Enterprise Mobility 4.1 デザイン ガイド
Cisco Validated Design I

2008 年 5 月

Text Part Number: OL-14435-01-J

【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、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

CONTENTS

はじめに

マニュアルの目的

このマニュアルでは、Wireless LAN Controller ソフトウェア リリース 4.1 で追加された機能を使用した、企業向けの Cisco Unified Wireless Network ソリューションの設計および実装について説明します。

対象読者

このマニュアルは、無線ネットワークの設計および実装を担当する経験豊富なネットワーク管理を対象としています。

マニュアルの構成

次の表に、このマニュアルの内容を示します。

章	説明
第 1 章「Cisco Unified Wireless Network Solution の概要」	企業向けの Cisco Unified Wireless Network の利点と特徴について説明します。
第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」	企業の Cisco Unified Wireless の展開における設計上および運用上の主な考慮事項について説明します。
第 3 章「WLAN 無線周波の設計に関する考慮事項」	さまざまな無線ローカル エリア ネットワーク（WLAN）環境における Radio Frequency（RF; 無線周波）の考慮事項を理解するために必要な RF の基本情報について説明します。
第 4 章「Cisco Unified Wireless Network アーキテクチャ ― 基本的なセキュリティ機能」	ネイティブに使用できる 802.11 セキュリティ オプションと Cisco Unified Wireless ソリューションの高度なセキュリティ機能について説明します。また、これらの機能を組み合せて最適な WLAN ソリューションを作成する方法も紹介します。
第 5 章「Cisco Unified Wireless QoS」	WLAN 実装の QoS（Quality of Service）について説明します。
第 6 章「Cisco Unified Wireless のマルチキャスト設計」	IP マルチキャスト転送における強化点を説明し、無線環境でのマルチキャストの展開方法に関する情報を提供します。
第 7 章「Cisco Unified Wireless Hybrid REAP」	Cisco Centralized WLAN アーキテクチャとこれに使用される Hybrid REAP（H-REAP）について説明します。
第 8 章「Cisco メッシュ型無線ネットワーキング」	無線メッシュの使用について説明します。
第 9 章「VoWLAN の設計に関する推奨事項」	Voice over WLAN（VoWLAN）ソリューションを展開する際の設計上の考慮事項について説明します。
第 10 章「Cisco Unified Wireless Guest Access Service」	中央集中型 WLAN アーキテクチャにおけるゲスト アクセス サービスの使用について説明します。
第 11 章「モバイル アクセス ルータ、ユニバーサル ブリッジ クライアント、および Cisco Unified Wireless」	モバイル アクセス ルータ、ユニバーサル ブリッジ クライアント、およびメッシュ ネットワークの使用について説明します。
第 12 章「Cisco Unified Wireless とモバイル IP」	Cisco Unified Wireless Network（WiSM）での Cisco Mobile Client（CMC; Cisco モバイル クライアント）の相互作用について説明します。
第 13 章「Cisco Unified Wireless ロケーションベース サービス」	Cisco Location-Based Service（LBS）ソリューションと、設計、構成、インストール、および展開に関して特別に考慮すべき領域について説明します。
用語集	このマニュアルで使用する主な用語をリストして定義します。

CHAPTER 1

Cisco Unified Wireless Network Solution の概要

この章では、企業向けの Cisco Unified Wireless Network の利点と特徴について説明します。Cisco Unified Wireless Network ソリューションは、ビジネス上重要なモビリティを実現するための、安全で拡張性があり、かつコスト効率の優れた無線 LAN を提供します。Cisco Unified Wireless Network は、無線と有線を統合した業界唯一のソリューションであり、費用対効果の高い、無線 LAN（WLAN）のセキュリティ保護、展開、管理の方法を提供し、企業が直面している問題を管理します。屋内と屋外に対応したこの強力なソリューションは、有線ネットワークと無線ネットワークの利点を統合することにより、総所有コストを低く抑えながら、高性能で、管理が容易な、安全性に優れた WLAN を提供します。

WLAN の概要

モバイル ユーザは、有線ユーザが現在享受しているのと同等のアクセス可能性、セキュリティ、QoS（Quality of Service）、および高可用性を求めています。会社、自宅、出張先、国内、海外を問わず、どこにいても接続に対するニーズがあります。技術的に困難であることは明白ですが、この課題を克服する役割をモビリティが果たします。企業は、モバイル ソリューションおよび無線ソリューションからビジネス バリューを導き出しています。かつて垂直的市場であったテクノロジーが今や主流となり、音声アプリケーション、リアルタイム情報、基幹アプリケーション（E メールやカレンダー）、企業データベース、サプライ チェーン管理、販売の自動化、顧客関係管理にアクセスするうえで欠かせないツールです。

WLAN ソリューションの利点

WLAN は、通信するための新しい手段をユーザに提供すると同時に、現在のビジネスのやり方に対応します。WLAN によって得られる利点は、次のとおりです。

- *ビルディングおよびキャンパス内でのモビリティ：*ネットワークへの常時接続が必要なアプリケーションおよびキャンパス環境内での移動が必要なアプリケーションの実装が簡単になります。
- *利便性：*大規模で開けた領域のネットワーク化が簡素化されます。
- *柔軟性：*ケーブルが届く範囲ではなく、最も適切または都合の良い場所で作業できるようになります。どこにいるかが重要なのではなく、作業を終わらせることが重要なのです。
- *一時的なスペースの設置が簡単に：*会議室、作戦室、またはブレインストーミング　ルームのネットワークを参加者の人数に合わせてすばやくセットアップできるようになります。
- *ケーブル配線コストの削減：*差分に対応できるように WLAN を導入するため、偶発的にケーブル プラントを設置する必要性が減少します。
- *簡単な追加、移動、変更、およびサポートコストと保守コストの削減：*一時的なネットワークのセットアップがさらに簡単になり、移行の問題やコストのかかる直前の修正が軽減します。
- *効率の向上：*調査の結果、WLAN ユーザのネットワーク接続時間は有線ユーザよりも 1 日あたり 15% 長いことが分かりました。
- *生産性の向上：*ネットワーク接続に簡単にアクセスできるようにすることで、ビジネス生産性ツールを有効利用できるようになります。生産性に関する調査では、WLAN ユーザの場合で 22% の増加が示されています。
- *共同作業が簡単に：*会議室など、どの場所からでもコレボレーション ツールにアクセスできるようになります。ファイルをその場で共有したり、必要な情報をすぐに用意できます。
- *オフィス空間のさらなる有効利用：*大人数のチームの会議など、どのようなグループにも対応できる柔軟性が得られます。
- *エラーの削減：*データは、ネットワーク アクセスを利用できるときではなく、収集時に直接システムに入力されます。
- *企業のパートナーおよびゲストに対する効率、パフォーマンス、およびセキュリティの向上：*ゲスト アクセス ネットワークを実装することで促進します。
- *ビジネスの回復力の向上：*従業員のモビリティが向上するため、WLAN で別の場所に迅速に再展開できるようになります。

WLAN システムの要件

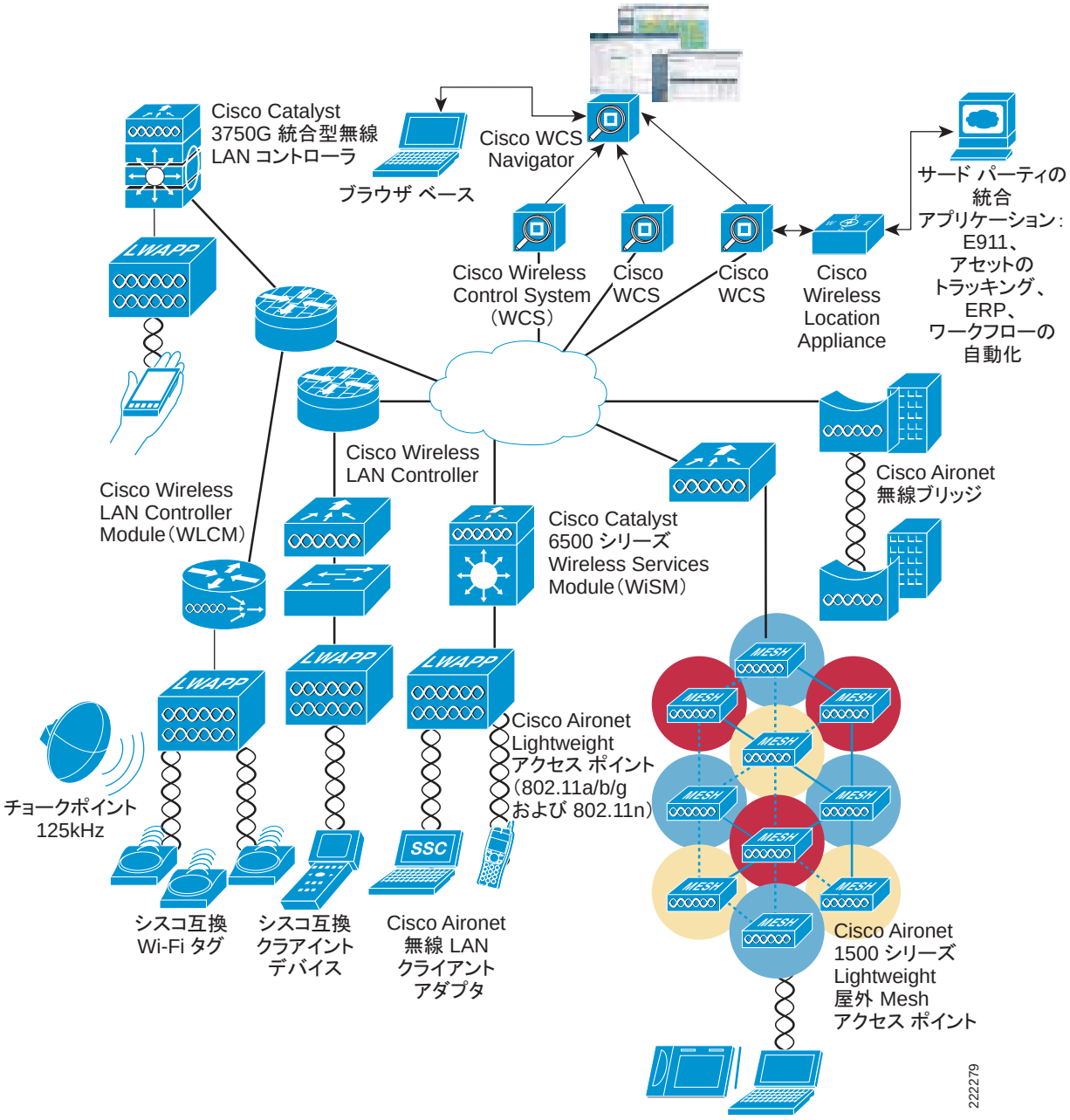
WLAN システムは、既存の有線企業ネットワークやキャンパスまたは個々のテレワーカ向けの支社内の独立したネットワークとして実行したり、小売、製造、または医療産業のアプリケーションと組み合わせて実行できます。WLAN では、リソースにケーブルで接続している場合と同様に、セキュリティで保護され、暗号化され、認証された通信を行えるようにし、データ、通信、およびビジネス サービスへのアクセスを提供する必要があります。

WLAN では、以下を行える必要があります。

- *従業員がネットワークに接続していないときもリソースへのアクセス可能性を維持：*このアクセス可能性により、従業員は、会議室で顧客と打ち合わせ中でも、社内の食堂で同僚と昼食をとっているときでも、隣接する建物でチームのメンバと共同作業しているときでも、ビジネスのニーズにさらに迅速に対応できるようになります。
- *未許可の保護されていない不正な WLAN アクセス ポイントから企業を保護：*IT マネージャは、不正アクセスポイントとそれらが接続されているスイッチ ポート、両方のアクセス ポイントでアクティブな参加、および RF 環境の継続的なスキャンおよび監視を行っているクライアント デバイスをすばやく自動的に検出して特定できる必要があります。
- *統合されたネットワーク サービスのすべての利点をモバイル ユーザにも提供：*リアルタイムのトラフィックを優先的に扱うことで、ビデオおよびオーディオ情報がすぐに届くようにする QoS を使用している WLAN では、IP テレフォニーおよび IP ビデオ会議がサポートされています。企業フレームワークの一部であるファイアウォールおよび侵入検出が、無線ユーザまで拡張されます。
- *許可されたユーザを分け、不正ユーザをブロック：*無線ネットワークのサービスをゲストおよびベンダーに安全に拡張できます。WLAN は、別のパブリック ネットワーク、つまりゲスト ネットワークに対するサポートを構成できる必要があります。
- *別の場所から来た従業員に、簡単かつセキュリティで保護されたネットワーク　アクセスを提供：*空いている部屋や、使用可能なイーサネット ポートを探す必要がありません。ユーザは WLAN のどの場所からでも安全にセキュリティにアクセスできる必要があります。従業員は IEEE 802.1x および Extensible Authentication Protocol（EAP; 拡張認証プロトコル）によって認証され、WLAN 上で送受信されるすべての情報は暗号化されます。
- *中央またはリモートのアクセス ポイントを簡単に管理：*ネットワーク管理者は、WLAN キャンパス展開、支社、または小売、製造、医療領域内の数百から数千ものアクセス ポイントを簡単に展開、運用、および管理できる必要があります。理想的なのは、中規模から大規模の組織に、有線 LAN に期待されるものと同等レベルのセキュリティ、スケーラビリティ、信頼性、展開のしやすさ、および管理性を提供する 1 つのフレームワークです。
- *拡張セキュリティ サービス*：WLAN Intrusion Prevention System（IPS; 侵入防御システム）および Intrusion Detection System（IDS; 侵入検知システム）の制御により、無線による脅威の抑止、セキュリティ ポリシーの遵守の強制、および情報の保護が可能になります。
- *音声サービス*：Cisco Unified Wired Network および Wireless Network と Cisco Compatible Extensions の音声対応クライアント デバイスを通じて、音声通信に無線ネットワークのモビリティと柔軟性をもたらします。
- *ロケーション サービス：*高価な資産の追跡、IT 管理、ロケーションに基づくセキュリティ、ビジネス ポリシーの強制など重要な用途で、WLAN インフラストラクチャ内部から直接、数百個から数千個の Wi-Fi およびアクティブな RFID デバイスを同時に追跡します。
- *ゲスト アクセス*：カスタマ、ベンダー、およびパートナーに対して有線および無線 LAN への簡単なアクセスを提供し、生産性の向上の支援、リアルタイムな共同作業の推進を行い、企業の競争力を維持して、WLAN の完全なセキュリティを保ちます。

エンタープライズの WLAN は、ネットワーク接続に最も効果的な手段の 1 つとなっています。図 1-1 は、Cisco Unified Wireless Network の要素を示しています。

図 1-1　企業における Cisco Unified Wireless Network のアーキテクチャ



次の 5 つの相互に接続された要素が連携して、統一されたエンタープライズクラスの無線ソリューションを提供します。

- クライアント デバイス
- アクセス ポイント
- ネットワーク統合
- 国際的なネットワーク管理
- モビリティ サービス

クライアント デバイスを基にして、各要素は、ネットワークのニーズの進化および成長に応じて機能を追加すると同時に、包括的でセキュリティで保護された WLAN ソリューションを作るために上位および下位の要素と相互に接続します。

Cisco Unified Wireless Network は、費用対効果の高い、WLAN のセキュリティ保護、展開、管理の方法を提供し、企業が直面している問題を管理します。このフレームワークは、有線および無線ネットワークを統合して拡張し、総所有コストを低く抑えながら、拡張性、管理容易性、安全性に優れた WLAN を提供します。Cisco Unified Wireless Network は、有線 LAN に期待されるレベルと同等のセキュリティ、信頼性、展開のしやすさ、管理を無線 LAN に対して提供します。

Cisco Unified Wireless Network の詳細は、次の URL を参照してください。
http://www.cisco.com/go/unifiedwireless

Cisco Unified Wireless Network

Cisco Unified Wireless Network の基本機能セットには、Cisco Aironet アクセス ポイント（AP）、Wireless Control System（WCS）、および Wireless LAN Controllers（WLC）が含まれます。たとえば、Cisco Catalyst 6500 Wireless Services Module（WiSM）、440X、2106 WLC、WLCM ISR モジュール、WS-C3750G 統合コントローラです。

基本機能セットは、現在、次の構成で展開可能です。

- AP および WLC
- AP、WLC、および WCS
- AP、WLC、WCS、および LBS

オプションの Cisco Compatible Extensions クライアント デバイス、および Cisco Secure Services Client を加えると、高度なエンタープライズクラスのセキュリティ、拡張された RF 管理、高度な相互運用性など、他の利点も得られます。

CHAPTER 2

Cisco Unified Wireless のテクノロジーおよびアーキテクチャ

この章では、企業で Cisco Unified Wireless を展開する場合の、設計上および運用上の主な考慮事項について説明します。

この章では、次の内容について説明します。

- LWAPP
- ローミング
- ブロードキャストおよびマルチキャストの処理
- 製品の選択
- 展開に関する考慮事項

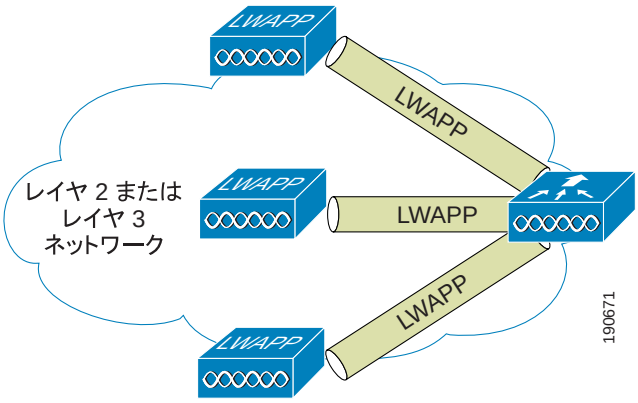
この章で扱う内容のほとんどは、この文書の後の章でさらに詳しく説明されます。Cisco Unified Wireless テクノロジーについて詳しく説明した資料としては、『*Deploying Cisco 440X Series Wireless LAN Controller*』（http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html）をお勧めします。

LWAPP の概要

Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）は、シスコの中央集中型 WLAN アーキテクチャの基盤となるプロトコルです。このプロトコルは、WLAN の設定や管理のほか、中央集中型 WLAN コントローラ（WLC）と WLAN クライアントの間のトラフィックのトンネリングの機能を提供します。図 2-1 は、基本的な中央集中型 WLAN アーキテクチャの概略図です。この図では、LWAPP AP は LWAPP 経由で WLC に接続されています。

（注）　WLAN の基本機能は同じであるため、WLC という用語は、一般的にすべての Cisco WLAN コントローラを表すために使用されています。コントローラがスタンドアロン アプライアンス、WLC モジュールを持つ ISR、サービス モジュールまたは統合 WLC を持つ Catalyst スイッチのいずれであっても関係ありません。

図 2-1　WLC に接続された LWAPP AP



LWAPP プロトコルは多数の機能コンポーネントから構成されますが、この文書では、中央集中型 WLAN ネットワークの設計および運用に影響を与えるものについてのみ説明します。

LWAPP の主な機能は、以下のとおりです。

- スプリット MAC トンネル
- L2 または L3 ベースのトンネル
- WLC ディスカバリ プロセス

スプリット MAC

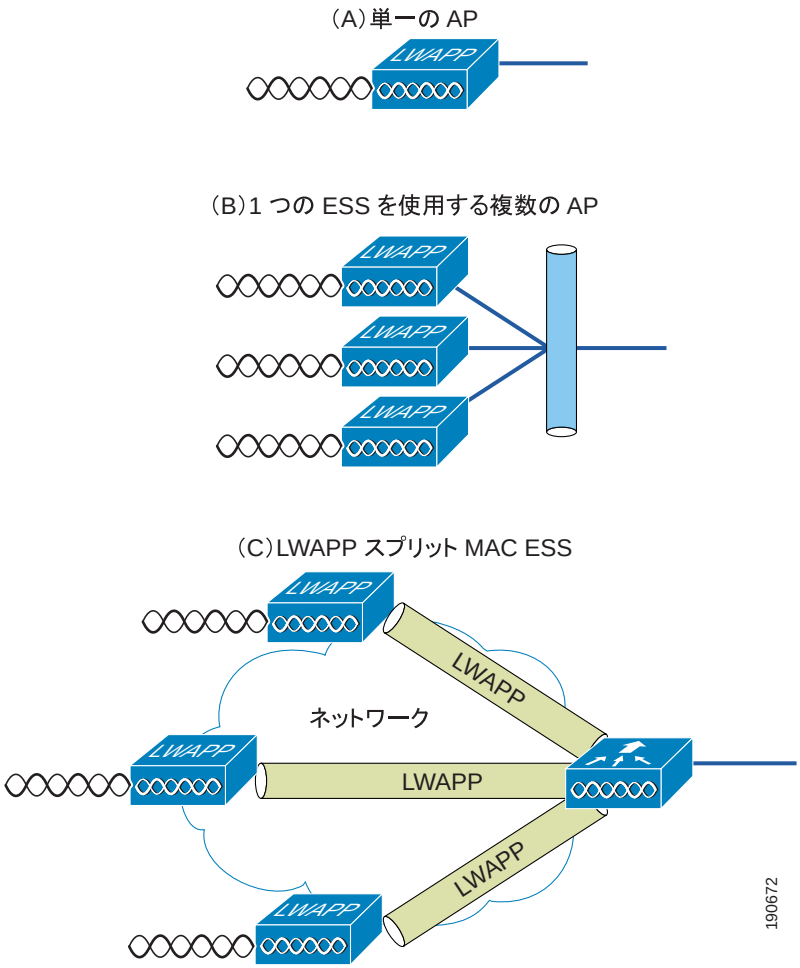
LWAPP プロトコルの主要なコンポーネントの 1 つに、スプリット MAC という概念があります。これは、802.11 プロトコルでの動作の一部を LWAPP AP が管理し、残りの部分を WLC が管理するというものです。図 2-2c は、スプリット MAC の概念を図に表したものです。

最も単純な汎用 802.11 AP は、Basic Service Set Identifier（BSSID）へのアソシエーションに基づいて有線ネットワークに WLAN クライアントをブリッジする 802.11 MAC レイヤ無線にすぎません。図 2-2a を参照してください。802.11 規格では、AP を 1 台だけ使用するという概念（前述）が拡張され、複数の AP に対して 1 つの Extended Service Set（ESS）を割り当てることができます。そして、そのように複数の AP が同じ ESS 識別子（ESSID; 通常は「SSID」と言う）を使用することで、WLAN クライアントがそれら複数の AP を経由して共通のネットワークに接続できるようになります。図 2-2b を参照してください。

LWAPP スプリット MAC の概念では、通常は個々の AP によって実行されるすべての機能を、LWAPP AP と WLC の 2 つの機能コンポーネントに割り振ります。この 2 つのコンポーネントは、ネットワーク経由で LWAPP プロトコルを使用してリンクされ、個々の AP を使用する場合と同等の無線 / ブリッジ サービスを、展開や管理がより容易な方法で提供します。

（注） スプリット MAC により、WLAN クライアントと WLC の有線インターフェイスとの間のレイヤ 2 接続はスムーズになりますが、すべてのトラフィックが LWAPP トンネルを通過できるわけではありません。WLC は、IP Ethertype フレームだけを転送します。デフォルトの動作では、ブロードキャストやマルチキャスト トラフィックは転送されません。WLAN の展開時にマルチキャストやブロードキャストの要件を検討するときには、このことが重要になりますので、覚えておいてください。

図 2-2　スプリット MAC の概念



単純で時間に依存した処理は、通常 LWAPP AP によってローカルで管理され、より複雑で時間への依存が少ない処理は WLC によって管理されます。

たとえば、LWAPP AP は次のような操作を扱います。

- クライアントと AP 間のフレーム交換ハンドシェイク
- ビーコン フレームの転送

- 省電力モードでのクライアントに対するフレームのバッファリングおよび転送
- クライアントからのプローブ要求フレームへの応答（プローブ要求は WLC にも送信され、そこで処理されます）
- 受信したプローブ要求の通知の WLC への転送
- 受信したすべてのフレームを持つスイッチへのリアルタイムでの信号品質情報のプロビジョニング
- 各無線チャネルにおけるノイズ、干渉、およびその他の WLAN の監視
- 他の AP の存在の監視
- 802.11 フレームの暗号化および復号化

その他の機能は WLC により処理されます。WLC が提供する MAC レイヤ機能には、次のようなものが含まれます。

- 802.11 認証
- 802.11 アソシエーションおよび再アソシエーション（モビリティ）
- 802.11 フレームの転送およびブリッジ
- 802.1X/EAP/RADIUS 処理
- 有線インターフェイス上の 802.11 トラフィックの終端、ただし、このガイドの後半で説明する REAP 機能および H-REAP 機能が設定された AP は除きます。

LWAPP トンネルは、次の 2 つのカテゴリのトラフィックをサポートしています。

- LWAPP 制御メッセージ：WLC と AP の間で制御、設定、および管理に関する情報を伝達するために使用されます。
- 無線クライアント データのカプセル化：レイヤ 2 無線クライアント トラフィックをカプセル化された IP Ethertype パケットで AP から WLC に転送します。

カプセル化されたクライアント トラフィックは、WLC に到達すると、対応する WLC の VLAN インターフェイスおよびポートにマップされます。このインターフェイスのマッピングは、WLC で WLAN の設定の一部として定義されます。通常、インターフェイス マッピングは静的に実行されますが、EAP 認証が正常に終了した場合、アップストリーム AAA サーバにより送信されるパラメータに基づいて、WLAN クライアントを特定の VLAN に動的にマップできます。WLAN の設定パラメータには、VLAN の割り当てのほか、SSID、動作状態、認証およびセキュリティの手段、および QoS に関するものがあります。

レイヤ 2 およびレイヤ 3 のトンネル

LWAPP では、イーサネット フレーム内（レイヤ 2）または UDP パケット内（レイヤ 3）でのトンネリングが可能です。これは、WLC 上で設定可能です。一度にサポートされる方式は 1 つだけです。また、すべての WLC でレイヤ 2 方式がサポートされているわけではありません。

レイヤ 2 トンネル

レイヤ 2 LWAPP を展開する場合、LWAPP トンネルで WLC と LWAPP AP の間のトラフィックをカプセル化するために Ethertype 0xBBBB が使用されているとしても、WLC と LWAPP AP では IP アドレスが必要になります。LWAPP AP と WLC の間の通信はすべて、Ethertype 0xBBBB を使用してカプセル化されます。

レイヤ 2 LWAPP は、AP の接続を確立したり、AP の設定を行ったりするための単純な方法の 1 つですが、一般に企業での展開ではこの方法は勧められません。したがって、本書ではこれ以上詳しくは説明しません。

現在、シスコがレイヤ 2 方式をベスト プラクティスとして推奨していない主な理由は、次のとおりです。

- LWAPP AP と WLC の間のレイヤ 2 接続により、ネットワーク内で AP や WLC を配置できる場所が制限される可能性があります。この制限を回避するために企業ネットワーク全体にレイヤ 2 転送を拡張することは、現在、ベスト プラクティスとして推奨されていません。
- レイヤ 2 LWAPP は、一部の LWAPP AP および WLC プラットフォームではサポートされていません。
- クライアント トラフィックの DSCP 値はトンネル内で保持されますが、レイヤ 2 LWAPP は、Ethertype フレームに対して対応する CoS マーキングを提供しないため、トンネルされたトラフィックに透過的なエンドツーエンドの QoS を提供することはできません。

レイヤ 3 トンネル

レイヤ 3 LWAPP は、推奨されるトンネル タイプです。この方式では、LWAPP AP と WLC 間の通信をスムーズにするために、IP UDP パケットが使用されます。L3 LWAPP は、トンネル パケットのフラグメンテーションおよび再アセンブリを実行できます。これにより、クライアント トラフィックは 1500 バイトの Maximum Transmission Unit（MTU; 最大転送単位）を使用できるようになり、トンネル オーバーヘッドの調整は不要になります。

（注） フラグメンテーションおよび再アセンブリの処理を最適化するため、WLC または AP が受信するフラグメントの数は制限されます。Cisco Unified Wireless Network を展開する上でサポートされる理想的な MTU のサイズは 1500 バイトですが、MTU が 500 バイト程度のネットワークであれば、ソリューションは問題なく動作します。

以下は、LWAPP 操作を示すためのレイヤ 3 LWAPP パケット キャプチャです。サンプル デコードは、Wireshark Network Analyzer を使用してキャプチャしたものです。

（注） Wireshark のデフォルト設定では、Cisco LWAPP パケットを正しくデコードすることはできません。この問題は、プロトコルの設定で SWAP Frame Control オプションを使用することで解決できます。

LWAPP コントロール パケット は、LWAPP コントロール パケットのデコードを示しています。WLC からのすべての LWAPP コントロール パケットと同様、このパケットも WLC から送信元 UDP ポート 12223 を使用して送られてきたものです。Control Type 12 は、AP 設定情報を LWAPP AP に渡すために WLC により使用される設定コマンドを表します。コントロール パケットのペイロードは AES で暗号化されています。この暗号化では、LWAPP AP が WLC との接続を最初に確立したときに実行される PKI 認証プロセスで生成されたキーが使用されます。

図 2-3　LWAPP コントロール パケット

LWAPP の 802.11 プローブ要求 は、802.11 プローブ要求を含む LWAPP パケットのデコードを示しています。すべての LWAPP でカプセル化される 802.11 フレームと同様、このパケットも UDP ポート 12222 を使用して LWAPP AP から WLC に送られるパケットです。この例では、RF 情報を WLC に提供するために、LWAPP パケットには RSSI 値と SNR 値も含まれています。

図 2-4　LWAPP の 802.11 プローブ要求

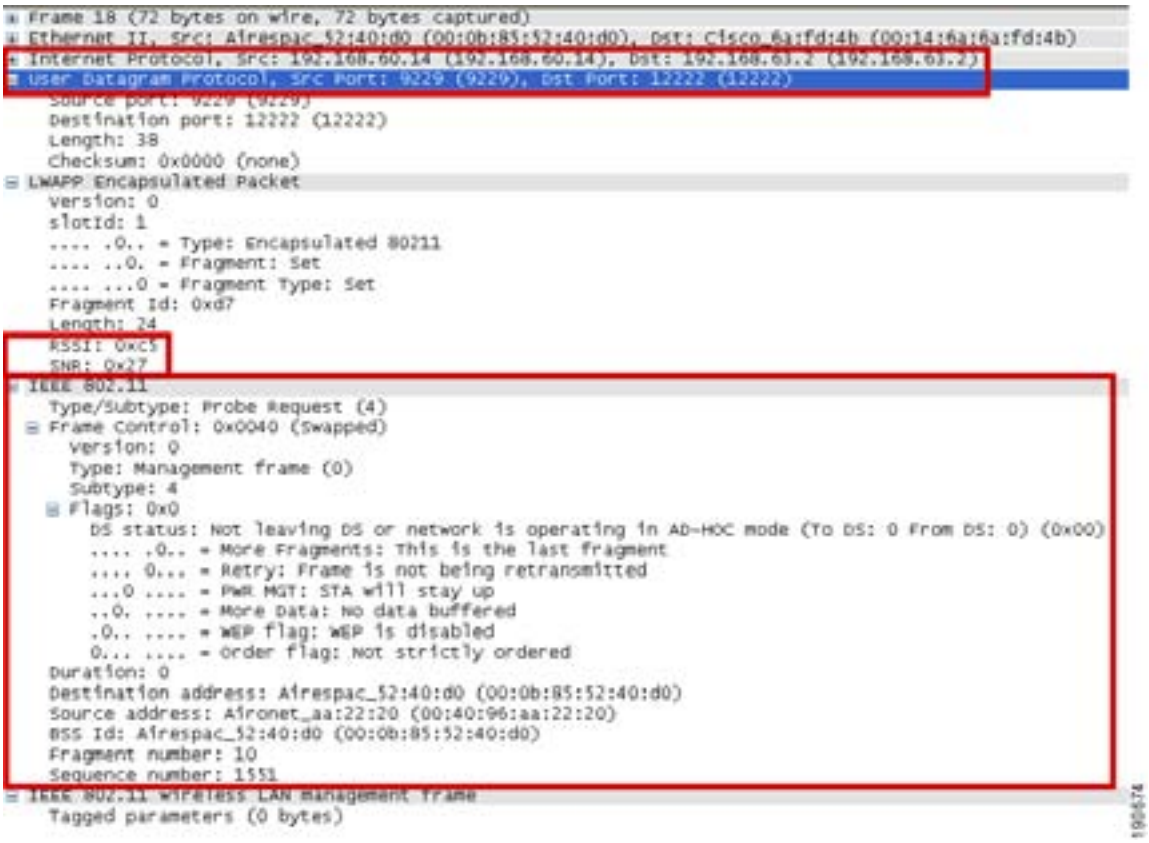
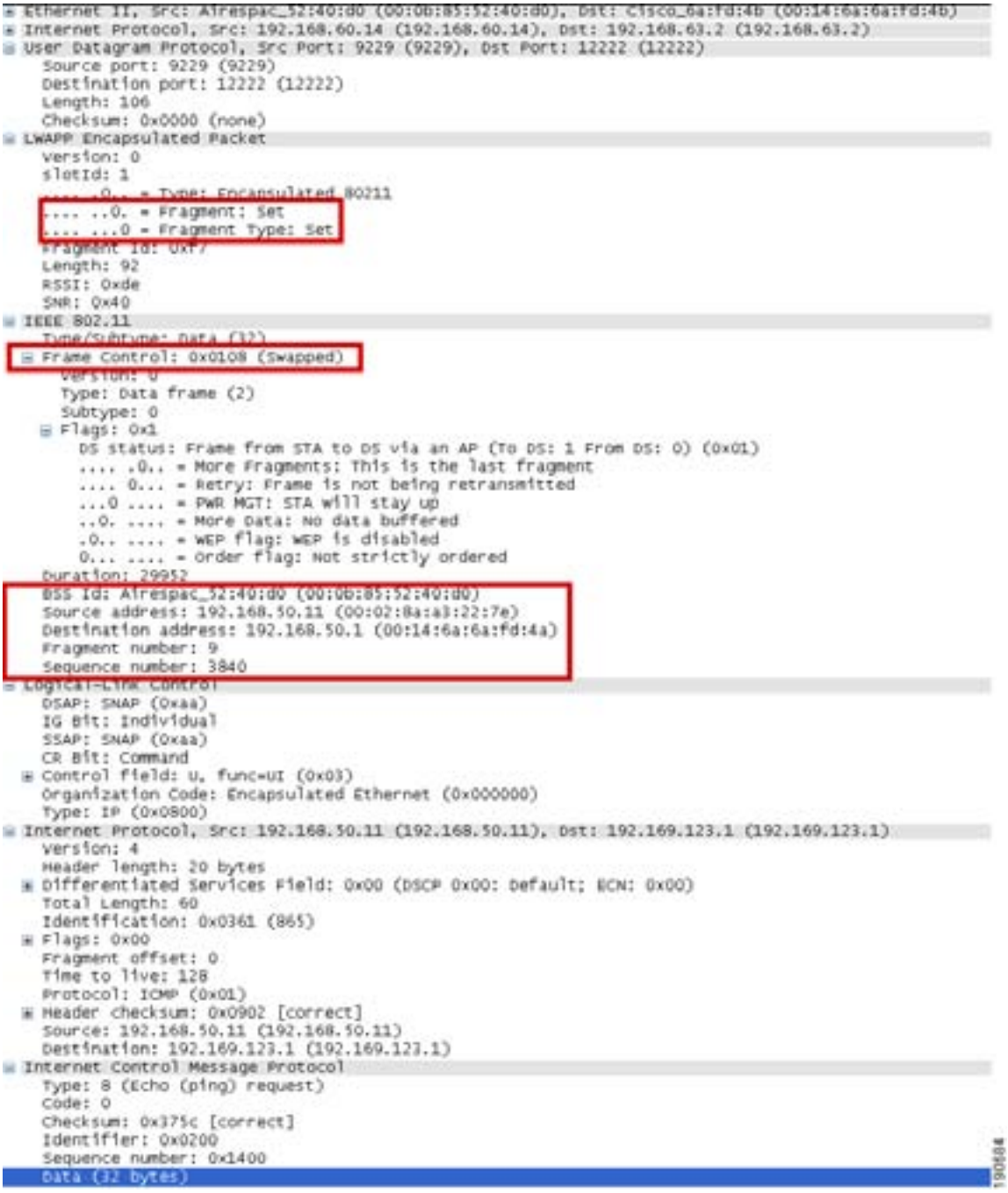


図 2-5 は、別の LWAPP で暗号化された 802.11 フレームを示していますが、この場合は、図 2-4 に示すような 802.11 データ フレームです。これには、完全な 802.11 フレームのほかに、WLC に対する RSSI と SNR の情報が含まれます。このキャプチャは、LWAPP で、802.11 のデータ フレームがその他の 802.11 のフレームと同様に扱われることを示しています。図 2-5 は、LWAPP AP と WLC の間の LWAPP パケットで、最小 MTU サイズに合わせたフラグメンテーションがサポートされていることを示しています。Wireshark デコードでは、フレーム コントロール デコード バイトがスワップされていることに注意してください。これは、一部の LWAPP AP がこれらのバイトをスワップすることを考慮して、LWAPP パケットの Wireshark プロトコルの解析中に実行されます。

図 2-5　LWAPP の 802.11 データ フレーム



WLC ディスカバリおよび選択

次の項では、リセット時のレイヤ 3 LWAPP AP の典型的な動作について説明します。検出 / 接続プロセスの詳細については、『*Deploying Cisco 440X Series Wireless LAN Controller*』（http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html）を参照してください。

リセットすると、次のような一連の処理が実行されます。

ステップ 1　AP がローカル IP サブネット上でレイヤ 3 LWAPP ディスカバリ メッセージをブロードキャストします。同一の IP サブネットに接続されている、レイヤ 3 LWAPP モード用に設定された WLC はすべて、ディスカバリ メッセージを受信します。その後、LWAPP ディスカバリ メッセージを受信した各 WLC は、AP に対してユニキャストされる LWAPP ディスカバリ応答メッセージで応答します。

ステップ 2　Over-the-Air Provisioning（OTAP）と呼ばれる機能が WLC で有効になっている場合、WLC にすでに接続している AP は、既知の WLC を、無線で他の AP に送信されるネイバー メッセージでアドバタイズします。初めて WLC の「検出」を試みている新しい AP は、これらのメッセージを受信し、OTAP メッセージでアドバタイズされた各 WLC に LWAPP ディスカバリ要求をユニキャストします（初期状態では、OTAP は IOS AP によりサポートされていません。つまり、IOS を使用する新しい AP は、OTAP を使用して WLC を検出できません）。LWAPP ディスカバリ要求メッセージを受信する WLC は、AP に LWAPP ディスカバリ応答をユニキャストします。

ステップ 3　AP は以前に学習した WLC IP アドレスをローカルの NVRAM に保持します。AP はこれらの WLC IP アドレスのそれぞれにユニキャスト LWAPP ディスカバリ要求を送信します。LWAPP ディスカバリ要求を受信する WLC は、AP に LWAPP ディスカバリ応答を送信することで応答します。前述のとおり、WLC の IP アドレスは、既に WLC に接続している既存の AP から送信される OTAP メッセージによって確認できます。NVRAM に保存される情報には、別のモビリティ グループのメンバとして以前に接続していた WLC のアドレス情報も含まれます（モビリティ グループの概念は、この文書の後半で詳しく説明します）。

ステップ 4　OTAP を使用しない場合は、ベンダー固有の DHCP オプションを使用して WLC の IP アドレスを返すように、DHCP サーバをプログラムできます。この場合、LWAPP AP に WLC のアドレスを「アドバタイズ」するために、「DHCP オファー」で「オプション 43」を使用します。AP は DHCP 経由で IP アドレスを受信する場合、DHCP「オファー」のオプション 43 フィールドで WLC の IP アドレスの情報を確認します。AP は、DHCP オプション 43 に含まれる各 WLC にユニキャスト LWAPP ディスカバリ メッセージを送信します。LWAPP ディスカバリ要求メッセージを受信する WLC は、AP に対して LWAPP ディスカバリ応答をユニキャストします。

ステップ 5　オプション 43 の情報の代わりに、AP は DNS 名 CISCO-LWAPP-CONTROLLER.localdomain を解決しようとします。この名前を解決できた場合、AP は、DNS 応答で返された個々の IP アドレスに対して、ユニキャスト LWAPP ディスカバリ メッセージを送信します。前述のとおり、LWAPP ディスカバリ要求メッセージを受信した各 WLC は、AP に対してユニキャスト LWAPP ディスカバリ応答で応答します。

ステップ 6　手順 1 ～ 5 の後、LWAPP ディスカバリ応答が受信されない場合、AP は検索アルゴリズムをリセットしてから、再開します。

通常、1 つまたは複数のシード WLC アドレスを提供するには、DHCP または DNS ディスカバリ メカニズムが使用されます。また、その後の WLC ディスカバリ応答では、WLC モビリティ グループの全メンバの一覧が提供されます。

LWAPP AP は通常、推奨 WLC を表す、最大 3 つまでの WLC の一覧を使用して設定されています。これらの WLC が使用できないか、オーバーサブスクライブされている場合、AP はディスカバリ応答で提供された WLC の一覧から最も負荷の少ない別の WLC を選択します。

コンポーネント

Cisco Unified Wireless のアーキテクチャを構成する主要コンポーネントは、Lightweight AP、WLC、および WCS の 3 つです。この項では、AP および WLC 製品のオプションについて説明します。

Cisco WCS はオプションのネットワーク コンポーネントで、Cisco Aironet Lightweight AP、Cisco 無線 LAN コントローラ、および Cisco Wireless Location Appliance と共に動作します。Cisco WCS を使用すると、ネットワーク管理者は、単一のソリューションを通じて、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、および無線 LAN システムの管理が可能になります。また、堅牢なグラフィック インターフェイスにより、無線 LAN を簡単かつコスト効率の優れた方法で展開し、運用できるようになります。詳細な傾向レポートや分析レポートの機能を備えた Cisco WCS は、ネットワークを継続的に運用するためには欠かせません。Cisco WCS の詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd802570d0.html

http://www.cisco.com/en/US/products/ps6305/products_installation_and_configuration_guides_list.html

WLC

Cisco Unified Wireless コントローラの機能はすべての Cisco WLC プラットフォームで同一で共通しているため、便宜上、このドキュメントでは、これらのコントローラをすべて WLC と呼びます。

各種 Cisco Unified Wireless WLC とその機能を簡単にまとめると、次のようになります。

- 2106：8 個のファスト イーサネット インターフェイスを持ち、最高 6 個の AP をサポートするスタンドアロン WLC。2 個のファスト イーサネット インターフェイスは、直接接続された AP への電力供給（802.3af 準拠）に使用できます。また、このインターフェイスを dot1q トランクとして設定し、有線ネットワークへの接続を提供することもできます。2106 は、ユーザ数、WAN 要件、クライアント ローミング要件などのために H-REAP が不向きな、小規模から中規模のオフィスに適しています。
- 4402：12 台、25 台、または 50 台の AP をサポートするスタンドアロンの WLC です。有線ネットワークへの接続を提供する dot1q トランクとして設定可能な SFP ベースのギガビット イーサネット ポートを 2 つ備えています。また、スイッチド ネットワークへの EtherChannel 接続を提供するために、ギガビット ポートをリンク集約することもできます。中規模のオフィスまたはビルディングに適しています。
- 4404：100 台の AP をサポートするスタンドアロンの WLC です。有線ネットワークへの接続を提供する dot1q トランクとして設定可能な SFP ベースのギガビット イーサネット ポートを 4 つ備えています。ギガビット　ポートをリンク集約して、スイッチド　ネットワークへの EtherChannel 接続を提供することもできます。大規模なオフィス、ビルディング、および小規模キャンパスに適しています。
- WLCM：WLC モジュールは、シスコの Integrated Service Router（ISR）シリーズ用に設計されたものです。現在は、6 台、8 台、または 12 台の AP をサポートしています。WLCM は、有線ネットワークへのルーテッド接続を提供する dot1q トランクとして設定可能な、ISR ルータ上のインターフェイスです。統合ソリューションを必要としている小規模から中規模のオフィスに適しています。

- WS-C3750G：Catalyst 3750 スイッチに統合されている WLC で、25 台または 50 台の AP をサポートしています。この WLC は、バックプレーン接続用に 2 つのギガビット イーサネット ポートを備えており、それぞれのポートを dot1q トランクとして設定して、3750 への接続を提供できます。また、3750 への単一の EtherChannel 接続を提供するために、ギガビット ポートをリンク集約することもできます。WLC は直接統合されているので、スタック可能な 3750 スイッチの高度なルーティング機能やスイッチング機能をすべて使用できます。中規模のオフィスまたはビルディングに適しています。仮想スイッチとして、50 台の AP をサポートする 4 台の 3750 をスタックした場合、最高 200 台の AP をサポートするように拡張できます。
- WiSM：シスコの Catalyst 6500 スイッチ シリーズ用に設計された WLC モジュール。1 モジュールあたり最大 300 台の AP をサポートします。6500 プラットフォームによっては、複数の WISM をインストールして、拡張性を大幅に向上できます。WiSM は、6500 バックプレーンへの接続を提供する dot1 トランクとして設定可能な、6500 上の単一の集約されたリンク インターフェイスです。大規模なビルディングまたはキャンパスに適しています。

表 2-1 は Cisco Unified Wireless コントローラをまとめたものです。

表 2-1　Cisco Unified Wireless コントローラの要約

製品	AP の数	インターフェイス	備考
2106	6	ファスト イーサネット 8 個	モビリティ アンカーにはできません。また、レイヤ 2 LWAPP はサポートしておらず、ファスト イーサネット インターフェイスのうち 2 つは 802.3af の PoE をサポートしています。
4402	12 または 25	ギガビット イーサネット 2 個	
4404	50 または 100	ギガビット イーサネット 4 個	
WLCM	6、8、または 12	ISR バックプレーン	モビリティ アンカーにはできず、レイヤ 2 LWAPP はサポートしていません。静的および動的 WLC インターフェイスだけのレイヤ 3 サブインターフェイス終端であり、dot1q トランクはサポートしていません。
WS-C3750G	25 または 50	3750 バックプレーン	統合 WLC により 3750 のスタック可能スイッチを完全装備
WiSM	300	6500 バックプレーン	モジュールは 6500 バックプレーンに直接接続

AP

Cisco Unified Wireless アーキテクチャでは、スタンドアロンと LWAPP の 2 種類の AP が使用されます。ここでは、各カテゴリで利用可能なさまざまな AP 製品モデルについて簡単に説明し、特性、機能、およびアプリケーションを比較します。Cisco 1500 シリーズ Mesh AP については、後で簡単に説明しますが、無線メッシュの活用方法や展開のガイドラインについては、この設計ガイドでは扱っていません。Cisco Mesh ソリューションの詳細については、以下のガイドを参照してください。

Cisco Mesh Networking Solution Deployment Guide：
http://www.cisco.com/en/US/partner/products/ps6548/products_technical_reference_book09186a008062b50e.html

Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide：
http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide/MeshAP.html

シスコのスタンドアロン AP

このカテゴリの AP は、従来の Aironet 製品ラインで構成されます。以下のモデルは、LWAPP 動作モードで入手するか、LWAPP モードにフィールド アップグレードできます。この機能を使用すると、企業では、混合無線トポロジに展開可能な共通の AP プラットフォーム上での標準化が可能になります。

第 1 世代のスタンドアロン AP は、次のとおりです。

- AP 1100：このシングル バンド 802.11b/g AP。一体型アンテナを持つ、エンタープライズ展開向けのエントリ レベル AP です。LWAPP AP の製品番号は AIR-LAP1121G-x-K9 です。x は地域コードになります。
- AP 1200：エンタープライズ展開をターゲットとした、単一帯域の 802.11b/g AP。1100 シリーズとは異なり、1200 は、外部アンテナへの接続をサポートしており、より柔軟性に優れています。802.11a 無線をサポートするようにフィールド アップグレードしたり、Lightweight（LWAPP）動作用にアップグレードしたりできます。LWAPP AP の製品番号は AIR-LAP1231G-x-K9 です。x は地域コードになります。
- AP 1230AG：両方の帯域にアンテナ用の外部コネクタを備えたデュアル バンド 802.11a/b/g AP。これは、1240AG のすべての機能（特に 802.3af PoE 規格）および RF パフォーマンスを備えているわけではありません。また、Lightweight（LWAPP）バージョンでも提供されますが、後から Lightweight 操作モードにアップグレードすることもできます。LWAPP AP の製品番号は AIR-LAP1232G-x-K9 です。x は地域コードになります。

第 2 世代のスタンドアロン AP は、次のとおりです。

- AP 1130AG：AG バージョンは一体型アンテナを備えたデュアル バンド（a/b/g）AP です。これは、壁面取り付け用に設計されており、一体型のデュアル バンド帯域アンテナを使用します。1130AG は、集中化された WLC ベースの展開での実装向けに Lightweight（LWAPP）バージョンで入手できます。スタンドアロン バージョンは、後から Lightweight 動作用にアップグレードできます。LWAPP AP の製品番号は AIR-LAP1131AG-x-K9 です。x は地域コードになります。
- AP 1240AG：小売や倉庫業務など、厳しい RF 環境での展開向けに設計されたデュアル バンド 802.11 a/b/g AP。1241AG は、両方の帯域にアンテナのための外部接続を備えています。これは、スタンドアロン カテゴリの中で最も多機能な AP です。Lightweight（LWAPP）バージョンでも入手可能です。柔軟性をより向上させるために、スタンドアロン バージョンを後から Lightweight 動作モードにアップグレードすることもできます。その他の目立った機能としては、LWAPP 操作モード用にインストール済みの証明書やハイブリッド REAP のサポート機能などがあります。LWAPP AP の製品番号は AIR-LAP1242AG-x-K9 です。x は地域コードになります。
- AP 1300：屋外展開用に設計された単一帯域 802.11b/g AP/ ブリッジ。一体型アンテナを備えています。また、外部アンテナアプリケーションをサポートするように、RP-TNC コネクタを付けたものを注文することもできます。LWAPP AP の製品番号は AIR-LAP1310G-x-K9 です。x は地域コードになります。

新しい第 3 世代の AP である Cisco 1252 は、新たに策定された 802.11n 規格のドラフト 2 をサポートする、ビジネス クラスの AP です。802.11n では、Multiple-Input Multiple-Output（MIMO）テクノロジーを使用して、最高 600 Mbps の合計データ レートが実現されます。Cisco 1252 は、デュアル バンド a/b/g、またはシングル バンド b/g 無線設定で使用可能であり、スタンドアロン AP（スタンドアロン）として、または統合（コントローラ）無線展開の一部として展開できます。Cisco 1252 には、展開の柔軟性を最大限に向上させるための、各種 2.4 GHz および 5 GHz 外部アンテナで使用可能な RP-TNC コネクタが備わっています。また、Cisco 1252 は、802.11n でのスループット レートをより高めるための、ギガビット 10/100/1000 インターフェイスを内蔵しています。Cisco 1252 は、高帯域幅を必要とする厳しい RF 環境への展開を前提に設計されています。スタンドアロン バージョンの製品番号は、AIR-AP1252AG-x-K9（デュアル バンド）および AIR-AP1252G-x-K9（シングル バンド）です。Cisco Unified Wireless バージョンの製品番号は、AIR-LAP1252AG-x-K9（デュアル バンド）および AIR-LAP1252G-x-K9（シングル バンド）です。

Cisco LWAPP AP

このカテゴリの AP は、従来の Airespace 製品ラインで構成されていますが、上記のスタンドアロン AP モデルも含まれています。次のモデルは、WLC トポロジだけで使用できます。

- AP 1010：エンタープライズ向けの基本的な LWAPP/WLC 展開用の、デュアル バンドでゼロタッチ設定の 802.11a/b/g AP。1010 には、内部デュアル セクター アンテナが付属しています。製品番号は AIR-AP1010-x-K9 です。x は地域コードになります。
- AP 1020：1010 と同様ですが、内部セクター アンテナに加え、2.4 および 5 GHz 外部アンテナ用の RP-TNC コネクタも含まれています。製品番号は AIR-AP1020-x-K9 で、x は地域コードを示します。
- AP 1030：REAP AP または リモート エッジ AP とも呼ばれます。1030 は 1020 と同じ能力、機能、パフォーマンスを有していますが、これに加え、小規模な支社のように WLC を展開するには実用的ではない環境に展開できます。製品番号は AIR-AP1030-x-K9 です。x は地域コードになります。
- AP 1500：屋外、ポイントツーポイント、マルチポイント MESH 展開用に特別に設計されたデュアル バンド AP。802.11a 帯域はバックホールに使用され、b/g 帯域は無線クライアント アクセスに使用されます。1500 は、MESH トポロジでの最適なルーティングのために（特許出願中の）Adaptive Wireless Path Protocol（AWPP）を使用します。

表 2-2 および表 2-3 はここで説明した AP の比較の要約です。

表 2-2　AP の比較（1）

Cisco シリーズ	802.11b/g	802.11a	802.11n	スタンドアロン	LWAPP	ブロードキャストされる SSID の数	インストール済みの証明書
1000	はい	はい	いいえ	いいえ	はい	16	はい
1100	はい	いいえ	いいえ	はい	はい	8[1]	いいえ
1130AG	はい	はい	いいえ	はい	はい	8[1]	はい[2]
1200	はい	オプション	いいえ	はい	はい	8[1]	はい[2]
1230AG	はい	はい	いいえ	はい	はい	8[1]	はい[2]
1240AG	はい	はい	いいえ	はい	はい	8[1]	はい[2]
1252AG	はい	はい	はい	はい	はい	8[1]	はい
1252G	はい	いいえ	はい	はい	はい	8[1]	はい
1300	はい	いいえ	いいえ	はい	はい	8[1]	いいえ
1500	はい	はい	いいえ	いいえ	はい	16	はい

1. 16 BSSID は、将来のリリースでサポートが予定されています。
2. 2005 年 8 月より前に出荷された装置では、シスコより提供されるユーティリティを使用して自己署名証明書をロードする必要があり、11g 無線が必要となります。

表 2-3　AP の比較（2）

Cisco シリーズ	オフィスおよび同様の環境	厳しい屋内環境	屋外
1010	推奨[1]	推奨しない	推奨しない
1020	推奨[1]	推奨[1]	推奨しない
1100	推奨	推奨しない	推奨しない
1130AG	理想	推奨しない	推奨しない
1200	推奨[2]	推奨	推奨[2]
1230AG	推奨	推奨	推奨[2]
1240AG	推奨[2]	理想	推奨[2]
1300	推奨しない	推奨しない	理想[3]
1500	推奨しない	推奨しない	理想[1]

1. またはリモート オフィスの場合は 1030LWAPP 展開のみ。
2. 耐候性 NEMA 定格の筐体で展開する場合は屋外で使用可能。特に、吊り天井の上での展開に適しています。
3. スタンドアロン展開のみ。

詳しくは、次のリンクを参照してください。
http://www.cisco.com/en/US/partner/products/ps6108/prod_brochure0900aecd8035a015.html

モビリティ グループ、AP グループ、および RF グループ

Cisco Unified Wireless アーキテクチャにおける重要な「グループ」の概念には、次の 3 種類があります。

- モビリティ グループ
- AP グループ
- RF グループ

この項では、Cisco Unified Wireless アーキテクチャにおけるこれらのグループの目的と用途について説明します。動作および設定の詳細は、次の URL を参照してください。

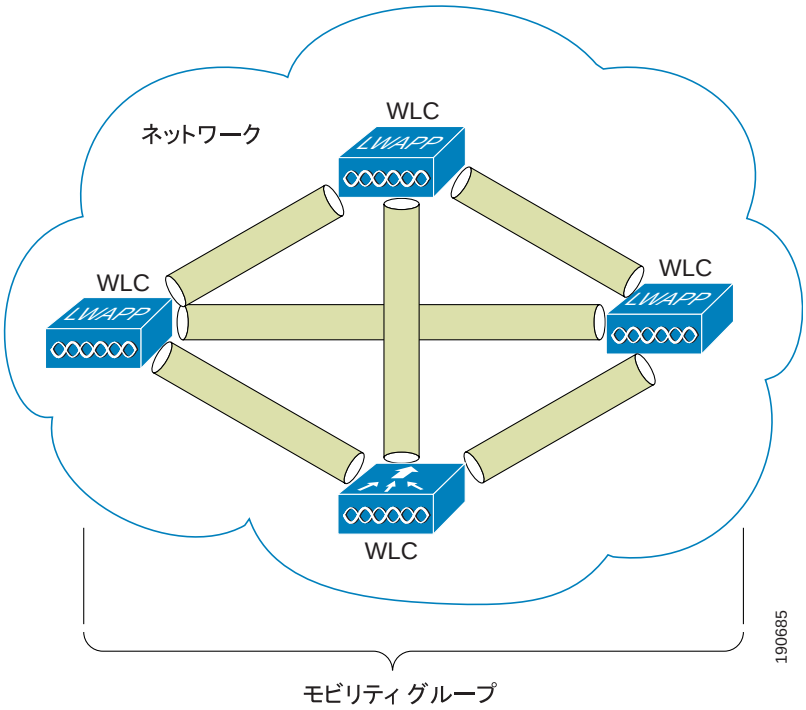
- Deploying Cisco 440X Series Wireless LAN Controller
  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
  http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html

モビリティ グループ

モビリティ グループとは、必須のエンド クライアント、AP、および RF 情報を共有することで 1 つの仮想 WLC として機能する WLC のグループのことです。モビリティ ドメイン内の WLC は、その WLC が直接接続されている AP やクライアントから得た情報だけではなく、モビリティ グループ全体の他のメンバから受け取ったデータにも基づいた判断を下すことができます。

モビリティ グループは、図 2-6 に示すように、メンバ WLC 間にメッシュ状の認証トンネルを形成し、WLC がグループ内のほかの WLC に直接問い合わせることができるようにします。

図 2-6　WLC モビリティ グループ



モビリティ グループの定義

モビリティ グループは簡単に作成できて、これについては詳しく文書化されていますが、以下の点に留意してください。

- モビリティ グループごとに、最大 24 の WLAN コントローラおよび 3600 の AP がサポートされています。企業で、複数の WLAN コントローラおよび AP が使用されていることがありますが、これらは別のモビリティ グループのメンバとして設定する必要があります。
- WLC は、同一のモデルやタイプでなくても、モビリティ グループのメンバにできます。たとえば、4402、4404、WiSM、WLCM、3750G を自由に組み合わせてグループを構成できますが、実行されているソフトウェアのバージョンは同じでなければなりません。ソフトウェアが違っているとモビリティ グループを構成できないわけではありませんが、統合無線展開全体で機能の同一性を保証するには、共通のソフトウェア バージョンの使用を強くお勧めします。
- モビリティ グループでは、グループ内のすべての WLC が同じ仮想 IP アドレスを使用する必要があります。
- 各 WLC には同一の「モビリティ ドメイン名」を使用します。また、WLC は、それぞれの [Static Mobility Members] リストでピアとして定義する必要があります。
- モビリティ グループ メンバ（WLC）の間で無線クライアントがシームレスにローミングできるようにするには、モビリティ グループを構成するすべての WLC で、WLAN の SSID とセキュリティ設定を同一に設定する必要があります。

モビリティ グループの用途

モビリティ グループは、別の WLC に接続している AP 間でのシームレスなクライアント ローミングを実現するために使用されます。モビリティ グループの主な目的は、無線カバレッジ領域の包括的なビューを提供するために、複数の WLC 間に仮想 WLAN ドメインを作成することです。モビリティ グループの使用は、異なる WLC に接続された複数の AP が、カバレッジが重複するように展開されている場合にだけ効果的です。たとえば、キャンパスや支社、キャンパス内の複数のビル間など、それぞれ異なるコントローラにアソシエートされている 2 つの AP が、物理的にまったく別の場所にあり、これらのカバレッジが重複（接触）していない場合には、モビリティ グループは有効ではありません。

モビリティ グループの例外

Cisco Unified Wireless ソリューションにより、ネットワーク管理者は、ネットワーク内の「アンカー」WLC とその他の WLC の間の静的なモビリティ トンネル（自動アンカー）を定義できるようになります。このオプションは、特に、無線ゲスト アクセス サービスの展開時に使用します。

自動アンカー機能を使用した場合、指定されたアンカー WLC にマップできる（外部）WLC の数は、24 個未満です。外部 WLC は自動アンカーに接続されているため、外部 WLC どうしがモビリティ関係を確立することはありません。アンカー WLC では、静的モビリティ トンネルを必要とする外部 WLC ごとに「静的モビリティ グループ メンバ」エントリを定義する必要があります。同様に、静的モビリティ トンネルが設定されている外部 WLC のそれぞれについて、アンカー WLC を外部 WLC の「静的モビリティ グループ メンバ」として定義する必要があります。

動的なコントローラ間クライアント ローミングのサポートを目的とした場合、WLC は 1 つのモビリティ グループのメンバにしかなれません。「自動アンカー」として設定されている WLC は、外部 WLC と同じモビリティ グループに属する必要はありません。WLC は、あるモビリティ グループのメンバであると同時に、別のモビリティ グループのメンバである外部 WLC を起点とする WLAN の自動アンカーとして機能するようにできます。

モビリティ アンカーの設定の詳細は、第 10 章「Cisco Unified Wireless Guest Access Service」を参照してください。

AP グループ

典型的な展開シナリオでは、各 WLAN は WLC ごとに単一の動的なインターフェイスにマップされます。しかし、ここで、最大 100 台までの AP をサポートする 4404-100 WLC が使用される展開シナリオを考えてみてください。各 AP に 25 ユーザがアソシエートされているとします。その結果、2,500 人のユーザが 1 つの VLAN を共有することになります。お客様の設計によっては、サブネットのサイズを非常に小さくすることが要求される場合もあります。このような要求に対処するには、WLAN を複数のセグメントに分割するのも 1 つの方法です。WLC の AP グループ機能により、コントローラ上の複数の動的インターフェイス（VLAN）で 1 つの WLAN をサポートできるようになります。そのためには、AP のグループを特定の動的インターフェイスにマップします。AP は、従業員のワークグループごとに論理的にグループ化するか、ロケーションごとに物理的にグループ化できます。図 2-7 は、サイト固有の VLAN に基づく AP グループの使用を示しています。

（注） AP グループでは、グループの境界を越えたマルチキャスト ローミングは許可されていません。これについては、このデザイン ガイドの後半で詳しく説明します。

図 2-7　AP グループとサイト固有の VLAN

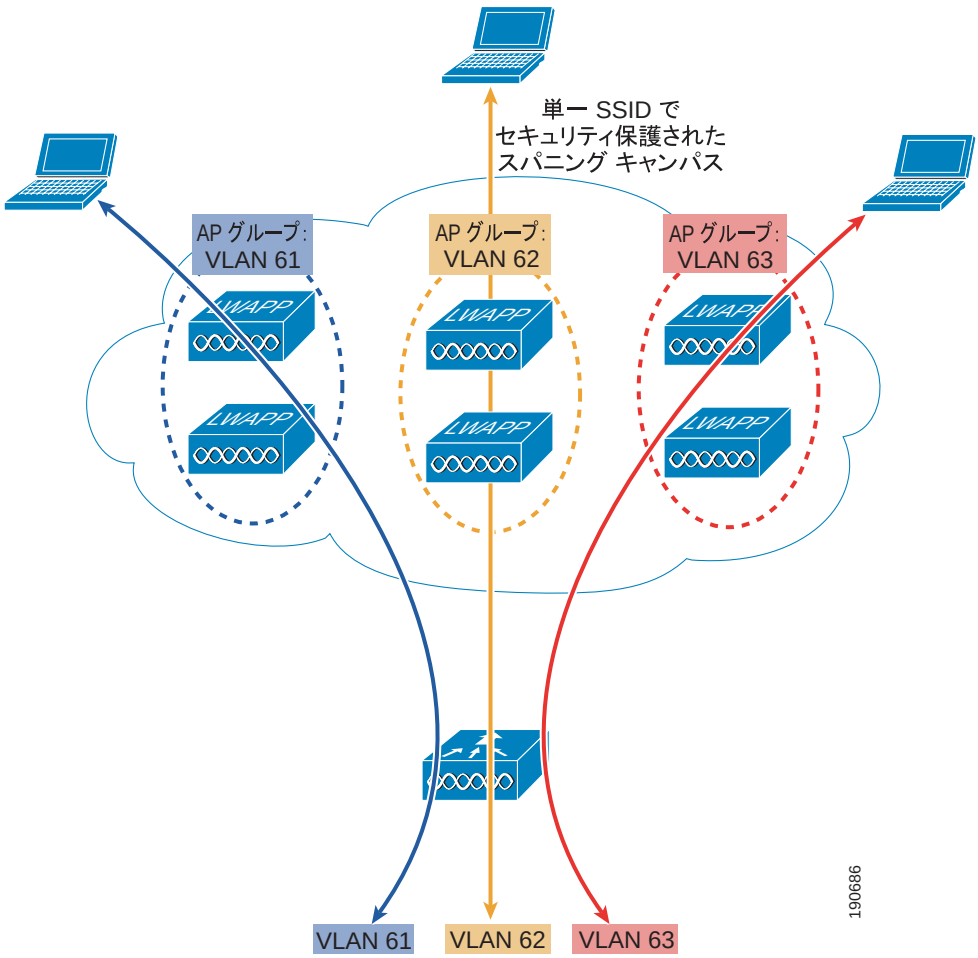


図 2-7 では、3 つの動的インターフェイスが設定され、それぞれがサイト固有の VLAN（61、62、および 63）にマッピングされています。サイト固有の VLAN およびアソシエートされた AP は、それぞれ AP グループ機能を使用して同一の WLAN SSID にマッピングされます。VLAN 61 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 61 IP サブネットで IP アドレスを取得します。同様に、VLAN 62 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 62 サブネットで IP アドレスを取得します。サイト固有 VLAN 間のローミングは、レイヤ 3 ローミング イベントとして WLC により内部的に処理されます。したがって、無線 LAN クライアントでは元の IP アドレスが維持されます。

RF グループ

RF グループ（RF ドメインとも呼ばれる）も、展開に考慮しなければならない重要な事項の 1 つです。RF グループとは、802.11b/g や 802.11a などの 802.11 PHY のタイプに基づいて、動的な Radio Resource Management（RRM）の設定を一括して調整および計算する WLC のクラスタです。

802.11 PHY タイプごとに RF グループが存在します。WLC を RF ドメインにグループ化すると、ソリューションの動的な RRM アルゴリズムが複数の WLC で使用され、特定の RF ドメインの RRM がフロア、ビルディング、さらにキャンパス間で使用されるようになります。RF グループおよび RRM については、このドキュメントの後半でさらに詳しく説明しますが、概要をまとめると次のようになります。

- LWAPP AP は、定期的にネイバー メッセージを無線で送信します。これには、WLC の IP アドレスと、AP のタイムスタンプおよび BSSID からハッシュされた Message Integrity Check（MIC）が含まれています。
- ハッシュ アルゴリズムでは、共有秘密（RF グループ名）が使用されます。共有秘密は、WLC で設定され、各 AP にプッシュされます。同じ秘密を共有する AP は、MIC を使用して、互いに送信されたメッセージを検証できます。異なる WLC に属する AP が、検証されたネイバー メッセージを -80 dBm 以上の信号強度で受信すると、その WLC は動的に RF グループのメンバになります。
- RF グループのメンバによって、RF グループの「マスター」電力およびチャネル スキームを管理する RF ドメイン リーダーが選ばれます。
- RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析し、マスター電力とチャネル計画が割り出されます。
- RRM アルゴリズム：
  - すべての AP 間の信号強度を -65 dBm に均一化（最適化）しようとします。
  - 802.11 相互チャネルの干渉およびコンテンションを回避しようとします。
  - 802.11 以外の干渉を回避しようとします。
- RRM アルゴリズムでは、ダンプニング計算を使用してシステム全体の動的な変更を最小限に抑えます。最終的には、絶えず変動する RF 環境に対応する、最適に近い電力とチャネル計画が動的に割り出されます。
- RF グループ リーダーおよびメンバは、指定された更新間隔（デフォルトでは 600 秒）で RRM メッセージを交換します。更新間隔の合い間に、RF グループ リーダーは RF グループの各メンバにキープ アライブ メッセージを送信し、リアルタイムの RF データを収集します。1 つの RF グループあたりの最大コントローラ数は 20 です。

ローミング

企業の 802.11 ネットワークのローミングは、802.11 クライアントがその AP アソシエーションを ESS 内のある AP から同じ ESS 内の別の AP に変更することを表します。ネットワークの機能および設定によっては、クライアント、WLC、およびネットワークのアップストリーム ホップでイベントがいくつか発生する可能性がありますが、基本的には、ローミングは単に AP アソシエーションの変更にすぎません。

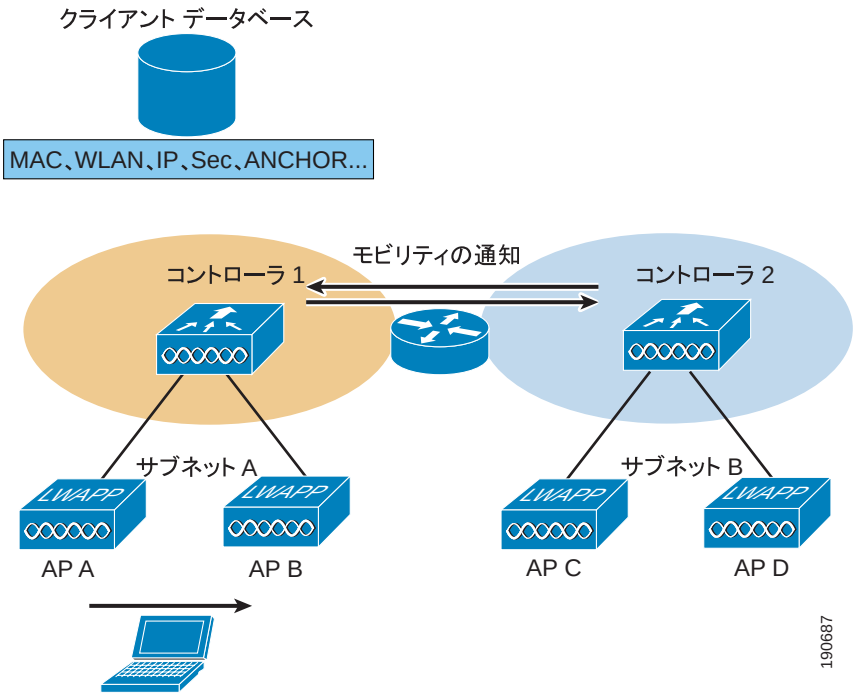
無線クライアントが AP の認証を受けて AP にアソシエートするときには、対応する WLC（AP の接続先）により、クライアント データベースにそのクライアントのためのエントリが作成されます。このエントリには、クライアントの MAC および IP アドレス、セキュリティ コンテキストおよびアソシエーション、QoS コンテキスト、WLAN、およびアソシエートされた AP が含まれます。WLC はこの情報を使用して、フレームを転送し、無線クライアント間で送受信されるトラフィックを管理します。

無線クライアントがそのアソシエーションをある AP から別の AP に移動するときには、WLC はクライアント データベースの新しい AP に関する情報をアップデートするだけです。必要に応じて、新しいセキュリティ コンテキストおよびアソシエーションも確立されます。

レイヤ 2 のローミングは、同じクライアント サブネットで、クライアントがある AP を離れて別の AP に再アソシエートするときに発生します。ほとんどの場合、ローミング先の AP は元の AP と同じ WLC に接続されています。

上の説明は、1 つの WLC データベースがクライアントに関するすべての情報を保持している最も単純なローミング シナリオを例にしたものです。WLC よりアップストリームにあるネットワーク要素は、図 2-8 に示すように、ある AP から別の AP にクライアントが移動しても影響を受けません。

図 2-8　レイヤ 2 でのローミング



WLAN を同一のサブネットに接続している WLC が複数存在しているときに、クライアントが異なる WLC に接続されている AP の間をローミングする場合は、WLC の間でモビリティ通知が交換されます。このモビリティ通知により、WLC の間でクライアントのコンテキスト情報が渡されます。

クライアント サブネット間での WLC から WLC へのローミング

異なる WLC に接続されている AP 間でクライアントがローミングするときに、これらの WLC でクライアント サブネットや VLAN が同一ではないと、レイヤ 3 ローミングが実行されます。ローミング先（外部（foreign））のモビリティ データベースとホーム（アンカー）WLC のモビリティ データベースの間で、モビリティ通知が交換されます。

レイヤ 3 ローミングは、無線クライアントが 1 つの VLAN またはサブネットから別の VLAN またはサブネットに移動する、より複雑なローミング方法です。WLAN システムにより、クライアント サブネットを透過的に変更するための措置が講じられない限り、レイヤ 3 ローミング イベントは、アップストリーム サービスを使用するクライアント通信に悪影響を与えます。既存のクライアント セッションは、ハングするか、最終的にタイムアウトして切断されます。Cisco Unified Wireless ソリューションでは、モビリティ トンネルを使用し、アップストリーム ネットワークに対して透過的にレイヤ 3 ローミングが実行されます。モビリティ トンネルには、次の 2 種類があります。

- アシンメトリック モビリティ トンネル（WLC リリース 4.0 以前のデフォルト）
- シンメトリック モビリティ トンネル（WLC リリース 4.1 以降の新規オプション）

（注） WLC リリース 4.1 では、デフォルトでアシンメトリック トンネリングが使用されます。シンメトリック トンネルを使用する場合は、管理者が明示的に設定する必要があります。

レイヤ 3 ローミング：アシンメトリック モビリティ トンネル

レイヤ 3 ローミング シナリオでは、無線クライアントに戻るトラフィックは、アンカー WLC を通過します。アンカー WLC は、Ethernet-over-IP（EoIP）トンネルを確立して、クライアント トラフィックを外部 WLC へ転送します。その後、クライアント トラフィックは、外部 WLC からクライアントへ配信されます。クライアントからのトラフィックはすべて、外部 WLC での WLAN のマップ先である、対応する VLAN インターフェイスに転送されます。クライアントの元の IP アドレスとデフォルト ゲートウェイ IP（MAC）アドレスは変更されません。ローカル サブネット宛のトラフィックを除き、すべてのトラフィックはデフォルト ルータに転送されます。ここで、外部 WLC により、クライアントのデフォルト ゲートウェイ MAC アドレスが、外部コントローラで動的インターフェイスまたは VLAN とアソシエートされているデフォルト ゲートウェイの MAC アドレスに置き換えられます。

図 2-9 は、アシンメトリック モビリティ トンネルを使用したクライアント レイヤ 3 ローミングを示しています。

図 2-9　レイヤ 3 でのローミング

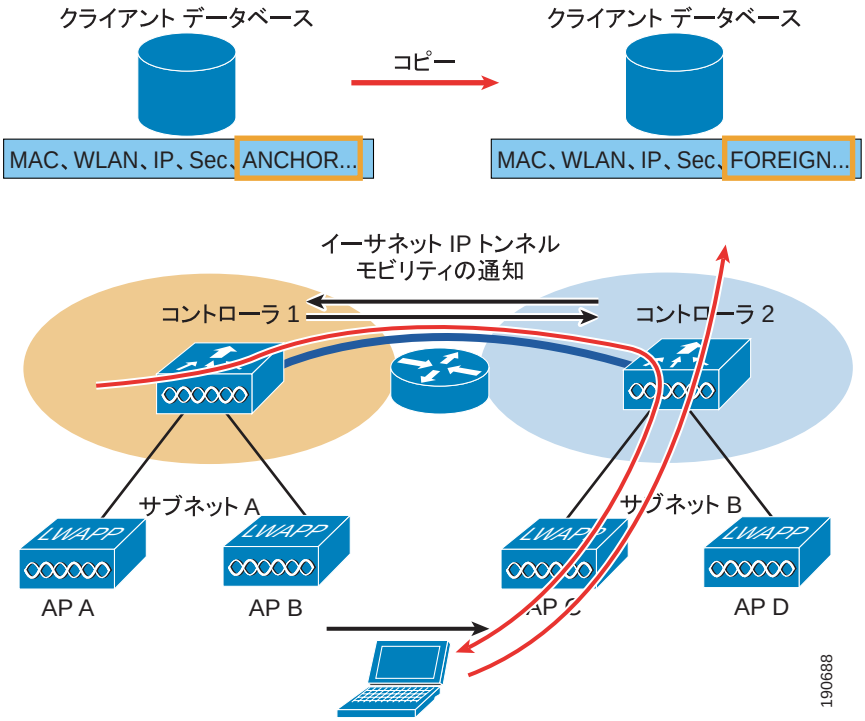


図 2-9 では、レイヤ 3 境界を越えたクライアントのローミング時に以下が実行されます。

1. クライアントは、WLC 1 上の AP B への接続を開始します。
2. これにより、WLC 1 のクライアント データベースに ANCHOR エントリが作成されます。
3. クライアントが AP B から移動し、AP C とのアソシエーションを開始すると、WLC 2 は、クライアント MAC アドレスに関する情報を持つ WLC を求めて、モビリティ グループのピアに モビリティ通知を送信します。
4. WLC 1 は通知、ハンドシェイク、および ACK に応答します。
5. ローミング クライアントのクライアント データベース エントリが WLC 2 にコピーされ、FOREIGN としてマークされます。PMK データ（RADIUS サーバからのマスター キー データ）も WLC 2 にコピーされます。これにより、RADIUS サーバから完全な再認証を受ける必要がなくなるため、WPA2/802.11i クライアントのローミング時間が短縮されます。
6. クライアントと AP 間で簡単なキー交換が実行され、クライアントは WLC 2 のデータベースに追加されます。このデータベースは、クライアント エントリが FOREIGN とマークされている点を除けば、アンカー コントローラのエントリとほとんど同じです。
7. WLAN クライアントに送信されるデータは、アンカー WLC から外部（foreign）WLC へ EoIP でトンネルされます。
8. WLAN クライアントにより送信されるデータは、外部コントローラのローカル インターフェイス VLAN から送出されます。

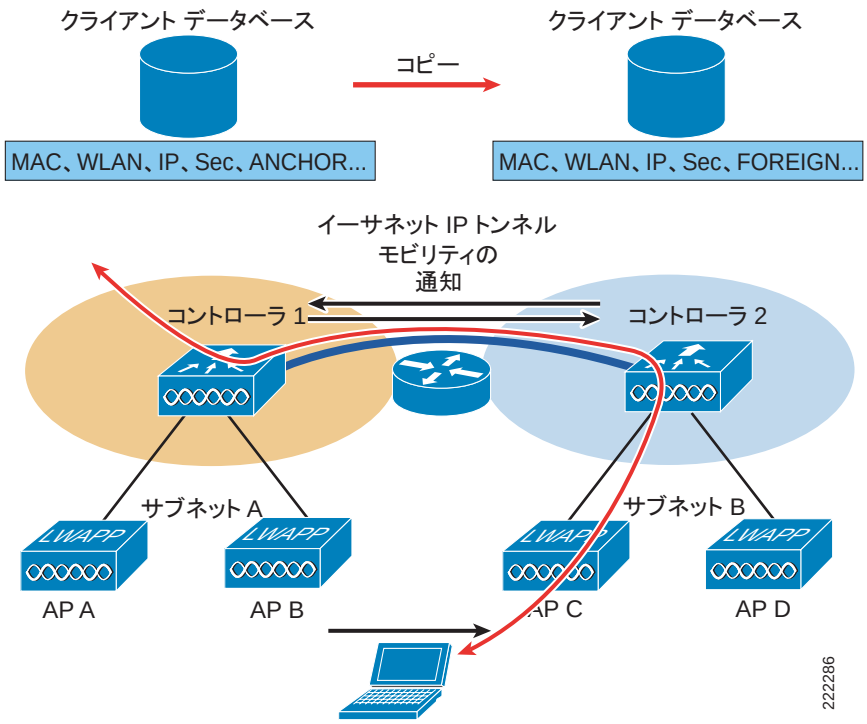
前述の「アシンメトリック」レイヤ 3 ローミング手順では、レイヤ 3 境界を越えた透過的なローミングの問題は解決されますが、アシンメトリック フローは、アップストリーム ネットワークで別の問題が発生する原因になります。特に、無線クライアント トラフィックが、ファイアウォール、NAC、IPS/IDS アプライアンスなどの近接するアプライアンスやモジュールを通じて双方向にフローすると予想される場合には、問題が発生することがあります。また、たとえば、次ホップの

ルーテッド インターフェイスで uRPF チェックが有効になっている場合、クライアントが別のサブネットにローミングした後でトラフィックがドロップされます。これが、Cisco Unified Wireless ソリューションにシンメトリック モビリティ トンネル機能が導入された理由です。

レイヤ 3 ローミング：シンメトリック モビリティ トンネル

WLC リリース 4.1 以降、図 2-10 に示すとおり、外部 AP/WLC とアンカー WLC の間の動的な双方向トンネリングをサポートするように WLC を設定できるようになりました。

図 2-10　レイヤ 3 ローミング：シンメトリック モビリティ トンネル



WLC のレイヤ 3 モビリティ ハンドオフ手順はそのままであり、変更されていません。ただし、WLC リリース 4.1 では、クライアントがレイヤ 3 ローミングを実行するときに、ソリューションの自動アンカー トンネリング メカニズムに関連する既存の機能を使用して、動的なシンメトリック トンネルが作成されます。

デフォルトでは、シンメトリック トンネリングは有効になっていません。コントローラの Web 設定インターフェイス、WCS テンプレート、またはコントローラの CLI を使用して、明示的に設定する必要があります。シンメトリック モビリティ トンネル動作は、特定のモビリティ グループのメンバであるコントローラ全てに対し有効にしてください。そうしないと、予期しない動作が発生する可能性があります。

図 2-11 と図 2-12 は、双方向モビリティ トンネルの Wireshark プロトコル トレースを示しています。

図 2-11　双方向モビリティ トンネル（1）

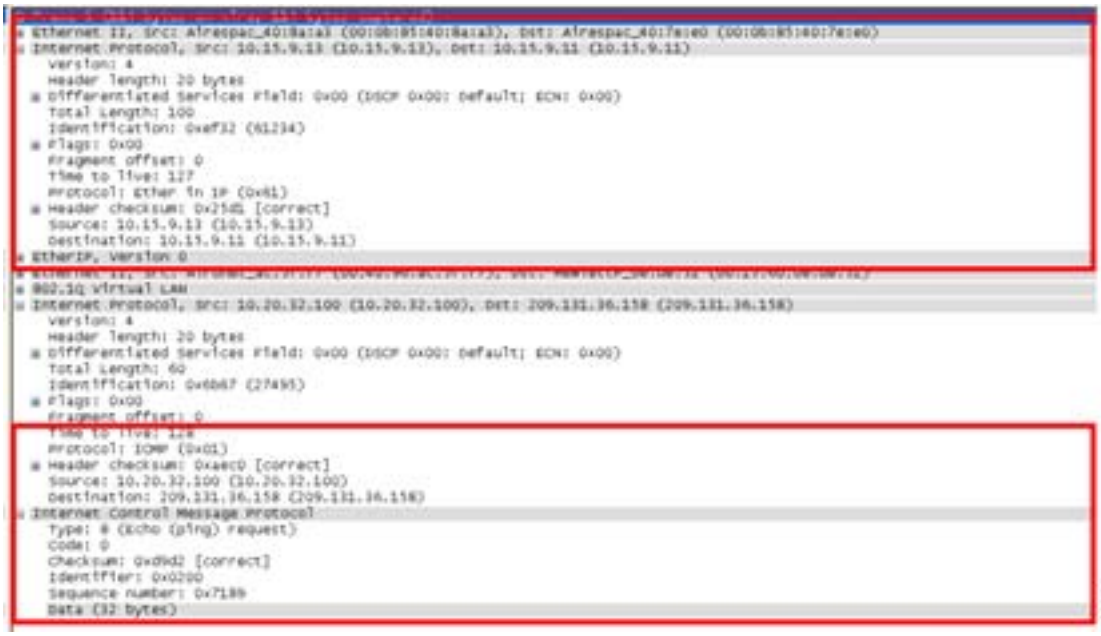
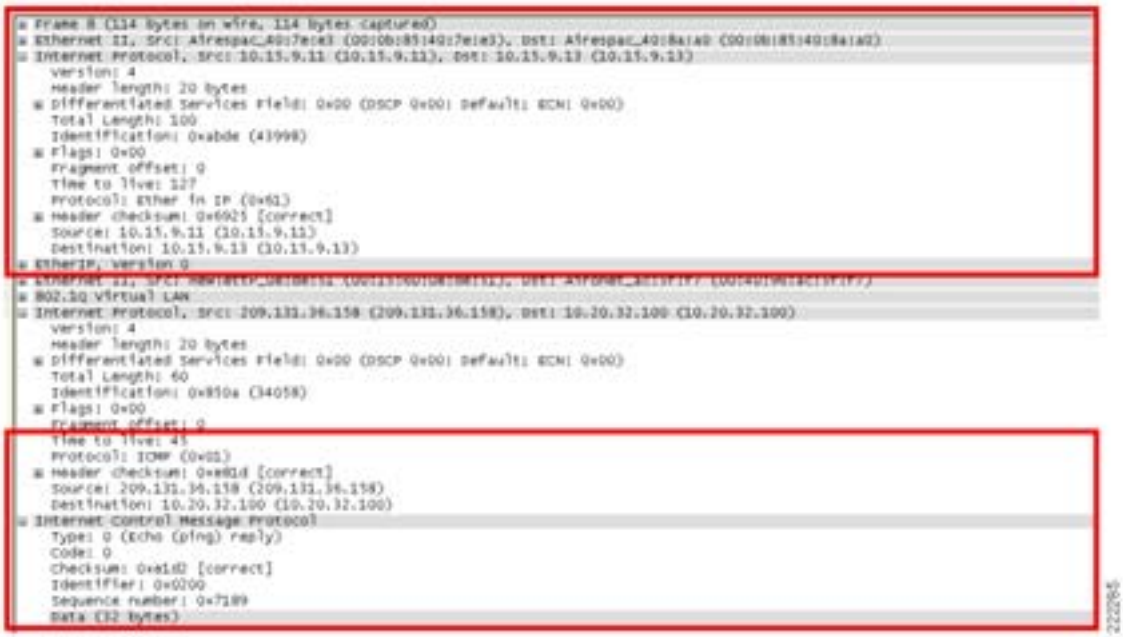


図 2-12　双方向モビリティ トンネル（2）



前述のプロトコル トレースでは、シンメトリック モビリティ トンネル（EtherIP）は、10.15.9.11（アンカー）と 10.15.9.13（外部）の 2 つの WLC 間に確立されています。図 2-11 では、コントローラ 10.15.9.13 上の AP にローミングしたクライアント 10.20.32.100 が、インターネット サイト 208.131.36.158（yahoo.com）に ICMP ping 要求を送信しています。外部コントローラがクライアントのパケットをアンカー コントローラへトンネルしている点に注意してください。コントローラがアシンメトリック モビリティ トンネリング用に設定されていた場合、このパケットは、外部コントローラにより、WLAN にアソシエートされている VLAN インターフェイスにローカルで転送されるため、トレースには表示されません。図 2-12 では、ping 応答は、アンカー コントローラにより受信され、同じモビリティ トンネルを経由して、外部コントローラに転送されています。これは、シンメトリック トンネルと同じです。

レイヤ 3 ローミングに関する重要な情報

レイヤ 3 ローミングは非常に便利な機能ですが、4.1 ソフトウェア リリースで展開する場合は、次の点に注意する必要があります。

- 現時点では、マルチキャストのグループ メンバーシップはクライアント ローミング中に転送されません。つまり、クライアントがマルチキャスト ストリームを受信し、マルチキャスト ストリームが壊れる外部 WLC に移動した場合は、再確立する必要があります。
- Unified Wireless ソリューションでは、モビリティ アンカーと EoIP トンネルの概念に基づいたレイヤ 3 ローミングが使用されています。「アンカー WLC」は、クライアントが初めて WLAN にアソシエートしたときに使用された WLC です。その後、クライアントには、アンカー コントローラで WLAN に割り当てられたインターフェイスまたはサブネットに対応するアドレスが DHCP 経由で割り当てられます。現在、Unified Wireless ソリューションでは、ある WLAN に対して定義されたサブネット以外の静的 IP アドレスを持つクライアントが、その WLAN に接続することは許可されていません。静的クライアント アクセスが必要な展開シナリオで使用可能なソリューションとしては、モバイル IP の使用を検討してください。モバイル IP、およびモバイル IP の Cisco Unified Wireless アーキテクチャの互換性の詳細は、第 12 章「Cisco Unified Wireless とモバイル IP」を参照してください。

WLC でのブロードキャストおよびマルチキャスト

ここでは、WLC によるブロードキャストおよびマルチキャスト トラフィックの処理および WLC が設計に与える影響について説明します。

図 2-13 は、基本的な 802.11 のブロードキャスト動作またはマルチキャスト動作を図示したものです。この例のクライアント 1 が 802.11 のブロードキャスト フレームを送信すると、そのフレームは AP にユニキャストされます。その後、AP は、そのフレームを、無線インターフェイスと有線インターフェイスの両方にブロードキャストとして送信します。

図 2-13　802.11 ブロードキャスト / マルチキャスト

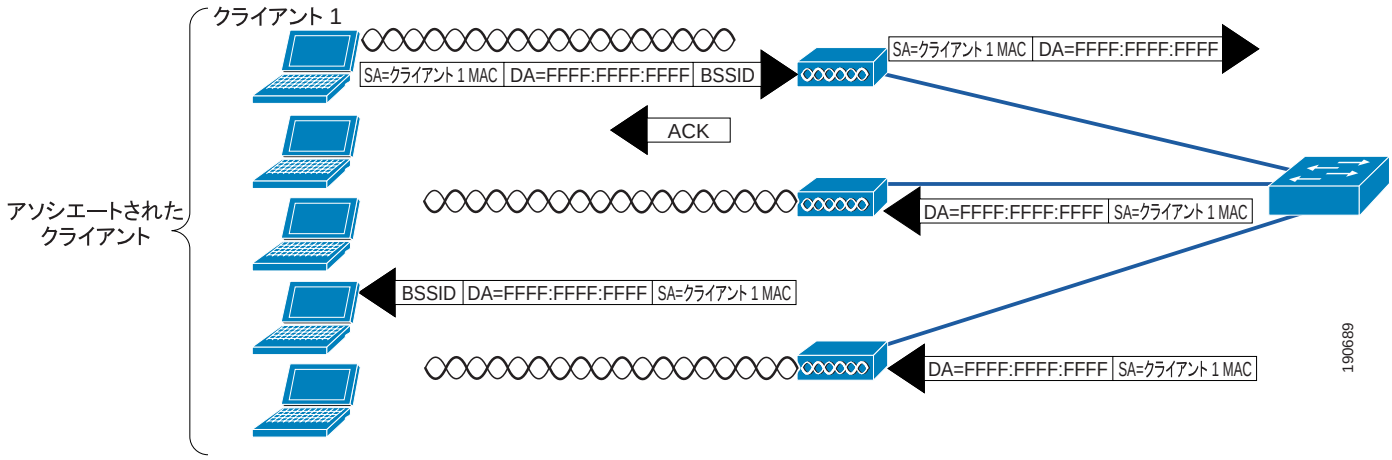
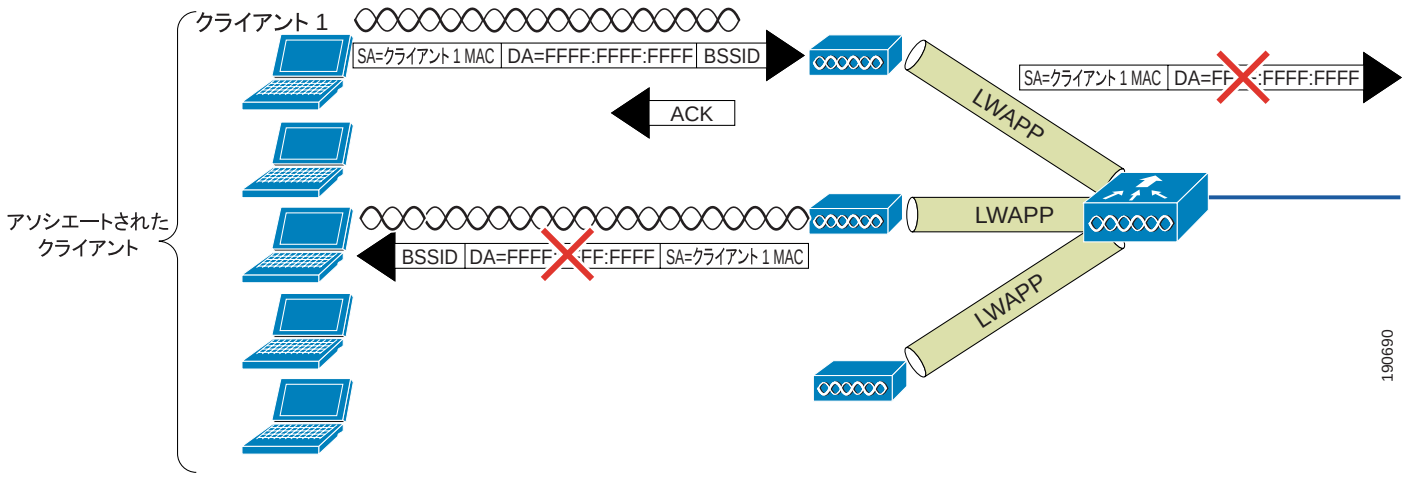


図 2-13 に示されているように、AP と同じ有線 VLAN 上に別の AP がある場合、それらの AP は、有線ブロードキャスト パケットを無線インターフェイスに転送します。

WLC の LWAPP スプリット MAC 方式では、図 2-17 に示すように、別の方法でブロードキャスト トラフィックを処理します。この場合、クライアントからブロードキャスト パケットが送信されると、AP またはコントローラは、そのパケットを WLAN に転送せず、ブロードキャスト メッセージと考えられるすべてのメッセージのサブセットのみを、WLC で指定された WLAN の有線インターフェイスに転送します。

(注)　どのような状況でどのようなプロトコルが転送されるかについては、次の項で説明します。

図 2-14　WLC ブロードキャストのデフォルトの動作



WLC ブロードキャストおよびマルチキャストの詳細

ブロードキャストおよびマルチキャスト トラフィックは、通常、WLAN ネットワーク内で特別に処理する必要があります。このトラフィックは最小限の共通ビットレートで送信しなければならないので、WLAN に余計な負荷がかかるからです。そして、それらのトラフィックを特別に処理することによって、アソシエートされているすべての無線デバイスで、ブロードキャストまたはマルチキャスト情報を確実に受信できるようになります。

WLC のデフォルトの動作では、ブロードキャストおよびマルチキャスト トラフィックは、WLAN からその他の無線クライアント デバイスに送信されないようにブロックされます。WLC は、クライアントの動作に影響を与えずにこの処理を実行できます。これは、ほとんどの IP クライアントは、ネットワーク情報を（DHCP から）取得して IP アドレスを MAC アドレスに解決（ARP）する以外の理由では、ブロードキャストまたはマルチキャスト タイプのトラフィックを送信しないからです。

DHCP

WLC は、アソシエートされている WLAN クライアントの DHCP リレー エージェントとして機能します。L3 クライアント ローミング中を除き、この WLC は、クライアント DHCP 要求を、ローカルに設定された DHCP サーバ、またはアップストリーム DHCP にユニキャストします（詳細については後述します）。DHCP サーバの定義は動的インターフェイスごとに設定されます。その後、このインターフェイスは、1 つまたは複数の WLAN にアソシエートされます。DHCP リレー要求は、動的インターフェイスのソース IP アドレスを使用して、このインターフェイス経由で転送されます。WLC は、特定のインターフェイスまたは WLAN に対してどの DHCP サーバを使用するかがわかっているため、有線または無線インターフェイスにクライアント DHCP 要求をブロードキャストする必要はありません。

前述の手順では、次のことが実現されます。

- DHCP 要求を WLC の外にブロードキャストする必要がなくなります。
- WLC は DHCP プロセスの一部となり、その結果、接続されている WLAN クライアントの MAC アドレスや IP アドレスの関係がわかるようになります。その後、WLC は DHCP ポリシーを施行し、IP スプーフィングや DoS 攻撃（サービス拒絶攻撃）を軽減できるようになります。

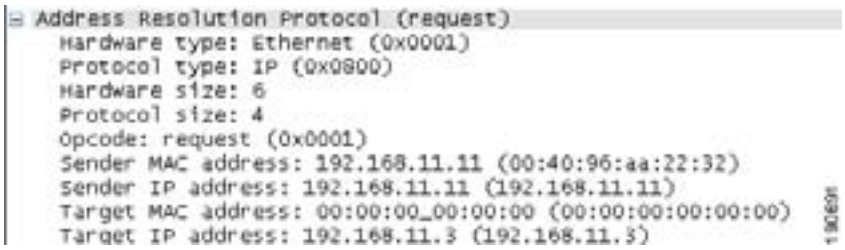
- WLC は、DHCP サーバの実際の IP アドレスではなく、仮想 IP アドレスを使用して、DHCP 応答メッセージをリレーできるようになります。前述の動作は WLC の CLI により設定されるもので、デフォルトで有効になっています。この仮想アドレスは、モビリティ グループを構成するすべての WLC により共有されます。DHCP プロキシの利点は、L3 クライアント ローミング中、または AP グループ境界を越えたクライアント ローミングで活かされます。このような場合、WLC はクライアントの DHCP 更新要求を受け取り、そのときに、クライアントがモビリティ グループ内でローミングしていることを確認して、クライアントが外部 WLC の新しいサブネットにローミングしたとしても既存の IP アドレスやサブネットの割り当てを更新（維持）できるようにします。ローミング（P. 2-18）を参照してください。

（注） アシンメトリック　モビリティ　トンネル方式が設定されている場合（デフォルト）、前述の仮想 IP/Proxy DHCP の動作は必須です。詳細は、前述の「ローミング」の項を参照してください。シンメトリック トンネル方式が使用されている場合には、WLC ベースの DHCP プロキシは必要ありません。これはクライアント トラフィックと DHCP 要求が常にアンカー コントローラにトンネルして戻されるからです。

ARP

WLAN クライアントは、他の IP クライアントに IP パケットを送信する前に、フレームの転送先となるターゲット クライアントの MAC アドレスを知っておく必要があります。このために、クライアントは通信先となる IP ホストの MAC アドレスを要求する ARP クエリをブロードキャストします（図 2-15 を参照）。

図 2-15　ARP フレーム



無線クライアントの ARP 要求を認識した WLC は、もう 1 つの無線クライアントのための ARP プロキシとして直接応答するか、または別の WLC に解決してもらうために有線インターフェイスに要求を転送します。この WLC が ARP ブロードキャストを WLAN に転送することはありません。

WLC のデフォルトの動作では、WLC のローカル ARP キャッシュに基づいて直接 ARP クエリーに応答します。この動作をオーバーライドするには、WLC CLI コマンド **: network arpunicast enable** を使用します。この場合、WLC はターゲットのために応答するのではなく、ターゲット ホストに直接 ARP 要求をユニキャストします。このターゲットは、要求元ホストに対して ARP 応答をユニキャストします。このコマンドの目的は、WLAN ネットワークから移動した可能性のある WLAN クライアントへ IP クライアントが過剰に再試行するのを防ぐことにあります。

その他のブロードキャストおよびマルチキャスト トラフィック

前述のとおり、WLC（デフォルト）は、無線ユーザに対してブロードキャストやマルチキャストを転送しません。第 6 章「Cisco Unified Wireless のマルチキャスト設計」で説明したとおり、マルチキャスト転送が有効になっている場合は、WLC の接続先インターフェイスで生成されるマルチキャスト トラフィックを最小限に抑えるための処理を実行する必要があります。

WLAN により明示的にサポートされるマルチキャスト アドレス グループを制限するために、標準的な対策をすべて講じる必要があります。マルチキャストが有効になっている場合、これは事実上グローバルな設定です。つまり、WLAN がマルチキャストを必要としているかどうかに関係なく、設定されているすべての WLAN で有効になっていることを意味します。Unified Wireless ソリューションでは、データ リンク レイヤとネットワーク レイヤのマルチキャスト トラフィックは区別されません。どちらも、特定のマルチキャスト トラフィックをフィルタできる WLC ではありません。したがって、次の手順の追加を検討する必要があります。

- WLC に接続しているインターフェイスで CDP を無効にします。
- WLC に接続されている VLAN で、受信した CDP および HSRP トラフィックをポート フィルタします。
- マルチキャストは、ゲスト WLAN を含む WLC のすべての WLAN で有効になるため、リンク レイヤのマルチキャスト セキュリティを含むマルチキャスト セキュリティを考慮する必要があることを覚えておいてください。

設計上の考慮事項

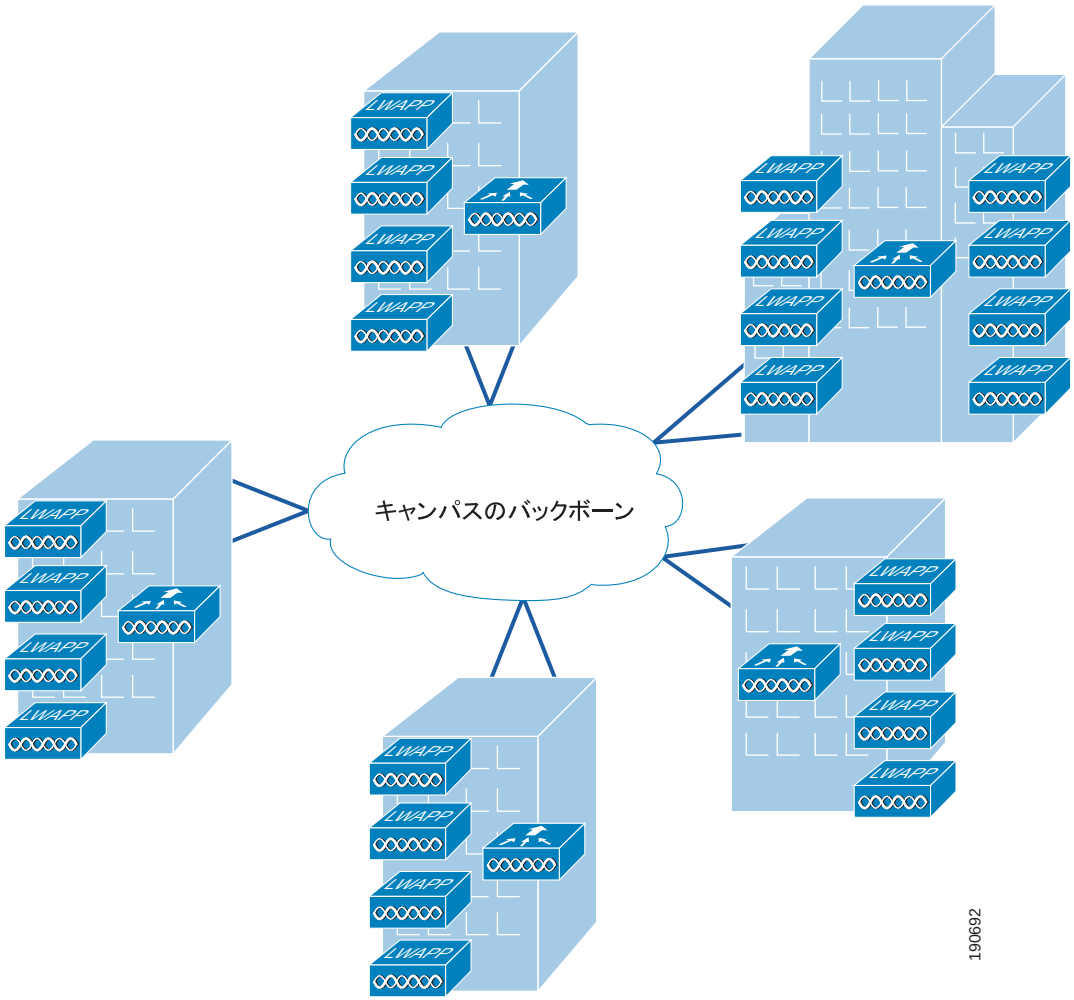
Cisco Unified Wreless 展開の設計における主な考慮事項は、AP 接続と WLC の場所および接続です。この項では、これらのトピックについて簡単にまとめ、必要に応じて標準的な推奨事項について説明します。

WLC の場所

Cisco Unified Wireless LAN ソリューションの柔軟性から、WLC の設置場所に関して、次のような選択肢が考えられます。

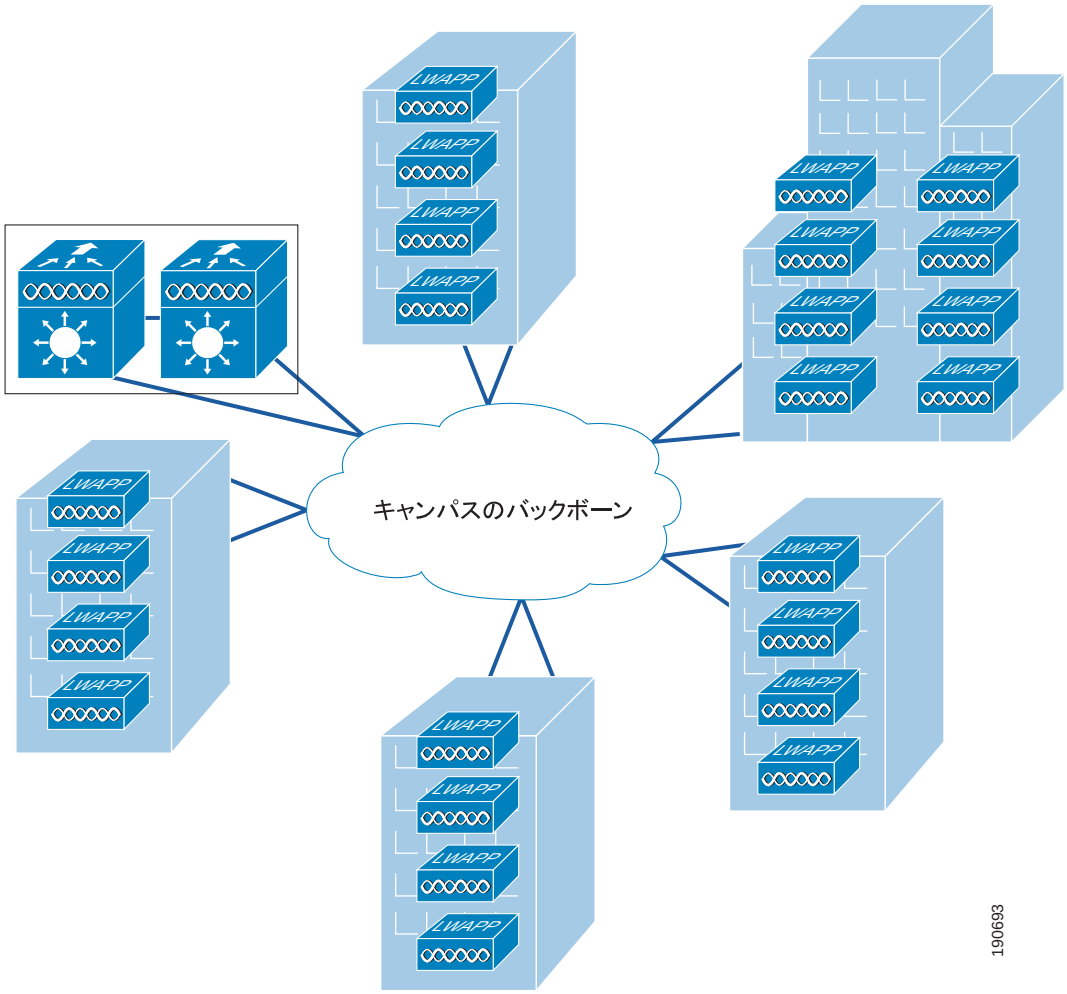
- 分散された WLC 展開：分散モデルでは、WLC はキャンパス ネットワーク全体、通常はビルディングごとに配置され、そのビルディングに存在する AP を管理します。WLC をキャンパス ネットワークに接続するためには、ビルディング内の分散ルータが使用されます。このシナリオでは、AP と WLC の間の LWAPP トンネルは通常ビルディング内にとどまります。図 2-16 は分散された WLC 展開を示しています。
- WLAN カバレッジがビルディング間で重複しない限り、分散された WLC をそれぞれ、別々の RF グループおよびモビリティ グループに設定できます。

図 2-16　分散された WLC



- 集中化された WLC 展開：このモデルでは、WLC は企業ネットワークの集中化された場所に配置されます。この展開モデルでは、キャンパス バックボーン ネットワークを経由するために AP/WLC LWAPP トンネルが必要です。集中化された WLC 展開の例を図 2-17 に示します。ただし、下の例では、集中化された WLC（Catalyst 6500 にある WiSM のペア）は、特定のビルディング内には示されていないことに注意してください。集中化された WLC クラスタは専用スイッチ ブロック経由でキャンパスの中心に接続されます。キャンパスの中心は、通常、データ センターと同じビルディングにあります。データ センターと WLC クラスタでは、通常、ネットワークおよびセキュリティ要件が異なるので、WLC をデータ センターのスイッチ ブロックに直接接続してはいけません。

図 2-17　集中化された WLC



WLC の集中化

このデザイン ガイドでは、一般的に、キャンパス環境全体の中心的な位置に WLC を展開することを推奨しています。モビリティ グループとレイヤ 3 ローミングを必要とする分散展開モデルは十分に証明されていますが、レイヤ 3 ローミングに関連するマルチキャスト サポートに現在不十分な点があるため、推奨されていません。これらへの対策が行われた場合、分散展開モデルの検討を妨げる障壁の大半は解消されます。リリース 4.1 以前は、そのほかにも、分散展開を非現実的なものにする機能的な問題（トンネル QoS およびアシンメトリック トンネリング）がありましたが、それらも解決されています。

レイヤ 3 ローミングに対応する最善策は、レイヤ 3 ローミングを使用せざるを得ないような展開シナリオを避けることです。現時点では、WISM モデルの持つ拡張性、および WLC の提供するブロードキャストまたはマルチキャスト抑制機能のため、大きなモビリティ サブネットの方が実現性が高くなっています。

WLC インフラストラクチャを中央集中化することにより、容量管理はさらに簡単になり、費用対効果も向上します。また、WLAN はよりミッション クリティカルになるため、中央集中型の実装により、可用性の高い WLC トポロジを作成しやすくなります。中央集中化により、容量管理や高可用性の問題に対応しなければならない場所が減少します。

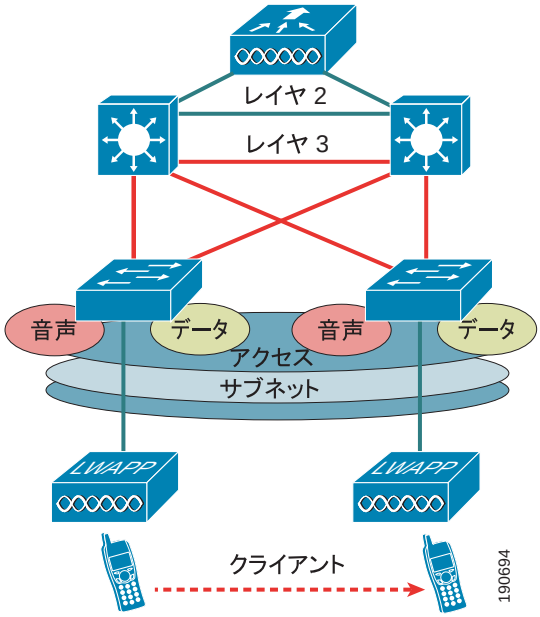
WLC を他のインフラストラクチャ コンポーネントと統合する場合にも同様の原理が当てはまります。集中化された WLC により、統合ポイントおよび統合デバイスの数を最小限に抑えられます。たとえば、NAC アプライアンスのようなインライン セキュリティ デバイスの実装を決定したとき、集中化された WLC の場合は統合ポイントが 1 か所ですが、分散ソリューションの場合は統合ポイントが *n* か所になります。*n* は、WLC の展開箇所の数を示します。

要約すると、集中化された WLC 展開の使用が推奨されるということです。集中化された WLC 展開を計画する場合、WLC に直接接続される有線ネットワーク インフラストラクチャの保護を考慮する必要があります。これは、WLC は基本的に、接続さえしていなければ「ネットワーク アクセス」およびこれに伴う脆弱性にさらされることのないような企業トポロジ内の場所にある「アクセス」ネットワークを接続するからです。したがって、アクセス レイヤ ネットワーク デバイスに関連する一般的なセキュリティ上の配慮事項をすべて検討する必要があります。たとえば、WiSM をベースとする展開では、DoS 攻撃やトラフィック ストームに対する保護などの機能を検討する必要があります。これは、多数のエンド ユーザに対してさまざまな WLAN サービスを提供すると同時に、複数レイヤにわたるマルチファンクション Catalyst 6500 スイッチ プラットフォームのバックプレーンに直接接続されている WISM が果たす役割は大変大きいからです。

分散された WLC ネットワークの接続

前述のとおり、分散された WLC は通常、キャンパス ネットワーク内のディストリビューション レイヤ ルータに接続されます。このような場合は、図 2-18 に示すように、レイヤ 2 リンクを経由して WLC をディストリビューション レイヤに接続することはお勧めしません。

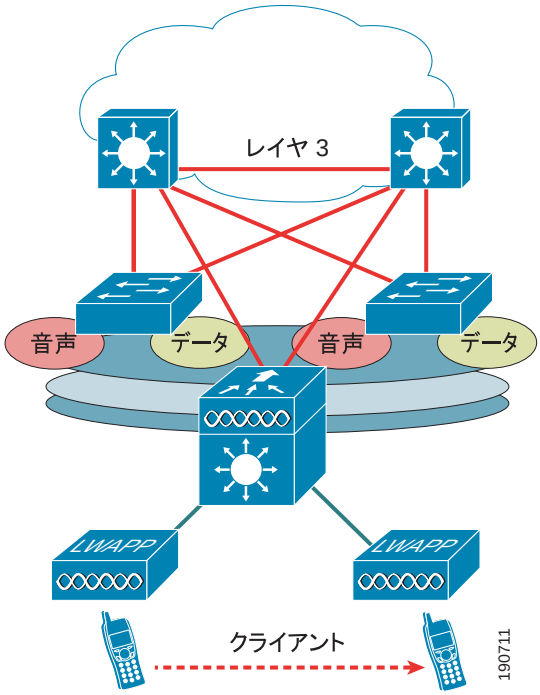
図 2-18　レイヤ 2 に接続された WLC



この推奨は、以下を含む多数の理由によるものです。

- 一般的なベスト プラクティスであるキャンパス設計では、レイヤ 3 アクセスを使用し、高速なコンバージェンスと簡単な操作を提供するために接続を分散することをお勧めします。レイヤ 2 に接続された WLC を入れると、このモデルは壊れます。
- レイヤ 2 WLC 接続では、HSRP など、ディストリビューション レイヤでのアクセス レイヤ機能およびアクセス レイヤのセキュリティ機能の導入が必要になります。ただし、ディストリビューション レイヤが適切なすべてのアクセス スイッチをサポートしていない場合や、アクセス機能をサポートするためにソフトウェアのバージョンを変更する必要がある場合は、問題になる可能性があります。
- 図 2-19 に示すように、レイヤ 3 に接続された WLC（この場合は 3750G）では、WLAN 関連のソフトウェアおよび設定を 1 つのデバイスに分離し、他のアクセス レイヤ ルーティング デバイスと同じルーティング設定を使用してディストリビューション レイヤに接続できます。

図 2-19　レイヤ 3 に接続された WLC



トラフィックの負荷と有線ネットワークのパフォーマンス

Unified Wireless ソリューションを展開する場合に、次のような疑問が生じることがよくあります。

- 有線バックボーンに対する LWAPP トラフィックの影響または負荷
- Unified Wireless 展開をサポートするために必要な最低限のパフォーマンス要件
- ネットワークのトラフィック負荷に関連して、分散された WLC 展開と集中化された WLC 展開の相対的な利点

ネットワークのトラフィック ボリューム全体に対して LWAPP トラフィックが与える影響を検証するうえで、考慮する点は主に 3 つあります。

- LWAPP コントロール トラフィックのボリューム：LWAPP コントロールに関連するトラフィックのボリュームは、ネットワークの実際の状態によって異なります。通常、ソフトウェアのアップグレード中や WLC のリブート中は多くなります。しかし、トラフィックの調査では、LWAPP コントロール トラフィックがネットワークにかける平均的な負荷は約 0.35Kb/sec であることが判明しています。このトラフィックは、ほとんどのキャンパスで無視できる量であり、集中化された WLC 展開と分散された WLC 展開を比較しても大差はありません。
- トンネリングによって生じるオーバーヘッド：レイヤ 3 LWAPP トンネルによって、WLAN クライアントとの間で送受信される通常の IP パケットに 44 バイトが追加されます。標準的な企業で見られる平均パケット サイズが約 300 バイト以下であることを考えると、約 15% のオーバーヘッドとなります。このオーバーヘッドは、ほとんどのキャンパスで無視できる量であり、集中化された WLC 展開と分散された WLC 展開を比較しても大差はありません。
- トラフィック エンジニアリング：集中化された WLC にトンネルされた WLAN トラフィックはすべて、WLC の場所からネットワークでの終点にルーティングされます。トンネルの距離と WLC の場所によっては、これ以外の方法では、WLAN クライアント トラフィックは指定された宛先への最適なパスをたどって進まない可能性があります。従来のアクセス トポロジや分散された WLC 展開の場合、クライアント トラフィックはエッジから入り、宛先アドレスに基づいてそのポイントから適切にルーティングされます。

しかし、集中化された展開モデルに関連する長いトンネルや潜在的に効率の悪いトラフィック フローは、クライアント トラフィックの大半が目的地としているネットワークの部分（データ センターなど）に WLC を配置することで、ある程度、緩和できます。企業のクライアント トラフィックのほとんどがデータ センターのサーバに向かうことと、企業のバックボーン ネットワークが低遅延であることを考えると、効率の悪いトラフィック フローに関連するオーバーヘッドは無視できますし、集中化された WLC 展開と分散された WLC 展開を比較しても大差はありません。

ほとんどの企業において、WLAN の導入によって、新しいアプリケーションがすぐに必要になることはありません。したがって、Cisco Unified Wireless Network を追加するだけで、キャンパスのバックボーン トラフィックの量に深刻な影響が出ることはありません。

AP 接続

AP は、エンド ユーザとは別のネットワーク上になければなりません。これは、インフラストラクチャ管理インターフェイスはエンド ユーザとは別のサブネット上にあるべきであると定義している一般的なベスト プラクティスと一致しています。さらに、Catalyst Integrated Security Features（CISF）を LWAPP AP スイッチ ポートで有効にして、WLAN インフラストラクチャの保護を強化することをお勧めします（H-REAP AP 接続については、第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照）。

展開を容易にするために、最新の WLC アドレス情報を提供する簡単なメカニズムを備えていることから、AP アドレス割り当て方法としては、一般に DHCP が推奨されています。AP に静的 IP アドレスを割り当てることができますが、詳細な計画および個々の設定が必要になります。静的 IP アドレスを設定できるのは、コンソール ポートを備えた AP だけです。

Cisco Unified Wireless Network に WLAN QoS 機能を効率的に提供するには、LWAPP AP と WLC の間の接続を提供する「有線」ネットワーク全体で QoS も有効にしておく必要があります。

運用および保守

ここでは、Cisco Unified Wireless 展開の運用および保守を簡単にするための展開上の一般的な考慮事項と推奨事項について説明します。

WLC ディスカバリ

AP のための、次のようにさまざまな WLC ディスカバリ メカニズム（前述）により、LWAPP AP の初期展開は非常に簡単になります。

- 制御された環境での WLC を使用して前もって行われる LWAPP AP のステージング（プライミング）
- 自動ディスカバリ メカニズムの 1 つ（DHCP、DNS、または OTP）を使用し、難しい設定なしに行われる展開

自動ディスカバリは非常に便利ですが、ネットワークへの接続後は、AP の接続先 WLC の制御は通常、ネットワーク管理者により行われます。その後、管理者により、通常動作中の AP のプライマリ WLC の定義や、バックアップのためのセカンダリ WLC およびターシャリ WLC の設定が行われます。

AP の分散

WLC ディスカバリ プロセスについては、この章ですでに説明しました。典型的な初期展開では、AP は、各 WLC の負荷に応じて、使用可能な WLC 全体に AP 自体を自動的に分散します。このプロセスにより展開は簡単になりますが、いくつかの運用上の理由から、自動分散の使用はお勧めしません。

物理的に同じ場所にある AP は、同じ WLC に接続する必要があります。これにより、一般的な管理、運用、および保守が簡単になり、担当者はさまざまな運用上の作業がその場所に与える影響を抑えることができるようになるほか、WLC 内でのローミングと WLC 間でのローミングのいずれにかかわる WLAN の問題を特定の WLC とすばやく関連付けることができるようになります。

複数の WLC にわたる AP 分散を制御するために使用されるツールは、次のとおりです。

- プライマリ、セカンダリ、ターシャリ WLC 名：各 AP は、プライマリ、セカンダリ、およびターシャリ WLC 名で設定できます。これにより、モビリティ グループの WLC 間の負荷の変化に関係なく、AP が接続するモビリティ グループ内の最初の 3 つの WLC が決まります。
- マスター WLC：初めて AP が モビリティ グループの WLC に接続するときには、マスター WLC はプライマリ、セカンダリ、およびターシャリ WLC で設定されていません。したがって、既知の WLC 負荷に応じて、どの WLC ともパートナーになることができます。WLC がマスター WLC として設定されている場合、プライマリ、セカンダリ、およびターシャリ WLC 定義を持たない AP はすべて、マスター WLC に接続されます。これにより、運用担当者は、新しく接続された AP を簡単に見つけられるようになります。また、プライマリ、セカンダリ、およびターシャリ WLC 名前パラメータを定義して、AP が稼働状態になるタイミングを制御できます。

ファームウェアの変更

Cisco Unified Wireless Network を運用するときには、WLAN ネットワーク全体の中断を最小限に抑えながら WLC ファームウェアをアップグレードする方法を考えることも重要です。そうしないと、ある WLC にアソシエートされているすべての AP が新しいソフトウェアをダウンロードしている間に、その WLC を単にアップグレードしたりリブートしたりしただけで、一部のロケーションの WLAN カバレッジが失われる可能性があります。

規定どおりの方法で AP をセカンダリ WLC に移行し、プライマリ WLC をアップグレードしてから、アップグレードした WLC に AP を戻すことをお勧めします。

この手順は、高可用性を実現できるように展開が設計された 1+1 シナリオでは、多少異なります。

- AP をプライマリ WLC からセカンダリへ移動
- プライマリ WLC をアップグレード
- すべての AP をプライマリ WLC に戻す
- セカンダリ WLC をアップグレード
- セカンダリ AP をセカンダリ WLC に戻す

N+1 シナリオの場合

- WLC のアップグレードの間、各 WLC がその AP を +1 WLC に移動する
- アップグレード後、AP をプライマリ WLC に戻す
- WLC がすべてアップグレードされたら、+1 WLC をアップグレードする

（注） プライマリ AP を制御された方法でプライマリ WLC に戻せるように、AP フェールバックは無効にしておく必要があります。

CHAPTER 3

WLAN 無線周波の設計に関する考慮事項

この章では、さまざまな無線ローカル エリア ネットワーク（WLAN）環境における Radio Frequency（RF; 無線周波）の考慮事項を理解するために必要な RF の基本情報について説明します。この章は、次の内容で構成されています。

- 規制区域と周波数
- IEEE 802.11 規格について
- 802.11b/g や 802.11a などの RF スペクトラムの実装
- RF 展開の計画
- WLAN カバレッジの手動による微調整
- Radio Resource Management（RRM）

RF の基礎

アメリカ合衆国では、工業用、科学用、および医療用（ISM）の無認可使用のために 3 つの帯域が割り当てられています。これらの ISM 帯域は、次のように定義されています。

- 900 MHz（902 ～ 928 MHz）
- 2.4 GHz（2.4 ～ 2.4835 GHz）（IEEE 802.11b/g はこの周波数範囲で動作）
- 5 GHz（5.15 ～ 5.35 および 5.725 ～ 5.825 GHz）（IEEE 802.11a はこの周波数範囲で動作）

各範囲には異なる特徴があります。低周波数は、広い範囲を公開しますが、帯域幅は限られているため、データ レートは低くなります。高周波数は、狭い範囲を公開し、サイズの大きいオブジェクトの場合は減衰量が増えることがあります。

以降の項では、802.11 無線での 2.4 GHz および 5 GHz の周波数範囲における通信を向上させるために使用される RF 特性について、具体的にいくつか紹介します。この項では、規制区域とその動作周波数の概要を示します。

規制区域

無認可の帯域で動作するデバイスは、正式な認可を得るプロセスは必要ありませんが、これらの帯域で動作する際、ユーザは政府がその地域に対して定めた規制に従う必要があります。世界中の各規制区域は、それぞれの基準に従ってこれらの帯域を監視しています。これらの区域で使用される WLAN デバイスは関連する行政の規制区域の規格に従う必要があります。規制要件が IEEE 802.11b/g および 802.11a 準拠製品の相互運用性に影響することはありませんが、管理機関は実際に規格で特定の基準を設定しています。たとえば、無線が生成したり、同じプロキシミティの別の無線から受信する干渉の量を最小限に抑えるための、WLAN のエミッション要件があります。関連する規制機関から製品の認証を受けることは、ベンダーの責任です。表 3-1 は Wi-Fi 製品に対する最新の規制区域の要約を示しています。主な規制区域は、FCC、ETSI、および電波法です。

多くのベンダーでは、規制当局の要件に準拠するほか、Wi-Fi 認証プログラム（www.wi-fi.org）を通じて、他のベンダーとの互換性も確認しています。

その他の国の規制送信電力の設定および許可されている周波数利用の一覧は、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a008059c96f.html

表 3-1　規制区域

規制区域	地理的地域
南・北・中央アメリカまたは United States Federal Communication Commission（FCC）	北、南、中央アメリカ、オーストラリア、ニュージーランド、アジアおよびオセアニアのさまざまな地域
ヨーロッパまたは European Telecommunications Standards Institute（ETSI）	ヨーロッパ（EU および非 EU 国の両方）、中東、アフリカ、アジアおよびオセアニアのさまざまな地域
日本（電波法）	日本
中国	中華人民共和国（中国大陸）
イスラエル	イスラエル
シンガポール[1]	シンガポール
台湾 [1]	中華民国（台湾）

1. シンガポールおよび台湾における無線 LAN に対する規制は、これらの国に固有のものであり、5 GHz 帯域での動作だけを対象としています。したがって、シンガポールおよび台湾は、5 GHz の操作だけに関する規制区域となります。2.4 GHz の操作の場合は、それぞれ ETSI および FCC が規制区域となります。

(注)　適合情報については、Cisco の Web サイトを参照してください。また、その国で許可されていることを調べるには、その国の規制当局に問い合わせてください。表 3-2 および表 3-3 に示されている情報は、一般的な指針として使用してください。地域的な要件を満たすシスコ製品に関する最新情報は、http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html を参照してください。

動作周波数

2.4 GHz 帯域の各規制は、動作時間の点では、比較的変わりがありません。FCC は 11 チャネル、ETSI は最大 13 チャネル、および日本は最大 14 チャネル許可していますが、チャネル 14 は 11b でしか使えません。

802.11a については、5.250 ～ 5.350 GHz（W53）の周波数範囲と、802.11a の追加チャネルとして 5.470 ～ 5.780 GHz の周波数範囲を公開する方向で各国が動き始めています。これらのさまざまな周波数については、この章の 802.11 に関する項で詳しく説明します。

802.11b/g の動作周波数およびデータ レート

1999 年 9 月に批准された 802.11b 規格は 2.4 GHz スペクトラムで動作し、1、2、5.5、および 11 Mbps のデータ レートをサポートします。802.11b は、ユーザに幅広く受け入れられ、ベンダーからもサポートされています。802.11b テクノロジーは、数千ものエンタープライズ組織で展開されており、一般に、最新のアプリケーションで受け入れ可能なスピードおよびパフォーマンスが認められています。

2003 年 6 月に批准された 802.11g 規格は、802.11b と同じスペクトラムで動作し、802.11b 規格との下位互換性を備えています。802.11g はさらに、6、9、12、18、24、36、48、および 54 Mbps のデータ レートをサポートします。

表 3-2 はさまざまな 802.11b/g チャネル周波数と、各規制区域での使用が規制当局によって許可されているかどうかを示しています。すべての規制区域で、これらの周波数すべてを使用できるわけではない点に注意してください。

表 3-2　802.11b および 802.11g の動作周波数範囲

チャネル識別子	中心周波数	FCC（アメリカ）	ESTI（EMEA）	電波法（日本）	MOC（イスラエル屋外）[1]
1	2412	X	X	X	
2	2417	X	X	X	
3	2422	X	X	X	
4	2427	X	X	X	
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467		X	X	X

表 3-2　802.11b および 802.11g の動作周波数範囲

チャネル識別子	中心周波数	FCC（アメリカ）	ESTI（EMEA）	電波法（日本）	MOC（イスラエル屋外）[1]
13	2472		X	X	X
14[2]	2484			X	

1. イスラエルでは、チャネル 1 ～ 13 は屋内で許可されています。
2. チャネル 14 は 802.11b のみ利用可能です。

802.11a の動作周波数およびデータ レート

5 GHz 無線帯域の無許可の領域で動作する 802.11a は、2.4 GHz 帯域で動作する電子レンジ、さまざまなコードレス電話、Bluetooth（狭い範囲での低速なポイントツーポイントのパーソナルエリアネットワークの無線規格）などのデバイスからの干渉の影響を受けません。802.11a 規格は別の周波数範囲で動作するため、既存の 802.11b または 802.11g に準拠した無線デバイスとは互換性がありませんが、これは、2.4 GHz および 5 GHz の機器であれば、同じ物理環境で干渉することなく動作できるということです。

これら 2 つのテクノロジー（802.11b/g と 802.11a）を選択するうえで、1 対 1 のトレードオフは必要ありません。これらは補完的なテクノロジーであり、将来の企業環境でも共存し続けます。これらのテクノロジーの実装の責任者は、2.4 GHz だけのネットワーク展開、5 GHz だけのネットワーク展開、またはこれらをくみあわせた展開の中から、経験に基づいて選択できる必要があります。既存の 802.11b ネットワークを使用する組織は、単純に既存の AP に新しい 802.11a ネットワークを展開し、802.11b による 11 Mbps カバレッジと同じ領域で、802.11a による 54 Mbps カバレッジを期待するわけにはいきません。これらの両方の帯域の技術的な特性のため、このようなカバレッジの互換性は実現しません。

802.11a では、通常、所定の電力およびアンテナ ゲインに対して短い範囲で、6、9、12、18、24、36、48 のデータ レート、および最大データ レート 54 Mbps を使用できますが、802.11b/g ではオーバーラップしない周波数チャネルが 3 つであるのに対し、地理的地域に応じてオーバーラップしない周波数チャネルが最大で 23 あります。この結果、ネットワーク キャパシティが増加し、スケーラビリティが向上して、近接するセルから干渉を受けずにマイクロセルラー展開を作成できるようになります。

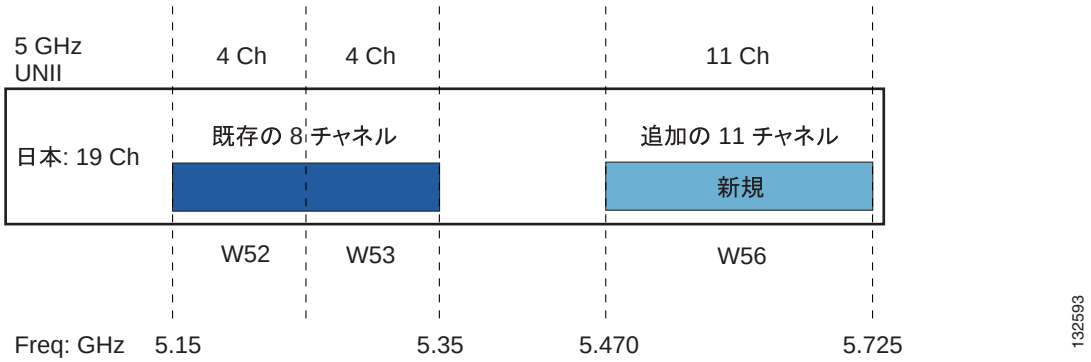
802.11a が動作する 5 GHz 帯域は、複数の異なる部分に分割されています。表 3-3 に示されている 802.11a の各帯域で、W52、W53、W56 は屋内で、また W56 は屋外でも使用できます。日本では、それぞれ 4 つのチャネルを持つ W52、W53、および 11 のチャンネルを持つ W56 帯域が使用できます。チャネルは、20 MHz 離して設定され、RF スペクトラムが 20 MHz であるため、オーバーラップしないチャネルとなります。

これら 3 つの UNII 帯域には、別々の制限があります。それぞれ、送信電力、アンテナ ゲイン、アンテナ スタイル、および用途の制約が異なります。W52 帯域と W53 帯域は、屋内での動作を目的として使用されます。W56 帯域は、屋内または屋外の 802.11a WLAN にも使用できます。

W52（5.150 ～ 5.250 GHz）のチャネルは、36、40、44、および 48 です。W53（5.250 ～ 5.350 GHz）のチャネルは、52、56、60、64 で、Dynamic Frequency Selection（DFS; 動的周波数選択）および Transmitter Power Control（TPC）が必要です。W56 のチャネルは、100、104、108、112、116、120、124、128、132、136、140 で、DFS および TPC が必要です。所定の範囲のすべてのチャネルをすべての規制区域で使用できるわけではありません。図 3-1 は、W52、W53、および W56 帯域のさまざまなチャネルと追加の新しい 11 チャネルを示しています。

総務省は 2007 年 1 月 31 日、5.6 GHz 帯（W56）を無線 LAN に解放する電波法関連の法律を改正しました。この改正では、新しく 11 のチャネルが追加され、使用可能なチャネル キャパシティは合計 19 に増えました（図 3-1 を参照）。

図 3-1　802.11 のチャネルのキャパシティ



新しく追加された 11 のチャネルは、屋内および屋外で使用できます。ただし、新しい 11 のチャネルを使用するには、無線が、802.11h の仕様で規定されている 2 つの機能（TPC および DFS）を備えている必要があります。DFS は、この周波数範囲で動作するレーダーを避けるために必要ですが、これは、動的周波数の計画など他の用途にも使用できます。802.11h は、Cisco Unified Wireless Network Software Release 3.1 以降サポートされています。

DFS は、特定の条件（レーダー信号の存在など）が満たされたときには必ず、トランスミッタに対して別のチャネルへの切り替えを動的に指示します。デバイスの DFS メカニズムは、送信前に、使用可能な動作範囲を監視し、レーダー信号を待ちます。信号が検出されると、レーダー信号にアソシエートされているチャネルが解放されるか、そのチャネルをトランスミッタが使用できないことを示すフラグが立てられます。送信デバイスは、動作前および動作中に、その環境で継続的にレーダーの存在を監視します。5 GHz 帯域の部分は、レーダー システムに割り当てられます。これにより WLAN では、現在のレーダー ユーザが同じ場所にまとめて配置されている場合に、それらのユーザへの干渉を回避できるようになります。

TPC により、AP がアソシエーション プロセスで WLAN クライアントと電力レベルをネゴシエートできるようになります。AP は、その WLAN クライアントに、その AP に対して使用することのできる送信電力の範囲を知らせて、そのレベルを満たすことができないクライアントを拒否できます。WLAN クライアントは、そのクライアントの送信電力レベルを、TPC ネゴシエーションで指定された範囲内に調節できます。これにより、WLAN からの干渉を最小限に抑え、WLAN クライアントのバッテリ寿命を最適化できるようになります。

米国 FCC 規制の最新情報の詳細は、
http://www.cisco.com/en/US/products/hw/wireless/ps469/products_white_paper0900aecd801c4a88.shtml を参照してください。

表 3-3 は、802.11a 規格の周波数を示しています。

表 3-3　802.11a の動作周波数の範囲

チャネル識別子	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	138	140
中心周波数 MHz	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700
帯域	W52				W53				W56										
場所	屋内				屋内				屋内および屋外										

IEEE 802.11 規格について

IEEE 802.11 とは、Institute for Electrical and Electronics Engineers（IEEE）内で作業しているグループで、OSI モデルの物理レイヤおよびリンクレイヤ（レイヤ 1 とレイヤ 2）の無線 LAN 標準を担当しています。これに対して、Internet Engineering Task Force（IETF）はネットワーク レイヤ（レイヤ 3）プロトコルを担当しています。802.11 作業グループでは、802.11 WLAN 規格の要素を担当する多数のタスク グループがあります。表 3-4 は、タスク グループ イニシアチブの一部の要約を示しています。

これらの作業グループの詳細は、http://www.ieee802.org/11/ を参照してください。

表 3-4　IEEE 802.11 タスク グループの活動

タスク グループ	プロジェクト
MAC	Physical Layer Entity（PHY）タスク グループと共に、WLAN のための 1 つの共通の MAC を開発する
PHY	赤外線、2.4 GHz FHSS、2.4 GHz DSSS という 3 つの WLAN PHY を開発する
a	5 GHz UNII 帯域のための PHY を開発する
b	2.4 GHz 帯域で高レートな PHY を開発する
c	802.11 MAC でのブリッジ動作を扱う（スパニング ツリー）
d	その他の規制区域（国）の 802.11 動作のための物理レイヤ要件を定義する
e	QoS のために 802.11 MAC を強化する
f	マルチベンダー使用のために Inter Access Point Protocol（IAPP）の推奨案を作成する
g	802.11b に対して高速な PHY 拡張を開発する（54 Mbps）
h	802.11 MAC と 802.11a の PHY Dynamic Frequency Selection（DFS）、Transmit Power Control（TPC）を強化する
i	802.11 MAC のセキュリティおよび認証メカニズムを強化する
j	802.11 の規格を強化し、日本における 4.9 GHz および 5 GHz のチャネル選択の追加に向けて修正する
k	無線およびネットワーク測定のための上位レイヤにインターフェイスを提供するため、Radio Resource Measurement 拡張を定義する
m	802.11 系列の仕様の文書に関する、編集上の管理、修正、改訂、明確化、および翻訳を行う
n	2.4 GHz、5 GHz 帯域における高スループット拡張（MAC SAP で >100 MB/s）を重点的に扱う
o	Voice over WLAN での高速なハンドオフ（目標は 50 ms あたり）を提供する
p	料金徴収、車両安全サービス、車でのコマース トランザクションなど、車両を対象とした車両用通信プロトコルを中心に扱う
r	高速な BSS 遷移および高速なローミングを定めた規格を開発する
s	完全に網羅するように向上されたメッシュ ネットワークの MAC および PHY を定義する
t	製造業者、テスト ラボ、サービス プロバイダ、ユーザが 802.11 WLAN デバイスおよびネットワークのパフォーマンスをコンポーネントおよびアプリケーション レベルで測定できるようにするパフォーマンス メトリック、測定方法論、テスト条件を提供する
u	IEEE 802.11 アクセス ネットワーク（ホットスポット）と外部ネットワークの間に機能およびインターフェイスを提供する

表 3-4　IEEE 802.11 タスク グループの活動（続き）

タスク グループ	プロジェクト
v	ステーション（STA）に対してネットワーク管理を提供する 802.11 MAC/PHY への拡張を提供する
w	アクション管理フレーム、認証解除フレーム、アソシエーション解除フレームなどの、選択した IEEE 802.11 管理フレームのデータの整合性、データ発信元の信頼性、応答の保護、データの機密保持を実現するメカニズムを提供する

Direct Sequence Spread Spectrum

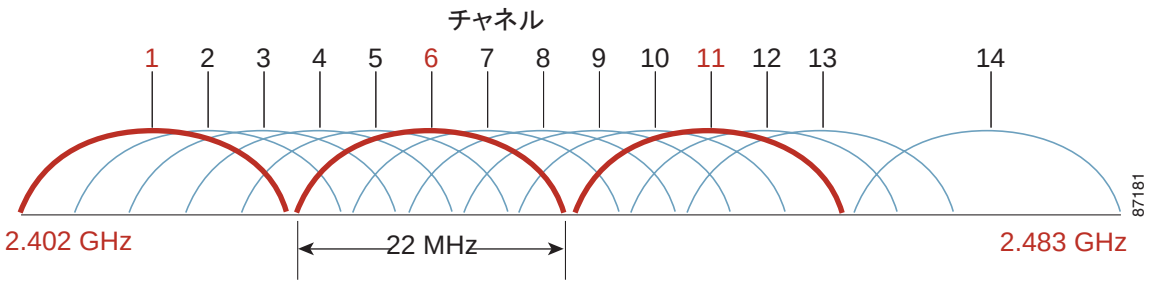
Direct Sequence Spread Spectrum（DSSS）は、冗長情報を RF 信号に符号化します。これにより、802.11 無線は、チャネルでバックグラウンド ノイズまたは干渉があったとしても、パケットの受信を理解する確立が高くなります。すべてのデータ ビットは、チッピング シーケンスまたはバーカー シーケンスと呼ばれるビット文字列またはチップに拡張されます。IEEE 802.11 によって指示されているチッピング レートは 1 ビットあたり 11 チップです。1 および 2 Mbps のレートで Binary Phase-Shift Keying（BPSK; 2 位相偏移変調）/Quadrature Phase-Shift Keying（QPSK; 4 位相偏移変調）を使用し、11 および 5.5 Mbps レートで 8 チップ（CCK; Complimentary Code Keying）を使用します。これは、11 Mbps ではデータの 1 ビットに対して 8 ビットが送信されるということです。チッピング シーケンスは、スペクトル拡散周波数範囲で並列に送信されます。

IEEE 802.11b Direct Sequence チャネル

IEEE 802.11b の Direct Sequence（DS）チャネル セットでは、14 チャネルが定義されています。送信される各 DS チャネルは 22 MHz ですが、チャネル用は 5 MHz だけです。結果として、隣接するチャネルからの信号が互いに干渉しあうなど、チャネルのオーバーラップが発生します。14 チャネルの DS システム（US の場合、使用可能なチャネルは 11）では、間隔が 25 MHz のオーバーラップしないチャネルは 3 つだけ（チャネル 1、6、および 11）です。

このチャネルの間隔によって、オフィスやキャンパスなどの複数 AP 環境でのチャネルの仕様および割り当てが決まります。AP は通常、隣接する AP がオーバーラップしないチャネルに割り当てられる、セルラー形式で企業内に展開されます。または、1 つの領域に 33 Mbps の帯域幅を提供するように（ただし、1 つのクライアントには 11 Mbps だけ）、チャネル 1、6、および 11 を使用して、AP を同じ場所にまとめて設置することもできます。同様に 802.11g を使用した場合の集約帯域幅は 162 Mbps で、最大データ レートは 54 Mbps になります。図 3-2 は、チャネルの割り当て方法を示しています。

図 3-2　IEEE 802.11 DSS のチャネル割り当て



IEEE 802.11g

802.11g は、802.11b と同じスペクトラムである 2.4 GHz の帯域でより高いデータ レート（最大 54 Mbps）を提供します。802.11g は 802.11b との下位互換性があり、6、9、12、18、24、36、48、54 Mbps のデータ レートも提供します。802.11g は、802.11a と同様（IEEE 802.11a OFDM の物理レイヤ（P. 3-8）を参照）、高いデータ レートで同じ変調技術 Orthogonal Frequency Division Multiplexing（OFDM）を使用します。

表 3-5 は、さまざまなデータ レートに対する 802.11g の変調と伝送の種類を示しています。

表 3-5　802.11g の変調および伝送の種類

変調	伝送の種類	サブチャネルあたりのビット数	データ レート（Mbps）
BPSK	DSSS	NA	1
QPSK	DSSS	NA	2
CCK	DSSS	NA	5.5
BPSK	OFDM	125	6
BPSK	OFDM	187.5	9
CCK	DSSS	NA	11
QPSK	OFDM	250	12
QPSK	OFDM	375	18
16-QAM	OFDM	500	24
16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

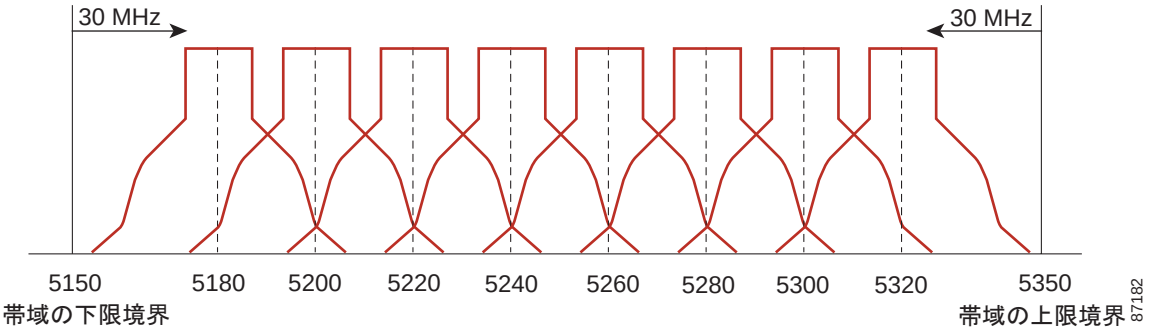
IEEE 802.11a OFDM の物理レイヤ

IEEE 802.11a は、6 ～ 54 Mbps のデータ レートで 5.0 GHz UNII 周波数で動作する、OSI モデルの物理レイヤに対する要件を定義します。IEEE 802.11a は、シングル キャリア システムと比較してマルチキャリア システムである Orthogonal Frequency Division Multiplexing（OFDM）を使用します。OFDM を使用すると、サブチャネルはオーバーラップが可能になるため、スペクトラム効率が高くなります。OFDM で可能な変調技術は、802.11b で使用されるスペクトル拡散技術よりも効率的です。

IEEE 802.11a のチャネル

802.11a のチャネルは、チャネルの中心周波数を表しています。チャネルの周波数は点線の両側の 10 MHz です。図 3-3 に示すように、チャネル間には 5 MHz の間隔があります。

図 3-3　チャネル セットの例（W52、W53 の場合）



日本の 802.11a 規格の場合、合計 19 チャネルをサポートしています。帯域は、5.150 ～ 5.250 GHz（W52）、5.250 ～ 5.350 GHz（W53）、および 5.470 ～ 5.725 GHz（W56）の 3 つです。

RF 電力の用語

dB、dBi、dBm の各単位は、それぞれ、システムのポイントで測定したとき、無線で感知したとき、または基準電力レベルと比較したときの電力の変化量を表すために使用されます。次の項では、Effective Isotropic Radiated Power（EIRP）の説明に加えて、これらの用語の違いを説明し、使用に関する指針を示します。

dB

*デシベル（dB）*という用語は、電力レベルの減衰または増幅に主に使用されます。dB は、別の標準化された値に対する信号の対数比です。たとえば、dBm の場合は 1 ミリワットに対して値が比較され、dBw の場合は 1 ワットに対して値が比較されます。

計算は、次のとおりです。

電力（dB 単位）= 10 * log10（信号 / 基準）

適切な数字を当てはめると（たとえば、信号に 100mW、基準に 1mW）、dB の値として 20（100 = 10 の 2 乗、つまり指数が 2 となり 10 を掛けることで 20 となる）が算出されます。

これは対数（線形ではなく指数としての増減を意味する）であり、ある基準に対する値の比率であることを覚えておいてください。また、これを 10 倍することも忘れないようにしてください。

対数である場合、いくつかの一般的な規則があります。3dB の増減は、それぞれ、信号（電力）が 2 倍または 1/2 になったことを意味します。10dB の増減は、信号が元の値の 10 倍になったか、1/10 になったことを意味します。

屋内の WLAN および屋外の WLAN 展開は両方とも、RF 展開において異なる課題があり、これらは分けて分析する必要があります。ただし、屋内使用に関しては、ある経験則があります。9dB 増加するたびに、屋内のカバレッジ領域が 2 倍になります。9dB 減少するたびに、屋内のカバレッジ領域が 2 分の 1 になります。

dBi

dBi という用語は、アンテナの電力ゲインの格付けを表すために使用されます。実際のアンテナを、同じ電力をすべての方向に送信する等方性アンテナ（理論上または架空のアンテナ）と比較する際に dBi が使用されます。

アンテナはこの理想の測定値と比較され、すべての FCC 計算でこの単位（dBi）が使用されます。たとえば、Cisco の全方向性 AIR-ANT4941 のゲインは 2.2dBi です。これは、アンテナの最大エネルギー密度が等方性アンテナよりも 2.2dB 多いことを意味しています。

dBm

dBm という用語は、dB の項で説明したものと同じ計算を使用しますが、基準値は 1 ミリワットです。

したがって、dB の項で示した例で考えると、無線で電力が 1 mW から 100 mW に変化した場合、電力レベルは 0 dBm から 20 dBm へ変化します。

dBm はトランスミッタ電力を表すだけでなく、レシーバの感度も表します。信号は送信した時点から値が減るため、レシーバの感度は、マイナス dBm（-dBm）で表されます。感度は、信号が理解できないと見なす前にレシーバが受信可能な最小電力を示します。

Effective Isotropic Radiated Power

無線の設定に基づいて送信される電力は、dBm またはミリワットで表されされますが、システム全体のアンテナから受ける最大エネルギー密度は、Effective Isotropic Radiated Power（EIRP）として測定されます。これは、さまざまなコンポーネントの dB 値を合計したものです。EIRP は、総務省や FCC や ETSI などの規制当局が電力制限を決定するために使用する値で、放射しているアンテナの第 1 フレネル内の最大エネルギー密度を表します。EIRP は、トランスミッタ電力（dBm 単位）をアンテナ ゲイン（dBi 単位）に加算し、ケーブル損失（dB 単位）を差し引くことで算出されます。たとえば、Cisco Aironet ブリッジを、約 15m（50 フィート）の長さの同軸ケーブルで、固定された皿型アンテナに接続している場合、数字を当てはめると次のようになります。

- ブリッジ：20 dBm
- 約 15 m（50 フィート）のケーブル：3.3 dBm（ケーブル損失のため、負の値）
- 皿型アンテナ：21 dBi
- EIRP：20-3.3+21=37.7 dBm（FCC の場合）

詳細は、http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml を参照してください。

RF 展開の計画

RF 設計における考慮事項のほとんどは、相互に依存しているか、または、実装に依存しています。したがって、要件および環境の大部分に対して「万能な」テンプレートはありません。

Cisco Wireless Control System（WCS）の統合された RF 予測ツールを使用すると、LWAPP AP の配置、設定、パフォーマンスやカバレッジの予測などの、詳細な無線 LAN の設計を作成できます。IT 担当者は、Cisco WCS に実際のフロア図面をインポートし、さまざまなビルディング コンポーネントに RF 特性を割り当てて、設計精度を高めることができます。

グラフィカルなヒート マップは、IT 担当者が、予想される無線 LAN の動作を視覚的に表現して、計画をより容易にし、展開をより迅速化するために役立ちます。また、WCS には、組織が不規則な形状のビルでの WLAN 展開の設計およびサポートを容易に行えるようにするための描画ツールが用意されています。図 3-4 は、計画ツールの例です。

図 3-4　計画ツール

オーバーラップする WLAN カバレッジのさまざまな展開の種類

無線ネットワークで設定する WLAN カバレッジのオーバーラップの規模は、使用状況によって異なりますが、一部の例外を除き、すべての設計は再送信とデータ レートの変化を最小限に抑えるように展開する必要があります。無線ネットワークは、ロケーション管理、音声、またはデータ専用のネットワーク、これらの組み合わせに対して展開できます。違いは、配置されている AP のパターンとカバレッジ領域で RF がオーバーラップする量にあります。WLAN 展開を計画するときは、WLAN 展開の今後の用途を考慮に入れる必要があります。

データ専用の展開だけでなく、付加サービスもサポートするように WLAN 展開を変えることは、単に AP を追加するだけでは済みません。詳細なサイトサーベイが必要になるほか、既存の AP を再配置が必要になる可能性もあります。

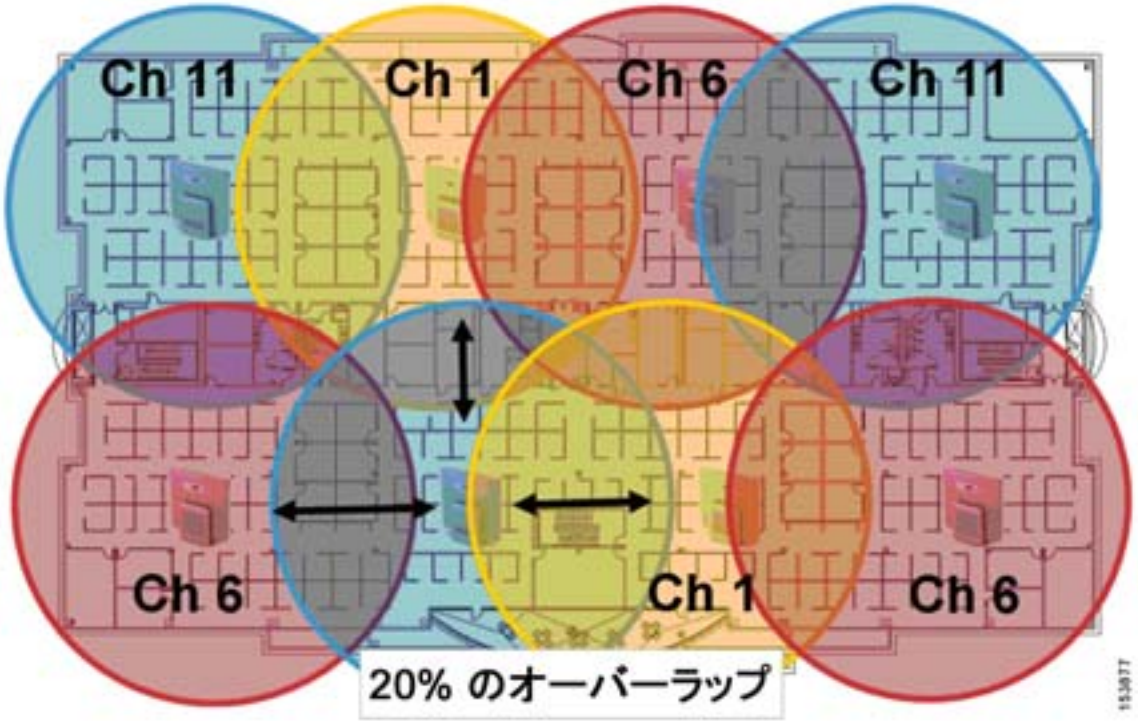
データ専用の展開

データ専用の展開の場合、大量のオーバーラップは必要ありません。これは、802.11 クライアントが、データ レートを下げ、時間をかけて転送することで、近くの AP からの低レベルの信号に応答するからです。必要なオーバーラップは、WLAN のデータ レート要件（P. 3-15）で説明されているように、WLAN のデータ レート要件によって決まります。データ専用ネットワークでは、AP 間の最適な距離は、通常約 36 ～ 39 m（120 ～ 130 フィート）ですが、AP の間隔を見積もる際は、RF 環境によって結果が異なるため、壁の密度、機械、エレベータ、スチール製のケージがある広い空間など、RF カバレッジに影響を与えるオブジェクトの要素を念頭に置くようにしてください。RRM はこのような展開向けに開発されたもので、RF カバレッジを制御する上で非常に便利です。

音声 / 展開

図 3-5 は、音声ネットワークのパターンとオーバーラップを示しています。

図 3-5　音声用の単一フロア サイトの調査



AP は互いに近くにまとめられ、データ専用の展開に比べ、多くのオーバーラップがあります。これは、音声クライアントは、パケットがドロップされないように、より良い AP に移動する必要があるからです。また、通常は、従来よりも小規模のセルで実行し、オーバーラップしているセルが -67 dBm 以上になるようにします。これは、1 つのセル全体における同質性を高め、ハンドヘルドでのプロセッサの負荷を減らすなど、さまざまな効果をもたらし、リンクの安定性を高め、遅延を減らします。定義された領域で必要な AP は 1 つだけですが、遅延およびロード バランシングの対策として、オーバーラップしているチャネルに 2 つの AP を設置し、その展開において Received Signal Strength Indication（RSSI）が常に 35 を超えるようにすることをお勧めします。7920 音声展開の場合は、展開において Received Signal Strength Indication（RSSI）が常に 35 を超えるようにすることをお勧めします。これは VoIP 電話の受信率を高めると同時に、加入超過をある程度許容して電話に対するローミング オプションを強化するためです。

低ノイズ バックグラウンドを配慮した設計は、セル内の比較的高いエネルギー密度と同様に重要であることを、忘れないでください。これは、AP に対して最適なベースライン電力設定が 3.5 ～ 50 mW の範囲内であるということです。これには通常、10 mW でカバレッジ モデルを展開する場合よりも約 15% 多い AP が必要となります。

既存の WLAN、802.11 に準拠していない不正な製品による干渉（たとえば、電子レンジや各種コードレス電話）など、問題のある特定の領域や干渉の原因となる可能性があるものを特定して、その特徴を調べるには、サイトの事前調査が有効です。すべての利害関係者によって確認され認証される必要がある設計に従い、カバレッジ モデルが、利害関係者によって示された機能要件に準拠していることを確認するには、サイトの事後調査を究極の監査メカニズムとして考える必要があります。

間隔を見積もる行う際は、RF 環境によって結果が異なる可能性があるため、壁の密度、機械、エレベータ、スチール製のケージがある広い空間など、RF カバレッジに影響を与えるオブジェクトの要素を忘れないようにしてください。フォークリフト、人々の集団、クレーンや同様の搬送装置によって領域を移動する大きな物体など、一時的な動きも考慮に含めるようにします。WLC は一般に、サイトの予備評価に非常に効果的な方法で、WLAN インフラストラクチャを高速に展開し、領域の RF 測定に使用できます。医療、小売、製造業界などで一般的に見られる複雑な領域には、サイトサーベイをエンドユーザに実施してもらうことも効果的な方法です。

無線音声の展開の詳細は、第 9 章「VoWLAN の設計に関する推奨事項」、および 7920 展開ガイド（http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html）を参照してください。

Lightweight AP およびコントローラを 7920 の音声動作用に設定する方法については、http://www.cisco.com/en/US/docs/wireless/technology/7920/design/guide/7920DG.html を参照してください。

Location-Based Service 展開

3 つ目の展開の種類は Location-Based Service（LBS）展開です。これは、究極のセル カバレッジだけでなく、最適な AP の場所に依存するため、現在のアプリケーションの中でも最も複雑です。ロケーション管理の展開は、WLAN インフラストラクチャを使用して、何千ものデバイスを同時に追跡できます。例としては、Wi-Fi タグ タイプの展開または資産追跡展開があります。これは、無線ネットワークで機器やデバイスを探したり、無線ネットワークのどこに無線クライアントがあるのかを図やダイアグラムで単純に示したりするものです。これを使用することで、不正クライアントや AP の場所を示すことで、無線インフラストラクチャのセキュリティを強化し、クライアントのトラブルシューティング能力を大幅に向上させることができます。

ロケーション管理の展開については、AP は交互にずらして配置されます。図 3-6 は典型的な配置パターンを示しています。交互にずらすと、デバイスの場所をより正確に見積もることができます。

図 3-6　単一フロアのロケーション管理の展開の例

ロケーションベースのサービスについては、第 13 章「Cisco Unified Wireless ロケーションベース サービス」、および http://www.cisco.com の『WiFi Location Based Services - Design and Deployment Considerations』というタイトルのホワイト ペーパーを参照してください。

Cisco 7921G と Cisco 7920 は、シスコの VoWLAN 端末です。WLAN に QoS を展開する一般的な理由の 1 つとして、これらの端末を使用する、ということがあります。

7920 および 7921G 端末の詳細は、以下の資料を参照してください。

- Cisco Unified Wireless IP Phone 7921G Version 1.0(2)

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html
- Cisco Unified Wireless IP Phone 7920 Version 3.0

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00801739bb.html
- VoWLAN インフラストラクチャを展開する場合は、単に WLAN に QoS を提供すればよいというわけではありません。音声 WLAN では、サイトサーベイのカバレッジ要件、ユーザの動作、ローミング要件、およびアドミッション制御について検討する必要があります。これらの要件については、以下のガイドで説明しています。
  - Design Principles for Voice Over WLAN

    http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/net_implementation_white_paper0900aecd804f1a46.html
  - Cisco Unified Wireless IP Phone 7921G Deployment Guide

    http://www.cisco.com/en/US/products/hw/phones/ps379/products_implementation_design_guides_list.html
  - Cisco Wireless IP Phone 7920 Design and Deployment Guide

    http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

WLAN のデータ レート要件

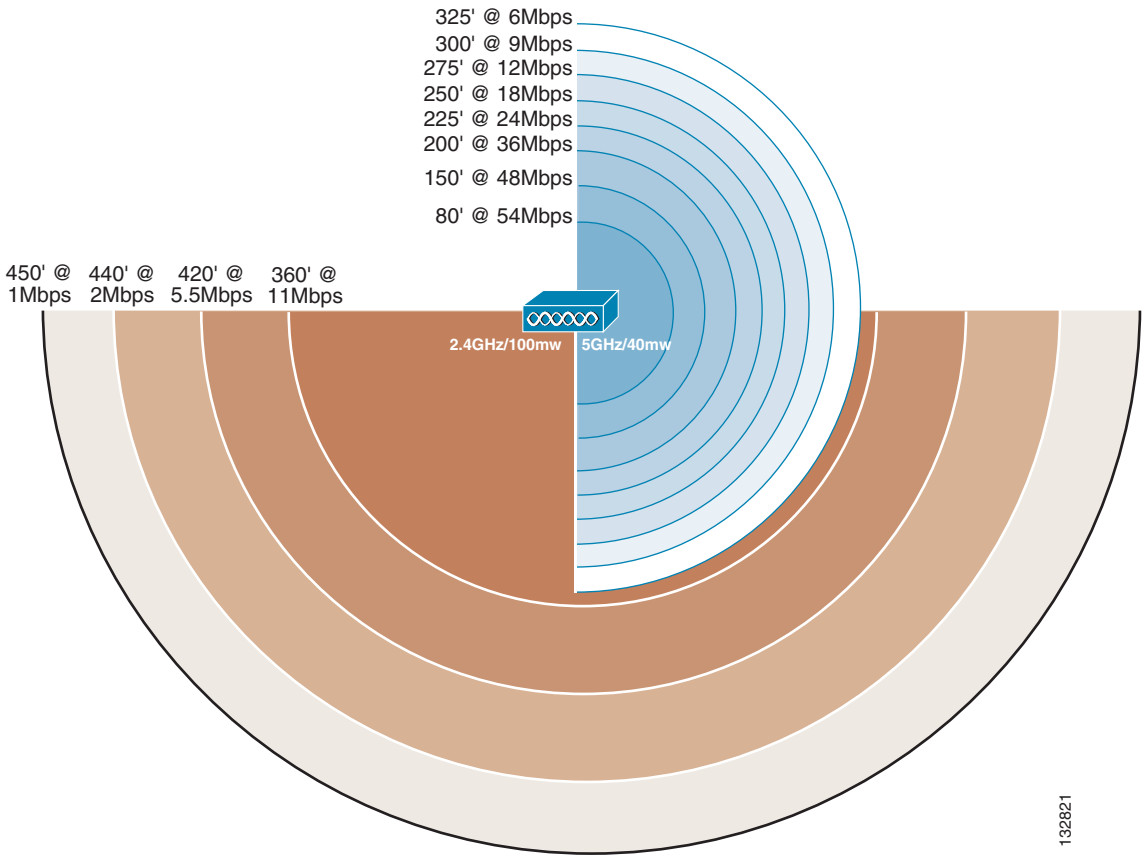
データ レートは AP のカバレッジ領域に影響を与えます。図 3-7 に示すように、データ レートが低い場合（1 Mbps など）は、データ レートが高い場合（54 Mbps など）よりも AP からのカバレッジ領域が広域になります（ただし、この図は正確な比率で描かれていません）。つまり、異なるデータ レートの 図 3-8 に示すように、データ レート（および電力レベル）はカバレッジとその結果として設置に必要な AP の数に影響します。計画プロセスの一部として、必要なデータ レート、必要な範囲、および必要な信頼性を考慮します。

カバレッジ領域に対するデータ レート

AP では、無線リンク上で異なる符号化技法を使用して異なるデータ レートを実現しており、データがノイズからより簡単に回復されるようになります。これは、さまざまなレシーバ感度でさまざまなデータ レートに対して確認されることです。1 Mbps のデータ レートでパケットに送信される記号またはチップの数は、11 Mbps で同じパケットに使用される記号の数を上回ります。これは、低いデータ レートでデータを送信する方が、高いビット レートで同じデータを送信するよりも時間がかかるということです。また、無線にアソシエートされているクライアントが複数ある場合は、同じ長さのパケットの送信により多くの時間がかかるため、データ レートが低いクライアントが、データ レートの高いクライアントの最大データ スループットに影響を与えます。

図 3-7 に示されているとおり、実際のカバレッジ直径は、環境、電力レベル、アンテナ ゲインなどの要因によって異なります。

図 3-7　カバレッジと比較したデータ レート

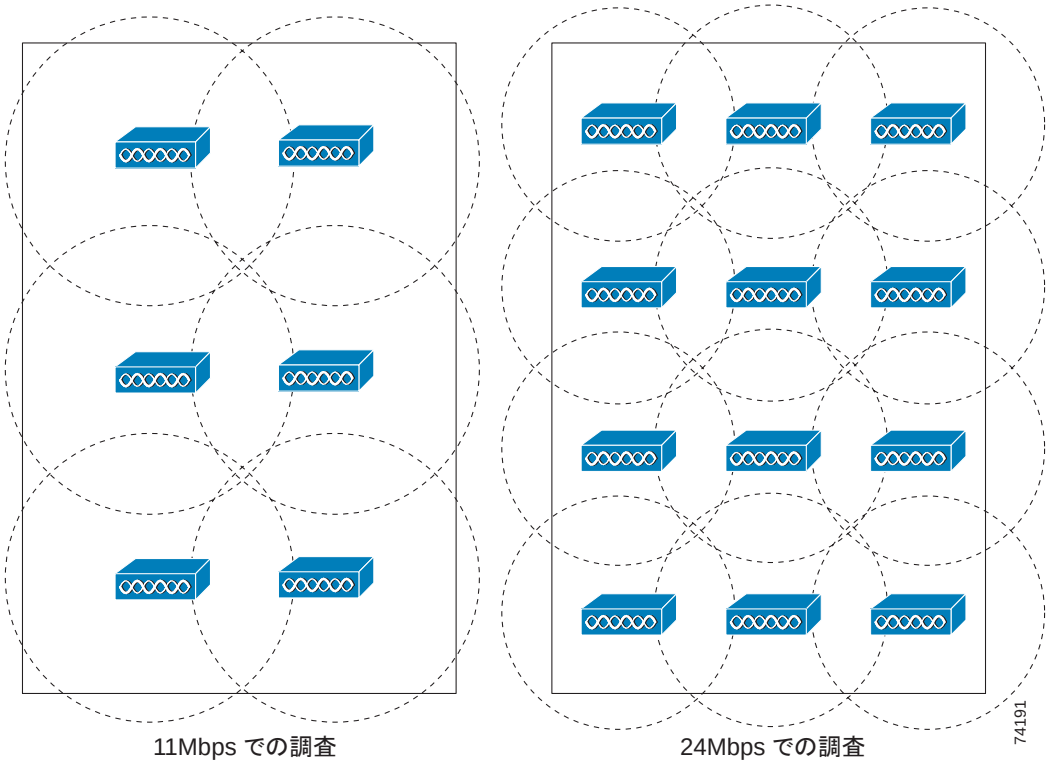


たとえば、屋内で NIC カード上の標準アンテナと AP を使用した場合、1 Mbps の円の直径は約 210 m（700 フィート）となり、11 Mbps の円の直径は約 60 m（200 フィート）となります。これは、屋内環境のタイプに左右されます。オープン プラン オフィスのビルディングは、オフィスが壁で仕切られているビルディングとは異なります。アンテナのゲインを上げると、距離が長くなり、放射が均等に行われるのではなく、特定方向に集中するように放射パターンの形状が変化します。

異なるデータ レートに対する AP の密度

最小限必要な信頼性のあるデータ レートは、電力設定、アンテナ ゲイン、および場所と共に、設計上必要となる AP の数に直接影響します。図 3-8 は、さまざまなデータ レートに対するカバレッジの比較と AP 密度を示しています。最小データ レートが 11 Mbps の 6 個の AP は、領域に対して適切にサービスを提供できますが、同じカバレッジ領域に対して 24 Mbps の最小データ レートをサポートするには、2 倍の数の AP が必要になり、48 Mbps の最小データ レートをサポートするにはさらに多くの AP が必要になります。

図 3-8　カバレッジの比較と異なるデータ レートに対する AP の密度



選択するデータ レートは、サポートされるアプリケーションの種類によって異なりますが、カバレッジとのトレードオフを考慮して、一般的な要件を上回らないようにする必要があります。一般的な WLAN 環境では、高いデータ レートは最大のスループットを提供し、パフォーマンスに関するサポートの問題を最小限に抑えます。通常は、物理的な機能や、ネットワークがクライアント集中型かどうかによって、範囲の要件が決まります。一部のクライアントは、高いデータ レート、広い範囲、または AP などのインフラストラクチャ要素の遅延やジッタ レートをサポートしていないことがあります。

AP およびクライアントのデフォルトの設定を選択することで、すべてのデータ レートに対応するのは、一見論理的に見えます。ただし、最大のカバレッジが得られる*最高*のレートにデータ レートを制限することには、主に 3 つの理由があります。

- ブロードキャストおよびマルチキャスト（有効な場合）は、アソシエートされている最も低いデータ レートで送信されます（すべてのクライアントがパケットを受信できるようにするため）。これにより、低いレートでフレームが処理されるまでトラフィックは待機しなければならないため、WLAN のスループットは低下します。
- 低いビット レートはサービスされていますが、距離が遠いために、低いデータ レートでネットワークにアクセスしているクライアントは、遅延を発生させることで、全体のスループットを低下させます。ネットワークの他の部分にパフォーマンスの影響を与えないように、クライアントを近くの AP に強制的に移動させることをお勧めします。
- たとえば、すべてのデータ レートをサポートするために 54 Mbps のサービスが AP で指定および提供されている場合、低レートのクライアントは、計画されているよりもカバレッジ領域の広い AP にアソシエートします。これにより、セキュリティ上の危険が増し（ビルディング外部からのアソシエーションが許可されるため）、他の WLAN への干渉を生じる可能性があります。

クライアント密度とスループット要件

無線 AP には、データ レートよりも実際のクライアント データ スループットを低下させる 2 つの特性があります。

- AP の集約スループットは、データ レートより少なくなります。これは、802.11 がすべてのパッケージを ACK する信頼性のある転送メカニズムを提供しており、結果としてチャネル上のスループットを半分にするからです。
- AP は共有ハブと類似しています。つまり、チャネルは、そのチャネル上の AP にアソシエートされているすべてのクライアントで共有されるため、衝突が発生してデータのスループットを低下させるのです。

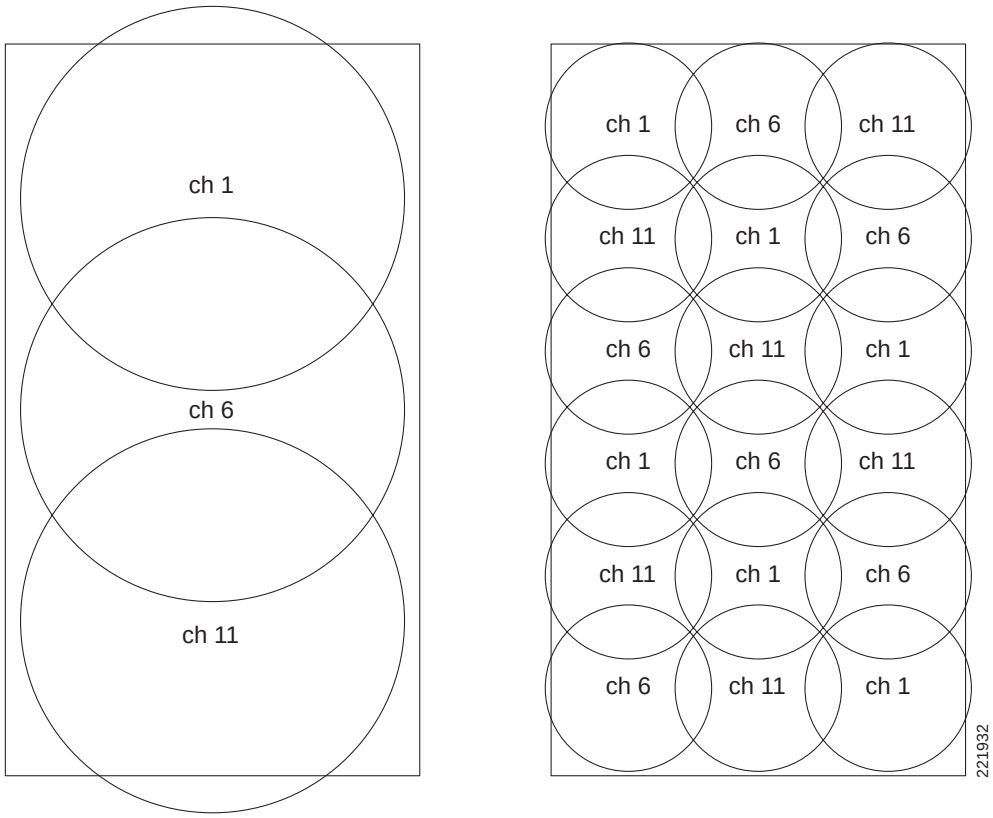
これを考慮して、アクティブなアソシエーション（アクティブ クライアント）の最大数を見積もる必要があります。これは、特定のアプリケーションに応じて若干調整できます。

各セルは、セル内にあり所定の AP にアソシエートされているすべてのクライアント デバイスによって共有される集約スループットを提供します。これは、基本的にセルをコリジョン ドメインとして定義します。最小データ レートを決定したら、無線 LAN の各ユーザに提供する必要がある平均スループットの量を考えます。

簡単なバーコード スキャナ アプリケーションの例を考えましょう。802.11b AP を 11 Mbps のデータ レートで使用すると、集約スループットが 5 ～ 6 Mbps になるため、このようなアプリケーションに対する帯域幅としては、25 Kbps もあれば十分です。簡単な割り算を行うと、理論上サポート可能なユーザの数は 200 となります。この数字は、多数のクライアントに関連する 802.11 の管理オーバーヘッドおよびパケットの衝突のため、実際には達成できません。1 Mbps のシステムでは、20 人のユーザが同じ AP を同様の帯域幅で使用できます。

1 つの AP で提供される集約スループットを利用するユーザの数を抑えることで、ユーザあたりの潜在的なスループットを増やすことができます。これは、カバレッジ領域のサイズを小さくするか、同じカバレッジ領域の重複しないチャネルに別の AP を追加することで実現します。カバレッジ領域を小さくするには、AP の電力またはアンテナ ゲインを減らすと、結果としてカバレッジ領域のクライアントが少なくなります。これは、同じ領域全体に対してより多くの AP が必要になり、展開コストが増加することを意味しています。この例を 図 3-9 に示します。

図 3-9　クライアント パフォーマンスを高めるために出力電力を変更



1 フロアあたり 180 ユーザ
トランスミッタの出力 30mW
アクセス ポイント 3 個
1 AP あたり 60 ユーザ
データ レート 11Mbps

1 フロアあたり 180 ユーザ
トランスミッタの出力 5mW
アクセス ポイント 18 個
1 AP あたり 10 ユーザ
データ レート 11Mbps

（注） AP の電力設定に合わせてクライアントの電力を調整する必要があります。クライアントの設定を高くしても、パフォーマンスの向上にはつながりません。また、近くのセルで干渉を発生させる可能性があります。

WLAN のカバレッジ要件

企業が異なれば、カバレッジ要件も異なります。WLAN に特別な共通領域をカバーする必要がある企業もあれば、WLAN にビルディングの各フロア、吹き抜けやエレベーターを含むビルディング全体、または駐車場や車道を含むキャンパス全体を含める必要がある企業もあります。カバレッジ要件は、必要な AP の数に影響するだけでなく、特殊アンテナ、屋外の筐体、避雷器などの他の要件を生み出すこともあります。

電力レベルとアンテナの選択

電力レベルおよびアンテナの選択は、AP の配置を決めるうえで、密接な関連しています。これらの 2 つの内容によって、環境内の所定の場所での RF の位置および電力の強さが決まります。必要なカバレッジ領域を生成する適切なアンテナを選択することに加え、電力レベルを制御し、最適なチャネルおよび電力計画を提供する RRM を使用することをお勧めします。詳細は、Radio Resource Management（Auto-RF）（P. 3-28）を参照してください。

アンテナは、無線システムに対して、以下の 3 つの基本的な特性を示します。

- ゲイン：アンテナが放射する電力の密度を、すべての方向に均等に RF エネルギーを放射する理論上のアンテナと比較して示すための尺度。
- 方向：アンテナ伝送パターンの形状。アンテナの種類によって、放射パターンも異なり、ゲインの方向や大きさも変わってきます。
- 偏向：電界の方向を示します。RF 信号は電界と磁界の両方を持ちます。電界が垂直である場合、電波は垂直に偏向されていると言えます。

アンテナによく似た例に、懐中電灯の反射器があります。反射器が光線を特定の方向に集め、強めるのは、無線システムの RF ソースに対して皿型のパラボラ アンテナが行っていることとよく似ています。

ゲインおよび方向によって、範囲、速度、および信頼性が決まります。偏向は信頼性とノイズの分離に影響します。

全方向性アンテナ

全方向性アンテナは、等方性アンテナと比較すると、放射パターンが異なっています。等方性アンテナは理論上のもので、物理的なアンテナはすべて等方性アンテナとは異なります。全方向性アンテナは、水平面では 360 度、垂直面では 75 度のほとんど対称的な放射パターンを持ちます（ダイポール アンテナが垂直に立てられていることを前提としています）。全方向性アンテナの放射パターンは、通常、ドーナツのような形をしています。

アンテナの種類（全方向性または方向性）は、特定の方向、パターン、および密度での RF エネルギーの大部分に集中化することで RF カバレッジに影響を与えるため、アンテナの選択に応じて、アンテナによって生成される RF パターンを考慮する必要があります。

たとえば、図 3-10 の全方向性アンテナは、垂直方向および水平方向に RF 放射パターンを示しています。これは、実際の測定結果であり、完全なドーナツ状にはなっていませんが、なぜドーナツ型と呼ばれるようになったかは、この結果からもわかります。先に説明したように、他の RF に影響する要素（部屋にいる人々、施設に格納されているデバイスの量、屋外展開の場合は木に生えている葉、他の RF ソースからの干渉など）が実際の RF カバレッジ パターンに影響を与えることがあります。

図 3-10　全方向性の RF パターン

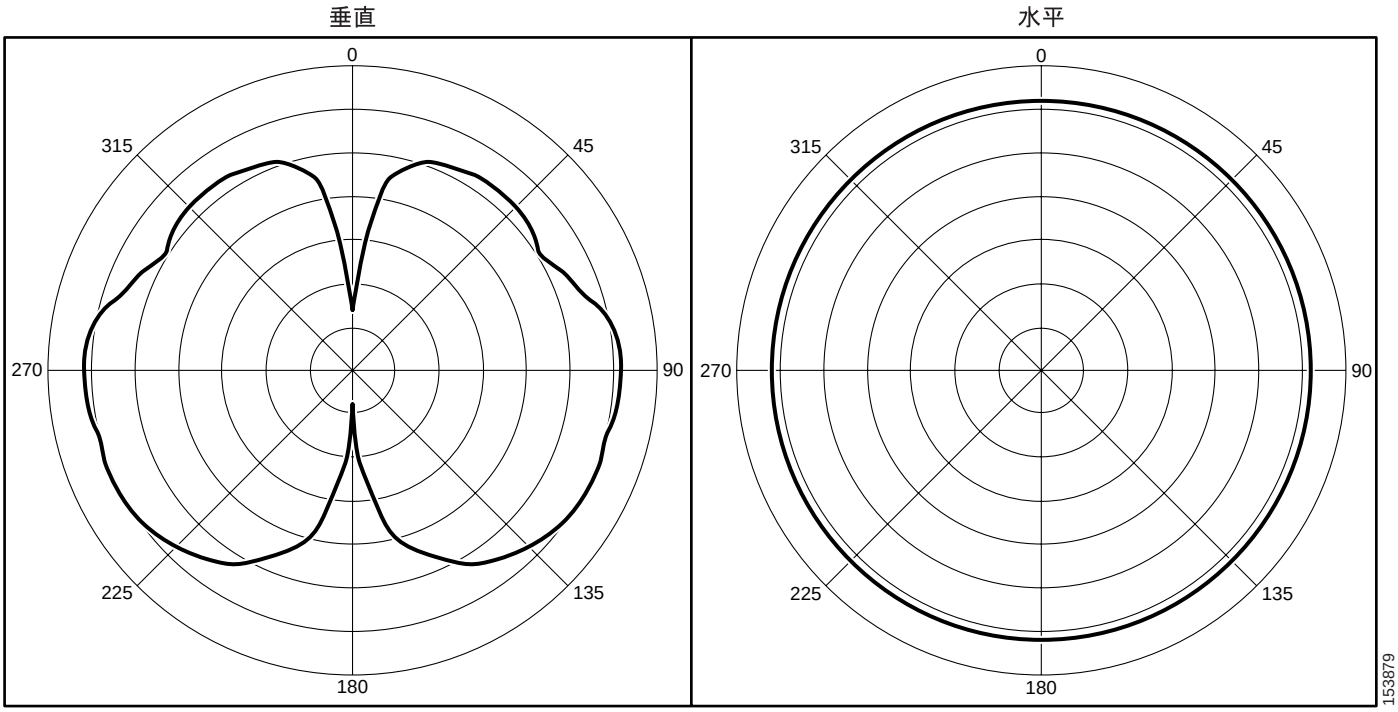
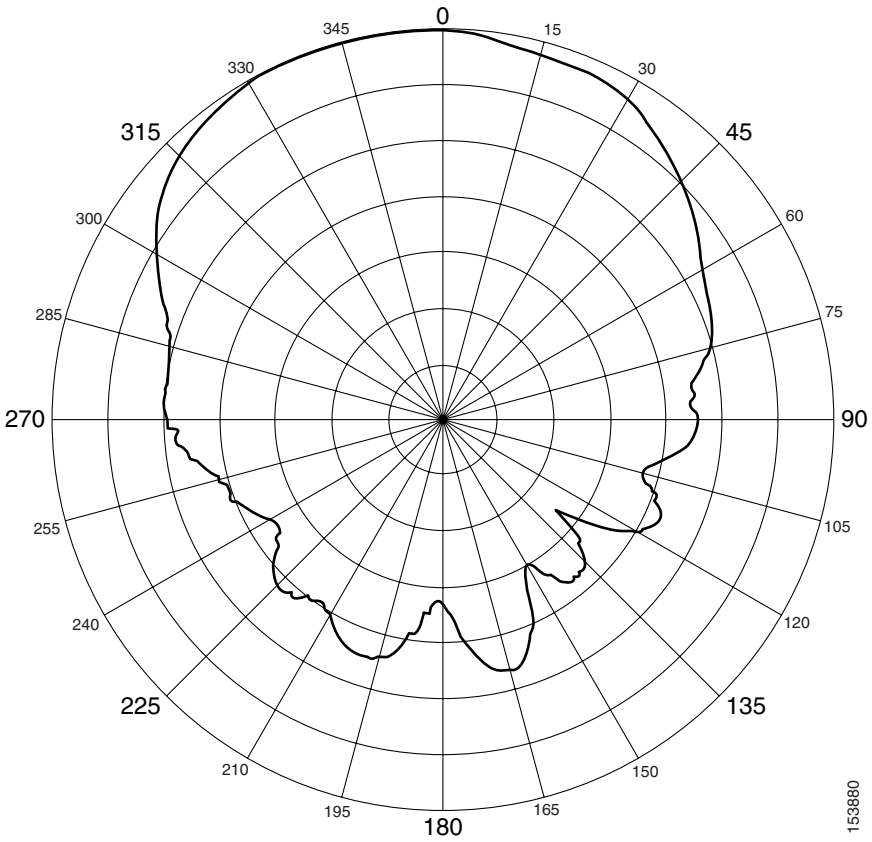


図 3-10 のパターンを見ると、特に、ビルディングの外部に向けて放射するパターンとなる外壁に取り付ける場合、これは壁面で使用するには不向きなアンテナである可能性があります。このアンテナは、無線ネットワークをビルディングの外部のハッカーに開放し、無線ネットワークを危険にさらすかもしれません。

パッチ アンテナ

パッチ アンテナは指向性アンテナの一種です。パッチ アンテナは、壁面またはアンテナが取り付けられた場所から外に向けて電波を放射するだけでなく、背面および側面に突出部もあり、これによって弱いながらも使用できる可能性のある RF 領域が生成されます。図 3-11 は、壁面取り付けダイバーシティ パッチ アンテナの実際の水平方向のパターンを示しています。カバレッジ領域の大部分は、パッチ アンテナの前面ですが、背面および側面の中央領域からの RF パターンに注意してください。アンテナによって放射パターンや無線接続できる場所が決まるため、アンテナの選択は重要です。

図 3-11　壁面取り付けパッチ アンテナの水平平面



アンテナの選択の詳細は、次の URL にある『Cisco Antenna Selection 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

セキュリティ ポリシー要件

良い RF 設計は、カバレッジが必要ない領域の意図しない RF 放射を効果的に最小限に抑えられます。たとえば、WLAN カバレッジがビルディング内部のみで必要であり、外部では不要の場合、電力を正しく設定し、AP を適切に配置し、ビルディングまたは領域の中心に向けて内側向きの指向性アンテナを正しく設置することで、ビルディング外部の RF カバレッジの量を最小化できます。RF 送信レベルを調整し、カバレッジ領域に適切なアンテナを使用することで、ビルディング外部に放射される RF の量を減らし、セキュリティの危険性を減少させることができます。このようにすることで、ビルディングまたはカバレッジ領域外のハッカーに対する無線ネットワークの露出を抑え、無線ネットワークの妥協を避けることができます。

RF 環境

WLAN およびその機器のパフォーマンスは、その RF 環境、機器、選択、カバレッジ設計、監査の質、設定、および展開の質によって異なります。以下は、チャネルに干渉し、なんらかの方法で信号の RF の特性を変え、無線通信を妨害する可能性がある、環境的なマイナス要因の一例です。

- 2.4 GHz のコードレス電話
- 金網と化粧しっくいで作られた壁
- ファイリング キャビネットおよび金属製の装置ラック
- 変圧器
- 高荷重の電動機
- 防火壁および防火扉
- コンクリート
- 冷蔵庫
- 硫黄プラズマ照明（Fusion 2.4 GHz 照明システム）
- 空調配管
- その他無線装置
- 電子レンジ
- HVAC 導管
- フォークリフトや金属製の組み立てなどの大規模な一時的要素
- その他の WLAN 機器

WLC は、チャネルおよび電力設定だけでなく、サイトの事前計画および RF の課題の初期調査に最適なリソースですが、多くの場合、上記の環境的要因をきっかけに、必要な領域すべてで必要なデータ レートがサポートされていることを確認するために、サイトサーベイが必要になります。

RF 展開とベスト プラクティス

いくつかの設計上の考慮事項は、一般的なベスト プラクティスに従うことで対処できます。以下は、ほとんどの状況に適用されます。

- ユーザの数と所定の AP のスループット。一般に推奨される AP あたりのユーザ数は、データだけのユーザの場合で 15 ～ 25 です。7920 VoIP（または同様の音声デバイス）無線端末の場合、データが存在するときの音声ユーザ数は 7 ～ 8 です。この数字は、あくまでも指針であり、使用する端末によって異なる可能性があります。端末の要件を確認してください。
- AP データ レートは、設計されたもの、およびサイトサーベイが実施されたものに限定する必要があります。低いデータ レートを有効にすると、同一チャネル干渉およびクライアントに対するスループットの変化が増す原因になることがあります。
- AP の数は、カバレッジおよびスループット要件に依存し、変化する可能性があります。たとえば、シスコ内部の Information Systems（IS）グループは現在、データ専用動作については、38,000 平方フィートのフロア空間あたり 6 個の AP を使用しています。

（注） 環境の変動性に基づき、必要な AP の数および最適な配置を決めるために、サイトの調査を実施することをお勧めします。

WLAN カバレッジの手動による微調整

次のように、さまざまな要素が WLAN カバレッジに影響します。

- チャネルおよびデータ レートの選択
- ロケーション管理、音声、またはデータ専用の重複する WLAN カバレッジ
- 電力レベル
- アンテナの選択（全方向性、または指向性アンテナ）

所定のデータ レートおよび場所に対して、WLAN 設計者がカバレッジ領域またはカバレッジ形状を変えるために、電力レベルを変更したり、別のアンテナの使用を決める可能性があります。電力レベルの変更やチャネルの選択は、次に示すように手動で行うことができます。また、Cisco Wireless Controller では Radio Resource Management（RRM）アルゴリズムにより、これを自動的に行えます。これは、Auto-RF とも呼ばれています。電力レベルおよびチャネルの管理には、Radio Resource Management（RRM）を使用することをお勧めします。チャネル変更アルゴリズムは、干渉源が非常に破壊的（かつ永続的）な場合にだけチャネル形状の変更が行われるように、極めて複雑であることを忘れないでください。変更した場合、クライアントの再アソシエートが必要になり、音声コールはドロップされます。AP 電力の変更はクライアントには影響しません（詳細は、Radio Resource Management（Auto-RF）（P. 3-28）を参照）。

チャネルおよびデータ レートの選択

チャネル選択は、特定の領域で許可されている周波数に依存します。たとえば、北アメリカおよび ETSI 2.4 GHz チャネル セットでは、1、6、および 11 の 3 つのオーバーラップしないチャネルの割り当てが許可されています。5 GHz チャネル セットでは、23 のチャネルが許可されています。

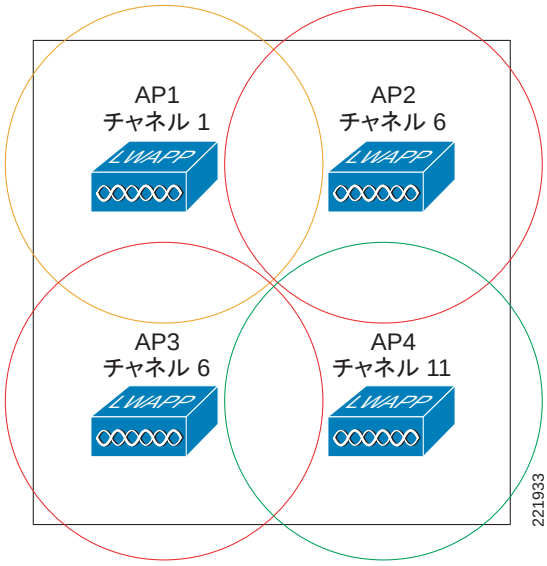
チャネルは、次のようにカバレッジ セルに割り当てる必要があります。

- オーバーラップしているセルは、オーバーラップしていないチャネルを使用する必要があります。
- 複数のセルでチャネルを再利用する必要がある場合、これらのセル間のオーバーラップが最小限になるようにする必要があります。図 3-12 はこのパターンを示しています。802.11a の展開では、セルがオーバーラップするので、チャネルの近接を避ける必要があります。

チャネルの選択に関する推奨事項

以下に示すように、チャネルの選択は手動で行うことができます。

図 3-12　AP に割り当てられたチャネル



実際の展開での使用を考えているものと同じ周波数でサイトサーベイを行う必要があります。サイトによってはノイズ バックグラウンドが高い場合があり、1 つまたは複数のチャネルを使用するうえで妨げとなることがあります。サイトサーベイにより、特定の場所にある特定のチャネルが干渉およびマルチパスに対してどのように反応するかをより正確に把握できます。チャネル選択は、チャネル相互および隣接チャネルの干渉を計画するうえで役立つほか、周波数を再利用できる場所に関する情報を提供します（図 3-13 を参照）。

高層ビルディングでは、フロア間のセルのオーバーラップを確認します。特に、窓がある場合は、その規則性に従って確認します。事例の約 10% では、慎重な事前計画と AP の場所の選択が必要になります。オフィス タワー、病院、大学の講堂ビルディングなどの高層構造では、カバレッジ計画を三次元で考えます。802.11b および 802.11g の 2.4 GHz の波形は多くの壁を通過します。802.11a の 5 GHz の波形では、周波数が高いため、所定の電力で適切なエネルギーの量を壁を通して送信する傾向は約半分になります。特に、2.4 GHz の Wi-Fi LAN では、カバレッジ モデルに隣接するフロアの窓をカバーするセルが含まれている場合は、同じフロアだけでなく、隣接するフロアでのセルのオーバーラップも回避する必要があります。チャネルが 3 つだけの場合は、これは、慎重な三次元での計画を行うことで達成できます。

最終ステップとして、WLAN ネットワークのセットアップ後、必ず選択したチャネルを使用してサイトを再テストし、干渉を確認します。RRM アルゴリズムは理論であり、ネットワークの物理トポロジによって異なることを念頭においてください。したがって、AP の配置を三次元的に考慮し、サンプリング間隔に対して最適なチャネル / 電力設定を行うようにします。

手動でのチャネル選択

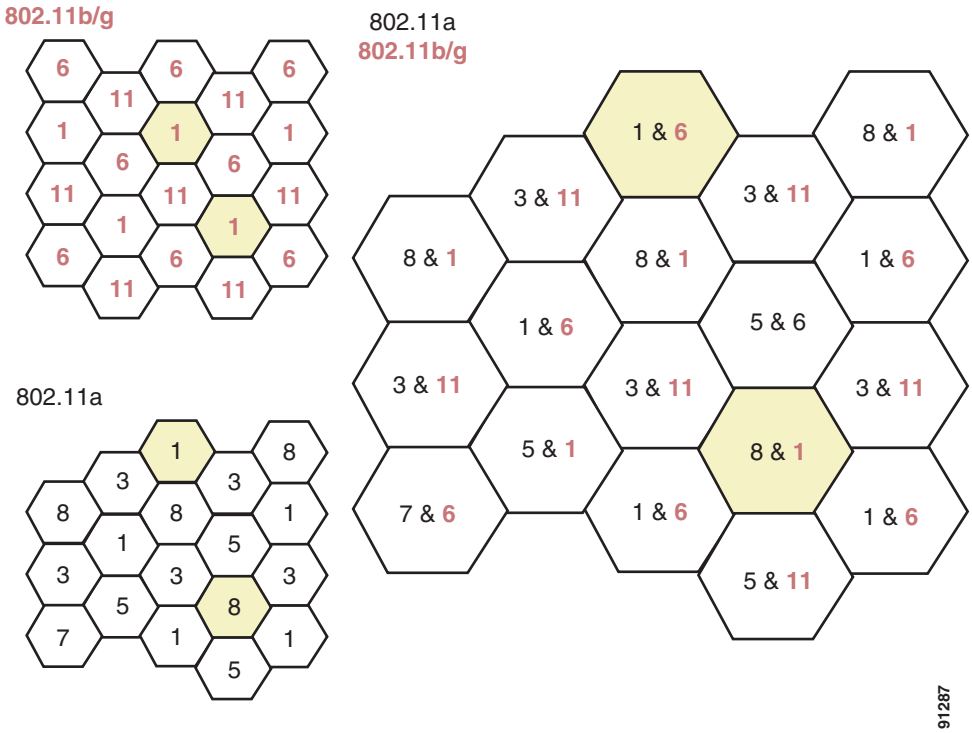
図 3-13 は、無線選択で、802.11b/g 無線の 1 つを設定するための Web ページのスクリーンショットです。右上では、チャネル 11 が手動で選択され、送信電力が最高レベルの 1 に設定されています（8 の場合、AP は最も低いレベルに設定）。

(注)　割り当て方法は、手動でこれらの設定を制御する必要がある場合を除いて、通常はグローバル設定のままにします。これにより、コントローラが RRM で決定されたとおり、動的にチャネル番号を変更できます。詳細は、Radio Resource Management（Auto-RF）（P. 3-28）を参照してください。

図 3-13　チャネルの割り当て

図 3-14 に示すように、デュアルバンド展開方式を実装することもできます。図の左上の部分は 802.11b/g だけの展開を示しています。この場合は、3 つのオーバーラップしないチャネル（チャネル 1、6、11）を使用して、相互チャネルの干渉が最小のパターンをマップしています。同じチャネル上にあり、別のアクセス ポイントのカバレッジ パターンとオーバーラップしながら十分な電力レベルで動作している、近くの AP からの干渉のことです。この図には、8 つのオーバーラップしないチャネルを使用した 802.11a 展開も示されています。図の右側は、デュアルバンド展開でチャネルをマップする方法を示しています。

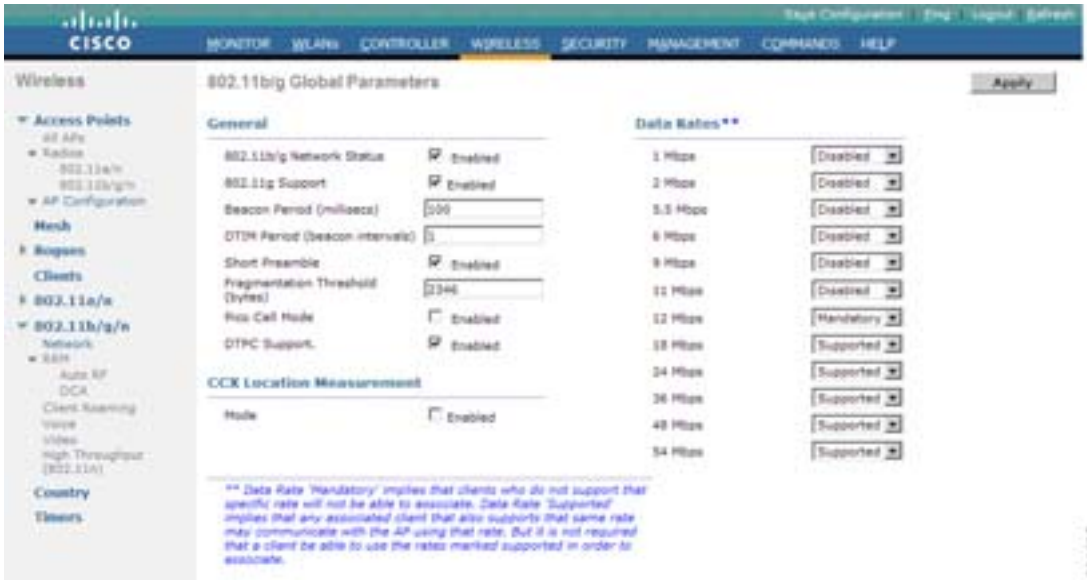
図 3-14　デュアル バンド展開の図



データ レートの選択

図 3-15 は、802.11b/g のグローバル パラメータの Web ページのスクリーンショットです。データ レートは画面の右側に示されています。

図 3-15　データ レートの割り当て



Mandatory、Supported、および Disabled のデータ レート

無線デバイスでのデータ伝送に使用するデータ レートを指定するには、データ レート設定を使用します。データ レート、範囲、および信頼性の間には、直接的な相関関係があります。データ レートが低いほど、所定の電力設定に対する信頼性が増し、範囲が増えます。サイトは仕様によって異なりますが、カーペットを敷いた空間についての妥当な経験則では、データ レートが半減すると信頼性のレベルは半比例して増加します。範囲は通常、データ レートが半減にするたびに約 30% 増加するという要素の影響を受けます。-67 dBm のエッジ内のカバレッジ領域の平方フィートの管理は、このテクニックを使用すると効率よく管理できます。クライアント、アプリケーション、またはユーザのニーズに合うようにデータ レートを設定することが、効果的な RF 設計要素となります。これは、AP の展開前に考慮する必要があります。

データ レートは 1 秒あたりのメガビット数で現します。各データ レートは次の 3 つのモードのいずれかに設定できます。

- Mandatory：このレートでの伝送を、ユニキャストとマルチキャストの両方を含むすべてのパケットに対して許可します。少なくとも 1 つの AP のデータ レートが Mandatory に設定され、この AP にアソシエートするすべてのクライアントが、ネットワークを使用するための無線でこのデータ レートを物理的にサポートできる必要があります。さらに、AP にアソシエートする無線クライアントについては、最も低い必須データ レートで現在パケットを受信でき、無線が最大の必須データ レートを物理的にサポートしている必要があります。複数のデータ レートが必須に設定されている場合は、マルチキャストおよびブロードキャスト フレームは、アソシエートされているすべてのクライアントで共通の最高の必須伝送レート（すべてのクライアントで最も低い必須受信レート）で送信されます。これにより、すべてのクライアントがブロードキャスト パケットを受信できます。最も低い必須レートは通常、1 Mb/s に設定されます。
- Supported：このレートでの伝送をユニキャスト パケットだけに許可します。AP はこのレートではユニキャスト パケットだけを送信します。マルチキャストおよびブロードキャスト パケットは、必須に設定されているデータ レートのいずれかで送信されます。無線クライアントは常に、最も高いデータ レートで送受信しようとします。無線クライアントは、ユニキャスト パケットを送受信するために、Supported または Mandatory に設定された最も高いデータ レートを AP とネゴシエートします。無線クライアント デバイスは、任意の必須レートまたはネゴシエートしたレートより低いレートでブロードキャストまたはマルチキャスト パケットを受信できます。
- Disabled：AP はこのレートではデータを送信しません。

最低または最高の必須レートの設定

AP にアソシエートされている複数のクライアントは、干渉、障害物、または AP からの距離に応じて、異なる伝送レートを使用できます。たとえば、802.11b クライアントが AP から離れた場所にあり、それが原因で 1Mb/s の速度でしか送受信できない場合、最低必須レートが（図 3-15 を参照）1 Mb/s に設定されているため、クライアントは AP にアソシエートできます。54Mb/s で AP にアソシエートしている別の 802.11g クライアントについては、すべてのクライアントが受信できる最高必須レートが 1 Mb/s であるため、AP はブロードキャストおよびマルチキャストを 1 Mb/s で送信します。最低必須レートが 5.5 Mb/s に設定された場合、802.11 クライアントは、最低必須レートでブロードキャスト パケットを受信できないため、AP にアソシエートできません。

図 3-15 では、最高必須レートが 11 Mb/s に設定されていることに注意してください。最高必須レートは、クライアントの無線が物理的に送信できる必要があるものを AP に示しています。これは、そのレートで実際にパケットを送受信するということではありません。無線が物理的にそのレートをサポートするということです。無線クライアントは、最低必須レートでパケットを受信できるだけで構いません。802.11b デバイスの無線は 11 Mb/s で物理的に送信できるため、802.11b デバイスは 図 3-15 に示されている AP にアソシエートできます。より高いデータ レート（18 Mb/s など）が必須に設定されている場合は、802.11g クライアントは AP にアソシエートできます。

OFDM レート（11 Mb/s より高いレート）を必須に設定すると、802.11b 接続は無効になります。これは、たとえば、802.11g データ レートを必須にしたり、802.11 レートを無効にすることで、すべてのクライアントの最小伝送レートを設定することで AP から 802.11b クライアントを排除できるようになります。このようなことが可能になるのは、同じ 1,500 バイトのパケットでも、より低いデータ レートでは送信に時間がかかるためです。したがって、AP にアソシエートされているすべての無線クライアントに有効なデータ レートも低くなります。

Radio Resource Management（Auto-RF）

Cisco WLAN の「スプリット MAC」アーキテクチャ（第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照）では、802.11 のデータと管理プロトコルの処理およびアクセス ポイントの機能は、Lightweight アクセス ポイントと集中化された WLAN コントローラの間で分散されています。具体的には、プローブ応答や MAC レイヤの暗号化など、時間依存型のアクティビティはアクセス ポイントで処理されます。システム規模での可視性が必要となるその他すべての機能は、コントローラに送信されます。

WLAN ネットワークのリアルタイム RF 管理には、システム全体の可視性が必要であり、コントローラ レベルに実装されています。コントローラは、RF ネットワーク グループ内の AP から転送される情報により、有効な RF チャネル / 電力計画に関する必要な情報を学習します。

（注） RF ネットワーク グループ（RF グループ）は、モビリティ グループと同じではありません。モビリティ グループは、ローミング イベントでクライアントが IP アドレスを変更する必要がないように、1 ～ 25 のコントローラのモビリティ ドメインを定義します。これは、クライアントにサービスする新しい AP を扱う「外部」コントローラに「アンカー」コントローラからクライアント データを転送するための Ethernet over IP トンネルを構築することで実現されます。

Radio Resource Management（RRM）は、Auto-RF とも呼ばれており、RF カバレッジ領域を管理するために、チャネル（動的なチャネル割り当て）および電力（動的な送信電力の管理）を調整できます。RPM により、AP の電力レベルが、近接する AP とのベースラインの信号強度が -65 dBm（設定可能）に保たれるように調整されます（Auto-RF 動作の概要（P. 3-29）を参照）。現在 AP が配置されているチャネルで、近くに干渉源があることが分かると、AP のチャネルを調整します。無線ネットワークの感度およびスループットが最適になるよう、継続的に RF カバレッジを最適化します。

（注） RRM により実行される送信電力の制御および動的な周波数管理は、802.11h で定義された UNII-2 帯域での動作で要求される TPC や DFS ではありません。

RRM は RF 環境が静的ではないことを理解します。RF に影響を与えるさまざまな要素（部屋にいる人々、施設に格納されているデバイスの量、屋外展開の場合は木に生えている葉、他の RF ソースからの干渉など）が変化すると、RF カバレッジが、これらの要素および変化に応じて調整されます。これらの要素は常に変化しているため、RF カバレッジを監視し、周期的に調整することが必要になります。

WLC ソフトウェア リリース 4.1.185 では、Radio Resource Management（Auto-RF）の機能が大幅に強化されました。変更点および操作の詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008072c759.shtml

Auto-RF 動作の概要

各コントローラは、RF ネットワーク グループ名を使用して設定されます（WLC Controller -> General メニューの RF Network Name）。各 RF グループ（Group Mode が有効の場合）で、コントローラはリーダーを選び、RF ドメインを形成します。リーダーの役割は、コントローラのグループからネットワーク全体のネイバー情報を収集し、システム全体の最適なマップのために、チャネル / 電力計算を行うことです。Group Mode が選択されていない場合は、コントローラは、LWAPP 経由で接続されている AP から集められたネイバー データだけに基づいて計算を行い、AP 間の信号を -70 dBm に最適化しようとします。

AP は Radio Resource Management（RRM）ネイバー パケットを定期的に、最大電力で送信します。これらのメッセージには、RF グループ 名、BSSID、およびタイム スタンプのハッシュであるフィールドが含まれています。AP は、この RF ネットワーク名で送信された RRM のネイバー パケットだけを受信します。

隣接 AP がネイバー メッセージを受信すると、AP はコントローラに転送する前にメッセージを検証します。AP がメッセージ ハッシュを検証し、同じ RF グループに属することを確認すると、パッケージはコントローラに送信されます。それ以外の場合は、AP はネイバー パケットをドロップします。AP は、LWAPP パケット ステータス フィールドを受信したネイバー パケットの SNR および RSSI にして、検証したメッセージをコントローラに転送します。

表 3-6 は、システム内のデバイスのさまざまな機能の概要を示しています。

（注） TPC は電力レベルの下方調整だけを実行します。カバレッジ ホールの検出と修正は、AP の電力レベルを上昇させます。

Auto-RF は、自動 RF アルゴリズムとは別に実行される不正の検出（チャネル スキャン）と混同しないようにする必要があります。AP はすべての国に固有のチャネルを周期的に監視することで（チャネル スキャン）、不正の検出を実行します。AP は他のチャネルをリッスンするため、最大で 60 ミリ秒の間「オフチャネル」になります。この間に収集されたパケット ヘッダーはコントローラに送信され、そこで不正なアクセス ポイント、Service Set Identifier（SSID; サービス セット ID）がブロードキャストかどうか、不正なクライアント、アドホック クライアント、および干渉しているアクセス ポイントを検出するための分析が行われます。

デフォルトでは、各アクセス ポイントがオフチャネルになるのはその時間の約 0.2% です。これは、すべてのアクセス ポイントに統計的に分散されるので、隣接する 2 つのアクセス ポイントが同時にスキャンを実行して、WLAN のパフォーマンスに悪影響を及ぼすことはありません。AP がクライアントから受信したパケットは、LWAPP ステータス フィールドと共にコントローラへ転送され、パケットの受信中に AP が受信したすべてのパケットの RSSI および Signal-to-Noise Ratio（SNR; 信号対雑音比）を含む無線情報がコントローラに提供します。

表 3-6　デバイスの機能

デバイス	機能
RF グループ リーダー	RF グループの WLC からデータを収集し、システム全体の TX Power Control（TPC）および Dynamic Channel Assignment（DCA）のために分析します。TPC は電力レベルの下方調整だけを行います。
ローカル WLC	データを収集し、カバレッジ ホールの検出と修正アルゴリズムを実行します。クライアントで必要な場合は、電力レベルの上方調整を行います。
Light-weight アクセス ポイント	• 設定された間隔で、すべてのチャネルに関するネイバー メッセージを最大電力で送信します。 • 受信したネイバー メッセージのネイバー ハッシュを検証します。 • 設定したチャネルのノイズ、干渉、および IDS/ 不正の検出をスキャンし、プロファイルに失敗した場合は警告します。

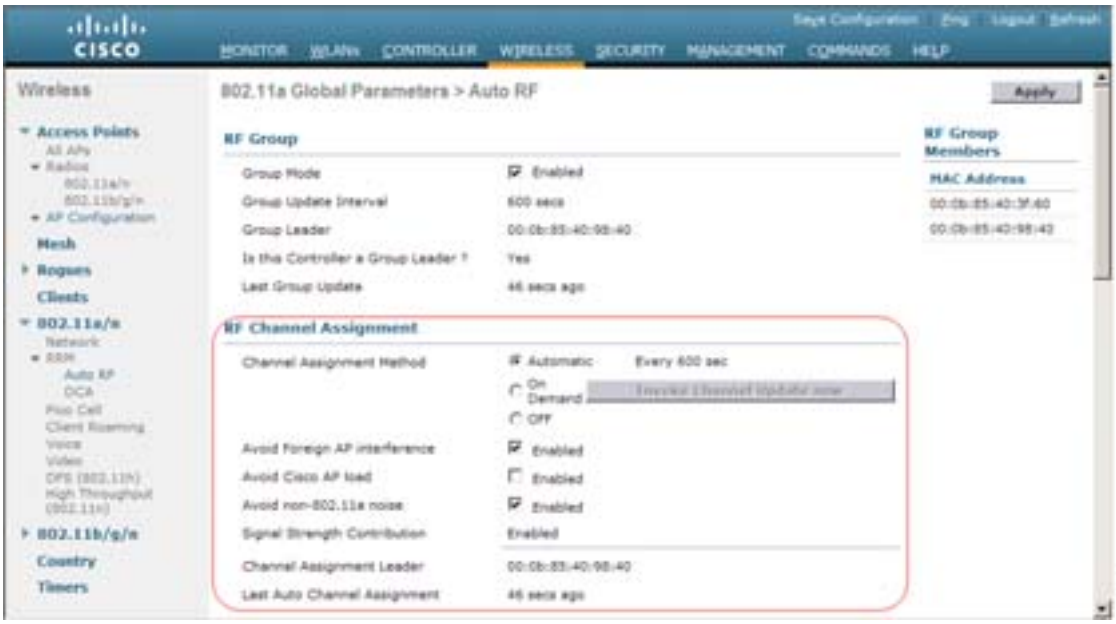
Auto-RF の変数および設定

Auto-RF は Channel Selection（**Wireless > 802.11b/g/n > Configure**）Web ページの Channel Selection のグローバル設定を使用して有効化または無効化することができます（図 3-13 を参照）。この Web ページでは、AP のチャネルおよび伝送レベルを手動で設定できます。さらに、グローバル Auto-RF Web ページから有効化または無効化できます。Auto-RF は帯域ごとに設定され、RF グループの計算は 802.11b/g の帯域と 802.11a の別の計算セットの両方に対して行われる点に注意してください。2 つの無線で同じ設定を共有する必要はありません。ただし、これらの設定はコントローラにアソシエートされているすべての AP に適用されます。Auto-RF の設定変数は、Auto-RF の設定ページのグローバル パラメータに表示されます（図 3-16 を参照）。

Auto-RF の設定 Web ページの最初の変数セットは、RF グループに対応しています。これらは、コントローラが他のコントローラとの動的なグループ化に加わるかどうかを決定します。動的なグループ化は、隣接していて、モビリティ グループの別のコントローラにアソシエートされている可能性がある AP をコントローラが把握する際に役立ちます。これが無効の場合、コントローラは、把握しているアクセス ポイント（つまり、アソシエートされている AP）のパラメータだけを最適化します。グループ リーダーは、選択されたリーダーの MAC アドレスを示します。コントローラの MAC アドレスは、Inventory Web ページ（上部のメニューで **Controller**、**Inventory** の順にクリックするとこの Web ページが表示されます）で見つけられます。

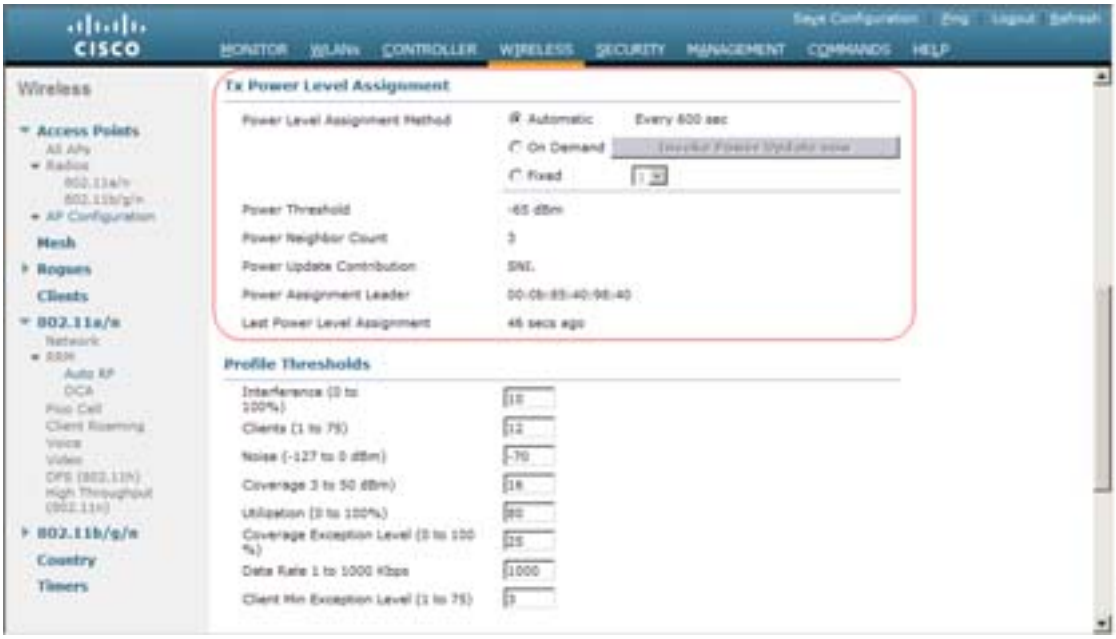
Auto-RF の設定 Web ページは、3 ページ（またはセクション）に分かれており、これらの 3 ページの間を移動するためのスクロール バーがあります。最初のページ（図 3-16 を参照）は、動的なチャネルの割り当てに関する設定です。AP が配置されているチャネルをコントローラで自動的に変更できるようにします（詳細は、チャネルの動的割り当て（P. 3-34）を参照）。

図 3-16　Auto-RF（1 ページ目）



RF チャネルの割り当ての次は、送信（TX）電力レベルを割り当てるセクションです（図 3-17 を参照）。この Web ページでは、すべての AP の電力レベルを修正したり、自動調整したりできます。また、この Web ページには、AP のネイバーの数と、調整している電力のしきい値も示されます。

図 3-17　Auto-RF（2 ページ目）



3 つ目の Web ページはプロファイルのしきい値の設定です。

図 3-18　Auto-RF（3 ページ目）

WLC は、AP から渡された情報を分析し、これらのしきい値それぞれについて、パスまたは失敗のステータスを決定します。これらのパス / 失敗のプロファイルは、**show ap auto-rf** *radio ap_name* コマンドの出力によく見られます（次の例を参照）。**Monitor > 802.11b/g Radios > Detail** Web ページでは、同じ情報をグラフ形式で見ることもできます。

サンプルの show ap auto-rf コマンドの出力

```
show>ap auto-rf 802.11b <access point name>
Number of Slots . . . . . . . . . . . . . . . . . . . . . . 2
AP Name . . . . . . . . . . . . . . . . . . . . . . . . . . <AP name>
MAC Address . . . . . . . . . . . . . . . . . . . . . . . . 00:0b:85:1b:df:c0
Radio Type . . . . . . . . . . . . . . . . . . . . . . . . . RADIO_TYPE_80211b/g
Noise Information
    Noise Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -93 dBm
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -90 dBm
 .
 .
 .
    Channel 11 . . . . . . . . . . . . . . . . . . . . . . -95 dBm
Interference Information
    Interference Profile . . . . . . . . . . . . . . . . . FAILED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -69 dBm @ 31 % busy
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -58 dBm @ 26 % busy
 .
 .
 .
    Channel 11. . . . . . . . . . . . . . . . . . . . . . -68 dBm @ 26 % busy
Load Information
    Load Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Receive Utilization . . . . . . . . . . . . . . . . . 0 %
    Transmit Utilization . . . . . . . . . . . . . . . . . 0 %
    Channel Utilization . . . . . . . . . . . . . . . . . 26 %
    Attached Clients . . . . . . . . . . . . . . . . . . .  2 clients
Coverage Information
    Coverage Profile . . . . . . . . . . . . . . . . . . .. PASSED
    Failed Clients . . . . . . . . . . . . . . . . . . . . 0 clients
Client Signal Strengths
    RSSI -100 dBm. . . . . . . . . . . . . . . . . . . . . 0 clients
    RSSI -92 dBm . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    RSSI -52 dBm . . . . . . . . . . . . . . . . . . . . . 1 clients
Client Signal To Noise Ratios
    SNR 0 dBm . . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 5 dBm . . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 10 dBm . . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    SNR 45 dBm . . . . . . . . . . . . . . . . . . . . . . 1 clients
Nearby APs
Radar Information
Channel Assignment Information
    Current Channel Average Energy . . . . . . . . . . . . -68 dBm
    Previous Channel Average Energy . . . . . . . . . . . . -51 dBm
    Channel Change Count . . . . . . . . . . . . . . . . . 21
    Last Channel Change Time . . . . . . . . . . . . . . . Thu Mar 9 12:18:03 2006
    Recommend Best Channel . . . . . . . . . . . . . . . . 11
RF Parameter Recommendations
    Power Level . . . . . . . . . . . . . . . . . . . . . 1
    RTS/CTS Threshold . . . . . . . . . . . . . . . . . . 2347
    Fragmentation Threshold . . . . . . . . . . . . . . . 2346
    Antenna Pattern . . . . . . . . . . . . . . . . . . . 0
```

次の項では、Auto-RF 変数の一部について説明します。

チャネルの動的割り当て

802.11 MAC レイヤでは、Carrier-Sense Multiple Access/Collision Avoidance（CSMA/CA）が使用されます。CSMA/CA では、同じ圏内の同じチャネル上の 2 つの AP は、無線チャネルを共有するため、異なるチャネルにある 2 つの AP と比較してキャパシティが約半分になります。これは、802.11 MAC では、チャネルがビジー状態であることが検知され、このチャネルが解放されるまで、フレームの送信が延期されることによるものです。802.11 MAC により、そのチャネル自体の AP セルの一部ではないトラフィックの伝送が延期させられた場合は、干渉とみなされます。同一チャネルの別の AP からの干渉は、通常、同一チャネル干渉と呼ばれ、大半の 2.4 GHz 802.11 の展開で発生します。これは、オーバーラップしないチャネルが少ないため、一部のチャネルのオーバーラップが発生するのを避けることができないからです。設計、計画、および動的な無線管理の目標の 1 つに、同一チャネル オーバーラップを最小限に抑えるということがあります。これにより、同一チャネル干渉が最小になり、AP トラフィックの容量が最大にされます。Cisco Unified Wireless Network では、AP のチャネルを動的に割り当てて、競合を避けることで、この問題および他の同一チャネル干渉の問題に対処します。WLC、つまり指定された WLC（RF グループ リーダー）は、システム全体を認識できるため、チャネルの「再利用」方法を制御し、同一チャネル干渉を最小限に抑えることができます。

WLC は、さまざまなリアルタイムの RF 特性を検証して、以下のようにチャネルの割り当てを効率的に処理します。

- ノイズ：ノイズにより、クライアントや AP の信号品質が制限されます。また、ノイズの範囲や周期は、さまざまです。干渉の種類、および干渉が及ぼす影響は、さまざまです。ノイズが増加すると、有効なセルのサイズが減少します。WLC は、定期的に、AP の RF 環境を再評価し、チャネルの選択を最適化して、システム全体の容量を維持しつつノイズの原因を回避します。過剰なノイズのためにチャネルが使用できなくなることは避けられます。また、他の無線ネットワークがある場合、WLC は、他のネットワークを補完するために、使用するチャネルを切り替えます。たとえば、チャネル 6 に 1 つのネットワークがある場合、近接する WLAN はチャネル 1 または 11 に割り当てられます。これによって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルが使用中で、使用可能なキャパシティがない場合、WLC はこのチャネルを回避することがあります。
- クライアントの負荷：チャネル構造を変更する際には、クライアントの負荷を考慮して、現在 WLAN システムに存在するクライアントへの影響を最小限に抑えるようにします。WLC は、チャネルを最適に割り当てるため、周期的にチャネルの割り当てを監視します。ネットワークのパフォーマンスが大幅に向上する場合や、パフォーマンスが低い AP でパフォーマンスを向上させる場合にだけ、チャネルが変更されます。

WLC は、RF 特性情報を総合して、システム全体のチャネルの割り当てを決定します。最終的には、3 次元空間における最適なチャネル設定が実現します。この場合、全体的な WLAN の設定で、上下のフロアにある AP が考慮されます。

干渉の検出と回避

Cisco Unified Wireless の展開における *干渉*とは、Cisco WLAN システム以外の 802.11 トラフィック（たとえば、不正な AP や近接する WLAN などのトラフィック）のことです。こうした干渉は、特定の電子レンジや各種コードレス電話などの 802.11 に準拠していない製品が原因となることもあります。また、場合によっては、アーク溶接や連邦 / 軍事レーダー施設などのさまざまな原因によって Electromagnetic Interference（EMI; 電磁干渉）が発生することもあります。AP は、常にすべてのチャネルをスキャンして干渉の主な原因を調べます。

802.11 の干渉の量が、事前に定義されたしきい値に達すると、WLC は、チャネルを再割り当てして干渉が存在するシステムのパフォーマンスを最適化しようと試みます。その場合、近接する AP が同じチャネルに存在する結果となることがありますが、干渉源となる AP があるためにまったく使用できないようなチャネルに存在するよりは、論理的には優れたシナリオです。

たとえば、WLC は、近接する AP をチャネル 1 またはチャネル 6 に切り替えることで、チャネル 11 上の不正な AP に応答できます。

送信電力の動的制御

カバレッジ領域を維持するためには、AP の電力レベルを適切に保つことが不可欠です。これは、領域をカバーする電力量が（最大ではなく）正確であるようにするためだけでなく、電力の過剰使用により放射領域に対する不要な干渉が発生するのを防ぐためでもあります。また、AP の電力設定は、AP の損失が発生した場合に、リアルタイムでフェールオーバーされるように、ネットワークの冗長性を制御するためにも使用されます。WLC は、リアルタイムの WLAN の状態に基づいて AP の送信電力レベルを動的に制御するために使用されます。通常は、電力を必要最小限に抑えることでキャパシティを増やし、AP 間の干渉を減らすことができます。RRM は、近接する AP を -65 dBm で認識できるように AP のバランスを保とうとします。AP の停止が検知されると、その周囲の AP の電力が自動的に増加し、AP が使用不可能になったことで生じたカバレッジのギャップが埋められます。

RRM アルゴリズムは、ユーザ エクスペリエンスが最適になるように設計されています。たとえば、AP の電力がレベル 4（レベル 1 が最大でレベル 8 が最低）まで下がり、あるユーザの Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）の値が許容しきい値を下回った場合、そのクライアントに対して最適なエクスペリエンスを提供できるように、AP の電力が増やされます。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）が有効になっている場合、アクセス ポイントによりチャネルが追加され、ビーコンに電力情報が送信されます。DTPC を使用しているクライアント デバイスは、この情報を受信して、自動的に設定を調整します。

カバレッジ ホールの検出と修正

カバレッジ ホールの検出および修正アルゴリズムは、クライアントの信号レベルの品質に基づいて、カバレッジ ホールを特定し、それらのクライアントがアソシエートされている AP の送信電力を増加させることを目的としています。

このアルゴリズムでは、クライアントの SNR レベルが指定された SNR しきい値を下回ったときに、カバレッジ ホールが存在するかどうかを確認します。SNR しきい値は、AP ごとに、主にそれぞれの AP の送信電力に基づいて決定されます。

1 つのクライアントの平均 SNR が、少なくとも 60 秒間しきい値を下回った場合は、WLAN クライアントがローミングできるロケーションがないことを示しているとみなされます。そのようなクライアントに対しては、AP の送信電力が増大され、カバレッジ ホールが修正されます。

クライアントとネットワークのロード バランシング

IEEE 802.11 の規格では、クライアントがどのようなプロセスでどのような場合にローミングするかが定義されていないため、特定の状況におけるクライアントの動作を簡単に予測することはできません。たとえば、会議室のすべてのユーザが、空き容量は大量にあっても離れた場所にある複数の AP ではなく、近接した 1 つのアクセス ポイントにアソシエートされることがあります。

WLC では、すべての AP にクライアントがどのように分散されているかを示す、集中化されたビューが提供されます。これは、複数の「良好な」AP が使用可能な場合に、新しいクライアントをネットワークのどこに接続するかを決定する際に使用されます。設定されている場合、WLC は、AP プローブ応答を活発に使用してクライアントを最適な AP に導き、WLAN のパフォーマンスを向上させることができます。その結果、無線ネットワーク全体にキャパシティが均等に分散されます。このロード バランシングは、クライアントの接続中ではなく、クライアントのアソシエーションで行われることを忘れないようにしてください。

CHAPTER 4

Cisco Unified Wireless Network アーキテクチャ ー 基本的なセキュリティ機能

Cisco Unified Wireless Network ソリューションは 802.11 のセキュリティ機能を基に設計されており、RF、802.11、およびネットワークベースのセキュリティ機能を強化することで全体的なセキュリティ強化を図っています。802.11 規格には無線媒体のセキュリティが盛り込まれていますが、さらに、Cisco Unified Wireless Network ソリューションではシステム全体のエンドツーエンド セキュリティを実現するため、アーキテクチャと製品のセキュリティ機能を利用し、WLAN エンドポイント、WLAN インフラストラクチャ、クライアント通信、基幹有線ネットワークを保護します。

802.11 の基本的なセキュリティ機能

ここでは、802.11 無線ネットワークで現在使用できる企業向けセキュリティ機能について説明します。

当初の 802.11 プロトコルは脆弱なセキュリティが問題視されていました。データ漏洩に関するこうした問題を解消するため、その後新しく登場したのが 802.11i 規格です。この規格では、強力な認証方式と暗号化方式を採用することで無線通信の機密性要件を実現しています。

このガイドの後半では、WLAN のその他のセキュリティ問題を取り上げます。現在、各標準化機関がこれらの問題の改善に努めています。また、Cisco Unified Wireless Network ソリューションにも対応策が取り入れられています。

WLAN のセキュリティの実装基準

WLAN ネットワークでは、認証と暗号化の両方がセキュリティの基準となります。WLAN ネットワークの一般的なセキュリティ メカニズムは次のとおりです。

- オープン認証、暗号化なし
- Wired Equivalent Privacy（WEP）
- Cisco WEP Extensions（Cisco Key Integrity Protocol + Cisco Message Integrity Check）
- Wi-Fi Protected Access（WPA）
- Wi-Fi Protected Access 2（WPA 2）

WPA と WPA 2 は、「Wi-F」ブランドを考案した国際的な Wi-Fi 団体である Wi-Fi Alliance によって定義されています。Wi-Fi Alliance は、IEEE 802.11 製品の相互運用性を認定し、これらが無線 LAN の国際的な標準規格となるようあらゆる市場を通じて普及活動を行っています。Wi-Fi Alliance では、他の Wi-Fi 認定製品との相互運用性を認定するための、メンバ製品のテスト方法を定義するテスト スイートを用意しています。

802.11 セキュリティ メカニズムとして最初に定義された WEP は、静的な暗号化方式を使用して無線ネットワークを保護していました。WEP は、ある程度のセキュリティ レベルには適合しますが、企業の通信を保護するには不十分と考えられています。簡単に説明すると、802.11 の WEP 規格は、暗号キーの管理方法の問題に対応していませんでした。暗号化メカニズム自体に、クライアント トラフィックを監視するだけで WEP キーを解読できてしまうという欠点が確認されたのです。Cisco WLAN 製品は、802.1x 認証と動的キー生成を採用し、WEP 暗号化をさらに強化した Cisco Key Integrity Protocol（CKIP）と Cisco Message Integrity Check（CMIC）を導入することで、これらの問題に対応しています。802.11i は、従来の 802.11 規格に存在するセキュリティの脆弱性に対処すべく、IEEE によって導入された規格です。最初の 802.11 規格以降 802.11i が承認されるまでの期間は、いくつかの暫定的なソリューションが採用されてきました。

WPA は、Wi-Fi Alliance が発表した 802.11i ベースのセキュリティ ソリューションで、WEP の脆弱性に対応しています。WPA は、Temporal Key Integrity Protocol（TKIP）を使用して、事前共有キーまたは RADIUS/802.1x ベースの認証を用いた暗号化および動的暗号キーの生成を行います。WPA に採用されたメカニズムは、ハードウェアをアップグレードしなくても WEP ソリューションの欠点に対処できるように設計されています。WPA2 は、次世代の Wi-Fi セキュリティであり、802.11i 規格をベースとしています。WPA2 は、Wi-Fi Alliance が認定する、承認済み IEEE 802.11i 規格の相互運用可能な実装方式です。WPA 2 には、「エンタープライズ」と「パーソナル」の 2 種類の認定があります。エンタープライズ モードでは、RADIUS/802.1x ベースの認証と事前共有キーのサポートが条件となります。パーソナル モードで必要となるのは、クライアントと AP が共有する共通キーだけです。WPA2 には AES という新しい暗号化メカニズムが導入されているので、通常は WLAN クライアントと AP を最新バージョンのハードウェアへアップグレードする必要がありますが、Cisco LWAPP AP はいずれも WPA2 に対応しています。

表 4-1 は、各種の仕様の概要です。

表 4-1　WLAN のセキュリティ機能

機能	静的 WEP	802.1x WEP	WPA	WPA2（エンタープライズ）
識別	ユーザ、マシン、または WLAN カード	ユーザまたはマシン	ユーザまたはマシン	ユーザまたはマシン
認証	共有キー	EAP	EAP または事前共有キー	EAP または事前共有キー
整合性	32 ビット Integrity Check Value（ICV）	32 ビット ICV	64 ビット Message Integrity Code（MIC）	CRT/CBC-MAC（Counter mode Cipher Block Chaining Auth Code; CCM）AES の一部
暗号化	静的キー	セッションキー	TKIP を使用した Per Packet Key ローテーション	CCMP（AES）
キーの配布	1 回限り、手動	Pair-wise Master Key（PMK）のセグメント	PMK から導出	PMK から導出
初期ベクトル（IV）	プレーン テキスト、24 ビット	プレーン テキスト、24 ビット	拡張初期化ベクトル（IV）― 65 ビット（抽出 / シーケンス）	48 ビットのパケット番号（PN）
アルゴリズム	RC4	RC4	RC4	AES
キーの長さ	64/128 ビット	64/128 ビット	128 ビット	128 ビット
サポートしているインフラストラクチャ	なし	RADIUS	RADIUS	RADIUS

Cisco Wireless Security Suite は、必須の、または既存の認証、プライバシーおよびクライアント インフラストラクチャに基づいて、さまざまなセキュリティ手段を提供するオプションを備えています。Cisco Wireless Security Suite は、WPA および WPA2 をサポートし、次の機能を提供します。

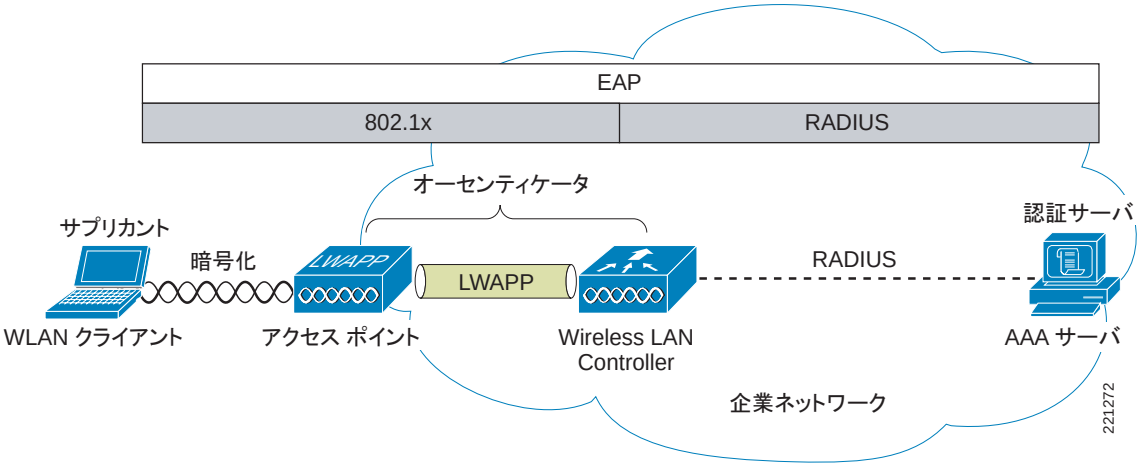
- 次の EAP 方式を使用する 802.1x ベースの認証：
  - Cisco LEAP、EAP-Flexible Authentication via Secure Tunneling（EAP-FAST）
  - PEAP-Generic Token Card（PEAP-GTC）
  - PEAP-Microsoft Challenge Authentication Protocol Version 2（PEAP-MSCHAPv2）
  - EAP-Transport Layer Security（EAP-TLS）
  - EAP-Subscriber Identity Module（EAP-SIM）
- 暗号化：
  - AES-CCMP 暗号化（WPA2）
  - TKIP 暗号化拡張機能：WPA TKIP Cisco Key Integrity Protocol（CKIP）および Cisco Message Integrity Check（CMIC）を使用した、キー ハッシュ（パケット単位での暗号キーの生成）、Message Integrity Check（MIC; メッセージ整合性チェック）、およびブロードキャスト キー ローテーション
  - 40 ビット、104 ビット、および 128 ビットの静的および動的 IEEE 802.11 WEP キーのサポート

（注） 128 ビットの WEP をサポートしている AP およびクライアントはありません（128 ビット WEP キーに IV が追加されるので、合計キー サイズは 152 ビットになります）。サポートされていたとしても、WEP キーが長くなることによって WEP 特有のセキュリティ問題は解消されません。

用語

このガイドで使用されている一般的な用語を図 4-1 に示します。

図 4-1　安全な無線トポロジ



このソリューションの基本的な物理構成要素は次のとおりです。

- WLAN クライアント
- アクセス ポイント（AP）
- Wireless LAN Controller（WLC）
- AAA サーバ

さらに図 4-1 は、802.1X 認証プロセスで使用する基本的な役割とそれらの関係を示しています。

- 802.1X サプリカント（無線ソフトウェア）は WLAN クライアント上に配置されます。
- AP と WLC（LWAPP スプリット MAC アーキテクチャを使用）は 802.1X オーセンティケータとして動作します。
- AAA サーバは認証サーバです。

図 4-1 は、クライアントと認証サーバ間で EAP パケットを伝送する際の 802.1X および RADIUS プロトコルの役割も示しています。802.1X と EAP については、この章の後半で詳しく説明します。

802.1X

802.1X はポート単位でアクセスを制御するための IEEE 規格です。認証されたユーザにのみ WLAN ネットワークへのアクセスを許可する手段として、802.11i セキュリティ ワークグループによって採用されました。

- 802.11 アソシエーション プロセスでは、各 WLAN クライアントの「仮想」ポートが AP に作成されます。
- AP は、802.1X ベース トラフィック以外のすべてのデータ フレームをブロックします。
- 802.1X フレームは EAP 認証パケットを伝送します。この認証パケットは、AP によって AAA サーバへ渡されます。
- EAP 認証に成功すると、AAA サーバは EAP 成功メッセージを AP へ送信します。このメッセージを受け取った AP は、該当する WLAN クライアントから仮想ポートへのデータ トラフィックを許可します。
- 仮想ポートを開く前に、認証された WLAN クライアントと AP 間のデータ リンクが暗号化されます。これは、特定のクライアントのために開いたポートへ他の WLAN クライアントがアクセスできないようにするためです。

Extensible Authentication Protocol

Extensible Authentication Protocol（EAP）は、認証プロトコルとそれを伝送するトランスポート プロトコルとの分離を定めている IETF RFC です。これらを分離することにより、EAP プロトコル自体を変更しなくても、802.1X、UDP、RADIUS などのトランスポート プロトコルを使用してこの認証プロトコルを伝送できます。

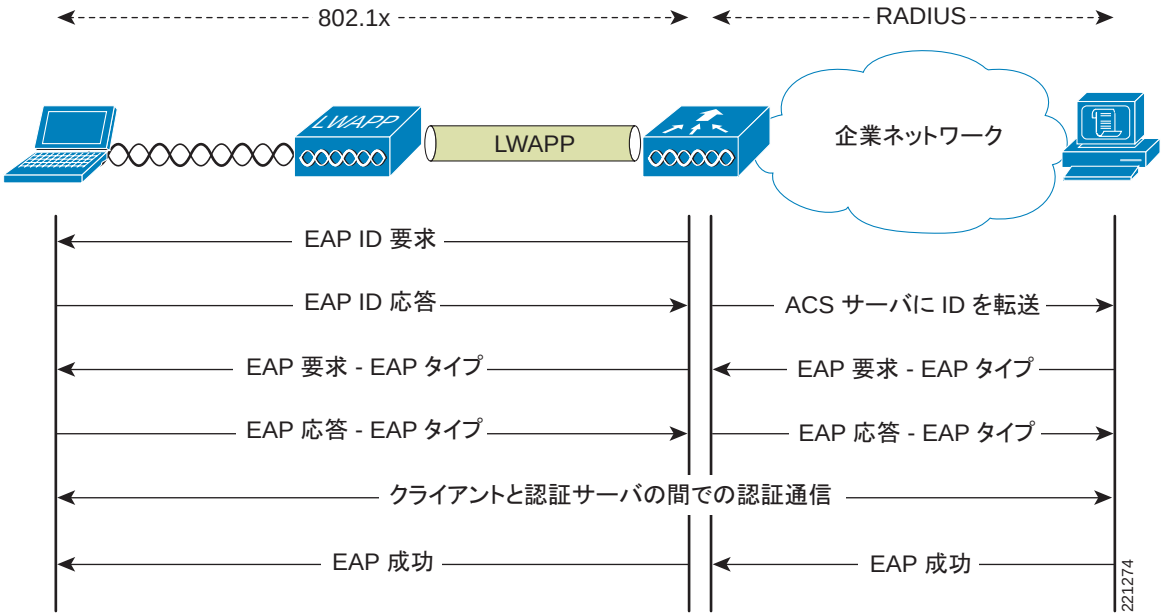
基本的な EAP プロトコルは比較的シンプルであり、次の 4 種類のパケットで構成されます。

- EAP 要求：要求パケットはオーセンティケータからサプリカントへ送信されます。要求パケットにはそれぞれ、要求内容（サプリカントの ID や使用する EAP タイプなど）を示すタイプ フィールドがあります。さらに、シーケンス番号を付けることで、オーセンティケータとピアは、各 EAP 要求に対応する EAP 応答を判別できます。
- EAP 応答：応答パケットはサプリカントからオーセンティケータへ送信されます。その際、どの EAP 要求に対する応答であるかを示すシーケンス番号が付与されます。否定応答（NAK）でない限り、通常、EAP 応答は EAP 要求に対応しています。
- EAP 成功：認証に成功すると、オーセンティケータからサプリカントへ成功パケットが送信されます。
- EAP 失敗：認証に成功しなかったときは、オーセンティケータからサプリカントへ失敗パケットが送信されます。

802.11i 準拠のシステムで EAP を使用すると、AP は EAP パススルー モードで動作します。つまり、コード フィールド、ID フィールド、長さフィールドをチェックした上で、クライアント サプリカントから受け取った EAP パケットを AAA へ転送します。同様に、オーセンティケータ（AP）は、AAA サーバから受け取った EAP パケットをサプリカントへ転送します。

図 4-2 は、EAP プロトコル フロー例を示しています。

図 4-2　EAP プロトコル フロー



認証

それぞれの要求に応じて、PEAP、EAP-TLS、EAP-FAST などさまざまな認証プロトコルを使用して安全な無線環境を構築できます。どの認証プロトコルも、現在、基盤のトランスポートとして 802.1X、EAP、および RADIUS を使用しています。これらのプロトコルでは、認証に成功した WLAN クライアントだけがネットワークにアクセスできます。また、WLAN ネットワークをユーザが認証することも可能です。

このソリューションでは、RADIUS プロトコルで伝達されるポリシーに従ってアクセス権を付与したり、RADIUS アカウンティング処理を行うこともできます。

認証を実行するために使用する EAP タイプについては、この後で詳しく説明します。EAP プロトコルの選択に影響を与える主要因は、現在使用している認証システム（AAA）です。理想的なのは、新しい認証システムを導入するのではなく、既存の認証システムを利用して安全な WLAN 環境を構築することです。

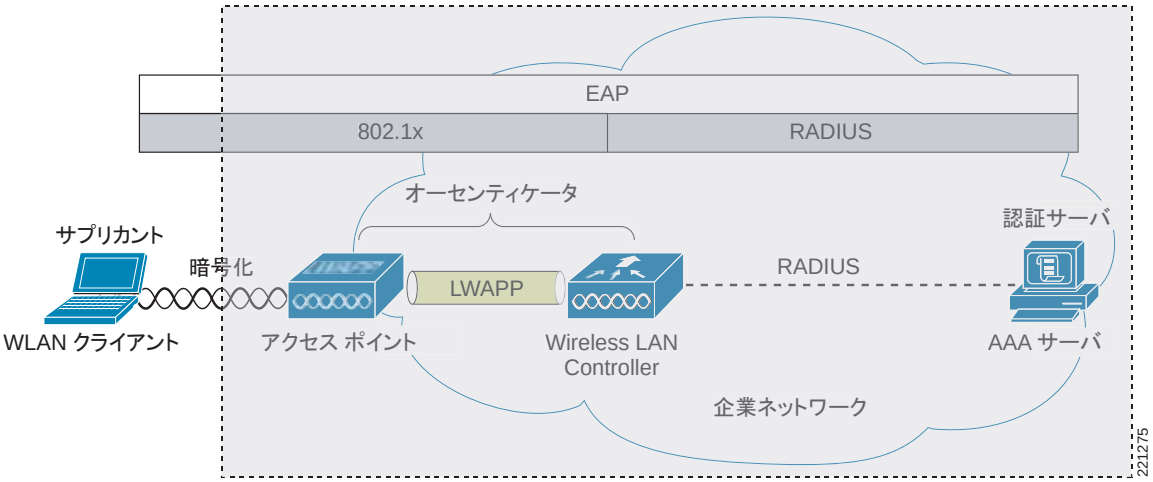
サプリカント

802.1X では、WLAN 認証で使用するクライアント ソフトウェアを「サプリカント」と呼んでいます。Cisco Secure Services Client（CSSC）4.1 は有線ネットワークと無線ネットワークを両方ともサポートしており、一般的なすべての EAP に対応しているサプリカントです。WLAN NIC メーカーがサプリカントを提供する場合や、オペレーティング システムにサプリカントが組み込まれている場合もあります。たとえば、Windows XP は PEAP MSCHAPv2 と EAP-TLS をサポートしています。

CSSC の詳細は、http://www.cisco.com/en/US/products/ps7034/index.html を参照してください。

図 4-3 は、認証アーキテクチャ全体におけるサプリカントの位置付けを示しています。サプリカントの役割は、アップストリームのオーセンティケータ（この場合は WLC）に対して、EAP および 802.1X を使用したエンドユーザ認証を中継することです。サプリカントから EAP メッセージを受け取ったオーセンティケータは、RADIUS を使用して、それらのメッセージを AAA サーバへ転送します。

図 4-3　WLAN クライアント サプリカント



現在、各種の認証ソリューションや顧客の要望を反映したさまざまな EAP サプリカントが市販されています。

表 4-2 は、一般的な EAP サプリカントの機能をまとめたものです。

- PEAP MSCHAPv2：Protected EAP MSCHAPv2。Transport Layer Security（TLS）トンネル（SSL の IETF 標準）を使用して、WLAN クライアントと認証サーバ間のカプセル化 MSCHAPv2 交換を保護します。
- PEAP GTC：Protected EAP Generic Token Card（GTC）。TLS トンネルを使用して、汎用トークン カード交換（ワンタイム パスワードや LDAP 認証など）を保護します。
- EAP-FAST：EAP-Flexible Authentication via Secured Tunnel。PEAP の場合と同様のトンネルを使用します。ただし、PKI（Public Key Infrastructure; 公開鍵インフラストラクチャ）は必要ありません。
- EAP-TLS：EAP Transport Layer Security。PKI を使用して、WLAN ネットワークと WLAN クライアントの両方を認証します。クライアント証明書と認証サーバ証明書が必要です。

表 4-2　一般的な各種サプリカントの比較

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
シングル サインオン（MSFT AD のみ）	あり	あり	あり[1]	あり
ログイン スクリプト（MSFT AD のみ）	あり	あり	一部	あり[2]
パスワード変更（MSFT AD）	あり	あり	あり	N/A
Microsoft AD データベースのサポート	あり	あり	あり	あり
ACS ローカル データベースのサポート	あり	あり	あり	あり
LDAP データベースのサポート	あり[3]	なし	あり	あり

表 4-2　一般的な各種サプリカントの比較（続き）

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
OTP 認証のサポート	あり[4]	なし	あり	なし
RADIUS サーバ証明書の必要性	なし	あり	あり	あり
クライアント証明書の必要性	なし	なし	なし	あり
匿名性	あり	あり[5]	あり[6]	なし

1. サプリカントによって異なります。
2. このスクリプトをサポートするには、マシン アカウントとマシン認証が必要です。
3. LDAP データベースを使用する場合は自動プロビジョニングがサポートされません。
4. サプリカントによって異なります。
5. サプリカントによって異なります。
6. サプリカントによって異なります。

オーセンティケータ

Cisco Secure Wireless Solution の場合、オーセンティケータは Wireless LAN Controller（WLC）です。この WLC は、802.1X ベース サプリカントと RADIUS 認証サーバ間でやり取りされる EAP メッセージのリレーとして動作します。

認証に成功すると、WLC は次の情報を受け取ります。

- EAP 成功メッセージが含まれている RADIUS パケット
- EAP 認証時に認証サーバによって生成された暗号キー
- 通信ポリシーに関する RADIUS VSA（vendor-specific attribute; ベンダー固有属性）

図 4-4 は、認証アーキテクチャ全体における「オーセンティケータ」の論理的位置付けを示しています。オーセンティケータは 802.1X プロトコルを使用してネットワーク アクセスを制御し、サプリカントと認証サーバ間で EAP メッセージを中継します。

図 4-4　オーセンティケータの位置付け

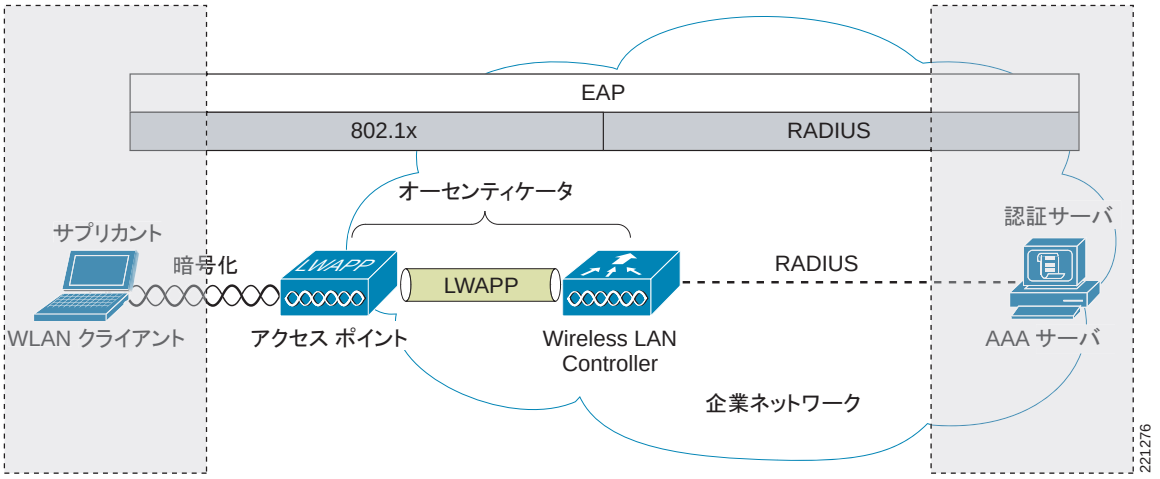


表 4-3 に、PEAP 認証のデコード例を示します。左側の 4 列は無線 802.1X デコードです。右側の 3 列は、同じ PEAP 認証の RADIUS トランザクションを表しています。

EAP 交換シーケンスは次のとおりです。

- AP がクライアントに対して、クライアント ID を要求するパケット #1 を送信します。これによって EAP 交換が開始されます。
- パケット #2 はクライアント ID です。このパケットは RADIUS サーバへ転送されます。この ID に基づいて、RADIUS サーバは EAP 認証を続行するかどうかを判断します。
- パケット #3 を送信し、RADIUS サーバは、認証の EAP 方式として PEAP を使用することを要求します。実際の要求は、RADIUS サーバで設定されている EAP の種類によって異なります。クライアントが PEAP 要求を拒否した場合、RADIUS サーバは他の種類の EAP を提案します。
- パケット #4 ～ 8 は PEAP の TLS トンネル セットアップです。
- パケット #9 ～ 16 は PEAP 内での認証交換です。
- パケット #17 は、認証に成功したことを知らせる EAP メッセージです。

  認証が成功したことをサプリカントとオーセンティケータに通知する以外に、パケット #17 は、RADIUS VSA の形式で指定された認証情報と暗号キーもオーセンティケータに伝送します。

表 4-3　EAP トランザクション

#	送信元	送信先	プロトコル	情報	送信元	送信先	RADIUS 情報
1	AP	クライアント	EAP	要求、ID			
2	クライアント	AP	EAP	応答、ID	WLC	AAA	Access-Rq 1、id=114
3	AP	クライアント	EAP	要求、PEAP	AAA	WLC	Access-Ch 11、id=115
4	クライアント	AP	TLS[1]	Client Hello	WLC	AAA	Access-Rq 1、id=116
5	AP	クライアント	TLS	Server Hello、証明書	AAA	WLC	Access-Ch 11、id=116
6	クライアント	AP	TLS	Client Key Exchange、Change Cipher Spec、暗号化されたハンドシェイク メッセージ	WLC	AAA	Access-Rq 1、id=117
7	AP	クライアント	TLS	Change Cipher Spec、暗号化されたハンドシェイク メッセージ	AAA	WLC	Access-Ch 11、id=117
8	クライアント	AP	EAP	応答	WLC	AAA	Access-Rq 1、id=118
9	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-Ch 11、id=118
10	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Rq 1、id=119
11	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-Ch 11、id=119
12	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Rq 1、id=120
13	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-Ch 11、id=120
14	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Rq 1、id=121
15	AP	クライアント	TLS	アプリケーション データ	AAA	WLC	Access-Ch 11、id=121
16	クライアント	AP	TLS	アプリケーション データ	WLC	AAA	Access-Rq 1、id=122
17	AP	クライアント	EAP	成功	AAA	WLC	Access-Accept 2、id=122

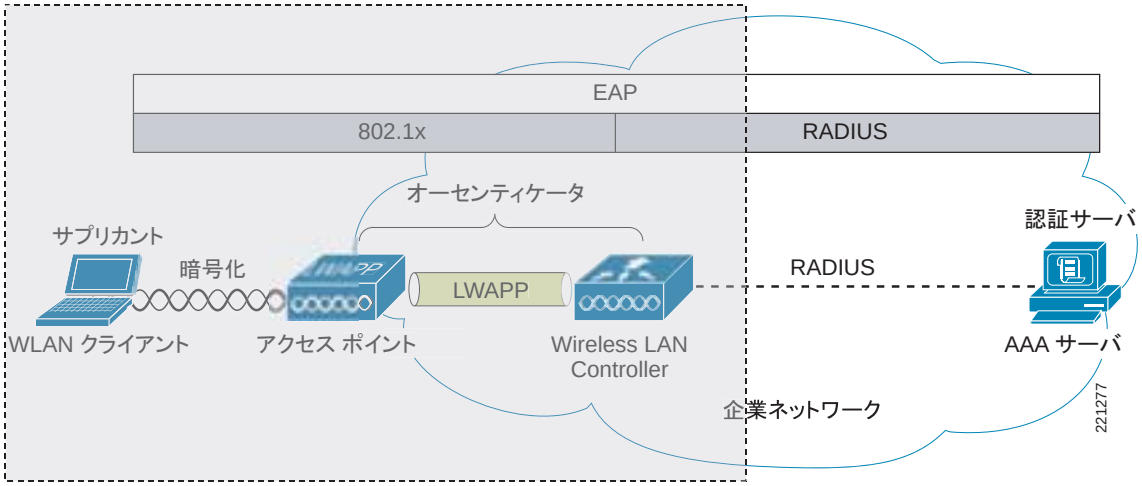
1. TLS トランザクションは EAP パケットとして伝送されます。

認証サーバ

Cisco Secure Unified Wireless ソリューションで使用する認証サーバは Cisco Access Control Server（ACS）です。Cisco ACS は、Windows 2000 サーバまたは Windows 2003 サーバにソフトウェアとしてインストールされている場合と、アプライアンスとして提供される場合があります。また、特定の WLAN インフラストラクチャ デバイスに認証サーバ ロールを実装することもできます。たとえば、IOS AP にローカル認証サービスを追加する、WLC でローカル EAP 認証をサポートする、Cisco WLSExpress に AAA サービスを統合する、AAA サーバで必要なタイプの EAP をサポートするなどの方法があります。

図 4-5 は、無線認証アーキテクチャ全体における認証サーバの論理的位置付けを示しています。この場合、認証サーバは、RADIUS トンネル経由で EAP 認証を実行します。

図 4-5　認証サーバの位置付け



EAP 認証に成功すると、認証サーバは EAP 成功メッセージをオーセンティケータへ送信します。このメッセージは EAP 認証プロセスが成功したことをオーセンティケータに通知し、同時に Pair-wise Master Key（PMK）をオーセンティケータに渡します。WLAN クライアントと AP 間のその後の通信では、この PMK を基にして暗号化ストリームが作成されます。次に、RADIUS での EAP 成功メッセージのデコード例を示します。

```
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0x7a (122)
    Length: 196
    Authenticator: 1AAAD5ECBC487012B753B2C1627E493A
    Attribute Value Pairs
        AVP: l=6  t=Framed-IP-Address(8): Negotiated
        AVP: l=6  t=EAP-Message(79) Last Segment[1]
            EAP fragment
            Extensible Authentication Protocol
                Code: Success (3)
                Id: 12
                Length: 4
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
        AVP: l=6  t=User-Name(1): xxxxxxx
        AVP: l=24  t=Class(25): 434143533A302F313938662F63306138336330322F31
        AVP: l=18  t=Message-Authenticator(80): 7C34BA45A95F3E55425FDAC301DA1AD7
```

暗号化

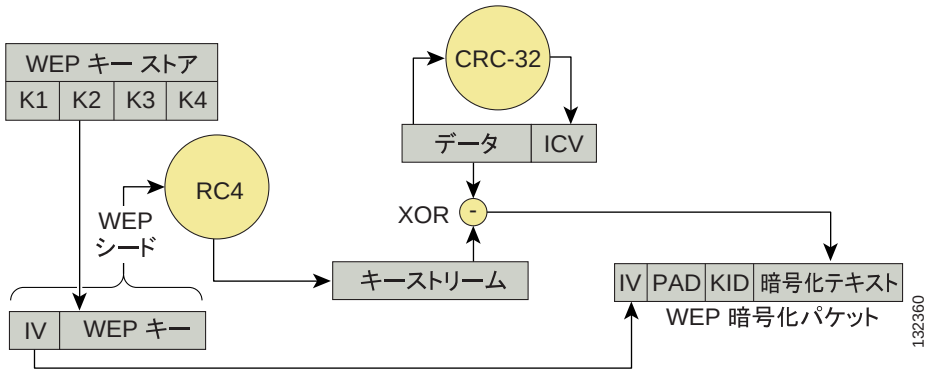
暗号化は WLAN セキュリティの必須要素であり、ローカル RF ブロードキャスト ネットワーク上で機密性を確保するには不可欠な機能です。802.11 規格が最初に採用されたときは、Wired Equivalent Privacy（WEP）が標準的な暗号化技術でした。その後、WEP にはさまざまな面で不備があることがわかり、この暗号化技術では WLAN の安全性を十分に確保できないと考えられています。WEP についてはこのガイドでも説明しています。既存のクライアント環境をサポートするため、現在、ほとんどの WLAN 製品が WEP をサポートしています。新しく導入する場合は、TKIP（WPA）または AES（WPA2）暗号を使用する必要があります。

暗号化キーは PMK を基にして生成されます。ダイナミック WEP 環境の場合、WEP 鍵は PMK の一部です。一方、WPA および WPA2 では、この後説明する 4 ウェイ ハンドシェイクの実行時に暗号化キーが生成されます。

WEP

図 4-6 に WEP 暗号化プロセスを示します。まず、WEP キーと初期化ベクトル（IV）が連結され、この結合キーをシードとして RC4 キーストリームが生成されます。次に、生成したキーストリームと WLAN データの XOR 演算が実行されます。フレームごとに異なる IV ストリームが使用されます。つまり、フレームごとに異なる結合キーを使用して新しい RC4 キーストリームが生成されます。ただし、IV の再利用率が高いこと、ストリーム暗号（RC4）を基にしてブロック暗号を生成することから、その脆弱性が指摘されています。事実、現在市販されている一般的なツールで解読することができます。前述したように、WEP はできる限り使用しないでください。

図 4-6　WEP のカプセル化プロセス



LWAPP WLAN ソリューションは 3 つの WEP キー長をサポートしています。標準の 40 ビット キーと 104 ビット キー、そして 128 ビット キーです。128 ビット キーの使用は推奨されていません。このキー長をサポートしている WLAN クライアントがあまりないためです。また、128 ビット キーを使用したとしても、WEP 暗号自体の脆弱性は解決されません。

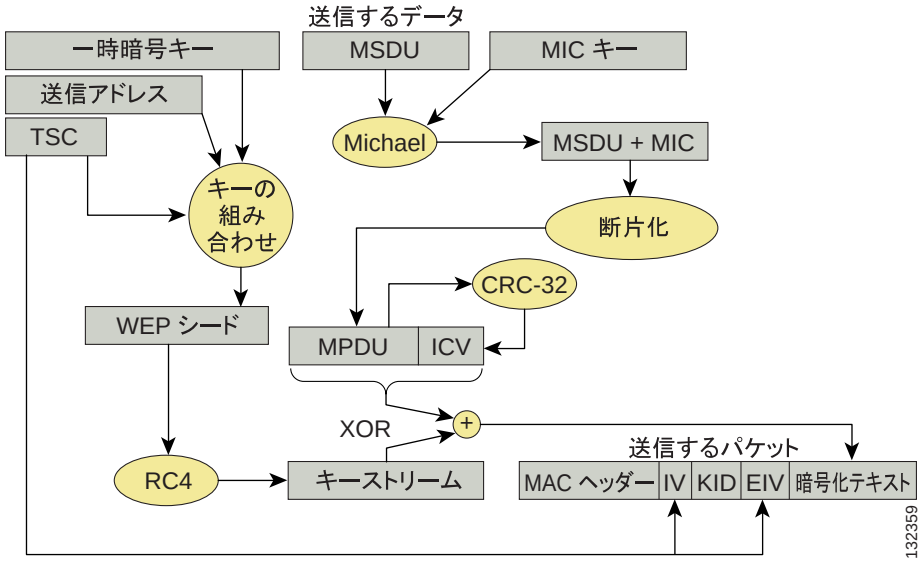
TKIP 暗号

802.11i では企業レベルの 2 つの暗号メカニズム Temporal Key Integrity Protocol（TKIP）と Advanced Encryption Standard（AES）が規定されており、これらは Wi-Fi Alliance によって WPA および WPA2 として認定されています。

TKIP は、WPA として認定されている暗号方式です。これまで指摘されていた 802.11 WEP 暗号方式の脆弱性が改善されており、従来と同じ RC4 コア暗号化アルゴリズムを採用しているので、既存の WLAN 装置にも対応しています。WEP の既知の弱点をすべて克服しており、さらに WLAN クライアント デバイスを新しくする必要がないことから、今後しばらくは TKIP（WPA）が主流となることでしょう。ただし、WPA2 の AES 暗号の方が、IT 業界の規格や基準により柔軟に対応できます。

図 4-7 は TKIP の基本フロー図です。

図 4-7　WPA TKIP

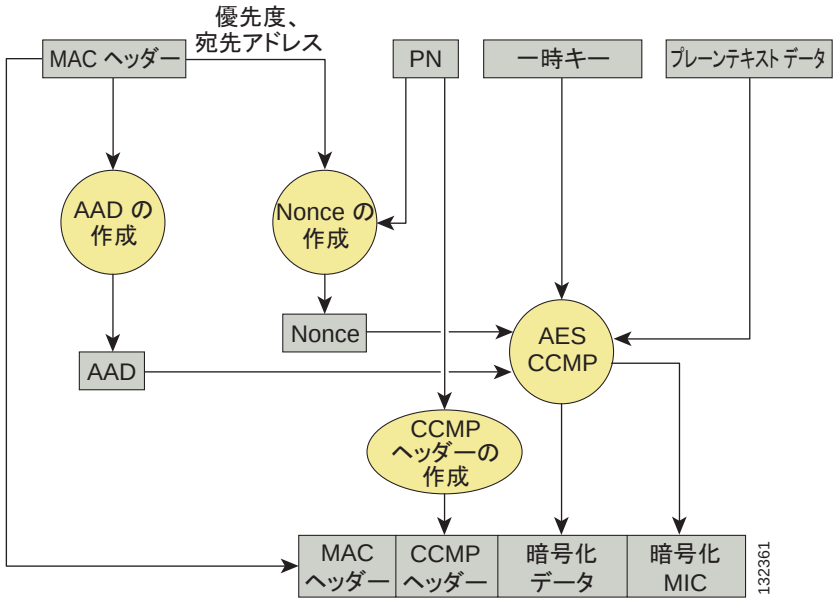


TKIP には 2 つの大きな役割があります。1 つは、MAC Service Data Unit（MSDU; MAC サービス データ ユニット）の RC4 暗号を使用してパケットごとにキーを生成すること。もう 1 つは、暗号化されたパケットの Message Integrity Check（MIC; メッセージ完全性チェック）を実行することです。パケットごとのキーは、送信アドレス、初期化ベクトル（IV）、および暗号キーのハッシュです。フレーム送信のたびに IV が変わるので、RC4 暗号で使用されるキーはフレームごとに異なります。Michael アルゴリムを使用して MIC キーとユーザ データが結合され、MIC が生成されます。Michael は、演算オーバーヘッドが小さく、高いパフォーマンスを得られるアルゴリズムですが、攻撃を受けやすいという欠点もあります。そのため WPA では、WLAN クライアントを一時的に切断し、60 秒間は新しいキー ネゴシエーションを行えなくする予防措置がとられています。ただし、この動作自体が一種の DoS 攻撃となる可能性があります。多くの WLAN 実装は、必要に応じて、この対抗機能を無効できるようになっています。

AES 暗号

図 4-8 は、基本的な AES counter mode/CBC MAC Protocol（CCMP）のフロー図です。CCMP は AES 暗号モードの 1 つであり、カウンタ モードは機密性を実現し、CBC MAC はメッセージの完全性を維持します。

図 4-8　WPA2 AES CCMP



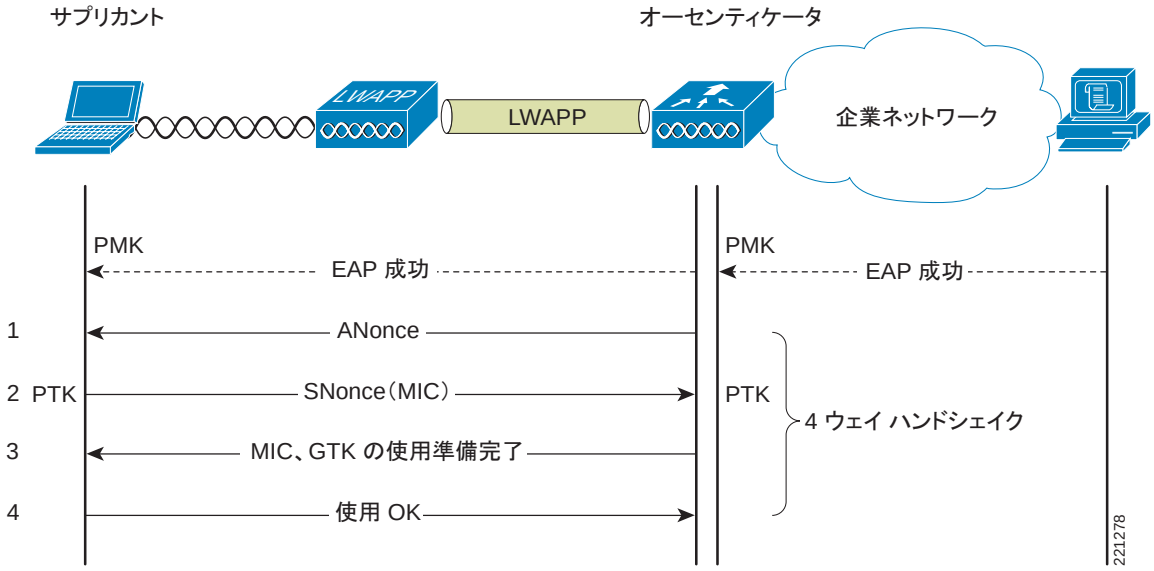
CCMP 手順では、追加の認証データ（AAD）が MAC ヘッダーから取得され、CCM 暗号化プロセスに組み込まれます。これによってフレームが保護され、フレーム内の非暗号化部分の改ざんを防ぎます。

リプレイ アタックを防ぐため、連続したパケット番号（PN）が CCMP ヘッダーに追加されます。この PN と MAC ヘッダーの各部を使用してナンスが生成され、さらにこのナンスが CCM 暗号化プロセスで使用されます。

4 ウェイ ハンドシェイク

4 ウェイ ハンドシェイクは、無線データ フレームの暗号化で必要となる暗号キーを生成するための方式です。図 4-9 は、暗号キー生成時のフレーム交換を示しています。これらのキーを「一時キー」といいます。

図 4-9　4 ウェイ ハンドシェイク



暗号化に必要なキーは、EAP 認証セクションで生成した PMK に基づいて作成されます。この PMK は EAP 成功メッセージとしてオーセンティケータに送信されますが、サプリカントには転送されません。サプリカントは PMK を独自に生成するためです。

1. オーセンティケータは、オーセンティケータ ナンス（ANonce）が含まれている EAPOL-Key フレームを送信します。これはオーセンティケータが生成した乱数です。
   a. サプリカントは、ANonce とサプリカント ナンス（SNonce）を基にして PTK を生成します。これはクライアント / サプリカントによって生成される乱数です。
2. サプリカントは、SNonce、（再）アソシエーション要求フレームの RSN 情報エレメント、および MIC を含む EAPOL-Key フレームを送信します。
   a. オーセンティケータは ANonce と SNonce を基にして PTK を生成し、EAPOL-Key フレームの MIC を検証します。
3. オーセンティケータは、ANonce（ビーコンまたはプローブ応答メッセージから取得した RSN 情報エレメント）、MIC（一時キーをインストールするかどうかを決定）、およびカプセル化されたグループ一時キー（GTK）（マルチキャスト暗号キー）を含む EAPOL-Key フレームを送信します。
4. サプリカントは EAPOL-Key フレームを送信して、一時キーがインストールされているかどうかを確認します。

Cisco Compatible Extensions

Cisco Compatible Extensions プログラムは、Cisco WLAN インフラストラクチャで利用できるクライアント デバイスの普及を促進し、シスコ独自の最新機能を活用して、セキュリティ、モビリティ、QoS（Quality of Service）、およびネットワーク管理を向上することを目的としています。

図 4-10 に示すように、Cisco Compatible Extensions は 802.11 規格、IETF 規格、および Wi-Fi Alliance 認定に基づいており、WLAN 機能のスーパーセットを構成しています。Cisco Unified Wireless Network の導入を計画していない場合でも、Cisco Compatible Extensions WLAN アダプタを使用すれば、WLAN クライアント デバイスが対応している規格や認定を簡単に追跡できます。

図 4-10　Cisco Compatible Extensions の構成

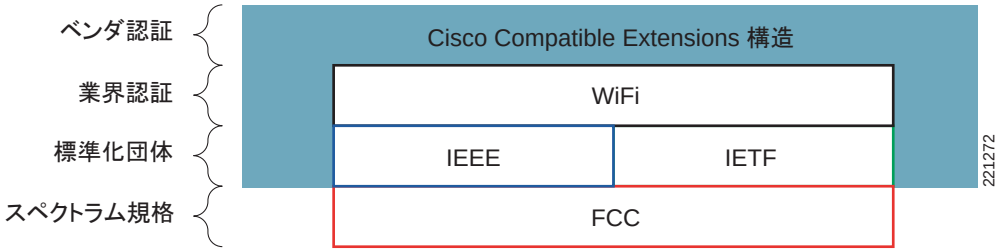


図 4-11 は、Cisco Compatible Extensions のセキュリティ機能を認定レベルごとにまとめたものです。Cisco Compatible Extensions 認定は、該当する Wi-Fi 認定だけでなく、Cisco Compatible Extensions 認定の一環として既にテストされている EAP サプリカントも指定します。

（注） ラップトップに必要な機能であっても、主にデータ アプリケーションで使用する Application-Specific Device（ASD; 特定用途向けデバイス）では必要ないものがあります。データ ASD には、データ収集デバイス、PDA、プリンタなどがあります。音声 ASD には、シングル モード、デュアル モード、スマートフォンがあります。

Cisco Compatible Extensions のバージョン一覧は、http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html で参照できます。

図 4-11　Cisco Compatible Extension のセキュリティ機能

セキュリティ	v1	v2	v3	v4	ASD
WEP	x	x	x	x	
IEEE 802.1X	x	x	x	x	x
LEAP	x	x	x	x	x
PEAP と EAP-GTC（PEAP-GTC）		x	x	x	オプション
EAP-FAST			x	x	x
PEAP と EAP-MSCHAPv2（PEAP-MSCHAP）				x	
EAP-TLS ASD には、LEAP、EAP-Fast、または EAP-TLS が必要				x	x
Cisco TKIP（暗号化）	x				
WiFi Protected Access（WPA）: 802.1X + WPA TKIP		x	x	x	
LEAP を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）		x	x	x	x
PEAP-GTC を使用		x	x	x	
EAP-FAST を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）			x	x	x
PEAP-MSCHAP を使用				x	
EAP-TLS を使用（ASD には、LEAP、EAP-Fast、または EAP-TLS が必要）				x	x
IEEE 802.11i–WPA2: 802.1X + AES			x	x	
LEAP を使用			x	x	
PEAP-GTC を使用			x	x	
EAP-FAST を使用			x	x	
PEAP-MSCHAP および EAP-TLS を使用				x	
ネットワーク アドミッション制御（NAC）				x	

221405

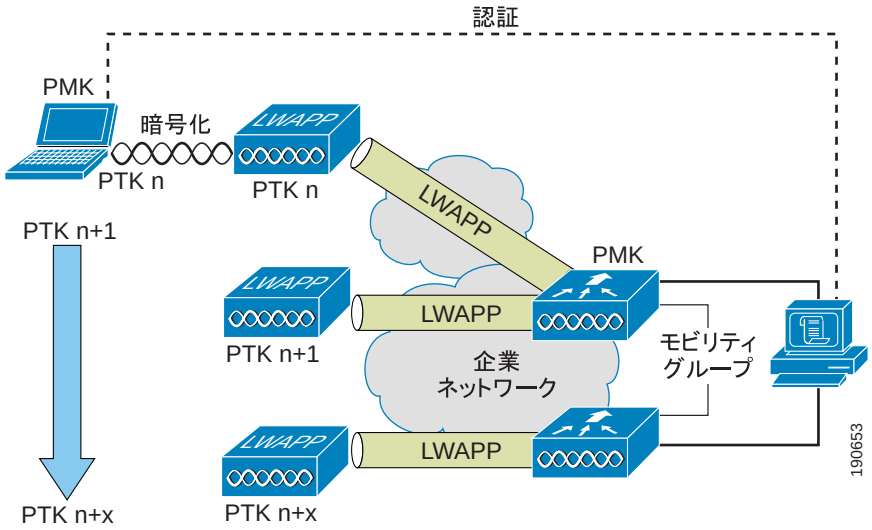
Cisco Compatible Extensions バージョン 5 には、クライアント側での Management Frame Protection（MFP; 管理フレーム保護）など、新しいセキュリティ機能が追加されています。管理フレーム保護（P. 4-30）を参照してください。

Proactive Key Caching および CCKM

Proactive Key Caching（PKC）は 802.11i の拡張機能です。PKC を使用すると、AP でのクライアント 802 x/EAP 認証時に生成される PMK を事前に（クライアント ローミング イベントの前に）キャッシュできます（図 4-12 を参照）。WLAN クライアントがローミングしようとしている AP に、そのクライアントの PMK がすでにキャッシュされている場合、完全な 802.1x/EAP 認証が不要となります。代わりに、WLAN クライアントは WPA の 4 方向のハンドシェイク プロセスを使用して、その AP との通信に使用する新しいセッション暗号キーを安全に導出します。

キャッシュされた PMK の AP への配布は、Unified Wireless 環境では大幅に簡略化されます。PMK がコントローラにキャッシュされ、そのコントローラに接続するすべての AP が PMK を利用できるようになります。さらに、アンカー コントローラが属しているモビリティ グループの他のすべてのコントローラも、この PMK を共有します。

図 4-12　Proactive Key Caching アーキテクチャ



Cisco Centralized Key Management（CCKM）は、Fast Secure Roaming（FSR; 高速セキュア ローミング）を実現するために Cisco Compatible Extensions クライアントがサポートしているシスコの標準規格です。ローミング プロセスを促進するための主要メカニズムは PKC と同じであり、キャッシュされた PMK を使用します。ただし、CCKM での実装は多少異なります。この場合、これら 2 つのメカニズムは互いに互換性がありません。FSR および CCKM の詳細は、http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801c5223.html を参照してください。

各 WLAN クライアントのキー キャッシュの状態を確認するには、**show pmk-cache all** コマンドを使用します。このコマンドを実行すると、キーをキャッシュしているクライアント、およびそのクライアントが使用しているキー キャッシュ機能を確認できます。

802.11r ワークグループは、802.11 の FSR メカニズムの標準化を進めています。WLC コントローラは、次の例に示すように、同じ WLAN（802.1x + CCKM）上で CCKM と PKC の両方をサポートします。

```
WLAN Identifier.................................. 1
Network Name (SSID).............................. wpa2
…
Security
   802.11 Authentication:........................ Open System
   Static WEP Keys.............................. Disabled
   802.1X........................................ Disabled
   Wi-Fi Protected Access (WPA/WPA2)............. Enabled
      WPA (SSN IE)............................... Disabled
      WPA2 (RSN IE).............................. Enabled
         TKIP Cipher............................. Disabled
         AES Cipher.............................. Enabled
   Auth Key Management
         802.1x.................................. Enabled
         PSK..................................... Disabled
         CCKM.................................... Enabled
…
(Cisco Controller) >show pmk-cache all
PMK-CCKM Cache
                              Entry
Type        Station           Lifetime   VLAN Override        IP Override
------    --------------    --------   ------------------   ---------------
CCKM    00:12:f0:7c:a3:47   43150                             0.0.0.0
RSN     00:13:ce:89:da:8f   42000                            0.0.0.0
```

Cisco Unified Wireless Network アーキテクチャ

図 4-13 は Cisco Unified Wireless Network アーキテクチャ構成の概略図です。このアーキテクチャは、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）アクセス ポイント、メッシュ LWAPP AP（MAP）、Wireless Control System（WCS）、および Wireless LAN Controller（WLC; 無線 LAN コントローラ）で構成されています。Wireless LAN Controller Module（WLCM）と Wireless Services Module（WiSM）で WLC プラットフォームを構成することもできます。さらに、Cisco Access Control Server（ACS）とその Authentication/Authorization/Accounting（AAA; 認証、認可、アカウンティング）機能によって、無線ユーザの認証と認可を行う RADIUS サービスを提供します。

図 4-13　Cisco Unified Wireless Network アーキテクチャ

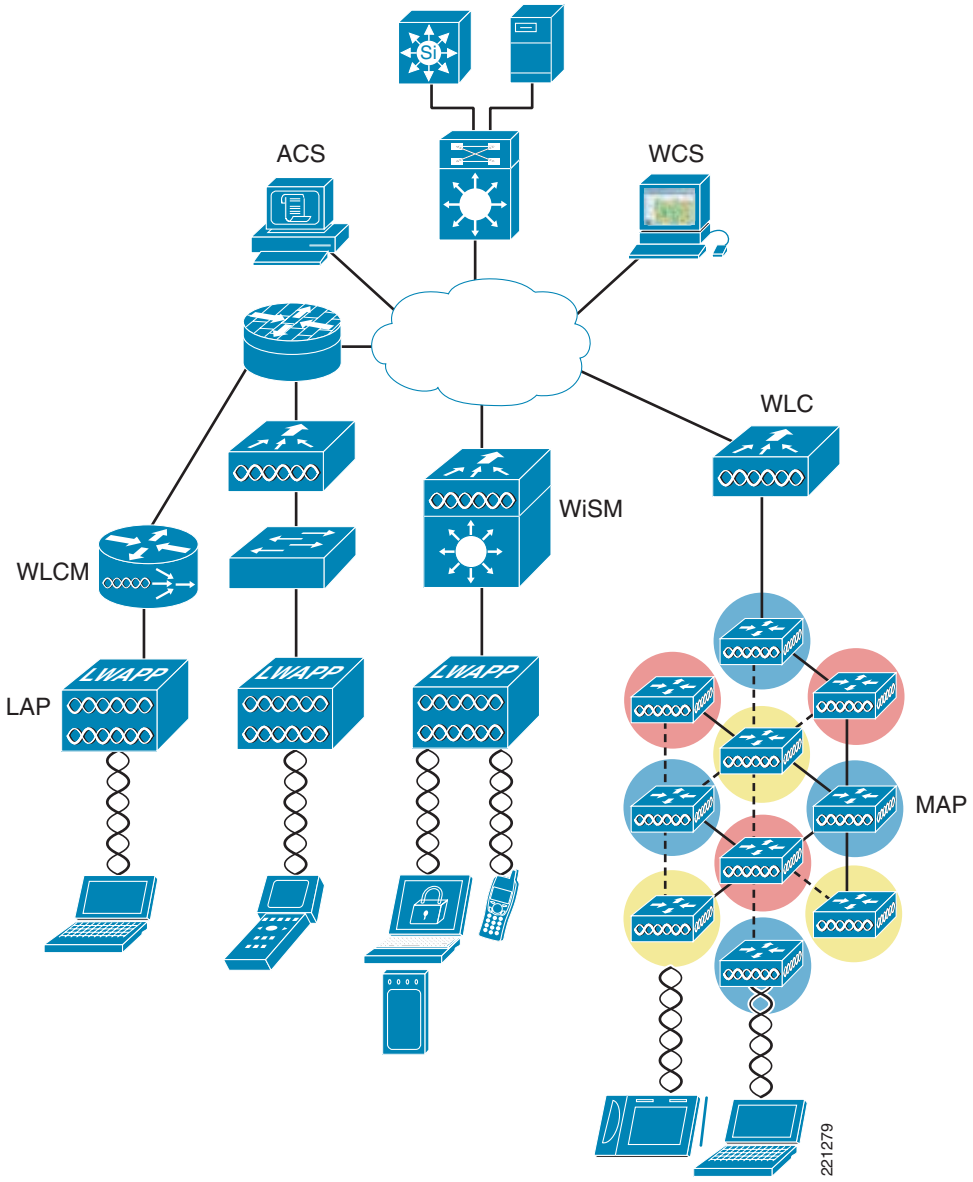
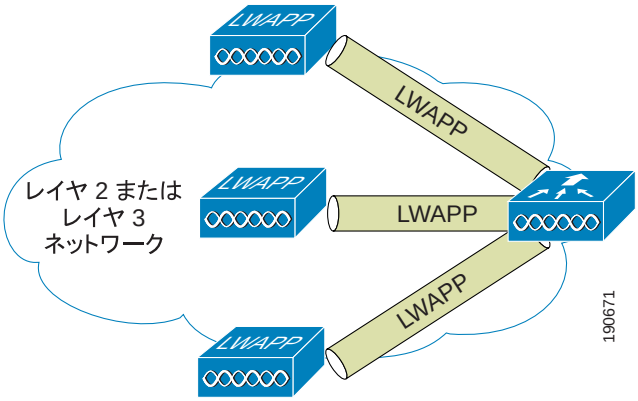


図 4-14 はこのアーキテクチャの主要機能です。LAP が LWAPP プロトコルを使用して WLC と通信し、トラフィックをトンネル処理する仕組みを示しています。

図 4-14　LAP と WLC の接続



LWAPP には 3 つの主要機能があります。

- LAP を制御および管理する
- WLAN クライアント トラフィックを WLC へトンネリングする
- Cisco Unified Wireless System の管理に必要な 802.11 データを収集する

LWAPP の機能

システムの展開と管理が簡単であるほど、そのシステムのセキュリティ管理も容易になります。スタンドアロン型の「重い」AP を使用していた初期の WLAN システムの場合、AP の導入と設定は、何百ものファイアウォールをそれぞれ個別に設置し、管理することを意味していました。最新のファームウェアがインストールされているか、設定は適切か、セキュリティ対策に問題はないかを常に気にしていなければならなかったのです。さらに、AP は物理的に安全でない領域に設置されることが多く、AP が盗まれ、その情報が漏れると、また別の不正行為に発展する可能性があります。

LWAPP は、展開、設定、および物理的セキュリティの問題に次のように対処します。

- AP の操作と管理はユーザが直接行いません。LWAPP 接続を介して WLC が AP を管理します。これにより、設定機能とファームウェア機能が WLC に移行し、WCS による集中管理が可能になります。
- AP は自身の設定を WLC からダウンロードします。また、WLC で設定が変更されたときは、AP が自動的に更新されます。
- AP のファームウェアを WLC と同期させ、常に適切なバージョンのファームウェアが実行されるようにします。
- 重要な設定データを WLC に保存し、AP には IP アドレス情報のみを保存します。AP に物理的問題が発生した場合でも、NVRAM には設定情報が保存されていないので、悪用される心配がありません。
- LAP と WLC は互いに認証し、AES によって LWAPP 制御チャネルを暗号化します。

上記のようなセキュリティ上の利点に加え、WLAN トラフィックをトンネリングする LWAPP ベース アーキテクチャを利用すれば、ソリューション全体のセキュリティを損なうことなく、簡単に導入できます。アクセス スイッチで dot1q トランキングを設定したり、クライアント サブネットを追加したりしなくても、複数の WLAN VLAN をサポートする LAP をアクセス レイヤ スイッチに配備できます。すべての WLAN クライアント トラフィックはトンネル経由で（WLC が配置されている）中央サイトへ送信されるので、WLAN のアクセスとセキュリティに関するポリシーを企業レベルで容易に導入できます。

Cisco Unified Wireless のセキュリティ機能

802.11 のセキュリティ機能に物理的なセキュリティを追加し、展開の容易な LWAPP アーキテクチャを採用すれば、WLAN 環境全体のセキュリティが向上します。上記で説明した LWAPP プロトコル自体のセキュリティ機能に加え、Cisco Unified Wireless ソリューションには次のセキュリティ機能が備わっています。

- 機能強化された WLAN セキュリティ オプション
- ACL 機能とファイアウォール機能
- Dynamic Host Configuration Protocol（DHCP）と Address Resolution Protocol（ARP; アドレス解決プロトコル）による保護
- ピアツーピア ブロッキング
- 無線 Intrusion Detection System（IDS; 侵入検知システム）
  - クライアントの除外
  - 不正 AP 検出
- 管理フレーム保護
- 動的な無線周波数管理
- アーキテクチャ統合
- IDS 統合

機能強化された WLAN セキュリティ オプション

Cisco Unified Wireless Network ソリューションはさまざまな WLAN セキュリティ オプションをサポートしています。たとえば、WLC で複数の WLAN を作成し、従来のプラットフォームではオープン ゲスト WLAN ネットワークや WEP ネットワークを使用して、それ以外では WPA と WPA2 セキュリティ設定を組み合わせるなど、それぞれ異なる WLAN セキュリティ設定を使用できます。

各 WLAN SSID は、WLC 上の同じ dot1q インターフェイスまたは異なる dot1q インターフェイスに割り当てることができます。また、モビリティ アンカー（自動アンカー モビリティ）を介して、別のコントローラへ Ethernet over IP（EoIP）トンネルで伝送できます。

802.1x に基づいて WLAN クライアントを認証する場合、認証成功時に WLC に渡される RADIUS 属性を使用して dot1q VLAN 割り当てを制御できます。

図 4-15 と図 4-16 は、Unified Wireless WLAN 設定画面の一部を示しています。このサンプル画面には、次の 3 つの設定項目が表示されています。

- WLAN SSID
- WLAN がマッピングされている WLC インターフェイス
- セキュリティ方式（その他の WPA オプションと WPA2 オプションも選択できますが、この図には表示されていません）

図 4-15　WLAN General タブ

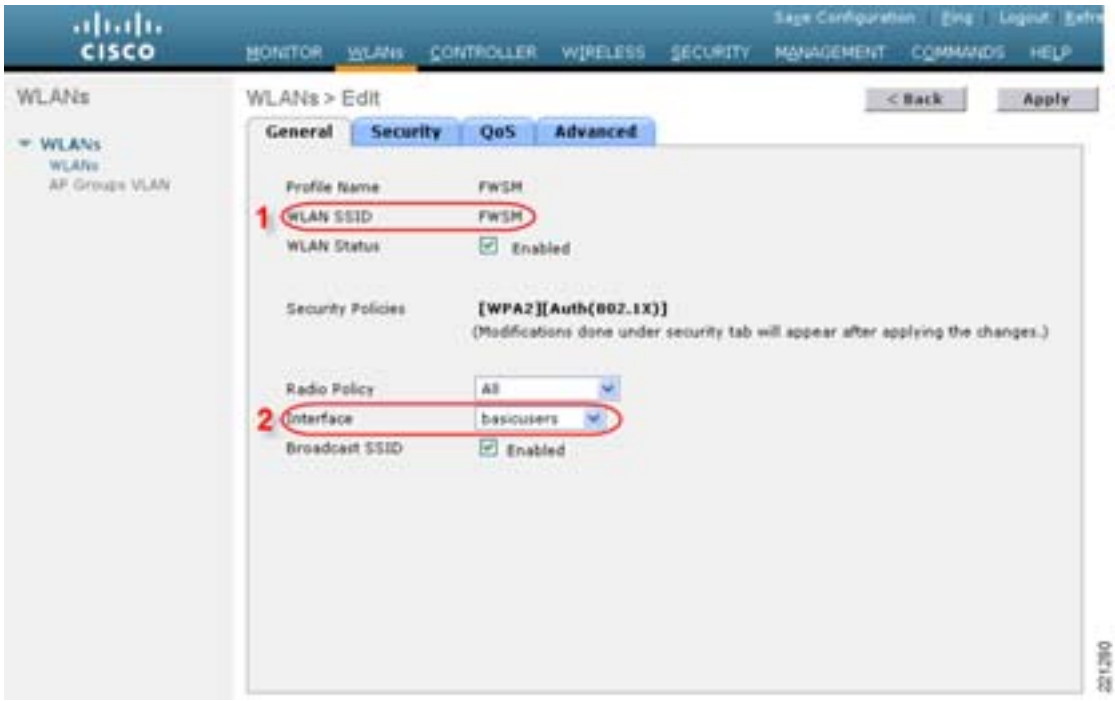
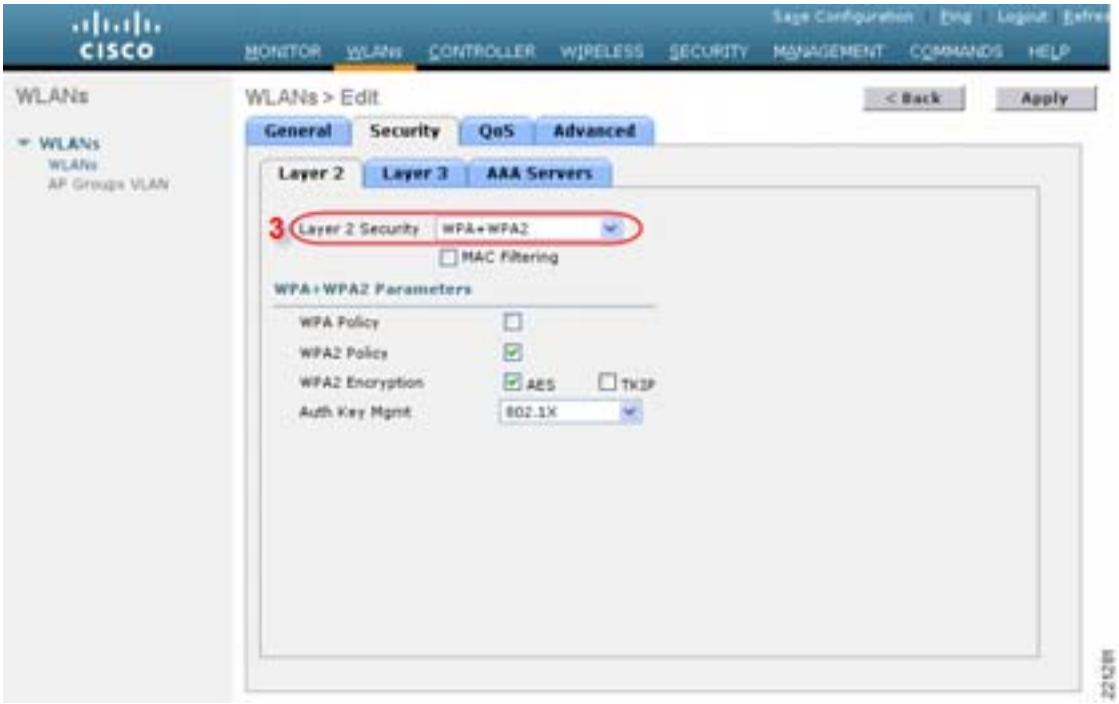


図 4-16　WLAN Layer 2 Security タブ



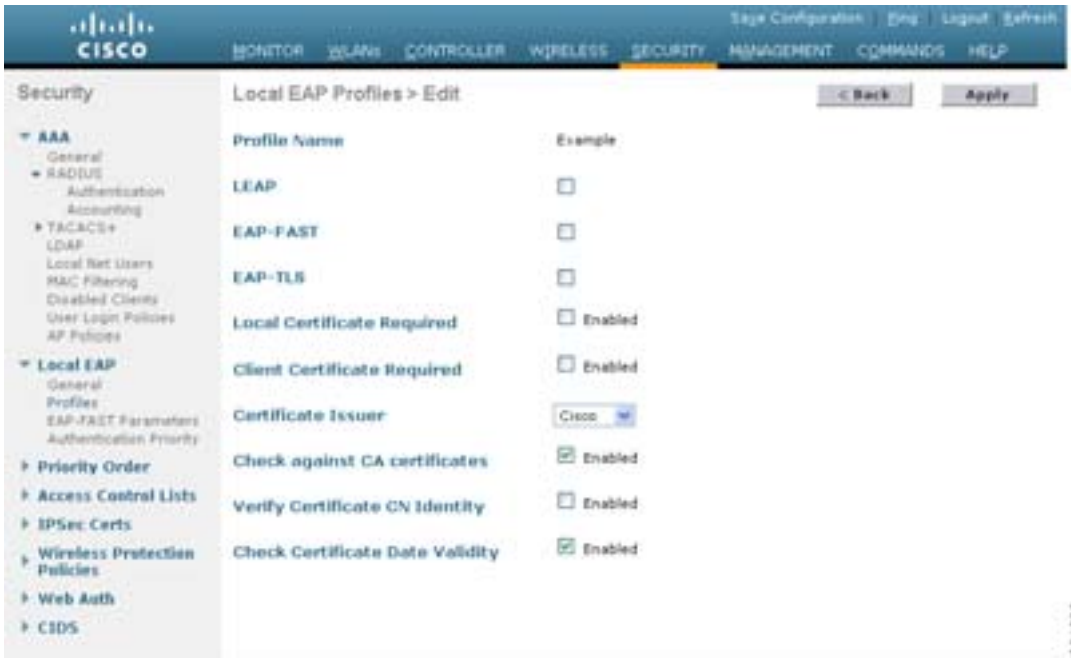
ローカル EAP 認証

WLC ソフトウェア リリース 4.1 にはローカル EAP 認証機能が備わっており、外部 RADIUS サーバが用意されていない場合や利用できなくなった場合に、この機能が役立ちます。図 4-17 に示すように、ローカル認証に切り替えるまでの遅延時間を指定できます。RADIUS サーバの機能が回復すると、ローカル認証から RADIUS サーバ認証へ自動的に切り替わります。

図 4-17　ローカル認証タイムアウト

WLC でローカルにサポートされている EAP の種類は、LEAP、EAP-FAST、および EAP-TLS です。ローカル EAP のプロファイル例を図 4-18 に示します。

図 4-18　ローカル EAP のプロファイル



WLC は、自身のローカル データベースを使用してデータを認証できます。また、LDAP ディレクトリにアクセスして、EAP-FAST 認証または EAP-TLS 認証に必要なデータを取得することもできます。図 4-19 に示すように、優先的に使用するユーザ資格情報データベースを選択できます。

図 4-19　ローカル EAP の優先順位

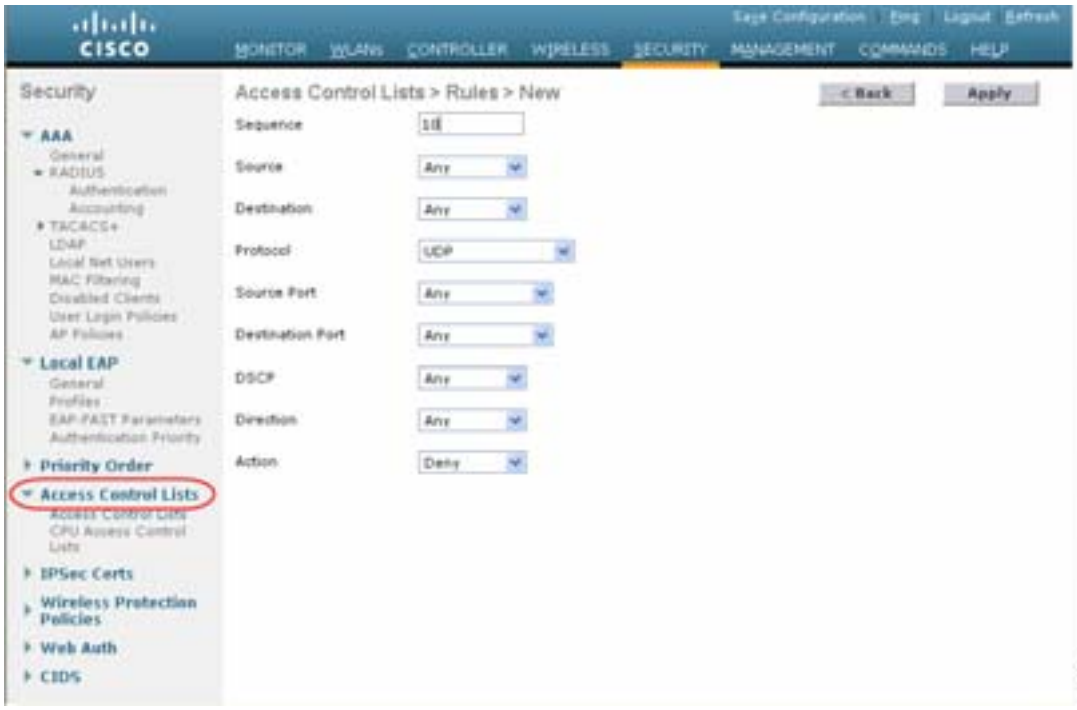
ACL 機能とファイアウォール機能

各 WLC で設定されているインターフェイスに対して、または WLC の CPU 自体に対して、Access Control List（ACL; アクセス コントロール リスト）を定義できます。これらの ACL を使用して特定の WLAN にポリシーを適用し、指定したアドレスやプロトコルへのアクセスを制限したり、WLC 自体の保護を強化したりできます。

インターフェイス ACL は、その ACL の適用対象となるインターフェイス経由でやり取りされる WLAN クライアント トラフィックを制御します。CPU ACL は、WLC 上のインターフェイスとは関係なく、WLC システムがやり取りするすべてのトラフィックに適用されます。

図 4-20 は ACL 設定ページを示しています。ACL では、転送元と転送先のアドレス範囲、プロトコル、転送元と転送先のポート、Differentiated Services Code Point（DSCP）、および ACL の適用方向を指定できます。さまざまな規則に基づいて ACL を作成できます。

図 4-20　ACL の設定ページ



DHCP および ARP の保護

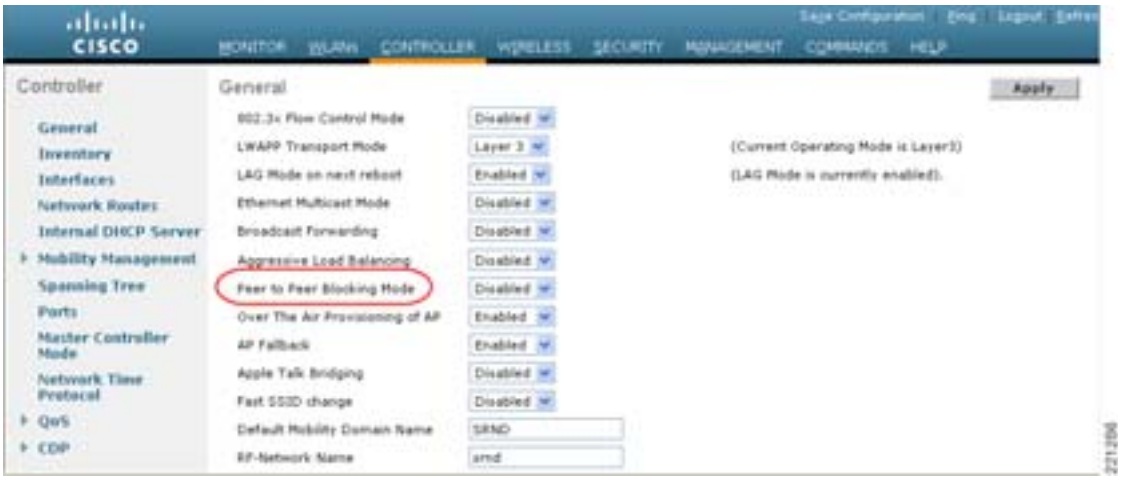
WLC は、WLAN クライアント DHCP 要求のリレー エージェントとして機能します。その際、WLC は、DHCP インフラストラクチャを保護するためのいくつかのチェックを実行します。中でも重要なのは、DHCP 要求に含まれている MAC アドレスが、その要求の送信元 WLAN クライアントの MAC アドレスと一致するかどうかを検証することです。このように、それぞれのインターフェイスで、WLAN クライアントを 1 つの DHCP 要求（IP アドレス）に制限することによって、消耗攻撃を受けないようにします。WLC のデフォルト設定では、WLAN クライアントからのブロードキャスト メッセージを同じ WLAN に返送しないようになっています。これは、WLAN クライアントが DHCP サーバになりすまし、DHCP 情報を悪用するのを防ぐためです。

MAC アドレスと IP アドレスとの関連付けを管理する WLC は、WLAN クライアントの ARP プロキシとして機能しますしたがって WLC は、重複する IP アドレスや ARP スプーフィング攻撃を阻止できます。WLC は、WLAN クライアント間の直接的な ARP 通信を許可しません。これもまた、WLAN クライアント デバイスを狙った ARP スプーフィング攻撃の防止に役立ちます。

ピアツーピア ブロッキング

WLC は、同じ WLAN 上でのクライアント間通信をブロックするように設定できます。その場合、必ずルータ経由で通信が行われるので、同じサブネット上でのクライアント間攻撃を防止できます。図 4-21 は、WLC でのピアツーピア ブロッキングの設定を示しています。これは WLC のグローバル設定なので、その WLC で構成されているすべての WLAN に適用されます。

図 4-21　ピアツーピア ブロッキング



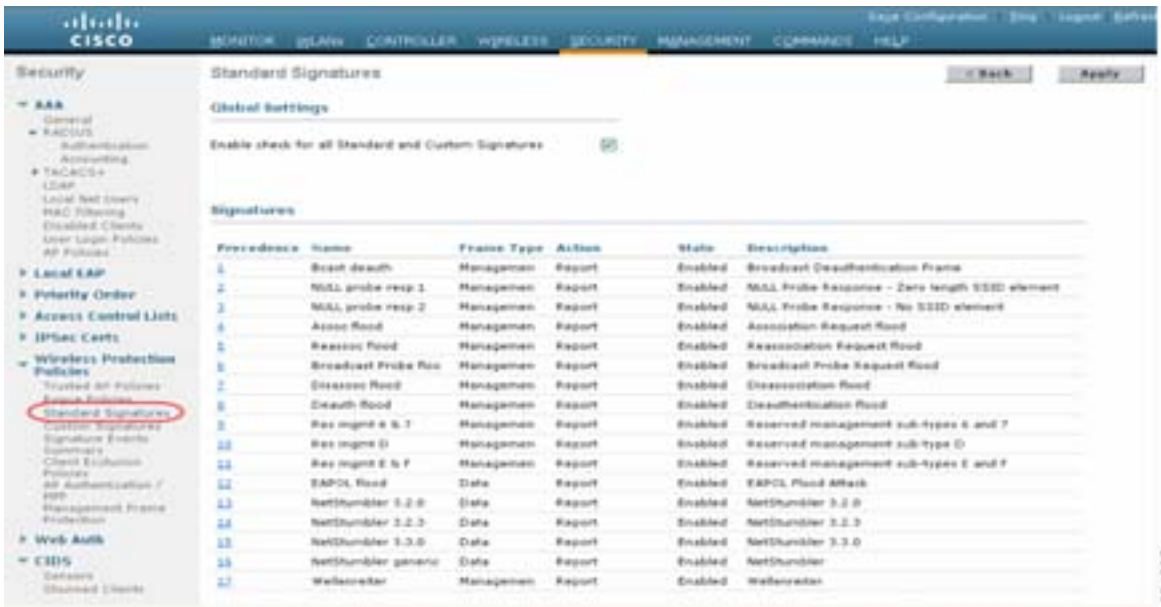
無線 IDS

WLC は、接続されているすべての LAP から取得した情報に基づいて WLAN IDS を解析します。さらに、WLC および WCS への攻撃が検出された場合はそれを報告します。無線 IDS 解析は、有線ネットワーク IDS システムで一般的に実行される解析を補うための機能です。WLC に備わっている無線 IDS 機能は、有線ネットワーク IDS システムの対象とならない 802.11 および WLC 関連の情報を解析します。

WLC ソフトウェア リリースには、WLC で使用する無線 IDS のシグニチャ ファイルが含まれていますが、これらのファイルは独自に更新することができます。カスタム シグニチャは Custom Signatures ウィンドウに表示されます。

図 4-22 は、WLC の Standards Signatures ウィンドウを示しています。

図 4-22　標準の WLAN IDS シグニチャ

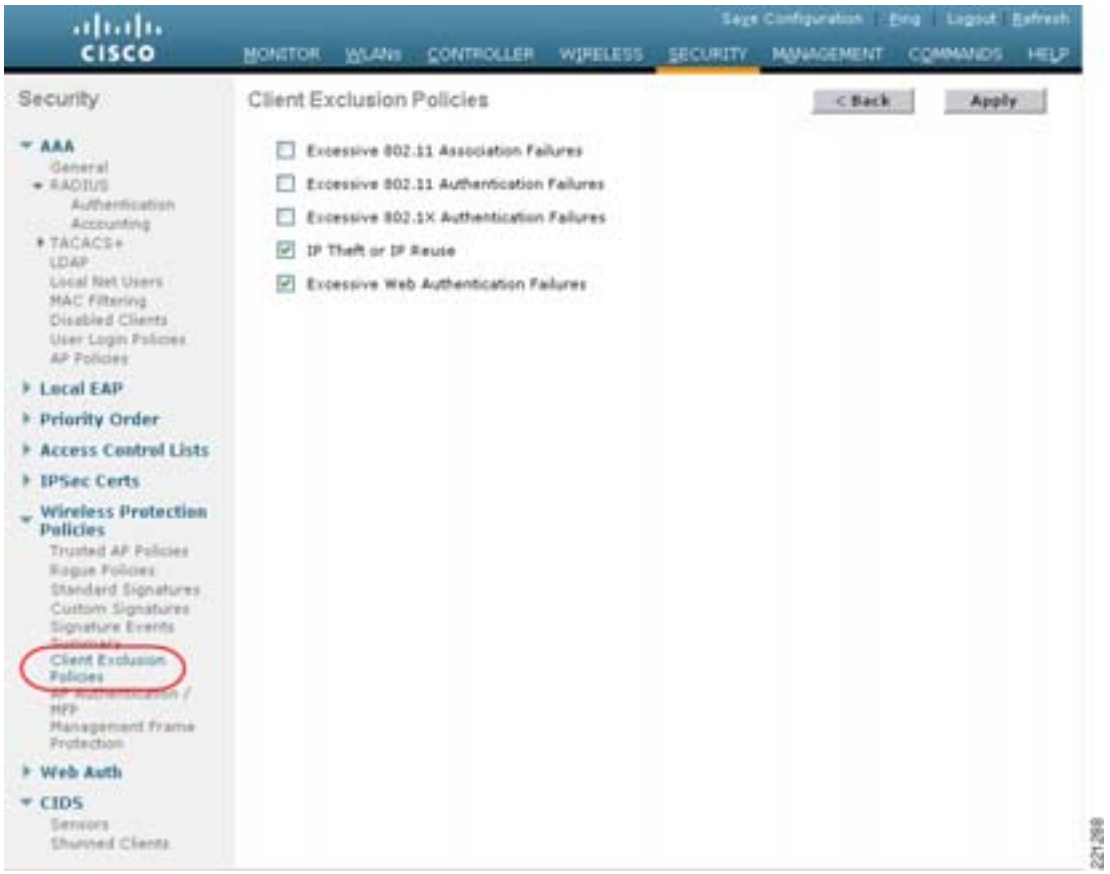


クライアントの除外

WLC には、無線 IDS 以外にも、WLAN インフラストラクチャと WLAN クライアントを保護するための機能が備わっています。WLC には、動作が不審な WLAN クライアントを除外するポリシーを実装できます。図 4-23 は Exclusion Policies ウィンドウを示しています。このウィンドウでは、現在サポートされている次のクライアント除外ポリシーを指定できます。

- Excessive 802.11 Association Failures：不審なクライアントまたは DoS 攻撃
- Excessive 802.11 Authentication Failures：不審なクライアントまたは DoS 攻撃
- Excessive 802.1X Authentication Failures：不審なクライアントまたは DoS 攻撃
- External Policy Server Failures：ネットワークベースの IPS サーバが除外するクライアントを特定
- IP Theft or IP Reuse：不審なクライアントまたは DoS 攻撃
- Excessive Web Authentication Failures：DoS 攻撃またはパスワードクラッキング攻撃

図 4-23　クライアントの除外ポリシー

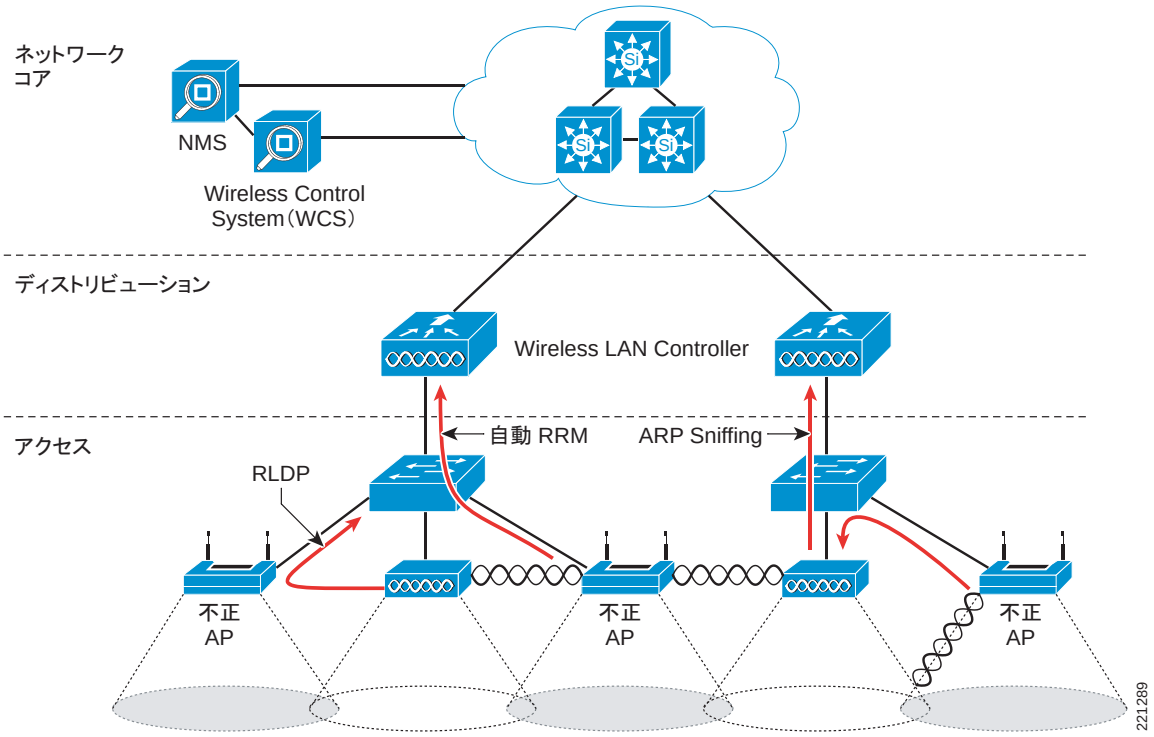


不正 AP

図 4-24 に示すように、Cisco Unified Wireless Networking ソリューションには徹底した不正 AP 対策が設けられています。具体的な機能は次のとおりです。

- 無線検出：ビーコンおよび 802.11 プローブ応答を観測または傍受することによって、不正デバイスを検出します。
- 不正 AP の特定：検出された RF 特性および管理対象 RF ネットワークの既知のプロパティに基づいて、不正デバイスの所在を突き止めます。
- 有線検出：不正デバイスを追跡し、有線ネットワークとの関連性を特定します。
- 不正 AP の切り離し：不正 AP へのクライアント接続を阻止します。

図 4-24　不正な無線 AP の検出



電波 /RF 検出

AP RF 検出には、次の 2 つのモデルがあります。

- 標準の AP 配置
- 監視モード AP 配置

どちらの配置モデルも RF 検出をサポートしており、不正 AP だけでなく、アドホック クライアントと不正クライアント（不正 AP のユーザ）の検出に関する情報も収集できます。監視用として設定されている AP は RF チャネルのスキャンのみを行い、クライアント アソシエーションやデータ伝送はサポートしません。

不正 AP を探すため、LAP はチャネルを 50ms 間停止して不正クライアントの有無を調べ、ノイズとチャネル干渉を監視します。どのチャネルをスキャンするかは、802.11a および 802.11b/g のグローバル WLAN ネットワーク パラメータで設定します。不正なクライアントやアクセス ポイントが検出されると、その情報がコントローラに送信されます。コントローラが収集する情報は次のとおりです。

- 不正 AP の MAC アドレス
- 不正 AP の名前
- 不正接続しているクライアントの MAC アドレス
- フレームが WPA または WEP で保護されているかどうか
- プリアンブル
- 信号対雑音比（SNR）
- 受信信号強度表示（RSSI）

不正情報を受け取った WLC は、問題のクライアントまたは AP をすぐには不正と見なさず、他の AP からも同様の報告があるか、次の検出サイクルが完了するまで様子を見ます。同じ AP が再度同じチャネルに移動して、不正アクセス ポイント、不正クライアント、ノイズ、および干渉を監視します。同じクライアントまたはアクセス ポイントが検出された場合、WLC はそれらを不正と特定します。WLC は次に、その不正アクセス ポイントがローカル ネットワークに接続されているか、または単なる隣接 AP かを調べます。いずれの場合も、管理対象の Unified Wireless Network に属していない AP は不正と見なされます。

監視モードの AP はユーザ トラフィックを伝送せず、チャネル スキャン専用となります。ある特定の領域について WLAN サービスをサポートせず、不正 AP と不正クライアントの監視のみを行う場合は、通常、この配置モードを使用します。

位置特定

WCS の位置特定機能を使用すれば、不正 AP のおおよその位置を示すフロア図面を作成できます。この例を図 4-25 に示します。このフロア図面には、正規 AP の位置がすべて示されています。また、不正 AP の位置がどくろアイコンで強調表示されています。

Cisco Unified Wireless Location 機能の詳細は、http://www.cisco.com/en/US/products/ps6386/index.html を参照してください。

図 4-25　不正 AP マッピング

有線検出

AP が数台しかない支社のように、上記で説明した WCS 不正位置検出機能を利用できない場合もあれば、正確なフロア図面を入手できいない場合もあります。そのような場合に備え、Cisco Unified Wireless ソリューションには、「有線」ベースの検出オプションも 2 つ用意されています。

- 不正検出器 AP
- Rogue Location Discovery Protocol（RLDP; 不正ロケーション検出プロトコル）

AP が不正検出器として構成されている場合は、無線機能がオフになり、有線ネットワーク上で、不正 AP にアソシエートされているクライアント（つまり不正クライアント）の MAC アドレスをリッスンするという役割が与えられます。不正検出器は、これらの不正クライアントの MAC アドレスが含まれている ARP パケットをリッスンします。いずれかの ARP を検出すると、それを WLC に報告し、不正 AP が Cisco Unified Wireless Network と同じネットワークに接続されているかどうかを検証します。ARP 情報をすみやかに収集するには、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）ポートを使用して、不正 AP 検出器をすべてのブロードキャスト ドメインに接続しておく必要があります。複数の不正 AP 検出器を設置することで、一般的なネットワーク上に存在するさまざまなブロードキャスト ドメインに接続できます。

不正クライアントが無線ルータ（一般的な家庭用 WLAN デバイス）の背後に設置されている場合、有線ネットワークではそれらの ARP 要求を確認できません。したがって、不正検出器 AP に代わる方法が必要になります。さらに、（メイン キャンパス ネットワークのように）多数のブロードキャスト ドメインが存在する環境では、不正検出器 AP は実用的な対処方法とはいえません。

このようなときは RLDP オプションが役立ちます。この場合、不正 AP を検出するために、標準 LAP はクライアントとして不正 AP にアソシエートし、テスト パケットをコントローラに送信します。つまり、AP は標準 AP としての動作を停止し、一時的にクライアント モードに切り替わります。これによって、問題の不正 AP が実際にネットワーク上に配置されているかどうかを確認すると共に、ネットワーク上での不正 AP の論理的位置を示す IP アドレス情報を通知します。支社では位置情報を取得するのが難しいこと、また不正 AP が雑居ビルに設置されている可能性があることを考えると、不正 AP 検出器と RLDP は、ロケーションベースの不正 AP 検出を促進する有益な手段といえます。

不正 AP の阻止

不正 AP に接続しているクライアント、または不正なアドホック接続クライアントを阻止するには、近隣の LAP が 802.11 認証解除パケットを送信します。ただし、隣接 WLAN の正規 AP に認証解除パケットを送信するのは違法なので、その AP が本当に不正 AP であることを確認してからこの処理を行う必要があります。Cisco Unified Wireless Network ソリューションから不正 AP の自動阻止機能が削除されているのはそのためです。

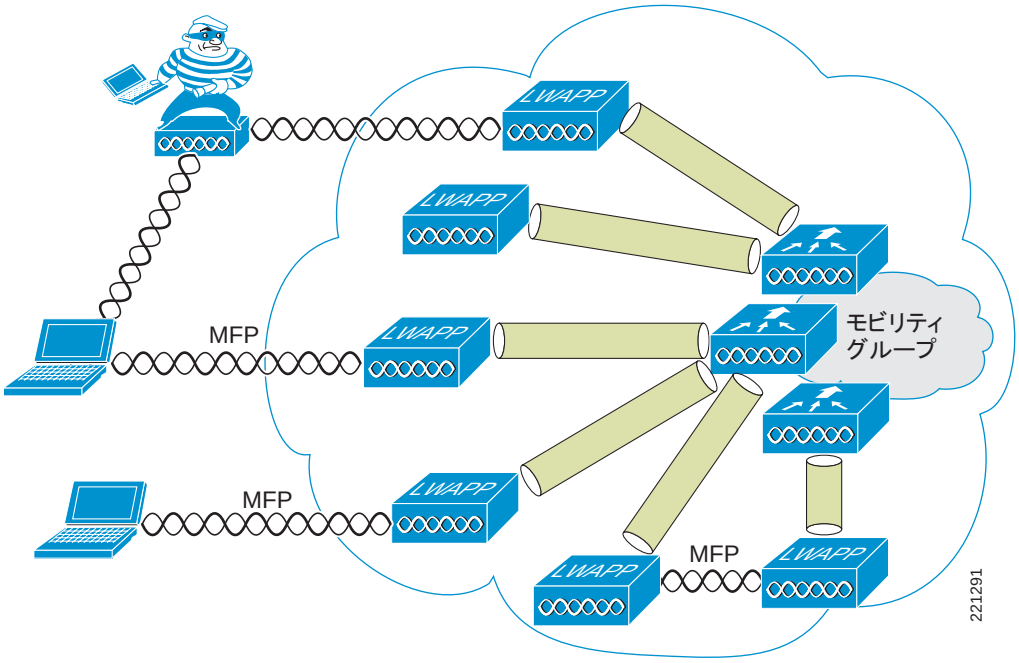
不正 AP クライアントがその企業の WLAN クライアントがどうかを確認するには、問題のクライアントの MAC アドレスと、802.1X 認証時に AAA が収集した MAC アドレスとを比較します。これによって、攻撃を受けている可能性のある WLAN クライアント、またはセキュリティ ポリシーに従っていないユーザを特定できます。

管理フレーム保護

802.11 の問題点の 1 つは、暗号化しない状態で管理フレームが送信され、メッセージ完全性チェックも実施されないので、スプーフィング攻撃を受けやすいということです。WLAN 管理フレームのスプーフィングは、WLAN ネットワーク攻撃で利用される危険性があります。この問題に対処するため、シスコは、802.11 管理フレームに Message Integrity Check（MIC; メッセージ完全性チェック）を挿入するデジタル シグニチャ メカニズムを開発しました。これによって、WLAN 展開の正規メンバを識別すると同時に、不正インフラストラクチャ デバイスを探し、有効な MIC がないことからスプーフィングされたフレームを突き止めることができます。

管理フレーム保護（MFP）で使用される MIC は、メッセージの単純な CRC ハッシュではありません。この MIC にはデジタル シグニチャ コンポーネントも含まれています。MFP の MIC コンポーネントはフレームが改ざんされていないことを保証し、デジタル シグニチャ コンポーネントは、MIC が WLAN ドメインの有効なメンバによってのみ生成されることを保証します。MFP で使用されるデジタル シグニチャ キーは、モビリティ グループ内のすべてのコントローラで共有され、グループごとに固有のキーが割り当てられます。したがって、同じモビリティ グループ内の各 WLC で、すべての WLAN 管理フレームを検証することができます。（図 4-26 を参照）。

図 4-26　管理フレーム保護



現在、インフラストラクチャ側とクライアントの両方で MEP が可能ですが、クライアントがモビリティ グループ MFP キーを判別し、無効なフレームを検出して拒否できるようにするには、Cisco Compatible Extensions v5 WLAN クライアントが必要です。

MFP には次のような利点があります。

- WLAN ネットワーク インフラストラクチャによって生成された 802.11 管理フレームを認証する
- 正規 AP の MAC または SSID をスプーフィングし、不正行為や Man-In-the-Middle 攻撃の発覚を免れようとする悪質な AP を検出できる
- 不正 AP および WLAN IDS シグニチャをより効率的に検出できる
- Cisco Compatible Extensions v5 を使用しているクライアント デバイスを保護できる
- バージョン 12.3(8)/v2.13 のスタンドアロン AP/WDS/WLSE でサポートされる

MFP を使用するには 2 つの手順が必要です。まず WLC 上で MFP を有効にし（図 4-27 を参照）、次に、モビリティ グループ内の WLAN で MFP を有効にします（図 4-28 を参照）。

図 4-27　コントローラでの MFP の有効化

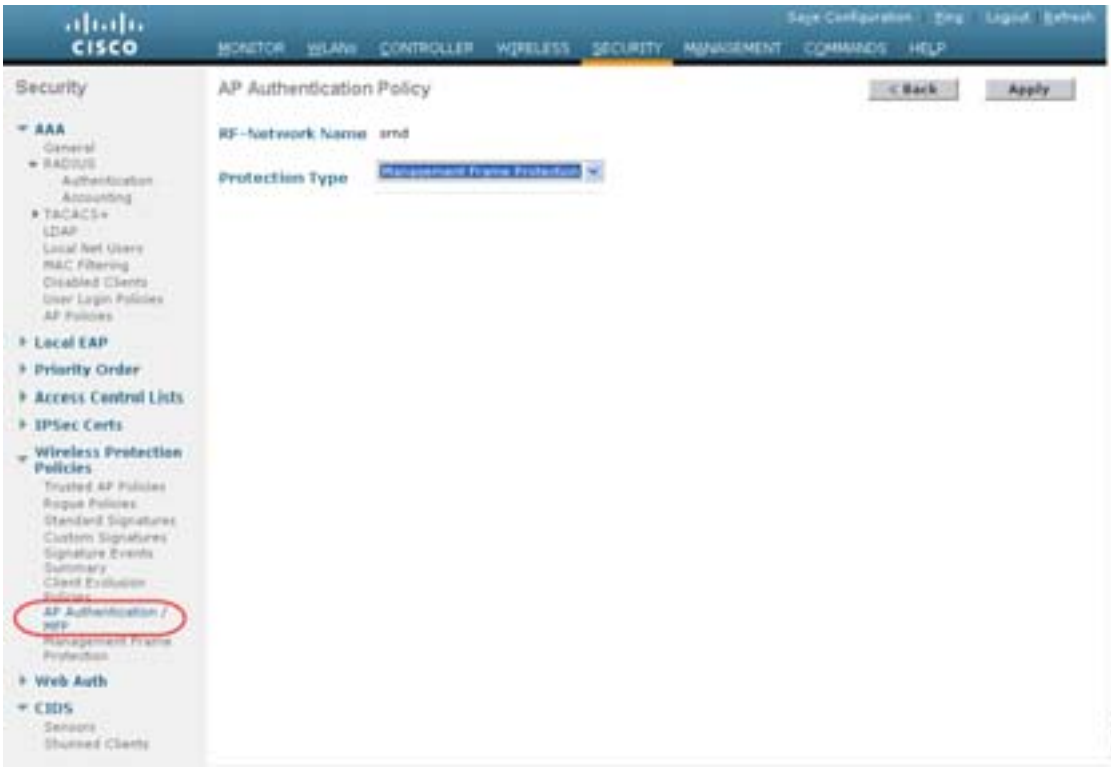
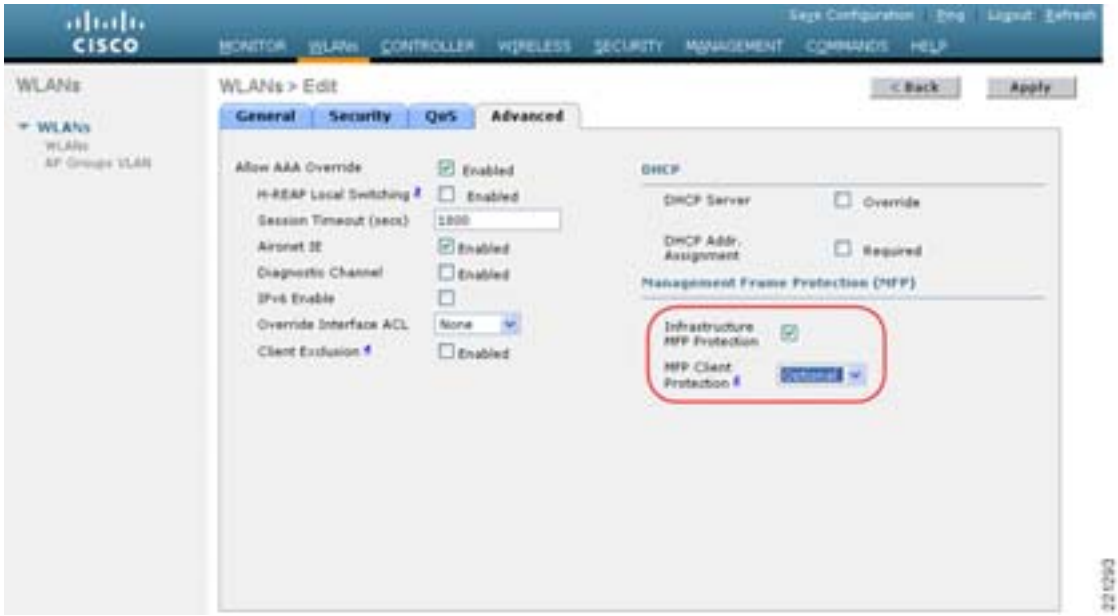


図 4-28　WLAN ごとの MFP の有効化



クライアントの管理フレーム保護

Cisco Compatible Extensions v5 WLAN クライアントは MFP をサポートします。図 4-28 に示すように、WLAN ごとに MFP を有効化できます。

WLAN クライアントに MFP を適用する方法は、基本的には AP の場合と同じです。つまり、管理フレームで MIC を使用します。これによって、信頼できる管理フレームをクライアントが識別できるようになります。WPA2 認証プロセスで、MIC 暗号キーがクライアントに渡されます。クライアント MFP は WPA2 でのみ使用できます。WPA クライアントと WPA2 クライアントが同じ WLAN を共有している場合は、クライアント MFP を Optional に設定する必要があります。

WCS のセキュリティ機能

不正 AP 検出のロケーション サポートとは別に、WCS にはさらに 2 つの Unified Wireless セキュリティ機能が備わっています。WLC 設定検証管理とアラーム報告インターフェイスです。

設定検証

WCS では、必要に応じて、または定期的に、設定監査レポートを生成できます。このレポートでは、現在の WLC 設定と、WCS データベースに保存されている既知の有効な設定の登録アクセス ポイントとを比較します。現在実行されている設定と、データベースに保存されている設定の間に相違が見つかった場合は、画面レポートとしてネットワーク管理者に通知されます（図 4-29 を参照）。

図 4-29　監査レポートの例

アラームとレポート

WLC で直接生成され、企業のネットワーク管理システム（NMS）に送信されるアラームとは別に、WCS もアラーム通知を送信することができます。コンポーネントによって送信されるアラームの種類が異なるのはもちろんですが、これらアラーム通知方式の違いはそれだけではありません。WLLC は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップを使用してアラーム（NMS システムのみが解釈可能）を送信します。一方 WCS は、Simple Mail Transfer Protocol（SMTP; 簡易メール転送プロトコル）E メールを使用して、アラーム メッセージを管理者に送信します。

WCS では、リアルタイム レポートと予約レポートの両方を生成できます。さらに、そのレポートをエクスポートしたり、E メールで送信することも可能です。レポート対象の項目は次のとおりです。

- アクセス ポイント
- 監査
- クライアント
- インベントリ
- メッシュ
- パフォーマンス
- セキュリティ

アーキテクチャ統合

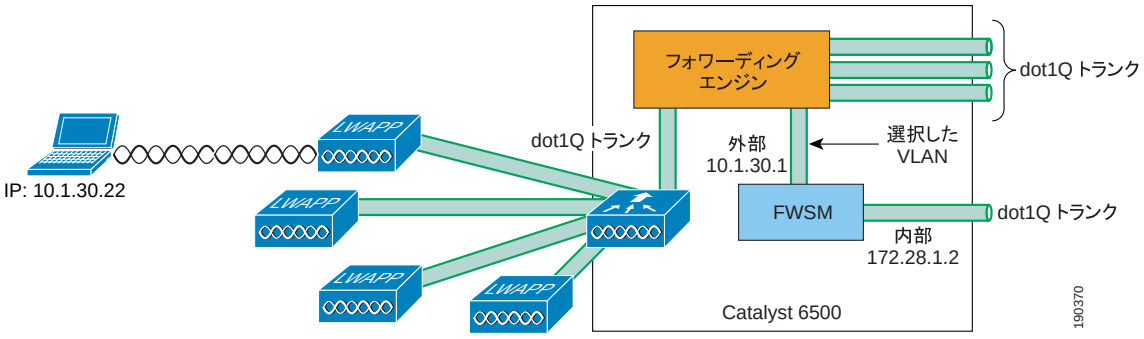
Cisco IOS、シスコのサービス モジュール、およびネットワーク モジュールには、さまざまな種類のセキュリティ サービスが統合されています。また、スタンドアロン アプライアンスやソフトウェアとしてもセキュリティサービスを提供しています。

Cisco Unified Wireless Network アーキテクチャは、WLAN クライアントと上流有線ネットワーク間のレイヤ 2 接続をサポートしているので、これらのセキュリティ サービスをソリューションへ簡単に統合できます。つまり、クライアント トラフィックの途中に配置する必要があるアプライアンスやモジュールを、WLAN クライアントと有線ネットワークの間に簡単に挿入することができます。たとえば、WLSM ベースの従来の環境の場合、WLAN クライアント トラフィックを Cisco Firewall Service Module（FWSM）経由でやり取りできるようにするには、Cisco 6500 上に VRF-Lite を実装する必要があります。一方、Cisco Unified WLAN 環境では、WiSM によって、（WLAN）クライアント VLAN が FWSM へ直接マッピングされます。Cisco Unified Wireless 製品で、レイヤ 2 の物理的または論理的なインターフェイスに WLAN トラフィックを直接マッピングできない WLAN コントローラは、ISR ベースの WLC モジュールだけです。ISR WLAN モジュールは、ISR に備わっているすべての IOS 機能と IPS 機能にアクセスできるわけではありません。WLAN クライアントからの IP トラフィックは、ルータの IOS VRF 機能を使用して、特定の ISR サービス モジュールへ中継する必要があります。

図 4-30 は、WiSM と FWSM モジュールのアーキテクチャ統合例を示しています。この例では、WLAN クライアントは、外部ファイアウォール インターフェイスと同じサブネットに配置されています。ルーティング ポリシーや VRF 設定を使用しなくても、WLAN クライアントの両方向のトラフィックをファイアウォール経由で送受信できます。

WLAN 環境に Cisco Network Admission Control（NAC; ネットワーク アドミッション制御）アプライアンス（以前の Cisco Clean Access）を取り入れれば、ネットワーク上のエンド デバイスが企業ポリシーに準拠しているかどうかを確認し、最新のセキュリティ ソフトウェア要件を満たしており、必要なシステム パッチを適用しているデバイスのみに接続を許可することができます。上記で説明した FWSM モジュールと同様、Cisco NAC アプライアンスも Cisco Unified Wireless Network アーキテクチャにレイヤ 2 で統合できます。したがって、NAC ポリシーの適用対象となる無線ユーザ VLAN を厳密に制御できます。

図 4-30　ファイアウォール モジュール統合の例



ネットワーク レイヤでの統合が容易なことに加え、Cisco Unified Wireless Network ソリューションを Cisco IDS 環境に統合すれば、Cisco IDS でブロックされたクライアントを Cisco Unified Wireless Network から除外することができます。

これらのソリューションの設計と設定、および Cisco Security Agent（CSA）の WLAN 機能については、
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns386/c649/ccmigration_09186a0080871da5.pdf の『Secure Wireless Design Guide 1.0』を参照してください。

Cisco Integrated Security Features

Cisco Catalyst スイッチに備わっている Cisco Integrated Security Features（CISF）は、ネットワークへ無線アクセスした不正ユーザからの攻撃を緩和します。ここでは、これらの攻撃、WLC がこれらの攻撃から保護する方法、CISF がアクセス スイッチで有効な場合にネットワークの保護にどのように役立つのかについて説明します。

（注） ここでは、アクセス スイッチ上で CISF が有効になっているときに阻止できる攻撃についてのみ説明します。無線ネットワーク上でのあらゆる攻撃を包括的に分析するものではありません。

攻撃の種類

攻撃は、有線ネットワークまたは無線ネットワークで発生します。ただし、無線ネットワーク接続の場合、ネットワークに物理的にアクセスしなくても攻撃が可能です。WLC および CISF には、攻撃を防ぐために特別に設計された機能が用意されています。

- MAC フラッディング攻撃
- DHCP 不正サーバ攻撃
- DHCP 消耗攻撃
  - ARP スプーフィング攻撃
  - IP スプーフィング攻撃

MAC フラッディング攻撃

MAC フラッディング攻撃は、スイッチの Content-Addressable Memory（CAM; 連想メモリ）テーブルをいっぱいにして、スイッチの処理能力を超える LAN トラフィックを発生させようとする攻撃手法です。この種の攻撃では、macof（dsniff パッケージの一部）などのツールを使用して、送信元と宛先の MAC アドレスおよび IP アドレスがランダムに割り当てられた大量のフレームが生成されます。

イーサネット スイッチのレイヤ 2 の学習メカニズムは、パケットの送信元 MAC アドレスに基づいています。ポートが新しい送信元 MAC アドレスを受信するたびに、ポートが属している VLAN のポートの CAM テーブル エントリをスイッチが作成します。スイッチにこれらのエントリを格納するために使用できる有限のメモリで考えた場合、通常、macof ユーティリティは 10 秒未満で CAM テーブルをいっぱいにします。CAM テーブルのサイズは限られています。他のエントリの期限が切れる前に CAM テーブルに大量のエントリが入力されると、CAM テーブルはいっぱいになり、新規エントリを受け付けられなくなります。

スイッチの CAM テーブルがいっぱいになると、次にトラフィックを受け取ったとき、CAM テーブルの特定の MAC アドレスに対応するポート番号を見つけられません。スイッチは本質的に、パフォーマンスおよびセキュリティに有害なハブのような役割を果たします。オーバーフローによってローカル VLAN 内のトラフィックが氾濫するため、接続先の VLAN 内のトラフィックを侵入者に見られます。

レイヤ 3 では、macof のターゲットとなったランダムな IP 宛先は、マルチキャスト アドレス空間も使用します。したがって、マルチキャストが有効になっているディストリビューション レイヤのスイッチでは、Protocol Independent Multicast（PIM）プロセスが偽のルートを処理しようとするときに、CPU 使用率が非常に高くなります。

DHCP 不正サーバ攻撃

DHCP 不正サーバ イベントは、意図的な攻撃の結果として発生すると場合と、ユーザがネットワーク セグメント上に DHCP サーバを誤って設置し、IP アドレスを発行し始めた結果である場合が考えられます。侵入者が DHCP サーバを起動し、DNS サーバまたはデフォルト ゲートウェイを表す IP アドレスを発行してユーザをだまし、自分の制御下にあるコンピュータにユーザ トラフィックをリダイレクトする可能性があります。

DHCP 消耗攻撃

DHCP 消耗攻撃は、特定のセグメント上の DHCP スコープ内のアドレスすべてを使い果たすことを目的としています。その結果、正規ユーザの IP アドレス要求が DHCP で拒否され、ネットワークにアクセスできなくなります。Gobbler は、DHCP 消耗攻撃を自動的に実行するパブリック ドメイン ハッキング ツールです。DHCP の消耗攻撃は、単純な DoS メカニズムであることもあれば、トラフィックを傍受するための悪意のあるコンピュータにトラフィックをリダイレクトする、悪意のある不正なサーバ攻撃と組み合わせて使用されることがあります。

ARP スプーフィングベースの Man-In-the-Middle 攻撃

Man-In-the-Middle（MIM）攻撃は、悪意のあるユーザがネットワークで移動中のデータを傍受（また、場合によっては変更）する、ネットワーク セキュリティ侵害です。たとえば、ARP スプーフィングを利用した MIM 攻撃では、余計な Address Resolution Protocol（ARP; アドレス解決プロトコル）要求を発行して攻撃用コンピュータにトラフィックを誘導します。その後、そのコンピュータは、特定の LAN セグメント上で実行される IP セッションに割り込んで不正行為を働きます。ARP スプーフィングでは、ettercap、dsniff、arpspoof などのハッキング ツールが使用されます。特に、Ettercap は特定の LAN セグメントのすべてのステーションを表示する高度なユーザ インターフェイスを持ち、さまざまな種類の IP セッションのパスワードを盗聴する組み込みのインテリジェント パケット盗聴機能が含まれています。

IP スプーフィング攻撃

IP スプーフィング攻撃は、別のユーザの IP アドレスで偽装して DoS 攻撃を実行します。たとえば、攻撃者は攻撃の際に別のユーザの IP アドレスを送信元としてサードパーティ システムに ping を実行します。ping の応答はサードパーティ システムの別のユーザに送信されます。

無線展開シナリオの CISF

ここでは、さまざまな unifies wireless 展開シナリオについて説明します。次のセクションでは、WLC 機能および CISF 機能が無線攻撃を阻止する仕組みを説明します。

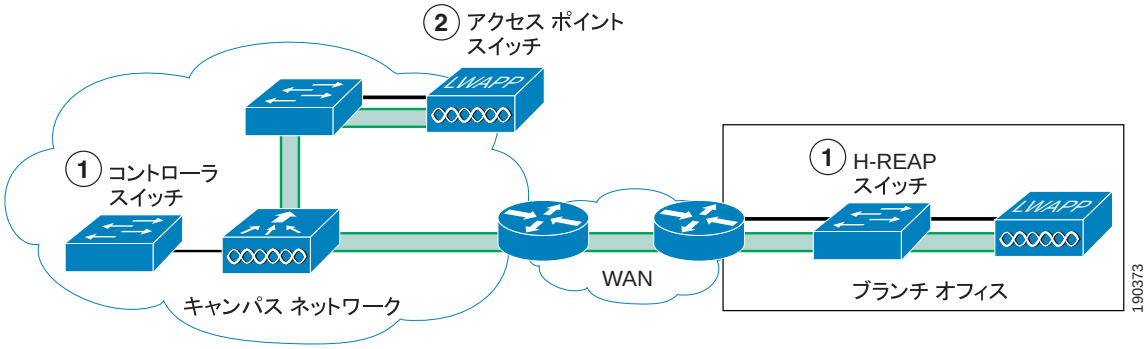
CISF は現在、Access Point（AP; アクセス ポイント）から直接利用することはできません。アクセス スイッチ上でだけ使用可能です。このため、これらの機能の利点は、トラフィックがスイッチ経由の無線攻撃者からである場合にだけ利用できます。

アクセス スイッチの定義は、次の 3 つの場所をアクセス スイッチと見なすことができるため、Unified Wireless ソリューションの定義とは若干異なります。

- ネットワークでコントローラ インターフェイスが終端するポイント
- ネットワーク上で標準 LAP が終端するポイント
- Hybrid Remote Edge Access Point（H-REAP; ハイブリッド リモート エッジ アクセス ポイント）がネットワークで終端するポイント

これらの位置は図 4-31 に示されています。

図 4-31　アクセス スイッチ



CISF に関係する接続は、コントローラ スイッチと H-REAP スイッチです。AP スイッチについては、WLAN トラフィックがこのスイッチで終端しておらず、AP はスイッチ ポートに接続している単一のデバイスとして存在しているだけであるため、ここでは取り上げません。AP スイッチは、セキュリティの面で考えると、アクセス クライアントとして見なされます。

（注） LAP と標準クライアントの大きな違いは、LAP の Differentiated Services Code Point（DSCP）値を信頼できる点です。

以下のシナリオは、無線ユーザ間の攻撃にのみ適用されます。無線ユーザと有線ユーザはそれぞれ別のサブネットでサポートされることを前提としており（シスコのベスト プラクティスで推奨）、サブネット間の攻撃は、ここでの説明の対象外となります。

次の 3 つのシナリオについて考えます。

- シナリオ 1：ターゲットがアソシエートされている AP が、攻撃者が接続されている AP と同じ場合
- シナリオ 2：ターゲットが攻撃者のものとは異なる AP にアソシエートされている場合
- シナリオ 3：ターゲットが攻撃者のものとは異なる AP にアソシエートされており、この AP が別のコントローラに接続されている場合

シナリオ 1 の場合、攻撃者とターゲットの両方が同じ AP にアソシエートされており、トラフィックは H-REAP または WLC にローカルです。したがって CISF は役に立ちませんが、Cisco Unified Wireless Networks のセキュリティ機能によってこれらの問題を解決できます。2 つ目および 3 つ目のシナリオは、CISF が有効なシナリオです。

複数レベルの認証が必要となる企業の WLAN 環境では、通常、1 つの SSID につき複数の VLAN を使用します。その場合、H-REAP AP または WLC のファスト イーサネット ポートと、アクセス スイッチ上の対応するポートとの間に、802.1q トランクを設定する必要があります。複数の VLAN を定義することで、データ トラフィックと、AP および WLC の管理トラフィックとを分離することができます。企業のセキュリティ ポリシーでユーザの種類ごとに異なる種類の認証および暗号化を使用する（ゲスト アクセスにはオープン認証を使用して暗号化は行わない、従業員には dot1x 認証と強力な暗号化を使用する、など）必要性も考えられます。これは、H-REAP AP または WLC 上で複数の SSID と VLAN を定義することで行えます。

上記のテスト構成では、WLC または H-REAP AP とアクセス スイッチの間でトランク接続を使用します。

CISF の無線機能

ここでは、無線攻撃の阻止を目的とする CISF の各機能について説明します。

MAC フラッディング攻撃を緩和するためのポート セキュリティの使用

ポート セキュリティは、ポートで許可される MAC アドレスの最大数を設定します。アドレスは、アドレス テーブルに手動で追加するか、動的に追加するか、または両方を組み合わせて追加することができます。アドレス テーブルの MAC アドレスの数が最大に達し、アドレス テーブルの MAC アドレスを持たないステーションがトラフィックを送信しようとすると、パケットがハードウェアにドロップされます。

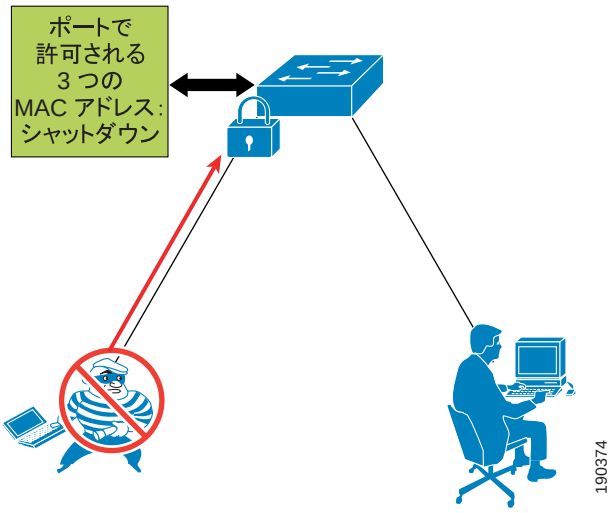
スイッチのアクセス ポートでポート セキュリティを有効にすると、そのポートを通過できる MAC アドレスの数が制限されるため、MAC フラッディングの発生を防げます。違反への応答が **shutdown** に設定されている場合、ポートはエラーで無効な状態になります。応答が **restrict** に設定されている場合、不明な送信元 MAC アドレスを持つトラフィックはドロップされます。

無線ネットワークにおけるポート セキュリティ

一般に、H-REAP AP または WLC に接続されたスイッチ ポート上でポート セキュリティを有効にすることは、お勧めしません。ポート セキュリティを使用するということは、スイッチがポートから学習し、許可する MAC アドレスの実際の数を把握するということです。H-REAP AP または WLC の場合、スイッチが学習するさまざまな送信元 MAC アドレスは、通常、無線ユーザに対応しています。スイッチ ポート上のポート セキュリティを設定すると、有線ネットワーク上の特定の数のユーザだけが許可されます。

たとえば、特定の MAC だけにアクセス ポイント経由でのトラフィックの送信を許可するセキュリティ ポリシーを設定できます。この場合、H-REAP AP または WLC の MAC フィルタリングとスイッチのポート セキュリティを組み合わせると、選択されたユーザだけが有線ネットワークにアクセスできるようになります。ただし、通常は、企業は 従業員のモビリティを促進するために WLAN を実装します。つまり、H-REAP AP または WLC にアソシエートされるユーザの数は、どのような状況においても事前に決められていません。したがって、AP に接続するユーザの数を判断できない状況では、スイッチ ポートのポート セキュリティを有効にしてもメリットはありません。それどころか、「違反が見つかったときにポートをシャットダウンする」ようにポートのセキュリティ ポリシーを設定している場合は、不本意な DoS 攻撃が発生する可能性があります。そうなると、その AP に接続しているすべてのユーザがネットワーク接続を失います。図 4-32 は、ポート セキュリティを使用して無線 MAC フラッディング攻撃を阻止する例を示しています。ここでは、ポートをロックして、SNMP トラップを送信しています。

図 4-32　ポート セキュリティの使用



ポート セキュリティの効果

（上記で説明したように）この攻撃を阻止する手段としてポート セキュリティが有効でないとしても、無線ユーザによる MAC フラッディング攻撃は成功しません。その理由は 802.11 プロトコルそのものにあります。AP とのアソシエーションは MAC ベースです。つまり、AP は、既知のユーザ（既知の MAC）との間でのみトラフィックを送受信します（トランスレーショナル ブリッジ）。MAC フラッディング攻撃が無線ユーザから起動された場合、AP にアソシエートされていないランダムな送信元 MAC アドレスを持つ 802.11 フレームはすべてドロップされます。許可される唯一のフレームは、おそらくスイッチがすでに学習している、悪意のあるユーザの MAC を持つフレームです。したがって、アクセス ポイント自身の基本的な動作によって、スイッチが MAC フラッディング攻撃を受けるのを防ぎます。

DHCP 消耗攻撃を緩和するためのポート セキュリティの使用

有線アクセスに関しては、スイッチに接続している PC が Gobbler などのツールを利用して DHCP 消耗攻撃をしかけてきた場合、ポート セキュリティで事前に阻止できます。ただしこれは、ポート セキュリティによって攻撃が緩和されたというよりも、攻撃ツール自体の制約に大きく起因しています。こうした攻撃が失敗する唯一の理由として、Gobbler は、送信元 MAC アドレスを使用して DHCP 要求を生成することがあげられます。したがって、ポート保護による軽減が可能です。

しかし、攻撃者がイーサネット パケットで MAC アドレスを使用し、その MAC アドレスを DHCP ペイロード（chaddr フィールド）で変更した場合は、ポート セキュリティで攻撃を阻止できません。現在実行できるのは、スイッチ ポートの DHCP レート リミッタを使用して攻撃を遅らせることだけです。

無線 DHCP 消耗攻撃

Unified Wireless 展開では、DHCP 消耗攻撃に対する脆弱性は、ユーザ トラフィックを WLC と H-REAP のどちらが終端させるかによって異なります。

WLC は、クライアントの MAC アドレスが chaddr と一致することを確認するために DHCP 要求を検証するので、DHCP 消耗攻撃からネットワークを保護します。アドレスが一致しない場合は、DHCP 要求はドロップされます。

H-REAP の場合、ユーザ VLAN がローカルで終端すると、DHCP 要求がコントローラに送られず、chaddr を解析できません。このアクセス方法にも、有線アクセスと同様のセキュリティ考慮事項が適用されます。賢い（無線）攻撃者は、AP にアソシエートされている MAC アドレスを使用してランダムな DHCP 要求を生成し、DHCP パケット ペイロード内の要求 MAC アドレスだけを変更します。送信元 MAC と、AP へのアソシエート時に使用された MAC が同じなので、AP はこのパケットを有効と見なしてしまいます。

不正 DHCP サーバ攻撃を緩和するための DHCP スプーフィングの使用

DHCP スヌーピングは、DHCP スヌーピング バインディング テーブルを構築して管理し、信用できない DHCP メッセージをフィルタすることで、セキュリティを提供する、DHCP のセキュリティ機能です。これは、エンド ユーザに接続された信頼できないインターフェイスと、DHCP サーバまたは他のスイッチに接続された信頼できるインターフェイスとを区別することで行われます。エンド ユーザのポートは、DHCP 要求だけの送信に制限され、その他の種類の DHCP トラフィックは送信できません。信頼できるポートでは、DHCP メッセージの転送はすべて許可されます。DHCP スヌーピング テーブルは VLAN ごとに作成され、クライアントの IP アドレス /MAC アドレスを信頼できないポートに結び付けます。DHCP スヌーピングを有効にすることで、ユーザが認証されていない DHCP サーバから信頼できない（ユーザ側の）ポートに接続して DHCP 要求への応答を開始するのを防ぎます。

無線アクセス用の DHCP スヌーピング

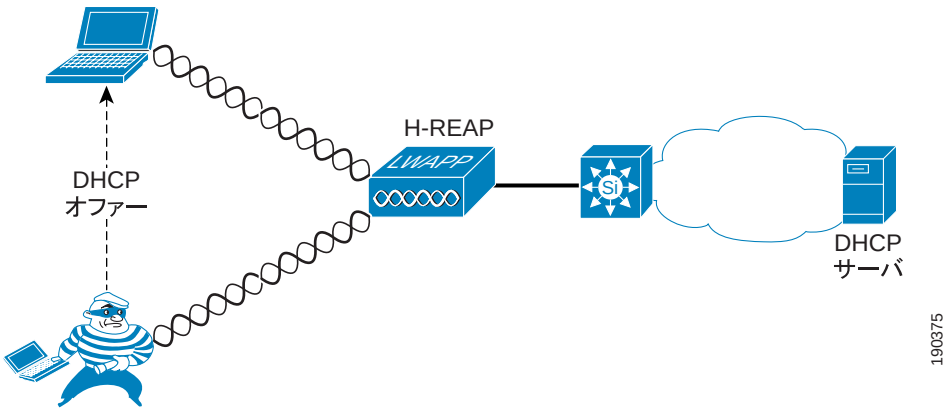
WLC はクライアントからのすべての DHCP 要求を管理し、DHCP リレー エージェントとして機能します。WLAN クライアントからの DHCP 要求は、同じ WLAN にブロードキャストされません。WLC から DHCP サーバへユニキャストされます。これにより、WLC に接続している他の WLAN クライアントを、不正な DHCP サーバ攻撃から保護できます。

H-REAP 802.1q トランク インターフェイス経由で VLAN に接続しているクライアントは、不正な DHCP サーバ攻撃から保護されません。

CISF 機能（この場合は DHCP スヌーピング）は、AP ではなくスイッチに実装されていることに注意してください。つまり、トラフィックがスイッチを経由する場合のみ、不正サーバからの悪質なメッセージがスイッチで捕捉されます。

図 4-33 は、DHCP スヌーピングを使用して、不正な DHCP サーバ攻撃を緩和する例と、スイッチが DHCP 保護を提供する前に攻撃が発生する仕組みについて示しています。

図 4-33　不正な DHCP サーバ攻撃に対して使用されるセキュリティ



DHCP スヌーピングの効果

DHCP スヌーピングは VLAN ごとに有効にできるので、トランク ポートで機能します。異なる VLAN のクライアントに対して、トランク ポートで受け取った DHCP 要求にそれぞれ異なる DHCP スヌーピング エントリが挿入されます。DHCP スヌーピングがトランク ポート上で機能するという事実は非常に重要です。これによって、H-REAP のローカル インターフェイス上で複数の SSID または VLAN が設定されている場合でも、WLAN 環境に CISF 機能を適用できます。攻撃者がターゲットと同じ WLAN/VLAN に接続している場合でも、H-REAP が異なれば、スイッチは DHCP スプーフィング攻撃を阻止できます。ただし、攻撃者とターゲットが同じ H-REAP にアソシエートされている場合、攻撃はスイッチを経由しないため検出されません。

DHCP スヌーピングは、DHCP サーバへの DHCP 要求をレート制限することで、DHCP サーバ攻撃から保護することもできます。

Man-In-the-Middle 攻撃を緩和するための Dynamic ARP Inspection（DAI）の使用

アクセス スイッチで、VLAN ごとに Dynamic ARP Inspection（DAI）を有効にします。DAI は、gratuitous ARP（GARP）を含めた ARP 要求／応答と、DHCP スヌーピングによって DHCP バインディング テーブルに挿入された MAC/IP エントリを比較します。スイッチが、DHCP バインディング テーブルのエントリと一致しない ARP メッセージを受け取ると、パケットは無効化され、ログ メッセージがコンソールに送信されます。DAI は ARP 汚染攻撃を防ぎます。この攻撃によってターゲットの ARP テーブルが改ざんされると、ettercap を利用した MIM 攻撃につながる可能性があります。ARP メッセージは、攻撃者が接続されているポートで直接フィルタされます。

無線アクセス用の DAI

WLC は、WLC 自体で DAI と似ている機能を実行することで、MIM 攻撃を防ぎます。WLC に直接接続している VLAN では、アクセス スイッチ上で DAI を有効にしないでください。WLC では GARP を使用して、レイヤ 3 クライアント ローミングをサポートします。

H-REAP とアクセス スイッチ間のトランク上で構成されている VLAN ごとに DAI を有効にできます。したがって、H-REAP に複数の SSID/VLAN が存在する無線環境では DAI が役立ちます。ただし、H-REAP 展開では、DAI 機能の有効性に影響を与える 2 つの状況が考えられます。次のシナリオは、攻撃者が H-REAP にアソシエートしており、攻撃相手にレイヤ 2 で隣接していることを前提としています。

- シナリオ 1：一方のターゲットは無線で、攻撃者と同じ AP にアソシエートされており、もう一方のターゲットはデフォルト ゲートウェイ。最も一般的な攻撃方法です。
- シナリオ 2：両方のターゲットが無線。

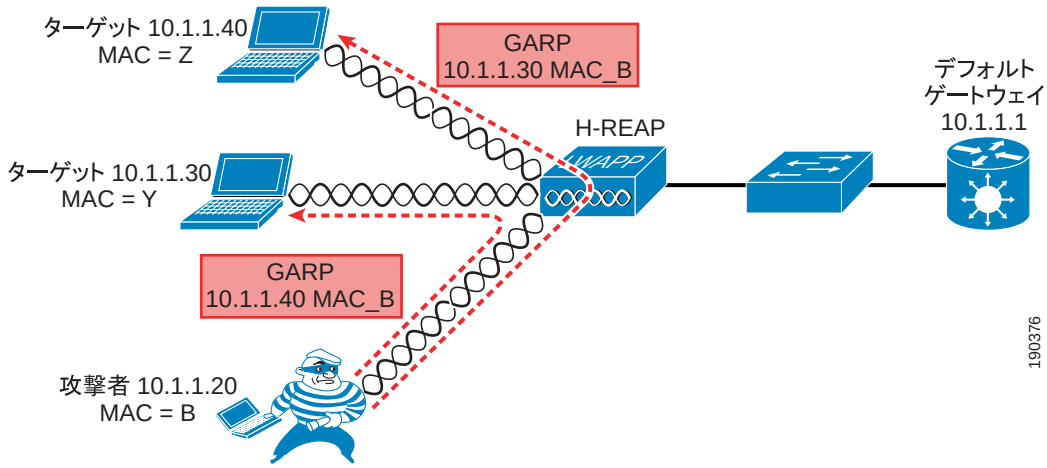
これらの 2 つのシナリオから、どのような場合にトラフィックがスイッチを経由して停止されるかがわかります。

シナリオ 1 の MIM 攻撃は、GARP を使用して、デフォルト ゲートウェイおよび無線ターゲット上の ARP テーブル エントリを変更し、トラフィックを攻撃者にリダイレクトしようといいうものです。DAI によってデフォルト ゲートウェイの GARP は阻止できますが、スプーフィングされた無線クライアントの GARP には何も作用しません。このように、MIM 攻撃の威力が多少は軽減されますが、完全に防ぐことはできません。

シナリオ 2 では、MIM 攻撃は GARP を無線クライアントに送信しますが、DAI を実装しているスイッチはこれらの GARP を認識しないため、攻撃をブロックできません。

図 4-34 は、サブネット上の 2 つの IP 接続ノード間のトラフィックを転送するために、これらのノードに GARP が送信される攻撃メカニズムの例を示しています。

図 4-34　Dynamic ARP Inspection



DAI の効果

図 4-34 に示すように、攻撃が完全に成功するのは、トラフィックが終始 H-REAP で処理され、スイッチを経由しない場合だけです。通常、攻撃者が狙っているトラフィック（パスワードやアカウント情報など）は無線クライアントから有線ネットワーク（サーバまたはインターネット）へ伝送されるので、それほど危険ではありません。

デフォルト ゲートウェイと無線クライアントが攻撃ターゲットとなるこのシナリオは、「半二重の MIM 攻撃」といえます。Ettercap は、現在すべてのトラフィックを侵入者に送信している無線ユーザの ARP テーブルを変更できますが、デフォルト ゲートウェイに対する GARP は、次の例に示すように、スイッチによって傍受され、メッセージはログに記録されます。

```
4507-ESE#sh ip arp inspection log
Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Wed Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Feb 3 2003) DHCP
Deny
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:49 PDT Tue Feb 3 2003) DHCP Deny
```

ログには MAC アドレスが記録されているため、管理者は攻撃者のアソシエーションを解除することで、攻撃を阻止する処置を取ることができます。

VLAN で DAI が設定されている場合は、特定のポートから送られる ARP 要求の氾濫を防ぐために、ARP レート リミッタがグローバルに設定されます。レート リミッタのデフォルト値は、15 パケット / 秒（pps）です。この制限を超えると、スイッチは攻撃を防ぐためにポートを無効にします。この場合、MIM 攻撃を起動するには、攻撃者はまずレイヤ 2 で隣接しているユーザを探す必要があります。そのためには、ettercap が一連の GARP を生成し、サブネット上の各 IP アドレスに要求します。このようにして、アドレスの実際の所有者が応答すると、ettercap はテーブルを作成します。

実験を行ったところ、ettercap を実行するとすぐにこの制限に達し、ポートはシャットダウンされました。これは有線シナリオでは受け入れられますが、無線シナリオの場合は、AP に接続されているポートをシャットダウンすると、すべての無線ユーザが外部との接続を失い、潜在的な MIM 攻撃が DoS 攻撃へと変わります。

（DAI を有効にすると発生する）この潜在的な DoS を防ぐため、AP に接続しているスイッチのポートでは ARP レート リミッタを無効にすることをお勧めします。無効にするには、次のインターフェイス レベル コマンドを使用します。

```
ip arp inspection limit none
```

または、しきい値を 15pps よりも大きい値に変更するという方法もあります。ただし、これは、攻撃の起動に使用される特定のツールの実装によって異なるため、一般的な対処方法ではありません。

IP および MAC スプーフィングを緩和するための IP Source Guard の使用

アクセス スイッチのインターフェイス上で有効にした場合、IP Source Guard は DHCP スヌーピング バインディング テーブルの内容に基づいて、Per-port Access Control List（PACL）を動的に作成します。この PACL は、DHCP バインディング タイムで発行された IP アドレスからトラフィックが送信されるように強制し、他の偽装したアドレスでトラフィックが転送されないようにします。これは、手動でアドレスを変更したり、hping2 のようなアドレス スプーフィングを行うよう設計されたプログラムを実行して、攻撃者が有効なアドレスになりすますのも防ぎます。この機能には、着信アドレスをフィルタするオプション（ポート セキュリティ）があります。この場合も、DHCP スヌーピング バインディング テーブルの MAC アドレスを使用します。

攻撃者は通常、実際の自分の身元を隠すために偽のアドレスを使用して、ターゲットに対する DoS 攻撃などの攻撃を起動します。

無線アクセス用の IP Source Guard

無線アクセスの場合、アクセス スイッチを H-REAP に接続しているトランク ポート上で IP Source Guard を有効にします。これにより、DHCP バインディング テーブルのエントリと一致しない無線ユーザから送られたトラフィックをスイッチでフィルタできるようになります。

WLC の背後に配置されている VLAN では IP Source Guard を有効にする必要がありません。WLC にも同様の機能が備わっており、クライアントが使用している IP アドレスと、そのクライアントに割り当てられている IP アドレスが同じかどうかが確認されます。

（標準の LAP と異なり）H-REAP では WLAN クライアントの MAC-IP アドレス バインディング関係をチェックできないので、H-REAP 展開では IP Source Guard が役に立ちます。

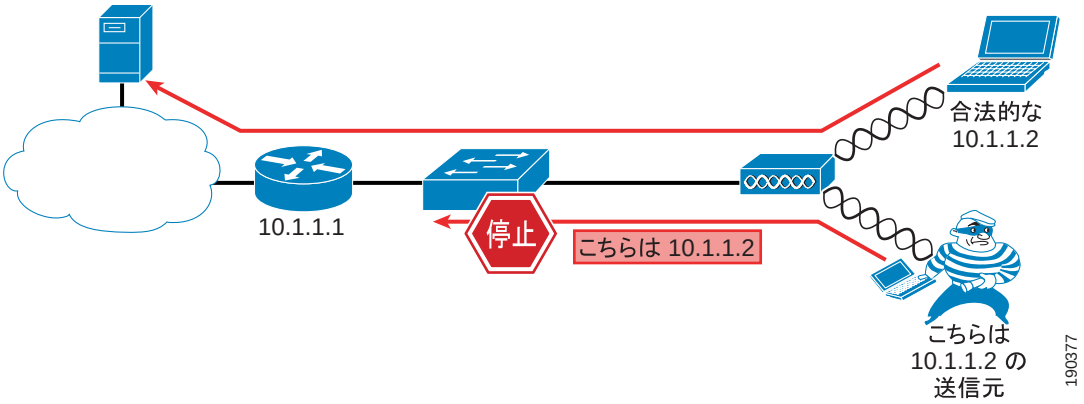
テストでは、次の 2 つのシナリオについて考えました。

- シナリオ 1：ターゲットは、同じ AP にアソシエートされている別の無線ユーザによって表されます。

- シナリオ 2：ターゲットは、別の AP にアソシエートされている別の無線ユーザです。

図 4-35 は IP Source Guard を使用して IP および MAC スプーフィング攻撃を緩和する例を示しています。

図 4-35　IP Source Guard による MIM の阻止



IP Source Guard の効果

この機能の有効性は、攻撃者がどのような手段でアドレスをスプーフィングするか、およびどのような状況を想定するかによって異なります。

AP へのアソシエーションはクライアント MAC アドレスに基づいて行われるので、受信したフレームに不明な送信元アドレスが含まれている場合、AP はそのフレームを破棄します。IP スプーフィング攻撃を起動するとき、攻撃者は、自分の MAC アドレスを使用するか、または、同じ AP に接続された別のユーザの MAC アドレスを使用します。ランダムな MAC アドレスを使用したり、別の AP に接続されているユーザの MAC アドレスを使用するなど、その他すべての組み合わせの場合は、AP がフレームを破棄するため、攻撃は失敗に終わります。

MAC アドレスは攻撃者自身のものであり、IP アドレスのみが偽装された場合、スイッチ上で IP Source Guard を有効化することにより、2 番目のシナリオではすべての攻撃を阻止できます。しかし、トラフィックが常に AP を経由する最初のシナリオでは、CISF 機能が適用されないので、攻撃を阻止できません。その他のシナリオでは、CISF によって攻撃が阻止されます。これは、攻撃者が送信してきたパケットでは IP が偽装されており、DHCP スヌーピング テーブルに登録されていないためです。

ただし、攻撃者が、同じ AP に接続している正規無線ユーザの MAC アドレスと IP アドレスを両方とも偽装した場合、攻撃者はその正規ユーザと見なされるので、どちらのシナリオでも攻撃は成功します。

ホットスポット環境で暗号化を使用していない場合や、WEP の脆弱性が悪用された場合は、MAC アドレスと IP アドレスの両方を偽装される危険性があります。できる限り強力な暗号化を使用してください。

結果の要約

テストの結果は、表 4-4 に示すとおりです。

表 4-4　テスト結果

ターゲットとされた攻撃	適用可能性	考慮事項	ソリューション
MAC フラッディング	なし	Macof が送信元および宛先としてランダムな MAC アドレスを使用	AP はアソシエーション テーブルにない送信元 MAC からのフレームを破棄
DHCP 消耗	H-REAP では可 コントローラが不正な DHCP 要求を破棄	MAC の要求は DHCP ペイロードへ送られる	なし（レート制限）
不正な DHCP サーバ	H-REAP では可 コントローラが WLAN からの DHCP オファーをブロック	不正な DHCP サーバは無線であることが前提	なし
無線クライアント間の MIM	H-REAP では可 コントローラが GARP をブロック	この場合トラフィックはスイッチを経由しない	なし
別の AP 上の無線クライアント間の MIM	H-REAP では可 コントローラが GARP をブロック	ハッカーはケーブルに向けて送られるトラフィックだけ傍受可能	違反 DAI
無線クライアントと有線クライアント間の MIM	H-REAP では可 サポートされているコントローラ構成ではない	ハッカーはケーブルに向けて送られるトラフィックだけ傍受可能	違反 DAI
IP スプーフィング	H-REAP では可 コントローラが IP アドレスと MAC アドレス バインディングをチェック	ID スプーフィングを防ぐには、地上波の暗号化が必要	IP Source Guard

テストを行ったのは、有線アクセス上の CISF 機能によってターゲットとされた攻撃だけで、攻撃者が無線である可能性も常に考慮されています。ターゲットはシナリオによっては、有線の場合もあれば無線の場合もあります。最後に、表 4-4 に記載されているソリューションは、アクセス スイッチ上の CISF 機能で現在利用可能なものを示しています。これらの機能が役に立たない場合は、アクセス ポイントで直接利用できる機能を使用した別のソリューションをお勧めします。

参照資料

- Deploying Cisco 440X Series Wireless LAN Controller
  http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html
- Cisco Wireless LAN Controller Configuration Guide, Release 4.1
  http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html
- Cisco Wireless Control System Configuration Guide, Release 4.1
  http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/ccfig41.html

CHAPTER 5

Cisco Unified Wireless QoS

この章では、WLAN 実装の QoS（Quality of Service）について説明します。ここでは WLAN QoS 全般について説明します。セキュリティ、セグメンテーション、および Voice over WLAN（VoWLAN）などのトピックにも QoS コンポーネントが含まれますが、これらのトピックについてここでは詳しく取り上げません。また、Cisco Centralized WLAN アーキテクチャの機能についても説明します。

この章は、Cisco Unified Wireless テクノロジーを使用して企業の WLAN 展開の設計および実装に取り組んでいるユーザを対象としています。

QoS の概要

QoS とは、さまざまなネットワーク テクノロジーを介して、選択されたネットワーク トラフィックにディファレンシエーテッド サービスを提供するネットワークの機能のことです。QoS テクノロジーには、次の利点があります。

- キャンパス、WAN、およびサービス プロバイダ ネットワークで使用されるビジネス マルチメディアおよび音声アプリケーションに基盤を提供します。
- ネットワーク マネージャは、ネットワーク ユーザに対してサービス レベル契約（SLA）を制定できます。
- ネットワーク リソースをさらに効率的に共有でき、ミッションクリティカルなアプリケーションの処理を効率化します。
- 時間依存型マルチメディアおよび音声アプリケーションのトラフィックを管理し、このトラフィックがベストエフォート型のデータ トラフィックよりも優先度が高く、帯域幅が大きく、かつ遅延が少なくなるようにします。

QoS を使用して、WLAN および WAN などの LAN 全体で帯域幅をより効率的に管理できます。QoS により、次の点で拡張された、信頼性のあるネットワーク サービスが提供されます。

- 重要なユーザおよびアプリケーションに対する専用の帯域幅のサポート
- ジッタおよび遅延の制御（リアルタイムのトラフィックで必要）
- ネットワーク輻輳の管理および最小化
- トラフィック フローを円滑化するネットワーク トラフィックのシェーピング
- ネットワーク トラフィックの優先度の設定

Wireless QoS の展開方式

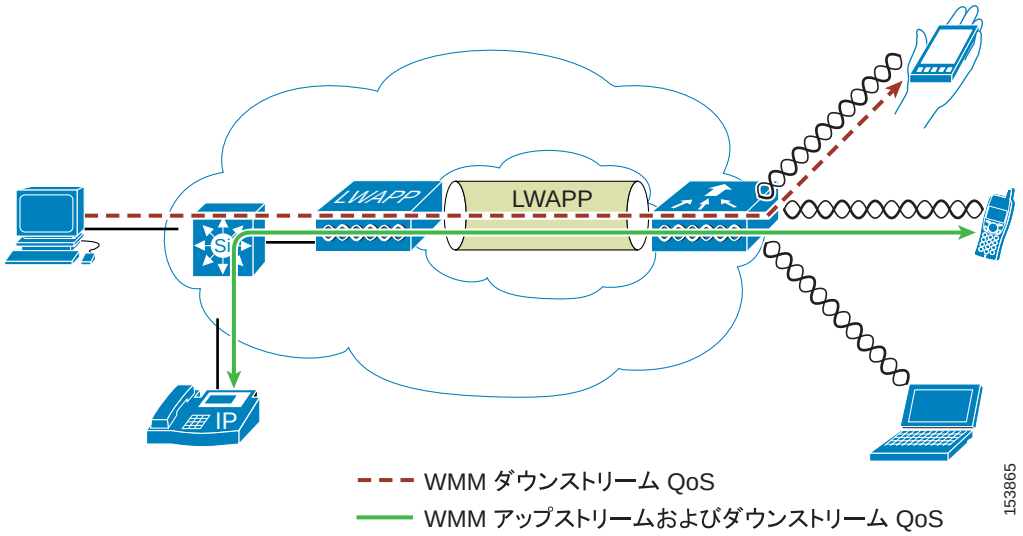
従来、WLAN は主に低帯域幅のデータ アプリケーション トラフィックの伝達に使用されていました。現在では、WLAN は縦方向の環境（小売、金融、教育など）および企業環境に拡張され、時間依存型のマルチメディア アプリケーションと共に高帯域幅のデータ アプリケーションの伝達に使用されています。この要件に対応するために、無線 QoS が必要になりました。

シスコを含む複数のベンダーでは、音声アプリケーション対応の専用無線 QoS 方式をサポートしています。QoS の導入速度を速め、複数のベンダーの時間依存型アプリケーションに対応するには、無線 QoS に対する統一手法が必要です。IEEE 802.11 標準化委員会内の IEEE 802.11e グループにより、標準の定義は完了しています。しかし、802.11e 規格の採択は初期段階にあり、多くの標準と同じく、多数の任意の選択要素があります。802.11i の 802.11 セキュリティ規格の際と同様、Wi-Fi Alliance などの業界グループおよびシスコのような業界トップのメーカーは、認証プログラムを使用して主要な機能や互換性を確実に備えられるよう、WMM プログラムおよび Cisco Compatible Extensions プログラムを介して WLAN QoS の主要な要件を定義しています。

Cisco Unified Wireless 製品は、Wi-Fi Alliance が発表した IEEE 802.11e に基づく QoS システムである Wi-Fi MultiMedia（WMM）、WMM Power Save、および WMM Admission Control をサポートしています。

図5-1 は、Cisco Unified Wireless テクノロジーの機能に基づく Wireless QoS の展開例を示しています。

図 5-1　QoS の展開例



QoS パラメータ

QoS は、通信の質およびサービスの可用性を反映した通信システムのパフォーマンスの基準として定義されています。サービスの可用性は、QoS の重要な要素です。QoS を正常に実装するには、ネットワーク インフラストラクチャがどのような状況下でも使用可能でなければなりません。ネットワークの通信の質は、遅延、ジッタ、および損失で決まります（表 5-1 を参照）。

表 5-1　QoS パラメータ

通信の質	説明
遅延	遅延とは、パケットが送信エンドポイントから伝送されて受信エンドポイントへ到達するまでにかかる時間を意味します。この間隔は、エンドツーエンド遅延と呼ばれ、次の 2 つの領域に分けることができます。 • 固定ネットワーク遅延 — 符号化および復号化の時間（音声およびビデオ）、および電気パルスまたは光パルスがメディアを通過して送信先へ届くまでの限られた時間が含まれます。 • 可変ネットワーク遅延 — 通常、伝送に必要な時間全体に影響を及ぼす可能性のあるキューイングや輻輳などのネットワークの状態を意味します。
ジッタ	ジッタ（遅延差異）は、パケット間のエンドツーエンド遅延の差です。たとえば、あるパケットが発信エンドポイントから送信先エンドポイントまでネットワークを通過するのに 100 ms かかり、次のパケットでは同じ伝送に 125 ms かかる場合、ジッタは 25 ms となります。
損失	損失（パケットの損失）は、伝送された総数が正常に送受信された場合のパケットの比較基準です。損失は、ドロップしたパケットの割合で示されます。

アップストリームおよびダウンストリーム QoS

図 5-2 は、*無線アップストリーム*および*ダウンストリーム* QoS の定義を示しています。

図 5-2　アップストリームおよびダウンストリーム QoS

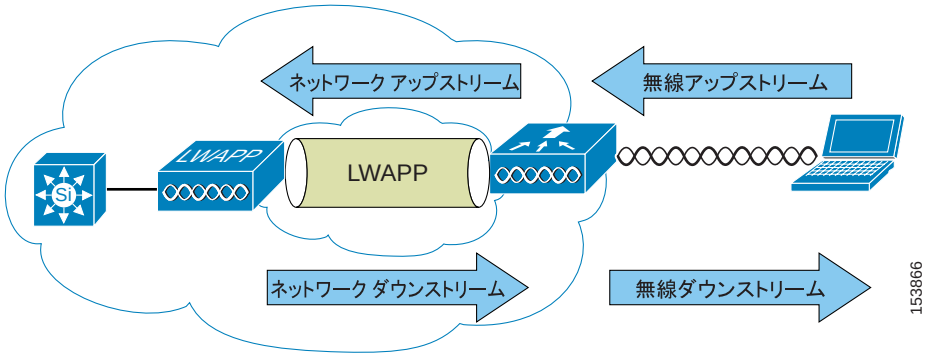


図 5-2 は、以下について示しています。

- *無線ダウンストリーム* QoS — AP から発信され WLAN クライアントまで伝送されるトラフィック。無線ダウンストリーム QoS が今なお最も一般的な展開であるため、この章で最も重要な焦点となっています。クライアントの無線アップストリーム QoS は、クライアントの実装によって異なります。

- *無線アップストリーム* QoS ― WLAN クライアントから発信され AP まで伝送されるトラフィック。WMM では、WMM をサポートする WLAN クライアントのアップストリーム QoS が提供されます。
- *ネットワーク ダウンストリーム* ― WLC から発信され AP まで伝送されるトラフィック。この時点で QoS を適用して、AP へのトラフィックの優先順位付けとレート制限を行えます。イーサネットのダウンストリーム QoS の設定は、この章では取り上げません。
- *ネットワーク アップストリーム* ― AP から発信され WLC まで伝送されるトラフィック。AP は、その AP のトラフィック分類ルールに従って、AP からアップストリーム ネットワークまでのトラフィックを分類します。

QoS およびネットワークのパフォーマンス

QoS 機能の適用は、負荷の軽いネットワークでは容易に検出されないことがあります。メディアの負荷が軽いときに遅延、ジッタ、および損失が顕著な場合、それはシステム障害、ネットワーク設計の不備、またはアプリケーションの遅延、ジッタ、および損失の要件がネットワークと適合していないことを示しています。ネットワークの負荷が増大するにつれて、QoS 機能がアプリケーションのパフォーマンスに作用し始めます。QoS は、選択されたトラフィック タイプに対する遅延、ジッタ、および損失を許容できる限度内で維持するように作用します。AP から無線ダウンストリーム QoS のみが提供される場合、無線アップストリームのクライアント トラフィックはベストエフォートと認識されます。クライアントは、AP からのベストエフォート伝送に対しても、またアップストリーム伝送に対しても他のクライアントと競合します。特定の負荷状況下では、クライアントにアップストリームの輻輳が発生し、AP で QoS 機能を適用しても、QoS 依存型アプリケーションのパフォーマンスが許容不可能なまでに低下することがあります。理想的にアップストリームおよびダウンストリーム QoS を操作するには、AP と WLAN クライアントの両方で WMM を使用するか、WMM およびクライアントの独自の実装を使用します。

（注） WLAN クライアント上で WMM のサポートがなくても、Cisco Unified Wireless ソリューションはネットワークのアップストリームとダウンストリームの両方でネットワークの優先順位を付けることができます。

（注） WLAN クライアントの WMM へのサポートは、クライアント トラフィックが自動的に WMM の恩恵を得ているという意味ではありません。WMM の利点を求めるアプリケーションが適切な優先度の分類をそのトラフィックに割り当て、オペレーティング システムはその分類を WLAN インターフェイスに渡す必要があります。VoWLAN 端末などの専用デバイスでは、設計の一部としてこの機能があります。しかし、PC のような汎用プラットフォームに実装する場合、WMM 機能からよい結果を得るにはアプリケーション トラフィックの分類と OS のサポートを実装しておく必要があります。

802.11 DCF

802.11 のデータ フレームは、Distributed Coordination Function（DCF; 分散コーディネーション機能）を使用して送信されます。DCF は次の 2 つの主要コンポーネントで構成されています。

- フレーム間スペース（SIFS、PIFS、および DIFS）。
- ランダム バックオフ （コンテンション ウィンドウ）。DCF を 802.11 ネットワークで使用して RF メディアへのアクセスを管理します。

802.11e ベースの Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）を展開するには、DCF の基本的な理解が必要です。DCF の詳細は、次の URL で IEEE 802.11 の仕様を参照してください。http://ieeexplore.ieee.org/xpl/standardstoc.jsp?isnumber=14251&isYear=1997

フレーム間スペース

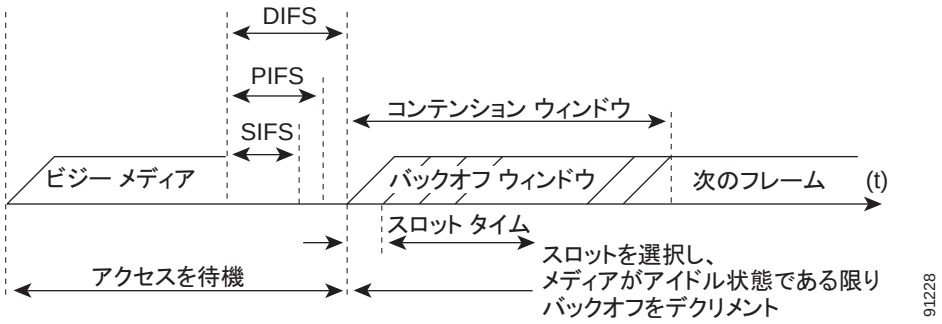
802.11 は、現在、次の 3 つのフレーム間スペース（IFS）を定義しています（図 5-3 を参照）。

- 短いフレーム間スペース（SIFS）― 10µs
- ポイント フレーム間スペース（PIFS）― SIFS + 1 x スロット タイム = 30µs
- DCF フレーム間スペース（DIFS）― 50µs SIFS + 2 x スロット タイム = 50µs

（注） このフレーム間スペースの例で使用しているベース タイミングは、802.11b に基づいています。802.11g と 802.11a ではタイミングが異なりますが、同じ原則が適用されます。

フレーム間スペース（SIFS、PIFS、および DIFS）により、キャリア検知でチャネルの空きが示された後に、最初にチャネルにアクセスするトラフィックを 802.11 で制御できます。通常、802.11 の管理フレームとコンテンションを起こさないフレーム（フレーム シーケンスの一部であるフレーム）では SIFS が使用され、データ フレームでは DIFS が使用されます。

図 5-3　フレーム間スペース



ランダム バックオフ

DCF を使用しているデータ フレームが送信可能になると、そのデータ フレームは次の手順で処理を行います。

1. 0 ～最小コンテンション ウィンドウ（CWmin）の範囲のランダム バックオフ番号を生成します。
2. DIFS 間隔の間、チャネルが空くまで待機します。
3. チャネルがまだ空いている場合には、チャネルが空いているスロット タイム（20 µs）ごとの、ランダム バックオフ番号のデクリメントを開始します。
4. 別のステーションが先に 0 に達したなどでチャネルが使用中になると、デクリメントは停止し、手順 2 ～ 4 が繰り返されます。
5. ランダム バックオフ番号が 0 に達するまでチャネルが空いている状態のままであれば、フレームを送信できます。

図 5-4 は、DCF プロセスが実行される様子を示した簡単な例です。この簡易化 DCF プロセスでは、確認応答は示されず、断片化は発生しません。

図 5-4　分散コーディネーション機能の例

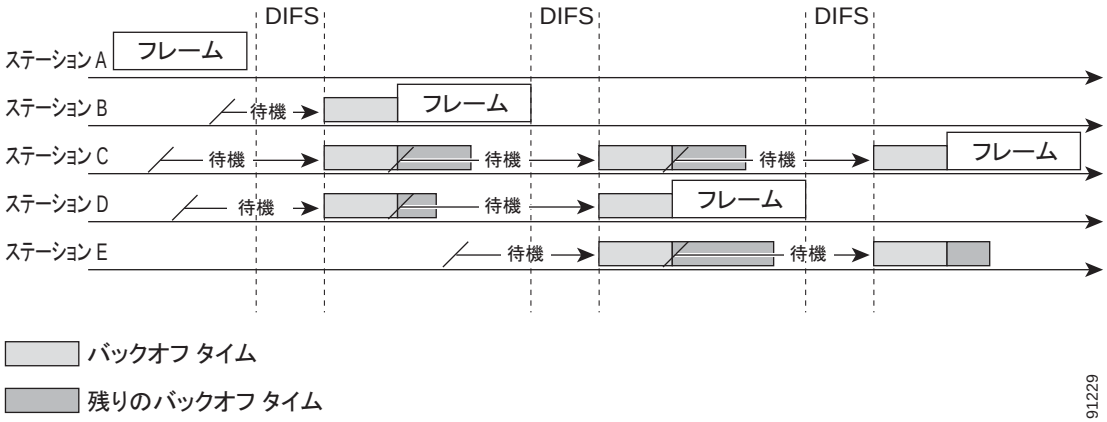


図 5-4 で示している DCF の手順は次のとおりです。

1. ステーション A は正常にフレームを送信します。他の 3 ステーションもフレームを送信しようとしていますが、ステーション A のトラフィックが完了するまで待つ必要があります。
2. ステーション A が伝送を完了した後も、すべてのステーションはなお DIFS の間待機する必要があります。DIFS が完了すると、フレームの送信を待機していたステーションが、スロット タイムごとに 1 度バックオフ カウンタのデクリメントを開始し、各フレームを送信できます。
3. ステーション B のバックオフ カウンタがステーション C および D の前に 0 に達したので、ステーション B がフレームの送信を開始します。
4. ステーション C および D はステーション B の送信を検知すると、バックオフ カウンタのデクリメントを停止し、ステーション B のフレームが送信され DIFS が過ぎるまで待機しなければなりません。
5. ステーション B がフレームを送信している間、ステーション E は送信するフレームを受信しますが、ステーション B が送信中のため、ステーション C および D と同じように待機しなければなりません。
6. ステーション B が送信を完了し、DIFS が過ぎると、送信すべきフレームを持つステーションがバックオフ カウンタのデクリメントを開始します。この場合、ステーション D のバックオフ カウンタが最初に 0 に達し、フレームの送信を開始します。
7. トラフィックが別のステーションに届くと、このプロセスが継続します。

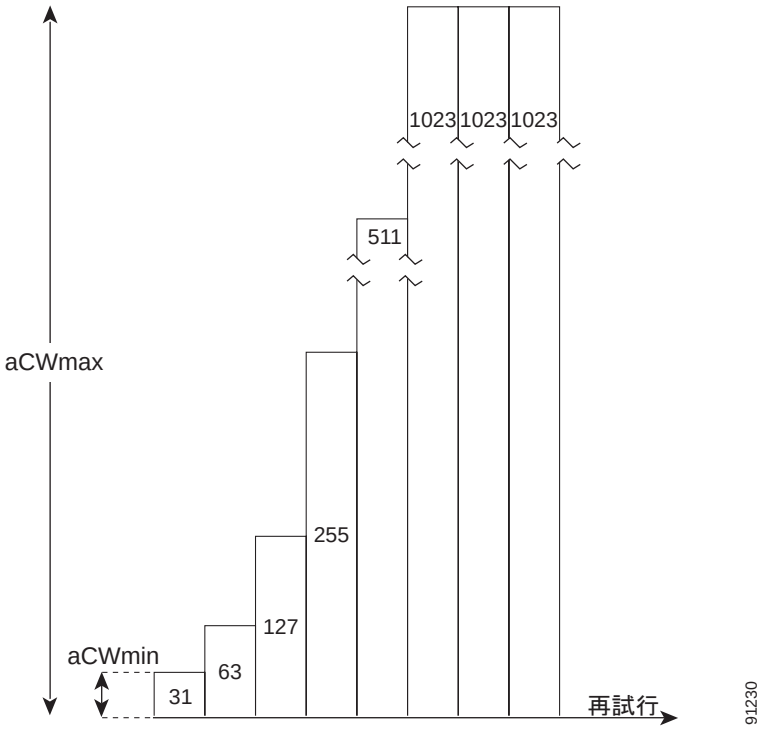
CWmin、CWmax、および再試行

DCF はコンテンション ウィンドウ（CW）を使用して、ランダム バックオフのサイズを制御します。コンテンション ウィンドウは、次の 2 つのパラメータで定義されています。

- aCWmin
- aCWmax

ランダム バックオフで使用される初期のランダム番号は、0 ～ aCWmin です。初期ランダム バックオフがフレームを正常に送信せずに時間切れになった場合、ステーションまたは AP は再試行カウンタを増加し、ランダム バックオフ ウィンドウのサイズを倍加します。このサイズの倍加は、サイズが aCWmax と等しくなるまで続行します。再試行は、最大再試行回数または有効時間（TTL）に達するまで続行します。バックオフ ウィンドウを倍加するこのプロセスは、通常、*バイナリ指数バックオフ*と呼ばれています。図 5-5 はこれを示したもので、aCWmin が 2^5-1 の場合 2^6-1 に増加し、その後次のバックオフ レベルでは aCWmax 値である 2^{10}-1 にまで増加しています。

図 5-5　再試行に伴うランダム バックオフ範囲の増加



（注） これらの値は 802.11b に基づいており、別の物理レイヤの実装では異なります。

Wi-Fi マルチメディア

この項では、WMM の実装について説明します。

- WMM のアクセス
- WMM の省電力
- アクセス コントロール

WMM のアクセス

WMM は、802.11e 草案の一連の機能に対応した Wi-Fi Alliance の認証です。この認証はクライアントと AP の両方を対象としており、WMM の操作を認定します。WMM は、主に、802.11e の EDCA コンポーネントの実装です。Wi-Fi の追加認証が、802.11e の別のコンポーネントを対象に計画されています。

WMM の分類

WMM では IEEE が開発した 802.1P 分類方式が使用されています（現在では 802.1D 分類の一部となっています）。

この分類方式には 8 つの優先度があり、WMM はこれを AC_BK、AC_BE、AC_VI、および AC_VO の 4 つのアクセス カテゴリにマッピングします。これらのアクセス カテゴリは、表 5-2 に示されているように WMM デバイスに必要な 4 つのキューにマッピングします。

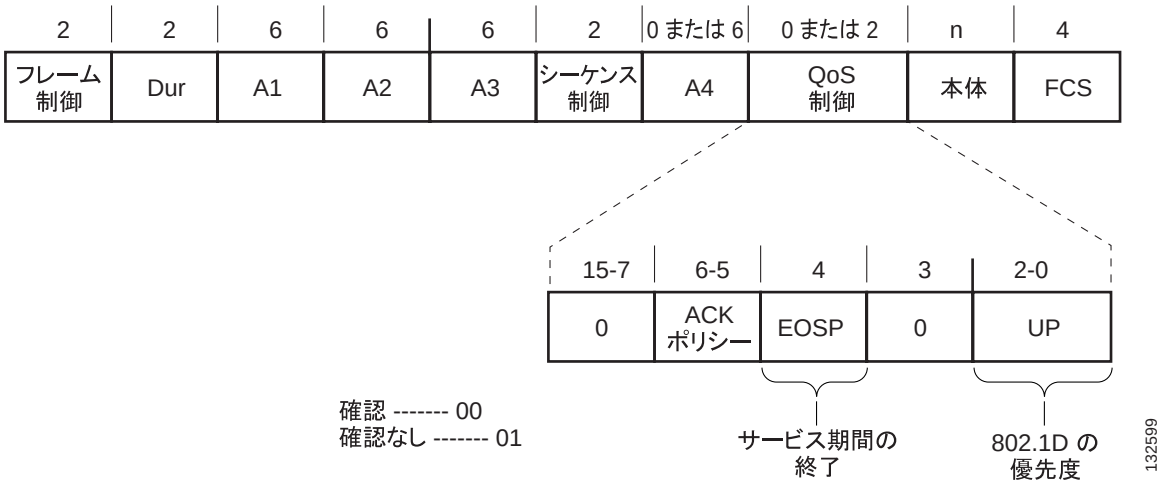
表 5-2　表 2 802.1P および WMM の分類

優先度	802.1P の優先度	802.1P の指示	アクセス カテゴリ	WMM の指示
最低	1	BK	AC_BK	バックグラウンド
	2	-		
	0	BE	AC_BE	ベストエフォート
	3	EE		
	4	CL	AC_VI	ビデオ
	5	VI		
	6	VO	AC_VO	音声
最高	7	NC		

図 5-6 は、WMM データ フレーム形式を示しています。8 つの 802.1P 分類は WMM で 4 つのアクセス カテゴリにマッピングされますが、802.11D の分類はフレーム内で送信されます。

（注） WMM および IEEE 802.11e の分類はシスコのネットワークで推奨および使用されている分類とは異なります。シスコのネットワークで使用される分類は、IETF 推奨の分類に基づいています。分類の主な違いは、音声とビデオのトラフィックをそれぞれ 5 および 4 に変更している点です。これにより、6 つの分類をレイヤ 3 ネットワーク制御に使用できます。両方の標準に準拠するために、Cisco Unified Wireless ソリューションではトラフィックが無線と有線の境界を横切る際に、種々の分類標準間の変換が実行されます。

図 5-6　WMM フレーム形式



WMM キュー

図 5-7 は、WMM クライアントまたは AP で実行されるキューイングを示しています。4 つの個別キューが、各アクセス カテゴリに 1 つずつあります。これらのキューはそれぞれ、前述した DCF メカニズムに対するのと同様の方法で無線チャネルを確保するために競います。この際、各キューには異なるフレーム間スペース、CWmin、および CWmax の値が使用されます。異なるアクセス カテゴリからの複数のフレームが内部で衝突した場合、優先度の高いフレームが送信され、優先度の低いフレームはバックオフ パラメータをキューイング メカニズムの外部のフレームと衝突した場合と同様に調整します。このシステムは、Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）と呼ばれています。

図 5-7　WMM キュー

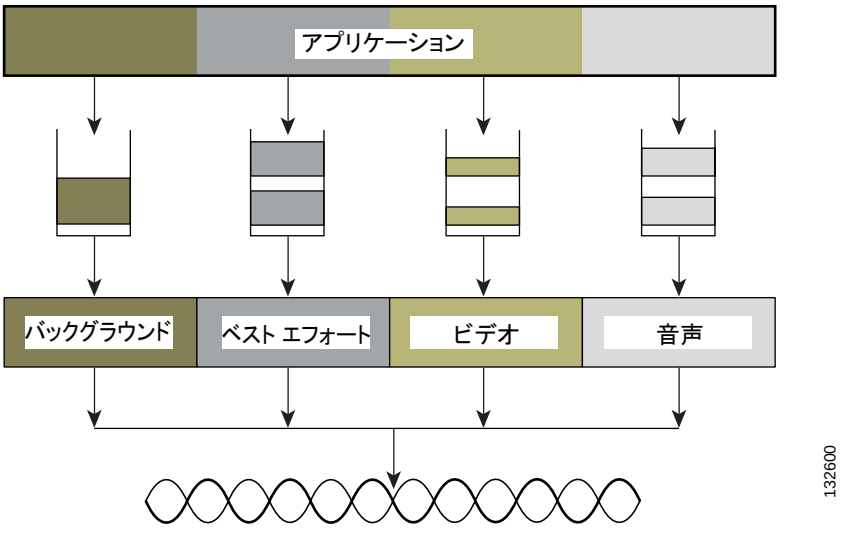
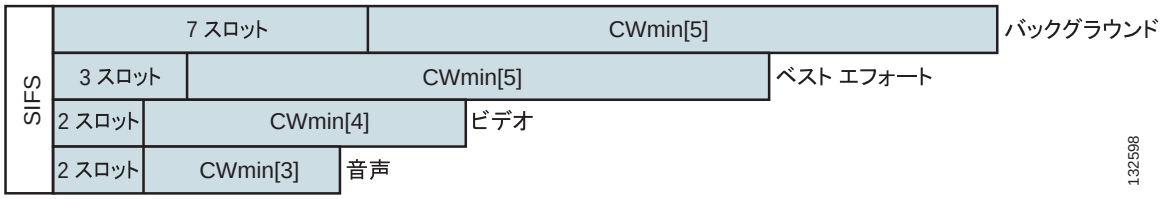


図 5-8 は、EDCF の背後の原則を示しています。ここでは、異なるフレーム間スペースと CWmin および CWmax の値がトラフィックの分類ごとに適用されています（図内では、明確にするため Cwmax は省略）。異なるトラフィック タイプは各ランダム バックオフをカウント ダウンする前に異なるインターフェイス スペースを待機させることができ、ランダム バックオフ番号の生成に使用される CW 値もトラフィックの分類により異なります。たとえば、音声の CWmin[3] は 2^3-1 で、ベストエフォート トラフィックの CWmin[5] は 2^5-1 です。優先度が高いトラフィックではフレーム間スペースが小さく、CWmin 値も小さいため、ランダム バックオフが短くなるのに対し、ベストエフォート トラフィックではフレーム間スペースが長く、CWmin 値も大きくなるため、ランダム バックオフ数が平均して高くなります。

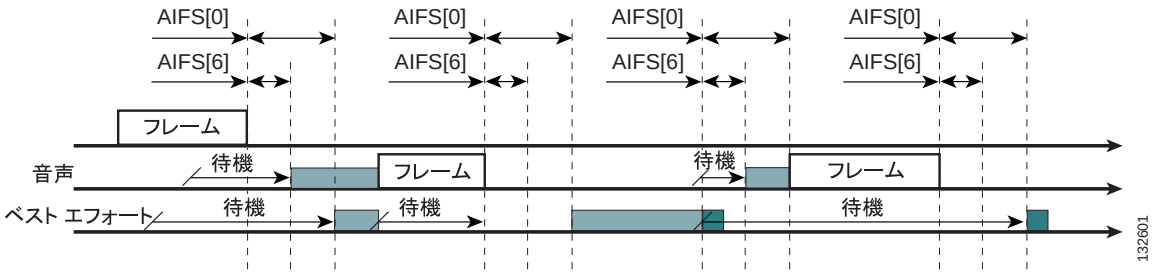
図 5-8　アクセス カテゴリのタイミング



EDCA

図 5-9 は、EDCA プロセスを示しています。

図 5-9　EDCA の例



EDCA プロセスでは、次の順序で処理が行われます。

1. ステーション X がフレームを送信中に、他の 3 つのステーションでフレームを送信する必要があると判断されました。フレームはすでに送信中なので各ステーションは待機し、ランダム バックオフを生成します。
2. ステーション Voice には音声のトラフィック分類があるので、Arbitrated Interframe Space（AIFS; 調停フレーム間スペース）2 があり、初期 CWmin 3 を使用します。したがって、ランダム バックオフのカウントダウンを待機する必要があるのは 2 スロット タイムで、ランダム バックオフ値は短くなります。
3. ベストエフォートの CWmin 値は 5 なので、ベストエフォートには 3 の AIFS があり、ランダム バックオフ タイムは長くなります。

4. Voice には最短ランダム バックオフ タイムがあるので、最初に送信を開始します。Voice が送信を開始すると、他のすべてのステーションは待機します。
5. Voice ステーションが送信を終えると、すべてのステーションはそれぞれの AIFS の間待機し、その後再びランダム バックオフ カウンタのデクリメントを開始します。
6. 次にベストエフォートがランダム バックオフ カウンタのデクリメントを完了し、送信を開始します。他のすべてのステーションは待機します。送信を待機している Voice ステーションがある場合でも、このように進行します。これは、ランダム バックオフのデクリメント プロセスで最終的にはベストエフォート バックオフが高優先度トラフィックと同様のサイズにまで縮小されるため、音声トラフィックがベストエフォート トラフィックを絶対に必要だとしていないこと、およびランダム プロセスが、場合に応じて、ベストエフォート トラフィックに対して小さいランダム バックオフ番号を生成することを示しています。
7. 他のトラフィックがシステムに入ると、このプロセスが継続します。表 5-3 および 表 5-4 に示されているアクセス カテゴリの設定は、デフォルトでは、802.11a 無線と同一で、WMM で定義されている式に基づいています。

(注)　表 5-3 は、クライアントのパラメータ設定を示しています。この設定は、AP の設定とは多少異なっています。AP では、AC 音声およびビデオの AIFSN 値が高くなっています。

表 5-3　WMM クライアント パラメータ

AC	CWmin	CWmax	AIFSN	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	1	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	1	3.264 ms	1.504 ms

表 5-4　WMM AP パラメータ

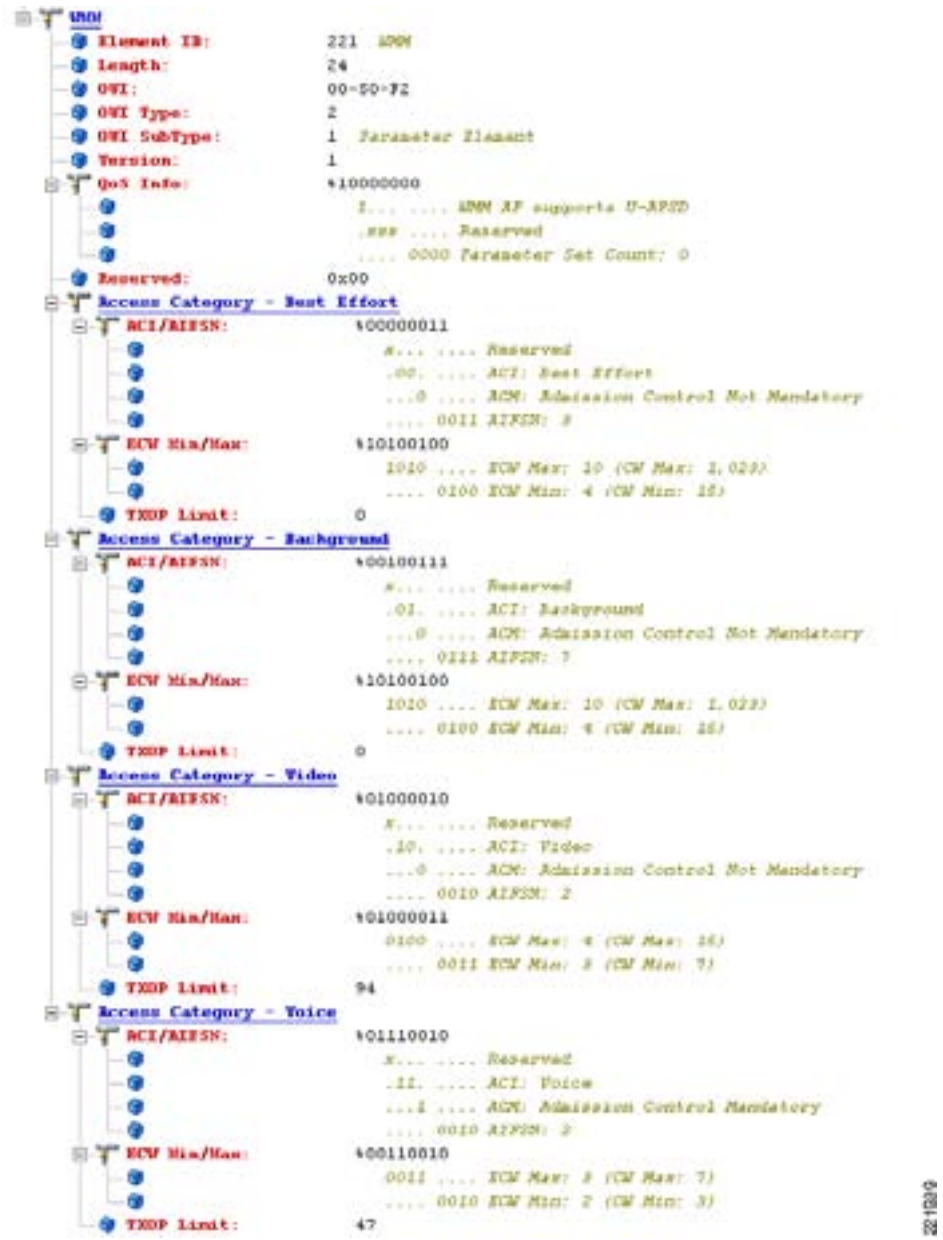
アクセス カテゴリ	CWmin	CWmax	AIFSN	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_BK	aCWmin	aCWmax	7	0	0
AC_BE	aCWmin	4*(aCQmin+1)-1	3	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016 ms	3.008 ms
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.504 ms

異なる AIFS、CWmin、および CWmax 値が全体に及ぼす影響は、その影響が実際には統計に基づくことが多いため、タイミング ダイアグラムに示すことは困難です。AIFS とランダム バックオフ ウィンドウのサイズを比較する方が簡単です（図 5-8 を参照）。

例の音声フレームとバックグラウンド フレームを比較すると、これらのトラフィック カテゴリの CWmin 値はそれぞれ 2^3-1（7）、2^5-1（31）で、AIFS は 2、7 です。そのため、フレームを送信するまでの遅延は、音声フレームでは平均 5（2+7/1）スロット タイム、バックグラウンド フレームでは平均 22（7+31/2）スロット タイムになります。したがって、音声フレームは統計的にはバックグラウンド フレームの前に送信される傾向がずっと強くなります。

図 5-10 は、プローブ応答内の WMM 情報を示しています。この要素に含まれる WMM アクセス カテゴリ情報とは別に、クライアントはアドミッション制御を必要とする WMM カテゴリについても認識します。この例で明らかなように、音声 AC ではアドミッション制御が必須に設定されています。そのため、クライアントは要求を AP に送信し、受け入れられてからでないと、その AC を使用できません。アドミッション制御については、この章の後半で詳しく説明します。

図 5-10　プローブ応答の WMM 要素情報



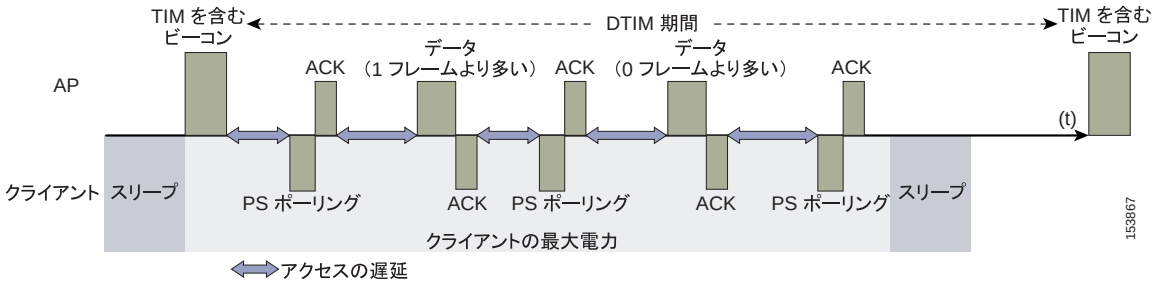
U-APSD

Unscheduled Automatic Power-Save Delivery（U-APSD; 不定期自動省電力配信）は、次の 2 つの主要な利点を持つ機能です。

- U-APSD の第 1 の利点は、音声クライアントが AP との間で音声フレームの送受信を同期化できることです。それによって、クライアントは音声フレームの各タプルの送受信間に省電力モードになることができます。U-APSD をサポートしているアクセス カテゴリのフレームが WLAN クライアントから送信されると、AP はその WLAN クライアントに対してキューイングされているそのアクセス カテゴリのあらゆるデータ フレームの送信を開始します。U-APSD クライアントは、AP から End of Service Period（EOSP; サービス時間終了）ビット セットを含むフレームを受信するまで、AP の接続を待機し続けます。EOSP ビット セットによって、クライアントは省電力モードに戻れることを通知されます。このトリガー メカニズムでは、Delivery Traffic Indication Message（DTIM; 配信トラフィック通知メッセージ）間隔によって制御された間隔において、通常のビーコン方式の待機より、クライアントの電源の使用を効率化できると見なされています。なぜなら、通常の待機では、音声の遅延要件とジッタ要件から、WVoIP クライアントはコール中に省電力モードになれず、その結果通話時間が短縮されてしまうか、または DTIM 間隔が短くなり、その結果待機時間が短縮されてしまうからです。U-APSD の使用により、長時間の DTIM 間隔を使用して、コールの質を犠牲にせずにスタンバイ時間を最大限にできます。U-APSD 機能はアクセス カテゴリ全体で個別に適用できるため、AP で音声 AC に U-APSD を適用しながら、他の AC では標準の省電力機能を使用できます。
- この機能の第 2 の利点は、コール キャパシティの増大です。AP からのデータ フレームをバッファされた伝送のカップリングには WLAN クライアントから取り込んだデータ フレームが含まれ、AP からのフレームはフレーム間スペースおよびランダム バックオフなしで送信できるので、コールによるコンテンションの発生を緩和します。

図 5-11 は、標準 802.11 の省電力配信プロセスにおけるフレーム交換の例を示しています。

図 5-11　標準のクライアント省電力



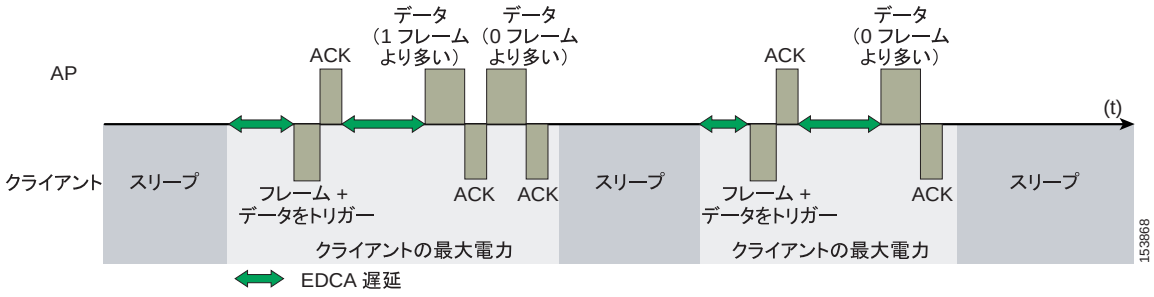
省電力モードにあるクライアントは、まず、AP ビーコンに TIM が存在することを検出して、AP でデータが待機していることを認識します。クライアントは、そのデータを取得するために AP を省電力ポーリング（PS-Poll）する必要があります。クライアントに送信されたデータが複数のフレームの送信を要求している場合、AP はこれを送信済みデータ フレーム内に示します。このプロセスで、クライアントは、バッファされたすべてのデータを取得するまで、AP に省電力ポーリングを送信し続ける必要があります。

これは 2 つの主要な問題点を提示しています。まず、このプロセスは、非常に非効率的で、PS ポーリングおよび通常のデータ交換を要求し、DCF に関連する標準アクセス遅延を発生します。第 2 の問題点は、音声トラフィックに対してより重大な側面となります。つまり、バッファ済みデータの取得が DTIM に依存しており、それが多様なビーコン間隔となります。標準のビーコン間隔は 100 ms であり、DTIM 間隔はこの整数の倍数となります。その結果、音声コールには通常は許容されないジッタ レベルが発生し、音声端末は、音声コールの進行中、省電力モードをフル送信に切り替えて動作を受信します。これにより、許容できる音声の質を確保できますが、バッテリの寿命は短く

なります。Cisco Unified Wireless IP Phone 7921G では、ビーコンの TIM を待たずに PS ポーリング要求を生成できる PS ポーリング機能を提供することによって、この問題に対処しています。この機能により、7921G はフレームを送信したときにフレームのポーリングを実行し、その後、省電力モードに戻ることができます。この機能では U-APSD ほどの効率性は得られませんが、U-APSD を使用できない WLAN で 7921G のバッテリの寿命を伸ばすことができます。

図 5-12 は、U-APSD を使用したトラフィック フローの例を示しています。この場合、トラフィックを取得するためのトリガーは AP へのクライアントのトラフィック送信です。AP は、フレームを確認すると、データがキューイングされ、待機していることをクライアントに伝えます。それにより AP はデータをクライアントへ通常は TXOP バーストとして送信します。この場合、最初のフレームだけに EDCF アクセス遅延が発生します。すべての後続のフレームは、その結果、確認応答フレームの後で直接送信されます。VoWLAN 実装では、AP でキューイングされている可能性があるフレームは 1 つだけであるため、VoWLAN クライアントはそのフレームを AP から受信した後はスリープ モードに入ることできます。

図 5-12　U-APSD



この方法は、以前の方式の短所を両方とも克服し、はるかに効率的です。ポーリングのタイミングは、クライアント トラフィックにより制御されます。これは音声の場合には対称になるので、クライアントが 20 ms ごとにフレームを送信した場合、フレームの受信も 20 ms になると想定されます。それにより、発生する最大ジッタは、n * 100 ms ではなく 20 ms になります。

TSpec アドミッション制御

トラフィック仕様（TSpec）では、802.11e クライアントから AP にそのトラフィック要件に関する信号を送信できます。802.11e MAC 定義には、アクセスを優先させるための 2 つのメカニズムがあります。そのメカニズムとは、コンテンションベースの EDCA オプションおよび送信権（TXOP）により提供される制御されたアクセス オプションです。クライアントがそのクライアント自体のトラフィック特性を指定できる TSpec 機能とはどのようなものかを説明する場合、制御されたアクセス メカニズムが自動的に使用されるようになり、TSpec 要求に一致する特定の TXOP がクライアントに対して許可される、というのは簡単に思い浮かぶことです。しかし、それだけではありません。TSpec 要求は、EDCA のさまざまなアクセス カテゴリ（AC）の使用を制御するために使用できます。クライアントが特定の優先度タイプのトラフィックを送信できるようになる前に、TSpec メカニズムを使用してそれを要求しておく必要があります。たとえば、音声 AC を使用しようとしている WLAN クライアント デバイスは、まずその AC の使用を要求する必要があります。AC の使用を TSpec 要求で制御するかどうかは、TSpec 要求により制御される音声 AC とビデオ AC では設定可能であり、ベストエフォート AC とバックグラウンド AC については TSpec 要求なしで使用できます。802.11e Hybrid Coordinated Channel Access（HCCA）ではなく EDCA AC を使用して TSpec 要求を満たすことも多くの状況で可能です。これは、トラフィック パラメータが非常に単純なため、特定の TXOP を作成してアプリケーションの要求を満たさなくても、キャパシティを割り当てることによってパラメータを満たせるためです。

（注）　7921G では TSpec をサポートしていますが、Cisco 7920 WVoIP 端末では TSpec アドミッション制御をサポートしていません。

Add Traffic Stream

Add Traffic Stream（ADDTS）機能は、WLAN クライアントが AP へのアドミッション要求を実行する方法です。アドミッション要求では、次の 2 つのいずれかの形式で TSpec 要求の信号が AP に送信されます。

- ADDTS アクション フレーム ― これは AP にアソシエートされたクライアントが通話を開始または終了したときに発生します。ADDTS には TSpec が含まれており、Traffic Stream Rate Set（TSRS; トラフィック ストリーム レート セット）IE（Cisco Compatible Extensions v4 クライアント）が含まれる場合もあります。
- アソシエーションおよび再アソシエーション メッセージ ― STA がトラフィック ストリームをアソシエーションの一部として確立しようとすると、アソシエーション メッセージには 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。STA が別の AP にローミングすると、再アソシエーション メッセージには 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。

ADDTS には、トラフィック要求を説明する TSpec 要素が含まれます。Cisco 7921 WLAN 端末と Cisco AP 間の ADDTS 要求と応答の例は、図 5-13 と図 5-14 を参照してください。データ レートおよびフレーム サイズなど、トラフィックの要件を説明する主要なデータとは別に、TSpec 要素もクライアント デバイスが使用する最小物理レートを AP に伝えます。これにより、そのステーションがどのくらいの時間を消費してこの TSpec を送受信できるかを算出でき、その結果 AP がその TSpec を満たすリソースがあるかどうかを算出できるようになります。TSpec アドミッション制御は、コールが開始されたときとローミングを要求中に WLAN クライアントにより使用されます（ターゲット クライアントは VoIP 端末）。ローミングの際には、TSpec 要求が再アソシエーション要求に追加されます。

図 5-13　ADDTS 要求のデコード

図 5-14　ADDTS 応答のデコード

WLAN インフラストラクチャ対応の QoS 拡張機能

Cisco Centralized WLAN アーキテクチャには、WMM サポート機能のほかに複数の QoS 機能があります。これらの機能のうち主要なものは、WLC の QoS プロファイルです。プラチナ、ゴールド、シルバー、およびブロンズの 4 つの QoS プロファイルを設定できます（図 5-15 を参照）。

図 5-15　QoS プロファイル オプション

図 5-16 に示すプロファイルごとに、帯域幅の契約、RF 使用制御、および許可された最大の 802.1P 分類を設定できます。

図 5-16　QoS プロファイルの設定

通常、ユーザごとの帯域幅契約の設定はデフォルト値のままにして、802.11 WMM 機能を使用してデファレンシエーテッド サービスを提供することをお勧めします。

特定のプロファイルを使用する WLAN に対しては、そのプロファイルの 802.1P 分類によって次の 2 つの重要な動作が制御されます。

- WLC から送信されるパケットに使用する Class of Service（CoS; サービス クラス）値の決定

  プロファイルに設定された CoS 値は、そのプロファイルを使用する WLAN のすべての LWAPP パケットのマーキングに使用されます。たとえば、プラチナ QoS プロファイルを使用している WLAN の場合、802.1P マークが 6 なら、コントローラの AP マネージャ インターフェイスから送信される LWAPP パケットは CoS 5 としてマーキングされます。CoS は、Cisco QoS ベースライン推奨事項に準拠するようにコントローラで調整されます。設定に IEEE CoS のマーキングを維持するのがなぜ重要かについては、次のポイントで説明します。WLC へのネットワーク接続で DSCP ではなく CoS を信頼するようにネットワークが設定されている場合、CoS 値によって AP が受信する LWAPP パケットの DSCP が決まり、さらに、この DSCP によって WLAN トラフィックの WMM 分類とキューイングが決まります（フレームの WLAN WMM 分類は、そのフレームを搬送する LWAPP パケットの DSCP 値から導出）。
- その WLAN に接続したクライアントが使用できる最大 CoS 値の決定

  802.1P 分類によって、そのプロファイルを使用する WLAN で許可される最大 CoS 値が設定されます。

WMM 音声トラフィックは CoS 6 で AP に着信し、CoS 6 に基づき、このトラフィックに対して CoS から DSCP へのマッピングが AP で自動的に実行されます。WLC 設定の CoS 値が 6 より小さい値に設定されている場合、この変更された値が AP の WLAN QoS プロファイルで使用されて、使用されている最大 CoS マーキングが設定され、それにより、使用する WMM AC が設定されます。

重要な点は、Unified Wireless Network では常に IEEE 802.11e 分類をベースにして考え、IEEE 分類と Cisco QoS ベースラインとの変換を Unified Wireless Network ソリューションで実行できるようにすることです。

WLAN はさまざまなデフォルト QoS プロファイルを使用して設定できます（図 5-17 を参照）。各プロファイル（プラチナ、ゴールド、シルバー、およびブロンズ）は、代表的な使用に対して注釈が付けられます。さらに、クライアントには、AAA を使用して ID に基づいて QoS プロファイルを割り当てることができます。一般的な企業では、ユーザごとの帯域幅契約や Over-the-Air QoS などの WLAN 展開パラメータをデフォルト値のままにしておき、WMM および有線 QoS などの標準 QoS ツールを使用することによって、クライアントに最適な QoS を提供できます。

図 5-17　WLAN QoS プロファイル

QoS プロファイル以外に、WLAN ごとの WMM ポリシーも制御できます（図 5-18 を参照）。次の 3 つの WMM オプションがあります。

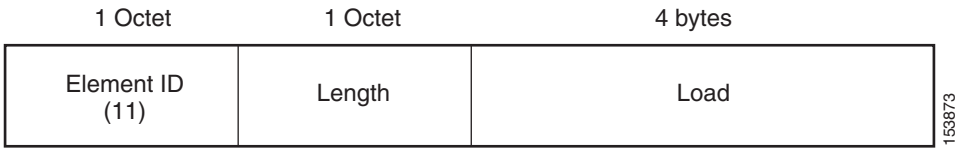
- Disabled ― WLAN で WMM 機能はアドバタイズされず、WMM ネゴシエーションも許可されません。
- Allowed ― WLAN で WMM クライアントと WMM 以外のクライアントが許可されます。
- Required ― WMM 対応クライアントを WLAN にアソシエートできます。

図 5-18　WLAN WMM ポリシー

IP 電話

図 5-19 は、Cisco AP がアドバタイズする基本的な QoS Basis Service Set（QBSS; 基本サービス セット）情報要素（IE）を示しています。Load フィールドは、現在その AP のデータを送信するのに使用されている有効な一部の帯域幅を示しています。

図 5-19　QBSS 情報要素



特定の状況でサポートする必要のある QBSS IE は、次の 3 つです。

- 旧 QBSS （草案 6 （先行標準））
- 新 QBSS （草案 13 802.11e（標準））
- 新規分散型 CAC 負荷の IE（シスコの IE）

使用する QBSS は WLAN 上の WMM および 7920 の設定に依存します。

7920 電話のサポートは、図 5-18 に図示されているように、WLC WLAN 構成のコンポーネントです。これにより、AP にビーコンの適切な QBSS 要素を含めることができます。7920 や 7921G など、QoS 要件のある WLAN クライアントは、これらのアドバタイズされた QoS パラメータを使用して、アソシエートすべき最良の AP を決定します。

WLC は、クライアント Call Admission Control（CAC; コール アドミッション制御）制限または AP CAC 制限を使用して 7920 をサポートします。これらの機能は、次のとおりです。

- クライアント CAC 制限 ― 7920 は、クライアントに設定されたコール アドミッション制御設定を使用します。これは、2.01 以前の旧 7920 コードをサポートします。
- AP CAC 制限 ― 7920 は、WLAN アドバタイズメントから習得したコール アドミッション制御設定を使用します。

WMM、クライアント CAC 制限、および AP CAC 制限のさまざまな組み合わせにより、次のように異なった QBSS IE が送信されます。

- WMM だけが有効な場合、IE 番号 2（802.11e 標準）QBSS Load IE がビーコン応答とプローブ応答で送信されます。

- 7920 クライアント CAC 制限がサポートされる場合、IE 番号 1（以前の標準 QBSS IE）が BG 無線のビーコン応答とプローブ応答で送信されます。
- 7920 AP CAC 制限がサポートされる場合、IE 番号 3 QBSS IE が BG 無線のビーコンとプローブ応答で送信されます。

（注） さまざまな QBSS IE が同一の ID を使用するので、これらの 3 つの QBSS は相互に排他的です。たとえば、ビーコン応答およびプローブ応答には 1 つの QBSS IE だけを含めることができます。

アドミッション制御パラメータの設定

図 5-20 は、コントローラの音声パラメータ設定の設定画面の例を示しています。

図 5-20　音声パラメータの設定

アドミッション制御パラメータは、無線が対応でき、通常の ADDTS 要求により VoWLAN コールを開始させることができる、最大 RF 帯域幅で構成されています。

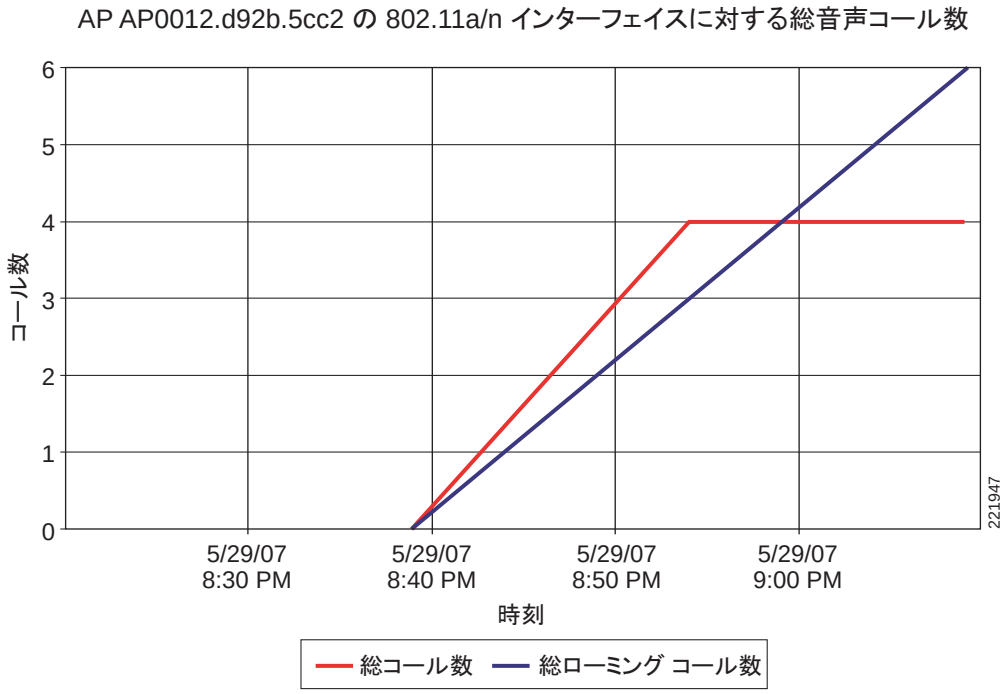
Reserved Roaming Bandwidth は、その AP にローミングしようとしている通話中の VoWLAN クライアントに対して、アソシエーションまたは再アソシエーション時の ADDTS に応答できるようにどれだけのキャパシティを取っておくかを設定します。

これらのパラメータに基づいてアドミッション制御を有効にするには、Admission Control (ACM) チェックボックスをオンにします。それによって、AP のキャパシティに基づくアドミッション制御が有効化されますが、エリア内の他の AP のチャネル負荷の影響の可能性は考慮されません。キャパシティ計算にこの「チャネル負荷」を算入するには、Admission Control（ACM) チェックボックスと共に Load-Based AC チェックボックスをオンにします。

Metrics Collection オプションでは、音声コールまたはビデオ コールのデータを収集して、WCS で使用できるようにするかどうかを指定します。

図 5-21 は、WCS で使用できる音声統計レポートの一例を示しています。レポート内容は、1 つの AP の無線で確立されたコールと、その AP にローミングしたコール数です。このレポートおよび他の音声統計は、スケジュール設定するか、または一時的に使用できるほか、グラフィック表示またはデータ ファイルとして公開が可能です。

図 5-21　WCS の音声統計



(注)　コール アドミッション制御は、音声およびビデオ QoS プロファイルのためにだけ実行されます。

TSpec アドミッション制御の影響

TSpec アドミッション制御の目的は、WLAN へのクライアント アクセスを拒否することではなく、優先度の高いリソースを保護することです。したがって、TSpec アドミッション制御を使用していないクライアントが、そのトラフィックをブロックされることはありません。トラフィックを送信しようとしたときに、単にトラフィックが再分類されるだけです（そのクライアントが保護された AC で WMM に準拠したトラフィック送信する場合は不適切）。

表 5-5 と 表 5-6 は、アクセス制御が有効化されている場合の分類への影響をトラフィック ストリームが確立されているかどうかに基づいて示しています。

表 5-5　アップストリーム トラフィック

	確立されたトラフィック ストリーム	トラフィック ストリームなし
アドミッション制御なし	動作に変化なく、パケットは従来どおりネットワークに送信されます。UP は max = WLAN QoS 設定に制限されます。	動作に変化なく、パケットは従来どおりネットワークに送信されます。UP は max = WLAN QoS 設定に制限されます。
アドミッション制御	動作に変化なく、パケットは従来どおりネットワークに送信されます。UP は max = WLAN QoS 設定に制限されます。	パケットが WMM クライアントのネットワークに入ってから、パケットについて BE（CoS および DSCP の両方）に対してリマークされます。WMM 以外のクライアントに対して、パケットは WLAN QoS と共に送信されます。

表 5-6　ダウンストリーム トラフィック

	確立されたトラフィック ストリーム	トラフィック ストリームなし
アドミッション制御なし	変化なし	変化なし
アドミッション制御	変化なし	UP について WMM クライアントの BE に対してリマークします。WMM 以外のクライアントに対して、WLAN QoS を使用します。

802.11e、802.1P、および DSCP のマッピング

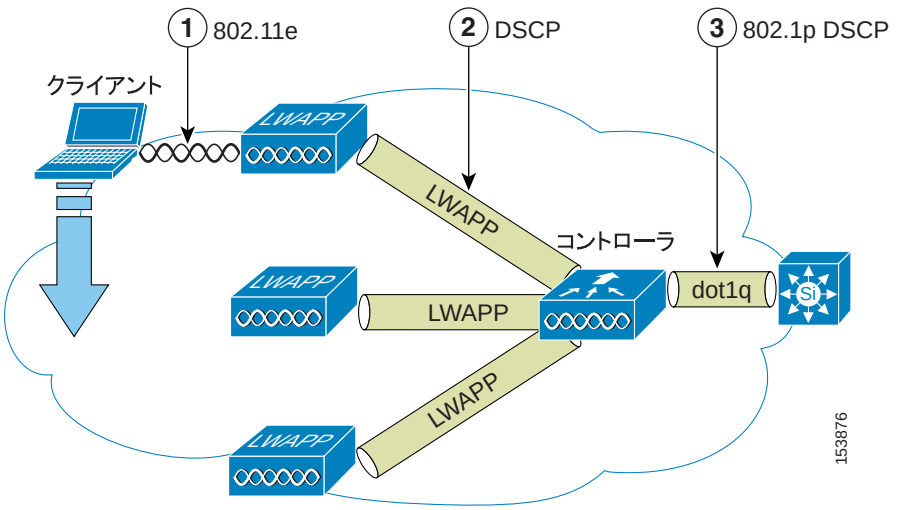
Unified Wireless Network 内の WLAN データは LWAPP（IP UDP パケット）を介してトンネリングされます。WLAN フレームに適用された QoS 分類を維持するためには、DSCP と CoS 間の分類のマッピング プロセスが必要になります。

たとえば、WLAN クライアントから WMM で分類されたトラフィックが送信された場合、このトラフィック フレームには 802.1P 分類が含まれています。AP はこの分類を DSCP 値に変換する必要があります。それによって、このフレームを伝送する LWAPP パケットが WLC へ達するまでの間、適切な優先度で確実に処理されるようになります。AP に送信される LWAPP パケットの場合も、同様のプロセスが WLC で必要です。

WMM 以外のクライアントからのトラフィックを分類するメカニズムも必要です。それによって、WMM 以外のクライアントの LWAPP パケットにも AP および WLC によって適切な DSCP 分類が割り当てられます。

図 5-22 は、LWAPP WLAN ネットワークのさまざまな分類メカニズムを示しています。

図 5-22　WMM と 802.1P との関係



複数の分類メカニズムとクライアントの機能には、複数の戦略が必要です。

- LWAPP 制御フレームには優先順位が必要です。LWAPP 制御フレームは CS6 の DSCP 分類でマーク付けされます。
- WMM を有効化したクライアントは、WLC への LWAPP パケットに対する該当 DSCP 分類へマップされたフレームの分類が割り当てられています。このマッピングは、QoS ベースラインへの準拠に必要な変更を除いて、IEEE CoS から DSCP へのマッピングの標準に従っています。この DSCP 値は、WLC において、WLC インターフェイスから発信される 802.1Q フレーム上で CoS 値に変換されます。
- WMM 以外のクライアントには、その WLAN のデフォルトの QoS プロファイルに一致するよう設定された LWAPP トンネルの DSCP があります。7920 電話をサポートする WLAN の QoS プロファイルがプラチナに設定されている場合、その WLAN からのデータ フレーム パケットについても EF の DSCP 分類となります。
- WLC からの LWAPP データ パケットには、WLC へ送信された有線データ パケットの DSCP によって決定される DSCP 分類があります。AP から WMM クライアントへのフレーム送信時に使用される 802.11.e 分類は、DSCP 分類から WMM 分類へ変換する AP テーブルによって決定されます。

（注） AP から WLAN クライアントに送信されるトラフィックに使用される WMM 分類は、LWAPP パケットの DSCP 値に基づき、含まれている IP パケットの DSCP 値には基づきません。そのため、エンドツーエンドの QoS システムの整備が重要になります。

QoS ベースラインの優先度のマッピング

LWAPP AP と WLC で QoS ベースラインの変換が実行されることによって、表 5-7 に示す WMM 値は IEEE 値ではなく適切な QoS ベースライン DSCP 値にマッピングされます。

表 5-7　アクセス ポイントの QoS 変換値

AVVID 802.1 UP ベースのトラフィック タイプ	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
ネットワーク制御	-	7	-
ネットワーク間制御（LWAPP 制御、802,11 管理）	48	6	7
音声	46（EF）	5	6
ビデオ	34（AF41）	4	5
音声制御	26（AF31）	3	4
バックグラウンド（ゴールド）	18（AF21）	2	2
バックグラウンド（ゴールド）	20（AF22）	2	2
バックグラウンド（ゴールド）	22（AF23）	2	2
バックグラウンド（シルバー）	10（AF11）	1	1
バックグラウンド（シルバー）	12（AF12）	1	1
バックグラウンド（シルバー）	14（AF13）	1	1
ベストエフォート	0（BE）	0	0, 3
バックグラウンド	2	0	1
バックグラウンド	4	0	1
バックグラウンド	6	0	1

LWAPP ベースの AP への QoS 機能の展開

WLAN QoS を AP に展開する場合には、次の事項を検討します。

- 有線 LWAPP AP は、レイヤ 2 CoS（802.1P）情報の読み書きを実行します。WLC と AP はレイヤ 3 分類（DSCP）情報に基づいて WLAN クライアントのトラフィック分類を伝達します。この DSCP 値は中間ルータによって変更される可能性があるため、宛先が受信する レイヤ 2 分類は、LWAPP トラフィックの送信元でマーキングされたレイヤ 2 分類を示していないことがあります。
- AP では NULL VLAN ID は使用されなくなりました。そのため、L2 LWAPP は、事実上 QoS をサポートしていません。これは、AP が 802.1P/Q タグを送らず、L2 LWAPP にはフォールバックする外部 DSCP がないためです。
- AP では、フレームを再分類するのではなく、CoS 値または WLAN プロファイルに基づいて優先度を決定します。
- AP では、無線出力ポートでのみ EDCF のようなキューイングを実行します。
- AP では、イーサネット出力ポートでのみ FIFO キューイングを実行します。

WAN QoS と H-REAP

WLC に転送されるデータ トラフィックがある WLAN の場合、動作は Hybrid Remote Edge Access Point（H-REAP; ハイブリッド リモート エッジ アクセス ポイント）以外の AP と同じです。WMM トラフィックがある、ローカルにスイッチされた WLAN の場合、AP でアップストリーム トラフィックに対して dot1q VLAN タグに dot1p 値がマーキングされます。これはタグ付き VLAN 上でだけ発生し、ネイティブ VLAN では発生しません。

ダウンストリーム トラフィックに対しては、H-REAP で、イーサネット側から受信した dot1q タグに基づき、ローカルにスイッチされた VLAN の無線で WMM 値のキューイングとマーキングが行われます。

WLAN QoS プロファイルはアップストリームとダウンストリームの両方のパケットに適用されます。ダウンストリームの場合、デフォルトの WLAN 値より高い 802.1P 値を受信したときには、デフォルトの WLAN 値が使用されます。クライアントがデフォルト WLAN 値より高い WMM 値を送信した場合、アップストリームでは、デフォルト WLAN 値が使用されます。WMM 以外のトラフィックの場合、AP からのクライアント フレームには CoS マーク付けはありません。

（注） 現在、バグ CSCsi78368 が WLC からのトラフィックの CoS マーキングに影響を及ぼしており、WLC から送信されたフレームにマーキングされている CoS が、QoS プロファイルによって設定された値を示し、クライアントがマーキングした WMM CoS を示していません。

無線 QoS 展開のガイドライン

有線ネットワークにおける QoS 展開のルールが、無線ネットワークの QoS 展開にも適用されます。QoS 展開でまず最も重要なガイドラインは、自分のトラフィックを理解することです。プロトコル、遅延に対するアプリケーションの影響度、およびトラフィックの帯域幅について理解してください。QoS によって帯域幅が増えるわけではありません。QoS では単に、帯域幅の割り当てに対する制御が強化されます。

スループット

802.11 QoS 展開で重要な検討事項は、ビット レートだけではなくフレーム サイズの視点から、提供されたトラフィックを理解することです。これは、802.11 スループットが提供されたトラフィックのフレーム サイズに敏感に反応するためです。

表 5-8 は、フレーム サイズがスループットに及ぼす影響を示しています。パケットのサイズが小さくなると、スループットも減少します。たとえば、3Mbps のレートでトラフィックを提供するアプリケーションが 11 Mbps 802.11b ネットワーク上で展開されているときに、使用するフレーム サイズの平均が 300 バイトの場合、AP 上で QoS をどのように設定してもアプリケーションのスループット要件を達成できません。これは、802.11b が、そのスループットとフレーム サイズの組み合わせでは要求されたスループットをサポートできないからです。1,500 バイトのフレーム サイズを持つ、同じ量の提供されたトラフィックでは、この問題は発生しません。

表 5-8　フレーム サイズで比較したスループット

	300	600	900	1200	1500	フレーム サイズ（バイト）
11g - 54 Mbps	11.4	19.2	24.6	28.4	31.4	スループットの Mbps
11b - 11 Mbps	2.2	3.6	4.7	5.4	6	スループットの Mbps

LAN スイッチにおける QoS の設定例

AP スイッチの設定

AP スイッチの場合、AP から渡される LWAPP パケットの DSCP を信頼する必要があるため、AP スイッチでの QoS 設定は比較的単純です。AP から送られてくる LWAPP フレームには CoS のマーキングはありません。この設定の例を以下に示します。なお、この設定では分類のみ行っています。ローカルの QoS ポリシーに応じて、必要ならキューイング コマンドを追加してください。

```
interface GigabitEthernet1/0/1
 switchport access vlan 100
 switchport mode access
 mls qos trust dscp
 spanning-tree portfast
end
```

AP DSCP 値を信頼する点においては、アクセス スイッチは WLC によりそのスイッチに対して設定されたポリシーを単に信頼しているだけです。クライアント トラフィックに割り当てられた最大 DSCP 値は、その AP 上で WLAN に割り当てられた QoS ポリシーに基づきます。

WLC スイッチの設定

WLC 接続スイッチでの QoS 分類決定は、AP 接続スイッチの場合に比べて多少複雑です。これは、WLC から送られてくるとトラフィックの DSCP を信頼するか、CoS を信頼するかの選択が可能なためです。この決定では、以下の点を考慮する必要があります。

- WLC から発信されるトラフィックは、アップストリーム（WLC またはネットワークに送信）か、またはダウンストリーム（AP および WLAN クライアントに送信）です。ダウンストリーム トラフィックは LWAPP でカプセル化されています。アップストリーム トラフィックは AP および WLAN クライアントからのトラフィックであり、WLC から発信された、LWAPP カプセル化またはカプセル開放された WLAN クライアント トラフィックです。
- LWAPP パケットの DSCP 値は WLC 上の QoS ポリシーによって制御されます。LWAPP トンネル ヘッダーによってカプセル化された WLAN クライアント トラフィックに設定されている DSCP 値は、WLAN クライアントによって設定された値から変更されていません。
- WLC から発信されるフレームの CoS 値は、アップストリーム / ダウンストリーム、カプセル化 / カプセル開放の別にかかわらず、WLC の QoS ポリシーによって設定されます。

以下の例では、WLC の設定の CoS を信頼することを選択しています。この選択の理由は、この場合、WLAN QoS を集中管理できるため、WLC 設定の他に WLC スイッチ接続で追加のポリシーを管理する必要がないことです。より詳細な制御を必要とする場合は、WLAN クライアントの VLAN 上で QoS 分類ポリシーを実装してください。

```
interface GigabitEthernet1/0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 11-13,60,61
 switchport mode trunk
 mls qos trust cos
end
```

トラフィック シェーピング、Over-the-Air QoS、および WMM クライアント

トラフィック シェーピングと Over-the-Air QoS は、WLAN WMM 機能がない場合には有用なツールですが、802.11 トラフィックの優先順位付けに直接対応しているわけではありません。WMM クライアントまたは 7920 端末をサポートする WLAN では、これらのクライアントの WLAN QoS メカニズムに頼ってください。これらの WLAN には、トラフィック シェーピングも Over-the-Air QoS も適用しないでください。

WLAN 音声および Cisco 7921G と 7920

Cisco 7921G と Cisco 7920 は Cisco の VoWLAN 端末です。WLAN に QoS を展開する一般的な理由の 1 つとして、これらの端末の使用があります。

それぞれの端末の詳細は、以下の資料を参照してください。

- Cisco Unified Wireless IP Phone 7921G バージョン 1.0（2）— http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html
- Cisco Unified Wireless IP Phone 7920 バージョン 3.0 — http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00801739bb.html

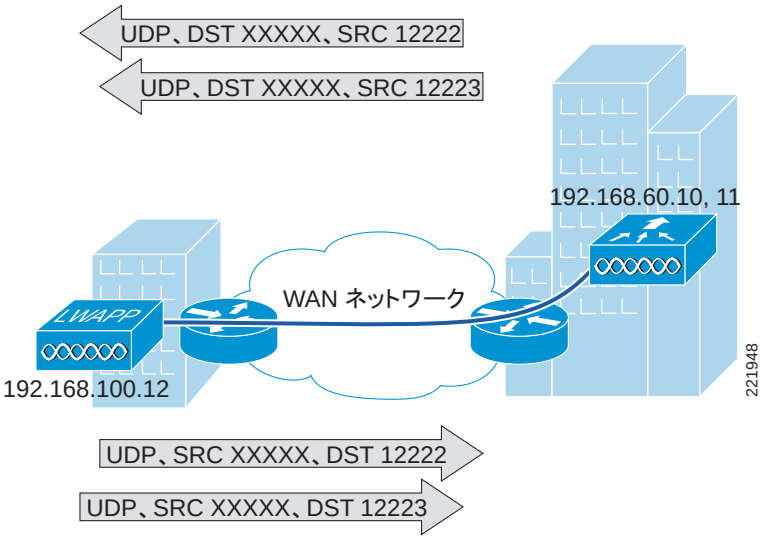
VoWLAN インフラストラクチャを展開する場合、単に WLAN に QoS を提供するだけでよいわけではありません。音声 WLAN では、サイト調査のカバレッジ要件、ユーザの挙動、ローミング要件、およびアドミッション制御について検討する必要があります。これらの要件については、以下のガイドで説明しています。

- 『Design Principles for Voice Over WLAN』 — http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/net_implementation_white_paper0900aecd804f1a46.html
- 『Cisco Wireless IP Phone 7920 Design and Deployment Guide』 — http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7920/5_0/english/design/guide/7920ddg.html

WAN 接続を介した LWAPP

この項では、LWAPP AP が 図 5-23 のように WAN リンクを介して展開されているときの QoS 戦略について説明します。

図 5-23　WAN 経由の LWAPP トラフィック



LWAPP トラフィックの分類

LWAPP AP は、通常、次の 2 つのタイプに分類されます。

- LWAPP コントロール トラフィック — UDP ポート 12223 によって識別
- LWAPP 802.11 トラフィック — UPD ポート 12222 によって識別

LWAPP コントロール トラフィック

LWAPP コントロール トラフィックは、通常、次の 2 つの追加タイプに分類されます。

- 初期化トラフィック — LWAPP AP がブートして LWAPP システムに接続するときに生成されます。たとえば、コントローラの検出、AP 設定、AP ファームウェアの更新によって生成されるトラフィックなどです。

（注） コントローラからの LWAPP イメージ パケットはベストエフォートとしてマーキングされますが、その確認応答は CS6 としてマーキングされます。この場合、プロトコルのウィンドウ機能はなく、各追加パケットは確認応答を受信してからでないと送信されません。このタイプのハンドシェイクでは、WAN からのファイルのダウンロードの影響が最小化されます。

- バックグラウンド トラフィック ― WLAN ネットワークのメンバとして動作している LWAPP AP によって生成されます。たとえば、LWAPP ハートビート、RRM、不正 AP 測定値などです。バックグラウンド LWAPP コントロール トラフィックは、CS6 としてマーキングされます。

図 5-24 と 図 5-25 は、初期 LWAPP コントロール メッセージの例を示しています。図 5-26、図 5-27、および 図 5-28 は、バックグラウンド LWAPP コントロール メッセージの例を示しています。

初期 LWAPP コントロール メッセージの完全なリストには、次のものが含まれています。

- LWAPP discovery メッセージ
- LWAPP join メッセージ
- LWAPP config メッセージ
- 初期 LWAPP RRM メッセージ

この項では AP イメージ ダウンロードについても触れていますが、通常、これは AP 初期化には含まれず、ファームウェアの変更時にのみ発生します。

図 5-24　LWAPP 検出メッセージ

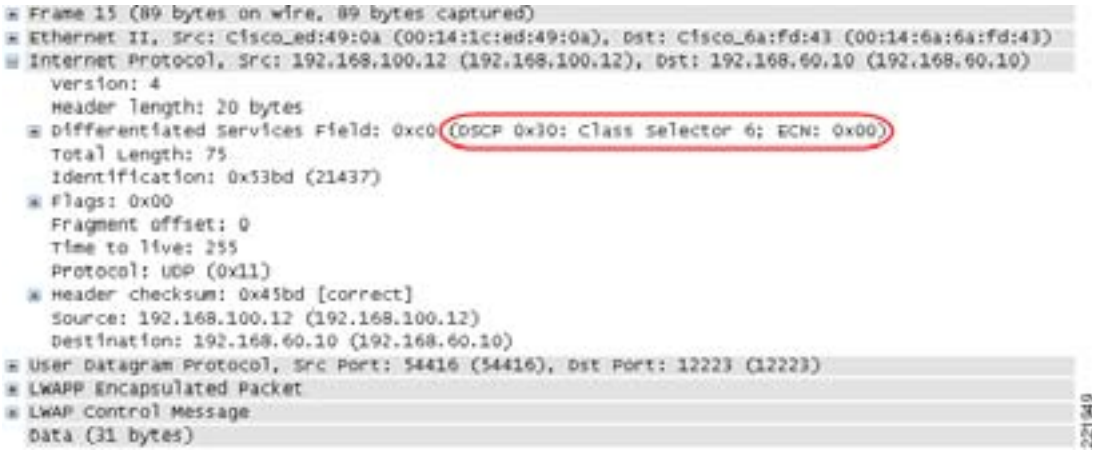


図 5-25　LWAPP イメージ応答

```
⊞ Frame 20 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_ed:49:0a (00:14:1c:ed:49:0a), Dst: Cisco_6a:fd:43 (00:14:6a:6a:fd:43)
⊟ Internet Protocol, Src: 192.168.100.12 (192.168.100.12), Dst: 192.168.60.11 (192.168.60.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
    Total Length: 60
    Identification: 0x53bf (21439)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x45c9 [correct]
    Source: 192.168.100.12 (192.168.100.12)
    Destination: 192.168.60.11 (192.168.60.11)
⊞ User Datagram Protocol, Src Port: 54416 (54416), Dst Port: 12223 (12223)
⊞ LWAPP Encapsulated Packet
⊞ LWAP Control Message
  Data (16 bytes)
```

221960

図 5-26　LWAPP ハートビート メッセージ

```
⊞ Frame 110 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Cisco_6a:fd:41 (00:14:6a:6a:fd:41), Dst: Cisco_84:15:42 (00:14:6a:84:15:42)
⊟ Internet Protocol, Src: 192.168.100.12 (192.168.100.12), Dst: 192.168.60.11 (192.168.60.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
    Total Length: 60
    Identification: 0x6cb8 (27832)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 254
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x2dd0 [correct]
    Source: 192.168.100.12 (192.168.100.12)
    Destination: 192.168.60.11 (192.168.60.11)
⊞ User Datagram Protocol, Src Port: 54416 (54416), Dst Port: 12223 (12223)
⊞ LWAPP Encapsulated Packet
⊞ LWAP Control Message
  Data (16 bytes)
```

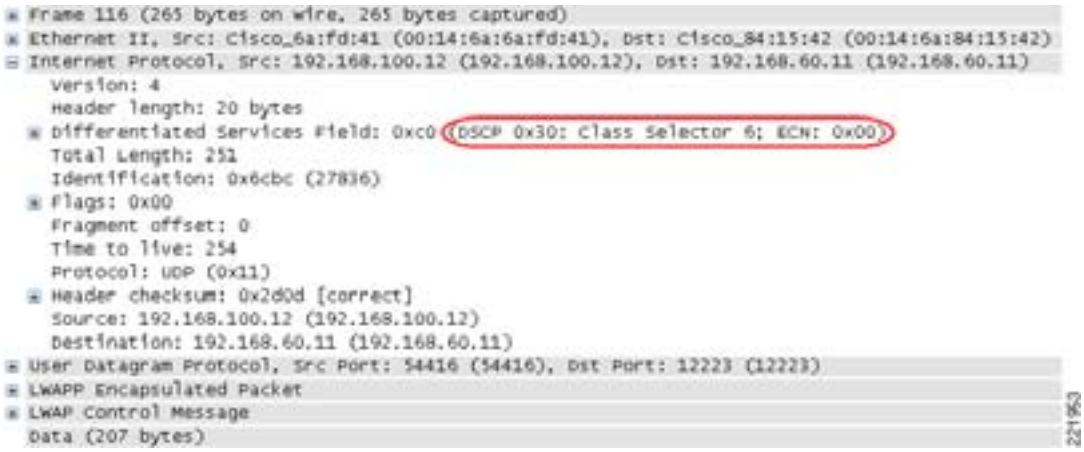
221961

図 5-27　LWAPP 統計

```
⊞ Frame 114 (202 bytes on wire, 202 bytes captured)
⊞ Ethernet II, Src: Cisco_6a:fd:41 (00:14:6a:6a:fd:41), Dst: Cisco_84:15:42 (00:14:6a:84:15:42)
⊟ Internet Protocol, Src: 192.168.100.12 (192.168.100.12), Dst: 192.168.60.11 (192.168.60.11)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
    Total Length: 188
    Identification: 0x6cbb (27835)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 254
    Protocol: UDP (0x11)
  ⊞ Header checksum: 0x2d4d [correct]
    Source: 192.168.100.12 (192.168.100.12)
    Destination: 192.168.60.11 (192.168.60.11)
⊞ User Datagram Protocol, Src Port: 54416 (54416), Dst Port: 12223 (12223)
⊞ LWAPP Encapsulated Packet
⊞ LWAP Control Message
  Data (144 bytes)
```

221962

図 5-28　LWAPP RRM



LWAPP 802.11 トラフィック

LWAPP 802.11 コントロール トラフィックは、通常、次の 2 つの追加タイプに分類されます。

- 802.11 管理フレーム ― プローブ要求やアソシエーション要求および応答などの 802.11 管理フレームは、自動的に DSCP CS6 として分類されます。
- 801.11 データ フレーム ― クライアント データとクライアントからの 802.1X データは、WLAN の QoS 設定に従って分類されますが、WLC から送られる 802.1X フレーム入りのパケットは CS4 としてマーキングされます。802.11 データ トラフィック分類は、WLAN 設定に適用されている QoS に依存します。また、自動設定はされません。WLAN データ トラフィックのデフォルトの分類はベストエフォートです。

分類に関する考慮事項

LWAPP コントロール トラフィックに使用される DSCP 分類は CS6 です。これは BGP（ボーダー ゲートウェイ プロトコル）、OSPF（Open Shortest Path First）、EIGRP（Enhanced IGRP）などの IP ルーティング プロトコルに使用される IP ルーティング クラスです。

現在の LWAPP DSCP 分類では、WLAN システムにとって最適な分類を表現していますが、各カスタマーの QoS ポリシーやニーズと一致しない可能性があります。

特に例を挙げると、WLAN ネットワークで生成される CS6 に分類されるトラフィックの量を最小化することを望むカスタマーもいます。このようなカスタマーは、プローブ要求などのクライアント アクティビティによる CS6 トラフィックの生成を停止させる必要がある場合があります。これを実行する最も簡単なメカニズムは、LWAPP 802.11 CS6 トラフィックを別の DSCP に再分類することです。LWAPP UDP の使用ポートが LWAPP データの使用ポートとは異なるため、deep packet inspection の助けを借りなくても DSCP のデフォルトのマーキングによって、このトラフィックをマーキングしなおすことができます。

また、カスタマーによっては、LWAPP 初期化トラフィックがルーティング トラフィックに絶対に影響しないようにする必要があることもあります。そのための最も簡単なメカニズムは、バックグラウンド レートを超えた LWAPP コントロール トラフィックに対して優先度を低くしたマーキングをすることです。

LWAPP トラフィックの量

Cisco のテストで、AP ごとのバックグラウンド トラフィックの平均はおよそ 305 ビット / 秒であることがわかっています。

AP ごとの初期トラフィック平均の計算はもっと難しくなります。これは、それぞれの AP がリブートしてから稼働状態になるまでの時間が、WAN の速度および WLC と AP に依存するためです。実際には、この差はごくわずかです。ラボ テスト ネットワークでの最適な初期トラフィックの場合、18 秒間で平均 2614 ビット / 秒になる可能性があります。RTT が 100 ms の WAN リンクでは、20.3 秒間で平均 2318 ビット / 秒になります。

ルータ設定の例

この項では、CS6 のマーキング変更または LWAPP コントロール トラフィックの負荷に対処する場合のガイドラインとして使用できるルータ設定の例を示します。

この例では、192.168.101.0/24 サブネット上で LWAPP AP を使用し、AP マネージャを備える WLC を 192.168.60.11 と 192.168.62.11 で使用しています。

クライアントが生成した CS6 パケットのマーキング変更

次の例では、CS6 としてマーキングされた LWAPP データ パケットをより適切な値である CS3 にマーキングしなおすための設定例を示しています。このマーキング変更によって、ネットワーク制御のレベルではなくコール制御のレベルで、トラフィックの分類がより適切な分類に変更されます。

```
class-map match-all LWAPPDATACS6
 match access-group 110
 match  dscp cs6
!
policy-map LWAPPDATACS6
 class LWAPPDATACS6
  set dscp cs3
!
interface FastEthernet0
 ip address 192.168.203.1 255.255.255.252
service-policy input LWAPPDATACS6
!
access-list 110 remark LWAPP Data
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12222
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12222
access-list 111 remark LWAPP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12223
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12223
```

定義済みのレートを超えた LWAPP コントロール トラフィックの DSCP の変更

次の例では、WAN サイトから送られる LWAPP コントロール トラフィックのレートを制限して、CS6 としてマーキングされたコントール トラフィックがルーティング トラフィックに及ぼす影響を最小化するための設定例を示しています。レート制限の設定では、非準拠のトラフィックが削除されるのではなく、単に再分類されます。

(注)　この設定は例であり、推奨ではありません。普通の状況では、WAN 接続を介した AP 展開の設計ガイドラインに従っていれば、LWAPP コントロール トラフィックが WAN ルーティング プロトコル接続に影響する可能性はほとんどありません。

```
interface Serial0
 ip address 192.168.202.2 255.255.255.252
 rate-limit output access-group 111 8000 3000 6000 conform-action transmit
exceed-action set-dscp-transmit 26
access-list 111 remark LWAPP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 12223
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 12223
!
```

WLAN QoS と 802.11e の詳細は、『IEEE 802.11 Handbook, A designers companion (second edition)』（Bob O'Hara and Al Petrick 著）を参照してください。

CHAPTER 6

Cisco Unified Wireless のマルチキャスト設計

はじめに

この章では、IP マルチキャスト転送における Cisco Unified Wireless Network のマルチキャストについて説明し、無線環境でのマルチキャストの展開方法に関する情報を提供します。マルチキャスト パフォーマンス機能を使用するための前提条件として、マルチキャスト対応ネットワークが、コントローラと Access Point（AP; アクセス ポイント）間のすべてのルータに設定されていることが必要です。マルチキャストをサポートしないネットワークに備えて、コントローラでは元のユニキャスト パケット転送メカニズムも引き続きサポートされます。

IP マルチキャストは、情報を宛先グループに配信するためのプロトコルです。IP マルチキャストでは、ネットワークのそれぞれのリンク上で情報を配信する最も効果的な戦略を使用しています。宛先へのリンクが分かれる場合にのみコピーが作成され、ネットワークのそれぞれのホップで情報のコピーが 1 つだけ送信されます。通常、現在のネットワーク アプリケーションの多くはユニキャスト パケットを使用します。つまり 1 つの送信元に 1 つの宛先が対応します。しかし、複数の受信先に対して同じデータが必要な場合、個別のユニキャスト パケットとして、送信元からすべての受信先に対してデータを複製するとネットワークの負荷が増大します。IP マルチキャストによって、動的に形成された一連の受信先に一連の送信元から効率的にデータを転送できます。

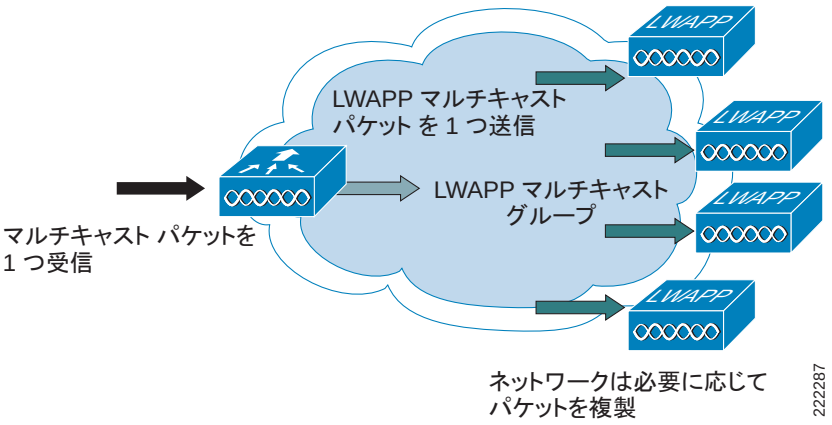
現在は、ビデオなどの、受信先の大規模なグループに宛てた一方向のストリーミングメディアには、通常 IP マルチキャストが使用されています。多くのケーブル テレビ局、教育機関、および大企業では、コンテンツの配信に IP マルチキャストを展開しています。さらに、マルチキャストを使用してオーディオおよびビデオ会議に利用されています。大学構内および商業ネットワークでマルチキャストが広く使用されているその他の例として、ファイルの配信があります。特にオペレーティング システムのイメージおよびアップデートをリモート ホストに配信する場合などです。また、金融部門で株価情報表示および "hoot-n-holler" システムなどのアプリケーション用に IP マルチキャストが展開されています。

Cisco Unified Wireless Network でのマルチキャスト転送の概要

Cisco Unified Wireless Network Software Release 4.1 では、無線ネットワークで効率的にマルチキャストを使用するためのサポートが強化されています。3.1 以前のソフトウェア リリースでは、マルチキャスト用のパケットは、実際には無線ネットワーク上のユニキャストでした。マルチキャストのサポートは、3.2 で追加されましたが、必要なブロードキャストを有効にするためにはまだ設定の制限がありました。4.1 では、コントローラ ソフトウェア リリースによってブロードキャストとマルチキャストの個別のサポートが可能になり、ネットワークをマルチキャスト、ブロードキャスト、またはマルチキャストとブロードキャスト両方での使用のために設定できるようになりました。

図 6-1 で示しているように、現在の Cisco Unified Wireless マルチキャスト サポートでは、コントローラで受信した、ファースト ホップ ルータに接続されている VLAN からの各マルチキャスト フレームはコピーされ、アソシエートされている AP のコントローラで設定されたマルチキャスト グループに送信されます。マルチキャスト パケットを含むマルチキャスト LWAPP パケットでは、WLAN ビットマップを使用します。WLAN ビットマップからは、パケットの転送に使用する必要がある WLAN の 着信 AP が通知されます。AP で LWAPP パケットが受信された場合、AP では外部 LWAPP カプセル化が取り除かれ、LWAPP WLAN ID ビットマスクで識別された（WLAN にアソシエートされているすべての無線上の）各 WLAN にマルチキャスト パケットが送信されました。

図 6-1　4.1 以前のバージョンでのマルチキャスト転送メカニズム



LWAPP マルチキャスト グループは、各アクセス ポイントにマルチキャスト パケットを送信するために効率的に使用されます。これによって、ネットワーク内のルータで、標準のマルチキャスト技術を使用してマルチキャスト パケットを AP に複製して配信できるようになります。LWAPP マルチキャスト グループでは、コントローラがマルチキャストの送信元になり、AP がマルチキャストの受信先になります。

（注） 新しいマルチキャスト パフォーマンス機能を使用するための前提条件は、マルチキャスト対応ネットワークが、コントローラと AP 間のすべてのルータに設定されていることです。マルチキャストをサポートしないネットワークに備えて、コントローラでは元のユニキャスト パケット転送メカニズムも引き続きサポートされます。

（注） マルチキャストが有効になっていると、ファースト ホップ ルータからの VLAN 上で受信されたマルチキャスト パケットはその種類にかかわらず、HSRP hello パケット、ルータの EIGRP および PIM マルチキャスト パケットすべてを含め、無線ネットワーク経由で送信されます。

管理者がマルチキャストを有効にして（マルチキャスト モードはデフォルトで無効になっています）、LWAPP マルチキャスト グループを設定すると、アクセス ポイントで、コントローラへの通常の接続プロセス中（ブート時）に、コントローラの LWAPP マルチキャスト グループのアドレスがダウンロードされます。アクセス ポイントがコントローラに接続し、コントローラの設定をダウンロードした後、そのアクセス ポイントから、コントローラの LWAPP マルチキャスト グループへの Internet Group Management Protocol（IGMP）接続要求が発行されます。これによって、コントローラと AP 間のマルチキャスト対応ルータでマルチキャスト状態に対する通常のセットアップが開始します。マルチキャスト グループの送信元 IP アドレスは、コントローラの管理インターフェイスの IP アドレスであり、レイヤ 3 モードで使用される AP マネージャの IP アドレスではありません。AP がコントローラの LWAPP マルチキャスト グループに接続すると、クライアント マルチキャスト トラフィックのマルチキャスト アルゴリズムが次に示すように機能します。

マルチキャスト グループの送信元が有線 LAN 上にある場合

- コントローラで、ファースト ホップ ルータに接続されているいずれかのクライアント VLAN からのマルチキャスト パケットが受信されると、受信されたパケットは、ベストエフォートの QoS 分類で管理インターフェイスを経由して LWAPP マルチキャスト グループに送信されます。LWAPP マルチキャスト パケットの QoS ビットは、最低レベルでハードコード化されており、ユーザが変更することはできません。
- マルチキャスト対応ネットワークでは、LWAPP マルチキャスト パケットが、LWAPP マルチキャスト グループに接続されている各アクセス ポイントに配信されます。このとき、ルータでは、マルチキャスト パケットがすべての AP に到達するように、必要に応じて配信時にパケットを複製する通常のマルチキャスト メカニズムが使用されます（図 6-1）。これによって、コントローラでマルチキャスト パケットを複製する必要がなくなります。
- アクセス ポイントでは、他のマルチキャスト パケットを受信できますが、現在の接続先のコントローラから受信したマルチキャスト パケットだけが処理され、その他のコピーは破棄されます。複数の WLAN が、元のマルチキャスト パケットの送信元 VLAN インターフェイスにアソシエートされている場合、AP からそのマルチキャスト パケットが（LWAPP ヘッダーの WLAN ビットマップに従って）各 WLAN を経由して送信されます。また、WLAN が両方の無線（802.11g および 802.11a）に設定されている場合、WLAN にアソシエートされているクライアントがあれば、それらのクライアントがマルチキャスト トラフィックを要求しなかった場合でも、両方の無線から WLAN を使用してマルチキャスト パケットが送信されます。

マルチキャスト グループの送信元が無線クライアントである場合

- マルチキャスト パケットは、標準の無線クライアント トラフィックと同様に、AP からコントローラへの LWAPP カプセル化されたユニキャストです。
- コントローラでは、マルチキャスト パケットのコピーが 2 つ作成されます。1 つ目のコピーは、マルチキャスト パケットを受信した WLAN にアソシエートされている VLAN から送信され、これによって、有線 LAN 上の受信先でマルチキャスト ストリームを受信できるようになり、ルータで新しいマルチキャスト グループを認識できるようになります。パケットの 2 つ目のコピーは、無線クライアントでマルチキャスト ストリームを受信できるように、LWAPP カプセル化され、LWAPP マルチキャスト グループに送信されます。

無線マルチキャスト ローミング

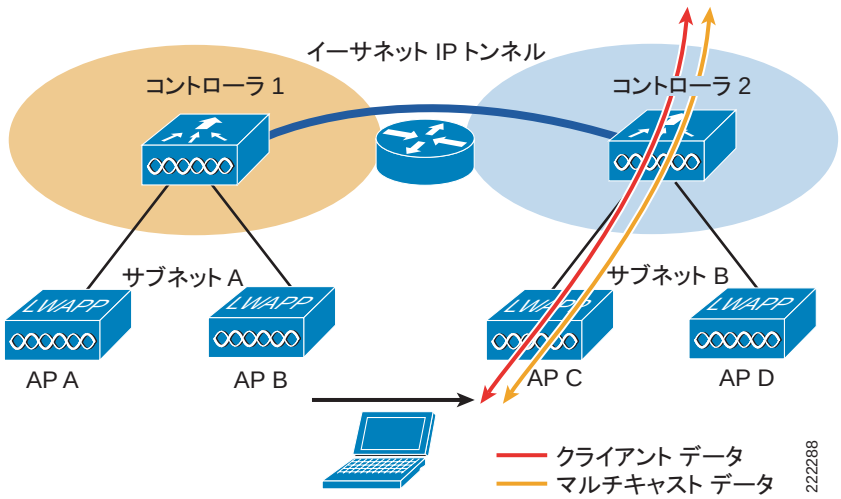
無線環境でのマルチキャスト クライアントの重要な課題は、WLAN 内を移動するときにマルチキャスト グループ メンバシップを保持することです。AP 間の移動時に無線接続でパケットドロップすると、クライアントのマルチキャストアプリケーションが中断する原因となりえます。Internet Group Management Protocol（IGMP）は、動的なグループ メンバーシップ情報の保守において重要な役割を果たします。

IGMP の基本的な知識は、クライアントのマルチキャスト セッションがネットワーク内を移動するときに何が起こっているかを理解するのに重要です。レイヤ 2 ローミングでは、外部（foreign）AP が、正しく設定されていれば、既にそのマルチキャストグループに属しており、トラフィックがネットワーク上の別のアンカーポイントにトンネルされないという単純な理由で、セッションは維持されます。レイヤ 3 ローミング環境は、この方法およびコントローラに設定したトンネリング モードに応じて、これよりもやや複雑になります。無線クライアントから送信された IGMP メッセージが影響を受けます。コントローラ上のデフォルトのモビリティ トンネリング モードは、アシンメトリックです。第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」で説明したように、これは、クライアントへのリターン トラフィックがアンカー WLC に送信されてから、アソシエートされているクライアント接続が配置されている外部 WLC に転送されることを意味します。アウトバウンド パケットは、外部 WLC インターフェイスに転送されます。シンメトリック モビリティ トンネリング モードでは、インバウンドおよびアウトバウンド トラフィックはアンカー コントローラにトンネルされます。モビリティ トンネリングの詳細は、第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照してください。

アシンメトリック マルチキャスト トンネリング

アシンメトリック マルチキャスト トンネリングで、クライアントが、別の WLC にアソシエートされた別のサブネット上の新しい AP に移動する場合、外部 WLC によってマルチキャスト グループ メンバシップが照会され、IGMP グループ メンバシップ レポートが送信されます。これにより、VLAN にアソシエートされた外部 WLC 動的インターフェイスに転送され、クライアントは外部サブネットを介してマルチキャスト ストリームに再接続します。図 6-2 は、通常のデータとマルチキャスト データのトラフィック フローを示しています。

図 6-2　アシンメトリック トンネリング



（注）　クライアントが移動する場合、マルチキャスト セッションにわずかな中断が生じます。アプリケーションによっては、使用できない場合があります。

マルチキャスト対応ネットワーク

新しいマルチキャスト パフォーマンス機能を使用するための前提条件は、マルチキャスト対応ネットワークが、コントローラと AP 間のすべてのルータに設定されていることです。マルチキャスト対応ネットワークでは、パケットをネットワーク上の多数のホストに効率的な方法で配信できます。IP マルチキャストは、1 つの情報ストリームを企業の数千もの受信先に同時に配信することによってトラフィックを軽減する帯域幅節約技術の 1 つです。パケットは、ネットワーク内の各レイヤ 3 ポイントで必要に応じて複製されます。コントローラと AP 間に複数のルータがある場合は、PIM などのマルチキャスト ルーティング プロトコルが必要です。マルチキャスト対応ネットワークの設定の詳細は、次の URL http://www.cisco.com/go/multicast を参照してください。

LWAPP マルチキャスト予約ポートおよびアドレス

コントローラでは、宛先ポートが 12222 ～ 12224 のマルチキャスト グループに送信されるマルチキャスト パケットはすべてブロックされます。また、マルチキャスト グループ アドレスが、コントローラの LWAPP マルチキャスト グループ アドレスと同じパケットはすべてコントローラでブロックされます。これによって、断片化された LWAPP カプセル化パケットが、別のコントローラから再送信されることを防止できます（詳細は、断片化と LWAPP マルチキャスト パケットを参照）。ネットワーク上のマルチキャスト アプリケーションで、これらの予約ポートまたは LWAPP マルチキャスト グループ アドレスを使用しないようにしてください。

コントローラでのマルチキャスト転送の有効化

コントローラ経由の IP マルチキャスト トラフィックはデフォルトで無効になっています。マルチキャスト トラフィックが無効な場合、WLAN クライアントではマルチキャスト トラフィックを受信できません。WLAN クライアントに対してマルチキャスト トラフィックを有効にする手順は、次のとおりです。

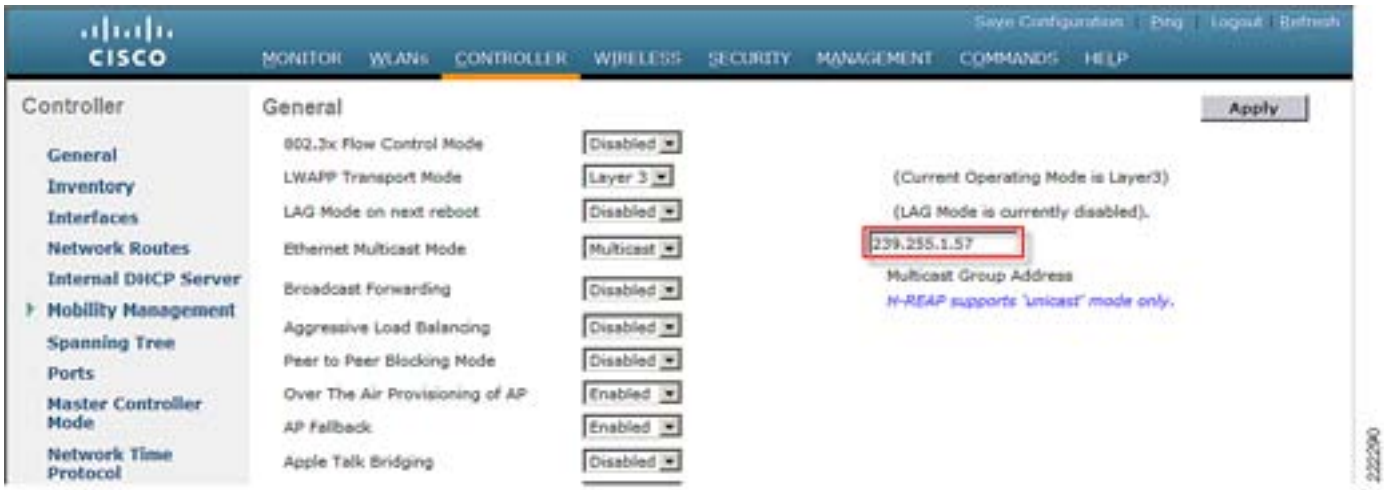
ステップ 1　マルチキャストが有効なネットワークがある場合、Ethernet Multicast Mode で **multicast** を選択して、ネットワークでパケットを複製する方法を使用します。

ステップ 2　マルチキャストが有効なネットワークがない場合、Ethernet Multicast Mode で **unicast** を選択して、コントローラでパケットを複製する方法を使用します。

ステップ 3　Controller General Web ページで、LWAPP Transport Mode が Layer 3 に設定されていることを確認します。マルチキャスト パフォーマンス機能は、このモードだけで動作します。

ステップ 4　Ethernet Multicast Mode のドロップダウン メニューから、Multicast を選択して、マルチキャスト グループ アドレスを入力します。図 6-3 にこのオプションを示しています。

図 6-3　GUI を使用して Ethernet Multicast Mode を有効にするコマンド



Ethernet Multicast Mode を有効にする CLI コマンド

ステップ 1　CLI コマンド：**configure network multicast global enable** を有効にします

ステップ 2　CLI コマンド：**config network multicast mode multicast** *<IP アドレス>* を有効にします

show network コマンドを使用して、コントローラでマルチキャスト モードになっていることを確認し、**show lwapp mcast** を使用して、AP のグループを確認します。他には、ルータで **show ip mroute** および **show ip igmp membership** を使用すると便利です。

マルチキャスト展開における考慮事項

LWAPP マルチキャスト アドレスの選択における推奨事項

注意　OSPF、EIGRP、PIM、HSRP、およびその他のマルチキャスト プロトコルで使用される予約済みリンク ローカル マルチキャスト アドレスを含め、任意のマルチキャスト アドレスを LWAPP マルチキャスト グループに割り当てることができますが、お勧めしません。

シスコでは、管理用スコープのブロック 239/8 からマルチキャスト アドレスを割り当てることをお勧めします。IANA では、プライベート マルチキャスト ドメインで使用するために、管理用スコープのアドレスとして 239.0.0.0 ～ 239.255.255.255 の範囲が予約されています（その他の制限については、次に示す注意を参照）。これらのアドレスは、RFC 1918 で定義されている予約済みのプライベート IP ユニキャストの範囲（10.0.0.0/8 など）と事実上よく似ています。ネットワーク管理者は、インターネット上での競合を気にすることなく、管理しているドメイン内でこの範囲のマルチキャスト アドレスを自由に使用できます。この管理用またはプライベートのアドレス空間は、企業内で使用する必要があり、Autonomous System（AS; 自律システム）を出入りしないようブロックする必要があります。

（注）　239.0.0.*X* または 239.128.0.*X* アドレス範囲を使用しないでください。これらの範囲のアドレスは、リンクのローカル MAC アドレスとオーバーラップしており、IGMP スヌーピングが有効になっている場合でもすべてのスイッチ ポートがフラッディングします。マルチキャスト MAC アドレスの重複の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00802d4643.shtml#wp1002391

シスコでは、企業ネットワーク管理者がこのアドレス範囲を企業ネットワーク内のさらに細かい地理上の管理用スコープに分けて、特定のマルチキャスト アプリケーションのスコープを限定することをお勧めします。これによって、高レートのマルチキャスト トラフィックがキャンパス（帯域幅が十分）から出て WAN リンクを混雑させることを防止できます。また、高帯域幅のマルチキャストを効率的にフィルタリングすることによって、高帯域幅のマルチキャストがコントローラおよび無線ネットワークに到達することを防止できます。

マルチキャスト アドレスのガイドラインの詳細は、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00802d4643.shtml

断片化と LWAPP マルチキャスト パケット

コントローラで受信されたマルチキャスト パケットは、宛先アドレスとして LWAPP マルチキャスト グループを使用して LWAPP 内にカプセル化され、管理インターフェイス（送信元アドレス）経由で AP に転送されます。リンクの MTU を超えるパケットの場合は、コントローラによってパケットが断片化され、両方のパケットが LWAPP マルチキャスト グループに送信されます。別のコントローラが、この LWAPP カプセル化マルチキャスト パケットを有線ネットワーク経由で受信すると、パケットが再カプセル化される可能性があり、通常のマルチキャスト パケットのように処理されて、このコントローラの AP に転送されることになってしまいます。

これを防止するには、次の 2 つのオプションがあり、いずれのオプションもそれ自体で効果があります。1 つ目のオプションは、すべてのコントローラを同一の LWAPP マルチキャスト グループ アドレスに割り当てます。2 つ目のオプションは、標準のマルチキャスト フィルタリング技術を適用して、LWAPP カプセル化マルチキャスト パケットが他のコントローラに送信されないようにします。表 6-1 は、これら 2 つの技術の長所と短所を示しています。

表 6-1　同一のマルチキャスト グループを使用する場合と異なるグループを使用する場合の長所と短所

	長所	短所
すべてのコントローラの LWAPP マルチキャスト グループを同一にする	追加の断片化保護処理を施す必要がありません。	各コントローラのマルチキャスト トラフィックがネットワーク全体でフラッディングします（AP で、AP のコントローラ管理インターフェイスと同じ送信元 IP アドレスを持たないマルチキャスト パケットがドロップされます）。
標準のマルチキャスト技術を使用して LWAPP マルチキャスト フラグメントをブロックする	アドレス範囲を使用できるため、ネットワーク全体のフラッディングを防止できます。	マルチキャスト対応コントローラに設定されているすべての VLAN に接続されているファースト ホップ ルータに、ACL フィルタリングを適用する必要があります。

すべてのコントローラの、同一 LWAPP マルチキャスト グループへの割り当て

2 つ目のコントローラからこれらの LWAPP カプセル化パケットが再送信されないように、コントローラで、LWAPP マルチキャスト グループおよび LWAPP 予約ポート宛ての着信マルチキャスト パケットをブロックします。予約ポートをブロックすることによって、コントローラはカプセル化された LWAPP マルチキャスト パケットの断片化パケットの最初の部分をブロックします。ただし、2 つ目のパケットにはポート番号が含まれていないため、2 つ目のパケットは、マルチキャスト グループ アドレス（宛先アドレス）でフィルタするだけでブロックできます。コントローラは、宛先アドレスが、コントローラに割り当てられている LWAPP マルチキャスト グループ アドレスと同じになっているパケットをすべてブロックします。

ただし、各コントローラを同じ LWAPP マルチキャスト グループに割り当てると、別の問題が生じます。AP で LWAPP マルチキャスト グループへの接続に使用される IGMP バージョン 1 および 2 は、Any Source Multicast（ASM）であるため、AP では、ネットワーク内のマルチキャスト グループのすべての送信元からのマルチキャスト トラフィックを受信します。つまり、AP では、ネットワーク上のすべてのコントローラが同一のマルチキャスト グループ アドレスで設定されている場合も、それらのコントローラからのマルチキャスト パケットを受信し、マルチキャスト境界は適用されません。1 つのコントローラのマルチキャスト トラフィックが、ネットワーク全体のすべての AP にフラッディングし、各 AP では、ネットワーク全体の無線マルチキャスト クライアントから送信されているマルチキャスト トラフィックを受信します（送信元アドレスが AP のコントローラの管理アドレスとは異なる場合はドロップします）。ローカルから送信された、HSRP、PIM、および EIGRP などのクライアント VLAN からのマルチキャスト パケットおよび OSPF マルチキャスト パケットもネットワーク全体でフラッディングします。

（注） Cisco IOS AP（1240 など）では IGMPv2 が使用され、VxWorks AP（1030 など）では IGMPv1 が使用されます。

標準のマルチキャスト技術を使用した、WLAN 上のマルチキャストの制御

通常の境界技術をマルチキャスト対応ネットワークで使用する必要があります。これらの技術には、IP マルチキャスト トラフィックおよび Auto-RP メッセージをフィルタリングする **ip multicast boundary** インタフェースモードコマンドの使用が含まれます。

(注)　マルチキャスト境界が適用されていない場合、ネットワーク内の任意の場所にある有線クライアントは、LWAPP マルチキャスト ストリームを要求して、すべての送信元からそのストリームを受信できます。マルチキャスト ストリームは、LWAPP マルチキャスト パケットにカプセル化されている場合は暗号化されていません。したがって、このようなアクセスを防ぐためにマルチキャスト境界を実装することをお勧めします。

以前は、IP マルチキャスト データグラムの Time To Live フィールドで、**ttl-threshold** コマンドを使用して、Auto-RP の管理用境界を作成していました。このタスクは、IP マルチキャスト トラフィックおよび Auto-RP メッセージをフィルタリングする **ip multicast boundary interface mode** コマンドの使用に代わってきています。シスコでは、新しいコマンドを使用することをお勧めします。

その他の有用なコマンドとして、**ip multicast rate-limit** インタフェースコマンドがあります。このコマンドでは、無線 VLAN で低レートが強制されます。このコマンドを使用しないと、ネットワーク エンジニアが高レート マルチキャスト アドレスをフィルタリングする場合でも、低レート マルチキャスト アドレスはそのレートを超過できません。

無線クライアント VLAN の一般的な例を次に示します。マルチキャスト対応ネットワークに使用するその他のマルチキャスト コマンドの詳細は、http://www.cisco.com/go/multicast を参照してください。マルチキャスト対応トラフィックにフィルタリングを実行することによって、Sasser ワームなどの、マルチキャスト アドレスを使用した TCP および ICMP 転送に依存する特定ワームの伝搬を防ぐことができます。マルチキャスト グループ アドレスを使用してこれらのタイプのトラフィックをブロックしても、これらのアドレスでは通常、ストリーミングに UDP または TCP が使用されるため、ほとんどのアプリケーションに影響はありません。

次の例では、任意の送信元からのマルチキャスト グループ範囲 239.0.0.0 ～ 239.127.255.255 宛てのパケットのパケット レートが 128 Kbps に制限されます。この例では、下位の管理用スコープ アドレスには含まれないマルチキャスト アドレスすべてに境界が設定されます。また、Vlan40 を使用するホストは、239.0.0.0 ～ 239.127.255.255 の下位管理用グループだけに接続できるようになります。

```
mls qos
!
class-map match-all multicast_traffic
  description Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0
  match access-group 101
!
policy-map multicast
 description Rate Limit Multicast traffic to 2.56mps with burst of 12800 bytes
  class multicast_traffic
   police cir 2560000 bc 12800 be 12800 conform-action transmit exceed-action drop
!
interface Vlan40
 description To Wireless Clients
 ip address 10.20.40.3 255.255.255.0
 ip pim sparse-mode
 ip multicast boundary 1
 ip igmp access-group 30
 standby 40 ip 10.20.40.1
 standby 40 preempt
 service-policy output multicast
!
access-list 1 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
multicast boundary
access-list 1 permit 239.0.0.0 0.127.255.255
!
access-list 30 remark Only Allow IGMP joins to this Multicast Group Range
access-list 30 permit 239.0.0.0 0.127.255.255
!
access-list 101 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
class-map
access-list 101 permit ip any 239.0.0.0 0.127.255.255
```

コントローラの配置がマルチキャスト トラフィックおよびローミングに与える影響

（注） 分散型と中央集中型のどちらの展開においても、マルチキャスト　ストリームのレートは制限されず、ACL は保存できません。有効になると、マルチキャスト トラフィックは、HSRP、EIGRP、OSPF、および PIM パケットを含む無線に転送されます。

ここでは、分散型と中央集中型の 2 種類の展開について説明し、それぞれの展開がマルチキャスト クライアントのローミングに与える影響について示します。中央集中型の展開では、WLC WLAN インターフェイスは同じ VLAN/ サブネットに接続され、マルチキャスト クライアントが WLC の AP から他の WLC の AP に移動する際にマルチキャスト ストリームは中断されません。中央集中型の展開では、フラットな WLC クライアント マルチキャスト ネットワークが作成されます。中央集中型の WLC がマルチキャスト ローミングに影響を与えることがない理由は、マルチキャスト ストリームが、特定の WLAN を使用する 1 つのマルチキャスト クライアントから要求されると、マルチキャスト トラフィックを要求したクライアントが 1 つも WLAN アクセス ポイントにアソシエートされていなくても、マルチキャスト ストリームが、この WLAN を使用する、すべての無線（802.11g および 802.11a）、すべての WLC に接続されているすべての AP に対して出力されるためです。VLAN にアソシエートされている WLAN が複数ある場合は、AP からマルチキャスト パケットが WLAN ごとに送信されます。ユニキャスト モードとマルチキャスト モードの LWAPP パケットには両方とも、パケットの転送で経由する必要のある WLAN を受信側 AP に伝える WLAN ビットマップが含まれます。

分散型の展開では、WLAN が同じでも、WLC が別の VLAN に接続されるため、このような問題はありません。これは、マルチキャスト クライアントが新しい WLC に移動するときに、WLC がクライアントのマルチキャスト グループ メンバシップについて最初に照会するということです。この時点で、クライアントはグループ メンバシップ レポートを送信し、WLC によって、ローカル VLAN にアソシエートされた VLAN 経由でこのメッセージが適切なマルチキャスト グループ アドレスに転送されます。これにより、クライアントは外部 WLC を介してマルチキャスト セッションを再開できます。

分散型展開では、WLAN SSID が同じであっても WLC は異なる VLAN に接続されているため、AP 上のマルチキャスト トラフィックの量が軽減されます。WLAN マルチキャスト トラフィックは、WLC の VLAN のクライアント要求によって異なります。表 6-2 は、分散型と中央集中型の展開の長所と短所を示しています。

表 6-2　中央集中型 WLC および分散型 WLC の長所と短所

	長所	短所
中央集中型のすべての WLC WLAN が同じ VLAN（サブネット）に接続されている	いずれのクライアント VLAN で開始したマルチキャスト トラフィックでもすべての AP に送信されるため、いずれの AP にローミングしてもクライアントはマルチキャスト ストリームを受信します。	1 つのクライアントだけがマルチキャスト トラフィックを要求した場合、すべてのコントローラに接続されているすべての AP がストリームを受信して、AP にアソシエートされているクライアントがある場合はそれらのクライアントがマルチキャスト ストリームを要求しなかった場合でも AP からストリームを送信します。
異なる VLAN およびサブネットに接続されている分散型 WLC	マルチキャスト ストリームは、対象のコントローラに接続されている AP に分離されます。	クライアントの移動後にマルチキャスト ストリームを確立したことによる中断

その他の考慮事項

マルチキャスト展開におけるその他の考慮すべき 2 つの分野は、AP グループの実装時、および H-REAP と REAP の実装時です。AP グループで、同じコントローラ上の AP は、同じ WLAN（SSID）を別の VLAN にマップできます。異なるグループの AP 間でのクライアントの移動は現在サポートされていないため、この操作をするとマルチキャスト セッションが正しく機能しません。現在、WLC は WLAN で設定された VLAN に対してのみマルチキャストを転送し、AP グループで設定された VLAN については考慮しません。

REAP および H-REAP AP を使用すると、WLAN のローカル終端が WLC ではなくネットワーク エッジで可能になり、マルチキャスト動作がそのエッジで制御されます。H-REAP WLAN が WLC で終端し、マルチキャストがその WLC で有効になっている場合に、H-REAP ネットワークが存在する場所まで LWAPP マルチキャストグループを拡張することが許可されているときは、マルチキャストは、その H-REAP WLAN に配信されます。

LWAPP マルチキャスト パケットをネットワーク経由で H-REAP に送信できない場合でも、これらはユニキャスト メッセージであるため、その H-REAP の WLAN クライアントは、WLC に接続されているネットワークに IGMP 接続要求を送信できます。

CHAPTER 7

Cisco Unified Wireless Hybrid REAP

このガイドですでに説明したとおり、Cisco Unified Wireless ソリューションは、LWAPP AP（LAP）と WLAN コントローラ（WLC）の間で Lightweight Access Point Protocol（LWAPP）を使用して、AP を管理すると共に WLAN クライアント トラフィックを伝達します。

ローカライズされた 1 つ以上の WLC を使用した LAP の展開は、中規模から大規模のキャンパス環境では一般的です。しかし、小規模のブランチ ロケーションでは無線接続を必要としていても、WLC の展開が実用的でないケースも考えられます。メイン キャンパスに中央集中型 WLC を配置し、ブランチでは標準の LAP を展開する場合、LAP は WAN 経由でメイン キャンパスへの LWAPP 接続を確立します。ブランチのすべての無線ユーザ トラフィックは WAN を経由して中央集中型 WLC に送信されます。この方法は、ブランチからアクセスするサービスの大半がメイン キャンパスに存在する場合には有効です。しかし、ブランチの無線クライアントがローカルのネットワーク リソース（プリンタやサーバなど）にアクセスする必要がある場合、クライアント トラフィックがローカル デバイスに送信されるまでに WAN を 2 度経由（ブランチから中央、中央からブランチ）しなければならないため、この方法は有効ではありません。このため、リモート エッジ AP（REAP）と Hybrid REAP（H-REAP）が開発されました。

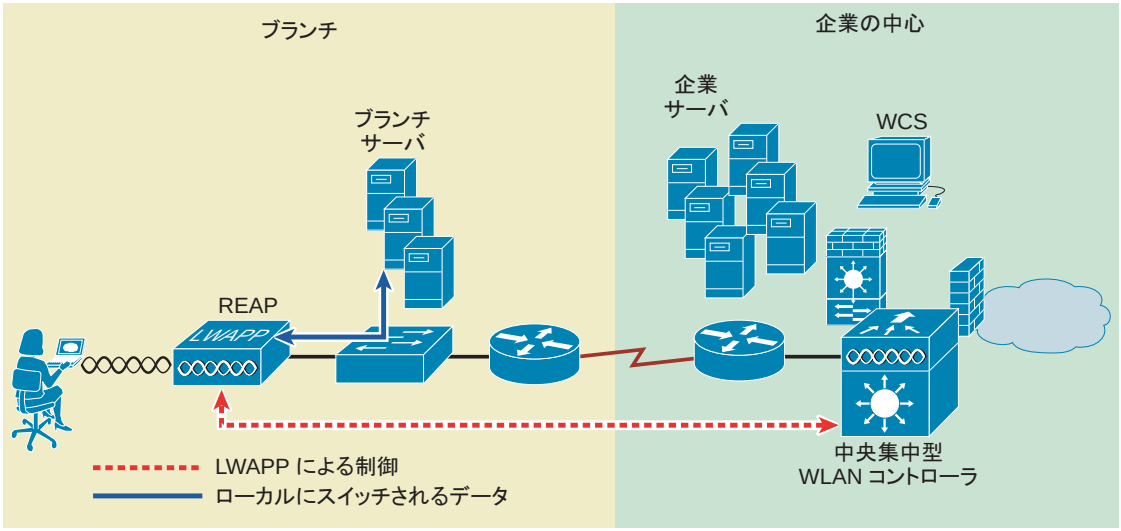
リモート エッジ AP

リモート エッジ AP（REAP）は、次のようなリモート（ブランチ）ロケーションに展開するために設計された特別な目的を持つ LWAPP ベース AP です。

- ブランチまたはリモート ロケーションの無線ユーザが、ローカルのネットワーク リソースにアクセスする必要がある環境。または、WAN リンクの停止時にローカル無線接続を維持する必要がある環境。
- ローカル接続が必要な中央サイトとリモート ロケーションの間の WAN 帯域幅が制限されている環境。このシナリオでは、帯域幅が制限された WAN リンクを通じて（標準の IP パケットで）リモート サイトにルートバックするためだけに、すべての無線ユーザ トラフィックを中央集中型 WLC へトンネルするのは非現実的です。
- 特定の場所に対して適切な無線カバレッジを提供するために必要な AP が 2 ～ 3 台の環境。これは通常、特に無線カバレッジの必要な小規模のリモート サイトが多数存在する場合に、すべての場所で WLC を展開して管理するよりもコスト効率が高くなります。

REAP AP は、LWAPP コントロール プレーンを WLAN データ プレーンから切り離すことによって、このようなリモートのブランチ ロケーションのニーズに対応できるように設計されています。これによって、LWAPP の制御および管理データが中央集中型 WLC に戻される間、WLAN はレイヤ 2 スイッチ上でローカルに終端することができます。この方法では、中央集中型アーキテクチャの利点が維持されます。図 7-1 は、高水準の REAP トポロジの図を示しています。

図 7-1　高水準 REAP トポロジ



シスコの REAP AP 1030 は、最大 16 の WLAN をサポートできます。すべての WLAN はローカルにスイッチできますが、1030（REAP の動作に合わせた設定時）には、標準的な中央集中型トポロジに展開された LWAPP AP と比較して、次のような制限があります。

- 802.1Q トランキングをサポートしていません。すべての WLAN が単一のローカル VLAN/ サブネット上で終端します。
- WAN リンクが停止すると、WLAN 1 以外のすべての WLAN が無効になり、ブロードキャストされなくなります（ブロードキャストが有効な場合）。

シスコでは、802.1Q トランキング経由で WLAN を VLAN にマップすることが可能な Hybrid リモート エッジ AP（H-REAP）と呼ばれる新しいバージョンの REAP を導入することで、このような制限に対処しています。さらに、H-REAP AP は、ローカル スイッチング WLAN と中央スイッチング WLAN を同時にサポートできます。この章では以降、主に H-REAP AP の適用、機能、制限事項、および構成について説明し、該当する場合は、H-REAP プラットフォームと従来の 1030 REAP プラットフォームの違いを明らかにします。

Hybrid REAP

サポートされているプラットフォーム

WLC

H-REAP AP は、バージョン 4.0 以降のソフトウェア イメージを持つ、次の WLC プラットフォームでサポートされます。

- Cisco 2100 シリーズ
- Cisco 4400 シリーズ
- Cisco 6500 シリーズ WiSM
- Cisco WLC Module for Integrated Service Router（ISR）
- Cisco Catalyst C3750G-24WS

アクセス ポイント

次の LWAPP 対応 AP は、H-REAP 機能をサポートしています。

- Cisco 1131 シリーズ
- Cisco 1242 シリーズ

Cisco 1130 シリーズと 1240 シリーズの AP に関する詳細は、AP（P. 2-10）を参照してください。

IOS ベースの 1130/1240 シリーズ AP を LWAPP モードの動作に変換するためのガイドラインについては、次の URL にアクセスしてください。
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

H-REAP 機能は、Cisco 1000 シリーズの LWAPP AP ではサポートされません。ただし、基本的な REAP 機能は 1030 でもサポートされています。

H-REAP の用語

この項では、H-REAP の用語と定義について概要を説明します。

スイッチング モード

H-REAP AP は、無線ユーザ トラフィックを単一の VLAN のみにマップ可能な 1030 シリーズの REAP AP とは異なり、WLAN ごとに次のスイッチング モードを同時にサポートできます。

- ローカル スイッチング：ローカル スイッチング WLAN は、802.1Q トランキング経由で別個の VLAN 隣接するルータまたはスイッチのいずれか）に無線ユーザ トラフィックをマップします。必要に応じて、1 つ以上の WLAN を同じローカル 802.1Q VLAN にマップできます。

ローカル スイッチング WLAN にアソシエートされたブランチ ユーザは、そのトラフィックをオンサイト ルータによって転送します。オフサイト（中央サイト）宛のトラフィックは、ブランチのルータによって、標準の IP パケットとして転送されます。

AP の制御および管理に関連するすべてのトラフィックは、LWAPP 経由で別々に中央集中型 WLC に送信されます。

- 中央スイッチング：中央スイッチング WLAN は、LWAPP 経由で、無線ユーザ トラフィックとすべてのコントロール トラフィックを、ユーザ トラフィックが WLC 上の動的なインターフェイスまたは VLAN にマップされている中央集中型 WLC にトンネルします。これは、LWAPP モードの通常の動作です。

  中央スイッチング WLAN にアソシエートされたブランチ ユーザのトラフィックは、中央集中型 WLC に直接トンネルされます。そのユーザが（そのクライアントがアソシエートされた）ブランチ内部のコンピューティング リソースと通信する必要がある場合、そのユーザのデータは WAN リンクを通じて標準の IP パケットとしてブランチ ロケーションに戻されます。WAN リンクの帯域幅によっては、望ましい結果が得られない場合があります。

動作モード

H-REAP AP には、次の 2 種類の動作モードがあります。

- 接続モード：WLC に到達可能な状態です。このモードでは、H-REAP AP と WLC が LWAPP 接続されます。
- スタンドアロン モード：WLC に到達できない状態です。H-REAP は、WLC との LWAPP 接続を失ったか、または確立に失敗しました。この状態は、ブランチ サイトと中央サイト間の WAN リンクが停止した場合などに発生します。

H-REAP の状態

H-REAP WLAN は、その構成とネットワーク接続によって、次のいずれかの状態に分類できます。

- 中央認証 / 中央スイッチング：WLAN が 802.1x、VPN、または Web などの中央認証方式を使用している状態です。ユーザ トラフィックは、LWAPP 経由で WLC に送信されます。この状態は H-REAP が接続モードの場合にのみサポートされます（図 7-2 を参照）。この例では、802.1X が使用されていますが、他のメカニズムも同様に適用できます。
- 認証ダウン / スイッチング ダウン：H-REAP がスタンドアロン モードのときに、中央スイッチング WLAN 上記）は、ビーコン送信とプローブ応答を停止します。既存のクライアントはアソシエート解除されます。
- 中央認証 / ローカル スイッチング：WLAN は中央認証を使用しますが、ユーザ トラフィックは、ローカルにスイッチされます。この状態は H-REAP が接続モードの場合にのみサポートされます（図 7-3 を参照）。この例では、802.1X が使用されていますが、他のメカニズムも同様に適用できます。
- 認証ダウン / ローカル スイッチング：中央認証が必要な WLAN 上記参照）が、新しいユーザを拒否します。すでに認証済みのユーザは、セッションのタイムアウトまで引き続きローカルにスイッチされます（セッションのタイムアウトが設定されている場合）。WLAN にアソシエートされている（既存の）ユーザがなくなるまで、WLAN はビーコン送信およびプローブ応答を継続します。この状態は、AP がスタンドアロン モードに移行した結果として発生します（図 7-4 を参照）。
- ローカル認証 / ローカル スイッチング：WLAN がオープン、静的 WEP、共有、または WPA2 PSK セキュリティ方式を使用している状態です。ユーザ トラフィックはローカルにスイッチされます。これらのセキュリティ方式だけが、H-REAP がスタンドアロン モードになったときにローカルでサポートされます。WLAN はビーコン送信およびプローブ応答を継続します（図 7-5 を参照）。既存のユーザは接続されたままで、新しいユーザ アソシエーションが受け入れられます。AP が接続モードの場合、これらのセキュリティ タイプの認証情報は WLC に転送されます。

図 7-2　中央認証 / 中央スイッチング WLAN

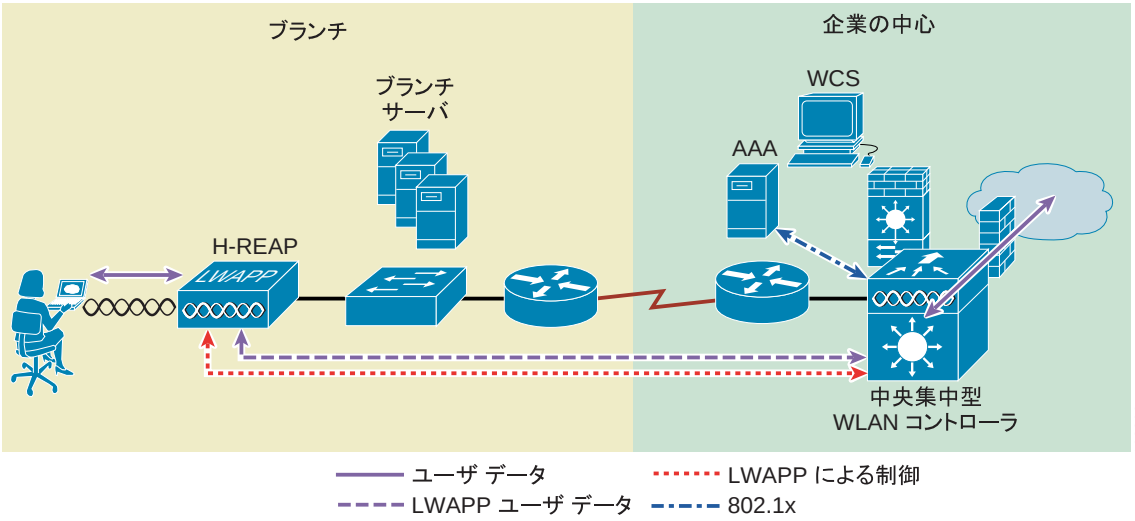


図 7-3　中央認証 / ローカル スイッチング WLAN

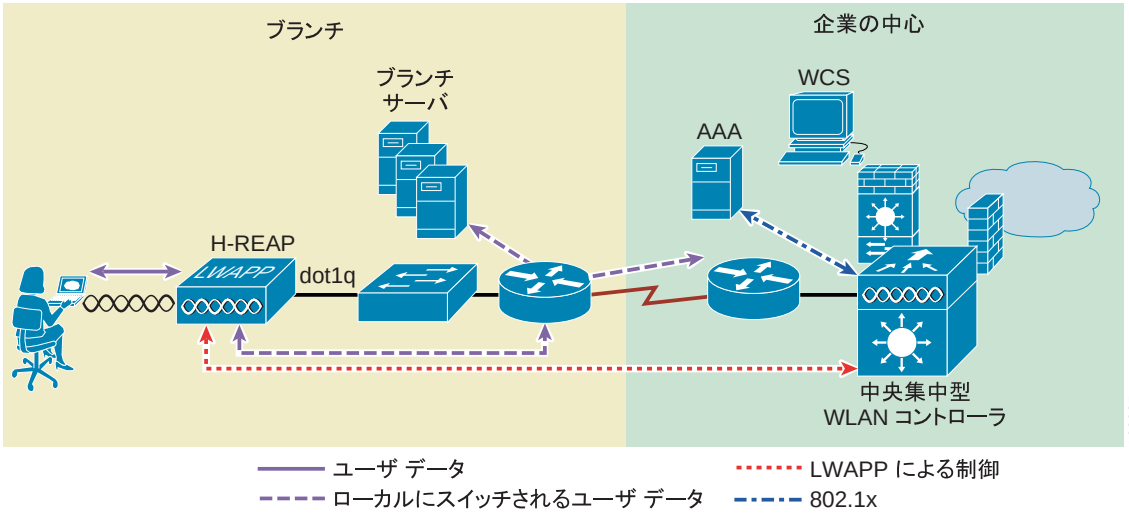


図 7-4　認証ダウン / ローカル スイッチング

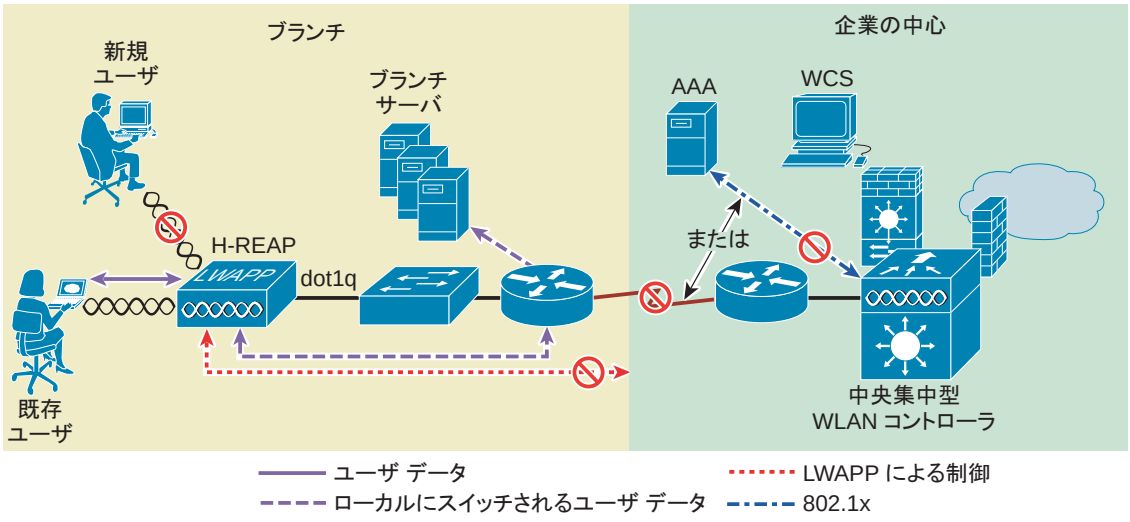
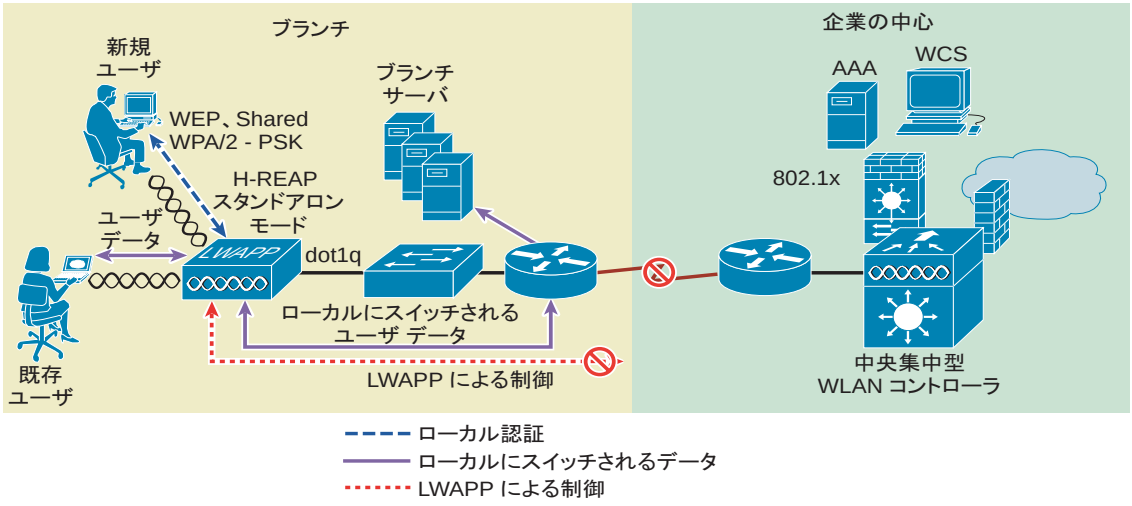


図 7-5　ローカル認証 / ローカル スイッチング WLAN



（注） AP がどの動作モードにあるかに関係なく、すべての 802.11 認証およびアソシエーション処理が H-REAP で発生します。接続モードのときは、H-REAP はすべてのアソシエーション / 認証情報を WLC に転送します。スタンドアロン モードのときは、AP はこれらのイベントを WLC に通知することができません。そのため、中央認証 / スイッチング方式を使用する WLAN を使用することができません。

H-REAP アクセス ポイントは、スタンドアロン モードに移行後、ローカル スイッチング WLAN のクライアント接続を維持します。ただし、アクセス ポイントが WLC との接続を再確立すると、すべての既存のクライアントをアソシエート解除し、WLC からのアップデートされた設定情報を（必要に応じて）適用し、クライアント接続を再度可能にします。

適用

H-REAP AP は、その拡張機能によって、次のようにさらにより柔軟に展開できます。

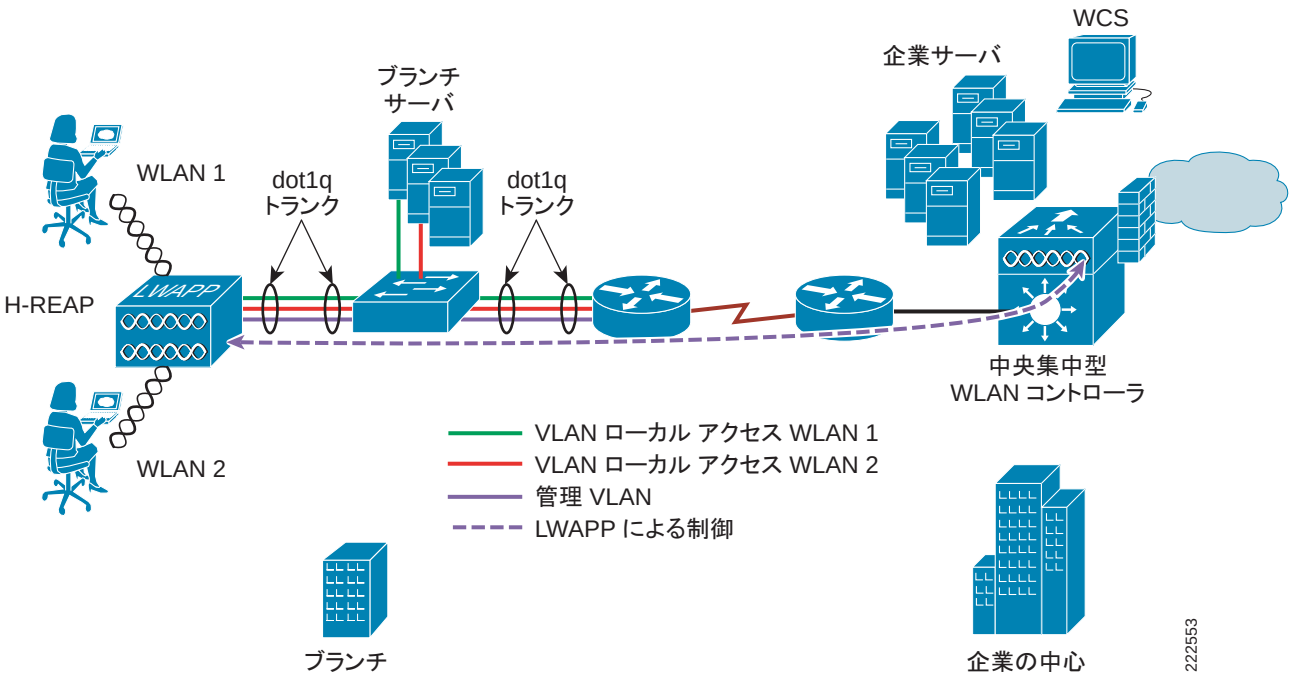
- ブランチの無線接続
- ブランチのゲスト アクセス
- パブリック WLAN ホットスポット

ブランチの無線接続

REAP と H-REAP の第 1 の目標は、無線ユーザ トラフィックを WAN 上で中央集中型の WLC にトンネルするのではなく、ローカルで終端させるというブランチ ロケーションの無線接続のニーズに対応することです。

H-REAP は個々の WLAN を特定の 802.1Q VLAN にマップできるため、ブランチ ロケーションではより効率的にセグメンテーション、アクセス コントロール、および QoS ポリシーを各 WLAN 上に実装できます。図 7-6 を参照してください。

図 7-6　H-REAP トポロジ



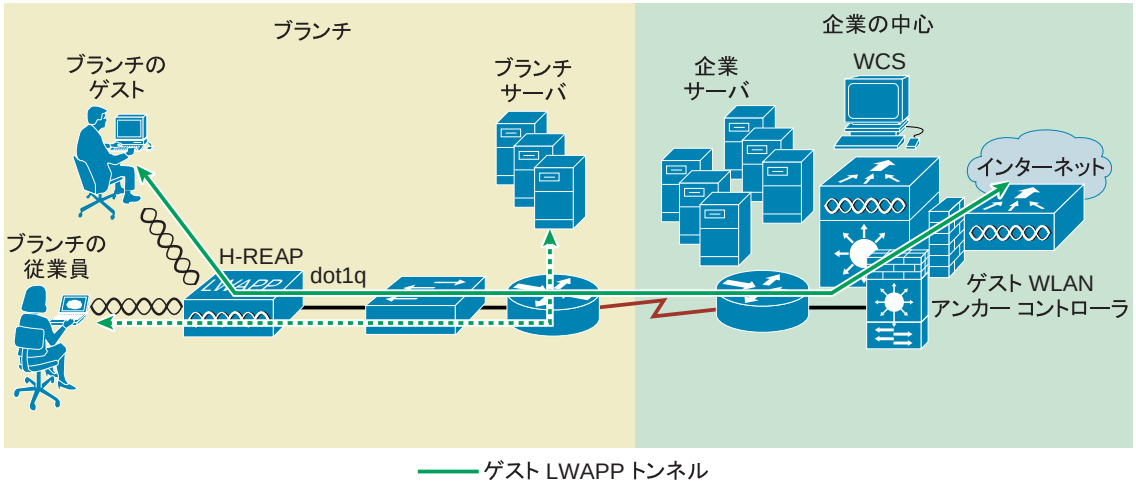
ブランチのゲスト アクセス

標準の REAP AP をブランチで使用する場合の課題の 1 つは、次の理由から実現が困難なゲスト アクセスの実装です。

- すべての WLAN は同一のローカル VLAN にマップされるため、ゲスト ユーザとブランチ ユーザの区別およびセグメント化が難しくなります。
- すべてのユーザ トラフィックはローカルにスイッチされるため、何とかしてゲスト アクセス トラフィックをセグメント化して中央サイトにルートバックし、アクセス コントロールと認証を実施する必要があります。または、ブランチでローカル インターネット アクセスが使用可能な場合は、セグメンテーションとアクセス コントロールの両方をローカルに実装する必要があります。

H-REAP AP は、ローカルと中央の同時スイッチングを導入することによって、このような課題の克服を支援します。H-REAP トポロジでは、ゲスト アクセス用に指定された SSID/WLAN を LWAPP 経由で中央集中型 WLC にトンネルできます。この中央コントローラでは、対応するインターフェイスまたは VLAN を直接、Cisco SSG/ISG、Cisco NAC アプライアンスなどのアクセス コントロール プラットフォームのインターフェイスにスイッチすることが可能です。または、中央集中型 WLC 自体で、ゲスト アクセス WLAN に対する Web 認証を実行できます。いずれの場合も、ゲスト ユーザのトラフィックが、他のブランチ オフィスのトラフィックから分割（分離）されます。図 7-7 は、H-REAP AP を使用したゲスト アクセス トポロジの例を示しています。詳細は、第 10 章「Cisco Unified Wireless Guest Access Service」を参照してください。

図 7-7　H-REAP の中央スイッチングを使用したブランチのゲスト アクセス



中央 Web 認証を使用する（ゲスト）WLAN を、ブランチでローカルにスイッチされるように設定することもできます。この場合、ブランチ クライアントは、Web 認証のためだけに中央集中型 WLC（仮想アドレス 1.1.1.1）にリダイレクトされます。認証後、すべてのクライアント トラフィックは、H-REAP 設定に基づきローカル VLAN インターフェイスを通してスイッチされます。Web ログインまたはログオフにアソシエートされている（WLC 仮想アドレス宛ての）すべてのトラフィックは、LWAPP 経由で中央集中型 WLC に直接トンネルされます。

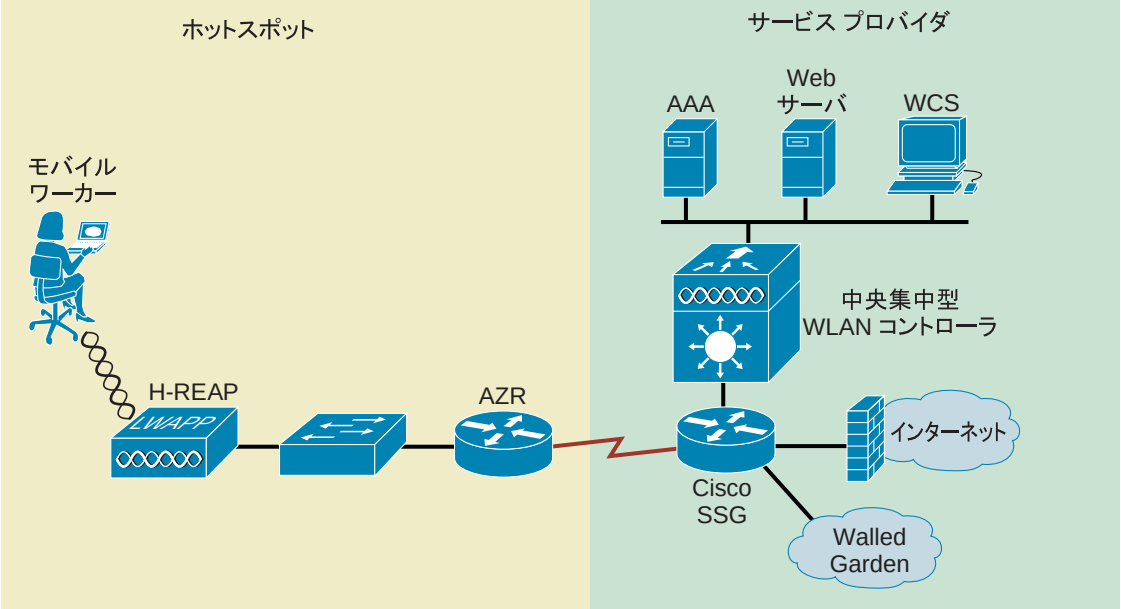
パブリック WLAN ホットスポット

多くのパブリック ホットスポットのサービス プロバイダが、複数の SSID/WLAN の実装を始めています。この理由の 1 つは、オペレータが、Web ベースのアクセス用のオープンな認証 WLAN と、より安全なパブリック アクセス用に 802.1x/EAP を使用する別の WLAN を提供することを希望しているためです。

WLAN を個別の VLAN にマップできる H-REAP AP は、1、2 台の AP しか必要としない小規模地域のホットスポット展開で、スタンドアロン AP に取って代わっています。

図 7-8 は、H-REAP AP を使用したホットスポット トポロジの例を示しています。

図 7-8　H-REAP ローカル スイッチングを使用したホットスポット アクセス



Unified Wireless 機能のサポート

H-REAP モードの動作に基づく、サポートされている機能および認証タイプのマトリクスについては、表 7-1 を参照してください。

表 7-1　サポートされている機能および認証タイプ

機能	接続モード 中央スイッチング	接続モード ローカル スイッチング	スタンドアロン モード	備考
認証オープン	あり	あり	あり	
認証共有	あり	あり	あり	
認証 WPA/2-802.1x	あり	あり	なし	AP がスタンドアロン モードに移行すると、既存の認証済みクライアント セッションは接続されたままですが、新しい認証はできなくなります。WLC 接続が復元されない場合、WLAN ビーコン / プローブ応答は、最後のクライアントのアソシエート解除までサポートされます。
認証 WPA/2-PSK	あり	あり	あり	AP がスタンドアロン モードに移行すると、既存の認証済みクライアントは接続されたままで、新しいクライアント接続が許可されます。
認証ゲスト アクセス（Web 認証）	あり	あり	なし	
VPN	あり	あり	なし	
L2TP	あり	あり	なし	
NAC	あり	あり	なし	
CCKM 高速ローミング	なし	なし	なし	
PKC 高速ローミング	なし	なし	なし	
CAC および TSPEC	あり	あり	なし	

表 7-1　サポートされている機能および認証タイプ（続き）

機能	接続モード 中央スイッチング	接続モード ローカル スイッチング	スタンドアロン モード	備考
クライアント ロード バランシング	なし	なし	なし	
ピアツーピア ブロッキング	あり	なし	なし	
WIDS	あり	あり	なし	
RLDP	あり	あり	なし	
RADIUS/TACACS 認証	あり	あり	なし	
RADIUS/TACACS アカウンティング	あり	あり	なし	

展開の考慮事項

次の項では、H-REAP AP の展開に関するさまざまな実装と運用上の注意について説明します。

WAN リンク

H-REAP AP を予想どおりに機能させるためには、WAN リンク特性に関する次のことに留意してください。

- 遅延：特定の WAN リンクに 100 ms を超える遅延を許可すべきではありません。AP は、30 秒ごとにハートビート メッセージを WLC に送信します。ハートビート応答がない場合、AP は 5 回連続（1 秒に 1 回ずつ）でハートビート メッセージを送信して、まだ接続しているかどうかを確認します。接続が失われている場合は、H-REAP AP がスタンドアロン モードに切り替わります（動作モードの定義については、動作モード（P. 7-4）を参照）。AP 自体は、比較的高い遅延耐性を持っています。ただしクライアントでは、AP は、認証に関連付けられたタイマーがリンク遅延に対して敏感であり、そのために、<100 ms の制約が要求されます。そうでなければ、クライアントは、認証のタイムアウトを待機することになり、それによって、ルーピングなどの、その他の予測不可能な動作が発生する可能性があります。
- 帯域幅：所定のロケーションで最大 8 台の H-REAP が展開されている場所での展開には、WAN リンクは 128 Kbps 以上が必要です。8 台を超える H-REAP を展開する場合、比例的により高い帯域幅が WAN リンクに提供される必要があります。
- パス MTU：WLC ソフトウェア リリース 4.0 以降では、500 バイト以上の MTU が必要で、これは、1030 REAP と H-REAP AP の両方に適用されます。

ローミング

先に述べたように、H-REAP AP が接続モードのときは、すべてのクライアント プローブ、アソシエーション要求、802.1x 認証要求、および対応する応答メッセージが LWAPP コントロール プレーンを経由して H-REAP AP と WLC の間で送受信されます。このことは、AP がスタンドアロン モードのときに、オープン、静的 WEP、および WPA PSK ベースの WLAN など、これらの認証方式を使用するために LWAPP 接続を必要としない場合にも当てはまります。

- 動的 WEP/WPA：これらのキー管理方式の 1 つを使用して H-REAP AP 間をローミングするクライアントは、ローミングを行うたびに完全な認証を実行します。認証が成功すると、新しいキーが AP とクライアントに渡されます。この動作は、標準の中央集中型 WLAN 展開と同じですが、H-REAP トポロジでは WAN 上でリンク遅延変動があり、それがローミングにかかる合計時間に影響する可能性があります。使用されている WAN 特性、RF 設計、バックエンド認証ネットワーク、および認証プロトコルによって、ローミング時間が 50 ～ 1,500 ms の間で変化する場合があります。

- WPA2：クライアントのローミングにかかる時間を短縮するために、WPA2 では IEEE 802.11i 仕様に基づくキー キャッシング機能を導入しています。シスコでは、この仕様に Proactive Key Caching （PKC）と呼ばれる拡張機能を追加しました。現在 PKC は、Microsoft の Zero Config Wireless サプリカントと Funk（Juniper）の Odyssey クライアントでのみサポートされています。Cisco CCKM も WPA2 と互換性があります。

  WLAN が中央またはローカルにスイッチされるかに関係なく、H-REAP は PKC をサポートしません。そのため、H-REAP AP 間をローミングする PKC 対応クライアントは、完全な 802.1x 認証を受けることになります。無線 IP テレフォニーなどのアプリケーションをサポートする、予測可能な高速ローミングが必要なリモートのブランチ ロケーションでは、ローカル WLC（サービス統合型ルータ用の Cisco WLC2100 または NM-WLC）の展開を検討する必要があります。

- Cisco Centralized Key ManagementCCKM- シスコが開発したプロトコルで、CCKM 対応クライアントのセキュリティ資格情報は WLC にキャッシュされ、モビリティ グループ内の他の AP に転送されます。クライアントが他の AP にローミングおよびアソシエートするとき、その資格情報が AP に転送されるため、2 段階プロセスでクライアントを再びアソシエートして認証できます。これにより、AAA サーバでの完全認証を実行する必要がなくなります。現在、H-REAP AP は CCKM 高速ローミングをサポートしていません。そのため、CCKM 対応クライアントは、ある H-REAP から別の H-REAP に移動するたびに、完全な 802.1x 認証を受けます。

- レイヤ 2 スイッチの CAM テーブルの更新：クライアントがローカルにスイッチされる WLAN 上で、ある AP から別の AP にローミングしたときに、現在の H-REAP は、クライアントがポートを変更したことをレイヤ 2 スイッチに通知しません。スイッチは、クライアントがデフォルト ルータに対して ARP 要求を実行するまで、クライアントがローミングしたことを認識しません。この動作は、わずかですが、ローミング性能に影響を与える可能性があります。

（注） （所定のローカル スイッチング WLAN 上で）WLAN を異なる VLAN/ サブネットにマップする H-REAP 間をローミングするクライアントは、ローミング先のネットワークに適した IP アドレスを含むように IP アドレスを更新します。

Radio Resource Management

接続モードの間、すべての Radio Resource Management（RRM）機能は、基本的に使用可能です。ただし、一般的な H-REAP 展開は少数の AP で構成されているため、ブランチ ロケーションで RRM 機能が動作しない場合があります。たとえば、Transmit Power Control（TPC）を行うために、最低 4 台の H-REAP がお互いに近接している必要があります。TPC なしでは、カバレッジ ホール保護などの機能が使用できません。Cisco Auto RF 機能に関する詳細は、第 3 章「WLAN 無線周波の設計に関する考慮事項」を参照してください。

ロケーション サービス

上記で述べたように、H-REAP 展開は一般的に所定のロケーションで少数の AP のみで構成されます。シスコでは、高レベルのロケーション確度を達成するため、AP の数と配置に関する完全なガイドラインを用意しています。または、H-REAP 展開からロケーション情報を取得することも可能ですが、リモート ロケーション展開で確度のレベルは大きく異なる可能性があります。したがって、シスコの設計上の推奨事項に従う場合を除いて、一般的な H-REAP 展開で最適なロケーション確度の仕様を達成できる可能性は非常に低くなります。詳細は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf

QoS の考慮事項

中央でスイッチされる WLAN では、H-REAP は標準の LAP と同様に QoS を処理します。ローカルにスイッチされる WLAN は、QoS を異なる方法で実装します。

WMM トラフィックにローカルでスイッチされる WLAN の場合、AP はアップストリーム トラフィックに対する dot1q VLAN タグの dot1p 値をマーク付けします。これはタグ付き VLAN でだけ発生し、ネイティブ VLAN では発生しません。

ダウンストリーム トラフィックの場合、H-REAP はローカルにスイッチされるイーサネットから受信する dot1p タグを使用し、RF リンクを通して所定のユーザ宛てのフレームにアソシエートされている WMM 値をキューに入れ、マーク付けします。

WLAN QoS プロファイルは、アップストリーム パケットとダウンストリーム パケットの両方に適用されます。デフォルト WLAN 値より高い 802.1p 値を受信した場合、ダウンストリームでは、デフォルト WLAN 値が使用されます。クライアントがデフォルト WLAN 値より高い WMM 値を送信した場合、アップストリームでは、デフォルト WLAN 値が使用されます。WMM 以外のトラフィックの場合、AP からのクライアント フレームには CoS マーク付けはありません。

詳細は、第 5 章「Cisco Unified Wireless QoS」を参照してください。

DSCP 設定に基づいてトラフィックが正しく処理されるために、適切なキューイング / ポリシング メカニズムを WAN 上で実装することを強くお勧めします。適切なプライオリティ キューは、（DSCP CS6 でマーク付けされている）LWAPP コントロール トラフィックのために予約して、輻輳が原因で接続モードとスタンドアロン モード間を H-REAP が間違って循環しないようにする必要があります。

H-REAP を使用した WLC 展開上の一般的な考慮事項

キャンパス内のいずれの WLC も H-REAP をサポートすることは可能ですが、ブランチ ロケーションの数および展開される H-REAP 合計数によって、H-REAP 展開をサポートするための専用 WLC を使用することは（管理上の観点から）有効です。

H-REAP は一般的にメイン キャンパス内で LAP と同じポリシーを共有せず、各ブランチ ロケーションは、基本的に独立した RF およびモビリティ ドメインです。単一 WLC を複数の論理 RF およびモビリティ ドメインに分割できない場合でも、専用 WLC によって、ブランチ固有の設定およびポリシーを論理的にキャンパスから切り離すことができます。

展開した場合、専用 H-REAP WLC をメイン キャンパスのものとは異なるモビリティおよび RF ネットワーク名を使用して設定する必要があります。「専用」WLC に接続されたすべての H-REAP は、その RF および モビリティ ドメインのメンバとなります。

ここでは、Auto-RF の観点から、十分な H-REAP が所定のブランチ内に展開されたと想定します（Radio Resource Management（P. 7-11）参照）。WLC は、各ブランチにアソシエートされている RF カバレッジを自動管理しようとします。

独自のモビリティ ドメインに統合された H-REAP が存在しても、利点（または不都合）はありません。これは、クライアント トラフィックがローカルにスイッチされるためです。EoIP モビリティ トンネルは、クライアントと H-REAP とのローミングが発生する（同じモビリティ ドメインの）WLC 間で呼び出されません。

専用 WLC が H-REAP 展開に使用される場合、ネットワークの可用性を確保するためにバックアップ WLC も展開する必要があります。標準の LAP の展開では、指定された WLC とのアソシエーションを強制するために、WLC 優先度を H-REAP に設定する必要があります。

WAN リンクの中断

動作モード（P. 7-4）から H-REAP の状態（P. 7-4）の項で説明したように、特定の H-REAP モードと機能では、WLC と LWAPP コントロール プレーンを接続する必要があります。H-REAP がスタンドアロン モードのときに影響を受ける機能の概要を次に示します。

EAP 802.1x WLAN と Web 認証 WLAN

クライアントがローミングする、またはセッションが再認証されるまで、既存のローカル スイッチング クライアントが接続されたままになります。新たなクライアント認証が許可されません。

既存の中央スイッチング クライアントが切断され、新たなクライアント認証は許可されません。

H-REAP の状態（P. 7-4）で説明したように、オープン、静的 WEP、または WPA/2-PSK で構成された WLAN は、接続モードとスタンドアロン モードのどちらでも機能するため、802.1x や Web 認証などの RADIUS サービスを必要とする WLAN と同じような影響は受けません。リモートのブランチ ロケーションで WAN リンクの中断時に無線接続を維持する必要がある場合は、上述した 3 つのレイヤ 2 セキュリティ ポリシーの 1 つに基づいてバックアップ WLAN を実装することをお勧めします。この中では、WPA2-PSK が最も強力なセキュリティを提供するため、これを強くお勧めします。

その他の機能

次の機能は、H-REAP がスタンドアロン モードのときは使用できません。

- H-REAP でローカル管理される DFS サポートを除く無線リソース管理
- 無線による侵入検知
- ロケーションベースのサービス
- NAC
- 不正デバイス検出
- AAA Override

無線構成

次の無線構成情報は、H-REAP がスタンドアロン モードのときに維持されます。

- DTIM
- ビーコン期間
- 短いプリアンブル
- 電力レベル
- 国番号
- チャネル番号
- ブラックリスト

H-REAP の制限事項と注意事項

ローカル スイッチングの制限事項

WLC 上で次のセキュリティ方式のいずれかが特定の WLAN に対して構成された場合は、その WLAN を H-REAP AP でローカル スイッチングに構成することはできません。

- IPSEC

- CRANITE
- FORTRESS[1]

(注)　外部集約プラットフォームへの VPN パススルーは許可されます。ただし、WLC が強要する VPN パススルー制限は許可されません。

サポートされる WLAN の最大数

H-REAP AP は 8 つの WLAN をサポートします。そのため、H-REAP AP がサポートする WLAN の ID は、1 ～ 8 にする必要があります。WLAN ID の 9 ～ 16 は伝播されません。

ネットワーク アドレス変換（NAT/PAT）

WLC

LAP は異なる 2 つの IP アドレスを使用して 2 段階で WLC と通信するため、WLC は AP との通信時に NAT 境界の背後に配置することはできません。

- WLC ディスカバリ：LAP は最初に、WLC の管理 IP アドレスを使用して WLC のリストを照会します。管理 IP は、DHCP オプション 43 または DNS を介して取得するか、手動で構成できます（初期設定（P. 7-18）を参照）。検出フェーズは、AP が接続する WLC を適格な WLC のリストから特定するために使用されます。これは、適格な WLC の AP 管理 IP アドレスを含む LWAPP コントロール メッセージを送信することによって伝達されます。
- WLC の接続：AP は取得した AP 管理 IP アドレスを使用して適格な WLC に接続します。AP 管理 IP アドレスは、NAT でサポートすることはできません。これは、AP がこのアドレスを検出フェーズで取得するためです。NAT の 1:1 関係が確立されている場合でも、WLC は、AP が WLC と接続するために使用する IP アドレスとして、AP マネージャの外部 NAT アドレスを渡すことができません。

AP

標準の 1:1 静的 NAT は、NAT 境界の背後にある 1 台以上の AP をサポートするために使用できます。また、複数の LAP（H-REAP または標準）も PAT を使用できます。このシナリオでは、単一の IP NAT プールが「過負荷」に設定されるか、WAN インターフェイス（またはループバック インターフェイス）が「過負荷」で使用されます。次に、過負荷（PAT）方式が使用されたときの動作の概要を示します。

1. AP はブート時に、「内部ローカル」の IP アドレスを DHCP から取得し、LWAPP コントロール ポート 12223 を使用して、ランダムな送信元ポート（5xxxx）で WLC ディスカバリ プロセスを開始します。Cisco IOS PAT は、AP によって選択された内部ローカルの送信元ポート番号を保存し、「NAT プール」IP アドレスまたはインターフェイス IP アドレス（内部グローバル）を使用して変換を行います。次の例を参照してください。

```
Pro Inside global     Inside local        Outside local      Outside global
udp 10.20.3.19:54417 192.168.1.121:54417 10.15.9.253:12223  10.15.9.253:12223
```

2. AP が WLC に接続し、802.11 データがアップストリームに送信された後、IOS PAT プロセスは 802.11 データ トラフィックを同じ内部ローカル ポート番号を使用して発信し、LWAPP ポート 12222 を使用して WLC に送信します。次の例を参照してください。

```
Pro Inside global     Inside local        Outside local      Outside global
udp 10.20.3.19:54417   192.168.1.121:54417 10.15.9.253:12222 10.15.9.253:12222
```

3. WLC から AP に送信されたすべてのトラフィックは、管理データか 802.11 データかに関係なく、内部グローバル IP アドレスおよびポート番号 54417 上記の例を想定）に送信されます。そこで、IOS PAT はデータを適切な内部ローカル アドレスに変換します。各 AP は WLC との通信に一意の送信元ポートを使用しているため、複数の AP をサポートできます。

上記の例の PAT 変換は、初めて AP がブートするときに行われます。ただし、AP は 2 度目と場合によっては 3 度目をしばしばリセットし、リセットするたびに新しい IP アドレスを取得します（DHCP が使用されていると想定）。AP は同じ内部ローカル送信元ポート番号を異なる内部ローカル IP アドレスと共に使用しようと試みているため、PAT プロセスに問題が生じます。最初の変換エントリがまだ存在するため、PAT は新しい（一意の）内部グローバル送信元ポートを作成します。次の例を参照してください。

```
Pro Inside global       Inside local         Outside local      Outside global
udp 10.20.3.19:54417    192.168.1.121:54417 10.15.9.253:12222 10.15.9.253:12222
udp 10.20.3.19:54417    192.168.1.121:54417 10.15.9.253:12223 10.15.9.253:12223
udp 10.20.3.19:1322     192.168.1.122:54417 10.15.9.253:12222 10.15.9.253:12222
udp 10.20.3.19:1323     192.168.1.122:54417 10.15.9.253:12223 10.15.9.253:12223
```

上記の例では、AP が 2 度目をリセットした後で PAT が作成した変換に注目してください。内部ローカル 192.168.1.121 の最初の変換エントリは、AP が新しい IP の取得時にリセットしたため、使用されなくなります。このシナリオでは、AP は内部ローカル IP 192.168.1.122 と送信元ポート 1323 を使用して WLC と通信しており、問題はありません。問題は、802.11 データが WLC に送信されたときに発生します。上記の例では、LWAPP 管理データとして同じ内部グローバル ポート（1323）によって発信される代わりに、PAT は別のポート 1322 を使用して 802.11 データを発信します。WLC は 802.11 データを受信しますが、1323 を使用してすべての 802.11 データを AP に返します。このポートのミスマッチのため、AP は 802.11 データを受信せず、事実上 LWAPP データ プレーンを中断します。

（注） これは、中央でスイッチされる WLAN 特有の問題です。ローカルにスイッチされる WLAN は、それらの WLAN 用の WLC ポート 12222 に 802.11 データが送信されないため、影響を受けません。

回避策は次のとおりです。

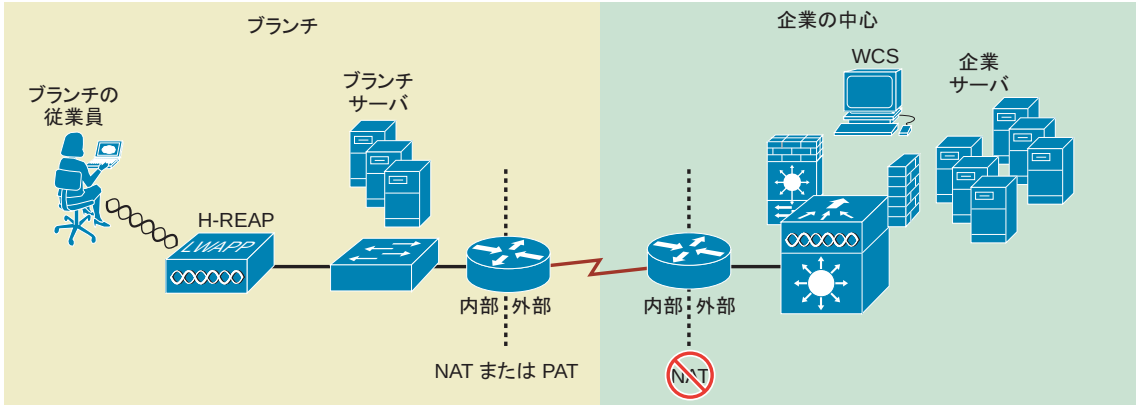
- 動的 DHCP が使用された場合、よりアグレッシブな NAT 変換エントリのタイムアウトを UDP ポートの 12222 と 12223 に確立します。これらのポートの変換タイムアウトを 20 ～ 25 秒の間で設定します。20 秒未満の場合、AP が WLC とのアソシエーションを失うリスクがあります。設定時間が長すぎると、古くなったエントリはすばやくタイムアウトしない場合があり、AP が望ましくないポートを使用し続けることになります。次の設定例を参照してください。

```
ip nat translation port-timeout udp 12222 20
ip nat translation port-timeout udp 12223 20
```

- 各 AP に静的 DHCP 予約を作成します。AP が連続リセットを実行する場合、AP は同じ IP を使用し続け、PAT はセカンダリまたはターシャリ送信元ポート バインディングを作成しません。このオプションは、DHCP をリモート / ブランチ ロケーションでローカルに実装する場合にのみ実用的です。
- PAT 対象の AP に IP アドレスを手動で割り当てます。IP 設定オプションについては、H-REAP の設定（P. 7-18）を参照してください。この場合も同様に、AP が連続リセットを実行する場合、AP は同じ IP を使用し続け、PAT はセカンダリまたはターシャリ送信元ポート バインディングを作成しません。

図 7-9 は、NAT/PAT を使用した H-REAP を示しています。

図 7-9　NAT/PAT を使用した H-REAP



RADIUS 割り当て VLAN

RADIUS ベースの VLAN 割り当ては、中央スイッチング H-REAP WLAN でサポートされます。この機能は、H-REAP がスタンドアロン モードのときは使用できません。

Web 認証（ゲスト アクセス）

WLC ベースの Web 認証は、H-REAP が接続モードである限り、ローカル スイッチング WLAN と共に使用できます。Web 認証を使用するこのような WLAN は、H-REAP がスタンドアロン モードのときは使用することができません。

クライアント間通信の制限

（H-REAP による）ローカル スイッチング WLAN にアソシエートされた 2 台以上のクライアントは、WLC 上のピアツーピア ブロッキング モードが有効な場合でも、相互の通信が阻害されることはありません。これは、ローカルにスイッチされる無線トラフィックが WLC を経由しないためです。

中央でスイッチされる H-REAP WLAN では、WLC 上のピアツーピア ブロッキング モード設定に基づいて、クライアント間通信が制限されます。

H-REAP のスケーリング

- サイトごと：リモート ロケーションごとに展開できる H-REAP の数に制限はありません。ただし、次の場合はローカル WLC の展開を強くお勧めします。
  - リモート ロケーションが VoWLAN の展開を計画している場合。ローミング（P. 7-10）で説明したように、ローミング性能は、WAN のバックホールの可用性とリンク特性の影響を受ける可能性があります。これは、802.11i や Cisco CCKM などのキー キャッシング方式が使用されている場合にも、これらの方式は H-REAP で現在サポートされていないため、当てはまります。
  - WAN の信頼性 / 性能：認証、無線リソース管理、およびその他のアップストリーム サービスに依存するブランチの WLAN トポロジが、WAN バックホールの可用性にのみ左右される場合。往復遅延は 100 ms 以下に制限される必要があり、輻輳を管理するために適正な QoS キューイング メカニズムが使用できる必要があります。
- WLC ごと：H-REAP モードで動作可能な AP の台数に制限はありません。WLC ごとの H-REAP AP の総数は、特定の WLC モデルでサポートされる LAP の最大数にだけ制限されます。

インライン電源

以前の Cisco 1030 シリーズ REAP AP は 802.3af のみをサポートしていますが、Cisco 1130 シリーズと 1240 シリーズの AP は、シスコのインライン電源仕様と 802.3af 標準の準拠の両方をサポートしています。

管理

H-REAP AP は、標準的な LWAPP AP の管理と同様に、WLC の GUI または Cisco Wireless Control SystemWCS を介して管理および監視できます。唯一の例外は、H-REAP が、WAN 停止が原因で到達不可能になった場合です。管理および WCS の詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/partner/products/ps6305/products_data_sheet0900aecd802570d0.html

http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/ccfig41.html

H-REAP の設定

初期設定

適格な Cisco 1130 または 1240 シリーズ AP では、WLC に接続して H-REAP の動作に合わせて設定できるように、次の最低限の情報を必要とします。

- IP アドレス
- デフォルト ゲートウェイのアドレス
- 1 台以上の WLC の管理インターフェイス IP アドレス

これらの情報は、次の 4 種類の方法のいずれかで入手できます。

- シリアル コンソール ポート経由の静的な設定
- WLC アドレスが静的に設定された DHCP
- DHCP オプション 43 （第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照）
- WLC アドレスの DNS 解決を使用する DHCP（第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照）

シリアル コンソール ポート

以前の 1030 シリーズ REAP とは違って、1130 と 1240 シリーズの AP には、接続用の基本パラメータの設定に使用可能なシリアル コンソール ポートが用意されています。コンソール ポート方式で初期設定を行う手順は、次のとおりです。シリアル コンソール ポート方式は、AP が WLC に接続されておらず、LWAPP イメージ 12.3(11)JX 以降を実行している場合にのみ使用できます。

（注） ステップ 4 a. と d. は、H-REAP AP に IP アドレスを割り当てるためにブランチで DHCP が使用されていない場合にのみ実行します。使用するアドレスは、所定のブランチ ロケーションで使用されているアドレス方式に準拠する必要があります。

（注） 次のシリアル コンソール手順は、「初期状態で」初めて展開された新しい LAP に対してのみ実施できます。次の手順は、以前に WLC と接続 / 通信したことのある LAP に使用することはできません。

ステップ 1　標準の Cisco DB9/RJ45 コンソール ケーブルを使用して、Hyper Terminal またはその他の互換性のある端末通信ソフトウェアを実行しているラップトップに AP を接続します。すべてのシスコ製デバイスと同様に、シリアル パラメータを 9600bps、8 データ ビット、1 ストップ ビット、およびフロー制御なしに設定する必要があります。

ステップ 2　AP の電源を入れます。コンソール ポートを介して AP を設定する場合は、AP をネットワークに接続しないでください。AP が WLC を検出して接続すると、下記に示す設定を実行することができなくなります。したがって、最初の設定が完了するまで AP をネットワークから切断しておく必要があります。

ステップ 3　AP がローカル イメージのロードを完了したら、**enable** と入力してから、有効なパスワードとして **Cisco** と入力して、exec セッションを確立します。

ステップ 4　<ap-mac-address># プロンプトで、次のコマンドを使用して IP、マスク、ゲートウェイ、ホスト名、およびプライマリ WLC を設定します。

a. **lwapp ap ip address** <IP アドレス > < サブネット マスク >
b. **lwapp ap ip default-gateway** <IP アドレス >
c. **lwapp ap hostname** <AP のホスト名 >（オプション）
d. **lwapp ap controller ip address** <IP アドレス >

（注） DHCP が使用され（WLC IP が静的に設定された DHCP（P. 7-20）を参照）、WLC 管理 IP アドレスを定義するために DHCP オプション 43 または DNS 方式を使用しない場合は、ステップ 4 で **lwapp ap controller ip address** <IP アドレス > コマンドのみを入力します。

前述のコマンドは、直接 NVRAM に保存されます。

ステップ 5　静的な設定を確認するには、次のコマンドを入力します。

show lwapp ip config

次のような出力が表示されます。

```
AP0014.1ced.494e# sho lwapp ip config
LWAPP Static IP Configuration
IP Address          10.20.104.50
IP netmask          255.255.255.0
Default Gateway     10.20.104.1
Primary Controller 10.20.30.41

AP0014.1ced.494e#
```

エラーが発生した場合は、ステップ 4 のコマンドを繰り返して修正します。

ステップ 6　1 つ以上の静的なエントリをクリアするには、次のコマンドを使用します。

a. **clear lwapp ap ip address**
b. **clear lwapp ap ip default-gateway**
c. **clear lwapp ap controller ip address**
d. **clear lwapp ap hostname**

ブランチ ネットワークに接続されると、AP がブートしてディスカバリ要求をステップ 4 d. で定義した各 WLC に送信します。その後で、AP は、最も使用頻度の低い WLC に接続します。

（注） 何らかの理由で、設定する AP が以前に WLC と接続（アソシエート）したことがある場合、上記のコマンドは拒否され、「ERROR!!! Command is disabled.」というエラーが表示されます。AP が WLC に接続すると、上記のコマンドは使用できなくなります。セキュリティ上の理由からこのような設計になっています。以前に接続した LAP で静的 IP パラメータの設定が必要な場合、これらのパラメータを WLC の GUI またはコマンドライン インターフェイスから確立する必要があります。

WLC IP が静的に設定された DHCP

この方式は、DHCP を使用して、IP アドレスとデフォルト ゲートウェイで AP を動的に設定します。DHCP サービスは、外部サーバを使用してローカルにまたはリモートで、または IOS 内部に常駐している DHCP サービスを使用してローカルに、実装できます。WLC 管理インターフェイス IP アドレスは、AP コンソール インターフェイスを使用して手動で設定できます。この作業は、ブランチ オフィスまたはオンサイトに出荷する前に実行できます。シリアル コンソール ポート（P. 7-18）を参照してください。ブランチ ネットワークに接続されると、AP がブートしてディスカバリ要求を定義された各 WLC に送信します。その後で、AP は、最も使用頻度の低い WLC に接続します。

（注） 上記のオプションは、「初期状態で」初めて展開された新しい LAP に対してのみ実施できます。このオプションは、以前に WLC と接続 / 通信したことのある LAP に使用することはできません。

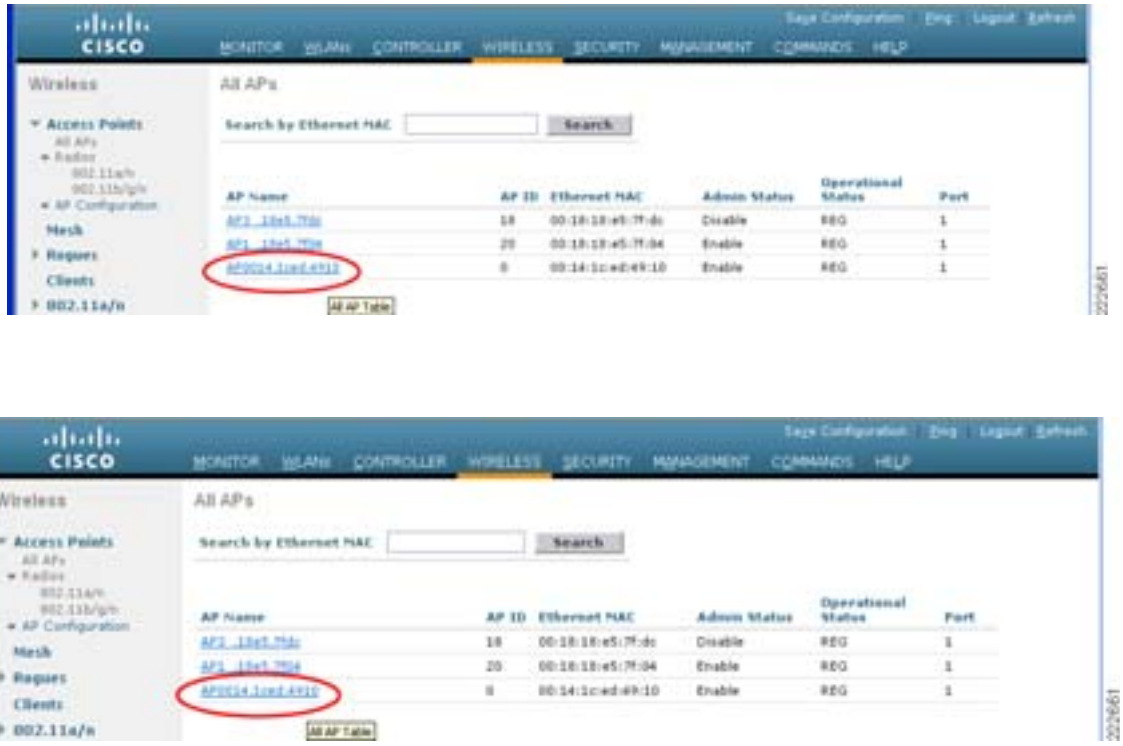
H-REAP の動作のための LAP の設定

次の設定作業は、WLC の GUI インターフェイスを使用して実施します。

H-REAP 対応 LAP が初めて WLC と接続する場合は、デフォルトでローカル AP モードに設定されます。LAP は、ローカル スイッチング パラメータを設定する前に H-REAP モードに設定する必要があります。

ステップ 1　WLC の Wireless 設定タブで、新しく接続する LAP を特定して、AP Name 列にある該当する LAP 名をクリックします（図 7-10 を参照）。

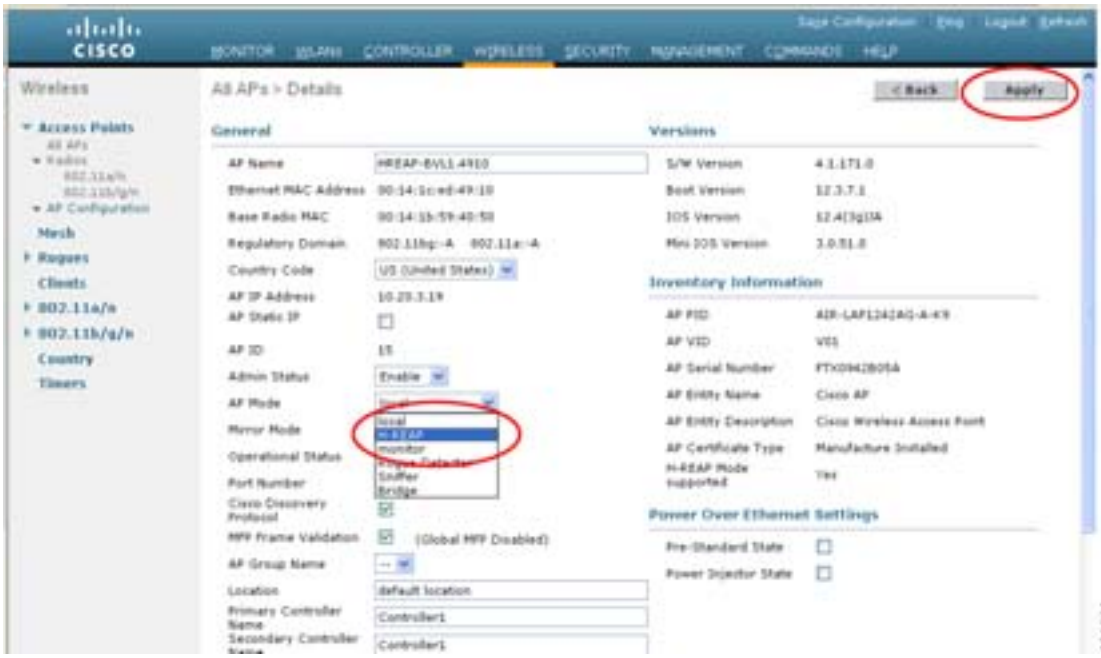
図 7-10　Wireless 設定タブ



ステップ 2　AP モード を定義します。

AP モードのドロップダウン リストから、**H-REAP** を選択します（図 7-11 を参照）。

図 7-11　無線の設定：AP モード



ステップ 3　AP 名および必要に応じてロケーション名を設定します。

ステップ 4　AP を接続するプライマリ WLC を特定し、必要に応じて、プライマリ（またはセカンダリ）WLC が到達不可能になった場合のセカンダリ WLC とターシャリ WLC を特定します。

これらの名前は、大文字小文字が区別され、システム名に対応します。指定された WLC のすべてが使用できない場合、AP は自動ロード バランシングに基づいて、モビリティ グループに属する他の WLC の 1 つに接続します。

ステップ 5　**Apply** をクリックします。

AP がリブートして、H-REAP モードで WLC に再接続します。

（注）　H-REAP AP がリブートしても、そのインターフェイスはまだ 802.1q トランキング モードに設定されません。したがって、AP は VLAN タグを含まない DHCP 要求を発行するため、H-REAP AP にアドレスを割り当てるための DHCP スコープはネイティブ VLAN に設定する必要があります。

VLAN サポートの有効化

H-REAP AP が H-REAP モードで WLC に再接続された後は、次の手順に従ってください。

ステップ 1　WLC の Wireless 設定下にある AP を探して、AP 名をクリックします。

AP の詳細ウィンドウに新しい H-REAP 設定が表示されています（図 7-12 を参照）。

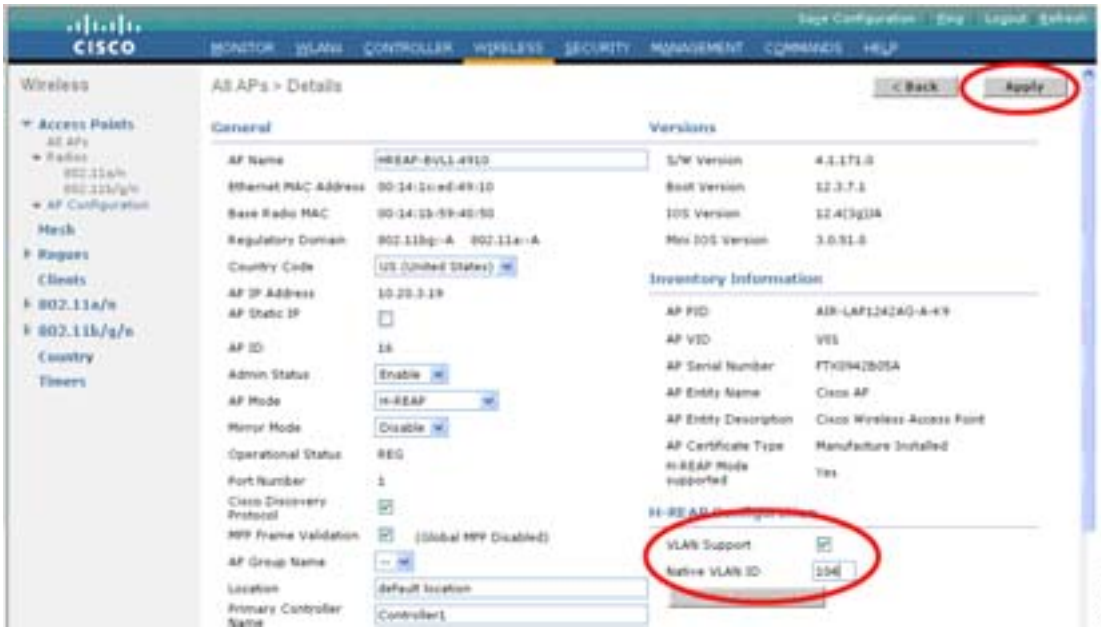
ステップ 2　**VLAN Support** チェックボックスをオンにします。

Native VLAN ID 定義ウィンドウと VLAN Mappings ボタンが追加されています。

ステップ 3　ネイティブ VLAN として定義された VLAN 番号を入力します。

ステップ 4　**Apply** をクリックします。

図 7-12　無線設定



高度な設定

次の手順は、ローカル スイッチングまたは中央スイッチングを実行するための H-REAP AP の設定方法を示しています。また、設定プロセスに関する注意点も含まれています。

ローカル スイッチングのための WLAN の選択

WLAN を H-REAP AP 上のローカル VLAN にマップする前に、まず、WLAN を H-REAP ローカル スイッチングに適合させる必要があります。

ステップ 1　WLC の Web GUI で、**WLANs** タブをクリックします。

ステップ 2　ローカルにスイッチする WLAN を探して、そのプロファイル名をクリックします（図 7-13 を参照）。

図 7-13　WLANs タブ

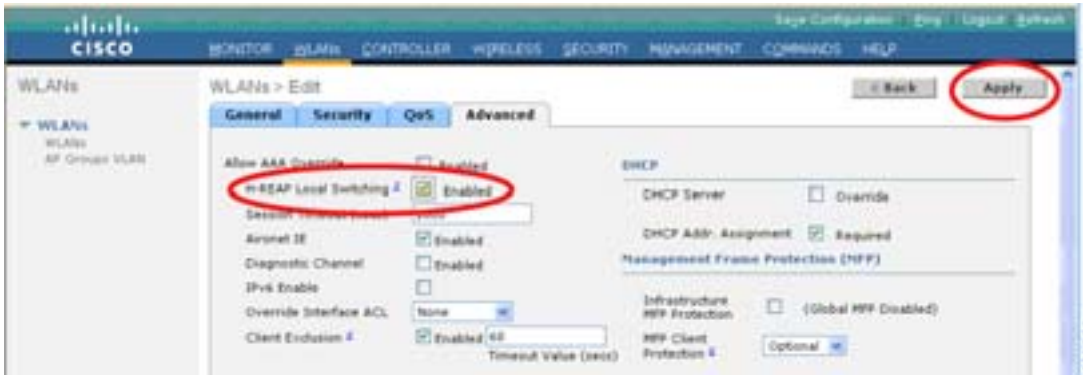
WLAN 上の H-REAP サポートの設定

ステップ 3　WLAN 編集ページで、**Advanced** タブをクリックします（図 7-14 を参照）。

図 7-14　WLANs：Edit

ステップ 4　Advanced 設定ウィンドウで、H-REAP Local Switching の横のチェックボックスをオンにします（図 7-15 を参照）。

図 7-15　H-REAP ローカル スイッチングの有効化



ステップ 5　**Apply** をクリックします。

H-REAP ローカル スイッチング（VLAN）の設定

WLAN が H-REAP をサポートするように設定したら、次の手順を実行します。

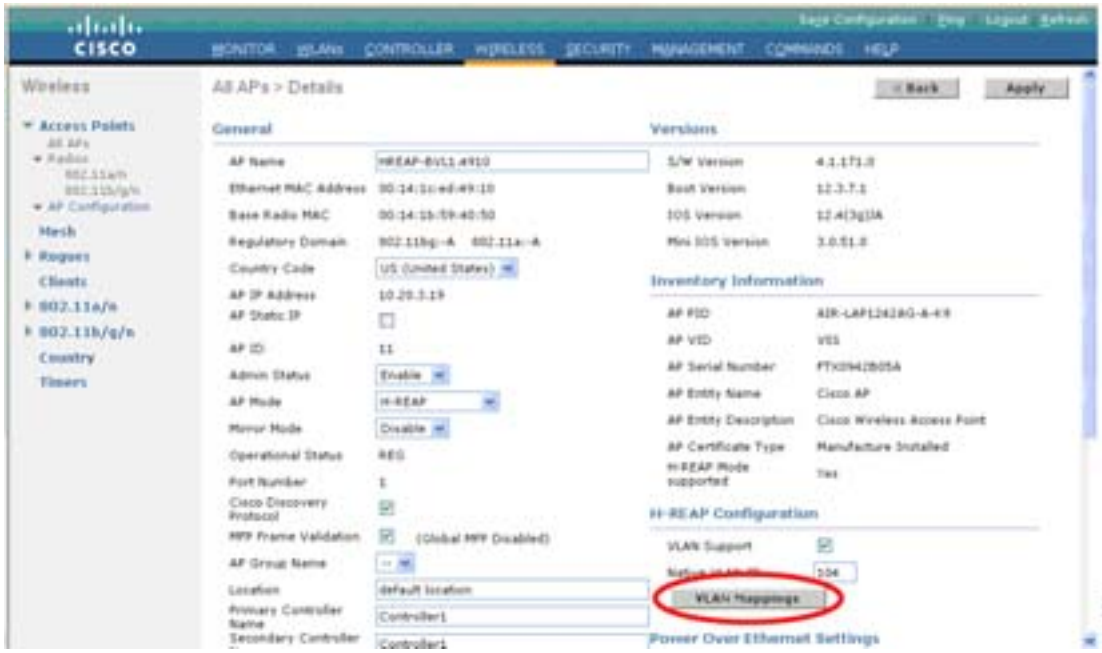
ステップ 1　**Wireless** タブをクリックします。

ステップ 2　AP のリストから、H-REAP を見つけて AP 名をクリックします（図 7-16 を参照）。

図 7-16　Wireless タブ：AP

ステップ 3　AP Details 設定ページで、**VLAN Mappings** をクリックします（図 7-17 を参照）。

図 7-17　All APs：Details



WLAN とローカル VLAN のマッピング設定

VLAN Mappings ページに、H-REAP ローカル スイッチング用に設定されたすべての WLAN と設定可能な VLAN ID フィールドが表示されます（図 7-18 を参照）。

図 7-18　VLAN マッピング

（注） 最初に表示される VLAN ID は、中央集中型 WLC の WLAN インターフェイス設定から継承されます。

ステップ 1　WLAN/SSID ごとに、ローカルに関連する VLAN ID を設定します。

複数の WLAN を同じローカル VLAN ID にマップできます。

ステップ 2　**Apply** をクリックします。

（注）　灰色のボックスで表示されたすべての WLAN は中央でスイッチされ、WLAN が WLC で管理目的のために有効になっているかどうかに応じてアクティブになる場合とならない場合があります。中央でスイッチされる WLAN に関連付けられたすべてのユーザ トラフィックは、トンネルを通過して WLC に戻されます。

中央スイッチング WLAN は、WLAN オーバーライド機能を使用して不要な WLAN を隠すことによって、H-REAP から除外できます。

（注）　ローカル スイッチング WLAN ごとに、アソシエートされている VLAN 用に構成された DHCP ヘルパー アドレスまたはローカル DHCP プールを設定する必要があります。

リモート専用 WLAN の WLC 動的インターフェイスの設定

上記のサンプル設定は、所定の WLAN をメイン キャンパスおよび 1 つ以上のリモート サイト ロケーションで使用することを想定しています。ただし、H-REAP ローカル スイッチングだけが使用されている 1 つ以上のリモート サイトで使用するためには、WLAN を排他的に定義する必要がある場合があります。

このシナリオでは、WLAN はメイン キャンパスで使用されなくても、ローカルの動的なインターフェイスにマップする必要のある WLC 上に作成されます。WLC のデフォルトの動作では、新しく作成された WLAN を管理インターフェイスにマップします。各サイトで（リモート）WLAN はローカルにスイッチされますが、WLC で WLAN を「ダミーの」インターフェイス /VLAN にマップするための対策を行う必要があります。WLAN を WLC 管理インターフェイスにマップしたままにしないでください。これにより、設定を間違えたために無線クライアント トラフィックが誤って管理サブネットにアクセスしないようにします。

この脆弱性を軽減する一番早い方法は、社内の他のネットワークとの DHCP サービスまたは論理接続が存在しない孤立した VLAN にマップする WLC 上で動的なインターフェイスを作成することです。この VLAN は、その他の対策として、NAC アプライアンスまたはファイアウォールとマップすることもできます。

H-REAP の確認

H-REAP AP のアドレスの確認

- DHCP を使用してアドレスを割り当てる場合は、DHCP サーバの構成設定、正しいサブネット、マスク、およびデフォルト ゲートウェイを確認します。
- AP DHCP スコープがネイティブ VLAN で定義されていることを確認します。
- AP が静的アドレスで構成された場合は、**show lwapp ip config** コマンドを使用して、AP アドレス、サブネット、マスク、およびゲートウェイが、ブランチ ロケーション内部で使用されているアドレス方式と矛盾しないことを確認します。詳細は、シリアル コンソール ポート（P. 7-18）を参照してください。

WLC の解決設定の確認

- WLC の解決に DHCP オプション 43 を使用している場合は、DHCP サーバ上の VCI と VSA の文字列形式が正しいことを確認します。
- 正しい WLC 管理 IP アドレスが DHCP サーバ上に設定されていることを確認します。
- DNS 解決を使用している場合は、CISCO-LWAPP-CONTROLLER@localdomain の DNS クエリーが、ブランチ ロケーションから作成できることと、1 つ以上の有効な WLC 管理 IP アドレスに解決されることを確認します。
- 有効な DNS サーバ アドレスが DHCP を介して割り当てられていることを確認します。
- WLC IP が手動で設定された場合は、**show lwapp ip config** コマンドを使用して、ネットワークから切断された AP のシリアル コンソール ポート経由の設定を確認します。詳細は、シリアル コンソール ポート（P. 7-18）を参照してください。

トラブルシューティング

この項では、いくつかの一般的な問題に関するトラブルシューティング ガイドラインについて説明します。

H-REAP が WLC に接続できない

H-REAP AP が目的の WLC に接続していない場合は、次の項目を確認してください。

- ブランチ ロケーションから中央集中型 WLC へのルーティングを確認します。AP サブネットから WLC 管理 IP アドレスが ping できることを確認します。
- LWAPP プロトコル（UDP ポートの 12222 と 12223 が ACL またはファイアウォールでブロックされていないことを確認します。
- H-REAP がモビリティ グループ内の他の WLC に接続していないことを確認します。

  モビリティ グループ内の WLC が、「マスター コントローラ」として指定されていないかどうか確認します。「マスター コントローラ」として指定されていると、H-REAP は目的の WLC 以外の WLC に接続する可能性があります。

ローカル スイッチング WLAN にアソシエートされたクライアントが IP アドレスを取得できない

- 802.1q トランキングが、AP が接続されているスイッチまたはルータのポート上で有効になっている（および AP の設定に適合している）ことを確認します。
- IP ヘルパー アドレスまたはローカル DHCP プールが、問題の WLAN の最初のレイヤ 3 ホップで VLAN （サブインターフェイス）用に設定されていることを確認します。

クライアントがローカル スイッチング WLAN を認証できない、またはローカル スイッチング WLAN にアソシエートできない

ローカル スイッチング WLAN が中央認証を使用する場合：

- H-REAP がスタンドアロン モード（WAN バックホール ダウン）になっていないことを確認します。
- 有効な RADIUS 認証サーバが WLAN 用に構成されていることを確認します。
- WLC から RADIUS 認証サーバにアクセスできることを確認します。
- RADIUS サーバが正常に動作していることを確認します。
- 認証サービスとユーザの資格情報が RADIUS サーバ上で設定されていることを確認します。

ローカル スイッチング WLAN が事前共有キーを使用する場合：

- クライアント上の WPA または WEP 設定が WLAN の設定と一致することを確認します。
- 無線クライアントが認証 / アソシエートするために、WLAN SSID をブロードキャストする（無効な場合）必要があるかどうか確認します。

クライアントが中央スイッチング WLAN を認証できない、または中央スイッチング WLAN にアソシエートできない

中央スイッチング WLAN が中央認証を使用する場合：

- H-REAP がスタンドアロン モード（WAN バックホール ダウン）になっていないことを確認します。
- 有効な RADIUS 認証サーバが WLAN 用に構成されていることを確認します。
- WLC から RADIUS 認証サーバにアクセスできることを確認します。
- RADIUS サーバが正常に動作していることを確認します。
- AAA 認証クライアントの場合は、認証サービスとユーザの資格情報が RADIUS サーバ上で設定されていることを確認します。

ローカル スイッチング WLAN が事前共有キーを使用する場合：

- クライアント上の WPA または WEP 設定が WLAN の設定と一致することを確認します。
- 無線クライアントが認証 / アソシエートするために、WLAN SSID をブロードキャストする（無効な場合）必要があるかどうか確認します。

H-REAP デバッグ コマンド

この項では、高度なトラブルシューティングで使用可能なデバッグ コマンドについて説明します。

WLC デバッグ コマンド

WLC のシリアル コンソール インターフェイスを使用して、次のコマンドを入力し、その出力を確認できます。

debug lwapp events enable

debug lwapp packets enable

H-REAP AP デバッグ コマンド

H-REAP のシリアル コンソール インターフェイスを使用して、次のコマンドを入力し、その出力を確認できます。

debug lwapp client packet

debug lwapp client mgmt

debug lwapp client config

debug lwapp client event

debug lwapp reap load

debug lwapp reap mgmt

CHAPTER 8

Cisco メッシュ型無線ネットワーキング

この章では、屋外環境で Cisco メッシュ型無線ネットワークを展開するための設計の詳細について説明します。主にメッシュ型の展開に関する設計上の考慮事項について説明しますが、ソリューション コンポーネントと相互作用についても説明します。Cisco メッシュ型無線ソリューションの詳細は、『Cisco Aironet 1500 Series Wireless Mesh AP Version 5.0 Design Guide』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/technology/mesh/design/guide/MeshAP.html

はじめに

Cisco メッシュ型無線ソリューションを展開することで、コスト効率の優れた安全な屋外向け Wi-Fi ネットワークを実現できます。屋外無線アクセスにより、普及しつつある費用のかからない Wi-Fi クライアントを活用して、ユーザの生産性と応答性を向上する新しいサービスやアプリケーションを使用できるようになります。

屋外無線アクセスの需要が増大していることから、厳しい予算とリソースの減少という問題に直面したお客様は、既存のツール、知識、およびネットワーク リソースを最大限に活用する無線 LAN（WLAN）ソリューションによって、コスト効率の優れた方法で展開を簡素化し、WLAN セキュリティの問題に対応する必要があります。Cisco メッシュ型無線ソリューションは、メッシュ型無線テクノロジー固有の優れた特性を備え、現在のネットワーク要件を効率的にサポートし、ビジネス アプリケーションの統合の基盤を築く屋外 WLAN ソリューションです。

屋外無線ソリューションは、標準の屋内 WLAN と比較して、特に次のような面でいくつかの課題があります。

- 環境
- カバレッジ
- 総所有コスト（TCO）
- 物理的なデバイス セキュリティ

屋外環境は屋内環境よりも厳しく、屋外に展開する屋内装置を収納して保護するには、特殊な装置またはエンクロージャを必要とします。

展開時には、屋内無線ネットワークよりも広い領域をカバーするよう試みます（それで、完璧というわけではありません）。屋外での展開の課題としては、干渉の原因を制御しにくいことがあり、適切な有線接続を探して、メッシュ型無線ネットワークを有線ネットワークに接続し、メッシュ型ネットワーク デバイスで電力を利用できるようにします。

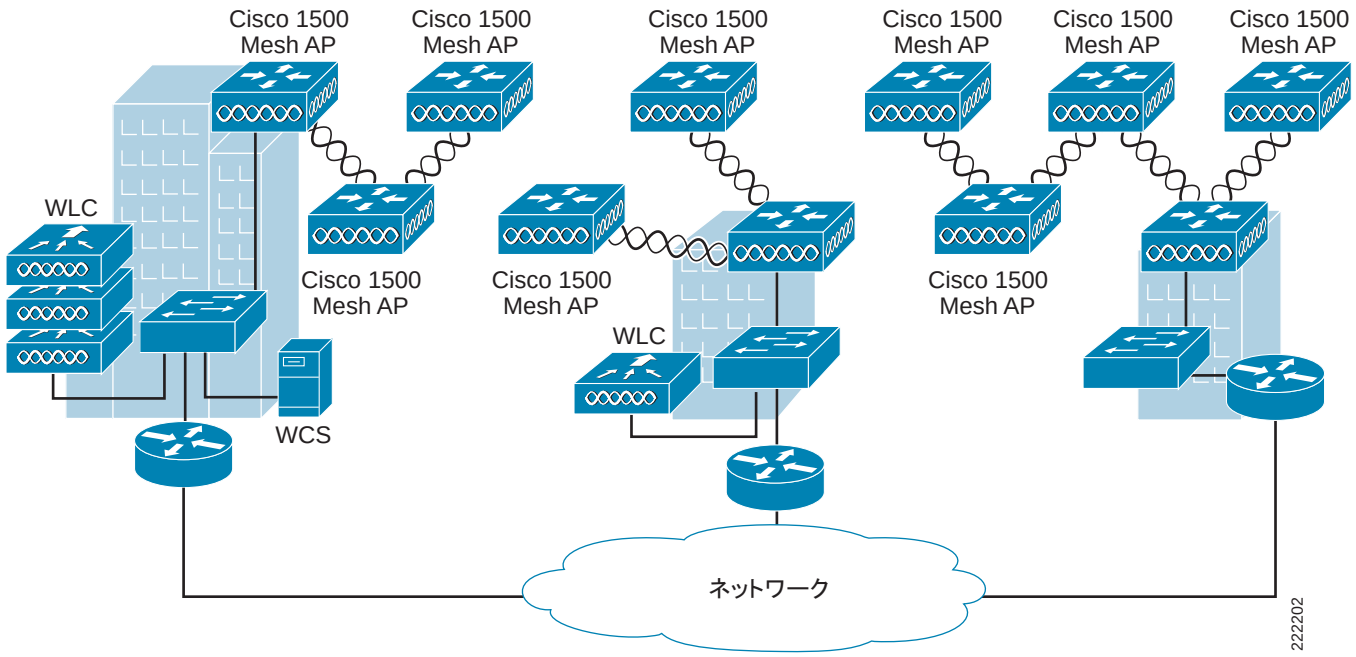
また、屋外展開では、特殊な無線周波（RF）に関するスキルが必要であり、屋内展開よりもユーザ密度が低く、ビルディング内よりも規制が少ない環境に展開される可能性があります。これらの特性は、屋外ソリューションの TCO を圧迫するため、展開や管理が簡単なソリューションが必要となります。

Cisco メッシュ型無線ソリューションには、3 つの主なコンポーネントがあります。

- Cisco 1500 シリーズ Mesh AP：メッシュおよびバックホール クライアント接続に WLAN クライアント アクセスを提供する屋外アクセス ポイント
- Cisco Wireless LAN Controller（WLC）：AP 制御機能に中央ポイントを提供
- Cisco Wireless Control System（WCS）：大規模な実装においてスケーラビリティ、管理容易性、および可視性を向上する管理プラットフォーム

図 8-1 は、メッシュ AP、WLC、および WCS で構成された簡単なメッシュ ネットワーク展開を示しています。この展開例では、有線ネットワークに接続された 3 つのメッシュ AP があります。これらの AP は、ルーフトップ AP（RAP）として指定されています。メッシュ ネットワーク内のその他の AP はすべて単なるメッシュ AP（MAP）です。MAP および RAP のいずれのメッシュ AP もすべて、WLAN クライアント アクセスを提供できますが、多くの場合、RAP は、設置される場所がら、クライアント アクセスの提供に適していません。次の例では、RAP は、各ビルディングのルーフ上に配置され、それぞれの場所でネットワークに接続されています。一部のビルディングでは、メッシュ AP からの LWAPP セッションを終端するための WLC が配置されていますが、すべてのビルディングで WLC が必要なわけではありません。LWAPP セッションは、必要に応じて、WAN 上の WLC が配置されている別の場所にバック ホールできます。

図 8-1　メッシュ ソリューション図



Cisco 1500 シリーズ Mesh AP

図 8-2 に示されている Cisco 1500 シリーズ Mesh AP は、メッシュ型無線ソリューションのコア コンポーネントであり、無線 LAN コントローラと WCS の既存の機能と新規の機能を活用します。

図 8-2　Cisco 1510 および 1520 メッシュ型無線 AP

Cisco 1500 シリーズ Mesh AP には、3 つのタイプがあります。

- AP1520：同時に動作する次の 2 つの無線で構成される屋外アクセス ポイント
  - クライアント アクセスに使用する 2.4 GHz 無線
  - 別の 1500 シリーズ Mesh AP へのデータ バックホールに使用する 5.8/4.9 GHz 無線
- AP1520 は、モジュール設計にもなっており、次のオプションのアップリンク インターフェイスを設定できます。
  - ケーブル電源付きケーブル モデム DOCSIS 2.0
  - 100BaseBX SFP 付きファイバー インターフェイス
  - 1000BaseT ギガビット イーサネット
- AP1510：同時に動作する次の 2 つの無線で構成される屋外アクセス ポイント
  - クライアント アクセスに使用する 2.4 GHz 無線
  - 別の 1500 シリーズ Mesh AP へのデータ バックホールに使用する 5.8/4.9 GHz 無線

  また、AP1510 には、WLC への接続、または接続されているブリッジ用 LAN セグメントに使用できる、イーサネット ポートがあります。
- AP1505：次の 1 つの 2.4 GHz 無線で構成される屋外アクセス ポイント
  - クライアント アクセスとバックホールに使用される 2.4 GHz 無線
  - AP1510 と同様に、AP1505 にも有線イーサネット ポートがあります。

1500 シリーズ Mesh AP をさまざまな地形に展開するときに、さまざまなアンテナを使用して柔軟性が提供されます。802.11j で規定される 4.9GHz 周波数無線は、802.11a 相当のテクノロジーが使用されており、バックホール無線またはリレー無線としてシステムで使用されます。2.4 GHz 無線経由で AP に到達した無線 LAN クライアントのトラフィックは、AP バックホール無線を通じて渡されるか、WLC イーサネット接続に到達するまで他の 1500 シリーズ Mesh AP を通じてリレーされます。

1500 シリーズ Mesh AP には、ブリッジ機能を提供する 10/100 イーサネット接続も備わっています。このイーサネット接続は、個別の電力供給システムを通じて Power over Ethernet（PoE）をサポートします。

(注)　パワー インジェクタはこの製品に固有のものであり、シスコのその他の電力供給ソリューションは Cisco 1500 シリーズ Mesh AP には適していません。

Cisco 1500 シリーズ Mesh AP は、LWAPP を使用して、無線メッシュ内の無線コントローラや他の 1500 シリーズ Mesh AP と通信します。

1500 シリーズ Mesh AP は、図 8-3 に示すように、アンテナを垂直にして下向きに取り付けるように設計されています。

図 8-3　1500 シリーズ Mesh AP の設置

Cisco Wireless LAN Controller

メッシュ型無線ソリューションは、Cisco 4400 シリーズ Wireless LAN Controller（WLC）（図 8-4）、および Cisco Wireless Services Module（WiSM）（図 8-5）でサポートされます。いずれのプラットフォームも、多数のアクセス ポイントに対応できるように拡張可能であり、レイヤ 2 およびレイヤ 3 LWAPP 接続の両方をサポートできるため、メッシュ型無線の展開用に推奨されます。

図 8-4　Cisco 4400 Wireless LAN Controller

図 8-5　Cisco Wireless Services Module

Cisco Wireless LAN Controller の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/wireless/products_category_buyers_guide.html?linkpos=3#number_3

Wireless Control System（WCS）

Cisco Wireless Control System（WCS）は、メッシュ型無線の計画、設定、および管理用のプラットフォームです。ネットワーク マネージャがメッシュ型無線ネットワークを中央から設計、制御、および監視できるようにするためのツールを提供します。

Cisco WCS を使用すると、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 WLAN システムの管理のためのソリューションが提供されます。グラフィック インターフェイスにより、無線 LAN を簡単かつコスト効率の優れた方法で展開し、運用できるようになります。Cisco WCS は、詳細な傾向レポートや分析レポートの機能を備えており、ネットワークを継続的に運用するためには欠かせません。

メッシュ型無線の運用

メッシュ型無線の展開では、複数の 1500 Mesh AP が同一のネットワークの一部として展開されます。Mesh AP は、メッシュを形成するために親、子、および近隣の関係を相互に形成し、規定のプライマリ WLC まで戻る LWAPP トンネルを確立します。親、子、および近隣の関係の詳細は、メッシュの近隣、親および子（P. 8-10）を参照してください。

MAP では、Adaptive Wireless Path Protocol（AWPP）を使用し、他の 1500 Mesh AP を経由して WLC に到達する最良のパスを決定します。MAP と RAP 間の無線リンクがメッシュ型無線を形成します。これを使用して、トラフィックが WLAN クライアントから（LWAPP トンネル経由で）WLC に伝送され、ブリッジ トラフィックが MAP イーサネット ポートに接続されたデバイス間で伝送されます。

メッシュ型無線では、次の 2 つの異なるトラフィック タイプを同時に伝送できます。

- LWAPP トンネル経由の WLAN クライアント トラフィック
- MAP ブリッジ トラフィック

WLAN クライアント トラフィックは WLC 上で終端し、ブリッジ トラフィックはメッシュ型無線の MAP のイーサネット ポート上で終端します。

メッシュ型無線の MAP のメンバーシップは、次のようなさまざまな方法で制御できます。デフォルトの AP 認証は EAP ですが、事前共有キー（PSK）を使用した認証も設定できます。メッシュ メンバーシップを制御したり、メッシュ型無線をセグメント化したりするために、認証に加えてブリッジ グループ名（BGN）が使用されます。

ブリッジの認証

メッシュ AP は、有効になっていて、有線イーサネット接続経由でネットワークに接続されている場合、次の手順で WLC に接続します。

1. AP がブートすると、静的 IP が事前に設定されていない場合は、必要に応じて DHCP サーバ経由で IP アドレスを取得します。
2. メッシュ AP は、LWAPP ディスカバリ要求を送信します。
3. WLC は、要求を受信すると、ディスカバリ応答で応えます。
4. この時点で、メッシュ AP は LWAPP join リクエストを発行します。
5. WLC は、LWAPP join レスポンスを発行し、EAP 認証を進めます。
6. メッシュ AP は、現在のイメージ バージョンに基づき、新しいイメージをダウンロードしてリブートする場合があります。
7. リブート後、メッシュ AP は再び WLC への接続と再認証を要求します。

（注）　PSK は、WLC 上で設定されている場合、EAP の代わりに使用できます。

メッシュ AP が WLC への接続に使用する有線接続が存在しない場合は、メッシュ AP は次の手順でコントローラに接続します。

1. ブート後、メッシュ AP は 802.11 アソシエーションを形成し、その 802.11a 接続経由で LWAPP ディスカバリ要求を発行します。
2. WLC に接続されたメッシュ AP が検出されると、そのメッシュ AP は、IP アドレスが静的に設定されていなければ DHCP サーバを使用して IP アドレスを取得します。
3. この時点で、メッシュ AP は LWAPP 接続要求を発行します。

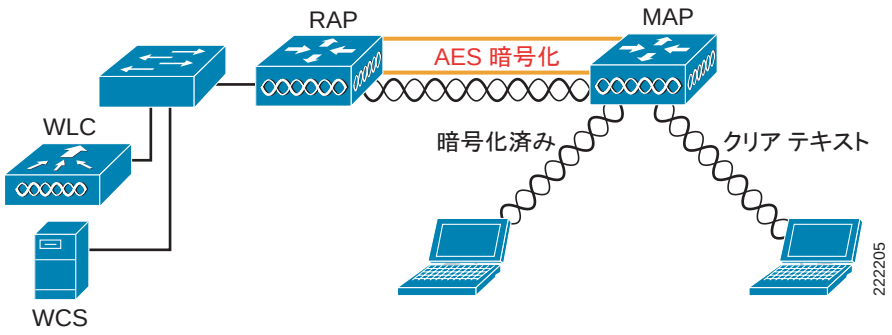
4. WLC は、LWAPP 接続応答を発行し、EAP 認証を進めます。
5. メッシュ AP は、現在のイメージ バージョンに基づき、新しいイメージをダウンロードしてリブートする場合があります。
6. リブート後、メッシュ AP はその親を再び検出し、コントローラへの再接続と再認証を再び要求します。

メッシュ型無線の暗号化

前に説明したように、メッシュ型無線は、MAP と RAP の間のトラフィックをブリッジします。このトラフィックは、メッシュ型無線によりブリッジされた有線デバイスからのトラフィック、またはメッシュ AP からの LWAPP トラフィックである可能性があります。このトラフィックは、メッシュ型無線リンクを経由するときに、常に AES で暗号化されます（図 8-6 を参照）。

AES 暗号化は、メッシュ AP が他のメッシュ AP との近隣関係を確立する過程で確立されます。メッシュ AP 間で使用される暗号キーは、EAP 認証プロセスで自動的に生成されます。

図 8-6　メッシュの暗号化



AWPP メッシュ型無線ルーティング

Cisco メッシュ型無線ネットワークの中核を成すのは、Cisco Adaptive Wireless Path Protocol（AWPP）です。

このプロトコルは、特にメッシュ型無線ネットワーキング用に設計されており、そのパスはリンクの品質とメッシュ AP のホップ数に基づいて決定されます。また、AWPP は、容易な展開、高速コンバージェンス、および最低限のリソース消費を実現するように設計されています。

AWPP の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_press_coverage0900aecd804ab5f6.pdf

簡易メッシュの展開例

図 8-7 に示す簡易メッシュ展開の設計における主要なネットワーク コンポーネントは、次のとおりです。

- WCS：メッシュ ネットワークの管理、運用、および最適化における主要コンポーネント。

- Wireless LAN Controller：Lightweight アクセス ポイントと他の無線 LAN コントローラとの間のリアルタイム通信を可能にし、中央集中型のセキュリティ ポリシー、無線 Intrusion Prevention System（IPS; 侵入防御システム）機能、RF 管理、QoS（Quality of Service）、およびモビリティを実現します。
- ネットワークとメッシュの間のルータ：セキュリティやポリシーを適用して施行することのできるレイヤ 3 境界を提供します。このルータは、RAP のレイヤ 2 切り離しも行います。この切り離しが必要なのは、RAP がトラフィックをローカル イーサネット ポートからメッシュにブリッジするので、不要なトラフィック フラッディングによってリソースが消費されないように、このトラフィックを制限してソリューションをサポートする必要があるからです。
- RAP：有線ネットワークに接続されたメッシュ AP。メッシュ型無線 AP のパス ホームとなります。
- 複数の MAP。

（注） RAP 無線は、MAP メッシュの中心に向かって接続されています。これは、メッシュの平均ホップ数を最小にする最適な構成です。RAP をメッシュの端に向かって接続すると、ホップ数が増加します。

図 8-7　簡易メッシュの展開

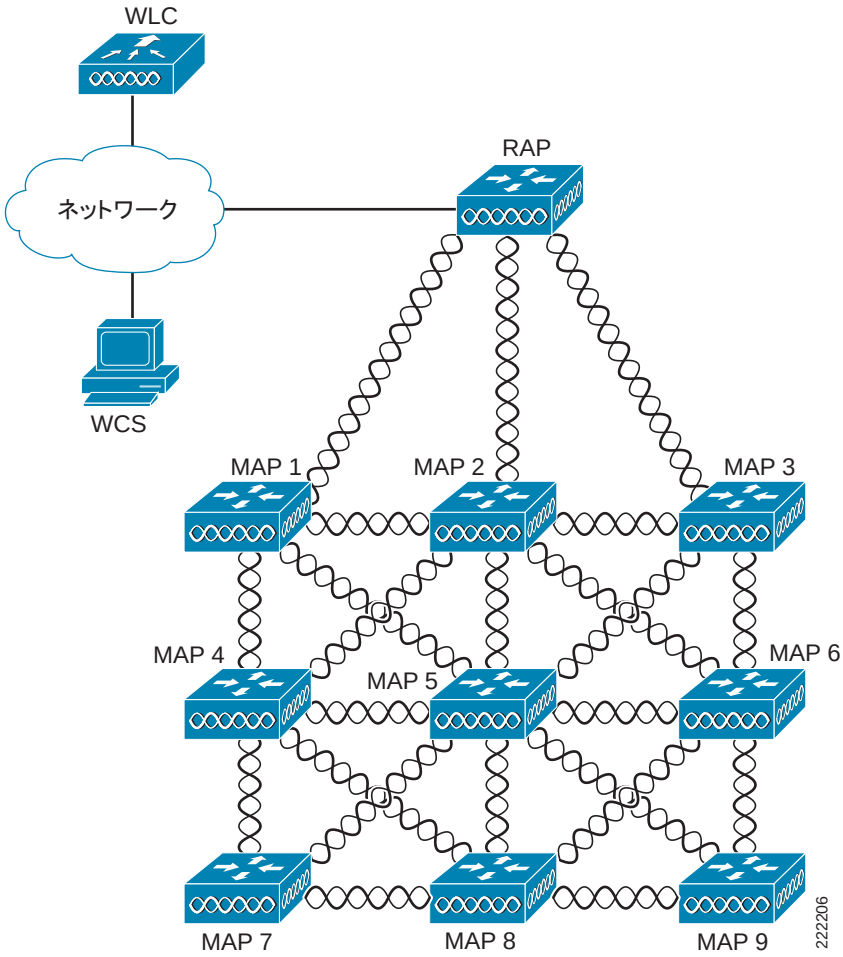


図 8-8 は、物理的構成に対して考えられる論理図の 1 つの例を示しています。この例では、MAP5 が他のすべての MAP のパス ホームとして構成されています。

図 8-8　論理メッシュ図

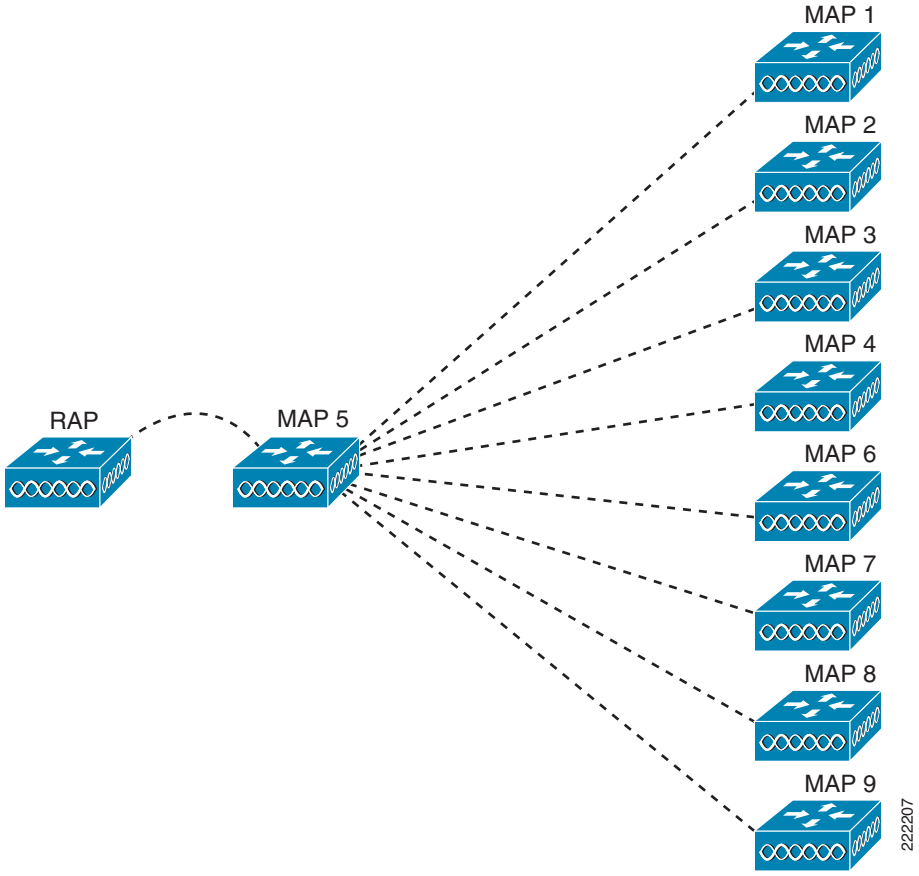
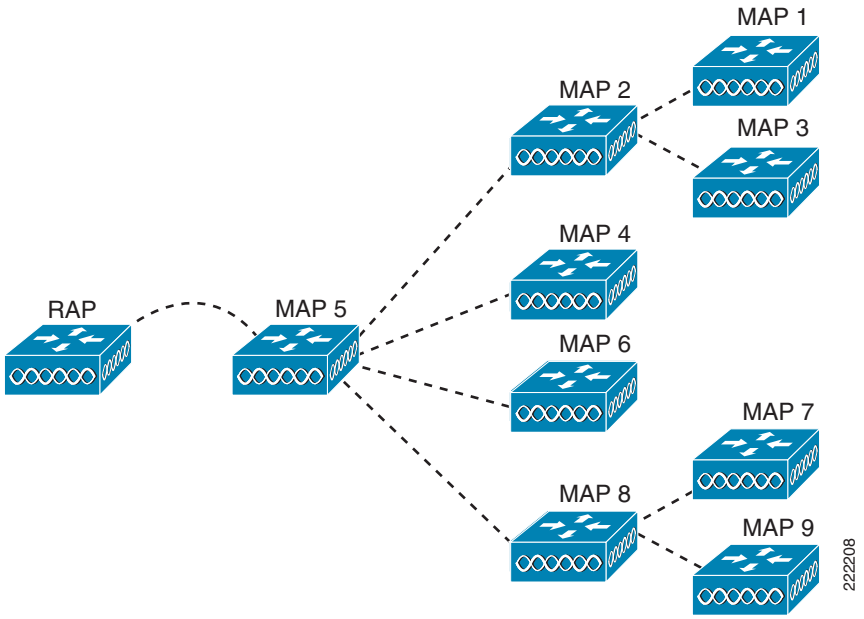


図 8-9 は、別の論理図を示しています。ここでは、MAP5 への間接パス上の Signal-to-Noise Ratio（SNR; 信号対雑音比）が小さいので、他の MAP に対して、SNR がより大きいリンクに沿って MAP5 へ到達するホップを追加することを検討できます。

図 8-9　同等でないメッシュ パス



上記のどちらの場合も、MAP5 はすべてのトラフィックのパス ホームとなっています。理想的には、RAP からのカバレッジは、他の MAP（たとえば MAP2）が RAP まで戻るパスを持つようにするほか、MAP5 への信号が損失した場合にトラフィックを MAP2 経由にできるようにします。

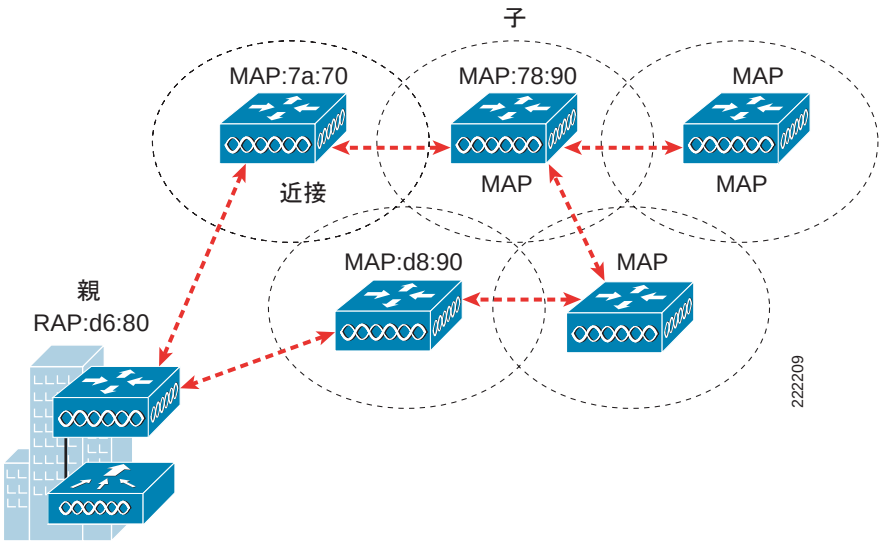
メッシュの近隣、親および子

メッシュ AP と別のメッシュ AP との間には、次の 3 とおりの関係があります。

- メッシュ内の*近隣* AP とは、RF 範囲内にあるものの、その「緩和」値が別の近隣 AP より小さいため、親または子として選択されていない AP のことです（緩和値の計算（P. 8-14）を参照）。
- *親* AP とは、最適な緩和値に基づいて RAP まで戻る最適ルートとして選択された AP のことです。親は RAP そのもの、または別の MAP のいずれかです。
- *子* AP とは、親 AP を RAP まで戻る最適ルートとして選択した AP です。図 8-10 の例は、小さいメッシュを示しています。この例では、MAP:7a:70 の親は、RAP:d680 です。MAP:7a:70 の子は、MAP:78:90 です。また、Map:7a:70 は、MAP:d8:90 と近隣関係を持っています。

（注） メッシュ AP は、他のメッシュ AP の親であったり、子であったりしますが、RAP はいずれの AP の子でもない唯一のメッシュ AP です。

図 8-10　親、子、および近隣

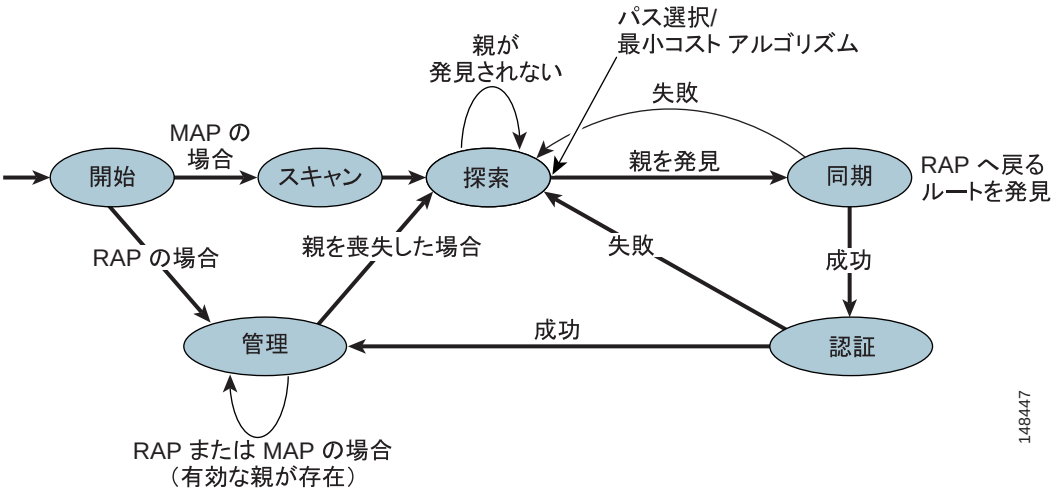


AWPP の目的は、RAP まで戻るメッシュを経由した、MAP の最適なバックホール リンク パスを見つけることです。そのために、メッシュ AP は、近隣 AP に対して活発に要請メッセージを送信します。要請メッセージの送信中に、メッシュ AP は、RAP まで戻る間にある使用可能な近隣メッシュ AP をすべて調べ、どの近隣メッシュ AP を使用した場合に最良のパスとなるかを判断し、その近隣メッシュ AP と同期化します。

図 8-11 は、メッシュ AP が接続を確立する際のメッシュ AP の状態図を示しています。

まず、メッシュ AP は、そのメッシュ AP が RAP であるかどうかを判断する必要があります。メッシュ AP は、イーサネット インターフェイス経由で WLC と通信できる場合は、RAP になります。メッシュ AP は、RAP である場合、直ちに管理状態になります。管理状態の場合、メッシュ AP は、コントローラへの LWAPP 接続を確立しているので、他のメッシュ AP を探索する必要はありませんが、要請メッセージには応答する必要があります。メッシュ AP は、RAP でない場合、スキャン プロセスを開始します。このとき、メッシュ AP は使用可能なすべてのチャネルをスキャンし、他のメッシュ AP からの情報を要請します。

図 8-11　メッシュ AP の状態図



この場合、主に次の 2 つのことが暗黙的に実行されます。

- RAP はチャネルを変更しないため、RAP からメッシュを構築するために使用されるチャネルは RAP の設定内で定義されます。デフォルトでは、RAP はチャネル 161 を使用します。
- もともと RAP のみが要請メッセージに応答できるため、メッシュは RAP から構築されます。

メッシュ AP は、RAP でない場合、次のモードで上記の状態図に従って動作します。

- スキャン：AP は、メッシュ ビーコンを使用してすべてのバックホール チャネルをスキャンします。このメカニズムは、無線アクセス ネットワークで使用する 802.11 ビーコン メカニズムと似ています。ビーコンに使用するフレームは、NEIGHBOR_UPDATE と呼ばれます。基本的には、NEIGHBOR_UPDATE フレームはネットワークによってアドバタイズされるので、新しいノードはスキャンを実行して迅速に近隣 AP を検出できます。ネットワーク（WLAN コントローラ経由で）に接続後、それぞれの RAP と MAP は NEIGHBOR_UPDATE フレームをブロードキャストします。10dB 未満の SNR で更新された近隣 AP は、すべて破棄されます。このプロセスをパッシブ スキャンといいます。
- 探索：メッシュの他のメンバに要請メッセージを送信します。これらの要請メッセージに対して正しい応答を発行するメッシュ AP が、近隣 AP になります。
- 同期：メッシュ AP は、その近隣 AP のそれぞれからパス情報を取得し、緩和値がより大きな近隣 AP が、要請メッセージを送信しているメッシュ AP の親になります。近隣 AP が複数の RAP にレポートを送信する場合、緩和値の最も大きな RAP が選択されます。
- 認証：メッシュ AP は、その親 AP 経由で確立した接続を通じて WLC の認証を受けます。これが、標準の証明書に基づく LWAPP AP 認証です。
- 管理：メッシュ AP は、他のメッシュ AP の要請メッセージに応答し、定期的に要請メッセージを発行してメッシュ内の変更を確認します。メッシュ AP が WLC や WCS で認識されるのは、管理状態になってから後のことです。探索モードのメッシュ AP は、すべてのチャネル上で要請メッセージを送信可能であり、親 AP によって検出された場合にのみメッセージの送信を停止します。しかし、管理状態では、メッシュ RAP によって定義されたチャネル上でのみ要請メッセージが送信されます。

メッシュ ネットワーク内のバックグラウンド スキャン

Cisco 1500 シリーズ AP では、バックグラウンド スキャンを使用することで、近隣チャネルの最適パスと親を積極的かつ継続的に監視できます。アクセス ポイントは、現在のチャネル上だけではなく近隣チャネル上も探索しているので、潜在的な代替の最適パスと親のリストは大きくなります。

親が損失する前にこの情報を特定し、より高速な切り替えとアクセス ポイントに対する最適なリンクの発見が可能になります。さらに、新しいチャネル上のリンクが、現在のチャネルよりコスト距離が優れている（ホップが少なく、SNR が強力）ことが判明した場合は、アクセス ポイントを新しいチャネルに切り替えることができます。

他のチャネル上でのバックグラウンド スキャン、およびそれらのチャネル上の近隣 AP からのデータ収集は、2 つのアクセス ポイント間のバックホール上で実行されます。

- 1510 アクセス ポイントでは、バックホール（プライマリ）は 802.11a リンク上で動作します。
- 1505 アクセス ポイントでは、バックホールは 802.11b/g リンク上で動作します。

バックグラウンド スキャンは、コマンドライン インターフェイスを使用して、コントローラ上でグローバルに有効にできます。

config mesh background-scanning {enable | disable}

バックグラウンド スキャンが有効であることを確認するには、次のコマンドを入力します。

show mesh background-scanning

バックグラウンド スキャンは、デフォルトで有効になります。

(注)　音声コールが新しいチャネルに切り替わると、遅延が増加することがあります。

Dynamic Frequency Selection（DFS; 動的周波数選択）を必要とするチャネルを使用している場合は、他のチャネルで近隣 AP を検索すると時間がかかることがあります。

バックグラウンド スキャンの動作についてよく理解できるようにするため、以下にいくつかのシナリオを紹介します。図 8-12 では、メッシュ アクセス ポイント MAP1 が、最初に起動したときに、ルート アクセス ポイント RAP1 と RAP2 の両方を親の候補として認識します。RAP2 経由のルートの方がコスト距離がより短いため、MAP1 の親として RAP2 が選択されます。

リンクが確立されると、バックグラウンド スキャンでは、より適切なパスと親を探して、すべてのチャネルが継続的に監視されます。RAP2 は、引き続き MAP1 の親として動作し、リンクが切れるか、別のチャネル上でより適切なパスが見つかるまで、チャネル 2 上で通信を行います。

図 8-12　メッシュ アクセス ポイント MAP1 による親の選択

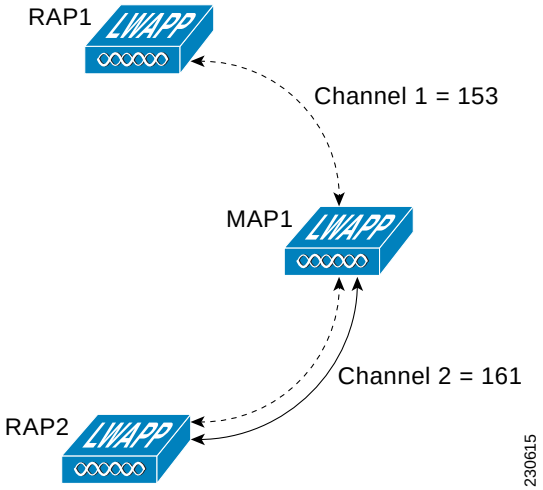
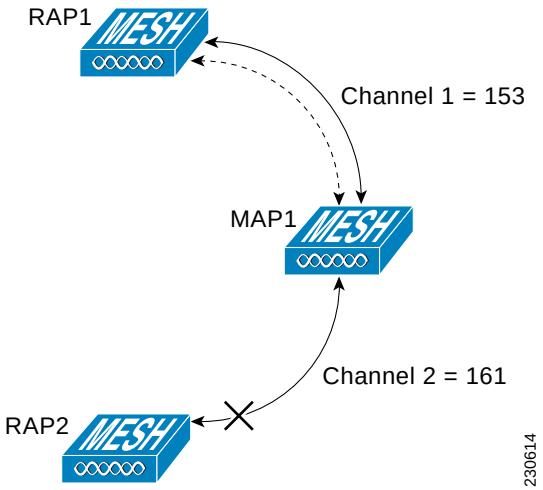


図 8-13 では、MAP1 と RAP2 の間のリンクが失われています。実行中のバックグラウンド スキャンのデータから、RAP1 とチャネル 1 が、MAP1 に対する次に適した親および通信パスとして特定されたため、RAP2 へのリンクが切断された後、追加スキャンを必要せずに、そのリンクが直ちに確立されます。

図 8-13　バックグラウンド スキャンによる新しい親の特定



コントローラ上でバックグラウンド スキャ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 background-scanning {enable | disable}

バックグラウンド スキャンが有効であることを確認するには、次のコマンドを入力します。

show mesh background-scanning

緩和値の計算

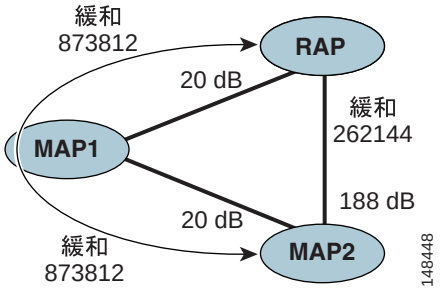
緩和値を算出するには、各近隣 AP の SNR およびホップ値を使用し、さまざまな SNR しきい値に基づいた乗数を適用します。この乗数を使用する目的は、拡散関数をさまざまなリンクの質を反映した SNR に適用することです。

親 AP は、調整された緩和値を使用して選択されます。調整された緩和値とは、各近隣の緩和値を RAP へのホップ数で割った値のことです。

調整された緩和値 = 各ホップの最小緩和値 / ホップ数

図 8-14 では、MAP2 で MAP1 経由のパスが優先されます。なぜならば、このパスを経由して調整された緩和値（436906）は、MAP2 から RAP への直接パスの緩和値（262144）よりも大きいからです。

図 8-14　親パスの選択



SNR スムージング

WLAN のルーティングにおける課題の 1 つは、RF に持続性がないということです。適切なパスを判断し、パスの変更が必要になる時期を決定するときには、この点を考慮する必要があります。特定の RF リンク上の SNR は、実質的には時間の経過と共に変化します。これらの変動に基づいてルート パスを変更すると、ネットワークがパフォーマンスの非常に低い不安定な状態になります。時間の経過による変動を排除して基本となる SNR 値を効率的に取得するには、スムージング機能を適用します。これにより、調整された SNR が提供されます。

現在の親に対する近隣候補の評価では、親間のフラッピングを削減するために、親には、その親の算出された緩和値に加えて、20% の「ボーナス緩和値」が与えられます。ボーナス緩和値が割り当てられた親の候補は、RAP への最適なルートを提供し、子がルートを切り替えられるようにする必要があります。親の切り替えは、LWAPP および他の上位レイヤの機能に対して透過的に実行されます。

ループ防止

ルーティング ループが作成されないようにするために、AWP では、ルート自体の MAC アドレスを含むすべてのルートが破棄されます。つまり、ホップ情報は別として、ルーティング情報には、各ホップから RAP への MAC アドレスが含まれています。これにより、1500 シリーズ Mesh AP では、ループするルートを容易に検出して破棄できます。

最適な親メッシュの選択

AWPP 状態マシンの探索状態において、OPS アルゴリズムが実装されます。AWPP（無線バックホールを持つ RAP と MAP の両方）における親選択アルゴリズムの基本的な手順は次のとおりです。

- 近隣 AP を持つチャネルのリストは、スキャン状態のパッシブ スキャンによって生成されます。このリストは、すべてのバックホール チャネルの一部分です。
- 近隣 AP が存在するチャネルは探索状態で活発的にスキャンされ、バックホール チャネルは最適な近隣緩和値を持つチャネルに変更されます。
- 親は最適な近隣 AP に設定され、親子間のハンドシェークは探索状態で完了します。
- 親の管理と最適化は、管理状態で行われます。

このアルゴリズムは起動時に実行され、親が見つからず、他の親候補が存在しないと、通常は LWAPP ネットワークとコントローラが探索されます。すべての近隣プロトコル フレームは、チャネル情報を持っています。以下で説明するように、親の管理技術と最適化技術は、どちらも変更されません。

- 親の管理は、子ノードが宛先の指定された NEIGHBOR_REQUEST を親に送信し、親が NEIGHBOR_RESPONSE で応答することによって実行されます。
- 親の最適化とリフレッシュは、子ノードがその親と同じチャネル上で NEIGHBOR_REQUEST ブロードキャストを送信し、このチャネル上の近隣ノードからの応答をすべて評価することによって実行されます。最も現実的なメッシュ ネットワークでは、チャネル バックホールを 1 つだけ設計します。
- 親 MAP とは、RAP まで戻る最良のパスを持つ MAP です。AWPP は、緩和値を使用して最良のパスを決定します。緩和値は、コストとは反対のものと見なすことができます。また、優先パスとは、より高い緩和値を持つパスのことです。

Routing Around an Interface

この機能はオプションであり、ユーザはコントローラの CLI を使用してのみこの機能を設定できます。この機能が有効な場合は、プライマリ バックホール（a 無線）上に過渡的干渉が存在すると、セカンダリ バックホール（b/g 無線）上でパケットが転送されます。

Routing Around an Interface（RAI）には、2 種類の動作モードがあります。

- **Config mesh secondary-backhaul enable**：すべての AP 上で RAI がグローバルに有効になります。RAI を適切に機能させるためには、ユーザは、最初のホップの先にあるすべての AP 上の "b/g" チャネルを、最初のホップの "b/g" 無線上で使用されているのと同じチャネルに設定する必要があります。RRM（自動 RF）が有効な場合は、RRM によって AP 上のチャネルが変更され、RAI は機能しません。
- **Config mesh secondary-backhaul enable force-same-secondary-channel**：1 つのホップ MAP をルートとするサブツリー全体で同じセカンダリ チャネルを持つようにします。RRM を無視するか、2 ホップまたはそれよりも深いところにある MAP に手動で割り当てます。

設計の詳細

屋外メッシュ型無線の展開方法は、それぞれのケースで異なり、場所、障害物、使用可能なネットワーク インフストラクチャに関して抱えている問題もさまざまです。これらの問題には、通常、ユーザ、トラフィック、および可用性に基づいた設計要件と併せて対処できます。この項では、設計上の重要な検討事項を説明し、メッシュ型無線設計の例を示します。

メッシュ型無線設計の制約

1500 Mesh AP のメッシュ型無線ネットワークを設計および構築する場合は、さまざまなシステム特性について検討する必要があります。システム特性には、バックホール ネットワークの設計に適用されるものと、WLC の設計に適用されるものがあります。

- 推奨バックホールは 18 Mbps である：最適なバックホール レートとしては、MAP の最大 WLAN カバレッジ距離にも適した 18 Mbps が選択されています。つまり、MAP 間の距離が、18 Mbps バックホールを使用するような距離である場合は、MAP 間のシームレスな WLAN クライアント カバレッジが可能です。ビット レートがこれより低い場合、1500 Mesh AP 間の距離を大きくできますが、WLAN クライアント カバレッジでギャップが生じ、バックホール ネットワークのキャパシティが小さくなる可能性があります。バックホール ネットワークのビット レートを増加すると、さらに多くの 1500 Mesh AP が必要になるか、メッシュ AP 間の SNR が減少し、メッシュの信頼性と相互接続性が制限されます。メッシュ型無線 バックホールのビット レートは、メッシュ チャネルと同様、RAP で設定されます。
- バックホール ホップの数は 3 または 4 に制限する必要がある：ホップの数を 3 または 4 に制限して、まず十分なバックホール スループットを確保することをお勧めします。各メッシュ AP では、バックホール トラフィックの送受信に同一の無線が使用されるからです。これは、スループットがホップごとにほぼ半分になることを意味しています。たとえば、18 Mbps の最大スループットは最初のホップで約 10 Mbps、2 度目のホップで 5 Mbps、3 度目のホップで 2.5 Mbps となります。
- RAP ごとの MAP 数：RAP ごとに設定可能な MAP の数については、現在ソフトウェアでの制限はありません。ただし、メッシュでのボトル ネックを回避するためには、1 つの RAP につき 20 の MAP に制限することをお勧めします。
- コントローラごとの AP 数：コントローラごとの AP の数は、コントローラのキャパシティによって決まります。
- 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の数は、24 に制限されています。

クライアント WLAN

メッシュ AP クライアント WLAN では、標準的な 802.11bg LWAPP の展開により使用可能になる、セキュリティや無線管理の機能全般にわたるあらゆる WLAN の機能が提供されます。

クライアント WLAN の目標では、次の事項についてメッシュの展開全体で考慮する必要があります。

- 必要なビット レート。ビット レートを高くするとカバレッジが狭くなります。これは、メッシュ バックホールにより制限されます。
- 必要なスループット。アプリケーションのスループット要件、および Cisco 1500 Mesh AP で予想される同時クライアント数。
- 必要なカバレッジ。異なる 1500 Mesh AP 間のカバレッジが連続している必要があるか、またはメッシュ展開は個別のアクティブ ゾーンの集まりであるか。
- 必要なセキュリティ メカニズム。WLAN は、パブリックまたはプライベートのいずれでの使用を意図したものであるか。クライアント アクセスに必要なセキュリティ。

ブリッジング バックホール パケット

ブリッジ サービスは、通常のコントローラベースのサービスとは多少異なって扱われます。ブリッジ パケットは LWAPP によりカプセル化されないため、ブリッジ パケット内に外部 DSCP 値は存在しません。したがって、AP で受信された IP ヘッダー内の DSCP 値は、AP 間のパス（バックホール）についての説明のとおり、テーブルへの索引付けに使用されます。

MAP に接続された LAN 上のステーションから受信されたブリッジド フレームは、決して変更されません。802.1p 分類に対するオーバーライド値は存在しません。したがって、ブリッジング モードでは、LAN トラフィック分類は適切に保護される必要があります。

フレームは、無線メッシュ ブリッジへの入力時に受信されると、MAP LAN に正確に転送されます。

1500 では、DSCP のタグが変更されません。

- 入力ポート上で、1510 は、DSCP マーキングを確認し、IP パケットをカプセル化して、対応する 802.1p 優先度を適用します。
- 出力ポート上で、1510 は、IP パケットのカプセル化を解除して、未変更の DSCP マーキング付きで有線上に IP パケットを配置します。

この優先度を有効にするためには、イーサネット デバイス（IP ビデオ カメラなど）が、パケットの DSCP をマーキングする機能を備えている必要があります。

バックホール接続上のクライアント アクセス

バックホール トラフィックを同時に送信しながら、5.8 GHz および 4.9 GHz バックホール接続上でクライアント アクセスを可能にできます。この機能は、展開時に 2.4 GHz クライアントと 5 GHz クライアントの両方をサポートする必要がある場合に、特に有用です。このオプションの機能は、デフォルトでは無効ですが、CLI コマンド インターフェイスで次のコマンドを使用して有効にできます。

(Cisco Controller) >config mesh client-access *enable/disable*

図 8-15 に示すように、GUI では、メッシュ機能のセクションでこの機能を有効にできます。

図 8-15　クライアント アクセス

メッシュの可用性の増加

メッシュ型無線セルには、携帯電話のネットワークを作成するのに使用されるセルとよく似たプロパティがあります。このテクノロジーにより、セルの最大サイズを定義し、同じ物理領域をカバーするより小さなセルを作成して可用性やキャパシティをさらに高めることができます。これは、セルへの RAP の追加によるものです。さらに大規模なメッシュの展開時と同様に、同一チャネルで RAP を使用するかどうか（図 8-16 を参照）、または異なるチャネルを使用するかどうか（図 8-17 を参照）を決定します。領域に RAP を追加すると、その領域に対するキャパシティおよび復元力が追加されます。

図 8-16　同一チャネルを持つセルごとの 2 つの RAP

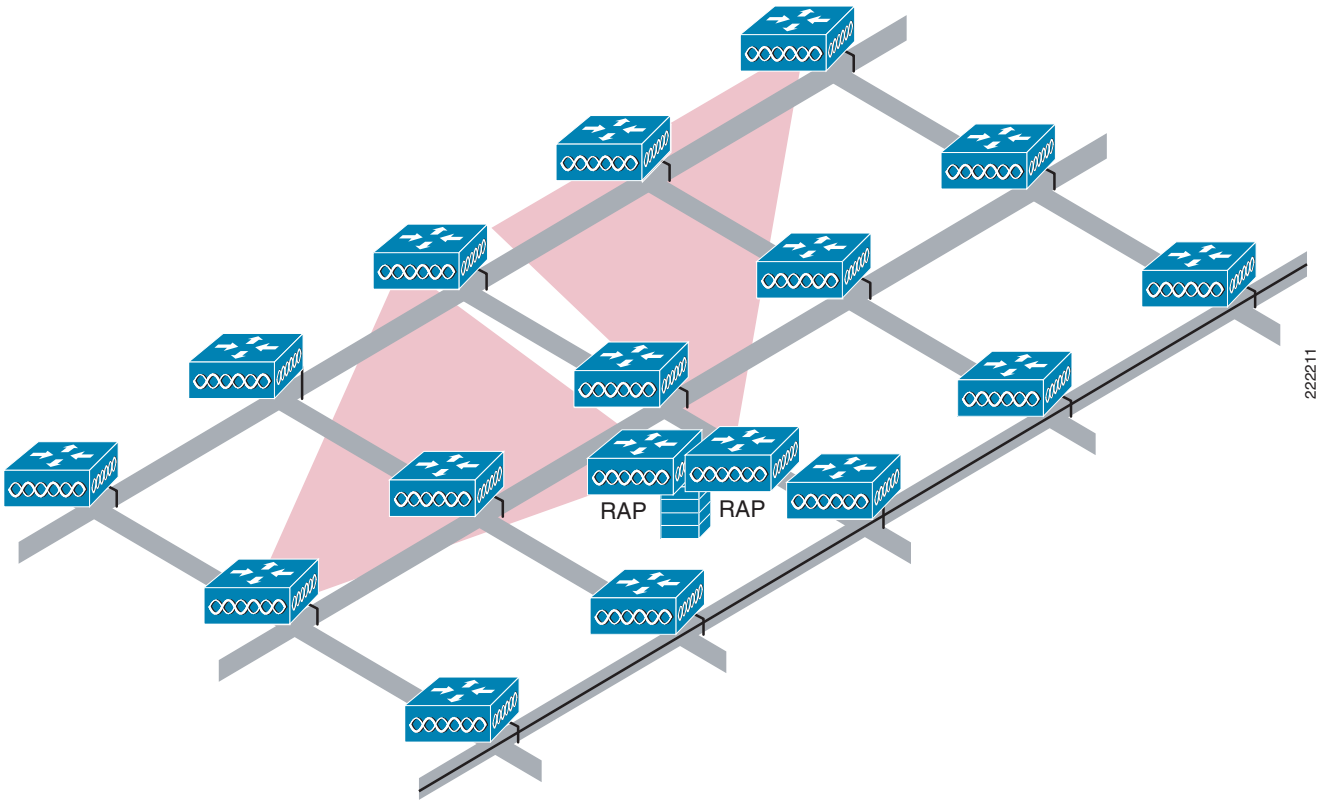
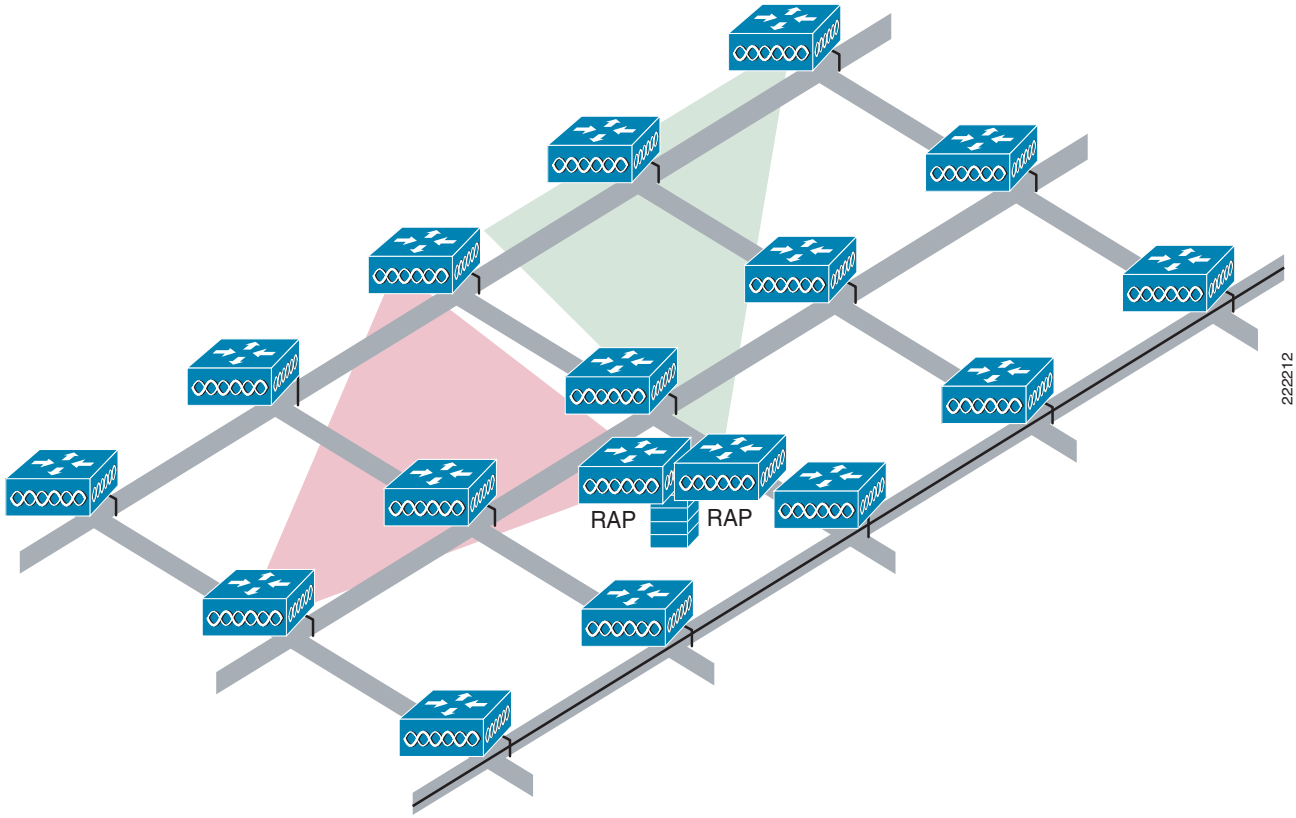


図 8-17　異なるチャネル上のセルごとの 2 つの RAP



複数の RAP

複数の RAP を展開する前に、それらの RAP を展開する目的について検討する必要があります。ハードウェアにダイバーシティ機能を持たせるために RAP を追加することを検討している場合は、追加する RAP をプライマリ RAP と同じチャネル上に展開します。その理由は、メッシュがある RAP から別の RAP に移る場合のコンバージェンスの時間を最小限に抑えるためです。RAP ハードウェアにダイバーシティ機能を持たせることを計画している場合は、RAP ごとに 32 MAP という制限がある点に注意する必要があります。

主にキャパシティを増加させるために追加の RAP を展開する場合は、追加の RAP を近隣する RAP とは異なるチャネルに展開して、バックホール チャネルでの干渉を最小限に抑える必要があります。

2 番目の RAP を異なるチャネルに追加する場合は、チャネル プランニングまたは RAP セル分割を使用して、潜在的なコリジョン ドメインの範囲が小さくなるようにします。チャネル プランニングでは、オーバーラップしない異なるチャネルを同じコリジョン ドメイン内の RAP に割り当てて、コリジョンが発生する確率を最小限に抑えます。RAP セル分割は、コリジョン ドメインを減少させるための簡単で効果的な方法です。メッシュ ネットワークに全方向性のアンテナを持つ 1 つの RAP を展開する代わりに、指向性アンテナを持つ 2 つ以上の RAP を展開できます。これらの RAP を異なる周波数のチャネルで動作するように配置して、大きなコリジョン ドメインを独立して動作する複数の小さなコリジョン ドメインに分割します。

メッシュ型無線のブリッジング機能が複数の RAP で使用されている場合、これらの RAP はすべて同一のサブネット上にあり、ブリッジ クライアントに一貫性のあるサブネットが確実に提供されるようにする必要があります。

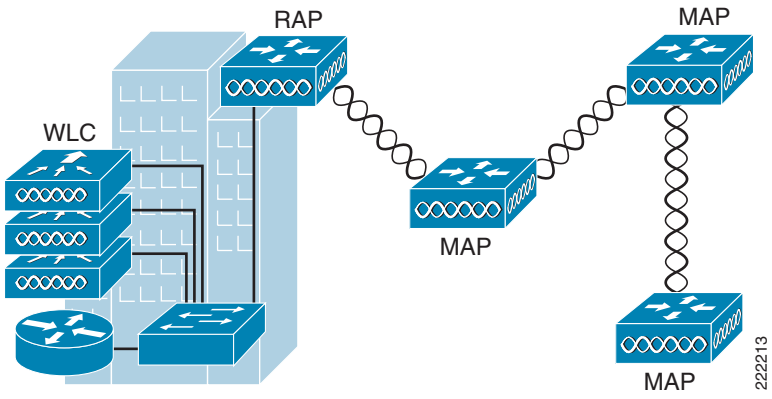
異なるサブネット上に複数の RAP を配置してメッシュを構築すると、フェールオーバー時に MAP のコンバージェンスの時間が増加する可能性があります。なぜならば、MAP が異なるサブネット上の別の RAP へフェールオーバーする必要があり、適切な IP アドレスを DHCP サーバから取得する必要があるからです。この現象が発生しないようにする 1 つの方法は、サブネットの境界で切り離されているネットワークのセグメントに対して異なる BGN を使用することです。この方法でセグメント化すると、MAP は異なるサブネット上の RAP にアソシエートしないので、RAP を追加したことによりコンバージェンスが低速化し、高可用性を実現するための費用がかかるのを避けることができます。

複数のコントローラ

WLC の集中化には運用上の利点があり、そうした利点を得るには LWAPP AP へのリンクの速度とキャパシティ、およびこれらの AP を使用した WLAN クライアントのトラフィック プロファイルを犠牲にする必要があります。

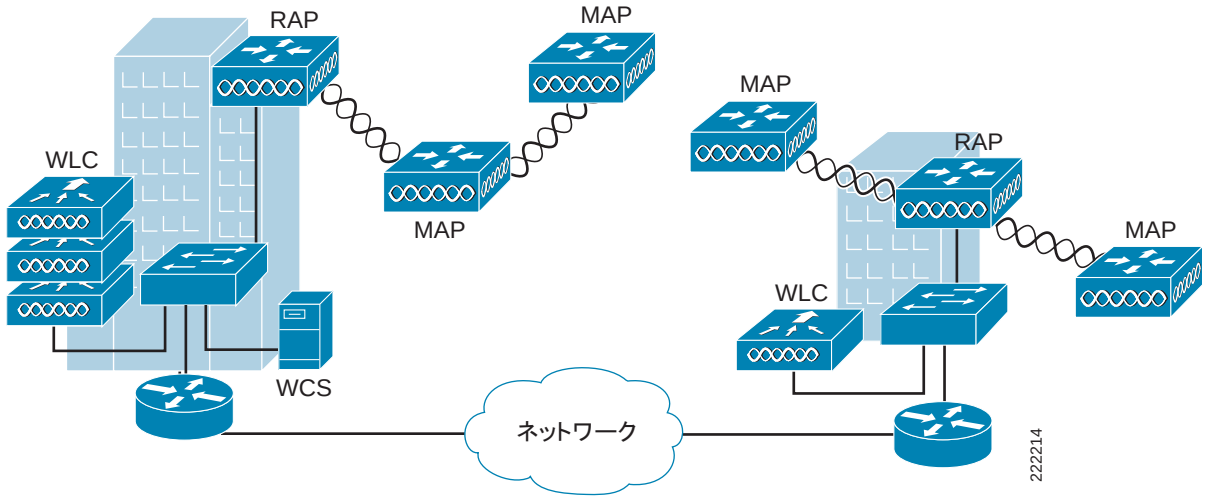
WLAN クライアント トラフィックをインターネットやデータ センターなどの特定のサイトに集中化することが見込まれている場合、コントローラをこれらのトラフィックの中心となっているサイトと同じサイトに集中化させると、トラフィックの効率を犠牲にすることなく運用上の利点を得ることができます（図 8-18 を参照）。

図 8-18　中央集中型コントローラ



WLAN のクライアントのトラフィックが主にピアツーピアである場合は、図 8-19 に示すように、分散コントローラ モデルが適しています。そのような場合、別のロケーションへのトラフィックは少なくなり、大半の WLAN トラフィックがその領域のクライアントどうしのものになる可能性があります。多くのピアツーピア アプリケーションが遅延とパケット損失に対して感度が高い場合、ピア間のトラフィックが最も効率の高いパスを通ることを確認する必要があります。

図 8-19　分散型コントローラ



大半の展開でクライアント サーバ トラフィックとピアツーピア トラフィックを組み合わせている場合は、WLC 配置のハイブリッド モデルが使用される可能性があります。この場合、Points of Presence（PoP；アクセス ポイント）がネットワークの戦略的ロケーションに配置されたコントローラのクラスタで作成されます。

どのような場合でも、メッシュ型無線ネットワークで使用される LWAPP モデルは、LWAPP AP（メッシュ型無線の RAP と MAP）と無線 LAN コントローラの間の高速かつ遅延の少ないネットワークを実現するように設計されます。

複数のメッシュ型無線モビリティ グループ

メッシュ型無線の WLAN カバレッジは、モビリティ グループで使用可能なコントローラの最大数によって制限されることはありません。モビリティ グループの一部である WLAN は、別のモビリティ グループで複製可能であり、WLAN クライアントはこれらのモビリティ グループ間でローミングできます。

モビリティ グループ間でのローミングは、メッシュ型無線ネットワークの背後にあるネットワークトポロジに応じて、レイヤ 2 またはレイヤ 3 で実行される可能性があります。レイヤ 3 ローミングがモビリティ グループ間で実行されるときには、モビリティ トンネリングは実行されません。そのため、クライアントは新しい DHCP アドレスを要求する必要があり、セッションが中断されます。

設計の例

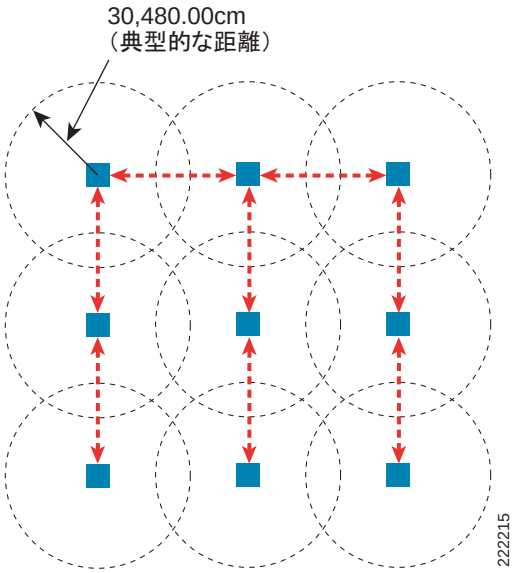
この項では、都会または郊外地域での WLAN カバレッジのサンプル設計について説明します。適切なカバレッジを実現するためには、セル サイズの制限とチャネル間隔について理解しておくことが大切です。次の例では、メッシュ展開におけるこれらの準備方法について説明します。

MAP の密度と距離

セルの計画では、2 つの距離について考慮する必要があります。1 つは一般的なバックホールの半径であり、もう 1 つは一般的な 2.4 クライアント アクセスの半径です。バックホール データにメッシュを単に追加する場合は、半径が 150 m に制限されます。ただし、完全なクライアント カバレッジを実現しようとすると、半径は 90 m に制限されます。

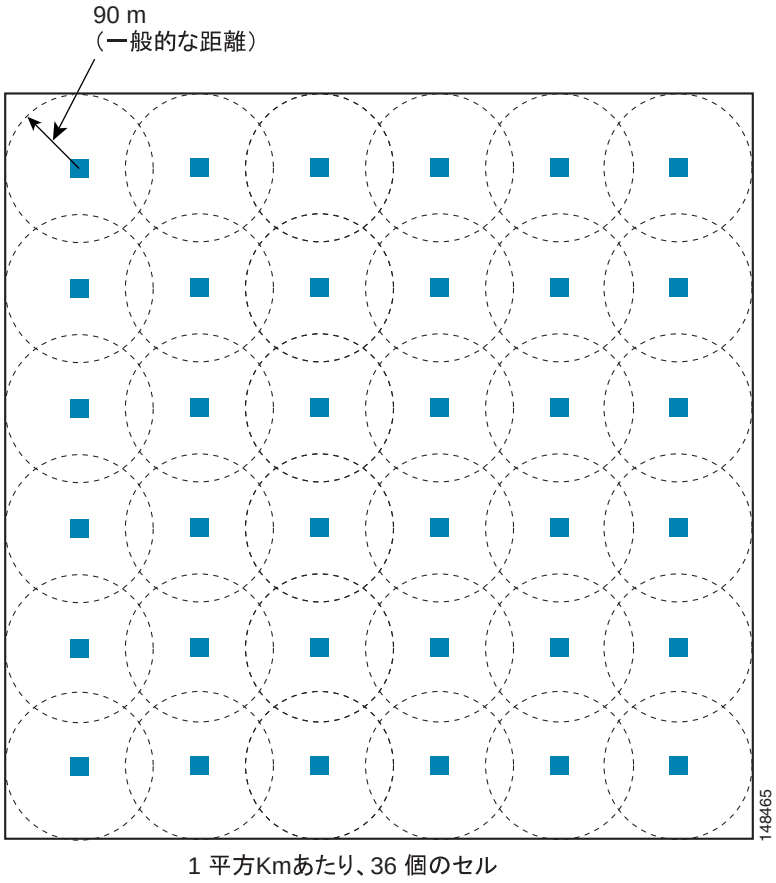
バックホールの周囲でのメッシュ展開を設計しており、シームレスな WLAN カバレッジを実現するつもりではない場合は、一般的なセル サイズの半径である 304 m を使用できます。

図 8-20　304 m の距離の例



シームレスな WLAN カバレッジを実現する展開では、セルの半径を約 90 m にすることをお勧めします。一部オーバーラップしている 1 平方 Km あたりのセルの数は 36 です（図 8-21 を参照）。

図 8-21　90 m の距離の例

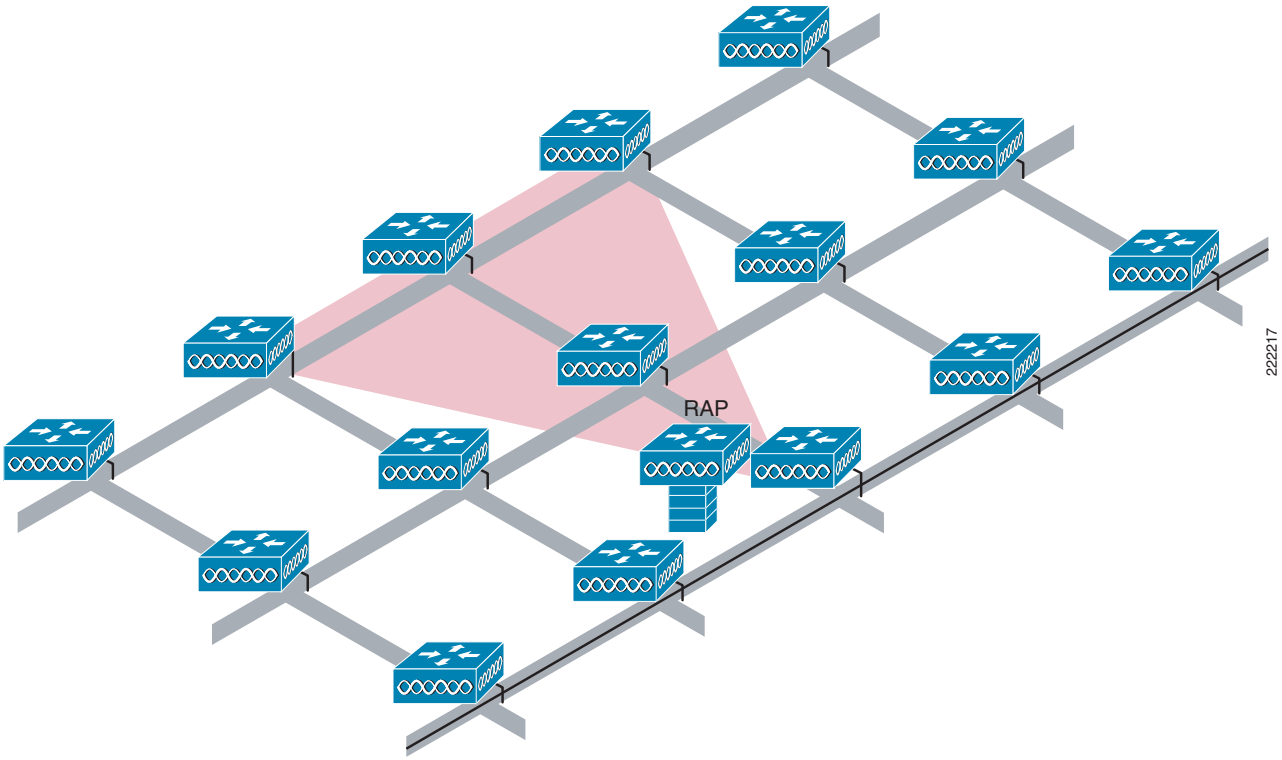


1 平方Kmあたり、36 個のセル

RAP の設置場所を探す場合に目標とするのは、その RAP が設置される場所で RF アンテナを組み合わせて使用するように設計して、セルのコア内の MAP への良好な RF リンクが確立されるようにすることです。

これは、RAP の物理的ロケーションをセルの端にすることが可能であり、指向性アンテナを使用してセルの中心へのリンクを確立することを意味します。

図 8-22　メッシュ型無線のレイアウトの概略図



複数のセルをレイアウトする場合、標準の WLAN プランニングに類似したチャネル プランニングを使用してチャネルのオーバーラップを避けます。図 8-23 に示すように、B2 と D3 が同じチャネルを共有していますが、オーバーラップはしていません。この図で同じチャネルを共有しているその他のセルについても、同様のことが言えます。同じチャネルを共有しているセルは、次のとおりです。

- B2 と D3
- B3 と D2
- B4 と C2
- C3 と D4

可能なら、メッシュが RAP 接続の損失を補うために拡張した場合には、チャネル プランニングもチャネルのオーバーラップを最小限にします（図 8-24 を参照）。

図 8-23　さまざまなセルのレイアウト

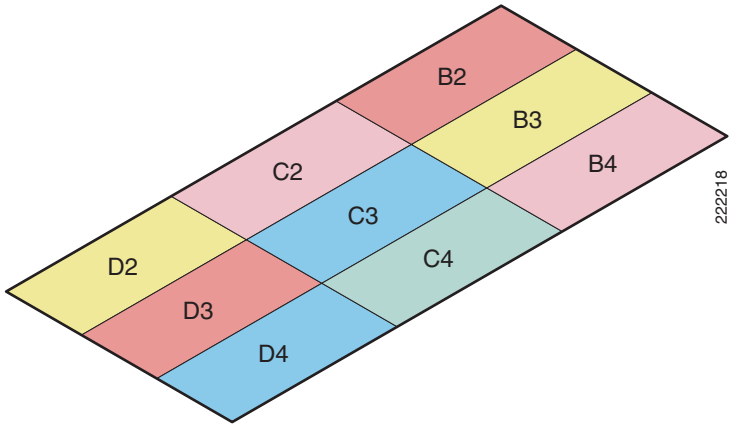
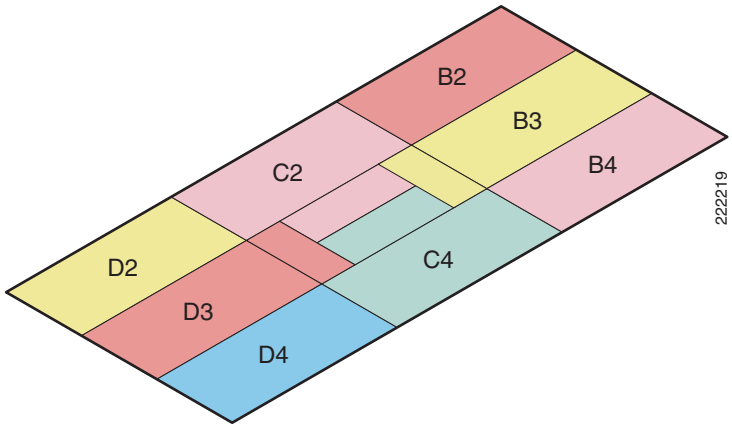


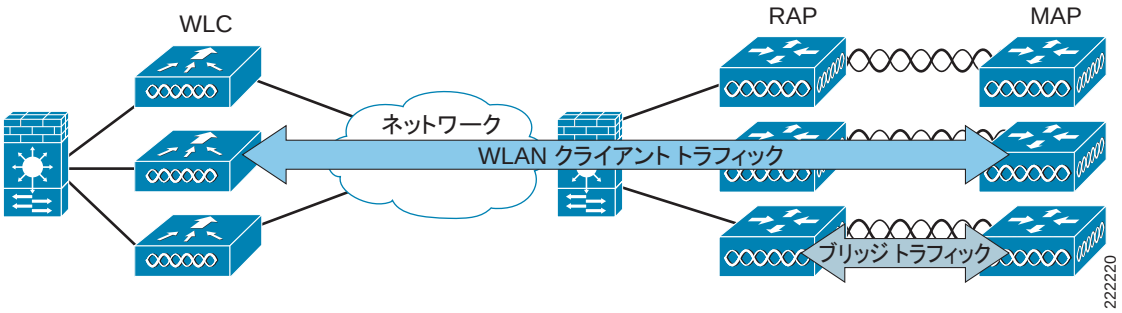
図 8-24　フェールオーバー カバレッジ



各ネットワークへの Cisco 1500 Mesh AP の接続

メッシュ型無線では、ブリッジされたトラフィックまたは WLAN クライアント トラフィックが終端するロケーションが有線ネットワーク上に 2 つあります。最初のロケーションは、RAP が有線ネットワークに接続される地点であり、ブリッジングが有効な場合には、すべてのブリッジされたトラフィックが有線ネットワークに接続される地点になります。2 つめのロケーションは、WLC が有線ネットワークに接続される地点です。こ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されます。これについては、図 8-25 を参照してください。メッシュからの WLAN クライアント トラフィックは、無線 LAN コントローラにトンネルされ、WLAN が割り当てられた VLAN 上で終端します。メッシュ上の各 WLAN に対するセキュリティとネットワーク構成は、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変わります。

図 8-25　メッシュ ネットワーク トラフィックの終端

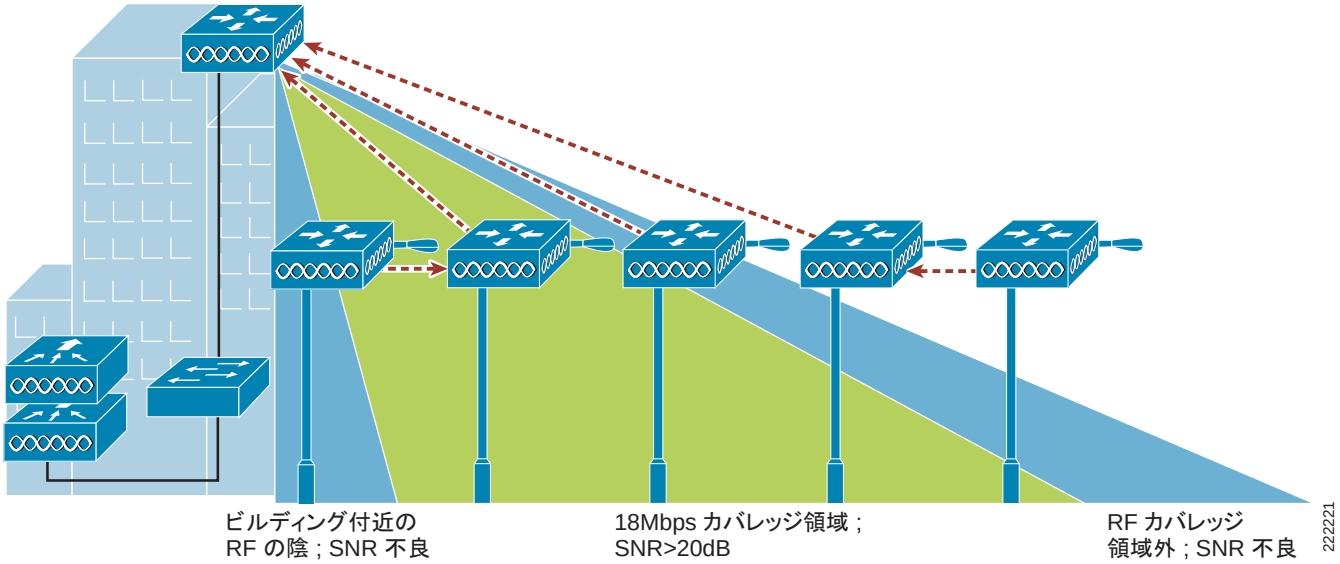


屋外 AP への接続では、屋内 AP の場合とは異なり、有線ネットワークに対するファイアウォールを設定する必要はありません。MAP をブリッジング アプリケーションに使用でき、その MAP により有線 MAP ポート上でセキュリティが制限されるからです。

メッシュ AP の物理配置

MAP の設置場所を選ぶときには、障害となる高い建物、街灯柱の場所、電力オプションなどの問題に注意してください。大半の環境では街灯柱がありますが、それらのすべてに光センサースイッチが装備されているわけではありません。光電池とは、街灯柱が自動的に夜間に点灯し、昼間に消灯するようにするために、街灯柱でよく使用される機能のことです。街灯の電力タップを街灯柱の回路と光電池の間に挿入すると、街灯からの電力を切り替えることができます。街灯柱に光電池がない場合は、別の方法で AP に電力を供給する必要があります。街灯柱の種類および電力の切り替え方法に注意してください。ルーフトップ MAP を配置する場合は、メッシュへの第一ホップとして指定された特定の MAP または MAP のグループがカバレッジエリアとなるようにするために、指向性アンテナが役立ちます。RAP に全方向性アンテナを使用する計画を立てている場合は、そのアンテナを建物の端に向けて取り付けて、無線カバレッジがブロックされないようにします。図 8-26 は、メッシュ内の RAP と MAP 間のカバレッジの関係を示しています。

図 8-26　AP の配置


ビルディング付近の
RF の陰 ; SNR 不良
18Mbps カバレッジ領域 ;
SNR>20dB
RF カバレッジ
領域外 ; SNR 不良
222221

AP 1500 の代替展開オプション

Cisco 1500 シリーズ Mesh AP ソリューションでは、次のような代替展開モードをサポートしています。

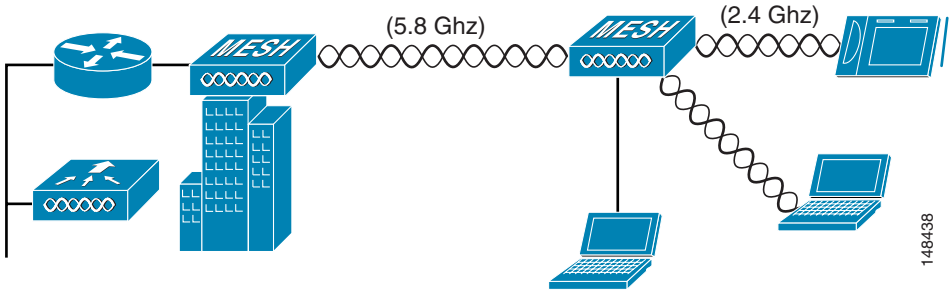
- WLAN バックホール
- ポイントツーマルチポイント無線ブリッジング
- ポイントツーポイント無線ブリッジング

これらの展開方法は、都市環境で LAN セグメントを接続するために役立ちます。また、LAN セグメントのバックアップ接続を補完するために使用することもできます。ブリッジされたネットワーク構成では、クライアント WLAN をサポートすることもできます。次の代替展開方法のいずれでも、メッシュ WLAN クライアント トラフィックを同時にサポートできます。

無線バックホール

Cisco 1500 Mesh AP は、簡易無線バックホール ソリューションを提供できます。このソリューションでは、1500 Mesh AP を使用して 802.11b/g サービスが WLAN および有線クライアントに提供されます。この場合、基本的には、1 つの MAP を持つメッシュ型無線として構成されます。図 8-27 は、このタイプの展開の例を示しています。

図 8-27　無線バックホール

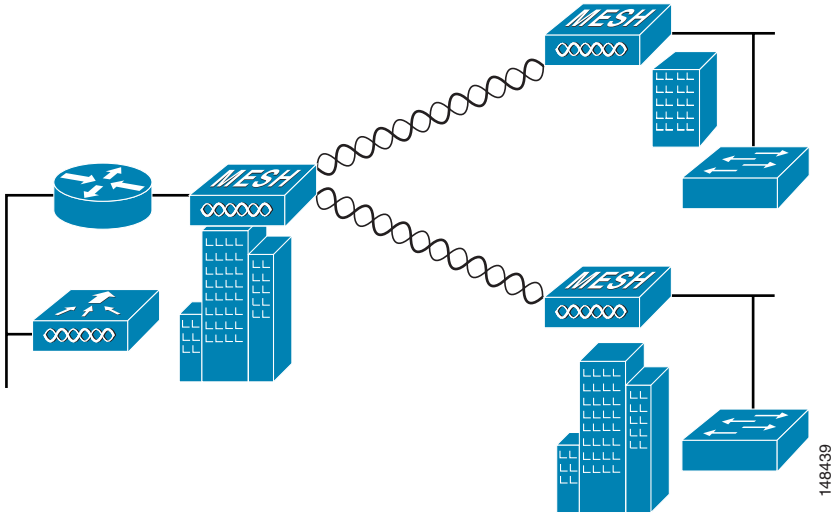


ポイントツーマルチポイント無線ブリッジング

ポイントツーマルチポイント ブリッジングのシナリオでは、ルート ブリッジの役割を果たす RAP が、非ルート ブリッジである複数の MAP を、それらの MAP がアソシエートされた有線 LAN に接続します。デフォルトでは、この機能はすべての MAP で無効になっています。

イーサネット ブリッジングが使用されている場合は、各 MAP のコントローラ上でそれを有効にする必要があります。図 8-28 は、1 つの RAP および 2 つの MAP を持つ簡単な展開を示していますが、これは、基本的に WLAN クライアントを持たないメッシュ型無線として構成されています。クライアントのアクセスに対してイーサネット ブリッジングを有効にすることはできますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

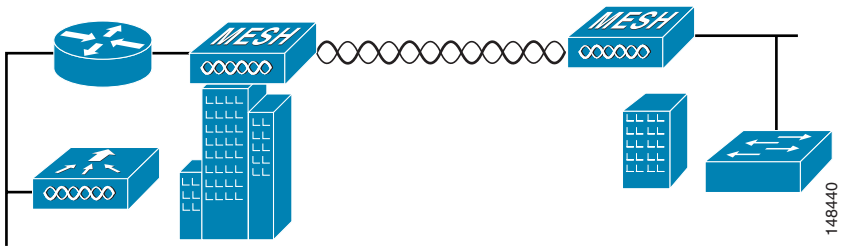
図 8-28　ポイントツーマルチポイント無線ブリッジング



ポイントツーポイント無線ブリッジング

ポイントツーポイント無線ブリッジングのシナリオでは、1500 Mesh AP を使用してレイヤ 2 ネットワークを拡張できます。そのためには、バックホール無線を使用して、2 つのスイッチド ネットワークのセグメントをブリッジします（図 8-29 を参照）。これは、基本的には、1 つの MAP を持ち WLAN クライアントを持たないメッシュ型無線です。ポイントツーマルチポイント ネットワークと同様、クライアントのアクセスに対してイーサネット ブリッジングを有効にすることはできますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

図 8-29　ポイントツーポイント無線ブリッジング



CHAPTER 9

VoWLAN の設計に関する推奨事項

この章では、Voice over WLAN（VoWLAN）ソリューションを展開する際の設計上の考慮事項について詳しく説明します。WLAN 固有の設定は、使用されている VoWLAN デバイスおよび WLAN の設計によって異なります。この章では、第 3 章「WLAN 無線周波の設計に関する考慮事項」で説明されている、VoWLAN の展開において一般に適用される主要な RF およびサイト調査に関する考慮事項についてより詳しく説明します。

アンテナに関する考慮事項

VoWLAN の多くのネットワーク要件は、アンテナの選択に至るまで、WLAN の計画全般にわたって影響を及ぼします。アンテナに関する主な考慮事項は、次のとおりです。

- アクセス ポイント（AP）アンテナの選択
- アンテナの配置
- ハンドセットアンテナの特性

AP アンテナの選択

音声アプリケーション用のダイバーシティ天井マウント アンテナをお勧めします。天井マウント アンテナは、すばやく簡単に設置できます。また、アンテナの放射部分をオープン スペースに配置するため、信号の伝搬と受信を最も効率的に行うことができます。すべてのアンテナを、金属などの高反射面から波長 1 ～ 2 に配置することをお勧めします。2.4 GHz ウェーブは 12.5 cm（4.92 インチ）で、5 GHz は 6 cm（2.36 インチ）です。アンテナと反射面との間の 1 つまたは複数の波長を分離することにより、AP 無線では送信される電波の受信感度が向上し、無線送信時のヌルの生成を減らすことができます。11g と 11a で使用されている Orthogonal Frequency Division Multiplexing（OFDM）により、リフレクション、ヌル、およびマルチパスに関する問題が軽減されます。ただし、アンテナを適切に配置し、適切なタイプのアンテナを使用すると、より良好な結果が得られます。天井タイルそのものが、天井の上部領域に伝送されカバレッジ領域に反射して戻ってくる信号の緩衝材となります。

アンテナのタイプおよびフォーム ファクタにはさまざまなものがありますが、あらゆる用途と場所に適したアンテナのタイプおよびアンテナ モジュールはありません。各種アンテナ、および Cisco Aironet アンテナの製品番号の詳細は、『Cisco Aironet Antennas and Accessories Reference Guide』（http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html）を参照してください。

AP にアンテナを取り付けるときには、屋内の音声アプリケーション用の Cisco AIR-ANT5959（2.4 GHz 用）および ANT5145V-R（5 GHz 用）を使用することをお勧めします。これら 2 つのアンテナには次のような利点があります。

- ロー ゲイン全方向性カバレッジおよびアンテナ ダイバーシティ
- 上方傾斜角の低減。床上へのカバレッジの拡散の可能性が低減され、天井タイルの上にあるエアー ダクトなどの金属物からのリフレクションが低減されます。
- ほとんどの天井タイル上の T バーへの取り付けが容易

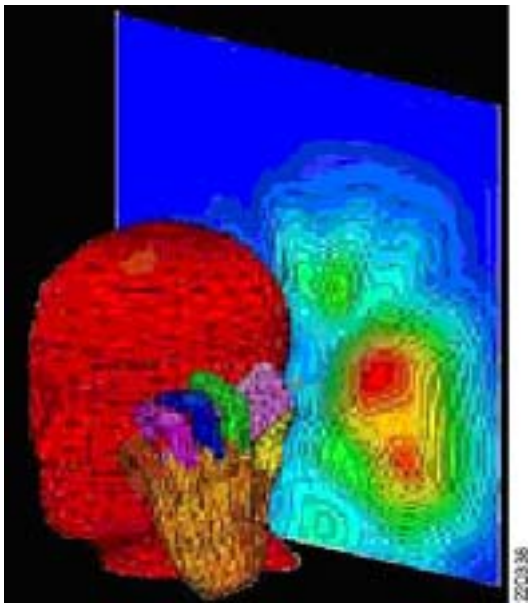
ハイ ゲイン アンテナは信号を水平平面に拡散させ、これにより、多くのノイズを拾う大規模セルが作成されます。この結果、Signal-to-Noise Ratio（SNR; 信号対雑音比）が低くなり、パケット エラーの比率が高まります。SNR は次の 2 つの条件によって定義されます。

- 信号：ある無線から送信され、中断されずに他の無線が受信できる放射エネルギー。すなわち、Wi-Fi では、送信無線によって、受信無線がデコード可能な 802.11 プロトコルのパケットが送信されます。
- ノイズ：受信無線の周波数範囲内の送信エネルギーのうち、その無線でデコードできないもの。

プロトコル パケットとバックグラウンド ノイズ間のエネルギー差が大きいほど、プロトコル パケットを適切に受信することができ、パケット エラー レートおよびビット エラー レートが減少します。カバレッジ領域の設計では、複数のチャネルを使用して、高いコール キャパシティを維持したままでの最も低いパケット エラー レートの作成が行われます。

ハイ ゲイン アンテナを使用すると、カバレッジ領域が増えるため、Wi-Fi チャネル上のコール数も減少します。音声の場合、人間の頭と体が 5dB の信号を減衰させるため、壁面マウント パッチよりも天井マウント アンテナが推奨されます（図 9-1 を参照）。天井マウント アンテナは、たいていの壁面マウント アンテナよりも人間の頭と体による減衰を防ぐように、適切に配置されます。

図 9-1　頭と体による減衰



アンテナの位置決め

天井マウント アンテナでは、通常、携帯電話へのより適切な信号パスが使用されます。頭などの障害物による減衰があるため、推奨カバレッジ セル サイズでは信号損失が考慮されます。アンテナのゲインは受信と送信の両方で同程度になることを理解しておくことが大切です。アンテナ ゲインは、送信電力の増加を表すものではありません。送信電力を発生させるのは無線です。アンテナは、パッシブ デバイスにすぎません。ゲインは、無線信号の焦点を、ある方向、平面、およびビーム幅に合わせることで導出されます。それは、懐中電灯のリフレクタによって、電球から放射される光の焦点が合わせられるのと同じです。

WLAN RF 計画の詳細は、第 3 章「WLAN 無線周波の設計に関する考慮事項」を参照してください。

ハンドセットアンテナ

Cisco Unified Wireless IP Phone 7920 および 7921G には、電話の本体から伸びるアンテナが付いています。電話の持ち方は、手による信号減衰にほとんど影響しません。

電話本体にアンテナが内蔵されている場合は、ユーザの電話の持ち方によって 4dB の信号減衰が起こることがあります。手でアンテナを覆って頭で電話を支えた場合には、9dB の信号減衰が起こることがあります。屋内での展開の場合、一般的に、信号が 9dB 減衰するごとにカバレッジ領域は半減します。図 9-1 は、頭で支えた場合のハンドセットからの放射電力の違いの例を示しています。

2.4 GHz スペクトラムを使用するハンドセットでは、通常、ダイバーシティ アンテナを使用しません。2.4 GHz 波長はおよそ 5 インチであり、実際にアンテナ ダイバーシティを実装して信号の受信感度を向上させることはできないからです。そのため、AP においてのみリンクの質を高めることができます。電話と AP 間のリンクの質を最適にするには、AP がデフォルト設定で動作する必要があります。デフォルト設定では、ダイバーシティ アンテナとダイバーシティを有効にできます。

Cisco 7921G などの 802.11a 端末では、11a 無線用のダイバーシティ アンテナ ソリューションが使用されます。

チャネルの使用率

802.11、802.11b、および 802.11g のいずれの規格でも、2.4 GHz 帯域が使用されます。これらすべての規格で、同じ帯域を同時に使用する必要があるため、オーバーヘッドが増加し、チャネル スループットが減少します。多くのサイトには、すでに 2.4 GHz Wi-Fi 帯域を使用している製品があります。また、そのほかにも多数の製品が、Wi-Fi で使用されるのと同じ 2.4 GHz 帯域を使用しています。たとえば、Bluetooth 機器、コードレス電話、ビデオ ゲーム コントローラ、監視カメラ、電子レンジなどです。2.4 GHz 帯域の輻輳やチャネル割り当ての制約を考えると、新たに VoWLAN を展開するときには、5 GHz Wi-Fi 帯域の使用を検討する必要があります。5 GHz で使用可能なチャネルは、ほとんどのサイトで自由に使用できます（図 9-2 を参照）。VoWLAN トラフィックに W53 チャネルを使用する場合、レーダーが存在してはなりません。このため、いずれかの新しいサイトで追加テストを実施し、W53 のチャネルを設定でブロックすべきかどうかを確認することをお勧めします。このテストを実施する理由は、AP が標準使用時にレーダーを検知した場合、その AP は 10 秒以内にチャネルを離れなければならないからです。

図 9-2　オフィスでの 2.4 GHz と 5 GHz の標準チャネル使用率

Cisco Unified Wireless Network をインストールする前に、チャネル干渉および AirMagnet、Wild Packets、Cognio などのツールの使用に関して、サイトをテストする必要があります。Wireless Control System（WCS）AP オンデマンド統計ページには、次の項目についてのスペクトラム レビューが記載されています。

- チャネル別ノイズ
- チャネル別干渉
- クライアント数と RSSI との比較
- クライアント数と SNR との比較
- チャネル レーダー探知の時間変化

Dynamic Frequency Selection（DFS; 動的周波数選択）および AP の 802.11h 標準

米国の Federal Communications Commission（FCC）、European Telecommunications Standards Institute（ETSI）および日本の総務省などの監督機関は、無線周波数の使用に関する標準を定めています。5 GHz 帯域の一部は、現在（過去においても）、気象レーダーなどのレーダーで使用されています。ほとんどの 5 GHz レーダー システムでは、一般に波長の短い高周波数を使用していますが、一部の WiFi W53 帯域を重複して使用するシステムも存在します。2007 年 1 月に、総務省は 5.6 GHz 帯域（W56）を無線 LAN に開放しました。これらの周波数が新たに使用可能になったことにより、「干渉のない」ように AP の設定を管理することが必要になりました。AP のレーダー パルスを定期的に監視し（通常、軍事、衛星、気象観測所から）、レーダーが探知された場合は自動的に「クリーン」チャネルに切り替える必要があります。

レーダーが探知された場合、システムで次のことを実行する必要があります。

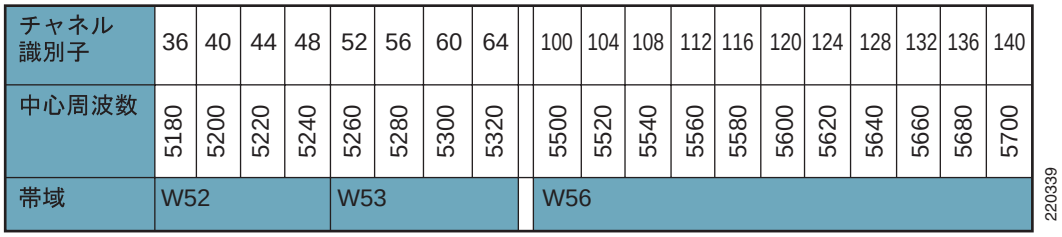
- 200 ミリ秒以内にパケット伝送を中止
- 10 秒以内に制御伝送を中止
- 30 分間、チャネル上での伝送を回避
- 伝送前に 60 秒間、新規チャネルをスキャン

W53 のレーダー要件では、音声アプリケーションを稼動させる前にレーダーのテストを実施することが求められています。これは、レーダー回避に必要な動作が音声コールの質に影響する可能性があるためです。Cognio Spectrum Expert も、レーダーの存在をテストするためのすぐれたツールです。テスト中にレーダーが探知された場合、該当するチャネルを使用しないように AP を設定できます。

5 GHz 帯域のチャネル

図 9-3 は、日本での 802.11a のチャネル割り当てを示しています。DFS 要件には、従来の 8 つの W52 および W53 チャネル（36 ～ 64）と、11 の新しい W56 チャネル（100 ～ 140）が含まれます。5 GHz 帯域には現在 19 のチャネルがあります。これらは重複しないチャネルであり、すべて同じ場所に配置できます。2.4 GHz には重複しないチャネルは 3 つしかありません。1 つのカバレッジ領域に共存配置チャネルを許容する設計により、カバレッジ領域で取得可能なコール数が集約されます。

図 9-3　802.11a チャネル割り当て



日本で割り当てられているチャンネルとアクセスポイントの対応表は以下の URL を参考にしてください。

ワイヤレス LAN 適合状況
http://www.cisco.com/japanese/warp/public/3/jp/product/hs/wireless/airo1500/prodlit/pdf/wlancs.pdf

図 9-4 に示すように、チャネルを基準とするチャネルベースの設計を単一フロアに実装できます。複数フロア設計では、フロア間でチャネルを分離して、チャネル相互の干渉を減少させることができます。

図 9-4　単一フロアのチャネル設計

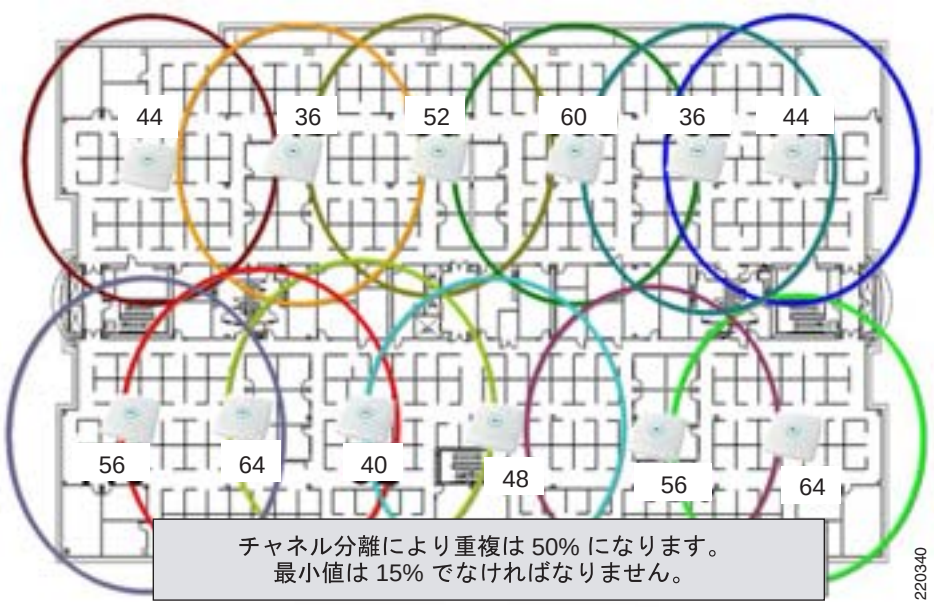
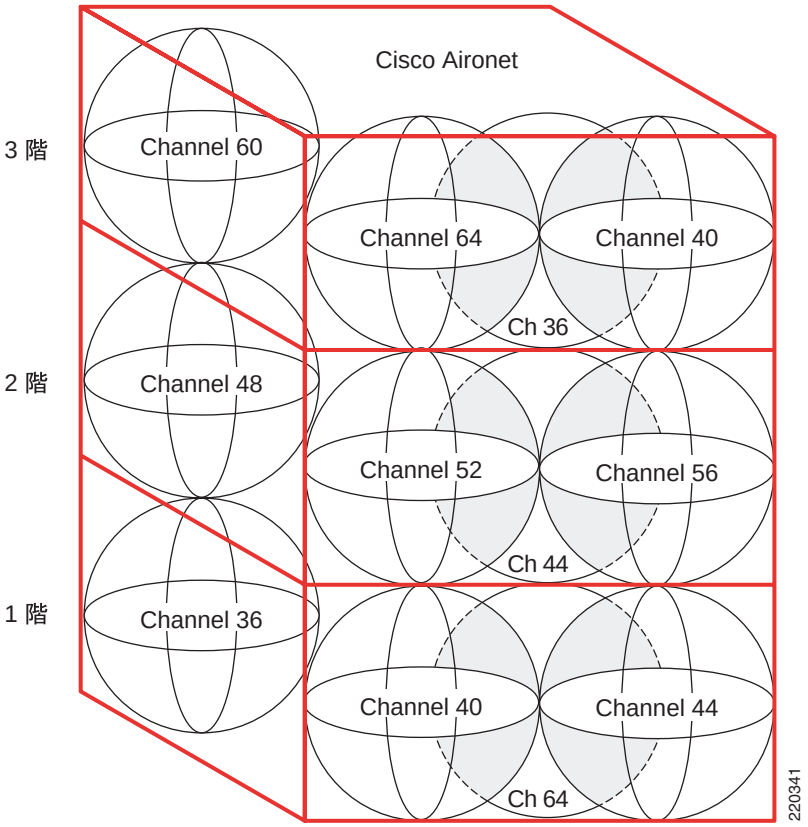


図 9-5 は、垂直チャネル分離を示しています。

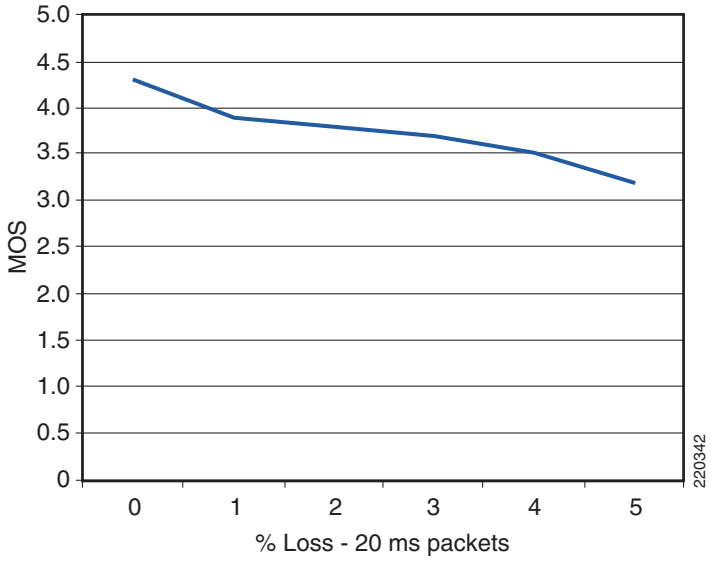
図 9-5　垂直チャネル分離



コール キャパシティ

Wi-Fi チャネルのコール数は、多くの要因によって制限されます。まず、AP および VoWLAN クライアントによって使用されるメディアは、RF スペクトラムです。RF スペクトラムは、シールド ツイストペア CAT 5 ケーブルなどの電磁干渉からシールドできません。Wi-Fi でセグメンテーションに最も近いのは、チャネル分離です。この、802.11 のオープンな共有メディアは、高パケット損失の原因となることがあります。このようなパケット損失の大部分には、802.11 フレームを再送することで対処しますが、その結果としてジッタが発生します。図 9-6 は、パケット損失の関係を Mean Opinion Score（MOS; 平均オピニオン評点）として示しています。

図 9-6　実際のパケット損失



802.11a では、802.11g と同様、最も低いデータ レート（6 Mbps）によって最も高いカバレッジ範囲が実現します。同じ電力レベルの場合、最も低いパケット エラーも 6 Mbps です。

許容可能な音声のカバレッジ領域は、5% 以下のパケット エラー レートが維持される領域です。MOS スコアは次のようにランク付けされています。

- 4.4：最高 G.711 MOS スコア
- 4.3 ～ 4.0：「非常に満足」から「満足」
- 4.0 ～ 3.6：「一部のユーザにとって満足」

図 9-6 は、5% のパケット エラー レートによって MOS が低下し、スピーチの質が「一部のユーザにとって満足できる」レベルまで低下した例を示しています。

電話のカバレッジ領域の境界は、そのカバレッジ領域の MOS が「非常に満足である」というカテゴリに当てはまる場所です。この章では、カバレッジ領域の境界を*セルの境界*と呼びます。複数の電話クライアントやデータ クライアントどうしの干渉、相互チャネルの干渉、その他の説明のつかない干渉が発生する可能性があるため、音声に対しては、パケット エラー レートが 1% のセルの境界が必要です。セルの境界およびカバレッジ設計については、この章の他のセクションで詳しく定義されています。

802.11 および 802.11b で従来の 2.4 GHz Wi-Fi クライアントをサポートする必要がない場合は、1、2、5.5、および 11 のレートを無効にすることをお勧めします。これらのレートが無効な場合、1 つ以上の 802.11g データ レートを「必須」に設定する必要があります。データ レート 6 は通常「必須」に設定することが推奨されるデータ レートですが、これはセル サイズ設計要件によって異なり、高ビット レートを使用する必要がある場合があります。可能であれば、802.11b/g ネットワークよりも 802.11g 専用ネットワークが推奨されます。ほとんどのデータ クライアントおよび電話クライアントは、AP からビーコンとプローブ応答でアドバタイズされたデータ レートを認識します。したがって、クライアントは、AP によってアドバタイズされた「必須」データ レートで、管理、制御、マルチキャスト、およびブロードキャスト パケットを送信します。クライアントは、ユニキャスト パケットを AP によってアドバタイズされた任意のデータ レートで送信できます。一般に、これらのユニキャスト パケットは、AP とクライアント間のリンクに対して最も信頼性の高いデータ レートを提供できるデータ レートで送信されます。AP は、クライアント リンクごとに固有のデータ レートでユニキャスト パケットを送信できます。

パケットの受信において、SNR を考慮することは重要です。無線受信器は、AP または電話機のいずれかです。SNR はリンクの両方の無線で同じではありません。SNR とマルチパス干渉は、AP およびカバレッジ領域の境界で考慮する必要があります。パス損失は、リンクの両方の終端で同じであると想定できます。

音声アプリケーションに対しては、実際の電話機を使用して、希望するデータ レートでセルの境界を設定することをお勧めします。Wi-Fi アプリケーションにおいて AP と電話間で送信される音声パケットは、通常、標準サイズ 236 バイトのユニキャスト RTP G711 パケットです。Real-Time Transport Protocol（RTP）パケットは UDP および IP プロトコルに基づいているため、RTP はコネクションレスです。通話の信号強度、SNR、データ レート、およびエラー レートは、スタンドアロン AP または Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）コントローラ上の AP 統計から確認できます。図 9-7 および図 9-8 は、802.11g および 802.11a の電話クライアントのセルの境界における dBm 値のサンプルを示しています。図 9-9 は、コール ストリーム統計を示しています。ストリーム メトリックは、音声メトリックを有効にした後に WCS で表示できます。メトリックを有効にするパスは、Configure > Controller > ipaddress > 802.11bg > Voice Parameters > Enable Voice Metrics です。

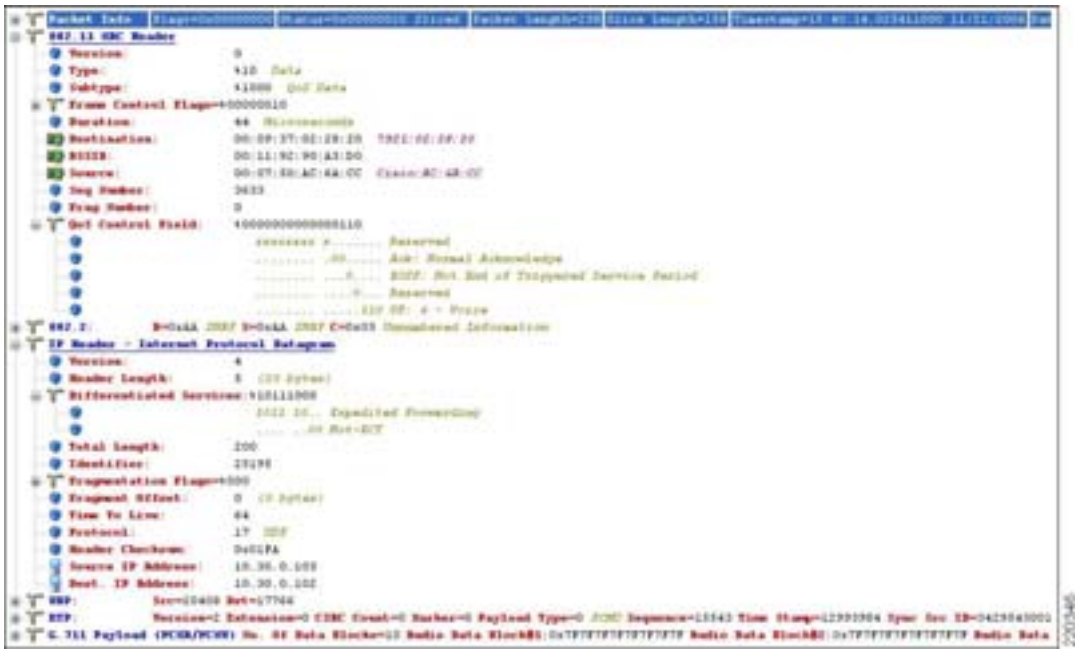
図 9-7　11g クライアント統計

図 9-8　11a クライアント統計

図 9-9　WLC コール メトリック

図 9-10 は、デコードされた RTP パケットを示しています。このパケットは、7960 電話から発信されています。Over-the-Air QoS マーキングは、QoS ベースライン マーキング 5 から、802.11e 仕様に準拠するユーザ優先度 6 に変更されています。Cisco 7920 および 7921 電話のコール統計は、電話に表示することも、電話の IP アドレスを使用して電話をブラウズして確認することもできます。実際の電話でテストしてセルの境界を特定した後は、より自動化されたツールを使用してこれらの数値を適合させ、サイトのカバレッジ設計を完了できます。

図 9-10　VoWLAN キャプチャのサンプル



信号レベルが測定されている場所でマルチパス干渉がある場合は、報告される値がパケットごとに変動する可能性があります。パケットは、前のパケットより 5dB 高いか、低い可能性があります。所定の測定場所での平均値が算出されるまでに数分かかることがあります。

AP コール キャパシティ

AP ごとの同時音声ストリーム数の計画は、VoWLAN 展開の計画プロセスのキーとなる部分です。AP の音声ストリーム キャパシティを計画する際は、次の点を考慮してください。

（注） 同一 AP に関連付けられている 2 つの電話間のコールは、2 つのアクティブな音声ストリームとしてカウントします。

- 無許可の（共有）802.11 チャネルの使用率によって、AP が伝送できる同時音声ストリーム数が確定されます。
- チャネルの使用率と AP のパフォーマンスによって音声ストリーム数が決定されるため、同じチャネルと次のチャネルの分離が非常に重要になります。2 つの AP が同一の場所にあり、同一チャネルで動作していても、音声ストリーム数は 2 倍にはなりません。実際、AP が 1 つの場合よりも音声ストリームが少なくなることがあります。
- セル キャパシティまたは帯域によって、同時に実行可能な音声ストリーム数が決定されます。
- ハンドセットおよび VoWLAN 展開でサポートされているハンドセット QoS 機能を、考慮する必要があります。
- ハンドセットにはさまざまな WLAN QoS 機能があり、これらは WLAN 展開で有効化されている機能に影響を与え、最終的には AP ごとのコール キャパシティを決定します。ほとんどの VoWLAN ハンドセットでは、その電話でサポートされる AP ごとのコール数についての指針が示されています。そして、それは、ハンドセットで最適な QoS 機能を使用でき、チャネル キャパシティにフル アクセスできる最良のケースでの値を示していると考える必要があります。

チャネルでサポート可能な実際の音声ストリーム数は、環境要因やクライアントでの WMM および Cisco Compatible Extension 仕様の遵守など、多くの問題に左右されます。図 9-11 は、コールの質の向上やチャネル キャパシティの拡大に非常に役立つ Cisco Compatible Extension 仕様を示しています。シミュレーションでは、5 GHz チャネルが 14 ～ 18 コールをサポートできることを示しています。すなわち、1 つのカバレッジ セルには 20 の AP があり、それぞれの AP は異なるチャネル上で動作しており、各チャネルでは 14 の音声ストリームがサポートされています。このカバレッジ セルは 280 のコールをサポートできます。複数の 802.11b クライアントが 1 つのチャネルを使用している場合、そのチャネルでは 7 つの音声ストリームがサポートされるため、重複しない 3 つのチャネル上に 3 つの AP を持つカバレッジ セルでは 21 の音声ストリームがサポートされます。

図 9-11　Cisco Compatible Extension VoWLAN 機能

How Cisco Compatible Extensions Benefits VoWLAN Call Quality	
Feature	**Benefit**
CCKM Support for EAP-Types	Locally Cached Credentials Means Faster Roams
Unscheduled Automatic Power Save Delivery (U-APSD)	More Channel Capacity and Better Battery Life
TSPEC-Based Call Admission Control (CAC)	Managed Call Capacity for Roaming and Emergency Calls
Voice Metrics	Better and More Informed Troubleshooting
Neighbor List	Reduced Client Channel Scanning
Load Balancing	Calls Balanced Between APs
Dynamic Transmit Power Control (DTPC)	Clients Learn a Power to Transmit At
Assisted Roaming	Faster Layer 2 Roams

220352

図 9-11 は、次のことを示しています。

- Cisco Centralized Key Management（CCKM）は Extensible Authentication Protocol（EAP）認証クライアントに高速クライアント ローミングを提供し、これによってコールの質が向上します。
- Call Admission Control（CAC; コール アドミッション制御）によってコールの質を向上し、E911 およびローミング コール用の帯域予約を作成できます。
- AP　支援ローミングおよび近接リストによって、コールの質が向上し、バッテリの寿命が延びます。
- 音声メトリックは管理に役立ちます。
- Unscheduled Automatic Power Save Delivery（U-APSD; 不定期自動省電力配信）および Dynamic Transmit Power Control（DTPC: 送信電力の動的制御）によってバッテリの寿命が延びます。
- 負荷分散および DTPC はコールの質を向上させます。

Cisco Compatible Extensions 機能には、さまざまな利点があります。

バッファ メモリの量、CPU 速度、および無線品質は、AP 無線のパフォーマンスを左右する主要な要因です。QoS 機能はチャネル内の音声およびデータ トラフィックを優先順位付けします。QoS の詳細は、第 5 章「Cisco Unified Wireless QoS」を参照してください。

802.11e、WMM、および Cisco Compatible Extensions 仕様では、セルが音声ストリームで過負荷にならないように、負荷を分散できます。CAC は、コールを再起動するのに十分なチャネル キャパシティがあるかどうかを判断します。ない場合、電話は別のチャネルをスキャンします。U-ASPD の主な利点は、WLAN クライアントの電力の節約です。これは、WLAN クライアントからのフレームの送信を可能にし、節電のために AP でバッファされるクライアント データ フレームの転送をトリガーすることによって実現されます。近隣リスト オプションでは、近隣 AP のチャネル番号とチャネル キャパシティを含むリストが電話に提供されます。これによってコールの質が向上し、高速ローミングが実現し、バッテリの寿命が延びます。

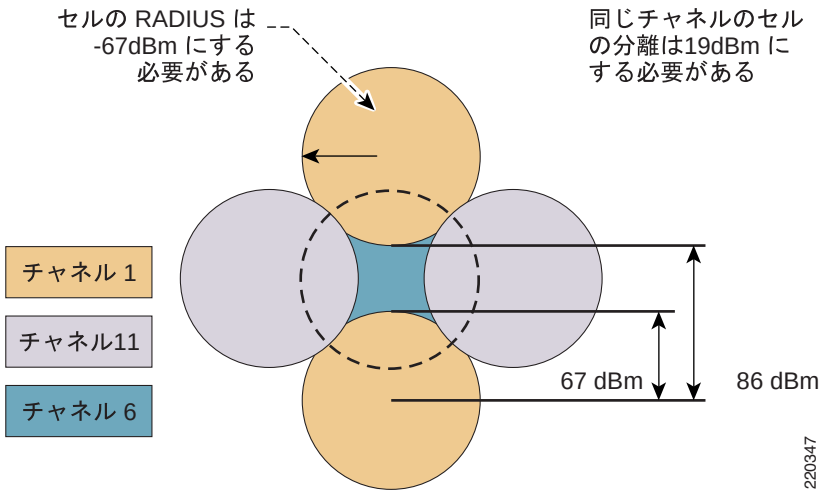
U-APSD および CAC の詳細は、第 3 章「WLAN 無線周波の設計に関する考慮事項」を参照してください。

セルの境界の設計

802.11b/g/a VoWLAN ハンドセットの展開ガイドラインでは、セルの境界線の最小電力を -67dBm にする設計が推奨されています（図 9-12 を参照）。これにより、以前に設計されたデータ WLAN で使用されていたセルよりも小さいセルが作成されます。-67dBm のしきい値は、パケット エラーを 1% にするために通常推奨される値ですが、そのためには、SNR 値を 25dB 以上にする必要があります（この要件には、その地域のノイズ条件が影響します）。したがって、特定の電話タイプの見込みチャネル カバレッジ領域を決定する場合は、電話で計測される信号強度とノイズの両方を、AP によって提供されるクライアント統計を使用して検証する必要があります。スタンドアロン AP および LWAPP AP 上でのこれらの値の決定については、図 9-8 および図 9-11 を参照してください。

-67dBm という信号強度の測定値は、802.11b 準拠の電話のベンダーで長年にわたって使用されてきました。テストの結果、この経験に基づく測定値を 802.11g および 802.11a 準拠の電話のクライアントにも適用できることが確認されています。

図 9-12　セルの境界の測定



（注） 図 9-12 は、-86 dBm の理想的な分離方法を簡略化して示したものです。このように 19dBm を分離させることは、たいていの展開では実現不可能なことです。RF の設計基準として特に重要なのは、セル半径を -67 dBm にすることと、セル間のオーバーラップが推奨値である 20% になるようにすることです。これらの制約に従って設計することにより、チャネル分離が最適化されます。

5 GHz セルの場合、使用可能なチャネル数から考えても、同一チャネルの分離に関して考慮しなければならないことは、あまりありません。802.11a では、周波数がオーバーラップしない 3 つのチャネルしか存在しない 2.4 GHz 帯域とは対照的に、チャネルが 19（電話機が W56 に対応していることが前提）あるため、ほとんどの場合に 2 チャネル分離が可能です。

5 GHz および 2.4 GHz の両方で、セルの境界を、指定チャネルに必要な最高データ レートでパケット エラー レート 1% が維持されるようなフロア レベルに配置する必要があります。802.11b の場合、データ レートは 11 Mbps です。したがって、AP の場所を中心として電話機の信号が AP によって認識されるフロア上の場所までがセルとなり、その境界は -67 dBm です。

802.11g および 802.11a 電話クライアントは、最大 54 Mbps のレートを実現できる可能性があります。現在のチップ セットは 54 Mbps をサポートしていますが、送信電力は実際それぞれ異なっています。電話クライアントと AP 間のすべてのリンクを、一致する送信電力レベルで確立することを強くお勧めします（送信電力の動的制御（P. 9-16）を参照）。

特定のデータ レートに対してカバレッジ セルを作成できます。高密度展開または小さいフロア空間に多数のコールが必要な展開では、チャネル数および 54 Mbps というデータ レートを考慮して、802.11a が推奨されます。802.11a で低いデータ レートを無効にして、データ レート 24 Mbps を「必須」に設定し、36 ～ 54 のレートをそのまま有効にしておくことができます。

セルの境界を -67 dBm に設定した後、1% のエラー レートが発生している場所を特定して、SNR 値を確認します。

-67 dBm のセルの境界は、次のように決定されます。

- 電話を、必要な送信電力に設定します。
- AP を、一致する送信電力に設定します。
- AP と必要なアンテナを、電話を使用する場所に配置します。
- アクティブなコールを使用して、または G711 コーデックと同一サイズのパケットを送受信する間に、-67 dBm セル境界への信号レベルを測定します。

個々の電話端末のデータ シートで、特定の Wi-Fi 帯域においてその電話端末でサポートされている送信電力レベルとデータ レートをよく確認します。Cisco Unified Wireless IP Phone のデータ シートは、http://www.cisco.com/en/US/products/hw/phones/ps379/index.html にあります。他のベンダーの電話については、各ベンダーの Web サイトを確認してください。

80211a の最大送信電力レベルは、チャネルおよび AP のモデルによって異なります。802.11g の最大送信電力レベルは、モデルごとに異なります。Cisco Aironet AP のデータ シートで、どのモデルの AP がどのデータ レートに対応しているかをよく確認する必要があります。図 9-13 は、日本の電波法で規定されているチャネル別の Max EIRP（dBm）を示しています。

図 9-13　チャネルの Max EIRP

5GHz	W52				W53				W56										
チャネル	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140
のMax EIRP	10	10	10	10	10	10	10	10	17	17	17	17	17	17	17	17	17	17	17

220353

5 GHz 帯域での最大許容送信電力は、6dB 単位で変化します。これは、すべてのチャネルを使用可能なサイトで最大許容送信電力を使用する場合、すべてのチャネルのセル カバレッジが同じになるわけではないことを意味します。また、動的なチャネル選択が使用されている場合、セル カバレッジ エッジはチャネル数によって変化する可能性があります。ただし、動的なチャネル選択は調整可能です（第 3 章「WLAN 無線周波の設計に関する考慮事項」を参照）。動的なチャネル選択のデフォルト モードでは、チャネルごとの最大送信電力レベルの相違に対応します。

すべての AP 上のセル送信電力は、電話の最大または希望送信電力を超えてはなりません。電話の最大送信電力または設定送信電力が 10 dBm の場合、すべての AP の最大送信電力が 10 dBm であることが推奨されます。したがって、AP の最大送信電力を同じレベルに設定するか、それが不可能であれば、次に大きい送信電力レベルに設定する必要があります。片通話を避けるために、同じ送信電力に設定することが推奨されます。一般に、AP は電話よりもレシーバの感度およびダイバーシティがすぐれているため、やや低い強度の電話信号を受信できる必要があります。同じ送信電力の詳細は、送信電力の動的制御（P. 9-16）を参照してください。

デュアル バンド カバレッジ セル

第 3 章「WLAN 無線周波の設計に関する考慮事項」で、2.4 GHz と 5 GHz 帯域のチャネル カバレッジ設計について説明されています。デュアル モード AP において 2.4 GHz チャネルと 5 GHz チャネルの両方で同じセル カバレッジを提供する場合、2.4 GHz チャネルは 5 GHz チャネルと同じ（または低い）送信電力を持つ必要があります。多くのサイトでは、SNR 計算式のノイズ レベルは 10dB 低くなります。802.11g 無線のレシーバの感度は、一般に同じデータ レートの 11a 無線よりも 2dBM すぐれています。たとえば、7921G のデータ シートでは、データ レート 36 Mbps での受信感度は、802.11g の場合は -78 dBm で、802.11a の場合は -76 dBm となっています。したがって、ノイズ フロアを 10 dB 向上させると、802.11a セルの感度は 8 dBm 向上します。802.11g と 802.11a とのパス損失の差異など他にも項目があるため、正比例はしません。ただし、同じカバレッジ セルを希望する場合は、802.11g ネットワークの電力レベルを 11a ネットワークよりも 1 または 2 レベル引き下げる必要があります。

送信電力の動的制御

Cisco Aironet AP ではデフォルトで DTPC が有効になっています。DTPC は、Wireless LAN Controller により自動化されており、スタンドアロン AP 上で設定できます。DTPC を使用するには、クライアントで少なくとも Cisco Compatible Extensive v2 機能がサポートされている必要があります。

DTPC では次のことが実現されます。

- 電話の送信電力を AP の送信電力と一致するように設定します。
- AP はクライアントに知らせるために送信電力をアドバタイズします。
- 片通話を防止します。すなわち、RF トラフィックは単方向でのみ受信されます。

DTPC により、電話の送信電力を AP の送信電力に自動的に一致させることができます。図 9-14 の例では、電話の送信電力が 5 mW から 100 mW に変更されています。

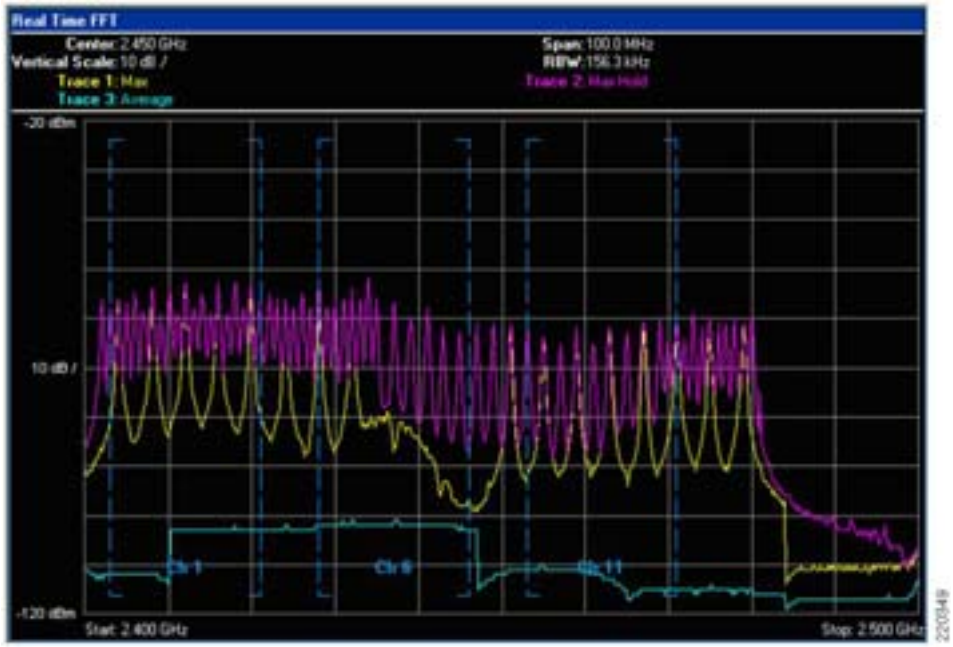
図 9-14　クライアントと AP の電力の一致

802.11g および 802.11a のライセンス要件では、クライアントの送信電力は 100mW ありません。アクセス ポイントの最大設定送信電力が、クライアント電話端末のハードウェア サポートより高い値にならないようにすることを強くお勧めします。電話の送信電力が AP よりやや低い方が、AP の送信電力が電話より少ないよりも望ましいとされますが、送信電力が一致していると、片通話（典型的なケースとしては、ユーザが相手の声を聞き取りにくい）が発生する可能性を減らすことができます。

ユーザにとってローカルな干渉源

干渉はユーザによってローカルですが、近接ユーザにも影響する可能性があります。Bluetooth（BT）は、Wi-Fi 2.4 GHz チャネルと干渉するパーソナル エリア ネットワークで使用される一般的な RF プロトコルです。図 9-15 は、実際の BT 信号が 802.11b/g クライアントで使用されるすべての 2.4 GHz チャネルにまたがっていることを示しています。この図は電話に取り付けられた BT ヘッドセットを使用した 802.11g コールに基づくものです。図 9-16 は、BT ヘッドセットからのジッタも示しています。

図 9-15　標準的な BT イヤピースの 802.11b/g 2.4 GHz スペクトラムにおける Bluetooth（BT）信号パターン

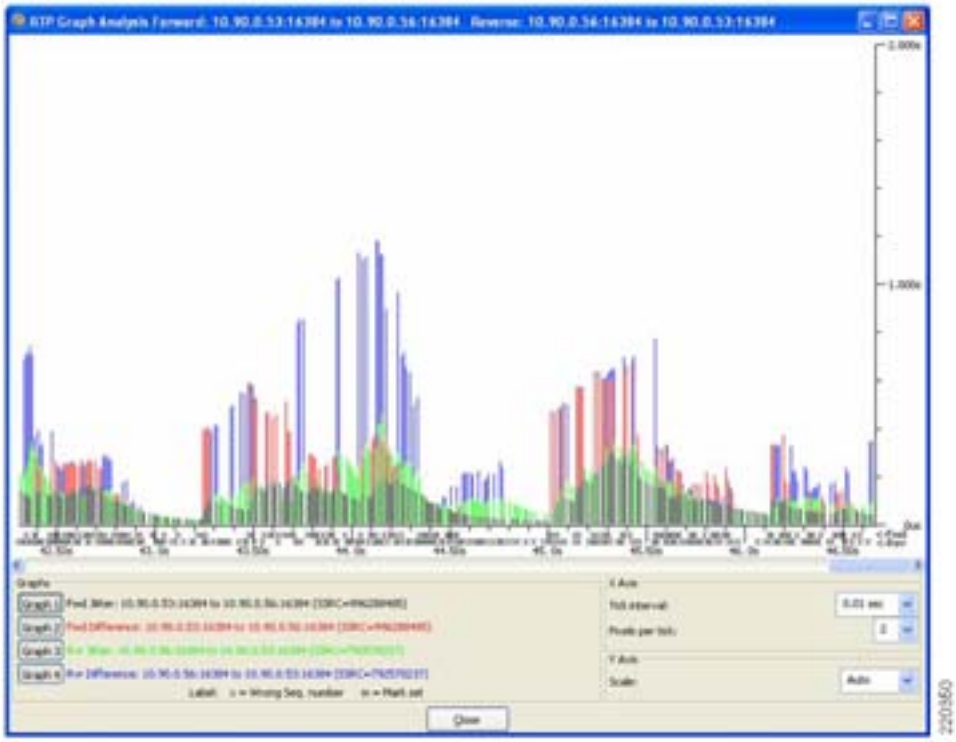


ピンクは、最大ホールド回線、すなわちテスト中に達した最大送信電力を示す回線です。**黄色**は、10 秒の最新サンプル期間における最大送信電力を示しています。**青緑色**は、テスト期間における平均送信電力を示します。**縦の破線**は、重複しない 3 つの 802.11b/g チャネル、**Ch1、Ch6、**および **Ch11** を区切っています。グラフは 2.400 GHz（左）から 2.500 GHz（右）までを示しています。Ch11 の縦の青線の右端からが、欧州と日本で使用されている 802.11 スペクトラム部分です。このデータは、北米の規制ドメイン用に設定されている AP およびクライアントでキャプチャされました。このグラフは、BT イヤピースが容易に FCC 認定外に伝送していたことを示しています。

BT 信号は非常に狭いことに注意してください。BT はデータを単一周波数（MHz）で送信し、送信を中止し、802.11 2.4 GHz 帯域の別の周波数に移動した後、データを送信します。これが絶え間なく繰り返されます。802.11b および 802.11g 信号は、混合周波数 22 MHz で送信されます。無線はその周波数 22 MHz に残ります。22 MHz のグループをチャネルと呼びます。最大ホールド回線は、検索モードでの BT の強度を示します。信号レベルは 50mW（17dBm）OFDM 802.11g 無線より上です。この強度および長さの信号により、802.11b/g 電話は VoWLAN コールをドロップします。BT 信号の強度が低いと、ジッタが発生して MOS 値が低くなります。

図 9-16 は、それぞれ BT イヤピースを使用する 3 つの同時通話の Ethereal ジッタ分析の例を示しています。

図 9-16　ジッタ分析の例



3 つのコールはすべて同一 AP 上にあり、この AP 上の他の電話へのコールでした。

CHAPTER 10

Cisco Unified Wireless Guest Access Service

企業が無線 LAN（WLAN）テクノロジーを導入することにより、従業員やネットワーク リソースが固定ネットワーク接続の制約から解放され、大企業や中小企業の行動の取り方に変化が生じてきました。

また、WLAN によって、個人が公共の場所からインターネットや会社のネットワークにアクセスする方法も変化しました。公衆無線 LAN（ホットスポット）の出現により、モバイル ワーカーは、事実上どこからでも会社のネットワークにアクセスできることが当たり前だと考えています。

はじめに

パブリック アクセスのパラダイムは、企業にも広がってきています。企業が、ビジネスパートナー、訪問客、ゲストに座る場所と電話連絡の外線を提供するだけで十分であった時代はとうの昔に過ぎ去りました。移動性の高い情報オンデマンド文化には、オンデマンド ネットワーク接続が必要です。社内のネットワーク リソースにアクセスできずに客先で半日費やしてしまうと、打ち合わせやサービス、営業活動の生産性に影響を与え、また、外出している個人の全体的な生産性は低下します。このような理由から、エンタープライズ ゲスト アクセス サービスは、重要性を増し、企業環境に不可欠のものとなっています。

ゲスト ネットワーキングが重要性を増していることが広く知られている一方で、社内情報やインフラストラクチャ資産の安全性に対する不安があることも事実です。皮肉なことに、多くの企業がそれと知らず、ゲストを野放し状態にし、適切に導入されていない有線または無線ネットワーク経由でインターネットにアクセスできる方法を探させているのです。このようなゲストは、真のハッカーではなく、悪意はありませんが何かをしようとする者です。そのため、表面上は、ゲスト アクセス ソリューションの実装が危険なことのように思われますが、実装が適切であれば、たいていのゲスト アクセス ソリューションを実装した企業では、実装プロセスに関連したネットワーク監査によって、全体的なセキュリティ状況が改善されます。

全体的なセキュリティの改善に加えて、ゲスト アクセス ネットワークの実装によって、次のようなメリットが得られます。

- 日付、期間、帯域幅などの変数に基づく、ゲストの認証と権限付与の制御
- ネットワークを使用中または使用したことのあるユーザをトラックする監査メカニズム

さらに、無線ベースのゲスト アクセスのメリットには、次のものが含まれます。

- かつてはネットワーク接続のなかったロビーや共有施設などを含め、より広範なカバレッジを提供します。
- ゲスト アクセスの領域や部屋を設定する必要がなくなります。

範囲

企業でゲスト アクセスを提供する際、複数のアーキテクチャを実装できます。この章の目的は、考えられるソリューションをすべて紹介することではありません。その代わりに、この章では、Cisco Unified Wireless ソリューションを使用した無線ゲスト ネットワーキングの実装を中心に説明します。その他のトポロジ シナリオにおける有線および無線ゲスト アクセス サービスの展開に関する詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.html#anchor5

無線ゲスト アクセスの概要

理想としては、無線ゲスト ネットワークの実装で、企業の既存の無線および有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲスト アクセスを必要とするあらゆる場所で、キャンパス無線ネットワークを介して実装されます。
- ゲスト トラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ 2 またはレイヤ 3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲスト アクセスを制御する外部プラットフォームの実装を伴います。
- ゲスト ユーザ資格情報の管理：スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロール プラットフォーム内に常駐している場合と、AAA またはその他の管理システムのコンポーネントになっている場合があります。

Cisco Unified Wireless ソリューションを使用したゲスト アクセス

Cisco Unified WLAN ソリューションは、中央集中型アーキテクチャ内で EtherIP（RFC3378）を使用することにより、柔軟で簡単な実装方法で無線ゲスト アクセスの展開を提供します。EtherIP は、2 つの WLC エンドポイント間にあるレイヤ 3 トポロジ上のトンネルを作成する際に使用されます。このアプローチのメリットは、ゲスト トラフィックを企業から分離するために実装が必要となる、プロトコルやセグメンテーション テクニックを追加しなくていいことです。中央集中型 WLAN アーキテクチャを使用したゲスト アクセス トポロジの例については、図 10-1 を参照してください。

図 10-1　中央集中型コントローラのゲスト アクセス

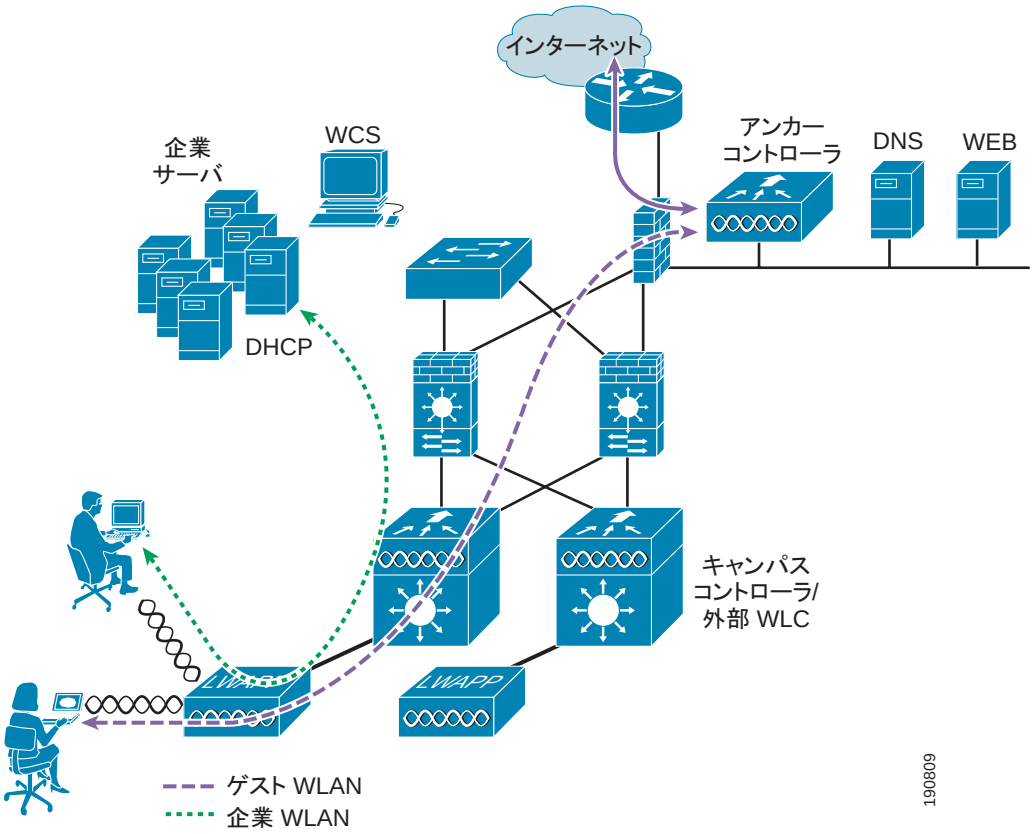


図 10-1 に示すように、WLC が企業 DMZ に配置され、「アンカー」機能を実行します。このアンカー コントローラは、ネットワーク上のその他のキャンパス WLC を起点とする EoIP トンネルの終端処理に関与します。これらの「外部」コントローラは、企業全体にプロビジョンされたさまざまな WLAN（1 つ以上のゲスト WLAN を含む）の終端、管理、および標準の動作に関与します。ゲスト WLAN は、対応する VLAN にローカルにスイッチされるのではなく、代わりに EoIP トンネルを経由してアンカー コントローラに転送されます。具体的には、ゲスト WLAN のデータ フレームが、LWAPP を使用して AP から外部コントローラにカプセル化されてから、外部 WLC からアンカー WLC で定義されたゲスト VLAN に EoIP でカプセル化されます。このように、ゲスト ユーザ トラフィックは、社内の他のトラフィックによって認識されることなく、また相互作用することなく、透過的にインターネットに転送されます。

WLAN コントローラ ゲスト アクセス

WLC Guest Access ソリューションは、内蔵型であり、アクセス コントロール、Web ポータル、または AAA サービスを実行するための外部プラットフォームを必要としません。こうした機能はすべて、アンカー コントローラ内で構成および実行されます。ただし、これらの機能のうち 1 つまたはすべてを外部で実装するためのオプションがあり、これについてはこの章の後半で説明します。

サポートされているプラットフォーム

トンネル終端、Web 認証、およびアクセス コントロールを含むアンカー機能が、次の WLC プラットフォームでサポートされています（バージョン 4.0 以降のソフトウェア イメージを使用した場合）。

- Cisco 4400 シリーズ
- Cisco 6500 シリーズ（WISM）
- WLC と統合した Cisco 3750

次の WLC プラットフォームは、アンカー機能に使用できませんが、標準のコントローラ展開と指定したアンカー コントローラへのゲスト モビリティ トンネルの起点（外部 WLC）として使用できますできます。

- Cisco WLAN Controller Module for Integrated Service Router（ISR）
- Cisco 2100 シリーズ

無線ゲスト アクセスをサポートする自動アンカー モビリティ

自動アンカー モビリティ、つまりゲスト WLAN モビリティは、Cisco Unified Wireless ソリューションの主要な機能です。EoIP トンネルを使用して、プロビジョンされたゲスト WLAN を 1 つ以上の（アンカー）WLC にマップできます。自動アンカー モビリティによって、ゲスト WLAN と関連するすべてのゲスト トラフィックを、インターネット DMZ に常駐するアンカー コントローラに企業ネットワークを通して透過的に転送できます（図 10-2 を参照）。

図 10-2　自動アンカー EoIP トンネル

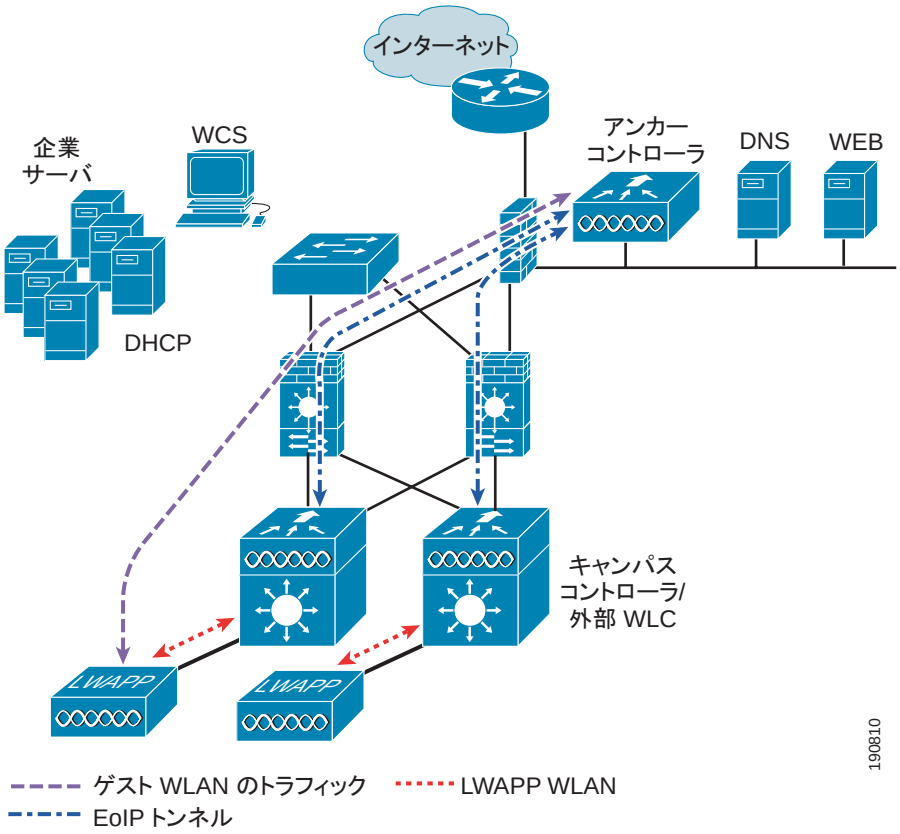
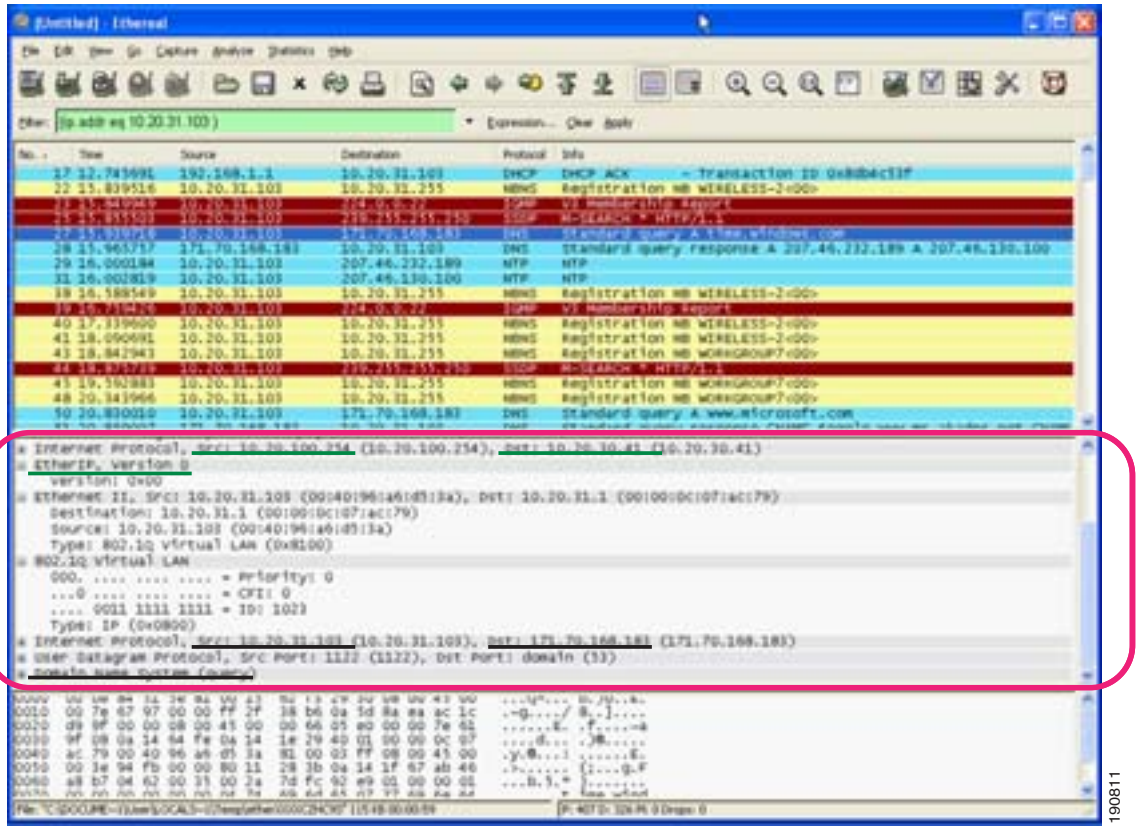


図 10-3 は、ゲスト WLAN がプロビジョンされた外部コントローラとローカル Web 認証を実行しているアンカー コントローラ間の EtherIP トンネル（強調表示部分）のスニファ トレースを示しています。図中の最初の IP 詳細は、外部コントローラとアンカー コントローラ間の EtherIP トンネルを示しています。2 番目の IP 詳細は、ゲスト トラフィックの詳細です（この場合は、DNS クエリー）。

図 10-3　EtherIP スニファ トレースのサンプル



アンカー コントローラ展開ガイドライン

この項では、無線ゲスト アクセスをサポートするためのアンカー コントローラの展開に関するガイドラインを提供します。

アンカー コントローラの位置決め

アンカー コントローラは、ゲスト WLAN トラフィックの終端とそれに続くインターネットへのアクセスに関与するため、通常は企業のインターネット DMZ 内に配置されます。これによって、社内の認証されたコントローラとアンカー コントローラ間の通信を的確に管理するためのルールをファイアウォール内に確立できます。このルールには、送信元または送信先のコントローラのアドレス、WLC 間通信用の UDP ポート 16666、およびクライアント トラフィック用の IP プロトコル ID 97 EtherIP に対するフィルタリングが含まれます。その他に必要なルールは次のとおりです。

- SNMP 用の TCP 161 と 162
- TFTP 用の UDP 69
- HTTP 用 または GUI アクセスの HTTPS 用の TCP 80 または 443
- Telnet 用、または CLI アクセスの SSH 用の TCP 23 または 22

トポロジによっては、ファイアウォールを使用して、外部の脅威からアンカー コントローラを保護できます。

最大のパフォーマンスを引き出すために、また、ネットワーク内の位置決めが推奨されていることから、ゲスト アンカー コントローラをゲスト アクセス機能のサポートに専念させることをお勧めします。つまり、アンカー コントローラを、ゲスト アクセスの他に、社内の他の LWAPP AP（LAP）の制御や管理に使用しないようにします。

DHCP サーバ

前述したように、ゲスト トラフィックは、EoIP を経由してレイヤ 2 に転送されます。したがって、DHCP サービスを実装できる最初のポイントは、ローカルのアンカー コントローラ上か、クライアントの DHCP 要求を外部サーバに中継できるコントローラ上になります。設定例については、ゲスト アクセスの設定（P. 10-15）を参照してください。

ルーティング

ゲスト トラフィックは、アンカー コントローラで出力されます。ゲスト WLAN は、アンカー上の動的なインターフェイスまたは VLAN にマップされます。トポロジによって、このインターフェイスが、ファイアウォール上のインターフェイスに接続される場合と、インターネット境界ルータに直接接続される場合があります。したがって、クライアントのデフォルト ゲートウェイ IP は、ファイアウォールの IP か、または最初のホップ ルータ上の VLAN またはインターフェイスのアドレスになります。入力ルーティングの場合は、ゲスト VLAN が直接、ファイアウォール上の DMZ インターフェイスに接続されるか、境界ルータ上のインターフェイスに接続されることが考えられます。いずれの場合も、ゲスト（VLAN）サブネットは、直結ネットワークと認識され、それに応じてアドバタイズされます。

アンカー コントローラのサイジングとスケーリング

企業における展開の多くで、ゲスト ネットワーキングを最も効率的にサポートするプラットフォームは、Cisco 4400 シリーズ コントローラです。このコントローラを EoIP トンネル終端によるゲスト アクセスのサポートに限定して展開する場合、コントローラはネットワーク内の LAP の管理に使用しないと考えられるため、12 個の AP をサポートする 4402 で十分です。

1 台の 4400 シリーズ コントローラで、社内にある最大 40 台の外部コントローラからの EoIP トンネルをサポートできます。さらに、4400 は、同時に最大 2,500 ユーザをサポートし、2Gbps の転送能力があります。

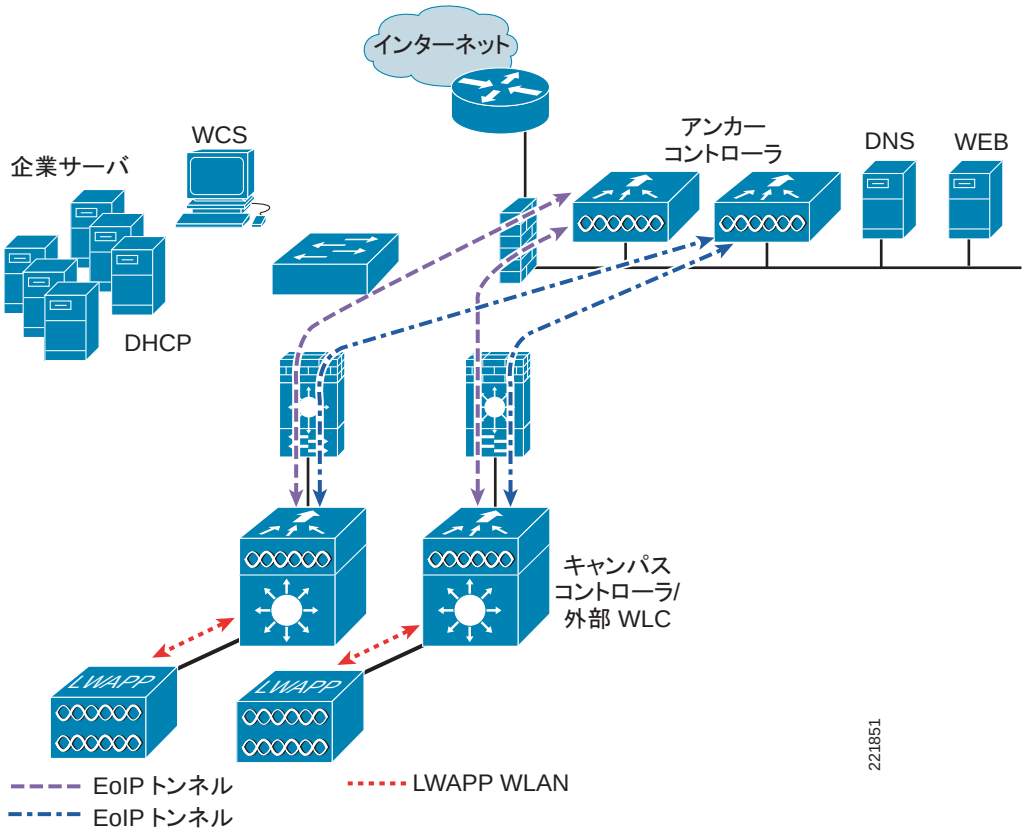
アンカー コントローラの冗長性

Unified Wireless ソリューション ソフトウェアのリリース 4.1 からは、「ゲスト N+1」冗長性機能が自動アンカー / モビリティ機能に追加されました。この新機能には、自動 ping 機能が導入されています。この機能によって、外部コントローラが積極的に ping をアンカー コントローラに送信して、コントロールとデータ パスの接続を確認できます。障害が発生したり、アクティブなアンカーに到達できなくなった場合には、外部コントローラが次のことを行います。

- アンカーが到達できなくなっていることを自動的に検出
- 到達できないアンカーに以前にアソシエートされた無線クライアントを自動的に解除
- 無線クライアントを代替アンカー WLC に自動的に再びアソシエート

ゲスト N+1 冗長性により、所定のゲスト WLAN に 2 つ以上のアンカー WLC を定義できます。図 10-4 は、アンカー コントローラの冗長性を備えた、一般的なゲスト アクセス トポロジを示しています。

図 10-4　ゲスト アンカーの N+1 冗長性を備えたゲスト アクセス トポロジ



ゲスト N+1 冗長性については、次のことに留意してください。

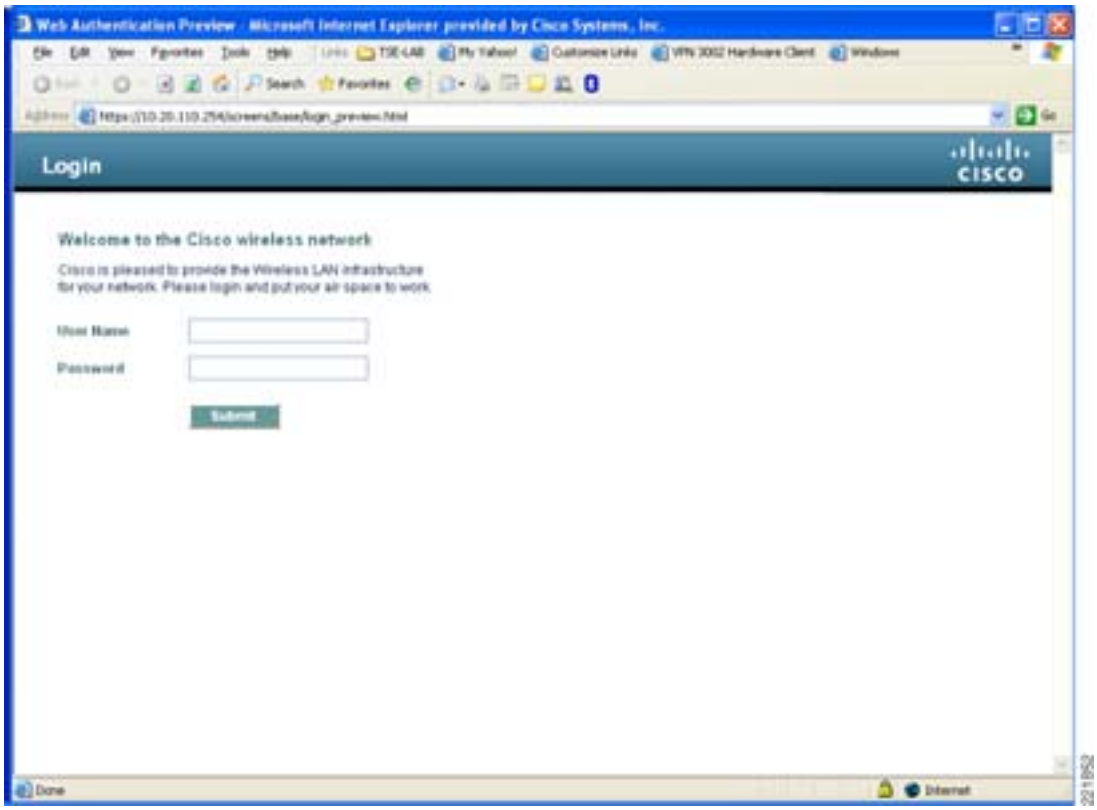
- 所定の外部コントローラの負荷は、ゲスト WLAN に設定されたアンカー コントローラのリスト全体で無線クライアント接続のバランスを取ります。1 つのアンカーを、1 つ以上のセカンダリ アンカーを持つプライマリ アンカーとして指定する方法は、現在のところありません。
- 到達できなくなっているアンカー WLC にアソシエートされた無線クライアントは、WLAN 用に定義された別のアンカーに再びアソシエートされます。これが発生し、Web 認証が使用されている場合には、クライアントは Web ポータル認証ページにリダイレクトされ、資格情報の再送信を要求されます。

（注） Cisco Unified Wireless Network でマルチキャストが有効でも、ゲスト トンネルではマルチキャスト トラフィックはサポートされません。

Web ポータル認証

Cisco Centralized Guest Access ソリューションは、組み込み型の Web ポータルを備えています。このポータルは、認証用のゲスト資格情報を要求するのに使用され、免責条項または利用規定の表示機能と単純なブランディング機能を備えています（図 10-5 を参照）。

図 10-5　コントローラの Web 認証ページ



Web ポータル ページは、すべての Cisco WLAN Controller プラットフォーム上で使用でき、WLAN がレイヤ 3 Web ポリシーベースの認証用に設定された場合にデフォルトで呼び出されます。

よりカスタマイズされたページが必要な場合は、管理者が、カスタマイズされたページをインポートしてローカルに保存するオプションが用意されています。また、会社で外部 Web サーバを使用する場合は、内部サーバを使用せずに外部サーバにリダイレクトするようにコントローラを設定できます。Web ページの設定に関するガイドラインについては、ゲスト アクセスの設定（P. 10-15）を参照してください。

ユーザ リダイレクション

たいていの Web ベースの認証システムでは一般的なことですが、ゲスト クライアントを WLC の Web 認証ページにリダイレクトする場合は、ゲスト クライアントが Web ブラウザ セッションを起動して、対象 URL を開く必要があります。リダイレクションが正常に動作するには、次の条件を満たす必要があります。

- DNS 解決：ゲスト アクセス トポロジでは、有効な DNS サーバが DHCP 経由で割り当てられ、認証前のユーザからその DNS サーバへアクセスできるようにする必要があります。クライアントが認証で Web ポリシー WLAN にアソシエートすると、DHCP と DNS を除くすべてのトラフィックがブロックされます。そのため、DNS サーバは、アンカー コントローラから到達可能にする必要があります。トポロジによっては、DNS を許可するためにファイアウォールを通してコンジットを開く必要がある場合と、インターネット境界ルータ上の ACL を変更する必要がある場合があります。

（注） 静的 DNS 設定のクライアントは、設定された DNS サーバがゲスト ネットワークからアクセスできるかどうかによって、機能しない場合があります。

- 解決可能なホームページ URL：ゲスト ユーザのホームページ URL は、DNS によってグローバルに解決可能である必要があります。たとえば、ユーザのホームページが、会社のイントラネットの外側では解決できない社内用ホームページである場合、そのユーザはリダイレクトされません。この場合、ユーザは www.yahoo.com や www.google.com などの一般サイトへの URL を開く必要があります。
- HTTP ポート 80：ユーザのホームページは解決可能ですが、HTTP ポート 80 以外のポート上にある Web サーバに接続された場合、ユーザはリダイレクトされません。また、ユーザが WLC の Web 認証ページにリダイレクトされるには、ポート 80 を使用する URL を開く必要があります。

（注） ポート 80 に加え、コントローラがリダイレクションを監視できるように、追加ポート番号を 1 つ設定するオプションは次のとおりです（この設定は、コントローラの CLI を通してのみ使用可能）。<*controller_name*> config> **network web-auth-port** <*port*>

ゲスト資格情報の管理

ゲスト資格情報は、リリース 4.0 以降の WCS を使用して、一元的に作成および管理できます。ネットワーク管理者は、WCS 内に限定的な特権アカウントを作成し、ゲスト資格情報を作成する目的の Lobby Ambassador アクセスを許可します。このようなアカウントでは、Lobby Ambassador に許可されている機能は、ゲスト資格情報を作成して、Web ポリシーが WLAN に設定されたコントローラに割り当てることだけです。設定に関するガイドラインについては、ゲスト アクセスの設定（P. 10-15）を参照してください。

WCS 内の多くの設定タスクと同様に、ゲスト資格情報はテンプレートを使用して作成されます。リリース 4.1 からは、次の新しいゲスト ユーザ テンプレートのオプションおよび機能が導入されました。

- ゲスト テンプレートには、2 種類あります。1 つは、有効期間を制限するかまたは無制限にした、即時のゲスト アクセスをスケジューリングするためのゲスト テンプレートです。もう 1 つは、管理者が「将来の」ゲスト アクセスをスケジューリングして、曜日と時間帯によるアクセス制限を提供します。
- このソリューションにより、管理者はゲスト ユーザに資格情報を E メールで送信できるようになります。さらに、「スケジュール」ゲスト テンプレートが使用されると、アクセスが提供される新しい日（間隔）ごとに、資格情報が自動的に E メールで送信されます。
- （ゲスト）WLAN SSID および WCS のマッピング情報（キャンパス / ビルディング / フロアの場所）に基づくか、または WLAN SSID および特定のコントローラまたはコントローラのリストに基づいて、ゲスト資格情報を WLC に適用できます。後者の方法は、この章で説明するように、ゲスト モビリティ アンカー方式でゲスト アクセスを展開する場合に使用されます。

詳細は、WCS を使用したゲスト管理（P. 10-31）を参照してください。

Lobby Ambassador がゲスト テンプレートを作成すると、ゲスト アクセス トポロジに応じて 1 つ以上のコントローラに適用されます。WLAN が 「*Web*」*ポリシーで設定した WLAN* だけが、適用可能なテンプレートの候補コントローラとして一覧表示されます。これは、ゲスト テンプレートを WCS マップ ロケーションの基準に基づいてコントローラに適用する場合にも当てはまります。

適用されたゲスト資格情報は、（アンカー）WLC 上にローカルに保存され（Security > Local Net Users）、ゲスト テンプレートで定義された「ライフタイム」変数の期限までそこで保持されます。資格情報の有効期限が切れている場合でも、無線ゲストがアソシエートされアクティブな場合は、WLC がトラフィック転送を停止してそのユーザの WEBAUTH_REQD ポリシー状態に戻ります。ゲスト資格情報が（コントローラに）再適用されない場合、そのユーザは二度とネットワークにアクセスすることができません。

（注） ゲスト資格情報に関連付けられたライフタイム変数は、WLAN セッション タイムアウト変数とは無関係です。WLAN セッション タイムアウトの時間を過ぎてもユーザが接続したままの場合は、認証が解除されます。その後、ユーザは、Web ポータルにリダイレクトされ、資格情報の有効期限が切れていない場合には、再度アクセスするためにログインをやり直す必要があります。面倒な認証のリダイレクトを避けるには、ゲスト WLAN セッション タイムアウト変数を適切に設定する必要があります。

ローカル コントローラの Lobby 管理者のアクセス

中央集中型 WCS 管理システムが展開されていないか使用できない場合、ネットワーク管理者は、Lobby 管理者の特権だけを付与したローカル管理者のアカウントをアンカー コントローラ上に設定できます。Lobby 管理者のアカウントを使用してコントローラにログインしたユーザは、ゲスト ユーザ管理機能にアクセスできます。ローカル ゲスト管理で使用可能な設定オプションは、WCS を通して使用可能な機能とは対照的に、限られています。次のオプションが含まれます。

- ユーザ名
- 生成パスワード（チェックボックス）
- 管理者割り当てパスワード
- 確認パスワード
- 有効期間：日 : 時 : 分
- SSID（チェックボックス）
- レイヤ 3 Web ポリシー認証用に設定された WLAN だけを表示
- 説明

WCS によってコントローラに適用された資格情報は、管理者がコントローラにログインしたときに表示されます。ローカルの Lobby 管理者のアカウントには、WCS によって以前に作成されたゲスト資格情報を変更または削除する特権が与えられます。WLC 上でローカルに作成されるゲスト資格情報は、コントローラの設定が WCS で更新されない限り、WCS に自動的に表示されません。WLC 設定の更新の結果として WCS にインポートされる、ローカルに作成されるゲスト資格情報は、編集して WLC に再適用できる、新しいゲスト テンプレートとして表示されます。

ゲスト ユーザの認証

ゲスト資格情報の管理（P. 10-10）で説明したように、管理者が WCS またはコントローラ上でローカルのアカウントを使用してゲスト ユーザ資格情報を作成した場合は、それらの資格情報は、コントローラ上でローカルに保存されます。そのコントローラは、中央集中型ゲスト アクセス トポロジの場合に、アンカー コントローラとなります。

無線ゲストが Web ポータルを通してログインした場合、コントローラは次の順番で認証を処理します。

1. コントローラが、ユーザ名とパスワードをローカル データベースでチェックし、そこに存在すれば、アクセスを許可します。

ユーザ資格情報が見つからなかった場合は、次のように処理されます。

2. コントローラが、外部 RADIUS サーバがゲスト WLAN 用に設定されているかどうかチェックします（WLAN 構成設定の下）。設定例については、外部 RADIUS 認証（P. 10-51）を参照してください。そのように設定されている場合は、コントローラが、そのユーザ名とパスワードで RADIUS アクセス要求パケットを作成し、選択された RADIUS サーバに転送して認証します。

特定の RADIUS サーバがゲスト WLAN 用に設定されていない場合は、次のように処理されます。

3. コントローラが、グローバルな RADIUS サーバの設定をチェックします。「ネットワーク」ユーザを認証するように設定されたすべての外部 RADIUS サーバは、ゲスト ユーザ資格情報を使用して照会されます。設定例については、外部 RADIUS 認証（P. 10-51）を参照してください。それ以外では、どの RADIUS サーバでも「ネットワーク ユーザ」がオンになっておらず、また上記 1 または 2 でユーザが認証されていない場合、認証は失敗します。

（注） RADIUS サーバは、WLC Security > AAA > RADIUS 設定でネットワーク ユーザのチェックボックスがオフになっている場合でも、ネットワーク ユーザ認証をサポートするために使用できます。ただし、これを実現するには、サーバが特定の WLAN の Security > AAA Servers 設定で明示的に選択されている必要があります。設定例については、外部 RADIUS 認証（P. 10-51）を参照してください。

外部認証

WLC および WCS のゲスト アカウント管理（Lobby Ambassador）機能は、WLC 上のローカル認証用にゲスト ユーザ資格情報を作成して適用するためだけに使用できます。ただし、既存のゲスト管理 / 認証ソリューションが、有線ゲスト アクセスまたは NAC ソリューションの一部として、すでに企業に展開されている場合があります。その場合は、ゲスト ユーザの認証（P. 10-11）で説明したように、Web ポータル認証を外部 RADIUS サーバに転送するようにアンカー コントローラ / ゲスト WLAN を設定できます。

コントローラが Web ユーザを認証するために使用するデフォルトのプロトコルは、Password Authentication Protocol（PAP; パスワード認証プロトコル）です。外部 AAA サーバに対して Web ユーザを認証している場合は、そのサーバがサポートしているプロトコルを確認する必要があります。また、Web 認証に CHAP または MD5-CHAP を使用するようにアンカー コントローラを設定できます。Web 認証プロトコル タイプは、WLC のコントローラ設定で設定されます。

Cisco Secure ACS と Microsoft ユーザ データベースを使用した外部認証

ゲスト アクセスの展開で、ゲスト ユーザの認証に Cisco ACS と Microsoft ユーザ データベースの使用を検討している場合は、次の Cisco ACS 設定に関する注意事項を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html

特に、次の URL を参照してください。
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html#wp1041223

ゲスト パススルー

無線ゲスト アクセスのもう 1 つの形態は、ユーザ認証をすべて省略して、オープン アクセスを可能にすることです。ただし、企業は、アクセスを許可する前に利用規定または免責条項のページをユーザに表示することが必要になる場合があります。そのような場合は、Web ポリシーをパススルーするようにゲスト WLAN を設定できます。このシナリオでは、ゲスト ユーザが、免責情報を含むポータル ページにリダイレクトされます。また、パススルー モードには、ユーザが接続する前に E メール アドレスを入力するオプションもあります（サンプル ページについては、図 10-6 および図 10-7 を参照）。設定例については、ゲスト アクセスの設定（P. 10-15）を参照してください。

図 10-6　Welcome AUP ページのパススルー

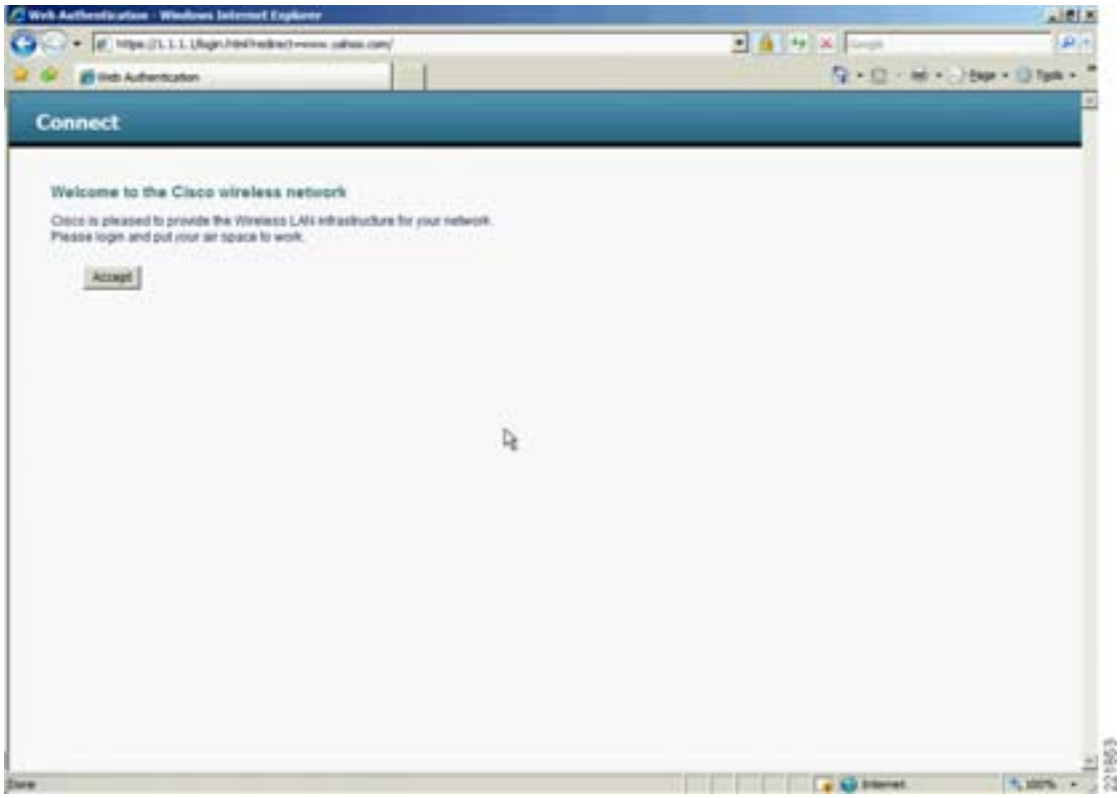
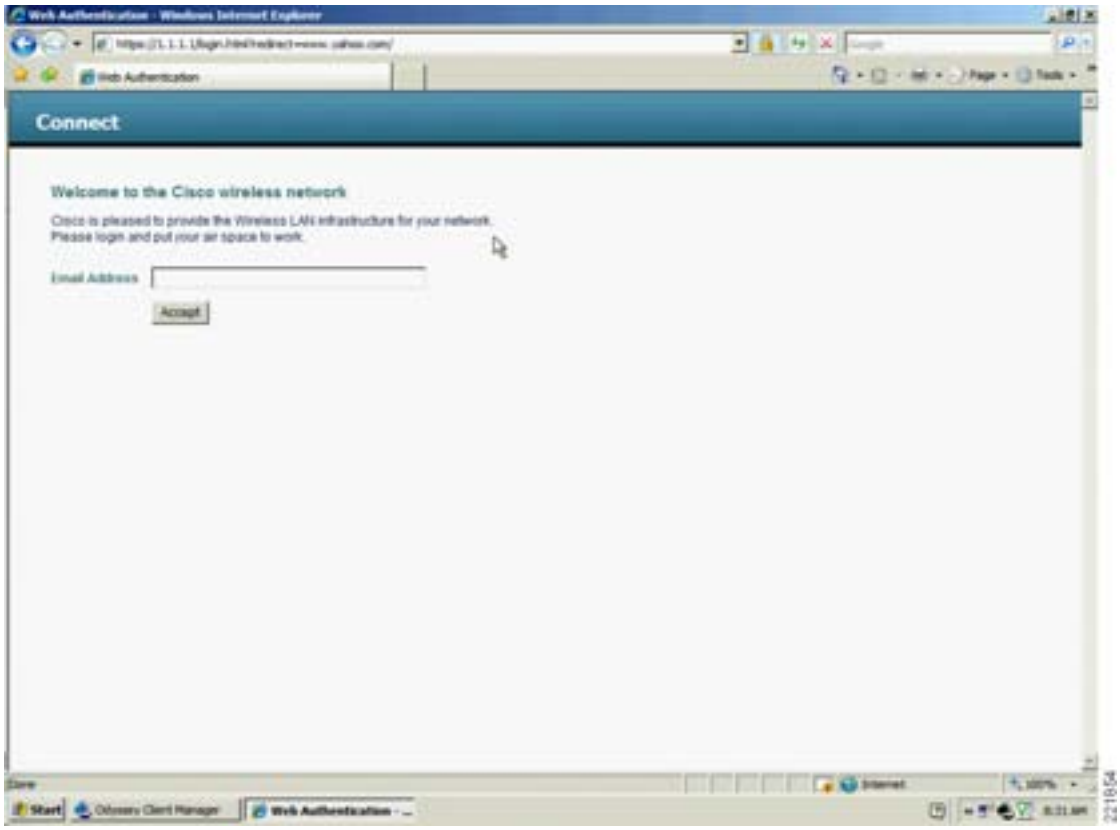


図 10-7　E メールを含むページのパススルー



ゲスト アクセスの設定

この項では、Cisco Unified Wireless ソリューション内で無線ゲスト アクセス サービスを有効にする方法について説明します。設定作業では、Web ブラウザの Windows IE6（限定）を使用する必要があります。コントローラとの Web セッションは、次のコントローラの管理 IP アドレスへの HTTPS セッションを開くことによって、確立されます。**https://** *管理 IP* またはオプションでコントローラのサービス ポート IP アドレス。

次の手順では、アンカー WLC を除き、コントローラと LAP のインフラストラクチャがすでに展開されているものとします。詳細は、アンカー コントローラ展開ガイドライン（P. 10-6）を参照してください。

（注） この項で説明する設定手順は、記載された順序に従って実行することをお勧めします。

設定セクション全体を通じて、次の用語が使用されます。

- 外部 WLC：企業のキャンパス全体またはブランチ ロケーションに展開され、LAP のグループの管理および制御に使用される 1 つ以上の WLC を指します。外部コントローラが、ゲスト WLAN をゲスト モビリティ EoIP トンネルにマップします。
- アンカー WLC：企業 DMZ 内に展開され、ゲスト モビリティ EoIP トンネル終端、Web リダイレクション、およびユーザ認証を実行するために使用される 1 つ以上の WLC を指します。

（注） この項では、特定の設定画面キャプチャの関連する部分だけを示します。

Cisco Unified Wireless Guest Access ソリューションの実装は、次の設定カテゴリに分類できます。

1. アンカー WLC の設置およびインターフェイス設定：ここでは、1 つ以上のアンカー WLC の実装に関する設置の要件、手順、および注意点について簡単に説明します。既存の Unified Wireless 展開にゲスト アクセスを初めて実装する場合、アンカー WLC は通常、企業ネットワークのインターネット エッジに設置される新しいプラットフォームです。
2. モビリティ グループの設定：ここでは、外部 WLC が、1 つ以上のゲスト アンカー WLC への EoIP トンネルの起点となるように設定する必要があるパラメータについて説明します。モビリティ グループの設定自体で EoIP トンネルが作成されるわけではなく、ゲスト アクセス WLAN サービスをサポートするために、外部 WLC とアンカー WLC 間のピア関係が確立されます。
3. ゲスト WLAN の設定：ゲスト WLAN（外部 WLC を起点とする）をアンカー WLC にマップするのに必要な WLAN 固有の設定パラメータに焦点を当てます。ゲスト アクセス ソリューションの設定のこの部分において、外部 WLC とアンカー WLC 間に EoIP トンネルが作成されます。この項では、Web ベースの認証のレイヤ 3 リダイレクションを起動するために必要な設定についても説明します。
4. ゲスト アカウント管理：ここでは、WCS または アンカー WLC の Lobby 管理者インターフェイスを使用して、アンカー WLC でローカルにゲスト ユーザ資格情報を設定および適用する方法の概要について説明します。
5. その他の機能とソリューション オプション：次のような、設定が可能なその他の機能について説明します。
   a. Web ポータル ページの設定と管理
   b. 外部 Web リダイレクションのサポート
   c. 事前認証 ACL

d. アンカー WLC DHCP の設定
e. 外部 RADIUS 認証
f. 外部アクセス コントロール

アンカー WLC の設置およびインターフェイスの設定

アンカー コントローラの位置決め（P. 10-6）で説明したように、アンカー WLC は、ゲスト アクセスだけに使用して、社内の LAP の制御および管理には使用しないことをお勧めします。

この項では、アンカー WLC 上のインターフェイス設定のすべてを扱っているわけではありません。読者は、初期ブート時に必要な、シリアル コンソール インターフェイスを使用した WLC の初期化と設定プロセスに精通していることを前提とします。そうでない場合は、次の URL を参照してください。
http://www.cisco.com/en/US/partner/docs/wireless/controller/4400/quick/guide/ctrlv32.html

この項では、ゲスト アクセス トポロジ内にアンカーとして展開する WLC 上でのインターフェイスの設定に関する情報と注意事項を記載します。

シリアル コンソール インターフェイスを使用した初期設定の一環として、次の 3 つの静的インターフェイスを定義する必要があります。

- コントローラ管理：このインターフェイス /IP は、ネットワーク上の他のコントローラとの通信に使用されます。また、外部コントローラを起点とする EoIP トンネルの終端にも使用されるインターフェイスです。
- AP マネージャ インターフェイス：AP 管理にコントローラを使用しない場合でも、このインターフェイスは設定する必要があります。シスコでは、管理インターフェイスと同じ VLAN およびサブネット上に、AP マネージャ インターフェイスを設定することをお勧めします。
- 仮想インターフェイス：コントローラのクイックスタート　インストール　マニュアルでは、1.1.1.1 などのアドレスの仮想 IP を定義するように推奨されています。このアドレスは、同じモビリティ グループのメンバであるすべてのコントローラで同じアドレスにする必要があります。また、仮想インターフェイスは、コントローラがクライアントを Web 認証のためにリダイレクトするときのソース IP アドレスとしても使用されます。

ゲスト VLAN インターフェイスの設定

前述したインターフェイスは、コントローラに関連付けられた動作と管理機能に使用されます。ゲスト アクセス サービスを実装するには、もう 1 つのインターフェイスを定義する必要があります。これは、ゲスト トラフィックをインターネットにルーティングするためのインターフェイスです。アンカー コントローラの位置決め（P. 10-6）で説明したように、ゲスト インターフェイスは、ファイアウォール上のポートに接続される場合と、インターネット境界ルータ上のインターフェイスに切り替えられる場合があります。

新しいインターフェイスの定義

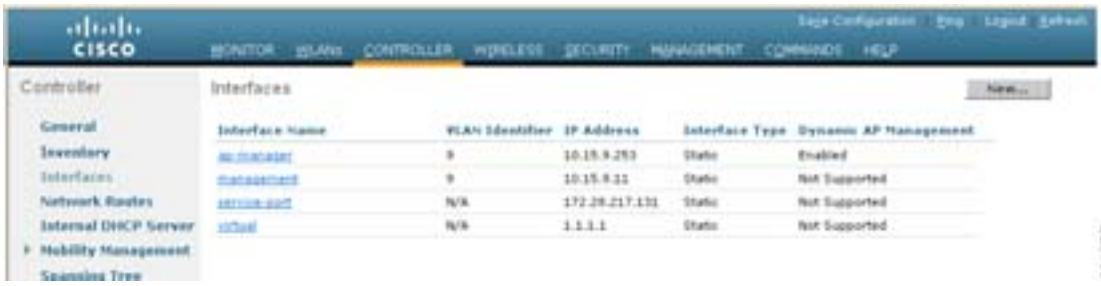
次の手順を実行して、ゲスト トラフィックをサポートするインターフェイスを定義および設定します。

ステップ 1　**Controllers** タブをクリックします。

ステップ 2　左側のペインで、**Interfaces** をクリックします。

ステップ 3　New をクリックします（図 10-8 を参照）。

図 10-8　Controller インターフェイス



インターフェイス名と VLAN ID の定義

ステップ 4　インターフェイス名と VLAN ID を入力します（図 10-9 を参照）。

図 10-9　インターフェイス名と VLAN ID

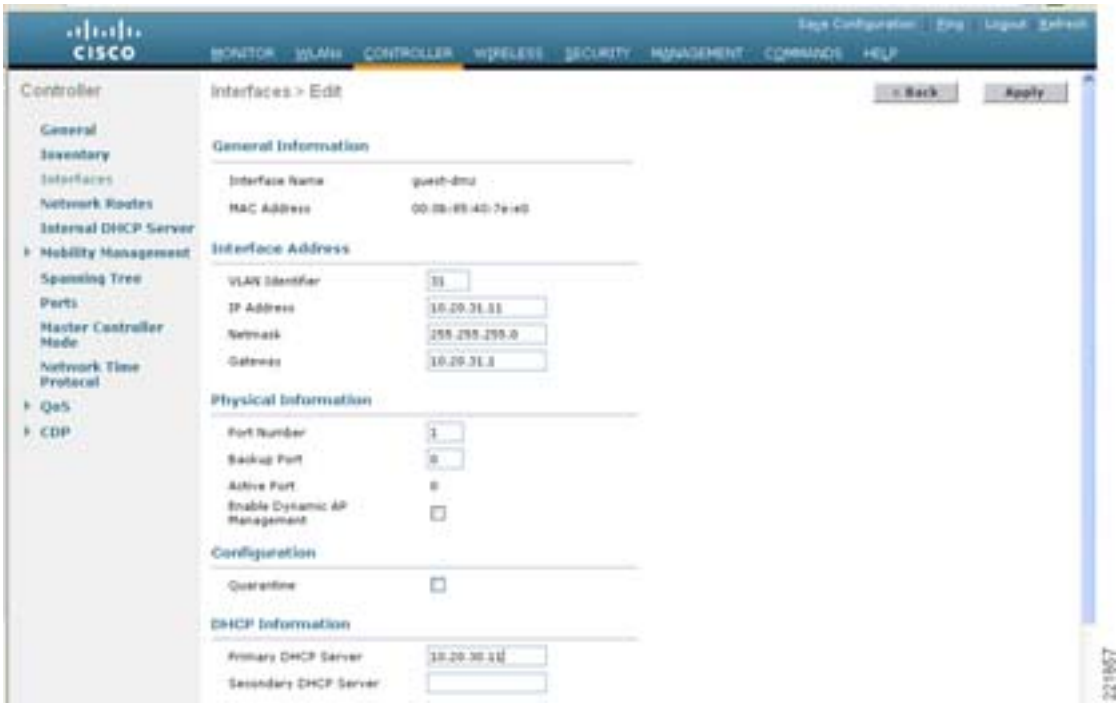
インターフェイス プロパティの定義

ステップ 5　次のプロパティを定義します。

- インターフェイス IP
- マスク
- ゲートウェイ（アンカー コントローラに接続されたファイアウォールまたはネクスト ホップ ルータの場合）
- DHCP サーバ IP（外部 DHCP サーバを使用している場合は、Primary DHCP Server フィールドのそのサーバの IP アドレスを使用します）

  図 10-10 を参照してください。

図 10-10　インターフェイス プロパティの定義



(注)　DHCP サービスをアンカー コントローラ上でローカルに実装する必要がある場合は、Primary DHCP Server フィールドにコントローラの管理 IP アドレスを入力します。アンカー WLC の設置およびインターフェイスの設定（P. 10-16）を参照してください。
ゲスト N+1 冗長性が DMZ に実装されている場合、展開されている追加のアンカー WLC ごとに、上記のインターフェイス設定を繰り返します。

モビリティ グループの設定

次のデフォルトのモビリティ グループ パラメータは、標準の中央集中型 WLAN 展開の一部として、外部 WLC に定義しておく必要があります。ゲスト アクセスの自動アンカー モビリティをサポートするには、モビリティ グループ ドメイン名でアンカー WLC も設定する必要があります。

アンカー WLC のデフォルト モビリティ ドメイン名の定義

アンカー WLC のデフォルト モビリティ ドメイン名を設定します。アンカーのモビリティ ドメイン名は、外部 WLC に設定した名前と異なる必要があります。以下の例では、企業の無線展開にアソシエートされている WLC（外部コントローラ）は、すべてモビリティ グループ「SRND」のメンバです。一方、ゲスト アンカー WLC は、別のモビリティ グループ名「ANC」で設定されます。これは、企業の無線展開にアソシエートされているプライマリ モビリティ ドメインから、アンカー WLC を論理的に区別しておくために行われます。

ステップ 1　Controllers タブをクリックします。

ステップ 2　Default Mobility Domain Name フィールドに名前を入力します。

ステップ 3　**Apply** をクリックします（図 10-11 を参照）。

図 10-11　アンカー WLC 上のデフォルト モビリティ ドメイン名の定義

アンカー WLC のモビリティ グループ メンバの定義

ゲスト WLAN をサポートする企業での展開内のすべての外部 WLC は、ゲスト アンカー WLC のモビリティ グループ メンバとして定義する必要があります。

ステップ 1　**Controllers** タブをクリックします。

ステップ 2　左側のペインで、**Mobility Management** をクリックし、**Mobility Groups** をクリックします（図 10-12 を参照）。

図 10-12　モビリティグループメンバの定義

モビリティ グループ メンバとして外部コントローラを追加

ステップ 3　New をクリックして、ゲスト アクセス WLAN をサポートする各外部コントローラの MAC と IP アドレスを定義します（図 10-13 を参照）。

図 10-13　アンカー WLC への外部コントローラの追加

（注）　上に示した 図 10-13 の「Group Name」は、外部 WLC の「Default Mobility Domain Name」で設定される名前です。これは、アンカー WLC に使用される名前と異なる必要があります。メンバの IP アドレスと MAC アドレスは、外部 WLC の管理インターフェイスにアソシエートされたアドレスです。ゲスト WLAN をサポートする追加の各外部 WLC に対して、上記の手順を繰り返します。複数のアンカーが展開されている場合（ゲスト N+1 冗長性）、アンカー WLC のデフォルト モビリティ ドメイン名の定義（P. 10-18）と アンカー WLC のモビリティ グループ メンバの定義（P. 10-19）の手順を繰り返します。

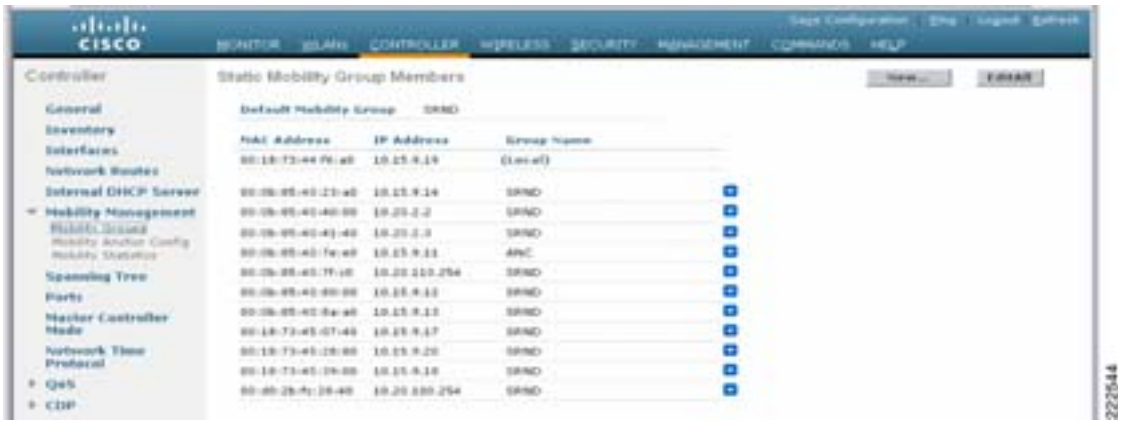
外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加

無線ゲスト アクセスをサポートする自動アンカー モビリティ（P. 10-4）で説明したように、各外部 WLC は、アンカー WLC 上で終端する EoIP トンネルにゲスト WLAN をマップします。そのため、アンカー WLC は、各外部コントローラのモビリティ グループのメンバとして定義する必要があります。下の例で、アンカー WLC のグループ名エントリが「ANC」で（アンカー WLC のモビリティ グループ メンバの定義（P. 10-19）を参照）、企業の無線展開を構成しているもう一方の WLC がモビリティ グループ「SRND」のメンバであることに注意してください。

ステップ 1　New をクリックして、アンカー WLC の IP、MAC アドレス、およびグループ名をモビリティ メンバ テーブルに追加します。

ステップ 2　追加の外部コントローラごとにこの手順を繰り返します（図 10-14 を参照）。

図 10-14　外部 WLC へのアンカー コントローラの追加



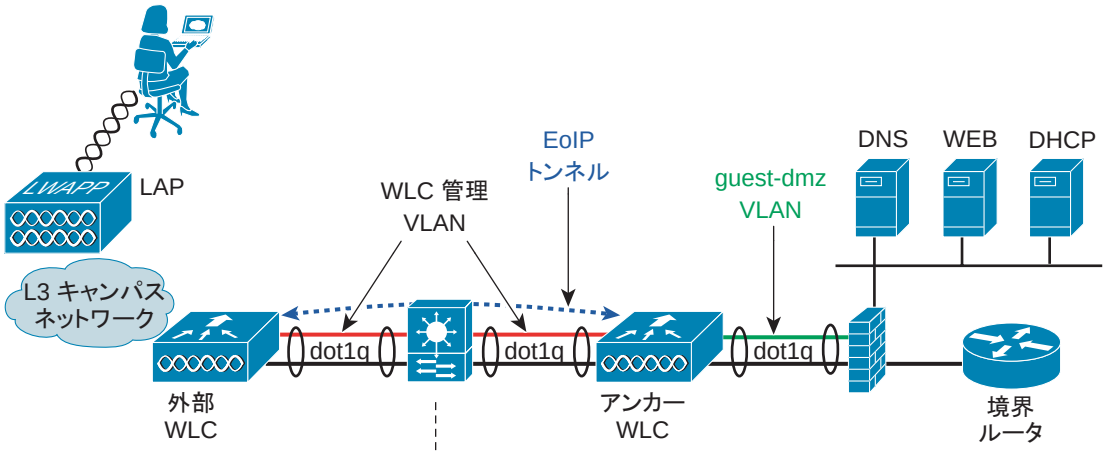
(注)　ゲスト N+1 冗長性機能が展開されている場合、2 つ以上のアンカー WLC エントリが各外部 WLC のモビリティ グループ メンバ リストに追加されます。

ゲスト WLAN の設定

次の項では、単一のゲスト WLAN の設定方法について説明します。ゲスト WLAN は、ゲスト アクセスが必要な AP を管理するすべての外部 WLC 上で設定します。アンカー WLC が明らかにゲスト WLAN にアソシエートされた LAP の管理に使用されない場合でも、アンカー WLC は、ゲスト WLAN を使用して設定する必要があります。なぜならば、アンカー WLC は、WLAN の論理拡張機能で、そこでユーザ トラフィックがアンカー WLC 上のインターフェイス /VLAN に最終的にブリッジされるためです（AP と外部コントローラ間では LWAPP、外部コントローラとアンカー コントローラ間では EoIP を使用）。

(注)　WLAN Security、QoS、および Advanced 設定タブで定義する *すべてのパラメータは、アンカーおよび外部 WLC の両方で同じ設定にする必要がある*ことに注意することが非常に重要です。図 10-15 は、以下で説明する WLAN 設定の概略図を示しています。

図 10-15　WLAN の設定



外部 WLC WLAN サマリー
SSID = Guest
WLAN ステータス = 有効
無線のポリシー = 802.11b/g のみ
インターフェイス = 管理
ブロードキャスト SSID = 有効
レイヤ 2 セキュリティ = なし
レイヤ 3 セキュリティ = なし + Web + 認証
AAA サーバ = なし
QOS = Bronze (Background)
WMM = 無効
高度 = デフォルト + DHCP 必須

モビリティ設定
デフォルト モビリティ グループ名 = SRND
静的モビリティ メンバ:
00:0b:85:40:7e:e0　10.15.9.11　ANC

アンカー WLC WLAN サマリー
SSID = Guest
WLAN ステータス = 有効
無線のポリシー = 802.11b/g のみ
インターフェイス = guest-dmz
ブロードキャスト SSID = 有効
レイヤ 2 セキュリティ = なし
レイヤ 3 セキュリティ = なし + Web + 認証
AAA サーバ = なし
QOS = Bronze (Background)
WMM = 無効
高度 = デフォルト + DHCP 必須

モビリティ設定
デフォルト モビリティ グループ名 = ANC
静的モビリティ メンバ:
00:18:73:44:f6:a0　10.15.9.19　SRND

（注） WLAN Security、QoS、および Advanced 設定タブで定義するパラメータは、*アンカーおよび外部コントローラの両方で同じ設定にする必要があります。*

外部 WLC：ゲスト WLAN の設定

ステップ 1　**WLANs** タブをクリックして、**New** をクリックします（図 10-16 を参照）。

図 10-16　ゲスト WLAN の設定

ゲスト WLAN SSID の定義

ステップ 2　将来のゲスト ユーザが、直感的に理解できるか、または認識しやすい SSID を定義します。

コントローラで自動的に VLAN ID を割り当てます。管理者は、他の SSID/WLAN で使用されていなければ、1 ～ 16 の ID を選択できます。

ステップ 3　プロファイル名の定義

ステップ 4　**Apply** をクリックします（図 10-17 を参照）。

図 10-17　ゲスト WLAN SSID の定義

新しい WLAN の作成後に、図 10-18 に示すように、設定ページが表示されます。

図 10-18　WLAN の設定ページ

(注)　ゲスト WLAN のために外部 WLC によって使用されるインターフェイスは、「管理」インターフェイスです。外部 WLC がアンカー WLC への EoIP トンネルを確立するためには、管理インターフェイスを選択する必要があります。上に示した 図 10-15 では、ファイアウォールにスイッチされるローカルの動的なインターフェイスに WLAN が、アンカー WLC によってマップされることに注意してください。

ゲスト WLAN のパラメータおよびポリシーの定義

General Configuration タブで、次の手順を実行します。

ステップ 1　WLAN Status の隣のボックスをクリックして WLAN を有効にします。

ステップ 2　ゲスト アクセスをサポートする帯域を制限する場合は、必要に応じて、無線ポリシーを設定します。

a. ブロードキャスト SSID はデフォルトで有効になるので、有効なままにします。

b. デフォルトでは、WLAN は WLC の「管理」インターフェイスに割り当てられます。これを変更しないでください。

(注)　インターフェイス名は、管理インターフェイスに設定する必要があります。これにより、外部コントローラがその管理 IP を介して EoIP トンネルの起点となります。

ステップ 3　**Security** タブをクリックします（図 10-19 を参照）。

図 10-19　ゲスト WLAN の一般ポリシーの定義

ステップ 4　レイヤ 2 セキュリティを、デフォルトの設定（802.1x WPA/WPA2）から **none** に設定します（図 10-20 を参照）。

図 10-20　WLAN レイヤ 2 のセキュリティ設定

ステップ 5　**Layer 3** タブをクリックします（図 10-21 を参照）。

図 10-21　ゲスト WLAN のレイヤ 3 セキュリティ設定

ステップ 6　**Web Policy** チェックボックスをオンにします（追加オプションのリストが表示されます）。

WLC が認証前にクライアント間で DNS トラフィックを受け渡しすることを示す、警告のダイアログ ボックスが表示されます。

ステップ 7　Web ポリシーに **Authentication** または **Pass-through** を選択します（ゲスト ユーザの認証（P. 10-11）を参照）。

（注）　事前認証 ACL は、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続することを許可する ACL を適用するために使用できます。ACL は、Security > Access Control Lists で設定されます。事前認証 ACL が Web 認証ポリシーと共に使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト /URL に解決して接続することができなくなります。

ステップ 8　**QoS** タブを選択します（図 10-22 を参照）。

図 10-22　ゲスト WLAN QoS の設定

ステップ 9　必要に応じて、ゲスト WLAN にアップストリーム QoS プロファイルを設定します。デフォルトは「Silver (Best Effort)」です。この例では、ゲスト WLAN は最低の QoS クラスに再割当されています。

ステップ 10　**Advanced** タブをクリックします（図 10-23 を参照）。

図 10-23　ゲスト WLAN の高度な設定

ステップ 11　セッション タイムアウトを設定します（オプション）。

（注）　セッション タイムアウト が 0（デフォルト）より大きくなると、有効期限後に強制的に認証が解除され、ユーザは Web ポータルで再認証を要求されます。

ステップ 12　DHCP Addr. Assignment を「Required」に設定します。

（注）　ゲスト ユーザが、静的 IP 設定を使用してゲスト ネットワークの使用を試みるのを防ぐため、DHCP Addr. Assignment を「Required」に設定することをお勧めします。

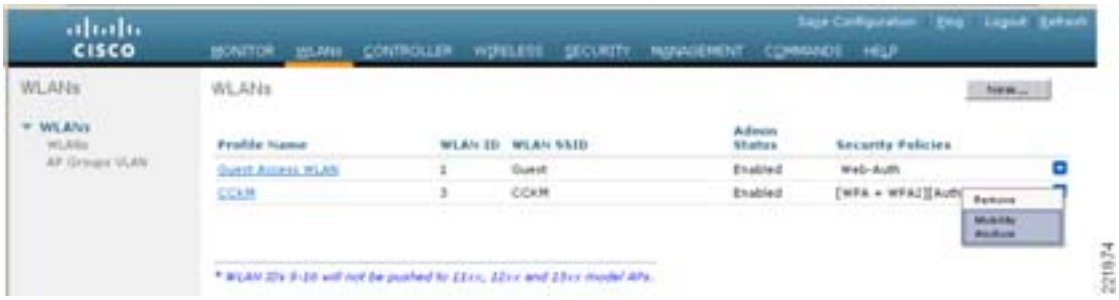
ステップ 13　最後に、**Apply** をクリックします。

ゲスト WLAN モビリティ アンカーの設定

ステップ 1　外部 WLC 上の WLAN メニューから、新しく作成されたゲスト WLAN を探します。

ステップ 2　右側のプルダウン選択リストから **Mobility Anchors** を強調表示してクリックします（図 10-24 を参照）。

図 10-24　WLAN モビリティ アンカー



ステップ 3　Switch IP Address (Anchor) プルダウン選択リストで、ネットワーク DMZ 内で展開されたアンカー WLC の管理インターフェイスに対応する IP アドレスを選択します。これは、外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加（P. 10-20）で設定されたものと同じ IP アドレスです。

ステップ 4　**Mobility Anchor Create** をクリックします（図 10-26 を参照）。

図 10-25　Switch IP Address (Anchor) からの管理インターフェイスの選択

図 10-26　WLAN モビリティ アンカーの選択

ゲスト WLAN モビリティ アンカーの確認

設定されると、図 10-27 に示す画面には、ゲスト WLAN に割り当てられたモビリティ アンカー（上記で選択）が表示されます。

図 10-27　ゲスト WLAN モビリティ アンカーの確認

確認作業を容易にするために、ページには、モビリティ トンネル データ パスと LWAPP 制御パスがアンカーで設定されているかどうかが表示されます。両方または片方が「down」と表示されている場合には、ゲスト アクセスのトラブルシューティング（P. 10-56）でトラブルシューティングのヒントを参照してください。右側のプルダウン選択リストには、宛先アンカー WLC に ping を送信するオプションがあります。

ステップ 5　終了する場合は、**Back** をクリックします。

ステップ 6　展開されている追加の各アンカー WLC （ゲスト N+1 冗長性）に対して、上記の手順を繰り返します。

これで、ゲスト WLAN の設定は終了です。ゲスト WLAN をサポートする追加の各外部 WLC に対して、外部 WLC：ゲスト WLAN の設定（P. 10-22）から ゲスト WLAN モビリティ アンカーの確認（P. 10-28）のすべての手順を繰り返します。

アンカー WLC 上でのゲスト WLAN の設定

アンカー コントローラ上でのゲスト WLAN の設定は、WLAN インターフェイスおよびモビリティ アンカー設定（以下で詳細を説明）で多少の違いがある点を除き、外部コントローラの設定と同じです。

（注） ゲスト WLAN に定義する SSID は、外部 WLC 上で定義される SSID とまったく同じにする必要があります。

アンカー WLC：ゲスト WLAN インターフェイス

上記のように、アンカー WLC 上でゲスト WLAN に設定するパラメータは、WLAN がマップされるインターフェイスを除いて同じです。この場合、ゲスト WLAN はアンカー WLC 上でインターフェイスまたは VLAN に割り当てられ、アンカー WLC によってファイアウォール上のインターフェイスまたはインターネット境界ルータに接続されます。

ステップ 1　**WLANs** タブをクリックします。

ステップ 2　次の点を除いて、外部 WLC 上で設定した場合と同様に、ゲスト WLAN を作成、設定、および有効化します。

WLAN の一般設定の **Interface** で、ゲスト VLAN インターフェイスの設定（P. 10-16）で作成されたインターフェイス名を選択します（図 10-28 を参照）。

ステップ 3　**Apply** をクリックします。

図 10-28　アンカー WLC ゲスト WLAN インターフェイスの設定

アンカー WLC：ゲスト WLAN モビリティ アンカーの定義

外部 WLC とは設定が異なる 2 つ目のパラメータは、WLAN モビリティ アンカー設定です。ゲスト WLAN モビリティ アンカーは、アンカー WLC 自体です。

ステップ 1　**WLANs** タブをクリックします。

ステップ 2　ゲスト WLAN を探して、**Mobility Anchors** をクリックします。

ステップ 3　プルダウン選択リストから、アンカー コントローラを表す IP アドレスを選択します。この IP アドレスの隣に（Local）と表示されています。

ステップ 4　**Mobility Anchor Create** をクリックします（図 10-29 を参照）。

図 10-29　ゲスト WLAN モビリティ アンカーの定義

ゲスト WLAN モビリティ アンカーは、*ローカル*であることに注意してください（図 10-30 を参照）。

図 10-30　ゲスト モビリティ アンカーの確認

ゲスト WLAN のモビリティ アンカーはアンカー WLC 自体なので、データとコントロール パスのステータスは常に「up」と表示されます。「up」と表示されない場合、ローカル WLC をアンカーとして Switch IP Address (Anchor) ドロップダウン メニューから選択したことを確認します。

ステップ 5　ゲスト N+1 冗長性を実装している場合、展開されている追加のアンカー WLC ごとに WLAN の設定を繰り返します。それ以外の場合、これでゲスト WLAN をアンカー WLC 上で作成するのに必要な設定手順が完了します。

ゲスト アカウント管理

- ゲスト資格情報をローカルのアンカー コントローラ上で管理する場合は、次のいずれかの方法で資格情報を作成して適用できます。
- WCS の Lobby Ambassador 管理者またはスーパー ユーザ / ルート管理者アカウントを使用する
- コントローラ上で直接、ローカルの Lobby 管理者アカウントまたは読み込み / 書き込みアクセスできるその他の管理アカウントを使用する

WCS を使用したゲスト管理

次の設定例では、WCS バージョン 4.1.83 以降がインストールおよび設定され、Lobby Ambassador のアカウントが作成されているものとします。WCS のインストールと設定の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcswst.html

ゲスト アカウントの作成については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a0080831841.html#wp1075155

(注) ゲスト テンプレートを作成する前に、個々の WLC 設定が WCS と同期していることを確認してください。

システム管理者が割り当てた Lobby Ambassador の資格情報を使用して WCS にログインします（図 10-31 を参照）。

図 10-31　WCS のログイン

ログインすると、図 10-32 に示すような画面が表示されます。

図 10-32　WCS の Lobby 管理者インターフェイス

ゲスト テンプレートには、次の 2 種類があります。

- **ゲスト ユーザの追加**テンプレートを使用すると、管理者がゲスト資格情報を作成し、ただちに 1 つ以上のアンカー WLC に適用できます。
- **ゲスト ユーザのスケジュール** テンプレートを使用すると、将来の月、日、時刻に 1 つ以上のアンカー WLC に適用されるゲスト資格情報を、管理者が作成できます（図 10-33 を参照）。

図 10-33　ゲスト ユーザ テンプレート オプション

ゲスト ユーザの追加テンプレートの使用

ステップ 1　プルダウン選択リストから、**Add Guest User** を選択して **Go** をクリックします。

ステップ 2　図 10-34 に示すようなテンプレートが表示されます。

図 10-34　ゲスト ユーザの追加テンプレート

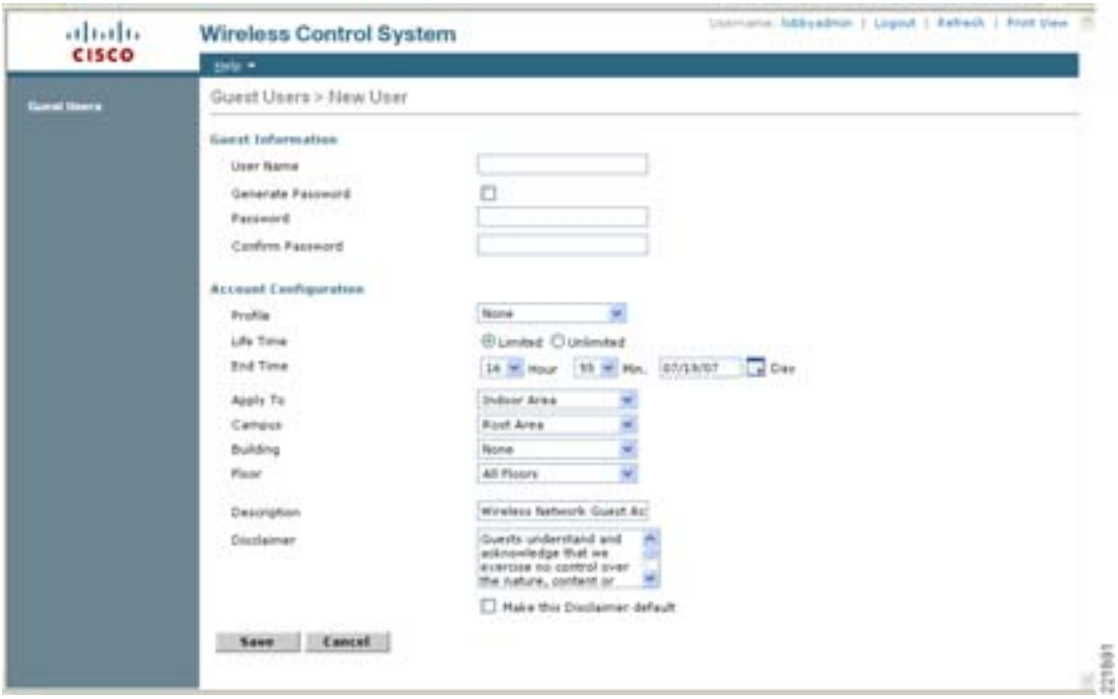
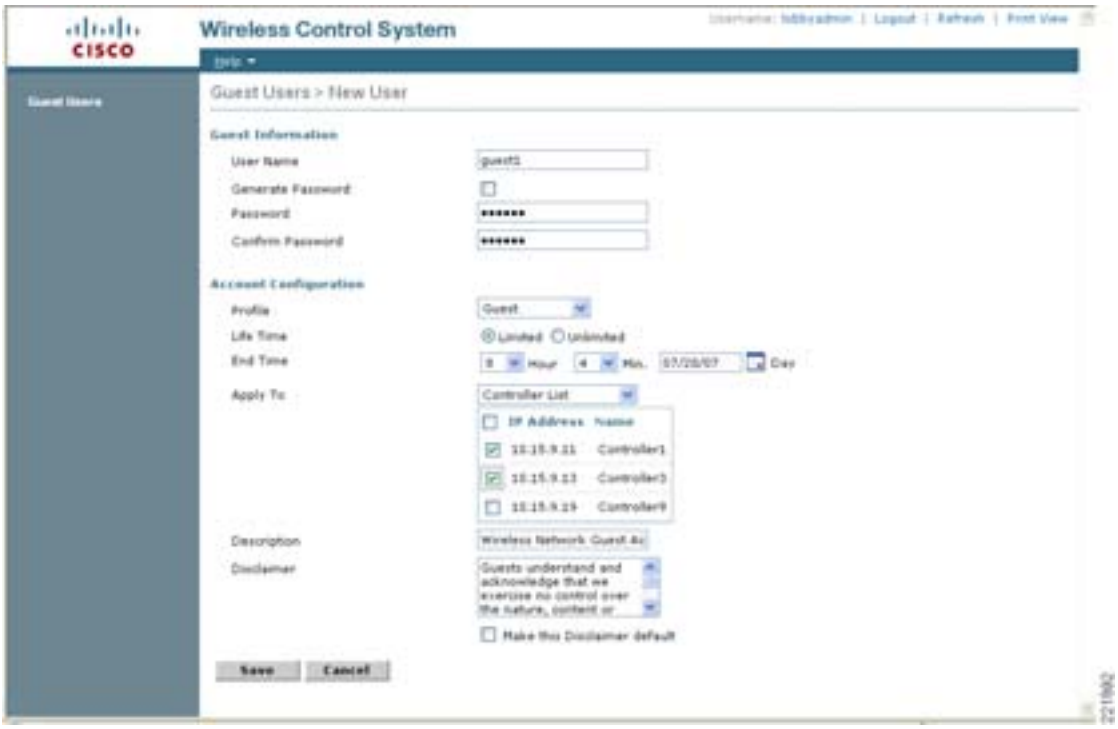


図 10-35 は、ゲスト ユーザ アカウント作成の例を示しています。

図 10-35　ゲスト ユーザ アカウントの作成



ステップ 3　Guest Information にユーザ名とパスワードを入力します。

パスワードは、大文字と小文字が区別されます。ユーザ名は、24 文字以下に制限されています。管理者には、**Generate Password** チェックボックスをクリックすることによって、パスワードの自動生成を許可するオプションもあります。

ステップ 4　**Account Configuration** で、次の項目を選択します。

- Profile：プルダウン選択リストに、L3 Web ポリシーが設定された WLAN（SSID）のリストが表示されます。
- Life Time：「limited」または「unlimited」を選択します。
- End Time：ゲスト アカウントが「limited」の場合、資格情報の有効期限が切れる月、日、時刻を選択します。
- Apply To：プルダウン選択リストから **Controller List** を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをクリックします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。

（注）　図 10-35 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的 / 地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1) WLAN 展開が WCS マッピング データベースに統合されている場合、2) ゲスト WLAN（Web ポリシーが設定された WLAN）がモビリティ アンカーを使用しない場合に限られます。

- Description：説明を入力します。説明は、Security > Local Net Users で資格情報を適用する WLC に表示されます。これはゲストに送信できる E メールにも含まれ、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。
- Disclaimer：ゲスト ユーザに送信できる E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

ステップ 5　最後に、**Save** をクリックします。図 10-36 に示すサマリ画面が表示され、資格情報がアンカー コントローラに適用されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます

図 10-36　ゲスト アカウントの正常な作成

ステップ 6　**Print/Email Guest User Credentials** をクリックします。図 10-37 に示すような画面が表示されます。

図 10-37　ゲスト ユーザ詳細の印刷または E メールでの送信

（注）　ゲスト アカウント情報のユーザへの E メール送信をサポートするように SMTP メール サーバを設定する方法の詳細は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a008082e66c.html#wp1055882）を参照してください。

アカウントの詳細を印刷または E メールで送信すると、図 10-38 に示すような画面が表示されます。**User Name** をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、User Name の隣のボックスをオンにしてプルダウン選択リストから **Delete Guest User** を選択することにより、ゲスト アカウントを削除できます。

図 10-38　WCS ゲスト ユーザのサマリ

（注）　ユーザがアクティブな状態で WCS からユーザ テンプレートを削除すると、そのユーザの認証が解除されます。

ゲスト ユーザのスケジュール テンプレートの使用

ゲスト アカウントの設定の詳細は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a0080831841.html#wp1075155）を参照してください。

図 10-39 は、ゲスト ユーザ テンプレート オプションを示しています。

図 10-39　ゲスト ユーザ テンプレート オプション

ステップ 1　プルダウン選択リストから、**Schedule Guest User** を選択して **Go** をクリックします。

図 10-40 に示すようなテンプレートが表示されます。

図 10-40　ゲスト ユーザのスケジュール テンプレート

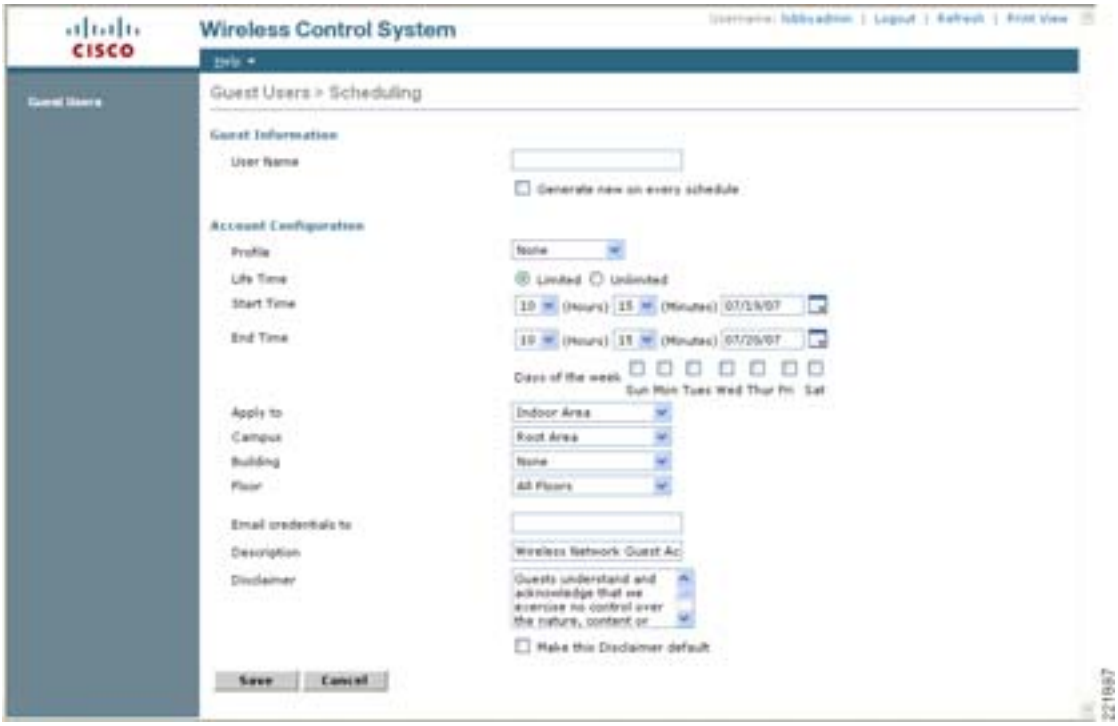
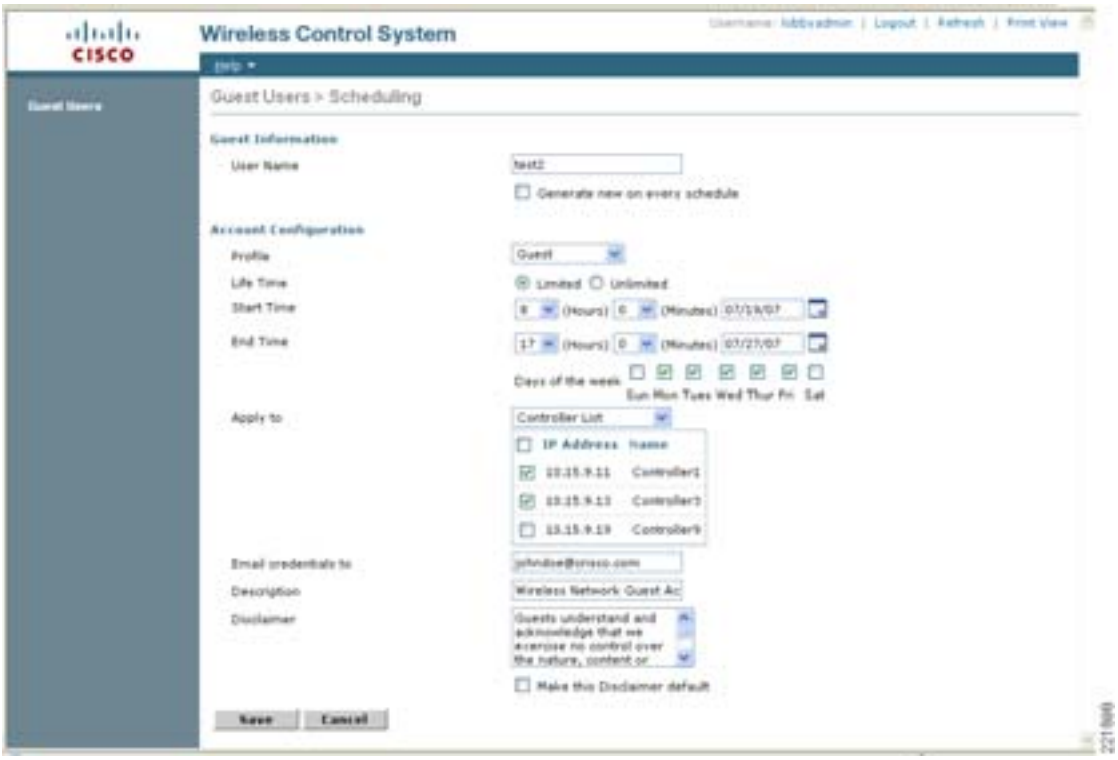


図 10-41 は、ゲスト ユーザ アカウントのスケジュールの作成例を示しています。

図 10-41　ゲスト ユーザ アカウントのスケジュールの作成



ステップ 2　Guest Information にユーザ名を入力します。ユーザ名の長さは、24 文字まで可能です。スケジュールベースのテンプレートを使用する場合、管理者には、アクセスが提供される新しい日ごとに、ユーザ名が自動生成できるようにするオプションもあります。また、このテンプレートを使用する場合、ユーザ パスワードが自動生成されます。手動でパスワードを割り当てるオプションはありません。

ステップ 3　Account Configuration で、次の項目を選択します。

- Profile：プルダウン選択リストに、L3 Web ポリシーが設定された WLAN（SSID）のリストが表示されます。
- Life Time：「limited」または「unlimited」を選択します。
- Start Time：アカウントがアクティブになる時刻、月、日を選択します。

（注）　開始時刻は、アカウントが作成される当日に開始することはできません。開始時刻は、アカウントが作成される日から 1 日以上過ぎている必要があります。

- End Time：アカウントが制限されている場合、終了時刻、月、日を選択します。

（注）　開始日から終了日までの期間は、30 日を超えることはできません。

- Days of Week：アカウントの有効期間に応じて、管理者はアクセスできる曜日を管理できます。アクセスが許可される曜日の隣のチェックボックスをクリックします。

(注)「Days of the Week」が選択されている場合、開始および終了時刻は、それぞれの日のうちでアクセス可能な期間を表します。有効期限が切れるとその日のうちに、WCS は適用可能なコントローラから資格情報を削除します。アクセスが許可される新しい日 / 間隔ごとに、WCS によって新しいパスワード（必要に応じてユーザ名）が自動生成され、ゲスト ユーザに E メールで送信され、新しい資格情報が適用可能な WLC に再適用されます。「Days of the Week」が定義されていない場合、開始日時に基づいてアクセスが開始され、終了日時まで常にアクティブになります。

- Apply To：プルダウン選択リストから **Controller List** を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをクリックします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。

(注) 図 10-41 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的 / 地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1) WLAN 展開が WCS マッピング データベースに統合されている場合、2) ゲスト WLAN（Web ポリシーが設定された WLAN）がモビリティ アンカーを使用しない場合に限られます。

- E-mail Credentials to：アカウントを設定するユーザの E メール アドレスを入力します。これは必須フィールドです。

(注) SMTP メール サーバは、ゲスト アカウント情報の送信に使用できるように、WCS で設定する必要があります。詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6305/products_configuration_guide_chapter09186a008082e66c.html#wp1055882

- Description：説明を入力します。説明は、Security > Local Net Users で資格情報を適用する WLC に表示されます。説明は、ゲストに送信できる E メールにも含まれ、どのような資格情報をネットワークへのアクセスに使用するかを知らせます。
- Disclaimer：ゲスト ユーザに送信される E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

ステップ 4　最後に、**Save** をクリックします。図 10-42 に示す画面が表示され、スケジュールされたアカウントが作成されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

図 10-42　スケジュールされたアカウントの正常な作成

ステップ 5　必要に応じて、**Print/Email Guest User Credentials** をクリックします。図 10-43 に示すような画面が表示されます。

図 10-43　ゲスト ユーザ詳細の印刷または E メールでの送信

アカウントの詳細を印刷または E メールで送信すると、図 10-44 に示すようなサマリ画面が表示されます。**User Name** をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、User Name の隣のボックスをオンにしてプルダウン選択リストから **Delete Guest User** を選択することにより、ゲスト アカウントを削除できます。

図 10-44　WCS ゲスト ユーザのサマリ

(注)　ユーザがアクティブな状態で WCS からユーザ テンプレートを削除すると、そのユーザの認証が解除されます。

これで、WCS の Lobby Ambassador インターフェイスを使用したゲスト アカウントの作成に必要な手順は終了です。

アンカー コントローラ上でのゲスト資格情報の直接管理

次の手順では、ネットワーク管理者が、Lobby 管理者の特権を使用して 1 つ以上のアンカー コントローラ上にローカル管理アカウントを設定しているものとします。

ステップ 1　システム管理者が割り当てた Lobby 管理者の資格情報を使用してアンカー コントローラにログインします。コントローラの Web 管理に対して HTTP/HTTPS を許可するには、ファイアウォールを通してコンジットを開く必要があります。アンカー コントローラの位置決め（P. 10-6）を参照してください。

ログインすると、図 10-45 に示すような画面が表示されます。

図 10-45　アンカー コントローラのログイン

ステップ 2　**New** をクリックします。

図 10-46 に示すような画面が表示されます。

図 10-46　ローカル WLC ゲスト資格情報の作成

ステップ 3　ユーザ資格情報を作成するには、次の手順を実行します。

a. ユーザ名とパスワードを入力します（手動または自動）。

b. ゲスト アカウントを適用する WLAN/SSID を選択します。その際、L3 Web ポリシーが設定された WLAN だけが表示されます。

c. 資格情報の有効期間を入力します。

d. ユーザの説明を入力します。

ステップ 4　**Apply** をクリックします。

図 10-47 に示すような画面に、新しく追加されたゲスト ユーザが表示されます。

図 10-47　アンカー WLC ゲスト ユーザのリスト

この画面では、次の機能を実行できます。

- 既存のユーザの編集（右端のリンク。非表示）
- 既存のユーザの削除（右端のリンク。非表示）
- 新しいユーザの追加

ユーザ アカウントの最大数の設定

コントローラ上で指定可能なゲスト ユーザ アカウントのデフォルト数は 512 です。この値は、次の手順を実行することによって変更できます。

ステップ 1　**Security** タブをクリックします（図 10-48 を参照）。

図 10-48　ユーザ アカウントの最大数の設定

ステップ 2　左側のペインで、AAA プロパティの下の **General** をクリックします。

ステップ 3　ユーザ データベース エントリの最大数を設定します（512 ～ 2,048 の間）。

ステップ 4　**Apply** をクリックします。

最大同時ユーザ ログイン

WLC 上のローカル ユーザ アカウントの同時ログインの最大数は、設定が可能です。同時ログイン数を無制限にする場合は、値を 0 にします。値を 1 ～ 8 に制限することもできます。ユーザ ログインの最大数は、次の手順で設定されます。

ステップ 1　**Security** タブをクリックします（図 10-49 を参照）。

図 10-49　ユーザ ログイン ポリシー

ステップ 2　左側のペインで、AAA の下の **User Login Policies** をクリックします。

ステップ 3　同時ユーザ ログインの最大数を設定します（0 ～ 8 の間）。

ステップ 4　**Apply** をクリックします。

ゲスト ユーザの管理に関する注意事項

次の点に注意してください。

- ゲスト アカウントは、上記の方法か、2 つの方法を同時に使用して追加できます。
- WCS の使用時に、コントローラの設定が最近 WCS と同期されていない場合、Lobby 管理者はローカルのアンカー コントローラ上で作成された可能性のあるユーザ アカウントを表示できないことがあります。この場合に、すでに WLC で設定されているユーザ名で WCS の Lobby 管理者がアカウントを追加しようとすると、ローカル設定が WCS 設定で上書きされます。
- ローカル管理者がユーザ　アカウントをローカルのコントローラ上に追加するときには、WCS 経由で作成されたものも含めて、作成されたすべてのアカウントを表示できます。
- ゲスト ユーザが WLAN に対して認証された状態で、資格情報が WCS またはローカルのコントローラ上から削除されると、ユーザ トラフィックが停止し、ユーザの認証が解除されます。

その他の機能とソリューション オプション

Web ポータル ページの設定と管理

内部 Web サーバと関連機能は、ローカルのアンカー コントローラ上でホストされます。認証またはパススルー用の Web ポリシーを使用するように WLAN を設定した場合は、デフォルトで内部 Web サーバが呼び出されます。それ以上の設定は必要ありません。内部ポータルには、オプションの設定パラメータがいくつか用意されています。

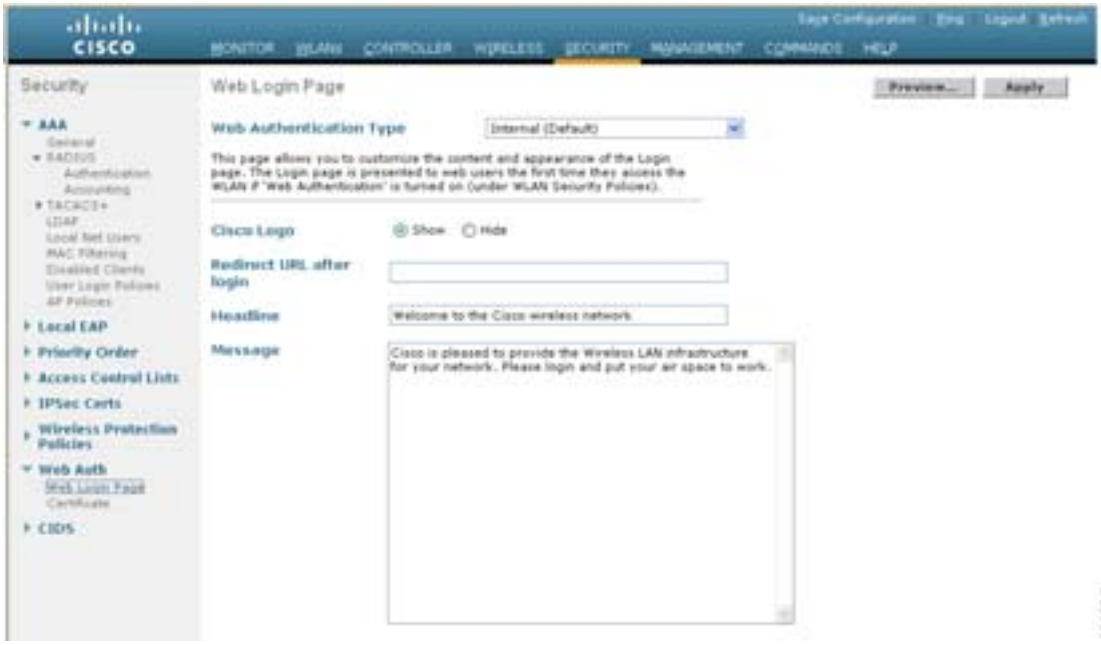
内部 Web ページの管理

ステップ 1　**Security** タブをクリックします。

ステップ 2　左側のペインで、**Web Auth** をクリックして、**Web Login Page** をクリックします。

図 10-50 に示すような設定画面が表示されます。ポータル ページに表示される見出しとメッセージ情報を変更できます。また、認証後のリダイレクト URL を選択することもできます。

図 10-50　Web ログイン ページ設定画面



ステップ 3　**Apply** をクリックします。

ステップ 4　必要に応じて、**Preview** をクリックして、ユーザに表示されるリダイレクト先のページを確認します。

Web ページのインポート

カスタマイズされた Web ページをダウンロードして、ローカルのアンカー コントローラ上に保存できます。カスタマイズされた Web ページをインポートするには、次の手順を実行します。

ステップ 1　**Commands** タブをクリックします（図 10-51 を参照）。

図 10-51　Web ページのインポート

ステップ 2　File Type で **Web Auth Bundle** を選択します。

ステップ 3　ファイルが存在する TFTP サーバの IP アドレスとファイル パスを指定します。

ステップ 4　**Download** をクリックして、ダウンロードを開始します。

Web 認証バンドルをダウンロードする際には、次の点に注意してください。

- プルダウン選択リストから **Web Auth Bundle** を選択して、ファイルがコントローラ上の正しいディレクトリに保存されるようにします。
- **Web 認証バンドル**は、カスタム Web ログイン ページにアソシエートされている、HTML ファイルとイメージ ファイルの **.tar** ファイルである必要があります。ダウンロード後に、WLC によってファイルが untar され、適切なディレクトリに格納されます。
- **Web 認証バンドル**（**tar** ファイル）は、1MB より大きくてはなりません。
- HTML ログイン ページのファイル名は、**login.html** にする必要があります。

カスタマイズされた Web ページのダウンロードと使用方法の詳細は、次の URL を参照してください。http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/c41users.html#wp1049431

インポートした Web 認証ページの選択

コントローラにダウンロードしたカスタマイズ済みの Web 認証ページを使用するには、次の手順を実行します。

ステップ 1　**Security** タブをクリックします。

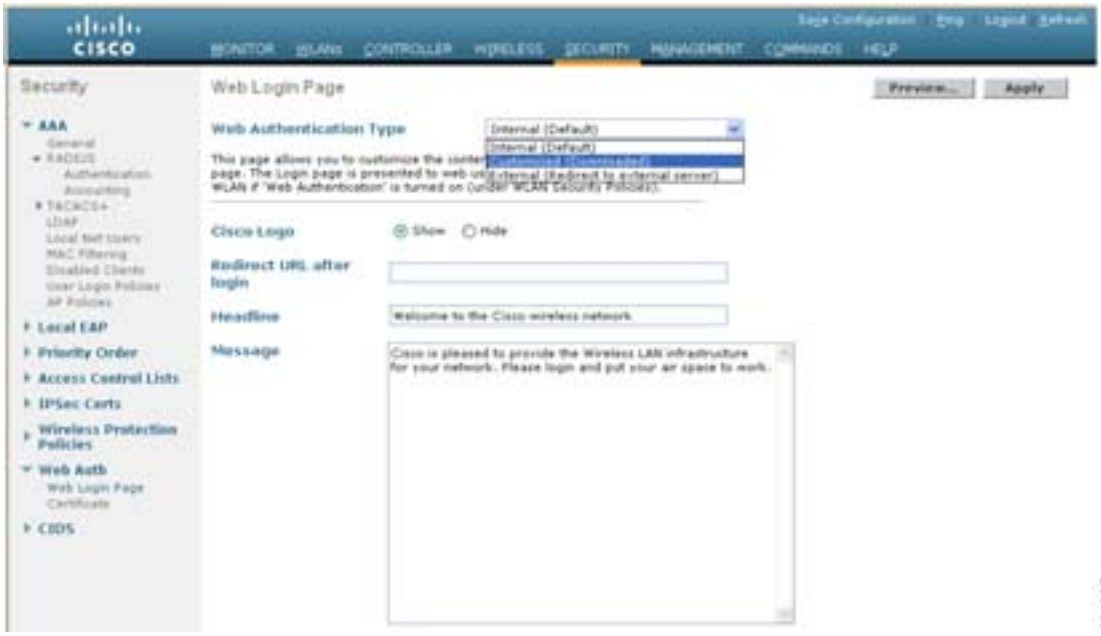
ステップ 2　左側のペインで、**Web auth** をクリックして、**Web Login Page** をクリックします。

ステップ 3　Web Authentication Type プルダウン選択リストから **Customized** (Downloaded) を選択します。

ステップ 4　**Preview** をクリックして、ダウンロードしたページを表示します。

ステップ 5　最後に、**Apply** をクリックします（図 10-52 を参照）。

図 10-52　インポートした Web 認証ページの選択



内部 Web 証明書の管理

Web 認証ログイン ページでは、ユーザ資格情報を保護するために SSL が使用されます。コントローラでは、簡単な自己署名証明書が使用されます。証明書が自己署名されたものであるため、ゲストユーザが図 10-53 に示すような認証ページにリダイレクトされると、次のようなポップアップ アラートが表示されます。

図 10-53　Web 証明書セキュリティ アラート（IE6）

この時点で、**Yes** をクリックして先に進むか、**View Certificate** を選択してそのページを信頼されたサイトとして手動でインストールできます。Web サーバでは、アンカー WLC の設置およびインターフェイスの設定（P. 10-16）で設定された仮想インターフェイスの IP アドレスがソース アドレスとして使用されます。ホスト名を IP アドレスと共に指定する場合は、ホスト名が DNS によって解決されるときに、次の条件を満たすようにする必要があります。

- クライアントが Web 認証ページにリダイレクトされる。
- ユーザが、ホスト名とホスト IP アドレスの矛盾が原因の Web 認証エラーに遭遇しない。

外部 Web 証明書のインポート

信頼できるルート CA によって発行された正式な Web 証明書が必要な場合は、次の手順を実行することによって、コントローラにダウンロードできます。

ステップ 1　**Security** タブをクリックします。

左側のペインで、**Web Auth** をクリックして、**Certificate** をクリックします（図 10-54 を参照）。

図 10-54　外部 Web 証明書のインポート

ステップ 2　**Download SSL Certificate** チェックボックスをオンにします。

ステップ 3　証明書のダウンロードに必要な情報を各フィールドに入力します。

ステップ 4　**Apply** をクリックします。

ステップ 5　証明書をダウンロードしたら、サーバを再起動します。

外部 Web リダイレクションのサポート

企業では、有線のゲスト アクセスまたは NAC 機能をサポートする Web ポータル システムがすでに展開されている場合があります。そのような場合は、無線ゲスト ユーザを外部 Web ポータルにリダイレクトするように、アンカー コントローラを次の手順で設定できます。

ステップ 1　**Security** タブをクリックします。

ステップ 2　左側のペインで、**Web auth** をクリックして、**Web Login Page** をクリックします（図 10-55 を参照）。

図 10-55　外部 Web リダイレクションのサポート

ステップ 3　Web Server IP フィールドと URL フィールドに入力します。

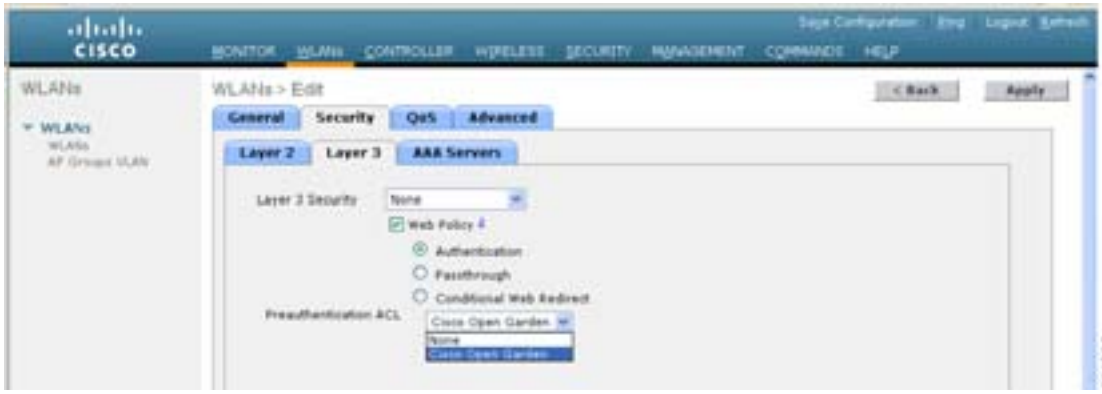
ステップ 4　**Apply** をクリックします。

外部 Web サーバを使用したコントローラの Web 認証の詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/controller/4.1/configuration/guide/c41users.html#wp1063837

アンカー WLC 事前認証 ACL

事前認証 ACL は、ゲスト WLAN に適用できます。これにより、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続できます。事前認証 ACL はゲスト WLAN のレイヤ 3 セキュリティ設定で適用されます。有効になっている場合、アンカー WLC 上でのみ実行されます（図 10-56 を参照）。

図 10-56　WLAN 事前認証 ACL



特定の ACL は、Security > Access Control Lists で設定されます（図 10-57 および 図 10-58 を参照）。

図 10-57　WLC アクセス コントロール リスト

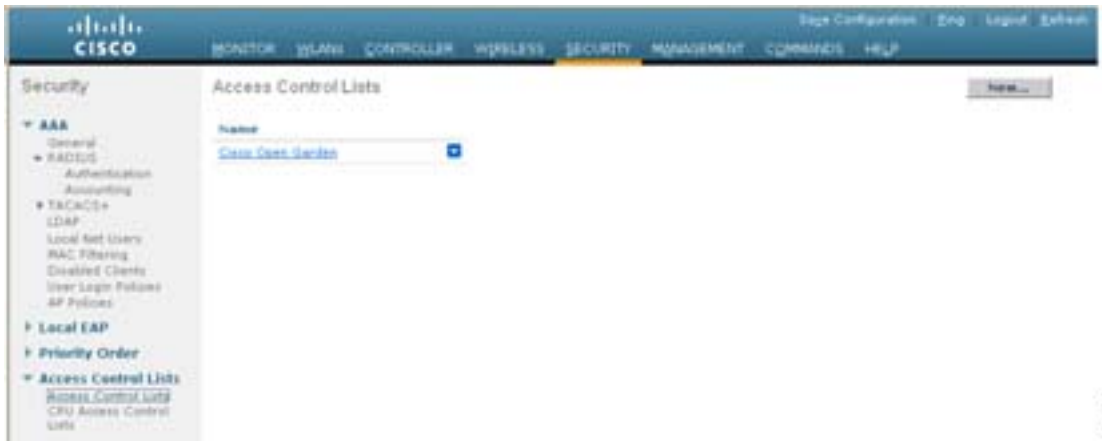
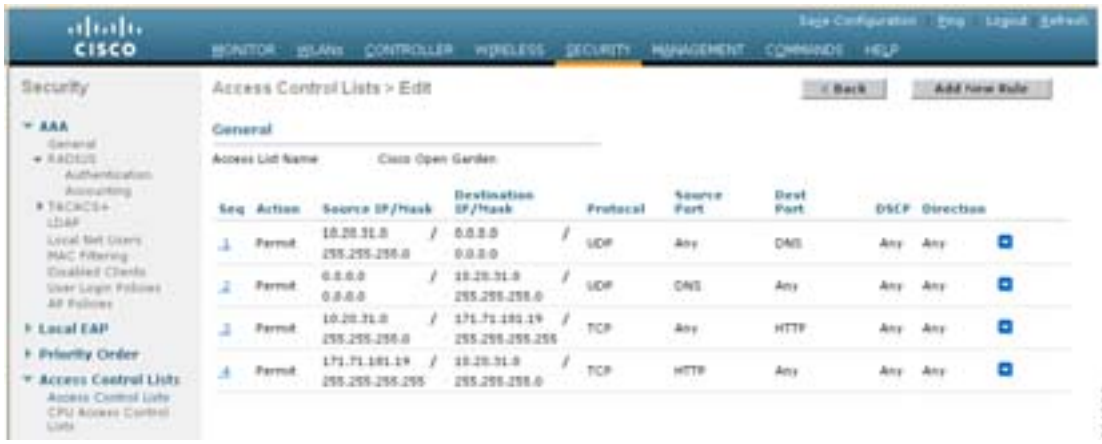


図 10-58　事前認証 ACL の例



(注)　事前認証 ACL が Web 認証ポリシーと共に使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト /URL に解決して接続することができません。

アンカー コントローラ DHCP の設定

アンカー コントローラがゲスト アクセス WLAN の DHCP サービスを管理する場合は、次の手順を実行します。

(注)　アンカー コントローラは、ゲスト N+1 冗長性を実装している場合、DHCP サービスを管理するために使用することはできません。なぜなら、2 つ以上の WLC 間で単一のゲスト VLAN/ サブネットのアドレス リースを同期するメカニズムがないからです。

新しい DHCP スコープのアンカー コントローラへの追加

ステップ 1　**Controllers** タブをクリックします。

ステップ 2　左側のペインで、**Internal DHCP Server** をクリックします

ステップ 3　**New** をクリックします（図 10-59 を参照）。

図 10-59　新しい DHCP スコープの追加

スコープ名の定義

ステップ 4　スコープの名前を定義して、**Apply** をクリックします（図 10-60 を参照）。

図 10-60　スコープ名の定義

ステップ 5　**Scope Name** をクリックして、編集します（図 10-61 を参照）。

図 10-61　DHCP スコープの編集

スコープ プロパティの定義

ステップ 6　最低限必要な次の情報を定義します。

- プールの開始と終了
- ネットワーク
- マスク
- デフォルト ルータ
- DNS サーバ

ステップ 7　Status として **Enabled** を選択し、**Apply** をクリックします（図 10-62 を参照）。

図 10-62　スコープ プロパティの設定と有効化

外部 RADIUS 認証

ゲスト ユーザの認証（P. 10-11）で説明したように、ゲスト資格情報をローカルのアンカー コントローラ上に作成して保存する代わりに、外部 RADIUS サーバを使用してゲスト ユーザを認証できます。この方法を使用する場合は、ゲスト アカウント管理（P. 10-31）で説明した Lobby 管理機能は使用できません。その他のいくつかのゲスト管理システムと外部 RADIUS サーバの併用が考えられます。

外部 RADIUS サーバを使用するようにゲスト WLAN を設定するには、アンカー コントローラ上で次の設定手順を実行します。

RADIUS サーバの追加

ステップ 1　**Security** タブをクリックします

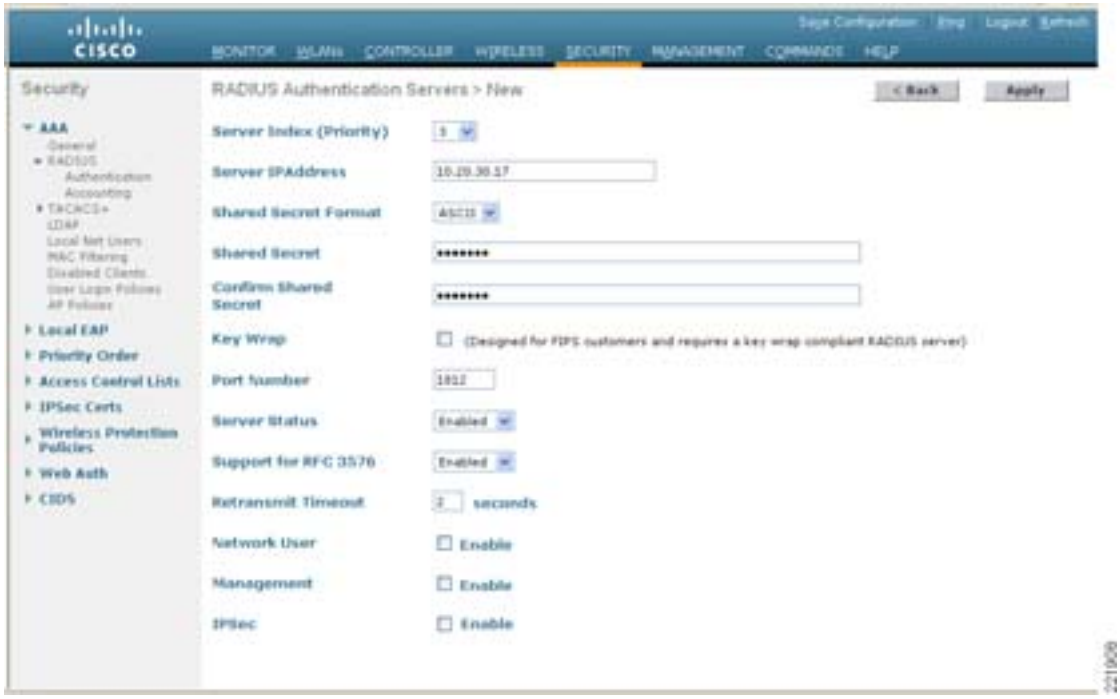
サマリ画面が表示されます（図 10-63 を参照）。

図 10-63　サマリ画面

ステップ 2　**New** をクリックします。

図 10-64 に示すような画面が表示されます。

図 10-64　RADIUS サーバの設定



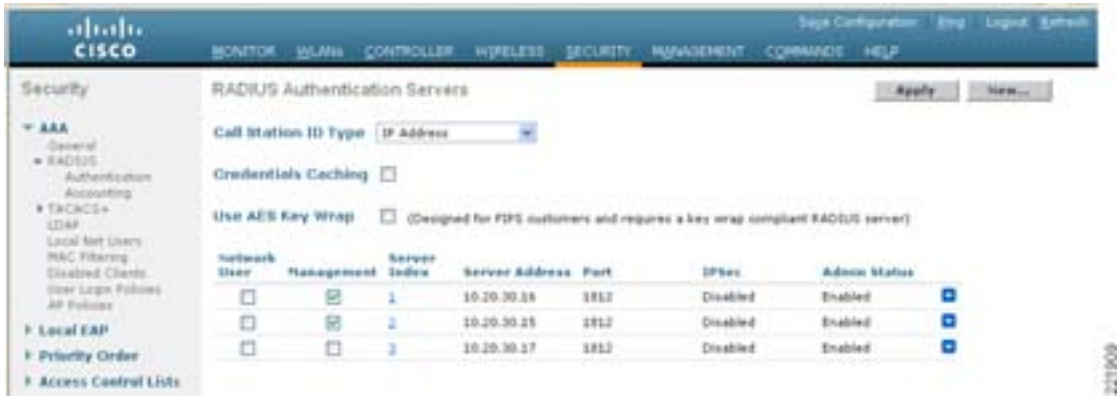
ステップ 3　RADIUS サーバの設定をするには、RADIUS サーバ上で指定したように、IP アドレス、共有秘密、および認証ポート番号を設定します。

Network User チェックボックスがオフになっていると、RADIUS サーバは、特定の WLAN の RADIUS 設定でそのサーバが明示的に選択されているときにだけユーザ認証に使用されます。また、Network User チェックボックスがオンになっていると、RADIUS サーバが、そのサーバの優先順位に基づいて、すべてのユーザ認証に使用されます。

ステップ 4　**Apply** をクリックします。

図 10-65 に示すサマリ画面には、新しく追加されたサーバが表示されます。

図 10-65　サマリ画面



ステップ 5　RADIUS サーバを選択するには、**WLANs** タブをクリックします。

図 10-66 に示すような画面が表示されます。

図 10-66　WLANs タブ

ステップ 6　ゲスト WLAN を探して、その **Profile Name** をクリックします。

図 10-67 に示すように、ゲスト WLAN の設定画面が表示されます。

図 10-67　ゲスト WLAN の設定画面

ステップ 7　WLAN Security タブで **AAA Servers** を選択します。

ステップ 8　Authentication Servers のプルダウン選択リストから、Web 認証に使用する RADIUS サーバを選択します。

外部アクセス コントロール

この章で説明した中央集中型ゲスト アクセス トポロジは、Cisco NAC Appliance などの外部アクセス コントロール プラットフォームと統合できます。

このシナリオでは、企業で、有線ゲスト アクセス サービスをサポートするためのアクセス コントロール プラットフォームがインターネットの DMZ に展開されているものとします（図 10-68 を参照）。

図 10-68　外部アクセス コントロールを使用した無線ゲスト アクセス

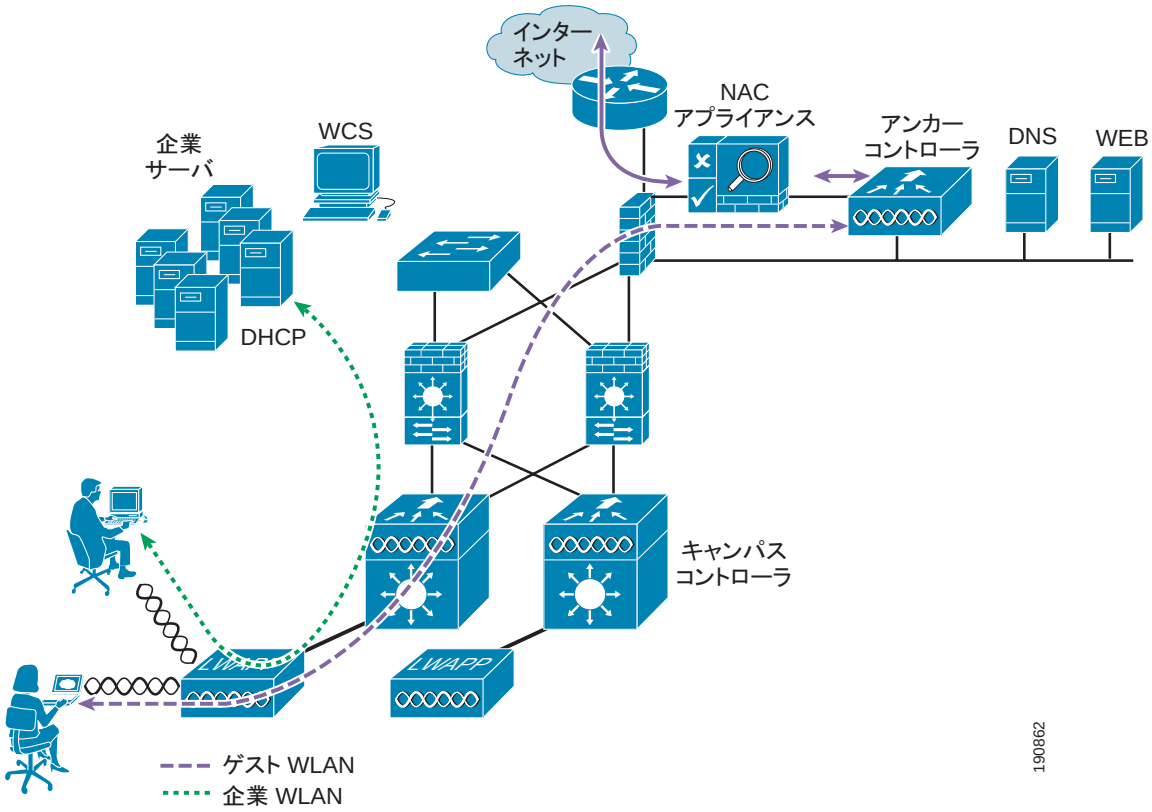


図 10-68 に示すように、無線ゲスト アクセス トポロジは、アンカー コントローラ上のゲスト VLAN インターフェイスが、ファイアウォールや境界ルータに接続する代わりに Cisco NAC Appliance などのアクセス コントロール プラットフォームの inside インタフェースに接続する点を除いて同じです。

このシナリオでは、NAC Appliance が、リダイレクション、Web 認証、およびその後のインターネットへのアクセスを処理します。キャンパス コントローラとアンカー コントローラは、NAC アプライアンスまたはその他のいくつかのプラットフォームを使用してゲスト アクセスを制御している DMZ に全社的なゲスト WLAN トラフィックをトンネルするためだけに使用されます。

ゲスト WLAN、キャンパス、およびアンカー コントローラの設定は、上記の例と同じです。唯一の違いは、ゲスト WLAN のセキュリティ設定でレイヤ 3 Web ポリシーが有効になっていない点です（図 10-69 および 図 10-70 を参照）。

図 10-69　ゲスト WLAN のレイヤ 3 セキュリティ ポリシー

図 10-70　ゲスト WLAN の L2 セキュリティ設定

上記の設定では、セキュリティ ポリシーを使用せずに WLAN が設定されます。ゲスト トラフィックは、アンカー コントローラを通過して、Cisco NAC Appliance の inside インタフェースまたは信頼されていないインターフェイスに到達し、ユーザが認証されるまでブロックされます。

DHCP は、ローカルのコントローラ上でホストするか、外部の NAC Appliance または専用サーバ経由でホストできます。

Cisco NAC Appliance またはその他の外部アクセス コントロール プラットフォーム固有の設定については、この章では説明しません。詳しい設定ガイドラインについては、プラットフォーム固有のマニュアルを参照してください。

ゲスト アクセス機能の確認

ゲスト アクセス サービスは、ユーザが次の条件を満たしている場合に正しく機能します。

- ゲスト WLAN にアソシエートできる。
- DHCP 経由で IP アドレスを受信する。
- ブラウザを開くと、Web 認証ページにリダイレクトされる。
- 資格情報を入力して、インターネット（またはその他の許可されたアップストリーム　サービス）に接続する。

ゲスト アクセスのトラブルシューティング

以降の確認作業とトラブルシューティング作業は、次のことを前提としています。

- このソリューションでは、アンカー コントローラ上の Web 認証機能が使用されている。
- ユーザ資格情報が、ローカルのアンカー コントローラ上で作成および保存されている。

次のようなさまざまな症状のトラブルシューティングを実行するには、少なくとも、外部のキャンパス コントローラからアンカー コントローラに ping できる必要があります。それが不可能な場合は、ルーティングを確認します。

その次に、次の高度な ping コマンドを実行できる必要があります。これらのコマンドは、コントローラのシリアル コンソール インターフェイスを通してだけ実行できます。

- **mping** *neighbor WLC ip*

  このコマンドは、LWAPP 制御チャネルを通して近隣のコントローラに ping します。
- **eping** *neighbor WLC ip*

  このコマンドは、LWAPP データ チャネルを通して近隣のコントローラに ping します。

標準の ICMP ping が通っても mping が通らない場合は、各 WLC のデフォルトのモビリティ グループ名が同じであることと、各 WLC の IP、MAC、およびモビリティ グループ名がすべての WLC のモビリティ メンバ リストに入力されていることを確認します。

ping と mping は通っても eping が通らない場合は、ネットワークで IP プロトコル 97（Ethernet-over-IP）がブロックされていないことを確認します。

ユーザがゲスト WLAN に接続できない

- ゲスト WLAN をサポートするアンカー コントローラとすべての外部コントローラでゲスト WLAN が有効になっていることを確認します。
- ゲスト WLAN SSID がブロードキャストされていることを確認します。
- クライアント アダプタまたはソフトウェアの設定を確認します。

ユーザが DHCP 経由で IP アドレスを取得できない

- WLAN の設定がアンカー コントローラ上と外部コントローラ上で同じであることを確認します（WLAN インターフェイスおよびモビリティ アンカーを除く。アンカー WLC 上でのゲスト WLAN の設定（P. 10-29）を参照）。
- ゲスト WLAN がアンカー WLC 上で有効になっていることを確認します。
- アンカー コントローラのゲスト VLAN インターフェイスの設定で、DHCP サーバのアドレスが適切かどうかをチェックします。
  - 外部 DHCP サーバを使用している場合は、IP アドレスが外部サーバのアドレスになっている必要があります。
  - アンカー コントローラから外部 DHCP サーバにアクセスできることを確認します。
  - DHCP サービスにアンカー コントローラを使用している場合は、DHCP サーバの IP アドレスがコントローラの管理 IP アドレスになっている必要があります。
  - コントローラ上で DHCP スコープが設定され有効になっていることを確認します。
  - DHCP スコープのネットワーク マスクとゲスト VLAN インターフェイスのマスクが一致していることを確認します。
  - DHCP スコープが、ネットワーク インフラストラクチャに割り当てられたすべてのアドレスと重複していないことを確認します。

ユーザが Web 認証ページにリダイレクトされない

次の解決方法では、ユーザがゲスト WLAN にアソシエートして IP アドレスを取得できることを想定しています。

- 有効な DNS サーバが DHCP を介してクライアントに割り当てられていることを確認します。
- DNS サーバがアンカー コントローラから接続可能なことを確認します。
- Web ブラウザで開かれている URL が解決可能なことを確認します。
- Web ブラウザで開かれている URL が HTTP ポート 80 に接続していることを確認します。

（注） 内部 Web 認証サーバは、80 およびユーザが定義したもう 1 つのポート番号以外のポート上の入力要求をリダイレクトしません（ユーザ リダイレクション（P. 10-9）を参照）。

ユーザが認証されない

- アンカー コントローラ上のユーザ資格情報がアクティブなことを確認します。

  通常は、ゲスト資格情報に対して有効期間が設定されます。資格情報は、期限が切れていると、アンカー コントローラ上の Security > Local Net Users リストに表示されません。WCS を使用して、ローカルのコントローラ上でユーザ テンプレートを適用し直すか、ユーザ資格情報を作成し直してください。WCS を使用したゲスト管理（P. 10-31）およびゲスト資格情報の管理（P. 10-10）を参照してください。
- ユーザ パスワードを確認します。

ユーザがインターネットまたはアップストリーム サービスに接続できない

- アンカー コントローラと、アンカー コントローラに接続されているファイアウォールまたは境界ルータ間のルーティングを確認します。
- 必要に応じて、ファイアウォールまたはインターネット境界ルータの NAT 設定を確認します。

システム監視

以降では、トラブルシューティングに役立つ可能性のあるいくつかの監視コマンドについて説明します。

アンカー コントローラ

シリアル コンソール ポートから：

```
Cisco Controller) >show client summary

Number of Clients.............................. 1

MAC Address       AP Name            Status         WLAN  Auth  Protocol  Port

----------------  -----------------  -------------  ----  ----  --------  ----

00:40:96:ac:5f:f8  10.15.9.19        Associated     3     Yes   Mobile    1
```

プロトコルが Mobile になっていることに注目してください。Auth フィールドには、実際のユーザの状態が反映されます。ユーザが Web 認証をパスすると、このフィールドに YES と表示されます。パスしなかった場合は、このフィールドに NO と表示されます。

AP 名にも注目してください。これは、外部コントローラ（起点コントローラ）の管理 IP アドレスです。

サマリ情報に示されたクライアントの MAC アドレスを使用して、詳細を表示します。

```
(Cisco Controller) >show client detail 00:40:96:ac:5f:f8
Client MAC Address.............................. 00:40:96:ac:5f:f8
Client Username ................................ romaxam
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 3
BSSID........................................... 00:00:00:00:00:02
Channel......................................... N/A
IP Address...................................... 10.20.31.100
Association Id.................................. 0
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 86316
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.15.9.19
Mobility Move Count............................. 1
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... wlan-user
VLAN............................................ 31
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 0
      Number of Bytes Sent...................... 0
      Number of Packets Received................ 0
      Number of Packets Sent.................... 0
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... Unavailable
      Signal to Noise Ratio..................... Unavailable
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
```

コントローラの Web 設定、および管理インターフェイスの Clients > Detail で同じ情報を得ることができます（図 10-71 を参照）。

図 10-71　Anchor WLC Monitor > Client Detail

外部のキャンパス コントローラ

シリアル コンソール ポートから：

```
(WiSM-slot3-1) >show client summary

Number of Clients.............................. 2

MAC Address        AP Name            Status         WLAN  Auth  Protocol  Port

-----------------  -----------------  -------------  ----  ----  --------  ----

00:40:96:ac:5f:f8  AP3_.18e5.7fdc     Associated     1     Yes   802.11g   29
```

アンカー コントローラでは Protocol フィールドが Mobile になっていましたが、同じクライアントに対してこの Protocol フィールドは 802.11g になっていることに注目してください。外部のキャンパス コントローラでは、必ずユーザが Authenticated として表示され、AP name にはクライアントがアソシエートされている実際の AP が反映されます。

次のコマンドを実行すると、さらに詳しい情報を得られます。

```
(WiSM-slot3-1) >show client detail 00:40:96:ac:5f:f8
Client MAC Address.............................. 00:40:96:ac:5f:f8
Client Username ................................ N/A
AP MAC Address.................................. 00:17:df:35:86:50
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:17:df:35:86:50
Channel......................................... 11
IP Address...................................... Unknown
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.15.9.13
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... management
VLAN............................................ 9
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 308244
      Number of Bytes Sent...................... 700059
      Number of Packets Received................ 2527
      Number of Packets Sent.................... 1035
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... -75 dBm
      Signal to Noise Ratio..................... 25 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      AP3_.18e5.7fdc(slot 0) ....................
antenna0: 37 seconds ago -73 dBm................. antenna1: 4294510568 seconds ago
-128 dBm
```

コントローラの Web 設定、および管理インターフェイスの Clients > Detail で同じ情報を取得できます（図 10-72 を参照）。

図 10-72　Foreign WLC Monitor > Client Detail

デバッグ コマンド

シリアル コンソールからは、次のデバッグ コマンドも使用できます。

```
debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable
```

CHAPTER 11

モバイル アクセス ルータ、ユニバーサル ブリッジ クライアント、および Cisco Unified Wireless

3200 シリーズ モバイル アクセス ルータの概要

Cisco 3200 シリーズ モバイル アクセス ルータ（MAR）は、無線ネットワーク間のシームレスなモビリティと相互運用性を実現する、小型で高性能なネットワーク アクセス ソリューションです。コンパクトな設計なので、防衛、公安、国土保安、および運輸分野での車載に適しています。無線、セルラー、衛星、WLAN を利用した複数のネットワークでシームレスな通信モビリティが可能になり、ピアツーピア ネットワーク、階層型ネットワーク、またはメッシュ ネットワーク経由でビジネスに不可欠な音声、画像、データをやり取りできます。

Cisco 3200 ルータを使用してモバイル ネットワークを構築すれば、3200 ルータ上の無線接続（セルラーや WLAN ベースなど）を介して、PC、監視カメラ、デジタル ビデオ レコーダ、プリンタ、PDA、スキャナなどのあらゆるデバイスをホーム ネットワークに接続できます。

Cisco 3200 シリーズは 1 つ以上の PC104/Plus モジュールで構成され、これらをスタックすることで無線ルータ構成を形成します。これらのモジュラー カードは、カード バンドルとして、または耐環境性に優れた Cisco 3200 エンクロージャ（3200 Rugged Enclosure）に組み込まれた完全なシステムとして提供されます。Cisco 3200 シリーズのルータ バンドルは、Cisco 3230 モデルと Cisco 3270 モデルで構成されています。図 11-1 の左側は Cisco 3200 Rugged Enclosure バンドル、右側は Cisco 3270 Rugged Enclosure バンドルです。

図 11-1　Rugged Enclosure バンドル：Cisco 3200（左）、Cisco 3270（右）

MAR3200

221954

Cisco 3270

Cisco 3200 シリーズ Rugged Enclosure オプションは乗り物への搭載に適しており、公安、運輸、防衛、保安市場特有のモビリティ ニーズに対応しています。この Rugged Enclosure オプションは完全密封型で、厳しい温度変化、高度環境、強い衝撃や振動、湿気、水濡れ、埃など、過酷な環境に耐えられるように設計されています。

Rugged Enclosure の詳細は、次の URL にある 3200 Rugged Enclosure のデータ シートを参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd8028e3a7.html

Cisco 3200 カード バンドルの詳細は、次の URL にある Cisco 3200 Wireless and Mobile Routers のデータ シートを参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd800fe973.html

Cisco 3200 シリーズと無線ネットワーク アクセス

このようなさまざまな無線オプションと接続モードにより、Cisco 3200 MAR は移動中もネットワークへの「常時」IP 接続を提供できます。これらのルータは乗り物への搭載に適しています。また、Cisco IOS Mobile Networks に対応し、ローカル IP ノードからレイヤ 3 サブネット間をローミングする際に、潜在的に発生するアドレス変更を非表示にする機能を備えています。これによって、モバイル ネットワーク上の IP ホストは、ルータが移動中でもネットワークに透過的に接続できます。

たとえば、バスに 3200 MAR を搭載すると、バスで街中を移動している間も乗客はインターネットに接続できます。接続を維持するためにクライアント コンピュータに特殊なソフトウェアをインストールする必要はありません。この透過的な通信は、パケットをモバイル アクセス ルータにトンネルするモバイル IP デバイスによって達成されます。これについては、この章で詳しく説明します。

Cisco Unified Wireless Network のリリース 4.1 では、Workgroup Bridge（WGB; ワークグループ ブリッジ）のサポートが追加されています。この機能拡張がなされる前は、3200 MAR を Cisco Unified Wireless Network に接続するには Universal Work Group Bridge（UWGB; ユニバーサル ワークグループ ブリッジ）モードを使用する必要がありました。

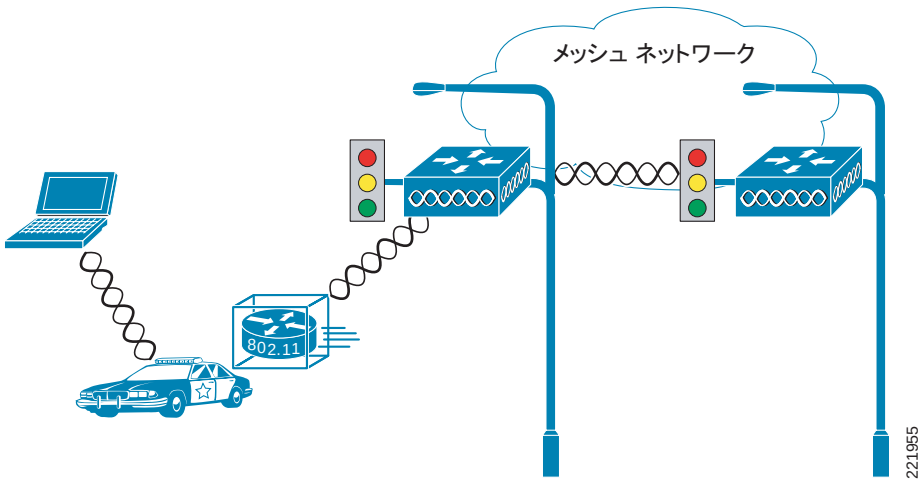
WGB を使用することで、3200 MAR は、Cisco Unified Wireless Network の WGB クライアントとして動作できます。3200 MAR は Cisco 802.11 Unified Wireless Network への WGB 接続をサポートするほか、WGB 対応の他の WLAN ソリューションへの接続にも使用できます。モバイル アクセス ルータの UWGB は、WGB 機能に取って代わられることはありません。実際に、WGB モードをサポートしない 802.11 無線ネットワークに 3200 MAR を接続する必要がある環境では非常に便利です。これらタイプのネットワーク接続では、UWGB モードの 3200 MAR は 802.11 無線ネットワークへの通常の無線クライアントとして認識されます。

3200 MAR のもう 1 つの無線アクセス方法とは、その有線ファスト イーサネットとシリアル インターフェイス接続を使用するというものです。これらの接続では、セルラー デバイスと衛星デバイスを統合できます。これらのデバイス タイプのオプションについては、本書では説明しません。詳細は次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/prod_brochure0900aecd80374174.html

車両ネットワークの例

ここでは、3200 MAR の WGB 機能を使用してメッシュ WLAN に接続するメッシュ ネットワークでの 3200 MAR 用の簡単なアプリケーションについて説明します（図 11-2 を参照）。

図 11-2　車両ネットワークの例



次の点に注意してください。

- モバイル ユニットに取り付けられている Cisco 3200 シリーズ ルータでは、車両内および車両の周りにあるクライアント デバイスの接続を車両のローミング時に維持できます。
- 車両に取り付けられた Cisco 3200 シリーズ ルータの Wireless Mobile Interface Card（WMIC; 無線モバイル インタフェース カード）は、アクセス ポイントとして 802.11b/g および 4.9 GHz 無線クライアントへの接続を提供するよう設定されます。
- ラップトップ、カメラ、またはテレマティクス デバイスなどの車両内無線クライアントからのネットワークへの接続には、イーサネット インターフェイスが使用されます。
- メッシュ AP への接続用に、別の WMIC が WGB として設定されます。これによって、車両の移動時に、アーキテクチャのルート デバイスを通した透過的なアソシエーションと認証を確保できます。
- シリアル インターフェイスを使用すると、CDMA や GPRS などのセルラー ネットワークに接続する無線 WAN モデムに接続できます。帯域幅が最大であることから、無線 802.11 接続は推奨サービスとして扱われます。ただし、WLAN 接続を使用できない場合は、セルラー技術によるバックアップ リンクを使用できます。ルーティング優先度またはモバイル IP の優先度によって、接続の優先度を設定できます。

単純なブリッジ クライアント データ パスの例

MAR に接続されている IP デバイスは、自身がモバイル ネットワークの一部であることを認識しません。IP デバイスで、ネットワーク内の別のノードと通信する必要がある場合、IP デバイスのトラフィックはデフォルトのゲートウェイである Cisco 3200 シリーズ ルータに送信されます。Cisco 3200 シリーズ ルータはトラフィックをメッシュ AP の WLAN に転送し、WLAN でデータ パケットが LWAPP にカプセル化され、ネットワーク経由でコントローラに転送されます。

図 11-3 で示しているように、Cisco 3200 シリーズ ルータから WGB バックホール リンクを経由してトラフィックが送信されます。次にトラフィックは、WLAN を経由してコントローラに送信され、コントローラからコントローラ インターフェイスを経由して有線ネットワークに転送されます。MAR に接続されているいずれかのクライアント宛てのリターン トラフィックは、メッシュ ネットワークのコントローラに返すよう指定する静的ルート経由で転送されます。

図 11-3　単純なレイヤ 2 データ パスの例

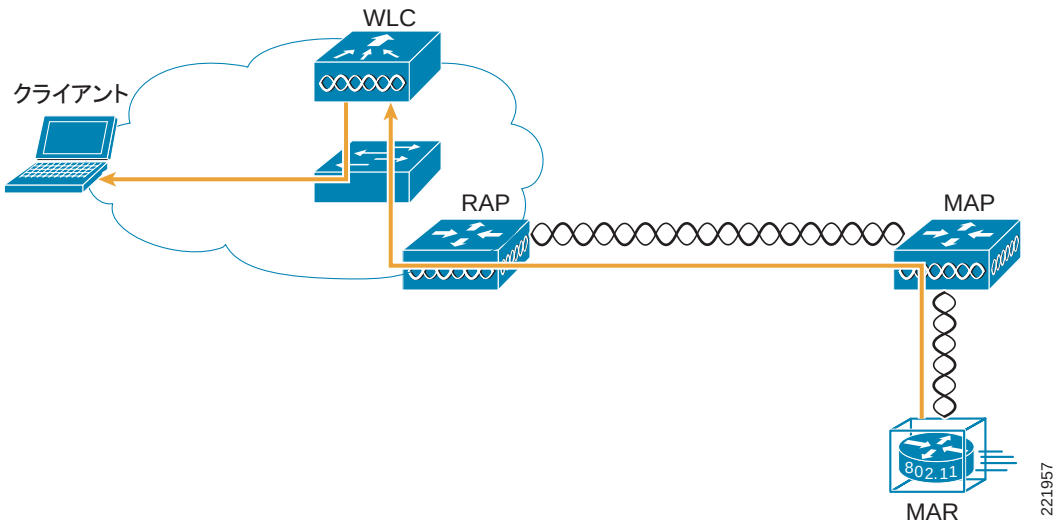
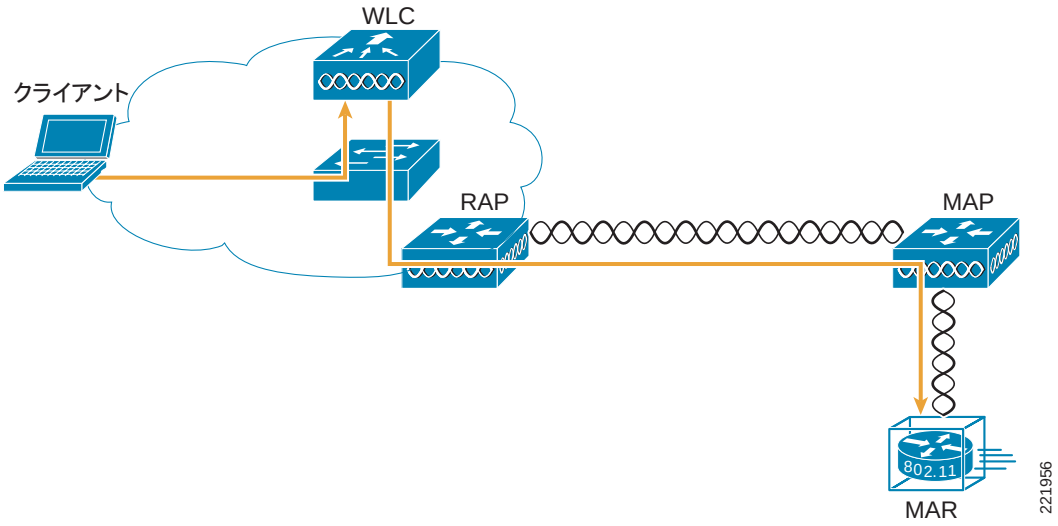


図 11-4 は、MAR へのリターン パスを示しています。モバイル IP では、静的ルーティングの必要がありません。これについては、この章で詳しく説明します。モバイル IP を使用できない場合、簡単な展開では NAT を使用することがあります。

図 11-4　クライアントへのリターン データ パス



このデータ パスの例は、MAR でバックフォールに WMIC だけを使用している場合の純粋なレイヤ 2 メッシュのトラフィックを示しています。展開をもっと複雑にする必要がある場合（セカンダリ セルラー バックホール リンクなど）は、モバイル IP が必要です。

モバイル IP 環境での Cisco 3200 シリーズ

現代の大都市の多くのモバイル ネットワークで使用されている無線技術には、都市全体を対象範囲にできる 802.11 メッシュ型無線ネットワークがあります。このネットワークでは、車内ビデオなど帯域幅集中型のアプリケーション向けの高速アクセスを利用できます。メッシュ型無線ネットワークの拡張が実用的ではないカバレッジ領域の場合、CDMA 1x RTT などのセルラー サービスで補完できます。この方法では、セルラー サービスを使用して、接続におけるギャップを埋めて、バックアップ無線接続を確保できます。この追加のバックアップ インターフェイスには、2 つの個別のネットワーク間でのクライアントのローミングを可能にするためのモバイル IP が必要です。

郵便の手紙が封筒に記載された住所に配達されるのと同じように、IP ネットワークでは、固定 IP アドレスに基づいてルーティングが行われます。ネットワーク上のデバイスには、そのネットワークで割り当てられた IP アドレスに従い、通常の IP ルーティングで到達できます。ただし、モバイル ネットワークの場合、デバイスが自分のホーム ネットワークから離れた場所へ移動すると、それまでの IP ルートでは到達できません。そのため、そのデバイスのアクティブ セッションが終了してしまいます。

モバイル IP を使用すると、無線事業者が同じかどうかにかかわらず、ユーザが別のネットワークへ移動したときも同じ IP アドレスが維持されるので、個々のローミング クライアントはセッションまたは接続を中断せずに通信を続けることができます。

モバイル IP のモビリティ機能は物理レイヤやリンク レイヤではなくネットワーク レイヤで実行されるので、Cisco 3200 などのモバイル デバイスは接続と実行中のアプリケーションを維持しながら異なるタイプの無線ネットワークや有線ネットワークを移動できます。モバイル IP が有効なネットワーク接続は、セッション レイヤを維持する必要のあるあらゆるアプリケーションに適しています。

モバイル IP ネットワークの概要は、第 12 章「Cisco Unified Wireless とモバイル IP」を参照してください。

WMIC ローミング アルゴリズム

次の 4 つの基本的なトリガーが発生した時点で WMIC スキャンが開始され、より適したルート ブリッジまたはアクセス ポイントが検出されます。

1. 8 個の連続したビーコンの損失
2. データレートの変動
3. データ最大再試行回数の超過（WMIC のデフォルト値は 64）
4. 信号強度しきい値におけるドロップの測定期間

上記の 3 番と 4 番だけは、**packet retries** コマンドおよび **mobile station period** *X* **threshold** *Y*（単位は dBm）を使用して設定できます。それ以外はハードコード化されます。

8 つの連続したビーコンの損失が生じたためにクライアントでスキャンが開始すると、「Too many missed beacons」というメッセージがコンソールに表示されます。この場合、WMIC は、ユニバーサル ブリッジ クライアントとして、他の無線クライアントとよく似た動作で機能します。別のトリガー メカニズムである「モバイル ステーション」は、定期的ではなく、*period* と *threshold* という 2 つの変数を使用します。モバイル ステーションが設定されている場合、モバイル ステーション アルゴリズムが 2 つの変数（データ レートの変動と信号強度）を評価し、次のように対応します。

- ドライバで、親へのパケットの送信レートが長期間低下している場合、WMIC は新しい親のスキャンを開始します（設定した期間ごとに 1 回以下）。
- 信号強度（しきい値）が設定可能レベルを下回った場合、WMIC は新しい親のスキャンを開始します（設定した期間ごとに 1 回以下）。

データレートの変動は、次のコマンドを使用して表示できます。

```
debug dot11 dot11Radio 0 trace print rates
```

ただし、この場合、動作中の実際のデータ レート変動アルゴリズムは表示されず、データ レートの変化だけが表示されます。表示されるデータ レート低下の大きさに応じて、スキャンする期間が決まります。

期間は、アプリケーションに応じて設定する必要があります。デフォルトは 20 秒です。この遅延期間によって、たとえば、しきい値が設定した値を下回る場合に、WMIC がより適切な親をスキャンし続けることがないように防止できます。

しきい値によって、より適切な親をスキャンするためにアルゴリズムがトリガーされるレベルが設定されます。このしきい値は、*ノイズ + 20 dBm* に設定する必要がありますが、-70 dBm（しきい値の入力値は正の数のため +70）より上に設定しないでください。デフォルトは -70 dBm です。

基本的な設定例

この項では、3200 MAR の設定例を示します。これは、オープン認証と WEP 暗号化を使用する UWGB クライアントの設定手順として使用できます。これには、VLAN の作成、割り当て、DHCP などその他の基本的な設定手順も含まれています。

Cisco 32XX への接続

ステップ 1　コンソール ケーブルを、PC のシリアル ポートとモバイル アクセス ルータ コンソール ポート（DB9 メス）の両方に接続します。DB9-to-DB9 ストレート ケーブルを使用します。

（注）　RJ-45 to DB9 メス アダプタを追加して、Home AgentHA; ホーム エージェント）へのアクセスに使用するものと同じコンソール ケーブルを使用することもできます。

3200 シリーズでの IP アドレス、DHCP、および VLAN の設定

ステップ 2　モバイル ルータに接続してログインします。ループバック インターフェイスを作成して、IP アドレスを割り当てます。

ステップ 3　**vlan database** CLI コマンドを使用して、VLAN データベースに VLAN 2 を作成します。

ステップ 4　VLAN 3 および VLAN 2 インターフェイスを設定します。

VLAN 3 は、AP として機能する 2.4 GHz WMIC2W2 に使用します。VLAN 2 は、4.9 GHz WMIC（W3）に使用します。FA2/0、FA2/1、および FA2/3 を VLAN 3 に、FA2/2 を VLAN 2 に設定します。

ステップ 5　WMIC 1 と MARC との接続用に、VLAN データベースに VLAN 4 を作成します（表 11-1 を参照）。

表 11-1　インターフェイスの例

接続先	インターフェイス	無線タイプ	VLAN	説明
PC	FastEthernet2/0	なし	3	エンド デバイス用ファースト イーサネット リンク
WMIC 1（W1）	FastEthernet2/1	2.4 GHz	4	メッシュ ネットワークへの 2.4 GHz UWGB 接続
WMIC 2（W2）	FastEthernet2/3	2.4 GHz	3	モバイル ルータの周囲に 2.4 GHz AP ホットスポットを提供
WMIC 3（W3）	FastEthernet2/2	4.9 GHz	2	ワークグループ ブリッジとして機能する 4.9 GHz アップリンク

ステップ 6　次のコマンドを使用して、VLAN 3 に DHCP サーバを設定します。

```
ip dhcp pool mypool
   network 10.40.10.0  /28
default-router 10.40.10.1
ip dhcp excluded-address 10.40.10.1 10.40.10.3
```

ステップ 7　VLAN 3 上の有線クライアントに、10.40.10.0/28 サブネットの DHCP IP アドレスが正しく割り当てられていることを確認します。

WMIC の設定

WMIC ワークグループ ブリッジの設定

WMIC は、アソシエートされた 802.11 接続用の WGB クライアント モードをサポートできます。これは、**distance** コマンドをサポートする唯一の動作モードです。また、UWGB クライアント モードでの制限を克服しているため、Cisco メッシュ環境での MAR に設定するモードとして推奨されています。UWGB の制限を含む UWGB の詳細は、WMIC ユニバーサル ブリッジ クライアントの設定（P. 11-9）を参照してください。

WGB には次の 3 つのインストール モードがあります。

- *Automatic*：ブリッジ インストールとアライメント モードを起動し、そのユニットがネットワーク ロールを自動的に決定します。ユニットが別の Cisco ルート デバイスに 60 秒以内にアソシエートできる場合、ユニットは非ルート ブリッジ ロールを担います。デバイスをルート ブリッジ モードまたは非ルート ブリッジ モードに設定すると、60 秒の自動検出フェーズを回避できます。
- *Root*：デバイスがルート ブリッジとして動作し、メインのイーサネット LAN ネットワークに直接接続します。このモードでは、ユニットは他の Cisco ブリッジと無線クライアント デバイスからのアソシエーションを受け入れます。
- *Non-root*：デバイスがリモート LAN ネットワークに接続し、無線インターフェイスを使用して Cisco ルート デバイスとアソシエートしなければならないことを指定します。

WMIC がロールを自動的に決定するように設定するには、次の手順に従ってください。

ステップ 1　dot11 インターフェイスで、次のコマンドを入力します。

```
station-role {root [bridge | non-root workgroup-bridge install [automatic | root |
non-root]}
```

station-role コマンドは、WMIC のロールがアソシエート先のデバイスに基づいて選択されることを指定します。

ステップ 2　WMIC ロールを設定します。

- **station-role root bridge**：3200 MAR WMIC がルート ブリッジ デバイスとして動作することを指定します。このモードは、無線クライアント アソシエーションには対応してません。
- **station-role workgroup-bridge**：3200 MAR WMIC がワークグループ ブリッジ モードで動作することを指定します。デバイスは、ワークグループ ブリッジとして Aironet アクセス ポイントに、またはクライアントとしてブリッジにアソシエートし、そのイーサネット ポートに接続されているデバイスに対して無線 LAN 接続を提供します。

ステップ 3　mobile station コマンドを実行します。

```
mobile station
```

非ルート ブリッジまたはワークグループ ブリッジをモバイル ステーションとして設定するには、このコマンドを使用します。この機能を有効にしていると、ブリッジは弱い Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）、過度な無線干渉、または高いフレーム損失率を検出するたびに、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すると、WMIC は現在のアソシエーションを失う前に、新しいルート アソシエーションを検索して新しいルート デバイス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化されている（デフォルト設定）場合、WMIC は現在のアソシエーションを失うまで新しいアソシエーションを検索しません。

WMIC ユニバーサル ブリッジ クライアントの設定

この項の最初で説明したとおり、WMIC は UWGB として設定できます。UWGB モードでは、WGB をサポートしない 802.11 ネットワーク環境でも WMIC に対応できます。このようなネットワーク環境としては、非 Cisco メッシュ ネットワークがあげられます。現在、Cisco Unified Wireless Network で UWGB モード クライアントを使用する場合、AP ごとに UWGB クライアントを 1 つしか設定できないという制限があります。

そのため、WMIC には次の機能があります。

- IOS と非 IOS アクセス ポイントにアソシエートする。
- 相互運用性：UWGB は非 Cisco ルート デバイスを汎用クライアントとして使用することでルーティング トラフィックを転送できます。UWGB はルート デバイスへの通常の無線クライアントとして表示されます。ルート デバイスとして、WMIC はすべての Cisco Compatible Extension v3 機能やさまざまな v4 機能を使用して Cisco Compatible Extension クライアントをサポートしています。

```
station-role workgroup-bridge universal (mac address)
```

（注） WMIC のブリッジ先のアソシエートされている VLAN の MAC アドレスを使用する必要があります。たとえば、VLAN の MAC アドレスを使用してください。VLAN の MAC アドレスを取得するには、MAR ルータ カードにコンソールから入り、**show mac-address-table** コマンドを実行します。

アクセス ポイントとしての WMIC の設定

WMIC はルート アクセス ポイントとして設定できます。このロールでは、WMIC は無線クライアントからアソシエーションを受け取ります。モバイル ホットスポットを展開する予定であれば、これは便利な設定となります。次のコマンドを dot11 インターフェイス設定で実行して、WMIC をアクセス ポイントとして設定してください。

```
station-role root access-point
```

これによって、WMIC はルート アクセス ポイントとして機能します。。

セキュリティ

この章のセキュリティの項では、3200 MAR のセキュリティ機能の根底にある概念については詳しく説明しません。これらのセキュリティ メカニズムの詳細は、第 4 章「Cisco Unified Wireless Network アーキテクチャ ― 基本的なセキュリティ機能」を参照してください。

認証タイプ

この項では、WMIC に設定できる認証タイプについて説明します。認証タイプは、WMIC に設定する SSID に関連します。無線デバイスが通信するには、その前にオープン認証、802.1x/EAP ベースの認証、または共有キー認証を使用して互いを認証する必要があります。また、セキュリティを強化するため、無線デバイスは EAP 認証を使用してネットワークを認証する必要もあります。EAP 認証はユーザのネットワーク上の認証サーバに依存する認証タイプです。

WMIC では、4 つの認証メカニズム、つまり認証タイプが使用され、同時に複数を使用できます。

WMIC が使用できる 4 つの認証タイプは次のとおりです。

- WMIC へのオープン認証
- WMIC への共有キー認証
- ネットワークへの EAP 認証
- ネットワークへの MAC アドレス認証

認証メカニズムの詳細は、第 4 章「Cisco Unified Wireless Network アーキテクチャ ― 基本的なセキュリティ機能」を参照してください。

暗号化とキー管理

3200 MAR WMIC は、暗号化とキー管理には Wired Equivalent Privacy（WEP）、Wi-Fi Protected Access（WPA）、および Cisco Centralized Key Management（CCKM）をサポートしています。これらのセキュリティの詳細は、第 4 章「Cisco Unified Wireless Network アーキテクチャ ― 基本的なセキュリティ機能」を参照してください。

セキュリティ設定

WMIC のデフォルト SSID は、ゲスト モードでも設定される *autoinstall* です。ゲスト モードでは、WMIC はこの SSID をビーコンでブロードキャストし、SSID を持たないクライアント デバイスがアソシエートできるようにします。また、デフォルトでは、autoinstall に割り当てられている認証タイプはオープンです。これによって、セキュリティ設定をまったく持たないクライアントでも 3200 MAR に接続できます。MAR のセキュリティを確保するには、この設定のデフォルトを変更する必要があります。

認証タイプの SSID への割り当て

ここからは、ルート デバイス モードの WMIC に SSID の認証タイプを設定するコマンドについて説明します。また、各コマンドのコマンド コンポーネントとオプション設定コンポーネントについても説明します。

- **dot11 ssid** *ssid-string*

  このコマンドは SSID を定義します。SSID には最大 32 文字の英数字を使用できます。SSID では大文字と小文字が区別されます。
- **authentication open [mac-address** *list-name* [alternate]] [[optional] **eap** *list-name*]

— （オプション）現在の SSID の認証タイプをオープンに設定します。オープン認証では、どのクライアント デバイスでも認証が可能であり、WMIC との通知を試みることもできます。

— （オプション）SSID の認証タイプをオープン（MAC アドレス認証を使用）に設定します。このアクセス ポイントは、すべてのクライアント デバイスに MAC アドレス認証を実行させ、そのあとでネットワークへの参加が許可されるようにします。*list-name* には、認証方式のリストを指定します。方式リストの詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfathen.html

クライアント デバイスが MAC または EAP のどちらを使用してもネットワークに接続できるようにするには、alternate キーワードを使用します。いずれか一方の認証に成功したクライアントは、ネットワークへの参加を許可されます。

— （オプション）SSID の認証タイプをオープン（EAP 認証を使用）に設定します。WMIC は、他のすべてのクライアント デバイスに EAP 認証を実行させ、そのあとでネットワークへの参加が許可されるようにします。*list-name* には、認証方式のリストを指定します。クライアント デバイスがオープンまたは EAP 認証のどちらかを使用してアソシエートでき、認証されるようにするには、optional キーワードを使用してください。この設定は、おもに特殊なクライアントアクセス可能性を必要とするサービス プロバイダで使用されています。

（注） EAP 認証に設定されているルート デバイスは、アソシエートするすべてのクライアント デバイスに EAP 認証を実行させます。EAP を使用していないクライアント デバイスはルート デバイスと通信できません。

- **authentication shared**

  [**mac-address** *list-name*] [**eap** *list-name*]

  — （オプション）SSID の認証タイプを共有キーに設定します。

  （注） 共有キーのセキュリティには欠陥があるため、使用しないことをお勧めします。

  （注） 共有キーによる認証は、1 つの SSID にのみ割り当てることができます。

  — （オプション）SSID の認証タイプを共有キー（MAC アドレス認証を使用）に設定します。*list-name* には、認証方式リストを指定します。

  — （オプション）SSID の認証タイプを共有キー（EAP 認証を使用）に設定します。*list-name* には、認証方式リストを指定します。

- **authentication network-eap** *list-name* [**mac-address** *list-name*]

  — （オプション）SSID の認証タイプを EAP 認証とキーの配布に設定します。

  — （オプション）SSID の認証タイプを Network-EAP（MAC アドレス認証を使用）に設定します。アクセス ポイントにアソシエートするすべてのクライアント デバイスが、MAC アドレス認証を実行する必要があります。*list-name* には、認証方式リストを指定します。

- **authentication key-management** {[wpa] [cckm]} [optional]

  — （オプション）SSID のキー管理タイプを WPA、CCKM、または両方に設定します。**optional** キーワードを使用すると、WPA または CCKM に設定されていないクライアント デバイスがこの SSID を使用できます。**optional** キーワードを使用しないと、WPA または CCKM クライアントのみが SSID を使用できます。SSID に対して CCKM を有効にするには、Network-EAP 認証も有効にする必要があります。SSID に対して WPA を有効にするには、オープン認証または Network-EAP 認証、もしくは両方を有効にする必要があります。

（注） 802.11b 無線と 802.11g 無線のみが WPA と CCKM を同時に有効にできます。

（注） CCKM または WPA を有効にする前に、暗号化モードを TKIP/AES-CCMP を含む暗号化スイートに設定する必要があります。CCKM と WPA の両方を有効にするには、暗号化モードを TKIP を含む暗号化スイートに設定する必要があります。

（注） 事前共有キーのない SSID の WPA を有効にした場合、キー管理タイプは WPA です。事前共有キーのある WPA を有効にした場合、キー管理タイプは WPA-PSK です。

（注） CCKM をサポートするには、ルート デバイスがネットワーク上の WDS デバイスとやりとりする必要があります。

dot1x 資格情報の設定

この項では、EAP で使用する dot1x 資格情報を設定するコマンドについて説明します。また、各コマンドのコマンド コンポーネントとオプション設定コンポーネントについても説明します。

1. **eap profile** *profile-name-string*

   EAP プロファイルを作成します。

2. **dot1x credentials** *profile*

   dot1x 資格情報プロファイルを作成し、dot1x 資格情報設定サブモードを入力します。

3. **method [fast|gtc|leap|md5|mschapv2|tls]**

   認証目的で EAP 認証方式を選択します。

（注） EAP 認証に設定されているデバイスは、アソシエートするすべてのルート デバイスに EAP 認証を実行させます。EAP を使用していないルート デバイスはデバイスと通信できません。

4. **dot11 ssid** *ssid-string*
5. **authentication network-eap** *list-name*

   （オプション）SSID の認証タイプを EAP 認証とキーの配布に設定します。

6. **dot1x credentials** *profile*

   dot1x 資格情報プロファイルを作成し、dot1x 資格情報設定サブモードを入力します。

7. **dot1x eap profile** *profile-name-string*

   EAP プロファイルを指定します。これは上記の手順 2 で作成したプロファイルです。

8. **authentication key-management {[wpa] [cckm]} [optional]**

   （オプション）SSID のキー管理タイプを WPA、CCKM、または両方に設定します。**optional** キーワードを使用すると、WPA または CCKM に設定されていないクライアント デバイスがこの SSID を使用できます。**optional** キーワードを使用しないと、WPA または CCKM クライアント

のみが SSID を使用できます。SSID に対して CCKM を有効にするには、Network-EAP 認証も有効にする必要があります。SSID に対して WPA を有効にするには、オープン認証または Network-EAP 認証、もしくは両方を有効にする必要があります。

（注） 802.11b 無線と 802.11g 無線のみが WPA と CCKM を同時に有効にできます。

（注） CCKM または WPA を有効にする前に、暗号化モードを TKIP/AES-CCMP を含む暗号化スイートに設定する必要があります。CCKM と WPA の両方を有効にするには、暗号化モードを TKIP を含む暗号化スイートに設定する必要があります。

（注） 事前共有キーのない SSID の WPA を有効にした場合、キー管理タイプは WPA です。事前共有キーのある WPA を有効にした場合、キー管理タイプは WPA-PSK です。

（注） CCKM をサポートするには、ルート デバイスがネットワーク上の WDS デバイスとやりとりする必要があります。

AES 暗号化を使用した EAP-TLS 認証の例

SSID を無効にする、または SSID 機能を無効にするには、SSID コマンドの **no** フォームを使用します。この例では、SSID *bridgeman* の認証タイプをオープン（EAP 認証を使用）に設定します。SSID *bridgeman* を使用したブリッジは、EAP 方式名 *adam* を使用して EAP 認証を試みます。この例では、SSID *bridgeman* の認証タイプを設定して、EAP-TLS 認証（AES 暗号化を使用）を実行します。この SSID を使用したブリッジは、サーバ ID *adam* を使用して EAP 認証を試みます。

```
!
dot11 ssid bridgeman
authentication open eap eap_adam
authentication network-eap eap_adam
authentication key-management wpa
infrastructure-ssid
!
!
interface dot11radio 0
encryption mode ciphers aes-ccm
ssid bridgeman
!
```

このブリッジにアソシエートされたワークグループ ブリッジ、非ルート ブリッジ、およびリピータ ブリッジでの構成は、次のコマンドも含みます。

```
!
eap profile authProfile
method tls
exit
!
dot1x credentials authCredentials
username adam
password adam
!
dot11 ssid bridgeman
authentication open eap eap_adam
authentication network-eap eap_adam
authentication key-management wpa
dot1x eap_profile authProfile
dot1x credentials authCredentials
infrastructure-ssid
!

interface dot11radio 0
encryption mode ciphers aes-ccm
ssid bridgeman
!
!
```

この例は、EAP 認証のルート側の RADIUS/AAA 設定を示します。

```
!
aaa new-model
aaa group server radius rad_eap
server 13.1.1.99 auth-port 1645 acct-port 1646
!
aaa authentication login eap_adam group rad_eap
aaa session-id common
radius-server host 13.1.1.99 auth-port 1645 acct-port 1646 key 7 141B1309
radius-server authorization permit missing Service-Type
ip radius source-interface BVI1
!
```

WDS と対話するルート デバイスの設定

CCKM を使用した非ルート ブリッジをサポートするには、使用しているルート デバイスがネットワーク上の WDS デバイスと対話する必要があり、認証サーバがルート デバイスのユーザ名とパスワードで構成されている必要があります。無線 LAN に WDS と CCKM を設定する方法については、次の URL にある『Cisco IOS Software Configuration Guide for Cisco Access Points』の第 11 章を参照してください。
http://www.cisco.com/en/US/docs/wireless/access_point/12.2_13_JA/configuration/guide/i12213sc.html

ルート デバイスで、次のコマンドをグローバル設定モードで入力します。

```
bridge(config)# wlccp ap username username password password
```

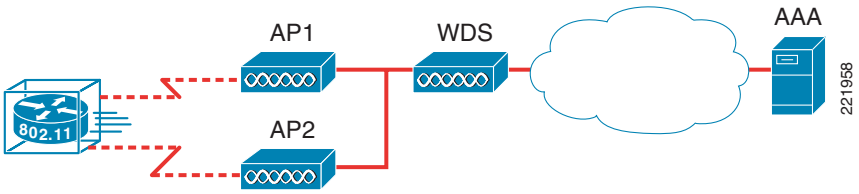
(注)　ルート　デバイスを認証サーバ上のクライアントとしてセットアップしたときと同じユーザ名とパスワードを設定する必要があります。

この WDS/CCKM 構成では、クライアントと AP は次のように対話します。

- AP1 と AP2 が WDS を認証する
- WDS がクライアントのセキュリティ資格情報をキャッシュする
- アソシエーションで、AP1 はキー関連情報を取得し、セッションに必要な動的キーを生成する
- 再アソシエーションで、AP2 がキー関連情報を取得し、セッションの動的キーを生成する
- RADIUS サーバに対して、クライアントが 1 度だけ認証を行う

図 11-5 は、クライアント、AP、および WDS の関係を示しています。

図 11-5　WDS と CCKM の対話



WPA のその他の設定

事前共有キーをブリッジに設定して、グループのキー アップデートの頻度を調整するには、2 とおりの設定が可能です。

事前共有キーの設定

802.1x ベースの認証が利用できない無線 LAN 上の WPA をサポートするためには、ブリッジ上に事前共有キーを設定する必要があります。事前共有キーは ASCII 文字または 16 進数として入力できます。キーを ASCII 文字として入力する場合は 8 ～ 63 文字を入力します。ブリッジは、「Password-based Cryptography Standard」（RFC2898）で規定されているプロセスに従ってこのキーを展開します。キーを 16 進数として入力する場合は、64 桁の 16 進数を入力する必要があります。WPA-PSK は、一部の既知の攻撃ツールに対して脆弱性があるので注意してください。ただし、WPA-PSK 認証メカニズムは、小規模から中規模のビジネスやエンタープライズ ネットワークではなく、コンシューマ ネットワークでの使用向けであり、エンタープライズクラスの WGB やメッシュ環境での使用はお勧めしません。

幸運なことに、オフラインの辞書攻撃は WPA-PSK ネットワークにはそれほど効果がありません。これは IEEE が PSK ハッシュとして pbkdf2 アルゴリズムを選択したためです。20 文字に満たないパスフレーズから生成されたキーは、辞書攻撃を受ける可能性が高くなります。WPA-PSK を使用する場合は、真ランダム キーのみを使用することをお勧めします。

グループ キー更新の設定

WPA プロセスの最後の段階で、ルート デバイスは、認証された非ルート ブリッジにグループ キーを配布します。次のオプションの設定を使って、非ルート ブリッジのアソシエーションとアソシエーション解除をベースにして、グループ キーを変更、配布するようにルート デバイスを設定できます。

- Membership termination：ルート デバイスは、任意の認証された非ルート ブリッジがルート デバイスからアソシエーションを解除するときに、新しいグループ キーを生成、配布します。この機能は、グループキーが現在アソシエートしているブリッジでのみ利用できるようにします。

- Capability change ルート デバイスは、最後の非キー管理の非ルート ブリッジがアソシエーションを解除するときに動的グループ キーを生成および配布し、最初の非キー管理の非ルート ブリッジが認証するときに、静的に設定されたキーを配布します。WPA 移行モードでは、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。

特権 EXEC モードから、次の手順に従って、WPA 事前共有キーとグループ キー更新オプションを設定します。

1. SSID の SSID 設定モードを入力します。

   ```
   dot11 ssid ssid-string
   ```

2. ブリッジの事前共有キーを、静的 WEP キーも利用する WPA を使って入力します。

   ```
   wpa-psk { hex | ascii } [ 0 | 7 ] encryption-key
   ```

   16 進数または ASCII 文字を使用してキーを入力します。16 進数を使用する場合は、256 ビットのキーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合は、8 桁以上の文字、数字、または記号を入力する必要があります。入力したキーをブリッジが展開します。ASCII 文字は 63 文字まで入力できます。

WPA と事前共有キーの設定例

次の例は、WPA および静的 WEP を使用する非ルート ブリッジ用の事前共有キーを、グループ キー更新オプションと共に設定する方法を示しています。

```
!
!
dot11 ssid given-ssid
wpa-psk ascii talboeitm65
!
!
```

Cisco 3200 シリーズ製品の詳細

Cisco 3200 シリーズのインターフェイス

上記の項で説明したとおり、3200 MAR シリーズのルータは、アプリケーションのニーズに合わせてさまざまな PC104/Plus モジュールでカスタム設計できます。複数のイーサネットとシリアル インターフェイス用のルータ、および最大 3 枚の WMIC カードを設計できます。ルータ自体は、*カード*と呼ばれるスタック可能な PC104/Plus モジュールで構成されています。次のカード構成が可能です。

- 2.4 GHz 無線 WMIC x 2
- 4.9 GHz WMIC x 1
- Fast Ethernet Switch Mobile Interface Card（FESMIC; ファースト イーサネット スイッチ モバイル インターフェイス カード）x 1
- Serial Mobile Interface Card（SMIC; シリアル モバイル インターフェイス カード）x 1
- Mobile Access Router Card（MARC; モバイル アクセス ルータ カード）x 1

図 11-6 は、このスタック可能なカード構成を示しています。一般的な用途向けとして、Rugged Enclosure 3230 および 3270 バンドルが用意されています。

図 11-6　カードの接続

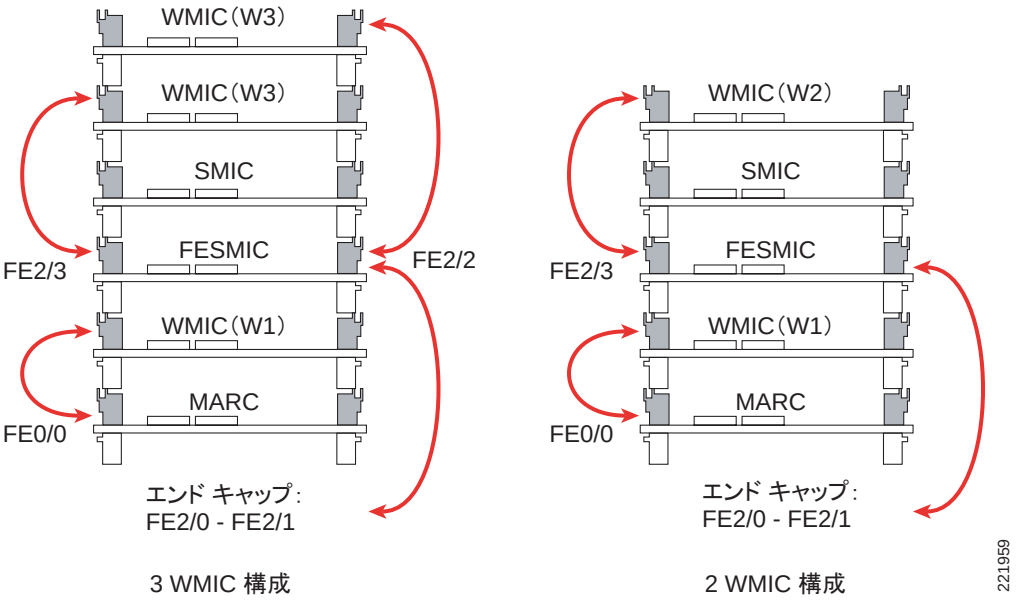


図 11-6 では、3200 MAR の 2 つの構成例が示されています。

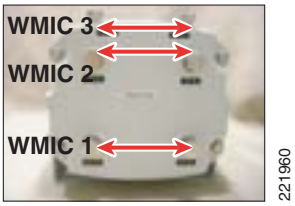
- WMIC x 2、FESMIC x 1、SMIC x 1、MARC x 1
- WMIC x 3、FESMIC x 1、SMIC x 1、MARC x 1

3200 MAR の構成オプションの詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd800fe973.html

Cisco 3230 エンクロージャの接続

Cisco 3230 MAR エンクロージャの背面には、3 組の RP-TNC コネクタがあります。各組が 1 枚の WMIC カードに対応しています。下の組は W1 カード用です。その上の組は W2 用です。モバイル ルータの最上部の組は W3 用です。図 11-7 はアンテナ接続を示しています。

図 11-7　WMIC RP TNC ロケーション



次の表は、ポートとインターフェイスの関係を示したもので、3200 MAR に別のデバイスを接続する必要がある場合に役立ちます。

表 11-2 は、Cisco 3230 MAR での WMIC セットアップを示しています。

表 11-2　WMIC ポート

	内部配線ポート
WMIC 1（W1）	FastEthernet 2/1
WMIC 2（W2）	FastEthernet 2/3
WMIC 3（W3）	FastEthernet 2/2

表 11-3 は、Cisco 3230 MAR 上のシリアル インターフェイスのセットアップを示しています。

表 11-3　SMIC ポート

	内部配線ポート	インターフェイス タイプ
シリアル 0	Serial 1/0	DSCC4 シリアル
シリアル 1	Serial 1/1	DSCC4 シリアル
内部	Serial 1/2	DSCC4 シリアル
内部	Serial 1/3	DSCC4 シリアル

Cisco 3270 Rugged Enclosure の構成

新しくリリースされた Cisco 3270 モバイル アクセス ルータは、ポート密度、ファイバ、ギガビット イーサネット機能を向上します。プラットフォームに内部変更により、より大きなプロファイルが必要となりました。高性能 3270 ルータ カードとその追加インターフェイスを収容するために、3270 の Rugged Enclosure のサイズは、3230 バンドルに使用された Rugged Enclosure の約 2 倍となっています。これにより、Cisco 3230 バンドルの Rugged Enclosure では収容可能カード数が最大 7 枚であったことと比べても、はるかに多くの PC104+ カードの増設が可能となりました。

Cisco 3270 ルータでは、WMIC を内部接続するという概念は変わらず保持されています。WMIC の相互接続性は、3230 バンドルに関して前述の項で説明したものとまったく同じです。3270 エンクロージャのエンド キャップを最大限有効に利用するため、WMIC を使用しないときは、RJ-45 WMIC コンソール ポートをファスト イーサネット ポートに変換できるようになっています。これらの接続を 図 11-8 に示します。

図 11-8　Cisco 3270

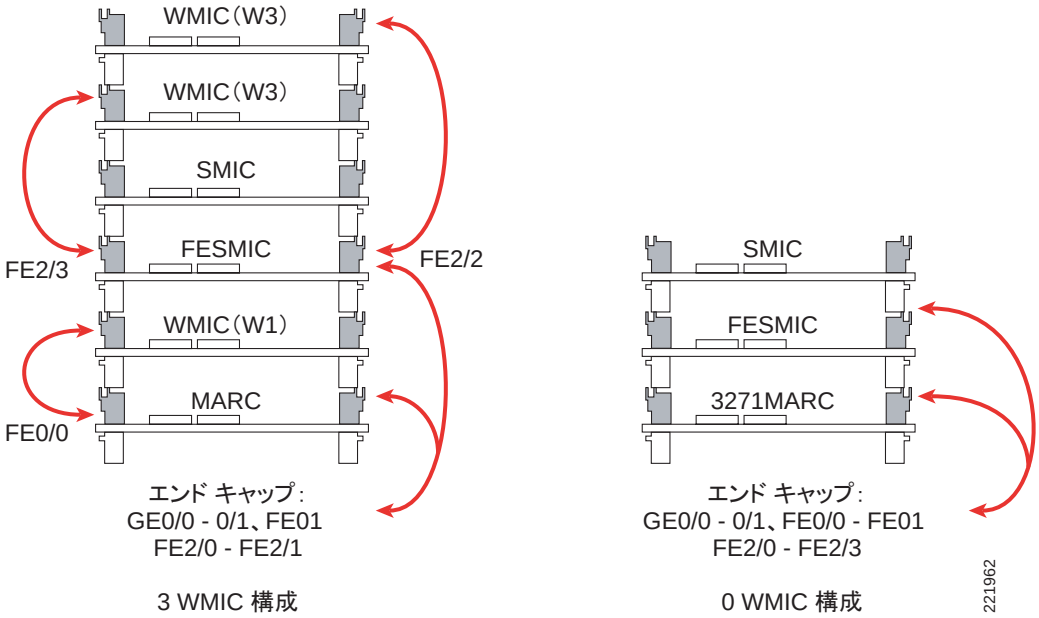
3270 エンクロージャでは、未使用の RJ-45 WMIC コンソール ポートを、エンド キャップ上のファスト イーサネット インターフェイスに変換する機能を備えるため、3270 の 8 つのポートすべてをエンド キャップのコネクタに引き出すことができます。また、3270 は、エンド キャップのコネクタに引き出すスマート シリアル インターフェイスを通じて非同期 / 同期シリアル ポートの機能を保持します。

Cisco 3270 Rugged Router は、有線または無線ネットワークから同時に実行される複数のアプリケーションをサポートするように設計された高パフォーマンス プロセッサ カードです。オンボード ハードウェアの暗号化により、Cisco 3270 は暗号化プロセスをルータ CPU からオフロードし、モバイル ネットワーク向けに安全なデータ サービスを提供します。

Cisco 3251 Mobile Access Router Card（MARC）の約 2 倍のフォーム ファクタを持つ Cisco 3270 では、ファイバ、ギガビット イーサネット コッパー、USB などさまざまなネットワーク インターフェイスを選択できるほか、より多くの周辺機器を接続できます。さらに、Cisco 3270 は、将来のカード拡張に備えて PC/104-Plus カードの 2 番目のスタックに対応でき、上記の 3201 Mobile Interface Card は完全サポートしています。

図 11-9 は、Cisco 3270 MAR の 2 つの構成例を示しています。

図 11-9　3270 WMIC の構成オプション



詳細は、次の URL にある Cisco 3200 Rugged Enclosure のデータ シートを参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/products_data_sheet0900aecd804c207b.html

Cisco 3200 シリーズ WMIC の機能

Cisco IOS を実行する WMIC には次のソフトウェア機能が備わっています。

- VLAN

  dot1Q VLAN は、無線インターフェイスとイーサネット インターフェイスの両方でトランクできます。システムごとに最大 32 個の VLAN をサポートできます。

- QoS

  無線インターフェイス上のトラフィックに優先順位を付け、サービスの品質を維持するための機能です。WMIC では、QoS で WMM に必要な要素がサポートされます。WMM によって、Wi-Fi 無線接続を経由したオーディオ、ビデオ、および音声アプリケーションのユーザ エクスペリエンスが向上します。WMM は、IEEE 802.11e QoS 仕様のサブセットの 1 つです。WMM は EDCA 方法を使用して、QoS 優先メディア アクセスをサポートします。

- 複数の BSSID

  アクセス ポイント（AP）モードでは、最大 8 個の BSSID がサポートされます。

- RADIUS アカウンティング

  WMIC を AP モードで実行する場合、WMIC のアカウンティングを有効にして、認証されている無線クライアント デバイスに関するデータをネットワーク上の RADIUS サーバに送信できます。

- TACACS+ 管理者認証

  TACACS+ では、サーバベースの詳細なアカウンティング情報、および認証プロセスと認可プロセスにおける柔軟性のある管理上の制御を実現できます。TACACS+ では、WMIC にアクセスしようとする管理者をセキュアに集中化して検証できます。

- 拡張セキュリティ

  次の 3 つの高度なセキュリティ機能がサポートされます。

  — WEP キー：Message Integrity Check（MIC; メッセージ完全性チェック）および WEP キー ハッシュ CKIP

  — WPA

  — WPA2

- 拡張認証サービス

  非ルート ブリッジまたはワークグループ ブリッジで、他の無線クライアント デバイスと同様にネットワークに対して認証を実行できます。非ルート ブリッジまたはワークグループ ブリッジにネットワークのユーザ名とパスワードを設定すると、LEAP、EAP-TLS、または EAP-FAST を使用して、WEP、WPA、または WPA2 設定で認証を実行できます。

- 802.1x オーセンティケータ

  AP モードでは、MAR は、WLAN クライアントとして標準の 802.1x EAP タイプをサポートします。

- 迅速でセキュアなローミング

  WGB モードと UWGB モードの CCKM を使用します。

- ユニバーサル ワークグループ ブリッジ

  クライアントとしてシスコ以外の AP との相互運用性をサポートします。

- Repeater モード

  アクセス ポイントが、無線リピータのように機能して、無線ネットワークのカバレッジ領域を拡張できます。

Cisco 3200 シリーズ ブリッジの考慮事項

Cisco **C**ompatible eXtensions（CCX）プログラムでは、高度な WLAN システム レベル機能およびシスコ固有の WLAN の技術を、サードパーティ製の Wi-Fi 対応ラップトップ、WLAN アダプタ カード、PDA、WI-FI 電話、および Application Specific Device（ASD）で実現できます。2.4 GHz WMIC では、CCX クライアントがサポートされます。2.4 GHz WMIC をユニバーサル ワークグループ ブリッジ クライアントとして設定すると、2.4 GHz WMIC は自身を Cisco Compatible Extension クライアントとして識別しません。ただし、Cisco Compatible Extension の機能をサポートします。表 11-4 はサポートされている機能を示しています。

Cisco Compatible Extensions プログラムの詳細は、次の URL にある Cisco Compatible Extensions のホーム ページを参照してください。
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html

表 11-4　Cisco Compatible Extensions Version 機能のサポート

機能	v1	v2	v3	v4	AP	WGB	WGB クライアント
セキュリティ							
Wi-Fi Protected Access（WPA）		X	X	X	X	X	X
IEEE 802.11i - WPA2			X	X	X	X	X
WEP	X	X	X	X	X	X	X
IEEE 802.1X	X	X	X	X	X	X	X
• LEAP	X	X	X	X	X	X	X
• EAP-FAST			X	X	X	X	X
CKIP（暗号化）	X				X	X	

表 11-4　Cisco Compatible Extensions Version 機能のサポート（続き）

機能	v1	v2	v3	v4	AP	WGB	WGB クライアント
Wi-Fi Protected Access（WPA）： 802.1X + WPA TKIP		X	X	X	X	X	X
• LEAP 対応		X	X	X	X	X	X
• EAP-FAST 対応			X	X	X	X	X
IEEE 802.11i- WPA2: 802.1X+AE			X	X	X	X	X
• LEAP 対応			X	X	X	X	X
• EAP-FAST 対応			X	X	X	X	X
CCKM EAP-TLS				X	X	X	X
EAP-FAST				X	X	X	X
モビリティ							
AP 支援ローミング		X	X	X	X	X	X
CCKM および LEAP を使用した迅速な再認証		X	X	X	X	X	X
CCKM および EAP-FAST を使用した迅速な再認証			X	X	X	X	X
MBSSID				X	X		
キープアライブ				X	X	X	
QoS と VLAN							
複数の SSID および VLAN をサポートする AP との相互運用性	X	X	X	X	X	X	
Wi-Fi Multimedia（WMM）			X	X	X	X	X
パフォーマンスと管理							
AP 固有の最大送信電力		X	X	X	X	X	X
自動保護切り替え（ASP）のためのプロキシ ARP 情報の要素の認識			X	X	X		
クライアント ユーティリティの標準化							
リンク テスト				X	X	X	X

ソフトウェアの機能とモバイル IOS 機能のサポートに関する詳細なリストは、次の URL にある『Cisco 3200 Series Mobile Access Router Software Configuration Guide』を参照してください。
http://www.cisco.com/en/US/products/hw/routers/ps272/products_configuration_guide_chapter09186a00800c797a.html#wp1035566.

Cisco 3200 シリーズの管理オプション

WMIC は次のインターフェイスを通じて管理できます。

- IOS Command-Line Interface（CLI; コマンドライン インターフェイス）。ターミナル エミュレーション ソフトウェアまたは Telnet/SSH セッションを実行している PC から使用します。IOS CLI には、WMIC コンソール接続、Telnet、または SSH からアクセスできます。
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）。
- Web GUI 管理。

CHAPTER 12

Cisco Unified Wireless とモバイル IP

はじめに

郵便の手紙が封筒に記載された住所に配達されるのと同じように、IP ネットワークでは、固定 IP アドレスに基づいてルーティングが行われます。ネットワーク上のデバイスには、そのネットワークで割り当てられた IP アドレスに従い、通常の IP ルーティングで到達できます。ただし、モバイル ネットワークの場合、デバイスが自分のホーム ネットワークから離れた場所へ移動すると、通常の IP ルーティングでは到達できません。そのため、そのデバイスのアクティブ セッションが終了してしまいます。

モバイル IP を使用すると、無線事業者が同じかどうかにかかわらず、ユーザが別のネットワークへ移動したときも同じ IP アドレスが維持されるので、個々のローミング クライアントはセッションまたは接続を中断せずに通信を続けることができます。モバイル IP のモビリティ機能は物理レイヤではなくネットワーク レイヤで実行されるため、モバイル デバイスは接続と実行中のアプリケーションを維持しながら異なるタイプの無線ネットワークや有線ネットワークを移動できます。個々のユーザがネットワーク境界を越えてローミングする間も通信の中断を避けるべきアプリケーションとして、リモート ログイン、リモート印刷、ファイル転送があげられます。また、ソフトウェア ライセンスやアクセス特権など、特定のネットワーク サービスも IP アドレスをベースにしています。これらの IP アドレスを変更すると、ネットワーク サービスが損なわれる可能性があります。

この章では、Cisco Unified Wireless Network を介したモバイル IP クライアントの相互関係について説明します。内容は次のとおりです。

- さまざまなレベルのモビリティ
- モビリティ ソリューションの要件
- Cisco Unified Wireless Network でのローミング
- モバイル IP 対応ネットワークでのローミング
- Cisco Unified Wireless Network でのローミング時のモバイル IP クライアントの特徴

さまざまなレベルのネットワーク モビリティ

ネットワーク モビリティには、次の 2 つのレベルがあります。

- 特定のレイヤ 2 ネットワーク内でのレイヤ 2 ローミング
  - すべての AP がトランクなしに同一のサブネット上にあります。
- 特定のレイヤ 2 ネットワークでのレイヤ 3 ローミング
  - Cisco Unified Wireless Network
  - モバイル IP クライアント

特定のレイヤ 2 ネットワークでのレイヤ 2 ローミング（図 12-1 を参照）の例として、すべての AP WLAN が同一のサブネット上にあり、AP 間でクライアントがローミングする無線ネットワークがあります。このタイプの展開では、クライアントは、クライアント IP アドレスの変更またはネットワークでのモビリティの認識を必要とせずに 1 つの AP から別の AP にローミングできます。

特定のレイヤ 2 ネットワークでのレイヤ 3 ローミングは、前の AP の例と同様ですが、ここではクライアントが WLAN 間をローミングするときにそのまま同じサブネット上にいることも、別のサブネット上に移動することもできます。この例を 図 12-2 に示します。モバイル IP によるレイヤ 3 ローミングを採用することで、まったく別のレイヤ 2 ネットワーク間（セルラー、有線、802.11 無線）でのローミングが可能になります。図 12-3 は、クライアントが有線ネットワークから別のサブネット上の無線ネットワークにローミングする例を示しています。

シームレス モビリティでは、モバイル クライアント アプリケーションとリモート アプリケーションの両方が、エンドツーエンド IP アドレス指定での変更を認識しません。エンド アプリケーションでは、これらの IP アドレスを、配信不可になるかどうかにかかわらずデータ パケットで使用するか、またはデータ パケットに埋め込むことができます。これによって、2 つのクライアントが有線ネットワーク上にあり、モバイルではない状況がエミュレートされます。Cisco Unified Wireless Network およびモバイル IP では両方ともシームレス モビリティが提供されます。

Cisco Unified Wireless Network は、特定のレイヤ 2 ネットワークでのシームレスなレイヤ 3 ローミングの例で、モバイル IP（RFC 3344）を使用するクライアントは、任意のレイヤ 2 ネットワークでのシームレスなレイヤ 3 ローミングの例です。つまり、Cisco Wireless Unified Network では、レイヤ 3 ローミングはモビリティ グループ内の AP 間のローミングに制限されます。モバイル IP を使用すると、任意のレイヤ 2 ネットワーク（有線、802.11 無線、またはセルラー）をローミングに使用できます。Cisco Unified Wireless Network と Mobile IP ソリューションの両方で同じような機能が実行されるため、同様のコンポーネントが必要です。

図 12-1　レイヤ 2 でのネットワーク ローミング例

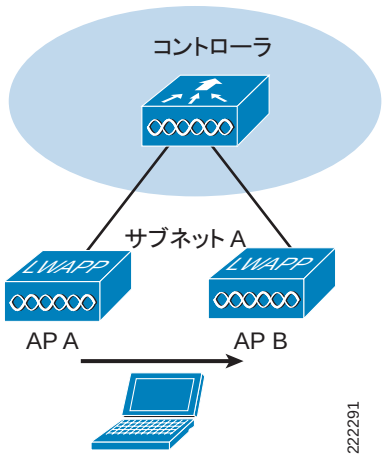


図 12-2　レイヤ 3 での CUWN ローミング例

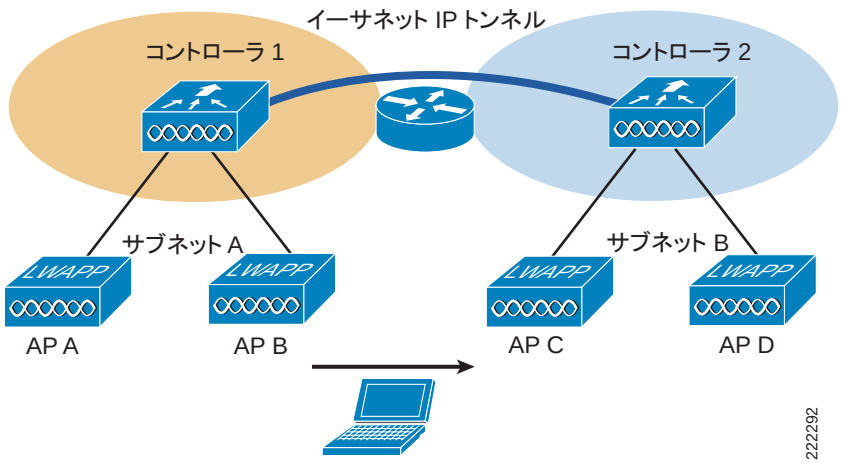
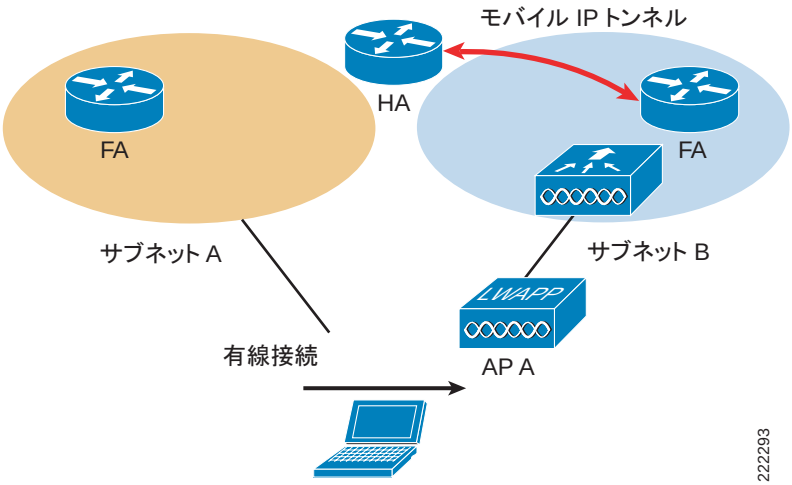


図 12-3　レイヤ 3 でのモバイル IP ローミング例



モビリティ ソリューションの要件

次の要件はすべてのモビリティ ソリューションに適用されます。

- ロケーション データベース
- 移動の検出
- ロケーションの検出
- アップデート シグナリング
- パスの再確立

これらの要件は、以降の項で説明します。

(注)　ここで説明するロケーション データベースは、第 13 章「Cisco Unified Wireless ロケーションベース サービス」で説明されている Location-Based Services（LBS; ロケーションベース サービス）のロケーション データベースとは関係ありません。

ロケーション データベース

Cisco Unified Wireless Network では、ファースト ホップ ルータが、ネットワークで実行されているルーティング プロトコル経由で無線クライアント宛てのパケットを受信し、それらのパケットをトランク経由で WLC に転送します。各 WLC では、WLC に登録されている AP 間で無線クライアントがローミングするときに、それらの無線クライアントのデータベースが保存されます。無線クライアントが次に別の WLC（外部 WLC）上の AP にローミングした場合、その WLC はモビリティ グループ内の他の WLC に照会して、これが新しいクライアントかローミング クライアントかを確認します。これがローミング クライアントの場合は、ホーム WLC の近くのファースト ホップ ルータは引き続き無線クライアント宛てのパケットを受信しますが、アソシエートされている AP の 1 つにそれらのパケットを転送する代わりに、外部 WLC に転送したのち、クライアントに転送します。Cisco Unified Wireless Network でのローミングについては、第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」で詳しく説明します。詳細は、ローミング（P. 2-18）を参照してください。

モバイル IP では、Home AgentHA; ホーム エージェント）がロケーション データベースを含みます。HA ではネットワーク ルーティング プロトコルが実行されるため、HA はモバイル IP クライアント宛てのパケットを受信して、そのクライアントの現在のロケーションにパケットを転送します。Cisco Unified Wireless Network とは異なり、HA は WLC 間の分散データベースを保持しません。HA は、他の HA に照会することはありません。HA に関する限り、ロケーション データベースは 1 つだけで、それは HA 自体です。これが、2 つのソリューションのロケーション データベース メカニズムが異なる点です。

移動の検出、ロケーションの検出、およびアップデート シグナリング

無線クライアントが新しい AP にローミングする場合、無線クライアントは無線ネットワークにアソシエートする必要があります。アソシエーション プロセスで、アソシエーション パケットは WLC に転送され、無線クライアントおよび無線クライアントのアソシエート試行元のロケーション（AP）が識別されます。この情報は、WLC が自身のロケーション データベース（WLC モビリティ データベース）のアップデートに使用します。クライアントが別の WLC にローミングした場合、この無線クライアントの元の WLC から、無線クライアント宛てのパケットがリモート WLC に転送されます。

モバイル IP では、モバイル IP クライアントが無線ネットワークに接続する際に HA に情報は何も提供されません。また、クライアントは自身がネットワーク間を移動したことを認識する必要があります。クライアントは通常、移動を 2 つの方法で検出します。1 つ目の方法は、Media Sense と呼ばれる Windows オペレーティング システムのレイヤ 2 通知機能です。この機能では、AP 間のローミング時に異なるレイヤ 2 メディアの接続解除および再接続が検出され、検出の発生時に Windows オペレーティング システムに信号が送信されます。これによって、インターフェイスで DHCP アドレスの DHCP サーバとの再ネゴシエーションを試行できます。移動検出の 2 つ目の方法では、Foreign Agent（FA; 外部エージェント）アドバタイズメントを使用します。FA アドバタイズメントは、モバイル IP クライアントに、このクライアントのサブネットを通知します。モバイル IP クライアントがこれらの定期的なメッセージのいずれかを受信すると、このクライアントが新しいサブネットに移動したことがわかります。これらの移動検出方法は通常、モバイル IP で使用されます。RFC 3344 には他の方法が指定されていますが、それらの方法は通常、使用されません。

モバイル IP では、ロケーションの検出は通常、次の 2 つの方法のいずれかで実行されます。1 つ目の方法では、モバイル IP は FA 宛ての IP アドレスを通知する FA アドバタイズメントを受信します。モバイル IP クライアントはこのアドレスを、FA からすでに入手していたアドレスと比較して、FA アドバタイズメントが新しい FA からである場合は通知します。次に、モバイル IP クライアントは、HA が新しい FA に新しいトンネルを構築してモバイル IP クライアントにパケットを転送できるように、HA に IP アドレスを転送します。2 つ目の方法では、クライアントは独自の FA として機能し、新しい DHCP IP アドレスを受信して、ロケーションが新しくなったことを HA に通知します。この時点で、HA はパケット転送用の、クライアントへのトンネルを構築できます。これは、連結型気付アドレスと呼ばれます。

Cisco Unified Wireless Network では、移動の検出は、無線クライアントの現在のアソシエート先の AP を認知しているネットワークによって実行されます。アップデート シグナリングは、無線クライアントから WLC に送信される最初のパケットによって実行されます。アップデート プロセスについては、第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」で詳しく説明します。詳細は、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps6590/products_ios_protocol_group_home.html.

パスの再確立

パスの再確立は、ロケーション データベースを含む HA からのクライアント宛てのパケットをクライアントで受信できるようにするためのメカニズムです。通常、元のパケットのカプセル化にはトンネリング メカニズムが使用されます。Cisco Unified Wireless Network では、パケットはアソシエートされている AP の無線クライアントに「常に稼動している」LWAPP トンネル経由で転送されます。WLC では、別の WLC にローミングした無線クライアントからモビリティ グループ内の他の WLC に転送されるすべてのパケットに対して動的 Ethernet over IP トンネルが使用されます。

モバイル IP では、複数のタイプのトンネル（GRE、UDP、および IP in IP を使用でき、使用されるトンネルのタイプは、モバイル IP クライアントと HA 間の機器、および HA でそのタイプのカプセル化がサポートされているかどうかによって異なります。たとえば、HA でクライアントが NAT ゲートウェイの背後にあることが検出された場合、HA では UDP トンネリングが使用されます。モバイル IP クライアントが GRE トンネリングを要求し、HA でそのトンネリングがサポートされている場合は、GRE が使用されます。通常、モバイル IP クライアントは IP in IP トンネリングを要求し、RFC 準拠のすべてのクライアントでこのタイプのトンネリングがサポートされます。

Cisco Unified Wireless Network でのローミング

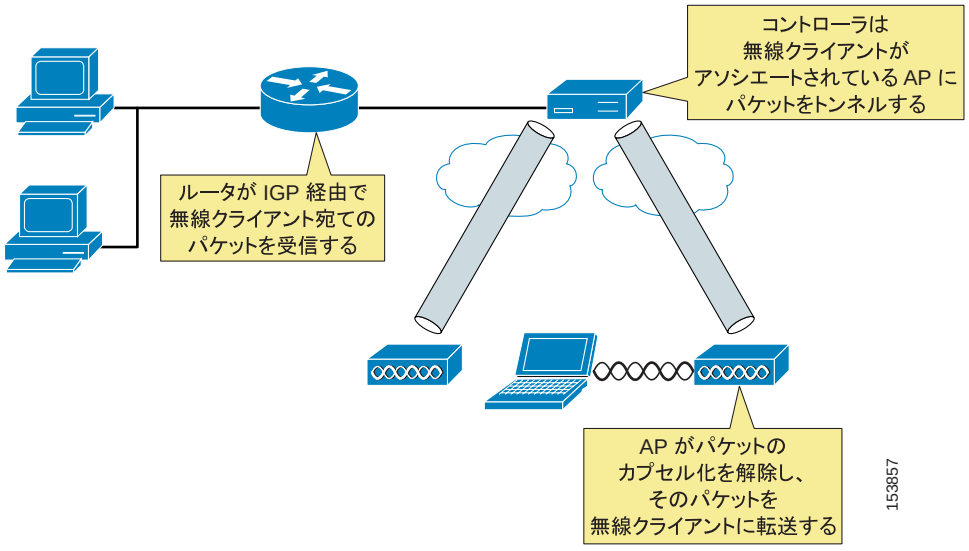
Cisco Unified Wireless Network は、無線クライアントに対するモビリティ プロキシとして機能します。これによって、ソフトウェアの追加や無線クライアントに関する追加情報を必要とせずに、ネットワークで無線クライアントに対してシームレスなモビリティを提供できるようになります（図 12-4 を参照）。

無線クライアントが AP にアソシエートされている場合、この AP は、WLC と AP の間に設定されている LWAPP トンネル経由でクライアントのパケットを WLC に転送します（LWAPP トンネルは AP のブート時に AP と WLC の間に設定されます）。WLC では、LWAPP トンネルの使用によって次の処理を実行できます。

- クライアントのアソシエート先の AP を認知する（LWAPP トンネルのエンドポイント）
- トンネルを経由してパケットをクライアントに転送して返す
- AP から複数ホップ離れている場合でもクライアントのトラフィックを受信する
- 無線クライアントとの送受信でパケットをフィルタする

クライアントでは、LWAPP トンネルの使用によって、デフォルト ゲートウェイが、物理的には複数ホップ離れている場合でも 1 ホップ離れているかのように見えます。

図 12-4　Cisco Unified Wireless Network でのローミング



クライアントが DHCP アドレスを要求すると、WLC はローカル DHCP プール（定義されている場合）からクライアントにアドレスを渡すか、DHCP 要求に外部 DHCP サーバのゲートウェイ アドレスを指定します。いずれの場合でも、WLC は DHCP サーバのアドレスが WLC 仮想インターフェイスのアドレスに設定されるように DHCP 応答内容を変更します。仮想 IP アドレスがルーティング テーブル（通常は 1.1.1.1）にない場合でも、WLC は、AP 間でのローミング時に（Microsoft Media Sense を使用している）Microsoft Windows オペレーティング システムで生じる無線クライアントの DHCP 更新を代行受信できます。また、同一アドレスがすべての WLC の仮想インターフェイスに含まれる場合、クライアントが別の WLC にアソシエートされている新しい AP にローミングしたとき、そのクライアントから送信される DHCP 更新を他の WLC は代行受信できます。

WLC は単に、無線クライアントの現在のロケーションを追跡して、そのクライアント宛てのパケットを適切な LWAPP トンネルからアソシエートされている AP に転送します。そのため、無線クライアントは、コントローラに登録されている AP 間で簡単にローミングできます。別の WLC に登録されている AP にクライアントがローミングすると、リモート WLC がモビリティ グループに照会して、クライアントがローミングしたかどうかを確認します。ローミングした場合、Ethernet over IP トンネルが設定され、クライアントを現在アソシエートしている AP に登録された WLC に、元の WLC からのクライアント トラフィックが転送されます。

別の WLC にアソシエートされている AP にローミングした無線クライアントから始まるトラフィックは、2 つの方法で処理できます。通常は、無線クライアントからのパケットの宛先 MAC アドレスが、外部 WLC によって無線クライアントのゲートウェイ MAC アドレスに変更されてから、パケットが転送されます。モビリティ アンカーが元の WLC で有効になっている場合は、2 つ目の方法で処理されます。この場合、トラフィックは元の WLC に転送して返されます。これによって、Reverse Path Forwarding（RPF）チェックなどのアドレス ポリシーが有効になっている場合に、トラフィックを適切なゲートウェイに送信できます。

Cisco Unified Wireless Roaming の詳細は、ローミング（P. 2-18）を参照してください。

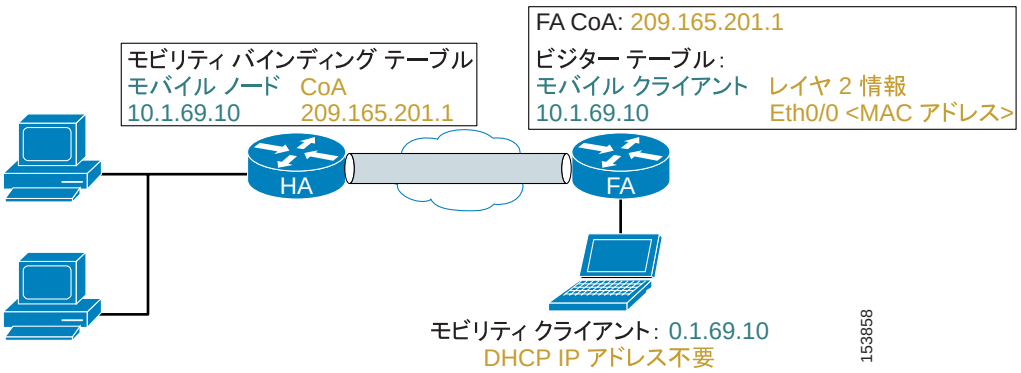
モバイル IP 対応ネットワークでのローミング

モバイル IP 対応ネットワークには、次の 3 つのコンポーネントが含まれます。

- Mobile Node（MN; モバイル ノード）：モバイル IP クライアント
- ホーム エージェント（HA）：MN のロケーション データベースを含み、Interior Gateway Protocol（IGP）によって MN への到達可能性をアドバタイズします。また、パケットを MN にトンネルします。
- 外部エージェント（FA）：（オプション）カプセル化およびカプセル解放の CPU 処理を MN からオフロードし、IP アドレス領域を節約します。FA は通常、企業のキャンパス環境では展開されません。

これら 3 つのコンポーネントのうち、実際にモビリティ ソリューションに必要なものは、MN と HA の 2 つだけです。3 つ目のコンポーネントの FA は、MN で DHCP をローカル IP アドレスに使用することによって MN が独自の FA として機能できるため、オプションとなっています。この場合、トンネルは MN で終端します。HA および FA のトンネリング は、HA に対するローカルの IP アドレス（10.1.69.10）が指定されている MN を示しています。ネットワークの他の部分では、MN は HA に直接接続されているかのように見えます。HA はモビリティ バインディング テーブルを使用して、MN の現在のロケーションにパケットを転送します。MN は HA に対して、MN の現在のロケーションをアップデートする必要があります。FA は、MN 宛てのパケットのカプセル化を解除し、インターフェイスを使用してそれらのパケットを転送します。FA は、HA でのレジストレーション プロセスにアクティブに関与することによって、必要な情報をグリーニングします。MN は実際にパケットを FA に送信します。FA はパケットを確認し、新しい IP ヘッダーを生成して、HA に情報を転送します。FA では、通常のスイッチング プロセスを使用して転送する代わりに、MN から送信されたパケットを HA に戻すリバース トンネリングを使用することもできます。リバース トンネリングによって、MN からのパケットが常に HA を出て、Reverse Path Forwarding（RPF）チェックを通るようになります。

図 12-5　HA および FA のトンネリング



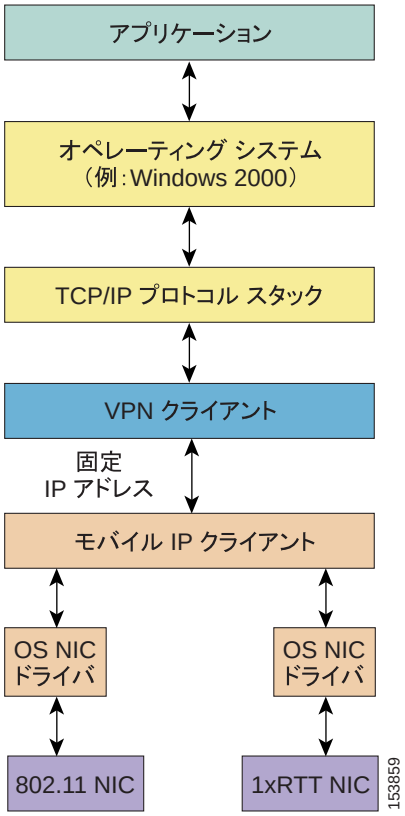
ネットワークがプロキシを実行し、無線クライアントにシームレス モビリティを提供する Cisco Unified Wireless Network とは異なり、モバイル IP クライアント、つまり MN が機能するためには次の 3 つの情報を認知しておく必要があります。

- MN のホーム アドレス（HA のローカル接続サブネット上）
- MN の HA アドレス（HA に現在のロケーションをアップデートできるように）
- MN の共有秘密鍵（MN と HA 間でのパケットの認証に使用）

モバイル ノードのホーム アドレスと HA アドレスはどちらも、動的に検出したり生成したりできますが、通常は、手動で MN に設定します。DHCP を使用して、オプション 68 によって MN に HA アドレスを伝達できます。HA では、MN の初めての登録時にホーム アドレスとして使用されるように、IP アドレスを MN に動的に割り当てることができます。使用しているモバイル IP クライアント ソフトウェアとその機能によって異なりますが、通常、共有秘密鍵は手動で設定する必要があります。

モバイル IP クライアントが Windows ホストにロードされると、モバイル IP クライアント機能は物理インターフェイスと TCP/IP スタックとの間に常駐します（図 12-6 を参照）。モバイル IP クライアント機能は、ホーム アドレスを TCP/IP スタックに送信して、MN が異なるネットワーク ロケーション間または異なるネットワーク間でローミングするときに、VPN クライアントを含めたホスト アプリケーションで固定 IP アドレスを確認できるようにします。物理インターフェイスは、FA が特定のサブネット上にあるかどうかによって、ローミング時に IP アドレスを持っている場合と持っていない場合があります。

図 12-6　Microsoft オペレーティング システムにおけるモバイル IP 機能の位置の例



モバイル IP クライアントは、ホストから受け取ったパケットを送信するためのインターフェイスを次の方法で制御します。

- インストール時に新しい仮想インターフェイス アダプタをインストールする。
- ホスト転送テーブルを変更する。

この仮想アダプタは、ホストには物理アダプタのように見えます（設定 1：モバイル IP クライアント インターフェイスおよびホスト テーブル処理の例の例を参照）。このアダプタが有効な場合、モバイル IP クライアントは仮想アダプタに最善のメトリックを渡せるように転送テーブルを変更し、Windows オペレーティング システムはホストから送信されるパケットを仮想アダプタに転送します。これによって、モバイル IP クライアントは、パケットの送信に使用する実際のインターフェイスを隠して、ホストの転送動作を変更できます。この例では、次の 3 つのインターフェイスが使用されます。

- 静的 IP アドレスを使用するローカル エリア接続。ゲートウェイなし。
- ホーム アドレスとゲートウェイが設定されたモバイル IP クライアント インターフェイス。
- モバイル IP によって 0.0.0.0 に指定されたアドレスを使用する無線接続。実際のアドレスは、Windows オペレーティング システムには示されません。

下位メトリック インターフェイスがモバイル IP クライアントのインターフェイスになるようにモバイル IP クライアントがホストの転送テーブルを処理することに注意してください。テーブルの参照時に、上位メトリックのルートを安全に無視できます。無線インターフェイス上の実際の DHCP IP アドレスは 10.20.41.12 です。宛先アドレスがこのゲートウェイになっているルートのメトリックは大きくなり、デフォルトのゲートウェイは仮想インターフェイス「設定 1 のイーサネット アダプタ MIPDRV」を経由します。

設定 1：モバイル IP クライアント インターフェイスおよびホスト テーブル処理の例

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IP Address . . . . . . . . . . . . : 10.20.30.249
Subnet Mask. . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
Ethernet adapter MIPDRV:
Connection-specific DNS Suffix . : srnd3.com
IP Address . . . . . . . . . . . . : 10.20.32.11
Subnet Mask. . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 10.20.32.1
Ethernet adapter Wireless Connection:
Connection-specific DNS Suffix . :
IP Address . . . . . . . . . . . . : 0.0.0.0
Subnet Mask. . . . . . . . . . . . : 0.0.0.0
Default Gateway . . . . . . . . . :
C:\>route print
===========================================================================
====
Interface List
0x1...........................MS TCP Loopback interface
0x2...00 d0 b7 a6 b8 47........Intel (R) 82559 Fast Ethernet LAN on Motherboard
- Packet Scheduler Miniport
0x3...00 4d 69 70 56 61 .......Cisco Systems Mobile Adapter - Packer Scheduler
Miniport
0x10005...00 12 f0 7c a5 ca......Intel (R) PRO/Wireless 2915ABG Network Connec
tion - Deterministic Network Enhancer Miniport
===========================================================================
=====
===========================================================================
=====
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.20.32.1 10.20.32.11 1
10.20.30.0 255.255.255.0 10.20.30.249 10.20.30.249 1
10.20.30.0 255.255.255.0 10.20.32.1 10.20.32.11 1
10.20.30.249 255.255.255.255 127.0.0.1 127.0.0.1 1
10.20.32.0 255.255.255.0 10.20.32.11 10.20.32.11 20
10.20.32.11 255.255.255.255 127.0.0.1 127.0.0.1 20
10.20.41.0 255.255.255.0 10.20.41.12 10.20.41.12 25
10.20.41.0 255.255.255.0 10.20.32.1 10.20.32.11 1
10.20.41.12 255.255.255.255 127.0.0.1 127.0.0.1 25
10.255.255.255 255.255.255.255 10.20.30.249 10.20.30.249 1
10.255.255.255 255.255.255.255 10.20.32.11 10.20.32.11 20
10.255.255.255 255.255.255.255 10.20.41.12 10.20.41.12 25
127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1
224.0.0.0 240.0.0.0 10.20.30.249 10.20.30.249 1
224.0.0.0 240.0.0.0 10.20.32.11 10.20.32.11 20
224.0.0.0 240.0.0.0 10.20.41.12 10.20.41.12 25
255.255.255.255 255.255.255.255 10.20.30.249 10.20.30.249 1
255.255.255.255 255.255.255.255 10.20.32.11 10.20.32.11 1
255.255.255.255 255.255.255.255 10.20.41.12 10.20.41.12 1
Default Gateway: 10.20.32.1
===========================================================================
=====
Persistent Routes:

None
```

MN でレイヤ 2 接続が確立されると、その MN では 2 つの異なるスレッドが開始されます。1 つのスレッドは、サブネット上に FA がない場合に、HA への連結型気付アドレス（CCoA）レジストレーションに IP アドレスを使用できるように ローカル IP アドレスを取得する DHCP プロセスです。もう 1 つのスレッドでは、接続先のサブネット上の FA が検索されます。MN がサブネットで FA を見つけると、MN は FA によってアドバタイズされた Care of Address（CoA; 気付アドレス）を使用して、HA および DHCP からの拒否で登録（アップデート）します。サブネット上の FA は、モバイル IP クライアントに対して次の 2 つの処理を実行します。

- HA は、MN 宛てのパケットを転送するために FA CoA を使用してトンネルを作成するので、MN でローカル アドレスを取得する必要がなくなります。FA は、HA へのレジストレーション時に導出したレイヤ 2 情報を使用してローカル インターフェイス上の MN ホーム アドレスにパケットを転送します。
- FA は、カプセル化およびカプセル化解除のトンネル パケット処理を自身にオフロードします。FA は、MN が直接接続されているインターフェイス上にあるため、トラフィックを MN に転送できます。

FA では、ビジター テーブルと呼ばれるテーブルにエントリが保持されます。このテーブルには、MN ホーム アドレス、MN の現在の接続先インターフェイス、およびレイヤ 2 カプセル化情報が格納されます。これによって、HA が MN 宛てのパケットを FA にトンネリングする場合、FA はパケットのカプセル化を解除して、ビジター テーブルで MN が使用しているインターフェイスを確認し、パケットをそのインターフェイスを使用して直接転送します。このテーブルがあるため、MN はサブネットにローカル IP アドレスを必要としません。

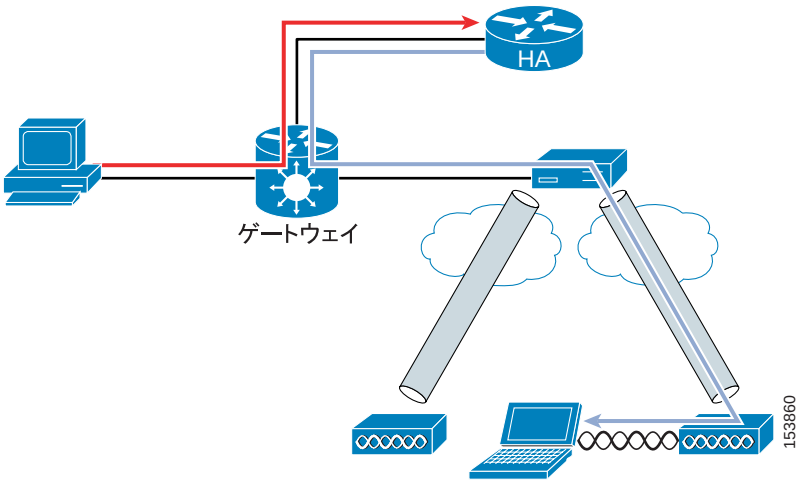
サブネットに FA がない場合、MN には HA がパケットの転送先にできるローカル IP アドレスが必要です。MN は、DHCP アドレスを受信すると、HA に登録（アップデート）して、MN と HA 間に直接トンネルを作成します。パケットのカプセル化の解除はすべて MN が実行します。（ホスト パケットが HA にトンネル経由で戻る）リバース トンネリングが有効な場合、全体的なソリューションは Cisco Unified Wireless Network に類似しています。クライアントからのパケットはトンネルされて HA に転送され、クライアント宛てのパケットは HA で受信され、トンネルされ、クライアントの現在のロケーションに転送されます。

図 12-5 と図 12-6 は機能上似ていますが、HA がルータであり、IGP を使用してモバイル IP クライアント宛てに自らをアドバタイズして、パケットを MN にトンネルできる点が異なります。

Cisco Unified Wireless Network でのローミング時のモバイル IP クライアントの特徴

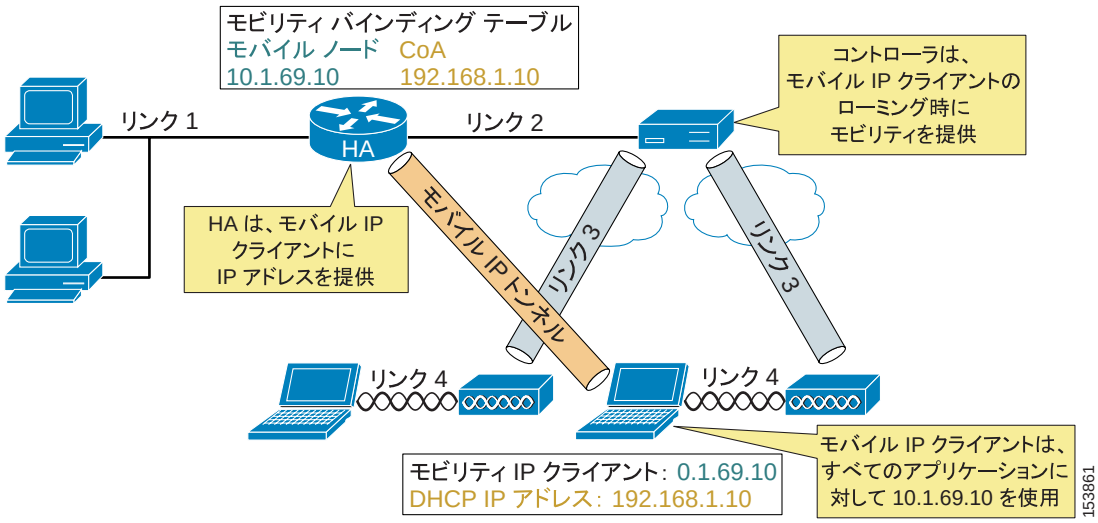
MN 宛てのトラフィックは、無線ネットワーク上の MN に到達するには、HA と WLC を経由する必要があります。リバース トンネルが有効な場合、パケットは、他のホストに転送する前に、HA を経由して戻す必要があります。図 12-7 は、リモート ホストから MN へのトラフィック パターンを示しています。赤色のフロー ラインは、ネットワークで、MN が HA に接続されていることが認識されていることを示しています。青色のフロー ラインは、MN へトンネルされたパケットを示しています。別の無線クライアントがパケットを MN に送信した場合、そのトラフィックも HA を経由する必要があります。

図 12-7　MN へのトラフィック フロー



MN へのトラフィックまたは MN からのトラフィックを他のホストからルーティングするため、WLC と HA を配置するときは、リンクの合計数を最小限に抑えます。モバイル IP と Cisco Unified Wireless Network では、ホストのロケーションがランダムなため、リンク 1 を最小化できません。モバイル ホストのロケーションを固定できないため、リンク 4 も最小化できません。リンク 3 は、RF 調査によって AP の配置が決まるため、最小化できません。これによって WLC と HA 間のリンクであるリンク 2 もそのままになります。

図 12-8　モバイル IP と Cisco Unified Wireless Network



基本的な HA 配置の原則は、次の 2 つです。

- HA 配置は可能な限りコアに近づける必要がある。
- Cisco Unified Wireless Network で使用した場合、HA 配置は可能な限り WLC に近づける必要がある。

最初の原則は単に、ネットワーク内のホストからネットワーク内の任意の場所へのトラフィックのリンクを最小限に抑える方法です。2 つ目の原則は、最小化できる唯一のリンクが HA と WLC 間のリンク 2 だというロジックに従っています。つまり、WLC と HA を可能な場合は同じ場所に設置する必要があるということです。最善のロケーションは、WLC が集中化されているコアのすぐ近くです。モバイル IP が分散された WLC 配置ネットワークで使用されている場合、HA はネットワーク内の、HA と WLC との間のリンク数が最も少なくてすむ集約ポイントに配置する必要があります。

モバイル IP クライアントは、Cisco Unified Wireless Network にローミングする場合、ローミング時に同じ DHCP IP アドレスを保持するため、同じ CCoA アドレスを保持できます。Cisco Unified Wireless Network では、基本となるモビリティが扱われており、モバイル IP クライアントは AP 間でローミングするときにいずれの変化も認識しません。モバイル IP クライアントにとっては、単一の大きなサブネット上でローミングしているかのように見えます。したがって、モバイル IP クライアントが無線ネットワークからローミングして離れるまでモバイル IP クライアント レベルでは変化はありません。

（注） Cisco Unified Wireless Network では、WLC でマルチキャストが有効な場合に共有無線ネットワーク上に不要なマルチキャスト トラフィックができるため、モバイル IP クライアントには CCoA モードをお勧めします。WLC でマルチキャスト トラフィックはデフォルトで無効になっているため、無線ネットワークに FA は必要ありません。Cisco Unified Wireless Network のマルチキャスト トラフィックの詳細は、第 6 章の「Cisco Unified Wirelss Network のマルチキャスト設計」を参照してください。

CHAPTER 13

Cisco Unified Wireless ロケーション ベース サービス

はじめに

企業の無線 LAN にロケーション トラッキング機能を統合すれば、ビジネス資産としての価値がさらに高まります。無線ユーザのロケーションを特定し、追跡することで、WLAN 計画および WLAN 展開の的確性が向上し、現在のネットワーク環境を最適化すると同時に、無線セキュリティを強化し、重要なビジネス アプリケーションの実用性と価値を高めることができます。また、RF 環境を把握し、制御しやすくなることもロケーション トラッキングの利点です。IT スタッフは、無線ネットワークの管理と展開を容易に行えるようになります。

企業のネットワーク管理者、セキュリティ担当者、ユーザ、および資産所有者は、次のような要件の解決に役立つロケーションベース サービスに大きな関心を寄せています。

- 重要な資産や主要スタッフの所在を迅速かつ効率的に確認する
- 資産と人員の効率的な割り当てにより、生産性を向上する
- 高価な資産の無断持ち出しを防止し、損失を削減する
- サービスに影響を与える重要な資産の所在をすばやく確認し、顧客満足度を高める
- WLAN の計画能力と調整能力を高める
- ワークフローの自動化を促進する
- セキュリティ ポリシーに基づいて Wi-Fi デバイス ロケーションを調整する

この章では、ロケーション認識 Cisco Unified Wireless Network（UWN）について説明します。主に設計上の考慮事項に着目しますが、展開時に特別に考慮すべきいくつかの内容にも触れます。ここではそれらの領域の概略を説明しますが、詳細と分析は、『Wi-Fi Location-Based Services: Design and Deployment Considerations』というタイトルの包括的なホワイト ペーパーを参照してください。このホワイト ペーパーは URL http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf で入手できます。

この章の内容は、次のとおりです。

- ラテレーション、アンギュレーション、およびロケーションのパターン作成アプローチを含む位置決めテクノロジーの基本
- Cisco RF フィンガープリントおよび従来の位置決めテクノロジーと比較した場合の利点
- Cisco Location Control ProtocolLOCP
- Cisco　UWN　においてロケーション精度をさらに強化するためのチョークポイント（およびチョークポイント トリガーの使用法）
- アクティブ、パッシブ、およびマルチモードを含む、RFID タグの各種テクノロジー
- Cisco Wireless Location Appliance に対する外部のサードパーティ製ロケーション クライアント アプリケーション インターフェイス

参考文献

次の補足資料には有益なサポート情報が含まれており、確認することをお勧めします。

- *Wi-Fi Location-Based Services: Design and Deployment Considerations* ー
  http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf
- Cisco Wireless Control System Support Documentation for Release 4.1 ー
  http://www.cisco.com/en/US/products/ps6305/tsd_products_support_series_home.html
- Cisco Wireless Location Appliance Support Documentation for Release 3.0 ー
  http://www.cisco.com/en/US/products/ps6386/tsd_products_support_series_home.html
- Cisco 4400 Series WLAN Controller Support Documentation for Release 4.1 ー
  http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html
- Cisco 2100 Series WLAN Controller Support Documentation for Release 4.1 ー
  http://www.cisco.com/en/US/products/ps7206/tsd_products_support_series_home.html
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers Support Documentation ー
  http://www.cisco.com/en/US/products/ps6915/tsd_products_support_series_home.html
- Cisco Wireless LAN Controller Module Support Documentation ー
  http://www.cisco.com/en/US/products/ps6730/tsd_products_support_model_home.html
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM) Support Documentation ー
  http://www.cisco.com/en/US/products/ps6526/tsd_products_support_model_home.html

ロケーション認識 Cisco UWN での、InnerWireless Vision（旧 PanGo）Locator ロケーション クライアントの使用に関する設計上の考慮事項は、次のホワイト ペーパーを参照してください。

- Design Considerations for Cisco ー PanGo Asset Tracking ー
  http://www.cisco.com/univercd/cc/td/doc/solution/pangoex.pdf

（注） このガイドで Cisco Unified Wireless Network（UWN）ソフトウェア リリース 4.1 について説明している場合、特に記載されていない限り、Cisco Location Appliance ソフトウェア リリース 3.0 も含まれています。

Cisco ロケーションベース サービスのアーキテクチャ

位置決めテクノロジー

ロケーション トラッキングと位置決めシステムは、モバイル デバイスのロケーション（*ローカリゼーション*）の特定に使用される測定技法によって分類できます。これらのアプローチには、監視下の環境におけるモバイル デバイスの位置の検知と測定に使用される特定の技法に違いがあります。一般的に、Real Time Location System（RTLS）は、次の項目に基づいて位置を決定する 4 つの基本カテゴリに分類できます。

- 基点のセル（*最も近いセル*）
- 距離（*ラテレーション*）
- 角度（*アンギュレーション*）
- ロケーションのパターン作成（*パターン認識*）

RTLS システムの設計者は、これらの技法から 1 つ以上を選択して実装できます。これは、伝播特性が大きく異なる複数の環境においてパフォーマンスを最適化しようとするいくつかのアプローチに見ることができます。これらの方式の 2 つ以上を組み合わせて使用し、位置の検知と測定を行う RTLS システムを含む 5 番目のカテゴリをサポートすることもよく議論されています。

基盤となる位置決定テクノロジーの種類に関係なく、RTLS の「リアルタイム性」は、最新のタイムスタンプ、信号強度の読み取り、または受信角度の測定がリアルタイムであることにすぎません。プローブ応答のタイミング、タグ ビーコン、およびロケーション サーバのポーリング間隔は、実際のデバイスの位置と、各報告間隔において観測される報告されたデバイスの位置の間に不一致を招く可能性があります。

『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Location Tracking Approaches」の項では、従来のロケーション トラッキングおよび位置決定システムの技術的な側面の基本について説明しています。従来のアプローチと RF フィンガープリントとの違いを理解するために、この章を参照することをお勧めします。ここでは、基点のセル、到達時間（ToA）、到達時間差（TDoA）、到達角度（AoA）、およびロケーションのパターン作成の概念が網羅されています。

RF フィンガープリントについて

Cisco RF フィンガープリントは、従来の信号強度ラテレーション技法で可能だったものに比べて、精度や確度を大幅に向上させる革新的なローカリゼーション アプローチです。Cisco RF フィンガープリントでは、カスタマイズされた調整機能と従来のアプローチよりも向上したパフォーマンスによって、Received Signal Strength Indication（RSSI; 受信信号強度表示）ベースのラテレーション アプローチが簡略化されます。

RF フィンガープリントは、対象環境または類似環境で収集されたデータから開発した RF 伝播モデルを使用して、Received Signal StrengthRSS; 受信信号強度）ラテレーションを大幅に向上させます。RF フィンガープリントには、ロケーションのパターン作成方法と同様の（ただし、より高速な）方法で RF モデルを特定の環境に調整する機能が備わっています。ただし、ロケーションのパターン作成とは異なり、RF フィンガープリントでは、特に似たような構造、内部、およびレイアウトの複数のフロアが配置されている状況では調整モデルを再利用できます。

さらに、Cisco RF フィンガープリントには、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Location Tracking Approaches」の項に記載されている従来のアプローチ以外に、次のいくつかの重要な利点があります。

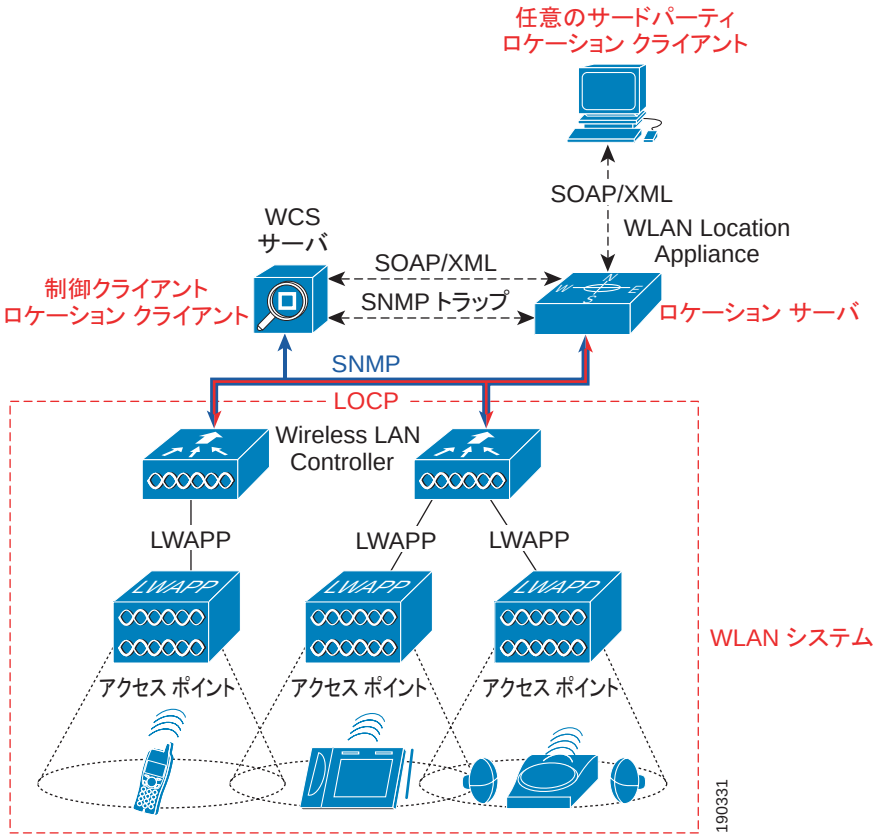
- 既存の LWAPP 対応 Cisco Unified Networking コンポーネントの使用：他のソリューションとは異なり、RF フィンガープリント機能搭載のロケーション認識 Cisco UWN は、各アクセス ポイントに設置しなければならない追加コストを要する特殊な受信装置やその他のハードウェアを必要としません。このことは、ロケーション認識 Cisco UWN の資本コストおよび継続的な維持コストを、専用オーバーレイ ロケーション インフラストラクチャを必要とするソリューションと比較して低く抑えるのに役立ちます。Cisco Location Appliance は、ロケーションと統計情報の履歴をサポートする集中化コンポーネントとして追加され、アプライアンスごとに最大 2,500 台のデバイスを同時に追跡するロケーション測位エンジンとして機能します。
- 専用のクライアント ハードウェアまたはソフトウェアの開発が不要：Cisco UWN のロケーション ベース サービスは、クライアント側ではなくネットワーク側のモデルとして実装されます。そのため、Cisco RF フィンガープリントでは、クライアントごとに専用のトラッキング ソフトウェアやロケーション対応ドライバをロードすることなく、多種多様な業界標準 Wi-Fi クライアントのロケーション トラッキングを実現できます。Cisco Compatible Extensions WLAN クライアント仕様バージョン 2 以降に適合するクライアントの WLAN 強化クライアント ローカリゼーションにより、ほとんどの場合、IEEE 802.11 クライアントを位置決めできます。これには、Cisco 792x シリーズなどの一般的な VoWLAN 端末や、専用のロケーション トラッキング クライアント ソフトウェアを簡単に入手したりインストールしたりすることができないその他のデバイスが含まれます。
- Cisco Compatible Extensions Wi-Fi Tag 仕様に対応する Wi-Fi アクティブ RFID 資産タグのサポート：ロケーション認識 Cisco UWN ソリューションでは RF フィンガープリントがネットワーク側モデルとして実装されるため、アクセス ポイント RSSI の検出と、この情報を資産タグが正しくローカライズされるためにネットワークに中継して戻すために資産タグに専用ソフトウェアをもつ必要がありません。したがって、ロケーション認識 Cisco UWN は、Cisco Compatible Extensions Wi-Fi Tag 仕様に適合する、AeroScout や WhereNet、G2 Microsystems、InnerWireless（旧 PanGo Networks）などのベンダーのアクティブ RFID 資産タグと相互運用できます。Cisco Compatible Extensions Wi-Fi Tag 仕様をサポートする RFID 資産タグにより、次のようなパフォーマンスの向上や高度な機能のサポートが実現されます。
  - テレメトリおよびセンサー情報
  - バッテリ、パニック、および改ざんのアラート
  - 動作検出通知
  - チョークポイント トリガーを使用した高精度かつ決定論的ロケーション
- 精度と確度の向上：Cisco RF フィンガープリントでは、純粋な三角測量技法や信号強度ラテレーション技法のみを採用したソリューションよりも大幅にパフォーマンスが向上します。通常、これらの技法は、環境内の減衰の影響を考慮しないため、パフォーマンスの低下に左右されやすくなります。Cisco RF フィンガープリントの利点は、従来のアプローチではできなかったことが開始点となります。Cisco RF フィンガープリントは、特に問題の環境に関係する場合に、まず RF 伝播をよりよく理解することから開始します。ロケーションのパターン作成アプローチにおける調整フェーズを除いて、一般的に、従来のラテレーション技法とアンギュレーション技法のどちらも、環境を直接考慮することはありません。RF フィンガープリントは、さらに進んで、収集された調整データのセットに統計分析技法を適用します。このことにより、Cisco Location Appliance は、非論理的なデータや異常なデータを排除し、精度を一層高めて、モバイル クライアントのロケーション予測をさらに洗練させることができます。これらの方式の結果、従来のソリューションに比べて、精度が高くなるだけでなく、確度が大幅に向上します。
- 調整作業の軽減：Cisco RF フィンガープリント テクノロジーには、ロケーション パターン作成ソリューションにおいて重要な利点がありますが、調整作業も大幅に軽減されます。両方のアプローチはオンサイト調整をサポートしていますが、Cisco RF フィンガープリント アプローチの方が、再調整の回数が少なくてすむため、アクセス ポイント間の距離を広げることができます。また、Cisco RF フィンガープリントは、同種の環境間で調整モデルを共有することができ、一般的な屋内環境での迅速な展開を促進するあらかじめパッケージ化された調整モデルをいくつか組み込むことができます。

Cisco RF フィンガープリントのこのような重要な利点の詳細は、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Location Based Services Architecture」の項を参照してください。

全体のアーキテクチャ

ロケーション認識 Cisco UWN の全体的なアーキテクチャを図 13-1 に示します。

図 13-1　ロケーション認識 Cisco Unified Wireless Network のアーキテクチャ



アクセス ポイントは、すべての Wi-Fi クライアント、802.11 アクティブ RFID タグ、不正アクセス ポイント、または不正クライアントの受信信号強度を、登録された WLAN コントローラに転送します。アクセス ポイントの通常の動作では、規制周波数区域内でチャネルの停止と他のチャネルのスキャンを周期的に繰り返しながら、プライマリ操作チャネル上でのこの情報の収集活動に集中します。収集された信号強度情報は、アクセス ポイントが現在登録されている WLAN コントローラに転送され、そこで情報が集約されます。Location Appliance は、SNMP を使用して各コントローラをポーリングし、追跡対象の各デバイス カテゴリの最新の信号強度情報を取得します。ロケーション トラッキング システムが Location Appliance なしで展開されている場合、Cisco Wireless Control System WCS は、この情報を各コントローラから直接取得します。Cisco Wireless Location Appliance は、Cisco WLAN コントローラから受信した RSSI 情報に基づいてロケーション計算を実行します。ソフトウェア リリース 4.1 では、精度を向上させるため、アクセス ポイントのアンテナの高さと方位角がこれらの RSSI ベースのロケーション計算の際に考慮されるようになりました。

ロケーション認識 Cisco UWN ソフトウェア リリース 4.1 から、Location Appliance では、資産タグのテレメトリ データ（たとえば、内蔵タグ センサーや外部環境センサーからのバッテリ ステータスなどのテレメトリ データなど）用に LOCP を使用して WLAN コントローラを定期的にポーリングすることにより、SNMP ベースのデータ収集機能が強化されました。LOCP はまた、WLAN コントローラが Cisco Compatible Extensions Wi-Fi Tag 仕様に準拠するタグから受信する、チョークポイント プロキシミティ通知および緊急事態通知の優先転送にも使用されます。

WCS と Location Appliance は、「同期化」と呼ばれるプロセス時に（調整マップやネットワーク設計などの）情報を交換します。このとき、新しい方のパートナーによって古い方のパートナーの設計および調整情報が更新されます。同期化は、オンデマンドでまたはスケジュール済みタスクとして実行され、そのタイミングは、WCS メイン メニュー バーの Administration > Scheduled Tasks メニュー オプションで決定されます。

デバイス ロケーションについての情報は、*ロケーション クライアント* アプリケーションを使用するエンドユーザに提供されます。通常、この役割は Cisco WCS が果たします。Cisco WCS は、ロケーション情報を視覚的に表示します。また、基本的な RF キャパシティ管理の強化、不正なアクセス ポイントおよびクライアントの検出の実行、および WLAN デバイス用に資産の視覚化を望んでいるお客様のために簡単に入手できるロケーション クライアント アプリケーションを提供します。

WCS と Cisco Wireless Location Appliance のバージョン間の互換性については、次の URL にある『Release Notes for Cisco Wireless Location Appliance *3.0*』を参照してください。
http://www.cisco.com/en/US/products/ps6386/prod_release_notes_list.html

このロケーション情報は、アプライアンス上で Simple Object Access Protocol/Extensible Markup Language（SOAP/XML）API を介して、任意のサードパーティ製のロケーション クライアント アプリケーションにも提供できます。SOAP/XML プロトコルを使用すると、これらのサードパーティ製アプリケーションは、医療、小売、製造、物流などの特定の垂直アプリケーションに対して、より個別に拡張されたロケーション クライアント機能を提供できる可能性があります。

Cisco Location Appliance は、外部システムに通知を発行することもできます。これにより、デバイスの移動、デバイスの不在、追跡対象デバイスのゾーンへの参加と退去、タグ バッテリ レベル、デバイスの位置の変更、緊急グループ、およびチョークポイント情報に基づいて、プロアクティブにロケーション通知を送信する機能が提供されます。これらすべての通知は、UDP-Syslog、Simple Network Management Protocol（SNMP）トラップ、E メール（SMTP）、および SOAP/XML などの複数の転送タイプで配信可能です。

Cisco LBS ソリューションのアーキテクチャに関する詳細は、次の場所にある『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Location Based Services Architecture」の項を参照してください。http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf

Cisco Wireless Location Appliance の役割

Cisco Location Appliance は、正規バージョンの WCS を含む Cisco Unified Wireless Network に追加されると、次のものを含むいくつかの重要な役割を担います。

- 位置決定アルゴリズムの実行
- 調整情報の保持
- ロケーション通知のトリガーと送信
- 統計と過去のロケーションの処理

WCS は、図 13-1 に示すように、Location Appliance が提供するサービスの *コントロール クライアント*と *ロケーション クライアント*の両方のユーザ インターフェイス（UI）として機能することによって、Location Appliance と連動します。Location Appliance には、保守と診断目的で、SSH またはコンソール セッションを介して直接アクセスできますが、通常は、WCS またはサードパーティ製ロケーション クライアント アプリケーションを介してすべてのオペレータおよびユーザと Location Appliance との対話が実行されます。

Cisco Location Appliance を Cisco Unified Wireless Network アーキテクチャに統合することによって、ベースレベル ロケーション機能を向上させることができます。これには、次のようなものが含まれます。

- スケーラビリティ：Cisco Location Appliance を追加すると、Cisco UWN のスケーラビリティが向上して、一度にオンデマンド トラッキングできるデバイス（WLAN クライアント、RFID タグ、不正アクセス ポイント、および不正クライアント）の台数が、Location Appliance 1 台あたり、従来の 1 台から同時に最大 2,500 台にまで増加します。さらに多くのデバイスのサポートが必要な展開では Location Appliance を追加でき、それらを 1 つまたは複数の WCS サーバで管理できます。
- 履歴および統計情報：Location Appliance は、ロケーションと統計の履歴情報を記録および管理します。これらの情報は、WCS または他のロケーション クライアントを介して表示できます。この履歴情報は、ロケーション傾向分析、資産損失調査、RF キャパシティの管理、およびネットワーク問題の解決の促進に使用できます。
- チョークポイント ロケーション：UWN リリース 4.1 から Location Appliance が組み込まれたことにより、*チョークポイント*と呼ばれる制約された物理領域を通る資産の通過に基づく、高精度で決定論的なローカリゼーションが可能になりました。これらの領域内およびタグ付きの資産の近接に配置された*チョークポイント トリガー*は、低周波（125kHz）の信号をタグに送信します。資産タグはその後、チョークポイント トリガーの ID をロケーション認識 Cisco UWN に送信します。これにより、チョークポイント トリガーの機能に応じて、半径 30 cm から 6 m 超までに及ぶ、正確なプロキシミティ ロケーションが提供されます。チョークポイント ロケーションは、高価な資産の盗難防止などの汎用使用から、製造プラントにおける使用などの業界固有のプロセス管理イベントまで、さまざまに適用されます。
- Cisco Extensions Wi-Fi Tag のテレメトリ情報および緊急事態通知：Cisco UWN リリース 4.1 から、シスコは 802.11 Wi-Fi ベースのアクティブ資産タグの拡張可能な仕様を作成するためにさまざまな資産タグ ベンダと提携しています。Cisco Compatible Extensions Wi-Fi Tag 仕様では、タグ ベンダがロケーション認識 Cisco UWN と相互運用するために使用できる、共通送信フォーマットが定義されています。これには、テレメトリ、タグ送信電力レベル、バッテリ情報、および緊急グループとチョークポイント用の高度なフィールドを含む、基準機能セットが含まれます。Location Appliance の追加により、ロケーション認識 UWN はこれらの新しく導入された機能を活用することができ、お客様にとっては、仕様に準拠したさまざまなベンダの資産タグを同じネットワーク上で「組み合わせて調和させる」機能が提供されるという利点があります。Cisco Compatible Extensions Wi-Fi Tag プログラムの詳細は、http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html を参照してください。

（注） 現時点では、チョークポイント トリガーと資産タグは、両方が同一ベンダから提供されている場合のみ相互に適合します。

- ロケーション通知：Cisco Location Appliance は、E メール、Syslog、SNMP トラップ、および SOAP/XML を介してロケーションベースのイベント通知を特定の宛先に直接送信できます。これらの通知は、次の条件下でトリガーされることが可能です。
  - クライアントまたは資産のロケーションが変化した
  - RFID タグのバッテリ レベルが設定値より低下した
  - クライアントまたはタグ付き資産が事前に決定されたマーカー位置から設定距離を逸脱した
  - 資産がチョークポイントの範囲に入った
  - クライアントまたはタグ付き資産が行方不明になった
  - 資産タグが、剥離、改ざん、あるいは緊急事態が発生したことを示した
- SOAP/XML Location Appliance Application Programming InterfaceAPILocation Appliance API によって、顧客とパートナーは、Cisco Wireless Location Appliance とインターフェイスするロケーションベース アプリケーションを作成できます。詳細については、SOAP/XML Application Programming InterfaceAPI; アプリケーション プログラミング インターフェイス）を参照してください。

精度と確度

位置決定システムのパフォーマンスについて議論する際に、一般的に最もよく使用される基準は*精度*です。これは、通常、受信している情報の品質を表します。*ロケーションの精度*とは、特にモバイル デバイスの予測位置と実際の位置の定量化可能な誤差を意味します。

ただし、実際の用途では多くの場合、ロケーションの精度の記述は、ソリューションがそのレベルで何回も確実に実行できなければあまり価値がありません。*確度*は、記述されたロケーション精度の再現可能性の直接的な指標です。そのため、ロケーション精度の記述には、成功したロケーション検出の再現性または信頼性のレベルに関する記述（*ロケーション確度*）を含める必要があります。

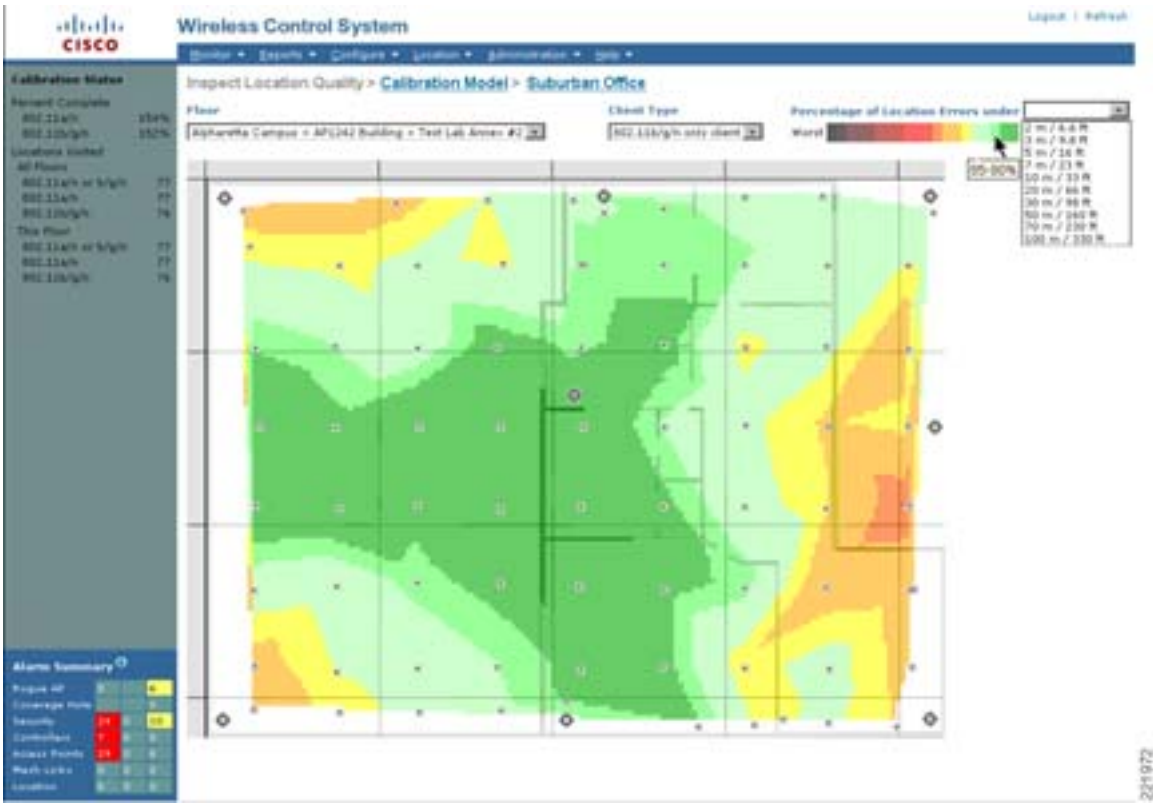
この章と参考文献（P. 13-2）の参考文献に記述されたベスト プラクティスに従って展開すると、ロケーション認識 Cisco UWN は優れた確度と精度を実現できます。Cisco Wireless Location Appliance を使用すると、システムは全体的に 90% の確度で 10 m の精度の基本パフォーマンスを提供できます。チョークポイント ロケーション機能の使用により、半径 30 cm 以下の問題解決において、精度のレベルをさらに洗練させることができる場合があります。

これらの基本パフォーマンス レベルは、システムに含まれる、設計、調整、および展開ツールを使用して実現できます。*Location Planning* 、および *Location Readiness* ツールなどの展開前の予測ツールと、*Location Inspector* などの展開後の確認ツールがあります。

Location Planning ツールは、Location Appliance の仕様内でのロケーション精度をサポートする WLAN 展開を作成するためのアクセス ポイントの配置および密度に対する提案を行います。ソフトウェア リリース 4.1 では、不規則な形をした多角形ビルディングのサポートが追加され、組織がそのような構造要件に対応するのに役立ちます。Location Readiness ツールを使用すると、ネットワーク エンジニアは、現在計画されているアクセス ポイント展開が Location Appliance の仕様内のロケーション精度をサポートするかどうかを事前に確認できます。

図 13-2 に示す Location Inspection ツールの使用により、システムの設計者は、実際の環境における調整後の基本精度および確度のレベルを評価できます。精度レベルを選択すると、Location Inspection ツールは、色分けされた形式で 0 ～ 5% から最大 95 ～ 100% のあらゆる確度レベルを表示します。結果を参照後、システム アーキテクトはインストール チームと協力して、システムのパフォーマンスが十分であることを確認するための必要な手順を行うことができます。

図 13-2　調整後のロケーション調査



これらのツールを使用すると、事前設定されたパフォーマンス目標を達成するための計画を立てるだけでなく、その目標が達成されたかどうかを確認することもできます。

ロケーションの精度の調整などを含む専門的なサービスの提供に関心がある場合、シスコでは Wireless LAN Location Planning and Design Professional Services を提供しています。このサービスでは、セキュリティで保護されたロケーションベースのソリューションの適切な展開に重要と識別されたサービスを含む統合ソリューションを提供するために、特別に訓練された WLAN エンジニアのスキルを活用しています。Cisco Wireless LAN Location Planning and Design Professional Services の詳細は、次の URL を参照してください。http://www.cisco.com/en/US/products/ps8306/serv_home.html

資産および不正なデバイスの追跡

ロケーション認識 Cisco UWN では、次の位置トラッキング情報を参照できます。

- アソシエートされているか、ロケーション認識 UWN を調査中の、*標準 WLAN クライアント*または *Wi-Fi 802.11 アクティブ RFID タグ*。このタイプの無線 LAN クライアントは、青色の四角アイコン を使用して WCS ロケーション フロア マップ上に表示されます。
- レイヤ 2 マルチキャストを介して通信する *802.11 アクティブ RFID 資産タグ*（Cisco Compatible Extensions Wi-Fi Tag 仕様に適合する資産タグを含む）。これらの資産タグは、WCS フロア マップ上に黄色いタグ アイコン として表示されます。ロケーション認識 Cisco UWN ソフトウェア リリース 4.1 では、予測ロケーションが同じ座標上である 2 つ以上のタグを表すために、*タグ サマリー アイコン* が導入されています。

- *不正アクセス ポイント*。無線 LAN インフラストラクチャで検出され、同じモビリティ グループまたは WLAN システムのメンバではないと判断されたアクセス ポイントのことです。このアクセス ポイントは、黒色の円で囲まれたドクロと交差した 2 本の骨のマーク  を使用して、WCS ロケーション フロア マップ上に表示されます。
- *不正クライアント*。不正アクセス ポイントにアソシエートされているクライアントです。不正クライアントは、黒色の四角で囲まれたドクロと交差した 2 本の骨のアイコン  を使用して、WCS ロケーション フロア マップ上に表示されます。

ロケーション認識 Cisco UWN では、WCS および Location Appliance に対して事前定義されているチョークポイントのロケーションも表示します。チョークポイントは、灰色の円で囲まれた青い星型のマーク  を使用して、WCS ロケーション フロア マップ上に表示されます。アイコンの周りの灰色の同心円帯は、WCS で定義されているチョークポイント範囲の相対的な表示を提供するために使用されます。WCS フロア マップ上のチョークポイント範囲表示は、表示のみを目的としていることに注意してください。実際のチョークポイント トリガーの送信電力および範囲は、ベンダの特定のユーティリティを使用して設定されます。

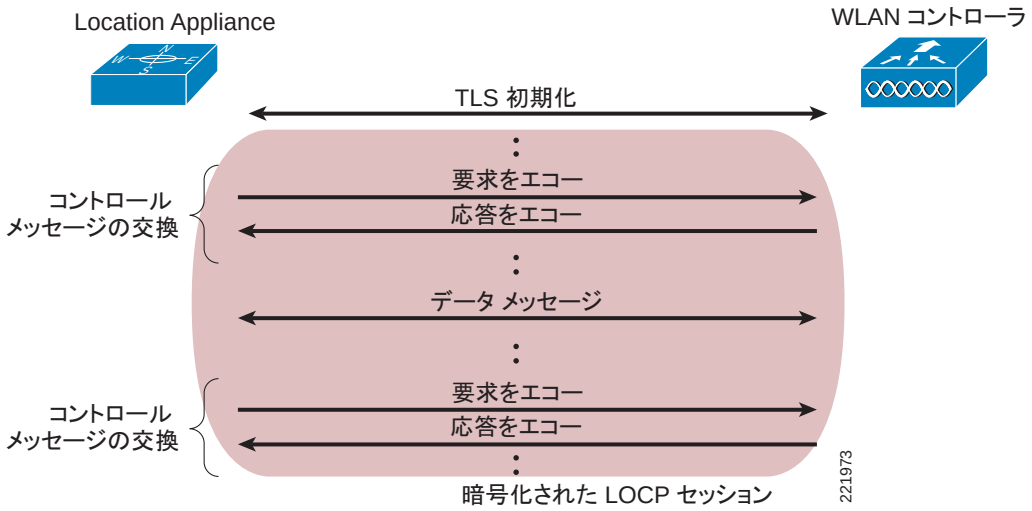
（注） ロケーション認識 Cisco UWN で追跡可能なそれぞれのデバイス クラスに関する詳細は、次の場所にある『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Location-Based Services Architecture」の項を参照してください。
http://www.cisco.com/univercd/cc/td/doc/solution/wifidesi.pdf

Cisco Location Control Protocol

Cisco UWN ソフトウェア リリース 4.1 で導入された Cisco Location Control ProtocolLOCP は、Location Appliance などの Unified Wireless Network のコンポーネントの間の新機能のサポートにおける、重要な一歩です。このリリースでは、LOCP は WLAN コントローラの従来の SNMP ポーリングを拡張し、新しく導入された Cisco Compatible Extensions Wi-Fi Tag プログラムと関連する、テレメトリ、チョークポイント、および緊急事態通知機能を転送する役割を果たします。

LOCP は、コネクション型転送またはコネクションレス型転送で実行でき、Transport Layer SecurityTLS を使用して保護可能な、双方向プロトコルです。このプロトコルにより、図 13-3 に示す Location Appliance と WLAN コントローラ間での基本的な LOCP パケット交換のように、一方のエンドポイントがそのパートナー エンドポイントがまだアクティブであるかどうかを決定することを可能にする、コントロール メッセージの継続的な交換が提供されます。

図 13-3　Location Appliance と WLAN コントローラの LOCP セッション



Cisco Unified Wireless Network ソフトウェア リリース 4.1 は、シスコの LOCP 導入の第一フェーズであり、Location Appliance と WLAN コントローラ間での情報の伝送をサポートするためのこの新しいプロトコルを次のように役立てます。

- 次のものを含む、Cisco Compatible Extensions Wi-Fi Tag テレメトリ
  - 動作、温度、気圧、湿度、距離、数量、およびステータス
  - バッテリ状態とバッテリの予測残量
- 次のものを含む、Cisco Compatible Extensions の優先度の高いタグ通知トラフィック
  - 緊急イベント（パニック ボタン、タグ剥離、改ざんアラート）
  - チョークポイント プロキシミティ
  - ベンダ固有のタグ情報（サードパーティ製のロケーション クライアントが使用）

これらの機能を提供するために LOCP がどのように使用されるのかというメカニズムは、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「The Cisco Location Control Protocol (LOCP)」の項で詳しく考察されているこのプロトコルの 1 つの側面です。さらに、ロケーション認識 UWN での LOCP の使用に関する設計上の考慮事項は、同じホワイトペーパーの「Tag Telemetry and Emergency Notification Considerations」の項を参照してください。

（注）　Cisco UWN リリース 4.1 において、LOCP は Location Appliance と WLAN コントローラ間の SNMP ポーリングを*置換するのではなく*、拡張することに注意してください。

設置および構成

Location Appliance および WCS の設置と構成

Cisco Wireless Location Appliance および WCS の設置と構成に関する詳細な手順は、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Installation and Configuration」の項を参照してください。

WCS の Location Server > Administration メニューの下に列挙されたパラメータの構成については、次の URL にある『Cisco Location Appliance Configuration Guide: Editing Location Server Properties』を参照してください。
http://www.cisco.com/en/US/products/ps6386/products_configuration_guide_chapter09186a008082d72f.html

ただし、工場出荷時の設定を変更したことによって留意すべき問題が発生する場合があります。この問題とロケーション対応無線 LAN の設計者が考慮する必要のあるその他の有益な情報（以下を含む）については、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Installation and Configuration」の項を参照してください。

- 履歴パラメータ
  - 履歴アーカイブ期間
  - 履歴データの消去
- 高度なパラメータ
  - 不明データのクリーンアップ間隔
  - DB ディスク メモリ
  - Java GC の実行
  - データベースの最適化
  - DB の空き容量
- ロケーション パラメータ
  - 計算回数の有効化
  - 相対的 RSSI 破棄時間
  - 絶対的 RSSI 破棄時間
  - RSSI の遮断
  - チョークポイントの使用
  - チョークポイントの範囲外タイムアウト
- 通知パラメータ
- LOCP パラメータ
- Location Appliance の二重イーサネット運用
- Location Appliance の時間同期
- Cisco Compatible Extensions ロケーション測定
- Location Appliance のパスワード設定
- Location Appliance の正常なシャットダウン（停止）

展開のベスト プラクティス

ロケーション認識 WLAN 設計の考慮事項

この 10 年間で、カバレッジの広さと最小限のアクセス ポイントを重視したモデルから、カバレッジの均一性と適切なセル間オーバーラップを最優先するモデルへと設計対象が変わってきました。その背景には、従来のデータ専用通信と異なる新しい無線アプリケーションへの関心が高まり、大量のパケット損失やローミング遅延が受け入れられなくなってきたことがあります。

同様に、ロケーション認識 WLAN アプリケーションを展開するには、従来の手法を見直さなければなりません。そのためには、「まったく新しい」ロケーション認識システムを設計すると同時に、既存の環境を拡張または改善する必要があります。最適なロケーション トラッキングを実現するための必須条件は、適切な数のアクセス ポイントを適切に配置することです。

『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Deployment Best Practices」の項では、以下を含む、ロケーション認識 WLAN 展開に関するいくつかのベストプラクティスについて詳しく説明しています。

- 受信信号の最小しきい値：モバイル デバイスを正確にトラッキングするには、アクセス ポイントが、モバイル デバイスの RSSI を、WCS で設定された *RSSI cutoff* 値以上のレベルで、それぞれのコントローラに報告することをお勧めします。最低 3 台のアクセス ポイント（最適な精度のためには 4 台以上が望ましい）は、このレベルの信号強度を報告するか、ローカライズ対象の任意のデバイスに対してより高いレベルの信号強度を報告する必要があります。このレベル未満で報告されたモバイル デバイスの RSSI は、Location Appliance での破棄対象になります。
- 適切なアクセス ポイントの配置：システムが潜在的なパフォーマンスを十分に発揮するには、アクセス ポイントの適切な配置が不可欠です。多くのオフィス無線 LAN では、アクセス ポイントが内部空間全体に分散されるため、周辺の作業領域にまで過剰にカバレッジが広がってしまいます。通常、これらのロケーションは、カバレッジ、WLAN の帯域幅、チャネルの再利用、セル間のオーバーラップ、セキュリティ、外観、および展開の実現可能性に基づいて選択されます。ただし、ロケーション認識 WLAN 設計では、アクセス ポイントをこれらの基準のみに基づいて配置するのではなく、基準とロケーション配置要件との間のバランスを取る必要があります。すべての環境に適切なアクセス ポイントの密度を導き出す単一ルールは存在しませんが、あらゆるロケーション認識設計の開始点として、『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「Deployment Best Practices」項の単一のしきい値と配置についての記載事項に従う必要があります。これらの推奨事項のうち、アクセス ポイントどうしの間隔を 15 ～ 21 m に保つことが重要です。
- ロケーション パフォーマンスの検証：設計および展開のベスト プラクティスを順守することで成功のために必要な基盤が提供されますが、パフォーマンスの最適化では、設計者（およびインストール担当者）に修正に関するフィードバックを提供するツールが重要な役割を果たします。Location Planning および Location Readiness などの予測ツールを使用すると、容易に（および効率的に）対処できる初期のうちにパフォーマンスの欠点を特定できます。Location Inspection などの展開後のツールでは、既知の調整位置と予測との比較と、ロケーション エラーの度合いの計算によって、調整領域全体の総合的な「実態調査」を行うことが可能です。ロケーション精度が仕様に準拠していない場合、*ロケーション デバッグ*機能を有効にすることによって詳細な調査が可能です。この機能では、特定の追跡対象デバイスのロケーション計算に使用されたアクセス ポイント、それらデバイスの信号強度、および信号強度測定を最後に受信したときのタイムスタンプが表示されます。Cisco UWN ソフトウェア リリース 4.1 で新しく追加された*ロケーション テスト ポイント*を使用すると、選択された MAC アドレスを有するデバイスの実際の物理位置と予測ロケーションを比較することによる、ロケーション精度の臨時チェックを行えます。
- 同一チャネルの過度の干渉の最小化：多くの場合、ロケーションベースのサービスは、一部に VoWLAN ハンドヘルド デバイス（Cisco 792x など）を含む既存の無線設計に追加されるか、または改良して使用されます。遅延に敏感なデバイスと連携して使用されるロケーション認識ソリューションを設計する場合は、環境内で同一チャネルの過度の干渉が発生しないように特別な注意を払う必要があります。このような場合、最適なロケーション認識設計のニーズは、正しく設計された無線音声インフラストラクチャの要件と十分バランスを取る必要があります。

- ロケーション表示の「ジッタ」の防止：デバイスが物理的に停止しているにもかかわらず、ロケーション表示上で移動しているように見える場合があります。これには、環境内の周囲の物体の移動やクライアントやクライアントのアンテナ システムの向きのわずかな経時変化など、さまざまな要因が考えられます。*ロケーション スムージング*は、この現象の是正を支援し、移動しないクライアントのロケーション ジッタを安定させるために使用されます。
- マルチドメイン設計の考慮事項：Cisco Wireless Location Appliance では、同時に最大 2,500 台のデバイス（WLAN クライアント、アセット タグ、不正アクセス ポイント、および不正クライアントを含む）のトラッキングを提供可能です。ほとんどの場合、単一の Location Appliance と WCS 管理システムで、大部分のアプリケーションに対応できるはずです。ただし、より大規模なネットワークでは、複数の Location Appliance と 1 台の WCS サーバか、1 台以上の Location Appliance と複数の WCS サーバを使用する必要がある場合があります。
- アンテナの考慮事項:ロケーション認識 Cisco UWN での使用でサポートされているアンテナの組み合わせ、サードパーティ製アンテナに関するヒント、およびアンテナ方向のベスト プラクティスに関する説明です。この項には Cisco UWN リリース 4.1 で新しく導入されたアンテナの垂直高さと方位角の機能に関する情報が含まれます。この機能により、WCS フロア マップにアクセス ポイントを配置するときに、アクセス ポイント アンテナの垂直高さと x 軸角度のオフセットを WCS で指定できます。
- サイト調整：付属の調整モデルの 1 つを使用するロケーション精度が期待値よりも低い場合、または対象環境が複雑で付属モデルの 1 つでは正しく表示されない場合に、展開後のロケーションを調整できます。この調整時に、802.11 無線クライアント デバイスは、その環境における RSSI の測定に使用されます。測定された RSSI は、Location Appliance が環境に割り当てられたパス損失モデルを微調整するために使用され、通常、その結果として精度および確度が向上します。この項には、サイト調整、調整の有効性、調整クライアントの選択、および調整パフォーマンス全体の向上に関する重要なヒントが含まれます。Cisco Compatible Extensions WLAN クライアント仕様バージョン 2 または以降と適合するクライアントを使用して調整を実行する場合の利点についても、この項で詳しく説明します。

RFID タグの考慮事項

現在市販用に製造されている RFID タグの大部分は、超小型回路とアンテナで構成された*パッシブ* RFID タグです。このタグは、パッシブ RFID タグ リーダーまたは*送信機*の電磁フィールド内に存在する場合にのみ活発に通信するため、パッシブ タグと呼ばれています。

現在市場に出回っている別の種類の一般的な RFID タグは、*アクティブ* RFID タグとして知られており、通常は、RF 通信に直接電源を供給するバッテリが内蔵されています。この内蔵電源によって、アクティブ RFID タグは、それ自体に関するさまざまな情報を RFID タグ リーダーに、連続的に*ビーコン送信*する、または要求されたときのみ送信できます。通常、アクティブ タグは、純粋なパッシブ タグ設計よりもサイズが大きく、より多くの情報を格納できます（メモリ容量が多いため）。

『Wi-Fi Location-Based Services: Design and Deployment Considerations』の「RFID Tag Considerations」の項では、RFID に精通していない読者向けに、アクティブ タグとパッシブ タグの両方のテクノロジーの基礎情報を提供しています。特に、次の項目について包括的に説明しています。

- パッシブ RFID テクノロジー：パッシブおよびセミパッシブ RFID タグ
- アクティブ RFID テクノロジー：ビーコン送信、トランスポンダ、および 802.11Wi-FiRFID タグ
- マルチモード RFID テクノロジー：単一のデバイスで複数のタグ テクノロジーを提供する比較的新しいカテゴリ
- チョークポイント トリガー：タグがオペレーション領域に入るときにタグをトリガーしてその設定または動作を修正する近接通信デバイス（通常は単に「チョークポイント」と言う）
- Location Appliance での RFID タグの使用：アセット タグ トラッキング、アセット タグの設定、および 802.11g ネットワーク上での 802.11b タグの使用を可能にする互換性のある RFID タグ
- タグ テレメトリおよび通知の考慮事項：テレメトリおよび緊急事態通知機能に依存するソリューションの設計に関する、初期のベスト プラクティスの推奨事項とその他の有用な情報を提供します。
- チョークポイント設計の考慮事項：Cisco UWN のロケーション検索機能をチョークポイントベースの近接ローカリゼーションによって拡張するソリューション設計に関する、ベスト プラクティスの推奨事項とその他の情報を提供します。

SOAP/XML Application Programming InterfaceAPI; アプリケーション プログラミング インターフェイス）

企業内でロケーションベース アプリケーションの展開を促進するために、Cisco Wireless Location Appliance には SOAP/XML API が付属しています。アプリケーションは、ビルディング、フロア、アクセス ポイント、チョークポイント、カバレッジ領域、およびデバイス リストを含むネットワーク全体のマップなどのコンポーネントを API 経由でインポートすることによって、Location Appliance に格納されているロケーション情報を使用できます。統計的なデバイス情報のほかに、現在と過去のロケーションのような実用的なデータもインポートできます。領域の境界定義、チョークポイント プロキシミティ、タグの緊急事態または不在ステータス、タグのバッテリ ステータス、許容領域、および許容距離によって、ロケーションベースのアラームと通知をアプリケーション内でトリガーできます。これらすべての機能によって、Cisco Wireless Location Appliance API との SOAP/XML API インターフェイスを使用して、ロケーション対応資産管理、Enterprise Resource Planning（ERP）ツール、ワークフロー自動化システムなどの外部ソフトウェア アプリケーションと統合できます。

高いレベルの視点から見れば、サードパーティ製アプリケーション システムは、SOAP/XML API を使用して、次の 4 つの基本コンポーネントで構成されたロケーション認識システムのメンバとして参加できます。

- ロケーション クライアント：ロケーション クライアントの主要な役割は、ロケーション サーバに保存されたロケーションおよび資産情報へのインターフェイスとして機能することです。
- コントロール クライアント：コントロール クライアントの主要な役割は、物理環境についての情報（ネットワーク設計、フロア マップ、調整モデル、アクセス ポイントのロケーションなど）および監視すべきネットワーク要素をサーバに入力することです。
- ロケーション サーバ：ロケーション サーバは Cisco UWN に一般的なロケーション サービスを提供し、デバイスのロケーションを予測するアルゴリズムの実行を担当します。
- WLAN システム：WLAN コントローラに組み込まれたソフトウェアだけでなく、無線ネットワークの主要コンポーネントとして機能するすべての監視対象モバイル デバイス（タグ、モバイル ステーション、不正クライアント、およびアクセス ポイント）と補助デバイス（チョークポイント トリガーなど）。

シスコ テクノロジー パートナーによるロケーション クライアント実装の詳細な説明は、次の場所にある『Design Considerations for Cisco PanGo Asset Tracking』を参照してください。
http://www.cisco.com/univercd/cc/td/doc/solution/pangoex.pdf

Location Appliance API は、ソリューション開発を促進するためのツールと共に、シスコ開発コミュニティに提供およびライセンスされています。統合サポートは、Cisco Developer Services Program から利用できます。このプログラムの詳細は、http://www.cisco.com/go/developersupport を参照してください。

GLOSSARY

A

AAA	Authentication、Authorization、Accounting（認証、認可、アカウンティング）
ACS	Cisco Access Control Server
AES	Advanced Encryption Standard（高度暗号化規格）
AP	アクセス ポイント

B

BSSID	Basic Service Set Identifier（基本サービス セット識別子）

C

CAM	Clean Access Manager
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CCX	Cisco Compatible Extensions
CKIP	Cisco Key Integrity Protocol
CMIC	Cisco Message Integrity Check
CSA	Cisco Security Agent
CSSC	Cisco Secure Services Client。Cisco Key Integrity Protocol（CKIP）および Cisco Message Integrity Check（CMIC）

D

DoS	Denial of Service（サービス妨害）

E

EAP	Extensible Authentication Protocol（拡張認証プロトコル）
EAP-FAST	EAP-Flexible Authentication via Secured Tunnel
EAP-TLS	EAP-Transport Layer Security

EIRP Effective Isotropic Radiated Power

ESSID Extended Service Set Identifier（拡張サービス セット識別子）― 通常は「SSID」

F

FWSM Firewall Services Module

I

IDS Intrusion Detection System（侵入検知システム）

IPS Intrusion Prevention System（侵入防御システム）

L

LAP LWAPP アクセス ポイント

LBS Location-based Service（ロケーションベース サービス）

LWAPP Lightweight Access Point Protocol（Lightweight アクセス ポイント プロトコル）

M

MAP メッシュ AP

MFP Management Frame Protection（管理フレーム保護）

MIC Message Integrity Check（メッセージ完全性チェック）

N

NAC Network Admission Control（ネットワーク アドミッション制御）

O

OFDM Orthogonal Frequency Division Multiplexing（直交周波数分割多重方式）

P

PEAP GTC Protected EAP Generic Token Card

PEAP MSCHAP Protected EAP Microsoft Challenge Handshake Authentication Protocol

PKI Public Key Infrastructure（公開鍵インフラストラクチャ）

R

RADIUS	Remote Authentication Dial-In User Service
RF	無線周波
RFID	Radio-Frequency Identification（無線タグ）
RLDP	Rogue Location Discovery Protocol（不正ロケーション検出プロトコル）
RSSI	Received Signal Strength Indication（受信信号強度表示）

S

SNR	信号対雑音比
SSID	IEEE 拡張サービス セット識別子
SSO	Single Sign-On（シングル サインオン）
SVI	Switched Virtual Interface（スイッチ仮想インターフェイス）

T

TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security

W

WCS	Wireless Control System
WEP	Wired Equivalent Privacy
Wi-Fi	Wi-Fi Alliance のブランド。製品とサービスの相互運用性を IEEE 802.11 テクノロジーに基づいて認定
WiSM	Wireless Services Module
WLAN	無線 LAN
WLC	Wireless LAN Controller
WLCM	Wireless LAN Controller Module
WLSM	Wireless LAN Services Module
WMM	Wi-Fi Multimedia（Wi-Fi マルチメディア）
WPA	Wi-Fi Protected Access