



Cisco ワイヤレス メッシュ アクセス ポイント リリース 8.7 設計および導入ガイド

初版：2018年4月9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、ネットワークボロジ図、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. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

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**

第 1 章

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 **1**

5508、3504、5520、および 8540 シリーズ Cisco コントローラにおけるメッシュ アクセス
ポイントのライセンス **1**

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**

周波数帯域 **7**

Dynamic Frequency Selection (動的周波数選択) **8**

アンテナ **9**

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) **10**

Cisco ワイヤレス LAN コントローラ **11**

Cisco Prime Infrastructure **11**

アーキテクチャ **11**

Control and Provisioning of Wireless Access Points **11**

メッシュ ネットワークの CAPWAP ディスカバリ	12
ダイナミック MTU 検出	12
Adaptive Wireless Path Protocol	12
トラフィック フロー	13
メッシュ ネイバー、親、および子	14

第 2 章**メッシュ導入モード 17**

ワイヤレス メッシュ ネットワーク	17
無線バックホール	18
ユニバーサル アクセス	18
ポイントツーマルチポイント無線ブリッジング	18
ポイントツーポイント無線ブリッジング	19
メッシュ レンジの設定 (CLI)	20
リリース 8.7 の Flex+Mesh の概要	21
新しい 8.7 の機能をサポートする Mesh COS AP	21
フレキシブル アンテナ ポート設定	22
Flex Mesh AP の実行モード	22
接続モード	22
スタンドアロン モード	22
放棄モードまたは永続 SSID モード	22
Flex Mesh COS AP のモード/状態の遷移	23
スタンドアロン モードの Flex AP に関する設計上の考慮事項	24
COS Flex RAP の特別なスタンドアロンモード	24
既存のフレックス接続 AP モードの設計	24
新しい要件をサポートするための設計上の考慮事項	25
メッシュの機能強化の設定	26
リリース 8.7 で RAP 永続モードをテストする手順	28

第 3 章**デザインの考慮事項 29**

無線メッシュの制約	29
無線バックホールのデータ レート	29

コントローラ プランニング 33

第 4 章

メッシュ導入リリース 8.4 の Air Time Fairness 35

メッシュ導入リリース 8.4 の Air Time Fairness 35

前提条件と 8.4 リリースでサポートされる機能 35

Cisco Air Time Fairness (ATF) の使用例 36

ATF 機能 37

メッシュの ATF 機能の概要 38

ATF の動作モード 41

メッシュの ATF の設定 41

第 5 章

サイトの準備と計画 45

サイトの調査 45

調査前チェックリスト 45

屋外サイトの調査 46

見通し (Line of Sight) の判別 47

天候 47

フレネルゾーン 47

ワイヤレス メッシュ配置のフレネルゾーン サイズ 49

隠しノードの干渉 49

優先される親の選択 50

優先親の選択基準 50

優先される親の設定 51

関連コマンド 52

共同チャネルの干渉 53

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 54

セルのプランニングと距離 54

Cisco レンジ カルキュレータの前提条件 59

メッシュ アクセス ポイントのコロケーション 62

屋内メッシュ ネットワークの特殊な考慮事項 63

メッシュ AP バックグラウンド スキャン リリース 8.3 65

DFS と非 DFS チャネル スキャン	66
メッシュ コンバージェンスの設定	68
ワイヤレス伝搬の特性	72
CleanAir	72
CleanAir AP 動作モード	73
Pseudo MAC (PMAC) とマージ	73
Event Driven Radio Resource Management と Persistence Device Avoidance	75
CleanAir アクセス ポイント配置の推奨事項	75
CleanAir Advisor	77
CleanAir のイネーブル化	77
ライセンス	77
ワイヤレス メッシュ モビリティ グループ	78
複数のコントローラ	78
メッシュ アベイラビリティの増加	79
複数の RAP	80
屋内メッシュと屋外メッシュの相互運用性	80

第 6 章

Cisco メッシュ アクセス ポイントのネットワークへの接続	83
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	84
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	85
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)	86
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)	87
メッシュ アクセス ポイントのロール定義	87
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	87
AP ロールの設定 (GUI)	88
AP ロールの設定 (CLI)	89
DHCP 43 および DHCP 60 を使用した複数のコントローラの設定	89
バックアップ コントローラ	91
RADIUS サーバを使用した外部認証および認可の設定	92
RADIUS サーバの設定	92

メッシュ アクセス ポイントの外部認証の有効化 (GUI)	93
メッシュ アクセス ポイントの外部認証の有効化 (CLI)	95
セキュリティ統計情報の表示 (CLI)	95
リリース8.2での Mesh PSK Key を使ったプロビジョニング	95
サポートされるワイヤレス メッシュのコンポーネント	96
機能の設定手順	96
メッシュ PSK GUI の設定	97
モビリティ グループのコントローラを使用したメッシュ PSK のプロビジョニング	103
PSK 事前プロビジョニング用の CLI コマンド	104
グローバル メッシュ パラメータの設定	104
グローバル メッシュ パラメータの設定 (GUI)	104
グローバル メッシュ パラメータの設定 (CLI)	111
グローバル メッシュ パラメータ設定の表示 (CLI)	113
リリース 8.2 の 5 GHz および 2.4 GHz のメッシュ バックホール	114
バックホール クライアント アクセス	118
バックホール クライアント アクセスの設定 (GUI)	119
バックホール クライアント アクセスの設定 (CLI)	119
ローカル メッシュ パラメータの設定	120
無線バックホールのデータ レートの設定	120
イーサネットブリッジングの設定	123
イーサネットブリッジングの有効化 (GUI)	125
ネイティブ VLAN の設定 (GUI)	126
ネイティブ VLAN の設定 (CLI)	126
ブリッジグループ名の設定	127
ブリッジグループ名の設定 (CLI)	127
ブリッジグループ名の確認 (GUI)	127
電力およびチャネルの設定	128
電力およびチャネルの設定 (GUI)	128
アンテナ利得の設定	128
アンテナ利得の設定 (GUI)	128
アンテナ ゲインの設定 (CLI)	129

動的チャンネル割り当ての設定	129
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	132
拡張機能の設定	133
イーサネット VLAN タギングの設定	133
イーサネット ポートに関する注意	134
VLAN 登録	136
イーサネット VLAN タギングの有効化 (GUI)	138
イーサネット VLAN タギングの設定 (CLI)	139
イーサネット VLAN タギング設定詳細の表示 (CLI)	140
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	140
ワークグループブリッジの設定	141
設定のガイドライン	144
設定例	146
WGB アソシエーションの確認	147
リンク テストの結果	149
WGB 有線/ワイヤレス クライアント	150
クライアント ローミング	151
WGB ローミングのガイドライン	152
設定例	152
トラブルシューティングのヒント	153
屋内メッシュ ネットワークの音声パラメータの設定	154
Call Admission Control (コール アドミッション制御)	154
QoS および DiffServ コード ポイントのマーキング	155
メッシュ ネットワークでの音声使用のガイドライン	160
ビデオのメッシュ マルチキャストの抑制の有効化	162
メッシュ ネットワークの音声詳細の表示 (CLI)	163
メッシュ ネットワークにおけるマルチキャストの有効化 (CLI)	167
IGMP スヌーピング	168
メッシュ AP のローカルで有効な証明書	168
設定のガイドライン	169
メッシュ AP の LSC と通常の AP の LSC の違い	170

LSC AP での証明書検証プロセス	170
LSC 機能の証明書の取得	170
ローカルで有効な証明書 (CLI) の設定	172
LSC 関連のコマンド	173
コントローラ GUI セキュリティ設定	175
展開ガイドライン	176

第 7 章

ネットワークの状態の確認	177
Show Mesh コマンド	177
一般的なメッシュ ネットワークの詳細の表示	177
メッシュ アクセス ポイントの詳細の表示	179
グローバル メッシュ パラメータ設定の表示	180
ブリッジ グループ設定の表示	181
VLAN タギング設定の表示	181
DFS の詳細の表示	182
セキュリティ設定と統計情報の表示	182
GPS ステータスの表示	183
メッシュ アクセス ポイントのメッシュ統計情報の表示	184
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)	184
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)	189
メッシュ アクセス ポイントのネイバー統計情報の表示	190
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)	191
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)	191

第 8 章

メッシュ アクセス ポイントのトラブルシューティング	193
インストールと接続	193
debug コマンド	194
リモート デバッグ コマンド	195
AP コンソール アクセス	195
AP からのケーブル モデムのシリアル ポート アクセス	196
設定	196

メッシュ アクセス ポイント CLI コマンド	198
メッシュ アクセス ポイント デバッグ コマンド	201
メッシュ アクセス ポイントのロール定義	201
バックホール アルゴリズム	201
パッシブ ビーコン (ストランディング防止)	202
メッシュ アクセス ポイントの IP アドレスの誤った設定	204
DHCP の誤った設定	204
ノード除外アルゴリズムについて	205
スループット分析	207

Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理	209
---	-----



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 2600、2700、3500、3600、および 3700 シリーズ アクセス ポイント)、さらに Cisco Prime Infrastructure を採用してスケーラブルな集中管理および屋内外の展開のモビリティを提供しています。Control and Provisioning of Wireless Access Points (CAPWAP) プロトコルは、ネットワークへのメッシュ アクセス ポイントの接続を管理します。

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

このマニュアルで説明する機能は、次の製品に該当します。

- Cisco Aironet 1570 (1572) シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1560 (1562) シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1540 (1542) シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1550 (1552) シリーズの屋外メッシュ アクセス ポイント
- Cisco Aironet 1530 シリーズ屋外メッシュ アクセス ポイント
- Cisco Aironet 1600、2600、3600、3500、1700、2700、および 3700 シリーズの屋内メッシュ アクセス ポイント
- Cisco ワイヤレス LAN コントローラのメッシュ機能
- Cisco Prime Infrastructure のメッシュ機能

この章の内容は、次のとおりです。

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

表記法

このマニュアルでは、次の表記法を使用しています。

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



(注) 「注釈」です。



ヒント 「問題解決に役立つ情報」です。



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



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

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

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



第 1 章

メッシュ ネットワーク コンポーネント

この章では、メッシュ ネットワーク コンポーネントについて説明します。

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

- Cisco Aironet シリーズ アクセス ポイント



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

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

この章の内容は、次のとおりです。

- [メッシュ アクセス ポイント \(1 ページ\)](#)
- [Cisco ワイヤレス LAN コントローラ \(11 ページ\)](#)
- [Cisco Prime Infrastructure \(11 ページ\)](#)
- [アーキテクチャ \(11 ページ\)](#)

メッシュ アクセス ポイント

5508、3504、5520、および 8540 シリーズ Cisco コントローラにおけるメッシュ アクセス ポイントのライセンス

Cisco 3504、5500 および 8500 シリーズ コントローラでメッシュ アクセス ポイントと非メッシュ アクセス ポイントの両方を使用する場合、7.0 リリース以降では、必要なライセンスが base ライセンスだけになりました。ライセンスの取得とインストールの詳細については、

http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html
の『Cisco Wireless LAN Controller Configuration Guide』を参照してください。

アクセス ポイントのロール

メッシュ ネットワーク内のアクセス ポイントは、次の 2 つの方法のいずれかで動作します。

1. ルート アクセス ポイント (RAP)
2. メッシュ アクセス ポイント (MAP)
3. メッシュ リーフ ノード

リリース 8.6 で追加されたメッシュ リーフ ノード モード

ワイヤレス バックホールのパフォーマンスの低下を避けるために、低パフォーマンスの IOS ベースのメッシュ AP はリーフ ノード、つまり基本的にはツリーの最後のノードとしてのみ動作するように設定できるようになりました。

The screenshot shows the configuration page for AP1542.F116.1CE8. The 'Block Child' checkbox is highlighted with a red box. The configuration includes fields for AP Role (RootAP), Bridge Type (Outdoor), Bridge Group Name (tme), and other settings. The 'Block Child' checkbox is currently unchecked.



(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。

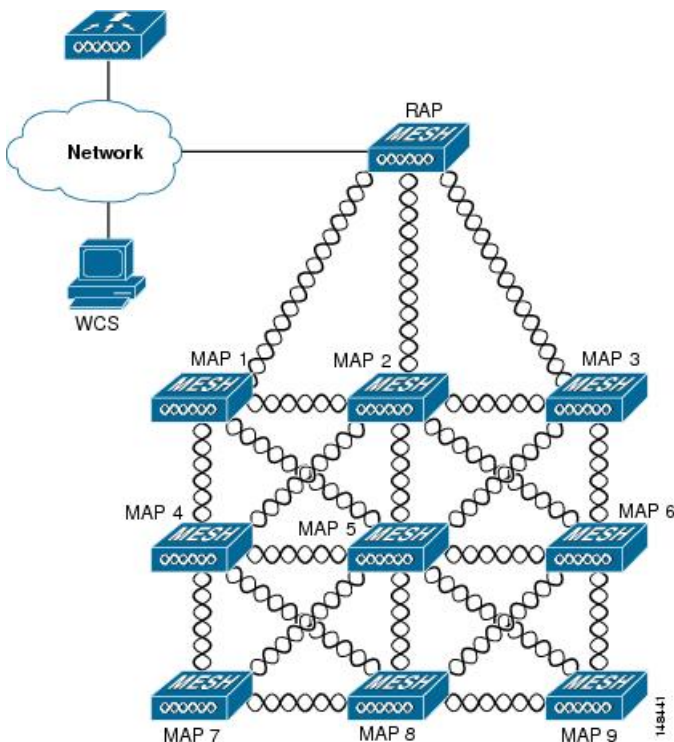
ブリッジモードのアクセスポイントでは、5 GHz 周波数のメッシュバックホールの CleanAir をサポートし、干渉デバイスレポート (IDR) と電波品質の指標 (AQI) レポートのみを作成します。



(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。ネットワーク全体で接続された有線/無線インターフェイスから BPDUを受信するとアップストリームデバイスに BPDU を転送します。

図 1: 単純なメッシュネットワーク階層

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。



ネットワークアクセス

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

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

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

メッシュアクセスポイントによる無線LANメッシュへのアクセスは次の認証方式で管理されます。

- MAC 認証：メッシュアクセスポイントが参照可能データベースに追加され、特定のコントローラおよびメッシュネットワークに確実にアクセスできるようにします。
- 外部 RADIUS 認証：メッシュアクセスポイントは、証明書付きの EAP-FAST のクライアント認証タイプおよび WLC 上で WPA2/PSK をサポートする Cisco ACS (4.1 以上) や ISE などの RADIUS サーバを使用して、外部から認証できます。

ネットワークのセグメント化

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

Cisco 屋内メッシュアクセスポイント

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

- Cisco Aironet 1600 シリーズ アクセスポイント
- Cisco Aironet 1700 シリーズ アクセスポイント
- Cisco Aironet 2600 シリーズ アクセスポイント
- Cisco Aironet 2700 シリーズ アクセスポイント
- Cisco Aironet 3500 シリーズ アクセスポイント
- Cisco Aironet 3600 シリーズ アクセスポイント
- Cisco Aironet 3700 シリーズ アクセスポイント
- Cisco Aironet 1530 シリーズ アクセスポイント
- Cisco Aironet 1540 シリーズ アクセスポイント
- Cisco Aironet 1550 シリーズ アクセスポイント
- Cisco Aironet 1560 シリーズ アクセスポイント
- Cisco Aironet 1570 シリーズ アクセスポイント
- Cisco Industrial Wireless 3700 シリーズ アクセスポイント



(注) 8.5 リリースでは次の AP がサポートされます。



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

エンタープライズ 11n/ac メッシュは、802.11n/ac アクセスポイントで動作するために CUWN 機能に追加される拡張機能です。エンタープライズ 11ac メッシュ機能は 802.11ac 以外のメッシュと互換性がありますが、バックホールとクライアントのアクセス速度が向上します。802.11ac 屋内アクセスポイントは、特定の屋内展開用のデュアルチャネル Wi-Fi インフラデバイスです。一方の無線をアクセスポイントのローカル（クライアント）アクセスに使用でき、もう一方の無線をワイヤレスバックホールに対して設定できます。ユニバーサルバックホールアクセスが有効な場合、リリース 8.2 の 5 GHz および 2.4 GHz 帯はローカル（クライアント）アクセスとバックホールのいずれにも使用できます。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台数が多く、アクセスポイントが従来の非メッシュワイヤレスカバレッジに対してローカルモードですでに展開されている場合に、煩雑になります。

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

- リリース 8.2 以降では、データバックホールとクライアントアクセスに 2.4 GHz 帯を使用（UBA が有効な場合）
- データバックホールおよびクライアントアクセスに 5 GHz 帯を使用（ユニバーサルバックホールアクセスが有効な場合）

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

Cisco 屋外メッシュ アクセス ポイント

Cisco 屋外メッシュアクセスポイントは、Cisco Aironet 1500 シリーズアクセスポイントから構成されます。1500 シリーズには、1572 11ac 屋外アクセスポイント、1552 および 1532 11n 屋外メッシュアクセスポイント、そして新しい 1540 および 1560 11ac Wave 2 シリーズが含まれます。

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

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。

アップリンク サポートには、ギガビット イーサネット (1000BASE-T) と、ファイバまたは ケーブル モデム インターフェイスに接続できる小型フォーム ファクタ (SFP) スロットが含まれます。1000BASE-BX までのシングルモード SFP とマルチモード SFP の両方がサポートされます。メッシュ アクセス ポイントのタイプに基づき、ケーブル モデムは DOCSIS 2.0 または DOCSIS/EuroDOCSIS 3.0 になります。

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

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

- **ローカル モード**：このモードでは、AP は割り当てられたチャンネル上のクライアントを処理できます。180 秒周期で周波数帯上のすべてのチャンネルをモニタ中にも、クライアントの処理が可能です。この間に、AP は 50 ミリ秒周期で各チャ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 AP でクライアント データ トラフィックをローカルでスイッチして、クライアント認証をローカルで実行することができます。コントローラに接続されている場合、FlexConnect モードではコントローラにトラフィックをトンネリングで戻すこともできます。
- **Flex+Bridge モード**：このモードでは、FlexConnect とブリッジモードの設定オプションの両方をアクセス ポイントで使用できます。
- **モニタ モード**：このモードでは、AP 無線は受信状態にあります。AP は、12 秒ごとにすべてのチャ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 に、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ワイヤレス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/無線バックホールに関係なく、ブリッジ/Flex+Bridge モードでだけ設定できます。有線バックホールを持つMAPの場合は、APモードを変更する前に、APロールをRAPに変更する必要があります。



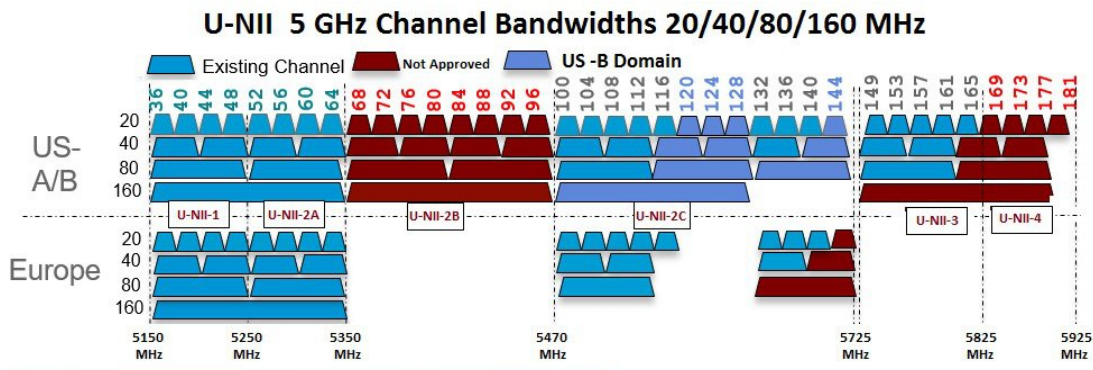
(注) 屋外メッシュ AP のすべてのモデルの詳細と仕様については、以下のリンクを参照してください。

- <https://www.cisco.com/c/en/us/products/wireless/outdoor-wireless/index.html?stickynav=1>

周波数帯域

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

図 2: AP1500 の 802.11a 無線でサポートされる周波数帯



米国 FCC

U-NII-1

屋内と屋外の利用可能周波数に追加

アンテナが 6 dBi の場合、最大電力は 30 dBm に増加 (1 ワット)

利得が 6 dBi を超えるすべての dB アンテナでは、電力を 1 dB 削減

屋外使用の場合、上方 30 度を超える方向での EIRP 電力は 125 mW (20.9 dBm) に制限

U-NII-2A と U-NII-2C

Dynamic Frequency Selection (DFS) レーダー検出が必須

新しい DFS テスト要件では、Terminal Doppler Weather Radar (TWDR) 周波数帯 (チャンネル 120、124、128) が使用可能周波数帯に追加

U-NII-3

周波数帯が 5825 MHz から 5850 MHz に拡張

欧州

U-NII-1

最大 23 dBm、屋外使用不可

U-NII-2A

最大 23 dBm、屋外使用不可

U-NII-2C

最大 30 dBm

U-NII-3

23 dBm で英国でのみ利用可能、屋内専用

Dynamic Frequency Selection (動的周波数選択)

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

既存のレーダーサービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要のあるデバイスに対して、動的周波数選択 (DFS) プロトコルに従って動作することを求めています。DFS では、無線デバイスがレーダー信号の存在を検出できる機能の採用を義務付けています。AP でレーダー信号が検出されると、最低 30 分間は伝送を停止して、レーダー信号を保護する必要があります。その後、AP は伝送のため別のチャンネルを選択しますが、伝送前にこのチャンネルをモニタリングする必要があります。使用する予定のチャ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 は新たな DFS チャンネルで、DFS スキャンを 60 秒間実行します。ただし、この新規 DFS チャンネルが隣接 AP ですでに使用されている場合、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。

図 3: DFS および TPC 周波数帯の要件

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

273989

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ため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

幅広いアンテナが提供されており、どのような地形や建物でもメッシュアクセスポイントを展開できます。サポートされるアンテナのリストについては、該当するアクセスポイントデータシートまたは発注ガイドを参照してください。

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

配置および設計、制限事項および機能、さらにアンテナの基礎理論や取り付け手順、規制に関する情報、技術仕様についても記載されています。 <http://www.cisco.com/c/ccc/prods-industry/selling-en/products/wireless/ap/aironet-acc.html>

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、お客様の責任で確認してください。
- 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。

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、3500、5508、5520、WiSM-2、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、3500、5500、および 8500 シリーズ Wireless LAN Controller 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 メッシュを視覚的に計画、設定、管理できるプラットフォームです。Prime Infrastructure を使用することで、ネットワーク管理者は、ワイヤレス メッシュ ネットワークの設計、コントロール、モニタリングを一元的に行えます。

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を提供できる Prime Infrastructure は、ネットワーク運用に不可欠です。

Prime Infrastructure は、組み込みデータベースと共に、サーバプラットフォームで実行されます。これにより、何百ものコントローラや何千もの Cisco メッシュ アクセス ポイントを管理でき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

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。

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は、このメッシュアクセスポイント用の静的 IP（存在する場合）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 の両方が失敗し、しかもコントローラとの CAPWAP 接続が成功しない場合。
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。

Adaptive Wireless Path Protocol

Adaptive Wireless Path Protocol (AWPP) は、ワイヤレスメッシュネットワーク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検出できます。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ング機能を実行して、RF 環境のエフェメラルな性質に、ネットワークの安定性が影響を受けないようにします。

トラフィック フロー

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

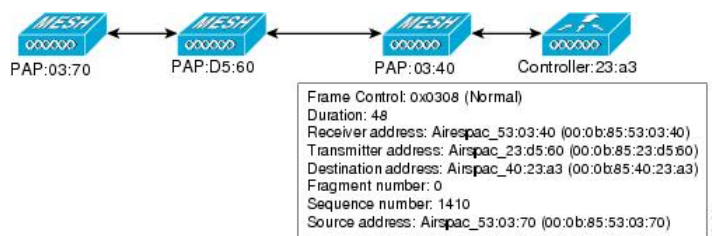
1. オーバーレイ CAPWAP トラフィック：標準の CAPWAP アクセス ポイントの配置内のフローで、CAPWAP アクセス ポイントと CAPWAP コントローラの間 CAPWAP トラフィックのことです。
2. ワイヤレス メッシュ データ フレーム フロー
3. AWPP 交換

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 4: ワイヤレス メッシュ フレーム (13 ページ) は、このタイプのフレーム構成の例を示しています。フレームの発信元アドレスは MAP:03:70、このフレームの送信先アドレスはコントローラ (メッシュ ネットワークはレイヤ 2 モードで動作しています)、トランスミッタ アドレスは MAP:D5:60、レシーバ アドレスは RAP:03:40 です。

図 4: ワイヤレス メッシュ フレーム



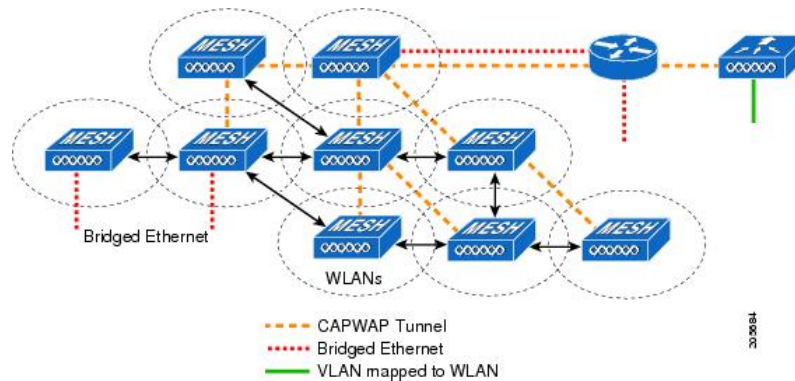
このフレームの送信により、トランスミッタとレシーバのアドレスは、ホップごとに変わります。各ホップでレシーバアドレスを判別するために AWPP が使用されます。トランスミッタ

アドレスは、現在のメッシュ アクセス ポイントのアドレスです。パス全体を通して、発信元アドレスと送信先アドレスは同一です。

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

メッシュ内の各メッシュ アクセス ポイントは、コントローラと共に、CAPWAP セッションを形成します。WLAN トラフィックは CAPWAP 内にカプセル化されるため、コントローラ上の VLAN インターフェイスにマップされます。ブリッジされたイーサネットトラフィックは、メッシュ ネットワーク上の各イーサネット インターフェイスから渡される可能性があり、コントローラのインターフェイスにマップされる必要はありません (図 5: 論理ブリッジと WLAN マッピング (14 ページ) を参照)。

図 5: 論理ブリッジと WLAN マッピング

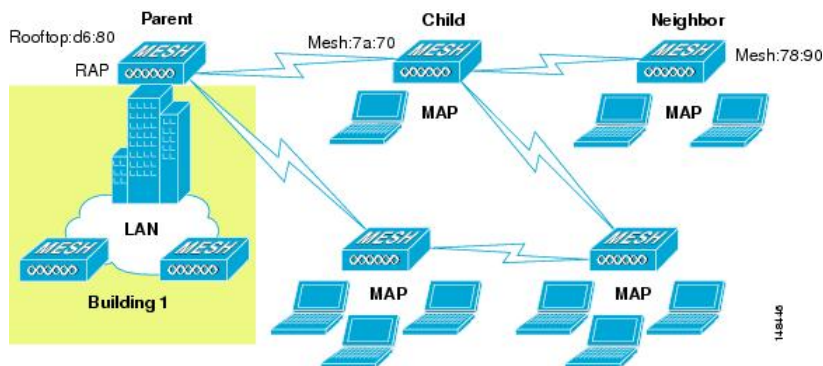


メッシュ ネイバー、親、および子

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 6: 親、子、およびネイバー アクセス ポイント (15 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 (ease value) は親よりも低いため、親や子としては選択されません。

図 6: 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。

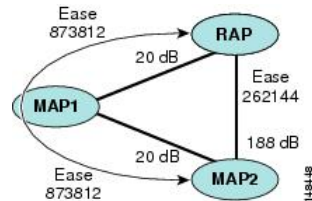
親メッシュ アクセス ポイントは、RAP に戻る最適なパスを提供します。AWPP は、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

容易度 (ease) 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 7: 親パスの選択 (16 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 (ease value、436906) が、MAP2 から RAP に直接進むパスの容易度の値 (ease value、262144) より大きいためです。

図 7: 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 (ease) = 最小値 (各ホップでの容易度 (ease)) ホップ数

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 \(17 ページ\)](#)
- [無線バックホール \(18 ページ\)](#)
- [ポイントツーマルチポイント無線ブリッジング \(18 ページ\)](#)
- [ポイントツーポイント無線ブリッジング \(19 ページ\)](#)
- [リリース 8.7 の Flex+Mesh の概要 \(21 ページ\)](#)

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 台の AP はすべて建物の屋根に設置され、RAP として機能しています。これらの RAP は、それぞれの場所でネットワークに接続します。

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



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

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、無線バックホールなどのワイヤレスメッシュリンクを通過する際に必ず AES 暗号化されます。

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

ユニバーサルアクセス

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



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

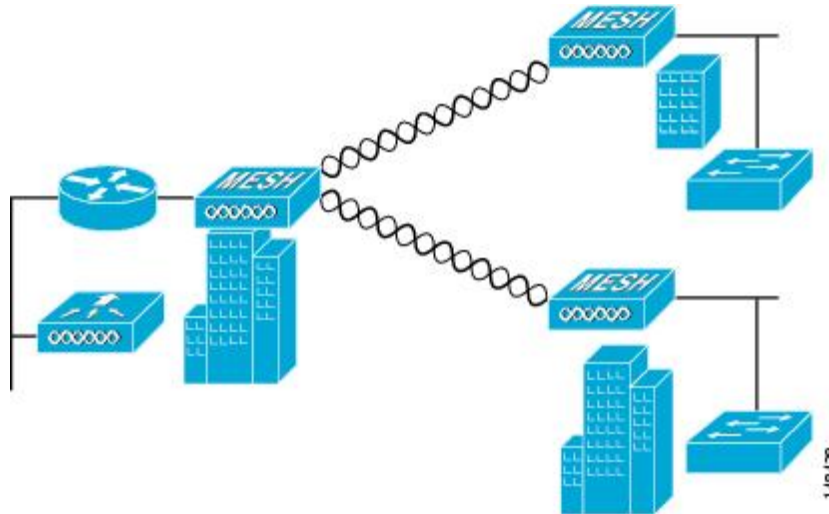
ポイントツーマルチポイント無線ブリッジング

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

図 8: ポイントツーマルチポイントブリッジングの例

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

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

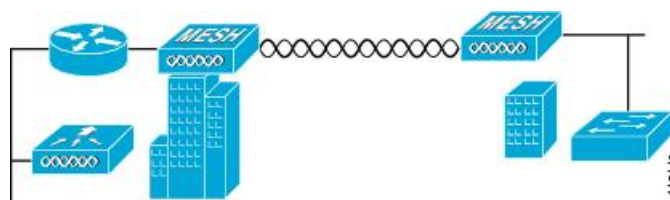


ポイントツーポイント無線ブリッジング

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

イーサネットブリッジドアプリケーションを使用する場合は、RAP およびそのセグメント内のすべての MAP でブリッジング機能を有効にすることをお勧めします。MAP のイーサネットポートに接続されたすべてのスイッチで VLAN Trunking Protocol (VTP) を使用していないことを確認する必要があります。VTP によってメッシュ全体のトランキングされた VLAN が再設定される場合があるので、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 9: ポイントツーポイントブリッジングの例



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

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



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

イーサネットブリッジングは、次の 2 つの場合に有効にする必要があります。

メッシュ ノードをブリッジとして使用する場合。

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

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

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

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

レンジ：150 ~ 132,000 フィート

メッシュレンジの設定 (CLI)

手順

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



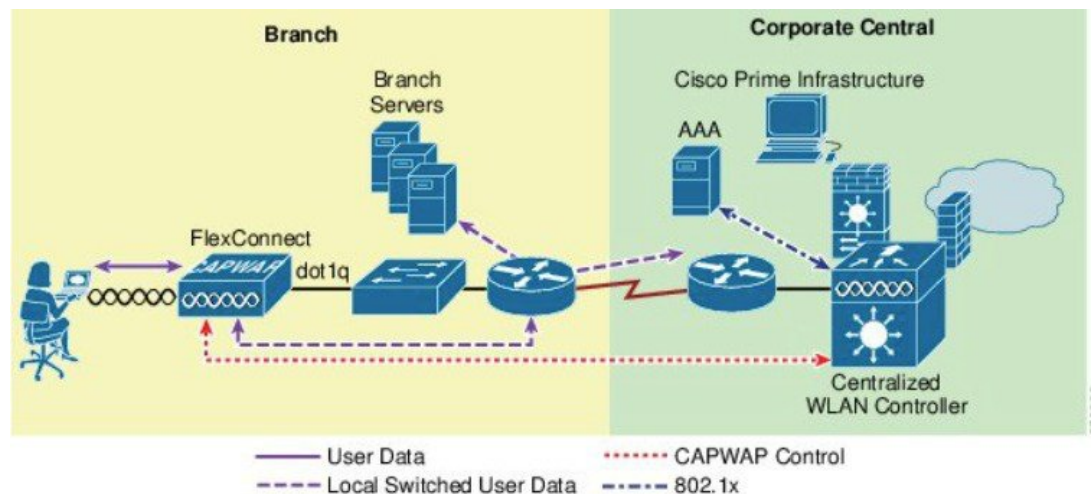
(注) 範囲と AP の密度を見積もる場合、次の URL にある範囲カルキュレータを使用できます。

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

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

リリース 8.7 の Flex+Mesh の概要

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



新しい 8.7 の機能をサポートする Mesh COS AP

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

Flex Mesh 機能は、リリース 8.7 以前でも IOS ベースのメッシュ AP でサポートされていますが、リリース 8.7 では、この機能は COS ベースのメッシュ AP でサポートされています。また、IPv6 も COS ベースのメッシュ AP でサポートされるようになりました。

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

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

フレキシブルアンテナポート設定

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

Flex Mesh AP の実行モード

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

接続モード

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

スタンドアロンモード

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

放棄モードまたは永続 SSID モード

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

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

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



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

Flex Mesh COS AP のモード/状態の遷移

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

スタンドアロンモードの Flex AP に関する設計上の考慮事項

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

COS Flex RAP の特別なスタンドアロンモード

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

既存のフレックス接続 AP モードの設計

- ローカルにスイッチされた WLAN は config.flex ファイルに保存され、Flex-Connect AP はスタンドアロンモードである限り、ローカルの WLAN SSID をブロードキャストします。
- 起動時、Flex-Connect AP はゲートウェイがプロビジョニングされている場合、ローカルにスイッチされた WLAN のブロードキャストのみを開始します。
- COS Flex-Connect AP は、ゲートウェイ情報がある時点で削除されると、スタンドアロンモードから移行し、ローカルにスイッチされた SSID のブロードキャストを停止し、ゲートウェイが再度プロビジョニングされるのを待機します。
- ゲートウェイがプロビジョニングされると、Flex-Connect AP は再度スタンドアロンモードに移行し、ローカルにスイッチされた SSID のブロードキャストを再度開始します。
- 有効なゲートウェイがなければ、ローカルネットワークに到達できずクライアントに接続する理由がないため、Flex-Connect AP は最終的に SSID のブロードキャストを停止します。

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

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

新しい要件をサポートするための設計上の考慮事項

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

```
# CAPWAP ap mesh strict-wired-uplink <true/false>
```
- 新しい設定パラメータの「`strict_wired_uplink`」は、ストレージディレクトリの `config.mesh` ファイルに保存されるため、リブートに関係なく永続的になります。このパラメータのデフォルト値は `false` になります。
- `strict_wired_uplink` 設定は、AP が Flex-Mesh Root AP として設定されている場合のみ有効です。その他のすべての AP モードおよびメッシュ AP 役割では、`strict_wired_uplink` を設定しても有効になりません。
- `strict_wired_uplink` が Flex Mesh Root AP に対して `true` の場合：
 - メッシュの再起動時に、有線アップリンクが直ちに選択される。
 - 有線アップリンクがブラックリストに記載されることがない。

- CAPWAP 稼動タイマーが実行されない。
 - Mesh Reboot タイマーが実行されない。
 - 有線の隣接関係の探索は、インターフェイスがダウンしていても常に true を返す。
 - ワイヤレス バックホールをアップリンクとして選択することはできない。
 - ワイヤレス バック ホールをダウンリンクとして使用し、メッシュの子ノードへの接続を提供できる。
- ゲートウェイの設定チェックによる問題を避けるためには、スタティック IP およびゲートウェイを Flex RAP に設定する必要があります（単なるダミーの IP またはゲートウェイであっても）。
 - スタティック IP とゲートウェイの設定により、Flex RAP はローカル ネットワークへの接続がない場合（つまり、IP とゲートウェイをプロビジョニングする DHCP サーバがない）でも、リブート後にスタンドアロンモードに移行できます。Flex RAP は、ネットワークへの接続が何もない場合であっても、ローカルにスイッチされた SSID をブロードキャストし続けます。
 - IP とゲートウェイが有効でない場合、AP が DHCP サーバに接続されると、DHCP IP がスタティック IP 設定を上書きし、DHCP IP とゲートウェイ設定が使われます。
 - 「永続的な SSID」機能を有効/無効にするシンプルな WLC CLI を提供する予定です。WLC と AP は、この設定を有効にするために通信が必要です。
 - AP の「show mesh config」も、この機能の現在のステータスをダンプします。

メッシュの機能強化の設定

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

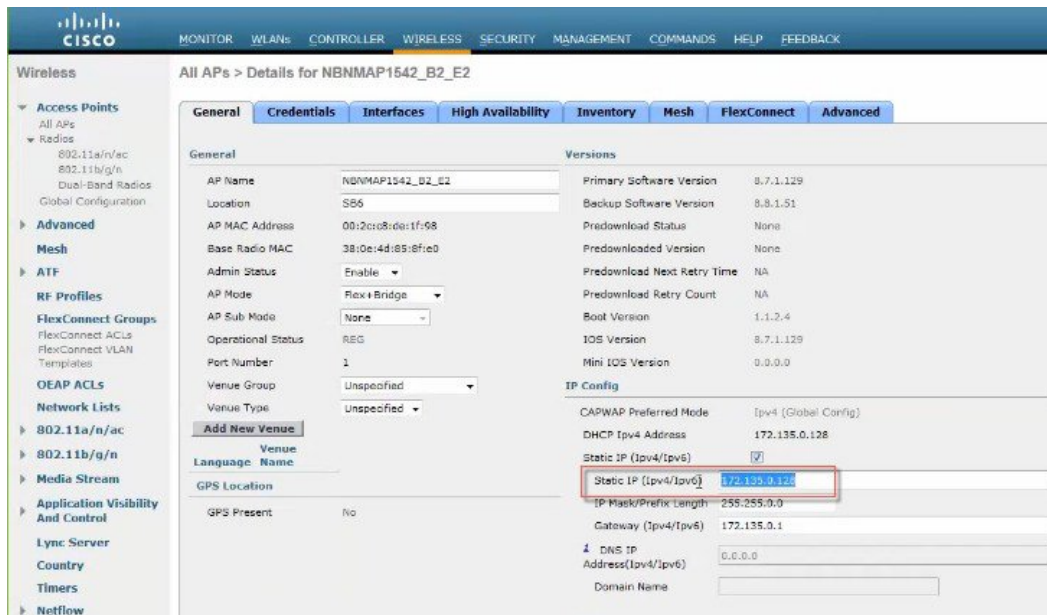
```
NBMAP1542_B2_E2#capwap ap mesh strict-wired-uplink
disable disable strict wired uplink
enable enable strict wired uplink
NBMAP1542_B2_E2#capwap ap mesh strict-wired-uplink
```

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

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

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

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



リリース 8.7 で RAP 永続モードをテストする手順

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

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



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 \(29 ページ\)](#)
- [コントローラ プランニング \(33 ページ\)](#)

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関係するもので、他の特徴はCAPWAPコントローラの設計に関係します。

無線バックホールのデータ 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応じて、802.11a/n/ac/g から選択されます。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。

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



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

各データ レートのバックホール リンクに必要な最小 LinkSNR を [表 1: バックホールのデータ レートと最小 LinkSNR の要件 \(30 ページ\)](#) に示します。

表 1: バックホールのデータ レートと最小 LinkSNR の要件

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

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

[表 2: 802.11n のバックホール データ レートと最小 LinkSNR 要件 \(31 ページ\)](#) 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 packets 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。
必要最小 LinkSNR はデータレートによって計算されます。

表 2: 802.11n のバックホール データ レートと最小 LinkSNR 要件

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

- 必要最小 LinkSNR を計算するために MRC の影響を考慮した場合。表 3: 802.11a/g に必要な LinkSNR の計算 (32 ページ) は、3 本の受信アンテナ (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。

$$\text{LinkSNR} = \text{最小 SNR} - \text{MRC} + \text{フェード マージン (9 dB)}$$

表 3: 802.11a/g に必要な LinkSNR の計算

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

表 4: 2.4 および 5 GHz での AP1552 の LinkSNR 要件 (32 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 4: 2.4 および 5 GHz での AP1552 の LinkSNR 要件

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

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 12	16QAM 3/4	17	1.7	9	24.3
2	MCS 13	64QAM 2/3	20	1.7	9	27.3
2	MCS 14	64QAM 3/4	22	1.7	9	29.3
2	MCS 15	64QAM 5/6	23	1.7	9	30.3



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

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

ホップ数は3か4に制限して、主に、十分なバックホールスループットを維持することをお勧めします。これは、各メッシュ アクセス ポイントはバックホールトラフィックの伝送と受信に同じ無線を使用するためです (つまり、スループットはホップごとに約半分になります)。たとえば、24 Mbps の最大スループットは、最初のホップで約 14 Mbps、2 番目のホップで 9 Mbps、3 番目のホップで 4 Mbps になります。

- RAP ごとの MAP 数

RAP ごとに設定できる MAP 数について、現在ソフトウェアによる制限はありません。ただし、1 台の RAP につき 20 台の MAP に数を制限することをお勧めします。

- コントローラ数

- モビリティ グループごとのコントローラ数は 72 に制限されます。

- コントローラごとにサポートされるメッシュ アクセス ポイントの数。

コントローラ プランニング

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

まなクラスタまたは PoP にグループ化される時、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 5: 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 (34 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 5: コントローラ モデル別にサポートされるメッシュ アクセス ポイント

コントローラ モデル	ローカル AP サポート (非メッシュ) ¹	最大メッシュ AP サポート
5508 ²	500	500
2504 ³	75	75
3504	150	150
WiSM2	500	500
5520	1500	1500
8540	6000	6000

¹ ローカル AP サポートは、コントローラモデル別にサポートされている非メッシュ AP の総数です。

² 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。

³ 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 2500、3504、5508、5520、8540 および WiSM-2 コントローラで完全にサポートされています。The屋内および屋外 AP には base ライセンス (LIC-CT508-Base) で十分です。TheWPlus ライセンス (LIC-WPLUS-SW) は、base ライセンスに含まれます。屋内メッシュ AP には WPlus ライセンスは必要ありません。



第 4 章

メッシュ導入リリース 8.4 の Air Time Fairness

- [メッシュ導入リリース 8.4 の Air Time Fairness \(35 ページ\)](#)

メッシュ導入リリース 8.4 の Air Time Fairness

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

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

前提条件と 8.4 リリースでサポートされる機能

メッシュ ATF は、ワイヤレス LAN コントローラ上の AireOS 8.4 以降のリリースでサポートされます。メッシュ ATF は、1550/128、1570、および他のすべての IOS ベースの AP でサポートされます。

AP	1550 (64 MB)	1550 (128 MB)	1570	3700	1530	1540	1560
機能	—	—	—	—	—	—	—
基本メッシュ	Yes	Yes	Yes	Yes	Yes	Yes	8.4
Flex+メッシュ	Yes	Yes	Yes	Yes	Yes	×	いいえ

AP	1550 (64 MB)	1550 (128 MB)	1570	3700	1530	1540	1560
高速コンバージョン (バックグラウンドスキャン)	いいえ	8.3	8.3	Yes	8.3	いいえ	8.4
RAP の有線クライアント	Yes	Yes	Yes	×	Yes	×	いいえ
MAP の有線クライアント	Yes	Yes	Yes	×	Yes	いいえ	8.4
デিজィチェーン	7.6	7.6	7.6	いいえ	7.6	いいえ	いいえ
LSC	Yes	Yes	Yes	Yes	Yes	×	いいえ
PSK プロビジョニング： MAP-RAP 認証	8.2	8.2	8.2	8.2	8.2	8.5	8.4
メッシュの ATF	いいえ	8.4	8.4	8.4	いいえ	×	いいえ

Cisco Air Time Fairness (ATF) の使用例

公共ホットスポット (スタジアム/空港/会議場/その他)

この場合、パブリック ネットワークは 2 社以上のサービス プロバイダー側や施設側と WLAN を共有しています。各サービスプロバイダーに対するサブスクリバをグループ化して、各グループに特定のダウンストリーム通信時間を割り当てることができます。

Education

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

一般企業、サービス業、小売業

この場合、施設は、従業員とゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービスプロバイダーによってさらに分割できます。ゲストはサービス レベルによってサブ

グループ化し、サブグループごとに一定の通信時間を割り当てることができます（有料のグループには、無料のグループよりも多く割り当てるとなど）。

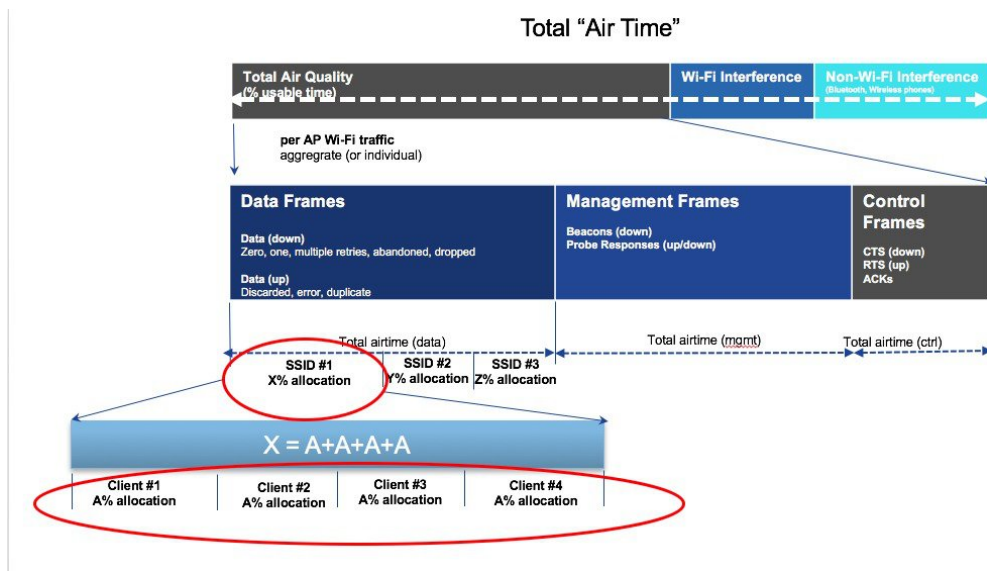
時間を共有するマネージド ホットスポット

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

ATF 機能

ATF 機能：

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



メッシュの ATF 機能の概要

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

Cisco IOS 11n および 11ac 屋内向け AP を配備したエンタープライズ/高密度スタジアム向けなどの大規模な Wi-Fi 導入では、8.1 MR1 および 8.2 リリースにおける SSID ごとの Airtime Fairness (ATF) と、SSID 内のクライアントごとの Airtime Fairness を実現できています。

ATF に対する要求は大規模な屋外ワイヤレス メッシュでも高まっていますが、そこでは、各 Wi-Fi ユーザに（複数の携帯事業者が Wi-Fi ホットスポットを通じて）SLA を適用できる重要な管理機能への要求も高まっています。しかし、Wi-Fi ユーザのトラフィックはすべて無線バックホールにより MAP と RAP 間でブリッジされます。また、バックホール ノード向けの無線バックホールでは SSID という概念が存在しないため、各バックホール ノードの SSID によってポリシーを適用することができません。そのため、屋外ワイヤレス メッシュ AP で各 Wi-Fi ユーザの無線通信時間を公平に扱うための簡単なソリューションは存在しません。しかし Client Access では、シスコのユニファイド ローカル モード AP で処理される方法と同様に、（Client Fair Sharing ポリシーの有無に関わらず）SSID を介して利用時間の公平性を簡単に確保できます。

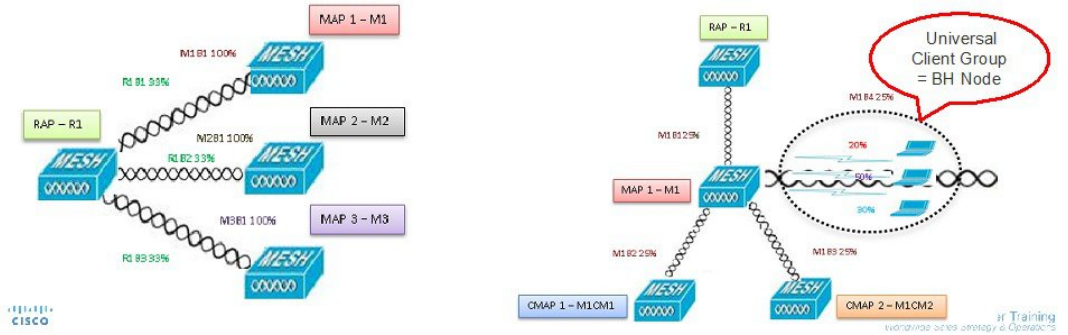
ATF をサポートするメッシュ ソリューションの概要を説明する前に、ATF について要約しておきましょう。Airtime Fairness (ATF) とは基本的に、SSID によって接続したクライアントに対して、ダウンストリーム方向の AP 無線通信時間を調整/適用するための機能です。ATF により、ワイヤレス ネットワークの各ユーザは無線通信時間の点で公平に扱われるため、SLA を（追加で）適用できます。つまり、特定 AP のワイヤレス キャパシティが特定のグループやユーザに偏ることを防止できる、重要な管理機能となります。サービスレベル契約 (SLA) とは、サービスプロバイダーが提供するサービス レベルを定義した、（内/外いずれかの）サー

ビスプロバイダーとエンドユーザとの間の契約です。SLA は顧客が受けるサービスを定義するため、アウトプットベースと言えます。

メッシュアーキテクチャでは一般に、無線バックホールで接続されたメッシュ AP（親/子 MAP）が同一チャンネルでメッシュ（親/子 MAP 間）接続します（拡張サブ無線バックホールについては後で説明します）。一方、ルート AP はコントローラに有線接続され、MAP はコントローラにワイヤレス接続されます。そのため、すべての CAPWAP や Wi-Fi のトラフィックは、無線バックホールおよび RAP によりコントローラに接続されます。物理的な配置について言えば、RAP は一般にルーフトップに配置され、複数のホップにある MAP は（メッシュネットワークのセグメント化ガイドラインに基づき）間隔を置いて配置されます。そのためメッシュツリー内の各 MAP は、各 MAP が同じメディアにアクセスするにも関わらず、本体のダウンストリームキャパシティを 100% ユーザに提供できます。では、メッシュを使用しないシナリオと比較しましょう。たとえばアリーナでは、隣り合う部屋に設置された隣接するローカルモード AP により、同一チャンネル上でそれぞれのクライアントに 100% のダウンストリームキャパシティで通信を提供することになります。このため、同じメディアにアクセスする 2 台の隣接 AP に接続されたクライアントに ATF を適用できません。メッシュツリーの MAP についても、同じことが言えます。屋外/屋内メッシュ AP では、メッシュでないローカルモード AP が ATF をサポートするのと同様に、一般クライアントが接続されるクライアント AP で ATF をサポートしている必要があります。また、クライアント AP 上のクライアント～RAP 間（1 ホップ）や MAP～RAP 間（複数ホップ）をブリッジする無線バックホールにおいても同様です。同じ SSID/ポリシー/ウェイト/Client Fair Sharing モデルを使用している無線バックホールで ATF をサポートするのは注意が必要です。無線バックホールには SSID がないため、常に、隠れたバックホールノードによってトラフィックをブリッジします。その後、RAP または MAP の無線バックホールでは、ダウンストリームの無線通信時間はバックホールノードの数に基づいて等しく公平に共有されます。このアプローチにより先述の問題を解決し、ワイヤレスメッシュネットワーク全体のユーザに公平性を提供します。つまり、2 番目のホップ MAP に接続するクライアントが 1 番目のホップ MAP に接続されたクライアントを失速させる中で、（MAP の Wi-Fi ユーザが物理的には分離されているものの）2 番目のホップ MAP が無線バックホールによって 1 番目のホップ MAP に接続している場合に役立ちます。このシナリオでは、無線バックホールが一般的なユニバーサルクライアントアクセス機能を通じて通常のクライアントにも接続を提供できる場合、ATF は通常のクライアントを単一ノードとみなし、それらをグループ化します。ノードの数（バックホールノード+通常のクライアントに対する単一ノード）に基づいて、ダウンストリームの無線通信時間を等しく公平に共有します。次のセクションでは、このソリューションを設計に組み込む方法についての詳細を説明します。

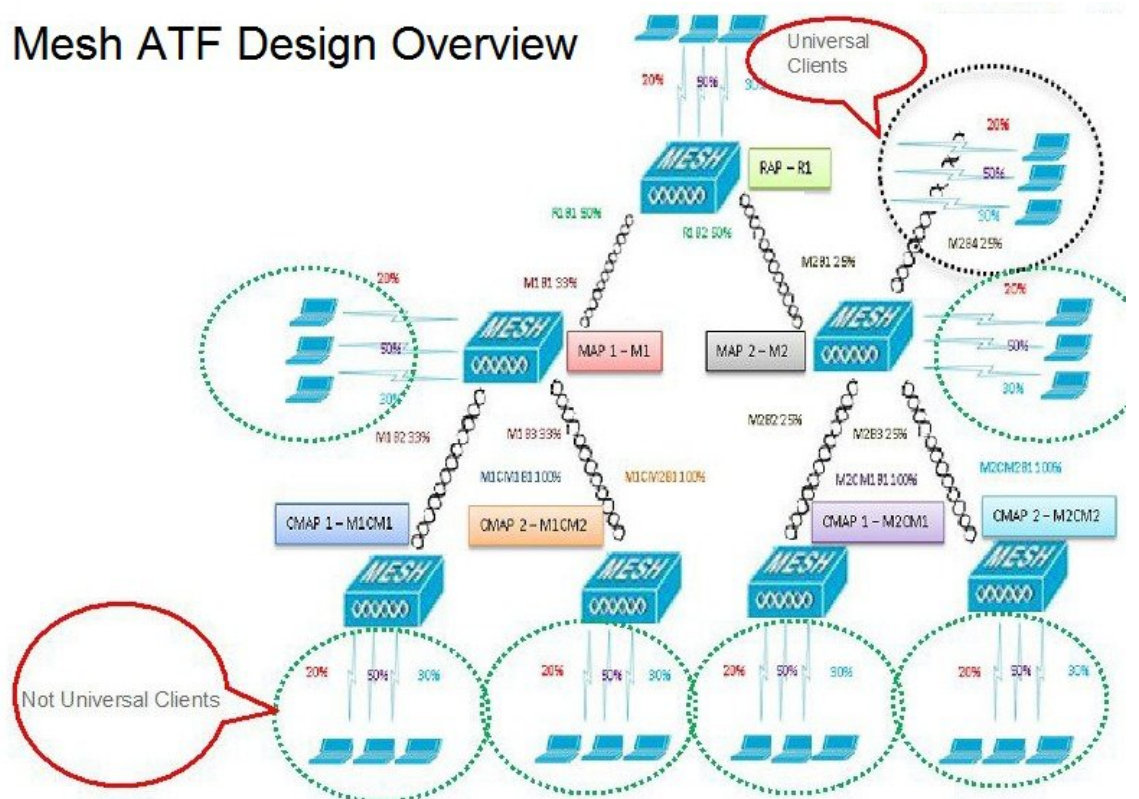
Mesh ATF Optimization on the Backhaul

- On Mesh Client Access Link radio will use per SSID/policy weight/client fair sharing model
- Client Group on the Universal Access Radio considered as one BH Node
- Strict or Optimized enforcement can be applied on the backhaul



メッシュ設計の全体像はこのようになります。

Mesh ATF Design Overview



ATF の動作モード

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

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

メッシュの ATF の設定

メッシュの ATF を設定するには、次の手順を実行します。

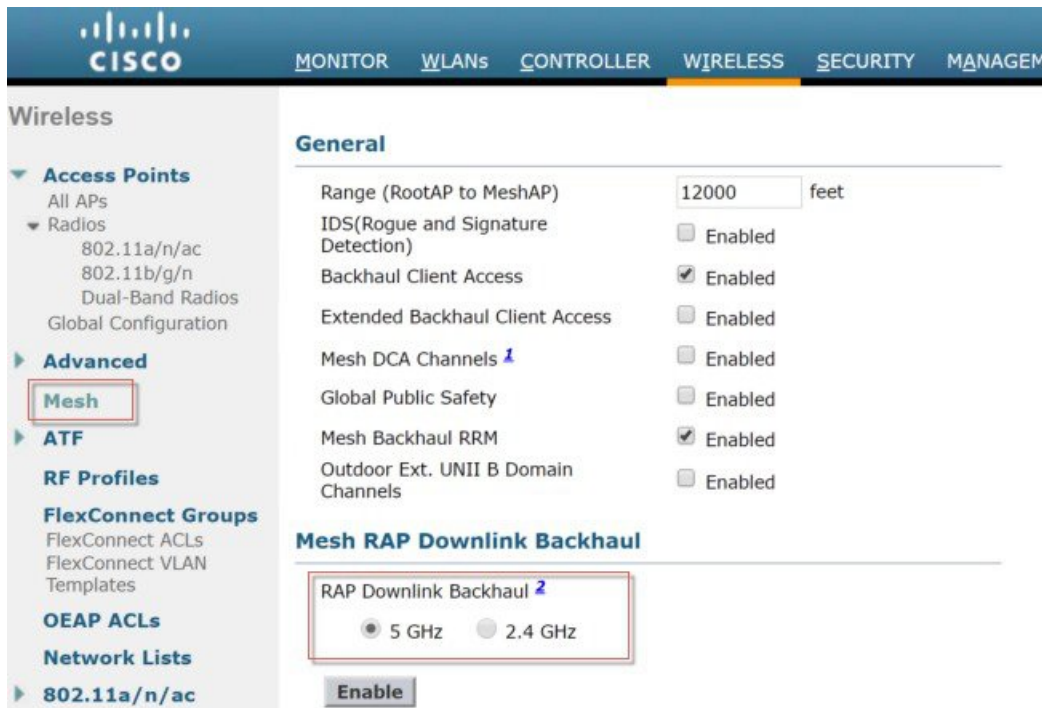
ステップ 1 [Backhaul Client Access] を有効または無効に設定します。

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

The screenshot shows the Cisco Wireless configuration interface. The 'Mesh' tab is selected in the left sidebar. Under the 'General' section, the 'Backhaul Client Access' checkbox is checked and highlighted with a red box. Other settings include 'Range (RootAP to MeshAP)' set to 12000 feet, 'IDS (Rogue and Signature Detection)' disabled, 'Extended Backhaul Client Access' disabled, 'Mesh DCA Channels' disabled, 'Global Public Safety' disabled, 'Mesh Backhaul RRM' disabled, and 'Outdoor Ext. UNII B Domain Channels' disabled.

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

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



The screenshot shows the Cisco Wireless configuration interface. The left sidebar has 'Mesh' selected under 'Advanced'. The main area is titled 'General' and contains several settings:

- Range (RootAP to MeshAP): 12000 feet
- IDS(Rogue and Signature Detection): Enabled
- Backhaul Client Access: Enabled
- Extended Backhaul Client Access: Enabled
- Mesh DCA Channels: Enabled
- Global Public Safety: Enabled
- Mesh Backhaul RRM: Enabled
- Outdoor Ext. UNII B Domain Channels: Enabled

Below the 'General' section is the 'Mesh RAP Downlink Backhaul' section, which includes:

- RAP Downlink Backhaul: 5 GHz 2.4 GHz
-

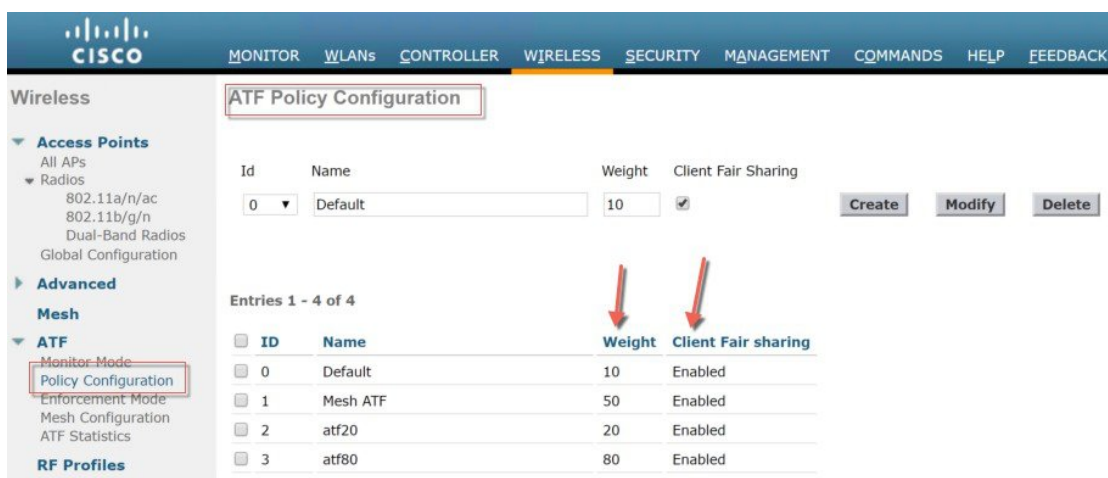
ステップ3 [ATF Policy] の [Weight] と [Client Sharing] を設定します

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

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

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

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



The screenshot shows the 'ATF Policy Configuration' page. The left sidebar has 'Policy Configuration' selected under 'ATF'. The main area displays a table of ATF policies:

Id	Name	Weight	Client Fair Sharing
0	Default	10	<input checked="" type="checkbox"/>

Buttons: Create, Modify, Delete

Entries 1 - 4 of 4

ID	Name	Weight	Client Fair sharing
0	Default	10	Enabled
1	Mesh ATF	50	Enabled
2	atf20	20	Enabled
3	atf80	80	Enabled

Red arrows point to the 'Weight' and 'Client Fair sharing' columns in the table below.

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

図 10:

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

The screenshot displays the Cisco Wireless Configuration interface. The left sidebar contains a navigation tree with the following items: Access Points (All APs, Radios: 802.11a/n/ac, 802.11b/g/n, Dual-Band Radios, Global Configuration), Advanced, Mesh, ATF (Monitor Mode, Policy Configuration, Enforcement Mode, Mesh Configuration, ATF Statistics), RF Profiles, FlexConnect Groups (FlexConnect ACLs, FlexConnect VLAN Templates), OEAP ACLs, Network Lists (802.11a/n/ac, 802.11b/g/n), Media Stream, Application Visibility And Control, Lync Server, and Country. The main configuration area is titled 'ATF Enforcement Mode Configuration'. It features three radio buttons for 'AP Name', 'AP Group Name', and 'Network', all set to 'None'. Below these are checkboxes for 'Radio Type' (802.11a and 802.11b). The 'Enforcement Type' section has radio buttons for 'Optimized' (selected) and 'Strict'. The 'Mode' section has 'Enable' and 'Disable' buttons. The 'Policy Enforcement' section includes dropdown menus for 'WLAN Id' and 'Policy Id' (both set to 'None'), and text input fields for 'SSID Name' and 'Policy Name'. 'Add' and 'Set to Default' buttons are located at the bottom of the policy enforcement section.

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

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

Wireless

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Mesh Universal Access Client Airtime Allocation

AP Name Radio Type Default % Alloc Per Node No of Nodes Override Override allocation on client

v51_map1_ap1572 802.11a 10 2 30 (5% - 90%)

AP Name	Radio Type	No of Nodes	Default % Alloc Per Node	Current % Allocation on Client Access Node	Current % Allocation on Backhaul Node
v51_map2_ap3700	802.11b	0	100	NA	NA
v51_map2_ap3700	802.11a	0	100	NA	NA
v51_map1c_ap3700	802.11b	0	100	NA	NA
v51_map1c_ap3700	802.11a	0	100	NA	NA
v51_map1b_ap370C	802.11b	0	100	NA	NA
v51_map1b_ap370C	802.11a	0	100	5	95
v51_map1_ap3700	802.11b	0	100	NA	NA

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - ATF
 - Monitor Mode
 - Policy Configuration
 - Enforcement Mode
 - Mesh Configuration
 - ATF Statistics
 - RF Profiles



第 5 章

サイトの準備と計画

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

- [サイトの調査 \(45 ページ\)](#)
- [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 \(54 ページ\)](#)
- [屋内メッシュと屋外メッシュの相互運用性 \(80 ページ\)](#)

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。サイトサーベイでは、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こと、作業は常に楽になります。
- 作業を遂行するための適切なツールや機器があるか?



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

屋外サイトの調査

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

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

メッシュ リンクの設計には、次の値を推奨します。

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

見通し (Line of Sight) 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5GHz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と電波を向けさせない限り、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ために、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、多湿環境は見通し (Line of Sight) に多少の影響を与え、若干の損失 (「レインフェード」や「フェードマージン」とも呼ばれる) を生みますが、それによるメッシュリンクへの影響はわずかです。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 11: ポイントツーポイントリンクのフレネルゾーン \(48 ページ\)](#) に示すように、フレネルエリアの60~70%に障害物がなければ、リンクを確立できます。

図 11: ポイントツーポイントリンクのフレネルゾーン

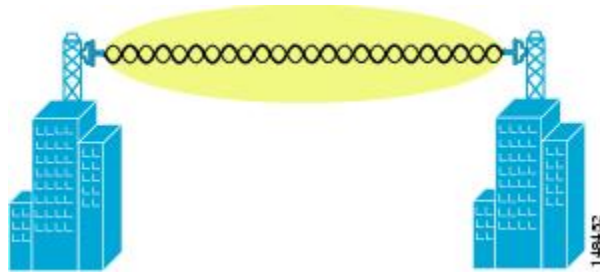


図 12: フレネルゾーン内の一般的な障害物 (48 ページ) は、障害物のあるフレネルゾーンを示しています。

図 12: 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)

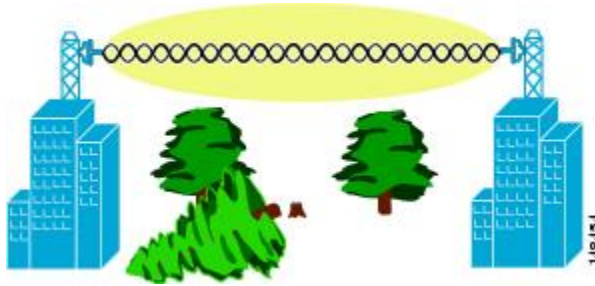
通常、最初のフレネルゾーンの 60% のクリアランスが推奨されるため、上の公式を 60% のフレネルゾーンクリアランスで表すと、次のようになります。

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

これらの計算は、平坦地に基づいたものです。

図 13: フレネルゾーンの障害物の除去 (49 ページ) は、ワイヤレス信号のフレネルゾーンにある障害物の除去を示しています。

図 13: 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、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れノードが発生することがあります。

図 14: 隠れノード

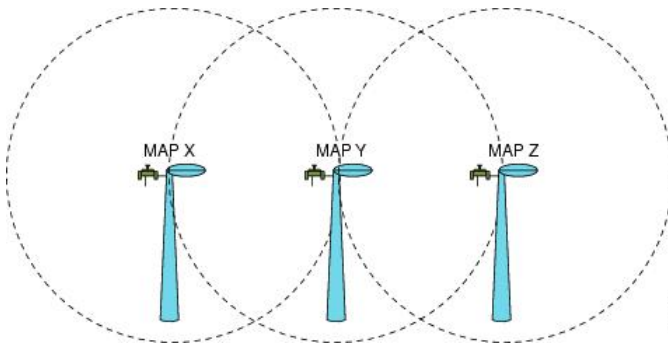


図 14: 隠れノード (49 ページ) は、次の 3 つの MAP を示します。

- MAP X
- MAP Y
- MAP Z

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

すべての WLAN で何らかの時点で隠しノードコリジョンが生じる可能性があります。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下では、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。また Radio Resource Management (RRM) 機能は 2.4 GHz 帯で動作しますが、これによって、セルの調整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下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せん。
- 優先される親は同じブリッジグループ名（BGN）に属します。設定された優先される親が同じ BGN に属さず、他の親が利用可能でない場合、子はデフォルトの BGN を使用して親 AP に join します。

優先される親の設定

優先親を設定するには、次のコマンドを入力します。

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

値は次のとおりです。

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



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

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

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

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

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



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

3. [Apply] をクリックします。



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

関連コマンド

優先親の選択に関連するコマンドは次のとおりです。

- 設定された親を削除するには、次のコマンドを入力します。

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

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

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

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

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

Cisco AP Identifier..... 9
Cisco AP Name..... MAP1
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... 12:12:12:12:12:12
IP Address Configuration..... DHCP
IP Address..... 209.165.200.225
IP NetMask..... 255.255.255.224
CAPWAP Path MTU..... 1485
Domain.....
Name Server.....
Telnet State..... Disabled
Ssh State..... Disabled
Cisco AP Location..... default location
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... 4404
Primary Cisco Switch IP Address..... 209.165.200.230
Secondary Cisco Switch Name.....
```

```

Secondary Cisco Switch IP Address..... Not Configured
Tertiary Cisco Switch Name..... 4404
Tertiary Cisco Switch IP Address..... 3.3.3.3
Administrative State ..... ADMIN_ENABLED
Operation State ..... REGISTERED
Mirroring Mode ..... Disabled
AP Mode ..... Local
Public Safety ..... Global: Disabled, Local: Disabled
AP subMode ..... WIPS
Remote AP Debug ..... Disabled
S/W Version ..... 5.1.0.0
Boot Version ..... 12.4.10.0
Mini IOS Version ..... 0.0.0.0
Stats Reporting Period ..... 180
LED State..... Enabled
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
Number Of Slots..... 2
AP Model..... AIR-LAP1252AG-A-K9
IOS Version..... 12.4(10:0)
Reset Button..... Enabled
AP Serial Number..... serial_number
AP Certificate Type..... Manufacture Installed
Management Frame Protection Validation..... Enabled (Global MFP Disabled)
AP User Mode..... CUSTOMIZED
AP username..... maria
AP Dot1x User Mode..... Not Configured
AP Dot1x username..... Not Configured
Cisco AP system logging host..... 255.255.255.255
AP Up Time..... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time..... 4 days, 06 h 15 m 00 s
Join Date and Time..... Mon Mar 3 06:19:47 2008

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

```

共同チャネルの干渉

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

ワイヤレスメッシュネットワークのカバレッジに関する考慮事項

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

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

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

セルのプランニングと距離

Cisco 1500 シリーズ アクセス ポイント用

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

非音声ネットワークでのセル計画と距離について、次の値を推奨します。

- RAP と MAP の比率：推奨最大比率は、RAP ごとに 20 の MAP です。
- AP 間の距離：各メッシュ アクセス ポイント間に 2000 フィート（609.6 m）以下の間隔をあけることを推奨します。バックホール上でメッシュネットワークを拡張する（クライアント アクセスなし）場合、セルの半径には 1000 フィート（304.8 m）を使用してください。
- ホップ カウント：3～4 ホップ
 - 1 平方マイル（1 マイル = 52,802 フィート）は 9 セルに相当し、およそ 3 つまたは 4 つのホップでカバーできます（[図 15: 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](#)（55 ページ）および [図 16: 2.3～2.7 のパス損失指数](#)（55 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 1.310×10^6 で、1 平方マイルあたりのセルは 25 個です。（[図 17: 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](#)（56 ページ）および [図 18: 2.5～3.0 のパス損失指数](#)（56 ページ）を参照）。

図 15: 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

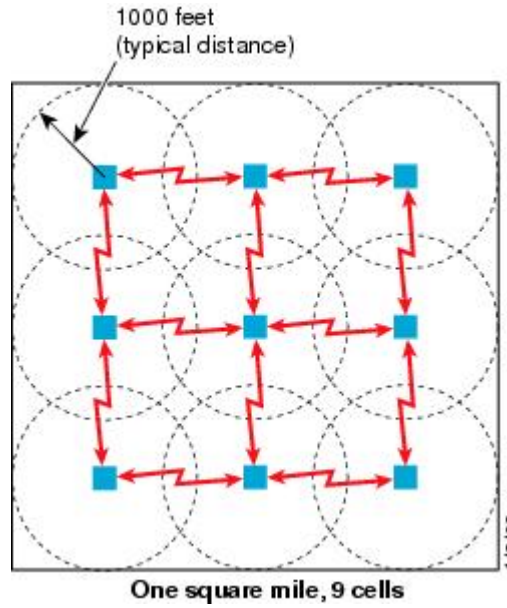


図 16: 2.3 ~ 2.7 のパス損失指数

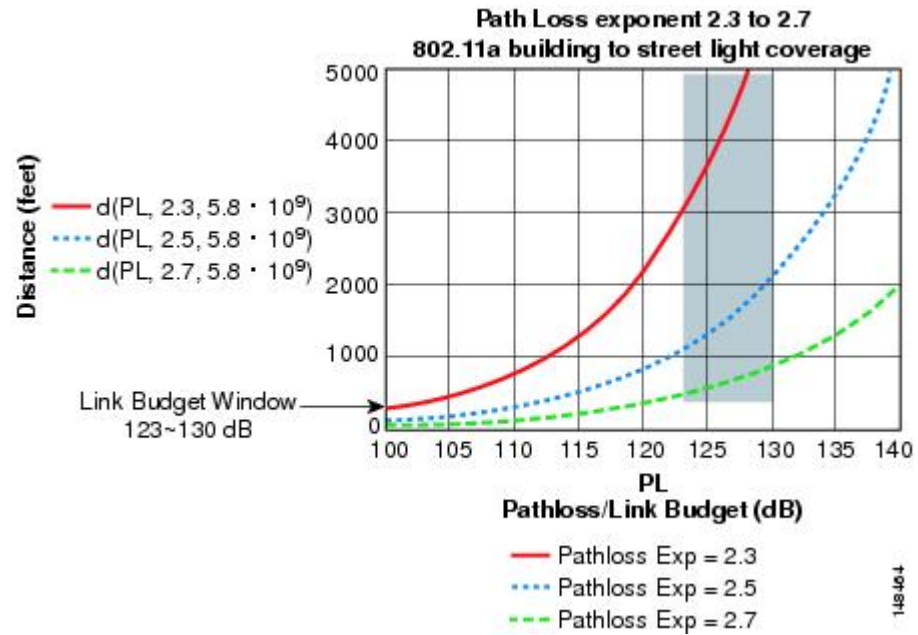


図 17: 非音声メッシュ ネットワークにおける半径 600 フィートのセルとアクセス ポイントの位置

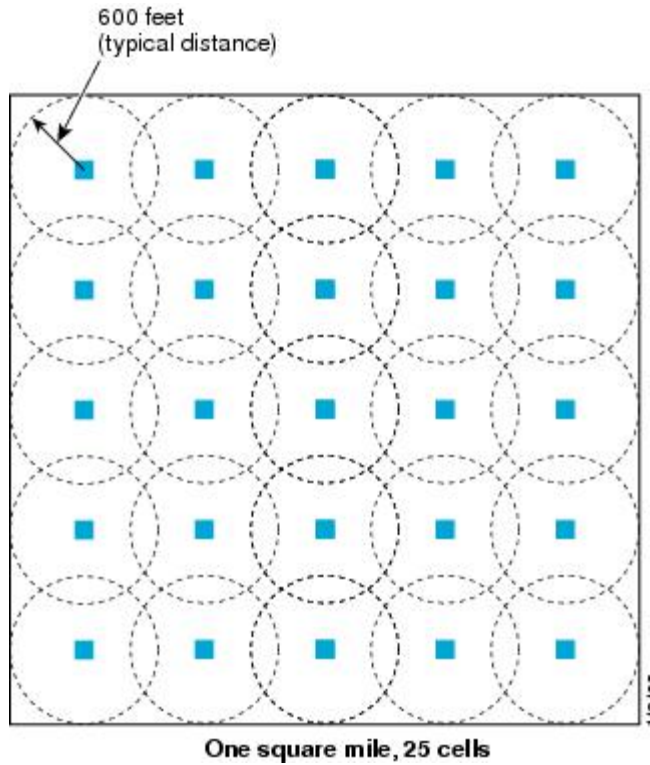
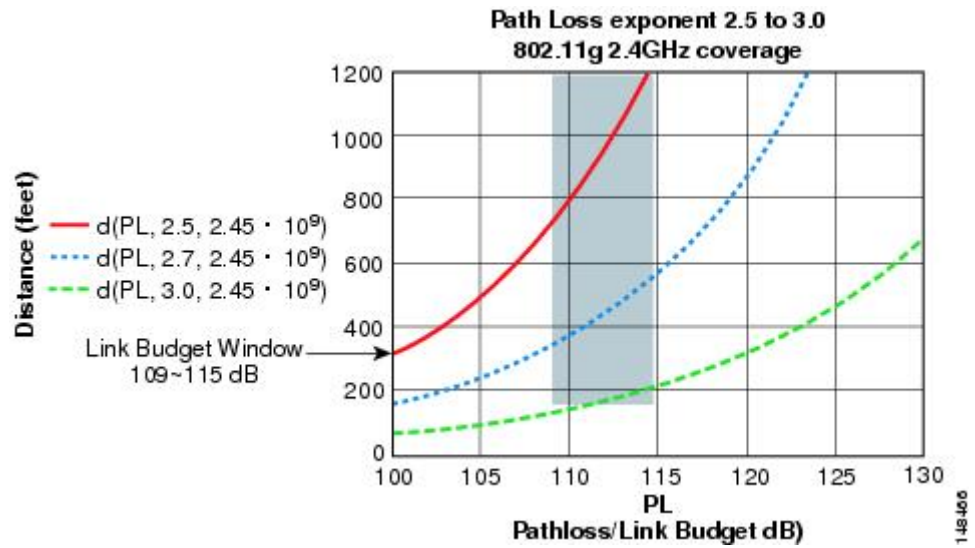


図 18: 2.5 ~ 3.0 のパス損失指数



Cisco 1550 シリーズ AP 用

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

AP1500 シリーズは 802.11n に対応しているため、到達範囲とキャパシティは比較的優れています。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、チャンネル結合などの 802.11n の利点もあります。1552 アクセスポイントは、比較的大容量のセルを提供できます。



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

2.4 および 5 GHz 帯の 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 6: -A/-B ドメインの 2.4 GHz 帯のリンク バジレット比較 (57 ページ) を参照してください。

表 6: -A/-B ドメインの 2.4 GHz 帯のリンク 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 1562 (-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	2412 ~ 2462 MHz
エア インターフェイス	802.11b/g/n	802.11a/b/g/n/acW2	802.11a/b/g/n/acW2	802.11 a/b/g/n
チャンネル帯域幅	20 MHz	20 MHz	—	20 MHz
Tx 空間ストリーム数	2	1562I の場合は 3SS、1562E/D モデルの場合は 2SS	1562I の場合は 3SS、1562E/D モデルの場合は 2SS	3SS
PHY データ レート	最大 144 Mbps ⁴	3SS では最大で 216 Mbps、2SS では 144 Mbps	3SS では最大で 216 Mbps、2SS では 144 Mbps	最大 216 Mbps
供給 Tx 電力	28 dBm、複合 ⁵	1562I の場合は 29 dBm 1562E/D の場合は 27 dBm	1562I の場合は 29 dBm 1562E/D の場合は 27 dBm	30 dBm

パラメータ	Cisco 1552 (-A ドメイン)	Cisco 1532 (-A ドメイン)	Cisco 1562 (-A ドメイン)	Cisco 1572 (-B ドメイン)
Rx 感度	6 Mbps で -94 dBm 54 Mbps で -79 dBm 150 Mbps で -73 dBm	6 Mbps で -92 dBm 54 Mbps で -76 dBm 216 Mbps で -71 dBm	6 Mbps で -92 dBm 54 Mbps で -76 dBm 216 Mbps で -71 dBm	6 Mbps で -93 dBm 54 Mbps で -81 dBm 216 Mbps で -76 dBm
受信チャンネル数	3	3 または 2	3 または 2	4
Rx ダイバーシティ	MRC	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 (外部アンテナ使用)	0.5 dB (外部アンテナ使用)	0.5 dB (外部アンテナ使用)

⁴ 2.4 GHz での 40 MHz チャンネル 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。

⁵ 複合電力は、AP1552 で 2 つの送信ストリームが有効な場合の電力です。

5 GHz 帯については、[表 7: -A/-B ドメインの 5 GHz 帯のリンク バジェット比較 \(58 ページ\)](#) を参照してください。

表 7: -A/-B ドメインの 5 GHz 帯のリンク 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 1562 (-A/B ドメイン)	Cisco 1572 (-B ドメイン)
周波数帯域	5745 ~ 5825 MHz	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	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	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/b/g/n/acW2	802.11a/b/g/n/acW2	802.11a/n/ac
チャンネル帯域幅	20 MHz、40 MHz	20 MHz、40 MHz、80 MHz	20 MHz、40 MHz、80 MHz	20 MHz、40 MHz、80 MHz

パラメータ	Cisco 1552 (-A ドメイン)	Cisco 1532 (-A ドメイン)	Cisco 1562 (-A/B ドメイン)	Cisco 1572 (-B ドメイン)
Tx 空間ストリーム数	2	2	3 または 2	3
PHY データ レート	最大 300 Mbps	最大 300 Mbps	1.300/867 Mbps	最大 1.3 Gbps
供給 Tx 電力	28 dBm、複合	27 dBm	29 または 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 -94 dBm 54 Mbps で -80 dBm 1300 Mbps で -65 dBm	6 Mbps で -94 dBm 54 Mbps で -80 dBm 1300 Mbps で -65 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) とリンクバジレ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 間リンクバジレ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 9Mbps とします。



(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。

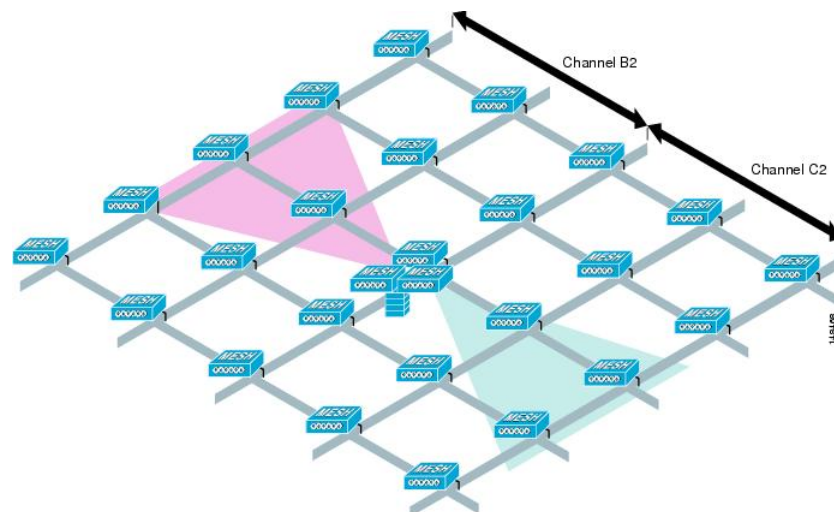
Cisco レンジカルキュレータの前提条件

- 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レンジカルキュレータが編集されていますが、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。
- レンジ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。
- レンジ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（またはアンテナ利得）、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。

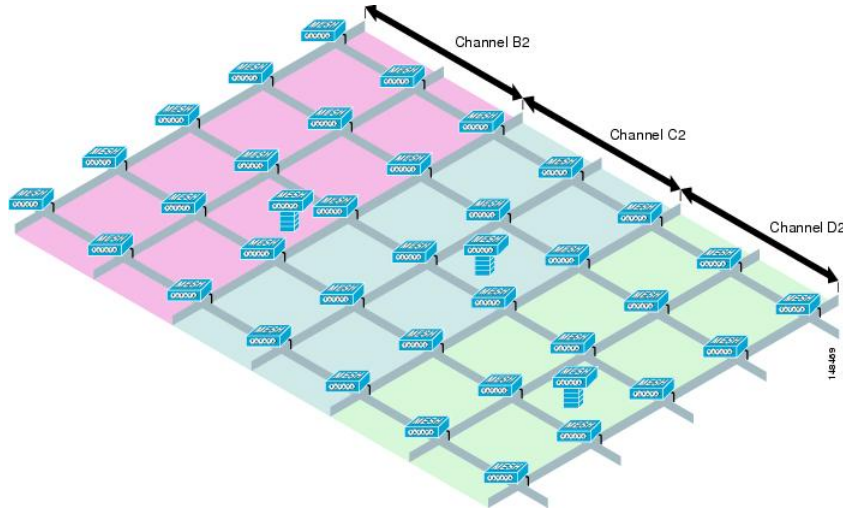
図 19: 複数の RAP の PoP (60 ページ) に示した RAP は、開始点に過ぎません。ゴールは、RAP のロケーションを RF アンテナの設計と組み合わせて使用し、セルのコア内で MAP に適切な RF リンクを確立することです。これは、RAP の物理的なロケーションをセルの端にでき、指向性アンテナが、セルのセンターへのリンクの確立に使用されることを意味します。そのため、図 19: 複数の RAP の PoP (60 ページ) に示すように、RAP の有線ネットワークのロケーションが、複数のセルの RAP に対するホストの役割をする可能性があります。

図 19: 複数の RAP の PoP



基本のセルの構成が決まれば、そのセルを複製して、もっと広いエリアをカバーできるようになります。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ンネルを使用するか、セルごとにバックホールチャンネルを変えるかを定める必要があります。図 20: 複数の RAP および MAP のセル (61 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ンネル (B2、C2、および D2) が選択され、セル間の共同チャンネル干渉を減らしています。

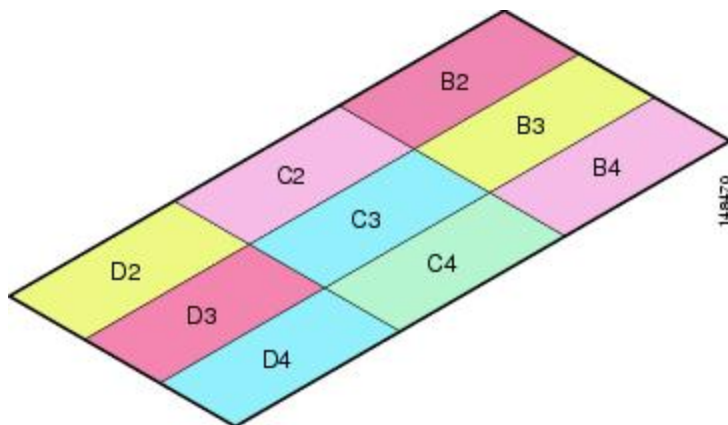
図 20: 複数の RAP および MAP のセル



さまざまなチャンネルを選択すると、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ンネル干渉が減ります。MAPはseekモードにフォールバックして隣接セルのネイバーを検出する必要があるためです。高トラフィック密度のエリアで、共同チャンネル干渉は、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、別のチャン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、同じチャンネルを使用しても、パフォーマンスはほとんど低下しないと考えられます。

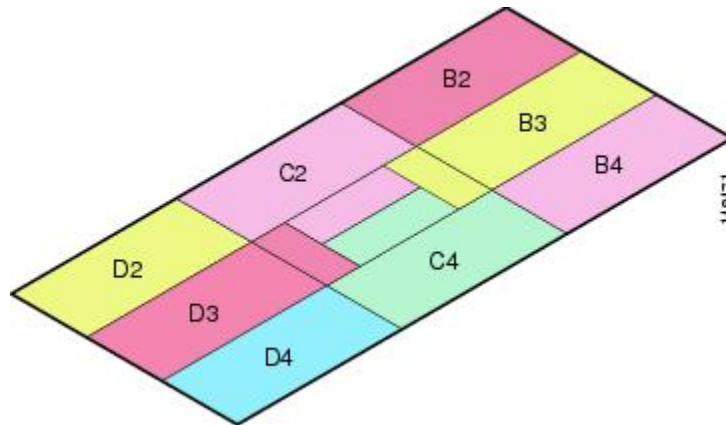
複数のセルをレイアウトする際には、標準のWLAN計画に似たチャンネル計画を使用し、チャンネルのオーバーラップを回避してください（図21:さまざまなセルのレイアウト（61ページ）を参照）。

図 21: 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、チャンネル計画でチャンネルオーバーラップを最小にする必要もあります（図22:フェールオーバーカバレッジ（62ページ）を参照）。

図 22: フェールオーバー カバレッジ



メッシュ アクセス ポイントのコロケーション

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

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

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

隣接チャネルでの AP1500 のコロケーション

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

コロケーションされた 2 つの AP1500 が、5.5 dBi 全方向性アンテナ付きのチャンネル 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、2.4 GHz 帯のローカル クライアント AP、および 5 GHz 帯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。
 - Radio Resource Manager (RRM) により、推奨される RSSI、PER (パケットエラーレート)、SNR、CU (チャンネル使用率)、セル カバレッジ、およびカバレッジ ホールの設定を 802.11b/g/n/ac 無線に実装できます。

図 23: 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

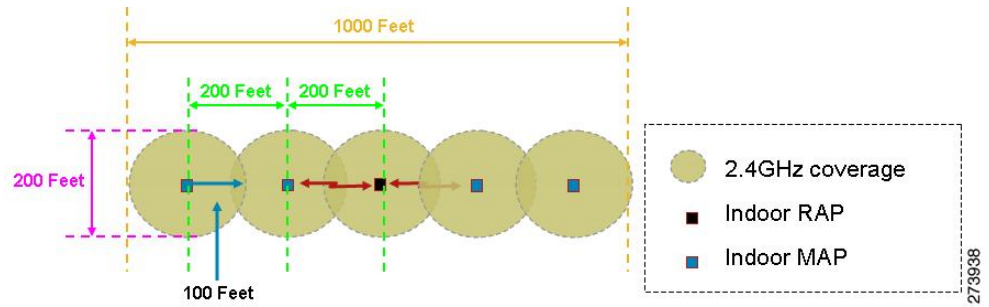
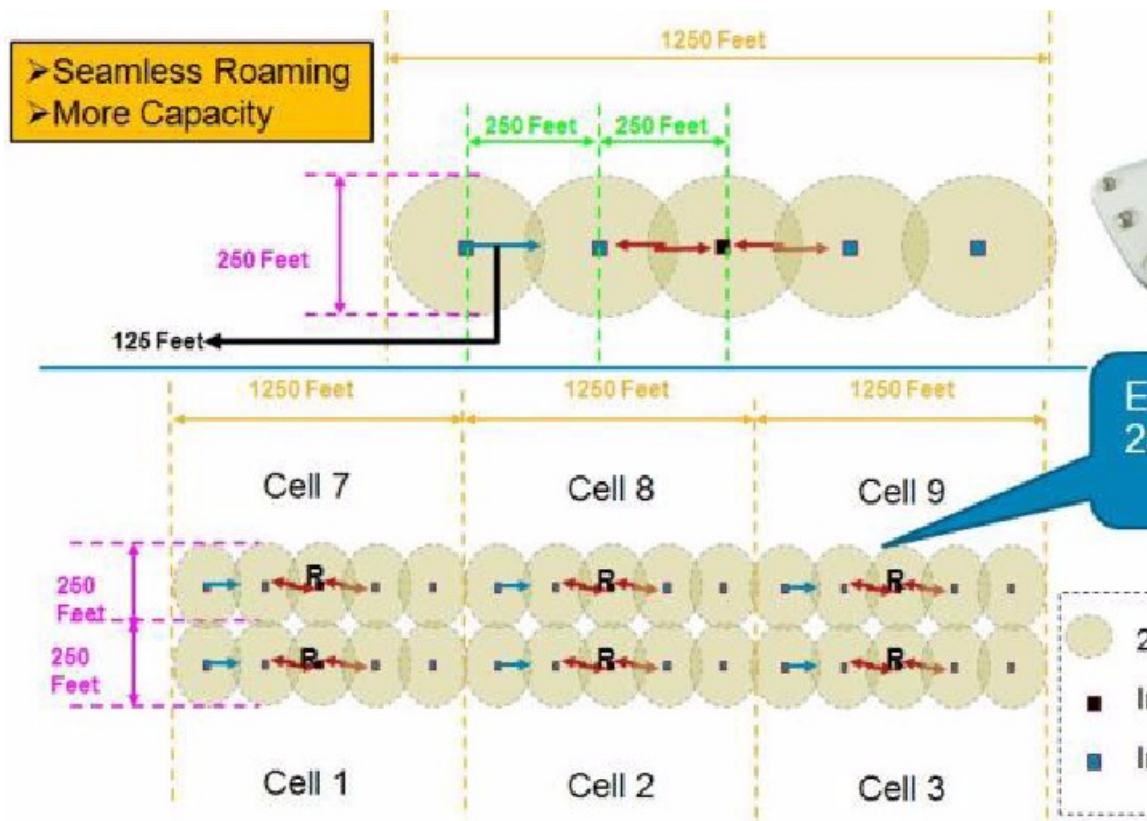


図 24: 屋内 11n メッシュ ネットワークにおける半径 125 フィート (38 m) のセルとアクセス ポイントの位置



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

メッシュ AP バックグラウンド スキャン リリース 8.3

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

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

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

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



(注) バックグラウンド スキャンのこのような実装は、Marvell ベースの AP に適用されます。具体的には、AP1550、AP1570、AP1560、および IW3702 です。

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

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

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

タイマー、およびロードの値に基づきます。オフチャネルネイバーの場合、AdjustedEase 値が使用され、オフチャネルごとに最適なネイバーが最高の AdjustedEase 値に基づいて特定されます。StickyEase はオンチャネル親のみに適用されます。

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

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

	親の損失の検出/ キープアライブ タイマー	チャンネル スキャン/ シーク	DHCP/CAPWAP 情報	ホップごとの時間 (秒)
規格	21 / 3 秒	すべての 2.4 および 5 GHz チャンネルの スキャン/ シーク	CAPWAP の更新/ 再スタート	48.6*
速い	7 / 3 秒	同じブリッジグループにあるチャンネルのみの スキャン/ シーク	DHCP および CAPWAP の維持	20.5*
Very Fast	4 / 1.5 秒	同じブリッジグループにあるチャンネルのみの スキャン/ シーク	DHCP および CAPWAP の維持	15.9*
CCN（クリアチャネル通知）/バックグラウンド スキャン Fast/Very Fast	50ms の場合は 4 / 3 秒	同じブリッジグループにあるチャンネルのみの スキャン/ シーク	DHCP および CAPWAP の維持	8 ～ 10 秒

DFS と非 DFS チャンネル スキャン

非 DFS チャンネル スキャン

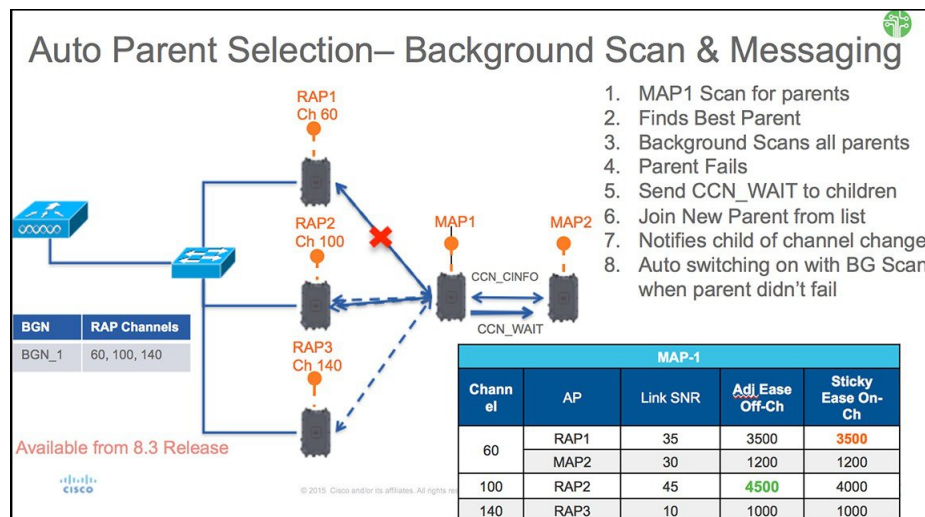
- MAP は定期的にオフチャネルになり、選択されたオフチャネルで NDReq ブロードキャスト パケットを送信します。さらに、すべての「到達可能な」ネイバーから NDResp パケットを受信します。
- オフチャネル スキャンは 3 秒ごとに発生します。オフチャネルごとに最大で 50 ミリ秒維持されます。

- 各ネイバーから適切にヒアリングするには、50 ミリ秒の滞留時間内に少なくとも4つのメッセージを送信できるよう、NDRReq が 10 ミリ秒ごとに伝送される必要があります。

DFS チャンネル スキャン

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

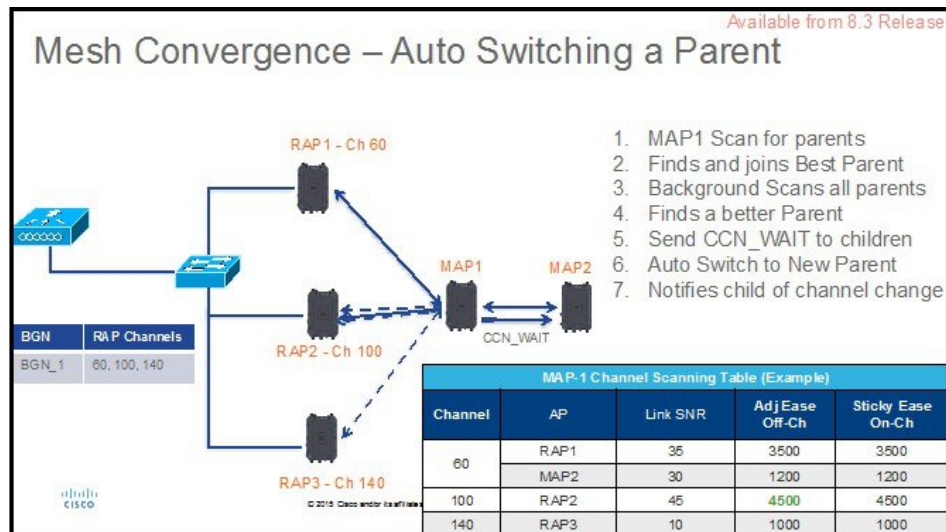
- DFS チャンネル上のオフチャンネル スキャン中に MAP がパケットを受信できるようにするには、最後の 50 ミリ秒に送信・受信がない場合に、他のすべてのオンチャンネル DFS ネイバーが AWPP メッシュ ビーコンを伝送する必要があります。
- これらのメッシュ ビーコンは、DFS チャンネル上でオフチャンネルを実行している MAP が「安全に送信できる」と宣言してオフチャンネルのアクティビティを実行できます。



上図は、「Standard」または「Fast/Very Fast」な構成の典型的なオフチャンネル コンバージェンス プロセスを示しています。



(注) 表内のタイマーは、図示のためにすぎません。



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

メッシュ コンバージェンスの設定

設定手順は非常に簡単で、新しいバックグラウンド スキャン機能呼び出します。

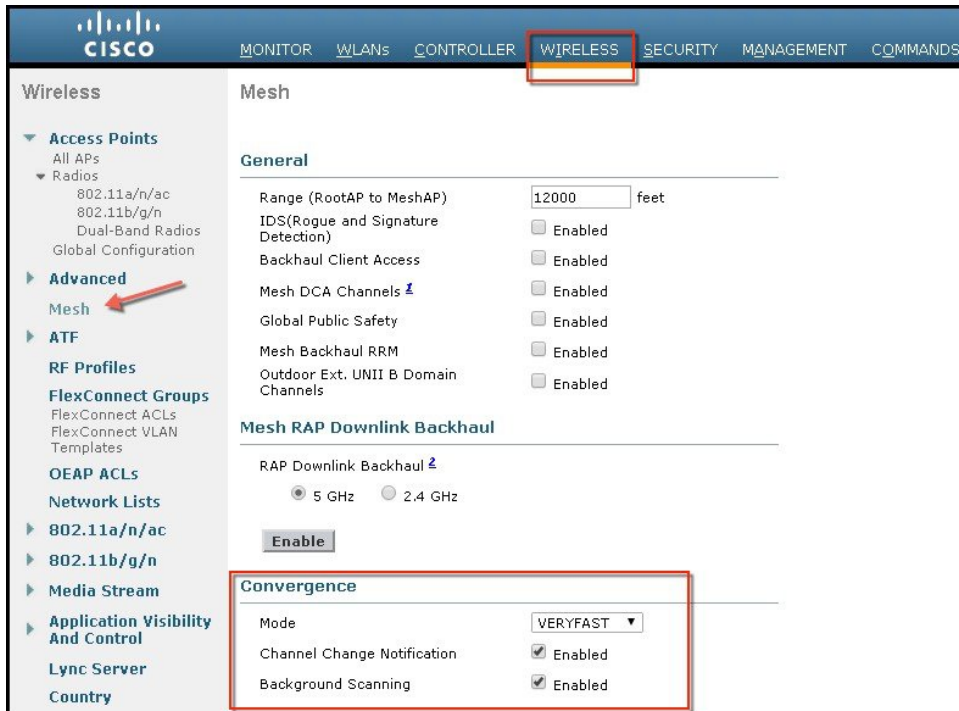
GUI を使用してコントローラを設定するには、次の手順を実行します。

手順の概要

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

手順の詳細

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



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

```
(Cisco Controller) >config mesh background-scanning ?
enable          Enable background scanning on Mesh
disable         Disable background scanning on Mesh

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

CCN (クリアチャンネル通知) は次の CLI コマンドを使用して設定します。

```
(Cisco Controller) >config mesh ccn ?
enable          Enables channel change notification
disable         Disables channel change notification

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

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



CLI からは次のコマンドを使用して、同じコンバージェンスが設定されます。

```
(Cisco Controller) >config mesh convergence ?
fast          Set fast convergence method
noise-tolerant fast Set noise-tolerant fast convergence method to handle unstable RF environment
standard      Set standard convergence method
very-fast     Set very fast convergence method

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

(注) Standard モードでは、CCN (クリアチャネル通知) およびバックグラウンドスキャンオプションは適用されません。

メッシュ機能の管理

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

Debug mesh convergence enable : デバッグ トレース

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

Debug mesh bgscan enable/disable

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

Show mesh convergence : 状態とカウンタの表示

```

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

```

Show mesh bgscan

```

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

```

```

Cyprus_MAP1#sh mesh bgscan
show MESH BG Scan

Background Scanning: Enabled

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

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

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

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

offChannel Requests Statistics
-----
Mac:18e7.28aa.e87f NDRspCnt:64 ch:149 last NDRsp rx at: 10:54:21 UTC Mar 28 2016

Cyprus_MAP1#

```


ワイヤレス伝搬の特性

表 8: 2.4 GHz 帯と 5 GHz 帯の比較 (72 ページ) は、2.4 GHz 帯と 5 GHz 帯の比較です。

2.4 GHz 帯の伝搬特性は 5 GHz 帯より優れていますが、2.4 GHz 帯はライセンスが不要という特徴があります。ノイズや干渉による影響を多く受けるのも 2.4 GHz 帯です。さらに、2.4 GHz 帯にはバックホールチャンネルが 3 つしかないため、同一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 8: 2.4 GHz 帯と 5 GHz 帯の比較

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

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

メッシュの CleanAir は 2.4 GHz 帯に実装でき、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 帯の Wi-Fi および非 Wi-Fi 干渉を検出し、数値で表して、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 帯の完全な CleanAir 機能と 5 GHz 帯での 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 帯の無線リソース管理（RRM）をサポートします。RRM は、ブリッジモード RAP に子 MAP がない場合、5 GHz 帯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（MMAPI） : 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を行うためです。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（オプション）（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せん。MSE とコントローラは、まず RF ネイバー リストを使用してマージの空間プロキシミティを確立します。

PMAC コンバージェンスおよびマージは次の要素に依存します。

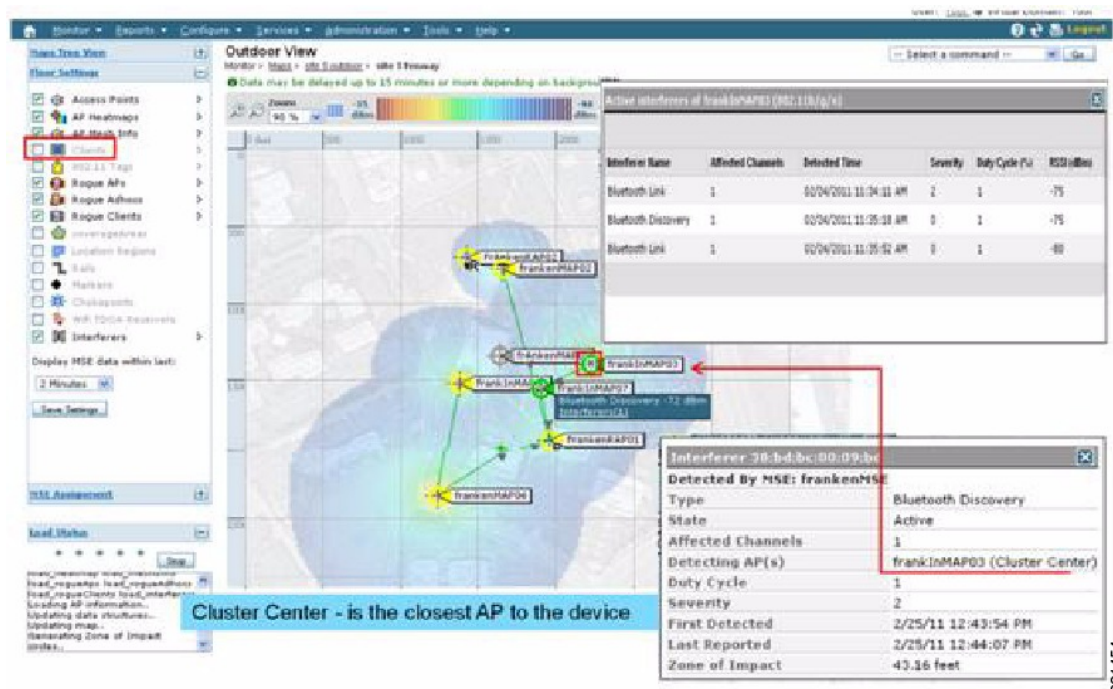
- センサーの密度
- 観測対象分類の品質
- 干渉源から AP までの RSSI
- AP での RF ネイバー リスト

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

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

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

図 25: 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周波数帯に関連しています。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せん。

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、以下を参照してください。 http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b4bdc1.shtml

CleanAir Advisor

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

CleanAir のイネーブル化

システムの CleanAir 機能を有効にするには、まず、[Wireless] > [802.11a/b] > [CleanAir] を選択してコントローラで CleanAir を有効にする必要があります。CleanAir はデフォルトで無効ですが、CleanAir は AP インターフェイスではデフォルトで有効です。

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 を有効にした後、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、無線の結果を CleanAir 詳細レベルで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、特定の干渉源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 base ライセンスで行うことができます。システムに MSE を追加するには、Prime Infrastructure Plus ライセンス、および MSE の Context-Aware ライセンスを選択する必要があります。

MSE または CMX での干渉ロケーションのために、各干渉源デバイスは 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 の永続干渉源ライセンスが MSE に組み込まれています。干渉源ライセンスは各 CleanAir AP の 5 つのライセンスのそれぞれのステージで、CleanAir AP が検出されるたびに開かれます。このプロセスは AP1552/1562/1572 に適用されます。干渉デバイスは、ライセンス数の観点からはクライアントやタグと同じです。追跡対象の干渉源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、使用可能なライセンス数のごく一部のみが使用されます。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、干渉源) 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) 各干渉源デバイスは、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、オペレーション的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にする必要があります。

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

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

メッシュアベイラビリティの増加

「セルのプランニングと距離」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 26: 同じチャンネルでセルごとに2つの RAP \(79 ページ\)](#)）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 27: 別のチャンネルでセルごとに2つの RAP \(79 ページ\)](#)）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 26: 同じチャンネルでセルごとに2つの RAP

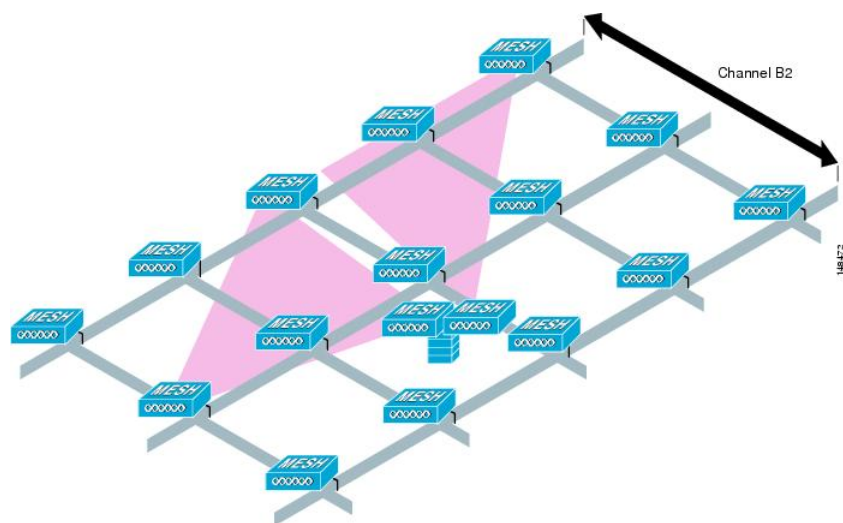
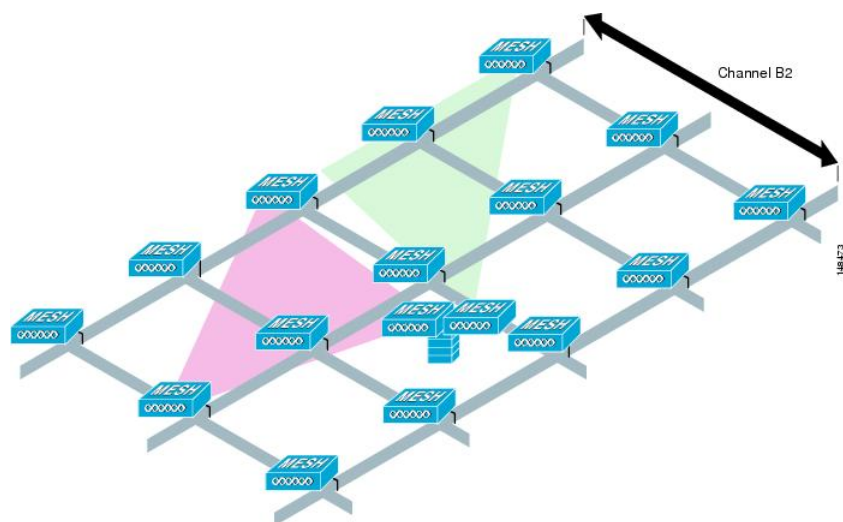


図 27: 別のチャンネルでセルごとに2つの RAP



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に、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 32 MAP を検討します。

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

チャンネル計画や RAP セル スプリットを介して、異なるチャンネルに 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。チャンネル計画では、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ン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、異なる周波数チャンネルで動作します。このプロセスにより、大きなコリジョンドメインが個別に動作する複数の小さなコリジョンドメインに分割されます。

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

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

屋内メッシュと屋外メッシュの相互運用性

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



注意

サードパーティの屋外ラックの屋内アクセス ポイントは、屋内 WLAN から駐車場のホップまでの単純かつ短距離の拡張などの、屋外での限られた配置でのみ配置できます。堅牢な環境および温度に関する仕様を備えているため、屋外ラックでは 1700、1800、2600、2700、2800、3500e/i、3600、3700、および 3800 アクセス ポイントを推奨します。さらに、AP が屋外ラック内にある場合、屋内アクセスポイントには、連結されたアンテナをサポートするためのコネクタがあります。SNR 値は増減しない場合もあるので、注意してください。また、より最適化された屋外の 1500 シリーズ アクセス ポイントと比較した場合、長期間のフェードにより、これらの AP のリンクが消失する場合があります。

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



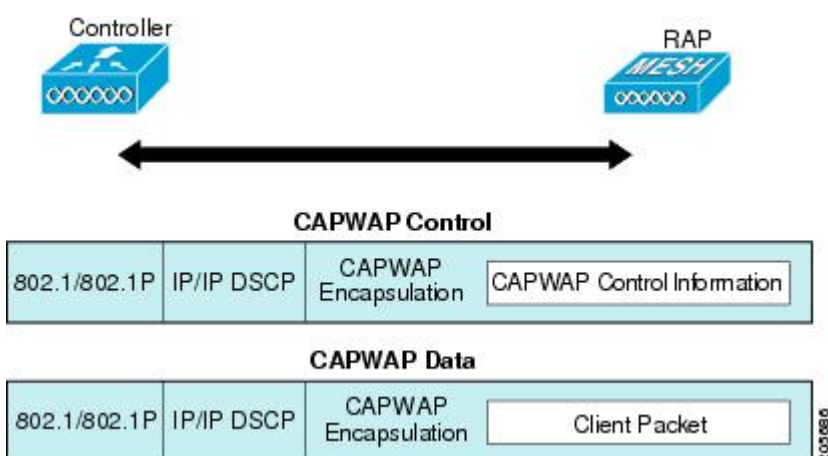
第 6 章

Cisco メッシュ アクセス ポイントのネットワークへの接続

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

ワイヤレスメッシュは、有線ネットワークの2地点で終端します。1つ目は、RAPが有線ネットワークに接続されているロケーションで、そこではすべてのブリッジトラフィックが有線ネットワークに接続しています。2つ目は、CAPWAPコントローラが有線ネットワークに接続するロケーションです。そのロケーションでは、メッシュネットワークからのWLANクライアントトラフィックが有線ネットワークに接続しています（[図 28: メッシュネットワークトラフィックの終端](#)（83 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 28: メッシュネットワークトラフィックの終端





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

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

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

この章の内容は、次のとおりです。

- [メッシュ ネットワークへのメッシュ アクセス ポイントの追加 \(84 ページ\)](#)
- [リリース8.2での Mesh PSK Key を使ったプロビジョニング \(95 ページ\)](#)
- [グローバル メッシュ パラメータの設定 \(104 ページ\)](#)
- [リリース 8.2 の 5 GHz および 2.4 GHz のメッシュ バックホール \(114 ページ\)](#)
- [バックホールクライアントアクセス \(118 ページ\)](#)
- [ローカル メッシュ パラメータの設定 \(120 ページ\)](#)
- [アンテナ利得の設定 \(128 ページ\)](#)
- [動的チャネル割り当ての設定 \(129 ページ\)](#)
- [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 \(132 ページ\)](#)
- [拡張機能の設定 \(133 ページ\)](#)

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。「アンテナ利得の設定」の項を参照してください。
- ステップ 10** シリアルバックホールのチャ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メッシュ アクセス ポイントは、すべての無線 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 29: [MAC Filtering] ページ

MAC Address	Profile Name	Interface	IP Address
00:62:ec:4a:4d:30	Any WLAN	management	10.70.0.243
00:6b:f1:16:1c:e8	Any WLAN	management	10.70.0.118
00:6b:f1:16:1d:b0	Any WLAN	management	10.70.0.204

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 [InterfaceName] 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せん。

- 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 ポートがアップリンクである場合)、802.11a/n/ac 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。
- アップリンクのイーサネット ポートでコントローラへの接続に失敗した MAP は、802.11a/n/ac 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/ac 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/ac 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 30: [All APs > Details for] ([Mesh]) ページ

The screenshot shows the Cisco Wireless configuration interface for an AP. The left sidebar lists various configuration categories like Access Points, Radios, Mesh, etc. The main area is titled 'All APs > Details for AP1572-7a7f.09c0' and has tabs for General, Credentials, Interfaces, High Availability, Inventory, and Mesh. The Mesh tab is active, showing configuration for the AP Role (set to RootAP), Bridge Type (Outdoor), Bridge Group Name (tme), and other mesh-related settings. A red box highlights the 'RootAP' dropdown menu.

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。

DHCP 43 および DHCP 60 を使用した複数のコントローラの設定

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

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

値は次のとおりです。

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

ステップ 3 次の構文を使用してオプション 60 の行を追加します。

```
option 60 ascii "VCI string"
```

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

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

ステップ 4 次の構文に従って、オプション 43 の行を追加します。

```
option 43 hex hex string
```

16 進文字列には、次の TLV 値を組み合わせて指定します。

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。

RADIUS サーバを使用した外部認証および認可の設定

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

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

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



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



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

RADIUS サーバの設定

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

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

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

ステップ 2 次のように証明書をインストールします。

- a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [ACS Certification Authority Setup] をクリックします。
- b) [CA certificate file] ボックスに、CA 証明書の場合 (パスと名前) を入力します (たとえば、c:\Certs\cra2048.cer)。
- c) [Submit] をクリックします。

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

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

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

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

メッシュ アクセス ポイントの外部認証の有効化 (GUI)

GUI を使用してメッシュ アクセス ポイントの外部認証をイネーブルにする手順は、次のとおりです。

ステップ 1 [Wireless] > [Mesh] を選択します。[Mesh] ページが表示されます (図 31 : [Mesh] ページ (93 ページ) を参照)。

図 31 : [Mesh] ページ

The screenshot shows the configuration page for Ethernet Bridging. Under the Security section, the Security Mode is set to EAP. The EAP option is highlighted with a red box. Below the Security section, there is a table with columns for Server ID, Server Address (Ipv4/Ipv6), Port, and Enabled.

Server ID	Server Address (Ipv4/Ipv6)	Port	Enabled
1	10.91.104.106	1812	<input checked="" type="checkbox"/>

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。

RADIUS サーバへのユーザ名の追加

- 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。

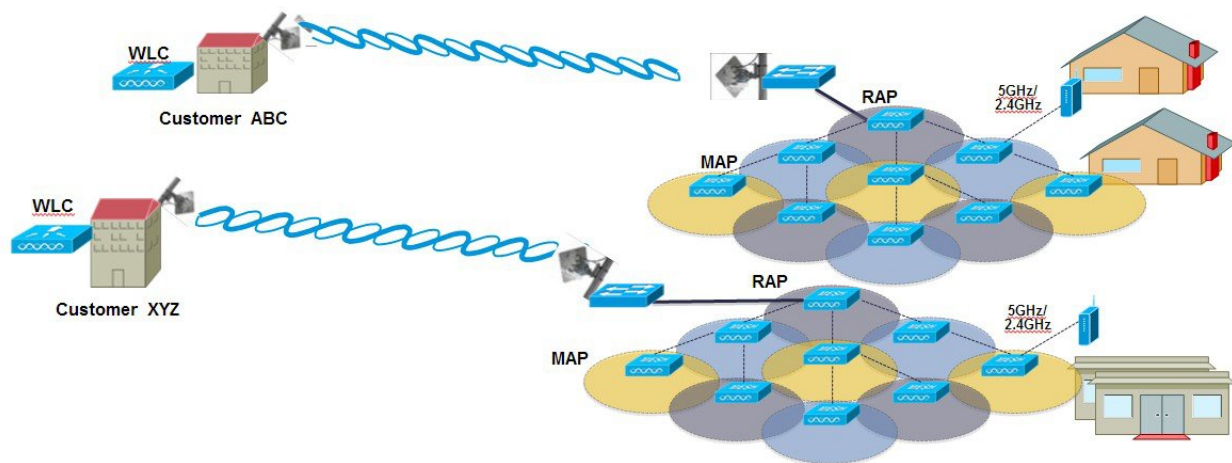
```
show mesh security-stats Cisco_AP
```

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 ポイントのパケットエラー統計、エラー数、タイムアウト数、アソシエーションと認証の成功数、再アソシエーション数、および再認証数が表示されます。

リリース 8.2 での Mesh PSK Key を使ったプロビジョニング

Cisco Mesh の導入時に、いずれの導入でもワイルドカードの MAC フィルタリングで AAA を使用し MAP アソシエーションを許可する場合、メッシュ アクセス ポイント (MAP) が現在 join 中のネットワークを終了し、別のメッシュ ネットワークへ join 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、この動作を制御できません。EAP セキュリティでは AP の MAC アドレスとタイプの組み合わせが使用されるため、制御設定を使用できないためです。PSK オプションでデフォルトのパスフレーズを使用すると、セキュリティ リスクとハイジャックの危険性が伴います。この問題は、MAP が移動車両 (公共交通機関、フェリー、船など) 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、MAP は SP のメッシュ ネットワークに固定される必要がなくなるため、MAP を別の SP ネットワークによってハイジャック/使用できます。このため導入環境では SP の対象顧客にサービスを提供できなくなります。

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に強化されたキーを使用します。コントローラソフトウェアリリース 8.1 以下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は、特別な注意が必要です。管理者は MAP ソフトウェアで PSK を有効化/無効化する際の影響を理解する必要があります。

サポートされるワイヤレス メッシュのコンポーネント

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

機能の設定手順

管理者はセキュリティ モードを PSK として設定する必要があります。また任意で新しい PSK を設定します。PSK が設定されていない場合、MAP 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 本ガイドで先述したように、コントローラに RAP を接続します。下記の設定の図の例のように、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
APB0AA.7792.7868	10.70.0.230	AIR-AP1832I-LUXK9	b0:aa:77:92:78:68	1 d, 04 h 11 m 51 s
AP6c20.560e.1a26	10.71.0.54	AIR-CAP1602E-A-K9	6c:20:56:0e:1a:26	1 d, 04 h 07 m 08 s
AP1572-7a7f.09c0	10.70.0.252	AIR-AP1572EAC-A-K9	1c:6a:7a:7f:09:c0	1 d, 04 h 07 m 15 s
AP7cad.74ff.d22e	10.70.0.254	AIR-CAP3702I-A-K9	7c:ad:74:ff:d2:2e	1 d, 03 h 59 m 30 s
APe44c.11f0.ea9d	10.70.0.252	AIR-CAP3602I-A-K9	e4:4c:11:f0:ea:9d	1 d, 03 h 52 m 20 s
AP7cad.74ff.d0e6	10.70.0.254	AIR-CAP3702I-A-K9	7c:ad:74:ff:d0:e6	1 d, 03 h 56 m 55 s
AP1532-3546.f14c	10.70.0.252	AIR-CAP1532E-A-K9	4c:4e:35:46:f1:4c	0 d, 02 h 10 m 49 s
AP1532-3546.f678	10.70.0.252	AIR-CAP1532E-A-K9	4c:4e:35:46:f6:78	0 d, 01 h 51 m 07 s

本ガイドに示すように、MAP の初期接続のオプションの 1 つでは、MAP の MAC アドレスを、RAP に接続される（スクリーンショットを参照）コントローラに入力する必要があります。

The screenshot shows the Cisco Security Mode configuration page. The left sidebar has 'AP Policies' selected. The main content area is divided into 'Policy Configuration' and 'AP Authorization List'.

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

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
 - Advanced
 - Mesh**
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - OEAP ACLs
 - Network Lists
 - 802.11a/n/ac
 - 802.11b/g/n
 - Media Stream
 - Application Visibility And Control
 - Lync Server
 - Country
 - Timers
 - Netflow
 - QoS

General

Range (RootAP to MeshAP) feet

IDS(Rogue and Signature Detection) Enabled

Backhaul Client Access Enabled

Extended Backhaul Client Access Enabled

Mesh DCA Channels Enabled

Global Public Safety Enabled

Mesh Backhaul RRM Enabled

Outdoor Ext. UNII B Domain Channels Enabled

Mesh RAP Downlink Backhaul

RAP Downlink Backhaul 5 GHz 2.4 GHz

Enable

Ethernet Bridging

VLAN Transparent Enabled

Security

Security Mode ▼

PSK Provisioning Enabled

Default PSK Enabled

ADD New Provisioning Key

Provisioning Key

Description

ADD

Key Index	TimeStamp	Description
1	Fri Nov 13 09:11:49 2015	tme123
2	Fri Nov 13 09:11:03 2015	Cisco123

External MAC Filter Authorization Enabled

Force External Authentication Enabled

LSC Only MAP Authentication Enabled

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

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

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

Security

Security Mode: PSK ▼

PSK Provisioning: Enabled

Default PSK: Enabled

ADD New Provisioning Key

Provisioning Key: Mesh123 ←

Description: Mesh123 |

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

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

The screenshot shows the Cisco Wireless GUI configuration page for AP1532-3546.f678. The breadcrumb navigation is "All APs > Details for AP1532-3546.f678". The "Mesh" tab is selected. The configuration includes:

- AP Role: MeshAP
- Bridge Type: Outdoor
- Bridge Group Name: tme
- Strict Matching BGN:
- Ethernet Bridging: Daisy Chaining:
- 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
- VLAN Support:

Below the configuration is the "Mesh RAP Downlink Backhaul" section with "5 GHz" selected and an "Enable" button. A red arrow points to the "Delete PSK" button.

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

This screenshot is identical to the one above, showing the configuration page for AP1532-3546.f678. A red arrow points to the "Delete PSK" button.

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

(注)

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

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

例に示すように、[Provisioning] ウィンドウを手動で有効化すると、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 configuration page for Mesh. The 'Security' section is expanded, and 'PSK Provisioning' and 'Default PSK' are both checked. A red arrow points to the 'PSK Provisioning' checkbox. Below this, there is a table of provisioning keys:

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

Below the table, there are several checkboxes for authentication options, all of which are currently unchecked:

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

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

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

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

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

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

マルチコントローラの設定で PSK または EAP セキュリティ付きのメッシュ 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があります。
 - 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 9: 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> <pre>config mesh ids-state {enable disable}</pre> <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
バックホール クライアント アクセス	<p>(注) このパラメータは、2つ以上の無線規格に対応したメッシュ アクセス ポイントに適用されます。</p> <p>バックホール クライアント アクセスが有効な場合は、無線バックホール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。無線バックホールは、ほとんどのメッシュ アクセス ポイントでは 5 GHz 帯で運用されます。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無線バックホールを介して送信され、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>デフォルト：無効</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>

パラメータ	説明
VLAN トランスペアレント	<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>デフォルト：イネーブル</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 デフォルト : EAP</p>

パラメータ	説明
External MAC Filter Authorization	

パラメータ	説明
	<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"> • AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。 • コントローラも、RADIUS サーバで設定する必要があります。 • 外部認証および認証用に設定されたメッシュ アクセス ポイントは、RADIUS サーバのユーザーリストに追加する必要があります。 <ul style="list-style-type: none"> • リモート認可および認証の場合、EAP-FAST は製造元の証明書 (CERT) を使用して、子メッシュ アクセス ポイントを認証します。また、この製造元証明書に基づく ID は、ユーザの確認においてメッシュ アクセス ポイントのユーザ名として機能します。 • IOS ベースのメッシュ アクセス ポイント (1130、1240) の場合、メッシュ アクセス ポイントのプラットフォーム名は、証明書内のイーサネットアドレスの前に位置します。つまり、外部 RADIUS サーバのユーザ名は、<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。 • 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。 <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</p>

パラメータ	説明
	<p>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、無線バックホール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。無線バックホールには、大部分のメッシュ アクセス ポイントで 5GHz 帯が使用されます。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 のみが無線バックホールを介して送信され、クライアント アソシエーションは 2 番目の無線のみを介して送信されます。

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

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

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

- **show mesh config** : グローバル設定を表示します。

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

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

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

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

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

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

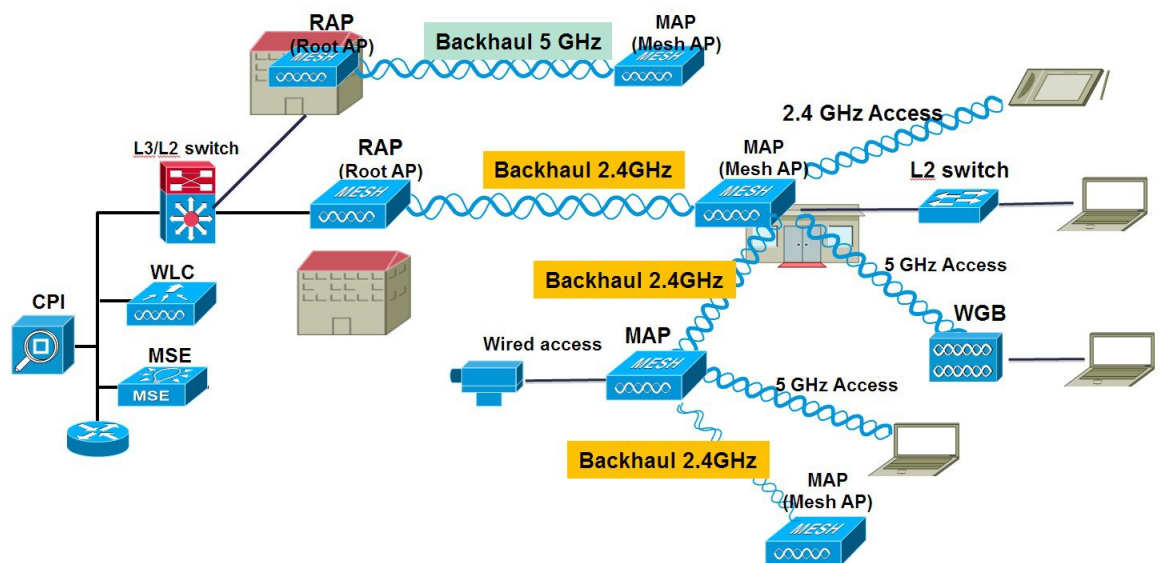
リリース 8.2 以前のワイヤレス メッシュ バックホールは 5 GHz でのみサポートされていました。リリース 8.2 ではワイヤレス メッシュ バックホールは、5 GHz および 2.4 GHz でサポートされます。

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

RAP が 5 GHz から 2.4 GHz へ設定の変更を取得すると、その変更内容は 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 帯に再接続されます。2.4 GHz を設定する場合は、2.4 GHz のバックホールが認識されるよう、すべてのコントローラでリリース 8.2 を実行してください。



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



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

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

The screenshot shows the Cisco Wireless Mesh configuration interface. The 'Wireless' menu is open, and the 'Mesh' configuration page is displayed. The 'General' section includes the following settings:

Setting	Value
Range (RootAP to MeshAP)	12000 feet
IDS(Rogue and Signature Detection)	<input type="checkbox"/> Enabled
Backhaul Client Access	<input checked="" type="checkbox"/> Enabled
Extended Backhaul Client Access	<input type="checkbox"/> Enabled
Mesh DCA Channels	<input type="checkbox"/> Enabled
Global Public Safety	<input type="checkbox"/> Enabled
Mesh Backhaul RRM	<input checked="" type="checkbox"/> Enabled
Outdoor Ext. UNII B Domain Channels	<input type="checkbox"/> Enabled

The 'Mesh RAP Downlink Backhaul' section is also visible, with the 'RAP Downlink Backhaul' option selected and the '2.4 GHz' radio button selected. A red arrow points to the '2.4 GHz' radio 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 に変更し、チャンネルを自ら選択する必要があります。ここでの変更内容はすべての MAP と、RAP のブランチの「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
APB0AA.7792.7868	0	b0:aa:77:92:52	Enable	UP	1 *	NA	NA	8 *	Internal
AP6c20.560e.1a26	0	34:a8:4e:ba:02	Enable	UP	6 *	Disable	DOWN	6 *	External
AP7cad.74ff.d22e	0	08:cc:68:cc:b8:7f	Enable	UP	6 *	Enable	UP	8 *	Internal
AP7cad.74ff.d0e6	0	08:cc:68:cc:b3:c0	Enable	UP	1 *	Enable	UP	8 *	Internal
APa44c.11f0.ea9d	0	f4:7f:35:d8:d4:3f	Enable	UP	11 *	Enable	UP	8 *	Internal
AP1572-7a7f.09c0	0	1c:6a:7a:7f:1e:d0	Enable	UP	11	Enable	UP	7 *	External
AP1532-9546.f678	0	20:bb:c0:72:1a:1f	Enable	UP	11	NA	NA	1	External
AP1532-9546.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 から同じチャンネルだけを継承して固定されます。

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

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

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


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

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

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

たとえばMAPのバックホールチャ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 Wireless Management interface for AP1532-3546.f678. The 'Mesh' tab is selected. A dialog box is overlaid on the interface 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、無線バックホール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。無線バックホールでは5GHz帯が使用されます。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無線バックホールを介して送信され、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、デージーチェーン導入のスレーブ AP と子 AP を除くすべてのメッシュ アクセス ポイントは再起動します。

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

バックホール クライアント アクセスの設定 (GUI)

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

図 32: 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

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

無線バックホールのデータ レートの設定

バックホールは、アクセスポイント間でワイヤレス接続のみを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。

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

図 33: 自動設定されたブリッジ レート

The screenshot shows the Cisco Wireless Controller GUI. The main navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMMANDS'. The 'WIRELESS' tab is selected. On the left, the 'Wireless' menu is expanded to show 'Access Points', 'Radios', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', 'FlexConnect Groups', 'OEAP ACLs', 'Network Lists', and 'Application Visibility And Control'. The main content area is titled 'All APs > Details for AP1572-7a7f.09c0'. It has several tabs: 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Mesh'. The 'General' tab is active. The configuration fields are as follows:

AP Role	RootAP
Bridge Type	Outdoor
Bridge Group Name	tme
Strict Matching BGN	<input type="checkbox"/>
Ethernet Bridging	<input type="checkbox"/>
Preferred Parent	none
Backhaul Interface	802.11a/n/ac
Bridge Data Rate (Mbps)	auto
Ethernet Link Status	UpDnDnNANA
PSK Key TimeStamp	Tue Aug 2 16:33:42 2016
VLAN Support	<input checked="" type="checkbox"/>
Native VLAN ID	70

Below the 'General' tab, there is a section for 'Mesh RAP Downlink Backhaul' with radio buttons for '5 GHz' (selected) and '2.4 GHz'. There is also an 'Enable' checkbox at the bottom of this section.



(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=18Mbps、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。

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。

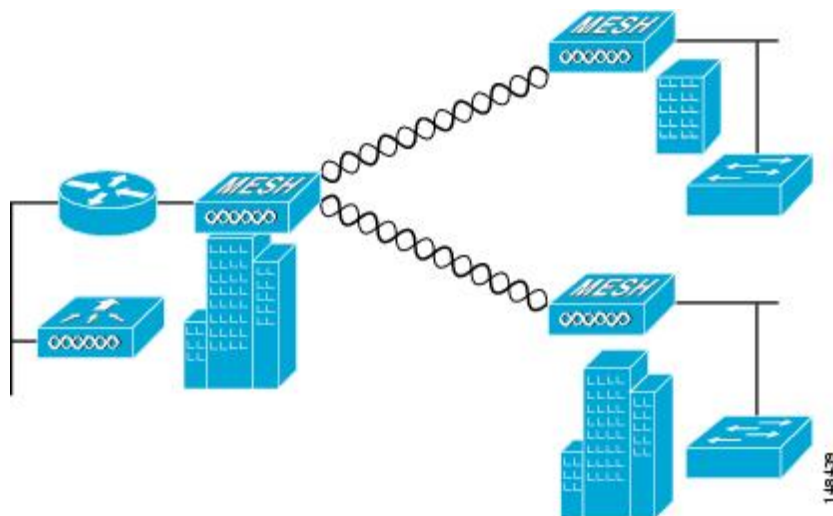
1. メッシュ ノードをブリッジとして使用する場合 (図 34: ポイントツーマルチポイントブリッジング (124 ページ) を参照)。



(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 34: 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)

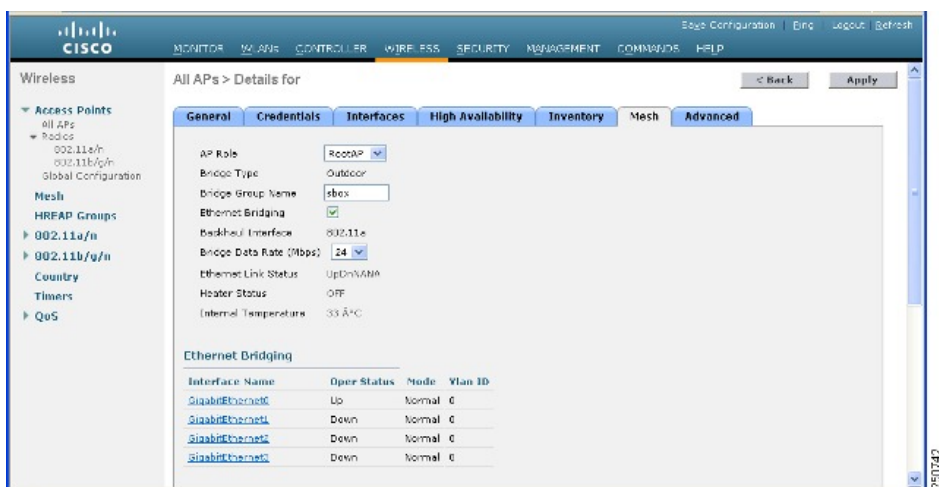
GUI を使用して RAP または MAP でイーサネットブリッジングをイネーブルにする手順は、次のとおりです。

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 35 : [All APs > Details for] ([Mesh]) ページ (125 ページ) を参照してください)。

図 35 : [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。

The screenshot shows the Cisco GUI for configuring an AP. The 'Wireless' section is active, and the 'All APs > Details for AP1572-7a7f.09c0' page is displayed. The 'Interfaces' tab is selected, and the 'VLAN Support' checkbox is checked. The 'Native VLAN ID' is set to 70. Other configuration options include AP Role (RootAP), Bridge Type (Outdoor), Bridge Group Name (tme), Ethernet Bridging (checked), Preferred Parent (none), Backhaul Interface (802.11a/n/ac), Bridge Data Rate (auto), and Ethernet Link Status (UpDnDnNANA).

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、同じチャネルにある2つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター (領域) のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字までの文字列です。

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

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

ブリッジグループ名の設定 (CLI)

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

```
config ap bridgegroupname set group-name ap-name
```

(注) BGN の設定後に、メッシュ アクセス ポイントがリブートします。

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

ステップ2 BGN を確認するには、次のコマンドを入力します。

```
show ap config general ap-name
```

ブリッジグループ名の確認 (GUI)

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

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

電力およびチャネルの設定

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

電力およびチャネルの設定 (GUI)

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

(注) 無線スロットは各無線に対して表示されます。

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

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

ステップ 4 無線の Tx Power Level を割り当てます。

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

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

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

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

アンテナ利得の設定

コントローラの GUI または CLI を使用して、取り付けられているアンテナのアンテナ 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。

アンテナ利得の設定 (GUI)

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

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

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

(注) 外部アンテナだけに設定可能な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、次の手順でコントローラの GUI を使用することで、動的チャネル割り当て (DCA) アルゴリズムが使用するチャネルを指定できます。この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の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オフにします。
- [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、join しているすべてのメッシュ アクセス ポイントのチャネル割り当てを必要に応じてコントローラが評価して更新します。

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

- [OFF] : DCA をオフにし、すべてのメッシュ アクセス ポイント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、チャネル変更の判断材料となる環境要因（信号、負荷、ノイズ、干渉など）に対する DCA アルゴリズムの感度を指定します。

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

デフォルト値は [Medium] です。

表 10: 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
大きい	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

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

- [20 MHz] : 20 MHz のチャンネル帯域幅 (デフォルト)

(注) グローバルに設定された DCA チャンネル幅設定を上書きするには、[802.11a/n Cisco APs] > [Configure] ページでアクセス ポイントの帯域幅を 20 MHz モードに設定します。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、4.9GHz チャンネルが動作する 802.11a 帯域で 4.9GHz チャンネルを設定する必要があります。4.9GHz 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。4.9GHz 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。5GHz 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

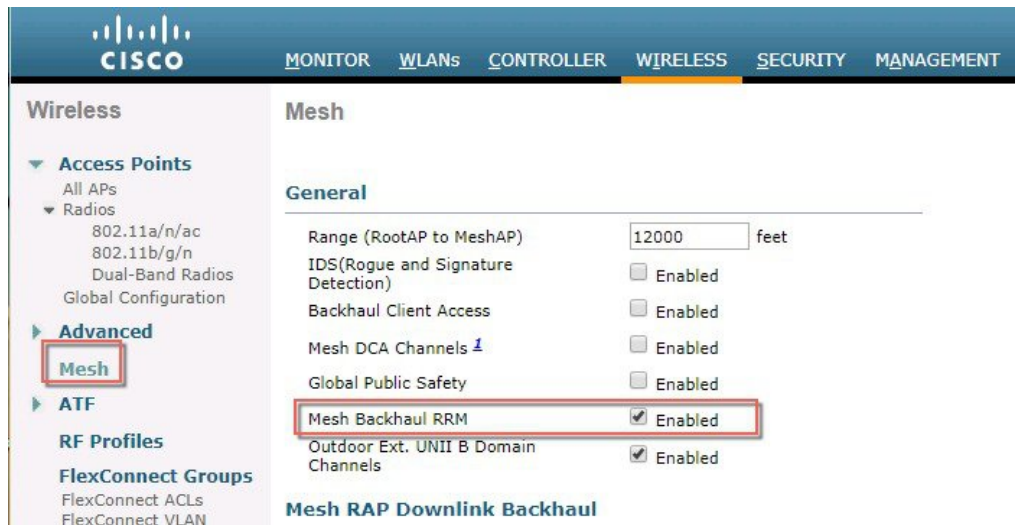
Radio Resource Management (RRM) は、次の場合に、ブリッジモードアクセスポイントの無線バックホールで有効にできます。

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

これらの条件が満たされている場合、完全な RRM が確立されます。この中には、伝送電力制御 (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>** : メッシュ無線バックホールの 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。



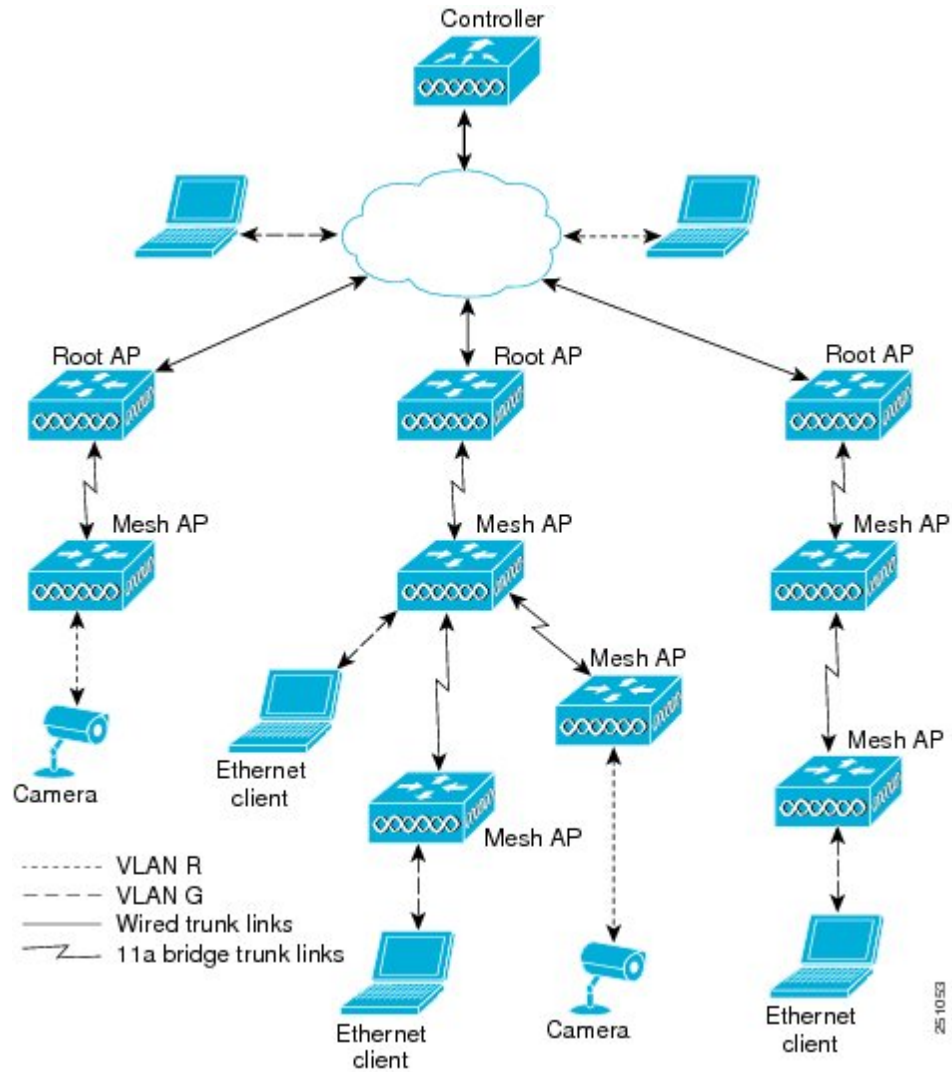
拡張機能の設定

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 36: 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 トランスペアレント モードを無効にするには、「グローバル メッシュ パラメータの設定」の項を参照してください。

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

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

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

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

- トランク モード：このモードでは、ユーザがネイティブ VLAN および許可された VLAN リストを設定する必要があります（デフォルトではありません）。このモードではタグ付きのパケットとタグなしパケットの両方が許可されます。タグなしパケットは許可され、ユーザ指定のネイティブ VLAN のタグが付けられます。許可された VLAN リスト内の VLAN のタグが付けられたタグ付きパケットは許可されます。
- キャンパス内の別々の建物に存在している 2 つの MAP 間でトラフィックを転送するようなブリッジングアプリケーションでは、トランク モードを使用します。

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



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

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

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

VLAN 登録

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



(注) VLAN 登録は自動的に行われます。ユーザの操作は必要ありません。

VLAN 登録の概要は次のとおりです。

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

イーサネット VLAN タギングのガイドライン

イーサネット タギングの以下のガイドラインに従います。

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

- VLAN タギングは、次のようにイーサネット インターフェイスでだけ設定できます。
 - AP1500 では、4 つのポートのうちポート 0 (PoE 入力)、ポート 1 (PoE 出力)、およびポート 3 (光ファイバ) の3つをセカンダリ イーサネット インターフェイスとして使用できます。ポート 2- ケーブルは、セカンダリ イーサネット インターフェイスとして設定できません。
 - イーサネット VLAN タギングでは、RAP のポート 0-PoE 入力は、有線ネットワークのスイッチのトランク ポートへの接続に使用します。MAP のポート 1-PoE 出力は、ビデオ カメラなどの外部デバイスへの接続に使用します。
- バックホール インターフェイス (802.11a 無線) は、プライマリ イーサネット インターフェイスとして機能します。バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。プライマリ イーサネット インターフェイスに必要な設定はありません。
- 屋内メッシュ ネットワークの場合、VLAN タギング機能は、屋外メッシュ ネットワークの場合と同様に機能します。バックホールとして動作しないアクセスポートはすべてセカンダリであり、VLAN タギングに使用できます。
- RAP にはセカンダリ イーサネット ポートがないため、VLAN タギングを RAP 上で実装できず、プライマリ ポートがバックホールとして使用されます。ただし、イーサネットポートが1つの MAP では VLAN タギングを有効にすることができます。これは、MAP のイーサネット ポートがバックホールとして機能せず、結果としてセカンダリ ポートになるためです。
- 設定の変更は、バックホールとして動作するイーサネット インターフェイスに適用されません。バックホールの設定を変更しようとする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witch のトランク ポートと RAP トランク ポートは一致している必要があります。

- RAP は常にスイッチのネイティブ VLAN ID 1 に接続する必要があります。RAP のプライマリ イーサネット インターフェイスは、デフォルトではネイティブ VLAN 1 です。
- RAP に接続されている有線ネットワークのスイッチポート（ポート 0-PoE 入力）は、トランク ポートでタグ付きパケットを許可するように設定する必要があります。RAP は、メッシュネットワークから受信したすべてのタグ付きパケットを有線ネットワークに転送します。
- メッシュ セクター宛以外の VLAN をスイッチのトランク ポートに設定しないでください。
- MAP イーサネット ポートで設定した VLAN は、管理 VLAN として機能できません。
- メッシュ アクセス ポイントが CAPWAP RUN 状態であり、VLAN 透過モードが無効な場合にのみ、設定は有効です。
- ローミングする場合、または CAPWAP が再び開始される場合は、必ず設定の適用が再び試行されます。

イーサネット VLAN タギングの有効化 (GUI)

VLAN タギングを設定する前に、イーサネットブリッジングを有効にする必要があります。

GUI を使用して RAP または MAP で VLAN タギングをイネーブルにする手順は、次のとおりです。

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

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

ステップ 3 詳細ページで、[Mesh] タブを選択します。

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

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

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

[Mode] ドロップダウンリストで [Access] を選択します。

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

[Apply] をクリックします。

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

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

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

[Mode] ドロップダウン リストで [trunk] を選択します。

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

[Apply] をクリックします。

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

発信パケットのトランク VLAN ID を指定します。

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

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

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

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

ステップ 5 [Apply] をクリックします。

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

イーサネット VLAN タギングの設定 (CLI)

MAP アクセス ポートを設定するには、次のコマンドを入力します。

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

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

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

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

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

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

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

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

イーサネット VLAN タギング設定詳細の表示 (CLI)

手順

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

```
show ap config ethernet ap-name
```

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

```
show mesh config
```

ワークグループブリッジとメッシュ インフラストラクチャとの相互運用性

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せん。

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せん。

現在のアーキテクチャでは、Autonomous AP がワークグループブリッジとして機能しますが、1 つの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帯（802.11b/g）および5 GHz帯（802.11a）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』の「Cisco Workgroup Bridges」の項を参照してください。その場所は次のとおりです。<https://www.cisco.com/c/en/us/support/wireless/8500-series-wireless-controllers/products-installation-and-configuration-guides-list.html>

サポートされるWGBモードおよび機能は次のとおりです。

- WGBとして設定された自律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チャンネルの同時使用に対応するアクセス ポイントは、ワークグループブリッジモードをサポートしません。

- クライアントモード WGB (BSS) はサポートされていますが、インフラストラクチャ WGB はサポートされていません。クライアントモード WGB 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 37: WGB の WPA セキュリティ設定

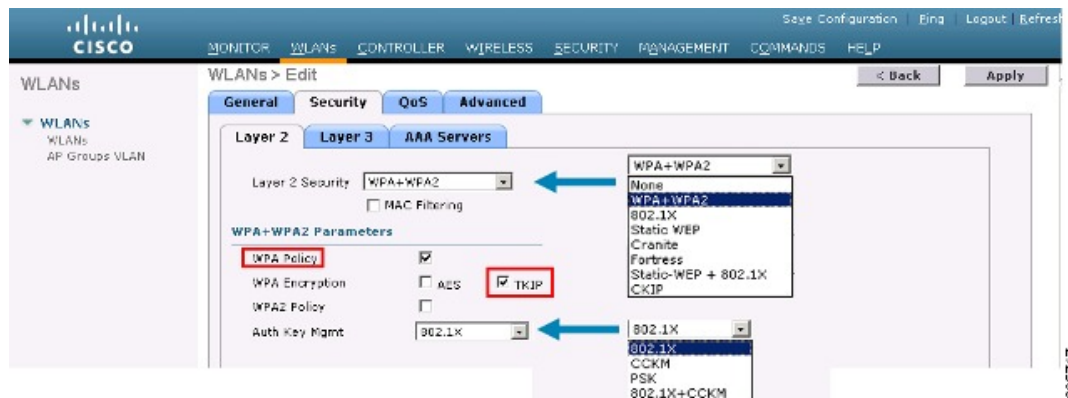
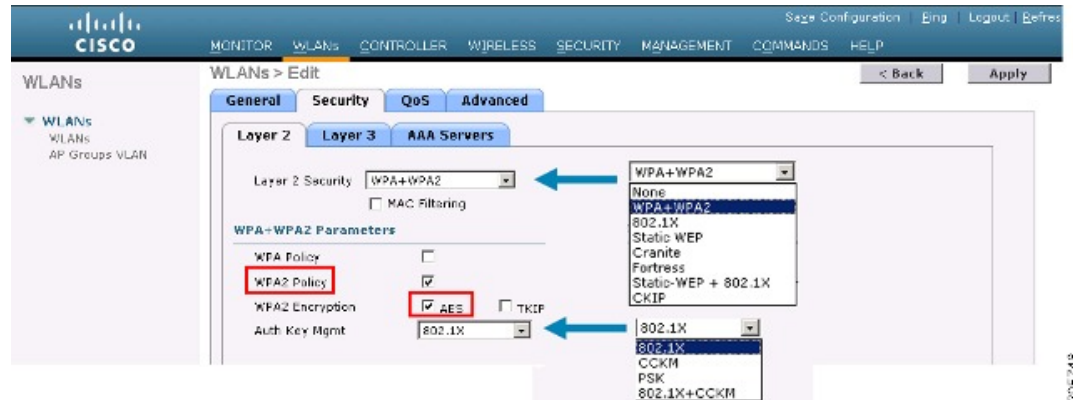


図 38: WGB の WPA-2 セキュリティ設定



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 39: クライアントが **WGB** であると認識されている

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:3a:2f:57:26	SkyRep-70:7b:a0	WLAN5	802.11g	Associated	Yes	29	Yes
00:06:50:fe:00:34	SkyRep-70:7b:a0	WLAN5	802.11b	Associated	Yes	29	No
00:13a:8d3:9e2c	RAP001b.2e26-f092-1130	Unknown	802.11a	Probing	No	29	No
00:15:5d:d4:25:d1	RAP001a.1449-f400Plus	WLAN5	802.11a	Associated	Yes	29	No
00:16:36:5f:4b:74	MAP2-0C1e.1448.ec00+3r	WLAN5	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 40: [Monitor] > [Clients] > [Detail] ページ (無線 WGB クライアントの場合) (144 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 41: [Monitor] > [Clients] > [Detail] ページ (有線 WGB クライアントの場合) (144 ページ) のようなページが表示されます。

図 40 : [Monitor] > [Clients] > [Detail] ページ (無線 WGB クライアントの場合)

The screenshot shows the Cisco configuration interface for a wireless WGB client. The page is titled "Clients > Detail" and includes a navigation menu with options like "Monitor", "WLANs", "Controller", "Wireless", "Security", "Management", "Commands", and "Help". The main content area is divided into two columns: "Client Properties" and "AP Properties".

Client Properties		AP Properties	
MAC Address	00:1b:0c:ac:a9:7f:0f	AP Address	00:1e:14:40:ec:00
IP Address	209.166.200.285	AP Name	MAP2-001e.1448.ec00H3r
Client Type	WGB Client	AP Type	802.11a
WGB MAC Address	00:1d:45:b5:74:44	WLAN Profile	WLANS
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 Pullable	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 41 : [Monitor] > [Clients] > [Detail] ページ (有線 WGB クライアントの場合)

The screenshot shows the Cisco configuration interface for a wired WGB client. The page is titled "Clients > Detail" and includes a navigation menu with options like "Monitor", "WLANs", "Controller", "Wireless", "Security", "Management", "Commands", and "Help". The main content area is divided into two columns: "Client Properties" and "AP Properties".

Client Properties		AP Properties	
MAC Address	00:0c:9a:2f:07:00	AP Address	00:0c:05:70:7b:e0
IP Address	70.1.0.54	AP Name	SkyRap170:7b:e0
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 Pullable	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

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。

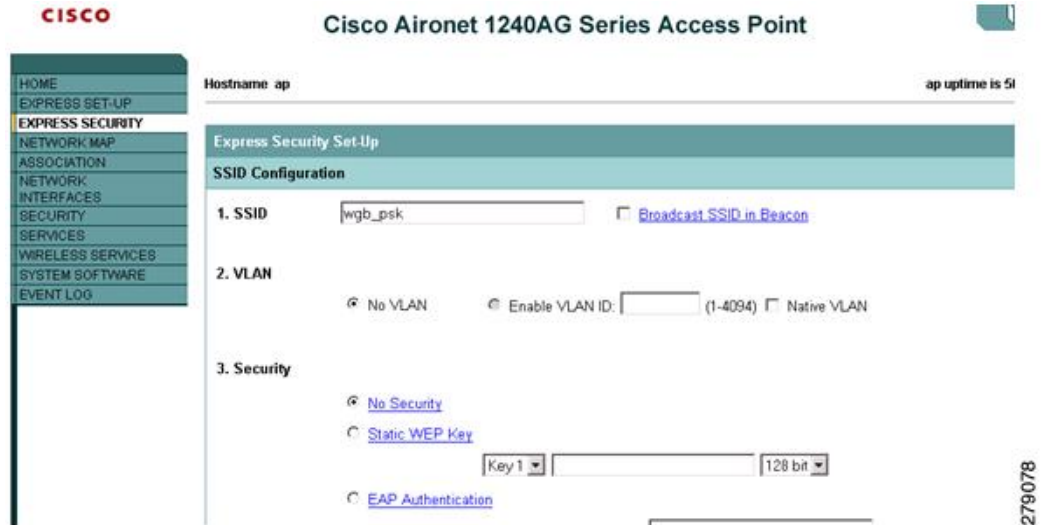
- SSID を無線インターフェイスにマッピングし、無線インターフェイスの役割を定義します。

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 42: [SSID Configuration] ページ



WGB アソシエーションの確認

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

```
WGB#show dot11 associations client
```

```
802.11 Client Stations on Dot11Radio1:
```

```
SSID [WGBTEST] :
```

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

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

図 43: 更新された WGB クライアント

The screenshot shows the Cisco WLC Monitor Clients page. A table lists three clients. The first two rows have blue arrows pointing to their MAC addresses with the label 'wgb'. The third row has a blue arrow pointing to its MAC address with the label 'wgb wireless client'.

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:e5:72	AP_1240	wgb_wpa2	wgb_wpa2	802.11a	Associa
00:40:96:ad:67:3b	AP_1240	wgb_psk	wgb_psk	N/A	Associa

279075

図 44: 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 'Search by MAC address'. A table lists two clients. The 'WGB' column for both clients is highlighted with a red box and contains the value 'Yes'.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:05:9a:3f:57:36	SkyRap:70:7b:a0	WLAN5	802.11g	Associated	Yes	29	Yes
00:04:60:fe:09:38	SkyRap:70:7b:a0	WLAN5	802.11b	Associated	Yes	29	No

279076

図 45: 更新された WGB クライアント

The screenshot shows the Cisco WLC Monitor Clients > Detail page. The 'Client Properties' section has 'Client Type' set to 'WGB', which is highlighted with a red box. The 'AP Properties' section shows details for the associated AP.

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	WLAN5
User Name		Status	Associated
Port Number	29	Association ID	1
Interface	management	802.11 Authentication	Open System
VLAN ID	70	Reason Code	0
CCK Version	CCKV5	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

279077

リンク テストの結果

図 46: 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			
Receive count	2	3	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

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:70:97:1c:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

```
(Cisco Controller) > show client summary
Number of Clients..... 7
```

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

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

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

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth
-------------	------------	---------	----------	------	------

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

クライアント ローミング

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

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

- アクセス ポイント経由ローミング：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 をサポートするネイバーアクセスポイントの BSSID、およびアソシエーション解除からの経過時間が含まれます。
- 拡張ネイバー リスト：音声アプリケーションを中心に、Cisco CX v4 クライアントのローミング能力とネットワーク エッジのパフォーマンスを向上させます。アクセスポイントは、ネイバーリストのユニキャスト更新メッセージを使用して、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

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。

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 (注: 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します)。

5. **show dot11 association** コマンドの出力を確認し、WGB がコントローラに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 対応であり、QoS は、2.4 および 5 GHz のローカル AP、2.4 および 5 GHz の AP、2.4 および 5 GHz の無線バックホールでサポートされます。CAC は、バックホールおよび CCXv4 クライアントでサポートされています (メッシュ アクセス ポイントとクライアント間の CAC を提供)。



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

Call Admission Control (コール アドミッション制御)

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



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

アクセスポイントには、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 はコンテンツION 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)。

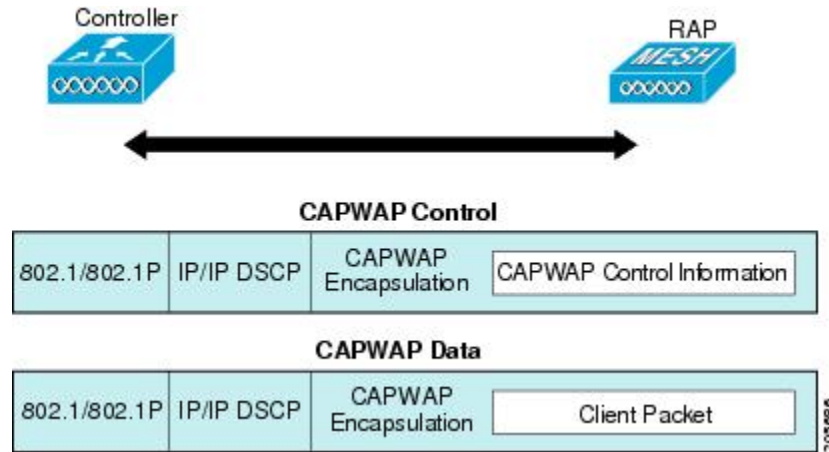
カプセル化

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 47: カプセル化

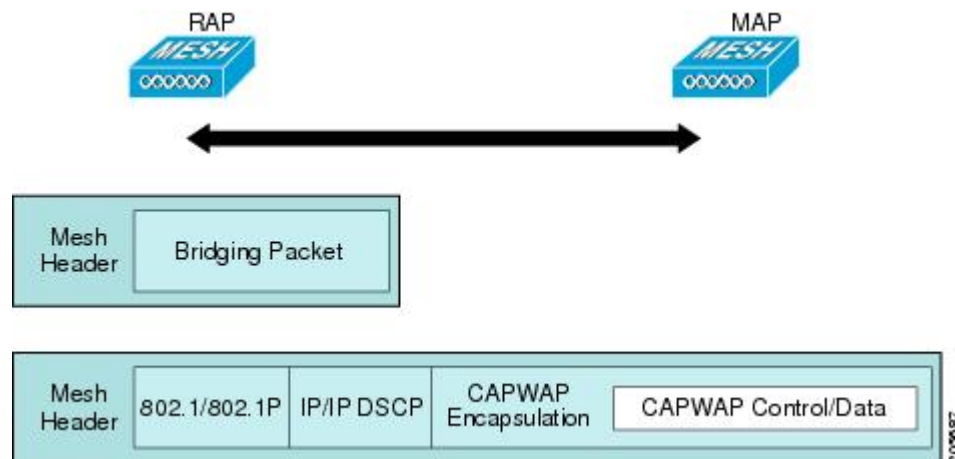


バックホールの場合、メッシュ トラフィックのカプセル化のタイプは 1 つだけです。ただし、2 つのタイプのトラフィック (ブリッジ トラフィックと CAPWAP 制御およびデータ トラフィック) がカプセル化されます。どちらのタイプのトラフィックもプロプライエタリメッシュヘッダーにカプセル化されます。

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 48: メッシュ トラフィックのカプセル化





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

メッシュ アクセス ポイントでのキューイング

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

AP1500 は、ワイヤレス クライアント 伝送用に 4 つの FIFO をサポートします。これらの FIFO は 802.11e Platinum、Gold、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。

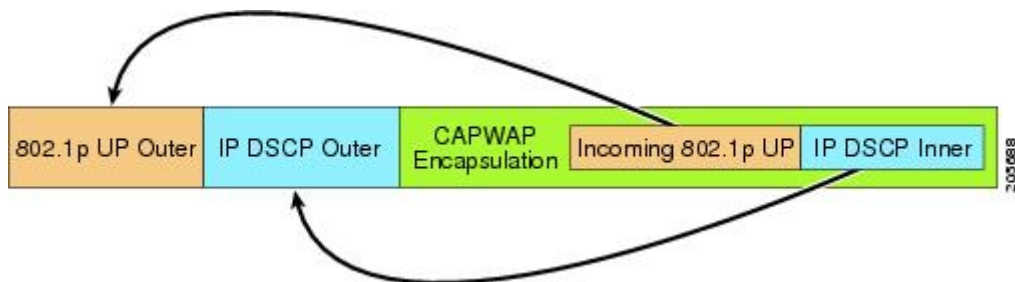
バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Silver、および Bronze に制限されます。Platinum キューは、CAPWAP 制御 トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

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 49: 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 11: 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。

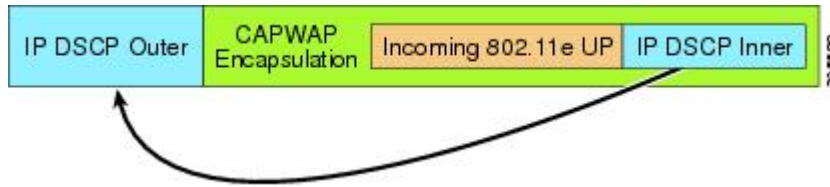
表 12: MAP からクライアントへのパスの QoS

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 50: 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 13: DSCP とバックホールキューのマッピング (159 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 13: 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。

CAPWAP 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/ac] または [802.11b/g/n] > [Global] パラメータ ページで、次のことを行う必要があります。
 - Dynamic Transmit Power Control (DTPC) を有効にする
 - 11 Mbps 未満のすべてのデータ レートを無効にする
- [802.11a/n/ac] または [802.11b/g/n] > [Voice] パラメータ ページで、次のことを行う必要があります。
 - 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/ac] または [802.11b/g/n] > [EDCA] パラメータ ページで、次のことを行う必要があります。
 - インターフェイスの EDCA プロファイルを [Voice Optimized] に設定する
 - 低遅延 MAC を無効にする
- [QoS > Profile] ページで、次の手順を実行する必要があります。
 - 音声プロファイルを作成して有線 QoS プロトコル タイプとして 802.1Q を選択する

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

ビデオのメッシュ マルチキャストの抑制の有効化

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)。



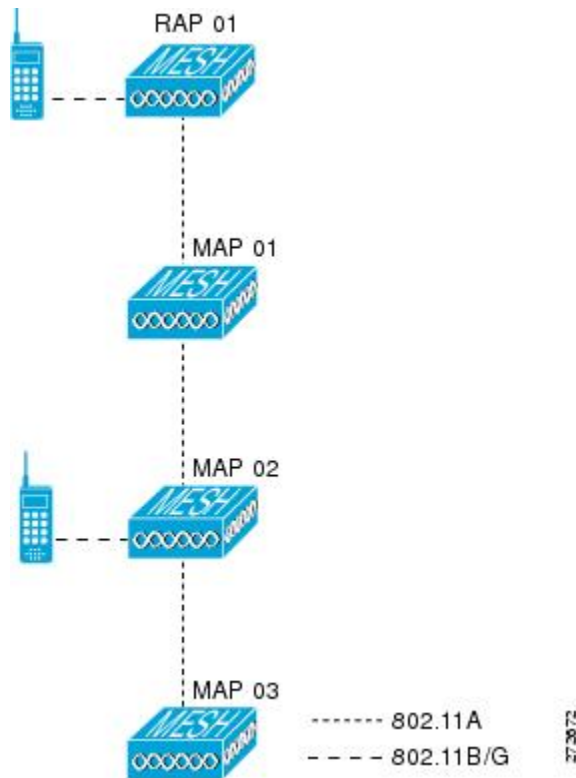
- (注) AP1540/1560 は、リリース 8.5 および 8.6 で「in-out」モードのみをサポートします。その他のすべてのモードは将来のリリースでサポートされる予定です。

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

メッシュ ネットワークの音声詳細の表示 (CLI)

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

図 51: 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 がコールを受信すると、802.11b/g の *calls* カラムにある既存の値が 1 増加します。上記の例では、*map2* の 802.11b/g でアクティブなコールは、新しいコールだけです。新しいコールが受信されるときに 1 つのコールがアクティブである場合、値は 2 になります。

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

show mesh cac callpath *AP_name*

Information similar to the following appears:

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



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

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

show mesh cac rejected *AP_name*

以下に類似した情報が表示されます。

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



(注) コールが **map2** 802.11b/g 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 ネットワークにおけるマルチキャストの有効化 (CLI)



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

手順

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

config network multicast global enable

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

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

config network multicast global disable

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



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

IGMP スヌーピング

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

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

コントローラ上で IGMP スヌーピングをイネーブルにするには、次のコマンドを入力します。

configure network multicast igmp snooping enable

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

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

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

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

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

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

音声の詳細については、次のマニュアルを参照してください。

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

メッシュ AP のローカルで有効な証明書

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

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



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

- MAP の無線プロビジョニング

設定のガイドライン

メッシュ AP に LSC を使用する場合は、次のガイドラインに従います。

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

メッシュ AP の LSC と通常の AP の LSC の違い

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

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

このプロファイルは、証明書の発行元として「cisco」を使用するようハードコーディングされています。このプロファイルは、メッシュ認証にベンダー証明書を使用できるよう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、コントローラのレポート後に失われます。

LSC AP での証明書検証プロセス

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

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

LSC 機能の証明書の取得

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

LSC の証明書を取得する手順は、次のとおりです。

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

ステップ 2 次の手順で、CA 証明書を取得します。

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

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

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

ステップ 4 次の手順で、コントローラに CA 証明書を設定します。

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

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

- a) [Request a certificate] リンクをクリックします。
- b) [advanced certificate request] リンクをクリックします。
- c) [Create and submit a request to this CA] リンクをクリックします。
- d) 次の画面に移動し、[Certificate Template] ドロップダウン リストから [Server Authentication Certificate] を選択します。
- e) 有効な名前、電子メール、会社、部門、市、州、および国/地域を入力します。（CAP 方式を使用し、ユーザ クレデンシャルのデータベースでユーザ名を確認する場合は忘れないでください）。
(注) 電子メールは使用されません。
- f) [Mark keys as exportable] をイネーブルにします。
- g) [Submit] をクリックします。
- h) ラップトップに証明書をインストールします。

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

証明書を変換するには、Linux マシンで次のコマンドを使用します。

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

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

ステップ 8 コントローラをリブートして、証明書が使用できるようにします。

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

```
show local-auth certificates
```

ローカルで有効な証明書 (CLI) の設定

ローカルで有効な証明書 (LSC) を設定するには、次の手順に従ってください。

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

ステップ 2 次のコマンドを入力します。

```
config local-auth eap-profile cert-issuer vendor prfMaPI500LIEAuth93
```

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 52: ローカルで有効な証明書ページ

The screenshot displays the 'Local Significant Certificates (LSC)' configuration page for an AP. The left sidebar shows the navigation menu with 'Certificate' > 'LSC' selected. The main content area is divided into 'General' and 'AP Provisioning' tabs, with 'AP Provisioning' active. Under 'AP Provisioning', there is a table for 'Certificate Type' with one entry: 'CA' with a status of 'Not Present' and an 'Add' button. Below this is the 'General' section with a checked checkbox for 'Enable LSC on Controller'. The 'CA Server' section contains a 'CA server URL' field with the value 'http://9.43.0.101/caserver' and a note '(Ex: http://10.0.0.1:8080/caserver)'. The 'Params' section includes several input fields: 'Country Code' (US), 'State' (San Jose), 'City' (San Jose), 'Organization' (Cisco), 'Department' (Sales), 'E-mail' (sales@cisco.com), and 'Key Size' (1024). A vertical ID '279072' is visible on the right side of the page.

図 53: 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、コントローラの CA 証明書データベースに対して LSC CA 証明書を次のように追加/削除します。

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

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

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

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

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

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

デフォルトのキーサイズ値は 2048 ビットです。

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

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

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

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

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

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

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

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

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

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

- **show certificate lsc summary**

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

- **show certificate lsc ap-provision**

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

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

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

コントローラ GUI セキュリティ設定

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

- ケース1：ローカルMAC認可とローカルEAP認証

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

例：

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

- ケース2：外部MAC認可とローカルEAP認証

WLCで次のコマンドを入力します。

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

または

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

- RAP/MAPのMACアドレスをコントローラのMACフィルタリストに追加しません。
- WLC で、外部 RADIUS サーバの詳細を設定します。
- WLC で、**config macfilter mac-delimiter colon** コマンド設定を入力します。
- 外部 RADIUS サーバで、RAP/MAP の MAC アドレスを次の形式で追加します。
User name: 11:22:33:44:55:66 Password: 11:22:33:44:55:66

展開ガイドライン

- ローカル認証を使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラ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 に切り替わるできません。

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



第 7 章

ネットワークの状態の確認

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

- [Show Mesh コマンド \(177 ページ\)](#)
- [メッシュアクセスポイントのメッシュ統計情報の表示 \(184 ページ\)](#)
- [メッシュアクセスポイントのネイバー統計情報の表示 \(190 ページ\)](#)

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](#)
- [グローバルメッシュパラメータ設定の表示](#)
- [ブリッジグループ設定の表示](#)
- [VLAN タギング設定の表示](#)
- [DFS の詳細の表示](#)
- [セキュリティ設定と統計情報の表示](#)
- [GPS ステータスの表示](#)

一般的なメッシュネットワークの詳細の表示

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

- `show mesh env {summary | AP_name}` : すべてのアクセスポイント (概要) または特定のアクセスポイント (`AP_name`) の温度、ヒーターのステータス、イーサネットのステータスを表示します。アクセスポイント名、ロール (RootAP または MeshAP)、およびモデルも示されます。

- 温度は華氏と摂氏の両方で示されます。
- ヒーター ステータスは ON または OFF です。
- イーサネット ステータスは UP または DOWN です。



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

(Cisco Controller) > **show mesh env summary**

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

(Cisco Controller > **show mesh env SB_RAP1**

```

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

Temperature..... 39 C, 102
F
Heater..... OFF
Backhaul.....
GigabitEthernet0
GigabitEthernet0 Status..... UP
  Duplex..... FULL
  Speed..... 100
  Rx Unicast Packets..... 988175
  Rx Non-Unicast Packets..... 8563
  Tx Unicast Packets..... 106420
  Tx Non-Unicast Packets..... 17122
GigabitEthernet1 Status..... DOWN
POE Out..... OFF
Battery..... N/A

```

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

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

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

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

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

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

```
(Cisco Controller) > show mesh neighbor summary ap1500:62:39:70
AP Name/Radio Mac Channel Snr-Up Snr-Down Link-Snr Flags State
mesh-45-rap1      165    15    18    16    0x86b UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0 149     5     6     5    0x1a60 NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F 149     7     0     0    0x860  BEACON
```



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

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

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

メッシュ アクセス ポイントの詳細の表示

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

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

```
(Cisco Controller) > show ap config general aps
Cisco AP Identifier..... 1
Cisco AP Name..... AP5
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-AB 802.11a:-AB
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-N
```

```

Switch Port Number ..... 1
MAC Address..... 00:13:80:60:48:3e
IP Address Configuration..... DHCP
IP Address..... 1.100.163.133
...
Primary Cisco Switch Name..... 1-4404
Primary Cisco Switch IP Address..... 2.2.2.2
Secondary Cisco Switch Name..... 1-4404
Secondary Cisco Switch IP Address..... 2.2.2.2
Tertiary Cisco Switch Name..... 2-4404
Tertiary Cisco Switch IP Address..... 1.1.1.4

```

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

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

```

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

Total No of Aps stranded : 0

```

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

```
(Cisco Controller) > show advanced backup-controller
```

```

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

```

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

```
(Cisco Controller) > show advanced timer
```

```

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

```

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

```
(Cisco Controller) > show ap slots
```

```

Number of APs..... 3
AP Name Slots AP Model          Slot0   Slot1   Slot2   Slot3
-----
R1      2    LAP1520          802.11A 802.11BG
H1      3    AIR-LAP1521AG-A-K9 802.11BG 802.11A 802.11A
H2      4    AIR-LAP1521AG-A-K9 802.11BG 802.11A 802.11A 802.11BG

```

グローバルメッシュパラメータ設定の表示

次のコマンドを使用して、グローバルメッシュ設定についての情報を取得します。

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

```
(Cisco Controller) > show mesh config
Mesh Range..... 12000
Backhaul with client access status..... disabled
Background Scanning State..... enabled
Mesh Security
Security Mode..... EAP
External-Auth..... disabled
Use MAC Filter in External AAA server..... disabled
Force External Authentication..... disabled
Mesh Alarm Criteria
Max Hop Count..... 4
Recommended Max Children for MAP..... 10
Recommended Max Children for RAP..... 20
Low Link SNR..... 12
High Link SNR..... 60
Max Association Number..... 10
Association Interval..... 60 minutes
Parent Change Numbers..... 3
Parent Change Interval..... 60 minutes
Mesh Multicast Mode..... In-Out
Mesh Full Sector DFS..... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

ブリッジグループ設定の表示

ブリッジグループ設定を表示するには、次のコマンドを入力します。

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

VLAN タギング設定の表示

VLAN タギング設定を表示するには、次のコマンドを入力します。

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

DFSの詳細の表示

DFSの詳細を表示するには、次のコマンドを入力します。

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

```
(Cisco Controller) > show mesh dfs history
ap1520#show mesh dfs history
Channel 100 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 10
minute(s), 24 second(s)).
Channel is set to 136 (Time Elapsed: 18 day(s), 22 hour(s), 10 minute(s), 24
second(s)).
Channel 136 detects radar and is unusable (Time Elapsed: 18 day(s), 22 hour(s), 9
minute(s), 14 second(s)).
Channel is set to 161 (Time Elapsed: 18 day(s), 22 hour(s), 9 minute(s), 14 second(s)).
Channel 100 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 40 minute(s), 24
second(s)).
Channel 136 becomes usable (Time Elapsed: 18 day(s), 21 hour(s), 39 minute(s), 14
second(s)).
Channel 64 detects radar and is unusable (Time Elapsed: 0 day(s), 1 hour(s), 20
minute(s), 52 second(s)).
Channel 104 detects radar and is unusable (Time Elapsed: 0 day(s), 0 hour(s), 47
minute(s), 6 second(s)).
Channel is set to 120 (Time Elapsed: 0 day(s), 0 hour(s), 47 minute(s), 6 second(s)).
```

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

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

セキュリティ設定と統計情報の表示

セキュリティ設定と統計情報を表示するには、次のコマンドを入力します。

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

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

AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
-----
Tx Packets 14, Rx Packets 19, Rx Error Packets 0
Parent-Side Statistics:
-----
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
```

```

Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Child-Side Statistics:
-----
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0

```

GPS ステータスの表示

手順

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

- すべてのメッシュ AP の場所の概要を表示するには、次のコマンドを入力します。

show mesh gps location summary

- 次のコマンドを入力して、特定のメッシュ AP の場所情報を表示します。

show mesh gps location ap-name

メッシュアクセスポイントのメッシュ統計情報の表示

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



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

メッシュアクセスポイントのメッシュ統計情報の表示 (GUI)

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

ステップ 2 特定のメッシュアクセスポイントの統計情報を表示するには、目的のメッシュアクセスポイントの青のドロップダウン矢印の上にカーソルを移動し、[Statistics] を選択します。選択したメッシュアクセスポイントの [All APs] > *AP Name* > [Statistics] ページが表示されます。

このページには、メッシュネットワークでのメッシュアクセスポイントのロール、メッシュアクセスポイントが属するブリッジグループの名前、アクセスポイントが動作するバックホールインターフェイス、および物理スイッチポート数が表示されます。このメッシュアクセスポイントのさまざまなメッシュ統計情報も表示されます。

表 14: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 packets の数。不正な形式の packets の例には、不正な形式のショート DNS packet 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 packets 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。

統計情報	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の再認証要求の失敗数。
	Reauthentication Request Timeouts	選択したメッシュアクセスポイントとその親の間で発生した再認証要求のタイムアウト回数。
	Reauthentication Requests Successful	選択したメッシュアクセスポイントとその親の間で発生した再認証要求の成功数。
	Unknown Association Requests	親メッシュアクセスポイントが子から受信した不明なアソシエーション要求の数。不明なアソシエーション要求は、子が不明なネイバーメッシュアクセスポイントの場合によくみられます。
	Invalid Association Requests	親メッシュアクセスポイントが選択した子メッシュアクセスポイントから受信した無効なアソシエーション要求の数。この状況は、選択した子が有効なネイバーであるが、アソシエーションが許可される状態ではないときに発生することがあります。

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

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、[LinkTest] を選択します。ポップアップ ウィンドウが表示されます。
- [Submit] をクリックしてリンクテストを開始します。リンクテストの結果が [Mesh > LinkTest Results] ページに表示されます。
- [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) $\text{パケットエラーレートの割合} = 1 - (\text{伝送に成功したパケット数} / \text{伝送したパケットの総数})$



第 8 章

メッシュ アクセス ポイントの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 \(193 ページ\)](#)

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 54: [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	MESHDEM01	N/A
1522MAP2	AIR-LAP1522AG-A-K9	00:22:be:42:fe:00	00:22:be:42:fe:00	1	MESHDEM01	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 55: [All APs Summary] ページ

All APs

Search by AP MAC

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
HJRAP1	00:1d:71:0d:e1:00	0 d, 22 h 12 m 37 s	Enable	REG	Bridge	MIC
HJMAP3	00:1d:71:0d:d5:00	0 d, 22 h 05 m 04 s	Enable	REG	Bridge	MIC
HJMAP1	00:1d:71:0c:f4:00	0 d, 22 h 04 m 48 s	Enable	REG	Bridge	MIC
HJMAP2	00:1d:71:0c:f0:00	0 d, 22 h 04 m 53 s	Enable	REG	Bridge	MIC
HPRAP1	00:1e:14:48:43:00	0 d, 05 h 35 m 24 s	Enable	REG	Bridge	MIC
HPMAP1	00:1b:d4:a7:78:00	0 d, 22 h 04 m 25 s	Enable	REG	Bridge	MIC

273952

ステップ 5 [AP Name] をクリックして詳細ページを表示し、[Interfaces] タブを選択して、アクティブな無線インターフェイスを表示します。

使用中の無線スロット、無線タイプ、使用中のサブバンド、動作状態（UP または DOWN）がまとめて表示されます。

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

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

コントローラ名の設定後、メッシュ アクセス ポイントがリブートします。

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

debug コマンド

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

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

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

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

リモートデバッグコマンド

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

コントローラでリモートデバッグを起動するには、次のコマンドを入力します。

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

APコンソールアクセス

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

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

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

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

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

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

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

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



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

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 56: ケーブルモデム コンソールのアクセス コマンド

```
R&P-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

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

279059

図 57: 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
taskInfo        taskPrioritySet   taskResume       taskShow         taskDelete
taskTrace       usfsShow          version          write_memory     taskSuspend
zone
-----
[HeapManager] [SA] [cm_hal] [docsis_ctl] [embedded_target] [enet_hal]
[event_log] [flash] [forwarder] [ip_hal] [msgLog] [non-vol] [pingHelper]
[snmp] [snoop] [usb_hal]

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

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

CM -> docsis_ctl

CM/DocsisCtl>
RAP-CM-N1#

```

279060



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

ケーブル モデム コンソール ポートの有効化

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



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

- ケーブル モデムの IP アドレスに次のコマンドを入力して、SNMP を介してケーブル モデム コンソール ポートを有効にします。

```
snmpset -c private IP_ADDRESS cmConsoleMode.0 i N
```

OID を使用して、次のコマンドを入力します。

```
snmpset -c private IP_ADDRESS  
1.3.6.1.4.1.1429.77.1.4.7.0 i N
```

IP_ADDRESS は任意の Ipv4 アドレス、N は整数、2 は読み取りと書き込みの有効化、1 は読み取り専用、0 は無効化です。

例 :

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

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

```
SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
```

OID を使用して、この行を入力します。

```
SA-CM-MIB::cmConsoleMode.0 = INTEGER: readWrite(2)
```

ケーブル モデムを使用した AP1572xC/AP1552C のリセット

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

次の snmpset コマンドを入力して、AP をリセットします。

```
Snmpset -v2c -c public IP ADDRESS 1.3.6.1.4.1.1429.77.1.3.17.0 i 1
```

IP ADDRESS は、ケーブル モデムの IPv4 アドレスです。

メッシュ アクセス ポイント CLI コマンド

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

```

H1 • show llbsh ?
  adjacency    l'ESH Adjacency
  astools      l'ESH Anti-strand tools
  backhaul     l'ESH backhaul
  channel      l'ESH channel
  canfig       l'ESH config paranenter
  dfs          l'ESH dfs lnformation
  ethernet     show mesh Ethernet bridging
  forwarding   l'ESH Forwarding
  inventory    platform inventory
  linktest     l'ESH linktest stats
  nmule        l'ESH node detail
  nprf         l'ESH NTP tool
  security     l'ESH Security show      |2
  simulation   show simulated configuration |3
  status       l'ESH status

```

```

H1 show mesh config
 rtsfhreshold1 la 0, ehs 0, a.1lin 0, c.0lex 0
 rtsfhreshold1 lbg 0, aifs 0, a.1Hin 0, a.1lax 0
 huRetries 0. 1lri<Rate 0 qOepth 0
 802.11Mat 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 capl01Bp client mb
AdminState ADHIN ENABLED
SuVer S. 2.98.0
NumFl1 ledSlots 2
Name HJRAP1
Location default location
Huarllame SEYf-C11ffROLLER
Huarrlp 209.165.200.227
Huartt.Ner 0.0.0.0
ApHocle Brld!JE!
ApSubl'lode Not [m]figured
OperationState UP
CAP11N' Path nru 1485
Link!U:liting disabled
ApRole RootAP
ApBac:khaul 802.11a
ApBac:khaulthannel 5805
ApBac:khaulSlot 1
ApBac:khaul11gEnabled 0
ApBac:l<haul1xRate 24000
Ethernet Brldg1rg State 0
Public Safety State enabled

```

```

HJHAP111lehoi.I nesh adjacency ?
all HESH Adjacency All
child HESH Adjacency Child
parent MESH Adjacency Parent

```

01

```

HJNap4#show mesh status
show MESH Status
MeshAP in state Maint
Uplink Backbone: Virtual-Dot11Radio0
Downlink Backbone: Dot11Radio1
Configured BGN: HuckJr
rxNeighReq 129790 rxNeighResp 66976 txNeighReq 33938 txNeighResp 129790
rxNeighReq 1147275 txNeighUpd 202060
nextChan 0 nextAnt 0 downAnt 0 downChan 0 curAnts 0
nextNeigh 1. malformedNeighPackets 4.poorNeighSnr 1
blacklistPackets 0.insufficientMemory 0.authenticationFailures 0
Parent Changes 3. Neighbor Timeouts 0
Vector through 0017.94fe.c3bf:
Vector ease 1 -1, FWD: 0017.94fe.c3bf

```

273949

```

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

```

273950

メッシュアクセスポイントデバッグコマンド

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

- **debug mesh ethernet bridging** : イーサネットブリッジングをデバッグします。
- **debug mesh ethernet config** : VLAN タギングに関連付けられているアクセスおよびトランクポート設定をデバッグします。
- **debug mesh ethernet registration** : VLAN レジストレーションプロトコルをデバッグします。このコマンドは、VLAN タギングに関連付けられています。
- **debug mesh forwarding table** : ブリッジグループが含まれている転送テーブルをデバッグします。
- **debug 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、社内でも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、孤立タイマーのリポートが実行された場合に孤立状態と見なされます。孤立タイマーのリポートが発生すると、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 を有効または無効にします。ディセーブルの場合、AP は孤立状態の AP リストをコントローラに送信しません。
- **show mesh astools stats** : 孤立状態の AP とそれぞれのリスナー (存在する場合) のリストを表示します。
- **debug mesh astools troubleshoot mac-addr start** : *mac-addr* の最適なネイバーに、リッスンを開始するメッセージを送信します。
- **debug mesh astools troubleshoot mac-addr stop** : *mac-addr* の最適なネイバーに、リッスンを停止するメッセージを送信します。
- **clear mesh stranded [all | mac of b/g radio]** : 孤立状態の AP エントリをクリアします。

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

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 アドレスを変更し、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」と判断しても、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できない場合があります。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 58: 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 Name
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せんが、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。

The screenshot displays the Cisco Wireless Management interface for the configuration of AP1562.EC4A.4D30. The 'General' tab is selected, and the 'AP Mode' dropdown menu is open, showing options: local, FlexConnect, monitor, Sniffer, Bridge, and SE-Connect. A red arrow points to the 'Bridge' option.

General		Versions	
AP Name	AP1562.EC4A.4D30	Primary Software Version	8.5.103.0
Location	default location	Backup Software Version	8.5.1.204
AP MAC Address	00:62:ec:4a:4d:30	Predownload Status	None
Base Radio MAC	00:62:ec:06:5d:40	Predownloaded Version	None
Admin Status	Disable	Predownload Next Retry Time	NA
AP Mode	Bridge	Predownload Retry Count	NA
AP Sub Mode	local	Boot Version	1.1.2.4
Operational Status	monitor	IOS Version	8.5.103.0
Port Number		Mini IOS Version	0.0.0.0
Venue Group		IP Config	
Venue Type	Unspecified	CAPWAP Preferred Mode	Ipv4 (Global Conf)
Add New Venue		DHCP Ipv4 Address	10.70.0.129
Language	Venue Name	Static IP (Ipv4/Ipv6)	<input type="checkbox"/>
Network Spectrum Interface Key	9118035629CC881ADEFE36B765B885A	Fabric	
GPS Location		Fabric Status	Disabled
GPS Present	No	Fabric L2 Instance ID	0



第 9 章

Cisco Prime Infrastructure によるメッシュ アクセス ポイントの管理

Cisco Prime Infrastructure は、企業全体の WLAN システム管理を行う最適なプラットフォームです。Cisco WCS は、メッシュを仮想化およびコントロールするための広範囲のツールを提供します。これらは、信号対雑音比のヒストグラム、メッシュの詳細情報、メッシュ アクセス ポイントのネイバーおよびリンク情報、7 日間の一時リンク情報、および電波干渉を特定し避けるツールなどを含みます。

この項では、次の Prime Infrastructure モニタリング機能について説明します。

Cisco Prime Infrastructure のメッシュ構成と監視の詳細については、以下のリンクで『PI Users Guide』を参照してください。 https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/user/guide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide.pdf



索引

C

- CAC [154](#)
 - メッシュ ネットワーク内の [154](#)
- CAPWAP [11](#)
- CleanAir [73, 75, 77](#)
 - Advisor [77](#)
 - アクセス ポイント配置の推奨事項 [75](#)
 - ライセンス [77](#)
 - 動作モード [73](#)

D

- Dynamic Frequency Selection (動的周波数選択) [8](#)

L

- LinkSNR 要件 [30, 31](#)

M

- mesh [189](#)
 - 統計情報 [189](#)
 - GUI を使用したアクセス ポイントの表示 [189](#)

P

- Pseudo MAC とマージ [73](#)

W

- Wplus ライセンス [34](#)

あ

- アクセス ポイントのロール [2, 87, 201](#)
 - 定義 [87, 201](#)

こ

- コントローラ ソフトウェアのアップグレード [84](#)
- コントローラ プランニング [33](#)

せ

- セルのプランニングと距離 [54, 57](#)
 - AP1520 シリーズ [54](#)
 - AP1550 シリーズ [57](#)

は

- バックアップ コントローラ [91](#)

ひ

- ビーム幅 [10](#)

ふ

- フレネルゾーン [45, 47](#)

め

- メッシュ レンジ [20](#)
 - 設定 [20](#)

ゆ

- ユニバーサル アクセス [18](#)

ろ

- ローカルで有効な証明書 [168](#)

わ

- ワイヤレス ソフトウェアの互換性マトリクス [84](#)

