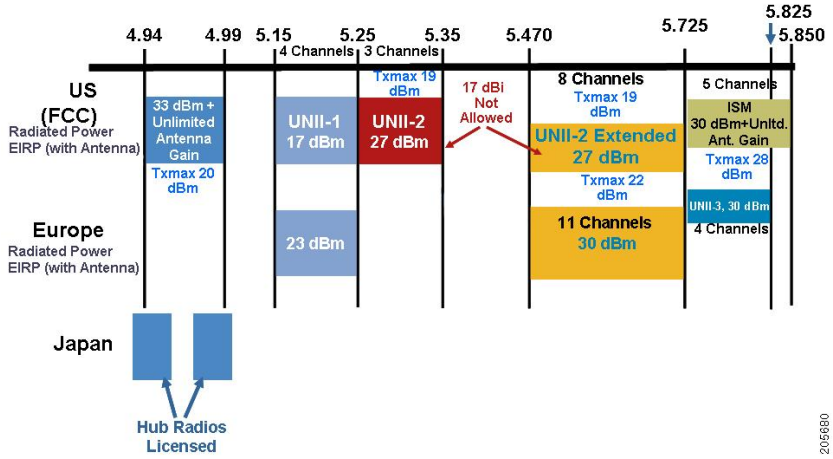
（注） 屋外メッシュ AP のすべてのモデルの詳細と仕様については、以下のリンクを参照してください。

- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1530-series/data_sheet_c78-728356.html
- http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1550-series/data_sheet_c78-641373.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1550/installation/guide/1550hig/1550_ch1.html
- http://wwwin.cisco.com/c/cec/prods-industry/selling-en/products/wireless/ap.html
- http://www.cisco.com/c/en/us/support/wireless/aironet-1572eac-outdoor-access-point/model.html
- http://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-1570-series/datasheet-c78-732348.pdf

周波数帯域

2.4 GHz および 5 GHz の両方の周波数帯域が屋内および屋外アクセス ポイントでサポートされます。

図 *2*：*AP1500* の *802.11a* 無線でサポートする周波数帯域



米国では、5 GHz 帯域は、5.150 ～ 5.250（UNII-1）、5.250 ～ 5.350（UNII-2）、5.470 ～ 5.725（UNII-2 拡張）、および 5.725 ～ 5.850（ISM）の 3 つの帯域で構成されています。UNII-1 と UNII-2 の帯域は隣接しており、802.11a では 2.4 GHz の 2 倍以上の大きさの 200 MHz 幅のスペクトルの連続 Swath として処理されます（表 1：周波数帯域，（8 ページ）を参照）。

インドの国ドメインである –D のドメインは次をサポートします。

- 20 MHz チャネル：169（5.845 GHz）および 173（5.865 GHz）
- 40 MHz チャネル：チャネル ペア 169/173（5.855 GHz）

（注） 周波数はアクセス ポイントが設定されている規制ドメインにより異なります。詳細については、http://www.cisco.com/en/US/docs/wireless/access_point/channels/lwapp/reference/guide/lw_chp2.html のドキュメント『Channels and Power Levels』を参照してください。

表 *1*：周波数帯域

周波数帯域用語	説明	サポート モデル
UNII-1[1]	5.15 ～ 5.25 GHz 周波数帯域で稼働する UNII デバイスに関する規制。-B reg のドメインを使用した屋内動作および屋外 AP。	すべての 11n/ac 屋内 AP および 1572

周波数帯域用語	説明	サポート モデル
UNII-2	5.25 ～ 5.35 GHz 周波数帯で稼働する UNII デバイスに関する規制。この帯域では、DFS と TPC が必須です。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。
UNII-2 拡張帯域	5.470 ～ 5.725 GHz の周波数帯域で動作する UNII-2 デバイスの規則。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。
ISM[2]	5.725 ～ 5.850 GHz の周波数帯域で動作する UNII デバイスの規則。	すべての 11n/ac 屋内 AP、1532、1552、1562、および 1572。

1 UNII は、Unlicensed National Information Infrastructure を意味しています。
2 ISM は産業、科学、および医療を意味しています。

（注） 規制に関する情報については、http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a.html を参照してください。

動的周波数選択

以前は、レーダーを搭載するデバイスは、他の競合サービスがなく周波数サブバンドで動作していました。しかし、規制当局の管理により、これらの帯域をワイヤレス メッシュ LAN（IEEE 802.11）などの新しいサービスに開放して共有できるようにしようとしています。

既存のレーダー サービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要のあるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFS では、無線デバイスがレーダー信号の存在を検出できる機能の採用を義務付けています。無線でレーダー信号が検出されると、最低30分間は伝送を停止して、そのサービスを保護する必要があります。その後、その無線は伝送のための別のチャネルを選択しますが、伝送前にこのチャネルをモニタリングする必要があります。使用する予定のチャネルで少なくとも 1 分間レーダーが検出されなかった場合には、新しい無線サービス デバイスはそのチャネルで伝送を開始できます。

AP は新たな DFS チャネルで、DFS スキャンを 60 秒間実行します。ただし、この新規 DFS チャネルが隣接 AP にすでに使用されている場合は、AP は DFS スキャンを実行しません。

無線がレーダー信号を検出して識別するプロセスは複雑なタスクであり、ときどきは誤った検出が起こります。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャネル レーダーを確実に検出するためのアクセス ポイントの機能など、非常に多くの要因が考えられます。

802.11h 規格では、DFS および Transmit Power Control（TPC）について、5 GHz 帯域に関連するものと指定しています。DFS を使用してレーダーの干渉を回避し、TPC を使用して Satellite Feeder Link の干渉を回避します。

（注） DFS は、米国では 5250 ～ 5350 および 5470 ～ 5725 周波数帯域に義務付けられています。ヨーロッパでは、DFS と TPC が上記帯域に義務付けられています

図 *3*：*DFS* および *TPC* 帯域の要件

アンテナ

概要

アンテナは、すべてのワイヤレス ネットワークの設置に重要なコンポーネントです。アンテナには次の 2 つの大きな種類があります。

- 指向性
- 全方向性

アンテナの種類それぞれには特定の用途があり、特定の設置タイプのときに最大に効果を発揮します。アンテナは、アンテナの設計によって決まる、ローブのあるカバレッジ エリアに RF 信号を配信するため、カバレッジが成功するかどうかは、アンテナの選択に重度に依存します。

アンテナによって、メッシュ アクセス ポイントに、ゲイン、指向性、偏波の 3 つの基本的な特性が与えられます。

- ゲイン：電力の増加の度合いを表します。ゲインは、アンテナが RF 信号に追加するエネルギーの増加量です。
- 指向性：伝送パターンの形状を表します。アンテナのゲインが増加すると、カバレッジエリアは減少します。カバレッジエリアや放射パターンは、度数で測ります。これらの角度は、度数で測定され、ビーム幅と呼ばれます。

（注） ビーム幅は、空間の特定の方向に向けて無線信号エネルギーを集中させるアンテナの能力の大きさとして定義されます。ビーム幅は通常、HB（水平ビーム幅）の度数で表現されます。通常、最も重要なビーム幅はVB（垂直ビーム幅）（上下）放射パターンで表現されます。アンテナのプロットまたはパターンを見るとき、角度は通常、メイン ローブの最大効果放射電力を基準とした場合の、メイン ローブの半電波強度（3 dB）ポイントで測定されます。

（注） 8 dBi アンテナは 360 度の水平ビーム幅で伝送するため、電波は全方位に電力を分散します。それにより、8 dBi アンテナからの電波は、ビーム幅がこれより狭い（360 度より小さい）14 dBi パッチアンテナ（またはサードパーティのディッシュ アンテナ）から送信された電波ほど遠くまではほとんど届きません。

- 偏波：空間を通る電磁波の電界の方向。アンテナは、水平方向または垂直方向のいずれかに偏向される可能性がありますが、他の種類の偏波が可能です。1 つのリンク内にあるアンテナは、それ以上無用な信号損失を避けるため、両方が同じ偏波を持つ必要があります。性能を向上させるため、アンテナを時々回転させると、偏波を変更し干渉を減少できます。RF 波を送信してコンクリートの谷間を下らせるときには垂直方向の偏波が、広範囲に伝搬させるときには水平方向の偏波の方が適しています。偏波は、RF エネルギーを隣接ストラクチャのレベルにまで減らすのが重要であるときに、RF Bleed-over を最適化するのにも利用できます。ほとんどの全方向性アンテナは、デフォルトとして垂直偏波を設定して出荷されています。

アンテナ オプション

幅広いアンテナが利用でき、さまざまな地形にメッシュ アクセス ポイントを展開する際の柔軟性を提供します。サポートされるアンテナのリストについては、該当するアクセス ポイント データシートまたは発注ガイドを参照してください。

シスコのアンテナおよびアクセサリについては、次の URL にある『*Cisco Aironet Antenna and Accessories Reference Guide*』を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

配置および設計、制限事項および機能、さらにアンテナの基礎理論や取り付け手順、規制に関する情報、技術仕様についても記載されています。

クライアント アクセス認定アンテナ（サードパーティ製アンテナ）

AP1500 は、サードパーティ製のアンテナと一緒に使用できます。ただし、次のことに注意してください。

- シスコは、未認定のアンテナやケーブルの品質、性能、信頼性についての情報を追跡したり保持したりしません。

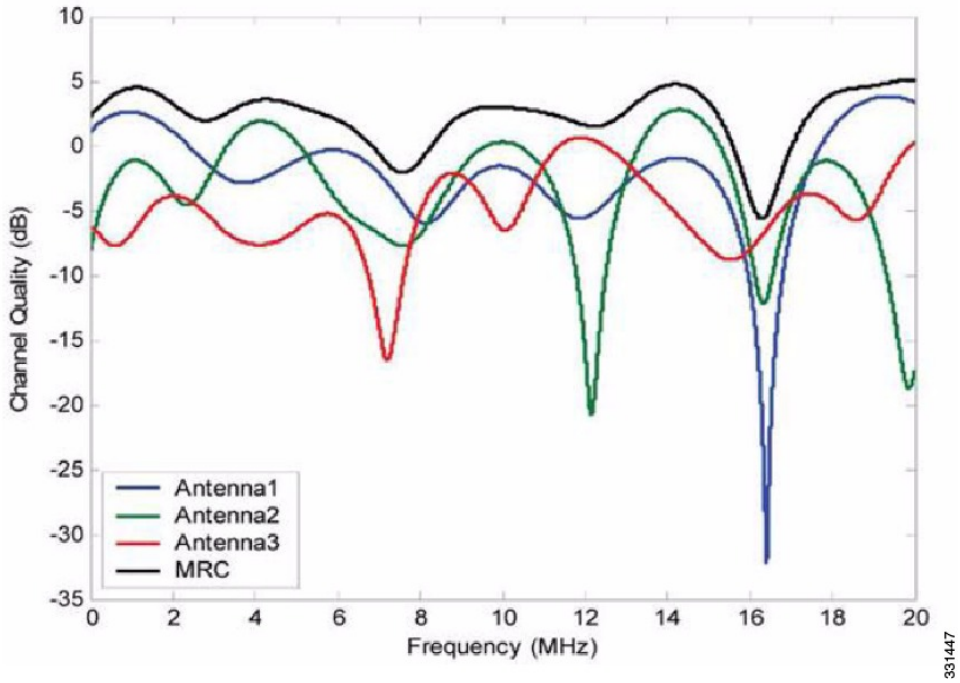
- RF 接続性および準拠性については、お客様の責任で使用してください。
- 準拠性を保証するのは、シスコ製のアンテナもしくは、シスコ製のアンテナと同一の設計およびゲインのアンテナの場合だけです。
- シスコ社以外のアンテナおよびケーブルについて、Cisco Technical Assistance Center（TAC）にトレーニングやカスタマー履歴の情報はありません。

最大比合成

この機能を理解するために、1 つのトランスミッタを装備した 802.11a/g クライアントが、複数のトランシーバを装備した 802.11n アクセスポイントにアップリンク パケットを送信する場合について考えてみます。アクセス ポイントは 3 本の受信アンテナそれぞれで信号を受信します。

受信した各信号の位相と振幅は、アンテナとクライアントの間隔の特性によって異なります。アクセス ポイントは、最適な信号を形成するために位相と振幅を調整することで、受信した 3 つの信号を処理して 1 つの強化された信号にします。使用されるアルゴリズムは最大比合成（MRC）と呼ばれ、通常すべての 802.11n アクセス ポイントで使用されます。MRC はアップリンク方向にだけ有用で、アクセス ポイントがクライアントをより適切に「ヒアリング」できるようにします。

図 *4*：*MRC* アルゴリズムによる受信信号の強化



Cisco ワイヤレス LAN コントローラ

ワイヤレス メッシュ ソリューションは、Cisco 2500、5500、および 8500 シリーズ ワイヤレス LAN コントローラでサポートされます。

Cisco 2500、5500、および 8500 シリーズ ワイヤレス LAN コントローラの詳細については、http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html を参照してください。

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、ワイヤレス メッシュの計画、設定、管理のためのグラフィカルなプラットフォームを提供します。Prime Infrastructure を使用すると、ネットワーク管理者は、ワイヤレス メッシュ ネットワークの設計、コントロール、モニタリングを中央の場所から行えます。

Prime Infrastructure はネットワーク管理者に、RF 予測、ポリシー プロビジョニング、ネットワーク最適化、トラブルシューティング、ユーザ トラッキング、セキュリティ モニタリング、およびワイヤレス LAN システム管理のソリューションを提供します。グラフィカル インターフェイスを使用したワイヤレス LAN の配置と操作は、簡単で費用有効です。詳細なトレンド分析および分析レポートにより、Prime Infrastructure は現行のネットワーク操作に不可欠なものになります。

Prime Infrastructure は、組み込みデータベースと共に、サーバ プラットフォームで実行されます。これにより、何百ものコントローラや何千もの Cisco メッシュ アクセス ポイントを管理可能にするスケーラビリティが提供されます。コントローラは、Prime Infrastructure と同じ LAN 上、別の経路選択済みサブネット上、または広域接続全体にわたって配置できます。

アーキテクチャ

アーキテクチャ

Control and Provisioning of Wireless Access Points

Control And Provisioning of Wireless Access Points（CAPWAP）は、ネットワークのアクセス ポイント（メッシュおよび非メッシュ）を管理するためにコントローラが使用するプロビジョニングと制御プロトコルです。リリース 5.2 で、Lightweight AP Protocol（LWAPP）が CAPWAP に置き換えられました。

（注） CAPWAP を使用すると、資本的支出（CapEx）と運用維持費（OpEx）が著しく減少し、シスコ ワイヤレス メッシュ ネットワーキング ソリューションが、企業、キャンパス、メトロポリタンのネットワークにおける費用有効でセキュアな配置オプションになります。

メッシュ ネットワークの CAPWAP ディスカバリ

メッシュ ネットワークの CAPWAP ディスカバリ プロセスは次のとおりです。

1. CAPWAP ディスカバリの開始の前に、メッシュ アクセス ポイントがリンクを確立します。その一方で、非メッシュ アクセス ポイントが、そのメッシュ アクセス ポイント用の静的 IP（ある場合）を使用して、CAPWAP ディスカバリを開始します。
2. メッシュ アクセス ポイントは、レイヤ 3 ネットワークのメッシュ アクセス ポイントの静的 IP を使用して CAPWAP ディスカバリを開始するか、割り当てられたプライマリ、セカンダリ、ターシャリのコントローラ用のネットワークを探します。接続するまで最大 10 回試行されます。

（注） メッシュ アクセス ポイントは、セットアップ中に、そのアクセス ポイントで設定されている（準備のできている）コントローラのリストを探します。

3. 手順 2 が 10 回の試行の後に失敗した場合、メッシュ アクセス ポイントは DHCP にフォールバックし、接続を 10 回試行します。
4. 手順 2 と 3 の両方に失敗し、コントローラに対して成功した CAPWAP 接続がない場合、メッシュ アクセス ポイントは LWAPP にフォール バックします。
5. 手順 2、3、4 の試行後にディスカバリがなかった場合、メッシュ アクセス ポイントは次のリンクを試みます。

ダイナミック MTU 検出

ネットワークで MTU が変更された場合、アクセス ポイントは、新しい MTU の値を検出し、それをコントローラに転送して、新しい MTU に調整できるようにします。新しい MTU でアクセス ポイントとコントローラの両方がセットされると、それらのパス内にあるすべてのデータは、新しい MTU 内で断片化されます。変更されるまで、その新しい MTU のサイズが使用されます。スイッチおよびルータでのデフォルトの MTU は、1500 バイトです。

XML 設定ファイル

コントローラのブート設定ファイル内のメッシュの機能は、XML ファイルに ASCII 形式で保存されます。XML 設定ファイルは、コントローラのフラッシュ メモリに保存されます。

（注） 現行リリースは、バイナリの設定ファイルをサポートしませんが、設定ファイルはメッシュ リリースからコントローラ ソフトウェア リリース 7.0 へのアップグレード後すぐにバイナリ状態になります。XML 構成ファイルは、リセット後に選択されます。

注意 XMLファイルを編集しないでください。修正された設定ファイルをコントローラにダウンロードすると、ブート時に巡回冗長検査（CRC）エラーが発生し、設定がデフォルト値にリセットされます。

XML設定ファイルは、CLI形式に変換すると、容易に読み込みや修正ができます。XMLからCLI形式に変換するには、設定ファイルを TFTP または FTP のサーバにアップロードします。コントローラはアップロード中に、XML から CLI への変換を開始します。

サーバ上では、CLI 形式で設定ファイルを読み取りまたは編集できます。その後、そのファイルをダウンロードして、コントローラに戻すことができます。コントローラでは、設定ファイルが再度 XML 形式に変換されて、フラッシュ メモリに保存され、新しい設定を使用してリブートされます。

コントローラは、ポート設定 CLI コマンドのアップロードおよびダウンロードをサポートしません。コントローラ ポートを設定したい場合は、次にまとめた関連コマンドを入力します。

（注） 次のコマンドは、ソフトウェアをリリース 7.0 にアップグレードすると、手動で入力できます。

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートでアップ リンク トラップおよびダウン リンク トラップを有効または無効にします。
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートで管理モードを有効または無効にします。
- **config port multicast appliance** *port* {**enable** | **disable**}：特定のコントローラ ポートに対し、マルチキャスト アプライアンス サービスを有効または無効にします。
- **config port power** {*port* | **all**} {**enable** | **disable**}：特定のコントローラ ポートまたはすべてのポートで Power-over-Ethernet（PoE）を有効または無効にします。

既知のキーワードおよび正しい構文を持つCLIコマンドはXMLに変換されますが、不適切なCLIコマンドは無視されてフラッシュ メモリに保存されます。無効な値を持つフィールドは、XML 検証エンジンにより、フィルタ アウトされ、デフォルト値にセットされます。検証は、ブート中に実行されます。

無視されたコマンドおよび無効な設定値を確認するには、次のコマンドを入力します。

show invalid-config

（注） このコマンドは、**clear config** コマンドまたは **save config** コマンドの前にしか実行できません。ダウンロードした設定に多数の無効なCLIコマンドが含まれている場合、分析のため、無効な設定を TFTP または FTP サーバにアップロードできます。

アクセスパスワードは、設定ファイルの中に隠されて（難読化されて）います。アクセスポイントまたはコントローラのパスワードをイネーブルまたはディセーブルにするには、次のコマンドを入力します。

config switchconfig secret-obfuscation {**enable** | **disable**}

Adaptive Wireless Path Protocol

Adaptive Wireless Path Protocol（AWPP）は、ワイヤレス メッシュ ネットワーキング用に設計されたもので、これを使用すると、配置が容易になり、コンバージェンスが高速になり、リソースの消費が最小限に抑えられます。

AWPP は、クライアント トラフィックがコントローラにトンネルされているために AWPP プロセスから見えないという CAPWAP WLAN の特性を利用します。また、CAPWAP WLAN ソリューションの拡張無線管理機能はワイヤレス メッシュ ネットワークに利用できるため、AWPP に組み込む必要はありません。

AWPP を使用すると、リモート アクセス ポイントは、RAP のブリッジ グループ（BGN）の一部である各 MAP 用の RAP に戻る最適なパスを動的に見つけられるようになります。従来のルーティング プロトコルとは異なり、AWPP は RF の詳細を考慮に入れています。

ルートを最適化するため、MAP はネイバー MAP をアクティブに送信要求します。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。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。

AWPP は、パスごとに信号の強度とホップ カウントについてコストを計算して、CAPWAP コントローラへ戻る最適なパスを自動で判別します。パスが確立されると、AWPP は継続的に条件をモニタし、条件の変化に応じてルートを変更します。また、AWPP は、条件情報を知らせるスムージング機能を実行して、RF 環境のエフェメラルな性質に、ネットワークの安定性が影響を受けないようにします。

トラフィック フロー

ワイヤレス メッシュ内のトラフィック フローは、次の 3 つのコンポーネントに分けられます。

1. オーバーレイ CAPWAP トラフィック：標準の CAPWAP アクセス ポイントの配置内のフローで、CAPWAP アクセス ポイントと CAPWAP コントローラの間の CAPWAP トラフィックのことです。
2. ワイヤレス メッシュ データ フレーム フロー
3. AWPP 交換

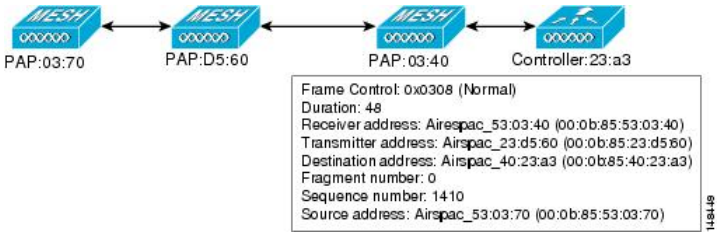
CAPWAP モデルはよく知られており、AWPP は専用プロトコルのため、ワイヤレス メッシュ データ フローについてだけ説明します。ワイヤレス メッシュ データ フローのキーは、メッシュ アクセス ポイント間で送信される 802.11 フレームのアドレス フィールドです。

802.11 データ フレームは、レシーバ、トランスミッタ、送信先、発信元の 4 つまでのアドレス フィールドを使用できます。WLAN クライアントから AP までの標準フレームでは、トランスミッ

タ アドレスと発信元アドレスが同じため、これらのアドレス フィールドのうち 3 つしか使用されません。しかし、WLANブリッジング ネットワークでは、フレームが、トランスミッタの背後にあるデバイスによって生成された可能性があるため、フレームの発信元がフレームのトランスミッタであるとは限らず、4 つのすべてのアドレス フィールドが使用されます。

図 5：ワイヤレス メッシュ フレーム，（17 ページ） は、このタイプのフレーム構成の例を示しています。フレームの発信元アドレスはMAP:03:70、このフレームの送信先アドレスはコントローラ（メッシュ ネットワークはレイヤ 2 モードで動作しています）、トランスミッタ アドレスはMAP:D5:60、レシーバ アドレスは RAP:03:40 です。

図 *5*：ワイヤレス メッシュ フレーム



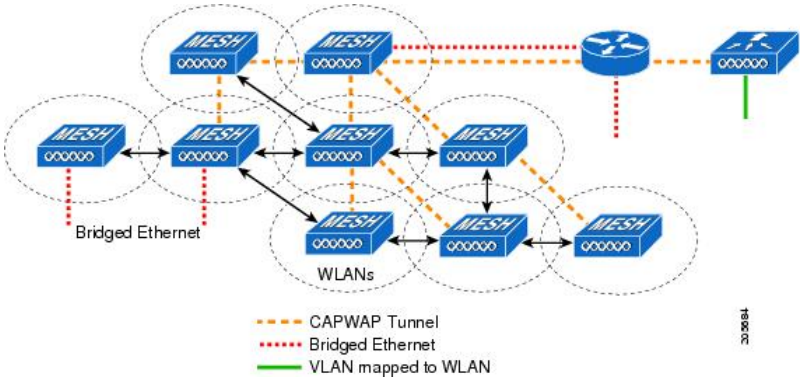
このフレームの送信により、トランスミッタとレシーバのアドレスは、ホップごとに変わります。各ホップでレシーバ アドレスを判別するために AWPP が使用されます。トランスミッタ アドレスは、現在のメッシュ アクセス ポイントのアドレスです。パス全体を通して、発信元アドレスと送信先アドレスは同一です。

RAP のコントローラ接続がレイヤ 3 の場合、MAP はすでに CAPWAP を IP パケット内にカプセル化してコントローラに送信済みのため、そのフレームの送信先アドレスはデフォルト ゲートウェイ MAC アドレスになり、ARP を使用する標準の IP 動作を使用してデフォルト ゲートウェイの MAC アドレスを検出します。

メッシュ内の各メッシュ アクセス ポイントは、コントローラと共に、CAPWAP セッションを形成します。WLAN トラフィックはCAPWAP 内にカプセル化されるため、コントローラ上の VLAN インターフェイスにマップされます。ブリッジされたイーサネット トラフィックは、メッシュ ネットワーク上の各イーサネット インターフェイスから渡される可能性があり、コントローラの

インターフェイスにマップされる必要はありません（図 6：論理ブリッジと WLAN マッピング, （18 ページ） を参照）。

図 *6*：論理ブリッジと *WLAN* マッピング

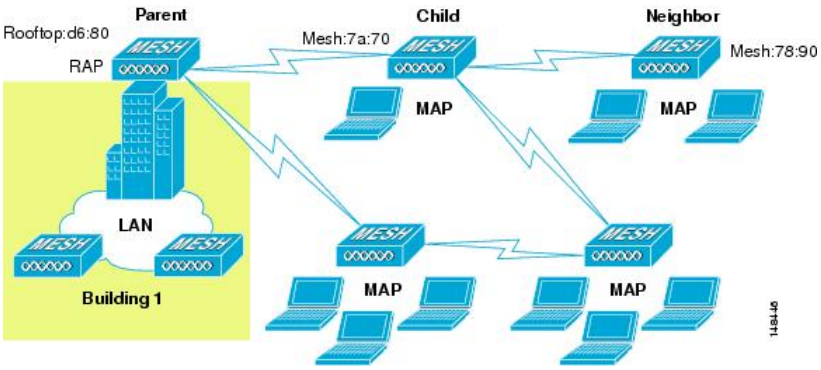


メッシュ ネイバー、親、および子

メッシュ アクセス ポイント間の関係は、親、子、ネイバーです（図 7：親、子、およびネイバー アクセス ポイント, （18 ページ） を参照）。

- 親アクセス ポイントは、容易度の値（ease value）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。
  - 容易度の値（ease value）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、他のアクセスポイントのRF範囲内にありますが、その容易度の値は親よりも低いため、親や子としては選択されません。

図 *7*：親、子、およびネイバー アクセス ポイント



最適な親を選択するための基準

AWPP は、次のプロセスに従って、無線バックホールを使用して RAP または MAP 用に親を選択します。

- *scan* ステートでは、パッシブ スキャニングによって、ネイバーのあるチャネルのリストが生成され、それが、すべてのバックホール チャネルのサブセットになります。
- *seek* ステートでは、アクティブ スキャニングによって、ネイバーを持つチャネルが探され、バックホール チャネルは最適なネイバーを持つチャネルに変更されます。
- *seek* ステートでは、親は最適なネイバーとしてセットされ、親子のハンドシェイクが完了します。
- *maintain* ステートでは、親のメンテナンスと最適化が実行されます。

このアルゴリズムは、起動時、および親が消失して他に親になりそうなものがない場合に実行され、通常は、CAPWAP ネットワークとコントローラのディスカバリが続けて実行されます。すべてのネイバー プロトコル フレームは、チャネル情報を運びます。

親メンテナンスは、誘導 NEIGHBOR_REQUEST を親に送信している子ノードおよび NEIGHBOR_RESPONSE で応答している親によって実行されます。

親の最適化とリフレッシュは、親が常駐しているチャネル上で NEIGHBOR_REQUEST ブロードキャストを送信している子ノードによって、そのチャネル上のネイバリング ノードからのすべての応答の評価によって発生し実行されます。

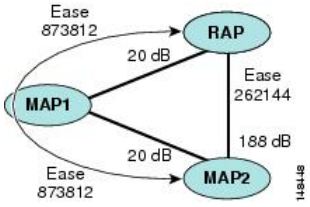
親メッシュ アクセス ポイントは、RAP に戻る最適なパスを提供します。AWPP は、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

容易度の計算

容易度は、各ネイバーの SNR とホップの値を使用し、さまざまな SNR しきい値に基づく乗数を適用して計算します。この乗数には、Spreading 機能を、さまざまなリンクの質に影響する SNR に適用するという意味があります。

図 8：親パスの選択，（19 ページ） では、親パスの選択で、MAP2 は MAP1 を通るパスを選択します。このパスを通る調整された容易度の値（436906）が、MAP2 から RAP に直接進むパスの容易度の値（262144）より大きいためです。

図 *8*：親パスの選択



親の決定

親メッシュ アクセス ポイントは、各ネイバーの容易度を RAP までのホップ カウントで割り算した、調整された容易度を使用して選択されます。

調整された容易度 = 最小値（各ホップでの容易度）ホップ カウント

SNR スムージング

WLANルーティングの難しいところは、RFのエフェメラルな性質です。最適なパスを分析して、パス内で変更がいつ必要かを決めるときに、この点を考慮しなければなりません。特定の RF リンクのSNRは、刻一刻と大幅に変化する可能性があり、これらの変動に基づいてルートパスを変更すると、ネットワークが不安定になり、パフォーマンスが深刻に低下します。基本的なSNRを効果的にキャプチャしながらも経時変動を除去するため、調整されたSNRを提供するスムージング機能が適用されます。

現在の親に対する潜在的なネイバーを評価するとき、親間のピンポン効果を減少させるため、親の計算された容易度に加えて、親に20%のボーナス容易度が与えられます。子がスイッチを作成するには、潜在的な親の方が著しくよくなければなりません。親スイッチングはCAPWAPおよびその他の高レイヤの機能に透過的です。

ループの防止

ルーティングループが作成されないようにするため、AWPPは、自分のMACアドレスを含むルートをすべて破棄します。つまり、ホップ情報とは別に、ルーティング情報がRAPへの各ホップのMAC アドレスを含むため、メッシュ アクセス ポイントはループするルートを容易に検出して破棄できます。

第 2 章

メッシュ導入モード

この章では、メッシュ導入モードについて説明します。内容は次のとおりです。

ワイヤレス メッシュ ネットワーク

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

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

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

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

（注） CAPWAP 経由での CAPWAP はサポートされません。

無線バックホール

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

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

ユニバーサル アクセス

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

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

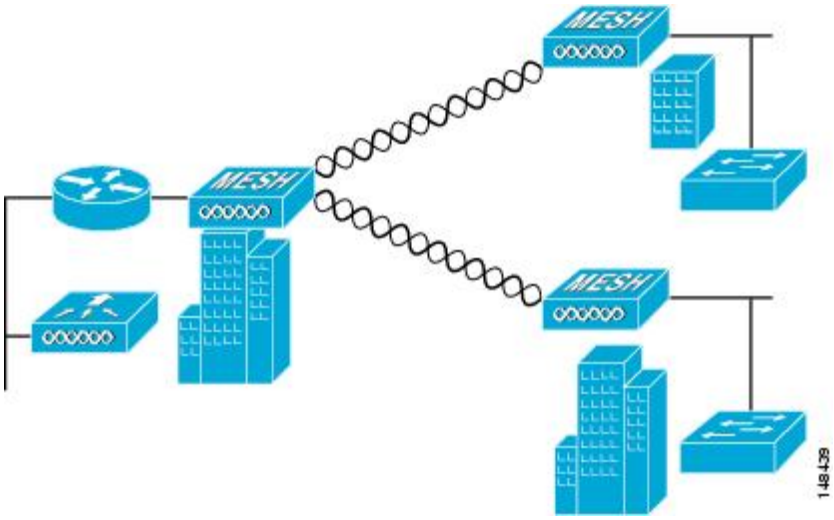
ポイントツーマルチポイント無線ブリッジング

ポイントツーマルチポイント ブリッジング シナリオでは、ルート ブリッジとして機能する RAP が、アソシエートされた有線 LAN を使用して複数の MAP を非ルート ブリッジとして接続します。デフォルトでは、この機能はすべての MAP に対して無効になっています。イーサネット ブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネット ブリッジングをイネーブルにする必要があります。

次の図は、1 つの RAP と 2 つの MAP がある単純な導入を示していますが、この構成は基本的に WLAN クライアントがないワイヤレス メッシュです。イーサネット ブリッジングを有効にする

ことでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアント アクセスに適していないことがあります。

図 *9*：ポイントツーマルチポイント ブリッジングの例



ポイントツーポイント無線ブリッジング

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

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

図 *10*：ポイントツーポイント ブリッジングの例

セキュリティ上の理由により、デフォルトでは MAP のイーサネット ポートは無効になっています。有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定する必要があります。コントローラの GUI を使用してイーサネット ブリッジングを有効にするには、[Wireless] > [All APs] > [Details for the AP] ページの順に選択し、[Mesh] タブをクリックして、[Ethernet Bridging] チェックボックスを選択します。

（注） バックホール無線の全体的なスループットはメッシュ ツリーの各ホップの半分になります。イーサネット ブリッジング対象のクライアントが MAP で使用され、大量のトラフィックが通過する際、スループット消費が高くなり、ダウンリンク MAP がスループット スタベーションによってネットワークから引き離される可能性があります。

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

メッシュ ノードをブリッジとして使用する場合。

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

該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP 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。

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

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

レンジ：150 ～ 132,000 フィート

デフォルト：12,000 フィート

メッシュ レンジの設定（CLI）

- ブリッジングを実行するノード間の距離を設定するには、**config mesh range** コマンドを入力します。
  レンジの指定後に、AP はリブートされます。

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

すべてのアクセス ポイントの範囲カルキュレータ：http://173.37.206.125/aspnet_client/system_web/2_0_50727/WNG_Coverage_Capacity_Calculator_V2.0_HTML/WNG_Coverage_Capacity_Calculator_V2.0.htm

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

第 3 章

デザインの考慮事項

この章では、設計上の重要な考慮事項について説明し、ワイヤレス メッシュの設計例を示します。

屋外のワイヤレス メッシュの導入はそれぞれが独自のため、利用できる場所や障害物、利用可能なネットワーク インフラストラクチャに伴い、環境ごとに課題が異なります。主要な設計要件には、想定されるユーザ、トラフィック、および可用性のニーズによって決まる設計基準もあります。この章の内容は、次のとおりです。

無線メッシュの制約

ワイヤレス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べきシステムの特徴は次のとおりです。これらの一部の特徴はバックホール ネットワークの設計に適用され、残りの特徴はCAPWAP コントローラの設計に適用されます。

ワイヤレス バックホール データ レート

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作成するために使用されます。バックホールインターフェイスはアクセス ポイントによって、802.11a/n/ac/g になります。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推測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延長できます。結果として、データ レートはセル カバレッジと必要なアクセス 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。

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。

（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。

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 1 に示します。

表 *2*：バックホールのデータ レートと *LinkSNR* の最小要件

802.11a データ レート（Mbps）	必要な最小 LinkSNR（dB）
54	31
48	29
36	26
24	22
18	18
12	16
9	15
6	14

- LinkSNR の必要最小値は、データ レートと次の公式で決まります：最小 *SNR* + フェードマージン。

  表 2 に、データ レート別の計算をまとめています。

  - 最小 SNR は、干渉とノイズがなく、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における値です。
  - 一般的なフェード マージンは約 9 ～ 10 dB です。

データ レート別の必要最小 LinkSNR の計算

表 *3*：*802.11n* のバックホール データ レートと最小 *LinkSNR* 要件

802.11n データ レート（Mbps）	空間ストリーム	必要な最小 LinkSNR（dB）
15	1	9.3
30	1	11.3
45	1	13.3
60	1	17.3
90	1	21.3
120	1	24.3
135	1	26.3
157.5	1	27.3
30	2	12.3
60	2	14.3
90	2	16.3
120	2	20.3
180	2	24.3
240	2	27.3
270	2	29.3
300	2	30.3

- 必要最小 LinkSNR を計算するために MRC の影響を考慮した場合。 表 3 は、3 本の Rx アンテナ（MRC ゲイン）を使用した AP1552 および 1522 の 802.11a/g（2.4 GHz および 5 GHz）に必要な LinkSNR を示します。

  LinkSNR = 最小 SNR - MRC + フェード マージン（9 dB）

表 *4*：*802.11a/g* に必要な *LinkSNR* の計算

802.11a/g MCS（Mbps）	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェード マージン（dB）	必要リンク SNR（dB）
6	BPSK 1/2	5	4.7	9	9.3
9	BPSK 3/4	6	4.7	9	10.3
12	QPSK 1/2	7	4.7	9	11.3
18	QPSK 3/4	9	4.7	9	13.3
24	16QAM 1/2	13	4.7	9	17.3
36	16QAM 3/4	17	4.7	9	21.3
48	64QAM 2/3	20	4.7	9	24.3
54	64QAM 3/4	22	4.7	9	26.3

表 4 に、802.11n のレートだけを考慮する場合の 2.4 および 5 GHz の AP1552 の LinkSNR 要件を示します。

表 *5*：*2.4* および *5 GHz* での *AP1552* の *LinkSNR* 要件

空間ストリーム数	11n MCS	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェードマージン（dB）	リンク SNR (dB)
1	MCS 0	BPSK 1/2	5	4.7	9	9.3
1	MCS 1	QPSK 1/2	7	4.7	9	11.3
1	MCS 2	QPSK 3/4	9	4.7	9	13.3
1	MCS 3	16QAM 1/2	13	4.7	9	17.3
1	MCS 4	16QAM 3/4	17	4.7	9	21.3
1	MCS 5	64QAM 2/3	20	4.7	9	24.3
1	MCS 6	64QAM 3/4	22	4.7	9	26.3
1	MCS 7	64QAM 5/6	23	4.7	9	27.3
2	MCS 8	BPSK 1/2	5	1.7	9	12.3

空間ストリーム数	11n MCS	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェードマージン（dB）	リンク SNR (dB)
2	MCS 9	QPSK 1/2	7	1.7	9	14.3
2	MCS 10	QPSK 3/4	9	1.7	9	16.3
2	MCS 11	16QAM 1/2	13	1.7	9	20.3
2	MCS 12	16QAM 3/4	17	1.7	9	24.3
2	MCS 13	64QAM 2/3	20	1.7	9	27.3
2	MCS 14	64QAM 3/4	22	1.7	9	29.3
2	MCS 15	64QAM 5/6	23	1.7	9	30.3

（注） 2 つの空間ストリームの場合、MRC ゲインは半分になります。つまり、MRC ゲインは 3 dB 少なくなります。これは、システムに 10 ログ（3/1 SS）ではなく 10 ログ（3/2 SS）があるためです。3 つの受信器で 3 SS がある場合は、MRC ゲインがゼロになります。

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

  ホップ数は 3 か 4 に制限して、主に、十分なバックホール スループットを維持することをお勧めします。これは、各メッシュ アクセス ポイントはバックホール トラフィックの伝送と受信に同じ無線を使用するためです（つまり、スループットはホップごとに約半分になります）。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 4 Mbps 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、現在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 に数を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るメッシュ アクセス ポイントの数。

コントローラの計画

次の項目は、メッシュ ネットワークに必要なコントローラの数に影響します。

- ネットワーク内のメッシュ アクセス ポイント（RAP および MAP）。

  RAP とコントローラを接続する有線ネットワークは、そのネットワーク内でサポートされるアクセス ポイントの総数に影響を与えることがあります。このネットワークによって、コントローラが、WLAN のパフォーマンスに影響なく、すべてのアクセス ポイントから利用できるようになっている場合、アクセス ポイントはすべてのコントローラにわたって最大の効率で等しく分散できます。これに当てはまらない場合で、コントローラがさまざまなクラスタまたは PoP にグループ化されるとき、アクセス ポイントの総数とカバレッジは減少します。

- コントローラごとにサポートされるメッシュ アクセス ポイント（RAP および MAP）の数。表 1を参照してください。

  本書では、わかりやすくするために非メッシュ アクセス ポイントを、ローカル アクセス ポイントと呼びます。

表 *6*：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）[3]	最大 メッシュ AP サポート
5508[4]	500	500
2504[5]	75	75
WiSM2	500	500
5520	1500	1500
8540	6000	6000

3 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 の総数です。
4 5508 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。
5 2504 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。

http://www.cisco.com/c/dam/assets/prod/wireless/cisco-wireless-products-comparison-tool/index.html#/

（注） メッシュは、Cisco 5508 コントローラで完全にサポートされています。The屋内および屋外 AP には基本ライセンス（LIC-CT508-Base）で十分です。TheWPlus ライセンス（LIC-WPLUS-SW）は、基本ライセンスに含まれます。屋内メッシュ AP には WPlus ライセンスは必要ありません。

第 4 章

メッシュ導入リリース8.4のAir Time Fairness

メッシュ導入リリース 8.4 の Air Time Fairness

このセクションでは、メッシュ AP の ATF を紹介し、その導入ガイドラインを提供します。このセクションでは、次のことを目的としています。

- メッシュ AP での ATF の概要を提供する
- サポートされている主要機能を強調する
- メッシュ AP での ATF 導入および管理についての詳細を提供する

前提条件と 8.4 リリースでサポートされる機能

メッシュ ATF は、ワイヤレス LAN コントローラ上の AireOS 8.4 以降のリリースでサポートされます。次の AP でメッシュ ATF がサポートされます。

AP	1550（64 MB）	1550（128 MB）	1570	3700	1530	1560
機能	–	–	—	–	–	–
基本メッシュ	Yes	Yes	Yes	Yes	Yes	8.4
Flex+メッシュ	Yes	Yes	Yes	Yes	Yes	×

AP	1550（64 MB）	1550（128 MB）	1570	3700	1530	1560
高速コンバージェンス（バックグラウンドのスキャン）	×	8.3	8.3	Yes	8.3	8.4
RAP の有線クライアント	Yes	Yes	Yes	No	Yes	No
MAP の有線クライアント	Yes	Yes	Yes	No	Yes	8.4
デイジーチェーン	7.6	7.6	7.6	×	7.6	×
LSC	Yes	Yes	Yes	Yes	Yes	No
PSK のプロビジョニング：MAP-RAP 認証	8.2	8.2	8.2	8.2	8.2	8.4
メッシュの ATF	×	8.4	8.4	8.4	×	8.4

Cisco Air Time Fairness （ATF）の使用例

公共ホットスポット（スタジアム/空港/会議場/その他）

この場合、パブリック ネットワークは 2 つ（またはそれ以上）のサービス プロバイダーと施設間で WLAN を共有しています。各サービス プロバイダーに対するサブスクライバをグループ化して、各グループに特定の割合の通信時間を割り当てることができます。

教育機関

この場合、大学は、学生、教員、およびゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービス プロバイダーによってさらに分割できます。各グループに特定の割合の通信時間を割り当てることができます。

一般企業、サービス業、小売業

この場合、施設は、従業員とゲスト間でWLANを共有しています。ゲストネットワークは、サービス プロバイダーによってさらに分割できます。ゲストは、通信時間の特定の割合を割り当てられている各サブグループがあるサービスの種類のレイヤによってグループ化できます。たとえば、有料のグループは、無料のグループより多くの通信時間が与えられます。

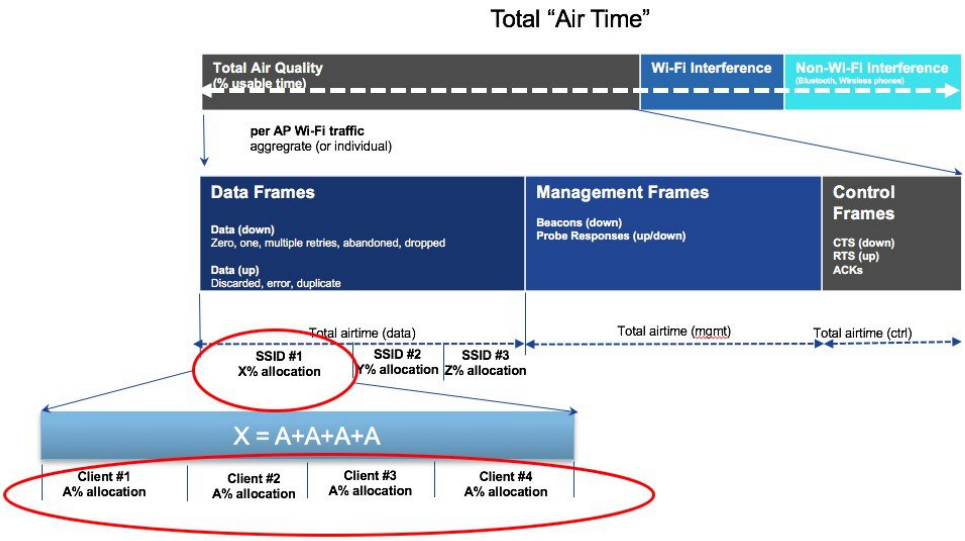
時間を共有する管理型ホットスポット

この場合、サービス プロバイダーまたは企業など、ホットスポットを管理するビジネス主体は、割り当てた後に通信時間をその他のビジネス主体にリースできます。

ATF 機能

ATF 機能：

- ATF ポリシーはダウンリンク方向（AP がクライアントにフレームを送信）にのみ適用されます。ダウンリンク、つまりAPからクライアント方向の通信時間のみが、APによって正確に制御されます。アップリンク方向、つまり、クライアントから AP への通信時間は測定できますが、厳密に制御することはできません。AP は、クライアントに送信するパケットの通信時間を抑制できますが、それぞれの通信時間を制限できないため、クライアントから「聞ける」パケットの通信時間のみを測定できます。
- ATF ポリシーはワイヤレス データ フレームにのみ適用されます。管理および制御フレームは無視されます。
- ATF が SSID ごとに設定される場合、各 SSID は設定されたポリシーに従って通信時間が許可されます。
- ATF は、通信時間ポリシーを超えるフレームをドロップするか保留するように設定できます。フレームが保留されると、問題となっている SSID に十分な通信時間が割り当てられた時点でバッファされて送信されます。もちろん、何フレームをバッファできるかについての制限があります。この制限を超えた場合、フレームがドロップされます。
- ATF はグローバルに有効または無効にすることができます。
- ATF は個々のアクセス ポイント、AP グループまたはネットワーク全体で有効または無効にすることができます。
- 割り当ては、SSID およびクライアントごとに適用されます。
- ダウンストリームだけに適用されます。
- WLC GUI/CLI および PI で設定できます。
- AP グループに対するネットワーク内のすべての AP または 1 つの AP に適用できます。
- 次のローカル モードの AP でサポートされています：**AP1260、1550-128Mb 1560 1570 1700、2600、2700、3500、3600、3700**。



メッシュの ATF 機能の概要

メッシュ AP の AirTime Fairness 機能は、以前のリリースにおけるローカル AP の ATF 機能サポートリリースと概念がよく似ています。次のガイドで機能と導入手順について確認することを強くお勧めします。 http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Air_Time_Fairness_Phase1_and_Phase2_Deployment_Guide.html

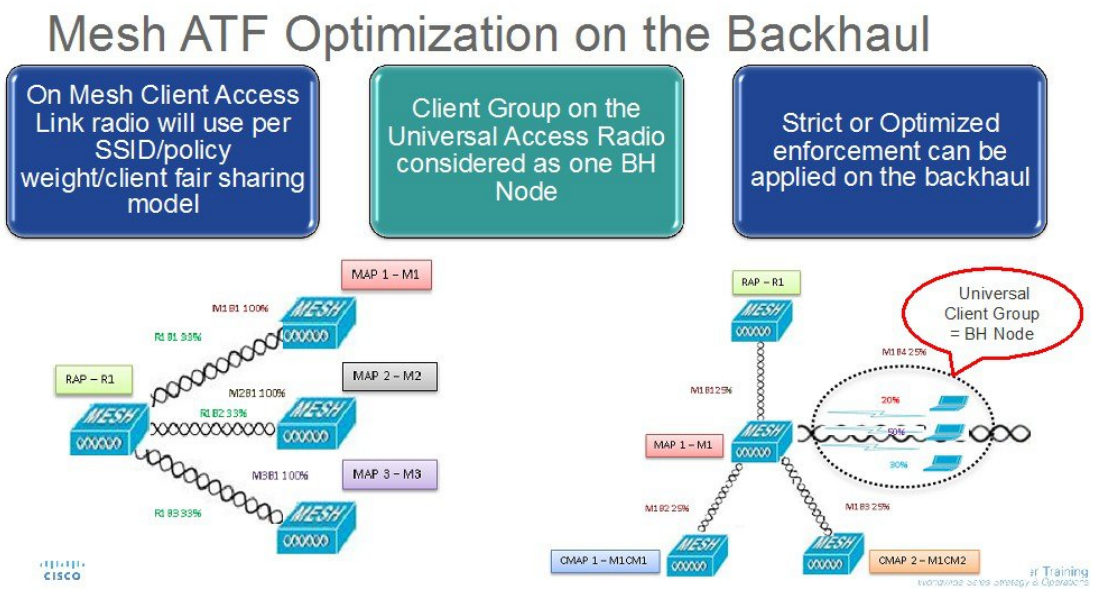
現在、Cisco IOS 11n および 11ac 屋内向け AP を配備したエンタープライズ、高密度スタジアム、およびその他の主要な Wi-Fi 導入では、8.1 MR1 および 8.2 リリースの「SSID ごと」の Airtime Fairness と、「SSID内のクライアントごと」の Airtime Fairness によってメリットが得られます。

同様に、現在、大規模な屋外ワイヤレス メッシュを導入している顧客から、AP の無線通信時間ダウンストリームの利用時に、屋外ワイヤレス メッシュ ネットワーク全体で Wi-Fi ユーザに公平性を提供して対応し、しかも屋外ワイヤレス メッシュ ネットワーク全体の Wi-Fi ユーザに（Wi-Fi ホットスポットを通じた複数のセルラー事業者が暗黙の対象）SLA を適用する重要な制御能力を管理者に提供できるようにしてほしいという声が上がっています。しかし、すべての Wi-Fi ユーザのトラフィックはワイヤレス バックホール無線により MAP と RAP 間でつながり、各バックホール ノードの SSID によってポリシーを適用するバックホール ノードのためのワイヤレス バックホール無線に関する SSID の概念が存在しないため、屋外ワイヤレス メッシュ AP により Wi-Fi の通信時間を利用するという点においては、屋外ワイヤレス メッシュ ネットワーク全体の Wi-Fi ユーザを公平に扱うための簡単なソリューションは存在しません。Client Access の無線のクライアントに関する限り、Cisco のローカル モード AP で処理される方法と同様に、（Client Fair Sharing あるなしに関わらず）SSID を通じて通信時間の公平性を調整することは非常に簡単です。

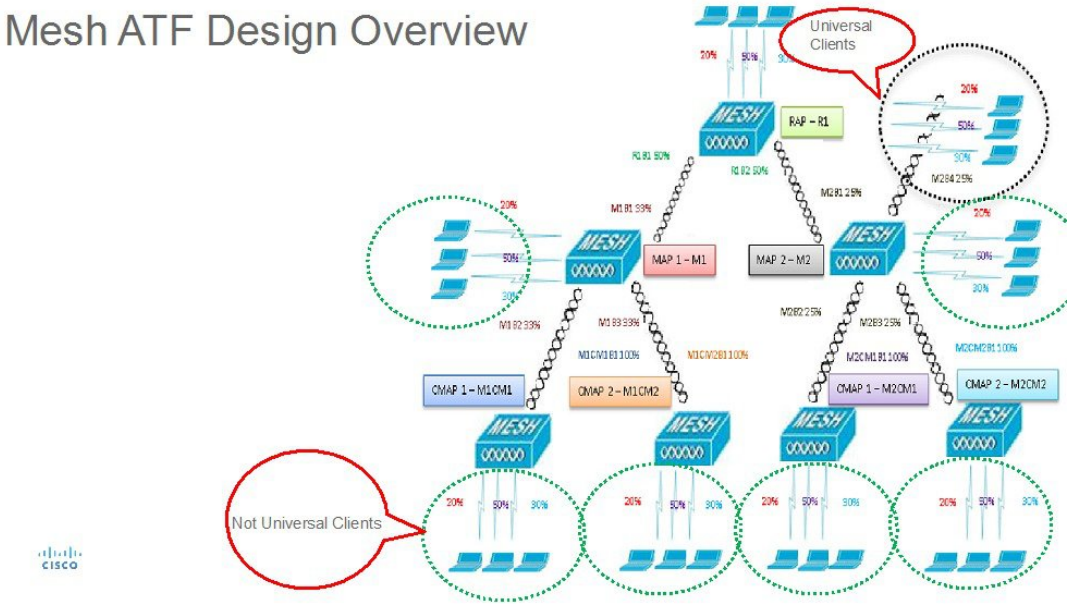
メッシュでの ATF をサポートするソリューションの概要を説明する前に、ATF について要約しておきましょう。Airtime Fairness（ATF）とは基本的に、SSID によって接続したクライアントに対して、ダウンストリーム方向の AP 無線通信時間を調整/適用する能力を提供するための概念です。結果として、ワイヤレス ネットワークの Wi-Fi ユーザは、無線通信時間を利用するという点にお

いて公平に扱われます。基本的には、これによってSLAを追加で適用するか、または単に特定のグループや特定のユーザがある特定のAP無線上でWiFiの通信時間を不公平に独占することを回避するための重要な制御が提供されます。サービス レベル契約（SLA）とは、サービス プロバイダーに期待されるサービス レベルを定義した、（内部または外部のいずれかの）サービスプロバイダーとエンドユーザ間の契約です。SLA は、顧客が受けるサービスを定義するのが目的であるということから、アウトプット ベースと言えます。

一般に、メッシュ アーキテクチャでは、メッシュ ツリーのメッシュ AP（親/子 MAP）は、親と子のMAP間のメッシュ接続用のバックホール無線上で、同じチャネルにアクセスします（ひとまず、拡張サブバックホール無線については忘れましょう）。一方、ルート AP はコントローラに有線接続され、MAPはコントローラに無線接続されます。そのため、すべてのCAPWAPやWi-Fiのトラフィックは、ワイヤレス バックホール無線およびRAPによりコントローラに接続されます。物理的な場所という点で、通常の場合RAPはルーフ トップに配置され、複数のホップにあるMAPは、メッシュ ネットワークのセグメント化のガイドラインに基づいて、互いに間隔を置いて配置されます。そのため、メッシュ ツリー内の各MAPは、各MAPが同じメディアにアクセスするにも関わらず、自身の無線通信時間ダウンストリームの 100% をユーザに提供できます。これを非メッシュのシナリオで比較しましょう。アリーナでは、互いに隣り合わせの異なる部屋に存在するネイバーのローカル モード AP が、同じチャンネル上でそれぞれのクライアントにサービスを提供して、それぞれが 100% の無線通信時間のダウンストリームを提供することが考えられます。したがって、ATF は同じメディアにアクセスする 2 つのネイバー AP で適用されるクライアントを制御しません。同様に、メッシュ ツリーのMAPには適用可能です。屋外・屋内メッシュ AP では、Airtime Fairness は、ATF が現在非メッシュ ローカル・モード AP 上でサポートされクライアントにサービスを実行しているように、通常のクライアントにサービスする Client Access 無線上でサポートされなければなりません。さらに、Client Access 無線上のクライアントへの、またはクライアントからのトラフィックを RAP へ接続する（1 ホップ）、または MAP から RAP へ接続する（複数ホップ）バックホール無線においてもサポートされなければなりません。同じSSID/ポリシー/ウェイト/Client Fair Sharing モデルを使用しているバックホール無線で ATF をサポートするのはやや微妙と言えます。バックホール無線にはSSIDがないため、常に隠れたバックホール ノードによってトラフィックを接続します。その後、RAP または MAP のバックホール無線では、無線通信時間ダウンストリームはバックホール ノードの数に基づいて等しく公平に共有されます。このアプローチは問題を取り除き、2 番目のホップ MAP に接続するクライアントが 1 番目のホップ MAP に関連するクライアントを止めたり、MAP の Wi-Fi ユーザが物理的な位置で分離されているものの、2 番目のホップ MAP がバックホール無線によって 1 番目のホップ MAP に接続したりする場合に、ワイヤレス メッシュ ネットワーク全体のユーザに公平性を提供します。このシナリオでは、バックホール無線が一般的な Client Access 機能を通じて通常のクライアントにサービスを実行するオプションを備えている場合、ATF は通常のクライアントを単一ノードとみなし、それらをグループ化します。ノードの数（バックホール ノード+通常のクライアントに対する単一ノード）に基づいて、無線通信時間ダウンストリームを等しく公平に共有することによって、通信時間が適用されます。次のセクションでは、このソリューションを設計に組み込む方法についての詳細を説明します。



より大きなメッシュ設計はこのようになります。



ATF の動作モード

ATF モニタ モードにより、ユーザは、使用される全体的な通信時間の統計情報を表示して取得、すなわち、すべての AP 送信における通信時間の使用を報告できるようになります。モニタ モードの ATF は、次のレベルで有効にできます。

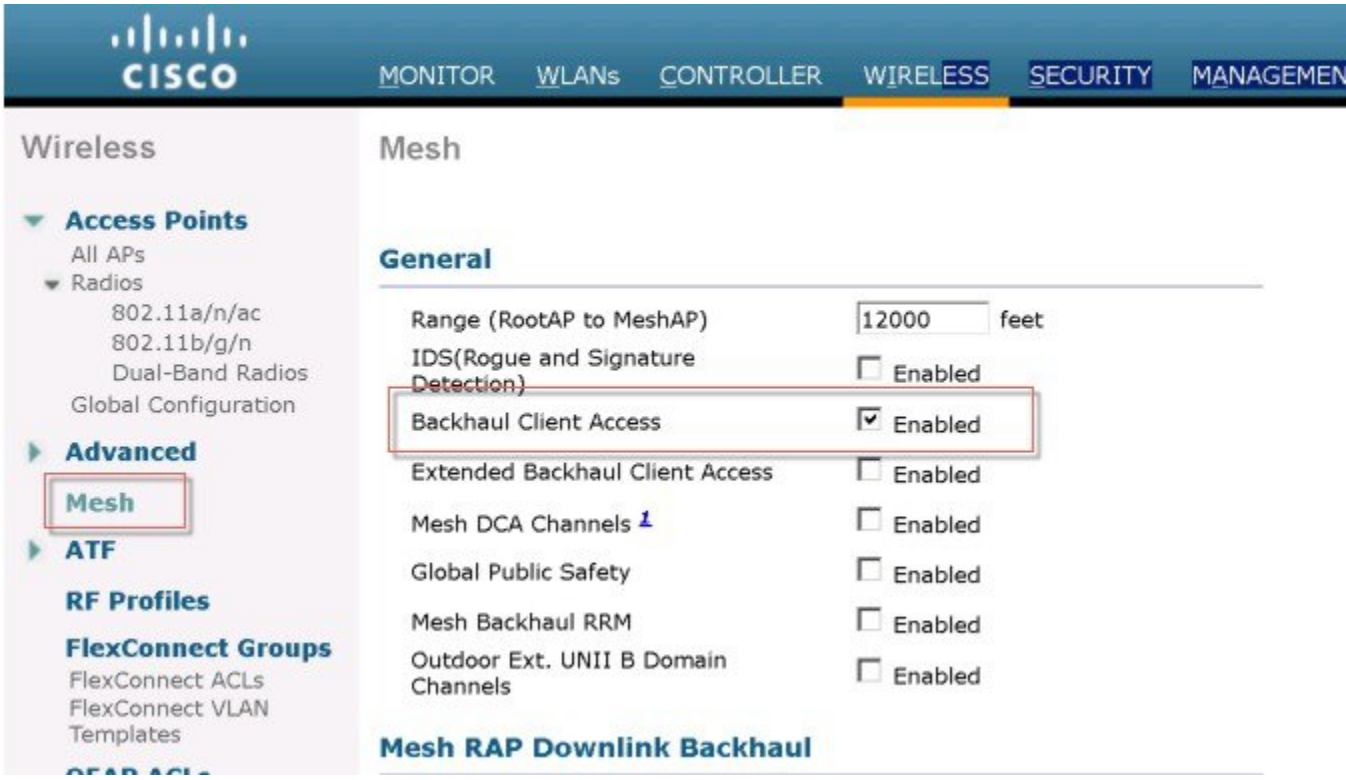
- 無効モード：デフォルトでは、ATF は WLC で無効
- モニタ モード：ネットワークの通信時間の使用状況を監視する
- 適用：ポリシー モード：ネットワークの ATF ポリシーを割り当てる
- 厳密な適用
- 最適化

メッシュの ATF の設定

メッシュの ATF を設定するには、次の手順を実行します。

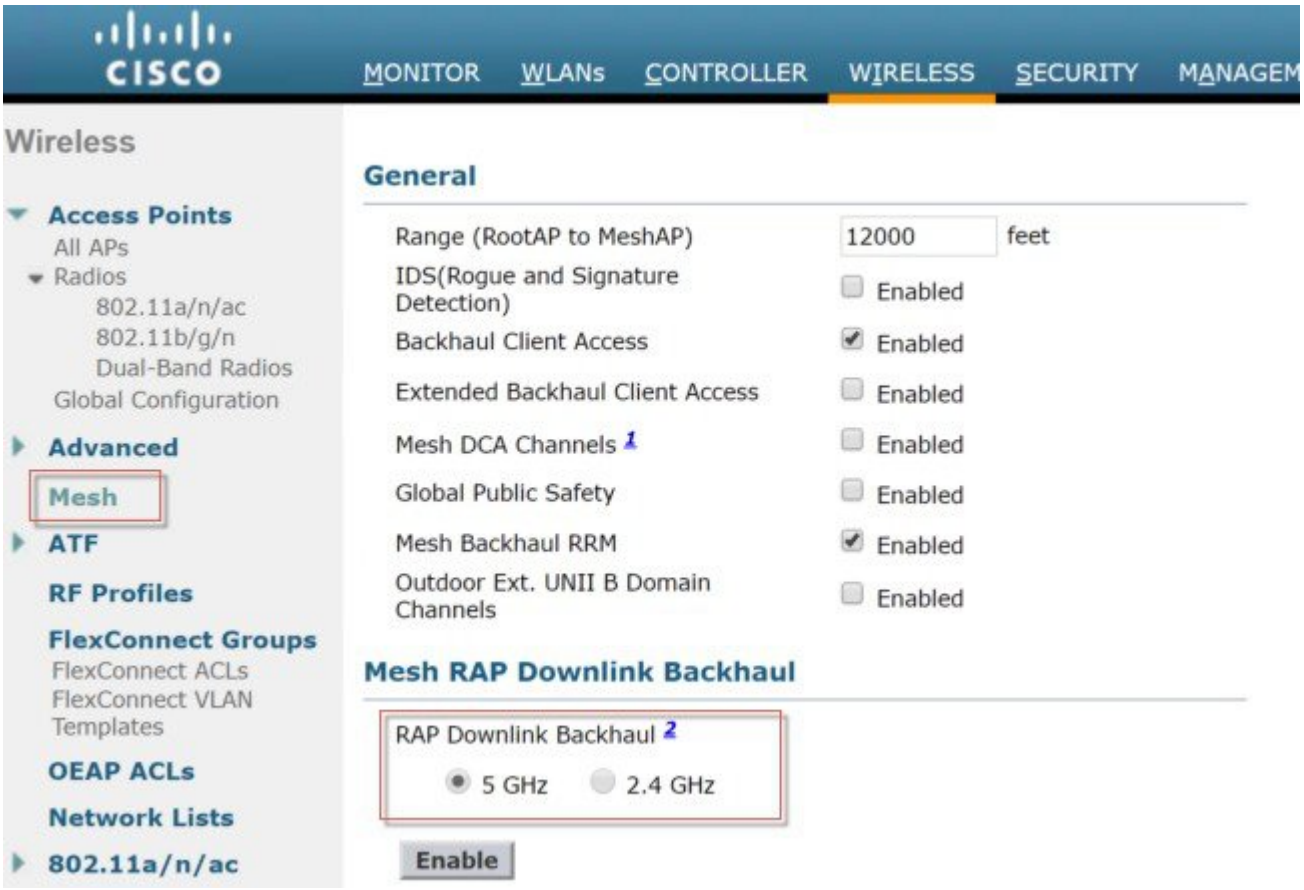
ステップ 1 [Backhaul Client Access] を有効または無効に設定します。

```
(5520-MA1) >config mesh client-access enable
```



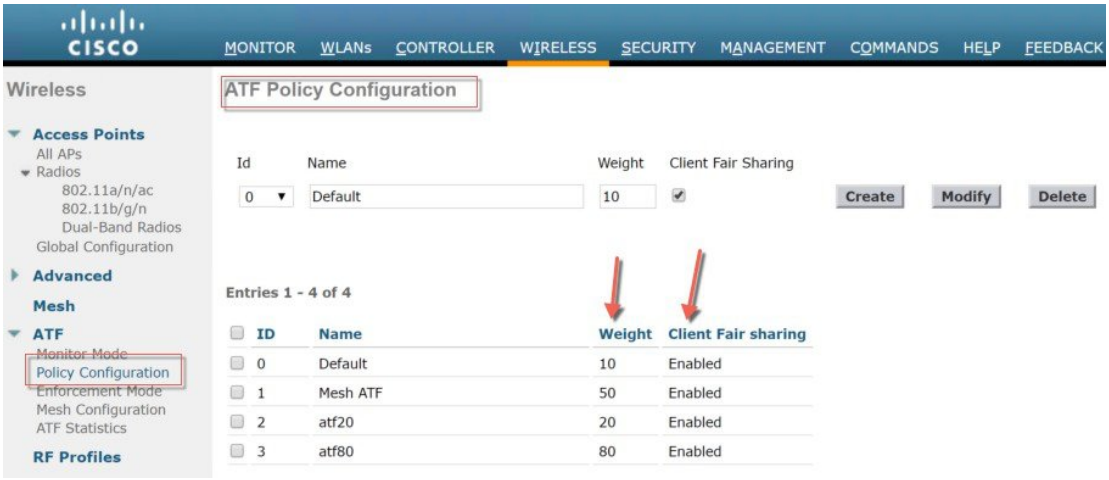
ステップ 2 [RAP Downlink Backhaul] を、[5 Ghz] または [2.4 Ghz] に設定します。

```
(5520-MA1) >config mesh backhaul slot <0/1> all
```



ステップ 3 [ATF Policy] の [Weight] と [Client Sharing] を設定します

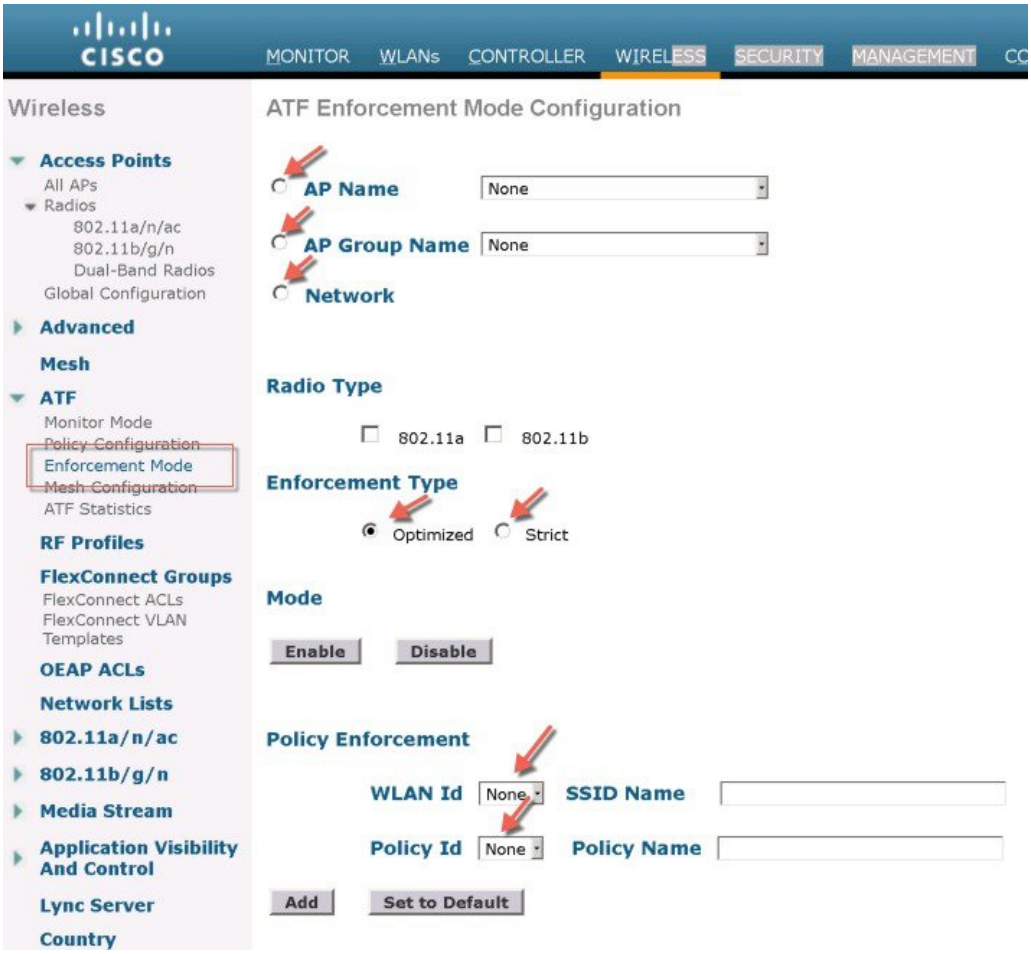
```
(5520-MA1) >config atf 802.11a mode ?

disable         Disables ATF
enforce-policy Configures ATF in enforcement mode
monitor         Configures ATF in monitor mode

(5520-MA1) >config atf 802.11a mode enforce-policy


(5520-MA1) >config atf policy create 1 mesh 25 client-sharing enable
```



ステップ 4 [Enforcement Mode] の [AP]、[AP Group]、[Network] と [Enforcement Type] を設定し、[WLAN] と [Policy] を適用します。

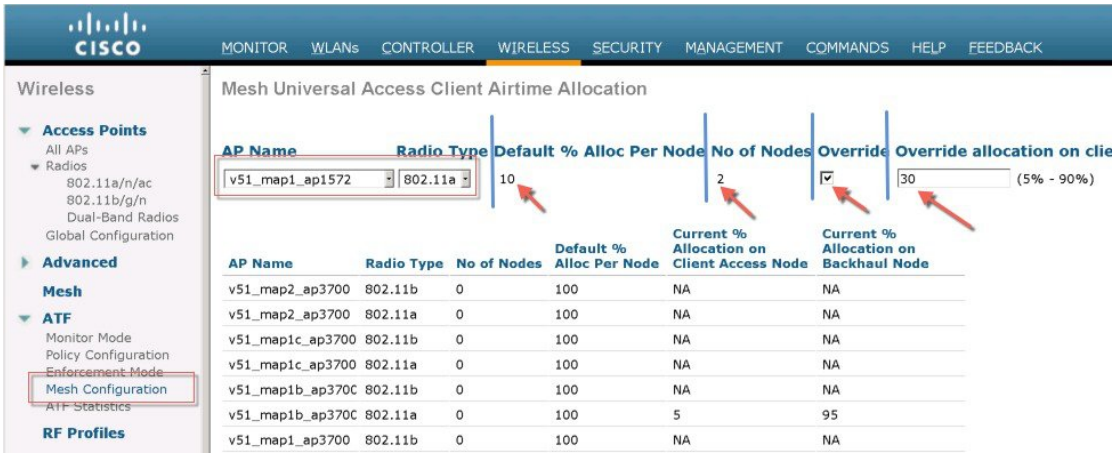
図 *11* :

```
(5520-MA1) >config atf 802.11a optimization enable
```



ステップ 5 [Mesh Universal Access Client Airtime Allocation] を設定します。

```
> config ap atf 802.11a client-access airtime-allocation <5 - 90> <ap-name> override enable
/disable
> config ap atf 802.11b client-access airtime-allocation <5 - 90> <ap-name> override enable/disable
```


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless
Access Points
All APs
Radios
802.11a/n/ac
802.11b/g/n
Dual-Band Radios
Global Configuration
Advanced
Mesh
ATF
Monitor Mode
Policy Configuration
Enforcement Mode
Mesh Configuration
ATF Statistics
RF Profiles
Mesh Universal Access Client Airtime Allocation
AP Name
Radio Type
Default % Alloc Per Node
No of Nodes
Override
Override allocation on clie
v51_map1_ap1572
802.11a
10
2
30
(5% - 90%)
AP Name
Radio Type
No of Nodes
Default % Alloc Per Node
Current % Allocation on Client Access Node
Current % Allocation on Backhaul Node
v51_map2_ap3700 802.11b 0 100 NA NA
v51_map2_ap3700 802.11a 0 100 NA NA
v51_map1c_ap3700 802.11b 0 100 NA NA
v51_map1c_ap3700 802.11a 0 100 NA NA
v51_map1b_ap370C 802.11b 0 100 NA NA
v51_map1b_ap370C 802.11a 0 100 5 95
v51_map1_ap3700 802.11b 0 100 NA NA

第 5 章

サイトの準備と計画

この章では、メッシュ ネットワークのサイト準備と計画について説明します。内容は次のとおりです。

サイトの調査

機器を設置する前に、無線サイトの調査を推奨します。サイトの調査では、干渉、フレネル ゾーン、または物流の問題などの問題を明らかにします。適切なサイト調査には、メッシュ リンクの一時的なセットアップや、アンテナの計算が正確かどうかを判別する測定などが含まれます。穴を開けたり、ケーブルを設置したり、機器を取り付けたりする前に、それが正しい場所かどうかを確認します。

（注） 電源が準備できていないときは、Unrestricted Power Supply（UPS）を使用してメッシュ リンクに一時的に電源を入れることを推奨します。

調査前チェックリスト

サイト調査の前に、次のことを確認します。

- ワイヤレス リンクの長さはどのくらいか?
- ライン オブ サイトはクリアか?
- リンクが稼働する最小の許容データ レートは?
- これは、ポイントツーポイントのリンクか、ポイントツーマルチポイントのリンクか?

- 正しいアンテナがあるか?
- アクセス ポイントの設置場所は、アクセス ポイントの重量を支えられるか?
- 両方のメッシュ サイトの場所にアクセスできるか?
- （必要であれば）適切な権限はあるか?
- パートナーはいるか?屋根や塔の上では、単独では決して調査や作業を行わないでください。
- オンサイトに出向く前に1500シリーズを設定したか?設定やデバイスの問題を先に解決しておくと、作業は常に楽になります。
- 作業を遂行するための適切なツールや機器があるか?

（注） 調査を行うときには、携帯電話や携帯の送受信兼用無線機があると便利です。

屋外サイトの調査

WLANシステムを屋外に設置するのは、屋内にワイヤレスを配置する場合とは異なるスキルセットが必要です。天候による災害、雷、物理的セキュリティ、その地域の規制などを考慮に入れなければなりません。

メッシュ リンクの適合が成功するかどうかを判別する際には、そのメッシュ リンクに対し、どの無線データ レートでどのくらい遠くまでの伝送を期待しているのかを定義してください。ワイヤレス ルーティングの計算にはデータ レートが直接は含まれないため、同じメッシュ全体を通して同じデータ レートを使用することを推奨します。

メッシュ リンクの設計には、次の値を推奨します。

- MAP の配置について、街路の上では、高さ 35 フィートを超えられません。
- MAP は、地面に向かって下向きに取り付けられたアンテナと一緒に配置されます。
- 一般的な 5 GHz の RAP から MAP までの距離は、1000 ～ 4000 フィートです。
- RAP は、一般的には塔か高い建物に設置します。
- 一般的な 5 GHz の MAP から MAP までの距離は、500 ～ 1000 フィートです。
- MAP は、一般的には低い建物の上か街灯に設置します。
- 一般的な 2.4 GHz の MAP からクライアントまでの距離は、500 ～ 1000 フィートです（アクセス ポイントのタイプによって異なります）。
- クライアントは、一般的にはラップトップ、スマートフォン、タブレット、CPE です。ほとんどのクライアントは 2.4 GHz 帯域で動作します。
- リリース 8.2 以降、2.4 GHz 無線をバックホールに使用でき、若干長い距離を実現できます。ただし、同時にスループットが低下する可能性があります。

ライン オブ サイトの判別

リンクが成功するかどうかを判別する際には、そのリンクに対し、どの無線データ レートでどのくらい遠くまでの伝送を期待しているのかを定義する必要があります。非常に近い、1 キロメートル以内のリンクは、クリアなライン オブ サイト（*LOS*）（障害物のないパス）があれば容易に到達できます。

メッシュ電波は 5 GHz 帯域で非常に高い周波数であるため電波波長が小さく、電力が同じであれば、低い周波数の電波ほど電波は遠くへ行きません。この高い周波数範囲によって、メッシュはライセンス不要の使用に対して理想的なものになっています。高ゲイン アンテナを使用して電波を特定の方向にしっかり電波を向かせない限り、電波が遠くまで届かないためです。

この高ゲイン アンテナ設定は、RAP を MAP に接続する場合にだけ推奨します。メッシュ リンクが 1 マイル（1.6 km）に限定されているため、メッシュの動作を最適化するのに、全方向性アンテナが使用されます。地球の屈曲は 9.6 km（6 マイル）ごとに変化するため、ライン オブ サイトの計算には影響しません。

天候

フリー スペース パスのロスとライン オブ サイトの他に、天候によってもメッシュ リンクの質は低下する場合があります。雨、雪、霧、多湿条件はライン オブ サイトに若干の障害となったり影響を与えたりし、メッシュ リンクにはほとんど影響しないような小さなロスをもたらします（レイン フェードやフェード マージンと呼ばれることもあります）。安定したメッシュ リンクを確立したのであれば、天候が問題になることはありませんが、リンクが開始できないほど弱い場合は、悪天候でパフォーマンスが低下したりリンクのロスが引き起こされたりします。

理想的にはライン オブ サイトが必要ですが、何も見えないような吹雪ではライン オブ サイトが認められません。また、嵐で雨や雪が問題になるかもしれない一方、その逆の天気によって別の条件が引き起こされる可能性も多々あります。たとえば、アンテナはおそらくマスト パイプ上にあり、嵐がマスト パイプまたはアンテナ構造に吹き付けていて、その揺れによってリンクが行ったり来たりしたり、アンテナの上に氷や雪の大きな塊ができたりします。

フレネル ゾーン

フレネル ゾーンは、トランスミッタとレシーバの間の目に見えるライン オブ サイト周辺の虚楕円です。無線信号はフリースペースを通って目的の場所に到達するため、フレネルエリアに障害物を検出して信号の質が低下することがあります。最高のパフォーマンスと範囲は、フレネル エリアに障害物がない場合に達成されます。フレネル ゾーン、フリー スペース ロス、アンテナ ゲイン、ケーブル ロス、データ レート、リンク距離、トランスミッタ電源、レシーバ感度、およびその他の変動要因は、メッシュ リンクがどのくらい遠くまで行くかを判別する役割を持ちます。

図 12：ポイントツーポイント リンクのフレネル ゾーン，（48 ページ） に示すように、フレネル エリアの 60 ～70 パーセントに障害物がなければ、リンクを確立できます。

図 *12*：ポイントツーポイント リンクのフレネル ゾーン

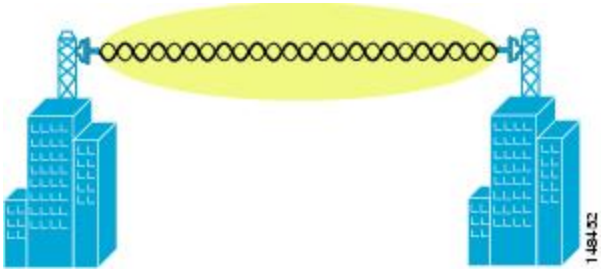
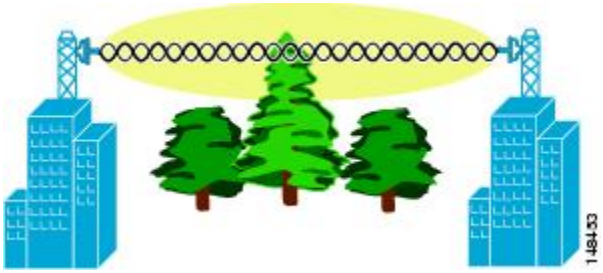


図 13：フレネル ゾーン内の一般的な障害物，（48 ページ） は、障害物のあるフレネル ゾーンを示しています。

図 *13*：フレネル ゾーン内の一般的な障害物



パス沿いの特定の距離におけるフレネル ゾーンの半径（フィート）は、次の方程式で計算できます。

F1 = 72.6 x (d/4 x f) の平方根

値は次のとおりです。

F1 = 最初のフレネル ゾーン半径（フィート）

D = パスの全長（マイル）

F = 周波数（GHz）

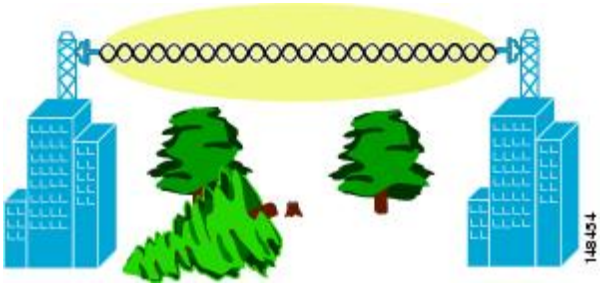
通常、最初のフレネル ゾーンの 60 % のクリアランスが推奨されるため、上の公式を 60 % のフレネル ゾーン クリアランスで表すと、次のようになります。

0.60 F1= 43.3 x (d/4 x f) の平方根

これらの計算は、平坦地に基づいたものです。

図 14：フレネル ゾーンの障害物の除去, （49 ページ） は、ワイヤレス信号のフレネル ゾーンにある障害物の除去を示しています。

図 *14*：フレネル ゾーンの障害物の除去



ワイヤレス メッシュ配置のフレネル ゾーン サイズ

可能な最小周波数 4.9 GHz におけるフレネル ゾーンの最大サイズの概算を求める場合、最小値は周波数ドメインによって異なります。記載している最小の数値は、米国の Public Safety のために割り当てられた使用可能帯域で、1 マイルの最大距離の場合、クリアランス要件のフレネル ゾーンは、9.78 フィート = 43.3 x 平方根 (1/(4*4.9)) です。このクリアランスは、ほとんどのソリューションで比較的簡単に達成できます。たいていの配置では、距離は1マイル（1.6 km）より短く、周波数は 4.9 GHz より大きいと想定され、フレネル ゾーンはより小さくなります。すべてのメッシュ配置では、フレネル ゾーンを設計の一部として考慮する必要がありますが、ほとんどの場合、フレネル クリアランス要件が問題になることはないと考えられます。

隠しノードの干渉

メッシュ バックホールは、そのメッシュ内のすべてのノードに同じ 802.11a チャネルを使用しますが、これによって WLAN バックホール環境に隠しノードができることがあります。

図 *15*：隠しノード

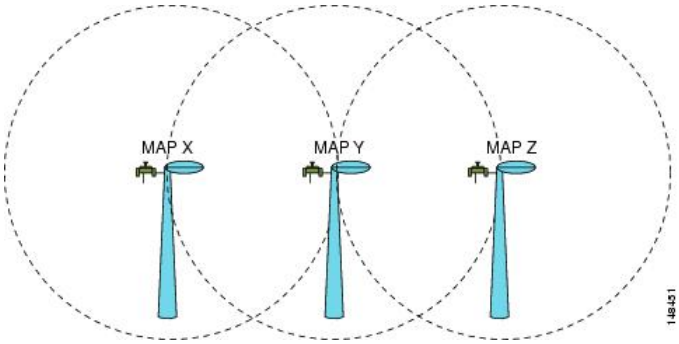


図 15：隠しノード, （49 ページ） は、次の 3 つの MAP を示します。

- MAP X
- MAP Y
- MAP Z

MAP Y と MAP Z にとって、MAP X が RAP に戻るルートの場合、MAP X と MAP Z の両方が同時に MAP Y にトラフィックを送信する可能性があります。RF 環境のため、MAP Y は MAP X と MAP Z の両方からのトラフィックが見えますが、MAP X と MAP Z は互いが見えません。これは、キャリア検知多重アクセス（CSMA）メカニズムでは、MAP X と MAP Z が同じ時間ウィンドウ中に送信するのを止められないことを意味します。これらのフレームのどちらかが 1 つの MAP に向かうと、フレーム間のコリジョンによって破損し、再送信が必要になります。

すべての WLAN で何らかの時点で隠しノード コリジョンが生じる可能性がありますが、MAP の修正された特性によって、重負荷や大きなパケット ストリームなどのトラフィック条件では、隠しノードのコリジョンがメッシュ WLAN バックホールの永続的な機能になります。

メッシュ アクセス ポイントは同じバックホール チャネルを共有するため、隠しノードと露出ノードは、ワイヤレス メッシュ ネットワークに付きものの問題になっています。Cisco メッシュ ソリューションでは、ネットワークのパフォーマンス全体に影響するこれら 2 つの問題を、できるだけ多く探し出して軽減しています。たとえば、AP1500 には少なくとも 2 つの無線があります。1 つは 5 GHz チャネルのバックホール アクセス用で、もう 1 つは、2.4 GHz クライアント アクセス用です。さらに、Radio Resource Management（RRM）機能は、2.4-GHz 無線で動作しますが、これによって、Cell Breathing と自動チャネル変更が可能であり、メッシュ ネットワーク内のコリジョン ドメインを効果的に削減できます。

この他にも、これら 2 つの問題をさらに軽減するためのソリューションがあります。コリジョンを減らして高負荷条件での安定性を向上させるため、802.11 MAC では、コリジョン発生が認識されたときに指数関数バックオフ アルゴリズムが使用され、競合ノードが指数関数的にバックオフしてパケットを再送信します。理論上、ノードが再試行すればするほど、コリジョンの可能性は小さくなります。実際には、競合するステーションが 2 つだけあって、隠しステーションにはなっていなければ、コリジョンはおそらく、ほんの 3 回も再試行するだけで、無視できるものになるでしょう。もっと多くの競合ステーションがある場合には、コリジョンが増加すると考えられます。そのため、同じコリジョン ドメインに数多くの競合ステーションがある場合、再試行制限回数を多くし、最大コンテンション ウィンドウを大きくする必要があります。さらに、ネットワーク内に隠しノードがある場合には、コリジョンは指数関数的には減らないものと考えられます。この場合、隠しノードの問題を軽減するために、RTS/CTS 交換が使用できます。

優先される親の選択

MAP に対して優先される親を設定できます。この機能を使用すると、細かい制御が可能になり、メッシュ環境でリニア トポロジを適用できます。AWPP を省略し、優先される親への移行を強制できます。

優先親の選択基準

子 AP は、次の基準に基づいて優先親を選択します。

- 優先される親は最良の親です。
- 優先される親には少なくとも 20 dB のリンク SNR があります（他の親はどんなに優れていても無視されます）。
- 優先される親には 12 dB ～ 20 dB の範囲内のリンク SNR がありますが、他の親が非常に優れていることはありません（つまり、SNR が 20 % 以上優れている）。SNR が 12 dB 未満の場合、設定は無視されます。
- 優先される親はブラックリストに掲載されません。
- 優先される親は、12 dB ～ 20 dB の範囲内の（DFS）のため、サイレント モードになりません。
- 優先される親は同じブリッジグループ名（BGN）に属します。設定された優先される親が同じ BGN に属さず、他の親が利用可能でない場合、子はデフォルトの BGN を使用して親 AP に join します。

優先される親の設定

優先親を設定するには、次のコマンドを入力します。

`(Cisco Controller) >` **config mesh parent preferred** *AP_name MAC*

値は次のとおりです。

- *AP_name* は、指定する必要がある子 AP の名前です。
- *MAC* は、指定する必要がある優先される親の MAC アドレスです。

（注） 優先される親を設定する場合、目的の親に対して実際のメッシュ ネイバーの MAC アドレスを指定してください。この MAC アドレスはベース無線の MAC アドレスで、最後の文字が f になります。たとえば、ベース無線の MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。これが、メッシュ ネイバー関係に使用される実際の MAC アドレスです。

次に、MAP1SB アクセス ポイントの優先される親を設定する例を示します。00:24:13:0f:92:00 は、優先される親の MAC アドレスです。

`(Cisco Controller) >` **config mesh parent preferred** *MAP1SB 00:24:13:0f:92:0f*

コントローラの GUI を使用して優先される親を設定する手順は、次のとおりです。

1. [Wireless] > [Access Points] > [AP_NAME] > [Mesh] を選択します。
2. [Preferred Parent] テキスト ボックスに優先される親の MAC アドレスを入力します。

（注） [Preferred Parent] の値をクリアするには、[Preferred Parent] テキスト ボックスで何も入力しないでください。

3 [Apply] をクリックします。

（注） 優先される親が入力されると、その他のメッシュ設定は、同時に設定できません。変更を適用してから 90 秒間待ってから、他のメッシュの変更を行えます。

関連コマンド

優先親の選択に関連するコマンドは次のとおりです。

- 設定された親を削除するには、次のコマンドを入力します。

  (Cisco Controller) > **config mesh parent preferred** *AP_name* **none**

- 子 AP の優先親として設定された AP に関する情報を取得するには、次のコマンドを入力します。

  (Cisco Controller) > **show ap config general** *AP_name*

次に、MAP1SB アクセス ポイントの設定情報を取得する例を示します。00:24:13:0f:92:00 は優先親の MAC アドレスです。

(Cisco Controller) > **show ap config general** *MAP1*

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... MAP1
Country code..................................... US - United States
Regulatory Domain allowed by Country.............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 12:12:12:12:12:12
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
CAPWAP Path MTU.................................. 1485
Domain.......................................
Name Server...................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 209.165.200.230
Secondary Cisco Switch Name......................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
Tertiary Cisco Switch IP Address................. 3.3.3.3
Administrative State ............................ ADMIN_ENABLED
```

```
Operation State ................................ REGISTERED
Mirroring Mode ................................. Disabled
AP Mode ........................................ Local
Public Safety .................................. Global: Disabled, Local: Disabled
AP subMode ..................................... WIPS
Remote AP Debug ................................ Disabled
S/W  Version ................................... 5.1.0.0
Boot  Version .................................. 12.4.10.0
Mini IOS Version ............................... 0.0.0.0
Stats Reporting Period ......................... 180
LED State....................................... Enabled
PoE Pre-Standard Switch......................... Enabled
PoE Power Injector MAC Addr..................... Disabled
Power Type/Mode................................. PoE/Low Power (degraded mode)
Number Of Slots................................. 2
AP Model........................................ AIR-LAP1252AG-A-K9
IOS Version..................................... 12.4(10:0)
Reset Button.................................... Enabled
AP Serial Number................................ serial_number
AP Certificate Type............................. Manufacture Installed
Management Frame Protection Validation.......... Enabled (Global MFP Disabled)
AP User Mode.................................... CUSTOMIZED
AP username..................................... maria
AP Dot1x User Mode.............................. Not Configured
AP Dot1x username............................... Not Configured
Cisco AP system logging host.................... 255.255.255.255
AP Up Time...................................... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time................................ 4 days, 06 h 15 m 00 s
Join Date and Time.............................. Mon Mar 3 06:19:47 2008

Ethernet Port Duplex............................ Auto
Ethernet Port Speed............................. Auto
AP Link Latency................................. Enabled
 Current Delay.................................. 0 ms
 Maximum Delay.................................. 240 ms
 Minimum Delay.................................. 0 ms
 Last updated (based on AP Up Time)............. 4 days, 06 h 17 m 20 s
Rogue Detection................................. Enabled
AP TCP MSS Adjust............................... Disabled
Mesh preferred parent........................... 00:24:13:0f:92:00
```

共同チャネルの干渉

隠しノードの干渉以外に、同一チャネルの干渉もパフォーマンスに影響する可能性があります。同一チャネルの干渉は、同じチャネルの隣接する無線がローカル メッシュ ネットワークのパフォーマンスに干渉するときに発生します。この干渉は、CSMA によるコリジョンまたは過度の遅延という形で現れます。いずれの場合でも、メッシュ ネットワークのパフォーマンスが低下します。適切なチャネル管理をすれば、ワイヤレス メッシュ ネットワーク上の同一チャネルの干渉は最小化できます。

ワイヤレスメッシュネットワークのカバレッジに関する考慮事項

この項では、それぞれのドメインでの準拠条件を守るために、都心もしくは郊外の地域で、最大のワイヤレス LAN カバレッジについて考慮する必要のある項目についてまとめています。

次の推奨事項は、障害物のない平坦地（グリーンフィールド導入）を前提としています。

そのエリアの実際の見積もりや部品表作成を開始する前に、サイト調査を行うことを常に推奨します。

セルの計画と距離

Cisco 1500 シリーズ アクセス ポイント用

RAP と MAP の比率は開始点です。一般的な計画用に、現在の比率は RAP ごとに 20 MAP になっています。

非音声ネットワークでのセル計画と距離について、次の値を推奨します。

- RAP と MAP の比率：推奨最大比率は、RAP ごとに 20 の MAP です。
- AP 間の距離：各メッシュ アクセス ポイント間に 2000 フィート（609.6 m）以下の間隔をあけることを推奨します。バックホール上でメッシュ ネットワークを拡張する（クライアント アクセスなし）場合、セルの半径には 1000 フィート（304.8 m）を使用してください。
- ホップ カウント：3 ～ 4 ホップ
  - 1 平方マイル（1 マイル = 52,802 フィート）は 9 セルに相当し、およそ 3 つまたは 4 つのホップでカバーできます（図 1および図 2を参照）。

- 2.4 GHz の場合、ローカル アクセス セル サイズの半径は 600 フィート（182.88 m）です。1 つのセル サイズは、およそ 1.310 x 106 で、1 平方マイルあたりのセルは 25 個です。（図 3 および図 4 を参照）。

図 ***16*** : 非音声メッシュ ネットワークにおける半径 ***1000*** フィートのセルとアクセス ポイントの位置

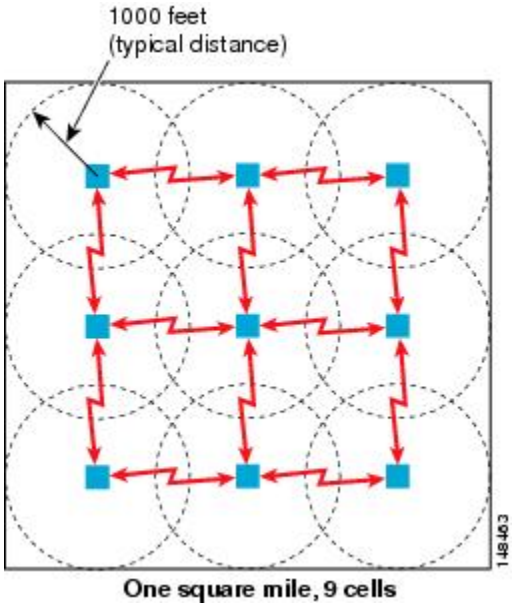


図 ***17*** : ***2.3*** ～ ***2.7*** のパス ロス指数

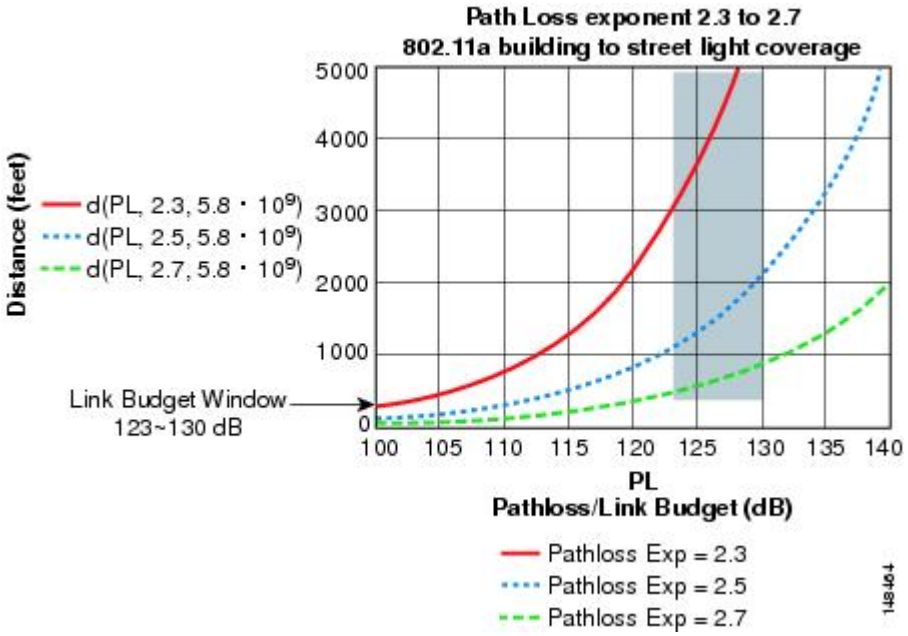


図 ***18*** : 非音声メッシュ ネットワークにおける半径 ***600*** フィートのセルとアクセス ポイントの位置

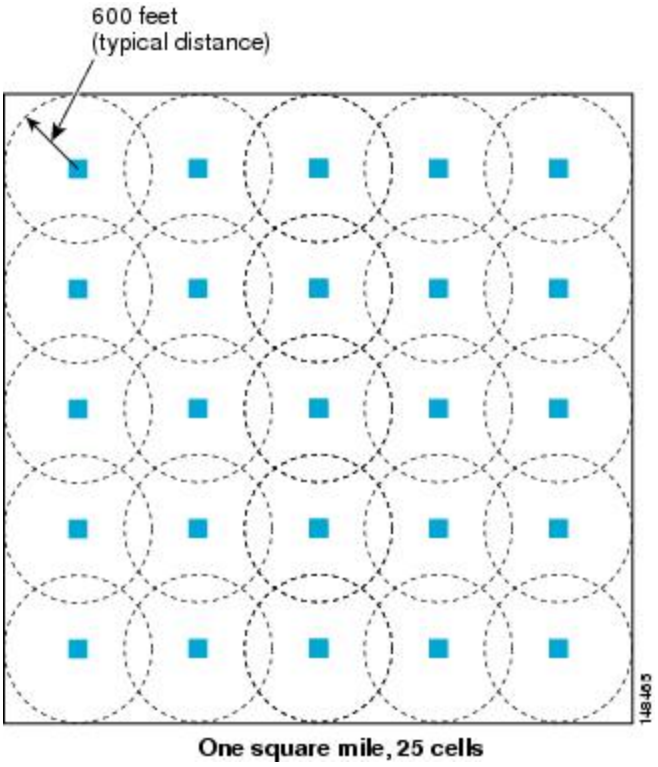
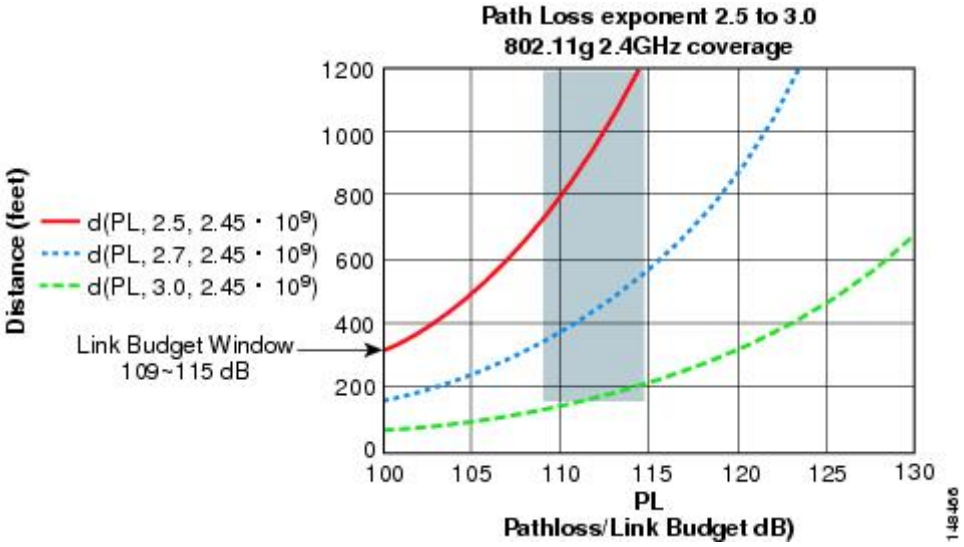


図 *19* : *2.5* ～ *3.0* のパス ロス指数



Cisco 1550 シリーズ AP 用

前の項で説明したように、セル半径 600 フィートおよび AP 間の距離 1200 フィートを推奨します。通常、AP 間の距離は AP からクライアントまでの距離の 2 倍にすることを推奨します。つまり、AP 間の距離を半分にすると、おおよそのセル半径になります。

AP1500 シリーズは、802.11n 機能を備えているため、比較的優れた範囲とキャパシティを備えています。ダウンストリームの ClientLink（ビーム形成）、アップストリームの MRC による高いレシーバ感度、複数のトランスミッタ ストリームといった利点に加え、チャネル結合などの 802.11n の利点もあります。1552 アクセス ポイントは、比較的大容量のセルを提供できます。

（注） リンク バジェットは国のドメインによって異なります。この項では、最も広く分散し、大きなドメインである -A と -E を考慮して説明します。

2.4 および 5 GHz 帯域の AP1572 シリーズと AP1552 シリーズのリンク バジェットの比較（-A ドメイン）

表 1を参照してください。

表 *7*：*-A/-B* ドメインの *2.4 GHz* 帯域のリンク バジェット比較

	Cisco 1562（-A ドメイン）	
周波数帯域	2412 ～ 2462 MHz	2412 ～ 2462 MHz
アンテナ タイプ	802.11a/b/g/n/acW2	1
帯域幅	20 MHz	20 MHz

	Cisco 1562（-A ドメイン）	
	1562I の場合は 3SS、1562E/D モデルの場合は 2SS	
	3SS では最大で 216 Mbps、2SS では 144 Mbps	

	Cisco 1562（-A ドメイン）	
最大送信電力	1562I の場合は 29 dBm 1562E/D の場合は 27 dBm	0 3 mBd
受信感度	6 Mbps で -92 dBm 54 Mbps で -76 dBm 216 Mbps で -71 dBm	6 spM で 3- mBd 4 5 spM で 8- mBd 6 12 spM で 7- mBd
受信チャネル数	3 または 2	4

	Cisco 1562（-A ドメイン）	
	（ドメイン）	（ドメイン）
ダイバシティ	MRC	MRC
外部アンテナ使用	0.5 dB（外部アンテナ使用）	5.0 dB（外部アンテナ使用）

6 2.4 GHz での 40 MHz チャネル ボンディングは適用されません。そのため、最大データ レートは 144 Mbps です。
7 複合電力は、AP1552 で 2 つの Tx ストリームが有効な場合の電力です。

5 GHz 帯域については、表 2 を参照してください。

表 *8*：*-A/-B* ドメインの *5 GHz* 帯域のリンク バジェット比較

	Cisco 1562（-A/B ドメイン）	
	（-A ドメイン）	（-B ドメイン）
動作周波数帯域	5.180 ～ 5.240 GHz 5.260 ～ 5.320 GHz 5.500 ～ 5.560 GHz 5.680 ～ 5.720 GHz 5.745 ～ 5.825 GHz	
802.11a/b/g/n/acW2 アンテナ タイプ		
802.11n/ac ネットワーク帯域幅	20 MHz、40 MHz、80 MHz	

	Cisco 1562（-A/B ドメイン）	
	（ドメイン	（ドメイン
xT 空間ストリーム数	3 または 2	3
YHP データレート	最大 1300/867 Mbps	最大 3.1 Gbps
送信電力 xT 複合電力	29 または 27 dBm	0 3 mBd
xR 感度	6 Mbps で –94 dBm 54 Mbps で –80 dBm 1300 Mbps で -65 dBm	6 Mbps で 29– mBd 45 Mbps で 08– mBd 02 Mbps で 06– mBd

5 GHz では、40 MHz チャネルを形成する 20 MHz チャネル ボンディングが使用可能です。これにより、データ レートを 300 Mbps まで増加できます。

前の項で説明したように、パス損失指数（PLE）とリンク バジェットの時間帯は連動します。完全なクリア パスの場合、PLE は 2.0 です。AP 間の場合、AP からクライアントまでよりクリアランスが大きくなります。AP 間では、PLE を 2.3 とすることができます。これは両方の AP の高さが約 10 m と見なすことができるためで、ライン オブ サイトが適切であることを意味します（ただし、フレネル ゾーン クリアランスはありません）。

AP からクライアントまでの場合、クライアントは 1 m 高いだけなので、PLE は 2.5 以上必要です。そのため、フレネル ゾーン クリアランスが小さくなります。これは 2.4 GHz および 5 GHz の両帯域に該当します。

5 GHz をメッシュのバックホールとして使用するので、-A ドメインの 5 GHz の AP 間リンク バジェットについて考えてみましょう。範囲を予測するためにレガシー データ レートを 9 Mbps とします（表 3 を参照）。

（注） これは、屋外 802.11n AP の最も低いデータ レートで、シスコの ClientLink（レガシー クライアントのビーム形成）の利点があります。ClientLink は、ダウンリンク方向に最大 4 dB のゲインを提供します。

表 *9*：*AP* 間 *RF* リンク バジェット、*5.8 GHz*：*9 Mbps*（*-A* ドメイン）

パラメータ	Cisco 1552 I/C	Cisco 1552 E/H
9 Mbps、20 MHz 帯域幅で供給される Tx 電力	28 dBm、複合	26 dBm、複合
Tx アンテナ ケーブル損失	0 dB	0.5 dB
Tx アンテナ ゲイン	4 dBi（内蔵アンテナ）	7 dBi
Tx ビーム形成（BF）	4 dB	4 dB
Tx EIRP	36 dBm	36.5 dBm
Rx アンテナ ゲイン	4 dBi	7 dBi
Rx アンテナ ケーブル損失	0 dB	0.5 dB
Rx 感度	9 Mbps で –91 dBm	9 Mbps で –91 dBm
システム ゲイン	131 dB	134 dB
フェード マージン	9 dB	9 dB

パラメータ	Cisco 1552 I/C	Cisco 1552 E/H
AP 間の範囲（LOS、PLE = 2.3）	829 m（2722 フィート）	1120 m（3675 フィート）

9 dB のフェードマージンを前提としています。これは、「ワイヤレス メッシュの制約」の項で必要な SNR 値を計算するための前提条件と矛盾しています。

AP からクライアントまでのリンク バジェット分析（-A ドメイン）

この項では、各帯域のシステム ゲイン値によって AP からどの程度クライアントを離すことができるかがわかるように、APからクライアントまでのリンク バジェット分析について説明します。この分析では、アップストリームおよびダウンストリームのシステム ゲインに焦点を当てます。リンクのアップストリームとダウンストリームのバランスが取れていることが理想ですが、実際にはバランスが取れない場合があります。一般には、AP のアンテナ ゲインおよび Tx 電力はクライアントより高くなります。しかし、一部の規制ドメインでは異なる EIRP 制限が必要なため、これが逆になることがあります。そのため、APからクライアントまでの距離を計算する場合、アップストリームとダウンストリームの低い方を使用します。これが決定要素になるためです。たとえば、ダウンストリームのゲインがアップストリームより高い場合、アップストリームのシステム ゲインによりクライアントだけが AP に接続できるため、セル サイズの決定にはアップストリームを使用する必要があります。

規制ドメインの Tx EIRP および Rx 感度の値によって、アップストリームとダウンストリームのどちらのシステムゲインが低いかを判断します。セルサイズは、ダウンストリームではなくアップストリームに基づいて決定する必要があります。

使用可能なクライアントのほとんどが 2.4 GHz クライアントであるため、2.4 GHz AP に焦点を当てます。

2.4 GHz の AP からクライアントまでのリンク バジェットでは、クライアントの Tx 電力が 20 dB、アンテナ ゲインが 0 dBi とします（表 4 を参照）。-A ドメインでは、2.4 および 5 GHz 帯域の EIRP 制限は 36 dBm です。

表 *10*：屋外 *11n AP/*クライアント間、*2.4 GHz*：*9 Mbps* データ レート（*–A* ドメイン）

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
	DS	US	DS	US	
供給 Tx 電力	28 dBm（AP）	20 dBm（クライアント）	28 dBm（AP）	20 dBm（クライアント）	9 Mbps、20 MHz 帯域幅の複合電力
Tx アンテナ ゲイン	2 dBi（AP）	0 dBi（クライアント）	4 dBi（AP）	0 dBi（クライアント）	

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
Tx ビーム形成（BF）	4 dB（AP）	0 dB（クライアント）	4 dB（AP）	0 dB（クライアント）	レガシー レートの ClientLinkDS でのみ有用
Tx EIRP	34 dBm	20 dBm	36 dBm	20 dBm	
Rx アンテナ ゲイン	0 dBi（クライアント）	2 dBi（AP）	0 dBi（クライアント）	4 dBi（AP）	
Rx 感度	–90 dBm（クライアント）	–94 dBm（AP）	–90 dBm（クライアント）	–94 dBm（AP）	AP1552 の 4.7 dB MRC ゲインを含む
システム ゲイン	124 dB	116 dB	126 dB	118 dB	
範囲（APからクライアント）		268 m（881 フィート）		323 m（1058 フィート）	LOS、PLE = 2.5

-A ドメインでは、2.4 GHz 帯域の AP からクライアントまでのリンク バジェットはアップストリームによって制限されます。つまり、アップストリームのシステム ゲインの方が低く、そのため決定要素はアップストリームになります。

各種 AP1552 モデルの 2.4 GHz の AP からクライアントまでのセル サイズは、次の 2 つの小さい方を使用して決定することができます。

- 2.4 GHz 帯域の AP からクライアントまでの距離（表 4 より）
- 5 GHz バックホールの AP 間距離の 2 分の 1（表 2より）

使用可能なクライアントのほとんどが 2.4 GHz クライアントであるため、セル サイズに 2.4 GHz の値を考慮することを推奨します（表 5 を参照）。

表 *11*：*AP*/クライアント間の最小距離と *AP* 間バックホール距離の *2* 分の *1*

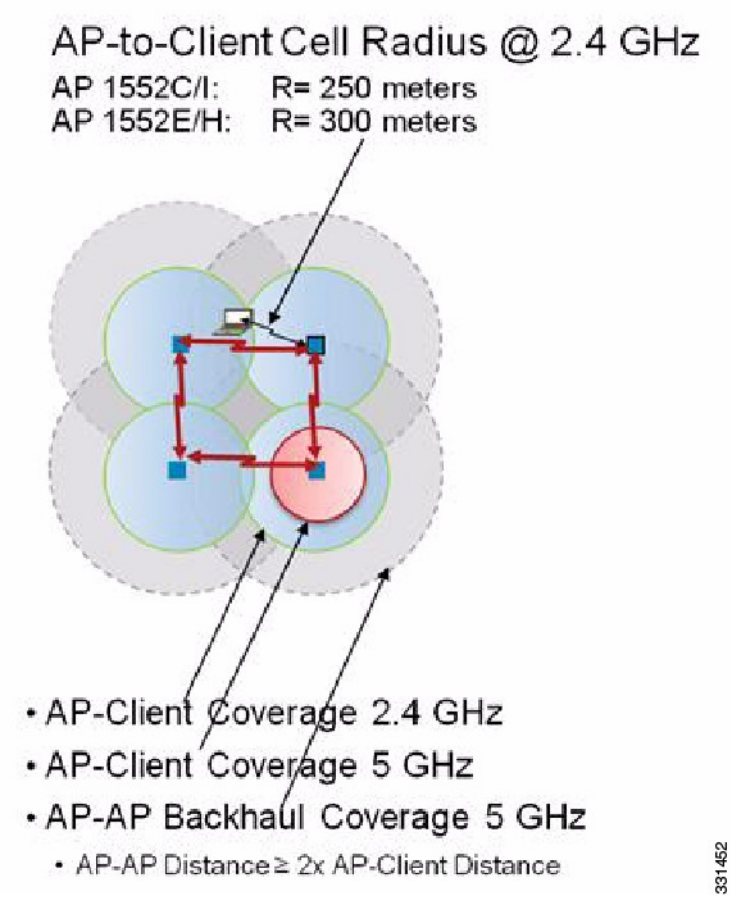
APタイプ（-A ドメイン）	AP/クライアント間（2.4 GHz）	AP間バックホール距離の2分の1（5 GHz）
1552 C/I	250 m（800 フィート）	415 m（1360 フィート）
1552 E/H	300 m（1000 フィート）	560 m（1840 フィート）

AP 間距離については、AP からクライアントまでの距離の 2 倍にすることができます（表 6を参照）。

表 *12*：セル半径の推奨値

AP タイプ（-A ドメイン）	AP からクライアント	AP 間
1552 C/I	250 m（800 フィート）	500 m（1600 フィート）
1552 E/H	300 m（1000 フィート）	600 m（2000 フィート）

図 *20*：*2.4 GHz* での *AP*/クライアント間のセル半径



前提条件は次のとおりです。

- 高さ：AP は 33 フィート（10 m）、クライアントは 3.3 フィート（1 m）
- 1 Mbps を超えるスループット
- AP 間距離を短くするとカバレッジが向上する

- ほぼ LoS。LoS が少ない場合、距離の前提条件を減らす必要がある
- 平坦地環境

AP 密度の結果：

- AP1552C および AP1552I：14 AP/平方マイル = 5.3 AP/平方 km
- AP1552E および AP1552H：9 AP/平方マイル = 3.5 AP/平方 km

これらの推奨事項により、健全なセルが実現する可能性が高くなります。

（注） 5 GHz クライアントの場合、周波数が高くなるに従い減衰が高くなるため、セル半径が比較的小さくなります。2.4 GHz 帯域のリンク バジェットは、5 GHz よりほぼ 13 dB 優れています。

2.4 および 5 GHz 帯域の AP1520 シリーズと AP1552 シリーズのリンク バジェットの比較（-E ドメイン）

-E ドメインでは、EIRP 制限がかなり低くなります。EIRP 制限は 2.4 Ghz で 20 dBm、5 GHz で 30 dBm です。

5 GHz をメッシュのバックホールに使用するため、5 GHz の場合を考えてみましょう。範囲を予測するためにレガシー データ レートを 9 Mbps とします。

（注） バックホールの場合、PLE は 2.3 です。

AP 間 RF リンク バジェット、5.6 GHz：9 Mbps（-E ドメイン）

表 *13*：*AP* 間 *RF* リンク バジェット、*5.6 GHz*：*9 Mbps*（*-E* ドメイン）

パラメータ	Cisco 1552 I/C	Cisco 1552 E/H
9 Mbps、20 MHz 帯域幅で供給される Tx 電力	22 dBm、複合	19 dBm、複合
Tx アンテナ ケーブル損失	0 dB	0.5 dB
Tx アンテナ ゲイン	4 dBi（内蔵アンテナ）	7 dBi
Tx ビーム形成（BF）	4 dB	4 dB
Tx EIRP	30 dBm	30.5 dBm
Rx アンテナ ゲイン	4 dBi	7 dBi
Rx アンテナ ケーブル損失	0 dB	0.5 dB

パラメータ	Cisco 1552 I/C	Cisco 1552 E/H
Rx 感度	9 Mbps で –91 dBm	9 Mbps で –91 dBm
システム ゲイン	125 dB	127 dB
フェード マージン	9 dB	9 dB
AP 間の範囲（LOS、PLE = 2.3）	471 m（1543 フィート）	575 m（1888 フィート）

内蔵アンテナを搭載したAP1552モデル（1552C/I）のシステム ゲインは、AP間距離が1543フィートの5 GHzバックホールのAP1522と同じです。

AP からクライアントまでのリンク バジェット分析（-E ドメイン）

この項では、2.4 GHz帯域のAPからクライアントまでのリンク バジェット分析について説明します。この分析では、アップストリームおよびダウンストリームのシステム ゲインに焦点を当てます。理想としてはリンクはアップストリームとダウンストリームでバランスが取れている必要がありますが、実際にはバランスが取れない場合があります。そのため、セル半径の決定要素はアップストリームとダウンストリームの低い方になります。

2.4 GHzのAPからクライアントまでのリンク バジェットでは、クライアントのTx電力が20 dB、アンテナ ゲインが0 dBiとします。

-E ドメインでは、EIRP 制限は 2.4 GHz 帯域で 20 dBm、5 GHz 帯域で 30 dBm です。

表 *14*：屋外 *11n AP/*クライアント間、*2.4 GHz*：*9 Mbps* データ レート（*-E* ドメイン）

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
	DS	US	DS	US	
供給 Tx 電力	15 dBm（AP）	20 dBm（クライアント）	13 dBm（AP）	20 dBm（クライアント）	9 Mbps、20 MHz 帯域幅の複合電力
Tx アンテナ ゲイン	2 dBi（AP）	0 dBi（クライアント）	4 dBi（AP）	0 dBi（クライアント）	
Tx ビーム形成（BF）	3 dB（AP）	0 dB（クライアント）	3 dB（AP）	0 dB（クライアント）	レガシー レートの ClientLinkDS でのみ有用
Tx EIRP	20 dBm	20 dBm	20 dBm	20 dBm	

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
Rx アンテナ ゲイン	0 dBi（クライアント）	2 dBi（AP）	0 dBi（クライアント）	4 dBi（AP）	
Rx 感度	–91 dBm（クライアント）	–94 dBm（AP）	–91 dBm（クライアント）	–94 dBm（AP）	AP1552 の 4.7 dB MRC ゲインを含む
システム ゲイン	111 dB	116 dB	111 dB	118 dB	
範囲（APからクライアント）	173 m（567 フィート）		173 m（567 フィート）		LOS、PLE = 2.5（5 dB のフェード マージン）

-E ドメインでは、2.4 GHz 帯域の AP からクライアントまでのリンク バジェットはダウンストリームによって制限されます。そのため、ダウンストリームのシステム ゲインが低くなります。したがって、決定要素はダウンストリームになります。

各種 AP1552 モデルの 2.4 GHz の AP からクライアントまでのセル サイズは、次の 2 つの小さい方を使用して決定することができます。

- 2.4 GHz 帯域の AP からクライアントまでの距離（表 8より）
- 5 GHz バックホールの AP 間距離の 2 分の 1（表 7 より）

使用可能なクライアントのほとんどが 2.4 GHz クライアントであるため、セル サイズに 2.4 GHz の値を考慮することを推奨します（表 9 を参照）。

表 *15*：*AP*/クライアント間の最小距離と *AP* 間バックホール距離の *2* 分の *1*

AP タイプ（-E ドメイン）	AP/クライアント間（2.4 GHz）	AP間バックホール距離の2分の1（5 GHz）
1552 C/I	180 m（600 フィート）	235 m（770 フィート）
1552 E/H	180 m（600 フィート）	288 m（944 フィート）

AP 間距離については、AP からクライアントまでの距離の 2 倍にすることができます（表 10 を参照）。

表 *16*：セル半径の推奨事項

AP タイプ（-E ドメイン）	AP からクライアント	AP 間
1552 C/I	180 m（600 フィート）	360 m（1200 フィート）
1552 E/H	180 m（600 フィート）	360 m（1200 フィート）

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

- すべての Cisco アクセス ポイントの範囲カルキュレータ：http://173.37.206.125/aspnet_client/system_web/2_0_50727/WNG_Coverage_Capacity_Calculator_V2.0_HTML/WNG_Coverage_Capacity_Calculator_V2.0.htm

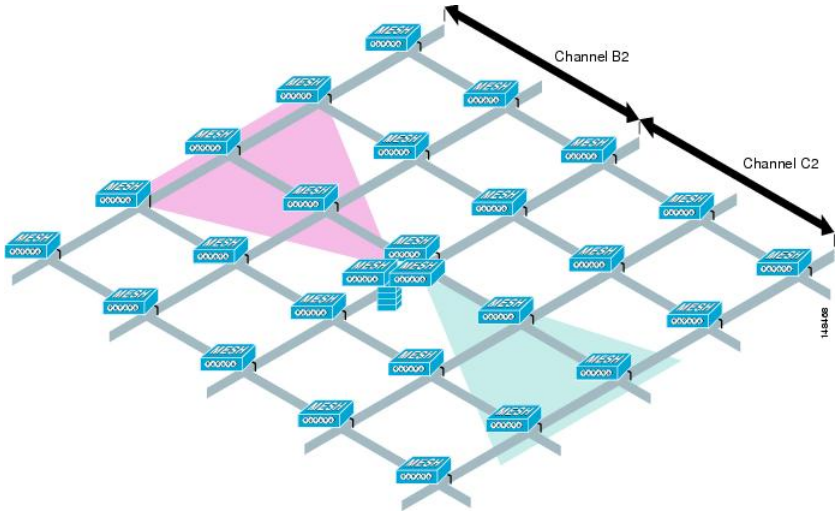
Cisco 範囲カルキュレータの前提条件

- 一覧表示された規制ドメインの送信電力および EIRP の制限内に収まるよう範囲カルキュレータが編集されています。この制限を超える場合があります。取り付けは、取り付ける地域の法律に従って行う必要があります。
- 効果的なパフォーマンスを実現するために、外部アンテナ モデルに対してすべてのアンテナ ポートを使用する必要があります。使用しない場合は、レンジが大幅に減少します。
- 送信電力は、両方の送信パスの総複合電力です。
- 受信感度は、3 つのすべての受信パスの複合感度です。つまり、MRC が含まれます。
- 範囲カルキュレータでは、ClientLink（ビームフォーミング）がオンになっていることを前提とします。
- 範囲カルキュレータを使用する場合に、規制ドメイン、選択されたアンテナ（またはアンテナ ゲイン）、および選択されたデータ レートに基づいて、利用可能な電力レベルが変わります。パラメータの変更後にすべてのパラメータを確認する必要があります。
- デフォルトで利用可能な 2 つとは異なるアンテナを選択できます。高ゲイン アンテナを入力し、EIRP 制限を超える電力を選択した場合は、警告が表示され、範囲が 0 になります。
- アクセス ポイントで認定されたチャネルのみを選択できます。
- 有効な電力レベルのみを選択できます。

図 21：複数の RAP の PoP, （71 ページ） に示した RAP は、開始点に過ぎません。ゴールは、RAP のロケーションを RF アンテナの設計と組み合わせて使用し、セルのコア内で MAP に適切な RF リンクを確立することです。これは、RAP の物理的なロケーションをセルの端にでき、指向性アンテナが、セルのセンターへのリンクの確立に使用されることを意味します。そのため、図

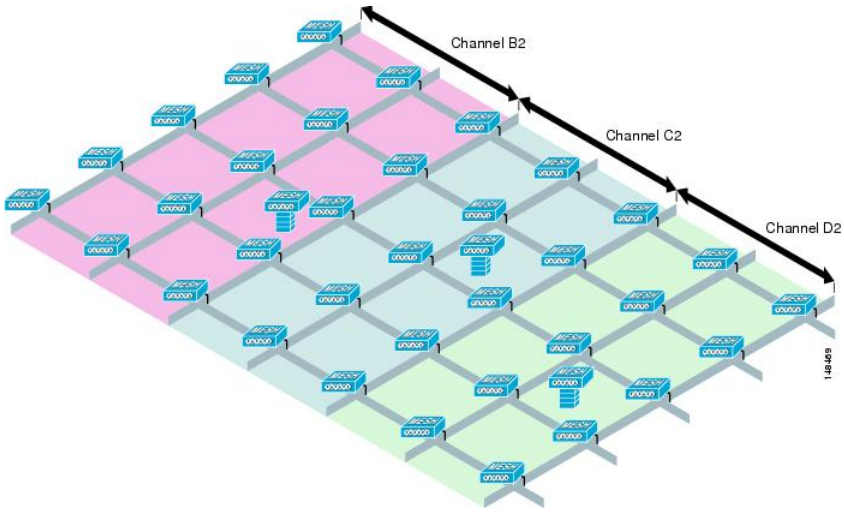
21：複数の RAP の PoP, （71 ページ） に示すように、RAP の有線ネットワークのロケーションが、複数のセルの RAP に対するホストの役割をする可能性があります。

図 *21*：複数の *RAP* の *PoP*



基本のセルの構成が決まれば、そのセルを複製して、もっと広いエリアをカバーできるようにできます。セルを複製する際は、すべてのセルに同じバックホール チャネルを使用するか、セルごとにバックホール チャネルを変えるかを決める必要があります。図 22：複数の RAP および MAP のセル, （71 ページ） の例では、セルごとにさまざまなバックホール チャネル（B2、C2、および D2）が選択され、セル間の共同チャネル干渉を減らしています。

図 *22*：複数の *RAP* および *MAP* のセル

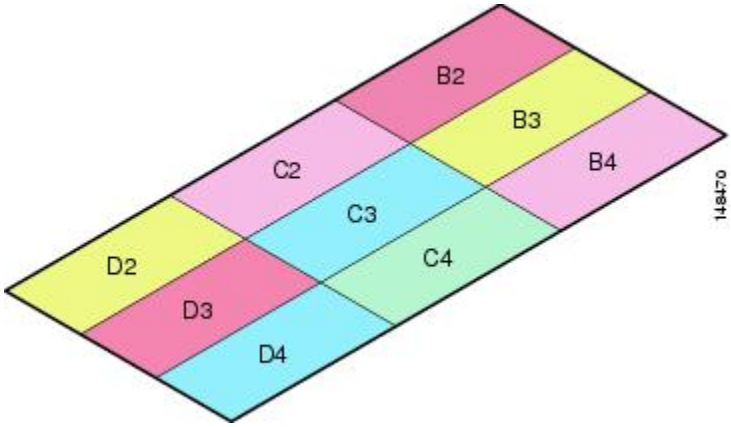


さまざまなチャネルを選択すると、より早いメッシュ コンバージェンスが犠牲になり、セル境界の共同チャネル干渉が減ります。MAP は seek モードにフォール バックして隣接セルのネイバーを検出する必要があるためです。高トラフィック密度のエリアで、共同チャネル干渉は、RAP の

周辺に最大の影響を与えます。RAPが1つのロケーションでクラスタ化されている場合、別のチャネル戦略によって最適なパフォーマンスが得られると考えられ、また、RAP がセル間で分散している場合には、同じチャネルを使用しても、パフォーマンスはほとんど低下しないと考えられます。

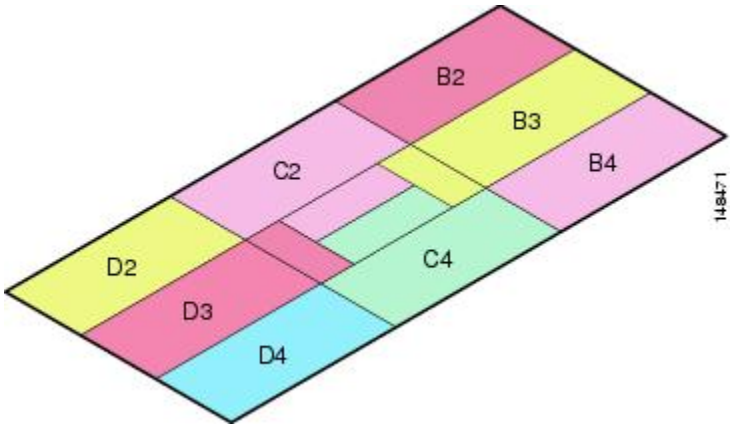
複数のセルをレイアウトする際には、標準のWLAN計画に似たチャネル計画を使用し、チャネルのオーバーラップを回避してください（図 23：さまざまなセルのレイアウト，（72 ページ） を参照）。

図 *23*：さまざまなセルのレイアウト



メッシュがRAP接続のロスをカバーするよう拡張されている場合には、できれば、チャネル計画でチャネル オーバーラップを最小にする必要もあります（図 24：フェールオーバー カバレッジ，（72 ページ） を参照）。

図 *24*：フェールオーバー カバレッジ



メッシュ アクセス ポイントのコロケーション

次の推奨事項は、複数の AP1500 を同じタワーにコロケーションする際に必要なアンテナセパレーションを決めるためのガイドラインとしてください。アンテナ、伝送パワー、およびチャネル間隔の推奨最小区切りについて記載しています。

適切な間隔をあけたりアンテナを選択するのは、アンテナの放射パターンやフリースペースパス損失、隣接または代替隣接のチャネル レシーバ拒否によって十分な切り分けをするのが目的で、コロケーションされた複数のユニットが独立して動作するためです。CCA ホールドオフによるスループット低下や、受信ノイズ フロアの増加によるレシーブ感度の低下をごくわずかに抑えることが重要です。

アンテナのプロキシミティ要件に従う必要がありますが、この要件は隣接および代替隣接のチャネル使用によって異なります。

隣接チャネルでの AP1500 のコロケーション

コロケーションされた 2 つの AP1500 が、チャネル 149（5745 MHz）とチャネル 152（5765 MHz）のような隣接チャネルで動作している場合、2 つの AP1500 の間の最小垂直距離は 40 フィート（12.192 m）です（この要件は 8 dBi の全方向性アンテナまたは 17 dBi の高ゲイン指向性パッチアンテナを搭載したメッシュ アクセス ポイントに適用されます）。

コロケーションされた 2 つの AP1500 が、5.5 dBi 全方向性アンテナ付きのチャネル 1、6、または 11（2412 ～ 2437 MHz）で動作している場合、最小垂直距離は 8 フィート（2.438 m）です。

代替隣接チャネルでの AP1500 のコロケーション

コロケーションされた 2 つの AP1500 が、チャネル 149（5745 MHz）とチャネル 157（5785 MHz）のような代替隣接チャネルで動作している場合、2 つの AP1500 の間の最小垂直距離は 10 フィート（3.048 m）です（この要件は 8 dBi の全方向性アンテナまたは 17 dBi の高ゲイン指向性パッチアンテナを搭載したメッシュ アクセス ポイントに適用されます）。

コロケーションされた 2 つの AP1500 が、5.5 dBi 全方向性アンテナ付きの代替隣接チャネル 1 と 11（2412 MHz と 2462 MHz）で動作している場合、最小垂直距離は 2 フィート（0.609 m）です。

要約すると、5 GHz アンテナの切り離しによって、メッシュ アクセス ポイントのスペーシング要件が決まります。また、アンテナのプロキシミティを遵守する必要がありますが、これは隣接および代替隣接のチャネル使用によって異なります。

屋内メッシュ ネットワークの特殊な考慮事項

次の屋内メッシュ ネットワークの考慮事項に注意してください。

- 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。
- Quality of Service（QoS）は、ローカルの 2.4 GHz クライアント アクセス無線、および 5 GHz でサポートされます。

- シスコは、アクセス ポイントとクライアントの間のコール アドミッション制御（CAC）を提供する CCXv4 クライアントの静的 CAC もサポートします。
- RAP と MAP の比率：推奨比率は、RAP ごとに 3 ～ 4 MAP です。
- AP 間の距離：
  - 11n および 11ac メッシュ AP の場合、セル半径 125 フィートで、各メッシュ AP 間に 250 フィート以下の間隔をあけることを推奨します。
- ホップ カウント：データには最大 4 ホップです。音声には 2 ホップ以下を推奨します。
- 音声ネットワーク上のクライアント アクセスの RF 考慮事項：
  - 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

    実行中のトラフィックがない場合は、CU を確認してください。

- 無線リソース管理（RRM）を使用して、802.11b/g/n 無線に、推奨される RSSI、PER、SNR、CU、セル カバレッジ、およびカバレッジ ホールの設定を実装できます（RRM は 802.11a/n 無線では使用できません）。

図 *25*：音声メッシュ ネットワークにおける半径 *100* フィート（*30.4 m*）のセルとアクセス ポイントの位置

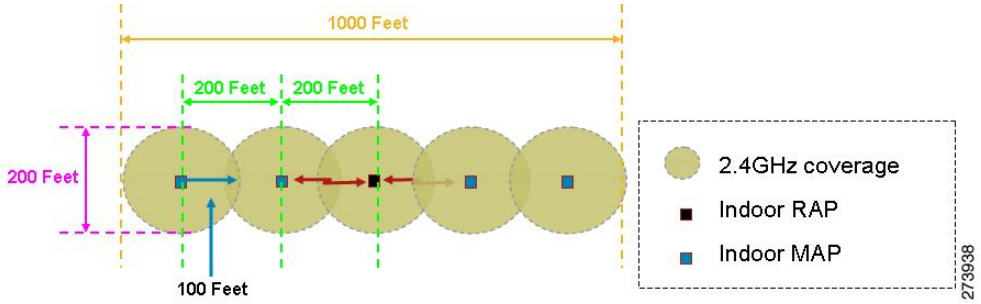
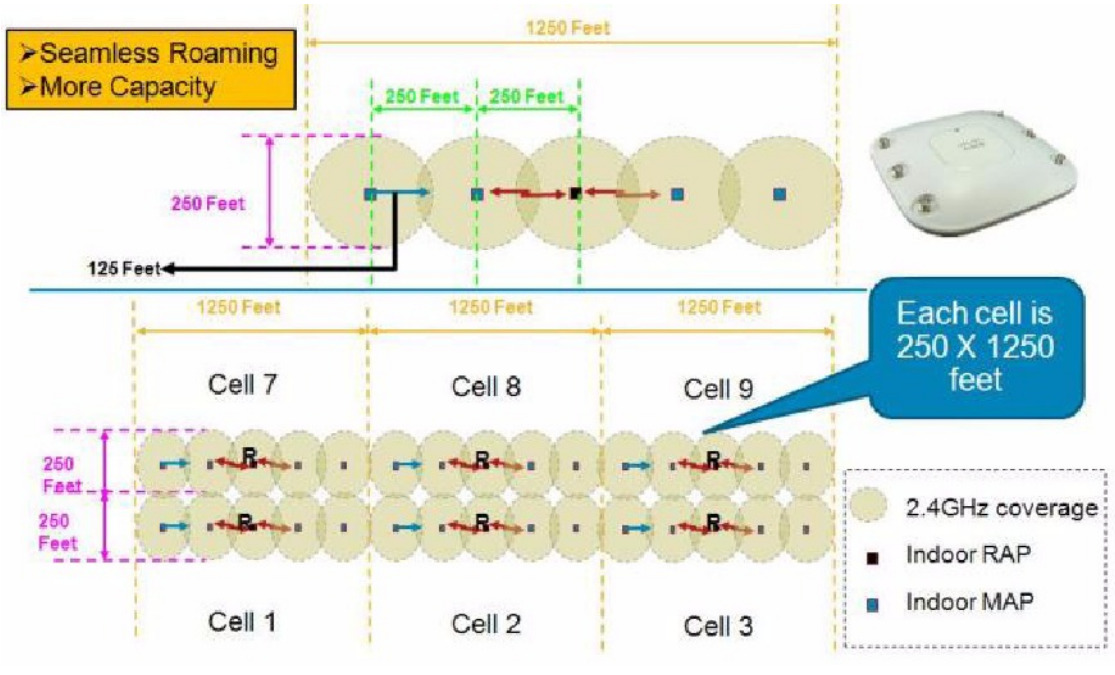


図 *26*：屋内 *11n* メッシュ ネットワークにおける半径 *125* フィート（*38 m*）のセルとアクセス ポイントの位置



（注） 指向性アンテナを使用していて、AP 間の距離が 250 フィート（76.2 m）を超えている場合でも、シームレスなローミングのために AP 間の距離を 250 フィート以下にすることを推奨します。

メッシュ AP バックグラウンド スキャン リリース 8.3

リリース 8.3 では、より高速なメッシュ コンバージェンスを実現する追加の拡張機能であるメッシュ AP バックグラウンド スキャン機能が導入されました。MAP にかかるコンバージェンス時間を短縮し、メッシュ ネットワークを高速に再コンバージェンスするために、リリース 8.0 および 8.1 の WLC ソフトウェアリリースですでに 2 つのメッシュ コンバージェンス機能が実装されています。

- メッシュ サブセット チャネル ベースのコンバージェンス（リリース 8.0）
- メッシュ クリア チャネル通知コンバージェンス（リリース 8.1）

両方の機能が導入されることで、メッシュ ツリーで 3 番目のホップ MAP が 10 秒かからずにデータ パスを再コンバージェンスおよび回復できます。

この新しいメッシュバックグラウンドスキャンおよび自動親選択によって、コンバージェンス時間や親選択の信頼性と安定性がさらに向上します。MAP はより適切な親をすべてのチャネルから見つけて接続し、常に最適な親とのアップリンクを維持できます。

（注） バックグラウンド スキャンのこのような実装は、Marvell ベースの AP に適用されます。具体的には、AP1550、AP1570、および IW3702 です。

子 MAP は、親とのアップリンクを維持するために、AWPP - Neighbor Discovery Request/Response（NDReq/NDResp）メッセージを使用します。これは、キープアライブとして機能します。NDResp メッセージの損失が連続して発生した場合、親は損失したと宣言され、子MAP は新しい親を探します。MAP は現在の**オンチャネル**のネイバーのリストを維持し、現在の親が失われたときは、同じサービング チャネル内で次に最適なネイバーにローミングします。ただし、同じチャネル内で他のネイバーが見つからなかった場合は、親を見つけるためにすべてまたはサブセットのチャネルでスキャン/シークを実行する必要があります。

各オフチャネル リスト ノードには、そのチャネルでリッスンしたすべてのネイバーを管理するネイバー リストがあります。各オフチャネル NDReq ブロードキャストで、ネイバーは NDResp パケットに基づいて最新の SNR 値が更新されます。misscount パラメータは、オフチャネル スキャンの試行にネイバーが応答しなかった回数を示します。各隣接ネイバーは、各バックグラウンド スキャン サイクル後に調整された容易度が最新の linkSNR 値で更新されます。

この機能は、時間がかかるスキャン/シークで他のチャネルで親を見つけることを回避しようとします。しかし子MAP をすべてのチャネルのすべてのネイバーで更新し続けるため、任意のチャネルのネイバーへの「切り替え」に役立ち、アップリンクの次の親としてそのネイバーを使用します。親の「切り替え」手順は、親の損失検出のようなトリガーされるイベントである必要はなく、子MAP で現在の親のアップリンクがアクティブであるときは「自動親選択アルゴリズム」を使用してより適切な親を識別します。「自動親選択アルゴリズム」は、新しい容易度の値に基づきます。コンバージェンスの計算を改善するため、リリース 8.3 ではよりスムーズでより高速な親またはネイバー検出と自動親接続アルゴリズムのために新しい「容易度」の値が導入されました。容易度の値は、SNR、ホップ数、タイマー、およびロードの値に基づきます。オフチャネル ネイ

バーの場合、AdjustedEase値が使用され、オフチャネルごとに最適なネイバーが最高のAdjustedEase値に基づいて特定されます。StickyEase はオンチャネル親のみに適用されます。

子MAPは、すべてのオフチャネルにわたる最適なネイバーの定期的な評価に基づいて最適な親を切り替えます。現在のオンチャネル親の stickyEase と比較して、別のオフチャネルのネイバーで最も高い adjustedEase 値を使用して、最適な次の親が特定されます。

次の表は、さまざまなコンバージェンス設定オプションに基づいた新しいコンバージェンス時間を示しています。最新の CCN およびバックグラウンド スキャン機能の実装と高速コンバージェンスにより、ファースト ホップ MAP は 3 ～ 4 秒のコンバージェンスを実現できます。

	親の損失の検出/キープ アライブ タイマー	チャネル スキャン/シーク	DHCP/CAPWAP 情報	ホップごとの時間（秒）
標準	21 / 3 秒	すべての 2.4 および 5 GHz チャネルのスキャン/シーク	CAPWAP の更新/再起動	48.6*
速い	7 / 3 秒	同じブリッジ グループにあるチャネルのみのスキャン/シーク	DHCP および CAPWAP の維持	20.5*
非常に高速	4 / 1.5 秒	同じブリッジ グループにあるチャネルのみのスキャン/シーク	DHCP および CAPWAP の維持	15.9*
CCN/バックグラウンドスキャン高速/非常に高速	50ms の場合は 4 / 3 秒	同じブリッジ グループにあるチャネルのみのスキャン/シーク	DHCP および CAPWAP の維持	8 ～ 10 秒

DFS と非 DFS チャネル スキャン

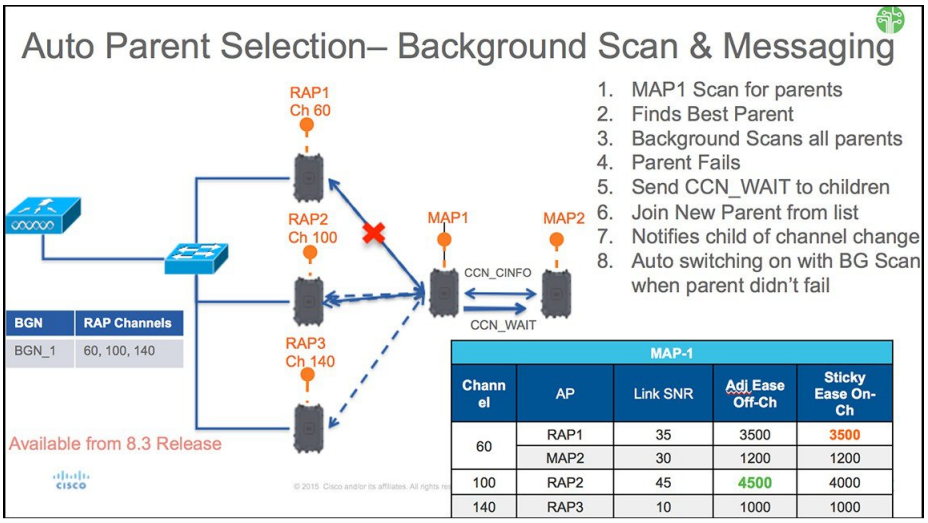
非 DFS チャネル スキャン

- MAP は定期的にオフチャネルになり、選択されたオフチャネルで NDReq ブロードキャスト パケットを伝送します。さらに、すべての「到達可能な」ネイバーから NDResp パケットを受信します。
- オフチャネル スキャンは 3 秒ごとに発生します。オフチャネルごとに最大で 50 ミリ秒維持されます。
- 各ネイバーから適切にヒアリングするには、50 ミリ秒の滞留時間内に少なくとも 4 つのメッセージを送信できるよう、NDReq が 10 ミリ秒ごとに伝送される必要があります。

DFS チャネル スキャン

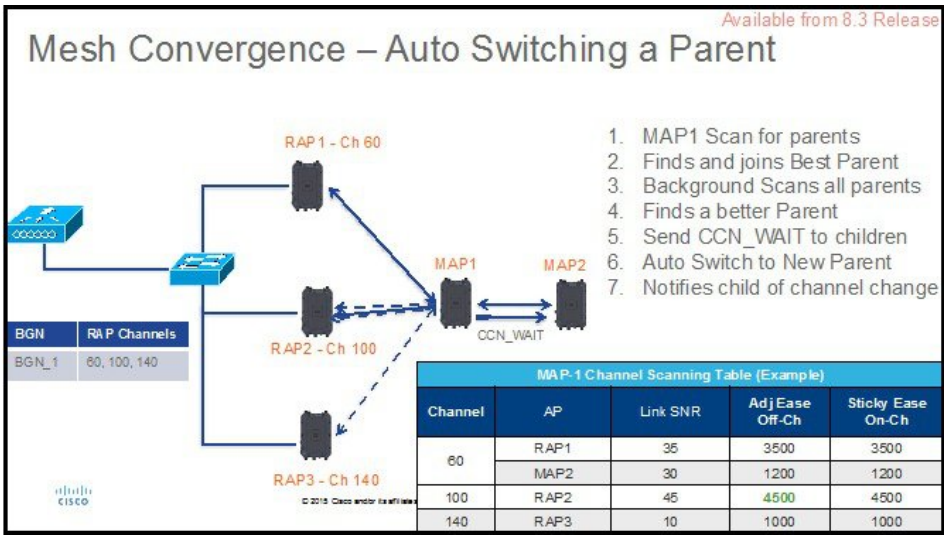
規制に従い、DFS チャネルが「安全に送信できる」と宣言するまで、AP はチャネル上を伝送しません（オフチャネル スキャンの無線で設定されているとき）。検出されたレーダー信号がある場合、伝送がなく、該当チャネルを AP のワイヤレス Tx/Rx に使用することを避ける必要があります。チャネルが安全に送信できることを確認する方法の 1 つは、AP がパッシブ スキャンを実行して DFS オンチャネルにある他のネイバーからパケットを受信するときです。

- DFS チャネル上のオフチャネル スキャン中に MAP がパケットを受信できるようにするには、最後の 50 ミリ秒に Tx/Rx がない場合に、他のすべてのオンチャネル DFS ネイバーが AWPP メッシュ ビーコンを伝送する必要があります。
- これらのメッシュ ビーコンは、DFS チャネル上でオフチャネルを実行している MAP が「安全に送信できる」と宣言してオフチャネルのアクティビティを実行できます。



上図は、「標準」または「高速/非常に高速」な構成の典型的なオフチャネル コンバージェンス プロセスを示しています。

（注） 表内のタイマーは、図示のためにすぎません。



下図は、元の親が依然として使用可能であっても、新しい「容易度値」によってより適切な親への切り替えが「容易度」の値によって要求されるときのメッシュ コンバージェンスおよび Parent Auto Switching を示しています。

メッシュ コンバージェンスの設定

設定手順は非常に簡単で、新しいバックグラウンド スキャン機能を呼び出します。

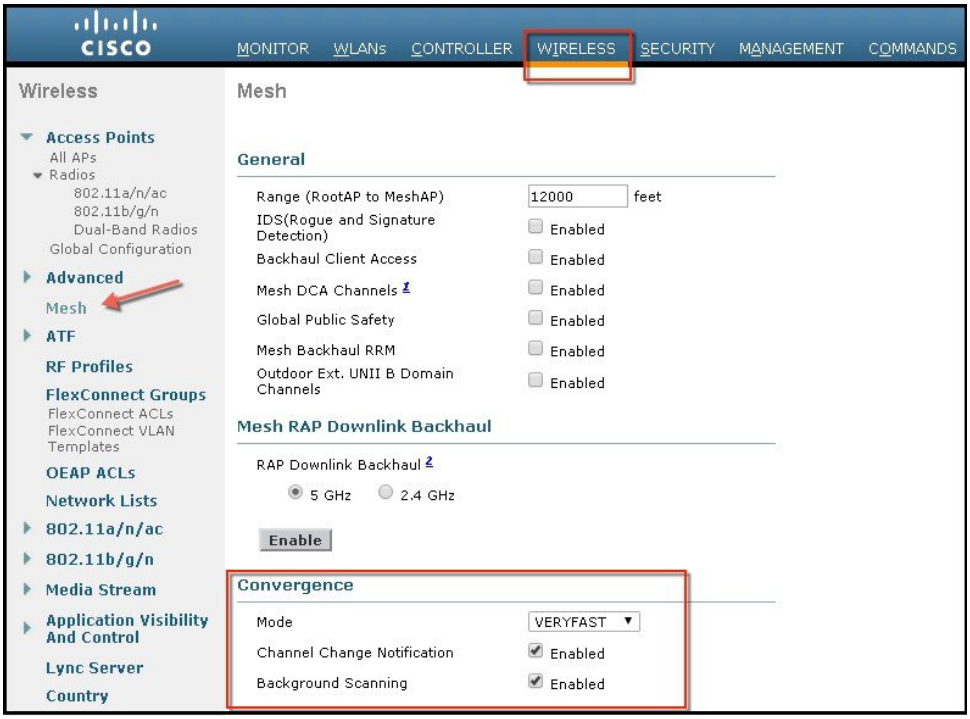
GUI を使用してコントローラを設定するには、次の手順を実行します。

手順の概要

1. コントローラで [Wireless] > [Mesh] タブを選択し、メッシュ設定の [Convergence] セクションでモードを選択し、CCN およびバックグラウンド スキャンを有効にします。
2. [Mode] にはコンバージェンス モードを選択するためのオプションが 3 つあることに注意してください。前述のように、選択したモードに応じてコンバージェンス時間が大幅に変化します。

手順の詳細

ステップ 1 コントローラで [Wireless] > [Mesh] タブを選択し、メッシュ設定の [Convergence] セクションでモードを選択し、CCN およびバックグラウンド スキャンを有効にします。



バックグラウンド スキャンは、次のコマンドを使用して CLI から設定します。

```
(Cisco Controller) >config mesh background-scanning ?

enable          Enable background scanning on Mesh
disable         Disable background scanning on Mesh

(Cisco Controller) >config mesh background-scanning enable
```

CCN は次の CLI コマンドを使用して設定します。

```
(Cisco Controller) >config mesh ccn ?

enable          Enables channel change notification
disable         Disables channel change notification

(Cisco Controller) >config mesh ccn enable
```

ステップ 2 [Mode] にはコンバージェンス モードを選択するためのオプションが 3 つあることに注意してください。前述のように、選択したモードに応じてコンバージェンス時間が大幅に変化します。

CLI からは次のコマンドを使用して、同じコンバージェンスが設定されます。

```
(Cisco Controller) >config mesh convergence ?

fast              Set fast convergence method
noise-tolerant-fast Set noise-tolerant fast convergence method to handle unstable RF environment
standard          Set standard convergence method
very-fast         Set very fast convergence method

(Cisco Controller) >config mesh convergence very-fast all
```

（注） 標準モードでは、CCN およびバックグラウンド スキャン オプションは適用されません。

メッシュ機能の管理

コンバージェンスの問題をデバッグおよびトラブルシューティングするために複数のコマンドが導入されています。

Debug mesh convergence enable：デバッグ トレース

```
AP1572-7a7f.09c0#debug mesh ?
  adjacency     MESH Adjacency debug
  channel       Mesh Channel debug
  convergence   Mesh convergence debug
  error         Mesh error debug
  ethernet      Mesh Ethernet debug
  event         Mesh event debug
  forwarding    Mesh forwarding debug
  link          MESH Link debug
  mperf         MESH BW test tool
  node          Mesh node debug
  port-control  Mesh port control debug
  reliable      Mesh Reliable Delivery debug
  security      MESH Security debug
  trace         trace address
```

Debug mesh bgscan enable/disable

```
Cyprus_MAP1#debug mesh ?
  adjacency     MESH Adjacency debug
  bgscan        Mesh bgscan debug
  channel       Mesh Channel debug
  convergence   Mesh convergence debug
  error         Mesh error debug
  ethernet      Mesh Ethernet debug
  event         Mesh event debug
  forwarding    Mesh forwarding debug
  link          MESH Link debug
  mperf         MESH BW test tool
  node          Mesh node debug
  port-control  Mesh port control debug
  reliable      Mesh Reliable Delivery debug
  security      MESH Security debug
  trace         trace address
```

Show mesh convergence：状態とカウンタの場合

```
AP1572-7a7f.09c0#sh mesh ?
  adjacency     MESH Adjacency
  backhaul      MESH backhaul
  channel       MESH channel
  config        MESH config paramenter
  convergence   MESH convergence info
  dfs           MESH dfs information
  ethernet      show mesh ethernet bridging
  forwarding    MESH Forwarding
  inventory     platform inventory
  linktest      MESH linktest stats
  lsc           MESH lsc details
  module        MESH module detail
  mperf         MESH BW tool
  security      MESH Security show
  simulation    MESH simulated configuration
  status        MESH status
```

Show mesh bgscan

```
Cyprus_MAP1#sh mesh ?
  adjacency     MESH Adjacency
  backhaul      MESH backhaul
  bgscan        MESH Background scanning info
  channel       MESH channel
  config        MESH config paramenter
  convergence   MESH convergence info
  dfs           MESH dfs information
  ethernet      show mesh ethernet bridging
  forwarding    MESH Forwarding
  inventory     platform inventory
  linktest      MESH linktest stats
  lsc           MESH lsc details
  module        MESH module detail
  mperf         MESH Bw tool
  security      MESH Security show
  simulation    MESH simulated configuration
  status        MESH status
```

```
Cyprus_MAP1#sh mesh bgscan
show MESH BG Scan

Background Scanning: Enabled

off Channel Neighbors
---------------------

Channel:149 MissCnt:0
Mac:1c6a.7a7f.11ef MissCnt:0 NDRespCnt:72972 HopCnt:1 AdjustedEase:15448576
Flags: UPDATED NEIGH BEACON OCNEIGH


Channel:153 MissCnt:0
Mac:1c6a.7a7f.107f MissCnt:0 NDRespCnt:2579 HopCnt:1 AdjustedEase:17048576 StickyEase:21848576
Flags: UPDATED NEIGH PARENT BEACON
Mac:5835.d9aa.e46f MissCnt:0 NDRespCnt:0 HopCnt:0 AdjustedEase:0
Flags: BEACON
Mac:18e7.28aa.e87f MissCnt:0 NDRespCnt:0 HopCnt:0 AdjustedEase:0
Flags: UPDATED CHILD BEACON

Aligned Offchannel neighbors
----------------------------

Channel:149 (POTENTIAL OFFCHANNEL)
Mac:1c6a.7a7f.11ef Ease:15448576

Channel:153 (ON-CHANNEL)
Mac:1c6a.7a7f.107f Ease:17048576


OffChannel Requests Statistics
------------------------------
Mac:18e7.28aa.e87f NDReqCnt:64 ch:149 last NDReq rx at: 10:54:21 UTC Mar 28 2016

Cyprus_MAP1#
```

ワイヤレス伝搬の特性

表 17：2.4 GHz 帯域と 5 GHz 帯域の比較, （84 ページ） は、2.4 GHz 帯域と 5 GHz 帯域の比較です。

2.4 GHz 帯域の伝搬特性は、5 GHz より優れていますが、2.4 GHz はライセンス不要の帯域で、今日まで歴史的に、5 GHz より多くのノイズや干渉に影響されてきました。さらに、2.4 GHz にはバックホール チャネルが 3 つしかないため、共同チャネル干渉の原因となります。そのため、同程度のキャパシティを得る最良の方法は、システム ゲイン（つまり、伝送パワー、アンテナゲイン、レシーブ感度、およびパス ロス）を削減して、もっと小さいセルを作成することです。セル

を小さくすると、1 平方マイルあたりのアクセス ポイント数を増やす（アクセス ポイント密度を増やす）必要があります。

表 *17*：*2.4 GHz* 帯域と *5 GHz* 帯域の比較

2.4 GHz 帯域の特性	5 GHz 帯域の特性
3 チャネル	22 チャネル（-A/-B の規制ドメイン）
共同チャネル干渉の傾向がより強い	共同チャネル干渉がない
低電力	高電力
低データ レートで、SNR 要求は低い	高データ レートで、SNR 要求は高い
5 GHz よりも伝搬特性はよいが、ノイズと干渉の影響を受けやすい	2.4 GHz よりも伝搬特性は悪いが、ノイズと干渉の影響を受けにくい
ライセンス不要の帯域。世界中で広く利用可能。	世界中で 2.4 GHz ほど広くは利用できない。ライセンスの必要な国もある。

2.4 GHz の方が波長が大きく、障害物に対する通過能力が大きいと言えます。また、2.4 GHz のデータ レートの方が小さく、他方の終端に信号が届く成功率が高くなります。

CleanAir

1550/1560/1570 シリーズ アクセス ポイントは、CleanAir のチップセットを含み、CleanAir の完全サポートを可能にします。

メッシュの CleanAir は 2.4 GHz 無線に実装でき、無線周波数（RF）を検出、位置を特定、分類、緩和すると同時にクライアントに完全な 802.11n/ac データ レートを提供します。これにより、キャリア クラス管理およびカスタマーエクスペリエンスを実現し、展開されたロケーションのスペクトルを制御できます。屋外プラットフォームの CleanAir 対応 RRM テクノロジーは、2.4 GHz 無線の Wi-Fi および非 Wi-Fi 干渉を検出し、定量化して、緩和します。ブリッジ モードで動作するアクセス ポイントは、2.4 GHz のクライアント アクセス モードの CleanAir をサポートします。

CleanAir AP 動作モード

ブリッジ（メッシュ）モード AP：CleanAir 対応のアクセス ポイントでは、2.4 GHz 帯域の完全な CleanAir 機能と 5 GHz 無線での CleanAir Advisor を提供します。これは、ブリッジ モードで動作するすべてのアクセス ポイントに適用されます。

Wi-Fi 無線との緊密なシリコン統合により、CleanAir ハードウェアは、接続されているクライアントのスループットを損なわずに、現在サービスが提供されているチャネルでトラフィック間のリッ

スンを行うことができます。つまり、クライアントトラフィックを中断しないライン レートの検出です。

ブリッジモードのアクセス ポイントは、WiFi 干渉源からの干渉を緩和できる 2.4 GHz 帯域の無線リソース管理（RRM）をサポートします。RRM は、ブリッジ モード RAP に子 MAP がない場合は、5 GHz 帯域でのみ使用できます。

CleanAir メッシュ AP は、各帯域の 1 つのチャネルだけを連続してスキャンします。通常の構成密度では、同じチャネルに多数のアクセス ポイントが存在する必要があります。また、RRM がチャネル選択を処理すると仮定すると、各チャネルには少なくとも 1 つのアクセス ポイントが必要です。2.4 GHz では、アクセス ポイントには少なくとも 3 つの分類ポイントを確保するための十分な密度があります。狭帯域変調（単一周波数上またはその周囲で動作）を使用する干渉源は、その周波数空間を共有するアクセスポイントだけに検出されます。干渉が周波数ホッピング タイプ（複数の周波数を使用、一般に全帯域を含む）の場合、帯域内での動作をヒアリングできるすべてのアクセス ポイントで検出されます。

モニタ モード AP（MMAP）：CleanAir モニタ モード AP は専用で、クライアント トラフィックを処理しません。モニタ モードでは、すべての帯域チャネルが定期的にスキャンされます。モニタ モードは、ブリッジ（メッシュ）モードのアクセス ポイントでは使用できません。これは、メッシュ環境ではアクセス ポイントはバックホールで相互に通信も行うためです。メッシュ AP（MAP）がモニタ モードの場合は、メッシュ動作は行いません。

ローカル モード AP：屋外アクセス ポイントがローカル モードで動作している場合、2.4 GHz と 5 GHz チャネルの両方で完全な CleanAir および RRM を実行することができます。主にプライマリ チャネルをスキャンしますが、定期的にオフチャネルになって残りのスペクトラムをスキャンします。拡張ローカル モード（ELM）wIPS の検出は、1532、1550、または 1570 では使用できません。

Spectrum Expert Connect モード（任意）（SE Connect）：SE Connect AP は、CleanAir AP をローカル アプリケーションのリモート スペクトル センサーとして使用するためにローカル ホストで実行されている Cisco Spectrum Expert アプリケーションの接続を可能にする専用スペクトル センサーとして設定されます。このモードでは、FFT プロット、詳細な測定値などの未加工スペクトル データを表示できます。このモードは、リモート トラブルシューティング専用です。

Pseudo MAC（PMAC）とマージ

PMAC とマージ現象はローカル モードの第 2 世代アクセス ポイントの現象と似ています。PMAC はデバイス分類の一部として計算され、Interference Device Record（IDR）に含まれます。各 AP は個別に PMAC を生成します。各レポートで PMAC は異なりますが（少なくともデバイスの測定された RSSI は各 AP で異なる可能性があります）、よく似ています。PMAC を比較および評価する機能をマージと呼びます。PMAC はカスタマー インターフェイスには表示されません。マージの結果だけがクラスタ ID の形式で使用できます。

同じデバイスが複数の AP によって検出されることがあります。すべての PMAC および IDR がコントローラ上で分析され、デバイス クラスタと呼ばれるレポートが生成され、デバイスを検出する AP およびデバイスを最も強いとしてヒアリングする AP を示すデバイス クラスタが表示されます。

このマージ空間プロキシミティでは、RF プロキシミティ（RF ネイバー関係）が同時に動作します。同様の IDR が 6 つあり、5 つが近隣の AP、残りの 1 つが離れた AP からの場合、同じ干渉源である可能性はありません。そのため、これらをすべて考慮してクラスタが形成されます。MSE とコントローラは、まず RF ネイバー リストを使用してマージの空間プロキシミティを確立します。

PMAC コンバージェンスおよびマージは次の要素に依存します。

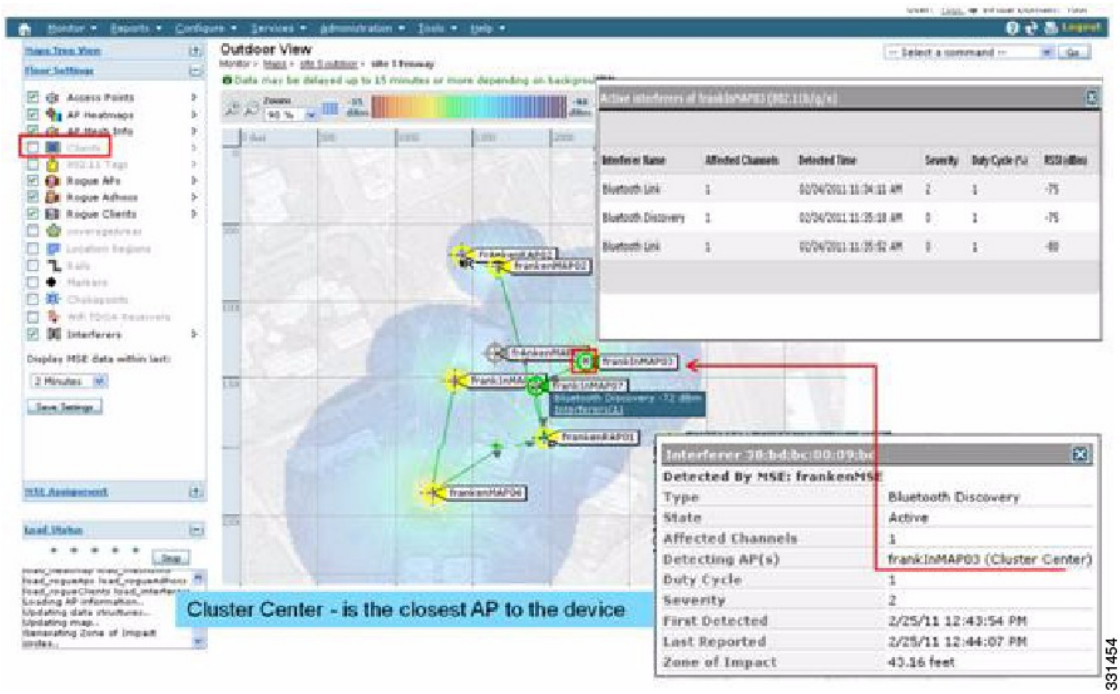
- センサーの密度
- 観測対象分類の品質
- 干渉源から AP までの RSSI
- AP での RF ネイバー リスト

したがって、メッシュ内の 2.4 GHz の RRM もマージを決定する際に重要な役割を担います。マージを行う可能性がある場合は、AP は RF ネイバーにする必要があります。RF ネイバー リストを参照し、マージに IDR の空間関係を考慮します。

メッシュにはモニタ モードがないため、コントローラのマージがコントローラで行われます。MSE がある場合は、コントローラのマージ結果はすべての裏付け IDR と共に MSE に転送されます。

複数の WLC（屋外での展開の場合など）では、マージは MSE で行われます。MSE は高度なマージを行い、干渉源のロケーションおよび履歴情報を抽出します。コントローラのマージ干渉源ではロケーションは行われません。ロケーションは MSE で行われます。

図 *27*：屋外での *Pseudo MAC* マージ



PMAC シグニチャ マージ後、デバイスをヒアリングできる AP およびクラスタの中央にする AP を特定できます。上記の図に示されている値は選択した帯域に関連しています。AP のラベル R は AP が RAP であることを示し、AP 間の線はメッシュ関係を示します。

Event Driven Radio Resource Management と Persistence Device Avoidance

CleanAir には、主な軽減機能が 2 つあります。両機能とも CleanAir によってのみ収集可能な情報を直接利用します。この 2 つの機能は、Event Driven Radio Resource Management（EDRRM）と Persistence Device Avoidance（PDA）です。メッシュ ネットワークでは、これらの機能は 2.4 GHz 帯域の非メッシュ ネットワークの場合とまったく同様に動作します。

（注） EDRRM と PDA はグリーンフィールド導入でだけ使用でき、デフォルトでオフに設定されています。

CleanAir アクセス ポイント配置の推奨事項

CleanAir は、Wi-Fi ネットワークの通常の動作に影響を与えないパッシブなテクノロジーです。CleanAir 導入とメッシュ導入には本質的な違いはありません。

非 Wi-Fi デバイスの特定には考慮すべき多くの変動要因があります。精度は、電力、デューティ サイクル、およびデバイスをヒアリングするチャネルの数によって向上します。高い電力、高いデューティ サイクル、および複数のチャネルに影響を与えるデバイスはネットワークへの干渉に対して重大であると見なされるため、これは便利です。

（注） 非 Wi-Fi デバイスのロケーションの精度は保証されません。

コンシューマ エレクトロニクスの世界には多くの変動要因があり、意図しない電気干渉もあります。現在のクライアントまたはタグのロケーション精度モデルから導出した精度の予測は、非 Wi-Fi ロケーションや CleanAir 機能には適用されません。

考慮すべき重要事項：

- CleanAir メッシュ AP は、割り当てられたチャネルだけをサポートします。
- 帯域カバレッジは、そのチャネルをカバレッジの対象にすることにより実装されます。
- CleanAir メッシュ AP のヒアリングは非常に優れており、アクティブなセルの境界が限界にはなりません。
- ロケーション ソリューションでは、RSSI カットオフ値は -75 dBm です。
- ロケーション分解能には高品質の測定値が少なくとも 3 つ必要です。

ほとんどの導入では、2.4 GHz 帯域内の同じチャネルに少なくとも 3 つの AP が隣接しているカバレッジ エリアを持つことは困難です。最小限の密度があるロケーションでは、ロケーション分解能がサポートされない可能性がありますが、アクティブなユーザ チャネルは保護されます。

導入に関する考慮事項は、必要なキャパシティに対するネットワークの計画、および CleanAir 機能をサポートするための適切なコンポーネントおよびネットワーク パスの配置によって異なります。RF プロキシミティ、および RF ネイバー関係の重要性は十分に理解する必要があります。また、PMAC とマージ プロセスに留意することも重要です。ネットワークの RF 設計が適切でなければ、ネイバー関係に影響し、その結果 CleanAir のパフォーマンスに影響します。

CleanAir の AP 密度に関する推奨事項は、通常のメッシュ AP の配置の場合と同じです。

屋外におけるロケーション分解能は最も近い AP に対してです。デバイスは物理的にそのデバイスに最も近い AP の近くに位置しています。最も近い AP Resolution を仮定することを推奨します。

1552 AP と 1572 AP（CleanAir）で構成されるインストールで少数の 1530 AP（非 CleanAir）を配置することもできます。この配置では、各アクセス ポイントが互いに完全に相互運用可能なためクライアントとカバレッジの観点から作業できます。CleanAir の完全な機能性は、CleanAir がイネーブルになっているすべてのアクセス ポイントによって決まります。検出は影響を受けることがあり、緩和は推奨されません。

CleanAir AP のアクティブにサービスを提供しているクライアントは、サービスを提供している割り当てられたチャネルのみモニタできます。近くに複数のアクセス ポイントを提供しているクライアントがあるエリアでは、CleanAir のアクセス ポイントによってサービスが提供されているチャネルは CleanAir 機能を促進できます。従来の非 CleanAir アクセス ポイントは RRM に依存して干渉の問題を緩和しますが、CleanAir アクセス ポイントがシステム レベルに対して行うようなタイプと重大度はレポートしません。

混合システムの詳細については、以下を参照してください。 http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b4bdc1.shtml

CleanAir Advisor

バックホール無線で CleanAir が有効な場合、CleanAir Advisor が始動します。CleanAir Advisor では、電波品質の指標（AQI）および干渉検出レポート（IDR）が生成されますが、これらのレポートはコントローラにのみ表示されます。イベント駆動型 RRM（ED-RRM）で実行されるアクションはありません。CleanAir Advisor は、ブリッジ モードの 1552 アクセス ポイントの 5 GHz バックホール無線のみに存在します。他のすべての AP モードでは、1552 アクセス ポイントの 5 GHz バックホール無線は CleanAir モードで動作します。

CleanAir のイネーブル化

システムの CleanAir 機能をイネーブルにするには、まず、[Wireless] > [802.11a/b] > [CleanAir] を選択してコントローラで CleanAir をイネーブルにする必要があります。CleanAir はデフォルトでディセーブルですが、CleanAir は AP インターフェイスではデフォルトでイネーブルです。

デフォルトのレポート インターバルが 15 分であるため、CleanAir をイネーブルにした後、電波品質情報がシステムに伝搬されるまで 15 分かかります。ただし、[Monitor] > [Access Points] > [802.11a/n] または [802.11b/n] を選択することで、無線の CleanAir 詳細レベルで結果を即座に確認できます。

ライセンス

CleanAir システムには CleanAir AP およびリリース 7.0 以降のリリースを実行しているコントローラが必要です。Cisco Prime Infrastructure を追加すると、表示を強化し、システム内で追加の情報を相互に関連付けることができます。MSE を追加すると、使用可能な機能がさらに増え、特定の干渉デバイスの履歴と場所が表示されます。CleanAir AP がライセンスであるため、CleanAir 機能の使用には追加ライセンスは必要ありません。Prime Infrastructure の追加は基本ライセンスで行うことができます。システムに MSE を追加するには、Prime Infrastructure Plus ライセンス、および MSE の Context-Aware ライセンスを選択する必要があります。

MSE または CMX での干渉ロケーションのために、各干渉デバイスは Context-Aware 内のロケーション ターゲットとしてカウントされます。100 の永久 Interferer ライセンスが MSE に組み込まれています。Interferer ライセンスは各 CleanAir AP の 5 つのライセンスのそれぞれのステージで、CleanAir AP が検出されるたびに開かれます。このプロセスは AP1552/1562/1572 に適用されます。干渉デバイスは、ライセンス数の観点からはクライアントやタグと同じです。追跡対象の干渉デバイスはクライアントやタグよりはるかに少なくする必要があるため、使用可能なシート数のごく一部のみ使用します。ユーザは、コントローラの設定メニューから検出および検索する干渉デバイスのタイプを制御できます。

Cisco Context-Aware ライセンスは、ターゲットの種類（クライアント、タグ、干渉）で管理および制限することができ、ユーザがライセンスの使用方法を完全に制御できます。

（注） 各干渉デバイスは、コンテキスト認識型サービス（CAS）ライセンスが 1 つ必要です。

Bluetooth デバイスの数が多すぎる場合、それらのデバイスによって多数の CAS ライセンスが利用される可能性があるので、Bluetooth デバイスの追跡をオフにすることを推奨します。

ワイヤレス メッシュ モビリティ グループ

モビリティ グループを使用すると、ピアに対する各コントローラがコントローラの境界を越えたシームレスなローミングを互いにサポートできます。AP は、CAPWAP Join プロセス後にモビリティ グループの他のメンバの IP アドレスを学習します。コントローラは、最大 24 台のコントローラを含めることができる単一のモビリティ グループのメンバにすることができます。モビリティは、72 台のコントローラ間でサポートされます。モビリティ リストには最大 72 のメンバ（WLC）、およびクライアントのハンドオフに参加している同じモビリティ グループ（またはドメイン）内の最大 24 のメンバを登録できます。クライアントの IP アドレスは、同じモビリティ ドメイン内で更新する必要はありません。この機能を使用する場合、IP アドレスの更新はコントローラベースのアーキテクチャでは無意味です。

複数のコントローラ

モビリティ グループ内の他の CAPWAP コントローラから CAPWAP コントローラまでの距離と、RAP からの CAPWAP コントローラの距離については、企業内の CAPWAP WLAN の配置と同様に考慮する必要があります。

CAPWAP コントローラを集中させると、オペレーション的に利点がありますが、その利点は、CAPWAP AP へのリンクのスピードおよびキャパシティ、およびこれらのメッシュ アクセス ポイントを使用している WLAN クライアントのトラフィック プロファイルに対するトレード オフとなります。

WLAN クライアント トラフィックを、インターネットやデータセンターなどの特定のサイトに集中させたい場合は、これらのトラフィック フォーカルポイントと同じサイトにコントローラを集中させると、トラフィックの効率を犠牲にしなくても操作上の利点を享受できます。

WLAN クライアント トラフィックが、よりピアツーピアの場合、分散されたコントローラ モデルの方が適している可能性があります。WLAN トラフィックの大多数は、そのエリアのクライアントで、他のロケーションに向かう比較的少量のトラフィックを伴う傾向があります。数多くのピアツーピアアプリケーションが遅延やパケット損失に影響されやすい場合、ピア間のトラフィックが最も効率のよいパスを通過するようにする必要があります。

大部分の配置に、クライアント サーバ トラフィックとピアツーピア トラフィックが混ざっている場合、CAPWAP コントローラのハイブリッドモデルが使用されていると考えられ、ネットワーク内の戦略的なロケーションに置かれたコントローラのクラスタと共に Points of Presence（PoP）が作成されます。

ワイヤレス メッシュ ネットワークで使用される CAPWAP モデルは、キャンパス ネットワーク向けに設計されています。つまり、CAPWAP メッシュ アクセス ポイントと CAPWAP コントローラ間のネットワークは高速で低遅延であると考えられています。

メッシュ アベイラビリティの増加

「セルの計画と距離」セクションでは、1 平方マイルのワイヤレス メッシュ セルが作成され、組み込まれました。このワイヤレス メッシュ セルは、携帯電話ネットワークの作成に使用されるセルに似た特性を持ちます。より大きなアベイラビリティやキャパシティに対して、同じ物理エリアをカバーするために、（定義された最大セル サイズより）小さいセルが作成される可能性があるからです。このプロセスは、セルに RAP を追加することで行われます。より大きなメッシュ配置と同様、同じチャネルで RAP を使用するか（図 28：同じチャネルでセルごとに 2 つの RAP, （91 ページ） を参照）、または別のチャネルに置いた RAP を使用するか（図 29：別のチャネルで

セルごとに 2 つの RAP, （91 ページ） を参照）を決める必要があります。エリアへの RAP の追加により、そのエリアのキャパシティと回復力が増大します。

図 *28*：同じチャネルでセルごとに *2* つの *RAP*

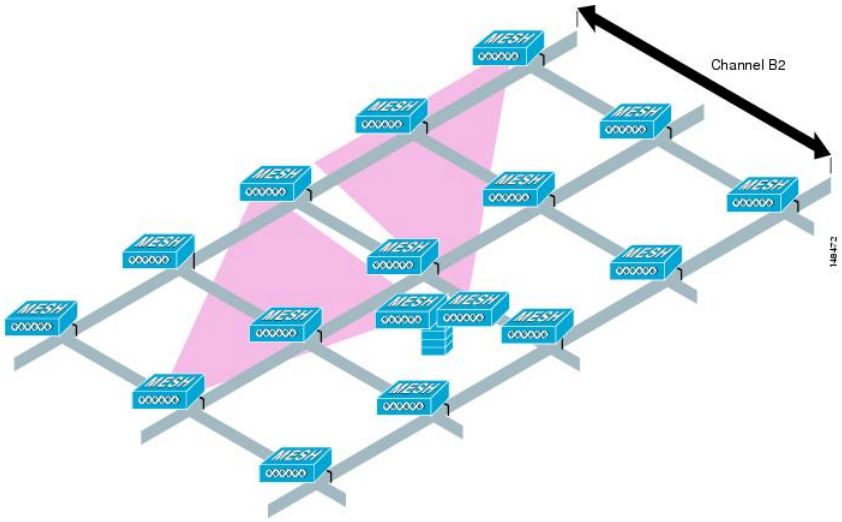
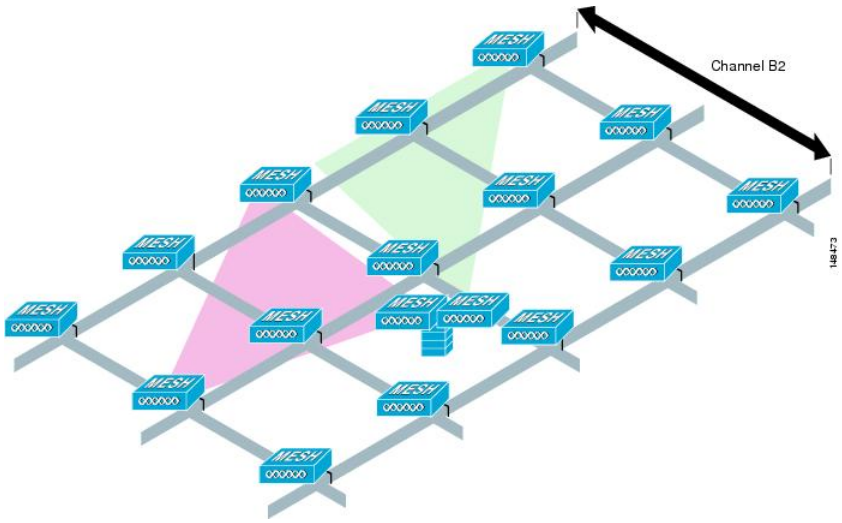


図 *29*：別のチャネルでセルごとに *2* つの *RAP*



複数の RAP

複数のRAPが配置される場合は、それらのRAPを配置する目的を考慮する必要があります。ハードウェア ダイバーシティを提供するために RAP を配置するのであれば、メッシュが 1 つの RAP から別の RAP へ転送する場合に、プライマリの RAP がコンバージェンス時間を最小にできるよう、同じチャネルに追加の RAP を配置する必要があります。RAP ハードウェア ダイバーシティを計画する場合は、RAP 制限ごとに 32 MAP を検討します。

キャパシティを第一に追加するために追加のRAPが配置される場合、バックホールチャネルの干渉を最小限にするために、追加の RAP が近隣の RAP と異なるチャネルに配置される必要があります。

チャネル計画や RAP セル スプリットを介して、異なるチャネルに 2 番めの RAP を追加しても、コリジョン ドメインが減ります。チャネル計画では、コリジョンの確率を最小限にするため、同じコリジョン ドメイン内のメッシュ ノードに異なる非オーバーラップ チャネルを割り当てます。RAP セル スプリットは単純ですが、コリジョン ドメインを減らすのに効果的な方法です。メッシュ ネットワークで全方向性アンテナと共に1つのRAPを配置する代わりに、方向性アンテナと共に2つ以上のRAPを配置できます。これらのRAPは互いに一緒に用いられ、異なる周波数チャネルで動作します。このプロセスにより、大きなコリジョン ドメインが個別に動作する複数の小さなコリジョン ドメインに分割されます。

メッシュ アクセス ポイントのブリッジ機能が複数の RAP と共に使用される場合、これらの RAP はすべて同じサブネット上になければならず、継続したサブネットがブリッジ クライアントに提供されるようにする必要があります。

異なるサブネット上の複数の RAP と共にメッシュを構築し、異なるサブネット上の別の RAP に MAP をフェールオーバーする必要がある場合、MAP コンバージェンス時間が増加します。このプロセスが起こらないようにする1つの方法として、サブネット境界で区切られているネットワークのセグメントに異なる BGN を使用する方法があります。

屋内メッシュと屋外メッシュの相互運用性

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 ポイントとの完全な相互運用性がサポートされています。これは、屋外から屋内にカバレッジを持ち込むのに役立ちます。屋内メッシュ アクセス ポイントは屋内でのみ使用することを推奨します。屋内メッシュ アクセス ポイントは、以下で説明されているような限られた状況でのみ屋外に配置してください。

注意 サードパーティの屋外ラックの屋内アクセス ポイントは、屋内 WLAN から駐車場のホップまでの単純かつ短距離の拡張などの、屋外での限られた配置でのみ配置できます。堅牢な環境および温度に関する仕様を備えているため、屋外ラックでは 1260、1700、2600、2700、3500e、3600、および3700アクセス ポイントを推奨します。さらに、APが屋外ラック内にある場合、屋内アクセス ポイントには、連結されたアンテナをサポートするためのコネクタがあります。SNR 値は増減しない場合もあるので、注意してください。また、より最適化された屋外の 1500 シリーズ アクセス ポイントと比較した場合、長期間のフェードにより、これらの AP のリンクが消失する場合があります。

モビリティ グループは、屋外メッシュ ネットワークと屋内 WLAN ネットワークの間で共有できます。1 台のコントローラで、屋内と屋外のメッシュ アクセス ポイントを同時に制御することもできます。同じ WLAN が屋内と屋外の両方のメッシュ アクセス ポイントからブロードキャストされます。

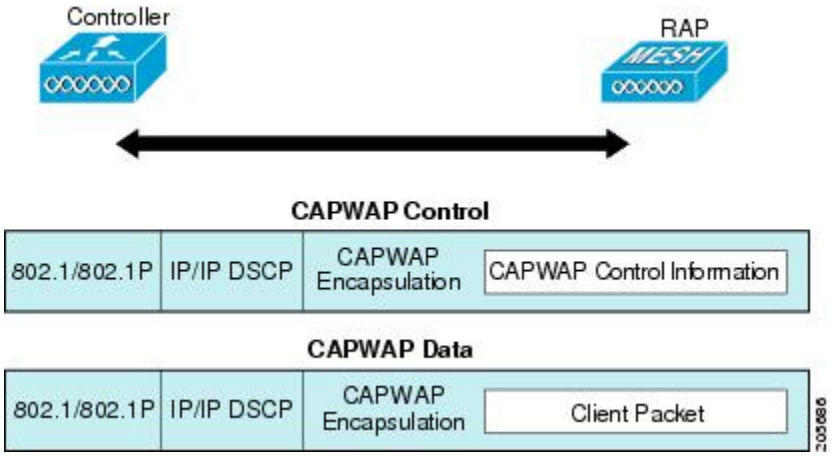
第 6 章

Cisco 1500 シリーズ 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 1500 シリーズ 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 30：メッシュ ネットワーク トラフィックの終端, （93 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、コントローラがコロケーション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 *30*：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 の設定の確認に関する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 ゲインの設定」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 ポイントの無線 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がありません。

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。

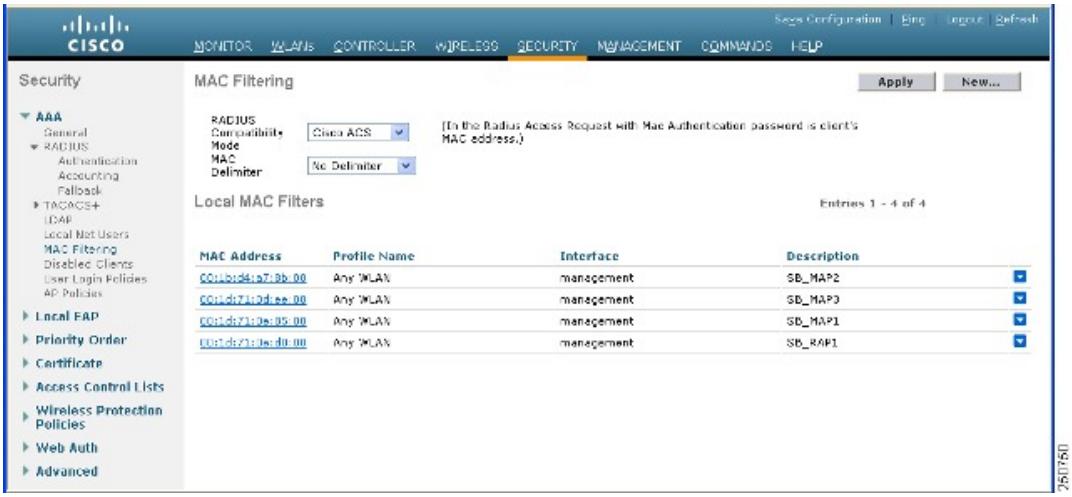
（注） メッシュ アクセス ポイントの MAC アドレスのリストは、ダウンロードして、Cisco Prime Infrastructure を使用してコントローラにプッシュすることもできます。

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のメッシュ 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 *31*：*[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 ポイントの無線 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、コントローラへのメッシュ 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のメッシュ 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 に設定された無線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 のコントローラとのアソシエーション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 である場合）、802.11a/n 無線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。ネットワークでのコンバージェンスを高速にするため、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 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 無線をプライマリ 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 トポロジをビルドしません。
- 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 の場合、または RAP が UP 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 無線が 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 無線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）

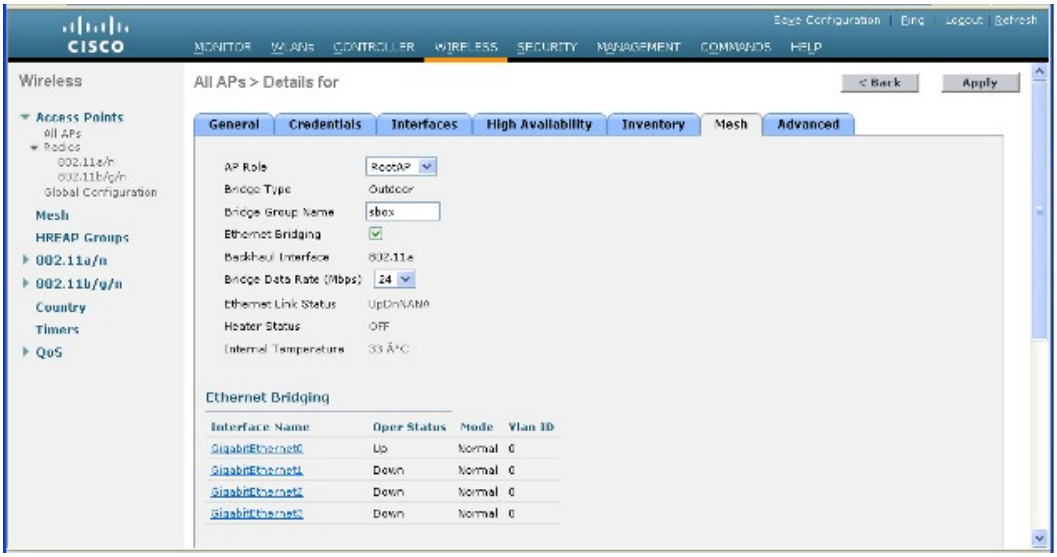
GUI を使用してメッシュ アクセス ポイントのロールを設定する手順は、次のとおりです。

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 *32*：*[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 1550 series access points, enter “Cisco AP c1550”
For Cisco 1520 series access points, enter “Cisco AP c1520”
For Cisco 1240 series access points, enter “Cisco AP c1240”
For Cisco 1130 series access points, enter “Cisco AP c1130”
```

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 進数文字列は、下に示すように TLV 値を連結することによって作成されたものです。

型 + 長さ + 値

タイプは、常に f1（16 進数）です。長さ 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。値 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 を持ったコントローラが 2 つあるとします。型は、f1（16 進数）です。長さは、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され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守し、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 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 コントローラが失敗した場合は、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、およびセカンダリ 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 を待機し、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応答を受信した場合はそのコントローラに join します。時間の制限に達すると、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、リストで次に使用可能なコントローラからの discovery response を待機します。

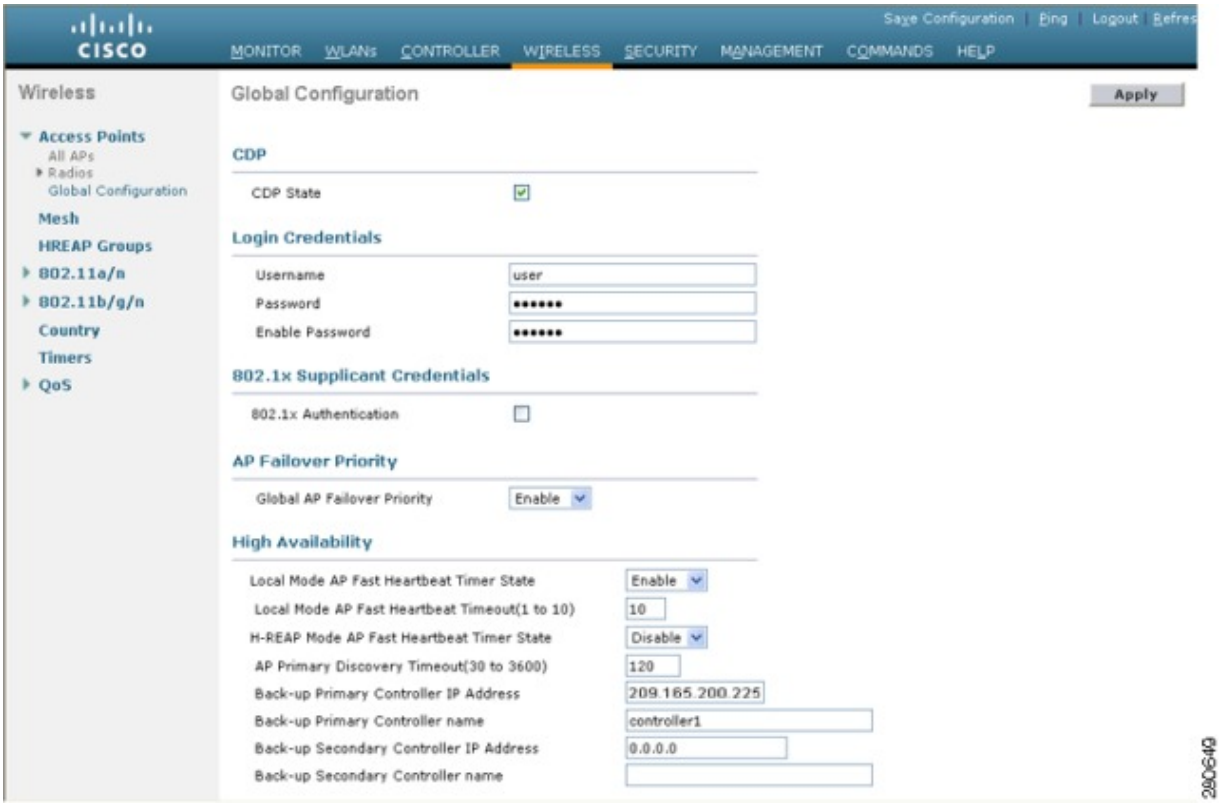
（注） メッシュ アクセス ポイントのプライマリ コントローラがオンラインに復帰すると、メッシュ アクセス ポイントはバックアップ コントローラとのアソシエーションを解除し、プライマリ コントローラに再接続します。メッシュ アクセス ポイントは、設定されているセカンダリ コントローラではなく、プライマリ コントローラにフォール バックします。たとえばプライマリ、セカンダリ、およびターシャリのコントローラを持つメッシュ アクセス ポイントが設定されている場合、プライマリとセカンダリのコントローラが応答なしになると、ターシャリ コントローラにフェール オーバーします。その後、プライマリ コントローラがオンラインに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 コントローラがオンラインに復帰しても、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。

バックアップ コントローラの設定（GUI）

コントローラの GUI を使用して、特定メッシュ アクセス ポイントのプライマリ、セカンダリ、およびターシャリのコントローラを設定し、すべてのメッシュアクセスポイントのプライマリおよびセカンダリのバックアップ コントローラを設定する手順は、次のとおりです。

ステップ 1 [Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます（図 33：[Global Configuration] ページ, （103 ページ）を参照）。

図 *33*：*[Global Configuration]* ページ



（注） メッシュ アクセス ポイントでは、ファスト ハートビート タイマーはサポートされていません。

ステップ 2 [AP Primary Discovery Timeout] フィールドで、30 ～ 3600 秒の範囲（両端を含む）の値を入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。デフォルト値は 120 秒です。

ステップ 3 すべてのアクセス ポイントにプライマリ バックアップ コントローラを指定する場合は、プライマリ バックアップ コントローラの IP アドレスを [Back-up Primary Controller IP Address] フィールドに指定し、コントローラの名前を [Back-up Primary Controller Name] フィールドに指定します。

（注） IP アドレスのデフォルト値は 0.0.0.0 であり、プライマリ バックアップ コントローラをは無効です。

ステップ 4 すべてのアクセス ポイントにセカンダリ バックアップ コントローラを指定する場合は、セカンダリ バックアップ コントローラの IP アドレスを [Back-up Secondary Controller IP Address] フィールドに指定し、コントローラの名前を [Back-up Secondary Controller Name] フィールドに指定します。

（注） IP アドレスのデフォルト値は 0.0.0.0 であり、セカンダリ バックアップ コントローラを無効にします。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 特定のアクセス ポイントのプライマリ、セカンダリ、およびターシャリのバックアップ コントローラを設定する手順は、次のとおりです。

a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
b) プライマリ、セカンダリ、およびターシャリ バックアップ コントローラを設定するアクセス ポイントの名前をクリックします。
c) [High Availability] タブをクリックします
d) 必要に応じて、このアクセス ポイントのプライマリ バックアップ コントローラの名前と IP アドレスを [Primary Controller] フィールドに指定します。

（注） この手順および次の 2 つの手順におけるバックアップ コントローラの IP アドレスの指定はオプションです。バックアップ コントローラが、メッシュ アクセス ポイントが接続されている Mobility Group（プライマリ コントローラ）の外部にある場合、プライマリ、セカンダリ、ターシャリのコントローラそれぞれの IP アドレスを入力する必要があります。コントローラ名および IP アドレスは、同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうしなければ、メッシュ アクセス ポイントがバックアップ コントローラに join できません。

e) 必要に応じて、[Secondary Controller] フィールドに、このメッシュ アクセス ポイントのセカンダリ バックアップ コントローラの名前と IP アドレスを指定します。
f) 必要に応じて、[Tertiary Controller] フィールドに、このメッシュ アクセス ポイントのターシャリ バックアップ コントローラの名前と IP アドレスを指定します。
g) [AP Failover Priority] の値を変更する必要はありません。メッシュ アクセス ポイントのデフォルト値は critical で、変更することができません。
h) [Apply] をクリックして、変更を確定します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

バックアップ コントローラの設定（CLI）

特定メッシュ アクセス ポイントのプライマリ、セカンダリ、およびターシャリのコントローラを設定し、すべてのメッシュ アクセス ポイントのプライマリおよびセカンダリのバックアップ コントローラを設定するには、コントローラの CLI で以下のステップを実行します。

ステップ 1 特定メッシュ アクセス ポイントのプライマリ コントローラを設定するには、次のコマンドを入力します。
config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

（注） このコマンドの *controller_ip_address* パラメータおよびそれに続く 2 つのコマンドはオプションです。バックアップ コントローラが、メッシュ アクセス ポイントが接続されている Mobility Group（プライマリ コントローラ）の外部にある場合、プライマリ、セカンダリ、ターシャリのコントローラそれぞれの IP アドレスを入力する必要があります。各コマンドで、*controller_name* および *controller_ip_address* は同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうしなければ、メッシュ アクセス ポイントがバックアップ コントローラに join できません。

ステップ 2 特定メッシュ アクセス ポイントのセカンダリ コントローラを設定するには、次のコマンドを入力します。
config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 3 特定メッシュ アクセス ポイントのターシャリ コントローラを設定するには、次のコマンドを入力します。
config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 4 すべてのメッシュ アクセス ポイントのプライマリ バックアップ コントローラを設定するには、次のコマンドを入力します。
config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

ステップ 5 すべてのメッシュ アクセス ポイントのセカンダリ バックアップ コントローラを設定するには、次のコマンドを入力します。
config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

（注） プライマリ、またはセカンダリ バックアップ コントローラ エントリを削除するには、コントローラの IP アドレスとして 0.0.0.0 を入力します。

ステップ 6 メッシュ アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定するには、次のコマンドを入力します。
config advanced timers ap-primary-discovery-timeout 間隔

interval の値は、30 ～ 3600 秒です。デフォルト値は 120 秒です。

ステップ 7 メッシュ アクセス ポイントのディスカバリ タイマーを設定するには、次のコマンドを入力します。
config advanced timers ap-discovery-timeout 間隔

interval の値は、1 ～ 10 秒です。デフォルト値は 10 秒です。

ステップ 8 802.11 認証応答タイマーを設定するには、次のコマンドを入力します。
config advanced timers auth-timeout 間隔

interval の値は、10 ～ 600 秒です。デフォルト値は 10 秒です。

ステップ 9 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 10 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 ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**
- show mesh config

show ap config general *Cisco_AP* コマンドに対しては、次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name........................ 1-5520
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 2-5520
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 3-5520
Tertiary Cisco Switch IP Address................. 1.1.1.4
```

show advanced backup-controllerコマンドに対しては、次のような情報が表示されます。

```
AP primary Backup Controller .................... controller1 10.10.10.10
AP secondary Backup Controller ................ 0.0.0.0
```

show advanced timers コマンドに対しては、次のような情報が表示されます。

```
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Primary Discovery Timeout (seconds)........... 120
```

show mesh config コマンドに対しては、次のような情報が表示されます。

```
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
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
```

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 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。

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

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。

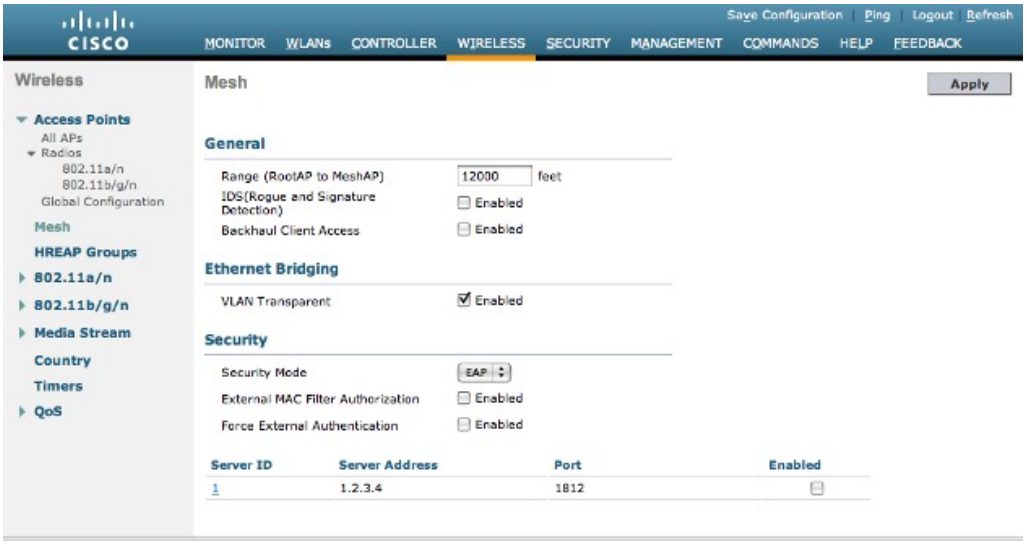
- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html（Windows）
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/（UNIX）

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イネーブルにする手順は、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 34：[Mesh] ページ, （109 ページ）を参照）。

図 *34*：*[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オンにします。

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。屋外 AP は、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場合、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 ポイントの場合、2 つのエントリ *platform_name_string-MAC_address* 文字列、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）

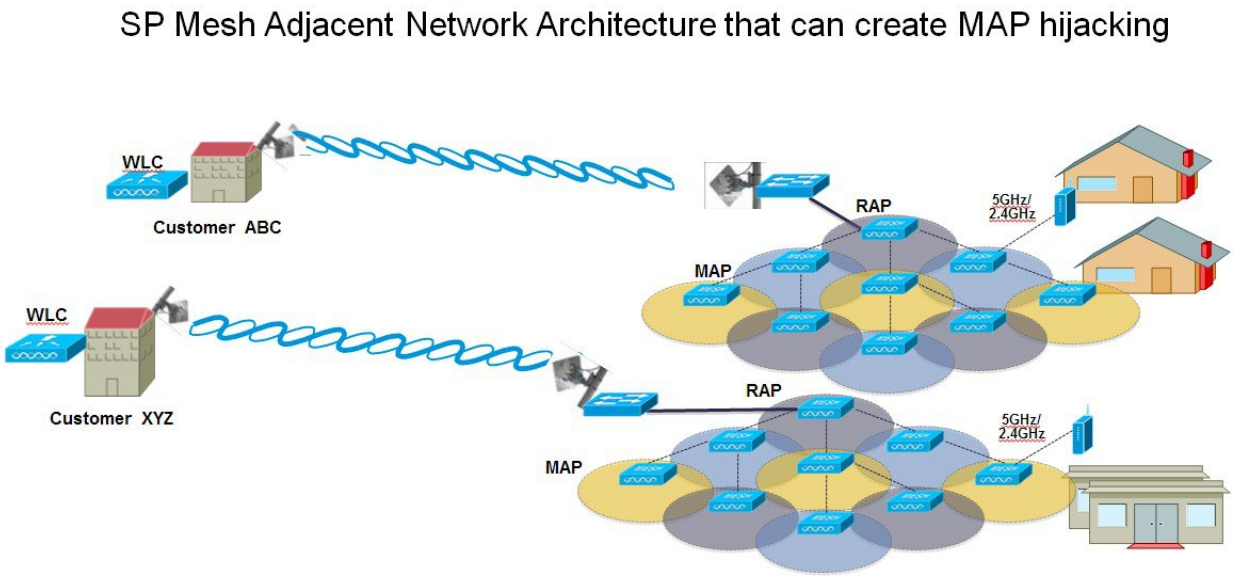
CLI を使用してメッシュ アクセス ポイントのセキュリティ統計を表示するには、次のコマンドを入力します。

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 でプロビジョニングするメッシュ PSK キー

Cisco Mesh 展開で顧客は、両方のメッシュ導入で MAP アソシエーションを許可するためにワイルドカードの MAC フィルタリングで AAA を使用する場合、メッシュ アクセス ポイント（MAP）が自分のネットワークを終了し、別のメッシュ ネットワークへ参加することを確認します。メッシュ AP のセキュリティが EAP-FAST を使用する可能性があるため、EAP セキュリティの場合、AP の MAC アドレスとタイプの組み合わせが使用されて使用可能な制御設定がないため、制御できません。デフォルトのパスフレーズの PSK オプションはセキュリティ リスクとハイジャックの可能性も示します。この問題は、MAP が移動車両（公共交通機関、フェリー、船など）に使用されるときに、2 つの異なる SP のオーバーラップ導入で顕著に現れます。この場合、SP のメッシュ ネットワークに「固定」するための MAP に制約事項がなく、MAP を別の SP ネットワークによってハイジャックする/慣れさせることができますが、導入で SP の対象カスタマーに対処することはできません。



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、このキーを使用します。特別な注意事項は、コントローラ ソフトウェア リリース 8.1 以下をアップグレードするかリリース 8.2 からダウンロードする場合に必要です。管理者は MAP のソフトウェアが PSK サポートの移行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

- WiSM-2、5500、7500 および 8500 シリーズ ワイヤレス LAN コントローラ
- AP をサポートするメッシュ AP 1550、1530 または 1570 シリーズおよびすべての屋内メッシュ。
- 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）。

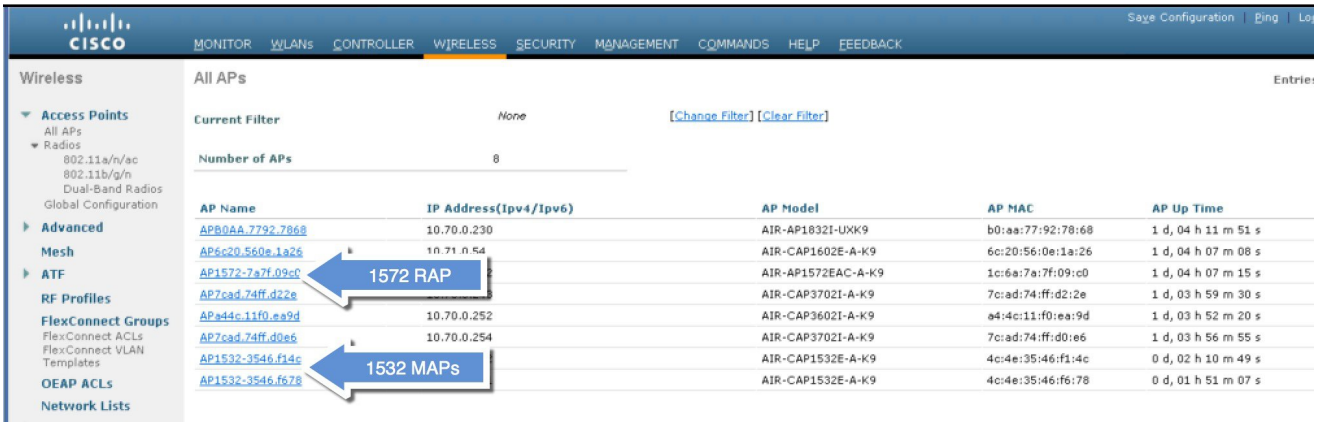
機能の設定手順

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 をデフォルト PSK キー「**cisco**」と組み合わせることはできません。

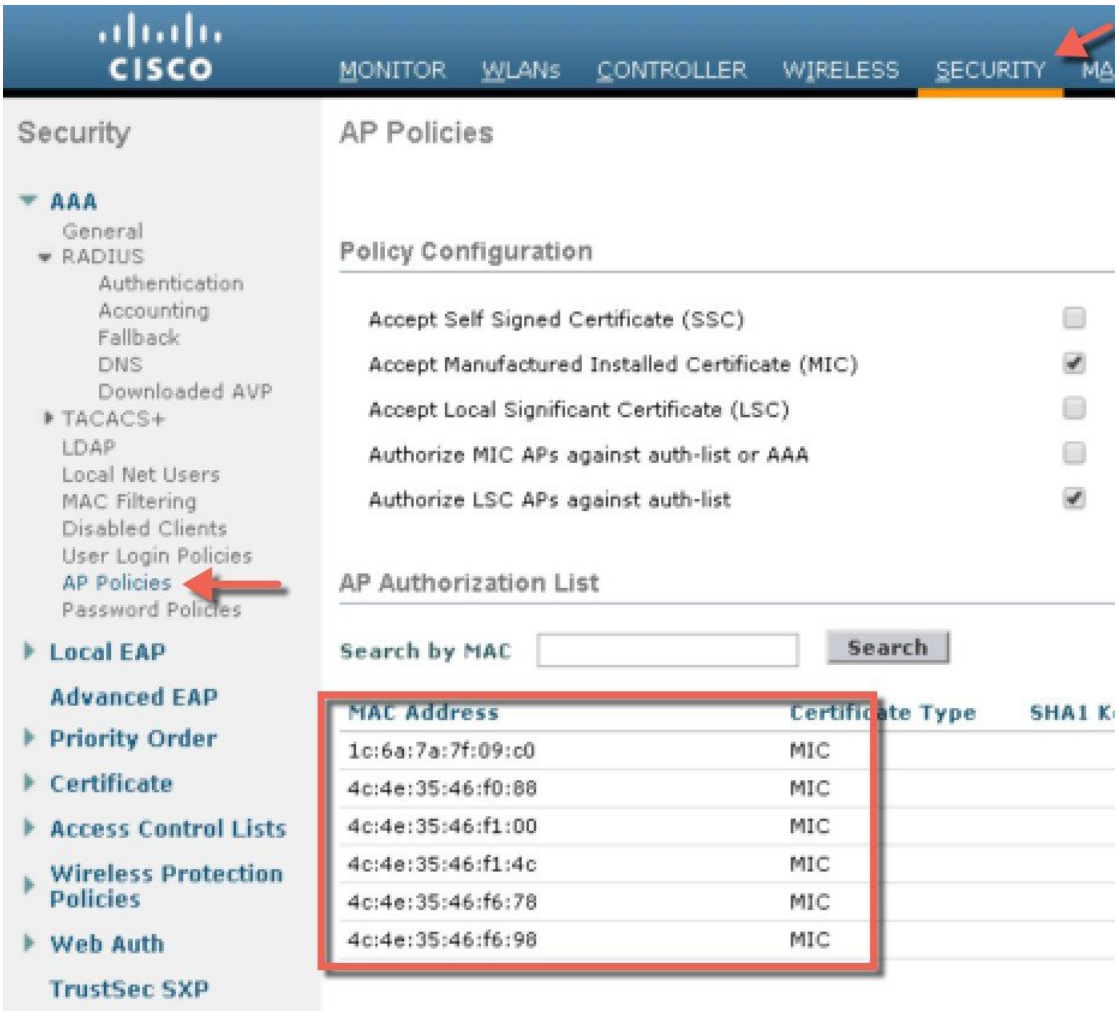
- プロビジョニングは、各 WLC にローカルであること
- ローカル プロビジョニングを可能にするために「有効化」された状態であること
- WLC に従うキー強度（小文字、大文字の特殊文字の組み合わせを含む英数字、長さ 3 ～ 32 文字、特殊文字をサポート、冗長なパスワードはサポートされない）。
- プロビジョニングされた PSK は、WLC で暗号化され、保存され、暗号化形式で AP に送信される。

メッシュ PSK GUI の設定

ステップ 1 この導入ガイドの上記の項で説明されている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のように 2 つの 1532 MAP が RAP 1572 に接続されます。



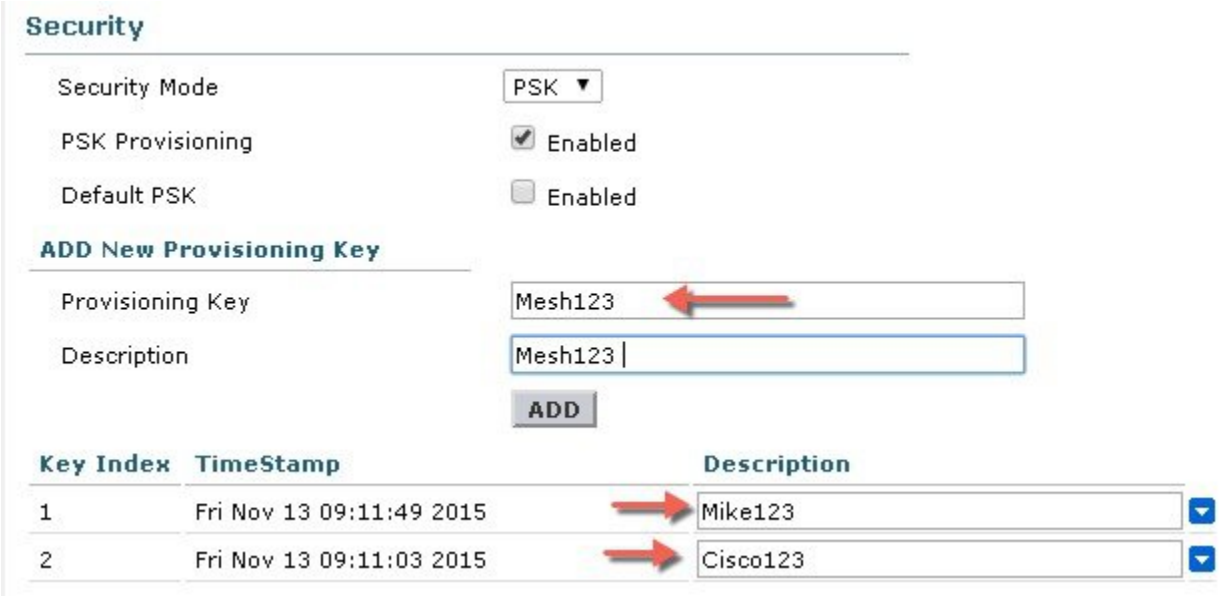
導入ガイドに示すように MAP の初期接続のオプションの 1 つは MAP の MAC アドレスをスクリーンショット に示したように RAP に接続されるこれらのコントローラに入力する必要があります。



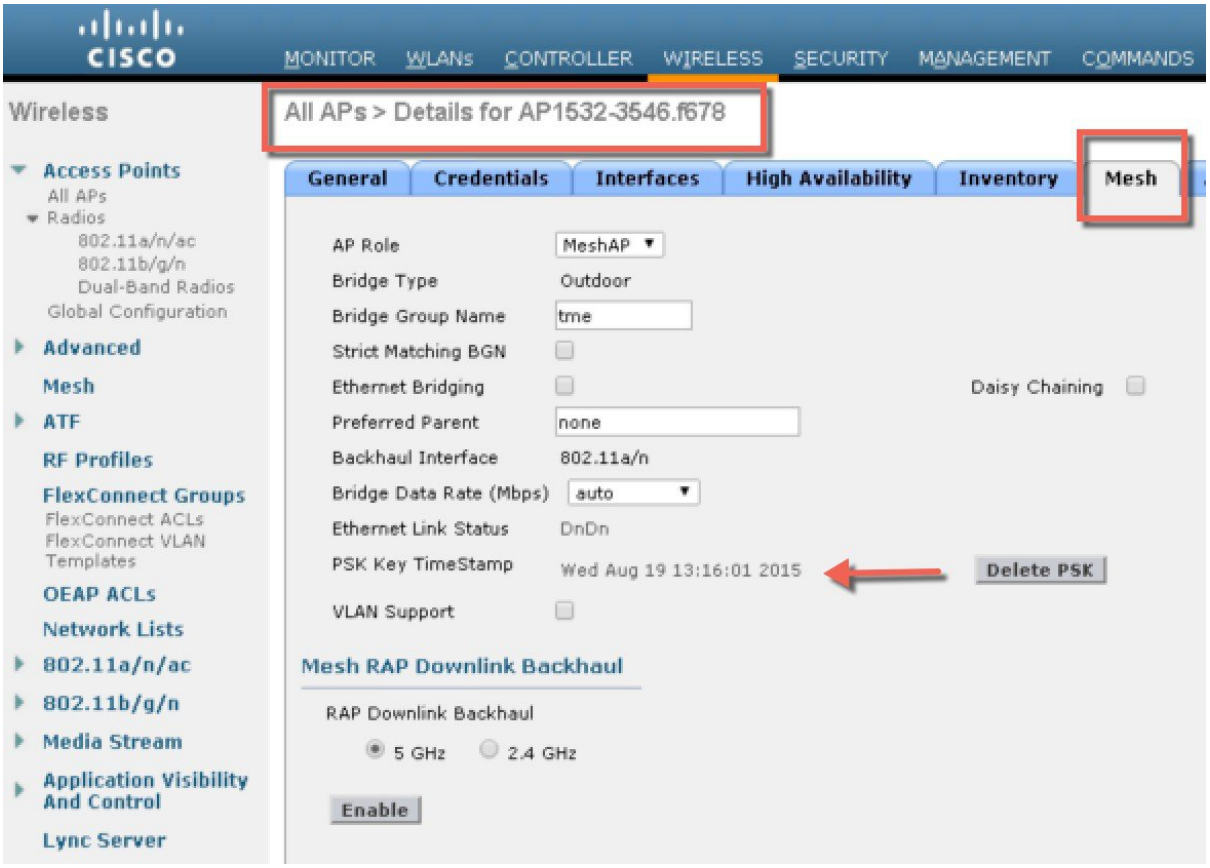
ステップ 2 [Wireless] > [Mesh] メニューから、PSK として [Security Mode] を選択し、[PSK Provisioning] を有効化します。

リリース 8.2 MAC 以前は、ワイルド カード文字を含む AAA 認証または EAP 認証は基本的に EAP がデフォルトの内部認証と共に使用される 3 つの方法しかなく、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には MAC アドレス プロビジョニングは十分には信頼できず、メッシュ AP が誤ってあるメッシュ ネットワークから他へ乗っ取られる高い可能性がありました。これによりメッシュ導入における問題やカバレッジ ホールを生じる可能性がありました。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。

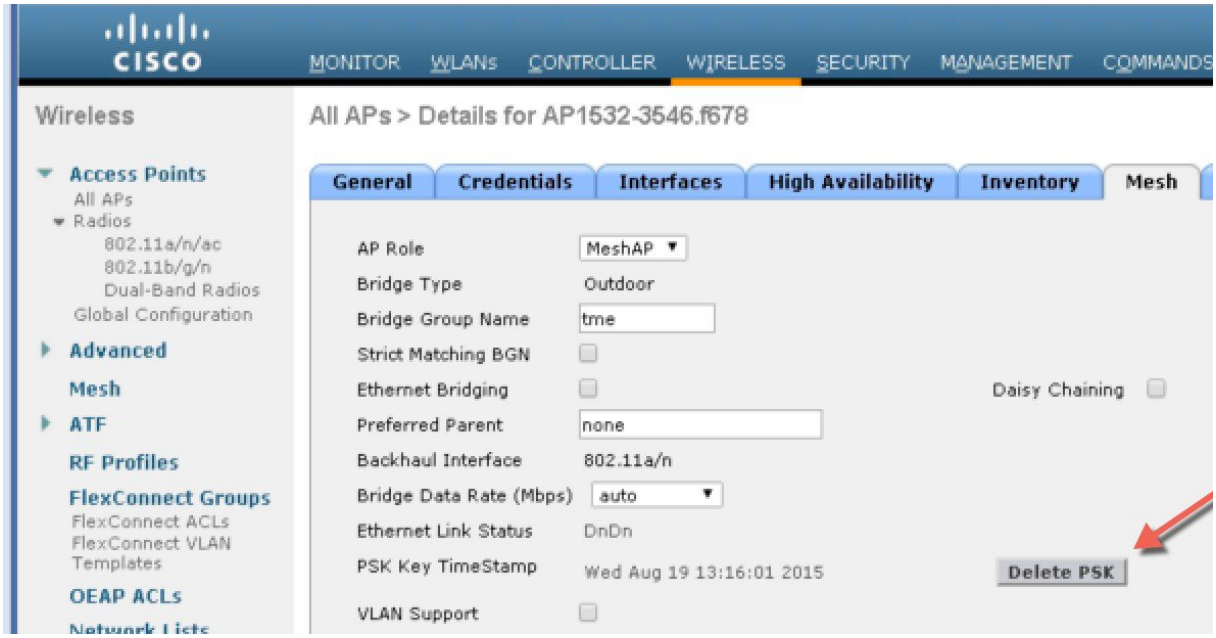
ステップ 3 例に示すようにプロビジョニング キーを入力して [ADD] を押下し、入力された値を適用します。
キーの値は一覧に表示されませんが、そのキーがコントローラにプロビジョニングされた時にタイム スタンプ付きのキーのインデックスだけが表示されます。最大 5 つのキーをプロビジョニングに使用される MAP のコントローラに入力できます。コントローラのフラッシュに常に保存されているこれらの 5 つのキーのいずれかを MAP がプロビジョニングのために使用できます。MD5 暗号化アルゴリズム（128-bit）がプロビジョニングされている PSK を暗号化するために使用され、新しいキーの設定時に AP に送信されます。



ステップ 4 コントローラが設定および有効化された PSK キーを持つと、キーは RAP に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。同じキーがメッシュ ネットワーク内の他のすべての子 MAP にも伝播されます。MAP では PSK キーの受信と RAP/MAP ネットワークへの認証のために何も行う必要はありません。
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 プロビジョニングされた PSK キーは、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には MAP または RAP から 削除できます。



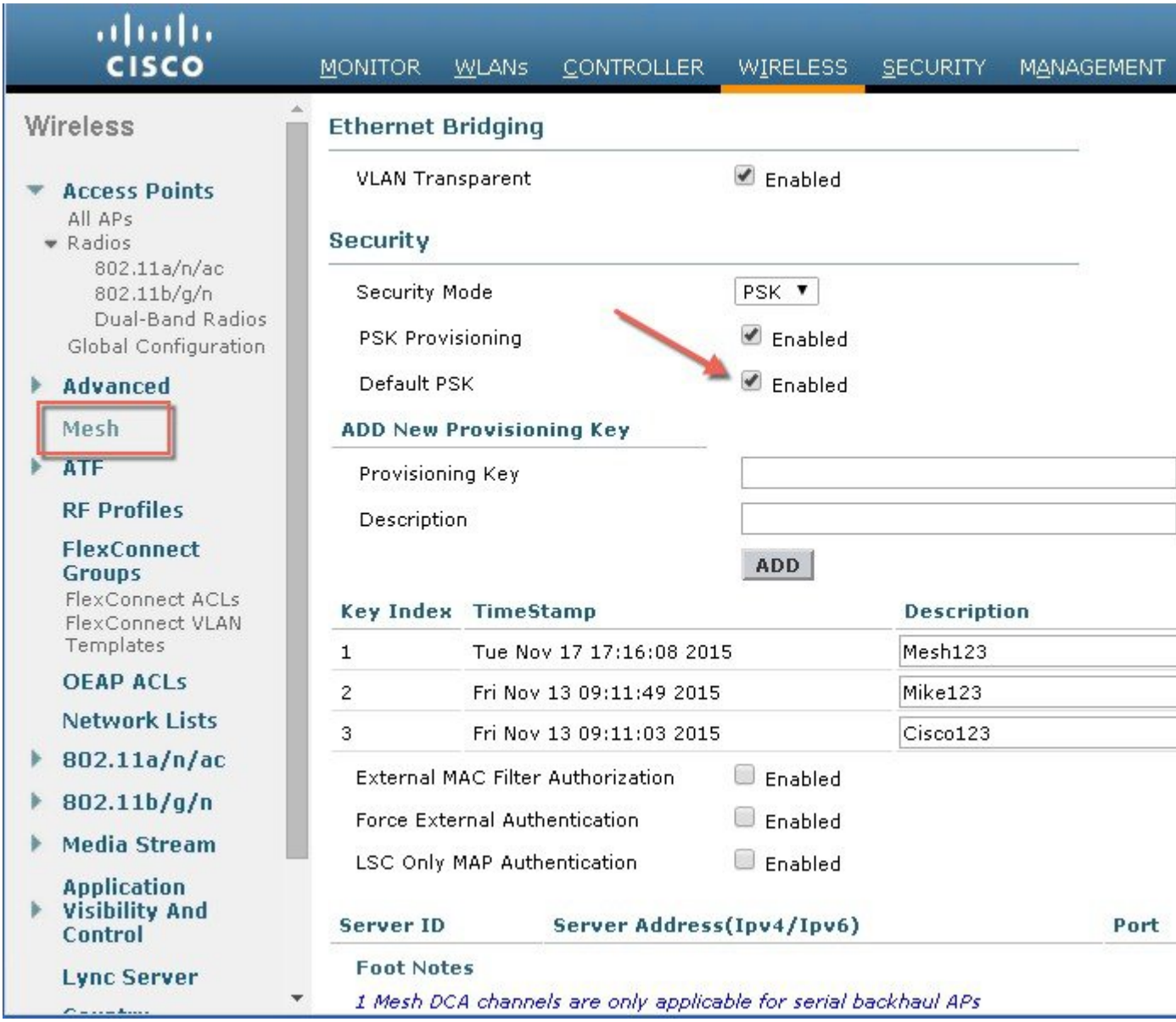
ステップ 6 MAP が誤ったネットワークに誤って接続し、そこからキーを取得した場合、管理者には誤った PSK キーを削除するオプションがあります。さらに、EAP セキュリティで参加すると、WLC GUI インターフェイスで PSK タイムスタンプの [Delete PSK] を使用して AP のプロビジョニングされた PSK を削除できます。このオプションは、AP が陳腐化して孤立状態になるか、無効な PSK および EAP セキュリティを使用して孤立状態のメッシュ AP に再参加した場合のメッシュ AP リカバリ オプションです。PSK キーが MAP から削除されると、デフォルト PSK キー「cisco」の使用に戻ります。

（注）

- パスフレーズ「cisco」を使用して PSK を設定することは、「デフォルトの cisco PSK」と同等であることを意味しません。プロビジョニングされた PSK は、「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、順番に RAP/MAP でも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ないことに注意してください。プロビジョニングされていない MAP をコントローラで PSK を有効化したメッシュ ネットワークに接続するために、[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化すると、デフォルトの「cisco」PSK キーを使用して MAP を接続可能になり、同時に新しい PSK キーを取得します。



（注） デフォルトの PSK キーを持つ MAP がプロビジョニングされたメッシュ ネットワークに接続しないように管理者がデフォルトの [Provisioning] ウィンドウを無効化することはメッシュにとって重要です。

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 を使用して参加しようとするが、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 の説明を常に書き込むことで後で思い出すことができます。またプロビジョニングされた PSK またはリカバリを保存すると AP で実行が必要になります。）

モビリティ グループのコントローラでメッシュ PSK のプロビジョニング

モビリティ グループで RAP の設定がある場合、同じ PSK キーまたはモビリティ グループのすべてのコントローラの 5 つの許容される 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。この方法では、異なるコントローラからの MAP の場合に認証できるようになります。PSK のスタンプを見ると MAP および PSK キーがどこから来たかを確認できます。

マルチコントローラの設定で PSK または EAP セキュリティ付きのメッシュ 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。

  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 事前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よう設定する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指定
- 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 *18*：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） この機能をイネーブルにすると、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。 この機能をディセーブルにすると、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 設定でアクティブ化されます。

パラメータ	説明
Backhaul Client Access	（注） このパラメータは、2 つ以上の無線があるメッシュ アクセス ポイント（1552、1240、1130、および 11n 屋内メッシュ AP）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、バックホール無線を介したワイヤレス クライアント アソシエーションが許可されます。通常、バックホール無線は、ほとんどのメッシュ アクセス ポイントで 5 GHz 無線です。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。 バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは 2 番目の無線のみを介して送信されます。 **デフォルト**：無効 （注） この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。
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、「拡張機能の設定」の項を参照してください。 VLAN 透過が有効な場合は、VLAN タグが処理されず、パケットがタグなしパケットとしてブリッジされます。 （注） VLAN 透過が有効な場合、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 透過が無効な場合は、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） 通常、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オフにする必要があります。 （注） デフォルトでは VLAN トランスペアレントがイネーブルになっており、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**：イネーブル

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

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 レポートをイネーブルまたはディセーブルにするには、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（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イネーブルまたはディセーブルにするには、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、バックホール無線を介したワイヤレス クライアント アソシエーションが許可されます。通常、バックホール無線はメッシュ アクセス ポイントのほとんどで 5 GHz です。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

  バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは 2 番目の無線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 レポートの状態がイネーブルかディセーブルかを示します。

```
(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
```

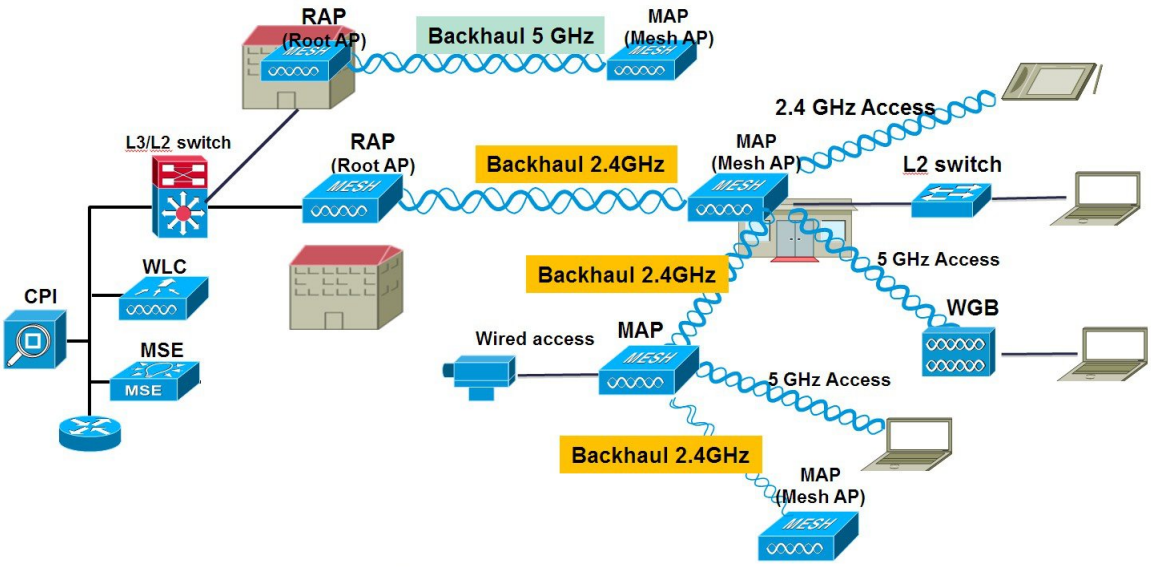
リリース 8.2 の 5 および 2.4 GHz のメッシュ バックホール

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することはできません。また 5 GHz 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距離を達成するために顧客が 2.4 GHz の無線周波数を好んで使用する場合があります。

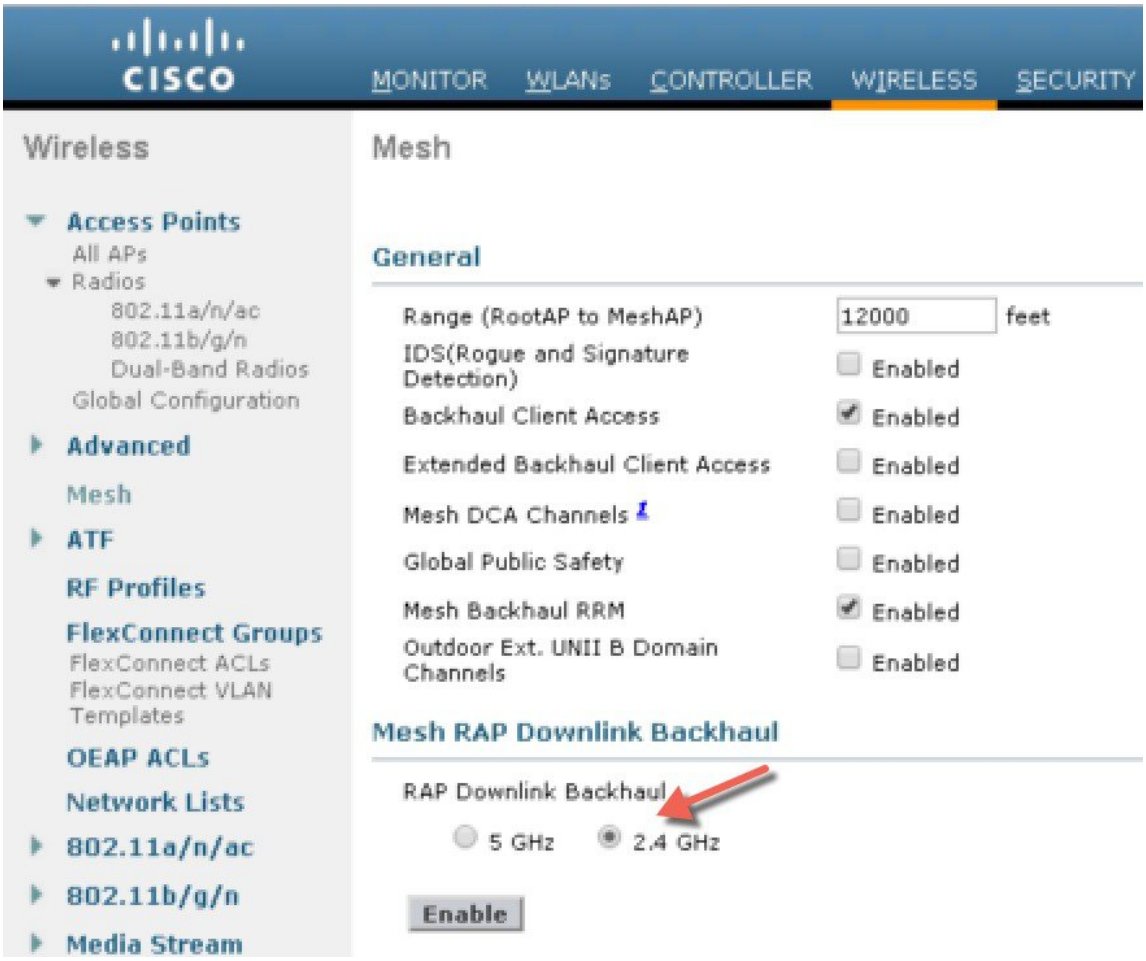
RAP が 5 GHz から 2.4 GHz へ設定の変更を取得すると、その選択が RAP からすべての MAP に送信され、5 GHz ネットワークから切り離されて 2.4 GHz に再接続されます。2.4 GHz を設定すると、2.4 GHz のバックホールが認識されるようにすべてのコントローラがバージョン 8.2 で設定されることに注意してください。

（注） RAP だけが 5 または 2.4 GHz のバックホール周波数に設定されます。RAP が設定されると、この周波数選択がすべての MAP にブランチを伝播します。



ステップ 1 メッシュ バックホールを 2.4 GHz に設定するには、コントローラ上の 1 つの簡単な手順が必要です。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。

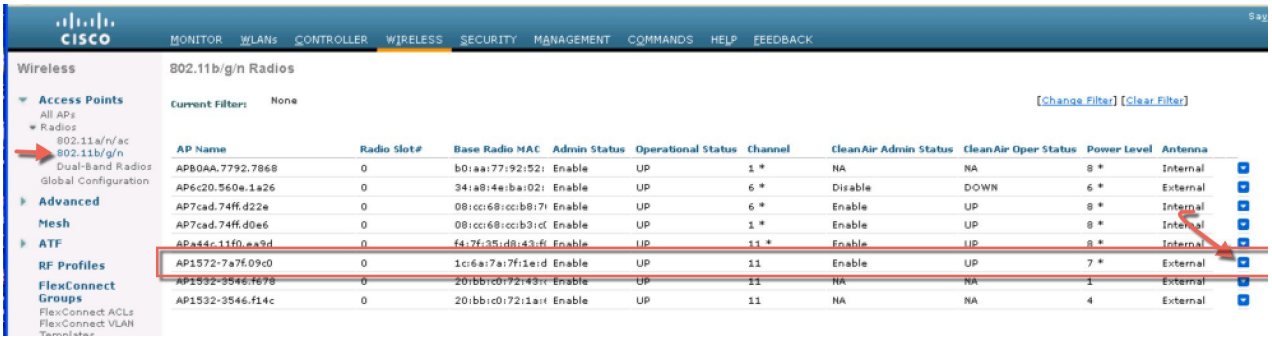
（注） 以下の例では、コントローラのグローバルの 2.4 GHz を示します。グローバル コンフィギュレーションでこれを行うと、すべてのメッシュ RAP に適用されます。チャネルのプロビジョニングは、個別の RAP でも行うことができ、この場合チャネルのプロビジョニングは親と子のこの特定の RAP ブランチにのみ適用されます。



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。

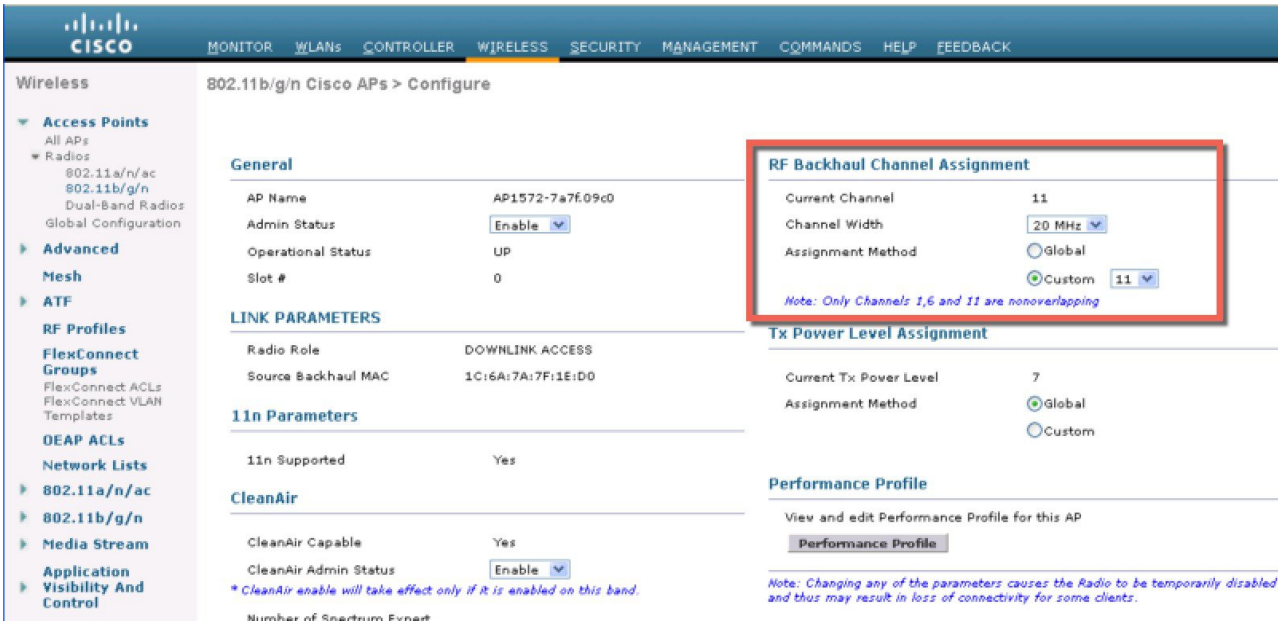
```
(5520-MA1) >show mesh ap tree

 ========================================================
||   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 に変更する必要があり、チャネルは選択されたカスタムである必要があります。またこの選択はすべての MAP とその RAP のブランチの「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それに固定されます。

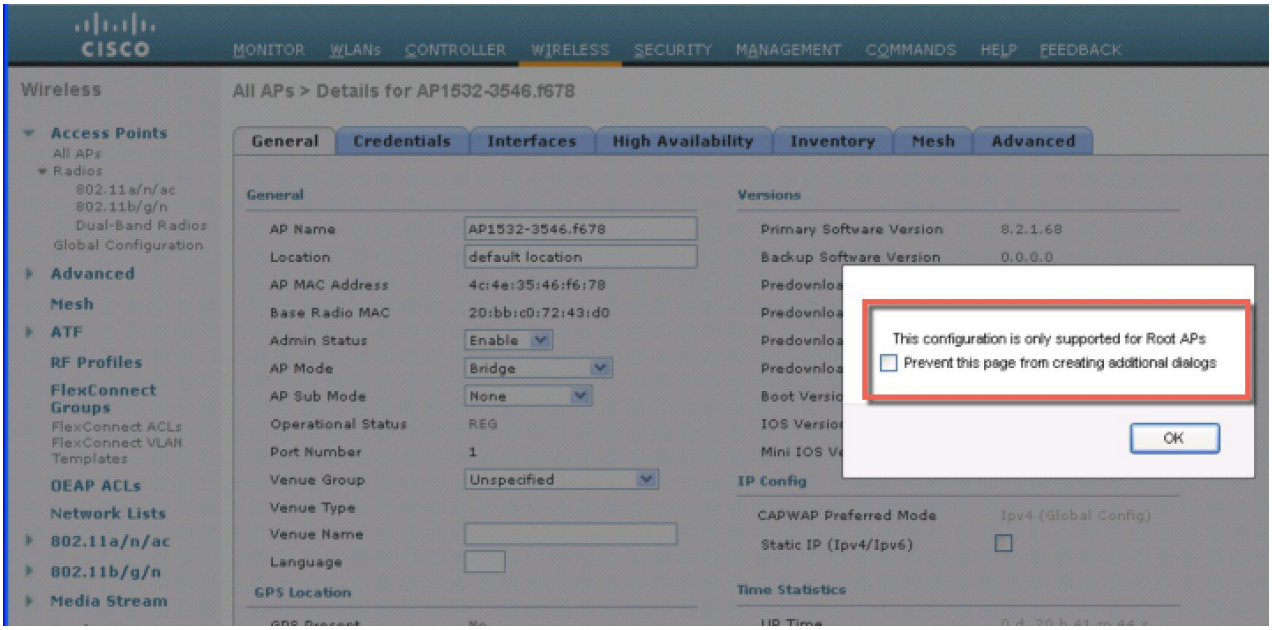


次の例に示すように、RAP でチャネル変更後は、MAP のチャネルが 2.4 GHz 帯域の CH11 に 変更されています。

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、バックホール無線を介したワイヤレス クライアント アソシエーションが許可されます。バックホール無線は 5 GHz 無線です。つまり、

バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは 2 番目の無線のみを介して送信されます。

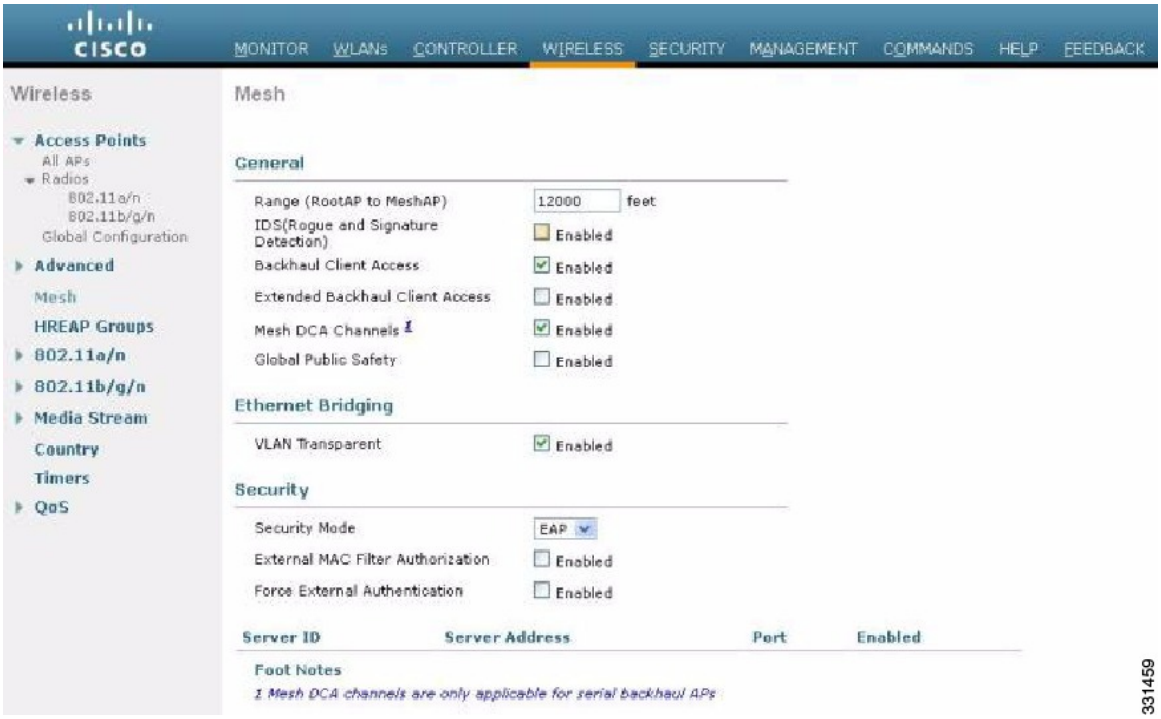
（注） バックホール クライアント アクセスはデフォルトで無効になります。この機能を有効にすると、デイジーチェーン導入のスレーブ AP と子 AP を除くすべてのメッシュ アクセス ポイントは再起動します。

この機能は、2 つの無線を使用するメッシュ アクセス ポイント（1552、1532、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 アクセスをイネーブル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 *35*：*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



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)
```

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、ネットワークで使用中の機能について次のローカル 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 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。
- 電源およびチャネル設定。「電力およびチャネルの設定」の項を参照してください。
- アンテナ ゲイン設定。「アンテナ ゲインの設定」の項を参照してください。
- 動的チャネル割り当て。「動的チャネル割り当ての設定」の項を参照してください。

ワイヤレス バックホール 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作成するために使用されます。バックホール インターフェイスは、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推測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延長できます。結果として、データ レートはセル カバレッジと必要なアクセス 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（より高いレートは、すべてのレートに影響を与える状況のためではなくそのレートに適切でない状況のため、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。

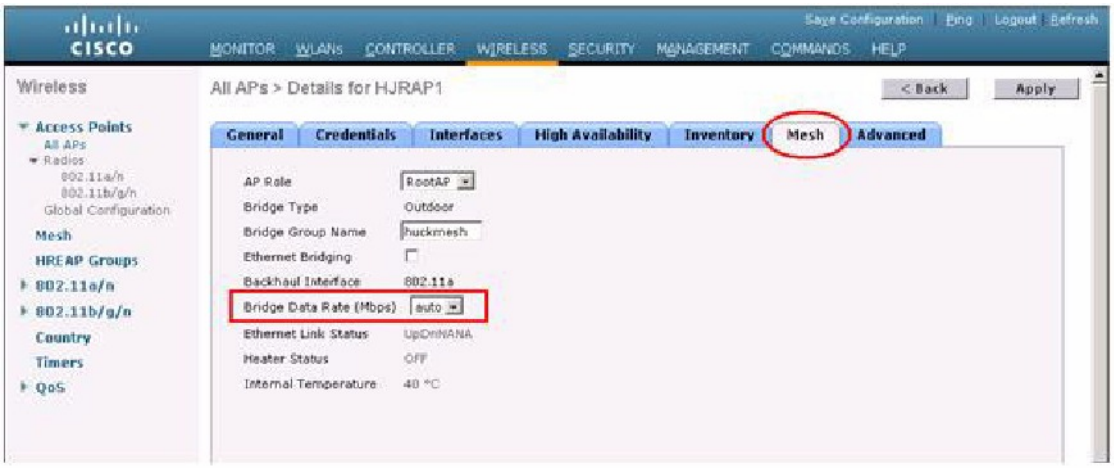
メッシュ バックホールを「Auto」に設定することをお勧めします。

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 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。

この図に、RAP が「Auto」バックホール データ レートを使用し、現在、子 MAP と 54 Mbps を使用していることを示します。

図 *36*：自動に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、バックホール無線の数など）によって異なります。

（注） 1552 802.11n を使用すると、スループットが向上し、キャパシティが増加します。最初に RAP から非常に太いバックホール パイプが提供されます。

図 *37* : ***AP1552*** バックホール スループット

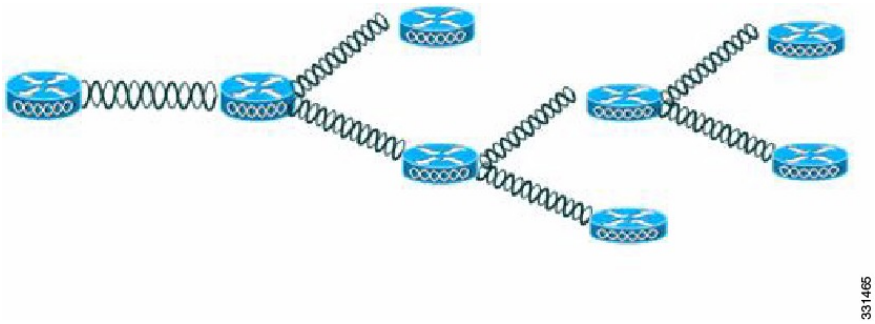


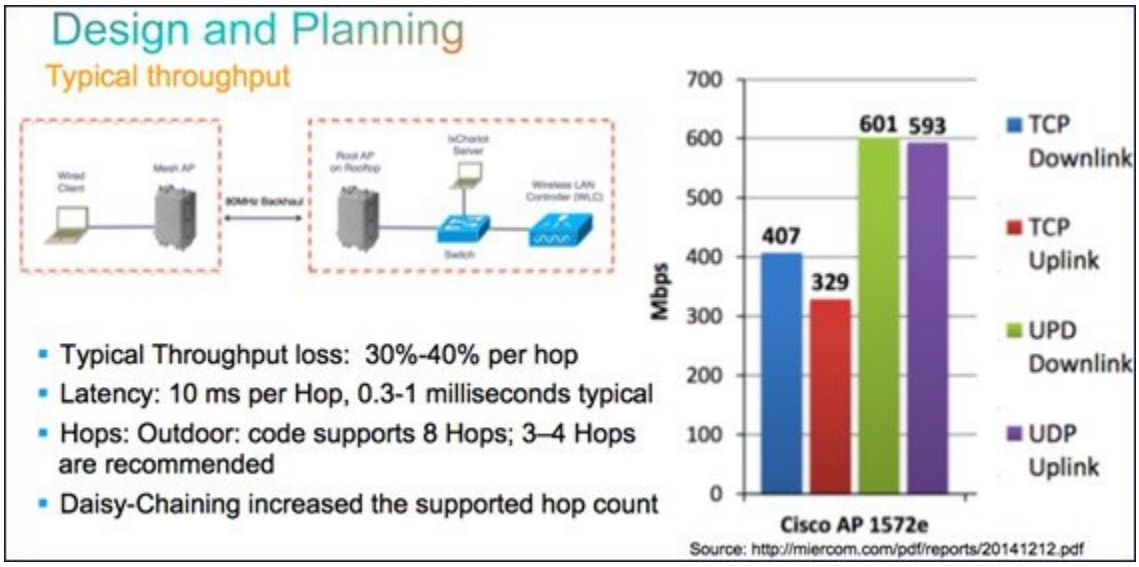
表 *19* : ***AP1552*** バックホール キャパシティ

Hops	RAP	1	2	3	4
最大スループット（20 MHz BH）	112 Mbps	83 Mbps	41 Mbps	25 Mbps	15 Mbps
最大スループット（40 MHz BH）	206 Mbps	111 Mbps	94 Mbps	49 Mbps	35 Mbps

上記に関する要件は次のとおりです。

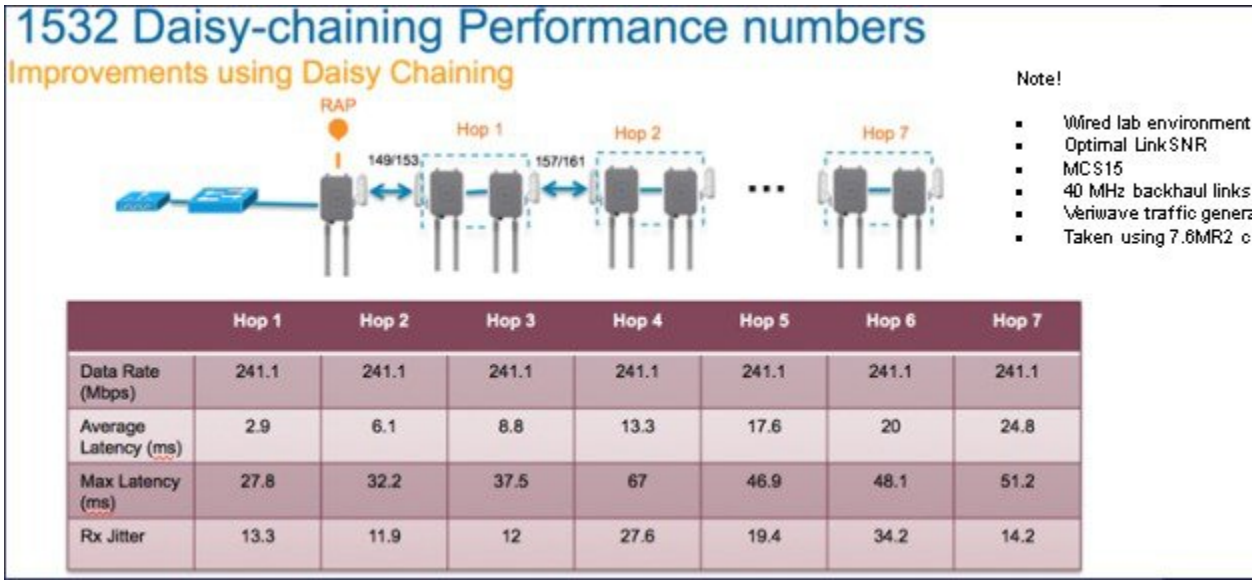
- パケット サイズは 1370 バイト（Veriwave クライアント）
- 5 GHz 802.11n
- MCS 15
- パケット損失は 1 % 未満
- クライアント アクセスおよびバックホール用の SNR が 40 dB を超える
- UDP トラフィック、セキュリティ有効、およびユニバーサル アクセス有効

1572 バックホール容量数



詳細については、http://miercom.com/pdf/reports/20141212.pdf を参照してください。

デイジーチェーンを使用した **1532** バックホール容量



	Hop 1	Hop 2	Hop 3	Hop 4	Hop 5	Hop 6	Hop 7
Data Rate (Mbps)	241.1	241.1	241.1	241.1	241.1	241.1	241.1
Average Latency (ms)	2.9	6.1	8.8	13.3	17.6	20	24.8
Max Latency (ms)	27.8	32.2	37.5	67	46.9	48.1	51.2
Rx Jitter	13.3	11.9	12	27.6	19.4	34.2	14.2

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。

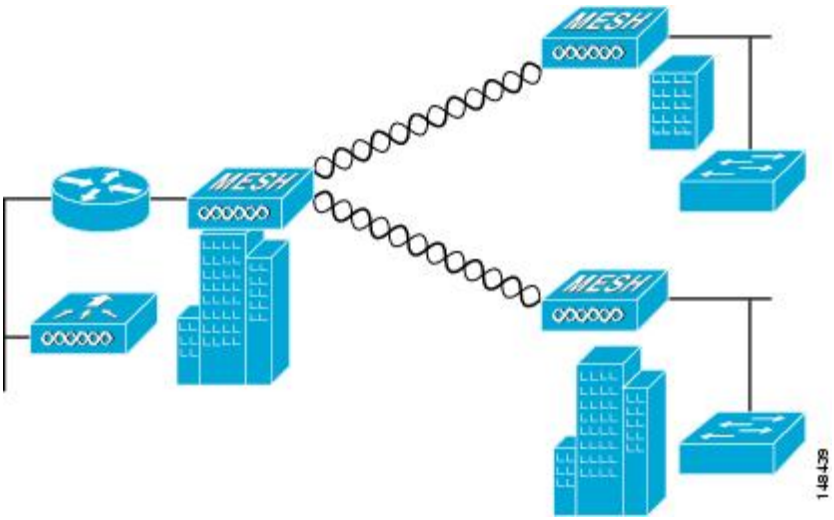
イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

1. メッシュ ノードをブリッジとして使用する場合（図 38：ポイントツーマルチポイント ブリッジング，（138 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 *38*：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）

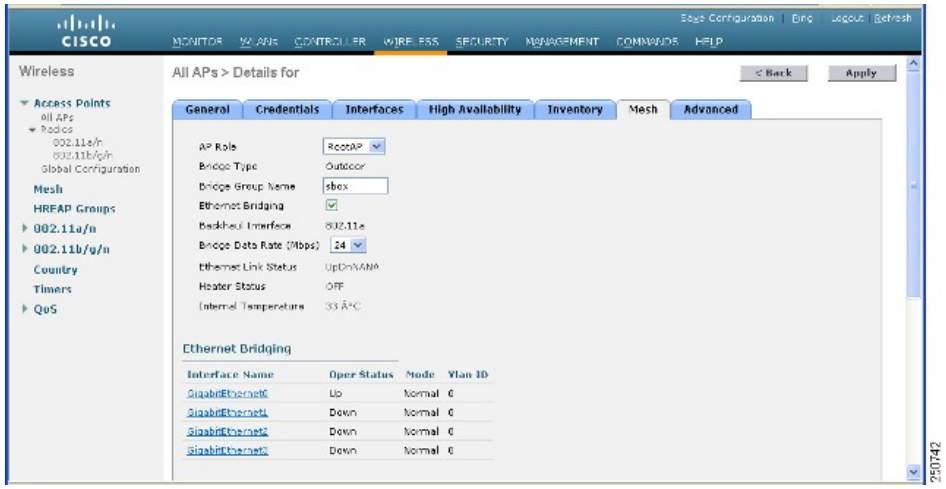
GUI を使用して RAP または MAP でイーサネット ブリッジングをイネーブルにする手順は、次のとおりです。

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 39：[All APs > Details for]（[Mesh]）ページ，（139 ページ）を参照してください）。

図 *39*：*[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オンにします。この機能を無効にする場合は、このチェックボックスをオフにします。

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を取る各親メッシュ 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オンにします。

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。

これは、アクセス ポイントにネイティブ VLAN 設定を適用します。

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アソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておくと、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、工場で設定されているデフォルトです。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 ポイントがリブートします。

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

Cisco 3200 との相互運用性の設定

Cisco AP1522 および AP1524PS は、Public Safety チャネル（4.9 GHz）と、2.4 GHz アクセスおよび 5.8 GHz バックホールで、Cisco 3200 と相互運用できます。

Cisco 3200 は車載ネットワークを作成します。車載ネットワークでは、PC、監視カメラ、デジタル ビデオカメラ、プリンタ、PDA、スキャナなどの装置が、メインのインフラストラクチャへと接続されている携帯電話ベースまたは WLAN ベースのサービスなどのワイヤレス ネットワークを共有できます。この機能により、警察車両などの車載展開から収集されたデータをワイヤレス インフラストラクチャ全体に統合できます。

この項では、Cisco 3200、AP1522、および AP1524PS 間の相互運用性を設定する際のガイドラインと詳細な手順について説明します。

1130、1240、および 1520（1522、1524PS）シリーズのメッシュ アクセス ポイントと Cisco 3200 との間の具体的な相互運用性の詳細については、表 20：メッシュ アクセス ポイントと Cisco 3200 の相互運用性, （142 ページ） を参照してください。

表 *20*：メッシュ アクセス ポイントと *Cisco 3200* の相互運用性

メッシュ アクセス ポイントのモデル	Cisco 3200 のモデル
1552、1522[8]	c3201[9]、c3202[10]、c3205[11]
1524PS	c3201、c3202
1524SB、1130、1240、屋内 802.11n メッシュ アクセス ポイント	c3201、c3205

8 Cisco 3200 に 802.11a 無線または 4.9 GHz 帯域で接続する場合は、AP1522 でユニバーサル アクセスが有効である必要があります。
9 モデル c3201 は 802.11b/g 無線を搭載した Cisco 3200 （2.4 GHz）です。
10 モデル c3202 は 4 ～ 9 GHz サブバンド無線を搭載した Cisco 3200 です。
11 モデル c3205 は 802.11a 無線を搭載した Cisco 3200 （5.8 GHz サブバンド）です。

Public Safety 4.9 GHz 帯域の設定ガイドライン

AP1522 または AP1524PS と Cisco 3200 を Public Safety ネットワークで相互運用するには、次の設定時のガイドラインを満たす必要があります。

- 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）。この機能は AP1524PS ではサポートされません。
- 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 Public Safety への対応を有効にする必要があります。
- AP1522 または AP1524PS でのチャネル番号の割り当てが Cisco 3200 無線インターフェイスでの割り当てと一致する必要があります。
  - Cisco 3200 との相互運用性を実現するために、チャネル 20（4950 GHz）～ 26（4980 GHz）、およびサブバンド チャネル 1 ～ 19（5 および 10 MHz）が使用されます。この設定の変更はコントローラで行います。メッシュ 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 に対してのみ行われます。MAP へのアップデートは、RAP によって伝搬されます。

Cisco 3200 のデフォルトのチャネル幅は 5 MHz です。WGB が AP1522 と AP1524PS にアソシエートできるようにチャネル幅を 10 または 20 MHz に変更するか、または AP1522 または AP1524PS 上のチャネルを 5 MHz 帯域（チャネル 1 ～ 10）または 10 MHz 帯域（チャネル 11 ～ 19）のチャネルに変更するか、いずれかを行う必要があります。

- 無線（802.11a）は、チャネルの設定時に無効にし、CLI の使用時に再び有効にする必要があります。GUI を使用する場合、チャネルの設定時に 802.11a 無線をイネーブルおよびディセーブルにする必要はありません。
- Cisco 3200 は、5、10、または 20 MHz 帯域内のチャネルをスキャンできます。ただし、これらの帯域をまたがるようにはスキャンできません。

電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 チャネルに合わされます。ローカル アクセスは、MAP とは無関係に設定できます。

電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） 無線スロットは各無線に対して表示されます。

ステップ 2 802.11 a/n 無線の [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 無線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 無線の 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 つの電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電力レベルは最大電力レベル（レベル 1）です。

（注） Radio Resource Management（RRM）はデフォルトでオフ（無効）になります。バックホールでは RRM をオン（有効）にすることができません。

ステップ 5 電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 ゲインの設定

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 ゲインと一致するように、メッシュ アクセス ポイントのアンテナ ゲインを設定する必要があります。

アンテナ ゲインの設定（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ゲイン設定があります。

ステップ 3 [Antenna Parameters] セクションで、アンテナ ゲインを入力します。
ゲインは 0.5 dBm 単位で入力します。たとえば、2.5 dBm = 5 です。

（注） 入力するゲイン値は、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 ゲインの設定（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 AP_name*

ここで、ゲインは 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動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを、コントローラの GUI を使用して指定する手順は、次のとおりです。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制約事項があるために、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オフにします。

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、コントローラは必要に応じて 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 ポイント無線をデフォルトで帯域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、すべての無線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オンにすると、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オフにします。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オンにすると、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オフにします。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オンにすると、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オフにします。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、チャネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する 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 *21*：*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

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

ステップ 10 802.11a/n/ac 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 帯域のすべての 802.11n 無線でサポートするチャネル帯域幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）

（注） [802.11a/n Cisco APs] > [Configure] ページで 20 MHz モードのアクセス ポイントの無線を静的に設定することで、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ことができます。アクセス ポイント無線で静的 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] カラムでそのチャネルのチェックボックスをオンにします。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オフにします。
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 帯域の拡張 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オンにします。

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 帯域で 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] カラムでチェックボックスをオンにします。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オフにします。
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オンにします。
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無線の MAC アドレス、前のチャネルと新規のチャネル、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 無線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無線リソース管理の設定

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無線で有効にできます。

- 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、伝送パワーコントロール（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 に再度参加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 バックホール無線の 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

この項では、次のトピックについて取り上げます。

- イーサネット VLAN タギングの設定

- 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運用性
- クライアント ローミング
- 屋内メッシュ ネットワークの音声パラメータの設定
- ビデオのメッシュ マルチキャストの抑制の有効化

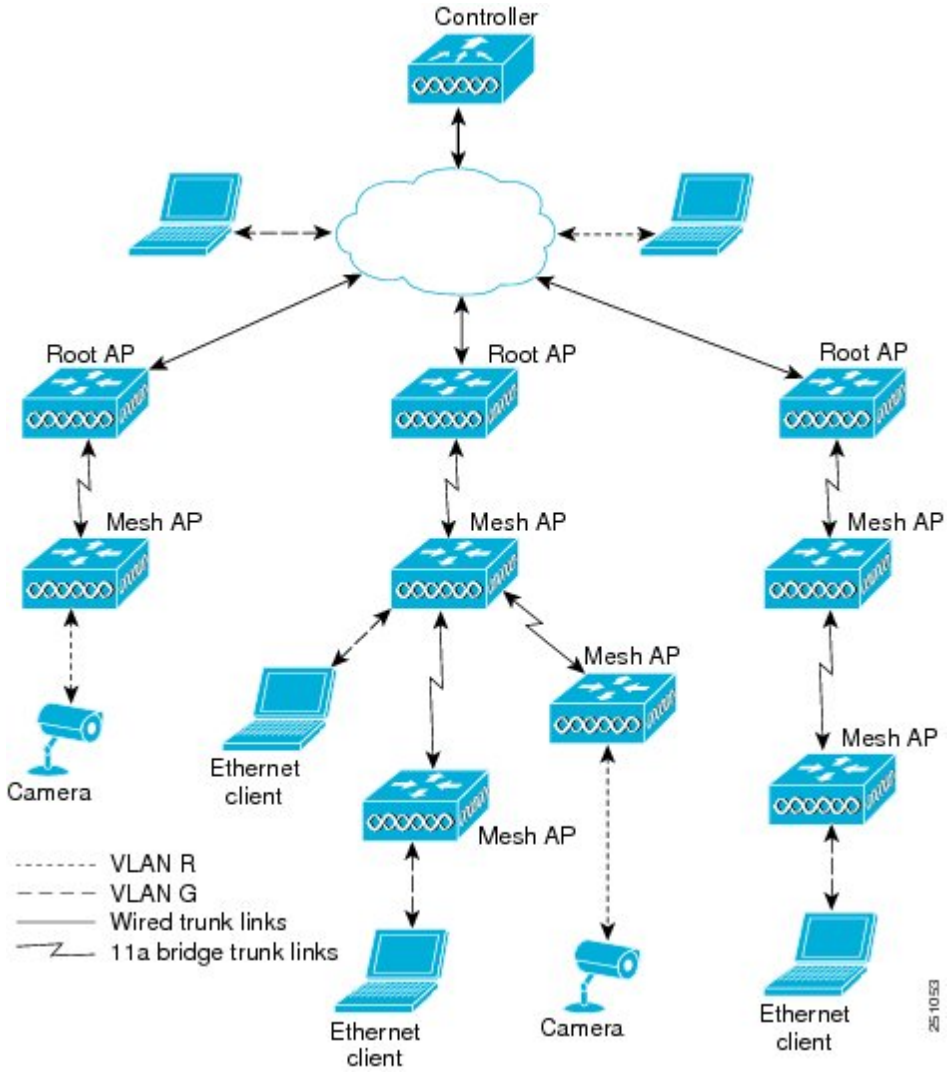
イーサネット VLAN タギングの設定

イーサネット VLAN タギングを使用すると、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 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 *40* : 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 透過が無効な場合、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 透過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 透過を無効にするには、「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 タギングの以下のガイドラインに従います。

- 安全上の理由により、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] オプションをオフにする必要があります。
- 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 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 透過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 タギングをイネーブルにする手順は、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オンに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）

- 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

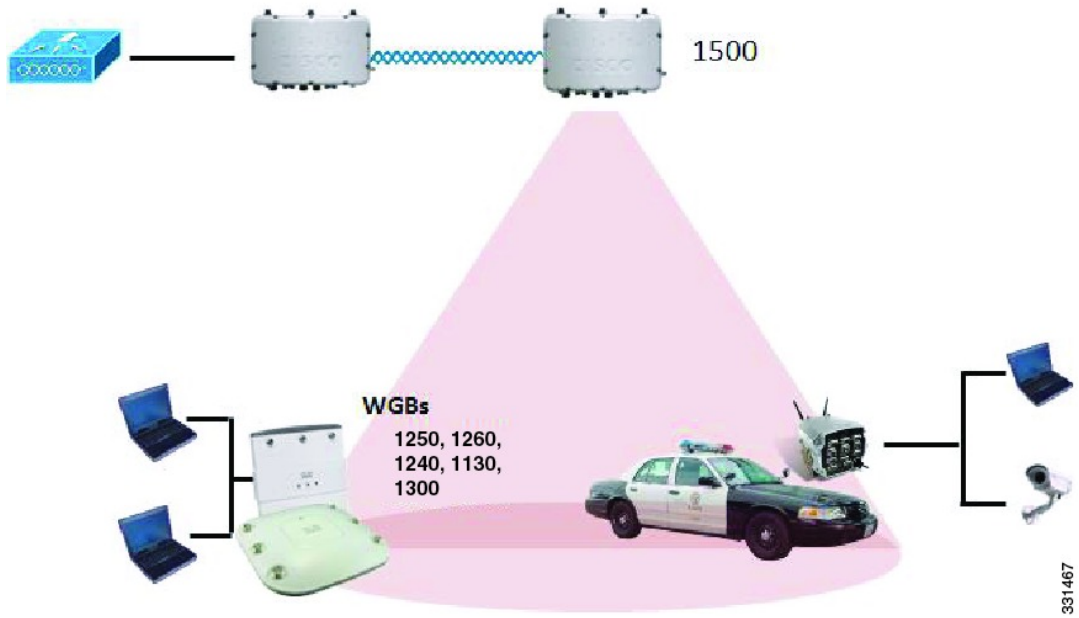
ワークグループ ブリッジとメッシュ インフラストラクチャとの相互運用性

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 にアソシエートされます。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無線でサポートされます。

図 *41*：*WGB* の例



現在のアーキテクチャでは、Autonomous AP は、ワークグループ ブリッジとして機能し、1 つの無線インターフェイスだけがコントローラ接続、有線クライアント接続用イーサネット インターフェイス、およびワイヤレス クライアント接続の他の無線インターフェイスに使用されます。コ

ントローラ（メッシュインフラストラクチャを使用）および有線クライアントのイーサネットインターフェイスに接続するには、dot11radio 1（5 GHz）を使用できます。dot11radio 0（2.4 GHz）は、ワイヤレス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 番目の無線のワイヤレス 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 つの無線を使用する場合、1 つの無線をクライアント アクセスに使用し、もう 1 つの無線をアクセス ポイントにアクセスするために使用できます。2 つの独立した無線が 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 番目の無線のワイヤレス クライアントはアソシエーション解除されません。一方の無線はルート AP（無線の役割）として設定し、もう一方の無線は WGB（無線の役割）として設定する必要があります。

（注） 一方の無線が WGB として設定された場合、もう一方の無線は 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での 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（802.11b/g）および 5 GHz（802.11a）無線の両方でサポートされます。

WGB はメッシュ アクセス ポイントに関連付けることができるため、設定されたサポートされるプラットフォームは自律 1600、1700、2600、2700、3600、3700、1530、1550、および 1570 です。設定手順については、『*Cisco Wireless LAN Controller Configuration Guide*』（http://www.cisco.com/

en/US/products/ps6366/products_installation_and_configuration_guides_list.html）の「Cisco Workgroup Bridges」の項を参照してください。

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アクセス ポイントでは Cisco IOS リリース 12.4.25d-JA 以降が実行され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。2 番目の無線を無効にすることをお勧めします。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。クライアント モード WGB では VLAN をトランクできませんが、インフラストラクチャ WGB ではトランクできます。
- 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 ポイントで一方の無線が WGB として設定された場合、もう一方の無線を 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、アソシエートされた WGB の背後で、ワイヤレス クライアント、WGB、および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 ポイントとアソシエートできません。

図 *42* : *WGB* の *WPA* セキュリティ設定

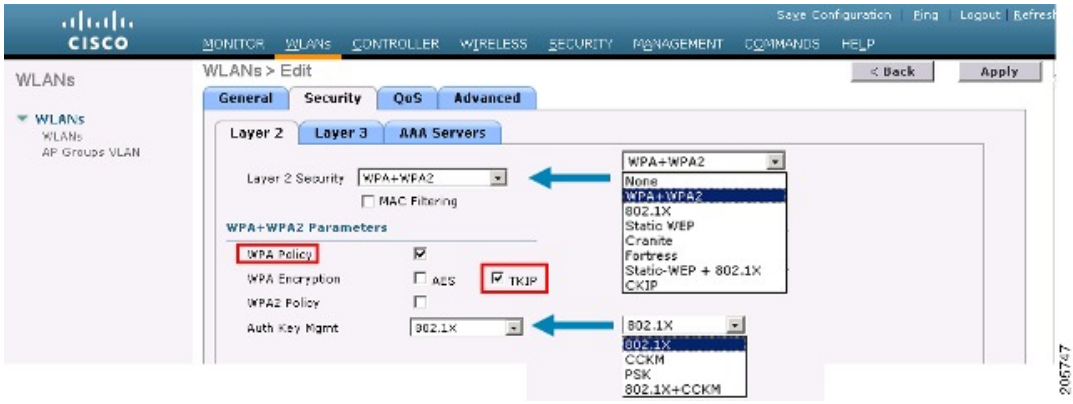
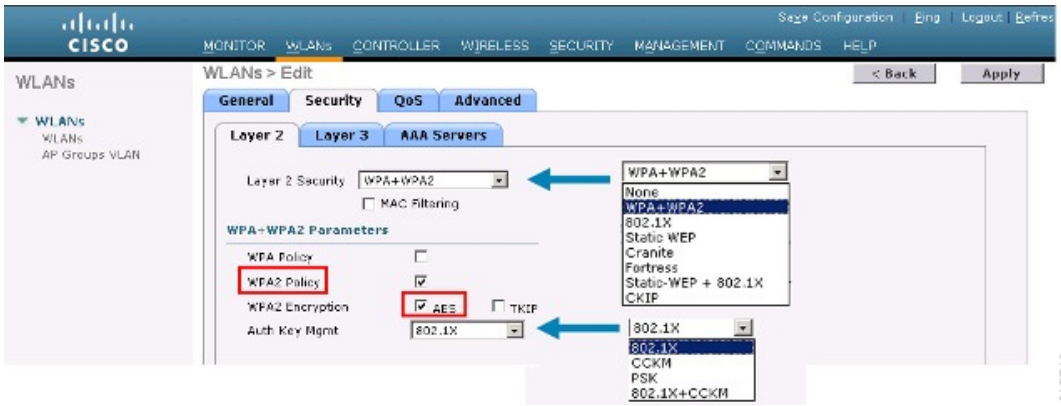


図 *43* : *WGB* の *WPA-2* セキュリティ設定



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 *44*：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 45：[Monitor] > [Clients] > [Detail] ページ（無線 WGB クライアントの場合），（161 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 46：[Monitor] > [Clients] > [Detail] ページ（有線 WGB クライアントの場合），（161 ページ） のようなページが表示されます。

図 *45*：*[Monitor] > [Clients] > [Detail]* ページ（無線 *WGB* クライアントの場合）

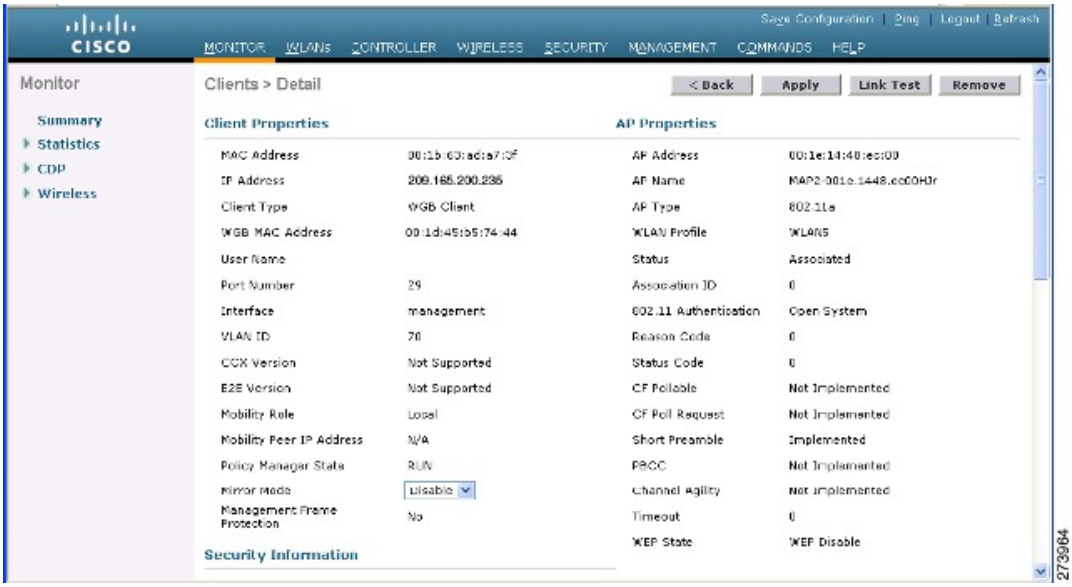
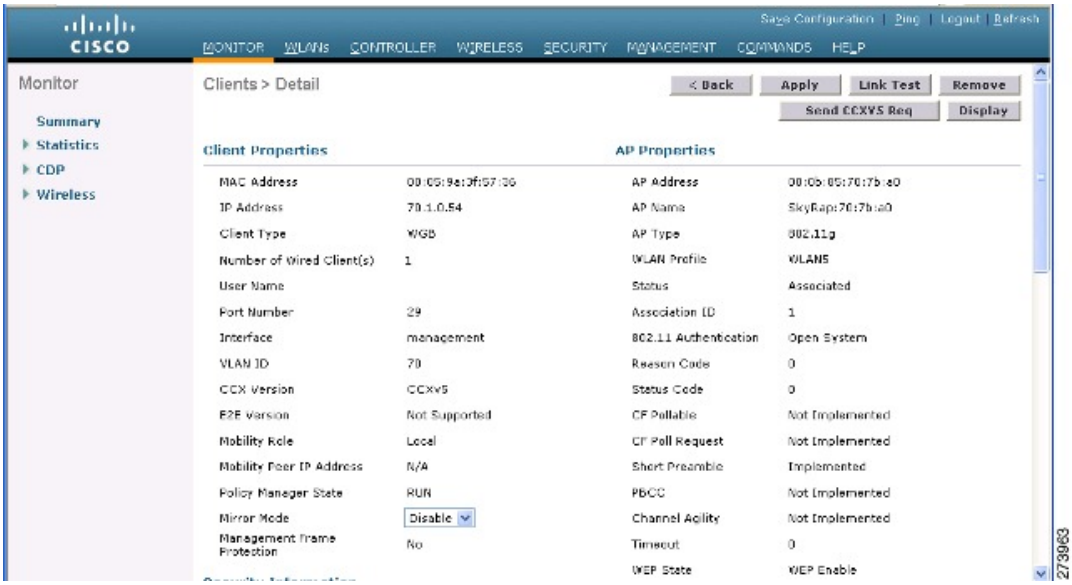


図 *46*：*[Monitor] > [Clients] > [Detail]* ページ（有線 *WGB* クライアントの場合）



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 無線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 無線を使用することをお勧めします。5 GHz 帯域を使用すると、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 つの無線がある WGB では、5 GHz 無線（無線 1）モードを WGB として設定します。この無線は、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 番目の無線 2.4 GHz（無線 0）モードをクライアント アクセスのルートとして設定します。
- 自律アクセス 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。自律側では、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 アソシエーションには 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 番目の無線（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。両方の無線で同じ 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 アソシエーションでは、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 が自律アクセス ポイントと対話する場合、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、WGB の背後にあるワイヤレス クライアントと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 AP から実行できます。
- WGB にアソシエートされたワイヤレス 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 リリース以降、WGB の背後にある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。

- WGB の背後にあるワイヤレス クライアントおよび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、他の無線のワイヤレス 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。

無線 0（2.4 GHz）をルート（自律 AP の 1 つの動作モード）として設定し、無線 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 グループに両方の無線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。

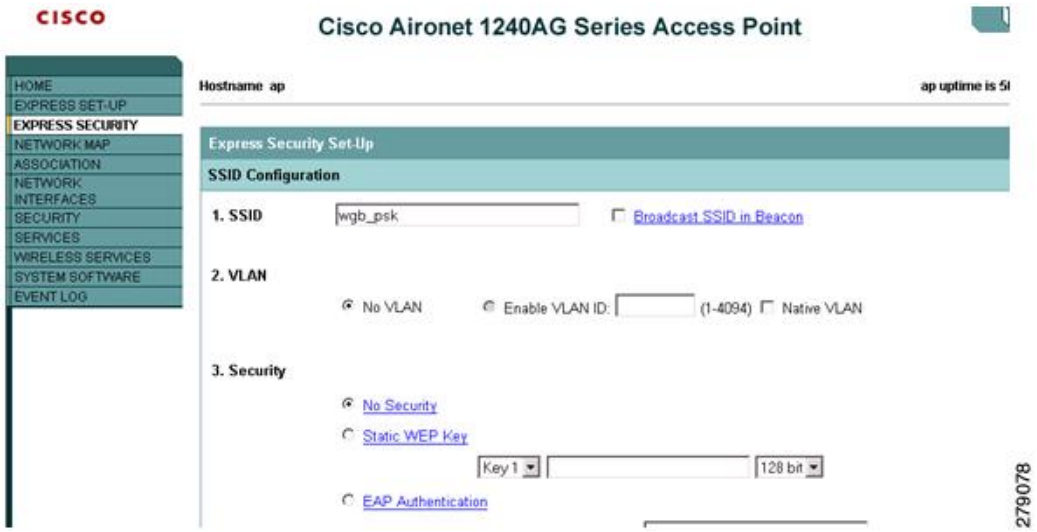
- SSID を無線インターフェイスにマッピングし、無線インターフェイスの役割を定義します。

次の例では、両方の無線で 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。すべての無線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 AP の GUI を使用して設定を行うこともできます。この GUI から 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 *47* : *[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 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、WGB の背後にあるワイヤレス/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。

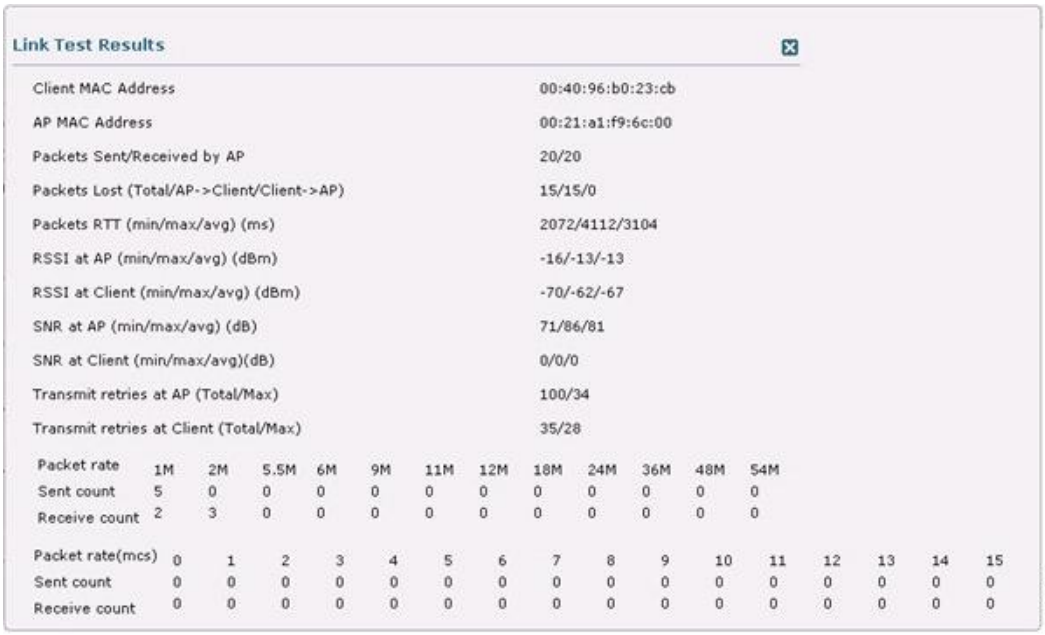
図 *48* : 更新された *WGB* クライアント

図 *49* : 更新された *WGB* クライアント

図 *50* : 更新された *WGB* クライアント

リンク テストの結果

図 *51*：リンク テストの結果



Link Test Results

Client MAC Address	00:40:96:b0:23:cb
AP MAC Address	00:21:a1:f9:6c:00
Packets Sent/Received by AP	20/20
Packets Lost (Total/AP->Client/Client->AP)	15/15/0
Packets RTT (min/max/avg) (ms)	2072/4112/3104
RSSI at AP (min/max/avg) (dBm)	-16/-13/-13
RSSI at Client (min/max/avg) (dBm)	-70/-62/-67
SNR at AP (min/max/avg) (dB)	71/86/81
SNR at Client (min/max/avg)(dB)	0/0/0
Transmit retries at AP (Total/Max)	100/34
Transmit retries at Client (Total/Max)	35/28

Packet rate	1M	2M	5.5M	6M	9M	11M	12M	18M	24M	36M	48M	54M
Sent count	5	0	0	0	0	0	0	0	0	0	0	0
Receive count	2	3	0	0	0	0	0	0	0	0	0	0

Packet rate(mcs)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sent count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Receive count	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

279071

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に接続された有線またはワイヤレス クライアントに対してWGB外部で実行することはできません。WGB自体から WGB に接続されたワイヤレス 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 ポイントにアソシエートされ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:d2	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 70 mph の速度がサポートされています。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 ポイント経由ローミング：クライアントによる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：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、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：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 は新しい親アソシエーションをスキャンします。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 は新しい親アソシエーションを検索し、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、限定チャネルのセットのみをスキャンするよう制限され、WGB のローミングが 1 つのアクセス ポイントから別のアクセス ポイントに切り替わ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 セットは、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、無線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 セットのみをスキャンします。この限定チャネルの機能は、WGB が現在アソシエートされているアクセス 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、チャネルが限定チャネル セット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

次に、ローミング設定を設定する例を示します。

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

no mobile station scan コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

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 にアソシエートされていない場合は、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 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（このコマンドは、WGB 内のアソシエートされ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アソシエートすることを忘れないでください）。
5. **show dot11 association** コマンドの出力を確認し、WGB がコントローラにアソシエートされていることを確認します。
6. WGB で 20 クライアントの制限が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 クライアントのアソシエーションは成功です。

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 に対応しており、ローカル 2.4 GHz アクセス無線および 5 GHz バックホール無線で QoS がサポートされます。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。

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 で輻輳が発生したときに、メッシュ アクセス ポイントは制御された Quality of Service（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。

アクセスポイントには、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。

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

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 トラフィックのあるエンドデバイスが、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）。

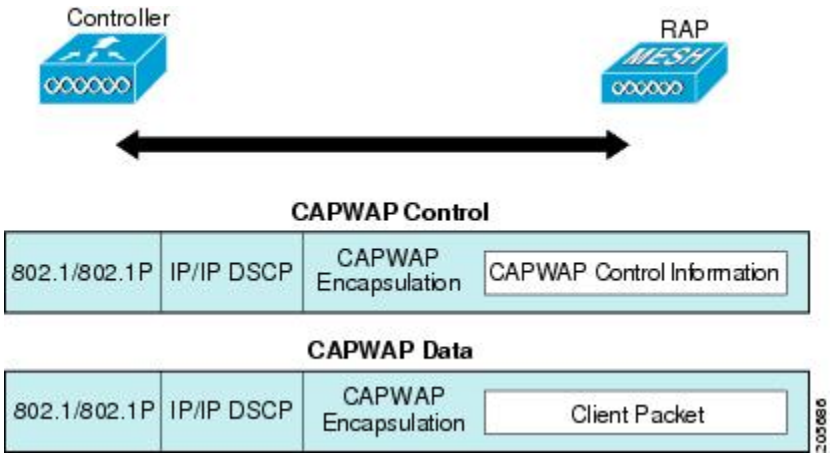
カプセル化

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

情報とディレクティブ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 *52*：カプセル化

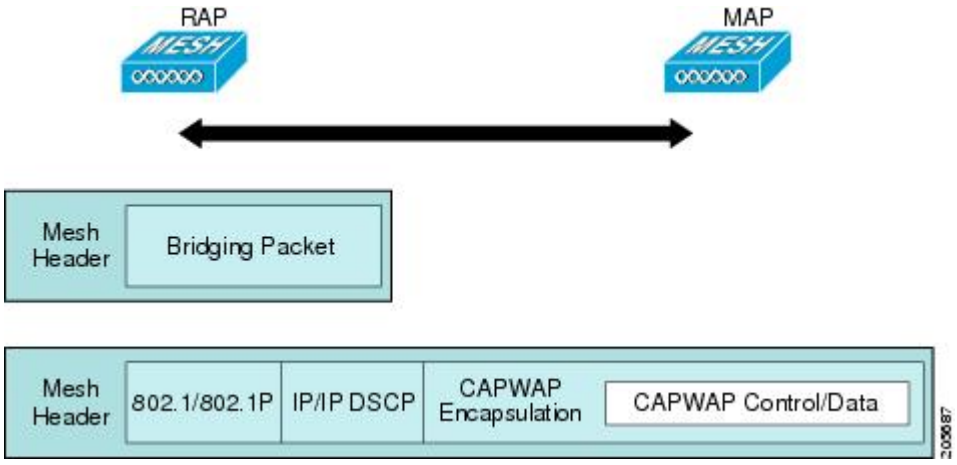


バックホールの場合、メッシュ トラフィックのカプセル化のタイプは 1 つだけです。ただし、2 つのタイプのトラフィック（ブリッジ トラフィックと CAPWAP 制御およびデータ トラフィック）がカプセル化されます。どちらのタイプのトラフィックもプロプライエタリ メッシュ ヘッダーにカプセル化されます。

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 *53*：メッシュ トラフィックのカプセル化



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。

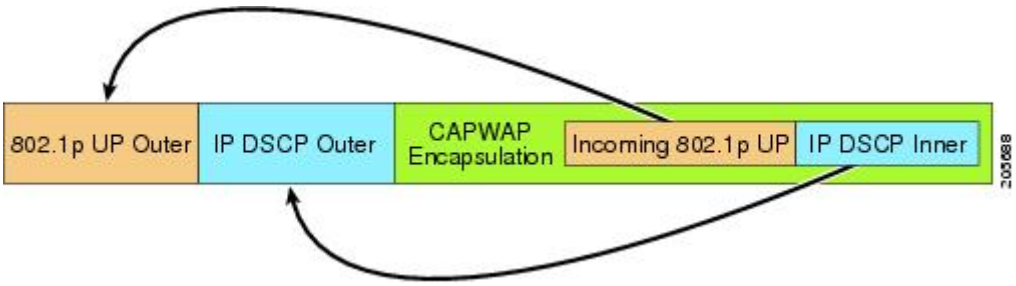
バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Siliver、および Bronze に制限されます。Platinum キューは、CAPWAP 制御トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

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 レートとアグレッシブが若干増加します。これらの変更の目的は、ビデオ アプリケーションから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 *54*：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、ノードのペア化（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 *22* : 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 *23* : *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 *55*：*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 24：DSCP とバックホール キューのマッピング，（176 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 *24*：*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 コード拡張では、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。

WMM 以外のワイヤレス クライアント 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、それらはその 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 では、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は、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] 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] 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。
  - 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] 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

メッシュ ネットワークでの音声コールのサポート

表 25：802.11a/n 無線および 802.11b/g/n 無線で可能な 1550 シリーズのコール，（179 ページ） に、クリーンで理想的な環境での実際のコールを示します。

表 *25*：*802.11a/n* 無線および *802.11b/g/n* 無線で可能な *1550* シリーズのコール

コール数 [12]	802.11a/n 無線 20 MHz	802.11a/n 無線 40 MHz	802.11b/g/n バックホール無線 20 MHz	802.11b/g/n バックホール無線 40 MHz
RAP	20	35	20	20
MAP1（最初のホップ）	10	20	15	20
MAP2（2 番目のホップ）	8	15	10	15

12 トラフィックは双方向 64K 音声フローです。VoCoder タイプ：G.711、PER <= 1%。ネットワークのセットアップはデイジーチェーン接続され、コールは 2 ホップを超えて伝送しません。外部干渉はありません。

コールを発信する間、7921 電話のコールの MOS スコアを観察します。3.5 ～ 4 の MOS スコアが許容可能です。

表 *26*：*MOS* 評価

MOS 評価	ユーザ満足度
> 4.3	たいへん満足している
4.0	満足している
3.6	一部のユーザが満足していない
3.1	多くのユーザが満足していない
< 2.58	—

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 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。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは、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で除去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。

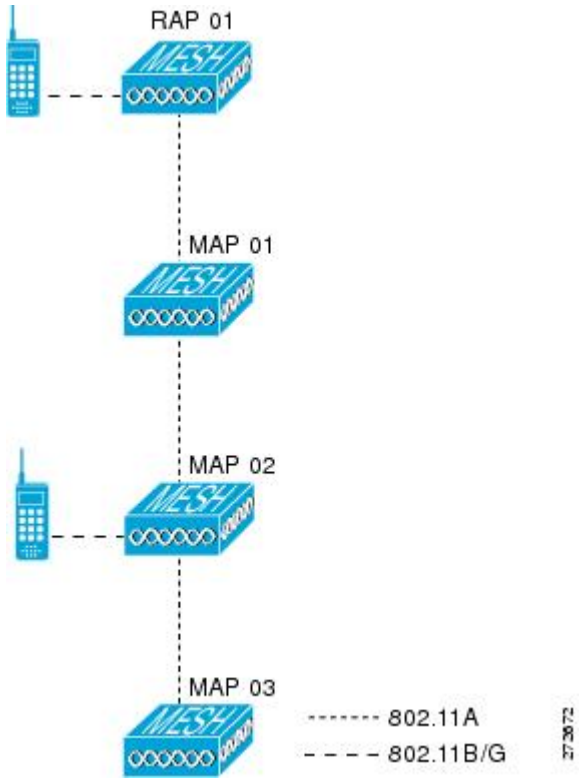
- マルチキャスト パケットが、イーサネット経由で MAP で受信されると、それらは RAP に送信されますが、それらはイーサネット経由で他の MAP に送信されず、MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。
- マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要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

（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）。

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 *56*：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 ポイントと無線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 カウントを示します。

（注） 無線タイプが同じ場合、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、メッシュ アクセス ポイント無線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 ポイント無線で受信された各コールによって、該当のコール サマリー カラムが 1 つずつ増加されます。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 *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 と 802.11a 無線の *calls* カラムに加わり、1 つのコールが map1 802.11a バックホール無線の *calls* カラムに加わり、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、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 *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 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 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 ネットワークでのマルチキャストの有効化（CLI）

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 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イネーブル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 グループに登録されているメッシュ アクセス ポイントに関連付けられている場合にだけ、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 スヌーピングをイネーブルにするには、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* を代行受信し、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 で無線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、イーサネットと無線に発生する可能性があります。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] をイネーブルにします。
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 *57*：ローカルで有効な証明書ページ

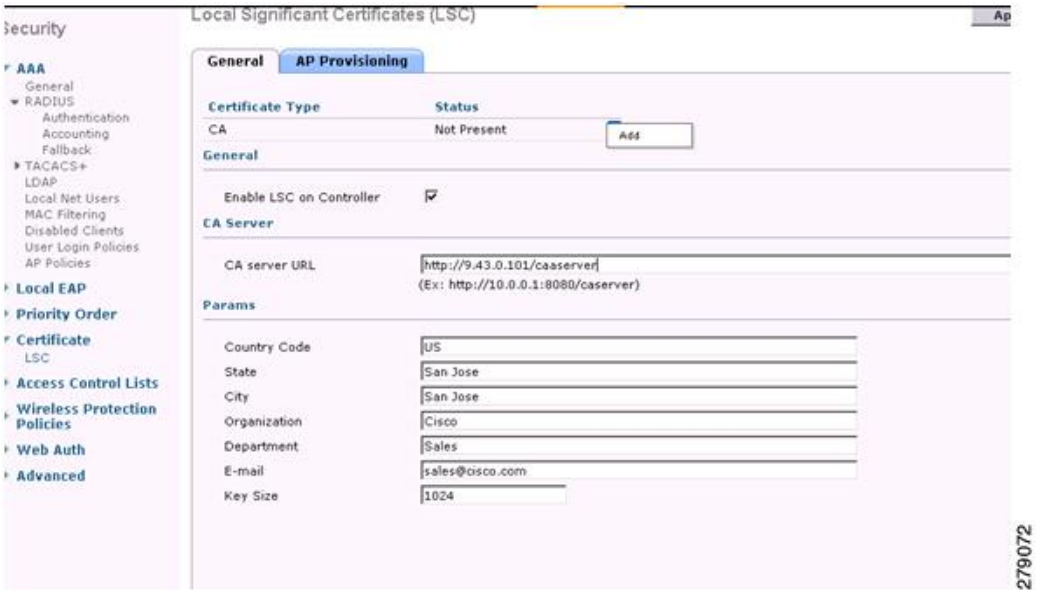
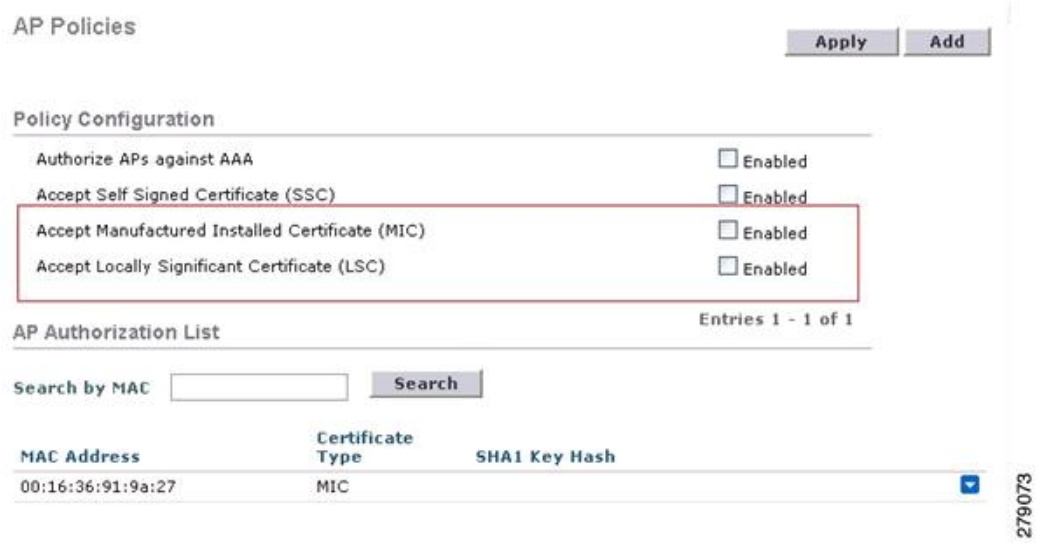


図 *58*：*AP* ポリシーの設定



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、次のように、コントローラの CA 証明書データベースに対して LSC CA 証明書を追加または削除します。

  - **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。コントローラは RA を使用して証明書要求を暗号化し、通信をセキュアにすることができます。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 操作を使用して、設定された CA サーバで RA 証明書を問い合わせ、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 しようとします。AP がコントローラに join しようとする前に、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 しようとします。AP がコントローラに join しようとする前に、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。有効な状態のため、AP が 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

この設定はこの機能に直接関連しませんが、この設定を使用すると、LSC を使用してプロビジョニングされた AP に関する必要な動作を実現できます。

- 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をインストールする必要があります。
- 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をインストールする必要があります。
- 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。

第 7 章

ネットワークの状態の確認

この章では、メッシュ ネットワークの状態の確認方法について説明します。内容は次のとおりです。

Show Mesh コマンド

show mesh コマンドは、次の各項にグループ化されています。

- 一般的なメッシュ ネットワークの詳細の表示
- メッシュ アクセス ポイントの詳細の表示
- グローバル メッシュ パラメータ設定の表示
- ブリッジ グループ設定の表示
- VLAN タギング設定の表示
- DFS の詳細の表示
- セキュリティ設定と統計情報の表示
- GPS ステータスの表示

一般的なメッシュ ネットワークの詳細の表示

一般的なメッシュ ネットワークの詳細を表示するには、次のコマンドを入力します。

- **show mesh env** {**summary** | *AP_name*}：すべてのアクセス ポイント（概要）または特定のアクセス ポイント（AP_name）の温度、ヒーターのステータス、イーサネットのステータスを

表示します。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。
- ヒーター 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 ステータスはアクセス ポイントに対して提供されていないため、**show mesh env** *AP_name* ステータス表示に N/A（該当なし）と表示されます。

```
(Cisco 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

(Cisco 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
```

- **show mesh ap summary**：外部認証のユーザ名を割り当てるために使用できる AP 証明書内の MAC アドレスを示す CERT MAC フィールドを表示するように改訂されました。

```
(Cisco Controller) > show mesh ap summary
AP Name AP Model           BVI MAC            CERT MAC          Hop Bridge Group Name
------- ---------------    -----------------  ----------------- ---- ----------------
R1      LAP1520            00:0b:85:63:8a:10  00:0b:85:63:8a:10 0    y1
R2      LAP1520            00:0b:85:7b:c1:e0  00:0b:85:7b:c1:e0 1    y1
H2      AIR-LAP1522AG-A-K9 00:1a:a2:ff:f9:00  00:1b:d4:a6:f4:60 1
Number of Mesh APs.............................. 3
Number of RAP................................... 2
Number of MAP................................... 1
```

- **show mesh path**：MAC アドレス、アクセス ポイントのロール、アップリンクとダウンリンクの SNR 率（dBs）（SNRUp、SNRDown）、および特定のパスのリンク SNR を表示します。

```
(Cisco Controller) > show mesh path mesh-45-rap1
```

```
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.
```

- **show mesh neighbor summary**：メッシュ ネイバーに関するサマリー情報を表示します。ネイバー情報には MAC アドレス、親子関係、およびアップリンクとダウンリンク（SNRUp、SNRDown）が含まれます。

```
(Cisco Controller) > show mesh neighbor summary ap1500:62:39:70
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
```

（注） 上の **show mesh** コマンドを確認したら、ネットワークのノード間の関係を表示して、各リンクの SNR 値を表示して、RF 接続を確認できます。

- **show mesh ap tree**：ツリー構造（階層）内のメッシュ アクセス ポイントを表示します。

```
(Cisco Controller) > show mesh ap tree
R1(0,y1)
|-R2(1,y1)
|-R6(2,y1)
|-H2(1,default)
Number of Mesh APs.............................. 4
Number of RAP................................... 1
Number of MAP................................... 3
```

メッシュ アクセス ポイントの詳細の表示

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 ap config general** *Cisco_AP*：メッシュ アクセス ポイントのシステム仕様を表示します。

```
(Cisco Controller) > show ap config general aps
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name........................ 1-4404
Primary Cisco Switch IP Address.................. 2.2.2.2
Secondary Cisco Switch Name...................... 1-4404
Secondary Cisco Switch IP Address................ 2.2.2.2
Tertiary Cisco Switch Name....................... 2-4404
Tertiary Cisco Switch IP Address................. 1.1.1.4
```

- **show mesh astools stats** [*Cisco_AP*]：すべての屋外メッシュ アクセス ポイントまたは特定のメッシュ アクセス ポイントのストランディング防止統計情報を表示します。

```
(Cisco Controller) > show mesh astools stats

Total No of Aps stranded : 0
> (Cisco Controller) > show mesh astools stats sb_map1

Total No of Aps stranded : 0
```

- **show advanced backup-controller**：設定されているプライマリおよびセカンダリのバックアップ コントローラを表示します。

```
(Cisco Controller) > show advanced backup-controller
AP primary Backup Controller ..................... controller1 10.10.10.10
AP secondary Backup Controller ..............  0.0.0.0
```

- **show advanced timer**：システム タイマーの設定を表示します。

```
(Cisco Controller) > show advanced timer
Authentication Response Timeout (seconds)........ 10
Rogue Entry Timeout (seconds)..................... 1300
AP Heart Beat Timeout (seconds)................... 30
AP Discovery Timeout (seconds)................... 10
AP Primary Discovery Timeout (seconds)........... 120
```

- **show ap slots**：メッシュ アクセス ポイントのスロット情報を表示します。

```
(Cisco Controller) > show ap slots
Number of APs.................................... 3
AP Name Slots AP Model            Slot0    Slot1   Slot2    Slot3
------------------------------  ------  -------  ------   ------
R1       2    LAP1520            802.11A  802.11BG
H1       3    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A
H2       4    AIR-LAP1521AG-A-K9 802.11BG 802.11A  802.11A 802.11BG
```

グローバル メッシュ パラメータ設定の表示

次のコマンドを使用して、グローバル メッシュ設定についての情報を取得します。

- **show mesh config**：グローバル メッシュ設定を表示します。

```
(Cisco Controller) > show mesh config
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
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
```

ブリッジ グループ設定の表示

ブリッジ グループ設定を表示するには、次のコマンドを入力します。

- **show mesh forwarding table**：設定されたすべてのブリッジと MAC テーブルのエントリを表示します。
- **show mesh forwarding interfaces**：ブリッジ グループと各ブリッジ グループ内のインターフェイスを表示します。このコマンドは、ブリッジ グループ メンバーシップのトラブルシューティングに役立ちます。

VLAN タギング設定の表示

VLAN タギング設定を表示するには、次のコマンドを入力します。

- **show mesh forwarding VLAN mode**：設定されている VLAN トランスペアレント モード（有効または無効）を表示します。
- **show mesh forwarding VLAN statistics**：VLAN の統計情報とパスを表示します。
- **show mesh forwarding vlans**：サポートされる VLAN を表示します。
- **show mesh ethernet VLAN statistics**：イーサネット インターフェイスの統計情報を表示します。

DFS の詳細の表示

DFS の詳細を表示するには、次のコマンドを入力します。

- **show mesh dfs history**：チャネル別のレーダー検出と結果の停止の履歴を表示します。

```
(Cisco Controller) > show mesh dfs history
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24 second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14 second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20
minute(s), 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47
```

```
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 second(s)).
```

- **show mesh dfs channel** *channel number*：指定したチャネルのレーダー検出と停止の履歴を表示します。

```
(Cisco Controller) > show mesh dfs channel 104
ap1520#show mesh dfs channel 104
Channel 104 is available
Time elapsed since radar last detected: 0 day(s), 0 hour(s), 48 minute(s), 11 second(s).
```

セキュリティ設定と統計情報の表示

セキュリティ設定と統計情報を表示するには、次のコマンドを入力します。

- **show mesh security-stats** *AP_name*：特定アクセス ポイントとその子のパケット エラー統計情報と、アソシエーション、認証、再アソシエーション、再認証についての失敗、タイムアウト、および成功のカウントを表示します。

```
(Cisco Controller) > show mesh security-stats ap417

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
Tx 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
```

GPS ステータスの表示

- すべての AP の場所の概要を表示するには、次のコマンドを入力します。
  show ap gps location summary

```
(Site5_AMC_02) >show ap gps location summary

AP Name             GPS Present   Latitude       Longitude      Altitude        GPS
location Age
------------------  -----------   ------------   -------------  --------------
------------------------
SJC24-RAP-EAST      NO            N/A            N/A            N/A             N/A
SJC21-RAP-NORTH     NO            N/A            N/A            N/A             N/A
SJC21-RAP-SOUTH     NO            N/A            N/A            N/A             N/A
Site5_21-17         NO            N/A            N/A            N/A             N/A
SJC22-ROOF-MAP      NO            N/A            N/A            N/A             N/A
Site5_21-28         NO            N/A            N/A            N/A             N/A
SJC-24-RAP-WEST     YES           37.42034194    -121.91973098  25.10  meters   000
days, 00 h 00 m 19 s
Site5_24-02         YES           37.41970399    -121.92051996  10.00  meters   000
days, 00 h 00 m 12 s
Site5_22-30         NO            N/A            N/A            N/A             N/A
Site5_23-200        NO            N/A            N/A            N/A             N/A
Site5_25-18         NO            N/A            N/A            N/A             N/A
Site5_22-15         NO            N/A            N/A            N/A             N/A
Site5_25-05         NO            N/A            N/A            N/A             N/A
```

- すべてのメッシュ AP の場所の概要を表示するには、次のコマンドを入力します。
  show mesh gps location summary
- 次のコマンドを入力して、特定のメッシュ AP の場所情報を表示します。
  show mesh gps location *ap-name*

メッシュ アクセス ポイントのメッシュ統計情報の表示

この項では、コントローラの GUI または CLI を使用して、特定のメッシュ アクセス ポイントのメッシュ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。

メッシュ アクセス ポイントのメッシュ統計情報の表示（GUI）

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2 特定のメッシュ アクセス ポイントの統計情報を表示するには、目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Statistics] を選択します。選択したメッシュ アクセス ポイントの [All APs] > *AP Name* > [Statistics] ページが表示されます
このページには、メッシュ ネットワークでのメッシュ アクセス ポイントのロール、メッシュ アクセス ポイントが属するブリッジグループの名前、アクセスポイントが動作するバックホールインターフェイス、

および物理スイッチ ポート数が表示されます。このメッシュ アクセス ポイントのさまざまなメッシュ統計情報も表示されます。

表 *27*：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。

統計情報	パラメータ	説明
Queue Stats	Gold Queue	定義した統計期間に gold（ビデオ）キューで待機しているパケットの平均数と最大数。
	Silver Queue	定義された統計期間中に Silver（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	定義した統計期間に platinum（音声）キューで待機しているパケットの平均数と最大数。
	Bronze Queue	定義した統計期間に bronze（バックグラウンド）キューで待機しているパケットの平均数と最大数。
	Management Queue	定義した統計期間に management キューで待機しているパケットの平均数と最大数。

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送信されたパケット数。
	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。

統計情報	パラメータ	説明
	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。
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。

メッシュ アクセス ポイントのメッシュ統計情報の表示（CLI）

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

- 特定のメッシュ アクセス ポイントのアソシエーションと認証、再アソシエーションと再認証に関して、失敗、タイムアウト、および成功の数などのパケット エラー統計情報を表示するには、次のコマンドを入力します。

  show mesh security-stats *AP_name*

  以下に類似した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 *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 アクセス ポイントのネイバー統計情報の表示

この項では、コントローラの GUI または CLI を使用して、選択したメッシュ アクセス ポイントのネイバー統計情報を表示する方法について説明します。さらに、選択したメッシュアクセスポイントとその親とのリンク テストの実行方法についても説明します。

メッシュ アクセス ポイントのネイバー統計情報の表示（GUI）

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2 特定のメッシュ アクセス ポイントのネイバー統計情報を表示するには、目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Neighbor Information] を選択します。選択されたメッシュ アクセス ポイントの [All APs > *Access Point Name* > Neighbor Info] ページが表示されます。
このページには、メッシュ アクセス ポイントの親、子、およびネイバーが表示されます。また、各メッシュ アクセス ポイントの名前と無線 MAC アドレスが表示されます。

ステップ 3 メッシュアクセスポイントとその親または子とのリンクテストを実行するには、以下の手順に従います。

a) 親または目的の子の青のドロップダウン矢印の上にカーソルを移動し、[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。

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。

c) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

ステップ 4 このページで任意のメッシュ アクセス ポイントの詳細を表示するには、次の手順を実行します。

a) 目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Details] を選択します。[All APs > Access Point Name > Link Details > Neighbor Name] ページが表示されます。

b) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

ステップ 5 このページで任意のメッシュ アクセス ポイントの統計情報を表示するには、次の手順を実行します。

a) 目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Stats] を選択します。[All APs > Access Point Name > Mesh Neighbor Stats] ページが表示されます。

b) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

メッシュ アクセス ポイントのネイバー統計情報の表示（CLI）

コントローラ CLI を使用して、特定のメッシュ アクセスポイントのネイバー統計情報を表示するには、次のコマンドを実行します。

- 特定のメッシュ 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**} *AP_Name*

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
```

- メッシュ アクセス ポイントとそのネイバーとのリンクのチャネルおよびSignal to Noise Ratio（SNR）を表示するには、次のコマンドを入力します。

  show mesh path *AP_Name*

  以下に類似した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 *AP_Name*

  以下に類似した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）

第 8 章

トラブルシューティング

この章では、トラブルシューティング情報について説明します。内容は次のとおりです。

インストールと接続

ステップ 1 RAP にするメッシュ アクセス ポイントをコントローラに接続します。

ステップ 2 目的の場所に無線（MAP）を配置します。

ステップ 3 コントローラ CLI で、**show mesh ap summary** コマンドを入力して、コントローラ上のすべての MAP と RAP を表示します。

図 *59*：*[Mesh AP Summary]* ページの表示

```
(Cisco Controller) >show mesh ap summary

AP Name               AP Model            BVI MAC             CERT MAC          Hop  Bridge Group Name  Enhanced Feature Set
----------------  ------------------  ----------------  ----------------  ---  ----------------  --------------------
1532MAP2-DaisyChained  AIR-CAP1532E-A-K9    4c:4e:35:46:f2:72  4c:4e:35:46:f2:72  0    default           N/A
1532RAP1              AIR-CAP1532E-A-K9    4c:4e:35:46:f2:64  4c:4e:35:46:f2:64  0    default           N/A
1532MAP1              AIR-CAP1532E-A-K9    4c:4e:35:46:f1:4e  4c:4e:35:46:f1:4e  1    default           N/A
1524PSRAP1            AIR-LAP1524PS-A-K9   00:22:be:41:23:00  00:22:be:41:23:00  0    MESHDEMO1         N/A
1522MAP2              AIR-LAP1522AG-A-K9   00:22:be:42:fe:00  00:22:be:42:fe:00  1    MESHDEMO1         N/A

Number of Mesh APs.............................. 3
Number of RAPs.................................. 2
Number of MAPs.................................. 1
Number of Flex+Bridge APs....................... 2
Number of Flex+Bridge RAPs...................... 1
Number of Flex+Bridge MAPs...................... 1
```

ステップ 4 コントローラ GUI で、[Wireless] をクリックして、メッシュ アクセス ポイント（RAP と MAP）の概要を表示します。

図 *60*：*[All APs Summary]* ページ

All APs

Search by AP MAC Search

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certific Type
iMeshRap1	00:19:30:76:32:72	0 d, 22 h 24 m 25 s	Enable	REG	Local	MIC
HJRAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
HJMAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
HJMAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
HJMAP2	00:1d:71:0c:f0:00	0 d, 22 h 04 m 53 s	Enable	REG	Bridge	MIC
HPRAP1	00:1e:14:48:43:00	0 d, 05 h 35 m 24 s	Enable	REG	Bridge	MIC
HPMAP1	00:1b:d4:a7:78:00	0 d, 22 h 04 m 25 s	Enable	REG	Bridge	MIC

273952

ステップ 5 [AP Name] をクリックして詳細ページを表示し、[Interfaces] タブを選択して、アクティブな無線インターフェイスを表示します。
使用中の無線スロット、無線タイプ、使用中のサブバンド、動作状態（UP または DOWN）がまとめて表示されます。

- すべての AP は 2 つの無線スロット（スロット 0 - 2.4 GHz とスロット 1 – 5 GHz）をサポートしています。

  同じメッシュ ネットワークに複数のコントローラを接続している場合、すべてのメッシュ アクセス ポイントに対するグローバル設定を使用してプライマリ コントローラの名前を指定するか、各ノードでプライマリ コントローラを指定する必要があります。指定しないと、負荷が最小のコントローラが優先されます。メッシュ アクセス ポイントがコントローラに以前接続されていた場合、メッシュ アクセス ポイントはコントローラの名前をすでに認識しています。

  コントローラ名の設定後、メッシュ アクセス ポイントがリブートします。

ステップ 6 [Wireless] > [AP Name] をクリックして、AP 詳細ページでメッシュ アクセス ポイントのプライマリ コントローラを確認します。

debug コマンド

次の 2 つのコマンドは、メッシュ アクセス ポイントとコントローラ間で交換されるメッセージを表示する場合にたいへん役立ちます。

```
(Cisco Controller) > debug capwap events enable
(Cisco Controller) > debug disable-all
```

debug コマンドを使用して、メッシュ アクセス ポイントとコントローラ間で行われるパケット交換のフローを表示できます。メッシュ アクセス ポイントで、検索プロセスが起動します。加入フェーズでクレデンシャルの交換が行われ、メッシュ アクセス ポイントがメッシュ ネットワークへの加入を許可されることが認証されます。

加入が正常に完了すると、メッシュ アクセス ポイントは CAPWAP 設定要求を送信します。コントローラは設定応答で応答します。メッシュアクセスポイントはコントローラからの設定応答を受信すると、各設定要素を評価し、それらを実装します。

リモート デバッグ コマンド

AP コンソール ポートへの直接接続またはコントローラのリモートデバッグ機能のいずれかによって、デバッグのために、メッシュ アクセス ポイント コンソールにログインできます。

コントローラでリモート デバッグを起動するには、次のコマンドを入力します。

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

AP コンソール アクセス

AP1500 にはコンソール ポートがあります。メッシュ アクセス ポイントにはコンソール ケーブルが付属していません。1550 シリーズのアクセス ポイントの場合、コンソール ポートは簡単にアクセスでき、アクセス ポイント ボックスを開く必要はありません。

AP1500 では、コードにコンソール アクセス セキュリティが埋め込まれており、コンソール ポートへの不正アクセスを防止し、セキュリティが拡張されています。

コンソール アクセス用の **ログイン ID** と**パスワード**はコントローラから設定します。次のコマンドを使用して、ユーザ名/パスワードの組み合わせを指定したメッシュ アクセス ポイントまたはすべてのアクセス ポイントに適用できます。

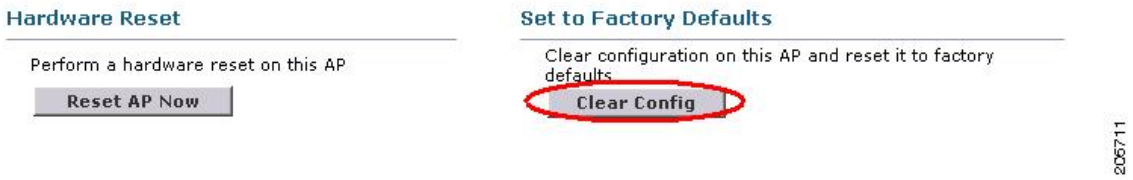
```
<Cisco Controller> config ap username cisco password cisco ?

all           Configures the Username/Password for all connected APs.
<Cisco AP>    Enter the name of the Cisco AP.
```

```
<Cisco Controller> config ap username cisco password cisco all
```

コントローラから適用されたユーザ名/パスワードがメッシュ アクセス ポイントのユーザ *ID* とパスワードとして使用されているか確認する必要があります。これは不揮発性設定です。ログイン *ID* とパスワードは、設定すると、メッシュ アクセス ポイントのプライベート設定に保存されます。

ログインに成功すると、トラップが Cisco Prime Infrastructure に送信されます。ユーザが 3 回連続してログインに失敗すると、ログイン失敗トラップがコントローラと Cisco Prime Infrastructure に送信されます。

注意 メッシュ アクセス ポイントは、別の場所に移動する前に、出荷時のデフォルト設定にリセットする必要があります。



AP からのケーブル モデムのシリアル ポート アクセス

コマンドは、CLI の特権モードからケーブル モデムに送信できます。コマンドを使用してテキスト文字列を取得し、ケーブル モデム UART インターフェイスに送信します。ケーブル モデムはそのテキスト文字列を独自のコマンドの 1 つとして解釈します。ケーブル モデムの応答が取得され、Cisco IOS コンソールに表示されます。ケーブル モデムからは、最大 9600 文字が表示されます。4800 文字を超えるテキストはすべて切り捨てられます。

モデムのコマンドは、元々ケーブル モデム用である UART ポートに接続されているデバイスがあるメッシュ AP でのみ使用できます。ケーブル モデムがない、または他のデバイスが UART に接続されているメッシュ AP でコマンドを使用した場合、コマンドは受け入れられますが、戻される出力は生成されません。明示的にフラグが付けられるエラーはありません。

設定

MAP の特権モードから次のコマンドを入力します。

`AP#`**send cmodem** *timeout-value modem-command*

modem コマンドは、ケーブルモデムに送信する任意のコマンドまたはテキストです。タイムアウト値の範囲は 1 ～ 300 秒です。ただし、取得されたデータが 9600 文字の場合、9600 文字を超え

るテキストは切り捨てられ、タイムアウト値とは関係なく、応答が AP コンソールにすぐに表示されます。

図 *61*：ケーブル モデム コンソールのアクセス コマンド

```
RAP-CM-N1#send ?
  *        All tty lines
  <0-16>   Send a message to a specific line
  cmodem   Enter cable modem command
  console  Primary terminal line
  log      Logging destinations
  vty      Virtual terminal

RAP-CM-N1#send cmodem ?
  LINE  Enter modem command string
  <cr>
```

279059

図 *62*：ケーブル モデム コンソールのアクセス コマンド

```
RAP-CM-N1#send cmodem ls
ls
CM>
CM> ls

!               ?               REM             cd              dir
find_command    help            history         instances       ls
man             pwd             sleep           syntax          system_time
usage
----
mbufShow        memShow         mutex_debug     ping            read_memory
reset           routeShow       run_app         shell           stackShow
start_idle_profiling            stop_idle_profiling             taskDelete
taskInfo        taskPrioritySet taskResume      taskShow        taskSuspend
taskTrace       usfsShow        version         write_memory    zone
----
[HeapManager] [SA] [cm_hal] [docsis_ctl] [embedded_target] [enet_hal]
[event_log] [flash] [forwarder] [ip_hal] [msgLog] [non-vol] [pingHelper]
[snmp] [snoop] [usb_hal]

CM>
RAP-CM-N1#send cmodem cd docsis
cd
CM>
CM> cd docsis
CM> cd docsis

Active Command Table:  CM DOCSIS Control Thread Commands (docsis_ctl)

CM -> docsis_ctl

CM/DocsisCtl>
RAP-CM-N1#
```

279060

注意 疑問符（?）と感嘆符（!）は、**send cmodem** コマンドでは使用できません。これらの文字は、Cisco IOS CLI で即座に別の意味に解釈されます。そのため、モデムに送信できません。

ケーブル モデム コンソール ポートの有効化

デフォルトでは、ケーブル モデム コンソール ポートは無効になります。これは、ユーザが自分の個人用のケーブル モデムを使用して、コンソールにアクセスできないようにするためです。AP1572IC、AP1572EC、AP1552C モデルでは、ケーブル モデム コンソールはアクセス ポイントに直接接続されます。コンソール ポートは、AP とケーブル モデムの間のシグナリングに必要です。SNMP を介して、または CMTS のコンフィギュレーション .cm ファイルにコマンドを追加して、ケーブル モデム コンソール ポートを有効にする 2 つの方法があります。

（注） AP1572EC、AP1572IC、AP1552C および AP1552CU の場合、ケーブル モデムを有効にする必要があります。

- ケーブル モデムの IP アドレスに次のコマンドを入力して、SNMP を介してケーブル モデム コンソール ポートを有効にします。
  ```
  snmpset -c private IP_ADDRESS cmConsoleMode.0 i N
  ```
  OID を使用して、次のコマンドを入力します。
  ```
  snmpset -c private IP_ADDRESS
  1.3.6.1.4.1.1429.77.1.4.7.0 i N
  ```
  IP_ADDRESS は任意の Ipv4 アドレス、N は整数、2 は読み取りと書き込みの有効化、1 は読み取り専用、0 は無効化です。

  例：
  ```
  snmpset -c private 209.165.200.224 cmConsoleMode.0 i 2
  ```

- コンフィギュレーション ファイルからケーブル モデム コンソール ポートを有効にします。コンフィギュレーション ファイル（.cm 拡張子）は、ケーブル モデム ヘッド エンドにロードされます。参加プロセスの一部としてケーブル モデムにプッシュされます。ケーブル モデム コンフィギュレーション ファイルに次の行を入力します。
  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```
  OID を使用して、この行を入力します。
  ```
  SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
  ```

ケーブル モデムを使用した AP1572xC/AP1552C のリセット

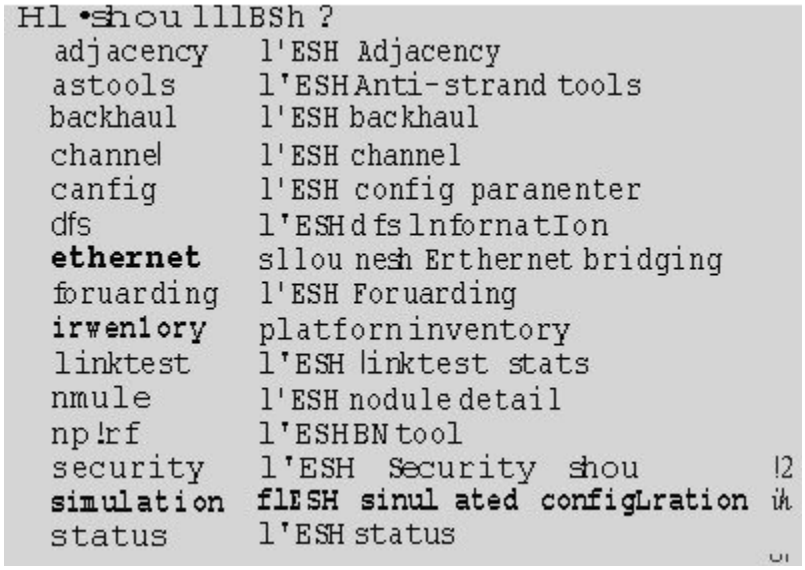
AP はアクセス ポイント内にあるケーブル モデムへ SNMP コマンドを入力してリセットできます。この機能を動作させるには、ケーブル モデム コンソール ポートを有効にする必要があります。

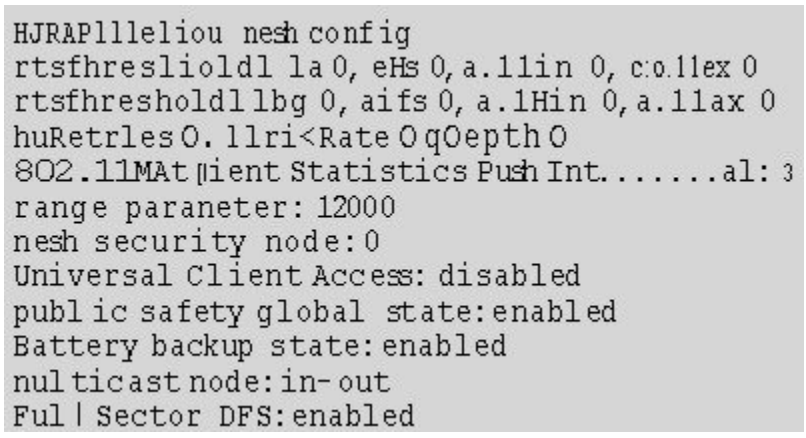
次の snmpset コマンドを入力して、AP をリセットします。
```
Snmpset -v2c -c public IP ADDRESS 1.3.6.1.4.1.1429.77.1.3.17.0 i 1
```

IP ADDRESS は、ケーブル モデムの IPv4 アドレスです。

メッシュ アクセス ポイント CLI コマンド

次のコマンドは、メッシュ アクセス ポイントで AP コンソール ポートを使用して直接入力できます。コントローラのリモート デバッグ機能を使用して入力することもできます。





```
HJRAPlllehou caplolBp client mb
Adnin5tate                          ADHIN ENABLED
SuVer                               S.2.98.0
NunFll ledSlots                     2
Nane                                HJRAPl
Location                            default location
Huarllame                           SEYf-CllffROLLER
Huarrlp                             209.165.200.227
Huartt.Ner                          0.0.0.0
ApHocle                              Brld!JE!
ApSubl'lode                         Not [:mf igured
OperationState                      UP
CAPllN'Path nru                      1485
Link!U:liting                       disabled
ApRole                              RootAP
ApBac:khaul                         802.l la
Ap8ac:khaulthannel                  5805
ApBac:khaulSlot                     1
ApBac:khaul llgEnabled              0
ApBac:l<haullxRate                  24000
Ethernet Brldglrg State             0
Public Safety State                 enabled
```

```
HJHAPlllehoi.I nesh adjacency ?
  alI      HESH Adjacency AlI
  child    HESH Adjacency Child
  parent MESH Adjacency Parent
                                    OI
```

```
HJMap4#shou mesh status '%
 shou MESH Status
 MeshAP in state Maint
 Uplink Backbone: Virtual-Dot11Radio0
 Downlink Backbone: Dot11Radio1
 Configured BGN: HuckJr
       rxNeighReq 129790 rxNeighRsp 66976 txNeighReq 33938 txNeighRsp 129790
       rxNeighRsp 1147275 txNeighUpd 202060
       nextchan 0 nextant 0 downAnt 0 downChan 0 curAnts 0
       nextNeigh 1. malformedNeighPackets 4.poorNeighSnr 1
       blacklistPackets 0,insufficientMemory 0, authenticationFailures 0
       Parent Changes 3, Neighbor Timeouts 0
       Vector through 0017.94fe.c3bf:
              Vector ease 1 -1, FWD: 0017.94fe.c3bf
                                                                    273949
```

```
HJNap4#show mesh forwarding link
 Current mesh links:
----------------------
 End Point  : 0017.94fe.c3bf
 Adjacency  : Exists
 Channel    : 161 on Dot11Radio1
 Type       : 2
 State      : 4
 Bundle     : member
 Bridge     : 1
 swidb      : Virtual-Dot11Radio0
 port state : OPEN
```

273950

メッシュ アクセス ポイント デバッグ コマンド

次のコマンドは、メッシュ アクセス ポイントで AP コンソール ポートを使用して直接入力しても、コントローラでリモート デバッグ機能を使用しても、入力できます。

- **debug mesh ethernet bridging**：イーサネット ブリッジングをデバッグします。
- **debug mesh ethernet config**：VLAN タギングに関連付けられているアクセスおよびトランク ポート設定をデバッグします。
- **debug mesh ethernet registration**：VLAN 登録プロトコルをデバッグします。このコマンドは、VLAN タギングに関連付けられています。
- **debug mesh forwarding table**：ブリッジ グループが含まれている転送テーブルをデバッグします。
- **debugs mesh forwarding packet bridge-group**：ブリッジ グループ設定をデバッグします。

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 に設定された無線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。

バックホール アルゴリズム

バックホールは、メッシュ アクセス ポイント間に無線接続だけを作成するために使用します。

デフォルトでバックホール インターフェイスは 802.11a です。バックホール インターフェイスを 802.11b/g に変更できません。

AP1500 には、デフォルトで「自動」データ レートが選択されています。

バックホール アルゴリズムは、孤立状態のメッシュ アクセス ポイントの状況に対処するために設計されました。このアルゴリズムは、各メッシュ ノードに高いレベルの復元力も追加します。

このアルゴリズムは、次のようにまとめることができます。

- MAP は常に、イーサネット ポートが UP の場合はイーサネット ポートを**プライマリ バックホール**として設定し、UP でない場合は 802.11a 無線として設定します（この機能により、

ネットワーク管理者は、イーサネット ポートを最初に RAP として設定し、社内で回復することができます）。ネットワークの高速コンバージェンスを可能にするため、メッシュ ネットワークへの最初の加入では、イーサネット デバイスを MAP に接続しないことを推奨します。

- UP であるイーサネット ポートで WLAN コントローラへの接続が失敗した MAP は 802.11a 無線を**プライマリ バックホール**として設定します。ネイバーの検索に失敗するか、802.11a 無線上でネイバーを経由した WLAN コントローラへの接続が失敗すると、イーサネット ポートで、再度**プライマリ バックホール**が UP になります。MAP は同じ BGN を持つ親を優先します。
- 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 トポロジをビルドしません。
- 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。
- RAP のイーサネット ポートが DOWN の場合、または RAP が UP であるイーサネット ポートでコントローラに接続できない場合、802.11a 無線が**プライマリ バックホール**として設定されます。ネイバーの検索に失敗するか、802.11a 無線上でネイバーを経由したコントローラへの接続が失敗すると、15 分後に、RAP が SCAN 状態になり、イーサネット ポートが最初に起動します。

前述のアルゴリズムを使用して、メッシュ ノードの役割を保持すると、メッシュ アクセス ポイントが不明状態になり、ライブ ネットワークで孤立状態になるのを避けることができます。

パッシブ ビーコン（ストランディング防止）

パッシブ ビーコンをイネーブルにすると、孤立状態のメッシュ アクセス ポイントで、802.11b/g 無線を使用して、無線でそのデバッグ メッセージをブロードキャストできます。孤立状態のメッシュ アクセス ポイントをリッスンし、コントローラとの接続がある隣接メッシュ アクセス ポイントは、それらのメッセージを CAPWAP 経由でコントローラに渡します。パッシブ ビーコンにより、有線接続のないメッシュ アクセス ポイントが孤立状態になるのを防ぎます。

デバッグ ログもバックホール以外の無線で、救難ビーコンとして送信できるため、隣接メッシュ アクセス ポイントをビーコンのリッスン専用にすることができます。

メッシュアクセスポイントでコントローラへの接続が失われると、コントローラで次の手順が自動的に起動されます。

- 孤立状態のメッシュ アクセス ポイントの MAC アドレスを識別する
- CAPWAP が接続されているすぐ近くのネイバーを見つける
- リモート デバッグによってコマンドを送信する
- チャネルを循環してメッシュ アクセス ポイントを追跡する

この機能を使用するために、知っている必要があるのは孤立状態の AP の MAC アドレスだけです。

メッシュアクセスポイントは、孤立タイマーのリブートが実行された場合に孤立状態と見なされます。孤立タイマーのリブートが発生すると、現在孤立状態のメッシュアクセスポイントで、孤立防止機能のパッシブ ビーコンが有効になります。

この機能は 3 つの部分に分けられます。

- 孤立状態のメッシュ アクセス ポイントによる孤立検出
- 孤立状態のメッシュ アクセス ポイントによって送信されるビーコン
  - 802.11b 無線をチャネル（1、6、11）にラッチする
  - デバッグをイネーブルにする
  - 孤立デバッグ メッセージを救難ビーコンとしてブロードキャストする
  - 最新のクラッシュ情報ファイルを送信する
- ビーコンの受信（リモート デバッグがイネーブルになっている隣接メッシュ アクセス ポイント）

構成されたメッシュ アクセス ポイントは定期的に孤立状態のメッシュ アクセス ポイントを検索します。メッシュ アクセス ポイントは定期的に孤立状態のメッシュ アクセス ポイントのリストと SNR 情報をコントローラに送信します。コントローラはネットワーク内の孤立状態のメッシュ アクセス ポイントのリストを保持します。

debug mesh astools troubleshoot *mac-addr* **start** コマンドを入力すると、コントローラはリストを検索して、孤立状態のメッシュ アクセス ポイントの MAC アドレスを見つけます。

孤立状態のアクセス ポイントのリッスンを開始するメッセージが最適なネイバーに送信されます。リッスンしているメッシュ アクセス ポイントは、孤立状態のメッシュ アクセス ポイントからの救難ビーコンを取得し、コントローラに送信します。

メッシュ アクセス ポイントは、リスナーの役割を担うと、孤立状態のメッシュ アクセス ポイントのリッスンを停止するまで、孤立状態のメッシュアクセスポイントをその内部リストから消去しません。孤立状態のメッシュ アクセス ポイントのデバッグ中に、そのメッシュ アクセス ポイントのネイバーが一定の割合で、現在のリスナーより優れた SNR をコントローラに報告した場合、ただちに孤立状態のメッシュ アクセス ポイントのリスナーが新しいリスナー（SNR が優れた）に変更されます。

エンドユーザ コマンドは次のとおりです。

- **config mesh astools** [**enable** | **disable**]：メッシュ アクセス ポイントの astools をイネーブルまたはディセーブルにします。ディセーブルの場合、AP は孤立状態の AP リストをコントローラに送信しません。
- **show mesh astools stats**：孤立状態の AP とそれぞれのリスナー（存在する場合）のリストを表示します。
- **debug mesh astools troubleshoot** *mac-addr* **start**：*mac-addr* の最適なネイバーに、リッスンを開始するメッセージを送信します。

- **debug mesh astools troubleshoot** *mac-addr* **stop**：*mac-addr* の最適なネイバーに、リッスンを停止するメッセージを送信します。
- **clear mesh stranded** [**all** | *mac of b/g radio*]：孤立状態の AP エントリをクリアします。

コントローラ コンソールは、30 分間、孤立状態の AP からのデバッグ メッセージでいっぱいになります。

動的周波数選択

以前は、レーダーを搭載するデバイスは、他の競合サービスがなく周波数サブバンドで動作していました。しかし、規制当局の管理により、これらの帯域をワイヤレス メッシュ LAN（IEEE 802.11）などの新しいサービスに開放して共有できるようにしようとしています。

既存のレーダー サービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要のあるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFS では、無線デバイスがレーダー信号の存在を検出できる機能の採用を義務付けています。無線でレーダー信号が検出されると、最低30分間は伝送を停止して、そのサービスを保護する必要があります。その後、その無線は伝送のための別のチャネルを選択しますが、伝送前にこのチャネルをモニタリングする必要があります。使用する予定のチャネルで少なくとも 1 分間レーダーが検出されなかった場合には、新しい無線サービス デバイスはそのチャネルで伝送を開始できます。

AP は新たな DFS チャネルで、DFS スキャンを 60 秒間実行します。ただし、この新規 DFS チャネルが隣接 AP にすでに使用されている場合は、AP は DFS スキャンを実行しません。

無線がレーダー信号を検出して識別するプロセスは複雑なタスクであり、ときどきは誤った検出が起こります。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャネル レーダーを確実に検出するためのアクセス ポイントの機能など、非常に多くの要因が考えられます。

802.11h 規格では、DFS および Transmit Power Control（TPC）について、5 GHz 帯域に関連するものと指定しています。DFS を使用してレーダーの干渉を回避し、TPC を使用して Satellite Feeder Link の干渉を回避します。

（注） DFS は、米国では 5250 ～ 5350 および 5470 ～ 5725 周波数帯域に義務付けられています。ヨーロッパでは、DFS と TPC が上記帯域に義務付けられています

図 *63* : ***DFS*** および ***TPC*** 帯域の要件

RAP の DFS

RAP ではレーダー検出の応答として、次の手順が実行されます。

1. RAP が、チャネルがレーダーに影響を受けるコントローラにメッセージを送信します。チャネルが、RAP およびコントローラで影響を受けるチャネルとしてマークされます。
2. RAP がそのチャネルを 30 分間ブロックします。この 30 分間は非占有期間と呼ばれます。
3. コントローラが、チャネルでレーダーが検出されたことを示す TRAP を送信します。TRAP は非占有期間が経過するまで留まります。
4. RAP は 10 秒間でチャネルから移行します。これは、チャネル移行時間と呼ばれます。システムがチャネルをクリアする時間として定義され、レーダーバーストの終わりからチャネルの最終送信の終わりまで測定されます。
5. RAP が Quite モードに入ります。Quite モードで、RAP がデータ伝送を停止します。ビーコンは引き続き生成され、プローブ応答も引き続き配信されます。Quiet モードは、チャネル移行時間（10 秒）が終了するまで存続します。
6. コントローラが新しいランダム チャネルを選択し、チャネル情報を RAP に送信します。
7. RAP が新しいチャネル情報を受信し、チャネル変更フレーム（ユニキャスト、暗号化）を MAP に送信し、各 MAP が同じ情報をセクターの下位の子に送信します。各メッシュ アクセス ポイントは、100 ミリ秒ごとに 1 回ずつ合計 5 回、チャネル変更フレームを送信します。
8. RAP が新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。RAP が新しいチャネルで、60 秒間レーダーの存在を

スキャンし続けます。このプロセスは、チャネル アベイラビリティ チェック（CAC）と呼ばれます。

9 MAP が新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。MAP が新しいチャネルで、60 秒間レーダーの存在をスキャンし続けます。

10 レーダーが検出されない場合、RAP がこの新しいチャネルですべての機能を再開し、セクター全体がこの新しいチャネルにチューニングされます。

MAP の DFS

MAP ではレーダー検出の応答として、次の手順が実行されます。

1 MAP が、レーダー発見の指示を親と、最終的にそのチャネルが影響を受けることを示している RAP に送信します。RAP がこのメッセージをコントローラに送信します。このメッセージは、RAP から送信されたものであるように表示されます。MAP、RAP、およびコントローラが 30 分間影響を受けるものとしてチャネルをマークします。

2 MAP が 30 分間チャネルをブロックします。この 30 分間は非占有期間と呼ばれます。

3 コントローラが、チャネルでレーダーが検出されたことを示す TRAP を送信します。TRAP は非占有期間が経過するまで留まります。

4 MAP は 10 秒間でチャネルから移行します。これは、チャネル移行時間と呼ばれます。システムがチャネルをクリアする時間として定義され、レーダーバーストの終わりからチャネルの最終送信の終わりまで測定されます。

5 MAP が Quite モードに入ります。Quite モードで、MAP がデータ伝送を停止します。ビーコンは引き続き生成され、プローブ応答も引き続き配信されます。Quiet モードは、チャネル移行時間（10 秒）が終了するまで存続します。

6 コントローラが新しいランダム チャネルを選択し、チャネルを RAP に送信します。

7 RAP が新しいチャネル情報を受信し、チャネル変更フレーム（ユニキャスト、暗号化）を MAP に送信し、各 MAP が同じ情報をセクターの下位の子に送信します。各メッシュ アクセス ポイントは、100 ミリ秒ごとに 1 回ずつ合計 5 回、チャネル変更フレームを送信します。

8 各メッシュ アクセス ポイントが新しいチャネルにチューニングし、サイレント モードになります。サイレント モード中は、レシーバだけが ON になります。パケット伝送は行われません。AP が新しいチャネルで、60 秒間レーダーの存在をスキャンし続けます。このプロセスは、チャネル アベイラビリティ チェック（CAC）と呼ばれます。MAP はコントローラから切断されない必要があります。この 1 分間、ネットワークは安定した状態を維持する必要があります。

DFS 機能により、レーダー信号を検出した MAP はそれを RAP まで伝送することができ、RAP はレーダーを経験したことがあるかのように動作し、セクターを移動します。このプロセスは、コーディネイテッド チャネル変更と呼ばれます。コントローラで、この機能はオンまたはオフにできます。コーディネイテッド チャネル変更は、デフォルトでイネーブルになっています。

DFS をイネーブルにするには、次のコマンドを入力します。

```
(Cisco Controller) > config mesh full-sector-dfs enable
```

ネットワークで DFS がイネーブルになっているかどうかを確認するには、次のコマンドを入力します。

```
(Cisco Controller) > show network summary
```

（注） レーダーを検出した MAP は、親の BGN が異ならない限り、RAP にメッセージを送信する必要があります。この場合、コーディネイテッド セクター変更のメッセージを送信しません。代わりに、MAP は再度 SCAN 状態になり、レーダーが発見されなかったチャネルで、新しい親を検索します。

（注） いずれのメッシュ アクセス ポイントもデフォルトの BGN を使用していないことを確認します。

（注） MAP で繰り返されたレーダー イベント（レーダーは 1 回トリガーすると、ほとんどすぐに再度トリガーする）により、MAP が切断されます。

DFS 環境での準備

この項では、DFS 環境での準備方法について説明します。

- コントローラが正しい国の地域に設定されていることを確認するには、次のコマンドを入力します。

  ```
  (Cisco Controller) > show country
  ```

- メッシュ アクセス ポイントの国とコントローラのチャネル設定を確認するには、次のコマンドを入力します。

  ```
  (Cisco Controller)> show ap config 802.11a ap-name
  ```

- メッシュに使用可能なチャネルを識別するには、次のコマンドを入力します。

  ```
  (Cisco Controller)> show ap config 802.11a ap-name
  ```

  許可されたチャネル リストを検索します。

  ```
  Allowed Channel List..................... 100,104,108,112,116,120,124,
  ..................................... 128,132,136,140
  ```

- AP コンソールで（またはコントローラからリモート デバッグを使用して）メッシュに使用可能なチャネルを識別するには、次のコマンドを入力します。

```
ap1520-rap # show mesh channels

HW: Dot11Radio1, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

チャネルの横のアスタリスクは、チャネルでレーダーが検出されたことを示します。

- リモート デバッグを起動するには、次のコマンドを入力します。

```
(Cisco Controller) > debug ap enable ap-name
(Cisco Controller) > debug ap command command ap-name
```

- DFS チャネルのレーダー検出と過去のレーダー検出を確認するためのデバッグ コマンドは、次のようになります。

show mesh dfs channel *channel-number*
show mesh dfs history

以下のような情報が表示されます。

ap1520-rap # **show mesh dfs channel** 132

```
Channel 132 is available
Time elapsed since radar last detected: 0 day(s), 7 hour(s), 6 minute(s), 51 second(s).
```

RAP はすべてのチャネルを調べ、各チャネルにアクティブなレーダーがあるかどうかを判断する必要があります。

```
ap1520-rap # show mesh dfs channel 132

Radar detected on channel 132, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 7 minute(s), 11 second(s)).
Channel is set to 100 (Time Elapsed: 0 day(s), 7 hour(s), 7 minute(s), 11 second(s)).
Radar detected on channel 116, channel becomes unusable (Time Elapsed: 0 day(s), 7
hour(s), 6 minute(s), 42 second(s)).
Channel is set to 64 (Time Elapsed: 0 day(s), 7 hour(s), 6 minute(s), 42 second(s)).
Channel 132 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 37 minute(s), 10
second(s)).
Channel 116 becomes usable (Time Elapsed: 0 day(s), 6 hour(s), 36 minute(s), 42
second(s)).
```

DFS のモニタ

DFS 履歴は、レーダーを検出するために、毎朝、またはより頻繁に実行する必要があります。この情報は消去されず、メッシュ アクセス ポイントのフラッシュに保存されます。そのため、ユーザは時間を合わせるだけで済みます。

```
ap1520-rap # show controller dot11Radio 1
```

以下に類似した情報が表示されます。

```
interface Dot11Radio1
```

```
Radio Hammer 5, Base Address 001c.0e6c.9c00, BBlock version 0.00, Software version 0.05.30
Serial number: FOC11174XCW
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: ETSI (OFDM) (EU) (-E)
Uniform Spreading Required: Yes
Current Frequency: 5540 MHz Channel 108 (DFS enabled)
Allowed Frequencies: *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *560
0(120) *5620(124) *5640(128) *5660(132) *5680(136) *5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)
Listen Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(6
0) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5660(132) 5680(136
) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165) 4950(20) 4955(21)
4960(22) 4965(23) 4970(24) 4975(25) 4980(26)
```

（注） アスタリスクは、このチャネルで DFS がイネーブルになっていることを示します。

周波数プランニング

隣接セクターの代替隣接チャネルを使用します。同じ場所に 2 つの RAP を展開する場合、それらの間に 1 つのチャネルを残しておく必要があります。

気象レーダーは 5600 ～ 5650 MHz 帯域で動作します。つまり、チャネル 124 および 128 が影響を受ける可能性があり、チャネル 120 と 132 も気象レーダーの活動に影響を受ける可能性があります。

メッシュ アクセス ポイントがレーダーを検出すると、コントローラとメッシュ アクセス ポイントは共にチャネルを設定されたチャネルとして保持します。コントローラはそれをメッシュ アクセス ポイントに関連付けられた揮発性メモリに保存し、メッシュ アクセス ポイントはそれを設定としてフラッシュに保存します。30 分の Quiet 時間後、コントローラは、メッシュ アクセス ポイントが新しいチャネルで設定されているかどうかに関係なく、メッシュアクセスポイントをスタティック値に戻します。これを避けるには、メッシュアクセスポイントを新しいチャネルで設定し、メッシュ アクセス ポイントをリブートします。

あるチャネルでレーダーが確実に検出されたら、次のように、そのチャネルおよび周囲の 2 つのチャネルを RRM 除外リストに追加する必要があります。

```
(Cisco Controller) > config advanced 802.11a channel delete channel
```

メッシュ アクセス ポイントは RRM によって選択された新しいチャネルに移行し、除外されたチャネルを考慮しません。

たとえば、チャネル 124 でレーダーが検出された場合、チャネル 120、124、および 128 を除外リストに追加する必要があります。さらに、RAP をそれらのチャネルで動作しないように設定します。

適切な信号対雑音比

ヨーロッパのインストールでは、信号対雑音比（SNR）の最小の推奨値が 20 dB に増えます。追加の dB は、DFS 以外の環境で検出されないパケット受信へのレーダー干渉の影響を緩和するために使用されます。

アクセス ポイントの配置

メッシュ アクセス ポイントのコロケーションには、最低 10 フィート（3.048 m）の垂直区切り、または 100 フィート（30.48 m）の水平区切りが必要です。

パケット エラー率のチェック

1 % 以上のエラー率が高いメッシュ アクセス ポイントには、ノイズと干渉に使用されるチャネルを変更するか、伝送パスに追加のメッシュ アクセス ポイントを追加して、メッシュ アクセス ポイントを別のセクターに移動するか、またはメッシュ アクセス ポイントを追加することによって、緩和策を適用する必要があります。

ブリッジ グループ名の誤った設定

メッシュ アクセス ポイントに、*bridgegroupname* が誤って指定され、意図されないグループに配置されることがあります。ネットワーク設計によっては、このメッシュアクセスポイントに到達して、その正しいセクターやツリーを見つけられたり、見つけられなかったりする可能性があります。メッシュアクセスポイントが互換性のあるセクターに到達できない場合、孤立状態になる可能性があります。

孤立状態のメッシュ アクセス ポイントを回復するために、デフォルトの bridgegroupname の概念がソフトウェアに導入されています。メッシュ アクセス ポイントは、設定された bridgegroupname を使用して他のメッシュ アクセス ポイントに接続できない場合、デフォルトの bridgegroupname を使用して接続を試みます。

この孤立状況の検出と回復のアルゴリズムは、次のようになります。

1. パッシブ スキャンを実行し、bridgegroupname に関係なく、すべてのネイバー ノードを検出します。
2. メッシュ アクセス ポイントは、AWPP を使用して、*my own bridgegroupname* でリッスンしたネイバーに接続します。
3. 手順 2 が失敗した場合、AWPP を使用して、デフォルトの bridgegroupname で接続を試みます。
4. 手順 3 で失敗した試行ごとに、ネイバーが除外リストに追加され、次の最適なネイバーへの接続が試行されます。
5. 手順 4 で AP がすべてのネイバーへの接続を失敗した場合、メッシュ アクセス ポイントがリブートされます。
6. 15 分間、デフォルトの bridgegroupname で接続した場合、メッシュ アクセス ポイントはスキャン状態になります。

メッシュ アクセス ポイントがデフォルトの bridgegroupname で接続できた場合、親ノードは、メッシュ アクセス ポイントをコントローラのデフォルトの子/ノード/ネイバー エントリとして報告するため、ネットワーク管理者は Cisco Prime Infrastructure になります。そのようなメッシュ アクセ

スポイントは通常の（非メッシュ）アクセスポイントとして動作し、すべてのクライアントを受け入れ、他のメッシュ ノードをその子とし、すべてのデータ トラフィックを通します。

（注） DEFAULT の未割り当ての BGN（NULL 値）と混同しないでください。これは、アクセス ポイントで独自の BGN を見つけられない場合に、接続に使用されるモードです。

メッシュ アクセス ポイントの BGN の現在の状態を確認するには、次のコマンドを入力します。

```
(Cisco Controller)> show mesh path Map3:5f:ff:60
00:0B:85:5F:FA:60 state UPDATED NEIGH PARENT DEFAULT (106B), snrUp 48, snrDown 48, linkSnr
 49
00:0B:85:5F:FB:10 state UPDATED NEIGH PARENT BEACON (86B) snrUp 72, snrDown 63, linkSrn 57
00:0B:85:5F:FA:60 is RAP
```

メッシュ アクセス ポイントの BGN の現在の状態を確認し、メッシュ アクセス ポイントのネイバー情報を確認するには、次の手順を実行します（GUI）。

[Wireless] > [All APs] > [AP Name] > [Neighbor info] を選択します。

図 *64*：子のネイバー情報

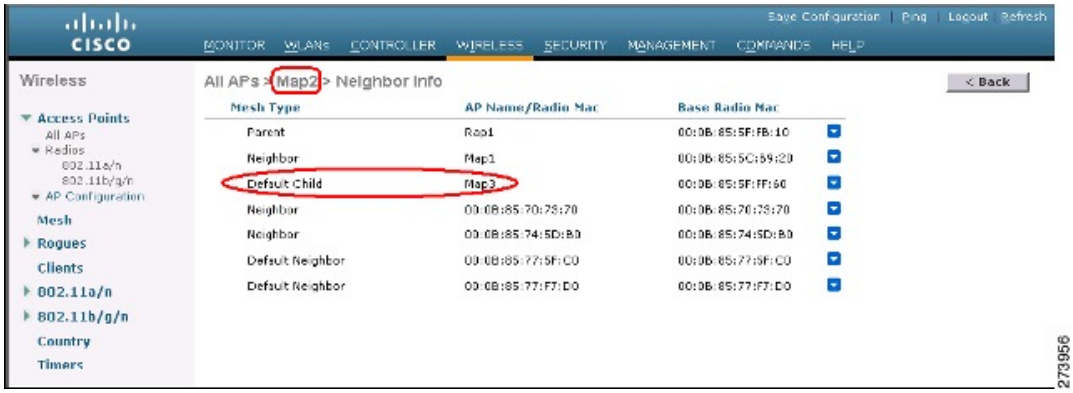


図 *65*：親のネイバー情報

メッシュ アクセス ポイントの IP アドレスの誤った設定

ほとんどのレイヤ 3 ネットワークは DHCP IP アドレス管理を使用して導入されますが、一部のネットワーク管理者は IP アドレスを手動で管理し、各メッシュ ノードに IP アドレスを静的に割り当てることを好みます。手動でのメッシュ アクセス ポイントの IP アドレスの管理は、大規模なネットワークでは悪夢になりかねませんが、小規模から中規模のネットワーク（10 ～ 100 メッシュ ノード程度）では、メッシュ ノードの数がクライアント ホスト数と比べてかなり少ないので道理にかなっています。

メッシュ ノードに IP アドレスをスタティックに設定すると、サブネットや VLAN などの誤ったネットワークに MAP を配置してしまう可能性があります。この誤りにより、メッシュ アクセス ポイントで、IP ゲートウェイを正しく解決できなくなり、WLAN コントローラを検出できなくなる可能性があります。そのようなシナリオでは、メッシュ アクセス ポイントがその DHCP メカニズムにフォールバックし、自動的に DHCP サーバを見つけて、IP アドレスを取得しようとします。このフォールバック メカニズムにより、誤って設定されたスタティック IP アドレスから、メッシュ ノードが孤立する可能性を回避し、ネットワーク上の DHCP サーバから正しいアドレスを取得できます。

手動で IP アドレスを割り当てる場合、最初に最も遠いメッシュ アクセス ポイントの子から IP アドレッシングを変更し、RAP まで戻ってくることを推奨します。これは、装置を移動する場合にも当てはまります。たとえば、メッシュアクセスポイントをアンインストールし、異なるアドレスが設定されたサブネットを持つメッシュ ネットワークの別の物理的場所に再展開する場合などです。

別のオプションは、RAP と共にレイヤ 2 モードのコントローラを、誤って設定された MAP がある場所に運ぶことです。設定変更が必要な MAP に一致するブリッジ グループ名を RAP に設定します。MAP の MAC アドレスをコントローラに追加します。メッシュ アクセス ポイントの概要詳細に、誤って設定された MAP が表示されたら、それを IP アドレスで設定します。

DHCP の誤った設定

DHCP フォールバック メカニズムがあっても、次のいずれかの状況が存在する場合に、メッシュ アクセス ポイントが孤立する可能性があります。

- ネットワークに DHCP サーバがない
- ネットワークに DHCP サーバがあるが、AP に IP アドレスを提供しないか、AP に誤った IP アドレスを提供している場合（誤った VLAN またはサブネット上など）。

こうした状況によって、誤ったスタティック IP アドレスで設定されているか、設定されていないか、または DHCP で設定されているメッシュ アクセス ポイントが孤立する可能性があります。このため、すべての DHCP 検出の試行回数、DHCP 再試行回数、または IP ゲートウェイ解決再試行回数を試しても接続できない場合、メッシュ アクセス ポイントがレイヤ 2 モードでコントローラの検出を試みることを確認する必要があります。言い換えると、メッシュ アクセス ポイントは、最初にレイヤ 3 モードでコントローラの検出を試み、このモードでスタティック IP（設定されている場合）と DHCP（可能な場合）の両方で試みます。次に、AP はレイヤ 2 モードで、コント

ローラの検出を試みます。レイヤ 3 およびレイヤ 2 モードの試行を何回か試みたら、メッシュ アクセス ポイントはその親ノードを変更し、DHCP 検出を再試行します。さらに、ソフトウェア除外リストに、正しい IP アドレスを取得できなかった親ノードが記載されます。

ノード除外アルゴリズムについて

メッシュネットワークの設計によっては、ノードがそのルーティングメトリックに従って、再帰的に真の場合でも、別のノードを「最適」だと判断することがありますが、ノードに正しいコントローラや正しいネットワークへの接続を提供することはできません。これは、誤った配置、プロビジョニング、ネットワークの設計のいずれかによって、または特定のリンクの AWPP ルーティング メトリックを、永続的または一時的な方法で最適化する状況を示す RF 環境の動的な性質によって、発生する典型的なハニーポットアクセスポイントのシナリオです。ほとんどのネットワークで、そのような状況の回復は一般に難しく、ノードを完全にブラックホール化またはシンクホール化し、ネットワークから除外させる可能性があります。次の現象が見られる場合がありますが、これらに限定されるわけではありません。

- ハニーポットにノードが接続しているが、静的 IP アドレスが設定されている場合に IP ゲートウェイが解決できない、または DHCP サーバから正しい IP アドレスが取得できない、あるいは WLAN コントローラに接続できない。
- いくつかの、または（最悪の場合）多数のハニーポット間をノードが循環している。

シスコのメッシュ ソフトウェアは、高度なノード除外リストアルゴリズムを使用してこの困難なシナリオを解決します。このノード除外リストアルゴリズムは、指数バックオフ、および TCP スライディング ウィンドウや 802.11 MAC などの高度な技術を使用します。

基本なアイデアは次の 5 つの手順に基づいています。

1. ハニーポットの検出：次の手順でハニーポットが最初に検出されます。

   次を試行することにより、AWPP モジュールによって親ノードが設定されます。

   - CAPWAP モジュールの固定 IP アドレス
   - DHCP モジュールの DHCP
   - CAPWAP による障害が発生したコントローラの検出および接続

2. ハニーポットの確定：ハニーポットが検出されると、それが確定されるまでの期間、除外リストのデータベースに配置されます。デフォルト値は 32 分です。その後、現在のメカニズムに障害が発生すると次にフォールバックされ、次の順序で他のノードが親になるよう試行されます。

   - 同じチャネル
   - 別のチャネル（最初は独自のブリッジグループ名を持つチャネル、次にデフォルトのチャネル）
   - 現在のすべての除外リストのエントリの確定をクリアした、別のサイクル
   - AP のリブート

3 非ハニーポットの信用：ノードが実際にはハニーポットではないにもかかわらず、次のような一時的なバックエンド状態によってハニーポットとして表示されることがよくあります。

- DHCP サーバが、起動して実行していないか、一時的に障害が発生している、あるいはリブートが必要な状態
- WLAN コントローラが、起動して実行していないか、一時的に障害が発生している、あるいはリブートが必要な状態
- RAP 上のイーサネット ケーブルが誤って外れている状態

このような非ハニーポットは、ノードができるだけ早くサービス状態に戻れるように正しく信用される必要があります。

4 ハニーポットの期限：期限に達すると、除外リストのノードは除外リストのデータベースから削除され、AWPP によって今後のために通常の状態に戻る必要があります。

5 ハニーポットのレポート：コントローラへの LWAPP のメッシュ ネイバー メッセージを介してコントローラにハニーポットがレポートされます。レポートは [Bridging Information] ページに表示されます。メッセージは、最初に除外リストに記載されたネイバーが見られた際にも表示されます。後続のソフトウェア リリースでは、このような状況が発生した場合、コントローラで SNMP トラップが生成され、Cisco Prime Infrastructure で記録できるようになります。

図 *66*：除外ネイバー

多くのノードは予定のイベントまたは予定外のイベント後にネットワークに加入または再加入を試みる可能性があるので、16 分のホールドオフ時間が実装されます。これは、システム初期化後、16 分間はノードが除外リストに追加されないことを意味します。

この指数バックオフおよび高度なアルゴリズムは独特であり、次のプロパティがあります。

- 親ノードが本当にハニーポットなのか、それとも一時的に機能が停止しているだけなのかをノードによって正しく判断できるようにします。
- ノードのネットワークへの接続が維持された時間に基づいて、良好な親ノードであると信用します。信用することで、本当に一時的な状況の場合は除外リストの確定時間をきわめて短くすることができ、中程度の機能停止の場合は適度にすることができます。

- 組み込みのヒステリシス機能があります。これは、多くのノードが同じネットワーク内に存在しないかどうか互いのノードの検出を試みている場所で初期状態の問題が発生した場合に使用されます。
- 組み込みメモリがあります。これは、除外リストデータベースでかつて親ノードとして登録されていた場合（あるいは今後親ノードになる場合）、現在誤って親ノードと見なされないように、時々ネイバーになり得るノードに使用されます。

ノード除外リストアルゴリズムは、メッシュネットワークの重大な孤立を防ぎます。このアルゴリズムは、ノードが迅速に再コンバージェンスして、正しいネットワークを探すことができる方法で AWPP に統合されます。

スループット分析

スループットはパケット エラー レートおよびホップ カウントによって決まります。

容量とスループットは直交概念です。スループットはノード N でのユーザ エクスペリエンスです。領域の合計容量はN個のノードの全体のセクターで計算され、入力および出力RAP数に基づいています。また個別の妨害チャネルがないことを想定しています。

たとえば、10 Mbps での 4 つの RAP はそれぞれ合計容量 40 Mbps を配信します。1 ユーザが 2 つのホップを経由する場合、論理的には各 RAP で TPUT ごとに 5 Mbps を受信できることになり、40 Mbps のバックホール容量を消費します。

Cisco Mesh ソリューションを使用する場合、ホップごとの遅延は 10 ミリ秒未満で、ホップごとの遅延の範囲は標準で 1 ～ 3 ミリ秒です。ジッタ全体も 3 ミリ秒未満になります。

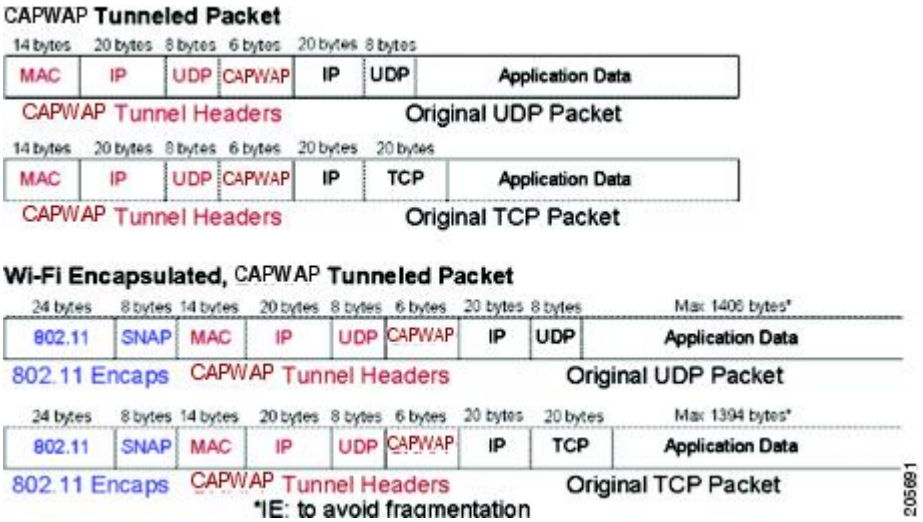
スループットは、ユーザ データグラム プロトコル（UDP）または Transmission Control Protocol（TCP）という、ネットワークを通過するトラフィックのタイプによって決まります。UDPはイーサネット経由で送信元アドレスおよび送信先アドレスを持つパケットおよびUDP プロトコルのヘッダーを送信します。確認応答（ACK）は行われません。パケットがアプリケーション層で配信されるかどうかは保証されません。

TCP は UDP と似ていますが、信頼性のあるパケット配信メカニズムです。パケットの ACK が行われ、スライディング ウィンドウ技術を使用することによって ACK を待つ前に送信者が複数のパケットを送信できます。クライアントが送信するデータの最大量が決められています（TCP ソケットバッファ ウィンドウと呼びます）。シーケンス番号により、送信したパケットを追跡し、パケットを正しい順序で到着させることができます。TCPは累積的にACKを使用し、現在どのくらいのストリームが受信されたかを受信側がレポートします。ACK は TCP のウィンドウ サイズ内であればいくつでもパケットを扱うことができます。

TCP はスロー スタートおよび乗法減少を使用してネットワーク輻輳やパケット損失に対応します。パケットが損失すると TCP ウィンドウは半分になり、バックオフ再送信タイマーが急激に増加します。ワイヤレスはインターフェイスの問題によりパケット損失の影響を受けますが、TCP はこのパケット損失に応答します。パケット損失からリカバリする際に接続が切断されないように、スロー スタート リカバリ アルゴリズムも使用されます。これらのアルゴリズムは、損失の多いネットワーク環境でトラフィック ストリーム全体のスループットを減少させる効果があります。

デフォルトでは、TCP の最大セグメント サイズ（MSS）は 1460 バイトで、1500 バイトの IP データグラムになります。TCP は 1460 バイトを超えるデータ パケットを分割し、スループットが少なくとも 30 % 減少します。さらに図 67：CAPWAP でトンネリングされたパケット，（234 ページ） に示されているように、コントローラによって IP データグラムが 48 バイトの CAPWAP トンネル ヘッダーにカプセル化されます。1394 バイトを超えるデータ パケットもコントローラによって分割され、スループットが最大 15 % 減少します。

図 *67*：*CAPWAP* でトンネリングされたパケット



第 9 章

Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理

Cisco Prime Infrastructure は、企業全体の WLAN システム管理を行う最適なプラットフォームです。Cisco WCS は、メッシュを仮想化およびコントロールするための広範囲のツールを提供します。これらは、信号対雑音比のヒストグラム、メッシュの詳細情報、メッシュ アクセス ポイントのネイバーおよびリンク情報、7 日間の一時リンク情報、および電波干渉を特定し避けるツールなどを含みます。

この項では、次の Prime Infrastructure モニタリング機能について説明します。

- マップを使用したメッシュ ネットワークのモニタリング
- メッシュ アクセス ポイントの状態のモニタリング
- メッシュ アクセス ポイントのメッシュ統計情報の表示
- メッシュ ネットワーク階層の表示
- メッシュ フィルタを使用したマップ画面およびメッシュ リンクの修正

- Cisco Prime Infrastructure によるキャンパス マップ、屋外領域およびビルディングの追加，236 ページ
- Cisco Prime Infrastructure によるマップへのメッシュ アクセス ポイントの追加，239 ページ
- Google Earth を使用したメッシュ アクセス ポイントのモニタリング，240 ページ
- Cisco Prime Infrastructure への屋内メッシュ アクセス ポイントの追加，244 ページ
- Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理，245 ページ
- ワークグループ ブリッジのモニタリング，261 ページ
- AP の [Last Reboot Reason] の表示，268 ページ

Cisco Prime Infrastructure によるキャンパス マップ、屋外領域およびビルディングの追加

メッシュ ネットワークを設定するには、次の順序でマップおよびマップ上のアイテム（ビルディングおよびメッシュ アクセス ポイント）を Cisco Prime Infrastructure に追加します。

ステップ 1 キャンパス マップを追加します。
ステップ 2 屋外領域マップを追加します。
ステップ 3 ビルディングを追加します。
ステップ 4 メッシュ アクセス ポイントを追加します。
これらのマップおよびコンポーネントを追加する詳細な手順を次に示します。

キャンパス マップの追加

単一のキャンパス マップを Cisco Prime Infrastructure データベースに追加するには、次の手順を実行します。

ステップ 1 マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。
（注） マップは任意のサイズにできます。これは、Prime Infrastructure が作業領域に適合するようマップを自動的にサイズ変更するためです。
ステップ 2 ファイル システムの任意の場所にあるマップを参照して、インポートします。
ステップ 3 [Monitor] > [Maps] を選択して、[Maps] ページを表示します。
ステップ 4 [Select a command] ドロップダウン リストから [New Campus] を選択し、[GO] をクリックします。
ステップ 5 [Maps > New Campus] ページで、キャンパス名とキャンパス問い合わせ先の名前を入力します。
ステップ 6 キャンパス マップが含まれているイメージ ファイル名を参照および選択してから、[Open] をクリックします。
ステップ 7 [Maintain Aspect Ratio] チェックボックスをオンにして、Prime Infrastructure でマップのサイズが変更されたときに、縦横比が変わらないようにします。
ステップ 8 マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。
（注） 水平方向スパンと垂直方向スパンは、キャンパスに追加するビルディングやフロア図面よりも大きい値にする必要があります。

ステップ 9 [OK] をクリックして、このキャンパス マップを Prime Infrastructure データベースに追加します。Prime Infrastructure に、データベース内のマップ、マップの種類、およびキャンパスのステータスの一覧を含む [Maps] ページが表示されます。

屋外領域の追加

屋外領域をキャンパス マップに追加するには、次の手順を実行します。

（注） 屋外領域マップがデータベース内にあるかどうかに関係なく、屋外領域を Cisco Prime Infrastructure データベース内のキャンパス マップに追加することができます。

ステップ 1 屋外領域のマップをデータベースに追加する場合は、マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。ファイル システムの特定の場所にあるマップを参照して、インポートします。

（注） 屋外領域を追加するのにマップは必要ありません。屋外領域をデータベースに追加するため、領域の寸法を定義する必要があるだけです。Cisco Prime Infrastructure では、作業領域に合わせてマップのサイズが自動的に調整されるため、マップは任意のサイズにすることができます。

ステップ 2 [Monitor] > [Maps] を選択して、[Maps] ページを表示します。

ステップ 3 目的のキャンパスをクリックします。Cisco Prime Infrastructure によって、[Maps > Campus Name] ページが表示されます。

ステップ 4 [Select a Command] ドロップダウン リストから [New Outdoor Area] を選択し、[GO] をクリックします。

ステップ 5 [Campus Name > New Outdoor Area] ページで、管理可能な屋外領域を作成する手順は、次のとおりです。

a) 屋外領域名を入力します。
b) 屋外領域問い合わせ先の名前を入力します。
c) 必要に応じて、屋外領域マップのファイル名を入力または参照します。
d) 屋外領域のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

ヒント ヒント：**Ctrl キーを押した状態でクリックする**ことで、キャンパス マップの左上隅にある境界領域のサイズを変更することもできます。境界領域のサイズを変更すると、屋外領域の水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

e) [Place] をクリックして、屋外領域をキャンパス マップ上に配置します。Cisco Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更された屋外領域の四角形が作成されます。
f) 屋外領域の四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。
g) [Save] をクリックして、この屋外領域とキャンパス上の位置をデータベースに保存します。Cisco Prime Infrastructure では、キャンパス マップ上の屋外領域の四角形の中に屋外領域名が保存されます。

（注） 屋外領域には、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 6 **[Save]** をクリックします。

キャンパス マップへのビルディングの追加

キャンパス マップをデータベースに追加したことがあるかどうかに関係なく、ビルディングを Cisco Prime Infrastructure データベースに追加できます。ここでは、ビルディングをキャンパス マップに追加する方法、または独立したビルディング（キャンパスの一部ではないビルディング）を Prime Infrastructure データベースに追加する方法を説明します。

Prime Infrastructure データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Maps] を選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。Cisco Prime Infrastructure によって、[Maps] > [Campus Name] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4 [Campus Name > New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成する手順は、次のとおりです。

a) ビルディング名を入力します。
b) ビルディング問い合わせ先の名前を入力します。
c) 地上のフロア数と地下のフロア数を入力します。
d) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。
ヒント：水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上にある境界領域のサイズを変更できます。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。
e) [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。Cisco Prime Infrastructure では、キャンパスマップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。
f) ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。
（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。
g) [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。Cisco Prime Infrastructure では、キャンパス マップ上のビルディングの四角形の中にビルディング名が保存されます。
（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5 **[Save]** をクリックします。

Cisco Prime Infrastructure によるマップへのメッシュ アクセス ポイントの追加

.PNG、.JPG、.JPEG、または .GIF 形式のフロア図面と屋外領域のマップを Cisco Prime Infrastructure データベースに追加した後に、メッシュ アクセス ポイント アイコンをマップ上に配置して、ビルディング内の設定位置を示すことができます。

メッシュ アクセス ポイントをフロア図面と屋外領域のマップに追加する手順は、次のとおりです。

ステップ 1 [General] タブの [Coverage Areas] コンポーネントで、目的のフロア図面または屋外領域のマップをクリックします。Cisco Prime Infrastructure に、アソシエートされたカバレッジ領域マップが表示されます。

ステップ 2 [Select a Command] ドロップダウン リストから、[Add Access Points] を選択し、[GO] をクリックします。

ステップ 3 [Add Access Points] ページで、マップに追加するメッシュ アクセス ポイントを選択します。

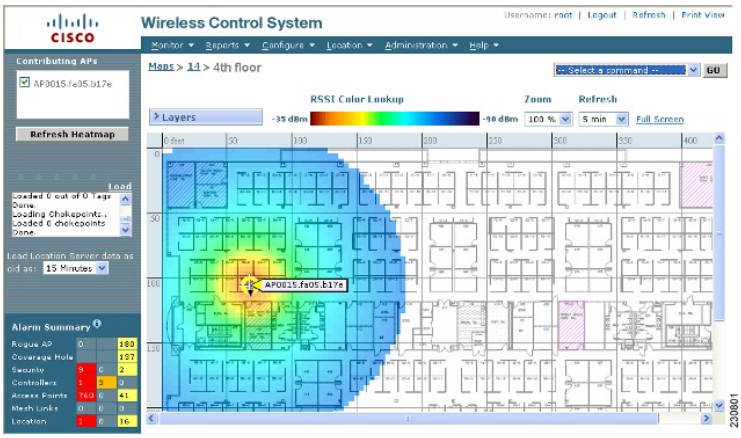
ステップ 4 [OK] をクリックして、メッシュ アクセス ポイントをマップに追加し、[Position Access Points] マップを表示します。

（注） メッシュ アクセス ポイント アイコンがマップの左上の領域に表示されます。

ステップ 5 アイコンをクリックしてドラッグし、物理位置を示します。

ステップ 6 各アイコンをクリックして、サイドバーでアンテナの方向を選択します。

図 *68*：アンテナ サイドバー



アンテナの角度は、マップの X 軸に対して相対的です。X（水平）座標および Y（垂直）座標の原点はマップの左上の角であるため、0 度はメッシュ アクセス ポイントの Side A を右に、90 度は Side A を下に、180 度は Side A を左に向けることになります。アンテナの Elevation（垂直面）は、最大 90 度までアンテナを垂直（上下）に移動するために使用されます。

各メッシュ アクセス ポイントがマップ上の正しい位置に設置されていること、またアンテナの方向が正しいことを確認します。マップを使用してカバレッジホールや不正アクセスポイントを発見するときは、正確なメッシュ アクセス ポイントの位置決めが重要です。

アンテナの Elevation（垂直面）および方向パターンの詳細については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

ステップ 7 [Save] をクリックして、メッシュ アクセス ポイントの位置と方向を保存します。Cisco Prime Infrastructure によって、カバレッジ領域の RF 予測が計算されます。この RF 予測は、カバレッジ領域マップ上の RF 信号の相対強度を示しているため、一般的には「ヒート マップ」として知られています。

（注） この表示は、乾式壁や金属の物体など、さまざまな建築資材の減退は考慮されていないため、実際の RF 信号の強度の近似値に過ぎません。また、RF 信号が障害物に反射する影響も表示されていません。

Google Earth を使用したメッシュ アクセス ポイントのモニタリング

Cisco Prime Infrastructure では、 Google Earth Map Plus と Google Earth Map Pro の両方がサポートされ、メッシュ アクセス ポイントおよびそのリンクがあれば表示されます。

Cisco Prime Infrastructure からの Google Earth の起動

Cisco Prime Infrastructure では、Google Earth Map Plus と Google Earth Map Pro の両方がサポートされ、メッシュ アクセス ポイントおよびそのリンクがあれば表示されます。

Google Earth マップを起動する手順は、次のとおりです。

ステップ 1 Google Earth Plus または Google Earth Pro を起動し、新しいフォルダを追加します。

ステップ 2 Google Earth Plus または Google Earth Pro にメッシュ アクセス ポイントの目印を作成します。

（注） Prime Infrastructure によってメッシュ アクセス ポイントが正しく認識されるように、目印を作成する際はメッシュ アクセス ポイントの正確な名前を使用する必要があります。

ステップ 3 新しいフォルダにメッシュアクセスポイントの目印を配置します。.KML ファイル形式でフォルダを保存します。

ステップ 4 Prime Infrastructure で、[Monitor] > [Google Earth Maps] を選択します。[Select a command] ドロップダウンリストから、[Import Google KML] を選択します。

ステップ 5 新しい Google KML フォルダをインポートします。フォルダ名の概要が表示されます。

図 *69*：*Google Earth* への新しいフォルダのインポート

ステップ 6 新しいフォルダの隣にある起動アイコンをクリックして、Prime Infrastructure から Google Earth マップを起動します。

Google Earth マップの表示

Google Earth マップを使用して、キャンパス マップ、メッシュ アクセス ポイントおよびリンク情報を表示できます。

Google Earth マップを表示する手順は、次のとおりです。

ステップ 1 Cisco Prime Infrastructure にログオンします。

ステップ 2 [Monitor] > [Google Earth Maps] の順に選択します。[Google Earth Maps] ページが開き、すべてのフォルダと、各フォルダに含まれるメッシュ アクセス ポイントの数が表示されます。

ステップ 3 表示するマップの [Launch] をクリックします。Google Earth が別ウィンドウでオープンし、ロケーションおよびそのメッシュ アクセス ポイントが表示されます。

（注） この機能を使用するには、コンピュータに Google Earth をインストールし、サーバからデータを受け取った時点で自動的に起動するように設定しておく必要があります。Google Earth は Google の Web サイトからダウンロードできます。

図 *70*：*[Google Earth Map]* ページ

ステップ 4 表示するマップの [Launch] をクリックします。Google Earth が別ウィンドウでオープンし、ロケーションおよびそのメッシュ アクセス ポイントが表示されます。

（注） この機能を使用するには、コンピュータに Google Earth をインストールし、サーバからデータを受け取った時点で自動的に起動するように設定しておく必要があります。Google Earth は Google の Web サイトからダウンロードできます。

図 *71*：*Google Earth Map* におけるメッシュ アクセス ポイントの詳細

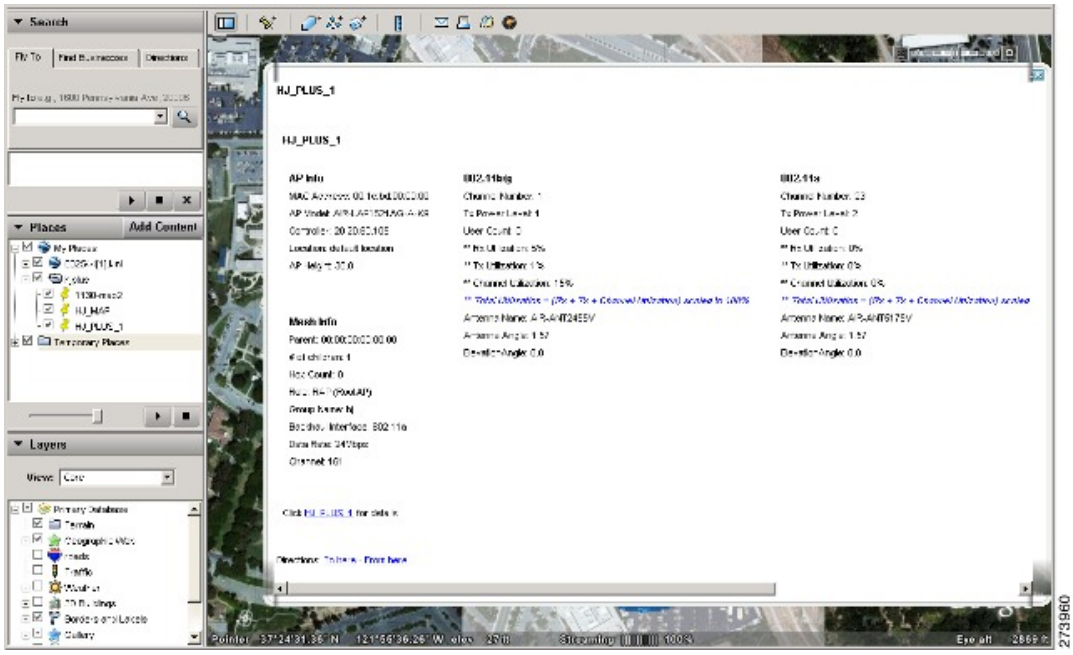


図 *72*：*Google Earth Map* におけるメッシュ リンクの詳細

Google Earth Map フォルダの詳細を表示する手順は、以下のとおりです。

ステップ 5 [Google Earth Map] ページで、目的のフォルダの名前をクリックして、そのフォルダの詳細ページを開きます。[Google Earth Details] ページには、メッシュ アクセス ポイントの名前と MAC アドレスまたは IP アドレスが表示されます。

（注） メッシュ アクセス ポイントを削除するには、該当するチェックボックスをオンにして、[Delete] をクリックします。フォルダ全体を削除するには、[Folder Name] の隣のチェックボックスをオンにして、[Delete] をクリックします。フォルダを削除すると、そのフォルダ内のすべてのサブフォルダとメッシュ アクセス ポイントが削除されます。

ステップ 6 [Cancel] をクリックして、詳細ページを閉じます。

Cisco Prime Infrastructure への屋内メッシュ アクセス ポイントの追加

屋内アクセス ポイントをブリッジ モードに直接設定して、これらのアクセス ポイントをメッシュ アクセス ポイントとして直接使用できます。それらの屋内アクセス ポイントがローカル モード（非メッシュ）になっている場合は、それらのアクセスポイントをコントローラに接続し、ラジオの役割をブリッジモード（メッシュ）に変更する必要があります。このタスクは、特に、配置しているアクセス ポイントの数が多い場合、アクセス ポイントがすでに従来の非メッシュ ワイヤレス カバレッジ用にローカル モードで配置されている場合、面倒になることがあります。

ローカル モードのメッシュ アクセス ポイントの場合、メッシュをインストールする前に、まずすべての屋内メッシュ アクセス ポイントをコントローラに接続し、モードとブリッジ モードに変更する必要があります。

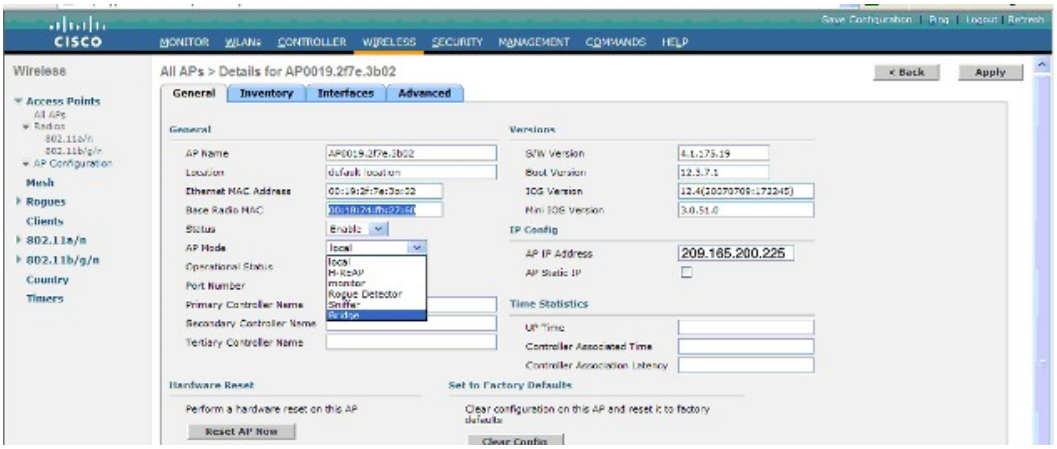
そのためには、すべての屋内アクセス ポイントを管理 IP アドレスと同じサブネット上のレイヤ 3 ネットワークに接続します。

屋内メッシュ 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 リストに追加します。すべての屋内アクセス ポイントがローカル モードでコントローラに接続されます。

Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理

その後、コントローラでそれぞれの屋内アクセス ポイントをローカル モードからブリッジ モードに変更できます。

図 *73*：*[All APs] > [AP Details Controller]* ページ



コントローラ上で屋内アクセス ポイントをブリッジ モードに変更したあと、これらの屋内メッシュ アクセス ポイントを Prime Infrastructure に追加します。

最初に、Prime Infrastructure から屋内メッシュ アクセス ポイントをブリッジ モードに設定することはできません。

Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理

Cisco Prime Infrastructure は、企業全体の WLAN システム管理を行う最適なプラットフォームです。Cisco WCS は、メッシュを仮想化およびコントロールするための広範囲のツールを提供します。これらは、信号対雑音比のヒストグラム、メッシュの詳細情報、メッシュ アクセス ポイントのネイバーおよびリンク情報、7 日間の一時リンク情報、および電波干渉を特定し避けるツールなどを含みます。

この項では、次の Prime Infrastructure モニタリング機能について説明します。

- マップを使用したメッシュ ネットワークのモニタリング
- メッシュ アクセス ポイントの状態のモニタリング
- メッシュ アクセス ポイントのメッシュ統計情報の表示
- メッシュ ネットワーク階層の表示
- メッシュ フィルタを使用したマップ画面およびメッシュ リンクの修正

マップを使用したメッシュ ネットワークのモニタリング

Cisco Prime Infrastructure のメッシュ ネットワーク マップから、次の要素の詳細にアクセスして表示することができます。

- Mesh Link Statistics
- Mesh Access Points
- Mesh Access Point Neighbors

この情報へのアクセス方法とこれらの各項目に対して表示された情報の詳細は、次の項に説明されています。

マップを使用したメッシュ リンクの統計のモニタリング

特定のメッシュ ネットワーク リンクの SNR、そのリンク上で送受信されたパケットの数を表示し、[Monitor > Maps] 画面からリンク テストを開始できます。

2 つのメッシュ アクセス ポイント間またはメッシュ アクセス ポイントとルート アクセス ポイント間の特定のメッシュ リンクに関する詳細を表示するには、次の手順を実行します。

ステップ 1 Cisco Prime Infrastructure で、[Monitor] > [Maps] を選択します。

ステップ 2 モニタする屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 3 カーソルを目的のリンクに対するリンク矢印上に移動します。[Mesh Link] ページが表示されます。

（注） マップ上にリンクを表示するには、[Layers] ドロップダウン リスト下の [AP Mesh Info] チェックボックスをオンにする必要があります。

ステップ 4 [Link Test]、[Child to Parent] または [Link Test]、[Parent to Child] のいずれかをクリックします。リンク テストが完了すると、結果のページが表示されます。

（注） リンク テストは 30 秒間稼働します。

（注） リンク テストを両方のリンク（子対親と親対子）に同時に実行できません。

ステップ 5 SNR 統計をある期間にわたってグラフィカルに表示するには、リンク上の矢印をクリックします。複数の SNR グラフを含むページが表示されます。

表示されるリンクのグラフは、次のとおりです。

- [SNR Up]：メッシュ アクセス ポイントの視点からのネイバーの RSSI 値を描画します。
- [SNR Down]：ネイバーがメッシュ アクセス ポイントへレポートする RSSI 値を描画します。
- [Link SNR]：SNR Up 値に基づく重み付けされフィルタ処理された測定を描画します。

- [Adjusted Link Metric]：ルート メッシュ アクセス ポイントへの最小コストのパスを決定するために使用された値を描画します。この値により、簡単に屋上アクセス ポイントに到達してホップ カウントを明らかにできます。この値が低くなるほど、パスは使用されにくくなります。
- [Unadjusted Link Metric]：ホップ カウントによって未調整のルート アクセス ポイントに到達する最小コストのパスを描画します。未調整のリンクの値が高いほど、パスが効果的であることを示します。

マップを使用したメッシュ アクセス ポイントのモニタリング

メッシュ ネットワーク マップから、次のメッシュ アクセス ポイントの概要を表示することができます。

- 親
- 子の数
- ホップ カウント
- ロール
- グループ名
- バックホール インターフェイス
- データ レート
- チャネル

（注） この情報は、すべてのメッシュ アクセス ポイントに表示される情報に追加されたものです（MAC アドレス、メッシュ アクセス ポイント モデル、コントローラ IP アドレス、位置、メッシュ アクセス ポイントの高さ、メッシュ アクセス ポイントのアップ タイム、および CAPWAP アップ タイム）。

メッシュ アクセス ポイントの設定情報の概要と詳細をメッシュ ネットワーク マップから表示するには、次の手順を実行します。

ステップ 1 Cisco Prime Infrastructure の GUI で、[Monitor] > [Maps] を選択します。

ステップ 2 モニタするメッシュ アクセス ポイントの屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 3 メッシュ アクセス ポイントの設定情報の概要を表示するには、カーソルをモニタするメッシュ アクセス ポイント上に移動します。選択したメッシュ アクセス ポイントの設定情報が記載されたページが表示されます。

ステップ 4 メッシュ アクセス ポイントの詳細な設定情報を表示するには、メッシュ アクセス ポイント ラベルの矢印部分をクリックします。メッシュ アクセス ポイントの設定の詳細が表示されます。

（注） メッシュ アクセス ポイントに IP アドレスがある場合には、メッシュ アクセス ポイント パネルの下部に [Run Ping Test] リンクも表示されます。

ステップ 5 [Access Point] 設定ページで次の手順に従って、メッシュ アクセス ポイントの設定の詳細を表示します。

a) [General] タブを選択し、AP 名、MAC アドレス、AP のアップ タイム、アソシエートされているコントローラ（登録済みおよびプライマリ）の動作ステータス、ソフトウェア バージョンなど、メッシュ アクセス ポイントの全般的な設定を表示します。

（注） メッシュ アクセス ポイントのソフトウェア バージョンには、*m* の文字と *mesh* という単語をカッコで囲んだものが付加されます。

b) [Interface] タブを選択し、メッシュ アクセス ポイントでサポートされるインターフェイスの設定詳細を表示します。インターフェイスのオプションは無線とイーサネットです。

c) [Mesh Links] タブを選択し、メッシュ アクセス ポイントの親およびネイバーの詳細（名前、MAC アドレス、パケット エラー率、およびリンク詳細）を表示します。このパネルからリンク テストを開始することもできます。

d) [Mesh Statistics] タブを選択し、メッシュ アクセス ポイントのブリッジ、キュー、およびセキュリティの統計に関する詳細を表示します。メッシュ統計情報の詳細については、「メッシュ アクセス ポイントのメッシュ統計情報の表示」の項を参照してください。

マップを使用したメッシュ アクセス ポイント ネイバーのモニタリング

メッシュ アクセス ポイントのネイバーの詳細をメッシュ ネットワーク マップから表示する手順は、次のとおりです。

ステップ 1 [Monitor] > [Maps] を選択します。

ステップ 2 モニタする屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 3 メッシュ アクセス ポイントのメッシュ リンクに関する詳細を表示するには、アクセス ポイント ラベルの矢印部分をクリックします。[Access Point] 画面が表示されます。

ステップ 4 [Mesh Links] タブをクリックします。

（注） マップ上のメッシュ アクセス ポイントの上にマウスを置いたときに表示されるメッシュ アクセス ポイントの設定概要パネルで、[View Mesh Neighbors] リンクをクリックすることにより、選択したメッシュ アクセス ポイントのネイバーのメッシュ リンク詳細を表示することもできます。

（注） 信号対雑音比（SNR）は、[View Mesh Neighbors] パネルにだけ表示されます。

（注） 表示されたパネルには現在および過去のネイバーの一覧に加えて、選択したメッシュ アクセス ポイント、ネイバー メッシュ アクセス ポイント、および子メッシュ アクセス ポイントを特定するためのラベルが、メッシュ アクセス ポイント マップのアイコンに表示されます。選択したメッシュ アクセス ポイントの [clear] リンクを選択して、マップから関係を示すラベルを削除します。

（注） メッシュ ネイバー ページの上部にあるドロップダウン リストには、表示されたマップの解像度（100 %）と表示された情報の更新間隔（5 分）が示されます。これらのデフォルト値は変更することができます。

メッシュ アクセス ポイントの状態のモニタリング

[Mesh Health] では、特に記載されている場合を除き、屋外および屋内メッシュ アクセス ポイントの全体的な状況をモニタします。この環境情報の追跡は、屋外に配置されたメッシュ アクセス ポイントの場合、特に重要です。次のようなファクタがモニタされます。

- 温度：メッシュ アクセス ポイントの内部温度（華氏と摂氏）を表示します（AP1500 のみ）。
- ヒーター ステータス：ヒーターのオン/オフを表示します（AP1500 のみ）。
- AP アップ タイム：メッシュ アクセス ポイントがアクティブで送受信できる状態になっている時間を表示します。
- CAPWAP 接続確立時間：CAPWAP 接続の確立に要した時間を表示します。
- CAPWAP アップ タイム：CAPWAP 接続がアクティブになっている時間を表示します。

Mesh Health 情報は、メッシュ アクセス ポイントの [General Properties] パネルに表示されます。

特定のメッシュ アクセス ポイントの Mesh Health の詳細を表示する手順は、次のとおりです。

ステップ 1 [Monitor] > [Access Points] の順に選択します。アクセス ポイントの一覧が表示されます

（注） [New Search] ボタンを使用しても、下図のメッシュ アクセス ポイントの概要を表示できます。[New Search] オプションを使用すると、表示されるアクセス ポイントの基準をさらに定義できます。検索の基準は、AP Type、AP Mode、Radio Type、および 802.11n Support です。

ステップ 2 [AP Name] リンクをクリックして、メッシュ アクセス ポイントの詳細を表示します。そのメッシュ アクセス ポイントの [General Properties] パネルが表示されます。

（注） Cisco Prime Infrastructure マップ ページからも、メッシュ アクセス ポイントの [General Properties] パネルにアクセスできます。パネルを表示するには、メッシュ アクセス ポイント ラベルの矢印部分をクリックします。タブ付きのパネルが表示され、選択したアクセス ポイントの [General Properties] パネルが表示されます。

表内の列の追加、削除、並べ替えを行うには、[Edit View] リンクをクリックします。表 28：モニタ アクセス ポイントの追加検索結果パラメータ，（250 ページ） は、[Edit View] ページで使用できるオプションのアクセス ポイントのパラメータを示しています。

表 *28*：モニタ アクセス ポイントの追加検索結果パラメータ

カラム	オプション
AP Type	アクセス ポイントの種類を示します（Unified または Autonomous）。
Antenna Azim.Angle	アンテナの水平方向の角度を示します。
Antenna Diversity	アンテナ ダイバーシティがイネーブルであるかディセーブルであるかを示します。アンテナ ダイバーシティは、適切なアンテナを選択するためにアクセス ポイントが 2 つの統合アンテナ ポートから無線信号をサンプリングすることをいいます。
Antenna Elev.Angle	アンテナの垂直方向の角度を示します。
Antenna Gain	無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）を示します。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 x 0.5 = 2dBm のゲインであることを意味します。

カラム	オプション
Antenna Mode	全方向性、指向性、または不適切などのアンテナモードを示します。
Antenna Name	アンテナの名前または種類を示します。
Antenna Type	内部アンテナか、外部アンテナかを示します。
Audit Status	次の監査ステータスのいずれかを示します。 • [Mismatch]：最新の監査で、Cisco Prime Infrastructure とコントローラ間の設定の相違が検出された。 • [Identical]：最新の監査で、設定の相違は検出されなかった。 • [Not Available]：監査ステータスは使用できない。
Bridge Group Name	必要に応じて、アクセスポイントが属するブリッジグループの名前を示します。
CDP Neighbors	全方向に接続したシスコ デバイスを示します。
Channel Control	チャネル コントロールが自動かカスタムかを示します。
Channel Number	Cisco 無線がブロードキャストしているチャネルを示します。
Controller Port	コントローラ ポートの数を示します。
Node Hops	アクセス ポイント間のホップ カウントを示します。
POE Status	アクセス ポイントの Power-over-Ethernet ステータスを示します。表示される値は次のとおりです。 • [Low]：イーサネットから供給されるアクセス ポイントの電力が低い。 • [Lower than 15.4 volts]：イーサネットから供給されるアクセス ポイントの電力が ?15.4 V 未満。 • [Lower than 16.8 volts]：イーサネットから供給されるアクセス ポイントの電力が ?16.8 V 未満。 • [Normal]：アクセスポイントの操作に十分な電力が供給されている。 • [Not Applicable]：電源がイーサネットではない。

カラム	オプション
Primary Controller	このアクセスポイントのプライマリ コントローラの名前を示します。
Radio MAC	無線の MAC アドレスを示します。
Reg. Domain Supported	規制区域がサポートされているかどうかを示します。
Serial Number	アクセス ポイントのシリアル番号を示します。
Slot	スロット番号を示します。
Tx Power Control	送信電力コントロールが自動かカスタムかを示します。
Tx Power Level	送信電力レベルを示します。
Up Time	アクセスポイントが送受信できる状態になっている時間（日、時間、分、秒）を示します。
WLAN Override Names	WLAN のオーバーライド プロファイル名を示します。
WLAN Override	WLAN のオーバーライドがイネーブルかディセーブルかを示します。各アクセス ポイントは 16 個の WLAN プロファイルに限定されます。各アクセス ポイントは、WLAN override 機能が有効にされない限り、すべての WLAN プロファイルをブロードキャストします。WLAN override 機能によって、アクセス ポイントごとに 16 個の任意の WLAN プロファイルを無効にできます。

メッシュ アクセス ポイントのメッシュ統計情報の表示

子メッシュ アクセス ポイントの認証の際、または子メッシュ アクセス ポイントの親メッシュ アクセス ポイントへのアソシエートの際に、メッシュの統計が報告されます。

子メッシュアクセスポイントがコントローラからのアソシエートを解除すると、セキュリティのエントリは削除され、表示されなくなります。

メッシュ アクセス ポイントに対して、次のメッシュ セキュリティの統計が表示されます。

- ブリッジング
- キュー
- セキュリティ

特定のメッシュ アクセス ポイントのメッシュ統計情報を表示する手順は、次のとおりです。

ステップ 1 [Monitor] > [Access Points] の順に選択します。アクセス ポイントの一覧が表示されます

（注） [New Search] ボタンを使用しても、アクセス ポイントの概要を表示できます。[New Search] オプションを使用すると、表示されるアクセス ポイントの基準をさらに定義できます。検索基準には、[AP Name]、[IP address]、[MAC address]、[Controller IP or Name]、[Radio type]、および [Outdoor area] が含まれます。

ステップ 2 目的のメッシュ アクセス ポイントの [AP Name] リンクをクリックします。
タブ付きのパネルが表示され、選択したメッシュ アクセス ポイントの [General Properties] ページが表示されます。

ステップ 3 [Mesh Statistics] タブをクリックします。3 つのタブが付いた、[Mesh Statistics] パネルが表示されます。

（注） [Mesh Statistics] タブとその下位のタブ（[Bridging]、[Queue]、[Security]）は、メッシュ アクセス ポイントに対してだけ表示されます。[Mesh Link Alarms] および [Mesh Link Events] リンクは、3 つのタブ付きパネルのそれぞれからアクセスできます。

（注） Cisco Prime Infrastructure マップからでも、メッシュ アクセス ポイントの [Mesh Securities] パネルにアクセスすることができます。パネルを表示するには、メッシュ アクセス ポイント ラベルの矢印部分をクリックします。

次の表では、ブリッジ、キュー、およびセキュリティの統計情報の概要とそれらの定義について説明しています。

表 *29*：ブリッジ メッシュ統計

パラメータ	説明
Role	メッシュ アクセス ポイントの役割。オプションは、メッシュ アクセス ポイント（MAP）とルート アクセス ポイント（RAP）です。
Bridge Group Name（BGN）	MAP または RAP がメンバーとなっているブリッジ グループの名前。BGN でのメンバーシップの割り当てを推奨します。割り当てられていない場合、デフォルトでは、MAP はデフォルトの BGN に割り当てられます。
Backhaul Interface	メッシュ アクセス ポイントの無線バックホール。
Routing State	親の選択の状態。表示される値は、Seek、Scan、および Maint です。Maint は、親の選択が完了すると表示されます。

パラメータ	説明
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	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	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	ネイバーのメッシュ アクセス ポイントに送信された 応答の数
Parent Changes	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	ネイバー タイムアウト回数。
Node Hops	MAP と RAP 間のホップ カウント。値のリンクをクリックすると、レポート内容の詳細やノードのホップ値が更新される頻度を設定したり、レポートをグラフィカルに表示したりできるサブパネルが表示されます。

表 *30*：キュー メッシュ統計

パラメータ	説明
Silver Queue	定義された統計期間中に Silver（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。ドロップされたパケットとキュー サイズもまとめて表示されます。
Gold Queue	定義した統計期間に gold（ビデオ）キューで待機しているパケットの平均数と最大数。ドロップされたパケットとキューサイズもまとめて表示されます。
Platinum Queue	定義した統計期間に platinum（音声）キューで待機しているパケットの平均数と最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。
Bronze Queue	定義した統計期間に bronze（バックグラウンド）キューで待機しているパケットの平均数と最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。
Management Queue	定義した統計期間に management キューで待機しているパケットの平均数と最大数。ドロップされたパケットとキュー サイズもまとめて表示されます。

表 *31*：セキュリティ メッシュ統計

パラメータ	説明
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するアソシエーション要求のエラーの合計数。
Association Request Success	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する正常なアソシエーション要求の合計数。
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するアソシエーション要求のタイムアウトの合計数。
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する認証要求のエラーの合計数。

パラメータ	説明
Authentication Request Success	選択したメッシュ アクセス ポイントとその親メッシュ ノードの間で発生する正常な認証要求の合計数。
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する認証要求のタイムアウトの合計数。
Invalid Association Request	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 ポイントから受信する無効のアソシエーション要求の合計数。この状態は、選択した子が有効なネイバーであっても、アソシエーションが許可された状態にない場合に発生することがあります。
Invalid Reassociation Request	親メッシュ アクセス ポイントが子から受信する無効の再アソシエーション要求の合計数。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。
Invalid Reauthentication Request	親メッシュ アクセス ポイントが子から受信する無効の再認証要求の合計数。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。
Packets Received	選択したメッシュアクセスポイントがセキュリティネゴシエーションの際に受信したパケットの合計数。
Packets Transmitted	選択したメッシュアクセスポイントがセキュリティネゴシエーションの際に送信したパケットの合計数。
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で発生する再アソシエーション要求のエラーの合計数。
Reassociation Request Success	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する正常な再アソシエーション要求の合計数。
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で発生する再アソシエーション要求のタイムアウトの合計数。

パラメータ	説明
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で発生する再認証要求のエラーの合計数。
Reauthentication Request Success	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正常な再認証要求の合計数。
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の合計数。
Unknown Association Requests	親メッシュ アクセス ポイントが子から受信する不明のアソシエーション要求の合計数。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。
Unknown Reassociation Request	親メッシュ アクセス ポイントが子から受信する不明の再アソシエーション要求の合計数。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。
Unknown Reauthentication Request	親メッシュ アクセス ポイント ノードがその子から受信する不明の再認証要求の合計数。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。

メッシュ ネットワーク階層の表示

メッシュ ネットワーク内のメッシュ アクセス ポイントの親子関係を、移動が容易な画面に表示できます。興味のあるメッシュ アクセス ポイントを選択するだけで [Map] ビューに表示するメッシュ アクセス ポイントのフィルタ処理をすることもできます。

選択したネットワークのメッシュ ネットワーク階層を表示するには、次の手順を実行します。

ステップ 1 [Monitor] > [Maps] を選択します。

ステップ 2 表示するマップを選択します。

ステップ 3 [Layers] 矢印をクリックして、メニューを展開します

ステップ 4 [AP Mesh Info] チェックボックスがオンになっていない場合には、オンにします。

（注） [AP Mesh Info] チェックボックスは、メッシュ アクセス ポイントがマップ上に存在する場合にのみ選択できます。メッシュ階層を表示するには、このチェックボックスをオンにする必要があります。

ステップ 5 [AP Mesh Info] 矢印をクリックして、メッシュの親子階層を表示します。

ステップ 6 メッシュ アクセス ポイントの横に表示されたプラス記号（+）をクリックして、その子を表示します。マイナス記号（-）が親メッシュ アクセス ポイントのエントリの横に表示されている場合には、すべての下位メッシュ アクセス ポイントが表示されます。

ステップ 7 各メッシュ アクセス ポイントの子の横の色付きドットの上にカーソルを移動して、これとその親間のリンクの詳細を表示します。表 32：ブリッジ リンク情報, （258 ページ） に、表示されるパラメータをまとめています。
ドットの色は、SNR 強度のクイック リファレンス ポイントを示します。

- 緑のドットは、SNR が高いことを表します（25dB 以上）。
- 黄のドットは、SNR が許容範囲内にあることを表します（20 ～ 25 dB）。
- 赤のドットは、SNR が低いことを表します（20dB 以下）。
- 黒のドットは、ルート アクセス ポイントを示します。

表 *32*：ブリッジ リンク情報

パラメータ	説明
Information fetched on	情報を集めた日時
Link SNR	リンクの Signal to Noise Ratio（SNR）
Link Type	階層化されたリンク関係
SNR Up	アップリンクの Signal to Noise Ratio（dB）
SNR Down	ダウンリンクの Signal to Noise Ratio（dB）
PER	リンクのパケット エラー率
Tx Parent Packets	親として動作する際のノードに対する TX パケット
Rx Parent Packets	親として動作する際のノードに対する RX パケット
Time of Last Hello	最後のハローの日時

メッシュ フィルタを使用したマップ画面およびメッシュ リンクの修正

メッシュ階層のページでは、ホップ値およびメッシュ リンクに表示するラベルに基づいて、マップ上に表示するメッシュ アクセス ポイントを決定するメッシュ フィルタも定義できます。

メッシュ アクセス ポイントとそのルート アクセス ポイント間のホップ カウントによって、メッシュ アクセス ポイントがフィルタ処理されます。

メッシュ フィルタリングを使用する手順は、次のとおりです。

ステップ 1 メッシュ リンクのラベルおよび色の表示を変更する手順は、次のとおりです。
[Mesh Parent-Child Hierarchical View] で、[Link Label] ドロップダウン リストからオプションを選択します。オプションは、[None]、[Link SNR]、および [Packet Error Rate] です。

[Mesh Parent-Child Hierarchical View] で、[Link Color] ドロップダウン リストからオプションを選択し、マップのメッシュ リンクの色を決定するパラメータ（[Link SNR] または [Packet Error Rate]）を定義します。

（注） リンクの色は、SNR 強度またはパケット エラー率のクイック リファレンス ポイントを示します。

表 *33*：*SNR* およびパケット エラー率のリンクの色の定義

リンクの色	リンク SNR	パケット エラー率（PER）
グリーン	SNR が 25 dB を超えている（高い値）ことを表します。	PER が 1% 以下であることを表します。
オレンジ	SNR が 20 ～ 25 dB（許容値）であることを表します。	PER が 1% より大きく 10% 未満であることを表します。
赤	SNR が 20 dB を下回っている（低い値）ことを表します。	PER が 10% より大きいことを表します。

（注） リンクのラベルおよび色の設定は、ただちにマップ上に反映されます。SNR と PER の両方の値を同時に表示することができます。

ステップ 2 メッシュ アクセス ポイントとその親との間のホップ カウントに基づいて、表示するメッシュ アクセス ポイントを変更する手順は、次のとおりです。
[Mesh Parent-Child Hierarchical View] で、[Quick Selections] ドロップダウン リストをクリックします。

適切なオプションをリストから選択します。

表 *34* : *[Quick Selections]* オプション

パラメータ	説明
Select only Root APs	マップ ビューにルート アクセス ポイントだけを表示したい場合は、この設定を選択します。
Select up to 1st hops	マップ ビューに 1 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 2nd hops	マップ ビューに 2 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 3rd hops	マップ ビューに 3 番めのホップだけを表示したい場合は、この設定を選択します。
Select up to 4th hops	マップ ビューに 4 番めのホップだけを表示したい場合は、この設定を選択します。
Select All	マップ ビューにすべてのアクセス ポイントを表示したい場合は、この設定を選択します。

[Update Map View] をクリックして画面を更新し、選択したオプションでマップ ビューを再表示します。

（注） マップ ビュー情報は Cisco Prime Infrastructure データベースから取得され、15 分おきに更新されます。

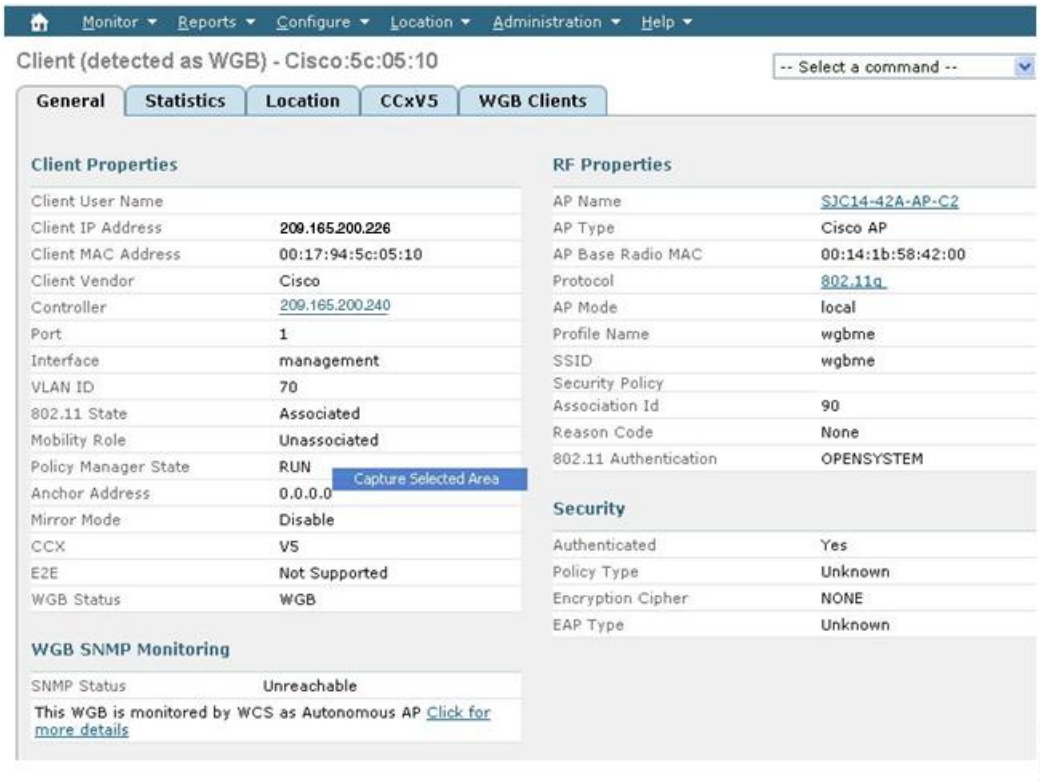
（注） メッシュ階層ビューで、メッシュ アクセス ポイントのチェックボックスをオンまたはオフにし、表示するメッシュ アクセス ポイントを変更することもできます。子アクセス ポイントを表示するには、ルート アクセス ポイントへの親アクセス ポイントを選択する必要があります。

ワークグループ ブリッジのモニタリング

ワークグループ ブリッジ（WGB）クライアントを個別にモニタできます。

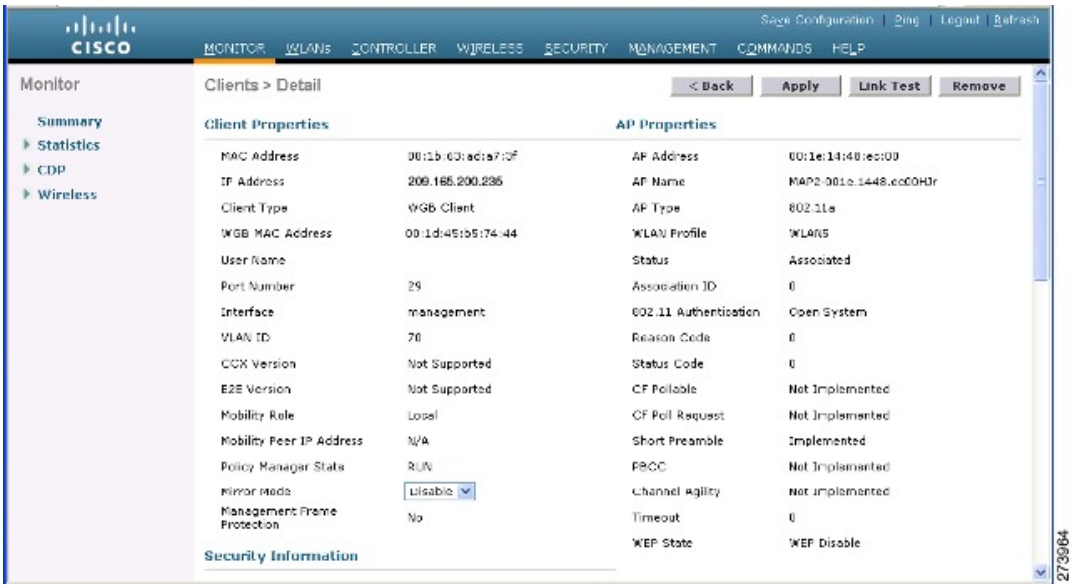
ステップ 1 Cisco Prime Infrastructure GUI で、[Monitor] > [WGBs] を選択します。

図 *74* : ***[Monitor] > [WGBs]***



ステップ 2　[WGB Clients] タブをクリックして、WGB クライアントの概要を表示します。

図 *75*：*[Monitor] > [WGBs] > [WGB Clients]* パネル



WGB 有線クライアントに対する複数の VLAN および QoS サポート

WGB は小型のスタンドアロン ユニットであり、イーサネット対応デバイス向けの無線インフラストラクチャ接続を提供します。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 は無線インターフェイスを介してルート AP に関連付けられます。これは、有線クライアントが無線ネットワークにアクセスできることを意味します。

この機能は、WGB の背後にあるスイッチに接続されている異なるデバイスで実行中のさまざまなアプリケーション用の VLAN に基づきトラフィックの分離を行います。WGB クライアントからのトラフィックは、DSCP/dot1p 値に基づきメッシュ バックホール内の正しいプライオリティ キューに送信されます。

（注）　Unified CAPWAP インフラストラクチャとの相互運用性のための WGB として使用されている Autonomous アクセス ポイントに特別な Autonomous イメージが必要です。このイメージは、次の正式な Autonomous リリースとマージされます。

WGB は、IAPP アソシエーション メッセージ内の有線クライアント VLAN 情報について WLC に通知します。WGB はパケットから 802.1Q ヘッダーを削除すると同時にパケットを WLC に送信

します。WLC は 802.1Q タグのない状態で WGB にパケットを送信し、WGB は、宛先 MAC アドレスに基づき有線スイッチに送信されるパケットに 802.1Q ヘッダーを追加します。

WLC は WGB クライアントを VLAN クライアントとして扱い、送信元 MAC アドレスに基づき正しい VLAN インターフェイスにパケットを転送します。

workgroup-bridge unified-VLAN-client コマンドを入力して、WGB で複数の VLAN サポートのために WGB Unified Client をイネーブルにする必要があります。この WGB Unified Client は、デフォルトではディセーブルです。

有線クライアントが接続されるスイッチ ポート上の VLAN に対応する WGB にサブインターフェイスを設定する必要があります。

ワークグループ ブリッジのガイドライン

WGB を設定する場合は、次のガイドラインに従います。

- WGB に設定されている各 VLAN のコントローラに動的インターフェイスを作成する必要があります。
- WGB とアクセス ポイント インフラストラクチャの無線アソシエーションには 1 つの WLAN（SSID）のみサポートされています。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。WGB は、メッシュ インフラストラクチャ内のネイティブ VLAN 内にないものはすべてドロップします。
- WLC、WGB に接続するスイッチ、および WGB の背後にあるスイッチには、同じネイティブ VLAN を設定することを推奨します。

  WGB イーサネット側のすべてのネイティブ VLAN クライアントは、WGB が関連付けられている同じ VLAN の一部です。WGB は、WGB が関連付けられている WLAN がマップされている VLAN の一部です。

  たとえば、WGB で 5 GHz 無線（dot11radio 1）がネイティブ VLAN 184 にマップされていて、WGB の背後のスイッチには VLAN 185 および 186 にのみ有線クライアントがある場合、ネイティブ VLAN が WGB 上のネイティブ VLAN（VLAN 184）と同一である必要はありません。

  しかし、VLAN 184 に有線クライアントを 1 つ追加し、WGB 内のこの VLAN クライアントがネイティブ VLAN に属している場合、スイッチに同じネイティブ VLAN を定義する必要があります。
- この機能では、WGB の背後にある VLAN クライアントのサブネット間のモビリティがサポートされていますが、WGB のすべての VLAN の動的インターフェイスをすべてのコントローラに設定する必要があるという制限があります。
- VLAN-pooling 機能との相互運用性はサポートされていません。VLAN-pooling 機能がイネーブルの場合、WGB とそのネイティブ VLAN クライアントが同じ VLAN の一部になります。
- WGB クライアントの AAA-override はサポートされていませんが、WGB の AAA-override はサポートされています。

- WGB VLAN クライアントにはレイヤ 3 マルチキャストのみサポートされており、レイヤ 2 マルチキャストはサポートされていません。
- WGB 内のクライアント数には 20 の制限があります（無線クライアントを含む）。
- WGB 有線クライアントのリンク テストはサポートされていません。
- WGB の背後にある無線および有線クライアントのローミングがサポートされています。
- WGB の背後にある有線クライアントのマルチキャストがサポートされています。
- ブロードキャストがサポートされています。
- Cisco 以外のワークグループ ブリッジは、メッシュ アクセス ポイントでサポートされます。

VLAN および QoS サポートの設定（CLI）

次の例では、VLAN 184 および 185 は、WGB の背後の有線スイッチ上にあります。WGB のネイティブ VLAN は 184 です。SSID はネイティブ VLAN 184 にマップされている自動 WGB です。無線 1（5 GHz）無線は、この SSID を使用して CAPWAP インフラストラクチャに接続するために使用されます。

```
ap#config t
ap(config)#workgroup-bridge unified-VLAN-client
ap(config)#int FastEthernet0.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#int FastEthernet0.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.185
ap(config-subif)#encapsulation dot1q 185
ap(config-subif)#bridge-group 185
ap(config-subif)#exit
ap(config)#int Dot11Radio 1.184
ap(config-subif)#encapsulation dot1q 184 native
ap(config-subif)#bridge-group 1
ap(config-subif)#exit
ap(config)#dot11 ssid auto-wgb
ap(config-ssid)#authentication open
ap(config-ssid)#infrastructure-ssid
ap(config-ssid)#VLAN 184
ap(config-ssid)#exit
ap(config)#int Dot11Radio 1
ap(config-if)#station-role workgroup-bridge
ap(config-if)#ssid auto-wgb
ap(config-if)#exit
ap(config)#bridge irb
ap(config)#hostname WGB
```

bridge irb コマンドは、他のよりハイエンドなプラットフォームからの Auto AP コードが保持されている、Integrated Routing and Bridging をイネーブルにするために使用されます。

前述の設定を機能させるには、WLC に動的インターフェイス 184 および 185 を設定する必要があります。WGB は、IAPP アソシエーション メッセージ内の有線クライアント VLAN 情報について WLC を更新します。WLC は WGB クライアントを VLAN クライアントとして扱い、送信元 MAC アドレスに基づき正しい VLAN インターフェイスにパケットを転送します。アップストリーム方向では、WGB はパケットから 802.1Q ヘッダーを削除すると同時にパケットを WLC に送信します。ダウンストリーム方向では、WLC は 802.1Q タグのない状態で WGB にパケットを送信し、WGB は、宛先 MAC アドレスに基づき 802.1Q ヘッダーを追加し、有線クライアントに接続するスイッチにパケットを転送します。

ワークグループ ブリッジの出力

次のコマンドを入力します。

```
WGB#sh bridge
Total of 300 station blocks, 292 free
Codes: P - permanent, S - self

Bridge Group 1:
```

Address	Action	Interface	Age	RX count	TX count
0023.049a.0b12	forward	Fa0.184	0	2	0
0016.c75d.b48f	forward	Fa0.184	0	21	0
0021.91f8.e9ae	forward	Fa0.184	0	110	16
0017.59ff.47c2	forward	Vi0.184	0	23	22
0021.5504.07b5	forward	Fa0.184	0	18	6
0021.1c7b.38e0	forward	ViO.184	0	6	0

Bridge Group 185:

0016.c75d.b48f	forward	Fa0.185	0	10	0
001e.5831.c74a	forward	Fa0.185	0	9	0

コントローラの WGB の詳細

コントローラに関する WGB の詳細を表示するには、次のコマンドを入力します。

(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:d2	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

WGB_1#**sh ip int brief**

Interface	IP Address	OK?	Method	Status	Protocol
BVI1	209.165.200.225	YES	DHCP	up	up
Dot11Radio0	unassigned	YES	unset	admindown	down
Dot11Radio1	unassigned	YES	TFTP	up	up
Dot11Radio1.184	unassigned	YES	other	up	up
Dot11Radio1.185	unassigned	YES	unset	up	up
FastEthernet0	unassigned	YES	other	up	up
FastEthernet0.184	unassigned	YES	unset	up	up
FastEthernet0.185	unassigned	YES	unset	up	up
Virtual-Dot11Radio0	unassigned	YES	TFTP	up	up
Virtual-Dot11Radio0.184	unassigned	YES	unset	up	up
Virtual-Dot11Radio0.185	unassigned	YES	unset	up	up

トラブルシューティングのヒント

WGB クライアントが WGB と関連付けられていない場合は、これらのヒントを参照して問題をトラブルシューティングします。

- WGB 上に設定されているネイティブ VLAN は、WGB が接続されているスイッチ上の VLAN と同じである必要があります。WGB 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。
- 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。
- Autonomous AP での show bridge コマンドの出力を確認し、その AP が正しいインターフェイスでクライアント MAC アドレスを読み取っていることを確認します。
- 特定の VLAN に対応するサブインターフェイスおよび異なるサブインターフェイスがブリッジ グループにマップされていることを確認します。
- WGB は、背後のスイッチ ポートをその MAC アドレス テーブル内のクライアントとして読み取ります。
- 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（このコマンドは、WGB と関連付けられ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関連付けることを忘れないでください）。

- WGB で 20 クライアントの制限が超えていないことを確認します。

AP の [Last Reboot Reason] の表示

Cisco Prime Infrastructure では、アクセス ポイントの詳細ページ（[Monitor] > [Access Points] > [AP Name]）の [General] パネルで最近実行されたリブートの理由を報告します。

[Last Reboot Reasons] の概要とその定義は、次のとおりです。

- none：アクセス ポイントがリブートの理由が不明であることをコントローラに報告しました
- dot11gModeChange：802.11g モードの変更が発生しました
- ipAddressSet：静的 IP アドレスの設定
- ip AddressReset：静的 IP アドレスのリセット
- rebootFromController：アクセス ポイントのリブートがコントローラから開始されました
- dhcpFallbackFail：DHCP へのフォールバックが発生しませんでした
- discoveryFail：検出が送信されませんでした
- noJoinResponse：接続応答が受信されませんでした
- denyJoin：コントローラでの接続の試みが拒否されました
- noConfigResponse：設定応答が受信されませんでした
- configController：設定済みまたはマスタ コントローラが検出されました
- imageUpgrade Success：イメージのアップグレードが成功しました
- imageOpcodeInvalid：無効なイメージ データのオペレーション コード
- imageCheckSumInvalid：無効なイメージの MD5 チェックサム
- imageDataTimeout：イメージ データのメッセージがタイムアウトしました
- configFileInvalid：無効な設定ファイル
- imageDownloadError：イメージのダウンロード中のプロセス エラー
- rebootFromConsole：リブート コマンドが AP コンソールから開始されました
- rapOverAir：ルート アクセス ポイント（RAP）が無線接続されました
- brownout：電源障害が原因でリブートが開始されました
- powerLow：低電力が原因でリブートが開始されました
- crash：ソフトウェア障害が原因でクラッシュが発生しました
- powerHigh：出力スパイクが原因でリブートが開始されました
- powerLoss：電力損失が原因でリブートが開始されました

- powerCharge：電源の変更が原因でリブートが開始されました
- componentFailure：コンポーネントの障害が原因でリブートが開始されました
- watchdog：ウォッチドッグ タイマーが原因でリブートが開始されました

索 引

ゆ

ろ

わ