Enterprise Mobility 8.5 設計ガイド

最終更新日:12/24/18

シスコシステムズ合同会社
http://www.cisco.com/jp

シスコは世界各国 200 箇所にオフィスを開設しています。
各オフィスの住所、電話番号、FAX 番号は
当社の Web サイトをご覧ください。
www.cisco.com/go/offices をご覧ください。

【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。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校（UCB）により、UNIX オペレーティング システムの UCB パブリック ドメイン バージョンの一部として開発されたプログラムを適応したものです。

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

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

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

CONTENTS

Cisco Unified Wireless Network ソリューションの概要

この章では、企業向けの Cisco Unified Wireless Network の利点および特徴の概要を示します。Cisco Unified Wireless Network ソリューションは、安全かつスケーラブルで費用効率の高い無線 LAN を提供し、ビジネスに不可欠なモビリティを実現します。Cisco Unified Wireless Network は、企業が直面する無線 LAN（WLAN）のセキュリティ、展開、管理、および制御の問題に費用効率の高い方法で対処するための、業界で唯一の有線およびワイヤレスの統合ソリューションです。この強力な屋内および屋外用ソリューションでは、有線および無線ネットワーク要素のベストな組み合わせにより、高性能で管理しやすく安全な WLAN を安い総所有コストで提供します。

WLAN の概要

モバイル ユーザには、有線ユーザが現在利用しているものと同等のアクセシビリティ、セキュリティ、Quality-of-Service（QoS）、および高可用性が必要です。仕事場、自宅、外出先や、国内でも海外でも、接続する必要があります。そこには技術的な課題が明らかに存在します。しかしここで、モビリティがあらゆるユーザのためにその役割を果たします。企業は、モバイル ソリューションとワイヤレス ソリューションからビジネス価値を引き出しています。かつては特定業種向けのテクノロジーであったものが今では主流となり、音声やリアルタイム情報、または電子メールやカレンダー、エンタープライズ データベース、サプライ チェーン管理、営業支援システム（SFA）、顧客関係管理（CRM）などの重要なアプリケーションにアクセスするうえで不可欠なツールとなっています。

WLAN ソリューションのメリット

WLAN によって実現されるメリットには次のようなものがあります。

- *ビルやキャンパス内のモビリティ*：常時稼働のネットワークを必要とし、さらにキャンパス環境内での移動を伴うことの多いアプリケーションの導入を実現します。
- *利便性*：大規模でオープンなユーザ エリアのネットワークをシンプルにします。
- *柔軟性*：ケーブルが届く範囲ではなく、最も適しているか便利な場所で作業できるようになります。重要なのは、どこで作業をするかではなく、作業を終わらせることです。
- *一時的なスペースのセットアップが容易*：参加者数の変動に合わせて、会議室、作戦指令室、またはブレインストーミング ルームのネットワーク設定を迅速に行うことができます。
- *ケーブル敷設費用の削減*：WLAN の実装により隙間なくカバーできるため、ケーブル設備を予定外に設置する必要性が減少します。

- *追加や移動、変更が容易で、サポートやメンテナンスのコストも削減*:一時的なネットワークのセットアップが非常に簡単になるため、移行に関する問題が軽減され、コストのかかる直前の変更も容易になります。
- *効率アップ*:調査により、WLAN ユーザは有線で接続しているユーザよりも 1 日に 15 % 長くネットワークに接続していることがわかっています。
- *生産性アップ*:ネットワーク接続へのアクセスをより簡単にすることで、ビジネスの生産性を向上させるツールの使用が促進されます。生産性の調査では、WLAN ユーザによるツールの使用が 22 % 増加していることがわかっています。
- *コラボレーションが容易*:会議室など任意の場所からのコラボレーション ツールへのアクセスが簡単になります。ファイルがその場で共有され、情報に対する要求が即座に処理されます。
- *オフィスのスペースの有効利用*:柔軟性が向上するため、大規模なチーム ミーティングなどのグループにも対応できます。
- *エラーの減少*:ネットワーク アクセスが使用可能な場合でも、収集されたデータを直接システムに入力できます。
- *企業のパートナーとゲストの効率、性能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実現できます。
- *ビジネスの復元力の向上*:WLAN によって従業員のモビリティが向上し、他の場所への再配置を迅速に行えるようになります。

WLAN システムの要件

WLAN システムは、既存の有線エンタープライズ ネットワークに付属するシステムとして、またはキャンパスやブランチ内の独立したネットワークとして稼働します。また WLAN は、小売、製造、または医療業界における、ロケーション ベースのサービスなどの用途で利用することができます。WLAN では、リソースに有線で接続されているかのようにデータや通信、ビジネス サービスにアクセスできる、安全かつ暗号化された承認済みの通信が許可される必要があります。

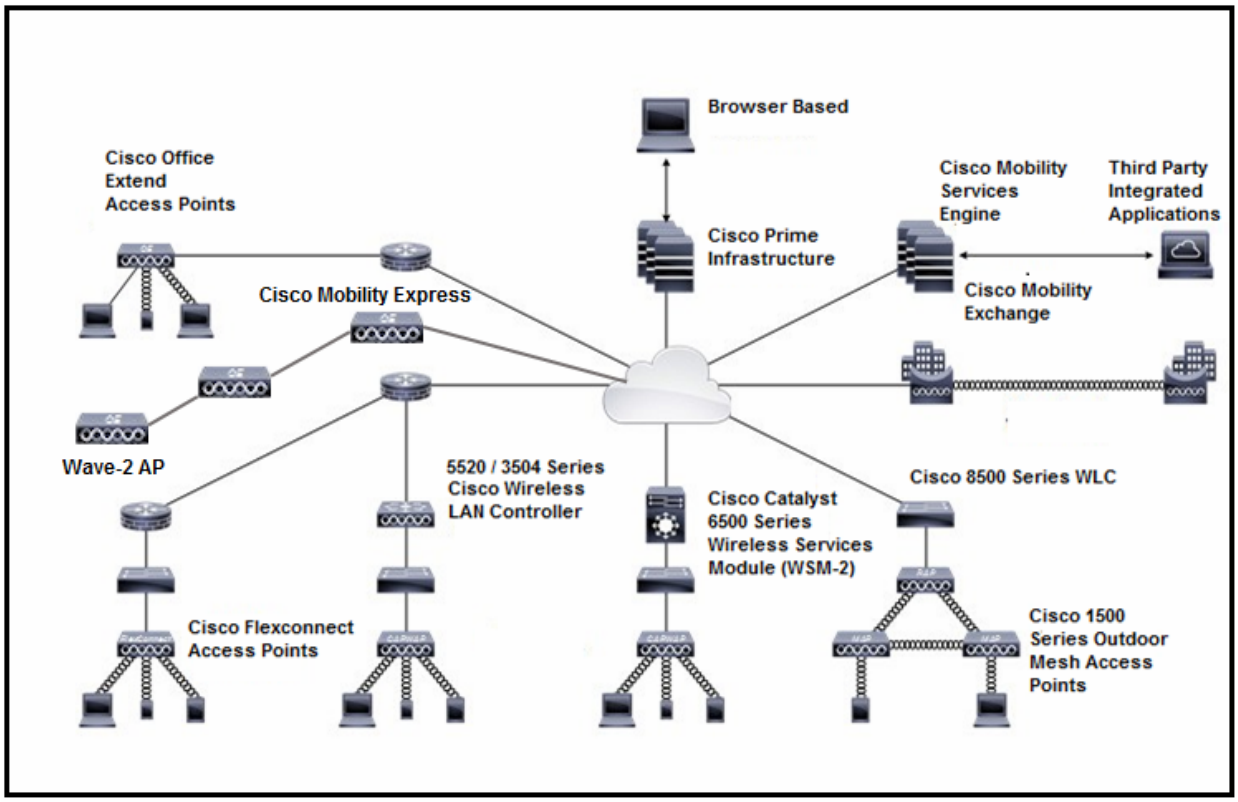
WLAN には次のような機能が必要となります。

- *従業員がネットワークに有線接続していないときもリソースへのアクセシビリティを維持*:このアクセシビリティにより、従業員は会議室で顧客と商談中でも、会社の食堂で同僚と昼食中でも、隣のビルでチームメートと一緒に作業中でも、ビジネス ニーズにより迅速に応えることができます。
- *無許可や安全でない、または「不正な」WLAN アクセス ポイント(AP)から企業を保護*:IT マネージャは、不正な AP やその AP が接続しているスイッチ ポート、さらには、そのような AP のアクティブな参加や、RF 環境を連続的にスキャンおよび監視しているクライアント デバイスを、簡単かつ自動的に検出および特定できる必要があります。
- *移動するユーザにまで統合ネットワーク サービスの利点を拡張*:QoS を使用する WLAN 上での IP テレフォニーと IP ビデオ会議に対応しています。リアルタイムのトラフィックを優先して処理することにより、ビデオと音声の情報がタイムラグなしで到着します。エンタープライズ フレームワークの一部であるファイアウォールと侵入検知システムが、ワイヤレス ユーザまで拡張されます。
- *許可されたユーザの分類と不正なユーザのブロック*:ワイヤレス ネットワークのサービスを、ゲストやベンダーまで安全に拡張できます。WLAN では、別のパブリック ネットワーク、すなわちゲスト ネットワークに対するサポートを設定できる必要があります。

- *他のサイトから来た従業員でも、簡単かつ安全にネットワークにアクセス*:空き部屋や利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、どの WLAN ロケーションからでもネットワークに安全にアクセスする必要があります。従業員は IEEE 802.1x および Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）によって認証され、WLAN 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 AP を簡単に管理*:ネットワーク管理者は、WLAN を導入したキャンパスやブランチ オフィス、または店舗や製造施設、医療機関などにある数百から数千の AP を簡単に展開、操作、管理できる必要があります。結果として、有線 LAN に期待されるものと同じレベルのセキュリティや拡張性、信頼性、展開しやすさ、管理を中規模から大規模な組織に提供する 1 つの枠組みが生まれることが理想です。
- *セキュリティ サービスの強化*:ワイヤレス経由で侵入する脅威を封じ込め、セキュリティ ポリシーのコンプライアンスを実施し、情報を保護するため、WLAN 侵入防御システム（IPS）および侵入検知システム（IDS）が制御します。
- *音声サービス*:Cisco Unified Wired and Wireless Network と Cisco Compatible Extensions の音声対応クライアント デバイスにより、音声通信にワイヤレス ネットワーキング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*:高価値資産のトラッキング、IT 管理、ロケーション ベースのセキュリティ、ビジネス ポリシーの適用などの不可欠な用途のための WLAN インフラストラクチャから直接、数百から数千の Wi-Fi およびアクティブ RFID デバイスを同時に追跡できます。
- *ゲスト アクセス*:顧客、ベンダー、パートナーが有線およびワイヤレス LAN に簡単にアクセスできるようにし、生産性を向上させ、リアルタイムのコラボレーションを促進し、会社の競争力を維持し、WLAN のセキュリティを完全に確保します。

企業内 WLAN は、より大規模な社内ネットワークやインターネットに接続するための最も効果的な方法の 1 つとなっています。図 1-1 では、Cisco Unified Wireless Network の要素を示します。

図 1-1　企業内の Cisco Unified Wireless Network アーキテクチャ



次のような相互接続された要素の連携により、統合されたエンタープライズ クラスのワイヤレス ソリューションが実現されます。

- クライアント デバイス
- アクセス ポイント（AP）
- コントローラを通じたネットワーク統合
- 世界クラスのネットワーク管理
- モビリティ サービス

クライアント デバイスの基本から始まり、ネットワークのニーズの発展と成長に応じてそれぞれの要素が機能を追加し、上下の要素と相互接続することで、総合的かつ安全な WLAN ソリューションが完成します。

Cisco Unified Wireless Network

Cisco Unified Wireless Network のコア コンポーネントに含まれるものは次のとおりです。

- Aironet アクセス ポイント（AP）
- ワイヤレス LAN コントローラ（WLC）
- Cisco Prime Infrastructure

Cisco Unified Wireless Network の詳細については、次の URL を参照してください。

http://www.cisco.com/go/unifiedwireless

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、企業の Cisco Unified Wireless Network を導入する場合の、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。

- CAPWAP
- コア コンポーネント
- ローミング
- WLC でのブロードキャストおよびマルチキャスト
- 設計上の考慮事項
- 運用およびメンテナンス

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 テクノロジーの詳細については、次の Web サイトにある Cisco 5500 シリーズ ワイヤレス LAN コントローラに関連する導入戦略を説明したシスコのホワイト ペーパーを参照してください。

http://www.cisco.com/en/US/products/ps10315/prod_white_papers_list.html

CAPWAP

Internet Engineering Task Force（IETF）標準規格の Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、シスコの中央集中型 WLAN アーキテクチャ（Cisco Unified Wireless Network ソリューションの機能アーキテクチャ）で使用される基盤となるプロトコルです。CAPWAP は、AP と WLAN コントローラ（WLC）の間の WLAN クライアント トラフィックのカプセル化と転送に加えて、AP と WLAN の設定および管理を行います。

CAPWAP は Lightweight Access Point Protocol（LWAPP）に基づいていますが、Datagram Transport Layer Security（DTLS）によるセキュリティ強化が追加されています。CAPWAP では User Datagram Protocol（UDP）を使用しており、インターネット プロトコル バージョン 4（IPv4）とインターネット プロトコル バージョン 6（IPv6）のどちらでも動作します。表 2-1 に、各 CAPWAP バージョンのプロトコルとポートの実装を示します。

表 2-1　CAPWAP のプロトコルおよびポート

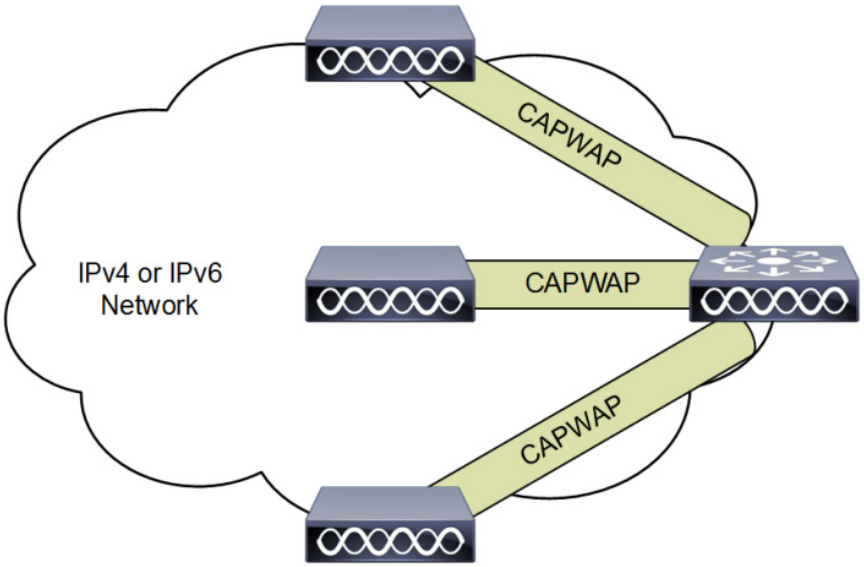
インターネット プロトコル	IP プロトコル	宛先ポート	説明
バージョン 4	17（UDP）	5,246	CAPWAPv4 制御チャネル
	17（UDP）	5,247	CAPWAPv4 データ チャネル
バージョン 6	136（UDP Lite）	5,246	CAPWAPv6 制御チャネル
	136（UDP Lite）	5,247	CAPWAPv6 データ チャネル

IPv6 では、AP と WLC のパフォーマンスに影響を与える User Datagram Protocol（UDP）の完全なペイロード チェックサムが必須です。IPv6 導入に対するパフォーマンスを最大化するために、AP および WLC では、ペイロード全体ではなくヘッダーのみのチェックサムを実行する UDP Lite を実装しています。

（注）　リリース 5.2 以降では、LWAPP は非推奨になっており、CAPWAP によって置換されています。5.2 以降で動作している WLC に接続する古い LWAPP AP は CAPWAP をサポートするように自動的にアップグレードされます。

図 2-1 は、CAPWAP AP が CAPWAP プロトコル経由で WLC に接続する基本的な中央集中型 WLAN 展開の概略図を示しています。リリース 8.0 以降では、CAPWAP は IPv4 と IPv6 のいずれのトランスポート モードでも動作可能です。デフォルトでは、IPv4 が推奨されますが設定可能です（この項で後述）。

図 2-1　WLC に接続された CAPWAP AP



(注)　CAPWAP 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、本書では中央集中型 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。

シスコでは、CAPWAP を実装するときは、次のガイドラインに従うことを推奨します。

- IP アドレッシング：WLC を正常に検出し、通信できるようにするには、AP に静的または動的な IPv4 または IPv6 アドレスを割り当てる必要があります。レイヤ 2 モードは CAPWAP ではサポートされません。
- ファイアウォール ルールおよび ACL：AP と WLC の間に配置されているデバイスに定義されているすべてのファイアウォール ルールおよび ACL は、CAPWAP プロトコルを許可するように設定されている必要があります（表 2-1 を参照）。
- IPv6 導入：IPv6 をサポートしていない古いファームウェアで動作している AP をサポートするために、少なくとも 1 台の WLC は IPv4 と IPv6 の両方用に設定されている必要があります。

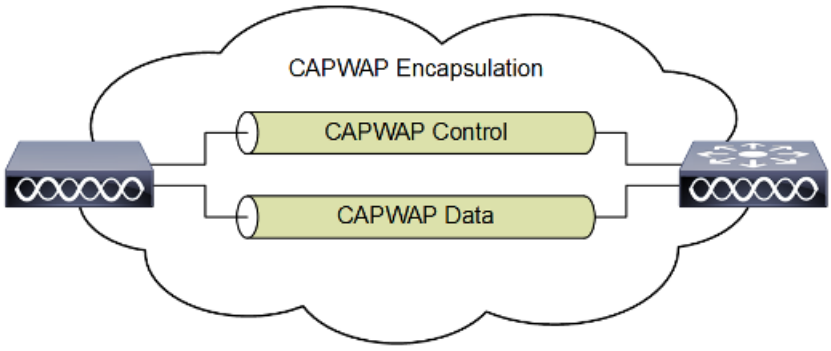
CAPWAP の主要機能は、以下のとおりです。

- スプリット MAC アーキテクチャ
- 暗号化
- レイヤ 3 トンネル
- WLC ディスカバリおよび選択

スプリット MAC アーキテクチャ

CAPWAP 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 CAPWAP 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 2-2 は、スプリット MAC の概念を示しています。

図 2-2　スプリット MAC アーキテクチャ



Access Point MAC Functions:

- 802.11: Beacons, Probe Responses.
- 802.11 Control: Packet Acknowledgements and Transmission.
- 802.11e: Frame Queuing and Packet Prioritization.
- 802.11i: MAC Layer Data Encryption and Decryption.

Controller MAC Functions:

- 802.11 MAC: Management: Association Requests and Actions.
- 802.11e: Resource Reservation.
- 802.11i: Authentication and Key Management.

図 2-3 に示す最も単純な汎用 802.11 AP は、基本サービス セット識別子（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。802.11 規格では、前述のシングル AP の概念が拡張され、図 2-4 に示すように、複数台の AP で Extended Service Set（ESS）を提供できます。この場合、複数台の AP で同じ ESS Identifier（ESSID、通常 SSID と呼ばれます）を使用することで、WLAN クライアントが複数の AP を経由して共通のネットワークに接続できます。

図 2-5 の CAPWAP 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、次の 2 つの機能コンポーネントに割り振ります。

- CAPWAP AP
- WLC

この 2 つのコンポーネントは、ネットワーク経由で CAPWAP 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、導入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 CAPWAP 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 の導入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 2-3　シングル AP

図 2-4　ESS に組み込まれた AP

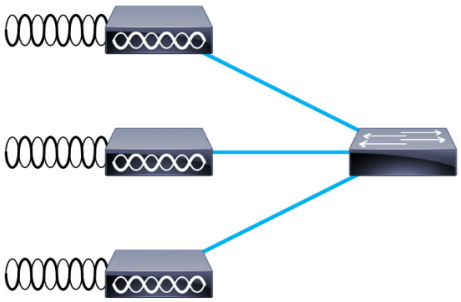
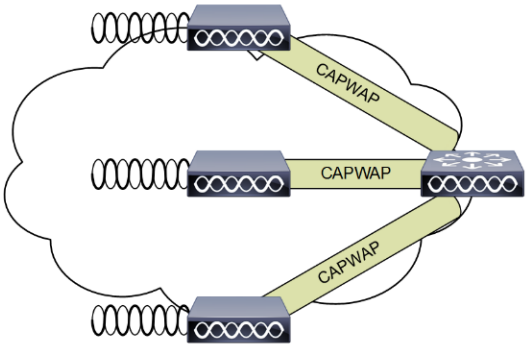


図 2-5　CAPWAP スプリット MAC ESS



単純で時間に依存した処理は、通常 CAPWAP 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、CAPWAP 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 フレームの伝送。
- 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伝送。
- 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。

その他の機能も WLC によって処理されます。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 フレームの変換およびブリッジング
- 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、FlexConnect AP（本書の後半で説明）は除く

CAPWAP 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。

- CAPWAP 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。
- ワイヤレス 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、WLC で対応するインターフェイス（VLAN）またはインターフェイス グループ（VLAN プール）にマッピングされます。このインターフェイスのマッピングは、WLC で WLAN の構成時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、WLC でローカルに定義したポリシーか、認証が正常に終了した時点でアップストリーム AAA サーバから転送される RADIUS が返却する属性に基づいて、WLAN クライアントを特定の VLAN に動的にマッピングすることもできます。

一般的な WLAN の設定パラメータには、VLAN の割り当てのほか、次のものがあります。

- SSID 名
- Operational State
- 無線ポリシー
- 認証およびセキュリティ方式
- QoS/アプリケーションの可視性と制御
- ポリシーのマッピング

暗号化

リリース 6.0 以降では、DTLS を使用して AP と WLC の間で交換される CAPWAP コントロール パケットおよびデータ パケットの暗号化のサポートを提供しています。DTLS は TLS に基づいた IETF プロトコルです。すべての Cisco アクセス ポイントおよびコントローラには、AP および WLC が相互認証と暗号キーの生成にデフォルトで使用する、製造元でインストールされる証明書（MIC）が付属しています。Cisco では、独自の認証局（CA）から証明書を発行することを希望する企業向けに追加のセキュリティを提供するローカルで有効な証明書（LSC）もサポートしています。

（注）　DTLS ではデフォルトで、**config ap dtls-cipher-suite** コマンドを使用してグローバルに定義されている RSA 128 ビット AES/SHA-1 暗号スイートを使用します。代替暗号方式としては、SHA-1 または SHA-256 を使用する 256 ビット AES があります。

CAPWAP 制御チャネルを保護するために DTLS は、デフォルトではイネーブルになっていますが、データ チャネルではデフォルトでディセーブルになっています。制御チャネルを保護するために、DTLS ライセンスは必要ありません。AP と WLC の間で交換されるすべての CAPWAP 管理トラフィックおよびコントロール トラフィックは、コントロール プレーン プライバシーを提供するためと中間者（MIM）攻撃を防止するためにデフォルトで暗号化および保護されます。

CAPWAP データ暗号化はオプションであり、AP ごとに有効化されます。データ暗号化を使用するには、AP で有効化する前に、WLC に DTLS ライセンスをインストールしておく必要があります。有効化されている場合、すべての WLAN クライアント トラフィックは AP で暗号化されてから WLC に転送されます。この逆も同様です。DTLS データ暗号化は OfficeExtend AP に対しては自動的に有効化されますが、他のすべての AP に対してはデフォルトで無効化されます。ほとんどの AP はデータ暗号化を必要としない保護されたネットワークに導入されます。反対に、OfficeExtend AP と WLC の間のトラフィックは保護されていないパブリック ネットワーク越しに転送されるため、これらの AP ではデータ暗号化が重要です。

（注）　現地の規制において DTLS 暗号化が許可されていることをご確認ください。たとえば、DTLS データ暗号化は現在ロシアでは禁止されています。

WLC での DTLS データ暗号化可用性は次のとおりです。

- Cisco 5508：DTLS データ サポートありでもなしでも注文できます。cisco.com では、DTLS サポートがあるファームウェア イメージと DTLS サポートがないファームウェア イメージが個別に提供されています。
- Cisco 2500、3504、5520、8540、WiSM2、vWLC：DTLS データ サポートを有効化するには、ライセンスを別途購入する必要があります。
- Cisco 3504、Flex 7500 および 8510：DTLS データ サポートが組み込まれています。DTLS データ サポートを有効化するためにライセンスを別途購入またはインストールする必要はありません。

DTLS データ暗号化が使用できる AP は次のとおりです。

- Cisco 1522、1530、1540、1550、1552、1560、1600、1700、1810、1815、1850、2600、2700、2800、3500、3600、3700、および 3800 シリーズ：DTLS データ暗号化はハードウェアで行われます。

(注)　DTLS データ暗号化を有効にすると、AP と WLC の両方のパフォーマンスに影響します。したがって DTLS データ暗号化は、保護されていないネットワーク越しに導入されている AP だけで有効化する必要があります。

レイヤ 3 トンネル

レイヤ 2 とレイヤ 3 のいずれのモードでも動作する LWAPP とは異なり、CAPWAP はレイヤ 3 でのみ動作し、AP と WLC の両方で IP アドレスの提示を必要とします。CAPWAP では、IPv4 導入には UDP、IPv6 導入には UDP または UDP Lite（デフォルト）を使用することで、中間ネットワーク越しの AP と WLC 間の通信を円滑にしています。CAPWAP でトンネル パケットのフラグメンテーションおよびリアセンブルを実施できます。これにより、WLAN クライアント トラフィックでは 1500 バイトの MTU 全体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リアセンブル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 を導入するうえ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。

以下の図は、IPv4 ネットワーク越しの CAPWAP 操作を示すための CAPWAP パケット キャプチャです。復号化のサンプルは、Wireshark パケット アナライザを使用してキャプチャしたものです。

図 2-6 は、CAPWAP コントロール パケットの復号化を示しています。WLC からのすべての CAPWAP コントロール パケットと同様、このパケットも WLC から UDP 宛先ポート 5246 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 CAPWAP AP に渡すために WLC により使用されるコンフィギュレーション コマンドを表します。CAPWAP コントロール パケットのペイロードは、AP が WLC に接続している場合、デフォルトで DTLS を使用して AES 暗号化されます。

図 2-6　CAPWAP コントロール パケット

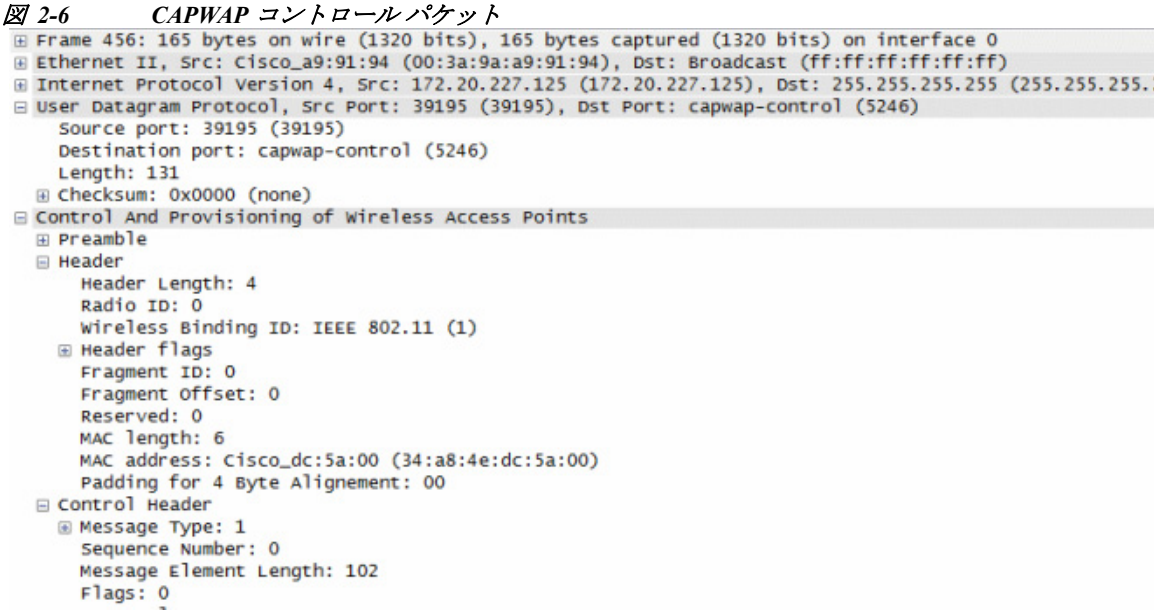


図 2-7 は、802.11 プローブ要求を含む CAPWAP パケットの復号化の一部を示しています。すべての CAPWAP でカプセル化される 802.11 フレームと同様、このパケットも UDP 宛先ポート 5246 を使用して CAPWAP AP から WLC に送られるパケットです。この例では、RF 情報を WLC に提供するために、CAPWAP パケットには、受信信号強度表示（RSSI）の値と信号対雑音比（SNR）の値も含まれています。この例では、DTLS データ暗号化は有効になっていません。

図 2-7　CAPWAP の 802.11 プローブ要求

```
⊞ Frame 668: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
⊞ Ethernet II, Src: Cisco_42:57:5c (44:d3:ca:42:57:5c), Dst: Cisco_da:78:20 (64:d8:14:da:78:20)
⊞ Internet Protocol Version 4, Src: 172.20.227.123 (172.20.227.123), Dst: 172.20.227.99 (172.20.227.99)
⊟ User Datagram Protocol, Src Port: 9590 (9590), Dst Port: capwap-data (5247)
    Source port: 9590 (9590)
    Destination port: capwap-data (5247)
    Length: 117
  ⊞ Checksum: 0x0000 (none)
⊟ Control And Provisioning of Wireless Access Points
  ⊞ Preamble
  ⊟ Header
      Header Length: 4
      Radio ID: 0
      Wireless Binding ID: IEEE 802.11 (1)
    ⊟ Header flags
        1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
        .0.. .... . = Fragment: Don't Fragment
        ..0. .... . = Last Fragment: More fragments follow
        ...1 .... . = Wireless header: Wireless Specific Information is present
        .... 0... . = Radio MAC header: No Radio MAC Address
        .... .0.. . = Keep-Alive: No Keep-Alive
        .... ..00 0 = Reserved: Not set
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      Wireless length: 4
      Wireless data: 00000000
    ⊟ Wireless data ieee80211 Frame Info: 00000000
        Wireless data ieee80211 RSSI (dBm): 0
        Wireless data ieee80211 SNR (dB): 0
        Wireless data ieee80211 Data Rate (Mbps): 0
      Padding for 4 Byte Alignement: 000000
⊞ IEEE 802.11 Probe Request, Flags: ........
```

図 2-8 は、別の CAPWAP 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 2-7 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。この図は、CAPWAP 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 2-8 は、AP と WLC の間の CAPWAP 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。

（注） Wireshark 復号化では、フレーム制御復号化バイトがスワップされています。これは、一部の AP がこれらのバイトをスワップすることを考慮して、CAPWAP パケットの Wireshark プロトコルの解析中に実行されます。この例では、DTLS データ暗号化は有効になっていません。

図 2-8　CAPWAP データ フレーム

```
Internet Protocol Version 4, Src: 172.20.227.100 (172.20.227.100), Dst: 172.20.227.125 (172.20.227.125)
User Datagram Protocol, Src Port: capwap-data (5247), Dst Port: 39195 (39195)
  Source port: capwap-data (5247)
  Destination port: 39195 (39195)
  Length: 42
⊞ Checksum: 0x0000 (none)
Control And Provisioning of Wireless Access Points
⊞ Preamble
⊟ Header
    Header Length: 2
    Radio ID: 1
    Wireless Binding ID: IEEE 802.11 (1)
  ⊟ Header flags
      1... .... . = Payload Type: Native frame format (see Wireless Binding ID field)
      .0.. .... . = Fragment: Don't Fragment
      ..0. .... . = Last Fragment: More fragments follow
      ...0 .... . = Wireless header: No Wireless Specific Information
      .... 0... . = Radio MAC header: No Radio MAC Address
      .... .0.. . = Keep-Alive: No Keep-Alive
      .... ..00 0 = Reserved: Not set
    Fragment ID: 0
    Fragment Offset: 0
    Reserved: 0
IEEE 802.11 Disassociate, Flags: ........
  Type/Subtype: Disassociate (0x0a)
⊞ Frame Control: 0x00A0 (Swapped)
  .000 0000 0000 0000 = Duration: 0 microseconds
  Destination address: Apple_d1:22:39 (18:20:32:d1:22:39)
  Source address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  BSS Id: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
  Fragment number: 0
  Sequence number: 0
```

CAPWAP モード

リリース 8.0 以降、Cisco Unified Wireless Network（CUWN）では、IPv4 と IPv6 のいずれのアドレッシングを使用しているアクセス ポイントおよびコントローラもサポートしています。ネットワーク管理者は AP と WLC の導入に純然たる IPv4 または IPv6 のネットワークを使用することもできれば、デュアルスタック ネットワークを使用して IPv4 から IPv6 への遷移を円滑にすることもできます。8.0 リリースの一環として CAPWAP プロトコルおよびディスカバリ メカニズムが拡張され、IPv6 がサポートされるようになりました。CAPWAP は、特定のネットワーク環境向けに IPv4（CAPWAPv4）モードまたは IPv6（CAPWAPv6）モードで動作可能になりました。

ネットワーク管理者は、両方の IP プロトコル バージョンをサポートするために、AP が WLC を接続するときの優先 CAPWAP モード（CAPWAPv4 または CAPWAPv6）を設定できます。優先モードは次の 2 つのレベルで設定できます。

- グローバル設定（図 2-9）
- AP グループ固有（図 2-10）

図 2-9　CAPWAP 優先モード(グローバル設定)

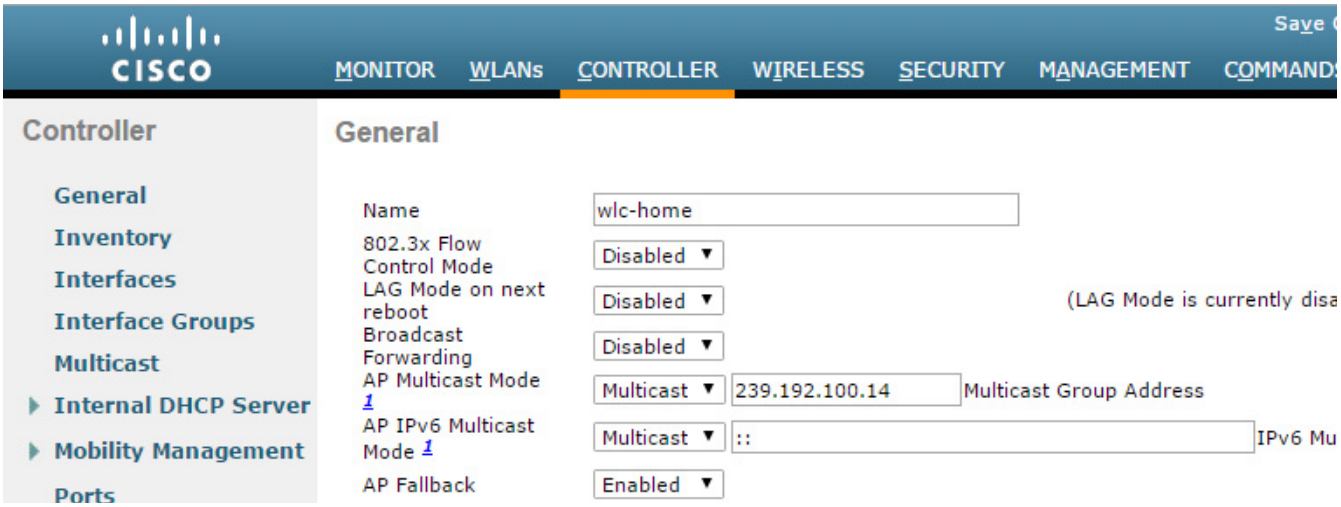
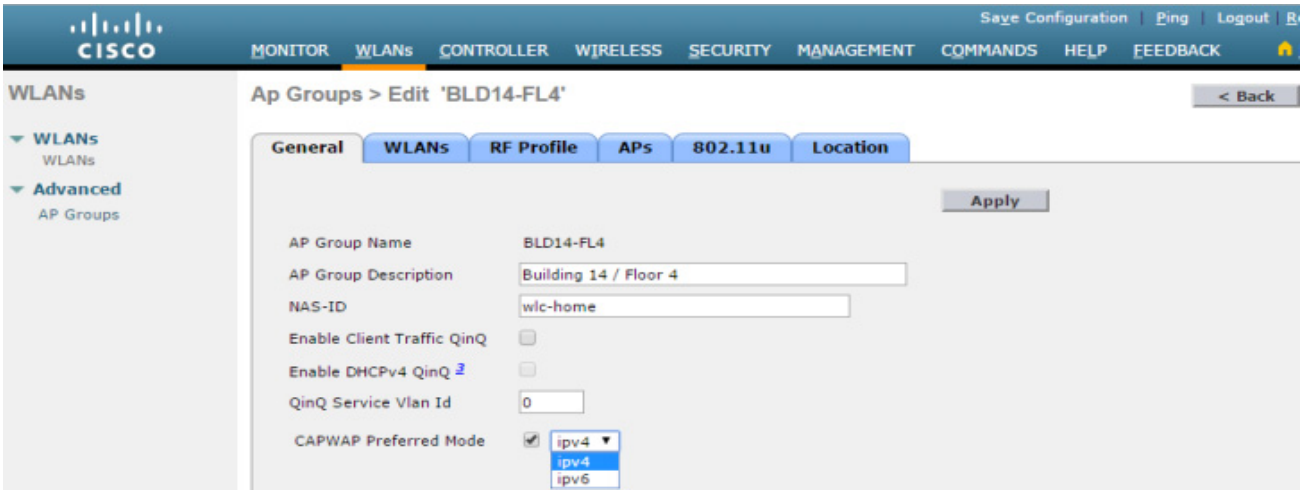


図 2-10　CAPWAP 優先モード(AP グループ固有)



CAPWAP モードでは、AP による選択は、AP と WLC の両方に実装されている IP アドレス バージョン、AP に定義されているプライマリ、セカンダリ、ターシャリの WLC アドレス、AP にプッシュされた優先モードなど、さまざまな要因に基づいて行われます。

使用可能な CAPWAP 動作モードの設定の概要を次に示します。

- デフォルト：グローバル優先モードは、IPv4 に設定され、デフォルト AP グループ優先モードは未設定に設定されます。AP にプライマリ、セカンダリ、またはターシャリ WLC IPv6 アドレスが準備されていない場合を除き、AP ではデフォルトでは IPv4 を優先することになります。
- AP グループ固有：優先モード(IPv4 または IPv6)は、AP グループの優先モードが設定されており、AP がそのグループに属している場合のみ、AP に適用されます。優先モードが定義されていない場合はグローバル優先モードが継承されます。
- グローバル：この優先モードは、デフォルト AP グループおよび優先モードが設定されていないその他のすべての AP グループに適用されます。デフォルト AP グループの優先モードは手動で定義できないことに注意してください。

- 接続失敗：優先モードが設定されている AP がコントローラに接続しようとして失敗すると、他のモードにフォールバックして同じコントローラへの接続を試行します。両方のモードが失敗すると、AP は次のディスカバリ応答に移動します。
- 静的設定：静的 IP 設定はグローバルまたは AP グループ固有の優先モードよりも優先されます。たとえば、グローバル優先モードが IPv4 に設定されており、AP にプライマリ コントローラの静的 IPv6 アドレスが定義されている場合、AP では CAPWAPv6 モードを使用して WLC を接続します。

AP グループ固有の優先モードを使用すると、さまざまな AP グループで利用する CAPWAP トランスポート モードに管理者が具体的に影響を与えることができるため柔軟性が向上します。これにより、異なるビルディングまたはサイトをまたがって導入されている AP が異なる CAPWAP モードを使用して動作できます。たとえば、すでに IPv6 に移行したキャンパスにある AP では CAPWAPv6 を使用して WLC を接続できる一方で、IPv6 にまだ移行していないリモート サイトにある AP では CAPWAPv4 を使用して WLC を接続できます。デュアルスタック設定の個々の WLC では、CAPWAPv4 モードと CAPWAPv6 モードのいずれのモードで動作している CAPWAP AP でもサポートできます。

（注）　IPv6 に対応していない古いイメージを実行している AP は、WLC に IPv4 アドレスが割り当てられている場合に限り、IPv6 対応 WLC を接続できます。IPv4 対応 WLC を接続しようとしている IPv6 対応 AP でも同様です（AP に IPv4 アドレスが割り当てられていることが前提）。IPv6 導入では、検出可能な WLC を 1 台以上、IPv4 をサポートするように設定することをお勧めします。

8.0 で追加された IPv6 強化の詳細については、『Cisco Wireless LAN Controller IPv6 Deployment Guide』を参照してください。

WLC ディスカバリおよび選択

CAPWAP 環境では、Lightweight AP は CAPWAP ディスカバリ メカニズムによって WLC を検知し、コントローラに CAPWAP 接続要求を送信します。AP が WLC を接続すると、WLC によって AP の構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。CAPWAP AP を Cisco Unified Wireless Network のアクティブ パートにするには、その前に AP が WLC を検出して接続する必要があります。

各 Cisco AP では、次のディスカバリのプロセスがサポートされています。

ステップ 1　ブロードキャスト ディスカバリ：AP は、IPv4 ブロードキャスト アドレス（255.255.255.255）に CAPWAP ディスカバリ メッセージを送信します。同じ VLAN に接続されているすべての WLC がディスカバリ メッセージを受信することになり、ユニキャスト IPv4 ディスカバリ応答で応じることになります。

ステップ 2　マルチキャスト ディスカバリ：AP は、すべてのコントローラ マルチキャスト グループ アドレス（FF01::18C）に CAPWAP ディスカバリ メッセージを送信します。同じ VLAN に接続されているすべての WLC がディスカバリ メッセージを受信することになり、IPv6 ディスカバリ応答で応じることになります。

ステップ 3　ローカルに保存されているコントローラの IPv4 または IPv6 アドレス ディスカバリ：AP が事前に WLC に関連付けられていた場合は、プライマリ、セカンダリ、およびターシャリ コントローラの IPv4 または IPv6 アドレスが AP の不揮発性メモリ（NVRAM）に保存されています。今後の導入用に AP にコントローラの IPv4 または IPv6 アドレスを保存するこのプロセスは、「*アクセス ポイントのプライミング*」と呼ばれます。

ステップ 4　DHCP ディスカバリ：DHCPv4 サーバや DHCPv6 サーバは、ベンダー固有のオプションを使用して AP に WLC の IP アドレスをアドバタイズするように設定されます。

- オプション 43 を使用した DHCPv4 ディスカバリ：DHCPv4 サーバはオプション 43 を使用して、1 個以上の WLC 管理 IPv4 アドレスを AP に提供します。オプション 43 値は DHCPv4 の OFFER パケットおよび確認応答パケットで AP に提供されます。
- オプション 52 を使用した DHCPv6 ディスカバリ：DHCPv6 サーバはオプション 52 を使用して、1 個以上の WLC 管理 IPv6 アドレスを AP に提供します。オプション 52 値は DHCPv6 のアドバタイズ パケットおよびリプライ パケットで AP に提供されます。

ステップ 5　DNS ディスカバリ：AP は cisco-capwap-controller.*localdomain*（localdomain は DHCP が割り当てる AP ドメイン名）を解決しようとして DNSv4 サーバや DNSv6 サーバに DNS クエリを送信します。

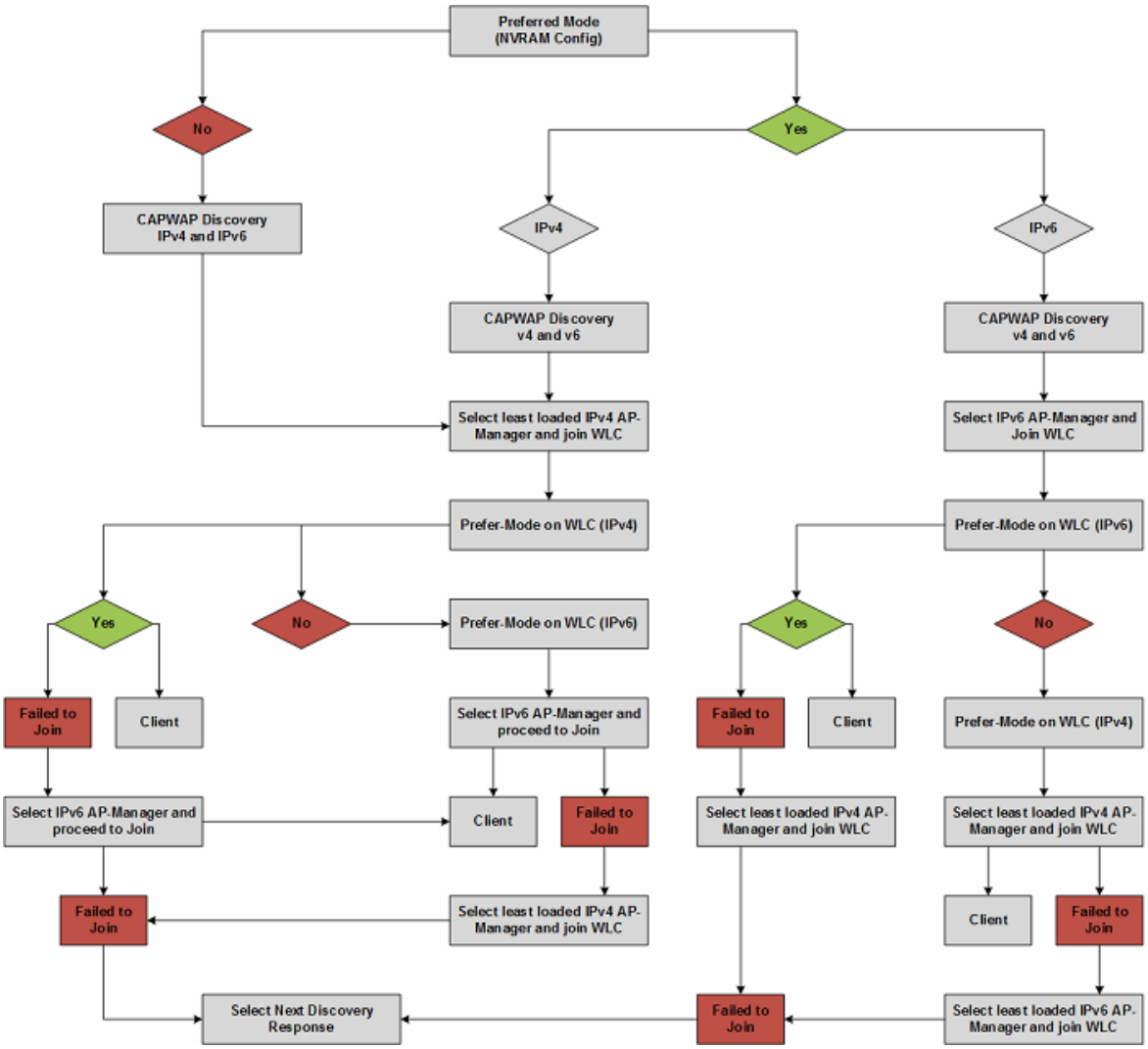
- DNSv4 ディスカバリ：WLC で管理しており、AP に提供される IPv4 アドレスごとに、cisco-capwap-controller ホスト名用のネーム サーバ上にアドレス レコードが定義されます。ネーム サーバでは、定義された各 A レコードに対する IPv4 アドレスのリストをクエリに対して返信します。
- DNSv6 ディスカバリ：WLC で管理しており、AP に提供される IPv6 アドレスごとに、cisco-capwap-controller ホスト名用のネーム サーバ上にアドレス レコードが定義されます。ネーム サーバでは、定義された各 AAAA レコードに対する IPv6 アドレスのリストをクエリに対して返信します。

AP に提供するために DNSv4 または DNSv6 ネーム サーバに最大 3 個のアドレス レコードを定義できます。各レコードは、プライマリ、セカンダリ、およびターシャリの WLC の IPv4 または IPv6 アドレスに対応します。

ステップ 6　ステップ 1 ～ 5 の後、CAPWAP ディスカバリ応答が受信されない場合、AP はディスカバリのプロセスをリセットしてから、再開します。

WLC の選択を終えた AP では、この AP にプッシュされた CAPWAP 優先モードに応じて、CAPWAPv4 と CAPWAPv6 のいずれによって接続するのかを選択します。

図 2-11　　AP CAPWAP ディスカバリの図

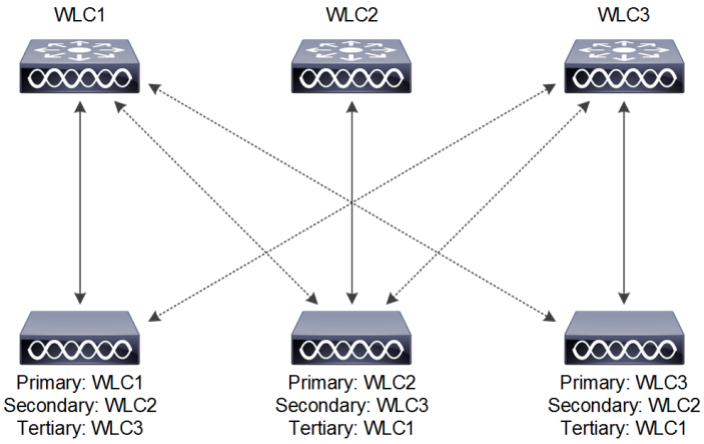


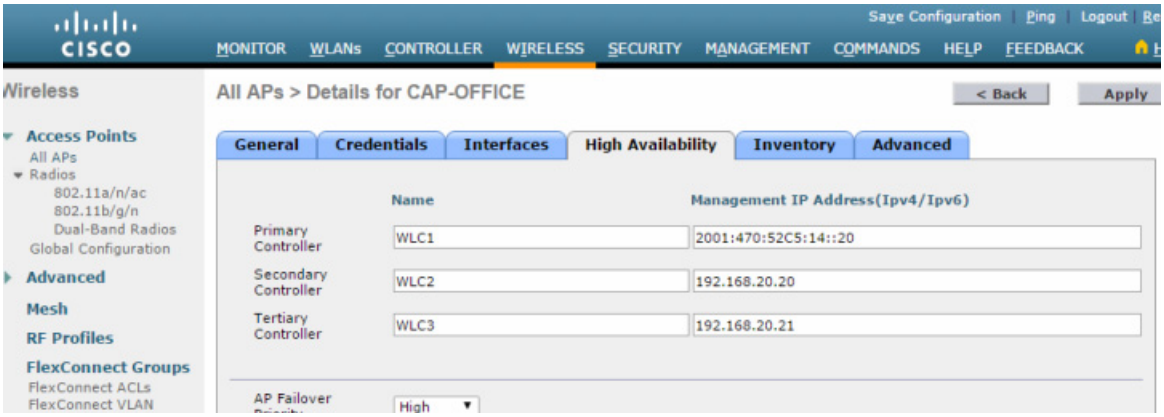
AP プライミング

大部分の導入では、DHCP または DNS ディスカバリを使用して 1 個以上のシード WLC アドレスが提供されます。後続の WLC ディスカバリ応答によって、WLC モビリティ グループ メンバーの完全なリストが AP に提供されます。通常、AP には、優先 WLC を表す、1 ～ 3 個の WLC 管理 IP アドレスのリスト（プライマリ、セカンダリ、およびターシャリ）が設定されています。

優先 WLC が使用できなくなるか、オーバーサブスクライブされている場合、AP は CAPWAP ディスカバリ応答で確認された WLC のリストから別の WLC、つまり、最も負荷の少ない WLC を選択します。

図 2-12　　AP プライミングの例





(注)　AP のプライミングを行う場合、プライマリ コントローラ、セカンダリ コントローラ、およびターシャリ コントローラの管理アドレスは、IPv4 と IPv6 のどちらも使用できます。定義されているアドレスに AP によって到達可能であれば問題ありません。ただし、単一のエントリに IPv4 アドレスと IPv6 アドレスの両方は定義できません。各エントリは、IPv4 または IPv6 のアドレス 1 個のみを含むことができます。

コア コンポーネント

Cisco Unified Wireless Network（CUWN）は、企業およびサービス プロバイダーに高性能でスケーラブルな 802.11ac ワイヤレス サービスを提供するように設計されています。Cisco ワイヤレス ソリューションは、中央集中型または分散型の導入における大規模無線 LAN の導入および管理をシンプルにするとともに同クラス最高のセキュリティ、ユーザ エクスペリエンス、およびサービスを提供します。

Cisco Unified Wireless Network は次の要素によって構成されます。

- Cisco Wireless LAN Controller（WLC）
- Cisco Aironet アクセス ポイント（AP）

- Cisco Prime Infrastructure（PI）
- Cisco Mobility Services Engine（MSE）

この項では、選択可能な WLC、AP、および PI の製品オプションについて説明します。詳細については、『Cisco Mobility Services Engine』を参照してください。

（注）　便宜上の理由からと一貫性を維持するために、このマニュアルでは、すべての Cisco Wireless LAN Controller を WLC、Aironet アクセス ポイントを AP、Cisco Prime Infrastructure を PI と表記します。

Cisco ワイヤレス LAN コントローラ

Cisco Wireless LAN Controller は、802.11a/n/ac プロトコルおよび 802.11b/g/n プロトコルをサポートする、エンタープライズクラスの高性能ワイヤレス スイッチング プラットフォームです。無線リソース管理（RRM）機能が搭載されているオペレーティング システムの制御下でコントローラを稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する CUWN ソリューションが実現されます。コントローラは、高性能なネットワークおよびセキュリティ ハードウェアを中心に設計されており、他に例のないセキュリティを備えた信頼性の高い 802.11 エンタープライズ ネットワークを実現します。

ここでは、8.1 リリースでサポートされている Cisco WLC の各種モデルおよびその機能について説明します。

表 2-2　シスコのワイヤレス コントローラの概要

	Cisco 2504 ワイヤレス コントローラ	**Cisco 5508 ワイヤレス コントローラ**	**Cisco 5520 ワイヤレス コントローラ**	**Cisco Flex 7510 ワイヤレス コントローラ**	**Cisco 8510 ワイヤレス コントローラ**	**Cisco 8540 ワイヤレス コントローラ**	**ワイヤレス サービス モジュール 2**	**仮想ワイヤレス コントローラ**
フォーム ファクタ	1U アプライアンス	1U アプライアンス	1U アプライアンス	1U アプライアンス	1U アプライアンス	2U アプライアンス	-	ソフトウェア
プラットフォーム統合	該当なし	該当なし	該当なし	該当なし	該当なし	該当なし	-	該当なし
拡張性	75 X アクセス ポイント 1,000 X クライアント 1 Gbps スループット	500 X アクセス ポイント 7,000 X クライアント 8 Gbps スループット	1500 X アクセス ポイント 20,000 X クライアント 20 Gbps スループット	6000 X アクセス ポイント 64,000 X クライアント 2000 X FlexConnect グループ	6000 X アクセス ポイント 64,000 X クライアント 10 Gbps スループット	6000 X アクセス ポイント 64,000 X クライアント 40 Gbps スループット	-	200（小）/3000（大）アクセス ポイント 6,000（小）クライアント/ 32,000（大）X クライアント 200（小）/3000（大）X FlexConne ct グループ

表 2-2　シスコのワイヤレス コントローラの概要（続き）

	Cisco 2504 ワイヤレス コントローラ	Cisco 5508 ワイヤレス コントローラ	Cisco 5520 ワイヤレス コントローラ	Cisco Flex 7510 ワイヤレス コントローラ	Cisco 8510 ワイヤレス コントローラ	Cisco 8540 ワイヤレス コントローラ	ワイヤレス サービス モジュール 2	仮想ワイヤレス コントローラ
基本 AP ライセンス	0.5、15、25、50 台の AP	0、12、25、50、100、250 台の AP の増分（CISL ベース）	0、50 台の AP	0、300、500、1000、2000、3000、6000 台の AP	0、300、500、1000、2000、3000、6000 台の AP	0 および 1000 AP	-	5 台の AP
AP 追加ライセンス	1.5、25 台の AP の増分（CISL ベース）	5、25、50、100、250 台の AP の増分（CISL ベース）	1 台の AP の増分（使用権）	100、200、500、1000 台の AP の増分（使用権）	100、200、500、1000 台の AP の増分（使用権）	1 AP の増分（使用権）	-	1,5 および 25 AP の増分（使用権）
High Availability（高可用性）	N+1	N+1 SSO	N+1 SSO	N+1 SSO	N+1 SSO	N+1 SSO	-	N+1
アップリンク インターフェイス	4 X 1G イーサネット ポート（RJ45）	8 X 1G イーサネット ポート（SFP）	2 X 1G/10G イーサネット ポート（SFP/SFP+）	1 X 10G イーサネット ポート（SFP+）	1 X 10G イーサネット ポート（SFP+）	4 X 1 G/10 G イーサネット ポート（SFP/SFP+）	-	1 X 仮想
電源	外部 AC 電源	AC（冗長 PSU オプション）	AC（冗長 PSU オプション）	AC/DC（デュアル冗長）	AC/DC（デュアル冗長）	AC/DC（デュアル冗長）	AC/DC (Catalyst シャーシ)	ホストに依存
位置付け	ブランチ、小規模オフィス	企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス	企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス	多数の分散したコントローラなしのブランチ オフィスに対応するセントラル サイトのコントローラ	企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ	企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ	エンタープライズ キャンパス	SP-Wi-Fi、コントローラなしのブランチ、小規模オフィス

Cisco 2504 ワイヤレス コントローラ

Cisco 2504 ワイヤレス コントローラは、中小企業およびブランチ オフィスにおいて、ワイヤレス機能をシステム全体で実現します。802.11n と 802.11ac の性能に合わせて設計された Cisco 2504 ワイヤレス コントローラは、Cisco Aironet アクセス ポイント間のリアルタイム通信を実現してワイヤレス ネットワークの導入と運用をシンプルにするエントリレベルのコントローラです。

Cisco 2504 ワイヤレス コントローラ	**導入タイプ**	ブランチ、小規模オフィス
	動作モード	すべてのモード
	最大スケール	75 AP 1,000 クライアント
	AP 数の範囲	5 ～ 75
	ライセンスの権限付与	CISL ベース
	Connectivity	4 X 1G イーサネット ポート（RJ-45）
	電源	外部 AC 電源
	最大スループット	1 Gbps
	FlexConnect の最大グループ数	30
	FlexConnect グループあたり最大 AP 数	20
	最大不正 AP 数	2,000
	最大不正クライアント数	2,500 台
	最大 RFID タグ数	500
	RF グループあたり最大 AP 数	500
	最大 AP グループ数	75
	最大インターフェイス グループ数	64
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	16
	最大 WLAN 数	16
	高速セキュア ローミング クライアント/PMK キャッシュ	700

Cisco 2504 ワイヤレス コントローラの詳細については、『Cisco 2500 Series Wireless Controllers』を参照してください。

Cisco 3504 ワイヤレス コントローラ

Cisco 3504 ワイヤレス コントローラは、コンパクト性、優れた拡張性、豊富なサービス、回復力、柔軟性を備えた業界初のマルチギガビット イーサネット プラットフォームで、中小企業および展開において次世代のワイヤレス ネットワークを可能にします。802.11ac Wave2 の性能に合わせて最適化された Cisco 3504 ワイヤレス コントローラは、中小企業およびブランチ オフィスに一元化された制御、管理、トラブルシューティングを提供します。

Cisco 3504 ワイヤレス コントローラ	**導入タイプ**	小～中規模のエンタープライズ キャンパスおよびフル サービス ブランチ
	動作モード	すべてのモード
	最大スケール	150 台の AP 3,000 のクライアント
	AP 数の範囲	1 - 150
	ライセンスの権限付与	使用権（EULA）、Cisco SMART Licensing
	Connectivity	1 X MGig（1、2.5、5 Gbps）、4 X 1 G イーサネット ポート（RJ-45）
	電源	外部 AC 電源
	最大スループット	4 Gbps
	最大 FlexConnect グループ数	100
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	600
	最大不正クライアント数	1,500
	最大 RFID タグ数	1,500
	RF グループあたり最大 AP 数	500
	最大 AP グループ数	150
	最大インターフェイス グループ数	512
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	4094
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	14,00

Cisco 2504 ワイヤレス コントローラの詳細については、Cisco 3500 Series Wireless Controllers（Cisco 3500 シリーズ ワイヤレス コントローラ）を参照してください。

Cisco 5508 ワイヤレス コントローラ

Cisco 5508 ワイヤレス コントローラは、ミッションクリティカルなワイヤレス用に信頼性の高いパフォーマンス、強化された柔軟性、およびゼロ サービスロスを提供します。音声やビデオなどのインタラクティブなマルチメディア アプリケーションがワイヤレス ネットワーク越しにそつなく動作可能になっており、クライアントはサービスの中断なしにタイミングよくローミング可能です。柔軟性の高いライセンスによってアクセス ポイントのサポートや高性能ソフトウェア機能を簡単に追加できます。

Cisco 5508 ワイヤレス コントローラ	**導入タイプ**	企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス
	動作モード	すべての AP モード
	最大スケール	500 AP 7,000 クライアント
	AP 数の範囲	12 ～ 500
	ライセンスの権限付与	CISL ベース
	Connectivity	8 X 1G イーサネット ポート（SFP）
	電源	AC（冗長 PSU オプション）
	最大スループット	8 Gbps
	FlexConnect の最大グループ数	100
	FlexConnect グループあたり最大 AP 数	25
	最大不正 AP 数	2,000
	最大不正クライアント数	2,500 台
	最大 RFID タグ数	5000
	RF グループあたり最大 AP 数	1000
	最大 AP グループ数	500
	最大インターフェイス グループ数	64
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	512
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	14,000

Cisco 5508 ワイヤレス コントローラの詳細については、『Cisco 5500 Series Wireless Controllers』を参照してください。

Cisco 5520 ワイヤレス コントローラ

Cisco 5520 シリーズ ワイヤレス LAN コントローラは、高度なスケーラビリティ、豊富なサービス、回復力、および柔軟性を備えたプラットフォームで、中規模から大規模なエンタープライズおよびキャンパスでの導入に最適です。シスコ ユニファイド アクセス ソリューションの一部である 5520 は次世代ワイヤレス ネットワークの 802.11ac Wave 2 用に最適化されています。

Cisco 5520 ワイヤレス コントローラ	**導入タイプ**	企業、キャンパス、およびすべてのサービスを実施するブランチ オフィス
	動作モード	すべての AP モード
	最大スケール	1,500 AP 20,000 クライアント
	AP 数の範囲	1 ～ 1,500
	ライセンスの権限付与	使用権（EULA）
	Connectivity	2 X 10G イーサネット ポート（SFP+）
	電源	AC（冗長 PSU オプション）
	最大スループット	20 Gbps
	FlexConnect の最大グループ数	1、500
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	24000
	最大不正クライアント数	32,000
	最大 RFID タグ数	25,000
	RF グループあたり最大 AP 数	3000
	最大 AP グループ数	1,500
	最大インターフェイス グループ数	512
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	4,095
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	40,000

Cisco 5520 ワイヤレス コントローラの詳細については、『Cisco 5500 Series Wireless Controller』を参照してください。

Cisco Flex 7500 ワイヤレス コントローラ

Cisco Flex 7500 ワイヤレス コントローラには、ブランチ ネットワーク内に FlexConnect ソリューションを導入する際のスケーリング要件を満たすように設計されたモデルがあります。FlexConnect は、アクセス ポイントが中央のコントローラによって制御および管理されながら、データはブランチ サイト内でローカルにスイッチングできるようにすることで、ワイヤレス ブランチ ネットワークをサポートするように設計されています。Cisco Flex 7500 シリーズ クラウド コントローラは、規模が大きいときにコスト効率の良い FlexConnect ソリューションを実現することを目指しています。

Cisco 5520 ワイヤレス コントローラ	**導入タイプ**	多数の分散したコントローラなしのブランチ オフィスに対応するセントラル サイトのコントローラ
	動作モード	FlexConnect、フレックス + ブリッジ
	最大スケール	6,000 台の AP 64,000 クライアント
	AP 数の範囲	300 ～ 6,000
	ライセンスの権限付与	使用権（EULA）
	Connectivity	2 X 10G イーサネット ポート（SFP+）/1 つがアクティブ
	電源	AC/DC（デュアル冗長）
	最大スループット	—
	FlexConnect の最大グループ数	2,000
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	32,000
	最大不正クライアント数	24000
	最大 RFID タグ数	50,000
	RF グループあたり最大 AP 数	6000
	最大 AP グループ数	6000
	最大インターフェイス グループ数	512
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	4,095
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	64,000

詳細については、『Cisco Flex 7500 Series Wireless Controllers』を参照してください。

Cisco 8510 ワイヤレス コントローラ

Cisco 8510 ワイヤレス コントローラは、非常にスケーラブルで柔軟性の高いプラットフォームであり、企業やサービス プロバイダーへの導入においてミッション クリティカルなワイヤレス ネットワーキングを実現します。

Cisco 8510 ワイヤレス コントローラ	**導入タイプ**	企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ
	動作モード	すべての AP モード
	最大スケール	6,000 台の AP 64,000 クライアント
	AP 数の範囲	300 ～ 6,000
	ライセンスの権限付与	使用権（EULA）
	Connectivity	2 X 10G イーサネット ポート（SFP+）/1 つがアクティブ
	電源	AC/DC（デュアル冗長）
	最大スループット	10 Gbps
	FlexConnect の最大グループ数	2,000
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	32,000
	最大不正クライアント数	24000
	最大 RFID タグ数	50,000
	RF グループあたり最大 AP 数	6000
	最大 AP グループ数	6000
	最大インターフェイス グループ数	512
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	4,095
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	64,000

Cisco 8510 ワイヤレス コントローラの詳細については、『Cisco 8500 Series Wireless Controllers』を参照してください。

Cisco 8540 ワイヤレス コントローラ

802.11ac Wave2 の性能に合わせて最適化された Cisco 8540 ワイヤレス コントローラは、高度なスケーラビリティ、豊富なサービス、回復力、および柔軟性を備えたプラットフォームで、中規模から大規模なエンタープライズおよびキャンパスでの導入において次世代のワイヤレス ネットワークを可能にします。

Cisco 8540 ワイヤレス コントローラ	**導入タイプ**	企業、大規模キャンパス、SP Wi-Fi、大規模ブランチ
	動作モード	すべての AP モード
	最大スケール	6,000 台の AP 64,000 クライアント
	AP 数の範囲	1 ～ 6,000
	ライセンスの権限付与	使用権（EULA）
	Connectivity	4 X 10G イーサネット ポート（SFP+）
	電源	AC/DC（ホットスワップ可能デュアル冗長 PSU）
	最大スループット	40 Gbps
	FlexConnect の最大グループ数	2,000
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	32,000
	最大不正クライアント数	24000
	最大 RFID タグ数	50,000
	RF グループあたり最大 AP 数	6000
	最大 AP グループ数	6000
	最大インターフェイス グループ数	512
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	4,095
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	64,000

Cisco 8540 ワイヤレス コントローラの詳細については、『Cisco 8500 Series Wireless Controllers』を参照してください。

Cisco ワイヤレス サービス モジュール 2

Catalyst 6500 シリーズ スイッチ用の Cisco Wireless Services Module 2（WiSM2）は統合ソリューションが適している中規模から大規模の単一サイト WLAN 環境におけるミッションクリティカルなワイヤレス ネットワーキングに最適です。WiSM2 はハードウェアのコストの削減に役立ち、またワイヤレス ネットワークの運用と所有にかかる総コストを減らすことができる柔軟な設定オプションが用意されています。

Cisco Wireless Services Module 2（WiSM2）	**導入タイプ**	企業の構内
	動作モード	すべての AP モード
	最大スケール	1,000 AP 15,000 クライアント
	AP 数の範囲	100 ～ 1,000
	ライセンスの権限付与	CISL ベース
	Connectivity	Catalyst バックプレーン内部
	電源	AC/DC（Catalyst シャーシの冗長 PSU オプション）
	最大スループット	10 Gbps
	FlexConnect の最大グループ数	100
	FlexConnect グループあたり最大 AP 数	25
	最大不正 AP 数	4,000
	最大不正クライアント数	5,000
	最大 RFID タグ数	10,000
	RF グループあたり最大 AP 数	2,000
	最大 AP グループ数	500
	最大インターフェイス グループ数	64
	最大インターフェイス/インターフェイス グループ	64
	最大 VLAN 数	512
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	30,000

詳細については、『Cisco Wireless Services Module 2』を参照してください。

仮想ワイヤレス LAN コントローラ

IT 管理者は、最大 3000 台のアクセス ポイントおよび 32000 のクライアントの設定、管理、トラブルシューティングを実行できます。Cisco Virtual Wireless Controller は、セキュアなゲスト アクセス、Payment Card Industry（PCI）基準に準拠した不正検出、ブランチ（ローカルでスイッチングが行われる）オフィスでの Wi-Fi による音声およびビデオに対応しています。

Cisco Virtual Wireless Controller（vWLC）	**導入タイプ**	SP-Wi-Fi、コントローラなしのブランチ、小規模オフィス
	動作モード	FlexConnect、フレックス + ブリッジ
	最大スケール	200 AP（小）/3,000 AP（大） 6,000 クライアント（小）/ 32,000 クライアント（大）
	AP 数の範囲	5 ～ 200
	ライセンスの権限付与	使用権（EULA）
	Connectivity	1（仮想）
	電源	ホスト依存
	最大スループット	N/A
	最大 FlexConnect グループ数	200（小）/3,000（大）
	FlexConnect グループあたり最大 AP 数	100
	最大不正 AP 数	800
	最大不正クライアント数	1,500
	最大 RFID タグ数	3,000
	RF グループあたり最大 AP 数	1,000
	最大 AP グループ数	200
	最大インターフェイス グループ数	—
	最大インターフェイス/インターフェイス グループ	—
	最大 VLAN 数	4,094
	最大 WLAN 数	512
	高速セキュア ローミング クライアント/PMK キャッシュ	6,000

詳細については、『Cisco Virtual Wireless Controller』を参照してください。

（注）　Cisco Virtual Wireless Controller は、VMWare の ESXi（5.x 以降）、Microsoft Hyper-V、Linux KVM を含む業界標準の仮想化インフラストラクチャでサポートされます。vWLC は、第 2 世代サービス統合型ルータ向用の Cisco Unified Computing System Express（UCS Express）でもサポートされます。8.5 リリースでは、Amazon AWS のサポートが追加されました。

Cisco Aironet アクセス ポイント

Cisco Aironet シリーズ ワイヤレス アクセス ポイントはブランチ オフィス、キャンパス、または大規模なエンタープライズの分散型または中央集中型のネットワークに導入できます。これらのワイヤレス アクセス ポイントは次のような多様な機能を提供し、ワイヤレス ネットワークのエンドユーザ エクスペリエンスを向上させます。

- Cisco CleanAir テクノロジー：RF 干渉を回避できるセルフヒーリング（自己修復）および自己最適化ネットワークを実現します。
- Cisco ClientLink 2.0 および 3.0：クライアントの信頼性とカバレッジを向上します。
- Cisco BandSelect：混合クライアント環境における 5 GHz クライアント接続を強化します。
- Cisco VideoStream：マルチキャストを使い、マルチメディア アプリケーションの機能を向上します。

（注）　Cisco 1500 シリーズ MESH AP については、後で簡単に説明しますが、ワイヤレス MESH アプリケーションや MESH 導入のガイドラインについては、本書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、『Cisco Mesh Networking Solution Deployment Guide』を参照してください。

屋内 802.11n アクセス ポイント

ここでは、8.1 リリースでサポートされている Cisco 屋内 802.11n AP の各種モデルおよびその機能について説明します。

	Cisco Aironet 600 シリーズ	Cisco Aironet 700W シリーズ	Cisco Aironet 1600 シリーズ	Cisco Aironet 2600 シリーズ	Cisco Aironet 3600 シリーズ
Wi-Fi 標準	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n	802.11a/b/g/n/ac
無線数	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）	トリプル（2.4 GHz および 5 GHz）
最大データ レート	300 Mbps	300 Mbps	300 Mbps	450 Mbps	450 Mbps（802.11n） 1.3 Gbps（802.11ac モジュール）
MIMO 無線の設計	2 X 3	2 X 2	3 X 3	3 X 4	802.11n：4 X 4 802.11ac：3 X 3
空間ストリーム	2 つの空間ストリーム	2 つの空間ストリーム	2 つの空間ストリーム	3 つの空間ストリーム	3 つの空間ストリーム
アンテナ	内部	内部	1600i 内蔵 1600e 外付け	2600i：内蔵 2600e：外付け	3600i：内蔵 3600e：外付け 3600p：外付け
CleanAir 2.0	—	—	CleanAir Express	Yes	Yes
ClientLink 2.0	—	—	Yes	Yes	Yes

	Cisco Aironet 600 シリーズ	Cisco Aironet 700W シリーズ	Cisco Aironet 1600 シリーズ	Cisco Aironet 2600 シリーズ	Cisco Aironet 3600 シリーズ
シスコの革新技術	—	BandSelect VideoStream	BandSelect VideoStream	BandSelect VideoStream	BandSelect VideoStream
モジュール方式	USB*	—	—	—	802.11ac Wave 1 モジュール USC スモール セル モジュール ワイヤレス セキュリティ モジュール（WSM）
電源	AC	DC、802.3afPoE、802.3at PoE+	DC、802.3afPoE	DC、802.3afPoE	DC、802.3afPoE、802.3at PoE+、Enhanced PoE、Universal PoE
インターフェイス	5 X 1G イーサネット ポート（RJ-45） 1 X 1G イーサネット WAN ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45） 4 X 1G イーサネット ユーザ ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45）

Cisco Aironet 600 シリーズ OfficeExtend

Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントは、家庭環境における安全性の高いエンタープライズ ワイヤレス カバレッジを実現します。これらのデュアル バンド 802.11n アクセス ポイントによって社内ネットワークが在宅テレワーカーおよびモバイル契約業者まで拡張されます。このアクセス ポイントは、自宅のブロードバンド インターネット アクセスに接続し、社内ネットワークへのセキュアなトンネルを確立します。これにより、リモートの従業員は、データ、音声、ビデオ、およびクラウド サービスにアクセスできるため、会社のオフィスにいるのと同じようなモビリティ エクスペリエンスを実現します。デュアル バンドで 2.4 GHz と 5 GHz の無線周波数を同時にサポートすることは、2.4 GHz 帯域を使用する一般的な家庭用デバイスによる輻輳の影響を社内のデバイスが受けないことを請け合うために役立ちます。Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントは、家庭内のトラフィックのセグメント化を行って個人の家庭内のデバイス用に企業データ アクセスの保護をサポートすることと、接続性を維持することによってテレワーカー向けに特に設計されています。

Cisco Aironet 600 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n
	動作モード	OfficeExtend
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	300 Mbps
	MIMO の設計	2 X 3
	空間ストリーム	2
	最大クライアント数	15
	最大 ClientLink 数	—
	ClientLink 2.0	—
	CleanAir	—
	VideoStream	—
	BandSelect	—
	不良 AP 検出	—
	適応型 wIPS	—
	電源	AC
	アンテナ	内部

Cisco Aironet 600 シリーズの詳細については、『Cisco Aironet 600 Series OfficeExtend Access Point』を参照してください。

Cisco Aironet 700W シリーズ

Cisco Aironet 700W シリーズは、ますます複雑化していく今日のワイヤレス アクセス需要に対応できるようにネットワークを刷新したいと考える接客業および教育業界のお客様向けのコンパクトで壁面プレートに取り付け可能なアクセス ポイントです。

Cisco Aironet 700W シリーズは、既存の 802.11a/g ネットワークの 6 倍以上のスループットを実現する 802.11n デュアルラジオ 2 X 2 多入力、多出力（MIMO）テクノロジーを採用することにより、802.11n 品質の高いパフォーマンスを低コストで実現します。

700W シリーズ アクセス ポイントは Cisco Unified Wireless Network の構成要素として、既存のネットワークとシームレスに統合できるため、総所有コストを抑え、投資を保護することができます。

Cisco Aironet 700W シリーズ	**Wi-Fi 標準**	802.11a/b/g/n
	動作モード	中央集中型、FlexConnect
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	300 Mbps
	MIMO の設計	2 X 2
	空間ストリーム	2
	最大クライアント数	100 ワイヤレス/4 有線
	最大 ClientLink 数	—
	ClientLink 2.0	—
	CleanAir	—
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3af PoE+
	アンテナ	内部

詳細については、『Cisco Aironet 700W Series』を参照してください。

Cisco Aironet 1600 シリーズ

新しい Cisco Aironet 1600 シリーズ アクセス ポイントは、エンタープライズクラスのパフォーマンスを発揮するエントリ レベルの 802.11n ベースのアクセス ポイントで、中小企業におけるネットワークのワイヤレス接続のニーズに対応できます。

Aironet 1600 シリーズは適切な価格でお客様に優れた性能を提供するだけでなく、スペクトル インテリジェンスによってカバレッジを向上する CleanAir Express、混合クライアント ベースを持つエントリ レベル ネットワーク用の ClientLink 2.0 などの高度な機能を提供します。これらの機能に加え、Aironet 1600 シリーズには 2 つの空間ストリームを備えた 802.11n ベースの 3 X 3 MIMO テクノロジーが搭載されているため、中小企業に最適です。

Aironet 1600 シリーズは、既存の 802.11a/g ネットワークの 6 倍以上のスループットを提供します。Cisco Aironet 1600 シリーズ アクセス ポイントは、Cisco Aironet ワイヤレス ポートフォリオの一員として、既存のネットワークとシームレスに統合できるため、総所有コストを抑え、投資を保護することができます。802.11n に移行するためのエントリ レベル パスを持つ Aironet 1600 シリーズは、拡張するアプリケーションおよび帯域幅に合わせた将来の拡張のためにネットワークにキャパシティを追加できます。

急速に進化するモビリティのニーズを考慮して設計された Cisco Aironet 1600 シリーズ アクセス ポイントは、適切な料金で高度な機能を提供することにより、個人所有デバイスの持ち込み（BYOD）の動向に対応します。

Cisco Aironet 1600 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	300 Mbps
	MIMO の設計	3 X 3
	空間ストリーム	2
	最大クライアント数	128
	最大 ClientLink 数	32
	ClientLink 2.0	Yes
	CleanAir	Yes：CleanAir Express
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE
	アンテナ	1600i：内蔵 1600e：外付け

詳細については、『Cisco Aironet 1600 Series』を参照してください。

Cisco Aironet 2600 シリーズ

Cisco Aironet 2600 シリーズ アクセス ポイントは、性能、機能性、および信頼性に優れた、クラス最先端の機能を魅力的な価格で提供します。802.11n ベースの Aironet 2600 シリーズには 3 X 4 MIMO が装備されており、3 つの空間ストリーム、Cisco CleanAir、ClientLink 2.0、および VideoStream テクノロジーを搭載し、干渉のない、高速なワイヤレス アプリケーション エクスペリエンスを実現します。Cisco Aironet 3600 シリーズに次ぐパフォーマンスと機能を備えた Aironet 2600 シリーズは、企業のワイヤレス テクノロジーに新しい基準を設定します。

急速に進化するモビリティのニーズを考慮して設計された Aironet 2600 シリーズ アクセス ポイントには、他のアクセス ポイントと比べて強化された BYOD 対応機能が適切な料金で組み込まれています。新しい Cisco Aironet 2600 シリーズは、他社製品と比較して、アクセス ポイントからより離れた範囲に信頼性の高い高速接続を維持することができます。その結果、450 Mbps データ レートをより広いエリアに提供します。コンシューマ デバイス用に最適化されている Aironet 2600 シリーズでは、競合ソリューションと比べてクライアント接続は高速で、モバイル デバイスのバッテリ電力は節約されます。

Cisco Aironet 2600 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	450 Mbps
	MIMO の設計	3 X 4
	空間ストリーム	3
	最大クライアント数	200
	最大 ClientLink 数	128
	ClientLink 2.0	Yes
	CleanAir	Yes
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3af PoE+
	アンテナ	2600i：内蔵 2600e：外付け

詳細については、『Cisco Aironet 2600 Series』を参照してください。

Cisco Aironet 3600 シリーズ

タブレット、スマートフォン、および高性能ラップトップの使用時に、他社製品と比較して最大 3 倍のカバレッジを提供します。業界初の 4 X 4 MIMO および 3 つの空間ストリームに対応したアクセス ポイントであり、ミッション クリティカルな用途に耐える高い信頼性を発揮します。モバイル デバイスやモバイル アプリケーションが急激に多様化し、それに伴うワイヤレス ネットワークのニーズも増加しており、昨今のソリューションはその対応に追われています。Cisco Aironet 3600 シリーズは、他社製品と比較して、アクセス ポイントからより離れた範囲に信頼性の高い高速接続を維持することができます。その結果、速度 450 Mbps の接続を最大 3 倍の広さのエリアに提供し、より多くのモバイル デバイスに最適なパフォーマンスを提供できます。Cisco Aironet 3600 シリーズは画期的なモジュラ型のプラットフォームであり、1.3 Gbps レートで稼動する着信 802.11ac クライアントをサポートする追加のモジュール拡張や、包括的なセキュリティおよび周波数帯の監視と制御を提供して、優れた投資保護を実現します。

Cisco Aironet 3600 シリーズは、パフォーマンスとクライアント カバレッジ範囲を増強する Cisco ClientLink 2.0 と、ネットワークのセルフヒーリング（自己修復）および自己最適化を可能にする Cisco CleanAir スペクトル インテリジェンスを搭載します。

Cisco Aironet 3600 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n 802.11ac（モジュール搭載）
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	トリプル（2.4 GHz、5 GHz、およびモジュール）
	最大データ レート	802.11n：450 Mbps 802.11ac：1.3 Gbps
	MIMO の設計	802.11n：4 X 4 802.11ac：3 X 3
	空間ストリーム	3
	最大クライアント数	802.11n：200 802.11ac：50
	最大 ClientLink 数	802.11n：128 802.11ac：7（ECBF）
	ClientLink 2.0	Yes（802.11ac クライアントに対する ECBF）
	CleanAir	Yes
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3at（PoE+）、Enhanced PoE、Universal PoE（UPOE）
	アンテナ	3600i：内蔵 3600e：外付け 3600p：外付け

詳細については、『Cisco Aironet 3600 Series』を参照してください。

屋内 802.11ac アクセス ポイント

ここでは、8.1 リリースでサポートされている Cisco 屋内 802.11ac AP の各種モデルおよびその機能について説明します。

	Cisco Aironet 1700 シリーズ	Cisco Aironet 1850 シリーズ	Cisco Aironet 2700 シリーズ	Cisco Aironet 3700 シリーズ
Wi-Fi 標準	802.11a/b/g/n/ac（Wave 1）	802.11a/b/g/n/ac（Wave 2）	802.11a/b/g/n/ac（Wave 1）	802.11a/b/g/n/ac（Wave 1）
無線数	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）	デュアル（2.4 GHz および 5 GHz）
最大データ レート	867 Mbps	1.7 Gbps	1.3 Gbps	1.3 Gbps
MIMO 無線の設計	3 X 3	4 X 4	3 X 4	4 X 4
空間ストリーム	2 つの空間ストリーム	4 つの空間ストリーム（SU MIMO） 3 つの空間ストリーム（MU MIMO）	3 つの空間ストリーム	3 つの空間ストリーム
アンテナ	1700i：内蔵	1850i 内蔵 1850e：外付け	2700i 内蔵 2700e 外付け	3700i：内蔵 3700e：外付け 3700p：外付け
CleanAir 2.0	CleanAir Express	CleanAir Express	Yes	Yes
ClientLink 3.0	送信ビーム フォーミング	送信ビーム フォーミング	Yes	Yes
シスコの革新技術	BandSelect VideoStream	BandSelect VideoStream	BandSelect High Density Experience VideoStream	BandSelect StadiumVision High Density Experience VideoStream
モジュール方式	—	USB 2.0*	—	802.11ac Wave 2 モジュール USC スモール セル モジュール ハイパーロケーション モジュール ワイヤレス セキュリティ モジュール（WSM）
電源	DC、802.3afPoE、+、Enhanced PoE	DC、802.3afPoE、+、Enhanced PoE	DC、802.3afPoE、+、Enhanced PoE	DC、802.3afPoE、802.3at PoE+、Enhanced PoE、Universal PoE

	Cisco Aironet 1700 シリーズ	Cisco Aironet 1850 シリーズ	Cisco Aironet 2700 シリーズ	Cisco Aironet 3700 シリーズ
インターフェイス	1 X 1G イーサネット アップリンク ポート（RJ-45） 1 X 1G イーサネット AUX ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45）自動 LAG あり 1 X 1G イーサネット AUX ポート（RJ-45）自動 LAG あり	1 X 1G イーサネット アップリンク ポート（RJ-45） 1 X 1G イーサネット AUX ポート（RJ-45）	1 X 1G イーサネット アップリンク ポート（RJ-45）

Cisco Aironet 1700 シリーズ

小規模または中規模のエンタープライズ ネットワークを運用している場合、Cisco Aironet 1700 シリーズ アクセス ポイントを導入することで、お手頃な価格で最新の 802.11ac Wi-Fi テクノロジーを入手できます。1700 シリーズは、802.11n よりも優れたパフォーマンスや重要な RF 管理機能を提供することで、ワイヤレス ネットワークの高まる要件に対応し、ワイヤレス エクスペリエンスを向上させます。

1700 シリーズは、802.11ac Wave 1 の標準機能をサポートしています。これには、最大 867 Mbps の理論的な接続レートが含まれます。

Cisco Aironet 1700 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n/ac（Wave 1）
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	867 Mbps
	MIMO の設計	3 X 3
	空間ストリーム	2
	最大クライアント数	200
	最大 ClientLink 数	—
	ClientLink 2.0	Yes：送信ビームフォーミング（TxBF）
	CleanAir	Yes：CleanAir Express
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3at PoE+、Enhanced PoE
	アンテナ	1700i：内蔵 1700e：外付け

詳細については、『Cisco Aironet 1700 Series』を参照してください。

Cisco Aironet 1850 シリーズ

小規模および中規模のネットワークに最適な Cisco Aironet 1850 シリーズは、エンタープライズ クラスの 4 X 4 MIMO（IEEE の新しい 802.11ac Wave 2 仕様をサポートする 4 空間ストリームのアクセス ポイント）を通じて、企業やサービス プロバイダーに業界トップクラスのパフォーマンスを提供します。Aironet 1850 シリーズは、スマートフォン、タブレット、高性能ラップトップなど、802.11ac Wave 1 または Wave 2 サポートを統合した新しい世代の Wi-Fi クライアントにも対応しています。

Cisco Aironet 1850 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n/ac（Wave 2）
	動作モード	中央集中型、FlexConnect（将来）
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	1.7 Gbps
	MIMO の設計	4 X 4
	空間ストリーム	4（SU-MIMO） 3（MU-MIMO）
	最大クライアント数	200
	最大 ClientLink 数	—
	ClientLink 3.0	Yes：送信ビームフォーミング（TxBF）
	CleanAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3af PoE+、Enhanced PoE
	アンテナ	1850i：内蔵 1850e：外付け

詳細については、『Cisco Aironet 1850 Series』を参照してください。

Cisco Aironet 2700 シリーズ

Cisco Aironet 2700 シリーズ Wi-Fi アクセス ポイント（AP）は、高密度の屋内環境にキャパシティを追加し、カバレッジ ギャップを埋めるために最適な料金で業界トップクラスの 802.11ac のパフォーマンスを提供します。Aironet 2700 シリーズでは、高速な 802.11ac Wi-Fi 無線を搭載するようになった新世代のスマートフォン、タブレット、および高性能ラップトップに、802.11ac の速度と機能を拡張します。

Aironet 2700 シリーズでは、最初の実装である 802.11ac Wave 1 をサポートしており、最大 1.3 Gbps の理論的な接続レートを提供します。今日のハイエンド 802.11n AP の概ね 3 倍となるレートが実現します。この高速化は、1 台だけではなく複数台の Wi-Fi デバイスを使用することが一般的な最近のモバイル ワーカーによる性能と帯域幅に対する期待を越えるために役立ちます。このため、ユーザは相対的に大きなトラフィック負荷を無線 LAN に加えており、これはデフォルトの企業アクセス ネットワークであるイーサネットを超えています。

Cisco Aironet 2700 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n/ac（Wave 1）
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	デュアル（2.4 GHz および 5 GHz）
	最大データ レート	1.3 Mbps
	MIMO の設計	3 X 4
	空間ストリーム	3
	最大クライアント数	200
	最大 ClientLink 数	128
	ClientLink 3.0	Yes
	CleanAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3at PoE+、Enhanced PoE
	アンテナ	2700i：内蔵 2700e：外付け

詳細については、『Cisco Aironet 2700 Series Access Point』を参照してください。

Cisco Aironet 3700 シリーズ

Cisco Aironet 3700 シリーズは、IEEE 802.11ac Wave 1 仕様に対応している、業界唯一の 4 X 4 MIMO、3 空間ストリームのエンタープライズ クラス アクセス ポイントです。企業とサービス プロバイダーのいずれのお客様にも業界トップクラスのパフォーマンスと高密度エクスペリエンス（HD エクスペリエンス）を提供します。Aironet 3700 シリーズを使用することで、スマートフォン、タブレット、高性能ラップトップなど、統合された 802.11ac サポートを含む新世代の Wi-Fi クライアントにもサポート対象を拡大できます。

最初の実装である 802.11ac Wave 1 では、現在のハイエンド 802.11n アクセス ポイントの約 3 倍に相当する最大 1.3 Gbps の速度を提供します。この製品により、エンタープライズ ネットワークおよびサービス プロバイダー ネットワークで、ワイヤレス ユーザの期待やニーズを超えるレベルのパフォーマンスと帯域幅を同様に提供できる必要な基盤を確立できます。

ワイヤレス アクセスは、その便利さにより、企業ユーザのネットワーク接続手段として急速に普及しつつあります。それに伴い、ワイヤレスに対する期待も拡大し、高密度エクスペリエンスを実現する同クラス最高の RF アーキテクチャを備えた革新的な専用チップセットを利用することで、ユーザに社内環境での自由な移動を許可しながら、日常の業務効率を低下させることなく、高い性能を提供できることが求められています。

Cisco Aironet 3700 シリーズ	**Wi-Fi 標準**	802.11a/b/g/n/ac（Wave 1）
	動作モード	中央集中型、FlexConnect、屋内メッシュ、OfficeExtend
	無線数	トリプル（2.4 GHz、5 GHz、およびモジュール）
	最大データ レート	1.3 Mbps
	MIMO の設計	4 X 4
	空間ストリーム	3
	最大クライアント数	200
	最大 ClientLink 数	128
	ClientLink 3.0	Yes
	CleanAir 2.0	Yes
	VideoStream	Yes
	BandSelect	Yes
	不良 AP 検出	Yes
	適応型 wIPS	Yes
	電源	DC、802.3af PoE、802.3at PoE+、Enhanced PoE、Universal PoE（UPOE）
	アンテナ	3700i：内蔵 3700e：外付け 3700p：外付け

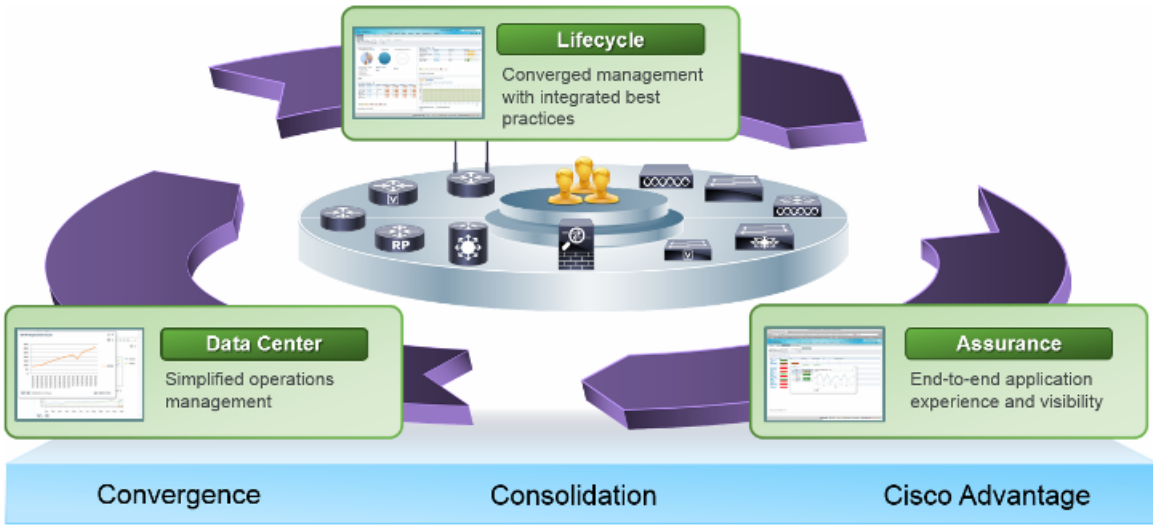
詳細については、『Cisco Aironet 3700 Series』を参照してください。

Cisco Prime Infrastructure

変化とは経験したことのない事件です。モバイル デバイスの急増、音声とビデオの広範なコラボレーション、クラウドとデータセンターの仮想化により、ネットワークはかつてない変化を迎えようとしています。新たな機会の到来に伴って、新たな多くの課題が到来します。高いサービス レベル、確実なアプリケーション配信、簡易化されたエンドユーザ エクスペリエンスを提供しながら、ビジネスの継続性を維持し、運用コストを管理することが必要とされています。

IT プロフェッショナルたちはこれらの課題に対処するために、単一のグラフィカル インターフェイスからネットワークを管理できる包括的なソリューションを必要としています。それが Cisco Prime Infrastructure ソリューションです。ブランチ オフィスにいるワイヤレス ユーザに、WAN をまたがり、アクセス レイヤを通じ、データセンターにまで拡張された、ネットワーク全体のライフサイクル管理とサービス アシュアランスを提供します。これを One Management（一元管理）と呼びます（図 2-13）。

図 2-13　Cisco Prime Infrastructure :One Management



Cisco Prime Infrastructure はネットワークをデバイス、ユーザ、アプリケーションにエンドツーエンドで接続し、すべてを兼ね備えたネットワーク管理です。装備する機能によって次の内容を実現できます。

- 一括管理：Day-0 および Day-1 プロビジョニングと、それ以降の保証のために単一の統合プラットフォームを提供します。これによりデバイスとサービスの導入が加速化され、エンドユーザ エクスペリエンスに影響を及ぼす問題をすばやく解決できるようになります。ネットワーク管理に要する時間を短縮できるため、ビジネスを拡大させるためにこれを利用する時間を最大化できます。
- シスコの付加価値機能を簡単に導入：シスコの差別化機能やサービスをより迅速かつ効率的に設計し、実装することができます。Intelligent WAN（IWAN）、コンバージド アクセスを実現した分散ワイヤレス、Application Visibility and Control（AVC）、ゾーンベース ファイアウォール、Cisco TrustSec 2.0 Identity-Based Networking Services などのテクノロジーをサポートしているため、シスコ デバイスに組み込まれたインテリジェンス機能を可能な限り迅速に活用できます。
- アプリケーションの可視性：パフォーマンス データを埋め込んだ Cisco 機器および業界標準の技術を設定し、ソースとして使用されてネットワーク全体のアプリケーション対応の可視性を提供します。これらのテクノロジーには、NetFlow、Network-Based Application Recognition 2（NBAR2）、Cisco Medianet テクノロジー、Simple Network Management Protocol（SNMP）などがあります。Cisco Prime Infrastructure では、アプリケーションの可視性とライフサイクル管理という斬新な組み合わせによって、基盤となるインフラストラクチャの実行状況のコンテキストからアプリケーションおよびサービスの実行状況に関する情報を提供することにより、問題の検出と解決を容易にします。
- モバイル コラボレーションの管理：ワイヤレス アクセスに関する誰が、いつ、どこで、何を、どのようにに答えます。これには、802.11ac サポート、相関する有線/無線クライアントの可視化、ユニファイド アクセス インフラストラクチャの可視化、空間マップ、Cisco Identity Services Engine（ISE）統合によるコンバージド型のセキュリティ/ポリシーの監視とトラブルシューティング、Cisco モビリティ サービス エンジン（MSE）および Cisco CleanAir 統合を使用したロケーション ベースの干渉源/不正/Wi-Fi クライアントの追跡、ライフサイクル管理、RF 予測ツールなどが含まれます。

- ネットワークをまたがる管理とコンピューティング：強力なライフサイクル管理およびサービス アシュアランスを提供して、ブランチ オフィス、キャンパス、およびデータセンターのネットワークで実行されている多数のデバイスおよびサービスの維持管理に役立ちます。ディスカバリ、インベントリ、構成、モニタリング、トラブルシューティング、レポート作成、管理などの重要な機能を提供します。単一のビューと単一の管理ポイントによってネットワークとコンピュータの両方にまたがる One Management（一元管理）のメリットを実現します。
- 分散ネットワークの可視性の一元化：大規模またはグローバルな組織は、通常、ドメイン、地域、または国ごとにネットワーク管理を分散しています。Cisco Prime Infrastructure オペレーション センターを使用すると、最大 10 個の Cisco Prime Infrastructure インスタンスを可視化できるため、中央での可視性と制御を維持しながら、ネットワーク管理インフラストラクチャを拡張できます。

ライセンス オプション

Cisco Prime Infrastructure は、インストール可能な単一のソフトウェア パッケージであり、ライセンス オプションによって機能とカバレッジを必要に応じて拡大、拡張できます。

- ライフサイクル：ルータ、スイッチ、アクセス ポイントなどのシスコ デバイスの全ライフサイクル フェーズ（設計、導入、運用、レポート）を通して、ネットワーク インフラストラクチャの管理に関連する日常の運用上の作業をシンプルにします。
- アシュアランス：豊富なパフォーマンス データのソースとして装置機器を使用しながらアプリケーション パフォーマンスの可視性を提供して、アプリケーション配信の一貫性と最適なエンドユーザ エクスペリエンスの保証に役立ちます。
- Cisco UCS サーバの管理：Cisco UCS B シリーズおよび C シリーズのサーバに対するライフサイクル管理および Assurance Management を提供します。
- オペレーション センター：中央の一元管理コンソールから最大 10 個の Cisco Prime Infrastructure インスタンスを可視化できます。Cisco Prime Infrastructure でサポートするインスタンスごとに 1 ライセンスが必要です。
- 高可用性使用権（RTU）：高可用性ペアを構成する 1 個のプライマリ インスタンスと 1 個のセカンダリ インスタンスを持つ高可用性構成が可能です。
- コレクタ：Cisco Prime Infrastructure 管理ノードでの NetFlow 処理の制限を上げます。このライセンスは、アシュアランス ライセンスと併せてご利用ください。
- 使用準備済みゲートウェイ RTU：使用準備済み機能で使用する別のゲートウェイを導入する権限が付与されます。この機能では、新しいデバイスがゲートウェイに接続して設定およびソフトウェア イメージを受信できます。

（注）　Cisco Prime Infrastructure 2.2 は新しいお客様に提供され、先行バージョンを実行している既存のお客様にはアップグレード オプションが提供されます。アップグレード オプションは、Cisco Network Control System（NCS）、Cisco Wireless Control System（WCS）、および Cisco Prime LAN Management Solution（LMS）をご利用のお客様にも提供されます。詳細については、http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/datasheet-listing.html を参照してください。

スケーリング

Cisco Prime Infrastructure 2.2 は、仮想アプライアンスまたは物理アプライアンスとして購入可能です。仮想アプライアンスは業界標準の VMware ハイパーバイザ上にインストールでき、さまざまな規模のネットワークをサポートするために複数のバージョンが提供されています。物理アプライアンスは大規模ネットワーク導入でも使用できます。この場合は、専用の CPU およびメモリ リソースが必要です。

- 物理アプライアンス（第 2 世代）：Cisco UCS C220 M4 ラック サーバがベースです。
- 仮想アプライアンス：ESXi バージョン 5.0、5.1、または 5.5。

表 2-3 に、Cisco Prime Infrastructure 2.2 の仮想アプライアンスと物理アプライアンスの両方に対する拡張マトリックスを示します。

表 2-3　Cisco Prime Infrastructure 2.2 の拡張マトリックス

パラメータ		Express 仮想アプライアンス	Express Plus 仮想アプライアンス	Standard 仮想アプライアンス	Pro 仮想アプライアンス	物理アプライアンス（Gen 1）	物理アプライアンス（Gen 2）
デバイス	最大 Unified AP 数	300	2,500 台	5,000	20,000	5,000	20,000
	最大 Autonomous AP 数	300	500	3,000	3,000	3,000	3,000
	最大 WLAN コントローラ数	5	25	500	1,000	500	1,000
	最大有線	300	1,000	6,000	13,000	6,000	13,000
	最大 NAM 数	5					
	最大デバイス数	1,000	4,000	15,000	20,000	15,000	20,000
クライアント	最大有線クライアント数	6,000	50,000	50,000	5=20,000	15,000	20,000
	最大無線クライアント数	4,000	30,000	75,000	200,000	75,000	200,000
	一時的ワイヤレス クライアント数（5 分間隔ごとのクライアント数）	1,000	5,000	25,000	40,000	25,000	40,000
モニタリング	維持イベント数/秒	100	100	300	1,000	300	1,000
	Netflow（フロー数/秒）	3,000	3,000	16,000	80,000	16,000	80,000
	Max Interfaces	12,000	50,000	250,000	350,000	250,000	350,000
	最大有効 NAM データ ポーリング数	5	5	20	40	20	40

表 2-3　Cisco Prime Infrastructure 2.2 の拡張マトリックス（続き）

パラメータ		Express 仮想アプライアンス	Express Plus 仮想アプライアンス	Standard 仮想アプライアンス	Pro 仮想アプライアンス	物理アプライアンス（Gen 1）	物理アプライアンス（Gen 2）
システム	最大サイト数/キャンパス	200	500	2,500	2,500	2,500	2,500
	最大グループ数	50	100	150	150	150	150
	最大仮想ドメイン数	100	500	1,200	1,200	1,200	1,200
	最大 GUI クライアント数	5	10	25	50	25	50
	最大 API クライアント数	2	2	5	5	5	5

ハイ アベイラビリティ

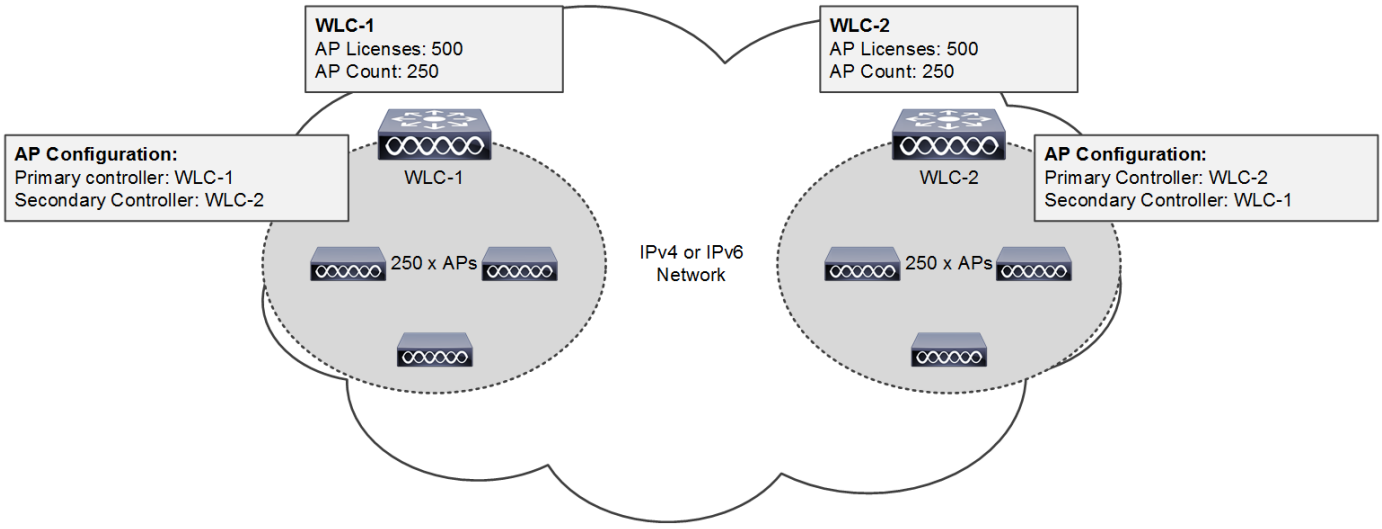
この項では、Cisco Unified Wireless Network で利用可能な高可用性（HA）導入オプションの概要を説明します。

AP およびクライアントのフェールオーバー

ワイヤレス コントローラの N+1 冗長性

WLC の冗長性は長い実績があり、よく知られています。冗長性は、バックアップとなり負荷を分担する複数のコントローラをネットワークに導入することによって実現されます。各 AP には IP アドレスおよび、優先されるプライマリと、セカンダリおよびターシャリの WLC の名前が設定されています。AP のプライマリ WLC が到達不能になった場合、AP は設定されているセカンダリ WLC にフェールオーバーします（その先も同様）。この冗長性モデルを N+1 と呼び、1 台（以上）のプライマリ WLC が到達不能になったときに AP および負荷をサポートする追加の WLC が利用可能であることを意味します（図 2-14 を参照）。

図 2-14　　ワイヤレス コントローラの N+1 冗長性



N+1 冗長性モデルを利用するには、バックアップ WLC ごとに追加の永続 AP ライセンスを購入する必要があります。バックアップ WLC は冗長性専用にしても、通常動作時に AP のサポートに使用してもかまいません。各 WLC は個別に管理され、設定を共有しません。障害発生時のシームレスな運用を確保するには、必要な WLAN、AP グループ、および RF グループを各バックアップ WLC に定義する必要があります。

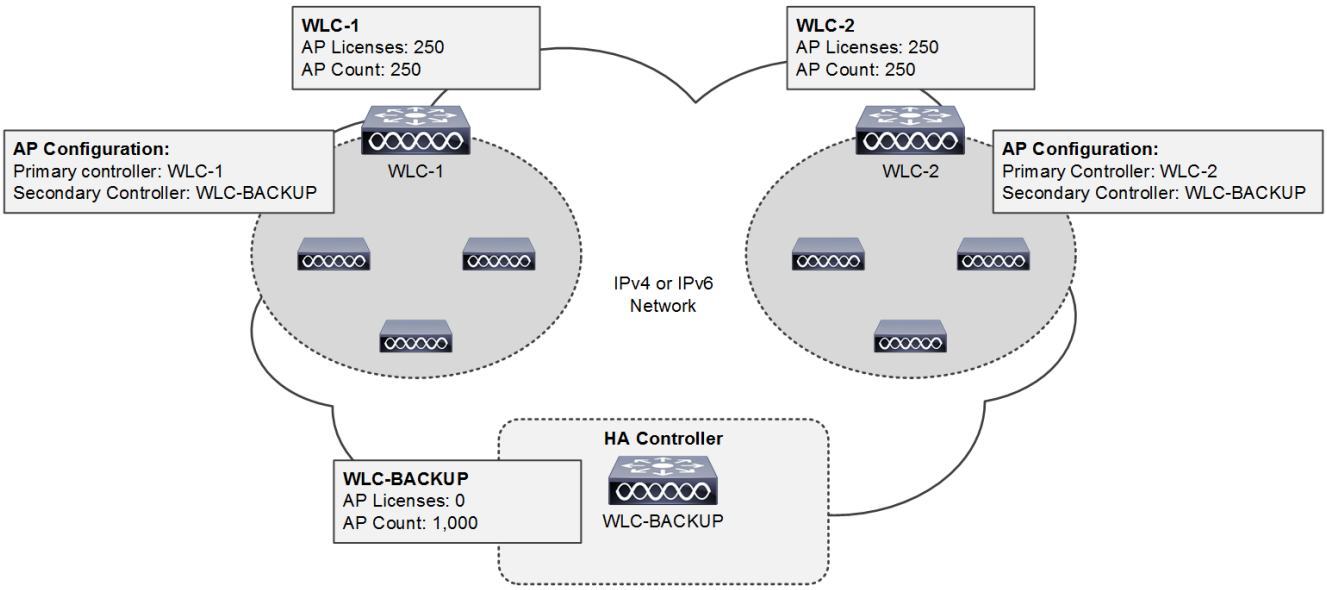
図 2-14 の例は、通常動作時にそれぞれ 250 台の AP をサポートしている 2 台の WLC を使用したシンプルな N+1 導入を示します。冗長性を実現するために各 WLC には 500 個の永続 AP ライセンスがインストールされており、WLC の 1 台が到達不能になったときにすべての AP が確実にサポートされるようになっています。WLC-1 に接続されている AP は WLC-2 をセカンダリ WLC として使用するように設定されている一方で、WLC-2 に接続されている AP は WLC-1 をセカンダリ WLC として使用するように設定されています。

(注)　大規模導入では、優先 WLC が使用できなくなるかオーバーサブスクライブされている場合、AP は CAPWAP ディスカバリ応答で確認された、モビリティ グループ内の WLC のリストから別の WLC、つまり、最も負荷の少ない WLC を選択します。

ワイヤレス コントローラの N+1 HA 冗長性

N+1 HA 機能は N+1 冗長性モデルを基礎として構築されており、複数のプライマリ WLC のバックアップとして単一の WLC を導入できるようになっています。前述したように、N+1 導入では、通常動作時に使用されないバックアップ WLC 用に追加の AP ライセンスを購入する必要があります。N+1 HA 導入では、複数のプライマリ WLC のバックアップ WLC として、HA-SKU WLC が追加の永続 AP ライセンスを必要とすることなく導入されています(図 2-15 を参照)。

図 2-15　　ワイヤレス コントローラの N+1 HA 冗長性



N+1 HA アーキテクチャでは、中央集中型と FlexConnect の両方の AP 導入に冗長性を提供できます。WLC 冗長性は同じキャンパスまたはサイト内で実現することも、地理的に離れたデータセンター間で実現することもできます。HA WLC は個別に管理され、プライマリ WLC と設定を共有しません。各 WLC は別々に設定および管理する必要があります。フェールオーバー時のシームレスな運用を確保するには、必要な WLAN、AP グループ、および RF グループを各 HA WLC に定義する必要があります。

プライマリ WLC が到達不能になるか故障すると、影響を受けた AP は HA WLC にフェールオーバーします。HA WLC には AP を最大 90 日間サポートするライセンスのみが付与されています。AP が HA WLC を接続し次第、90 日間のタイマーが開始されます。90 日間の有効期日を過ぎても AP が HA WLC に存在する場合は、警告メッセージが表示されます。HA WLC は、90 日間に限り、警告メッセージなしでセカンダリ WLC として使用できます。

図 2-15 の例は、500 台の AP を導入するためのシンプルな N+1 HA 導入を示します。両方のプライマリ WLC に 250 個の永続 AP ライセンスがインストールされています。この HA WLC モデルは当初 500 台の AP をサポートし、今後の拡張の余地をもたらすために選択されています。WLC-1 および WLC-2 に接続された AP は、セカンダリ WLC として WLC-BACKUP を使用するように設定されています。

（注）　HA-SKU は、2500 シリーズ、5500 シリーズ、7500 シリーズ、8500 シリーズのワイヤレス コントローラと WiSM2 で使用できます。N+1 HA 展開は、さまざまなモデルの WLC で構成できます（たとえば、5508 WLC をプライマリとして、5520 WLC HA-SKU をバックアップとして稼働するなど）。

（注）　vWLC の N+1 HA は、リリース 8.4 以降でサポートされます。

HA ステートフル スイッチオーバー ワイヤレス コントローラ冗長性

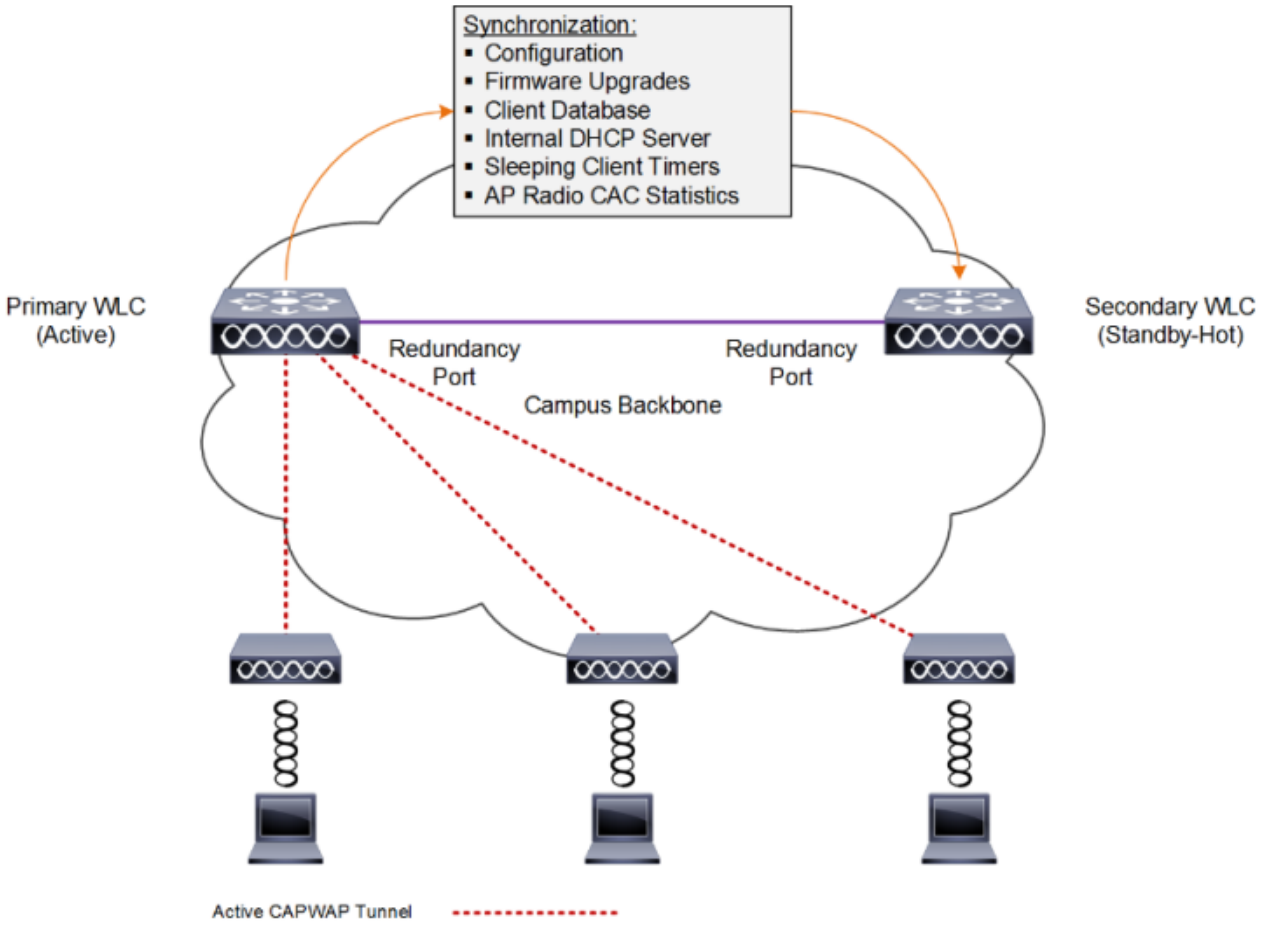
これまでの項で説明した N+1 と N+1 HA の冗長性アーキテクチャはいずれも、プライマリ WLC が到達不能になったときの AP フェールオーバーを実現しています。いずれのアーキテクチャも、プライマリ WLC に到達不能であることを AP が検出してセカンダリまたはターシャリの WLC にフェールオーバーする間、ワイヤレス サービスに影響が出ます。サービスに影響を与えない HA を実現するには、WLC 間で AP とクライアントの両方をシームレスに移行できるようにする必要があります。この WLC には、AP ステートフル スイッチオーバー（AP SSO）とクライアント ステートフル スイッチオーバー（クライアント SSO）の両方が実装されており、WLC フェールオーバー時のクライアント サービスのダウンタイムがゼロになり、SSID の非停止が実現されます。

HA ステートフル スイッチオーバー（SSO）は CUWN での推奨される HA 導入アーキテクチャです。この設計は、2 台の WLC が 1:1 プライマリ/セカンダリ ペアとして導入されている N+1 HA アーキテクチャを基盤としています。現在の構成および AP とクライアントの状態情報がプライマリとセカンダリのピア間で自動的に同期されます。大部分の導入では、プライマリ WLC には永続 AP ライセンスがインストールされている一方で、セカンダリ WLC は HA-SKU です（図 2-16 を参照）。

通常動作中、プライマリ WLC はアクティブ ロールを担当する一方で、セカンダリ WLC はスタンバイホット ロールを担当します。スイッチオーバーの発生後は、セカンダリ WLC がアクティブ ロールを担当し、プライマリ WLC がスタンバイホット ロールを担当します。それ以降のスイッチオーバーの後、ロールはプライマリおよびセカンダリ WLC 間で交換されます。これらの WLC は、冗長性管理インターフェイス（RMI）を通じて UDP キープアライブ パケットを交換することで、ピアと管理ゲートウェイの到達可能性をチェックします。

HA-SSO が有効化されるとすべての構成がアクティブ WLC で実行され、これがスタンバイホット WLC に自動的に同期されます。スタンバイホット WLC 上の CLI や Web UI では構成を実施できません。ファームウェア イメージもスタンバイホット WLC に配布されます。

図 2-16　　ワイヤレス コントローラの HA-SSO 冗長性



(注)　詳細については、『High Availability (SSO) deployment guide』(http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/HA_SSO_DG/High_Availability_DG.html) を参照してください。

HA-SSO アーキテクチャは、AP SSO とクライアント SSO の両方で構成されており、これらが組み合わさって、クライアントへのワイヤレス サービスに影響を与えることなく、1 秒未満の障害検出とフェールオーバーが実現されます。AP SSO が最初に追加されたのはリリース 7.3 であり、クライアント SSO が追加されたのはリリース 7.5 でした。

- AP SSO：AP でアクティブ WLC と CAPWAP トンネルを設定して、AP データベースのミラーコピーをスタンバイホット WLC と共有できます。AP はフェールオーバーの際に CAPWAP ディスカバリ状態になりません。任意の時点で、AP とアクティブ状態の WLC の間で維持される CAPWAP トンネルは 1 つだけです。AP SSO では、WLC またはネットワークのフェールオーバーなどによる、障害状態によって引き起こされるワイヤレス ネットワークの大規模なダウンタイムを削減することを全体的な目標としています。

- クライアント SSO：サービスに影響を与えずにシームレスなフェールオーバーを実現するには、クライアントおよび AP の両方をアクティブ WLC からスタンバイホット WLC へシームレスに移行できるようにする必要があります。SSO クライアントを使用すると、アクティブ WLC にクライアントが関連付けられたとき、またはクライアントのパラメータが変更されたときに、クライアント情報がスタンバイホット WLC に同期されます。完全に認証されたすべてのクライアントはスタンバイホット WLC に同期されるため、スイッチオーバー時のクライアント再関連付けが回避されて、クライアントに加え AP のフェールオーバーがシームレスになります。その結果、クライアント サービスのダウンタイムがゼロになり、SSID の停止が回避されます。

AP SSO とクライアント SSO は、3504、5500 シリーズ、7500 シリーズ、および 8500 シリーズの WLC と Wireless Services Module 2 でサポートされます。アプライアンス ベースの各 WLC では専用の冗長ポートがサポートされ、WiSM2 では冗長 VLAN が実装されています。冗長ポートはキープアライブ メッセージを交換するためと、設定および状態情報を同期するために使用されます。冗長ポートは直接接続されているか、中間レイヤ 2 ネットワークを通じて間接的に接続されています。表 2-4 に、WLC のモデルごとに HA SSO サポートの概要について説明します。

表 2-4　コントローラ プラットフォームごとの HA-SSO のサポート

プラットフォーム	冗長ポート	AP SSO	クライアント SSO
Cisco 2504 ワイヤレス コントローラ	×	×	No
Cisco 3504 ワイヤレス コントローラ	対応	対応（8.5 以上）	対応（8.5 以上）
Cisco 5508 ワイヤレス コントローラ	Yes	Yes（7.3 以上）	Yes（7.5 以上）
Cisco 5520 ワイヤレス コントローラ	Yes	Yes（8.1 以上）	Yes（8.1 以上）
Cisco Flex 7500 ワイヤレス コントローラ	Yes	Yes（7.3 以上）	Yes（7.5 以上）
Cisco 8510 ワイヤレス コントローラ	Yes	Yes（7.3 以上）	Yes（7.5 以上）
Cisco 8540 ワイヤレス コントローラ	Yes	Yes（8.1 以上）	Yes（8.1 以上）
Cisco ワイヤレス サービス モジュール 2	Yes：VLAN	Yes	対応
仮想ワイヤレス コントローラ（vWLC）	×	×	No

（注）　AP SSO およびクライアント SSO の実装はプライマリおよびセカンダリ WLC で動作しているソフトウェア リリースによって決まり、単独では設定できません。たとえば、HA が有効化されており、両方の WLC で 8.1 をサポートしている場合は、AP SSO とクライアント SSO の両方が実装されます。

冗長ポートおよび VLAN 設定

冗長ポートおよび VLAN は HA-SSO 導入では必須であり、設定および状態を同期するためと、キープアライブ パケットを交換するために使用されます。冗長ポート/VLAN はロール ネゴシエーションにも使用されます。3504、5500 シリーズ、7500 シリーズ、および 8500 シリーズ コントローラなどのアプライアンス ベースの WLC は専用のイーサネット冗長ポートを実装し、WiSM2 は冗長 VLAN を実装しています。

リリース 7.5 以降では、アプライアンス ベースの WLC の冗長ポートは、専用のイーサネット ケーブルを介して相互接続することも、専用のルーティング不能 VLAN を使用し、中間スイッチを介してレイヤ 2 で接続することもできます。光ファイバによるメディア コンバータ越しの直接接続もサポートされています。図 2-17 に、サポートされている冗長ポート接続オプションを示します。

図 2-17　冗長ポートの相互接続

WiSM-2 ベースの導入では、単一シャーシと複数シャーシの両方の導入で HA-SSO がサポートされています。複数シャーシ導入は、VSS を使用するか、リダンダンシー VLAN を拡張することでサポートされます。リダンダンシー VLAN はルーティング不可能な専用 VLAN である必要があります。図 2-18 に、シャーシ展開オプションを示します。

図 2-18　WiSM2 リダンダンシー VLAN

考慮事項

中間 L2 ネットワーク越しに冗長ポートまたは VLAN を接続するときは、次の考慮事項を満たす必要があります。

- ピア間のラウンド トリップ時間（RTT）遅延は 400 ミリ秒以下である必要があります（デフォルトでは 80 ミリ秒）。RTT は 100（デフォルト）～ 400 ミリ秒の範囲で設定可能なキープアライブ タイマーの 80 % です。RTT を大きくするときは、キープアライブ タイマーの設定を大きくする必要があります。
- ピア間に最低 60 Mbps の帯域幅が必要です。
- ピア間に最低 1,500 バイトの MTU パスが必要です。

トポロジ

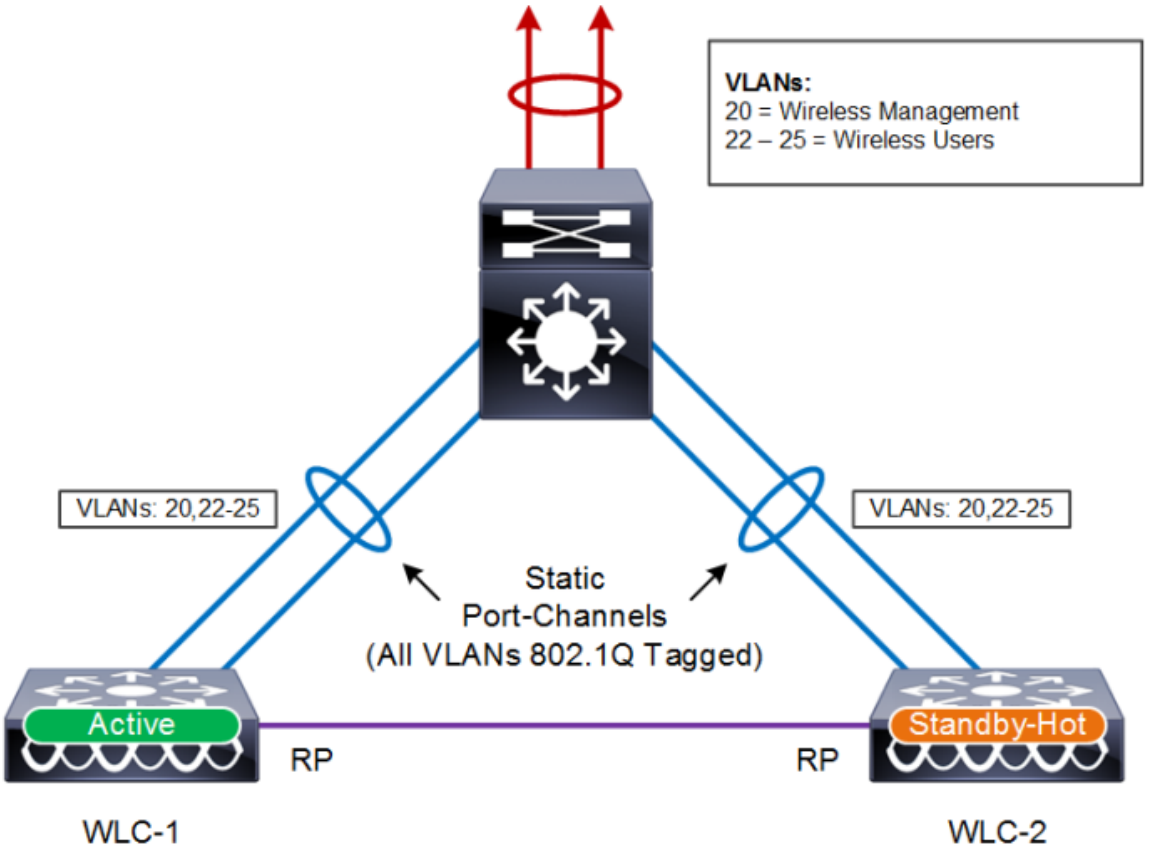
次の項では、Cisco Unified Wireless Network（CUWN）内に HA-SSO を導入するときの一般的なトポロジの概要を説明します。シンプルにするために、冗長ポートを直接接続したアプライアンス ベースの WLC を各例で示してあります。各トポロジは WiSM2 導入にも適用されます。

以下の各設計では、Catalyst ディストリビューション スイッチがワイヤレス サービス ブロックとコア レイヤの境界になっています。この境界は、LAN の 2 つの主要機能を実現しています。レイヤ 2 側では、ディストリビューション レイヤがスパニング ツリー プロトコル（STP）用の境界になって、レイヤ 2 障害の伝播を制限しています。レイヤ 3 側では、ディストリビューション レイヤは、ネットワークに入るときに IP ルーティング情報を要約する理論上の点になっています。この要約によって IP ルート テーブルが削減されてトラブルシューティングが容易になり、プロトコル オーバーヘッドが削減されて障害からのリカバリが迅速になります。

スタンドアロン ディストリビューション スイッチ

図 2-19 のトポロジは、ワイヤレス サービス ブロック内のスタンドアロン Catalyst スイッチに接続されている WLC の HA-SSO ペアを示します。冗長性は、復元力のあるスタックを形成するように複数のライン カードまたはスイッチを導入することによって実現されます。この設計では、シャーシまたはスタック全体の障害によって HA-SSO WLC がそれ以外のネットワークから孤立するため、ネットワークおよびハードウェアの障害に対する保護は最低限になっています。

図 2-19　スタンドアロン ディストリビューション スイッチを使用する HA-SSO



(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。これと等価な WiSM2 設計は、2 台の WiSM2 モジュールを設置した単一の Catalyst 6500 シリーズ シャーシで構成されます。

マルチレイヤ ディストリビューション スイッチ

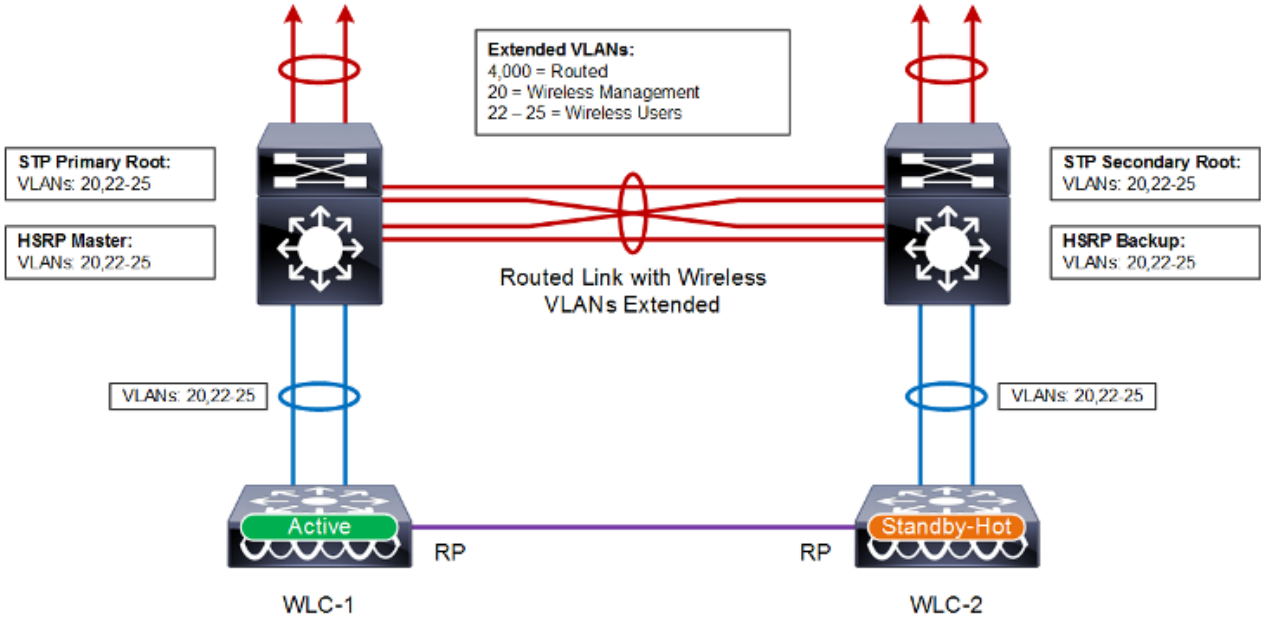
図 2-20 のトポロジは、マルチレイヤ設計を実装しているワイヤレス サービス ブロック内の Catalyst スイッチのペアに接続されている WLC の HA-SSO ペアを示します。このサンプル トポロジの Catalyst スイッチはレイヤ 3 接続であり、Catalyst スイッチ間でワイヤレス管理とワイヤレス ユーザ VLAN の拡張が必要であるため、複雑な設計になります。これは、スパニング ツリー プロトコルとファーストホップ ルーティング プロトコルを必要とするループを持つマルチレイヤ アーキテクチャに行き着きます。

- このアーキテクチャでは、Catalyst スイッチ間にルーテッド ポートもルーテッド ポートチャネルも実装できません。代わりに、リンクローカル VLAN とスイッチ仮想インターフェイス（SVI）の組み合わせを使用する必要があります。これにより、マルチレイヤ設計を維持しながら、Catalyst スイッチ間にワイヤレス VLAN を拡張できます。
- ループを避けるために、ワイヤレス VLAN ごとにスパニング ツリー プロトコル（STP）を有効化する必要があります。プライマリ WLC に接続している Catalyst スイッチを各 VLAN の STP ルート ブリッジとして設定する必要があります。

- 各ワイヤレス VLAN で、HSRP などのファーストホップ ルータの冗長性を有効化および設定する必要があります。プライマリ WLC に接続しているディストリビューション スイッチを各 VLAN の HSRP マスターとして設定する必要があります。

通常動作中は、アクティブ WLC に接続している Catalyst スイッチが各ワイヤレス管理 VLAN およびワイヤレス ユーザ VLAN のファーストホップ ルータです。これにより、STP ルートと HSRP マスターの両方を兼ねることで、Catalysts スイッチのペアをつなぐリンクを通過するトラフィックが最低限になります。プライマリ Catalyst スイッチが故障すると、HA-SSO によってスタンバイホット WLC へのフェールオーバーが行われます。プライマリ Catalyst スイッチがコアネットワークへの接続を失った場合、プライマリ WLC では、2 台の Catalyst スイッチ間で確立されたポートチャネルを通じてスタンバイホット WLC と引き続き通信できるため HA-SSO フェールオーバーは行われません。

図 2-20　　マルチレイヤ ディストリビューション スイッチを使用した HA-SSO

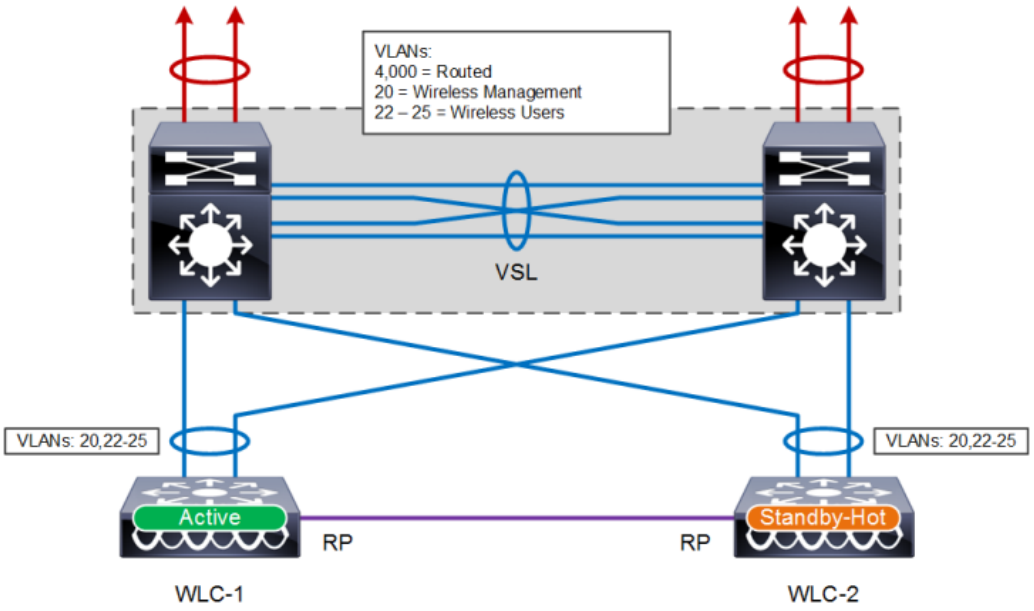


(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。同等な WiSM2 設計は、それぞれ 1 台の WiSM2 モジュールを設置したマルチレイヤ運用のために設定された 2 台の Catalyst 6500 シリーズ シャーシで構成されます。

VSS ディストリビューション スイッチ

図 2-21 のトポロジは、ワイヤレス サービス ブロック内のディストリビューション スイッチの VSS ペアに接続されている WLC の HA-SSO ペアを示しており、推奨される設計です。この設計では、通常運用時に VSS ペアの Catalyst スイッチをつなぐ仮想スイッチ リンクを通過するトラフィックが最低限になります。これは、アクティブとスタンバイホットのどちらの WLC も、どちらのスイッチとポートを介して接続されているためです。この設計では、VSS ペアでスイッチ障害が発生したときに、アクティブ WLC からスタンバイホット WLC へのスイッチオーバーも回避されます。ただし、VSS ペアでスイッチ障害が発生した場合、アクティブ WLC に接続されているポートの数が半減するおそれがあります。

図 2-21　　VSS を使用した HA-SSO



(注)　上記のアーキテクチャは WiSM2 導入にも当てはまります。同等な WiSM2 設計は、それぞれ 1 台の WiSM2 モジュールを設置した、VSS 構成に含まれる 2 台の Catalyst 6500 シリーズ シャーシで構成されます。

考慮事項

HA-SSO を実装するときは、次の考慮事項を検討する必要があります。

- Catalyst スイッチは、次の URL で公開されている Cisco Validated Design（CVD）で説明されている Cisco 推奨のベスト プラクティスに従って設定および導入されている必要があります: http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html。
- HA-SSO フェールオーバー時間は、ルーティング プロトコル、スパニング ツリー プロトコル、およびファーストホップ ルータの冗長性プロトコルによって添加されたコンバージェンス時間によって決まります。
- ワイヤレス管理、ワイヤレス ユーザ VLAN は、Catalyst スイッチと WLC の間で 802.1Q タギングされている必要があります。
- リンク アグリゲーション（LAG）を使用して Catalyst スイッチに HA-SSO WLC を接続することをお勧めします。WLC ポートは、復元力のあるスタックに含まれているシャーシまたはスイッチに搭載された異なるライン カード上のポート間で分散されている必要があります。VSS が導入されている場合、WLC ポートは両方の Catalyst スイッチ間で分散できます。
- WLC に接続しているネイバー Catalyst スイッチまたは VSS のポートチャネルのチャネル モードはモード オン（静的）に設定されている必要があります。WLC ソフトウェア リリース 8.1 では LACP プロトコルも PaGP プロトコルもサポートしていません。
- HA-SSO WLC をマルチレイヤ ディストリビューション スイッチに接続するときは、次の事項が適用されます。
- ワイヤレス管理 VLAN およびユーザ VLAN は、Catalyst ディストリビューション スイッチ間で 802.1Q タギングされます。この結果、ループを持つマルチレイヤ設計になります。

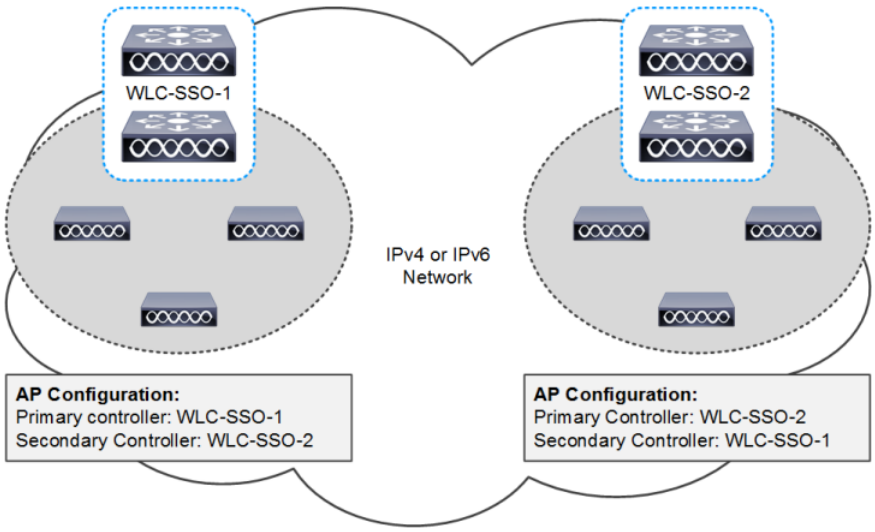
- ループを防止するために、ワイヤレス管理 VLAN およびワイヤレス ユーザ VLAN で Rapid Spanning Tree Protocol を有効化することをお勧めします。通常動作時にプライマリ WLC に接続している Catalyst スイッチは、各ワイヤレス VLAN の STP ルート ブリッジとして設定する必要があります。
- ワイヤレス管理 VLAN およびユーザ VLAN で HSRP などのファーストホップ ルーティング プロトコルを有効化する必要があります。通常動作時に プライマリ WLC に接続している Catalyst スイッチは、各 ワイヤレス VLAN の HSRP マスターとして設定する必要があります。
- アプライアンス ベースの WLC 冗長ポートは直接接続することも、レイヤ 2 で間接的に接続することもできます。間接的に接続するときは、各 Catalyst スイッチ間にルーティング不可能な専用 VLAN 2 つを拡張することをお勧めします。
- 冗長ポートが中間 L2 ネットワークを越えて拡張されている場合は、直前の項で説明した遅延、帯域幅、および MTU の要件を満たす必要があります。

HA-SSO と N+1 冗長性

大規模 Cisco Unified Wireless Network（CUWN）導入では、HA-SSO と N+1 冗長性の両方を組み合わせて、SSO-HA WLC が到達不能になった場合の AP フェールオーバーを実現できます（図 2-22）。これは、ビルディング、フロアなど明確な構造内でさまざまな HA-SSO ペアをサービス AP に割り当てる大規模 CUWN 導入で推奨される設計です。

この構成は、AP にプライマリ、セカンダリ、およびターシャリ WLC が設定されている N+1 HA 導入と完全に同様に機能します。AP のプライマリ WLC は割り当てられた HA-SSO WLC ペアとして設定されている一方で、セカンダリ（および任意でターシャリの）WLC は別の HA-SSO WLC ペアまたはスタンドアロン WLC として設定できます。AP は、プライマリ HA-SSO ペアのアクティブとスタンバイホットの両方の WLC が到達不能になったときに限り、セカンダリ WLC にフェールオーバーすることになります。セカンダリまたはターシャリ WLC へのフェールオーバーはステートレスです。

図 2-22　HA-SSO と N+1 冗長性



高速再起動

高速再起動の強化では、次の機能に変更を加える際のネットワークとサービスのダウンタイムを最大 73 % 削減することを目標としています。

- LAG コンフィギュレーションの変更
- モビリティ モードの変更
- Web 認証証明書の変更
- Clear Configuration

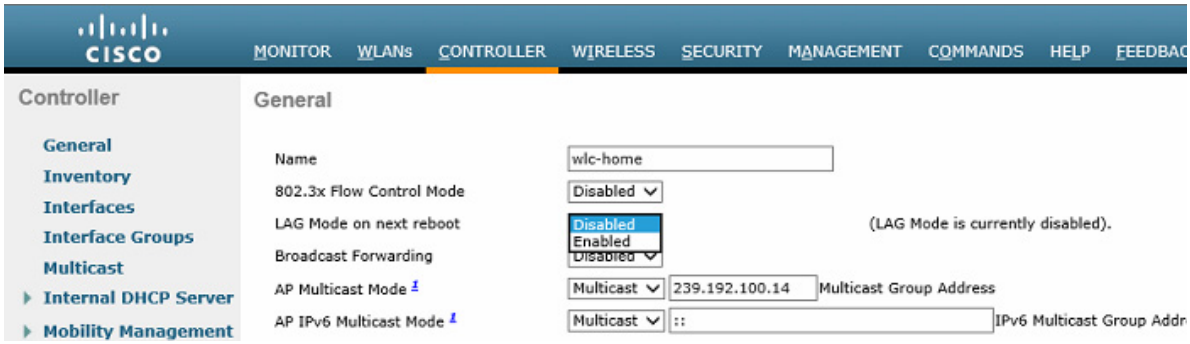
高速再起動がない場合、上記の変更を行うにはシステムの完全な再起動が必要です。高速再起動機能は、Cisco WLC 3504、WLC 5520、7510、8510、8540、およびリリース 8.1 以降の vWLC でサポートされます。高速再起動機能を呼び出すには、CLI で Restart コマンドを実行するか、Web UI で [Save and Restart] をクリックします。

リンク アグリゲーション（LAG）

リンク集約（LAG）は、802.3ad ポート集約標準の部分的な実装です。有効にした場合、WLC とネイバー スイッチの間に追加の帯域幅および耐障害性があれば、WLC のすべてのイーサネット ポートが LAG によって単一の 802.3ad ポートチャネルにバンドルされます。いずれかの WLC ポートまたは接続で障害が発生すると、トラフィックは、このバンドルに含まれる残存する他のいずれかのイーサネット ポートに自動的に移行されます。少なくとも 1 つのイーサネット ポートが機能している限り、ワイヤレス システムは稼働し続け、AP は存続し、クライアントはデータを送受信できます。

LAG は、WLC でグローバルに有効にされ（図 2-23）、Cisco WLC 2504、WLC 3504、5508、5520、および 8540 でサポートされます。LAG を有効にすると、すべてのイーサネット ポートがバンドルの対象になります。LAG を有効にするには、WLC のシステム全体をすぐに再起動するか、高速再起動を行う必要があります。

図 2-23　LAG モード



考慮事項

LAG を実装するときは、次の考慮事項を検討する必要があります。

- Cisco WLC は、LAG のインターフェイスで CDP アドバタイズメントを送信しません。
- LAG に含まれるすべての WLC イーサネット ポートは、同じ速度で動作する必要があります。ギガビット ポートと 10 ギガビット ポートを混在させることはできません。
- WLC に接続しているネイバー Catalyst スイッチまたは VSS のポートチャネルのチャネル モードはモード オン（静的）に設定されている必要があります。WLC ソフトウェア リリース 8.1 では LACP プロトコルも PaGP プロトコルもサポートしていません。
- WLC イーサネット ポートを別々の LAG グループに分けることはできません。
- すべてのイーサネット ポートが単一の論理ポートにバンドルされるため、サポートされる AP マネージャ インターフェイスは 1 つだけです。
- LAG を有効にした場合、動的 AP マネージャ インターフェイス、およびタグの付いていないインターフェイスはすべて削除されます。同時に、WLAN がすべて無効になり、管理インターフェイスにマッピングされます。管理インターフェイス、スタティック AP マネージャ インターフェイス、および VLAN タグ付き動的インターフェイスは、LAG ポートに割り当てられます。
- LAG が有効化されているときは、WLC がパケットを受信したポートと同じポートからパケットが送信されます。AP からの CAPWAP パケットがコントローラの物理ポート 1 に入ると、WLC によって CAPWAP ラッパーが除去され、パケットが処理され、物理ポート 1 からネットワークに転送されます。

モビリティ グループ、AP グループ、RF グループ

Cisco Unified Wireless Network 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

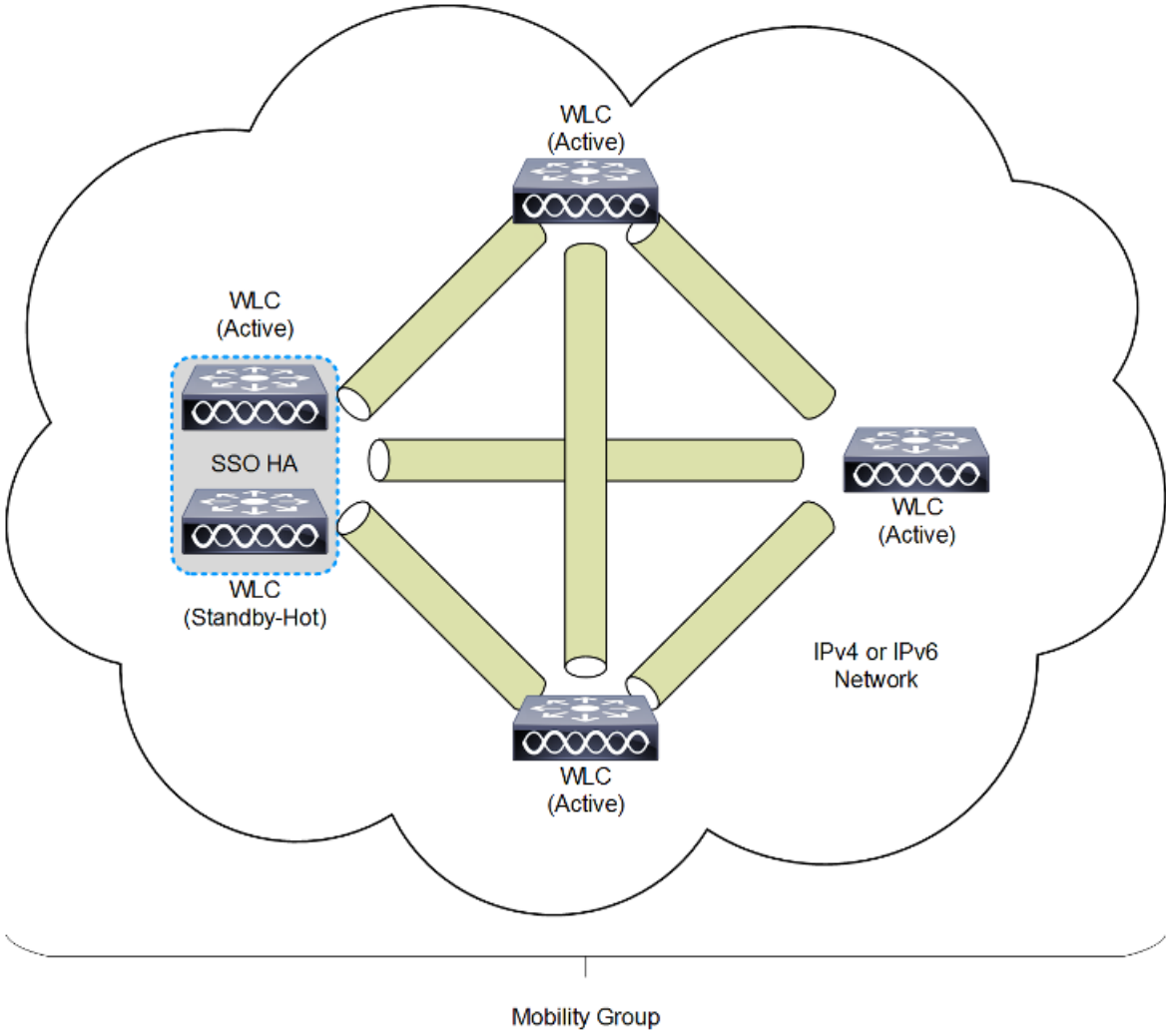
この項では、Cisco Unified Wireless Network におけるこれらのグループの目的と用途について説明します。

モビリティ グループ

モビリティ グループは、同じモビリティ グループ名で識別されるコントローラのセットで、ワイヤレス クライアントのローミングをシームレスに行う範囲を定義します。モビリティ グループを作成すると、ネットワーク内で複数の WLC を有効にして、コントローラ間またはサブネット間のローミングが発生した際に、クライアント、AP、RF に関する不可欠な情報を動的に共有してデータ トラフィックを転送できるようになります。同じモビリティ グループ内の WLC は、相互のアクセス ポイントを不正なデバイスとして認識しないように、クライアント デバイスのコンテキストと状態およびアクセス ポイントのリストを共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。

モビリティ グループは、図 2-24 に示すように、メンバー WLC 間にメッシュ状の認証トンネルを形成し、WLC がグループ内の他の WLC に直接問い合わせることができるようにします。

図 2-24　　WLC モビリティ グループ



リリース 8.0 以上では、インターネット プロトコル バージョン 4（IPv4）またはインターネット プロトコル バージョン 6（IPv6）を使用して WLC ピア間でモビリティ トンネルを設定できます。IPv4 トンネルまたは IPv6 トンネルの実装は各ピア用に定義されているモビリティ構成に基づきます。表 2-5 に、各モビリティ トンネル バージョンで実装されているプロトコルとポートの一覧を示します。

表 2-5　　モビリティ トンネルのプロトコルおよびポート

インターネット プロトコル	IP プロトコル	宛先ポート	説明
バージョン 4	17（UDP）	16,666	IPv4 モビリティ トンネル制御チャネル
	97（EITHERIP）	-	IPv4 モビリティ トンネル データ チャネル
バージョン 6	17（UDP）	16,666	IPv6 モビリティ トンネル制御チャネル
	17（UDP）	16,667	IPv6 モビリティ トンネル データ チャネル

モビリティ グループの考慮事項

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。ただし、以下に示すいくつかの重要な考慮事項があります。

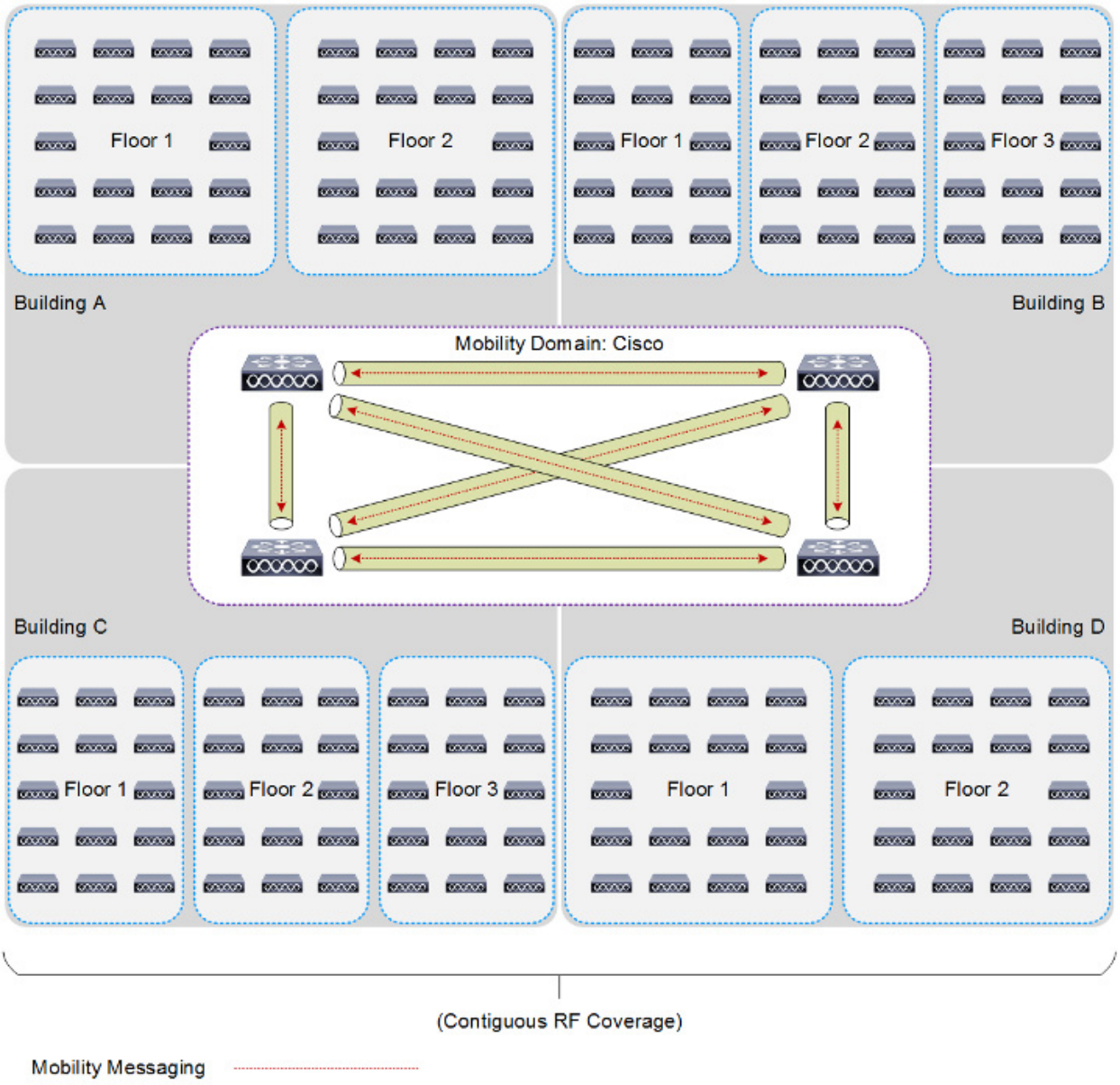
- 最大 24 台の WLC（任意のモデル）を単一のモビリティ グループに割り当てることができます。単一のモビリティ グループで、最大 144,000 台の AP がサポートされます（24 台の WLC X 6,000 台の AP = 144,000 台の AP）。エンタープライズ導入では、さらに多くの WLC および AP が構成されていることがありますが、これらは別のモビリティ グループのメンバーとして設定する必要があります。
- WLC は同一のモデルやタイプでなくても、モビリティ グループのメンバーにできます。ただし、各メンバーで同じバージョンのソフトウェアを実行している必要があります。
- メンバー間でソフトウェアが異なっていてもモビリティ グループは機能しますが、Cisco Unified Wireless Network 導入全体で機能の同一性を保証するために、共通のソフトウェア バージョンの使用を強く推奨します。
- スイッチオーバー（SSO）ありで WLC を導入する場合、各 WLC SSO ペアは単一のモビリティ ピアと見なされます。
- 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 で同一のモビリティ ドメイン名を使用する必要があり、相互の [Static Mobility Members] リストでピアとして定義する必要があります。この規則の例外となるのは、ゲスト アンカーを導入する場合であり、この場合は、ゲスト アンカー用に別のモビリティ グループを導入することをお勧めします。
- モビリティ グループ メンバー（WLC）の間でワイヤレス 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、特定の WLAN SSID とセキュリティの設定が一貫性を持っている必要があります。
- Cisco のベスト プラクティスでは、モビリティ グループのすべてのメンバーでマルチキャスト モビリティ機能を有効にすることをお勧めしています。この機能を利用するには、モビリティ グループの各メンバーに共通のローカル グループ マルチキャスト IPv4 アドレスを定義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 によって設定されたカバレッジが重複する導入の場合にだけ効果的です。それぞれ異なる WLC に関連付けられている 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（連続）していない場合には、モビリティ グループにメリットはありません。たとえば、キャンパスとブランチの間や複数のブランチ間のローミングです。

図 2-25　　モビリティ グループの例



モビリティ グループの例外

Cisco Unified Wireless Network 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、ワイヤレス ゲスト アクセス サービスおよび BYOD サービスの導入時に使用します。

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 にマッピングできる WLC の数は、わずか 71 個です。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 メンバー 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 メンバー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 グループのメンバーにしかなれません。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 グループのメンバーであると同時に、別のモビリティ グループのメンバーである外部 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 アンカー構成については、第 10 章「**Cisco Unified Wireless Network ゲスト アクセス サービス**」を参照してください。

AP グループ数

AP グループは、WLAN、RF、Hotspot 2.0、およびロケーション設定が共通している、ビルディング、フロア、リモート ブランチ オフィスなどの明確な区域内の AP の論理的なグループです。AP グループを利用してさまざまな AP グループに管理者が具体的な設定を割り当てできるため、Cisco Unified Wireless Network 導入で有用です。たとえば、AP グループを使用すると、キャンパス内のさまざまなビルディングにアドバタイズされる WLAN、WLAN クライアントに割り当てられるインターフェイスまたはインターフェイス グループ、高密度設計をサポートする特定のカバレッジ エリアの無線用の RRM と 802.11 の無線パラメータを制御できます。

サポートされている AP グループ固有の設定には次が含まれます。

- CAPWAP 優先モード：AP で IPv4 と IPv6 のいずれの CAPWAP モードを優先するのかを判別するために使用されます。
- NAS-ID：RADIUS 認証およびアカウンティングのために WLC によって使用されます。
- WLAN：WLAN 割り当て、インターフェイスとインターフェイス グループのマッピング、および NAC 状態。
- RF プロファイル割り当て：802.11、RRM、高密度、およびクライアント ロード バランシングの設定。
- Hotspot 2.0：802.11u の場所の構成および言語。
- ロケーション：HyperLocation 構成。

デフォルトでは、各 AP は「default-group」というデフォルト AP グループに自動的に割り当てられ、WLAN ID（1 ～ 16）がこのデフォルト グループにマッピングされます。16 を超える ID を含む WLAN には、カスタム AP グループを定義する必要があります。カスタマイズした AP グループが WLC に定義されている場合は、AP を手動でこの AP グループに割り当てる必要があります。

(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。詳細については、http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/ch5_QoS.html を参照してください。

表 2-6　シスコ ワイヤレス コントローラ AP グループの拡張(プラットフォーム別)

コントローラ プラットフォーム	最大 AP グループ数	AP グループあたり最大 AP 数
Cisco 2504 ワイヤレス コントローラ	75	75
Cisco 3504 ワイヤレス コントローラ	150	150
Cisco 5508 ワイヤレス コントローラ	500	500
Cisco 5520 ワイヤレス コントローラ	1,500	1,500
Cisco Flex 7500 ワイヤレス コントローラ	6,000	6,000
Cisco 8510 ワイヤレス コントローラ	6,000	6,000
Cisco 8540 ワイヤレス コントローラ	6,000	6,000
Cisco ワイヤレス サービス モジュール 2	1,000	1,000
Cisco 仮想ワイヤレス コントローラ	3,000	3,000

AP グループの考慮事項

AP 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。ただし、以下に示すいくつかの重要な考慮事項があります。

- AP は、AP グループに属していない場合には、「default-group」というデフォルト AP グループに割り当てられ、そのデフォルト グループに適用されているすべての設定を継承します。
- Cisco のベスト プラクティスとして、プライマリ、セカンダリ、およびターシャリ WLC 上のカスタマイズした AP グループ設定を一貫させることをお勧めします。定義されていない AP グループ名を持つ WLC を AP が接続する場合、AP では割り当てられた AP グループ(NVRAM)を維持しますが、default-group に適用されているすべての設定を継承することになります。その結果、AP の設定を誤り、ユーザ エクスペリエンスを低下させることがあります。
- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。WLAN インターフェイスが変更されると、AP グループ テーブル内の WLAN に対するインターフェイス マッピングにも反映されて新しい WLAN インターフェイスに変わります。
- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。WLAN インターフェイスが変更されても、AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。
- コントローラ上の設定をクリアすると、すべての AP グループ(「default-group」という AP グループを除く)が非表示となります。

- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。16 を超える ID を含む WLAN には、カスタム AP グループを定義する必要があります。
- OfficeExtend 600 シリーズ アクセス ポイントでは、最大で 2 つの WLAN と 1 つのリモート LAN がサポートされます。3 つ以上の WLAN と 1 つのリモート LAN を WLC で設定した場合は、カスタマイズした AP グループに Office Extend 600 シリーズ アクセス ポイントを割り当てる必要があります。WLAN 2 つとリモート LAN 1 つをサポートしている場合は、引き続きデフォルトの AP グループに該当します。さらに、WLAN およびリモート LAN の ID は 8 未満である必要があります。
- OfficeExtend アクセス ポイントはすべて同じ AP グループ内にあり、この AP グループに含まれる WLAN は 15 個以下にする必要があります。アクセス ポイント グループ内の OfficeExtend アクセス ポイントを持つコントローラは、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセス ポイントに最大 15 個の WLAN しか公開しません。
- すべての FlexConnect AP（同じブランチ/サイト内）を同じ AP グループおよび同じ FlexConnect グループに設定することをお勧めします。これにより、単一サイトのすべての AP で正しい WLAN-VLAN マッピングを継承するようになります。

AP グループの用途

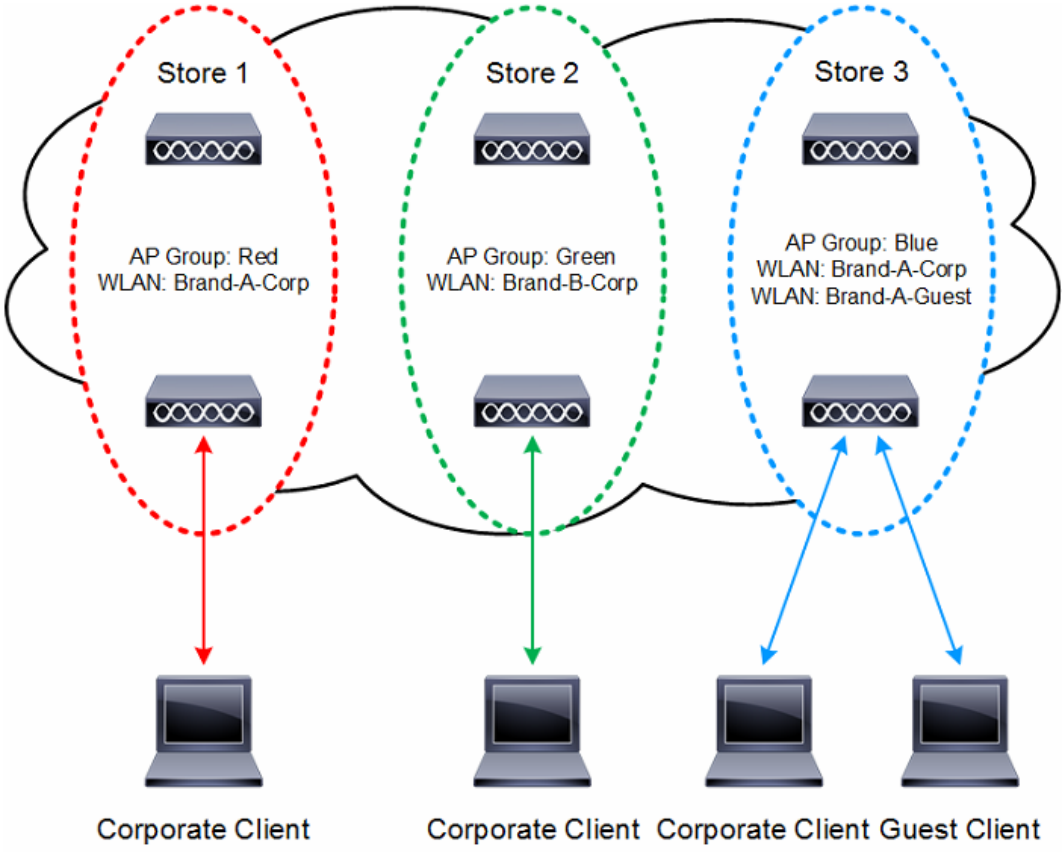
AP グループを使用すると、Cisco Unified Wireless Network に関する業務上の複数の課題を解決できます。ここでは、AP グループによってこれらの問題を解決できる一般的ないくつかの用途を解説します。

- 特定の地理的ロケーション内で AP によってアドバタイズされる WLAN を制御します。たとえば、キャンパス導入では、別々の AP グループを利用してゲスト WLAN を共用部分のみにアドバタイズすることも、キャンパス全体にすることもできます。小売店での導入では、AP グループを利用してさまざまなブランド ショップ（合併および買収）用に一意の SSID をアドバタイズしたり、ゲスト Wi-Fi サービスを一部の小売店に提供したりできます。

図 2-26 に示すように、リモート FlexConnect AP をサポートしている WLC には、異なるブランドのリモートの小売店をサポートするためとクライアント サポートのために 3 個の個別 AP グループが設定されています。ショップ 1 および 3 は同じブランドであり、企業の SSID は共通していますが、ショップ 3 では常連客向けにゲスト Wi-Fi を提供している一方でショップ 1 では提供していないため、ショップ 3 用に別の AP グループが必要です。

ショップ 2 は異なる企業 SSID を実装している異なるブランドです。ショップ 2 にあるクライアント デバイスはまだ標準の企業 SSID に移行されていないため、このショップをサポートするために個別の AP グループが必要です。

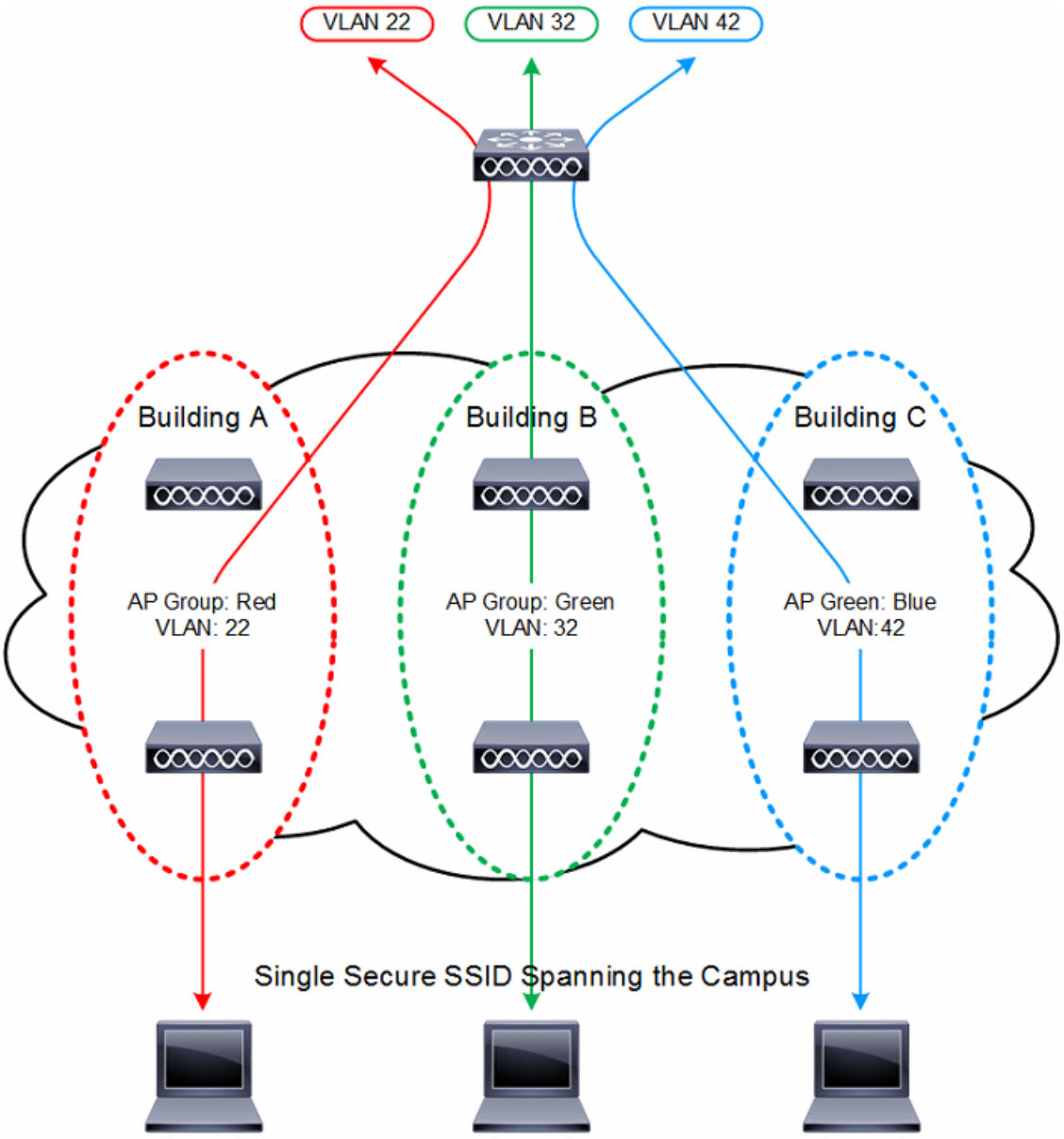
図 2-26　WLAN 割り当て用の AP グループ



- WLC 内の別のインターフェイスまたはインターフェイス グループに WLAN クライアントをマッピングすることによって、ブロードキャスト ドメインのサイズを縮小します。たとえば、キャンパス導入では、AP グループを利用して別々のビルディングまたはフロアにある WLAN クライアントを単一の WLC 上で別々のインターフェイスまたはインターフェイス グループにマッピングできます。

図 2-27 では、3 つの動的インターフェイスが WLC に設定され、それぞれにサイト固有の VLAN（VLAN 22、32、42）があります。サイト固有の VLAN および関連付けられた AP は、それぞれ AP グループを使用して同一の WLAN SSID にマッピングされます。VLAN 22 に対応する AP グループ内の AP 上の WLAN に関連付けられている企業ユーザは、VLAN 22 サブネットで IP アドレスを取得します。同様に、VLAN 32 に対応する AP グループ内の AP 上の WLAN に関連付けられている企業ユーザは、VLAN 32 サブネットなどで 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。

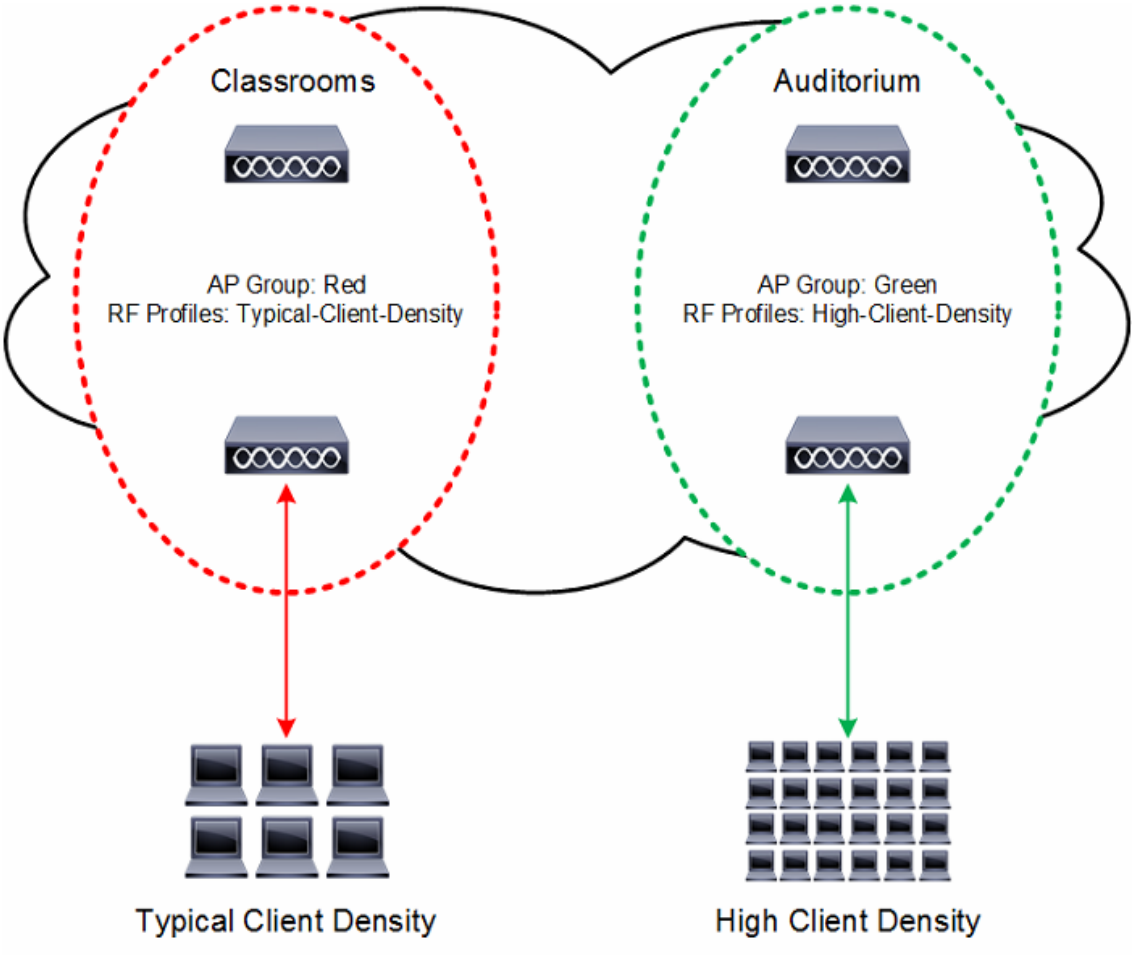
図 2-27　インターフェイス/インターフェイス グループ割り当て用の AP グループ



- 地理的ロケーション内で RF 環境を最適化して、さまざまなクライアント密度をサポートします。カバレッジ エリアにある AP を、異なるクライアント ニーズまたは密度をサポートするように最適化された異なる RF プロファイルに割り当てることができます。

図 2-28 に示すように、異なる AP およびクライアントの密度をサポートするように 2 つの AP グループが WLC に設定されています。1 つ目の AP グループは一般的な密度で導入されている AP およびクライアント用に設定されている一方で、2 つ目の AP グループは高密度で分布する AP とクライアントをサポートするように設定されています。

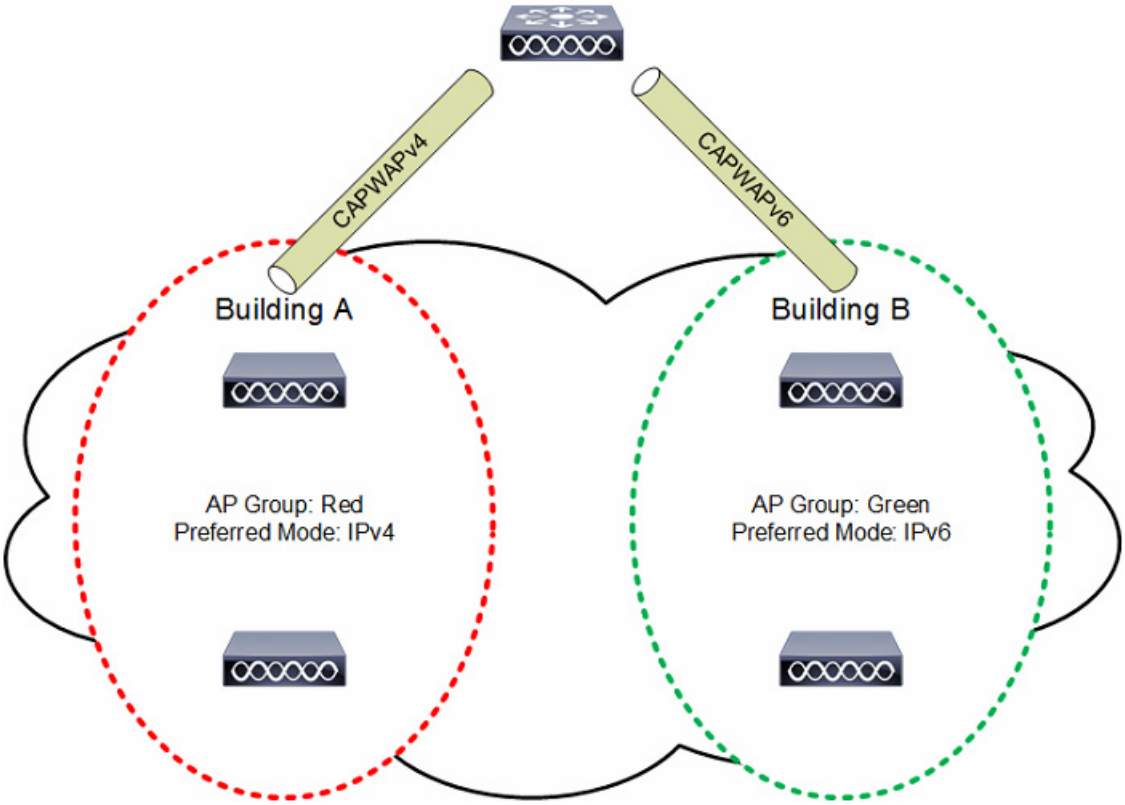
図 2-28　RF 最適化およびクライアント密度用の AP グループ



- インターネット プロトコル バージョン 4（IPv4）からインターネット プロトコル バージョン 6（IPv6）に AP を移行します。AP グループを利用すると、個々のビルディングまたはサイトの遷移に応じて AP CAPWAP 優先モードを IPv4 から IPv6 に切り替えることができます。

図 2-29 では、IPv4 から IPv6 への移行を支援する 2 つの AP グループが WLC に設定されています。各 AP グループには、WLC を接続するときに AP で使用する IP プロトコルを決定する、固有の CAPWAP 優先モードが設定されています。

図 2-29　　IPv6 移行用の AP グループ



RF グループ

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。コントローラ ソフトウェアは、1 つの RF グループで最大 20 台の WLC と 6,000 台の AP をサポートするように拡張できます。

RF グループおよび RRM については、第 3 章「WLAN RF の設計に関する考慮事項」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。

- CAPWAP 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。他の 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 グループのメンバーになります。
- RF グループのメンバーによって、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）します。
  - 802.11 の同一チャネル干渉および競合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ーは、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。更新間隔の合間に、RF グループ リーダーは各 RF グループ メンバーにキープアライブ 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 WLC 数は 20 です。

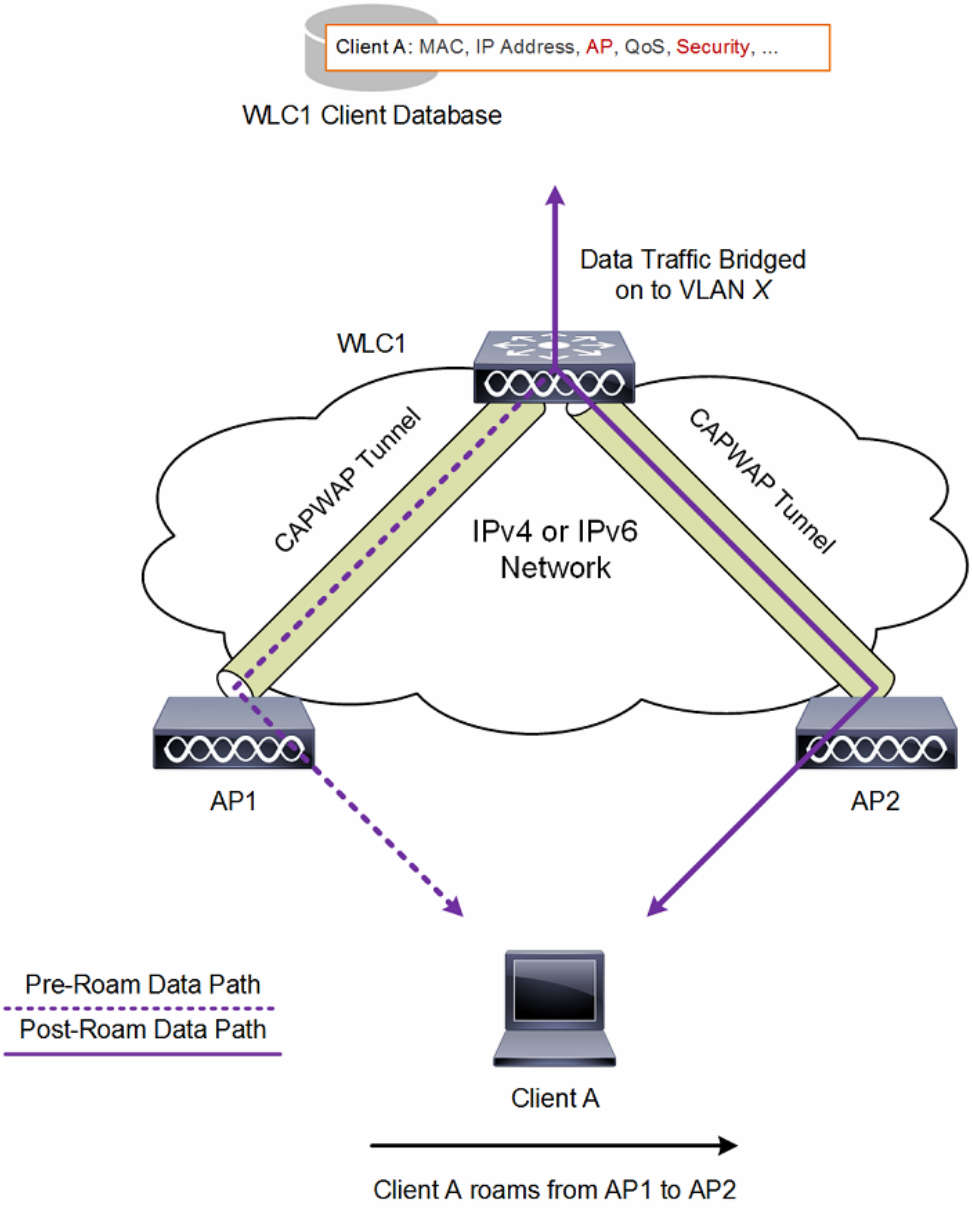
（注）　RF グループとモビリティ グループは、どちらも WLC のクラスタを定義するという点では同じですが、用途に関しては異なります。RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティと WLC の冗長性を実現します。

ローミング

モビリティ（ローミング）は、できるだけ遅れることなく、安全に、ある AP から別の AP へアソシエーションをシームレスに維持する WLAN クライアントの機能です。この項では、WLC が Cisco Unified Wireless Network に含まれている場合のモビリティの動作について説明します。

ある WLAN クライアントが AP に関連付けして認証すると、WLC は、クライアント データベースにそのクライアントに対するエントリを設定します。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、Quality of Service（QoS）コンテキスト、WLAN、SSID、および関連付けられた 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、ワイヤレス クライアントで送受信されるトラフィックを管理します。図 2-30 は、同じコントローラに参加している 2 つの AP の一方からもう一方にローミングするワイヤレス クライアントを示しています。

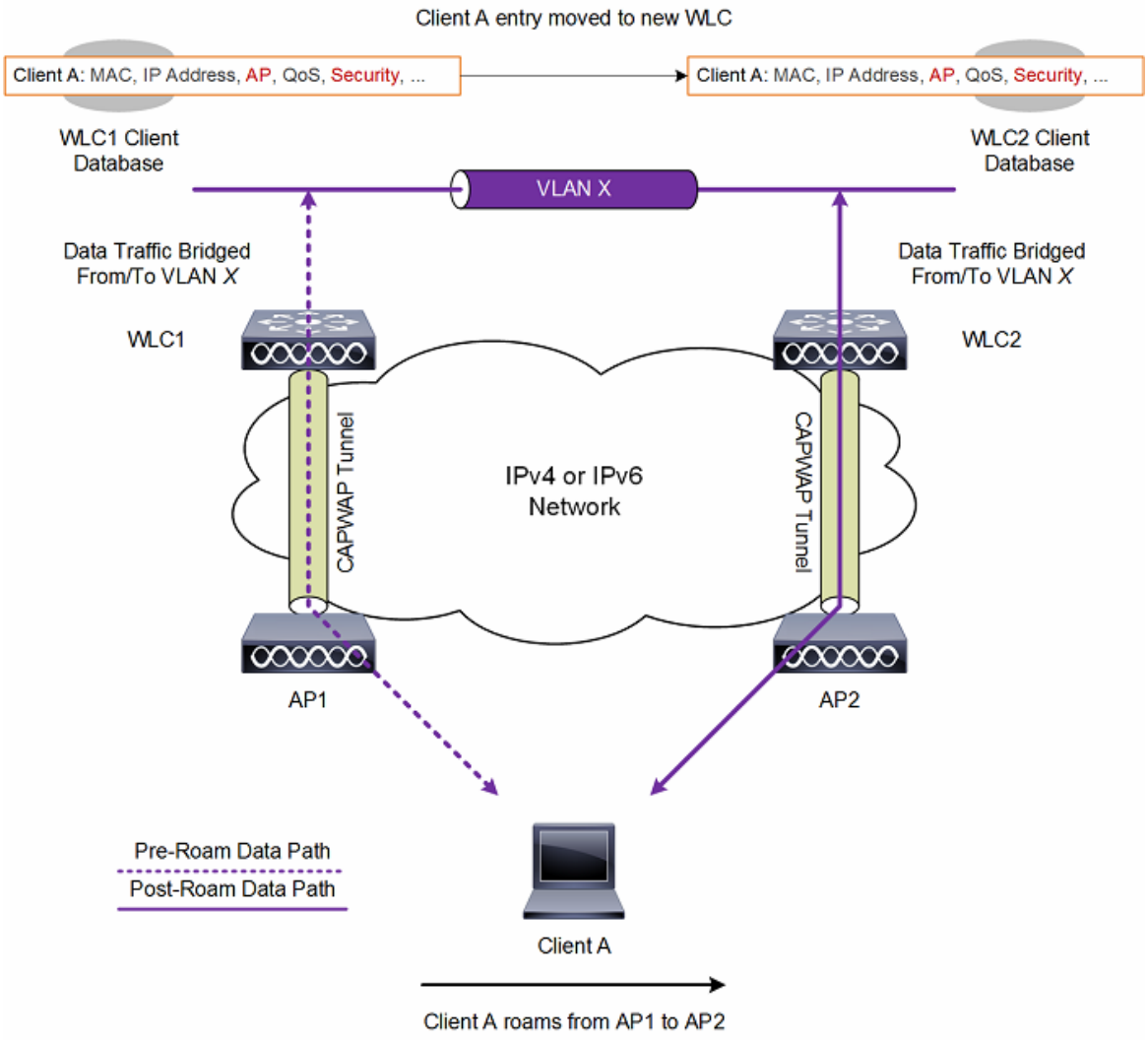
図 2-30　　コントローラ内ローミング



WLAN 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 は新規に関連付けられた AP を含むクライアント データベースをアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

しかし、クライアントが 1 つの WLC に接続された AP から別の WLC に接続された AP にローミングする際には、プロセスはより複雑になります。また、同一の VLAN 上でこれらの WLC が動作しているかどうかによっても異なります。図 2-31 は、WLC インターフェイスまたはインターフェイス グループが同じ VLAN をサポートしている場合に発生するコントローラ間ローミングを示します。

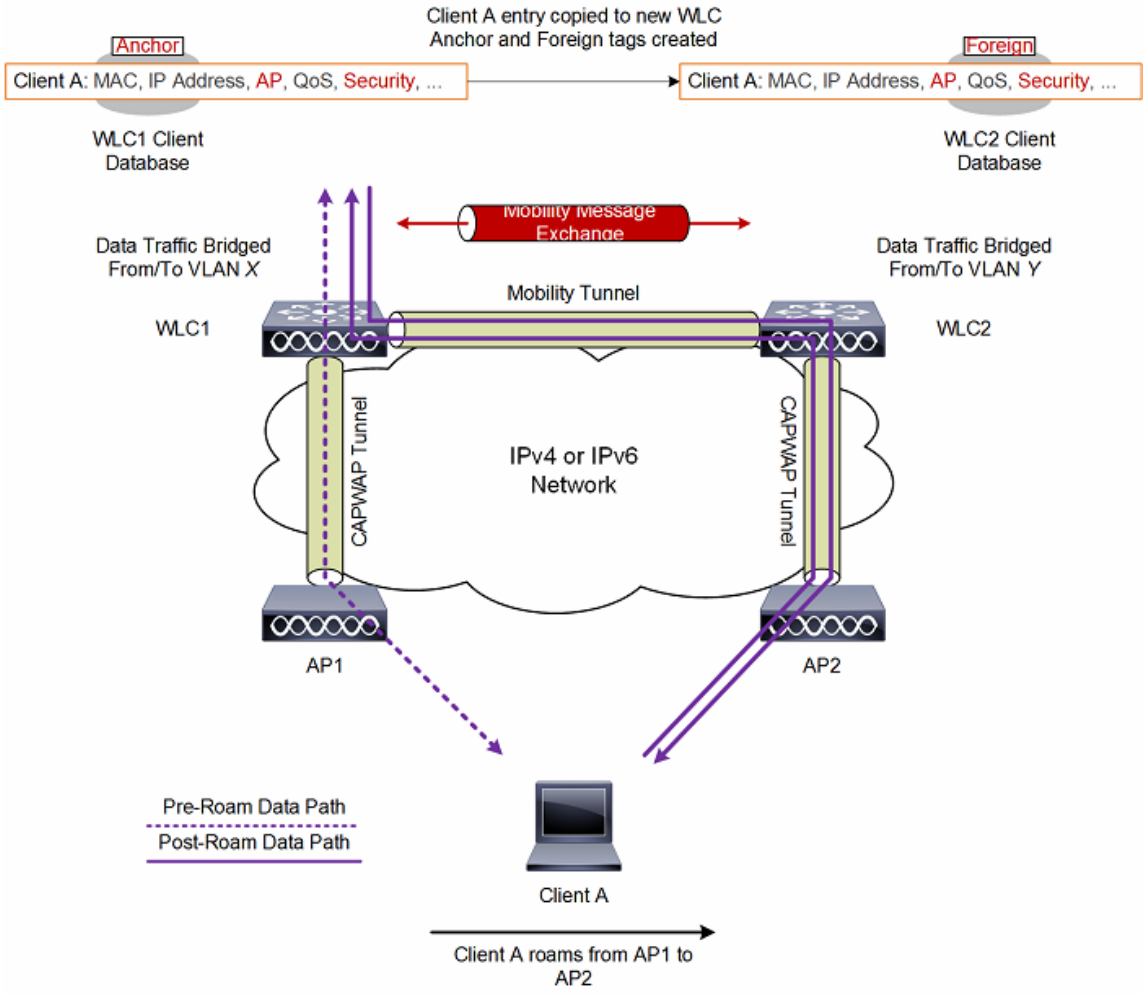
図 2-31　　コントローラ間ローミング



クライアントが新たなコントローラに接続された AP へ関連付けする場合、新たな WLC はモビリティ メッセージを元の WLC と交換し、クライアントのデータベース エントリは新たな WLC に移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たな AP 用にアップデートされます。このプロセスは、ユーザには透過的に行われます。

図 2-32 は、WLC インターフェイスが異なる VLAN 上にある場合に起こるサブネット間ローミングを示しています。

図 2-32　　サブネット間ローミング



サブネット間ローミングは、WLC がクライアントのローミングに関するモビリティ メッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベース エントリを新しい WLC に移動するのではなく、元のコントローラのクライアント データベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベース エントリが新しいコントローラのクライアント データベースにコピーされ、新しい WLC 内で「外部」エントリのマークが付けられます。ローミングはワイヤレス クライアントには透過的なまま行われ、クライアントは VLAN メンバーシップおよび元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両 WLC の WLAN に同一のネットワーク アクセス権限を設定し、ソースベースのルーティングやソースベースのファイアウォールを設定しないでおく必要があります。そうしない場合、ハンドオフ後クライアントに接続上の問題が発生することがあります。

(注)　クライアントが Web 認証状態でローミングする場合、クライアントはモバイル クライアントして見なされるのではなく、別のコントローラ上の新しいクライアントとして見なされます。

IPv6 クライアント モビリティ

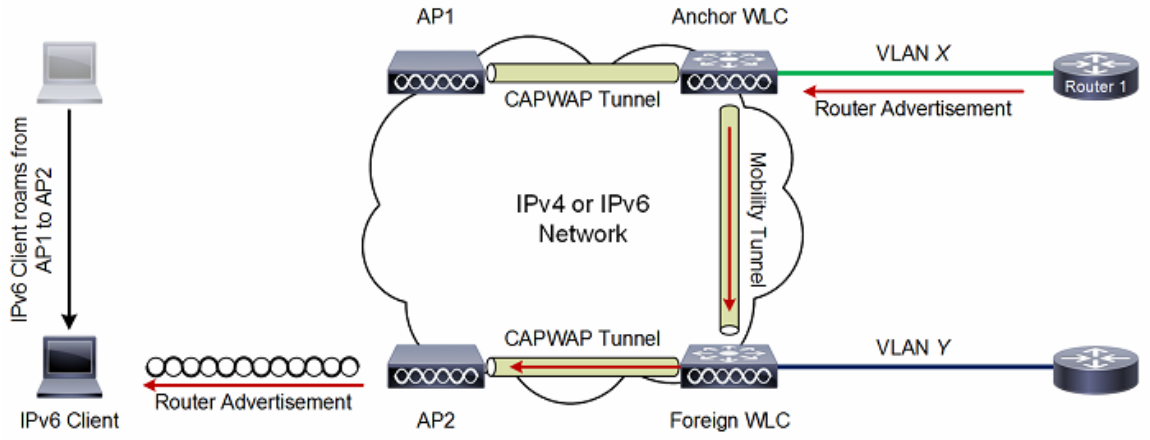
WLC をまたがる IPv6 クライアントのローミングに対応するためには、Neighbor Solicitation（NS）、Neighbor Advertisement（NA）、Router Advertisement（RA）、Router Solicitation（RS）などの ICMPv6 メッセージに対処して、IPv6 クライアントが確実に同じレイヤ 3 ネットワーク上にとどまるようにする必要があります。IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。必要な唯一の設定は、WLC が、同じモビリティ グループに属している必要があることです。

WLC をまたがる IPv6 クライアント モビリティのプロセスは次のとおりです。

- クライアントで元々接続していた VLAN に両方の WLC がアクセスできる場合、ローミングは、クライアント レコードが新しい WLC にコピーされる単なるレイヤ 2 ローミング イベントであり、トンネリングによってアンカー WLC に戻されるトラフィックはありません。
- クライアントが接続されていた元の VLAN に 2 台目の WLC がアクセスできない場合は、レイヤ 3 ローミング イベントが発生することになります。クライアントからのすべてのトラフィックはアンカー コントローラへのモビリティ トンネルを使用してトンネリングされる必要があります。リリース 7.x と 8.x による混合 WLC 導入では、モビリティ トンネルは EtherIP を使用する IPv4 ベースになります。純然たる 8.0 導入では、モビリティ トンネルは IPv4 ベースと IPv6 ベースのどちらも可能で、EtherIP（IPv4）または CAPWAP（IPv6）を使用することになります。
  - クライアントで元の IPv6 アドレスを保持することを確実化するために、元の VLAN からの RA がアンカー WLC によって外部 WLC に送信され、ここで AP からの L2 ユニキャストを使用してクライアントに配送されます。
  - ローミングされたクライアントが DHCPv6 を介してアドレスを更新するか、SLAAC を介して新しいアドレスを生成する場合、RS、NA、および NS のパケットは引き続き元の VLAN にトンネリングされるため、クライアントでは割り当てられた VLAN に適用できる IPv6 アドレスを受信します。

図 2-33 は、WLC インターフェイスが異なる VLAN 上にある場合に起こる、IPv6 クライアントのサブネット間ローミングを示しています。このプロセスは、ローミングされたクライアントのトラフィックがアンカー WLC にトンネリングされる、図 2-32 に示すサブネット間ローミングと同一です。ICMPv6 の RS、NA、および NS パケットすべてがアンカー WLC にトンネリングされるため、IPv6 クライアントは元の VLAN および IPv6 アドレスを維持でき、シームレスなローミング エクスペリエンスが実現されます。

図 2-33　　IPv6 サブネット間ローミング



(注)　リリース 8.5 以降では、IPv6 インターフェイスで SNMP over IPSec（Simple Network Management Protocol over Internet Protocol Security）がサポートされます（セキュア ローミング）。

Cisco Unified Wireless Network（CUWN）でサポートされている各種の高速ローミング方式について説明する前に、クライアントが PSK または 802.1X キー管理を使用して WPA2 WLAN に接続するときの認証方法と検証方法を理解することが重要です。この情報は、各方式用に高速セキュア ローミングを実装する方法を理解するうえで、追加のコンテキストを提供するため重要です。

WPA/WPA2-PSK 方式と WPA/WPA2-EAP 方式では、WLAN クライアントの認証と検証の方法は異なりますが、キー管理プロセスのルールは両方式で同一です。WPA2 WLAN のキー管理が PSK と 802.1X のいずれでも、使用した特定の認証方式によってクライアントがいったん検証されると、Master Session Key（MSK）を元のキー マテリアルとして使用して、フォーウェイ ハンドシェイクと呼ばれるプロセスが WLC/AP とクライアントの間のキー ネゴシエーションを開始します。

プロセスの概要を次に示します。

- MSK は、802.1X キー管理による WPA/WPA2 では EAP 認証フェーズで取得され、PSK による WPA/WPA2 では事前共有キーから取得されます。
- クライアントおよび WLC/AP では、この MSK からペアワイズ マスター キー（PMK）を取得します。
- この 2 種類のマスター キーを取得し終えると、クライアントおよび WLC/AP は、マスター キーをシードとするフォーウェイ ハンドシェイクを開始して実際の暗号化キーをネゴシエートします。
  - Pairwise Transient Key（PTK）：PTK は PMK から取得され、クライアントとのユニキャスト フレームを暗号化するために使用されます。
  - Group Transient Key（GTK）：Group Transient Key（GTK）は GMK から取得され、この特定の SSID または AP でのマルチキャストまたはブロードキャストを暗号化するために使用されます。

高速セキュア ローミングは、CUWN に含まれる AP 間でのクライアント ローミングの所要時間を短縮することを目的としています。高速ローミングは、ローミング時の後続の EAP 認証やフォーウェイ ハンドシェイクを回避できる、キー管理と配布の巧みなテクニックを実装することによって実現されます。これらのフェーズを回避することでクライアントが新しい AP に再関連付けするための所要時間が短縮され、Voice over IP（VoIP）などの時間的精度が要求されるアプリケーションに関する知覚可能な遅延を限定的にします。

次の項では、8.0 リリースで使用可能な、サポートされている各高速セキュア ローミング方式の概要を説明します。

（注）　この項で説明する各高速セキュア ローミング方式の詳細（パケットのキャプチャおよびデバッグを含む）については、次の URL にある Cisco トラブルシューティング テックノート『802.11 WLAN Roaming and Fast-Secure roaming』を参照してください：
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html。

Cisco Centralized Key Management

Cisco Centralized Key Management（CCKM）は、シスコが企業 WLAN 用に開発した最初の高速セキュア ローミング方式であり、WLAN で 802.1X セキュリティまたは EAP セキュリティが有効化されている場合のローミングの遅延を軽減するソリューションです。これはシスコの独自プロトコルであるため、Cisco Compatible Extension（CCX）互換のシスコおよびサードパーティ製のクライアントのみでサポートされています。

CCKM は、WEP、TKIP、AES など WLAN で使用可能な多様な暗号化方式のいずれでも実装できます。複数の EAP 方式もサポートしています（クライアント デバイスでサポートされている CCX バージョンに依存）。

CCKM を使用する場合、WLAN への最初のアソシエーションは WPA および WPA2 と類似しており、MSK（ここでは、ネットワーク セッション キーとも呼ぶ）は RADIUS サーバとの成功した認証から相互に取得されます。このマスター キーは認証成功後にサーバから WLC に送信されて、このクライアント セッションの存続中に後続のキーを生成するためのベースとしてキャッシュされます。WLC およびクライアントは、ユニキャスト（PTK）および、マルチキャストとブロードキャスト（GTK）の暗号化キーを取得するために、フォーウェイ ハンドシェイクを実施しながら（WPA および WPA2 と同様）、CCKM に基づいて高速セキュア ローミングに使用されるシード情報を取得します。

CCKM クライアントが新しい AP にローミングする場合、クライアントでは単一の再アソシエーション要求フレームを CAPWAP AP に送信し（単一の MIC および順次増分される乱数を含む）、新しい PTK を取得するために十分な情報（新しい BSSID MAC アドレスを含む）を提供します。この再アソシエーション要求では、WLC および新しい AP は新しい PTK を取得するために十分な情報も持っているため、単に単一の再アソシエーション応答で応答し、EAP 認証とフォーウェイ ハンドシェイクの両方が回避されます。

概要：

- CCX 互換のシスコおよびサードパーティ製のクライアントのみでサポートされます。
- さまざまな暗号化方式および EAP 方式をサポートしています（CCX のバージョンに依存）。
- 高速ローミングは、802.1X 認証と EAP 認証およびフォーウェイ ハンドシェイクを回避することによって実行されます。

- 中央集中型導入と FlexConnect 導入（ローカルまたは中央でスイッチング）の両方でサポートされています。
  - 中央集中型：同じモビリティ グループ内の AP および WLC をまたがって機能します。
  - FlexConnect：同じ FlexConnect グループ内の AP をまたがって機能します。
- FlexConnect WLAN は、中央またはローカルのスイッチングを使用するローカル認証または中央集中型認証用に設定できます。
- FlexConnect AP は接続モードとスタンドアロン モードでサポートされていますが、スタンドアロン モードでの MSK の共有方法に関する制限事項があります。

ペアワイズ マスター キー キャッシング

ペアワイズ マスター キー（PMK）キャッシング、別名 Sticky Key Caching（SKC）は、802.11i のセキュリティの改定の一環として IEEE 802.11 標準によって推奨された、第 1 の高速セキュア ローミング方式です。PMK キャッシングでは、クライアントによる AP との関連付けが可能であり、802.1X 認証または EAP 認証と、フォーウェイ ハンドシェイクに成功すると、PMK がキャッシュに保存されます。ローミングによって AP を去ったクライアントが戻ってきた場合、クライアントでは 802.1X 認証または EAP 認証を回避できます。

PMK キャッシングは 802.1X または PSK キー管理を使用して WPA2 WLAN でサポートされており、WLAN インフラストラクチャとクライアント サポートの両方を必要とします。

- 任意の AP への最初のアソシエーションは WLAN への通常の初回認証と似ており、802.1X または PSK の認証と、フォーウェイ ハンドシェイクが成功してからでないと、クライアントはデータ フレームを送信できません。
- ワイヤレス クライアントが、新しい AP（それまでに関連付けしたことのない AP）にローミングした場合、クライアントは 802.1X または PSK の認証とフォーウェイ ハンドシェイク全体を再度実行する必要があります。

このワイヤレス クライアントがローミングによって AP（それまでに関連付けしたことのある AP）に戻る場合、このクライアントは複数の PMKID をリストしている再アソシエーション要求フレームを送信します。このフレームは、クライアントがそれまでに認証されたことのあるすべての AP からキャッシュした PMK をこの AP に伝達します。クライアントはこのクライアント用の PMK もキャッシュしている AP にローミングして戻ってきているため、新しい PMK を取得するための再認証を必要としません。クライアントでは、新しい一時的な暗号化キーを取得するために、WPA2 フォーウェイ ハンドシェイクを行うのみです。ローミングによる復帰はクライアントに設定可能な限定された時間間隔内（Windows でのデフォルト 720 分）に発生する必要があります。

CUWN 中央集中型導入では、各 CAPWAP AP 用のキャッシュ済み PMK は WLC によって管理および維持されます。各 AP のクライアントごとに別々の PMK が生成されるため、拡張性は限られています。したがって、PMK キャッシングは大規模エンタープライズ導入には推奨されず、広く採用されてはいません。

概要：

- シスコのマニュアルでは、Sticky Key Caching（SKC）と呼ばれています。
- 802.1X または PSK キー管理を使用した WPA2 WLAN でのみサポートされています。

- 効率的でないキー管理により拡張性が大幅に制限されるため、大規模エンタープライズ導入に適していません。WLC でキャッシュできる PMK エントリは、クライアントあたり最大 8 台の AP に限られます。クライアントが 8 台を超える AP 間をローミングすると、新しく作成されたエントリを保存するために古いキャッシュ エントリが削除されます。
- 高速ローミングはローミング時の 802.1X または PSK の認証を回避することによって実施されます。高速ローミングは次の場合に限り実現されます。
  - クライアントはそれまでに関連付けされたことのある AP にローミングします。
  - AP および WLC にはこのクライアント用の PMK キャッシュ エントリがあります。つまり、このキャッシュ エントリは一連のローミングによって削除されていません。
- モビリティ ドメインの WLC をまたがっては機能しません。WLC ではモビリティ ピアと PMK を交換しません。
- FlexConnect 導入ではサポートされていません。

Proactive Key Caching

事前認証とも呼ばれる Proactive Key Caching（PKC）は、802.11i のセキュリティの改定の一環として IEEE 802.11 標準によって推奨された、第 2 の高速セキュア ローミング方式です。PKC は Autonomous AP を使用した導入を目的としていましたが、CUWN で効率良く機能するように改変されました（詳細は後述）。

PKC は、実装の目的を反映して、ローミングに先だって、WPA2 802.1X クライアントによるネイバー AP との 802.1X 認証や EAP 認証が可能です。WPA2 クライアントでは現在の AP に接続されている間に 802.1X 認証を実行できます。事前認証は、現在の AP によって実施され、EAPOL パケットがネイバー AP に中継されて、ここで RADIUS サーバへのクエリが行われ、PMK がキャッシュされます。ネイバー AP の選択方法を判別する検出メカニズムがなかったことが、事前認証の大きな課題になっています。その結果、最初のクライアント関連付けは、システムに存在する AP と同じ数の RADIUS 認証と PMK に至ることがありました。

CUWN では、クライアントの PMK を中央でキャッシュおよび管理することにより、インテリジェントで効率的な実装を実現します。この仕組みが機能するためには、AP が共通の管理統制下にあって、PMK をキャッシュして WLAN システム内のすべての AP に配布する中央集中型デバイスが配置されている必要があります。CUWN では、WLC が制御下のすべての CAPWAP AP 用にこの作業を実行し、モビリティ メッセージングを使用してモビリティ グループ内の他の WLC 間で PMK を交換します。キャッシュされたクライアントの PMK はクライアント セッションの存続中使用されます。

この高速セキュア ローミング方式では、クライアントおよび WLC によってキャッシュされた元の PMK を再利用するため、ローミング時に 802.1X 認証および EAP 認証が回避されます。クライアントでは、新しい暗号化キーを取得するために実行する必要があるのは WPA2 フォーウェイ ハンドシェイクのみです。

- ワイヤレス クライアントが特定の AP に接続するたびに、クライアント MAC アドレス、AP MAC アドレス（WLAN の BSSID）、およびこの AP によって取得された PMK に基づいて PMKID がハッシュされます。PKC ではすべての AP および特定のクライアント用に同じ元の PMK をキャッシュするため、クライアントが別の AP にローミングする場合、新しい PMKID をハッシュするうえで変更される値は新しい AP MAC アドレスのみです。

- クライアントが新しい AP へのローミングを開始して再アソシエーション要求フレームを送信するとき、キャッシュされた PMK を高速セキュア ローミングに使用したことを AP に伝達する必要がある場合、クライアントは WPA2 RSN 情報要素に PMKID を追加します。クライアントは、ローミング先の BSSID（AP）の MAC アドレスをすでにわかっているため、この再アソシエーション要求で使用されている新しい PMKID をハッシュするだけになります。クライアントからこの要求を受信すると、AP は、すでに保持している値（キャッシュした PMK、クライアント MAC アドレス、およびそれ自体の AP MAC アドレス）を使用して PMKID のハッシュも行い、PMKID が一致したことを確認する正常再アソシエーション応答によって応答します。新しい暗号化キーを取得するための WPA2 フォーウェイ ハンドシェイクを開始するシードとして、キャッシュした PMK を使用できるため、EAP 認証フェーズが回避されます。

概要：

- シスコのマニュアルでは Proactive Key Caching（PKC）と呼ばれていますが、802.11i の改定の一環として定義されている内容と同じ実装ではありません。
- WPA2 WLAN では、802.1X キー管理を使用してデフォルトで有効化されています。
- 高速ローミングはローミング時の 802.1X 認証および EAP 認証を回避することによって実施されます。
- 中央集中型導入用にサポートされています。
- 拡張に対応しているため、大規模エンタープライズ導入に適しています。
- 単一モビリティ ドメイン内の WLC をまたがって機能します。
- FlexConnect 導入ではサポートされていません。

Opportunistic Key Caching

WLAN ベンダー各社は Opportunistic Key Caching（OKC）という語と Proactive Key Caching（PKC）という語を互換的に使用していますが、両者は同一ではありません。この 2 方式の主な違いは、OKC は IEEE 802.11 で規定されていないため、標準ではない点です。OKC は、PMK の管理と AP 間での配布の方法についても PKC とは動作が異なります。

前述したように、PKC（事前認証）には、クライアントを事前認証しているネイバー AP を判別するメカニズムがなかったという大きな制限事項がありました。単一の WPA2 クライアント接続が、システム内の AP 数と同数の RADIUS 認証および PMK に至ることがありました。

ベンダー各社は、規定されているモビリティ ゾーン内のすべての AP にクライアントの最初の PMK を配布することにより、こういった効率の悪さを OKC によって解消しようとしました。クライアントは接続時に 802.1X 認証または EAP 認証と、フォーウェイ ハンドシェイクを実行し、クライアントの接続先のゾーンにあるすべての AP に取得した PMK を配布します。その結果、クライアントは各ネイバー AP で RADIUS 認証を実行する必要なくネイバー AP で事前認証されます。高速ローミングは、モビリティ ゾーン内の別の AP にクライアントがローミングするときに、802.1X および EAP の交換を回避することで実施されます。

OKC の主な欠点は、モビリティ ゾーン内の AP に PMK を配布する方法にあります。Datagram Transport Layer Security（DTLS）などのメカニズムを使用して AP の管理および制御プロトコルを保護していない場合、PMK の配布は保護されていません。

CUWN では、FlexConnect 導入用に 802.1X キー管理を使用して WPA2 WLAN 上で OKC がデフォルトでサポートされています。FlexConnect 導入では、FlexConnect グループに PMK を配布する AP がモビリティ ゾーンによって定義されます。クライアントが正常に認証されると、FlexConnect グループ内のすべての AP に WLC によって PMK が配布されます。シスコの CAPWAP 実装は DTLS を使用して保護されているため、PMK キーの配布が保護されています。

PMK の配布は WLC によって管理されているため、すべての FlexConnect AP が接続モードである必要があります。サイトにある FlexConnect AP がスタンドアロン モードに遷移した場合、高速セキュア ローミングは既存のクライアントに対してのみ提供可能です。

概要:

- Opportunistic Key Caching（OKC）という語は Proactive Key Caching（PKC）という語と互換的に使用されていますが、両者は同一ではありません。
- IEEE 802.11 標準として規定されていません。
- FlexConnect 導入用に 802.1X キー管理を使用して WPA2 WLAN でデフォルトで有効化されています。
- 高速ローミングはローミング時の 802.1X 認証および EAP 認証を回避することによって実施されます。
- FlexConnect のみでサポートされています（ローカルまたは中央でスイッチング）。
- PMK を最初に生成する時点で、FlexConnect AP が接続モードである必要があります。
- 同じ WLC に関連付けられている同じ FlexConnect グループ内の AP をまたがって機能します。

802.11r を使用した高速セキュア ローミング

802.11r（802.11 標準による正式名称は Fast BSS Transition、別名 FT）は、AP 間の高速遷移を実行するためのソリューションとして IEEE によって正式に承認された、最初の高速セキュア ローミング方式です。802.11r の改定は 2008 年に正式に承認されており、WLAN 上でキーを処理およびキャッシングするためのキー階層を明確に定義しています。

このテクニックの説明は他の方式と比べて複雑になっています。これは、新しい概念と、別々のデバイスにキャッシュされる PMK の複数階層（各デバイスが別々のロールを持つ）が導入されており、高速セキュア ローミングのためのオプションが増えているためです。そこで、この方式と、選択可能なオプションごとの実装方法について概要を説明します。

- ハンドシェイク メッセージング（PMKID、ANonce、SNonce 交換など）は再アソシエーション フレームではなく、802.11 の認証フレームまたはアクション フレームで行われます。PMKID キャッシング方式とは異なり、アソシエーション（または再アソシエーション）メッセージ交換の後で実行される個別のフォーウェイ ハンドシェイク フェーズは回避されます。新しい AP とのキー ハンドシェイクは、この新しい AP にクライアントが完全にローミングまたは再関連付けする前に開始されます。
- 高速ローミング ハンドシェイクの方式は、Over-the-Air と Over-the-DS（分散システム）の 2 方式が提供されています。
- 802.11r ではキー階層の層が増えています。
- このプロトコルでは、クライアントがローミングするときのキー管理用のフォーウェイ ハンドシェイクを回避しているため（このハンドシェイクを必要としないで新しい暗号化キーの PTK および GTK を生成）、802.1X または EAP を認証に使用する場合に限らず、PSK を使用する WPA2 セットアップにも適用できます。これにより、これらのセットアップでのローミングがさらに高速化されます。EAP およびフォーウェイ ハンドシェイクの交換は発生しません。

802.11r では、最初の AP への接続が確立されるときにワイヤレス クライアントが WLAN インフラストラクチャに対する最初の認証を 1 回だけ実行し、同じ FT モビリティ ドメインにある AP 間でのローミング時には高速セキュア ローミングを実行します。同じ SSID（別名 Extended Service Set（ESS））を使用する AP は同じ FT キーを処理します。AP で FT モビリティ ドメイン キーを処理する方法は、PKC および OKC と同じです。CUWN では、WLC が制御下のすべての CAPWAP AP 用にこの作業を実行し、モビリティ メッセージングを使用してモビリティ グループ内の他の WLC ピア間で FT キーを交換します。

次にキー階層の概要を示します。

- MSK は引き続き、最初の 802.1X および EAP の認証フェーズからクライアント サプリカントおよび RADIUS サーバ上で取得されます（認証成功時に RADIUS サーバから WLC に転送）。この MSK は、FT キー階層のシードとして使用されます。EAP 認証方式ではなく WPA2-PSK を使用する場合は、PSK が MSK です。
- ペアワイズ マスター キー R0（PMK-R0）は、FT キー階層の第 1 レベルのキーである MSK から取得されます。この PMK-R0 のキーを保持しているのは WLC およびクライアントです。
- ペアワイズ マスター キー R1（PMK-R1）という第 2 レベルのキーは PMK-R0 から取得されます。このキーを保持しているのは、クライアントと、PMK-R0 を保持している WLC によって管理されている AP です。
- FT キー階層の最後のレベルである第 3 レベルのキーは PTK です。これは、802.11 ユニキャスト データ フレームを暗号化するために使用される最後のキーです（WPA/TKIP または WPA2/AES を使用する他の方式と同様）。この PTK は FT で PMK-R1 から取得され、キーを保持しているのはクライアントと、この WLC によって管理されている AP です。

802.11r は、デフォルトで、中央集中型導入と FlexConnect 導入（中央またはローカルでスイッチング）の両方でサポートされています。FlexConnect を採用するためには中央集中型の WLAN 認証にする必要があります。802.11r はローカル認証を使用している FlexConnect AP やスタンドアロン モードで動作している FlexConnect AP ではサポートされません。所定の 802.11r ローミング ドメインに含まれている FlexConnect AP は、同じ FlexConnect グループに属している必要があります。

概要：

1. PSK または 802.1X キー管理を使用している WPA2 WLAN でのみサポートされています。
2. 高速ローミングはローミング時に 802.1X 認証および EAP 認証とフォーウェイ ハンドシェイクを回避することによって実施されます。
3. 中央集中型導入と FlexConnect（中央とローカルでスイッチング）導入の両方でサポートされています。
   a. 中央集中型：同じモビリティ グループ内の WLC をまたがって機能します。
   b. FlexConnect：同じ FlexConnect グループ内の AP をまたがって機能します。
4. FlexConnect を使用するには、WLAN が中央集中型認証用に設定されている必要があります。ローカル認証はサポートされません。高速セキュア ローミングはスタンドアロン モードで動作している FlexConnect AP ではサポートされていません。

（注）　IEEE 802.11r およびその他の 802.11 修正の詳細については、802.11r Fast Transition ローミングを参照してください。

考慮事項

高速セキュア ローミング方式を WLAN で選択する場合に検討する必要のある複数の考慮事項を次に示します。

- 高速セキュア ローミング方式は、セキュリティが有効化されている WPA2 WLAN 上の AP 間をクライアントが移動するときのローミング プロセスを高速化するために開発された方式であるという点を理解することが重要です。WLAN セキュリティを設定していない場合は、802.1X 認証、EAP 認証、フォーウェイ ハンドシェイクのいずれもなく、これらを回避することでローミングを高速化できません。
- 802.11r は、WPA2-PSK をサポートしている唯一の高速セキュア ローミング方式です。802.11r は、フォーウェイ ハンドシェイクを回避して WPA2-PSK ローミング イベントを高速化します。
- WLAN がローカル認証用に設定されている場合は、いずれの高速セキュア ローミング方式も FlexConnect 導入で機能しません。ローカル認証が有効化されている場合、クライアントはローミング時に完全な認証を実行することになります。
- すべての高速セキュア ローミング方式に長所と短所がありますが、最終的には、実装しようとしている特定の方式がワイヤレス クライアント ステーションでサポートされていることを確認する必要があります。特定の WLAN/SSID に接続するワイヤレス クライアントによってサポートされている最良の方式を選択する必要があります。たとえば、導入によっては、シスコ ワイヤレス IP フォン（CCKM を使用する WPA2/AES はサポートし、802.11r はサポートしない）用に CCKM を使用する WLAN を作成してから、802.11r をサポートしているワイヤレス クライアント用に 802.11r/FT を介して WPA2/AES を使用する（またはサポートされていれば OKC/PKC を使用する）別の WLAN を作成できます。
- 使用可能ないずれの高速セキュア ローミング方式もサポートしない 802.1X クライアントの場合は、AP 間のローミング時に常に遅延が発生します。この 802.1X クライアントは、ローミング イベントの際に、802.1X または EAP の認証とフォーウェイ ハンドシェイク全体を実行する必要があります。この結果、アプリケーションおよびサービスに中断が発生するおそれがあります。
- 別の WLC によって管理される AP 間では、WLC が同じモビリティ グループに属している限り、すべての高速セキュア ローミング方式（PMKID/SKC を除く）がサポートされます（コントローラ間ローミング）。

Adaptive 11r

802.11r 対応 WLAN は、ワイヤレス クライアント デバイスのローミングを高速化します。ローミング エクスペリエンスを向上させるためには、Apple iOS デバイスを 11r 対応 WLAN に接続できるようにすることをお勧めします。ただし、WLAN で 11r を有効にすると、FT AKM のビーコンおよびプローブ応答を認識しないレガシー デバイスを WLAN に接続できなくなります。何らかの方法で、クライアント デバイスの機能を識別して 11r 対応デバイスを FT 対応デバイスとして WLAN に接続可能にし、同時に、レガシー デバイスを 11i/WPA2 デバイスとして接続できるようにする必要があります。Cisco WLC ソフトウェア リリース 8.3 は、802.11i 対応 WLAN 上の 802.11r を Apple デバイスに対して選択的に有効化することができます . 対応する Apple デバイスはこの機能を識別し、WLAN で FT アソシエーションを行います。シスコ ワイヤレス インフラストラクチャでは、非 FT WLAN で FT アソシエーションをネゴシエートできるデバイスから、WLAN 上で FT アソシエーションを行うことが、可能になります。

さらに、AireOS コード 8.3 が動作している WLC では、SSID 上で 802.11k および 11v 機能がデフォルトで有効になります。これらの機能により、ローミングすべきタイミングとネイバー AP に関する情報がクライアントに通知され、ローミングが必要な時にスキャニングして時間を無駄にすることがなくなるので、クライアントのローミング状況の改善に役立ちます。Apple デバイスはデュアルバンドをサポートするため、802.11k ネイバー リストは、[1] に適応してデュアルバンドで更新されます。

シスコのインフラストラクチャ側では、シスコの AP がビーコンとプローブで Adaptive 802.11r のサポートをアドバタイズし、Over-the-DS FT 機能が設定されます。

クライアント側では、iOS 10 以降を実行する Apple デバイスが IE 上で Adaptive 11r 機能サポートを検索します。capability bit が設定されている場合は、機能ビットが AKM（dot1x または PSK）を検索し、それに応じて FT dot1x または FT PSK を使用します。Apple デバイスは、FT をサポートする IE をアソシエーション要求で送信します。それにはベンダー固有の OUI も含まれます。

Cisco WLAN は、アソシエーション要求を処理し、アソシエーション応答で 802.11r サポートに応答して FT アソシエーションを許可します。フォーウェイ ハンドシェイクには FT アソシエーションが含まれています。

この機能は、ローカル モードおよび FlexConnect モードの AP、すべての 802.11n および 802.11ac Wave 1 AP、Wave2 AP 用の AireOS コード リリース 8.3[2] 以降および 8.3.11.0 でサポートされます。

WLC でのブロードキャストおよびマルチキャスト

この項では、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 2-34 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、ワイヤレス 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。AP と同じ有線 VLAN 上に別の AP がある場合、それらも、有線ブロードキャスト パケットをワイヤレス インターフェイスに転送します。

1. 最適な WiFi 接続ソリューションをサポートしている Apple デバイスは次のとおりです。

iPhone 6s 以降

iPhone 6s Plus 以降

iPad Air 2 以降

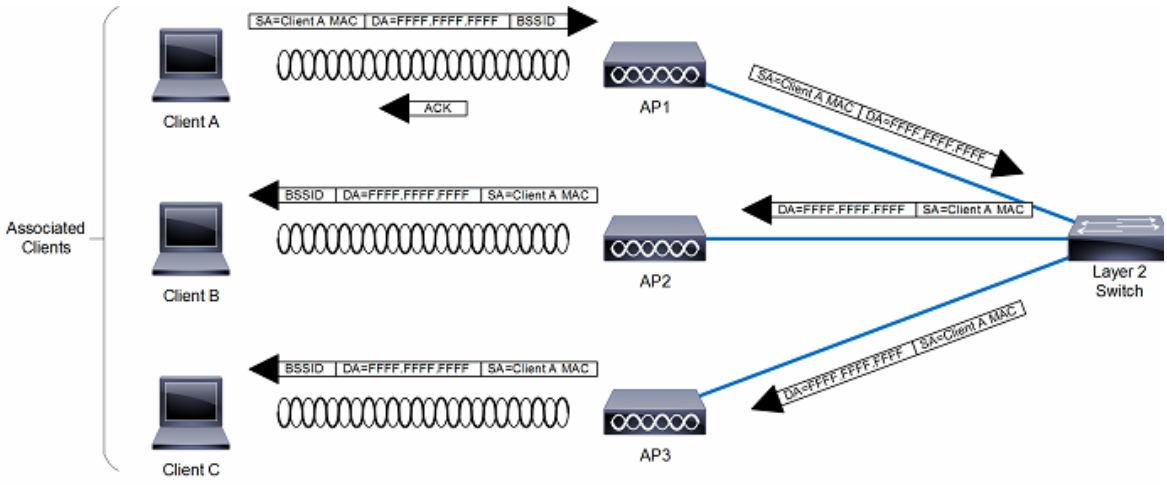
iPad mini 4 以降

iPad Pro 以降

iPhone SE

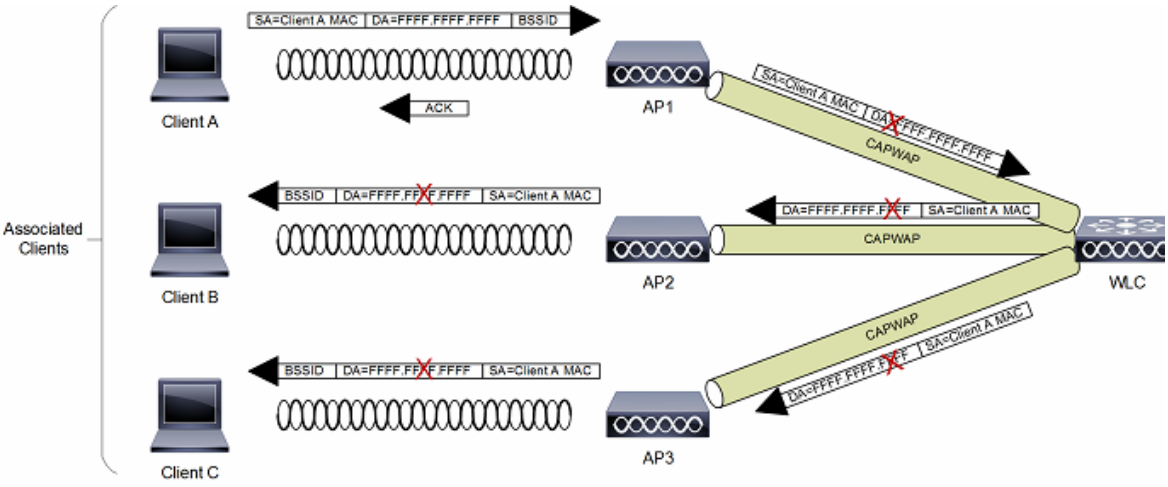
2. AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、ハイパーロケーション モジュール、3602P、AP3700 シリーズ アクセス ポイント + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、AP1040/1140/1260 シリーズ アクセス ポイント。

図 2-34　802.11 ブロードキャスト/マルチキャストの動作



WLC の CAPWAP スプリット MAC 方式では、図 2-35 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 WLC 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。

図 2-35　WLC ブロードキャストのデフォルトの動作



(注)　どのような状況で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。

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データ 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。これによって、関連付けされているすべてのワイヤレス デバイスで、ブロードキャストまたはマルチキャストの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 からその他のワイヤレス 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取得する（DHCP）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、関連付けされている 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 に関連付けされます。DHCP リレー要求は、指定された動的インターフェイスの送信元 IP アドレスを使用して、この動的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、有線およびワイヤレス 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。

この方式により、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 スプーフィングやサービス妨害（DoS）攻撃を軽減できるようになります。

VideoStream

VideoStream 機能では、無線でブロードキャスト フレームをユニキャスト ストリームに変換することで、IP マルチキャスト ストリームの無線配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。VideoStream はすべての Cisco AP でサポートされています。

次に、コントローラ上で VideoStream を設定するための推奨ガイドラインを示します。

- AP1100 および AP1200 は信頼できるマルチキャスト機能をサポートしていません。
- マルチキャスト機能が有効であることを確認します。ベスト プラクティスとして、コントローラ上の IP マルチキャストは multicast-multicast モードで設定することをお勧めします。
- クライアント デバイス上の IP アドレスを確認します。デバイスには、それぞれの VLAN の IP アドレスが必要です。
- AP にコントローラが接続されていることを確認します。
- クライアントが 802.11a/n/ac の速度で設定された WLAN に関連付けられることを確認します。

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 は、デフォルトでワイヤレス 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「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明示的に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。Cisco Unified Wireless Network ソリューションでは、データ リンク層とネットワーク層のマルチキャスト 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能力は WLC にはありません。したがって、次の手順の追加を考慮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、リンク層のマルチキャスト 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 Wireless Network 導入の設計における主な考慮事項は、WLC のロケーションと AP および WLC の接続です。この項では、中央集中型（ローカル モード）AP 導入に関するトピックについて簡単にまとめ、標準的な推奨事項について適宜説明します。FlexConnect AP 展開における推奨事項と設計上の考慮事項については、この項では扱いません。代わりに第 7 章「FlexConnect」で説明します。

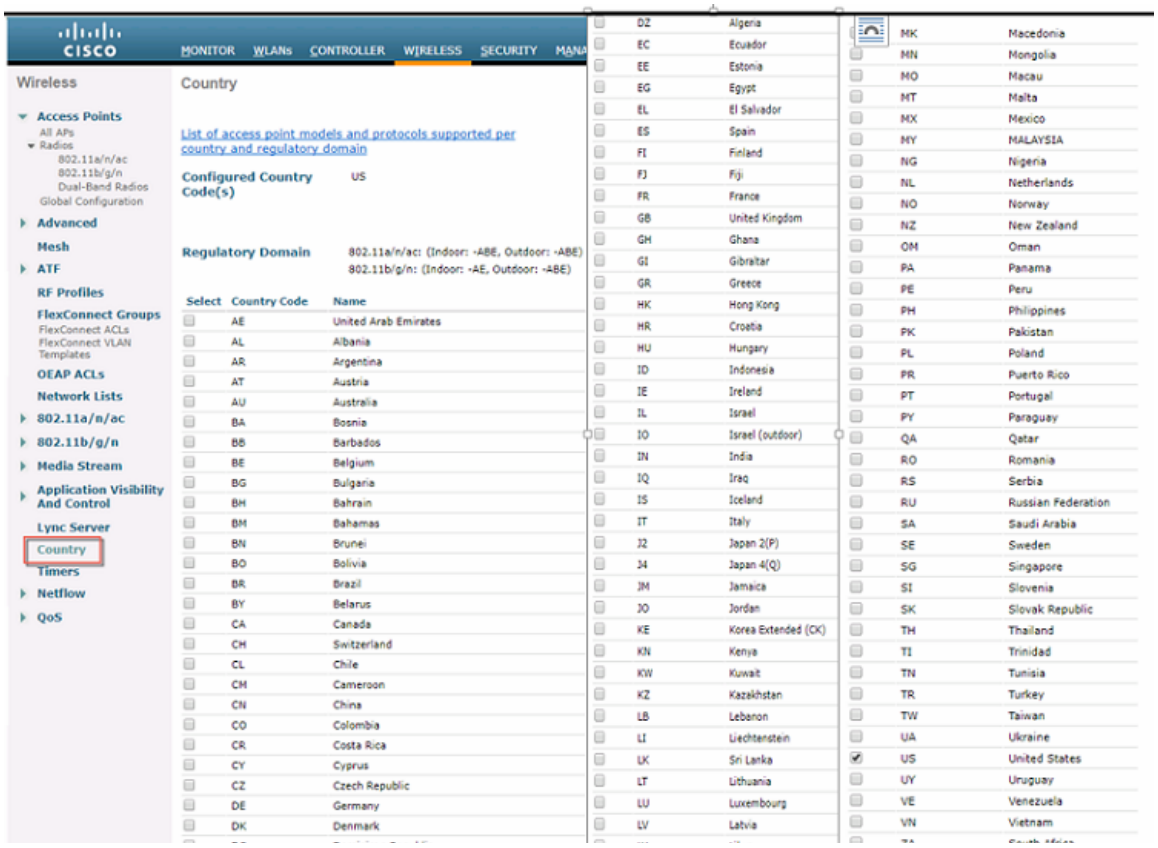
WLC のロケーション

Cisco Unified Wireless Network では、導入の規模と種類に応じて、WLC を中央に配置することも、キャンパス内に分散させることもできます。さまざまな展開タイプと考慮事項については、以下の項で説明します。

分散型の WLC 導入

8.2 より前のリリースでは、WLC で 20 カ国しかサポートされませんでした。リリース 8.2 以降の WLC では、さまざまな地域固有の AP による分散コントローラ構成と同時国サポートが 110 カ国を対象にサポートされます。

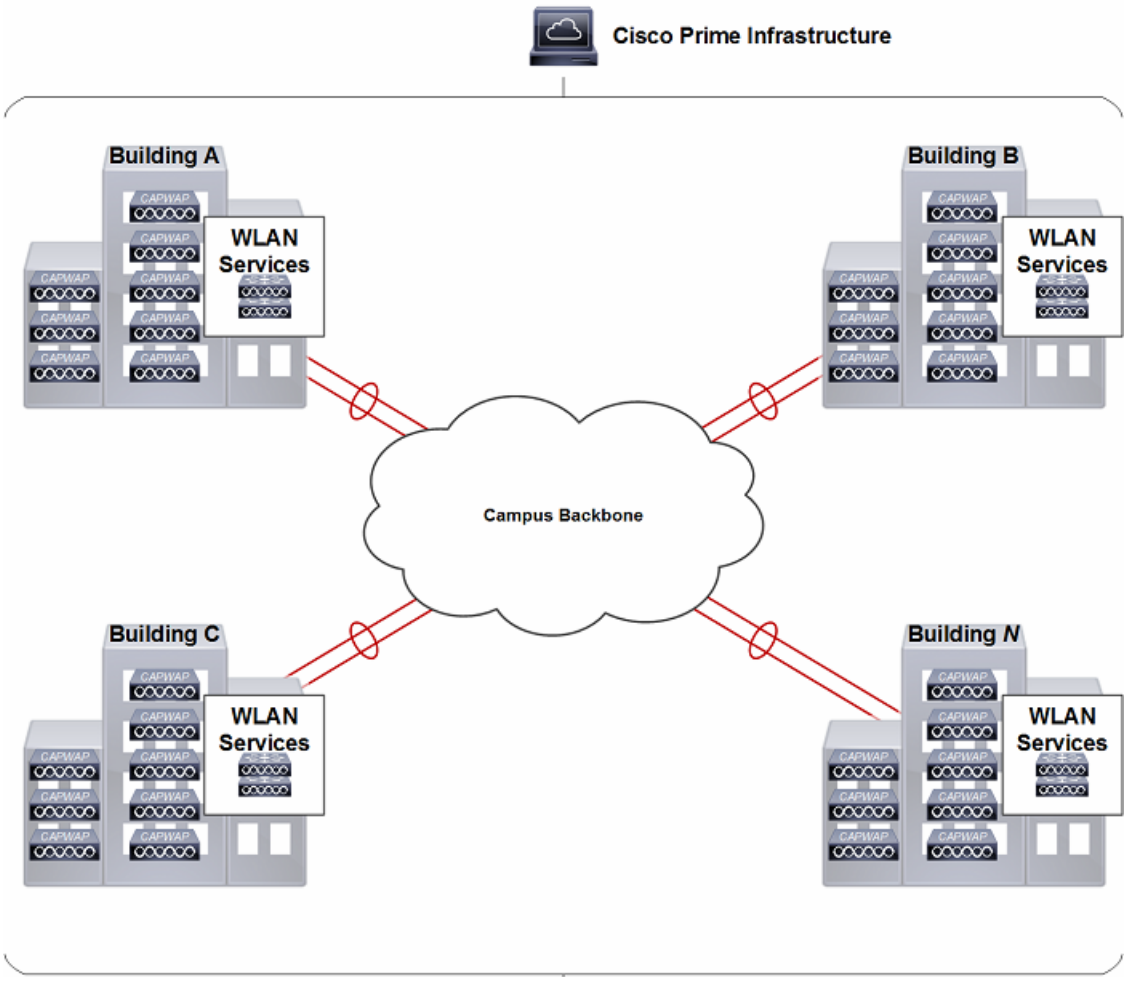
http://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html#wp9005314



分散型の WLC 展開

図 2-36 は分散型の WLC 展開を示しています。このモデルでは、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、各ビルディング内のディストリビューション レイヤ スイッチが使用されます。このシナリオでは、AP と WLC の間の CAPWAP トンネルは各ビルディング内にとどまります。

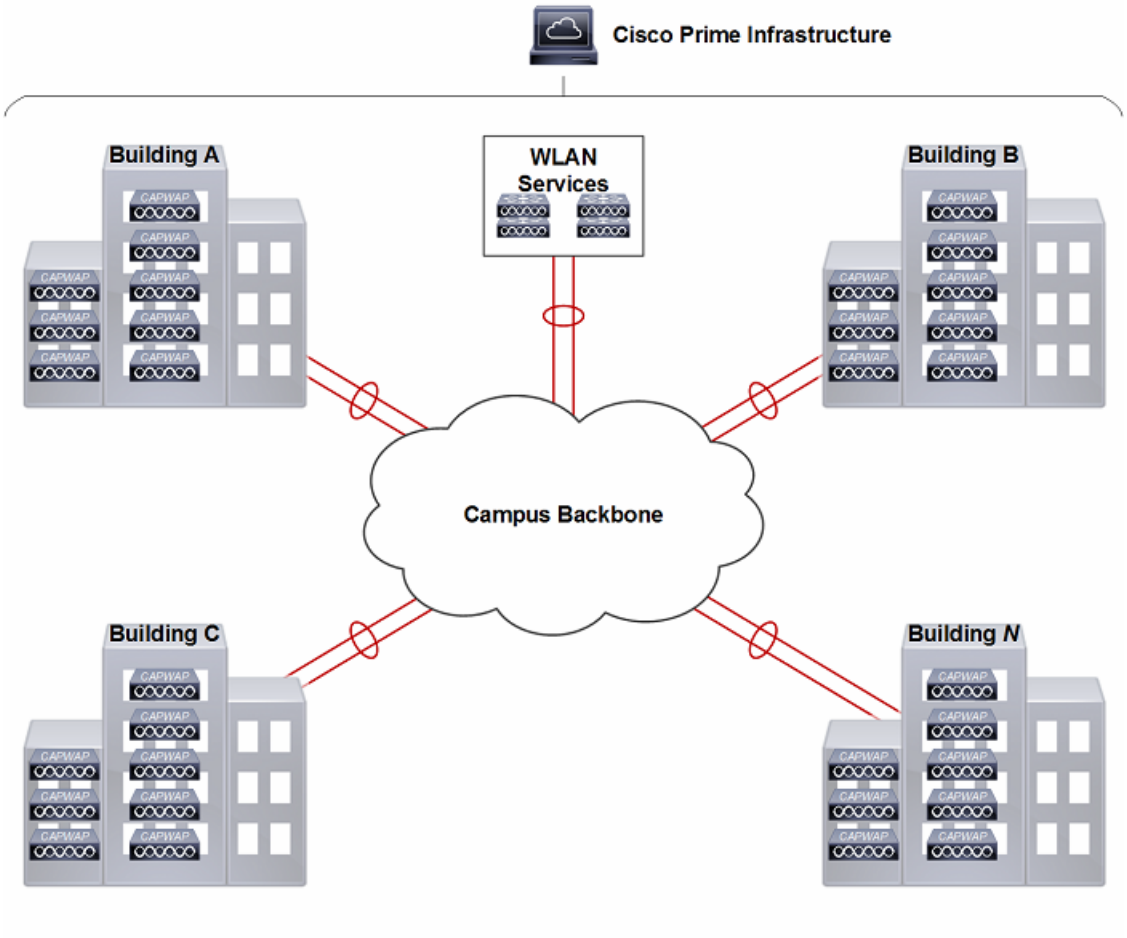
図 2-36　　分散型の FWLC 導入



中央集中型の WLC 導入

図 2-37 は中央集中型の WLC 展開を示しています。このモデルでは、WLC はキャンパス ネットワークの集中化された場所に配置されます。この導入モデルでは、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 CAPWAP トンネルが必要です。下図の例では、中央集中型の WLC が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。中央集中型の WLC のプールは専用スイッチ ブロック経由でキャンパス コアに接続されます。キャンパス コアは、通常、データセンターと同じビルディングにあります。データセンター内と WLC プールでは、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 2-37　　キャンパス内の中央集中型 WLC



リファレンス アーキテクチャ

WLC の配置に関するシスコの推奨事項は、Cisco Unified Wireless Network 導入の規模と拡張によって異なります。次の項では、それぞれシスコの階層型設計の方針に基づく小規模、中規模、大規模、およびきわめて大規模なキャンパス ネットワークの推奨される WLC 配置と冗長構成によるリファレンス アーキテクチャについて説明します。ローカルモード AP を使用するリモート ブランチ オフィス導入のリファレンス アーキテクチャも、この項の終わりに示してあります。

（注）　Cisco Validated Design およびベスト プラクティスの詳細については、http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html を参照してください

小規模キャンパス

図 2-38 は、コラスプト コアとして動作するディストリビューション レイヤを実装する小規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。ディストリビューション レイヤは、WLC、WAN、およびインターネット エッジへの接続を提供します。WLC は LAN の規模に応じてディストリビューション レイヤに直接接続することも、専用スイッチ ブロックを介して接続することもできます（図を参照）。この例の小規模キャンパスは、複数台のアクセス レイヤ スイッチを配置した単一のビルディングです。

図 2-38　　小規模キャンパスのリファレンス設計

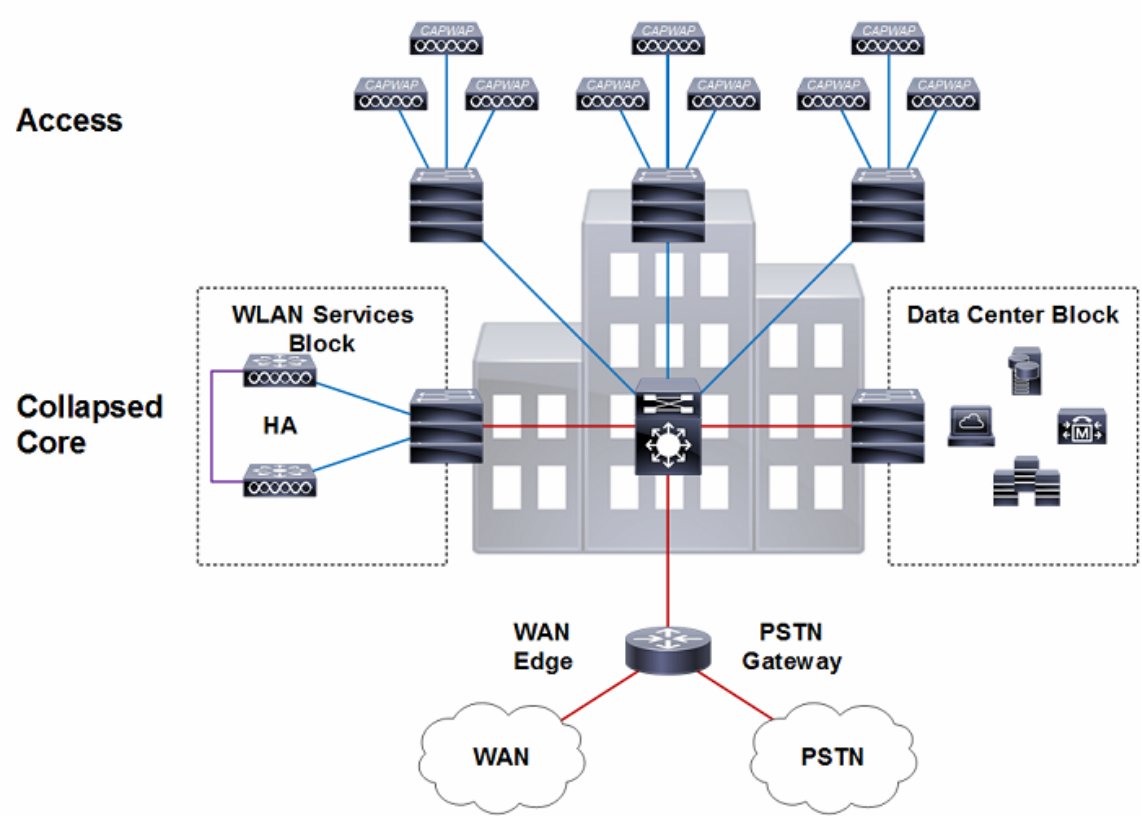
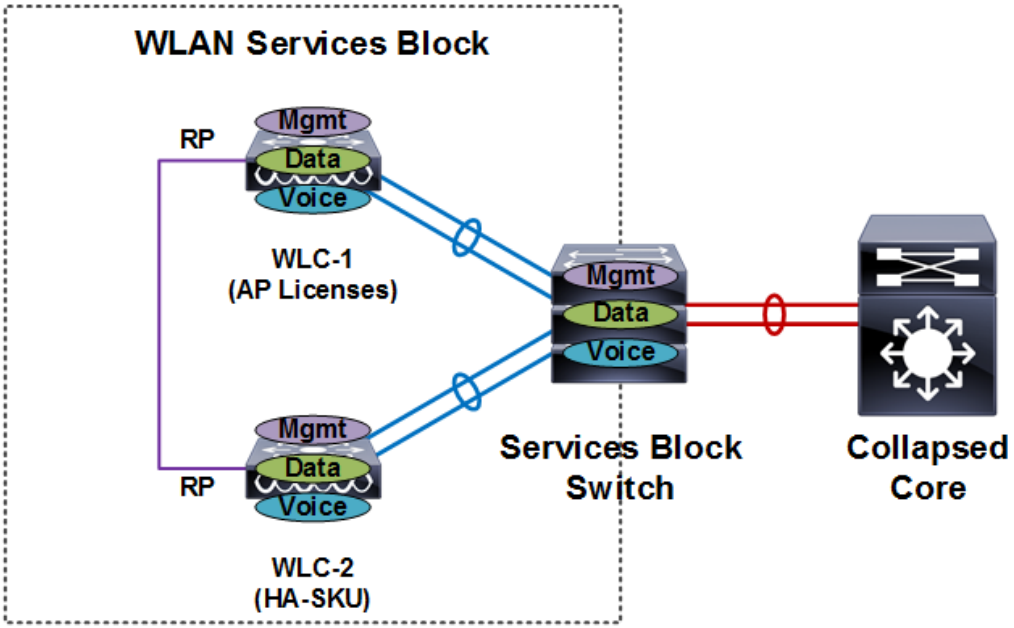


図 2-39 は、小規模キャンパス ネットワーク導入用のワイヤレス サービス ブロックの詳細を示します。この例では、ディストリビューション レイヤに接続する専用サービス スイッチ ブロック（Catalyst シャーシ、つまり復元力のあるスタック）に WLC のペアが接続されています。このサービス スイッチ ブロックはサービス専用にすることも、データセンターとサービス ブロックの両方に接続することもできます。このスイッチ ブロックはルート集約用に EIGRP または OSPF を実装しているレイヤ 3 リンクを使用してディストリビューション レイヤに接続されています。この例の WLC は中央集中型であると見なされます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してサービス スイッチ ブロックに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とサービス スイッチ ブロックの間でいずれも 802.1Q タギングされています。このサービス スイッチ ブロックは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

図 2-39　小規模キャンパスとワイヤレス サービス ブロックの詳細



小規模キャンパス導入では Cisco 5508 または Cisco 5520 WLC のペアを HA-SSO 用に設定することをお勧めします。選択する WLC モデルは、サイトで必要とされる具体的なスループットによって決まることになります。両方の WLC が同じ物理データセンターにあるため、両方の WLC 用の冗長ポートは直接接続されています。AP は HA-SSO ペアをプライマリ WLC として使用するように設定されています。アクティブとスタンバイホットの WLC 間ですべての構成が自動的に同期されます。

中規模キャンパス

図 2-40 は、専用のディストリビューション レイヤを実装する中規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。大規模なネットワーク用に専用ディストリビューション レイヤを導入するメリットは詳しく文書化され、理解されています。このアーキテクチャの WLC は、専用スイッチ ブロックを介してコア レイヤに直接接続しています。この例の中規模キャンパスは、それぞれ複数のアクセス レイヤ スイッチが配置されている複数のフロアのある単一のビルディングです。

図 2-40　　キャンパス WLC 導入の詳細

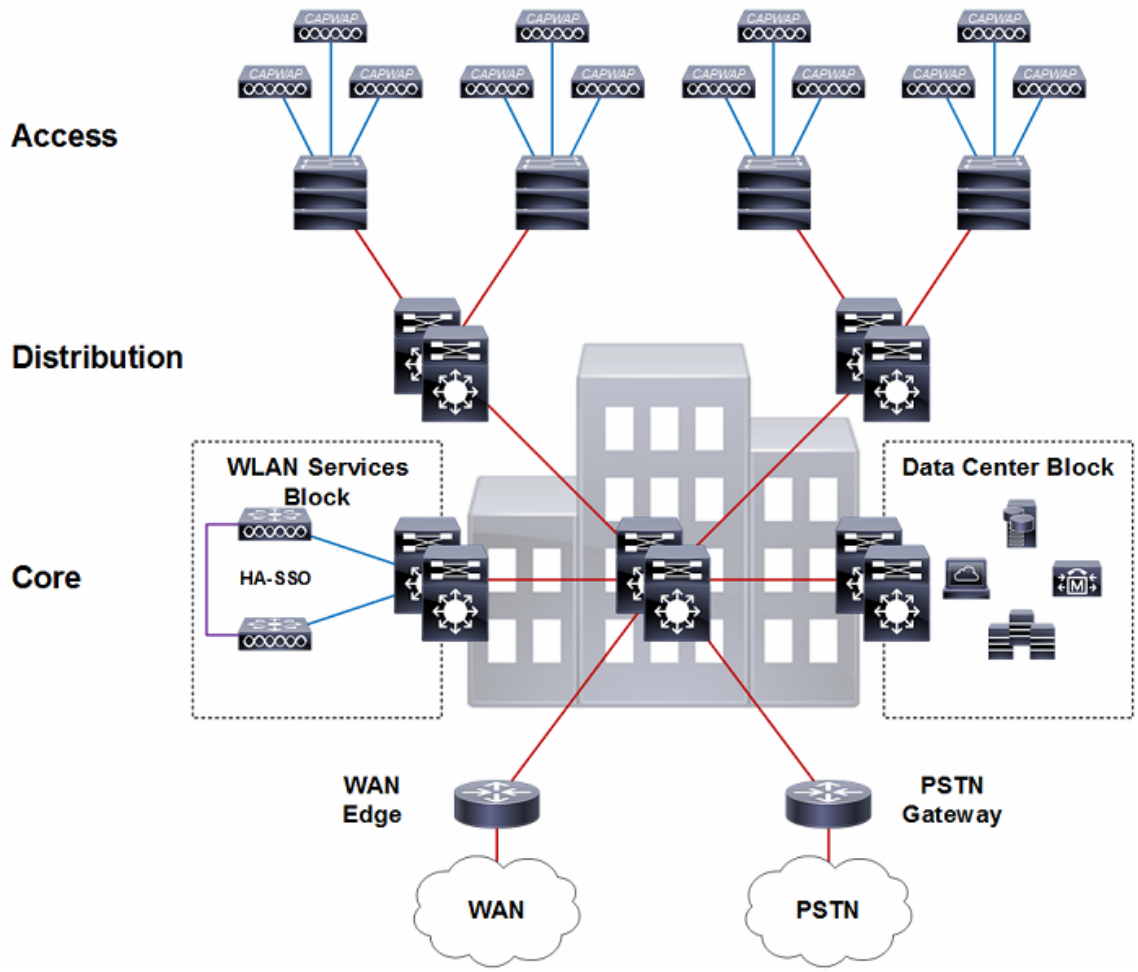
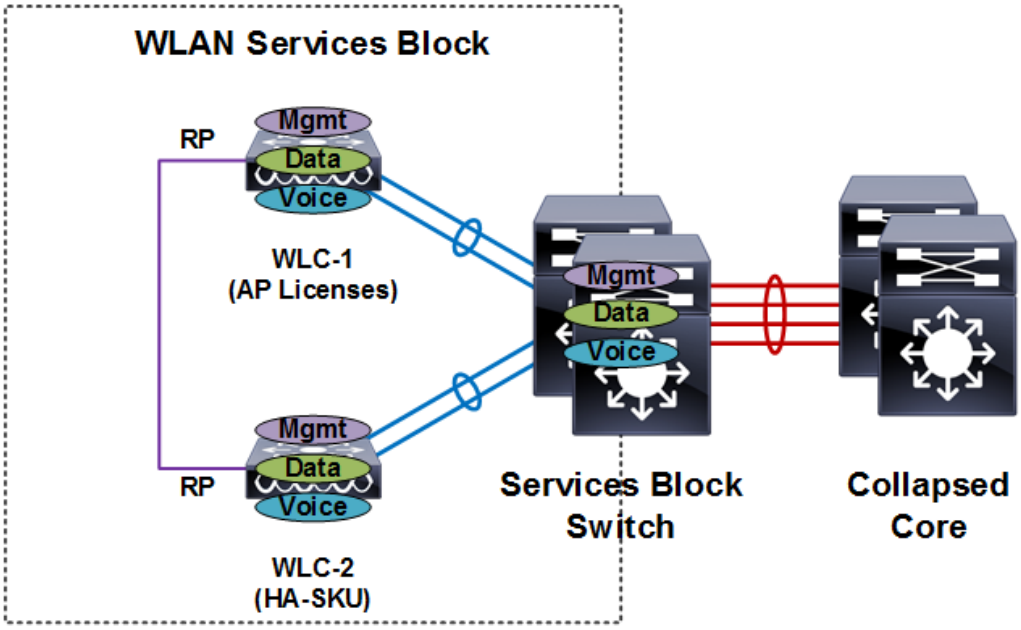


図 2-41 は、中規模キャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、コア レイヤに接続する専用サービス スイッチ ブロックに WLC のペアが接続されています。このサービス スイッチ ブロックはマルチレイヤまたは VSS 用に設定されている Catalyst スイッチのペアです。このサービス スイッチ ブロックはルート集約用に EIGRP または OSPF を実装しているレイヤ 3 リンクを使用してコア レイヤに接続されています。この例の WLC は中央集中型であると見なされます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してサービス スイッチ ブロックに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とサービス スイッチ ブロックの間でいずれも 802.1Q タギングされています。このサービス スイッチ ブロックは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

図 2-41　　中規模キャンパスとワイヤレス サービス ブロックの詳細



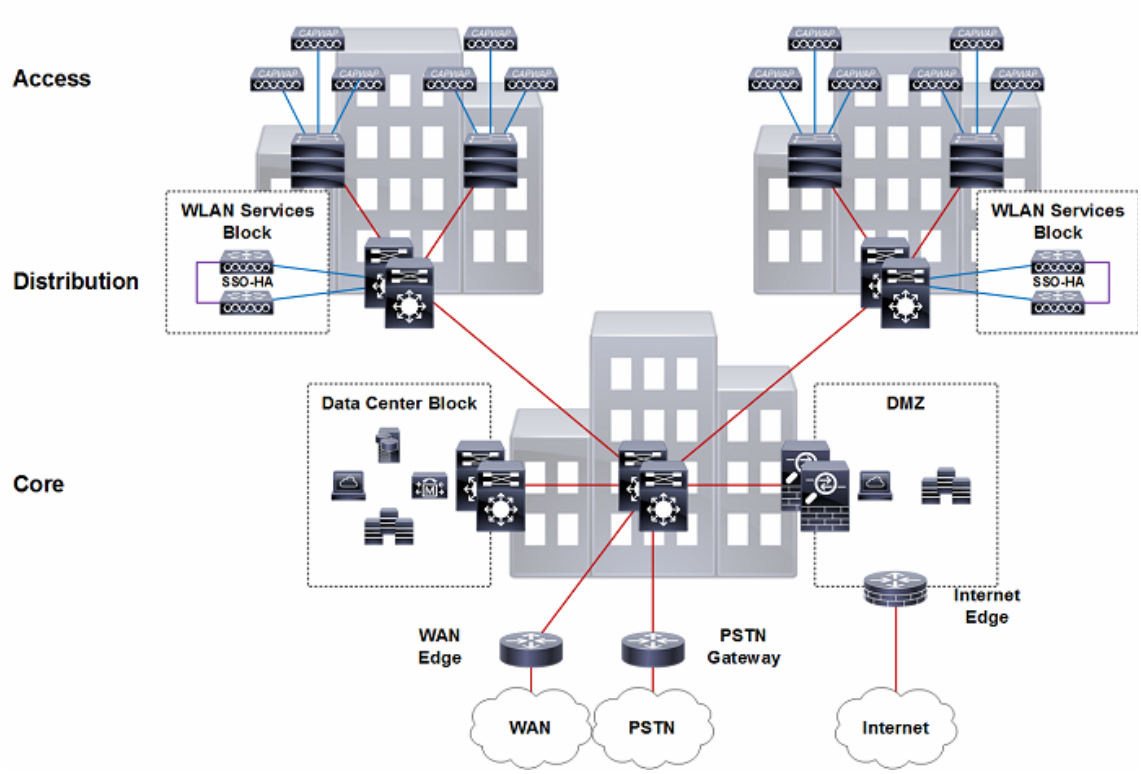
中規模キャンパス展開では、HA-SSO 用に設定された Cisco 3504、Cisco 5508、または Cisco 5520 WLCのペアを使用することを推奨します。選択する WLC モデルは、サイトで必要とされる具体的なスループットによって決まることになります。両方の WLC が同じ物理データセンターにあるため、両方の WLC 用の冗長ポートは直接接続されています。AP は HA-SSO ペアをプライマリ WLC として使用するように設定されています。アクティブとスタンバイホットの WLC 間ですべての構成が自動的に同期されます。

大規模キャンパス

図 2-42 は、キャンパス コアに接続される複数のビルディングで構成される大規模キャンパス ネットワークの CUWN 展開で推奨される WLC 配置を示しています。このアーキテクチャの WLC はビルディング間で分散されており、WLC の各ペアが所定のビルディングにある AP を管理します。このアーキテクチャの WLC は各ビルディング内でディストリビューション レイヤに直接接続されています。

WLC の複数のペアがキャンパス全体に分散されているため、各 WLC は同じモビリティ グループのメンバーとして割り当てられて、ローミングするクライアントにキャンパス全体でシームレスなモビリティを提供します。各ビルディングの WLC には、所定の各ビルディングのディストリビューション レイヤで終端されている異なるワイヤレス管理 VLAN およびユーザ VLAN が割り当てられています。モビリティ トンネルは、キャンパス コアを通じて外部 WLC とアンカー WLC の間でローミング ユーザのトラフィックを転送するために使用されます。

図 2-42　大規模キャンパスのリファレンス設計



WLC をビルディング間に分散させると、1 つの CUWN によってサポートされるワイヤレス クライアントの数が増えるため、拡張性に関する複数の長所があります。ワイヤレス ネットワークに追加されるデバイスが増えるほど、サービス ブロック スイッチによって処理および保守されるレイヤ 2 およびレイヤ 3 のテーブル エントリの数が指数関数的に増えます。この結果、サービス ブロック スイッチで CPU 負荷が高くなります。

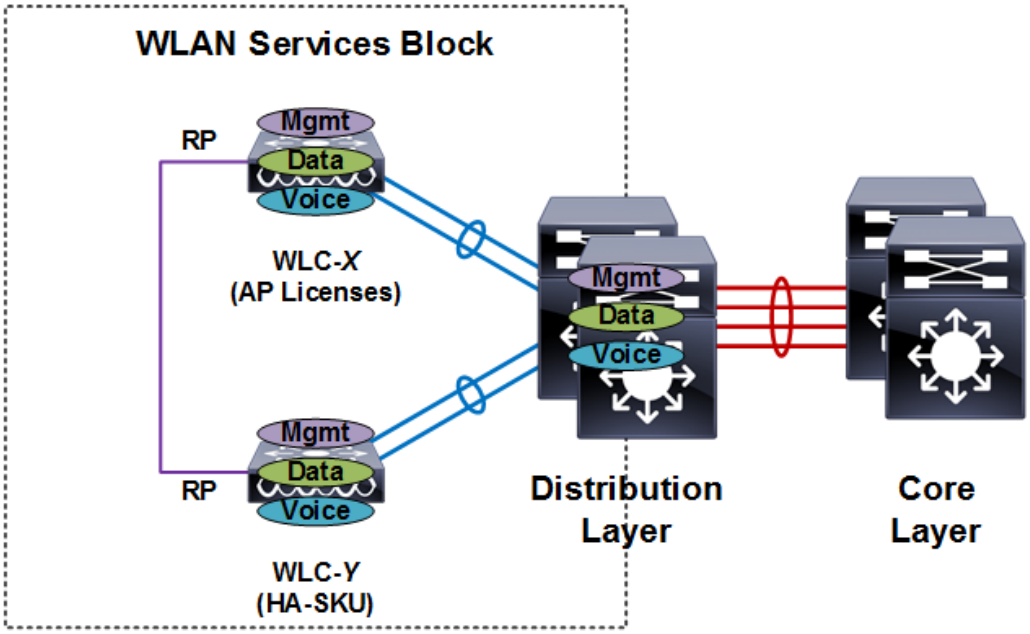
この考慮事項が重要であるのはなぜでしょう。現行世代の WLC は、最大 6,000 台の AP と 64,000 台のクライアントをサポートするように拡張できます。純然たる IPv4 環境では、この結果、サービス ブロック スイッチで処理および保守するエントリが 128,000 個に及ぶことがあります。大部分のワイヤレス クライアントはデュアルスタックもサポートしているため、処理と保守の対象となるエントリの数がさらに増えます。

ベスト プラクティスとして、25,000 台以上のワイヤレス クライアントをサポートしている大規模キャンパス導入では WLC を分散させることをお勧めします。WLC を分散させると、MAC、ARP、および ND の処理およびテーブル メンテナンスがディストリビューション レイヤ スイッチ間に展開されて、CPU の負荷が低下します。このアーキテクチャでは、ディストリビューション レイヤ障害の際に影響を受けたディストリビューション レイヤが学習し直す必要があるのはエントリのサブセットのみであるためコンバージェンスも高速です。サポートしているクライアントが 25,000 台未満のキャンパス導入の場合は、専用スイッチ ブロックを介して WLC がコアに接続されている中央集中型 WLC アーキテクチャを利用できます（「中規模キャンパス」を参照）。

図 2-43 は、大規模キャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、各ビルディング内のディストリビューション レイヤ スイッチに WLC の各ペアが接続されています。ディストリビューション レイヤ スイッチは、レイヤ 3 リンクを使用してコア レイヤに接続している、マルチレイヤまたは VSS として設定された Catalyst スイッチです。EIGRP または OSPF がルート集約に使用されます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用してディストリビューション スイッチに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC とディストリビューション スイッチの間でいずれも 802.1Q タギングされています。このディストリビューション スイッチは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

図 2-43　大規模キャンパスとワイヤレス サービス ブロックの詳細



大規模キャンパス導入では、各ディストリビューション レイヤ内の Cisco 5520 または 8540 WLC のペアを HA-SSO 用に設定することをお勧めします。ビルディングごとに選択する WLC モデルは、各ビルディングで必要な AP の数とスループットによって決まります。ディストリビューション レイヤ スイッチの物理的な場所に応じて、両方の WLC の冗長ポートを直接接続することも専用レイヤ 2 VLAN 越しに拡張することもできます。

各ビルディング内の AP はローカル HA-SSO ペアをプライマリ WLC として使用するように設定されています。異なるビルディングの HA-SSO ペアをセカンダリ WLC として設定して N+1 冗長性を使用することで追加の冗長性が実現されます。必要な WLAN、AP グループ、および RF グループはプライマリとセカンダリの両方の HA-SSO ペアに定義されています。

(注)　ディストリビューション レイヤ スイッチの構成要件は、マルチレイヤと VSS のいずれとして設定されているかに応じて異なります。実装ごとの要件の詳細については、この章のハイ アベイラビリティ (2-42 ページ)を参照してください。

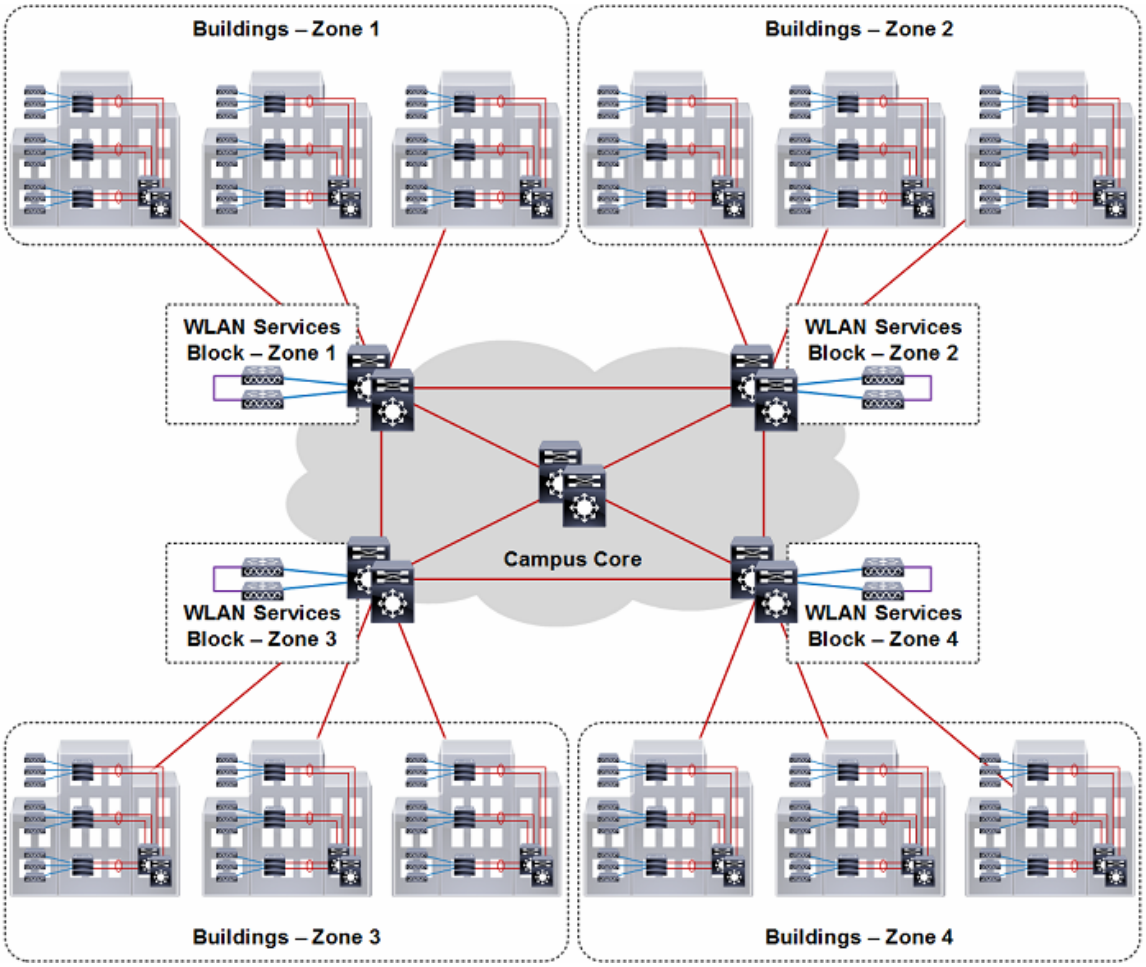
きわめて大規模なキャンパス

図 2-44 に、分散されたコア レイヤに接続している数百棟のビルディングをサポートしているきわめて大規模なキャンパス ネットワーク用の CUWN 導入に推奨される WLC の配置を示します。分散された各コア スイッチはキャンパス コア内でディストリビューション レイヤとして機能しています。キャンパス内の大規模ビルディングは独自のディストリビューション レイヤおよびアクセス レイヤを実装する一方で、小規模ビルディングはアクセス レイヤのみを実装します。

このアーキテクチャの WLC は、コア レイヤ スイッチ間で配分されて、ここで WLC の各ペアがビルディングのグループの AP を管理します。各ワイヤレス サービス ブロックは最大 6,000 台の AP、25,000 台のクライアント、および 40 Gbps のスループットをサポートできます。各ワイヤレス サービス ブロック内の WLC には、ビルディングの各グループを処理している分散スイッチまたはコア レイヤ スイッチで終端されている異なるワイヤレス管理 VLAN およびユーザ VLAN が割り当てられています。必要なワイヤレス サービス ブロックの数は、サポートする必要のあるワイヤレス デバイスの数に基づいて決定されます。

図 2-44 のキャンパス ネットワークの例では、4 つの個別ワイヤレス サービス ブロックを実装しており、各ブロックは特定のゾーンに配置されているビルディングのグループをサポートしています。この CUWN 設計は最大 24,000 台の AP と 100,000 台のクライアントをサポートするように容易に拡大できます。

図 2-44　　きわめて大規模なキャンパスのリファレンス設計



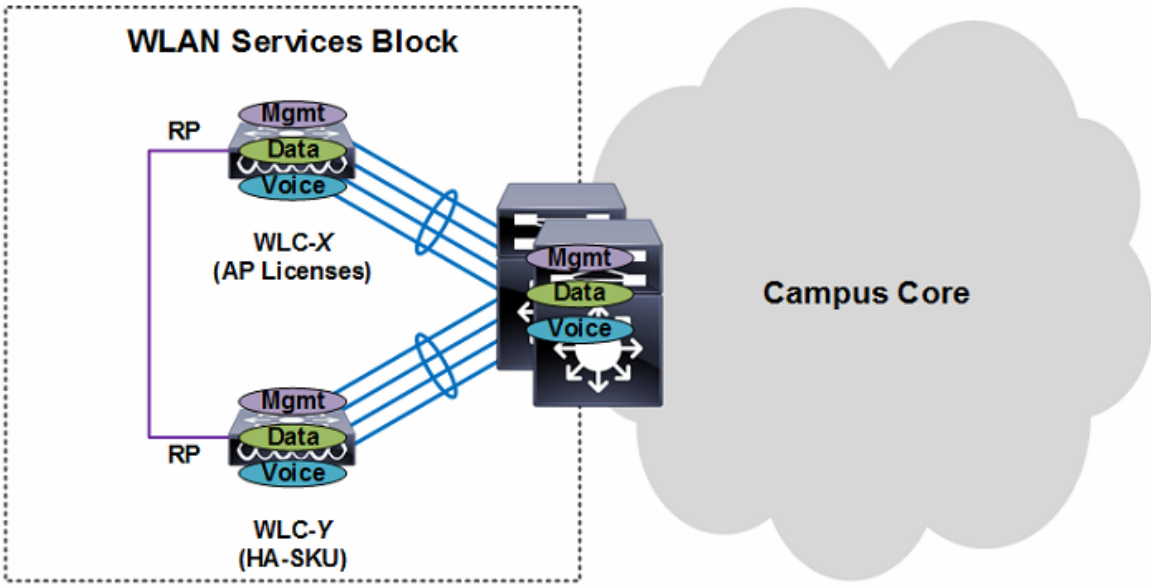
きわめて大規模なキャンパス用のモビリティ グループの設計も重要な考慮事項であり、ビルディングとゾーンの間に実現されているワイヤレス カバレッジによって異なります。理想に従って各ゾーンにビルディングが配置されており、ワイヤレス カバレッジ エリアを表しています。

- 各ゾーン内およびゾーン間に連続的なワイヤレス カバレッジが実現されている場合、定義するモビリティ グループは単一にすることができます。WLC の各ペアは同じモビリティ グループのメンバーとして設定されます。ワイヤレス クライアントは、元のネットワーク メンバーシップを維持しながらキャンパス全体でシームレスにローミングできます。
- 連続的なワイヤレス カバレッジが各ゾーン内でのみ実現されている場合は、個別のモビリティ グループを導入する必要があります。WLC の各ペアには個別のモビリティ グループを設定します。ワイヤレス クライアントはゾーン内でネットワーク メンバーシップを維持でき、別のゾーンにある AP に接続するときは新しいネットワークが割り当てられます。
- 連続的なワイヤレス カバレッジが一部のゾーン間で実現されている場合は、該当するゾーンを処理している WLC を同一のモビリティ グループに割り当てることができます。ワイヤレス クライアントは該当ゾーン内でネットワーク メンバーシップを維持でき、別のゾーンにある AP に接続するときは新しいネットワークが割り当てられます。

図 2-45 は、きわめて大規模なキャンパス導入用のワイヤレス サービス ブロックの詳細を示します。この例では、WLC の各ペアは、各ビルディング グループを処理するディストリビューションおよびコア レイヤ スイッチに接続されています。このディストリビューション スイッチまたはコア レイヤ スイッチは、レイヤ 3 リンクを使用して相互接続されている、マルチレイヤまたは VSS として設定されている Catalyst スイッチです。EIGRP、OSPF、または BGP がルート集約に使用されます。

WLC は、802.1Q VLAN タギング用に設定されたスタティック ポートチャネルを使用して分散コア スイッチに接続します。ワイヤレス管理、データ、および音声の VLAN は、WLC と分散スイッチまたはコア スイッチの間でいずれも 802.1Q タギングされています。このディストリビューションまたはコア スイッチは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

図 2-45　きわめて大規模なキャンパスとワイヤレス サービス ブロックの詳細



きわめて大規模なキャンパス導入では、各ディストリビューション レイヤ内の Cisco 8540 WLC のペアを HA-SSO 用に設定することをお勧めします。ディストリビューション レイヤ スイッチの物理的な場所に応じて、両方の WLC の冗長ポートを直接接続することも専用レイヤ 2 VLAN 越しに拡張することもできます。

各ゾーン内の AP は指定された HA-SSO ペアをプライマリ WLC として使用するように設定されています。異なるゾーンの HA-SSO ペアをセカンダリ WLC として設定して N+1 冗長性を使用することで追加の冗長性が実現されます。必要な WLAN、AP グループ、および RF グループはプライマリとセカンダリの両方の HA-SSO ペアに定義されています。

(注)　ディストリビューション レイヤ スイッチの構成要件は、マルチレイヤと VSS のいずれとして設定されているかに応じて異なります。実装ごとの要件の詳細については、この章のハイ アベイラビリティ (2-42 ページ)を参照してください。

ブランチ

Cisco Unified Wireless Network では、ワイドエリア ネットワーク (WAN) 越しに接続されているリモート ブランチ オフィスをサポートする 2 種類のアーキテクチャを提供しています。ブランチ サイトのネットワーク管理者は、ローカル モードまたは FlexConnect モードで動作する AP を実装できます。2 種類の CUWN アーキテクチャは動作が異なり、解決するビジネス ニーズも異なります。この項では、ローカル モード AP 導入に限って詳細を説明します。FlexConnect AP 導入の詳細および推奨事項については、第 7 章「FlexConnect」を参照してください。

ローカル モード AP を実装するブランチ サイトは、WLC がブランチ内に直接配置される小規模キャンパス アーキテクチャに従います。すべての CAPWAP トンネルはブランチ内にあります。ローカル モード AP を配置した複数のブランチ サイトが導入されている場合は、WAN によって接続された 1 か所以上のブランチに WLC が導入されているため、分散アーキテクチャであると見なされます。

図 2-46 は、コラスプト コアとして動作するディストリビューション レイヤを実装する小規模ブランチ ネットワークの CUWN 展開で推奨される WLC 配置を示しています。ディストリビューション レイヤは、WLC、WAN、およびインターネット エッジへの接続を提供します。WLC はブランチの規模に応じてディストリビューション レイヤに直接接続することも (図を参照)、専用スイッチ ブロックを介して接続することもできます。この例のブランチ ネットワークは、ディストリビューション レイヤ 1 つ、アクセス レイヤ スイッチ 2 台の単一のビルディングです。

図 2-46　　小規模ブランチのリファレンス設計

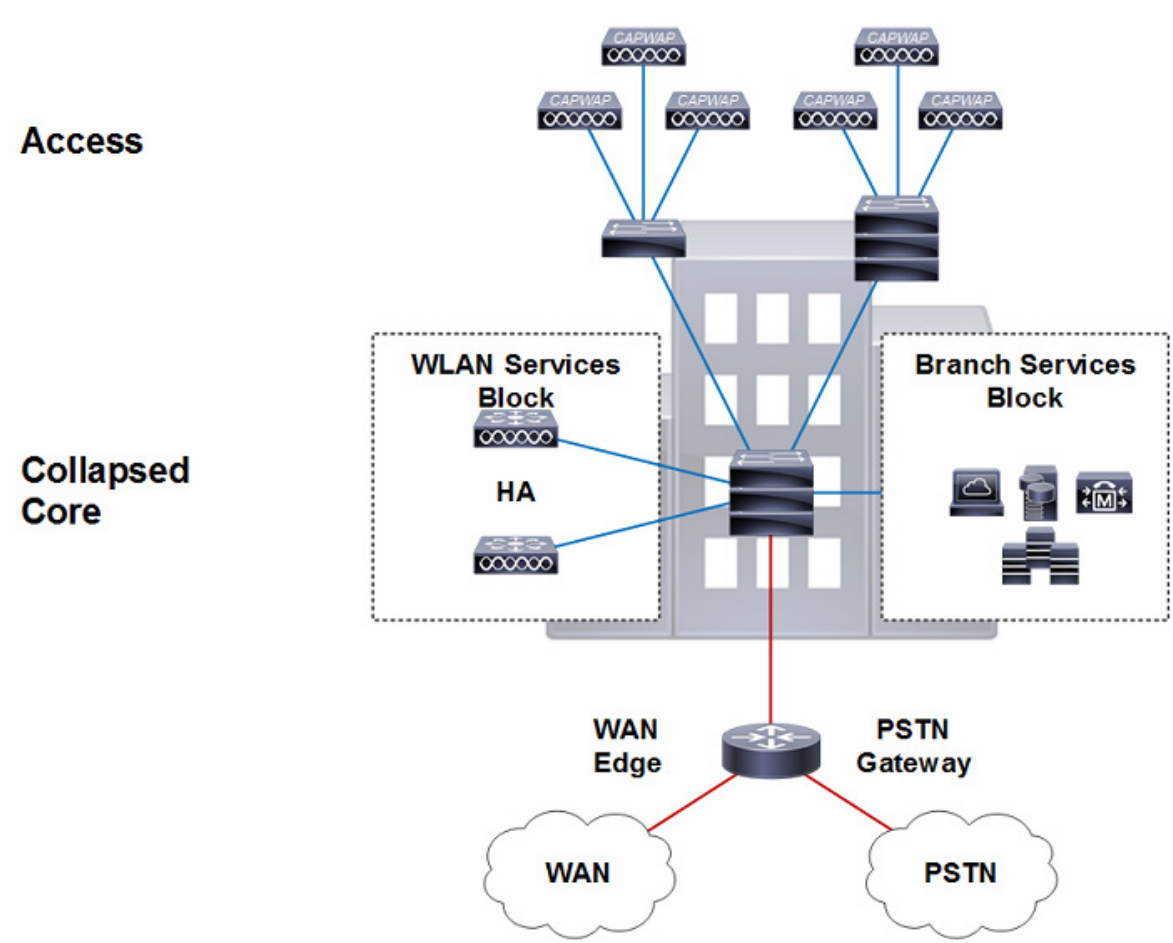
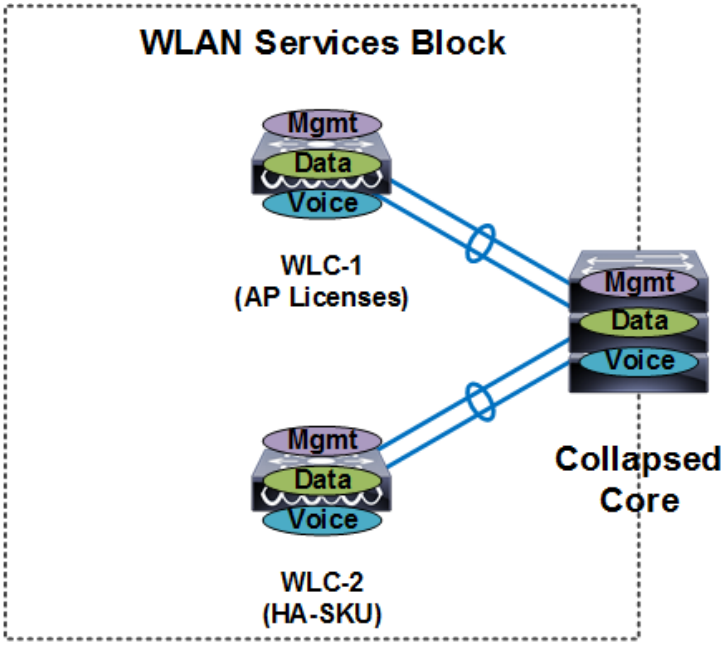


図 2-47 は、ブランチ ネットワーク導入用のワイヤレス サービス ブロックの詳細を示します。この例では、802.1Q VLAN タギング用に設定されているスタティック ポートチャネルを使用して WLC のペアがディストリビューション レイヤに直接接続されています。ワイヤレス管理、データ、および音声の VLAN は、WLC とディストリビューション レイヤの間でいずれも 802.1Q タギングされています。このディストリビューション レイヤは、ワイヤレス VLAN ごとのファーストホップ ユニキャストおよびマルチキャスト ルーティングを提供します。

図 2-47　　小規模ブランチとワイヤレス サービス ブロックの詳細



ブランチ オフィスでの導入では、Cisco 2504 WLC のペアを N+1 HA 用に設定することをお勧めします。Cisco 2504 WLC は、ブランチ オフィスでの導入専用に設計されており、最大 75 台の AP をサポートするように拡張できます。両方の WLC に同じモビリティ グループが設定および割り当てられており、同じインターフェイスまたはインターフェイス グループ、WLAN、AP グループ、および RF グループをサポートするように設定されています。AP は、永続ライセンスを持つ WLC をプライマリ WLC、HA-SKU WLC をセカンダリ WLC として使用するように設定されています。

(注)　シスコでは、ワイドエリア ネットワーク越しに中央集中型 WLC を使用するローカル モード AP の導入をサポートしていません。WAN 越しにリモート AP をサポートする必要がある場合は、FlexConnect アーキテクチャを実装することをお勧めします。

トラフィック負荷と有線ネットワークのパフォーマンス

Cisco Unified Wireless Network ソリューションを導入する場合に、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 CAPWAP トラフィックの影響または負荷。
- ユニファイド ワイヤレス導入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、分散型の WLC 導入と中央集中型の WLC 導入の相対的なメリット。

ネットワークのトラフィック ボリューム全体に対して CAPWAP 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。

- CAPWAP コントロール トラフィックのボリューム
- トンネリングによって生じるオーバーヘッド
- トラフィック処理

CAPWAP コントロール トラフィックのボリューム

CAPWAP 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。たとえば、通常ソフトウェアのアップグレード中や WLC の再起動中は多くなります。しかし、トラフィックの調査では、CAPWAP 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 0.35 Kbps 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、中央集中型導入モデルと分散型導入モデル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

CAPWAP 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。一般的な企業で見られる平均パケット サイズが約 300 バイト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、中央集中型導入モデルと分散型導入モデル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

中央集中型の WLC にトンネルされた WLAN トラフィックはすべて、WLC のロケーションからネットワークでの最終宛先までルーティングされます。トンネルの距離と WLC のロケーションによっては、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 トポロジや分散型の WLC 導入の場合、クライアント トラフィックはエッジからネットワークに入り、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、中央集中型の導入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宛先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る量であり、中央集中型導入モデルと分散型導入モデル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 トラフィックのボリュームに深刻な影響が出ることはありません。

AP 接続

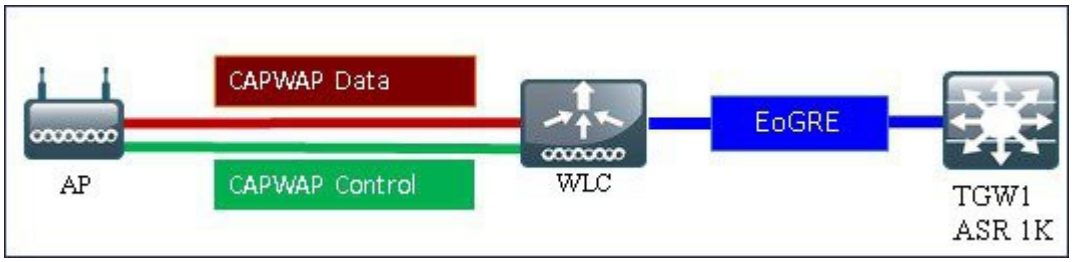
AP は、エンド ユーザ（802.11 クライアント）とは別のサブネット上になければなりません。これは、インフラストラクチャ管理インターフェイスはエンド ユーザとは別のサブネット上にあるべきであると定義している一般的なベスト プラクティスのガイドラインと一致しています。さらに、Catalyst Integrated Security Features（CISF）を CAPWAP AP スイッチ ポートで有効にして、WLAN インフラストラクチャの保護を強化することを推奨します（FlexConnect AP 接続については、第 7 章「FlexConnect」を参照）。

導入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式としては、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 内で WLAN QoS 機能を効率的に提供するには、CAPWAP 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。

WLC EoGRE トンネリング

Ethernet over GRE（EoGRE）は、ホット スポットからの Wi-Fi トラフィックを集約するための新しい集約ソリューションです。このソリューションでは、顧客宅内機器（CPE）デバイスで、エンド ホストから届いたイーサネット トラフィックをブリッジし、そのトラフィックを IP GRE トンネルでイーサネット パケットにカプセル化できます。IP GRE トンネルがサービス プロバイダーのブロードバンド ネットワーク ゲートウェイで終端すると、エンド ホストのトラフィックが終了し、エンド ホストに対するサブスクライバ セッションが開始されます。



トンネリングの一般的なメリット

- クライアントは、さまざまなテクノロジーやベンダーが混在するアクセス ネットワーク上で IP アドレスとポリシーを維持できます。
- WLC に接続する L2 スイッチでの MAC アドレスのスケーリング制限を回避できます。
- 合法的傍受（LI）。

EoGRE トンネリングが携帯電話事業者にもたらすメリット：

- 3G および 4G トラフィックをオフロードして OpEx の削減とネットワーク効率の向上を実現することによってネットワークの輻輳を軽減します。
- 弱いセル信号がなくても 3G および 4G コアへのアクセスを提供し、サブスクライバの維持に寄与します。
- 高密度のメトロ環境においてユーザ ベースまたは帯域幅ベースの CapEx を削減します。

EoGRE トンネリングが有線および Wi-Fi 事業者にもたらすメリット:

- WiFi セキュリティとサブスクライバ制御を提供します。
- スケーラブルで管理しやすく安全なワイヤレス接続を提供します。
- 新しい収益分配ビジネス モデルを実現します。
- 新しいロケーションベースのサービスを提供する WiFi プラットフォームを提供します。

EoGRE トンネリングがサブスクライバにもたらすメリット:

- WiFi ネットワーク上のサブスクライバに高品質のエクスペリエンスを提供します。
- アクセス ネットワーク全体にわたって統一された方法で課金します。
- 3G または 4G から WiFi、WiFi から WiFi などの無線アクセス テクノロジーをまたがるモビリティを提供します。
- Wi-Fi プラットフォーム内で複数のオプションを提供し、ロケーションベースのサービスを実現します。
- リリース 8.2 以降では、EoGRE トンネリングはダイナミック インターフェイスでサポートされます。
- ダイナミックな IPv6 AP 管理インターフェイスはサポートされていません。
- リリース 8.3 では、IPv6 ダイナミック インターフェイスはトンネル インターフェイスとしてのみサポートされます。
- リリース 8.3 では、IPv6 アドレスを割り当てることができるダイナミック インターフェイスの最大数は 16 です。
- リリース 8.3 の TGW では、IPv4 と IPv6 の両方のアドレス形式がサポートされます。最大で 10 個のトンネル ゲートウェイを作成できます。
- リリース 8.4 では、WLC およびフレックス接続 AP から TGW への EoGRE IPv4 および IPv 6 トンネルがサポートされます。
- リリース 8.5 では、プライマリおよびセカンダリ TGW のフェールオーバーと冗長性のサポートが追加されました。
- リリース 8.5 では、EoGRE トンネルを管理するための SNMP MIB が追加されています。

サポートされるコントローラと AP

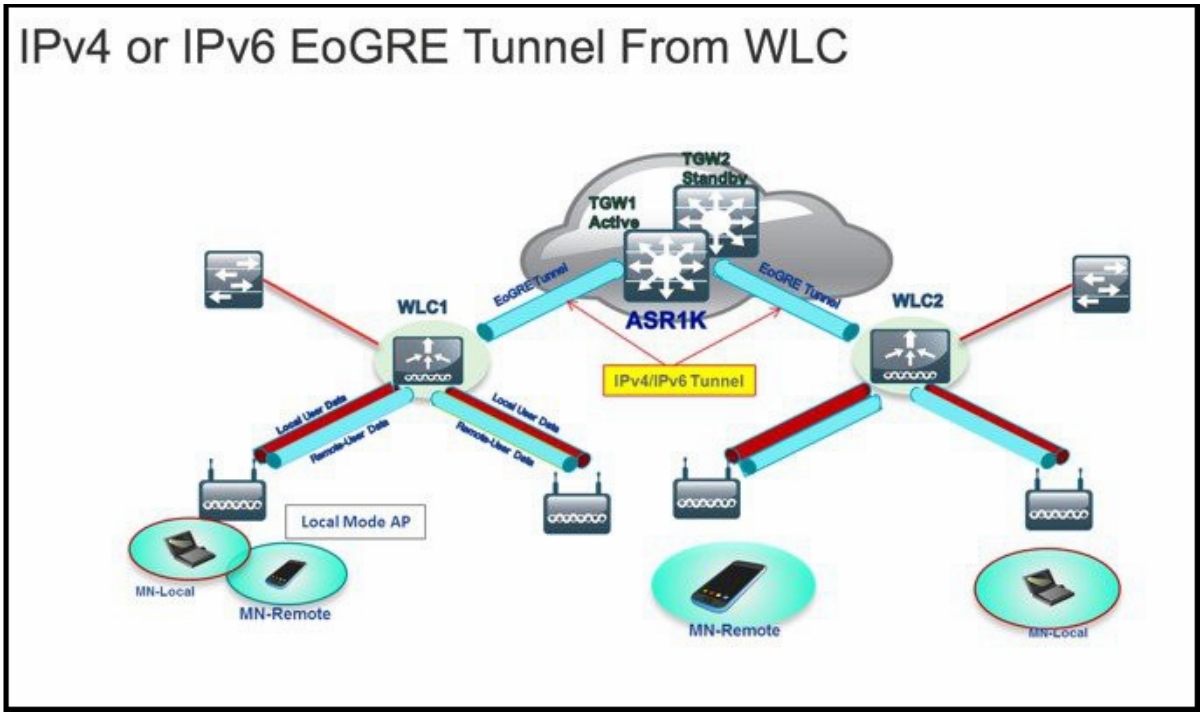
- Cisco 3504、5508、5520 シリーズ、WiSM-2、および 8500 シリーズ ワイヤレス LAN コントローラ。
- リリース 8.2 以降では、2500 シリーズおよび vWLC で EoGRE がサポートされます。
- 7500 コントローラでは、TGW への EoGRE 直接トンネルが設定されたフレックス接続 AP のみサポートされます。
- Cisco WLC 8.4 のサポート対象アクセス ポイント:3800、2800、1800、3700、2700、1700、1600、3600、2600、2700、702i、3500、702w、1540、1560、1552、1532、1572。

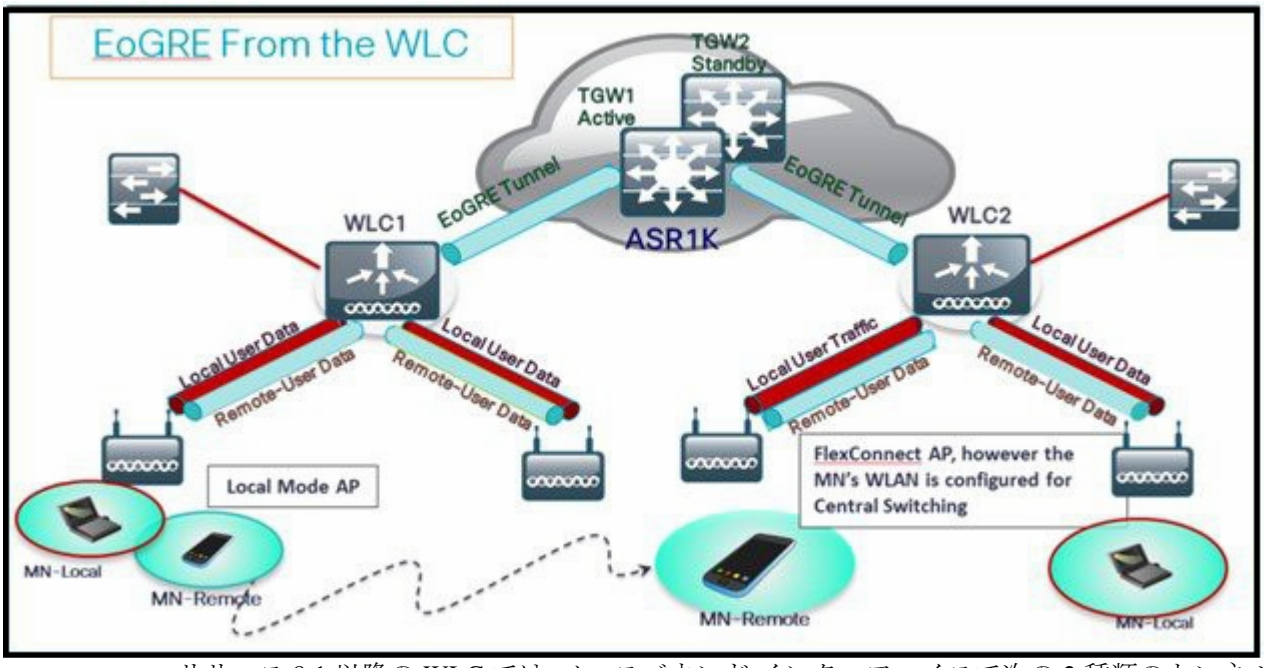
EoGRE トンネル システムの設計オプション

設計 1：WLC ベースの EoGRE トンネル

- CAPWAP 制御パス（AP WLC）
- CAPWAP データ パス（AP WLC）
- EoGRE データ フロー（WLC-TGW）

この設計モデルでは、WLC から ASR 1000 などトンネル ゲートウェイへのトンネルが生成されます。リリース 8.2 以降のコントローラでは、最大で 10 個のトンネル ゲートウェイ構成、10 個の EoGRE トンネル ゲートウェイ、そしてトンネルごとに 10 個のプロファイルがサポートされます。各プロファイルは、複数のレルムを使用して設定することもできます。レルムが設定されている場合は、@ の後のユーザ名になります。レルムは @ の後の文字列です（例：user_name@realm）。冗長性を確保するために複数のトンネルを設定できます。その場合、プライマリまたはアクティブ トンネルで障害が発生すると、セカンダリまたはスタンバイ トンネルが EoGRE トンネルのオペレーションを引き継ぎます。EoGRE トンネル設定では、コントローラ内およびコントローラ間のモビリティもサポートされます。





リリース 8.1 以降の WLC では、ノースバウンド インターフェイスで次の 2 種類のトンネル設定がサポートされます。

1. PMIPv6（RFC 5213）で定義されている IP/GRE – L3
2. Ethernet over GRE – L2

(注)　このガイドでは、EoGRE トンネルについてのみ説明します。

WLAN ごとに 1 種類のトンネルのみサポートされます。EoGRE は、オープン WLAN または 802.1x ベースの WLAN でサポートされます。トンネル クライアントでは、EAP-SIM または EAP-AKA モードのみがサポートされます。その他の認証モードは、トンネル クライアントでサポートされません。

オープン SSID の WLAN を使用する場合は、すべてローカル/シンプル クライアントまたはすべてトンネル クライアントがサポートされますが、同じ WLAN 上に混在させることはできません。ただし、802.1x で認証されたシンプルまたはトンネル EoGRE クライアントは同じ WLAN 上でサポートされます。

8.3 より前のリリースでは、オープンおよび WPA2-802.1X 用に設定された WLAN のみがサポートされました。

現在は、内部 WebAuth および WPA2-PSK 用に設定された WLAN に EoGRE トンネル プロファイルを割り当てることができるようになりました、WPA2-PSK/WPA2-802.1X および内部 WebAuth が設定された WLAN もサポートされます。

クライアントは、認証に基づいてローカル モードまたはトンネル モードに分けられます。WLC では、同じ WLAN 上で**リモート トンネル**や**ローカル**などの 2 種類のユーザ トラフィックがサポートされます。

ローカル ユーザ トラフィックは、WLC によってローカルにブリッジされるトラフィックとして定義されます。

リモート トンネル ユーザ トラフィックは、リモートトンネル ユーザのトラフィックとして定義され、WLC によって TGW にトンネリングされます。

EoGRE ユーザの AAA のオーバーライドがサポートされています。トンネル ゲートウェイは AAA プロキシとして機能することもできます。

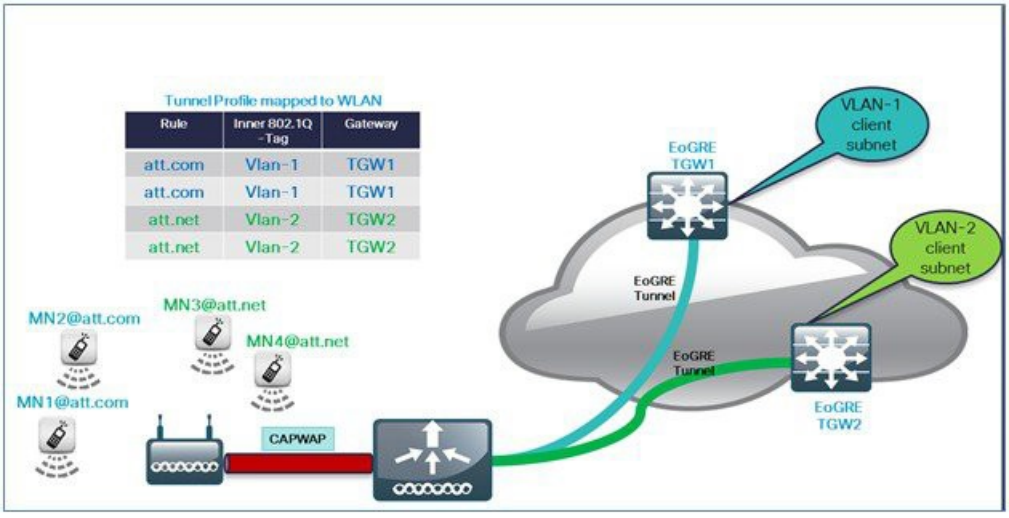
コントローラで EoGRE EAP 認証済みクライアントの AAA オーバーライドが有効担っている場合：

- WLC は、Access Accept を解析し、EoGRE、GTPv2、PMIPv6 などの MPC プロトコル タイプを探します。
- Protocol-Type AVP が存在する場合、WLC はそのトンネル タイプに関連するすべてのパラメータを探します。スタティック プロファイルは無視され、AAA によって提供されるパラメータがトンネルの設定に使用されます。
- AVP が存在しない場合、WLC は WLC のスタティック プロファイルを使用し、ユーザ名から抽出したレルムに基づいてトンネル タイプを判断します。
- 一部のパラメータが存在しない場合、認証は失敗します。たとえば、T-GW IP 以外のパラメータがすべて存在する場合でも、クライアント認証は失敗します。
- MPC-Protocol-Type が None の場合、MPC プロトコル タイプはシンプル IP になります。

AAA サーバから返される可能性がある属性には、User-Name、Calling-Station-Id、gw-domain-name、mn-service、cisco-mpc-protocol-interface、eogre_vlan_id などがあります。

一般的な展開：WLC EoGRE トポロジ

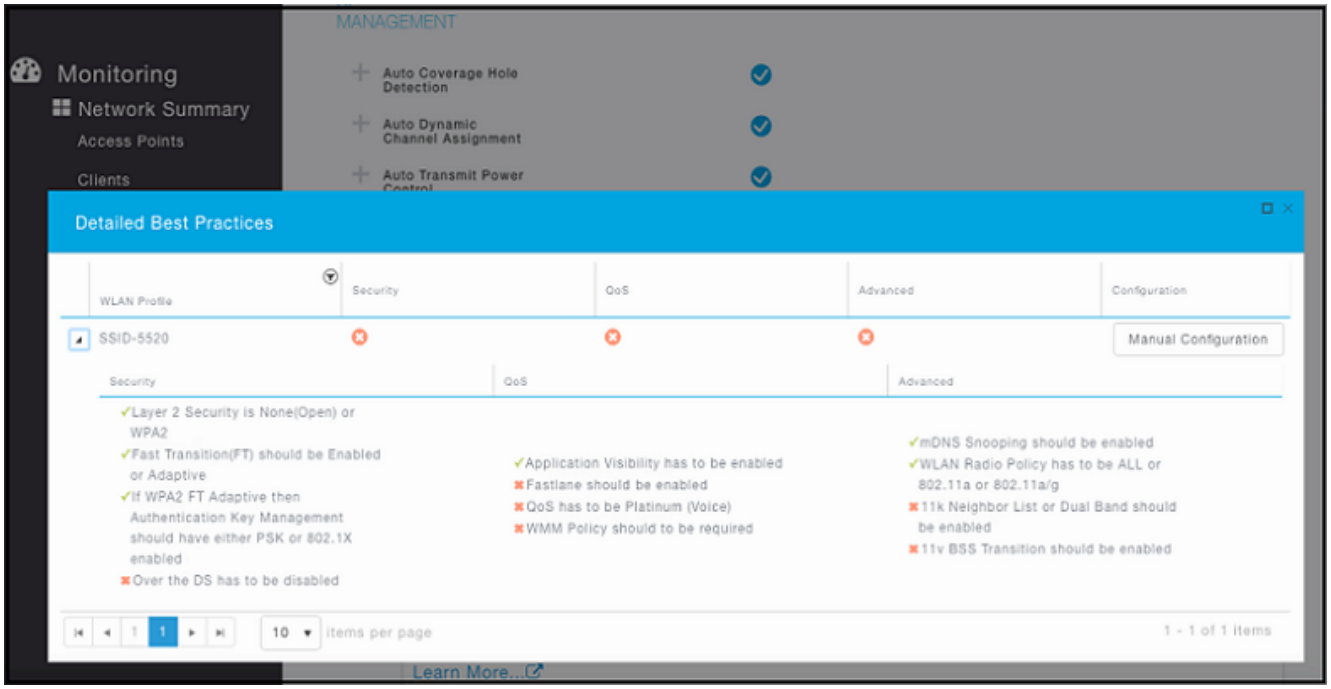
この一般的な EoGRE の展開設定では、2 人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の 2 人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続するときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN2 および TGW2 に接続する必要があります。この設定では、それぞれ 1 つのレルムを含む 2 つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。



設計 2：FlexConnect AP ベースの EoGRE トンネル

- CAPWAP 制御パス（フレックス AP と WLC 間）
- EoGRE データ パス（フレックス AP と TGW 間）
- トンネルが確立されると、データは FC AP から直接 TGW に流れます。

この設計では、AP からの直接トンネルにより、データ プレーンとコントロール プレーンがコントローラと AP から分離されます。ネットワークのコアへのデータ パス ルーティングが最適化されるため、中央のデータ スループットはコア ネットワークの容量によってのみ制限されます。コントローラ内またはコントローラ間のモビリティはサポートされませんが、クライアントはローカル スイッチング モードの同じ FlexConnect グループに引き続きローミングできます。

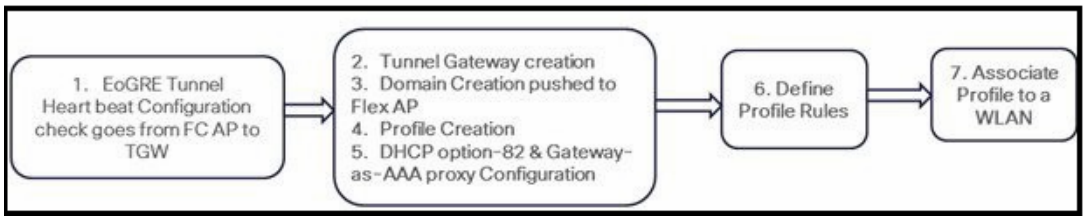


- FlexConnect AP：EoGRE は、オープン WLAN および 802.1x ベースの WLAN でサポートされます。
- 802.1x で認証された「シンプル」または「トンネル」EoGRE クライアントは同じ WLAN 上でサポートされます。
- クライアントは、認証に基づいてローカル モードまたはトンネル モードに分けられます。
- トンネル クライアントでは、EAP-SIM または EAP-AKA モードがサポートされます。
- オープン SSID WLAN では、すべてローカル クライアントまたはすべてトンネル クライアントのいずれかがサポートされます。
- EoGRE ユーザの AAA のオーバーライドがサポートされています。
- トンネル GW は AAA プロキシとして機能することもできます。
- FlexConnect AP では、TGW 障害検出と代替 TGW へのスイッチオーバーがサポートされます。

- TGW では、アクティブ/スタンバイ モードによるフォールト トレランスがサポートされます。
- コントローラ内およびコントローラ間のモビリティは、FlexConnect AP モードでサポートされます。
- スタンドアロン モードでは、モビリティは FlexConnect グループ内でのみサポートされ、トンネル GW は AAA およびアカウンティング プロキシとして設定できます。
- トンネル GW では、「設定可能」DHCP オプション 82 がサポートされます。
- リリース 8.4 以降では、FlexConnect で IPv6 アドレスがサポートされます。

基本的な Flex AP EoGRE 設定

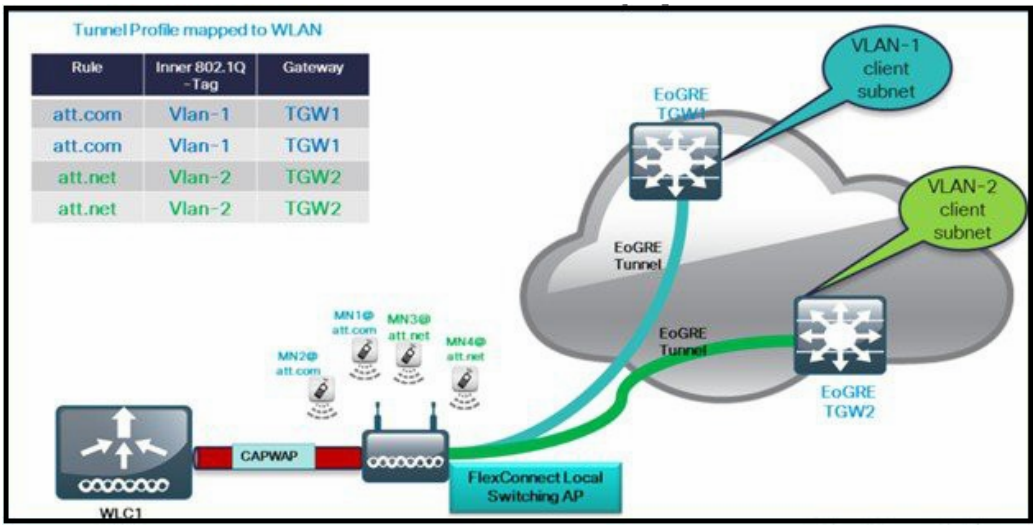
- Flex AP に EoGRE トンネルを設定する場合：
- WLAN にプロファイルを適用すると、WLC または FC AP トンネルに同じトンネル設定が適用されます。
- FC AP がローカル スイッチ モードになっている場合、FC AP ゲートウェイ トンネルが自動的に適用されます。
- ローカル モードの AP に接続しているクライアントは、WLC-TGW トンネルを介して通信します。
- FC AP に接続しているクライアントは、FC AP-TGW トンネルを介して通信します。
- クライアントの選択も、AAA またはプロファイル オーバーライドの影響を受けます。



（注）　冗長トンネル設定モードでは、EoGRE トンネル モードに設定されているすべての FC AP からキープアライブ ping が送信されます。

一般的な展開：FlexConnect AP - EoGRE トポロジ

この一般的な FC AP - EoGRE トンネル展開設定では、2 人のユーザ MN1 と MN2 が Realm @att.com に接続し、他の 2 人のユーザ MN3 と MN4 が Realm @att.net に接続しています。次の図に示すように、ユーザ MN1 と MN2 は接続するときに VLAN1 および TGW1 上にいる必要があり、ユーザ MN3 と MN4 は VLAN-2 および TGW2 に接続する必要があります。この設定では、それぞれ 1 つのレルムを含む 2 つのプロファイルが作成され、同じドメイン内の TGW1 と TGW2 に適切にマッピングされます。この展開シナリオでは、トンネルはローカル スイッチング モードの FlexConnect AP と TGW1 および TGW2 間に直接設定され、データ トラフィックはすべてコントローラをバイパスして流れます。



その他の設計と設定の詳細については、次のリンクにある EoGRE 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

運用およびメンテナンス

ここでは、Cisco Unified Wireless Network 導入の運用およびメンテナンスを簡単にするための導入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、次のようなさまざまな WLC ディスカバリ メカニズム（前述）により、CAPWAP AP の初期導入は非常に簡単になります。次のオプションがあります。

- 制御された環境での WLC を使用して前もって行われる CAPWAP 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 または DNS）を使用し、難しい設定なしに行われる導入

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、通常動作中の特定の AP のプライマリ WLC の定義が、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 の設定に加えて行われます。

AP 分散

通常の初期 WLAN 導入では、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導入は簡単になりますが、いくつかの運用上の理由から、自動分散方式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、およびメンテナンスが簡単になり、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。

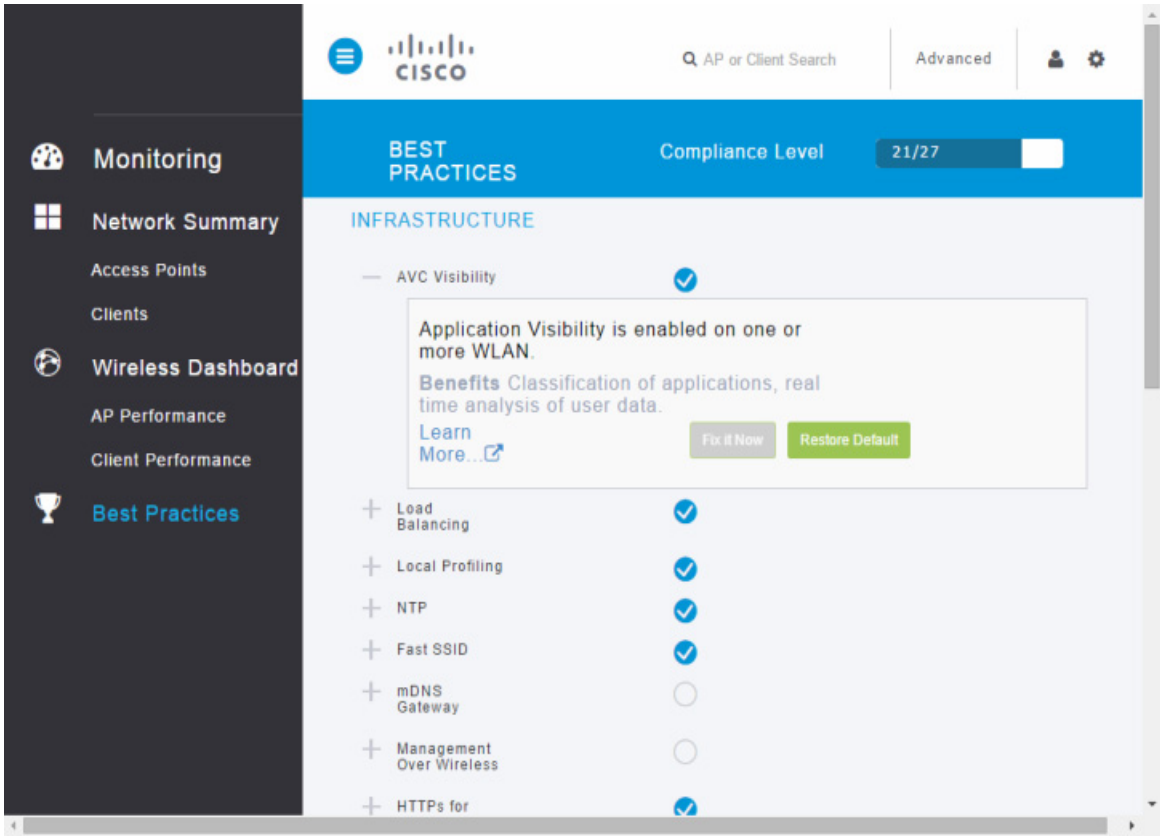
複数の WLC にわたる AP 分散を制御するために使用される要素は、次のとおりです。

- 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、AP にはプライマリ、セカンダリ、およびターシャリ WLC は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（モビリティ グループ内にある）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。

ベスト プラクティス

CUWN ソフトウェア リリース 8.1 以降では、ネットワーク導入エンジニア向けに、WLAN コントローラ用ダッシュボードにベスト プラクティス チェックリストが提供されています（図 2-48）。このチェックリストは、シスコの推奨するベスト プラクティスに合わせて WLC 設定を微調整するために使用します。このチェックリストでは、WLC 上のローカル設定と推奨されるベスト プラクティスを比較して、異なっているすべての機能を強調表示しています。このチェックでは、ベスト プラクティスを適用するための簡単な設定パネルも提供しています。ベスト プラクティスの採用は、すべての CUWN 導入において強く推奨されます。

図 2-48　　ベスト プラクティス ダッシュボード



このダッシュボードでは推奨される各機能を順守していることをチェックし、それぞれの準拠に関するフィードバックを提供します。ベスト プラクティス得点は、有効化されている推奨機能の数に従って表示されます。各推奨機能はインフラストラクチャ、セキュリティ、RF 管理のいずれかに分類されており、大部分はダッシュボードからクリック 1 回で直接有効化できます。特定の機能の詳細およびメリットもダッシュボードに示されています。

表 2-7　　リリース 8.1 のベスト プラクティス

インフラストラクチャ	セキュリティ	RF 管理
• Application Visibility and Control（アプリケーションの可視性およびコントロール） • ロード バランシング • ローカル プロファイリング • NTP • 高速 SSID • mDNS スヌーピング • ワイヤレスによる管理 • 安全な Web アクセス • Aironet IE • マルチキャスト転送 • コントローラの高可用性	• WLAN の 802.1X • 不正ポリシー • 不正しきい値 • SSH/Telnet アクセス • Client Exclusion • レガシー IDS • ローカル管理パスワード ポリシー • CPU ACL	• SSID 制限 • クライアント BandSelect • 40 MHz チャネル幅 • 自動動的チャネル割り当て • 自動送信電力制御 • 自動カバレッジ ホール検出 • CleanAir • イベント駆動型無線リソース管理

（注） 現時点でのベスト プラクティスを網羅したリストが次の URL のダッシュボードにあります: http://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc.html

Apple デバイスと ISE RADIUS のベスト プラクティス

リリース 8.5 では、シスコ ネットワークにおける Apple デバイスのパフォーマンス強化を目的に Apple デバイス関連のベスト プラクティスが多数追加されます。また、ISE を Radius サーバとして使用する場合に推奨される ISE のベスト プラクティスも追加されています。

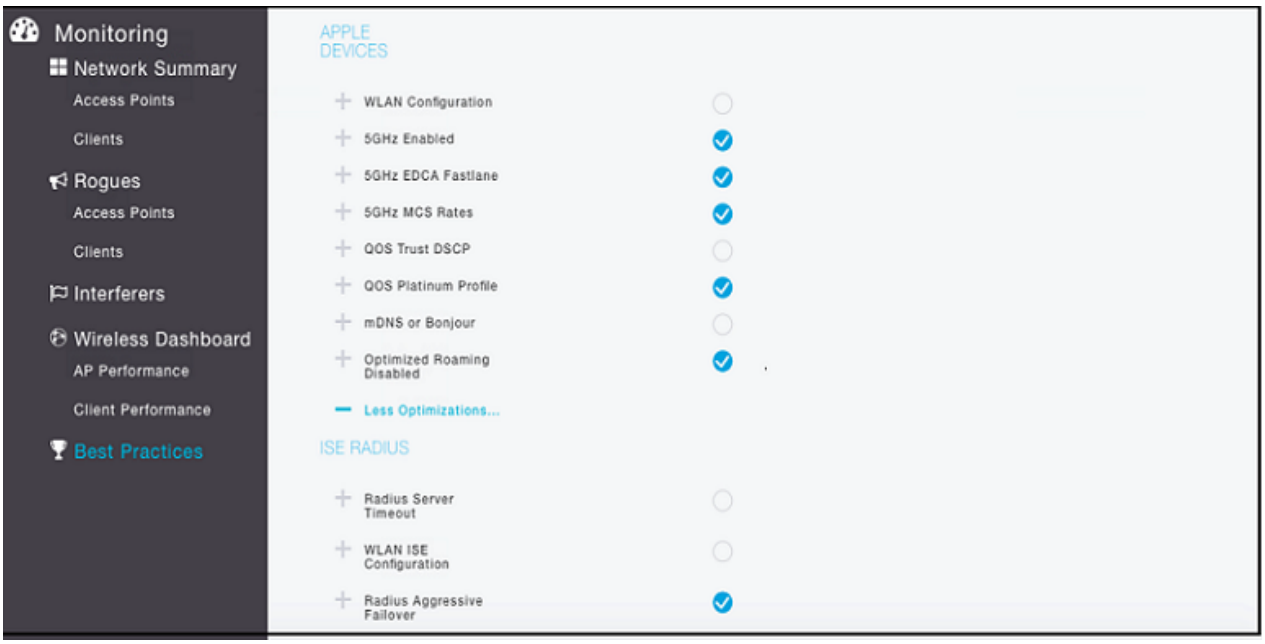
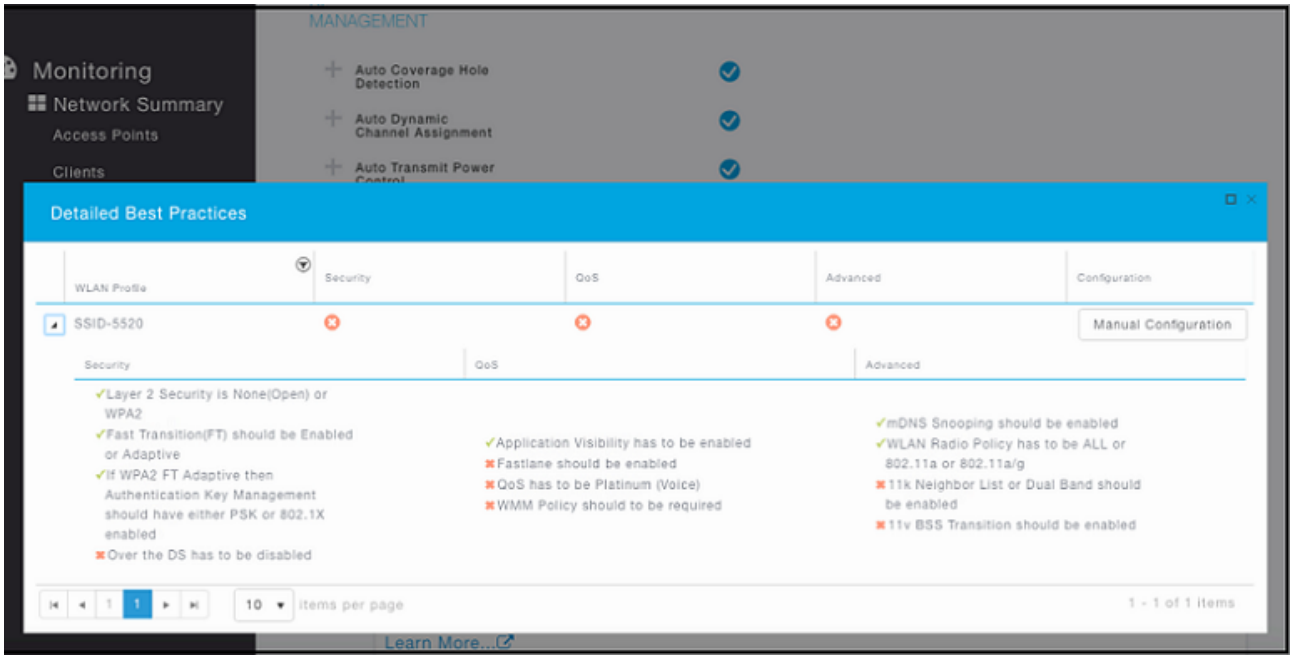
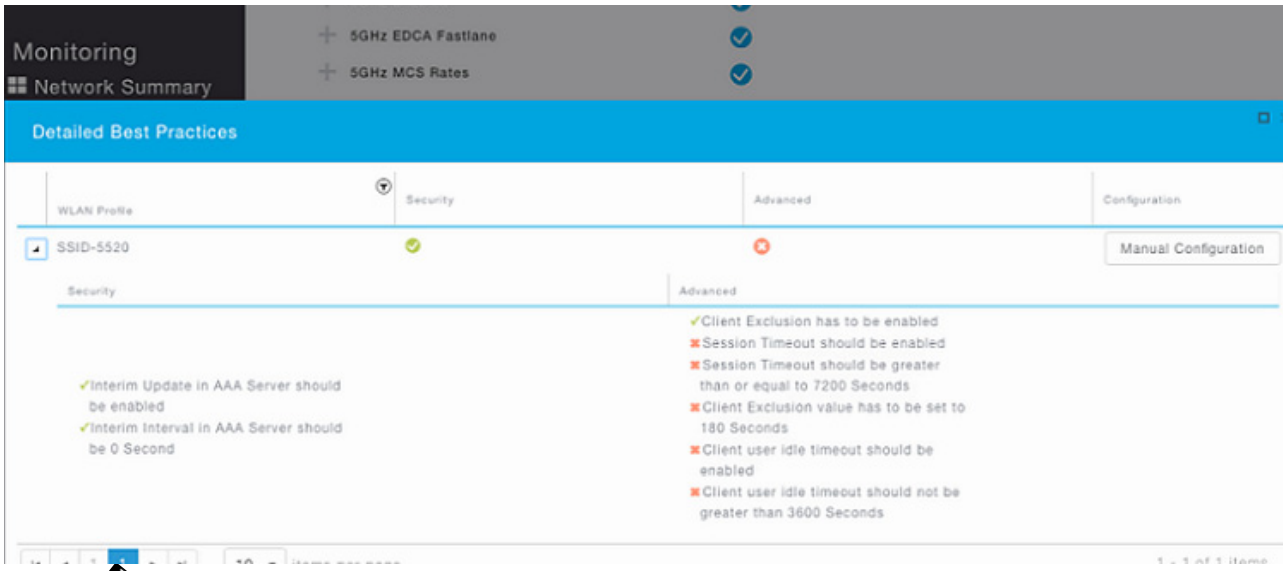


表 2-8　　リリース 8.5 のベスト プラクティス

Apple デバイス	ISE RADIUS
ISE RADIUS	RADIUS サーバのタイムアウト
5GHz の有効化	WLAN ISE 設定
5 GHz EDCA Fastlane	RADIUS アグレッシブ フェールオーバーの無効化
5 GHz MCS レート	
QoS Trust DSCP	
QOS Platinum プロファイル	
mDNS または Bonjour の有効化	
最適化されたローミングの無効化	

これらのセクションの WLAN 設定のベスト プラクティスを展開すると、WLAN ごとに有効化および無効化できるベスト プラクティスの詳細なリストが表示され、ベスト プラクティス機能のギャップが一目でわかります。





（注） ダッシュボードで提供される最新のベスト プラクティスの一覧については、https://www.cisco.com/c/en/us/td/docs/wireless/controller/best-practices/base/b_bp_wlc.html を参照してください。

CHAPTER 3

WLAN RF 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）環境における無線周波（RF）の考慮事項を理解するために必要な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。

- 規制区域および RF の考慮事項
- IEEE 802.11 規格
- 802.11b/g/n（2.4 GHz）および 802.11a/n/ac（5 GHz）などの RF スペクトルの実装
- RF 導入の計画
- 無線リソース管理（RRM）のアルゴリズムおよび構成
- RF プロファイルおよび調整

RF の基礎

米国では、工業用、科学用、および医療用（ISM）のライセンス不要の用途のために 3 つの主帯域が割り当てられています。

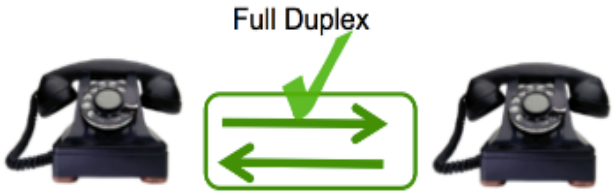
これらの ISM 帯域は、次のように定義されています。

- 900 MHz 帯域：902 ～ 928 MHz
- 2.4 GHz 帯域（IEEE 802.11b/g/n）：2.4 ～ 2.4835 GHz
- 5 GHz 帯域（IEEE 802.11a/n/ac）：
- 5.150 ～ 5.250 GHz（UNII-1）：当初は屋内使用向けのみでしたが、米国では現在、屋内と屋外の両方が許可されています。
  - 5.250 ～ 5.350 GHz（UNII-2a）
  - 5.350 ～ 5.470 GHz（U-NII-2b）：提案されていますが、まだ承認されていません。
  - 5.5504 ～ 5.725 GHz（UNII-2c）
  - 5.725 ～ 5.875 GHz（UNII-3）
  - 5.825 ～ 5.925 GHz（U-NII-4）

900 MHz 帯域は Wi-Fi には使用されません。残りの各帯域には異なる特徴があり、Wi-Fi について言えば、カバレッジとキャパシティに関する目標や、使用する場所ですでに占有されているスペクトルに応じて、適しているかどうかが変わります。詳細については、この章で説明する導入に関する考慮事項を参照してください。

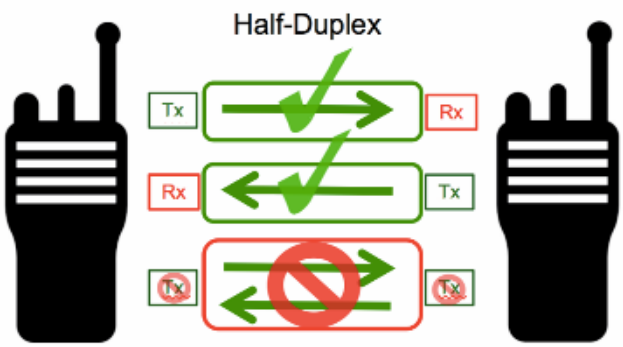
Wi-Fi が今日の LAN 実装と異なる点を理解することが重要です。今日の有線 LAN は、ほとんどの場合、全二重のスイッチド インフラストラクチャです。つまり、トラフィックが同時に送受信され、アクティブ ポート間でスイッチされるため、クライアントは同時に送受信できます。電話による会話は全二重です。図 3-1 を参照してください。

図 3-1　　全二重の会話の例



一方、Wi-Fi は半二重です（図2）。つまり、ユーザは、媒体上のクライアント/アクセスポイント（AP）への送信（Tx）またはそれらからの受信（Rx）のいずれかが可能です。クライアントとネットワークは、交代でその媒体（共有ブロードキャストおよびコリジョン ドメイン）にアクセスします。Wi-Fi は競合ベースです。つまり、媒体へのアクセスを試みるステーションに関するルールが存在し、衝突（複数のステーションが同時に媒体にアクセスすることによる）が公平に解決されるため、すべてのステーションが機会を得ます。

図 3-2　　半二重の会話の例



異なる周波数割り当て（チャネル）を使用して、クライアントの物理的なグループが分離されます。特定のチャネルで動作する AP が使用可能な通信時間は有限で、AP に接続している各クライアントは、その AP のチャネルが提供する必要のある通信時間を共有します。AP を頻繁に使用するクライアントが増加するほど、各クライアントが個別に取得する通信時間が減少します。1 つまたは複数のクライアントに対してより高いデータ レートをサポートする（通信時間をより効率的に使用できるようになる）と、すべてのクライアントの使用可能な通信時間が増加し、個々のユーザに割り当てられる潜在的な帯域幅が大きくなります。

特定のチャネル上のすべてのクライアントは、それらが最終的に所属するネットワークとは関係なく、同じチャネル上で動作する他の AP へと広がる共通コリジョン ドメインを共有します。このため、同じチャネルを使用し、相互にヒアリングできる他のクライアントおよび AP と、使用可能な通信時間を共有することになります。チャネルに AP が追加されるたびに、通信時の管理オーバーヘッドが増大します。この追加の管理トラフィックの影響により、各ユーザが使用できる通信時間の合計がさらに減少し、パフォーマンスが低下します。

帯域幅 = 通信時間 X データ レート

単一の AP が提供できるものよりも大きな帯域幅が必要な場合（つまり、狭いエリアに多数のユーザがいる場合）は、複数の AP が必要になります。非オーバーラップ チャネルに実装される各 AP は、そのカバレッジ エリアに通信時間の分離されたチャンクを提供します。同じチャネル上の AP は、互いの範囲に入らない状態を維持する必要があります。シスコの RRM は、これを管理します。出力とチャネルの選択を管理して、複数の AP およびネイバーを調整し、最大限のパフォーマンスを実現します（このドキュメントの無線リソース管理（RRM）を参照）。

ネットワークのチャネル割り当ておよび再使用は、通信時間の効率性、最終的にはクライアントに提供可能な帯域幅を決定する大きな要因です。2 個の AP が同じチャネル上で相互にヒアリングできる場合は、オーバーラップする BSS を注意深く管理しないと、同一チャネル干渉を発生させる可能性があります。同一チャネル干渉が自分自身の AP によるものか、自分の AP とネイバーによるものかは重要ではありません。いずれにしても、AP はチャネルを共有する必要があります。適切な物理設計を行うには、次の 4 点を考慮する必要があります。

- AP の配置
- AP の動作帯域（2.4 GHz または 5 GHz）
- AP のチャネルの選択
- AP の電力レベルの割り当て

優れた設計の目標は、最小限の同一チャネル干渉でクライアント デバイスが使用できる潜在的な帯域幅を最大化する均一のワイヤレス カバレッジ（全体に同様の状態）を生み出すことです。

シスコの無線リソース管理（RRM）は、測定された無線メトリックを使用して、最適なチャネルと電力の組み合わせを計算し、割り当てます。無線の監視には、そのインフラストラクチャ内の Wi-Fiネットワーク動作と、そのスペクトルの既存外部ユーザの Wi-Fi および非 Wi-Fi が含まれます。RRM は同一チャネル割り当てを緩和し、電力を均一化しますが、使用可能なオープン チャネルがない場合または単に AP どうしが近すぎる場合に残る唯一の選択肢は、既存のユーザとのチャネルの共有です。この状態は輻輳環境で発生し、異なる 2 つのネットワークが同じ帯域幅を共有しなければならない場合があります。どちらかのネットワークがビジー状態でない場合は、もう一方がその帯域幅をすべて使用することがあります。両方のネットワークがビジー状態になると、公平なアクセスを確保するように設計された 802.11 の競合メカニズム（Listen Before Talk 方式）により、帯域幅が半分ずつ共有されます。

規制区域

無認可帯域で動作するデバイスは、エンドユーザによる正式なライセンス プロセスを必要としません。ただし、ISM 帯域において 802.11 で動作するように設計され、作成されたデバイスは、それが使用される地域の政府の規制に準拠する義務があります。「無認可」は「ルールがない」ことを意味しません。シスコのワイヤレス機器は、特定の地域の規制要件に従って動作するように設計され、認定されています。規制に関する表示は、事前プロビジョニング地域の製品番号に含まれています。

エンド ユーザは、正しく実装し、指定された地域向けの正しい機器が使用されていることを確認する責任を負います。各地域のシスコ セールスは、選択に関する案内を提供できます。ユニバーサル AP をプロビジョニングする場合は、AP の GPS 位置を確認するためにスマートフォン アプリケーションを使用して少なくとも 1 個の AP をプロビジョニングする必要があります。これにより、AP がそれをアクティブ化した地域に物理的に位置するようになります。1 個目の UAP のプロビジョニングが完了したら、有効になっている無線インターフェイスを使用して、最初の UAP から他の UAP をプロビジョニングできます。

世界の各規制機関は、それぞれの基準に従って無認可帯域を監視しています。WLAN デバイスは、該当する政府規制機関の規格に従う必要があります。規制要件が IEEE 802.11b/g/n および 802.11a/n/ac 準拠製品の相互運用性に影響することはありませんが、規制機関は製品の実装に関して特定の基準を設定しています。たとえば、無線（Wi-Fi に限らない）が生成したり、近接した場所の他の無線から受信する干渉の量を最小限に抑えるために設計された WLAN の RF エミッション要件があります。該当する規制機関から製品の認証を受けることは、WLAN ベンダーの責任です。また、設置されたものがその要件を超えないことを確認することは、設置者の責任です。シスコでは、規制要件を満たすアンテナと無線の組み合わせの使用を推奨し、認定しています。

シスコでは、規制当局の要件に準拠するほか、各種の Wi-Fi アライアンス（WFA）認定プログラム（www.wi-fi.org）を通じて、他のベンダーとの相互運用性を確認しています。

動作周波数

802.11b/g/n の 2.4 GHz 帯域の規制は、動作時間の点では、比較的変わりがありません。FCC（米国）は 11 チャネル、ETSI（および世界中の他のほとんどの地域）は最大 13 チャネル、そして日本は最大 14 チャネル許可していますが、チャネル 14 で動作するには特別なライセンスと動作モードが必要になります。

802.11a/n/ac の 5.0 GHz 帯域の規制を準拠する国では、それらの国が許可するチャネルやそれらの国での動作に関するルールの多様性が増大しています。一般に、802.11ac の進歩により、大半の国で、5 GHz Wi-Fi に関してより多くのスペクトルを開くことが現在検討されています。また、すべての国で、5 GHz の非オーバーラップ チャネルが、2.4 GHz のいずれの場所で使用可能な非オーバーラップ チャネルよりも多く存在します。

テクノロジーが進化し、規制ルールが変更されるにつれて、これらの周波数帯域と関連プロトコルにも変化の可能性が生まれ、実際に変化しています。シスコのすべての AP は、その規制認定と許可された周波数およびチャネルが、個別のデータとしてドキュメント化されています。

2.4 GHz - 802.11b/g/n

世界の大半の国では、「2.4 GHz 帯域」と通称される周波数帯域は、周波数 2400 ～ 2483 MHz の合計 83 MHz の使用可能スペクトルで構成されます。

現在、3 つのプロトコル仕様が、2.4 GHz 帯域の 802.11 Wi-Fi 動作に関して許可されています。IEEE によって作成された規格である 802.11b、802.11g、および 802.11n は、世界中の個別の規制機関によって承認されています。その他の多数の非 Wi-Fi テクノロジーも、動作のために 2.4 GHz 帯域を使用します。電子レンジ、ベビー モニタ、ゲーム コンソール、Bluetooth デバイス、コードレス電話などは、そのごくわずかな例にすぎません。これらの他の非 Wi-Fi デバイスは「Wi-Fi 信号の干渉」となる典型的な存在です。それは、これらのデバイスが 2.4 GHz 帯域での Wi-Fi 動作に干渉する可能性があり、実際に干渉しているためです。コンシューマ Wi-Fi デバイスも 2.4 GHz 帯域を多く使用します。多数の比較的古い（しかし広く使用されている）コンシューマ アクセス ポイント（ワイヤレス ルータとも呼ばれる）は、2.4 GHz 無線でのみ動作する単一帯域デバイスです。限られた量のスペクトルに結び付けられている 2.4 GHz 帯域にアクセスするさまざまなユーザの集合体により、この帯域では輻輳の問題が拡大しつつあります。

このため、2.4 GHz 帯域で Wi-Fi の導入を成功させることは、有望ではありません。この状況は、明らかに、2.4 GHz 帯域が 5 GHz 帯域よりも早く満杯になり、サポート可能なユーザが少なくなることを意味します。帯域での輻輳はローカルな現象であり、地域によっては問題がない場合もあります。事前現地調査により、用途に応じて、業務に必要なものを確認できます。

802.11b

802.11b プロトコルは 1999 年に、802.11 規格の改訂版として批准されました。このプロトコルは、5.5 および 11 Mbps のデータ レートをサポートし、幅広いユーザの承認とベンダーのサポートを獲得しています。802.11b は、今日の Wi-Fi 通信用に最初に標準化された仕様であったため、何千もの組織で展開されています。これは、現在使用可能なすべてのプロトコルのなかで最も非効率的なプロトコルです。そのため、このプロトコルを使用することにより、比較的少ない通信時間で、使用可能な通信時間がごく短時間で使い尽くされます。また、より少ないユーザしかサポートできません。802.11b は、単一トランスミッタ/レシーバ設計に基づいており、信頼性に影響を与えるマルチパス周波数現象が発生するとともに、設計もより複雑なものになります。一般に、その他の 802.11b 専用クライアントは、多くの場合、物流、小売り、または医療業界で使用される用途別アプライアンス（バーコード スキャナ、プリンタなど）に見られます。802.11b をサポートできる今日の無線機器は、通常、802.11n 用に設計されているすべての無線機器に実装され、それによって信頼性が向上します（MRC レシーバ）。ただし、802.11b 規格の効率性は改善されません。

802.11g

802.11 IEEE の改訂版として 2003 年に批准された 802.11g プロトコルは、802.11b 規格と同じスペクトルで動作し、802.11b 規格との後方互換性を備えています。802.11g 規格は、まったく異なる変調方式（OFDM）を使用し、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。後方互換性はありますが、この互換性は、802.11b に必要な通信時間と追加の管理オーバーヘッドという代償をともない、802.11g のみのクライアント環境で運用する場合に 802.11g によって実現される全体的なゲインを減少させます。802.11b と 802.11g の混在環境におけるパフォーマンスは、セルの潜在的なキャパシティの 50 % 程度を犠牲にするものになります。802.11b の設計に似た初期の 802.11g 無線も単一のレシーバとトランスミッタを持ち、実装において同様の信頼性に関する問題が多数発生します。

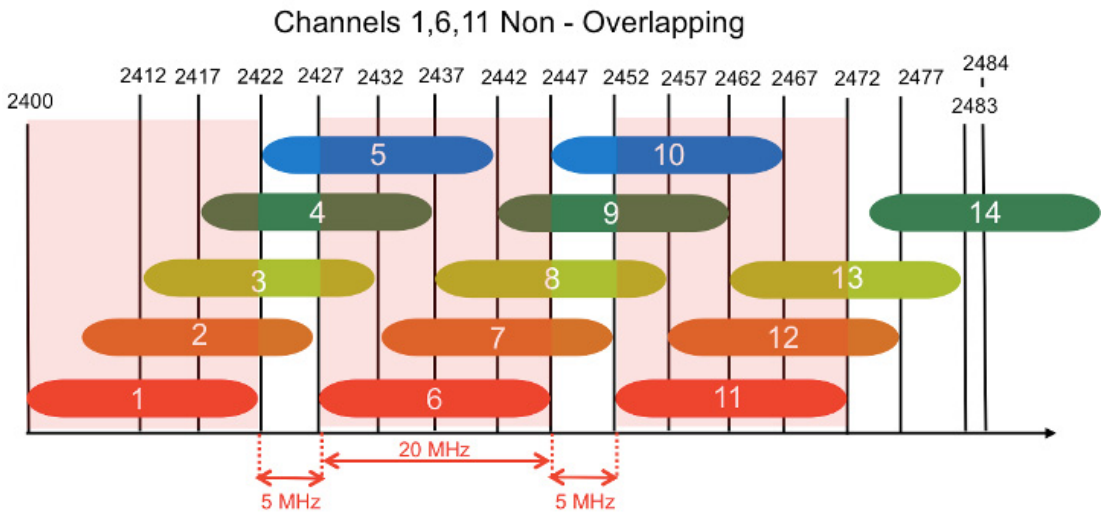
802.11n

802.11n は、802.11 規格の改訂版として 2009 年に批准されたプロトコルであり、2.4 GHz 帯域または 5 GHz 帯域のいずれかで使用できます。このプロトコルでは、複数の無線による MIMO（Multiple Input Multiple Output）が導入されており、複数の空間ストリームの同時エンコーディングが可能です（理論上、同じ通信時間で最大 4 倍のデータを処理できるが、3 つの空間ストリームが実際の上限）。2.4 GHz 帯域は、最大 216 Mbps までのデータ レートをサポートします（20 MHz のチャネルと 3 つの空間ストリーム トランスミッタを仮定した場合）。また、802.11n では、40 MHz のより広いチャネルの動作が指定されています。この動作は、単一の 40 MHz のチャネルを作成するために 2 つの 20 MHz チャネルを必要とするため、一般に「束ねられたチャネル」と呼ばれます。非オーバーラップ チャネルを 3 つしか使用できないことに関連する干渉の問題のために、シスコでは、2.4 GHz でのチャネルのボンディング（束ねること）をサポートしていません（図 3-3）。3 つの空間ストリームをサポートするデバイスの数は、よりハイエンドのラップトップおよびタブレットとアクセス ポイントに制限されます。2 空間ストリーム デバイスは、より多く存在しますが、やはり、ラップトップとタブレットに制限されます（いくつかの最新のスマートフォンは複数の空間ストリームをサポートするようになっています）。すべての場合において、802.11n 製品には、複数のレシーバ/アンテナに依存して初期の 802.11b および 802.11g/a レシーバに関連する信頼性の問題を軽減する、MRC（最大比合成）と呼ばれるレシーバに関する技術が導入されており、Wi-Fi の全体的な信頼性とパフォーマンスが向上しています。このため、今日の 802.11n ベースの無線通信は、802.11g 規格に基づいて動作する場合に信頼性が改善されます。

2.4 GHz Wi-Fi チャネルの計画

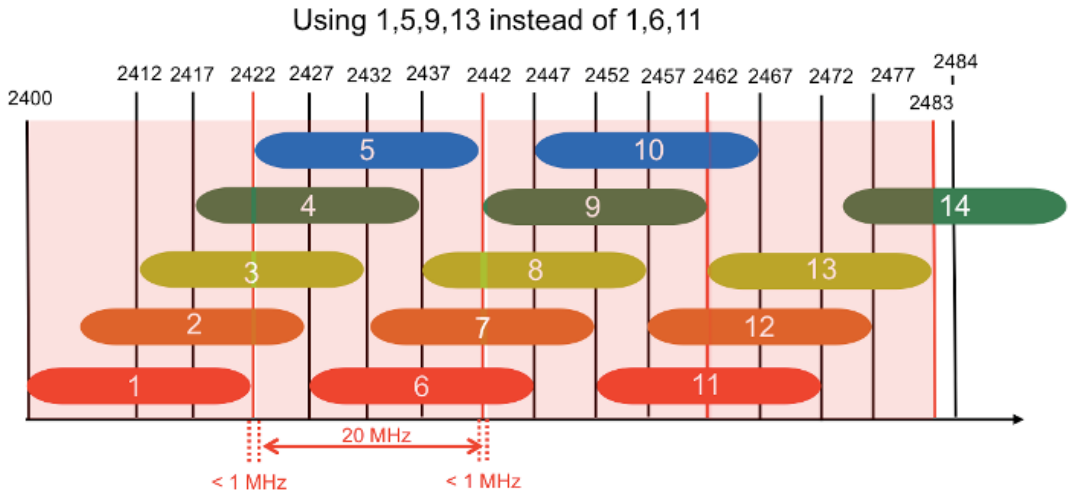
2.4 GHz 帯域のチャネル計画では 14 のオーバーラップ チャネルが識別されますが、次の図では、これらのうちの 3 つのチャネル（1、6、11）の部分が強調されています。他のすべてのチャネルが境界をオーバーラップまたは共有していることに注意してください。米国では、非干渉チャネル動作に 1、6、11 のみを使用できます。

図 3-3　　2.4 GHz チャネル（1、6、11 を選択した場合）



（注）　一部の規制区域では、4 チャネル計画が機能することが示唆されています。これは何度となく取り上げ続けられていますが、チャネルの境界の外側で起こることについては、あまり詳しく述べられていません。他はともかく最小密度の環境では、単に、この計画が実用的に機能するためにチャネル間に残されているスペースが不十分です。また、世界の大半の国で 1、6、11 が承認されており、ほとんどの無線がこのチャネル計画にデフォルト設定されていることを考慮してください。このような状況で、1、5、9、13 を選択すると、標準チャネルを使用するどの無線も、少なくとも 1 つのチャネル（ほとんどの場合に 2 つのチャネル）と干渉します。シスコでは、これらの理由で、そのような選択を推奨していません。

図 3-4　2.4 GHz チャネル(1、5、9、13 を選択した場合)



2.4 GHz での輻輳を低減させるための有効な戦略には、次の方法による自己干渉の削減が含まれます。

1. 802.11b データ レートを無効化する：これにより、カバレッジ/干渉エリアが削減されるとともに、最も非効率的なプロトコルが通信から排除されます。
2. 比較的高い最小必須データ レートを選択する：これによっても、有効なカバレッジ/干渉が削減され、12 ～ 18 Mbps のデータ レートが高密度展開で使用されます。
3. どの AP にも 3 ～ 4 つを超える SSID（WLAN）を割り当てない（各 AP は設定済みの各 WLAN をブロードキャストする必要があるため）：これにより、物理チャネルに関連する管理オーバーヘッドを大幅に削減できます。
4. 既知の非 Wi-Fi 干渉源を排除する：これらを識別し、評価し、位置を特定するために CleanAir が役立ちます。

ソリューションに含まれない、隣接する Wi-Fi ネットワークからの干渉については、そのすべてにおいて追加のハードウェアが必要になり、設計が複雑化します。2.4 GHz でのクリティカルな動作に関する正当なニーズがある場合は、このレベルの設計経験がある人物を雇用することを推奨します。

5 GHz：802.11a/n/ac

5 GHz 無線帯域の無認可領域で動作する 802.11a/n/ac 無線は、2.4 GHz 帯域で動作する「すべて」のデバイスからの干渉の影響を受けません（コンシューマ デバイスからの非 Wi-Fi 干渉を含む）。Wi-Fi に使用可能な 5 GHz 帯域は、100 MHz から 300 MHz まで世界各国で大きく異なる場合があります。ただし、どの場合も 2.4 GHz スペクトルよりも大きな帯域幅を使用できます。

802.11a/n/ac 規格は別の周波数範囲で動作するため、2.4 GHz 帯域デバイスと 5 GHz 帯域デバイスは同じ物理環境で相互に干渉することなく動作できます。シスコのほとんどの AP は、2.4 GHz と 5 GHz の両方のデュアルバンド動作をサポートします。5 GHz Wi-Fi での使用については、802.11a、802.11n、および 802.11ac の 3 つのプロトコル仕様が批准されています。周波数/チャネルの範囲は、5 GHz の異なる周波数セグメントに分割されます。また、この周波数範囲も時間をかけて増やされました。米国では、次の周波数範囲があります。

- 5.150 ～ 5.250 GHz（UNII-1 - 4 チャネル：36 ～ 48）
- 5.250 ～ 5.350 GHz（UNII-2 ～ 4 チャネル 52 ～ 64）

- 5.470 ～ 5.725 GHz（UNII-2c ～ 12 チャネル 100 ～ 144）
- 5.725 ～ 5.825 GHz（UNII-3 ～ 5 チャネル 140 ～ 165）
- 5.825 ～ 5.925 GHz（U-NII-4 ～ 4 チャネル 169 ～ 181）

3 つのプロトコルはすべて、同一のメカニズムを使用しているため、後方互換性があります。また、共通のエンコーディング テクノロジーを採用しているため、同時に使用した場合にも特に目立つ不利益なしに正常に連携します。主な違いは、通信時間の効率性です。

5 GHz 帯域でのチャネル割り当ては非常に単純です。これは、すべての割り当てが、チャネル間で維持される 5 MHz の最小分離による非オーバーラップ チャネルであるためです。

802.11a

802.11a は、802.11 規格の改訂版として 1999 年に批准されたプロトコルであり、動作する帯域と、802.11b との後方互換性が不要であることを除き、ほとんどの点で 802.11g 規格と同じです。802.11a は、6、9、18、24、36、48、および 54 Mbps の速度をサポートします。これは、2015 年には一般にレガシー プロトコルと見なされており、多数のネイティブ 802.11a デバイスが広く残っていることはないと思われます。無線では依然として 802.11a プロトコルが使用されていることがありますが、ほとんどの場合、このプロトコルは、少なくとも 802.11n ネイティブのデバイスで使用されています。

802.11n

802.11n は、802.11 規格の改訂版として 2009 年に批准されたプロトコルであり、2.4 GHz と 5 GHz で動作できます。また、いくつかの機能が拡張されていて、2 倍のチャネル幅による広いチャネル動作（20 ～ 40 MHz）が可能になっており、2 倍のキャパシティまたは速度を期待できます。このプロトコルでは、無線設計に MIMO（Multiple Input Multiple Output）という新しい概念が導入されました。複数の空間ストリームを使用することで、同じ信号内の個別のデータ ストリームを同時にエンコードできます。これにより、一度に送信できるデータの密度が増加し、桁違いの大きさのキャパシティと速度が実現されます。802.11n のデータ レートは、空間ストリームの変化する数（個別の無線設計によって決定される）と、使用されるエンコーディング方式に対応する必要がありました。新しいデータ レート構造では、標準データ レートに代わるものとして MCS（変調および符号化方式）が採用されました。

表 3-1　802.11n の MCS 1 ～23 のデータ レート

MCS 索引	空間ストリーム	変調タイプ	符号化レート	データ レート（Mbit/秒）			
				20 MHz チャネル		40 MHz チャネル	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
0	1	BPSK	1/2	6.5	7.2	13.5	15
1	1	QPSK	1/2	13	14.4	27	30
2	1	QPSK	3/4	19.5	21.7	40.5	45
3	1	16-QAM	1/2	26	28.9	54	60
4	1	16-QAM	3/4	39	43.3	81	90
5	1	64-QAM	2/3	52	57.8	108	120
6	1	64-QAM	3/4	58.5	65	121.5	135
7	1	64-QAM	5/6	65	72.2	135	150

表 3-1　802.11n の MCS 1 ～ 23 のデータ レート（続き）

MCS 索引	空間ストリーム	変調タイプ	符号化レート	データ レート（Mbit/秒）			
				20 MHz チャネル		40 MHz チャネル	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
8	2	BPSK	1/2	13	14.4	27	30
9	2	QPSK	1/2	26	28.9	54	60
10	2	QPSK	3/4	39	43.3	81	90
11	2	16-QAM	1/2	52	57.8	108	120
12	2	16-QAM	3/4	78	86.7	162	180
13	2	64-QAM	2/3	104	115.6	216	240
14	2	64-QAM	3/4	117	130	243	270
15	2	64-QAM	5/6	130	144.4	270	300
16	3	BPSK	1/2	19.5	21.7	40.5	45
17	3	QPSK	1/2	39	43.3	81	90
18	3	QPSK	3/4	58.5	65	121.5	135
19	3	16-QAM	1/2	78	86.7	162	180
20	3	16-QAM	3/4	117	130	243	270
21	3	64-QAM	2/3	156	173.3	324	360
22	3	64-QAM	3/4	175.5	195	364.5	405
23	3	64-QAM	5/6	195	216.7	405	450

MIMO（または複数の空間ストリームの使用）では、動作するために個別のトランスミッタとレシーバ（コード化される空間ストリームごとに 1 つずつ）が必要です。無線が増えると、必要な電力およびアンテナも増えます。このため、特定の無線がサポートする空間ストリームの正確な数は、多くの場合、特定のデバイスで使用可能な電力と設備に関連する設計で決定されます。実際には、デバイスが備える電力と空間が多いほど、そのデバイスがサポートできる空間ストリームが増えます。そのため、ほとんどの場合、多数のラップトップやタブレットと同様に、有線接続された電源を持つ AP が複数の空間ストリームをサポートします。限られたバッテリと空間しか持たないスマートフォンは、一般に、単一の空間ストリームをサポートします（例外もあるが多くはない）。また、コストとパフォーマンスに関連するさまざまな機能も備えています。トランスミッタは多くの電力を消費します。SISO（Single Input Single Output）は、複数のトランスミッタ（および複数の空間ストリームをサポートする機能）をサポートしない場合でも、改善が進んでいる複数のレシーバ（および劇的に改善されたレシーバ技術である MRC）をサポートします。802.11n 無線では、通常、「3x3:2」、「2x3:2」、または「1x2:1」という注記が示されます。これは、「（#TX）x（#RX）」（# はサポートされる空間ストリーム）を意味します。

802.11ac

802.11ac は、802.11 規格の修正版として 2013 年に批准されたプロトコルです。

（注）　802.11ac 規格は 1 つしかありませんが、11ac は 2 つの異なる時期に市場に投入されており、市場では一般に「Wave 1」および「Wave 2」と呼ばれています。どちらもこの記事の執筆日時点ですでにリリースされています。

802.11n で得られた多数の教訓に基づいて作成された 802.11ac は、最大 160 MHz のチャネルにより最大 8 つの空間ストリームを許可します。市場に投入された最初の Wave 1 製品では、最大 80 MHz のチャネルと 3 つの空間ストリームがサポートされていました。802.11ac Wave 1 に関して Wi-Fi 認証されたすべてのデバイスは、20、40、および 80 MHz チャネル幅で動作する必要があります。802.11n の仕様では、40 MHz 動作はベンダー オプションであり、クライアント機能とネットワーク設計の不一致が許可されました。すべての 802.11n デバイスが 40 MHz チャネル計画を利用できるわけではなく、チャネル数の削減によるゲインは見られません。

現在市場に投入されている Wave 2 製品は、最大 4 つの空間ストリームと 160 MHz チャネル幅を実装しています。160 MHz チャネル幅は、2 つの 80 MHz チャネルを 1 つのチャネルに束ねる（合計で 4 つの 20 MHz チャネル割り当てを消費する）ことによって形成されています。ここでも、4 つの空間ストリームは 4 つのトランスミッタとレシーバ（およびアンテナ）を意味します。このため、単一帯域無線の 8 つの Tx/Rx チェーンによる設備の問題がただちに生じます。

（注）　最大 4 つの空間ストリームをサポートする 802.11n とまったく同様に、4 つ目の空間ストリームからのゲインが非常に小さいため、実際の制限は 3 つの空間ストリームでした。802.11ac の 8 つの空間ストリームは、単一の 5 GHz 無線では実現しそうにありません。一部のメーカーが 2.4 GHz の 4 つの空間ストリームと 5 GHz の 4 つの空間ストリームを 8 つの空間ストリームとして売り込んでいることには注意が必要です。これらは、まったく同じものというわけではありません。空間ストリームの詳細については、Rob Lloyd が「Fundamentals of Spatial Streams」で行っている優れた概説を参照してください。

Wi-Fi に対する Wave 2 の他の大きな貢献として、MU-MIMO（Multi User MIMO）があります。802.11acの MU-MIMO により、個別の空間ストリーム上の複数のクライアントに同時に対応することが可能になります。802.11ac の詳細については、『802.11ac: The Fifth Generation of Wi-Fi Technical White Paper』を参照してください。

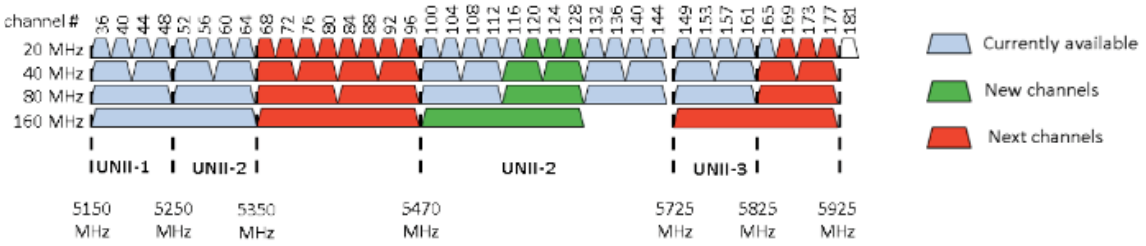
米国の 5 GHz の新しい FCC –B ドメイン

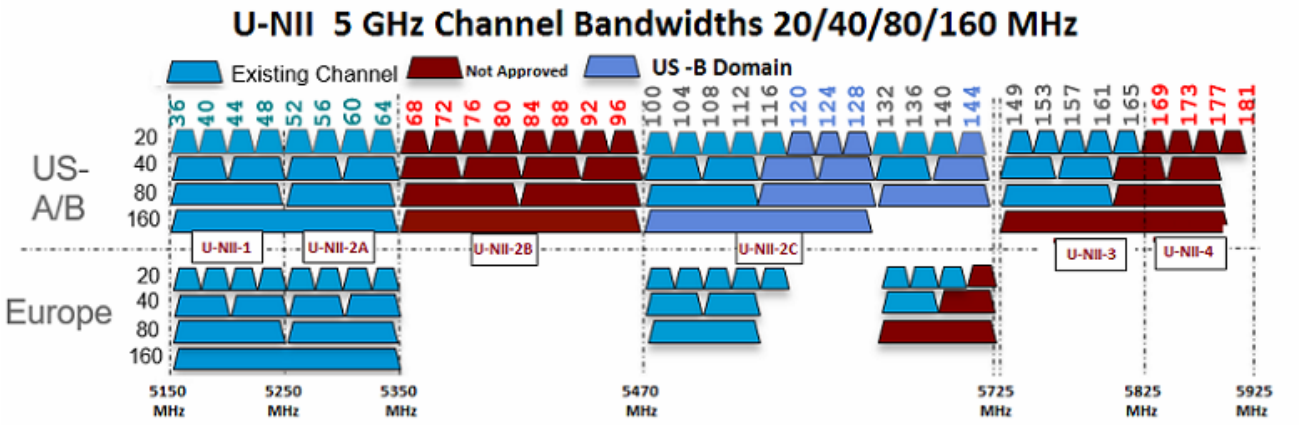
- 8.2MR1 の後の新しいソフトウェア リリースでは、–B ドメインがサポートされるようになりました。
- 2016 年 6 月現在、シスコは –A SKU を制限しており、米国で提供していません。
- 米国では、新しい連邦通信委員会（FCC）指令 14 ～ 30 により、–A SKU の実装内容が変更され、その結果として -B が導入されました。変更内容は次のとおりです。
  - U-NII-1 帯域（5150 ～ 5250 MHz）が屋外で使用できるようになりました。
  - U-NII-1 の送信電力が 1 W に増加しました。ただし、水平方向 30 度を超える等価等方輻射電力/Equivalent Isotropically Radiated Power（EIRP）を屋外で使用する場合には追加の制限があります。
  - Terminal Doppler Weather Radar（TWDR）帯域（チャネル 120、124、および 128）を動的周波数選択（DFS）の新しいテスト要件で使用できるようになりました。
  - U-NII-3（5.725 ～ 5.85 MHz）の新しい電力スペクトル密度および上下帯域境界エミッション要件が導入されました。

米国の 5 GHz チャネル計画

- これまでにない大きさのチャネル（20/40/80/160 MHz）を消費可能なプロトコルの作成は、今日の既存チャネルに対する多大な圧力をともないます。規制による制限のために、2 つの異なる周波数範囲のチャネルをいつでも束ねることができるわけではありません（11ac の 80+80 モードでこれが実現されるとしても）。また、今日の定義されているチャネルの間にはギャップがあるため、実際上の制限も存在します。米国では、より多くのスペクトルがすでに許可されており（チャネル 120、124、128 の復帰）、2 つの 160 MHz チャネルの可能性を利用することが容易になっています。範囲のギャップを埋める追加のスペクトルがすでに要求されています。また、さらに多くのことを可能にする追加のスペクトルも現在検討されています。世界各地のその他の規制機関も注目しています。
- 20、40、80、および 160 MHz チャネルに関する米国でのチャネルおよび帯域割り当てを次の図に示します。この図には、要求されている将来の割り当ても示されています。

図 3-5　現在の米国の 5 GHz 802.11 Wi-Fi チャネル計画





802.11ac に関するデータ レートは、より多くの空間ストリーム（1 ～ 8）、より広いチャネル（20/40/80/160 MHz）、またはエンコーディング レートの拡張の 3 つの形式で増加しています。802.11n は、2 チャネル幅および 4 つの空間ストリーム（実際には 3 つのみ）に制限されていました。そのため、速度を定義するために MCS 1 ～ 23が使用されました。0 ～ 7 で 1 つの空間ストリームのデータ レートが定義され、以降、8 ～ 15、16 ～ 23 と繰り返して、まず 2 つの空間ストリーム、次に 3 つの空間ストリームが定義されました。シスコでは、現在、8 つの空間ストリームを使用しています。このために必要な措置がありました。より単純な方法もあるかもしれませんが、現在、MCS 0 ～ 9 によって変調と符号化レートのみが定義されています。追加の空間ストリームまたは追加のチャネル幅の影響を計算するために乗数が使用されます。次の表に、最大 2 つの空間ストリームとすべてのチャネル幅を示します。これは、あまり簡単なものではありませんが、課題と取り組んできた長期的な視野で見れば比較的簡単です。表の後の乗数ルールに注意してください。

表 3-2　802.11ac の MCS データ レート

MCS 索引	変調タイプ	符号化レート	空間ストリーム	20 MHz	40 MHz	80 MHz	160 MHz
0	BPSK	1/2	1	7.2	15.12	32.4	64.8
0	BPSK	1/2	1	14.4	30.24	64.8	129.6
1	QPSK	1/2	1	14.4	30.24	64.8	129.6
1	QPSK	1/2	1	28.8	60.48	129.6	259.2
2	QPSK	3/4	1	21.7	45.57	97.65	195.3
2	QPSK	3/4	1	43.4	91.14	195.3	390.6
3	16-QAM	1/2	1	28.9	60.69	130.05	260.1
3	16-QAM	1/2	1	57.8	121.38	260.1	520.2
4	16-QAM	3/4	2	43.3	90.93	194.85	389.7
4	16-QAM	3/4	2	86.6	181.86	389.7	779.4
5	64-QAM	2/3	2	57.8	121.38	260.1	520.2
5	64-QAM	2/3	2	115.6	242.76	520.2	1040.4
6	64-QAM	3/4	2	65	136.5	292.5	585
6	64-QAM	3/4	2	130	273	585	1170
7	64-QAM	5/6	2	72.2	151.62	324.9	649.8
7	64-QAM	5/6	2	144.4	303.24	649.8	1299.6
8	256-QAM	3/4	3	86.7	182.07	390.15	780.3
8	256-QAM	3/4	3	173.4	364.14	780.3	1560.6
9	256-QAM	5/6	3	96.3	202.23	433.35	866.7
9	256-QAM	5/6	3	192.6	404.46	866.7	1733.4

1. MCS 9 の 20 MHz は、空間ストリーム 1、2、4、5、7、8 の仕様によれば正当ではありません。
2. 各空間ストリームによる追加分は 100 % です。たとえば、MCS 0 では 1 つの空間ストリームの場合はデータレートが 7.2、2 つ空間ストリームの場合はその 2 倍、3 つの空間ストリームの場合はその 3 倍になります。
3. チャネル幅乗数は、20 MHz 速度に対して 40 MHz は 2.1 倍、80 MHz は 4.5 倍、160 MHz は 9 倍です。たとえば、MCS 0 の 20 MHz の場合は 1 つの空間ストリームで 7.2 Mbps、40 MHz の場合はその 2.1 倍の 15.2 Mbps になります。

802.11ac では、Wi-Fi に関する効率性が大幅に向上しています。デバイスのサポートに関して言えば、空間ストリームの数が増えることは、電力とアンテナが増えることを意味します。無線設計は改善され続けており、すでに、より小さなデバイスへのより多くの空間ストリームの実装が見られるようになっています。現在、多数のクライアントが 1 ～ 2 つの空間ストリームに制限されていますが、すべての 802.11ac クライアントは、認定を得るために最大 80 MHz のチャネル動作をサポートする必要があります。160 MHz チャネルは米国での現在のスペクトル割り当てにおいて窮地に陥っており、一部の規制区域では不可能にいたっています。ちなみに、現在 80 MHz で動作する 3 空間ストリームの Wave 1 クライアントは 1.3 Gbps のデータ レートを達成できます。シスコも、将来的にはより高い速度をサポートする予定です。

802.11ad

802.11ad は、2.4 GHz または 5 GHz を使用しないという点で 802.11a/b/g/n/ac とは異なります。当初 WiGig と呼ばれたこの規格は、60 GHz 帯域の周波数を利用します。ミリ波周波数範囲が非常に高いため、範囲は一般に非常に近距離のデバイスに制限されます。周波数が高いほど伝達に要するエネルギーが多くなります。範囲は小さくても、潜在的スループットが高い（最大 7 Gbps）このテクノロジーは、パーソナル エリア ネットワークやワイヤレス USB/ビデオ アプリケーションに最適であると指摘されています。

IEEE 802.11 規格について

IEEE 802.11 は、米国電気電子技術者協会（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 規格を担当しています。これに対して、インターネット技術特別調査委員会（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 作業グループには、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。次の表 3-3 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については、http://www.ieee802.org/11/ を参照してください。

表 3-3　IEEE タスク グループの活動

タスク グループ	プロジェクト
MAC	物理レイヤ エンティティ（PHY）タスク グループとともに、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 帯域で高レートの 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（第 5 章を参照）。
f	マルチベンダー使用のためにアクセス ポイント間通信プロトコル（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/n/ac の PHY 動的周波数選択（DFS）、送信電力制御（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	ローミングを容易にするために、AP に関連付けられた 802.11k 対応クライアントは、適切なネイバー AP のリストを要求する。802.11k 対応 AP は、同じ WLAN にあるネイバー AP の、現在の Wi-Fi チャネル番号が付いたリストを使用して応答する。
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。

表 3-3　IEEE 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
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 Mbps 以上）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、車を使用したコマース 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	802.11r では、クライアントが現在の AP から離れる前でも新しい AP との最初のハンドシェイクが実行される、ローミングの新しい概念が導入されている。これは、高速移行（FT）と呼ばれる。
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 プロバイダー、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測定指標、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。
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。
ac	この改訂版は、5 GHz 帯域で非常に高いスループット（500 ～ 1000 Mbps）をサポートするための 802.11 MAC および PHY に対する機能拡張を指定する。

構成の考慮事項

2.4 GHz または 5 GHz のどちらに対応した設計にするか

Wi-Fi は今日では比較的成熟した技術です。依然として Wi-Fi が存在しない場所もありますが、現在では、何らかの信号カバレッジを持たない人や場所の存在を見つけることは困難です。このことは、独立した隣人が増加するほど Wi-Fi 干渉が増大するか増大する可能性があることにもよく表れています。これは、多くの場合、さまざまな企業の多数のオフィスが単一のビルおよびスペクトルを共有する複合施設で最悪の状況を生み出します。

Wi-Fi は、壁や床を通過するとともに、他の Wi-Fi および 非 Wi-Fi デバイスからも同様にすべての干渉を受け入れつつ動作する必要があるため、この点は非常に重要です。このことは、ネットワーク デバイスが他のネットワークからの信号を受信可能なレベルまで、それらのデバイスがそれらの他のネットワークと、使用可能な通信時間を共有することを意味します。自分と隣人がともにヘビー ユーザである場合、ネットワークがオーバーラップするエリアでは、どちらのユーザも期待される接続速度を下回る帯域幅しか使用できません。どちらのネットワークも、他のネットワークによるチャネルへのアクセスを待つことで時間を浪費します（そして、通信における時間の浪費はスループットを低下させます）。

密集した大都市、複合施設、またはショッピング モールで 2.4 GHz を使用することは、最高の状態でも不安定にしか成功せず、最悪の場合には頻繁に使用できなくなる可能性があります。世界の大半の地域では、ベスト プラクティスとして、3 つの非オーバーラップ チャネルを使用することが推奨されます。複数の異なるネットワーク オーナーが存在する高密度展開環境では、一部のオーナーが、過剰に混み合ったスペクトルにおいて何らかのメリットを得ることを期待して、常に、他の 8 ～ 10 チャネルの使用を試み続けます。多くの場合、そのようなメリットは得られません。実際には、他のネットワークとオーバーラップするチャネルを選択することにより、どのネットワークにとっても状況は悪化します。

2 個の AP が同じチャネル上にある場合、各 AP の競合メカニズムが、それらの間のチャネルへの公平なアクセスを可能にします。異なるもののオーバーラップしているチャネル上の AP は、オーバーラップする周波数上の 802.11 パケットを復調できず、それらのパケットはノイズとしてのみ認識されます。802.11 MAC レイヤがない場合、2 個の AP 間での調整は不可能です。両方の AP のセルに関して、エラーと衝突が増え、使用率が膨らむとともに貴重な通信時間が浪費されます。4 チャネル計画が可能（1、5、9、13）な地域にいる場合は、多数のクライアント ドライバがデフォルトでチャネル 12 および 14 を有効にしないことに注意してください。また、ほとんどのコンシューマと多数の AP システムは、デフォルトでチャネル 1、6、11 を使用します。このような状況では、チャネル 6 がチャネル 5 および 9 の両方と干渉し、チャネル 11 が チャネル 9 および 13 と干渉します（その逆の干渉もあります）。隣人がチャネル 1、6、11 を使用している場合は、自分もそれらを使用する必要があります。それにより、パフォーマンスが向上します。

事業運営に不可欠な用途の場合は、5 GHz の使用を計画します。以前は、5 GHz デバイスがあまり普及していなかったため、この計画は今よりも困難でした。今日では、ほとんどのメーカーが製品の規格として 802.11ac に焦点を合わせており、802.11ac は 5 GHz でのみ動作するため、状況が異なっています。

どうしても 2.4 GHz 上に重要な機能を展開する必要がある場合は、その要件が保持される理由と要因（具体的にはデバイス）を理解し、それらを最新のハードウェアによって置き換えることを検討します。非常に多くの 2.4 GHz 無線を相互に接近させて配置することしかできず、チャネルがいっぱいになると、それらもいっぱいになります。

Wi-Fi Alliance の認定データベース（Wi-Fi Alliance の認定製品検索）で調べると、今日のデバイスには 5 GHz をサポートするものが多く含まれていることを確認できます。最新の検索結果を参照し、これらの状況を検討に加えてください。

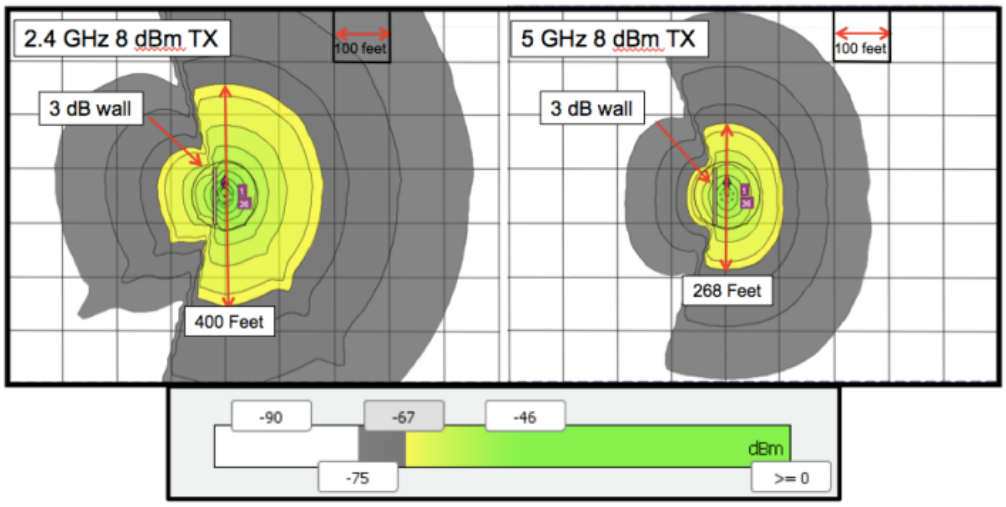
- 2015 年 8 月現在、5 GHz の 802.11n 動作について、2,409 機種のスマートフォン/タブレットが認定されています。
  - そのうちの 477 機種は、2013 年に認定済み。
  - 2014/15 年に認定された 591 機種は、すべて 802.11ac。
  - 同じ期間に Wi-Fi Alliance が認定した 2.4 GHz 専用デバイスは合計 3,167 機種で、これは現在の市場の 24 %（6 ヵ月前の 32 % から減少）。
  - これらの大半はローエンドのコンシューマ デバイス。

表 3-4　2.4 GHz と 5 GHzのメリットおよびデメリット

周波数帯域	メリット	デメリット
2.4 GHz	範囲が広い。周波数が増えるほど伝達距離が短くなるため（送信電力が等しい場合）。	相互干渉と少ないキャパシティのために、同じ物理スペースに設定できる AP が少ない。
	オブジェクトの貫通性が高く、屋内の範囲に優れている。	相互干渉と少ないキャパシティのために、同じ物理スペースに設定できる AP が少ない。
	スペクトル/チャネルが少ない。	輻輳が増加する。
		不適切な不正実装による干渉のリスクが増大する。
		非 Wi-Fi デバイスに関して任意の帯域が使用されることにより、一般に、干渉が増加する。
		束ねられたチャネルを使用し、スループットを向上させるために使用できるチャネル数が不十分なため、干渉が増加する。
5 GHz	範囲が狭く、自己干渉が少ないため、より多くの AP を使用し、より多くのユーザをサポートできる。	範囲が狭いと、一般に、より多くの AP が必要になる（UNII_3 の高い電力レベルは一般に AP 側でのみサポートされる）。
	より多くのチャネル、帯域幅、キャパシティを利用できる。	
	使用できるコンシューマ Wi-Fi デバイスおよび非 Wi-Fi デバイスが少ない。輻輳が少ない。	
	802.11ac は 5 GHz でのみ動作する。	
		範囲が狭いため、低密度ホットスポット カバレッジ モデルに適さない。

図 3-6 に、2.4 GHz 帯域（左）と 5 GHz 信号（右）の両方について、同じ Tx 電力設定での使用可能な信号の相違を示します。UNII-3 帯域では、電力を 23 dBm まで増加でき、5 GHz のカバレッジが 2.4 GHz よりも広くなりますが、これはこの帯域のみです。各 AP に関して使用可能な固定帯域幅を共有するユーザの人数は、セルの到達範囲に含まれるユーザの人数です。

図 3-6　2.4 GHz および 5 GHz の伝達距離



どのプロトコルを有効にする必要があるか

802.11 規格で使用可能な複数のプロトコル規格が存在します。実際に、Wi-Fi Alliance 認定を得るには依然として 1999 年以降に批准されたすべての規格が必要であり、それらの規格は、802.11 規格が属している帯域をサポートするすべてのハードウェアに含まれています。ただし、このことは、それを使用する必要があることを意味しません。ユーザによる、サポートする（またサポートしない）プロトコルの選択は、ネットワークの効率性に大きな影響を与える可能性があります。

この「効率性」は、通信時間の使用を意味します。ステーションによる通信の開始または終了がより迅速になれば、他のステーションが使用できる通信時間が増えます。前述のように、802.11b は、2.4 GHz で実装された最初のプロトコルの一つです。今日では、802.11b が、他のすべての Wi-Fi プロトコルのなかで唯一の例となっています。これは、802.11b が、コーディングと変調の両方の方式に関して、以降に批准された他のすべてのプロトコルとまったく異なるためです。

802.11b、a、および g は、グループとして、すべてが 800 ミリ秒の広いガード インターバルを使用していました。ガード インターバルとは、送信される無線記号（文字）が通信時に衝突することを防ぐための、それらの記号間の時間間隔です。802.11n および 802.11ac にはオプションのショート ガード インターバルがありますが、実際には、すべての製品がこのオプションを実装しています。802.11n のデータ レートの表（表 3-1：802.11n の MCS 1 ～ 23 のデータ レート）で、ショート ガード インターバルによって提供されるメリットを確認できます。これらは非常に重要です。

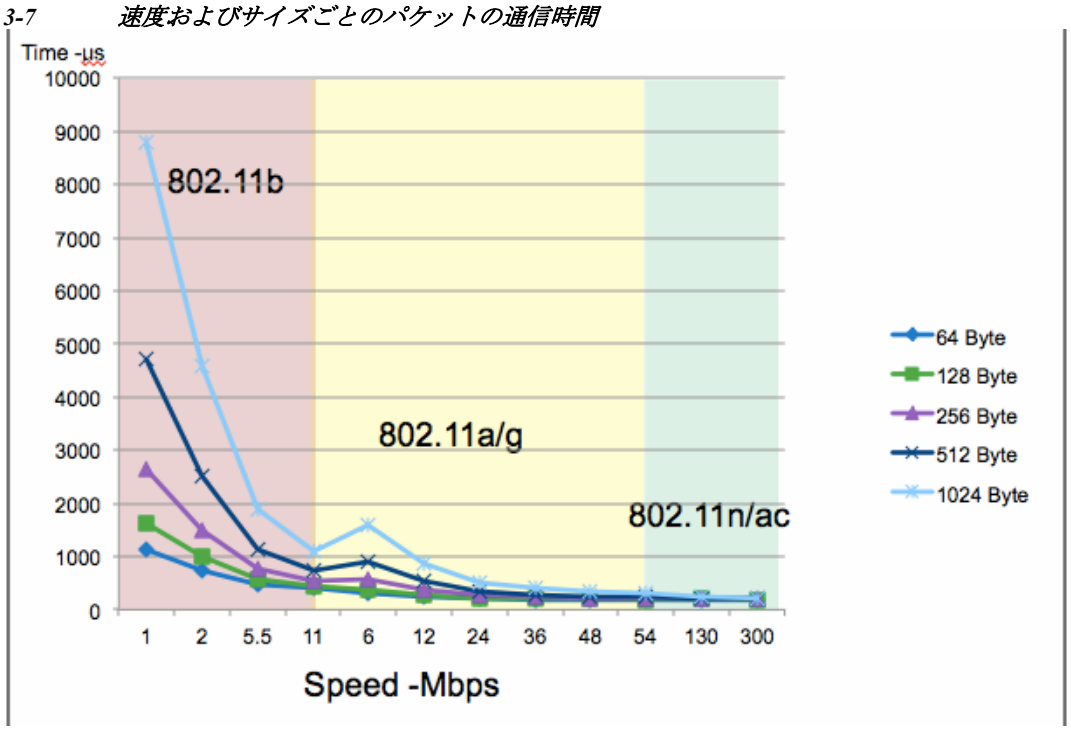
802.11n および 802.11ac は、ブロック ACK（ブロック確認応答）も提供します。これは、パケットの大きなブロックをすべて一度に確認応答することを可能にして、効率性を大きく向上させます。レガシー プロトコルはすべて、パケットの送信と応答の取得を 1 つずつ行います。これは、現在の規格ではほぼ不要になった信頼性のために、非常に多くのフレームをトランザクションに追加します。

たとえるならば、ゴルフ カートには自動車と同じように 4 つの車輪と 1 つのハンドルがありますが、それでは F1 レースに出場できないようなものです。この例の結論は明らかですが、制限なしの Wi-Fi ネットワークでは同様の状況が発生します。

次の図 3-7では、無線で異なるサイズのパケットを使用する異なるプロトコル規格およびデータレートの通信時間要件を比較しています。この図は、集約によるメリットが実現される前の、パケットごとに消費される通信時間（マイクロ秒単位）を示します。802.11n または ac の控えめの速度でも、802.11b が 1024 バイト パケットを 1 つ転送する前に 20 の 1024 バイト パケットを転送できることが、容易に見て取れます。

（注）　より低いデータ レートでは、特定のパケット サイズに必要な通信時間が長くなります。このため、毎秒の対応可能なデータの総量が減少します。結果として、使用可能な帯域幅が減少します。

図 3-7　速度およびサイズごとのパケットの通信時間



ネットワーク設計者の関心事項は、すべてのユーザが使用できるサービスを提供することです。幸いにも、今日では、全般的に見て、ネイティブ 802.11b またはレガシー プロトコルに関する「実際の」要件が存在する環境はほとんどありません。

Cisco WLC には、大半の一般的な速度および必要な速度の実装に使用できるいくつかのオプションがあります。適切に調整されたネットワークを一から実装するために必要なものを確実に理解できるように、さまざまなネットワーク タイプと決定上のポイントについて後で詳しく説明します。

DFS チャネルとは何か、またそれを使用する必要はあるか

5 GHz で使用できるチャネルの多くは、DFS チャネルと呼ばれます。DFS とは Dynamic Frequency Selection（動的周波数選択）の略で、TPC（送信電力制御）とともに、UNII-2 および UNII-2e 帯域（チャネル 52 ～ 144）での動作時のレーダーの共存緩和（すなわち、検出と回避）を定義します。これらのメカニズムは、802.11 規格の改訂版で詳しく規定されています。

802.11h 規格は、5 GHz 帯域を合法的に使用するプライマリ ユーザでもあるサテライトおよびレーダーへの干渉などの問題を解決するために策定されました。プライマリ ユーザは、UNII-2 および UNII-2e の周波数範囲よりも優先されます。これは、この周波数の使用条件としてプライマリ ユーザに干渉しないための Wi-Fi の役割です。この規格は主に欧州の規制に対処するために導入されましたが、今日では世界の他の多くの地域でも、Wi-Fi で使用可能な 5 GHz スペクトルを増やすという同じ目標を達成するために使用されています。

2004 年に、米国は、802.11h 認定を必要とするルールによって UNII-2e（「e」は「拡張」を表す）帯域にチャネル 100 ～ 140 を追加しました。これにより、この範囲の 5 GHz 周波数のプライマリ ライセンス ユーザと問題なく共存することが可能になりました。欧州では、これらのチャネルは、現在使用可能な5 GHz スペクトルのほとんどに当たります。欧州では、ルールとメカニズムの問題が解決される前は、5 GHzの 4 つのチャネルのみに制限されていました。同じ頃、米国には合計 13 のチャネルを使用できる UNII-1、2、および 3 がありました。

ライセンス付与された帯域のユーザに干渉しないための要件は、次のように非常に単純です。

1. Wi-Fi 機器は、レーダーおよびサテライトのエミッションを検出できる必要がある。
2. この範囲内のチャネルを使用する前に、「チャネル マスター」（インフラストラクチャ AP）は、まず 60 秒間リッスンし、チャネルがレーダーによって使用されていないことを確認する必要がある。
3. レーダーの信号が検出された場合、Wi-Fi チャネル マスターとそれに関連付けられたすべてのクライアントは、チャネルをすぐに放棄する必要があり、30 分間（レーダー エミッションが検出されない場合に Wi-Fi を使用するためにチャネルが再び未使用状態になるための時間）は戻ることができない。

2004 年前半、UNII-2e チャネルは米国のネットワーク管理者たちの間で不評を買いました。当初、クライアントでの新しいルールの採用が遅れました。そのため、これらのチャネルをインフラストラクチャで使用すると、一部のクライアントが使用できないチャネルを誤って設定してしまう可能性がありました（一部のユーザは実際に誤って設定しました）。これにより、それらのクライアント タイプに対するカバレッジホールが生まれました。また、実稼働ネットワークでの DFS 動作（スキャンの必要性とそれに要する時間）に関する過度の懸念もありました。その懸念とは、DFS がレーダーを検出した場合、チャネルが変更され、その 1 分後に送信が再開されますが、これが中断状態のように見えることでした。しかし、RRM によって AP が最初は非 DFS チャネルに配置されるため、この動作は中断を伴うものではありません。チャネルは 30 分間ブロックされ、必要なリスニング時間をクリアするバックグラウンド スキャンにより、再び RRM で使用できるようになります。チャネルが使用可能になれば、ユーザはそれを使用するか、現在のチャネルにとどまるかを、そのどちらがクライアントに適しているかを基準に選択できます。

これらのチャネルおよび 802.11h ロジックが追加されてから 10 年が経過しました。欧州では、DFS によって 5 GHz の Wi-Fi の可能性が引き出され、その可能性は現在も伸ばされており、大きく開花しようとさえしています。さまざまなクライアント ベンダーが存在しますが、その大半が、クライアントに必要な追加のロジックがないことから DFS チャネルを明確にサポートしています。

空港や積み出し港から 5 マイル（約 8 km）以内の場所にいて、懸念がある場合は、シスコの AP によるチャネル範囲のモニタリングによって評価してください。シスコは、DFS の動作と柔軟性のための認定ハードウェア モデルおよび機能で業界をリードしています。チャネルのモニタリングにより、干渉の可能性を認識し、影響を受けるチャネルを特定することができます。

サイトの調査

サイト調査は重要なツールです。これにより、周囲の運用者を確認できます。また、さらに重要なこととして、目的のカバレッジ ゾーンに干渉する場所とその度合いを確認できます。設置場所、既存のケーブル設備、インフラストラクチャ要件、アーキテクチャ上の不審点などを特定し、特定のアプリケーションに必要なカバレッジを得るための計画を策定することもできます。RF は周囲の物理環境と相互に作用し、すべての建物およびオフィスは異なっているため、各ネットワークもある程度異なったものになります。残念ながら、Wi-Fi に関しては、あるサイズですべてに対応できるということはありません。ただし、導入タイプごとの推奨事項があり、発生する可能性のある事態を一般化することは可能です。サイト調査をしばらくの間実行していない場合は、調査しないことを決める前に、次の点について、最後に調査した後に変化した内容に留意してください。

1. プロトコルおよび無線技術
2. ユーザのネットワーク使用方法（あらゆる人が、ほとんどあらゆることに使用すると考えられる）
3. ネットワークがサポートするクライアントの数（今日のユーザは少なくとも 2 台、多くの場合はそれ以上の数のデバイスを所持するため、ユーザ数よりもはるかに多いと考えられる）
4. ネットワークの主要な使用目的（初期計画および導入時から変化している可能性が非常に高い）

初期の WLAN 設計では、あらゆる場所の数人の一時ユーザの信号を取得するためにカバレッジが重視されていましたが、今日の WLAN 設計では、ユーザ数が増えているためにキャパシティがより重視されており、ネットワークに要求されるものが飛躍的に増加しています。キャパシティ設計では、セルの帯域幅を共有している多数のユーザを管理するために、より近接した位置により多くの AP が必要とされます。高まる配置密度も計画に入れる必要があります。

ユーザが独自に調査と計画を行う場合は、ツールが重要です。オンラインでまたはダウンロードして使用できる複数の無料ツールが存在します。ただし、専門的な結果が必要な場合は、専門的なツールを使用する必要があります。

無料ツールは、より小規模の、あまり複雑ではないプロジェクト向きのシンプルなソリューションを提供します。しかし、複数のフロア/複数の建物敷地でユビキタスなマルチメディア カバレッジを提供する必要がある場合は、成功させるために必要な要因のバランスを取ることができる優れたツールが必要になります。計画ツールは、今日使用されている無線技術およびアプリケーションとともに進化しました。設計要素およびアプリケーションに関する知識は、優れた計画を生み出すために必要です。

Cisco Prime Infrastructure には計画ツールが組み込まれており、CPI と多数の主要な調査および計画アプリケーション（Ekahau ESS、Airmagnet Pro Planner、Survey など）の間でマップと計画をインポートおよびエクスポートできます。

サイト調査の詳細については、『Site Survey Guidelines for WLAN Deployment』を参照してください。

今、802.11ac に関するサイト調査を完了すれば、ネットワークの拡大と継続的な進化につれて繰り返し使用できる優れた情報を得ることができます。これを部分的にまたは全体として委託すべきかどうかは、プロジェクトの規模と Wi-Fi に関して持っている知識のレベルによって決まります。

RF 導入の計画

WLAN カバレッジのさまざまな導入の種類

ワイヤレス ネットワークの設計で設定する WLAN カバレッジの規模は、主として、必要なクライアントの使用状況および密度によって決まります。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つつ、優れたクライアント ローミングおよびスループットをサポートするように展開する必要があります。ワイヤレス ネットワークは、データ専用、音声、ビデオ、およびロケーション認識型サービス、または、今日ではより一般的になっているこれらの組み合わせに対して導入できます。優れた堅牢なキャパシティベース カバレッジをそれぞれ大規模に記述するという要件のために、現在では、これらのアプリケーション タイプ間の相違は非常に小さくなっています。ロケーション認識型サービスでは、優れたロケーションの三角測量と Hyper-Location 技術に関するガイドラインのために、いくつかの AP 配置基準が追加されます。リアルタイム マルチメディア（音声およびビデオ）アプリケーションには、双方向ライブ実装に関する異なる遅延要件があります。ただし、全般的には、すべてのアプリケーションが、特定のエリアで期待されるユーザ数に関してアプリケーションを実行可能にするために必要な最小限のカバレッジ レベルを記述します。

キャンパスや企業での配備の大半については、カバレッジとキャパシティが主な関心事項であり、容易に達成できます。ショッピング モールやアパートなどの高密度クライアント実装または高干渉ロケーションの場合は、外部アンテナなどの追加機器を適切に導入して拡張する必要がある場合があります。アプリケーション固有のガイドライン、推奨事項、および設定の詳細については、次のガイドに記載されている詳細な情報を参照してください。

- 『Best Practices—Location-Aware WLAN Design Considerations』
- 『Microsoft Lync Client/Server in a Cisco Wireless LAN』
- 『Cisco Jabber and UCM on a Cisco Wireless LAN』
- 『Application Visibility and Control Feature Deployment Guide』（8.1）
- 『Wireless LAN Design Guide for High Density Client Environments』
- 『Cisco Wireless Mesh Access Points, Design and Deployment Guide, Release 8.1』

カバレッジ要件

ほとんどのアプリケーション固有カバレッジ ガイドラインでは、設計上の推奨事項として、適切な動作に必要なセル エッジでの信号レベルまたはカバレッジが示されています。これは、通常、-67 dBm などの負の RSSI 値です。この数値は -92 dBm のノイズ フロアで 25 dB の優れた信号対雑音比を前提としていることを理解することが重要です。ノイズ フロアが -92 dBm を超える場合、-67 dBm では、アプリケーションの機能を実行するために必要な最小データ レートをサポートするために信号が十分ではない可能性があります。

ロケーション認識型サービスの場合は -67 dBm の仕様に従ってネットワークを展開することで問題ありませんが、ロケーション認識型アプリケーションにとって重要なことは、クライアントがネットワークをどのようにヒアリングするかではなく、ネットワークがクライアントをどのようにヒアリングするかです。ロケーション認識型の場合、クライアントを計算に含めるには、3 個以上の AP において -75 dBm 以上のレベルでクライアントをヒアリングする必要があります（- 72 が推奨設計の最小値）。

クライアントは、カバレッジを計画する際の重要な考慮事項です。今日のクライアントは、あらゆる形とサイズで提供されており、結果として、特定の RF 信号に関するそれらのオピニオンに基づいて個々の実装が大きく異なる可能性があり、実際に異なっています。たとえば、セル エッジで調査に使用しているラップトップには -67 dBm と表示され、タブレットには -68 dBm と表示され、スマートフォンには -70 dBm と表示される可能性があります。これらはすべて非常に異なるオピニオンであり、各個人が使用するローミングおよびデータ レートに影響を与えます。このさまざまなオピニオンに対応するためのオーバービルディングにより、問題の発生しない設置が保証されます。測定する際は、アプリケーションをサポートするデバイスを使用することが最善のアプローチです。使用しているスマートフォンでは調査ツールよりも一般に 5 dB 低くなることを理解すると、設計のための優れたルール（調査ツールによる測定値がどのようなものであっても 5 dB 加算または減算するなど）を策定できます。その後、結果としての実装をテストし、調整します。

高密度クライアントのカバレッジ要件

ネットワークの成功を大きく左右する要因の一つは、高クライアント密度エリアです。前述のように、AP のセル境界に含まれるすべてのクライアントは、そのセルの潜在的な帯域幅（通信時間）を共有します。これを示す単純な計算式により、この概念をわかりやすく示すために「555」のルールを使用します。5 GHz で 1 Gbps を 200 の同時クライアントが均等に共有する場合、各クライアントは 5 ミリ秒の通信時間を要し、5 Mbps を受信します。

1000 Mbps/200 = 5 Mbps

1 秒/200 = 5 ミリ秒

実際には、セル全体にわたるさまざまな条件のために、より多くのクライアントでより多くのオーバーヘッド、衝突、およびエラーが発生します。そのため、一部のクライアントは 5 Mbps 超を得ることができますが、一部のクライアントではそれ以下になります。これは、セルのみの平均的な状況です。同様の条件下での優れた平均セル スループットは、得られるマイレッジの正確な予測を提供します。

より多くの帯域幅を提供することは、計算式を変更することと同じくらい単純であり、2 ～ 5 Mbps で 100 のクライアントをサポートする必要がある場合は、クライアント間で共有するより多くの帯域幅を提供するために、異なるチャネルの別の AP が必要になります。異なるチャネルを使用する限り、AP を追加して追加のキャパシティを得ることができます。チャネルの最初の再使用が、そのチャネルを使用して別の AP によってヒアリングされない限り、既存のチャネルを再使用して、より大きな規模でこれを達成することができます。

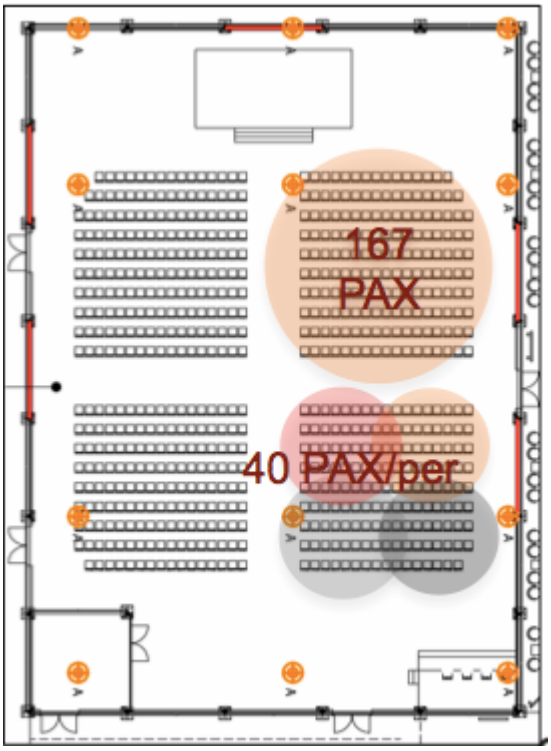
同じチャネル上の 2 個の AP が相互にヒアリングできる場合、それらはチャネルを均等に共有します（それぞれ均等にビジー状態であると仮定）。802.11 規格では、これを保証するために、競合メカニズムが仕様に組み込まれています。ただし、両方のセルがチャネルを共有（それぞれ 50 % の通信時間を取得）しているため、実際にはこれらのユーザのために帯域幅を増やしておらず、管理トラフィックを実質的に倍増させる 2 個の AP があるため、使用可能な通信時間がさらに減少します。

使用可能なチャネルが 3 つしかない 2.4 GHz では、選択できるチャネルが多い 5 GHz よりもはるかに早く、チャネルの再使用が問題になります。伝達特性も関係します。2.4 GHz では 5 GHz よりも遠くからヒアリングされるため、2.4 GHz オプションを使用したより狭い物理エリアで、再使用の数がさらに制限されます。

5 GHz では複数のチャネル幅を検討できます。チャネル幅の選択肢が広いほど、全体的なチャネルの数を減らすことができます（ただし、引き換えに、セルあたりのキャパシティが大きくなります）。

より大きなセルはより多くのユーザをカバーします。特定の物理エリアで帯域幅を増やすために、より小さなセルは、より大きなキャパシティを生み出すことになります。次の図では、各座席区画に 167 の座席があり（図 3-8 では座席が PAX として表されています）、1 個の AP で区画全体をカバーできます。または、より小さなセルを設計することにより、同じエリアで使用できる 4 個の AP を配置し、使用可能な帯域幅を 4 倍に増やすことができます。

図 3-8　　ユーザとセル密度



ほとんどの企業の配備では、全方向性の内部アンテナ AP を使用して、より高密度の会議室などを適切に処理しています。シスコの RRM は、これを機能させるために必要なチャネルと電力を処理します。過度に多い AP が 過度に近接している特定のポイントでは、RRM は、可能な最適効率を実現するために設定しますが、使用可能なスペクトルが存在する必要があり、それがない場合は何もできません。AP の電力のみを大幅に削減することができ、その場合、全方向性アンテナパターンが他の隣接 AP をヒアリングすることで、ユーザ エクスペリエンスが影響を受けます。AP あたり 2500 平方フィート以上でのカバレッジ レベルは、20/40 MHz チャネルを使用する場合 5 GHz で良好です。2500 平方フィートを下回る 2.4 GHz のセル密度に関する要件の場合は、AP の送受信パターンを物理的に制限し、有用なより小さいセルを得るために、指向性アンテナが必要になると考えられます。

高密度クライアント/AP 環境を管理および設定するために特別に開発された多数の機能が存在します。これらは、HDX（高密度エクスペリエンス）と呼ばれる機能グループに含まれます。各機能の詳細については、次の HDX 導入ガイドを参照してください。

『高密度エクスペリエンス（HDX）導入ガイド』

ローミングおよび音声のカバレッジ要件

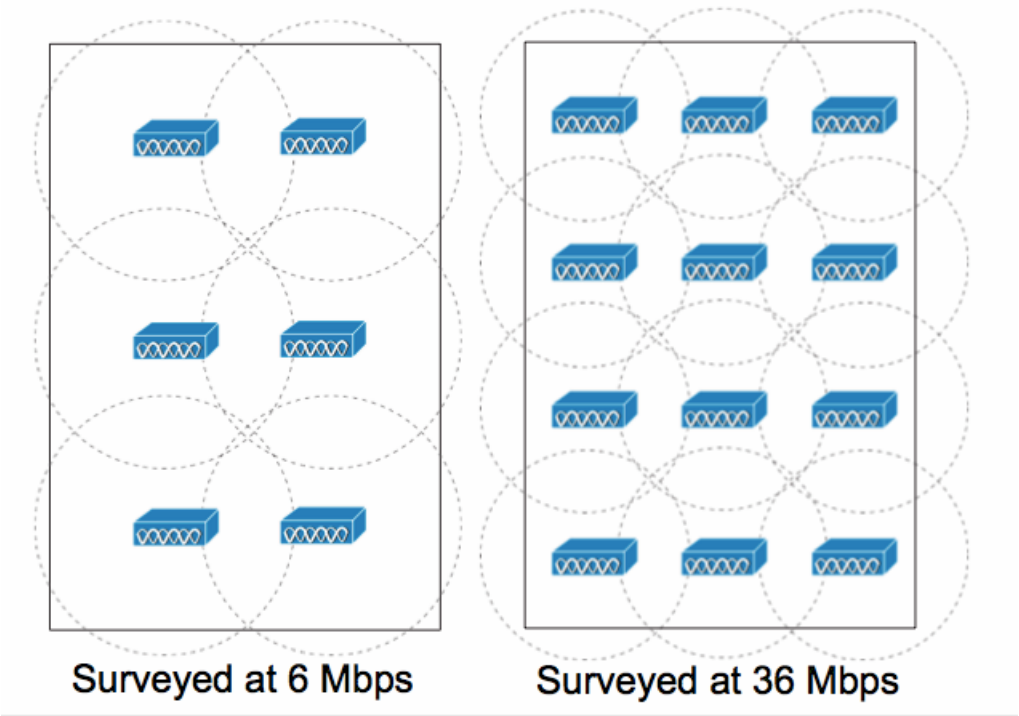
クライアント ローミングにより、クライアントは、サービス/カバレッジの中断を最小限に抑えながら、ある AP のカバレッジ ゾーンから別の AP のカバレッジ ゾーンに移動できます。これは、モビリティの非常に重要な部分です。これを有効にするには、考慮すべき要素が多数あります。たとえば、クライアントがそのアソシエーションおよび認証を AP 間で移行させる方法や、それにかかる時間を考慮する必要があります。頻繁に見落とされる点は、ネットワーク設計自体です。クライアントがローミングするには、ローミング先となるものが存在する必要があります。クライアントが 1 つのセルのカバレッジから正常に離れ、遅延なしに別のセルのカバレッジ内でアソシエーションを確立するには、セルが適切なカバレッジによってオーバーラップしている必要があります。オーバーラップが小さすぎると、「スティッキ」クライアントを助長することになります。つまり、クライアントが、別の AP のカバレッジ エリアに移動した後も元の AP を保持し続けます。

ネットワーク カバレッジを設計する場合は、必要な信号範囲で取得しているオーバーラップの総量を考慮してください。オーバーラップは、カバレッジ エリア全体の 10 ～ 15 %（音声の場合は 15 ～ 20 %）である必要があります。会話はリアルタイムで行われるため、音声には特に影響があります。カバレッジが切れると、音声が途切れ、場合によっては通話が中断されます。オーバーラップを計算する簡単な方法は、-67 dBm に到達する AP からの距離を測定し、その距離を 1.4 倍（15 ～ 20 % の場合）または 1.3 倍（10 ～ 15 % の場合）にして、それが次の AP までの距離であるかどうかを確認します。

データ レートも重要です。使用可能なセル サイズは、データ レートが低くなると増加し、データ レートが高くなると減少します。より高いデータ レートは、より高い SNR を必要とします。また、ノイズ フロアは論理的に一定であるため、クライアントが信号（AP）に近づくほど、SNR が高くなり、結果としてデータ レートが高くなります。設定で最小データ レートを適用できます。その場合、クライアントが特定のデータ レートをサポートできなくなると、そのクライアントは移動する必要があります。

図 3-9 は、セルのオーバーラップと、データ レートがセル サイズに与える影響を示しています。

図 3-9　セル密度と異なるデータ レートでのオーバーラップ



適切な物理設計により、物理レイヤでのローミングが可能になり、サポートされます。クライアントのみがローミングするタイミングを決定します。また、この決定はクライアントによるネットワークの監視に基づいて行われます。クライアントがネットワーク インフラストラクチャの監視に基づいてより適切な決定を行うために特に役立つように、802.11 仕様に複数の改訂版が追加されました。ローミングと優れたローミング移行を実現するシスコのハードウェア/ソフトウェアの設定の詳細については、次のガイドを参照してください。シスコでは、802.11r、802.11k、および 802.11v をサポートしています。これらは、クライアントが適切な決定を行う機能を支援するとともに、設計目標を実現するためにインフラストラクチャからのいくつかの制御を可能にします。

- 『高密度エクスペリエンス（HDX）導入ガイド』（「最適化ローミング」を参照）
- 『802.11 WLAN Roaming and Fast-Secure Roaming on CUWN』
- 『802.11r, 802.11k, and 802.11w Deployment Guide, Cisco IOS-XE Release 3.3』

ロケーション認識型のカバレッジ要件

ロケーション認識型展開は、他のタイプと少し異なります。この展開の目的は、クライアント、タグ、および IOT センサーが特定のマップ上に存在する文脈において、それらの適切なロケーション解決を提供することです。この情報は、複数の AP によって取得される最も基本的な形式のクライアント RSSI 測定値から得ます（クライアントの位置を三角測量するために少なくとも 3 個の AP が必要です）。AP を展開するために選択するパターンは、クライアントの「位置」を正確に特定するネットワークの機能には大きな影響をおよぼす可能性があります。

適切なロケーション解決のために、AP は、境界や角を定義する AP とともに互い違いのパターンでレイアウトされます。両方のセクションの中央に引いた直線上の AP を使用してカバレッジを取得できます。ただし、これでは、すべてのロケーションのクライアントをヒアリングし、三角測量するために十分な AP が提供されません（3 個の AP が必要であることを思い出してください）。このフロアに関するカバレッジおよびキャパシティ要件では、最初から多数の AP が必要です。このため、非常に高い確率で、「適切なロケーション計算を行うために必要なものをすでに持っている」というカバレッジ要件が存在します。

図 3-10　2.4 GHz の単一フロア ロケーション AP 配置の例

「Best Practices—Location-Aware WLAN Design Considerations」は必読の章です。また、設計の物理要件は変化していないため、依然として非常に大きな関連性があります。『Wi-Fi Location Based Services 4.1 Design Guide』は、その全体が理論の優れた参考書となっています。特に、最初の章である「Location Tracking Approaches」によって技術をよく理解できます。

フレキシブル ラジオ アーキテクチャ（FRA）無線とカバレッジ要件

シスコの最新のイノベーションであるフレキシブル ラジオ AP モデル 2800/3800 は、従来のデュアルバンド無線のいくつかの課題を解決するように設計されています。上記の各カバレッジ シナリオでこれらの無線を使用すると、ソリューションが向上します。

高密度は、単一のアクセス ポイントから 2 つの独立した 5 GHz チャネルを可能にする 2800/3800 のデュアル 5 GHz の能力に影響されます。

- 内蔵アンテナ モデルは、マクロ/マイクロ セルまたはセル内のセルとして実装されます。FRA RRM ロジック（「RRM」の項で詳しく説明します）は、2 つのセル間でクライアントをバランスさせるロジックも提供します。これにより、セル境界内の帯域幅が倍増します。2800/3800 I モデルのセル境界は、古い 2700/3700 および 2600/3600 モデルとほぼ同じサイズです。

- E モデルまたは外部アンテナ モデルは、2 つの 5 GHz マクロ セルを提供できます。これにより、同じイーサネット ケーブル/スイッチ ポートを使用して 2 つの 5 GHz セルを獲得する実装が可能になります。2 番目のアンテナとそれに取り付ける Dart コネクタが必要ですが、両方合わせても追加のアクセス ポイントとスイッチ ポート（さらにアンテナが必要になります）よりはるかに安く上がります。これは特に既存の高密度エリアを更新する場合に便利です。ほとんどの場合、AP 以外のすべてを再利用でき、5 GHz のキャパシティを劇的に増やせるからです。

音声カバレッジ：AP2800/3800 はどちらも RRM の FRA（フレキシブル ラジオ アサインメント）アルゴリズムに参加します。FRA は、2.4 GHz と 5 GHz の正しいバランスを計算し、2.4 GHz 無線の過剰利用を防止します。一般に、音声は 5 GHz でのみ実装する必要があります。FRA を使用すると、5 GHz の高密度と 2.4 GHz 無線の適切なサイズと密度を同時に達成できるため、この実装に大いに役立ちます。FRA には、フレキシブル インターフェイスをモニタリング ロール（両方の帯域）に配置できるようにすることによって 5 GHz の過剰密度を防止する機能が組み込まれています。これにより、RF メトリック（RRM 観測、ロケーション情報）の分解能が高まります。

ロケーション サービス カバレッジに関する考慮事項：AP3800/2800 モデルはどれもロケーション解決を大幅に向上させます。I/E/P モデルでは、フレキシブル ラジオをモニタ ロールに変換することで両方の帯域での滞留時間を大幅に増やし、ロケーション アルゴリズムの入力をより多く生成します。これも FRA アルゴリズムによって管理されます。FRA は、2.4 GHz を正しいサイズに設定し、冗長無線をモニタ モードにする機能を使ってロケーション解決を実際に向上させます。

（注） 非フレキシブル AP では、過度の 2.4 GHz 無線に対する唯一の解決策は無線を完全に無効にすることです。これを行うと、2.4 GHz の可視性とロケーション解決が低下します。2800/3800 H モデルは、AoA 計算をサポートするアンテナを備えた専用の AP で、ロケーション解決と精度を大幅に向上させることができます。H モデルはまた、独自の BlueTooth 無線とアンテナをホストして BLE アプリケーションをサポートします。このため、あらゆるロケーション ユース ケースに対応できるクラス最高の無線です。お使いのアプリケーションが非常に精度の高いロケーション結果を必要としている場合は、ぜひこの無線を検討してください。

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設計の選択は、AP の配置/カバレッジの結果を決めるうえで密接に関連しています。これらの 2 つの内容によって、環境内の所定の場所のどこでどれくらい電波が強いのかが決まります。必要なカバレッジ エリアを作り出すのに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 の使用を推奨します。詳細については、本書の *RRM* に関する項を参照してください。

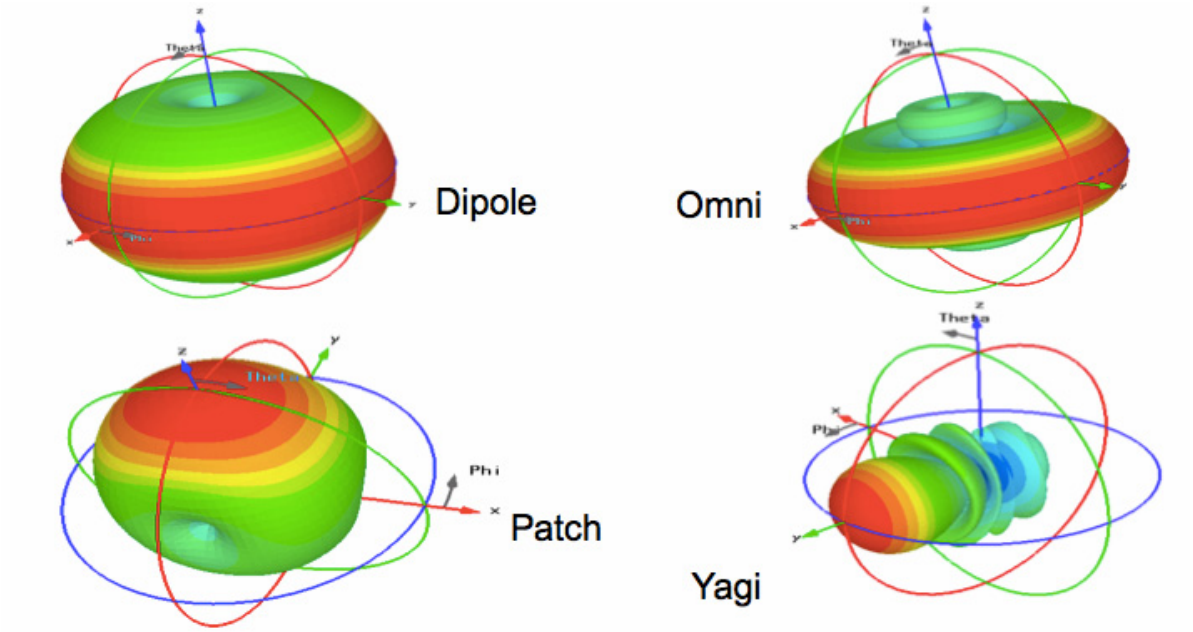
アンテナは、無線システムに対して、以下の 3 つの基本的な特性を示します。

- 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（等方性）のアンテナと比較して示すための尺度。ゲインは受信信号にも影響を与えます。レシーバに提供される信号を増大させることにより、より弱いクライアント デバイスを補助することができます。
  - 前後比（FTB）：ゲインの反対は信号の拒否です。アンテナのゲインの反対方向はアンテナの焦点よりも感度が低くなります。この特性を利用して、たとえば、アンテナの背後の不要な信号からセルを隔離することができます。

- 指向性：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。高い指向性を持つアンテナは、非常に厳格なビームパターンを生成します。焦点のエリア外では信号が急速に減衰します。これにより、より多くのセルを同じ物理スペースに、干渉なしに配置できます。
- 偏波：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、電波は垂直に偏波されます。

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。ただし、アンテナは AP の耳と口の両方であるため、特定のアンテナの特性は送受信の両方に作用します。異なる目的に使用できるように、多数の異なるアンテナ設計が存在します。比較的よく知られている設計の一部を、次の図 11 に示します。

図 3-11　アンテナ設計のタイプ



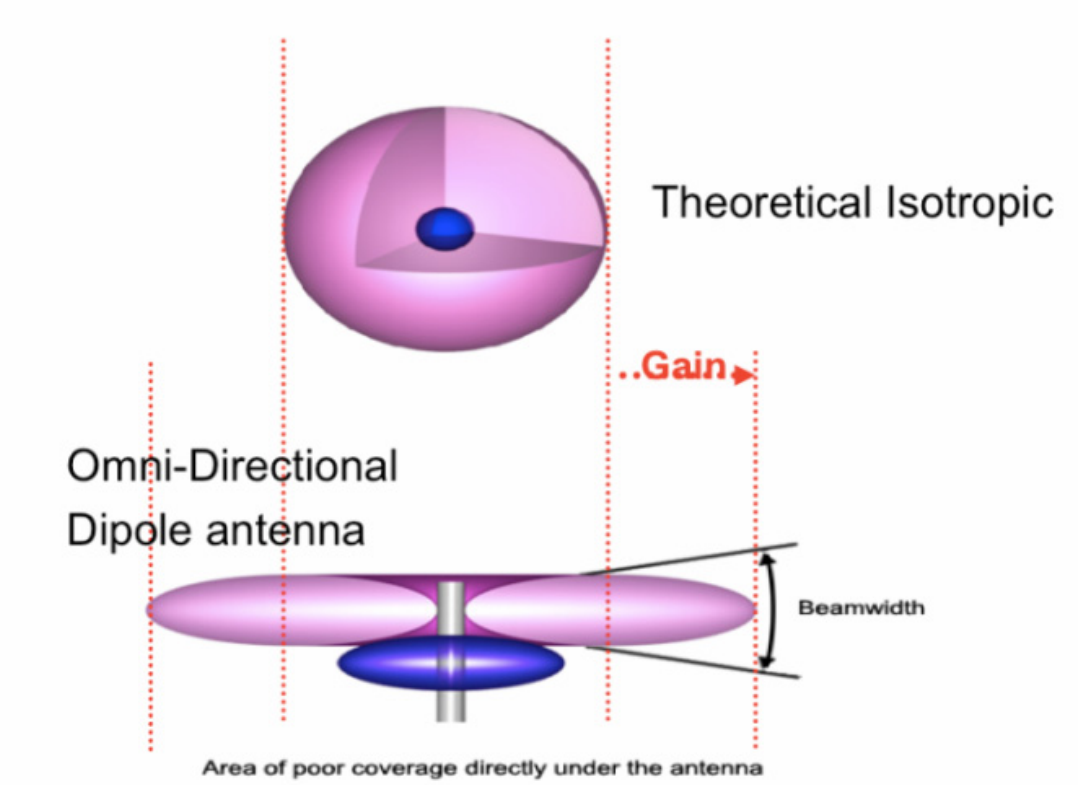
ゲインおよび指向性によって、範囲、速度、および信頼性が決まります。偏波は信頼性とノイズの分離に影響します。

アンテナの選択の詳細については、『Cisco Aironet Antennas and Accessories Reference Guide』を参照してください。

全方向性アンテナ

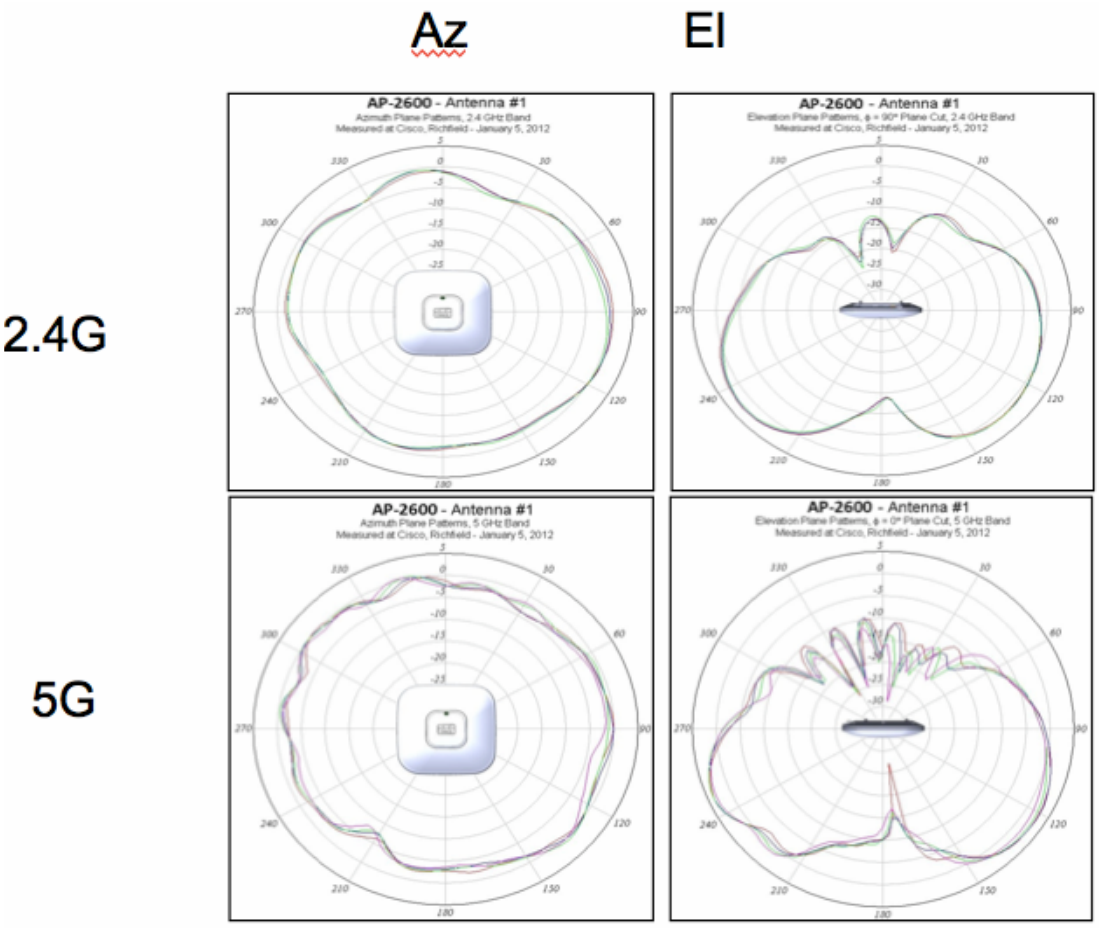
全方向性アンテナは、等方性アンテナと比較すると、放射パターンが異なっています。等方性アンテナは理論上のもので、物理的なアンテナはすべて等方性アンテナとは異なります。等方性アンテナの放射パターンの形におけるいかなる変化もゲインとして発生し、方向性が増大します。全方向性のダイポール アンテナは、水平面では 360 度、垂直面では 75 度のほとんど対称的な放射パターンを持ちます（ダイポール アンテナが垂直に立てられていることを前提としています）。全方向性アンテナの放射パターンは、通常、ドーナツのような形をしています。このため、方向性を持ちます。特定の全方向性アンテナの定格ゲイン（dBi 単位）が大きいほど、エネルギーが集中化し（通常、垂直面において）、それが方向性になります。次の図 12 に示されている等方性と全方向性のダイポール アンテナの比較を参照してください。側面からの図であることに注意してください。

図 3-12　　等方性アンテナと全方向性アンテナ



AP 1140 以降の最新の内部アンテナ AP モデルは、複数のトランスミッタとレシーバを備えた内部アンテナ スタブを使用します。単純なダイポール アンテナとは異なり、これは、改善されたドーナツ形のパターンを生成します。次のアンテナのプロットでは、仰角平面と、エネルギーが主に図 13 の下方に集中している様子に注意してください。

図 3-13　Cisco AP 2600i の 2.4 GHz と 5 GHz の放射パターン



これにより、AP の背後（ほとんどの設置で天井に向けられている部分）が最も感度が低くなります。

全方向性アンテナは、ある程度は、よく機能し、導入も簡単です。増大するキャパシティ要件に対応するために AP の密度が高まっている場合は、自己干渉によるチャネル使用率の増加が見られます。これは、最大カバレッジに合わせてアンテナ パターンが設計されているために発生します。AP あたり 3000 ～ 6000 平方フィート（約 280 ～ 560 平方メートル）のカバレッジを内部アンテナで管理でき、カバレッジ要件が非常に小さいかこれより高密度である場合は、指向性アンテナを考慮する必要があります。

指向性アンテナ

指向性アンテナは全方向性アンテナとは異なり、エネルギーを特定の方法で集中させ、異なるカバレッジの目標を達成します。一般に、指向性アンテナは、特にゲインのため（電力を増大させるため）に使用されると想定されています。このアンテナはその目的でも使用され、より大きな距離を実現しますが、より多くの場合に、Wi-Fi において送受信セルのサイズ（と形）を制御するために使用されます。

現在のシスコの屋内 AP（3600e、2600e、3700e、2700e）では、アンテナの選択肢はすべて、異なるカバレッジ距離用に設計されたデュアルバンド（各アンテナが 2.4 GHz と 5 GHz をカバー）のパッチ タイプ アンテナです。最も一般的なものは次の 3 つです。

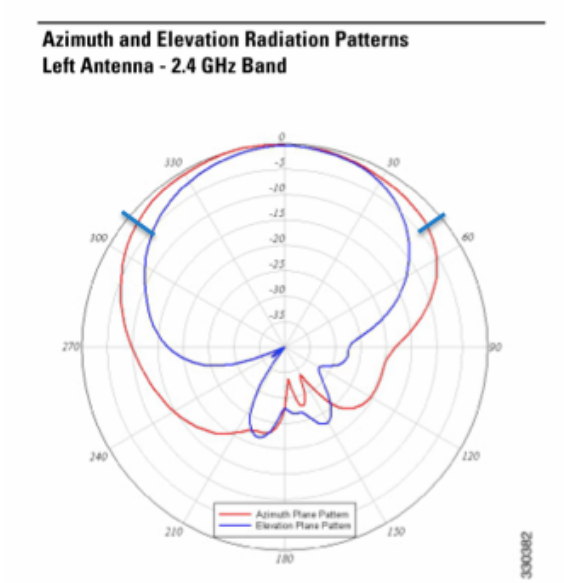
図 3-14　シスコの高密度用途向けの指向性アンテナ

Photo	Name/Part No.	Beam	Use Case
	Dual-Band Stadium Antenna 3702p + AIR-ANT2513P4M-N	2.4/5GHz 30°/30° Az 30°/30° Elev	Primary overhead coverage (10-30 m)
	Dual-Band Patch Antenna 3702e/p + Air-ANT2566D4M-r	65°/65° Az 65°/65° Elev	Augmentation and medium distance HD coverage (5-10m to client)
	Dual-Band Patch Antenna 3702e/p + AIR-ANT2566P4W-R	105°/125° Az 70°/60° Elev	Augmentation and short-distance HD coverage (<5m to client)

各アンテナは特定の目的を念頭に置いて設計されています。アンテナの選択に関して考慮すべき項目の 1 つは、ビーム幅です。ビーム幅はアンテナのカバレッジ エリアを記述します。ただし、そのカバレッジのエッジがどれほどハードまたはソフトかは記述しません。このため、プロットのアンテナのパターンを確認する必要があります。

次のプロットは、AIR-ANT2566D4M-R アンテナの 1 つのアンテナのものです。このアンテナは、一般的なエリアに優れたカバレッジを提供するように設計されています。2.4 GHz でのこのアンテナのビーム幅は 105^{o} X 70^{o} であり、アンテナのピーク ゲインが 3 dB まで下降するポイントを記述します。指向性アンテナで重要なことは、この 3 dB の後に起こることです。次のアンテナ プロットでは、定格ビーム幅で青色の印が付いていることに注意してください。ゲインは、定格ビーム幅の後に鋭角に下降しています。これは、より大きなキャパシティを得るために、より多くの AP を相互により近接させて配置する場合に、何が起こる必要があるかを正確に示しています。

図 3-15　AIR-ANT2566D4M-R アンテナのアンテナ プロット



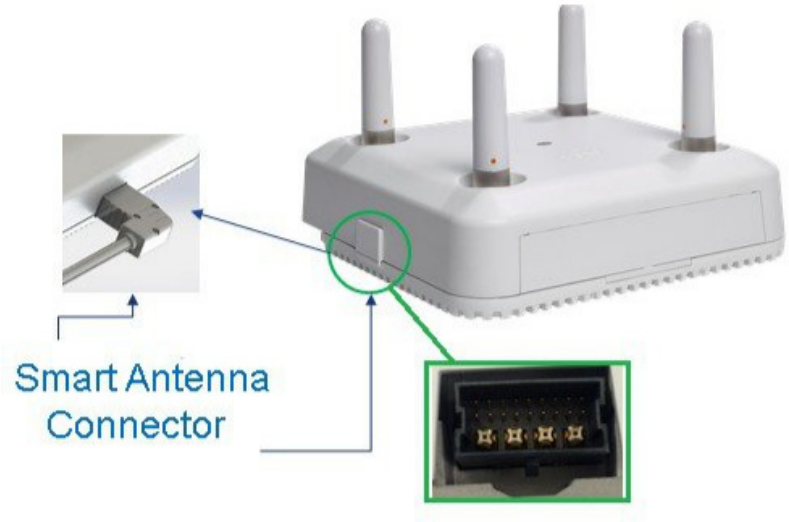
アンテナがヒアリングできない場合、AP に干渉しない可能性があります。2.4 GHz には 3 つのチャネルしかないため、高密度展開でのチャネルの再使用にはすでに問題があります。適切なアンテナを使用すると、セル サイズを縮小し、より多くの無線を相互により近接させ、2.4 GHz ユーザ向けの設計で適切なキャパシティを提供できます。5 GHz にはより多くのチャネルがあります。ただし、20/40/80 MHz のチャネル幅では、より早くチャネルを使用し尽くしてしまい、セルの分離でも問題が多くなります。

指向性アンテナを使用して解決できるその他の問題には、ショッピング モールなどの高干渉環境が含まれます。ショッピング モール内の大半の店舗は何らかの種類の Wi-Fi を設置しており、これが Wi-Fi の干渉を発生させます。指向性アンテナを使用し、AP の耳の焦点を内側に合わせて、アンテナの背後の受信感度を低下させることにより、近隣の店舗から自分の店舗を分離することができます。これは、アンテナの前後比によって発生する現象です。ちょうど、手をカップの形で耳に当てて遠くの音を聞くことと似ています。この動作により、音響エネルギーの焦点が耳の中になりますが、耳への周囲のノイズを遮断することにもなります。このため、信号対雑音比が改善され、音が明瞭に聞こえるようになります。AP に指向性アンテナを配置すると、その耳が焦点を持ち、同じように「ノイズの少ない明瞭な音が聞こえる」ようになります。

新しいアンテナ設計

- 2800/3800 E シリーズの外部アンテナ コネクタは、以前のアクセス ポイントのアンテナ コネクタと同じです。アクセス ポイントをデュアル バンド（2.4 および 5 GHz）動作（デフォルト モード）で使用する場合、動作に違いはありません。RF 範囲とセル サイズは以前の AP 2700 and 3700 シリーズに似ているため、新しいサイト調査を実施する必要はありません。
- 以前の外部アンテナ バージョンとは異なり、新しい 2800 および 3800 シリーズ アクセス ポイントは、デュアル 5-GHz 動作の機能をサポートします。このモードでは、外部アンテナ モデルでスマート アンテナ コネクタを使用する必要があります。なぜなら、追加の 5-GHz 無線は、プライマリ 5-GHz 無線によって使用されるアクセス ポイントで同じ上部アンテナを使用できないからです。
- スマート アンテナ コネクタを取り付けると、XOR 無線（ソフトウェアで無線 0 として定義されている無線）は、その RF をスマート アンテナ コネクタに切り替えます。

- スマート アンテナ コネクタは、使用されているアンテナのタイプを検出でき、16 本のデジタル回線と 4 本のアナログ RF 回線を備えています。



スマート アンテナ コネクタを示す図

スマート アンテナが取り付けられていない場合、ユニットの上のアンテナは Dual Radiating Element（DRE）モードになります。スマート アンテナが取り付けられている場合、XOR（モードに応じて 2.4 または 5 GHz）はスマート コネクタから発信されます。このモードでは、XOR 無線（モニタ モードでない限り）は、1 帯域の 2.4 GHz またはその他の帯域の 5 GH に設定することしかできません。これは Single Radiating Element（SRE）モードです。

アンテナ制御（デフォルトで、スマート アンテナ コネクタが使用されている場合）

スマート コネクタと一緒に設計されている新しいアンテナに加え、RP-TNC コネクタを使用する従来のアンテナもスマート コネクタを使用して 2800/3800e シリーズに取り付けることができます。

シスコ スマート アンテナ コネクタ P/N AIR-CAB002-DART-R

このトピックの詳細については、次の URL にある AP-3800 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_aironet_series_2800_3800_access_point_deployment_guide.pdf

Hyperlocation モジュールを備えた 3600/3700 シリーズを使用したスマート コネクタ

3700 シリーズのスマート アンテナ コネクタは少し動作が異なります。Hyperlocation モジュールが 3600 または 3700 シリーズ アクセス ポイントに取り付けられている場合は、特別なアンテナ アレイを使用してロケーション精度を高めることができます。Hyperlocation アレイは、2800 および 3800 シリーズと互換性がありません。

Hyperlocation 機能の概要

Hyperlocation の概要

Hyperlocation は、最新の Hyperlocation Module と Advanced Security の組み合わせであり、以前の WSSI/WSM: AIR-RM3000M モジュールに代わる製品です。以前のモジュールは、高度な Hyperlocation アンテナ システムに対応しておらず、したがって Hyperlocation をサポートできません。

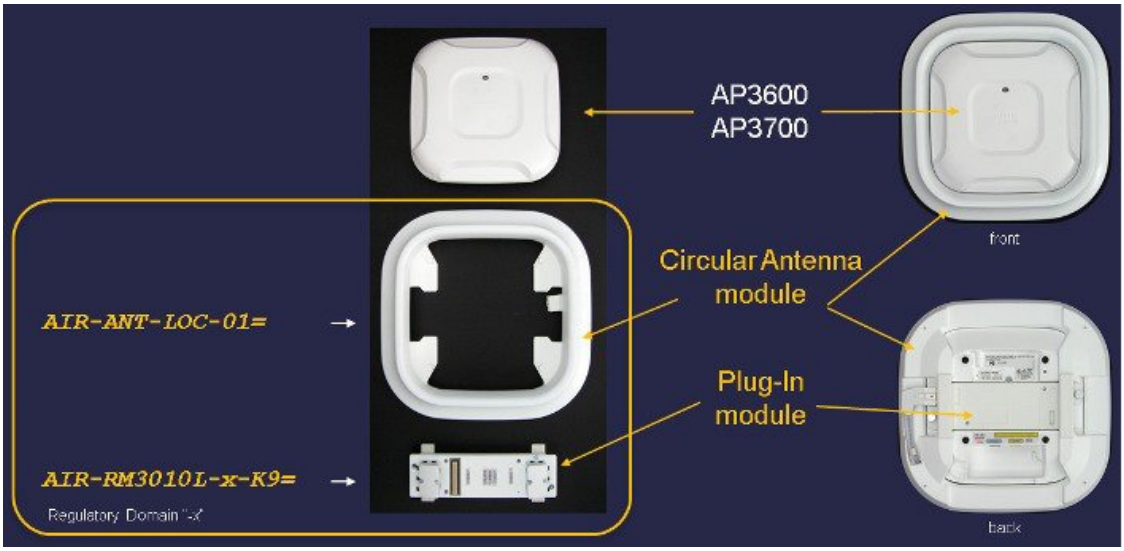
- 従来の WSM に類似した高度な WSM サポートを（スタンドアロン モジュールとして）、802.11 20、40、および 80 MHz で実現（非サービング無線）
- 高度な WSM および位置（Hyperlocation アンテナとともに使用する場合）

- FastLocate のサポート（非サービング無線）
- 統合された Bluetooth Low Energy（BLE）ビーコン送信機能

到来角（AoA）を使用して位置を計算する Hyperlocation の方式は、ネットワーク上の関連付けられた（接続された）802.11 OFDM クライアント（つまり 802.11a/g/n/ac クライアント）を追跡します。この方式は、RSSI（RF 信号強度）のみに基づく従来のリアルタイム位置情報システム（RTLS）よりもはるかに正確です。

最終的な位置計算では、より正確な位置アセスメントを行うために、シスコの AoA 方式だけでなく、RSSI などのその他の多くのファクタも考慮されます。

（注）　AoA Hyperlocation は、現時点では「純粋」な 802.11b クライアントを追跡しません。AoA は、OFDM エミッション、つまり 802.11a/g/n/ac でアソシエートしているクライアントと最もよく連携するからです。したがって、802.11b のクライアントは、従来の RSSI データを使用して追跡されます。のクライアントは従来の RSSI を用いて追跡されます。



Cisco Hyperlocation システムのコンポーネント – アンテナ アレイはスマート アンテナ コネクタを使用してプラグイン モジュールを介して接続される

Hyperlocation の詳細については、次の URL にある Hyperlocation 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/Halo-DG/b_hyperlocation-deployment-guide.html

RF 導入のベスト 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。

- シスコでは、特定の AP に対して、次に示す AP あたりのユーザ数を推奨します。
  - データだけのユーザの場合で 30 ～ 50
  - 音声ユーザの場合で 10 ～ 20

この数字はあくまでも指針であり、使用する AP モデル、端末、またはアプリケーションによって異なる可能性があります。端末/アプリケーション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、およびサイト調査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。最初の共通の最小データ レートは 12 Mbps です。
- 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、シスコ内部の情報システム(IS)グループは現在、3000 平方フィート(約 280 平方メートル)のフロア空間あたり 1 個の AP を使用しています。

無線リソース管理(RRM)

シスコの RRM(無線リソース管理)は、すでに長い歴史を持ちます。一般にはほとんど知られていないことですが、RRM の一連のアルゴリズムは、4.1 以降、コードのリリースのたびに更新されています。これらのアルゴリズムの変更頻度には正当な理由があります。質問が変化し続けるため、回答も変化し続ける必要があるのです。技術は、単一の 20 MHz チャネルでの単純なカバレッジに基づく Wi-Fiネットワーク動作のバランスを取ることから、同じスペクトルですべてが相互動作する、20 MHz、40 MHz、80 MHz、そして近い将来、160 MHz のチャネルおよび電力ソリューションに対応することに移行しました。また、ほとんどの場合、後方互換性とプロトコルの混在も考慮する必要があります。組織が標準化されていても、ほぼ確実に、標準化されていないネイバーと内部リソースが存在します。

RRM の機能

RRM は、4 つのアルゴリズムで構成されます。

1. RF グループ化
2. DCA(動的チャネル割り当て)
3. TPC(送信電力制御)
4. CHDM(カバレッジ ホールの検出および軽減)
5. FRA(フレキシブル ラジオ アサインメント)(AP 2800/3800 などの FRA ハードウェアを管理します)

RRM は大きなテーマですが、ユーザの介入をほとんどまたはまったく必要とせずに RF 環境を動的な方法で管理するために設計されました。アルゴリズムの簡単な説明は、設定作業を理解するために役立ちます。RRM のデフォルト設定は、一般に、初期設定としては最適です。新しいコントローラでは、0 日目セットアップ ウィザードを使用して、作業中の展開タイプを選択することにより、多くの設定を最適化できます。高度な設定も手動で行うことができます。

RF グループ化

RF グループ化アルゴリズムは、選出または指定されたリーダーのもとでの識別およびグループ化を担います。同じネットワークに属しているすべてのリソースを（WLC も AP も同様に）識別およびグループ化します。これは RF グループを形成し、論理設定ドメインになります。ネットワーク リソースは、コントローラの初期設定で入力された RF グループ名によって識別されます。グループ名は、同じネットワーク上のすべての WLC によって共有されます。コントローラに接続されている AP は、コントローラからグループ名を学習した後、無線により、それを他の AP がヒアリングできる NDP メッセージでブロードキャストし、RF ネイバーがどのような状態かをコントローラに報告します。ノイズ、干渉、チャネル使用率、そのネイバーが特定の AP から見てどの程度近く（遠く）にあるかが報告され、RRM を構成するアルゴリズムによる後続のアクションのために保存されます。

（注）　RRM 設定はすべて RF グループ リーダーでのみ実行され、メンバー コントローラで行われた設定は実行中の RRM アルゴリズムに影響せず、そのコントローラ/帯域がネットワークの RF グループ リーダーになった場合にのみ有効になります。

自動 RF グループ化

RF グループ化は、デフォルトでは自動的に実行されます。また、複数コントローラ構成では、同じ RF グループに属しているどのコントローラも、1 つ以上の WLC を RF グループ リーダーとして指定する選出プロセスに参加します。2.4 GHz（802.11b、g、n）帯域および 5 GHz（802.11a、n、ac）帯域にはそれぞれ独自の RF グループ リーダーが必要です。両方の RF グループ リーダーは同じ物理コントローラ上に存在できます。ただし、両方の RF グループ リーダーは必ずしも同じ物理コントローラ上に存在していません。また、FRA が導入されるまでは、両方の RF グループ リーダーが同じ物理コントローラ上に存在する必要があるという要件は実際にはありませんでした。FRA では、両方の帯域が RF グループ リーダーとして指定された同じ物理 WLC 上に存在する必要があります。今後のベスト プラクティスは、静的 RF グループ化手法を使用して大規模展開を制御できるようにすることです。展開がコントローラの単一 HA ペアを基盤としている場合は、すでに両方の帯域が同じ物理 WLC 上に存在します。そうでない場合は、静的 RF グループ化を使用してください。

自動 RF グループ化を効果的に機能させるには、同じ RF グループに含める各コントローラにアクティブ AP が接続されていて、それらの AP が少なくとも 1 つの別のコントローラの AP をヒアリングできる必要があります。最初に、グループとして形成するコントローラに AP を接続する必要があります。そうしないと、各コントローラは、それ自体が RF グループ リーダーであると想定します。サイトごとに単一のコントローラを組み込むようにし、それらのサイトが地理的に離れている場合、一方のサイトの AP がもう一方の地理的に離れたサイトの AP をヒアリングしないため、各コントローラは各サイトの両方の帯域でそれ自体のグループ リーダーになります。

静的 RF グループ化

静的 RF グループ化により、ユーザは RF グループ リーダーを選択し、グループ メンバーを手動で割り当てることができます。すべての WLC は、相互に有線ネットワーク パスを持つ必要があります。無線コンポーネントが存在しないため、アクティブ AP は静的グループを形成する必要はありませんが、コントローラ間の有線接続は必須です。RF グループが作成されると、RRM は無線メトリックを使用して同様に動作します。

（注）　静的 RF グループ化を使用することはベスト プラクティスというわけではありませんが、使用することを強く推奨します。常に RF グループ リーダー上でアクティブな状態を維持することは混乱を招く場合があるからです。この混乱は、グループ内の WLC が増えるにつれて大きくなります。

RF グループ リーダーの WLC 階層

多数のコントローラ モデルが存在しますが、一部のモデルは他のモデルよりも高機能です。自動モードと静的モードの両方で、2500 シリーズ コントローラが 8520 コントローラを差し置いてグループ リーダーになることを防止する階層が適用されます。最も高機能なコントローラが、RF グループ リーダーとして選択される必要があります。

RF グループ リーダーには、RF グループと RRM を管理するために使用されるすべての測定、設定、および計算が送信され、保存されます。RF グループ リーダー上の WLC の RRM 設定は、RRM が RF グループに対して使用する設定です。すべてのコントローラ上の RRM 設定を同期化することが重要です。自動 RF グループ化モードでは、いくつかの理由から RF グループ リーダーが変更される可能性があります。設定が異なる場合、リーダーが変更されると、RF グループの動作が変化します。

RF グループ リーダー レベルでの設定は、RF グループ全体に影響を与えるため、グローバルと見なされます。RRM では RF プロファイルを使用できます。これを作成して、個別の AP グループ(AP の機能または物理属性別のサブ グループ)に適用すると、複数のコントローラに伝達され、グローバル設定が上書きされるため、異なる RF 環境またはロールのローカリゼーションが可能になります。高クライアント密度モデル設計とカバレッジ モデル設計では、正常に機能するために、少なくとも異なるデータ レートと TPC しきい値が必要です。RF プロファイルは AP グループ(たとえば、異なるカバレッジ モデルの一連の AP)に適用でき、それぞれに個別の設定を適用できます。

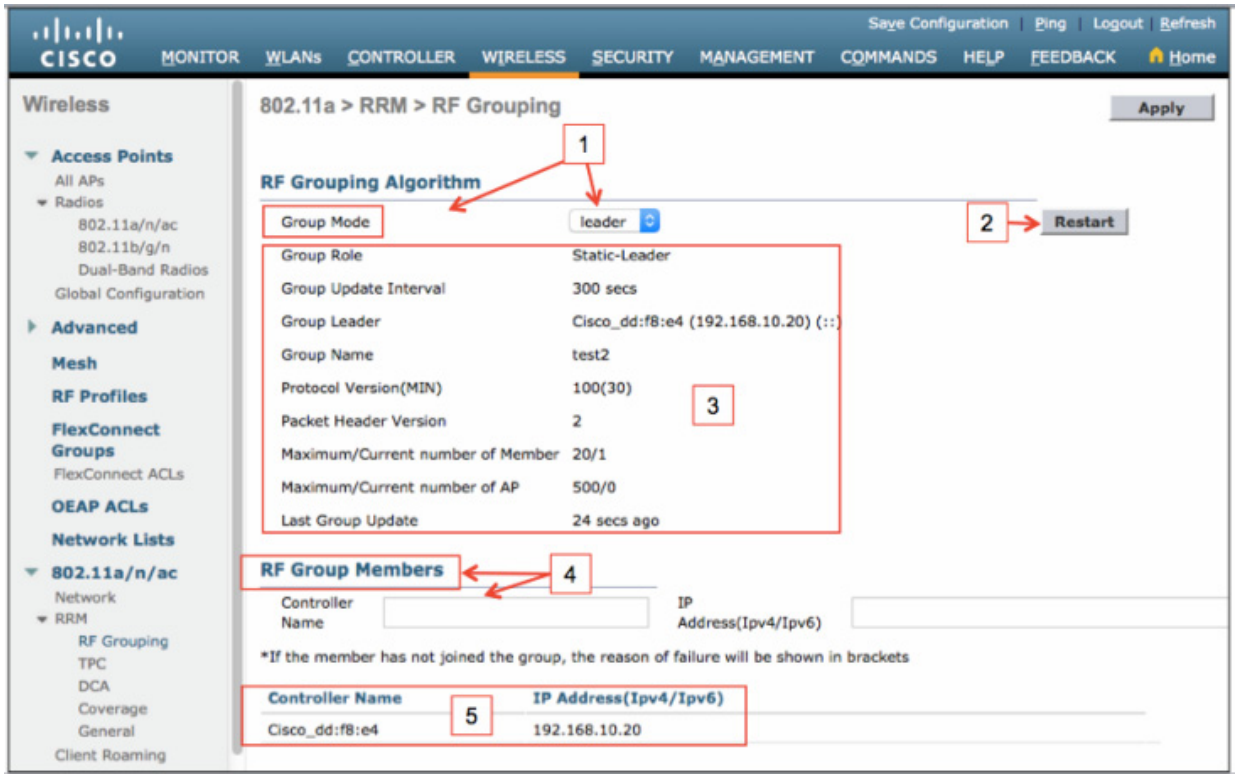
RRM の RF グループ化アルゴリズムの仕様の詳細については、『Radio Resource Management White Paper RF Grouping Algorithm』を参照してください。このドキュメントには、グループ化のメカニズムや無線測定のアクティビティおよび間隔に関する説明が記載されています。

RF グループ化の設定

WLC GUI で、[Wireless]、[802.11a/n/ac] または [802.11b/g/n]、[RRM]、[RF Grouping] の順に移動します。

(注)　設定に関する情報が例として提供されており、設定を開始するのに役立ちます。RF グループ化に関する情報は、新しい製品や機能の導入とともに必然的に変化します。そのため、特定のニーズに関する詳細な分析については、『Radio Resource Management White Paper - RF Grouping Algorithm』にある本書の最新バージョンを参照することを強く推奨します。

図 3-16　RRM RF グループ化 UI の設定



1. Group Mode：RF グループ化アルゴリズムのデフォルト モードは [AUTO] です。これは、ほとんどの配備に適しています。共有 RF ドメインで動作する多数のコントローラがある場合は、リーダーを選択し、メンバー WLC を追加することによって、[Static] モードを使用します。[Static] を選択する場合は、RF グループ内で設定できる AP の数に実際の制限があります。5500 シリーズまでのすべてのコントローラの場合、この制限はライセンス付与されている AP の数の 2 倍です。75xx および 85xx の場合の制限は 6000 個の AP です。同様の空間およびビルディングの場合は、AP とコントローラのグループをともに保持するように RF グループ化を設計します。RF グループにとって重要なことは、相互にヒアリングでき、一緒に設定する必要のある AP が、同じ RF グループに含まれ、同じ RF グループ リーダーによって管理される必要があるということです。地理的に離れた施設については、新しい RF グループを作成します。
2. Restart：モードを変更し、変更内容を適用したら、[Restart] ボタンを使用してグループ化アルゴリズムを「再起動」します。
3. 情報欄：表示されているコントローラのステータス（現在のモード、現在の RF グループ リーダー、プロトコル バージョン、アルゴリズムの間隔、現在の AP、およびメンバー コントローラ数）をユーザに通知します。プロトコル バージョンは、すべてのバージョンを同時に使用できるわけではないため重要です（『Cisco Wireless Solutions Software Compatibility Matrix』の「IRCM」の項を参照）。
4. RF Group Members：メンバー コントローラを静的リーダーに追加するために使用されます。
5. 現在のメンバーとステータスの一覧：メンバー ステータス メッセージの完全な一覧については、『Radio Resource Management White paper RF Grouping Algorithm』を参照してください。

DCA（動的チャネル割り当て）

動的チャネル割り当ては、スペクトルのモニタリングと、AP を配置する最適なチャネル計画の選択を担当します。干渉は最も大きな関心事項です。干渉が減ると、使用できる帯域幅（通信時間）が増えるからです。これを実行するために、DCA は、次の 4 つのパラメータをモニタします。

- 信号：使用しているネットワーク/RF グループによって作成されるすべての Wi-Fi 信号。
- ノイズ：Wi-Fi として識別されないすべての RF 信号。これには、弱いために復調できない衝突およびパケットも含まれます。
- 干渉：不正なデバイスまたは使用している RF グループに含まれないデバイスからのすべての Wi-Fi 信号。
- 負荷：RF グループ内の AP の相対的なチャネル使用率。

ユーザは、DCA 設定の上記のメトリックに優先順位を付ける方法を制御できます。4 つのパラメータはすべて常に使用されますが、計算時のウェイトを調整できます。DCA は、AP ごとに観察される上記の 4 要素に基づいて各チャネルを採点し、その AP がその環境で動作するために最適なチャネルを決定します。

DCA の選択には、802.11n および 802.11ac AP の場合にチャネル帯域幅が含まれます。これにより、設定される動作チャネル幅が選択されます。20/40/80 MHz の選択が行われる場合もあります。動作環境と設計に自信がない場合、ほとんどの企業ロケーションでの現在のベスト プラクティスは、40 MHz（2 つの 20 MHz チャネル）動作です。80 MHz チャネルを使用すると、チャネルごとに 4 つの 20 MHz チャネルが消費され、インフラストラクチャで不要な干渉が発生する可能性があります（これに関する特別な設計を行っていない場合）。

DCA は、接続されている各 AP の規制を認識し、ローカル ルールに違反する恐れなく、複数の国およびドメインを管理できます。また、DCA は、レーダーに関して、すべての DFS チャネルをモニタします。これにより、使用可能なチャネルが管理され、レーダーが検出された場合に代替チャネルが選択されます。RF グループ内のすべての AP に関する決定は、RF グループ リーダー レベルで行われ、関連 AP を設定するためにローカル コントローラに返送されます。

チャネルの変更により、アクティブなネットワークが中断される場合があります。このため、DCA には次の 2 つの主要な動作モードがあります。

- 安定状態：通常
- 起動モード：アグレッシブ

通常の動作時には、起動後に正常な初期チャネル計画が実行されていることが想定されています（詳細については、本書の「起動モード」を参照）。その後、DCA は安定動作状態のヒステリシスを適用することにより、チャネルの変更を多少抑制します。このヒステリシスは、AP があるチャネルに切り替わることを許可する前に、そのチャネルがどの程度優れている必要があるかを決定します。ヒステリシスは、ユーザが選択できます。デフォルトは中程度で、一般にはこれが適しています。Wi-Fi には、その性質上、バースト性があるため、ほとんどが短時間ですが RF の状態が頻繁に変化する可能性があり、実際に変化します。短時間のバーストに基づくチャネル変更により、頻繁に中断をともなうチャネル変更が発生します。DCA は、傾向に基づいてネットワーク全体のチャネル計画を管理します。ネットワーク全体にわたる変更を、分離されたまたは短時間のピーク イベントに基づけることにより、クライアントに関する問題が発生する傾向があります。RRM は、重大な問題に対する高い感度を維持し、緊急用の非常に迅速な変更を管理できます。このルールの注目すべき例外については、この後の、DCA 設定の EDRRM に関する説明を参照してください。

起動モードでは、ヒステリシスがないことが想定されています。これは、初期チャネル計画の積極的な選択と、選択したスペクトルでの無線カバレッジの拡大を目的としています。

ネットワークに次のような変更を加える場合には、これを覚えておくことが重要です。

- 追加の無線を追加する。
- チャネル幅の割り当てを変更する（802.11n または 802.11ac 無線を追加する）。
- サービスから無線を削除する。

これらのことはすべて、動作環境の大きな変更を意味します。起動モードを呼び出すと、新しい疑問に対する最適なソリューションが確保されます。RRM は通常の状況でこれらに関する調整を行いますが、適用されたヒステリシスによってそれを実行します。そのため、新しい動作環境の場合は、最適な回答にならない場合があります。

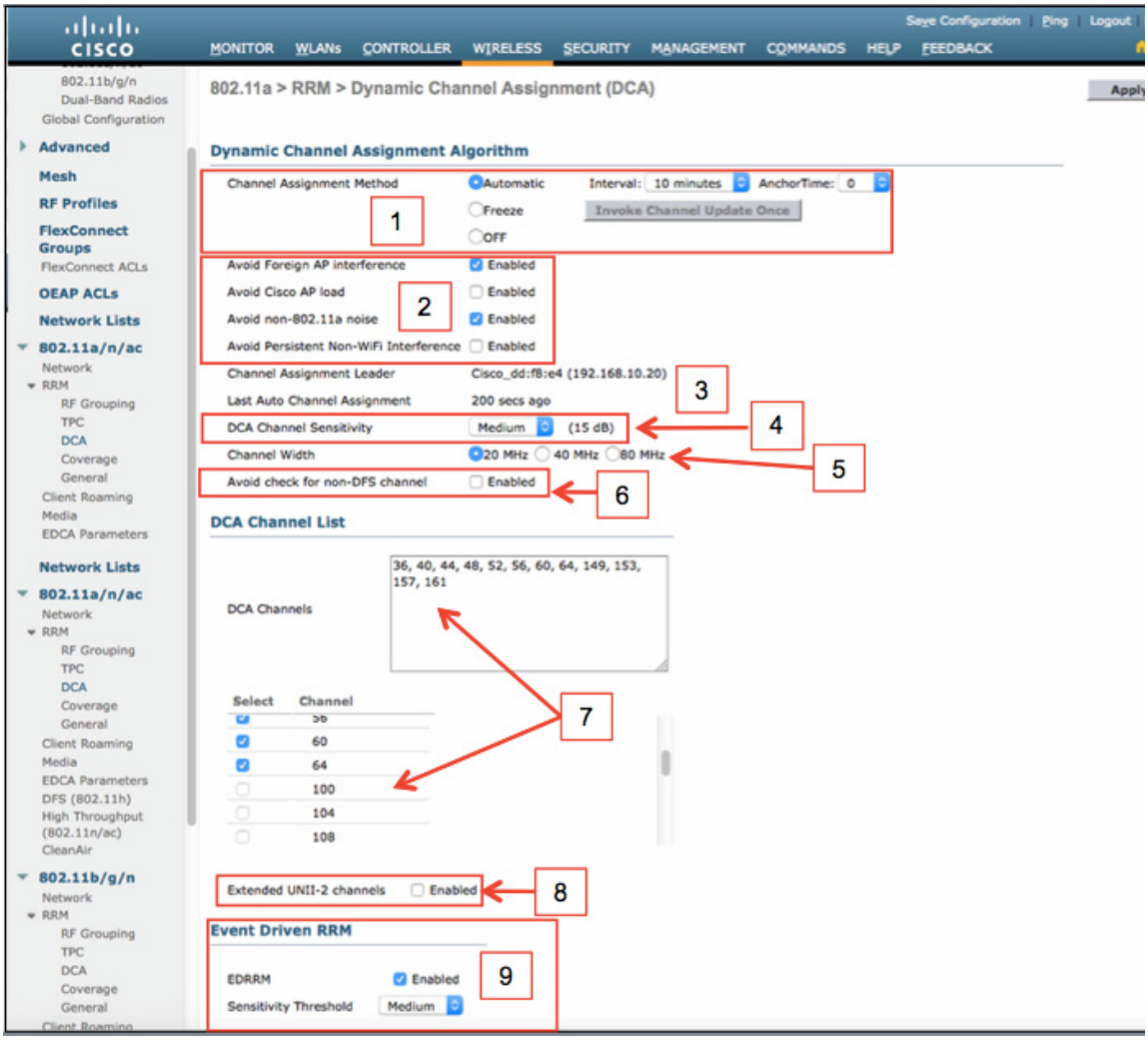
DCA のデフォルト設定は非常に適切です。今日のネットワークの大半がこれらの設定で動作しています。デフォルトの変更は、問題を解決するためにのみ理解し、実行する必要があります。

DCA の設定

DCA のデフォルト設定は次のとおりです。デフォルト設定は、ほとんどの配備に適しています。例外については、後で説明します。DCA の設定画面を次に示します。ここでは、例として、5 GHz の画面が示されています。2.4 GHz の画面との大きな違いは、次のチャネル幅の選択（4）です。2.4 GHz では、束ねられたチャネルはサポートされません。複数 AP 環境では、これを実際に使用するための十分なチャネルまたはスペクトルがないためです。

（注）　次の設定に関する説明は、DCA の機能のサブセットです。詳細な説明については、『Radio Resource management White Paper - DCA』を参照してください。この文書には、機能とバージョンに関する最新のコンテンツが記載されています。

図 3-17　　5 GHz での DCA の設定



DCA の設定要素

1. Channel Assignment Method：DCA を実行するかどうか、およびその実行方法を制御します。デフォルト設定は [Automatic] です。

- Automatic：DCAは 10 分(600 秒)ごとに実行されます。
  - DCA の間隔は、10 分～ 24 時間の範囲で変更できます。また、アンカー時間を選択できます。選択されるアンカー時間は 0 ～ 23(24 時制の時間を表す)です。アンカー時間を [3](午前 3 時)に設定し、間隔を [4] に設定すると、午前 3 時から 4 時間ごとに DCA が実行されます。

- Freeze：DCA の実行が完了した後に、チャネル計画が凍結され、DCA は継続して実行されますが変更は加えられません。[Invoke Channel Update Once] ボタンを押すと、チャネルが 1 回更新され、チャネルの変更と「次回に」スケジュール設定されている DCA の実行が組み合わせて実行されます。これは、オンデマンドで [Freeze] に優先されます。ただし、1 サイクルのみで、そのサイクルについてのみチャネルの変更が許可されます。
- OFF：DCA 機能をオフにします（非推奨、以下を参照）。

2. これらの選択により、DCA が何をどのように決定するかを調整できます。

- Avoid Foreign AP interference：デフォルトでは有効になっています。これは、ネイバーの不正 AP をカウントし、DCA のそれらへの対処を促します。輻輳エリアにいる場合は、この機能を無効にする方が適切である場合があります。輻輳ネイバー環境では、これにより、チャネル変更が何度も開始される可能性があります。ただし、最初はデフォルトを試みてください。
- Avoid Cisco AP load：デフォルトでは無効になっています。これは、使用している（シスコの）AP 上のみの負荷を測定します。この機能により、DCA は条件の影響を受けやすくなり、「より多くの」チャネル変更が促されます。実際には、一時的な負荷ピークの間のクライアント エクスペリエンスが改善されます。
- Avoid non-802.11 noise：デフォルトでは有効になっています。これにより、802.11 として復調できない信号と定義されるノイズの寄与に優先順位が付けられます。これには、衝突のために理解不能な 802.11 となっていたり、単に弱いために適切に復調できない多数のノイズが含まれます。これは常に有効にする必要があります。
- Avoid Persistent Non-WiFi Interference：デフォルトでは無効になっています。CleanAir AP がある場合にこれを有効にすると、非 Wi-Fi の永続的信号（電子レンジ、アウトドア ブリッジング、ビデオ監視カメラなど）の寄与が可能になるため、有効にすることを推奨します。CleanAir がそのようなデバイスを検出すると、そのデバイスがそのときにアクティブでなくても、AP を検出するために影響を受けるチャネルにバイアスを追加できるようになり、より適切なチャネル選択が促されます。電子レンジは昼休みに頻繁に使用され、午後の遅い時間にも再び頻繁に使用されます。これにより、RRM は、365 日 24 時間干渉をヒアリングする可能性のあるデバイス上の影響を受けるチャネルを記憶し、それらのチャネルを避けるようになり、その時間に他の検索が行われなかった場合は期限切れになります。

3. Channel Assignment Leader：この帯域のグループ リーダーの MAC アドレスと IP アドレスを識別します。[Last Auto Channel Assignment] には、DCA が実行されてから経過した時間が秒単位で示されます。

4. DCA Channel Sensitivity：デフォルトは [Medium] です。この設定により、チャネルの変更を決定するために使用されるヒステリシスが決定されます。DCA は、現在のチャネルの得点を、使用可能な他のすべてのチャネルと比較します。このメトリックを満たすか超えるチャネルがある場合は、その優れたチャネルに変更します。[Medium] は、2.4 GHz では 10 dB、5 GHz では 15 dB 優れていることを指定します。どちらの帯域についても、[Low] は 5 dB（より積極的）、[High] は 20 dB（より消極的）です。これにより、チャネルを変更する場合にそのチャネルがどれだけ優れている必要があるかが決定されます。

5. Channel Width：デフォルトは [20 MHz]です。これにより、グローバル チャネル幅が選択されます。この選択は、RF プロファイルや個別の無線レベルで上書きされる可能性もあります。これは、802.11n および 802.11ac 対応 AP にのみ影響を与えます。[80 MHz] を選択することにより、802.11n 無線は 40 MHz に設定されます。

6. Avoid check for non-DFS channels：デフォルトでは無効になっています。DFS では、DCA チャネル一覧内に少なくとも 1 つの使用可能な 非 DFS チャネルが存在する必要があります。ETSI 規制のもとで屋外 AP を配備する場合は、屋外で使用可能な非 DFS チャネルが存在しないため、これを選択することにより、必要な 非 DFS チャネルの適用が防止されます。

7. DCA Channel List: 上側には、現在設定されているチャネルが示されます。このリストにより、チャネルを選択および選択解除できます。チャネルを追加または削除するには、変更を加える前に帯域(2.4 GHz または 5 GHz)を無効にする必要があります。
8. Extended UNII-2 channels: デフォルトでは無効になっています。有効にすると、チャネル 100 ～ 144 が DCA チャネル一覧に自動的に追加されます。これは現在のベスト プラクティスです(特に 802.11n/802.11ac 40/80 MHz チャネルを選択する場合)。
9. Event Driven RRM: EDRRM はデフォルトで有効になっています。有効にすることがベストプラクティスです。EDRRM により、RRM は CleanAir 電波品質(AQ)で機能できるようになり、分類された深刻な干渉が発生した CleanAir AP が、チャネルを変更して干渉を緩和することが可能になります。「深刻な」とは、非 Wi-Fi の干渉源が 100 % のデューティ サイクルでブロードキャストされることによって、その AP のチャネルが完全にブロックされ、クライアントまたは AP のどちらもが送信できない(通信の前にリッスンするが、リッスンのたびにエネルギーをヒアリングするため)状況を意味します。決定は、DCA とは無関係に AP で行われます(30 秒以内に行われます)。RRM は、この変更を認識し、1 時間にわたって AP の元に戻る変更を防止します。4 つの感度のしきい値があります。

表 3-5　ED-RRM AQ イベントしきい値のマッピング

Low	AQ=35
Medium	AQ=50(デフォルト)
大きい	AQ=60
Custom	ユーザしきい値(注意が必要)

1. 新規配備の場合: コントローラの再起動または DCA のリセット開始の前に、すべての AP が設置され、コントローラに関連付けられていることを確認します。

- DCA は、コマンド ラインで config 802.11a/b channel global restart コマンドを実行することによって再起動し、初期化することができます。動作を確認するには、GUI の DCA 設定ページで [wireless]、[802.11a/b]、[RRM]、[DCA] の順に選択すると、[Startup] が表示されます。

図 3-18　DCA

2. チャネル計画の要件に大きな変更があった場合はいつでも DCA を再初期化します。

- チャネル帯域幅の変更(20/40/80)
- 追加の AP の追加
- DCA チャネルの変更(たとえば、UNII2e チャネルの追加または削除)

3. デフォルト オプションは最適ですが、配備場所に多数の不正なネイバーが存在し、そのためにチャネル変更が毎日発生する場合に無効にできる [Avoid Foreign AP interference] は例外です。

TPC（送信電力制御）

Wi-Fi で重要なその他のコンポーネントは、AP の無線の送信電力です。TPC は、無線メッセージを使用して、RF グループ内のすべての AP をヒアリングし、測定します。各 AP が他の AP をどのようにヒアリングしているか、および他の AP がユーザ自身の AP をどのようにヒアリングしているかを継続的に追跡することにより、電力を動的に調整して、ネイバーへの干渉を発生させることなく、最適なカバレッジ（セル サイズ）を提供できます。TPC の計算では、規制要件（最大電力など）が継続的に追跡されます。これは、ほとんどの規制地域で、使用しているチャネルおよび帯域に応じて計算が変わるためです。現在、TPC の計算には TPCv1 と TPCv2 の 2 つの異なる方式があります。TPCv1 はデフォルトであり、TPCv2 は高密度展開カバレッジ用の代替方式です。

TPC は、最適な電力レベルを計算するために AP 間の無線による測定に依存しているため、実際には、フロア レベルのクライアントがそれをどのようにヒアリングしているかを認識していません。そのため、環境を調整するためにアルゴリズム内で選択できるものよりも広い範囲のカバレッジ レベルが存在します。その値は、設定しているセルのエッジに必要な dBm 値 であり、さまざまな AP の配置と設置ソリューションに合わせて調整が可能です。たとえば、天井が高い環境で AP が 60 フィート（18 m）間隔で配置され、フロアが 25 フィート（8 m）下に存在する場合があります。この場合、デフォルト値の -70 ではフロアで十分な電力とカバレッジを実現するには不適切であり、-60 という値が適切である可能性があります。

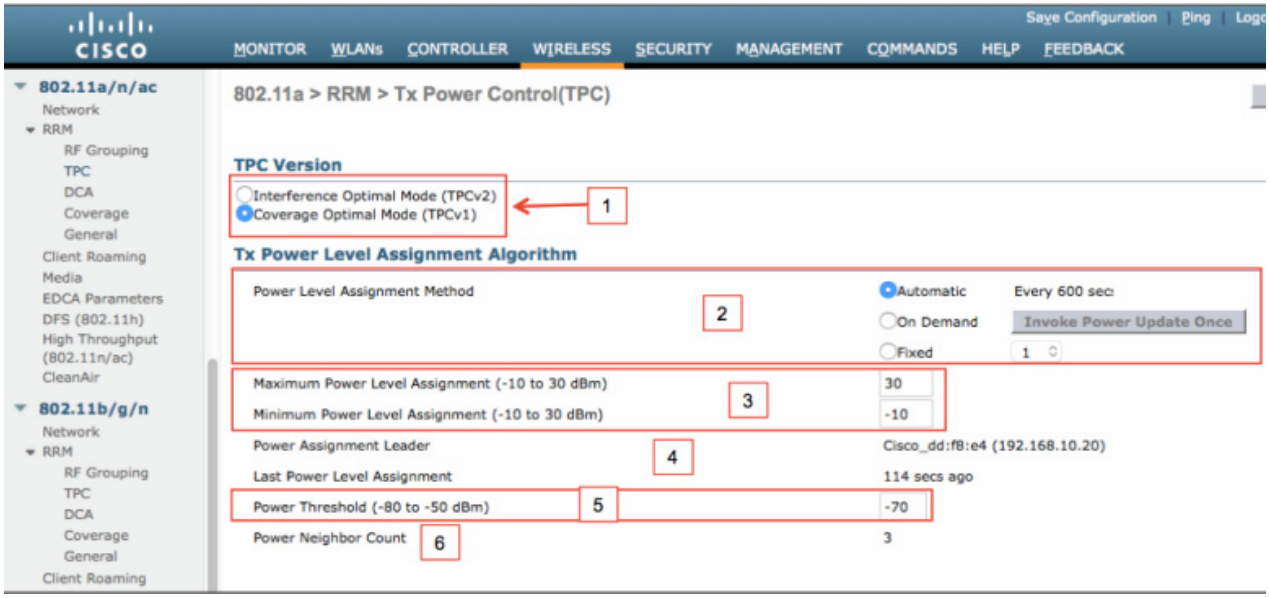
TPC には、RF プロファイルを使用して、または WLC 全体に関してグローバル レベルで適用できる上書き機能があります。これによって、管理者は、AP が超えない最小および最大電力レベルを指定できます。この機能は高クライアント密度環境での調整に役立ち、不十分な AP 配置オプションを修正することもできます。

以下のベスト プラクティスで、最適なカバレッジを実現するために TPC を調整する方法を詳しく説明します。

TPC の設定

TPC のデフォルトの選択は、通常の企業オフィス環境に適しています。デフォルトの TPC ユーザしきい値は、10 フィート（3 m）の天井の高さを想定しています。TPC の機能と設定のベスト プラクティスの詳細については、『RRM White Paper – Transmit Power Control』を参照してください。

図 3-19　TPC 設定 UI



1. TPC のバージョンの選択:デフォルトでは TPC v1 が選択されています。TPCv2 は高密度設計に使用できます。また、AP が相互に近接しており、電力が比較的低下しない場合に、チャネル モードと組み合わせて優れたキャパシティを生み出すことができます。広いオープンなエリアで AP セル サイズが 3000 平方フィート(約 280 平方メートル)以下の配備の場合は、これを考慮する必要があります(コマンド ライン引数の「channel mode」と組み合わせて使用)。これにより、TPCv2 機能が同じチャネルのネイバーのモニタのみに制限されます。これは RF グループ全体に影響を与えるグローバル コマンドであるため、1 つのバージョンのみを選択できます。これがメンバー コントローラで選択される場合は、そのコントローラがグループ リーダーにならない限り、RF グループには影響しません。
2. Power Level Assignment Algorithm

- Automatic:デフォルトであり、600 秒(10 分)間隔で実行されます。
- On Demand:[Invoke Power Update Once] が押されている場合に、次回にスケジュール設定された間隔(600 秒)でのみ実行されます。電力レベルは呼び出しコマンドが受信されない限り凍結されますが、TPC はバックグラウンドで動作し続けます。
- Fixed:電力レベルを手動ですべての AP に割り当てることができます。これは、いくつかの理由から推奨されません。
  - すべての AP は、電力レベルが選択済みであることが示されますが、5 GHz チャネルの割り当てによっては、dBm 単位の非常に異なる電源出力を持つ場合があります。アクセス ポイントのリファレンス ガイドを参照してください。また、ドキュメントで、使用しているモデルのチャネルと最大電力を参照してください。
  - これは、TPC アルゴリズムからすべての AP を除外します。

3. Min/Maximum Power Level Assignment：デフォルトは [Disabled] です（-10 dBm および 30 dBm の値はシスコの「どの」APでもサポートされないことに注意してください）。これは、コントローラごとに上書きされます。また、そのコントローラに接続された「すべて」の AP で許可される最小および最大電力レベルの設定が可能です。TPC がローカル コントローラの最小/最大値よりも大きい（または小さい）設定を適用しようとすると、その設定は、この設定によって上書きされます。エントリは dBm 単位であり、適用される AP で実際に許可されている電力に最も近い最大電力または最小電力が生成されるため、チャネルおよび最大電力について、上記を参照してください。この設定は、RF プロファイルで行い、一部の AP グループに適用することもできます。これは、複数のカバレッジおよびキャパシティ ゾーンを含む大規模な展開の場合に推奨されます。
4. Power Assignment Leader：帯域のアクティブな RF グループ リーダーを識別します。Last Power Level Assignment：最後の割り当て以降の時間を秒単位で示します。
5. Power Threshold (-80 to -50 dBm)：これは、TPC アルゴリズムに、セル エッジに関して必要な値を示します。TPC は、これを計算でネイバーのしきい値として使用して、AP の最適な電力レベルを決定します。

- TPCv1：デフォルトは -70 dBm です。10 フィート（約 3 m）の天井を持つ通常のオフィス スペースを想定しています。用途に 15 ～ 20 フィート超（約 4.5 ～ 6m 超）の高い天井が含まれる場合は、このしきい値を増やして調整し、フロアで適切な電力を得られるようにする必要がある可能性があります。測定は AP 間の NDP パケットを使用して行われます。すべての AP が通路に配置されている場合、これは、通路の左右どちらかの部屋のカバレッジに悪影響を与える可能性があります。測定を行う必要があり、緩和のために AP の配置を変更する必要がある場合があります。
- [TPCv2]：デフォルトは -65 dBm です。

6. [TPCv1 Channel Aware]：これはバージョン 8.5 で追加された新しい機能です。この機能を有効にすると、TPCv1 が計算の際に同一チャネル ネイバーを考慮できるようになります。これにより、TPC によるより積極的な割り当てが可能になるとともに、同一チャネル干渉が増加しないことが保証されます。これは通常、以前の TPCv1 アルゴリズム単体よりも 2 ～ 3dB 多い電力を悪影響なしで提供します。

CHDM（カバレッジ ホールの検出および軽減）

CHD はクライアントを測定します。CHD はこれをコントローラごとに行い、他の RRM アルゴリズムとは異なり、RF グループ リーダーで設定されて RF グループ全体に適用されるものではありません。CHD は、各 AP に関連付けられたクライアントをモニタし、クライアント RSSI の AP の測定に基づいて、クライアントが適切なカバレッジを得ているかどうかを判断します。これは、より近くより適切な（RF ワイス）AP が使用可能な場合にクライアントが意図的に AP への接続を保持しないことを想定しています。（スティッキー クライアントと呼ばれる状態）。クライアントはローミングのタイミングを単独で決定し、一部のクライアントは不適切な決定を下します。CHD は、アソシエート先の AP のネイバーを調べ、その他の近隣 AP がクライアントをどの程度ヒアリングできるかを判断することによってスティッキー クライアントを排除します。クライアントがより適切な AP 上に存在する必要があり、また存在できる場合、それは誤検出イベントとしてマークされ、アクションは実行されません。クライアントがスティッキーではない場合、その RSSI がカバレッジのしきい値を下回ると、クライアントのロケーションとそれに関連付けられていた AP に関するアラートとレポートが生成されます。

CHD は、アソシエート先の AP の電力出力を増やしてカバレッジの問題の軽減を試みることを、ローカルに（RRM TPC アルゴリズムの外部で）決定できる軽減コンポーネントも備えています。この機能は今でもアルゴリズムに含まれていますが、デフォルトの動作では、カバレッジ ホールが深刻であること（ネイバー AP が失われ、複数のクライアントが影響を受けているなど）を確認することに大きな重点が置かれています。

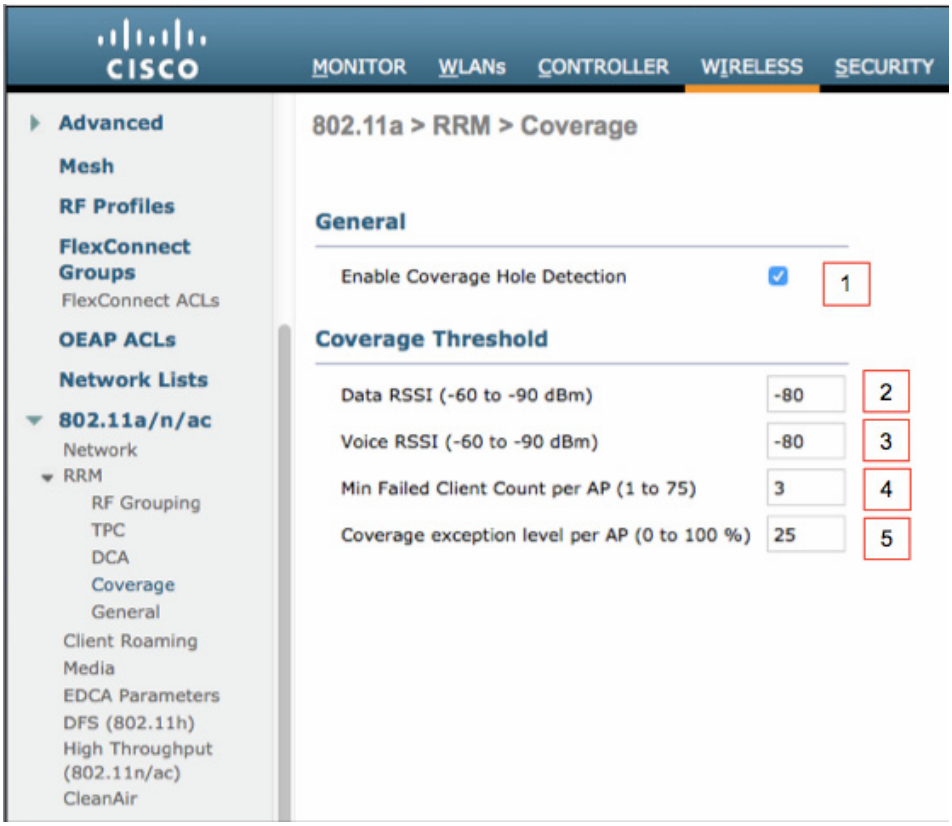
シスコは、スティッキー クライアントについて、最適化ローミング」と呼ばれる機能を使用したより直接的なアプローチを取っています。この機能は、CHD が生成したメトリックから方向を合わせて、関連付け解除を送信してクライアントがより適切な AP にローミングするよう促すことによってアクティブに介入します。(本文書で後述する「最適化ローミング」を参照してください)

カバレッジ ホールの検出および軽減(CHDM)設定

カバレッジ ホールの検出および軽減は、コントローラごとのアルゴリズムであり、RF グループ全体の管理のみを目的に RF グループ リーダーで設定されることはありません。モニタするコントローラで個別に設定する必要があります。ただし、カバレッジ ホールの軽減と特定の AP の電力レベルを上げるアクションは RF グループ レベルで連携し、その周囲の他の AP で電力レベルを強制的に変更します。

カバレッジ ホールの検出では、関連する AP 上のクライアント RSSI をモニタします。詳細については、『RRM White Paper』の「CHDM」の章を参照してください。

図 3-20　カバレッジ ホールの検出の設定 UI



1. カバレッジ ホールの検出の有効化/無効化:デフォルトでは有効になっています。これは、個別の WLAN で、または RF プロファイルで上書きできます。
2. データ RSSI しきい値:デフォルトは -80 dBm です。

(注)　データ RSSI のエントリは、ローミングの最適化がグローバル レベルで有効になっている場合に、ローミングの最適化のしきい値にも使用されます。有効にする前に「ローミングの最適化」を参照してください。

3. 音声 RSSI しきい値:デフォルトは -80 dBm です。
4. AP あたりの最小障害クライアント数:デフォルトは 3 です。この設定により、いくつのクライアントが上記の音声しきい値またはデータしきい値を超えるとカバレッジ ホールのアラートが生成されるかが決定されます。これは、下記のカバレッジ例外レベルと組み合わせて使用することもできます。
5. AP あたりのカバレッジ例外レベル:この設定により、特定の AP 上のすべてのクライアントのうち何 % がしきい値を超えるとカバレッジ ホールが宣言されるかが決定されます。これは、上記の最小障害クライアント数と組み合わせて使用することができます。

カバレッジ ホールの検出および緩和は、しきい値の例外によって高度に調整できますが、一般にはデフォルト設定で十分です。最小クライアント数とカバレッジ例外は連動します。たとえば、デフォルトのクライアント数 3 とカバレッジ例外 25 % の場合、3 つのクライアントがしきい値を下回っても、機能するには、現在関連付けられているクライアントが 12 存在する必要があります(12 の 25 % が 3)。CHDM も、障害が発生したクライアントが実際にカバレッジ ホールに含まれているかどうか、またはそのクライアントが単にローミングしていないかどうかを判断するために、各 AP 上のクライアントをリッスンします。ある AP からクライアントをヒアリングする方が、同じく現在そのクライアントに関連付けられている別の AP からヒアリングするよりも優れている場合、これは誤検出としてカウントされ、カバレッジ ホール イベントにはカウントされません。両方の条件が満たされる場合、カバレッジ ホールの軽減は、1 電力レベルずつ AP の電力を増やして、カバレッジの修正を試みることができます。その後、RRM は、次回の DCA および TPC の実行時にカバレッジ要件を再評価します。

ローミングの最適化

ローミングの最適化は、スティッキー クライアントの問題の解決に役立つツールです。スティッキー クライアントとは、より堅牢な接続が使用可能であるにもかかわらず、そこにローミングせずに特定のアクセス ポイントへのアソシエーションを保持し続けるクライアントのことです。クライアントはローミングするタイミングとローミング先を単独で決定します。そしてすべてのクライアントが同等に作られているとは限りません。ローミングの最適化機能は、この章で先に詳しく説明したカバレッジ ホール アルゴリズムと同様に、AP から収集されたリッチなデータを使用します。ローミングの最適化は、AP で測定されたクライアントのデータ RSSI を調べ、カバレッジ ホール設定ダイアログで設定されたデータ RSSI しきい値と比較します。クライアントがこのしきい値を下回る場合は、アソシエーション解除メッセージ(理由 4:タイムアウト)がクライアントに送信されます。デフォルト設定では、ローミングの最適化は無効になっており、カバレッジ ホールのデータ RSSI は CH 計算に使用されます。ローミングの最適化には、オプションのメトリックであるデータ レートもあります。これはデフォルトでは無効になっており、受信データ パケットの RSSI しきい値とデータ レートに基づいて二重ゲートを形成するために使用できます。データ レートも使用する場合、アソシエーション解除イベントをトリガーするには、両方を true にする必要があります。

特定のクライアントに対してトリガーされたローミングの最適化は、クライアントの RSSI がしきい値を下回る場合には、そのクライアントの再アソシエーションも防止します。クライアントがその AP に再アソシエートするには、再アソシエーションしきい値を 6 dB 上回る必要があります。あまり知られていない低 RSSI チェック機能を併用することが推奨されないのはこのためです。2 つのしきい値は相互に連携して動作せず、セルのアクセスを誤ってロックアウトしてしまう可能性があります。

ローミングの最適化の設定

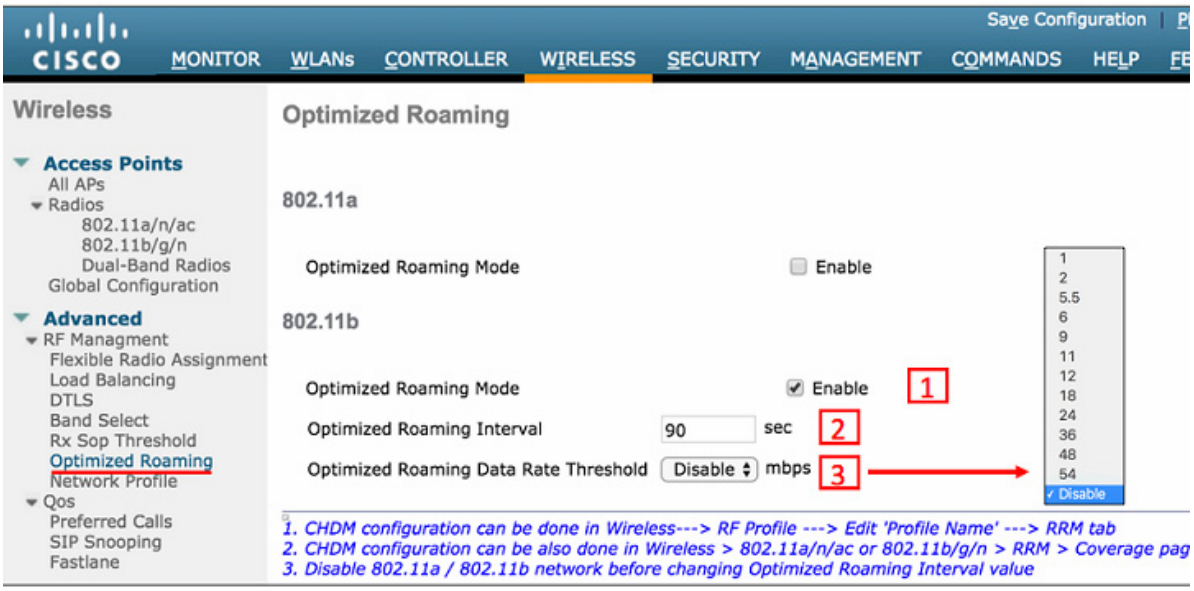
ローミングの最適化は、遠くのアクセス ポイントへのアソシエーションを保持し続けるスティッキー クライアントの問題を解決します。この機能は、クライアント データ パケットの RSSI と AP によって測定されたデータ レートに基づいてクライアントをアソシエーション解除します。この機能は、この文書で先に詳しく説明したカバレッジ ホール アルゴリズムによって生成されたデータを使用します。

クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートがローミングの最適化データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

- ローミングの最適化は、次のシナリオで実装されます。
  - エンタープライズ環境でプロアクティブにクライアントを切断することで厄介なスティッキー クライアントの問題を解決する。
  - 管理用のスタンドアロン Wi-Fi ホットスポットを実装する。
  - RSSI が設定されたしきい値より低い場合にクライアントをアソシエーション解除する。

この機能の仕組みとその適切な導入方法の詳細については、HDX(高密度エクスペリエンス)設計ガイドバージョン 8.0 および 8.1、またはワイヤレス LAN コントローラの技術リファレンス ページの最新情報を参照してください。

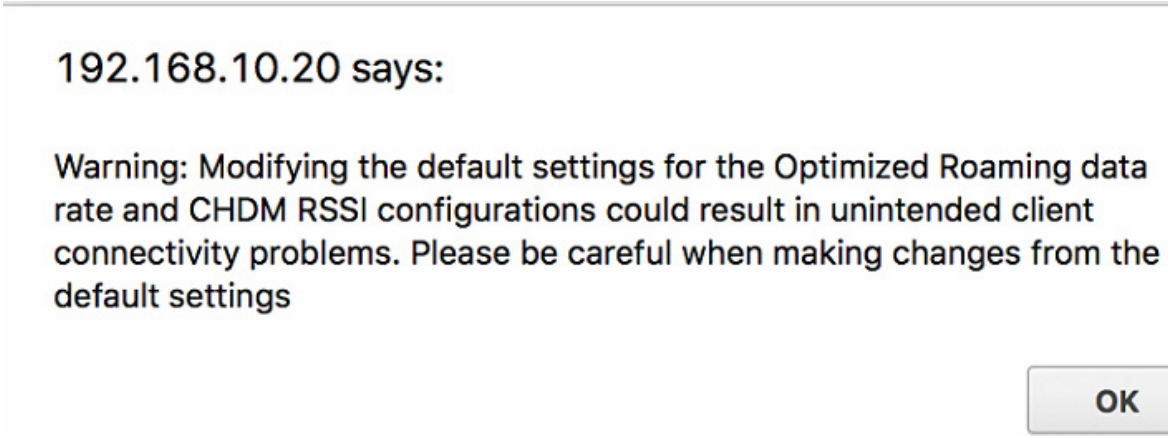
最適化ローミングは、RF グループ リーダー レベルではなく、コントローラごとに設定できます。決定は、コントローラ全体とそれに関連付けられているすべての AP に適用されます。個々の AP グループは、AP グループの RF プロファイルを使用して別に(グローバル CH しきい値レベル以外で)管理できます。これにより、必要に応じて SSID/AP グループ レベルできめ細かく管理できます。



有効/無効 - デフォルトで無効です。

最適ローミング間隔 – デフォルトは 90 秒です。この間隔を小さくすると、AP とコントローラに不必要な負荷がかかるため、TAC またはその他適切なテクニカル サポートによって指示されない限り、この間隔は変更しないことを強くお勧めします。その場合は、変更するネットワーク(帯域が 2.4 GHz または 5 GHz)を無効にする必要もあります。

1. 有効/無効 - デフォルトで無効です。
2. 最適ローミング間隔 – デフォルトは 90 秒です。この間隔を小さくすると、AP とコントローラに不必要な負荷がかかるため、TAC またはその他適切なテクニカル サポートによって指示されない限り、この間隔は変更しないことを強くお勧めします。その場合は、変更するネットワーク(帯域が 2.4 GHz または 5 GHz)を無効にする必要もあります。



3. データ レートしきい値:許容可能な最低データ レートを設定します。データ RSSI しきい値と組み合わせて使用します。これはトリガー決定を下すために使用される追加の条件であり、アソシエーション解除が送信されるためには、RSSI とデータ レートの両方の条件が満たされる必要があることに注意してください。

フレキシブル ラジオ アサインメント(FRA)アルゴリズム

フレキシブル ラジオ アサインメント アルゴリズムは、AP 2800/3800 シリーズ アクセス ポイントに含まれているフレキシブル ラジオ アーキテクチャ ハードウェアを管理するために、WLC バージョン 8.2.100.0 で導入されました。

FRA は、RF グループによって提供されるリッチな情報を使用してカバレッジを評価し、より有益なロールに再割り当てできる冗長 2.4 GHz(適切なカバレッジに不要)無線を特定します。これは次の 2 つのことを行います。

- 2.4 GHz インターフェイスの過飽和による破壊的な自己干渉を排除すると同時に、2.4 GHz を適切にカバーして使用可能なセルを提供します。
- 追加のハードウェア、ケーブル、またはスイッチポートを必要とせずに、デュアルバンド冗長無線を複数の有益なロールに転用できます。

過飽和は実際には簡単に生じます。2.4 GHz または 5 GHz の設計については、上記の「導入に関する考慮事項」の説明を参照してください。5 GHz の設計を行う場合(必須)、狭い帯域幅と 3 チャネルが使用可能であれば、非常に多くの 2.4 GHz 無線が生成されます。FRA の導入以前は、これを解決するには、通常、訓練を受けた専門家が導入前後に詳細な分析を実施し、カバレッジの問題を整理して、いくつかの 2.4 GHz 無線を無効にする必要がありました。この分析は、AP のネイバー関係について行われました。FRA は現在これと同じデータを使用します。

- AP 2800/3800 と RRM FRA アルゴリズムを組み合わせると、次の機能を備えたシンプルなソリューションを提供できます。
  - 効果的なカバレッジを測定する
  - ネイバー カバレッジでカバーできる AP のセルを分析する
  - それらのセルを冗長セルと認定する

- この分析の結果は RRM に戻されます。RRM は、顧客の選好と DCA に基づいて、現在不要なインターフェイスが最も役立つロールを特定します。
  - 2 番目の 5 GHz インターフェイス(5 GHz 容量を 98 % 増加させる)
  - モニタ:専用のセンサーによる 2.4 および 5 GHz のモニタリング(各チャネルの分解能を、クライアントにサービスを提供する無線の 24 倍に増やす)
  - DNA-c ワイヤレス保証センサー(アクティブ クライアント モードを提供し、DNA アーキテクチャのサービス保証の指示に従って周辺の AP でテストを実行する)

FRA は、RRM のネイバー(NDP)データベースを使用して次のことを行います。

- 隣接する 2.4 GHz AP 間の相対位置を特定する
- 各 AP が -67 dBm でカバーする必要があるエリアを計算する*
- 各 AP のカバレッジの結果を分析し、隣接する AP のカバレッジ オーバーラップをターゲット セルの合計カバレッジのパーセンテージとして評価する

* DNA-c ワイヤレス保証センサー ロールの場合、カバレッジは必ずしも -67 とは限らず、2.4 GHz カバレッジ要件よりも多くのセンサーを選択できるように信号レベルを引き下げることができます。

無線は、COF(カバレッジ オーバーラップ係数)が設定可能な必要なカバレッジしきい値を超えると冗長とマークされます。カバレッジ オーバーラップ係数は、特定の AP(AP-1)のセルが最大 3 つのネイバー AP によって -67 dBm で有効にカバーされる割合を表す 0 ～ 100 % の数値です。この数値が 100 % の場合、有効なクライアント カバレッジに悪影響を与えることなく、AP 1 を効果的に無効にできます。この無線を無効にするのではなく、上記の複数のロールのいずれかに再割り当てします。FRA は無線と冗長とマークします。これにより、そのインターフェイスを再利用して追加の価値/インテリジェンスをネットワークに提供できます。

FRA の詳細とそのカバレッジの計算方法については、『RRM White Paper – Flexible Radio Assignment』を参照してください。

(注)　FRA が機能するには、2.4 GHz RF グループ リーダーと 5 GHz RF グループ リーダーの両方が同じ物理 WLC 上に存在する必要があります。自動 RF グループ化を使用すると、ほとんどの場合、どちらも同じ物理 WLC 上に配置されますが、必ずしもそうなるとは限りません。複数の WISM または 5508 コントローラを運用している環境で FRA を有効にする場合は、静的 RF グループ設定を使用することを強く推奨します。

FRA は 3 つのモードで動作します。これらのモードは、グローバル FRA 設定ダイアログの [Service Priority] で選択できます。

- カバレッジ:カバレッジの推定が -67 dBm で保持され、DCA によるロールの選択が 5 GHz(優先)またはモニタ ロール(5 GHz がすでに飽和している場合)のいずれかである従来の設定です。
- クライアント認識型:8.5 で新しく導入されたモードで、カバレッジと同じ決定しきい値に従いますが、プライマリ 5 GHz チャネルが非常にビジーになった場合にモニタ ロールの割り当てを 2 番目の 5 GHz インターフェイスとしてサービスに組み入れることができます。

サービス保証:このモードでは、FRA 感度しきい値を満たすために必要な COF と FRA の積極性を変更するためのターゲット カバレッジ RSSI の両方が調整されます。出力には、カバーされるネットワークのパーセンテージも表示されます。積極性は、[Sensor Threshold] 選択ダイアログで調整できます。以下を参照してください。

FRA の詳細については、『Radio Resource Management White Paper』を参照してください。

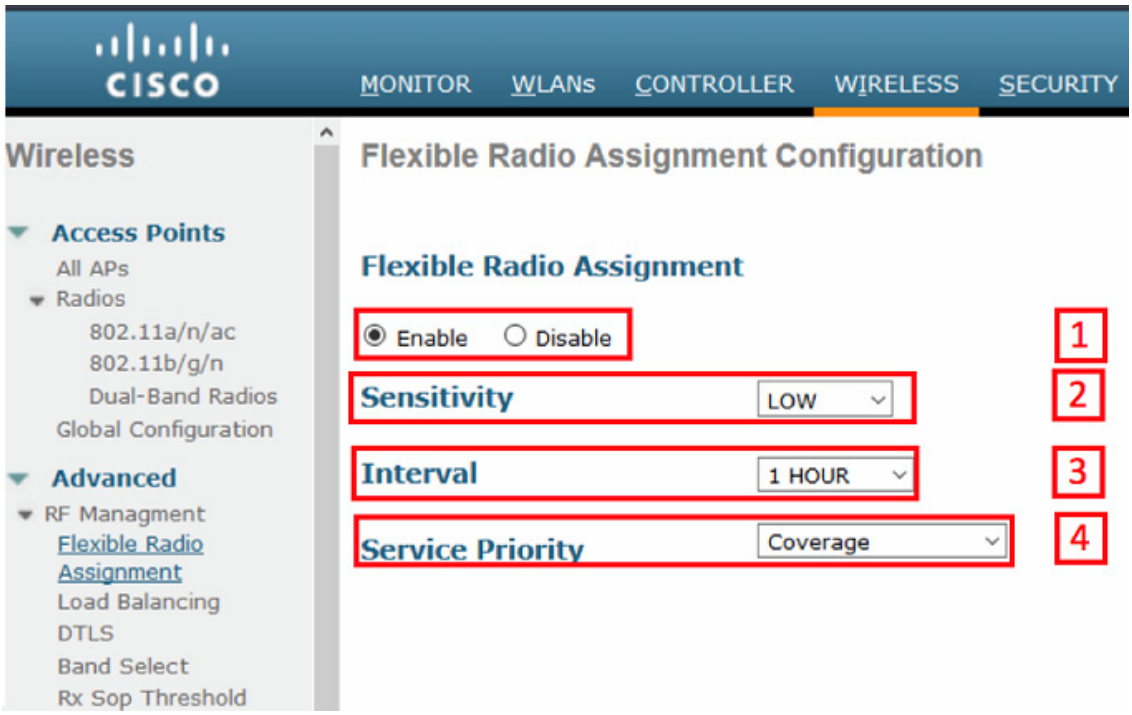
FRA の設定

FRA の設定では、RF グループ リーダー(グローバル)と AP(無線インターフェイスは FRA の自動モードか手動モードのいずれか)でアルゴリズムを実行します。RF グループ全体のためにグローバルまたは WLC レベルが実装されています。これを使用する場合、両方の RF グループ リーダー(2.4 GHz および 5 GHz)が同じ物理コントローラ上に存在する必要があります。8.2 ～ 8.5 リリースの WLC では、FRA アルゴリズムはデフォルトで無効になっています。

(注)　FRA は、8.6 ではおそらくデフォルトで有効になります。デフォルト値は新しく設置されたコントローラにのみ適用されます。新しいバージョンへのアップグレードでは、現在の設定が保持され、変更は加えられません。この機能が存在しないコード バージョンへのアップグレードの場合、デフォルト値は新しく追加された機能に適用されます。

設定の他の部分では、グローバル FRA アルゴリズムで制御する無線インターフェイスを指定します。無線設定レベルでは、デュアルバンド無線はすべてデフォルトで自動 FRA です。これにより、FRA をグローバル レベルで有効にするとすぐに、FRA はそれらの無線を制御できるようになります。無線のもう 1 つのオプションは手動モードです。手動モードでは、FRA による新しいロールの割り当てが防止されますが、アルゴリズムで COF を計算したり、それらの無線を出力に含めることを考慮してアルゴリズムを実行したりできます。ただし、変更は要求されません。

グローバル FRA 設定ダイアログ



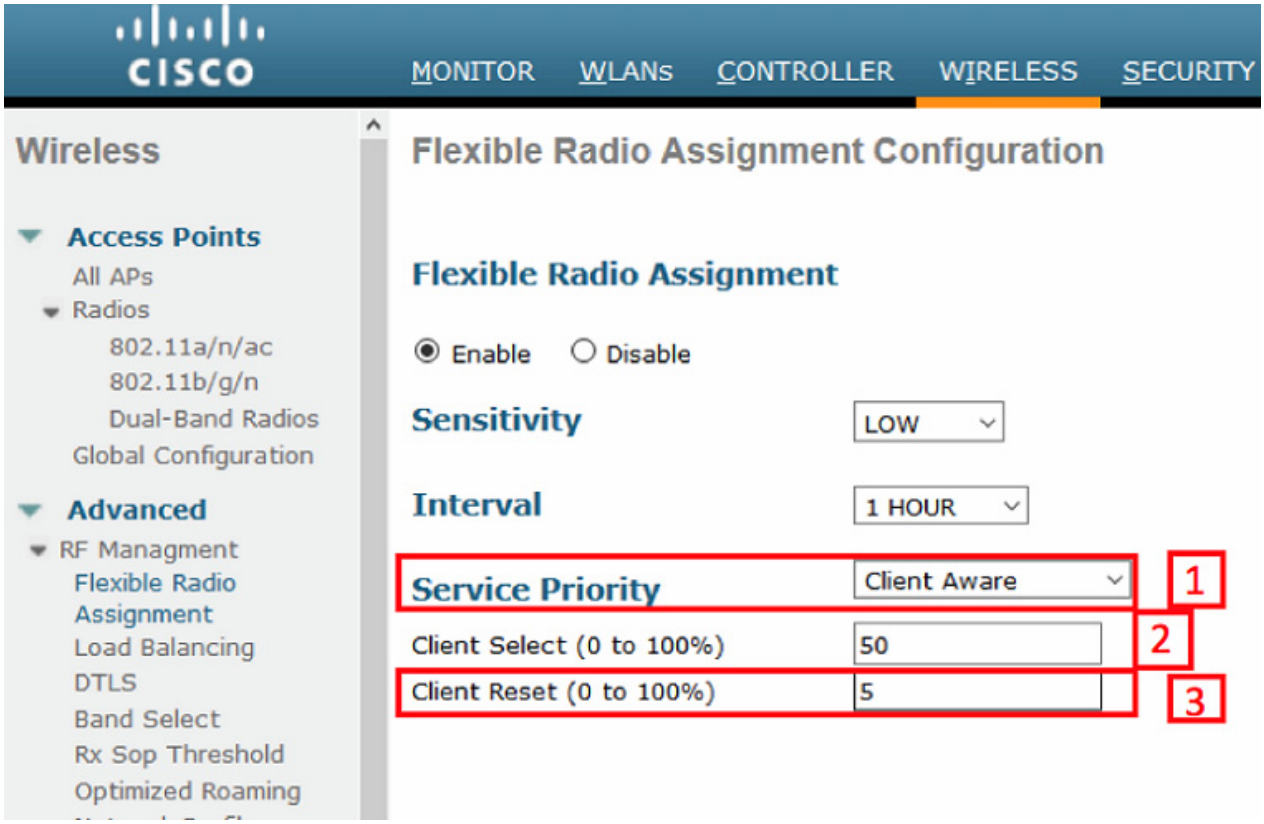
1. [Enable] または [Disable]: リリース 8.5 まではデフォルトで無効です。
2. [Sensitivity]: [Low](100 %)、[Medium](95 %)、[High](90 %)はCOF(より有益なロールへの再割り当てのために無線を冗長とマークするために必要なカバレッジ オーバーラップ係数)を示します。

3. [Interval]：最小 1 時間、最大 24 時間です。どの場合でも、DCA の実行間隔より大きくする必要があります。
4. [Service Priority]：（8.5 の新機能）FRA の実行モードを変更し、冗長無線を割り当てるロールに優先順位を付けられるようにします。

[Coverage]：これは 8.5 より前のバージョンで使用できる唯一の優先順位です。FRA のセル カバレッジ ターゲットが -67 dBm に設定され、選択した感度しきい値（低、中、高）が保持されます。DCA による冗長無線の優先順位は次のとおりです。

1. 2 番目の 5 GHz インターフェイス：DCA はまず、同一チャネル干渉に基づいて既存の 5 GHz チャネル計画にインターフェイスを追加しようとします。この計算は、チャネル幅（20/40/80/160）とネットワークの密度（既存の AP の密集度）によって大きく影響されます。インターフェイスを追加できない場合、DCA は冗長無線をモニタ ロールに配置します。
2. モニタ ロール：冗長デュアルバンド無線は、2.4 GHz と 5 GHz の両方の帯域に対するフルタイム スキャン モードに配置されます。8.4 より前のバージョンでは、関与するいずれかの無線（セルをカバーしている無線）がカバレッジ ホールを示していない限り、これは有効期間の割り当てでした。カバレッジ ホールの場合、無線は即座に 2.4 GHz でのサービスに戻ります。8.4 では、最初の割り当てが 30 秒以上モニタ ロールになった後に DCA が 5 GHz 割り当てを再評価できるようにするロジックが追加されました。DCA は、実行されるたびに無線が 5 GHz ロールに割り当て可能かどうかを確認し続けます。

[Client Aware]：バージョン 8.5 の新機能です。クライアント認識型では、カバレッジ サービス優先順位と同じ値（ターゲット -67 dBm およびしきい値）を使用して冗長性に関する決定を行います。ただし、無線のロールがモニタ ロールに配置されている場合、FRA は専用の 5 GHz インターフェイスに対する負荷をモニタし、DCA にこのインターフェイスを 5 GHz に追加するように強く働きかけることで、クライアント密度を高めることができます。これはオン デマンドの超高密度と考えてください。



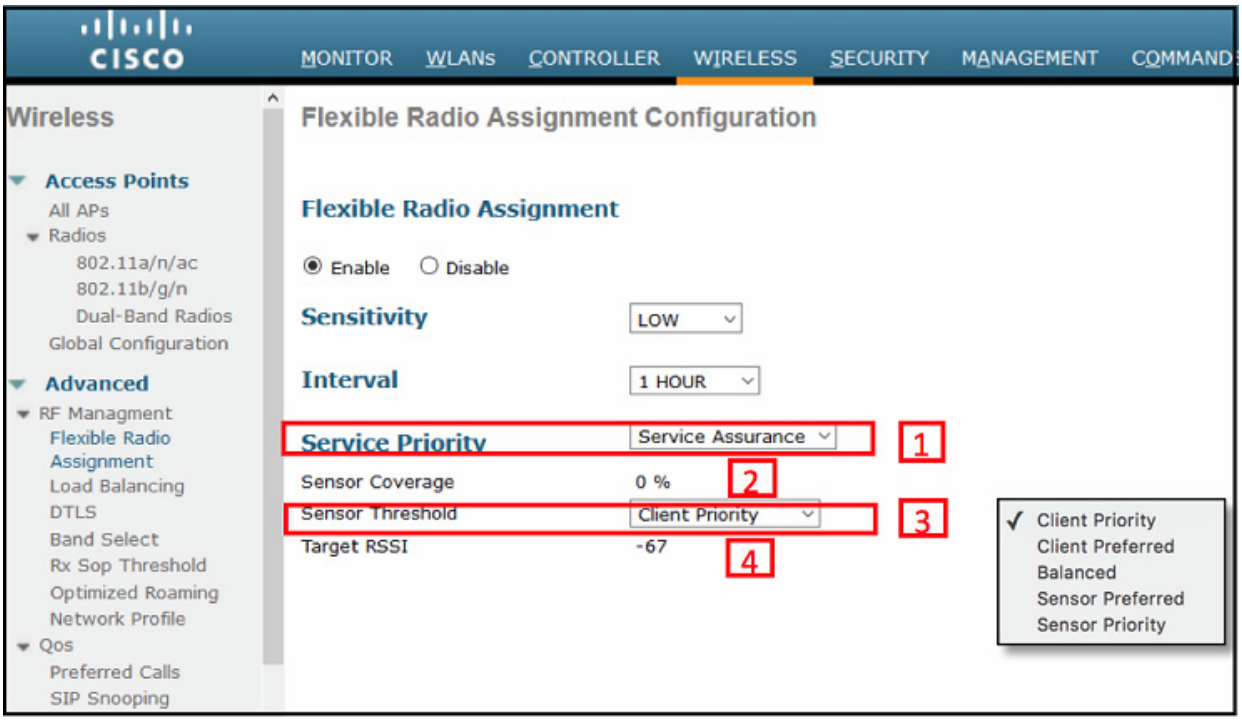
1. [Client Aware]:サービス優先順位モード。
2. [Client Select]:デフォルト値は 50 % です。つまり、専用の 5 GHz インターフェイスのチャネル使用率が 50 % に達すると、モニタ ロール デュアルバンド インターフェイスの 5 GHz クライアント サービス ロールへの移行がトリガーされます。
3. [Client Reset]:AP が 5 GHz AP として AP が動作し始めると、この設定により、デュアルバンド無線をモニタ ロールにリセットするために必要な、無線の合計チャネル使用率が減少します。

例:

1. [Client Aware] を選択した場合、会議室が多数の人でいっぱいになると、会議室にサービスを提供している単一の AP のフレキシブル ラジオがモニタ モードになります。
2. ユーザが専用の 5 GHz 無線にローミングするにつれて、この無線のチャネル使用率が上昇し始めます。チャネル使用率が [Client Select] トリガーしきい値を超えると、DCA は、同一チャネル干渉の許容可能なより低いしきい値を使って冗長インターフェイスを再評価し、それに応じて冗長無線を 5 GHz クライアント サービス ロールに移行します。
3. 両方の無線が 5 GHz になると、システムは両方の無線の合計チャネル使用率をモニタします。デュアル 5 GHz モードで無線 1 の CU が 30 %、無線 2 の CU が 30 % になると、両無線の合計 CU は 60 % になります。デフォルトでは、合計 CU が 5 % 低下すると(この例では 60 % - 5 % で 55 %)、無線は元のモニタ ロールに「リセット」されます。

通常は、緊急コールを発信して無線をモニタ ロールに戻すタイミングを判断するのに 5 % 以上のリセット トリガー バッファが必要になります。クライアントのパフォーマンスの問題を防止することが目的であれば、ロールの変更をトリガーする値は 50 % でおそらく十分です。これらの値は設定可能であるため、個別の要件に合わせてこの機能を調整できます。

[Service Assurance]:8.5 で追加された新しいサービス優先順位です。保証パッケージが追加された DNA-c の指示の下で冗長比をセンサーとして使用できます。FRA の場合、これはターゲット RSSI と設定済みの COF の両方を、[Service Assurance] 設定ダイアログで選択したセンサーしきい値に従って変更できることを意味します。



1. [Service Assurance] を有効にします。
2. [Sensor Coverage]:この値は FRA の設定と計算の積です。[Service Assurance] 優先順位を選択した FRA を初めて実行すると、前の FRA 計算時にセンサーが有効になっているという条件の下で、DNA が到達できる既知のネットワークのパーセンテージがこの値で示されます。この値は、FRA を設定して以下の残りの値に対して実行した後にのみ生成されます。
3. [Sensor Threshold]:5 つの積極性設定のうちの 1 つを選択できます。安全な値を優先するクライアント接続(カバレッジ サービス優先順位と同じ値)から始まり、漸進的にクライアントのカバレッジが減少し、センサーのカバレッジが積極的になります。
4. [Target RSSI]:計算に使用される RSSI で、カバレッジの積極性を徐々に高くするにつれて変化します。

(注)　[Sensor Threshold] 積極性を増やすことで、2.4 GHz のカバレッジを必要なカバレッジよりも小さくすることができます。これが意味することの詳細については、以下を参照してください。

表 3-6

センサーのしきい値	COF%	ターゲット RSSI
クライアントの優先順位	100	-67
優先されるクライアント	100	-70

表 3-6

センサーのしきい値	COF%	ターゲット RSSI
Balanced	100	-73
優先されるセンサー	95	-76
センサーの優先順位	90	-79

ターゲット RSSI が減少すると許容可能なセル サイズが増加し（大きくなり）、冗長とマークする無線の数を増やすためにセル全体にわたって低い電力レベルを許容できるようになります。[Swlwcting the Sensor Priority Sensor Threshold]：他の AP によって -79 dBm 以上の信号強度でセル エリアの 90 % がカバーされているインターフェイスを FRA が冗長とマークできるようにします。これにより、[Client Priority] よりもずっと多くのセンサーがカバレッジ オーバーラップ係数 100 % と -67 dBm 以上の信号強度を持つことが可能になります。

[Service Priority] が [Service Assurance] である場合に冗長とマークされた無線は、引き続き DCA に渡され、上記のとおり 5 GHz またはモニタ ロールを割り当てられます。ただし、DNA Center が保証テストを実行するためにインターフェイスをアクティブ クライアントに変える必要があると判断した場合、無線は呼び出されたときにアクティブ クライアントに変わります。テストが完了すると、無線は前のロールでのサービスに戻ります。

FRA の詳細については、『Radio Resource Management White Paper』を参照してください。

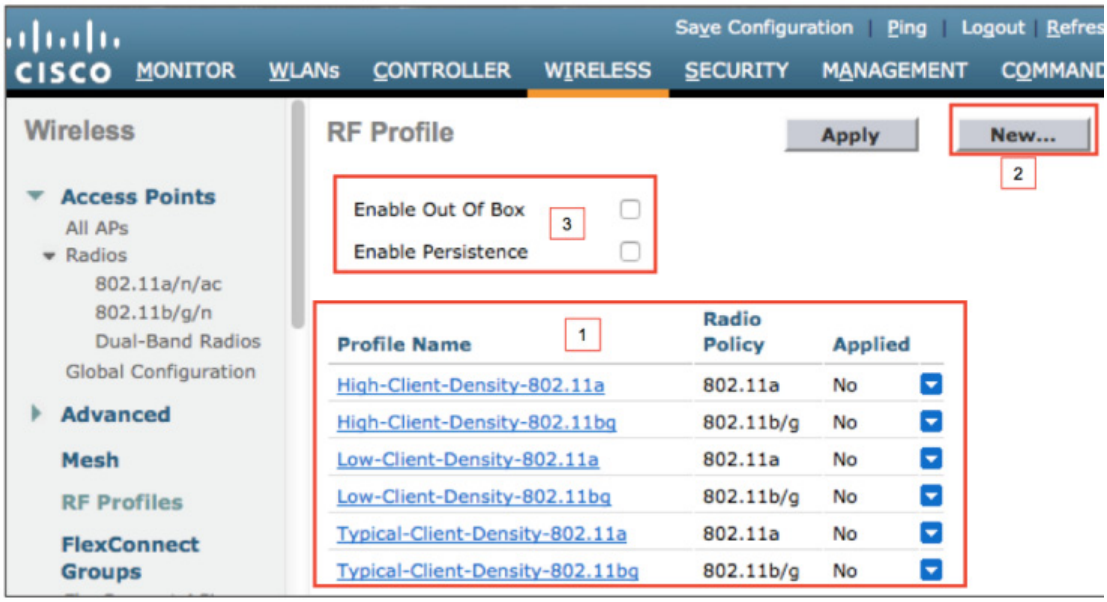
RF プロファイル

グローバル レベルの RRM は、RF グループに関連付けられたすべての AP に適用される設定パラメータを設定します。以前のように、ワイヤレス LAN コントローラの AP の最大数が比較的少なかったとき（100 程度）であれば、それでも問題はありませんでした。しかし、状況は変化し、AP の上限が飛躍的に高くなっただけでなく、ユーザによるネットワーク リソースの消費量も大幅に増えました。高クライアント密度またキャパシティ モデルやカバレッジ モデルなどの異なる使用例により、異なる最適化によって効率性を向上させるとともに設計目標を満たすことが必要になっています。高密度モデルの場合は、最小限の間隔で配置された多数の AP に近づく場合のユーザ エクスペリエンスを最適化する必要があります。カバレッジ モデルの場合は、薄いカバレッジ内の AP からの距離での最大セル カバレッジと信頼性の高い接続を最適化する必要があります。

RF プロファイルにより、同じ AP グループに含まれる AP の一部のグループに変更を適用することができます。AP 上の無線ごとに RF プロファイルを設定し、AP グループあたり 2 つの RF プロファイルを適用することができます。これの典型的な使用例は、高クライアント密度を管理するために大容量設計が必要な講堂や大劇場です。ただし、この劇場は通路やオープン エリアに囲まれており、それらの場所のカバレッジが大きな懸念事項となります。これらの AP のすべてに関する単一のグローバル RRM 設定は、いずれの環境向けにも最適化されていないと考えられる設定になります。劇場内部の AP は 1 つの AP グループ（おそらく、他の高クライアント密度ロケーションの AP によってグループ化される）に配置され、通路やオープン エリアなどのカバレッジ エリアの AP は別の AP グループに配置されます。現在では、目的の設計に必要な設定を最適化する RF プロファイルを設定できます。

RF プロファイルにより、RRM アルゴリズムを超える多数の機能を制御できます。HDX 機能の多くも、特定のグループ向けにカスタマイズできます。コントローラの [Wireless] メニューから、[Wireless]、[Advanced]、[RF Profiles] の順に選択します。

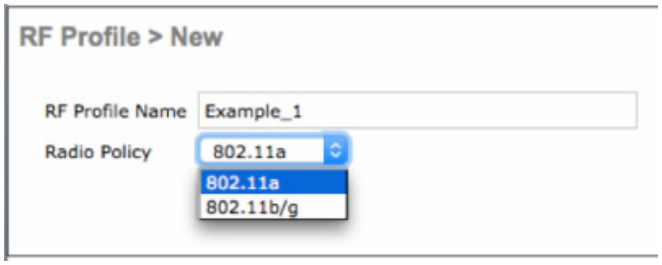
図 3-21　事前設定された RF プロファイル



1. 事前構築されたサンプル RF プロファイル。
2. New:カスタム RF プロファイルを作成します。
3. Enable Out Of Box:任意の新しい AP を、無線が無効になっている Out of Box AP グループに配置します。コントローラを再起動した後も Out of Box(OOB)を有効のままにする場合は、[Enable Persistence] を有効にします。

まず、RF プロファイルに含まれる設定オプションについて説明します。次に、サンプル プロファイルの使用目的と設定について説明します。新しい RF プロファイルを作成するには、[ワイヤレス(Wireless)] > [RF プロファイル(RF Profiles)] の順に移動し、「新規....」(図 19 の「2」)を選択して新規 RF プロファイルのダイアログを開きます。

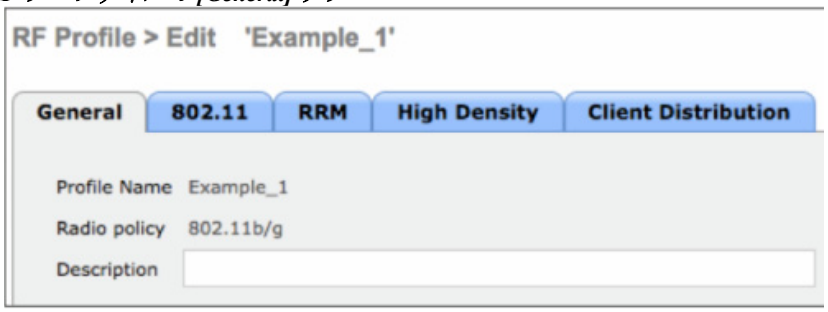
図 3-22　新規 RF プロファイルのダイアログ



まず、RF プロファイルに含まれる設定オプションについて説明します。次に、サンプル プロファイルの使用目的と設定について説明します。新しい RF プロファイルを作成するには、[ワイヤレス(Wireless)] > [RF プロファイル(RF Profiles)] の順に移動し、「新規....」(図 19の「2」)を選択して新規 RF プロファイルのダイアログを開きます。

RF プロファイル：[General]

図 3-23　RF プロファイルの [General] タブ

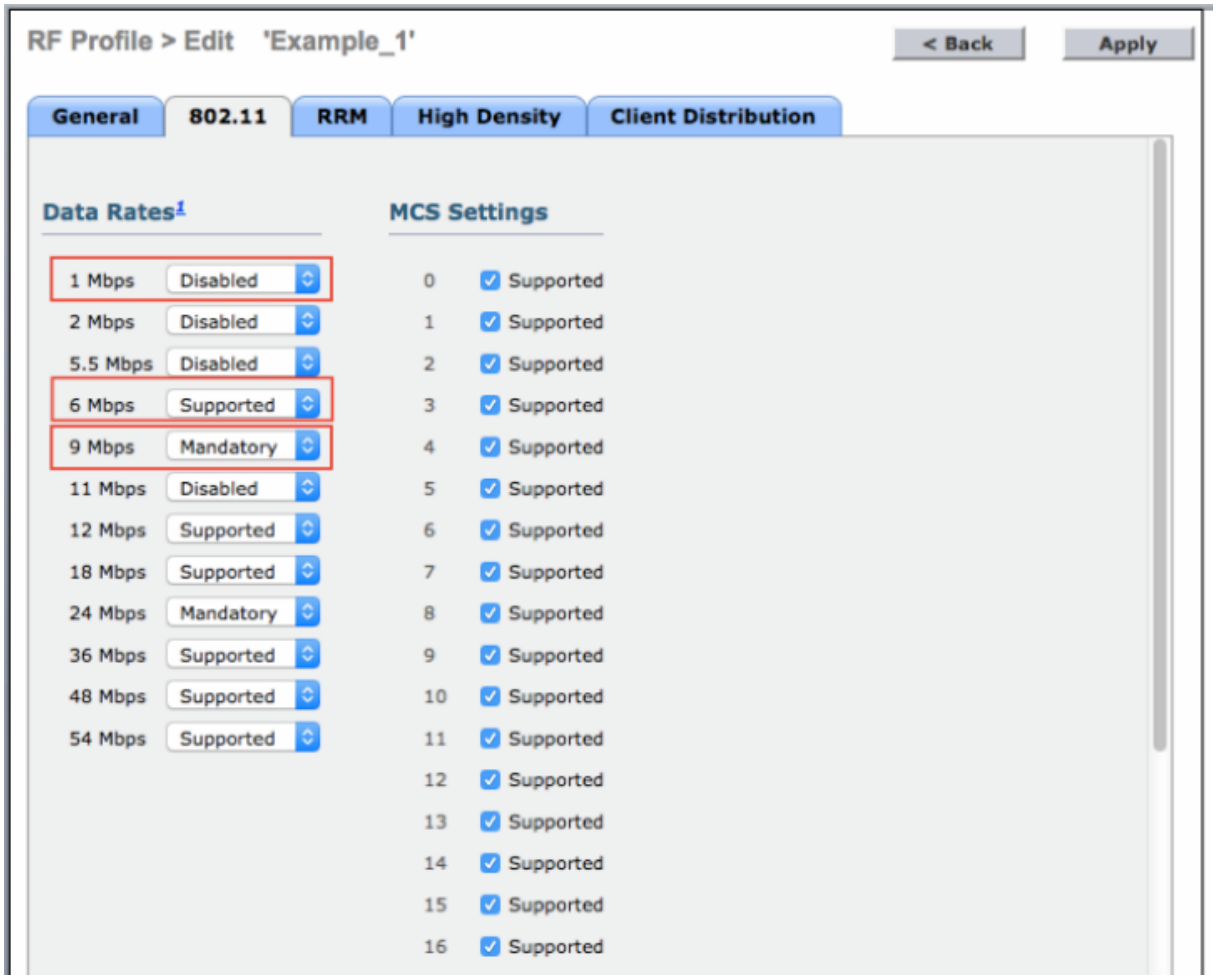


[General] タブでは、このプロファイルの使用に関する簡単な説明を入力できます（最大 64 文字）。[General] タブでは、作成されるプロファイルの対象帯域と RF プロファイル名が特定されます。これらはいずれも作成後に編集できません。作成時に名前を間違えた場合は、プロファイルを削除し、正しい名前で再作成する必要があります。

RF プロファイル：[802.11]

[802.11] タブでは、グローバルではなく、コントローラ固有のネットワーク設定を制御できます。RF プロファイルのこれらの設定は、それが適用される AP グループに関するコントローラのグローバル設定を上書きします。

図 3-24　RF プロファイルの [802.11] タブ



[802.11] タブでは、データ レートとそれらのモードを選択できます。シスコの AP では、データ レートは、次の 3 つの状態のいずれかになります。

1. Disabled：AP によって許可されません。
2. Supported：AP によって許可されますが、必須ではありません。
3. Mandatory：クライアントはこのデータ レートをサポートする必要があります。

最小(最も低い)の [Mandatory] データ レート(上記の例では 9 Mbps)によって、ビーコンおよびその他のすべての後続ブロードキャスト メッセージの送信速度が決定されます。最小の [Mandatory] データ レートとして 9 Mbps を使用してクライアントを AP に関連付けるには、クライアントが 9 Mbps 以上の速度で関連付けを完了できる必要があります。完了できない場合、クライアントの AP への参加が許可されません。これにより、AP のセル サイズが、9 Mbps をサポートするために十分近いクライアントに効果的に制限されます。これは、平均的な配備に関しては適切なデフォルト値です。高クライアント密度では値を 12 Mbps にするか、セル サイズが最小になる極端な高クライアント密度設計では、設計要件に応じて 18、24、または 36 Mbps を選択することもできます。

自動マルチキャストが設定されていない場合(デフォルトでは設定されている)、最大の [Mandatory] データ レート(上記の例では 2 つ目の [Mandatory] データ レート、24 Mbps)がデフォルトのマルチキャスト速度になります。

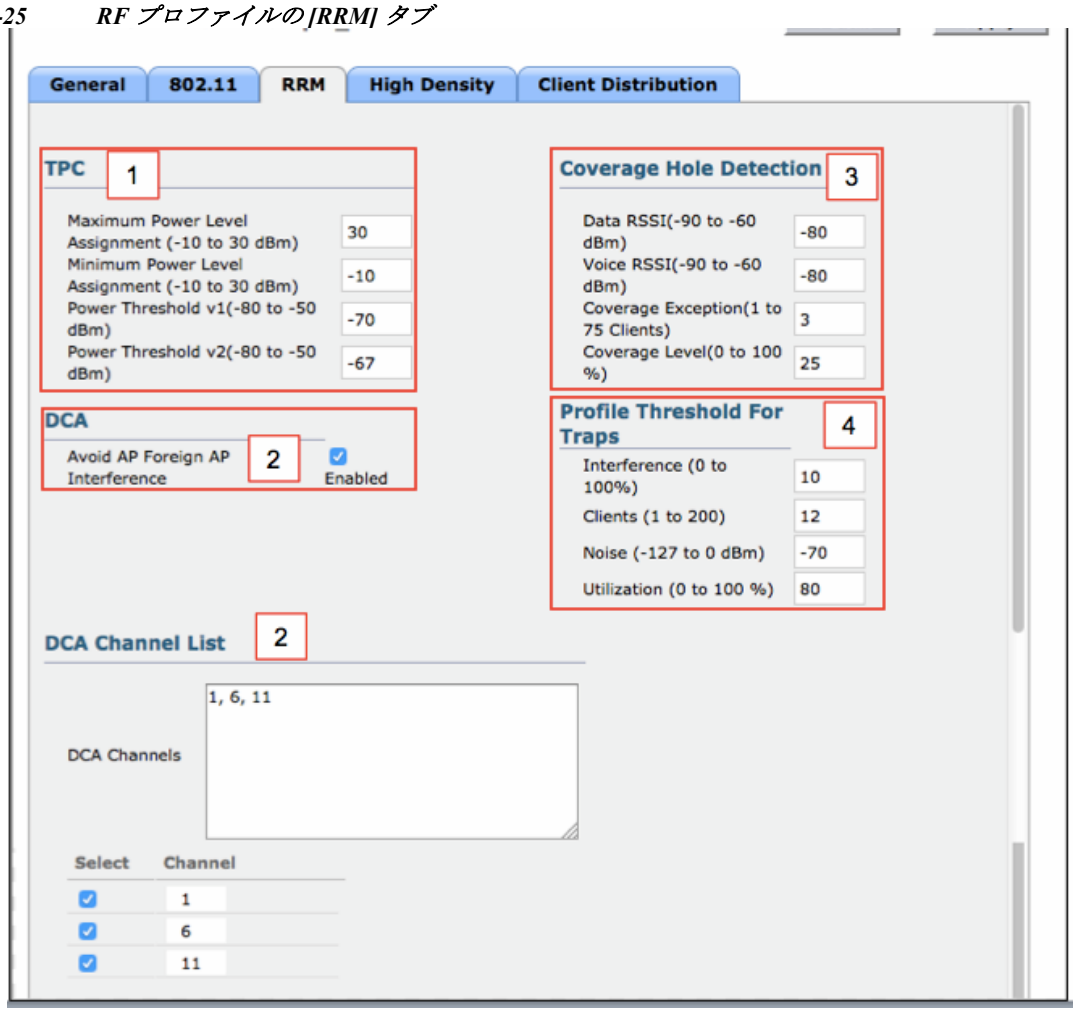
[Supported] としてマークされているデータ レートは、クライアントが使用でき、AP はそれに従います。

[Disabled] としてマークされたデータ レートには AP は従いません。

MCS データ レートは、有効または無効にすることだけができます。これらのレートを無効にすると、AP はそれらを使用できなくなります。すべてのデータ レートと選択内容は、ビーコン フレームの潜在的クライアントにブロードキャストされ、ここで変更がビーコン メッセージに反映されます。

RF プロファイル:[RRM]

図 3-25　RF プロファイルの [RRM] タブ



RF プロファイル内の [RRM] タブでは、RF グループ レベルで設定されているグローバル パラメータを上書きできます。

1. TPC:AP グループ全体に関してカスタム最小/最大電力レベルを割り当てることができ、TPCv1 または TPCv2 のいずれかに関してカスタム TPC しきい値を割り当てることもできます。注:TPC バージョンの選択はグローバル選択のみです。該当する場合は、TPCv1 または TPCv2 しきい値のいずれかが使用されます。

2. DCA：DCA のすべての機能が RF プロファイル レベルで含まれているわけではありませんが、外部 AP 干渉の回避などの最も重要な機能は十分実行できるため、不正なリッチ環境では無効にすることを推奨します。DCA チャネル リストのコピーを使用してカスタム チャネル計画を設定することもできます。RF プロファイル内でチャネルを使用可能にするには、そのチャネルをグローバル DCA チャネル リストで選択する必要があります。
3. [Coverage Hole Detection]：カバレッジ ホールの検出は完全に複製され、AP グループに割り当てられているすべての WLAN に適用されます。個々の WLAN では、コントローラごとのグローバル設定でカバレッジ ホールが有効または無効になっている場合があります。

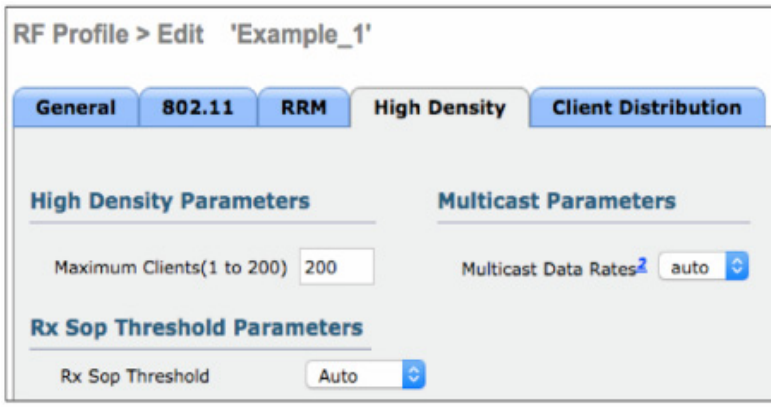
（注）　データ RSSI のエントリは、最適化ローミングがグローバル レベルで有効になっている場合には、最適化ローミングしきい値にも使用されます。有効にする前に「最適化ローミング」を参照してください。

4. [Profile Threshold For Traps]：RF プロファイル内の他のしきい値を設定できます。たとえば、高クライアント密度エリアでは、むしろすべての設定が通常のものになります。これにより、他の方法では過剰に低く設定される AP グループに役立つトラップ アラート メッセージを作成できます。

RF プロファイル：[High Density]

[High Density] タブでは、AP グループに関して、特定の HDX 機能を RF プロファイル レベルで最適化できます。

図 3-26　RF プロファイルの [High Density] タブ

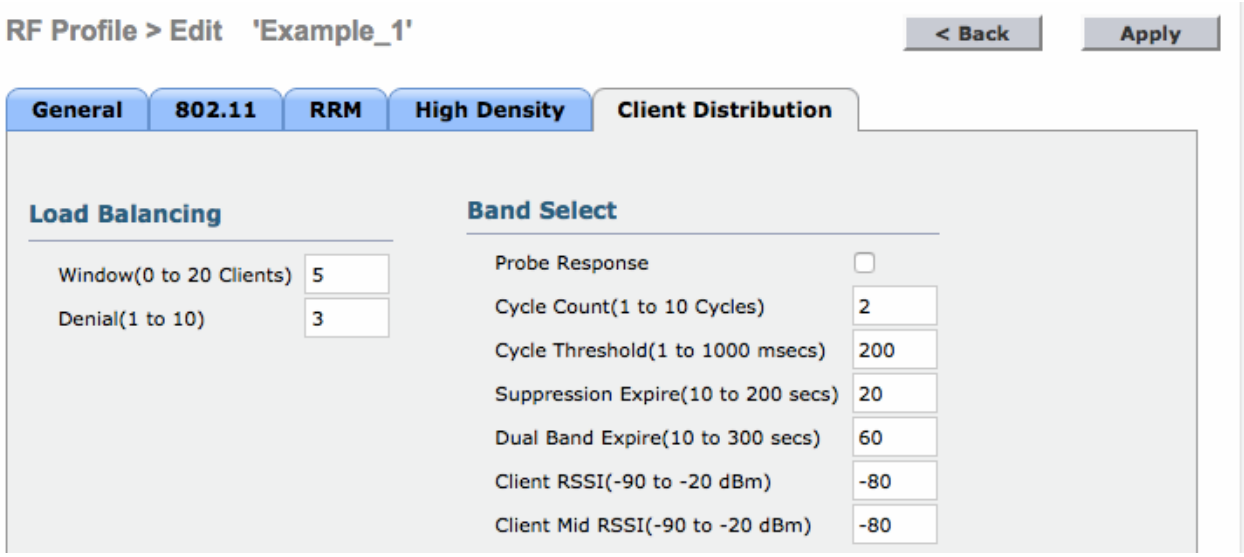


- High Density Parameters：無線インターフェイスで許可されるクライアントの最大数を選択できます。この選択により、選択された数を上回るクライアント数へのアクセスは単純に拒否されます。デフォルト値は 200 です。この設定はデフォルト値のままにすることを推奨します。
- Rx Sop：RX Start Of Packet Sensitivity しきい値を選択できます。選択できるのは、[High]、[Medium]、[Low]、[Auto] です。デフォルトは [Auto] です。RX-SOP とその仕組みおよび設定を十分に理解することを強く推奨します。RX-SOP は、Wi-Fi として受信されるために論理パケットが満たす必要のあるしきい値 RSSI を設定することにより、受信感度を変更します。RX-SOP の設定の詳細については、『High Density Experience Features Release 8.0』を参照してください。
- Multicast Parameters：デフォルトは [auto] です。また、すべてのマルチキャスト パケットが使用する単一の専用データ レートを選択できます。

RF プロファイル：[Client Distribution]

[Client Distribution] タブでは、[Load Balancing] および [Band Select] オプションを制御できます。

図 3-27　RF プロファイルの [Client Distribution] タブ



- Load Balancing：追加のクライアントがステータス コード 17 で拒否される AP に関するしきい値を設定できます。ステータス コード 17 は、AP 上のクライアントが多すぎるために現在 AP がこのリクエストを処理できないことを示します。0 ～ 20 のクライアント数と、アドミッションが付与される前に送信される拒否の数を選択できます。クライアント デバイスはステータス コード 17 を一般にサポートしているわけではないため、この設定は重要です。ロード バランシングは、適切なデータ レートと優れたネットワーク設計の選択により、より確実に実行されるようにすることができます。
- Band Select：802.11b/2.4 GHz プロファイルのみです。[Probe Response] チェックボックスを選択すると、RF プロファイル レベルでの帯域選択設定が有効になり、グローバル レベルでの設定が上書きされます。これにより、選択された AP グループでのみ、より積極的な帯域選択動作が可能になります。

WLAN Express

Release 8.0 で、新しい 0/1 日目起動ダイアログが導入されました。このダイアログは、ワイヤレス LAN コントローラの導入に関するベスト プラクティスを目標とした質問を通じて、ユーザを案内します。この設定ダイアログおよびオプションは、シスコ ワイヤレス LAN コントローラの設定のベスト プラクティスをサポートするように設計されています。このダイアログは、低、中、および高クライアント/AP 密度に適した RF 設定のアプリケーションをサポートし、データ レートに適した選択と、高密度環境をサポートするために設計された機能を適用します。どのビルディングまたは配備も同じではありませんが、アクセス ポイントの展開と意図するクライアント数に基づいて標準化を適用できます。

起動ダイアログに加えて、コントローラに含まれ、参照したり、そのまま適用したりすることができる、3 つの事前設定 RF プロファイルがあります。これらの設定は次のとおりです。

表 3-7　事前設定された RF プロファイル

	依存関係	標準 (企業:デフォルト プロファイル)	高密度 (スループット)	低密度 (カバレッジオープンスペース)	レガシー (RF オプションが無効の場合)
TPC しきい値	帯域ごとのグローバル 帯域ごとの固有 RF プロファイル	デフォルト	-65 dBm (5 GHz) -70 dBm (2.4 GHz)	-60 dBm (5 GHz) -65 dBm (2.4 GHz)	デフォルト
TPC 最小	帯域ごとのグローバル 帯域ごとの固有 RF プロファイル	デフォルト	7 dBm	デフォルト	デフォルト
TPC 最大	帯域ごとのグローバル 帯域ごとの固有 RF プロファイル	デフォルト	デフォルト	デフォルト	デフォルト
Rx 感度 (rxsop)	帯域ごとのグローバル(高度な Rx Sop) RF プロファイル	デフォルト	Medium	low	デフォルト
カバレッジ RSSI しきい値	帯域ごとのグローバル データおよび音声 RSSI(カバレッジ) RF プロファイル	デフォルト	デフォルト	高い	デフォルト
CCA しきい値	帯域ごとにグローバル 802.11a のみ(非表示) RF プロファイル	デフォルト	デフォルト	デフォルト	デフォルト
カバレッジ クライアント数	帯域ごとのグローバル(カバレッジ例外) RF プロファイル(カバレッジ ホールの検出)	デフォルト	デフォルト	Lower (1 ～ 3)	デフォルト
データ レート	帯域ごとにグローバル(ネットワーク) RF プロファイル	12 Mbps 必須 9 をサポート 1、2、5.5、6、11 Mbps 無効	12 Mbps 必須 9 をサポート 1、2、5.5、6、11 Mbps 無効	CCK レート有効 1、2、5.5、6、9、11、12 Mbps 有効	デフォルト
帯域選択	WLAN 単位	有効	有効	無効	有効

表 3-7　事前設定された RF プロファイル(続き)

	依存関係	標準(企業:デフォルト プロファイル)	高密度(スループット)	低密度(カバレッジオープンスペース)	レガシー(RF オプションが無効の場合)
SI	帯域ごとのグローバル(CleanAir)	Enable	有効	有効	有効
ED-RRM		無効	無効	無効	無効
PDA	帯域ごとのグローバル(DCA)	有効	有効	有効	有効
	帯域ごとのグローバル (802.11a/802.11b チャネル…)				
ロード バランシング	WLAN 単位	無効	有効	無効	無効
DCA 感度		デフォルト	大きい	大きい	デフォルト
チャネル	帯域ごとのグローバル(DCA) RF プロファイル	デフォルト	デフォルト	デフォルト	デフォルト

高密度

この文脈における「高密度」とは、平均セル サイズが 3000 ～ 2000 平方フィート(280 ～ 185 平方メートル)で、キャパシティ上の理由から複数の AP が展開されている任意のエリアと考えてください。通常のクライアント数は、セルあたり 50 ～ 100 クライアントです。

AP の距離間隔が約 60 フィート(18 m)の場合、3000 平方フィートのセル サイズになります。

AP の距離間隔が約 50 フィート(15 m)の場合、2000 平方フィートのセル サイズになります。

特定の劇場または講堂を設計している場合、平方メートルあたり 1 ユーザの密度を処理するためにキャパシティを増やすときは、最小データ レートおよび電力レベルに関する設計上の推奨事項に従ってください。

一般的な密度

一般的な密度は、企業での導入の他のほとんどすべてのエリアと、アクティブなクライアントが少し分散しているが連続的なカバレッジが提供されている共通エリアおよび立方体に適用されます。平均セル サイズは 3000 ～ 5000 平方フィート(280 ～ 460 平方メートル)で、セルあたりの平均ユーザ数は 10 ～ 30 人です。

AP の距離間隔が 60 フィート(18 m)の場合、3000 平方フィートのセル サイズになります。

AP の距離間隔が 80 フィート(24 m)の場合、5000 平方フィートのセル サイズになります。

低密度

低密度しきい値は、5000 平方フィート以上の非常に大きなセルに関して提供されます。このプロファイルでは、すべてのデータ レートが有効になっており、TPC しきい値を介して電力レベルが増やされ、セル エッジの最大距離に対応するカバレッジが提供されます。データ レートが低いほど、ユーザあたりの通信時間使用率が高くなります。そのため、この設定ではキャパシティが通信時間によって制限されます。これは、個別のホット スポット アプリケーションまたはオープン フィールドの屋外カバレッジに適した設定です。また、これは、いかなる選択も行わない場合、デフォルトの AP 設定に非常に近いものになります。

RF 電力の用語

dB、dBi、dBr、dBm などの各用語は、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。この項では、これらの用語の違いを説明し、使用に関する一般的なルールについて説明します。実効等方放射電力（EIRP）についても説明します。

dB

dB（デシベル）という用語は、信号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。これは、dB それ自体は測定単位ではないことを意味します。たとえば、dBm の場合は 1 ミリワットの電力に対して信号レベル値が比較され、dBW の場合は 1 ワットの電力に対して値が比較されます。

計算式は次のとおりです。

電力（dB 単位）= 10 X log10（信号/基準）

適切な数字を当てはめると（たとえば、信号に 100 mW、基準に 1 mW）、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、10 dB 増加するたびに 10 倍になることも覚えておいてください（たとえば、0 dBm = 1 mw、10 dBm = 10 mw、20 dBm = 100 mW、30 dBm = 1000 mW（1W））。

対数である場合、いくつかの一般的なルールがあります。3 dB 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。10 dB 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、一般的なルールがあります。9 dB 増加するたびに、屋内のカバレッジ エリアが 2 倍になります。9 dB 減少するたびに、屋内のカバレッジ エリアが 2 分の 1 になります。

dBm

dBm（dB ミリワット）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（0.001 W）です。Wi-Fi での電力は、常に 1 mW 未満です。

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 は送信電力を表すだけでなく、レシーバの感度も表します。Wi-Fi では比較的低い送信電力が使用されるため（受信される信号は常に 1 mW 未満）、レシーバの感度は、マイナス dBm（-dBm）で表されます。感度は、信号を理解不能と見なす前にレシーバが効果的に受信可能な最小電力を示します。

dBi

dBi（等方性 dB）という用語は、架空の等方性アンテナと比較される実際のアンテナの電力ゲインを表すために使用されます。等方性アンテナ（理論上または架空のアンテナ）は、同じ電力密度を完全に全方向に送信するアンテナです。

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、シスコの全方向性 AIR-ANT4941 アンテナのゲインは 2.2 dBi 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 2.2 dB 多いことを意味しています。

実効等方放射電力（EIRP）

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、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、FCC や ETSI などの規制当局が電力制限を決定および測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、送信電力（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、50 フィートの長さの同軸ケーブルで、固定されたパラボラ 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
- 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）
- パラボラ アンテナ：21 dBi
- EIRP：37.7 dBm

詳細および基礎数学については、シスコのテクニカル ノート『RF Power Values』を参照してください。

Cisco Unified Wireless Network アーキテクチャ：基本セキュリティ機能

Cisco Unified Wireless Network ソリューションは、Wireless Local Area Network（WLAN）エンドポイント、WLAN インフラストラクチャ、およびクライアント通信を保護するアーキテクチャと製品セキュリティ機能を使用するエンドツーエンドのセキュリティを提供します。

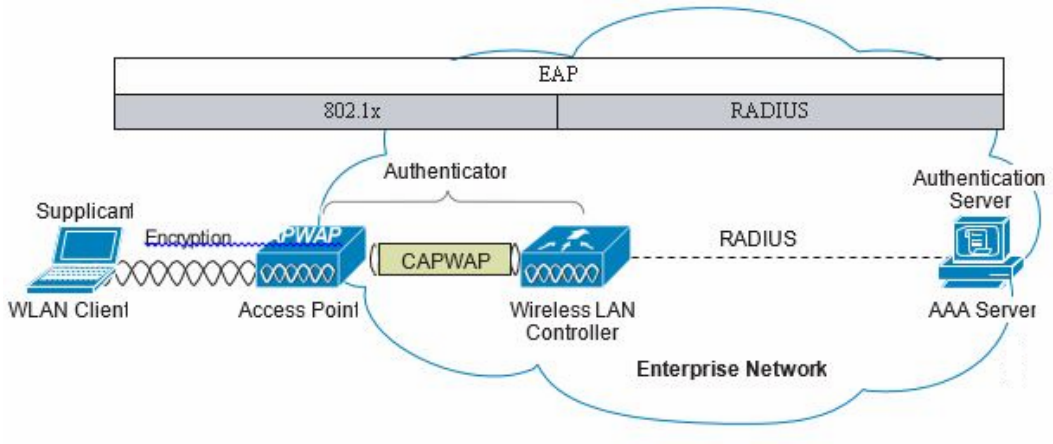
Cisco Unified Wireless Network ソリューションは、IEEE 802.11-2012 標準の基本セキュリティ機能を基盤としています。無線周波数（RF）とネットワーク ベースのセキュリティ機能を強化して全体的なセキュリティを保証します。

セキュアなワイヤレス トポロジ

図 4-1 では、セキュアなワイヤレス トポロジについて説明します。このトポロジは、802.1x 認証プロセスの基本的な役割を持つ次のコンポーネントで構成されます。

- クライアント上に 802.1x サプリカント（無線ソフトウェア）を持つ WLAN クライアント
- Control And Provisioning of Wireless Access Points（CAPWAP）を使用するアクセス ポイント（AP）およびワイヤレス LAN コントローラ（WLC）
- クライアントと認証サーバの間で Extensible Authentication Protocol（EAP）パケットを送受信する RADIUS プロトコル
- 認証サーバとしての認証、認可、およびアカウンティング（AAA）サーバ

図 4-1　　セキュアなワイヤレス トポロジ



WLAN のセキュリティ メカニズム

セキュリティは WLAN ネットワークの認証および暗号化を使用して実装されます。WLAN ネットワークのセキュリティ メカニズムは次のとおりです。

- オープン認証（暗号化なし）
- シスコの WEP 拡張（Cisco Key Integrity Protocol + Cisco Message Integrity Check）
- Wi-Fi Protected Access（WPA）
- WPA2（Wi-Fi プロテクテッド アクセス 2）
- Identity PSK（WPA2 PSK + Mac-Filtering）
- 拡張ローカル モード（ELM）の Cisco Adaptive Wireless Intrusion Prevention System（wIPS）

Wi-Fi Protected Access（WPA）

802.11 の WEP 標準が、暗号化キーの管理方法の問題の処理に失敗しました。暗号化メカニズム自体に問題があることがわかったため、クライアントのトラフィックを監視するだけで WEP キーが獲得できました。IEEE 802.11i 標準は、元の 802.11 WEP の標準に見つかったこれらのセキュリティの問題に対処します。

WPA および WPA2 は Wi-Fi Alliance で定義された 802.11i ベースのセキュリティ ソリューションです。Wi-Fi Alliance は IEEE 802.11 製品の相互運用性を証明し、あらゆる市場セグメントにわたって無線 LAN の標準を推進します。Wi-Fi Alliance の一連のテストでは、他の Wi-Fi 認定製品との相互運用性の認定を取得するために製品をテストする方法を定義します。

WPA は Temporal Key Integrity Protocol（TKIP）を使用して、事前共有キーまたは RADIUS/802.1x ベースの認証による暗号化と動的な暗号キーの生成を行います。WPA で導入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、より堅牢なセキュリティを WEP ソリューションに提供するように設計されています。

Wi-Fi Protected Access 2（WPA2）

WPA2 は、承認された IEEE 802.11i 標準を基礎とする次世代の Wi-Fi セキュリティであり、802.11i 標準の Wi-Fi Alliance の相互運用性を実装することによって認証されます。WPA2 は、企業と個人の分類の両方で認証を行います。

企業の分類には、RADIUS/802.1x ベースの認証と事前共有キーへの対応が必要となります。個人の分類にはクライアントと AP で共有する共通キーのみ必要です。

WPA2 で導入された Advanced Encryption Standard（AES）の新しいメカニズムでは、一般的に WLAN クライアントと AP のハードウェアのアップグレードが必要となります。ただし、すべてのシスコ CAPWAP ハードウェアは WPA2 に対応しています。

802.1X

802.1X は、802.11i のセキュリティ ワークグループによって採用された、ポートベースのアクセス コントロール用 IEEE フレームワークです。このフレームワークは、WLAN ネットワークに認証されたアクセスを提供します。

- 802.11 アソシエーション プロセスは、AP の各 WLAN クライアントに対する「仮想」ポートを作成します。
- この AP により、802.1X ベースのトラフィックを除くすべてのデータ フレームがブロックされます。
- 802.1X フレームは EAP 認証パケットを伝送します。EAP 認証パケットはそこから AP によって AAA サーバに渡されます。
- EAP 認証に成功すると、AAA サーバは AP に EAP 成功メッセージを送信します。その後 AP によって、WLAN クライアントから仮想ポートへデータ トラフィックが渡されることが許可されます。
- 仮想ポートを開く前に、WLAN クライアントと AP の間にデータ リンク暗号化が確立されます。これは、クライアントを認証するように設定されたポートに他の 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。

Identity PSK

Identity PSK（IPSK）機能は、ますます増加するインターネット接続デバイスをサポートし、802.1X セキュリティ プロトコルはサポートしません。これらのデバイスは、WSA PSK プロトコルを使用してネットワークに接続できます。IPSK 機能を使用すると、ネットワーク上の個々のデバイスまたはデバイス グループを一意の事前共有キーで簡単かつ安全に接続できます。

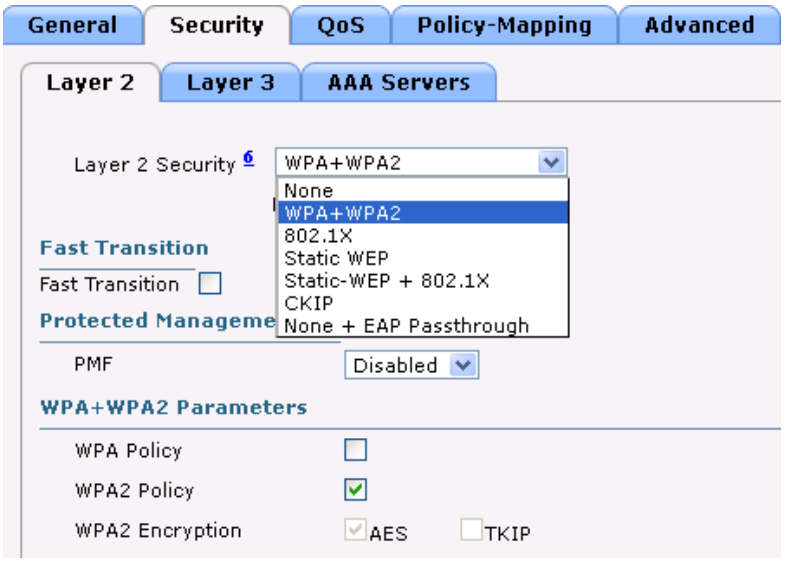
認証および暗号化

Cisco Wireless Security Suite は、必須または既存の認証、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を基礎とするセキュリティのアプローチのオプションを提供します。Cisco Wireless Security Suite では、ELM 機能を含む WPA、WPA2、WEP Extension および wIPS をサポートします。

次のオプションを使用できます。

- 次の EAP 方式を使用した 802.1X に基づく認証：
  - Cisco LEAP、すなわち Secure Tunneling（EAP-FAST）を介した EAP-Flexible Authentication
  - 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 Encryption WPA2
  - TKIP 暗号化拡張機能：キー ハッシング（パケットごとのキーイング）、メッセージ整合性チェック（MIC）、および WPA/WPA2 または WEP TKIP Cisco Key Integrity Protocol（CKIP）によるブロードキャスト キー ローテーション



非 802.1X 認証用の Identity PSK

Identity PSK は、WPA-PSK の手軽さと RADIUS 統合を組み合わせたもので、802.1X サプリカントをサポートしていない多くのデバイスにとって理想的な代替手段です。また、同じ WLAN 内のさまざまなクライアントに対して一意の事前共有キーを有効にする簡単な方法でもあります。柔軟性に優れているため、追加された AAA オーバーライド機能によりポリシーの配布を強化することもできます。

- WPA-PSK および Mac：RADIUS によってクライアントの MAC が認証され、パスフレーズが VSA の一部として WLC に送信されます。

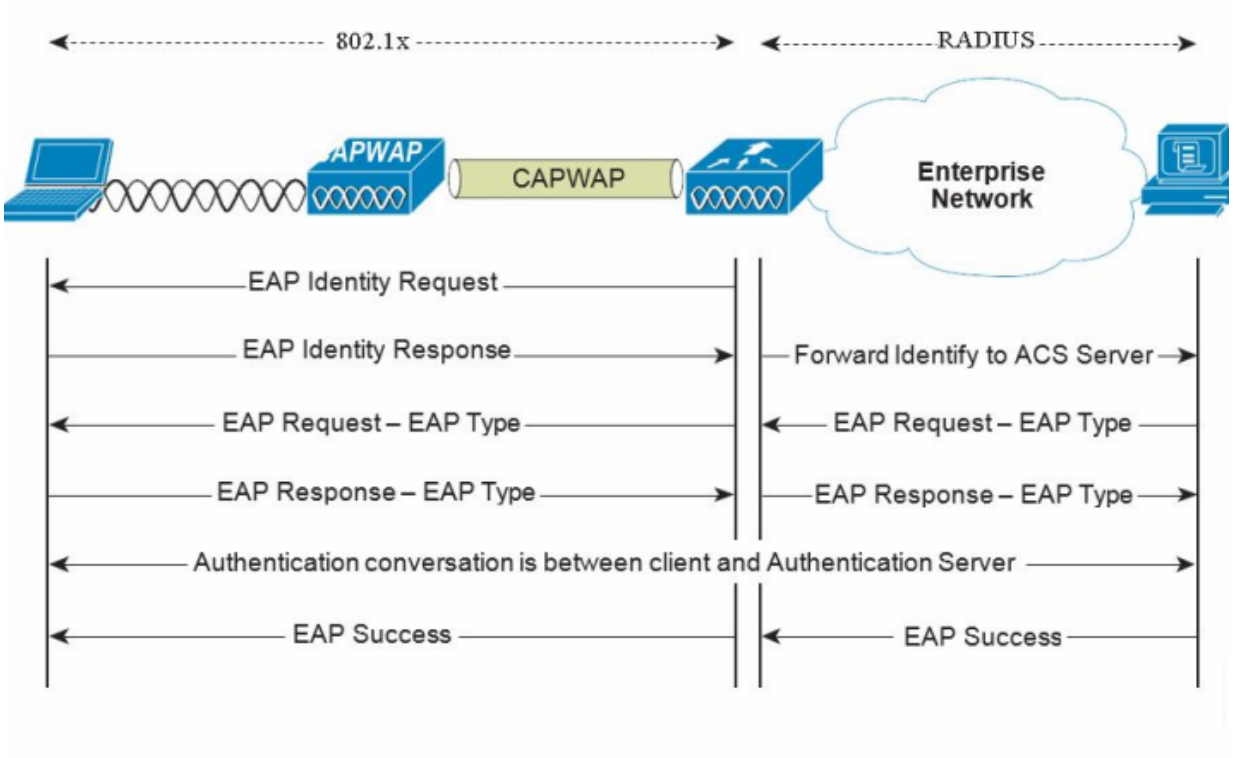
Extensible Authentication Protocol（EAP）

Extensible Authentication Protocol（EAP）は、トランスポート プロトコルから認証プロトコルを分離する必要があることを規定する IETF RFC です。これにより、802.1X や UDP、RADIUS などのトランスポート プロトコルによって EAP プロトコルを伝送できるようになります。認証プロトコル自体は変わりません。基本の EAP プロトコルには次の 4 種類のパケット タイプが含まれます。

- EAP 要求：要求パケットがオーセンティケータによってサプリカントに送信されます。各要求には type フィールドがあり、要求されている内容を示します。これには、使用されるサプリカント アイデンティティや EAP タイプなどが含まれます。シーケンス番号により、オーセンティケータおよびピアは、各 EAP 要求に対応する EAP 応答を一致できます。
- EAP 応答：応答パケットがサプリカントによってオーセンティケータに送信された後、シーケンス番号を使用して最初の EAP 要求と照合します。EAP 応答のタイプは通常 EAP 要求と一致しますが、応答が否定応答（NAK）の場合は除きます。
- EAP 成功：認証の成功が発生すると、成功パケットがオーセンティケータからサプリカントへ送信されます。
- EAP 失敗：認証の失敗が発生すると、失敗パケットがオーセンティケータからサプリカントへ送信されます。

EAP を 802.11i 準拠のシステムで使用すると、AP は EAP パススルー モードで動作します。パススルー モードではコード ID と長さフィールドを検査し、その後受信した EAP パケットをクライアント サプリカントから AAA に転送します。AAA サーバからオーセンティケータによって受信された EAP パケットが、サプリカントに転送されます。図 4-2 では、EAP プロトコルのフローの例を示します。

図 4-2　EAP プロトコルのフロー



認証

要件に応じて、安全な無線の展開には PEAP や EAP-TLS、EAP-FAST などのさまざまな認証プロトコルが使用されます。プロトコルに関係なく、無線の展開には 802.1X、EAP および RADIUS が基本的な伝送手段として必ず使用されます。

これらのプロトコルにより、WLAN クライアントの認証の成功に基づいたネットワーク アクセス コントロールが可能になります。その逆も同様です。このソリューションでは、RADIUS プロトコルによって伝送されるポリシーを介した承認のほか、RADIUS アカウンティングも提供します。

認証の実行に使用する EAP の種類については、以降で詳しく説明します。EAP プロトコルの選択に影響する主な要因は、現在使用されている認証システム（AAA）です。理想的には、安全な WLAN を展開するために新しい認証システムを導入する必要はありませんが、すでに使用されている認証システムを活用する必要があります。

サプリカント

市場で入手可能なさまざまな EAP サプリカントには、使用可能な認証ソリューションと顧客の要望の多様性が反映されています。

表 4-1 では、一般的な EAP サプリカントの概要を示します。

- EAP-FAST：EAP-Flexible Authentication via Secured Tunnel。PEAP で使用されているものと類似したトンネルを使用しますが、公開キー インフラストラクチャ（PKI）を使用する必要はありません。
- 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でのカプセル化された MSCHAPv2 の交換を保護します。
- PEAP GTC：Protected EAP Generic Token Card（GTC）。TLS トンネルを使用して、汎用トークン カードの交換（ワンタイム パスワードや LDAP 認証など）を保護します。
- EAP-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および認証サーバの証明書が必要となります。

表 4-1　一般的な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）	○	○	○[1]	○
ログイン スクリプト（MSFT AD のみ）	○	○	一部	○[2]
パスワード変更（MSFT AD）	○	○	○	該当なし
Microsoft AD データベース サポート	○	○	○	○
ACS ローカル データベース サポート	○	○	○	○
LDAP データベース サポート	○[3]	×	○	○
OTP 認証サポート	○[4]	×	○	非対応
RADIUS サーバ証明書は必要か	×	○	○	○

表 4-1　一般的なサプリカントの比較

	Cisco EAP-FAST	PEAP MS-CHAPv2	PEAP EAP-GTC	EAP-TLS
クライアント証明書は必要か	×	×	×	○
匿名	○	○[5]	○[6]	非対応

1. サプリカントに依存。
2. マシン アカウントとマシン認証はスクリプトをサポートするために必要です。
3. 自動プロビジョニングは、LDAP データベースではサポートされていません。
4. サプリカントに依存。
5. サプリカントに依存。
6. サプリカントに依存。

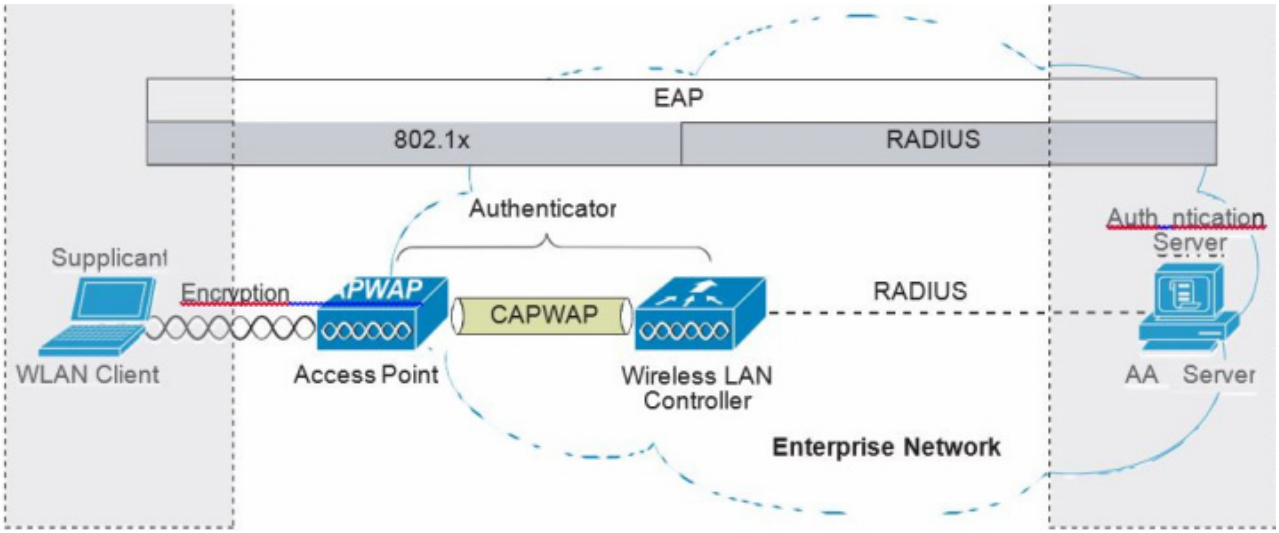
オーセンティケータ

WLC は、802.1X ベースのサプリカントと RADIUS 認証サーバ間で交換される EAP メッセージのリレーとして機能するオーセンティケータです。認証が正常に完了した場合、WLC は次のものを獲得します。

- EAP 成功メッセージを含む RADIUS パケット
- EAP 認証中に認証サーバで生成される暗号化キー
- 通信ポリシーの RADIUS ベンダー固有の属性（VSA）

図 4-3 では、全体的な認証アーキテクチャ内のオーセンティケータの論理的ロケーションを示します。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の間で EAP メッセージをリレーします。

図 4-3　　オーセンティケータのロケーション



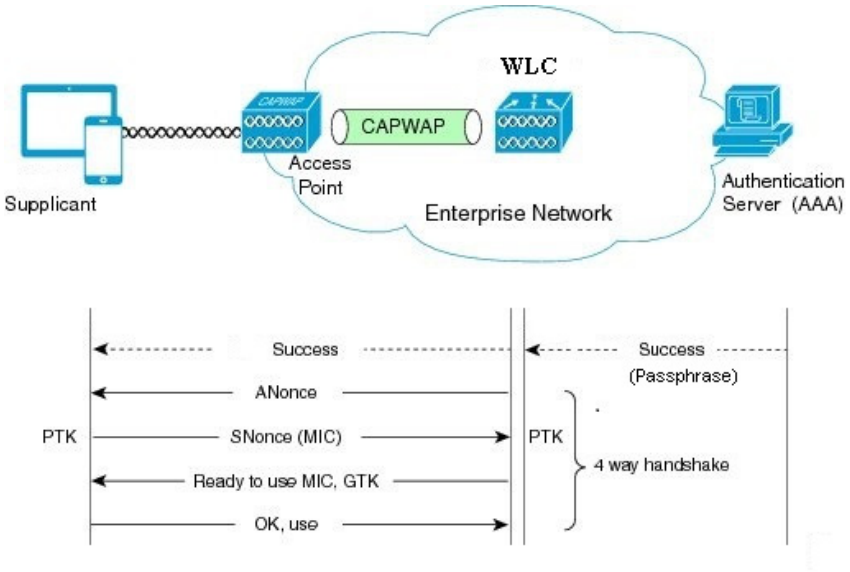
EAP の交換の手順は次のとおりです。

- パケット 1 が、AP によってクライアントに送信されます。このときクライアントの識別情報が要求されます。これにより、EAP 交換が開始されます。
- パケット 2 には、RADIUS サーバに転送されるクライアント ID が含まれています。パケット 2 内のクライアント ID に基づいて、EAP 認証を継続するかどうかを RADIUS サーバが判断します。
- パケット 3 には、認証のための EAP 方式として PEAP を使用する RADIUS サーバ要求が含まれます。実際の要求は、RADIUS サーバで設定された EAP の種類によって異なります。クライアントが PEAP 要求を拒否すると、RADIUS サーバは別の種類の EAP を提示できます。
- 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 内の認証交換です。
- パケット 17 は、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 EAP メッセージです。また、パケット 17 は暗号キーと認証情報を RADIUS VSA の形式でオーセンティケータに伝送します。

Identity PSK を使用するオーセンティケータ

- クライアントがアクセス ポイントによってブロードキャストされた SSID にアソシエーション要求を送信すると、ワイヤレス LAN コントローラはそのクライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバに中継します。
- RADIUS サーバは、認証を実行し（クライアントが許可されるかどうかを確認し）、ACCESS-ACCEPT または ACCESS-REJECT のいずれかの応答を WLC に送信します。
- ダイナミック PSK をサポートするため、認証サーバは認証応答を送信するだけでなく、この特定のクライアント用のパスフレーズも提供します。このパスフレーズは PSK の計算にも使用されます。

- RADIUS サーバは、ユーザ名、VLAN、QoS など、このクライアントに固有の追加パラメータも応答に含めることができます。1 人のユーザが複数のデバイスを所有している場合は、すべてのデバイスで同じパスフレーズを使用できます。
- WLC は、パスフレーズ/PSK 計算を受け取ると、次の図（図 4-x）に示すように、4 ウェイ ハンドシェイク プロセスを使用して PTK を生成します。

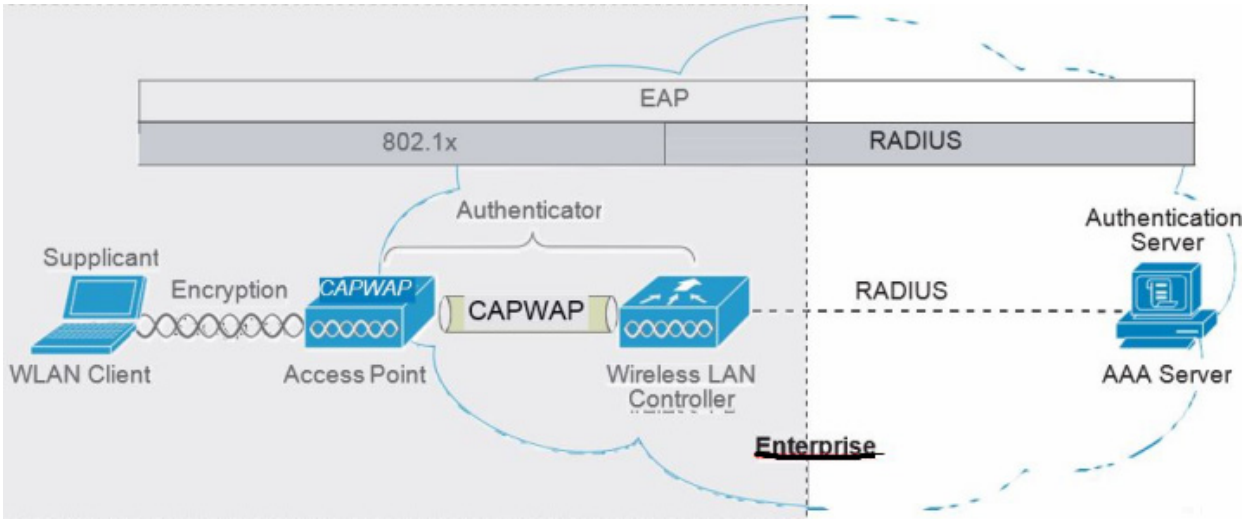


認証サーバ

Cisco Secure Unified Wireless Network ソリューションで使用される認証サーバは、Cisco Access Control Server（ACS）および Cisco Identity Services Engine（ISE）です。ACS は、Windows サーバにインストールされるソフトウェアまたはアプライアンスとして使用できます。ISE は、VM サーバにインストールされるソフトウェアとして使用できます。あるいは、特定の WLAN インフラストラクチャ デバイス内に認証サーバの役割を実装することもできます。たとえば、IOS AP 上のローカル認証サービス、WLC 内のローカル EAP 認証のサポート、必要な EAP タイプをサポートする任意の AAA サーバに組み込まれた AAA サービスなどです。

図 4-4 では、RADIUS トンネルを介して EAP 認証を実行する、全体的な無線認証アーキテクチャ内の認証サーバの論理的ロケーションを示しています。

図 4-4　　認証サーバのロケーション



EAP 認証が正常に完了すると、認証サーバからオーセンティケータに EAP 成功メッセージが送信されます。このメッセージは、EAP 認証プロセスが正常に行われたことをオーセンティケータに通知し、その結果として WLAN クライアントと AP の間の暗号化されたストリームを作成する際の基礎として使用される Pairwise Master Key（PMK）をオーセンティケータに渡します。

暗号化

暗号化は、ローカル RF ブロードキャスト ネットワーク上にプライバシーを提供する WLAN セキュリティの必須コンポーネントです。新しく展開を行う際は、TKIP（WPA/WPA2）または AES 暗号化を使用する必要があります。

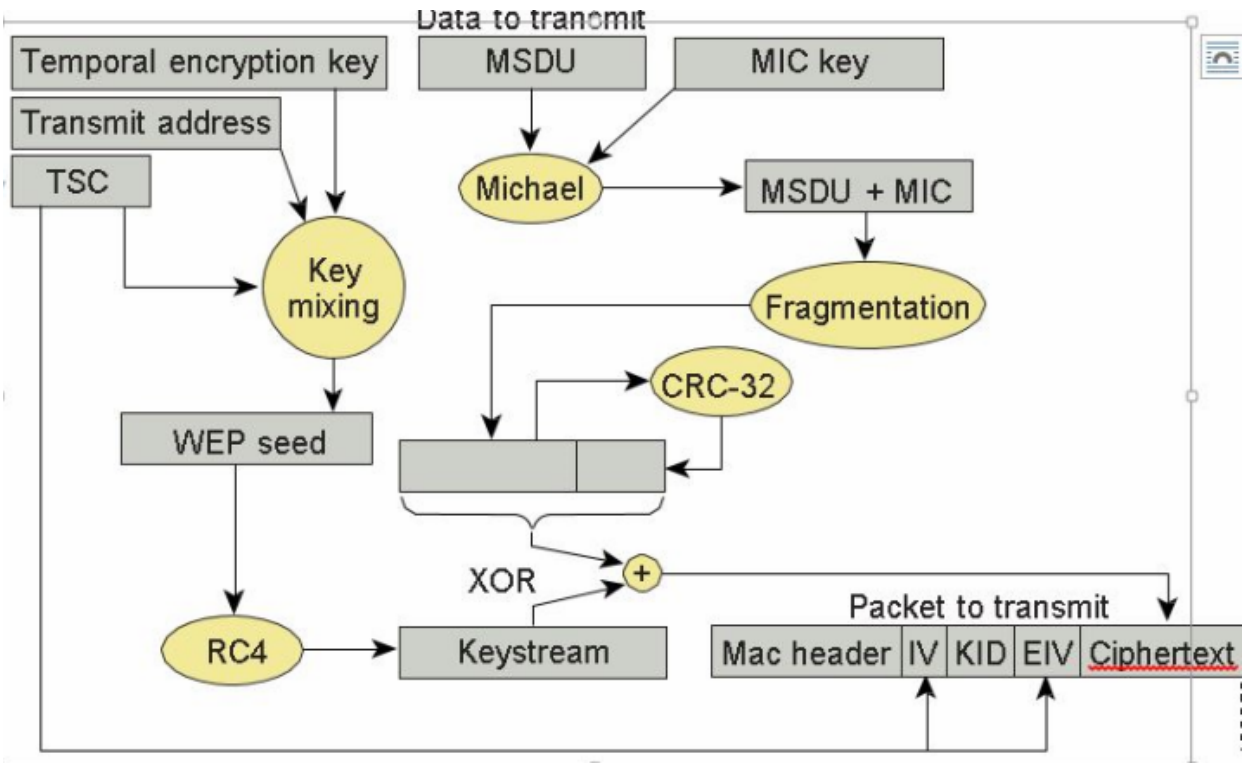
WPA および WPA2 では、暗号キーはフォーウェイ ハンドシェイク中に取得されます。フォーウェイ ハンドシェイクについてはこのセクションで後ほど説明します。

TKIP の暗号化

802.11i で指定されたエンタープライズ レベルの暗号化メカニズムは Wi-Fi Alliance による WPA/WPA2 および wIPS、すなわち Temporal Key Integrity Protocol（TKIP）、および Advanced Encryption Standard（AES）として認証されます。TKIP は認定された暗号化方式です。802.11 WEP 暗号化方式に関連した元の欠点に対応することによって、レガシーの WLAN 機器をサポートしています。TKIP ではこれを行うために、元の RC4 コア暗号化アルゴリズムを利用します。

WLAN クライアント デバイスのハードウェア更新サイクルから、数年間は TKIP および AES が一般的な暗号化となりそうです。AES 暗号化によって、より幅広い IT 業界の標準やベスト プラクティスに沿った WLAN 暗号化規格がもたらされるため、AES 暗号化が望ましい方式です。図 4-5 では、基本的な TKIP のフロー チャートを表示します。

図 4-5　　TKIP フロー チャート



TKIP の主な 2 種類の機能は、MAC Service Data Unit（MSDU）の RC4 暗号化を使用するパケットごとのキーと、暗号化されたパケット内にメッセージ完全性チェック（MIC）を生成することです。パケットごとのキーは、送信アドレス、フレームの初期化ベクトル（IV）、および暗号キーのハッシュです。IV はそれぞれのフレーム送信に従って変化するため、RC4 暗号化に使用されるキーはフレームごとに固有のものです。

MIC は、ユーザ データと MIC キーを組み合わせるために Michael アルゴリズムを使用して生成されるものです。Michael アルゴリズムにはトレードオフがあり、演算のオーバーヘッドが少なくパフォーマンスは良いものの、アクティブな攻撃にさらされやすくなる可能性があります。この問題に対処するため、WPA には、一時的な WLAN クライアントの切断や新しいキーのネゴシエーションを 60 秒間許可しないなどの攻撃を防御するための対策が含まれます。しかし、この動作自体が一種の DoS 攻撃になる場合もあります。多くの WLAN 展開では、このような対策機能を無効にすることもできます。

Wi-Fi® デバイスからの TKIP の削除

Wi-Fi Alliance および 802.11 WPA によると、Temporal Key Integrity Protocol（TKIP）を使用するワイヤレス ネットワークでは、ユーザまたは企業の Wi-Fi® ネットワークを保護するために十分なセキュリティが提供されません。TKIP は、一部の暗号攻撃に対して既知の脆弱性がある古いセキュリティ テクノロジーです。TKIP は、一部の暗号攻撃に対して既知の脆弱性がある古いセキュリティ テクノロジーです。TKIP および WEP では基盤となる暗号が同じため、結果的に多くの類似する攻撃に弱くなります。TKIP は、2004 年に WEP を実装したデバイス向けに設計された過渡期のメカニズムで、AES はサポートしていません。TKIP の既知の脆弱性により、TKIP を使用するネットワークは攻撃の影響を受けやすくなります。

推奨事項：

- ネットワーク管理者は、WPA2 をサポートしている機器を購入または導入する必要があります。
- ネットワーク管理者は、WPA2 のみを使用するように AP を設定する必要があります。
- 機器ベンダーは、内部調査で市場の需要がなくなったと示されたら、カスタマー ベースに対しては TKIP を使用しないよう助言し、製品内の機能を削除することによって、TKIP サポートから積極的に移行していく必要があります。

Wi-Fi Alliance は、機器ベンダーに対して短期間で TKIP の使用を減らし、市場の需要がなくなったら最終的にはすべての Wi-Fi デバイスから TKIP を削除することを推奨しています。少なくとも、ベンダーは、プライマリ デバイス インターフェイスから TKIP および「TKIP のみ」モードの設定を削除する必要があります。セカンダリ設定インターフェイス経由で「TKIP のみ」の設定モードにアクセスすることは可能です。セカンダリ インターフェイスにアクセスするには、レガシー デバイスを使用する展開のみに TKIP の使用を制限するためのメカニズムが必要です。その他の展開では、通常、プライマリ設定インターフェイスを使用します。

移行の例外：

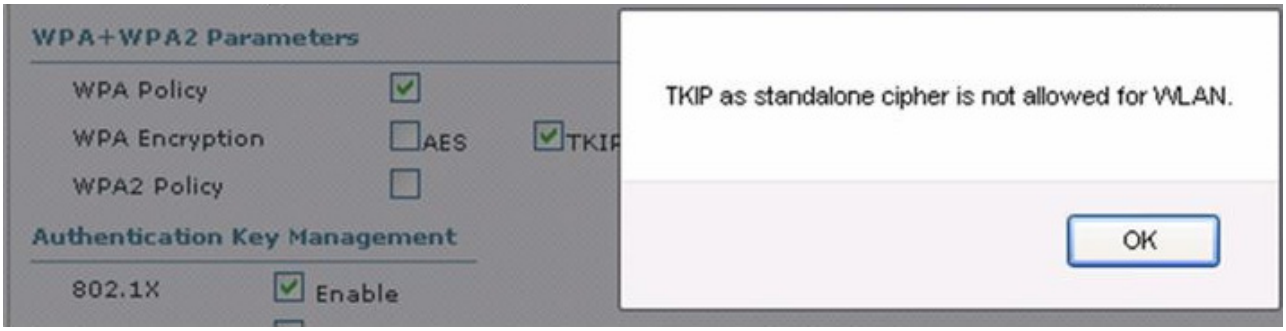
ベンダーは、プライマリ デバイス インターフェイスから TKIP および「TKIP のみ」モードの設定を削除する必要があります。セカンダリ設定インターフェイス経由で「TKIP のみ」の設定モードにアクセスすることは可能です（CLI）。

詳細については、『Technical Note - Removal of TKIP from Wi-Fi Devices』を参照してください。

シスコは、Wi-Fi Alliance が推奨するように、CLI モードからのみ TKIP を設定するための一連のコマンドを開発しました。

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers tkip <en/dis> <wlan#>
(Cisco Controller) >test wlan standalone-tkip <enable/disable> <wlan#>>
```

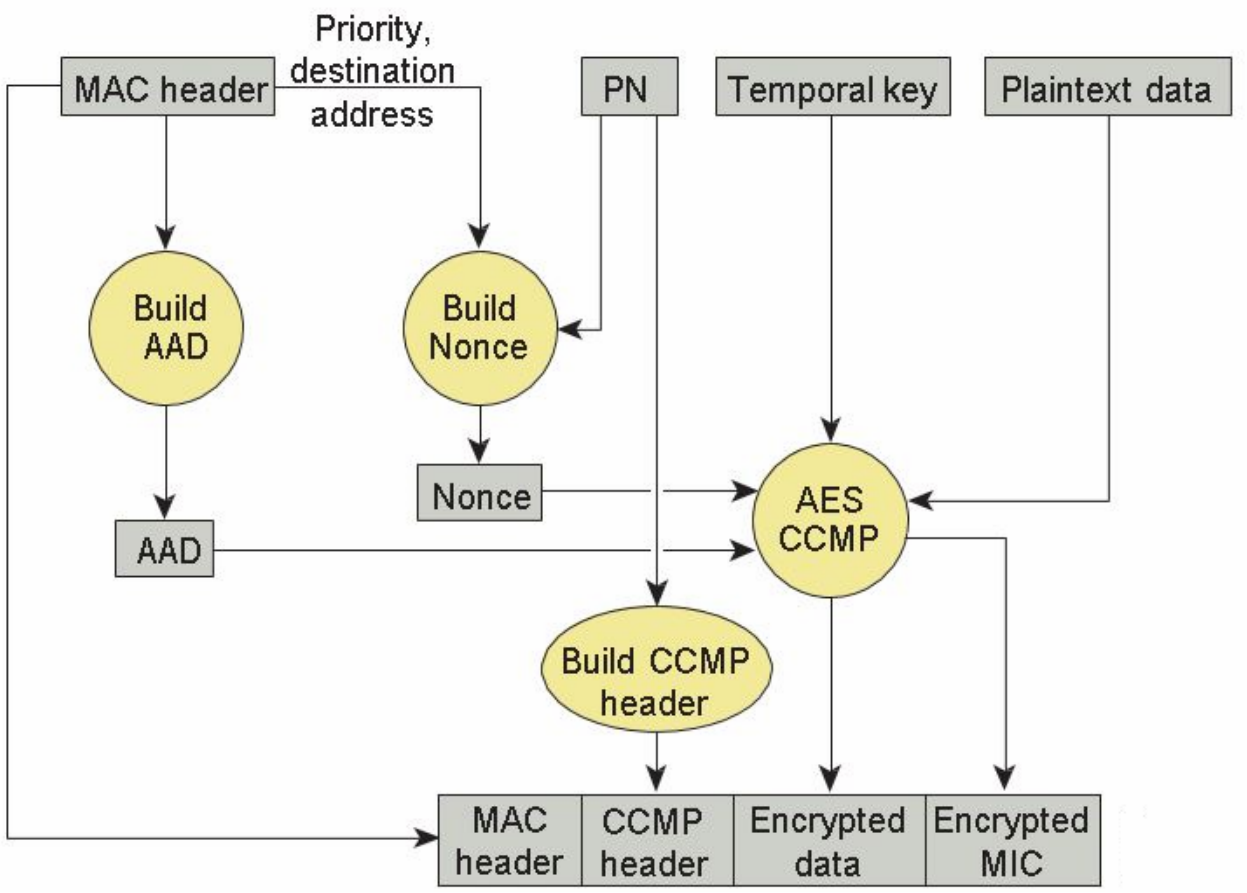
GUI インターフェイスから同じ設定が試行されると、画面に次のように表示されます。



AES の暗号化

図 4-6 では、基本的な AES カウンタ モード/CBC MAC Protocol（CCMP）のフロー チャートを示します。CCMP は、カウンタ モードが機密性を提供し、CBC MAC がメッセージの完全性を提供する AES 暗号化モードの 1 つです。

図 4-6　WPA2 AES CCMP



CCMP の手順では、追加の認証データ（AAD）は MAC ヘッダーから取り出され、CCM 暗号化プロセスに含まれます。これにより、フレームの暗号化されていない部分の変更からフレームを保護します。

リプレイ攻撃を防御するため、シーケンスト パケット番号（PN）は CCMP ヘッダーに含まれています。CCM 暗号化プロセスで順番に使用される nonce を生成するため、PN および MAC ヘッダーの一部が使用されます。

フォーウェイ ハンドシェイク

フォーウェイ ハンドシェイクは、無線データ フレームを暗号化するための暗号化キーを取得するために使用される方式です。図 4-7 では、暗号化キーを生成するために使用されるフレーム交換を図示します。これらのキーを一時キーと呼びます。

暗号化キーは、EAP 認証中に相互に取得される PMK から取得されます。この PMK は EAP Success メッセージの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。これは、サプリカントがコピーした PMK 自体で生成するためです。

1. オーセンティケータは、オーセンティケータの nonce（ANonce）を含む EAPOL キー フレームを送信します。ANonce はオーセンティケータによって生成される乱数です。

   サプリカントは、ANonce とサプリカントの nonce（SNonce）から PTK を取得します。SNonce 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。

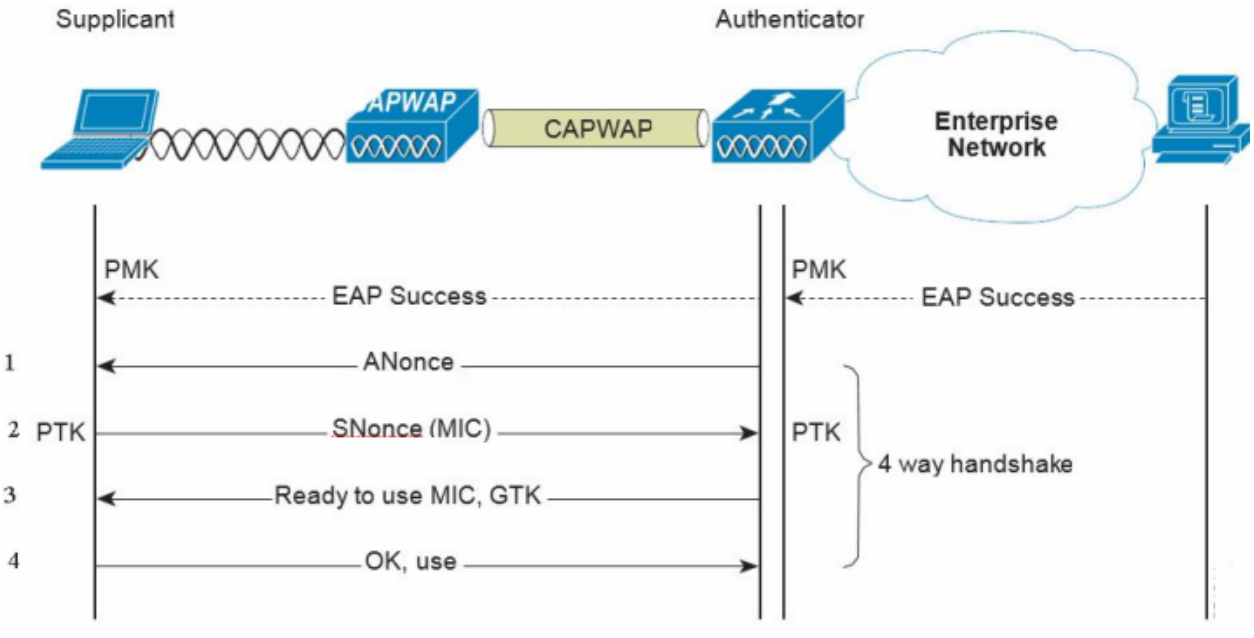
2. サプリカントは、SNonce、（再）アソシエーション要求フレームの RSN 情報要素、および MIC を含む EAPOL キー フレームを送信します。

   オーセンティケータは、ANonce および SNonce から PTK を取得し、EAPOL キー フレーム内の 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の RSN 情報要素、一時キーをインストールするかどうかを判断する MIC、およびカプセル化されたグループ一時キー（GTK）であるマルチキャスト暗号キーを含む EAPOL キー フレームを送信します。

4. サプリカントは EAPOL キー フレームを送信し、これらの一時キーが組み込まれたことを確認します。

図 4-7　　フォーウェイ ハンドシェイク

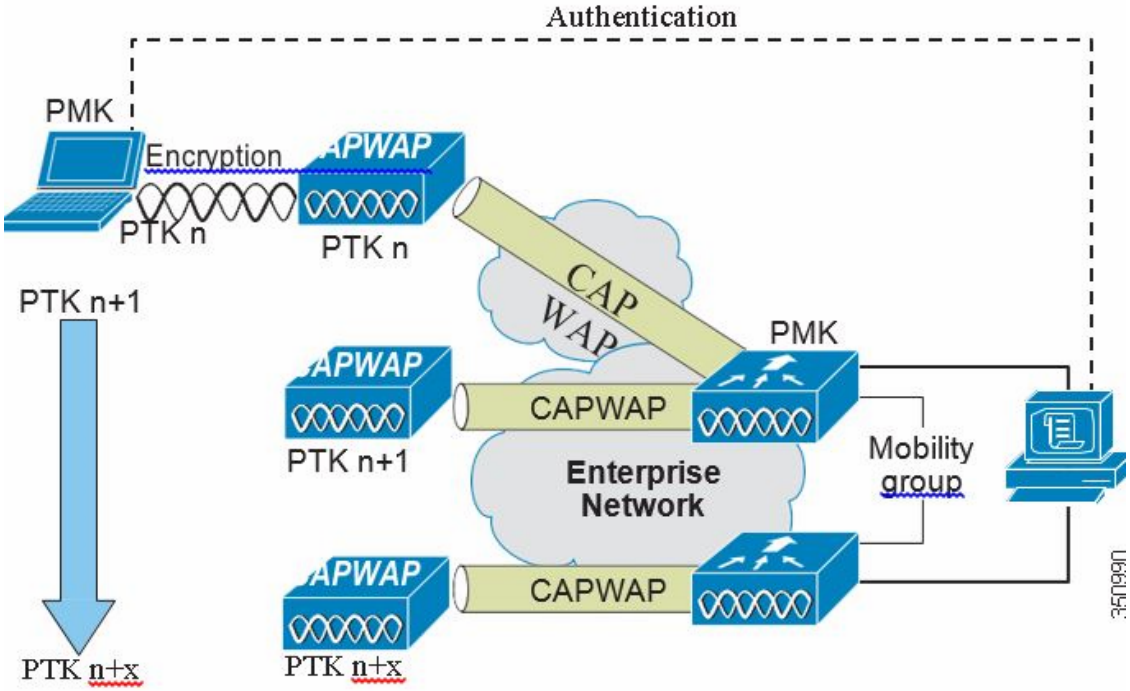


Proactive Key Caching（PKC）と CCKM

Proactive Key Caching（PKC）は、AP クライアント 802.1x/EAP 認証中に生成される PMK に対して予防的なキャッシング（クライアント ローミング イベントの前）を許可する 802.11i 拡張機能です（図 4-8 を参照）。クライアントがローミングしようとしている AP で（所定の WLAN クライアントの）PMK があらかじめキャッシュされている場合、完全な 802.1x/EAP 認証は必要ではありません。代わりに、WLAN クライアントはシンプルに WPA 4 方向ハンドシェイク プロセスを使用し、AP との通信用に新しいセッション暗号キーを安全に派生させます。

これらのキャッシュされた PMK の AP への配信は、Cisco Unified Wireless Network の展開では大幅に簡略化されています。PMK は単純にコントローラにキャッシュされるため、接続するすべての AP で使用可能になります。PMK は、アンカー コントローラを含むモビリティ グループを構成する他のすべてのコントローラとも共有されます。

図 4-8　Proactive Key Caching のアーキテクチャ



Cisco Centralized Key Management（CCKM）は、高速セキュア ローミング（FSR）を提供する Cisco Compatible Extensions クライアントでサポートされるシスコの標準です。ローミング処理を促進するための基本的なメカニズムは PKC と同じで、PMK キャッシュを使用します。ただし、CCKM の実装が少々異なるため、2 つのメカニズムの間に互換性はありません。

各 WLAN クライアントのキーのキャッシュの状態は、**show pmk-cache all** コマンドで確認できます。このコマンドにより、キーをキャッシュしているクライアントと、使用されているキー キャッシング メカニズムを識別します。802.11r ワークグループは、802.11 向けの FSR メカニズムの標準化を担当します。

WLC は次の例に示すように、WLAN -802.1x+CCKM の CCKM と PKC の両方をサポートします。

```
Security

   802.11 Authentication:..................... Open System
   FT Support................................. Disabled
   Static WEP Keys............................ Disabled

--More-- or (q)uit
   802.1X..................................... Disabled
   Wi-Fi Protected Access (WPA/WPA2)..........  Enabled
      WPA (SSN IE)............................ Enabled
         TKIP Cipher.......................... Disabled
         AES Cipher........................... Enabled
      WPA2 (RSN IE)........................... Enabled
         TKIP Cipher.......................... Disabled
         AES Cipher........................... Enabled
      Auth Key Management
         802.1x............................... Enabled
         PSK.................................. Disabled
         CCKM................................. Enabled
         FT-1X(802.11r)....................... Disabled
         FT-PSK(802.11r)...................... Disabled
         PMF-1X(802.11w)...................... Disabled
         PMF-PSK(802.11w)..................... Disabled
      FT Reassociation Timeout.....................20
      FT Over-The-DS mode.....................  Enabled
      GTK Randomization.......................  Disabled
      SKC Cache Support.......................  Disabled
      CCKM TSF Tolerance...................... 1000
```

Cisco Unified Wireless Network アーキテクチャ

図 4-9 では、CAPWAP AP、メッシュ CAPWAP、管理システム（WCS/NCS/PI）、およびワイヤレス LAN コントローラ（WLC）を含む Cisco Unified Wireless Network アーキテクチャの高レベルのトポロジを示します。

Cisco Access Control Server（ACS）または Identity Services Engine（ISE）および AAA 機能は、ソリューションを実現するため、無線ユーザの認証および許可をサポートする RADIUS サービスを提供します。

図 4-9　Cisco Unified Wireless Network アーキテクチャ

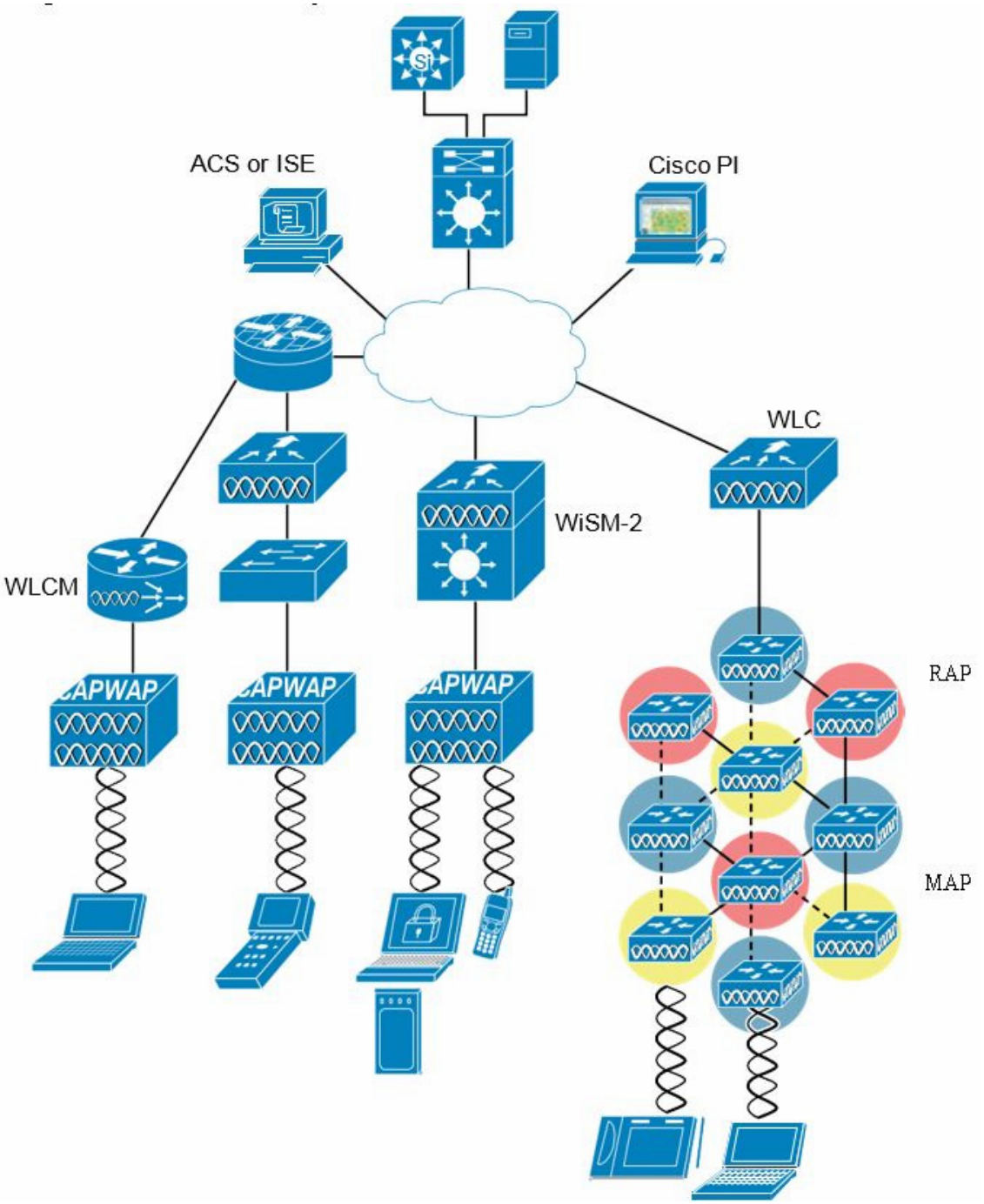
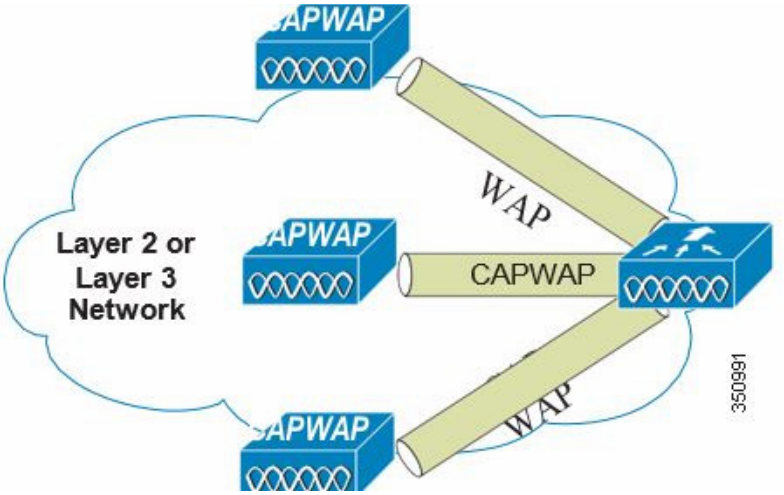


図 4-10 では、アーキテクチャの主要機能の 1 つである、AP がどのように CAPWAP プロトコルを使用して WLC へのトンネル トラフィックと通信するのかについて説明します。

図 4-10　　CAPWAP AP と WLC の接続



CAPWAP には次の 3 つの基本機能があります。

- AP の制御と管理
- WLC への WLAN クライアント トラフィックのトンネリング
- Cisco Unified Wireless IPv6 の管理に関する 802.11 データの収集

Cisco Unified Wireless Network のセキュリティ機能

ネイティブの 802.11 セキュリティ機能が、物理的なセキュリティや CAPWAP アーキテクチャの展開の容易さと組み合わさることで、WLAN の導入全体のセキュリティの向上に役立ちます。CAPWAP プロトコルに固有のセキュリティ上の利点に加えて、Cisco Unified Wireless Network ソリューションには次のようなセキュリティ機能もあります。

- 強化された WLAN セキュリティ オプション
- ACL およびファイアウォール機能
- Dynamic Host Configuration Protocol（DHCP）および Address Resolution Protocol（ARP）の保護
- ピアツーピア ブロック
- ワイヤレス侵入防御システム（wIPS）
  - クライアント除外
  - 不正 AP 検出
- 管理フレーム保護
- 動的 RF 管理
- アーキテクチャの統合
- IDS 統合

強化された WLAN セキュリティ オプション

Cisco Unified Wireless Network ソリューションでは、複数の WLAN セキュリティ オプションを同時にサポートします。たとえば、1 つの WLC 上に複数の WLAN を作成し、それぞれの WLAN に、オープンなゲスト WLAN ネットワークやレガシー プラットフォーム用の WEP のネットワークから WPA や WPA2 セキュリティ設定の組み合わせまで対応可能な独自の WLAN セキュリティを設定することができます。

それぞれの WLAN SSID は、WLC 上の同じ、または異なる dot1q インターフェイスにマッピングすることも、モビリティ アンカー（オート アンカー モビリティ）接続を介して別のコントローラにトンネリングされた Ethernet over IP（EoIP）にマッピングすることもできます。

WLAN クライアントが 802.1X を介して認証する場合、dot1q VLAN の割り当ては、認証成功時に WLC に渡される RADIUS 属性を使用して制御されます。

図 4-11、図 4-12、および図 4-13 では、Unified Wireless Network WLAN 設定画面のサブセットを示します。表示される主な設定項目は次の 4 つです。

- WLAN SSID
- WLAN がマッピングされている WLC インターフェイス
- レイヤ 2 セキュリティ方式（図 4-12）
- レイヤ 3 セキュリティ方式（図 4-13）

図 4-11　WLAN の [General] タブ

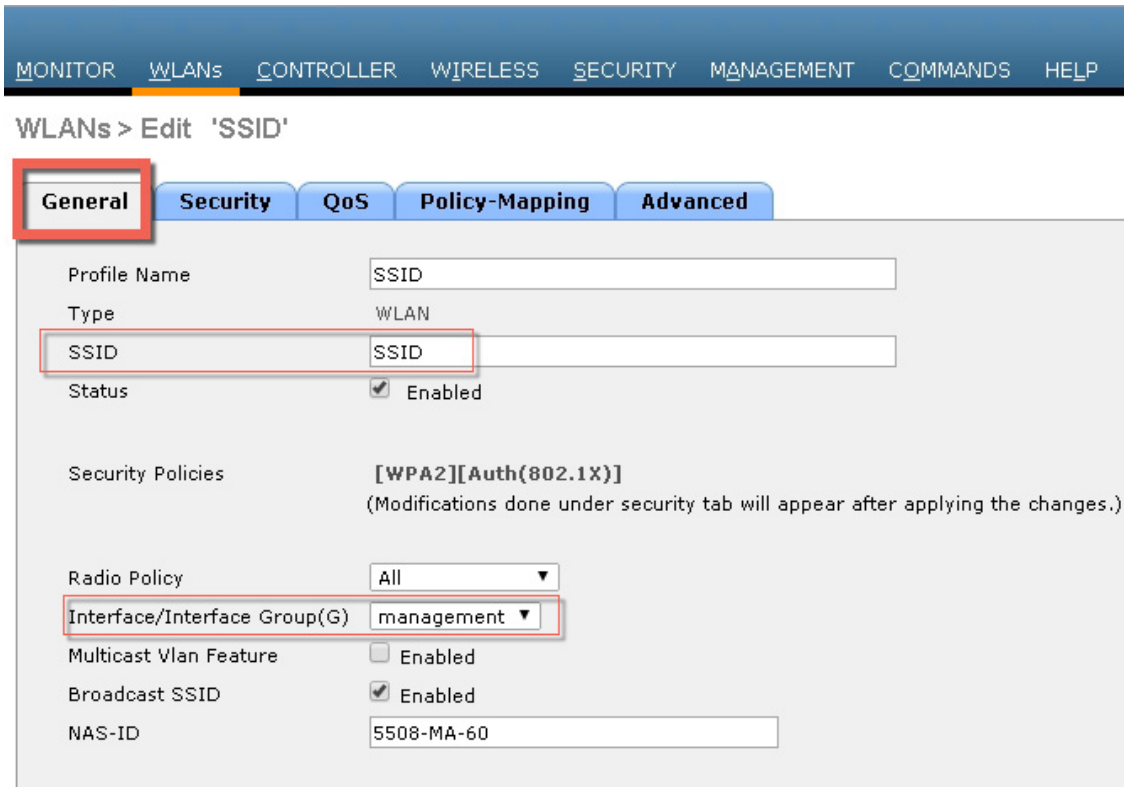


図 4-12　WLAN の [Layer 2 Security] タブ

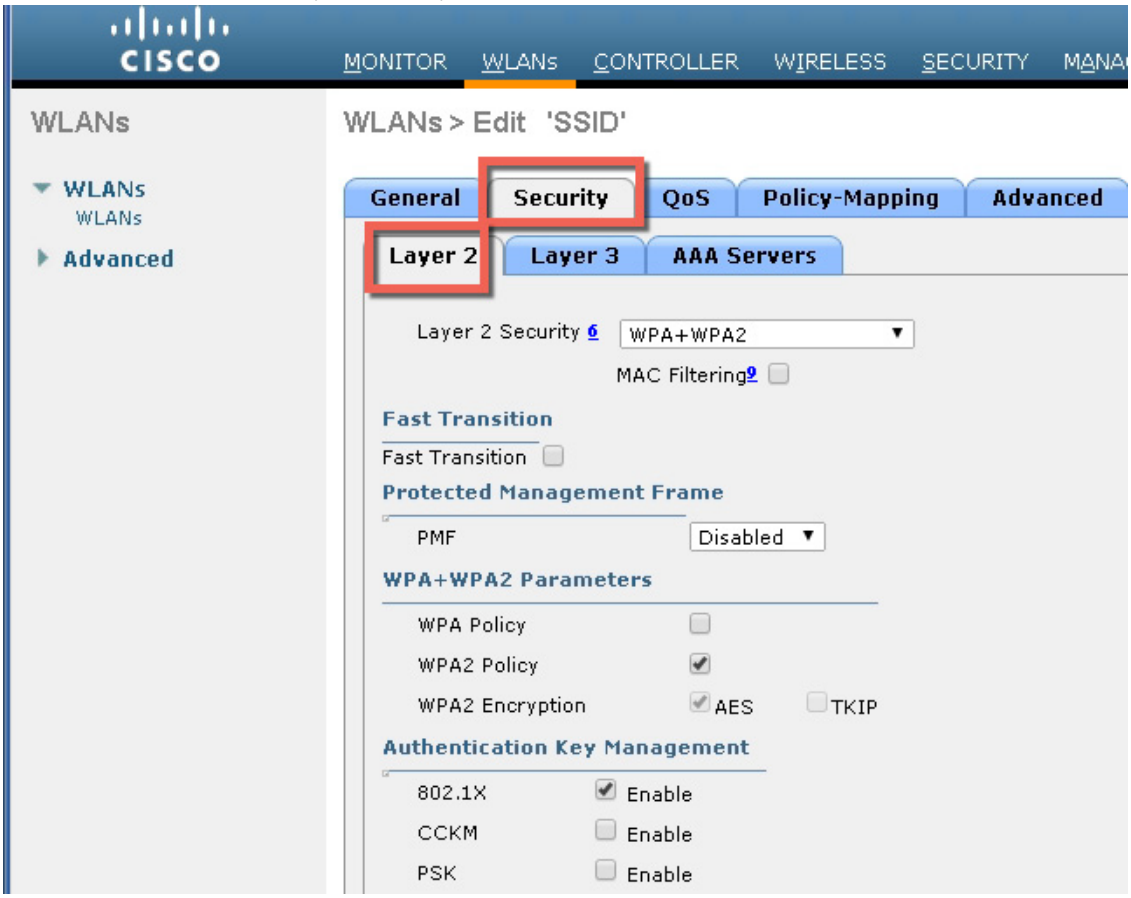
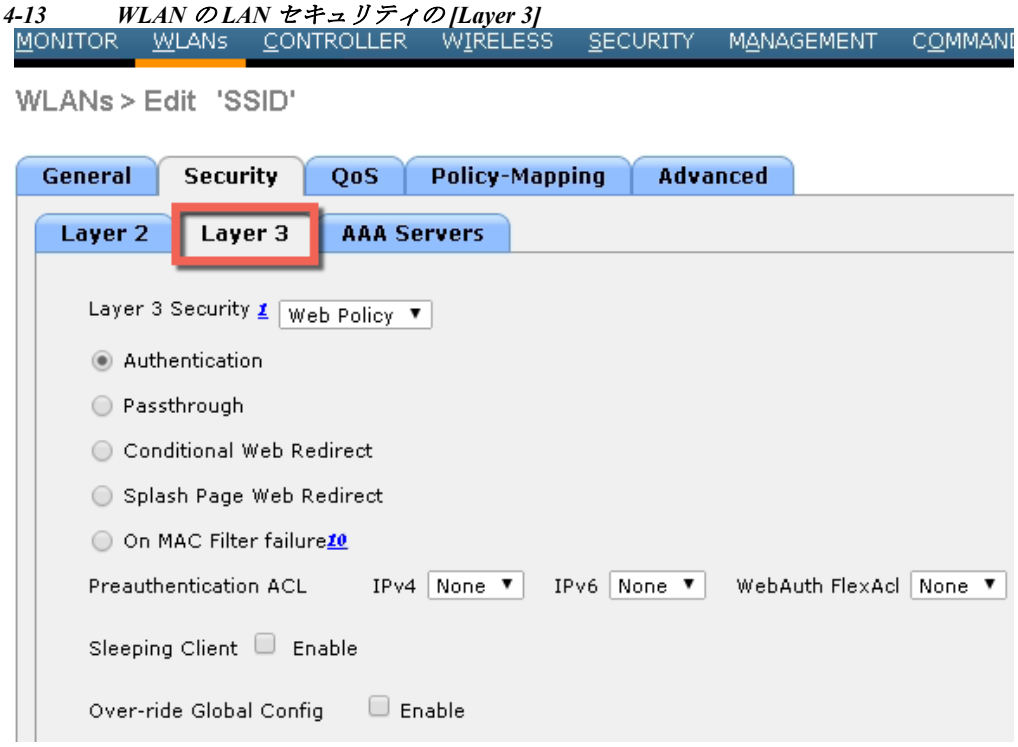


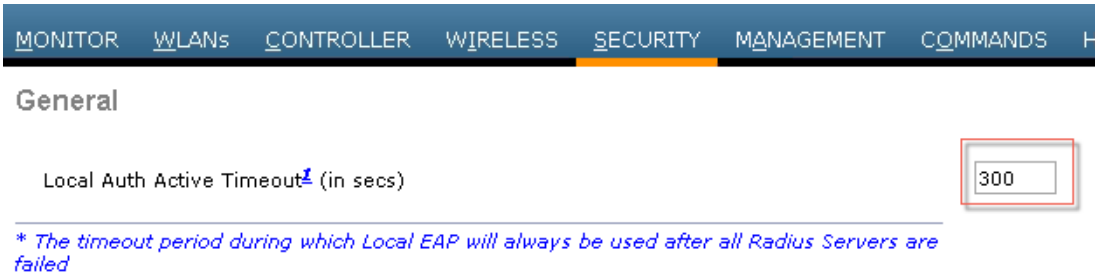
図 4-13　WLAN の LAN セキュリティの [Layer 3]



Local EAP Authentication

WLC ソフトウェアは、外部 RADIUS サーバが使用可能でない場合や使用不可になった場合に使用できる、ローカル EAP 認証機能を提供します。ローカル認証への切り替えが設定されるまでの遅延は、図 4-14 で示したとおりに設定します。RADIUS サーバの可用性が復旧されると、WLC は自動的にローカル認証から RADIUS サーバ認証へ再び切り替えます。

図 4-14　ローカル認証のタイムアウト



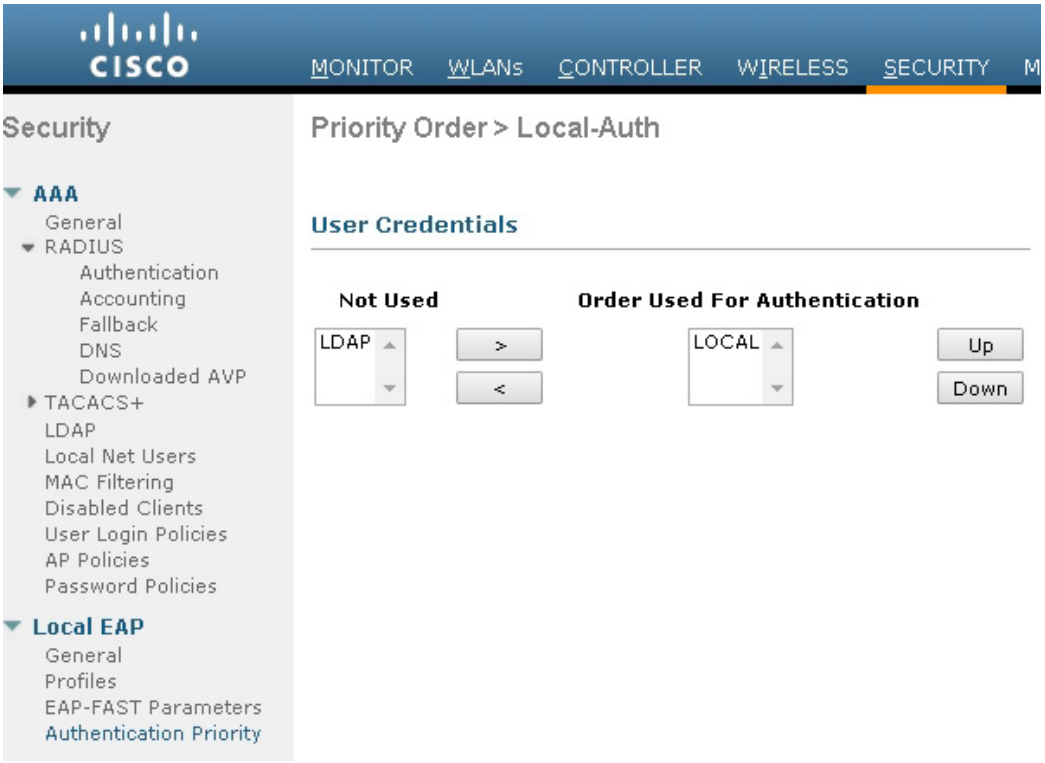
WLC 上でローカルでサポートされる EAP の種類は、LEAP、EAP-FAST、EAP-TLS および PEAP です。

図 4-15 では、ローカル EAP のプロファイルを選択できるウィンドウを示します。

図 4-15　ローカル EAP のプロファイル

WLC ではローカル データベースを使用してデータ認証を行うことができます。また、LDAP ディレクトリにアクセスして EAP-FAST または EAP-TLS 認証に関するデータを提供することもできます。ユーザ クレデンシャル データベースのプライオリティ（LDAP かローカルか）は、図 4-16 で示すとおりに設定可能です。

図 4-16　ローカル EAP のプライオリティ



ACL およびファイアウォール機能

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用 WLAN、あるいは CPU 宛てのすべてのトラフィックを制御するコントローラ CPU に適用できます。

または、Web 認証用に事前認証 ACL を作成することもできます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。

IPv4 ACL および IPv6 ACL のどちらもサポートされています。IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

- IPv4 および IPv6 の両方に最大 64 の ACL を定義し、各 ACL に最大 64 のルール（またはフィルタ）を適用できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。
- Cisco 5500 シリーズ コントローラ、Cisco 3504 シリーズ ワイヤレス コントローラ、および 8500 シリーズ ワイヤレス コントローラに CPU ACL を適用する場合は、Web 認証のために仮想 IP アドレスへのトラフィックを許可する必要があります。
- すべての ACL で、最後のルールとして暗黙の「deny all」ルールが適用されます。パケットがどのルールとも一致しない場合、コントローラによってドロップされます。
- Cisco 5500 シリーズ コントローラまたはコントローラ ネットワーク モジュールとともに外部の Web サーバを使用している場合は、WLAN 上で外部 Web サーバに対する事前認証 ACL を設定する必要があります。
- インターフェイスまたは WLAN に ACL を適用すると、1 Gbps ファイル サーバからのダウンロードの際にワイヤレス スループットが低下します。スループットを改善するには、インターフェイスまたは WLAN から ACL を削除するか、ポリシー レート制限制約機能を持つ隣接有線デバイスに ACL を移動するか、1 Gbps ではなく 100 Mbps を使用してファイル サーバを接続します。
- 有線ネットワークから受信した無線クライアントに向かうマルチキャスト トラフィックは WLC ACL では処理されません。ワイヤレス クライアントから送信された有線ネットワークまたは同じコントローラ上の他のワイヤレス クライアント宛のマルチキャスト トラフィックは、WLC ACL によって処理されます。
- ACL はコントローラ上で直接設定されるか、テンプレート経由で設定されます。ACL 名は固有の名前でなければなりません。
- クライアント（AAA によって上書きされる ACL）ごと、もしくはインターフェイスまたは WLAN で ACL を設定できます。AAA によって上書きされる ACL の優先度が最も高くなります。ただし、適用する各インターフェイス、WLAN、またはクライアントごとの ACL の設定は、お互いを上書きできます。
- ピアツーピア ブロッキングが有効になると、トラフィックは ACL で許可されてもピア間でブロックされます。
- 認証トラフィックは、DNS ベースの ACL が AP に対してローカルであっても、この機能がサポートされるように Cisco WLC を経由する必要があります。
- ACL を作成する場合は、CLI または GUI から 2 つのアクション（ACL または ACL ルールの作成と、ACL または ACL ルールの適用）を連続して行うことが推奨されます。

図 4-17 では、[ACL Configuration] ページを示します。ACL では、発信元アドレスと送信先アドレスの範囲、プロトコル、送信元ポートと宛先ポート、DSCP、および ACL が適用される方向を指定できます。ACL は、さまざまな規則の順序で作成できます。

図 4-17　[ACL Configuration] ページ

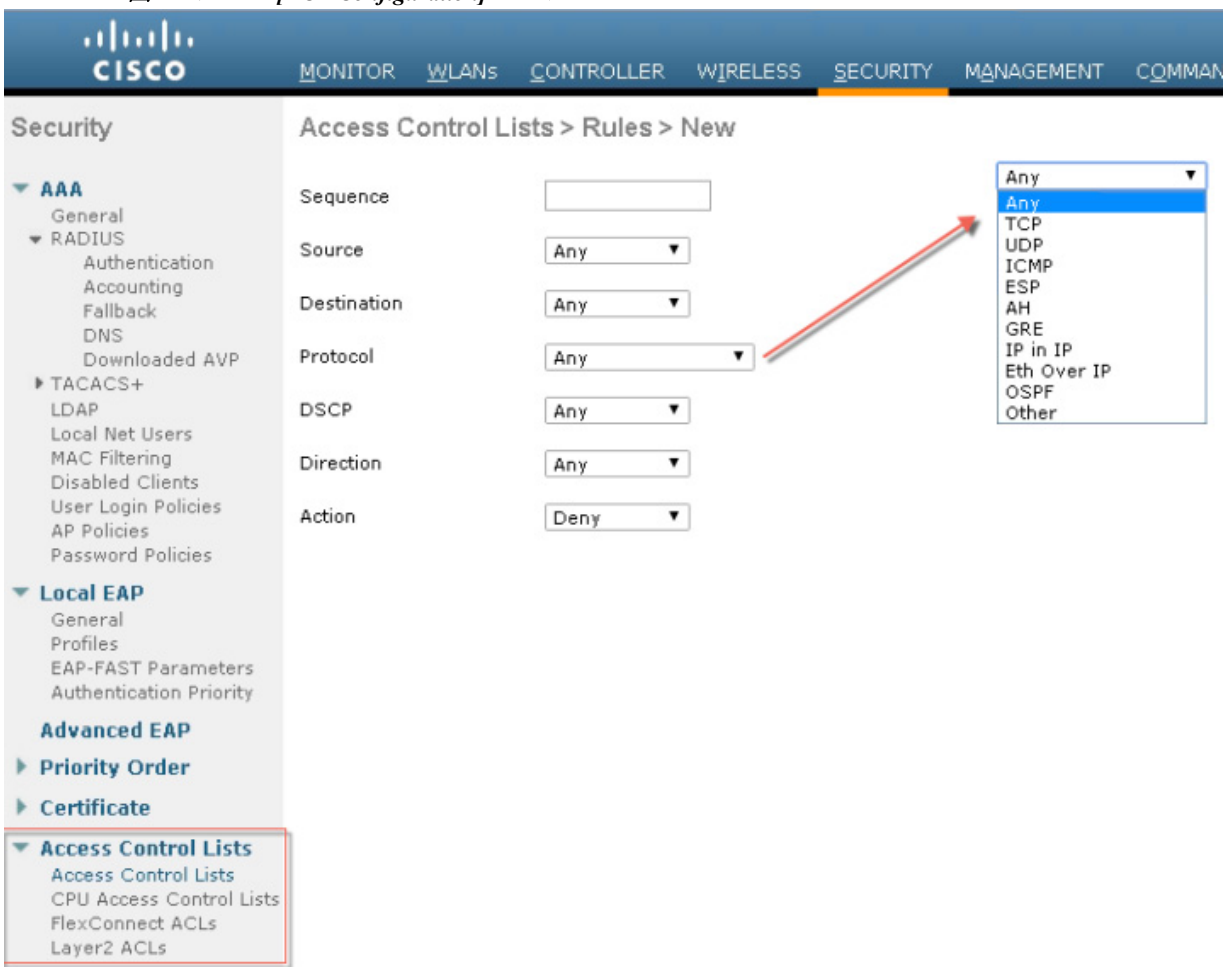
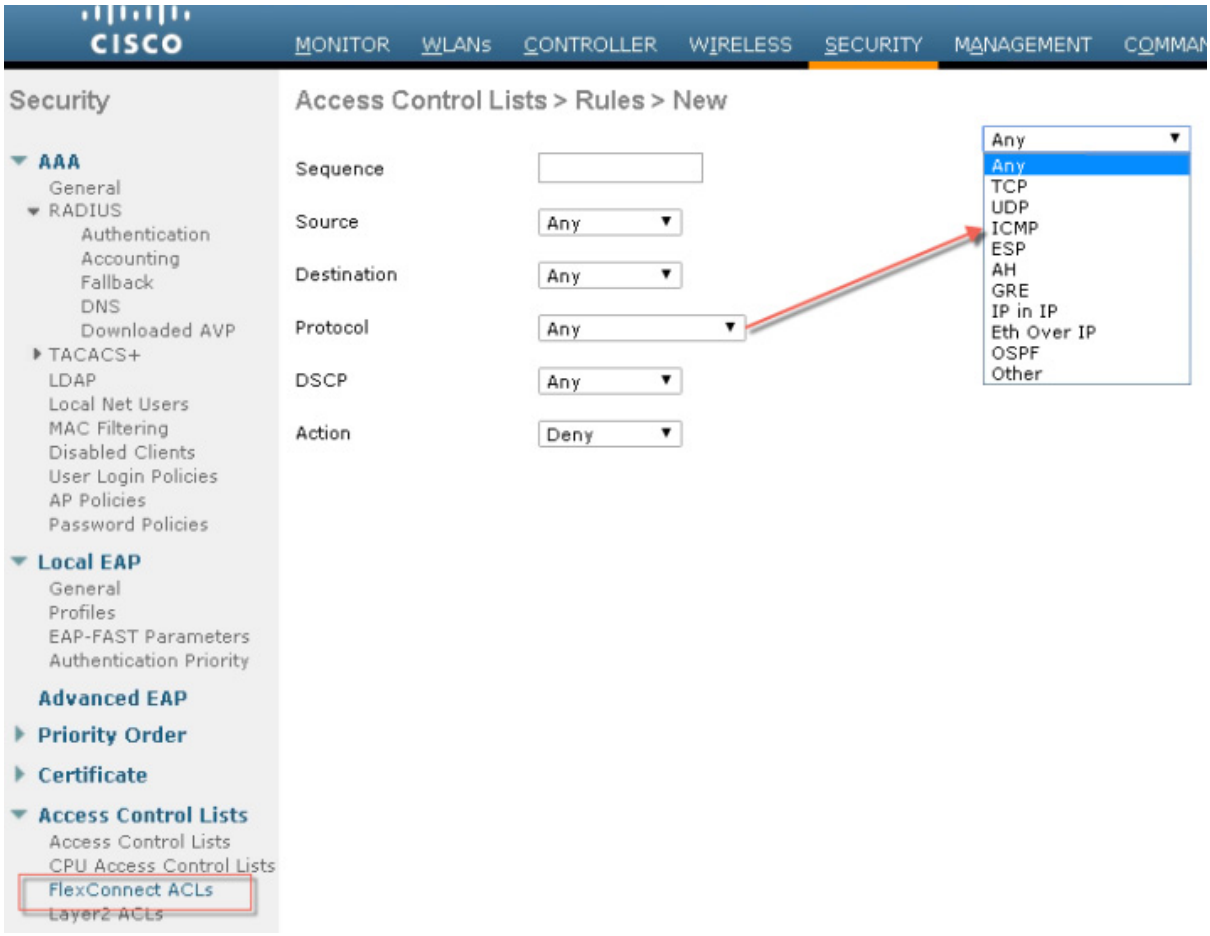


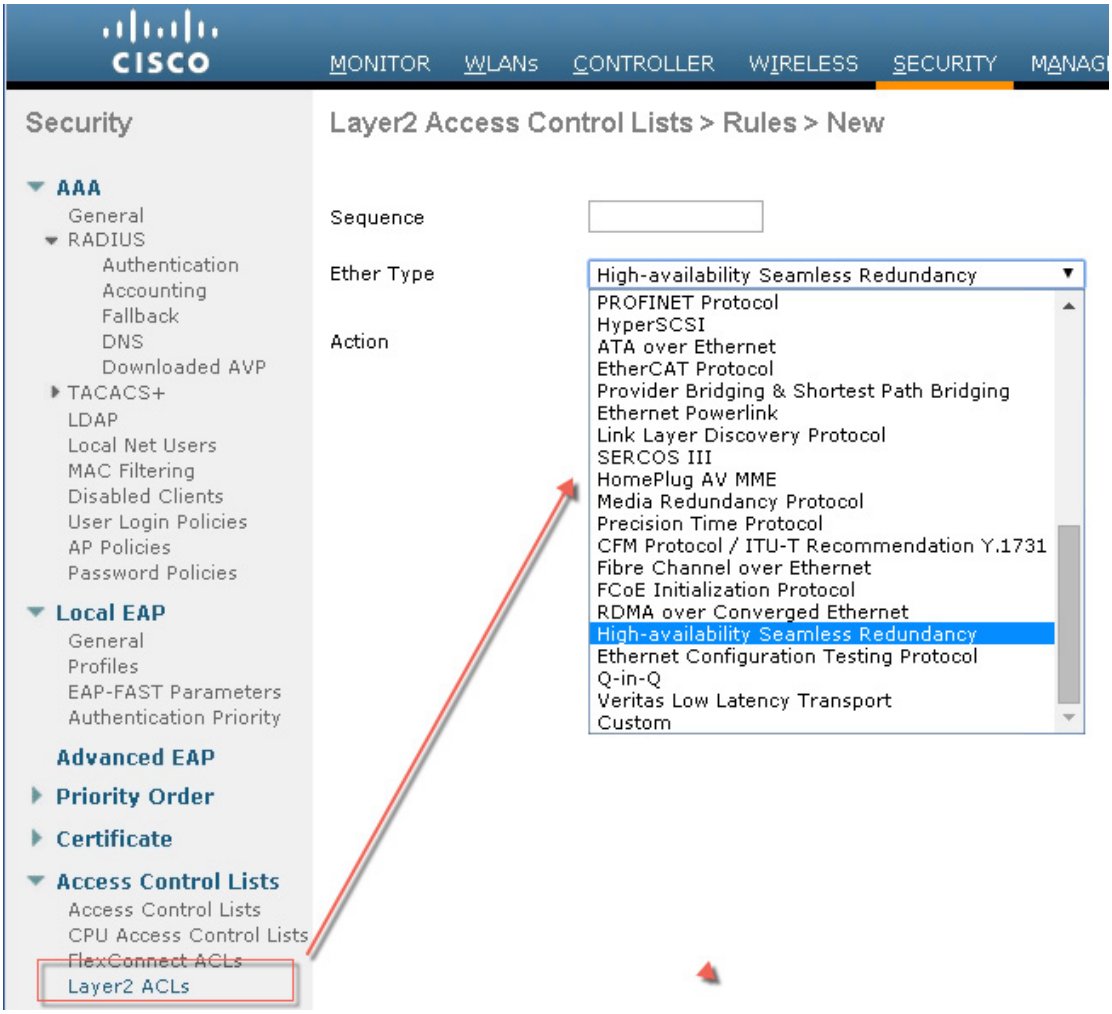
図 4-18　[Flex Connect ACL] の図



レイヤ 2 アクセス コントロール リスト

パケットに関連付けられた EtherType に基づいてレイヤ 2 アクセス コントロール リスト（ACL）のルールを設定できます。中央スイッチングの WLAN に PPPoE クライアントのみをサポートさせる必要がある場合は、この機能を使用してレイヤ 2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから PPPoE パケットのみを許可することができます。同様に、WLAN に IPv4 クライアントまたは IPv6 クライアントのみをサポートさせる必要がある場合は、レイヤ 2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから IPv4 または IPv6 パケットのみを許可することができます。ローカルにスイッチされる WLAN の場合、WLAN または FlexConnect AP のいずれかに同じレイヤ 2 ACL を適用できます。AP 固有のレイヤ 2 ACL は FlexConnect AP にのみ設定できます。これは、ローカルにスイッチされる WLAN にのみ適用されます。FlexConnect AP に適用されるレイヤ 2 ACL は WLAN に適用されるレイヤ 2 ACL よりも優先されます。

図 4-19　　WLC での設定に使用できるレイヤ 2 ACL の図



DNS ベースのアクセス コントロール リスト

DNS ベースの ACL は、Apple および Android デバイスなどのクライアント デバイスに使用されます。これらのデバイスを使用する場合、デバイスがアクセス権を持つ範囲を特定するために Cisco WLC に事前認証 ACL を設定できます。

Cisco WLC で DNS ベースの ACL を有効にするには、ACL の許可された URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。

Cisco WLC は ACL 名で設定され、事前認証 ACL が適用されるように AAA サーバによって返されます。ACL 名が AAA サーバによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

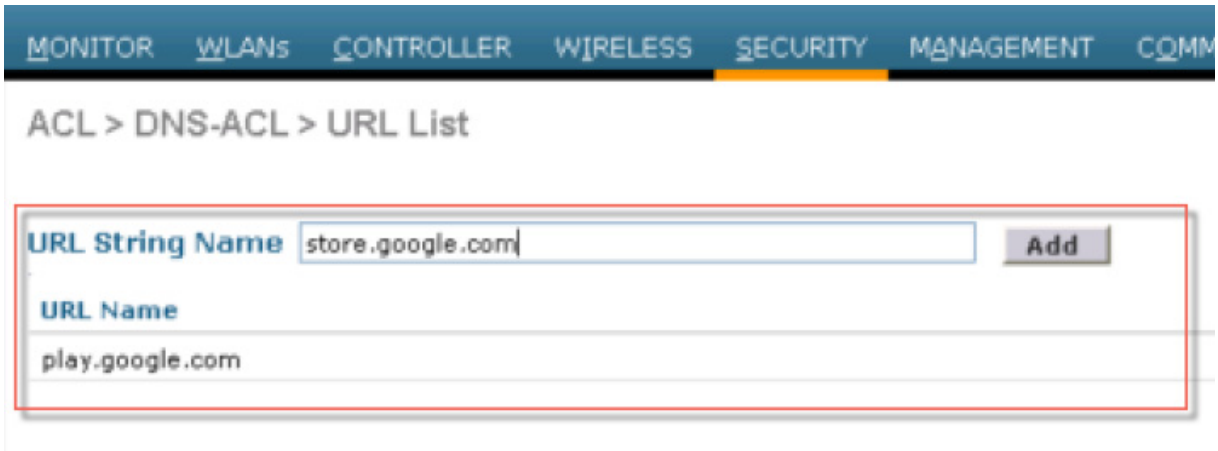
クライアント認証フェーズでは、ISE サーバが事前認証 ACL（url-redirect acl）を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL が Cisco WLC で受信されると、CAPWAP ペイロードは AP に送信され、クライアントの DNS スヌーピングが有効になり URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。ドメイン名が設定された URL に一致すると、DNS 応答が IP アドレスについて解析され、IP アドレスは CAPWAP ペイロードとして Cisco WLC に送信されます。Cisco WLC によって IP アドレスの許可リストに IP アドレスが追加されるため、クライアントは設定された URL にアクセスできます。

DNS ベースのアクセス コントロール リストでの制限

- 最大 10 の URL をアクセス コントロール リストに許可できます。
- Cisco WLC では、1 つのクライアントに対して 20 の IP アドレスが許可されています。
- ローカル認証は FlexConnect AP でサポートされていません。
- DNS ベースの ACL は、ローカル スイッチングを使用した FlexConnect AP ではサポートされません。
- DNS ベースの ACL は、Cisco 1130 および 1240 シリーズのアクセス ポイントでサポートされていません。
- 認証トラフィックは、DNS ベースの ACL が AP に対してローカルであっても、この機能がサポートされるように Cisco WLC を経由する必要があります。
- クライアントがアンカーされている場合は、それが自動アンカーであろうとローミング後のアンカーであろうと、DNS ベースの ACL は機能しません。
- DNS ベースの ACL は、SSID 上で RADIUS NAC（中央 Web 認証またはポスチャ）が実行される場合にのみ動作します。DNS ベースの ACL は、ローカル Web 認証や、RADIUS NAC の場合に使用されるリダイレクト ACL 以外の形式の ACL とは併用できません。

図 4-20　WLC で設定可能な DNS ベースの ACL の図



URL フィルタリングまたは ACL

URL フィルタリングは、リリース 8.3 で導入され、リリース 8.4 で機能が強化されました。URL フィルタリング機能により、Web サイトへのアクセスを制限することでネットワーク帯域幅の使用が最適化されます。この機能では、DNS スヌーピングを使用して、DNS サーバからワイヤレス クライアントに送信される DNS 応答をスヌープします。URL フィルタリングは、HTTP や HTTPS を含むすべてのプロトコルについて URL を制限する ACL ベースの実装です。URL フィルタリングの ACL は、すべての URL に対して、許可/拒否アクションに関連付けられる一連の URL として定義されます。ACL タイプは、ホワイトリストまたはブラックリストのどちらかとなります。ホワイトリスト ルールとブラックリスト ルールの混在はサポートされていません。アクセス URL が設定でブロックされた場合にブロックされたページをクライアントにリダイレクトするために使用される外部サーバの IP アドレスが設定されます。

WLC はクライアントへの DNS 応答をスヌープし、URL が設定（ACL ルール）で許可される場合は、DNS 応答がクライアントに送信されます。URL が設定（ACL ルール）によって許可されていない場合、解決済み IP は外部サーバの IP（後ほど設定します）で上書きされてクライアントに返されます。この外部サーバはブロックページをクライアントにリダイレクトします。DNS 応答が ACL にヒットしたときに、ある特定の ACL で許可された DNS 応答と拒否された DNS 応答を計数するカウンタが表示されます。

URL フィルタリングの設定

URL フィルタリングは、ローカル ポリシーによって WLAN、インターフェイス、または個々のクライアント セッションに割り当てられている ACL およびルールを使用して、許可または拒否する URL を決定します。次の手順では、2 つの一般的なシナリオに基づいて、URL に基づく ACL ルールを作成する方法を示します。

- シナリオ 1:特定の URL へのアクセスを拒否するためのルールが定義されているリスト タイプ「Blacklist」を使用した ACL。これは、一般的に「ブラックリスト」と呼ばれます。
- シナリオ 2:特定の URL へのアクセスのみを許可するためのルールが定義されているリスト タイプ「Whiitelist」を使用した ACL。これは一般的にホワイトリスト化と呼ばれます。

アクセス コントロール リストの適用

URL ACL は、ローカル ポリシーを使用して動的にクライアントに割り当てることも、WLAN やインターフェイスに直接割り当てることもできます。

- ローカル ポリシー - URL ACL は、ローカル ポリシーが割り当てられているすべてのクライアントに適用されます。ローカル ポリシーを使用して割り当てられた URL ACL は優先順位が最も高く、WLAN やインターフェイスに割り当てられている URL ACL をオーバーライドします。
- WLAN - URL ACL は、対象の WLAN に関連付けられたすべてのクライアントに適用されます（クライアントにローカル ポリシー経由で URL ACL が割り当てられている場合を除く）。WLAN に割り当てられた URL ACL は、インターフェイスに割り当てられた URL ACL をオーバーライドします。
- インターフェイス:URL ACL は、特定のインターフェイスに転送されるすべてのトラフィックに適用されます。

プラットフォームのサポート

1. この機能は、3504（リリース 8.5 以降）、5520、および 8540 でサポートされます。5508、8510、vWLC、2504、および ME ではサポートされません。
2. ローカル モードと [Flex central switching] でのみサポートされます。

考慮事項

1. ワイルドカード サポート（「*.domain.com」など）
2. 最大 10 件
3. ワイルドカード 1 つ当たりサブドメイン 5 つ
4. URL フィルタリングには次のものが含まれます。
    1. URL 100 件のサポート

a. サブ URL（www.domain.com と www.domain.com/resources など）はサポート対象外

2. URL は最大 32 文字までサポート
3. この機能は AVC に依存しません。DNS スヌーピングのみに基づいて動作します
4. URL フィルタリング ACL 名を返す RADIUS サーバはサポートされていません
5. リバース DNS はサポートされていません。ダイレクト IP による（DNS を介さない）クライアント アクセスは許可されません
6. IPv6 はサポートされません。

設定手順

1. ACL をホワイトリストまたはブラックリストとして設定し、ドメインへのアクセスを許可または拒否する
2. 外部サーバの IP アドレスを設定する
3. 作成した URL ACL を次のいずれかに関連付ける

a. インターフェイス

b. WLAN

c. ローカル ポリシー（最優先）

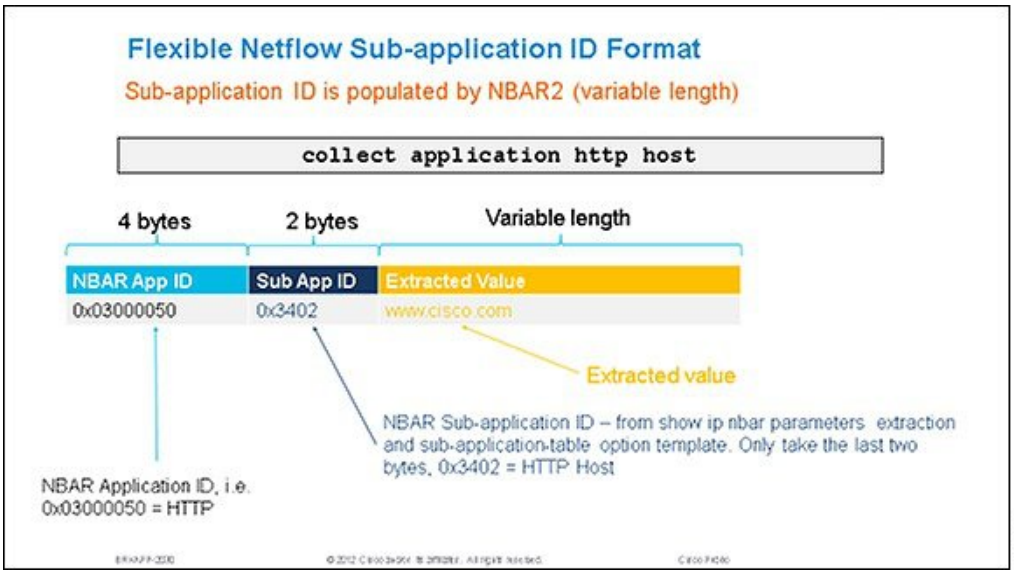
4. これで、すべてのプロトコルについて閲覧が特定のドメインに制限されます。

URL フィルタリングと ACL の設定に関する詳細については、次の URL にある導入ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_URL_ACL_Enhanced_Deployment_Guide.html

ドメイン フィルタリング

ドメイン フィルタリングは、8.3 リリースの一部として導入されている新しい拡張機能です。この拡張機能は、WLC で現在利用可能な Application Visibility Control（AVC）フィルタリングを補完します。AVC フィルタリングでは、特定の AirOS リリースのプロトコル パックで定義されているプロトコルとアプリケーションのみがサポートされ、特定のアプリケーションをドロップ、マーク、またはレート制限できます。ドメイン フィルタリングは、AVC をベースに構築されており、NBAR2 エンジンを使用してアプリケーション タイプ（HTTP など）とホスト（www.cisco.com など）の両方に一致するアプリケーション レイヤを詳細に調べます。8.3 リリースでは、管理者は、WLAN、インターフェイス、またはローカルに適用できる ACL とルールを定義できます。



ドメイン フィルタリングは、フィールド抽出を使用する NBAR2 エンジンフィルタリング機能に基づいています。最新の NBAR2 エンジンでは、120 個のカスタム アプリケーションがサポートされます。URL は、カスタム アプリケーションとして定義し、エンジンによって分類できます。

1. URL は、WLC で定義されている ACL を使用して分類されます。各 ACL には、一致する URL を決定するルールが定義されます。
2. NBAR2 エンジンは、渡されるパケットから URL フィールド（存在する場合）を抽出するように設定されます。フィールド抽出は、パフォーマンスを最適化するためにフローごとに実行されます。
3. WLC は、URL を抽出できるように NBAR2 エンジンに HTTP パケットを 渡します。ホスト名（www.cisco.com など）が存在する場合、NBAR2 エンジンは WLC にホスト名を URL として返します。
4. WLC は、抽出された URL をフィルタリングするロジックを実装しており、適切な転送アクション（フローの許可または拒否）を実行します。

- このリリースでは、最大で 100 個の URL ACL がサポートされます。
  - 各 ACL では、最大で 64 個のルールがサポートされます。
  - 各ルールには、許可アクションまたは拒否アクションのいずれかが設定されます。各 URL ACL には、トラフィックを許可する許可ルールが少なくとも 1 つ定義されている必要があります。

  - 各 ACL には、最後のルールとして暗黙の「deny all」ルールが設定されます。URL がどのルールとも一致しない場合、WLC によってドロップされます。
  - 各ルールは、優先順位に従って（低いものから高いものへ）検査されます。ACL 内の最初に一致したルールがフローに適用されます。
  - 各ルールでは、最大 32 文字がサポートされます。
  - 各ルールは、一致させたい正確なサブドメイン、ドメイン、およびトップ レベル ドメイン（www.cisco.com、tools.cisco.com、または partners.cisco.com）に一致する必要があります。
  - このリリースでは、ワイルドカードまたは正規表現を使用した部分一致（www.c*.com や *.cisco.com など）はサポートされません。
  - このリリースでは、フォルダ、ファイル名、または拡張子（www.cisco.com/resources/index.html など）はサポートされません。www.cisco.com に一致するルールは、www.cisco.com/c/en/us/support.index.html や http://www.cisco.com/c/en/us/buy.html にも適用されます。
  - ACL ごとに、許可または拒否アクションを含むワイルドカード（*）ルールが 1 つサポートされます。ワイルドカードはすべての URL に一致します。
- このリリースでは、一致した URL に対応する AVC プロファイルはサポートされません。URL ACL とルールは個別に定義され、WLAN、インターフェイス、またはローカル ポリシーに適用されます。
- このリリースでは、IPv6 はサポートされません（IPv4 のみサポートされます）。
- このリリースでは、PI はサポートされません。

(注)　リリース 8.4 では、HTTP URL のみがサポートされます。HTTPS URL のサポートは、将来のリリースで導入される予定です。

ドメイン フィルタリングの設定手順

ドメイン フィルタリングは、WLC でデフォルトによりグローバルに無効になっており、NBAR2 エンジンで HTTP ベースの URL を検査してフィルタリングする前に有効にする必要があります。

ドメイン フィルタリングでは、WLAN、インターフェイス、または個々のクライアントにローカル ポリシー経由で割り当てられた ACL を使用して、許可または拒否する HTTP ベースの URL を判断します。以下の手順では、2 つの一般的なシナリオについて、URL ベースの ACL とルールを作成する方法を示します。

- シナリオ 1:特定の HTTP URL へのアクセスを拒否する ACL とルールを定義する。これは一般的にブラックリスト化と呼ばれます。
- シナリオ 2:特定の HTTP URL へのアクセスのみを許可する ACL とルールを定義する。これは一般的にホワイトリスト化と呼ばれます。

URL ACL は、ローカル ポリシーを使用してクライアントに動的に割り当てるか、WLAN またはインターフェイスに直接割り当てることができます。

  - ローカル ポリシー - URL ACL は、ローカル ポリシーが割り当てられているすべてのクライアントに適用されます。ローカル ポリシーを使用して割り当てられた URL ACL は優先順位が最も高く、割り当てられている URL ACL をオーバーライドします。

- WLAN - URL ACL は、対象の WLAN に関連付けられたすべてのクライアントに適用されます（クライアントにローカル ポリシー経由で URL ACL が割り当てられている場合を除く）。WLAN に割り当てられた URL ACL は、
- WLC の URL ACL を WLAN、インターフェイス、ローカル ポリシーに割り当てる手順をオーバーライドします。

完全な展開シナリオと設定手順については、次のリンクにあるドメイン フィルタリング導入ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_domain_filtering.html

Umbrella（正式名称：Open DNS）フィルタリング

リリース 8.4 で導入された Cisco Umbrella は、マルウェアや侵害からデバイスをリアルタイムで保護するためのインサイトを提供する、クラウド提供型のネットワーク セキュリティ サービスです。進化を続けるビッグデータ手法やデータ マイニング手法を活用し、攻撃をプロアクティブに予測するとともに、カテゴリ ベースのフィルタリングも行います。

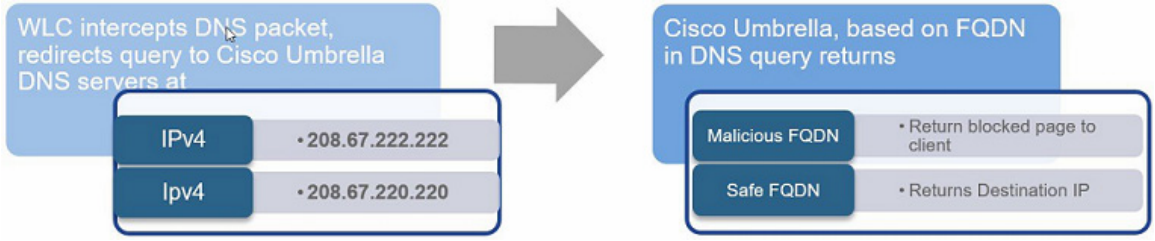
この機能の動作に関連する用語は次のとおりです。

API トークン：Cisco Umbrella Portal から発行され、デバイス登録にのみ使用されます。

デバイス ID：固有デバイス識別子です。ポリシーは ID ごとに適用されます。

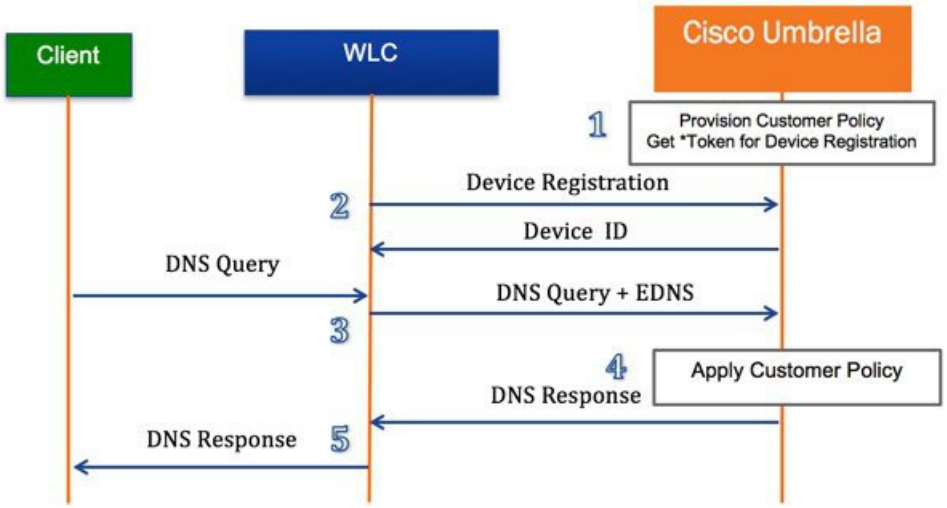
EDNS は、タグ付けされた DNS パケットを伝送する DNS の拡張機能です。

FQDN は完全修飾ドメイン名です。

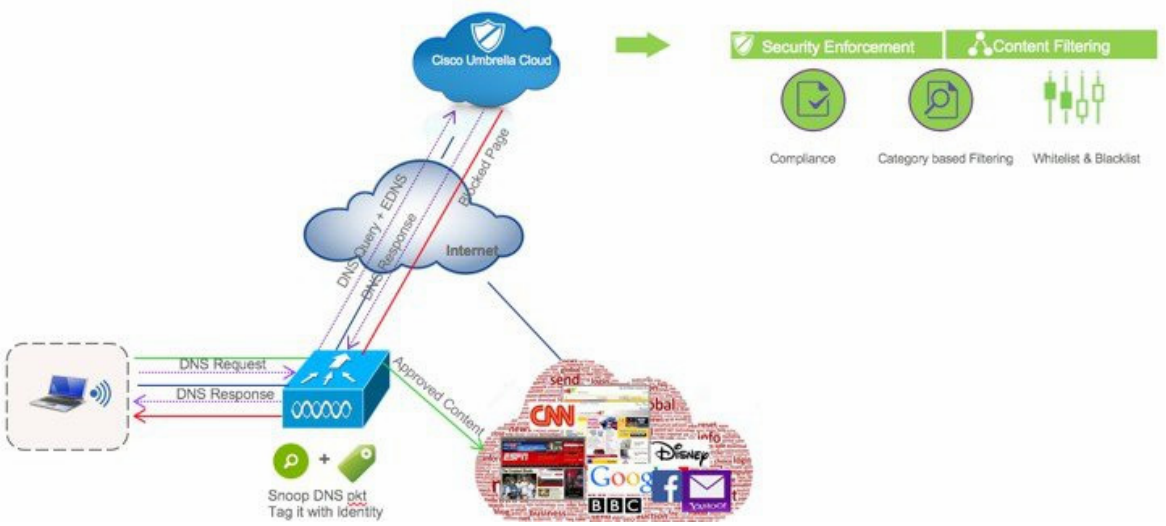


DNS 要求は常に Web 要求に先行します。ワイヤレス LAN コントローラは、クライアントからの DNS 要求を傍受し、クラウド（208.67.222.222、208.67.220.220）の Cisco Umbrella にクエリをリダイレクトします。Cisco Umbrella サーバは DNS クエリを実行し、ID ごとに事前設定済みのセキュリティ フィルタリング ルールを適用してドメインを悪意のあるドメイン（ブロックされたページがクライアントに返されます）または安全なドメイン（解決された IP アドレスがクライアントに返されます）としてマークします。

Cisco Umbrella の全般的なワークフロー



1. WLC の Cisco Umbrella サーバへの登録は 1 回限りのプロセスで、セキュアな HTTPS トンネルを介して行われます。
2. Cisco Umbrella ダッシュボードからデバイス（WLC）登録用の API トークンを取得します。
3. ワイヤレス LAN コントローラ上でトークンを適用します。これにより、デバイスが Cisco Umbrella アカウントに登録されます。次に、WLC に Cisco Umbrella プロファイルを作成します。プロファイルは ID として Cisco Umbrella に自動的にプッシュされ、ポリシーは ID ごとに適用されます。
4. ワイヤレス クライアントから Cisco Umbrella サーバにトラフィックが流れます。
5. ワイヤレス クライアントが WLC に DNS 要求を送信します。
6. WLC が DNS パケットをスヌープし、DNS パケットに Cisco Umbrella プロファイルのタグを付けます。プロファイルは、Cisco Umbrella にもあるパケットの ID です。
7. この EDNS パケットは、名前解決のために Cisco Umbrella サーバにリダイレクトされます。
8. Cisco Umbrella は、ID に応じてこの EDNS パケットにポリシーを適用し、組織のコンプライアンスを確保するためにカテゴリ ベースのフィルタリング ルールを提供します。
9. ルールに応じて、クエリされた DNS 要求に対する応答としてブロックされたページまたは解決された IP アドレスをクライアントに返します。



OpenDNS のサポート

- サポートされる WLC プラットフォームは、3504（リリース 8.5 以降）、5508、5520、7500、8510、および 8540 です。
- ME、2500、および vWLC はサポートされません
- サポートされる AP モードは、ローカル モードとフレックス セントラル スイッチングです。
- WLC で 10 個の OpenDNS プロファイルを設定可能
- ゲスト（外部 - アンカー）シナリオでは、プロファイルはアンカー WLC で適用されます。

OpenDNS の制限事項

- Web プロキシ経由のクライアントは、サーバ アドレスを解決するために DNS クエリを送信しません。
- アプリケーションまたはホストは、DNS にドメインを問い合わせる代わりに IP アドレスを直接使用します。

Cisco Umbrella ワイヤレス LAN コントローラの統合の設定

ステップ 1　Cisco Umbrella のプロビジョニングでは、Cisco Umbrella クラウドにユーザ アカウントを作成します。

サブスクリプションはアカウントごとで、Cisco Umbrella には 14 日間の無料トライアル ライセンスが付属しています。

永久ライセンスは、CiscoOne Advanced Subscription に含まれています。

ステップ 2　次に、ワイヤレス コントローラで GUI または CLI を使用して Cisco Umbrella を有効にします。

ステップ 3　WLC がセキュアな HTTPS トンネルを介してクラウド アカウントに登録します。

ステップ 4　WLC でプロファイル（ID）を設定します。プロファイルは、WLAN AP グループにマッピングするか、ローカル ポリシーに組み込むことができます。

ステップ 5　WLC が Cisco Umbrella クラウドに DNS パケットをリダイレクトします。

ステップ 6　Cisco Umbrella のセキュリティ ポリシーは ID ごとに適用されます。

ワイヤレス コントローラでの Cisco Umbrella の設定手順では、Cisco Umbrella の有効化、API トークンの設定、プロファイルの作成と WLAN、AP グループ、またはローカル ポリシーへのマッピングを行います。

ポリシーの優先順位は高いものから順に次のとおりです。

a. ローカル ポリシー
b. AP Group
c. WLAN

Cisco Umbrella プロファイルをローカル ポリシーにマッピングすると、属性（ユーザ ロール、デバイス タイプなど）の動的な評価に基づいてきめ細かい差別化されたユーザ ブラウジング エクスペリエンスを提供できます。

完全な展開シナリオと設定手順については、次のリンクにある『Umbrella Integration Guide』を参照してください。
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_cisco_umbrella_wlan_integration_guide.html

DHCP および ARP 保護

WLC は、WLAN クライアントの DHCP 要求のリレー エージェントとして動作します。その際、WLC は DHCP インフラストラクチャを保護するために、いくつかのチェックを実行します。最も重要なチェックは、DHCP 要求に含まれている MAC アドレスが、要求を送信する WLAN クライアントの MAC アドレスに一致することを確認することです。これにより、WLC 自体のインターフェイスに対する 1 つの DHCP 要求（IP アドレス）に WLAN クライアントを制限し、それによって DHCP 枯渇攻撃を防御します。WLC は、デフォルトでは WLAN クライアントからのブロードキャスト メッセージを WLAN に再転送しないため、WLAN クライアントが DHCP サーバとして動作したり、誤った DHCP 情報をスプーフィングしたりすることが防止されます。

WLC は MAC アドレスと IP アドレスの関係を維持することで、WLAN クライアントの ARP プロキシとして機能します。これにより、重複した IP アドレスおよび ARP スプーフィング攻撃を WLC がブロックできるようになります。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。これにより、WLAN クライアント デバイス宛ての ARP スプーフィング攻撃も防止できます。

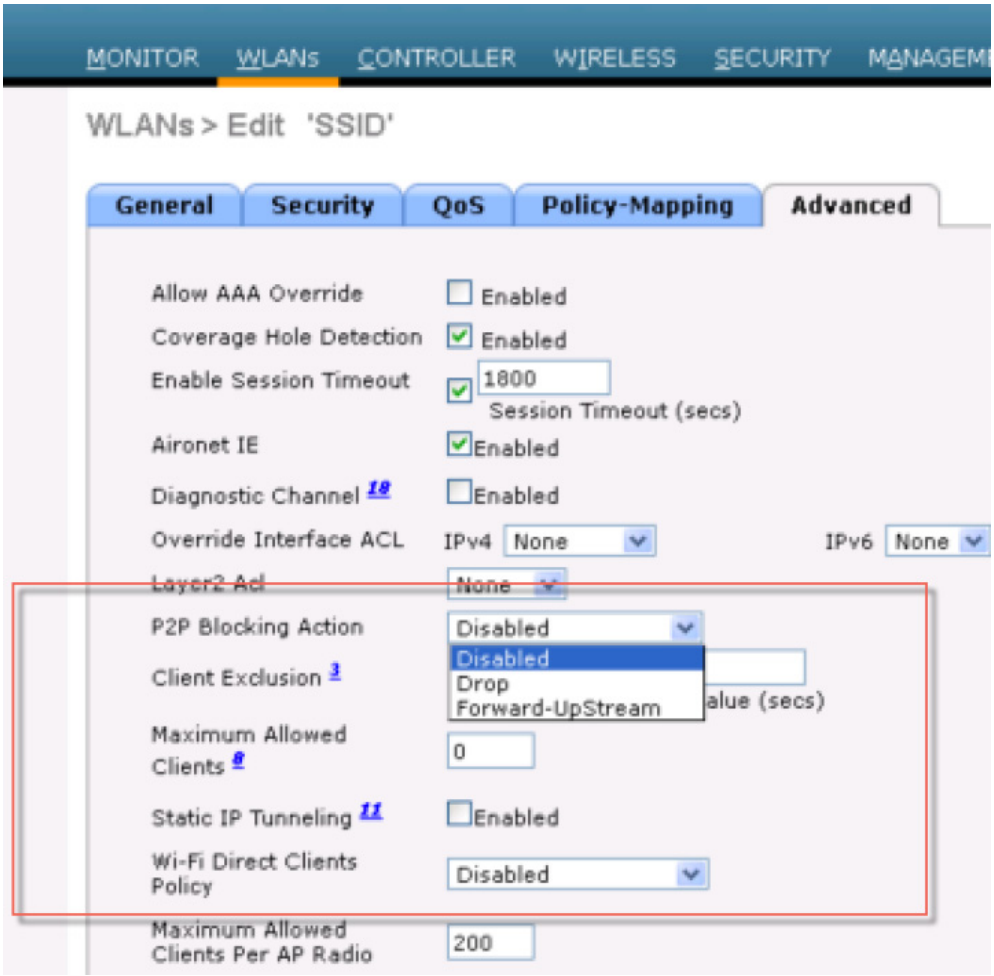
ピアツーピア ブロック

WLC は、同じ WLAN のクライアント同士の通信をブロックするように設定できます。ルータを介して通信するように強制することで、同じサブネットのクライアント同士で見込まれる攻撃を防止します。

図 4-21 は、WLC 上でのピアツーピア ブロックの設定画面です。

(注)　これは WLC のグローバル設定ではなく、以降のリリースで特定の WLAN に適用されます。

図 4-21　ピアツーピア ブロック



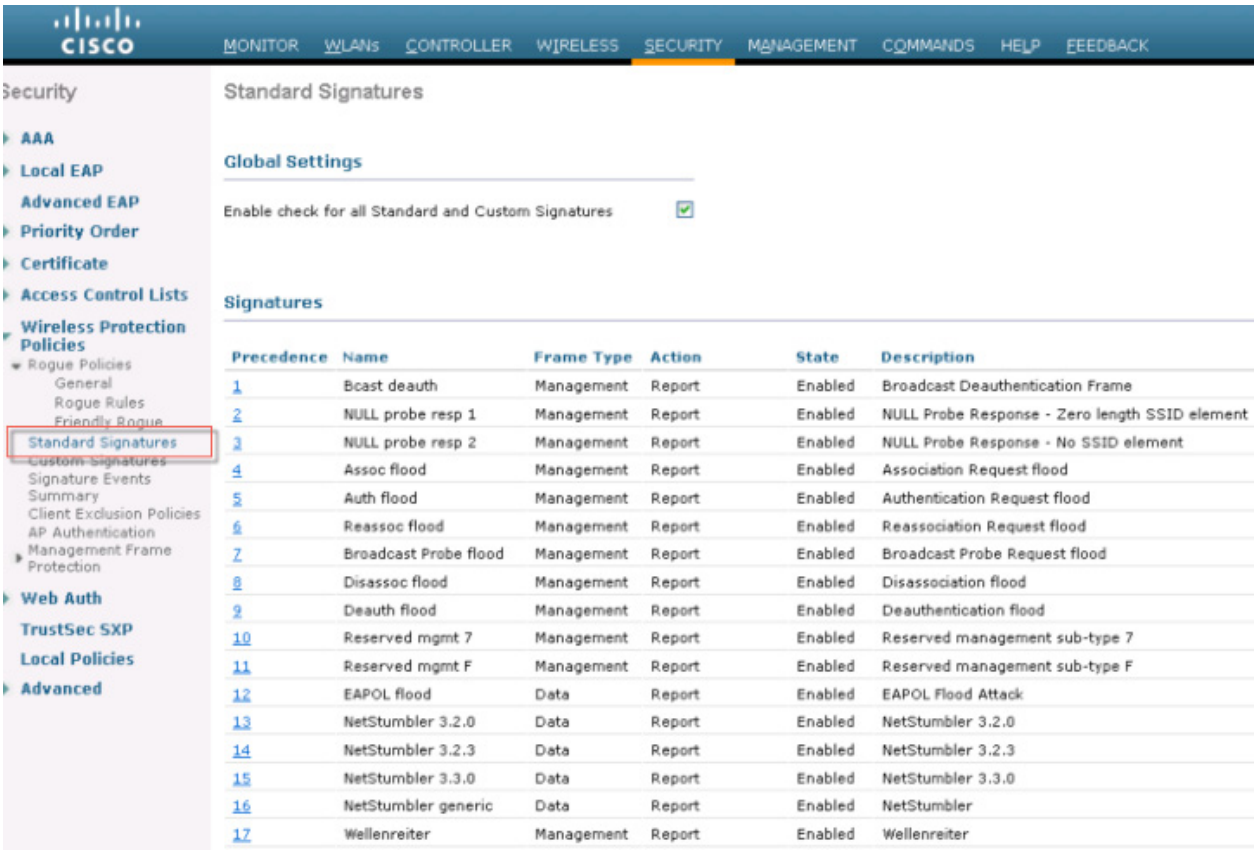
無線 IDS

WLC は、接続されたすべての AP から取得した情報を使用して WLAN の IDS 分析を行い、WLC のほか WCS に対して検出された攻撃も報告します。無線 IDS 分析は、有線ネットワーク IDS システムで実行できる分析を補完するものです。WLC の組み込みの無線 IDS 機能では、有線ネットワーク IDS システムから見ることのできない、または使用できない 802.11 および WLC 固有の情報を分析します。

WLC によって使用される無線 IDS シグニチャ ファイルは WLC ソフトウェア リリースに含まれています。ただし、別のシグニチャ ファイルを使用して個別に更新することが可能です。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 [Standard Signatures] ウィンドウです。

図 4-22　標準の WLAN IDS シグニチャ



Cisco Adaptive Wireless Intrusion Prevention System

シスコの適応型 Wireless Intrusion Prevention System(wIPS)は、無線の脅威の検出およびパフォーマンスの管理のための高度な手法です。この手法では、ネットワーク トラフィック分析、ネットワーク デバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。インフラストラクチャに完全に統合されたソリューションを採用すると、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワークインテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃をより正確に特定し事前に防止することができます。

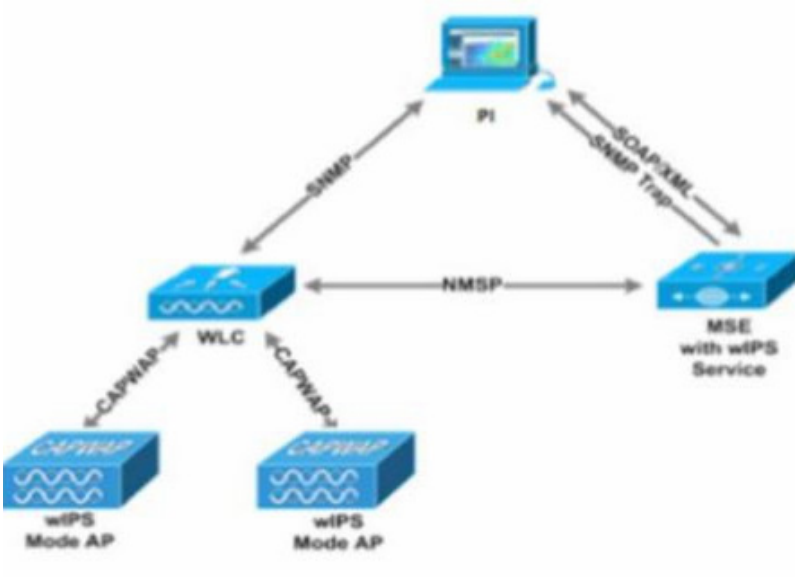
Cisco Adaptive wIPS には、Cisco Mobility Services Engine(MSE)が必要です。MSE は、Cisco Aironet アクセス ポイントの継続的なモニタリングによって収集された情報の処理を一元化します。シスコの適応型 wIPS の機能と、MSE への Cisco Prime Infrastructure の統合により、wIPS サービスで wIPS ポリシーとアラームの設定、監視、およびレポートを行うことができます。

シスコの適応型 wIPS はコントローラに設定されていません。代わりに、プロファイル設定が Cisco Prime Infrastructure から wIPS サービスに転送され、wIPS サービスによってそのプロファイルがコントローラに転送されます。プロファイルはコントローラのフラッシュメモリに格納され、アクセス ポイントがコントローラに join するとアクセス ポイントへ送信されます。アクセス ポイントのアソシエートが解除され、別のコントローラへ join すると、アクセス ポイントは新しいコントローラから wIPS プロファイルを受信します。wIPS 機能のサブセットを備えたローカル モードまたは FlexConnect モードのアクセス ポイントは、拡張ローカル モード アクセス ポイント、または ELM AP と呼ばれます。アクセス ポイントが次のいずれかのモードであれば、そのアクセス ポイントを wIPS モードで動作するように設定できます。

ワイヤレス IPS 通信プロトコル

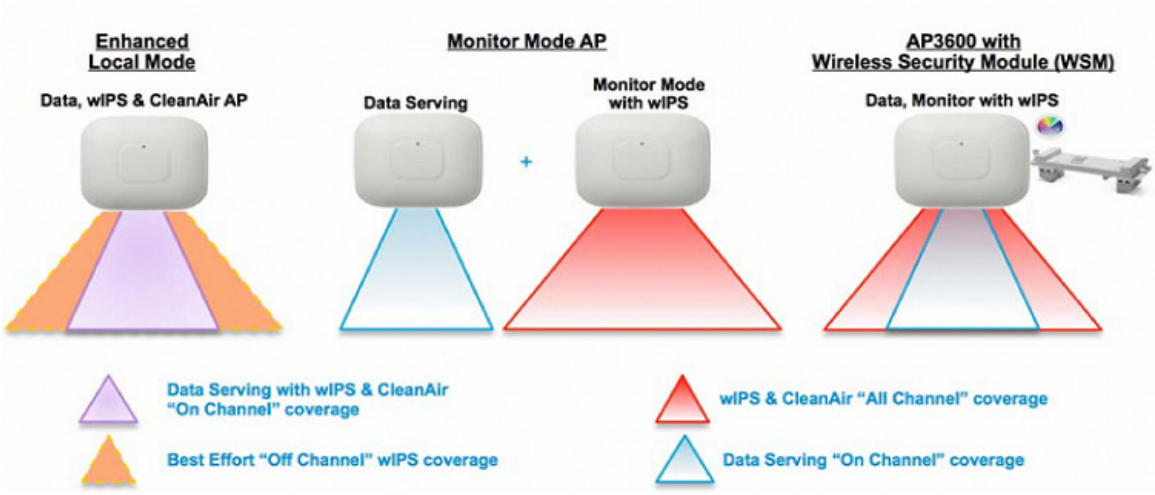
各システム コンポーネント間の通信を行うため、多くのプロトコルが使われています。

- CAPWAP(Control and Provisioning of Wireless Access Points):このプロトコルは、アクセス ポイントとコントローラ間の通信に使用されます。これは、アラーム情報をコントローラに行き来させ、設定情報をアクセス ポイントに適用する双方向トンネルを提供します。CAPWAP 制御メッセージは DTLS で暗号化され、CAPWAP データには DTLS による暗号化のオプションがあります。
- NMSP(Network Mobility Services Protocol):このプロトコルは、ワイヤレス LAN コントローラと Mobility Services Engine 間の通信に使用されます。ワイヤレス IPS 構成の場合、このプロトコルは、アラーム情報をコントローラから MSE へ集約し、ワイヤレス IPS 設定情報をコントローラに適用する経路を提供します。このプロトコルは暗号化されます。
  - コントローラ TCP ポート:16113
- SOAP/XML(Simple Object Access Protocol):このプロトコルは MSE と PI 間の通信方式です。このプロトコルは、MSE で実行するワイヤレス IPS サービスに設定パラメータを配布するために使用します。
  - oMSE TCP ポート:443
- SNMP(Simple Network Management Protocol):このプロトコルは、Mobility Services Engine から Prime Infrastructure に wIPS アラーム情報を転送するために使用されます。さらに、ワイヤレス LAN コントローラから Prime Infrastructure に不正アクセス ポイント情報を伝えるためにも使われます。



wIPS 導入モード

7.4 リリース以降、Cisco Adaptive Wireless IPS には wIPS モード アクセス ポイントの 3 つのオプションがあります。wIPS モード アクセス ポイントの違いを詳細に理解するために、各モードについて説明します。



wIPS を使用するローカル モード

wIPS を使用するローカル モードには「on-channel」の wIPS 検出があり、クライアントにサービスを提供しているチャネルで攻撃者を検出できます。他のすべてのチャネルでは、ELM がベスト エフォート型の wIPS 検出を提供します。

これは、すべてのフレームの無線が短時間「off-channel」になることを意味します。「off-channel」でも、チャネルのスキャン中に攻撃が発生すると攻撃は検出されます。

AP3600 の wIPS を使用するローカル モードの例では、2.4 GHz の無線がチャネル 6 で動作しています。AP は継続的にチャネル 6 をモニタし、チャネル 6 の攻撃はすべて検出および報告されます。攻撃者がチャネル 11 を攻撃すると、AP が「off-channel」のチャネル 11 のスキャン中でも攻撃が検出されます。

ELM の機能は次のとおりです。

- チャネル スキャン（2.4 GHz および 5 GHz）に 24 時間 365 日の wIPS セキュリティ スキャンを追加し、ベスト エフォート型のオフチャネル サポートを提供します。
- アクセス ポイントはクライアントに追加サービスを提供し、G2 シリーズのアクセス ポイントではチャネル（2.4 GHz および 5 GHz）に対する CleanAir スペクトラム解析も実行します。
- データを提供するローカルおよび FlexConnect AP での Adaptive wIPS スキャン。
- 個別のオーバーレイ ネットワークを必要としない保護。
- ワイヤレス LAN の PCI コンプライアンスをサポートします。
- フル 802.11 および 802.11 以外の攻撃を検出します。
- 調査およびレポート機能を追加します。
- 統合または専用 MM AP を柔軟に設定できます。
- AP での事前処理によってデータ バックホールを最小化します（つまり、非常に低い帯域幅のリンクでも機能します）。
- データ提供への影響を縮小します。

モニタ モード

モニタ モードでは、「off-channel」の wIPS 検出を行います。アクセス ポイントは長時間各チャネルを一時停止することによって、すべてのチャネルの攻撃を検出できます。2.4 GHz 無線はすべての 2.4 GHz チャネルをスキャンし、5 GHz チャネルはすべての 5 GHz チャネルをスキャンします。追加のアクセス ポイントをクライアント アクセスのためにインストールする必要があります。

モニタ モード機能の一部は次のとおりです。

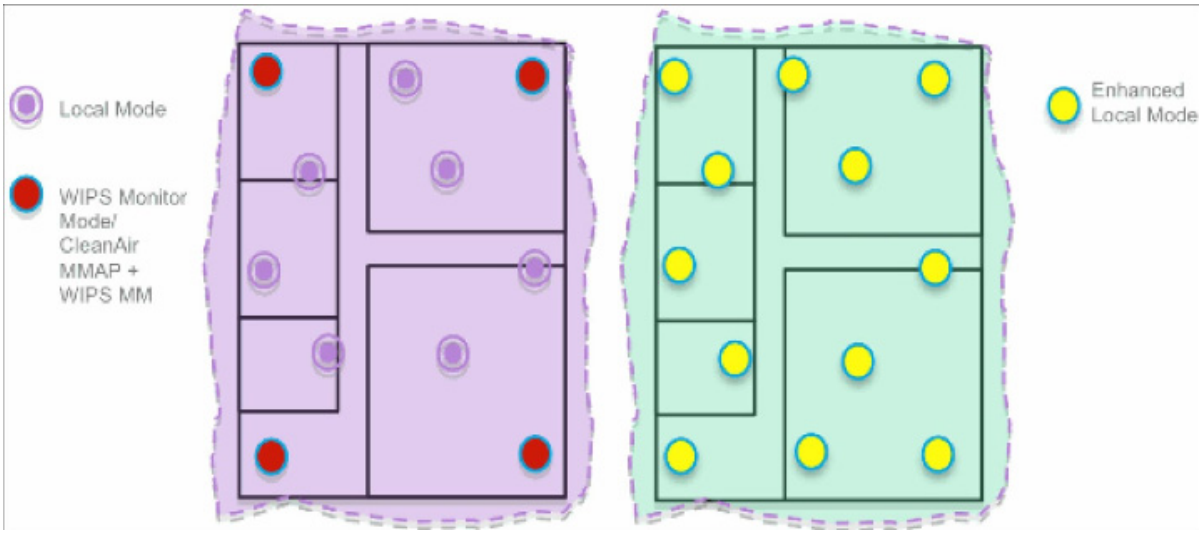
- モニタ モード アクセス ポイント（MMAP）はモニタ モード専用であり、すべてのチャネル（2.4 GHz および 5 GHz）に wIPS セキュリティ スキャンを追加することもできます。
- G2 シリーズのアクセス ポイントは、すべてのチャネル（2.4 GHz および 5 GHz）で CleanAir スペクトラム解析を実行できます。
- MMAP はクライアントにサービスを提供しません。

モニタ専用モードと ELM

図 4-23 では、wIPS モニタ モードの標準的な展開と ELM 機能を持つ AP の比較を示します。両方のモードの一般的な対象範囲は次のようになっています。

- wIPS のモニタ専用モードの AP（図 4-23 では赤色で表示）は、一般的に 15,000 ～ 35,000 平方フィートを対象範囲とします。
- ELM 機能を持つ AP（図 4-23 では黄色で表示）は、一般的に 3,000 ～ 5,000 平方フィートを対象範囲とします。

図 4-23　モニタ モードと ELM の比較



従来の wIPS 展開の場合、5 つのローカル モード AP ごとに 1 つのモニタ モード AP という比率を推奨します。これは、最適なカバレッジ範囲を実現するネットワーク設計や専門知識により異なる場合があります。ELM により、既存のすべての AP で ELM ソフトウェア機能を有効にするだけで、パフォーマンスを維持しつつ、モニタ モード wIPS 操作をローカル データ サービス モード AP に効果的に追加できます。

ワイヤレス セキュリティ モジュール（WSM）搭載の AP 3600/3700：ワイヤレス セキュリティとスペクトルの進化形

WSM モジュール（AIR-RM300M=）を搭載した Cisco 3600/3700 シリーズ アクセス ポイントは、「オンチャネル」と「オフチャネル」の組み合わせを使用します。つまり、AP3600/3700 の 2.4 GHz および 5 GHz が、クライアントにサービスを提供しているチャネルをスキャンする一方で、WSM モジュールがモニタ モードで動作し、すべてのチャネルをスキャンします。

WSM モジュールには次のような機能があります。

- クライアントへのサービス提供、wIPS セキュリティ スキャン、および CleanAir テクノロジーを使用したスペクトラム解析を同時に実行できる業界初のアクセス ポイントです。
- 独自のアンテナで 2.4 GHz および 5 GHz の専用無線を提供し、2.4 GHz および 5 GHz 帯域のすべての無線チャネルに対する 24 時間 365 日のスキャンを実行できます。
- 単一のイーサネット インフラストラクチャが実現することで、管理するデバイス数の削減で運用は簡素化され、AP3600 ワイヤレス インフラストラクチャおよびイーサネット有線インフラストラクチャへの投資回収率を最適化します。

シスコの第 1 世代ワイヤレス セキュリティ モジュール（AIR-RM3000M=）は、20 MHz チャネルに対する無線攻撃のみスキャンできます。11ac レートでの攻撃は検出できません。シスコは、11ac レートに対する攻撃を検出し、MSE にレポートできる高度なセキュリティを備えた新しいモジュール（AIR-RM3010L-x-K9=）を導入しました。

次の比較表は、2 つのセキュリティ モジュールの違いを示しています。製品番号が異なっており、WSM は 20 MHz チャネルのみスキャンできますが、ASM は 20/40/80 MHz をスキャンできます。どちらも 3600 および 3700 AP に搭載される、フィールド アップグレード可能なモジュールです。第 2 世代モジュールは、ロケーションを正確に特定するためのハイパー ロケーション アンテナ アレイを搭載しており、アンテナ アレイから独立して動作できます。

Part number	AIR-RM3000M=	AIR-RM3010L-x-K9=
Scanning	802.11n scanning capability on 20 MHz (non-serving radio)	802.11n and **802.11ac** scanning capability on 20, 40, 80 MHz (non-serving radio)
Module Integration	Plug in module for AP 3600/3700	Plug in module for AP 3600/3700 **with or without** Hyperlocation antenna array for location accuracy

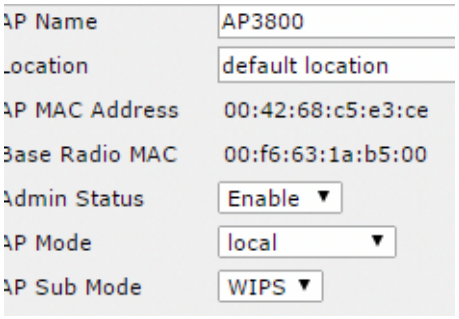
2800、3800、および 1560 AP での WIPS モニタリング

フレキシブル ラジオ アサインメントでは、統合無線の動作ロールを手動で設定することも、利用可能な RF 環境に基づいて AP でインテリジェントに決定することもできます。AP は、ワイヤレス セキュリティ モニタリングおよび 5 GHz ロールで動作できます。このロールでは、一方の無線が 5 GHz クライアントにサービスを提供し、もう一方の無線が 2.4 GHz と 5 GHz の両方をスキャンして wIPS 攻撃者、CleanAir 干渉源、および不正なデバイスを検出します。

無線がそのサービス チャネル上にある場合は「オンチャネル」と見なされ、他のチャネルをスキャンしている場合は「オフチャネル」と見なされます。AP に WIPS スキャンを設定できる展開シナリオは 3 つあります。

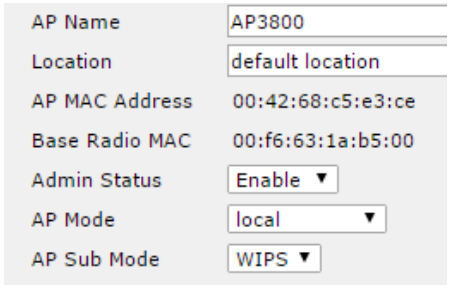
ELM がグローバル モードで FRA 無線がクライアント サービス モード：ベストエフォートのオフチャネル サポートを提供します。

wIPS を使用するローカル モードには「on-channel」の wIPS 検出があり、クライアントにサービスを提供しているチャネルで攻撃者を検出できます。他のすべてのチャネルでは、ELM がベストエフォート型の wIPS 検出を提供します。ベストエフォートでの検出では、フレームごとに無線が短時間「オフチャネル」になります。「オフチャネル」の場合、そのチャネルをスキャン中に攻撃が行われると、攻撃が検出されます。ELM クライアント サービス モードの FRA 無線は、引き続きクライアントにサービスを提供できます。

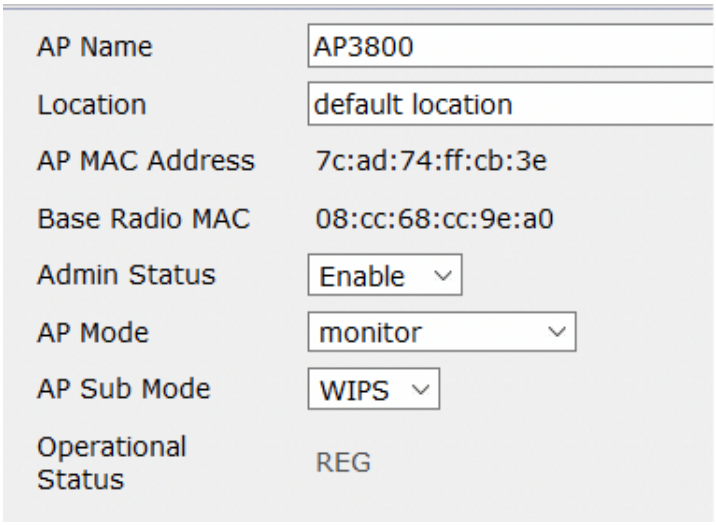


ELM がグローバル モードで FRA 無線がモニター モード:

ELM モードでは、無線スロット 1（5 GHz）に対するベストエフォートのスキャンが実施されます。一方、FRA 無線のモニタ モードでは、専用の wIPS 検出が「オフチャネル」で実施されます。つまり、アクセス ポイントが各チャネルに長時間留まり、すべてのチャネルに対する攻撃を検出します。モニタ モードの FRA 無線はクライアントにサービスを提供できません。



モニタ モードの AP：すべてのチャネル（2.4 GHz および 5 GHz）に対して専用の wIPS セキュリティ スキャンを実施し、無線攻撃を検出します。

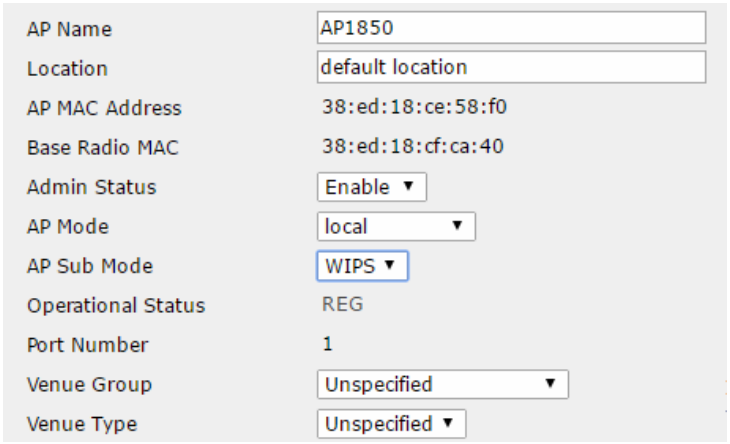


1800 AP プラットフォーム（1810、1815、1850、および 1830）での WIPS モニタリング

同様に、1810、1815、1850、および 1830 を含む 1800 Wave 2 アクセス ポイントをネットワークに展開し、wIPS 攻撃者、CleanAir 干渉源、および不正なデバイスを無線でスキャンできます。AP プラットフォームでは、wIPS スキャンはローカル モードでのみサポートされます。モニタ モードではサポートされません。

ELM モード – WIPS をサブ モードとして使用するローカル AP モード

wIPS を使用したローカル モードでは、「オンチャネル」での wIPS 検出が可能です。それにより、攻撃者がクライアント用のチャネルで検出されます。他のすべてのチャネルでは、ELM がベストエフォート型の wIPS 検出を提供します。ベストエフォートでの検出では、フレームごとに無線が短時間「オフチャネル」になります。「オフチャネル」の場合、そのチャネルをスキャン中に攻撃が行われると、攻撃が検出されます。ELM クライアント サービス モードの FRA 無線は、引き続きクライアントにサービスを提供できます。



追加情報と設定手順については、次のリンクにある wIPS 導入ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/technology/wips/deployment/guide/WiPS_deployment_guide.html

on-channel および off-channel のパフォーマンス

AP がチャネルにアクセスしたときに、攻撃を検出および分類するためにそのチャネルに留まる時間を、一時停止時間と呼びます。ELM の主機能は、データ、音声およびビデオ クライアント、サービスのパフォーマンスに影響を与えることなく、on-channel 攻撃で効果的に機能します。これに対し、ローカル モードでは、攻撃を検出および分類するための最低限の一時停止時間を提供する off-channel スキャンは場合によって変化します。

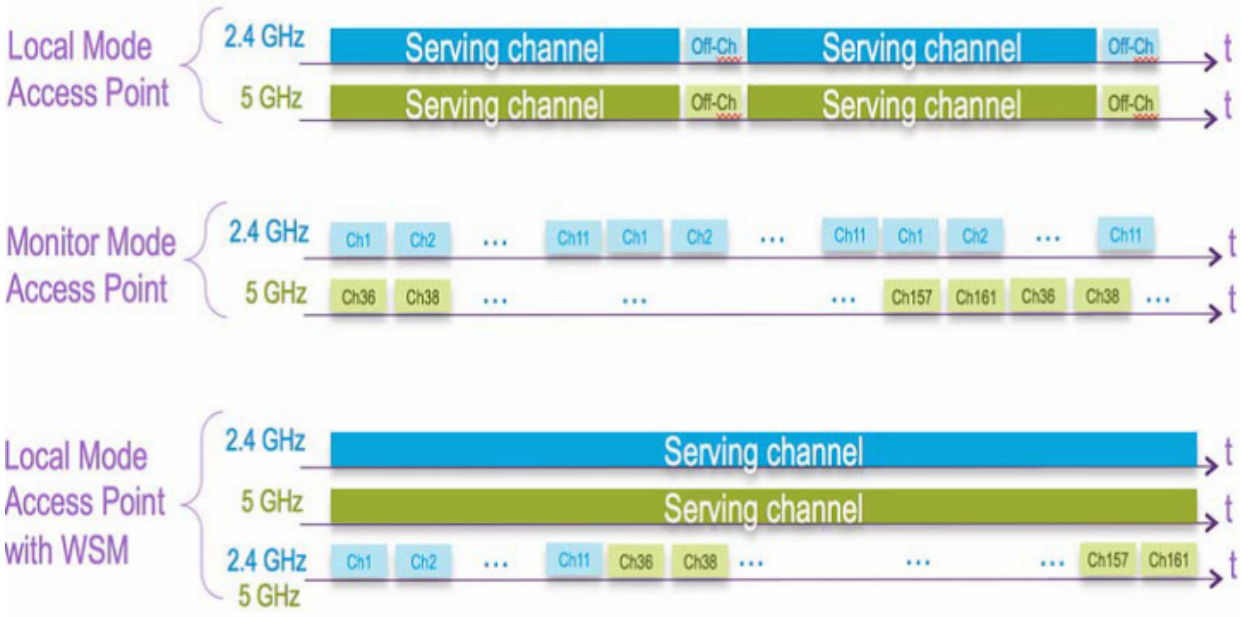
たとえば、音声クライアントが AP に関連付けられている場合、無線リソース管理（RRM）により、サービスが影響を受けないことを保証するため、音声クライアントがアソシエート解除されるまでスキャンが延期されます。この例では、off-channel 中の ELM による検出はベスト エフォート型と見なされます。すべてのチャネル、カントリー チャネルまたは DCA チャネルで近隣の ELM AP で動作することで効果が増します。したがって、保護範囲を最大化するために、ローカル モードのすべての AP で ELM を有効にすることが推奨されます。すべてのチャネルでフルタイムの専用スキャニングが必要な場合、シスコではモニタ モードの AP を展開することを推奨します。

通常、ローカル モードとモニタ モードの AP の相違点は以下のとおりです。

- ローカル モード AP：WLAN クライアントにタイム スライシング off-channel スキャニングを提供し、各チャネルで 50 ミリ秒間リスニングして、設定によりすべてのチャネル、カントリー チャネルまたは DCA チャネルのスキャニングを実行します。
- モニタ モード AP：WLAN クライアントにサービスを提供せず、スキャニングだけを行い、各チャネルで 1.2 秒間リスニングして、すべてのチャネルをスキャンします。

次の図で、無線の動作について説明します。無線がサービス チャネル上にあるときは「on-channel」、無線が他のチャネルをスキャンしているときは「off-channel」と見なされます。

ローカル モードの AP はほとんど「on-channel」で、「off-channel」の攻撃者を検出することは困難です。モニタ モードの AP は常時「off-channel」ですが、クライアントにサービスを提供することはできません。WSM モジュールは両方を最適に組み合わせます。



WAN リンクをまたぐ ELM

シスコは、低帯域幅 WAN リンクでの ELM AP の展開など、困難なトポロジにおける機能の最適化に努めてきました。ELM 機能は、AP での攻撃シグニチャの判別のための事前処理を行い、低速リンクで機能するように最適化されています。シスコは、WAN 経由の ELM のパフォーマンスを検証する基準をテストおよび測定することを推奨します。

CleanAir 統合

Cisco CleanAir テクノロジーは、ワイヤレス干渉の影響を緩和して 802.11n ネットワークに対しパフォーマンスの保護を提供する、セルフ ヒーリングと自己最適化が可能なスペクトラム対応の無線ネットワークです。

ELM 機能は、モニタ モード AP の展開と同様のパフォーマンスとメリットにより CleanAir 操作を補完し、次のような既存の CleanAir スペクトラム対応のメリットをもたらします。

- 専用シリコン レベル RF インテリジェンス
- スペクトラム対応、セルフ ヒーリング、自己最適化
- 非標準のチャネル脅威および干渉の検出と緩和
- Bluetooth、マイクロ波、コードレス電話などの非 Wi-Fi 検出
- RF ジャマーなどの RF 層 DOS 攻撃の検出と特定

ELM wIPS アラーム フロー

攻撃は、信頼できる AP で発生した場合にのみ該当します。ELM AP は攻撃を検出した後、管理システム Cisco Prime に攻撃を通知し、関連付けて、報告します。アラーム フローの一般的なプロセスは次のとおりです。

1. 攻撃が、信頼できる AP に対して発生します。
2. ELM 機能を持つ AP の検出が CAPWAP を介して WLC に通知されます。
3. NMSP を介して MSE に透過的に渡されます。
4. MSE 上の wIPS データベースにログインし、SNMP トラップを介して、管理システム Cisco Prime に送信します。
5. 管理システム Cisco Prime に表示されます。

Cisco Adaptive wIPS アラーム

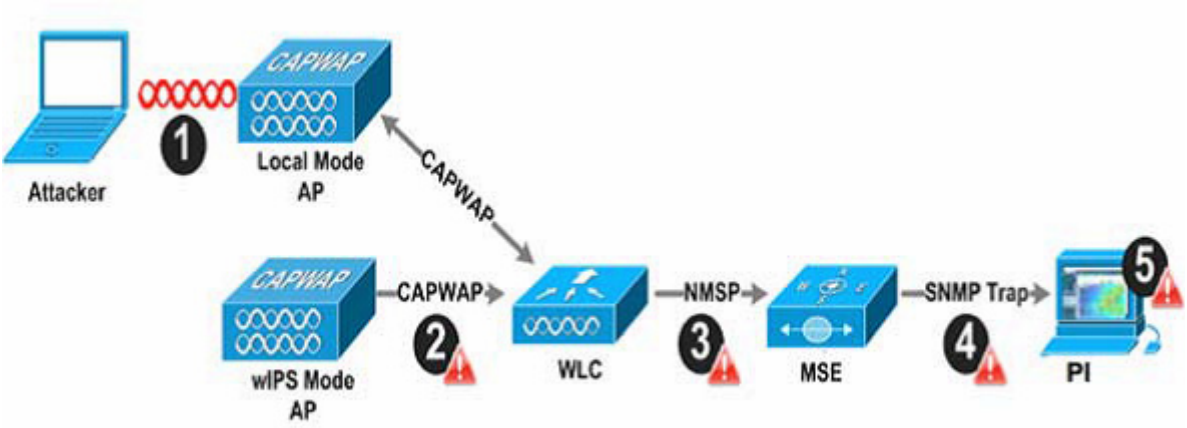
コントローラは、潜在的な脅威の通知として動作する 5 つの Cisco 適応型 wIPS アラームをサポートします。Cisco Prime Infrastructure を使用して、ご使用のネットワーク トポロジに基づいてこれらのアラームを有効にする必要があります。詳細については、『Cisco Prime Infrastructure User Guide』を参照してください。

- VPN で保護されていないデバイス：すべてのコントローラのトラフィックが VPN 接続を介してルーティングされるように、ワイヤレス クライアントとアクセス ポイントがセキュアな VPN を介して通信していない場合に、コントローラはアラームを生成します。
- WPA ディクショナリ攻撃：WPA のセキュリティ キー上でディクショナリ攻撃が発生した場合、コントローラはアラームを生成します。攻撃は、クライアントとアクセス ポイント間の最初のハンドシェイク メッセージの前に検出されます。

- 検出された WiFi ダイレクト セッション：クライアントの WiFi ダイレクト セッションが Wifi ダイレクトで検出された場合にコントローラはアラームを生成し、エンタープライズの脆弱性が回避されます。
- RSN インフォメーション エレメント Out-of-Bound サービス拒否：RSN インフォメーション エレメントの容量が大きくて、アクセス ポイントのクラッシュが生じた場合、コントローラはアラームを生成します。
- DS パラメータ セット DoS：コントローラは、複数のチャネルが重複している間にクライアントのチャネルで混乱が生じた場合にアラームを生成します。

Adaptive wIPS システムは、通信のリニア チェーンに従って、エアウェーブのスキャンから取得した攻撃情報を Prime Infrastructure のコンソールに伝播します。

図 4-24　脅威検出のアラーム フロー



1. Cisco 適応型ワイヤレス IPS システムでアラームをトリガーさせるためには、正規のアクセス ポイントまたはクライアントに対して攻撃が仕掛けられる必要があります。正規のアクセス ポイントおよびクライアントは、同じ「RF グループ」名をブロードキャストする「信頼する」デバイスによって、Cisco Unified Wireless Network 内で自動的に検出されます。この設定では、ローカルモード アクセス ポイントとそれらに関連付けられたクライアントのリストが動的に管理されます。SSID グループ機能を使用して、SSID によってデバイスを信頼するようにシステムを設定することもできます。WLAN インフラストラクチャに害を及ぼすと見なされた攻撃だけが残りのシステムに伝播されます。
2. ワイヤレス IPS モード アクセス ポイント エンジンによって攻撃が識別されると、アラームの更新がワイヤレス LAN コントローラに送信され、CAPWAP 制御トンネル内にカプセル化されます。
3. ワイヤレス LAN コントローラは、アラームの更新をアクセス ポイントから、Mobility Services Engine を実行するワイヤレス IPS サービスに透過的に転送します。この通信に使用されるプロトコルは NMSP です。
4. Mobility Services Engine 上のワイヤレス IPS サービスによって受け取られたアラームの更新は、アーカイブと攻撃追跡のためにアラーム データベースに追加されます。SNMP トラップが攻撃情報を格納する Prime Infrastructure に転送されます。同じ攻撃を参照する複数のアラーム更新が受け取られた（たとえば、複数のアクセス ポイントで同じ攻撃が認識された）場合、1 つの SNMP トラップだけが Prime Infrastructure に送信されます。
5. アラーム情報を含む SNMP トラップは Prime Infrastructure によって受信され、表示されます。

導入に関する考慮事項:必要なコンポーネント

Cisco 適応型ワイヤレス IPS システムの基本システム コンポーネントを次の通りです。

- wIPS モニタ モードのアクセス ポイント、wIPS またはワイヤレス セキュリティ モジュールを使用するローカル モードのアクセス ポイント
- ワイヤレス LAN コントローラ
- ワイヤレス IPS サービスを実行する Mobility Services Engine
- Prime Infrastructure

適応型ワイヤレス IPS システムに必要な最小コード バージョン:

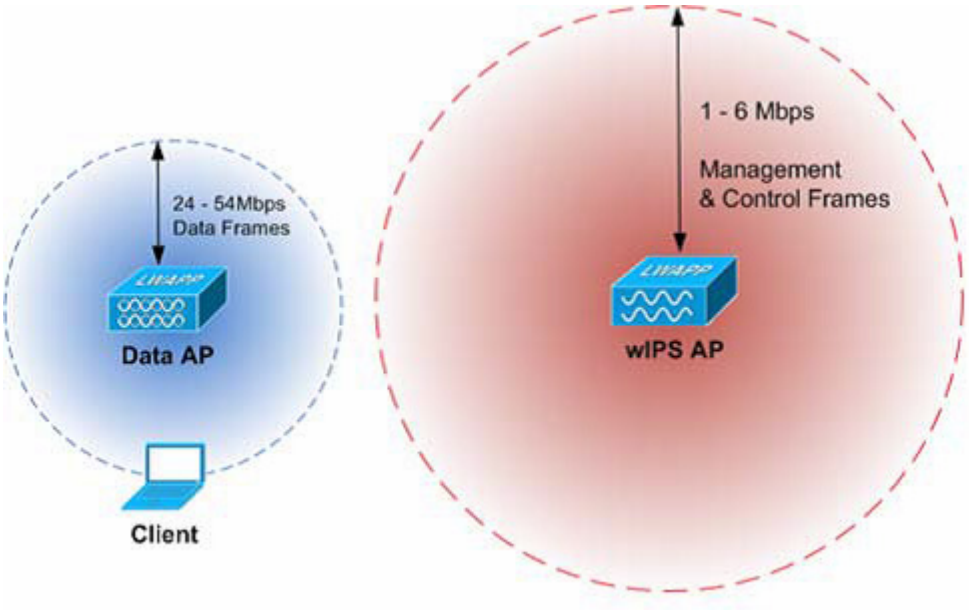
- Cisco Mobility Services Engine ソフトウェア リリース 5.2.xxx 以降で使用可能
- Cisco Prime Infrastructure バージョン 1.3 が必要
- Cisco Wireless LAN Controller で 7.2.xxx 以降が必要
- リリース 7.2 以降のワイヤレス IPS 機能には、モニタ モードの(つまり、クライアントにサービスを提供しない)アクセス ポイントが必要
- リリース 7.2.xxx 以降のワイヤレス IPS 機能には、wIPS を使用するローカル モードの(つまり、クライアントにサービスを提供しない)アクセス ポイントが必要

ワイヤレス セキュリティ モジュール(WSM)に必要な最小コード バージョン:

- ワイヤレス LAN コントローラ:バージョン 7.4.XX 以降
- Cisco Prime Infrastructure:バージョン 1.3.XX 以降
- Mobility Services Engine:バージョン 7.4.XX 以降

必要な wIPS アクセス ポイント数

Adaptive wIPS システムを構成する前に、アクセス ポイントのセルの通信範囲が、フレームが受信され、復号化される実際の範囲より小さいことを考慮することが重要です。この相違の理由は、アクセス ポイントの通信範囲が、最弱リンク(一般的な構成では WLAN クライアント)によって制限されるためです。WLAN クライアントの出力がアクセス ポイントの最大出力より本質的に低いため、セルの範囲はクライアントの能力に制限されます。さらに、アクセス ポイントを全出力以下で実行し、ワイヤレス ネットワークに RF 冗長性とロード バランシングを組み込むことをお勧めします。これらの先述の事項とシスコのアクセス ポイントの優れたレシーバ感度の組み合わせによって、Adaptive wIPS システムは、広範囲の監視を行いながら、クライアントがサービスするインフラストラクチャより少ないアクセス ポイント密度で構成できます。



上の図で示すように、ワイヤレス IPS の構成は、大半の攻撃で障害の発生に使われる 802.11 管理および制御フレームの検知に基づきます。これは、24 Mbps から 54 Mbps の高いスループット データ レートを提供するために調査されるデータ アクセス ポイントと異なります。

特定の環境に必要なワイヤレス IPS アクセス ポイント数を正確に決定するために、多数の要因があります。目的とする構成のセキュリティ要件と環境条件はそれぞれ異なるため、すべての構成のニーズに対処する確実なルールはありませんが、いくつかの一般的なガイドラインを考慮する必要があります。

必要な wIPS アクセス ポイント数に影響する主な要因を次に示します。

アクセス ポイント密度の推奨事項

アクセス ポイント カバレッジの占有面積は周波数と環境に基づいて測定できますが、新しい wIPS モードを使用する場合は他の要素も wIPS アクセス ポイント密度の推奨事項に関係します。すべてのアクセス ポイント モードで同じ距離をモニタできますが、次の理由から、異なる密度で各モードを展開することを推奨します。

wIPS を使用するローカル モードのアクセス ポイントは、クライアントへのサービス提供を対象としています。wIPS を使用するローカル モードを展開する場合、すべてのアクセス ポイントを wIPS を使用するローカル モードにすることを推奨します。

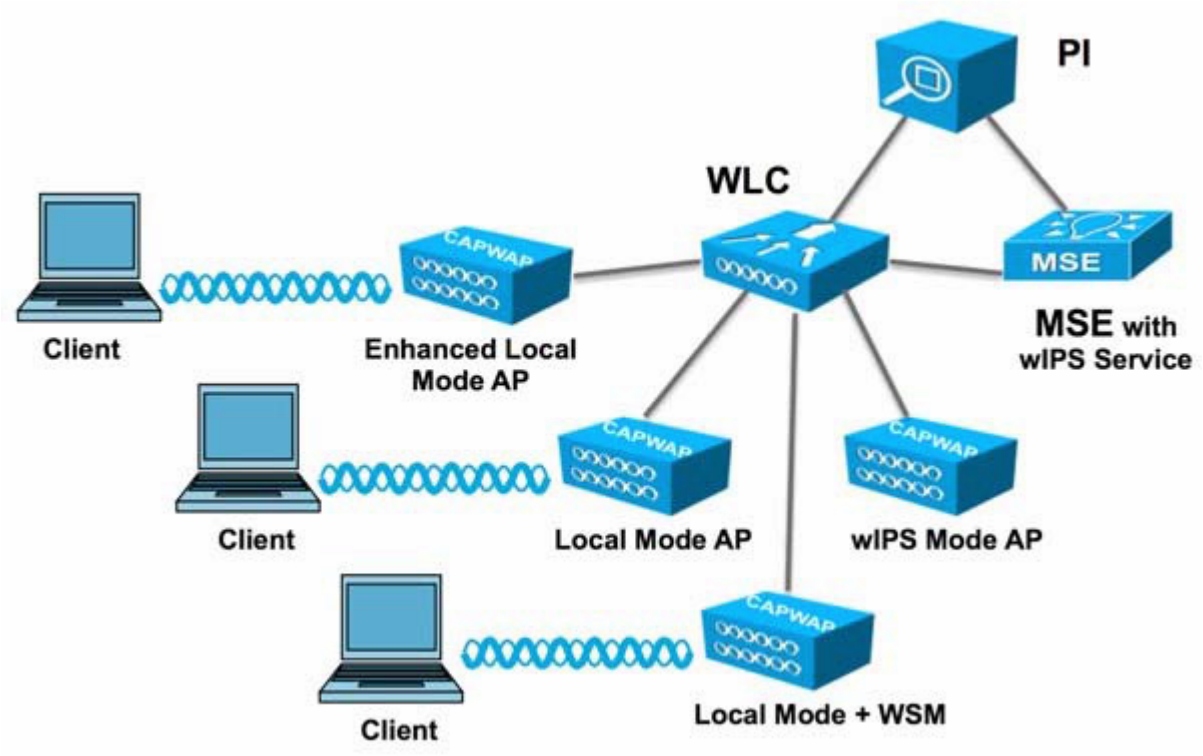
モニタ モードのアクセス ポイントの場合、ローカル モードとモニタ モードのアクセスポイントの比率を 1:5 にすることを推奨します。

最後に、WSM モジュールには、2.4 GHz および 5 GHz 帯域の両方ですべてのチャネルをモニタする単一の無線があります。無線はスキャンするチャネルを追加するため、検出時間を短縮するために WSM モジュールを 2:5 の密度で展開することを推奨します。

	Good	Better	Best
Features	Enhanced Local Mode	Monitor Mode AP	AP3600 with Wireless Security Module (WSM)
Deployment Density (#WSM : #AP)	1:1	1:5	1:5 – CleanAir 2:5 - wIPS
Serving Wireless data clients while Securing and Monitoring	Y	N	Y
Shared Ethernet infrastructure for Wireless Data and Monitoring	Y	N (Requires a separate Ethernet connection for a Data AP and for Monitoring AP)	Y
wIPS Security Scanning	• 7x24 On-channel • Best effort Off-Channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
CleanAir Spectrum Intelligence	• 7x24 On-channel	• 7x 24 All channels on 2.4 and 5 GHz	• 7x 24 All channels on 2.4 and 5 GHz
Feature off-load – eliminating jitter from off channel scanning	N	N	Y

Cisco Unified Wireless Network に統合された wIPS

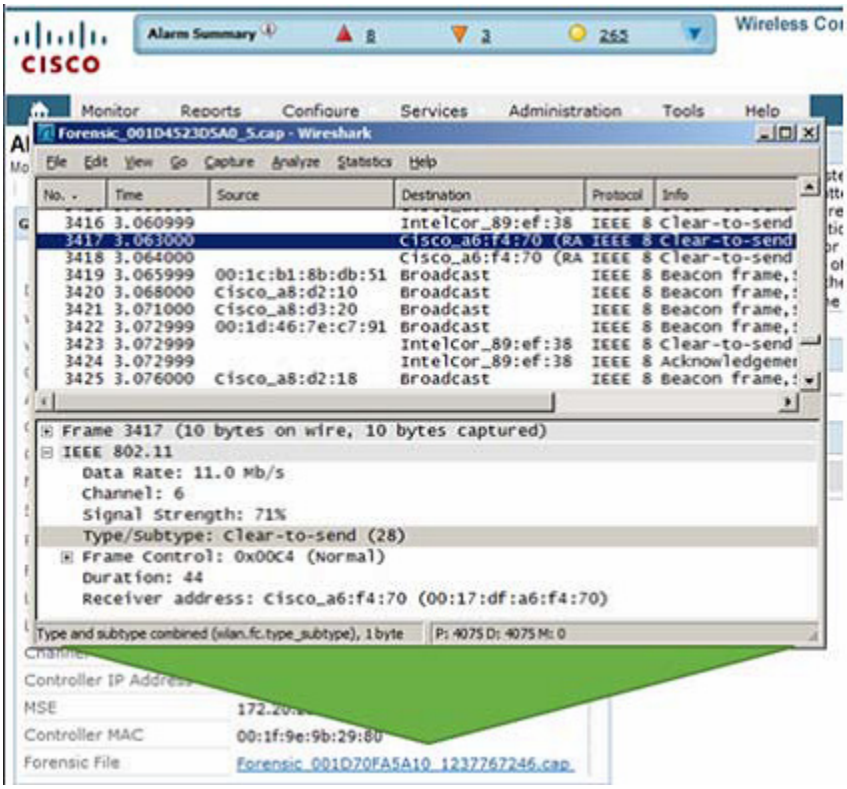
統合 wIPS 構成は、非 wIPS モードのアクセス ポイントと wIPS モードのアクセス ポイントを同じコントローラ上で混合させ、同じ Prime Infrastructure によって管理するシステム設計です。ローカル モード、FlexConnect モード、wIPS を使用するローカル モード、モニタ モード、および WSM モジュールを備えた 3600 シリーズ アクセス ポイントを組み合わせることができます。wIPS 保護およびデータのオーバーレイによって、コントローラや Prime Infrastructure を含む多くのコンポーネントが共有されるため、インフラストラクチャ コストの重複が削減されます。



フォレンジック

Cisco Adaptive wIPS システムは、詳しい調査とトラブルシューティングの目的で、攻撃フォレンジックをキャプチャする機能を提供します。基本レベルで、フォレンジック機能は、一連のワイヤレス フレームをログに記録し、抽出する機能を持つ切り替えベースのパケット キャプチャ ファシリティです。この機能は、PI の wIPS プロファイル設定内から攻撃単位で有効にします。

この機能をイネーブルにすると、エアウェーブに特定の攻撃アラームが見られたら、フォレンジック機能がトリガーされます。元のアラームをトリガーした wIPS モード AP のバッファ内に格納されたパケットに基づいて、フォレンジック ファイルが作成されます。このファイルは CAPWAP によってワイヤレス LAN コントローラに転送され、次に NMSP によって、Mobility Services Engine で実行するワイヤレス IPS サービスに転送されます。このファイルは、ユーザがフォレンジックに設定したディスク容量制限に達するまで、MSE のフォレンジック アーカイブに保存されます。デフォルトでこの制限は 20 GB で、この制限に達すると、最も古いフォレンジック ファイルが削除されます。フォレンジック ファイルには、フォレンジック ファイルへのハイパーリンクを含むアラームを Prime Infrastructure で開くことでアクセスできます。このファイルは、「CAP」ファイル形式で保存されており、WildPacket's Omnipeek、AirMagnet Wi-Fi Analyzer、Wireshark、またはこの形式をサポートしているその他のパケット キャプチャ プログラムを使用してアクセスできます。詳細については、Wireshark を参照してください。



クライアント除外

ワイヤレス IDS 以外に、WLC では追加の手順で WLAN インフラストラクチャと WLAN クライアントを保護することができます。WLC は、動作が脅威または不適切と見なされる WLAN クライアントを除外するポリシーを実行できます。図 4-25 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含む [Exclusion Policies] ウィンドウを示します。

- Excessive 802.11 association failures：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive 802.11 authentication failures：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive 802.1X authentication failures：可能性のある不正なクライアントまたは DoS 攻撃
- Maximum 802.1X - AAA Failure Attempts（1 ～ 10）
- IP theft or IP reuse：可能性のある不正なクライアントまたは DoS 攻撃
- Excessive web authentication failures：可能性のある DoS またはパスワード クラッキング攻撃

図 4-25　クライアント除外ポリシー

不正なデバイスおよびポリシーの管理

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

Rogue Location Discovery Protocol

Cisco Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモード（デフォルトでは無効になっています）では、不正なチャネルに移動してクライアントとして不正 AP に接続するようアクティブな AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、RLDP 機能によって有線ネットワーク上で不正 AP が検出されたことをネットワーク管理者に知らせるアラームが設定されます。RLDP の不正 AP の検出精度は 100 % です。オープン AP と NAT AP を検出します。

不正なデバイスの検出

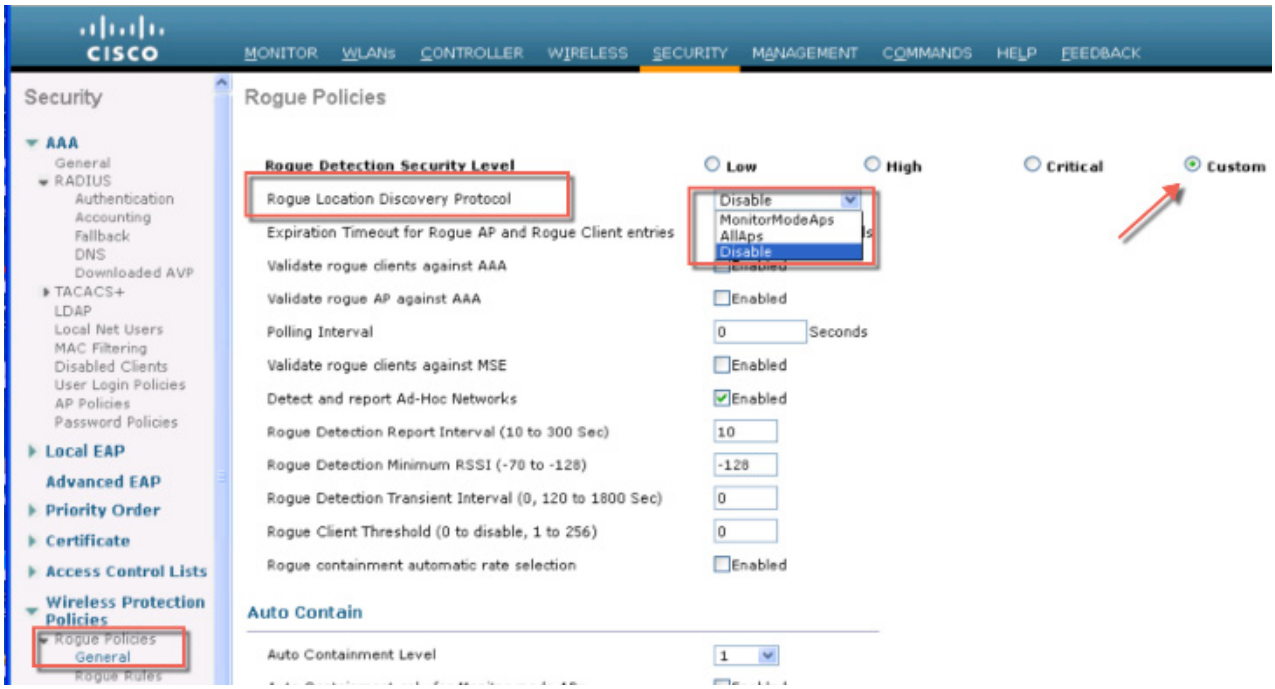
コントローラは、すべての近隣のアクセス ポイントを継続的に監視し、不正なアクセス ポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラは不正なアクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）を使用し、不正検出モードのアクセス ポイントが接続されて、不正がネットワークに接続されているかどうかを特定します。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDP のサイクルが終了すると、クライアントはアクセス ポイントに再接続します。不正なアクセス ポイントが検出された時点で（自動設定）、RLDP のプロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみ RLDP を使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があると RLDP が判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDP は、オープン認証に設定されている不正なアクセス ポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。

図 4-26　RLDP 設定の図

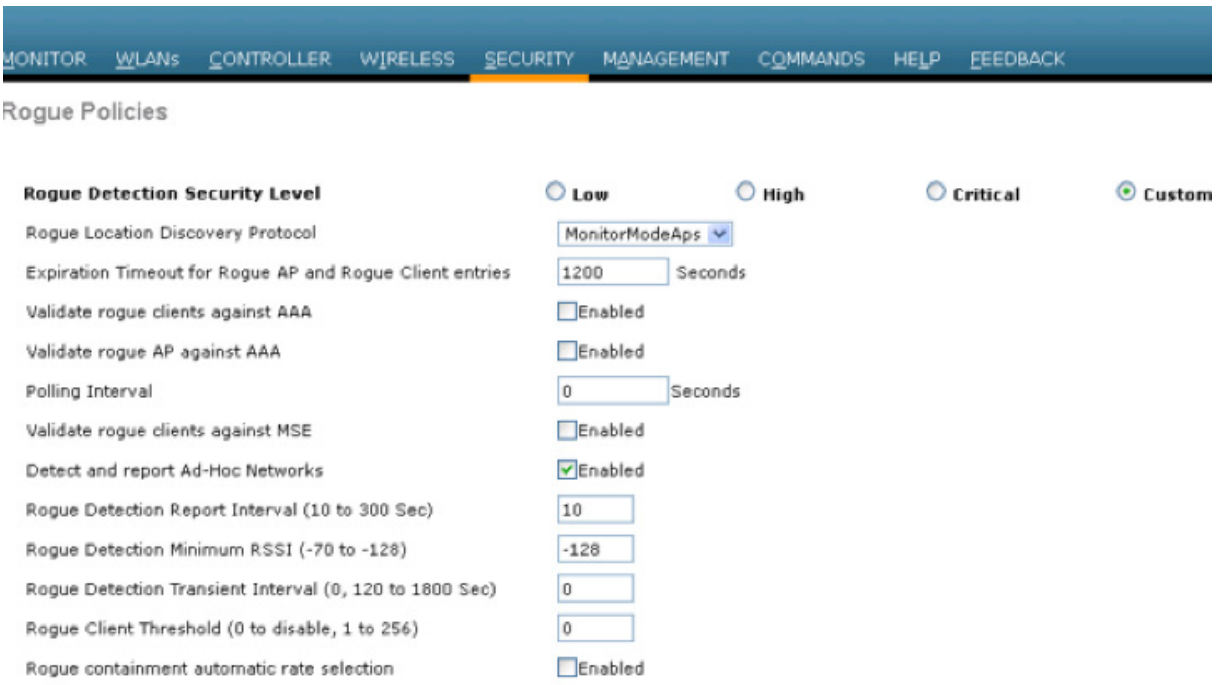


不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセス ポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、モニタ モードのアクセス ポイントだけを使用するようにコントローラを設定できます。

不正検出ポリシーのパラメータ

該当するアクセス ポイントで不正検出が有効になっていることを確認します。コントローラに join されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます（OfficeExtend アクセス ポイントを除く）。

1. [Rogue Detection Security Level] のオプションは次のとおりです。
   - [Low]：小規模な導入向けの基本不正検出。
   - [High]：中規模な展開向けの自動阻止を備えた基本不正検出。
   - [Critical]：機密性の高い展開向けの自動阻止と RLDP を備えた基本不正検出。
   - [Custom]：自動 RLDP の場合、セキュリティ レベルを [Custom] モードにする必要があります。[Custom] モードの場合でも RLDP のスケジューリングはありません。
2. [Rogue Location Discovery Protocol] AP のオプションは次のとおりです。
   - [Disable]：すべてのアクセス ポイントで RLDP を無効にします。これはデフォルト値です。
   - [All APs]：すべてのアクセス ポイントで RLDP を有効にします。
   - [Monitor Mode APs]：モニタ モードのアクセス ポイントでのみ RLDP を有効にします。



3. [Rogue Client Validation]：AAA、MSE サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントであるかどうかを検証し、[Validate Rogue Client] を選択します。

   MSE は、不正クライアントが有効で認識されたクライアントであるかどうかに関する情報を返します。コントローラは、不正クライアントを阻止するか、脅威と見なすことができます。

4. [Detect and Report Ad-Hoc Networks]：必要に応じて、アドホック不正検出および報告を選択します。

5. [Rogue Detection Report Interval]：AP からコントローラに不正検出レポートを送信する間隔を秒数で入力します。有効な範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。

6. [Rogue Detection Minimum RSSI]：AP が不正を検出し、不正エントリがコントローラで作成されるために必要な受信信号強度インジケータ（RSSI）の最小値を入力します。有効な範囲は -128 ～ 0 dBm で、デフォルト値は 0 dBm です。この機能は、すべての AP モードに適用できます。RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

7. [Rogue Detection Transient Interval]：不正が AP により最初にスキャンされた後、スキャンされる時間間隔。連続的に不正がスキャンされると、更新情報が定期的にコントローラへ送信されます。したがって、非常に短い時間だけアクティブで、その後は活動を停止する一時的な不正が AP によってフィルタリングされます。有効な範囲は 120 ～ 1800 秒で、デフォルト値は 0 秒です。不正検出の一時的間隔は、監視モードの AP にのみ適用されます。

   この機能には次の利点があります。

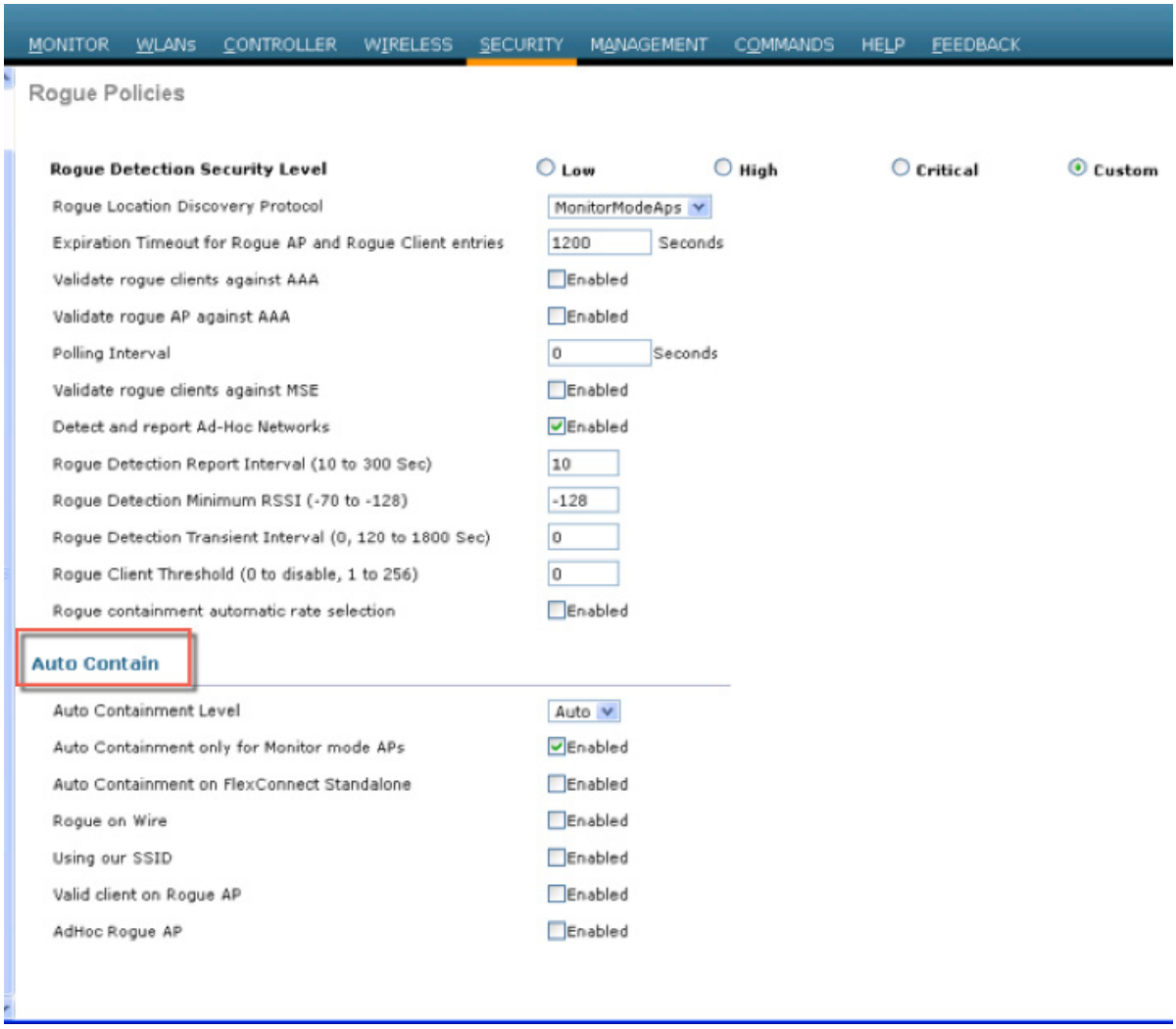
   - AP からコントローラへの不正 AP レポートが短くなる。
   - 一時的不正エントリをコントローラで回避できる。
   - 一時的不正への不要なメモリ割り当てを回避できる。

8. [Rogue Client Threshold]：しきい値。値が 0 の場合、rogue client threshold パラメータは無効になります。
9. [Rogue Containment Automatic Rate Selection]：このオプションを使用して、ターゲットの不正に最良のレートを使用するためにレートを最適化できます。AP は不正 RSSI に基づいて最良のレートを選択します。
10. [Containment]：コントローラに自動的に特定の不正デバイスを阻止させる場合は、次のパラメータを有効にします。
    - [Auto Containment Level]：自動阻止レベルを設定します。デフォルトで、自動阻止レベルは **1** に設定されています。[Auto] を選択すると、コントローラは有効な阻止を必要とする AP を動的に選択します。
    - [Auto Containment only for Monitor mode APs]：モニタ モード アクセス ポイントに自動阻止を設定します。
    - [Auto Containment on FlexConnect Standalone]：自動阻止に対する FlexConnect スタンドアロン モードのアクセス ポイント。
    - AP が接続 FlexConnect モードのときに自動阻止を設定した場合、自動阻止は続行されます。スタンドアロン AP がコントローラに再アソシエートされると、自動阻止が停止し、以降のアクションは AP が関連付けられているコントローラの設定によって決まります。FlexConnect AP のアドホック SSID および管理対象 SSID で自動阻止を設定することもできます。
    - [Rogue on Wire]：有線ネットワークで検出される不正の自動阻止を設定します。
    - [Using Our SSID]：ネットワークの SSID をアドバタイズする不正の自動阻止を設定します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
    - [Valid Client on Rogue AP]：該当する不正が関連付けられても、警告が生成されるだけです。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
    - [AdHoc Rogue AP]：このパラメータをオフにしておくと、該当するパラメータがオフでも、該当するネットワークが検出されても、警告が生成されるだけです。

注意　Auto Contain パラメータのいずれかを選択して [Apply] をクリックすると、「**この機能を使用すると法的責任を問われる場合があります。続行しますか?（Using this feature may have legal consequences. Do you want to continue?）**」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz および 5 GHz の周波数は一般に公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

図 4-27 は、不正ポリシー設定のオプション、RLDP セキュリティ レベルおよび AP での有効化を示しています。また、AAA または MSE に対する検証設定も示しています。

図 4-27　不正ポリシーの設定

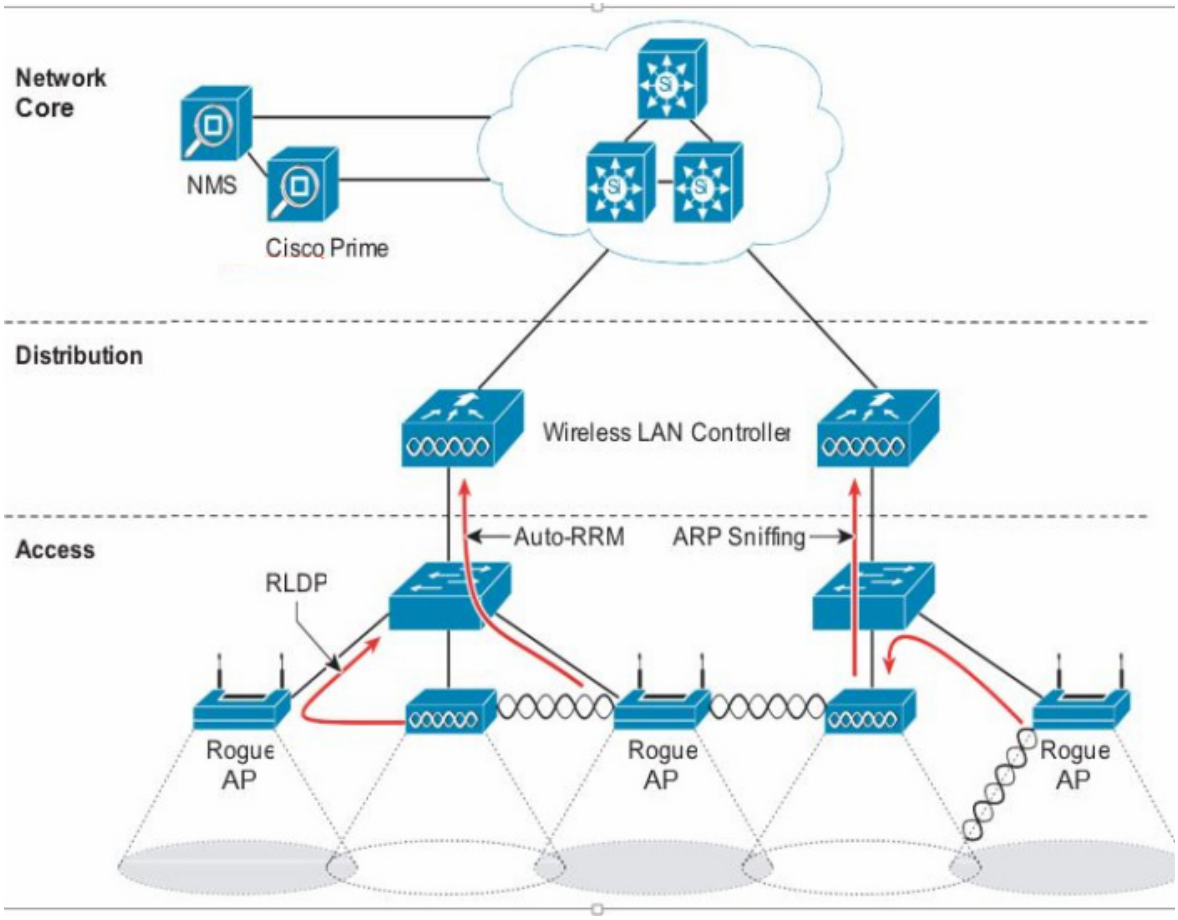


Rogue AP

図 4-28 で示したとおり、Cisco Unified Wireless Network ソリューションは不正 AP に完全なソリューションを提供します。このソリューションが提供する機能は次のとおりです。

- Air/RF の検出：ビーコンと 802.11 プローブの応答を検出またはスニッフィングすることによる不正なデバイスを検出すること。
- 不正 AP の検索：検出された RF 特性および管理された RF ネットワークの既知の特性を使用して、不正なデバイスを見つけること。
- 有線の検出：有線ネットワークに不正デバイスを関連付けたり追跡したりするためのメカニズム。
- 不正 AP の分離：不正 AP へのクライアント接続を防ぐメカニズム。

図 4-28　Unified Wireless Network での不正 AP 検出



Air/RF 検出

2 台の AP の RF 検出の導入モデルは次のとおりです。

- 標準 AP の導入
- モニタ モード AP の導入

これらの導入モデルはいずれも RF の検出をサポートするため、不正 AP に限定されませんが、アドホック クライアントや不正なクライアント（不正 AP のユーザ）が検出されたときにも情報を把握できます。モニタ モード用に設定された AP は RF チャネルのスキャン専用であり、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 を検索すると、AP は 50 ミリ秒間オフチャネルになって、不正なクライアントをリッスンし、ノイズやチャネルの干渉をモニタします。スキャンされたチャネルは 802.11a および 802.11b/g のグローバル WLAN ネットワーク パラメータで設定されます。

検出された不正と思われるクライアントやアクセス ポイントは、次の情報を収集するためにコントローラに送信されます。

- 不正 AP の MAC アドレス
- 不正 AP 名

- 不正に接続されたクライアントの MAC アドレス
- WPA、WEP または WEP2 でフレームが保護されているかどうか
- プリアンブル
- SNR
- 受信信号強度表示（RSSI）
- スイッチポート トレース

WLC が信頼済み AP から別のレポートを受け取るか、2 回目の検出サイクルが完了するまで、不正と思われるクライアントやアクセス ポイントは不正に分類されません。信頼済み AP は不正と思われるクライアントや AP のチャネルに移動して、不正なクライアントや AP、ノイズ、干渉をモニタします。同じクライアントや AP がもう一度検出されると、WLC 上で不正として分類されます。

いったん不正デバイスとして分類されると、WLC はこの不正 AP がローカル ネットワークに接続されているか、または単にネイバー AP であるかを確認します。いずれの場合でも、管理対象の Cisco Unified Wireless Network 外部の AP は不正として見なされます。

モニタ モードでは、信頼済み AP はユーザ トラフィックを伝送しないため、チャネルのスキャン専用です。顧客が特定のサービス エリアの WLAN をサポートしたくないが、そのエリアで 不正 AP および不正なクライアントをモニタしたい場合に、最も一般的に使用されるのがモニタ モードです。

場所

Cisco Prime Infrastructure のロケーション機能を使用して、不正 AP のおおよその場所を示す間取り図を提示することができます。間取り図にはすべての正規の AP の場所が表示され、不正 AP の場所がドクロのアイコンで強調表示されます。Cisco Unified Wireless Network のロケーション機能の詳細については、『Cisco Wireless Location Appliance』を参照してください。

有線の検出

AP の数が少ない支社や、間取り図情報が利用可能でないなど、不正な AP の場所を示す Cisco Prime Infrastructure の機能が有効でない場合があります。このような場合、Cisco Unified Wireless Network ソリューションでは 2 種類の有線ベースの検出オプションを使用できます。

- Rogue Detector AP
- Rogue Location Discovery Protocol（RLDP）

AP が Rogue Detector として設定されている場合、その AP の無線はオフになり、AP の役割は有線ネットワークをリッスンして不正 AP に関連付けられたクライアント、すなわち*不正なクライアント*の MAC アドレスを検出することになります。Rogue Detector は、不正なクライアントの MAC アドレスを含む ARP パケットをリッスンします。そのような ARP が検出されると、AP はその旨を WLC に報告し、Cisco Unified Wireless Network と同じネットワークに不正 AP が接続されているかどうかを検証します。

ARP 情報をとらえる可能性を最大まで上げるため、Rogue AP Detector は Switched Port Analyzer（SPAN）ポートを使用しているすべての使用可能なブロードキャスト ドメインに接続されます。一般的なネットワークに存在するさまざまな集約ブロードキャスト ドメインを把握するために、複数の Rogue AP Detector を展開することができます。

不正なクライアントが無線ルータ（共通のホーム WLAN デバイス）の背後にある場合、ARP 要求は有線ネットワークで認識されないため、Rogue Detector AP に代わる手段が必要となります。また、モニタすべきブロードキャスト ドメインが大量にあるような一部の展開（メイン キャンパス ネットワークなど）については、Rogue Detector AP が実用的でない場合もあります。

このような状況では RLDP オプションが役立ちます。この場合、不正 AP が検出されると、標準の AP はその不正 AP にクライアントとしてアソシエートし、コントローラにテスト パケットを送信しようとします。このとき、AP は標準 AP としての動作を停止して、一時的にクライアント モードに移行する必要があります。この動作によって、不正 AP がネットワーク上に実際に存在していることが確認され、その不正 AP のネットワーク上の論理的な場所を示す IP アドレス情報が提示されます。支社内のロケーション情報を取得する難しさと、マルチテナントの建物内で不正 AP が検出される可能性を組み合わせて考えると、Rogue AP Detector と RLDP はロケーション ベースの不正 AP 検出を強化する便利なツールです。

スイッチ ポート トレース

Cisco Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、*ネイバー リスト*にないフレームから検出された BSSID アドレスが記載されています。ネイバー リストには、確認済み AP または*ネイバー*の既知の BSSID アドレスが含まれます。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法では、Cisco Prime Infrastructure はコントローラから受け取った情報を単純に収集します。さらに、有線の不正アクセス ポイントのスイッチ ポートの自動または手動スイッチ ポート トレース（SPT）も組み込むことができます。自動 SPT は、大規模なワイヤレス ネットワークに適しています。

不正 AP が Cisco Prime Infrastructure に報告されると、自動 SPT が自動的に起動します。自動 SPT は、不正 AP の有線のロケーションの関連付けを基礎とする、より高速なスキャン方法です。トレースを実行し、回線上で検出された不正アクセス ポイントを封じ込められるようにするために、Cisco Prime Infrastructure を使用して、自動 SPT および自動封じ込めの基準を設定できます。

不正 AP を自動的に封じ込める必要があることを複数のコントローラが報告した場合、Cisco Prime Infrastructure は最も強い RSSI を報告したコントローラを検出し、そのコントローラに封じ込め要求を送信します。

不正 AP の封じ込め

不正 AP に接続されたクライアント、または不正なアドホックに接続されたクライアントは、近隣の AP から 802.11 認証解除パケットを送信することによって封じ込めることができます。近隣の WLAN 内にある正規の AP にこの作業を行うことは違法であるため、当該の AP が本当に不正 AP であることを確認する手順を行ってから作業する必要があります。不正 AP の自動封じ込め機能がソリューションから削除されたのは、これが理由です。

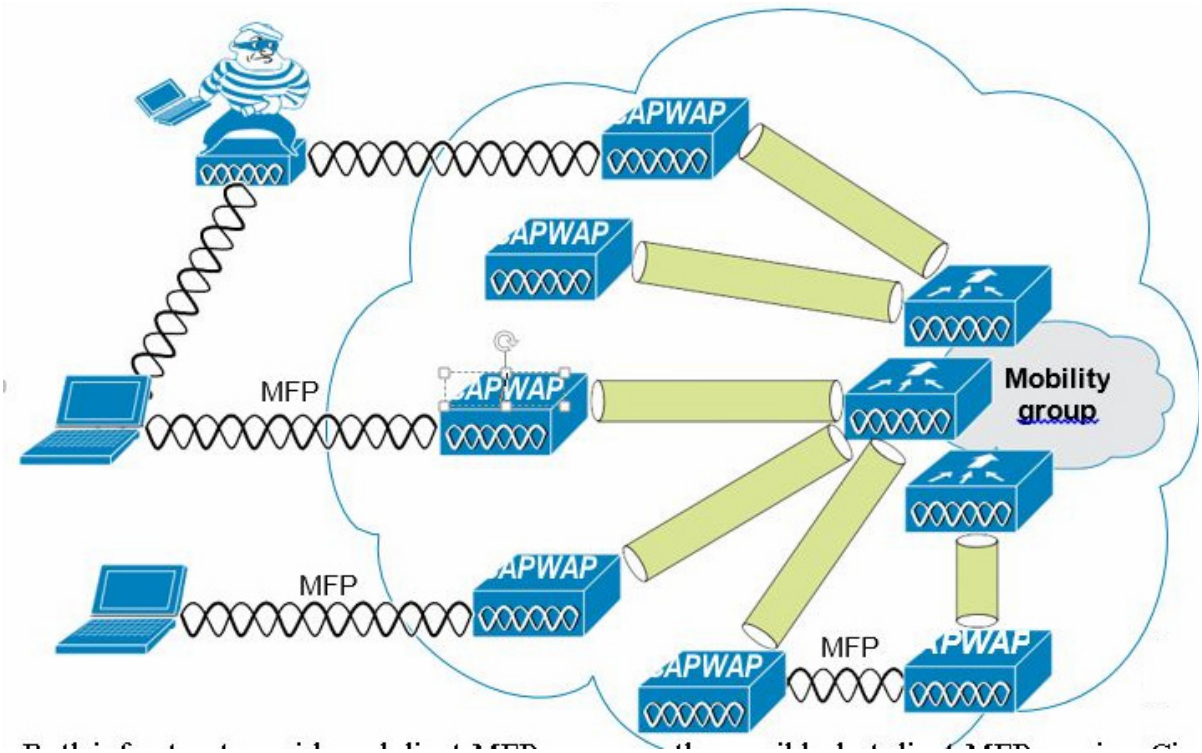
企業の WLAN にも不正 AP クライアントが存在するかどうかを判断するには、クライアントの MAC アドレスと、802.1X 認証中に AAA によって収集された MAC アドレスを比較します。これにより、改ざんされた可能性のある WLAN クライアントやセキュリティ ポリシーに従っていないユーザの識別が可能になります。

Management Frame Protection

802.11 の課題の 1 つは、暗号化や Message Integrity Check のない平文で管理フレームが送信され、そのためにスプーフィング攻撃に対して脆弱であるということです。WLAN 管理フレームのスプーフィングが WLAN ネットワークの攻撃に使用される可能性があります。この問題に対処するため、シスコでは 802.11 管理フレームに Message Integrity Check（MIC）を挿入するためのデジタル署名メカニズムを作成しました。これにより、WLAN の展開の正規のメンバーを識別できるほか、不正なインフラストラクチャ デバイスや、有効な MIC の不足によりスプーフィングされたフレームを識別できます。

Management Frame Protection（MFP）で使用される MIC は、メッセージの簡単な CRC ハッシュだけではなく、デジタル署名のコンポーネントも含みます。MFP の MIC コンポーネントによってフレームが改ざんされていないことが確認され、デジタル署名コンポーネントによって MIC が WLAN ドメインの正規メンバーによって生成されたことが確認されます。MFP で使用されるデジタル署名キーはモビリティ グループのすべてのコントローラ間で共有されます。したがって、異なるモビリティ グループのキーがそれぞれ異なるため、すべての WLAN 管理フレームはそのモビリティ グループ内の WLC によって検証できます（図 4-29）。

図 4-29　Management Frame Protection



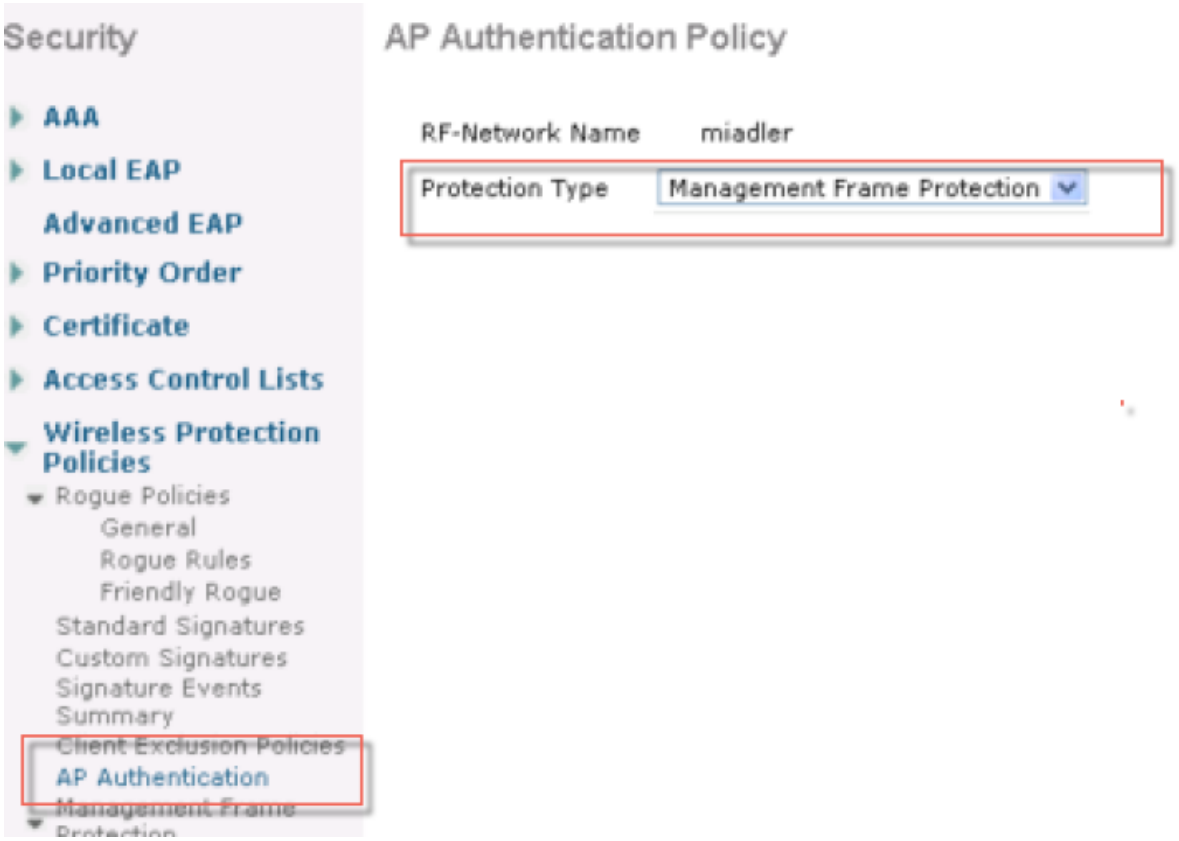
現在はインフラストラクチャ側とクライアント MFP の両方が可能ですが、クライアント MFP の場合は、Cisco Compatible Extensions v5 WLAN クライアントが、無効なフレームを検出および拒否する前にモビリティ グループの MFP キーを学習する必要があります。

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。
- 不正 AP や中間者攻撃の一部として検出されないように有効な AP MAC または SSID をスプーフィングする悪意のある不正の検出を可能にする。
- ソリューションの不正 AP と WLAN IDS シグニチャ検出の効率を上げる。
- Cisco Compatible Extensions v5 を使用するクライアント デバイスの保護を提供する。
- スタンドアロン AP でサポートされる。

MFP を有効にするには 2 つの手順が必要です。まず WLC の [Security] タブで MFP を有効にし（図 4-30）、モビリティ グループ内の WLAN で MFP を有効にします（図 4-26）。

図 4-30　コントローラでの MFP の有効化



Cisco TrustSec SXP

Cisco TrustSec を使用すると、組織はアイデンティティベースのアクセス コントロールを通じて、人、場所、時を問わずネットワークとサービスをセキュリティで保護できます。このソリューションでは、データの整合性および機密保持サービス、ポリシーベースの管理、中央集中型のモニタリング、トラブルシューティング、およびレポーティング サービスも提供されます。TrustSec をカスタマイズされたプロフェッショナル サービスと組み合わせると、ソリューションの導入と管理を簡素化できます。CTS は、Cisco ボーダレス ネットワークの基盤となるセキュリティ コンポーネントです。

Cisco TrustSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。Cisco TrustSec は、ネットワークに入るようにセキュリティ グループ（SG）がパケットを分類するために認証中に取得したデバイスおよびユーザ クレデンシャルを使用します。このパケット分類は、Cisco TrustSec ネットワークへの進入時にパケットにタグを付けることで維持されます。これにより、パケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグはセキュリティ グループ タグ（SGT）と呼ばれ、エンドポイント デバイスはこの SGT に基づいてトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。Cisco TrustSec セキュリティ グループ タグは WLAN の AAA オーバーライドを有効にする際にだけ適用されます。

Cisco TrustSec アーキテクチャのコンポーネントの 1 つが、セキュリティ グループベースのアクセス コントロールです。セキュリティ グループ ベースのアクセス コントロール コンポーネントで、Cisco TrustSec ドメインのアクセス ポリシーは、トポロジとは無関係で、ネットワーク アドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティ グループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティ グループ番号のタグが付けられます。

Cisco デバイスは SGT 交換プロトコル（SXP）を使用して、Cisco TrustSec 向けのハードウェア サポートがないネットワーク デバイスに SGT を伝播します。SXP は、すべてのスイッチで CTS ハードウェアがアップグレードされるのを防ぐためのソフトウェア ソリューションです。WLC では、TrustSec アーキテクチャの一部として SXP がサポートされます。SXP は、CTS 対応のスイッチに SGT 情報を送信します。SGT で示されたロール情報に従って、適切なロールベース アクセス コントロール リスト（RBACL）をアクティブにすることができます。デフォルトでは、コントローラは常にスピーカー モードで動作します。ネットワーク上で SXP を実装するには、出口のディストリビューション スイッチのみを CTS 対応にすればよく、他のすべてのスイッチは CTS 非対応でかまいません。

SXP は、任意のアクセス レイヤとディストリビューション スイッチ間、または 2 つのディストリビューション スイッチ間で動作します。SXP は TCP をトランスポート層として使用します。アクセス レイヤ スイッチ上でネットワークに join している任意のホスト（クライアント）に対する CTS-enabled 認証は、CTS 対応ハードウェアを備えたアクセス スイッチの場合と同様に実行されます。アクセス レイヤ スイッチは CTS 対応ハードウェアではありません。したがって、データ トラフィックがアクセス レイヤ スイッチを通過するとき、そのトラフィックの暗号化または暗号による認証は行われません。SXP は、認証されたデバイス（つまりワイヤレス クライアント）の IP アドレスと、対応する SGT をディストリビューション スイッチに渡すために使用されます。ディストリビューション スイッチが CTS 対応ハードウェアの場合は、そのディストリビューション スイッチがアクセス レイヤ スイッチに代わってパケットに SGT を挿入します。ディストリビューション スイッチが CTS 対応ハードウェアでない場合は、ディストリビューション スイッチの SXP が、CTS ハードウェアを備えたすべてのディストリビューション スイッチに IP-SGT マッピングを渡します。出口側では、ディストリビューション スイッチの出力 L3 インターフェイスで RBACL が適用されます。

次に、Cisco TrustSec SXP に関するガイドラインをいくつか示します。

- SXP は次のセキュリティ ポリシーでのみサポートされます。
  - WPA2-dot1x
  - WPA-dot1x
  - 802.1x（Dynamic WEP）
  - RADIUS サーバを使用した MAC フィルタリング
  - RADIUS サーバを使用した Web 認証によるユーザ認証

- SXP は IPv4 クライアントと IPv6 クライアントの両方でサポートされます。
- コントローラは常にスピーカー モードで動作します。

詳細については、『Cisco TrustSec』を参照してください。

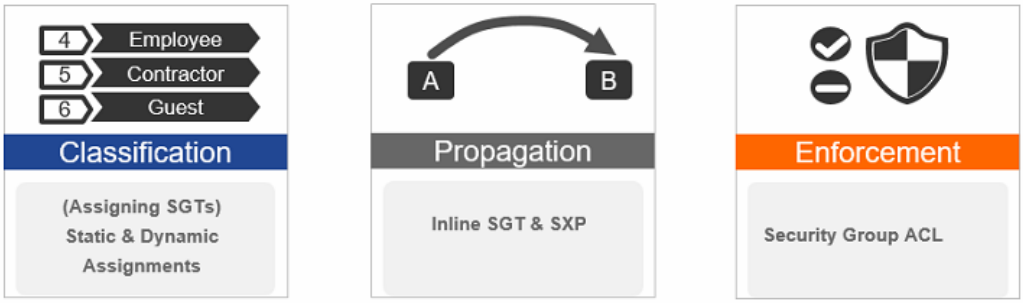
Cisco TrustSec SXP の制約事項

- SXP は FlexConnect アクセス ポイントではサポートされません。
- SXP がサポートされるのは、中央認証を使用し、中央でスイッチされるネットワークだけです。
- デフォルトでは、SXP はローカル モードのみで動作する AP 向けにサポートされています。
- デフォルト パスワードの設定は、コントローラとスイッチの両方で一致している必要があります。
- 耐障害性は AP でのローカル スイッチングが必要になるため、この機能はサポートされません。
- ユーザをローカル認証するための静的 IP-SGT マッピングはサポートされません。
- IP-SGT マッピングでは、外部 ACS サーバを使用した認証が必要です。
- 自動アンカー/ゲスト アンカー モビリティでは、RADIUS サーバから外部 WLC に渡された SGT 情報を EoIP/CAPWAP モビリティ トンネル経由でアンカー WLC に通信できます。その後、アンカー WLC は、SGT-IP マッピングを構築し、SXP を介して別のピアに伝達できます。

リリース 8.4 の WLC 上の Cisco TrustSec（CTS）

Cisco TrustSec（CTS）アーキテクチャを使用すると、各エンティティがそのネイバーによって認証および信頼され、データの機密性、信頼性、および整合性の保護に役立つセキュアな通信リンクが確立される、エンドツーエンドのセキュア ネットワークを構築できます。また CTS では、ネットワーク全体での一貫性のある統合された一連のポリシーの作成が促進されます。以下の項では、AireOS WLC の CTS インフラストラクチャのサポートに関連する具体的な側面について説明します。

実装



TrustSec ドメインに接続するエンド ポイントはすべて、ISE によってロール、デバイス タイプ（その他のクライアント属性）などのエンド ユーザ ID に基づいて分類され、SGT（セキュリティ グループ タグ）と呼ばれる一意のタグに関連付けられます。このタグは、認証成功時にクライアント認証を要求したデバイスと共有されます。これにより、クライアント ID 属性に基づいてクライアントをグループ化し、アクセス コントロール エンティティ（ACE）の数を大幅に削減できます。SGACL を使用する主な利点は、アクセス ACE の統合とこれらの従来のアクセス リストのメンテナンスに付随する運用コストの削減です。

TrustSec ソリューションは、TrustSec ドメイン内の 3 つの異なるフェーズにわたって実現されます。

a. **クライアント分類**：クライアントは、入口で中央集中型ポリシー データベース（ISE）によって分類され、ロールなどのクライアント ID 属性に基づいて一意の SGT が割り当てられます。
b. **伝達**：IP と SGT のバインディングは、SXPv4 またはインライン タギング手法を使用して伝達されます。
c. **SGACL ポリシーの適用**：AP は、セントラル/ローカル スイッチング（セントラル認証）のエンフォースメント ポイントになります。

AP 上の SXPv4

WLC は、引き続き SXPv2 スピーカー モードをサポートし、IP と SGT のバインディングをネイバー デバイスに伝達します。SXPv4 はサポートされません。AP は、SXPv4 リスナー モードとスピーカー モードをサポートします。

CTS PAC プロビジョニングおよびデバイス登録

CTS ネットワークに参加しているすべてのデバイスは、認証され、信頼される必要があります。認証プロセスを促進するために、CTS ネットワークに接続された新しいデバイスは、デバイス内で CTS のデバイスの認証に特に必要であるクレデンシャルと、一般的な CTS 環境情報を取得するための登録プロセスを経なければなりません。

WLC のデバイス登録は、ISE サーバによる PAC プロビジョニングの一部として、WLC によって開始されます。WLC は、EAP-FAST が開始し、PAC を取得します。これには、LOCAL-EAP EAP-FAST PAC プロビジョニングのインフラストラクチャが使用されます。取得した PAC はデバイス ID に一意にマッピングされます。デバイス ID を変更すると、以前のデバイス ID に関連付けられた PAC データが PAC ストアから削除されます。PAC のプロビジョニングに使用する RADIUS サーバ インスタンスが有効になると、PAC プロビジョニングがトリガーされます。

高可用性（HA）設定の場合、PAC はスタンバイ ボックスに同期されます。

環境データ

CTS 環境データとは、デバイスが CTS 関連機能を実行するための一連の情報または属性を指します。

セキュアな RADIUS アクセスリクエストが送信されて、デバイスが Cisco TrustSec ドメインに初めて参加するときに、デバイス（AirOS WLC）は認証サーバから環境データを取得します。認証サーバは、環境有効期間終了タイムアウト属性などの属性とともに RADIUS Access-Accept を返します。これは、Cisco TrustSec デバイスがその環境データを更新する必要がある頻度を制御する時間間隔になります。

インライン タギング

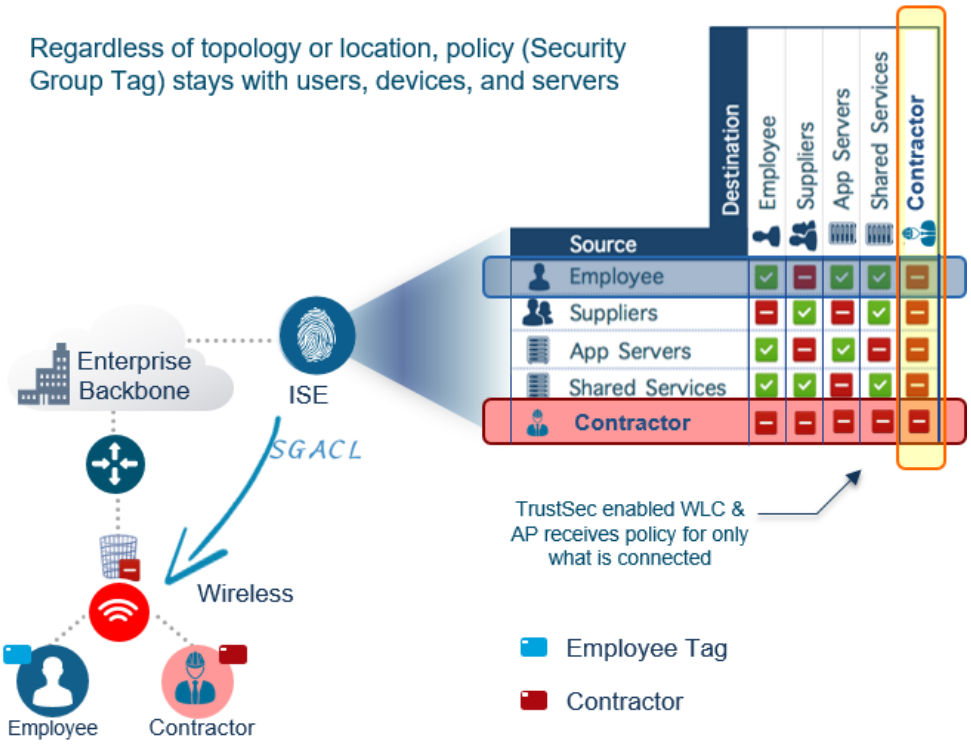
インライン タギング機能は、コントローラまたはアクセス ポイントが送信元 SGT（S-STG）を理解するために使用するトランスポート メカニズムです。次の 2 つのタイプが対象になります。

- セントラル スイッチング：中央でスイッチングされるパケットの場合、WLC は、WLC 上のワイヤレス クライアントから送信されたすべてのパケットに対し、Cisco メタ データ（CMD）タグを付けることによってインライン タギングを実行します。DS から受信するパケットに対するインライン タギングでは、WLC はさらに、パケットからヘッダーを除去し、AP が S-SGT タグを学習できるように CAPWAP を介してパケットを AP に送信します。SGACL は AP で適用されます。
- ローカル スイッチング：ローカルにスイッチングされるパケットの場合、AP は、AP 上のクライアントから送信されたパケットに対してインライン タギングを実行します。トラフィックを受信すると、AP はローカルにスイッチングされるパケットと中央でスイッチングされるパケットの両方を処理し、パケットの S-SGT タグを使用して SGACL ポリシーを適用します。

WLC でワイヤレス TrustSec が有効になっている場合は、オプションで SXP を有効にしてスイッチとタグを交換するように設定することもできます。また、SXP スピーカー モードとインライン タギングの両方のモードがサポートされます。ただし、AP で SXP とワイヤレス TrustSec の両方を同時に有効にすることはできません。

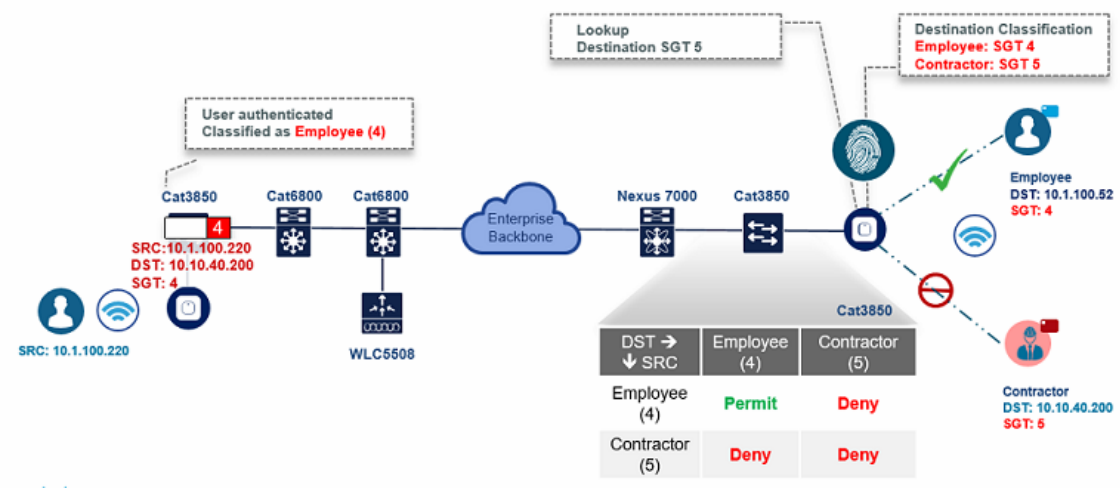
ワーク フロー

WLC は、ISE から SGACL ポリシーのダウンロードする前に、EAP-FAST TLS トンネルを介して PAC（Protected Access Credential）プロビジョニングを開始する必要があります。これは、認証されたクライアントの SGT タグに基づいて必要な SGACL をダウンロードするために使用されます。現在、ISE では、すべての既知の送信元 SGT（S-SGT）からの任意の宛先 SGT（D-SGT）について、SGACL ポリシーのダウンロードがサポートされます。ワイヤレス クライアントが ISE によって認証されると、WLC はクライアントに関連付けられている SGT を受け取ります。WLC はクライアント SGT を D-SGT として処理し、接続先の SGACL ポリシー名を ISE からダウンロードします。返されるポリシー名は、特定のクライアント D-SGT と対になったすべての有効かつ既知の S-SGT になります。D-SGT に関連付けられているこれらのポリシーは、WLC にキャッシュされ、クライアントがアソシエートしている AP にプッシュされます。



クライアントは、入り口で中央集中型ポリシー データベース（ISE）によって分類され、ポリシー ルールに従ってクライアント ID に基づいて一意の S-SGT が割り当てられます。出口側では、SGACL がダウンロードされ、D-SGT に関連付けられたポリシーが適用されます。

1. ローカルおよびセントラル スイッチ トラフィックに対する SGACL は、WLC でなく AP で適用されます。
2. ローカル認証を行うフレックス モード AP では、エンフォースメント ポイントは AP になります。



WLC 8.4 上の ワイヤレス TrustSec サポート

表 4-2

機能	プラットフォーム
SGT インライン タギング、SG-ACL 適用	AP 17xx、27xx、37xx、18xx、28xx、38xx WLC 3504、5520、8540
SXPv2	AP 17xx、27xx、37xx、18xx、28xx、38xx WLC 3504、5520、8540
SXPv4	AP 17xx、27xx、37xx、18xx、28xx、38xx、WLCs 3504、5520、および 8540

管理システムのセキュリティ機能

不正 AP 検出に対するロケーション機能のサポート以外に、管理システム Cisco Prime には Unified Wireless Network セキュリティに関する 2 つの機能があります。1 つは WLC 設定の確認管理、もう 1 つはアラームおよびレポート発行インターフェイスです。

設定の確認

管理システム Cisco Prime には設定の監査レポートをオンデマンドまたは定期的に発行する機能があります。このレポートでは、WLC および登録済みのアクセスポイントの現在稼働している完全な設定と、管理システム Cisco Prime データベースに保存されている既知の有効な設定を比較します。現在稼働している設定と保存されているデータベース設定の間にある例外が明記され、画面のレポートを介してネットワーク管理者に通知されます（図 4-30）。

アラームおよびレポート

WLC から直接生成され、エンタープライズ ネットワーク管理システム Cisco Prime に送信できるアラームのほか、管理システムではアラーム通知の送信も可能です。さまざまなコンポーネントによって送信されるアラームのタイプとは別に、アラーム通知方法の主な違いは、WLC が Simple Network Management Protocol（SNMP）のトラップを使用してアラーム（NMS システムでしか解釈できない）を送信する一方で、管理システム Cisco Prime は SMTP 電子メールを使用して管理者にアラーム メッセージを送信することです。

管理システム Cisco Prime ではリアルタイムのレポートと定期的なレポートが提供されます。これらのレポートはエクスポートや電子メールによる送信が可能です。管理システム Cisco Prime から提供されるレポートの内容は次のとおりです。

- アクセス ポイント
- 監査
- クライアント
- インベントリ

- Mesh
- パフォーマンス
- セキュリティ

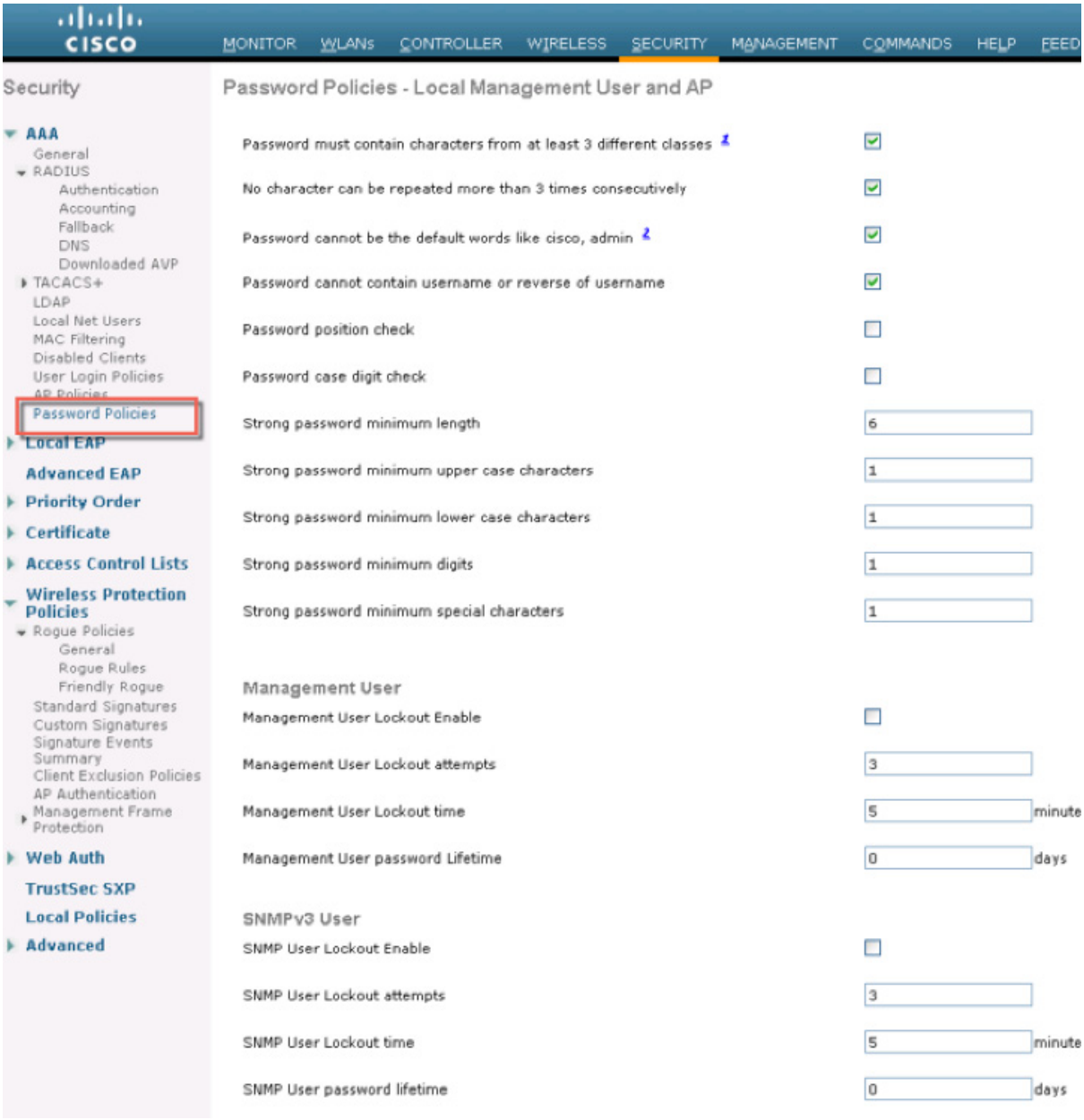
パスワード ポリシー

パスワード ポリシーを使用すると、管理者は、コントローラおよびアクセス ポイントの追加管理ユーザ用に新しく作成されたパスワードに対し、強力なパスワード チェックを適用できます。新規パスワードには次の要件が適用されます。

- コントローラが旧バージョンからアップグレードされた場合、古いパスワードはすべて現状のまま維持されます。ただし、パスワードの強度は低下します。システムのアップグレード後、強力なパスワード チェックが有効になると、それ以降は強力なパスワード チェックが適用され、以前に追加されたパスワードの強度のチェックまたは変更は行われません。
- [Password Policy] ページで設定された内容によっては、ローカル管理、アクセス ポイント、管理ユーザ、および SNM3 ユーザの設定が影響を受けます。

図 4-31 では、ローカル管理ユーザ、AP、管理ユーザ、および SNMPv3 ユーザのパスワード ポリシーを示します。

図 4-31　　パスワード ポリシー：ローカル管理ユーザおよびAP



Cisco Unified Wireless QoS、AVC および ATF

この章では、WLAN 実装のコンテキストでの Quality of Service（QoS）、Application Visibility and Control（AVC）、Airtime Fairness（ATF）について説明します。この章では、WLAN QoS および AVC 全般について説明します。セキュリティやセグメンテーション、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。

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、特定のネットワーク トラフィックに対して、さまざまなネットワーク テクノロジーを介して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機能のことです。QoS テクノロジーには次のような利点があります。

- キャンパス、WAN、およびサービス プロバイダー 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構成要素を提供します。
- ネットワーク マネージャが、ネットワーク ユーザとのサービス レベル契約（SLA）を規定できます。
- ネットワーク リソースをより効率的に共有でき、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。
- 時間的に制約がある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、LAN および WAN 全体の帯域幅をより効率的に管理できます。QoS により、次の点で強化された信頼性の高いネットワーク 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の専用帯域幅のサポート
- ジッタおよび遅延の制御（リアルタイム トラフィックに必要）
- ネットワークの輻輳の管理と最小化
- トラフィック フローをスムーズにするネットワーク 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

ワイヤレス QoS の導入スキーム

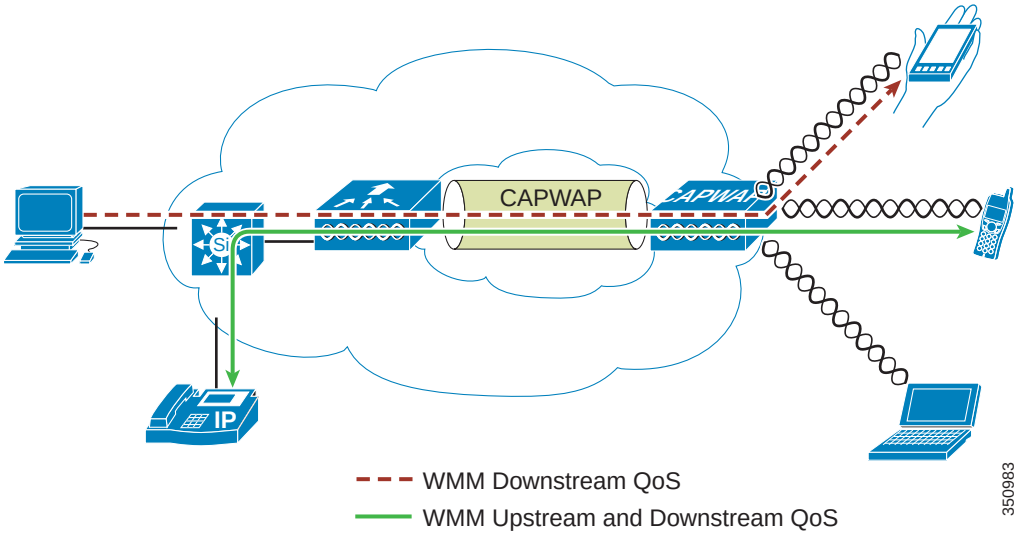
従来、WLAN は主に低帯域幅のデータ アプリケーション トラフィックの伝送に使用されていました。現在では、WLAN は特定業種（小売、金融、教育など）および企業環境に拡張され、時間に制約があるマルチメディア アプリケーションとともに、高帯域幅のデータ アプリケーションを伝送するために使用されています。この要件に対応するために、ワイヤレス QoS が必要になりました。

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ワイヤレス QoS 方式をサポートしています。QoS の導入速度を高め、複数のベンダーの時間に制約のあるアプリケーションに対応するには、ワイヤレス QoS に対する統一されたアプローチが必要です。IEEE 802.11 標準化委員会内の IEEE 802.11e ワーキング グループは標準の定義を完了し、802.11e 標準の採用も完了されています。多くの標準と同様に、多くのオプション コンポーネントがあります。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、認証プログラムによって主要な機能と相互運用性を実現できるよう、WMM プログラムおよび Cisco Compatible Extensions プログラムを通じて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 が公開した 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 では、Cisco Unified Wireless テクノロジーの機能に基づくワイヤレス QoS の導入例を示します。

図 5-1　　QoS の導入例



QoS パラメータ

QoS は、伝送品質およびサービスの可用性を反映した伝送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 を正しく実装するには、ネットワーク インフラストラクチャの可用性が高くなければなりません。

ネットワークの伝送品質は、遅延、ジッター、および損失で決まります（表 5-1 を参照）。

表 5-1　QoS の伝送品質

要素	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。この時間はエンドツーエンド遅延と呼ばれ、2 つの領域に分けられます。 • 固定ネットワーク遅延：符号化および復号化の時間（音声およびビデオの場合）、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宛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（または遅延変動）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、あるパケットが送信元エンドポイントから宛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 必要であり、次のパケットは同じ伝送に 125 ms 必要である場合、ジッターは 25 ms となります。
損失	損失（パケットの損失）は、伝送されたパケット総数に対する、正常に送受信されたパケット数の比較基準です。損失は、ドロップされたパケットの割合で表されます。

無線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*無線ダウンストリーム* QoS の定義を示しています。

図 5-2　アップストリーム QoS とダウンストリーム QoS

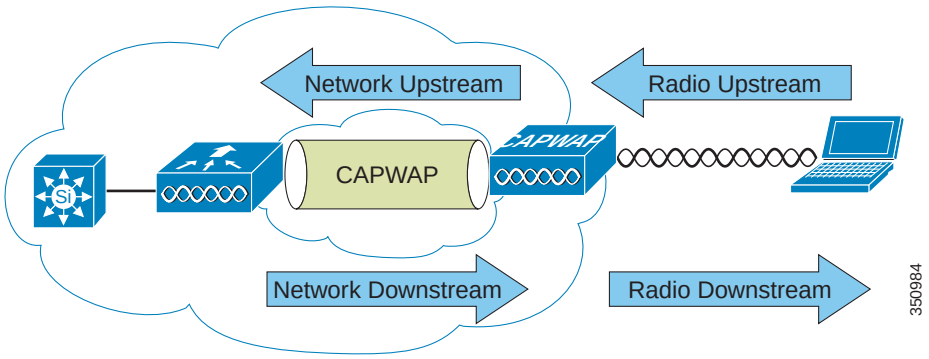


図 5-2 は、以下のことについて示しています。

- *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 が今でも最も一般的な展開であるため、この章の最重要点となっています。無線クライアントのアップストリーム QoS は、クライアントの実装に依存しています。
- *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*: ワイヤレス LAN コントローラ（WLC）から発信され、AP まで伝送されるトラフィック。このポイントで QoS が適用され、AP へのトラフィックの優先度付けおよびレート制限を行うことができます。

（注）　*イーサネットのダウンストリーム* QoS の設定は、本書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、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 ネットワークへ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簡単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、ジッター、および損失が顕著な場合、それはシステム障害や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、ジッター、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えると、アプリケーションのパフォーマンスへの QoS 機能の適用が始まります。QoS は、選択されたトラフィック タイプの遅延、ジッター、および損失を、妥当な範囲内に維持しようとします。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して処理されます。クライアントは、アップストリーム伝送において他のクライアントと競合し、AP からのベスト エフォート伝送とも競合します。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 の影響を受けやすいアプリケーションのパフォーマンスが許容できないほど低下することがあります。理想的には、アップストリーム QoS およびダウンストリーム QoS を操作するためには 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 クライアントにおける WMM のサポートは、クライアント トラフィックが WMM から自動的にメリットを得ているという意味ではありません。WMM のメリット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 ハンドセット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。ただし、PC のような汎用的なプラットフォームに実装する場合は、アプリケーションのトラフィック分類と OS によるサポートがないと、WMM 機能の効果が望めません。

WLAN クライアント上で WMM のサポートがなくても、Cisco Unified Wireless Network 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。

802.11 Distributed Coordination Function

802.11 のデータ フレームは、Distributed Coordination Function（DCF）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、DIFS などを含む IFS。詳細は後述）
- ランダム バックオフ（競合ウィンドウ）。

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）を展開するには、DCF の基本的な理解が必要です。DCF の詳細については、次の Web ページで IEEE 802.11 の仕様を参照してください。

http://www.ieee802.org/11/

これらの 802.11 DCF コンポーネントについては、以降のセクションで詳しく説明します。

フレーム間スペース

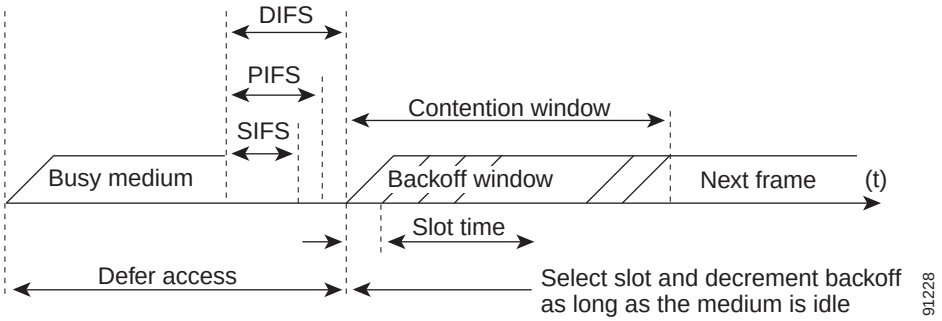
802.11 標準では、フレーム間スペース（IFS）を次のように定義しています。

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

（注）　図 5-3 で示した IFS の例で使用しているベース タイミングは、802.11b の場合のものです。802.11g と 802.11a のタイミングは異なりますが、適用する原則は同じです。

IFS では、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 の管理フレームと競合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 を参照）。

図 5-3　フレーム間スペース



ランダム バックオフ

DCF のデータ フレームが送信可能になると、DCF は次の手順で処理を行います。

1. 0 から最小競合ウィンドウまでの範囲のランダム バックオフ番号を生成します（aCWmin、aCWmax および再試行（5-7 ページ）を参照）。
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は、チャネルが空いているスロット時間（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. ステーションが 0 に達した場合など、チャネルが使用中になると、デクリメントを停止し、手順 2 ～ 3 を繰り返します。
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たままであれば、フレームを送信できます。

図 5-4 は、DCF プロセスが動作する様子を示した簡単な例です。この DCF プロセスでは、確認応答は示されず、フラグメンテーションは発生しません。

図 5-4　Distributed Coordination Function（DCF）の例

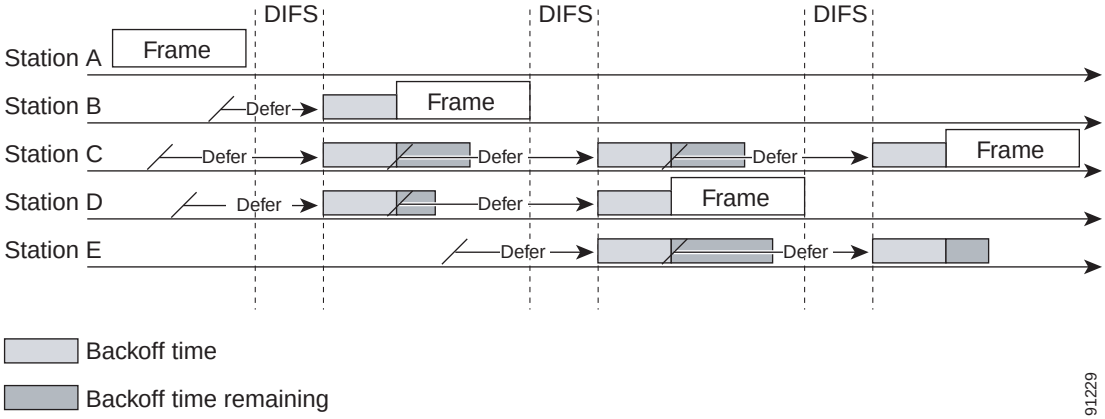


図 5-4 で示している DCF の手順は次のとおりです。

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 つの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さらに DIFS の間待機する必要があります。
3. 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、スロット時間ごとに 1 回ずつバックオフ カウンタのデクリメントを開始します。
4. 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 より先に 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。
5. 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 が経過するまで待機する必要があります。
6. 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 が送信中であるため、ステーション C および D と同様に待機する必要があります。
7. ステーション B が送信を完了し、DIFS が経過すると、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。

トラフィックが別のステーションに到達すると、このプロセスが続行されます。

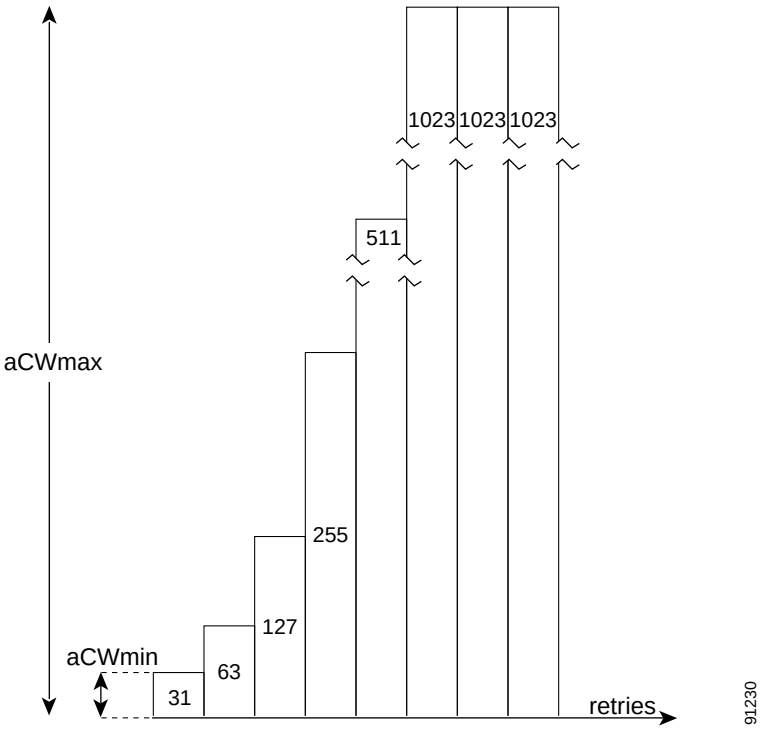
aCWmin、aCWmax および再試行

DCF は競合ウィンドウ（CW）パラメータを使用して、ランダム バックオフのサイズを制御します。CW は、次のパラメータで定義されます。

- aCWmin：最小競合ウィンドウ
- aCWmax：最大競合ウィンドウ

ランダム バックオフで使用されるランダム番号は、最初は 0 ～ aCWmin です。最初のランダム 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分し、ランダム バックオフ ウィンドウのサイズを 2 倍にします。このサイズの倍増は、サイズが aCWmax と等しくなるまで続行されます。再試行は、最大再試行回数または存続可能時間（TTL）に達するまで続行されます。バックオフ ウィンドウを倍増させ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。詳しくは図 5-5 で示します。ここでは、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 実装に対するものです。別の物理層の実装では、値が異なる場合があります。

Wi-Fi マルチメディア

ここでは、Wi-Fi マルチメディア（WMM）に関する次の 3 つの重要なトピックについて説明します。

- WMM のアクセス
- WMM の分類
- WWM キュー

WMM のアクセス

WMM は、802.11e ドラフトの機能セットをサポートする Wi-Fi Alliance 認定です。この認定はクライアントと AP の両方を対象にしており、WMM の動作を認定します。WMM は基本的に、802.11e の EDCA コンポーネントの実装です。新しく追加される Wi-Fi 認定では、802.11e の他のコンポーネントへの対応も予定されています。

WMM の分類

WMM では 802.1P 分類方式（IEEE 802.1D MAC ブリッジ標準の一部）が使用されています。この分類方式には 8 つの優先度があり、WMM ではこれが次の 4 つのアクセス カテゴリにマッピングされます。

- AC_BK：バックグラウンド
- AC_BE：ベスト エフォート
- AC_VI：ビデオ
- AC_VO：音声

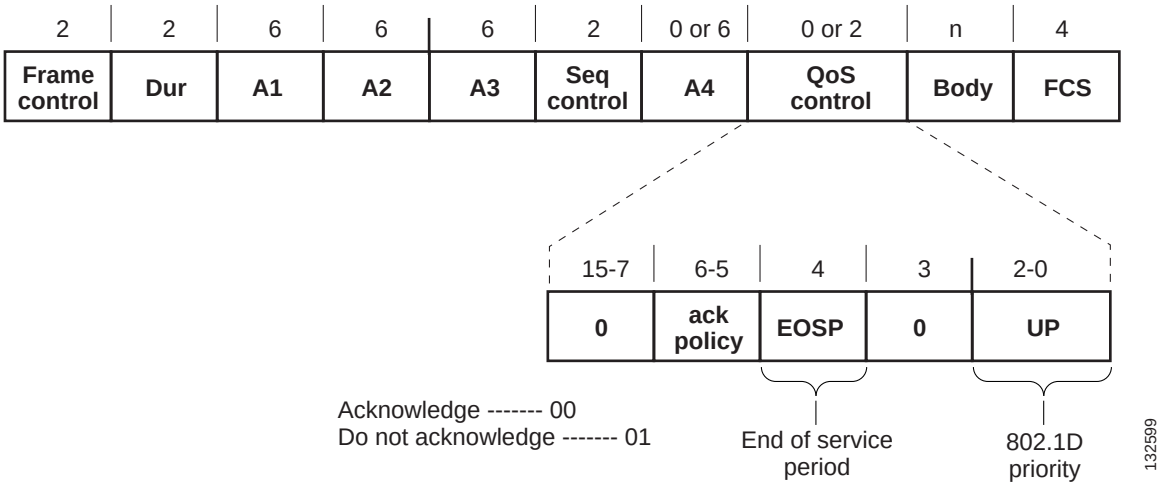
表 5-2 で示すように、これらのアクセス カテゴリは WMM デバイスに必要な 4 つのキュー（WMM キュー（5-9 ページ）を参照）にマッピングされます。

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 での名称	アクセス カテゴリ_WMM の指定
最低	1	BK	AC_BK
	2	-	
	0	BE	AC_BE
	3	EE	
	4	CL	AC_VI
	5	VI	
	6	VO	AC_VO
高品質	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ることに注意してください。

図 5-6　WMM のフレーム形式



WMM および IEEE 802.11e の分類は、Cisco Unified Wireless Network で推奨および使用されている、IETF 勧告に基づく分類とは異なります。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 のユーザ プライオリティ（UP）に変更している点です。これにより、分類 6 をレイヤ 3 ネットワークの制御に使用できます。両方の標準に準拠するため、Cisco Unified Wireless Network ソリューションでは、トラフィックがワイヤレスと有線の境界を横切る際に、さまざまな分類標準間の変換が実行されます。

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。アクセス カテゴリごとに 1 つずつ、4 つに分けられたキューが存在します。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。このとき、各キューには異なる IFS、aCWmin、および aCWmax の値が使用されます。異なるアクセス カテゴリの複数のフレームが内部で競合した場合は、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外部フレームと競合したときのように自身のバックオフ パラメータをキューイング メカニズムに合わせて調整します。このシステムは、Enhanced Distributed Channel Access（EDCA）と呼ばれています。

図 5-7　　WMM キュー

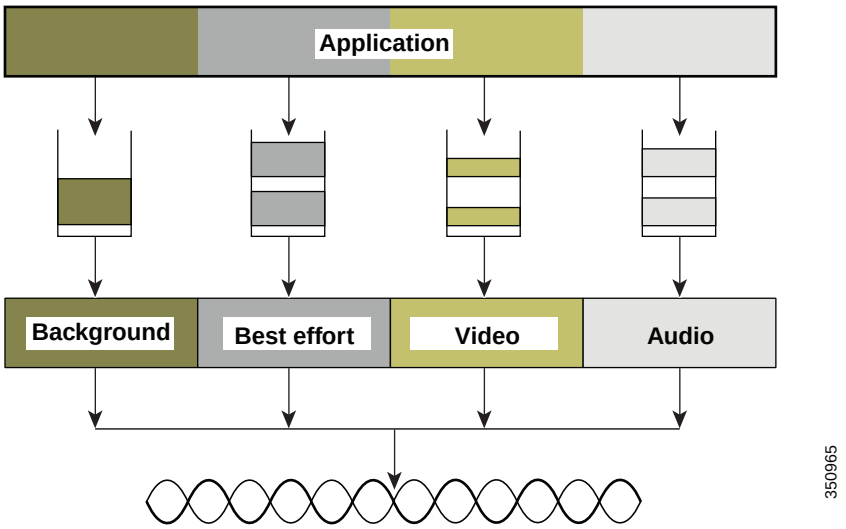
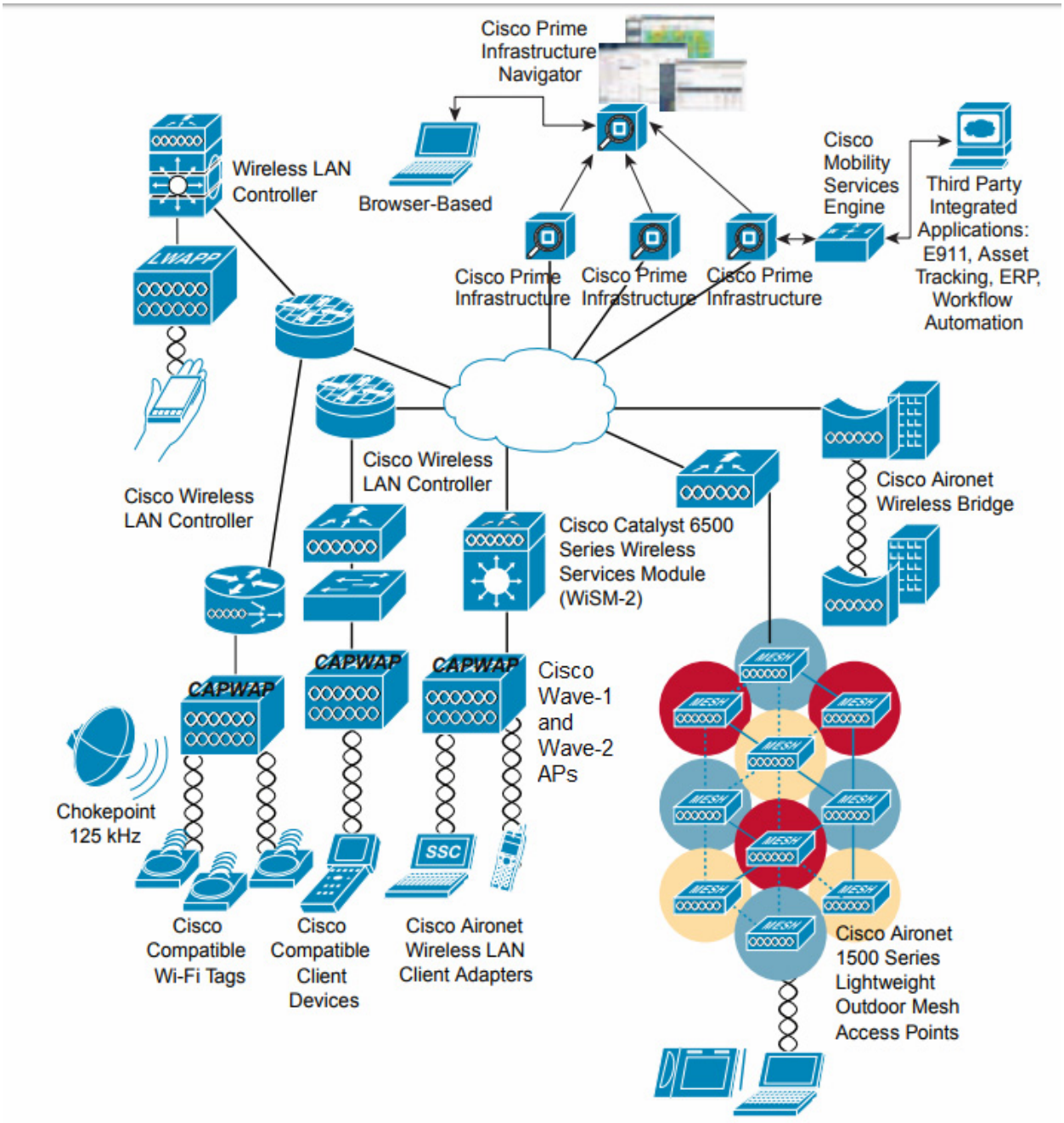


図 5-8 は、EDCF の背後の原則を示しています。ここでは、異なるフレーム間スペースと aCWmin および aCWmax の値が、トラフィックの分類ごとに適用されています（明確にするため aCWmax は示されていません）。トラフィック タイプが異なると、ランダム バックオフをカウント ダウンする前に別の IFS を待機させることができます。ランダム バックオフ番号の生成に使用される aCW 値も、トラフィックの分類によって異なります。たとえば、音声の aCWmin[3] は 23 - 1 で、ベスト エフォート トラフィックの aCWmin[5] は 25 - 1 です。優先度が高いトラフィックでは IFS が小さく aCWmin 値も小さいため、ランダム バックオフが短くなりますが、一方ベストエフォート トラフィックでは IFS が長く aCWmin 値も大きくなるため、ランダム バックオフ数が平均して大きくなります。

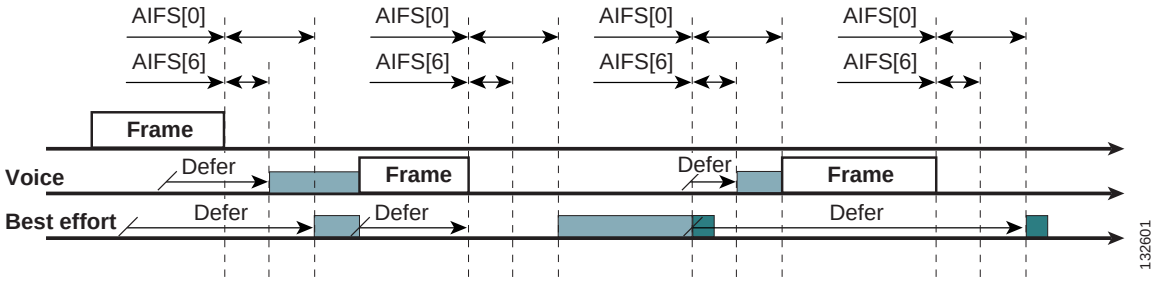
図 5-8　　アクセス カテゴリのタイミング



Enhanced Distributed Channel Access

図 5-9 は、Enhanced Distributed Channel Access（EDCA）のプロセスの例を示しています。

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 つのステーションがフレームを送信する必要があると判断します。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. 音声のステーションには音声のトラフィック分類があるため、2 の*調停フレーム間スペース*（AIFS）があり、3 の初期 aCWmin 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 のスロット時間です。ランダム バックオフ値も短くなります。
3. ベスト エフォートの aCWmin 値は 5 なので、ベスト　エフォートのステーションには 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. 音声のステーションのランダム バックオフ タイムが最短であるため、ここが最初に送信を開始します。音声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. 音声の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 ステーションがランダム 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音声のステーションがある場合でも、この動作が発生します。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、音声トラフィックによってベスト エフォート トラフィックが漸減しないこと、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、このプロセスが続行されます。

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 無線と同じで、WMM で定義されている式に基づいています。

（注）　表 5-3 に、クライアントのパラメータ設定を示します。この設定は、AP の設定とは若干異なります。AP では、音声およびビデオのアドミッション制御（AC）に対する AIFS[n] が大きくなります。

表 5-3　WMM クライアント パラメータ

AC	CWmin	aCWmax	AIFS[n]	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_BK	CWmin	aCWmax	7	[0]	0
AC_BE	CWmin	4 X（aCQmin + 1）- 1	3	[0]	0
AC_VI	（CWmin + 1）/2 - 1	CWmin	1	6.016 ms	3.008 ms
AC_VO	（CWmin + 1）/4 - 1	（CWmin + 1）/2 - 1	1	3.264 ms	1.504 ms

表 5-4　WMM AP パラメータ

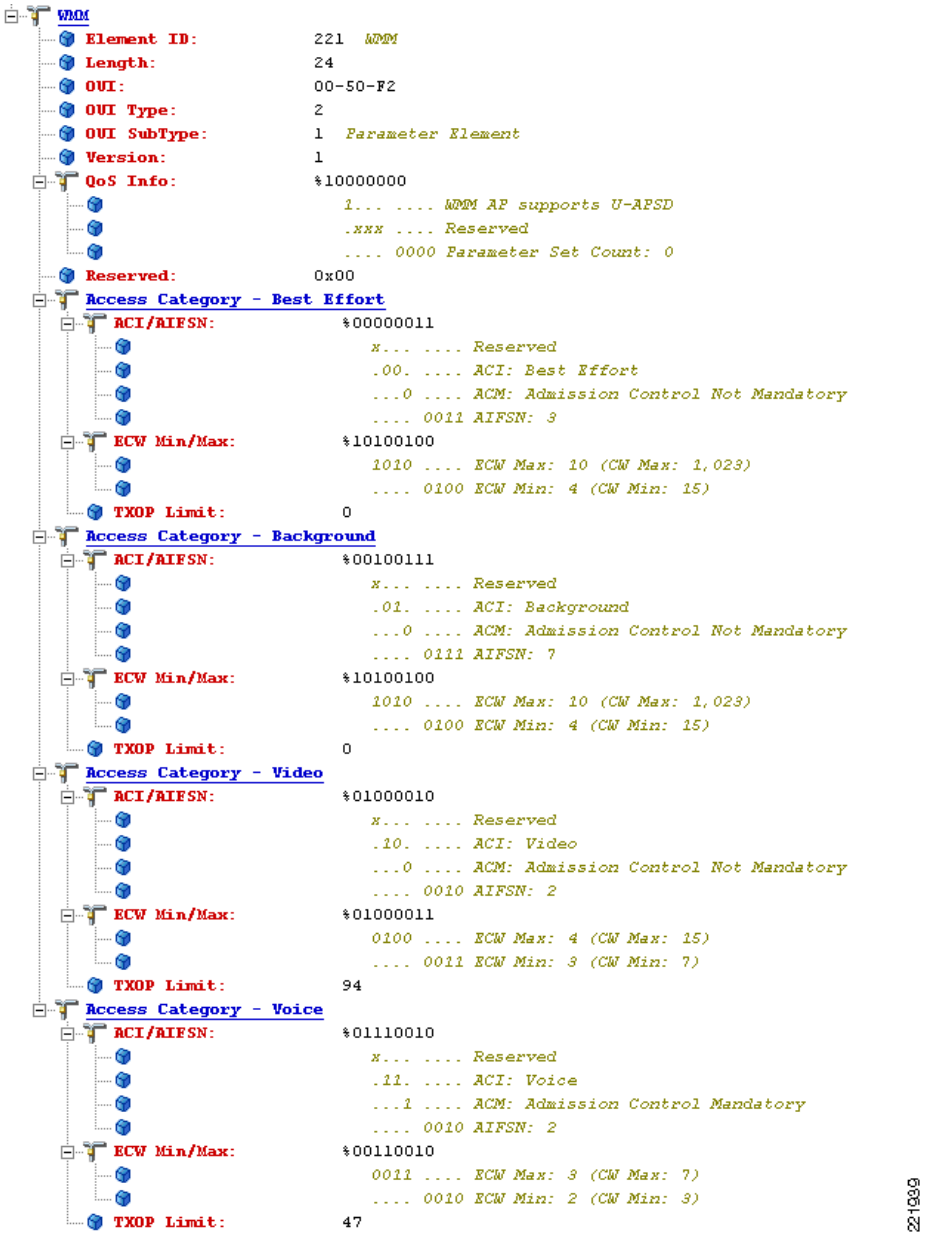
アクセス カテゴリ	CWmin	aCWmax	AIFS[n]	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_BK	CWmin	aCWmax	7	[0]	0
AC_BE	CWmin	4 X（aCQmin + 1）- 1	3	[0]	0
AC_VI	（CWmin + 1）/2 - 1	CWmin	2	6.016 ms	3.008 ms
AC_VO	（CWmin + 1）/4 - 1	（CWmin + 1）/2 - 1	2	3.264 ms	1.504 ms

異なる AIFS、CWmin、および aCWmax の値が全体に及ぼす影響は、その影響が本来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）。

例として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。フレームを送信するまでの平均の遅延は、音声フレームでは 5（2 + 7/1）スロット時間、バックグラウンド フレームでは 22（7 + 31/2）スロット時間です。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強くなります。

図 5-10 では、プローブ応答内の WMM 情報を示します。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。この例で示すとおり、音声アドミッション制御（AC）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、この章で後述します。

図 5-10　　プローブ応答の WMM 要素情報



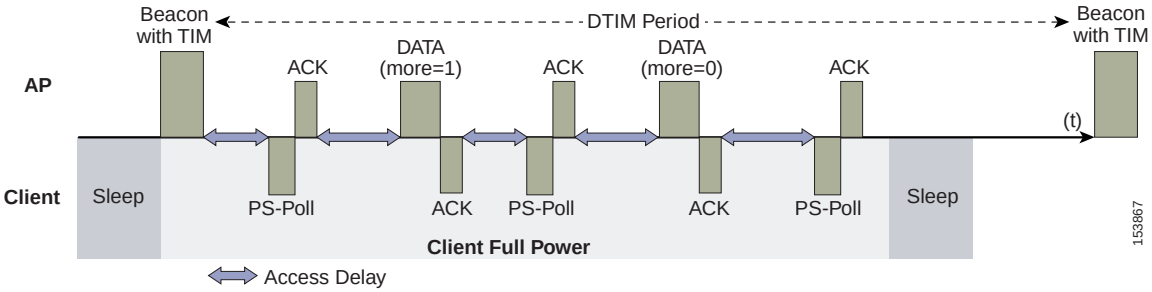
不定期自動省電力配信

不定期自動省電力配信（U-APSD）は、次の 2 つの主要な特長を持つ機能です。

- 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できることです。そのため、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 カテゴリ内で WLAN クライアントからフレームが送信されると、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）ビットが設定されたフレームを受信するまで、AP をリッスンし続けます。EOSP ビットによって、省電力モードに戻れることがクライアントに通知されます。このトリガー メカニズムでは、Delivery Traffic Indication Message（DTIM）の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も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。それは、音声の遅延要件とジッター要件により、無線 VoIP 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るか、DTIM 間隔が短くなり、結果として待機時間が短縮されてしまうためです。U-APSD を使用すれば、長い 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 を適用しつつ、他の AC では標準の省電力モード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と、WLAN クライアントから取り込んだトリガー データ フレームを組み合わせることで、IFS およびランダム バックオフなしで AP からのフレームを送信できます。これにより、コールによる競合の発生が緩和されます。

図 5-11 では、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

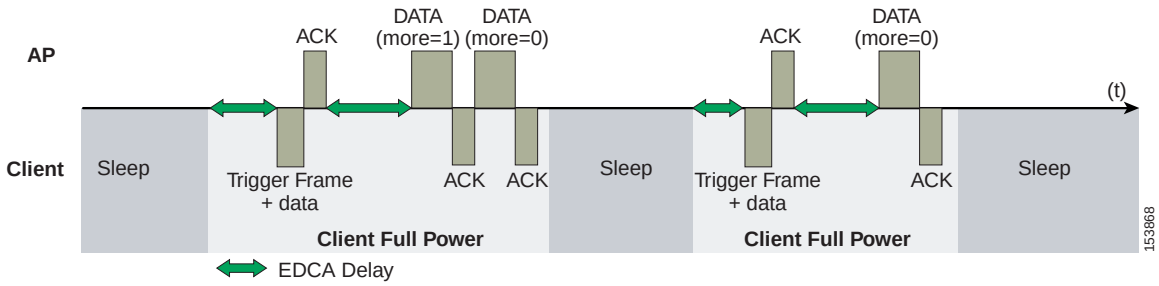


省電力モードにあるクライアントは、まず AP ビーコン内の TIM の存在を介して、AP でデータが待機していることを検出します。クライアントはデータを取得するために AP を省電力ポーリング（PS-Poll）する必要があります。クライアントに送信されたデータが複数のフレームの送信を要求している場合、AP はそのことを送信済みデータ フレーム内に示します。このプロセスでは、すべてのバッファ済みデータを取得するまで、クライアントが AP に PS-Poll を送信し続ける必要があります。

このことは、2 つの大きな問題点を提示しています。1 つ目の問題は、このプロセスが通常のデータ交換だけでなく PS ポーリングも必要とするため、DCF に関連する標準アクセス遅延に対処するには非常に非効率的であるということです。2 つ目は、音声トラフィックにはさらに重大な問題ですが、バッファ済みデータの取得が DTIM に依存しており、それによってビーコン間隔が異なるということです。標準のビーコン間隔は 100 ミリ秒であり、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ー レベルが発生し、音声ハンドセットは、音声コールの進行中に、省電力モードをフル送受信動作に切り替えます。これにより、許容できる音質を確保できますが、バッテリの寿命は短くなります。Cisco 7921G Unified Wireless IP Phone 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 と同じ効率性は得られませんが、U-APSD を使用しない 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 では、U-APSD を使用したトラフィック フローの例を示します。この場合、トラフィックを取得するためのトリガーは、クライアントによる AP へのトラフィック送信です。AP は、フレームを確認応答すると、データがキューイングされていることと、接続を継続する必要があることをクライアントに伝えます。その後 AP は、データをクライアントへ送信します。通常は TXOP バーストとして送信しますが、この場合は最初のフレームだけに EDCF アクセス遅延が発生します。そして、確認応答フレーム後の後続フレームがすべて直接送信されます。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 つのみです。VoWLAN クライアントは、そのフレームを AP から受信した後でスリープ モードに入ることができます。

図 5-12　　U-APSD



このアプローチは、以前の方式の短所を両方とも克服した、はるかに効率的な方法です。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。クライアント トラフィックは音声の場合には対称になるので、クライアントが 20 ミリ秒ごとにフレームを送信した場合、フレームの受信も 20 ミリ秒ごとになると想定されます。それにより、発生する最大ジッターは *n* x 100 ミリ秒ではなく 20 ミリ秒になります。

TSpec アドミッション制御

Traffic Specification（TSpec）では、802.11e クライアントが自身のトラフィック要件を AP に通知できます。802.11e MAC 定義には、競合ベースの EDCA オプションと、送信権（TXOP）によって提供される制御されたアクセス オプションという、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。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際、簡単に思い浮かぶのは、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、というものです。しかし、必ずしもそうとは限りません。TSpec 要求を使用して、EDCA のさまざまなアクセス カテゴリ（AC）の使用を制御することもできます。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、音声アクセス カテゴリを使用しようとしている WLAN クライアント デバイスは、最初にその AC を使用するための要求を行う必要があります。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 で設定可能です。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、多くの場合可能です。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。

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*を送信する際に使用されます。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 要求が AP に送信されます。

- ADDTS アクション フレーム：AP に関連付けられたクライアントが通話を開始または終了したときに作成されます。ADDTS には TSpec が含まれています。トラフィック ストリーム レート セット（TSRS）情報要素（IE）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：ステーションがトラフィック 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 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。ステーションが別の 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 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 ハンドセットと Cisco AP の間の ADDTS 要求と応答の例については、図 5-13 および図 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るようになります。したがって、その TSpec を満たすリソースがあるかどうかを AP で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の要求中に、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 ハンドセット）。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。

TSpec のサポートは、クライアントには必要ありません。ただし、WLAN が、音声またはビデオのコール アドミッション制御（CAC）を使用して設定されている場合、TSpec をサポートしていないクライアントでは、ベスト エフォート型 QoS で音声またはビデオのパケットを送信する必要があります（QoS プロファイル（5-20 ページ）を参照）。したがって、この WLAN が音声またはビデオの QoS レベルで設定され、CAC が有効になっている場合、ADDTS ロジックを使用していないクライアントの正しい動作は、ベスト エフォート型にマーキングされた音声およびビデオ トラフィックを送信することです。TSpec 対応のクライアントに ADDTS 要求の拒否が存在していれば、Wi-Fi チャネルの利用率は、設定された CAC 制限よりも高くなります。そのクライアントでは、音声パケットおよびビデオ パケットがクライアントの仕様ごとにベスト エフォート型でマーキングされます。

図 5-13　　ADDTS 要求の復号化

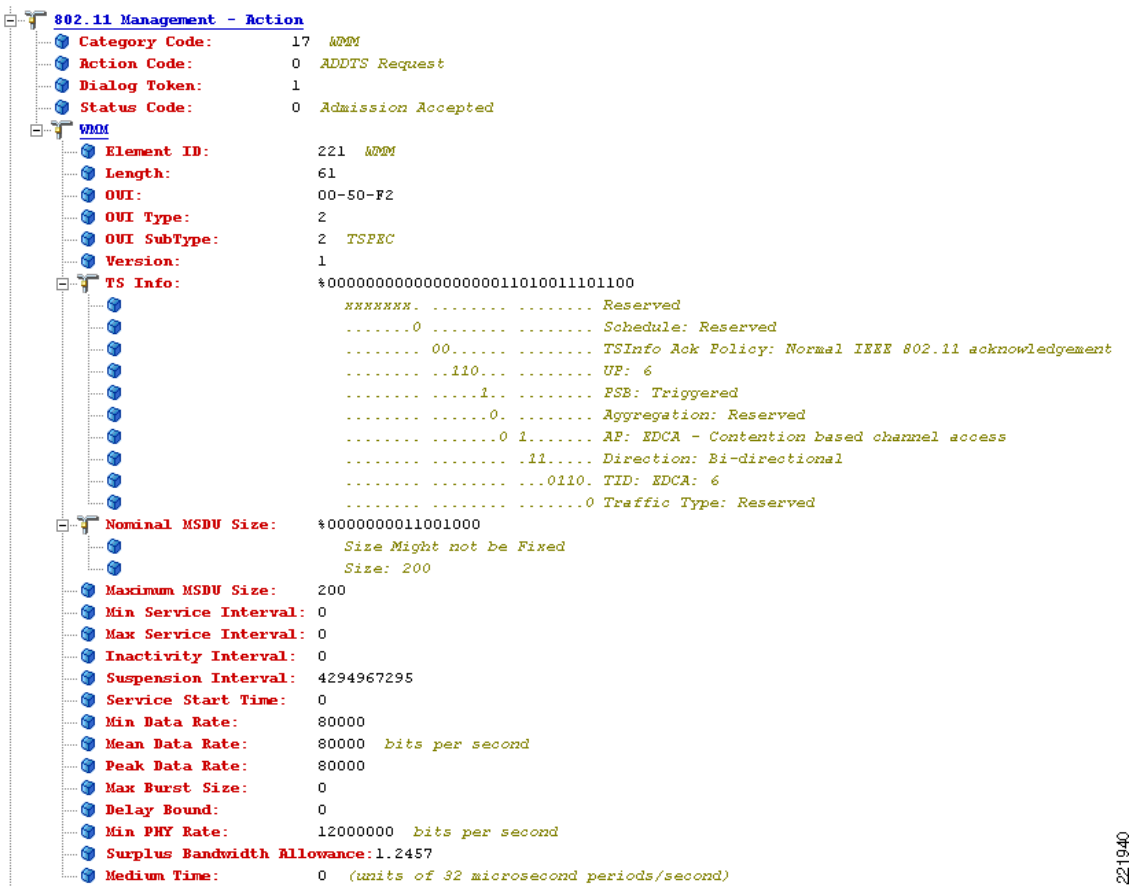
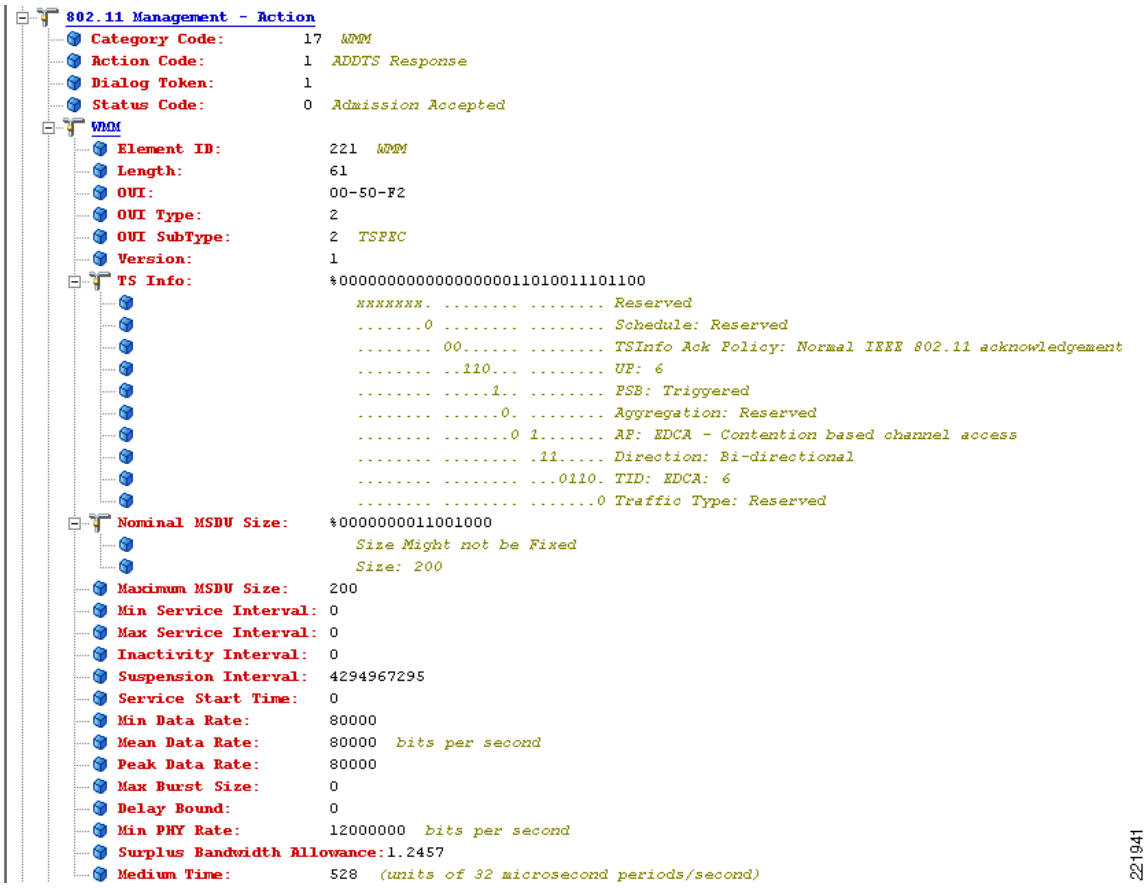


図 5-14　　ADDTS 応答の復号化



WLAN インフラストラクチャ対応の-QoS 拡張機能

シスコ*集中管理型 WLAN アーキテクチャ*には、WMM サポート機能のほかにいくつかの QoS 拡張機能があります。その機能は次のとおりです。

- QoS プロファイル
- WMM Policy
- Voice over IP 電話
- アドミッション制御パラメータ

これらの機能の詳細については、以降の項を参照してください。

QoS プロファイル

これらのプロファイルの中で最も重要なものが、WLC によって使用される QoS プロファイルです。図 5-15 で示すように、QoS プロファイルは次のように設定できます。

- ブロンズ:バックグラウンド
- ゴールド:ビデオ アプリケーション
- プラチナ:音声アプリケーション
- シルバー:ベスト エフォート

図 5-15　QoS プロファイル オプション

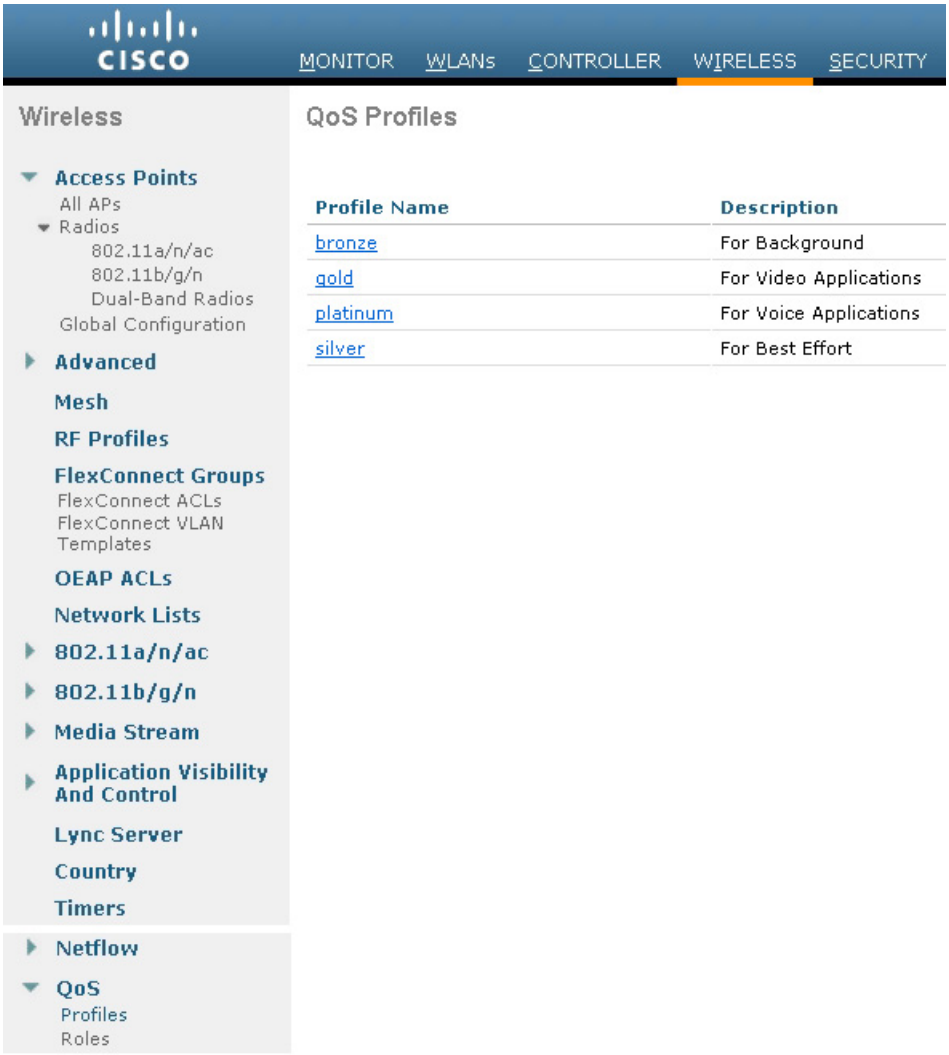


図 5-15 に示すプロファイルごとに、帯域幅の契約、RF 使用制御、および許可された最大の 802.1P 分類を設定できます。

(注)　シスコでは通常、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 機能を使用して差別化サービスを提供することを推奨しています。

特定のプロファイルを使用する WLAN については、そのプロファイルの音声またはその他の分類によって次の 2 つの重要なサービス クラス（CoS）の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 CoS 値の決定

  CoS パラメータの値を使用して、そのプロファイルを使用する WLAN のすべての CAPWAP（*Control And Provisioning of Wireless Access Points*）パケットの CoS がマーキングされます。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、コントローラのアプリケーション マネージャ インターフェイスから送信される CAPWAP パケットは 5 の CoS 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 WLC で調整されます。設定に IEEE CoS のマーキングを維持することが重要である理由については、次に説明します。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 WLAN が設定されている場合、AP が受信する CAPWAP パケットの DSCP は CoS 値によって決まります。また、その結果として WLAN トラフィックの WMM 分類とキューイングが決まります。これは、フレームの WLAN WMM 分類が、そのフレームを伝送する CAPWAP パケットの DSCP 値から派生するためです。

- 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 の音声トラフィックは、CoS 6 で AP に着信し、CoS 6 に基づいて、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 未満の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ます。そしてそれにより、使用する WMM アドミッション制御（AC）が設定されます。

重要な点は、Cisco Unified Wireless Network では常に IEEE 802.11e 分類の観点から考え、IEEE 分類と Cisco QoS ベースラインとの間の変換を 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 5-16 を参照）。各 QoS プロファイルは、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、認証、許可、およびアカウンティング（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、クライアントに最適な QoS を提供するためには、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 や有線 QoS などの標準 QoS メカニズムを使用する必要があります。

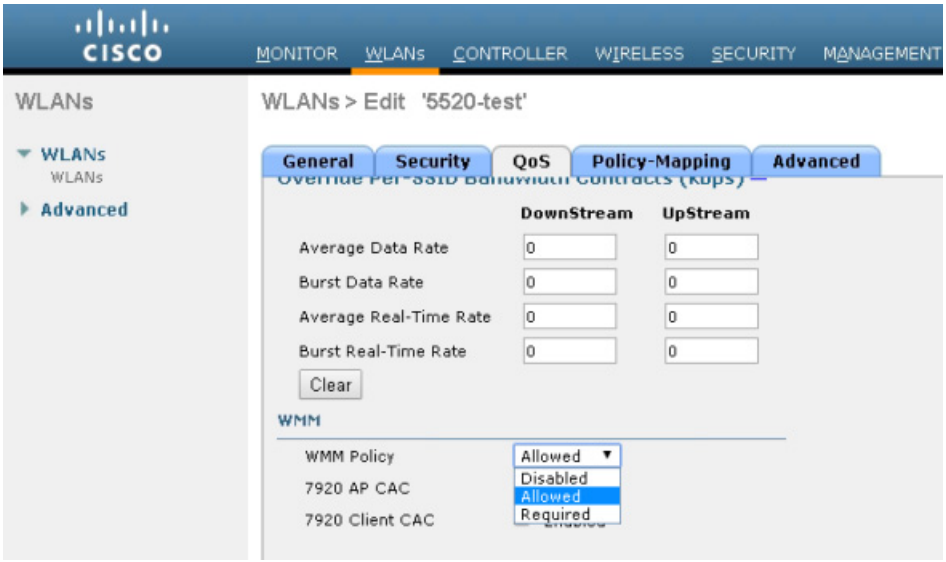
図 5-16　WLAN QoS プロファイル

WMM ポリシー

QoS プロファイル以外に、WLAN ごとの WMM ポリシーによって追加の WMM オプションも制御できます（図 5-17 を参照）。WMM オプションには次のようなものがあります。

- [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 対応クライアントのみをこの WLAN にアソシエートできます。

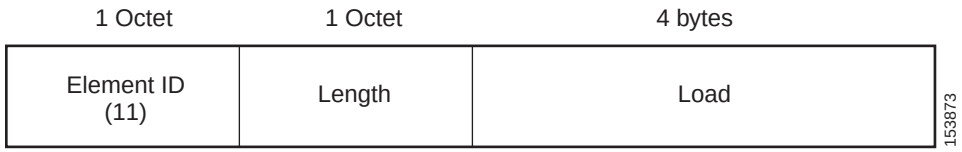
図 5-17　WLAN WMM ポリシー



IP フォン

図 5-18 では、Cisco AP がアドバタイズする基本的な QoS Basis Service Set（QBSS）情報要素（IE）を示します。[Load] フィールドは、現在その AP のデータを送信するために使用されている有効な帯域幅の一部を示しています。

図 5-18　QBSS 情報要素



実際に、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：Draft 6（先行標準）
- 新 QBSS：Draft 13 802.11e（標準）
- 新分散型 CAC 負荷の IE：シスコの情報要素

使用する QBSS は WLAN 上の WMM および Cisco 792x VoIP 電話の設定に依存します。

図 5-19 で示しているとおり、792x 電話のサポートは、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。Cisco 792x 電話など 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、アソシエート先として最適な AP を決定します。

WLC は、クライアント コール アドミッション制御（CAC）制限を使用して 792x 電話をサポートします。このサポートには以下が含まれています。

- 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 以前のレガシーな 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 CAC 設定を使用します。

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

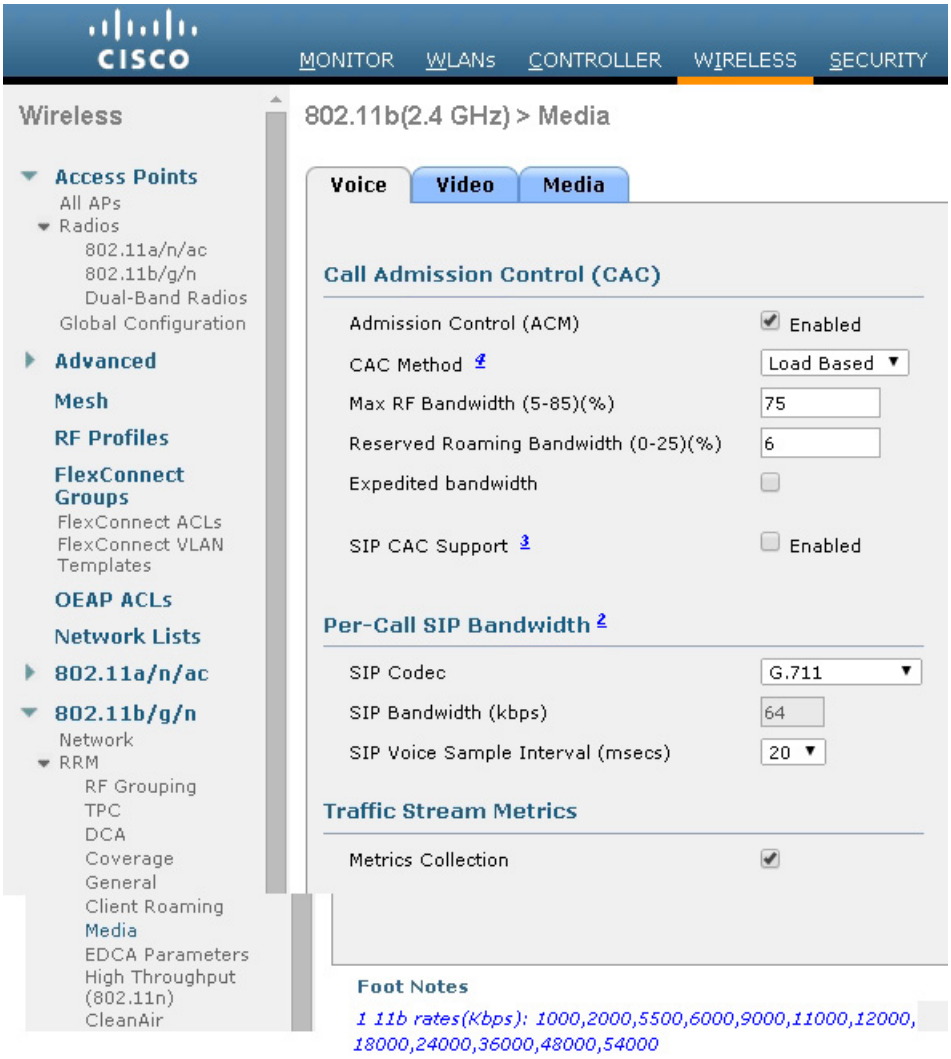
- WMM だけが有効な場合、IE 番号 2（802.11e 標準）QBSS Load IE がビーコン応答とプローブ応答で送信されます。
- 7920 クライアント CAC 制限がサポートされる場合、IE 番号 1（先行標準 QBSS IE）が 802.11b/g 無線のビーコン応答とプローブ応答で送信されます。
- 7920 AP CAC 制限がサポートされる場合、IE 番号 3 QBSS IE が bg 無線のビーコン応答とプローブ応答で送信されます。

（注）　さまざまな QBSS IE が同じ ID を使用するため、これら 3 つの QBSS は相互に排他的です。たとえば、ビーコン応答とプローブ応答には QBSS IE を 1 つだけ含めることができます。

アドミッション制御パラメータ

図 5-19 では、コントローラの音声、ビデオ、およびメディア パラメータを設定するためのの設定画面の例を示しています。

図 5-19　音声パラメータの設定



CAC 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、[Max RF Bandwidth (%)] を含みます。この値の範囲は、チャネル帯域幅の 5 ～ 85 % です。

[Reserved Roaming Bandwidth (%)] パラメータは、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、また通話中の VoWLAN クライアントのうちのどれがその AP にローミングしようとしているかを指定します。

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になりますが、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、[Load-Based AC] チェックボックスと [Admission Control (ACM)] チェックボックスの両方をオンにします。

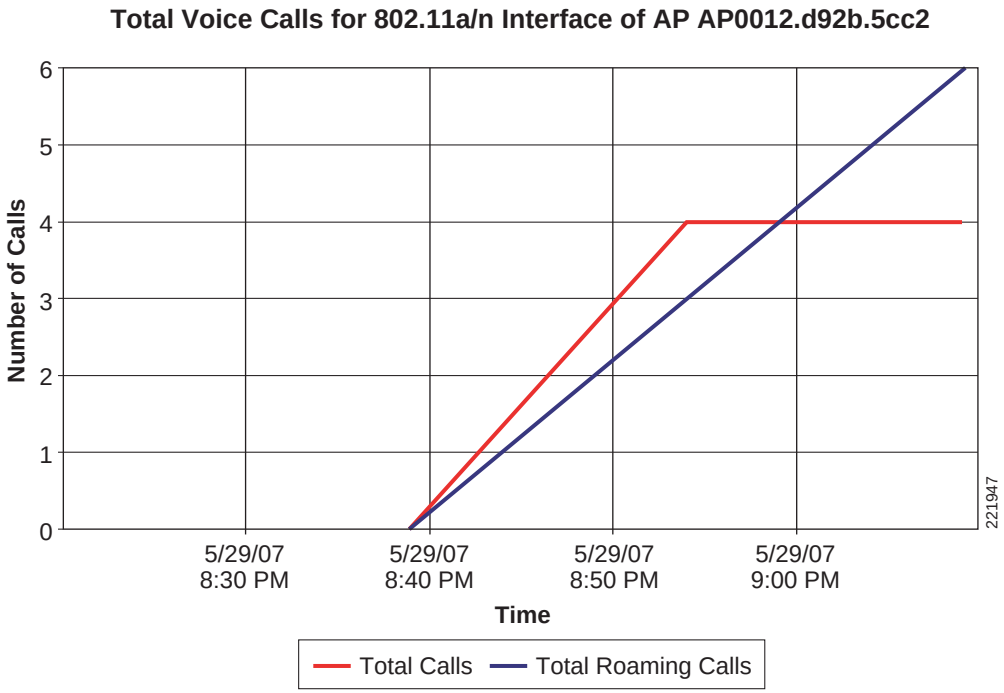
(注)　音声およびビデオの負荷ベースの CAC は、非メッシュ AP に適用されます。メッシュ AP の場合は、スタティック CAC のみが適用されます。

SIP CAC のサポートには、スタティックまたは負荷ベースの CAC が必要です。*スタティック* CAC を使用している場合は、SIP CAC のサポートにより、AP でのコールの数を設定できます。通常、Wi-Fi チャネル上のコールのサブスクリプションによって品質が影響を受けないようにするためにコール数を管理する方法としては、ダイナミックな負荷分散型アプローチの方が優れています。

[Voice Parameters] ウィンドウ（図 5-19）の [Metrics Collection] オプションで、Cisco Prime Infrastructure で使用するために音声コールまたはビデオ コールでデータを収集するかどうかを指定します。

図 5-20 では、Cisco Prime Infrastructure で使用できる音声統計レポートの一例を示します。この例では、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を示しています。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、または要求に応じて（一時的に）使用でき、Cisco Prime Infrastructure でグラフィック表示したり、ファイルへ書き込んだりすることができます。

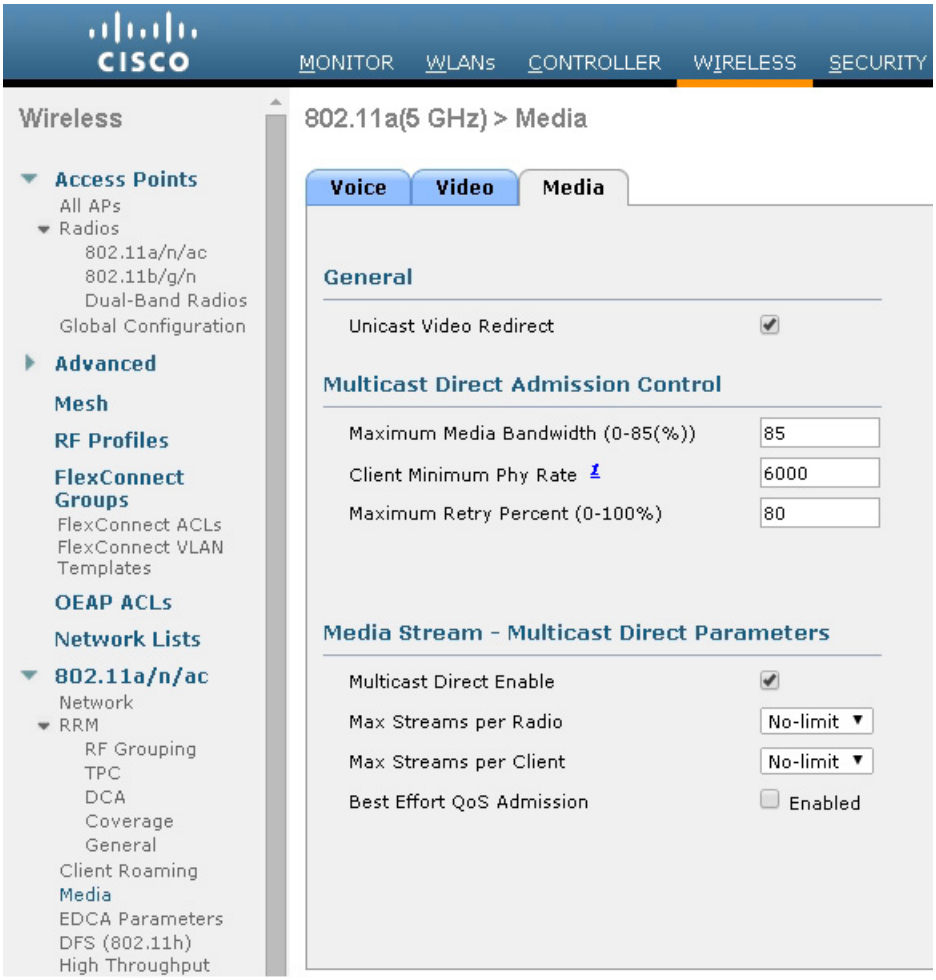
図 5-20　Cisco Prime Infrastructure の音声統計



（注）　CAC は、音声とビデオの QoS プロファイルに対してのみ実行されます。

図 5-20 では、音声 CAC のコール用に予約されている帯域幅の割合が小さい場合の影響を示します。4 つのコールに対して十分な帯域幅が予約されましたが、コールは他の Wi-Fi チャネルにローミングすることが可能でした。図 5-21 では、メディア ストリーミング用の CAC オプションを示します。*最大 RF 帯域幅*は音声、ビデオおよびメディア ストリーミングの間で共有されます。[Voice]、[Video] および [Media] タブにはそれぞれ固有の *最大 RF 帯域幅*があります。この最大 RF 帯域幅を合計して、Wi-Fi チャネルのメディアの完全な帯域幅予約の総計を得ます。各タブのフィールドには 85 % という最大値が表示されていますが、全体的な最大 RF 帯域幅値は実際には 3 つすべてのフィールドの合計です。[Voice] タブの最大 RF 帯域幅が 85% に設定されている場合、[Video] タブと [Media] タブでは [Max RF Bandwidth] フィールドをゼロに設定する必要があります。音声、ビデオ、データすべての CAC の動作に帯域幅を必要とする場合、各タブのフィールドを 25% に設定します。そうすると、メディアのチャネル帯域幅の制限が 75% になります。それぞれのメディアのタイプに帯域幅の 4 分の 1 を割り当て、データに帯域幅の 4 分の 1 を割り当てるわけです。

図 5-21　WLC の [802.11a (5 GHz)] > [Media] ウィンドウ



ビデオ用 CAC は、音声 CAC と似た動作をします。ビデオ用 CAC の目的は、アクティブなビデオコールの品質が Wi-Fi チャネルに追加されたビデオによる悪影響を受けないよう、ビデオ コールの量を制限することです。

(注)　この件やその他の設定オプションの詳細については、WLC の構成ガイドを参照してください。

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（保護されたアドミッション制御においてそのクライアントが 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 および表 5-6 は、アドミッション制御が有効または無効であ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

AC 有効	トラフィック ストリームが確立	トラフィック ストリームなし
無効	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。ユーザ優先度（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。
有効	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る前に、パケットが 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では、パケットは WLAN QoS を使用して送信されます。

表 5-6　ダウンストリーム トラフィック

AC 有効	トラフィック ストリームが確立	トラフィック ストリームなし
無効	変更なし	変更なし
有効	変更なし	WMM クライアントの BE に対して UP をリマークします。WMM 以外のクライアントに対しては、WLAN QoS を使用します。

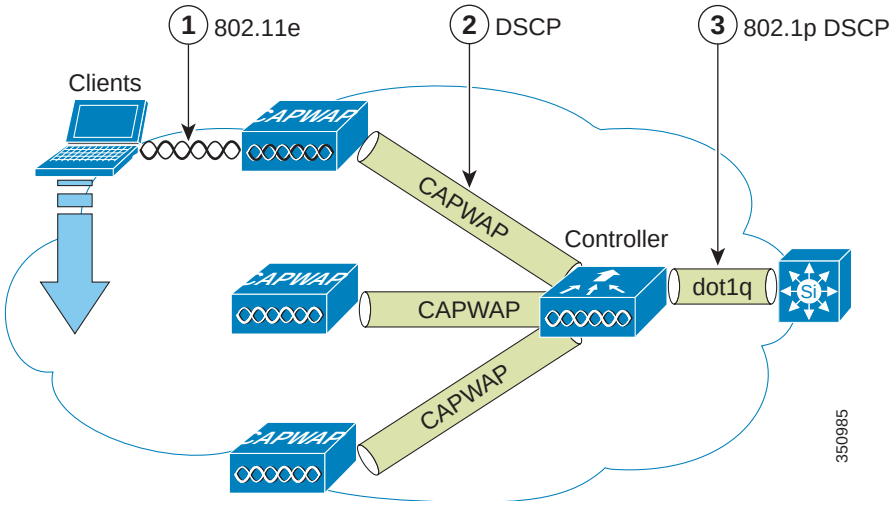
802.11e、802.1P および DSCP のマッピング

Unified Wireless Network 内の WLAN データは CAPWAP（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、WLC は DSCP と CoS の間の分類のマッピング プロセスを使用します。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 CAPWAP 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。これに類似したプロセスは、AP に向かう CAPWAP パケットに対して WLC でも発生する必要があります。

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 CAPWAP パケットにも AP および WLC によって適切な DSCP 分類（分類に関する考慮事項（5-38 ページ）を参照）が割り当てられます。

図 5-22 では、CAPWAP WLAN ネットワークのさまざまな分類メカニズムを示します。

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。戦略とは次のようなものです。

- CAPWAP 制御フレームには優先順位が必要です。CAPWAP 制御フレームは CS6（IP ルーティング クラス）の DSCP 分類でマーク付けされます。
- WMM を有効にしたクライアントには、対応する DSCP 分類にマッピングされたフレームの分類があります。対応する分類とは WLC に送信される CAPWAP パケットの DSCP 分類です。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 QoS プロファイルに合わせて設定された CAPWAP トンネルの DSCP があります。792x 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 AP 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 CAPWAP 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 802.11e 分類は、DSCP 分類を 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、含まれている IP パケットの DSCP 値ではなく、CAPWAP パケットの DSCP 値に基づきます。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

CAPWAP 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 で示すとおり、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[1]

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	56	7	—
ネットワーク間制御（CAPWAP 制御、802.11 管理）	48	6	7
音声	46（EF）	5	6
ビデオ	34（AF41）	4	5
音声管理	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
背景	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

1. 表に記載されていない DSCP 値に対する IEEE 802.11e UP（ユーザ優先度）値は、DSCP の上位（MSB）3 ビットを考慮して算出されます。たとえば、DSCP 32（バイナリ 100 000）に対する IEEE 802.11e UP 値は、10 進数に変換される MSB（100）値で、これは 4 になります。DSCP 32 の 802.11e UP 値は 4 です。

CAPWAP ベースの AP への QoS 機能の展開

WLAN QoS 機能を AP に展開する場合には、次の事項を検討します。

- 有線 CAPWAP 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）情報に依存して、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、CAPWAP 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 が使用されなくなりました。そのため、レイヤ 2 CAPWAP 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、レイヤ 2 CAPWAP 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。
- 無線出力ポートに限り EDCF に類似した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 FlexConnect

WLC に転送されるデータ トラフィックがある WLAN の場合、動作はハイブリッド リモート エッジ FlexConnect AP 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る WLAN の場合、FlexConnect 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。これはネイティブでないタグ付きの VLAN 上でのみ発生します。

ダウンストリーム トラフィックの場合、FlexConnect AP はイーサネット側から受信した dot1q タグを使用して、ローカルにスイッチされた VLAN の無線で WMM 値に対してキューイングとマーキングを行います。

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。ダウンストリーム トラフィックの場合、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。アップストリームの場合、クライアントがデフォルト WLAN 値より高い WMM 値を送信したときには、デフォルトの WLAN 値が使用されます。WMM 以外のトラフィックでは、AP からのクライアント フレームに CoS マーキングは含まれません。

QoS プロファイルに対するクライアントごとの Flexconnect AAA のオーバーライドは、リリース 8.4.100.0 以上の 802.11ac Wave 2 AP でサポートされています。この機能を使用して、QoS は特定のユーザに対して選択的に微調整できます。

Apple デバイス用 Fastlane

QoS は、輻輳した環境でトラフィックを効率よく伝送するための主要なコンポーネントです。QoS を利用することで、ビジネス運営上の重要性を反映したマーキングをアプリケーションに適用できます。有線インフラストラクチャでは、このマーキングの使用により、マーキング値に基づいて異なる優先度を設定したり、アプリケーション カテゴリまたはマーキングに基づいて帯域幅の割り当てや制御を実施したりすることができます。ワイヤレス環境では、8 つのユーザ優先度キューのいずれか 1 つにアプリケーションをアソシエーションする目的でもマーキングが使用されます。また、キューへのアソシエーションを使用して、アプリケーションがワイヤレス メディアにアクセスする頻度を統計に基づいて変えることもできます。インフラストラクチャ レベルで適切なマーキングを行うことで、ダウンストリーム トラフィックが最適化され、ビジネスへの関連性が高いアプリケーションは、統計上優先的にトラフィックを受信でき、リアルタイム アプリケーションには非インタラクティブ アプリケーションより高い優先順位を付けることができます。クライアント端末が QoS マーキングを適切に運用していれば、同じ効果がアップストリームにも適用されます。

Apple iOS デバイスは、IETF の推奨に従って QoS マーキングを行います。WLC AireOS code 8.3 では、Fastlane 機能を有効にすることにより、次のような便利な機能を活用することができます。

- WLC QoS 設定がグローバルに最適化され、リアルタイム アプリケーションのサポートが向上します。
- Apple iOS デバイスでは、WMM TSPEC/TCLAS ネゴシエーションを実行することなく、アップストリーム音声トラフィックを送信できます。インフラストラクチャがこれらの端末の音声マーキングに対応します。
- QoS プロファイルを Apple iOS 10 デバイスに適用して、アップストリームで QoS マーキングが適用されるアプリケーションと、ベスト エフォートまたはバックグラウンドで送信されるアプリケーションを決定することができます。

機能の概要

シスコのインフラストラクチャ側では、ターゲット WLAN で機能が有効になり次第、シスコの AP が Fastlane のサポートをアドバタイズします。

クライアント側では、iOS 10 以上が動作する Apple デバイスで、AP ビーコン応答とプローブ応答に設定された情報要素について、Fastlane がサポートされている必要があります。Apple iOS 10 デバイスは、Fastlane のサポートをマーキングする特定の IE も送信します。

最初の WLAN で Fastlane を有効にすると、Wi-Fi デバイスの QoS サポートが最適になるようにコントローラが自動的に設定されます。特に、グローバル プラチナ プロファイルが音声へのトラフィックを許可するように設定されて、そのプロファイルにより、ユニキャスト デフォルト プライオリティやマルチキャスト デフォルト プライオリティのパラメータがベスト エフォートに設定されます。ユーザ単位での 帯域幅契約はプロファイル上で無効になり、802.1p に準じたものとなります。プラチナ プロファイルは、ターゲットの WLAN に接続されます。ワイヤレス CAC（ACM）と優先帯域幅は、両方の帯域の音声キュー用に有効となっており、最大音声帯域幅が 50 % に設定されます。カスタマイズされた DSCP-to-UP マップと UP-to- DSCP マップは、IETF RFC 4594[1] および draft-szigetti-ieee-802-11-01[2] で推奨された値をマッピングするように設定されます。アップストリーム トラフィックには DSCP が信頼されています。AutoQoS プロファイルが作成され、差別化 QoS 処理を必要とすることの多い、広く普及した一般的な 32 のアプリケーションに対し、推奨されたマーキングが適用されます。ターゲット WLAN で、アプリケーションの可視性が有効になると、この自動 QoS プロファイルが自動的に適用されます。

Apple iOS 10 デバイスは QoS プロファイルを受信できます（標準的な Apple プロファイル プロビジョニング テクニックを使用してプロビジョニングされます）。この QoS プロファイルでは、ホワイトリストに登録できるアプリケーションの一覧が示されます。ホワイトリストのアプリケーションには、Apple Service_Type 方式を使用して、アップストリーム QoS マーキングを適用することが許可されます。ホワイトリストにないアプリケーションは、Fastlane ネットワークではアップストリーム QoS マーキングを適用しません。デフォルトでは、すべてのアプリケーションがホワイトリストに追加されています（例：QoS ホワイトリストのない状態では、すべてのアプリケーションで QoS マーキングが可能です。ホワイトリストが導入されると、ホワイトリスト内のアプリケーションのみが Service_Type 方式による QoS マーキング適用となり、他のアプリケーションは、ベスト エフォートもしくはバックグラウンドの QoS 処理を受けます）。Fastlane をサポートする iOS 10 デバイスと、Fastlane が設定された WLAN とのアソシエーションが行われた場合は、以前受信した QoS プロファイルが適用されます。また、AP は iOS 10 の QoS マーキングを信頼します。特に、音声としてマーキングされたトラフィックは、クライアントがアドミッション コントロール（ADDTS）を実行していなくとも信頼されます。

この機能は、AireOS コード リリース 8.3 向け 802.11n および 802.11ac wave 1 AP と、[3] Wave 2 AP 向け 8.3.110.0 について、ローカル モードと FlexConnect モード AP でサポートされています。

1. https://tools.ietf.org/html/rfc4594
2. https://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11-02
3. AP1600/2600 シリーズ アクセス ポイント、AP1700/2700 シリーズ アクセス ポイント、AP3500 シリーズ アクセス ポイント、AP3600 シリーズ アクセス ポイント + 11ac モジュール、WSM、HALO、3602P、AP3700 シリーズ アクセス ポイント + WSM、HALO、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP1530 シリーズ アクセス ポイント、AP1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、2800 シリーズ アクセス ポイント、3800 シリーズ アクセス ポイント、AP1040/1140/1260 シリーズ アクセス ポイント

設定手順

1. 新しい WLAN を作成します。Fastlane は、デフォルトでは有効化されていません。

この設定は、次の GUI または CLI コマンドを使用して変更できます。

```
config qos Fastlane enable/disable wlan <wlan id>
```

WLAN で Fastlane を有効にすると、変更がグローバルに適用されて両方の帯域が一時的に無効になるので、そのことを伝える警告メッセージが表示されます（コマンドが完了すると自動的にどちらの帯域も再び有効になります）。

2. 以下を確認します。

- WLAN の [QoS] タブで [Fastlane] が有効になっている。
- WLAN の [QoS] プロファイルが [プラチナ（Platinum）] に設定されている。

アクセス ポイント + 11ac モジュール、WSM、Hyperlocation モジュール、3602P、AP3700 シリーズ アクセス ポイント + WSM、3702P、OEAP600 シリーズ OfficeExtend アクセス ポイント、AP700 シリーズ アクセス ポイント、AP700W シリーズ アクセス ポイント、AP 1530 シリーズ アクセス ポイント、AP 1550 シリーズ アクセス ポイント、AP1570 シリーズ アクセス ポイント、2800 シリーズ アクセス ポイント、3800 シリーズ アクセス ポイント、1560 シリーズ Mesh AP、AP 1040/1140/1260 シリーズ アクセス ポイント。

- [ワイヤレス（Wireless）] > [QoS] > [プロファイル（Profiles）] > [プラチナ（Platinum）] の順に移動すると、[ユニキャストのデフォルト優先順位（Unicast Default Priority）] と [マルチキャストのデフォルト優先順位（Multicast Default Priority）] が [ベストエフォート（Best Effort）] に設定されている。[有線 QoS プロトコル（Wired QoS protocol）] が [なし（None）] に設定されている。
- [ワイヤレス（Wireless）] > [QoS] > [QoS マップ（QoS Map）] の順に移動すると、QoS マップが有効になっており、[アップストリームで DSCP を信頼する（Trust DSCP Upstream）] が選択されている。QoS マップは、既知の DSCP 値を IETF 推奨値にマッピングするための 19 個の例外を作成します。他の DSCP 値はすべて、その上位（MSB）3 ビットに合致する一般的な UP にマッピングされます。
- [ワイヤレス（Wireless）] > [802.11a/n/ac] > [メディア（Media）] の順に移動すると、[コールアドミッション制御（Call Admission Control）] が有効になっており、[音声（Voice）] トラフィックに 50 % の最大 RF 帯域幅が割り当てられている。[ワイヤレス（Wireless）] > [802.11b/g/n] > [メディア（Media）] ページでも、同じ設定が表示されます。
- [ワイヤレス（Wireless）] > [802.11a/n/ac] > [EDCA パラメータ（EDCA Parameters）] の順に移動すると、[EDCA プロファイル（EDCA Profile）] が [Fastlane] になっている。[ワイヤレス（Wireless）] > [802.11b/g/n] > [EDCA パラメータ（EDCA Parameters）] ページでも、同じ設定が表示されます。

設定ガイドラインの補足

1. [アプリケーションの可視性（Application Visibility）] は Fastlane 設定のオプション要素です。[アプリケーションの可視性（Application Visibility）] を有効にしなくても、WLAN で Fastlane を有効にすることは可能です。

Fastlane WLAN で [アプリケーションの可視性（Application Visibility）] が有効になっている場合、推奨される Auto-QoS-AVC Profile が WLAN に適用されます。Fastlane を無効にしない限り、他の AVC プロファイルは適用できません。

CLI コマンド:

```
config wlan avc <wlan id> visibility enable
```

2. Fastlane は WLAN ごとに無効にすることができます。無効にすると、WLAN QoS ポリシーは [シルバー（Silver）]（デフォルト）に戻り、[アプリケーションの可視性（Application Visibility）] がデフォルト（[無効（Disabled）]）にリセットされます。必要に応じて、コマンド完了後に WLAN を編集し、アソシエーションされた QoS プロファイルを手動で変更することで、[アプリケーションの可視性（Application Visibility）] を有効にすることができます。

CLI コマンド:

```
Config qos Fastlane disable wlan <wlan id>
```

3. すべての WLAN で Fastlane を無効にすると、WLC のグローバル QoS 設定もデフォルトに戻すことができます。無効にするには、[Fastlane] グローバル設定ページを使用します。Fastlane が有効な WLAN が 1 つでも残っている場合、Fastlane をグローバルで無効にすることはできません。Fastlane をグローバルで無効にすると、QoS プロファイル [プラチナ（Platinum）] がデフォルトにリセットされます（[最高優先順位（Maximum Priority）] は [音声（Voice）] のままですが、[ユニキャストのデフォルト優先順位（Unicast Default Priority）] と [マルチキャストのデフォルト優先順位（Multicast Default Priority）] は [音声（Voice）] にリセットされます）。[音声（Voice）] ではワイヤレス CAC（ACM）が無効になり、アソシエーションされた最大帯域幅がデフォルト値の 75 % に戻ります。QoS マップが無効になり、アップストリーム QoS は、DSCP ではなく UP を使用します。

CLI コマンド:

```
Config qos Fastlane disable global
```

（注）　WLC のグローバル QoS 設定をデフォルトに戻すには Fastlane をグローバルで無効にする必要がありますが、Fastlaneをグローバルで有効に戻す必要はありません。最初の WLAN で Fastlane を有効にすると、Fastlane のグローバル パラメータも有効になります。

無線 QoS の展開に関するガイドライン

有線ネットワークにおける QoS 展開のルールが、WLAN での 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なく、帯域幅の割り当てに対する制御が強化されるだけです。

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 QoS 設定は、AP から渡される CAPWAP パケットの DSCP を信頼する必要があるため、比較的単純です。AP から送られてくる CAPWAP フレームには CoS のマーキングはありません。次にこの設定の例を示します。この設定では分類のみ行っていることに注意してください。ローカルの QoS ポリシーに応じて、キューイング コマンドを追加できます。

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

AP DSCP 値を信頼するという点においては、アクセス スイッチは WLC によってその AP に設定されたポリシーを信頼しています。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 に適用された QoS ポリシーに基づきます。

WLC スイッチの設定

WLC に接続されたスイッチでの QoS 分類決定は、AP に接続されたスイッチの場合よりも少々複雑です。これは、WLC から送られてくるトラフィックの 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。この決定を行う際は、次のことを考慮してください。

- 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）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 CAPWAP でカプセル化されたものです。アップストリーム トラフィックは、WLC から発信された、CAPWAP でカプセル化またはカプセル化解除された WLAN クライアント トラフィックです。
- CAPWAP パケットの DSCP 値は WLC の QoS ポリシーにより制御されます。（CAPWAP 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、アップストリームかダウンストリームか、カプセル化かカプセル化解除かの別にかかわらず、WLC の QoS ポリシーによって設定されます。

次の例では、WLC の CoS 設定を信頼することを選択しています。選択の理由は、この設定例では WLAN QoS を集中管理できるため、WLC スイッチ接続で WLC 設定や追加のポリシーを管理する必要がないことです。

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

より詳細な制御が必要な場合は、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。

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便利なツールですが、802.11 トラフィックの優先順位付けには直接対応していません。WMM クライアントまたは 792x ハンドセットをサポートする 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 音声とシスコの電話機

Cisco Unified Communication エンドポイントのデータ シートは、次のページで入手できます。

http://www.cisco.com/en/US/prod/voicesw/ps6788/ip_phones.html

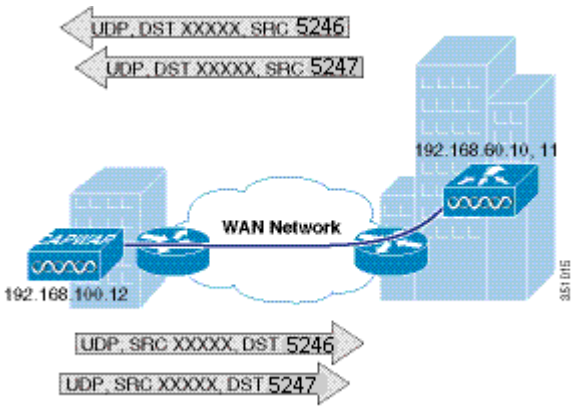
Cisco Jabber の一般的な概要については、次のページを参照してください。

http://www.cisco.com/web/products/voice/jabber.html

WAN 接続を介した CAPWAP

ここでは、図 5-23 で示すように CAPWAP AP が WAN リンク上に展開されている場合の QoS 戦略について説明します。

図 5-23　WAN 上の CAPWAP トラフィック



CAPWAP のトラフィック分類

CAPWAP AP は一般的に、次の 2 種類に分類できます。

- CAPWAP 制御トラフィック：UDP ポート 5246 によって識別される
- CAPWAP 802.11 トラフィック：UDP ポート5247 によって識別される

CAPWAP 制御トラフィック

CAPWAP 制御トラフィックはさらに、次の 2 種類に分類できます。

- 初期化トラフィック：CAPWAP AP がブートして CAPWAP 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。

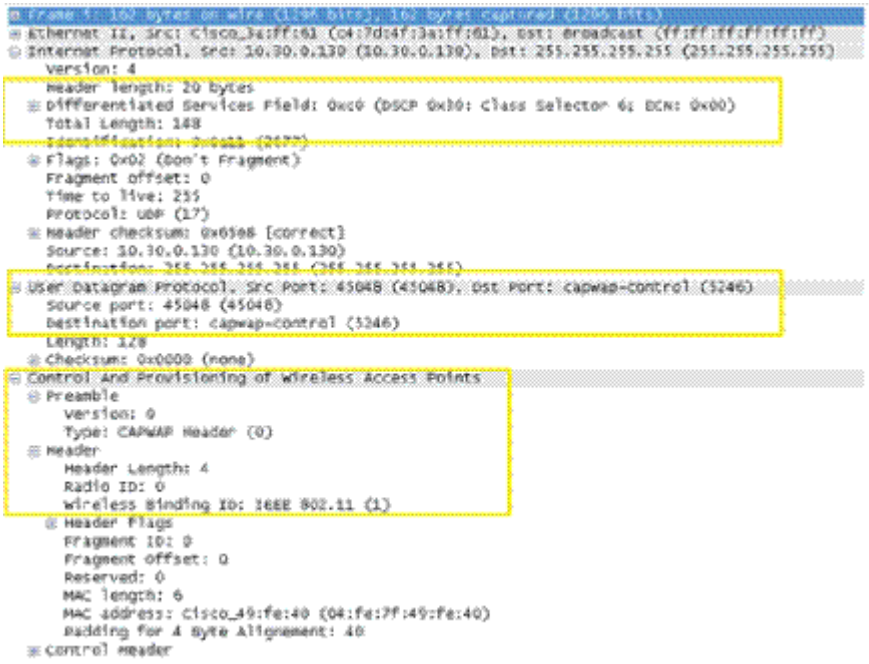
(注)　コントローラからの CAPWAP イメージ パケットはベスト エフォートとしてマーキングされますが、その確認応答は CS6 としてマーキングされます。この場合、スライディング ウィンドウ プロトコルが使用されないため、各追加パケットは確認応答を受信してからでないと送信されないことに注意してください。このタイプのハンドシェイクでは、WLAN からのファイルのダウンロードの影響が最小化されます。

- 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ーとして動作している CAPWAP AP によって生成されます。たとえば、CAPWAP ハートビート、無線リソース管理（RRM）、不正 AP 測定値などです。バックグラウンド CAPWAP 制御トラックは、CS6 としてマーキングされます。

図 5-23 では、初期 CAPWAP 制御メッセージの例を示します。初期 CAPWAP 制御メッセージのリストには、次のものが含まれています。

- CAPWAP ディスカバリ メッセージ
- CAPWAP ジョイン メッセージ
- CAPWAP コンフィギュレーション メッセージ
- 初期 CAPWAP RRM メッセージ

図 5-24　WISM-2 での CAPWAP 検出要求



CAPWAP 802.11 トラフィック

CAPWAP 802.11 制御トラフィックは一般的に、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 CS6 の DSCP 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 から送信される 802.1X フレームを含むパケットは 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 ポリシーに依存します。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

CAPWAP 制御トラフィックに使用される DSCP 分類は CS6（IP ルーティング クラス）です。これは Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）などの IP ルーティング プロトコルを対象としています。

現在の CAPWAP 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、ユーザ自身の 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、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限に抑えたい場合があります。場合によっては、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ります。これを実行するための最も簡単な方法は、CAPWAP 802.11 CS6 トラフィックを、より QoS 優先度の低い DSCP 値に再分類することです。CAPWAP UDP の使用ポートが CAPWAP データの使用ポートと異なるため、ディープ パケット インスペクション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。

また場合によっては、CAPWAP 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ります。これを実行するための最も簡単な方法は、バックグラウンド レートを超えた CAPWAP 制御トラフィックに対して、優先度の低いマーキングをすることです。

ルータの設定例

ここでは、CS6 の再マーキングや CAPWAP 制御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 CAPWAP AP を使用し、AP マネージャを持つ 2 つの 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 パケットの再マーキング

次の例では、CS6 としてマーキングされた CAPWAP 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ます。この再マーキングにより、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 CAPWAPDATACS6
 match access-group 110
 match  dscp cs6
!
policy-map CAPWAPDATACS6
 class CAPWAPDATACS6
  set dscp cs3
!
interface FastEthernet0
 ip address 192.168.203.1 255.255.255.252
service-policy input CAPWAPDATACS6
!
access-list 110 remark CAPWAP Data
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5247
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5247
access-list 111 remark CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
```

定義済みのレートを超えた CAPWAP 制御トラフィックの DSCP の変更

次の例では、WAN サイトから送られる CAPWAP 制御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制御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ます。レート制限の設定では、非準拠のトラフィックがドロップされるのではなく、単に再分類されることに注意してください。

(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 の展開の設計ガイドラインに従っていれば、CAPWAP 制御トラフィックが 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 CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
!
```

WLAN QoS と 802.11e の詳細については、『*IEEE 802.11 Handbook: A Designer's Companion 2nd Edition*』(Bob O'Hara/Al Petrick 著)を参照してください。ISBN:978-0-7381-4449-8

リリース 8.1 MR1 での QoS マッピング

現在、異なるベンダーのクライアントと AP 間の Differentiated Services Code Point(DSCP; DiffServ コード ポイント)とユーザ優先度(UP)のマッピングの中に誤って割り当てられているものがあります。このため、ハードウェアが異なると、DSCP が示す UP が異なって認識されるため、混乱を招いています。つまり、同じ DSCP の同じパケットが 2 台の異なるクライアント(A)と(B)から送信された場合、クライアントが使用する内部の DSCP と UP のマッピングによって UP が異なる場合があります。同様に、パケットが AP からクライアントに送信される場合も、DSCP と UP のマッピングが異なる場合があります。そのため、特定の DSCP が、同じネットワーク上で特定の UP を示すとは保証されません。

802.11u 標準の一部として提案されているソリューションが、8.1 MR1 以降のコードで使用可能です。

- ユーザ向けに、WLC の DSCP と UP 間のマッピングを設定する手法が提供されています。
- 対応するクライアントは、参加すると、AP から AP 以外の STA への再アソシエーション フレームで QoS マップを送信します。
- AP がすでにアソシエートされている場合に、このマップを変更すると、マップは非要請フレームとして送信されます。

この機能拡張により、パケットを送信すると、すべてのクライアントが同じ QoS マップを使用します。その結果、クライアントの製造元に関係なく同じ UP が使用されます。

802.11u 標準に準拠していないクライアントは、QoS マップを含むフレームを受信しません。ただし、これらのクライアントによって送信されたパケットは、設定されている新しい DSCP と UP 間のマッピングに従います。

QoS マップを無効にすると、現在のデフォルト マップが AP とクライアントにプッシュされます。表 5-8 に、デフォルトの QoS マッピングを示します。

表 5-8　デフォルトの QoS マッピング

VVID 802.1p UP ベースのトラフィック タイプ	VVID 802.1p CoS	VVID IP DSCP	IEEE IP DSCP	IEEE 802.11e UP	注
予約済み（ネットワーク制御）	7	56	56	7	TBD
予約済み	6	48	—	—	TBD
音声	5	46（EF）	48	6	
ビデオ	4	34（AF41）	40	5	
音声管理	3	26（AF31）	32	4	
バックグラウンド（ゴールド）	2	18（AF21）	16	3	
バックグラウンド（ゴールド）	2	20（AF22）	16	3	
バックグラウンド（ゴールド）	2	22（AF23）	16	3	
バックグラウンド（シルバー）	1	10（AF11）	8	2	
バックグラウンド（シルバー）	1	12（AF12）	8	2	
バックグラウンド（シルバー）	1	14（AF13）	8	2	
ベスト エフォート	0	0（BE）	0、24	0	
バックグラウンド	0	2	8	1	
バックグラウンド	0	4	8	1	
バックグラウンド	0	6	8	1	
有線からの不明 DSCP	Access Port	D	Do Not Care	D >> 3	AP 上

コントローラ管理者による QoS マッピングの設定

コントローラ管理者は、QoS マッピングを設定できます。

- すべての UP の下限から上限の DSCP の範囲は 0 ～ 7 です。[QoS Map Set] には、それぞれ 8 レベルのユーザ優先度に対応した [DSCP Range] フィールドがあります。DSCP 範囲の値は、0 ～ 63、または 255 です。
  - 各ユーザ優先度の DSCP 範囲は重複していない。
  - DSCP の上限値は DSCP の下限値以上である。
  - DSCP 範囲の上限値と下限値が 255 に等しい場合、対応する UP は使用されない。

- DSCP の例外として、特定の DSCP で特定の UP を明示的にマーキングできます。[DSCP Exception] フィールドは任意で [QoS Map Set] に含まれます。含まれている場合、[QoS Map Set] には最大 21 の [DSCP Exception] フィールドがあります。
- QoS マップを有効化または無効化します。
- ユーザ設定のマッピングはクライアントに送信され、アップ ストリーム トラフィックとダウン ストリーム トラフィックの両方で使用されます。

(注)　現在、設定された QoS プロファイルに基づいて着信 DSCP パケットを制限しています。QoS プロファイルごとにデフォルトの DSCP 値があります。DSCP 値がデフォルト値より大きいパケットは、デフォルト値までに制限されます。

QoS マップで、制限値を動的にする必要があります。すべての UP が、DSCP の下限と上限の範囲内で設定されます。制限値は QoS プロファイル UP の DSCP の上限にする必要があります。たとえば、UP 5 では、30 ～ 40 が設定されます。したがって、ゴールド QoS プロファイルは DSCP 40 に制限する必要があります。

CLI からの QoS マッピングの設定

考えられる間違ったマーキングまたは予期せぬマーキングを補償するために、AireOS コントローラ コード 8.1 MR1 では、DSCP と UP 間の変換テーブルをカスタマイズして設定できます。また、802.11e UP マーキングの代わりに、クライアントの 802.11 アップストリーム フレームの DSCP マーキングを信頼することもできます。

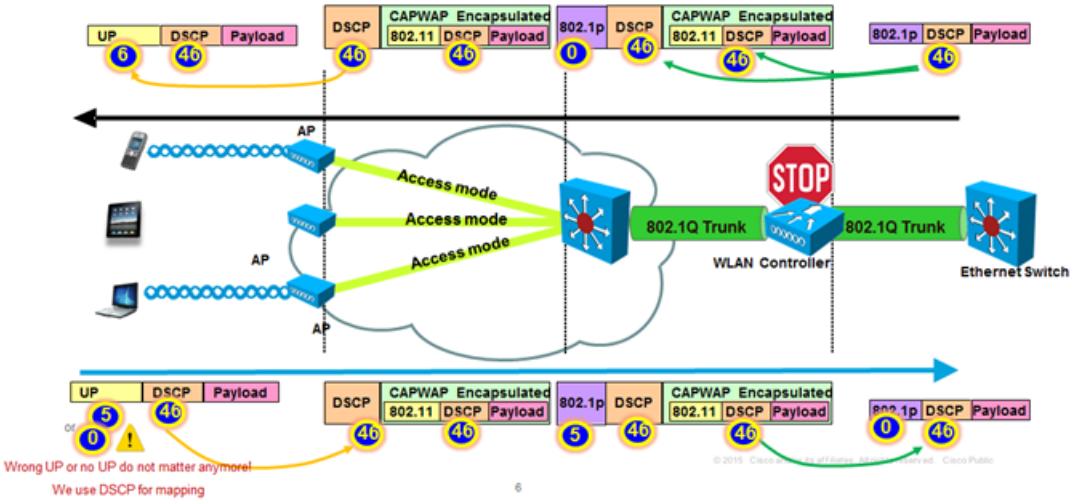
DSCP のアップストリームを信頼するには、コントローラのコマンド ラインから 2 つのコマンドを使用して有効化します。

(Cisco Controller) **>config qos qosmap trust-dscp-upstream enable**

(Cisco Controller) **>config qos qosmap enable**

この機能を有効にすると、UP の代わりに DSCP が使用されます。ダウンストリームでは、すでに、DSCP が CAPWAP 外部ヘッダーの QoS マーキングを決定するために使用されています。したがって、ダウンストリームのマーキング ロジックは変更されません。アップストリーム方向では、DSCP を信頼すると、予期しない、または欠落した UP マーキングが補償されます。AP は、着信 802.11 フレームの DSCP 値を使用して、CAPWAP ヘッダーの外部マーキングを決定します。引き続き QoS プロファイルのシーリング（上限）ロジックが適用されますが、マーキング ロジックは、フレームの [UP] フィールドではなく [DSCP] フィールドに対して動作します。プラチナ プロファイルの場合、アップストリーム トラフィックの外部ヘッダーでは、UP が欠落しているか、または予期しない値の場合でも、DSCP 46 が保持されます。

図 5-25　例:プラチナ プロファイルの影響– 8.1 MR

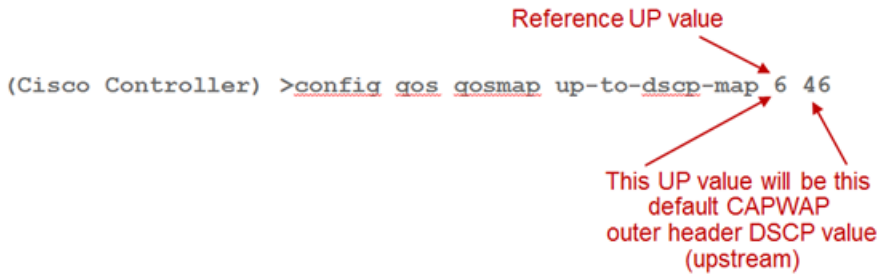


(注)　DSCP 信頼モデル(ワイヤレス クライアントは予期しない UP を使用します)。

ビデオ プロファイルでは、DSCP は 34 に制限されます。つまり、アップストリームとダウンストリームで、CAPWAP 外部ヘッダーの DSCP 値を導出するために DSCP が使用されますが、引き続き QoS プロファイルの上限が適用されます。

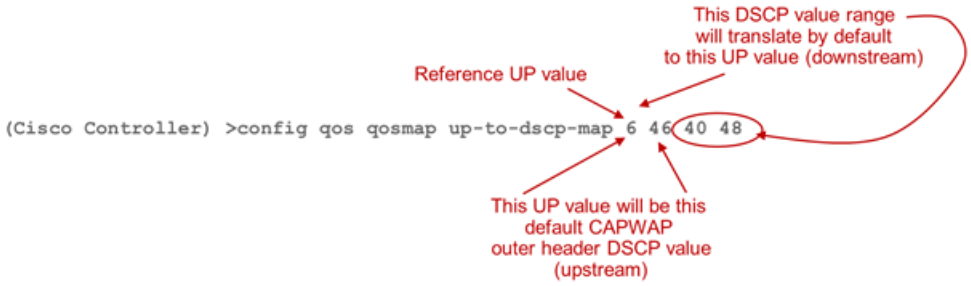
AireOS コントローラ コード 8.1 MR1 では、DSCP から UP、および UP から DSCP への変換値を手動で定義できます。この柔軟性によって、アップストリームとダウンストリームの予期せぬ QoS マーキングに対処し、一貫したポリシーを維持することができます。UP と DSCP の間のカスタマイズされたマッピングは、単一のコマンドで設定されます。たとえば、アップストリームでは UP 6 が常に DSCP 46 に変換されるとすると、この組み合わせは次のコマンドを使用して設定されます。

(Cisco Controller) **>config qos qosmap up-to-dscp-map 6 46**



同じコマンドを拡張して、逆マッピングを設定することもできます。たとえば、アップストリームで DSCP 40 ～ 48 が UP 6 に変換されるとすると、この組み合わせは次のコマンドを使用して設定されます。

(Cisco Controller) **>config qos qosmap up-to-dscp-map 6 46 40 48**



前述の設定は推奨される設定ではなく、単なる例である点に注意してください。7 つの UP とそれぞれの DSCP へのマッピングも同じロジックを使用して設定します。また、アップストリームのデフォルト値（前述の例では 46）が、ダウンストリーム方向に定義された範囲内（前述の例では 40 ～ 48）にある必要はない点にも注意してください。たとえば、アップストリームでは UP 6 を DSCP 34 に変換するが、ダウンストリームでは DSCP 40 ～ 48 を UP 6 に変換することに決定した場合は、次のコマンドを入力できます（これは設定可能なだけで、推奨設定ではありません）。

(Cisco Controller) **>config qos qosmap up-to-dscp-map 6 34 40 48**

また、ダウンストリーム トラフィックの DSCP と UP 間のマッピングの範囲内で例外を設定できます。たとえば、ネットワーク内で DSCP 44 とマーキングされた特定のトラフィックは UP 5 に変換されるとすると、次のように、DSCP 44 を例外として、40 ～ 48 の範囲を UP 6 に変換するように設定できます。

(Cisco Controller) **>config qos qosmap up-to-dscp-map 6 46 40 48**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 44 5**

この例外は、アップストリーム マッピングではなく、ダウンストリーム マッピングに適用される点に注意してください。アップストリーム マッピングは、DSCP マップに合致するように決定されたルールに従います。

Cisco AireOS リリース 8.1 MR1 での QoS マップの設定

QoS マップを設定するには、次の手順を実行します。

ステップ 1　手動マッピングを設定すると、ターゲット ネットワークがフレームを転送する方法が変更されるため、必ず事前に、これらのネットワークを無効化しておきます。

(Cisco Controller) **>config 802.11a disable network**

(Cisco Controller) **>config 802.11b disable network**

ステップ 2　QoS マップは、デフォルトで無効になっています。マップが有効な場合は、変更を加えるためカスタム マッピングを一時的に無効にします。

(Cisco Controller) **>config qos qosmap disable**

これで、QoS マップは無効になります。

ステップ 3　DSCP と UP の間のカスタム マッピングを設定します。7 つの UP をすべて設定し、カスタマイゼーションを有効にする必要がある点に注意してください。次に例を示します。

(Cisco Controller) **>config qos qosmap up-to-dscp-map 0 0 0 63**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 1 8**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 2 10**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 3 18**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 4 34**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 5 32**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 6 46**

(Cisco Controller) **>config qos qosmap up-to-dscp-map 7 0**

最初の行は 2 つの目的を実現しています。つまり、UP 0 を DSCP 0 にマッピングするが、すべての DSCP 値を UP 0 にマッピングしています。これによって、IETF RFC 4594 セクション 3.1 に準拠でき、すべての未指定の DSCP 値を 0 にリセットできます。

ステップ 4　例えば、次のように、標準トラフィックの例外を設定します。

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 8 1**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 10 2**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 12 2**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 14 2**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 16 0**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 18 3**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 20 3**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 22 3**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 24 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 26 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 28 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 30 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 32 5**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 34 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 36 4**

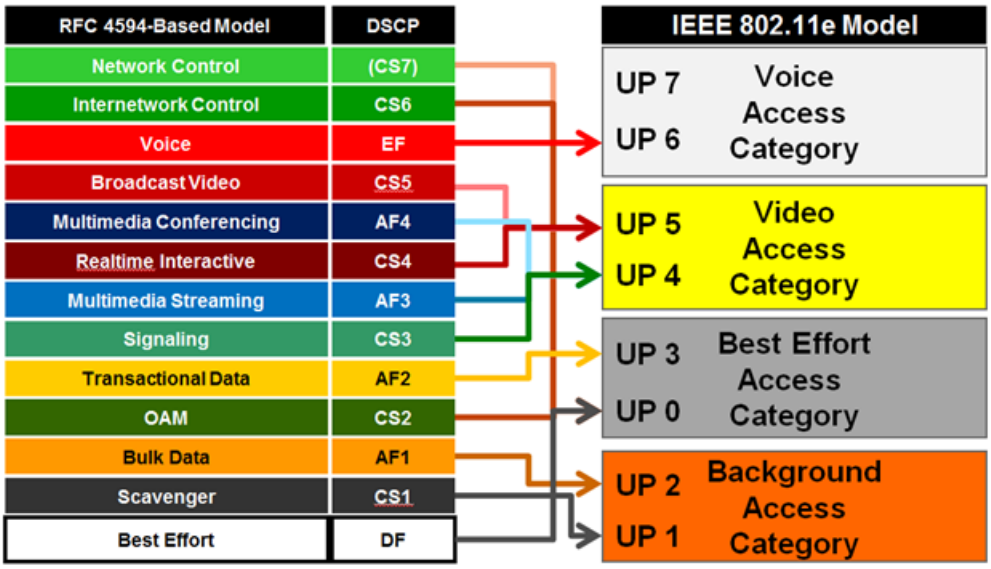
(Cisco Controller) **>config qos qosmap dscp-to-up-exception 38 4**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 40 5**

(Cisco Controller) **>config qos qosmap dscp-to-up-exception 46 6**

これらの例外は、標準の DSCP 値を適切な UP 値にマッピングします。このコマンドを使用すると、最大 21 まで例外を設定できる点に注意してください。

前述の設定は、次の図に示すシスコが推奨するマッピングを反映しています。



ステップ 5　また、アップストリーム方向では、UP 値の代わりに、ワイヤレス クライアント パケットの DSCP を使用することもできます。アップストリームで、DSCP の信頼を有効にすると、アップストリーム トラフィックに対して UP と DSCP 間の変換値は使用できない点に注意してください。ただし、ダウンストリーム トラフィックに対しては、DSCP 範囲の UP への変換、およびすべての例外を使用できます。

(Cisco Controller) >**config qos qosmap trust-dscp-upstream enable**

アップストリームの DSCP の信頼が有効になります。

ステップ 6　設定中はいつでも、作成した例外を削除できます。

(Cisco Controller) >**config qos qosmap delete-dscp-exception**

ステップ 7　手動マッピング全体を削除することもできます。

(Cisco Controller) >**config qos qosmap default**

ステップ 8　設定が完了したら、マッピングを確認できます。

(Cisco Controller) >**show qos qosmap**

```
Status: Disabled
        UP-TO-DSCP Map:
        Up      Default DSCP    Start DSCP      End DSCP
        0       0               0               63
        1       8
        2       10
        3       18
        4       34
        5       32
        6       46
        7       0
        Exception List:
        DSCP    UP
        8        1
        10       2
        12       2
        14       2
        16       0
        18       3
```

```
        20        3
        22        3
        24        3
        26        4
        28        4
        30        4
        32        5
        34        4
        36        4
        38        4
        40        5
        46        6
Trust DSCP Upstream: Enabled
```

ステップ 9　設定が完了したら、手動マッピングを有効化して、ネットワークを再度有効にすることができます。

(Cisco Controller) **>config qos qosmap enable**

これで、QoS マップが有効になりました。

(Cisco Controller) **>config 802.11a enable network**

（Cisco Controller）**>config 802.11b enable network**

Application Visibility and Control の概要

AVC はワイヤレス ネットワークにおけるアプリケーション認識制御を提供し、管理性と生産性を高めます。すでにさまざまな ASR および WLC プラットフォームで AVC がサポートされています。これはエンドツーエンドのソリューションであるため、FlexConnect AP に組み込まれている AVC のサポートもエンドツーエンドまで拡大されます。ネットワークのアプリケーションが完全に可視化されるため、管理者はアプリケーションに対してアクションを実行できます。

AVC には次の機能とコンポーネントがあります。

- Network Based Application Recognition（NBAR2）と呼ばれる次世代ディープ パケット インスペクション（DPI）テクノロジーが、アプリケーションの識別と分類を可能にします。NBAR は、ステートフル L4 ～ L7 分類をサポートし、Cisco IOS ベースのプラットフォームで利用できるディープパケット インスペクション テクノロジーです。NBAR2 は NBAR に基づいており、NBAR を使用するすべての IOS 機能に共通のフロー テーブルを提供するなどの追加の要件を満たしています。NBAR2 は、アプリケーションを認識し、Quality of Service（QoS）やアクセス コントロール リスト（ACL）などの他の機能にその情報を渡します。他の機能は、この分類に基づいてアクションを実行します。
- QoS、ドロップ、レート制限アプリケーションを使用してマークを適用できます。

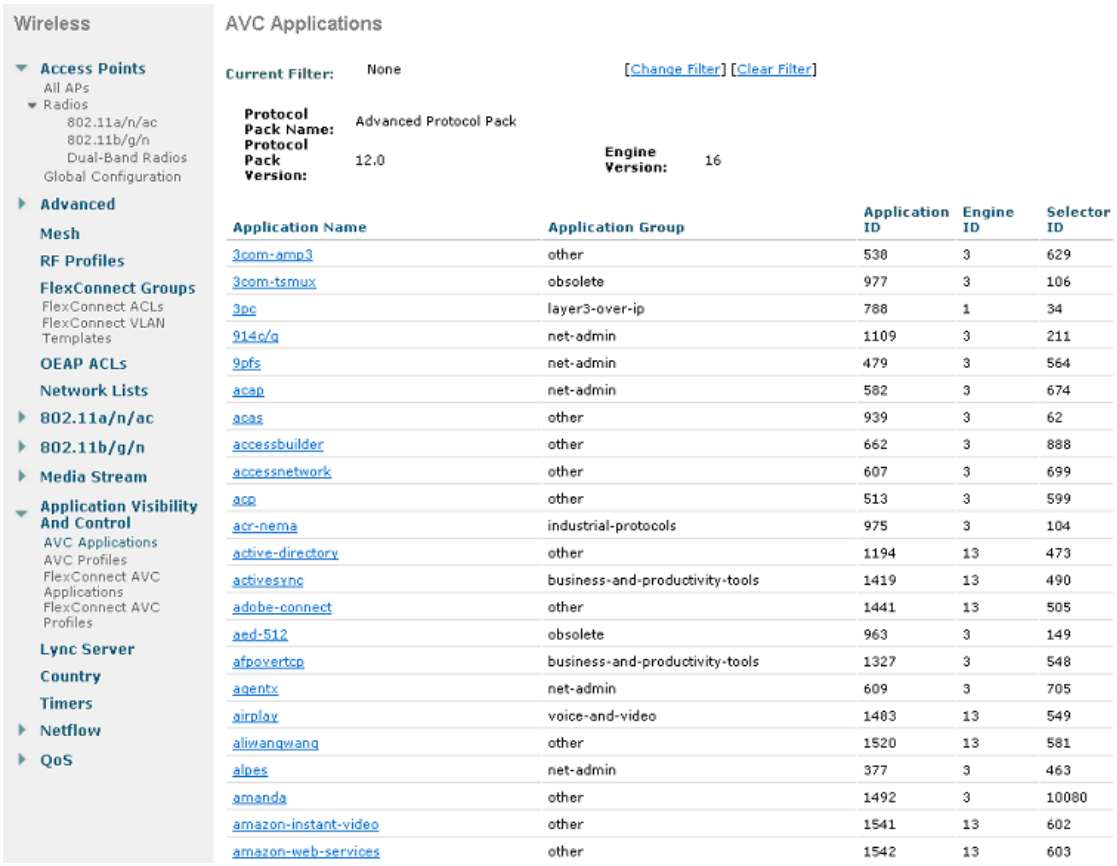
AVC により、WLAN でまたはユーザごとに、アプリケーションを表示、管理、制御できます。ネットワーク管理者は、GUI 表示で、どのアプリケーションがワイヤレス ネットワークで使用されているか、どこで誰によって帯域幅が使用されているかを確認できます。管理者は、Netflix や YouTube など、帯域幅を著しく消費するアプリケーションを通じてプライベート サイトまたは制限されているサイトにアクセスしたユーザが、ワイヤレス ネットワークを不正利用していないかを確認できます。WLC で実行される Network Based Application Recognition（NBAR2）エンジンにより、AVC は 13000 を超えるアプリケーションに対するアプリケーション認識制御を実現します。それらのアプリケーションを検出するアルゴリズムが含まれたプロトコル パック ファイルは、コントローラにプリロードされているか、最新バージョンに動的にアップグレードすることができます。

NBAR AVC の主な使用例としては、キャパシティ プランニング、ネットワーク使用量のベースライン化、帯域幅を消費しているアプリケーションの把握などがあります。アプリケーション使用状況の傾向分析により、ネットワーク管理者はネットワーク インフラストラクチャのアップグレードを計画し、ネットワーク輻輳時に帯域幅を大量に消費するアプリケーションから重要なアプリケーションを保護してユーザ エクスペリエンスを向上させ、優先順位付けと解除を行い、特定のアプリケーション トラフィックをドロップすることができます。

AVC は、リリース 7.4 以降、ローカル モードと FlexConnect モードの 2500、3504、5520、8540、2500、5508、7500、8500、および WiSM2 コントローラでサポートされています（セントラル スイッチング用に設定された WLAN についてのみ）。リリース 8.1 では、5508、5500、8500 シリーズ、7500、WiSM2、および vWLC における FlexConnect AP のローカル スイッチング WLAN 用 Application Visibility and Control（AVC）がサポートされています。リリース 8.5 以降、WLC 3500 のサポートが追加されています。

NBAR の主な使用例としては、キャパシティ プランニング、ネットワーク使用量のベースライン化、帯域幅を消費しているアプリケーションの把握などがあります。アプリケーション使用状況の傾向分析により、ネットワーク管理者はネットワーク インフラストラクチャのアップグレードを計画し、ネットワーク輻輳時に帯域幅を大量に消費するアプリケーションから重要なアプリケーションを保護してユーザ エクスペリエンスを向上させ、優先順位付けと解除を行い、特定のアプリケーション トラフィックをドロップすることができます。

.



NBAR でサポートされている機能

NBAR は、次のタスクを実行できます。

- 分類:アプリケーション/プロトコルの識別。
- AVC:分類されたトラフィックの可視性が得られ、またドロップまたはマーク（DSCP）アクションによるトラフィックの制御も可能です。
- NetFlow:Lancope 社の Stealth Watch を使用して、NBAR 統計情報を Cisco Prime Assurance Manager（PAM）などの NetFlow コレクタや 8.2 リリース以降に更新します。
- WLC 上の NBAR/AVC フェーズ 2 では、1349 の異なるアプリケーションについて分類とアクションを実行できます。
- ドロップ、マーク、レート制限の 3 つのアクションは、分類されたどのアプリケーションでも可能です。
- WLC では、最大 16 個の AVC プロファイルを作成できます。
- 各 AVC プロファイルには最大 32 のルールを設定できます。
- AVC プロファイルは、複数の WLAN にマッピングできます。ただし、1 つの WLANが保持できるのは、1 つの AVC プロファイルのみです。
- WLC には、NetFlow エクスポータおよびモニタを 1 つずつのみ設定できます。
- NBAR 統計情報は GUI の上位 30 のアプリケーションについてのみ表示されます。CLI を使用すると、すべてのアプリケーションの統計情報を表示できます。
- NBAR は、中央のスイッチング用に設定されている WLAN でのみサポートされます。
- WLAN にマッピングされた AVC プロファイルにマーク アクションのルールがある場合、そのアプリケーションは、WLAN に設定された QoS プロファイルをオーバーライドする AVC ルールに設定された QoS プロファイルに準じます。
- 方向マーキングは、特定のアプリケーションの双方向、アップストリームまたはダウンストリームのいずれかにのみ適用できます。
- 現在、レート制限は、3 つのアプリケーションにのみ適用できます。
- WLC 上の NBAR エンジンによってサポートまたは認識されていないアプリケーションは、UNCLASSFIED トラフィックのバケット配下でキャプチャされます。
- IPv6 トラフィックは分類できません。
- AAA による AVC プロファイルのオーバーライドは、8.0 リリース以降でサポートされています。
- AVC プロファイルは、WLAN ごとに設定してユーザごとに適用できます。
- Flex Connect AVC は vWLC でサポートされています。

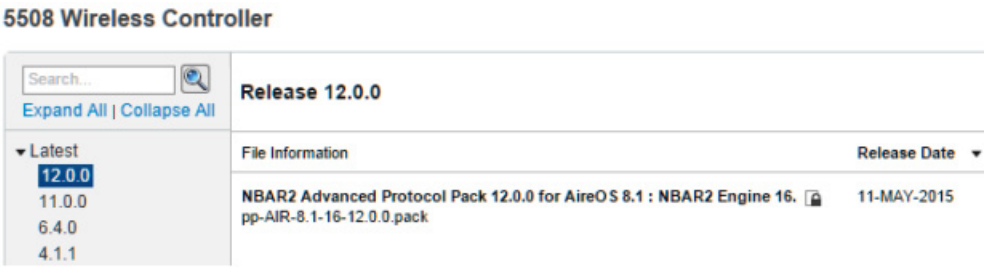
サポートされているアプリケーションを動的に更新するために、プロトコル パックの AVC サポートが追加されています。プロトコル パックは、コントローラ上のイメージを置き換えることなくシグネチャのサポート機能を更新できるソフトウェア パッケージです。新しいプロトコルのサポートが追加されたときに、動的にプロトコル パックをロードできるオプションがあります。メジャーとマイナーの 2 種類のプロトコル パックがあります。

- メジャー プロトコル パックには、新しいプロトコル、更新プログラム、およびバグ フィックスのサポート機能が含まれています。
- マイナー プロトコル パックには新しいプロトコルのサポート機能は含まれていません。
- プロトコル パックは、個々の特定のプラットフォーム タイプ、ソフトウェア バージョン、リリースを対象としています。プロトコル パックはソフトウェア タイプ「NBAR2 プロトコル パック」を使用して CCO からダウンロードできます。

プロトコル パックは、特定のバージョンの NBAR エンジンと合わせてリリースされます。たとえば、WLC 8.5 には NBAR エンジン 23 が付属しているため、そのためのプロトコル パックはエンジン 23 向けに記述されています（pp-AIR-8.1-23-12.pack）。プロトコル パックのロードは、プラットフォーム上のエンジンのバージョンが、プロトコル パックで要求されるバージョン以上（上記の例では 23）である場合に可能です。

リリースでサポートされているプロトコルの完全な一覧は、次のリンクに掲載されています。

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html



現在ロードされているプロトコル パックを表示するには、**show** コマンドを使用します。

(Cisco Controller) **>show avc protocol-pack version**

```
AVC Protocol Pack Name: Advanced Protocol Pack AVC Protocol Pack Version: 12.0
```

現在の NBAR2 エンジンのバージョンを表示するには、**show** コマンドを使用します。

(Cisco Controller) **>show avc engine version**

```
AVC Engine Version: 16
```

WLAN 上の AVC および QoS のインタラクション

コントローラの AVC/NBAR2 エンジンは、特定の WLAN の QoS 設定と相互運用します。NBAR2 機能は DSCP 設定に基づいています。同じ WLAN に AVC と QoS が設定されている場合、アップストリーム方向とダウンストリーム方向でパケットは次のように処理されます。

アップストリーム

1. 内部 DSCP の有無にかかわらずパケットがワイヤレス側（ワイヤレス クライアント）から送信されます。
2. AP は WLAN（QoS ベースの設定）に設定されている CAPWAP ヘッダーに DSCP を追加します。
3. WLC は CAPWAP ヘッダーを削除します。
4. コントローラの AVC モジュールは、DSCP を上書きして、AVC プロファイルに設定済みのマーキングされた値にし、それを送信します。

ダウンストリーム

1. 有線側の内部 DSCP 値の有無にかかわらずパケットがスイッチから送信されます。
2. AVC モジュールは内部 DSCP 値を上書きします。
3. コントローラで、WLAN QoS 設定（802.1p 値、つまり 802.11e に準拠）と NBAR で上書きされた内部 DSCP 値が比較されます。WLC は、小さいほうの値を選択し、それを DSCP の CAPWAP ヘッダーに格納します。

4. WLC は、外部 CAPWAP の QoS WLAN 設定と AVC の内部 DSCP 設定を伴うパケットを AP へ送信します。
5. AP は CAPWAP ヘッダーを取り除き、AVC DSCP 設定を使用して、パケットを無線で送信します。AVC がアプリケーションに適用されていない場合、そのアプリケーションは WLAN の QoS 設定を採用します。

アンカー/外部コントローラ設定による AVC の動作

アンカーおよび外部コントローラ コンフィギュレーションの場合、AVC にアプリケーション制御が必要な場所を設定する必要があります。アンカー/外部設定では多くの場合、AVC はアンカー コントローラで有効にする必要があります。AVC プロファイルの適用は、アンカー コントローラ上の WLAN で実行されます。アンカー コントローラのリリースが 7.4 以上である場合は、上記のセットアップが機能します。

ローカル ポリシーに接続される AVC プロファイル

リリース 8.0 では、AVC プロファイルを特定のデバイス タイプのクライアントのローカル ポリシーにマッピングできます。ローカル ポリシーに AAA オーバーライドに基づいて別の AVC/mDNS プロファイル名を設定して、同じ WLAN 上のプロファイルで許可されていないサービスがポリシーによって使用可能となるのを制限できます。

WLC のプロファイリングとポリシー エンジンの概要

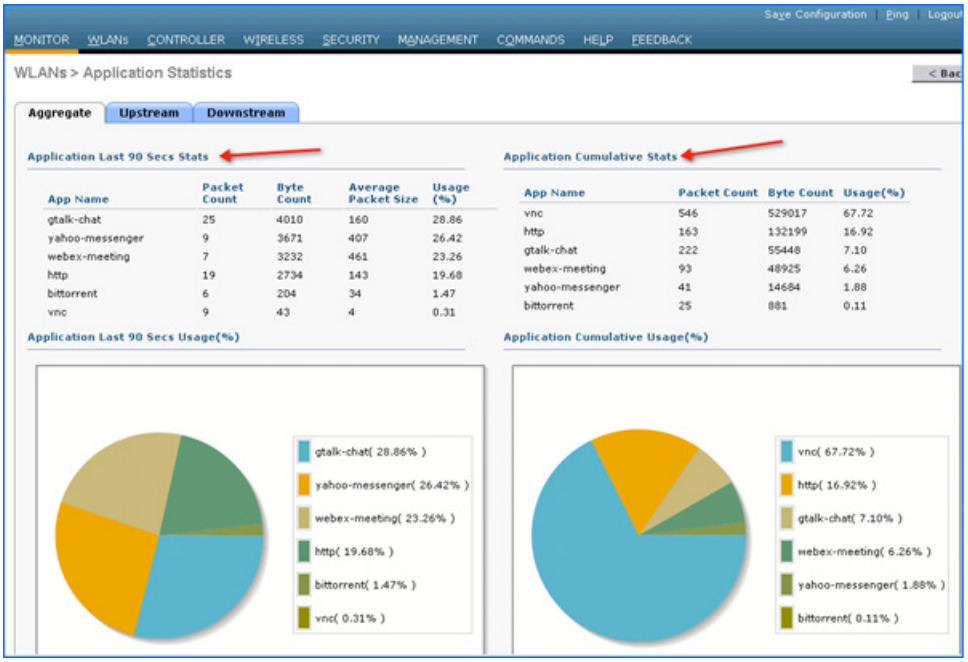
シスコには、現在、ISE を通じてデバイス ID、オンボーディング、ポスチャ、およびポリシーを提供する豊富な機能セットが用意されています。WLC のこの新しい機能では、HTTP、DHCP などのプロトコルに基づいてデバイスのプロファイリングを実行し、ネットワーク上のエンド デバイスを識別します。デバイス ベースのポリシーを設定し、ネットワーク上のユーザ単位またはデバイス ポリシー単位でそれらを適用できます。また、WLC は、ユーザ単位またはデバイス エンドポイント単位の統計情報と、デバイスごとに適用可能なポリシーも表示します。

BYOD（Bring Your Own Device）では、この機能がネットワーク上のさまざまなデバイスの認識に影響をもたらします。この機能によって、WLC 自体の内部で小規模に BYOD を実装できます。

AVC モニタリング

前述のとおり、次のようにトラフィックの可視性をモニタできます。

- すべての WLAN を対象にグローバルに
- 個々の WLAN
- 個々のクライアント



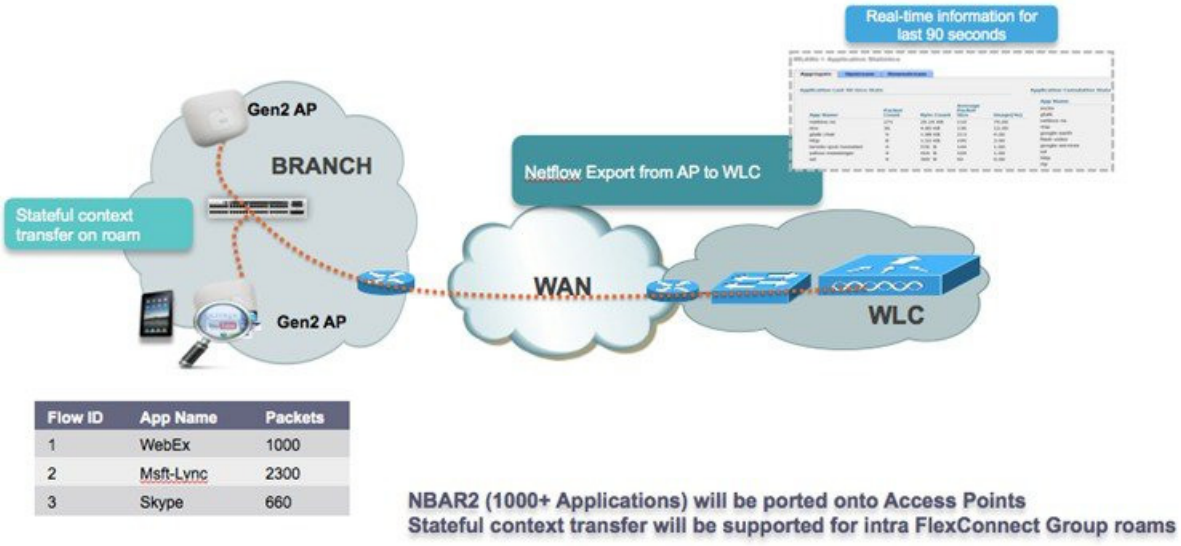
FlexConnect の Application Visibility and Control

NBAR AVC の主な使用例として、キャパシティ プランニング、ネットワーク使用量のベースライン化、帯域幅を消費するアプリケーションのより適切な把握などがあります。アプリケーション使用状況の傾向分析により、ネットワーク管理者はネットワーク インフラストラクチャのアップグレードを計画し、ネットワーク輻輳時に帯域幅を大量に消費するアプリケーションから重要なアプリケーションを保護してユーザ エクスペリエンスを向上させ、優先順位付けと解除を行い、特定のアプリケーション トラフィックをドロップすることができます。

AVC は、リリース 7.4 以降、ローカル モードと FlexConnect モードの 3504、vWLC、5520、8540、2500、5508、7500、8500、および WiSM2 コントローラでサポートされています（セントラル スイッチング用に設定された WLAN についてのみ）。リリース 8.1 では、FlexConnect AP のローカル スイッチング WLAN 用 Application Visibility and Control（AVC）がサポートされています。Flex AVC の詳細については、第 7 章「FlexConnect」を参照してください。

FlexConnect AP での AVC の動作方法

- NBAR2 エンジンは、FlexConnect AP 上で稼働します。
- DPI エンジン（NBAR2）を使用して、アクセス ポイントでアプリケーションの分類が行われ、L7 シグニチャを使用してアプリケーションが識別されます。
- AP はアプリケーション情報を収集し、90 秒ごとにコントローラにエクスポートします。
- リアルタイム アプリケーションは、コントローラのユーザ インターフェイスでモニタされます。
- FlexConnect アクセス ポイントで分類されたアプリケーションでは、アクション、ドロップ、マーキング、またはレート制限を実行できます。



AVC FlexConnect のファクトおよび制限

- FlexConnect AP の AVC では、1000 種類以上のアプリケーションを分類し、アクションを実行できます。
- FlexConnect AP で稼働するプロトコル パックは、WLC 上で稼働するプロトコルパックとは異なります。
- AVC による GUI の統計情報は、デフォルトでは上位 10 のアプリケーションに対して表示されます。これを、上位 20 または 30 のアプリケーションに変更することもできます。
- FlexConnect グループ内のローミングがサポートされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドはサポートされません。
- マルチキャスト トラフィックは、AVC アプリケーションではサポートされません。
- FlexConnect AVC の NetFlow エクスポート は 8.1 ではサポートされません。

NBAR NetFlow モニタ

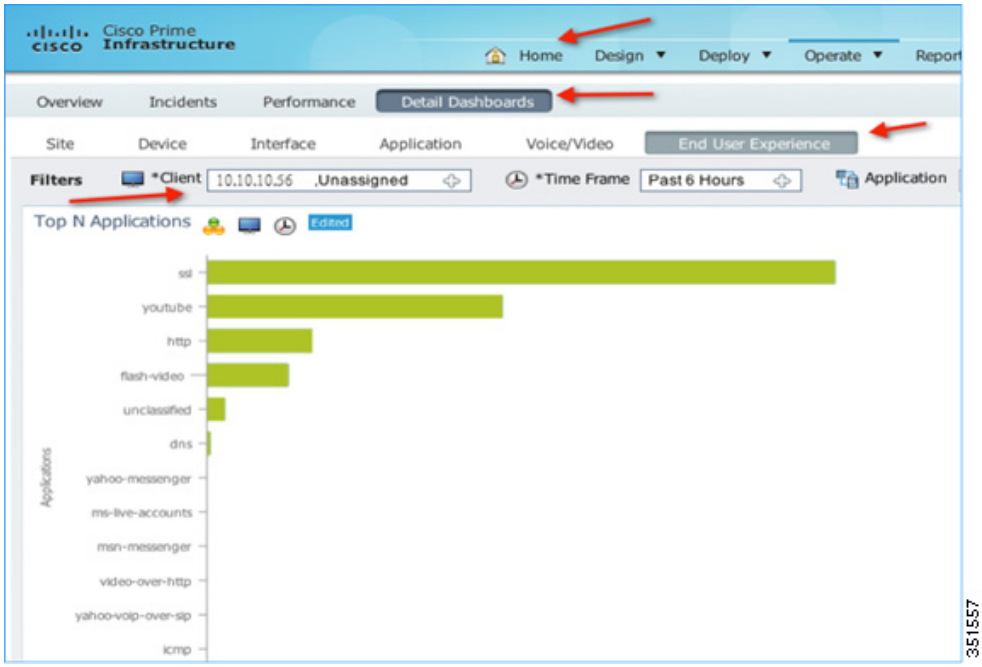
NetFlow モニタを WLC に設定し、WLC で生成されるすべての統計情報を収集することができます。さらに、これらの統計情報は NetFlow コレクタにエクスポートできます。次の例では、Cisco Performance Application Manager（PAM）が NetFlow コレクタとして使用されています。PAM は Cisco Prime Infrastructure で稼働するライセンス付きのアプリケーションです。

モニタ エントリが作成され、エクスポータ エントリが同じものにマッピングされた場合は、それを WLAN にマッピングする必要があります。

エクスポータ エントリを WLAN にマッピングするには、次の手順に従います。

1. [WLANs] をクリックします。
2. 特定の [WLAN ID] をクリックします。
3. [QoS] タブをクリックします。
4. [NetFlow Monitor] ドロップダウン リストから作成されたモニタ エントリを選択します。
5. [Apply] をクリックします。

Cisco Prime には、PAM を事前に設定する必要があります。PAM に WLAN が設定され、ワイヤレス クライアントが特定の事前設定されたアプリケーションとトラフィックをやり取りした後、管理者は WLAN ごとのアプリケーションの使用状況を表示できます。[Home] > [Detail Dashboards] > [End User Experience] に移動します。[Filters] 領域で、WLAN として [Network Aware] を選択し（次の例では **10.10.10.56** クライアント）、[GO] をクリックします。



Lancope による Netflow のサポート

IP トラフィック フローでは、一連のパケットが、送信元/宛先 IP アドレス、トランスポート ポート、方向などの共通の属性を伴い、ネットワーク デバイスを通過します。ワイヤレス フローのその他の共通属性としては、SSID や AP MAC があります。共通の属性を持つこれらのパケットがフローに集約され、Netflow コレクタにエクスポートされます。8.2 より前のリリースでは、コントローラがエクスポートした Netflow データは PI（Prime Infrastructure）によってのみ分析され、サードパーティ製の Netflow コレクタとの互換性はありませんでした。

リリース 8.2 では、強化された Netflow レコード エクスポータが導入されています。新しい Netflow v9 では、（RFC 3954 で定義されている）17 の異なるデータ レコードが、Lancope など外部のサードパーティ製 Netflow コレクタに送信されます。強化されたフロー レコード データ エクスポート機能は、WLC 5520、8510、8540 に追加されています。

8.2 より前のリリースでは、コントローラの Netflow 機能によって、クライアントの IP アドレス、SSID、アプリケーションの統計情報だけが送信されていました。その場合、Cisco Prime などの互換性のある Netflow コレクタではアプリケーションの統計情報を表示できましたが、5 タプルの完全なフロー情報は得られず、5 タプルを必要とする多くのサードパーティ製 Netflow コレクタとの互換性も確保されていませんでした。

8.2 より前のリリースによって WLC がエクスポートする現行の Netflow レコードでは、次のフィールドのみサポートされています。

- Application Tag
- クライアントの MAC アドレス
- AP MAC アドレス
- WlanID
- Source IP
- Dest IP
- 送信元ポート
- 宛先ポート
- プロトコル
- フロー開始時刻
- フロー終了時刻
- 方向（Direction）
- パケット数
- バイト数
- VLAN Id–Mgmt/Dyn
- TOS：DSCP 値
- Dot1x ユーザ名

Netflow の配置に関する考慮事項

- WLC では、1 つのモニタとエクスポータのみサポートされています。
- WLC では、コントローラごとに 1 つのタイプの Netflow レコードのみ、グローバルにサポートされます。
- フロー レコードは直接エクスポートされ、コントローラには表示されません。

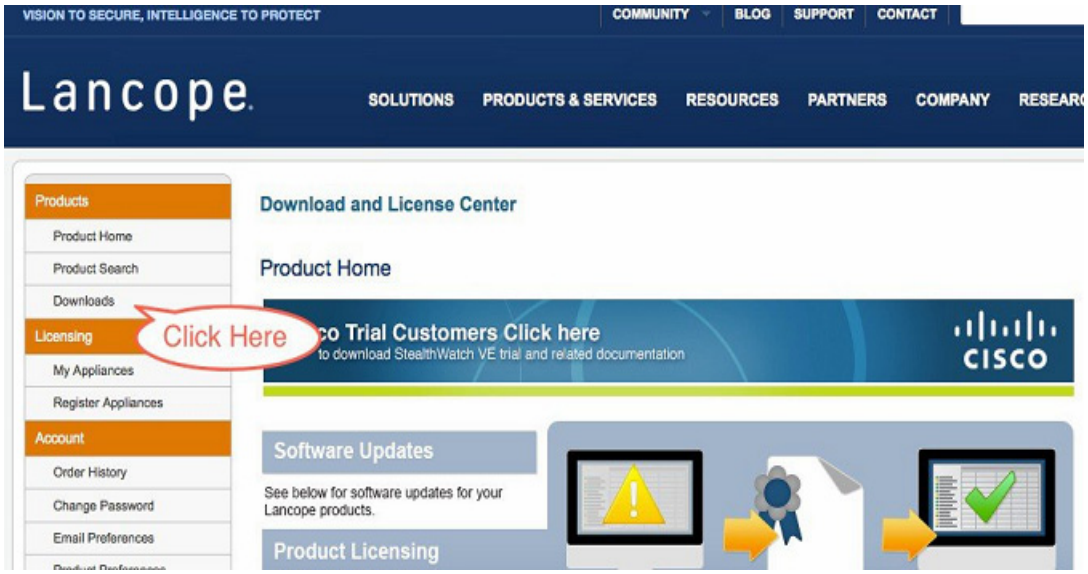
- 現在のアプリケーションの可視性の統計情報は、引き続きコントローラに表示されます。
- モニタのパラメータの変更により、WLAN の無効化と有効化が必要になります。
- 新しいレコードは、8510、5520、および 8540 コントローラでのみサポートされます。
- 2500、5508、7500、および WiSM2 コントローラはサポートされません。
- Netflow 統計情報は 30 秒間隔で送信されます（ユーザ設定不可。現在の値は 90 秒）。
- Netflow レコードは、新しいフロー レコードを持つ未分類のアプリケーションにも送信されます。
- Netflow は、その WLAN で AVC を有効にする際に送信されます。
- IPv6 トラフィックは、リリース 8.2 の Netflow ではサポートされていません。
- 初期テンプレートを送信する Netflow は、コントロール プレーンから送信されます。
- サービス ポートでの Netflow のエクスポートはサポートされていません。

評価目的での Lancope ソフトウェアの取得（参考）

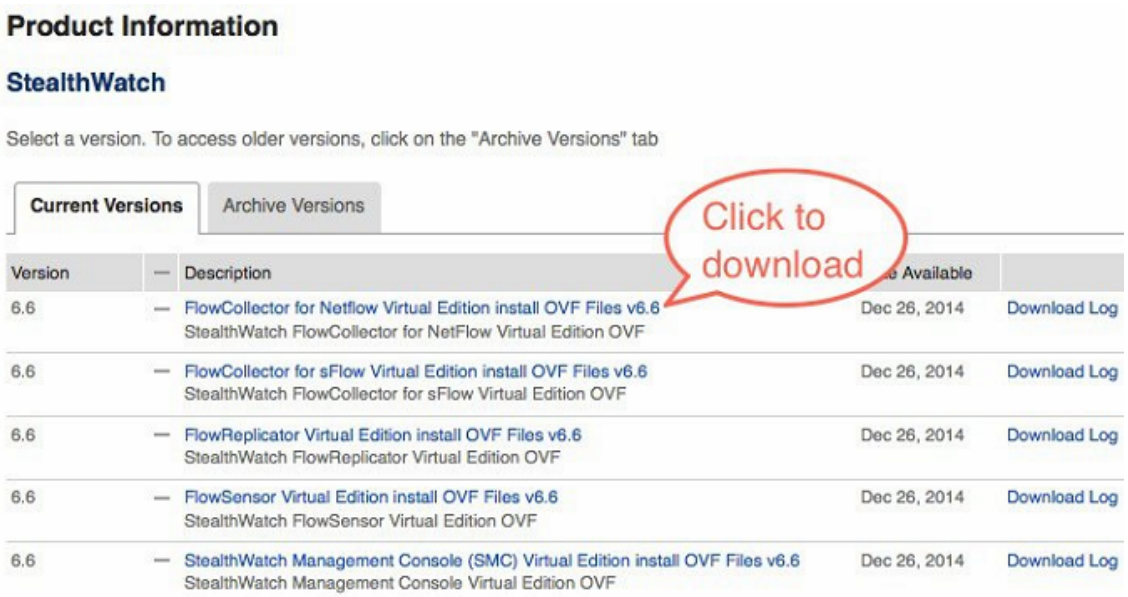
Lancope ソフトウェアは、次に示す URL からダウンロードできます。

https://www.lancope.com/stealthwatch-evaluation-application

1. Stealth Watch Evaluation にサインアップして、ソフトウェアをダウンロードします。



2. 次に最新の「FlowCollector for Netflow Virtual Edition install OVF Files v 6.6」をダウンロードします。



3. 詳細な設定情報については、『Lancope Installation Guide』を参照してください。

WLC での Netflow 設定

8.2 より前のリリースでは、WLC での Netflow 設定は、固定レコード ipv4_client_app_flow_record を Netflow モニタに関連付けることで行っていました。現在ではこの方法に加えて、ipv4_client_src_dst_flow_record という新しい固定レコードがサポートされています。これは以下に示す CLI と GUI でも使用できます。

(注)　コントローラで使用できる Netflow エクスポータは 1 つだけであるため、新旧のレコード形式のいずれかを使用することになります。

CLI からの設定

構成の変更内容

```
(Cisco Controller) > config flow add monitor <My_Netflow_Monitor record>
```

CLI からの設定手順

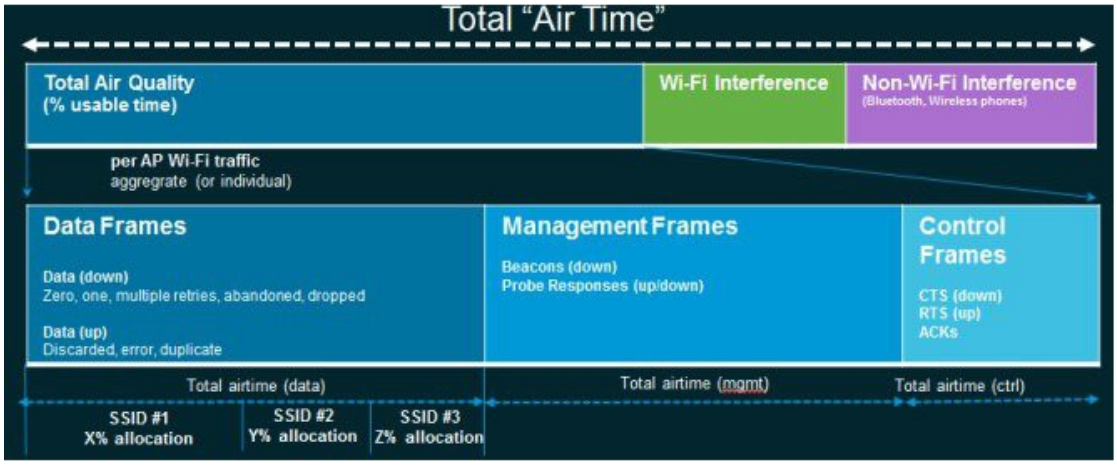
```
config flow create monitor <My_Netflow_Monitor>
config flow create exporter My_Netflow_Exporter A.B.C.D port 2055
config flow add monitor My_Netflow_Monitor exporter My_Netflow_Exporter
config flow add monitor My_Netflow_Monitor record ipv4_client_src_dst_flow_record
config wlan flow 1 monitor My_Netflow_Monitor enable
```

Air Time Fairness：ATF

Air Time Fairness（ATF）フェーズ 1 について

QoS の従来（有線）の実装は出力帯域幅を調整します。ワイヤレス ネットワーキングを使用して、伝送メディアはさまざまなレートでデータを送信する電波を介しています。出力帯域幅を調整する代わりに、フレームを送信するのに必要な通信時間量を調整するほうがより効果的です。Air Time Fairness（ATF）は、（出力帯域幅とは対照的に）ダウンリンク通信時間を調整するワイヤレス QoS の形式です。大規模で高密度の Wi-Fi 導入がこの機能を促進します。ワイヤレス ネットワークのオーナーは、アプリケーションに Wi-Fi ネットワークの全帯域幅の固定された割合を割り当てることを要求します。同時に、複数の携帯電話プロバイダーはオペレータ間で使用の公平性を維持する必要があります。

フレームが送信される前に、フレームを送信するのに十分な通信時間量があることを確認するために、その SSID 用の ATF 量がチェックされます。各 SSID は、トークン バケット（1 つのトークン = 通信時間の 1 マイクロ秒）を持つと見なされます。トークン バケット内にフレームを送信するために十分な通信時間が含まれる場合、無線で送信されます。それ以外は、フレームをドロップまたは保留できます。フレームのドロップについての概念は明確ですが、フレームの保留についてはさらに説明が必要です。フレームの保留とは、フレームがアクセス カテゴリ キュー（ACQ）に許可されないことを意味します。代わりに、クライアント プライオリティ キュー（CPQ）に残り、（フレームがドロップされる時点で、CPQ が容量に到達しなければ）対応するトークン バケットに十分な量のトークンが含まれたときに送信されます。ATF に関係する作業の大部分はアクセス ポイントで行われます。ワイヤレス コントローラは、機能を設定し、結果を表示するためだけに使用されます。



Cisco Air Time Fairness（ATF）の使用例

パブリック ホットスポット（スタジアム/空港/コンベンション センターなど）

この例では、パブリック ネットワークが複数のサービス プロバイダーおよび施設との間で WLAN を共有しています。各サービス プロバイダーのサブスクライバをグループ化して、各グループに特定の割合のエアタイムを割り当てることができます。

Education

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

一般企業、サービス業、小売業

この場合、施設は、従業員とゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービス プロバイダーによってさらに分割できます。ゲストはサービス レベルによってサブグループ化し、サブグループごとに一定の通信時間を割り当てることができます（有料のグループには、無料のグループよりも多く割り当てるなど）。

時間を共有するマネージド ホットスポット

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

ATF 機能

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

ATF の動作モード

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

- 無効モード：デフォルトでは、ATF は WLC で無効
- モニタ モード：ネットワークの通信時間の使用状況を監視する
- 適用—ポリシー モード：ATF ポリシーをネットワークに割り当てます。

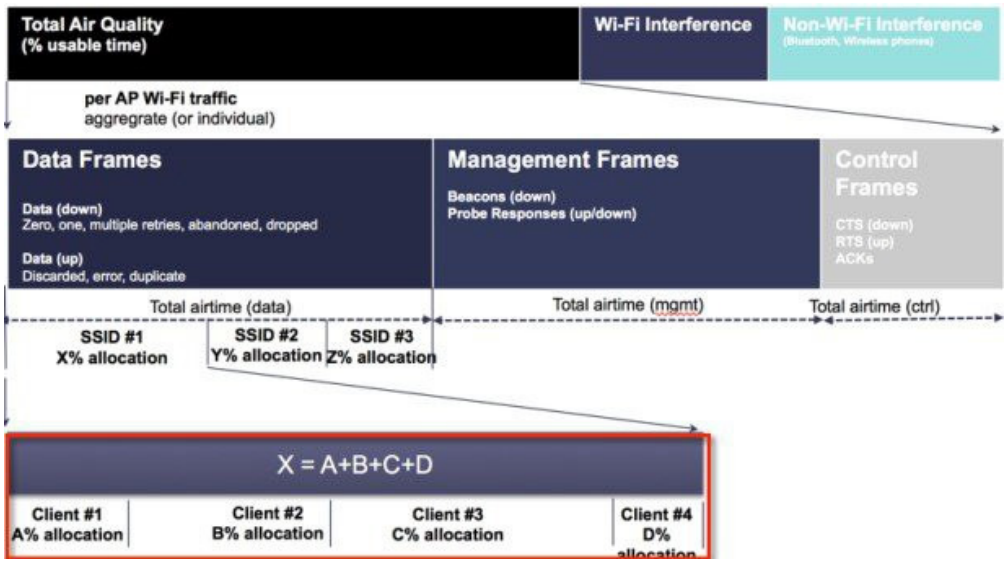
Air Time Fairness：Client Fair Sharing（ATF：フェーズ 2 リリース 8.2）

機能説明

クライアントごとの ATF Client Fair Sharing が 8.2 リリースで導入されます。クライアントの公平な共有によって、SSID/WLAN 内のクライアントが無線の帯域幅の使用率に基づいて均等に処理されるようにします。

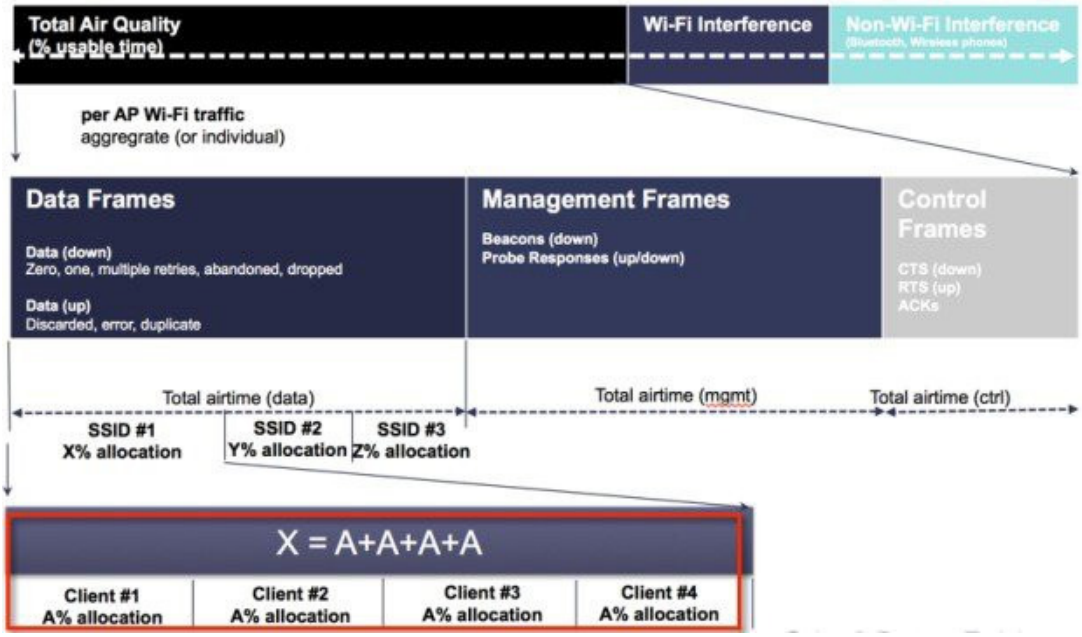
利点

8.2 より前のリリースでは、SSID に基づいてエアタイムが付与されていました。しかし SSID ベースの Airtime Fairness では、SSID 内のクライアントが、無線帯域幅の使用率に基づいて公平に扱われる保証がありません。それにより、1 つまたは少数のクライアントが、SSID/WLAN 全体に割り当てられているエアタイムをすべて使用してしまい、同じ SSID 内のクライアントの Wi-Fi 利用を阻害するリスクがあります。



この問題に対応するために、8.2 リリースでは、各 ATF ポリシーで、ポリシーに関するクライアント間の公平な分配を有効または無効にできるオプションが用意されています。このオプションを、ワイヤレス LAN コントローラで作成時に実行して、ポリシーを変更できます。カスタマーは、このオプションまたは機能を使用して、SSID に接続するクライアント間の通信時間の公平な共有を提供できます。次に示すように、SSID に接続するクライアントすべてが同じ通信時間を取得します。

ATF フェーズ 2（Client Fair Sharing を使用）



Mesh Deployments リリース 8.4 の Air Time Fairness

Mesh ATF は、ワイヤレス LAN コントローラの AireOS 8.4 リリース以上でサポートされています。Mesh ATF は、**1550-128Mb、1570、1700、2600、2700、3500、3600、3700** でサポートされています。

表 5-9

	アクセス ポイント						
	1550（64 MB）	**1550（128 MB）**	**1570**	**3700**	**1530**	**1540**	**1560**
機能							
基本メッシュ	Yes	Yes	Yes	Yes	Yes	はい	8.4
Flex+メッシュ	Yes	Yes	Yes	Yes	○	×	いいえ
高速コンバージェンス（バックグラウンドスキャン）	いいえ	8.3	8.3	Yes	8.3	いいえ	8.4

表 5-9

	アクセス ポイント						
	1550（64 MB）	**1550（128 MB）**	**1570**	**3700**	**1530**	**1540**	**1560**
RAP の有線クライアント	Yes	Yes	○	No	Yes	×	No
デイジーチェーン	7.6	7.6	7.6	いいえ	7.6	×	いいえ
LSC	Yes	Yes	Yes	Yes	○	×	いいえ
PSK プロビジョニング：MAP-RAP 認証	8.2	8.2	8.2	8.2	8.2	8.5	8.4
メッシュの ATF	いいえ	8.4	8.4	8.4	×	×	No

メッシュでの ATF 機能の概要

現時点では、Cisco IOS 11n、11ac Indoor AP によるエンタープライズ クラス、高密度スタジアム、およびその他主要な Wi-Fi 導入では、「SSID 単位」ベースの Airtime Fairness と、8.1 MR1 および 8.2 リリース以降による「SSID 内クライアント」ベースの Airtime Fairness が適用されています。

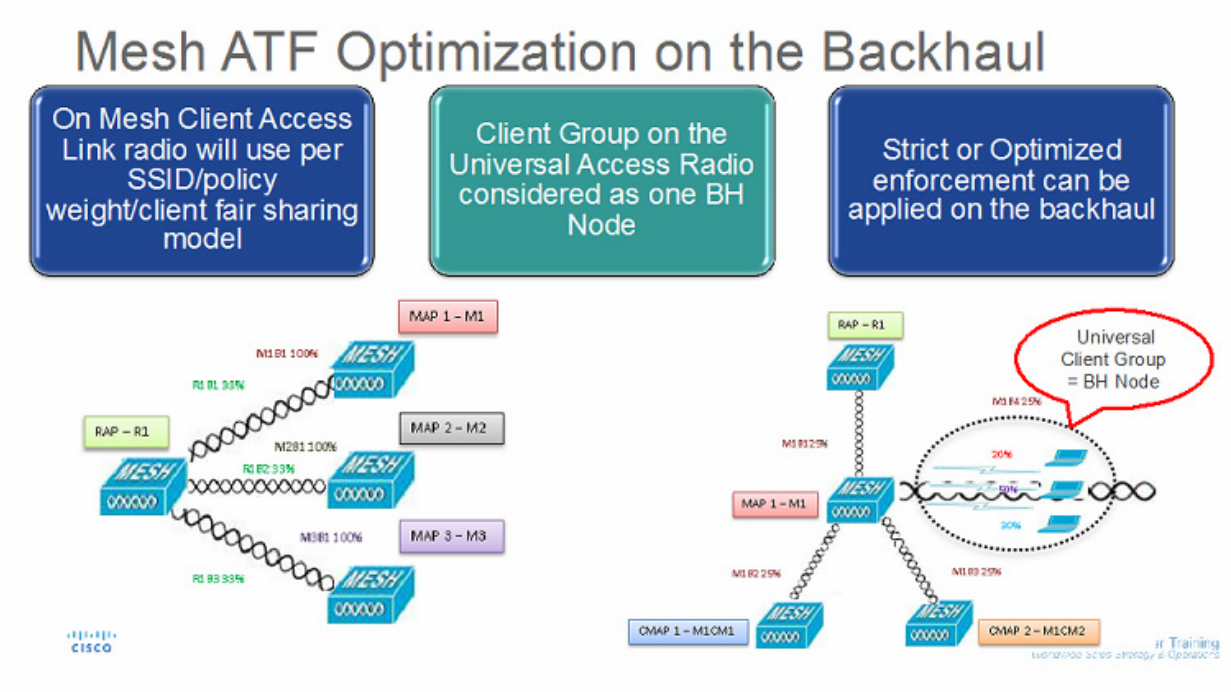
同様に、大規模な屋外ワイヤレス メッシュを導入しているお客様が要求していることは、AP 無線のエアタイム ダウンストリームの使用について屋外ワイヤレス メッシュ ネットワーク全体の Wi-Fi ユーザに公平性を提供し、また管理者が屋外ワイヤレス メッシュ ネットワーク全体の Wi-Fi ユーザにサービス レベル契約（SLA）（Wi-Fi ホットスポットを通じて複数の携帯電話事業者が実現）を提供できるようにすることです。ただし、Wi-Fi ユーザのトラフィックがすべて MAP と RAP 間でワイヤレス バックホール無線を通じてブリッジされることと、バックホール ノードのワイヤレス バックホール無線には SSID の概念がなく、SSID を通じて各バックホール ノードにポリシーが適用されないことにより、屋外ワイヤレス メッシュ ネットワーク全体の Wi-Fi ユーザが、屋外ワイヤレス メッシュ AP を通じて、Wi-Fi エアタイム利用の公平性を確保することは簡単ではありません。クライアント アクセス無線のクライアントに関する限り、シスコ ユニファイド ローカル モード AP と同様に、SSID（Client Fair Sharing あり/なし）を通じて Airtime Fairness を規制するのは容易です。

メッシュでの ATF サポートのソリューション概要を示す前に、ATF：Airtime Fairness（ATF）が基本的に、SSID を通じて関連付けられたクライアントについて、ダウンストリーム方向の AP 無線エアタイムを規制/適用する概念であることを確認しておきましょう。それにより、ワイヤレス ネットワークの Wi-Fi ユーザが、無線 WiFi エアタイムの使用について公平に扱われます。これによって、SLA を追加して適用するか、単純に特定のグループまたは個人が特定の AP 無線で WiFi エアタイムを不公平に使用することを拒否するかを制御できます。

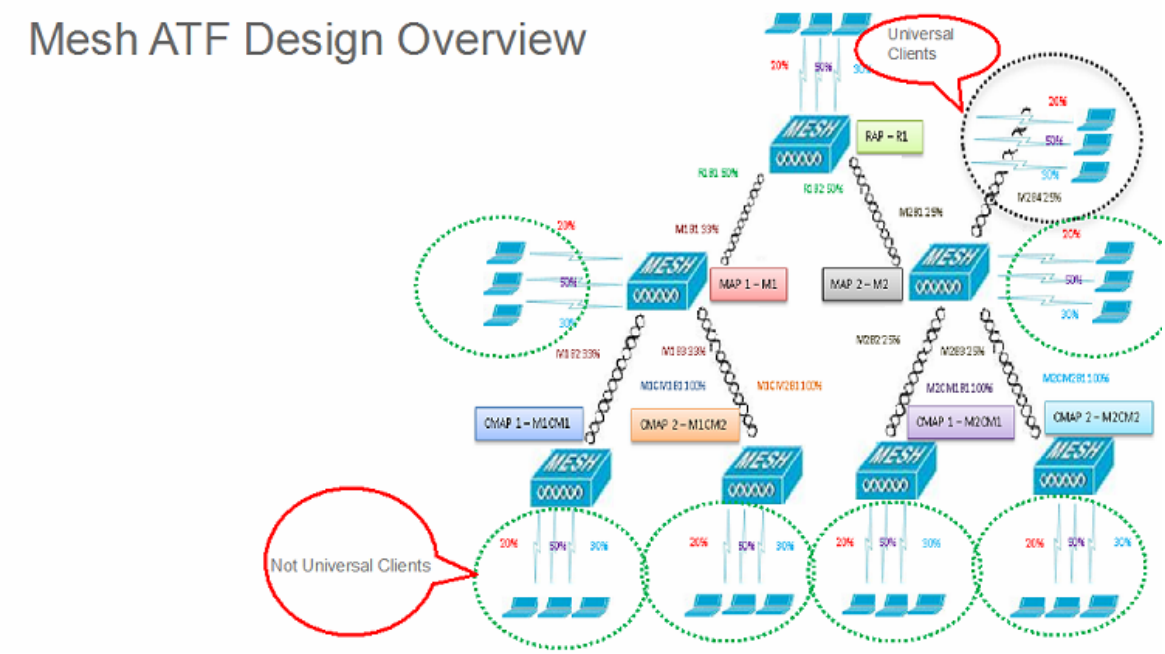
サービス レベル契約（SLA）とは、サービス プロバイダーが提供するサービス レベルを定義した、（内/外いずれかの）サービス プロバイダーとエンドユーザとの間の契約です。SLA は、顧客が利用できるサービスを定義するという点で、出力ベースであると言えます。

一般的にメッシュ アーキテクチャでは、メッシュ ツリー内のメッシュ AP（親、子 MAP）は、親と子 MAP 間のメッシュ接続用バックホール無線の同じチャネルにアクセスします（ここでは拡張サブバックホール無線は除外します）。一方、ルート AP はコントローラに有線接続され、MAP はコントローラに無線接続されます。そのため、すべての CAPWAP や Wi-Fi のトラフィックは、無線バックホールおよび RAP によりコントローラに接続されます。物理的な配置について言えば、RAP は一般にルーフ トップに配置され、複数のホップにある MAP は（メッシュ ネットワークのセグメント化ガイドラインに基づき）間隔を置いて配置されます。そのためメッシュ ツリー内の各 MAP は、各 MAP が同じメディアにアクセスするにも関わらず、本体のダウンストリーム キャパシティを 100 % ユーザに提供できます。メッシュ以外のシナリオでは、異なるルームで隣接するローカル モードのユニファイド AP が、同じチャネル上のそれぞれのクライアントに 100 % の無線エアタイム ダウンストリームを提供することになります。この場合 ATF は、同じメディアにアクセスする異なる 2 つの隣接 AP でクライアントの適用を制御できません。これはメッシュ ツリー内の MAP についても同様です。

屋外/屋内のメッシュ AP については、非メッシュのユニファイド ローカル モード AP で現在 ATF をサポートしているのと同様に、Airtime Fairness を、通常のクライアントにサービスを提供するクライアント アクセス無線でサポートする必要があります。また、RAP に対するクライアント アクセス無線（1 ホップ）または RAP に対する MAP（複数のホップ）によってクライアント間のトラフィックをブリッジする、バックホール無線でもサポートする必要があります。同じ SSID/ポリシー/ウェイト/クライアントの Fair Sharing モデルによってバックホール無線の ATF をサポートする方法は、多少複雑になります。バックホール無線には SSID がなく、常に隠されたバックホール ノードを通じてトラフィックがブリッジされます。そのため、RAP または MAP のバックホール無線では、バックホール ノード数に基づいて無線エアタイム ダウンストリームが公平に分配されます。この方法によって問題が解消され、2 番目のホップ MAP が 1 番目のホップ MAP にバックホール無線を通じてワイヤレス接続されている状況で、2 番目のホップ MAP に関連付けられているクライアントが 1 番目のホップ MAP に関連付けられているクライアントをストールさせた場合に、MAP 内の Wi-Fi ユーザが物理的に離れていても、ワイヤレス メッシュ ネットワーク全体のユーザが公平に扱われます。このシナリオでは、バックホール無線でユニバーサル クライアント アクセス機能を通じて通常のクライアントにサービスを提供できる場合、ATF は通常のクライアントを単一ノード内にグループ化します。ノードの数（バックホール ノード+通常のクライアントに対する単一ノード）に基づいて、ダウンストリームの無線通信時間を等しく公平に共有します。以下の項では、このソリューションを設計に適用する方法を詳細に示します。



さらに規模の大きなメッシュ設計はこのようになります



ATF の動作モード

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

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

設定と導入の詳細については、次のリンクから『ATF Deployment Guide（ATF 導入ガイド）』を参照してください。

http://www.cisco.com/c/en/us/support/wireless/wireless-lan-controller-software/products-technical-reference-list.html

Cisco Unified Wireless のマルチキャスト設計

はじめに

この章では、Cisco Unified Wireless Network の IP マルチキャスト転送について説明し、ワイヤレス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、コントローラとアクセス ポイント（AP）の間のすべてのルータに設定されている必要があります。マルチキャストをサポートしないネットワークに対応するため、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、情報を宛先の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率的な戦略を使用しています。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、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。すなわち、1 つの送信元に 1 つの宛先が対応します。しかし、複数の受信先で同じデータが必要な場合、送信元からすべての受信先に対して個別のユニキャスト パケットと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。

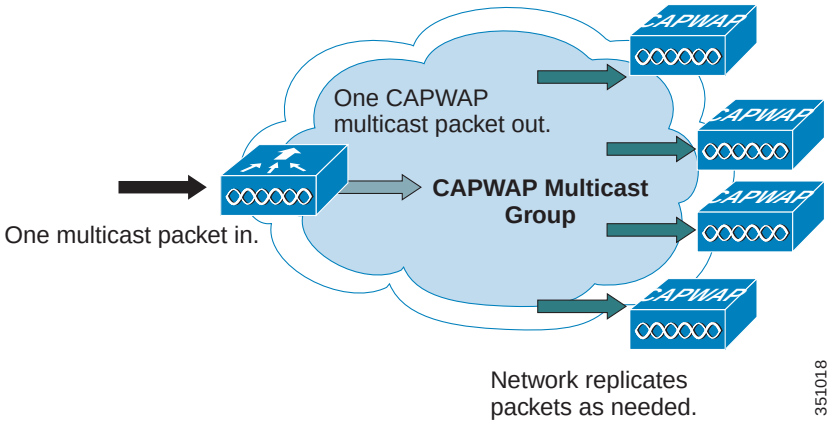
現在、受信先の大規模なグループに宛てた一方向のストリーミング　メディア（ビデオなど）には、通常 IP マルチキャストが使用されています。多くのケーブル テレビ局、教育機関、および大企業では、コンテンツ配信のために IP マルチキャストが展開されています。さらに、マルチキャストを使用した音声およびビデオ会議も利用されています。その他、キャンパスおよび商用ネットワークでマルチキャストが広く使用されている例として、ファイルの配信があります。特に、オペレーティング システムのイメージおよびアップデートをリモート ホストに配信する場合などです。また、金融部門において、株価情報表示および hoot-n-holler システムなどのアプリケーションのために IP マルチキャストが展開されています。

IPv4 マルチキャスト転送の概要

Cisco Unified Wireless Network ソフトウェアのリリースでは、ワイヤレス ネットワークで効果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。

現在の Cisco Unified Wireless マルチキャスト サポートでは、ファースト ホップ ルータに接続されている VLAN からコントローラが受信した各マルチキャスト フレームがコピーされ、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（図 6-1 を参照）。マルチキャスト パケットを含むマルチキャスト CAPWAP 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 の受信側 AP が通知されます。AP が CAPWAP パケットを受信すると、AP は外部 CAPWAP カプセル化を解除し、CAPWAP 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）WLAN にマルチキャスト パケットを送信します。

図 6-1　　マルチキャスト転送メカニズム



グローバル マルチキャスト モードを有効にすると、各アクセス ポイントにマルチキャスト パケットが配信されます。これにより、ネットワーク内のルータが標準的なマルチキャスト テクノロジーを使用して、AP に対してマルチキャスト パケットを複製および配信できるようになります。CAPWAP マルチキャスト グループの場合は、コントローラがマルチキャスト送信元になり、AP がマルチキャスト受信側になります。

（注）　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 AP の間のすべてのルータに設定されます。マルチキャストをサポートしないネットワークに対応するため、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 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、すべてのルータ、ルーティング プロトコルおよび PIM マルチキャスト パケットを含め、ワイヤレス 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）、CAPWAP マルチキャスト グループを設定し、IGMP スヌーピングを有効にすると、コントローラへの通常の参加プロセス中（ブート時）に、アクセス ポイントがコントローラの CAPWAP マルチキャスト グループのアドレスをダウンロードします。アクセス ポイントがコントローラに参加し、コントローラの設定をダウンロードした後、その AP はコントローラの CAPWAP マルチキャスト グループに参加するための Internet Group Management Protocol（IGMP）Join 要求を発行します。これにより、マルチキャスト対応ルータで、コントローラと AP の間のマルチキャスト ステートに関する通常のセットアップが開始されます。マルチキャスト グループの送信元 IP アドレスは、レイヤ 3 モードに使用される AP マネージャの IP アドレスではなく、コントローラの管理インターフェイスの IP アドレスです。AP がコントローラの CAPWAP マルチキャスト グループに参加すると、クライアントのマルチキャスト トラフィックのマルチキャスト アルゴリズムは次のように動作します。

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

- コントローラでは、ファースト ホップ ルータ上の任意のクライアント VLAN からマルチキャスト パケットを受信した場合、管理インターフェイスを介して、ベスト エフォートの QoS 分類で、CAPWAP マルチキャスト グループにパケットを送信します。CAPWAP 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、CAPWAP マルチキャスト パケットが、CAPWAP マルチキャスト グループに参加している各アクセス 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 を参照）。これにより、コントローラでは、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、現在の参加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。元のマルチキャスト パケットの送信元である VLAN インターフェイスに複数の WLAN が関連付けられていた場合、AP は各 WLAN を使用してマルチキャスト パケットを送信します（CAPWAP ヘッダー内の WLAN ビットマップに従う）。さらに、WLAN が両方の無線（802.11g と 802.11a）上にある場合、関連付けられたクライアントがあれば、そのクライアントでマルチキャスト トラフィックを要求しなかった場合でも、両方の無線で WLAN SSID 宛てにマルチキャスト 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ワイヤレス クライアント上にある場合

- マルチキャスト パケットは、標準のワイヤレス クライアント トラフィック同様に、AP からコントローラへの（CAPWAP カプセル化された）ユニキャストです。
- コントローラは、マルチキャスト パケットのコピーを 2 つ作成します。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 に関連付けられている VLAN から送信されます。これにより、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、CAPWAP カプセル化され、ワイヤレス 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、CAPWAP マルチキャスト グループに送信されます。

ワイヤレス マルチキャスト ローミング

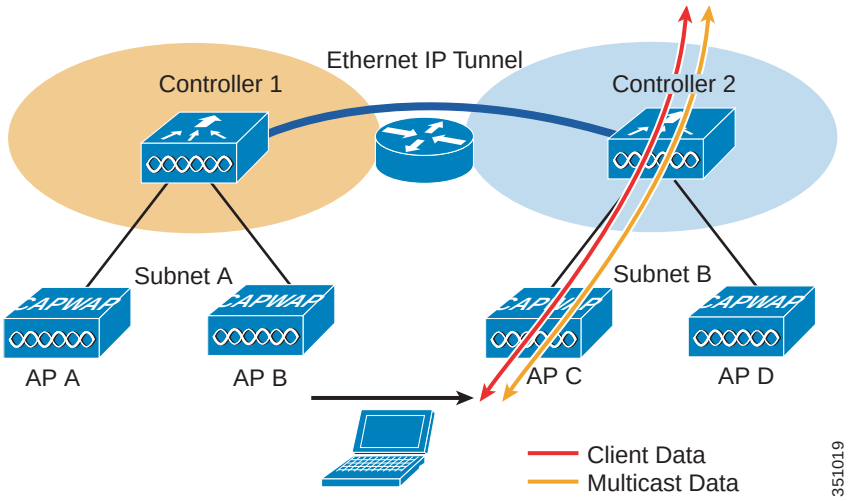
ワイヤレス環境のマルチキャスト クライアントでは、WLAN 内を移動するときのマルチキャスト グループ メンバーシップの維持が大きな課題となります。AP 間の移動時にワイヤレス接続でパケットがドロップすると、クライアントのマルチキャスト アプリケーションが中断する場合があります。グループ メンバーシップ情報の動的メンテナンスでは、Internet Group Management Protocol（IGMP）が重要な役割を果たします。

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ために重要です。レイヤ 2 ローミングの場合、適切に設定されている外部 AP であればすでにそのマルチキャスト グループに属しており、トラフィックはネットワーク上の別のアンカー ポイントにトンネリングされないため、セッションはそのまま維持されます。レイヤ 3 ローミング環境では仕組みがもう少し複雑で、コントローラに設定したトンネリング モードによって異なっており、ワイヤレス クライアントから送信された IGMP メッセージに影響します。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 モードは非対称です。第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」で説明したとおり、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、関連付けられた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。発信パケットは、外部 WLC インターフェイスに向けて転送されます。同期モビリティ トンネリング モードでは、着信と発信の両方のトラフィックがアンカー コントローラまでトンネリングされます。モビリティ トンネリングの詳細については、第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照してください。

非対称マルチキャスト トンネリング

非対称マルチキャスト トンネリングでは、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 にクライアントが移動すると、外部 WLC によってマルチキャスト グループ メンバーシップがクエリされ、IGMP グループ メンバーシップ レポートが送信されます。IGMP グループ メンバーシップ レポートは VLAN に割り当てられた外部 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 ストリームに再度参加します。図 6-2 では、通常のデータとマルチキャスト データのトラフィック フローを示します。

図 6-2　非対称トンネリング



（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るため、アプリケーションによっては使用に適してい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 AP の間のすべてのルータに設定されます。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、単一の情報ストリームを企業の何千もの受信者に同時に配信することによってトラフィックを削減する技術であり、帯域幅を大量に消費します。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 の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については、次の URL を参照してください。
http://www.cisco.com/go/multicast

CAPWAP マルチキャスト予約ポートおよびアドレス

コントローラは、5246、5247、および 5248 の宛先ポートを持つマルチキャスト グループに送信されたすべてのマルチキャスト パケットをブロックします。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 CAPWAP 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、フラグメント化された CAPWAP 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（詳細については、フラグメンテーションと CAPWAP 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 CAPWAP 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 IPv4 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には、次の手順に従います。

IPv4 マルチキャスト モードの有効化（GUI）

ステップ 1　[Controller] > [Multicast] の順に選択して [Multicast] ページを開きます。

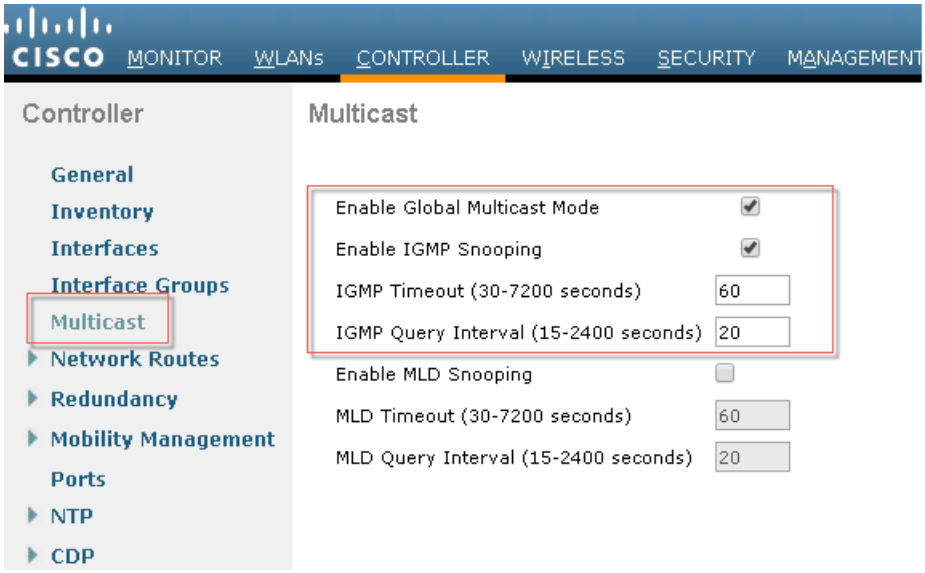
ステップ 2　[Enable Global Multicast Mode] チェックボックスをオンにして、マルチキャスト パケットの送信を設定します。デフォルト値は [disabled] です。

（注）　FlexConnect では、ユニキャスト モードのみがサポートされています。

ステップ 3　IGMP スヌーピングを有効にする場合は、[Enable IGMP Snooping] チェックボックスをオンにします。IGMP スヌーピングを無効にするには、チェックボックスをオフのままにします。デフォルト値は [disabled] です。

ステップ 4　IGMP タイムアウトを設定するには、30 ～ 7200 秒の範囲内の値を [IGMP Timeout] テキスト ボックスに入力します。特定のマルチキャスト グループに対してクライアントが存在するかどうかを確認するために、コントローラから、1 つのタイムアウト値につき 3 つのクエリーが *timeout/3* の間隔で送信されます。クライアントから、IGMP レポートを通じて応答を受け取らなかった場合、コントローラはこのクライアントのエントリを MGID テーブルからタイムアウトします。特定のマルチキャスト グループに対するクライアントが残されていない場合、クライアントは IGMP タイムアウト値が経過するまで待ってから、コントローラから MGID エントリを削除します。一般的な IGMP クエリー（つまり、宛先アドレス 224.0.0.1）がコントローラによって必ず生成され、MGID 値 1 を使用してすべての WLAN 上で送信されます。

ステップ 5　IGMP クエリー間隔（秒数）を入力します。



IGMP スヌーピングが無効になっている場合は、次のようになります。

- コントローラは、マルチキャスト データをアクセス ポイントへ送信する際は必ずレイヤ 2 MGID を使用します。作成された各インターフェイスには、1 つのレイヤ 2 MGID が割り当てられます。たとえば、管理インターフェイスの MGID は 0 となります。また、作成された 1 つ目の動的インターフェイスに割り当てられる MGID は 8 となり、動的インターフェイスが作成されるにつれて 1 増えます。
- クライアントからの IGMP パケットはルータへ転送されます。それにより、ルータの IGMP テーブルは、最後のレポータとしてクライアントの IP アドレスで更新されます。

IGMP スヌーピングが有効になっている場合は、次のようになります。

- コントローラは、アクセス ポイントへ送信されるすべてのレイヤ 3 マルチキャスト トラフィックに必ずレイヤ 3 MGID を使用します。すべてのレイヤ 2 マルチキャスト トラフィックについては、引き続きレイヤ 2 MGID を使用します。
- ワイヤレス クライアントからの IGMP レポート パケットは、クライアントに対するクエリーを生成するコントローラによって消費または吸収されます。ルータによって IGMP クエリーが送信されると、コントローラによって IGMP レポートが送信されます。このレポートでは、コントローラのインターフェイス IP アドレスがマルチキャスト グループのリスナー IP アドレスとして設定されています。それにより、ルータの IGMP テーブルは、マルチキャスト リスナーとしてコントローラ IP アドレスで更新されます。

- マルチキャスト グループをリッスンしているクライアントが、あるコントローラから別のコントローラへローミングしたときは、リッスンしているクライアント用のすべてのマルチキャスト グループ情報が、最初のコントローラから 2 番目のコントローラへ送信されます。それにより、2 番目のコントローラは、クライアント用のマルチキャスト グループ情報をただちに作成できます。2 番目のコントローラでは、クライアントがリッスンしていた全マルチキャスト グループのネットワークに IGMP レポートが送信されます。このプロセスは、クライアントへのマルチキャスト データのシームレスな転送に役立ちます。
- リッスンしているクライアントが、別のサブネットのコントローラにローミングした場合は、マルチキャスト パケットは、Reverse Path Filtering（RPF; 逆方向パス転送）のチェックを避けるために、クライアントのアンカー コントローラへトンネリングされます。アンカーは、マルチキャスト パケットをインフラストラクチャ スイッチへ転送します。MGID はコントローラ固有です。2 つの異なるコントローラの同一 VLAN から送られて来る同一マルチキャスト グループのパケットは、2 つの異なる MGID へマップされる可能性があります。

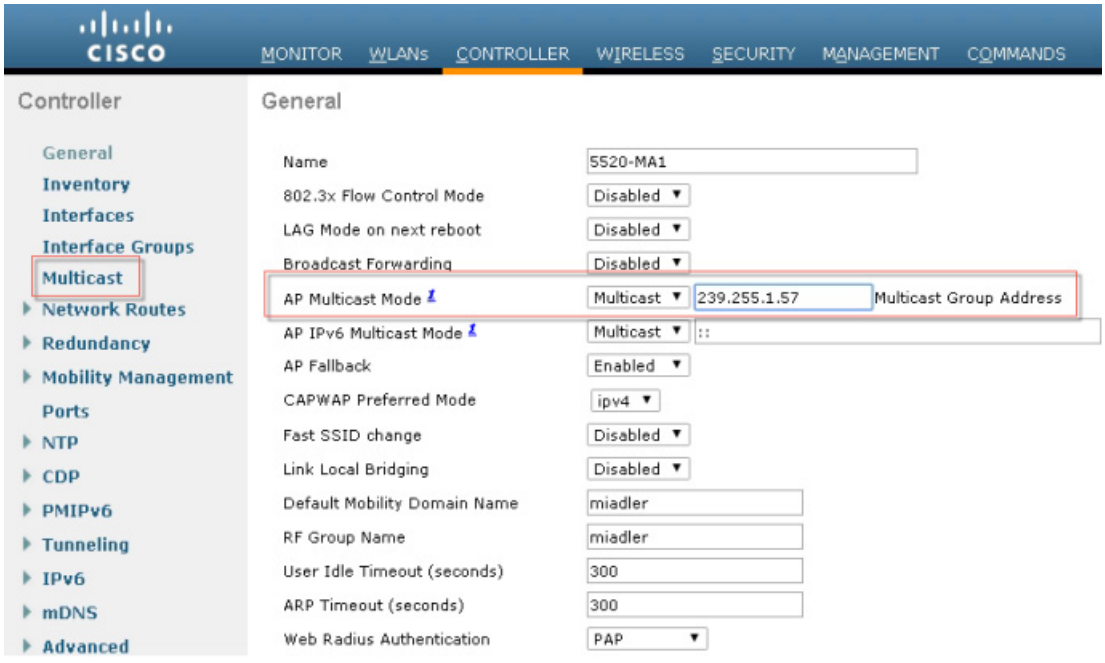
（注）　Cisco WLC の VLAN ごとにサポートされるマルチキャスト アドレス数は 100 です。

ステップ 6　マルチキャスト対応ネットワークがある場合は、[AP Multicast Mode] ドロップダウン リストから [Multicast] を選択して、ネットワークがパケットを複製する方式を使用します。

ステップ 7　マルチキャスト対応ネットワークがない場合は、[AP Multicast Mode] ドロップダウン リストから [Unicast] を選択して、コントローラがパケットを複製する方式を使用します。

ステップ 8　[AP Multicast Mode] ドロップダウン リストから [Multicast] を選択し、マルチキャスト グループ アドレスを入力します。図 6-3 にオプションを示します。

図 6-3　GUI を使用してイーサネット マルチキャスト モードを有効にするコマンド



マルチキャスト モードについて

ネットワークがパケット マルチキャストをサポートしている場合は、コントローラで使用されるマルチキャストの方法を設定できます。

コントローラは次の 2 つのモードでマルチキャストを実行します。

ユニキャスト モード:コントローラにアソシエートしているすべてのアクセス ポイントに、すべてのマルチキャスト パケットがユニキャストされます。このモードは非効率的ですが、マルチキャストをサポートしないネットワークでは必要な場合があります。

マルチキャスト モード:マルチキャスト パケットは CAPWAP マルチキャスト グループに送信されます。この方法では、コントローラ プロセッサのオーバーヘッドが軽減され、パケット レプリケーションの作業はネットワークに移されます。これは、ユニキャストを使った方法より、はるかに効率的です。

マルチキャスト モードが有効な場合に、コントローラがマルチキャスト パケットを有線 LAN から受信すると、コントローラは CAPWAP を使用してパケットをカプセル化し、CAPWAP マルチキャスト グループ アドレスへ転送します。コントローラは、必ず管理インターフェイスを使用してマルチキャスト パケットを送信します。マルチキャスト グループのアクセス ポイントはパケットを受け取り、クライアントがマルチキャスト トラフィックを受信するインターフェイスにマップされたすべての BSSID にこれを転送します。アクセス ポイントからは、マルチキャストはすべての SSID に対するブロードキャストのように見えます。

マルチキャストの展開に関する考慮事項

CAPWAP マルチキャスト アドレスを選択する際の推奨事項

注意　お勧めはしませんが、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 CAPWAP マルチキャスト グループに割り当てることができます。

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推奨します。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 の範囲を予約しています（その他の制限については下記を参照）。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、自律システム（AS）を出入りしないようブロックする必要があります。

（注）　アドレス範囲 239.0.0.*X* および 239.128.0.*X* は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 ローカル MAC アドレスとオーバーラップし、IGMP スヌーピングがオンの場合でも、すべてのスイッチ ポートに向けてフラッディングします。

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」を限定することを推奨します。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。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ワイヤレス ネットワークに到達することも防止できます。

マルチキャスト アドレスのガイドラインの詳細については、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

フラグメンテーションと CAPWAP 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 CAPWAP マルチキャスト グループを使用して CAPWAP 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。パケットがリンクの MTU を超える場合は、コントローラによってパケットがフラグメント化され、両方のパケットが CAPWAP 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 CAPWAP 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、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、いずれも単独で有効です。1 つ目は、すべてのコントローラを同じ CAPWAP マルチキャスト グループ アドレスに割り当てるオプションです。2 つ目は、標準のマルチキャスト フィルタリング技術を適用して、CAPWAP 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するオプションです。すべてのコントローラが同一の CAPWAP マルチキャスト グループを保持しているか、または異なる CAPWAP マルチキャスト グループを保持しているかによって、これらの 2 つの手法には、表 6-1 に示す長所と短所があります。

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

操作	長所	短所
すべてのコントローラの CAPWAP マルチキャスト グループが同一である	フラグメンテーション保護対策を施す必要がない	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する（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る）
標準のマルチキャスト技術を使用して CAPWAP 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る	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 上のファーストホップ ルータに ACL フィルタリングを適用する必要がある

すべてのコントローラの CAPWAP マルチキャスト グループが同一である

2 つ目のコントローラからこれらの CAPWAP カプセル化パケットが再送信されないように、コントローラが CAPWAP マルチキャスト グループおよび CAPWAP 予約済み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。予約済み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 CAPWAP マルチキャスト パケットのフラグメント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、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、コントローラに割り当てられている CAPWAP マルチキャスト グループ アドレスと宛先アドレスが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 CAPWAP マルチキャスト グループに割り当てると、別の問題が発生します。CAPWAP マルチキャスト グループへ参加するために AP が使用する IGMP バージョン 1 および 2 は、Any Source Multicast（ASM）であるため、AP 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送信されたマルチキャスト トラフィックを受信します。これは、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、AP はすべて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ないことを意味します。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 はネットワーク全体のワイヤレス 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）。また、ローカルで送信された 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。

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** インターフェイス　モード　コマンドの使用が含まれます。

（注）　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、CAPWAP 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（マルチキャスト境界が適用されていない場合）。マルチキャスト ストリームが CAPWAP マルチキャスト パケットにカプセル化されている場合、マルチキャスト ストリーム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推奨します。

これまでは、IP マルチキャスト データグラムのパケット存続時間（TTL）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。この作業は、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** インターフェイス モード コマンドの使用に取って代わられています。シスコは新しいコマンドを使用することを推奨します。

その他の便利なコマンドとして、**ip multicast rate-limit interface** コマンドがあります。このコマンドは、ワイヤレス VLAN に低レートを強制します。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しても、低レート マルチキャスト アドレスがそのレートを超過できなくなります。

ワイヤレス クライアント VLAN の一般的な例は次のとおりです。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 コマンドの詳細については、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でフィルタリングを実行することによって、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（Sasser ワームなど）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、下位の管理スコープ アドレスには含まれないすべてのマルチキャスト アドレスにも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参加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 トラフィックと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 は適用できません。マルチキャスト トラフィックが有効になると、HSRP、EIGRP、OSPF、および PIM パケットを含むすべてのマルチキャスト トラフィックがワイヤレス LAN に転送されます。

ここでは、分散型と中央集中型の 2 つの異なる展開と、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/サブネットにアタッチされ、マルチキャスト クライアントがある WLC の AP から他の WLC の AP に移動する際、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ないのは、マルチキャスト ストリームが WLAN 上の 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 つもアクセス ポイントの WLAN に関連付けられていなくても、この WLAN、すべての無線（802.11g および 802.11a）およびすべての WLC に接続されているすべての AP に対してマルチキャスト ストリームが出力されるためです。VLAN に関連付けられている 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 CAPWAP 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 にアタッチされるため、このような問題はありません。このことは、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 メンバーシップを最初にクエリすることを意味します。この時点で、クライアントはグループ メンバーシップ レポートを返信します。このメッセージは WLC によって、ローカル VLAN に関連付けられた VLAN 経由で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 にアタッチされているため、AP 上のマルチキャスト トラフィックの量が削減されます。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 で、分散型展開と中央集中型展開の長所と短所を示します。

表 6-2　中央集中型 WLC 展開および分散型 WLC 展開の長所と短所

配置	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 ストリームを受信する	1 つのクライアントのみがマルチキャスト トラフィックを要求した場合、すべてのコントローラにアタッチされているすべての AP がストリームを受信し、AP に関連付けら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、その AP がストリームを送信する
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、コントローラにアタッチされている AP に分離される	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が生じる

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 FlexConnect と AP の実装時です。AP グループでは、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 間でクライアントが移動すると、マルチキャスト セッションが正しく機能しません。それは、この動作が現在サポートされていないためです。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。

FlexConnect 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。FlexConnect 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、FlexConnect ネットワークの場所まで CAPWAP 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 FlexConnect WLAN に配信されます。

CAPWAP マルチキャスト パケットがネットワークを FlexConnect AP に送信できない場合でも、これらのパケットはユニキャスト メッセージであるため、その FlexConnect AP 上の 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 Join 要求を送信できます。

802.11v およびダイレクト マルチキャストに関する情報

リリース 8.1 から、コントローラは、ワイヤレス ネットワーク管理に対するさまざまな機能拡張について記載されたワイヤレス ネットワークに関する 802.11v 改訂をサポートします。

このような機能強化の 1 つがクライアントでスリープ時間を延ばしてバッテリ寿命を改善できるようにする**ネットワーク支援型電力節約**です。たとえば、多くのモバイル デバイスは、特定のアイドル期間を利用してアクセス ポイントとの接続を維持するため、ワイヤレス ネットワークで以降のタスクを実行するときにより多くの電力を消費します。

もう 1 つの機能強化は、WLAN 上で関連付けられたクライアントに要求を送信して、アドバタイズにより、適切な AP をクライアントが選択できるようにする**ネットワーク支援型ローミング**です。これは、ロード バランシングと、接続が不安定なクライアントの管理の両方に役立ちます。

802.11v Network Assisted Power Savings の有効化

ワイヤレス デバイスはクライアントへの接続を維持するためにさまざまな方法でバッテリを消費します。

- 定期的に起動して DTIM を含むアクセス ポイント ビーコンをリッスンする。DTIM は、アクセス ポイントがバッファされたブロードキャストとマルチキャスト トラフィックのどちらをクライアントに提供するかを示します。
- アクセス ポイントとの接続を維持するために、null フレームをキープアライブ メッセージの形式でアクセス ポイントに送信します。
- デバイスは、定期的に、ビーコンをリッスン（DTIM フィールドがない場合も）して、対応するアクセス ポイントとクロックを同期させます。

このすべてのプロセスがバッテリを消費し、その消費は特にデバイス（Apple など）に影響します。これは、これらのデバイスが保守的なセッション タイムアウト推定を使用しているために、頻繁にスリープ解除してキープアライブ メッセージを送信するためです。802.11 標準は、802.11v なしのローカル クライアントのセッション タイムアウトの無線クライアントと通信するため、コントローラまたはアクセス ポイントの機能は含まれていません。

ワイヤレス ネットワーク上の上記タスクによるクライアントの電力を節約するために、802.11v 標準の次の機能が使用されます。

- Directed Multicast Service
- Base Station Subsystem（BSS）最大アイドル期間

Directed Multicast Service

Directed Multicast Service（DMS）を使用して、クライアントは、必要なマルチキャスト パケットをユニキャスト フレームとして送信するようにアクセス ポイントに要求します。それによりクライアントは、スリープ モードで無視していたマルチキャスト パケットを受信し、またレイヤ 2 の信頼性を確保できます。また、ユニキャスト フレームができるだけ高いワイヤレス リンク レートでクライアントに送信されるため、クライアントは無線の持続期間を短縮してパケットをすばやく受信できるようになり、バッテリの電力が節約されます。ワイヤレス クライアントはマルチキャスト トラフィックを受信するために DTIM 間隔ごとにスリープ解除する必要がないため、スリープ間隔を延ばすことができます。

BSS の最大アイドル時間

BSS 最大アイドル期間は、アクセス ポイント（AP）が接続先のクライアントからフレームが受信されないという理由でそのクライアントの関連付けを解除しないタイムフレームです。これにより、クライアント デバイスがキープアライブ メッセージを頻繁に送信しないようになります。アイドル期間タイマー値は、アクセス ポイントからクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。このアイドル時間値は、クライアントがアクセス ポイントにフレームを送信せず、アイドル状態を維持可能な最大時間を意味します。したがって、クライアントは、キープアライブ メッセージを頻繁に送信することなく、より長い間スリープ モードを維持します。これがバッテリの電力の節約につながります。

802.11v Network Assisted Power Savings（CLI）の設定

- BSS 最大アイドル期間の値を設定するには、次のコマンドを入力します。
  - **config wlan usertimeout** *wlan-id*
  - **config wlan bssmaxidle {enable | disable}** *wlan-id*
- DMS を設定するには、次のコマンドを入力します。
  - **config wlan dms {enable | disable}** *wlan-id*

IPv6 マルチキャストの概要

マルチキャスト アドレスは、異なるノードに属する一連のインターフェイスに対応する ID です。マルチキャスト アドレスは、通常、同様のコンテンツ（ビデオなど）の受信に関心のあるインターフェイス グループを識別するために使用されます。この場合のメッセージ交換モデルは、1 対多モデルです。マルチキャスト アドレスはすべて FF00::/8 ブロックの中から割り当てられます。

また、マルチキャスト アドレスには関連付けられたスコープがあります。スコープは、ユニキャスト アドレス用に定義されたスコープとよく似ています。

- リンク ローカル：リンク ローカル マルチキャスト アドレスは、リンク上のシステムのみで使用され、ネットワーク機器によってそのリンクから転送されることはありません。この動作は、リンク ローカル ユニキャスト アドレスと同様です。
- オーガナイゼーション：オーガナイゼーション マルチキャスト アドレスは、組織内でのみ使用されます。これらのアドレスは、ユニキャストのユニーク ローカル アドレスと同様です。
- グローバル：グローバル マルチキャスト アドレスは、ユニキャストのグローバル一意アドレスと同様に、インターネット上で使用できます。

IPv6 マルチキャスト アドレス用に追加で定義されたスコープがあります。

- インターフェイス ローカル：インターフェイス ローカル マルチキャスト アドレスは、ノード内でのマルチキャストの伝送に使用されます。
- サイト ローカル：サイト ローカル マルチキャスト アドレスは、単一サイト内で使用されます。

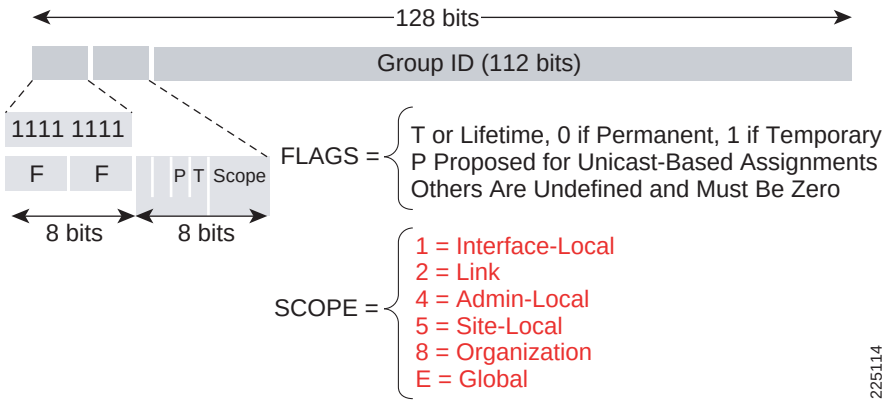
図 6-4 は、IPv6 マルチキャスト アドレス形式を示しています。

ユニキャスト アドレス空間と同様に、いくつかの予約済みのマルチキャスト アドレスや特殊用途のマルチキャスト アドレスがあります。一般的なマルチキャスト グループとその用途を以下に示します。現在割り当てられているマルチキャスト アドレスの詳細なリストについては、次の URL を参照してください。http://www.iana.org/assignments/ipv6-multicast-addresses

IPv6 システムで見られるより一般的なマルチキャスト アドレスには次が含まれます。

- FF02::1：リンク ローカル、すべてのノードのアドレス
- FF02::2：リンク ローカル、すべてのルータのアドレス
- FF02:0:0:0:0:1:FFXX:XXXX：リンク ローカル、要請ノード アドレス

図 6-4　　マルチキャスト アドレスの形式



マルチキャスト リスナー検出（MLD）

シスコ ソフトウェアでは、IPv6 マルチキャスト ルーティングを実装するため、次のプロトコルがサポートされています。

- MLD for IPv6。MLD は、直接アタッチされているリンク上のマルチキャスト リスナー（特定のマルチキャスト アドレスを宛先としたマルチキャスト パケットを受信するために使用するノード）を検出するために IPv6 ルータとコントローラで使用されます。MLD には 2 つのバージョンがあります。MLD バージョン 1 はバージョン 2 のインターネット グループ管理プロトコル（IGMP）for IPv4 をベースとしています。MLD バージョン 2 はバージョン 3 の IGMP for IPv4 をベースとしています。シスコ ソフトウェアの IPv6 マルチキャストでは、MLD バージョン 2 と MLD バージョン 1 の両方が使用されます。
  MLD バージョン 2 は、MLD バージョン 1 と完全な下位互換性があります（RFC 2710 で規定）。MLD バージョン 1 だけをサポートするホストは、MLD バージョン 2 を実行しているルータと相互運用します。MLD バージョン 1 ホストと MLD バージョン 2 ホストの両方が混在する LAN もサポートされています。
- PIM-SM は、相互に転送されるマルチキャスト パケット、および直接接続されている LAN に転送されるマルチキャスト パケットを追跡するためにルータ間で使用されます。
- PIM in Source Specific Multicast（PIM-SSM）は PIM-SM と類似していますが、IP マルチキャスト アドレスを宛先とした特定の送信元アドレス（または特定の送信元アドレスを除くすべてのアドレス）からのパケットを受信する対象をレポートする機能を別途備えています。

ワイヤレス LAN コントローラの IPv6 マルチキャスト サポート

リリース 8.0 以降では、ワイヤレス LAN コントローラが IPv6 マルチキャスト対応の MLDv1 スヌーピングをサポートしています。それによって、要求元のクライアントへのマルチキャスト フローをインテリジェントに追跡および配信できます。

（注）　以前のバージョンのリリースとは異なり、IPv6 ユニキャスト トラフィックのサポートでは、コントローラで**グローバル マルチキャスト モード**を有効にする必要がなくなりました。IPv6 ユニキャスト トラフィックのサポートは自動的に有効になります。

IPv6 のマルチキャストを設定するには、次の手順に従います。

ステップ 1　IPv6 マルチキャストを有効にするには、[Enable Global Multicast Mode] チェック ボックスをオンにします。

ステップ 2　[Enable MLD Snooping] チェックボックスをオンにして、IPv6 の転送先の決定をサポートします。

（注）　MLD スヌーピングを有効にするには、コントローラの**グローバル マルチキャスト モード**を有効にする必要があります。

ステップ 3　マルチキャスト モードを設定します。

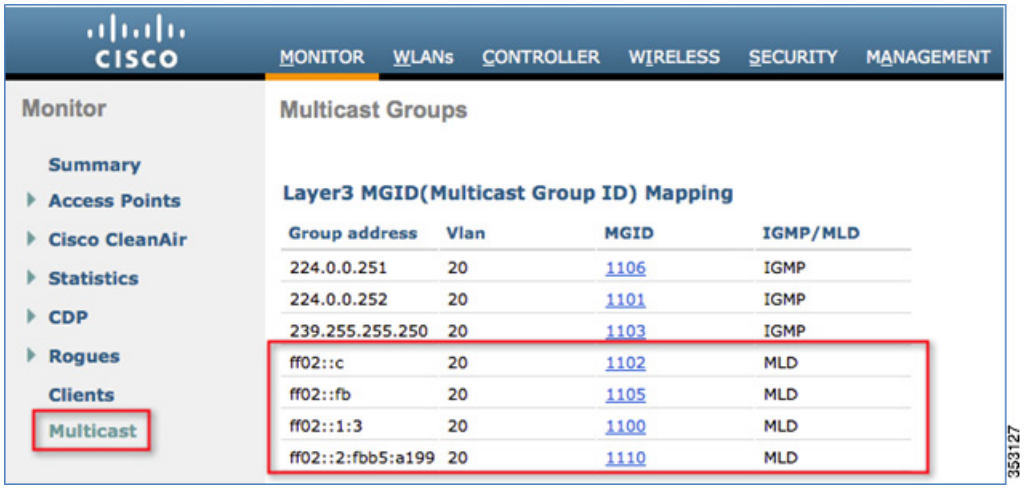
a. [MLD Timeout] テキスト ボックスで、30 ～ 7200 秒の範囲内の値を入力して MLD タイムアウトを設定します。

b. [MLD Query Interval] テキスト ボックスに、15 ～ 2400 秒の値を入力します。

c. [Apply] をクリックします。

d. [Save Configuration] をクリックします。

ステップ 4　IPv6 マルチキャスト トラフィックがスヌーピングされたことを確認するには、[Monitor] > [Multicast] に移動します。IPv4（IGMP）と IPv6（MLD）の両方のマルチキャスト グループが表示される点に注意してください。そのグループ アドレスに参加しているワイヤレス クライアントを表示するには、[MGID] をクリックします。



マルチキャスト ドメイン ネーム システム：mDNS/Bonjour

表 6-3 に、リリース 7.4 から 8.5 までの Bonjour 機能を示します。

表 6-3　フェーズ 1、2、3、および 4 のサービスの概要

Bonjour - 7.4（フェーズ 1）	Bonjour - 7.5（フェーズ 2）	Bonjour - 8.0（フェーズ 3）	Bonjour - 8.1（フェーズ 4）
• 有線およびワイヤレス サービス向けに mDNS ゲートウェイを使用する Bonjour サービス • インターフェイス単位または WLAN 単位で適用される Bonjour サービス ポリシー • コントローラにキャッシュされる mDNS サービス • L2 ドメインで認識されるすべてのコントローラで使用可能な Bonjour サービス • アンカー コントローラでサポートされる Bonjour サービス • L2 および L3 ローミングとともにサポートされる Bonjour サービス • 100 種類のサービスと、サービスごとに 64 のサービス プロバイダー • セントラル モードの FlexConnect AP のサポート	• L3 ドメイン全体にわたる mDNS サービスのサポート • 10 の有線 VLAN 上での Bonjour サービスのスヌーピングに対応する mDNS AP の導入 • LSS（ロケーション固有サービス） • Bonjour サービスのプライオリティ MAC • 起点に基づくサービス検出 • 6400 種類のサービスとサービス タイプごとのサービス プロバイダー	• アクセス ポリシーで制御されるサービス検出を備えた Bonjour GW • アクセス ポリシーへのデバイス サービスのマッピング • Bonjour グループおよび単一のアクセス ポリシーの管理 • ローカル ポリシーによる Bonjour プロファイルの制御 • Cisco Prime から特定の Bonjour サービスを管理するための Bonjour 管理者の配置	• サポートされるサービスの数が増加

マルチキャスト ドメイン ネーム システムについて

マルチキャスト ドメイン ネーム システム（mDNS）サービス ディスカバリは、ローカル ネットワークでサービスを通知し、検出する手段を提供します。mDNS サービス検出により、ワイヤレス クライアントは、異なるレイヤ 3 ネットワークでアドバタイズされる Apple Printer や Apple TV などの Apple サービスにアクセスできます。mDNS は、IP マルチキャスト経由で DNS クエリを実行します。mDNS では設定不要の IP ネットワーキングがサポートされています。

Bonjour プロトコルはサービス アナウンスとサービス クエリによって動作し、デバイスは、次を含む特定のアプリケーションに問い合わせたり、アドバタイズしたりできます。

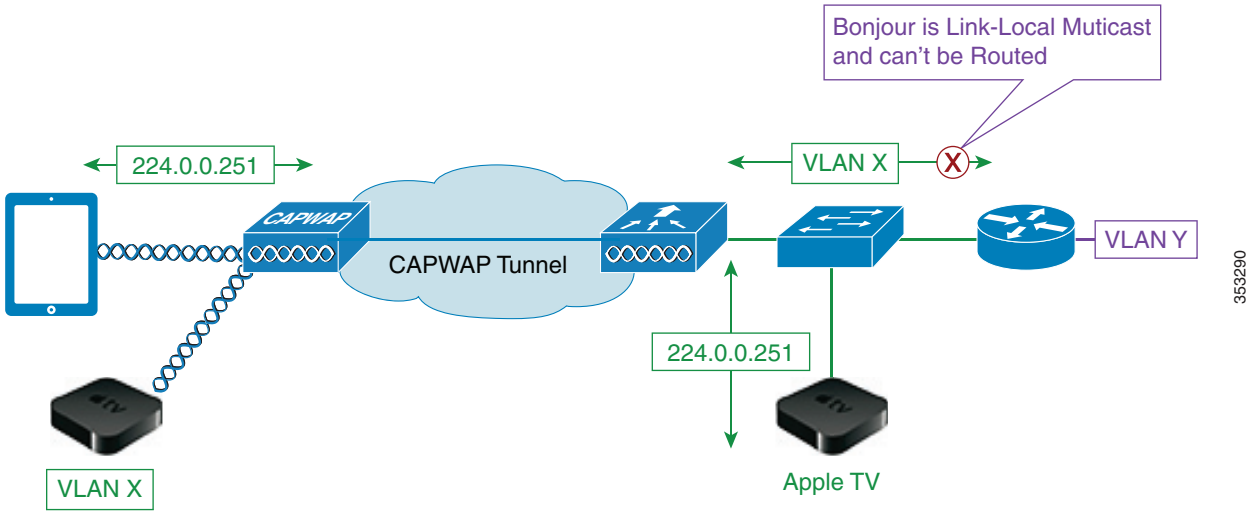
- 印刷サービス
- ファイル共有サービス
- リモート デスクトップ サービス
- iTunes ファイル共有

- iTunes ワイヤレス iDevice 同期（Apple iOS v5.0 以降）
- 次のストリーミング サービスを提供する AirPlay：
  - iOS v4.2 以降でのミュージックのブロードキャスト
  - iOS v4.3 以降でのビデオのブロードキャスト
  - iOS v5.0 以降での全画面ミラーリング（iPad2、iPhone4S 以降）

各クエリまたはアドバタイズメントはサブネット上のすべてのクライアントへ配信するために、Bonjour マルチキャスト アドレスに送信されます。Apple の Bonjour プロトコルは UDP ポート 5353 で動作する mDNS に依存しており、次の予約済みグループ アドレスに送信します。

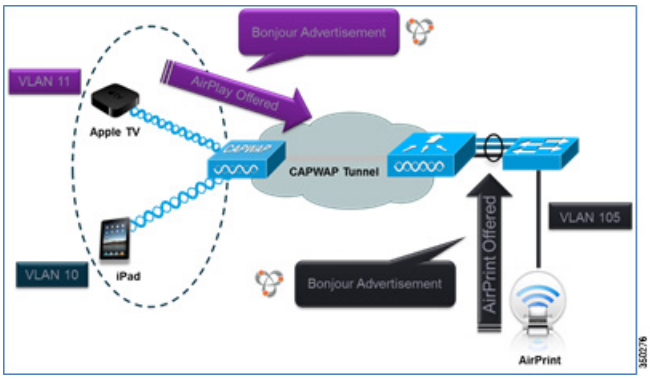
- IPv4 グループ アドレス：224.0.0.251
- IPv6 グループ アドレス：FF02::FB

Bonjour プロトコルで使用するアドレスは、リンクローカル マルチキャスト アドレスであるため、ローカル L2 ドメインにのみ転送されます。存続可能時間（TTL）が 1 に設定され、リンクローカル マルチキャストは設計によってローカルに留まることを意味しているため、ルータはマルチキャスト ルーティングを使用してトラフィックをリダイレクトすることができません。

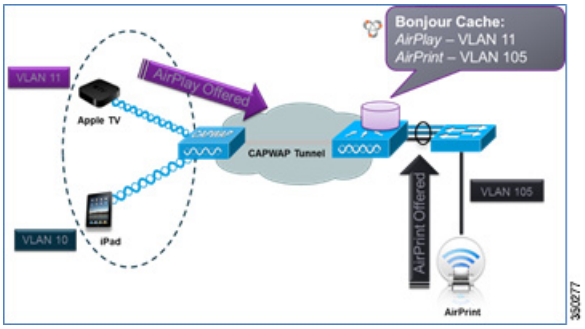


この問題を解決するために、Cisco WLC が Bonjour ゲートウェイとして機能します。WLC は Bonjour サービスをリッスンしながら、AppleTV などのソース/ホストからの Bonjour アドバタイズメント（AirPlay や AirPrint など）をキャッシュすることによって、サービスの要求が開始されたときに Bonjour クライアントに応答します。次の図は、このプロセスを示しています。

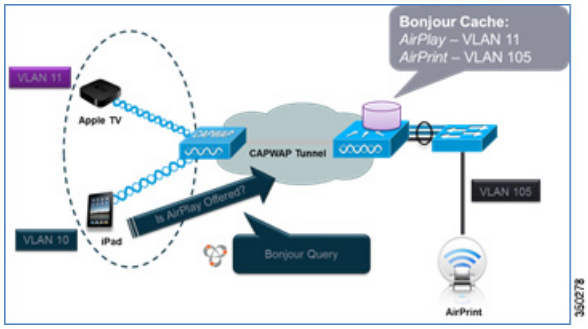
ステップ 1　コントローラが Bonjour サービスをリッスンします。



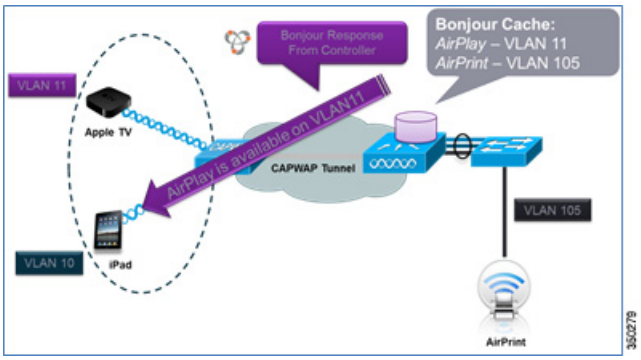
ステップ 2　コントローラは、それらの Bonjour サービスをキャッシュします。



ステップ 3　コントローラは、クライアントのサービス クエリをリッスンします。



ステップ 4　コントローラは、Bonjour サービスのクライアント クエリに対してユニキャスト応答を送信します。

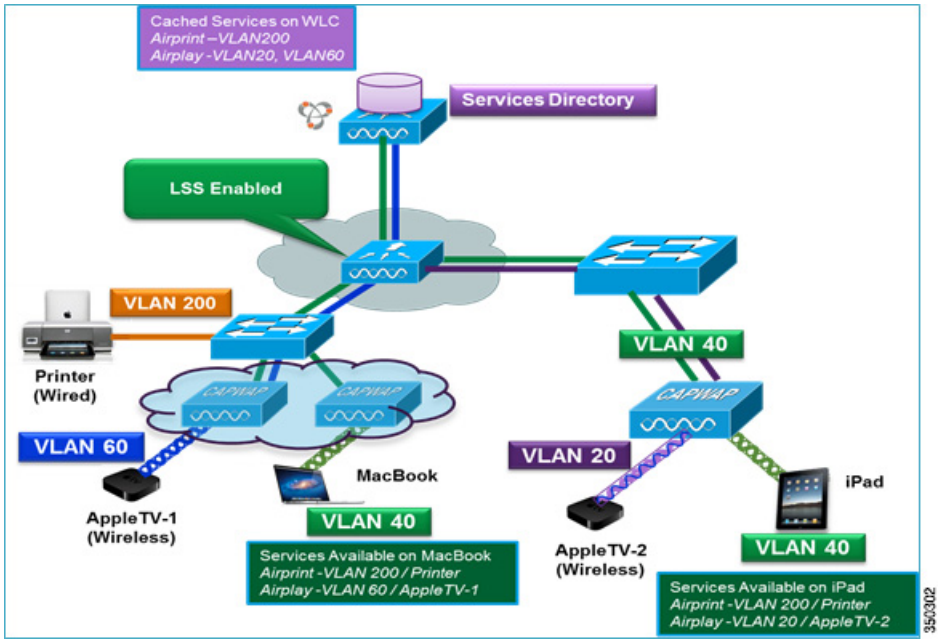


Location Specific Services（ロケーション固有サービス）

mDNS サービス アドバタイズメントおよび mDNS クエリ パケットの処理では、ロケーション固有サービス（LSS）をサポートしています。コントローラが受信するすべての有効な mDNS サービス アドバタイズメントは、新しいエントリをサービス プロバイダーのデータベースに挿入する際に、サービス プロバイダーからのサービス アドバタイズメントに関連付けられた AP の MAC アドレスにタグ付けされます。クライアント クエリに対する応答記述では、クエリ中のクライアントに関連付けられた AP の MAC アドレスを使用してサービス プロバイダー データベースのワイヤレス エントリをフィルタリングします。ワイヤレス サービス プロバイダーのデータベース エントリは、LSS がサービスに対して有効になっている場合、AP-NEIGHBOR-LIST に基づいてフィルタリングされます。LSS がサービスに対して無効になっている場合、ワイヤレス サービス プロバイダーのデータベース エントリは、そのサービスに対するワイヤレス クライアントからのクエリに応答する場合、フィルタリング対象ではありません。

LSS は、ワイヤレス サービス プロバイダーのデータベース エントリだけに適用されます。有線サービス プロバイダー デバイスのロケーションは認識されません。

LSS の状態は、ORIGIN が有線に設定されているサービスに対して有効にすることはできません。この逆も同じです。



mDNS AP

mDNS AP 機能により、コントローラは、表示されない VLAN 上の有線サービス プロバイダーの可視性を獲得できます。mDNS AP として AP を設定し、AP がコントローラに mDNS パケットを転送するようにできます。コントローラの VLAN の可視性は、AP が mDNS アドバタイズメントをコントローラに転送することで実現されます。AP とコントローラ間の mDNS パケットは、ワイヤレス クライアントからの mDNS パケットと同様に、Control and Provisioning of Wireless Access Points（CAPWAP）データ トンネルで転送されます。CAPWAP v4 のトンネルのみがサポートされます。AP をアクセス ポートまたはトランク ポートに設置して有線側からの mDNS パケットを学習し、コントローラに転送することができます。特定の AP からの mDNS パケット転送を開始または停止する際、コントローラで提供される設定可能なノブを使用できます。また、この設定を使用して、AP が有線側から mDNS アドバタイズメントをスヌープする必要のある VLAN を指定できます。AP がスヌープできる VLAN の最大数は 10 です。

AP がアクセス ポートに設置されている場合、スヌープするように AP の VLAN を設定しないでください。クエリーが送信されると、AP はタグ付けされていないパケットを送信します。mDNS アドバタイズメントが mDNS AP によって受信されると、VLAN 情報はコントローラに渡されません。mDNS AP のアクセス VLAN 経由で学習されるサービス プロバイダーの VLAN は、コントローラで 0 として保持されます。

デフォルトでは、mDNS AP はネイティブ VLAN でスヌープします。mDNS AP が有効な場合、ネイティブ VLAN のスヌーピングはデフォルトで有効になっており、VLAN 情報はネイティブ VLAN で受信したアドバタイズメントに対して 0 として渡されます。

mDNS AP 機能は、ローカル モードとモニタ モードの AP でのみサポートされます。mDNS AP 設定は、グローバル mDNs スヌーピングを無効にしてもそれぞれの mDNS AP で保持されます。mDNS AP がリセットされるか、同じコントローラまたは別のコントローラに接続している場合は、次のいずれかになります。

- グローバル スヌーピングがコントローラで無効になっている場合、ペイロードが AP に送信されて mDNS スヌーピングは無効になります。
- グローバル スヌーピングがコントローラで有効になっている場合、リセットまたはアソシエーションの手順より前の AP の設定が保持されます。

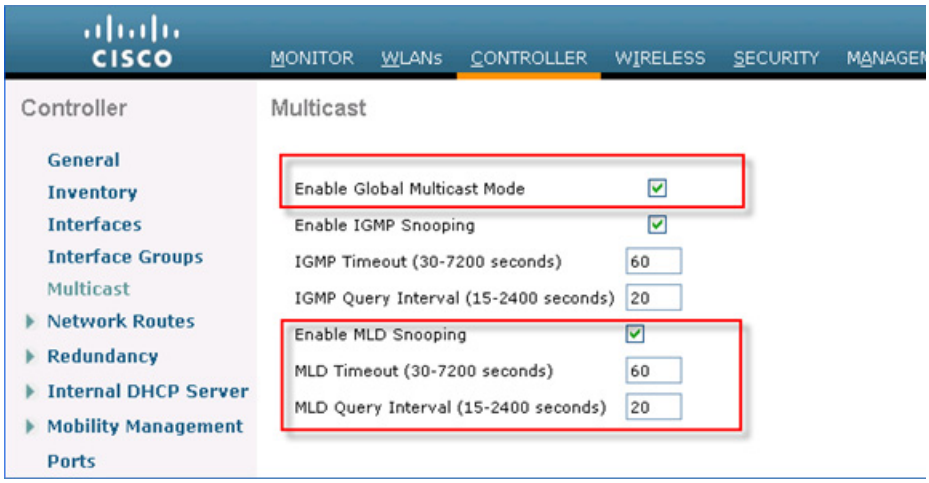
mDNS AP 機能のプロセス フローは次のとおりです。

アップリンク（有線インフラストラクチャ - AP - コントローラ）

1. 設定された VLAN で mDNS 802.3 パケットを受信します。
2. 受信した mDNS パケットをCAPWAP を介して転送します。
3. 受信した VLAN に基づいてマルチキャスト グループ ID（MGID）を入力します。

ダウンリンク（コントローラ - AP - 有線インフラストラクチャ）

1. コントローラから CAPWAP を介して mDNS クエリーを受信します。
2. 有線インフラストラクチャに 802.3 パケットとしてクエリーを転送します。
3. VLAN は専用 MGID で識別されます。



マルチキャスト DNS の設定の制限

- IPv6 を介した mDNS はサポートされません。
- ローカル側で切り替えられた WLAN およびメッシュ アクセス ポイントでは、FlexConnect モードのアクセス ポイントで mDNS はサポートされていません。
- mDNS はリモート LAN ではサポートされません。
- mDNS は Cisco AP 1240 および AP 1130 ではサポートされません。
- サードパーティの mDNS サーバまたはアプリケーションは mDNS 機能を使用する Cisco WLC ではサポートされていません。サードパーティ サーバまたはアプリケーションによってアドバタイズされるデバイスは、Cisco WLC で mDNS のサービスまたはデバイス テーブルに正しく入力されません。

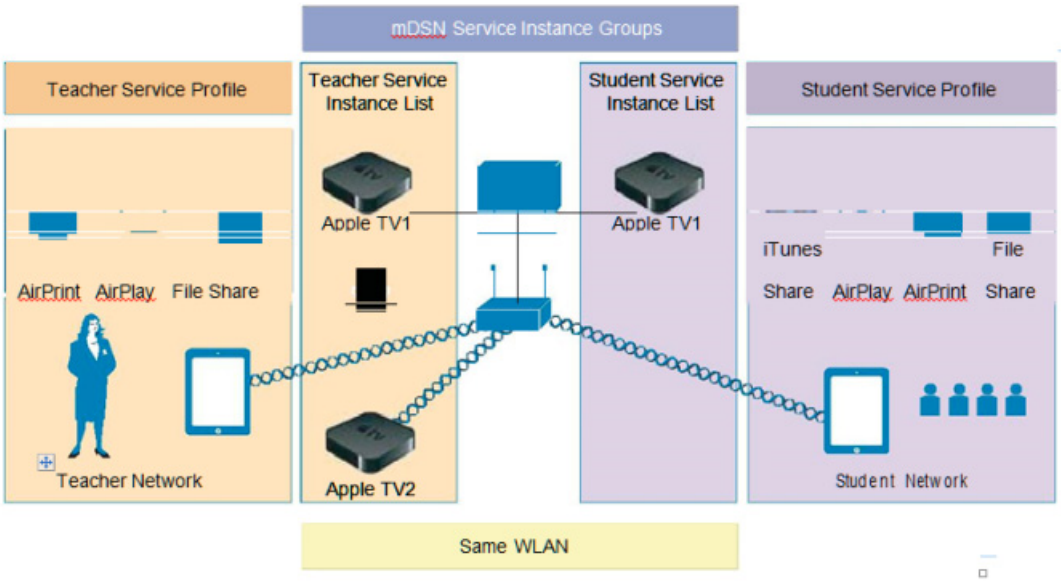
- Layer2 ネットワークでは、Apple サーバとクライアントが同じサブネット内にある場合、Cisco WLC での mDNS スヌーピングは不要です。ただし、これはスイッチング ネットワークの動作に依存します。mDNS スヌーピングと予期したとおりに連動しないスイッチを使用している場合は、Cisco WLC 上で mDNS を有効にする必要があります。
- ビデオは、WMM が有効な状態の Apple iOS 6 ではサポートされていません。
- mDNS AP は同じサービスまたは VLAN に対して同じトラフィックを複製することはできません。
- DLSS フィルタリングはワイヤレス サービスのみに制限されます。
- LSS、mDNS AP、プライオリティ MAC アドレスおよび送信元ベースの検出機能は、コントローラの GUI を使用して設定できません。
- mDNS AP 機能は CAPWAP V6 ではサポートされません。
- DISE ダイナミック mDNS ポリシーのモビリティはサポートされません。
- mDNS のユーザ プロファイル モビリティは、ゲスト アンカーではサポートされません。
- iPad、iPhone などの Apple デバイスは、Bluetooth を使用して Apple TV を検出できます。このため、Apple TV がエンド ユーザに表示されることがあります。mDNS のアクセス ポリシーでは Apple TV をサポートしていないため、シスコは、Apple TV では Bluetooth を無効にすることを推奨します。

（注）　mDNS モードをサポートしている AP モデルと、サポートされている mDNS AP については、WLC の最新のリリース ノートを参照してください。
https://www.cisco.com/c/en/us/td/docs/wireless/controller/release/notes/crn84.html

Bonjour ポリシーと新しい要件の概要

Bonjour ゲートウェイは、VLAN 間の Bonjour サービスをスヌーピングおよびキャッシュして、定期的にサービスを更新します。WLC は、ワイヤレス デバイスおよび有線デバイスによって公開されるすべての Bonjour サービスのプロキシとして動作します。8.0 より前のリリースでは、Bonjour ゲートウェイは、クエリ中のクライアントのクレデンシャルとその場所に基づいてキャッシュされた有線またはワイヤレス サービス インスタンスをフィルタする機能が不十分でした。

リリース 8.0 の Bonjour ポリシーの導入によって、管理者は、誰がどこで Bonjour サービス インスタンスを使用しているか識別するように設定できます（これはすべて同じWLANに適用される）。Bonjour ポリシーを導入することで、管理者は、特定の WLAN で許可するサービス、または特定の WLAN で使用する必要があるサービスを選択するために複数の WLAN を作成する必要がなくなりました。ユーザ 802.1x 認証に基づいて、AAA サーバまたは ISE は「CISCO-AV-PAIR」形式で USER-ROLE または BONJOUR-PROFILE を返すように設定できます。この値は、ワイヤレス コントローラで作成されたポリシーと一貫しています。ユーザ認証に基づいて、設定されたポリシーとプロファイルを同じ WLAN 上の特定のユーザに適用されます。



上の図に示すように、Bonjour サービスに改善が加えられています。Bonjour ポリシーが導入され、サービス インスタンス（MAC アドレス）の設定ごとに、サービス インスタンスがどのように共有されるかを指定できるようになりました。次のように指定されます。

- サービス インスタンスを誰と（ユーザ ID）共有するか。
- サービス インスタンスをどのロール（クライアント ロール）と共有するか。
- サービス インスタンスへのアクセスを許可する場所（クライアントの場所）

この設定は、有線およびワイヤレス サービス インスタンスに適用でき、クエリへの応答は、各サービス インスタンスに設定されたポリシーのみに基づきます。これによって、場所、ユーザ ID、またはロールに基づいてサービス インスタンスを選択的に共有できます。ほとんどのサービス公開デバイスが有線で接続されているため、これによってワイヤレス サービス インスタンスと同等の有線サービスのフィルタリングが可能になります。クライアントに関連付けられている mDNS プロファイルが、クエリに応答する前にクエリ中のサービス タイプを確認し、その一方で、アクセス ポリシーがクエリ中のクライアントの場所、ロール、またはユーザ ID に基づいて、特定のサービス インスタンスのさらなるフィルタリングを許可します。

Bonjour アクセス ポリシーでは、クライアント クエリのフィルタリングに次の 2 つのレベルがあります。

- mDNS プロファイルを使用するサービス タイプ レベル
- サービス インスタンスに関連付けられたアクセス ポリシーを使用するサービス インスタンス レベル

WLC によって検出およびキャッシュされた単一のサービス インスタンスまたは一連のサービス インスタンスは、アクセス ポリシー フィルタに関連付けることができます。このアクセス ポリシー フィルタは、どのクライアントとどのようなクライアント コンテキスト（ロールまたはユーザ ID）がサービス インスタンスを表示およびアクセスできるかを決定するレンズのように動作します。

（注） アクセス ポリシーが設定されていないサービス インスタンスは、デフォルトでは管理者ユーザ ロールのみにサービス インスタンスの受信を許可するデフォルト アクセス ポリシーにマッピングされます。追加のユーザを設定し、デフォルト ポリシーに追加できます。

- Bonjour アクセス ポリシー フィルタは、サービスを公開しているデバイスの MAC アドレスで識別された特定のサービス インスタンスに設定できます。
- Bonjour アクセス ポリシーは、Bonjour サービスを公開しているデバイスの複数の MAC アドレスを含むサービス グループ名に関連付けられます。
- その後、サービス グループ名は、サービス インスタンスが WLC で検出され、キャッシュされると、そのサービス インスタンスにアタッチされます。
- クライアント クエリへの応答時にサービス インスタンスのリストが調査され、クエリ中のクライアントの場所、ロール、またはユーザ ID にサービス インスタンスへのアクセスが許可されているかどうかを確認するため、各サービス インスタンスが評価されます。その後、応答に同じ内容が内包されます。

複数のサービス グループに同じ MAC アドレスが設定されている場合、サービス インスタンスがこの MAC アドレスに設定されているすべてのサービス グループ名に関連付けられることを意味します。MAC アドレスのサービス グループ名に関連付けられたアクセス ポリシーはすべて、そのサービス インスタンスを含んでいると判断されるまで、評価されます。現在、単一の MAC アドレスあたり最大 5 つのサービス グループがサポートされています。サービス グループの設定は、mDNS スヌーピングが無効またはオフラインの場合でも実行でき、アクセス ポリシーはサービスが検出されるタイミングを左右します。また、スヌーピングがすでに有効な場合は、動的に実行されます。

Bonjour サービス グループ

サービス グループ名は、一連の MAC アドレスに関連付けることができます。サービス グループに設定できる MAC アドレスの最大数は、プラットフォームに応じて、検出可能なサービス インスタンスのグローバル最大数によって制限されます。

- リリース 8.0 のサービス制限は、5508、WiSM2、vWLC で 6400 サービス、7510 および 8510 UC コントローラでは 16000 サービスです。
- リリース 8.1 では、サポートされている AP ライセンス数やクライアント数に応じたサービス制限に変更されており、5508 と WiSM-2 コントローラのサービス制限が変更されました。

	Bonjour キャッシュ @ フル スケール	**Bonjour キャッシュ @ 80 % スケール**
リリース 8.0 の 5508	6400	6400
リリース 8.1 の 5508	1000	2400
リリース 8.0 の WiSM2	6400	6400
リリース 8.1 の WiSM2	2000	4800
5520、7500、8500、vWLC	16,000	16,000
3504（8.5 リリース）	1600	1600
2504（8.0 リリース）	6400	6400
リリース 8.1 の 2500	推奨されない	非推奨
2500（8.2 リリース）	200	200

上記の表に示すように、リリース 8.1 の 5508 コントローラは、フル スケールで 1000 サービスのみに縮小されています（500 AP および 7000 クライアント）。80 % スケール（400 AP および 5400 ユーザ）では、同じ 5508 コントローラが 2400 サービスをサポートします。同様に、WiSM2 は、フル スケールで 2000 サービス（1000 AP と 15000）を、80 % スケールで 4800 サービスをサポートします。7500 と vWLC コントローラでは、Bonjour サービスの数は変更されていません。5520 および 8500 シリーズ コントローラでは、リリース 8.1 で 16,000 サービスがサポートされています。2504 コントローラでは、メモリの制限によってサービス数が大幅に低下しており、リリース 8.1 では Bonjour サービスの実行が推奨されていませんでした。したがって、2504 では Bonjour をテストや非常に限定されたサービス数についてのみ使用するように推奨されていました。リリース 8.2 では、8.2 ソフトウェアをインストールした 2504 コントローラで最大 200 の Bonjour サービスを実行できるように変更されています。

有線およびワイヤレスのロケーション固有のサービス

各 MAC アドレスには一意の名前が設定されます。この名前は、サービス インスタンス名の場合もあれば、有線およびワイヤレスの両方、またはどちらか一方の MAC アドレスの場所の場合もあります。

1. AP-NAME、AP-GROUP、または AP-LOCATION を使用した場所の設定時には柔軟性が求められるため、管理者は必要な場所のタイプを設定する必要があります。この設定は、サービスを公開しているデバイスと同じ場所からしか、クライアントがそのサービスにアクセスできないことを意味しています。MAC アドレスのグローバルな最大制限を超えない限り、サービス グループには必要な数の MAC アドレスを設定できます。

   ワイヤレス サービス インスタンスの場合、デバイスの場所は変更できます。ただし、サービス インスタンスと同じ場所にあるデバイスのみが必要な場合は、このようなワイヤレス サービス プロバイダーに対してキーワード「same」を設定できます。

   有線サービスの場合、有線クライアントは AP に関連付けられないため、同じ場所は適用されません。

2. 場所に対してキーワード「Any」が設定されている場合は、デバイスにアクセスしようとするクライアントを場所に基づいてフィルタリングしないことを意味します。つまり、その MAC アドレスのサービス グループに関連付けられたポリシーによってロールおよびユーザ ID クレデンシャルが許可されていれば、クライアントは任意の場所からサービスにアクセスできます。

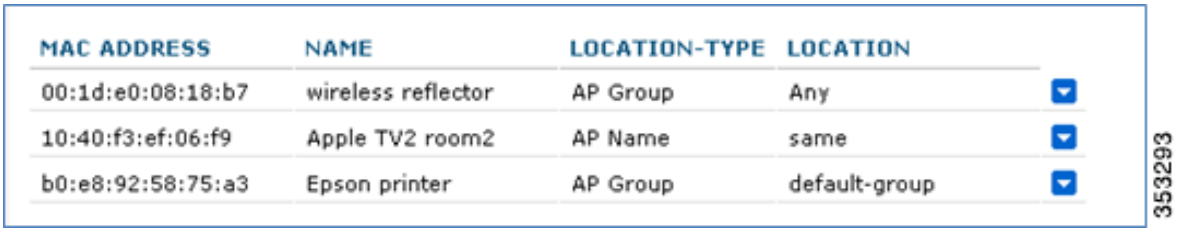
3. キーワード「ap-name」が使用されている場合は、その AP に関連付けられているクライアントのみが、サービス インスタンスにアクセスできます。

（注）　場所の検証は暗黙的で、クライアントのロールとユーザ ID クレデンシャルが確認される前であっても、第 1 レベルのアクセス ポリシー フィルタリングとして実行されます。

表 6-4 は、AppleTV-teachers という名前のサービス グループでの考えられるポリシー設定を示しています。

表 6-4　サービス グループ名によるポリシー設定の例

サービス グループ名	MAC アドレス	サービス名	ロケーション タイプ	ロケーション
AppleTV-teachers	e8:b7:48:9b:f0:20	AppleTV-class1	AP-GROUP	6-FLR
	e8:b7:48:9b:f0:21	AppleTV-class2	AP-NAME	AP4403.a740.bc97
	—	—	—	—
	e2:34:23:11:32:eb	AppleTV-class9	AP-NAME	同じ
	—	—	—	—
	e8:c7:38:9c:f1:32	AppleTV -class3	AP-GROUP	any



デバイス アクセス ポリシーの構造とルール

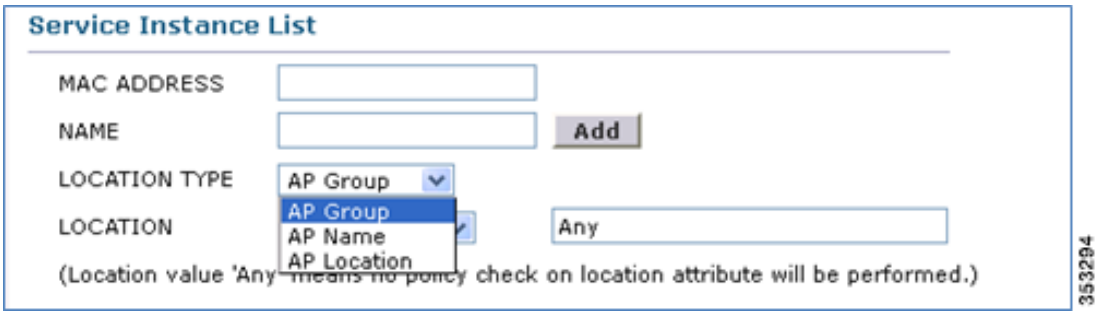
ここでは、クライアント コンテキスト属性、その構造、ポリシーを構成するルール コンポーネント、およびルールとポリシーを評価する方法という観点からアクセス ポリシーについて説明します。これは、mDNS クエリを作成したクライアントの mDNS 応答に、特定のサービス インスタンスを含める必要があるかどうかを判断するために役立ちます。さらに、複数のサービス インスタンスが同じアクセス ポリシーにマッピングされている場合、特定の mDNS クエリに関しては、特定のクエリのポリシー評価のオーバーヘッドを最適化するために、同じアクセス ポリシー マッピングを持つそれらのすべてのインスタンスに対して 1 回だけポリシーが評価されます。

mDNS ポリシーのクライアント コンテキスト属性

mDNS クエリを開始するクライアントは、クライアントのコンテキストを表す一連の属性に関連付けることができます。属性、たとえば場所は、クライアントが異なる場所に移動すると動的に変更されます。Bonjour アクセス ポリシー ルールを明確化するために、次に列挙された属性のみが使用されます。表 6-5 に、属性のリストとそれらを取得する方法について示しています。ユーザは、論理 OR 演算を使用してこれらの属性を組み合わせてルールを定式化し、そのルールをポリシーにアタッチできます。複数のルールをプロビジョニングできる場合でも、1 つのポリシーは単一のルールで構成されます。

表 6-5　　属性およびそれらの使用方法

No.	属性名	説明	設定内で使用する場合
1	ROLE	「teacher」や「student」などの文字列で、クライアントの DB と一貫しています。ISE または AAA によってクライアントにロールを関連付けることができます。	管理者は、ルールを作成するためにロール名とユーザ ID を追加する必要があります。
2	LOCATION	クライアントの場所は文字列で、クライアントのAPの「ap-location」です。	これを使用してルールを設定する場合は、場所を指定する次の 3 つのいずれかを指定できます。 • ap-location • ap-name • ap-group name
3	USER-ID	802.1x 認証中に、AAA または ISE によって、クライアントがクライアント DB に一貫しているかどうかが一意に識別されます。	ユーザは、ユーザ ID を使用してポリシーを設定する際に、まったく同じ文字列名を使用する必要があります。



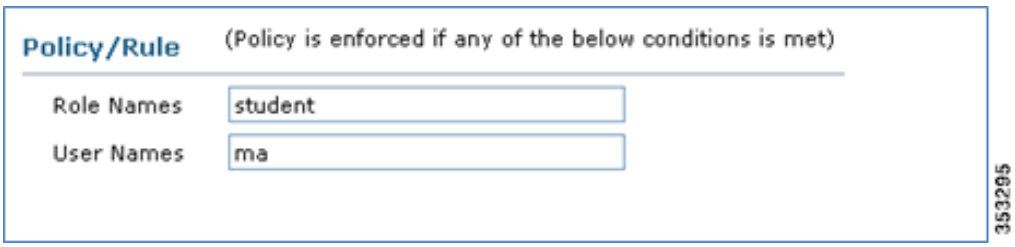
アクセス ポリシー ルール

アクセス ポリシー サービス グループは名前で識別され、1 つのルールに関連付けられます。

ルールはロールまたはユーザ ID（カンマ区切りのリスト）を使用して定義されます。これは、mDNS クエリを作成するクライアントは、そのロールがポリシー ロールにリストされている中のいずれかであるか、またはクライアント ユーザ ID がユーザ ID リストにリストされている中のいずれかである場合に、サービス インスタンスへのアクセスが許可されることを意味しています。

ルールは、次のように定義されます。

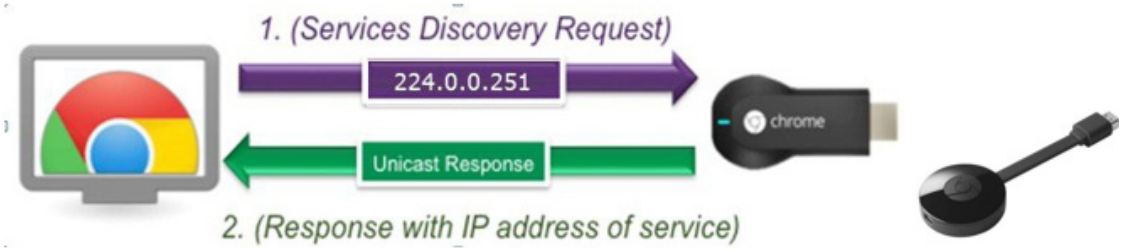
[ROLE=teacher, student] AND [USER-ID = John, Mike]



Google Chromecast による mDNS リリース 8.2 のサポート

Chromecast は Google のメディア ストリーミング デバイスであり、高解像度ディスプレイの HDMI ポートに接続することができます。これにより、第 1 世代デバイスの 2.4 ワイヤレス接続によって、クライアント画面から大型画面（Chromecast デバイス搭載）に映写することができます。ユーザは Chrome ブラウザ（Windows7 ～ 10 または Mac ラップトップ）または Android の Chromecast アプリから、テレビ画面に音声/ビデオ コンテンツを表示させることができます。

Google は最近、新しい Chromecast と Chromecast Ultra（イーサネット ポート付き）をリリースしました。これらの製品では、2.4/5 GHz Wi-Fi サポートと内蔵適応型アンテナ システムにより、高解像度と低バッファリングが確保されています。



Chromecast には検出のための 2 つのプロトコルが実装されています。1 つは DIAL Protocol over SSDP です。これは、Google Cast の旧来の version1 で使用されているプライマリ システムです。2 番目のプロトコルでは mDNS（マルチキャスト ドメイン ネーム システム）プロトコルを使用して、ワイヤレス ネットワーク上で使用可能な Chromecast を検索します。v2 API をサポートする Chromecast を検出する方法としてはこちらがメインであり、一般的です。このドキュメントでは、Chromecast による mDNS デバイス検出に焦点を当てます。Chromecast 検出用に DIAL プロトコルを使用するデバイスについては、このドキュメントでは扱っていません。

（注）　Chromecast がサポートするアプリが増えています（chromecast.com/apps）。シスコでは、Windows7 および MacBook Air クライアントで Chrome ブラウザ（Chromecast 拡張機能をインストール）をテストし、Android Samsung Galaxy S4、S6 Edge phone で Chromecast アプリをテストしました。

導入の考慮事項

mDNS プロトコルは、サービス通知やサービス クエリを受けて作動します。このためデバイスは下記のような特定のアプリケーションに対するクエリとアドバタイズを行うことができます。

- 印刷サービス
- ファイル共有サービス
- リモート デスクトップ サービス
- iTunes ファイル共有
- iTunes ワイヤレス iDevice 同期（Apple iOS v5.0 以降）
- 次のストリーミング サービスを提供する AirPlay：
  - iOS v4.2 以降でのミュージックのブロードキャスト
  - iOS v4.3 以降でのビデオのブロードキャスト
  - 全画面ミラーリング（iOS v5.0 以降（iPad2、iPhone4S 以降））

上記に加えて、次の特定のアプリケーションでは、mDNS を使用した Chromecast 検出を追加しています。

- Chromecast 拡張機能を有効にしたブラウザ（Windows7、MacBook Air）でのフルスクリーン ミラーリング
- Chromecast アプリ（Samsung Galaxy S4、Edge S6 phone）を使用した Android デバイスのミラーリング

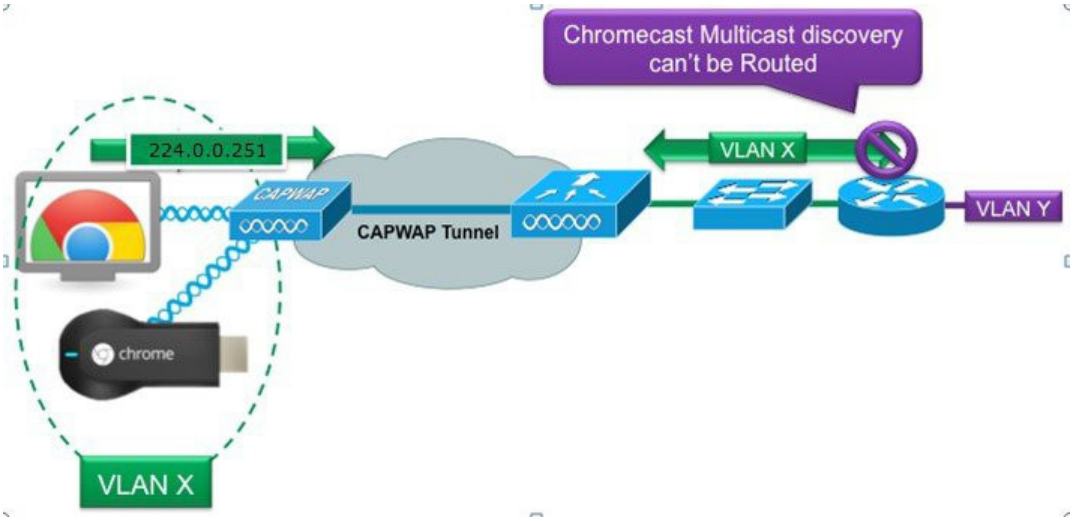
各クエリまたはアドバタイズメントが mDNS マルチキャスト アドレスに送信されると、サブネット上のすべてのクライアントに配信されます。その場合は UDP ポート 5353 で動作する mDNS を使用して、各クエリまたはアドバタイズメントを次の予約グループ アドレスに送信します。

- IPv4 グループ アドレス – 224.0.0.251

mDNS プロトコルが使用するアドレスは、リンクローカル マルチキャスト アドレスであるため、ローカル L2 ドメインでのみ転送されます。ルータはマルチキャスト ルーティングを使用してトラフィックをリダイレクトすることはできません。これは、存続可能時間（ttl）が 1 に設定されており、リンクローカル マルチキャストは設計上ローカルであり続けるためです。これは、VLAN にセグメント化された大規模なネットワークには適していません。これより前のリリースでは、ユーザはエンドツーエンドでマルチキャストを設定し、このドキュメントで示すように VLAN 間でマルチキャスト パケットをルーティングする必要がありました。

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-6/chromecastDG76/ChromecastDG76.html#pgfId-23144

mDNS を制御するには、ローカル セグメントのサイズを制限することが重要になります。



この問題を解決するために、Cisco WLC が Chromecast ゲートウェイとして機能します。WLC は Chromecast サービスをリッスンし、Chromecast サーバなどの送信元/ホストからの Chromecast アドバタイズメントをキャッシュします。サービスに対する要求が開始されると、Chrome クライアントに応答します。次にこのプロセスを示します。

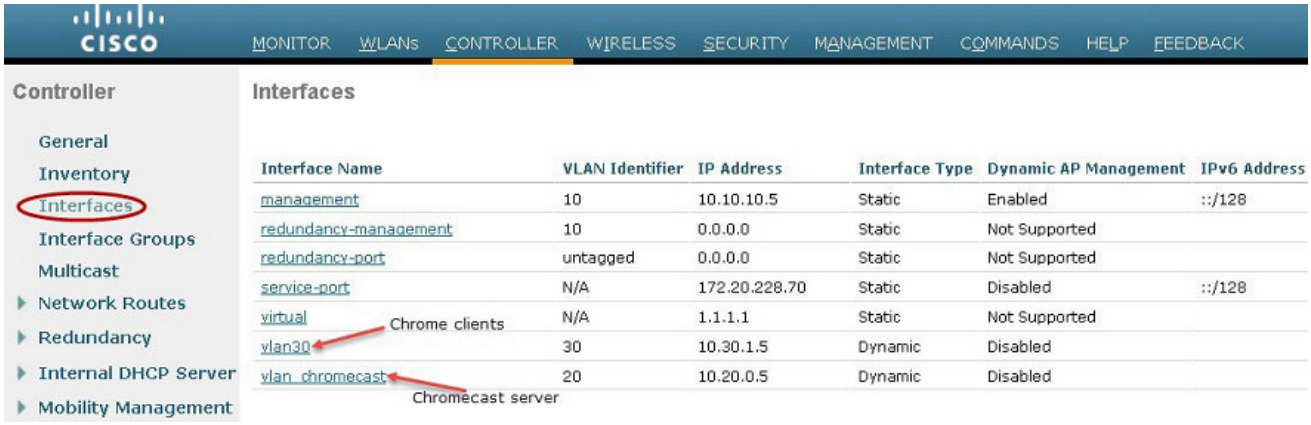
1. コントローラは Chromecast サービス/アドバタイズメントをリッスンします。
2. WLC はそれらの Chromecast サービスをキャッシュします。
3. Chromecast サービスに対するクライアントのクエリをリッスンします。
4. WLC は Chromecast サービスに対するクライアント クエリにユニキャスト応答を送信します。

8.2 リリース以降、WLC は Chromecast 用 mDNS ゲートウェイ機能をサポートしています。ユーザはコントローラでマルチキャストを有効にする必要はありません。WLC は mDNS サービスのすべてのアドバタイズメントをスヌーピングし、また無線または有線ネットワークには同じものを転送しません。クライアントは、同じかまたは異なる VLAN に Chromecast サービス プロバイダーとして存在できます。mDNS AP がサポートされているため、コントローラは、コントローラから見えない VLAN 上にある有線 Chromecast サービス プロバイダーに対する可視性が得られます。

WLAN 上で UI を通じて Chromecast 用 NS ゲートウェイを設定

ステップ 1　クライアント VLAN とは 別個の VLAN にある Chromecast サービス用に、ダイナミック インターフェイスを作成し、WLC で Chromecast 機能の設定とデモンストレーションを行います。

次の例では、クライアントと Chromecast サーバ用の異なるインターフェイスと VLAN を示しています。



ステップ 2　クライアント用の WLAN を作成します。デフォルトでは、WLAN で mDNS スヌーピングが有効になっています。確認するには、[WLAN id] > [Advanced] タブを選択し、[mDNS Snooping] オプションが [Enabled] になっていることを確認します。default-mdns-profile として [mDNS Profile] を選択し、必要な mDNS サービスが特定の WLAN にアドバタイズされるようにします。[適用（Apply）] をクリックします。

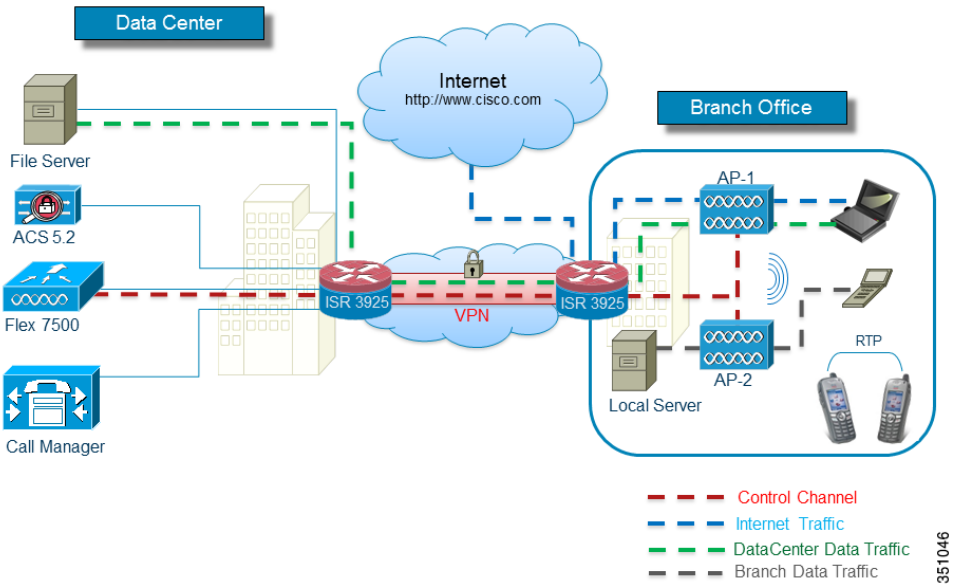
Wi-Fi の考慮事項

Chromecast デバイスでは 802.1x がサポートされていないため、Chromecast 用に WPA2 PSK（Pre-Shared Key）をサポートする別個の SSID を作成することをお勧めします。

FlexConnect

FlexConnect（以前は、ハイブリッド リモート エッジ アクセス ポイントまたは H-REAP と呼ばれていました）は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションです。これにより、各オフィスにコントローラを導入することなく、ブランチ オフィスやリモート オフィスにあるアクセス ポイント（AP）を、本社オフィスからワイドエリア ネットワーク（WAN）リンク経由で設定して制御できます。FlexConnect アクセス ポイント（AP）は、クライアント データ トラフィックをローカルに切り替え、クライアント認証をローカルに実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

図 7-1　　FlexConnect のアーキテクチャ



（注）　FlexConnect 機能マトリクスについては、http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b3690b.shtml#matrix を参照してください。

サポートされるプラットフォーム

FlexConnect は、次のコンポーネントでのみサポートされます。

- Cisco AP-1130、AP-1240、AP-1040、AP-1140、AP-1260、AP-1250、AP-3500、AP-1600、AP-2600、AP-3600、AP-3700、AP-1700、AP-2700、AP 700、AP-1520、AP-1530、AP-1550、AP-1570 アクセス ポイント
- 1815i、1815W、1815-OEAP、1540 1560 レガシー AP:3500、OEAP 600、3600、2600、1600、3700、2700、1700、702、702W、802、1530、1552WU、1550、1570、1800 シリーズ、2800 シリーズ、3800 シリーズ
- Cisco 5520、8540、Flex 7500、Cisco 8500、4400、5500、3504、2500 シリーズ コントローラ
- Cisco WiSM-2
- Cisco 仮想コントローラ（vWLC）

FlexConnect の用語

わかりやすくするために、ここではこの章全体で使用される FlexConnect 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

FlexConnect AP は、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）にワイヤレス 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、オンサイト ルータによってトラフィックが転送されます。オフサイト（セントラル サイト）に送信されるトラフィックは、ブランチ 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、Control and Provisioning of Wireless Access Points（CAPWAP）プロトコル経由で、中央集中型ワイヤレス LAN コントローラ（WLC）に個別に送信されます。

中央スイッチング

中央スイッチング WLAN は、CAPWAP 経由で、ワイヤレス ユーザ トラフィックと制御トラフィックの両方を中央集中型 WLC にトンネリングします。ここで、ユーザ トラフィックは WLC 上のダイナミック インターフェイスまたは VLAN にマップされます。これは、CAPWAP 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 に直接トンネリングされます。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 リンクを介して、標準 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、望ましい動作が得られない場合があります。

動作モード

FlexConnect 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、FlexConnect AP とその WLC が CAPWAP 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。FlexConnect はその WLC との CAPWAP 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 サイトとセントラル サイト間の WAN リンクが停止した場合などに発生します。

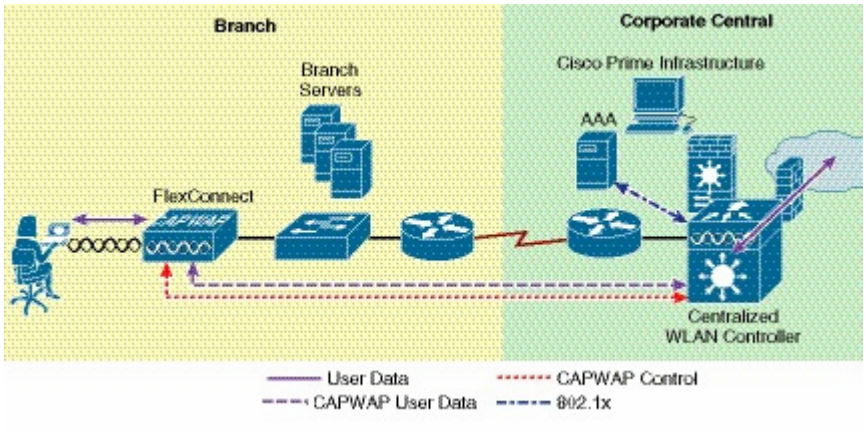
FlexConnect の状態

FlexConnect 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されます。

中央認証/中央スイッチング

WLAN が、802.1X、VPN、または Web などの中央集中型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 CAPWAP 経由で WLC に送信されます。この状態は、FlexConnect 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、他のメカニズムにも同様に適用できます。

図 7-2　中央認証/中央スイッチング WLAN



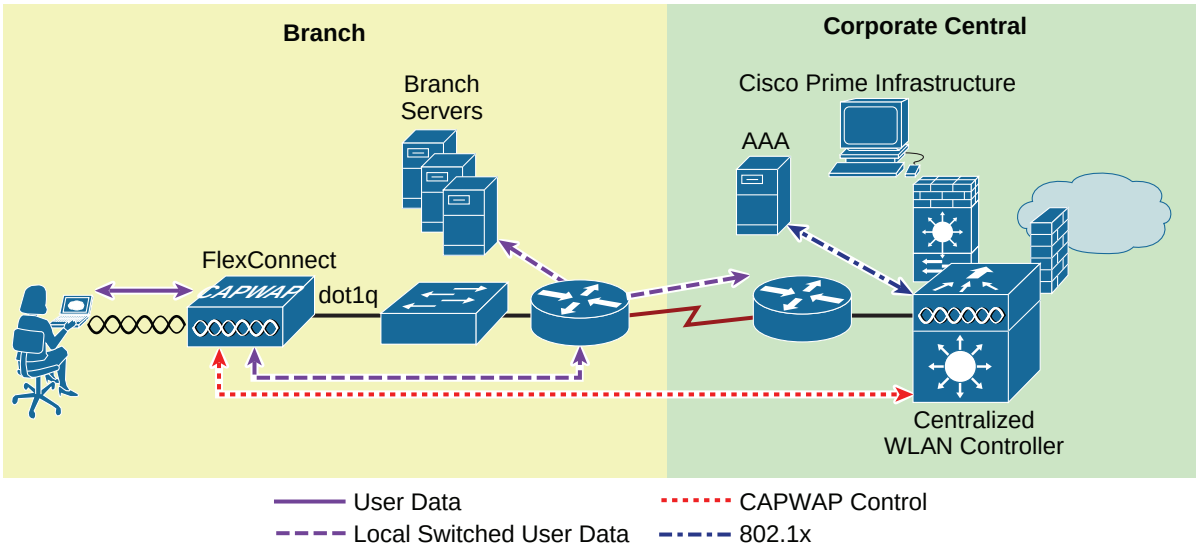
認証ダウン/スイッチング ダウン

FlexConnect AP がスタンドアロン モードのときは、中央スイッチング WLAN(上記)がプローブ要求に対してビーコンを送ったり、応答したりすることはありません。既存のクライアントのアソシエーションは解除されます。

中央認証/ローカル スイッチング

WLAN は中央集中型認証を使用しますが、ユーザ トラフィックがローカルにスイッチングされる状態です。この状態は、FlexConnect AP 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）。図 7-3 の例では 802.1X が使用されていますが、他のメカニズムにも同様に適用できます。

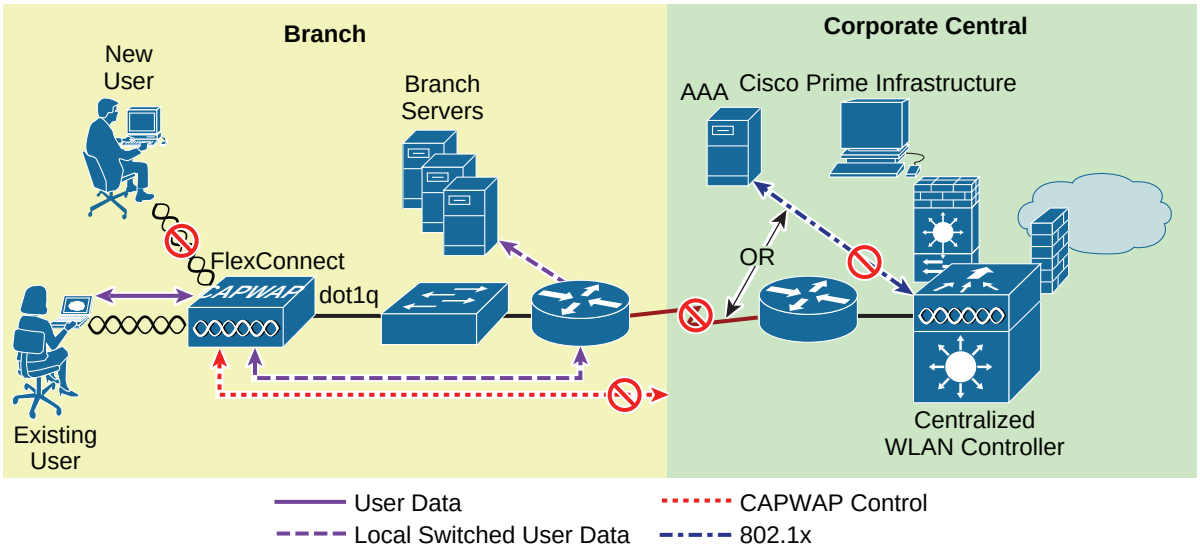
図 7-3　中央認証/ローカル スイッチング WLAN



認証ダウン/ローカル スイッチング

中央集中型認証を必要とする WLAN（上述のとおり）は、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ングされます（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）。

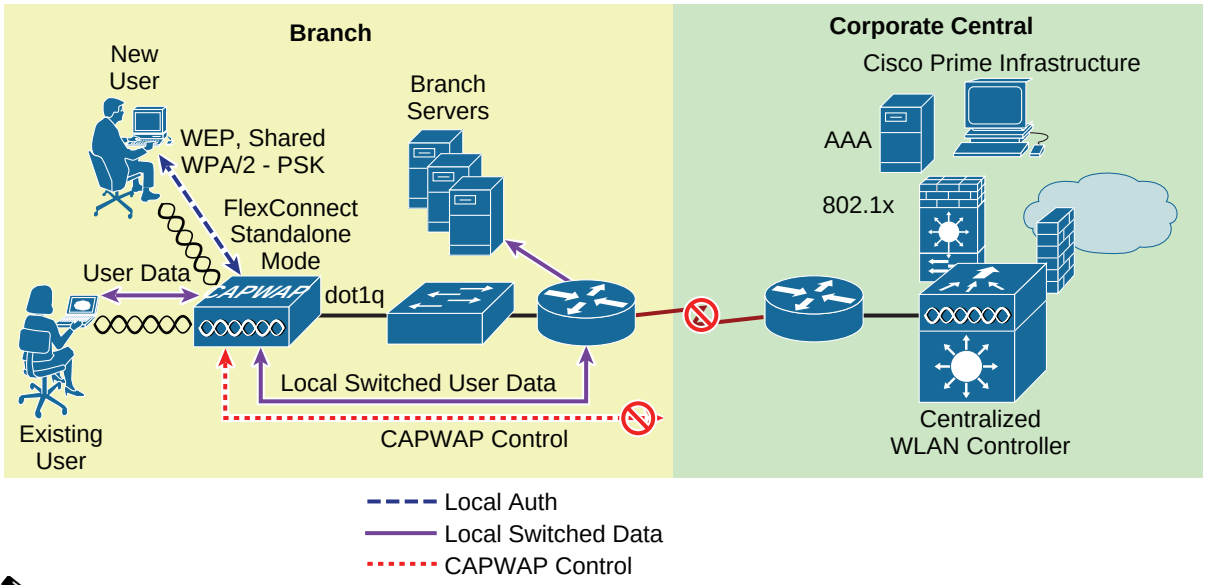
図 7-4　認証ダウン/ローカル スイッチング



ローカル認証/ローカル スイッチング

WLAN がオープンなセキュリティ方式、スタティック WEP、共有型セキュリティ方式、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ングされます。FlexConnect がスタンドアロン モードになると、これらのセキュリティ方式だけがローカルにサポートされます。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、新しいユーザの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 7-5　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発生します。接続モードのときは、FlexConnect AP 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、中央集中型認証/スイッチング方式を使用する WLAN は使用できなくなります。

アプリケーション

FlexConnect AP は、次のように、きわめて柔軟な展開が可能です。

- ブランチのワイヤレス接続
- ブランチのゲスト アクセス
- WLAN 公共ホットスポット
- ブランチ サイトでのワイヤレス BYOD

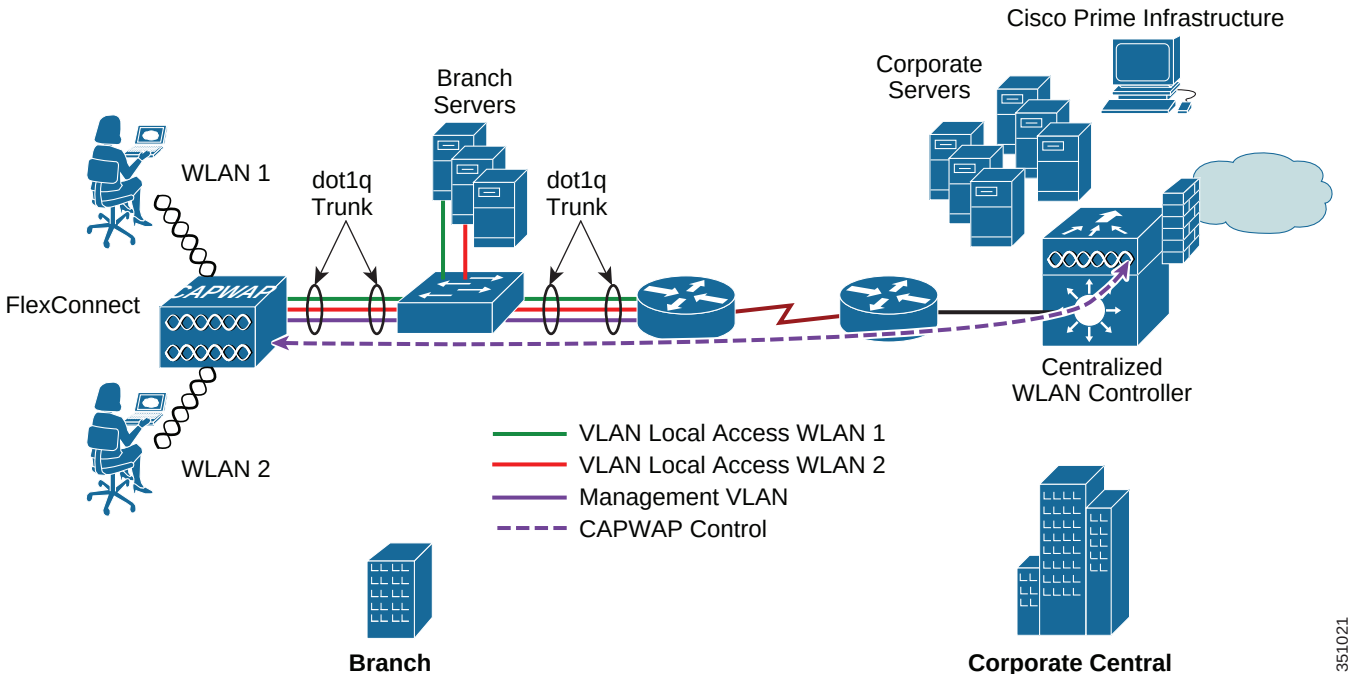
ブランチのワイヤレス接続

FlexConnect は、ワイヤレス ユーザ トラフィックを WAN 経由で中央の WLC にトンネリングするのではなく、ローカルに終了できるようにすることで、ブランチ ロケーションのワイヤレス接続のニーズに対応します。FlexConnect により、ブランチ ロケーションでは図 7-6 に示すように、WLAN ごとにセグメンテーション、アクセス制御、および QoS ポリシーをより効果的に実装できます。

ブランチのゲスト アクセス

中央集中型 WLC 自身が、図 7-6 に示すように、ゲスト アクセス WLAN に対して Web ネットワーク認証を実行できます。ゲスト ユーザのトラフィックは、他のブランチ オフィスのトラフィックから分割（隔離）されます。ゲスト アクセスの詳細については、第 10 章「Cisco Unified Wireless Network ゲスト アクセス サービス」を参照してください。

図 7-6　FlexConnect トポロジ

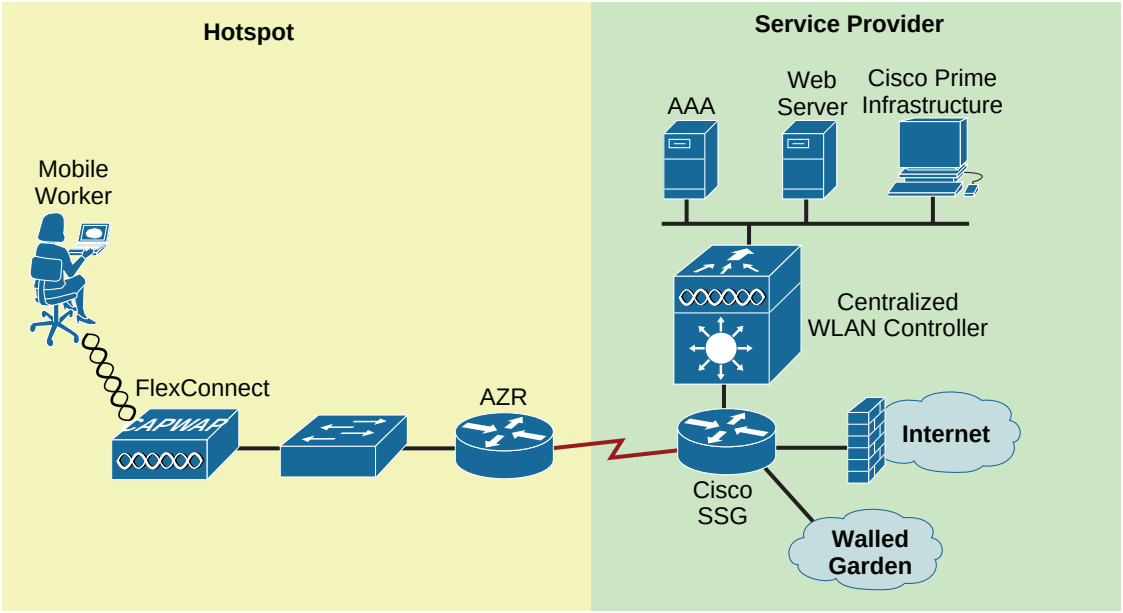


WLAN 公共ホットスポット

多くの公共ホットスポット サービス プロバイダーは、複数の SSID/WLAN の実装を始めています。この理由の 1 つは、Web ベースのアクセス用のオープン認証 WLAN と、これとは別に、より安全なパブリック アクセス用に 802.1x/EAP を使用する WLAN も提供したいと考える事業者も存在するためです。

WLAN を個別の VLAN にマップできる FlexConnect AP は、1、2 個の 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 の代替手段となります。図 7-7 は、FlexConnect 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。

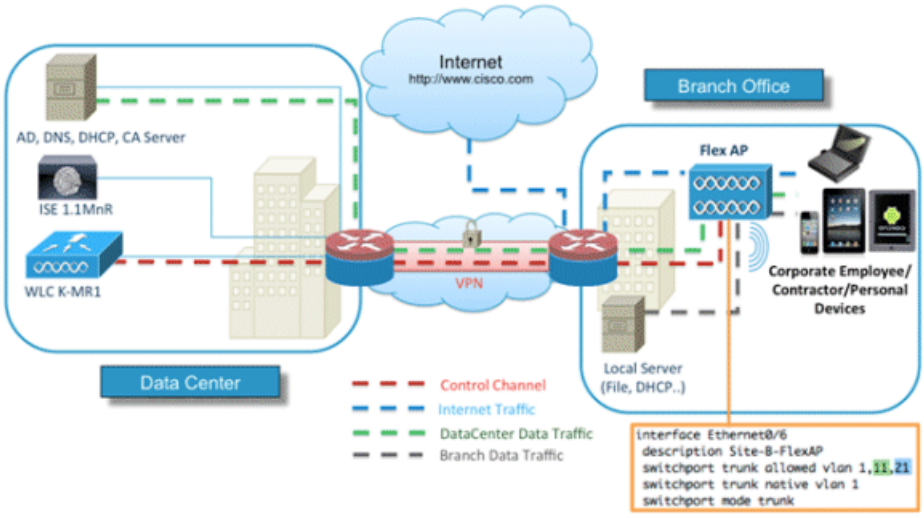
図 7-7　FlexConnect ローカル スイッチングを使用したホットスポット アクセス



ブランチ サイトでのワイヤレス BYOD

リリース 7.2.110.0 は、ローカルにスイッチングされ、中央で認証されるクライアントに対し、FlexConnect AP の ISE 機能をサポートします。また、リリース 7.2.110.0 は ISE 1.1.1 と統合されているため、ワイヤレス環境において、たとえば以下のような BYOD ソリューションを提供します。

- デバイスのプロファイリングとポスチャ
- デバイスの登録とサプリカントのプロビジョニング
- 個人用デバイスのオンボード（iOS または Android デバイスのプロビジョニング）



構成の考慮事項

ここでは、FlexConnect AP の導入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

FlexConnect AP を予測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 リンクで 100 ミリ秒を超える遅延が発生しないように管理する必要があります。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、FlexConnect AP はスタンドアロン モードに切り替わります。

  同様に、AP と WLC はエコー CAPWAP パケットを交換して、接続の有無を確認します。エコー CAPWAP パケットの応答がない場合、AP は 5 回連続（3 秒に 1 回ずつ）でエコー CAPWAP パケットを送信して、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、FlexConnect AP はスタンドアロン 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（7-3 ページ）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、認証に関連付けられたタイマーはリンク遅延に対して敏感であり、100 ミリ秒未満の制約が要求されます。遅延がそれ以上になると、クライアントは認証を待機しながらタイムアウトとなる可能性があり、この結果、ルーピングなど、その他の予測不可能な動作が発生するおそれがあります。

- 帯域幅：1 つのロケーションに 8 ヵ所以下の AP を展開する場合は、WAN リンクに 128 kbps 以上の帯域幅が必要です。8 ヵ所を超える AP を展開する場合、比例配分により高い帯域幅を WAN リンクにプロビジョニングする必要があります。

- パス MTU：500 バイト以上の MTU が必要です。

ローミング

FlexConnect 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、CAPWAP コントロール プレーンを経由して AP と WLC の間で交換されます。これは、オープン、スタティック WEP、および WPA PSK ベースの WLAN にも当てはまります。AP がスタンドアロン モードのときは、これらの認証方式を使用するために CAPWAP 接続を必要としませんが、その場合も同様です。

- ダイナミック WEP/WPA：これらのキー管理方式のいずれかを使用して FlexConnect AP 間をローミングするクライアントは、ローミングする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。ただし、FlexConnect トポロジ内では、WAN 全体でさまざまなリンク遅延が生じることがあり、この結果、合計ローミング時間に影響が及ぶ可能性があります。使用されている WAN の特性、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応じて、ローミング時間が変動する場合があります。

- WPA2：クライアントのローミング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）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。

ワイヤレス 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の動作が必要となるリモート ブランチ ロケーションでは、ローカル WLC（UCS ブレード上の仮想コントローラ、または 2500 WLC）の導入を検討する必要があります。

- Cisco Centralized Key Management（CCKM）：CCKM はシスコが開発したプロトコルです。このプロトコルでは、CCKM 対応クライアントのセキュリティ クレデンシャルが 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、クレデンシャルがこの 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。CCKM 対応クライアントは、ある FlexConnect から別の FlexConnect に移動するたびに、完全な 802.1x 認証を受けます。
- CCKM/OKC 高速ローミングで FlexConnect アクセス ポイントを使用するには、FlexConnect グループが必要となります。高速ローミングは、完全な EAP 認証で使用されたマスター キーの派生キーをキャッシュすることにより実現します。これにより、ワイヤレス クライアントが別のアクセス ポイントにローミングする際に、簡単かつ安全にキー交換できるようになります。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。しかし、たとえば 300 のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対する CCKM/OKC キャッシュを送信することは現実的ではありません。限定した数のアクセス ポイントから成る FlexConnect グループを作成すれば（たとえば、1 つのリモート オフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM/OKC キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがそのいずれかにアソシエートするときだけとなります。
- 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ングされる WLAN 上で、ある AP から別の AP にローミングしたときに、FlexConnect 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 ルータに対する 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、ローミングのパフォーマンス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 FlexConnect AP 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アドレスとなるように、自身の IP アドレスを更新します。

無線リソース管理

接続モードの間、すべての無線リソース管理（RRM）機能は、基本的に使用可能です。ただし、一般的な FlexConnect 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、伝送パワー コントロール（TPC）を行うには、最低 4 ヵ所の FlexConnect AP 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。

ロケーション サービス

FlexConnect 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厳格なガイドラインを用意しています。このため、FlexConnect 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。

QoS の考慮事項

中央でスイッチングされる WLAN では、FlexConnect AP は標準の AP と同様に QoS を処理します。ローカルにスイッチングされる WLAN は、異なる方法で QoS を実装します。

Wi-Fi MultiMedia（WMM）トラフィックを扱う、ローカルにスイッチングされる 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 タグ内の dot1p 値をマーク付けします。これはタグ付き VLAN でのみ行われ、ネイティブ VLAN では行われません。

ダウンストリーム トラフィックの場合、FlexConnect はローカルにスイッチングされるイーサネットから受信する dot1p タグを使用し、RF リンクを介して所定のユーザ宛てに送信されるフレームに関連付けられている WMM 値をキューに入れ、マーク付けします。

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で WLAN QoS プロファイルが適用されます。ダウンストリームでは、デフォルトの WLAN 値より高い 802.1p 値を受信した場合、デフォルトの WLAN 値が使用されます。アップストリームでは、クライアントがデフォルトの WLAN 値よりも高い WMM 値を送信すると、デフォルトの WLAN 値が使用されます。WMM 以外のトラフィックでは、AP からのクライアント フレームに CoS マーキングは含まれません。

詳細については、第 5 章「Cisco Unified Wireless QoS、AVC および ATF」を参照してください。

（注）　シスコでは、DSCP 設定に基づいてトラフィックが正しく処理されるように、適切なキューイング/ポリシング メカニズムを WAN 全体で実装することを強く推奨します。輻輳が原因となり、FlexConnect AP が接続モードとスタンドアロン モードとの切り替えを繰り返してしまう事態を防止するため、CAPWAP 制御トラフィック用の適切なプライオリティ キューを予約する必要があります。

FlexConnect ソリューション

FlexConnect ソリューションは、以下を実現します。

- トラフィックの中央集中型制御および管理
- 各ブランチ オフィスでのクライアント データ トラフィックの分散
- トラフィック フローを最も効率的な方法で確実に宛先に送信

アクセス ポイントの制御トラフィックを中央で集中管理する利点

AP 制御トラフィックを中央で集中管理する利点は、次のとおりです。

- モニタリングとトラブルシューティングの一括管理
- 管理の容易性
- データセンター リソースへのセキュアでシームレスなモバイル アクセス

- ブランチの占有面積の削減
- 運用コスト節約の向上

クライアント データ トラフィックを分散する利点

クライアント データ トラフィックを分散する利点は、次のとおりです。

- WAN リンクが完全に停止した場合や、コントローラが使用不能になった場合でも、運用上のダウンタイムが生じない（サバイバビリティ）
- WAN リンクで障害が発生した場合の、ブランチ内のモビリティの回復力。
- ブランチの拡張性の向上最大 100 ヵ所の AP および 250,000 平方フィート（AP あたり 5000 平方フィート）まで拡張可能なブランチの規模をサポート

中央クライアント データ トラフィック

Cisco FlexConnect ソリューションは、中央クライアント データ トラフィックもサポートしますが、ゲスト データ トラフィックのみに制限されます。表 7-1 と 表 7-2 は、データ トラフィックが中央のデータセンターでもスイッチングされるゲスト クライアント以外にのみ適用される、WLAN セキュリティ タイプの制限の概要を示します。

表 7-1　中央でスイッチングされるゲスト ユーザ以外のレイヤ 2 セキュリティのサポート

WLAN レイヤ 2 セキュリティ	タイプ	結果
なし	該当なし	許可
WPA + WPA2	802.1x	許可
	CCKM	許可
	802.1x + CCKM	許可
	PSK	許可
802.1x	WEP	許可
Static WEP	WEP	許可
WEP + 802.1x	WEP	許可
CKIP	—	許可

（注） これらの認証の制限は、データ トラフィックが各ブランチに分散されるクライアントには適用されません。

表 7-2　中央およびローカルにスイッチングされるユーザのレイヤ 3 セキュリティのサポート

WLAN レイヤ 3 セキュリティ	タイプ	結果
Web Authentication	内部	許可
	外部	許可
	カスタマイズ	許可
Web パススルー	内部	許可
	外部	許可
	カスタマイズ	許可
Conditional Web リダイレクト	外部	許可
スプラッシュ ページ リダイレクト	External	許可

主要な設計要件

FlexConnect AP はブランチ サイトに展開され、WAN リンクを介してデータセンターから管理されます。AP あたりの最小帯域幅制限を 24 kbps に維持し、ラウンドトリップ遅延を 300 ミリ秒以下に抑えることを強く推奨します（表 7-3 を参照）。

最大伝送ユニット（MTU）は、500 バイト以上にする必要があります。

表 7-3　帯域幅の最小値

展開タイプ	WAN 帯域幅（最小）	WAN RTT 遅延（最大）	ブランチあたり AP 数（最大）	ブランチあたりクライアント数（最大）
データ	64 kbps	300 ms	5	25
データ	640 kbps	300 ms	50	1000
データ	1.44 Mbps	1 秒	50	1000
データ + 音声	128 kbps	100 ms	5	25
データ + 音声	1.44 Mbps	100 ms	50	1000
データ + Flex AVC	75 Kbps	300 ms	5	25

主要な設計要件は次のとおりです。

- 最大 100 ヵ所の AP および 250,000 平方フィート（AP あたり 5000 平方フィート）まで拡張できるブランチの規模をサポート
- 一元的な管理およびトラブルシューティング
- 運用上のダウンタイムなし
- クライアント ベースのトラフィック セグメンテーション
- コーポレート リソースへのシームレスで、セキュアなワイヤレス接続
- PCI 準拠
- ゲストのサポート

FlexConnect グループ

各ブランチ サイトのすべての FlexConnect AP により、1 つの FlexConnect グループが構成されるため、FlexConnect グループの使用によって各ブランチ サイトの構成が簡素化します。

(注)　FlexConnect グループは、AP グループに類似するものではありません。

FlexConnect グループは主に、次のような課題を解決するよう設計されています。

- コントローラで障害が発生した場合、ワイヤレス クライアントはどのようにして 802.1X 認証を行い、データセンターのサービスにアクセスすればいいですか。
- ブランチとデータセンターの間の WAN リンクで障害が発生した場合、ワイヤレス クライアントはどのようにして 802.1X 認証を行えばいいですか。
- WAN で障害が発生した場合、ブランチのモビリティに影響がありますか。
- FlexConnect ソリューションでは、ブランチの運用上のダウンタイムがなくなるのですか。

スタンドアロン モードの FlexConnect AP がバックアップ RADIUS サーバに対して完全な 802.1X 認証を実行できるように、コントローラを設定することができます。

(注)　バックアップ RADIUS アカウンティングはサポートされません。

ブランチの復元力を高めるために、管理者はプライマリ バックアップ RADIUS サーバ、またはプライマリ/セカンダリ バックアップ RADIUS サーバの両方を設定できます。これらのサーバは FlexConnect AP がコントローラに接続されていない場合にのみ使用されます。

デフォルトの FlexConnect グループ数

リリース 8.4 では、コントローラに Default Flex Connect Group オプションが追加されました。8.4 より前のリリースでは、FC 設定は FC グループを通じてのみ可能であり、グループ内でサポートされる AP 数に制限がありました。AP 数が膨大で、一部の設定が類似している小売業での導入では、アクセス ポイントのプロビジョニングのために多数の FC グループを作成するのは面倒な作業です。解決策として、default-apgroup と類似する default-flex-group を使用できます。管理者が設定した FC グループに含まれない FC モードである AP がコントローラに接続すると、AP は default-flexgroup に属することになり、このグループから設定を取得します。

コントローラが起動すると、「default-flexgroup」が作成されて保存されます。このグループは手動で削除または追加することはできません。同様に、default-flexgroup に対して、アクセス ポイントを手動で追加または削除することもできません。このグループには、いくつかのパラメータについてグループ作成時のデフォルト設定があり（管理者が設定する他のグループと同様）、グループに属する AP の最大数に制限はありません。設定の変更は、グループに属するすべての AP に伝播されます。グループの設定はリセットしても保持されます。

管理者が設定したグループが削除されるか、AP がグループから手動で削除されると、その AP は default-flexgroup に属し、このグループから設定を継承します。カスタマイズされたグループに AP が追加された場合は、default-flexgroup 設定が削除され、新しい設定が AP にプッシュされます。

次の機能はサポートされていません。

- 効率的なイメージ アップグレード?
- PMK キャッシュ分散?
- 高速ローミング

次の機能はサポートされています:?

- VLAN サポート（ネイティブ VLAN、WLAN-VLAN マッピング）
- VLAN ACL マッピング?
- Web 認証、Web ポリシー、ローカル スプリット マッピング?
- ローカル認証ユーザ?
- RADIUS 認証?
- 中央 DHCP または NAT-PAT?
- フレックス AVC
- VLAN 名 ID マッピング?
- マルチキャスト オーバーライド

その他の設定の詳細については、『Controller Configuration Guide（コントローラ設定ガイド）』を参照してください。

FlexConnect グループの設定

FlexConnect が接続モードまたはスタンドアロン モードのときに、ローカル拡張認証プロトコル（LEAP）を使用したローカル認証をサポートするように FlexConnect グループを設定するには、次の手順を実行します。

ステップ 1　[Wireless] > [FlexConnect Groups] の下の [New] をクリックします。

ステップ 2　グループ名を Store 1 として割り当てます。

ステップ 3　グループ名を設定したら、[Apply] をクリックします。

ステップ 4　新しく作成したグループ名 Store 1 をクリックします。

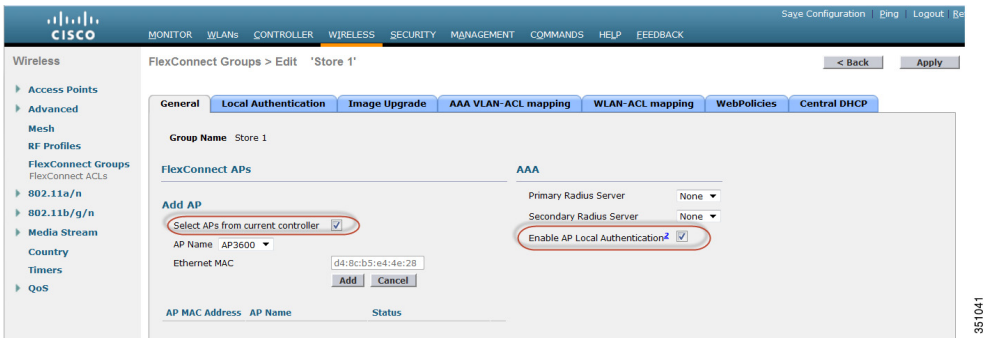
ステップ 5　[Add AP] をクリックします。

ステップ 6　AP がスタンドアロン モードのときにローカル認証を有効にするには、[Enable AP Local Authentication] チェックボックスをオンにします。

ステップ 7　[AP Name] ドロップダウン メニューを有効にするには、[Select APs from current controller] チェックボックスをオンにします。

ステップ 8　この FlexConnect グループに含める必要がある AP を [AP Name] ドロップダウン メニューから選択します。

ステップ 9　[Add] をクリックします。



ステップ 10　ステップ 7 とステップ 8 を繰り返し、この FlexConnect グループ Store 1 に必要なすべての AP を追加します。

(注)　AP グループと FlexConnect グループ間の比率を 1 対 1 に維持することにより、ネットワーク管理を簡略化できます。

ステップ 11　[Local Authentication] > [Protocols] タブに移動し、[Enable LEAP Authentication] チェックボックスをオンにします。

ステップ 12　[Apply] をクリックします。

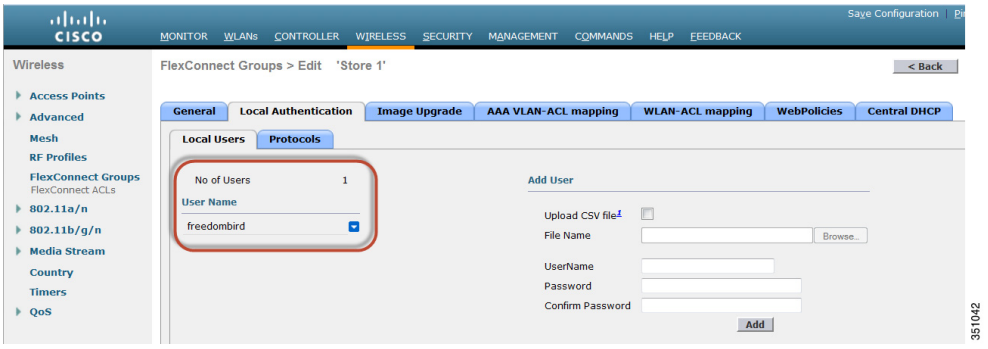
(注)　バックアップ コントローラがある場合は、双方の FlexConnect グループが同一であり、FlexConnect グループごとに AP の MAC アドレス エントリが含まれていることを確認します。

ステップ 13　[Local Authentication] > [Local Users] タブに移動します。

ステップ 14　AP 上にある LEAP サーバ内にユーザ エントリを作成するには、[UserName]、[Password]、および [Confirm Password] フィールドを設定し、[Add] をクリックします。

ステップ 15　ステップ 13 を繰り返し、必要なローカル ユーザ名をすべて追加します。100 人を超えるユーザを設定または追加することはできません。

ステップ 16　すべてのローカル ユーザ情報の入力が完了したら、[Apply] をクリックします。ユーザ数が検証されます。

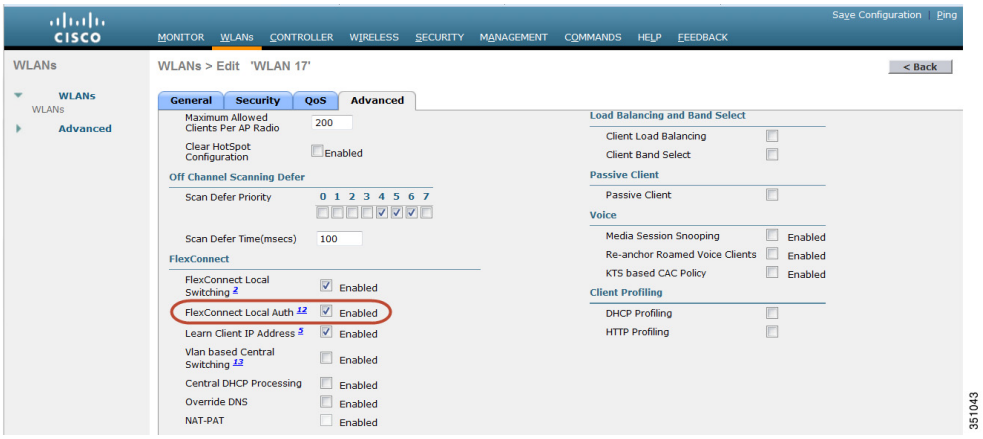


ステップ 17　上部のペインで [WLANs] をクリックします。

ステップ 18　AP グループの作成時に作成された [WLAN ID] 番号をクリックします。この例では WLAN 17 です。

ステップ 19　[WLAN] > [Edit for WLAN ID 17] の下の [Advanced] をクリックします。

ステップ 20　接続モードでローカル認証を有効にするには、[FlexConnect Local Auth] チェックボックスをオンにします。



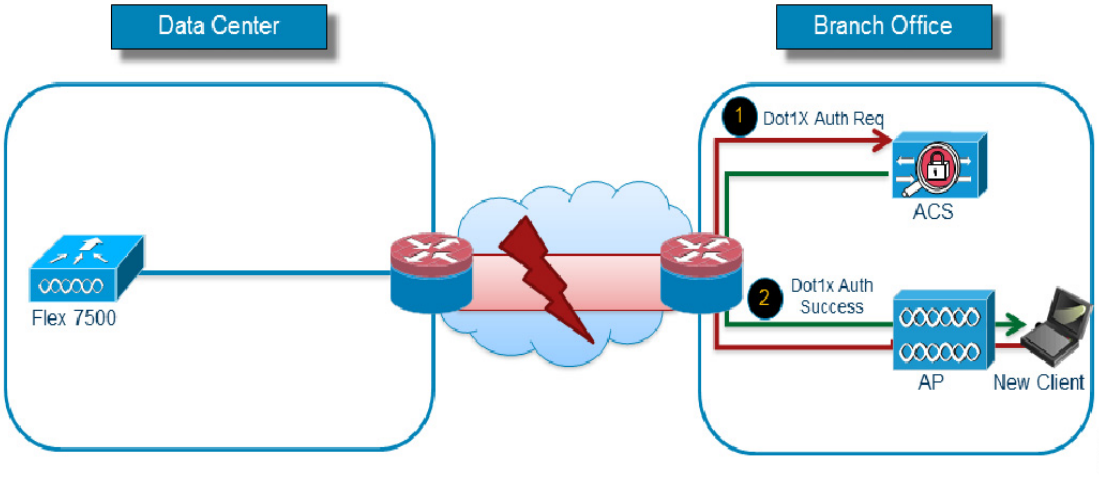
(注)　ローカル認証は、ローカル スイッチングを使用する FlexConnect のみでサポートされます。WLAN の下でローカル認証を有効化する前に、必ず FlexConnect グループを作成してください。

ローカル認証

図 7-8 に示すように、FlexConnect ブランチ AP がコントローラとの接続を失った場合でも、クライアントは引き続き 802.1X 認証を実行できます。RADIUS/ACS サーバにブランチ サイトから到達可能な限り、ワイヤレス クライアントは、引き続き認証とワイヤレス サービスへのアクセスを行います。

つまり、RADIUS/ACS がブランチ内部にあれば、クライアントは WAN が停止している間でも、認証とワイヤレス サービスへのアクセスを行います。

図 7-8　ローカル認証:AP オーセンティケータ



- WAN の障害、WLC の障害、および RADIUS サーバの障害を視野に入れ、ブランチの復元力を強化するためにローカル バックアップ RADIUS サーバを設定します。
- この機能は、セントラル サイトとの WAN 遅延が大きいリモート オフィスでも使用されます。
- プライマリ バックアップ RADIUS サーバを設定することも、プライマリとセカンダリの両方のバックアップ RADIUS サーバを設定することもできます。スタンドアロン モードの FlexConnect AP は、バックアップ RADIUS サーバに対して完全な 802.1X 認証を実行するように設定できます。
- これらのサーバは、FlexConnect AP がコントローラに接続されていない場合か、または WLAN がローカル認証用に設定されている場合に使用されます。
- RADIUS/ACS がブランチ内部にある場合、クライアントは WAN が停止している間でも、認証とワイヤレス サービスへのアクセスを行います。

(注)　ローカル バックアップ RADIUS サーバを設定する場合は、次の制限事項に注意してください。ローカル バックアップ RADIUS サーバをブランチで使用する場合は、オーセンティケータとして機能するすべての AP の IP アドレスを、この RADIUS サーバに追加する必要があります。

(注)　ローカル認証機能は、FlexConnect バックアップ RADIUS サーバ機能と組み合わせて使用できます。FlexConnect グループにバックアップ RADIUS サーバ機能とローカル認証機能の両方を設定した場合、FlexConnect AP はまず、プライマリ バックアップ RADIUS サーバを使用してクライアントの認証を試行します。次に、セカンダリ バックアップ RADIUS サーバによる認証を試行し(プライマリに到達できない場合)、最後に FlexConnect AP 自体のローカルな EAP サーバによる認証を試行します(プライマリとセカンダリの両方に到達できない場合)。

ローカル EAP

スタンドアロン モードまたは接続モードの FlexConnect AP が、最大 100 人の静的に設定されたユーザに対して LEAP または EAP-FAST 認証を実行できるように、コントローラを設定できます。特定の FlexConnect グループがコントローラに参加すると、コントローラはユーザ名およびパスワードの静的リストを、この FlexConnect グループ内の個々の FlexConnect AP に送信します。グループ内の各 AP は、自身にアソシエートされたクライアントのみを認証します。

この機能が適しているのは、カスタマーがスタンドアロン AP ネットワークから軽量な FlexConnect AP ネットワークに移行するときに、大きなユーザ データベースを保持したくない場合や、スタンドアロン AP で利用可能な RADIUS サーバ機能を置き換える、新たなハードウェア デバイスを追加したくない場合です。

PEAP、EAP-TLS 認証のサポート

FlexConnect AP は LEAP および EAP-FAST クライアント認証用の RADIUS サーバとして設定できます。スタンドアロン モードであり、WLAN 上でローカル認証機能が有効にされている場合は、FlexConnect AP はローカル RADIUS を使用して、AP 自身の dot1x（802.1X）認証を行います。リリース 7.5 のコントローラでは、PEAP、EAP-TLS の EAP 方式もサポートされます。

CCKM/OKC 高速ローミング

Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミングで FlexConnect AP を使用する場合には、FlexConnect グループが必要となります。高速ローミングは、ワイヤレス クライアントを別の AP にローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスター キーの派生キーをキャッシュすることにより実現します。

この機能により、クライアントをある AP から別の AP へローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。

しかし、たとえば 300 の AP を持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対する CCKM/OKC キャッシュを送信することは現実的ではありません。限定した数の AP から成る FlexConnect グループを作成すれば（たとえば、1 つのリモート オフィス内の 4 つの AP のグループを作成）、クライアントはその 4 つの AP 間でのみローミングします。CCKM/OKC キャッシュがその 4 つの AP 間で配布されるのは、クライアントがそのいずれかにアソシエートするときだけとなります。

この機能とバックアップ RADIUS およびローカル認証（ローカル EAP）により、ブランチ サイトの運用上のダウンタイムがなくなります。

FlexConnect グループは、FlexConnect AP が接続モードまたはスタンド アロンモードであり、クライアントに CCKM/OKC 高速ローミングが必要な場合に使用します。

この機能により、クライアントが AP から別の AP へローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。

FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM/OKC キャッシュ情報を取得する必要があります。これにより、キャッシュ情報をコントローラに送り返すことなく、すばやく処理できます。

（注）　CCKM/OKC 高速ローミングは FlexConnect AP でのみサポートされます。

FlexConnect VLAN オーバーライド

現在の FlexConnect アーキテクチャでは、WLAN から VLAN への厳密なマッピングが行われます。このため、FlexConnect AP 上で特定の WLAN にアソシエートされたクライアントは、この WLAN にマッピングされる VLAN に従う必要があります。この方式は、異なる VLAN ベースのポリシーを継承するために、クライアントを異なる SSID にアソシエートする必要があるので、さまざまな制約があります。

リリース 7.2 以降では、ローカル スイッチングが設定された個々の WLAN に対する、VLAN の AAA オーバーライドがサポートされています。AP には、動的に VLAN を割り当てるために、個々の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、または FlexConnect グループの ACL-VLAN マッピングを使用した設定に基づいて事前に作成された、VLAN 用のインターフェイスがあります。AP でサブインターフェイスを事前作成するために、WLC が使用されます。

FlexConnect VLAN オーバーライドの要約

- AAA VLAN オーバーライドは、中央およびローカル認証モードでローカル スイッチングが設定された WLAN に対し、リリース 7.2 からサポートされています。
- AAA オーバーライドは、ローカル スイッチングが設定された WLAN 上で有効にする必要があります。
- FlexConnect AP には、動的な VLAN 割り当て用に、WLC から VLAN が事前に作成されている必要があります。
- AAA オーバーライドから返された VLAN が AP クライアント上にない場合、IP は AP のデフォルト VLAN インターフェイスから取得されます。

FlexConnect VLAN に基づく中央スイッチング

リリース 7.3 以降では、FlexConnect AP からのトラフィックは、FlexConnect AP 上に VLAN が存在するかどうかに応じて、中央またはローカルでスイッチングされます。

コントローラ ソフトウェア リリース 7.2 では、ローカルにスイッチングされる WLAN に対する VLAN の AAA オーバーライド（動的な VLAN 割り当て）により、AAA サーバから提供される VLAN 上にワイヤレス クライアントが配置されます。AAA サーバから提供された VLAN が AP に存在しない場合、クライアントはその AP 上で WLAN にマッピングされた VLAN に配置され、トラフィックはこの VLAN 上でローカルにスイッチングされます。さらに、7.3 よりも前のリリースでは、FlexConnect AP からの特定の WLAN のトラフィックは、WLAN の設定に応じて中央またはローカルでスイッチングされます。

FlexConnect VLAN 中央スイッチングの要約

FlexConnect AP が接続モードの場合に、ローカル スイッチングが設定された WLAN 上のトラフィック フローは、次のようになります。

- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在しない場合、トラフィックは中央でスイッチングされます。この VLAN が WLC 上に存在する場合は、AAA サーバから返されたこの VLAN とインターフェイスがクライアントに割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在しない場合、トラフィックは中央でスイッチングされます。その VLAN が WLC にも存在しない場合、クライアントには WLC 上で WLAN にマッピングされた VLAN とインターフェイスが割り当てられます。
- VLAN が AAA 属性の 1 つとして返され、その VLAN が FlexConnect AP データベースに存在する場合、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

FlexConnect AP がスタンドアロン モードの場合に、ローカル スイッチングが設定された WLAN 上のトラフィック フローは、次のようになります。

- AAA サーバによって返された VLAN が FlexConnect AP データベースに存在しない場合、クライアントはデフォルト VLAN（つまり、FlexConnect AP 上で WLAN にマッピングされた VLAN）に配置されます。AP が接続モードに戻ると、このクライアントは認証を解除され、トラフィックが中央でスイッチングされます。
- AAA サーバによって返された VLAN が FlexConnect AP データベースに存在する場合、クライアントは返された VLAN に配置され、トラフィックはローカルにスイッチングされます。
- AAA サーバから VLAN が返されない場合、クライアントには、その FlexConnect AP 上で WLAN にマッピングされた VLAN が割り当てられ、トラフィックはローカルにスイッチングされます。

VLAN 名のオーバーライド

VLAN 名のオーバーライド機能は、中央の 1 つの RADIUS サーバによって複数のブランチを認証する構成で役立ちます。ブランチの数が数百規模に及ぶ場合、全サイトで VLAN の ID を標準化することは非常に困難です。この場合、ブランチ ロケーションごとに異なる VLAN ID にローカルにマッピングされる、一意の VLAN 名を提供する設定が必要となります。

このように、サイトごとに異なる VLAN ID を使用する設計では、レイヤ 2 ブロードキャスト ドメインあたりのクライアント数を制限できるため、サイジングと拡大縮小の観点からも有益です。

FlexConnect VLAN 名オーバーライドの要約

- VLAN 名オーバーライド機能は、ローカル スイッチング WLAN での中央およびローカル認証の両方に対応します。
- AAA サーバから複数の VLAN 属性が返される場合は、VLAN 名属性が優先されます。
- Aire-Interface-Name 属性と Tunnel-Private-Group-ID 属性の両方が返される場合は、Tunnel-Private-Group-ID 属性のほうが優先されます。

- AAA サーバから不明の VLAN 名属性が返された場合、クライアントには、AP 上に存在する WLAN-VLAN ID マッピングがデフォルトで適用されます。
- この機能は、スタンドアロン モードでもサポートされます。

FlexConnect ACL

FlexConnect 上での ACL の導入に伴い、AP からローカルにスイッチングされるデータ トラフィックの保護と整合性のために、FlexConnect AP でのアクセス制御の必要性を満たすメカニズムが用意されています。FlexConnect ACL を WLC 上に作成し、VLAN-ACL マッピングを使用して、この ACL に FlexConnect AP 上の VLAN または FlexConnect グループ上の VLAN（AAA オーバーライド VLAN 用）を設定する必要があります。これらの ACL は AP にプッシュされます。

FlexConnect ACL の要約

- コントローラ上に FlexConnect ACL を作成します。
- この ACL を、AP レベルでの VLAN ACL マッピングに基づき、FlexConnect AP 上に存在する VLAN に適用します。
- VLAN-ACL マッピングに基づき、FlexConnect グループに存在する VLAN にも適用できます（一般に AAA オーバーライドされた VLAN に対して行います）。
- VLAN に対して ACL を適用する際に、適用する方向として、*ingress*、*egress*、または *ingress and egress* を選択します。

FlexConnect ACL の制限事項

- 1 つの WLC には、最大 512 個の FlexConnect ACL を設定できます。
- 個々の ACL には 64 個のルールを設定できます。
- FlexConnect グループまたは FlexConnect AP あたり最大 32 個の ACL をマッピングできます。
- FlexConnect AP 上には、一度に最大 16 の VLAN と 32 個の ACL を設定できます。

クライアント ACL サポート

リリース 7.5 以前では、VLAN で FlexConnect ACL がサポートされます。また、VLAN の AAA オーバーライドもサポートされます。クライアントに対して VLAN の AAA オーバーライドが行われた場合、このクライアントはオーバーライドされた VLAN 上に配置され、この VLAN の ACL が適用されます。ローカルにスイッチされるクライアントに対し、AAA サーバから ACL が送られてきた場合は、この ACL は無視されます。リリース7.5ではこの制限事項が解決され、ローカルにスイッチされる WLAN に対し、クライアント ベースの ACL がサポートされます。

FlexConnect スプリット トンネリング

スプリット トンネリングにより、クライアントによって送信されたトラフィックを、FlexConnect ACL を使用し、パケットの内容に基づいて分類するメカニズムが導入されました。一致するパケットは FlexConnect AP からローカルにスイッチングされ、それ以外のパケットは CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング機能には、企業の SSID 上のクライアントがローカル ネットワーク上のデバイス（プリンタ、リモート LAN ポート上の有線マシン、またはパーソナル SSID 上のワイヤレス デバイス）と直接通信でき、CAPWAP を介してパケットを送信することで WAN 帯域幅を消費することがないという、OEAP 構成に対するさらなるメリットがあります。

適切なルールを規定した FlexConnect ACL を作成することで、ローカル サイトまたはネットワークに存在するすべてのデバイスを許可できます。企業の SSID 上のワイヤレス クライアントからのパケットが、OEAP 上で設定されている FlexConnect ACL のルールに一致した場合、そのトラフィックはローカルにスイッチングされ、それ以外のトラフィック（つまり暗黙的に拒否されたトラフィック）は、CAPWAP を介して中央でスイッチングされます。

スプリット トンネリング ソリューションでは、セントラル サイトのクライアントにアソシエートされているサブネットまたは VLAN が、ローカル サイトには存在しないことを前提としています（つまり、セントラル サイトにあるサブネットから IP アドレスを受け取るクライアントのトラフィックは、ローカルにスイッチングできません）。

スプリット トンネリングは、WAN 帯域幅の消費を軽減するために、ローカル サイトに属するサブネットに対してトラフィックをローカルにスイッチングするように設計された機能です。FlexConnect ACL ルールに一致するトラフィックはローカルにスイッチングされます。NAT 操作の実行により、クライアントの送信元 IP アドレスは、ローカル サイトまたはネットワークでルーティング可能な FlexConnect AP のインターフェイス IP アドレスに変更されます。

スプリット トンネルの要約

- スプリット トンネリング機能は、FlexConnect AP のみによってアドバタイズされる、中央でのスイッチングが設定された WLAN 上でサポートされます。
- スプリット トンネリングを設定した WLAN 上では、必要な DHCP を有効化する必要があります。
- スプリット トンネリングの設定は、FlexConnect AP ごと、または FlexConnect グループ内のすべての FlexConnect AP に対して、中央スイッチングが設定された WLAN ごとに適用されます。

スプリット トンネリングの制限事項

- FlexConnect ACL ルールは、同じサブネットを送信元および宛先とする permit/deny 文を使用して設定できません。
- スプリット トンネリングが設定された、中央でスイッチングされる WLAN 上のトラフィックをローカルにスイッチングできるのは、ワイヤレス クライアントがローカル サイト上にあるホスト宛のトラフィックを送信した場合のみです。トラフィックが、ローカル サイト上のクライアントまたはホストにより、上記のとおり設定された WLAN 上のワイヤレス クライアントに送信された場合は、宛先に到達できません。

- マルチキャストまたはブロードキャスト トラフィックについては、スプリット トンネリングはサポートされていません。マルチキャストまたはブロードキャスト トラフィックは、FlexConnect ACL に一致しても中央でスイッチングされます。
- スプリット トンネル機能は、外部アンカー ローミング シナリオではサポートされていません。

耐障害性

FlexConnect の耐障害性機能により、FlexConnect AP で次の状態が生じた場合でも、ブランチ クライアントに対するワイヤレス アクセスとサービスが可能になります。

- プライマリ コントローラへの接続を失ったとき。
- セカンダリ コントローラに切り替わるとき。
- プライマリ コントローラとの接続を再確立するとき。

FlexConnect の耐障害性とローカル EAP とを組み合わせることで、ネットワーク停止時のゼロ ブランチ ダウンタイムを実現できます。この機能はデフォルトで有効であり、無効にすることはできません。つまり、コントローラまたは AP での設定は不要です。ただし、耐障害性が円滑に機能し、適用可能であるためには、次の条件を満たす必要があります。

- WLAN の順序と設定は、プライマリおよびバックアップ コントローラで同じであることが必要です。
- VLAN マッピングは、プライマリおよびバックアップ コントローラで同じであることが必要です。
- モビリティ ドメイン名は、プライマリおよびバックアップ コントローラで同じであることが必要です。
- プライマリおよびバックアップ コントローラとして FlexConnect 7500 を使用する必要があります。

耐障害性の要約

- コントローラの設定を変更しない限り、FlexConnect AP が同じコントローラに再接続する場合、クライアントが切断されることはありません。
- 設定に変更がなく、バックアップ コントローラがプライマリ コントローラと同じである限り、FlexConnect AP がバックアップ コントローラに接続する場合、クライアントが切断されることはありません。
- コントローラの設定に変更がない限り、FlexConnect AP がプライマリ コントローラに再接続する場合、その無線はリセットされません。

耐障害性の制限事項

- ローカル スイッチングによる、中央またはローカルの認証を使用する FlexConnect のみでサポートされます。
- 中央で認証されるクライアントは、FlexConnect AP がスタンドアロン モードから接続モードに切り替わる前にクライアント セッション タイマーが切れた場合、完全な再認証が必要となります。
- プライマリおよびバックアップ コントローラは、同じモビリティ ドメインに属している必要があります。

ピアツーピア ブロッキング

ピアツーピア(P2P)ブロッキングは、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に対してサポートされます。WLAN ごとのピアツーピア設定は、コントローラによって FlexConnect AP にプッシュされます。P2P ブロッキングでは、WLAN に対して次の 3 つのいずれかの動作を設定できます。

- 無効化:P2P ブロッキングを無効にし、同じサブネット内のクライアント宛のトラフィックをコントローラ内でローカルにブリッジします。これはデフォルト値です。
- ドロップ:コントローラは同じサブネット内のクライアント宛のパケットを破棄します。
- アップストリーム転送:パケットはアップストリーム VLAN に転送されます。コントローラ上のデバイスは、パケットに関して実行すべきアクションを決定します。

P2P の要約

- P2P ブロッキングは、WLAN ごとに設定します。
- WLAN ごとの P2P ブロッキングの設定は、WLC によって FlexConnect AP にプッシュされます。
- WLAN 上で P2P ブロッキング アクションをドロップまたはアップストリーム転送として設定すると、FlexConnect AP では P2P ブロッキングが有効化されたとみなされます。

P2P の制限事項

- FlexConnect ソリューションでは、特定の FlexConnect AP または AP のサブセットのみに P2P ブロッキング設定を適用することはできません
- これは、SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチング クライアントのための統一ソリューションは、P2P アップストリーム転送をサポートしています。しかし、これは FlexConnect ソリューションでサポートされません。これは、P2P ドロップとして扱われ、クライアント パケットは、次のネットワーク ノードに転送されずにドロップされます。
- 中央スイッチング クライアント用の統一ソリューションは、異なる AP にアソシエートされたクライアントに対する P2P ブロッキングをサポートしています。ただし、このソリューションでは、同一の AP に接続するクライアントだけがターゲットとなります。この制限の回避策として、FlexConnect ACL を使用できます。

ローカル スイッチング WLAN のための FlexConnect WGB/uWGB サポート

リリース 7.3 から、シスコのワーク グループ ブリッジとユニバーサル ワーク グループ ブリッジ(WGB/uWGB)、および WGB の背後にある有線またはワイヤレス クライアントがサポートされ、ローカル スイッチングが設定された WLAN 上の通常のクライアントとして動作します。

アソシエーションの後、WGB は各有線またはワイヤレス クライアントに IAPP メッセージを送信し、これに対して FlexConnect AP は次のように動作します。

- FlexConnect AP が接続モードの場合、すべての IAPP メッセージをコントローラに転送し、コントローラはローカル モード AP と同様に IAPP メッセージを処理します。有線またはワイヤレス クライアント宛のトラフィックは、FlexConnect AP からローカルにスイッチングされます。
- スタンドアロン モードの AP は、IAPP メッセージを処理します。WGB 上の有線またはワイヤレス クライアントは、登録と登録解除を行うことができる必要があります。FlexConnect AP は接続モードに移行するときに、有線クライアントの情報をコントローラに送信します。FlexConnect AP がスタンドアロン モードから接続モードに移行するとき、WGB は登録メッセージを 3 回送信します。

  有線またはワイヤレス クライアントは WGB の設定を継承します。つまり、AAA 認証、AAA オーバーライド、FlexConnect ACL などの個別の設定は、WGB の背後にあるクライアントについては不要です。

FlexConnect WGB/uWGB の要約

- FlexConnect AP 上で WGB をサポートするために、WLC 上で特別な設定は不要です。
- 耐障害性は、WGB および WGB の背後にあるクライアントに対してサポートされています。
- WGB がサポートされている IOS AP は、1240、1130、1140、1260、1250 です。

FlexConnect WGB/uWGB の制限事項

- WGB の背後にある有線クライアントは、常に WGN 自体と同じ VLAN にあります。ローカル スイッチングが設定された WLAN の FlexConnect AP では、WGB 背後のクライアントに対する複数 VLAN はサポートされません。
- ローカル スイッチングが設定された WLAN 上の FlexConnect AP にアソシエーションされている場合、WGB の背後では、最大 20 台のクライアント（有線またはワイヤレス）がサポートされています。
- ローカル スイッチングが設定された WLAN にアソシエーションされている WGB の背後にあるクライアントについては、WebAuth はサポートされません。

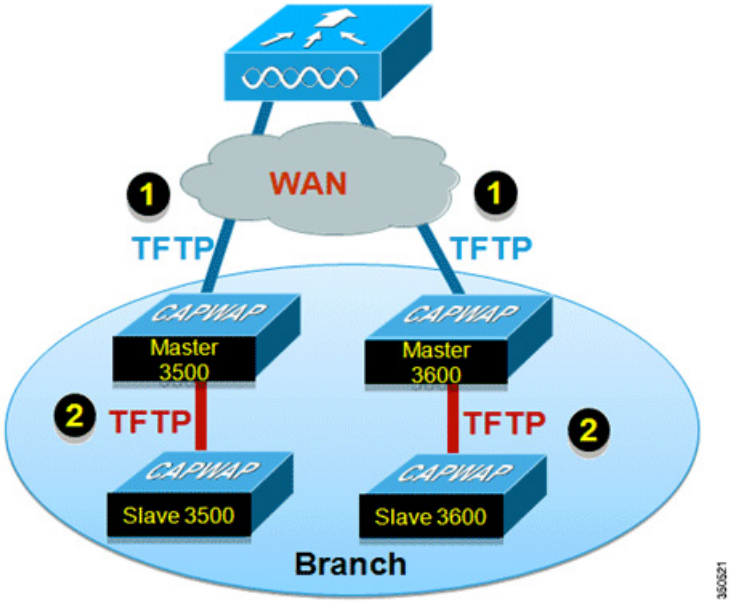
FlexConnect AP イメージのスマート アップグレード

イメージのプレダウンロード機能は、ダウンタイムをある程度削減する効果があります。しかし、すべての FlexConnect AP は WAN リンク経由でそれぞれの AP イメージをプレダウンロードしなければならないため、大幅な遅延が発生します。

効率的な AP イメージ アップグレードでは、個々の FlexConnect AP のダウンタイムが削減されます。基本的な原理は、各 AP モデルにつき、それぞれ 1 つの AP のみがコントローラからイメージをダウンロードし、マスター（サーバ）として機能します。同モデルのその他の AP はスレーブ（クライアント）となり、マスターから AP イメージをプレダウンロードします。

サーバからクライアントへの AP イメージの配布はローカル ネットワーク上で行われるため、WAN リンクで遅延が発生しません。この結果、プロセスの実行時間が短縮されます。

図 7-9　　AP イメージのスマート アップグレード



AP イメージのスマート アップグレードの要約

- FlexConnect グループごとに、各 AP モデルのマスターおよびスレーブ AP が選出されます。
- マスターは WLC からイメージをダウンロードします。
- スレーブは、マスター AP からイメージをダウンロードします。
- ダウンタイムが削減され、WAN帯域幅を節約できます。

FlexConnect ローカル スイッチングの VideoStream

リリース 8.0 では、ブランチ オフィス環境用に、ローカル スイッチングによる VideoStream 機能が導入されました。

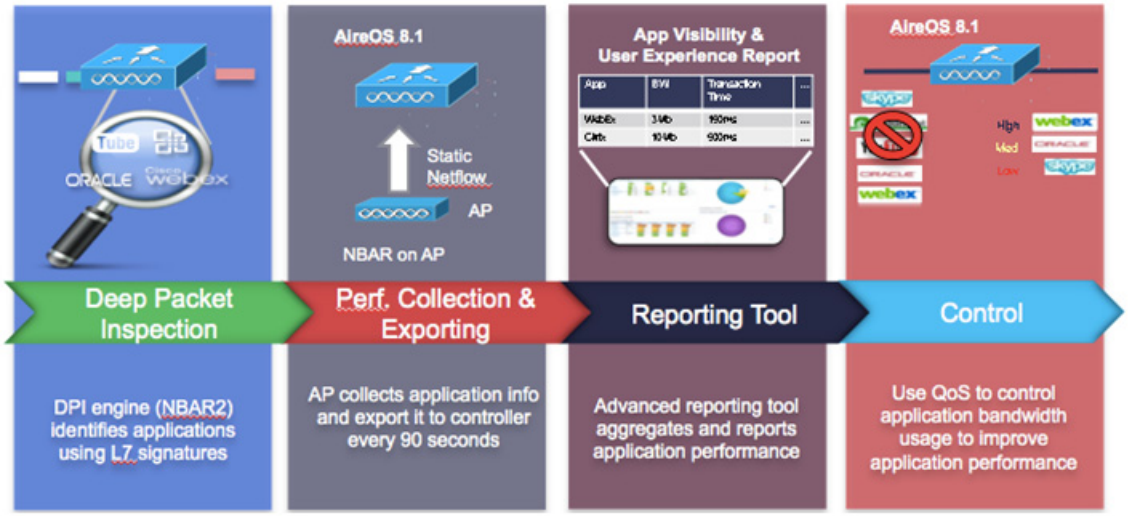
この機能により、エンタープライズ環境で現在実現されている機能と同様に、ワイヤレス アーキテクチャでも、ブランチ間のマルチキャスト ビデオ ストリーミングの展開が可能となります。

この機能は、ブランチ ネットワーク内でビデオ ストリームとクライアントの規模を拡大する場合に、ビデオ配信の質が低下するという欠点を補います。VideoStream は、ワイヤレス クライアントに対するビデオ マルチキャストの信頼性を高め、ブランチ内のワイヤレス帯域幅の使用効率を向上させます。

FlexConnect の Application Visibility and Control

AVC は、ワイヤレス ネットワークでのアプリケーション対応制御を可能にし、管理性と生産性を向上させます。AVC は、ASR、ISR G2 および WLC プラットフォーム上ですでにサポートされています。FlexConnect AP に組み込まれている AVC のサポートは、さらに機能拡張され、エンドツーエンドのソリューションとなっています。ネットワーク内のアプリケーションは完全に可視化され、管理者はアプリケーションに対し、特定のアクションを実行できます。

図 7-10　FlexConnect の Application Visibility and Control



- FlexConnect AP 上で NBAR2 エンジンが実行されます。
- DPI エンジン（NBAR2）を使用して、アクセス ポイントでアプリケーションの分類が行われ、L7 シグニチャを使用してアプリケーションが識別されます。
- AP はアプリケーション情報を収集し、90 秒ごとにコントローラにエクスポートします。
- リアルタイム アプリケーションは、コントローラのユーザ インターフェイスでモニタされます。
- FlexConnect アクセス ポイントで分類されたアプリケーションでは、アクション、ドロップ、マーキング、またはレート制限を実行できます。

AVC の仕様および制限

- FlexConnect AP の AVC では、1000 種類以上のアプリケーションを分類し、アクションを実行できます。
- FlexConnect AP で稼働するプロトコル パックは、WLC 上で稼働するプロトコルパックとは異なります。
- AVC による GUI の統計情報は、デフォルトでは上位 10 のアプリケーションに対して表示されます。これを、上位 20 または 30 のアプリケーションに変更することもできます。
- FlexConnect グループ内のローミングがサポートされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドはサポートされません。

- マルチキャスト トラフィックは、AVC アプリケーションではサポートされません。
- リリース 8.1 では、FlexConnect AVC の NetFlow エクスポートはサポートされません。

展開に関する一般的な考慮事項

- いずれの WLC でも FlexConnect AP 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 AP 合計数に応じて、FlexConnect 展開をサポートするための専用 WLC の使用を検討することは（管理上の観点から）有効です。
- FlexConnect AP は一般的に、メイン キャンパス内の AP と同じポリシーは共有しません。各ブランチ ロケーションは、基本的にそれ自体が RF およびモビリティ ドメインです。単一の WLC を複数の論理 RF およびモビリティ ドメインに分割することはできませんが、専用 WLC を使用することで、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。
- 専用 FlexConnect WLC を展開する場合は、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 に参加するすべての FlexConnect AP は、その RF およびモビリティ ドメインのメンバーとなります。
- 自動 RF の観点から、WLC は十分な数の FlexConnect AP が所定のブランチ内に展開されていると想定し、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。
- 各 FlexConnect AP を独自のモビリティ ドメインに統合しても、利点も不都合もありません。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ングされるためです。EoIP モビリティ トンネルは、クライアントが FlexConnect AP にローミングする（同じモビリティ ドメインの）WLC 間では実行されません。
- FlexConnect 展開に専用 WLC を使用する場合、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 AP 展開と同様、指定の WLC とのアソシエーションが強制的に適用されるように、FlexConnect AP にも WLC 優先度を設定する必要があります。
- 分散ブランチ オフィスを展開する場合は、最小 WAN 帯域幅、最大 RTT、最小 MTU、フラグメンテーションなど、特定の構成要件を考慮する必要があります。
- 使用する AP モデルが FlexConnect をサポートしていることを確認します。AP モデル OEAP600 は、FlexConnect モードをサポートしていません。
- UDP ポート 5246 で CAPWAP 制御チャネルのトラフィックが優先されるように、QoS を設定します。
- 静的 IP アドレスまたは DHCP アドレスのいずれかを持つ FlexConnect AP を展開することができます。DHCP サーバがローカルで使用可能になっており、ブートアップ時に AP に IP アドレスを提供できる必要があります。
- FlexConnect は最大で 4 つの断片化されたパケット、または最低 500 バイトの最大伝送単位（MTU）WAN リンクをサポートします。
- ラウンドトリップ遅延は、AP とコントローラ間で 300 ミリ秒を超えないようにする必要があります。ラウンドトリップ遅延を 300 ミリ秒以下に抑えられない場合は、ローカル認証を実行するよう AP を設定します。
- FlexConnect には、堅牢な耐障害性手法が実装されています。AP とコントローラが同一の設定を有する場合、クライアントと FlexConnect AP 間の接続（再結合またはスタンバイ）はそのまま維持され、クライアントではシームレスな接続が行われます。

- FlexConnect AP のプライマリ コントローラとセカンダリ コントローラの設定が同一であることが必要です。そうでない場合、AP がその設定を失い、特定の機能（WLAN オーバーライド、VLAN、静的チャネル番号など）が期待どおりに動作しない場合があります。さらに、FlexConnect AP の SSID とそのインデックス番号が、両方のコントローラで同一であることを確認してください。
- クライアント接続は、AP がスタンドアロン モードから接続モードに移行するときに RUN 状態になっている、ローカルにスイッチングされたクライアントに対してのみ復元されます。AP がスタンドアロン モードから接続モードに移行すると、AP の無線もリセットされます。
- AP がコントローラへの接続を確立すると、セッション タイムアウトと再認証が行われます。
- セッション タイマーが切れると、クライアントのユーザ名、現在の（サポートされる）レート、リッスン インターバルの値はデフォルト値にリセットされます。クライアント接続が再確立されるときに、コントローラはクライアントの元の属性を復元しません。
- 複数の FlexConnect グループを 1 つのロケーションで定義できます。ロケーションごとの FlexConnect AP の展開数に制限はありません。
- FlexConnect モードでは、AP はユニキャスト形式でのみマルチキャスト パケットを受信できます。
- FlexConnect AP は、真のマルチキャストを除くすべての機能に対して、1 対 1 ネットワーク アドレス変換（NAT）設定とポート アドレス変換（PAT）をサポートします。ユニキャスト オプションを使用して設定されている場合、NAT の境界を越えるマルチキャストもサポートされます。FlexConnect AP は、中央でスイッチングされるすべての WLAN に対して真のマルチキャストが動作するようにしたい場合を除き、多対 1 の NAT/PAT 境界もサポートします。

（注） NAT と PAT は FlexConnect AP ではサポートされていますが、対応するコントローラではサポートされていません。シスコは、NAT/PAT 境界の背後にコントローラを置く構成はサポートしません。

- AP で、これらのセキュリティ タイプがローカルにアクセス可能である場合、VPN および PPTP は、ローカルにスイッチングされるトラフィックに対してサポートされます。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect ローカル スイッチング用に設定された WLAN ではサポートされません。
- ワーク グループ ブリッジおよびユニバーサル ワーク グループ ブリッジは、ローカルでスイッチングされるクライアントの FlexConnect AP でサポートされます。
- FlexConnect AP はクライアント ロード バランシングをサポートしません。
- FlexConnect は、IPv4 の動作と同様にトラフィックをローカル VLAN にブリッジすることによって、IPv6 クライアントをサポートします。
- FlexConnect では、IPv6 ACL、ネイバー探索キャッシュ、IPv6 NDP パケットの DHCPv6 スヌーピングはサポートされていません。
- ローカル スイッチング WLAN を使用する FlexConnect AP は、IP ソース ガードを実行して ARP スプーフィングを防ぐことはできません。中央でスイッチングされる WLAN では、ワイヤレス コントローラは IP ソース ガードおよび ARP スプーフィングを実行します。ローカル スイッチングを使用する FlexConnect AP の ARP スプーフィング攻撃を防止するために、シスコは ARP インスペクションの使用を推奨します。

Cisco Aironet Wave 2 AP でのモバイル コンシェルジュのサポート（Hotspot 2.0）

すべての Cisco Aironet Wave 2 AP で、モバイル コンシェルジュがサポートされています。

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークを接続するのに役立ちます。

ネットワークが提供するサービスは 2 つのプロトコルに分類できます。

- 802.11u MSAP
- 802.11u Hotspot 2.0

AireOS コード 8.5 以降、11ac Wave-2 AP（1800 シリーズ、2800 および 3800）で Passpoint を有効にできます。これは Wave-1 AP と同等の機能を超える、最新の Passpoint 2.0 テクノロジーへの更新です。

Cisco AP では Passpoint 認定と、AP モデル間の相互運用性が広範にサポートされています。WLC では、AireOS 8.2 コード以降 Passpoint 2.0 がサポートされており、8.5 では Wave-2 AP のサポートが追加されています。また、8.5 が動作する Mobility Express でも Passpoint 2.0 機能を使用できます。

CHAPTER 8

Cisco ワイヤレス メッシュ ネットワーク

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

(注) Cisco Wireless Mesh Networking の構成や導入などの詳細については、『Cisco Mesh Access Points, Design and Deployment Guide, Release 8.5』を参照してください。

メッシュ ネットワーキングでは、Cisco 1500 シリーズの屋外および屋内メッシュ アクセス ポイント（AP）、Cisco Wireless LAN Controller（WLC）、Cisco Prime Infrastructure を組み合わせて、スケーラブルな集中管理と屋内外の展開のモビリティを提供しています。Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、ネットワークへのメッシュ AP の接続を管理します。

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

この章で説明する機能は、次の製品に該当します。

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

メッシュ アクセス ポイント

アクセス ポイントのロール

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

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

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

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

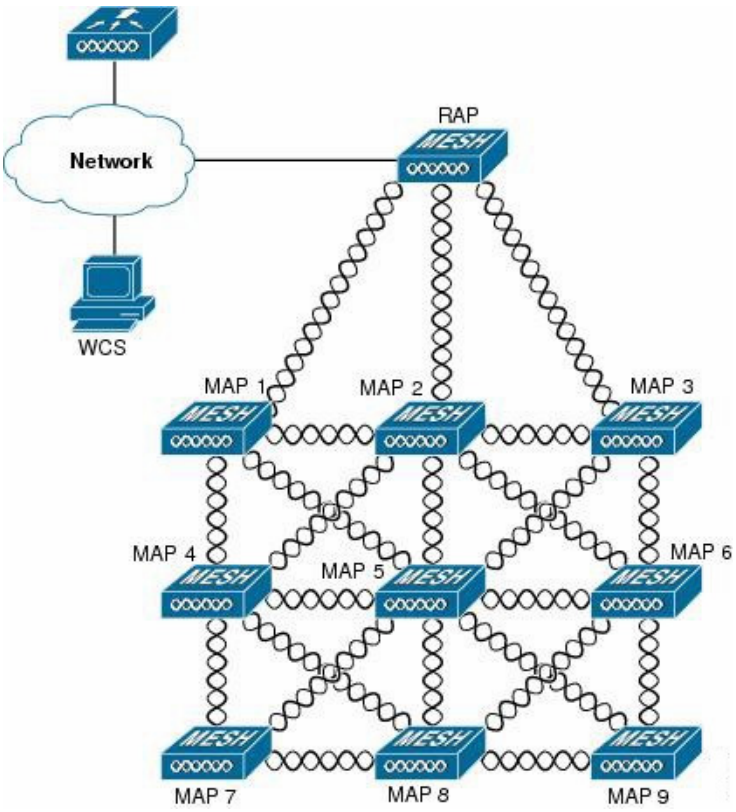
MAP は MAP 間および RAP への通信に 802.11a/n 無線バックホールを使用して無線接続を行います。MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。

ブリッジ モードのアクセス ポイントでは、CleanAir によって周波数 5 GHz のメッシュ バックホールがサポートされ、干渉デバイス レポート（IDR）および電波品質の指標（AQI）レポートのみが生成されます。

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

図 8-1 は、メッシュ ネットワーク内の MAP と RAP の間にある関係を示しています。

図 8-1　　単純なメッシュ ネットワーク階層



ネットワークアクセス

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

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

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

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

- MAC 認証: メッシュ アクセス ポイントが参照可能データベースに追加され、特定のコントローラおよびメッシュ ネットワークに確実にアクセスできるようにします。
- 外部 RADIUS 認証: メッシュ アクセス ポイントは、証明書付きの拡張認証プロトコル（EAP-FAST）のクライアント認証タイプをサポートする Cisco ACS（4.1 以上）または ISE 2.X などの RADIUS サーバを使用して、外部から認証できます。

ネットワークのセグメント化

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

Cisco 屋内メッシュ アクセス ポイント

屋内メッシュは次のアクセス ポイントで使用できます。

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

（注）　Cisco 1040 シリーズ、1140 シリーズ、および 1260 シリーズのアクセス ポイントは、シスコ ワイヤレス リリース 8.0 と同等の機能を備えています。シスコ ワイヤレス リリース 8.1 以降で導入された機能は、これらのアクセス ポイントではサポートされません。

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

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

エンタープライズ 11ac メッシュは、P2P、P2MP、およびアーキテクチャのメッシュ タイプをサポートします。

屋内アクセス ポイントをブリッジ モードに直接設定して、これらのアクセス ポイントをメッシュ アクセス ポイントとして直接使用できます。これらのアクセス ポイントがローカル モード（非メッシュ）である場合は、これらのアクセス ポイントをコントローラに接続し、AP モードをブリッジ モード（メッシュ）に変更する必要があります。このシナリオは、特に、展開しているアクセス ポイントの数が多い場合や、従来の非メッシュ ワイヤレスをカバーするためにアクセス ポイントをすでにローカル モードで展開している場合に猥雑になることがあります。

Cisco 屋内メッシュ アクセス ポイントは、次の 2 つの同時に動作する無線を装備しています。

- UBA が有効になっている場合にデータ バックホールおよびクライアント アクセスに使用される 2.4 GHz 無線（リリース 8.2 以降）
- データ バックホールおよびクライアント アクセスに 5 GHz 帯を使用（ユニバーサル バックホール アクセスが有効な場合）

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

Cisco 屋外メッシュ アクセス ポイント

Cisco 屋外メッシュ アクセス ポイントは、Cisco Aironet 1500 シリーズ アクセス ポイントから構成されます。1500 シリーズには、1572 11ac 屋外アクセス ポイント、1552/1532 11n 屋外メッシュ アクセス ポイント、および 1540/1560 11ac Wave 2 シリーズが含まれています。

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

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

AP1500 には、次の 2 種類の構成モデルがあります。

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

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

AP1500 は、厳しい環境向けハードウェア格納ラックに設置します。厳しい環境に対応する AP1500 は、Class I、Division 2、Zone 2 の厳しい環境での安全基準を満たしています。

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

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

(注) これらのモードは、GUI と CLI のどちらを使用しても設定できます。設定手順については、『Cisco Wireless LAN Controller Configuration Guide』を参照してください。Cisco ワイヤレス メッシュ アクセス ポイント リリース 8.5 設計および導入ガイド

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

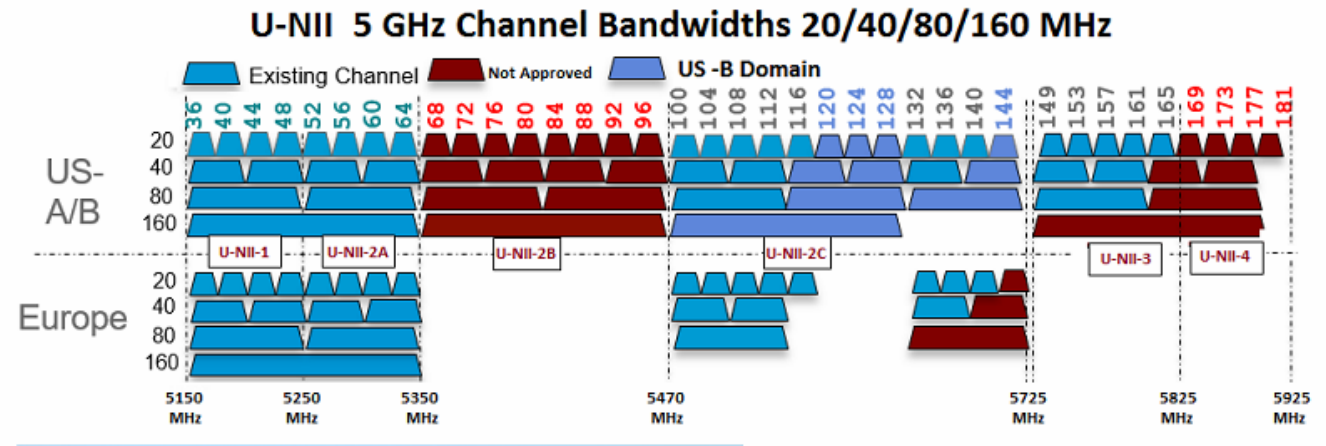
屋外メッシュ AP のすべてのモデルの詳細と仕様については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/products/wireless/outdoor-wireless/index.html?stickynav=1

周波数帯域

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

次に示すチャネル帯域は、すべての 1500 シリーズ メッシュ AP でサポートされます。

図 8-2　　メッシュ AP の 802.11a/n/ac 無線でサポートされる周波数帯域



米国 FCC

U-NII-1

屋内と屋外の利用可能周波数に追加

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

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

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

U-NII-2A と U-NII2C

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

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

U-NII-3

周波数帯が 5825 MHz から 5850 MHz に拡張

欧州

U-NII-1

最大 23 dBm - 屋外での使用不可

U-NII-2A

最大 23 dBm - 屋外での使用不可

U-NII-2C

最大 30 dBm

U-NII-3

英国では屋内用に 23 dBm でのみ使用可

動的周波数選択

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

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

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

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

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

アンテナ

概要

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

- 指向性
- 全方向性

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

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

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

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

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

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

アンテナ オプション

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

シスコのアンテナおよびアクセサリについては、『Cisco Aironet Antenna and Accessories Reference Guide』を参照してください。

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

クライアント アクセス認定アンテナ(サードパーティ製アンテナ)

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

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

Cisco Wireless LAN Controller

ワイヤレス メッシュ ソリューションは、Cisco 2500、3504、5500、および 8500 シリーズ ワイヤレス LAN コントローラでサポートされます。

Cisco 2500、3504、5500、および 8500 シリーズ ワイヤレス LAN コントローラの詳細については、https://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html を参照してください。

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、ワイヤレス メッシュを視覚的に計画、設定、管理できるプラットフォームです。Prime Infrastructure を使用することで、ネットワーク管理者は、ワイヤレス メッシュ ネットワークの設計、コントロール、モニタリングを一元的に行えます。

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

Prime Infrastructure は、組み込みデータベースと共に、サーバ プラットフォームで実行されます。これにより、何百ものコントローラや何千もの Cisco メッシュ アクセス ポイントを管理できるスケーラビリティが提供されます。コントローラは、Prime Infrastructure と同じ LAN 上、個別にルートが設定されたサブネット上、または広域接続全体にわたって配置できます。

アーキテクチャ

Control and Provisioning of Wireless Access Points

Control And Provisioning of Wireless Access Points（CAPWAP）は、コントローラがネットワーク内のアクセス ポイント（メッシュおよび非メッシュ）を管理するために使用するプロビジョニングおよび制御プロトコルです。

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

メッシュ ネットワークの CAPWAP ディスカバリ

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

ステップ 1　CAPWAP ディスカバリの開始前に、メッシュ アクセス ポイントがリンクを確立します。一方、非メッシュ アクセス ポイントの場合は、そのメッシュ アクセス ポイント用のスタティック IP（ある場合）を使用して、CAPWAP ディスカバリを開始します。

ステップ 2　メッシュ アクセス ポイントは、レイヤ 3 ネットワークのメッシュ アクセス ポイントのスタティック IP を使用して CAPWAP ディスカバリを開始するか、割り当てられたプライマリ、セカンダリ、ターシャリのコントローラ用のネットワークを探します。接続するまで最大 10 回試行されます。

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

ステップ 3　ステップ 2 が 10 回の試行の後に失敗した場合、メッシュ アクセス ポイントは DHCP にフォールバックし、接続を 10 回試行します。

ステップ 4　ステップ 2 とステップ 3 の両方に失敗し、コントローラに対して成功した CAPWAP 接続がない場合、メッシュ アクセス ポイントは LWAPP にフォール バックします。

ステップ 5　ステップ 2、ステップ 3、ステップ 4 の試行後にディスカバリがなかった場合、メッシュ アクセス ポイントは次のリンクを試みます。

ダイナミック MTU 検出

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

Mesh Deployments リリース 8.4 の Air Time Fairness

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

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

8.4 リリースでの前提条件とサポートされている機能

メッシュ ATF は、AireOS 8.4 とリリース ノートに記載されているその他すべてのサポート対象 AP でサポートされます。メッシュ ATF は、1550/128, 1570、およびその他すべての IOS ベースの AP でサポートされます。

表 8-1

	アクセス ポイント						
	1550（64 MB）	**1550（128 MB）**	**1570**	**3700**	**1530**	**1540**	**1560**
機能							
基本メッシュ	Yes	Yes	Yes	Yes	Yes	はい	8.4
Flex+メッシュ	Yes	Yes	Yes	Yes	○	×	いいえ
高速コンバージェンス（バックグラウンド スキャン）	いいえ	8.3	8.3	Yes	8.3	いいえ	8.4
RAP の有線クライアント	Yes	Yes	○	No	Yes	×	いいえ

表 8-1

	アクセス ポイント						
	1550（64 MB）	**1550（128 MB）**	**1570**	**3700**	**1530**	**1540**	**1560**
MAP の有線クライアント	Yes	Yes	○	No	Yes	いいえ	8.4
デイジーチェーン	7.6	7.6	7.6	いいえ	7.6	×	いいえ
LSC	Yes	Yes	Yes	Yes	○	×	いいえ
PSK プロビジョニング: MAP-RAP 認証	8.2	8.2	8.2	8.2	8.2	8.5	8.4
メッシュの ATF	いいえ	8.4	8.4	8.4	×	×	No

Cisco Air Time Fairness（ATF）の使用例

公共ホットスポット（スタジアム/空港/会議場/その他）

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

Education

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

一般企業、サービス業、小売業

この場合、施設は、従業員とゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービス プロバイダーによってさらに分割できます。ゲストはサービス レベルによってサブグループ化し、サブグループごとに一定の通信時間を割り当てることができます（有料のグループには、無料のグループよりも多く割り当てるなど）。

時間を共有するマネージド ホットスポット

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

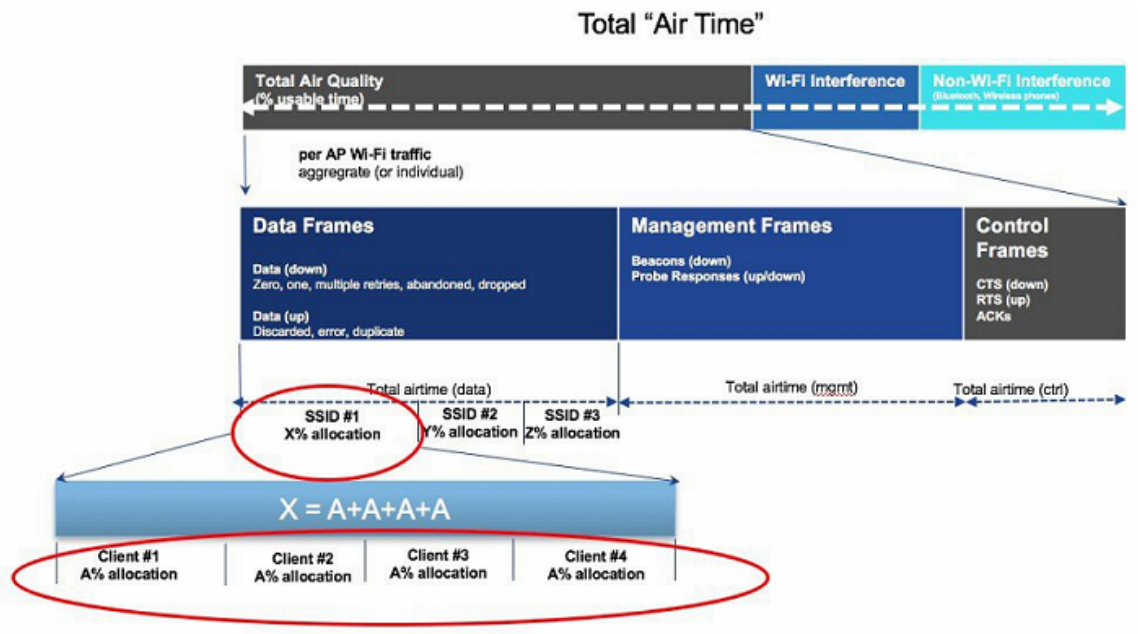
ATF の機能

ATF 機能：

- ATF ポリシーは、ダウンリンク方向（AP がクライアントにフレームを送信する方向）でのみ適用されます。ダウンリンク、つまり AP からクライアント方向の通信時間のみが、AP によって正確に制御されます。アップリンク方向（クライアントから AP）のエアタイムの測定も可能ですが、厳密に制御することはできません。AP は、クライアントに送信するパケットの通信時間を抑制できますが、それぞれの通信時間を制限できないため、クライアントから「聞ける」パケットの通信時間のみを測定できます。

- ATF ポリシーはワイヤレス データ フレームにのみ適用されます。管理および制御フレームは無視されます。
- ATF が SSID ごとに設定される場合、各 SSID は設定されたポリシーに従って通信時間が許可されます。
- ATF は、エアタイム ポリシーを超過したフレームをドロップまたは遅延させるように設定できます。フレームが保留されると、問題となっている SSID に十分な通信時間が割り当てられた時点でバッファされて送信されます。当然ながら、バッファが可能なフレーム数には制限があります。この制限を超えた場合、フレームがドロップされます。
- ATF はグローバルに有効または無効にすることができます。
- ATF は、個々のアクセス ポイント、AP グループ、またはネットワーク全体で有効または無効にすることができます。
- 割り当ては、SSID およびクライアントごとに適用されます。
- ダウンストリームだけに適用されます。
- WLC GUI/CLI および PI で設定できます。
- ネットワーク上のすべての AP、AP グループ、または 1 つの AP に適用できます。
- ローカル モードの AP（**AP1260、1550 128 Mb、1570、1700、2600、2700、3500、3600、3700**）でサポートされます。

(注)　COS ベースの AP または Wave-2 AP では、リリース 8.5 の ATF はサポートされません。



詳細と ATF 設定手順については、『Mesh Deployment Guide rel 8.5』（https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-5/b_mesh_85.html）を参照してください。

Adaptive Wireless Path Protocol

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

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

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

ルートを最適化するため、MAP はネイバー MAP をアクティブに送信要求します。要請メッセージのやり取りの際に、MAP は RAP への接続に使用可能なネイバーをすべて学習し、最適なパスを提供するネイバーを決定して、そのネイバーと同期します。AWPP では、リンクの品質とホップ数に基づいてパスが決定されます。

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

トラフィック フロー

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

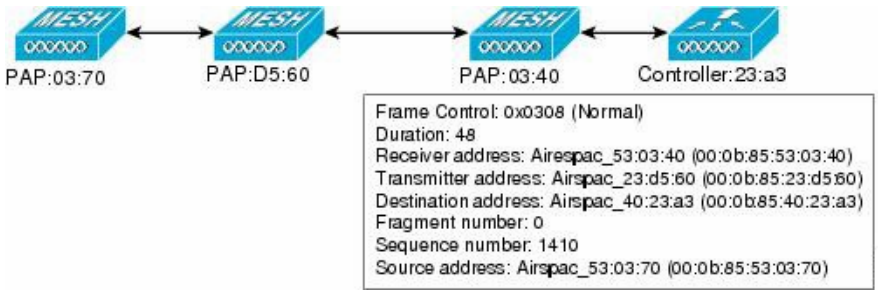
- オーバーレイ CAPWAP トラフィック：標準の CAPWAP アクセス ポイントの配置内のフローで、CAPWAP アクセス ポイントと CAPWAP コントローラの間の CAPWAP トラフィックのことです。
- ワイヤレス メッシュ データ フレーム フロー
- AWPP 交換

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

802.11 データ フレームは、レシーバ、トランスミッタ、送信先、発信元の 4 つまでのアドレス フィールドを使用できます。WLAN クライアントから AP までの標準フレームでは、トランスミッタ アドレスと発信元アドレスが同じため、これらのアドレス フィールドのうち 3 つしか使用されません。しかし、WLAN ブリッジング ネットワークでは、フレームが、トランスミッタの背後にあるデバイスによって生成された可能性があるため、フレームの発信元がフレームのトランスミッタであるとは限らず、4 つのすべてのアドレス フィールドが使用されます。

図 8-3 は、このタイプのフレーム構成の例を示しています。フレームの発信元アドレスは MAP:03:70、このフレームの送信先アドレスはコントローラ（メッシュ ネットワークはレイヤ 2 モードで動作しています）、トランスミッタ アドレスは MAP:D5:60、レシーバ アドレスは RAP:03:40 です。

図 8-3　　ワイヤレス メッシュ フレーム

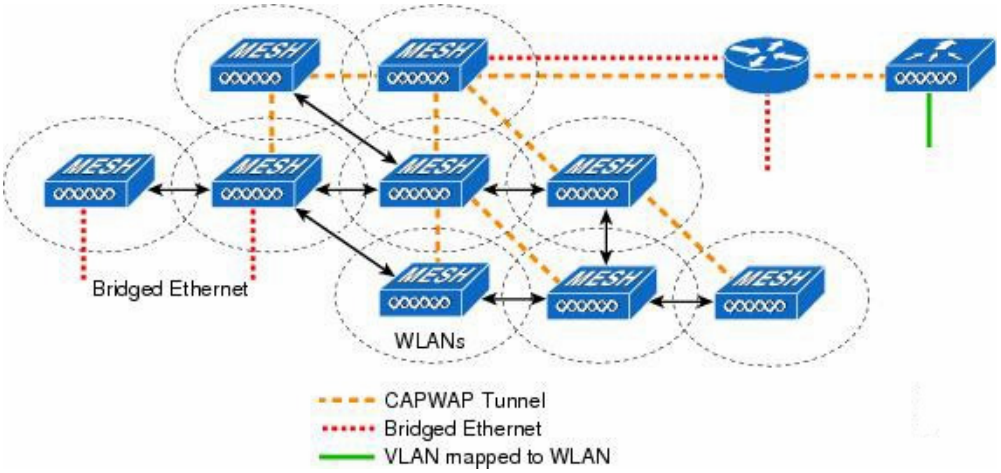


このフレームの送信により、トランスミッタとレシーバのアドレスは、ホップごとに変わります。各ホップでレシーバ アドレスを判別するために AWPP が使用されます。トランスミッタ アドレスは、現在のメッシュ アクセス ポイントのアドレスです。パス全体を通して、発信元アドレスと送信先アドレスは同一です。

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

メッシュ内の各メッシュ アクセス ポイントは、コントローラと共に、CAPWAP セッションを形成します。WLAN トラフィックは CAPWAP 内にカプセル化されるため、コントローラ上の VLAN インターフェイスにマップされます。ブリッジされたイーサネット トラフィックは、メッシュ ネットワーク上の各イーサネット インターフェイスから渡される可能性があり、コントローラのインターフェイスにマップされる必要はありません（図 8-4 を参照）。

図 8-4　　論理ブリッジと WLAN マッピング

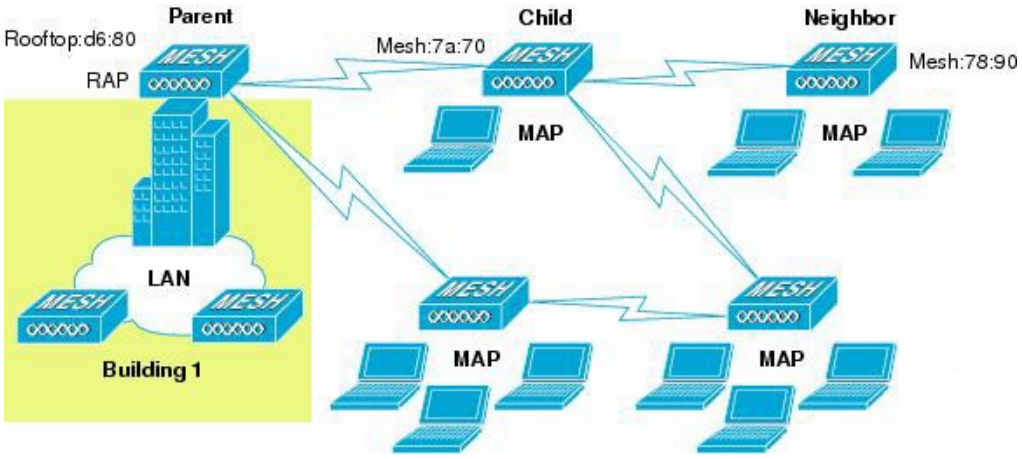


メッシュ ネイバー、親、および子

メッシュ アクセス ポイント間の関係は、親、子、ネイバーです（図 8-5 を参照）。

- 親アクセス ポイントは、容易度の値（ease value）に基づいて RAP への最適なルートを提供します。親は RAP 自身または別の MAP のいずれかです。
  - 容易度の値（ease value）は各ネイバーの SNR およびリンク ホップ値を用いて計算されます。複数の選択肢がある場合、通常は緩和値の高いアクセス ポイントが選択されます。
- 子アクセス ポイントは、RAP に戻る最適なルートとして親アクセス ポイントを選択します。
- ネイバー アクセス ポイントは、他のアクセス ポイントの RF 範囲内にありますが、その容易度の値（ease value）は親よりも低いため、親や子としては選択されません。

図 8-5　親、子、およびネイバー アクセス ポイント



最適な親を選択するための基準

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

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

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

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

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

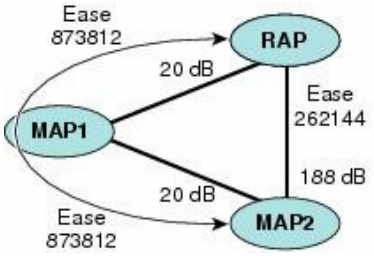
親メッシュ アクセス ポイントは、RAP に戻る最適なパスを提供します。AWPP は、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

容易度の計算

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

図 8-6 では、親パスの選択で、MAP2 は MAP1 を通るパスを選択します。このパスを通る調整された容易度の値（436906）が、MAP2 から RAP に直接進むパスの容易度の値（262144）より大きいためです。

図 8-6　　親パスの選択



親の決定

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

調整された容易度 = 最小値（各ホップでの容易度）ホップ カウント

SNR スムージング

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

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

ループの防止

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

メッシュ AP のバックグラウンド スキャン リリース 8.3

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

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

両方の機能を備えることで、メッシュ ツリーのサード ホップ MAP は、データ パスの再コンバージェンスと回復を 10 秒未満で行うことができます。

この新しいメッシュ バックグラウンド スキャンと自動親選択により、コンバージェンス時間と親選択の信頼性および安定性がいっそう向上します。MAP が任意のチャネルでより適切な親候補を見つけて接続し、最適な親とのアップリンクを常に維持できるようになるからです。

（注）　この BG スキャンの実装は、Marvell ベースの AP、具体的には、AP1550、AP1560、AP1570、IW3702 に適用できます。

子 MAP は、キープアライブとして機能する AWPP - Neighbor Discovery Request/Response（NDReq/NDResp）メッセージを使用して親とのアップリンクを維持します。NDResp メッセージが連続して失われた場合、親が失われたとみなされ、子 MAP は新しい親を見つけようとします。MAP は、現在のオンチャネルのネイバーのリストを保持し、現在の親を失ったときには、同じサービス チャネル内の次の最適なネイバー候補へのローミングを試みます。ただし、同じチャネルに他のネイバーが見つからない場合は、すべて/サブセットのチャネルをスキャン/シークして親を見つける必要があります。

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

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

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

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

表 8-2

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

DFS と非 DFS チャネル スキャン

非 DFS チャネル スキャン

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

DFS チャネル スキャン

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

- MAP がオフチャネル スキャン中に DFS チャネルを介してパケットを受信できるようにするため、その他すべてのオンチャネル DFS ネイバーは、直近の 50 ミリ秒間 Tx/Rx がない場合に AWPP メッシュ ビーコンを送信します。
- これらのメッシュ ビーコンにより、DFS チャネル上でオフチャネルを実行している MAP は、「安全に送信可能」と宣言してオフチャネル アクティビティを実行できます。

メッシュ導入モード

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

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

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

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

無線バックホール

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

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

ユニバーサル アクセス

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

ポイントツーポイント無線ブリッジング

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

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

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

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

1. メッシュ ノードをブリッジとして使用する場合。
2. MAP でイーサネット ポートを使用してイーサネット デバイス（ビデオ カメラなど）を接続する場合。

該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP に対してイーサネット ブリッジングを有効にします。たとえば、Hop 2 の MAP2 でイーサネット ブリッジングを有効にする場合は、MAP1（親 MAP）と、コントローラに接続している RAP でもイーサネット ブリッジングを有効にする必要があります。

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

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

範囲：150 ～ 132,000 フィート;

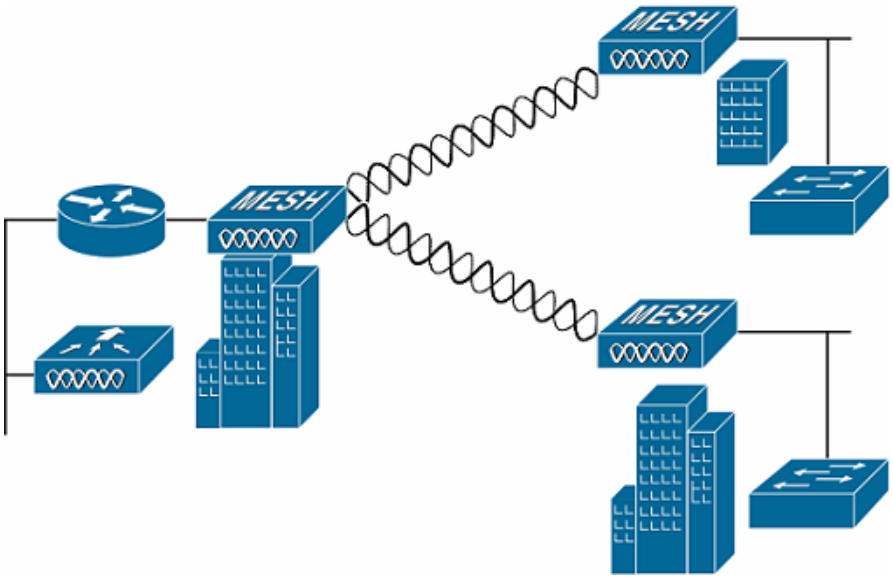
デフォルト：12,000 フィート

ポイントツーマルチポイント無線ブリッジング

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

図 8-7 は、1 つの RAP と 2 つの MAP がある単純な導入を示していますが、この構成は基本的に WLAN クライアントがないワイヤレス メッシュです。イーサネット ブリッジングを有効にすることでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアント アクセスに適していないことがあります。

図 8-7　　ポイントツーマルチポイント ブリッジングの例



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

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

- メッシュ ノードをブリッジとして使用する場合。
- MAP でイーサネット ポートを使用してイーサネット デバイス（ビデオ カメラなど）を接続する場合。

該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP に対してイーサネット ブリッジングを有効にします。たとえば、Hop 2 の MAP2 でイーサネット ブリッジングを有効にする場合は、MAP1（親 MAP）と、コントローラに接続している RAP でもイーサネット ブリッジングを有効にする必要があります。

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

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

- レンジ：150 ～ 132,000 フィート
- デフォルト：12,000 フィート

ワイヤレス バックホールのデータ レート

バックホールは、AP 間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは、AP に基づいてデフォルトで 802.11a または 802.11a/n になります。利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。また、レートはクライアント デバイスのスループットにも影響を与えることがあり、スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです。

Dynamic Rate Adaptation（DRA）には、パケット伝送のために最適な伝送レートを推測するプロセスが含まれます。レートを正しく選択することが重要です。レートが高すぎると、パケット伝送が失敗し、通信障害が発生します。レートが低すぎると、利用可能なチャネル帯域幅が使用されず、品質が低下し、深刻なネットワーク輻輳および障害が発生する可能性があります。

データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。低データ レート（6 Mbps など）のほうが、高データ レート（300 Mbps など）よりも AP からの距離を延長できます。結果として、データ レートはセル カバレッジ、および必要な AP の数に影響を与えます。異なるデータ レートは、ワイヤレス リンクで冗長度の高い信号を送信することにより（これにより、データをノイズから簡単に復元できます）、実現されます。1 Mbps のデータ レートでパケットに対して送信されるシンボル数は、11 Mbps で同じパケットに使用されたシンボル数より多くなります。したがって、低ビット レートでのデータの送信には、高ビット レートでの同じデータの送信よりも時間がかり、スループットが低下します。

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

ClientLink テクノロジー

多くのネットワークは、依然として 802.11a/g クライアントと 802.11n クライアントの混在をサポートします。802.11a/g クライアント（レガシー クライアント）は低データ レートで動作するため、古いクライアントにより、ネットワーク全体のキャパシティが減少することがあります。

Cisco ClientLink テクノロジーは、802.11a/g クライアントが、特にセル境界に近い場合に、最適なレートで動作できるように保証します。これにより、クライアントが混在するネットワークにおける 802.11n の採用に関連する問題を解決します。

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

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

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

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

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

Cisco ClientLink テクノロジーにより、クライアントが配置された場所で AP が SNR を効果的に最適化できるようになります。ClientLink は、ダウンリンク方向にほぼ 4 dB のゲインを提供します。SNR が改善され、再試行回数の減少やデータ レートの向上などの多くの利点が提供されます。たとえば、以前に 12 Mbps でパケットを受信できたセルの端にあるクライアントが 36 Mbps でパケットを受信できるようになります。ClientLink を使用した場合のダウンリンク パフォーマンスの一般的な測定値は、802.11a/g クライアントではスループットが 65 % 向上します。Wi-Fi システムがより高いデータ レート、少ない再試行回数で動作できるようにすることで、ClientLink はシステムのキャパシティ全体を拡張します。つまり、スペクトル リソースを効率的に利用できます。

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

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

最新情報については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_feature_matrix_for_802_11ac_wave2_access_points.html:

コントローラ プランニング

次の項目は、メッシュ ネットワークに必要なコントローラの数に影響します。

- ネットワーク内のメッシュ AP（RAP および MAP）。
- RAP とコントローラを接続する有線ネットワークは、そのネットワーク内でサポートされる AP の総数に影響を与えることがあります。このネットワークで、WLAN のパフォーマンスに影響を与えることなく、コントローラがすべての AP から等しく利用できるようになっている場合は、各 AP をすべてのコントローラにわたって均等に分散でき、効率が最大限に高められます。これに当てはまらず、コントローラがさまざまなクラスタまたは PoP にグループ化される場合は、AP の総数とカバレッジが減少します。
- コントローラごとにサポートされるメッシュ AP（RAP および MAP）の数。

本書では、わかりやすくするために非メッシュ AP をローカル AP と呼びます。

表 8-3　コントローラ モデル別にサポートされるメッシュ AP

コントローラ モデル	ローカル AP サポート（非メッシュ）[1]	サポート可能なメッシュ AP の最大数
5508[2]	500	500
2504[3]	75	75
3504	150	150
WiSM2	500	500
5520	1500	1500
8540	6000	6000

1. ローカル AP サポートは、コントローラ モデルでサポートされている非メッシュ AP の合計数です。
2. 5508 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。
3. 2504 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。

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

ワイヤレス メッシュ ネットワークのカバレッジに関する考慮事項

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

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

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

セルの計画と距離

Cisco 1520 シリーズ アクセス ポイント用

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

シスコでは、音声なしのネットワークでのセル計画と距離について、次の値を推奨します。

- RAP と MAP の比率:推奨最大比率は、RAP ごとに 20 の MAP です。
- AP 間の距離:各メッシュ AP 間に 2000 フィート（609.6 m）以下の間隔をあけることを推奨します。バックホール上でメッシュ ネットワークを拡張する（クライアント アクセスなし）場合、セルの半径には 1000 フィート（304.8 m）を使用してください。
- ホップ カウント:3 ～ 4 ホップ1 平方マイル（フィート換算で 52802）が 9 つのセル分で、およそ 3 または 4 のホップでカバーできます。
- 2.4 GHz の場合、ローカル アクセス セル サイズの半径は 600 フィート（182.88 m）です。1 つのセル サイズは 1.310 X 106 で、1 平方マイルあたりのセルは 25 個です。

メッシュ アクセス ポイントのコロケーション

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

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

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

隣接チャネルでの AP1500 のコロケーション

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

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

代替隣接チャネルでの AP1500 のコロケーション

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

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

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

CleanAir

1550 シリーズは、802.11n テクノロジーと統合無線および内部/外部アンテナを利用しています。1550 シリーズの AP は、現在の CleanAir 対応 Aironet 3600 および 3700 AP と同じチップセットをベースにしています。つまり、1550 シリーズの AP は CleanAir に対応しています。

7.3.101.0 リリースでは、2600 シリーズの AP は互いにメッシュ化でき、CleanAir 機能も搭載しています。

7.2.103.0 リリースでは、3600 シリーズの AP は互いにメッシュ化でき、CleanAir 機能も搭載しています。

7.0.116.0 リリースでは、3500 シリーズの AP は互いにメッシュ化でき、CleanAir 機能も搭載しています。

メッシュ（1552、2600、2700、3500、3600、3700）の CleanAir は 2.4 GHz 無線に実装でき、無線周波数（RF）を検出、位置を特定、分類、緩和すると同時にクライアントに完全な 802.11n データ レートを提供します。これにより、キャリア クラス管理およびカスタマー エクスペリエンスを実現し、展開されたロケーションのスペクトルを制御できます。屋外 11n プラットフォームの CleanAir 対応 RRM テクノロジーは、2.4 GHz 無線の Wi-Fi 干渉および Wi-Fi 以外の干渉を検出し、定量化して、緩和します。AP1552 は 2.4 GHz クライアント アクセス モードで CleanAir をサポートします。

CleanAir Advisor

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

ワイヤレス メッシュ モビリティ グループ

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

複数のコントローラ

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

CAPWAP コントローラを集中させると、操作上の利点がありますが、その利点は、CAPWAP AP へのリンクの速度とキャパシティ、およびこれらのメッシュ AP を使用している WLAN クライアントのトラフィック プロファイルに対するトレード オフとなります。

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

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

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

ワイヤレス メッシュ ネットワークで使用される CAPWAP モデルは、キャンパス ネットワーク向けに設計されています。つまり、CAPWAP メッシュ AP と CAPWAP コントローラ間のネットワークは高速で低遅延であることが前提となっています。

メッシュ可用性の向上

セルの計画と距離では、1 平方マイルのワイヤレス メッシュ セルが作成され、組み込まれました。このワイヤレス メッシュ セルは、携帯電話ネットワークの作成に使用されるセルに似た特性を持ちます。より大きな可用性やキャパシティに対して、同じ物理エリアをカバーするために、（定義された最大セル サイズより）小さいセルが作成される可能性があるからです。このプロセスは、セルに RAP を追加することで行われます。より大きなメッシュ配置と同様、同じチャネルで RAP を使用するか（図 8-8 を参照）、または別のチャネルに置いた RAP を使用するか（図 8-9 を参照）を決める必要があります。エリアへの RAP の追加により、そのエリアのキャパシティと回復力が増大します。

図 8-8　　同じチャネルでセルごとに 2 つの RAP

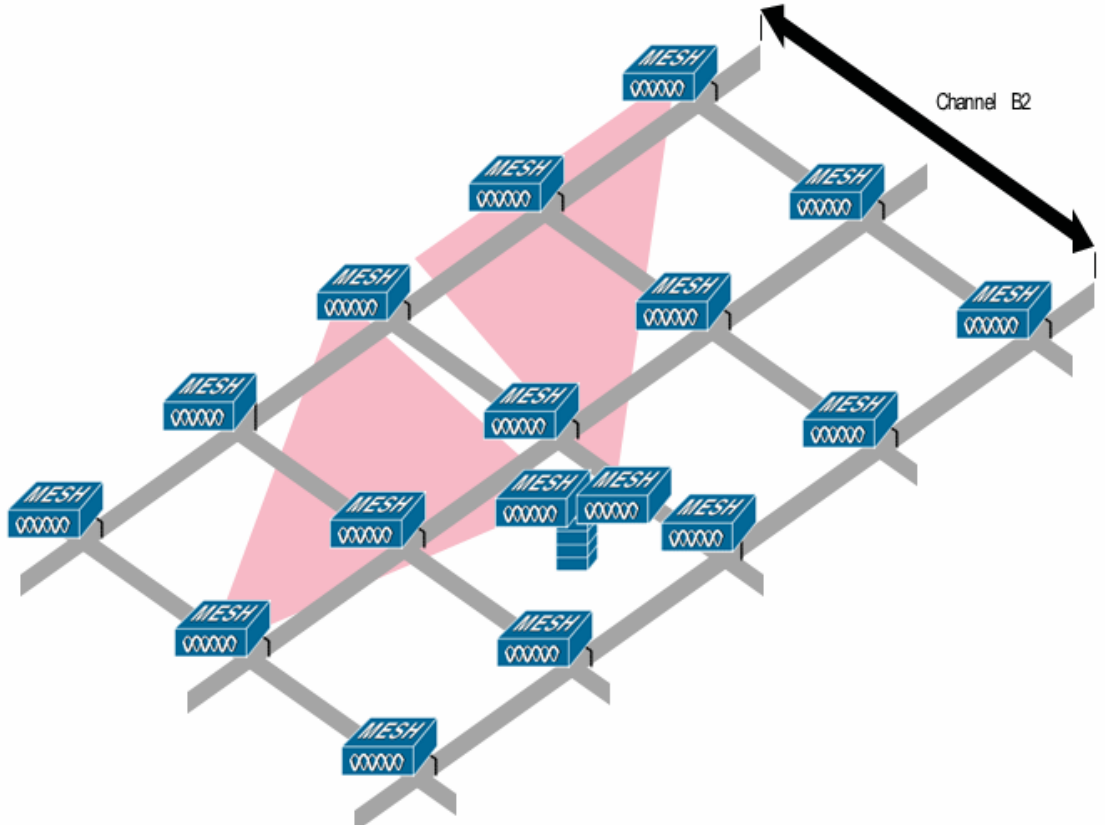
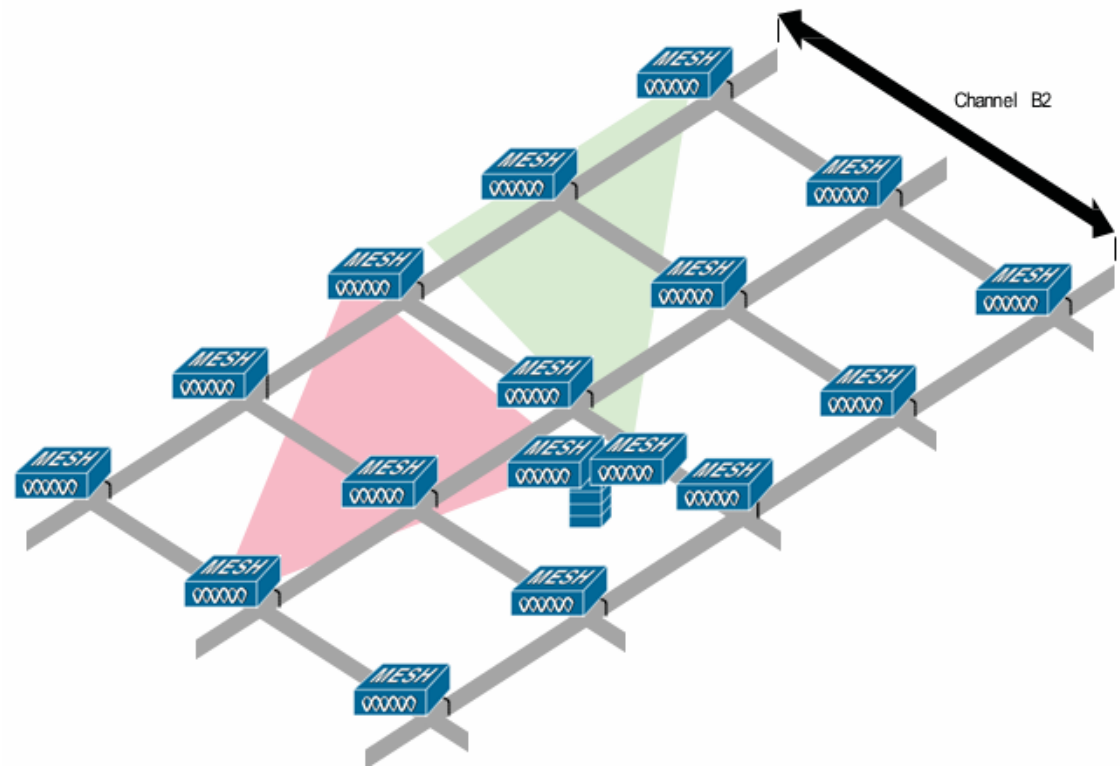


図 8-9　別のチャネルでセルごとに 2 つの RAP



複数の RAP

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

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

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

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

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

屋内メッシュと屋外メッシュの相互運用性

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

注意　サードパーティの屋外ラックの屋内 AP は、屋内 WLAN から駐車場のホップまでの単純かつ短距離の拡張などの、屋外での限られた配置でのみ配置できます。堅牢な環境および温度に関する仕様を備えているため、屋外ラックでは 1240、1250、1260、1700、2600、2700、3500e、3600、および 3700 AP を推奨します。さらに、AP が屋外ラック内にある場合、屋内 AP には、連結されたアンテナをサポートするためのコネクタがあります。SNR 値は増減しない場合もあるので、注意してください。また、より最適化された屋外の 1500 シリーズ AP と比較した場合、長期間のフェードにより、これらの AP のリンクが消失する場合があります。

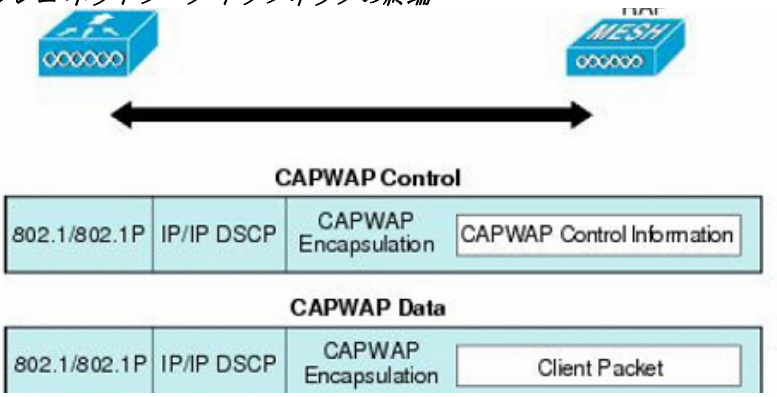
モビリティ グループは、屋外メッシュ ネットワークと屋内 WLAN ネットワークの間で共有できます。1 台のコントローラで、屋内と屋外のメッシュ AP を同時に制御することもできます。同じ WLAN が屋内と屋外の両方のメッシュ AP からブロードキャストされます。

Cisco 1500 シリーズ メッシュ AP のネットワークへの接続

ここでは、ネットワークに Cisco 1500 シリーズ メッシュ AP を接続する方法について説明します。

ワイヤレス メッシュは、有線ネットワークの 2 地点で終端します。1 つ目は、RAP が有線ネットワークに接続されているロケーションで、そこではすべてのブリッジ トラフィックが有線ネットワークに接続しています。2 つ目は、CAPWAP コントローラが有線ネットワークに接続するロケーションです。そのロケーションでは、メッシュ ネットワークからの WLAN クライアント トラフィックが有線ネットワークに接続しています（図 8-10 を参照）。CAPWAP からの WLAN クライアント トラフィックはレイヤ 2 でトンネルされ、WLAN のマッチングは、コントローラがコロケーションされている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、コントローラが接続されているネットワークのセキュリティ機能によって異なります。

図 8-10　メッシュ ネットワーク トラフィックの終端



(注)　HSRP 設定がメッシュ ネットワークで動作中の場合は、入出力マルチキャスト モードを設定することを推奨します。マルチキャスト設定の詳細については、『Cisco Mesh Access Points, Design and Deployment Guide』を参照してください。

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 RF 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。

主要な VoWLAN ソリューションであるソフトフォン アプリケーションは、多数のハードウェアおよびオペレーティング システム プラットフォームで使用できます。Cisco JabberTM アプリケーションにより、プレゼンスやインスタント メッセージ（IM）、音声、ビデオ、ボイス メッセージ、デスクトップ共有、および会議にアクセスできるようになります。スマートフォン、タブレット、ラップトップ用の Jabber ダウンロード、および Jabber の各バージョンの設計ガイドについては、『Cisco Jabber』を参照してください。

アンテナに関する考慮事項

VoWLAN のネットワーク要件は厳しさを増し、アンテナの選択など、WLAN の計画全般にわたって影響を及ぼしています。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）のアンテナの選択
- 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

シスコは、VoWLAN アプリケーション用に天井マウント アンテナを推奨します。天井マウント アンテナとアンテナ内蔵 AP は、すばやく簡単に設置できます。さらに重要な点は、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、信号の伝達と受信を最も効率的に行うことができます。アンテナを内蔵した Cisco AP は設置方法が最も簡単なうえ、内蔵アンテナにより、大半の設置に適した下り信号の伝達パターンを提供します。内蔵アンテナ ソリューションは、特に企業環境のオープン スペースへの設置に適しています。

シスコでは、さまざまな多入力、多出力（MIMO）デュアル バンド、デュアル放射素子全方向性アンテナおよび指向性（パッチ スタイル）アンテナを提供しています。これらの複数の素子アンテナは、最大比合成（MRC）などの IEEE 802.11n および 11ac テクノロジーや、ClientLink といったシスコ独自のパフォーマンス機能を有効活用するように設計されています。これらのテクノロジーは、（AP の複数のアンテナでキャプチャされた）クライアントの電話パケットを、より強力な単一の信号として結合します。結合された信号では、伝送される電話パケットと、一般的な 2.4 GHz または 5 GHz 帯域のノイズの間との、信号対雑音比（SNR）が向上します。MRC の重要な機能は、アップストリーム パケットのエラー レートを低減することです。Cisco AP では、複数のアンテナと 802.11 ClientLink ロジックを使用して、クライアント電話に高エネルギー パケットを配信することで、ダウンストリーム パケットのエラー レートを減らしています。これらの 2 つの機能により、個々の VoWLAN コールの平均オピニオン評点（MOS）値、および AP の Wi-Fi チャネルの全体的な容量が向上します。

シスコでは、すべてのアンテナを、金属などの高反射面から 1 ～ 2 波長離れた場所に配置することを推奨します。2.4 GHz の波長は 4.92 インチ（12.5 cm）で、5 GHz の波長は 2.36 インチ（6 cm）です。アンテナと反射面とを 1 波長以上離すことで、AP 無線での送信波の受信感度が向上し、無線送信時の null の生成を減らすことができます。802.11g/n および 802.11a/n/ac 仕様に採用されている直交周波数分割多重方式（OFDM）により、反射、null、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 エリアに反射して戻ってくる信号の緩衝材となります。

MRC の詳細については、IEEE レポートをお読みください。

ClientLink の詳細については、以下を参照してください。

- Cisco Wireless ClientLink 3.0 テクノロジー
- Cisco Aironet 3700 シリーズ ホワイト ペーパー

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、単体ですべての用途と場所に適したタイプはありません。各種アンテナの性能と製品番号の詳細については、『Cisco Aironet Antennas and Accessories Reference Guide』を参照してください。

シスコでは、同一の外部アンテナ ポートからデュアル バンド（2.4 GHz および 5 GHz）をサポートする AP にダイポール アンテナを接続する場合、Cisco Aironet ダイポール デュアル バンド AIR-ANT2524D シリーズのアンテナを使用することを推奨します。

Aironet ダイポール デュアル バンド アンテナには、次のような利点があります。

- 2.4 GHz および 5 GHz のデュアル バンドの同時送受信（デュアル バンド全方向性およびパッチ アンテナと同じ）をサポートします。Aironet ダイポール デュアル バンド アンテナのゲインは、2.4 GHz 帯域で 2.2 dBi、5 GHz 帯域で 4 dBi です。
- 小型であり、黒やグレー、白などの無彩色で提供されます。
- 連結式の回転する台座が付属します。

アンテナの方向

シスコでは、**複数のアンテナを持つ AP の場合、すべてのアンテナを同じ方向に向ける**ことを推奨します。

（注）　図 9-1 で示すように、多くのマーケティング素材では AP のアンテナがさまざまな方向に向けられた様子が示されていますが、シスコではこの慣例はお勧めしません。

図 9-1　アンテナがさまざまな方向に（誤って）向けられた AP

MRC と ClientLink の最適なパフォーマンスは、図 9-2 で示すように、AP のすべてのアンテナが同じ向きに配置されている場合に得られます。

図 9-2　アンテナが同じ方向に（正しく）向けられた AP

AP の 4 本すべてのアンテナを均一な直立ポジションにすることで、単一の空間ストリームによる 802.11n スマートフォンを使用する場合、カバレッジ セルの総合スループットが 2 Mbps 増加します。

一般的な推奨事項

Wi-Fi カバレッジ セルの帯域幅、およびクライアント アプリケーションのパフォーマンスを最適化するため（あらゆる形式のダイポール アンテナ タイプの場合）、シスコでは次のことを推奨します。

- AP の各アンテナ ポートにアンテナを取り付ける。
- 各ポートに同じモデルのアンテナを取り付ける。
- 各アンテナを同じ向きにする。

AP、および AP で実行されるプロトコルは、MRC および ClientLink を中心として設計されています。上記の推奨事項に従ったアンテナ システムを使用することで、このテクノロジー、および AP ハードウェアへの投資を最大限に活用できます。

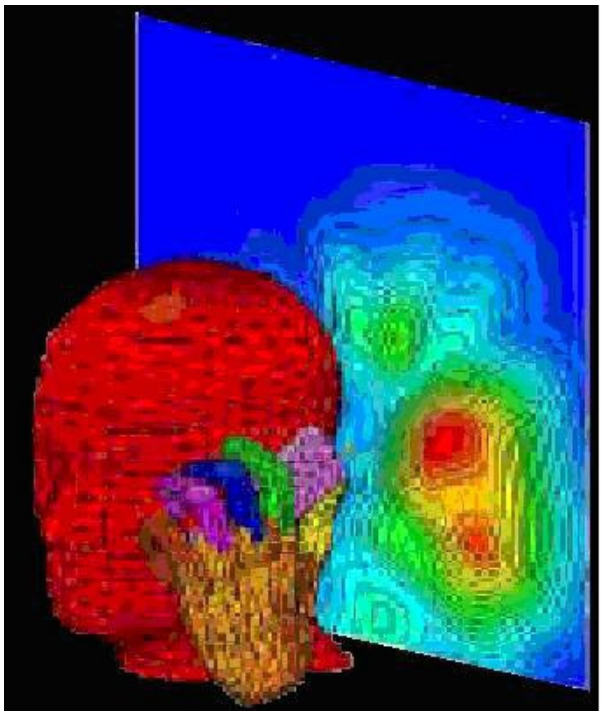
ゲインの高いアンテナは、信号を水平面に広く拡散させる可能性があり、これにより、多くのノイズを拾う大規模なセルが作成されます。この結果、信号対雑音比（SNR）が低くなり、パケット エラーの比率が高まります。SNR は、次の条件によって定義されます。

- 信号：ある無線から送信され、中断されずに別の無線によって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 パケットと背景雑音の間のエネルギーの差が大きいほど、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 エリアの設計では、複数のチャネルを使用して、高い音声通話容量を維持しつつ、パケット エラー レートを最低限に抑えます。

ゲインの高いアンテナを使用すると、カバレッジ エリアが増えるため、Wi-Fi チャネル上のコール数も減少します。音声の場合、人間の頭と体によって 5 dB の信号が減衰するため、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 9-3 を参照）。天井マウント アンテナは、人間の頭と体による減衰を防ぐように、多くの壁面マウント アンテナより適切に配置できます。

図 9-3　　頭と体による減衰



アンテナの配置

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、推奨されるカバレッジ 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相反的なものであることを理解しておくことが大切です。ゲインは受信と送信の両方で平等に適用されます。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。懐中電灯の反射器によって、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 計画の詳細については、第 3 章「WLAN RF 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

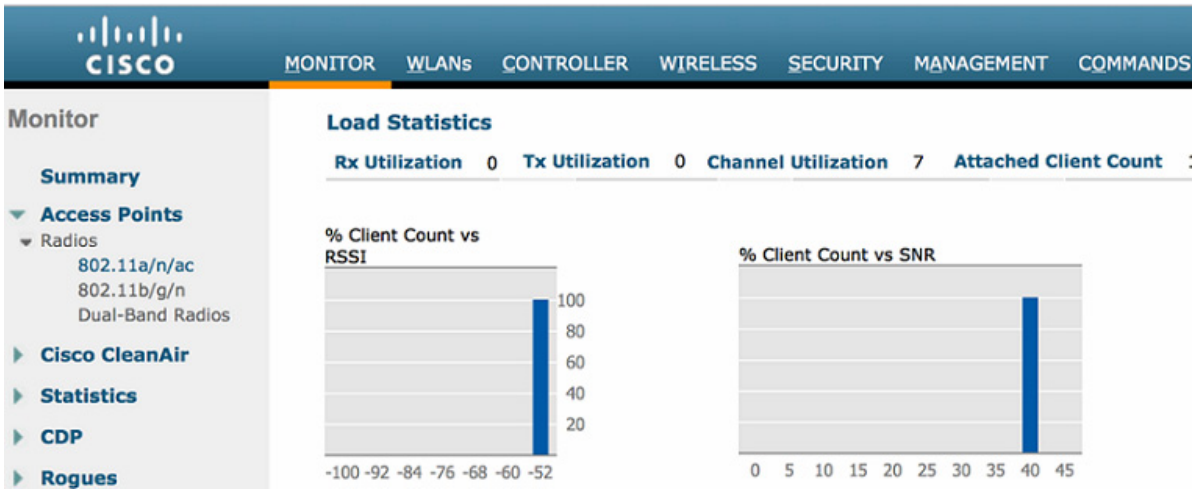
電話本体にアンテナが内蔵されている電話機については、ユーザの電話の持ち方によって 4 dB の信号減衰が起こることがあります。手でアンテナを覆って頭で電話を支えた場合には、9 dB の信号減衰が起こることがあります。一般的に、屋内での展開の場合は、信号が 9 dB 減衰するごとにカバレッジ エリアは半減します。図 9-3 では、頭で支えた場合のハンドセットからの放射電力の違いの例を示しています。

一般的なスマートフォンおよびタブレット コンピュータの Wi-Fi アンテナ システムの dB ゲインはマイナスです。一般的なスマートフォンのアンテナでは -3 または -4 dBi です。一般的なラップトップのゲインは 0～2 dBi のプラスです。アンテナ ゲインの違いは、同じ AP でのスマートフォン、タブレット、およびラップトップ間のカバレッジ エリアの違いに反映されます。スマートフォンやタブレットで最高のアプリケーション パフォーマンスを実現するには、スマートフォンやタブレット自体の Wi-Fi 機能に合った AP チャネル カバレッジを設計する必要があります。スマートフォン、タブレット、ラップトップと AP との間で最適なリンク品質を実現するためには、ClientLink が有効な状態で AP が動作する必要があります。ClientLink は、Cisco ワイヤレス LAN コントローラ（WLC）によってデフォルトで有効になっています。

チャネルの使用率

802.11、802.11b、802.11n-2.4 GHz、および 802.11n のプロトコル仕様では、同じ 2.4 GHz 帯域が使用されるため、これらのプロトコルの間に相互運用性があります。この相互運用性によって、802.11 保護プロトコルのロジック オーバーヘッドが増加し、チャネルの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 帯域の Wi-Fi 周波数を使用している製品がありますが、同じ周波数を使用するデバイスは他にも多数あります。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 帯域が混雑していることやチャネル割り当ての制約から、シスコでは、新たに VoWLAN を展開するときには 5 GHz Wi-Fi 帯域を使用することを推奨します。5 GHz で使用可能なチャネルは通常、ほとんどのサイトではそれほど多用されていません（図 9-4 を参照）。VoWLAN トラフィックに 5 GHz の UNII-2 チャネルを使用する場合、レーダーが存在してはならないことが重要となります。したがって、すべての新規サイトでは、特定の UNII-2 チャネルを設定でブロックすべきかどうかを判断するための追加テストを実施することを推奨します。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、レーダー信号が存在しなくなるまで、AP はこのチャネルを離れなければならないためです。

図 9-4　　2.4 GHz のチャネル使用率レポート



Cisco Unified Wireless Network をインストールする前に、AirMagnet、Wild Packets、Cognio などのツールを使用して、チャネルの干渉および使用率をテストできます。設計プロセスを支援するために、Cisco Prime Infrastructure によって生成される AP オンデマンド統計表示レポートは、次のようなスペクトル概要を提供します。

- 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
- チャネル使用率

ALOHAnet プロトコルでは、チャネル使用率が 33 % に到達すると、この無線チャネルを満杯と定義します。これは、チャネルがビジー状態であるため、パケットが送信できるようになるまでオープンなタイム スロットを待機する必要があることを意味します。図 9-4 で示したとおり、チャネル使用率が 46 % になると、チャネル使用率に関する、無線パケット化された ALOHA 標準を超えてしまいます。

2.4 GHz 帯域のチャネル使用率を減らすため、レガシー デバイスがクライアント構成に含まれていない場合は、クライアントを 5 GHz に移動して、レガシーである 1 Mbps および 2 Mbps のデータ レートを 2.4 GHz の構成から削除することを推奨します。

動的周波数選択（DFS）および AP の 802.11h 要件

米国の連邦通信委員会（FCC）、欧州電気通信標準化機構（ETSI）、およびその他の監督機関は、無線周波数の使用に関するそれぞれの要件を定めています。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 Wi-Fi 周波数と 5 GHz UNII-2 帯域を重複して使用するシステムも存在します。2006 年に FCC は 5.470 ～ 5.725 MHz 帯域範囲をライセンス不要の用途に開放しました。これらの周波数が新たに使用可能になったことで、*干渉のない* AP の設定を管理することが必要になりました。AP では、（通常、軍事、衛星、気象観測所から来る）レーダー パルスを定期的に監視し、レーダーが探知された場合は動的周波数選択（DFS）を使用して、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、この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

UNII-2 帯域のレーダー回避要件によって音声通話の品質に影響が及ぶ場合があるため、音声アプリケーションを稼働させる前に、レーダーのテストを実施することが求められています。Cisco Spectrum Expert は、特定のチャネルでレーダーの存在をテストするための優れたツールです。Spectrum Expert によるテスト中にレーダーが探知された場合は、該当するチャネルをブロックするように AP を設定できます。

5 GHz 帯域のチャネル

DFS 要件には、従来の 4 つの UNII-2 チャネル（52 ～ 64）と、8 つの新しいチャネル（100 ～ 116 と 132 ～ 140）が含まれます。5 GHz 帯域には現在 20 のチャネルがあります。これらのチャネルは重複しないため、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 エリアに共存配置チャネルを許容する設計により、カバレッジ エリアで取得可能なコール数が集約されます。

（注）　現在の法規制に関する情報については、シスコの Web サイトをご覧ください。また、自国で許可されている周波数については、各国の法的機関にお問い合わせください。

チャネルベースの設計は、図 9-5 に示すように、単一フロアに水平に実装できます。

図 9-5　単一フロアのチャネル設計

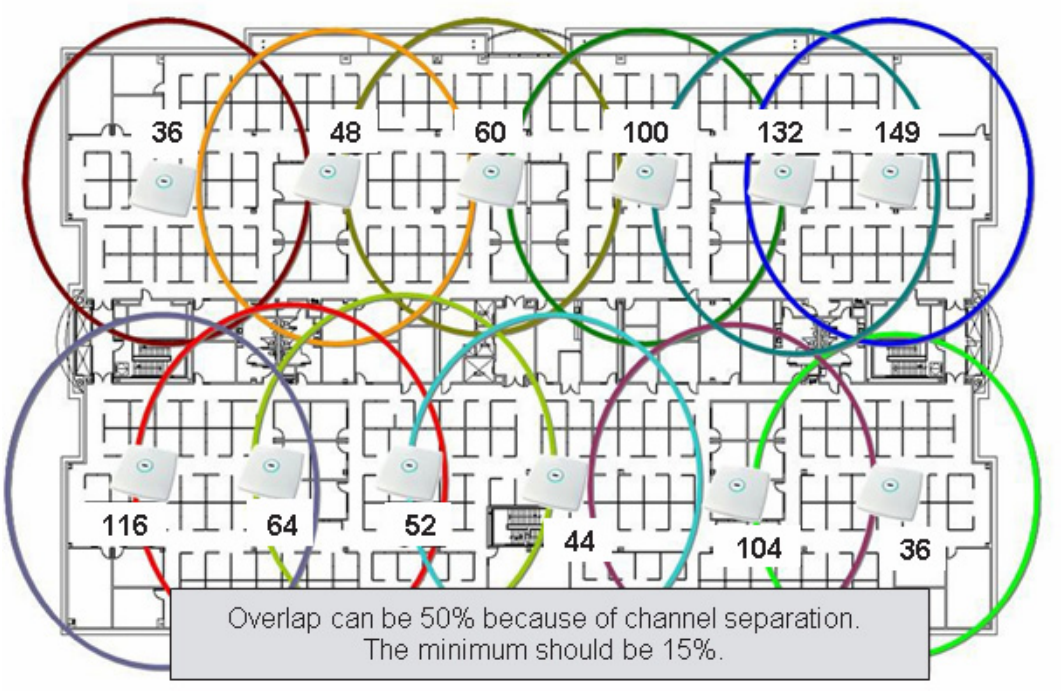
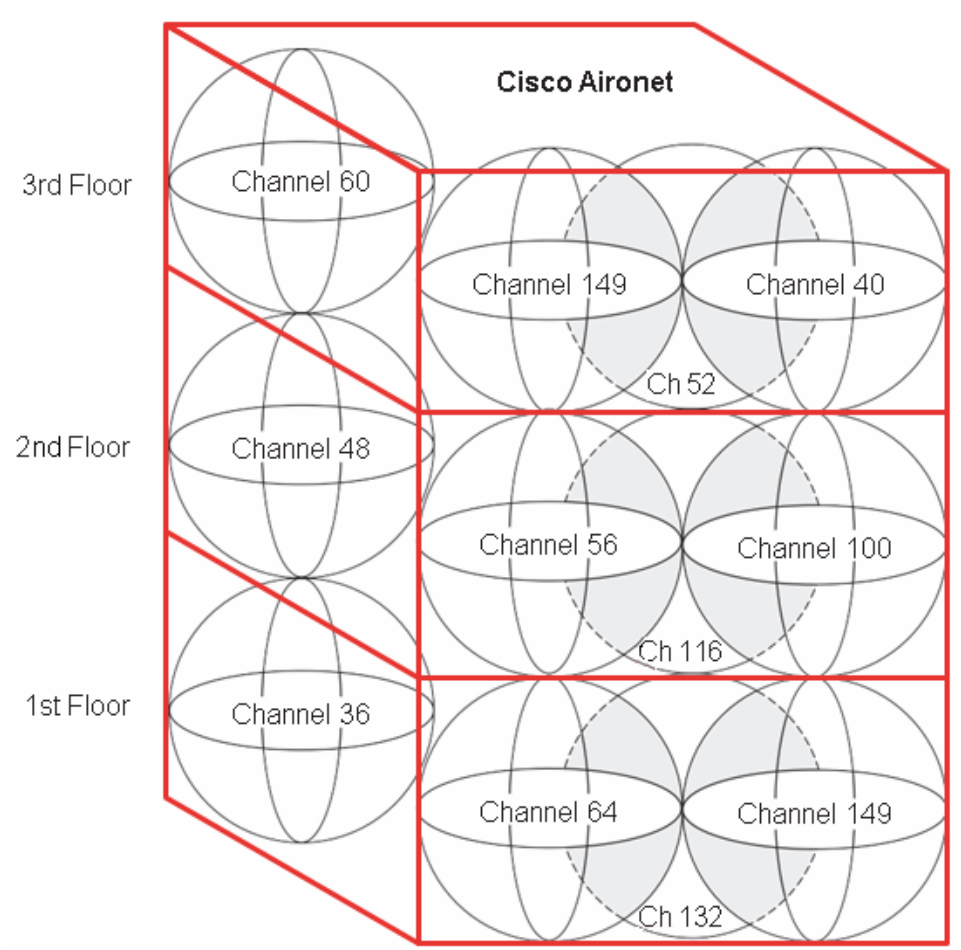


図 9-6 で示すとおり、複数フロア設計では、フロア間で垂直にチャネルを分離して、同一チャネル干渉を減少させることができます。

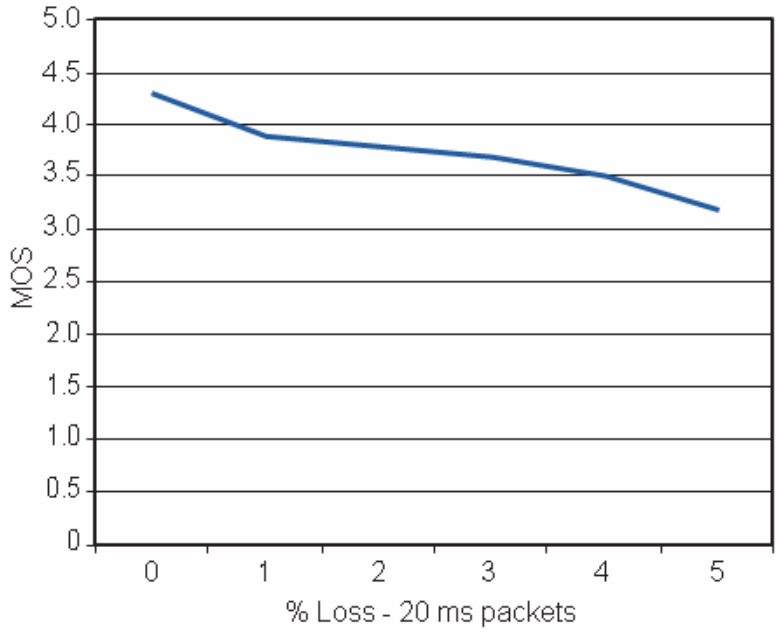
図 9-6　　垂直チャネル分離



コール キャパシティ

Wi-Fi チャネルのコール数は、さまざまな要因によって制限されます。まず、シールド付きツイストペア CAT 5 ケーブルとは異なり、AP および VoWLAN クライアントによって使用される RF スペクトルは、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。802.11 のオープンな共有 RF スペクトルは、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ーが発生します。図 9-7 では、パケット損失の関係を平均オピニオン評点（MOS）として示しています。

図 9-7　実際のパケット損失の図



802.11ac および 802.11n-2.4 G 仕様では、最高のカバレッジ エリアは最低のデータ レート（6 Mbps）で得られます。どのような電力レベルの場合でも、最も低いパケット エラーは 6 Mbps です。

許容可能な音声のカバレッジ エリアは、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：最も高い 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 9-7 は、5 % のパケット エラー レートによって MOS が低下し、通話の質が*一部のユーザにとって満足*できるレベルになった例を示しています。

電話のカバレッジ エリアのエッジは、そのカバレッジ エリアの MOS 評価が*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。本書では、こうしたカバレッジ エリアのエッジを*セル エッジ*と呼びます。複数の電話クライアントやデータ クライアント同士の干渉や同一チャネル干渉、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 エッジが必要です。セル エッジおよびカバレッジの設計については、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 MHz のデータ レートを無効にすることを推奨します。

これらのレートを無効にする場合は、1 つ以上の 802.11n-2.4 GHz データ レートを*必須*に設定する必要があります。シスコでは、6 MHz のデータ レートを必須に設定することを推奨しますが、これはセル サイズ設計要件によって異なり、場合によっては高ビット レートを使用する必要があります。可能な場合は、802.11b/g の混在ネットワークではなく 802.11n-2.4 GH のみのネットワークを構築することを推奨します。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。また、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。一般的に、ユニキャスト パケットは、AP とクライアントの間のリンクに対して最も信頼性の高いレートを提供できるデータ レートで送信されます。Cisco AP は、ClientLink 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。受信無線は、AP 無線または電話無線のいずれかです。多くの場合、SNR はリンクの両方の無線で同じではありません。AP、およびセル エッジで SNR とマルチパス干渉を考慮する必要があります。パス損失は、リンクの両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 エッジを設定することを推奨します。Wi-Fi アプリケーションにおいて AP と電話の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 Real-time Transport Protocol (RTP) G.711 パケットです。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型です。通話の信号強度、SNR、データ レート、およびエラー レートは、Autonomous AP またはコントローラベースの CAPWAP AP 上の AP 統計から確認できます。

シスコでは、アクティブ コールでカバレッジ テストを行うことを推奨します。双方向コールにより、ClientLink のダウンストリーム (AP からクライアントへ) のパケット サイズおよび、ユニキャスト パケットのタイプが決定されます。アップストリーム (クライアントから AP) では、AP 上で処理を行う MRC のパケット サイズおよびユニキャスト パケットのタイプが決まります。クライアントのセル エッジの範囲をテストする場合、シスコでは同じ場所から同じ AP に対してスマートフォン、タブレット、ラップトップ モデルの組み合わせをテストすること、またすべてのクライアントに同じ面積を使用することを推奨します。これは、すべての電話で同じスペースを共有できないために、電話機が同時にテストされないことを意味します。

図 9-8 では、2.4 GHz および 5 GHz の電話での、クライアント セル エッジの dBm 値の例を示します。

図 9-8　クライアント エッジの RSSI が -67 dBm で SNR が 59 dB の場合

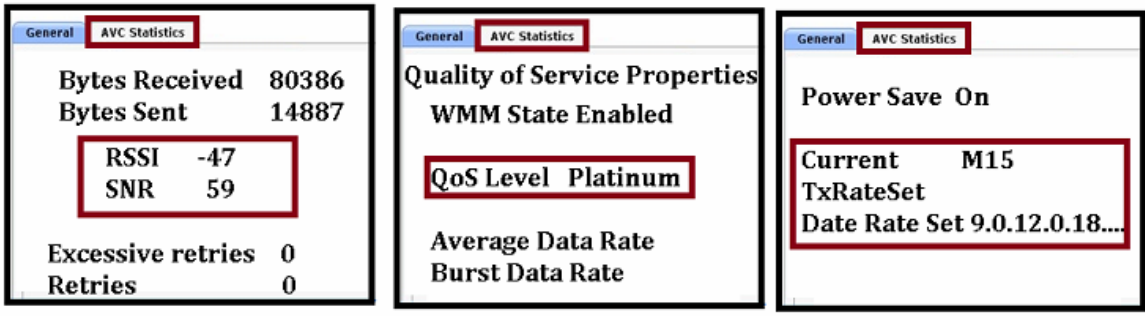
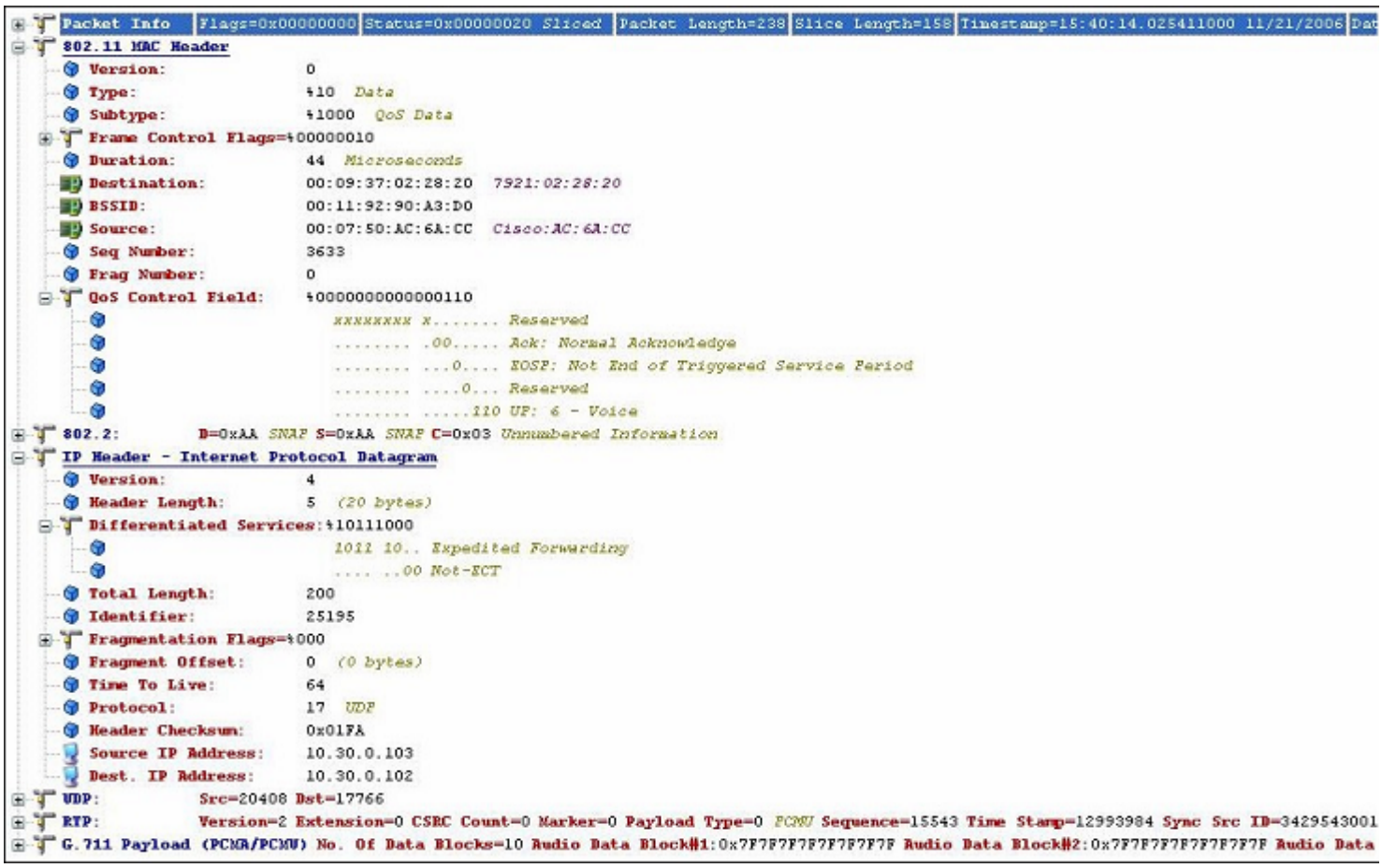


図 9-9 では、デコードされたオーディオ G.711 RTP パケットを示します。Cisco 7960 卓上電話から発信されたこのパケットは、AP から VoWLAN のエンドポイントへのダウンストリームです。Over-the-Air QoS マーキングは、802.11e 仕様に従い、QoS ベースライン マーキング 5 からユーザ プライオリティ 6 に変更されます。Cisco 電話のコール統計は、電話機上で見ることができます。また、電話機の IP アドレスを使用して、電話機内を参照しても見ることができます。セル エッジの dBm 値はその後、より調査に適したツールのベンチマーク値として使用できます。自動調査ツールにより、サイトのカバレッジ設計を効率化できます。

図 9-9　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。パケットの信号レベルは、前のパケットより 5 dB 程度上下する可能性があります。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

VoWLAN 展開の計画プロセスの鍵となる部分が、AP ごとの同時オーディオ ストリーム数の計画です。

(注)　同じ AP に関連付けられている 2 つの電話間のコールは、2 つのアクティブなオーディオ ストリームとみなされます。

AP のオーディオ 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。

- 免許不要の（共有）802.11 チャネルの使用率によって、AP が伝送できる同時オーディオ ストリーム数が実際に確定されます。
- チャネルの使用率と AP のパフォーマンスによってオーディオ 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 が同じ場所にあり、同じチャネルで動作していても、オーディオ ストリーム数は 2 倍にはなりません。実際、AP が 1 つの場合よりもオーディオ ストリームが少なくなることがあります。
- 同時に実行可能なオーディオ ストリーム数を決定するのは、セル キャパシティまたは帯域幅です。
- ハンドセットおよび VoWLAN 展開でサポートされている 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種類があり、それぞれ多様な WLAN QoS 機能を備えています。これらは WLAN 展開で有効化されている各機能に影響を与え、最終的には AP ごとの音声通話の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 あたりのコール数についての指針が示されています。ただし、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オーディオ ストリーム数は、環境要因やクライアントでの Wi-Fi Multimedia（WMM）仕様の遵守など、多数の問題に大きく依存します。

表 9-1 は、Cisco Compatible Extensions がどのように VoWLAN コールの質の向上に役立つかを示します。

表 9-1　Cisco Compatible Extensions による VoWLAN の質の向上

Cisco Compatible Extensions によって生じる VoWLAN の質に関する利点	
機能	**利点**
EAP タイプの CCKM サポート	クレデンシャルがローカルにキャッシュされるため、高速なローミングが可能
不定期自動省電力配信（U-APSD）	チャネル キャパシティおよびバッテリ寿命の拡張
TSPEC ベースのコール アドミッション制御（CAC）	ローミングおよび緊急通話に対するコール キャパシティの管理
音声メトリック	より適切な、より多くの情報に基づくトラブルシューティング
ネイバー リスト	クライアント チャネルのスキャンを低減
ロード バランシング	AP 間でのコール分散
ダイナミック伝送パワー コントロール（DTPC）	クライアントが伝送時の電力を学習
経由ローミング	高速なレイヤ 2 ローミング

表 9-1 から、次のことがわかります。

- Cisco Centralized Key Management（CCKM）は Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）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、これによって音声通話の質が向上します。
- コール アドミッション制御（CAC）によって音声通話の質が向上し、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。
- 経由ローミングおよびネイバー リストによって、音声通話の質が向上し、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。
- 不定期自動省電力配信（U-APSD）およびダイナミック伝送パワー コントロール（DTPC）によってバッテリの寿命が延びます。
- ロード バランシングおよび DTPC によって音声通話の質が向上します。

Cisco Compatible Extensions プログラムでは、Cisco Aironet 無線インフラストラクチャ製品、およびサードパーティ製ワイヤレス クライアント デバイスをサードパーティによって検証します。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決める主要な要因です。QoS 機能により、チャネル内の音声およびデータ トラフィックの優先順位付けが行われます。QoS の詳細な説明については、第 5 章「Cisco Unified Wireless QoS、AVC および ATF」を参照してください。

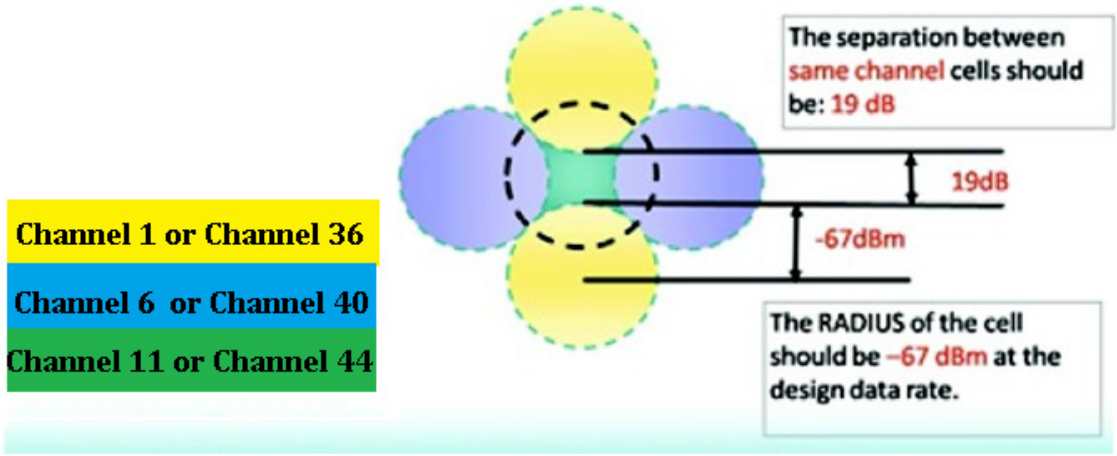
802.11e、WMM、および Cisco Compatible Extensions 仕様では、負荷を分散して、セルがオーディオ ストリームで過負荷にならないようにすることができます。CAC は、通話を開始するために十分なチャネル キャパシティがあるかどうかを判断します。ない場合、電話は別のチャネルをスキャンします。U-ASPD の主な利点は、WLAN クライアントの電力を節約することです。これには、WLAN クライアントからのフレーム送信時に、AP にバッファされているクライアント データ フレームが転送されるようにし、電力節減を実現します。ネイバー リスト オプションでは、近隣 AP のチャネル番号とチャネル キャパシティを示すリストが電話に提供されます。これによって音声通話の質が向上し、高速ローミングが実現し、バッテリの寿命が延びます。

セル エッジの設計

802.11b/g/a VoWLAN ハンドセットに関するシスコのガイドラインでは、セルの境界線の最小電力を -67 dBm にする設計が推奨されています（図 9-10 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。-67 dBm のしきい値は、パケット エラーを 1 % にするために一般的に推奨される値ですが、そのためには SNR 値を 25 dB 以上にする必要があります（この要件には、ローカルな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 エリアを決定する場合は、AP によって提供されるクライアント統計を使用して、電話で計測される信号強度とノイズの両方を検証する必要があります。Autonomous AP および CAPWAP AP 上でのこれらの値の決定については、表 9-1 を参照してください。

-67 dBm 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、同じ一般的な測定ルールを 802.11g/n および 802.11a/n/ac 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 9-10　　セル エッジの測定



(注)　図 9-10 で示した -86 dBm の分離は、簡略化されたものであり、理想的と考えられます。ほとんどの配置においては、このような 19 dBm の分離を実現することができません。最も重要な RF 設計基準は、-67 dBm のセル半径と、セル間の 20 % の推奨オーバーラップです。これらの制約を遵守して設計することによって、チャネルの分離が最適化されます。

5 GHz セルの場合、重複しない利用可能なチャネル数から考えて、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。802.11ac の 5 GHz 帯域にはチャンネルが 20（日本の場合は 19）あるため、ほとんどの場合に 2 チャネル分離が可能です。対照的に、2.4 GHz 帯域では、周波数がオーバーラップしないチャネルは 3 つしかありません。

5 GHz および 2.4 GHz 帯域の両方で、セル エッジを、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 レートが 1 % に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。空間ストリーム クライアントが 1 つの 2.4 GHz 帯域では、802.11n のデータ レートは 72 Mbps です。

チャネル幅が 40 MHz で空間ストリーム クライアントが 1 つの 5 GHz 帯域では、802.11n クライアントのデータ レートは 150 Mbps です。Jabber などのソフトフォン アプリケーションを実行するラップトップでは、3 つの空間ストリームをサポートできます。また、チャネル幅 40 MHz の 5 GHz 帯域で 450 Mbps のデータ レートをサポートできます。802.11ac クライアントおよびチャネル幅が 20 MHz で 1 つの空間ストリームをサポートしている 802.11n クライアントは、80 MHz 幅のチャネル上で 802.11ac の 3 つの空間ストリーム クライアントと、チャネル幅が 40 MHz の Wi-Fi チャネル アクセスを共有できます。

このような、クライアントの混在とプロトコルの混在は、802.11 仕様の一部です。このような、同じ Wi-Fi 周波数にクライアントが混在する場合の互換性は、802.11n および 802.11ac 仕様の一部です。

設計上の主な疑問として、帯域幅とコール キャパシティのカバレッジ エリアをどのように定義するかというものがあります。音声コール キャパシティは、802.11n-2.4 GHz と 802.11ac の場合と同様に、802.11n と 802.11ac でほぼ同じです。これは、AES 暗号化が 300 バイト未満である音声の G.711 または G.722 フレームのパケット サイズによるものです。このような小さなパケット サイズ、および 802.11 仕様の ACK ロジックにより、大型のストリーミング アプリケーションと比較して大きなオーバーヘッドが生成されます。ビデオ通話からは、小さな音声パケットと大きなビデオ パケットの両方が生成されます。ビデオ パケットは圧縮率が大きいため、音声に比べて間隔が空きます。シスコではガイドラインとして、カバレッジのセル エッジを確立することを推奨します。AP 上の電話の RSSI 値が -67 dBm の場合の、AP からの距離を測定します。

802.11n-2.4 GHz and 802.11ac の電話クライアントは、最大 54 Mbps のレートに対応できます。最新のチップ セットは多数のレートをサポートしていますが、送信電力機能が異なります。シスコでは、電話クライアントと AP の間のすべてのリンクを、適合する送信電力レベルで確立することを強く推奨します（送信電力の動的コントロールを参照）。

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。高密度展開や、狭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、802.11ac が推奨されます。802.11ac 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 Mbps 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 エッジは、次の手順で決定します。

- 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設置します。
- アクティブなコールを使用して、または G711 コーデックと同じサイズのパケットを送受信する間に、-67 dBm セル エッジへの信号レベルを測定します。

特定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。詳細については、『Data Sheets for Cisco Unified Wireless IP Phones』を参照してください。

2.4 GHz 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。5 GHz の最大送信電力レベルは、モデルによって異なります。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 9-11 では、チャネルごとの 5 GHz の最大送信電力の例を dBm 単位で示します。

図 9-11　チャネルの電力の割り当て

5 GHz 帯域での最大許容送信電力は、6 dB ほども変動します。これは、すべてのチャネルが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ることも意味しています。ただし、動的なチャネル選択は調整可能です。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した送信電力が 13 dBm の場合、すべての AP の最大送信電力を 13 dBm とす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。一般的に、AP は電話よりも受信感度およびダイバーシティが優れているため、若干低い強度の電話信号でも受信できるはずです。同じ送信電力の詳細は、「送信電力の動的コントロール」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 RF 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しました。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従来のデュアル モード AP の場合、2.4 GHz チャネルの送信電力は 5 GHz チャネルと同じ（通常はそれ以下）である必要があります。ほとんどのサイトで、SNR 式の 5 GHz のノイズ レベルは最大で 10 dB 低くなります。一般に、802.11n 無線の受信感度は、802.11ac 無線での同じデータ レートと比較した場合、1 dBm 優れています。たとえば、Cisco 8821 電話機のデータ シートでは、データ レート 36 Mbps での受信感度は、802.11n の場合は -84 dBm で、802.11ac の場合は -83 dBm となっています。したがって、ノイズ フロアの予想値を 10 dB 下げると、802.11ac セルの感度は 8 dBm 向上します。802.11n-2.4 GHz と 802.11ac のパス損失の違いなどのその他の詳細も影響するため、実際の受信感度は必ずしもこれに一致しません。ただし、同じカバレッジ セルを希望する場合は、802.11n-2.4 GHz ネットワークの電力レベルを 802.11ac 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。第 3 章では、AP2800/3800 モデルに同梱されている新しい Flexible Radio ハードウェアについても説明しています。このハードウェアと RRM FRA アルゴリズムにより、2.4 GHz カバレッジ バランスが大幅に改善するとともに、同一チャネル干渉が減少します。ハードウェアの柔軟な特性以外の、デュアル バンド AP と電力に関するアドバイスはどれも同じです。2.4 GHz と 5 GHz の両方の帯域で稼働している AP のみにこのハードウェアを適用することになるためです。

送信電力の動的コントロール

Cisco Aironet AP では、デフォルトでダイナミック伝送パワー コントロール（DTPC）が有効になっています。DTPC は Cisco WLC では自動化されていますが、Autonomous AP 上では設定が必要です。

DTPC の目的は、AP とクライアント Wi-Fi 無線の間の送信電力の不均衡により、片通話が生じる可能性を減らすことです。DTPC は、これを次の方法で実現します。

- 電話の送信電力を AP の送信電力と一致するように設定する
- クライアントが学習できるように、AP に送信電力をアドバタイズさせる

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 9-12 に示す例は、電話の送信電力レベルが 5 mW から 100 mW に変更されることを意味します。

図 9-12　クライアントと AP の電力の一致

802.11 のライセンス要件では、クライアントが最小送信電力を規定することは必須ではありません。また、規制で許容される最大送信電力を使用する Wi-Fi デバイスはごく小数です。一般的な Wi-Fi デバイスでは、最大送信電力は 100 mW 以下です。これは、AP とクライアントが互いにアソシエートして接続している場合、AP とクライアントの電力レベルを一致させることは Wi-Fi 仕様において必須ではないためです。アソシエーション中、互いにアソシエートされているにもかかわらず、両者が短時間だけ互いのカバレッジ エリアから外れる可能性は常にあります。アクティブなコール中にこのような事態が発生すると、音声が失われます。アクティブなコール中の互いの送信電力レベルが等しくない場合にも、音声が失われます。AP と電話の接続維持に役立つ 802.11 メカニズムはいくつかあり、そのうちの 1 つが、より低速のデータ レートをネゴシエートできる機能です。一般的に、低速データ レートのほうが、高速データ レートよりも伝送電力が高くなります。高密度の展開では、低速データ レートを避ける必要があります。これは、カバレッジ セルで高いスループットと容量が必要とされるにもかかわらず、パケット数の多い通話に低速データ レートを使用すると、この Wi-Fi チャネルおよび AP のすべてのクライアントのスループットが低下するためです。

シスコでは、AP の最大送信電力の設定が、クライアントの電話機がサポートする最大送信電力を超えないようにすることを強く推奨します。現行の Cisco AP は ClientLink をサポートするため、ClientLink を設定することを強く推奨します。ClientLink では、選択したクライアント宛ての信号を動的に作成します。ClientLink ロジックによって、転送されたパケットの信号伝播は変更されますが、ブロードキャストまたはマルチキャスト パケットの信号伝播は変更されません。ClientLink では、一般的な全方向性アンテナの、全方向で同じ信号エネルギーを持つ水平方向の信号伝播が削除されます。信号エネルギーは、選択したクライアントの方向で増加します。転送された信号は、選択されたクライアントでの信号エネルギーを増加させるため、電話機のダウンストリームの信号品質が向上します。これにより、コールの MOS 値が向上します。MOS 値が向上することによって再試行が減少し、すべてのクライアントのカバレッジ エリアのスループットが向上します。この信号はシェーピング済み信号として特定のロケーションに転送されるため、AP のその他のカバレッジ エリアでは信号が削減されます。これにより、ブロードキャストおよびマルチキャスト パケットと他の AP との間でチャネルが重複する領域で、チャネルのパフォーマンスが向上します。

シスコでは、電話機の各モデルを、そのモデルの Wi-Fi カバレッジ エリアに対してテストすることを推奨します。WLC は、電話機がアソシエートされた AP における各クライアントの受信信号強度インジケータ（RSSI）を報告します。RSSI フィールドに表示される値は、電話機から AP に送信されるパケットの信号強度です。この値は、電話機から送信されたパケットの、AP に受信された時点での信号強度を示します。電話機のカバレッジ エリアと、その電話機が AP のカバレッジのおおよその境界に配置されていることを確認することを推奨します。次に、電話機がアクティブなコール中のときの RSSI を確認します。この操作の目的は、セル エッジ（RSSI の推奨値 -67 dBm）で、そのパケットが高速データ レートで送信されることです。VoWLAN Wi-Fi カバレッジ エリアの範囲に対するセル エッジについては、図 9-10 を参照してください。図に示されている -39 という値は、クライアントの電話機またはデバイスが AP から数フィート以内にある場合に検出される、非常に強い信号です。

スマートフォンやタブレットの出現により、電話機のカバレッジのテストの重要性が増しています。これらのデバイスの Wi-Fi 機能は一般的に消費者向けのものであるため、これらのデバイスには通常、企業のサポートを想定した 802.11 機能はほとんど入っていません。ほとんどの消費者向けスマートフォンやタブレットでは、DTPC をサポートしていません。このためシスコでは、2.4 GHz および 5 GHz 帯域での最大送信電力を、お使いの最も弱いスマートフォンやタブレットの 2.4 GHz および 5 GHz 帯域での最大送信電力に合わせた dBm 値に設定することを推奨します。この WLC フィールドの値によって AP の送信電力が制限されるため、電話機から AP までの範囲のバランスを保つことができます。

802.11r および 802.11k 機能

IEEE 802.11k および 802.11r は、WLAN 環境における Basic Service Set（BSS）のシームレスな移行を可能にする主要な業界標準です。WLAN 7.2 リリースでは、シスコは 802.11r セキュア認証 Fast Transition プロトコルをサポートしています。IEEE 802.11k 仕様は、2008 年 6 月に承認されました。IEEE 802.11r 仕様は、2008 年 7 月に承認されました。802.11r 仕様は、2004 年 6 月の 802.11e セキュリティ仕様に従っています。

802.11k 仕様の簡単な説明については、こちらをお読みください。

802.11k 仕様の詳細については、こちらをお読みください。

802.11r 仕様の簡単な説明については、こちらをお読みください。

802.11k および 802.11k 対応のクライアント デバイスは、現在アソシエートされている AP に対し、近隣 AP のリスト（*ネイバー リスト*）の要求を送信します。この要求は、*アクション パケット* と呼ばれる 802.11 管理フレームの形式になります。AP は、同じ WLAN 上にある AP のネイバー リストと、それぞれの Wi-Fi チャネル番号を示すアクション パケットで応答します。

この応答のアクション パケットから、802.11k クライアントは次のローミング先の候補がどの AP であるかを知ることができます。802.11k の無線リソース管理（RRM）アルゴリズムを使用することで、スマートフォンは正確かつ迅速にローミングできるようになります。これは、オンコール ローミングが一般的に利用されるエンタープライズ環境における正常なコール品質のための要件です。

シスコでは、RRM によってネイバー リストの応答パケットで 2.4 GHz と 5 GHz 両方の AP チャネル番号を提供できるように、WLC で 802.11k を設定することを推奨します。また、VoWLAN コールだけでなく、すべてのアプリケーションとデバイスに 5 GHz 帯域の Wi-Fi チャネルを使用することを推奨します。

ネイバー リストからの情報があれば、802.11k クライアントは次のローミング先の AP を特定するために、すべての 2.4 GHz および 5 GHz チャネルをプローブする必要がなくなります。すべてのチャネルをプローブする必要がなくなれば、すべてのチャネルのチャネル利用率が減少するため、すべてのチャネルの帯域幅が増加します。また、ローミングにかかる時間が短縮され、クライアントはより適確な決定を下せるようになります。また、各チャネルの無線設定が変更されないうえ、各チャネルにプローブ要求が送信されないため、デバイスのバッテリ寿命が長くなります。これにより、デバイスでプローブ応答フレームをすべて処理する必要がなくなります。

802.11r および 802.11e 仕様は、同じ認証タイプ（EAP-FAST、LEAP、EAP-TLS、EAP-TTLS、EAP-SIM、PEAP バージョン 1 および 2）をサポートしています。このセキュリティ機能により、4 個のパケットをやり取りするだけで、802.11r 対応クライアントを AP で確実に認証できます。このパケットのうち 2 個は、AP 同士を接続するイーサネット有線接続を介して送信されます。残りの 2 個のパケットは、各 AP の Wi-Fi チャネルで送信されます。これにより、802.11r クライアントが実際にローミングする前に、ローミングしようとしている AP に対して確実に認証できるようになります。その結果、802.11r クライアントはローミング後、認証プロセスによる遅延を生じさせることなく、データ、ビデオ、および音声パケットを送受信できるようになります。802.11r パラメータが追加されることで 802.11 ヘッダーが変わるため、802.11r クライアント用の WLAN を 802.11r 対応でないクライアントと共有することはできません。つまり、802.11r 対応の WLAN によって SSID を割り当てられたすべてのクライアントに、アソシエーション パケットの 802.11r 要素に対応した Wi-Fi 無線ファームウェアが入っていなければならないことを意味します。802.11r 高速ローミングに対する制限は次のとおりです。

- Autonomous モードの AP でサポートされますが、無線ドメイン サービス（WDS）が必要です。
- ローカル認証 WLAN と中央認証 WLAN 間のローミングはサポートされません。

シスコでは 802.11r 仕様の使用を推奨します。802.11r では、WLAN に認証済みのクライアントとの間で Wi-Fi チャネルに送信されるパケット数が減少するので、ローミングにかかる時間が短縮されるためです。

ユーザにとってローカルな干渉源

干渉はユーザにとって局所的（ローカル）な事象ですが、近接ユーザにも影響する可能性があります。Bluetooth は、2.4 GHz Wi-Fi 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 9-13 は、実際の Bluetooth 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 Bluetooth ヘッドセットを使用した 802.11n-2.4 GHz 音声コールから取得したものです。図 9-14 では、Bluetooth ヘッドセットによるジッターも示しています。

図 9-13　一般的な Bluetooth イヤホンの 802.11b/g 2.4 GHz スペクトルにおける信号パターン

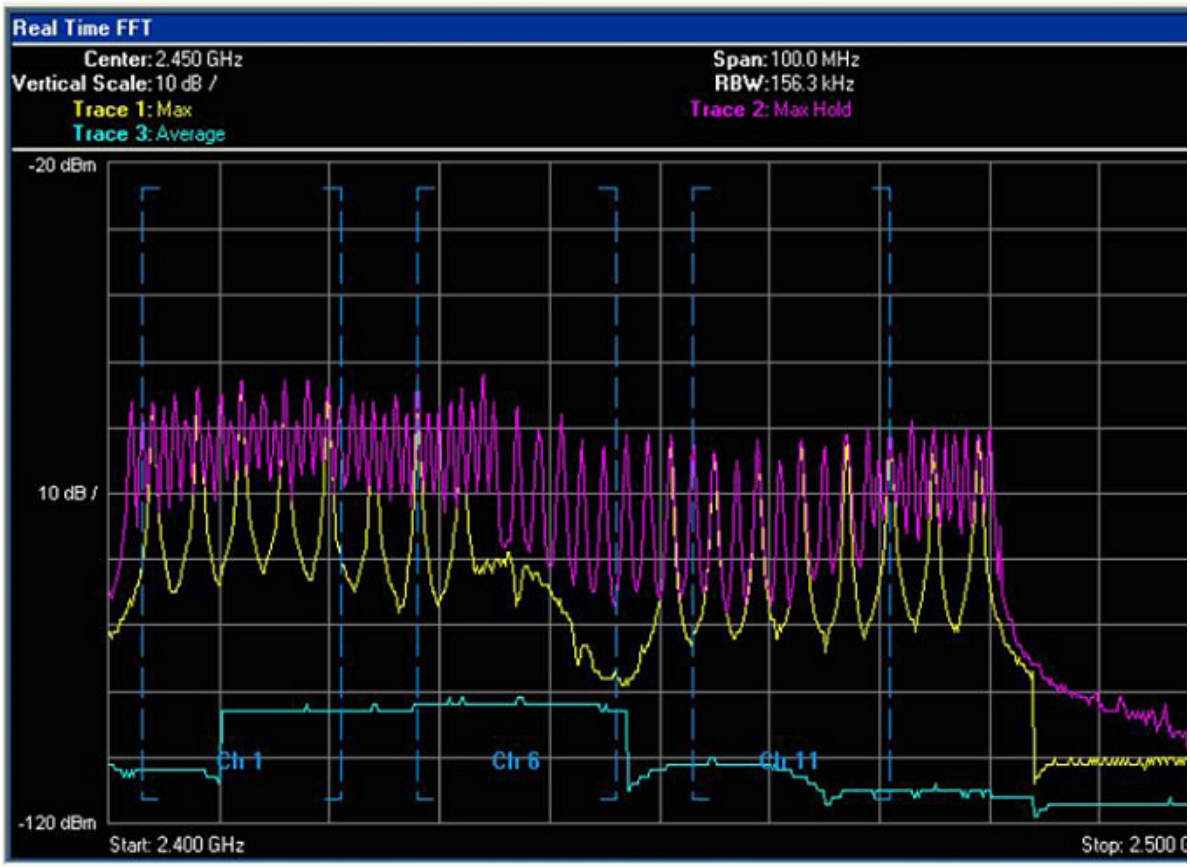
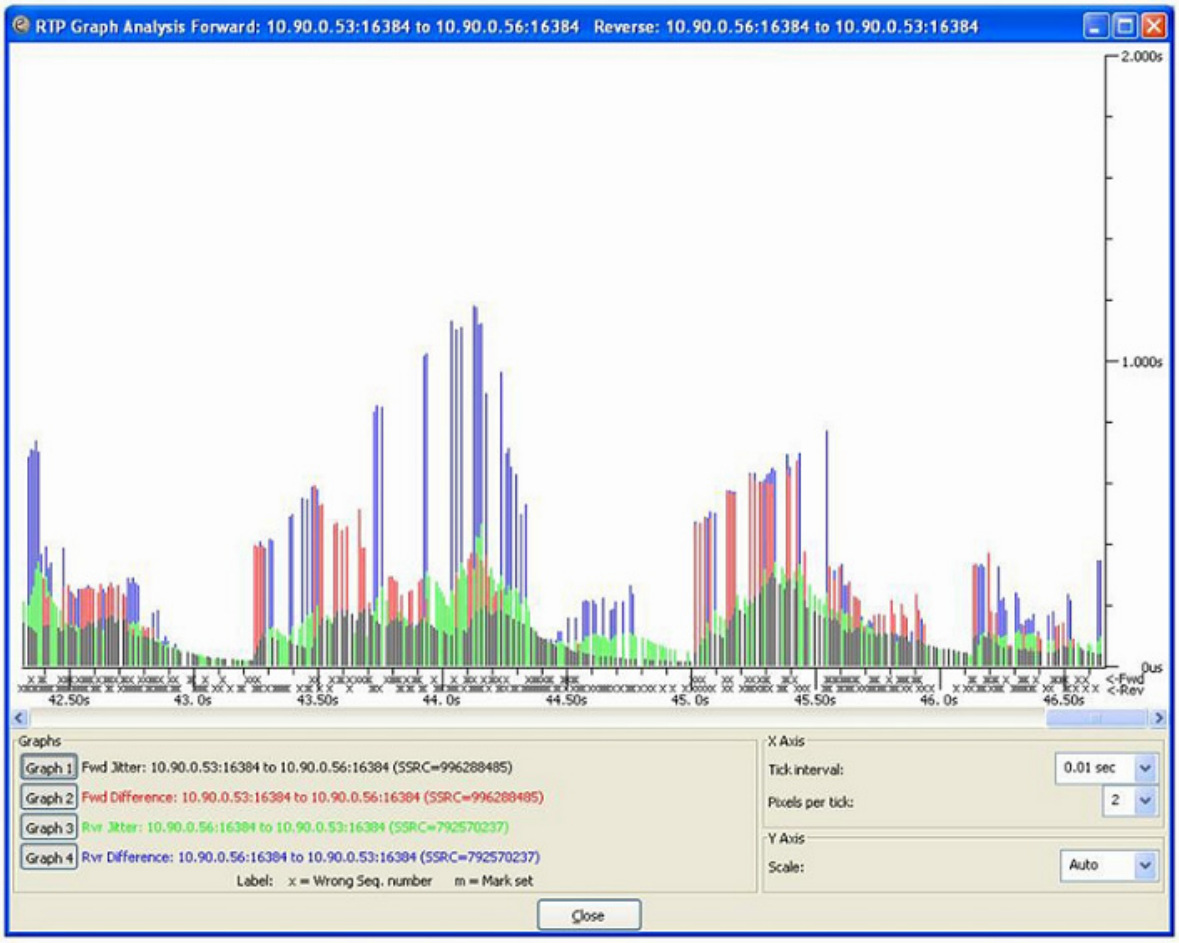


図 9-13 中の紫色の線は、最大ホールド、すなわちテスト中に到達した最大送信電力を示します。黄色い線は、最後のサンプル期間 10 秒の最大送信電力を示します。緑色の線は、テスト期間の平均送信電力を示します。縦の青い点線は、オーバーラップしない 3 つの 802.11b/g チャネルである Ch1、Ch6、および Ch11 を区分しています。この図は、左から右に 2.400 GHz から 2.500 GHz を表します。右端の Ch11 の青い縦線は、ヨーロッパと日本で使用されている 802.11 スペクトルの部分です。このキャプチャは、北米の規制ドメイン用に設定された AP とクライアントを使って取得されました。この図は、Bluetooth イヤホンが FCC 規制の外側で簡単に電波を送信していたことを示しています。

Bluetooth 信号が非常に狭いことに注目してください。Bluetooth は 1 つの MHz の周波数でデータを送信し、送信を停止し、802.11 2.4 GHz 帯域の別の周波数に移動して、データを送信します。この動作は繰り返し実行されます。802.11b と 802.11n-2.4 GHz の信号は、組み合わされた 22 MHz の周波数で送信されます。無線はその 22 MHz の周波数に留まります。22 MHz のこのグルーピングはチャネルと呼ばれます。最大ホールド線は、検索モードでの Bluetooth の強さを示しています。信号レベルは、50 mW（17 dBm）OFDM 802.11n-2.4 GHz 無線の信号レベルを上回っています。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。Bluetooth 信号の強度が低いと、ジッターが発生して MOS 値が低くなります。図 9-14 は、それぞれ Bluetooth イヤホンを使用する 3 つの同時通話での、Ethereal によるジッター分析の例を示します。

図 9-14　　ジッター分析の例



3 つのコールはすべて同じ AP 上にあり、この AP 上の他の電話へのコールでした。Wi-Fi および Bluetooth の干渉については、こちらの IEEE レポートをお読みください。

Wi-Fi OFDM と衝突したときの Bluetooth TDM パケットに対する障害に影響を与える要因には、次のようなものがあります。

- 相対電力
- 帯域幅
- 相互オーバーラップ
- 衝突する OFDM 信号の数

サンプルの Wi-Fi OFDM のパケットと Bluetooth 信号の間の干渉の影響に対するシミュレーションを行いました（図 9-15 を参照）。この図では、標準の GMSK Bluetooth の無歪信号の TDM 特性を示します。左側が時間と周波数（MHz）の関係、右側が時間と I/Q の振幅の関係を示しています。

図 9-15　IEEE 波形シミュレーション

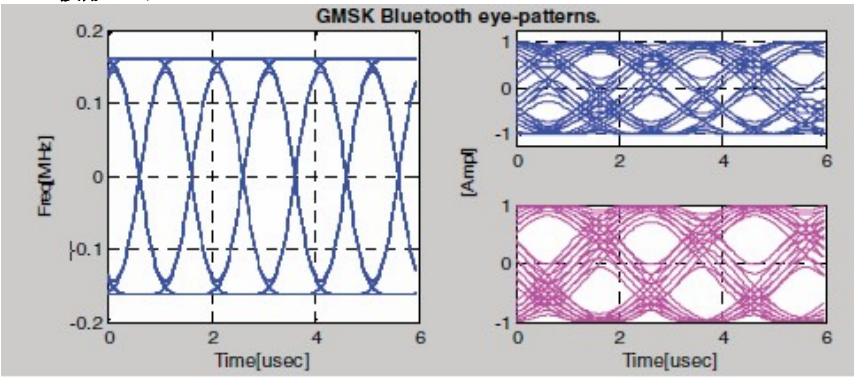


図 9-15 で示すように、ホッピング周期が 625 秒の Bluetooth パケットは、一度に複数の OFDM パケットと干渉する可能性があります。特に、高速の OFDM モード パケット（パケット長が Bluetooth よりはるかに短い）が衝突の対象となる場合は、必ず干渉が発生します。

CHAPTER 10

Cisco Unified Wireless Network ゲスト アクセス サービス

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 WLAN（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。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。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。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、次のような全般的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。

- かつては有線によるネットワーク接続もなかったロビーや共有施設などのエリアを含め、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。

スコープ

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 Network 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、次のドキュメントを参照してください。

Network Virtualization--Guest and Partner Access Deployment Guide

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：キャンパス ワイヤレス ネットワーク全体にわたってゲスト アクセスを必要とするあらゆる場所に実装されます。
- ゲスト トラフィックの分離：ゲストの移動場所を制限するために、キャンパス ネットワーク全体にレイヤ 2 またはレイヤ 3 手法を実装する必要があります。
- 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 Network 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 Ethernet in IP（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。Ethernet in IP 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されるプロトコルやセグメンテーション テクニックを追加する必要がないことです。

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

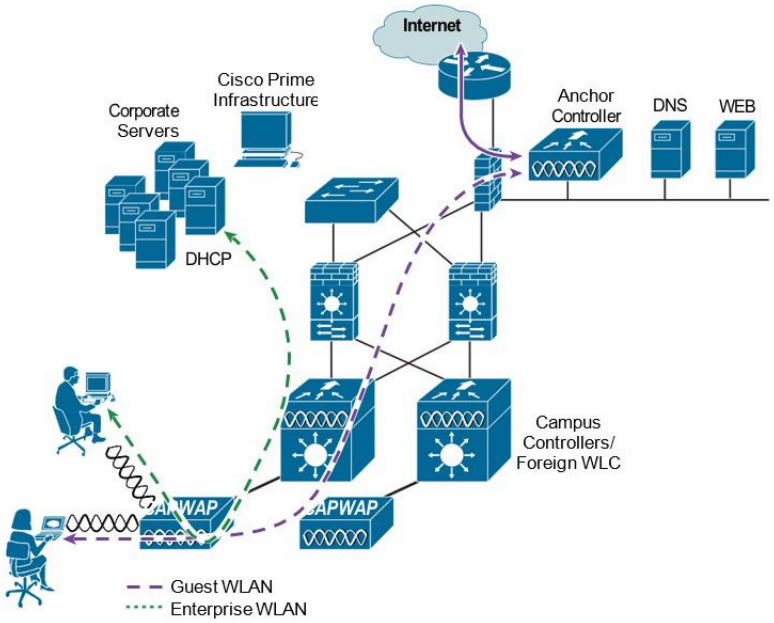


図 10-1 に示すように、アンカー コントローラが企業 DMZ 内に配置され、「アンカー」機能を実行します。アンカー コントローラは、ネットワーク上のその他のキャンパス コントローラを起点とする EoIP トンネルの終端処理に関与します。これらの「外部」コントローラは、企業全体にプロビジョニングされたさまざまな WLAN（1 つ以上のゲスト WLAN を含む）の終端、管理、および標準の動作に関与します。ゲスト WLAN は EoIP トンネルを経由してアンカー コントローラに転送されます。具体的には、ゲスト WLAN のデータ フレームが、CAPWAP を使用して AP から外部コントローラにカプセル化されてから、外部管理システムからアンカー 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

ゲスト アクセス 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。これらの機能はすべて、アンカー コントローラ内で設定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 8.1 以降を使用した場合）。

- WLC 2504
- WLC 3504

- WLC 5508
- WLC 5520
- WiSM-2
- WLC 8510
- WLC 8540

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（フォーリン WLC）として使用できます。

- 仮想 WLC

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 Network 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、プロビジョニングされたゲスト 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

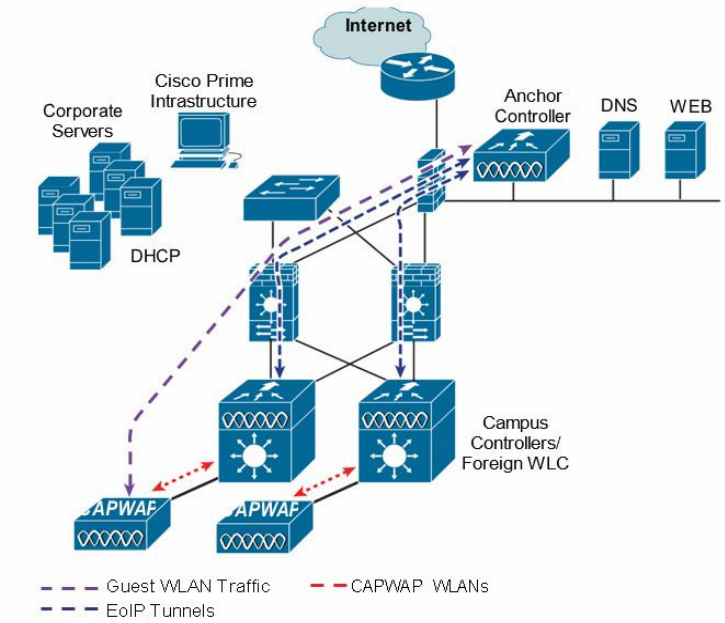
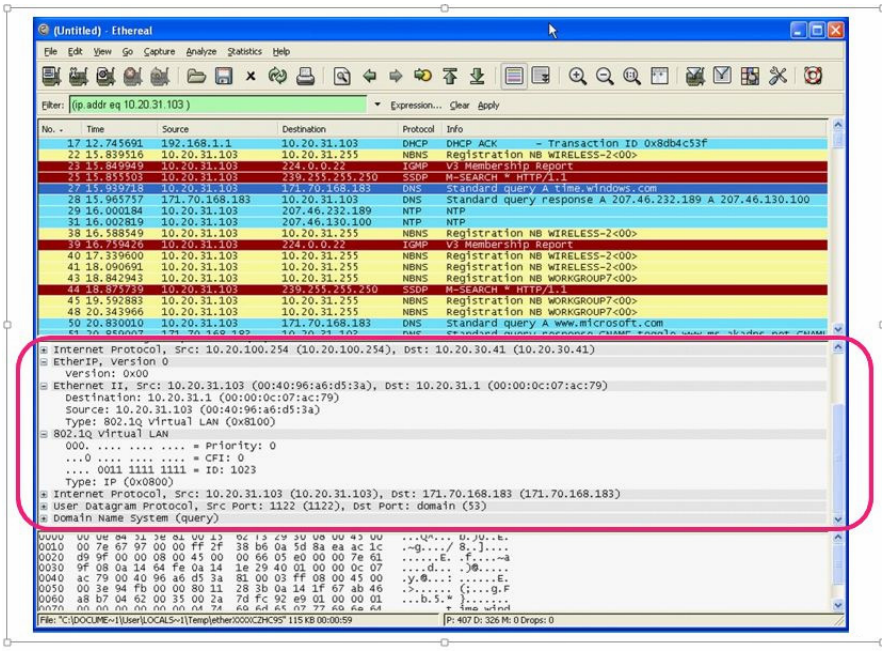


図 10-3 は、ゲスト WLAN がプロビジョニングされた外部コントローラとローカル Web 認証を実行しているアンカー コントローラ間の Ethernet in IP トンネル（強調表示部分）のスニファ トレースを示しています。図中の最初の IP 詳細は、外部コントローラとアンカー コントローラ間の Ethernet in IP トンネルを示しています。2 番目の IP 詳細は、ゲスト トラフィックの詳細です（この場合は、DNS クエリー）。

図 10-3　　Ethernet in IP 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 Ethernet in IP 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。

- UDP 161 および 162：SNMP
- TFTP 用の UDP 69
- HTTP 用または GUI アクセスの HTTPS 用の TCP 80、443、および 8443
- Telnet 用、または CLI アクセスの SSH 用の TCP 23 または 22
- NTP 用の UDP 123
- Syslog 用の TCP 514
- UDP 1812 および 1813 RADIUS

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強く推奨します。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 CAPWAP AP の制御や管理に使用しないようにします。

DHCP サービス

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」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 にマッピングされます。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コスト効率良くサポートするプラットフォームは、Cisco 2504 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 AP の管理に使用されないと考えられるため、12 個の AP をサポートする 2504 で十分です。

1 台のワイヤレス LAN コントローラで、社内にある最大 71 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。

ゲスト アンカー コントローラの選択は、アクティブなゲスト クライアント セッションの数によって定義されているか、またはコントローラ上のアップリンク インターフェイスの容量によって定義されているか、あるいはその両方で定義されたとおりのゲスト トラフィック量に依存します。

ゲスト アンカー コントローラあたりの総スループットとクライアントの制限は次のとおりです。

- 2504 WLC = 1 Gbps および 1000 ゲスト クライアント
- 3504 WLC = 4 Gbps および 3000 ゲスト クライアント
- 5508 WLC = 8 Gbps および 7,000 ゲスト クライアント
- 5520 WLC = 20 Gbps および 20,000 ゲスト クライアント
- Catalyst 6K WiSM-2 = 20Gbps および 15,000 ゲスト クライアント
- WLC 7500 = 10 Gbps および 20,000 ゲスト クライアント
- 8510 WLC = 10 Gbps および 20,000 のゲスト クライアント
- 8540 WLC = 40 Gbps および 64,000 のゲスト クライアント

アンカー コントローラの冗長性 N+1

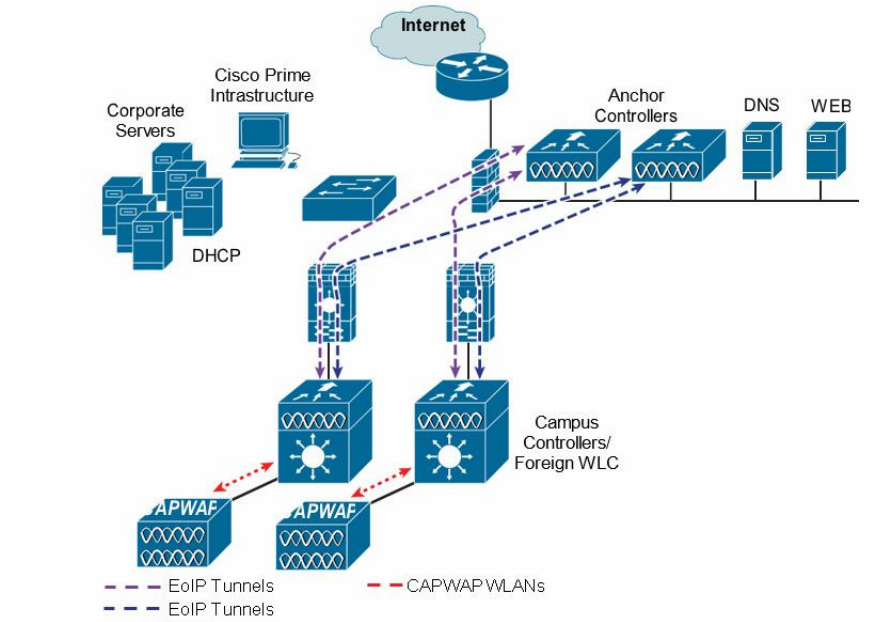
Cisco Unified Wireless Network ソリューション ソフトウェアでは、自動アンカー/モビリティ機能に追加された「ゲスト N+1」冗長性機能がサポートされます。この機能には、自動 ping 機能が導入されています。この機能によって、フォーリン コントローラが積極的に ping をアンカー コントローラに送信して、コントロールとデータ パスの接続を確認できます。障害が発生したり、アクティブなアンカーに到達できなくなった場合には、外部コントローラが次のことを行います。

- 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します。
- 到達できないアンカーに以前に関連付けられた無線クライアントの関連付けを自動的に解除します。
- 無線クライアントを代替アンカー WLC に自動的に再び関連付けます。

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 に関連付けら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関連付けられます。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、資格情報の再送信が要求されます。

(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。

アンカー コントローラの冗長性のプライオリティ

ゲスト アンカーの優先順位機能は、アンカー WLC 間での「アクティブ/スタンバイ」負荷分散を実現するメカニズムを提供します。これは、アンカー WLC ごとに固定のプライオリティを割り当て、負荷を最もプライオリティの高い WLC に分散するか、プライオリティ値が同じ場合はラウンド ロビン方式で負荷を分散することによって実現できます。

8.1 より前のリリース	リリース 8.1
すべてのゲスト クライアントが、アンカー WLC 間でラウンド ロビン方式で負荷分散されます。	すべてのゲスト クライアントが、ローカルの内部 WLC に関してプライオリティが最も高いアンカー コントローラに送信されます。
1 つのアンカーで障害が発生した場合は、ゲスト クライアントが残りのアンカー WLC 間で負荷分散されます。	1 つのアンカーで障害が発生した場合は、ゲスト クライアントが次にプライオリティが高いアンカーに送信されるか、残りのアンカーのプライオリティ値が同じ場合はラウンド ロビン方式でアンカーに送信されます

WLAN を設定するときに、ゲスト アンカーにプライオリティを設定できます。プライオリティ値は 、1（高）～ 3（低）の範囲か、primary、secondary、または tertiary のいずれかで、定義されたプライオリティがゲスト アンカーと一緒に表示されます。アンカー WLC 単位で許可されるプライオリティ値は 1 つだけです。ゲスト アンカーの選択は、単一のプライオリティ値に基づくラウンド ロビンで行われます。ゲスト アンカーがダウンした場合は、プライオリティが同じゲスト アンカーでフォールバックが行われます。プライオリティ値が同じすべてのゲスト アンカーがダウンした場合は、次に高いプライオリティに基づくラウンド ロビン ベースで選択が実行されます。デフォルトのプライオリティ値は 3 です。WLC をリリース 8.1 にアップグレードすると、プライオリティ 3 のマークが付けられます。プライオリティ設定はリブート後も保持されます。また、プライオリティ設定は、シームレスなスイッチオーバー用の HA ペア間で同期されます。同じ一連のルールが、IPv4 アドレッシングか、IPv6 アドレッシングかに関係なく、アンカー WLC の決定に適用されます。つまり、デュアル スタック ケースを含め、最も高いプライオリティ値が決定因子であって、アドレッシングではありません。

[Restrictions（機能制限）]

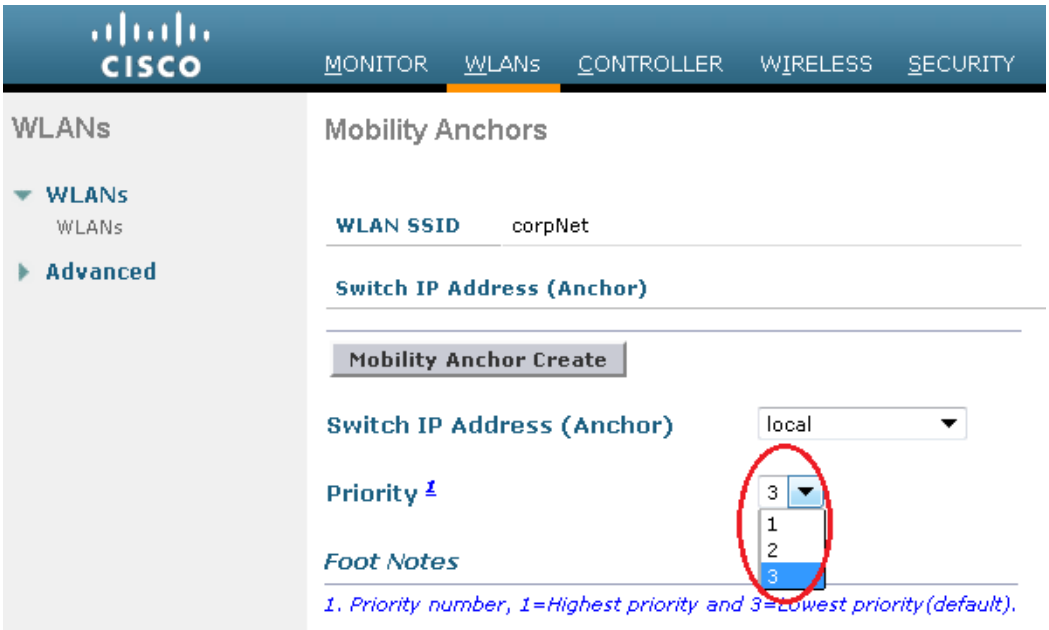
- プライオリティ値の使用回数に対するハード リミットはありません。
- この機能は、ワイヤレスと「旧式の」モビリティ モデルにのみ適用されます。
- WLAN 単位でサポートされる最大アンカー数は 24（8.1 より前のリリースの WLAN 単位の最大アンカー数と同じ）です。
- リリース 8.1 からダウングレードした場合は、この機能が以前のイメージではサポートされないため、無効になります。
- プライオリティが最も高いゲスト アンカーが起動すると、既存の接続はその新しいプライオリティの高いアンカーに移動せず、新しい接続のみがそのアンカーに移動します。
- この機能は、すべての内部 WLC とアンカー WLC がリリース 8.1 を使用している場合に適用されます。
- 内部/フォーリン コントローラに優先順位 0 のローカル アドレスがあってはなりません。出力内の優先順位 0 はローカル IP アドレスを示します。たとえば、トンネルの終端を持つ DMZ 上のアンカー WLC の場合です。

構成の考慮事項

- プライオリティ設定は、外部コントローラ WLAN 上でのみ行う必要があります。モビリティ リストに、0 値および同じコントローラが少数の WLAN 用のアンカー、および少数の WLAN 用のフォーリン コントローラとして機能していることを表す 0 以外の値が表示されていて、DMZ に WLC があり、その WLC に接続している AP が存在しない場合、その WLAN に対し優先順位は 0 以外であってはなりません。これはネットワーク上のすべてのクライアントの終端ポイントでなければならないからです。
- 外部 WLC に対する 0 のプライオリティとアンカー WLC に対する 0 以外のプライオリティが表示されないようにするのが理想です。たとえば、10.10.10.10（サイト A）と 20.20.20.20（サイト B）のプライオリティを 0 にしないようにして、DMZ コントローラ 172.10.10.10（サイト A）と 172.20.20.20（サイト B）のプライオリティを 0 以外の値にしないようにする必要があります。
- コントローラ固有の IP アドレスをアンカーとして選択した場合、ここで優先順位値 0 を設定することはできません。コントローラ固有の IP アドレスがアンカーとして選択された場合は、自動的にプライオリティが 0 に設定されます。

例

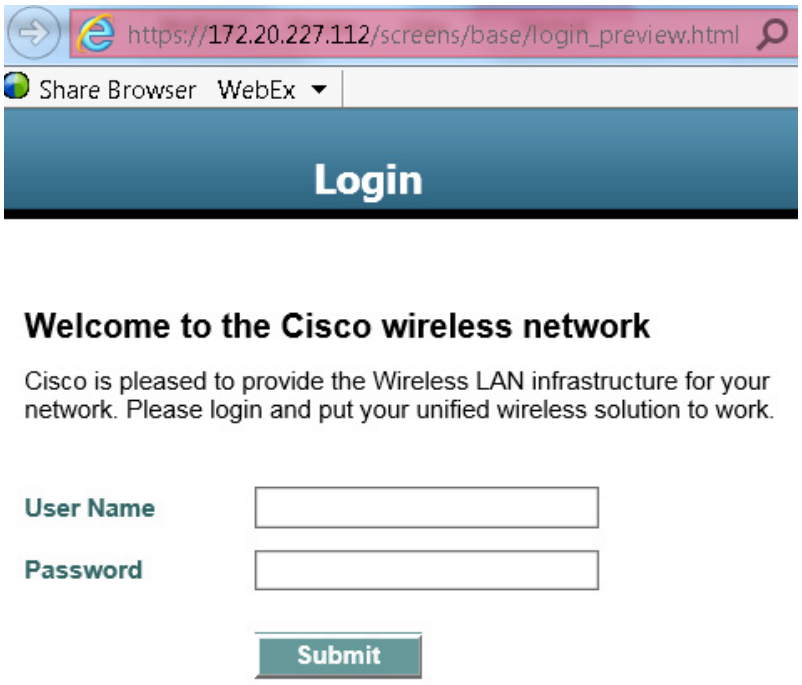
- ローカル アンカー WLC は、リモート アンカー WLC のグループより高いプライオリティのグループに分類される場合があります。
- ゲスト クライアントのトラフィックは、リモート WLC よりプライオリティ値の高い内部 WLC に対してローカルなアンカー WLC に流れます。
- ローカル アンカーはプライオリティ値が同じであるため、ゲスト クライアントのトラフィックがローカル アンカー WLC 間でラウンド ロビン方式で負荷分散されます。
- すべてのローカル アンカー WLC で障害が発生した場合は、トラフィックが次のプライオリティ レベルのリモート アンカー WLC 間でラウンド ロビン方式で負荷分散されます。



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情報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 コントローラ 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、カスタマイズされたページを管理者が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」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 に関連付けられると、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モニタできるように、追加ポート番号を 1 つ設定するオプションがあります。この設定は、コントローラの CLI を通してのみ使用可能です。

```
<controller_name> config> networkweb-auth-port <port>
```

ゲスト資格情報の管理

ゲスト資格情報は、管理システムまたはコントローラの Web UI 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、ゲスト資格情報を作成するためのロビー アンバサダー アクセスを許可する限定的な特権アカウントを管理システム内に作成できます。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。

管理システム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。次にいくつかの新しいゲスト ユーザ テンプレートのオプションおよび機能を示します。

- 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電子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電子メールで送信されます。
- （ゲスト）WLAN SSID および管理システムのマッピング情報（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。

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。*「Web」ポリシーで設定した* WLAN を持つコントローラだけが、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 テンプレートを管理システムのマップ 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、無線ゲストが関連付けられて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 コントローラのロビー管理者のアクセス

中央集中型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、ロビー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。ロビー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、管理システム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(User name)
- 生成パスワード
- 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:秒
- SSID
- ゲスト ロール プロファイル
- 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

管理システム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。ローカルのロビー管理者のアカウントには、管理システム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管理システムで更新されない限り、管理システムに自動的に表示されません。WLC 設定の更新の結果として管理システム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」で説明したように、管理者が管理システム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、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）。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。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 [Network User] 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。

外部認証

WLC およびゲスト 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」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、パスワード認証プロトコル（PAP）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。

ISE または 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 とともに ISE または 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。

Cisco Secure Access Control System

特に、次のドキュメントを参照してください。

Cisco Secure Access Control System インストレーション/アップグレード ガイド

ISE と Active Directory の統合：

Active Directory Integration with Cisco ISE

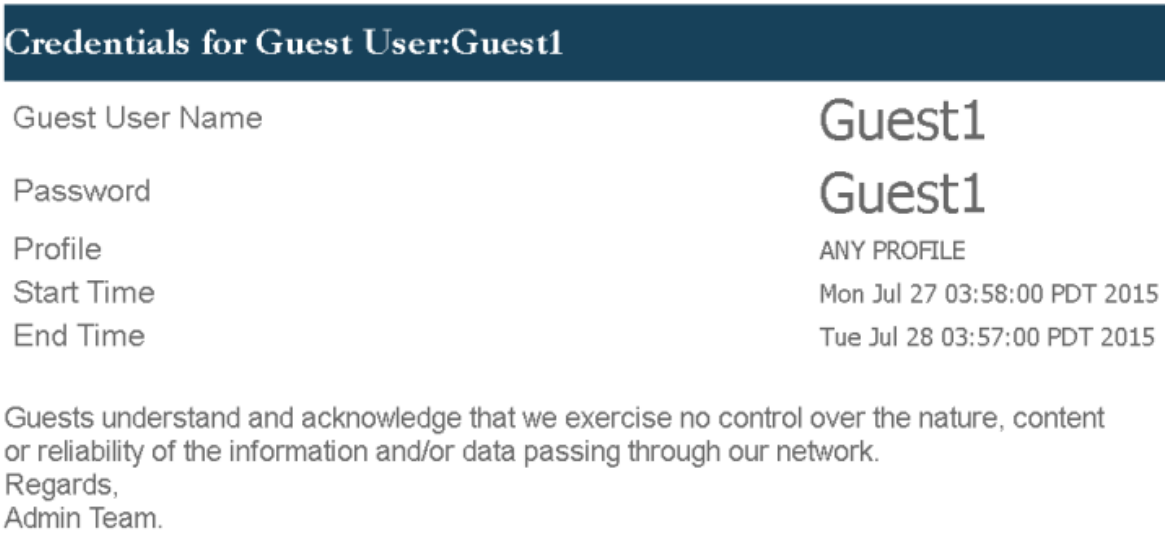
ゲスト パススルー

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電子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」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　　電子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 Network 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、コントローラの管理 IP アドレス（**https://***management_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 アドレスへの HTTPS セッションを開くことによって確立されます。

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。詳細については、「アンカー コントローラ展開ガイドライン」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推奨します。

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、AP 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 トンネルにマッピングします。
- 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 Network ゲスト アクセス 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。

- 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 Cisco Unified Wireless Network 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。
- 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。
- 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 にマッピングするのに必要な 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。ここでは、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。
- ゲスト アカウント管理: ここでは、コントローラまたはアンカー WLC のロビー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。
- 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。
  - Web ポータル ページの設定と管理
  - 外部 Web リダイレクションのサポート
  - 事前認証 ACL
  - アンカー WLC DHCP の設定
  - 外部 RADIUS 認証
  - 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」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推奨します。

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。

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特定の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推奨します。

- 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、192.0.2.1 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 グループのメンバー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送信元 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」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　[Controller] タブをクリックします。

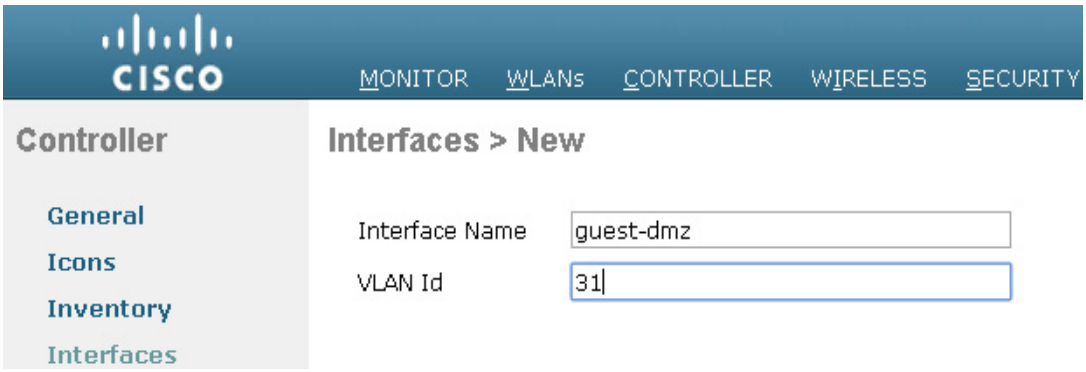
ステップ 2　左側のペインで、[Interfaces] をクリックします（図 10-8 を参照）。

図 10-8　コントローラ インターフェイス

ステップ 3　[New] をクリックします。

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）。

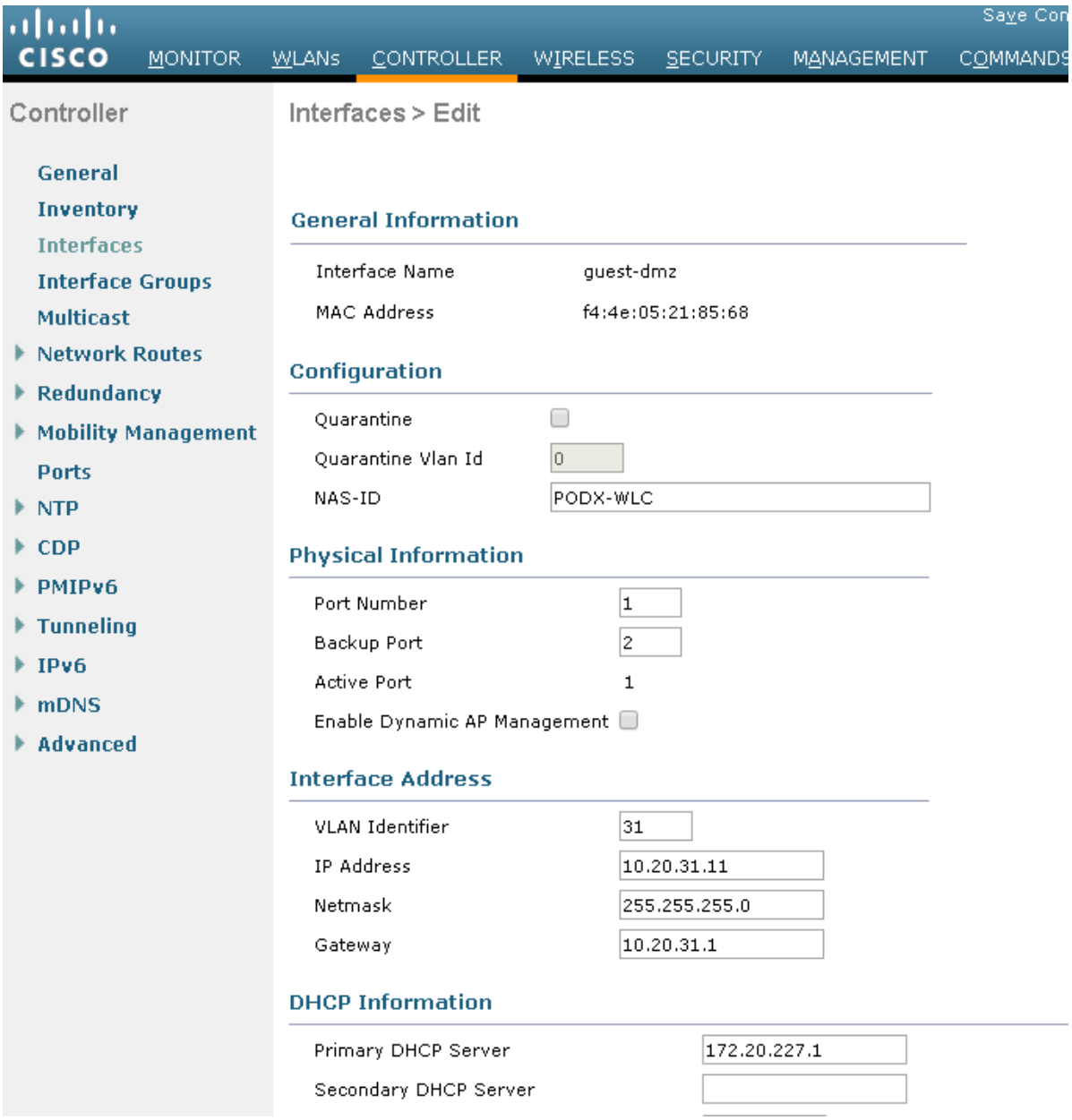
図 10-9　　インターフェイス名と VLAN ID



ステップ 5　次のプロパティを定義します。

- Interface IP
- Mask
- 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)　内部 DHCP サーバは推奨されませんが、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。内部 DHCP サーバのサポートがコントローラ プラットフォームに存在するかどうか確認します。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

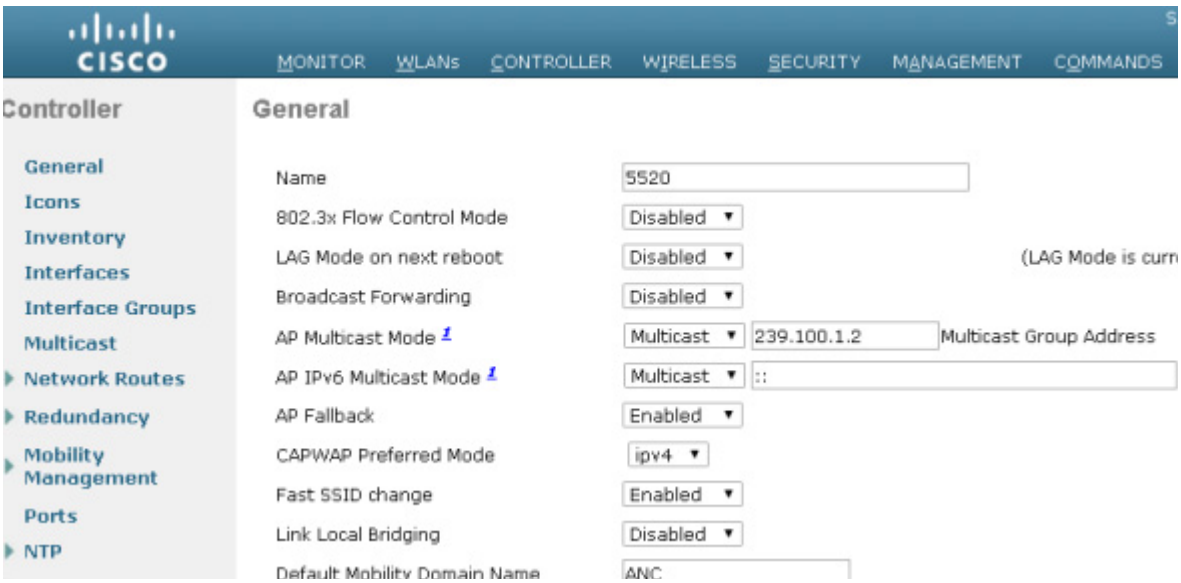
アンカー WLC のデフォルト モビリティ ドメイン名を設定します。アンカーのモビリティ ドメイン名は、外部 WLC に設定した名前と異なる必要があります。以下の例では、企業の無線展開に関連付けられている WLC（外部コントローラ）は、すべてモビリティ グループ「SRND」のメンバーです。一方、ゲスト アンカー WLC は、別のモビリティ グループ名「ANC」で設定されます。これは、企業の無線展開に関連付けられているプライマリ モビリティ ドメインから、アンカー WLC を論理的に区別しておくために行われます。

ステップ 1　[Controller] 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



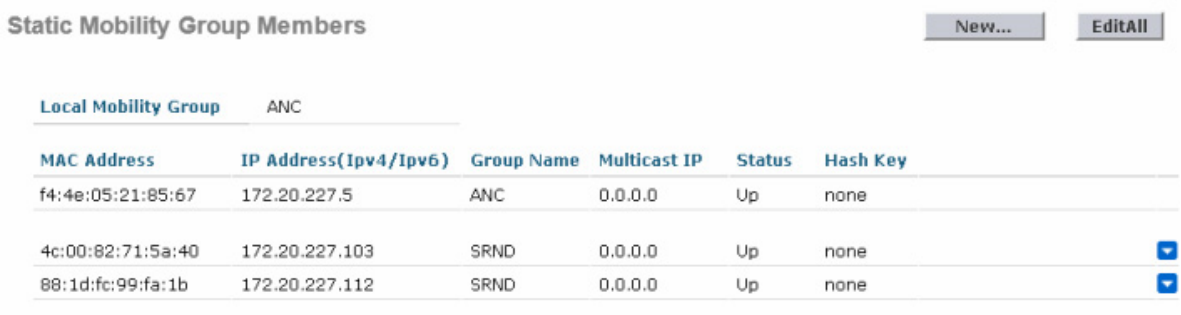
アンカー WLC のモビリティ グループ メンバーの定義

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 メンバーとして定義する必要があります。

ステップ 1　[Controller] タブをクリックします。

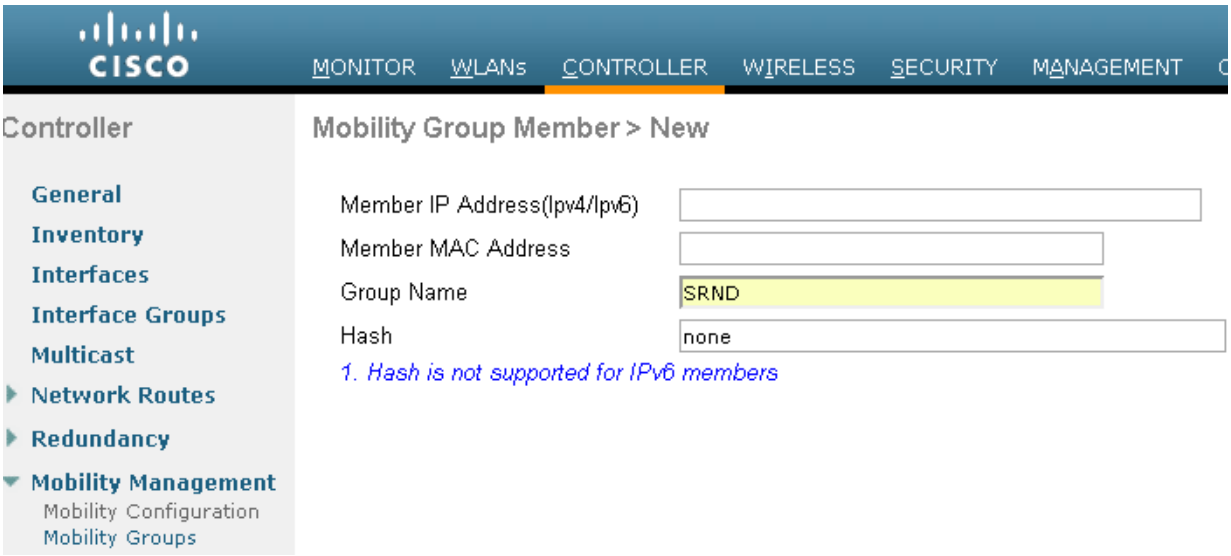
ステップ 2　左側のペインで、[Mobility Management] をクリックし、[Mobility Groups] をクリックします（図 10-12 を参照）。

図 10-12　　モビリティ グループ メンバーの定義



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。メンバーの 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関連付けられたアドレスです。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 アンカー冗長性）、「アンカー WLC のデフォルト モビリティ ドメイン名の定義」と「アンカー WLC のモビリティ グループ メンバーの定義」の手順を繰り返します。

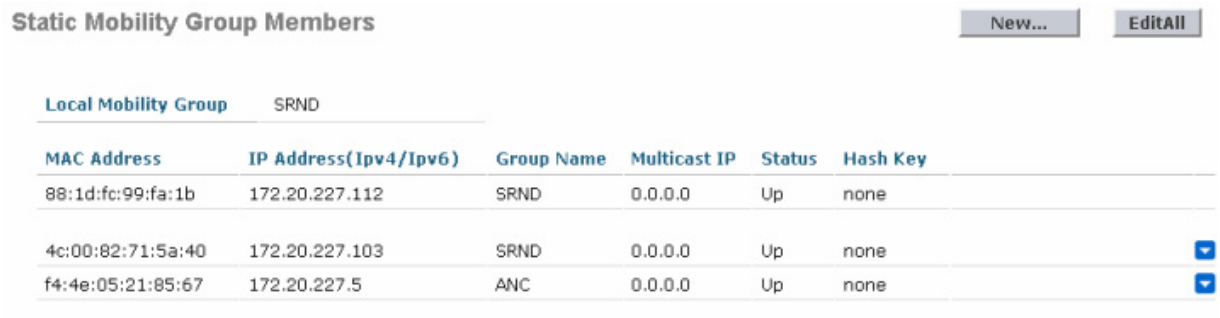
外部 WLC のモビリティ グループ メンバーとしてアンカー WLC を追加

「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」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 をマッピングします。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 グループのメンバー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 メンバーの定義」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」のメンバー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 メンバー 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



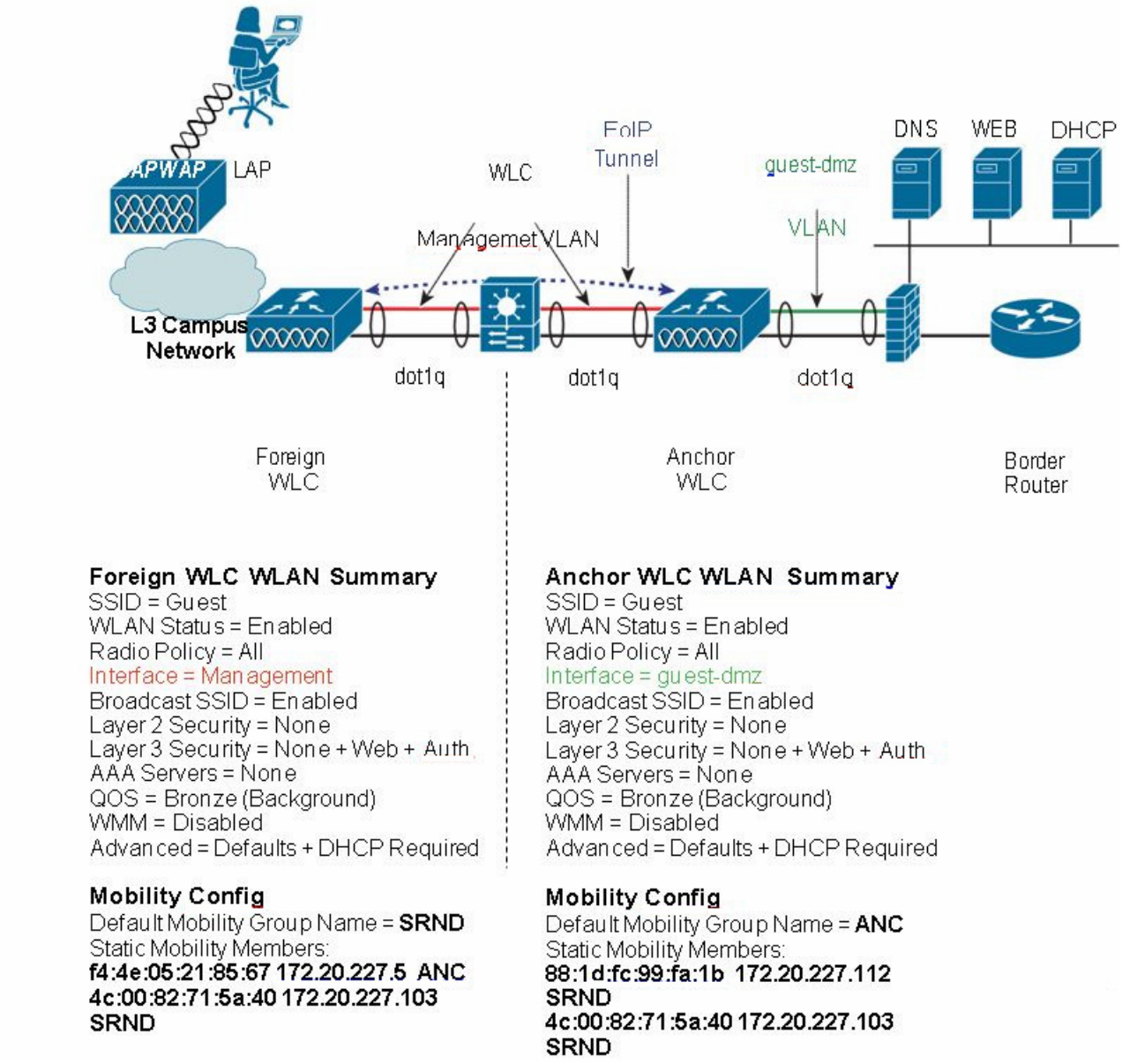
（注）　ゲスト アンカー冗長性機能が展開されている場合、2 つ以上のアンカー WLC エントリが各外部 WLC のモビリティ グループ メンバー リストに追加されます。

ゲスト WLAN の設定

この項では、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 に関連付けられた 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 CAPWAP、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 設定のハイ レベルの概略図を示しています。

図 10-15　WLAN の設定

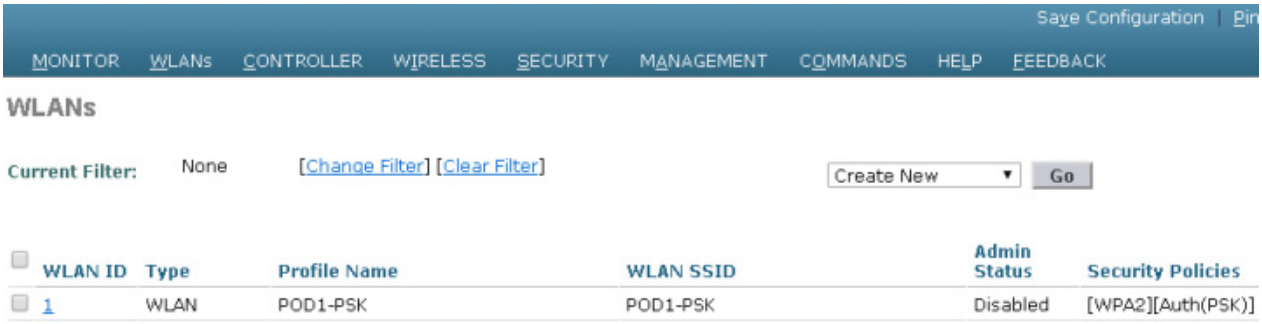


（注）　[WLAN Security]、[QoS]、および [Advanced] 設定タブで定義するパラメータは、アンカーおよび外部コントローラの両方で同じ設定にする必要があります。

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



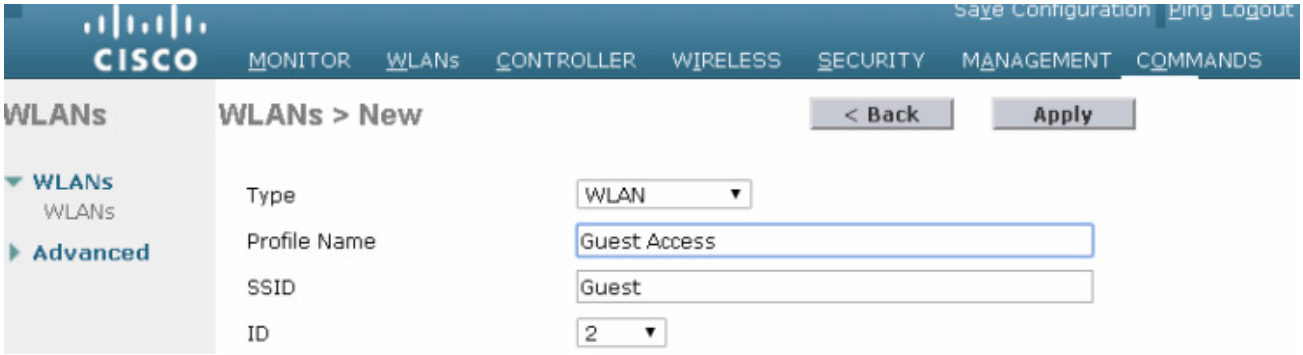
ステップ 2　将来のゲスト ユーザが、直感的に理解できるか、または認識しやすい SSID を定義します。

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　[Profile Name] を指定します。

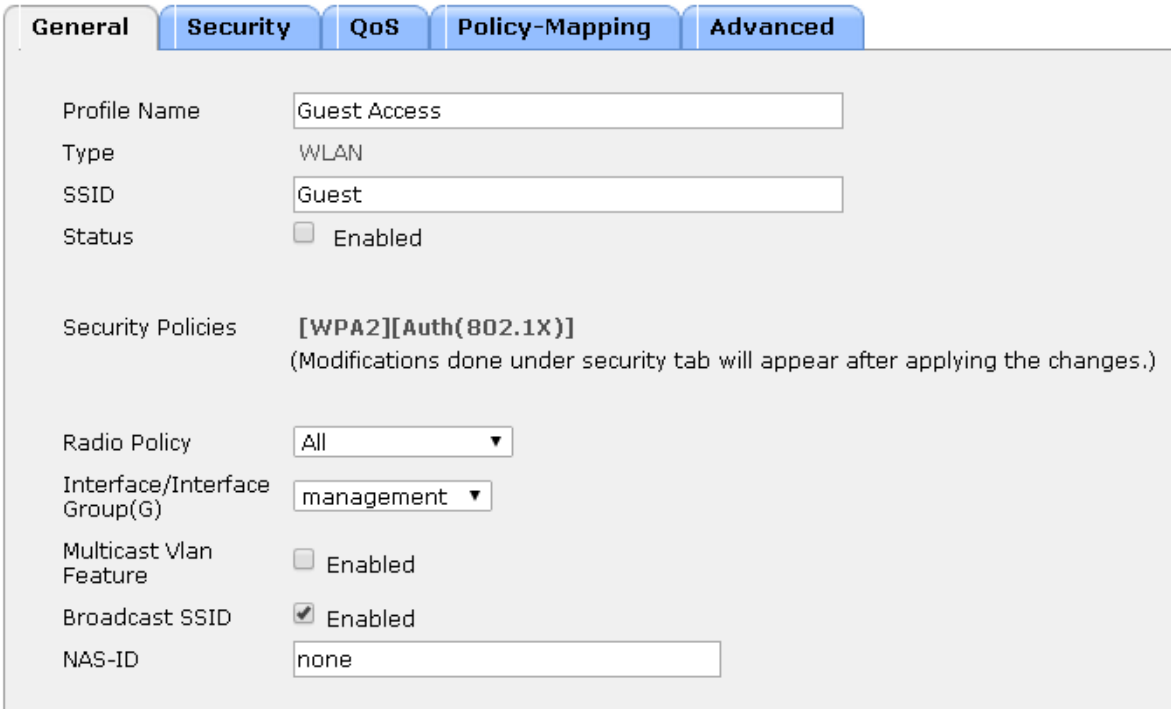
ステップ 4　[Apply] をクリックします。（図 10-17 を参照）。

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デフォルト インターフェイスは、管理インターフェイスです。EoIP トンネルがアンカーによって確立できない場合、外部コントローラは、以前に到達不能なアンカーと関連付けられていた無線クライアントの関連付けを解除してから新しいクライアントを割り当て、外部ゲスト WLAN 自体の下で設定されたインターフェイスにクライアントを再度関連付けます。このため、外部のゲスト WLAN をルーティング不可能なネットワークにリンクするか、あるいは到達不能 IP アドレスを持つ管理インターフェイスの DHCP サーバを設定することを推奨します。アンカーが到達不能になった場合、管理ネットワークへのゲスト クライアントのアクセスを防止します。

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。

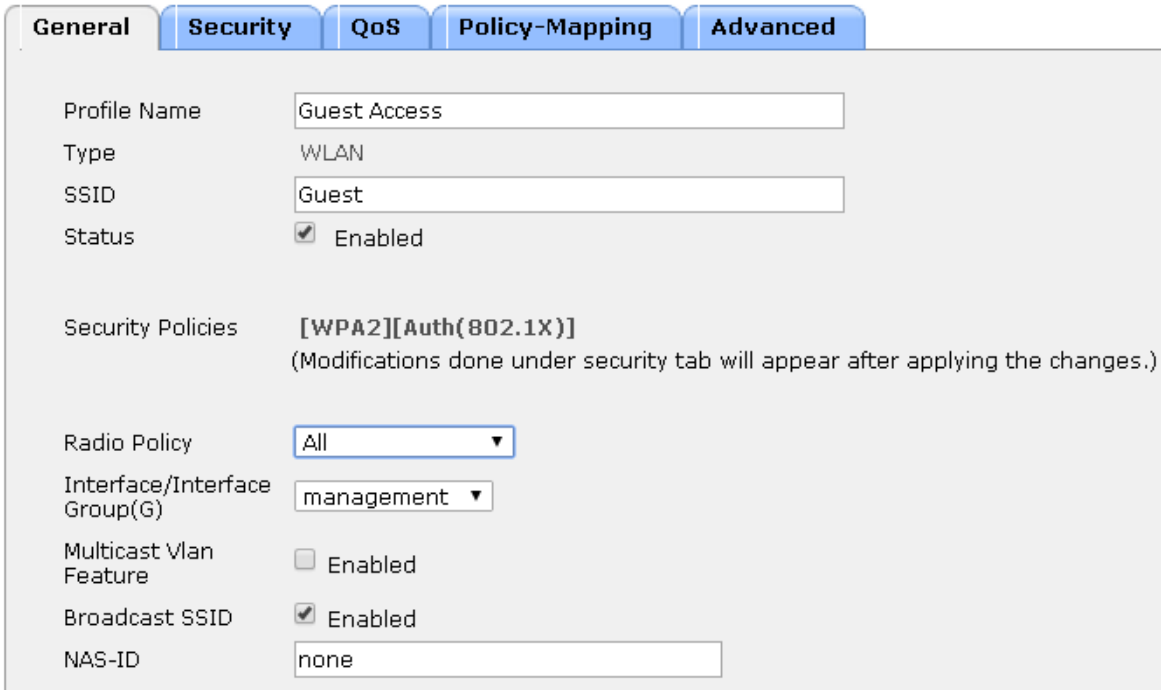
ステップ 1　[WLAN Status] の隣のボックスをクリックして WLAN を有効にします。

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。

- [Broadcast SSID] はデフォルトで有効になるので、有効なままにします。
- デフォルトでは、WLAN は WLC の [management] インターフェイスに割り当てられます。これは変更しないでください。

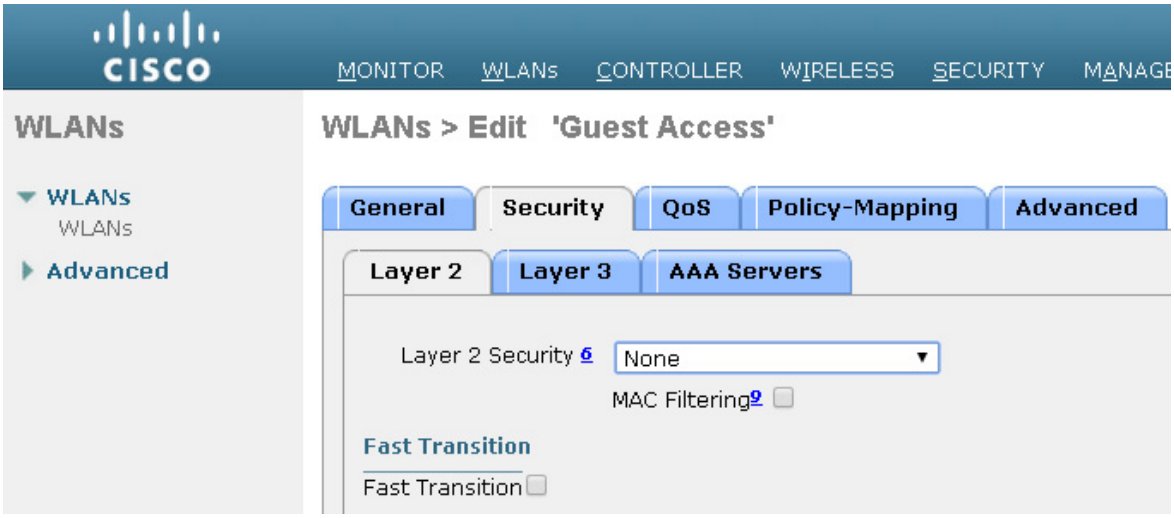
ステップ 3　[Security] タブをクリックします。(図 10-19 を参照)。

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 のレイヤ 2 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 10-22 を参照）。

図 10-21　WLAN のレイヤ 2 セキュリティ設定

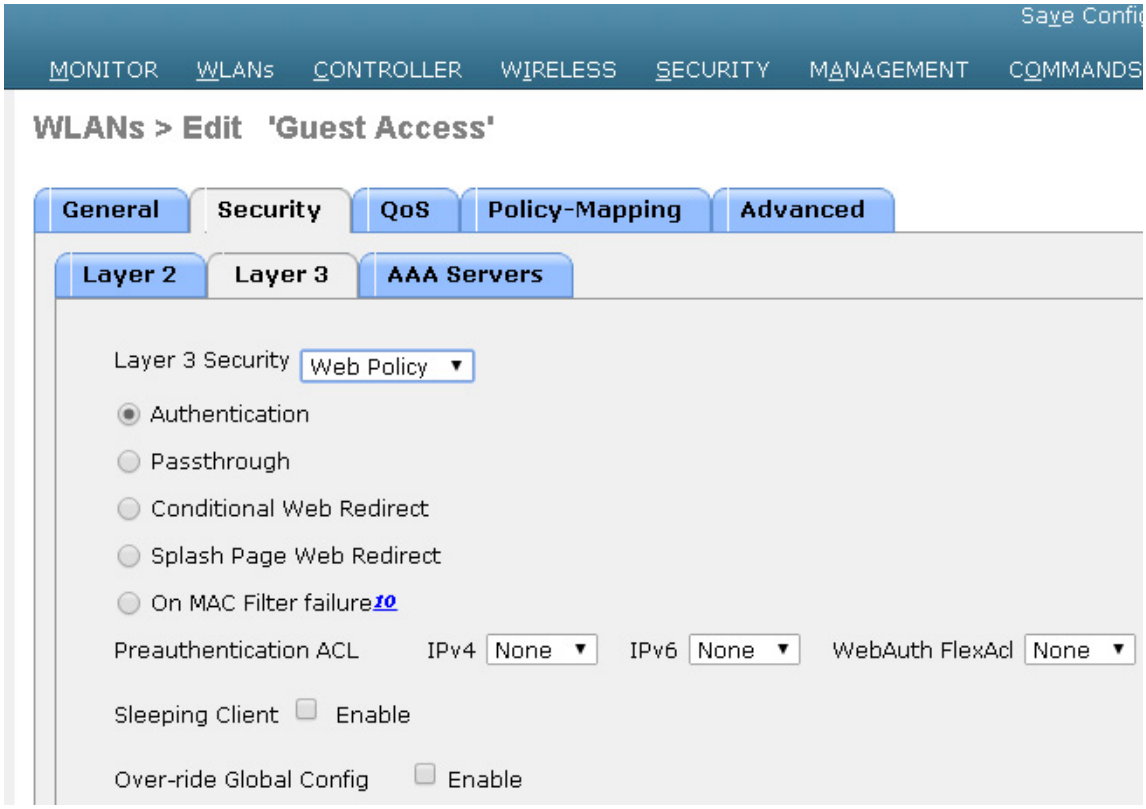
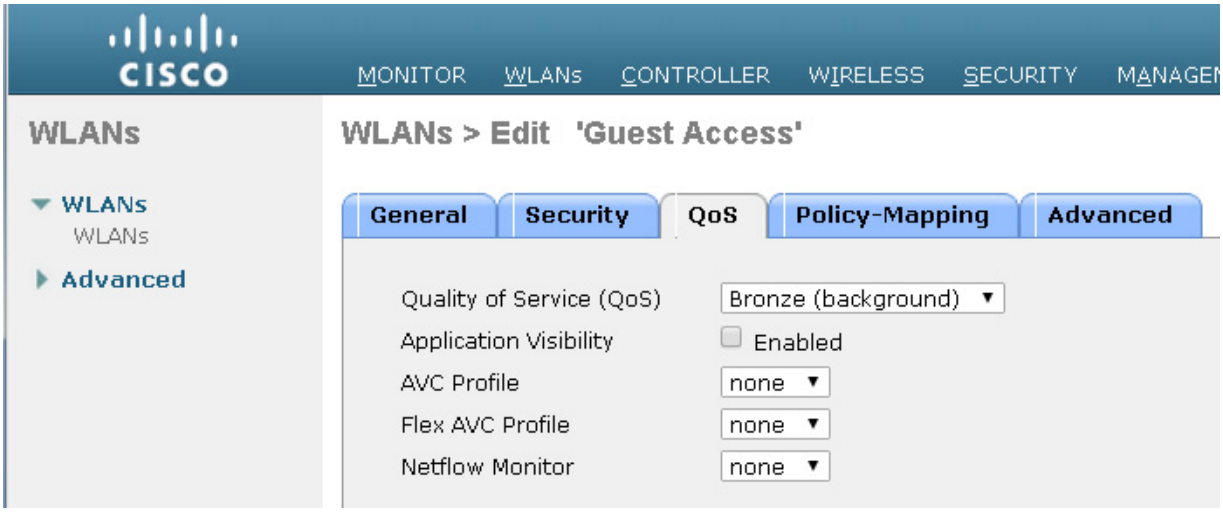


図 10-22　ゲスト WLAN のレイヤ 3 セキュリティ設定



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）。

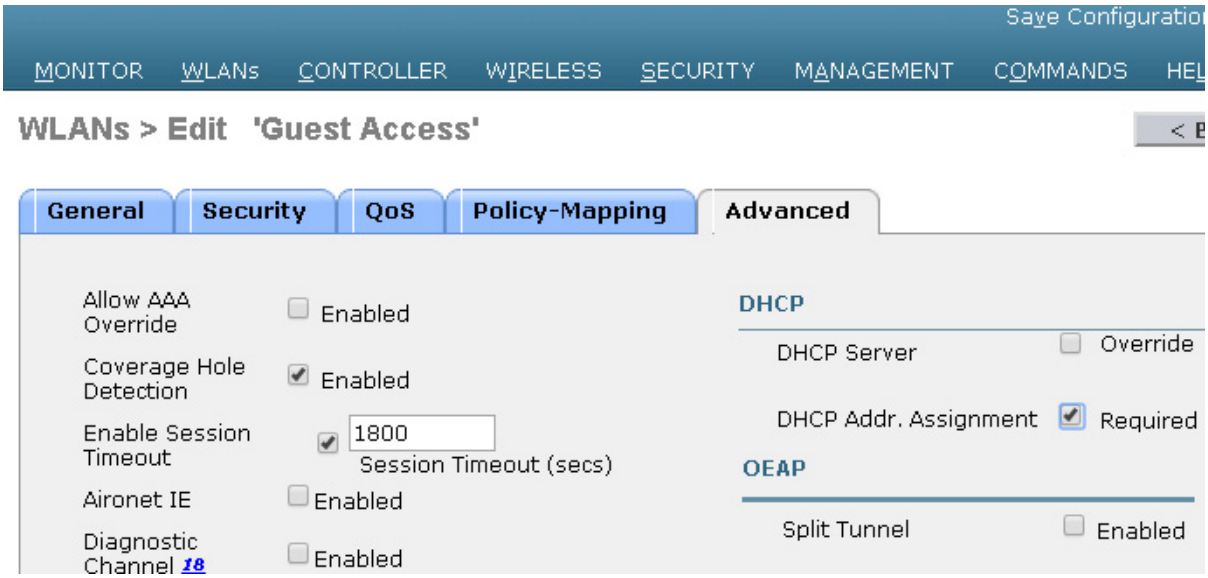
WLC が認証前にクライアント間で DNS トラフィックを受け渡しすることを示す、警告のダイアログボックスが表示されます。

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」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 認証ポリシーとともに使用される場合、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 10-23 を参照)。

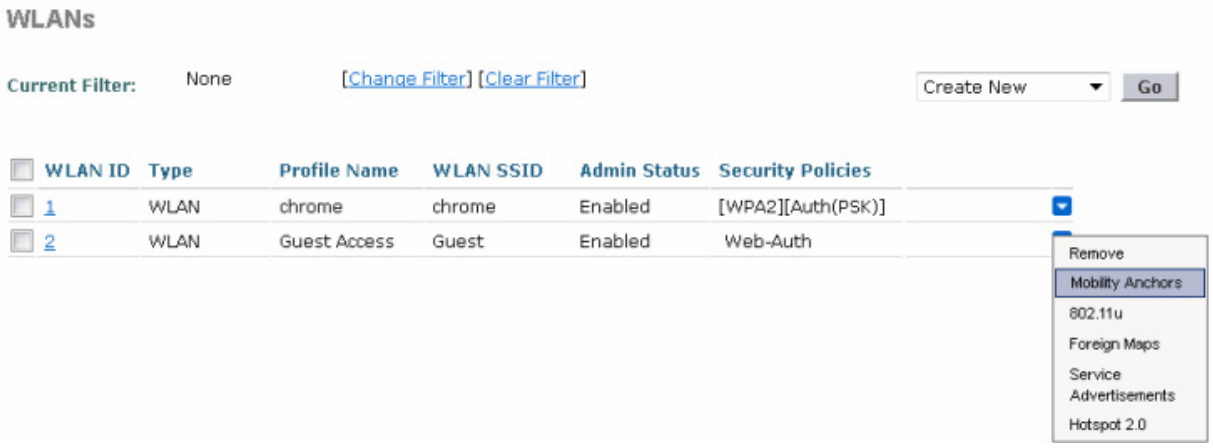
図 10-23　ゲスト WLAN QoS 設定



ステップ 9　オプションで、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 クラスに再割り当てされています。

ステップ 10　[Advanced] タブをクリックします。(図 10-24 を参照)。

図 10-24　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] に設定することを推奨します。

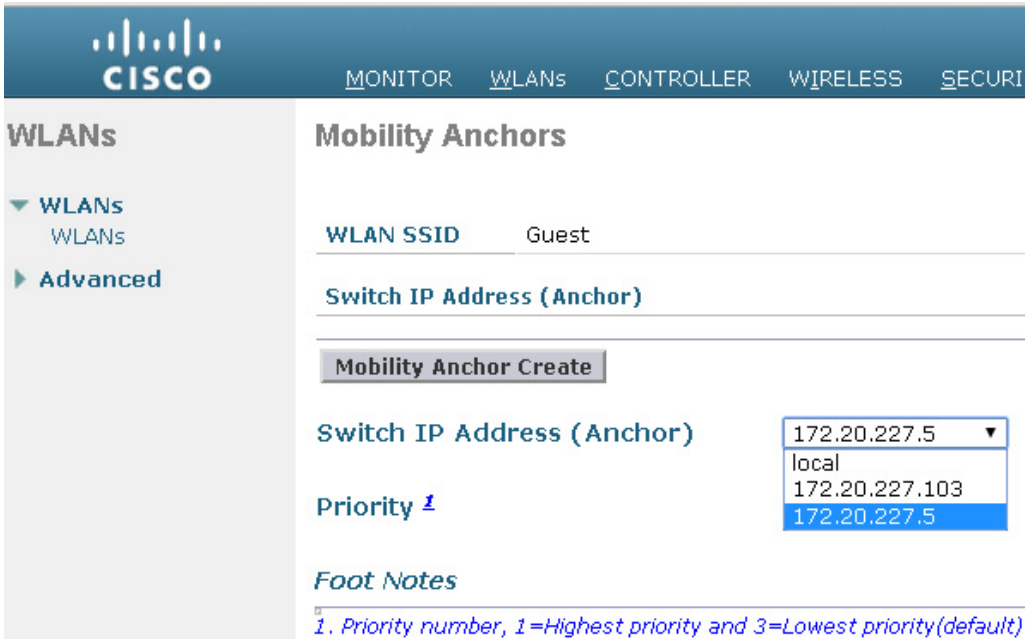
ステップ 13　最後に、[Apply] をクリックします。

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 10-25 を参照)。

図 10-25　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 メンバーとしてアンカー WLC を追加」で設定されたものと同じ IP アドレスです。

ステップ 4　[Priority] フィールドで、アンカー WLC のプライオリティの数値を選択します(複数のアンカー WLC が設定されている場合)。

ステップ 5　[Mobility Anchor Create] をクリックします。(図 10-27 を参照)。

図 10-26　[Switch IP Address (Anchor)] からの管理インターフェイスの選択

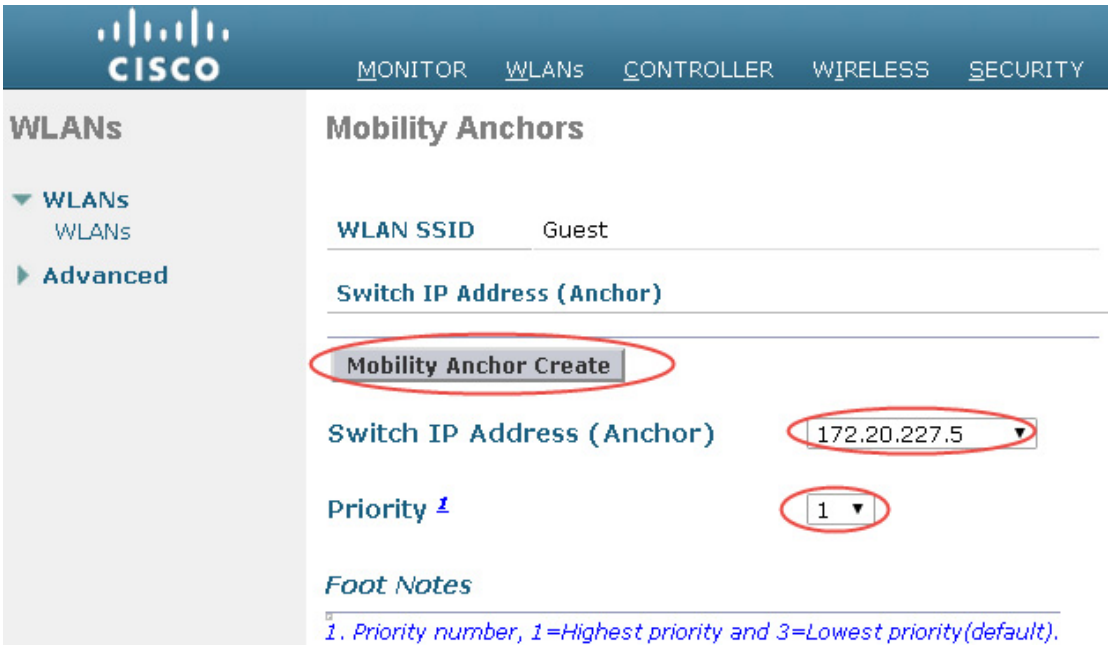
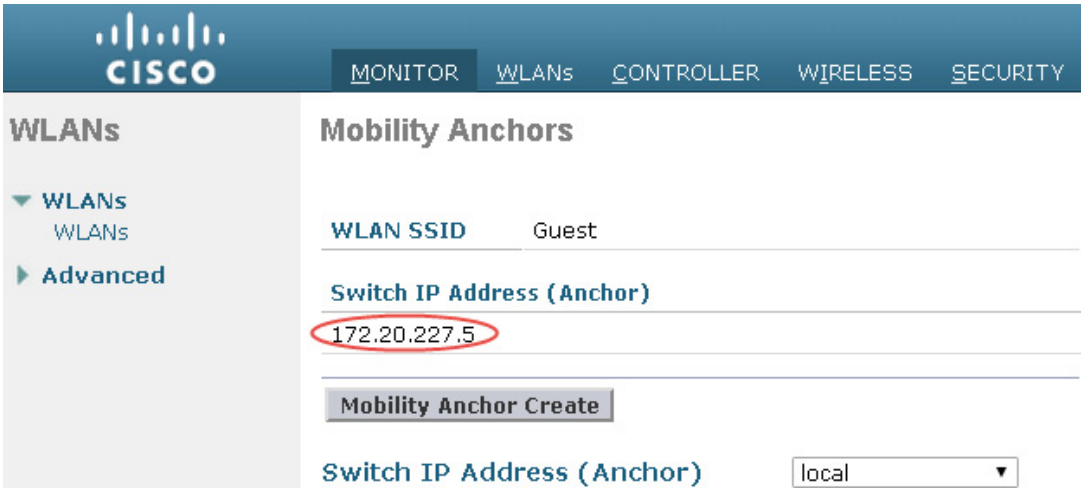
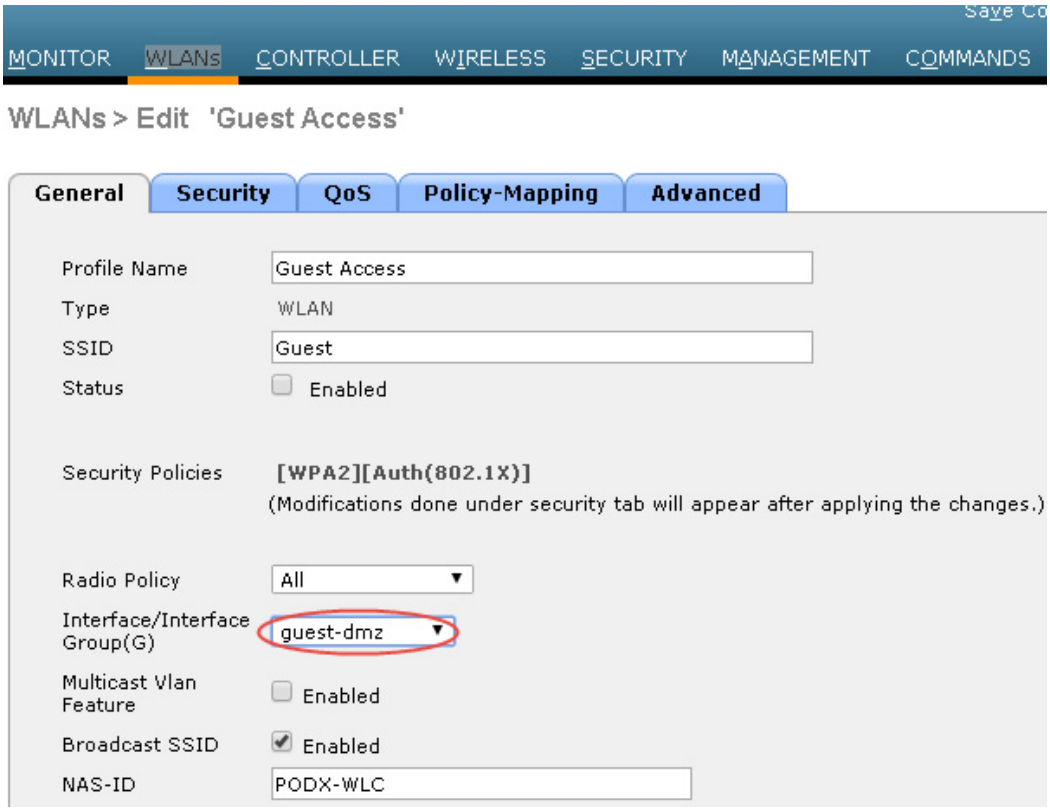


図 10-27　WLAN モビリティ アンカーの選択



設定されると、図 10-28 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 10-28　　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 CAPWAP 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。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 6　終了する場合は、[Back] をクリックします。

ステップ 7　展開されている追加の各アンカー WLC（ゲスト アンカー冗長性）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」から「ゲスト WLAN モビリティ アンカーの設定」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 がマッピング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。

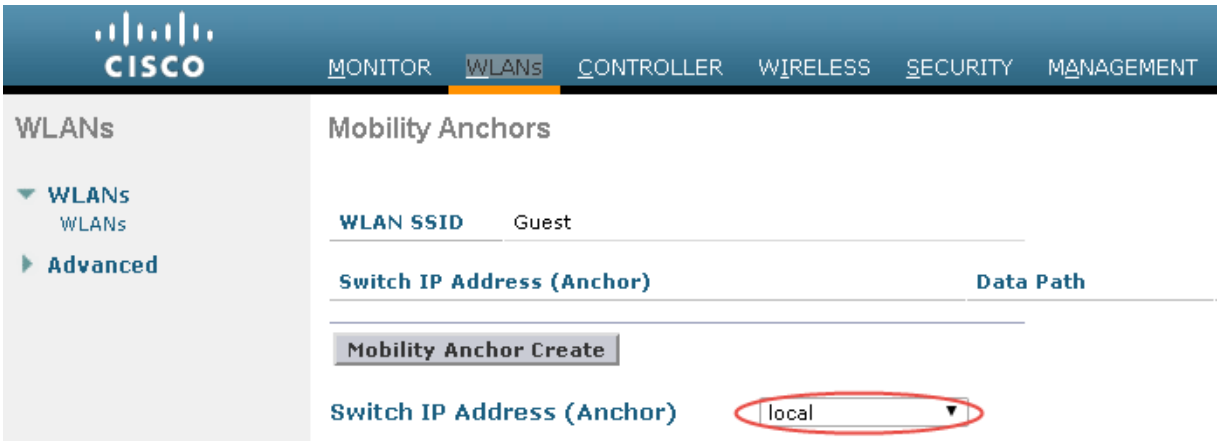
ステップ 1　[WLANs] タブをクリックします。

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 の一般的な設定の [Interface] で、「ゲスト VLAN インターフェイスの設定」で作成されたインターフェイス名を選択します（図 10-29 を参照）。

ステップ 3　[Apply] をクリックします。

図 10-29　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。

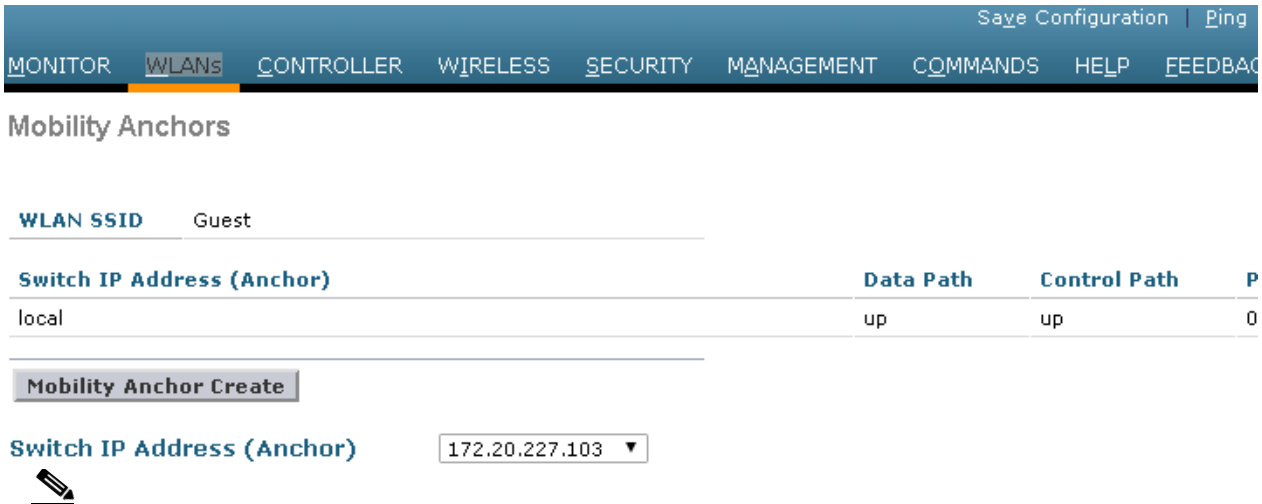
ステップ 1　[WLANs] タブをクリックします。

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。

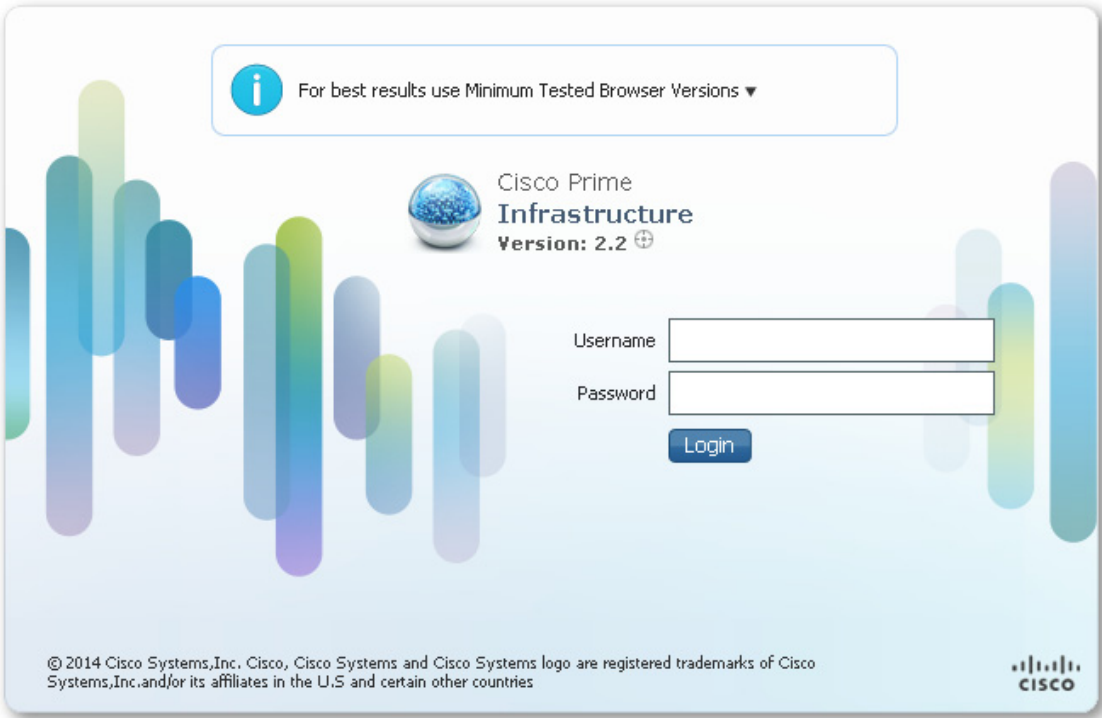
ステップ 4　[Mobility Anchor Create] をクリックします。（図 10-30 を参照）。

図 10-30　ゲスト WLAN モビリティ アンカーの定義



(注)　ゲスト WLAN モビリティ アンカーは、ローカルです（図 10-31 を参照）。

図 10-31　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。アンカー コントローラの SSID のプライオリティは常に 0 になります。

ステップ 5　ゲスト アンカー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 2 つのいずれかの方法で資格情報を作成して適用できます。

- 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、ローカルのロビー管理者アカウントまたは読み取り/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。

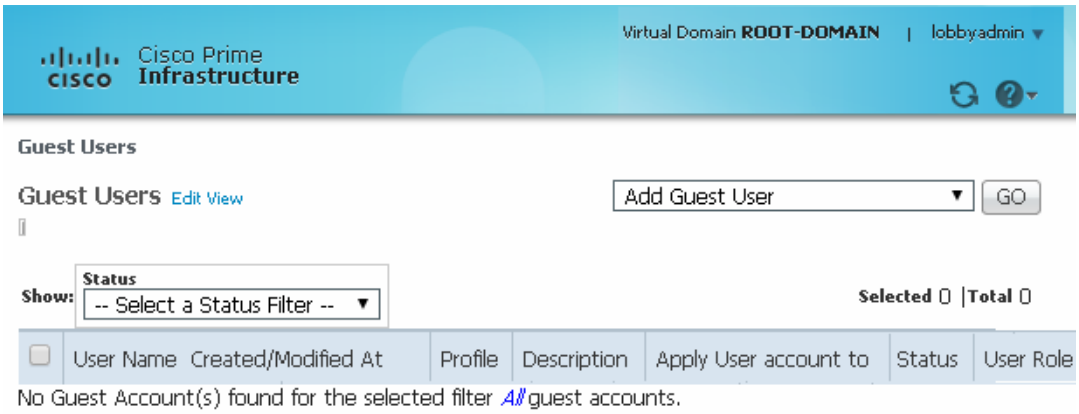
管理システムを使用したゲスト管理

次の設定例では、管理システム バージョン 2.2 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。

(注)　ゲスト テンプレートを作成する前に、個々の WLC 設定が管理システムと同期していることを確認してください。

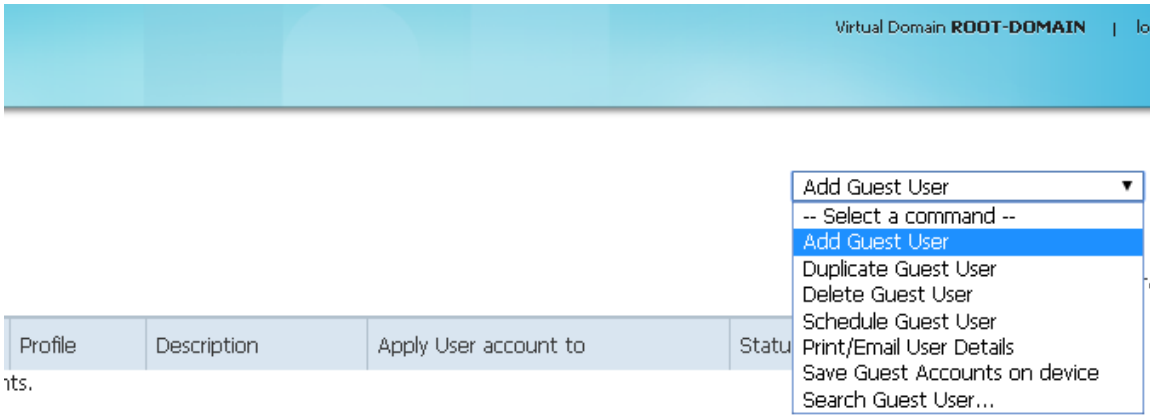
システム管理者が割り当てた Lobby Ambassador の資格情報を使用して管理システムにログインします（図 10-32 を参照）。

図 10-32　Lobby Ambassador



ログインすると、図 10-33 に示すような画面が表示されます。

図 10-33　　Cisco Prime Infrastructure のロビー管理者インターフェイス

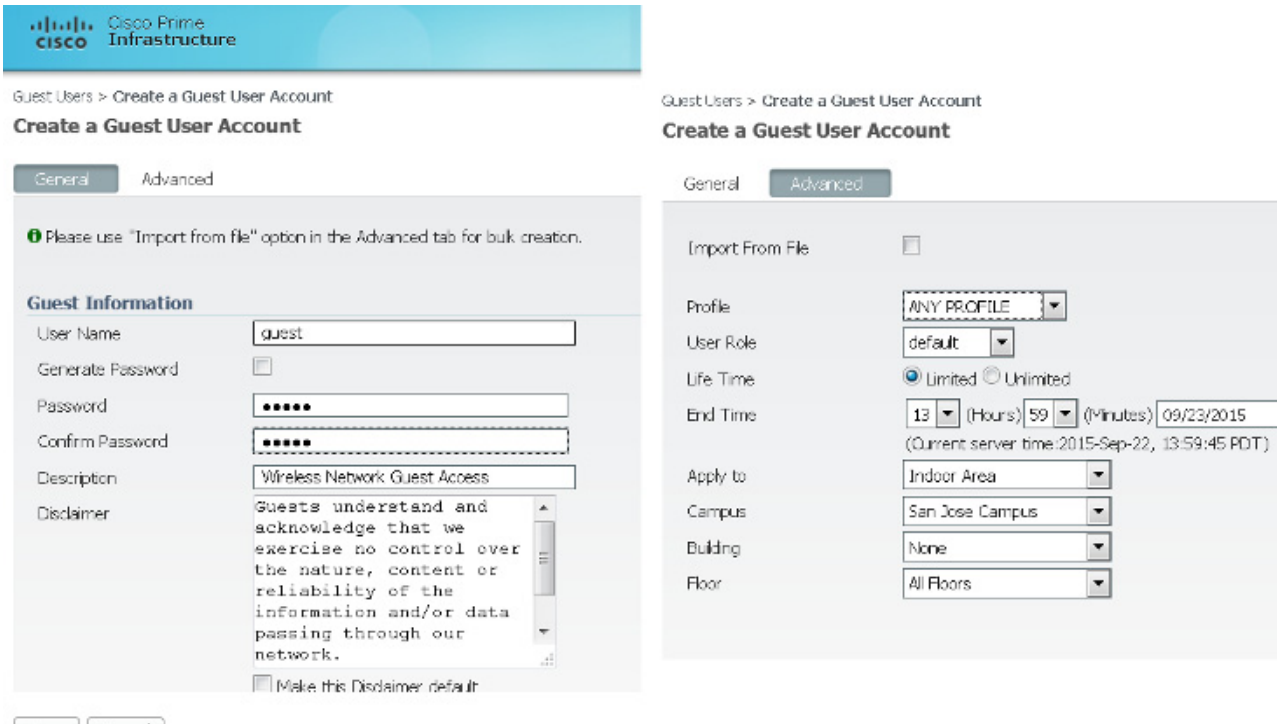


(注)　Cisco Prime Infrastructure は、正式には WCS および NCS と呼ばれていました。

ゲスト テンプレートには、次の 2 種類があります。

- [Add Guest User] 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。
- [Schedule Guest User] テンプレートを使用すると、管理者が将来の月、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作成できます(図 10-34 を参照)。

図 10-34　　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 10-35 に示すようなテンプレートが表示されます。

図 10-35　　ゲスト ユーザの追加テンプレート

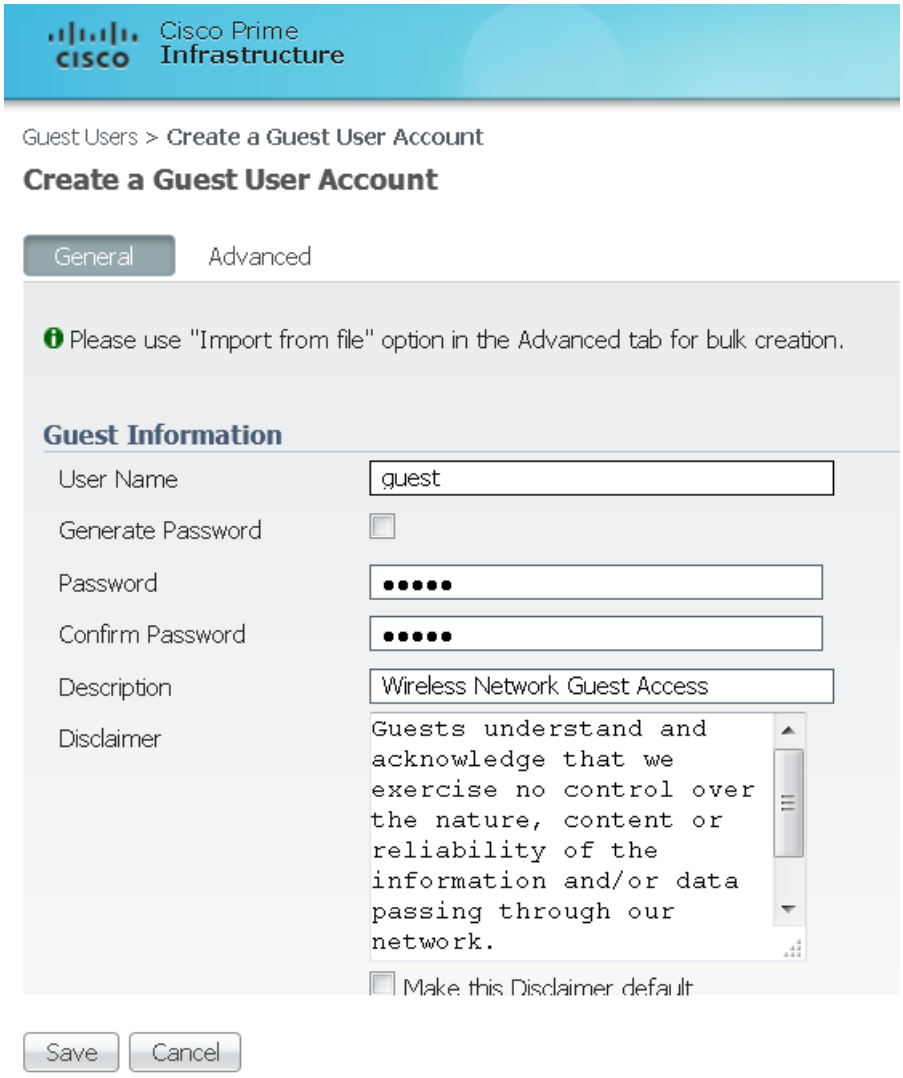
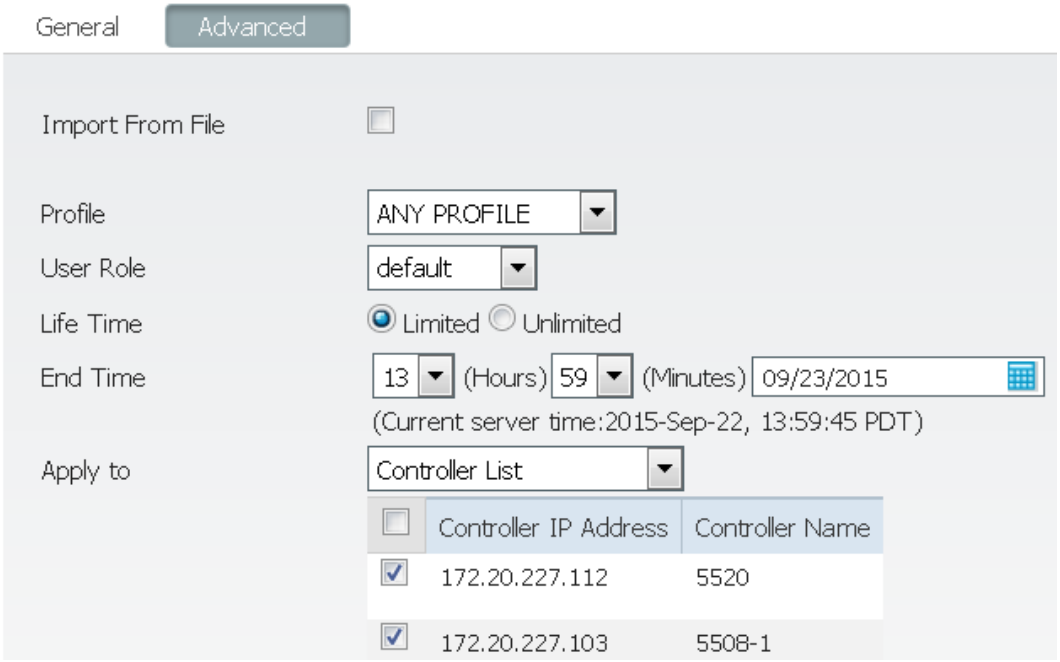


図 10-36 は、ゲスト ユーザ アカウント作成の例を示しています。

図 10-36　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オンにすることによって、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。

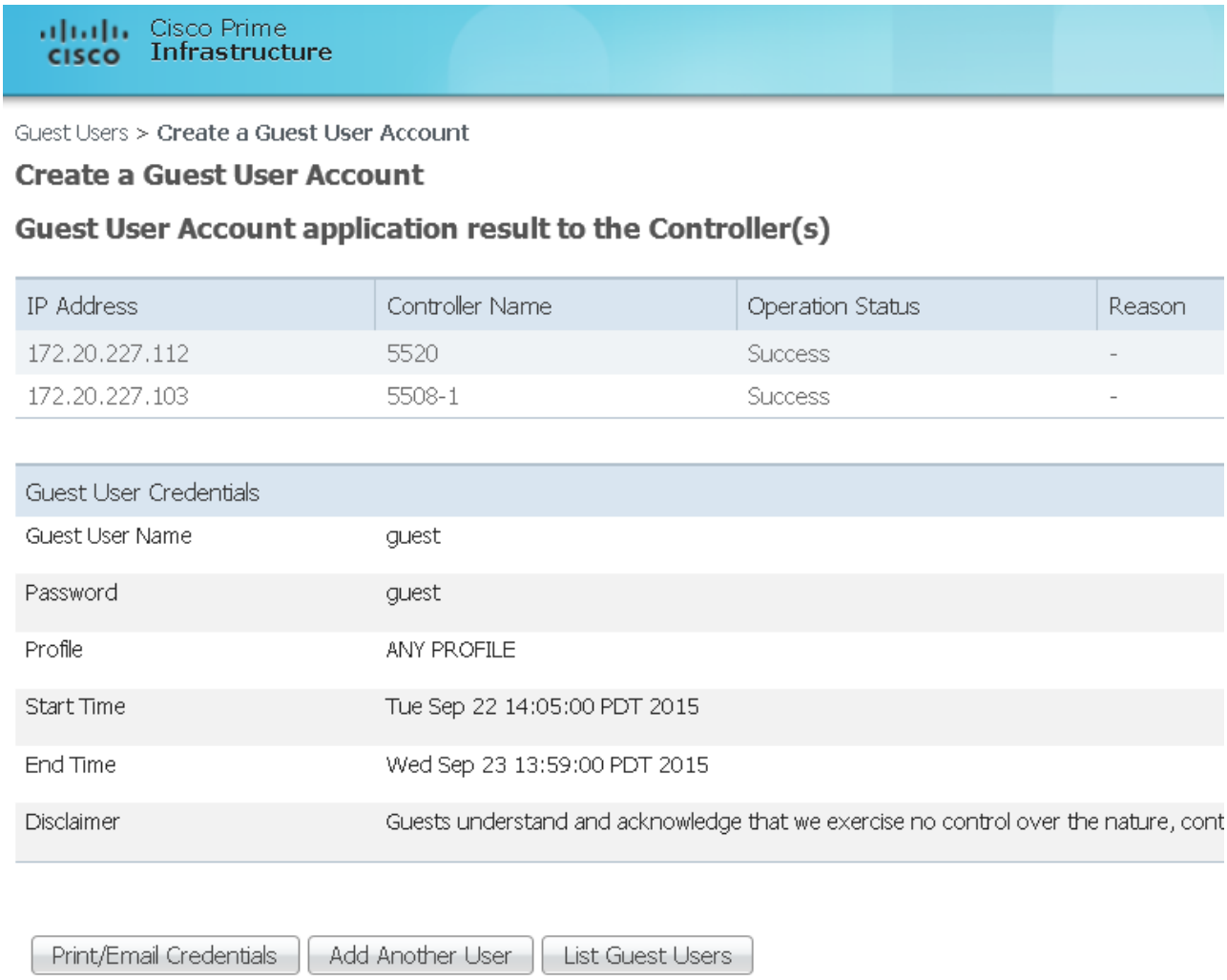
- [Profile]：プルダウン選択リストに、L3 Web ポリシーで設定された WLAN（SSID）のリストが表示されます。
- [User Role]：管理者により事前に定義され、ゲストのアクセス（契約者、顧客、パートナー、ベンダー、ビジターなど）に関連付けられています。
- [Life Time]：[limited] または [unlimited] を選択します。
- [End Time]：ゲスト アカウントが [Limited] の場合、資格情報の有効期限が切れる月、日、時刻を選択します。
- [Apply To]：プルダウン選択リストから [Controller List] を選択して、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オンにします。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 10-36 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 展開が管理システム 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電子メールにも含まれ、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電子メールで使用され、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。

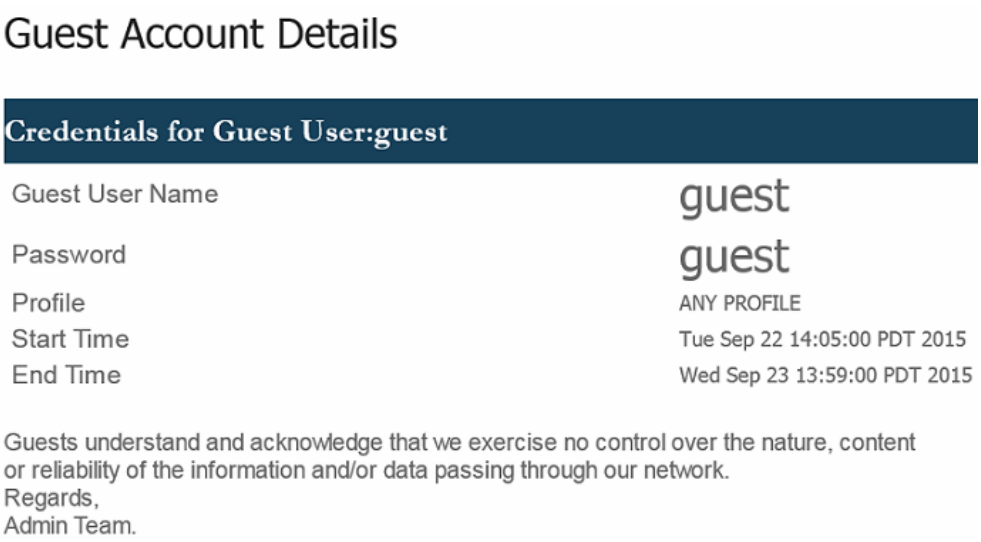
ステップ 5　設定が終わったら [Save] をクリックします。図 10-37 に示すサマリー画面が表示され、資格情報がアンカー コントローラに適用されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか電子メールで送信するオプションも表示されます。

図 10-37　　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 10-38 に示す画面が表示されます。

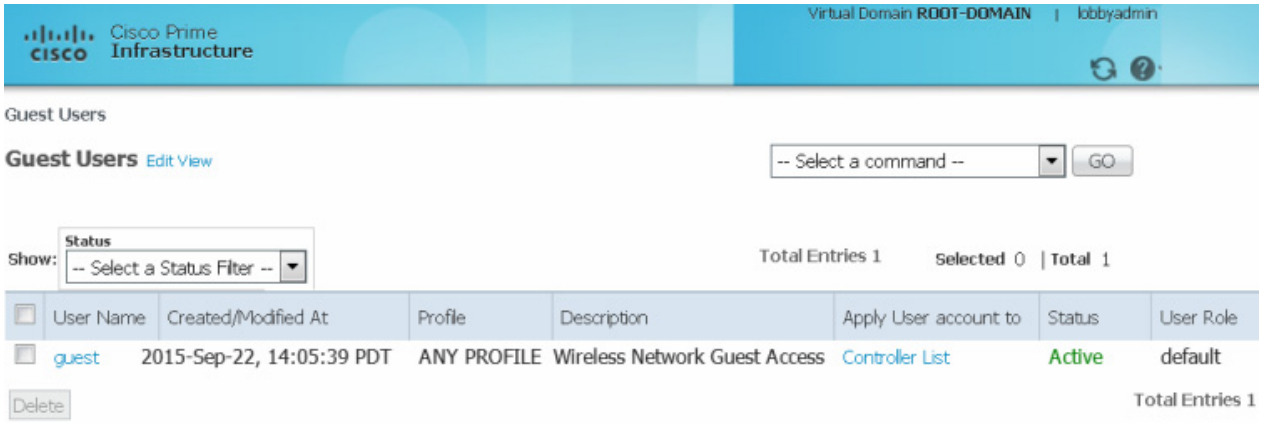
図 10-38　ゲスト ユーザ詳細の印刷または電子メールでの送信



(注)　ゲスト アカウント情報のユーザへの電子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、『Prime Infrastructure Configuration Guide』を参照してください。

アカウントの詳細を印刷または電子メールで送信すると、図 10-39 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 10-39　Cisco Prime Infrastructure ゲスト ユーザのサマリー



（注） ユーザがアクティブな状態で Cisco Prime Infrastructure 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については、『Prime Infrastructure Configuration Guide』を参照してください。

図 10-40 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。

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 10-41 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 テンプレート オプション

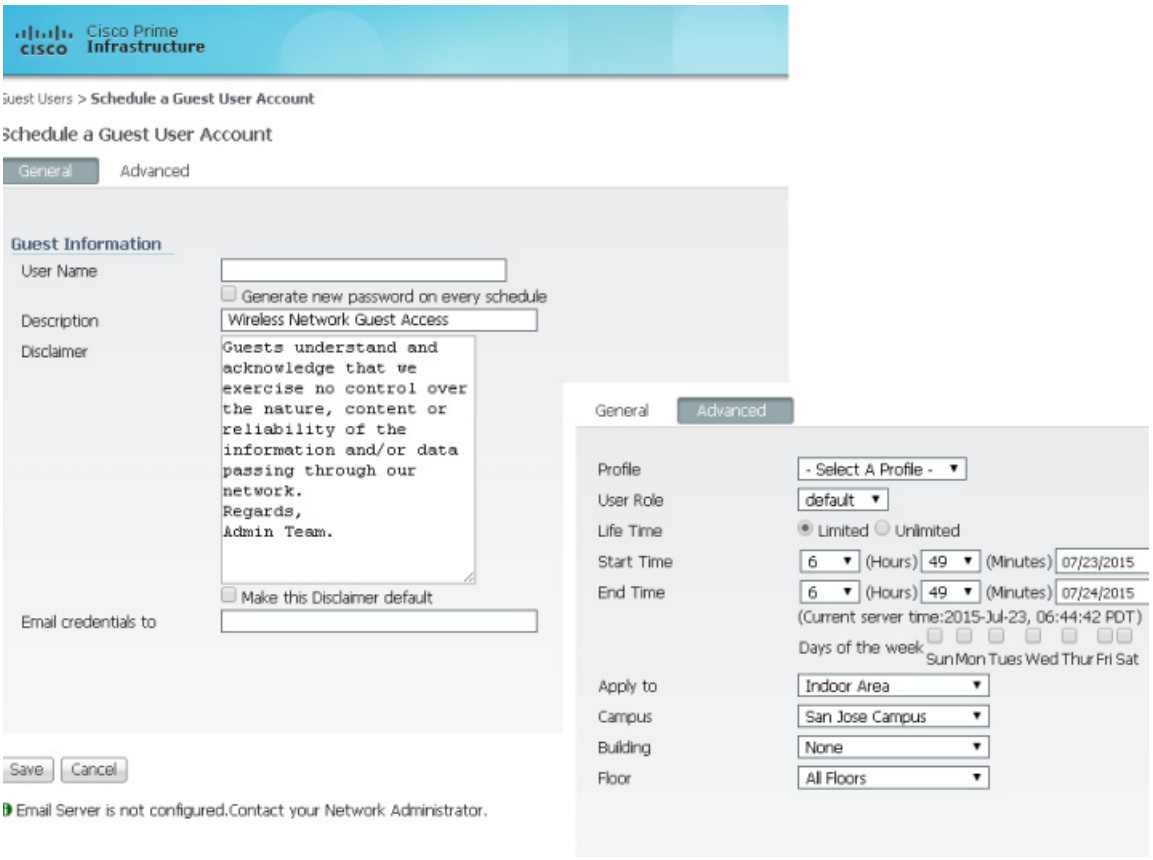


図 10-41　　ゲスト ユーザのスケジュール テンプレート

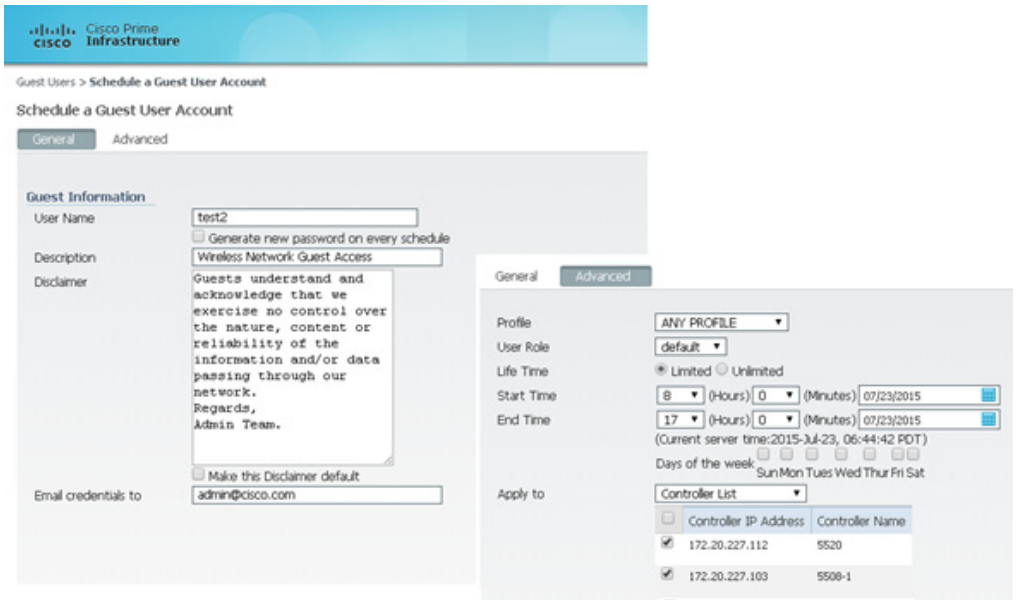
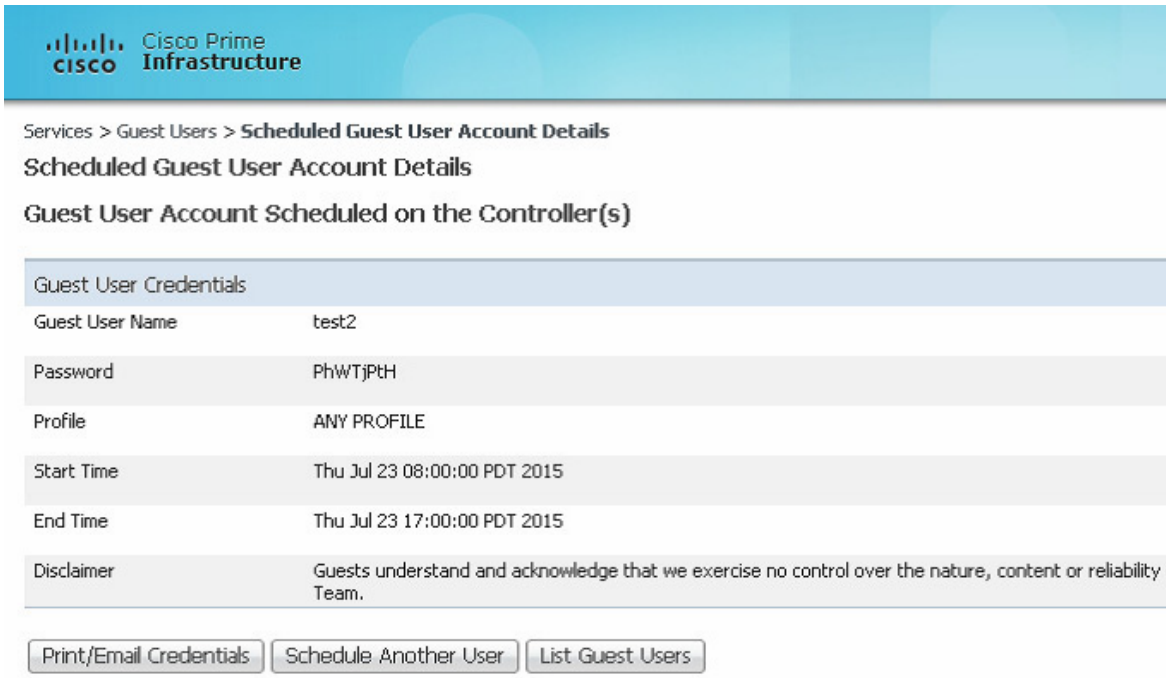


図 10-42 は、ゲスト ユーザ アカウントのスケジュールの作成例を示しています。

図 10-42　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な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 ポリシーで設定された WLAN（SSID）のリストが表示されます。
- [User Role]：管理者により事前に定義され、ゲストのアクセス（契約者、顧客、パートナー、ベンダー、ビジターなど）に関連付けられています。
- [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。開始日は、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、Cisco Prime Infrastructure 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、Cisco Prime Infrastructure 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 ユーザに電子メールで送信され、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オンにします。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 10-42 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 展開が管理システム 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。

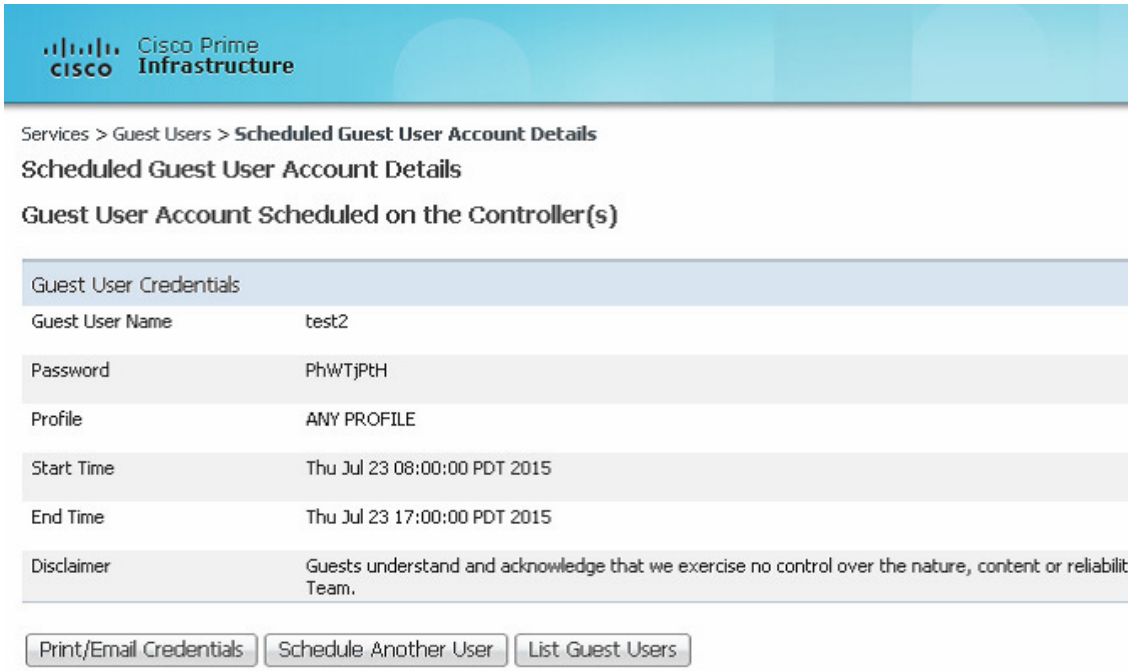
- [E-mail Credentials to]：アカウントを設定するユーザの電子メールアドレスを入力します。これは必須フィールドです。

（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、Cisco Prime Infrastructure で設定する必要があります。詳細については、『Cisco Wireless System Configuration Guide』を参照してください。

- [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電子メールにも含まれ、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電子メールで使用され、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。

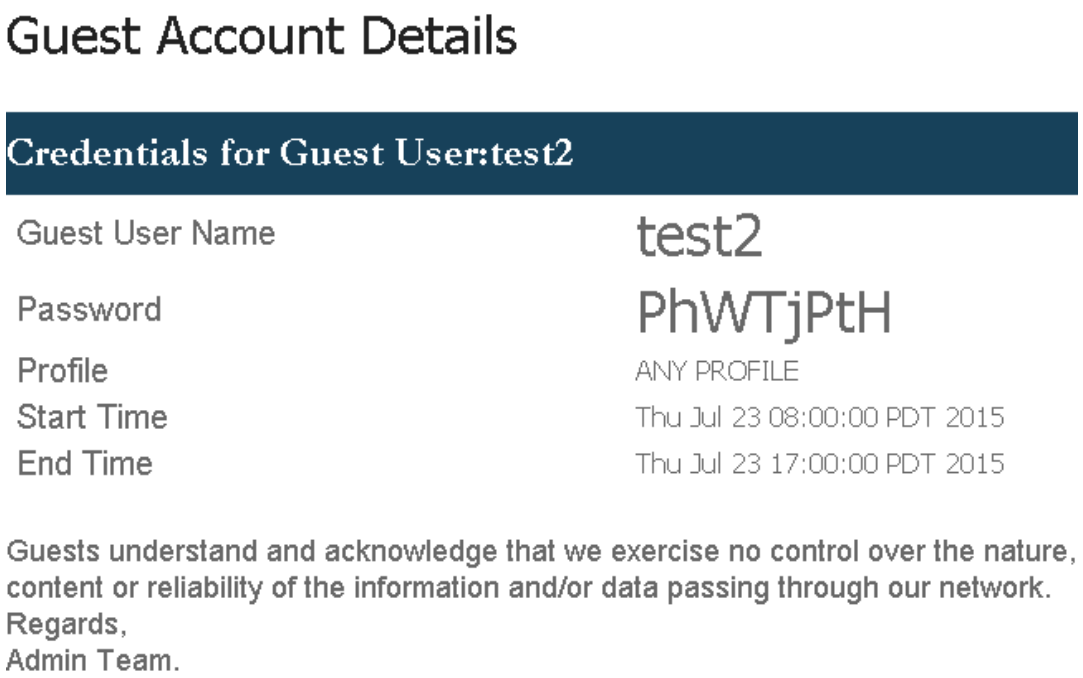
ステップ 4　設定が終わったら [Save] をクリックします。図 10-43 に示す画面が表示され、スケジュールされたアカウントが作成されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか電子メールで送信するオプションも表示されます。

図 10-43　　スケジュールされたアカウントの正常な作成



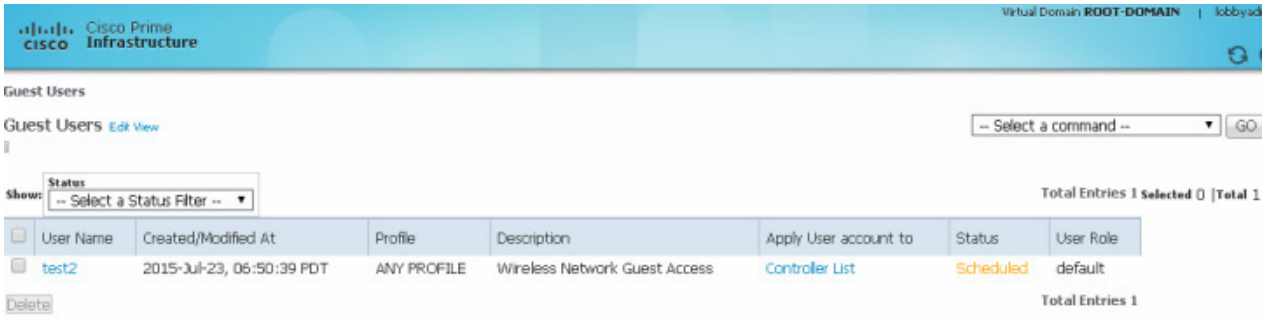
ステップ 5　必要に応じて、[Print/Email Guest User Credentials] をクリックします。図 10-44 に示す画面が表示されます。

図 10-44　　ゲスト ユーザ詳細の印刷または電子メールでの送信



アカウントの詳細を印刷または電子メールで送信すると、図 10-45 に示すようなサマリー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 10-45　Cisco Prime Infrastructure ゲスト ユーザのサマリー



(注)　ユーザがアクティブな状態で Cisco Prime Infrastructure 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、Cisco Prime Infrastructure 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。

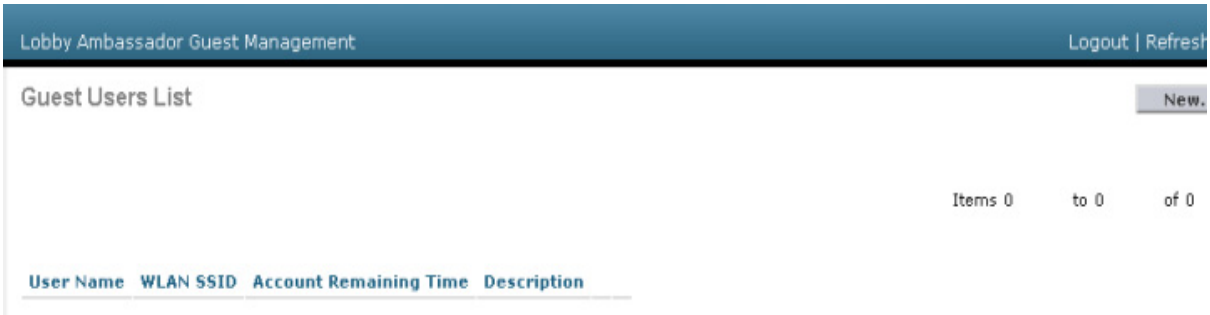
アンカー コントローラ上でのゲスト資格情報の直接管理

次の手順では、ネットワーク管理者が、ロビー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ロビー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」を参照してください。

ログインすると、図 10-46 に示すような画面が表示されます。

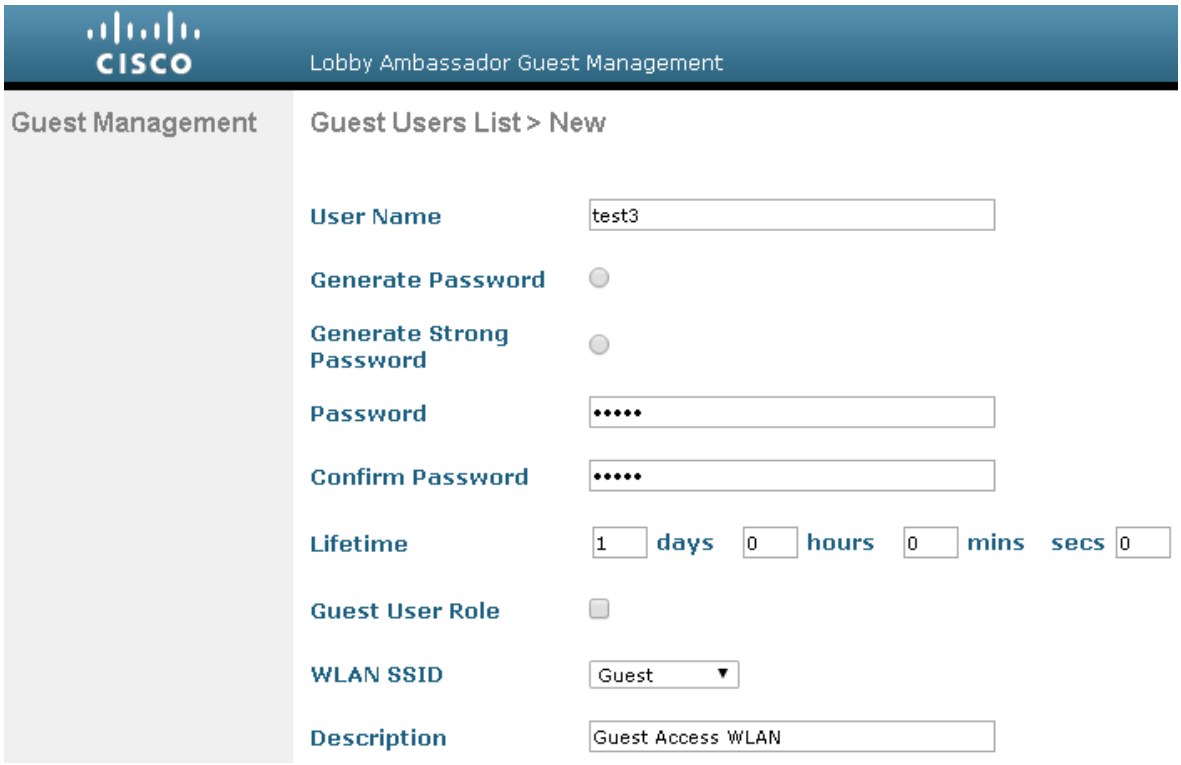
図 10-46　アンカー コントローラのログイン



ステップ 2　[New] をクリックします。

図 10-47 に示す画面が表示されます。

図 10-47　ローカル WLC ゲスト資格情報の作成



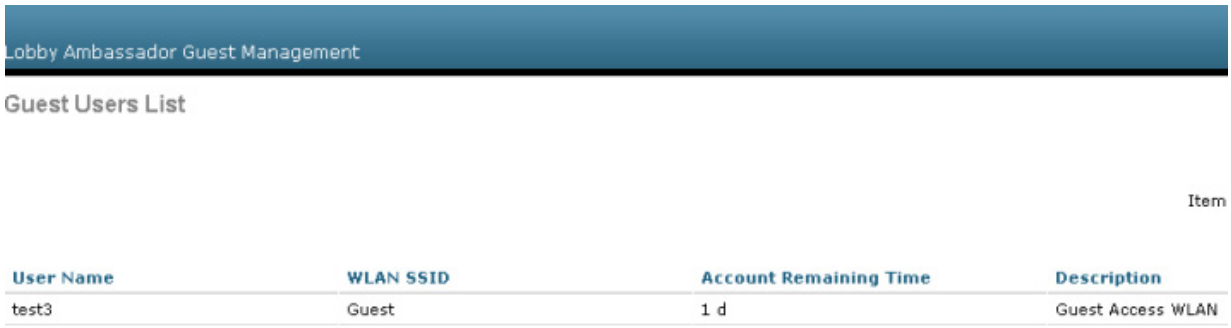
ステップ 3　ユーザ資格情報を作成するには、次の手順を実行します。

1. ユーザ名とパスワードを入力します（手動または自動）。
2. 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。
3. 資格情報の有効期間を入力します。
4. 必要に応じてユーザ ロールを入力します。
5. 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 10-48 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 10-48　　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。

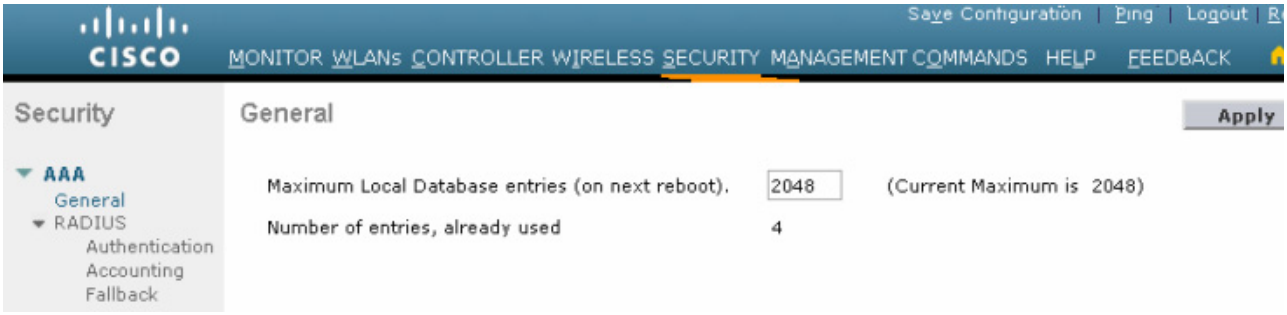
- 既存のユーザの編集（右端のリンク。非表示）
- 既存のユーザの削除（右端のリンク。非表示）
- 新規のユーザを追加します。

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 2048 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 10-49 を参照）。

図 10-49　　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（最大 2048）。

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を設定することができます。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 10-50 を参照）。

図 10-50　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）。

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

次の警告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。
- Cisco Prime Infrastructure の使用時に、コントローラの設定が最近 Cisco Prime Infrastructure と同期されていない場合、ロビー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 Cisco Prime Infrastructure のロビー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 Cisco Prime Infrastructure 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、Cisco Prime Infrastructure 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 Cisco Prime Infrastructure 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 トラフィックのフローが停止し、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。

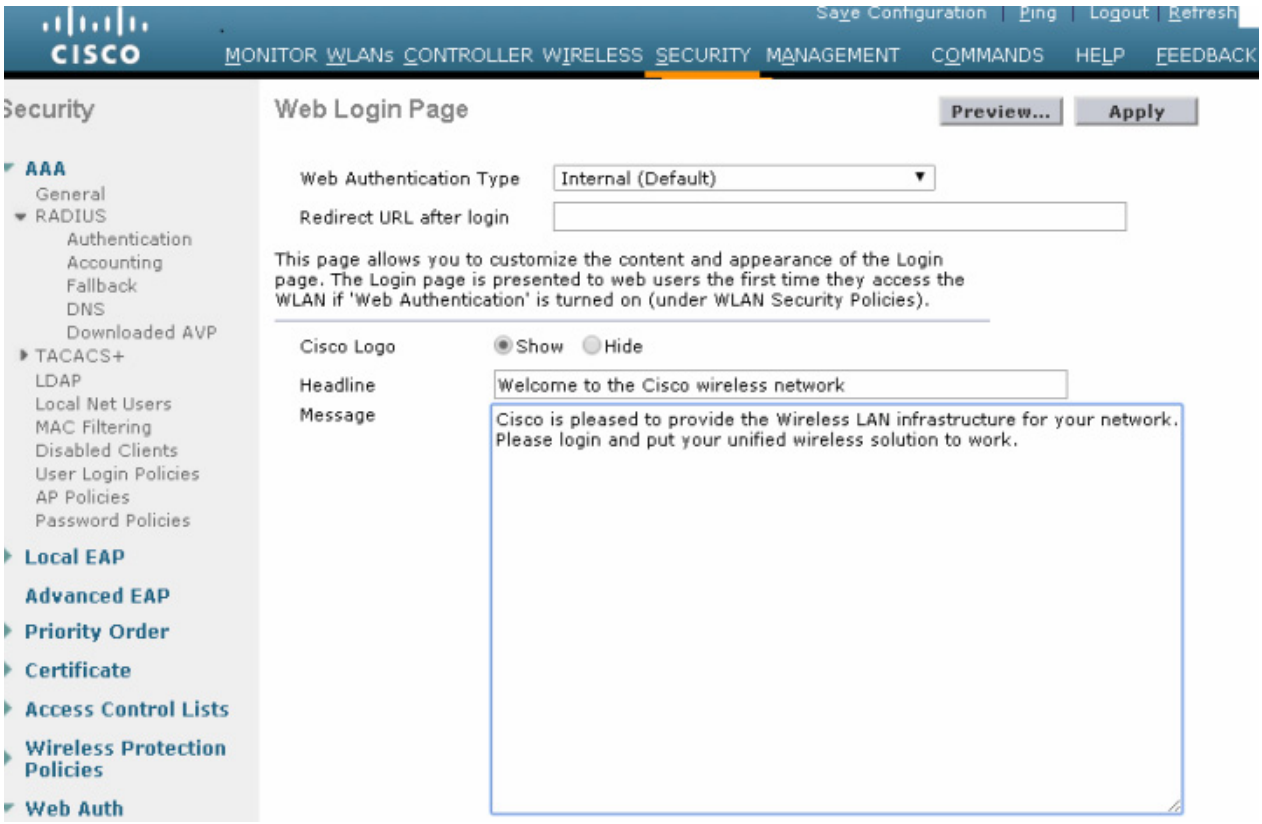
内部 Web ページの管理

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 10-51 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 10-51　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。

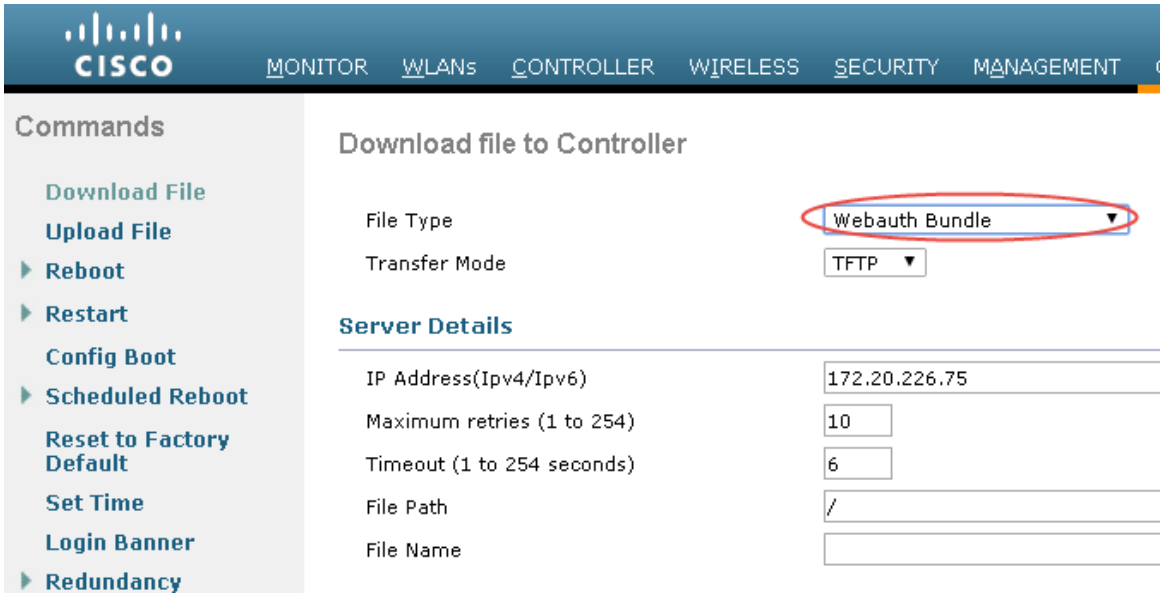
ステップ 4　必要に応じて、[Preview] をクリックして、ユーザに表示されるリダイレクト先のページを確認します。

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 10-52 を参照）。

図 10-52　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 Auth Bundle] は、カスタム Web ログイン ページに関連付けられている、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 Auth Bundle]（**.tar** ファイル）は、1 MB 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、『Cisco Wireless Controller Configuration Guide』を参照してください。

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。

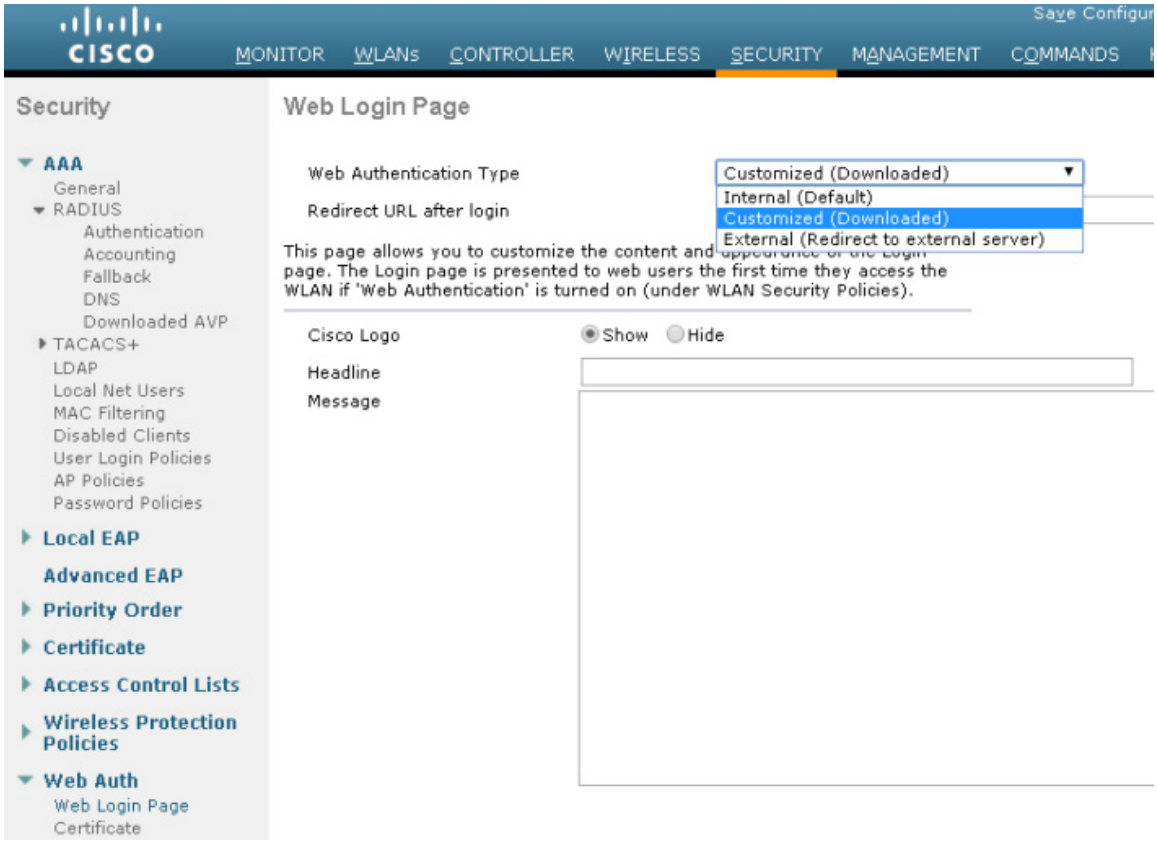
ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。

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 10-53 を参照）。

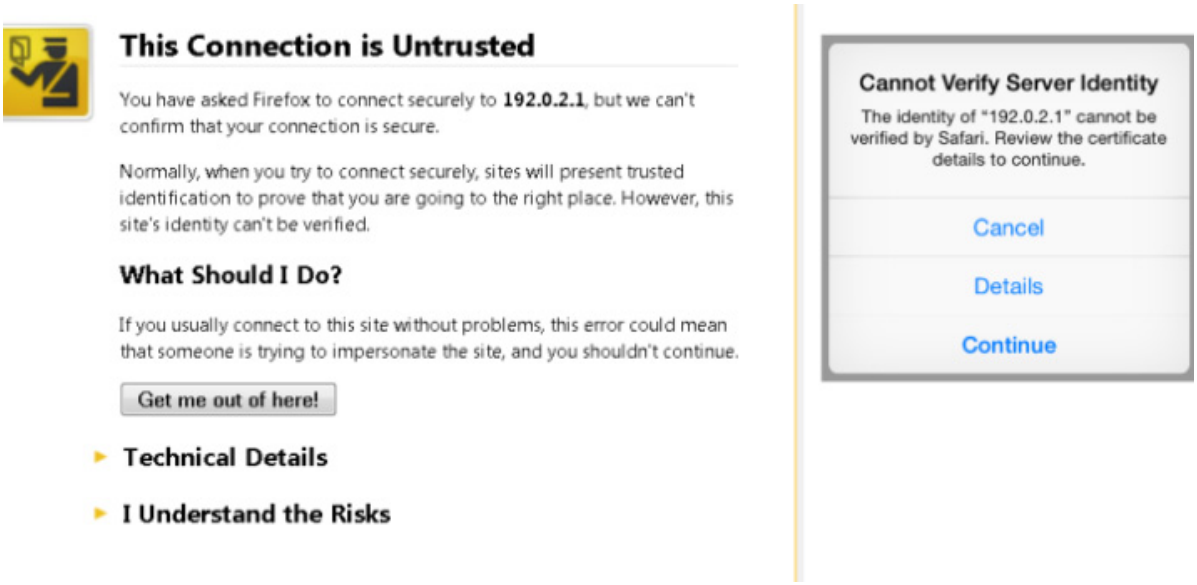
図 10-53　インポートした Web 認証ページの選択



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 10-54 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 10-54　Web 証明書セキュリティ アラート（Firefox 39.0 および Safari）



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」で設定された仮想インターフェイスの IP アドレスが発信元アドレスとして使用されます。ホスト名を IP アドレスとともに指定する場合は、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。

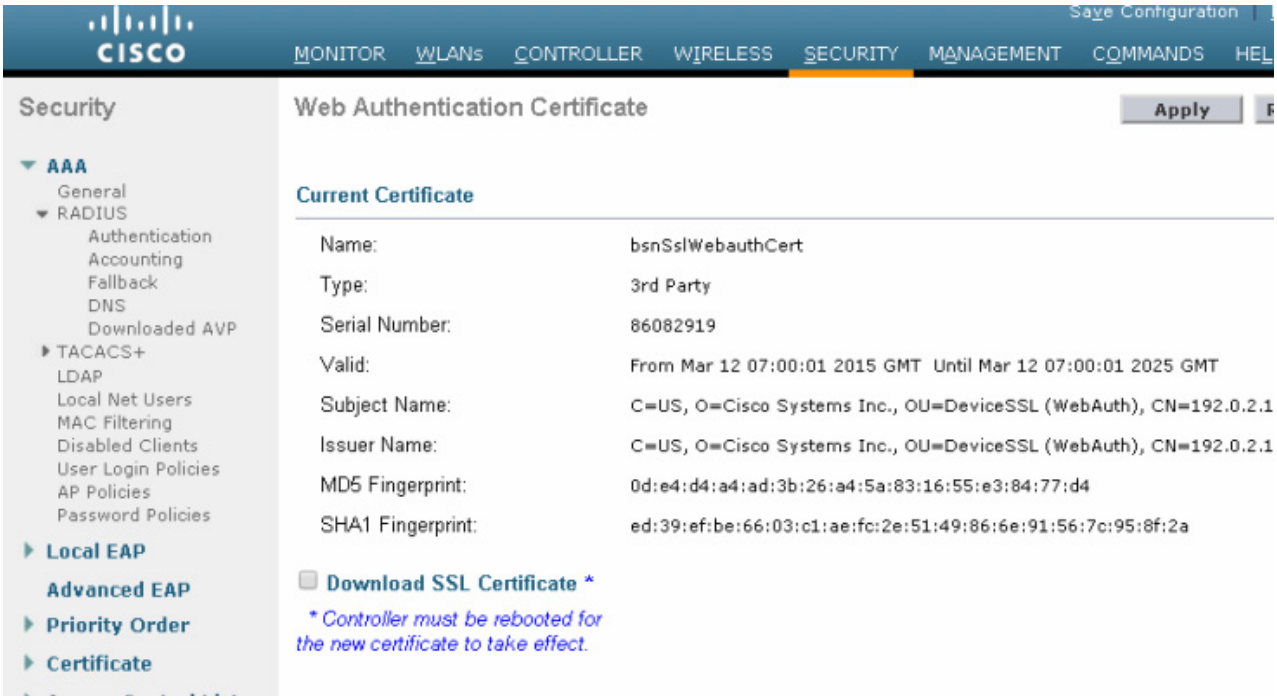
外部 Web 証明書のインポート

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 10-55 を参照）。

図 10-55　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。

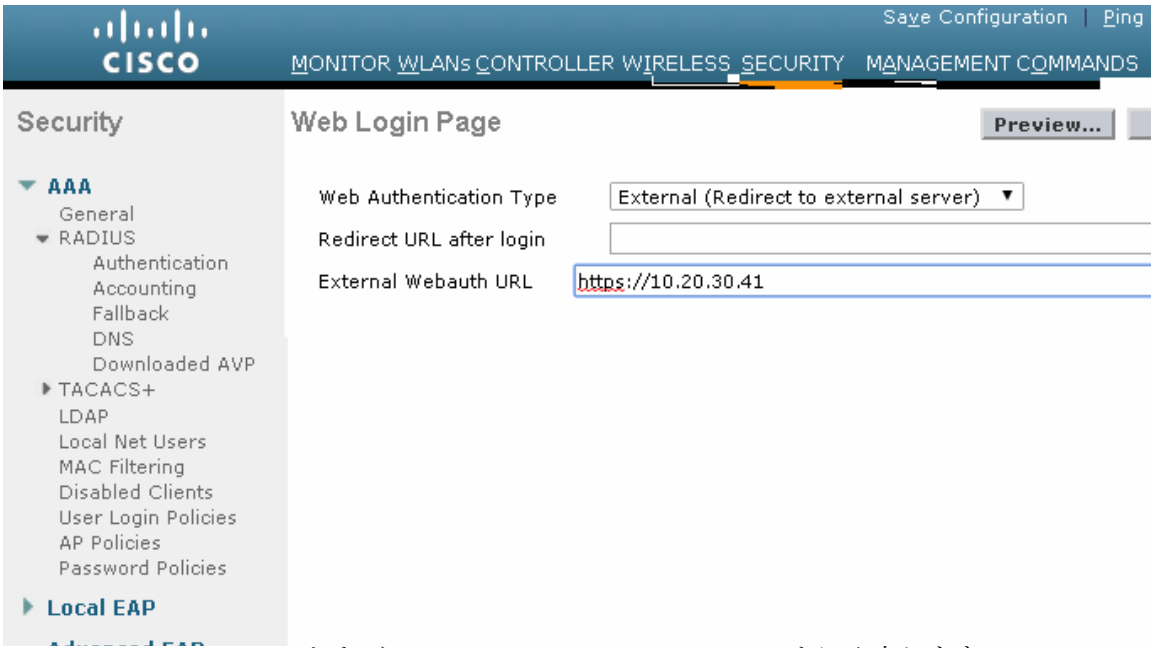
外部 Web リダイレクションのサポート

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 10-56 を参照）。

図 10-56　外部 Web リダイレクションのサポート



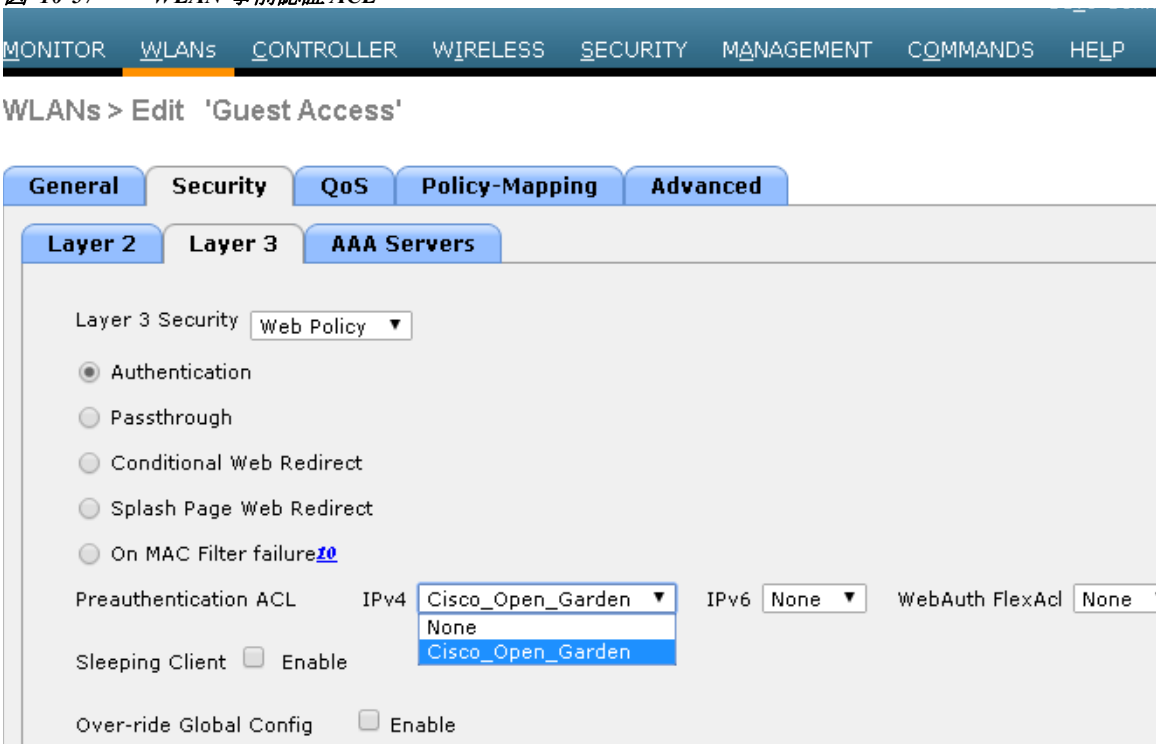
ステップ 3　[Redirect URL after login] および [External Webauth URL] フィールドに入力します。

ステップ 4　[Apply] をクリックします。

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 10-57 を参照）。

図 10-57　WLAN 事前認証 ACL

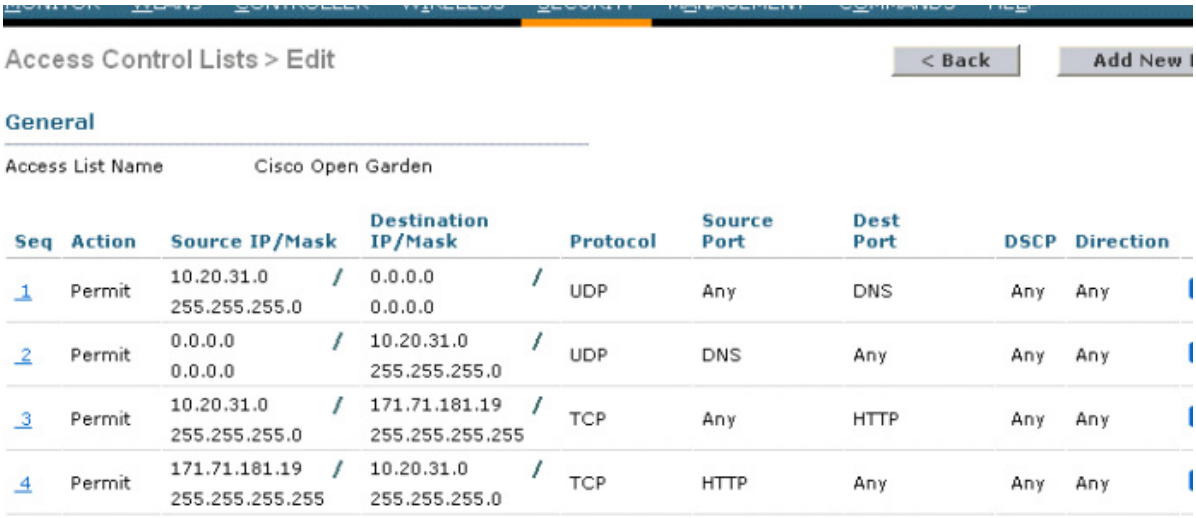


特定の ACL は、[Security] > [Access Control Lists] で設定されます（図 10-58 および図 10-59 を参照）。

図 10-58　WLC アクセス コントロール リスト

（注）　事前認証 ACL が Web 認証ポリシーとともに使用される場合、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。

図 10-59　事前認証 ACL の例



外部 RADIUS 認証

「ゲスト ユーザの認証」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」で説明したロビー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。

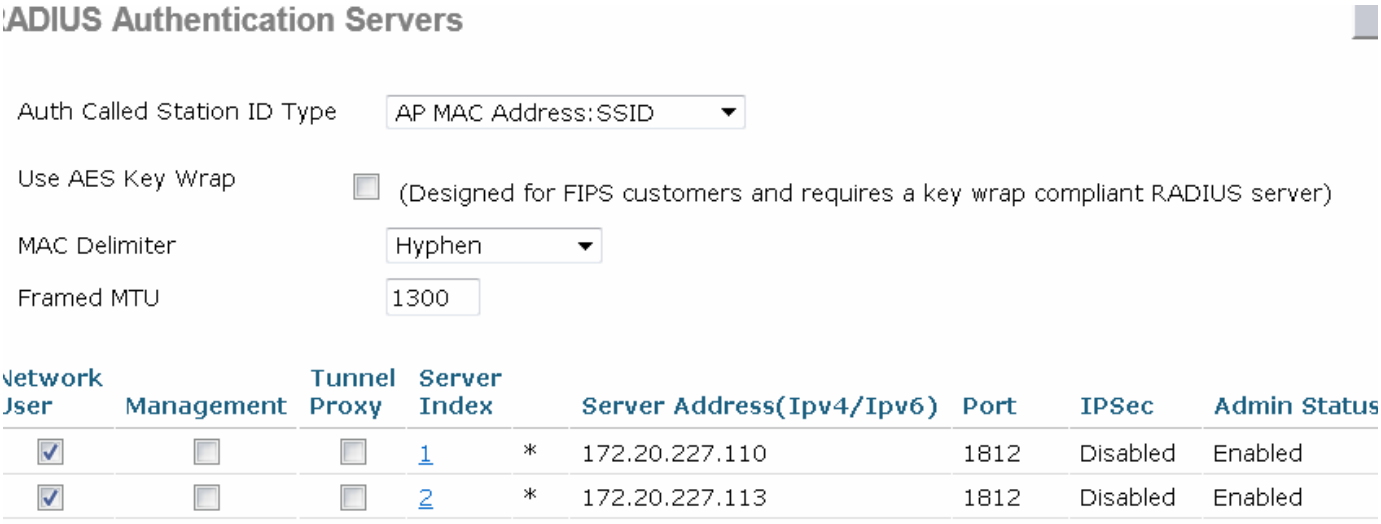
外部 RADIUS サーバを使用するようにゲスト WLAN を設定するには、アンカー コントローラ上で次の設定手順を実行します。

RADIUS サーバの追加

ステップ 1　[Security] タブをクリックします。

サマリー画面が表示されます（図 10-60 を参照）。

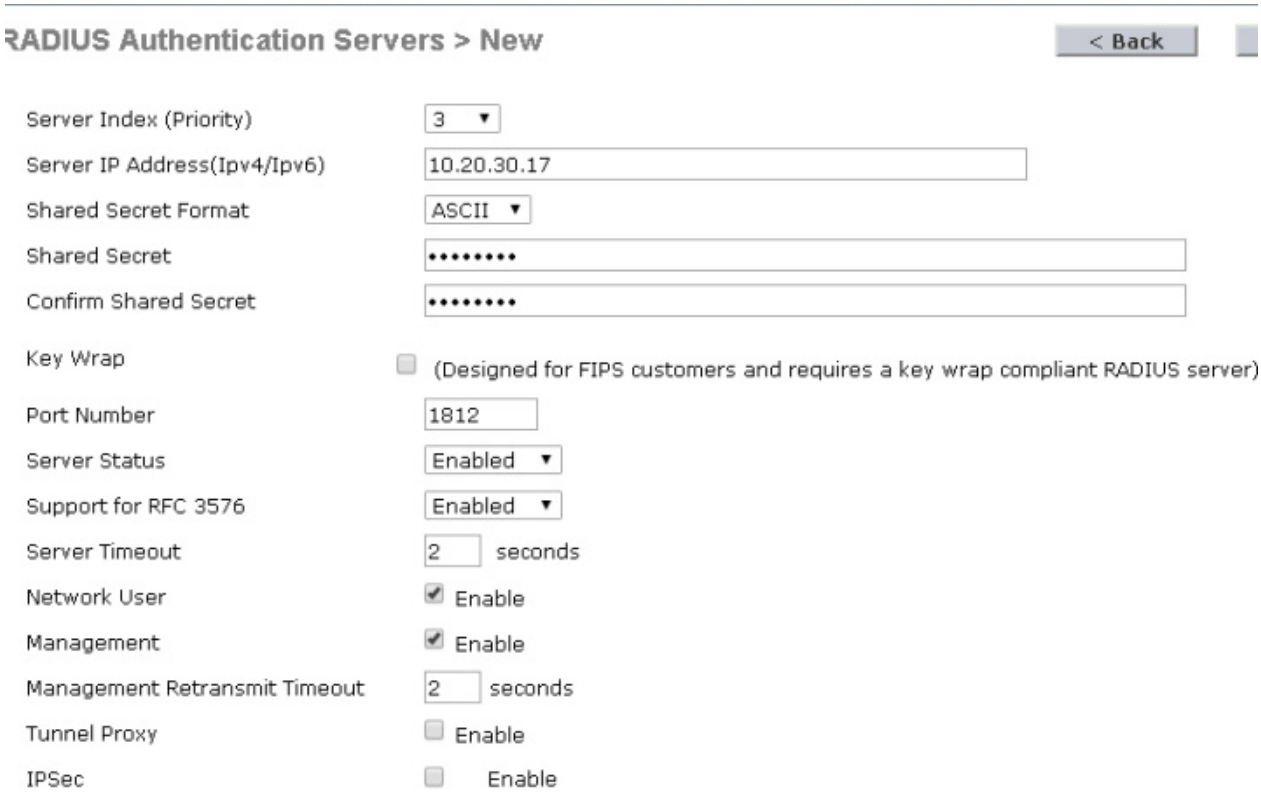
図 10-60　[Summary] 画面



ステップ 2　[New] をクリックします。

図 10-61 に示す画面が表示されます。

図 10-61　RADIUS サーバ設定の定義



ステップ 3　RADIUS サーバの設定を定義するには、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 10-62 に示すサマリー画面には、新しく追加されたサーバが表示されます。

図 10-62　[Summary] 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。

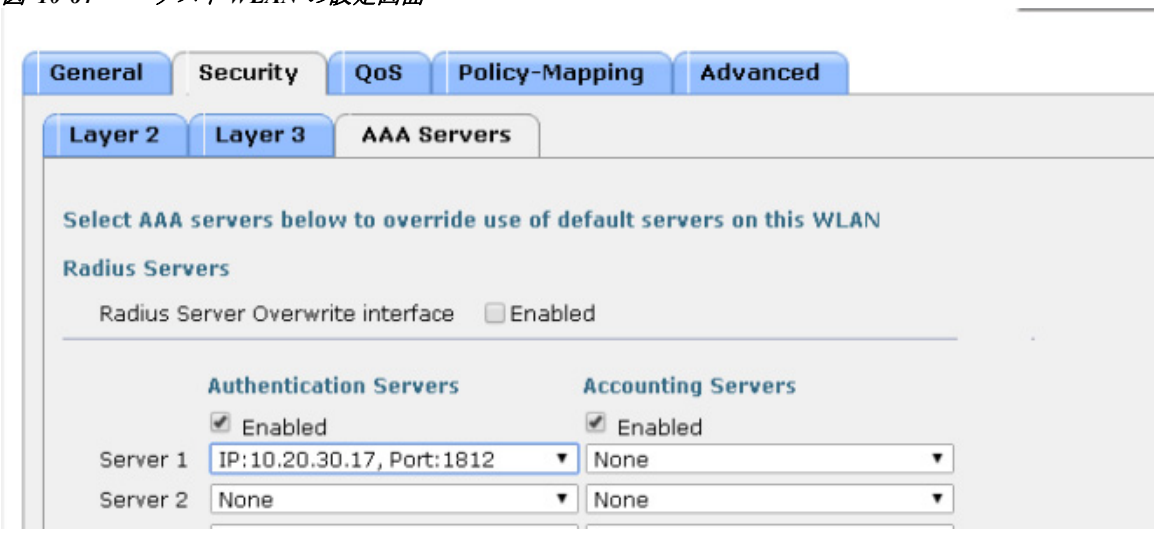
図 10-63 に示す画面が表示されます。

図 10-63　[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 10-64 に示すように、ゲスト WLAN の設定画面が表示されます。

図 10-64　　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。

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 への関連付けが可能。
- 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。

CMX ゲスト Wi-fi

CMX CONNECT & ENGAGE は、カスタマイズ可能なロケーション認識型のゲスト キャプティブ サービスです。このサービスを使用すると、カスタマイズされた直感的なオンボーディング エクスペリエンスを訪問者に提供できます。このサービスでは、次の 2 種類のオンボーディング エクスペリエンスを訪問者に提供できます。

カスタム ポータル:

- 施設の管理者が、カスタマイズしたブランディングおよび広告を使用してゲスト スプラッシュ ページを作成、ホストできます。
- OAuth 2.0 を使用した Facebook、Instagram、Foursquare とのソーシャル ネットワーク認証を提供します。
- OAuth 2.0 ユーザ ソーシャル情報を収集します。

Facebook Wi-Fi:

- 施設の管理者が施設の Facebook ページを、ビジターを対象とした無料 Wi-Fi ホットスポットとして利用できます。
- ビジターは、施設の Facebook ページにアクセスした後で、無料 Wi-Fi にアクセスできます。
- デモグラフィック レポートから施設のカスタマー ベースを把握できます。

Cisco CMX Connect サービスの新機能の一覧については、次の URL にある Cisco CMX ポータルを参照してください。
https://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html#~stickynav=1

CMX Connect

CMX Connect は、オンプレミスまたはクラウド ベースのソリューションとして使用できます。CMX Connect サービスを使用すれば、簡単にカスタマイズ可能なキャプティブ ポータルを作成したり、複数のオンボーディング オプションを通じて訪問者情報を収集したりすることができます。組織は、キャプティブ ポータル上で、またはモバイル アプリケーション、デジタル サイネージ、オフライン マーケティングなどの外部メディアを介して訪問者と関わり合うことができます。

包括的な導入ガイドについては、次の URL を参照してください。

https://support.cmxcisco.com/hc/en-us/articles/216598448-Set-Up-Cisco-CMX-Connect

ゲスト ユーザの管理(クライアントのホワイトリスト化)

ロビー アンバサダーの MAC フィルタリング機能の目的は、ゲスト ユーザ管理でワイヤレス LAN コントローラ上のクライアントのホワイトリスト化を行えるようにすることです。

この機能を使用すると、特定の WLAN SSID でクライアントをホワイトリスト化できます。最終目標は、特定の WLAN にアクセスできるクライアントを制御することです。この機能では、WLAN の MAC フィルタリング オプション、ロビー管理者ユーザの追加、WLAN でホワイトリスト化されたクライアントのリストを保存するための AAA データベースの再利用などの既存の機能を使用します。

ワーク フロー

この機能のシーケンスは次のとおりです。

1. グローバル管理者が WLC にロビー管理者のユーザ アカウントを追加します。
2. グローバル管理者が WLC 上の必要な WLAN でロビー管理者のアクセスを有効にします。
3. ロビー管理者が WLC 上のゲスト管理ページにログインします。
4. ロビー管理者が、クライアントのホワイトリスト化を有効にする必要がある(ロビー管理者がアクセスできる)WLAN を選択します。
5. ロビー管理者が WLAN の MAC フィルタリングを無効にします。
6. ロビー管理者に、現在接続しているクライアントのリストと選択した WLAN ですでに追加されている(ホワイトリスト化されている)クライアントが表示されます。

7. ロビー管理者が、アソシエートしているクライアントのリストからすべてのクライアントを選択するか、使用可能なフィルタリング オプションに基づいて特定のクライアントを選択します。
8. ロビー管理者が必須クライアントまたはすべてのクライアントをホワイトリスト バケットに追加します。
9. ロビー管理者が WLAN の MAC フィルタリングを有効にします。

読み取り/書き込み管理者とロビー管理者のロールは、次の順序で分類されます。

管理者特権を持つユーザ

- 読み取り/書き込みアクセス権を持つ管理者ユーザは、WLC にローカル管理者(ロビー管理者)を作成します。
- 読み取り/書き込み管理者は、クライアントのホワイトリスト化を有効にする選択済みの WLAN でロビー管理者アクセスを設定する必要もあります。

ユーザ ロビー管理者ロール

- WLC のゲスト ユーザ Web ページにログインします。
- ロビー管理者アクセスが有効になっている WLAN/SSID のリストとその WLAN/SSID に接続しているすべてのクライアントのリストを表示します。
- 選択した WLAN で MAC フィルタリング オプションを有効にするためのアクセス権を付与します。
- ホワイトリストにクライアント MAC アドレスを追加/削除するためのアクセス権を付与します。

802.11r、802.11k、802.11v、802.11w Fast Transition ローミング

802.11r Fast Transition ローミング

802.11r Fast Transition（FT）ローミングは、802.11 IEEE 標準の改訂版であり、ローミングの新しい概念です。Fast Transition（FT）と呼ばれるこの高速ローミングでは、クライアントがターゲット アクセス ポイント（AP）にローミングする前に、まず新規 AP との初期ハンドシェイクが行われます。

初期ハンドシェイクによって、クライアントと AP が事前にペアワイズ マスター キー（PTK）を計算できるようになります。クライアントが新規 AP に対して再アソシエーション要求または応答の交換を行うと、PMK キーがクライアントおよび AP に適用されます。FT キー階層により、クライアントは AP ごとに再認証を実行することなく、AP 間の Base Station Subsystem（BSS）を高速に移動できます。802.11r（FT）は、ローミングの際のハンドシェイクに伴うオーバーヘッドを排除することにより、AP 間のハンドオフ時間を短縮するとともに、セキュリティと QoS を確保します。FT は、Wi-Fi での音声やビデオのような、遅延の影響を受けやすいアプリケーションを実行するクライアント デバイスで役立ちます。

クライアント ローミングの方法

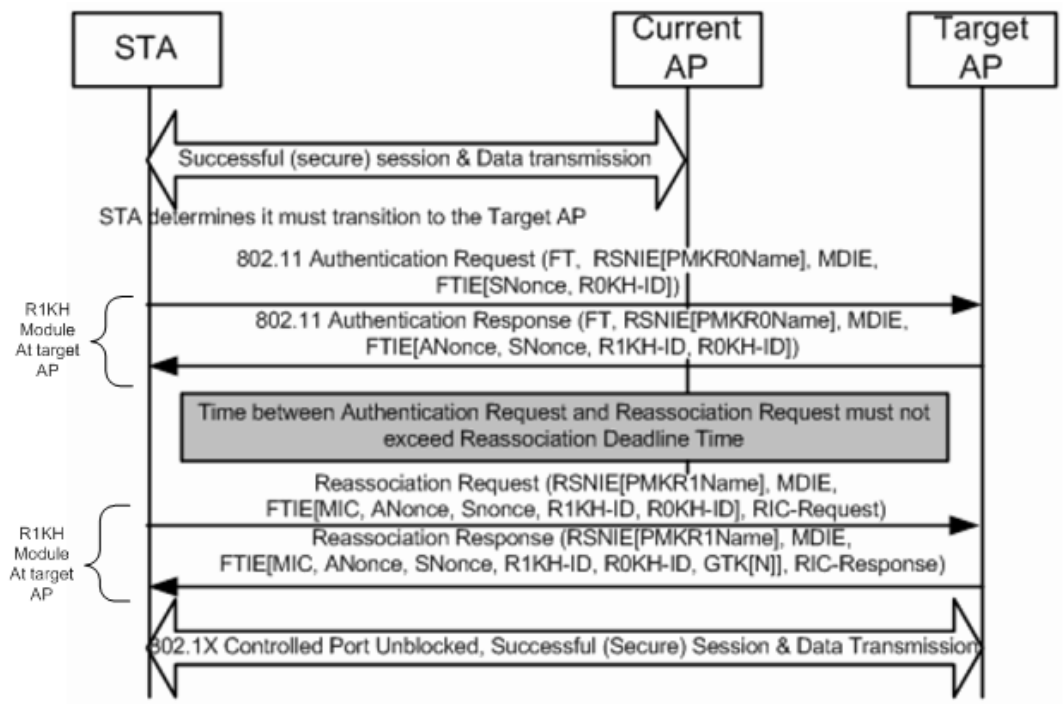
FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の方法のいずれかを使用して行われます。

- Over-the-Air FT ローミング
- Over-the-DS（分散システム）FT ローミング

Over-the-Air Fast Transition ローミング

クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。

図 11-1　RSN での Over-the-Air 高速 BSS 移行



コントローラ内の Over-the-Air ローミング

同一のコントローラに接続されている AP1 および AP2 間をローミングするクライアントは、デフォルトで次の動作を行います。

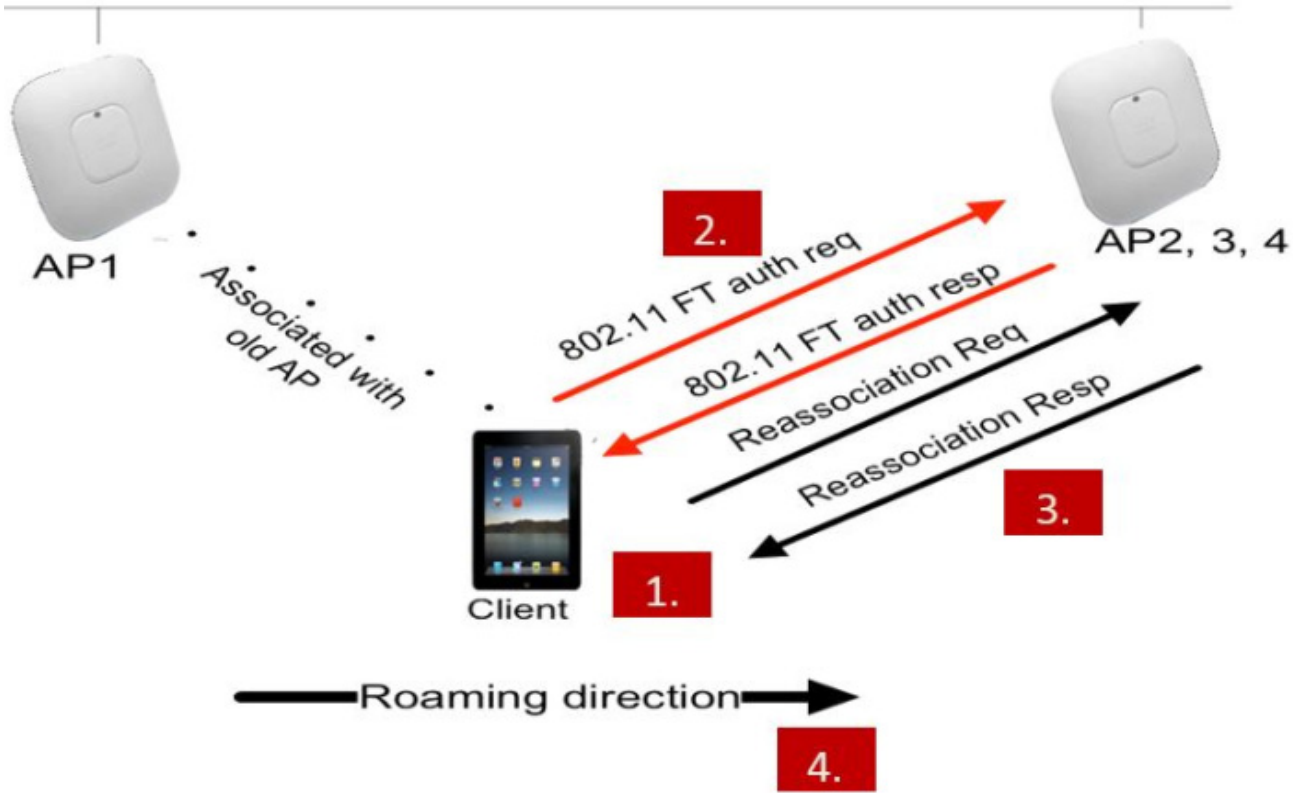
ステップ 1　クライアントは AP1 にアソシエートし、AP2 へのローミングを要求します。

ステップ 2　クライアントが AP2 に対して FT 認証要求を送信し、AP2 から FT 認証応答を受信します。

ステップ 3　クライアントが AP2 に対して FT 再アソシエーション要求を送信し、AP2 から FT 再アソシエーション応答を受信します。

ステップ 4　クライアントは AP1 から AP2 へのローミングを完了します。

図 11-2　　コントローラ内の Over-the-Air ローミング



コントローラ間の Over-the-Air ローミング

WLC1 と WLC2 など、同一モビリティ グループ内の異なるコントローラに接続されている AP1 および AP2 間をローミングするクライアントは、デフォルトで次の動作を行います。

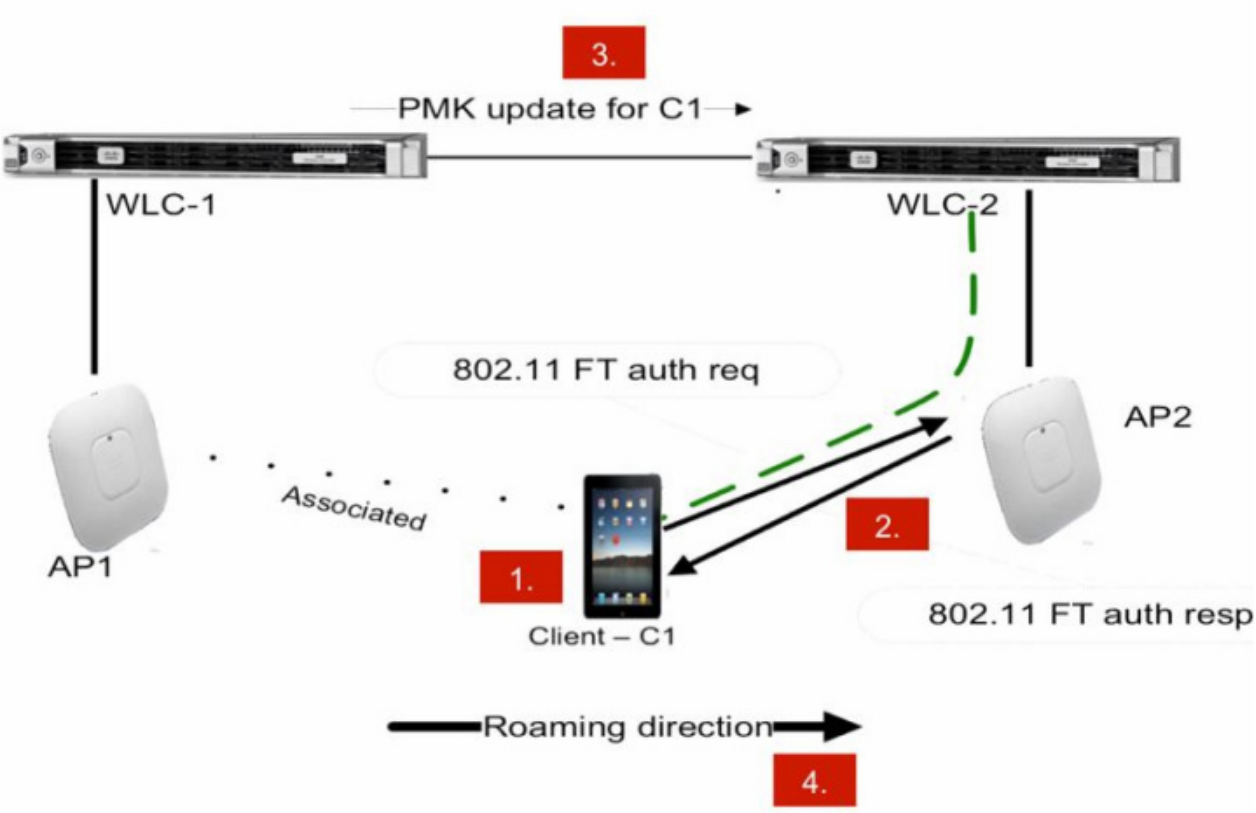
ステップ 1　クライアントは AP1 にアソシエートし、AP2 へのローミングを要求します。

ステップ 2　クライアントが AP2 に対して FT 認証要求を送信し、AP2 から FT 認証応答を受信します。

ステップ 3　WLC-1 は WLC-2 に対し、モビリティ インフラストラクチャを使用するローミング クライアントに関する PMK およびモビリティ メッセージを送信します。

ステップ 4　クライアントは AP1 から AP2 へのローミングを完了します。

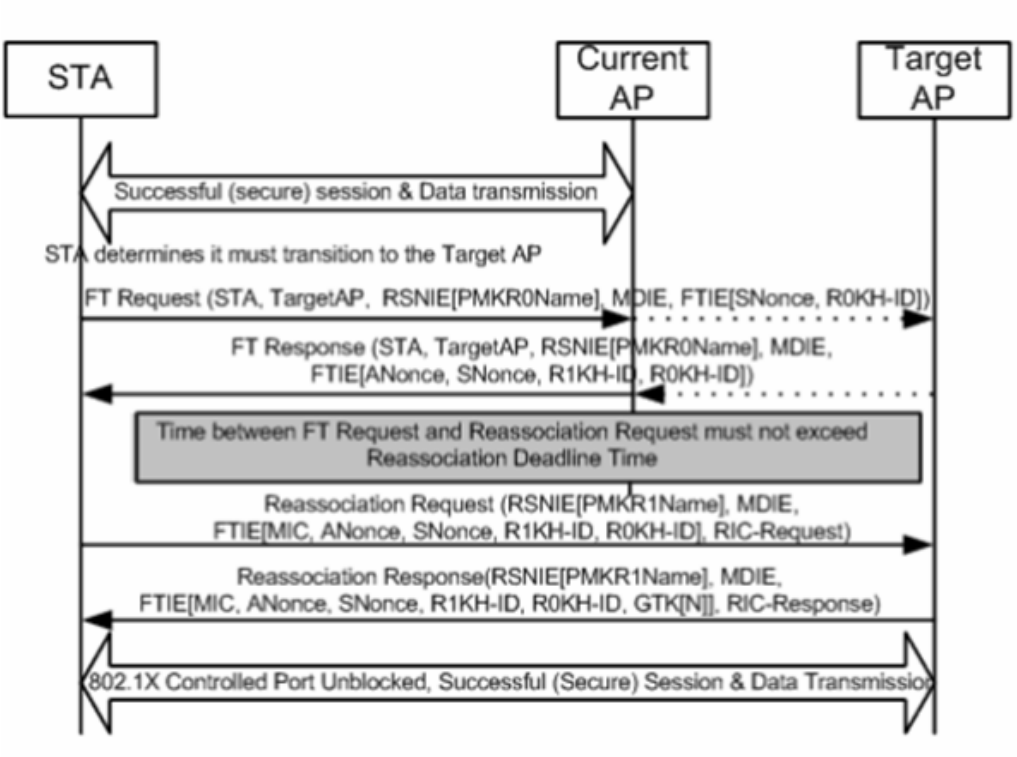
図 11-3　コントローラ間の Over-the-Air ローミング



Over-the-DS（分散システム）Fast Transition ローミング

DS（分散システム）上をローミングするクライアントは、現在の AP を介してターゲット AP と通信します。この通信はコントローラを介し、FT アクション フレームを使用して、クライアントと現在の AP 間を送信されます。

図 11-4　Over the DS ローミング



コントローラ内の Over-the-DS ローミング

同一のコントローラに接続されている AP1 および AP2 間をローミングするクライアントは、デフォルトで次の動作を行います。

ステップ 1　クライアントは AP1 にアソシエートし、AP2 へのローミングを要求します。

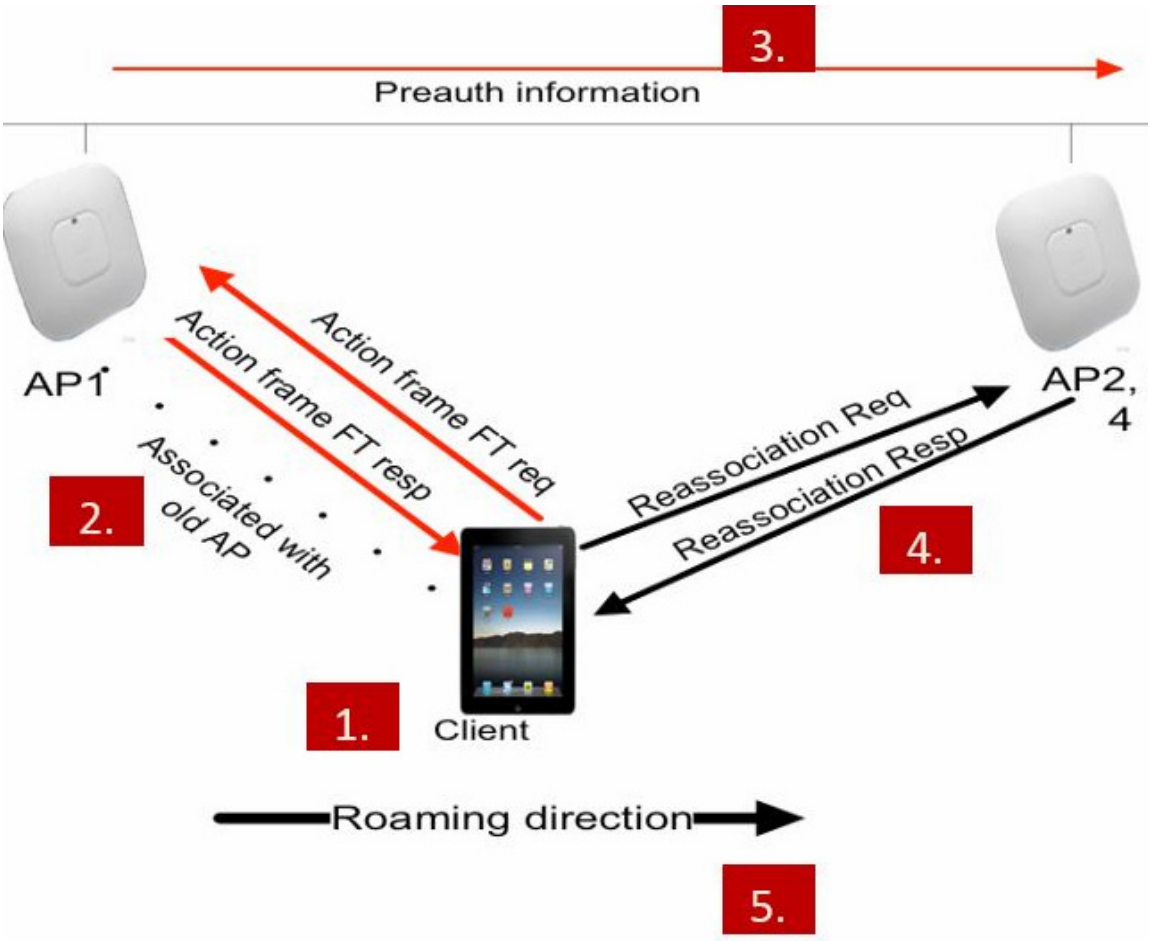
ステップ 2　クライアントが AP1 に対して FT 認証要求を送信し、AP1 から FT 認証応答を受信します。

ステップ 3　両方の AP は同一のコントローラに接続されているため、コントローラは AP2 に事前認証情報を送信します。

ステップ 4　クライアントが AP2 に対して FT 再アソシエーション要求を送信し、AP2 から FT 再アソシエーション応答を受信します。

ステップ 5　クライアントは AP1 から AP2 へのローミングを完了します。

図 11-5　コントローラ内の Over-the-DS ローミング



コントローラ間の Over-the-DS ローミング

WLC1 と WLC2 など、同一モビリティ グループ内の異なるコントローラにそれぞれ接続されている AP1 および AP2 間をローミングするクライアントは、デフォルトで次の動作を行います。

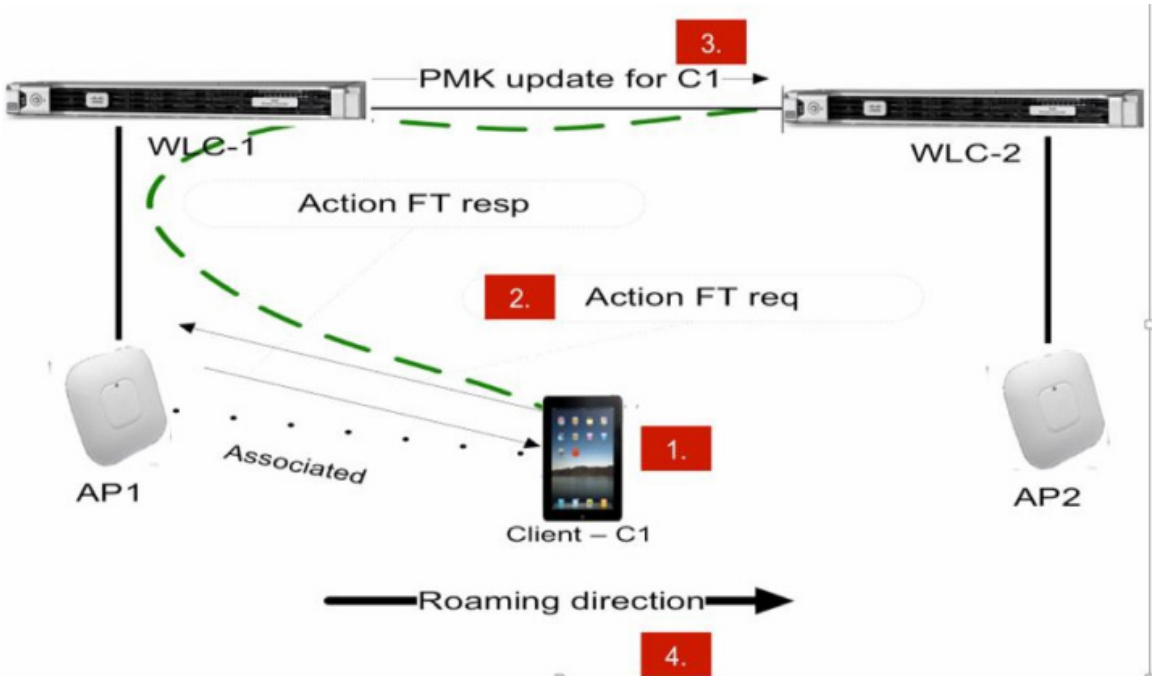
ステップ 1　クライアントは AP1 にアソシエートし、AP2 へのローミングを要求します。

ステップ 2　クライアントが AP1 に対して FT 認証要求を送信し、AP1 から FT 認証応答を受信します。

ステップ 3　WLC-1 は WLC-2 に対し、ローミング クライアントに関するペアワイズ マスター キー（PMK）およびモビリティ メッセージを送信します。

ステップ 4　クライアントは AP1 から AP2 へのローミングを完了します。

図 11-6　　コントローラ間の Over-the-DS ローミング



GUI を使用した Fast Transition ローミングの設定

GUI を使用して FT ローミングを設定するには、次の手順を実行します。

ステップ 1　[WLAN（WLANs）] をクリックします。

ステップ 2　[WLAN ID] を選択して、[Edit] ページを開きます。

ステップ 3　[Security] > [Layer 2] タブを選択します。

ステップ 4　ドロップダウンリストから [WPA+WPA2] を選択します。

FT の認証キー管理パラメータが表示されます。

ステップ 5　[Fast Transition] チェックボックスをオンにして、FT を有効にします。

ステップ 6　[Over the DS] チェックボックスをオンにして、Over the DS FT を有効にします。

（注）　[Over the DS] チェックボックスは、FT を有効にしている場合にのみオンに設定できます。

ステップ 7　[Reassociation Timeout] フィールドに、AP へのクライアントの再アソシエーション試行がタイムアウトになる秒数を入力します。有効範囲は 1 ～ 100 秒です。

（注）　[Reassociation Timeout] フィールドは、FT を有効にしている場合にのみ設定できます。

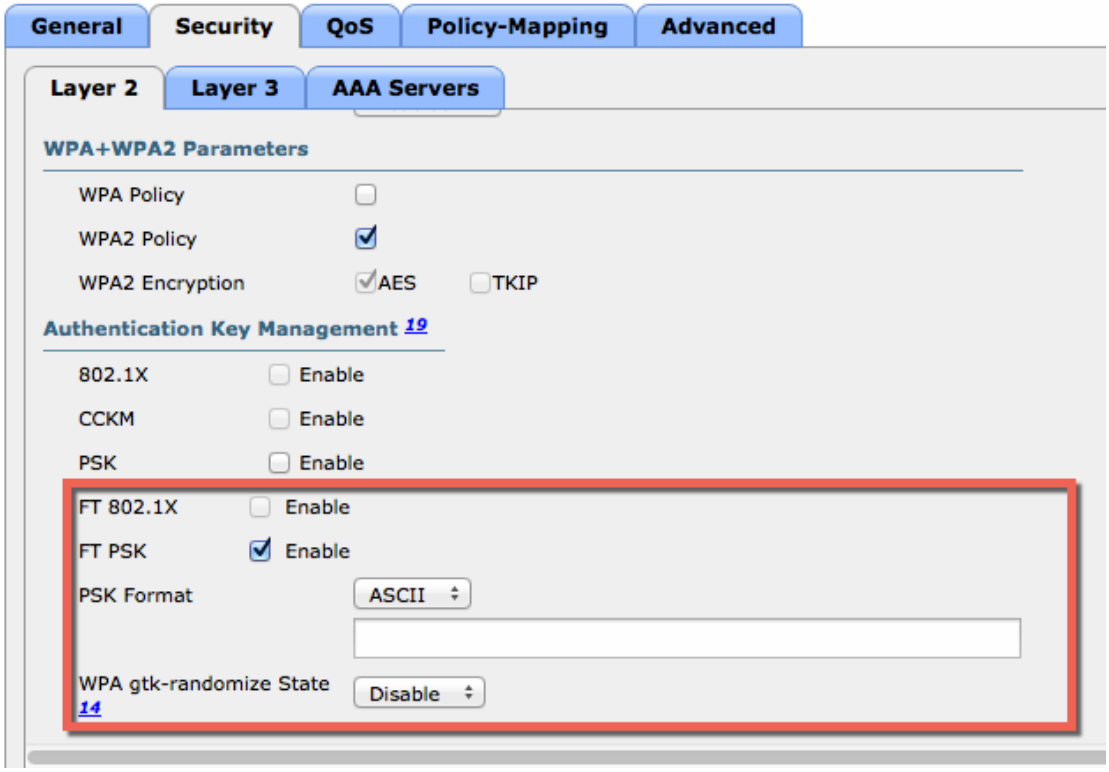
図 11-7　再アソシエーション タイムアウトの設定

ステップ 8　[Authentication Key Management] で、[FT 802.1X] または [FT PSK] の [Enable] チェックボックスをオンにし、このキーを有効にします。キーを無効にするには、[Enable] チェックボックスをオフにします。

（注）　[FT PSK] チェックボックスをオンにした場合は、[PSK Format] ドロップダウンリストから [ASCII] または [Hex] を選択して、キー値を入力します。

ステップ 9　[WPA gtk-randomize State] ドロップダウンリストから [Enable] または [Disable] を選択して、WPA グループ一時キー（GTK）のランダム化状態を設定します。

図 11-8　[Security] - [Layer 2] - [FT PSK]



ステップ 10　[Apply] をクリックします。

CLI を使用した Fast Transition ローミングの設定

FT ローミングを設定するには、次のコマンドを入力します。

config wlan security ft {**enable** | **disable**} *wlan-id*	802.11r Fast Transition パラメータを有効または無効にします。
config wlan security ft over-the-ds {**enable** | **disable**} *wlan-id*	分散システム上の 802.11r Fast Transition パラメータを有効または無効にします。これは、デフォルトでは無効になっています。
config wlan security ft reassociation-timeout timeout-in-seconds *wlan-id*	802.11r Fast Transition 再アソシエーションのタイムアウトを有効にします。範囲は 1 ～ 100 秒です。

WLAN 設定には、FT（Fast Transition）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

```
config wlan security wpa akm ft-psk {enable | disable} wlan-id
config wlan security wpa akm ft-802.1X {enable | disable} wlan-id
```

FT over a DS の AKM 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 wlan security wpa akm ft over-the-ds {**enable** | **disable**} *wlan-id*

WLAN、および WLAN の FT パラメータを表示するには、次のコマンドを入力します。

show wlan *wlan-id*

トラブルシューティングのサポート

- FT イベントのデバッグ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。

  debug ft events {**enable** | **disable**}

- FT のキー生成のデバッグ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。

  debug ft keys {**enable** | **disable**}

802.11r 高速移行の制約事項

- 802.11r FT 機能は、メッシュ AP をサポートしません。
- 802.11r FT 機能は、Cisco 600 シリーズ OfficeExtend AP など、Linux ベースの AP ではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードの FlexConnect AP ではサポートされません。
- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングは、FlexConnect AP ではサポートされません。
- クライアントがスタンドアロン モードの FlexConnect アクセス ポイントで Over-the-DS 事前認証を使用する場合、802.11r 高速ローミングはサポートされません。
- EAP LEAP 方式はサポートされません。WAN リンク遅延により、アソシエーション時間が最大 2 秒間抑制されます。
- FlexConnect AP がスタンドアロン モードに移行した場合、既存のクライアント接続は、セッション タイマーが切れるまで維持されます。AP がスタンドアロン モードである間は、新規の 11r クライアントは受け入れられません。
- 802.11r 高速ローミングでは、トラフィック仕様（TSPEC）はサポートされません。したがって、RIC IE の処理もサポートされません。
- FlexConnect AP に対して WAN リンク遅延が発生する場合は、高速ローミングも遅延します。音声またはデータの最大遅延を検証する必要があります。コントローラは、Over-the-Air および Over-the-DS 両方式のローミング中、802.11r 高速移行の認証要求を処理します。
- 802.11r FT 機能は、オープンな、WPA2 が設定された WLAN でのみサポートされます。
- 一部のレガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM スイートを認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、802.11r 以外の WLAN とはアソシエートできます。802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効になっている WLAN で 802.11i クライアントとしてアソシエートできます。回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。そうすることで、レガシー クライアントは、802.11r 対応 WLAN と正常にアソシエートできます。もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。

- FT リソース要求プロトコルを実装するクライアントが存在しないため、802.11r は FT リソース要求プロトコルをサポートしていません。また、リソース要求プロトコルは 802.11r 改訂のオプションです。
- サービス妨害（DoS）攻撃を回避するため、各コントローラでは、異なる AP と最大 3 回の FT ハンドシェイクが可能です。

802.11k 経由ローミング

802.11k では、11k 対応クライアントが、ローミングの候補となる既知のネイバー AP に関する情報を示すネイバー レポートを要求することができます。

ローミングを容易に行うため、AP にアソシエートした 11k 対応クライアントは、ネイバー AP のリストに対する要求を送信します。この要求は、アクション フレームと呼ばれる 802.11 管理フレームの形式で送信されます。同じ WLAN にあるネイバー AP の Wi-Fi チャネル番号が付いたリストを使用して、AP は応答します。この応答もアクション フレームです。クライアントは応答フレームに基づき、次のローミング先の AP 候補を識別します。クライアントは 802.11k Radio Resource Management（RRM; 無線リソース管理）プロセスを使用することで、効率的かつ高速にローミングを実行できます。

ネイバー リスト情報からローミング先の AP を決定することで、11k 対応クライアントはすべての 2.4 GHz および 5 GHz チャネルをプローブする必要がなくなります。すべてのチャネルをプローブする必要がなくなれば、チャネル利用率が減少するため、すべてのチャネルの帯域幅が増加します。ローミングにかかる時間も短縮され、クライアントによる判断が改善されます。また、チャネルごとに無線設定が変更されない上、各チャネルにプローブ要求が送信されないため、デバイスのバッテリ寿命が長くなります。これにより、デバイスではプローブ応答フレームをすべて処理する必要がなくなります。

802.11k での経由ローミング

802.11k 標準では、クライアントが、サービス セットの移行先候補となる既知のネイバー AP に関する情報を示すネイバー レポートを要求することができます。802.11k ネイバー リストを使用することで、アクティブなスキャンとパッシブなスキャンを制限することができます。

assisted roaming 機能は、インテリジェントでクライアントによって最適化されたネイバー リストに基づいています。802.11k ネイバー リストは動的かつオンデマンドで生成されます。コントローラ上では維持されません。同じコントローラ上にあっても、異なる AP にアソシエートされた 2 つのクライアントは、周囲の AP とのそれぞれの関係に応じて、異なるネイバー リストを受け取る可能性があります。

デフォルトでは、ネイバー リストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。ただし、802.11k ではデュアル リストを設定することで、両方の帯域のネイバーを返すことができます。

クライアントは、ビーコンで無線管理（RM）機能の情報要素（IE）をアドバタイズする AP にアソシエートした後に限り、ネイバー リスト要求を送信します。ネイバー リストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

コントローラが 802.11k ネイバー リスト要求を受信すると、次の処理が実行されます。

1. コントローラは RM ネイバー テーブルを検索し、クライアントが現在アソシエートしている AP と同じ帯域のネイバーのリストを作成します。
2. コントローラは、AP 間の受信信号強度表示（RSSI）、現在の AP の現在のロケーション、Cisco Prime Infrastructure からのネイバー AP のフロア情報、コントローラ上のローミング履歴情報に基づいて各ネイバーをチェックし、帯域ごとにリストするネイバーを 6 つに絞り込みます。このリストは、同じフロアの AP に対して最適化されています。

802.11k 情報要素（IE）

クライアントは、ビーコンで無線管理（RM）機能の情報要素（IE）をアドバタイズする AP にアソシエートした後に限り、ネイバー リスト要求を送信します。

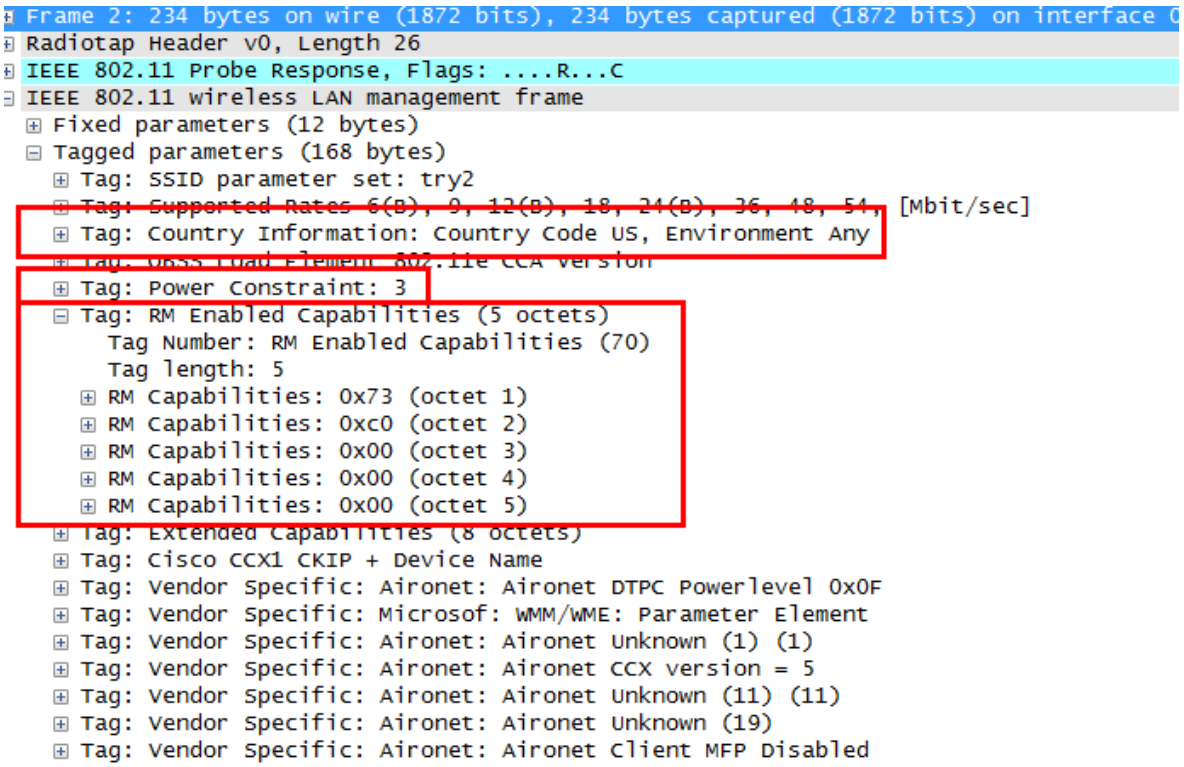
Apple ハンドヘルド デバイスとのスムーズな統合を可能にするため、AP のビーコンおよびプローブ応答には、以下の情報要素が実装されています。

- *国に関する要素*：国に関する情報要素には、ステーションが自身の属する規制ドメインを識別し、この規制ドメイン内で動作するための PHY の設定に必要となる情報が含まれます。
- *電力制約に関する要素*：電力制約に関する情報要素には、現在のチャネルでのローカルな最大送信電力をクライアントが判断するために必要な情報が含まれます。
- *RM 対応機能に関する要素*：RM 機能に関する要素は、5 オクテットの長さとなります。ビーコンまたはプローブ応答にこの要素が含まれる場合は、AP がネイバー リストを提供するための通知に、ビット 1 が使用されます。アソシエーション要求に使用される場合、ビット 1 はクライアントがネイバー リストを要求していることを表します。

これら 3 つの IE がすべて存在する場合は、この SSID が要求に応じてネイバー リストを提供できるように設定されていることを意味します。このリリースでは、ネイバー リストは IE に示されるクライアントのネイバー リスト機能ではなく、クライアントからの要求に応じて送信されます。

Wireshark による次のキャプチャ画面では、これらの情報要素を示します。

図 11-9　802.11k 情報要素



GUI を使用した経由ローミングの設定

GUI を使用して経由ローミングを設定するには、次の手順を実行します。

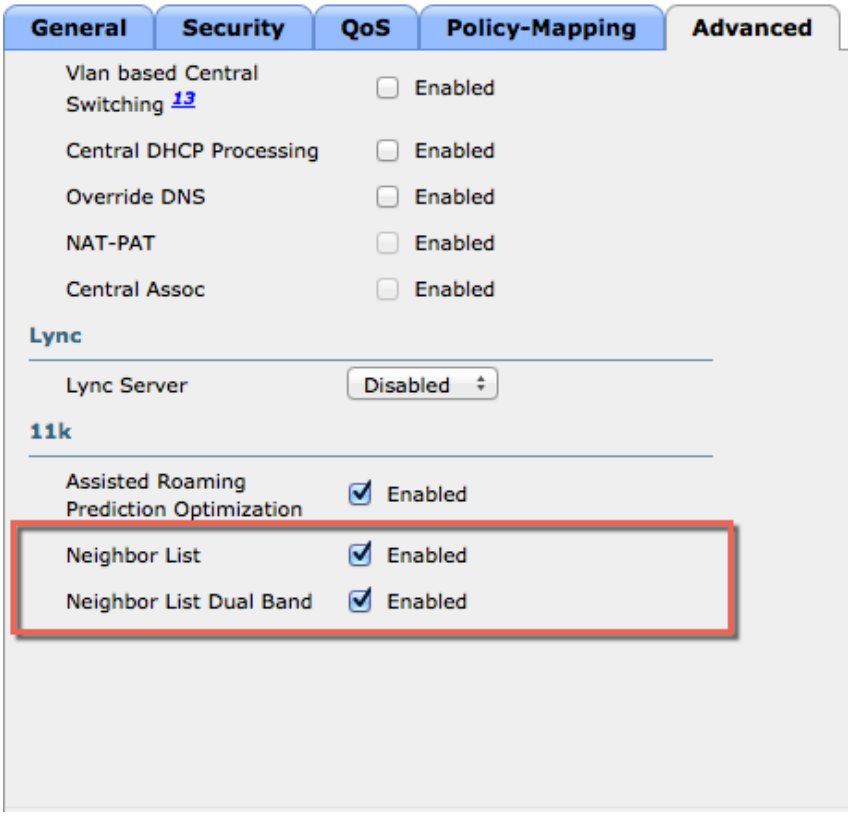
ステップ 1　[WLAN（WLANs）] をクリックします。

ステップ 2　[WLAN ID] を選択して、[Edit] ページを開きます。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　[11k] 領域で、[Neighbor List] および [Neighbor List Dual Band] チェックボックスをオンにします。

図 11-10　[Advanced] タブ - [Neighbor List]



CLI を使用した経由ローミングの設定

経由ローミングを設定するには、次のコマンドを入力します。

config wlan assisted-roaming neighbor-list enable *wlan-id*	WLAN の 802.11k ネイバー リストを設定します。WLAN を作成すると、デフォルトで assisted roaming がネイバー リストで有効になります。コマンドの no 形式では、経由ローミングのネイバー リストが無効になります。
config wlan assisted-roaming dual-list enable *wlan-id*	WLAN のデュアル バンド 802.11k デュアル リストを設定します。WLAN を作成すると、デフォルトで assisted roaming がデュアル リストで有効になります。コマンドの no 形式では、経由ローミングのデュアル リストが無効になります。
config wireless assisted-roaming floor-bias *dBm*	ネイバー フロア ラベル バイアスを設定します。有効な範囲は –5 ～ 25 dBm で、デフォルト値は –15 dBm です。

予測ベースのローミング：802.11k 以外のクライアントの経由ローミング

各クライアントに対し、予測ネイバー リストを生成することで、802.11k ネイバー リスト要求を送信する必要がなくなり、802.11k 以外のクライアントに対するローミングを最適化できます。予測ベースのローミングを WLAN で有効にすると、クライアントがアソシエーションまたは再アソシエーションに成功する度に、同一のネイバー リスト最適化が 802.11k 以外のクライアントに適用され、生成されたネイバー リストがモバイル ステーションのソフトウェア データ構造内に格納されます。クライアントは通常、アソシエーションまたは再アソシエーションを行う前にプローブを行うため、クライアント プローブの RSSI 値はネイバーごとに異なります。このため、異なる場所にあるクライアントには、それぞれ異なるネイバー リストが生成されます。このリストは最新のプローブ データによって生成され、クライアントがローミングする可能性の高い次の AP を予測します。

AP へのアソシエーション要求が、格納済みの予測ネイバー リスト内のエントリと一致しない場合、無線インフラストラクチャはアソシエーションを拒否し、好ましくないネイバーへのクライアントのローミングを抑止します。

- **Denial count**：クライアントがアソシエーションを拒否される最大回数です。
- **Prediction threshold**：経由ローミング機能を有効にするために、予測リスト内で必要となるエントリの最小数です。

GUI を使用した予測ベース ローミングの設定

GUI を使用して予測ベース ローミングを設定するには、次の手順を実行します。

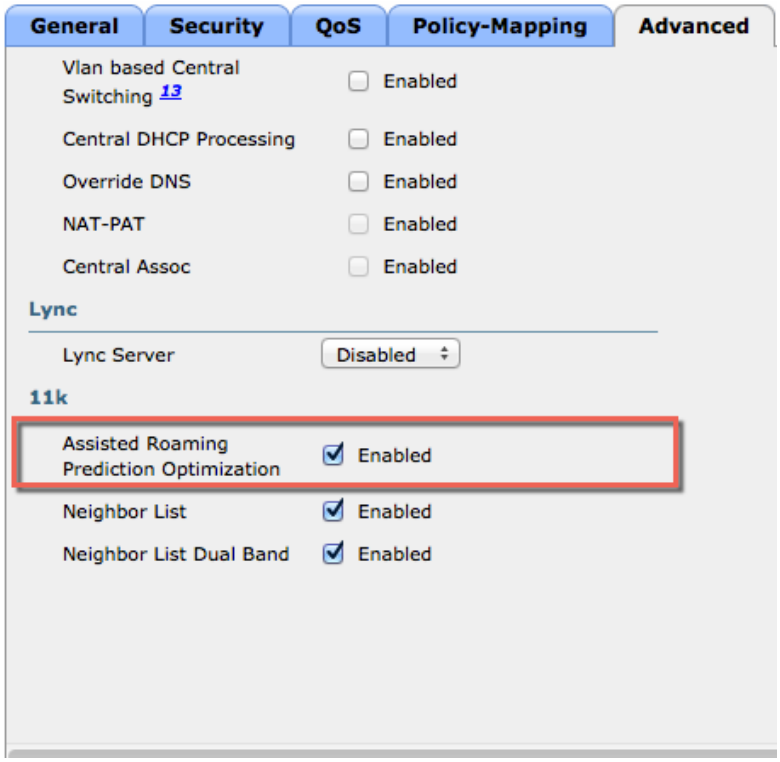
ステップ 1　[WLAN（WLANs）] をクリックします。

ステップ 2　[WLAN ID] を選択して、[Edit] ページを開きます。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　[11k] 領域で、[Assisted Roaming Prediction Optimization] チェックボックスをオンにします。

図 11-11　[Advanced] タブ - [Assisted Roaming Prediction Optimization]



CLI を使用した予測ベース ローミングの設定

予測ベース ローミングを設定するには、次のコマンドを入力します。

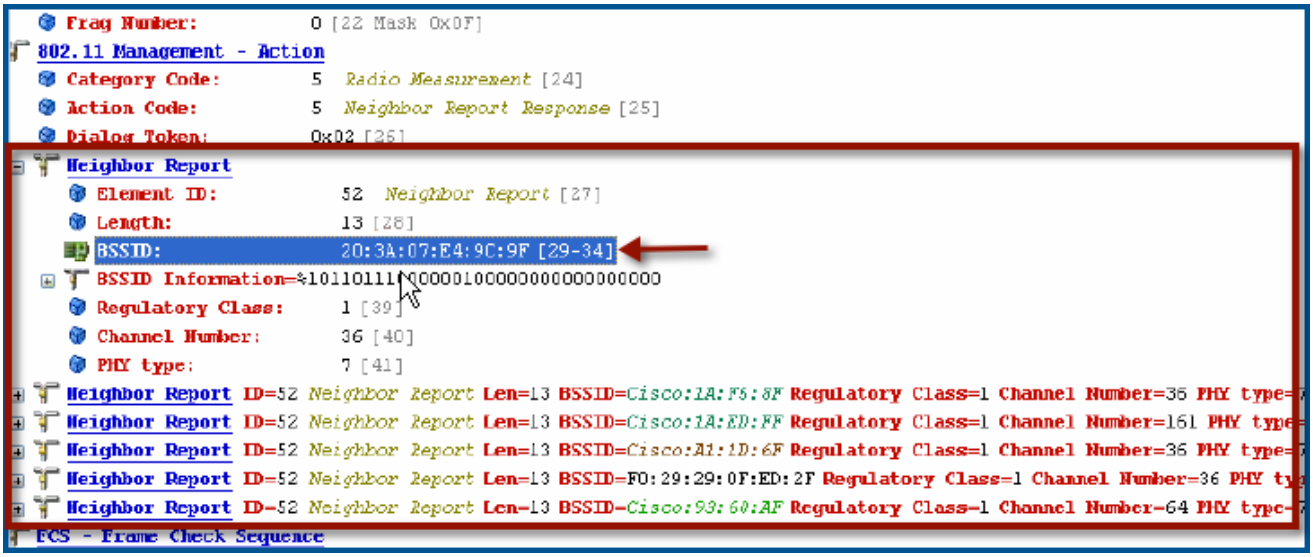
config wlan assisted-roaming prediction {**enable** | **disable**} *wlan-id*	WLAN の経由ローミング予測リストを設定します。デフォルトでは、経由ローミング予測リストはディセーブルです。 (注)　ロード バランシングが WLAN に対してすでに有効である場合、警告メッセージが表示され、ロード バランシングが WLAN に対して無効になります。
config assisted-roaming denial-maximum *count*	アソシエーション要求の送信先となる AP が、予測されたどの AP にも一致しない場合に、クライアントがアソシエーションを拒否できる最大回数を設定します。有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。

config assisted-roaming prediction-minimum *count*	予測リストが有効となるために必要な、予測 AP の最小数を設定します。デフォルト値は 3 です。 (注)　クライアントに割り当てられた予測内の AP 数が、指定した数より少ない場合、経由ローミングはこのローミングに適用されません。

ネイバー リストの応答

ネイバー リストには、次に示す Wireshark キャプチャ画面のように、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

図 11-12　802.11k ネイバー レポート



トラブルシューティングのサポート

- 経由ローミングにおいてクライアントをデバッグするには、次のコマンドを入力します。
  debug mac addr *client-mac-addr*
- すべての 802.11k イベントのデバッグを設定するには、次のコマンドを入力します。
  debug 11k all {**enable** | **disable**}
- ネイバーの詳細のデバッグを設定するには、次のコマンドを入力します。
  debug 11k detail {**enable** | **disable**}
- 802.11k エラーのデバッグを設定するには、次のコマンドを入力します。
  debug 11k errors {**enable** | **disable**}

- 受信したネイバー要求を検証するには、次のコマンドを入力します。

  debug 11k events {**enable** | **disable**}

- クライアントのローミング履歴のデバッグを設定するには、次のコマンドを入力します。

  debug 11k history {**enable** | **disable**}

- 802.11k 最適化のデバッグを設定するには、次のコマンドを入力します。

  debug 11k optimization {**enable** | **disable**}

- オフライン シミュレーション用にインポートするクライアント ローミング パラメータの詳細を取得するには、次のコマンドを入力します。

  debug 11k simulation {**enable** | **disable**}

802.11v 最大アイドル期間、Directed Multicast Service

リリース 8.0 から、コントローラはワイヤレス ネットワークに関する 802.11v 改訂をサポートします。これには、ワイヤレス ネットワーク管理に対する、次のようなさまざまな機能拡張が規定されています。

- ネットワーク支援型電力節約: クライアントのスリープ時間を延ばして、バッテリ寿命を向上させます。たとえば、モバイル デバイスは一定のアイドル期間を使用することで、アクセス ポイントへの接続を維持しておき、後述するタスクをワイヤレス ネットワーク内で実行するときに、より多くの電力を消費できます。
- ネットワーク支援型ローミング: より適切な AP とアソシエートできるように、アソシエートされたクライアントに WLAN がメッセージを送信する機能です。これは、ロード バランシングと接続状態の悪いクライアントの管理の両方に役立ちます。

802.11v ネットワーク支援型電力節約の有効化

ワイヤレス デバイスは、さまざまな方法でクライアントへの接続を維持するためにバッテリを消費します。

- 一定間隔でスリープ解除し、DTIM が含まれるアクセス ポイント ビーコンをリッスンします。DTIM は、AP がクライアントに送信する、バッファされたブロードキャストまたはマルチキャスト トラフィックを示します。
- アクセス ポイントとの接続を維持するために、null フレームをキープアライブ メッセージの形式でアクセス ポイントに送信します。
- デバイスは、定期的にビーコンをリッスンして（DTIM フィールドがない場合でも）、対応するアクセス ポイントとクロックを同期させます。
- このすべてのプロセスがバッテリを消費し、その消費は一部のデバイス（Apple など）に影響します。これらのデバイスは控えめに推定されたセッション タイムアウトを使用するために、頻繁にスリープ解除してキープアライブ メッセージを送信するためです。802.11 標準では、802.11v を使用しない限り、コントローラまたはアクセス ポイントがローカル クライアントのセッション タイムアウトについて、ワイヤレス クライアントと通信するメカニズムがありません。

クライアントの電力を節約するため、802.11v 標準の以下の機能が使用されます。

- Directed Multicast Service（DMS）
- Base Station Subsystem（BSS）最大アイドル期間

Directed Multicast Service

クライアントはアクセス ポイントに対し、必要なマルチキャスト パッケージをユニキャスト フレームとして送信するように要求します。これにより、クライアントはスリープ モードでは無視されるマルチキャスト パケットを受信でき、レイヤ 2 の信頼性も保証されます。また、ユニキャスト フレームができるだけ高いワイヤレス リンク レートでクライアントに送信されるため、クライアントは無線の持続期間を短縮してパケットをすばやく受信できるようになり、バッテリの電力が節約されます。ワイヤレス クライアントはマルチキャスト トラフィックを受信するために DTIM 間隔ごとにスリープ解除する必要がないため、スリープ間隔を延ばすことができます。

Base Station Subsystem 最大アイドル期間

BSS 最大アイドル期間は、接続先のクライアントからフレームが送信されないという理由で AP がこのクライアントをアソシエート解除しないタイムフレームです。これにより、クライアント デバイスはキープアライブ メッセージを頻繁に送信しないようになります。アイドル期間タイマー値は、AP からクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。このアイドル時間値は、クライアントが AP にフレームを送信しなくても、クライアントのアイドル状態が維持される最大時間を意味します。これにより、クライアントはキープアライブ メッセージを送信することなく、より長い間スリープ モードを維持できます。これは、バッテリの節電につながります。

CLI を使用した 802.11v ネットワーク支援型電力節約の設定

- BSS 最大アイドル期間の値を設定するには、次のコマンドを入力します。

  config wlan usertimeout *wlan-id*
  config wlan bssmaxidle {**enable** | **disable**} *wlan-id*
- DMS を設定するには、次のコマンドを入力します。

  config wlan dms {**enable** | **disable**} *wlan-id*

802.11v ネットワーク支援型電力節約のモニタリング

- AP の無線スロットごとの DMS 情報を表示するには、次のコマンドを入力します。

  show controller d1/d0 | begin DMS
- コントローラで処理される DMS 要求を追跡するには、次のコマンドを入力します。

  debug 11v all {**enable** | **disable**}
  debug 11v errors {**enable** | **disable**}
  debug 11v detail {**enable** | **disable**}

トラブルシューティングのサポート

- 802.11v デバッグを有効または無効にするには、WLC で次のコマンドを入力します。

  debug 11v detail

- アクセス ポイントで処理される DMS 要求を追跡するには、AP で次のコマンドを入力します。

  debug dot11 dot11v

802.11v BSS 移行管理

802.11v BSS 移行は、次の 3 つのシナリオに適用されます。

- **要請された要求**：クライアントは、より適切な AP と再アソシエートできるように、ローミングの前に 802.11v BSS 移行管理クエリを送信できます。
- **要請されないロード バランシング要求**：AP は負荷が高い場合、アソシエートされたクライアントに 802.11v BSS 移行管理要求を送信します。
- **要請されない最適化ローミング要求**：クライアントの RSSI とレートが要件を満たしていない場合は、AP はこのクライアントに 802.11v BSS 移行管理要求を送信します。

802.11v BSS 移行管理要求は、クライアントに示される提案です。クライアントは、提案に従うかどうかを自分で決定できます。クライアントのアソシエート解除を強制するには、アソシエート解除イミネント機能をオンにします。この機能では、クライアントが別の AP に再アソシエートしなければ、一定時間後にアソシエート解除されます。

Optimized Roaming + 802.11v

Disassociation 機能

Optimized Roaming 動作：90 秒（またはそれ以下）ごとにクライアントの統計情報をチェックし、RSSI やデータ レートに問題がある場合は、クライアントとのアソシエーションを解除します。

Optimized Roaming + 802.11v 動作：クライアントが BSS 移行に対応している場合は、クライアントとのアソシエーションを解除する代わりに、BSS 移行要求をクライアントに送信します。

アソシエーション RSSI のチェック

Optimized Roaming 動作：クライアントとのアソシエーション中にクライアントの RSSI をチェックします。RSSI チェックが失敗した場合、クライアントのアソシエーションを許可しません。

Optimized Roaming + 802.11v 動作：クライアントが BSS 移行に対応している場合は、クライアントのアソシエーションを許可するだけでなく、クライアント BSS 移行要求も送信します。

ロード バランシング + 802.11v

Optimized Roaming と同様に、ロード バランシングが失敗したときにクライアントを拒否した場合、クライアントはどの AP にアソシエートすればよいかはっきりわからず、負荷がかかっている同じ AP に何度も繰り返しアソシエートする可能性が著しく高くなります。

11v BSS 移行では、クライアントは負荷がかかっている AP にアソシエートしようとせず、提供されたリストからアソシエート先の AP を選択できます。

GUI を使用した 802.11v BSS 移行管理の設定

GUI を使用して 802.11v BSS 移行管理を設定するには、次の手順を実行します。

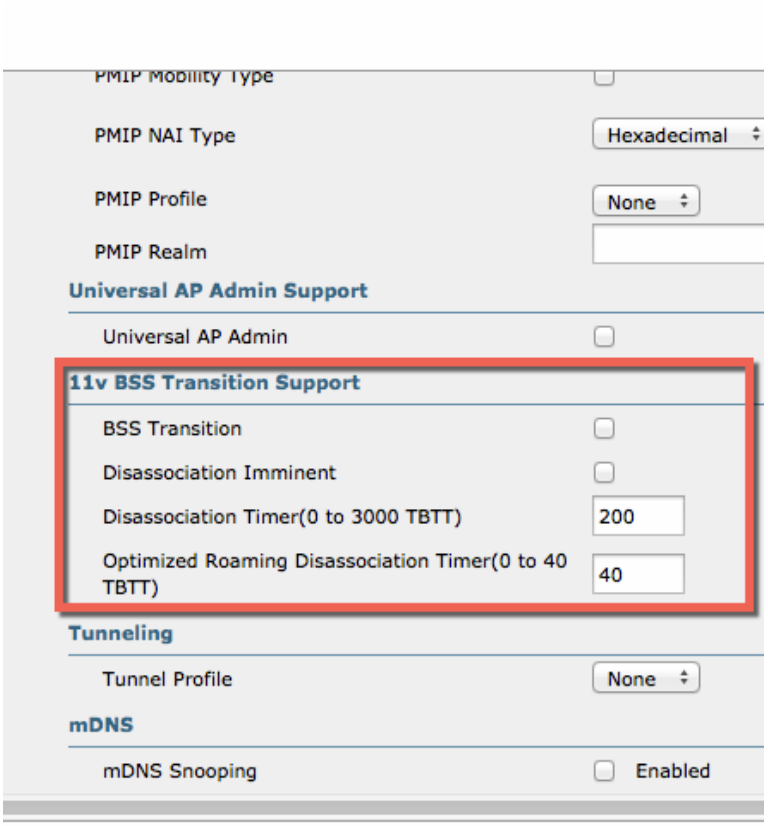
ステップ 1　[WLAN（WLANs）] をクリックします。

ステップ 2　[WLAN ID] を選択して、[Edit] ページを開きます。

ステップ 3　[Advanced] タブをクリックします。

ステップ 4　[11v BSS Transition Support] 領域で、[Disassociation Time] および [Optimized Roaming Disassociation Timer] フィールドに値を入力します。

図 11-13　[Advanced] タブ - [11v BSS Transition Support]



CLI を使用した 802.11v BSS 移行管理の設定

コントローラで 802.11v BSS 移行管理を有効にするには、次のコマンドを入力します。

config wlan bss-transition enable *wlan-id*	802.11v BSS 移行を有効にします。
config wlan disassociation-imminent enable *wlan-id*	STA のアソシエーションを解除します。
config wlan bss-transition disassociation-imminent oproam-timer <*timer*> <*WLAN id*>	要請されない最適化ローミング要求に使用します（TBTT = ビーコン間隔）。
config wlan bss-transition disassociation-imminent timer <*timer*> <*WLAN id*>	要請された要求、および要請されない要求に使用します。

11v BSS 移行のトラブルシューティング

802.11v BSS 移行のトラブルシューティングを行うには、次のコマンドを入力します。

```
debug 11v all
```

制約事項

クライアントが 802.11v BSS 移行をサポートしている必要があります。

802.11w 保護管理フレーム

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャスト メディアです。認証/認証解除、アソシエーション/アソシエーション解除、ビーコン、プローブなどの管理フレームは、ワイヤレス クライアントがネットワーク サービスのセッションを開始またはティアダウンするために使用します。暗号化により、一定レベルの機密保持を実現できるデータ トラフィックとは異なり、これらのフレームはすべてのクライアントによって受信および解釈される必要があるため、オープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。たとえば、攻撃者は AP にアソシエートされたクライアントを攻撃するために、AP からの管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、保護管理フレーム（PMF）サービスによって保護された、一連の堅牢な管理フレームにのみ適用されます。これには、アソシエーション解除フレーム、認証解除フレーム、ロバスト アクション フレームなどが含まれます。

以下の管理フレームはロバスト アクションとみなされ、保護されます。

- スペクトル管理
- QoS
- DLS
- ブロック ACK
- 無線測定
- 高速 BSS 移行
- SA クエリ
- 保護されたデュアル パブリック アクション
- ベンダー固有保護

802.11w がワイヤレス メディアに実装されている場合、次の動作が実行されます。

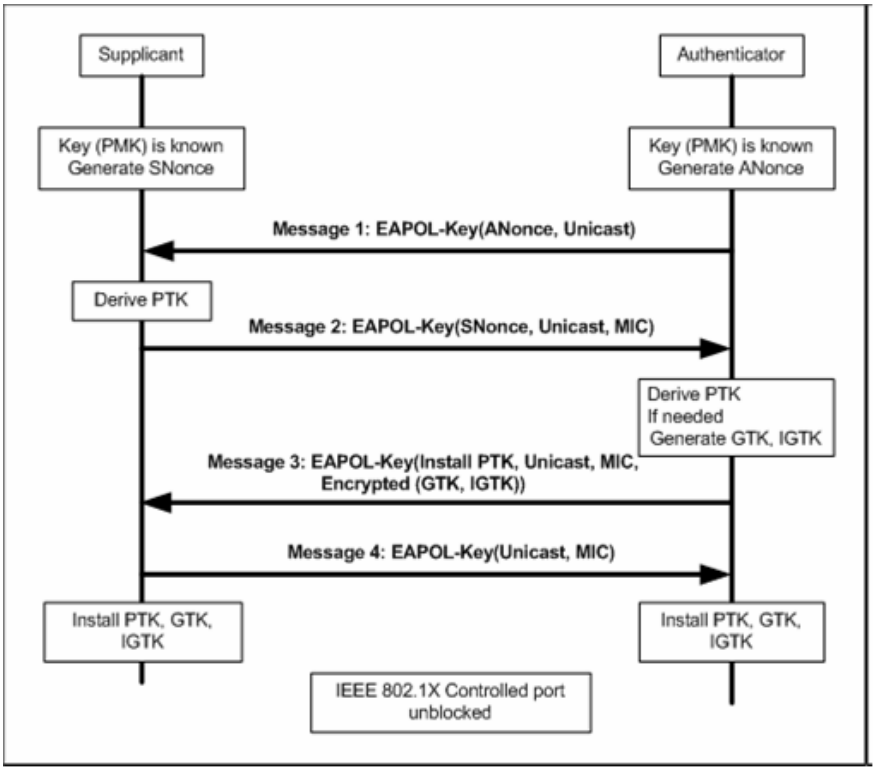
- **クライアント保護**：AP が認証解除フレームとアソシエーション解除フレームに対し、暗号化による保護を追加することで、DoS 攻撃でスプーフィングされることを阻止します。
- **インフラストラクチャ保護**：アソシエーションの復帰期間と SA クエリの手順から構成される、セキュリティ アソシエーション（SA）ティアダウン保護メカニズムを追加します。これにより、スプーフィングされたアソシエーション要求により、接続済みのクライアントが切断されることを阻止します。

802.11w で新たに導入された IGTK キーは、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用されます。

- **IGTK** は、オーセンティケータ STA（WLC）から割り当てられ、AP に送信されるランダムな値です。IGTK は、この AP からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用されます。

管理フレーム保護のネゴシエーションでは、AP は EAPOL キー フレーム内で GTK および IGTK 値を暗号化します。このフレームは、4 ウェイ ハンドシェイクにおけるメッセージ 3 内で送信されます。

図 11-14　4 ウェイ ハンドシェイクでの IGTK 交換

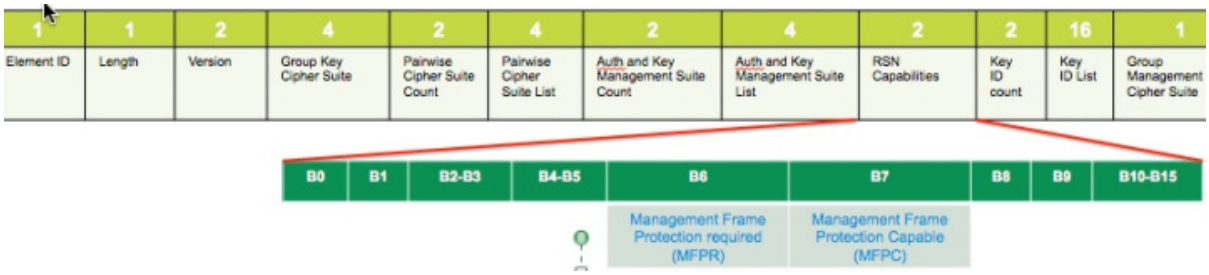


AP が後から GTK を変更する場合、AP はグループ キー ハンドシェイクを使用して、変更後の GTK および IGTK をクライアントに送信します。

802.11w では、新たに Broadcast/Multicast Integrity Protocol（BIP）が定義されています。このプロトコルは、IGTKSA の確立に成功した後、ブロードキャストおよびマルチキャストの堅牢な管理フレームに対して、データの整合性、およびリプレイ攻撃からの保護を実現します。BIP では、共有 IGTK キーを使用して計算された MIC が追加されます。

802.11w の情報要素（IE）

図 11-15　802.11w の情報要素

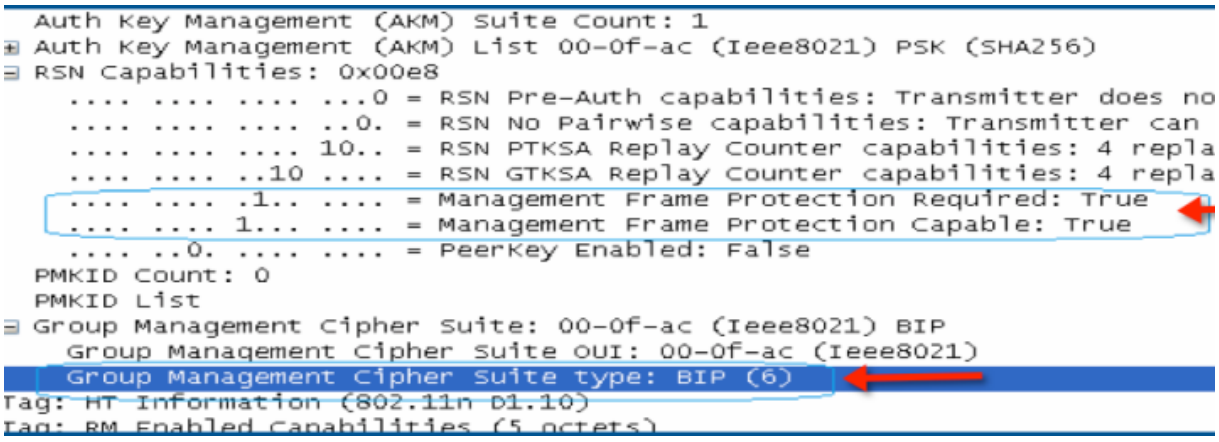


1. 変更は、RSNIE の RSN 機能フィールドで実行されます。
   - ビット 6：Management Frame Protection Required（MFPR）
   - ビット 7：Management Frame Protection Capable（MFPC）
2. AKM スイート セレクタに、新たな AKM スイート 5 および 6 が追加されました。
3. BIP に対応するため、タイプ 6 の新たな暗号スイートが追加されました。

WLC はアソシエーションおよび再アソシエーション応答に、修正 RSNIE を追加します。AP はビーコンおよびプローブ応答に、修正 RSNIE を追加します。

次の Wireshark キャプチャ画面は、RSNIE 機能、およびグループ管理暗号スイート要素を示します。

図 11-16　802.11w の情報要素



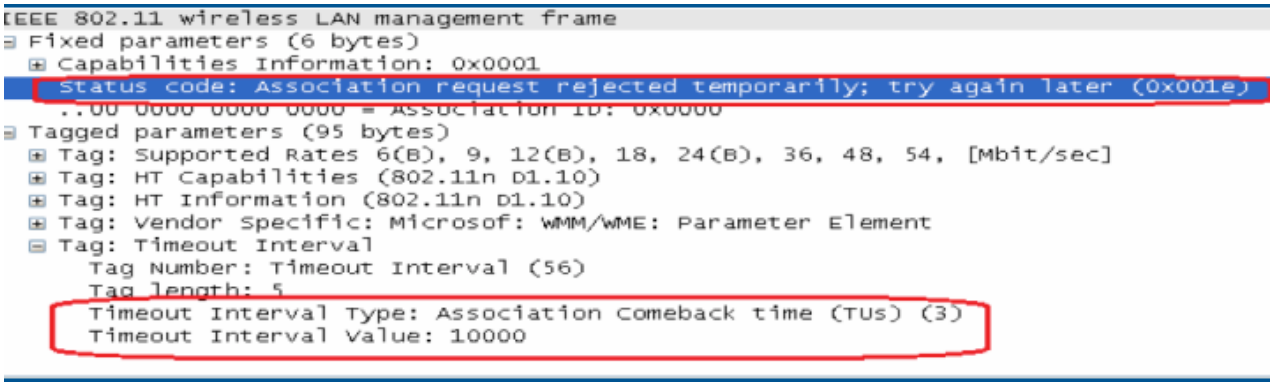
セキュリティ アソシエーションのティアダウン保護

セキュリティ アソシエーション（SA）のティアダウン保護は、リプレイ攻撃により、既存クライアントのセッションが切断されることを防止するメカニズムです。アソシエーションの復帰期間と SA クエリの手順を組み合わせることで、スプーフィングされたアソシエーション要求により、接続済みのクライアントが切断されることを防止します。

クライアントが有効なセキュリティ アソシエーションを有し、802.11w をネゴシエートしている場合は、AP はステータス コード 30 を使用して、新たなアソシエーション要求を拒否します。このステータス コードの内容は、「Association request rejected temporarily; Try again later（アソシエーション要求は一時的に拒否されました。後でやり直してください）」となります。AP は、SA クエリ手順により、元の SA が無効であると判断されない限り、既存アソシエーションを切断したり、その状態を変更したりすることはできません。また、AP のアソシエーション要求には、アソシエーション復帰期間の情報要素が含められます。これは、AP がこのクライアントとのアソシエーションを受け入れる準備が整うまでの期間を指定します。

次の図では、ステータス コード 0x1e（30）のアソシエーション拒否メッセージと、10 秒に設定されたアソシエーション復帰期間を確認できます。

図 11-17　アソシエーション拒否と復帰期間



クライアントに対する SA クエリがまだ実行されていない場合、AP は一致する SA クエリ応答を受信するまで、またはアソシエーション復帰期間が経過するまで、SA クエリを発行します。AP は有効な保護フレームを受信した時点で、SA クエリが正常に完了したと解釈します。一致するトランザクション識別子を含む SA クエリ応答が所定の期間内に受信されない場合は、AP は SA クエリ手順を再度実行することなく、アソシエーション プロセスを開始させます。

GUI を使用した保護管理フレームの設定

GUI を使用して保護管理フレームを設定するには、次の手順を実行します。

ステップ 1　[WLAN（WLANs）] をクリックします。

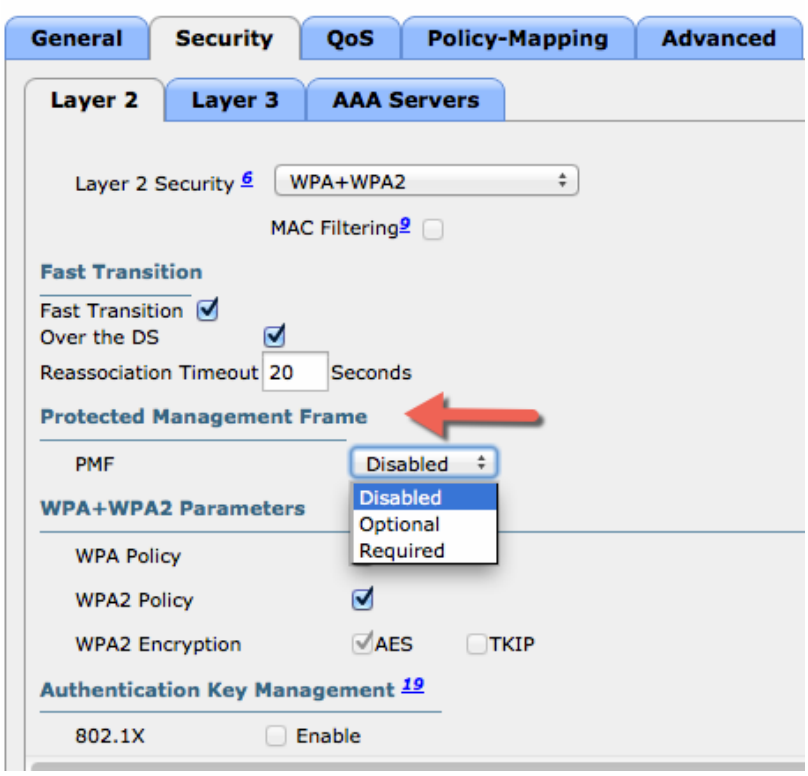
ステップ 2　[WLAN ID] を選択して、[Edit] ページを開きます。

ステップ 3　[Security] > [Layer 2] タブを選択します。

ステップ 4　ドロップダウンリストから [WPA+WPA2] を選択します。

（注）　4 ウェイ ハンドシェイクを使用して、802.11w IGTK キーが生成されます。このキーは、レイヤ 2 での WPA2 セキュリティ用に設定された WLAN でのみ使用できます。

図 11-18　[Security] - [Layer 2] - [Protected Management Frame 1]



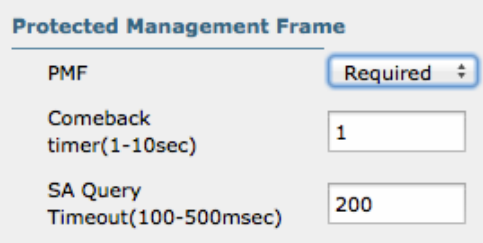
ステップ 5　[Protected Management Frame] 領域で、ドロップダウンリストから [PMF] 状態を選択します。次のオプションを使用できます。

- [Disabled]：WLAN の 802.11w MFP 保護を無効にします。
- [Optional]：クライアントが 802.11w をサポートしている場合に使用します。
- [Required]：802.11w をサポートしていないクライアントが WLAN とアソシエートできないようにします。

ステップ 6　PMF 状態を [Optional] または [Required] のいずれかとして選択する場合、次を行います。

- [Comeback Timer] フィールドに、アソシエーション復帰の間隔をミリ秒単位で入力します。復帰間隔は、有効なセキュリティ アソシエーションの後に、アクセス ポイントがクライアントと再度アソシエーションする時間です。
- [SA Query Timeout] フィールドに、セキュリティ アソシエーション（SA）クエリがタイムアウトするまでの最大時間を入力します。

図 11-19　[Security] - [Layer 2] - [Protected Management Frame 2]



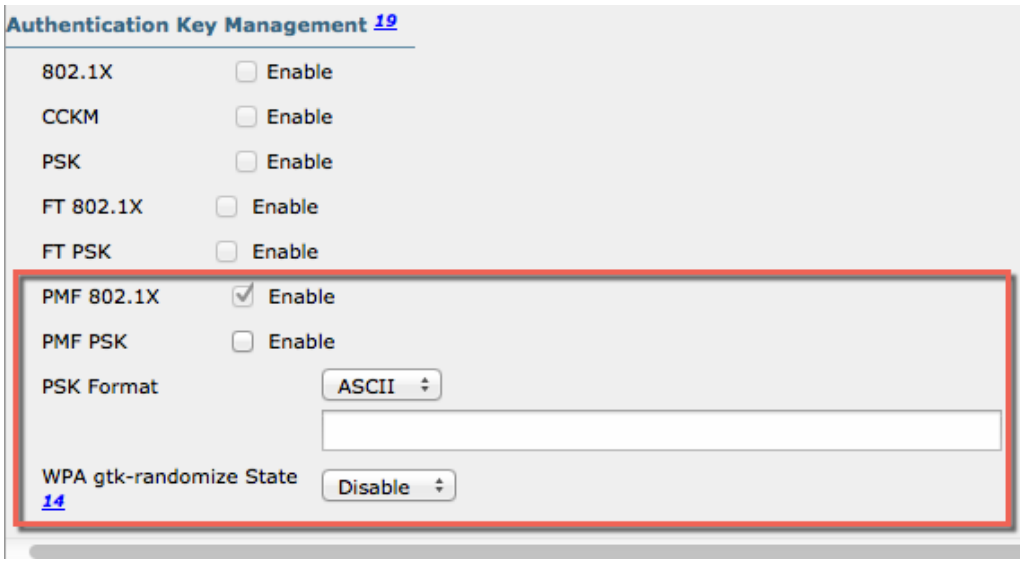
ステップ 7　[Authentication Key Management] 領域で、次を行います。

- [PMF 802.1X] チェックボックスをオンまたはオフにして、管理フレームを保護するために 802.1X 認証を設定します。
- [PMF PSK] チェックボックスをオンまたはオフにして、PMF 用に事前共有されているキーを設定します。
- [PSK Format] ドロップダウンリストから、ASCII または 16 進数のいずれかを選択し、PSK 値を入力します。

ステップ 8　[Apply] をクリックします。

ステップ 9　[Save Configuration] をクリックします。

図 11-20　Authentication Key Management



CLI を使用した保護管理フレームの設定

保護管理フレームを設定するには、次のコマンドを入力します。

Config wlan security pmf {disable | optional | required} *wlan-id* **Config wlan security pmf association-comeback** *timeout-in-seconds wlan-id* **Config wlan security pmf saquery-retrytimeout** *timeout-in-milliseconds wlan-id*	次のオプションにより PMF パラメータを設定します。 • association-comeback：802.11w のアソシエーションを設定します。有効な範囲は 1 ～ 20 秒です。 • Required：クライアントが WLAN の 802.11w MFP 保護をネゴシエートすることを要求します。 • Optional：WLAN の 802.11w MFP 保護を有効にします。 • Saquery-retry-time：すでにアソシエートされているクライアントへのアソシエーション応答で、アソシエーションを再試行できるようになるまでの時間（ミリ秒単位）です。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかが確認されます。クライアントがこの時間内に応答しない場合は、クライアント アソシエーションがコントローラから削除されます。SA クエリの再試行時間は、ミリ秒単位で指定します。指定できる範囲は 100 ～ 500 ミリ秒です。値は 100 ミリ秒の倍数で指定する必要があります。

WLAN 設定には、保護管理フレーム（PMF）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

- PMF の 802.1X 認証を設定するには、次のコマンドを入力します。

  config wlan security wpa akm pmf 802.1x {**enable** | **disable**} *wlan-id*

- PMF の事前共有キーのサポートを設定するには、次のコマンドを入力します。

  config wlan security wpa akm pmf psk {**enable** | **disable**} *wlan-id*

- WLAN の事前共有キーを設定するには、次のコマンドを入力します。

  config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk wlan-id*

（注） 暗号化が「なし」、WEP-40、WEP-104、および WPA（AES または TKIP）に設定されている WLAN では、802.11w を有効にすることはできません。

802.11w のモニタリング

WLAN、および WLAN の PMF パラメータを表示するには、次のコマンドを入力します。

show wlan *wlan-id*

トラブルシューティングのサポート

PMF のデバッグを設定するには、次のコマンドを入力します。

debug pmf events {**enable** | **disable**}

CHAPTER 12

ワイヤレス プラグ アンド プレイ

シスコ ネットワーク プラグ アンド プレイ ソリューションは、エンタープライズ ネットワークを利用するお客様にシンプルかつセキュアで統合されたソリューションを提供し、新しいブランチまたはキャンパス デバイスのロールアウトや既存のネットワークに対する更新のプロビジョニングを簡単に行うことができるようにします。このソリューションでは、クラウド リダイレクション サービス、オンプレミス、またはその組み合わせを使用して、シスコ ルータ、スイッチ、およびワイヤレス デバイスで構成されるエンタープライズ ネットワークのプロビジョニングをほぼゼロ タッチの導入エクスペリエンスとして、統合されたアプローチを提供します。

この導入ガイドでは、ワイヤレス アクセス ポイントのためのシスコのネットワークのプラグ アンド プレイ アプリケーションについて説明します。このアプリケーションでは、リモート サイトを事前プロビジョニングできます。大規模なサイトをプロビジョニングする場合、シスコのネットワーク プラグ アンド プレイ アプリケーションを使用してサイトを事前プロビジョニングしたり、サイトにアクセス ポイントを追加できます。その場合は、アクセス ポイント情報を入力し、必要に応じてブートストラップ設定をセットアップします。ブートストラップ設定によって、プラグ アンド プレイ エージェントが、WLC info、hostname、AP group、FlexGroup、AP mode などのアクセス ポイントを設定できるようになります。

事前プロビジョニングが不要な小規模サイトを作成する場合、アクセス ポイントは、シスコのネットワーク プラグ アンド プレイ アプリケーションで事前設定せずに、そのまま展開し、正当化できます。インストーラがアクセス ポイントをインストールして電源を入れると、DHCP、DNS またはクラウド リダイレクション サービスを使用して Cisco APIC-EM コントローラを自動検出します。自動検出プロセスが完了すると、AP はローカル PnP サーバの設定に従って WLC に接続するか、クラウド リダイレクション サービスと通信し、WLC と PnP サーバのどちらをターゲットとするかを確認します。

ワイヤレス PnP のサポート:

表 12-1

プラットフォーム	モデル
Cisco Aironet ワイヤレス アクセス ポイント	802.11n Generation 2 702I、702W、1600、2600、3600 802.11ac Wave 1、17/27/3700、18/28/3800 802.11ac Wave 2

APIC EM 1.5 の要件(以下の拡張制限の表も参照):

- **サーバ**:64 ビット x86(Ubuntu 14.04 LTS)
- **vCPU**:6(2.4 GHz)以上
- **RAM**:64 GB(単一ホストの導入)/32 GB(複数ホストの導入)

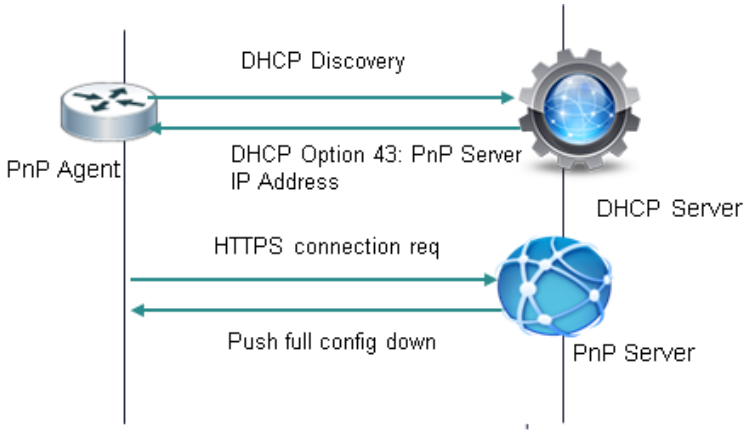
- **ネットワーク アダプタ**:1
- **ストレージ**:ハードウェア RAID 構成後に使用可能なストレージ 500 GB HDD
- **ディスク I/O**:200 MBps
- **ブラウザ**:Google Chrome または Firefox
- **ハイパーバイザ**:VMware vSphere 5.x/6.x（仮想アプライアンス）
- **アクセス ポイント**:最大 10,000

APIC EM アクセス ポイントの拡張制限:

仮想アプライアンス	コア	RAM	ハードディスク	CPU クロック速度	RAID（ハードウェア）
仮想マシン（32 GB）にインストールされた Cisco APIC-EM	12	32 GB	200 GB の内部データ ストア ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（64 GB）にインストールされた Cisco APIC-EM	8	64 GB	500 GB ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（64 GB）にインストールされた Cisco APIC-EM	12	64 GB	1 TB ディスク速度 15,000 RPM	2.9 GHz	RAID 10
仮想マシン（128 GB）にインストールされた Cisco APIC-EM	20	128 GB	2 TB ディスク速度 15,000 RPM	2.9 GHz	RAID 10

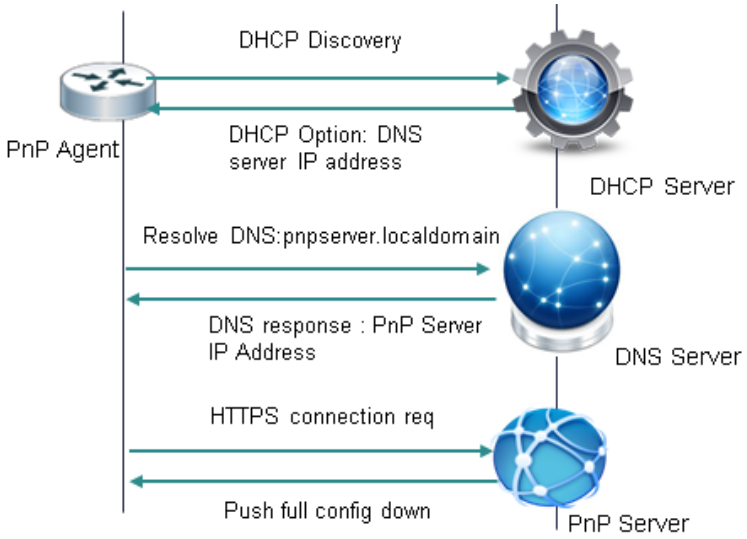
DHCP 要求/応答（Option43）:

アクセス ポイントの PnP エージェントが設定なしで起動し、DHCP を通じて IP アドレスを割り当てます。デバイスが DHCP 検出メッセージを送信します。DHCP サーバは、DHCP オプション 43 の一部として PnP サーバの IP アドレスを提供できます。DHCP 応答の一部として、PnP エージェントが APIC PnP サーバの IP アドレスである DHCP オプション 43 を受信すると、AP の PnP エージェントが PnP サーバに対する HTTPS 要求を開始します。セキュリティ クレデンシャルが検証されると、完全な設定が AP にプッシュされます。

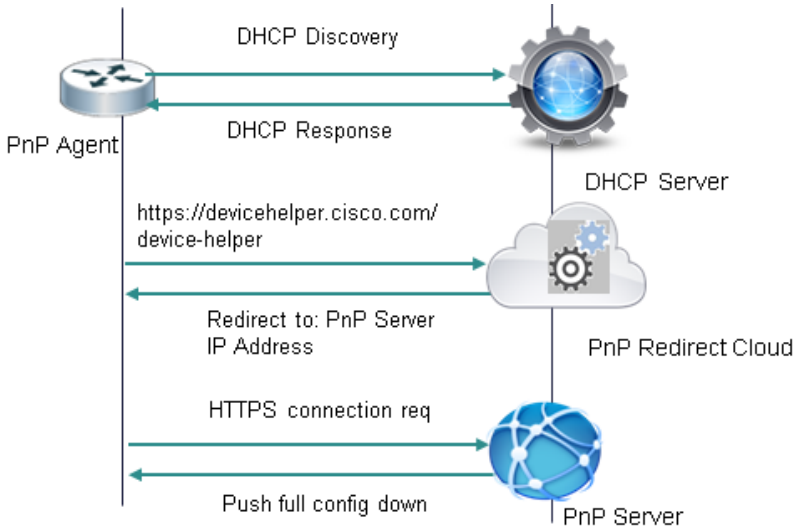


DNS レスポンス：

AP の PnP エージェントが設定なしで起動します。PnP エージェントが DHCP を通じて IP アドレスの割り当てを試みます。AP が DHCP 検出メッセージを送信します。DNS サーバの IP アドレスが DHCP 応答の一部として入力された場合は、AP の PnP エージェントが「pnpserver.localdomain」という名前に対して DNS クエリを送信します。DNS サーバは、これを APIC EM PnP サーバの IP アドレスに解決できます。AP の PnP エージェントが PnP サーバに対する HTTPS 要求を開始します。セキュリティ クレデンシャルが検証されると、完全な設定が AP にプッシュされます。



上記の例はどちらも、DHCP 応答または DNS 解決が管理されている、エンタープライズ マネージド ネットワークとサービス プロバイダー マネージド ネットワークの両方に適しています。AP が管理対象外のネットワークに接続する場合、あるいは DHCP サービスまたは DNS サービスが信頼できない場合には、PnP サーバの詳細にデバイスの所有者を関連付ける、別個のエンティティが必要になります。パブリック インターネットの Cisco PnP リダイレクト クラウド インスタンスにはこの機能があります。

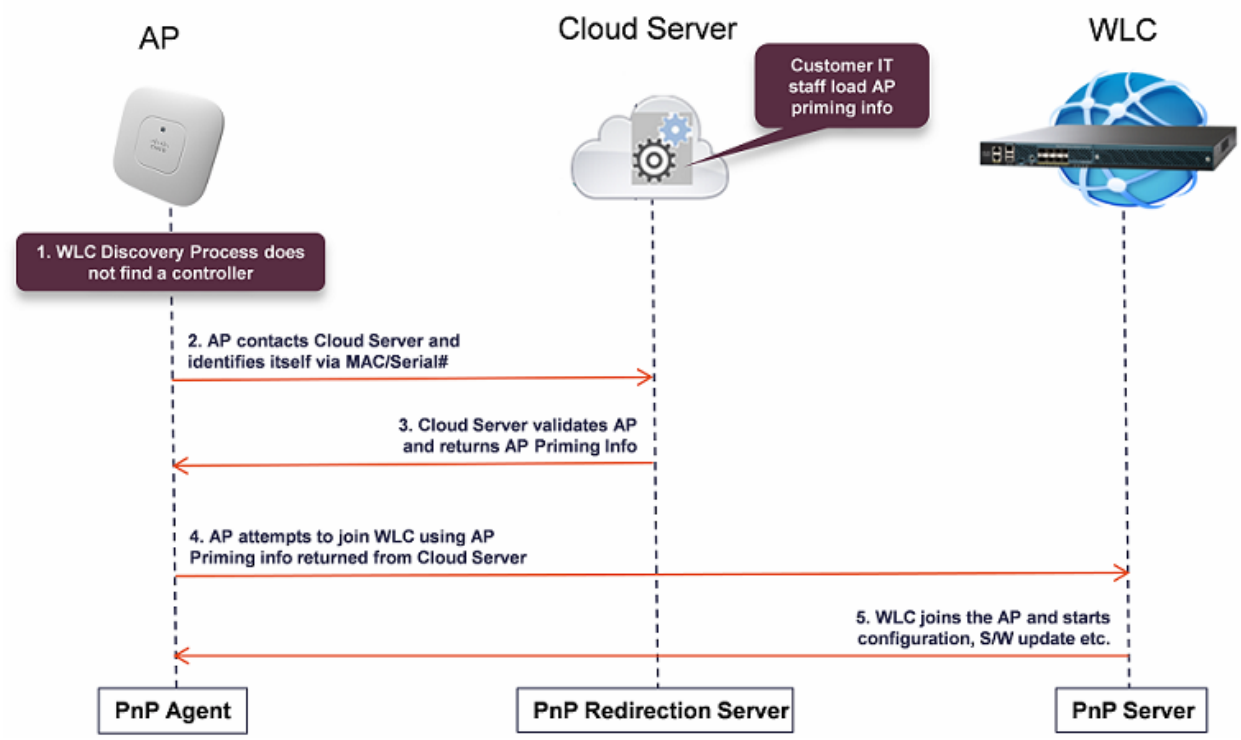


Cisco クラウド PnP リダイレクト サービス:

アクセス ポイント上の PnP エージェントは、最初に DHCP 検出を実行します。DHCP オプション 43 がなく、DNS サーバが pnpserver.localdomain を解決できない場合、AP は devicehelper.cisco.com に対する DNS ルックアップを実行します。このドメイン名は PnP リダイレクト クラウド サーバ（または PnPRC）に解決され、AP クレデンシャルが検証されます。クレデンシャルが検証されたら、顧客から提供されていた PnP サーバの IP アドレスに関連付ける必要があります。PnP サーバの IP アドレスは顧客ごとに異なり、一般的にエンタープライズまたはサービス プロバイダーでオンプレミスでホストされます。PnPRC は HTTPS GET 要求を PnP サーバの IP アドレスにリダイレクトします。このリダイレクト メカニズムは、AP が自動的にインターネット接続されるその他の使用例にも適用されます。

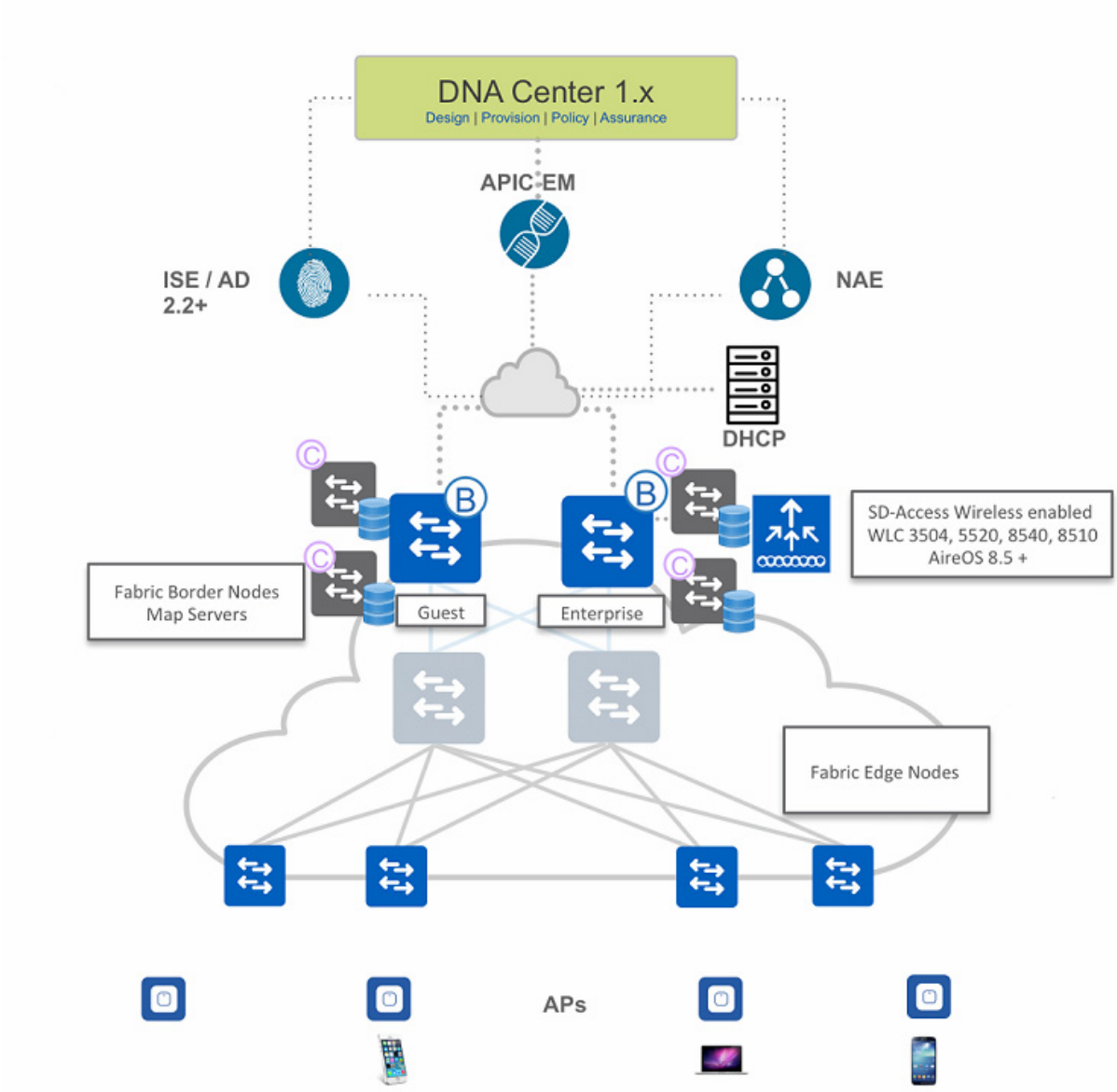
アクセス ポイント（AP）に対しては、ワイヤレス LAN コントローラ（WLC）が論理的に PnP サーバとして機能します。接続する正しい WLC を検出するために AP が使用するプロセスは、上記のプロセスに非常に似ています。WLC を検出できなかった場合、AP は PnPRC と通信して WLC の IP アドレス（論理的に PnP サーバの IP）を取得します。次に AP はこの IP アドレスを使用して、関連付けられている WLC に接続します。AP が認証されると、WLC は接続プロセスを完了し、AP のプロビジョニング プロセスを開始します。

このフローの概要を次に示します。



SD-Access ワイヤレス アーキテクチャの概要

ここでは、SD-Access ワイヤレス アーキテクチャに含まれる各種のコンポーネントのロールと用語について説明します。



- **コントロール プレーン ノード**:エンドポイント ID とデバイスの関係を管理するマップ システム
- **ボーダー ノード**:外部 L3 ネットワークを SDA ファブリックに接続するファブリック デバイス(コアなど)
- **エッジ ノード**:有線エンドポイントを SDA ファブリックに接続するファブリック デバイス(アクセス、ディストリビューションなど)
- **ファブリック ワイヤレス コントローラ**:ファブリックを有効にしたワイヤレス コントローラ(WLC)
- **ファブリック モード AP**:ファブリックを有効にしたアクセス ポイント。

- **DNA コントローラ**:エンタープライズ SDN コントローラは情報を共有する複数のサービス アプリケーションを使用して GUI 管理を抽象化します
- **グループ リポジトリ**:外部 ID サービス(ISE など)を活用して、ユーザまたはデバイスをグループに動的にマッピングし、ポリシーを定義する
- **分析エンジン**:外部データ コレクタ(NAE)を活用して、ユーザまたはデバイスのアプリケーション フローを分析し、ファブリック ステータスをモニタする

SD-Access ワイヤレス プラットフォームのサポート

SD-Access ワイヤレス アーキテクチャは AireOS リリース 8.5 以降を搭載した次のワイヤレス LAN コントローラでサポートされています。

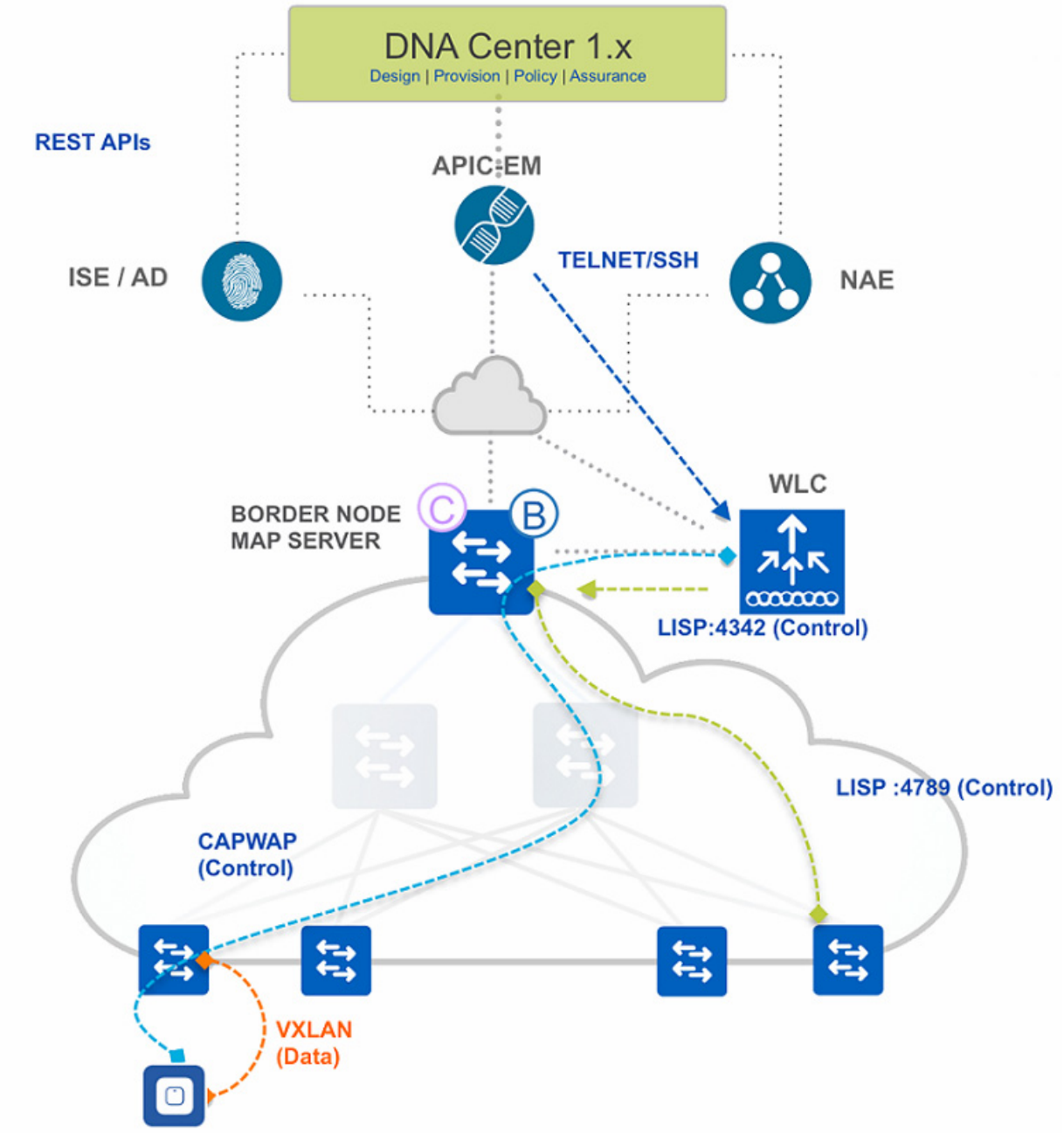
- AIR-CT3504
- AIR-CT5520
- AIR-CT8510
- AIR-CT8540

このアーキテクチャは、ローカル モードで Wave2 11ac アクセス ポイント用に最適化されています。

- AP1810
- AP1815
- AP1830
- AP1850
- AP2800
- AP3800

Wave 1 11ac アクセス ポイントでは、SD-Access ワイヤレスの限定された機能がサポートされています。

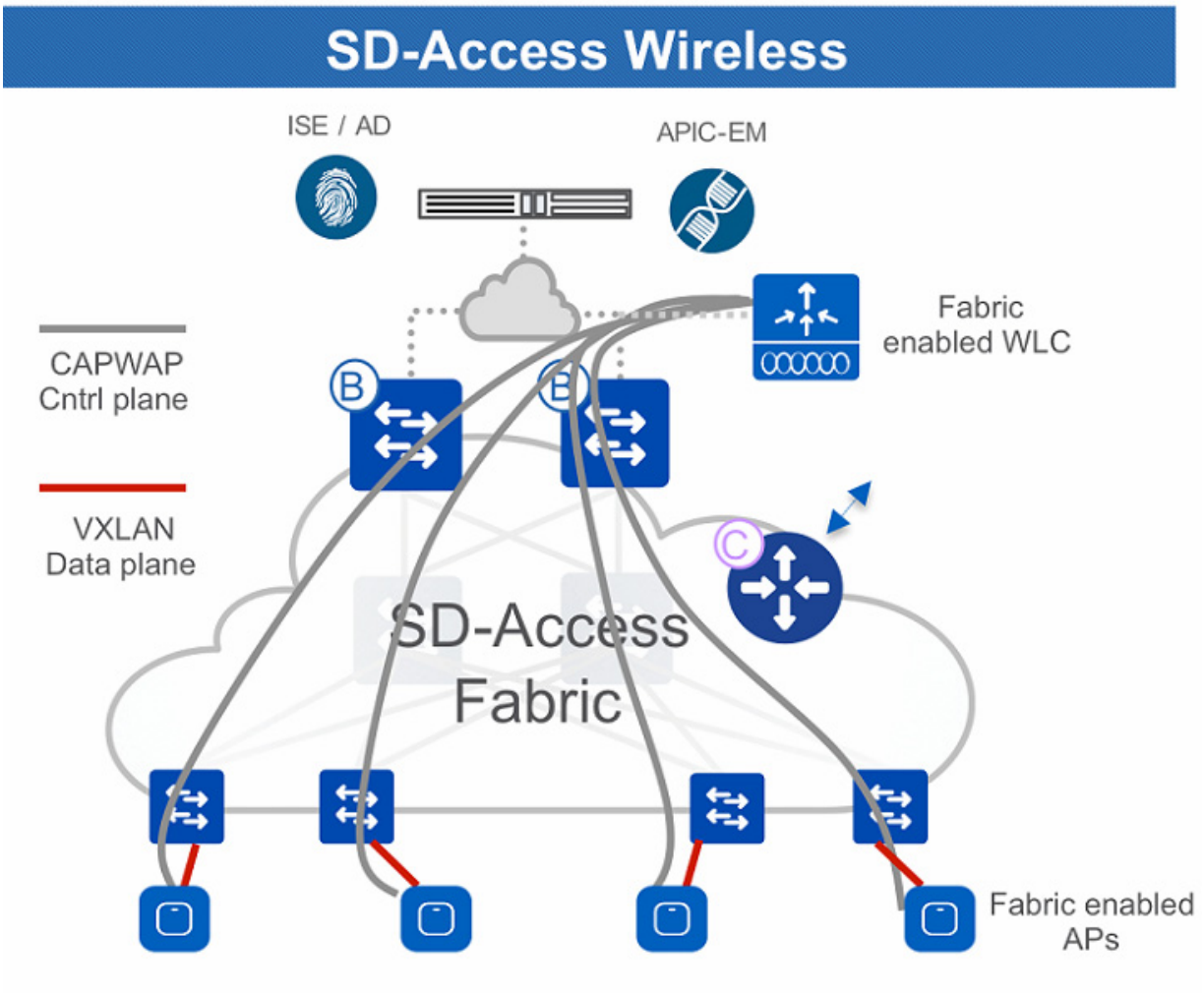
SD-Access ワイヤレス インターフェイス



- WLC <-> AP: コントロール プレーン WLC と AP の通信は、既存のモードと同様に CAPWAP を通じて行われます。
- AP <-> スイッチ:データ トラフィックが VXLAN トンネルのカプセル化によって AP からエッジ スイッチに切り替えられます。
- WLC <-> マップ サーバ:ワイヤレス LAN コントローラが、コントローラのポート 4342 で動作する LISP エージェントを使用して Mapserver と通信します。

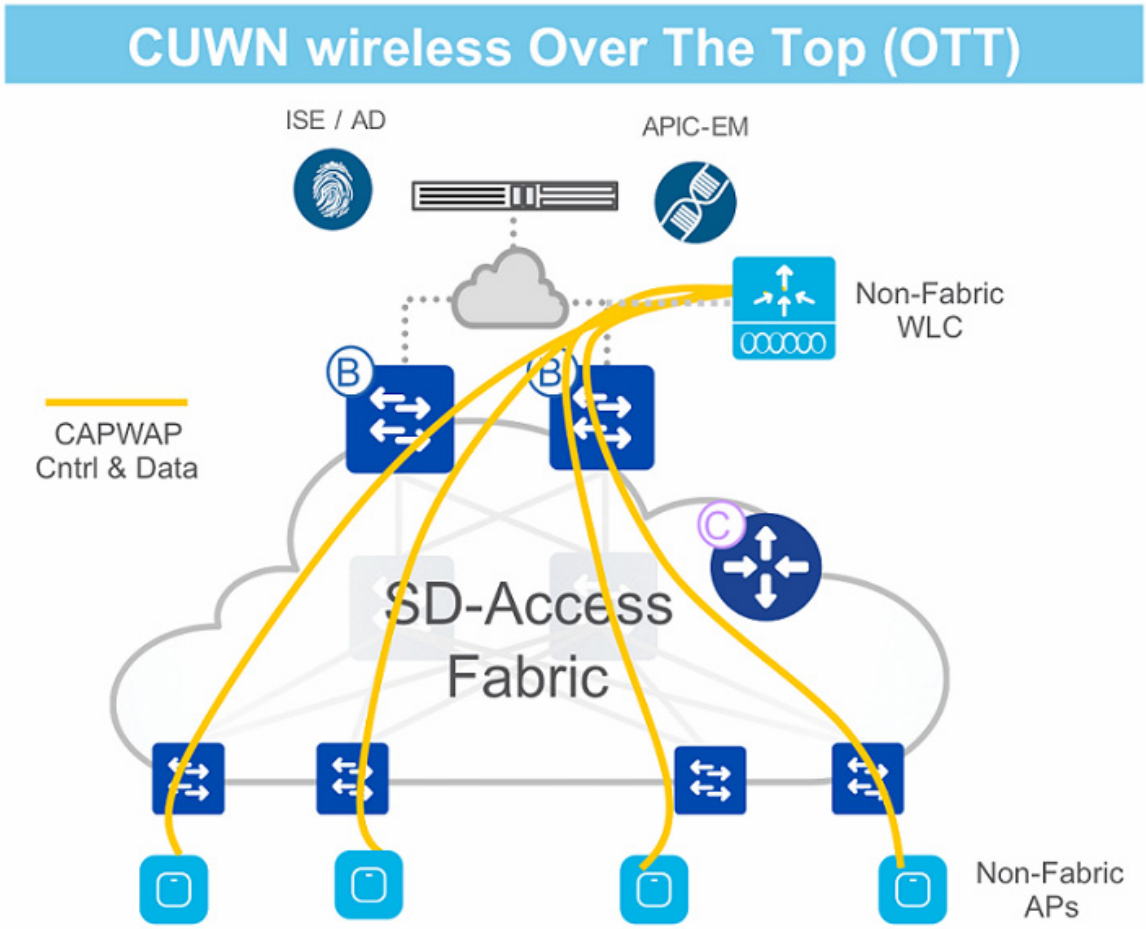
- WLC <-> APIC-EM：APIC-EM が SSH/Telnet を通じて CLI インターフェイスを使用して、WLC を設定します。
- スイッチ <-> Mapserver：ファブリック対応のスイッチが LISP ポート 4789 のマップ サーバと通信します。

サポートされている WLAN モード



- SD-Access ワイヤレスでは、トンネリングで WLC に戻る CAPWAP コントロール プレーンと、スイッチで分散処理される VXLAN データ プレーンを使用します

- WLC/AP がファブリックに統合され、アクセス ポイントがオーバーレイで接続します。



- WLC で終端するコントロール プレーンとデータ プレーン用の CAPWAP を使用した、従来型の CUWN アーキテクチャ。
- SDA ファブリックは AP と WLC 間の有線インフラストラクチャ内の伝送路にすぎません
- これが、完全な SDA 移行に向けた手順です。

SD-Access ワイヤレス機能のサポート

次の表に、SD-Access ワイヤレス アーキテクチャでサポートされている主要な機能の一部を示します。

表 12-2

オープン/固定 WEP	サポート
WPA-PSK	サポート
802.1x（WPA/WPA2）	サポート
MAC Filtering	サポート
ローカル EAP	サポート

表 12-2

AAA オーバーライド	サポート
内部/外部 WebAuth	サポート
事前認証 ACL	サポート
クライアントの IPv4 ACL	サポート
AVC	サポートあり*
ローカル プロファイリング	サポート
RADIUS プロファイル	サポート
QoS プロファイル	サポート
ユーザごとの BW 契約	サポート
wIPS	サポート
CMX 統合	サポート
NetFlow エクスポート	サポート
HA SSO	サポート

*Wave2 AP のみ

CHAPTER 13

Cisco Mobility Express AireOS® リリース 8.5

ソリューションの概要

Cisco Mobility Express ソリューションは、中小企業が簡単かつコスト効率よくエンタープライズクラスのワイヤレス アクセスを従業員や顧客に提供できるよう特別に設計されています。Cisco Mobility Express ソリューションを使用すれば、中小規模ネットワークで大企業と同じ品質のユーザ エクスペリエンスを体験できます。

Cisco Mobility Express ソリューションは、次のような特長を持つオンプレミス マネージド Wi-Fi ソリューションです。

- 802.11ac Wave 2 アクセス ポイントに組み込まれる仮想ワイヤレス LAN コントローラ機能
- 最大 100 台のアクセス ポイントまでの中小規模の導入に最適
- Cisco Aironet® 1540、1560、1815W、1815I、1815M、1830、1850、2800、および 3800 シリーズの 802.11ac Wave 2 アクセス ポイントでサポート
- 1810W、1700、2700、3700 などの他の Aironet® アクセス ポイントも管理可能
- 10 分以内でシンプルな Over-the-Air 展開ができ、さらに、ネットワーク プラグ アンド プレイを使用してワイヤレス LAN コントローラを展開し、新しいサイトで立ち上げが可能
- サイト サーベイに利用可能

相互運用性

- AireOS® リリース：AireOS® 8.4.100.0 以降を推奨。
- Cisco Prime Infrastructure：Prime Infrastructure リリース 3.0.1 以降。Mobility Express 上で実行される AireOS® リリースと互換性がある Prime Infrastructure バージョンを展開してください。
- Connected Mobility Experiences（CMX）：CMX Connect と CMX Presence Analytics がオンプレミス展開と CMX クラウド展開の両方でサポートされます。オンプレミスの場合は、CMX 10.3 以降を使用してください。Mobility Express 上で実行される AireOS® リリースと互換性がある CMX オンプレミス バージョンを展開してください。
- Cisco Identity Services Engine（ISE）：ISE リリース 1.2 以降。802.1x 認証をサポートします。

Mobility Express アクセス ポイント

Cisco Mobility Express ソリューションは次のコンポーネントで構成されます。

- **マスター アクセス ポイント**：仮想ワイヤレス LAN コントローラ機能を実行する Cisco Aironet® アクセス ポイントを、マスター AP と呼びます。仮想ワイヤレス LAN コントローラ機能を実行すると同時に、クライアントにサービスを提供することもできます。
- **従属アクセス ポイント**：Mobility Express ネットワークのマスター アクセス ポイントによって管理され、クライアントにサービスを提供するだけの Cisco Aironet® アクセス ポイントを、従属アクセス ポイントと呼びます。従属アクセス ポイントは、ワイヤレス LAN コントローラ機能を実行できる場合でもアクティブには実行しません。

アクセス ポイントがワイヤレス LAN コントローラ機能を実行できるようにする 2 つのパラメータがあります。これらのパラメータは、アクセス ポイントの **AP#show version** の出力に表示されます。リストの内容は次のとおりです。

- AP Image type
- AP Configuration

アクセス ポイントでワイヤレス LAN コントローラ機能を実行できるようにするには、2 つのパラメータに次の値を指定する必要があります。

- AP Image type：MOBILITY EXPRESS IMAGE
- AP Configuration：MOBILITY EXPRESS CAPABLE

（注）　CAPWAP イメージが動作するアクセス ポイントの場合、2 つのパラメーターは **AP#show version** の出力には表示されません。

マスター アクセス ポイント

仮想ワイヤレス LAN コントローラ機能を実行するマスター AP は、管理と制御の中心点です。次の表に、ワイヤレス LAN コントローラ機能を実行できるアクセス ポイントの一覧を示します。

表 13-1　マスター アクセス ポイントとして動作可能な Cisco Aironet® アクセス ポイント

マスター アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 1540 シリーズ	AIR-AP1540I-x-K9C AIR-AP1540D-x-K9C
Cisco Aironet® 1560 シリーズ	AIR-AP1562I-x-K9C AIR-AP1562E-x-K9C AIR-AP1562D-x-K9C
Cisco Aironet® 1815I シリーズ	AIR-AP1815I-x-K9C
Cisco Aironet® 1815M シリーズ	AIR-AP1815M-x-K9C
Cisco Aironet® 1815W シリーズ	AIR-AP1815W-x-K9C
Cisco Aironet® 1830 シリーズ	AIR-AP1832I-x-K9C

表 13-1　マスター アクセス ポイントとして動作可能な Cisco Aironet® アクセス ポイント

マスター アクセス ポイント	サポートされているモデル番号
Cisco Aironet® 1850 シリーズ	AIR-AP1852I-x-K9 AIR-AP1852E-x-K9
Cisco Aironet® 2800 シリーズ	AIR-AP2802I-x-K9 AIR-AP2802E-x-K9
Cisco Aironet® 3800 シリーズ	AIR-AP3802I-x-K9 AIR-AP3802E-x-K9

(注)　注:上記のモデル番号の「-x-」は、モデルの規制ドメインを示す実際の文字のプレースホルダです。

従属アクセス ポイント

従属アクセス ポイントは、Mobility Express ネットワークのマスター AP によって管理され、クライアントにサービスを提供するだけのアクセス ポイントです。従属 AP には 2 つのカテゴリがあります。最初のカテゴリはワイヤレス LAN コントローラ機能を実行できる一連の従属 AP で、2 番目のカテゴリはワイヤレス LAN コントローラ機能を実行できない一連の従属 AP です。次の表に、従属 AP として動作できるアクセス ポイントの一覧を示します。

表 13-2　従属アクセス ポイントと機能

従属アクセス ポイント	サポートされているモデル番号	機能
Cisco Aironet® 700i シリーズ	AIR-CAP702I-x-K9	Mobility Express の実行不可
Cisco Aironet® 700w シリーズ	AIR-CAP702W-x-K9	Mobility Express の実行不可
Cisco Aironet® 1540 シリーズ	AIR-AP1540I-x-K9 AIR-AP1540D-x-K9	Mobility Express の実行可
Cisco Aironet® 1560 シリーズ	AIR-AP1562I-x-K9 AIR-AP1562E-x-K9 AIR-AP1562D-x-K9	Mobility Express の実行可
Cisco Aironet® 1600 シリーズ	AIR-CAP1602I-x-K9 AIR-CAP1602E-x-K9	Mobility Express の実行不可
Cisco Aironet® 1700 シリーズ	AIR-CAP1702I-x-K9	Mobility Express の実行不可
Cisco Aironet® 1810 シリーズ	AIR-AP1810W-x-K9	Mobility Express の実行不可
Cisco Aironet® 1815I シリーズ	AIR-AP1815I-x-K9	Mobility Express の実行可

表 13-2　従属アクセス ポイントと機能

従属アクセス ポイント	サポートされているモデル番号	機能
Cisco Aironet® 1815M シリーズ	AIR-AP1815M-x-K9	Mobility Express の実行可
Cisco Aironet® 1815W シリーズ	AIR-AP1815W-x-K9	Mobility Express の実行可
Cisco Aironet® 1830 シリーズ	AIR-AP1832I-x-K9	Mobility Express の実行可
Cisco Aironet® 1850 シリーズ	AIR-AP1852I-x-K9 AIR-AP1852E-x-K9	Mobility Express の実行可
Cisco Aironet® 2600 シリーズ	AIR-CAP2602I-x-K9 AIR-CAP2602E-x-K9	Mobility Express の実行不可
Cisco Aironet® 2700 シリーズ	AIR-CAP2702I-x-K9 AIR-CAP2702E-x-K9	Mobility Express の実行不可
Cisco Aironet® 2800 シリーズ	AIR-AP2802I-x-K9 AIR-AP2802E-x-K9	Mobility Express の実行可
Cisco Aironet® 3600 シリーズ	AIR-CAP3602I-x-K9 AIR-CAP3602E-x-K	Mobility Express の実行不可
Cisco Aironet® 3700 シリーズ	AIR-CAP3702I-x-K9 AIR-CAP3702E-x-K9	Mobility Express の実行不可
Cisco Aironet® 3800 シリーズ	AIR-AP3802I-x-K9 AIR-AP3802E-x-K9	Mobility Express の実行可

（注） 上記のモデル番号の「-x-」は、モデルの規制ドメインを示す実際の文字のプレースホルダです。

スケール制限

Cisco Mobility Express では、単一の展開で最大 100 個のアクセス ポイントと最大 2000 台のクライアントがサポートされます。以下に、マスター アクセス ポイントごとの規模の制限を示します。

表 13-3　Cisco Mobility Express 規模の制限

マスター アクセス ポイント	サポートされるアクセス ポイントの数	サポートされるクライアントの数
Cisco Aironet® 1540 シリーズ	50	1000
Cisco Aironet® 1540 シリーズ	100	2000
Cisco Aironet® 1815I シリーズ	50	1000

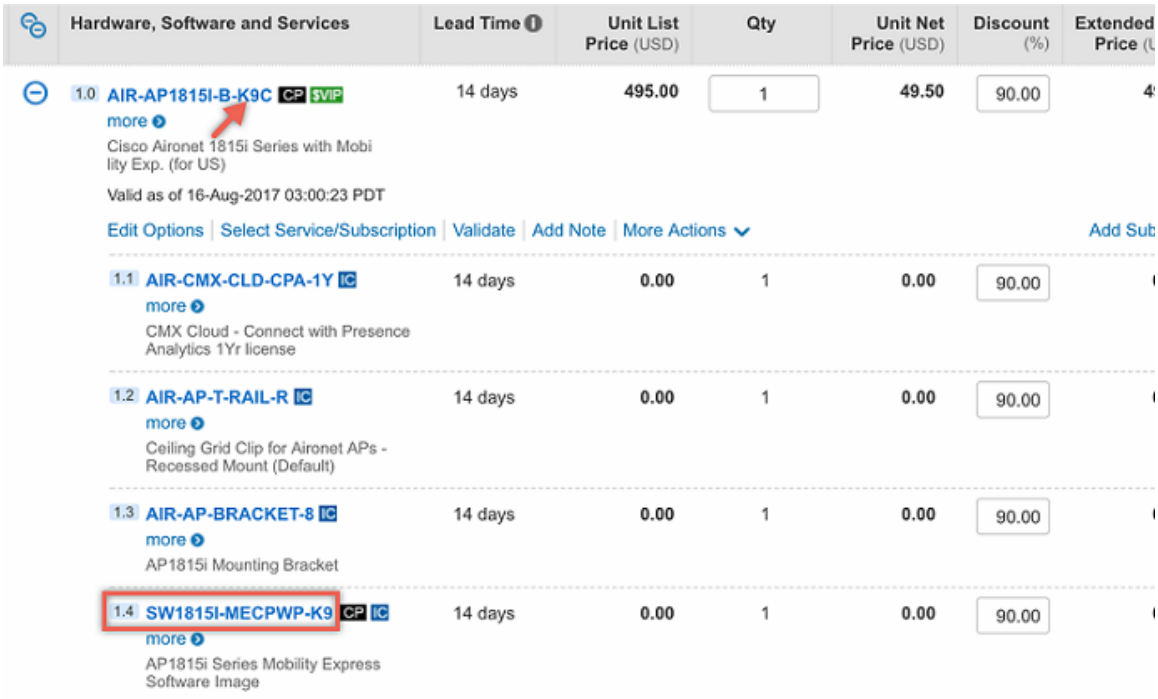
表 13-3　Cisco Mobility Express 規模の制限（続き）

マスター アクセス ポイント	サポートされるアクセス ポイントの数	サポートされるクライアントの数
Cisco Aironet® 1815M シリーズ	50	1000
Cisco Aironet® 1815W シリーズ	50	1000
Cisco Aironet® 1830 シリーズ	50	1000
Cisco Aironet® 1850 シリーズ	50	1000
Cisco Aironet® 2800 シリーズ	100	2000
Cisco Aironet® 3800 シリーズ	100	2000

Cisco Mobility Express によるアクセス ポイントの発注

ワイヤレス LAN コントローラを実行できるアクセス ポイントは、アクセス ポイントにプレインストールされている Cisco Mobility Express イメージを使用して発注できます。このようなアクセス ポイントを発注するには、発注時に SKU（最小在庫管理単位）名の末尾が「K9C」のアクセス ポイント SKU を選択してください。

たとえば（下の画像を参照）、-B 規制ドメインの 1815I アクセス ポイントを発注する場合は、AIR-AP1815I-B-**K9C** を選択します。オプションで、**SW1815I-MECPWP-K9**（Mobility Express ソフトウェア イメージ）も選択されていることを確認してください。



CAPWAP イメージが入っているアクセス ポイントを発注する場合は、発注時に末尾が「K9C」のアクセス ポイント SKU を選択しないでください。CAPWAP イメージが入っているアクセス ポイントを発注する場合は、発注時に SKU（最小在庫管理単位）名の末尾が「**K9**」の SKU を選択してください。

CAPWAP イメージが入っているアクセス ポイントは、Mobility Express イメージをインストールすることによってワイヤレス LAN コントローラ機能を実行できるアクセス ポイントに変換できることに注意してください。逆に、Mobility Express イメージを持つアクセス ポイントは、アプライアンスまたは vWLC ベースの展開に移行することで CAPWAP として動作するアクセス ポイントに変換できます。

Cisco Mobility Express の展開

Mobility Express イメージを持つアクセス ポイントを入手した後は、シンプルなプロセスによってアクセス ポイントにワイヤレス LAN コントローラを設定します。Cisco Mobility Express コントローラを設定する方法は複数あります。使用できる方法は次のとおりです。

1. CLI セットアップ ウィザード
2. Over-the-Air プロビジョニング セットアップ ウィザード
3. [ネットワークプラグアンドプレイ（Network Plug and Play）]

この章では、Over-the-Air プロビジョニング セットアップ ウィザードを使用してワイヤレス LAN コントローラを設定します。

前提条件

1. ワイヤレス LAN コントローラ機能が動作するマスター AP として設定するアクセス ポイントを決定します。設定が完了してマスター AP が動作可能になったら、その他の AP を Mobility Express ネットワークに追加できます。追加する AP のソフトウェア バージョンはマスター AP と同じでなければなりません。そうでない場合、AP はネットワークに参加できません。
2. DHCP サーバを決定します。アクセス ポイントとクライアントに外部 DHCP サーバ（スイッチやルータの DHCPサーバなど）を使用するか、Mobility Express 上の内部 DHCP サーバを使用するかを決定します。

（注）　内部 DHCP サーバと外部 DHCP サーバの併用はサポートされません。

外部 DHCP サーバを使用する場合は、マスター AP に接続する前にその DHCP サーバを最初に設定します。内部 DHCP サーバを使用する場合は、Day 0（初期設定）セットアップ ウィザードで設定できます。内部 DHCP サーバは一般にサイト サーベイに使用されます。そのため、特別な理由がない限り、アクセス ポイントとクライアントには外部 DHCP サーバを使用することを推奨します。

スイッチ ポートの設定

Mobility Express 展開では、マスター AP（クライアントへのサービスも提供）を含むアクセス ポイントによってすべてのクライアントが一元的に認証され、データ トラフィックがローカルにスイッチングされます。アクセス ポイントの接続先になるスイッチ ポートには、アクセス ポートまたはトランク ポートが使用できます。推奨はトランク ポートです。トランク ポートを使用すれば、管理トラフィックとクライアント データ トラフィックを別々の VLAN に分割できるからです。管理トラフィックとクライアント データ トラフィックを分割しない場合は、スイッチ ポートをアクセス ポートとして設定します。

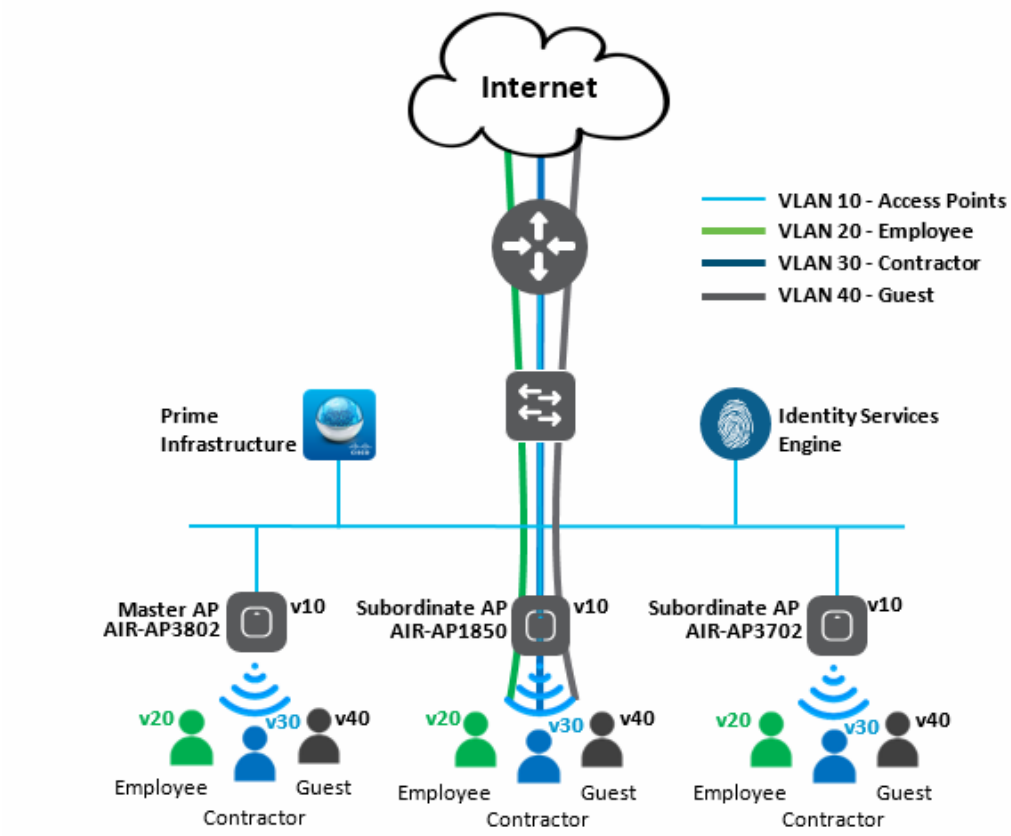
このガイドでは、外部 DHCP サーバを使用し、管理トラフィックとクライアント データ トラフィックに個別の VLAN を使用します。次に、アクセス ポイントのスイッチ ポートの設定例を示します。

```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk

interface GigabitEthernet1/0/38
description » Connected to Subordinate AP-Lobby«
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

上記の例では、すべてのアクセス ポイントがネイティブ VLAN 10 の IP アドレスを取得します。ワイヤレス LAN コントローラの管理 IP アドレスも VLAN 10 に割り当てられます。VLAN 10 は Day 0（初期設定）時に設定する必要があります。クライアント データ トラフィックは、VLAN 20、30、40 に割り当てられます。

（注）　Mobility Express 展開では、すべてのアクセス ポイントが同じ VLAN 内にいる必要があります。



アクセス ポイントのスイッチ ポートへの接続

指定されたマスター AP をスイッチ ポートに接続してください。スイッチ ポートが PoE + をサポートしている場合は、スイッチ ポートからアクセス ポイントに電力を供給できます。サポートしていない場合は、適切な電源か、パワー インジェクタを使用します。

アクセス ポイントは、起動時に DHCP 経由で IP アドレスを取得します。IP アドレスを取得した後、ワイヤレス LAN コントローラ機能が開始します。

ワイヤレス LAN コントローラ機能を実行できる複数のアクセス ポイントがスイッチ ポートに同時に接続されている場合、そのうちの 1 つが指定マスター AP に選ばれ、ワイヤレス LAN コントローラ機能が開始します。

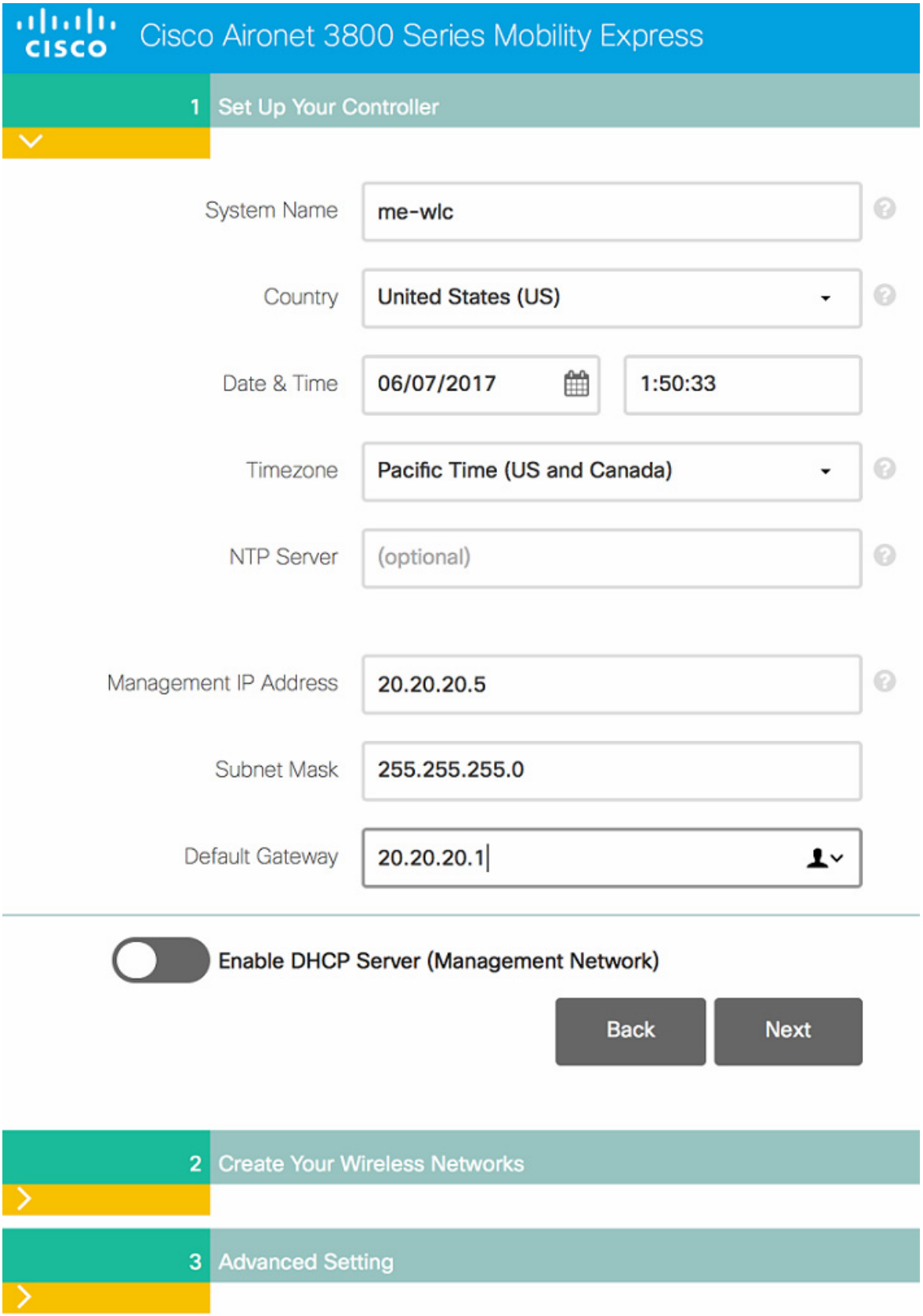
ワイヤレス LAN コントローラ機能が開始した後、**CiscoAirProvision** SSID をブロードキャストします。

マスター AP の設定

指定マスター AP でワイヤレス LAN コントローラを設定するには、次の手順に従います。

1. マスター AP を PoE 対応のスイッチ ポートに接続するか、外部電源を使用してマスター AP の電源をオンにします。
2. AP は、再起動を完了した後、CiscoAirProvision SSID をブロードキャストします。AP によっては、この処理に最大で 10 分かかる場合があります。
3. WiFi 対応 PC を CiscoAirProvision SSID に接続します。パスワードの入力を求められたら、「password」と入力します。
4. Web ブラウザを開き、mobilityexpress.cisco にアクセスしてセットアップ ウィザードに移動します。

5. ユーザ名とパスワードを入力して、ワイヤレス LAN コントローラの管理者アカウントを設定します。確認のためにパスワードをもう一度入力し、[開始] ボタンをクリックします。
6. [コントローラのセットアップ] セクションで、[システム] と [国] を入力します。[日時] はブラウザから自動的に入力されます。オプションで NTP サーバを入力することもできます。NTP サーバを空白のままにした場合、3 つの NTP プールが自動的に設定されます。[IP 管理] を有効にして、ワイヤレス LAN コントローラの [管理 IP アドレス]、[サブネット マスク]、[デフォルト ゲートウェイ] を入力します。DHCP サーバを有効にしないでください。この例では、外部 DHCP サーバを使用しているからです。[次へ] ボタンをクリックします。


Cisco Aironet 3800 Series Mobility Express
1 Set Up Your Controller
System Name
me-wlc
Country
United States (US)
Date & Time
06/07/2017
1:50:33
Timezone
Pacific Time (US and Canada)
NTP Server
(optional)
Management IP Address
20.20.20.5
Subnet Mask
255.255.255.0
Default Gateway
20.20.20.1
Enable DHCP Server (Management Network)
Back
Next
2 Create Your Wireless Networks
3 Advanced Setting

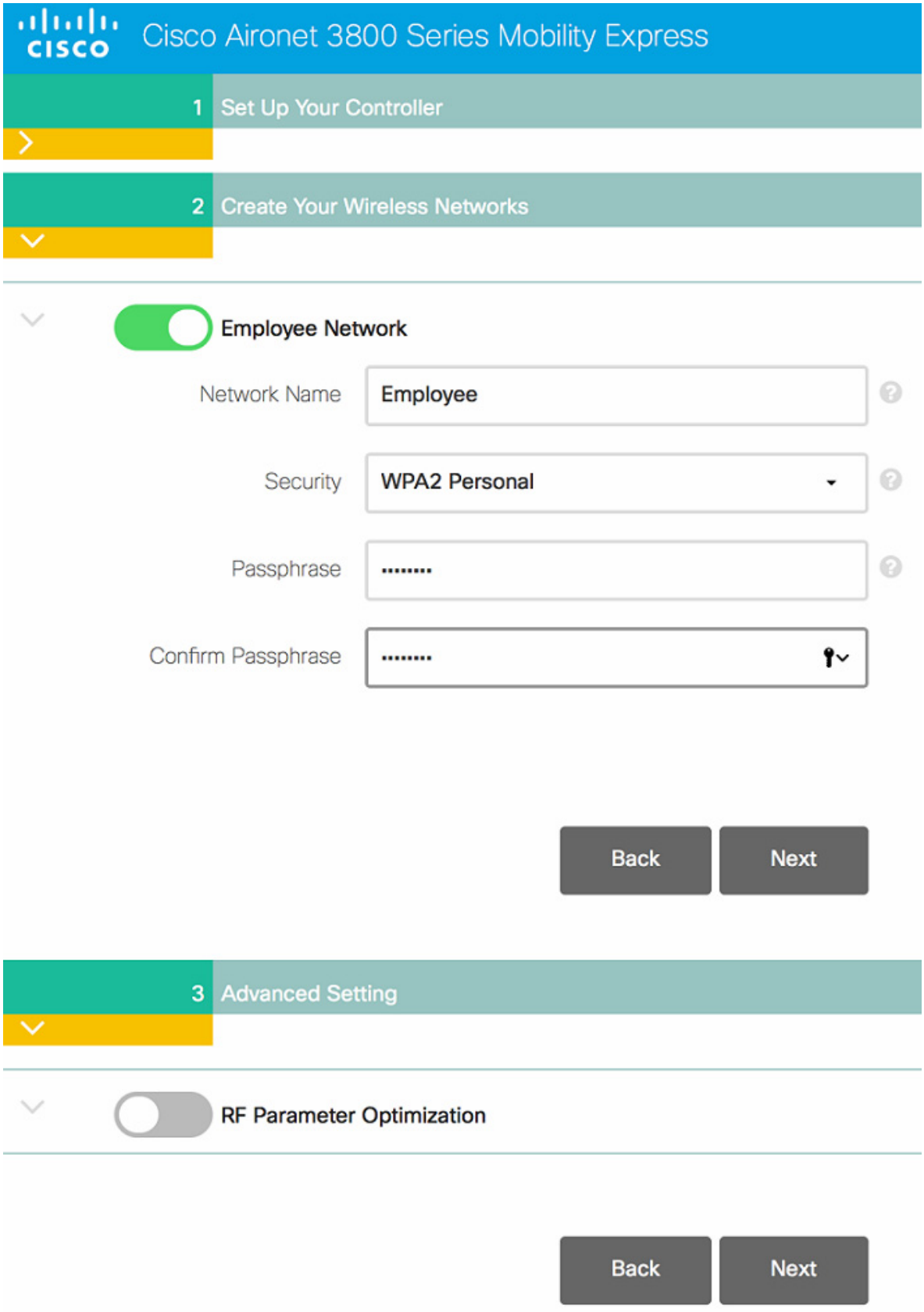
7. [ネットワーク名] を入力し、[セキュリティ] を選択して、従業員ネットワークを作成します。[WPA2 パーソナル] に、パスフレーズを 2 回入力します。[WPA2 エンタープライズ] に、RADIUS サーバの IP アドレスと共有秘密を入力します。

(注)　注: この時点では、WLAN クライアントはアクセス ポイントと同じネットワークに存在します。別の VLAN に WLAN クライアントを設定するには、[WLAN] セクションに進みます。

[次へ] をクリックします。

[詳細設定] で、[RF パラメータの最適化] を有効にします。展開の [クライアント密度] と [トラフィック タイプ] を選択します。

[次へ] をクリックします。

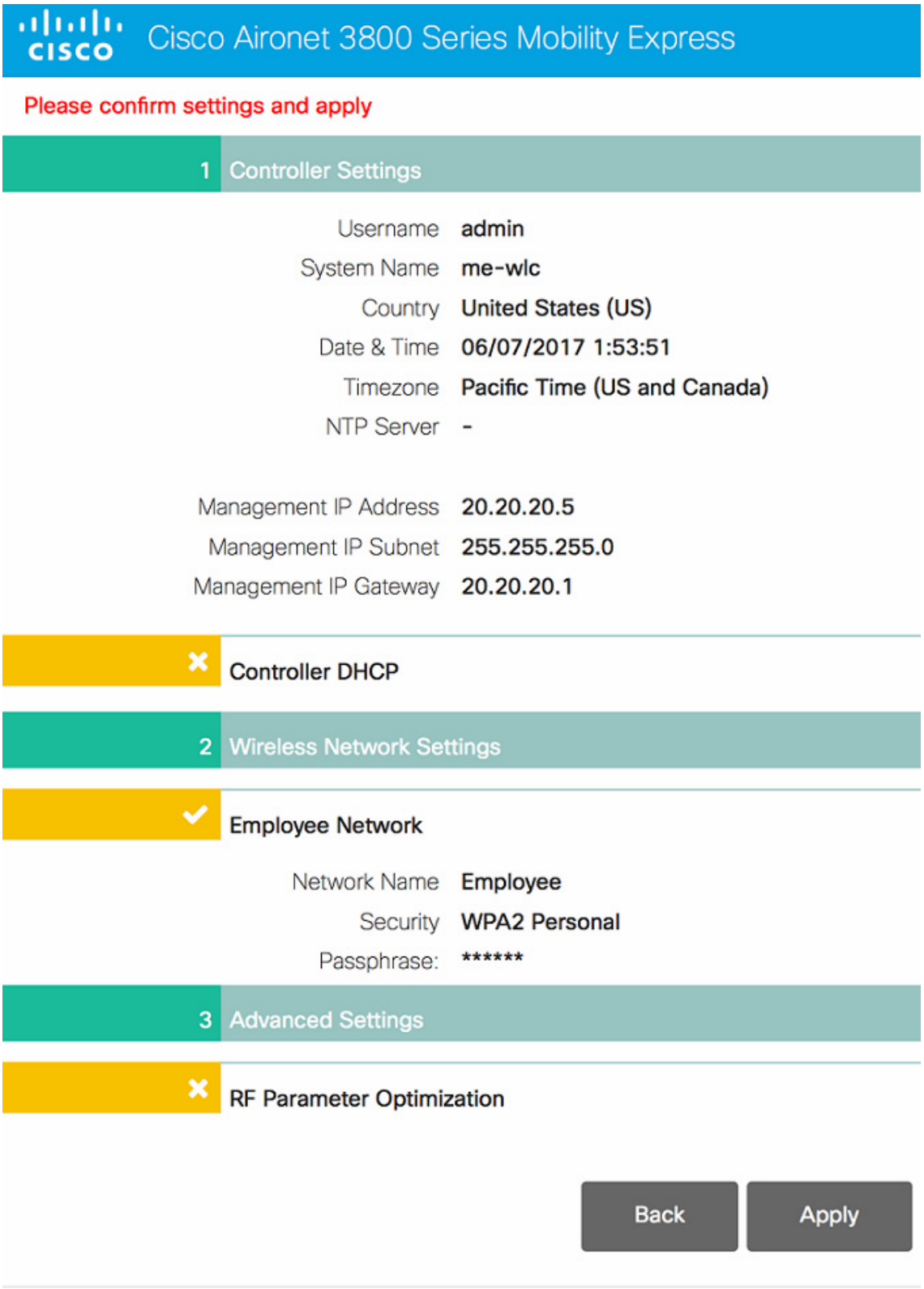

Cisco Aironet 3800 Series Mobility Express
1 Set Up Your Controller
2 Create Your Wireless Networks
Employee Network
Network Name
Employee
Security
WPA2 Personal
Passphrase
Confirm Passphrase
Back
Next
3 Advanced Setting
RF Parameter Optimization
Back
Next

8. 選択内容を確認して [適用] をクリックします。確認ウィンドウで [OK] をクリックします。

マスター AP が再起動して稼働状態に戻り、ワイヤレス コントローラ機能を実行します。

Web ブラウザを使用して、コントローラの WebUI（https://<管理 IP アドレス>）にアクセスします。管理 IP アドレスは上記の手順 6 で設定されていることに注意してください。

コントローラの WebUI インターフェイスにログインするには、[ログイン] をクリックして、上記の手順 5 で設定したユーザ名とパスワードを入力します。


Cisco Aironet 3800 Series Mobility Express
Please confirm settings and apply
1 Controller Settings
Username admin
System Name me-wlc
Country United States (US)
Date & Time 06/07/2017 1:53:51
Timezone Pacific Time (US and Canada)
NTP Server -
Management IP Address 20.20.20.5
Management IP Subnet 255.255.255.0
Management IP Gateway 20.20.20.1
Controller DHCP
2 Wireless Network Settings
Employee Network
Network Name Employee
Security WPA2 Personal
Passphrase: ******
3 Advanced Settings
RF Parameter Optimization
Back
Apply

Cisco Mobility Express の内部 DHCP サーバの設定

リリース 8.3.102.0 以降では、内部 DHCP サーバを有効にしてアクセス ポイントと WLAN のスコープを作成できます。Cisco Mobility Express では合計 17 個の DHCP スコープがサポートされています。また、内部 DHCP サーバを使用すると、外部 DHCP サーバなしで Cisco Mobility Express によるサイト サーベイを実行することもできます。

(注)　内部 DHCP サーバと外部 DHCP サーバの併用は、集中型 NAT のユースケースでサポートされます。

Cisco Mobility Express のサイト サーベイ用の設定

Cisco 802.11ac Wave 2 アクセス ポイントは、アクセス ポイントに組み込まれる仮想ワイヤレス コントローラ機能である Cisco Mobility Express を実行できます。Cisco Mobility Express では、アクセス ポイントをサイト サーベイに使用できるようにする内部 DHCP サーバもサポートされます。

前提条件

1. アクセス ポイント：Cisco Mobility Express ソフトウェアを実行している Cisco 802.11ac Wave 2 アクセス ポイント
2. 電源：サイト サーベイに使用するアクセス ポイントに応じて、電源アダプタまたはアクセス ポイントに十分な電力を供給できるバッテリ パックを使用
3. コンソール ケーブル（オプション）：Cisco Mobility Express は、CLI または Over-the-Air を使用して設定できます。CLI を使用して Cisco Mobility Express を設定するには、アクセス ポイントへのコンソール接続が必要

手順

ステップ 1　アクセス ポイントのコンソールに接続します。

ステップ 2　電源アダプタまたはバッテリ パックを使用してアクセス ポイントの電源をオンにします。

ステップ 3　アクセス ポイントが完全に起動してワイヤレス コントローラ機能を実行するまで待機します。

ステップ 4　CLI セットアップ ウィザードを使用してワイヤレス コントローラを設定します。

(注)　サイト サーベイでは、DHCP サーバが必要です。DHCP サーバは Cisco Mobility Express でサポートされています。以下に強調表示されている DHCP サーバの設定は、Cisco Mobility Express の DHCP サーバを有効にするために必須です。

```
Would you like to terminate autoinstall? [yes]:yes
Enter Administrative User Name (24 characters max):admin
Enter Administrative Password (3 to 24 characters max):Cisco123
Re-enter Administrative Password: Cisco123
System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc
Enter Country Code list(enter 'help' for a list of countries)[US]:US
Configure a NTP server now?[YES][no]:no
Configure the system time now?[YES][no]:yes
Enter the date in MM/DD/YY format:02/28/17
```

```
Enter the time in HH:MM:SS format:11:30:00
Enter timezone location index(enter 'help' for a list of timezones):5
Management Interface IP Address: 10.10.10.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Create Management DHCP Scope?[yes][NO]:yes
DHCP Network: 10.10.10.0
DHCP Netmask: 255.255.255.0
Router IP: 10.10.10.1
Start DHCP IP address: 10.10.10.10
Stop DHCP IP address: 10.10.10.250
DomainName: mewlc.local
DNS Server:[OPENDNS][user DNS]OPENDNS
Create Employee Network?[YES][no]:yes
Employee Network Name(SSID)?:site_survey
Employee VLAN Identifier?[MGMT][1-4095]:MGMT
Employee Network Security?[PSK][enterprise]:PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]:NO
Enable RF Parameter Optimization?[YES][no]:no
Configuration correct? If yes, system will save it and reset.[yes][NO]:yes
```

ステップ 5　アクセス ポイントが完全に起動するまで待ちます。ワイヤレス コントローラ機能が実行された後で、初期セットアップ ウィザード中に設定した管理ユーザ名またはパスワードを使用してコントローラに再度ログインします。

ステップ 6　（オプション）:CLI のセットアップ ウィザード中に、従業員ネットワーク セキュリティは、PSK に設定されています。これにより、クライアントの簡単な接続を無効にできます。不必要なクライアントが SSID に接続しないように SSID ブロードキャストを無効にすることもできます。PSK と SSID ブロードキャストを無効にするには、コントローラ CLI で次のコマンドを入力します。

```
(Cisco Controller)>config wlan disable 1
(Cisco Controller)>config wlan security wpa disable 1
(Cisco Controller)>config wlan broadcast-ssid disable wlan 1
(Cisco Controller)>config wlan enable 1
(Cisco Controller)>save config
```

ステップ 7　チャネル、送信出力、および Radio のチャネル幅を設定するには、最初に Radio を無効にして、変更を行ってから再度有効にします。

2.4GHz の Radio をチャネル 6 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b channel <ap name> <ap name> 6
(Cisco Controller)>config 802.11b enable <ap name>
```

2.4 GHz の Radio 送信出力をレベル 3 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11b disable <ap name>
(Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3
(Cisco Controller)>config 802.11b enable <ap name>
```

5 GHz の Radio をチャネル 44 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a channel <ap name> <ap name> 44
(Cisco Controller)>config 802.11a enable <ap name>
```

5 GHz の Radio 送信出力をレベル 5 に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5
(Cisco Controller)>config 802.11a enable <ap name>
```

5 GHz の Radio チャンネル幅を 40 MHz に変更するには、次の手順を実行します。

```
(Cisco Controller)>config 802.11a disable <ap name>
(Cisco Controller)>config 802.11a chan_width <ap name> 40
(Cisco Controller)>config 802.11a enable <ap name>
```

2800 および 3800 シリーズ アクセス ポイントをサイト サーベイに使用する場合は、XOR 無線に関する次の点に注意してください。

- XOR 無線のデフォルトの動作状態は 2.4 GHz です。
- 2.4 GHz から 5 GHz へアンテナ内蔵アクセス ポイントの XOR Radio の設定を変更できます。また、その逆も可能です。外付け（E）アンテナのアクセス ポイントでは、XOR 無線の設定を変更する前に、外部アンテナを DART コネクタに接続する必要があります。
- XOR（2.4 GHz）無線が 5 GHz で動作するように設定されている場合は、5 GHz 専用のラジオから 100 MHz 周波数を分離する必要があります。
- 内部（I）アクセス ポイントで XOR 無線が 5 GHz モードで動作するように設定されている場合は、送信電力（Tx）が固定され、変更できません。

2800 および 3800 シリーズ アクセス ポイントで XOR（2.4 GHz）無線が 5 GHz で動作するように設定するには、次の手順を実行します。

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn role ap manual client-serving
(Cisco Controller) >config 802.11-abgn band ap ap 5GHz
(Cisco Controller) >config 802.11-abgn enable ap
```

5 GHz で動作している XOR 無線をチャネル 40 に設定するには、次の手順を実行します。

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn channel ap ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```

5 GHz チャネル幅で動作している XOR 無線を 40 MHz に設定するには、次の手順を実行します。

```
(Cisco Controller) >config 802.11-abgn disable ap
(Cisco Controller) >config 802.11-abgn chan_width ap 40
(Cisco Controller) >config 802.11-abgn enable ap
```

Day 1（Day 0 の後）での DHCP スコープの作成

内部 DHCP サーバを有効にし、Day 0 時にセットアップ ウィザード、および Day 1 にコントローラの WebUI を使用して、DHCP スコープを作成できます。コントローラの WebUI を使用してスコープを作成し、WLAN に関連付けるには、次の手順を実行します。

手順

ステップ 1　[ワイヤレス設定] > [DHCP サーバ] に移動して、[新規プールの追加] ボタンをクリックします。

ステップ 2　[DHCP プールの追加] ウィンドウで、次のフィールドに入力します。

- WLAN のプール名を入力します。
- プール ステータスを有効にします。
- WLAN の VLAN ID を入力します。
- DHCP クライアントのリース期間（Lease Period）を入力します。デフォルトは 1 日（86,400秒）です。
- ネットワーク/マスクを入力します。
- DHCP プールの開始 IP を入力します。

- DHCP プールの終了 IP を入力します。
- DHCP プールのデフォルト ゲートウェイを入力します。

（注）　スコープの対象が集中型 NAT に接続するクライアントである場合は、[デフォルト ゲートウェイ] で [Mobility Express コントローラ] を選択する必要があります。

- DHCP プールのドメイン名（オプション）を入力します。
- ネーム サーバの IP アドレスを入力する必要がある場合は、[ネーム サーバ] で [ユーザ定義] を選択します。[OpenDNS] を選択すると、OpenDNS ネーム サーバの IP アドレスが自動的に入力されます。

ステップ 3　[適用] をクリックします。

ステップ 4　スコープを作成したら、DHCP スコープにマップされている VLAN を WLAN に割り当てます。WLAN に VLAN を割り当てるには、[ワイヤレス設定] > [WLAN] に移動します。

ステップ 5　WLAN が存在しない場合は、WLAN を作成します。WLAN が存在する場合は、既存の WLAN を編集し、[VLAN とファイアウォール] タブをクリックします。

ステップ 6　[VLAN とファイアウォール] タブで、次のように設定します。

- [クライアント IP の管理] がこの範囲の場合は、[ネットワーク（デフォルト）] を選択します。そうでない場合は、[Mobility Express コントローラ] を選択します。
- 集中型 NAT 化している WLAN である場合は、[Mobility Express コントローラ] を選択します。
- [VLAN タギングを使用する] で [はい] を選択します。
- ネイティブ VLAN ID を入力します。
- 以前に WLAN 用に作成された DHCP スコープを選択します。VLAN ID は、DHCP スコープを選択すると自動的に入力されます。

ステップ 7　[適用] をクリックします。

ワイヤレス ネットワークの作成

Cisco Mobility Express ソリューションでは、最大で 16 個の WLAN がサポートされます。各 WLAN には、一意の WLAN ID（1 ～ 16）、一意のプロファイル名、SSID が割り当てられます。また、異なるセキュリティ ポリシーを割り当てることもできます。

アクセス ポイントは、すべてのアクティブな WLAN SSID をブロードキャストし、WLAN ごとに定義されたポリシーを適用します。必要に応じて、個々の WLAN で SSID ブロードキャストを無効にできます。WLAN では、QoS、Application Visibility and Control、ローカル プロファイリングがサポートされます。さらに、802.11k、802.11r、802.11v、ファストレーンもサポートされます。

Cisco Mobility Express ソリューションでは、多数の WLAN セキュリティ オプションがサポートされています。次にその概要を示します。

1. Open
2. WPA2 パーソナル
3. WPA2 エンタープライズ（外部 RADIUS、AP）

（注）　AP はマスター AP を表し、認証はコント ローラーによって行われます。

ゲスト WLAN 向けに、次のような多数の機能がサポートされています。

1. CMX ゲスト接続
2. 内部スプラッシュ ページ
3. 外部スプラッシュ ページ

内部および外部のスプラッシュ ページ向けに、多数のアクセス タイプがサポートされています。リストの内容は次のとおりです。

a. ローカル ユーザ アカウント
b. Web 許諾
c. 電子メール アドレス
d. RADIUS
e. WPA2 パーソナル

(注)　RADIUS を使用した MAC フィルタリングやローカル WLC データベースもサポートされています。

WPA2 エンタープライズ/外部 RADIUS と MAC フィルタリングを備えた従業員 WLAN の作成

手順

ステップ 1　[ワイヤレス設定] > [WLAN] に移動して、[新規 WLAN の追加] ボタンをクリックします。[新規 WLAN の追加] ウィンドウが表示されます。

ステップ 2　[新規 WLAN の追加] ウィンドウの [一般] タブで、次のように設定します。

- プロファイル名を入力します。
- SSID を入力します。

ステップ 3　[WLAN セキュリティ] タブをクリックして、次のように設定します。

- [セキュリティ タイプ] で [WPA2 エンタープライズ] を選択します。
- [認証サーバ] で [外部 RADIUS] を選択します。
- [RADIUS 互換性] をドロップダウン リストから選択します。
- [MAC デリミタ] をドロップダウン リストから選択します。

ステップ 4　Radius サーバを追加して、次のように設定します。

- RADIUS IP を入力します
- RADIUS ポートを入力します
- 共有秘密を入力します。
- [適用] をクリックします。

ステップ 5　[適用] をクリックします。

CMX Connect 上にキャプティブ ポータルがあるゲスト WLAN の作成

手順

ステップ 1　[ワイヤレス設定] > [WLAN] に移動して、[新規 WLAN の追加] ボタンをクリックします。[新規 WLAN の追加] ウィンドウが表示されます。

ステップ 2　[新規 WLAN の追加] ウィンドウの [一般] タブで、次のように設定します。

- プロファイル名を入力します。
- SSID を入力します。

ステップ 3　[WLAN セキュリティ] タブで [ゲスト ネットワーク] を有効にします。

ステップ 4　[キャプティブ ポータル] で [CMX コネクト] を選択します。

ステップ 5　キャプティブ ポータル URL を入力します。

（注）　キャプティブ ポータルの URL は、https://yya7lc.cmxcisco.com/visitor/login の形式で入力する必要があります。「yya7lc」はご使用のアカウント ID です。

ステップ 6　ゲスト クライアントを別の VLAN 上に配置する必要がある場合は、[VLAN とファイアウォールl] タブをクリックし、[VLAN タギングを使用する] で [はい] を選択して次の情報を入力します。

- ネイティブ VLAN を入力します。これは AP の VLAN です。
- [VLAN ID] フィールドに、ゲスト クライアントの VLAN を入力します。

（注）　ゲスト VLAN はスイッチ ポートに設定する必要があります。

ステップ 7　[適用] をクリックします。

（注）　キャプティブ ポータルと、アクセス ポイントがあるサイトを作成し、そのキャプティブ ポータルとサイトを関連付けるには、CMX クラウドで追加の手順が必要になります。

ワイヤレス ネットワークの作成

Cisco Mobility Express コントローラのソフトウェア アップデートは、コントローラの Web インターフェイスを使用して実行できます。ソフトウェア アップデートによって、コントローラと、すべての従属しているアクセスポイントの両方の更新が保証されます。

コントローラに新たに参加する AP は、そのソフトウェアのバージョンとマスター AP のバージョンを比較し、一致しない場合は、ソフトウェア アップデートを要求します。ソフトウェア アップデートを実行するには、[ソフトウェア アップデート] ページで転送モードと対応する詳細を設定する必要があります。

（注）　マスター AP には、AP イメージはありません。マスター AP は、設定された転送モードからソフトウェア アップデートを要求しているアクセス ポイントへの新しいソフトウェアの転送を円滑化します。

Cisco Mobility Express のソフトウェア アップデートでは、次の転送モードがサポートされます。

1. Cisco.com：このソフトウェア アップデート方式では、ソフトウェア イメージを cisco.com から個々のアクセス ポイントに直接ストリーム配信できます。この転送モードでは、インターネット アクセスが必要で、ソフトウェアのダウンロードを開始する前に、EULA と SMARTNet の契約要件が満たされていなければなりません。
2. HTTP：Mobility Express ネットワークにある各アクセス ポイントのモデルが同一で、ユーザがローカル マシンから AP ファイルを使用できる場合は、HTTP 転送モードがサポートされます。

(注)　Mobility Express ネットワークで異なるモデルのアクセス ポイントが混在している場合は、cisco.com または TFTP 転送方式によるソフトウェア アップデートを使用する必要があります。

3. TFTP：Mobility Express ネットワークでは、TFTP 転送モードを使用してソフトウェア アップデートを実行できます。マスター AP は、TFTP サーバから個々のアクセス ポイントへのイメージの転送を円滑化します。AP のイメージは、要求に応じて TFTP サーバから保存および提供されます。

(注)　イメージの事前ダウンロード中にサービスが中断されることはありません。すべての AP でプレイメージのダウンロードが完了したら、Mobility Express ネットワークの再起動は、手動またはスケジュールをトリガーにできます。

cisco.com 転送モードを使用したソフトウェア アップデート

cisco.com 転送モードを使用したソフトウェア アップデート

Cisco.com によるソフトウェア アップデートは、Cisco Mobility Express 導入でサポートされているすべてのアクセス ポイントで動作します。cisco.com からのソフトウェア アップデートを開始するには、次の要件が満たされている必要があります。

- cisco.com から AP にソフトウェアをダウンロードするにはインターネット アクセスが必要
- ユーザ名とパスワードが設定された有効な cisco.com（CCO）アカウントが必要
- ユーザごとの EULA の承諾。マスター AP（ネットワーク内のすべての AP ではありません）が SMARTNet 契約を保持している必要があります。そうでない場合、ソフトウェア アップデートは開始されません。

cisco.com 転送モードを使用してソフトウェア アップデートを実行するには、次の手順を実行します。

手順

ステップ 1　Cisco.com 経由のソフトウェア アップデートを実行するには、[管理] > [ソフトウェア アップデート] に移動して次のように設定します。

- [転送モード] で [Cisco.com] を選択します。
- Cisco.com のユーザ名を入力します。
- Cisco.com のパスワードを入力します。

- [自動的に更新をチェック] を有効にします。確認は、30 日に一度行われます。
- Cisco.com から最新のソフトウェア リリースと推奨されるソフトウェア リリースを取得するには、[今すぐチェック] ボタンをクリックします。

ステップ 2　[Save] をクリックします。

ステップ 3　[更新] ボタンをクリックしてソフトウェア アップデート ウィザードを起動します。

ステップ 4　ソフトウェア アップデート ウィザードで、推奨されるソフトウェア リリースまたは最新のソフトウェア リリースを選択します。[次へ] をクリックします。

ステップ 5　すぐにソフトウェア アップデートを開始する場合は、[いますぐ更新] を選択します。または、[Schedule the Update for Later] を選択します。

（注）　[Schedule the Update for Later] を選択した場合は、[更新時間の設定] フィールドを設定します。

ステップ 6　ソフトウェア アップデートが完了した後にネットワーク内のすべてのアクセス ポイントを自動的に再起動する場合は、[自動再起動] チェックボックスをオンにします。[次へ] をクリックします。

ステップ 7　[確認 ボタンをクリックしてソフトウェア アップデートを開始します。

個々のアクセス ポイントでダウンロードの進行状況をモニタするには、[イメージの事前ダウンロードのステータス] を展開します。

高度な RF パラメーターの管理

Cisco Mobility は、管理者が設定できるいくつかの RF パラメータをサポートして、ネットワークの導入を最適化します。高度な RF パラメーターを管理するには、次の手順を実行します。

ステップ 1　Cisco Mobility Express でエキスパート ビューを有効にします。エキスパート ビューは、次に示すように、Cisco Mobility Express WebUI のトップ バナーからアクセスできます。エキスパート ビューでは、標準ビューでは使用できないさまざまなパラメータを設定できます。

ステップ 2　[RF の詳細パラメータ] には、次のパラメータがあります。

- [2.4 GHz 帯]: これはグローバル設定で、有効または無効にできます。
- [5.0 GHz 帯]: これはグローバル設定で、有効または無効にできます。
- [自動のフレキシブル ラジオ アサインメント]: フレキシブル ラジオ アサインメントをサポートする Cisco Mobility Express 展開に 2800 および 3800 シリーズのアクセス ポイントがある場合、ユーザはこのパラメータを有効または無効にできます。
- [イベント駆動型 RRM]: これはグローバル設定で、有効または無効にできます。
- [CleanAir 検出]: CleanAir は、2800 および 3800 シリーズのアクセス ポイントでサポートされます。ユーザはこのパラメータを有効または無効にできます。
- [5.0 GHz チャネル幅]: グローバル設定で、最良が設定されていますが、20、40、80、160 MHz のチャネル幅も選択できます。

- [2.4 GHz データ レート]: スライダを動かして、2.4 GHz 帯域のデータ レートを無効/有効にします。
- [5.0 GHz データ レート]: スライダを動かして、5.0 GHz 帯域のデータ レートを無効/有効にします。
- [DCA チャネルの選択]: 2.4 GHz と 5.0 GHz の両方の帯域の DCA に含めるチャネルを選択できます（個々のチャネルをクリック）。

(注)　下線の付いた緑色のチャネルは、そのチャネルが選択されていることを示します。

ステップ 3　[適用] をクリックします。

フェールオーバーと復元力

Cisco Mobility Express は、Cisco 1560、1815I、1815M、1815W、1830、1850、2800、および 3800 シリーズのアクセス ポイントでサポートされます。Cisco Mobility Express 環境でこれらのアクセス ポイントが混在している場合、マスター AP の選択プロセスは、アクティブ マスター AP のフェールオーバー時にどのアクセスポイントが（Mobility Express コントローラ機能を実行するために）選択されるかを決定します。VRRP は、新しいマスターの選択のため、マスター AP の障害を検出するために使用されます。

(注)　Mobility Express は、MAC 00-00-5E-00-01-VRID を使用します。VRID は 1 です。したがって、環境内でその他の VRRP インスタンスを実行している場合は、それらのインスタンスに 1 以外の VRID を使用してください。

新しいマスターの選出

マスターの選出プロセスは、一連の優先順位に基づいています。アクティブなマスター アクセス ポイントで障害が発生すると、選択プロセスが開始され、優先度が一番高いアクセス ポイントがマスター AP として選択されます。

マスター選択プロセス中に、コントローラの機能を実行しているマスター AP がダウンしていても、残りのアクセス ポイントは、スタンドアロン モードになり、接続しているクライアントとデータ トラフィックをローカルに処理し続けます。新しいマスターが選択された後で、スタンドアロン アクセス ポイントはコネクテッド モードに移行します。

前述のように、マスター アクセス ポイントの選択は、一連の優先度に基づいています。優先順位は次のとおりです。

1. ユーザ定義マスター: ユーザはマスター アクセス ポイントにするアクセス ポイントを選択できます。このような選択を行った場合、アクティブなマスターに障害が発生しても新しいマスターは選出されません。5 分後も現在のマスターがアクティブでない場合は、故障していると想定され、新しいマスターの選択を開始します。マスターを手動で定義するには、次の手順を実行します。

手順

ステップ 1　[ワイヤレスの設定] > [アクセス ポイント] に移動します。

ステップ 2　アクセス ポイントのリストで、マスター AP として選択するアクセス ポイントの [Edit] アイコンをクリックします。

ステップ 3　[一般] タブで、[Make me Controller] ボタンをクリックします。

ステップ 4　確認ウィンドウで、[はい] をクリックします。

（注）　前のマスターが再起動し、選択したアクセス ポイントがすぐにコントローラを起動してアクティブなマスターになります。

2. 次優先マスター：管理者は CLI から次優先マスターを設定できます。次優先マスターが設定されていて、アクティブなマスター AP で障害が発生した場合、次優先マスターとして設定されたアクセス ポイントがマスターとして選出されます。次優先マスターを設定するには、次の手順を実行します。

手順

ステップ 1　コントローラの CLI にログインします。

ステップ 2　次の CLI コマンドを実行します。

次優先マスターを設定するには、次の CLI コマンドを実行します。

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
<Cisco AP> Enter the name of the Cisco AP
```

次優先マスターを表示するには、次の CLI コマンドを実行します。

```
(Cisco Controller) >show ap next-preferred-master
```

次優先マスターをクリアするには、次の CLI コマンドを実行します。

```
Cisco Controller) >clear ap next-preferred-master
```

3. 最も能力の高いアクセス ポイント：最初の 2 つの優先順位が設定されていない場合、マスター AP 選出アルゴリズムでは、アクセス ポイントの能力に基づいて新しいマスターが選出されます。たとえば、最も能力が高いのは 3800 で、2800、1850、1830 がそれに続き、最も能力が低いのは 1815 シリーズです。

（注）　1815 シリーズ アクセス ポイントの能力はどれも同じです。

4. 最も小さいクライアント負荷：同じ能力を持つアクセス ポイント、つまり 3800 アクセス ポイントが複数存在する場合は、クライアント負荷が最も小さいアクセス ポイントがマスター アクセス ポイントとして選出されます。
5. 最も小さい MAC アドレス：すべてのアクセス ポイントが同一で、クライアント負荷も同じである場合は、MAC が最も小さいアクセス ポイントがマスターとして選出されます。

Mobility Express では、UWNC コントローラでサポートされるさまざまな機能がサポートされます。各リリースでサポートされる機能の一覧については、次のリンクを参照してください。
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-5/b_Mobility_Express_FlexConnect_Feature_Matrix.html