



Cisco ワイヤレス メッシュ アクセス ポイントの設計および導入ガイド リリース 8.1 および 8.2

初版：2015 年 06 月 12 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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧については、<http://www.cisco.com/go/trademarks> をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2015 Cisco Systems, Inc. All rights reserved.



目次

はじめに xi

対象読者 xii

マニュアルの構成 xii

表記法 xii

関連資料 xv

マニュアルの入手方法およびテクニカル サポート xv

メッシュ ネットワーク コンポーネント 1

メッシュ アクセス ポイント 2

5500 シリーズ コントローラでのメッシュ アクセス ポイントのライセンス 2

アクセス ポイントのロール 2

ネットワークアクセス 3

ネットワークのセグメント化 4

Cisco 屋内メッシュ アクセス ポイント 4

Cisco 屋外メッシュ アクセス ポイント 5

Cisco Aironet 1570 シリーズ アクセス ポイント 7

Cisco Aironet 1530 シリーズ アクセス ポイント 9

Cisco Aironet 1552 メッシュ アクセス ポイント 11

イーサネット ポート 16

複数の電源オプション 17

バッテリー バックアップ モジュール (任意) 18

1550 のリセット ボタン 19

1550 アクセス ポイントのリセット 21

1550 LED ステータスのモニタリング 21

周波数帯域 24

動的周波数選択 (DFS) 25

アンテナ 26

1552 のアンテナ構成	28
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)	31
最大比合成	31
Cisco 1500 危険場所認証	34
Cisco ワイヤレス LAN コントローラ	36
Cisco Prime Infrastructure	36
アーキテクチャ	37
Control and Provisioning of Wireless Access Points	37
メッシュ ネットワークの CAPWAP ディスカバリ	37
ダイナミック MTU 検出	38
XML 設定ファイル	38
Adaptive Wireless Path Protocol	39
トラフィック フロー	40
メッシュ ネイバー、親、および子	41
最適な親を選択するための基準	42
容易度の計算	43
親の決定	43
SNR スムージング	43
ループの防止	44
メッシュ導入モード	45
ワイヤレス メッシュ ネットワーク	45
無線バックホール	46
ユニバーサル アクセス	46
ポイントツーマルチポイント無線ブリッジング	46
ポイントツーポイント無線ブリッジング	47
メッシュ レンジの設定 (CLI)	48
デザインの考慮事項	51
無線メッシュの制約	51
ワイヤレス バックホール データ レート	51
ClientLink テクノロジー	55
ClientLink の設定 (CLI)	57
ClientLink に関連するコマンド	59
コントローラの計画	59

サイトの準備と計画	61
サイトの調査	61
調査前チェックリスト	61
屋外サイトの調査	62
ライン オブ サイトの判別	63
天候	63
フレネルゾーン	63
ワイヤレス メッシュ 配置のフレネルゾーン サイズ	65
隠しノードの干渉	65
優先される親の選択	66
優先親の選択基準	66
優先される親の設定	67
関連コマンド	68
共同チャネルの干渉	69
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	69
セルの計画と距離	70
Cisco 範囲カルキュレータの前提条件	82
メッシュ アクセス ポイントのコロケーション	85
屋内メッシュ ネットワークの特殊な考慮事項	85
ワイヤレス伝搬の特性	88
CleanAir	88
CleanAir AP 動作モード	89
Pseudo MAC (PMAC) とマージ	89
Event Driven Radio Resource Management と Persistence Device Avoidance	91
CleanAir アクセス ポイント配置の推奨事項	92
CleanAir Advisor	93
CleanAir のイネーブル化	93
ライセンス	93
ワイヤレス メッシュ モビリティ グループ	94
複数のコントローラ	94
メッシュ アベイラビリティの増加	95
複数の RAP	96
屋内メッシュと屋外メッシュの相互運用性	97

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	99
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	100
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	101
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)	102
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)	103
メッシュ アクセス ポイントのロール定義	103
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	104
AP ロールの設定 (GUI)	105
AP ロールの設定 (CLI)	105
DHCP 43 および DHCP 60 を使用した複数のコントローラの設定	106
バックアップ コントローラ	107
バックアップ コントローラの設定 (GUI)	109
バックアップ コントローラの設定 (CLI)	110
RADIUS サーバを使用した外部認証および認可の設定	113
RADIUS サーバの設定	114
メッシュ アクセス ポイントの外部認証の有効化 (GUI)	115
RADIUS サーバへのユーザ名の追加	115
メッシュ アクセス ポイントの外部認証の有効化 (CLI)	116
セキュリティ統計情報の表示 (CLI)	117
リリース 8.2 でプロビジョニングするメッシュ PSK キー	117
サポートされるワイヤレス メッシュのコンポーネント	118
機能の設定手順	118
メッシュ PSK GUI の設定	118
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	125
PSK 事前プロビジョニング用の CLI コマンド	125
グローバル メッシュ パラメータの設定	125
グローバル メッシュ パラメータの設定 (GUI)	126
グローバル メッシュ パラメータの設定 (CLI)	130
グローバル メッシュ パラメータ設定の表示 (CLI)	131

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	132
バックホール クライアント アクセス	137
バックホール クライアント アクセスの設定 (GUI)	138
バックホール クライアント アクセスの設定 (CLI)	139
ローカル メッシュ パラメータの設定	139
ワイヤレス バックホール データ レートの設定	139
イーサネットブリッジングの設定	143
イーサネットブリッジングの有効化 (GUI)	145
ネイティブ VLAN の設定 (GUI)	146
ネイティブ VLAN の設定 (CLI)	146
ブリッジグループ名の設定	147
ブリッジグループ名の設定 (CLI)	147
ブリッジグループ名の確認 (GUI)	148
Cisco 3200 との相互運用性	148
電力およびチャネルの設定	149
電力およびチャネルの設定 (GUI)	149
アンテナ ゲインの設定	150
アンテナ ゲインの設定 (GUI)	150
アンテナ ゲインの設定 (CLI)	151
動的チャネル割り当ての設定	151
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	154
拡張機能の設定	154
イーサネット VLAN タギングの設定	155
イーサネット ポートに関する注意	156
VLAN 登録	158
イーサネット VLAN タギングのガイドライン	158
イーサネット VLAN タギングの有効化 (GUI)	160
イーサネット VLAN タギングの設定 (CLI)	161
イーサネット VLAN タギング設定詳細の表示 (CLI)	161
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	162
ワークグループブリッジの設定	163
設定のガイドライン	167

設定例	169
WGB アソシエーションの確認	170
リンク テストの結果	172
WGB 有線/ワイヤレス クライアント	173
クライアント ローミング	174
WGB ローミングのガイドライン	175
設定例	176
トラブルシューティングのヒント	176
屋内メッシュ ネットワークの音声パラメータの設定	177
コール アドミッション制御	177
QoS および DiffServ コード ポイントのマーキング	177
メッシュ ネットワークでの音声使用のガイドライン	184
メッシュ ネットワークでの音声コールのサポート	185
ビデオのメッシュ マルチキャストの抑制の有効化	186
メッシュ ネットワークの音声詳細の表示 (CLI)	188
メッシュ ネットワークでのマルチキャストの有効化 (CLI)	191
IGMP スヌーピング	191
メッシュ AP のローカルで有効な証明書	192
設定のガイドライン	193
メッシュ AP の LSC と通常の AP の LSC の違い	193
LSC AP での証明書検証プロセス	194
LSC 機能の証明書の取得	194
ローカルで有効な証明書 (CLI) の設定	196
LSC 関連のコマンド	198
コントローラ GUI セキュリティ設定	200
展開ガイドライン	200
ネットワークの状態の確認	203
Show Mesh コマンド	203
一般的なメッシュ ネットワークの詳細の表示	203
メッシュ アクセス ポイントの詳細の表示	205
グローバル メッシュ パラメータ設定の表示	206
ブリッジ グループ設定の表示	207

VLAN タギング設定の表示	207
DFS の詳細の表示	207
セキュリティ設定と統計情報の表示	208
GPS ステータスの表示	208
メッシュ アクセス ポイントのメッシュ統計情報の表示	209
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)	209
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)	213
メッシュ アクセス ポイントのネイバー統計情報の表示	215
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)	215
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)	215
トラブルシューティング	217
インストールと接続	217
debug コマンド	218
リモート デバッグ コマンド	219
AP コンソール アクセス	219
AP からのケーブル モデムのシリアル ポート アクセス	220
設定	220
メッシュ アクセス ポイント CLI コマンド	223
メッシュ アクセス ポイント デバッグ コマンド	225
メッシュ アクセス ポイントのロール定義	225
バックホール アルゴリズム	225
パッシブ ビーコン (ストランディング防止)	226
動的周波数選択 (DFS)	228
RAP の DFS	229
MAP の DFS	230
DFS 環境での準備	231
DFS のモニタ	232
周波数プランニング	233
適切な信号対雑音比	233
アクセス ポイントの配置	234
パケット エラー率のチェック	234
ブリッジ グループ名の誤った設定	234

メッシュ アクセス ポイントの IP アドレスの誤った設定	236
DHCP の誤った設定	236
ノード除外アルゴリズムについて	237
スループット分析	239
Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理	241
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	242
キャンパス マップの追加	242
屋外領域の追加	243
キャンパス マップへのビルディングの追加	244
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	245
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	246
Cisco Prime Infrastructure からの Google Earth の起動	246
Google Earth マップの表示	247
Cisco Prime Infrastructure への屋内メッシュ アクセス ポイントの追加	250
Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理	251
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	252
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	252
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	253
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	255
メッシュ アクセス ポイントの状態のモニタリング	255
メッシュ アクセス ポイントのメッシュ統計情報の表示	258
メッシュ ネットワーク階層の表示	263
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	265
ワークグループブリッジのモニタリング	267
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	268
ワークグループブリッジのガイドライン	269
VLAN および QoS サポートの設定 (CLI)	270
ワークグループブリッジの出力	271
コントローラの WGB の詳細	272
トラブルシューティングのヒント	273
AP の [Last Reboot Reason] の表示	274



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 1040、1130、1140、1240、1250、1260、2600、3500e、3500i、3600e、3600i、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 1550 (1552) シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1040、1140、1260、2600、3500e、3500i、3600e、3600i、シリーズの屋内メッシュ アクセス ポイント
- シスコ 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。

- [対象読者, xii ページ](#)
- [マニュアルの構成, xii ページ](#)
- [表記法, xii ページ](#)
- [関連資料, xv 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](#), xv 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 , (1 ページ)	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 , (45 ページ)	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 , (51 ページ)	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。
サイトの準備と計画 , (61 ページ)	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 , (99 ページ)	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 , (203 ページ)	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 , (217 ページ)	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 , (241 ページ)	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 「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。（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 lichamelijke letsels 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].)
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. 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").

警告タイトル	説明
¡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 Wireless LAN Controller Configuration Guide*』
- 『*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。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*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 15X0 シリーズ メッシュ 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, 2 ページ](#)
- [Cisco ワイヤレス LAN コントローラ, 36 ページ](#)
- [Cisco Prime Infrastructure, 36 ページ](#)
- [アーキテクチャ, 37 ページ](#)

メッシュ アクセス ポイント

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

Cisco 5500 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 (LIC-CT5508-X) 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 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、5 GHz 周波数のメッシュ バックホールの CleanAir をサポートし、干渉デバイス レポート (IDR) と電波品質の指標 (AQI) レポートのみを作成します。

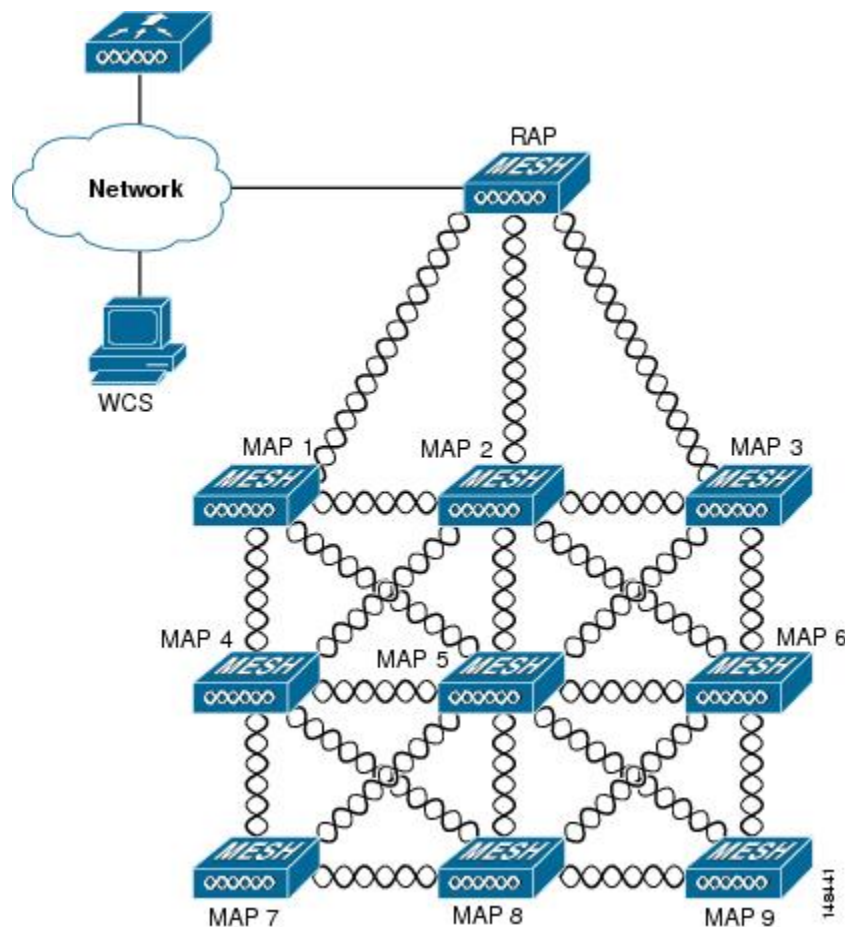


(注)

RAP または MAP はブリッジプロトコルデータ ユニット (BPDU) 自体を生成しません。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せん。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

屋内メッシュは次のアクセス ポイントから入手できます。

- 802.11n
 - 1040
 - 1140
 - 1260
- 802.11n+CleanAir
 - 1600
 - 2600
 - 3500e
 - 3500i
 - 3600
- 802.11ac+CleanAir



(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。バックホールは、5 GHz 無線でのみサ

ポートされます。ユニバーサルバックホールアクセスが有効な場合、5 GHz 無線はローカル（クライアント）アクセスとバックホールに使用できます。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の量が大きく、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。

- クライアントアクセスに使用される 2.4 GHz の無線
- ユニバーサルバックホールアクセスが有効になっている場合、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 11n 屋外メッシュアクセスポイント、およびが含まれます。

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 protocols 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。

AP1500 には、ケーブルありとケーブルなしの2つの異なる構成があります。

- ケーブル構成は、ケーブルより線に取り付け可能であり、Power-Over-Cable (POC) をサポートします。
- ケーブルなし構成は、複数のアンテナをサポートします。この構成は、柱や建物壁面に取り付け可能で、電源関連のオプションをいくつか用意しています。

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。

AP1500 は、危険な場所用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。

次のモードでは、メッシュ アクセス ポイントは非メッシュ 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ン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ンネルをモニタ中にも処理が可能です。この間に、AP は 50 ミリ秒周期で各チャンネルをリッスンし、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、チャンネル上の 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 モードでクライアント 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。
- 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ンネルをスキャンし、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 はチャン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。MAP に有線バックホールがある場合、AP モードを変更する前に、RAP に AP ロールを変更する必要があります。

Cisco Aironet 1570 シリーズ アクセス ポイント

Cisco Aironet 1570 シリーズは、Wi-Fi カバレッジを屋外に拡張しようと考えている企業およびキャリア クラスの両方のネットワーク オペレータに最適な屋外アクセス ポイントです。これは、パフォーマンスが業界最高レベルのパフォーマンスを誇るアクセス ポイントであり、データ接続速度が最大 1.3 Gbps の最新の Wi-Fi 規格である 802.11ac に対応しています。この産業クラスのアクセス ポイントは、4x4 Multiple Input Multiple Output (MIMO) のスマートアンテナテクノロジーと3空間ストリームをサポートしており、最適なパフォーマンスを実現します。Aironet 1570 により、より広い地域にカバレッジを拡張し、高いスループットを提供します。このアクセス ポイントは、近くにいる多数のユーザが RF 干渉を生成する場合のように、管理が不可欠な高密度な環境にも適しています。1572 の特徴は次のとおりです。

- 最先端のキャリアグレード屋外用 Wi-Fi AP
- 2.4 GHz と 5 GHz のデュアルバンド、内蔵 5 GHz 無線での 802.11ac Wave 1 サポート
- 法律で規定された最大放射 RF 電力
- High Density Experience (HDX)
 - Cisco CleanAir 2.0 テクノロジーは、自動設定用の統合スペクトラムインテリジェンスと 80 MHz チャネルでの自動復旧ネットワークを提供します。
 - ClientLink 3.0 は、従来の 802.11ac と 802.11n のデータ レートの信頼性を向上させ、カバレッジを拡大します。
 - クライアントが最適なアクセス ポイントに接続できるようにするための最適化ローミング。
 - 無線パフォーマンスを最大化するための Cisco ASIC 設計を使用したターボ パフォーマンス。
- 4 x 4:3 Multiple-Input Multiple-Output (MIMO) テクノロジーによる 802.11ac の範囲とパフォーマンスの向上
- 1.3 Gbps (5 GHz) 802.11ac データ レート
- シスコ フレキシブル アンテナ ポート テクノロジー
- DOCSIS 3.0/EuroDOCSIS/JapanDOCSIS 3.0、24 x 8 光ファイバ/同軸ハイブリッド (HFC) ケーブル モデム オプション
- 4 つのアンテナ MIMO と 3 つの空間ストリームによる無線感度と範囲パフォーマンスの向上

- 複数のアップリンク オプション (ギガビット イーサネット 10/100/1000 BaseT、ファイバ SFP、ケーブル モデム)
- 電源 : AC、DC、ケーブル、UPOE、PoE-Out (802.3at)
- 4G LTE 共存
- NEMA タイプ 4X 認定カバー
- モジュール オプション : 投資保護と将来保証
- 目立たないプロファイル デザイン
- 統合または自律運用

AP1572IC

AP1572IC には次のような機能があります。

- 2つの無線 (2.4 GHz と 5 GHz)
 - 2 GHz : 4x4:3
 - 5 GHz : 4x4:3
- 電源オプション :
 - 40 ~ 90 VAC、50 ~ 60 Hz、準方形波、パワー オーバー ケーブル
 - 10 ~ 16 VDC
- コンソール ポート
- LTE および WiMAX 信号除去 (2.1/2.3 GHz : 30 dB、2.5 GHz : 35 dB)
- DOCSIS および EuroDOCSIS 3.0 24x8
- GPS オプション

AP1572EC

AP1572EC には次のような機能があります。

- 2つの無線 (2.4 GHz と 5 GHz)
 - 2 GHz : 4x4:3
 - 5 GHz : 4x4:3
- 電源オプション :
 - 40 ~ 90 VAC、50 ~ 60Hz、準方形波、パワー オーバー ケーブル
 - 10 ~ 16 VDC
 - 802.3at PoE-Out 対応

- コンソール ポート
- LTE および WiMAX 信号除去 (2.1/2.3 GHz : 30 dB、2.5 GHz : 35 dB)
- GPS オプション

AP1572EAC

AP1572EAC には次のような機能があります。

- 2つの無線 (2.4 GHz および 5 GHz)
 - 2 GHz : 4x4:3
 - 5 GHz : 4x4:3
- 電源オプション :
 - 100 ~ 277 VAC、50 ~ 60Hz
 - 10 ~ 16 VDC
 - UPoE
 - AIR-PWRINJ1550-2 付きの PoE
 - AC/DC 電源から電力が供給される場合の 802.3at PoE-Out 対応
- コンソール ポート
- LTE および WiMAX 信号除去 (2.1/2.3 GHz : 30 dB、2.5 GHz : 35 dB)
- GPS オプション



(注) 詳細については、『[1572 Deployment Guide](#)』を参照してください。

Cisco Aironet 1530 シリーズ アクセス ポイント

Cisco Aironet 1530 シリーズ アクセス ポイントは、さまざまなアプリケーションをサポートするように設計されています。洗練されたプロファイルで、アクセス ポイントは、カバレッジが必要で特定の配置の要件を引き続き満たす場所に展開されます。

主な特徴は次のとおりです。

- ウルトラ ロープロファイル、屋外 AP
- 802.11n デュアルバンド (2.4 GHz および 5 GHz)
- モデル : 内部 (1532I) または外部 (1532E) アンテナ。
 - フレキシブル アンテナ ポート : シングル バンドまたはデュアルバンド アンテナの SW 設定ポート

- 統合または自律モード：新しいブート ロジックが、同じ HW PID からの AP の統合ブートまたは自律ブートを可能にします
- 2.4 GHz または 5 GHz のブリッジング：ポイントツーポイントまたはポイントツーマルチポイントのトポロジ
- デイジーチェーン：シリアル バックホールまたは拡張ユニバーサル アクセス

詳細情報などのサポート ドキュメントについては、http://www.cisco.com/en/US/products/ps12831/tsd_products_support_series_home.html を参照してください。

AP1532I

AP1532I には次のような機能があります。

- 2 つの無線 (2.4 GHz および 5 GHz)
 - 2 GHz : 3x3:3
 - 5 GHz : 2x3:2
- UPoE および DC 電源 (48 V)
- コンソール ポート
- 重量 : 2.3 kg (5.07 ポンド)
- LTE および WiMAX 信号除去 (2.1/2.3 GHz : 30 dB、2.5 GHz : 35 dB)
- 23 x 17 x 10 cm (9 x 7 x 4 インチ) (3.0 リットル以下に相当)

AP1532E

AP1532E には次のような機能があります。

- 2 つの無線 (2.4 GHz および 5 GHz)
 - 2 GHz : 2x2:2
 - 5 GHz : 2x2:2
- PoE+ (802.3at) および DC 電源 (48 V)
- コンソール ポート
- 重量 : 2.5 kg (5.5 ポンド)
- LTE および WiMAX 信号除去 (2.1/2.3 GHz : 30 dB、2.5 GHz : 35 dB)
- 自律ブリッジング機能 (1310 および 1410 の製品ラインの後継)
- 26 x 17 x 10 cm (10 x 7 x 4 インチ) (3.0 リットルに相当)



(注) 詳細については、『[1532 Deployment Guide](#)』を参照してください。

Cisco Aironet 1552 メッシュ アクセス ポイント

Cisco Aironet 1550 シリーズの屋外メッシュ アクセス ポイントは、メッシュ ネットワークで使用
する目的で設計されたモジュール方式の無線屋外 802.11n アクセス ポイントです。このアクセス
ポイントは、ポイントツーマルチポイント メッシュの無線接続およびワイヤレス クライアント
アクセスを同時にサポートします。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 ポイントのリレー 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。これにより、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。

1550 シリーズのアクセス ポイントは、802.11n テクノロジーと統合無線および内部/外部アンテナ
を利用しています。1552 屋外プラットフォームは、Multiple Input Multiple Output (MIMO) WLAN
無線で構成されます。2x3 MIMO と 2 つの空間ストリーム、ビーム形成を採用し、統合スペクト
ルインテリジェンス (CleanAir) を備えています。

CleanAir は、無線周波数 (RF) 干渉を検出、位置を特定、分類、緩和すると同時に 11n のフル
データ レートを提供して、最適なクライアントエクスペリエンスを実現します。屋外 11n プラッ
トフォームの CleanAir テクノロジーは、2.4 GHz 無線の Wi-Fi および非 Wi-Fi 干渉を緩和します。

1550 シリーズのアクセス ポイントには、2.4 GHz および 5 GHz MIMO 無線の 2 つの無線がありま
す。2.4 GHz 無線は主にローカル アクセスに使用し、5 GHz 無線はローカル アクセスおよびメッ
シュ モードでのワイヤレス バックホールの両方に使用します。



(注) wIPS サブモードは、Cisco 1532、1552、および 1572 シリーズのメッシュ アクセス ポイントで
はサポートされません。



(注) 2.4 GHz 無線は 1552 AP のバックホールには使用できません。

2 GHz b/g/n 無線には次の特長があります。

- 2.4 GHz ISM 帯域で稼働します。
- 米国ではチャンネル 1 ~ 11、欧州では 1 ~ 13、日本では 1 ~ 13 をサポートします。
- 802.11b/g/n 動作用に 2 つのトランスミッタがあります。
- 5 つの電力レベルで出力電力を設定できます。
- 無線には、最大比合成 (MRC) を可能にするレシーバが 3 つあります。

5 GHz a/n 無線には次の特長があります。

- UNII-2 帯域 (5.25 ~ 5.35 GHz) 、 UNII-2 拡張/ETSI 帯域 (5.47 ~ 5.725 GHz) 、 および高い方の ISM 帯域 (5.725 ~ 5.850 GHz) で動作します。
- 802.11a 動作用に 2 つのトランスミッタがあります。
- 規制ドメインに応じて電力設定を変更できます。3 dB の手順では、出力電力を 5 つの電力レベルで設定できます。
- 無線には、最大比合成 (MRC) を可能にするレシーバが 3 つあります。

1550 シリーズのアクセス ポイントには次の特長があります。

- レガシー クライアントと相互運用性があり、バックホールのパフォーマンスを向上させます。
- AP がローカル モードで設定されている場合は、マルチキャスト VideoStream がサポートされます。
- ホットスポット 2.0 は AP がローカルおよび FlexConnect またはメッシュ モードで設定される時にサポートされます。
- AP1552 は、高品質な VoWLAN コールに対応可能な QoS です。
- 接続されたクライアントに 2.4 GHz から 5 GHz へ移動するように通知する帯域選択がサポートされています。
- AP1552 では、DTLS のサポートにより、ブリッジ モードを除くすべてのサポート対象 AP モードのデータを暗号化できます。
- 5 GHz の無線上で CleanAir を有効にするには、コントローラの GUI で [Wireless] > [Radios] > [802.11a] > [Configure] と選択します。
- AP1552 がブリッジ モードの場合、CleanAir Advisor が動作可能になります。CleanAir Advisor は CleanAir レポートを生成し、干渉を識別します。イベント駆動型 RRM は無効です。したがって、無線は送信電力の電力レベルまたはチャンネルを変更しません。

モデルは、外部アンテナを使用するモデルとアンテナが内蔵されたモデルに大別できます。1552C モデルは、統合型 DOCSIS/EuroDOCSIS 3.0 ケーブル モデムで構成されます。DOCSIS 3.0 ケーブル モデムは、8 DS および 4 US (8x4) 、 304x108 Mbps を提供します。EuroDOCSIS 3.0 ケーブル モデムは 4 US および 4 DS (4x4) 、 152x108 Mbps を提供します。DOCSIS 2.0 ケーブル モデムは最大 40 Mbps のスループットのみを提供できましたが、DOCSIS 3.0 ケーブル モデムは 290 Mbps の DS スループットおよび 100 Mbps の US スループットを提供できます。

1552 アクセス ポイントには次のモデルがあります。

- [1552E](#), (13 ページ)
- [1552C](#), (14 ページ)
- [1552I](#), (14 ページ)
- [1552H](#), (15 ページ)

- 1552CU, (15 ページ)
- 1552EU, (16 ページ)

Cisco 1550 シリーズ アクセス ポイントの詳細については、<http://www.cisco.com/en/US/products/ps11451/index.html> を参照してください。

1552E

Cisco Aironet 1552E 屋外アクセス ポイントは、標準モデルのデュアル無線システムで、IEEE 802.11a/n (5 GHz) および 802.11b/g/n (2.4 GHz) 標準に準拠したデュアルバンド無線を備えています。1552E には、デュアルバンドアンテナ用の外部アンテナ接続が 3 つあります。イーサネットおよびファイバ Small Form Factor Pluggable (SFP) バックホール オプションおよびバッテリー バックアップ オプションがあります。このモデルには、PoE 出力ポートもあり、ビデオ監視カメラに電力を供給できます。柔軟性の高いモデルである Cisco Aironet 1552E は、自治体やキャンパス展開、ビデオ監視、採掘現場、データ オフロード用に十分な機能を備えています。

1552E モデルには次の特長があります。

- 重量 17.3 ポンド (7.9 kg)、外部アンテナを除く
- 2 つの無線 (2.4 GHz および 5 GHz)
- 3 つの外部デュアルバンド全方向性アンテナ (2.4 GHz で 4 dBi、5 GHz で 7 dBi)
- 垂直ビーム幅 : 2.4 GHz で 29°、5 GHz で 15°
- 位置合わせされたコンソール ポート
- 高い Equivalent Isotropically Radiated Power (EIRP)
- イーサネットおよびファイバによる複数のアップリンク
- オプションの Small Form Factor Pluggable (SFP) ファイバ モジュール (AP と一緒に発注可能)。AP は、SFP ファイバまたは銅線モジュールを使用できます。
- IP デバイス (ビデオ カメラなど) に接続するための 802.3af 準拠の PoE 出力オプション
- AC 電源 (100 ~ 480 VAC)
- パワー インジェクタを使用した PoE 入力
- バッテリー バックアップ オプション (6 AH)



(注) 1552E モデルにはケーブル モデムはありません。1552E バッテリーは 1552H に使用できません。

- AP1552E は、アドオンとして Ethernet Passive Optical Network (EPON) SFP と一緒に発注することができます。EPON SFP はギガビットのデータ レートを提供します。



(注) EPON SFP 機能を別に購入してインストールする必要があります。

1552C

サービスプロバイダーがすでにブロードバンドケーブルネットワークを構築している場合は、Cisco Aironet 1552C アクセスポイントを導入すると、内蔵ケーブルモデムインターフェイスに接続することで、シスコの次世代屋外ワイヤレスメッシュによってネットワーク接続をシームレスに拡張できます。Cisco Aironet 1552C 屋外メッシュアクセスポイントは、電源およびバックホール用の DOCSIS 3.0/EuroDOCSIS 3.0 (8x4 HFC) ケーブルモデムを装備したデュアル無線システムです。IEEE 802.11a/n (5 GHz) および 802.11b/g/n (2.4 GHz) 標準に準拠したデュアルバンド無線を備えています。1552C は、3 素子、デュアルバンドアンテナを内蔵しており、サービスプロバイダーの高さ制限である 30 cm 以内に容易に収まります。このモデルは、3G データオフロードおよびパブリック Wi-Fi に最適です。

1552C モデルには次の特長があります。

- 軽量 (14 ポンド (6.4 kg))、ロープロファイルの AP
- 2 つの無線 (2.4 GHz および 5 GHz)
- DOCSIS/EuroDOCSIS 3.0 ケーブル モデム
- 位置合わせされたコンソール ポート
- ケーブル モデムのバックホールをサポート
- 3 素子アレイ アンテナを内蔵 (2.4 GHz で 2 dBi、5 GHz で 4 dBi)
- 入力モジュール、Power-over-Cable 電源 (40 ~ 90 VAC)
- 便利な穴が 2 つある型押しカバー。この穴は、スティング コネクタ (RF/電源入力) 用ロックナットを締め、ヒューズパッドを調整して信号を減衰させるのに使用



(注) 1552C モデルには、バッテリー バックアップ、ファイバ SFP サポート、PoE 出力、パワーインジェクタまたはイーサネットポートを使用した PoE 入力、AC 電源オプションはありません。

1552I

Cisco Aironet 1552I 屋外アクセスポイントは、ロープロファイルの軽量モデルです。小型でスッキリした外観は周辺環境に溶け込みます。また、小容量電源によりエネルギー効率に優れています。1552I には PoE 出力やファイバ SFP ポートはありません。

1552I モデルには次の特長があります。

- 軽量 (14 ポンド (6.4 kg))、ロープロファイルバージョン
- 2 つの無線 (2.4 GHz および 5 GHz)

- 位置合わせされたコンソール ポート
- AC 電源 (100 ~ 277 VAC)
- 穴のない型押しカバー
- 街路灯の TAP をサポート



(注) 1552I モデルには、バッテリー バックアップ、ファイバ SFP サポート、ケーブル モデム、PoE 出力はありません。

1552H

このアクセス ポイントは、石油やガスの精製所、化学プラント、採掘現場、製造工場などの危険な環境向けに設計されています。Cisco Aironet 1552H 屋外アクセス ポイントは、Class 1、Div 2/Zone 2 危険な場所向けの認定を受けています。機能は 1552E モデルと同様ですが、バッテリー バックアップはありません。

1552H モデルには次の特長があります。

- 重量 14 ポンド (6.4 kg)
- 2 つの無線 (2.4 GHz および 5 GHz)
- 危険な場所 (Haz Loc) 向けバージョン
- パワー インジェクタを使用した Power-over-Ethernet (PoE) 入力
- 位置合わせされたコンソール ポート
- デュアルバンド外部全方向性アンテナ 3 本
- 端子ブロック付き AC 入力モジュール
- AC 電源 (100 ~ 240 VAC、ATEX 認証要件に準拠)
- ファイバ SFP バックホール オプション
- IP デバイス (ビデオ カメラなど) に接続するための 802.3af 準拠の PoE 出力オプション
- バッテリー バックアップ オプション (危険な場所向け特殊バッテリー)

Cisco Aironet 1552 メッシュ アクセス ポイントのハードウェアおよび設置手順の詳細については、を参照してください。 http://www.cisco.com/en/US/products/ps11451/prod_installation_guides_list.html

1552CU

1552CU モデルには次の特長があります。

- 2 つの無線 (2.4 GHz および 5 GHz)
- 位置合わせされたコンソール ポート
- AC 電源 (40 ~ 90 VAC)

- 穴のない型押しカバー
- 外部高ゲインアンテナ (2.4 GHz で 13 dBi、5 GHz で 14 dBi)
- ケーブル モデム

1552EU

1552EU モデルには次の特長があります。

- 2つの無線 (2.4 GHz および 5 GHz)
- 位置合わせされたコンソール ポート
- AC 電源 (90 ~ 480 VAC)
- PoE 802.3af
- 外部高ゲインアンテナ (2.4 GHz で 13 dBi、5 GHz で 14 dBi)
- バッテリー
- AP1552EU は、アドオンとして Ethernet Passive Optical Network (EPON) SFP と一緒に発注することができます。EPON SFP はギガビットのデータ レートを提供します。



(注) EPON SFP 機能を別に購入してインストールする必要があります。

イーサネット ポート

AP1500 は 4 つのギガビット イーサネット インターフェイスをサポートします。

- ポート 0 (g0) : Power over Ethernet (PoE) 入力ポート PoE (入力)
- ポート 1 (g1) : PoE 出力ポート PoE (出力)
- ポート 2 (g2) : ケーブル接続
- ポート 3 (g3) : ファイバ接続

コントローラ CLI と Cisco Prime Infrastructure では、これら 4 つのインターフェイスのステータスを照会できます。

コントローラ CLI では、**show mesh env summary** コマンドを使用してポートのステータスを表示します。

- 4 つのポートの Up または Down (Dn) のステータスは、次の形式で報告されます。
 - port0(PoE-in):port1(PoE-out):port2(cable):port3(fiber)
- たとえば、次の表示の *rap1522.a380* では、ポートステータスが UpDnDnDn になっています。これは次を意味します。

- ポート 0 の PoE 入力 (g0) は Up、ポート 1 の PoE 出力 (g1) は Down (Dn)、ケーブル ポート 2 (g2) は Down (Dn)、ファイバ ポート 3 (g3) は Down (Dn)。

```
(controller)> show mesh env summary
AP Name      Temperature (C/F)  Heater  Ethernet  Battery
-----
rap1242.c9ef  N/A                N/A     UP         N/A
rap1522.a380  29/84              OFF     UpDnDnDn  N/A
rap1522.4da8  31/87              OFF     UpDnDnDn  N/A
```

複数の電源オプション

1550 シリーズ用

次の電源オプションがあります。

- Power-over-Ethernet (PoE) 入力
 - パワー インジェクタを使用した 56 VDC (1552E、1552H)
 - PoE 入力は 802.3af ではなく、PoE 802.3af 対応イーサネット スイッチでは動作しません
- AC 電源
 - 100 ~ 480 VAC (47 ~ 63 Hz) : AC または街路灯電源の接続 (1552E)
 - 100 ~ 240 VAC : AC または街路灯電源の接続 (1552H)
- 外部電源
 - 12 VDC : DC 電源ケーブルの接続 (全モデル)
- 内部バッテリー バックアップ (1552E、1552H)
- Power-over-Cable (PoC)
 - 40 ~ 90 VAC : ケーブル PoC の接続 (1552C)
- ビデオカメラなどの IP デバイスに接続するための 802.3af 準拠の PoE 出力 (1552E、1552H)
 - パワーインジェクタ (PoE-In) を電源として使用する場合は、(PoE 出力) は使用できません
- ビデオカメラなどの IP デバイスに接続するための 802.3af 準拠の PoE 出力 (1552E、1552H)

このポートは Auto-MDIX も実行します。これにより、クロス ケーブルまたはストレート ケーブルを接続できます。

1550 シリーズ アクセス ポイントは複数の電源に接続できます。アクセス ポイントは、使用可能な電源を検出し、次のデフォルトプライオリティを使用して優先電源に切り替えます。

- AC 電力または PoC 電力

- 外部 12 VDC 電力
- パワー インジェクタ PoE 電力
- 内部バッテリー電力

表 1 : 1552 モデルの電源オプション, (18 ページ) に、1552 アクセス ポイント モデルで使用可能な電源オプションを示します。

表 1 : 1552 モデルの電源オプション

電源オプション	1552E	1552H	1552C	1552I
AC	100 ~ 480 VAC 80 W	100 ~ 240 VAC 80 W	N/A	100 ~ 277 VAC 50 W
Power-over-Cable	N/A	N/A	40 ~ 90 V (準方形波) 45 W	N/A
PoE (パワー インジェクタ使用)	56 V +/- 10 %	56 V +/- 10 %	N/A	N/A
DC (公称 12 VDC)	11.4 ~ 15V	11.4 ~ 15V	11.4 ~ 12.6V	11.4 ~ 15V
バッテリー バックアップ	80W 時	35W 時	N/A	N/A

バッテリー バックアップ モジュール (任意)

次のバッテリー バックアップ 6 アンペア時間モジュールが用意されています。

- AIR-CAP-1552E-x-K9 モデル専用 AIR-1550-BATT-6AH

外部電源が使用できないとき、内部バッテリーを一時的にバックアップ電源として使用できます。AP1550 のバッテリー ランタイムは、次のとおりです。

- 770F (250C) で PoE 出力ポートをオフにしたデュアル無線で 2 時間の運転が可能
- 770F (250C) で PoE 出力ポートをオンにしたデュアル無線で 1.5 時間の運転が可能

アクセス ポイント ケーブルの設定では、バッテリー パックはサポートされていません。



(注) 取り付けブラケット、パワー インジェクタ、電源タップ アダプタなどの AP1520 用オプションハードウェアコンポーネントのリストについては、http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.htmlを参照してください。

1550 のリセット ボタン

1500 シリーズのアクセス ポイントの底面にはリセット ボタンがあります。リセット ボタンは、小さな穴の奥にあり、ネジとゴム製のガスケットで密閉されています。リセット ボタンを使用すると、次の機能を実行できます。

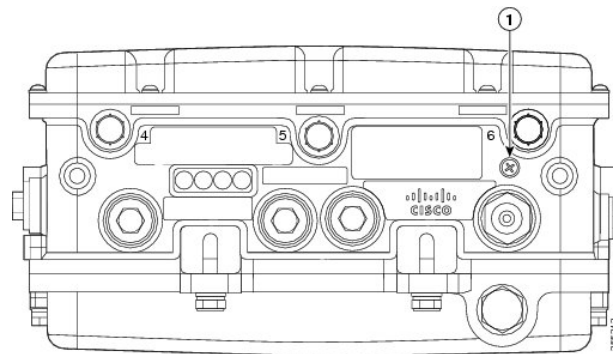
- アクセス ポイントのリセット：リセット ボタンを押している時間が 10 秒未満の場合、リセット中は LED が消灯し、リセットが終了すると再び点灯します。
- バッテリ バックアップ電源の無効化：リセット ボタンを押している時間が 10 秒を超える場合、LED が消灯し、点灯した後、消灯したままになります。

◦ 次のコマンドを入力すると、リモートでバッテリーをディセーブルにできます。

```
config mesh battery-statedisableAP_name
```

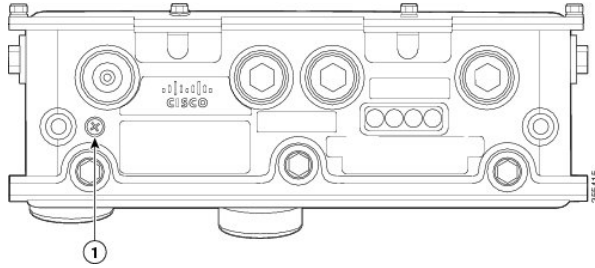
- LED のスイッチ オフ：リセット ボタンを押している時間が 10 秒を超える場合、LED が消灯し、点灯した後、消灯したままになります。

図 2：リセット ボタンの位置：モデル *AIR-CAP1552E-x-K9*、*AIR-CAP1552H-x-K9*



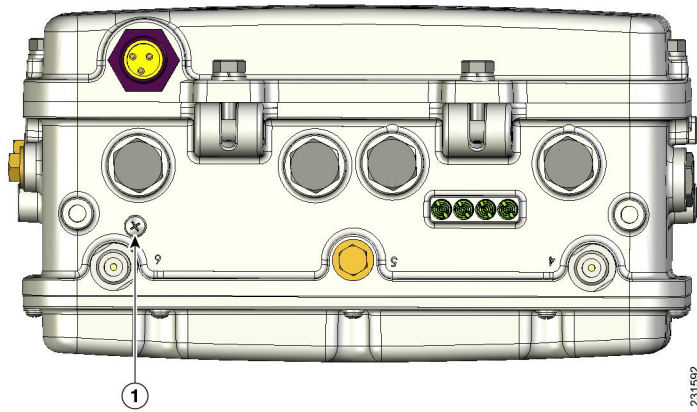
1	リセット ボタン
---	----------

図 3: リセット ボタンの位置: モデル *AIR-CAP1552C-x-K9*、*AIR-CAP1552I-x-K9*



1 リセット ボタン

図 4: 1520 シリーズのリセット ボタンの位置



1 リセット ボタンの位置

1550 アクセス ポイントのリセット

アクセス ポイントをリセットする手順は、次のとおりです。

- ステップ 1** プラス ドライバを使用してリセット ボタンのネジを取り外します。ネジをなくさないようにしてください。
- ステップ 2** まっすぐに伸ばしたペーパーリップを使用して、リセット ボタンを 10 秒未満の間、押します。この手順により、アクセス ポイントがリブート（電源が再投入）され、すべての LED が約 5 秒間消灯した後、再度点灯します。
- ステップ 3** リセット ボタンに再度ネジをねじ込み、プラス ドライバを使用して 2.49 ~ 2.71Nm（22 ~ 24 インチ ポンド）で締めます。

1550 LED ステータスのモニタリング

AP1550 の 4 つのステータス LED は、設置プロセス中に、接続や無線のステータス、アクセス ポイントのステータス、ソフトウェアのステータスを確認するのに便利です。ただし、アクセス ポイントが一度稼働し始めてそれ以上の診断が必要ない場合には、環境に配慮して LED を消灯することを推奨します。

アクセス ポイントが正常に動作しない場合は、装置の底面にある LED を確認します。この LED を使用して、装置のステータスを簡単に評価できます。

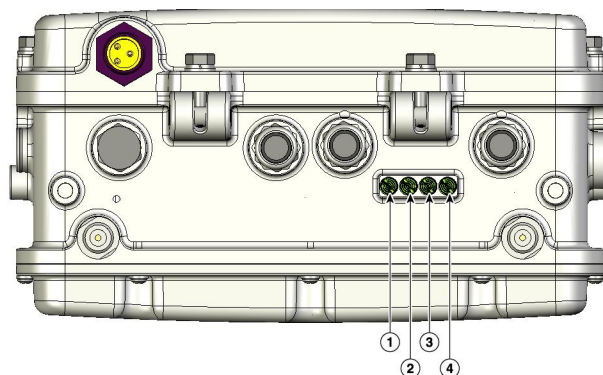


- (注) LED は、`config ap led-state {enable | disable} {cisco_ap_name | all}` コマンドを使用して有効または無効にします。

AP1550 には、4 つの LED ステータス インジケータがあります。

この図は、AP1550 LED の位置を示しています。

図 5: アクセス ポイントの装置底面にある LED



次の表は、各 LED とそれぞれのステータスを表します。

1	ステータス LED : アクセス ポイントとソフトウェアのステータス	3	RF-1 LED : スロット 0 (2.4GHz) とスロット 2 (1524SB は 5.8 GHz、1524PS は 4.9 GHz) の無線のステータス。
2	アップリンク LED : イーサネット、ケーブル、または光ファイバのステータス	4	RF-2 LED : スロット 1 (5.8GHz) とスロット 3 の無線のステータス。 ¹

¹ スロット 3 は無効



(注)

RF-1 LED と RF-2 LED は 2 つの無線を同時にモニタできますが、対象となる無線を特定することはできません。たとえば、RF-1 LED が赤色に点灯した場合、スロット 0 とスロット 2 のいずれかの無線、または両方の無線でファームウェア障害が発生していることになります。障害の原因となっている無線を特定するには、アクセス ポイント CLI やコントローラ GUI を使用して障害を調査し、問題を切り分ける必要があります。

表 2 : アクセス ポイントの LED 表示内容、(22 ページ) にアクセス ポイントの LED の表示内容を示します。

表 2 : アクセス ポイントの LED 表示内容

LED	色 ²³	意味
ステータス	消灯	アクセス ポイントの電源が入っていません。
	緑	アクセス ポイントが動作中です。
	緑色に点滅	Cisco IOS イメージファイルのダウンロードまたはアップグレードが進行中です。
	オレンジ	メッシュのネイバーアクセス ポイントの検出が進行中です。
	オレンジに点滅	メッシュの認証が進行中です。
	赤色、緑色、黄色で点滅	CAPWAP の検出が進行中です。
	赤	ファームウェアの障害です。サポート組織にお問い合わせを仰いでください。

LED	色 ²³	意味
アップリンク	消灯	物理的なコネクタが存在しません。アップリンクポートが動作していません。
	緑	アップリンク ネットワークが動作中です (ケーブル、光ファイバ、またはイーサネット)。
RF-1 スロット 0 2.4 GHz 無線	消灯	無線がオフになっています。
	緑	無線が動作中です。
	赤	ファームウェアの障害です。サポート組織に問い合わせを仰いでください。
RF-1 スロット 2 802.11a 無線	消灯	無線がオフになっています。
	緑	無線が動作中です。
	赤	ファームウェアの障害です。サポート組織に問い合わせを仰いでください。
RF-2 スロット 1 802.11a 無線	消灯	無線がオフになっています。
	緑	無線が動作中です。
	赤	ファームウェアの障害です。サポート組織に問い合わせを仰いでください。
RF-2 スロット 3	このリリースではディセーブル	—

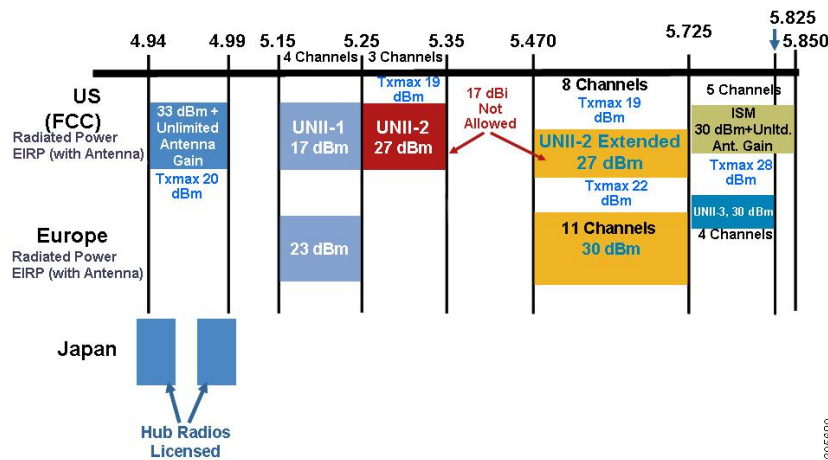
² すべての LED がオフの場合は、アクセス ポイントは電源オフです。

³ アクセス ポイントの電源が最初にオンにされると、すべての LED がオレンジになります。

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 6 : 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 3 : 周波数帯域, (24 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 チャンネル : 169 (5.845 GHz) および 173 (5.865 GHz)
- 40 MHz チャンネル : チャンネル 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 3 : 周波数帯域

周波数帯域用語	説明	サポート モデル
UNII-1 ⁴	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 と 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、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、および 1572。
ISM ⁵	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、および 1572。

⁴ UNII は、Unlicensed National Information Infrastructure を意味しています。

⁵ 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 (DFS)

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。無線がレーダー信号を検出すると、そのサービスを保護するために、少なくとも 30 分間送信を停止する必要があります。無線は、それをモニタした後にのみ送信されるように、別のチャンネルを選択します。使用する予定のチャンネルで少なくとも 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ンネルで伝送を開始できます。

AP は 60 秒間新しい DFS チャンネルで DFS スキャンを実行します。ただし、隣接する AP がその新しい DFS チャンネルをすでに使用している場合、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きます。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャンネル 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 7: DFS および TPC 帯域の要件

	Frequency (MHz)
1	5150 – 5250
2	5250 – 5350
	5470 – 5725
3	5725 – 5850

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、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。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

メッシュアクセスポイントをさまざまな地域に配置する際には、柔軟性を提供するため、多岐にわたるアンテナが利用できます。5 GHz はバックホールとして使用され、2.4 GHz はクライアントアクセスに使用されます。

表 4：外部 2.4 GHz および 5 GHz アンテナ、(27 ページ) は、AP1500 用にサポートされる、外部の 2.4 GHz および 5 GHz のアンテナのリストです。

表 4：外部 2.4 GHz および 5 GHz アンテナ

部品番号	モデル	ゲイン (dBi)
AIR-ANT2450V-N	2.4 GHz 小型全方向性 ⁶	5
AIR-ANT-2455V-N	2.4 GHz 小型全方向性	5.5
AIR-ANT2480V-N	2.4 GHz 全方向性	8.0
AIR-ANT5180V-N	5 GHz 小型全方向性 ⁷	8.0

部品番号	モデル	ゲイン (dBi)
AIR-ANT5140V-N	5 GHz 90 度、全方向性	4.0
AIR-ANT5114P-N	5 GHz patch2	14.0
AIR-ANT2547V-N	2.4 ~ 5 GHz デュアルバンド、全方向性	2.4 GHz で 4 dBi、5 GHz で 7 dBi

⁶ 小型全方向性アンテナは、アクセスポイントに直接取り付けます。

⁷ 小型全方向性アンテナは、アクセスポイントに直接取り付けます。

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。

表 5：シスコ製アンテナの水平ビーム幅および垂直ビーム幅、(28 ページ) は、シスコ製アンテナの水平ビーム幅および垂直ビーム幅の要約です。

表 5：シスコ製アンテナの水平ビーム幅および垂直ビーム幅

アンテナ	水平ビーム幅 (度数)	垂直ビーム幅 (度数)
AIR-ANT5180V-N	360	16
AIR-ANT5114P-N	25	29
AIR-ANT2547V-N	360	30

N コネクタ

すべての外部アンテナには、オス型 N コネクタが装備されています。

AP1552 E/H にはデュアルバンドアンテナを接続するための N コネクタが 3 つあります。

AP1552 C/I にはアンテナが内蔵されているため、N コネクタはありません。

各無線には、1 つ以上の TX/RX ポートがあります。各無線には、利用できる TX/RX ポートの 1 つ以上にアンテナを接続する必要があります。

5.8 GHz および 2.4 GHz のアンテナの位置は固定で、ラベル付けされています。

1552 のアンテナ構成

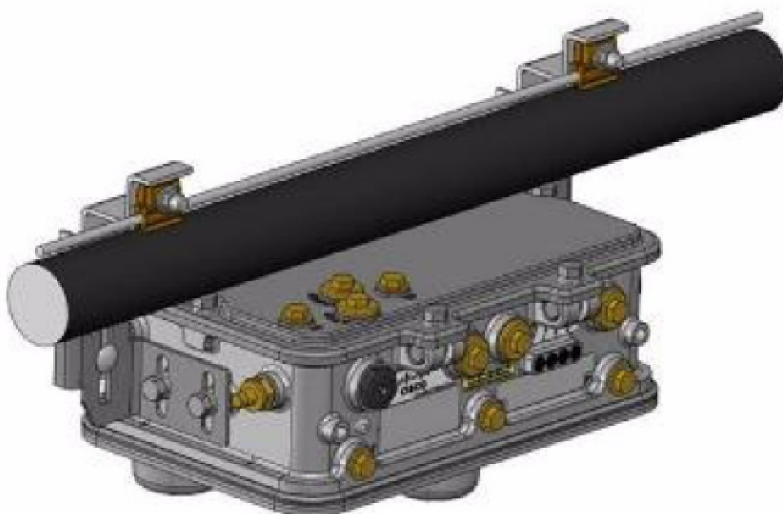
1552 アクセスポイントは、2.4 GHz および 5 GHz 周波数で動作する無線を使用した屋外使用向けに設計された次の 2 種類のアンテナをサポートします。

- 3本のデュアルバンドダイポールアンテナの統合アレイである、Cisco Aironet ロープロファイルデュアルバンド2.4/5 GHzダイポールアンテナアレイ (CPN 07-1123-01)
- 「スティック」アンテナと呼ばれる、Cisco Aironet デュアルバンド全方向性アンテナ (AIR-ANT2547V-N)

設置構成には、ケーブルより線取り付けと柱取り付けの2種類があります。

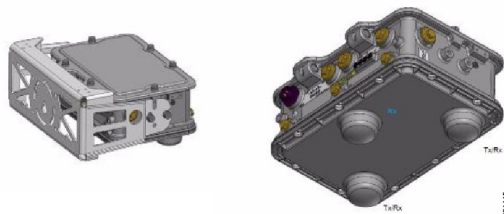
1552モデルCおよびIアクセスポイントには、ゲインが2.4 GHzで2 dBi、5 GHzで4 dBiの新しい統合デュアルバンドアンテナ3本が搭載されています。アンテナは、ケーブルより線取り付けおよび低コスト、ロープロファイルアプリケーションで動作します。

図 8 : 1552C ケーブル取り付け



331444

図 9 : 1552I 柱/壁面取り付け

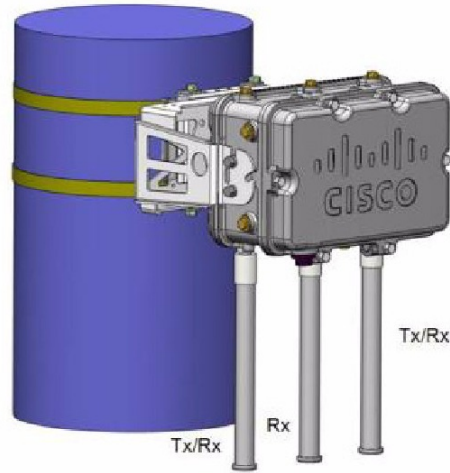


331444

1552 E および H アクセス ポイントは、底面に外部アンテナ用 N 型無線周波数 (RF) コネクタ 3 つ (アンテナポート 4、5、6) を備え、Multiple Input Multiple Output (MIMO) 操作をサポートします (以下の図を参照)。オプションの Cisco Aironet AIR-ANT2547V-N デュアルバンド全方向性

アンテナを使用する場合、2.4 および 5 GHz アンテナは直接アクセス ポイントに接続します。これらのアンテナには 2.4 GHz で 4 dBi のゲイン、5 GHz で 7 dBi のゲインがあります。

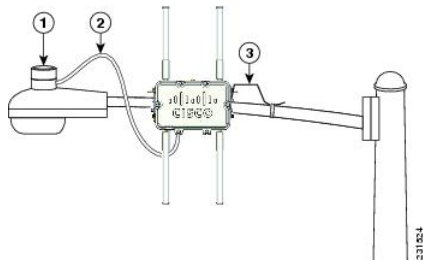
図 10: 1552 E 柱/壁面取り付け



331446

この図は、屋外 AP1500 の推奨取り付け例です。

図 11: メッシュ アクセス ポイントの屋外ポールトップの取り付け



1	屋外照明コントロール	3	6 AWG のアース線
2	街路灯の電源タップアダプタ		

AP1500 シリーズは、過去数年間にわたる屋外アクセス ポイント導入における経験に基づいて設計されています。これには耐雷に関する考慮事項も含まれています。AP1500 シリーズは、イーサネットポートと電源ポートに避雷回路が採用されています。入力イーサネットポートで、電源入力モジュール (PEM) にガス放電管 (GDT) を使用して雷の影響を緩和します。AC 電源では、高電流状態を緩和するヒューズと共に GDT も使用します。DC 電源では、ヒューズを使用して高電流状態を緩和します。

一般的ではありませんが、避雷効果を高めるためにアンテナポートに避雷手段を追加することもできます。

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。

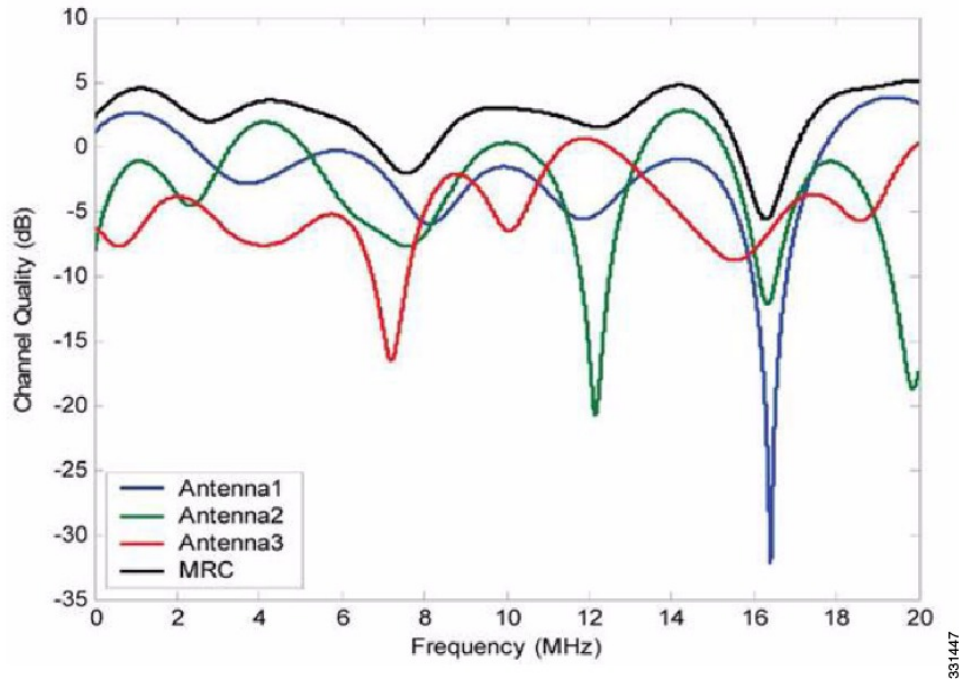
最大比合成

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 12: MRC アルゴリズムによる受信信号の強化



1550 シリーズ用

1552 シリーズ メッシュ アクセスポイントの MRC ゲインは 1520 シリーズ メッシュ アクセスポイントとは異なります。1520 シリーズ アクセスポイントには 802.11n 機能がありません。2.4 GHz 帯域では、このアクセスポイントには 1 つのトランスミッタと最大 3 つのレシーバだけがあります。そのため、2.4 GHz では SIMO (Single in Multiple out) です。5 GHz 帯域では、このアクセスポイントには 1 つのトランスミッタと 1 つのレシーバだけがあります。そのため、5 GHz 帯域では SISO (Single in Single out) です。MRC ゲインは、1552 アクセスポイントの 2.4 GHz 無線でのみ重要です。MRC は 5 GHz 無線では使用できません。2.4 GHz 無線には、AP 構成に応じて 1 本の Tx アンテナと最大 3 本のアンテナがあります。

1522 アクセスポイントでは、2.4 GHz Rx アンテナ 1 本、2 本、または 3 本を使用できるオプションがあります。このオプションを使用すると、24 Mbps 以上のデータレートに対する MRC ゲインは 2 本の Rx アンテナで約 3 dB、3 本の Rx アンテナで 4.5 dB になります。

1552 アクセスポイントでは、2.4 GHz および 5 GHz の両方の無線は 2x3 MIMO です。そのため、このアクセスポイントには 2 つのトランスミッタと 3 つのレシーバがあります。アンテナがデュアルバンドで、Rx アンテナを 2 本以下にするオプションがないことから、MRC が常に RX 感度に追加されます。これは MRC がベースバンドチップセットに埋め込まれているためです。

シスコのカスタマーデータシートの一般的な Rx 感度の数値は、1520 および 1550 シリーズ アクセスポイントで 3 本の Rx アンテナを前提としています。

AP1520 シリーズの無線に使用されるチップセットには、ゲインがなくなる低いデータ レートでのパケット開始で問題がありました。そのため、1520 シリーズ アクセス ポイントでは、12 Mbps 以上のデータ レートからの MRC ゲインが有用でした。この問題は、1552 アクセス ポイントに使用されている現在のチップセットで修正されています。1552 アクセス ポイントでは、低いデータ レートに対しても MRC ゲインが改善されています。2x3 MIMO 無線では、1x1 SISO 実装より感度が 4.7 dB 改善されています。

表 6 : AP1552 11a/g の MRC ゲイン, (33 ページ) および 表 7 : AP1552 11n の MRC ゲイン, (33 ページ) に、AP1552 11a/g および AP1552 11n の各 MRC ゲインを示します。

表 6 : AP1552 11a/g の MRC ゲイン

11a/g MCS (Mbps)	変調	3 RX からの MRC ゲイン (dB)
6	BPSK 1/2	4.7
9	BPSK 3/4	4.7
12	QPSK 1/2	4.7
18	QPSK 3/4	4.7
24	16QAM 1/2	4.7
36	16QAM 3/4	4.7
48	64QAM 2/3	4.7
54	64QAM 3/4	4.7

表 7 : AP1552 11n の MRC ゲイン

空間ストリーム数	11n MCS	変調	3 RX からの MRC ゲイン (dB)
1	MCS 0	BPSK 1/2	4.7
1	MCS 1	QPSK 1/2	4.7
1	MCS 2	QPSK 3/4	4.7
1	MCS 3	16QAM 1/2	4.7
1	MCS 4	16QAM 3/4	4.7
1	MCS 5	64QAM 2/3	4.7
1	MCS 6	64QAM 3/4	4.7

空間ストリーム数	11n MCS	変調	3RXからのMRCゲイン (dB)
1	MCS 7	64QAM 5/6	4.7
2	MCS 8	BPSK 1/2	1.7
2	MCS 9	QPSK 1/2	1.7
2	MCS 10	QPSK 3/4	1.7
2	MCS 11	16QAM 1/2	1.7
2	MCS 12	16QAM 3/4	1.7
2	MCS 13	64QAM 2/3	1.7
2	MCS 14	64QAM 3/4	1.7
2	MCS 15	64QAM 5/6	1.7



(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。

Cisco 1500 危険場所認証

標準の AP1500 ラックは、ほこりや湿気、水分が入らないよう保護するための NEMA 4X および IP67 規格をサポートする、高耐久高強度のラックです。

危険認定 (Class 1、Div 2、Zone 2)

石油精油所、油田、掘削基地、化学処理施設、露天堀りなどの危険性のある環境で作動させるには、特別な認証が必要です。この認証は Class 1、Div 2、または Zone 2 と表示されます。



(注) 米国およびカナダでは、この認証は CSA Class 1、Division 2 です。欧州 (EU) では、ATEX または IEC Class 1、Zone 2 です。

シスコには、米国および EU 向けの危険認定 SKU があります (AIR-LAP1552H-x-K9)。認証要件に従い、このSKUは修正されます。電気配線が偶発的損傷によってスパークや爆発を起こすのを防ぐために、危険場所認証にはすべての送電線がコンジットパイプを使用して設置されている必要があります。危険場所用のアクセスポイントには、側面から入力するコンジットインターフェイス カプラからディスクリートワイヤを受け取る内部電気取り付けコネクタが搭載されています。

す。電気配線が取り付けられると、電気コネクタが電気配線に直接触れないよう、その上にカバーが取り付けられます。本体の外側には、危険場所認証ラベル（CSA、ATEX、または IEC）があり、認証のタイプとその機器の動作が認可された環境がわかるようになっています。



(注) CSA の電源入力モジュール（米国およびカナダ）は、電源入力モジュール、グループ A、B、C、および D、T5v（120 □）温度コードです。ATEX の電源入力モジュール（EU）は、電源入力モジュール グループ IIC、IIB、IIA、T5（120 □）温度コードです。

危険認定（Div 1 > Div 2 および Zone 1 > Zone 2）

Class 1、Division 1/Zone 1 は、常時引火濃度の可燃性ガス、蒸気、液体が存在する環境を想定しています。Div 1 > Div 2 および Zone 1 > Zone 2 の場所の要件を満たすものとして、TerraWave Solutions CSA 認定の保護 Wi-Fi ラックを推奨します（表 8：TerraWave ラック，（35 ページ）を参照）。

表 8：TerraWave ラック

アクセス ポイント	格納ラックの製品番号	説明
屋内メッシュアクセスポイント	例：1240 シリーズ用 TerraWave XEP1242	Cisco 1242 アクセス ポイントが格納された 18 x12 x8 保護 Wi-Fi ラック
屋外メッシュアクセスポイント（1552）	例：TerraWave 製品番号：XEP1522	Cisco 1522 アクセス ポイントが格納された 18 x12 x 8 保護 Wi-Fi ラック

TerraWave ラックの詳細については、http://www.tessco.com/yts/partner/manufacture_list/vendors/terrawave/pdf/terrawavehazardouesenclosuresjan08.pdfを参照してください。

表 9：ハードウェア機能一覧，（35 ページ）に、AP1500 の各種モデルのハードウェア機能一覧を示します。

表 9：ハードウェア機能一覧

機能	1552E	1552H	1552C	1552I
無線数	2	2	2	2
外部アンテナ	Yes	Yes	—	—
内部アンテナ	—	—	Yes	Yes
CleanAir 2.4 GHz 無線	Yes	Yes	Yes	Yes
CleanAir 5 GHz 無線	—	—	—	—
ビーム形成（ClientLink）	Yes	Yes	Yes	Yes

機能	1552E	1552H	1552C	1552I
ファイバ SFP	Yes	Yes	—	—
802.3af PoE 出力ポート	Yes	Yes	—	—
DOCSIS 3.0 ケーブルモデム	—	—	Yes	—
HazLoc Class 1 Div 2/Zone 2	—	Yes	—	—
バッテリーバックアップオプション	Yes	Yes	—	—
電力オプション	AC、DC、パワーインジェクタ	AC、DC、パワーインジェクタ	40 ~ 90 VAC Power-over-Cable	AC、DC
コンソールポート外部アクセス	Yes	Yes	Yes	Yes



(注) PoE 入力は 802.3af ではないため、PoE 802.3af 対応イーサネットスイッチでは動作しません。パワーインジェクタが必要です。

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、管理に、グラフィカル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稼働します。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ク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ズ機能を実行して、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

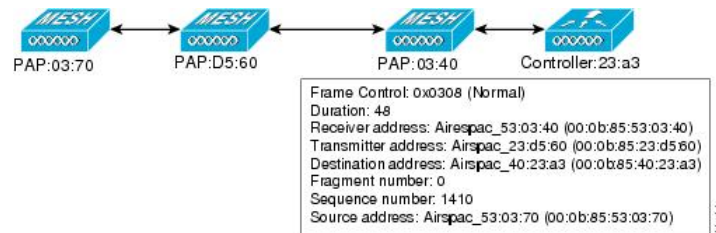
CAPWAP モデルはよく知られており、AWPP は専用プロトコルのため、ワイヤレスメッシュデータフローについてだけ説明します。ワイヤレスメッシュデータフローのキーは、メッシュアクセスポイント間で送信される 802.11 フレームのアドレスフィールドです。

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 13 : ワイヤレスメッシュフレーム、(41 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

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 13: ワイヤレスメッシュフレーム

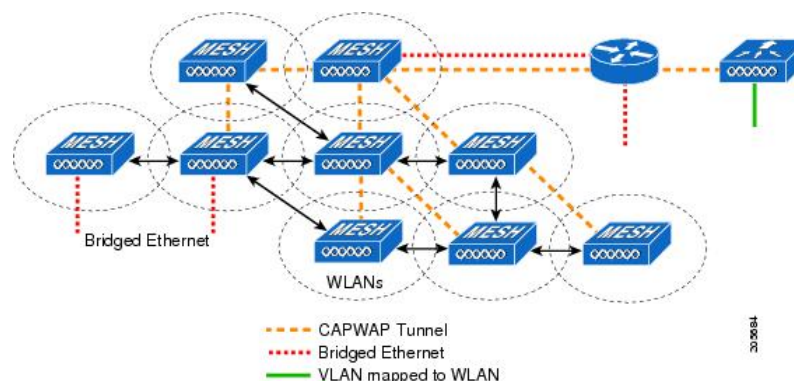


このフレームの送信により、トランスミッタとレシーバのアドレスは、ホップごとに変ります。各ホップでレシーバアドレスを判別するために AWPP が使用されます。トランスミッタアドレスは、現在のメッシュアクセスポイントのアドレスです。パス全体を通して、発信元アドレスと送信先アドレスは同一です。

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 14: 論理ブリッジとWLANマッピング, (41 ページ) を参照）。

図 14: 論理ブリッジとWLANマッピング

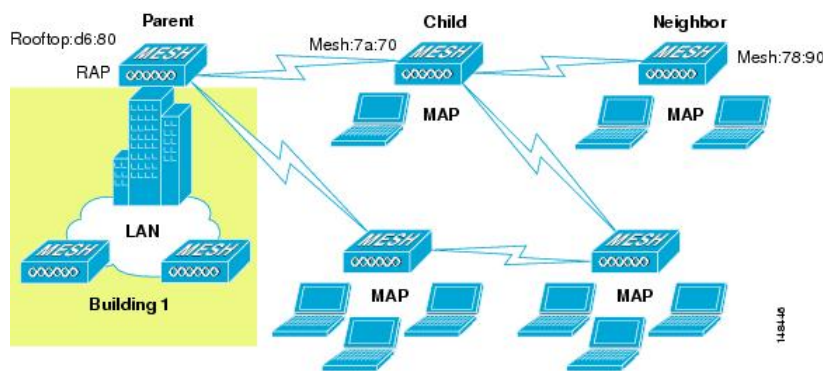


メッシュネイバー、親、および子

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 15: 親、子、およびネイバーアクセスポイント, (42 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 15: 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、パッシブスキャンニングによって、ネイバーのあるチャン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ンネルのサブセットになります。
- seek* ステートでは、アクティブスキャンニングによって、ネイバーを持つチャンネルが探され、バックホールチャンネルは最適なネイバーを持つチャン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、チャン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ンネル上で 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、そのチャン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。

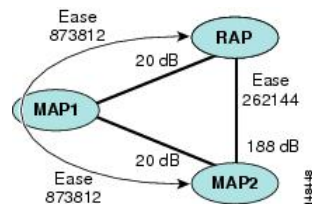
親メッシュアクセスポイントは、RAPに戻る最適なパスを提供します。AWPPは、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

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16: 親パスの選択, (43 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 16: 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](#), 45 ページ
- [無線バックホール](#), 46 ページ
- [ポイントツーマルチポイント無線ブリッジング](#), 46 ページ
- [ポイントツーポイント無線ブリッジング](#), 47 ページ

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](#)の項を参照してください。

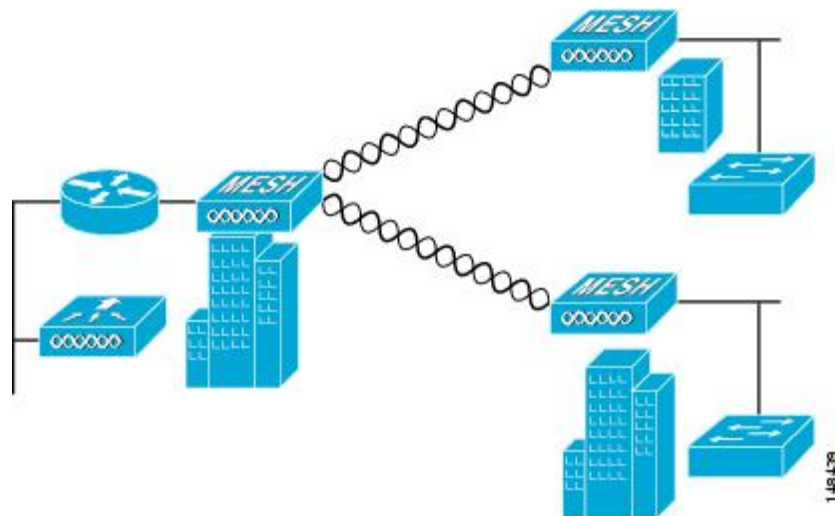
ポイントツーマルチポイント無線ブリッジング

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 17: ポイントツーマルチポイントブリッジングの例

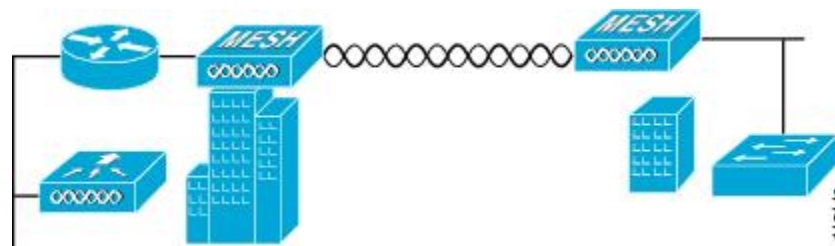


ポイントツーポイント無線ブリッジング

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 18: 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] ページと選択し、[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] と選択します。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。

範囲：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, 51 ページ](#)
- [ClientLink テクノロジー, 55 ページ](#)
- [コントローラの計画, 59 ページ](#)

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 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、利用可能なチャン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 10：バックホールのデータ レートと LinkSNR の最小要件](#)、(52 ページ) に示します。

表 10：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 11：802.11n のバックホール データ レートと最小 LinkSNR 要件](#)、(53 ページ) 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 11 : 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 12 : 802.11a/g に必要な LinkSNR の計算, (54 ページ) 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 12 : 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 13 : 2.4 および 5 GHz での AP1552 の LinkSNR 要件, (54 ページ) 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 13 : 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		4.7	9	21.3
1	MCS 5	64QAM 2/3	。	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		1.7	9	24.3
2	MCS 13	64QAM 2/3	。	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、24Mbps の最大スループットは、最初のホップで約 14Mbps、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。

ClientLink テクノロジー

多くのネットワークは、依然として 802.11n クライアントと 802.11ac クライアントの混在をサポートします。802.11a/g クライアント (レガシークライアント) は低データレートで動作するため、

古いクライアントにより、ネットワーク全体のキャパシティが減少することがあります。シスコのClientLink テクノロジーは、802.11a/g クライアントが、特にセル境界に近い場合に、最適なレートで動作できるようにすることで、クライアントが混在するネットワークにおける 802.11n の採用に関連する問題を解決します。

高度な信号処理が Wi-Fi チップセットに追加されました。複数の送信アンテナが 802.11a/g クライアントの方向に伝送を収束するために使用され、ダウンリンクの信号対ノイズ比と一定のレンジにおけるデータレートが増加するため、カバレッジホールが減少し、システム全体のパフォーマンスが向上します。このテクノロジーは、クライアントから受信された信号を合成する最適な方法を学習し、この情報を使用してパケットを最適な方法でクライアントに送り返します。このテクニックは、MIMO（複数入力複数出力）ビームフォーミング、送信ビームフォーミング、またはコフェーシングとも呼ばれ、高価なアンテナアレイを必要としない、市場で唯一のエンタープライズクラスかつサービス プロバイダークラスのソリューションです。

802.11n システムは、複数の無線信号を同時に送信することによりマルチパスを利用します。空間ストリームと呼ばれるこれらの各信号は、独自のトランスミッタを使用して独自のアンテナから送信されます。これらのアンテナ間には空間があるため、各信号は受信装置への若干異なるパスに従います（空間ダイバーシティと呼ばれる状況）。レシーバにも、独自の無線を使用する複数のアンテナがあります。各アンテナは受信した信号を独自にデコードし、各信号は他のレシーバの無線からの信号と結合されます。その結果、複数のデータストリームが同時に受信されます。これにより、以前の 802.11a/g システムよりも高いスループットが実現されますが、信号を解読する 802.11n 対応クライアントが必要になります。したがって、AP とクライアントの両方がこの機能をサポートする必要があります。問題が複雑であるため、第 1 世代のメインストリーム 802.11n チップセットでは、AP およびクライアントチップセットで 802.11n 送信ビームフォーミングが実装されていません。したがって、802.11n 標準伝送ビームフォーミングは将来利用可能になりますが、次世代のチップセットが市場に出るまで待つ必要があります。シスコは、この分野の発展をリードしていく所存です。

現行世代の 802.11n AP について、2 つ目の送信パスが 802.11n クライアントでは（空間ダイバーシティを実装するために）よく使用されてきましたが、802.11a/g クライアントでは十分に使用されていなかったことを、シスコは認識していました。つまり、802.11 a/g クライアントに対しては、余分な送信パスの機能の一部がアイドル状態のままでした。また、多くのネットワークでは、設置されている 802.11 a/g クライアントベースのパフォーマンスがネットワークの制限要素になることも認識していました。

802.11 a/g クライアントのパフォーマンス レベルを高めることで、このアイドル状態の機能を利用して全体的なネットワーク キャパシティを大幅に向上させるために、シスコは ClientLink という伝送ビーム形成テクノロジーにおける技術革新をもたらしました。

ClientLink は高度な信号処理手法と複数の送信パスを使用して、ダウンリンク方向で 802.11a/g クライアントが受信した信号を、フィードバックを必要とせずに、最適化します。特別なフィードバックが必要ないため、Cisco ClientLink は、既存のすべての 802.11a/g クライアントで動作します。

Cisco ClientLink テクノロジーにより、クライアントが配置された場所でアクセスポイントが SNR を効果的に最適化できるようになります。ClientLink は、ダウンリンク方向にほぼ 4 dB のゲインを提供します。SNR が改善され、再試行回数の減少やデータレートの向上などの多くの利点を提供されます。たとえば、以前に 12 Mbps でパケットを受信できたセルの端にあるクライアントが 36 Mbps でパケットを受信できるようになります。ClientLink を使用した場合のダウンリンクパ

パフォーマンスの一般的な測定値は、802.11a/g クライアントではスループットが 65% 向上します。Wi-Fi システムがより高いデータ レート、少ない再試行回数で動作できるようにすることで、ClientLink はシステムのキャパシティ全体を拡張します。つまり、スペクトル リソースを効率的に利用できます。

1552 アクセス ポイントの ClientLink は、AP3500 で使用可能な ClientLink 機能をベースにしています。したがって、アクセス ポイントは近接するクライアントに対してビームフォーミングを行い、802.11ACK でビームフォーミング情報を更新できます。したがって、専用アップリンクトラフィックがない場合でも、ClientLink は適切に動作します。これは、TCP および UDP 両方のトラフィックストリームに有用です。Cisco 802.11n アクセス ポイントでこのビーム形成を使用するためにクライアントが通過する必要がある RSSI ウォーターマークはありません。

ClientLink は、同時に 15 のクライアントにビーム形成を行うことができます。したがって、レガシークライアントの数が無線ごとに 15 を超える場合に、ホストは最良の 15 クライアントを選択する必要があります。AP1552 には 2 つの無線があるため、タイム ドメインで最大 30 個のクライアントに対してビームフォーミングを行えます。

ClientLink は、屋内および屋外 802.11n アクセス ポイント用の 11a/g レート (11b ではない) を示す、パケットのレガシー OFDM 部分に適用されますが、屋内 11n 用の ClientLink と屋外 11n 用の ClientLink には 1 つの違いがあります。屋内 11n アクセス ポイントの場合、SW は影響を受けるレートを 24、36、48、54 Mbps に制限します。これは、屋内環境でクライアントが離れた AP に固定されるのを回避するために行われます。また、スループットゲインが非常に小さいため、SW によって ClientLink が 11n クライアント用のレートで動作できなくなります。ただし、純粋なレガシークライアントに対しては明らかなゲインがあります。屋外 11n アクセス ポイントの場合、カバレッジを拡張する必要があります。そのため、24 Mbps 未満のレガシー データ レートがさらに 3 つ追加されました。屋外用の ClientLink は 6、9、12、18、24、36、48、54 Mbps のレガシー データ レートに適用されます。



(注) ClientLink はデフォルトで有効になっています。

ClientLink の設定 (CLI)

7.2 リリース以降から、コントローラ GUI を使用して ClientLink (ビーム形成) を設定することはできません。

ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを無効にします。

```
config {802.11a | 802.11b} disable network
```

ステップ 2 次のコマンドを入力して、802.11a または 802.11g ネットワーク上でビーム形成をグローバルにイネーブルまたはディセーブルにします。

```
config {802.11a | 802.11b} beamforming global {enable | disable}
```

デフォルト値は [disabled] です。

(注) ネットワーク上でビーム形成をイネーブルにすると、そのネットワーク タイプに該当するすべての無線で自動的に有効になります。

ステップ 3 次のコマンドを入力して、グローバル設定をオーバーライドして、特定のアクセスポイントのビーム形成をイネーブルまたはディセーブルにします。

```
config {802.11a | 802.11b} beamforming apCisco_AP {enable | disable}
```

デフォルトの値は、ネットワーク上でビーム形成が無効である場合はディセーブル、ネットワーク上でビーム形成が有効である場合はイネーブルになります。

ステップ 4 次のコマンドを入力して、ネットワークを再び有効にします。

```
config {802.11a | 802.11b} enable network
```

ステップ 5 次のコマンドを入力して、変更を保存します。

```
save config
```

ステップ 6 次のコマンドを入力して、ネットワークのビーム形成ステータスを表示します。

```
show {802.11a | 802.11b}
```

以下に類似した情報が表示されます。

```
802.11a Network..... Enabled
11nSupport..... Enabled
802.11a Low Band..... Enabled
802.11a Mid Band..... Enabled
802.11a High Band..... Enabled
...
Pico-Cell-V2 Status..... Disabled
TI Threshold..... -50
Legacy Tx Beamforming setting..... Enabled
```

ステップ 7 次のコマンドを入力して、特定のアクセスポイントのビーム形成ステータスを表示します。

```
show ap config {802.11a | 802.11b} Cisco_AP
```

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 14
Cisco AP Name..... 1250-1
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A      802.11a:-A
...
Phy OFDM parameters
Configuration ..... AUTOMATIC
Current Channel ..... 149
Extension Channel ..... NONE
Channel Width..... 20 Mhz
Allowed Channel List..... 36,40,44,48,52,56,60,64,100,
..... 104,108,112,116,132,136,140,
..... 149,153,157,161,165
TI Threshold ..... -50
Legacy Tx Beamforming Configuration ..... CUSTOMIZED
Legacy Tx Beamforming ..... ENABLED
```

ClientLink に関連するコマンド

ClientLink に関連するコマンドは次のとおりです。

- 次のコマンドを AP コンソールで入力します。
 - AP のビーム形成のステータスを確認するには、**show controller d0/d1** コマンドを入力します。
 - AP rbf テーブルでクライアントを見つけるには、**show interface dot110** コマンドを入力します。
 - AP に割り当てられたビーム形成レートを確認するには、**debug d0 trace print rates** コマンドを入力します。

- トラブルシューティングを行うには、AP コンソールで次のコマンドを使用します。

- 無線で ClientLink が有効であることを示すには、**show controllers | inc Beam** コマンドを入力します。

次のような出力が表示されます。

```
Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -50 dBm
Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -60 dBm
```

- ClientLink が特定のクライアントにビーム形成を行っていることを表示するには、**show interface dot11radio 1 lbf rbf** コマンドを入力します。

次のような出力が表示されます。

```
RBF Table:
Index      Client MAC      Reserved      Valid      Tx BF      Aging
1          0040.96BA.45A0  Yes           Yes        Yes        No
```

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 14：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、（60 ページ）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 14：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） ⁸	最大メッシュ AP サポート
5508 ⁹	500	500
2504 ¹⁰	50	50
WiSM2	500	500

⁸ 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。

⁹ 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。

¹⁰ 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。



(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。屋内および屋外 AP（AP152X）には基本ライセンス（LIC-CT508-Base）で十分です。WPlus 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

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, 61 ページ](#)
- [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, 69 ページ](#)
- [屋内メッシュと屋外メッシュの相互運用性, 97 ページ](#)

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、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いければなりません。

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。

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過し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 19 : ポイントツーポイントリンクのフレネルゾーン, (64 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 19 : ポイントツーポイントリンクのフレネルゾーン

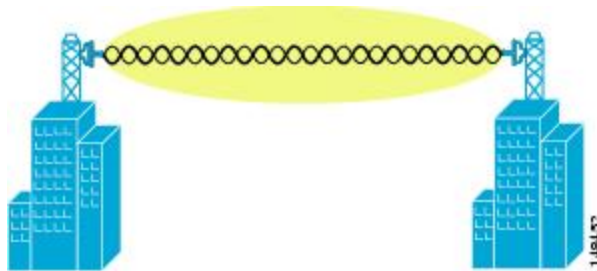


図 20 : フレネルゾーン内の一般的な障害物, (64 ページ) は、障害物のあるフレネルゾーンを示しています。

図 20 : 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。

$F1 = 72.6 \times (d/4 \times f)$ 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)

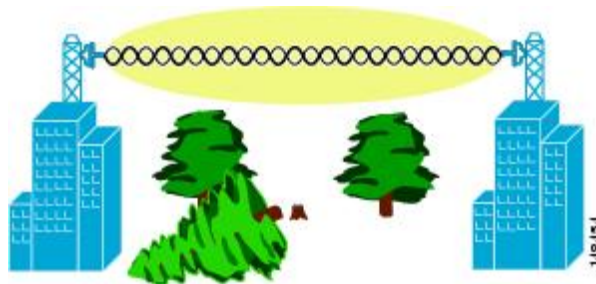
通常、最初のフレネルゾーンの 60% のクリアランスが推奨されるため、上の公式を 60% のフレネルゾーンクリアランスで表すと、次のようになります。

$0.60 F1 = 43.3 \times (d/4 \times f)$ の平方根

これらの計算は、平坦地に基づいたものです。

図 21：フレネルゾーンの障害物の除去、(65 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 21：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 = $43.3 \times \sqrt{1/(4 \times 4.9)}$ 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 チャン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 22：隠しノード

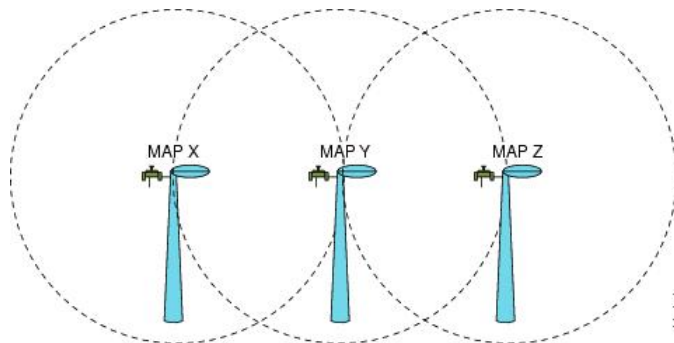


図 22：隠しノード、(65 ページ) は、次の 3 つの MAP を示します。

- 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。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いければ、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す。
- 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、MAPISB 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 MAPISB 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 MAPI

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 AP 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 (フィート換算で 52802) が、9 つのセル分で、およそ 3 または 4 のホップでカバーできます (図 23 : 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, (71 ページ) および 図 24 : 2.3 ~ 2.7 のパス ロス指数, (71 ページ) 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

25：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，（71 ページ） および図 26：2.5 ～ 3.0 のパス ロス指数，（72 ページ）を参照）。

図 23：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

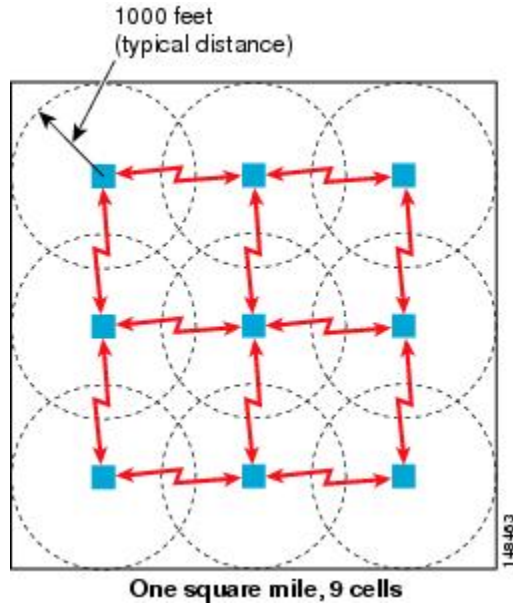


図 24：2.3 ～ 2.7 のパス ロス指数

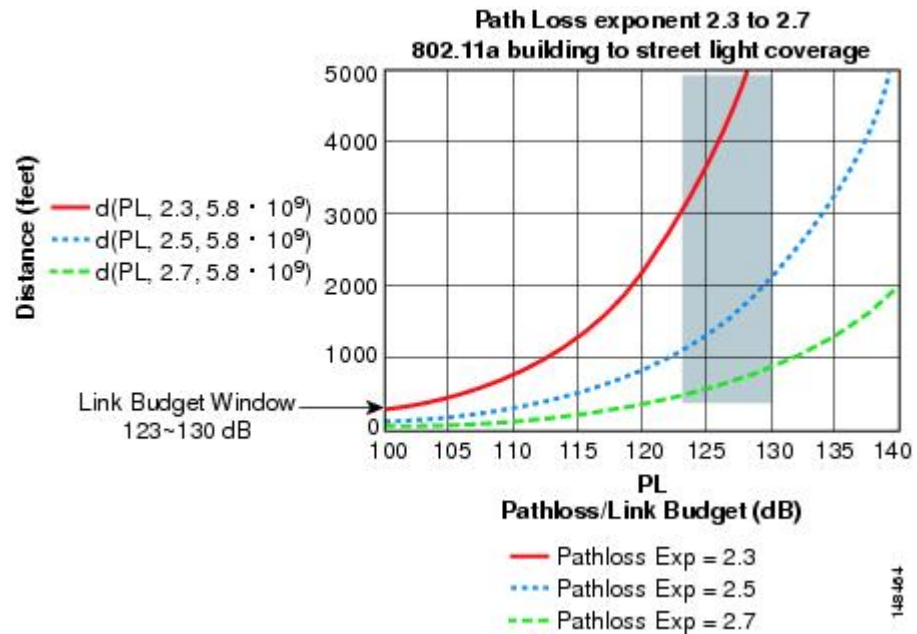


図 25：非音声メッシュ ネットワークにおける半径 600 フィートのセルとアクセス ポイントの位置

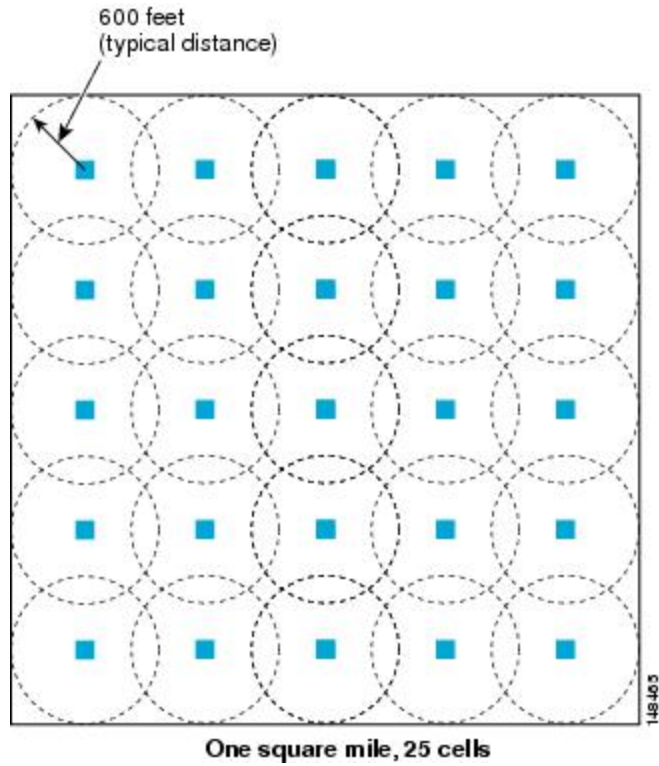
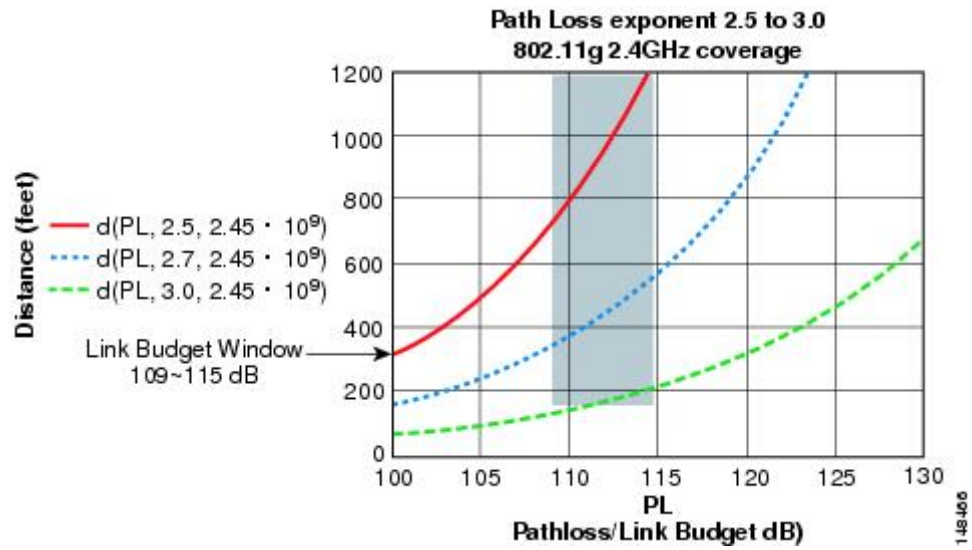


図 26 : 2.5 ~ 3.0 のパスロス指数



Cisco 1550 シリーズ AP 用

前の項で示されているように、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。

AP1550 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 バジレ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 バジレットの比較 (-A ドメイン)

表 15: -A/-B ドメインの 2.4 GHz 帯域のリンク バジレット比較, (73 ページ) を参照してください。

表 15: -A/-B ドメインの 2.4 GHz 帯域のリンク バジレット比較

パラメータ	Cisco 1552 (-A ドメイン)	Cisco 1532 (-A ドメイン)	Cisco 1572 (-B ドメイン)
周波数帯域	2412 ~ 2462 MHz	2412 ~ 2462 MHz	2412 ~ 2462 MHz
エア インターフェイス	802.11b/g/n	802.11b/g/n	802.11b/g/n
チャネル帯域幅	20 MHz	20 MHz	20 MHz
Tx 空間ストリーム数	2	1532I 用 3SS、1532E 用 2SS	3SS
PHY データ レート	最大 144 Mbps ¹¹	3SS で最大 216 Mbps 2SS で 144 Mbps	最大 216 Mbps
供給 Tx 電力	28 dBm、複合 ¹²	29 dBm	30 dBm
Rx 感度	6 Mbps で -94 dBm 54 Mbps で -79 dBm 150 Mbps で -73 dBm	6 Mbps で -95 dBm 54 Mbps で -75 dBm 216 Mbps で -69 dBm	6 Mbps で -93 dBm 54 Mbps で -81 dBm 216 Mbps で -76 dBm
受信チャネル数	3	3	4
Rx ダイバーシティ	MRC	MRC	MRC
アンテナケーブル損失	0.5 dB (外部アンテナ使用)	0.5 dB	0.5 dB

¹¹ 2.4 GHz で 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。

¹² 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 16：-A/-B ドメインの 5 GHz 帯域のリンク バジェット比較、(74 ページ) を参照してください。

表 16：-A/-B ドメインの 5 GHz 帯域のリンク バジェット比較

パラメータ	Cisco 1552 (-A ドメイン)	Cisco 1532 (-A ドメイン)	Cisco 1572 (-B ドメイン)
周波数帯域	5745 ~ 5825 MHz	5.280 ~ 5.320 GHz 5.500 ~ 5.560 GHz 5.680 ~ 5.700 GHz 5.745 ~ 5.825 GHz	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
エア インターフェイス	802.11a/n	802.11a/n	802.11a/n/ac
チャンネル帯域幅	20 MHz、40 MHz	20 MHz、40 MHz	20 MHz、40 MHz、80 MHz
Tx 空間ストリーム数	2	2	3
PHY データ レート	最大 300 Mbps	最大 300 Mbps	最大 1.3 Gbps
供給 Tx 電力	28 dBm、複合	27 dBm	30 dBm
Rx 感度	6 Mbps で -92 dBm 54 Mbps で -76 dBm 300 Mbps で -72 dBm	6 Mbps で -92 dBm 54 Mbps で -72 dBm 300 Mbps で -68 dBm	6 Mbps で -92 dBm 54 Mbps で -80 dBm 1300 Mbps で -60 dBm

5 GHz では、40 MHz チャンネルを形成する 20 MHz チャンネル 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、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、-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 17 : AP 間 RF リンク バジェット、5.8 GHz : 9 Mbps (-A ドメイン) , (75 ページ) 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 17 : 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
AP 間の範囲 (LOS、PLE = 2.3)	829 m (2722 フィート)	1120 m (3675 フィート)

9dB 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。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。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よって決める必要があります。

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 18：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）、(76 ページ) 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 18：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)	
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)	

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
	-90 dBm (クライアント)	-94 dBm (AP)	-90 dBm (クライアント)	-94 dBm (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、2.4GHz 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 18 : 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) , (76 ページ) より)
- 5 GHz バックホールの AP 間距離の 2 分の 1 (表 16 : -A/-B ドメインの 5 GHz 帯域のリンクバジェット比較, (74 ページ) 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 19 : 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, (77 ページ) を参照)。

表 19 : 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 20 : セル半径の推奨事項, (78 ページ) を参照)。

表 20: セル半径の推奨事項

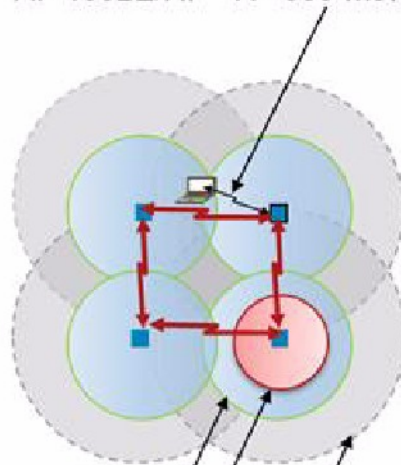
APタイプ (-A ドメイン)	AP からクライアント	AP 間
1552 C/I	250 m (800 フィート)	500 m (1600 フィート)
1552 E/H	300 m (1000 フィート)	600 m (2000 フィート)

図 27: 2.4 GHzでの AP/クライアント間のセル半径

AP-to-Client Cell Radius @ 2.4 GHz

AP 1552C/I: R= 250 meters

AP 1552E/H: R= 300 meters



- AP-Client Coverage 2.4 GHz
- AP-Client Coverage 5 GHz
- AP-AP Backhaul Coverage 5 GHz
 - AP-AP Distance $\geq 2x$ AP-Client Distance

331452

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 バジレットは、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 バジレットの比較 (-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 バジレット、5.6 GHz : 9 Mbps (-E ドメイン)

表 21: AP 間 RF リンク バジレット、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
Rx 感度	9 Mbps で -91 dBm	9 Mbps で -91 dBm
システム ゲイン	125 dB	127 dB

パラメータ	Cisco 1552 I/C	Cisco 1552 E/H
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 バジレット分析 (-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 バジレ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 バジレットでは、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 22: 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	
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)	

パラメータ	Cisco 1552 I/C		Cisco 1552 E/H		注
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 バジレ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 22 : 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) , (80 ページ) より)
- 5 GHz バックホールの AP 間距離の 2 分の 1 (表 21 : AP 間 RF リンク バジレット、5.6 GHz : 9 Mbps (-E ドメイン) , (79 ページ) 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 23 : 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, (81 ページ) を参照)。

表 23 : 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 24 : セル半径の推奨事項, (82 ページ) を参照)。

表 24: 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。

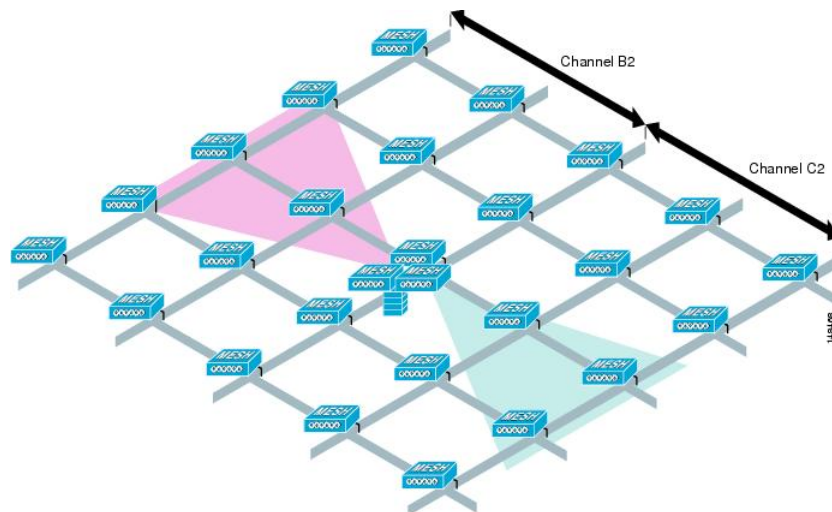
Cisco 範囲カルキュレータの前提条件

- 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ン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 28: 複数の RAP の PoP, (83 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、

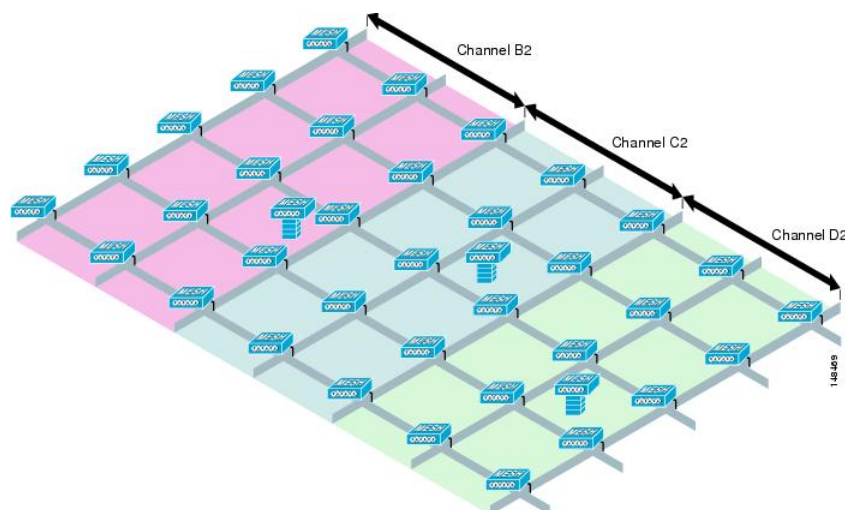
28：複数の RAP の PoP, (83 ページ) に示すように、RAP の有線ネットワークのロケーションが、複数のセルの RAP に対するホストの役割をする可能性があります。

図 28：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することができます。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定める必要があります。図 29：複数の RAP および MAP のセル, (83 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 29：複数の RAP および MAP のセル

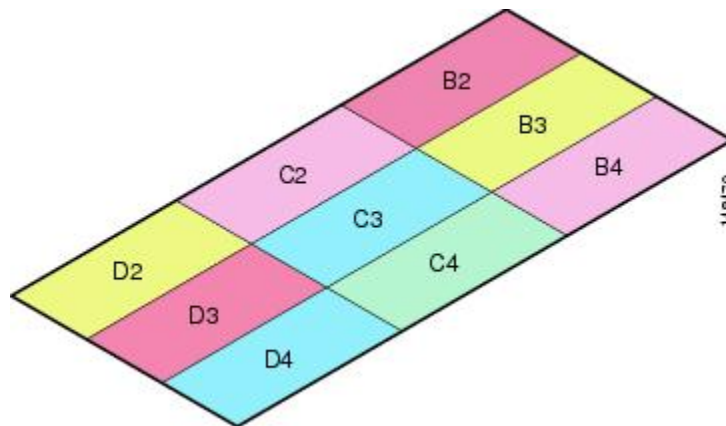


さまざまなチャネルを選択すると、より早いメッシュ コンバージェンスが犠牲になり、セル境界の共同チャネル干渉が減ります。MAP は seek モードにフォールバックして隣接セルのネイバーを検出する必要があります。高トラフィック密度のエリアで、共同チャネル干渉は、RAP の

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。

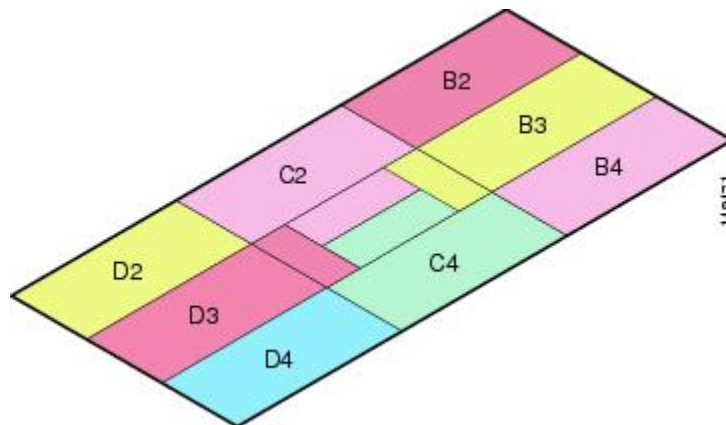
複数のセルをレイアウトするには、標準のWLAN計画に似たチャネル計画を使用し、チャネルのオーバーラップを回避してください（[図 30：さまざまなセルのレイアウト](#)、[\(84 ページ\)](#) を参照）。

図 30：さまざまなセルのレイアウト



メッシュがRAP接続のロスカバーするように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があります（[図 31：フェールオーバー カバレッジ](#)、[\(84 ページ\)](#) を参照）。

図 31：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、およびチャン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ンネル 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ンネル使用によって異なります。

隣接チャンネルでの AP1500 のコロケーション

コロケーションされた 2 つの AP1500 が、チャンネル 149 (5745 MHz) とチャンネル 152 (5765 MHz) のような隣接チャン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ンネル 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。

代替隣接チャンネルでの AP1500 のコロケーション

コロケーションされた 2 つの AP1500 が、チャンネル 149 (5745 MHz) とチャンネル 157 (5785 MHz) のような代替隣接チャン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ンネル 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ン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
 - 最小使用率のチャンネル（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 32: 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

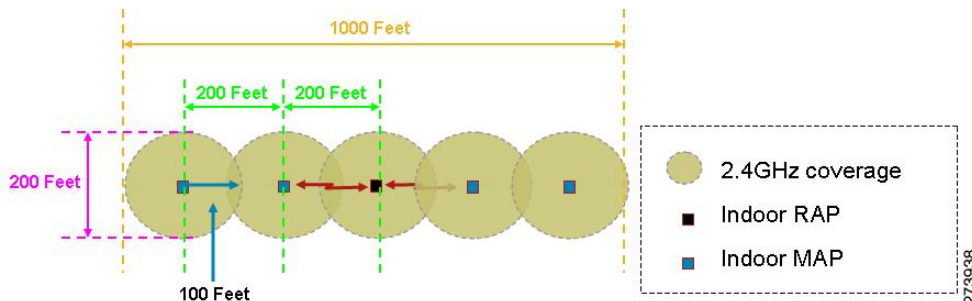
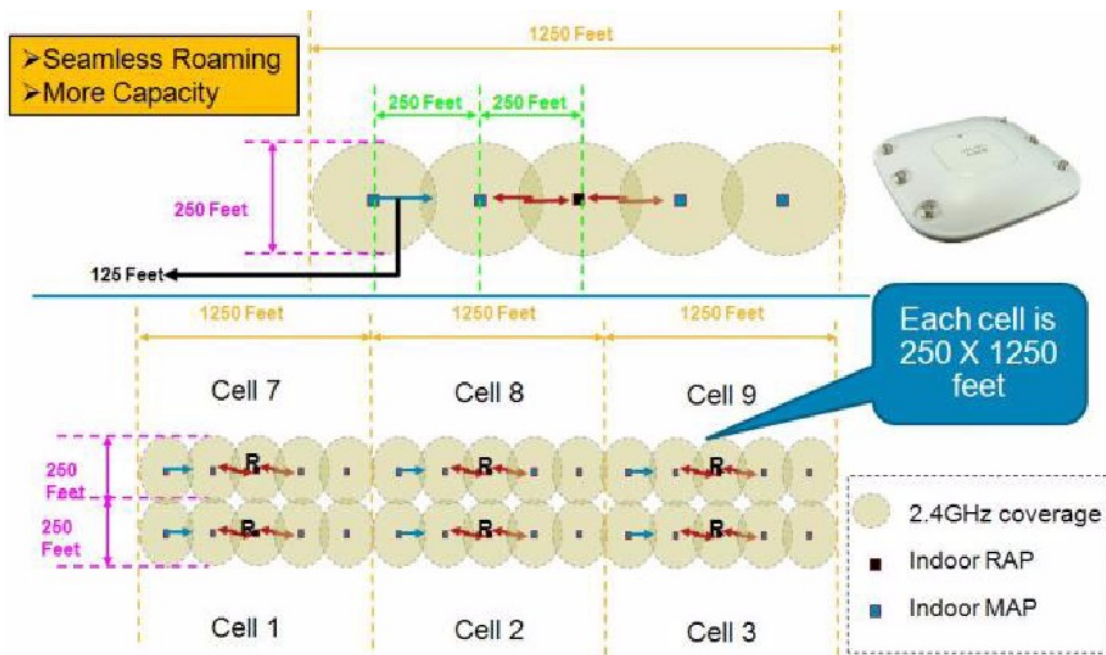


図 33: 屋内 11n メッシュネットワークにおける半径 125 フィート (38 m) のセルとアクセスポイントの位置



(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。

ワイヤレス伝搬の特性

表 25 : 2.4 GHz 帯域と 5 GHz 帯域の比較, (88 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ンネルが 3 つしかないため、共同チャン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 25 : 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 チャンネル	22 チャンネル (-A/-B の規制ドメイン)
共同チャンネル干渉の傾向がより強い	共同チャンネル干渉がない
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

1550/1570 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ンネルでトラフィック間のリ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 がいない場合は、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 つのチャン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、同じチャン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 がチャンネル選択を処理すると仮定すると、各チャン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認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（MMA） : 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、すべての帯域チャン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 チャン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ンネルをスキャンしますが、定期的にオフチャン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。

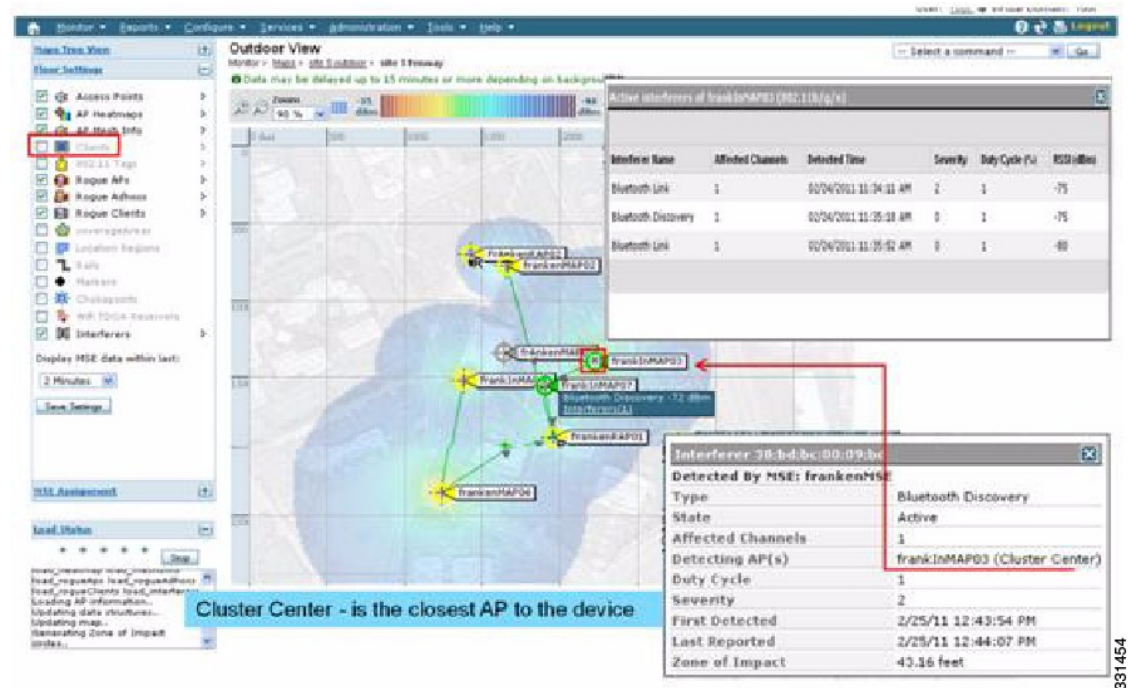
- センサーの密度
- 観測対象分類の品質
- 干渉源から AP までの RSSI
- AP での RF ネイバー リスト

したがって、メッシュ内の 2.4GHz 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 に転送されません。

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 34 : 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ン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、および複数のチャン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ンネルだけをサポートします。
- 帯域カバレッジは、そのチャン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 帯域内の同じチャンネルに少なくとも 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。アクティブなユーザチャン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ン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ンネルは 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、http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b4bdc1.shtmlを参照してください。

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 (IDR) というレポートが生成されますが、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 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 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ので、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ため、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、オペレーショナルに利点がありますが、その利点は、CAPWAP APへのリンクの速度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、同じチャンネルでRAPを使用するか (図 35 : 同じチャンネルでセルごとに2つのRAP, (96 ページ) を参照)、または別のチャンネルに置いたRAPを使用するか (図 36 : 別のチャンネルで

セルごとに2つのRAP, (96 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 35: 同じチャンネルでセルごとに2つのRAP

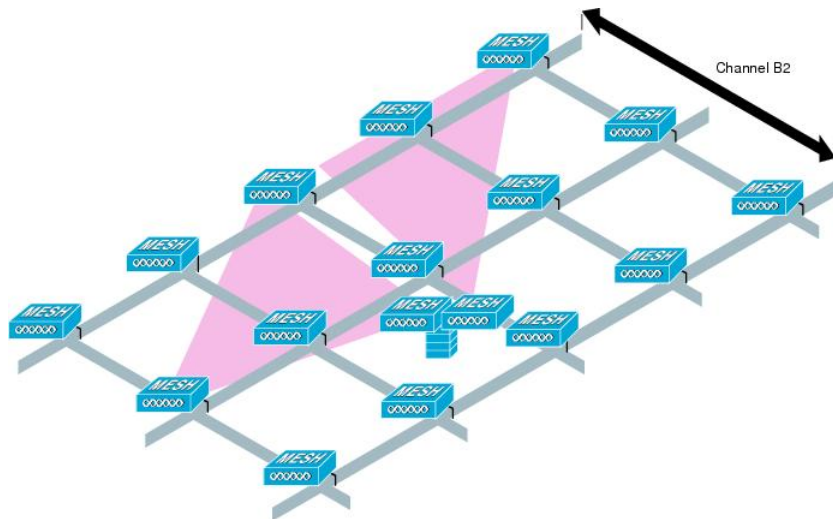
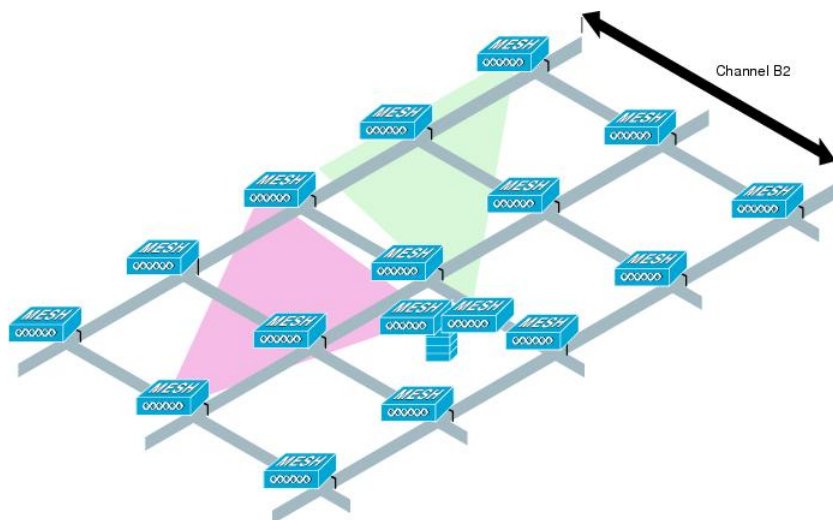


図 36: 別のチャンネルでセルごとに2つのRAP



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、同じチャンネルに追加の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32MAP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番目の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れないようにする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。



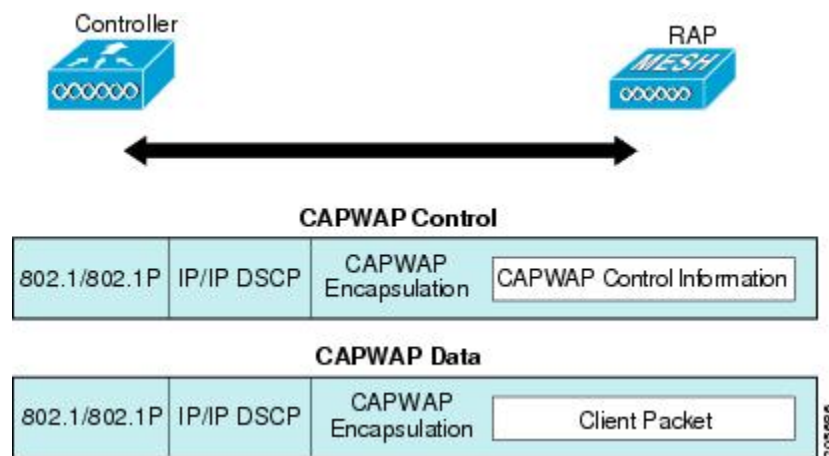
第 5 章

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 37: メッシュネットワークトラフィックの終端](#), (99 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 37: 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、「メッシュ ネットワークでのマルチキャストの有効化 (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](#), 100 ページ
- [リリース 8.2 でプロビジョニングするメッシュ PSK キー](#), 117 ページ
- [グローバル メッシュ パラメータの設定](#), 125 ページ
- [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](#), 132 ページ
- [バックホール クライアント アクセス](#), 137 ページ
- [ローカル メッシュ パラメータの設定](#), 139 ページ
- [アンテナ ゲインの設定](#), 150 ページ
- [動的チャネル割り当ての設定](#), 151 ページ
- [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](#), 154 ページ
- [拡張機能の設定](#), 154 ページ

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ンネルを設定します。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 チャンネル選択解除」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 チャンネルを設定します。「動的チャン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。



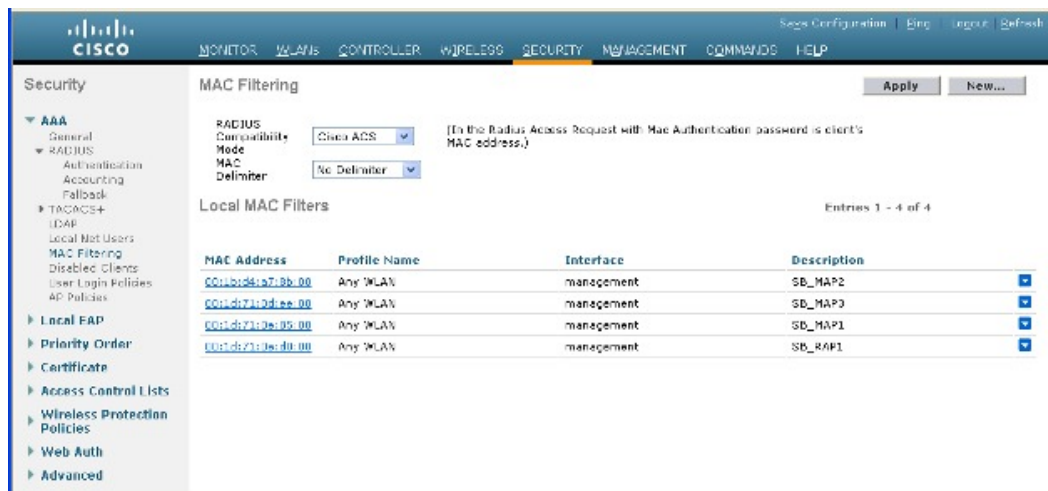
(注) メッシュ アクセス ポイントの MAC アドレスのリストは、ダウンロードして、Cisco Prime Infrastructure を使用してコントローラにプッシュすることもできます。

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 38 : [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。

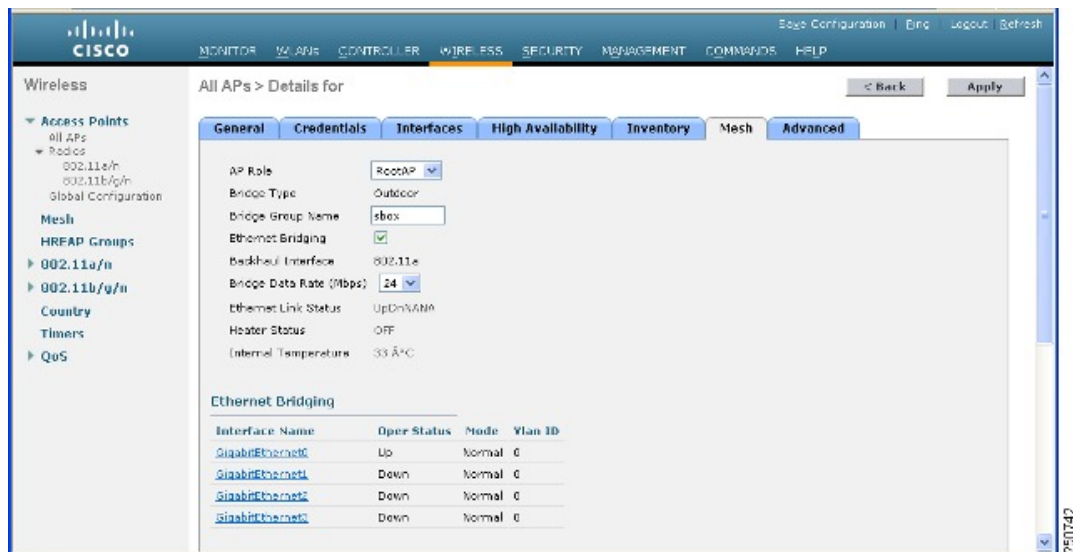
- MAP は常に、イーサネット ポートを、プライマリ バックホールとして設定し（イーサネット ポートが UP である場合）、802.11a/n 無線をセカンダリとして設定します。これによって、最初に、ネットワーク管理者がメッシュ アクセス ポイントを RAP として再設定する時間を取ることができます。ネットワークでのコンバージェンスを高速にするため、メッシュ ネットワークに参加するまではイーサネット デバイスを MAP に接続しないことをお勧めします。
- UP イーサネット ポートでコントローラへの接続に失敗した MAP は、802.11a/n 無線をプライマリ バックホールとして設定します。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 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。
- 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、 $2 \times 4 = 8 = 08$ (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 40 : [Global Configuration] ページ, (109 ページ) を参照)。

図 40 : [Global Configuration] ページ

The screenshot shows the Cisco GUI for Global Configuration. The left sidebar has a tree view with 'Wireless' expanded, showing 'Access Points' (All APs, Radios, Global Configuration), 'Mesh', 'HREAP Groups', '802.11a/n', '802.11b/g/n', 'Country', 'Timers', and 'QoS'. The main content area is titled 'Global Configuration' and includes an 'Apply' button. The configuration sections are:

- CDP**: CDP State is checked.
- Login Credentials**: Username is 'user', Password and Enable Password are masked with asterisks.
- 802.1x Supplicant Credentials**: 802.1x Authentication is unchecked.
- AP Failover Priority**: Global AP Failover Priority is set to 'Enable'.
- High Availability**:
 - Local Mode AP Fast Heartbeat Timer State: Enable
 - Local Mode AP Fast Heartbeat Timeout(1 to 10): 10
 - H-REAP Mode AP Fast Heartbeat Timer State: Disable
 - AP Primary Discovery Timeout(30 to 3600): 120
 - Back-up Primary Controller IP Address: 209.165.200.225
 - Back-up Primary Controller name: controller1
 - Back-up Secondary Controller IP Address: 0.0.0.0
 - Back-up Secondary Controller name: (empty)

(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。
- [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
 - 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。
 - [High Availability] タブをクリックします。
 - 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る必要があります。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。
- 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。
 - 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。
 - [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。
 - [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)

コントローラの CLI 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** 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-basecontroller_nameCisco_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る必要があります。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-basecontroller\_nameCisco\_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-basecontroller\_nameCisco\_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 primarybackup\_controller\_namebackup\_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 secondarybackup\_controller\_namebackup\_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-timeoutinterval**  
*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-timeoutinterval**  
*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-timeoutinterval**  
*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 generalCisco\_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 サーバのユーザー 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。

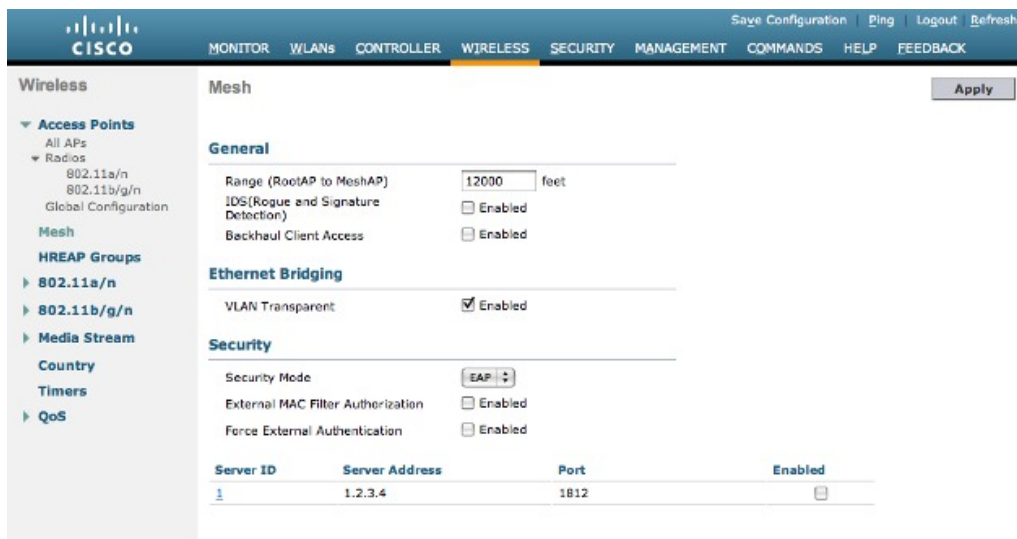
- [http://www.cisco.com/en/US/products/sw/secursw/ps2086/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html) (Windows)
- <http://www.cisco.com/en/US/products/sw/secursw/ps4911/> (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 41 : [Mesh] ページ、（115 ページ）を参照）。

図 41 : [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。

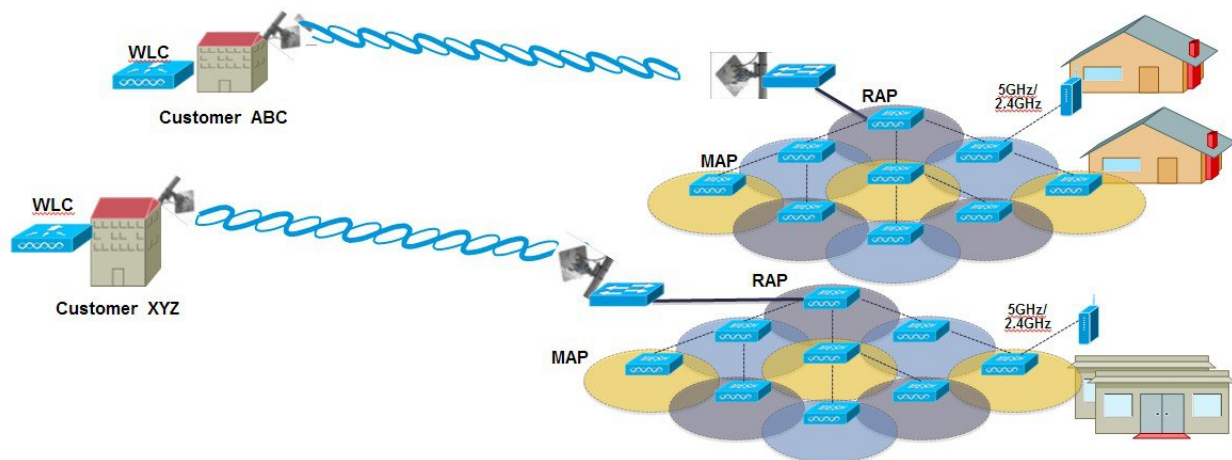
```
show mesh security-stats Cisco_AP
```

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 packets 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ヤードカードの 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。

### SP Mesh Adjacent Network Architecture that can create MAP hijacking



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。

| AP Name                          | IP Address(Ipv4/Ipv6) | AP Model           | AP MAC            | AP Up Time          |
|----------------------------------|-----------------------|--------------------|-------------------|---------------------|
| <a href="#">AP80AA.7792.7868</a> | 10.70.0.230           | AIR-AP1832I-UXX9   | b0:aa:77:92:78:68 | 1 d, 04 h 11 m 51 s |
| <a href="#">AP6c20.560e.1a26</a> | 10.71.0.54            | AIR-CAP1602E-A-K9  | 6c:20:56:0e:1a:26 | 1 d, 04 h 07 m 08 s |
| <a href="#">AP1572-7a7f-09c0</a> | 10.70.0.252           | AIR-AP1572EAC-A-K9 | 1c:6a:7a:7f:09:c0 | 1 d, 04 h 07 m 15 s |
| <a href="#">AP7cad.74ff.d22e</a> | 10.70.0.254           | AIR-CAP3702I-A-K9  | 7c:ad:74:ff:d2:2e | 1 d, 03 h 59 m 30 s |
| <a href="#">APa44c.11f0.ea9d</a> | 10.70.0.252           | AIR-CAP3602I-A-K9  | a4:4c:11:f0:ea:9d | 1 d, 03 h 52 m 20 s |
| <a href="#">AP7cad.74ff.d0e6</a> | 10.70.0.254           | AIR-CAP3702I-A-K9  | 7c:ad:74:ff:d0:e6 | 1 d, 03 h 56 m 55 s |
| <a href="#">AP1532-3546-f14c</a> | 10.70.0.252           | AIR-CAP1532E-A-K9  | 4c:4e:35:46:f1:4c | 0 d, 02 h 10 m 49 s |
| <a href="#">AP1532-3546-f678</a> | 10.70.0.252           | AIR-CAP1532E-A-K9  | 4c:4e:35:46:f6:78 | 0 d, 01 h 51 m 07 s |

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。

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - LDAP
    - Local Net Users
    - MAC Filtering
    - Disabled Clients
    - User Login Policies
    - AP Policies**
    - Password Policies
  - Local EAP
  - Advanced EAP
  - Priority Order
  - Certificate
  - Access Control Lists
  - Wireless Protection Policies
  - Web Auth
  - TrustSec SXP

**AP Policies**

**Policy Configuration**

- Accept Self Signed Certificate (SSC)
- Accept Manufactured Installed Certificate (MIC)
- Accept Local Significant Certificate (LSC)
- Authorize MIC APs against auth-list or AAA
- Authorize LSC APs against auth-list

**AP Authorization List**

Search by MAC

| MAC Address       | Certificate Type | SHA1 K |
|-------------------|------------------|--------|
| 1c:6a:7a:7f:09:c0 | MIC              |        |
| 4c:4e:35:46:f0:88 | MIC              |        |
| 4c:4e:35:46:f1:00 | MIC              |        |
| 4c:4e:35:46:f1:4c | MIC              |        |
| 4c:4e:35:46:f6:78 | MIC              |        |
| 4c:4e:35:46:f6:98 | MIC              |        |

**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。

**Security**

Security Mode

PSK Provisioning  Enabled

Default PSK  Enabled

**ADD New Provisioning Key**

Provisioning Key

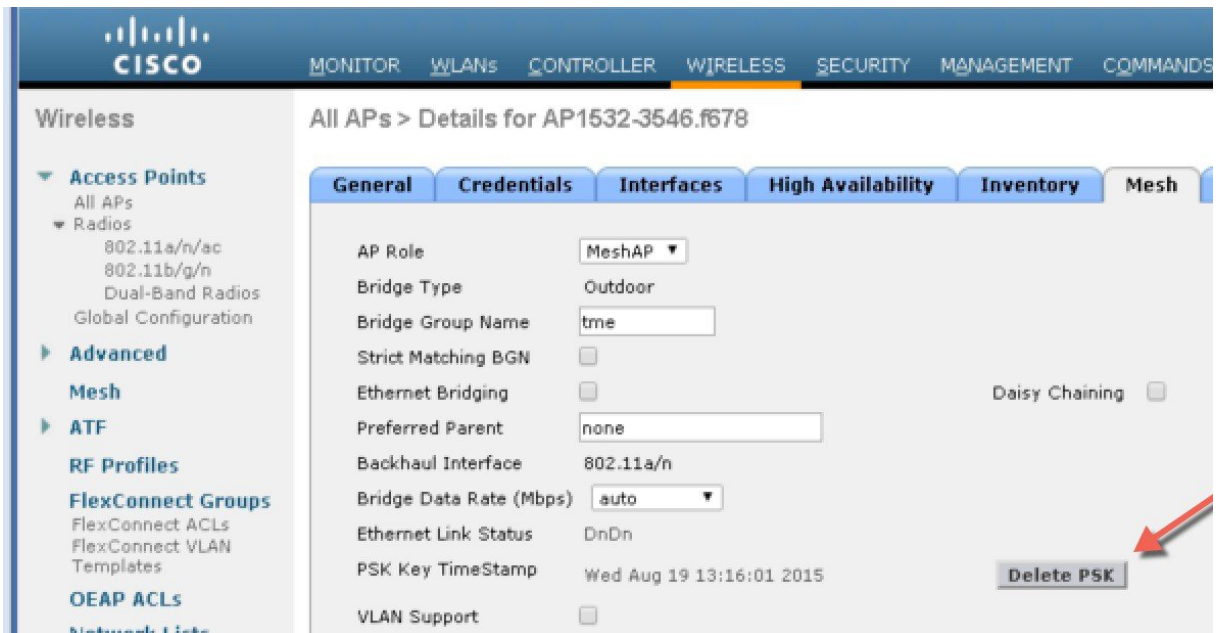
Description

| Key Index | TimeStamp                | Description |
|-----------|--------------------------|-------------|
| 1         | Fri Nov 13 09:11:49 2015 | Mike123     |
| 2         | Fri Nov 13 09:11:03 2015 | Cisco123    |

- 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。

The screenshot shows the Cisco Wireless configuration page for a specific AP. The breadcrumb navigation at the top is "All APs > Details for AP1532-3546.f678". The left sidebar contains a tree view with categories like "Access Points", "Radios", "Advanced", "Mesh", "ATF", "RF Profiles", "FlexConnect Groups", "OEAP ACLs", "Network Lists", "802.11a/n/ac", "802.11b/g/n", "Media Stream", "Application Visibility And Control", and "Lync Server". The main content area has tabs for "General", "Credentials", "Interfaces", "High Availability", "Inventory", and "Mesh". The "Mesh" tab is active, showing configuration fields for "AP Role" (MeshAP), "Bridge Type" (Outdoor), "Bridge Group Name" (tme), "Strict Matching BGN" (checkbox), "Ethernet Bridging" (checkbox), "Daisy Chaining" (checkbox), "Preferred Parent" (none), "Backhaul Interface" (802.11a/n), "Bridge Data Rate (Mbps)" (auto), "Ethernet Link Status" (DnDn), "PSK Key TimeStamp" (Wed Aug 19 13:16:01 2015), and "VLAN Support" (checkbox). A red arrow points to a "Delete PSK" button next to the PSK Key TimeStamp. Below these fields is the "Mesh RAP Downlink Backhaul" section, which includes "RAP Downlink Backhaul" with radio buttons for "5 GHz" (selected) and "2.4 GHz", and an "Enable" button.

**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。

The screenshot shows the Cisco Wireless Management interface. The left sidebar has 'Mesh' highlighted under 'Advanced'. The main content area is titled 'Security' and includes the following settings:

- Ethernet Bridging:** VLAN Transparent  Enabled
- Security Mode:** PSK
- PSK Provisioning:**  Enabled
- Default PSK:**  Enabled

Below these settings is the 'ADD New Provisioning Key' section with input fields for 'Provisioning Key' and 'Description', and an 'ADD' button.

| Key Index | TimeStamp                | Description |
|-----------|--------------------------|-------------|
| 1         | Tue Nov 17 17:16:08 2015 | Mesh123     |
| 2         | Fri Nov 13 09:11:49 2015 | Mike123     |
| 3         | Fri Nov 13 09:11:03 2015 | Cisco123    |

Additional security options include:

- External MAC Filter Authorization  Enabled
- Force External Authentication  Enabled
- LSC Only MAP Authentication  Enabled

At the bottom, there is a 'Foot Notes' section with the text: *1 Mesh DCA channels are only applicable for serial backhaul APs*

(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 26: 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)            | <p>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。</p> <p>範囲: 150 ~ 132,000 フィート</p> <p>デフォルト: 12,000 フィート</p> <p>(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。</p>                                    |
| IDS (Rogue and Signature Detection) | <p>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。</p> <p>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。</p> <p>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。</p> <p><b>config mesh ids-state {enable   disable}</b></p> <p>(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。</p> |

| パラメータ                  | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backhaul Client Access | <p>(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。</p> <p>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。</p> <p><b>デフォルト：無効</b></p> <p>(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。</p>                                                                                                                                                                                                                                                                                                                                                                      |
| VLAN Transparent       | <p>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。</p> <p>(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。</p> <p>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。</p> <p>(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。</p> <p>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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p><b>デフォルト：イネーブル</b></p> |

| パラメータ         | 説明                                                                                                                                                                                                                                                                                                                                                   |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Mode | <p>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。</p> <p>(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。</p> <p>(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。</p> <p>オプション: PSK または EAP</p> <p>デフォルト: EAP</p> |



| パラメータ                             | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External MAC Filter Authorization | <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• コントローラも、RADIUS サーバで設定する必要があります。</li> <li>• 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。 <ul style="list-style-type: none"> <li>◦ 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。</li> <li>◦ 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、<i>platform_name_string</i>-イーサネット MAC アドレスであり、たとえば <i>c1520-001122334455</i> のようになります。</li> </ul> </li> <li>• 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。</li> </ul> <p>(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。</p> <p>デフォルト：無効</p> |
| Force External Authorization      | <p>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。</p> <p>デフォルト：無効</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

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 レポートのステータスが有効か無効かを示します。

```
(Cisco Controller)> show mesh ids-state
```

```
Outdoor Mesh IDS (Rogue/Signature Detect): .... Disabled
```

- **show mesh config** : グローバル構成の設定を表示します。

```
(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

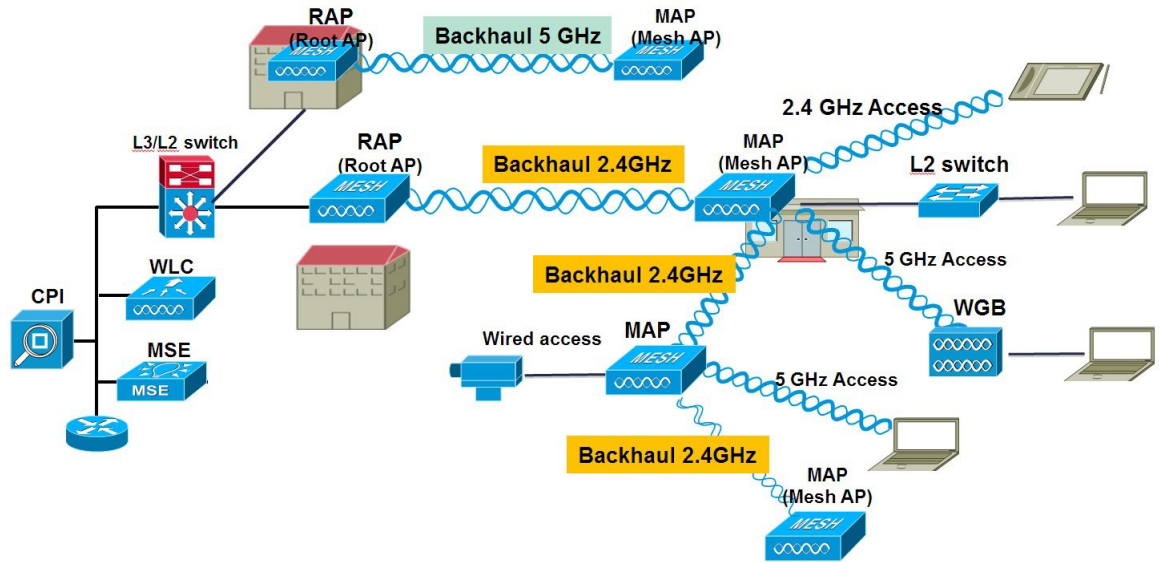
リリース 8.2 以前のワイヤレス メッシュ バックホールは 5 GHz でのみサポートされていました。リリース 8.2 ではワイヤレス メッシュ バックホールは、5 GHz および 2.4 GHz でサポートされません。

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。チャン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、この場合チャン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。

The screenshot displays the Cisco Wireless Mesh configuration interface. On the left, a navigation menu lists various wireless settings. The main content area is titled 'Mesh' and is divided into 'General' and 'Mesh RAP Downlink Backhaul' sections. In the 'General' section, the 'Range (RootAP to MeshAP)' is set to 12000 feet. Several checkboxes are present, with 'Backhaul Client Access' and 'Mesh Backhaul RRM' checked. The 'Mesh RAP Downlink Backhaul' section features two radio buttons: '5 GHz' and '2.4 GHz'. The '2.4 GHz' option is selected, and a red arrow points to it. Below the radio buttons is an 'Enable' button.

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 でチャンネルを 2.4 GHz に変更する必要があり、チャン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。

AP Name	Radio Slot#	Base Radio MAC	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Power Level	Antenna
AP80AA.7792.7868	0	b0:aa:77:92:52	Enable	UP	1 *	NA	NA	8 *	Internal
AP6c20.560a.1a26	0	34:a8:14e:ba:02	Enable	UP	6 *	Disable	DOWN	6 *	External
AP7cad.74ff.d22e	0	08:ccc:68:ccc:b8:17	Enable	UP	6 *	Enable	UP	8 *	Internal
AP7cad.74ff.d0e6	0	08:ccc:68:ccc:b3:c0	Enable	UP	1 *	Enable	UP	8 *	Internal
APa44c.11f0.ea9d	0	f4:7f:35:d8:43:ff	Enable	UP	11 *	Enable	UP	8 *	Internal
AP1572-7a7f.09c0	0	1c:6a:7a:7f:1e:d0	Enable	UP	11	Enable	UP	7 *	External
AP1932-3546.f678	0	20:bb:c0:72:1a:93	Enable	UP	11	NA	NA	1	External
AP1932-3546.f14c	0	20:bb:c0:72:1a:1f	Enable	UP	11	NA	NA	4	External

チャンネルがカスタム オプションで選択された後、そのチャンネルは 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 からの同じチャンネルだけを継承しそれに固定されます。

RF Backhaul Channel Assignment

Current Channel: 11

Channel Width: 20 MHz

Assignment Method: Global Custom (11)

Note: Only Channels 1, 6 and 11 are nonoverlapping

Tx Power Level Assignment

Current Tx Power Level: 7

Assignment Method: Global Custom

Performance Profile

View and edit Performance Profile for this AP

Performance Profile

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

次の例に示すように、RAP でチャンネル変更後は、MAP のチャンネルが 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ンネルを変更しようとする、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 からチャン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。

The screenshot shows the Cisco WMC interface for AP1532-3546.f678. The 'Mesh' tab is active, and a dialog box is shown with the following text:

This configuration is only supported for Root APs
 Prevent this page from creating additional dialogs
 OK

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、デジ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をリポートするよう求められます。

図 42: 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

The screenshot shows the Cisco GUI configuration for a Mesh AP. The 'Wireless' tab is active, and the 'Mesh' configuration page is displayed. The 'General' section includes the following settings:

- Range (RootAP to MeshAP): 12000 feet
- IDS (Rogue and Signature Detection): Enabled
- Backhaul Client Access: Enabled
- Extended Backhaul Client Access: Disabled
- Mesh DCA Channels: Enabled
- Global Public Safety: Disabled

The 'Ethernet Bridging' section shows:

- VLAN Transparent: Enabled

The 'Security' section shows:

- Security Mode: EAP
- External MAC Filter Authorization: Disabled
- Force External Authentication: Disabled

A table for 'Server ID' is visible at the bottom, with columns for 'Server ID', 'Server Address', 'Port', and 'Enabled'. A note at the bottom states: 'Mesh DCA channels are only applicable for serial backhaul APs'.

331459

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せん。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。

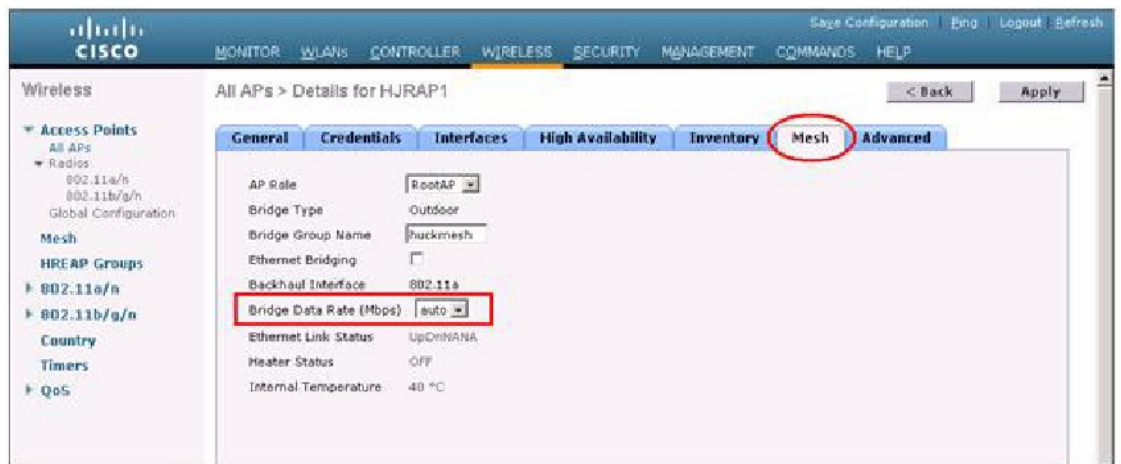
メッシュ バックホールを「Auto」に設定することをお勧めします。

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に影響を受けます）、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 43: 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
```

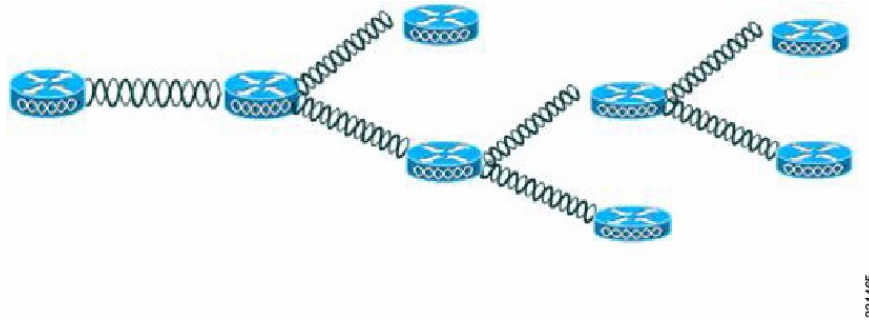
AP Name/Radio	Channel	Rate	Link-Snr	Flags	State
00:0B:85:5C:B9:20	0	auto	4	0x10e8fcb8	BEACON
00:0B:85:5F:FF:60	0	auto	4	0x10e8fcb8	BEACON DEFAULT
00:0B:85:62:1E:00	165	auto	4	0x10e8fcb8	BEACON
00:0B:85:70:8C:A0	0	auto	1	0x10e8fcb8	BEACON
HPMAP1	165	54	40	0x36	CHILD BEACON
HJMAP2	0	auto	4	0x10e8fcb8	BEACON

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 44: AP1552 バックホール スループット



831465

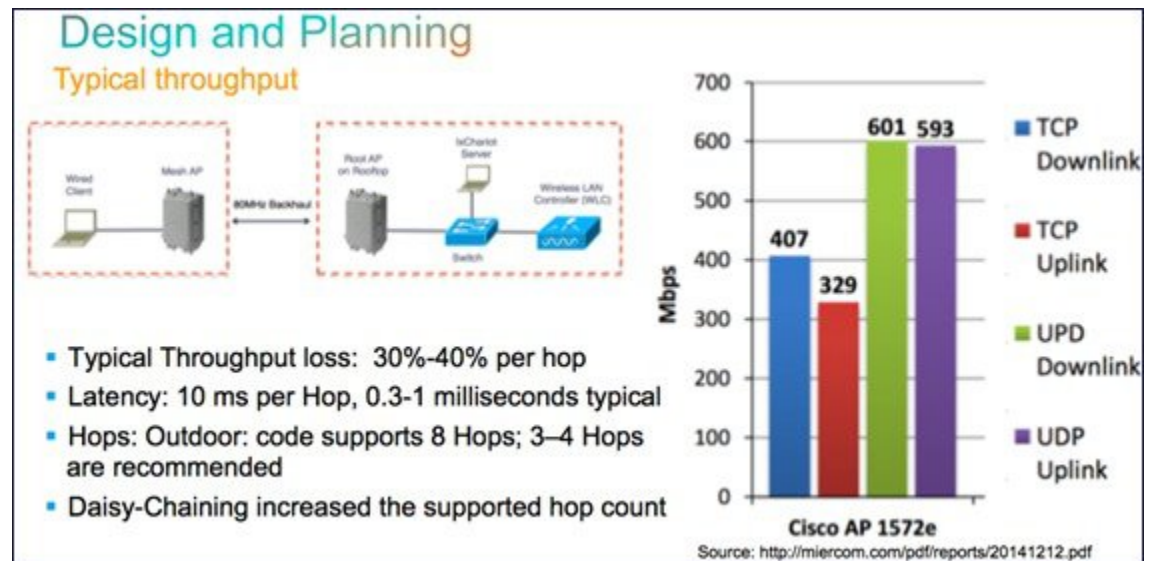
表 27: AP1552 バックホール キャパシティ

ホップ	RAP	1	2	3	4
最大スループット (20MHz BH)	112 Mbps	83 Mbps	41 Mbps	25 Mbps	15 Mbps
最大スループット (40MHz 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。

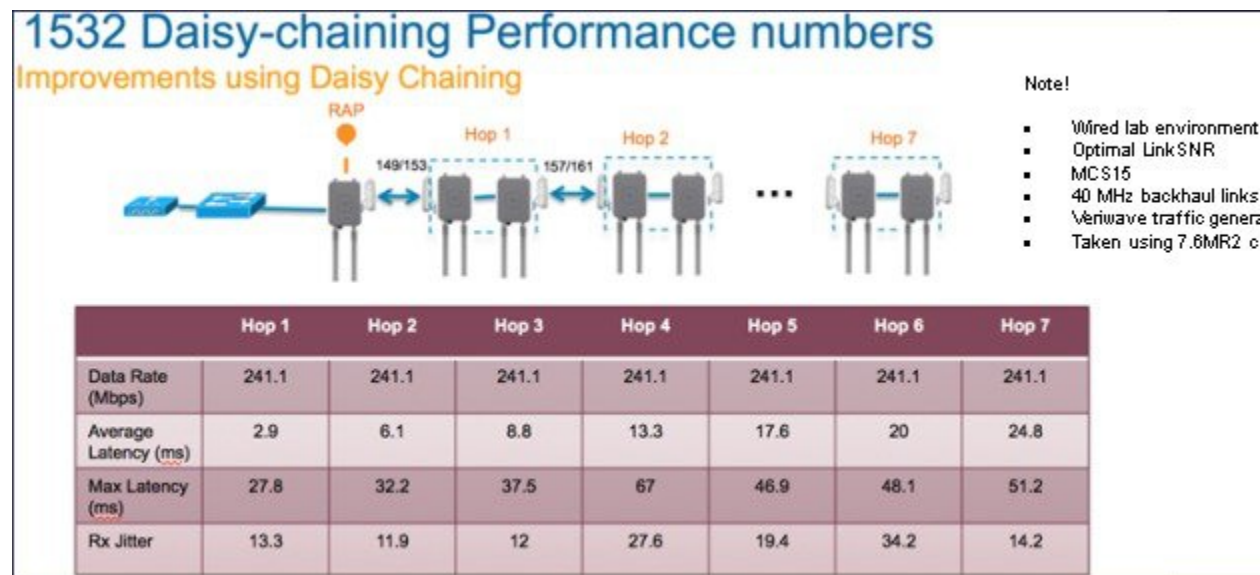
- パケットサイズは 1370 バイト (Veriwave クライアント)
- 5 GHz 802.11n
- MCS 15
- パケット損失は 1%未満
- クライアント アクセスおよびバックホール用の SNR が 40 dB を超える
- UDP トラフィック、セキュリティ有効、およびユニバーサル アクセス有効

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。

デージーチェーンを使用した 1532 バックホール容量



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)
[ControlandProvisioningofWirelessAccessPointsCAPWAP]
- 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。

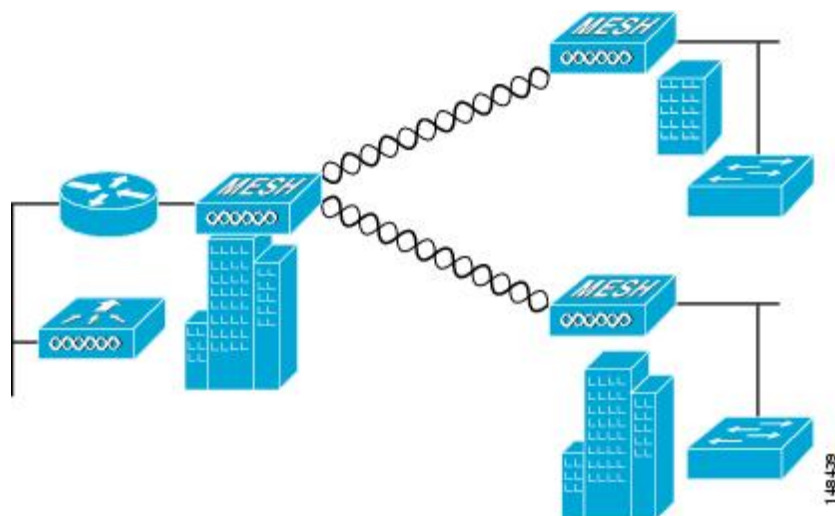
- 1 メッシュ ノードをブリッジとして使用する場合 (図 45: ポイントツーマルチポイントブリッジング, (144 ページ) を参照)。



(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 45: ポイントツーマルチポイントブリッジング

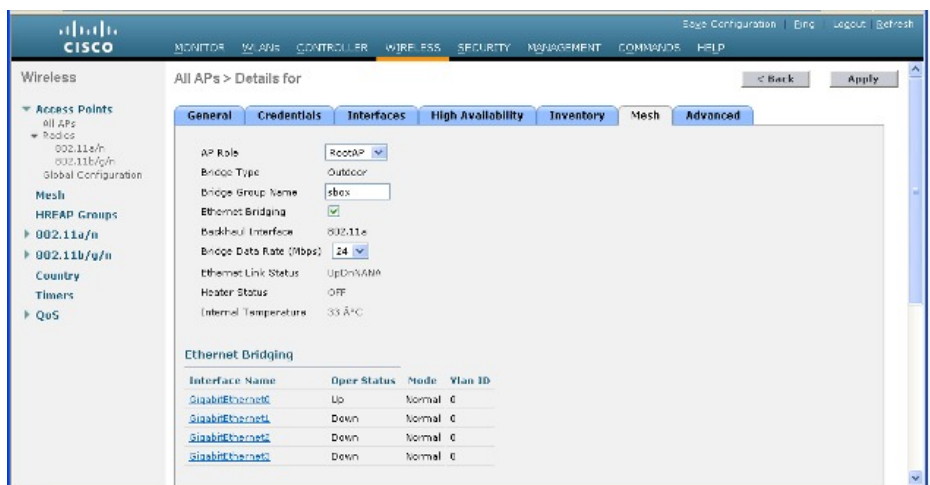


イーサネットブリッジングの有効化 (GUI)

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 46 : [All APs > Details for] ([Mesh]) ページ, (145 ページ) を参照してください)。

図 46 : [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、Hop2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。

General	Credentials	Interfaces	High Availability	Inventory	Mesh	AP
AP Role	RootAP					
Bridge Type	Outdoor					
Bridge Group Name						
Strict Matching BGN	<input type="checkbox"/>					
Ethernet Bridging	<input checked="" type="checkbox"/>				Daisy Chaining	<input type="checkbox"/>
Preferred Parent	none					
Backhaul Interface	802.11a					
Bridge Data Rate (Mbps)	auto					
Ethernet Link Status	DnDnDnNANA					
VLAN Support	<input checked="" type="checkbox"/>					
Native VLAN ID	161					

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ことで、同じチャンネルにある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、別々のチャンネルで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 チャンネル (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 28 : メッシュ アクセス ポイントと Cisco 3200 の相互運用性](#)、(148 ページ) を参照してください。

表 28 : 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
1522、1522 ¹³	c3201 ¹⁴ 、c3202 ¹⁵ 、c3205 ¹⁶
1524PS	c3201、c3202
1524SB、1130、1240、屋内 802.11n メッシュ アクセス ポイント	c3201、c3205

¹³ 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。

¹⁴ モデル c3201 は 802.11b/g 無線を搭載した Cisco 3200 (2.4 GHz) です。

¹⁵ モデル c3202 は 4 ~ 9 GHz サブバンド無線を搭載した Cisco 3200 です。

¹⁶ 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せん。

- 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** 無線のチャン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** 電力およびチャン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、チャン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。
- [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。
 - [802.11a (または 802.11b/g) Network Status] チェックボックスを選択解除します。
 - [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 29 : 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ンネル帯域幅を指定します。

- [20 MHz] : 20 MHz のチャンネル帯域幅 (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 チャン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 チャン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ン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ンネルパラメータの設定も表示されます。
- [Channel Assignment Leader] : チャン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 が現在のチャン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ンネルが表示されます。チャンネルを選択するには、[Select] カラムでそのチャンネルのチェックボックスをオンにします。チャンネルを除外するには、チャン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 チャンネル (100, 104, 108, 112, 116, 132, 136, および 140) は、チャン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 チャンネルリストにこれらのチャン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、これらのチャンネルが DCA チャンネルリストに含まれていることを確認します。チャンネルリストにこれらのチャンネルを含めるには、[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 チャンネルが動作する 802.11a 帯域で 4.9 GHz チャン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 チャン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。チャンネルを除外するには、チャン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ン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、チャンネルが変更された無線の MAC アドレス、前のチャンネルと新規のチャンネル、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 無線の動的チャン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)、動的チャンネル割り当て (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>` : 動的チャン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

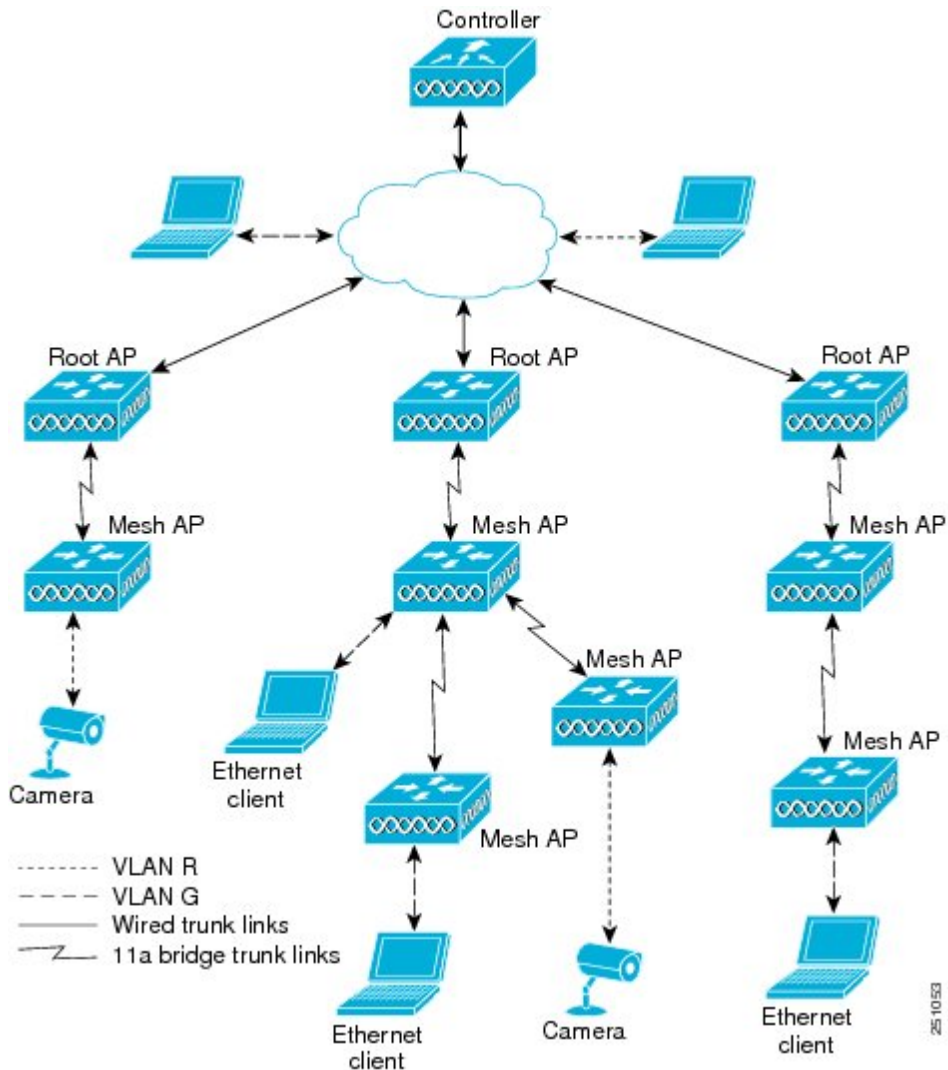
イーサネット VLAN タギングの設定

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 47: 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] オプションを選択解除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す。
 - (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
```

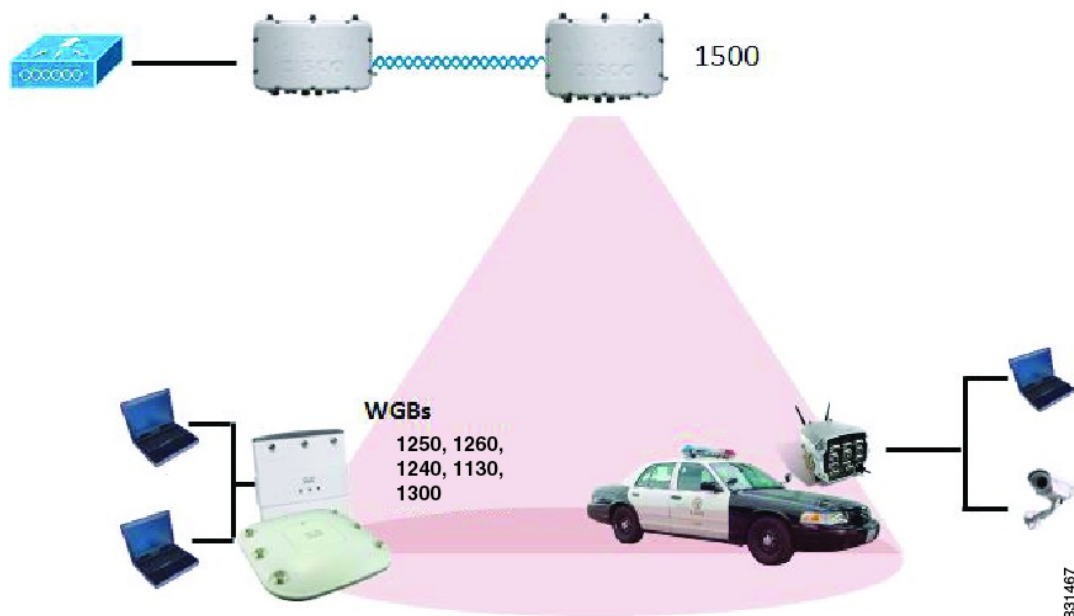
ワークグループブリッジとメッシュ インフラストラクチャとの相互運用性

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 48 : 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](https://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 49 : WGB の WPA セキュリティ設定

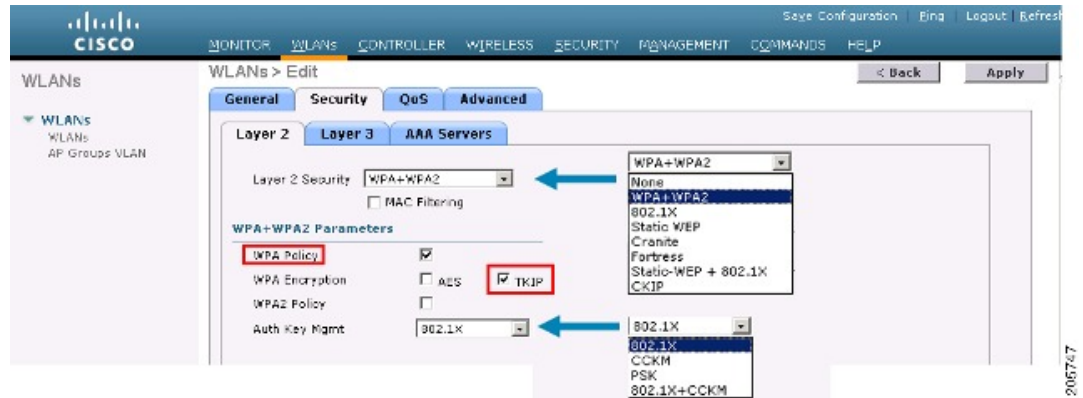
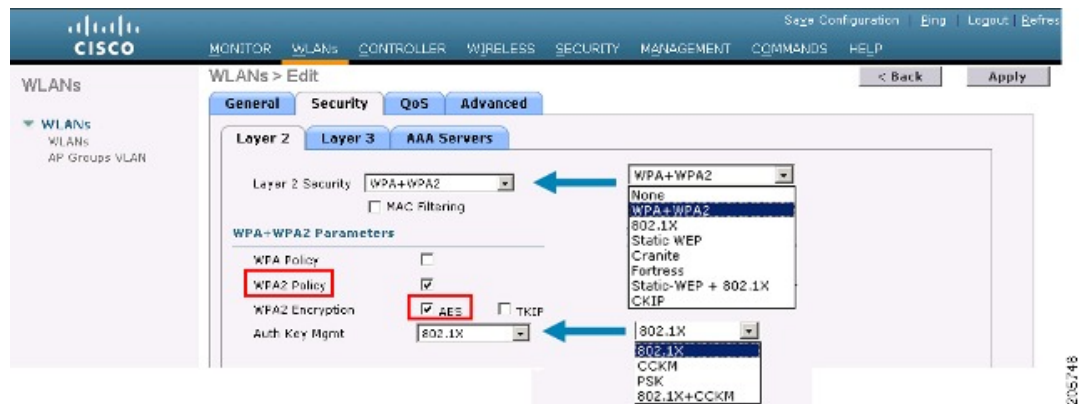


図 50 : WGB の WPA-2 セキュリティ設定



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 51: クライアントが *WGB* であると認識されている

The screenshot shows the Cisco WLC Monitor > Clients page. The table lists clients with columns for Client MAC Addr, AP Name, WLAN Profile, Protocol, Status, Auth, Port, and WGB. The WGB column has a dropdown arrow for each row, indicating the client type.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:3a:2f:57:36	EkyRep.70:7b:a0	WLANS	802.11g	Associated	Yes	29	Yes
00:06:90:fe:00:9a	EkyRep.70:7b:a0	WLANS	802.11b	Associated	Yes	29	No
00:13:80:d9:9a:0f	RAP001b.2e26.f992-1130	Unknown	802.11a	Prebing	No	29	No
00:15:5d:44:25:0d	RAP001a.1449.1400Plus	WLANS	802.11a	Associated	Yes	29	No
00:16:36:5f:4b:74	MAP2-001c.1448.ec0c-3f	WLANS	802.11a	Associated	Yes	29	No

- 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 52 : [Monitor] > [Clients] > [Detail] ページ（無線 WGB クライアントの場合）、（167 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 53 : [Monitor] > [Clients] > [Detail] ページ (有線 WGB クライアントの場合) , (167 ページ) のようなページが表示されます。

図 52 : [Monitor] > [Clients] > [Detail] ページ (無線 WGB クライアントの場合)

Client Properties		AP Properties	
MAC Address	00:1b:63:ad:a7:0f	AP Address	00:1e:14:40:ec:00
IP Address	200.165.200.236	AP Name	MAP2-001e.1448.ec00Hr
Client Type	WGB Client	AP Type	802.11s
WGB MAC Address	00:1d:45:b5:74:44	WLAN Profile	WLAN5
User Name		Status	Associated
Port Number	29	Association ID	0
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCX Version	Not Supported	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0
		WEP State	WEP Disable

図 53 : [Monitor] > [Clients] > [Detail] ページ (有線 WGB クライアントの場合)

Client Properties		AP Properties	
MAC Address	00:05:9e:3f:57:06	AP Address	00:0b:05:70:7b:40
IP Address	70.1.0.54	AP Name	SkyRap:70:7b:40
Client Type	WGB	AP Type	802.11g
Number of Wired Client(s)	1	WLAN Profile	WLAN5
User Name		Status	Associated
Port Number	29	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCX Version	CCXv5	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0
		WEP State	WEP Enable

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要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。

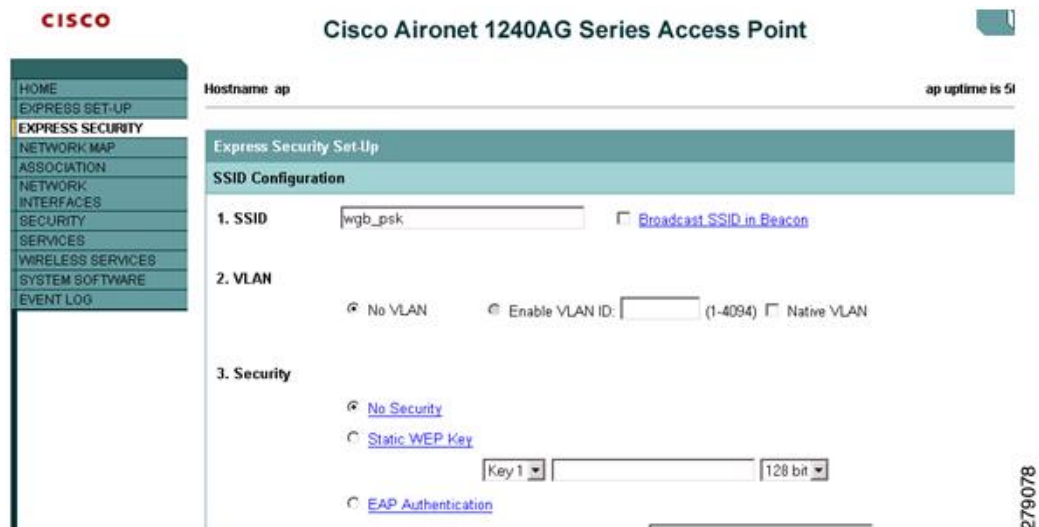
- SSID を無線インターフェイスにマッピングし、無線インターフェイスの役割を定義します。

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) #infrastructure-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 54 : [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 Dot11Radiol:

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 55 : 更新された WGB クライアント

The screenshot shows the Cisco WLC Monitor Clients page. The table lists three clients, all with WGB status set to 'Yes'. Arrows point to the 'wgb' column header and the 'wgb wireless client' label below the table.

Client MAC Addr	AP Name	WLAN Profile	WLAN SSID	Protocol	Status
00:15:63:eb:b3:cc	AP_1240	wgb_psk	wgb_psk	802.11a	Associa
00:40:96:a8:c5:72	AP_1240	wgb_wpa2	wgb_wpa2	802.11a	Associa
00:40:96:ad:67:3b	AP_1240	wgb_psk	wgb_psk	N/A	Associa

図 56 : 更新された WGB クライアント

The screenshot shows the Cisco WLC Monitor Clients page with a search filter. The table lists three clients, all with WGB status set to 'Yes'. A red box highlights the 'WGB' column header.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:9a:3f:57:36	SkyRap:70:7b:a0	WLANS	802.11g	Associated	Yes	29	Yes
00:04:60:fe:00:94	SkyRap:70:7b:a0	WLANS	802.11b	Associated	Yes	29	No

図 57 : 更新された WGB クライアント

The screenshot shows the Cisco WLC Monitor Clients page with detailed client properties. The 'Client Type' is highlighted in red, and the 'Link Text' button is circled in blue.

Client Properties		AP Properties	
MAC Address	00:05:9a:3f:57:36	AP Address	00:0b:85:70:7b:a0
IP Address	70.1.0.54	AP Name	SkyRap:70:7b:a0
Client Type	WGB	AP Type	802.11g
Number of Wired Client(s)	1	WLAN Profile	WLANS
User Name		Status	Associated
Port Number	29	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCX Version	CCXv5	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager State	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0
		WEP State	WEP Enable

リンク テストの結果

図 58: 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	0	0		
Receive count	2	3	0	0	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、チャンネル、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 での限定チャンネル スキャンの設定：鉄道などのモバイル環境では、WGB はすべてのチャンネルをスキャンする代わりに、限定チャン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時にハンドオフによる遅延が減少します。チャンネル数を制限することにより、WGB は必要なチャン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。この限定チャンネル 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、すべてのチャンネルまたは指定されたチャンネルに対するスキャンが実行されます。設定できるチャンネルの最大数に制限はありません。設定できるチャンネルの最大数

は、無線がサポートできるチャンネル数に制限されます。実行時に、WGBはこの限定チャンネルセットのみをスキャンします。この限定チャンネルの機能は、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ンネルリストにも影響します。チャンネルは、チャンネルが限定チャンネルセットに含まれる場合にのみ、既知のチャン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、すべてのチャン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を超えていないことを確認します。

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

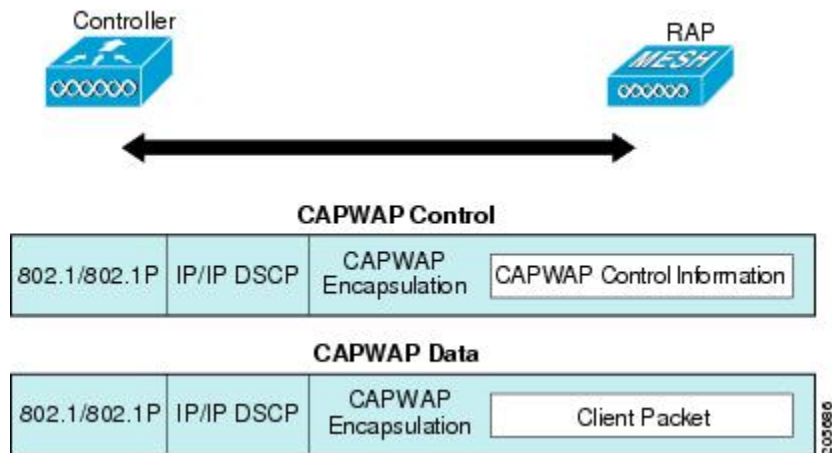
カプセル化

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 59: カプセル化

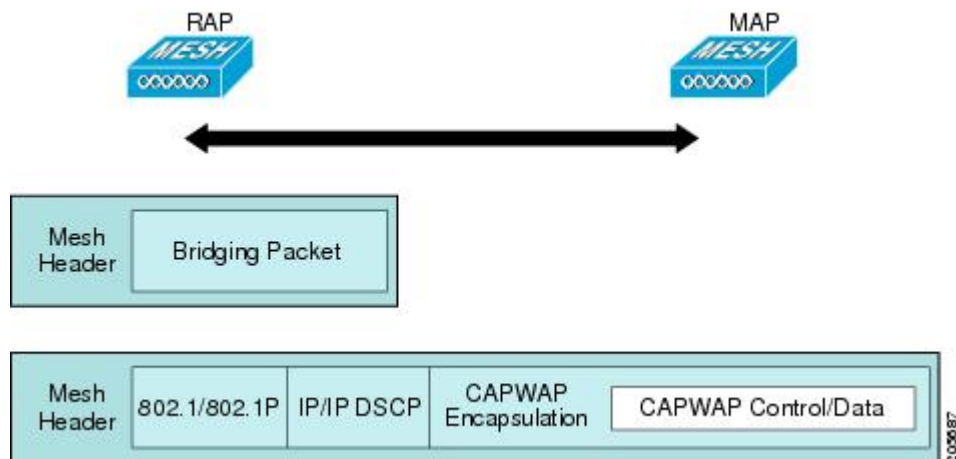


バックホールの場合、メッシュ トラフィックのカプセル化のタイプは1つだけです。ただし、2つのタイプのトラフィック（ブリッジトラフィックとCAPWAP制御およびデータトラフィック）がカプセル化されます。どちらのタイプのトラフィックもプロプライエタリメッシュヘッダーにカプセル化されます。

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 60: 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、Silver、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。

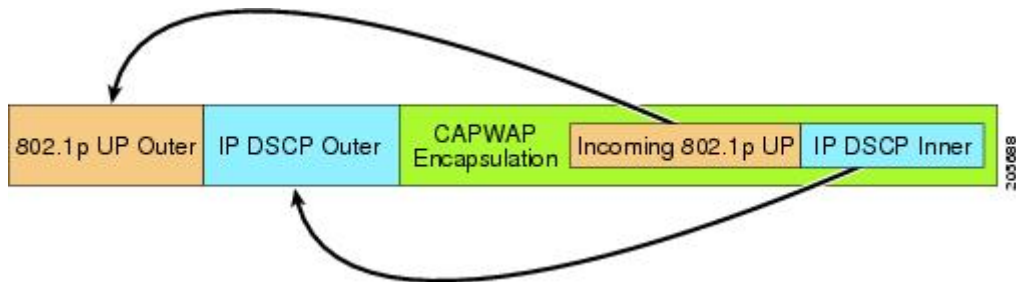
バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Silver、および Bronze に制限されます。Platinum キューは、CAPWAP 制御トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

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 61: 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 30: 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。

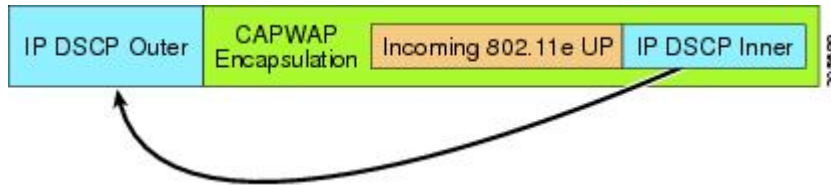
表 31: MAP からクライアントへのパスの QoS

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 62 : 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 32 : DSCP とバックホールキューのマッピング、(182 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 32 : 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。
- 音声はメッシュ 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
 - 音声はデータ要件より 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
 - 最小使用率のチャンネル (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 33 : 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、(185 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 33 : 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 17	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

¹⁷ 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이지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 34 : 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。

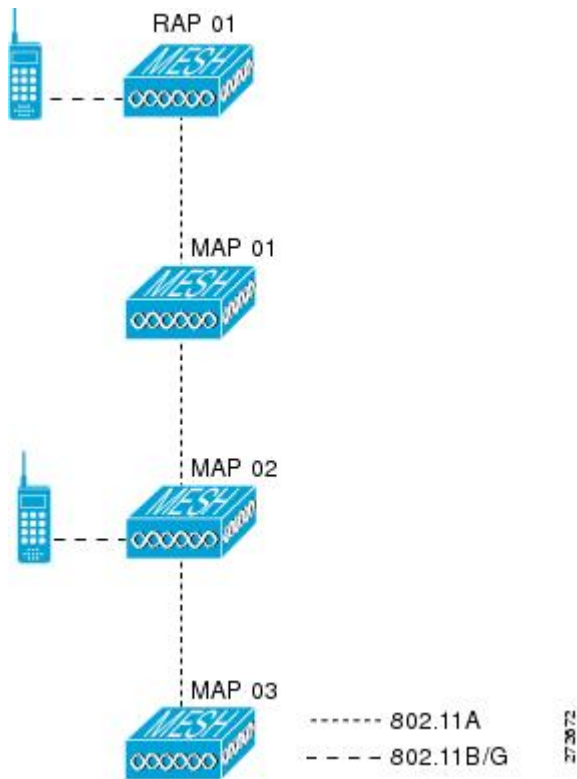


-
- (注) 802.11b クライアントが CAPWAP マルチキャストを受信する必要がある場合、マルチキャストをメッシュ ネットワーク上だけでなく、コントローラ上でグローバルに有効にする必要があります (**config network multicast global enable** CLI コマンドを使用)。マルチキャストをメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない場合、グローバルなマルチキャスト パラメータを無効にする必要があります (**config network multicast global disable** CLI コマンドを使用)。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

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 63: 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
SB_MAP1	1	11a	1
SB_MAP1	0	11b/g	0
SB_MAP2	1	11a	1
SB_MAP2	0	11b/g	1
SB_MAP3	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
SB_MAP1	1	11a	0
SB_MAP1	0	11b/g	0
SB_MAP2	1	11a	0
SB_MAP2	0	11b/g	1
SB_MAP3	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せん。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す。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 しようとしています。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 しようとしています。

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 しようとしています。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 しようとしています。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 しようとしています。



(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に設定可能にする必要があります (`config local-auth eap-profile cert-issuer vendor "prfMaP1500LIEAuth93"` 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 "prfMaP1500LIEAuth93"` コマンドは通常のコマンドですが、 "prfMaP1500LIEAuth93" 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。
- [Commands] > [Download File] を選択します。
 - [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。
 - 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。
 - [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。
- [Request a certificate] リンクをクリックします。
 - [Advanced certificate request] リンクをクリックします。
 - [Create and submit a request to this CA] リンクをクリックします。
 - 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。
 - 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。
 - [Mark keys as exportable] をイネーブルにします。
 - [Submit] をクリックします。
 - 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。証明書を变換するには、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 *prfMaP1500LIEAuth93*
- 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 64 : ローカルで有効な証明書ページ

Security Local Significant Certificates (LSC) Ap

AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Local EAP
Priority Order
Certificate
LSC
Access Control Lists
Wireless Protection Policies
Web Auth
Advanced

General AP Provisioning

Certificate Type	Status
CA	Not Present

General

Enable LSC on Controller

CA Server

CA server URL
(Ex: http://10.0.0.1:8080/caaserver)

Params

Country Code	<input type="text" value="US"/>
State	<input type="text" value="San Jose"/>
City	<input type="text" value="San Jose"/>
Organization	<input type="text" value="Cisco"/>
Department	<input type="text" value="Sales"/>
E-mail	<input type="text" value="sales@cisco.com"/>
Key Size	<input type="text" value="1024"/>

279072

図 65 : AP ポリシーの設定

AP Policies Apply Add

Policy Configuration

Authorize APs against AAA Enabled

Accept Self Signed Certificate (SSC) Enabled

Accept Manufactured Installed Certificate (MIC) Enabled

Accept Locally Significant Certificate (LSC) Enabled

AP Authorization List Entries 1 - 1 of 1

Search by MAC Search

MAC Address	Certificate Type	SHA1 Key Hash
00:16:36:91:9a:27	MIC	

279073

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 6 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, 203 ページ](#)
- [メッシュ アクセス ポイントのメッシュ統計情報の表示, 209 ページ](#)
- [メッシュ アクセス ポイントのネイバー統計情報の表示, 215 ページ](#)

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](#)
- [Public Safety 設定の表示](#)
- [セキュリティ設定と統計情報の表示](#)

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 ネイバーに関する概要情報を表示します。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** : 設定済みのプライマリおよびセカンダリ 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** : すべての設定済みのブリッジとそれらの MAC テーブル 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** : 設定済みの 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 およびパスの統計情報を表示します。
- **show mesh forwarding vlans** : サポートされている 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*** : 指定したチャン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*** : 指定したアクセスポイントとその子のアソシエーションと認証、および再アソシエーションと再認証に関して、パケットエラー統計情報と、失敗、タイムアウト、成功の数を表示します。

```
(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 location Age	GPS Present	Latitude	Longitude	Altitude	GPS
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-R00F-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 locationap-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 35: 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。
- 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、[Link Test] を選択します。ポップアップ ウィンドウが表示されます。
 - [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 > Link Test Results] ページに表示されます。
 - [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。
- 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。
 - [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。
- 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。
 - [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 7 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, 217 ページ](#)

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 66 : [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 67 : [All APs Summary] ページ

AP Name	AP MAC	AP Up Time	Admin Status	Operational Status	AP Mode	Certificate Type
iMeshRap1	00:19:30:76:32:72	0 d, 22 h 24 m 25 s	Enable	REG	Local	MIC
H3RAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
H3MAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
H3MAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
H3MAP2	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

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、別の場所へ移動する前に、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。

Hardware Reset

Perform a hardware reset on this AP

Reset AP Now

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Clear Config

206711

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 68: 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 69: 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せん。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。

```
H1 # show msh ?
  adjacency  l'ESH Adjacency
  astools    l'ESH Anti-strand tools
  backhaul   l'ESH backhaul
  channel    l'ESH channel
  canfig     l'ESH config parameter
  dfs        l'ESH dfs information
  ethernet  show mesh Ethernet bridging
  forwarding l'ESH Forwarding
  inventory  platform inventory
  linktest   l'ESH linktest stats
  nmule      l'ESH module detail
  nplrf      l'ESH NBN tool
  security   l'ESH Security show      12
  simulation  show simulated configuration 13
  status     l'ESH status
```

```
H1 # show mesh config
  rtsfhreshhold1 la 0, efs 0, a.1lin 0, co.1lex 0
  rtsfhreshhold1 lbg 0, aifs 0, a.1Hin 0, a.1lax 0
  huRetrles 0. 1lri <Rate 0 qOepth 0
  802.11MA client Statistics Push Int. ....al: 3
  range parameter: 12000
  mesh security node: 0
  Universal Client Access: disabled
  public safety global state: enabled
  Battery backup state: enabled
  multicast node: in-out
  Full Sector DFS: enabled
```

```
HJRAP111lehou caplo1Bp client mb
AdminState          ADHIN ENABLED
SuVer               S. 2.98.0
NumFl1 ledSlots    2
Name              HJRAP1
Location         default location
Huarllame           SEYf-CliffROLLER
Huarrlp             209.165.200.227
Huartt.Ner         0.0.0.0
ApHocle             Brl d!JE!
ApSubl'lode        Not f:mf igned
OperationState      UP
CAPllN' Path nru   1485
Link!U:liting      disabled
ApRole              RootAP
ApBac:khaul         802.11a
ApBac:khaulthannel 5805
ApBac:khaulSlot    1
ApBac:khaul1lgEnabled 0
ApBac:l<haul1xRate 24000
Ethernet Brl dglrg State 0
Public Safety State enabled
```

```
HJHAP111lehoi.I nesh adjacency ?
alI      HESH Adjacency Al I
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 rxNeighRep 66976 txNeighReq 33938 txNeighRep 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
suidb       : Virtual-Dot11Radio0
port state  : OPEN
```

273960

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** : ブリッジグループを含む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
- チャン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 無線をチャンネル (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** : 最適なネイバーの mac-addr にメッセージを送信し、リッスンを開始します。

- **debug mesh astools troubleshoot mac-addr stop** : 最適なネイバーの *mac-addr* にメッセージを送信し、リッスンを停止します。
- **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 (DFS)

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。無線がレーダー信号を検出すると、そのサービスを保護するために、少なくとも 30 分間送信を停止する必要があります。無線は、それをモニタした後にのみ送信されるように、別のチャンネルを選択します。使用する予定のチャンネルで少なくとも 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ンネルで伝送を開始できます。

AP は 60 秒間新しい DFS チャンネルで DFS スキャンを実行します。ただし、隣接する AP がその新しい DFS チャンネルをすでに使用している場合、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きます。誤った検出の原因には、RF 環境の不確実性や、実際のオンチャンネル 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 70: DFS および TPC 帯域の要件

	Frequency (MHz)
1	5150 – 5250
2	5250 – 5350
	5470 – 5725
3	5725 – 5850

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、チャン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。チャンネルが、RAP およびコントローラで影響を受けるチャンネルとしてマークされます。
- 2 RAP がそのチャンネルを 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、チャン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 秒間でチャンネルから移行します。これは、チャンネル移行時間と呼ばれます。システムがチャン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ンネルの最終送信の終わりまで測定されます。
- 5 RAP が Quiet モードに入ります。Quiet 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、チャンネル移行時間 (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 チャンネルを選択し、チャンネル情報を RAP に送信します。
- 7 RAP が新しいチャンネル情報を受信し、チャンネル変更フレーム (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、チャンネル変更フレームを送信します。
- 8 RAP が新しいチャン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、レーザーだけが ON になります。RAP が新しいチャンネルで、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、チャンネルアベイラビリティチェック (CAC) と呼ばれます。

- 9 MAP が新しいチャン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 が新しいチャンネルで、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 がこの新しいチャン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ン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、最終的にそのチャン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ンネルをマークします。
- 2 MAP が 30 分間チャン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、チャン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 秒間でチャンネルから移行します。これは、チャンネル移行時間と呼ばれます。システムがチャン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ンネルの最終送信の終わりまで測定されます。
- 5 MAP が Quiet モードに入ります。Quiet 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、チャンネル移行時間 (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ンネルを選択し、チャンネルを RAP に送信します。
- 7 RAP が新しいチャンネル情報を受信し、チャンネル変更フレーム (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、チャン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ン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 が新しいチャンネルで、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、チャン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ン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ンネル変更は、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 が異なる限り、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ンネルで、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ン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ン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
```

許可されたチャンネル 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ン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: Dot11Radiol, Channels:
100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
```

チャンネルの横のアスタリスクは、チャン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 チャン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 はすべてのチャンネルを調べ、各チャン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 Dot11Radiol
```



```
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 Dot11Radiol: 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) *5600(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(60) 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、このチャンネルで 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ンネルを使用します。同じ場所に 2 つの RAP を展開する場合、それらの間に 1 つのチャン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、チャンネル 124 および 128 が影響を受ける可能性があり、チャンネル 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ンネルを設定されたチャン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ン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ンネルで設定し、メッシュアクセスポイントをリブートします。

あるチャンネルでレーダーが確実に検出されたら、次のように、そのチャンネルおよび周囲の 2 つのチャンネルを 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ンネルに移行し、除外されたチャンネルを考慮しません。

たとえば、チャンネル 124 でレーダーが検出された場合、チャンネル 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 をそれらのチャン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なかったり、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

スポットは通常の（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 71 : 子のネイバー情報

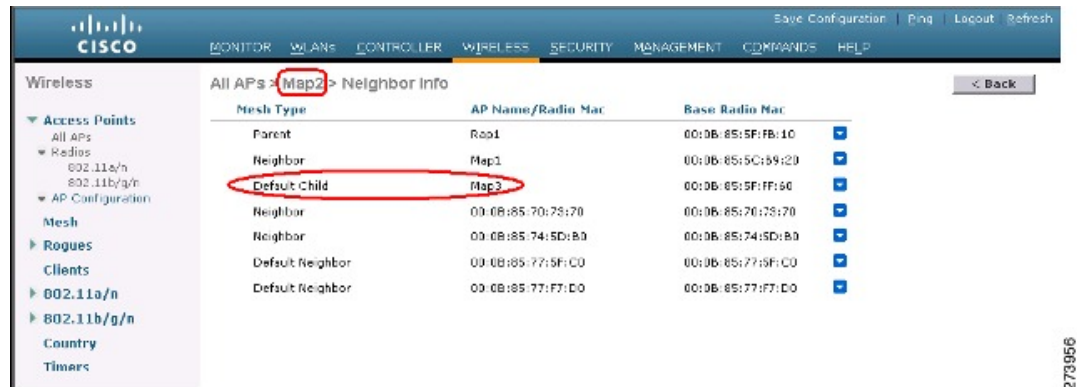


図 72 : 親のネイバー情報



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」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。

基本的なアイデアは次の 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 のリポート

- 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 73：除外ネイバー

All APs > sjc10-p1012-map1:62:40:d0 > Bridging Details < Back

Bridging Details		Bridging Links	
AP Role	MeshAP	Mesh Type	AP Name/Radio M
Bridge Group Name	betamesh	Parent	sjc14-41a-rap3-5e:9
Backhaul Interface	802.11a	Excluded Neighbor	00:0B:85:53:4B:30
Switch Physical Port	29	Neighbor	00:0B:85:5C:B8:A0
Routing State	Maintenance	Neighbor	00:0B:85:5C:B9:80
Malformed Neighbor Packets	0	Neighbor	00:0B:85:5F:FA:50
Poor Neighbor SNR reporting	1	Neighbor	00:0B:85:5F:FE:E0
Blacklisted Packets	212	Neighbor	00:0B:85:5F:FF:40
Insufficient Memory reporting	0	Neighbor	00:0B:85:5F:FF:E0

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ため、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行うことができます。

- 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。

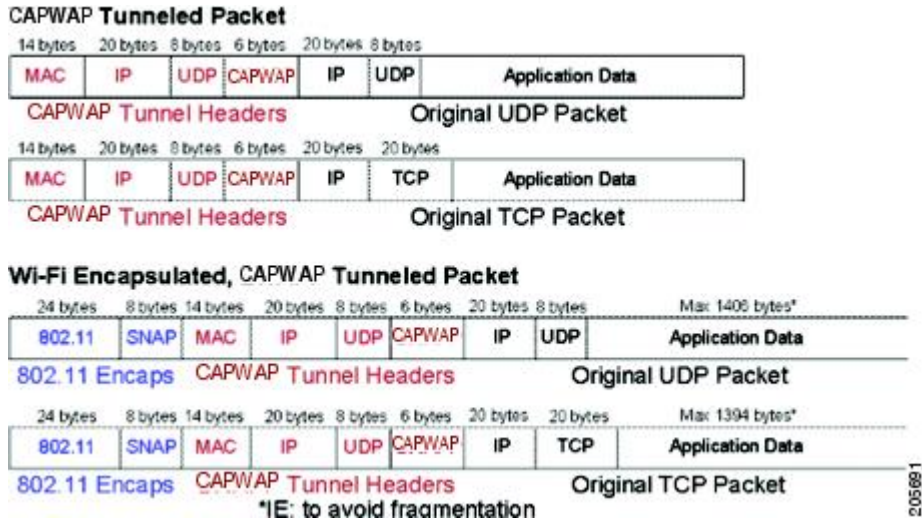
スループットは、ユーザ データグラム プロトコル (UDP) または Transmission Control Protocol (TCP) という、ネットワークを通過するトラフィックのタイプによって決まります。UDP はイーサネット経由で送信元アドレスおよび送信先アドレスを持つパケットおよび UDP プロトコルのヘッダーを送信します。確認応答 (ACK) は行われません。パケットがアプリケーション層で配信されるかどうかは保証されません。

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ตอบสนอง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74: CAPWAPでトンネリングされたパケット、(240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 74: CAPWAPでトンネリングされたパケット





第 8 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 日間の一時的リンク情報、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, 242 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, 245 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, 246 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, 250 ページ](#)
- [Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理, 251 ページ](#)
- [ワークグループブリッジのモニタリング, 267 ページ](#)
- [AP の \[Last Reboot Reason\] の表示, 274 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。
- 屋外領域名を入力します。
 - 屋外領域間い合わせ先の名前を入力します。
 - 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。
 - 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。
- [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。
 - 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。
 - [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せん。

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。

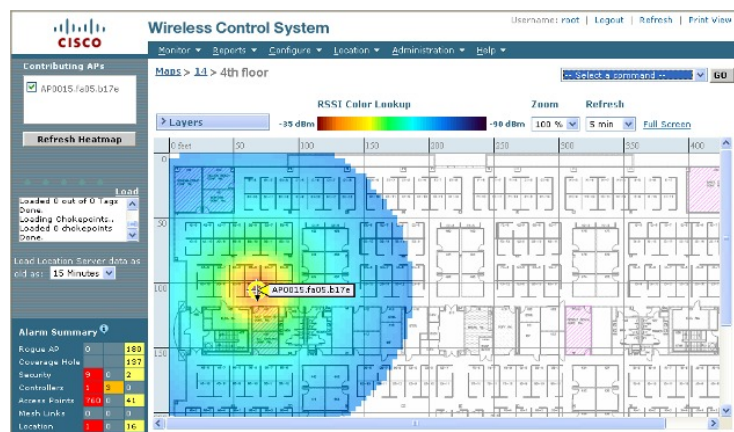
Cisco Prime Infrastructure によるマップへのメッシュ アクセス ポイントの追加

.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せん。
- 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 75: 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 を左に向けることとなります。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 76 : 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 77 : [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 78: Google Earth Map におけるメッシュアクセスポイントの詳細

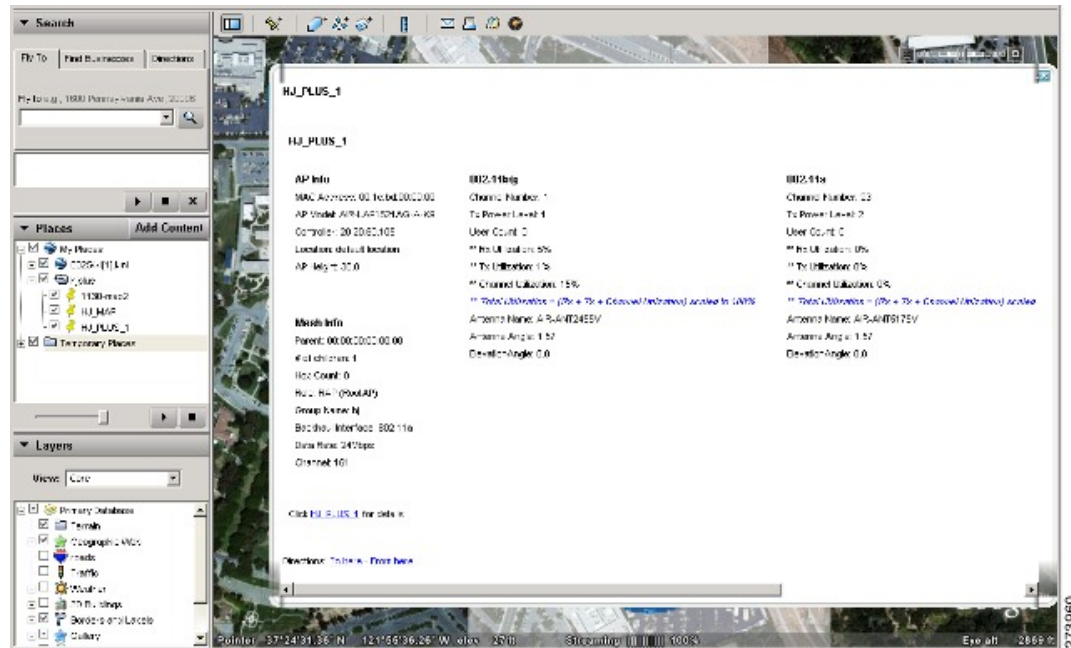


図 79: Google Earth Map におけるメッシュリンクの詳細



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。

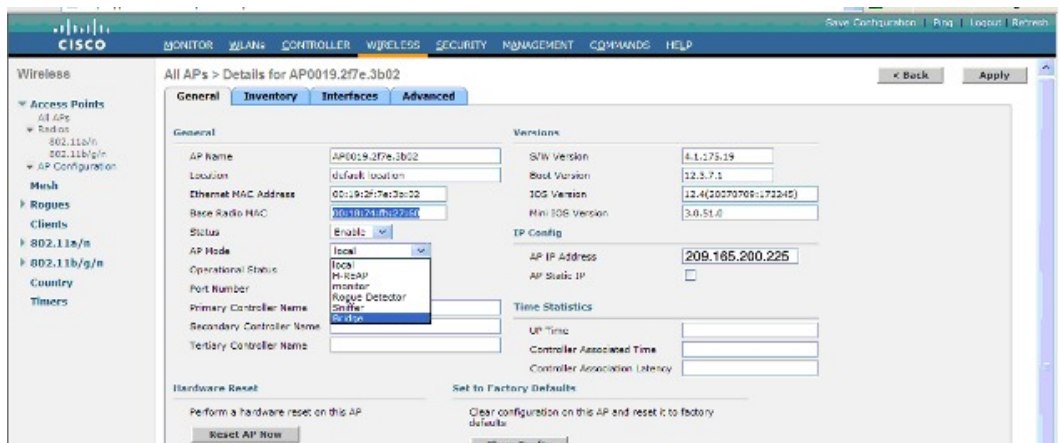
ローカルモードのメッシュ アクセス ポイントの場合、メッシュをインストールする前に、まずすべての屋内メッシュ アクセス ポイントをコントローラに接続し、モードとブリッジモードに変更する必要があります。

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。

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 80 : [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
- メッシュ アクセス ポイント
- メッシュ アクセス ポイント ネイバー

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
- チャンネル



(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。
- [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。
 - [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。
 - [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。
 - [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 36: モニタ アクセス ポイントの追加検索結果パラメータ, (256 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 36: 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、 $4 \times 0.5 = 2\text{dBm}$ 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。 <ul style="list-style-type: none"> • [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	チャンネル 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ンネルを示します。
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。 <ul style="list-style-type: none"> • [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 37: 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12dB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 38: 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 39: 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 40: [ブリッジリンク情報](#), (264 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 40: 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 41: 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)
緑	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 42 : [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。
パラメータ	説明
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 81 : [Monitor] > [WGBs]

The screenshot displays the Cisco Prime Infrastructure GUI for monitoring a Workgroup Bridge (WGB) client. The interface includes a navigation menu at the top with options like Monitor, Reports, Configure, Location, Administration, and Help. The main content area is titled 'Client (detected as WGB) - Cisco:5c:05:10' and features a dropdown menu for commands. Below this, there are several tabs: General, Statistics, Location, CCxV5, and WGB Clients. The 'General' tab is active, showing 'Client Properties' and 'RF Properties' sections. The 'Client Properties' section includes fields for Client User Name, Client IP Address (209.165.200.226), Client MAC Address (00:17:94:5c:05:10), Client Vendor (Cisco), Controller (209.165.200.240), Port (1), Interface (management), VLAN ID (70), 802.11 State (Associated), Mobility Role (Unassociated), Policy Manager State (RUN), Anchor Address (0.0.0.0), Mirror Mode (Disable), CCX (VS), E2E (Not Supported), and WGB Status (WGB). The 'RF Properties' section includes AP Name (SJC14-42A-AP-C2), AP Type (Cisco AP), AP Base Radio MAC (00:14:1b:58:42:00), Protocol (802.11g), AP Mode (local), Profile Name (wgbme), SSID (wgbme), Security Policy, Association Id (90), Reason Code (None), and 802.11 Authentication (OPENSYSTEM). A 'Security' section shows Authenticated (Yes), Policy Type (Unknown), Encryption Cipher (NONE), and EAP Type (Unknown). At the bottom, the 'WGB SNMP Monitoring' section shows SNMP Status (Unreachable) and a note: 'This WGB is monitored by WCS as Autonomous AP. Click for more details'. A vertical ID '205754' is visible on the right side of the screenshot.

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 82 : [Monitor] > [WGBs] > [WGB Clients] パネル

Client Properties		AP Properties	
MAC Address	00:1b:03:ac:a7:0f	AP Address	00:1e:14:40:ec:09
IP Address	209.165.200.235	AP Name	MAR2-001e.1448.ec00H3r
Client Type	WGB Client	AP Type	802.11a
WGB MAC Address	00:1d:45:15:74:44	WLAN Profile	WLAN5
User Name		Status	Associated
Port Number	29	Association ID	0
Interface	management	802.11 Authentication	Open System
VLAN ID	76	Reason Code	0
CCX Version	Not Supported	Status Code	0
E2E Version	Not Supported	CF Pollable	Not Implemented
Mobility Role	Local	CF Poll Request	Not Implemented
Mobility Peer IP Address	N/A	Short Preamble	Implemented
Policy Manager Status	RUN	PBCC	Not Implemented
Mirror Mode	Disable	Channel Agility	Not Implemented
Management Frame Protection	No	Timeout	0
		WEP State	WEP Disable

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 内には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	Vi0.184	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を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

A

AP1552C [14](#)
AP1552CU [15](#)
AP1552E [13](#)
AP1552EU [16](#)
AP1552H [15](#)
AP1552I [14](#)

C

CAC [177](#)
 メッシュ ネットワーク内の [177](#)
CAPWAP [37](#)
CleanAir [89, 92, 93](#)
 Advisor [93](#)
 アクセス ポイント配置の推奨事項 [92](#)
 ライセンス [93](#)
 動作モード [89](#)
ClientLink テクノロジー [56, 59](#)
 関連コマンド [59](#)
ClientLink の設定 (CLI) [57](#)

D

DOCSIS/EuroDOCSIS [12](#)

E

EPON SFP [16](#)

G

Google Earth マップ [246, 247](#)
 表示 [247](#)

L

LED ステータス [21](#)
 モニタリング [21](#)
LinkSNR 要件 [52, 53](#)

M

mesh [213](#)
 統計情報 [213](#)
 GUI を使用したアクセス ポイントの表示 [213](#)

N

N コネクタ [28](#)

P

Pseudo MAC とマージ [89](#)

W

WPlus ライセンス [60](#)

あ

アクセス ポイントのロール [2, 103, 225](#)
 定義 [103, 225](#)

こ

コントローラ ソフトウェアのアップグレード [100](#)
コントローラの計画 [59](#)

せ

セルの計画と距離 [70, 72](#)
AP1520 シリーズ [70](#)
AP1550 シリーズ [72](#)

は

バックアップ コントローラ [107](#)

ひ

ビーム幅 [27](#)

ふ

フレネル ゾーン [61, 63](#)

ま

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 [252](#)

め

メッシュ アクセス ポイントの状態のモニタリング [255](#)
メッシュ レンジ [48](#)
設定 [48](#)

ゆ

ユニバーサル アクセス [46](#)

ろ

ローカルで有効な証明書 [192](#)

わ

ワークグループブリッジ [267](#)
モニタリング [267](#)
ワイヤレス ソフトウェアの互換性マトリクス [100](#)
ワイヤレス バックホール データ レート [139](#)