エンタープライズ モビリティ 7.3 デザイン ガイド

Cisco Validated Design

改訂日：2013 年 6 月 21 日

Text Part Number: OL-14435-01-J

Cisco Validated Design

Cisco Validated Design プログラムは、お客様による信頼性の高い、確実かつ速やかな展開を容易にするために、デザイン、テスト、および文書化されたシステムおよびソリューションで構成されています。詳細については、www.cisco.com/go/validateddesigns をご覧ください。

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）は、障害も含めて本マニュアル作成時点のものです。シスコおよびそのサプライヤは、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、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、シスコおよびそのサプライヤは、このデザイン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サプライヤ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。

デザイン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デザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコ、そのサプライヤ、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

はじめに xv
本書の目的 i-xv
対象読者 i-xv
マニュアルの構成 i-xv

CHAPTER 1 Cisco Unified Wireless Network ソリューションの概要 1-1
WLAN の概要 1-1
WLAN ソリューションのメリット 1-1
WLAN システムの要件 1-2
Cisco Unified Wireless Network 1-5

CHAPTER 2 Cisco Unified Wireless のテクノロジーおよびアーキテクチャ 2-1
CAPWAP の概要 2-1
スプリット MAC 2-3
レイヤ 3 トンネル 2-5
WLC ディスカバリおよび選択 2-8
CAPWAP AP のリセット 2-8
コア コンポーネント 2-9
Cisco ワイヤレス LAN コントローラ 2-9
Cisco アクセス ポイント 2-12
CAPWAP AP 2-12
Cisco Prime Infrastructure 2-13
モビリティ グループ、AP グループ、および RF グループ 2-13
モビリティ グループ 2-14
モビリティ グループの定義 2-14
モビリティ グループの用途 2-15
モビリティ グループの例外 2-15
AP グループ 2-15
RF グループ 2-17
ローミング 2-17
WLC でのブロードキャストおよびマルチキャスト 2-21
WLC ブロードキャストおよびマルチキャストの詳細 2-22
DHCP 2-22
VideoStream 2-23

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 2-23
設計上の考慮事項 2-23
WLC のロケーション 2-23
分散型の WLC 展開 2-24
中央集中型の WLC 展開 2-24
WLC の中央集中化 2-25
分散型の WLC ネットワーク接続 2-26
トラフィックの負荷と有線ネットワークのパフォーマンス 2-27
CAPWAP コントロール トラフィックのボリューム 2-27
トンネリングによって生じるオーバーヘッド 2-27
トラフィック エンジニアリング 2-27
AP 接続 2-28
運用および保守 2-28
WLC ディスカバリ 2-28
AP 分散 2-28

CHAPTER 3 WLAN RF の設計に関する考慮事項 3-1
RF の基礎 3-1
規制区域 3-1
動作周波数 3-2
2.4 GHz : 802.11b/g/n 3-2
5 GHz : 802.11a/n/ac 3-2
導入に関する考慮事項 3-2
IEEE 802.11 規格について 3-4
ダイレクト シーケンス スペクトラム拡散方式（DSSS） 3-5
IEEE 802.11b ダイレクト シーケンス（DS）チャネル 3-6
IEEE 802.11g 3-6
IEEE 802.11a OFDM の物理レイヤ 3-7
IEEE 802.11a のチャネル 3-7
RF 電力の用語 3-7
dB 3-8
dBi 3-8
dBm 3-8
実効等方放射電力（EIRP） 3-8
RF 導入の計画 3-9
オーバーラップする WLAN カバレッジのさまざまな導入の種類 3-10
データ専用の導入 3-10
音声導入 3-10
ロケーション ベース サービスの導入 3-12

WLAN のデータ レート要件 3-13
カバレッジ エリアに対するデータ レート 3-13
異なるデータ レートに対する AP の密度 3-14
クライアント密度とスループット要件 3-16
WLAN のカバレッジ要件 3-17
電力レベルとアンテナの選択 3-18
全方向性アンテナ 3-18
パッチ アンテナ 3-19
ダイポール アンテナ 3-20
セキュリティ ポリシー要件 3-21
RF 環境 3-21
RF 導入のベスト プラクティス 3-22
WLAN カバレッジの手動による微調整 3-22
チャネルおよびデータ レートの選択 3-23
チャネルの選択に関する推奨事項 3-23
手動でのチャネル選択 3-24
データ レートの選択 3-25
データ レート モード 3-26
最低および最高の必須レートの設定 3-27
無線リソース管理（Radio Resource Management） 3-27
RRM 動作の概要 3-28
RRM コンフィギュレーションの設定 3-29
サンプルの「show ap auto-rf」コマンドの出力 3-32
チャネルの動的割り当て 3-33
干渉の検出と回避 3-34
送信電力の動的制御 3-34
カバレッジ ホールの検出と修正 3-34
クライアントとネットワークのロード バランシング 3-35

CHAPTER 4 **Cisco Unified Wireless Network アーキテクチャ：基本セキュリティ機能 4-1**
セキュアなワイヤレス トポロジ 4-1
WLAN のセキュリティ メカニズム 4-2
シスコの Wired Equivalent Privacy（WEP）Extension 4-2
Wi-Fi Protected Access（WPA） 4-3
Wi-Fi Protected Access 2（WPA2） 4-3
802.1X 4-3
認証および暗号化 4-4
Extensible Authentication Protocol（拡張認証プロトコル） 4-4
認証 4-5

サプリカント 4-5
オーセンティケータ 4-6
認証サーバ 4-7
暗号化 4-8
TKIP の暗号化 4-8
AES の暗号化 4-9
Four-Way ハンドシェイク 4-10
Proactive Key Caching と CCKM 4-11
Cisco Unified Wireless Network アーキテクチャ 4-13
CAPWAP の機能 4-14
覚えておく必要のある重要なポイント 4-14
Cisco Unified Wireless Network のセキュリティ機能 4-15
強化された WLAN セキュリティ オプション 4-15
ローカル EAP 認証 4-17
ACL およびファイアウォール機能 4-18
DHCP および ARP 保護 4-19
ピアツーピア ブロック 4-19
無線 IDS 4-20
Cisco Adaptive Wireless Intrusion Prevention System 4-21
モニタ専用モードと ELM 4-22
On-Channel および Off-Channel のパフォーマンス 4-23
WAN リンクをまたぐ ELM 4-23
CleanAir 統合 4-23
ELM wIPS アラーム フロー 4-24
クライアント除外 4-24
不正 AP 4-25
Air/RF 検出 4-26
ロケーション 4-27
有線の検出 4-27
スイッチ ポート トレース 4-28
不正 AP の封じ込め 4-28
管理フレーム保護 4-28
クライアント管理フレーム保護 4-30
管理システムのセキュリティ機能 4-31
設定の確認 4-31
アラームおよびレポート 4-32
アーキテクチャの統合 4-32
Cisco Integrated Security Features 4-33
攻撃のタイプ 4-33

MAC フラッディング攻撃 4-34
DHCP の不正サーバ攻撃 4-34
DHCP 枯渇攻撃 4-34
ARP スプーフィング ベースの中間者攻撃 4-34
IP スプーフィング攻撃 4-35
無線展開トポロジに対する CISF 4-35
ポート セキュリティの使用による MAC フラッディング攻撃の軽減 4-36
ワイヤレス ネットワークでのポート セキュリティ 4-36
ポート セキュリティの有効性 4-37
ポート セキュリティの使用による DHCP 枯渇攻撃の軽減 4-37
無線 DHCP 枯渇攻撃 4-38
DHCP スヌーピングによる不正な DHCP サーバ攻撃の軽減 4-38
ワイヤレス アクセスの DHCP スヌーピング 4-38
DHCP スヌーピングの有効性 4-39
ダイナミック ARP インスペクションによる中間者攻撃の軽減 4-39
ワイヤレス アクセスに対する DAI 4-39
DAI の影響 4-40
IP ソース ガードの使用による IP および MAC スプーフィングの軽減 4-41
無線アクセスに対する IP ソース ガード 4-42
IP ソース ガードの有効性 4-42
ターゲットへの攻撃の概要 4-43

CHAPTER 5 **Cisco Unified Wireless QoS 5-1**

QoS の概要 5-1
無線 QoS の展開方式 5-2
QoS パラメータ 5-2
無線アップストリームおよびダウンストリーム QoS 5-3
QoS およびネットワークのパフォーマンス 5-4
802.11 Distributed Coordination Function 5-4
フレーム間スペース 5-5
ランダム バックオフ 5-5
aCWmin、aCWmax および再試行 5-6
Wi-Fi Multimedia 5-7
WMM のアクセス 5-8
WMM の分類 5-8
WMM キュー 5-9
EDCA 5-10
不定期自動省電力配信（U-APSD） 5-13
TSpec アドミッション制御 5-15

WLAN インフラストラクチャ対応の QoS 拡張機能 5-18
QoS プロファイル 5-18
WMM ポリシー 5-20
Voice over IP 電話 5-21
アドミッション制御パラメータ 5-22
TSpec アドミッション制御の影響 5-24
802.11e、802.1P および DSCP のマッピング 5-25
QoS ベースラインの優先度のマッピング 5-26
CAPWAP ベースの AP への QoS 機能の展開 5-27
WAN QoS と FlexConnect 5-27
無線 QoS の展開に関するガイドライン 5-28
LAN スイッチにおける QoS の設定例 5-28
AP スイッチの設定 5-28
WLC スイッチの設定 5-28
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 5-29
WLAN 音声とシスコの電話機 5-29
WAN 接続を介した CAPWAP 5-29
CAPWAP のトラフィック分類 5-30
CAPWAP コントロール トラフィック 5-30
CAPWAP 802.11 トラフィック 5-31
分類に関する考慮事項 5-32
ルータの設定例 5-32

CHAPTER 6 **Cisco Unified Wireless のマルチキャスト設計 6-1**

概要 6-1
マルチキャスト転送の概要 6-1
無線マルチキャスト ローミング 6-3
非対称マルチキャスト トンネリング 6-4
マルチキャスト対応ネットワーク 6-4
CAPWAP マルチキャスト予約ポートおよびアドレス 6-5
コントローラでのマルチキャスト転送の有効化 6-5
Ethernet Multicast Mode を有効にする CLI コマンド 6-6
マルチキャストの配置に関する考慮事項 6-6
CAPWAP マルチキャスト アドレスを選択する際の推奨事項 6-6
断片化と CAPWAP マルチキャスト パケット 6-7
すべてのコントローラの CAPWAP マルチキャスト グループが同じになる 6-7
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 6-8
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 6-9
その他の考慮事項 6-10

CHAPTER 7 FlexConnect 7-1
サポートされるプラットフォーム 7-3
FlexConnect の用語 7-3
スイッチング モード 7-3
ローカル スイッチング 7-3
中央スイッチング 7-3
動作モード 7-4
FlexConnect の状態 7-4
中央認証 / 中央スイッチング 7-4
認証ダウン / スイッチング ダウン 7-4
中央認証 / ローカル スイッチング 7-5
認証ダウン / ローカル スイッチング 7-5
ローカル認証 / ローカル スイッチング 7-6
アプリケーション 7-7
ブランチのワイヤレス接続 7-7
ブランチのゲスト アクセス 7-7
パブリック WLAN ホットスポット 7-8
導入に関する考慮事項 7-9
WAN リンク 7-9
ローミング 7-10
無線リソース管理 7-11
ロケーション サービス 7-11
QoS の考慮事項 7-11
展開に関する一般的な考慮事項 7-11
FlexConnect ソリューション 7-12
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 7-12
クライアント データ トラフィックを配信する利点 7-12
中央クライアント データ トラフィック 7-13
Cisco Flex 7500 シリーズ Cloud Controller 7-13
動作モード 7-14
主要な設計要件 7-14
ブランチ ネットワーキング機能とベスト プラクティス 7-15
FlexConnect グループ 7-16
FlexConnect グループの設定 7-17
CLI を使用した確認 7-20
ローカル認証 7-20
ローカル EAP 7-21
CCKM/OKC 高速ローミング 7-21
FlexConnect VLAN オーバーライド 7-22

FlexConnect VLAN オーバーライドの要約 7-22
FlexConnect VLAN に基づく中央スイッチング 7-22
FlexConnect VLAN 中央スイッチングの要約 7-23
FlexConnect ACL 7-23
FlexConnect ACL の要約 7-24
FlexConnect ACL の制限事項 7-24
FlexConnect スプリット トンネリング 7-24
スプリット トンネルの要約 7-25
スプリット トンネリングの制限事項 7-25
耐障害性 7-25
耐障害性の要約 7-26
耐障害性の制限事項 7-26
ピアツーピア ブロック 7-26
P2P の要約 7-26
P2P の制限事項 7-26
ローカル スイッチング WLAN のための FlexConnect WGB/uWGB サポート 7-27
FlexConnect WGB/uWGB の要約 7-27
FlexConnect WGB/uWGB の制限事項 7-27
注意事項と制約事項 7-28

CHAPTER 8 **Cisco Wireless Mesh Networking** 8-1
アクセス ポイントのロール 8-2
ネットワーク アクセス 8-3
ネットワークのセグメント化 8-3
Cisco 屋内メッシュ アクセス ポイント 8-3
Cisco 屋外メッシュ アクセス ポイント 8-4
Cisco Aironet 1552 メッシュ アクセス ポイント 8-5
Cisco Aironet 1522 メッシュ アクセス ポイント 8-7
Cisco 1524SB メッシュ アクセス ポイント 8-7
イーサネット ポート 8-7
1550 シリーズの複数の電源オプション 8-8
Cisco ワイヤレス LAN コントローラ 8-9
Cisco Prime Infrastructure 8-9
アーキテクチャ 8-9
Control And Provisioning of Wireless Access Points 8-9
メッシュ ネットワークの CAPWAP ディスカバリ 8-9
Adaptive Wireless Path Protocol 8-10
トラフィック フロー 8-10

メッシュ ネイバー、親、および子 8-11
最適な親を選択するための基準 8-12
容易度の計算 8-12
親の決定 8-13
メッシュ導入モード 8-13
ワイヤレス バックホール 8-13
ユニバーサル アクセス 8-13
ポイントツーマルチポイント無線ブリッジング 8-14
ワイヤレス バックホール データ レート 8-15
ClientLink テクノロジー 8-15
コントローラの計画 8-17
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 8-17
セルの計画と距離 8-18
Cisco 1520 シリーズ AP 用 8-18
メッシュ アクセス ポイントのコロケーション 8-18
隣接チャネルでの AP1500 のコロケーション 8-18
代替隣接チャネルでの AP1500 のコロケーション 8-18
CleanAir 8-19
CleanAir Advisor 8-19
ワイヤレス メッシュ モビリティ グループ 8-19
複数のコントローラ 8-20
メッシュ アベイラビリティの増加 8-20
複数の RAP 8-22
屋内メッシュと屋外メッシュの相互運用性 8-22
Cisco 1500 シリーズ メッシュ AP のネットワークへの接続 8-23
メッシュ ネットワークへのメッシュ AP の追加 8-23

CHAPTER 9 **VoWLAN の設計に関する推奨事項 9-1**

アンテナに関する考慮事項 9-1
AP アンテナの選択 9-1
アンテナの方向 9-2
一般的な推奨事項 9-3
アンテナの配置 9-4
ハンドセット アンテナ 9-5
チャネル使用率 9-5
動的周波数選択（DFS）および AP の 802.11h 要件 9-6
5 GHz 帯域のチャネル 9-7
コール キャパシティ 9-8

AP コール キャパシティ 9-11
セルの境界の設計 9-13
デュアル バンド カバレッジ セル 9-16
送信電力の動的制御 9-16
802.11r および 802.11k 機能 9-18
ユーザにとってローカルな干渉源 9-19

CHAPTER 10 Cisco Unified Wireless Network ゲスト アクセス サービス 10-1
概要 10-1
スコープ 10-1
無線ゲスト アクセスの概要 10-2
Cisco Unified Wireless Network ソリューションを使用したゲスト アクセス 10-2
WLAN コントローラ ゲスト アクセス 10-3
サポートされるプラットフォーム 10-4
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 10-4
アンカー コントローラ展開ガイドライン 10-6
アンカー コントローラの位置決め 10-6
DHCP サービス 10-7
ルーティング 10-7
アンカー コントローラのサイジングとスケーリング 10-7
アンカー コントローラの冗長性 10-8
Web ポータル認証 10-9
ユーザ リダイレクション 10-10
ゲスト資格情報の管理 10-10
ローカル コントローラのロビー管理者のアクセス 10-11
ゲスト ユーザの認証 10-12
外部認証 10-12
ゲスト パススルー 10-13
ゲスト アクセスの設定 10-13
アンカー WLC の設置およびインターフェイスの設定 10-14
ゲスト VLAN インターフェイスの設定 10-15
モビリティ グループの設定 10-17
アンカー WLC のデフォルト モビリティ ドメイン名の定義 10-17
アンカー WLC のモビリティ グループ メンバの定義 10-18
外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加 10-19
ゲスト WLAN の設定 10-20
外部 WLC：ゲスト WLAN の設定 10-22
アンカー WLC 上でのゲスト WLAN の設定 10-28
アンカー WLC：ゲスト WLAN インターフェイス 10-28

ゲスト アカウント管理 10-30
管理システムを使用したゲスト管理 10-30
ゲスト ユーザの追加テンプレートの使用 10-32
ゲスト ユーザのスケジュール テンプレートの使用 10-36
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 10-40
ユーザ アカウントの最大数の設定 10-41
最大同時ユーザ ログイン 10-42
ゲスト ユーザの管理に関する注意事項 10-42
その他の機能とソリューション オプション 10-43
Web ポータル ページの設定と管理 10-43
内部 Web ページの管理 10-43
内部 Web 証明書の管理 10-45
外部 Web リダイレクションのサポート 10-47
アンカー WLC 事前認証 ACL 10-47
アンカー コントローラ DHCP 設定 10-49
新しい DHCP スコープのアンカー コントローラへの追加 10-49
外部 RADIUS 認証 10-51
RADIUS サーバの追加 10-51
外部アクセス コントロール 10-54
ゲスト アクセス機能の確認 10-56
ゲスト アクセスのトラブルシューティング 10-57
ユーザがゲスト WLAN に接続できない 10-57
ユーザが DHCP 経由で IP アドレスを取得できない 10-57
ユーザが Web 認証ページにリダイレクトされない 10-58
ユーザが認証されない 10-58
ユーザがインターネットまたはアップストリーム サービスに接続できない 10-58
システム モニタリング 10-58
アンカー コントローラ 10-58
外部のキャンパス コントローラ 10-60
debug コマンド 10-62

CHAPTER 11 **Cisco モビリティ サービス エンジン 11-1**
概要 11-1
背景説明 11-1
概要 11-2
用語 11-2
Mobility Services Engine 11-2
技術的な背景情報 11-4
RSSI 11-5

到達時間差 11-5
Active RFID Tags 11-5
システム アーキテクチャ 11-6
関連情報 11-9

はじめに

本書の目的

このマニュアルの目的は、Cisco ワイヤレス LAN コントローラ ソフトウェア リリース 7.3 に入っている機能を使用した、企業向け Cisco Unified Wireless Network ソリューションの設計と実装を説明することです。

対象読者

このマニュアルは、企業の無線ネットワークの設計と実装を担当する、経験豊富なネットワーク管理者を対象としています。

マニュアルの構成

次の表で、このマニュアルの章のリストおよび簡単な説明を示します。

セクション	説明
第 1 章「Cisco Unified Wireless Network ソリューションの概要」	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。
第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」	企業の Cisco Unified Wireless の実装における主要な設計や運用上の考慮事項を説明します。
第 3 章「WLAN RF の設計に関する考慮事項」	さまざまな無線 LAN（WLAN）環境における RF に関する考慮事項を理解するために必要となる無線周波数（RF）の基本的な情報を説明します。
第 4 章「Cisco Unified Wireless Network アーキテクチャ：基本セキュリティ機能」	Cisco Unified Wireless ソリューションにおいてネイティブで使用可能な 802.11 セキュリティ オプションと高度なセキュリティ機能について、また最適な WLAN ソリューションを作成するためにそれをどのように結合するかについて説明します。
第 5 章「Cisco Unified Wireless QoS」	WLAN の実装に関連する QoS について説明します。
第 6 章「Cisco Unified Wireless のマルチキャスト設計」	IP マルチキャストを転送することで実現される改善内容および、無線環境でマルチキャストを実装する方法を説明します。

セクション	説明
第 7 章「FlexConnect」	シスコの中央集中型 WLAN アーキテクチャおよび、それによる H-REAP の使用について説明します。
第 8 章「Cisco Wireless Mesh Networking」	ワイヤレス メッシュの使用について説明します。
第 9 章「VoWLAN の設計に関する推奨事項」	Voice over WLAN（VoWLAN）ソリューションを実装する場合の、設計上の考慮事項を説明します。
第 10 章「Cisco Unified Wireless Network ゲスト アクセス サービス」	中央集中型 WLAN アーキテクチャにおけるゲスト アクセス サービスの使用について説明します。
第 11 章「Cisco モビリティ サービス エンジン」	Cisco Mobility Services Engine（MSE）について、また設計や構成、導入、実装に関わる特別な考慮事項の対象となるエリアについて説明します。
用語集	本書で使用する主な用語の一覧とその定義を示します。

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 Solution は、ビジネスに不可欠なモビリティに、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）のセキュリティや展開、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無線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じアクセス性、セキュリティ、QoS、高い可用性が必要です。仕事場や自宅、外出先、または国内や海外からでも、接続の必要性は出てきます。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、モバイルおよび無線ソリューションからビジネス バリューを獲得しています。かつては垂直市場的な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へのアクセス、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 マネジメント、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へのアクセスを行う上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。

- *建物や構内のモビリティ：*常時ネットワークが必要で、さらに構内では移動が関わることの多い、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：*ケーブルの長さぎりぎりの場所でなく、最適で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、会議室や作戦指令室、ブレインストーミング ルームの高速なネットワーク設定が容易になります。
- *配線コストの削減：*WLAN を実装することでギャップを埋めることができるため、予定外のケーブル設備を設置する必要がなくなります。

- *追加や移動、変更が簡単で、サポートや保守の費用も削減：*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ります。移行の問題が軽減され、コストのかかる直前の変更も簡単にできます。
- *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分かっています。
- *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によって促進されます。
- *ビジネスの回復力の向上：*WLAN によって従業員のモビリティが向上することで、他の場所への迅速な再配置が可能になります。

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、または構内や支社内の独立したネットワークとして稼働します。また WLAN は、ロケーション ベースのサービスや、小売、製造、医療業界などの用途に結びつけることができます。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。

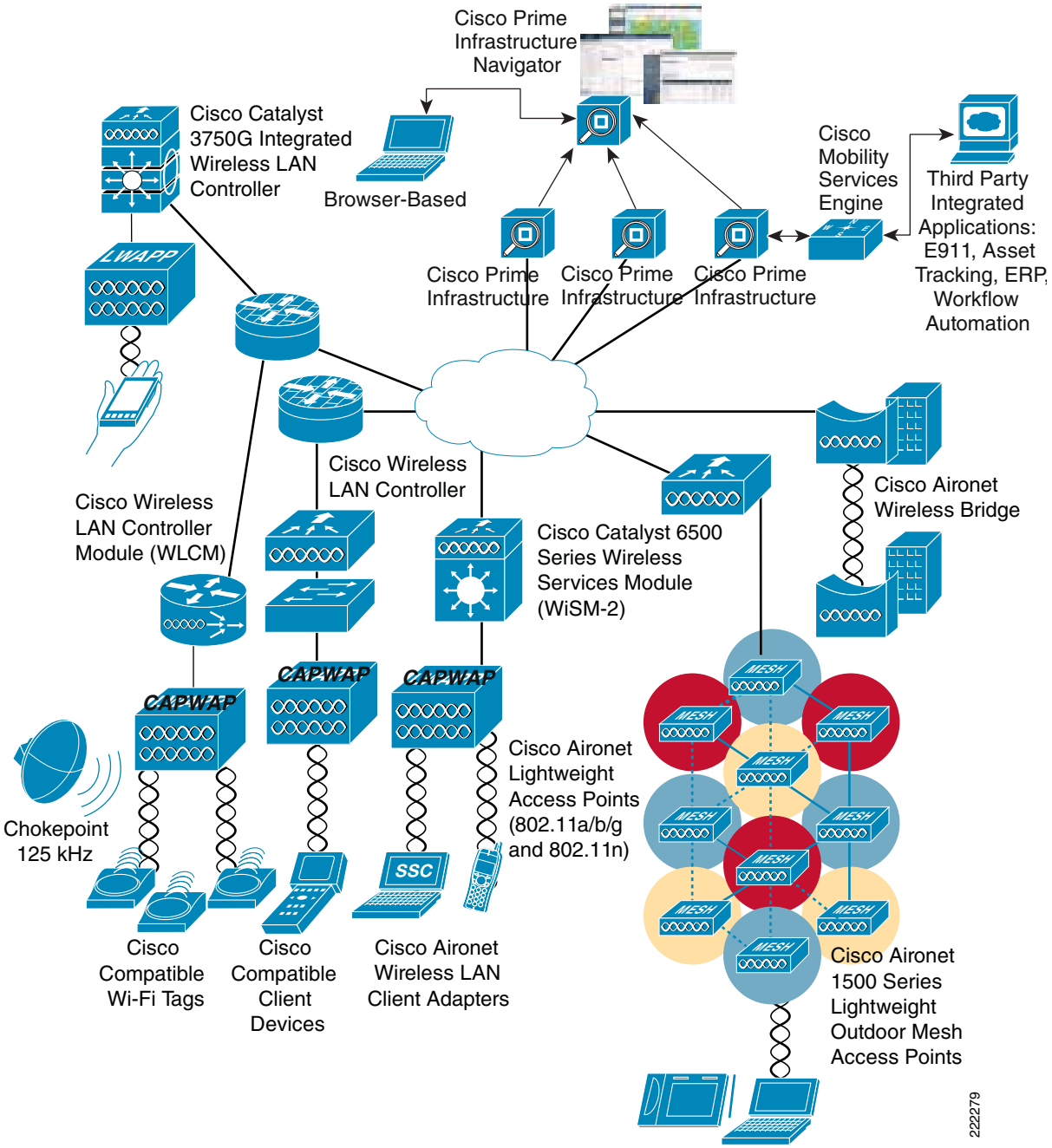
WLAN には次のような機能が必要となります。

- *社員がネットワークに有線接続していないときでもリソースへのアクセスを維持：*このアクセス性により、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、隣の建物でチームメートと一緒に作業中でも、ビジネス上のニーズに素早く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）からの企業の保護：*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 電話通信と 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、映像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、無線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：*無線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。
- *他の場所から来た従業員に簡単で安全なネットワーク アクセスを提供：*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（拡張認証プロトコル）によって認証され、WLAN で送受信されたすべての情報は暗号化されます。

- *簡単に中央またはリモートの AP を管理：*ネットワーク管理者は、WLAN を展開した構内や支社、また店舗や製造施設、医療機関などにある数百から数千の AP を簡単に展開、操作および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スケーラビリティ、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。
- *高度なセキュリティ サービス：*無線経由でやってくる脅威を封じ込め、セキュリティ ポリシーの遵守を実施し、情報を保護する WLAN 侵入防御システム（IPS）および侵入検知システム（IDS）を制御します。
- *音声サービス*：Cisco Unified 有線および無線ネットワークおよび Cisco Compatible Extensions の音声対応クライアント デバイスにより、音声通信に無線ネットワークのモビリティと柔軟性をもたらします。
- *ロケーション サービス：*価値の高い資産の追跡や 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、数百から数千の Wi-Fi およびアクティブ RFID デバイスを直接同時に追跡できます。
- *ゲスト アクセス：*顧客やベンダーに有線および無線 LAN への簡単なアクセスを提供し、生産性を向上させし、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、完全な WLAN セキュリティを維持します。

企業の WLAN は、より大規模な企業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ひとつとなっています。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 クラスの無線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 デバイスの基礎から始まり、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によって、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
- モビリティ サービス エンジン（MSE）

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

高度なエンタープライズ クラスのセキュリティ、*拡張 RF 管理*、*相互運用性の向上*など、その他のメリットを提供する Cisco のオプション コンポーネントの詳細については、次の URL を参照してください。

- Cisco Compatible Extensions クライアント デバイスについて
  http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html
- Cisco Secure Services クライアントについて
  http://www.cisco.com/en/US/products/ps7034/index.html

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 を展開する場合の、設計上および運用上の主な考慮事項について説明します。

この章では、次の内容について説明します。

- CAPWAP
- コア コンポーネント
- コンポーネントの機能グループ
- ローミング
- ブロードキャストとマルチキャストの処理
- 設計上の考慮事項
- 運用および保守

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展開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 の概要

ワイヤレス アクセス ポイント（CAPWAP）の制御およびプロビジョニングは、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、中央集中型 WLAN コントローラ（WLC）への WLAN クライアントによる双方向トンネリング トラフィックの管理に加えて、WLAN の設定および管理を行います。図 2-1 は、基本的な中央集中型 WLAN 展開のハイレベルの概略図を示します。この図では、CAPWAP AP は CAPWAP 経由で WLC に接続されます。

CAPWAP コントローラおよび LWAPP コントローラは、同じネットワークで展開が可能です。CAPWAP 対応ソフトウェアでは、AP は CAPWAP と LWAPP のいずれが稼働するコントローラに join できます。唯一の例外は Cisco Aironet 1140 シリーズの AP で、ここでは CAPWAP だけがサポートされているため、CAPWAP が稼働するコントローラにだけ join できます。たとえば、1130 シリーズの AP では、CAPWAP と LWAPP のいずれが稼働するコントローラにも join できますが、Aironet 1140 シリーズの AP が join できるのは、CAPWAP が稼働するコントローラだけです。

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

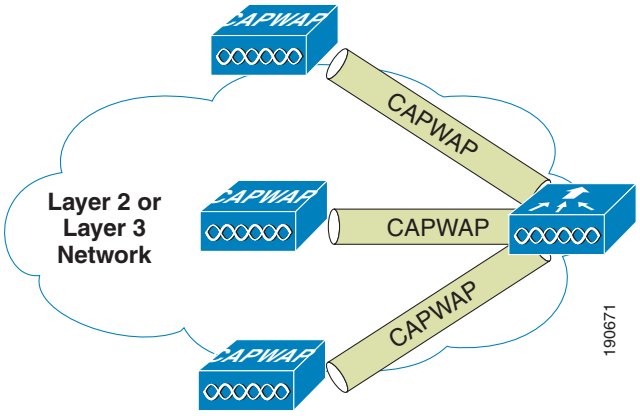
- LWAPP を使用する AP からのトラフィックのみを許容するようにファイアウォールが設定されている場合、CAPWAP を使用する AP からのトラフィックを許容するようにファイアウォールのルールを変更する必要があります。
- CAPWAP UDP ポート 5246 および 5247（LWAPP UDP ポート 12222 および 12223 と同等のポート）が有効になっており、AP がコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト（ACL）がコントローラと AP の間の制御パスにある場合は、新しいプロトコル ポートを開いて AP が孤立しないようにする必要があります。

CAPWAP AP では、ランダムな UDP 送信元ポートを使用し、コントローラ上のそれら宛先ポートに到達します。Cisco WLC リリース 5.2 では、LWAPP が削除され、CAPWAP に置き換えられています。ただし、新しく開封したばかりの AP があれば、コントローラから CAPWAP イメージをダウンロードする前に、LWAPP を使用してコントローラへのアクセスを試行することもできます。AP は、コントローラから CAPWAP イメージをダウンロードしたら、CAPWAP のみを使用して、コントローラとやり取りします。

（注） CAPWAP を使用してコントローラへの join を 60 秒間試行した後、AP は LWAPP の使用にフォールバックします。AP は、LWAPP を使用してコントローラを 60 秒以内に検出できないと、CAPWAP を使用してコントローラへの join を再度試行します。AP は、コントローラに join できるまで、CAPWAP と LWAPP を 60 秒ごとに切り替えるこのサイクルを繰り返します。

LWAPP リカバリ イメージを持つ AP（自律またはスタンドアロン モードまたは新しく開封したばかりの AP から移行した AP）は、コントローラから CAPWAP イメージをダウンロードする前に、LWAPP のみを使用してコントローラに join しようとします。

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、このデザイン ガイドでは、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。

CAPWAP の主な機能は、以下のとおりです。

- スプリット MAC トンネル

- L3 ベースのトンネル
- WLC ディスカバリ プロセス

スプリット MAC

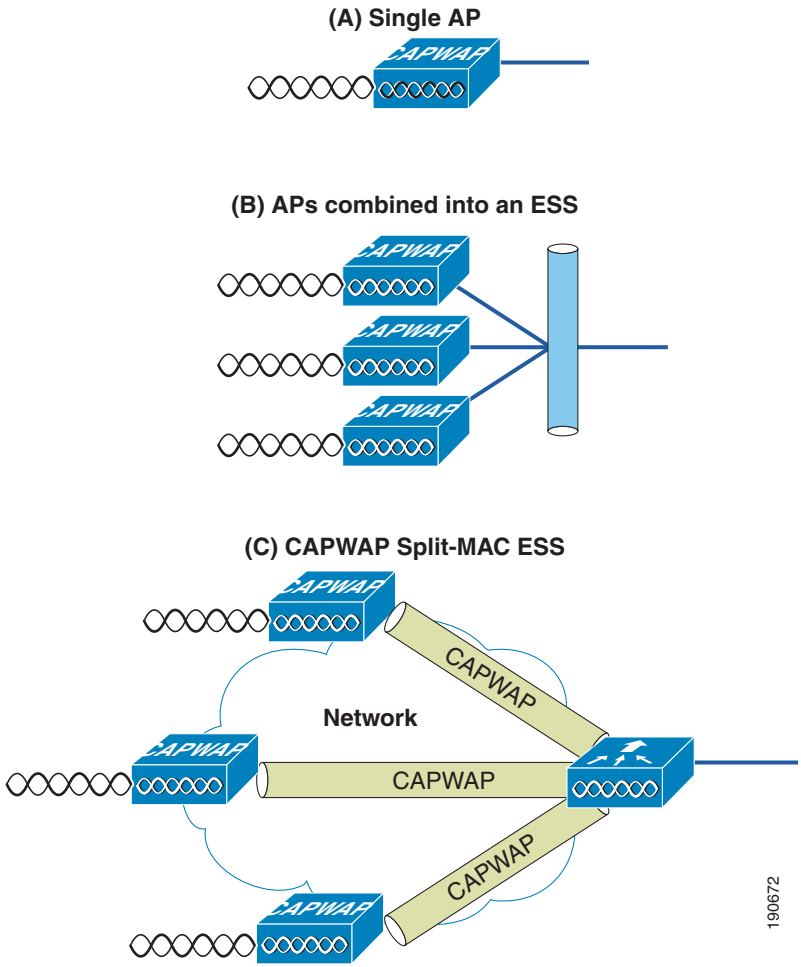
CAPWAP の主要なコンポーネントの 1 つに、*スプリット MAC* という概念があります。これは、802.11 プロトコルでの動作の一部を CAPWAP AP が管理し、残りの部分を WLC が管理するというものです。図 2-2 は、スプリット MAC の概念を図に表したものです。

図 2-2（A）に示す最も単純な汎用 802.11 AP は、Basic Service Set Identifier（BSSID）へのアソシエーションに基づいて有線ネットワークに WLAN クライアントをブリッジする 802.11 MAC レイヤ無線にすぎません。802.11 規格では、図 2-2（B）に示すように、AP を 1 台だけ使用するという概念（前述）が拡張され、複数の AP に対して同じ Extended Service Set 識別子（ESSID、通常 SSID と呼ばれます）を割り当てることで、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るようになります。

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、CAPWAP AP と WLC の 2 つの機能コンポーネントに割り振ります。この 2 つのコンポーネントは、ネットワーク経由で 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、展開や管理がより容易な方法で提供します。

（注）　*スプリット MAC* により、WLAN クライアントと WLC の有線インターフェイスとの間のレイヤ 2 接続はスムーズになりますが、すべてのトラフィックが 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 の展開時にマルチキャストやブロードキャストの要件を検討するときには、このことが重要になりますので、覚えておいてください。

図 2-2　CAPWAP スプリット MAC の概念



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

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

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

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。
- 無線クライアント データのカプセル化：レイヤ 2 無線クライアント トラフィックをカプセル化された IP EtherType パケットで AP から WLC に転送します。

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

レイヤ 3 トンネル

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

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

以下は、CAPWAP 操作を示すためのレイヤ 3 CAPWAP パケット キャプチャです。サンプル デコードは、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。

（注）　Wireshark のデフォルト設定では、Cisco CAPWAP パケットを正しくデコードすることはできません。この問題は、Wireshark の設定ウィンドウの [Protocol Preferences] タブで [SWAP Frame Control] オプションを選択することで解決できます。

図 2-3 は、CAPWAP コントロール パケットのデコードを示しています。WLC からのすべての CAPWAP コントロール パケットと同様、このパケットも WLC から送信元 UDP ポート 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 により使用される設定コマンドを表します。コントロール パケットのペイロードは AES で暗号化されています。この暗号化では、CAPWAP AP が WLC との接続を最初に確立したときに実行される PKI 認証プロセスで生成されたキーが使用されます。

図 2-3　CAPWAP コントロール パケット

```
⊞ Frame 456: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface 0
⊞ Ethernet II, Src: Cisco_a9:91:94 (00:3a:9a:a9:91:94), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 172.20.227.125 (172.20.227.125), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: 39195 (39195), Dst Port: capwap-control (5246)
    Source port: 39195 (39195)
    Destination port: capwap-control (5246)
    Length: 131
  ⊞ 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
      Fragment ID: 0
      Fragment Offset: 0
      Reserved: 0
      MAC length: 6
      MAC address: Cisco_dc:5a:00 (34:a8:4e:dc:5a:00)
      Padding for 4 Byte Alignement: 00
  ⊟ Control Header
    ⊞ Message Type: 1
      Sequence Number: 0
      Message Element Length: 102
      Flags: 0
```

図 2-4 は、802.11 プローブ要求を含む CAPWAP パケットのデコードを示しています。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 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、受信信号強度インジケータ（RSSI）の値と信号対雑音比（SNR）の値も含まれています。

図 2-4　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 2-5 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 2-4 に示すような 802.11 データ フレームです。これには、完全な 802.11 フレームのほかに、WLC に対する RSSI と SNR の情報が含まれます。このキャプチャは、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 2-5 は、CAPWAP 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。Wireshark デコードでは、フレーム コントロール デコード バイトがスワップされていることに注意してください。これは、一部の CAPWAP 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。

図 2-5　CAPWAP の 802.11 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
```

WLC ディスカバリおよび選択

この項では、リセット時のレイヤ 3 CAPWAP AP の典型的な動作について説明します。

ディスカバリ / join プロセスの詳細については、次の Web サイトにある『*Cisco Wireless LAN Controller Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_cg73.html

CAPWAP AP のリセット

レイヤ 3 CAPWAP AP をリセットすると、次のような一連の処理が実行されます。

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

ステップ 2　AP は以前に確認した WLC IP アドレスをローカルの NVRAM に保持します。AP はこれらの WLC IP アドレスのそれぞれにユニキャスト CAPWAP ディスカバリ要求を送信します。CAPWAP ディスカバリ要求を受信する WLC は、AP に CAPWAP ディスカバリ応答を送信することで応答します。前述のとおり、WLC の IP アドレスは、すでに WLC に接続している既存の AP から送信される OTAP メッ

セージによって確認できます。NVRAM に保存される情報には、別のモビリティ グループのメンバとして以前に接続していた WLC のアドレス情報も含まれます（詳細については、「モビリティ グループ、AP グループ、および RF グループ」（P.2-13）を参照してください）。

ステップ 3　ベンダー固有の DHCP オプションを使用して WLC の IP アドレスを返すように、DHCP サーバをプログラムできます。プログラムする場合、CAPWAP AP に WLC のアドレスを *アドバタイズ*するために、*DHCP オファー*で *オプション 43* を使用します。AP が DHCP 経由で IP アドレスを受信する場合、DHCP *オファー*のオプション 43 フィールドで WLC の IP アドレスの情報を確認します。AP は、DHCP オプション 43 に含まれる各 WLC にユニキャスト CAPWAP ディスカバリ メッセージを送信します。CAPWAP ディスカバリ要求メッセージを受信する WLC は、AP に対して CAPWAP ディスカバリ応答をユニキャストします。

ステップ 4　AP は、オプション 43 の情報なしで DNS 名 `CISCO-LWAPP-CONTROLLER.localdomain` を解決しようとします。この名前を解決できた場合、AP は、DNS 応答で返された個々の IP アドレスに対して、ユニキャスト CAPWAP ディスカバリ メッセージを送信します。前述のとおり、CAPWAP ディスカバリ要求メッセージを受信した各 WLC は、AP に対してユニキャスト CAPWAP ディスカバリ応答で応答します。

ステップ 5　ステップ 1 ～ 4 の後、CAPWAP ディスカバリ応答が受信されない場合、AP は検索アルゴリズムをリセットしてから、再開します。

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

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

コア コンポーネント

Cisco Unified Wireless Network ソリューションを構成する主要コンポーネントは、正式にはワイヤレス制御システム（WCS）、ネットワーク制御システム（NCS）、ワイヤレス LAN コントローラ（WLC）、および Cisco Mobility Services Engine（MSE）として知られる Cisco Prime Infrastructure です。この項では、Cisco Prime Infrastructure、WLC、および AP 製品のオプションについて説明します（MSE の詳細については、第 11 章「Cisco モビリティ サービス エンジン」を参照してください）。

Cisco ワイヤレス LAN コントローラ

Cisco Unified Wireless Network コントローラの機能はすべての Cisco WLC プラットフォームで同一かつ共通しているため、便宜上、このドキュメントでは、これらのコントローラをすべて WLC と呼びます。

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

- Cisco 2504 WLC：2504 コントローラは、Cisco AP および Cisco Prime Infrastructure と連携して動作して、システム全体にワイヤレス LAN 機能を提供します。2504 コントローラは、Cisco Unified Wireless Network のコンポーネントであり、ワイヤレス AP と他のデバイスとの間でリアルタイムの通信を行い、中央集中型セキュリティ ポリシー、ゲスト アクセス、ワイヤレス侵入防御システム（WIPS）、Context Aware（ロケーション）、受賞歴のある RF 管理、音声やビデオなどのモビリティ サービスの QoS、およびテレワーカー ソリューションに対する OEAP のサポートなどの機能を備えています。

Cisco 2504 WLC は、最低 5 台から最大 50 台まで（5 台単位）の AP をサポートし、小売業、大企業の支社、および中小企業向けにコスト パフォーマンスに優れたソリューションを提供します。2504 WLC には 4 個のギガビット イーサネット ポートが搭載されています。

- Cisco 5508 WLC：5508 コントローラは Cisco Aironet AP、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間でリアルタイムの通信を行います。また、中央集中型セキュリティ ポリシー、ワイヤレス侵入防御システム（wIPS）機能、RF 管理、および Quality of Service (QoS) を備えています。ワイヤレス ネットワークの例外的なエンドユーザ エクスペリエンスに対応するために、Cisco 5500 シリーズには、さまざまな機能が用意されています。
  - 統合された CleanAir テクノロジーは、自己回復、自己最適化が可能なワイヤレス ネットワークを有効にすることで 802.11n のパフォーマンスを保護します。
  - シスコの ClientLink テクノロジーは、802.11a/g および 802.11n クライアントが最適なレートで動作できるようにすることで、クライアントが混在するネットワークのキャパシティを最適化します。
  - Cisco Identity Services Engine は、有線およびワイヤレス ネットワーク全体にわたり、単一の中央集中化型管理ポイントを提供します。企業は、従業員、ゲスト、および請負業者にセキュアで、適切なアクセスを提供することにより、モバイル スマート フォン、タブレット、ラップトップの急激な増加に対応できます。
- Cisco Wireless Services Module 2（WiSM-2）：Cisco Catalyst 6500 スイッチ シリーズ専用に設計された WLC モジュール。1 モジュールあたり最大 1000 台の AP をサポートします。6500 プラットフォームによっては、複数の WISM-2 をインストールして、拡張性を大幅に向上できます。WISM-2 は、6500 バックプレーンへの接続を提供する dot1 トランクとして設定可能な、6500 上の単一の集約されたリンク インターフェイスです。大規模なビルディングまたはキャンパスに適しています。
- Cisco Virtual Wireless Controller（vWLC）：Virtual Wireless Controller は、Cisco Aironet アクセス ポイント、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間で、中央集中化されたリアルタイムの通信を行います。仮想化イニシアチブに対応した組織や中小企業での展開用に設計された Virtual Wireless Controller は、以下の機能を提供します。
  - 最大 200 カ所のブランチ ロケーションに対応する中央集中型ワイヤレス ネットワークの可視性と制御
  - IT マネージャが FlexConnect を介して最大 200 台のアクセス ポイントと 3000 のクライアントを設定、管理、およびトラブルシューティングする機能
  - セキュアなゲスト アクセス、Payment Card Industry（PCI）コンプライアンスのための不正検出、およびブランチ内部（ローカル スイッチング）での Wi-Fi の音声とビデオ
  - ブランチ ネットワーク用の Cisco FlexConnect ソリューションを備えた信頼性の高い接続
  - ブランチの WAN 障害のためリモート コントローラに接続されたアクセス ポイントの保護。ワイヤレス クライアントは、ローカル リソースへのアクセスとの接続が保持されます
- Cisco Flex 7500 WLC：7500 シリーズ コントローラは、単一のロケーションから何千ものワイヤレス ブランチを管理するために必要な可視性と制御を提供します。このコントローラには、次の機能が用意されています。
  - ブランチ ロケーションごとにローカル コントローラを必要としない、費用対効果の高いソリューションを提供します。
  - 統合リモート管理により、何千ものブランチの拡張された、一貫性のある制御を行うことができます。
  - 分散されたゲストと従業員のアクセスに対するセキュアな中央集中型ポリシー管理を提供します。
  - WAN 障害に対する復元力によって各ローカル ブランチの事業継続性を確保します。

  - データ トラフィックのローカル スイッチングによる効率的なネットワーキングにより、WAN 最適化および QoS ポリシーを実現できます。WAN を介したトンネリングは必要はありません。

- Cisco 8500 WLC : 8500 シリーズ コントローラは、Cisco Aironet アクセス ポイント、Cisco Prime Infrastructure、および Cisco Mobility Services Engine 間でリアルタイムの通信を行います。サービス プロバイダーおよび大規模キャンパスへの展開向けに設計された 8500 シリーズ コントローラは、以下の機能を提供します。
  - 最大 6000 のアクセス ポイント、64,000 のクライアント、および 6000 のブランチ ロケーション用の中央集中型タッチポイントに対応する、単一のラック ユニット スペース（1RU）における業界最大の拡張性
  - 10 ギガビット イーサネット接続のサポートによる高速化 : 冗長性のために 2 つの 10 ギガビット イーサネット ポートを装備
  - SSID の高可用性とワイヤレス クライアントへの影響の最小化を保証する 1 秒未満のアクセス ポイントのステートフル フェールオーバーによる高可用性
  - 冗長性のためのデュアル電源装置による高い復元力

表 2-1 に、利用可能な Cisco WLC を要約して示します。

表 2-1　Cisco WLC の要約

	Cisco 2500 Wireless LAN Controller	Cisco 5508 Wireless LAN Controller	Cisco Flex 7500 Wireless LAN Controller	Cisco 8500 Wireless LAN Controller	Cisco WLAN Controller Module for Cisco Integrated Services Router	Cisco Catalyst 6500 Series Wireless Services Module 2 (WISM-2)
Controller Type	Standalone	Standalone	Standalone	Standalone	Module	Module
Platform Integration	N/A	N/A	N/A	N/A	2900 and 3900 Series Integrated Services Routers	Series Switches
Number of Lightweight Access Points Supported	5, 15, 25 or 50	12, 25, 50, 100, 250 or 500	250, 300, 500, 1000, 2000 or 3000	300-6,000	25 and 50	1,000
Number of clients Supported	500	7000	30,000	64,000	1000	15,000
	Remote location, branch office or campus	Remote location, branch office or campus	Branch/Remote location from the corporate location through a WAN link	SP Wi-Fi and Large Enterprise Campus	Remote location, branch office, or small office	Large campus
Uplink Interfaces	Four 1-Gbps ports	Eight 1-Gbps ports	2 x 10 Gigabit Ethernet interfaces	2 x 10 Gigabit Ethernet interfaces	One 10-/1--- Mbps port	Eight 1-Gbps ports

Cisco アクセス ポイント

Cisco Unified Wireless Network では、Autonomous と CAPWAP の 2 種類の AP が使用されます。この項では、利用可能な CAPWAP AP のさまざまなモデルについて説明します。

（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 展開のガイドラインについては、この設計ガイドでは扱っていません。Cisco MESH ソリューションの詳細については、『*Cisco Mesh Networking Solution Deployment Guide*』（http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh.html）参照してください。

CAPWAP AP

表 2-2 に、利用可能な Cisco CAPWAP AP を要約して示します。

表 2-2　CAPWAP AP の要約

	3600 Series	3500 Series	2600 Series	1260 Series	1140 Series	1040 Series	600 Series
Data Rate	450 Mbps	300 Mbps	450 Mbps	300 Mbps	300 Mbps	300 Mbps	300 Mbps
Radio Design	4X4:3	2X3:2	3x4:3	2x3:2	2x3:2	2X2:2	2X2:2
CleanAir	☑	☑	☑				
ClientLink	ClientLink 2.0	☑	ClientLink 2.0	☑	☑		
BandSelect	☑	☑	☑	☑	☑	☑	
VideoStream	☑	☑		☑	☑	☑	
Rogue AP Detection	☑	☑	☑	☑	☑	☑	
Adaptive wIPS	☑	☑	☑	☑	☑	☑	
OfficeExtend	☑		☑				☑
FlexConnect	☑	☑	☑	☑	☑	☑	☑*
Wireless Mesh	☑*	☑		☑	☑	☑	
Future-proof Modularity	☑						
Data Uplink (Mbps)	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100/1000	10/100
Power	802.3af	802.3af	802.3af	802.3af	802.3af	802.3af	100 to 240 VAC, 50-60 Hz
Temperature Range in Celsius	(i) -0 to 40° C (e) -20 to 55°C	(i) -0 to 40° C (e) -20 to 55°C	(i) -0 to 40° C (e) -20 to 55°C	-20 to 55°C	-0 to 40°C	-0 to 40°C	0 to 40°C
Wi-Fi Standards	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、有線 / ワイヤレス アクセス、キャンパス、ブランチ ネットワークの包括的なライフ サイクル管理、エンドユーザの接続性に対する豊富な可視性、およびアプリケーション パフォーマンスの保証問題のための単一の統合ソリューションを提供します。Cisco Prime Infrastructure は、新しいサービスのロールアウト、モバイル デバイスのセキュアなアクセスと管理、企業 IT への「個人所有デバイスの持ち込み」（BYOD）の実現を加速します。アプリケーション パフォーマンスの可視性とネットワーク制御と緊密に結びつ蹴られたクライアントの認識によって、Cisco Prime Infrastructure は、経験に基づいた妥協のないエンドユーザの品質を保証します。Cisco Identity Services Engine（ISE）とのさらなる統合の深化により、セキュリティおよびポリシー関連の問題に関する可視性が拡張され、これらを解決するための明確な手順を含むクライアントのアクセス問題の全体像が示されます。

Cisco Prime Infrastructure は、次のような高レベルのタスク領域を含むライフ サイクル ワークフローに整理されます。

- デザイン：デザイン フェーズは、機能またはデバイス パターン、あるいはテンプレートの全体のデザインに焦点を当てます。デザイン領域は、設定テンプレートなどの再利用可能なデザイン パターンを作成する場所です。Cisco Prime Infrastructure では、事前定義されたテンプレートが提供されますが、独自のテンプレートを作成することもできます。これらのパターンおよびテンプレートは、ライフサイクルの展開フェーズでの使用を目的としています。
- 導入：導入フェーズは、以前に定義されたデザインまたはテンプレートをネットワークに導入することに焦点を当てます。導入領域は、デザイン フェーズで作成されたテンプレートを使用して、機能の導入方法を指定する場所です。展開段階では、テンプレートに定義した設定を 1 つまたは複数のデバイスにプッシュできます。
- 操作：操作領域は、毎日ネットワークをモニタし、ネットワーク デバイス インベントリと設定管理に関連する他の日常の操作またはアドホックの操作を実行する場所です。[Operate] タブには、毎日のモニタリング、トラブルシューティング、保守、および操作に必要なダッシュボード、Device Work Center、およびツールが含まれています。
- レポート：Cisco Prime Infrastructure では、システムおよびネットワーク ヘルスを監視し、問題をトラブルシューティングするために使用できるレポートを提供します。Cisco Prime Infrastructure の Report Launchpad では、レポートへのアクセスとすべてのタイプのレポート機能のスケジューリングを行います。
- 管理：管理領域は、システム設定を指定し、アクセス コントロールを管理し、データ収集設定を指定する場所です。

モビリティ グループ、AP グループ、および RF グループ

Cisco Unified Wireless 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

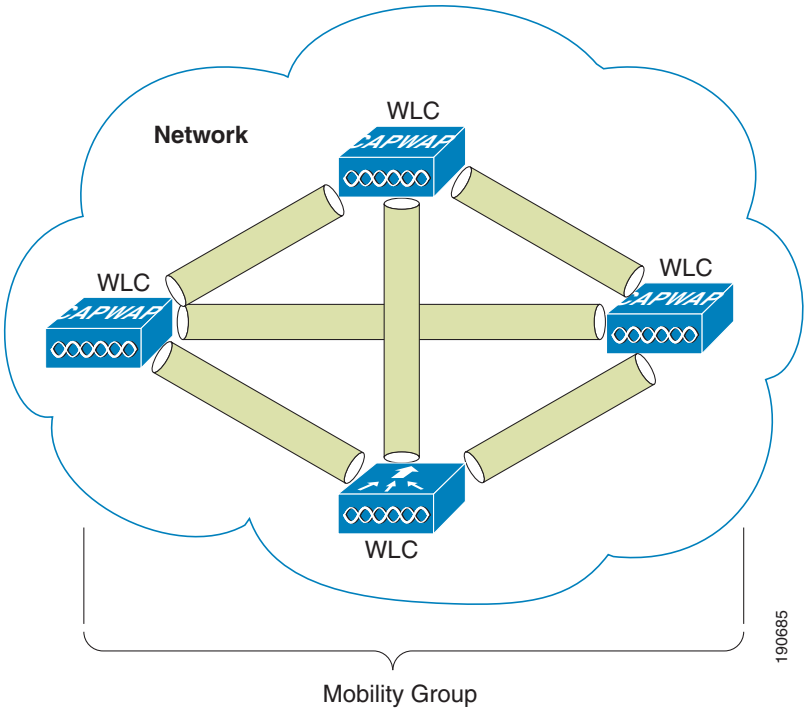
この項では、Cisco Unified Wireless Network におけるこれらのグループの目的と用途について説明します。

モビリティ グループ

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

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

図 2-6　　WLC モビリティ グループ



モビリティ グループの定義

モビリティ グループは簡単に作成できて、これについては詳しく文書化されています。ただし、以下に示すいくつかの重要な留意事項があります。

- 1 つのモビリティ グループには、最大 24 台の標準 WLC（Cisco 2500、5508、WiSM-2、7500、8500、仮想 WLC、WLCM2 シリーズ）を含めることができます。1 つのモビリティ グループには、最大 24 基の Wireless Services Module（WISM-2）ブレードを設定できます。したがって、1 つのモビリティ グループでは、最大 24000 の AP がサポートされます。企業で、複数の 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 グループのメンバとして設定する必要があります。
- WLC リリース 5.1 では、最大 72000 の AP を持つ 1 つのモビリティ グループに最大 72 の WLC（WLC あたり 1000 AP）を設定することができます。
- WLC は、同一のモデルやタイプでなくても、モビリティ グループのメンバにできます。Cisco 2500 シリーズ コントローラ、Cisco Flex 7500、Cisco 5500 シリーズ コントローラ、仮想コントローラ、8500 シリーズ、WiSM-2、SRE 向け Cisco ワイヤレス コントローラ ソフトウェア、また

は Cisco ワイヤレス LAN コントローラ モジュールを自由に組み合わせてグループを構成できますが、実行されているソフトウェアのバージョンは同じでなければなりません。デバイス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、統合ワイヤレス展開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。

- モビリティ グループでは、グループ内のすべての WLC が同じ仮想 IP アドレスを使用する必要があります。
- 各 WLC には同一の*モビリティ ドメイン名*（グループ名）を使用します。また、WLC は、それぞれの [Static Mobility Members] リストでピアとして定義する必要があります。
- モビリティ グループ メンバ（WLC）の間でワイヤレス 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 とセキュリティ設定を同一に設定する必要があります。

モビリティ グループの用途

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

モビリティ グループの例外

Cisco Unified Wireless 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 サービスの展開時に使用します。

自動アンカー機能を使用した場合、指定されたアンカー WLC にマッピングできる WLC の数は、71 個未満です。外部 WLC は自動アンカーに接続されているため、外部 WLC どうしがモビリティ関係を確立することはありません。アンカー WLC では、静的モビリティ トンネルを必要とする外部 WLC ごとに*静的モビリティ グループ メンバ*エントリを定義する必要があります。同様に、静的モビリティ トンネルが設定されている外部 WLC のそれぞれについて、アンカー WLC を外部 WLC の*静的モビリティ グループ メンバ*として定義する必要があります。

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

モビリティ アンカーの設定の詳細は、第 10 章「Cisco Unified Wireless 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

典型的な展開シナリオでは、各 WLAN は WLC ごとに単一の動的なインターフェイスにマッピングされます。しかし、ここで、最大 500 台までの AP をサポートする 5508 WLC が使用される展開シナリオを考えてみてください。各 AP に 25 ユーザがアソシエートされているとします。その結果、125,000 人のユーザが 1 つの VLAN を共有することになります。お客様の設計によっては、サブネットのサイズを非常に小さくすることが要求される場合もあります。このような要求に対処するには、WLAN を

複数のセグメントに分割するのも 1 つの方法です。Cisco AP グループ機能により、WLC 上の複数の動的インターフェイス（VLAN）で 1 つの WLAN をサポートできるようになります。そのためには、AP のグループを特定の動的インターフェイスにマッピングします。AP は、従業員のワークグループごとに論理的にグループ化するか、ロケーションごとに物理的にグループ化できます。図 2-7 は、サイト固有の VLAN に基づく AP グループの使用を示しています。

（注）　AP グループでは、グループの境界を越えたマルチキャスト ローミングは許可されていません。詳細については、第 6 章「Cisco Unified Wireless のマルチキャスト設計」を参照してください。

図 2-7　　AP グループとサイト固有の VLAN

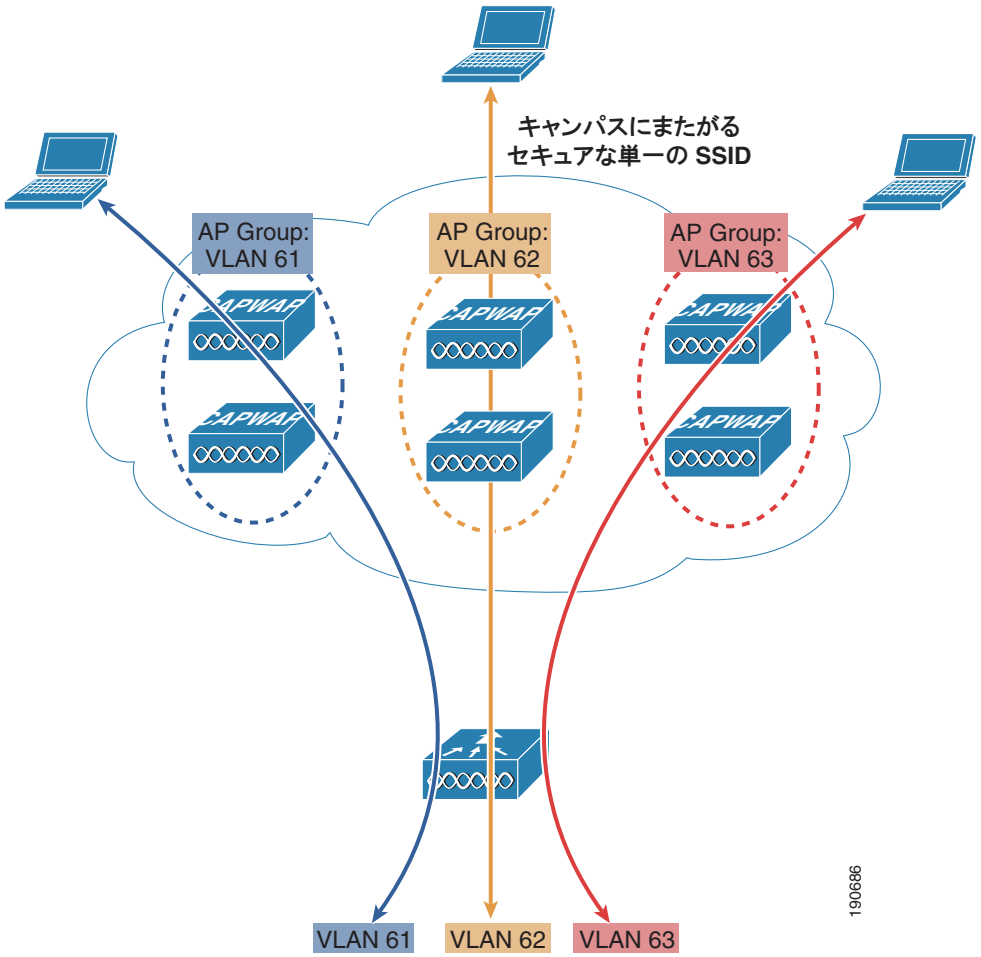


図 2-7 では、3 つの動的インターフェイスが設定され、それぞれがサイト固有の VLAN（61、62、および 63）にマッピングされています。サイト固有の VLAN およびアソシエートされた AP は、それぞれ AP グループ機能を使用して同一の WLAN SSID にマッピングされます。VLAN 61 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 61 IP サブネットで IP アドレスを取得します。同様に、VLAN 62 に対応する AP グループ内の AP 上の WLAN にアソシエートされている企業ユーザは、VLAN 62 IP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

RF グループ

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

802.11 PHY タイプごとに RF グループが存在します。WLC を RF ドメインにグループ化すると、ソリューションの動的な RRM アルゴリズムが複数の WLC で使用され、特定の RF ドメインの RRM がフロア、ビルディング、さらにキャンパス間で使用されるようになります。RF グループおよび RRM については、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。

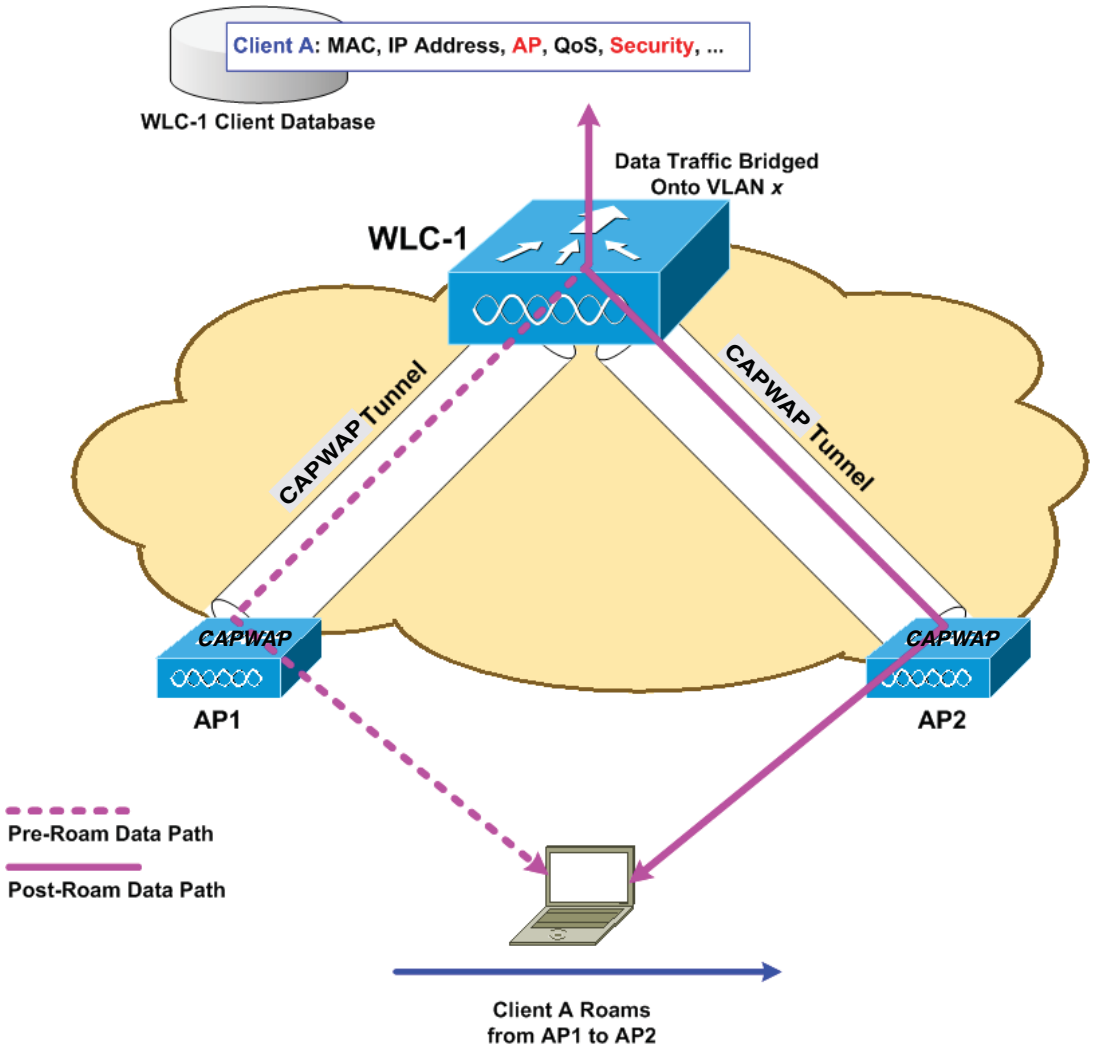
- CAPWAP AP は、定期的にネイバー メッセージを無線で送信します。これには、WLC の IP アドレスと、AP のタイムスタンプおよび BSSID からハッシュされた Message Integrity Check（MIC）が含まれています。
- ハッシュ アルゴリズムでは、共有秘密（RF グループ名）が使用されます。共有秘密は、WLC で設定され、各 AP にプッシュされます。同じ秘密を共有する AP は、MIC を使用して、互いに送信されたメッセージを検証できます。他の WLC に属する AP が、検証されたネイバー メッセージを -80 dBm 以上の信号強度で受信すると、その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

ローミング

モビリティ（ローミング）は、できるだけ遅れることなく、確実かつスムーズに、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ワイヤレス LAN クライアントの機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントが AP にアソシエートして認証すると、コントローラは、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、QoS コンテキスト、WLAN、SSID、およびアソシエートされた AP が含まれます。コントローラ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 2-8 は、両方の AP が同じコントローラに接続されたときにある AP から別の AP にローミングするワイヤレス クライアントを示します。

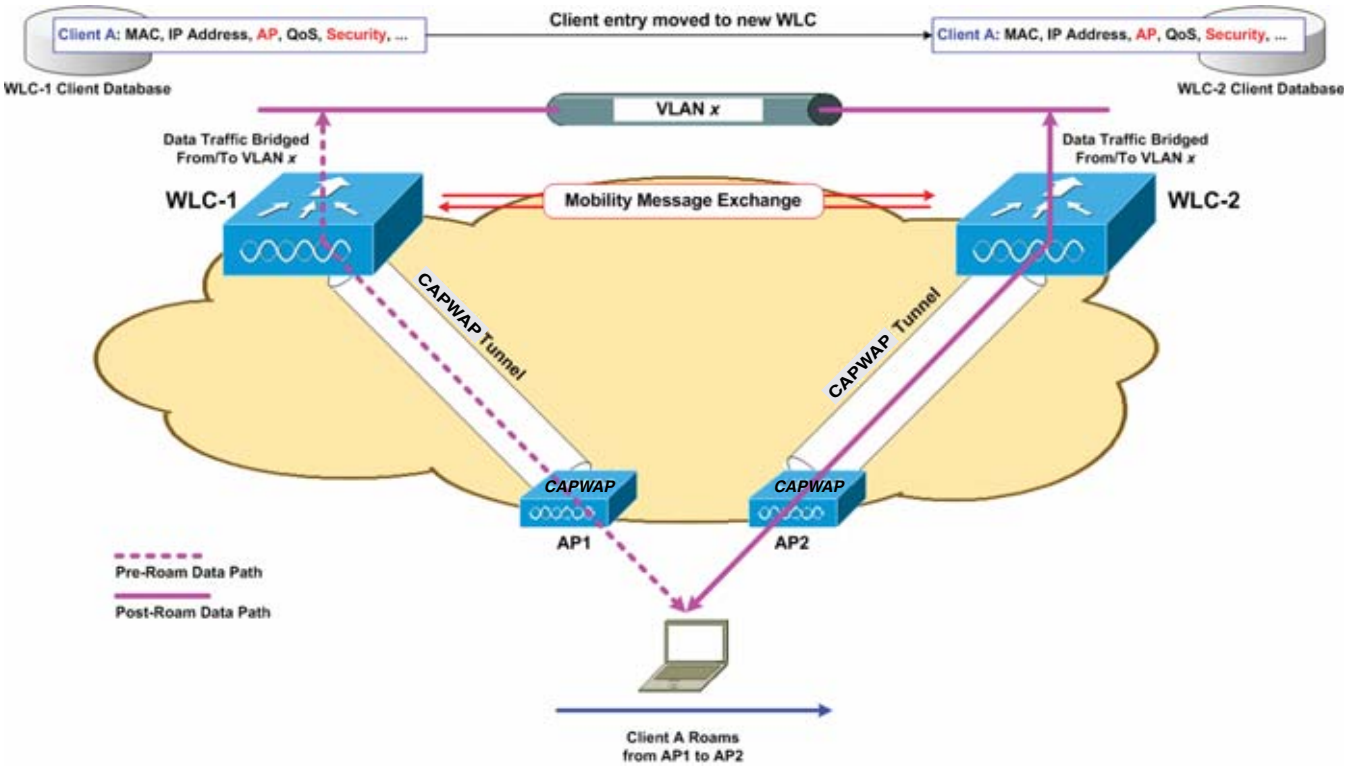
図 2-8　コントローラ内ローミング



ワイヤレス 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、コントローラは新規にアソシエートされた 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 つのコントローラに接続された AP から別のコントローラに接続された 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、同一のサブネット上でこれらのコントローラが動作しているかどうかによっても異なります。図 2-9 は、コントローラのワイヤレス LAN インターフェイスが同じ IP サブネット上に存在す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 2-9　コントローラ間ローミング

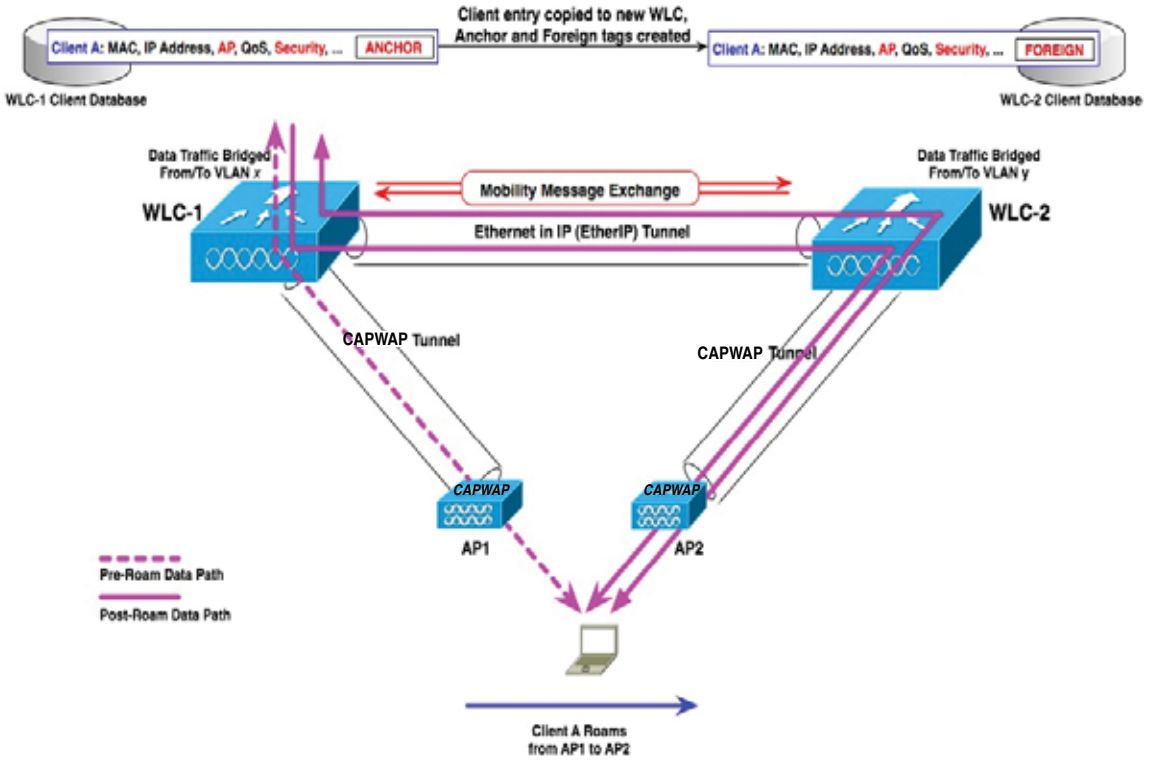


クライアントが新たなコントローラに接続された AP へアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たな AP に対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

（注）　802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

図 2-10 は、コントローラのワイヤレス LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを示します。

図 2-10　サブネット間ローミング



サブネット間ローミングは、コントローラ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 エントリを新しいコントローラ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、新しいコントローラ内で*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コントローラの 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。そのようにしない場合、ハンドオフ後クライアントにネットワーク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。

（注）　インターフェイスがタグなしの場合、ネイティブ IPv6 クライアントではシームレスなモビリティはサポートされません。

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 2-11 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。

図 2-11 802.11 ブロードキャスト / マルチキャスト

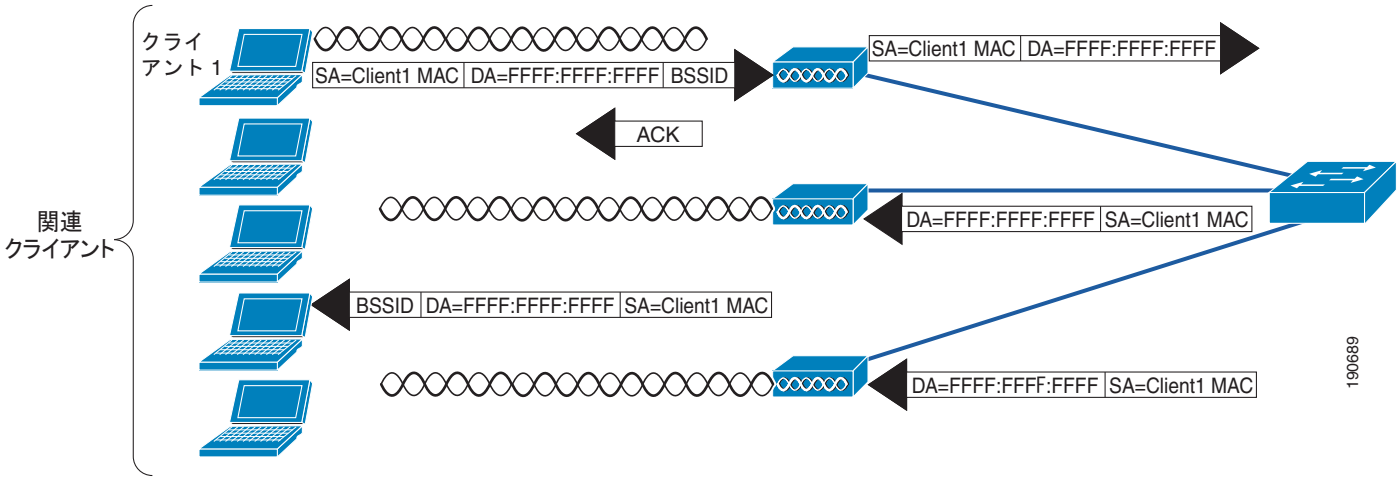
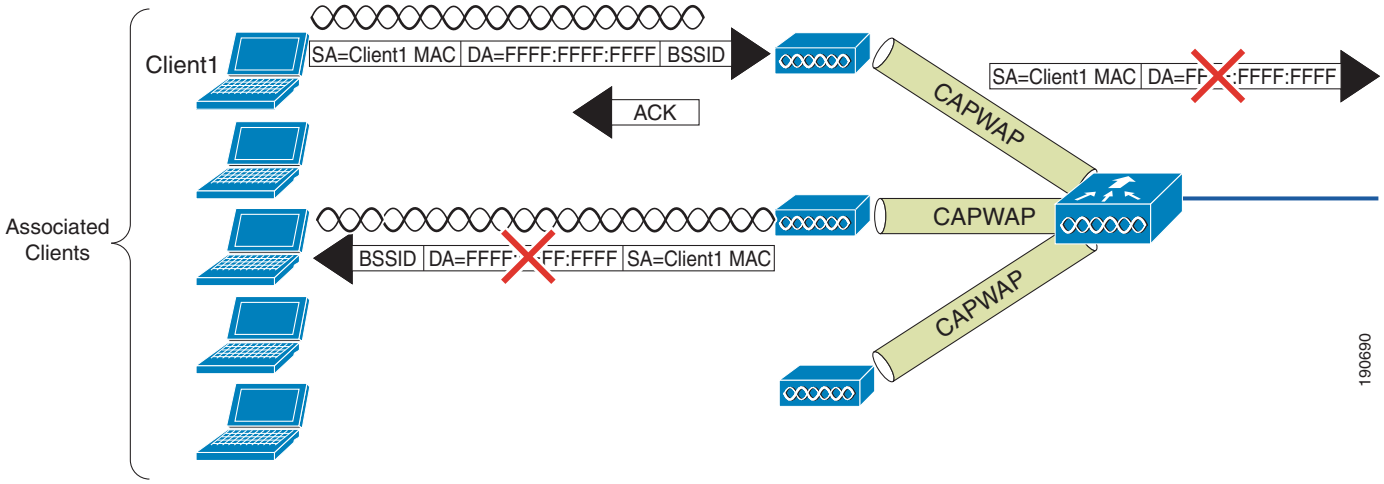


図 2-11 に示されているように、AP と同じ有線 VLAN 上に別の AP がある場合、それらの AP は、有線ブロードキャスト パケットをワイヤレス インターフェイスに転送します。

WLC の CAPWAP *スプリット MAC* 方式では、図 2-14 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 2-12WLC ブロードキャストのデフォルトの動作



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

WLC ブロードキャストおよびマルチキャストの詳細

ブロードキャストおよびマルチキャスト トラフィックは、通常、WLAN ネットワーク内で特別に処理する必要があります。このトラフィックは最小限の共通ビットレートで送信しなければならないので、WLAN に余計な負荷がかかるからです。これによって、アソシエート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、アソシエートされている WLAN クライアントの DHCP リレー エージェントとして機能します。L3 クライアント ローミング中を除き、この WLC は、クライアント DHCP 要求を、ローカルに設定された DHCP サーバ、またはアップストリーム DHCP にユニキャストします（詳細については後述します）。DHCP サーバの定義は動的インターフェイスごとに設定されます。その後、このインターフェイスは、1 つまたは複数の WLAN にアソシエートされます。DHCP リレー要求は、指定された動的インターフェイスのソース IP アドレスを使用して、このインターフェイス経由で転送されます。WLC は、特定のインターフェイスまたは WLAN に対してどの DHCP サーバを使用するかがわかっているため、有線またはワイヤレス 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。

この方法により、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拒絶（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。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推奨します。
- クライアント マシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。
- AP がコントローラに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 の速度で設定された WLAN に関連づ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「Cisco Unified Wireless のマルチキャスト設計」で説明したとおり、マルチキャスト転送が有効になっている場合は、WLC の接続先インターフェイスで生成されるマルチキャスト トラフィックを最小限に抑えるための処理を実行する必要があります。

WLAN により明示的にサポートされるマルチキャスト アドレス グループを制限するために、標準的な対策をすべて講じる必要があります。マルチキャストが有効になっている場合、これは事実上グローバルな設定です。つまり、WLAN がマルチキャストを必要としているかどうかに関係なく、設定されているすべての WLAN で有効になっていることを意味します。Cisco Unified Wireless Network ソリューションでは、データ リンク レイヤとネットワーク レイヤのマルチキャスト トラフィックは区別されません。どちらも、特定のマルチキャスト トラフィックをフィルタできる能力は 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 レイヤのマルチキャスト セキュリティを含むマルチキャスト セキュリティを考慮する必要があることを覚えておいてください。

設計上の考慮事項

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

WLC のロケーション

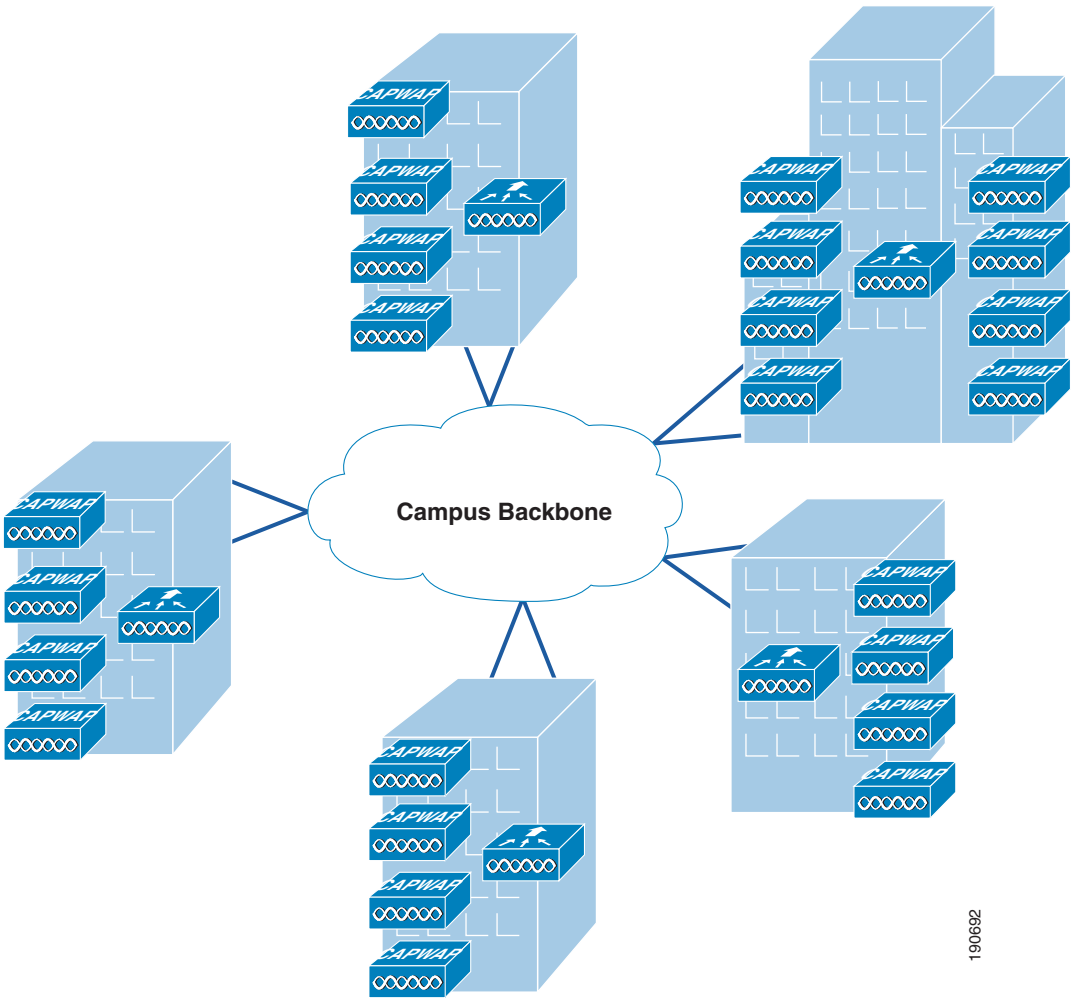
Cisco Unified Wireless Network ソリューションでは、次の項で説明するように、分散型または中央集中型により WLC を展開することができます。

分散型の WLC 展開

図 2-13 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、ビルディング内の分散ルータが使用されます。このシナリオでは、AP と WLC の間の CAPWAP トンネルは通常ビルディング内にとどまります。

WLAN カバレッジがビルディング間で重複しない限り、分散型の WLC をそれぞれ、別々の RF グループおよびモビリティ グループに設定できます。

図 2-13　　分散型の WLC 展開

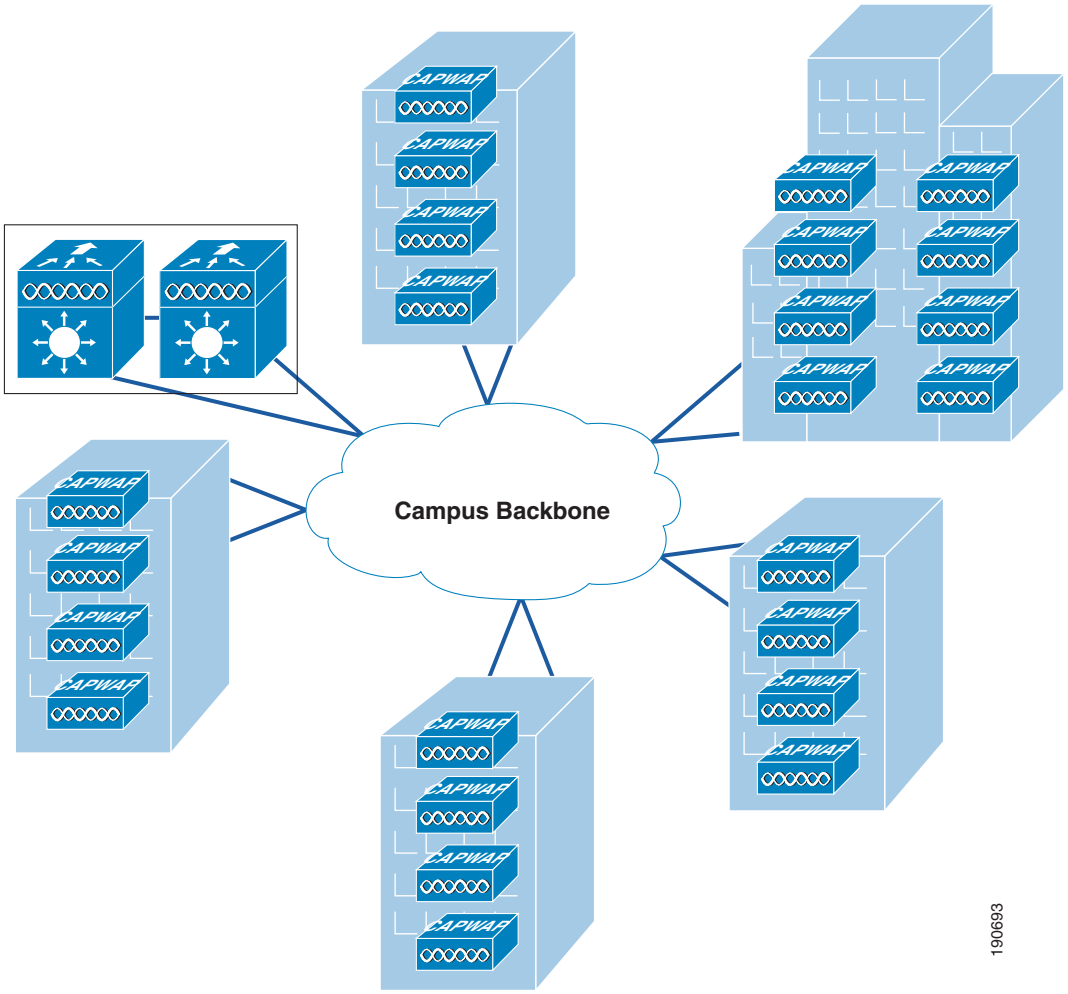


中央集中型の WLC 展開

図 2-14 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 は企業ネットワークの集中化された場所に配置されます。この展開モデルでは、キャンパス バックボーン ネットワークを経由するために AP/WLC 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 クラスタは専用スイッチ

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。データセンターと WLC クラスタでは、通常、ネットワークおよびセキュリティ要件が異なるので、WLC をデータセンターのスイッチ ブロックに直接接続してはいけません。

図 2-14　　中央集中型の WLC 展開



WLC の中央集中化

シスコでは、一般的に、キャンパス環境全体の中心的な位置に WLC を展開することを推奨しています。モビリティ グループとレイヤ 3 ローミングを必要とする分散展開モデルは十分に証明されていますが、レイヤ 3 ローミングに関連するマルチキャスト サポートに現在不十分な点があるため、推奨されていません。これらへの対策が行われた場合、分散展開モデルの検討を妨げる障壁の大半は解消されます。

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

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

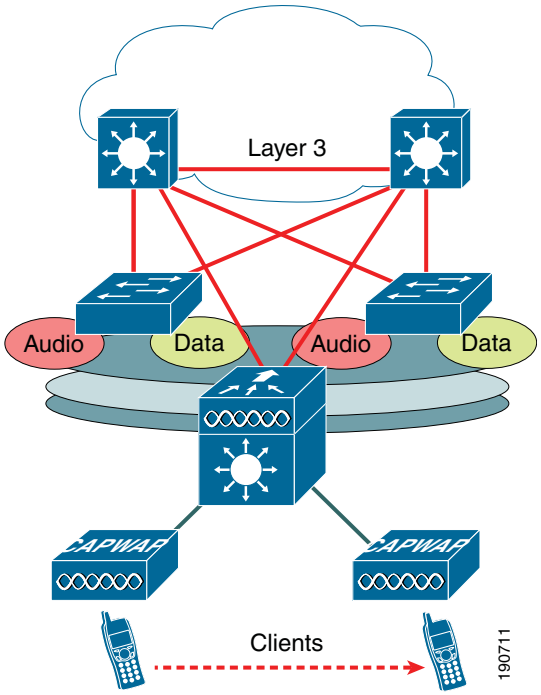
WLC を他のインフラストラクチャ コンポーネントと統合する場合にも同様の原理が当てはまります。中央集中型の WLC により、統合ポイントおよび統合デバイスの数を最小限に抑えられます。たとえば、NAC アプライアンスのようなインライン セキュリティ デバイスの実装を決定したとき、集中化された WLC の場合は統合ポイントが 1 か所ですが、分散ソリューションの場合は統合ポイントが *n* か所になります（この場合、*n* は、WLC の展開箇所の数を示します）。

要約すると、中央集中型の WLC 展開の使用が推奨されるということです。中央集中型の WLC 展開を計画する場合、WLC に直接接続される有線ネットワーク インフラストラクチャの保護を考慮する必要があります。これは、WLC は基本的に、接続さえしていなければ*ネットワーク アクセス*およびこれに伴う脆弱性にさらされることのないような企業トポロジ内の場所にある*アクセス* ネットワークを接続するからです。したがって、アクセス レイヤ ネットワーク デバイスに関連する一般的なセキュリティ上の配慮事項をすべて検討する必要があります。たとえば、WISM-2 をベースとする展開では、DoS 攻撃やトラフィック ストームに対する保護などの機能を検討する必要があります。これは、多数のエンド ユーザに対してさまざまな WLAN サービスを提供すると同時に、複数レイヤにわたるマルチファンクション Catalyst 6500 スイッチ プラットフォームのバックプレーンに直接接続されている WISM-2 が果たす役割は大変大きいからです。

分散型の WLC ネットワーク接続

図 2-15 レイヤ 3 に接続された WLC（この場合は 3750G）では、WLAN 関連のソフトウェアおよび設定を 1 つのデバイスに分離し、他のアクセス レイヤ ルーティング デバイスと同じルーティング設定を使用してディストリビューション レイヤに接続できます。

図 2-15　　レイヤ 3 に接続された WLC



トラフィックの負荷と有線ネットワークのパフォーマンス

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

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

ネットワークのトラフィック ボリューム全体に対して 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 のリブート中は多くなります。しかし、トラフィックの調査では、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 Kb/sec であることが判明しています。このトラフィックは、ほとんどのキャンパスで無視できる量であり、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

トンネリングによって生じるオーバーヘッド

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。標準的な企業で見られる平均パケット サイズが約 300 バイト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、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

トラフィック エンジニアリング

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デスティネーションに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 展開の場合、クライアント トラフィックはエッジから入り、宛先アドレスに基づいてそのポイントから適切にルーティングされます。

しかし、中央集中型の展開モデルに関連する長いトンネルや潜在的に効率の悪いトラフィック フローは、クライアント トラフィックの大半が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ますし、中央集中型の WLC 展開と分散型の WLC 展開を比較しても大差はありません。

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

AP 接続

AP は、エンド ユーザ（802.11 クライアント）とは別のネットワーク上になければなりません。これは、インフラストラクチャ管理インターフェイスはエンド ユーザとは別のサブネット上にあるべきであると定義している一般的なベスト プラクティス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）。

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

Cisco Unified Wireless Network に WLAN QoS 機能を効率的に提供するには、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。

運用および保守

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

WLC ディスカバリ

AP のための、次のようなさまざまな WLC ディスカバリ メカニズム（前述）により、CAPWAP AP の初期展開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展開

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

AP 分散

典型的な初期 WLAN 展開では、AP は、各 WLC の負荷に応じて、使用可能な WLC 全体に AP 自体を自動的に分散します。このプロセスにより展開は簡単になりますが、いくつかの運用上の理由から、自動分散の使用はお勧めしません。

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

複数の WLC にわたる AP 分散を制御するために使用される要素は、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。

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
- WLAN カバレッジの手動による微調整
- 無線リソース管理（RRM）のアルゴリズム

RF の基礎

アメリカ合衆国では、工業用、科学用、および医療用（ISM）のライセンス不要の用途のために 3 つの帯域が割り当てられています（図 3-1 を参照）。

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）
  - 5.250 ～ 5.350 GHz（UNII-2）
  - 5.725 ～ 5.875 GHz（UNII-3/ISM）

各帯域には異なる特徴があります。より低い周波数の 2.4 GHz 帯域は、広い範囲まで届きますが、帯域幅は限られているため、データ レートは低くなります。より高い周波数の 5 GHz 帯域は、狭い範囲しか届かず、固体の物体の場合は減衰量が増えることがあります。

この項では、規制区域とその動作周波数の概要を示します。

規制区域

ライセンス不要の帯域で動作するデバイスは、正式な認可を得るプロセスは必要ありませんが、ISM 帯域で動作する際、ユーザはその地域に対して定められた政府の規制に従う必要があります。世界中の各規制機関は、それぞれの基準に従ってこれらの帯域を監視しています。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、規制機関は規格で特定の基準を設定しています。たとえば、無線が生成したり、近接した場所の別の無線から受信する干渉の量を最小限に抑えるための、WLAN のエミッション要件があります。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。

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

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（世界中の他のほとんどの地域）は最大 13 チャネル、および日本は最大 14 チャネル許可していますが、チャネル 14 で動作するには特別なライセンスが必要になります。
802.11a/n/ac の 5.0 GHz 帯域の規制を準拠する国では、追加チャネルのために追加スペクトルを開放する方向で動き始めています。

これらの周波数帯域と関連するデータ レートについては、以降の項でより詳しく説明されています。

2.4 GHz：802.11b/g/n

1999 年に批准された 802.11b 規格は、1、2、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、最初に標準化された WLAN 通信方式として、何千ものエンタープライズ組織で展開されています。

2003 年に批准された 802.11g 規格は、802.11b と同じスペクトラムで動作し、802.11b 規格との下位互換性を備えています。802.11g 規格は、さらに、6、9、12、18、24、36、48、および 54 Mbps のデータ レートをサポートし、2.4 GHz 帯域で最も一般的な WLAN 通信方式です。

2009 年に批准された 802.11n 規格は 2.4 および 5 GHz 帯域で使用できます。2.4 GHz 帯域は、最大 144 Mbps までのデータ レートをサポートします（20 MHz 帯域幅と単一の送信ストリームを仮定した場合）。より高速のボンディング チャネル（20 MHz を超えるスペクトラムを使用）は、300 Mbps まで高速化できますが、これは家庭での導入において一般的であることに注意してください。企業ネットワークは 2.4 GHz 帯域で 20 MHz のデータ レートに限定されますが（スペクトラムの量が限られるため）、802.11n や 802.11ac テクノロジーによる 5 GHz 帯域を使用してさらに高速化できます。

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

導入に関する考慮事項

これら 2 つのテクノロジー（802.11a/n/ac と 802.11b/g/n）を選択するうえで、1 対 1 のトレードオフは必要ありません。これらは補完的なテクノロジーであり、将来の企業環境でも共存し続けます。これらのテクノロジーの実装の責任者は、2.4 GHz だけのネットワーク導入、5 GHz だけのネットワーク導入、またはこれらを組み合わせた導入の中から、経験に基づいて選択できる必要があります。既存の 802.11b/g ネットワークを使用する組織は、単純に既存の AP に新しい 802.11a ネットワークを展開し、

802.11b/g/n による 11 Mbps カバレッジと同じ領域で、802.11a/n/ac による 54 Mbps カバレッジを期待するわけにはいきません。これらの両方の帯域の技術的な特性のため、このようなカバレッジの互換性は実現しません。

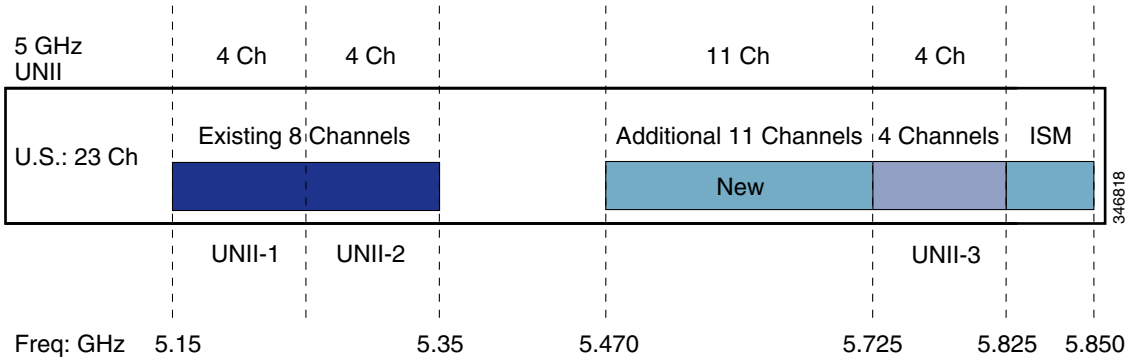
802.11a では、通常、所定の電力およびアンテナ ゲインに対してより短い範囲で 、6、9、12、18、24、36、48 のデータ レート、および最大データ レート 54 Mbps を使用できます。802.11b/g ではオーバーラップしない周波数チャネルが 3 つであるのに対し、802.11a には地理的地域に応じてオーバーラップしない周波数チャネルが最大で 23 あります。この結果、ネットワーク キャパシティが増加し、スケーラビリティが向上して、隣接するセルから干渉を受けずにマイクロセルラー展開を作成できるようになります。

802.11a/n/ac が動作する 5 GHz 帯域は、複数の異なる部分に分割されています。表 3-1 に示されているの各 UNII 帯域は、当初意図した用途とは異なり、適切な電力制限を有する屋内向けの 802.11a/n/ac デバイスですべて使用できます。当初、FCC ではそれぞれ 4 個のチャネルがある UNII-1、UNII-2 および UNII-3 帯域だけが定義されました。チャネルは、20 MHz 離して設定され、RF スペクトラムが 20 MHz であるため、オーバーラップしないチャネルとなります。

これら 3 つの UNII 帯域には、別々の制限があります。それぞれ、送信電力、アンテナ ゲイン、アンテナ スタイル、および用途の制約が異なります。UNII-1 帯域は、屋内での動作を目的として使用され、当初はアンテナを恒久的に接続する制約がありました。UNII-2 帯域と UNII-3 帯域は、屋内または屋外での動作を目的として使用され、外部アンテナが許容されます。

UNII-1（5.150 ～ 5.250 GHz）のチャネルは 36、40、44、および 48 です。UNII-2（5.250 ～ 5.350 GHz）のチャネルは、52、56、60、64 で、動的周波数選択（DFS）および送信電力制御（TPC）が必要です。新しい周波数範囲（5.470 ～ 5.725 GHz）のチャネルは 100、104、108、112、116、120、124、128、132、136、および 140 で、DFS および TPC が必要です。UNII-3（5.725 ～ 5.850）のチャネルは、149、153、157、161、および 165 で、DFS および TPC は必要ありません。所定の範囲のすべてのチャネルをすべての規制区域で使用できるわけではありません。図 3-1 は、UNII-1、UNII-2、および UNII-3 帯域のさまざまなチャネルと追加の新しい 11 チャネルを示しています。

図 3-1　802.11 のチャネルのキャパシティ



FCC は、5 GHz 802.11a チャネルの使用を取り扱う 2004 年の規制の改正を発表しました。この改正では、新しく 11 のチャネルが追加され、使用可能なチャネル キャパシティは 23 チャネルに増えました（図 3-1 を参照）。新しく追加された 11 のチャネルは、屋内および屋外で使用できます。ただし、新しいチャネルを使用するには、無線が、802.11h の仕様で規定されている TPC および DFS 機能に準拠している必要があります。DFS は、この周波数範囲で動作するレーダーを避けるために必要ですが、これは、動的周波数の計画など他の用途にも使用できます。802.11h は、2010 年以降の Cisco Unified Wireless Network によってサポートされています。

DFS は、特定の条件（レーダー信号の存在など）が満たされたときには必ず、トランスミッタに対して別のチャネルへの切り替えを動的に指示します。デバイスの DFS メカニズムは、送信前に、使用可能な動作範囲を監視し、レーダー信号を待ちます。信号が検出されると、レーダー信号にアソシエートされているチャネルが解放されるか、そのチャネルをトランスミッタが使用できないことを示すフラグ

が立てられます。送信デバイスは、動作前および動作中に、その環境で継続的にレーダーの存在を監視します。5 GHz 帯域の部分は、レーダー システムに割り当てられます。これにより WLAN では、現在のレーダー ユーザが同じ場所にまとめて配置されている場合に、それらのユーザへの干渉を回避できるようになります。

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

FCC 規制の最新情報の詳細は、次の Web サイトにあるシスコのホワイト ペーパー『*FCC Regulations Update*』を参照してください。

http://www.cisco.com/en/US/products/hw/wireless/ps469/products_white_paper0900aecd801c4a88.shtml

表 3-1 は、802.11a/n/ac 規格の周波数を示しています。

表 3-1　802.11a/n/ac の動作周波数の範囲

チャネル ID	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161	165
中心周波数（MHz）	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	5560	5580	5600	5620	5640	5660	5680	5700	5745	5765	5785	5805	5825
帯域	UNII-1				UNII-2															UNII-3				ISM

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 作業グループでは、802.11 WLAN 規格の要素を担当する多数のタスク グループがあります。表 3-2 は、タスク グループ イニシアチブの一部の要約を示しています。

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

表 3-2　IEEE 802.11 タスク グループの活動

タスク グループ	プロジェクト
MAC	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 帯域で高レートな PHY を開発する。
c	802.11 MAC でのブリッジ動作を扱う（スパニングツリー）。
d	その他の規制区域（国）の 802.11 動作のための物理レイヤ要件を定義する。
e	QoS のために 802.11 MAC を強化する。

表 3-2　IEEE 802.11 タスク グループの活動 （続き）

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	無線およびネットワーク測定のための上位レイヤにインターフェイスを提供するため、RRM 拡張を定義する。
k	無線およびネットワーク測定のための上位レイヤにインターフェイスを提供するため、無線リソース測定の拡張を定義する。
m	802.11 系列の仕様の文書に関する、編集上の管理、修正、改訂、明確化、および翻訳を行う。
n	2.4 GHz、5 GHz 帯域における高スループット拡張（MAC SAP で >100 Mbps）を重点的に扱う。
o	Voice over WLAN での高速なハンドオフ（目標は 50 ms あたり）を提供する。
p	料金徴収、車両安全サービス、車でのコマース トランザクションなど、車両を対象とした車両用通信プロトコルを中心に扱う。
r	高速な BSS 遷移および高速なローミングを定めた規格を開発する。
s	完全に網羅するように向上されたメッシュ ネットワークの MAC および PHY を定義する。
t	製造業者、テスト ラボ、サービス プロバイダー、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 メトリック、測定方法論、テスト条件を提供する。
u	IEEE 802.11 アクセス ネットワーク（ホットスポット）と外部ネットワークの間に機能およびインターフェイスを提供する。
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。

ダイレクト シーケンス スペクトラム拡散方式（DSSS）

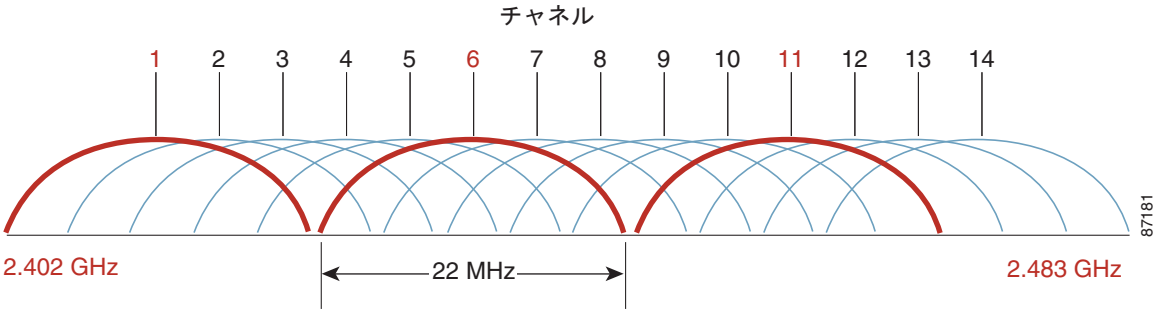
ダイレクト シーケンス スペクトラム拡散方式（DSSS）は、冗長情報を RF 信号に符号化します。これにより、802.11 無線は、チャネルでバックグラウンド ノイズまたは干渉があったとしても、パケットの受信を理解する確率が高くなります。すべてのデータ ビットは、チッピング シーケンスまたはバーカー シーケンスと呼ばれるビット文字列（チップ）に拡張されます。IEEE 802.11 によって指示されているチッピング レートは 1 ビットあたり 11 チップです。1 および 2 Mbps のレートで 2 位相偏移変調（BPSK）/4 位相偏移変調（QPSK）を使用し、11 および 5.5 Mbps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

IEEE 802.11b ダイレクト シーケンス（DS）チャネル

IEEE 802.11b のダイレクト シーケンス（DS）チャネル セットでは、14 チャネルが定義されています。送信される各 DS チャネルは 22 MHz ですが、チャネル用の分離は 5 MHz だけです。結果として、間隔が 25 MHz もない隣接するチャネルからの信号が互いに干渉しあうなど、チャネルのオーバーラップが発生します。14 チャネルの DS システム（米国の場合、使用可能なチャネルは 11）では、オーバーラップせず、干渉しないチャネルは 1、6、および 11 だけです（図 3-2 を参照）。

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

図 3-2　IEEE 802.11 DSS のチャネル割り当て



IEEE 802.11g

802.11g は、802.11b と同じスペクトラムである 2.4 GHz の帯域でより高いデータ レート（最大 54 Mbps）を提供します。802.11g は 802.11b との下位互換性があり、6、9、12、18、24、36、48、54 Mbps のデータ レートも提供します。802.11g は、802.11a/n/ac と同様、高いデータ レートで同じ変調技術である直交周波数分割多重（OFDM）を使用します（「IEEE 802.11a OFDM の物理レイヤ」（P.3-7）を参照）。

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

表 3-3　802.11g の変調および伝送の種類

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

表 3-3　802.11g の変調および伝送の種類 （続き）

16-QAM	OFDM	750	36
64-QAM	OFDM	1000	48
64-QAM	OFDM	1125	54

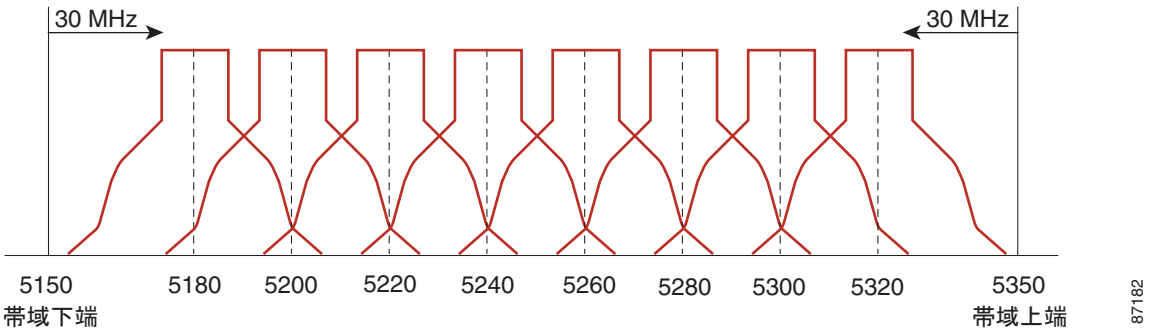
IEEE 802.11a OFDM の物理レイヤ

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

IEEE 802.11a のチャネル

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

図 3-3　チャネル セットの例



米国の 802.11a/n/ac 規格の場合、5 GHz 無認可帯域は 300 MHz のスペクトラムに対応し、12 チャネルをサポートします。その結果、米国では、5 GHz 帯域は実際に 3 つの帯域の集合体になります。

- 5.150 ～ 5.250 GHz（UNII-1）
- 5.250 ～ 5.350 GHz（UNII-2）
- 5.725 ～ 5.875 GHz（UNII-3）

RF 電力の用語

dB、*dBi*、および *dBm* の各用語は、それぞれ、システムのポイントで測定したとき、無線で感知したとき、または基準電力レベルと比較したときの電力の変化量を表すために使用されます。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、電力レベルの減衰または増幅に主に使用されます。dB は、別の標準化された値に対する信号の対数比です。たとえば、dBm の場合は 1 ミリワットに対して値が比較され、dBw の場合は 1 ワットに対して値が比較されます。

計算式は、次のとおりです。

```
power (in dB) = 10 * log10 (signal/reference)
```

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

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

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

屋内の WLAN および屋外の WLAN 展開は両方とも、RF 展開において異なる課題があり、これらは分けて分析する必要があります。ただし、屋内使用に関しては、一般的なルールがあります。9dB 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。9dB 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。

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 2.2dBi です。これは、アンテナの最大エネルギー密度が等方性アンテナよりも 2.2dB 多いことを意味しています。

dBm

dBm（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。信号は送信した時点から値が減るため、レシーバの感度は、マイナス dBm（-dBm）で表されます。感度は、信号を理解不能と見なす前にレシーバが受信可能な最小電力を示します。

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、約 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

詳細については、Cisco TechNote『*RF Power Values*』（http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00800e90fe.shtml）を参照してください。

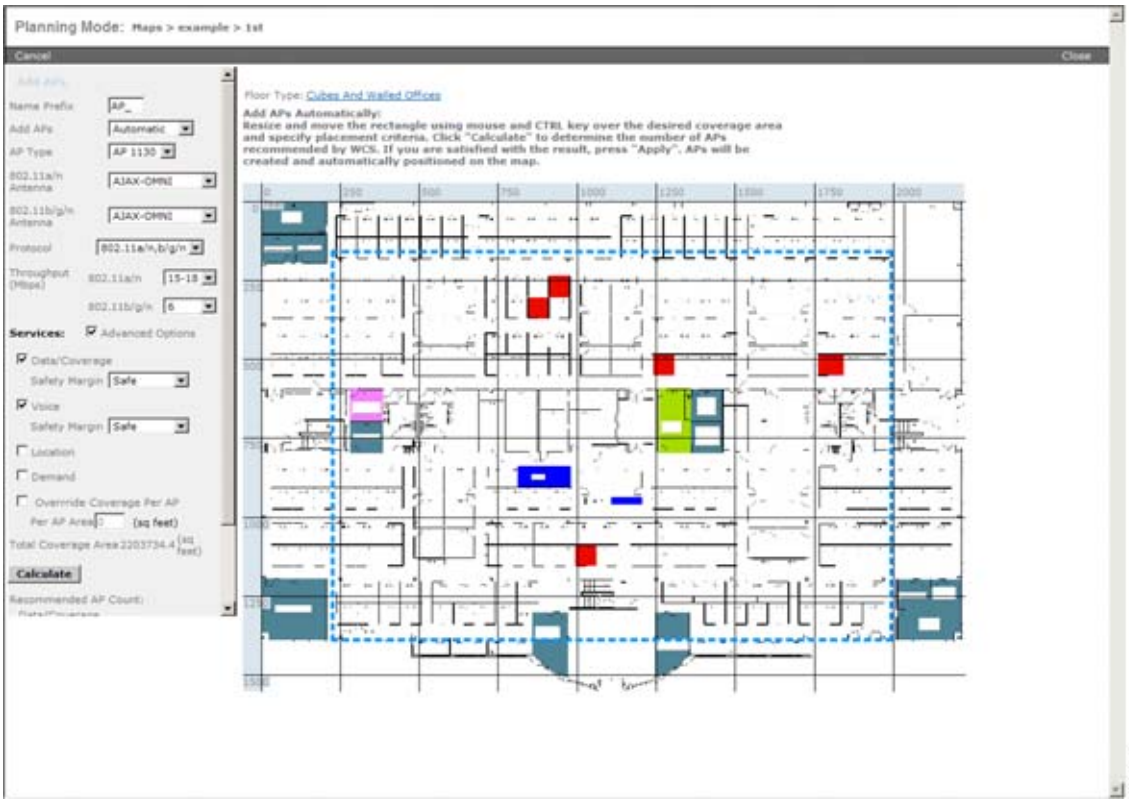
RF 導入の計画

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

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

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

図 3-4　Cisco Prime Infrastructure の計画ツール



オーバーラップする WLAN カバレッジのさまざまな導入の種類

無線ネットワークで設定する WLAN カバレッジのオーバーラップの規模は、使用状況によって異なりますが、一部の例外を除き、すべての設計は再送信とデータ レートの変化を最小限に抑えるように展開する必要があります。無線ネットワークは、データ専用、音声、ビデオ、およびロケーションベース サービス（LBS）、またはこれらの組み合わせに対して導入できます。違いは、配置されている AP のパターンとカバレッジ エリアで RF がオーバーラップする量にあります。

WLAN 導入を計画するときは、WLAN 導入の今後の用途を考慮に入れる必要があります。データ専用の導入だけでなく、付加サービスもサポートするように WLAN 導入を変えることは、単に AP を追加するだけでは済みません。詳細なサイト サーベイが必要になるほか、既存の AP を再配置が必要になる可能性もあります。

ネットワーク導入のさまざまなタイプの詳細については、以下のガイドを参照してください。

- 『*Cisco Unified Wireless iPhone 792x Deployment Guide*』
  http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7925g/7_0/english/deployment/guide/7925dply.pdf
- 『*Cisco VoWLAN Troubleshooting Guide: Site Survey and RF Design Validation*』
  http://www.cisco.com/en/US/docs/wireless/technology/vowlan/troubleshooting/8_Site_Survey_RF_Design_Valid.html
- 『*Cisco Site Survey Guide*: Deploying Cisco 7920 IP Phones』
  http://www.cisco.com/en/US/docs/wireless/technology/7920/site_survey/guide/survovr.html
- 『*Wireless LAN Design Guide for High Density Client Environments in Higher Education*』
  http://www.cisco.com/web/strategy/docs/education/cisco_wlan_design_guide.pdf
- 『*Cisco Wireless Mesh Access Points, Design and Deployment Guide*』
  http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh_chapter_0100.html
- 『*Wi-Fi Location-Based Services Design Guide: Best Practices Location-Aware WLAN Design Considerations*』
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich5.html

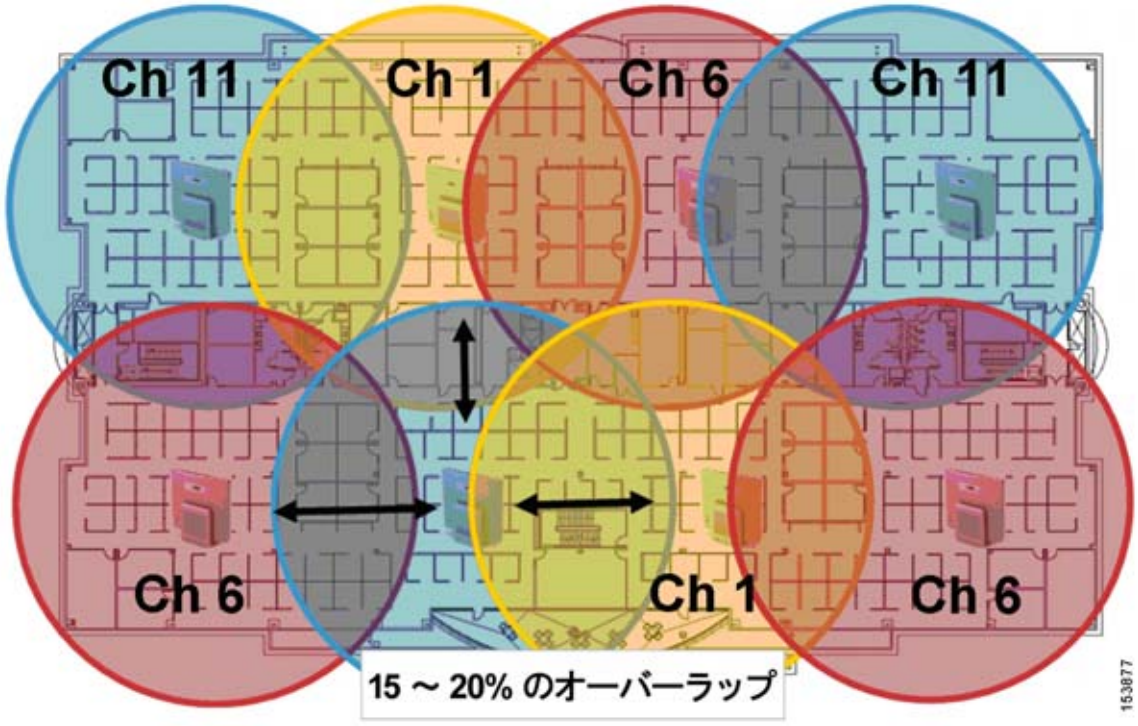
データ専用の導入

データ専用の導入の場合、大きなオーバーラップは必要ありません。これは、802.11 クライアントが、データ レートを下げ、時間をかけて転送することで、近くの AP からの低レベルの信号に応答するからです。必要なオーバーラップは、「WLAN のデータ レート要件」（P.3-13）で説明されているように、WLAN のデータ レート要件によって決まります。データ専用ネットワークでは、AP 間の最適な距離は、通常約 120 ～ 130 フィートです。ただし、AP の間隔を見積もる際は、壁の密度、機械、エレベータ、スチール製のケージがある広い空間など、RF カバレッジに影響を与えるオブジェクトの要素を念頭に置くようにしてください。結果は、RF 環境によって異なる可能性があります。無線リソース管理（RRM、WLC における *Auto-RF* とも呼ばれます）はこのような導入向けに開発されたもので、RF カバレッジを制御する上で非常に便利です。

音声導入

図 3-5 は、音声ネットワークのパターンとオーバーラップを示しています。

図 3-5　音声用の単一フロア サイトの調査



AP は互いに近くにまとめられ、データ専用の導入に比べ、多くのオーバーラップがあります。これは、音声クライアントは、パケットがドロップされないように、より良い AP に移動する必要があるからです。また、通常は、従来よりも小規模のセルで実行し、オーバーラップしているセルが -67 dBm 以上になるようにします。これは、1 つのセル全体における同質性を高め、クライアント デバイスでのプロセッサの負荷を減らすなど、さまざまな効果をもたらし、リンクの安定性を高め、遅延を減らします。定義されたエリアで必要な AP は 1 つだけですが、遅延およびロード バランシングの対策として、オーバーラップしていないチャネルに 2 つの AP を設置し、その導入において受信信号強度表示（RSSI）が常に 35 を超えるようにすることを推奨します。たとえば、Cisco 792x VoIP 電話機の導入の場合、導入において RSSI が常に 35 を超えるようにすることを推奨します。これは VoIP 電話の受信率を高めると同時に、join 超過をある程度許容するためです。また、電話に対するローミング オプションが強化されます。

低ノイズ バックグラウンドを配慮した設計は、セル内の比較的高いエネルギー密度と同様に重要であることを、忘れないでください。これは、AP に対して最適なベースライン電力設定が 35 ～ 50 mW の範囲内であることを意味します。これには通常、100 mW でカバレッジ モデルを導入する場合よりも約 15% 多い AP が必要となります。

既存の WLAN、不正クライアント、802.11 に準拠していない不正な製品による干渉（たとえば、電子レンジや各種コードレス電話）など、問題のある特定のエリアや干渉の原因となる可能性があるものを特定して、その特徴を調べるには、事前のサイト サーベイが有効です。すべての利害関係者によって確認され認証される必要がある設計に従い、カバレッジ モデルが、利害関係者によって示された機能要件に準拠していることを確認するために、事後のサイト サーベイを究極の監査メカニズムとして考える必要があります。サイト サーベイの詳細については、『*Cisco VoWLAN Troubleshooting Guide: Site Survey and RF Design Validation*』を参照してください。

http://www.cisco.com/en/US/docs/wireless/technology/vowlan/troubleshooting/8_Site_Survey_RF_Design_Valid.html

間隔を見積もる際は、RF 環境によって結果が異なる可能性があるため、壁の密度、機械、エレベータ、スチール製のケージがある広い空間など、RF カバレッジに影響を与えるオブジェクトの要素を忘れないようにしてください。結果は、RF 環境によって異なる可能性があります。フォークリフト、人々の集団、クレーンや同様の搬送装置によってエリアを移動する大きな物体など、一時的な動きも考慮に含めるようにします。

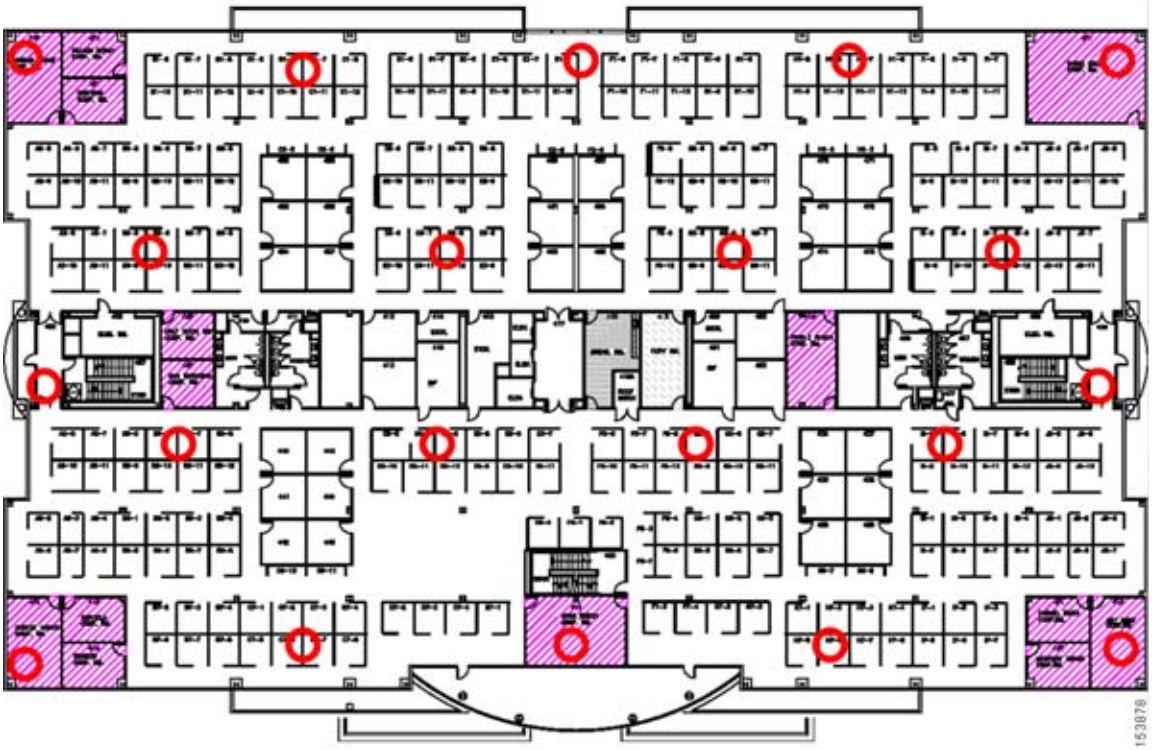
WLC は一般に、サイトの予備評価（*予測的なサイト サーベイ*）に非常に効果的な方法で、WLAN インフラストラクチャを高速に導入し、エリアの RF 測定に使用できます。医療、小売、製造業界などで一般的に見られる複雑なエリアには、サイト サーベイをエンドユーザに実施してもらうことも効果的な方法です。無線音声の導入の詳細については、第 9 章「VoWLAN の設計に関する推奨事項」を参照してください。

ロケーション ベース サービスの導入

3 つ目の導入の種類は、ロケーション ベース サービス（LBS）の導入です。これは、究極のセル カバレッジだけでなく、最適な AP の場所に依存するため、現在のアプリケーションの中でも最も複雑です。LBS の導入は、WLAN インフラストラクチャを使用して、何千ものデバイスを同時に追跡できます。LBS 例としては、無線ネットワークで機器やデバイスを特定する Wi-Fi タグ タイプの導入または資産追跡導入があります。LBS は、無線ネットワークのどこに無線クライアントがあるのかを図やダイアグラムで単純に示したりするためにも使用できます。この情報を使用することで、不正クライアントや AP の場所を提供し、無線インフラストラクチャのセキュリティを強化することができます。さらに、クライアントのトラブルシューティング能力を大幅に向上させることができます。

ロケーション ベースのサービスの導入では、AP は交互にずらして配置されます。交互にずらすと、デバイスの場所をより正確に見積もることができます。図 3-6 は典型的な配置パターンを示しています。

図 3-6　　単一フロアのロケーション管理の展開の例



ロケーション ベース サービスについては、第 11 章「Cisco モビリティ サービス エンジン」および次の Web サイトにあるシスコの『*Wi-Fi Location Based Services 4.1 Design Guide*』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/wifich1.html.

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

7920 および 7921G 端末の詳細は、以下の資料を参照してください。

- 『*Cisco Unified Wireless IP Phone 7921G*』

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet0900aecd805e315d.html

- 『*Cisco Unified Wireless IP Phone 7920*』

  http://www.cisco.com/en/US/products/hw/phones/ps379/products_data_sheet09186a00801739bb.html

VoWLAN インフラストラクチャを導入する場合は、単に WLAN に QoS を提供すればよいというわけではありません。音声 WLAN では、サイト サーベイのカバレッジ要件、ユーザの動作、ローミング要件、およびアドミッション制御について検討する必要があります。これらの要件については、以下のガイドで説明しています。

- 『*Design Principles for Voice Over WLAN*』

  http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/net_implementation_white_paper0900aecd804f1a46.html

- 『*Cisco Unified Wireless IP Phone 7921G Administration Guide*』

  http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7921g/5_0_1/english/administration/guide/21adm501.html

- 『*Cisco Wireless IP Phone 7920 Design and Deployment Guide*』

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

WLAN のデータ レート要件

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

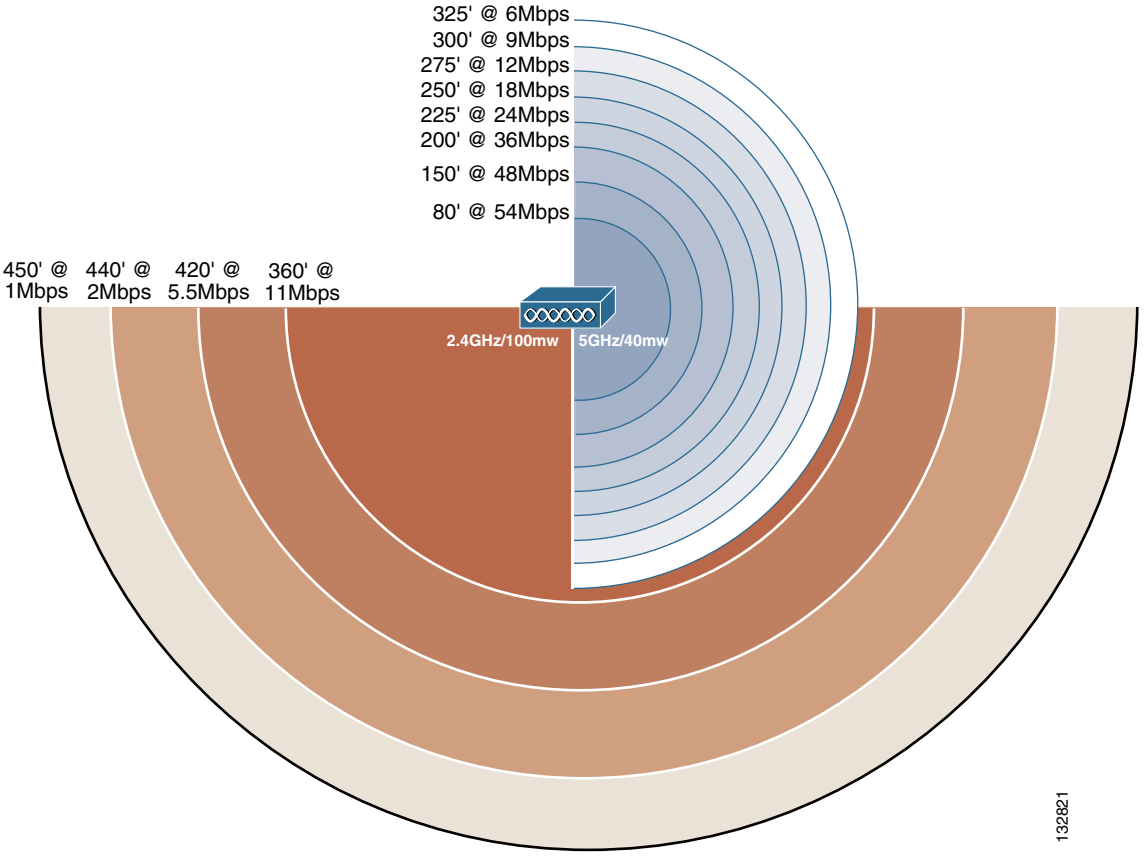
カバレッジ エリアに対するデータ レート

AP では、無線リンク上で異なる符号化技法を使用して異なるデータ レートを実現しており、データがノイズからより簡単に回復されるようになります。これは、さまざまなレシーバ感度でさまざまなデータ レートに対して確認されることです。1 Mbps のデータ レートでひとつのパケットに対して送信される *シンボル*（かけらの集まり）は、11 Mbps で同じパケットに使用されるシンボルの数を上回ります。これは、低いデータ レートでデータを送信する方が、高いビット レートで同じデータを送信するより

も時間がかかることを意味します。また、無線にアソシエートされているクライアントが複数ある場合は、同じ長さのパケットの送信により多くの時間がかかるため、データ レートが低いクライアントが、データ レートの高いクライアントの最大データ スループットに影響を与えます。

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

図 3-7　　カバレッジと比較したデータ レート

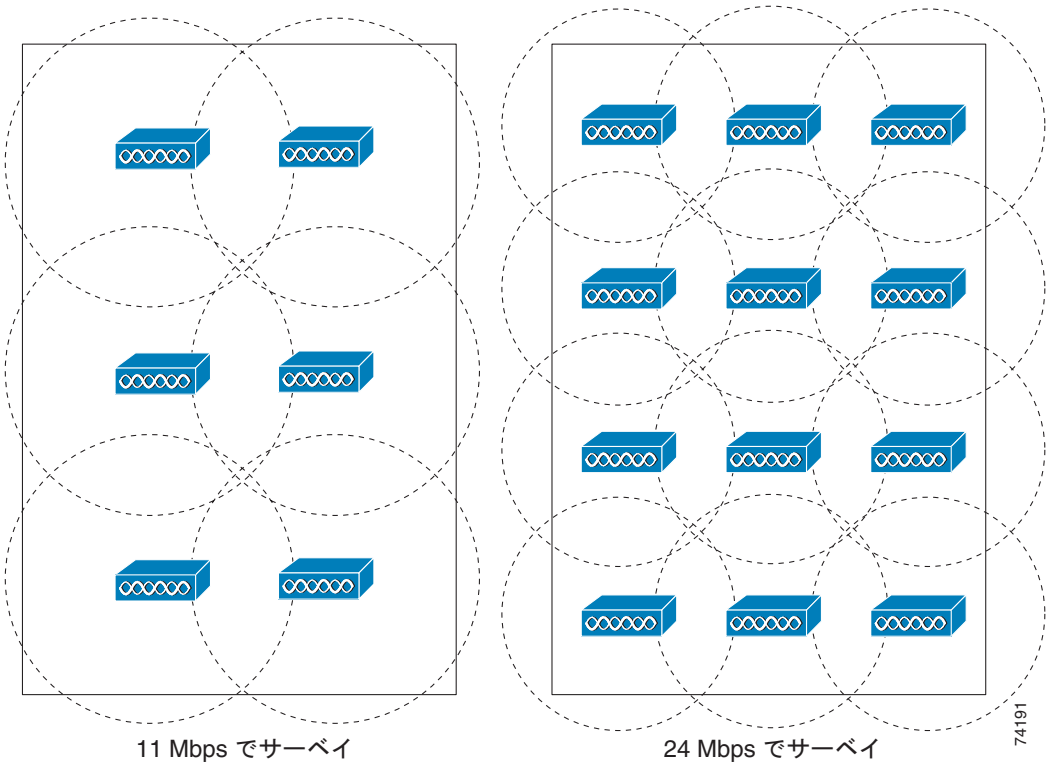


たとえば、屋内で NIC カード上の標準アンテナと AP を使用した場合、1 Mbps の円の直径は約 700 フィート（210 m）となり、11 Mbps の円の直径は約 200 フィート（60 m）となります。これらのカバレッジの直径は屋内環境のタイプに左右されます。オープン プラン オフィスのビルディングは、オフィスが壁で仕切られているビルディングとは異なります。アンテナのゲインを上げると、距離が長くなり、放射が均等に行われるのではなく、特定方向に集中するように放射パターンの形状が変化します。

異なるデータ レートに対する AP の密度

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

図 3-8　カバレッジの比較と異なるデータ レートに対する AP の密度



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

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

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

クライアント密度とスループット要件

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

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

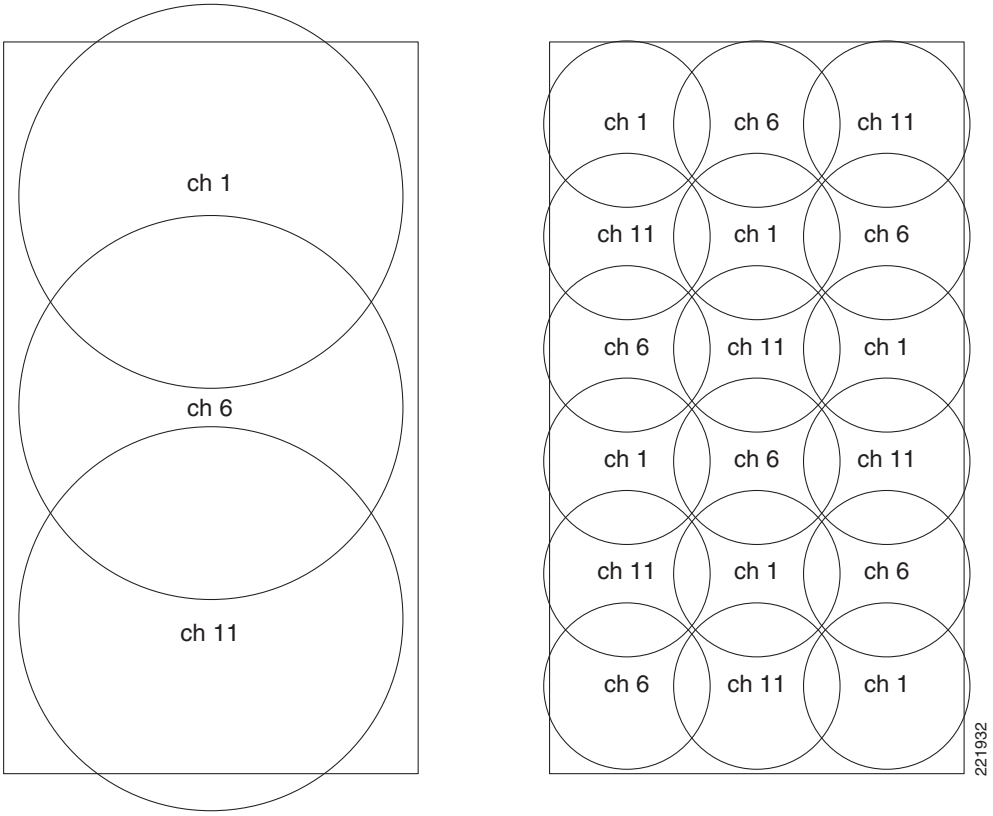
これを考慮して、アクティブなアソシエーション（アクティブ クライアント）の最大数を見積もる必要があります。これは、特定のアプリケーションに応じて若干調整できます。

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

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

1 つの AP で提供される集約スループットを利用するユーザの数を抑えることで、ユーザあたりの潜在的なスループットを増やすことができます。これは、カバレッジ エリアのサイズを小さくするか、同じカバレッジ エリアの重複しないチャネルに 2 番目の AP を追加することで実現します。カバレッジ エリアを小さくするには、AP の電力またはアンテナ ゲインを減らすと、結果としてカバレッジ エリアのクライアントが少なくなります。これは、同じエリア全体に対してより多くの AP が必要になり、導入コストが増加することを意味しています。この例を図 3-9 に示します。

図 3-9　クライアント パフォーマンスを高めるために出力電力を変更



180 ユーザー/フロア
30 mW 送信電力
3 アクセス ポイント
60 ユーザー/AP
11 Mbps データ レート

180 ユーザー/フロア
5 mW 送信電力
18 アクセス ポイント
10 ユーザー/AP
11 Mbps データ レート

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

WLAN のカバレッジ要件

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

電力レベルとアンテナの選択

電力レベルおよびアンテナの選択は、AP の配置を決めるうえで、密接に関連しています。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 を使用することを推奨します。詳細については、「無線リソース管理（Radio Resource Management）」（P.3-27）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。
- 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。
- 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ていると言えます。

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

ゲインおよび指向性によって、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。

アンテナの選択に関する詳細については、次の Web サイトにあるシスコの『*Antenna Selection Guide*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

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。水平面では 360 度、垂直面では 75 度のほとんど対称的な放射パターンを持ちます（ダイポール アンテナが垂直に立てられていることを前提としています）。全方向性アンテナの放射パターンは、通常、ドーナツのような形をしています。

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

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

図 3-10　全方向性の RF パターン

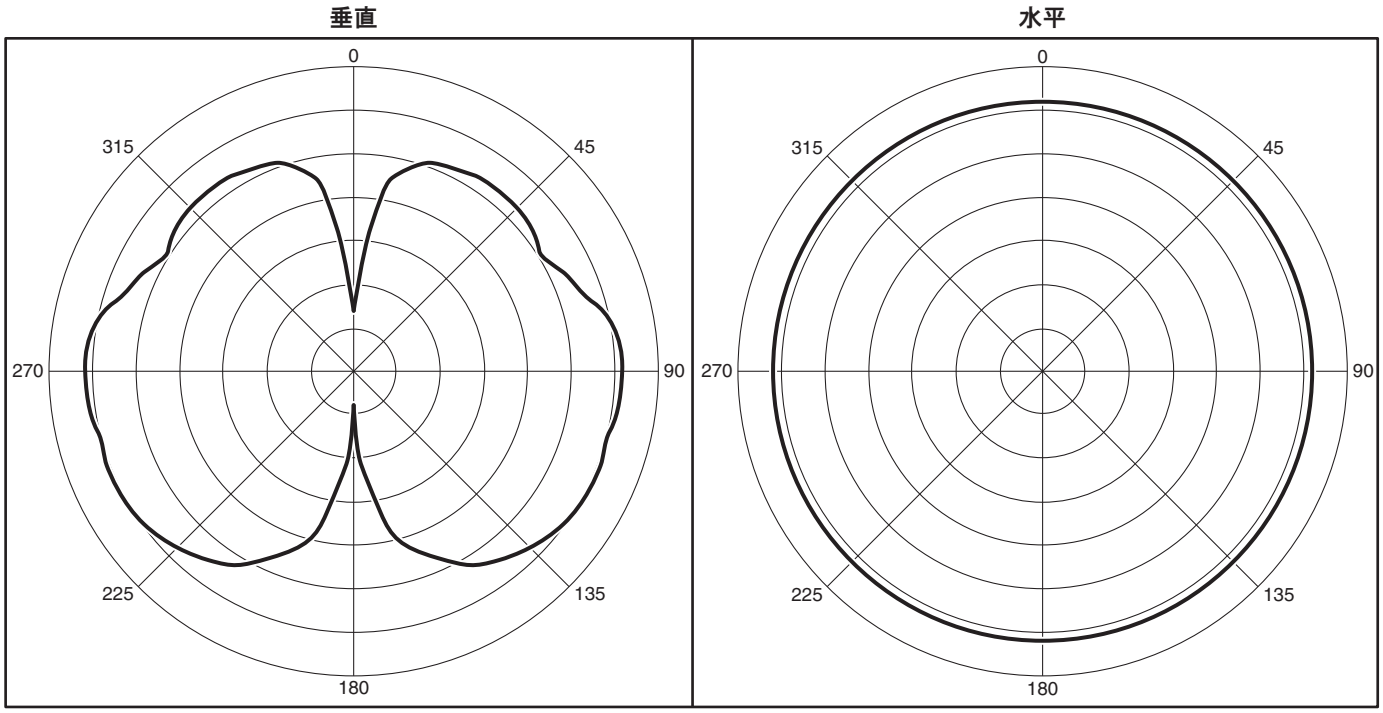
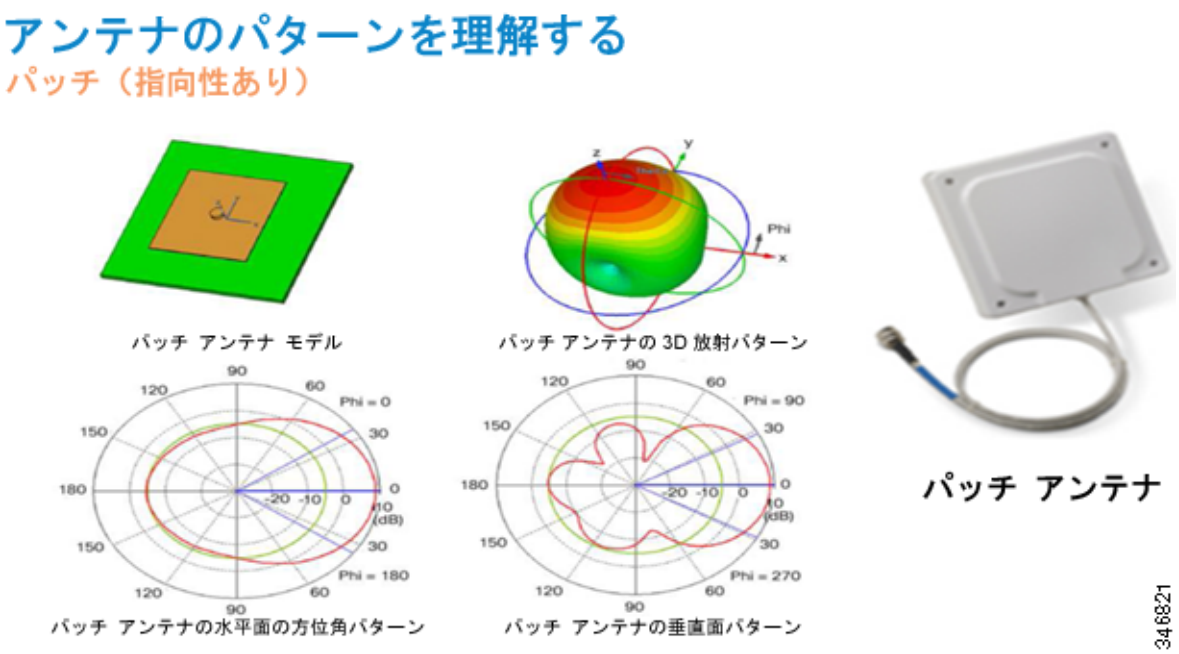


図 3-10 のパターンを見ると、特に、ビルディングの外部に向けて放射するパターンとなるように外壁に取り付ける場合、これは壁面で使用するには不向きなアンテナである可能性があります。

パッチ アンテナ

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

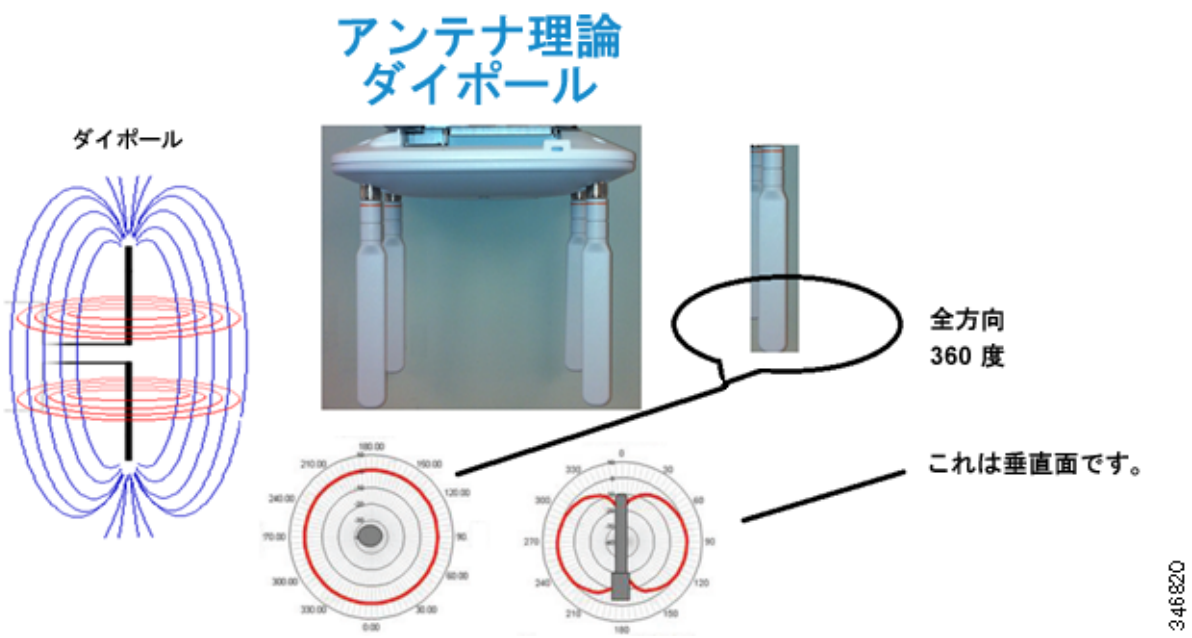
図 3-11　壁面取り付けパッチ アンテナの水平平面



ダイポール アンテナ

ダイポール アンテナ（図 3-12 を参照）は、無線アンテナの最も基本的なタイプです。これらは、さまざまな供給メカニズムおよび放射エレメントにより、さまざまな形状で提供されます。ダイポール アンテナは、理論的観点から最もシンプルかつ最も実用的なアンテナであり、今日最も一般的に見られるタイプのアンテナです。

図 3-12　ダイポール アンテナ



セキュリティ ポリシー要件

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

RF 環境

WLAN およびその機器のパフォーマンスは、その RF 環境、機器、選択、カバレッジ設計、監査の質、設定、および導入の質によって異なります。さまざまな環境上なマイナス要因が、チャネルに干渉し、なんらかの方法で信号の RF の特性を変え、無線通信を妨害する可能性があります。次に例を示します。

- 2.4 GHz のコードレス電話および Bluetooth
- 金網と化粧しっくいで作られた壁
- ファイリング キャビネットおよび金属製の装置ラック
- ワイヤレス カメラ
- スパークを発生する可能性のある高荷重の電動機、溶接機、ロボットなど
- 電波を反射させる追加金属が組み込まれた防火壁および防火扉
- コンクリート

- 冷蔵庫
- 空調配管
- アマチュア無線（ハム）などその他無線装置
- 電子レンジ、特に業務用塗料乾燥機器
- 指向性または再試行の増加をもたらす可能性のあるアンテナの近くの HVAC 導管
- フォークリフトや金属製の組み立てなどの大規模な一時的要素
- 自社の WLAN 機器とは別個の他の WLAN 機器（近隣の企業など）

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

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 15 ～ 25
  - （Cisco 792x VoIP 無線端末または同様の端末を使用する場合）データが存在するときの音声ユーザ数は 7 ～ 8

  この数字は、あくまでも指針であり、使用する端末によって異なる可能性があります。端末の要件を確認してください。
- AP データ レートは、設計されたもの、およびサイトサーベイが実施されたものに限定する必要があります。低いデータ レートを有効にすると、同一チャネル干渉およびクライアントに対するスループットの変化が増す原因になることがあります。
- AP の数は、カバレッジおよびスループット要件に依存し、変化する可能性があります。たとえば、シスコ内部の情報システム（IS）グループは現在、データ専用動作については、3,000 平方フィートのフロア空間あたり 6 個の AP を使用しています。

（注）　環境の変動性に基づき、必要な AP の数および最適な配置を決めるために、サイトサーベイを実施することを推奨します。

WLAN カバレッジの手動による微調整

数多くの要素が WLAN カバレッジに影響します。次の内容で構成されています。

- チャネルおよびデータ レート選択
- ロケーションベースのサービス、音声、またはデータ専用の重複する WLAN カバレッジ
- 電力レベル
- アンテナの選択（指向性または全方向性アンテナ）

所定のデータ レートおよび場所に対して、WLAN 設計者がカバレッジ エリアまたはカバレッジ形状を変えるために、電力レベルを変更したり、別のアンテナの使用を決める可能性があります。電力レベルの変更やチャネルの選択は、次に示すように手動で行うことができます。または、Cisco Prime

Infrastructure では RRM アルゴリズムにより、これを自動的に行えます。電力レベルおよびチャネルの管理には、RRM を使用することを推奨します。チャネル変更アルゴリズムは、干渉源が非常に破壊的（かつ永続的）な場合にだけチャネル トポロジの変更が行われるように、きわめて複雑であることを忘れないでください。変更した場合、クライアントの再アソシエートが必要になり、音声コールはドロップされます。AP 電力の変更はクライアントには影響しません。詳細については、図 3-16 を参照してください。

チャネルおよびデータ レートの選択

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

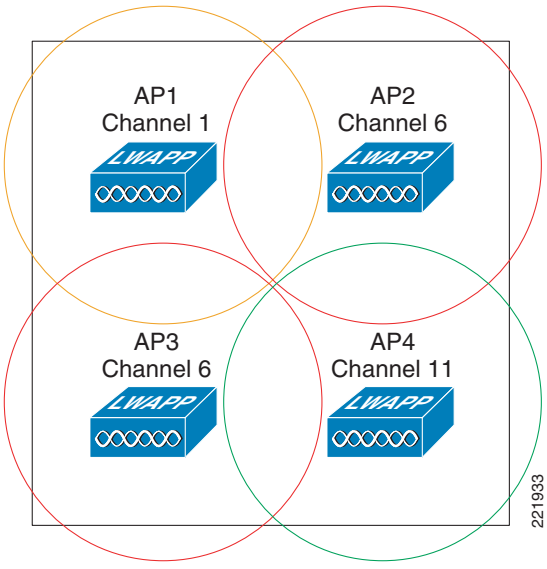
チャネルは、次のようにカバレッジ セルに割り当てる必要があります。

- オーバーラップしているセルは、オーバーラップしていないチャネルを使用する必要があります。
- 複数のセルでチャネルを再利用する必要がある場合、これらのセル間のオーバーラップが最小限になるようにする必要があります。図 3-13 はこのパターンを示しています。802.11a/n/ac の展開では、セルがオーバーラップするので、チャネルの隣接を避ける必要があります。

チャネルの選択に関する推奨事項

図 3-13 は、一般的な 2.4 GHz 帯域のチャネルの設定例を示します。通常、チャネルの選択は自動的に行われますが、「手動でのチャネル選択」（P.3-24）で説明されているように、手動で行うこともできます。

図 3-13　AP に割り当てられたチャネル



実際の展開での使用を考えているものと同じ周波数でサイトサーベイを行う必要があります。これらは接続と AP の最適な配置のための環境をテストするために使用されます。サイトによってはノイズ バックグラウンドが高い場合があり、1 つまたは複数のチャネルを使用するうえで妨げとなることがあります。サイト サーベイにより、特定の場所にある特定のチャネルが干渉およびマルチパスに対して

どのように反応するかをより正確に把握できます。チャネル選択は、チャネル相互および隣接チャネルの干渉を計画するうえで役立つほか、周波数を再利用できる場所に関する情報を提供します（図 3-14 を参照）。

（注）　サイト サーベイの詳細については、Bruce E.Alexander 著『*802.11 Wireless Network Site Surveying and Installation*』（2005 年、Cisco Press）を参照してください。

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

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

手動でのチャネル選択

図 3-14 は、[wireless] メニューで、802.11b 無線の 1 つを設定するための Web ページのスクリーンショットです。右上では、チャネル 11 が手動で選択され、送信電力が最高レベルの 1 に設定されています（8 の場合、AP は最も低いレベルに設定）。

（注）　割り当て方法は、手動でこれらの設定を制御する必要がある場合を除いて、通常はグローバル設定のままにします。これにより、WLC が RRM で決定されたとおり、動的にチャネル番号を変更できます。詳細については、「無線リソース管理（Radio Resource Management）」（P.3-27）を参照してください。

図 3-14　Channel Assignment

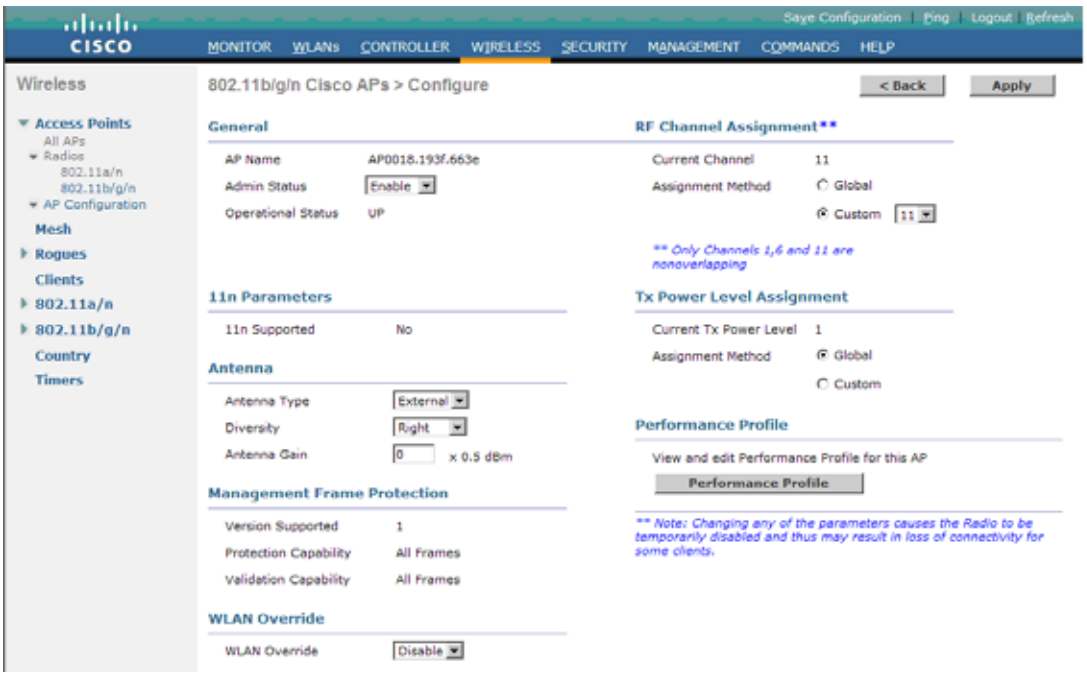
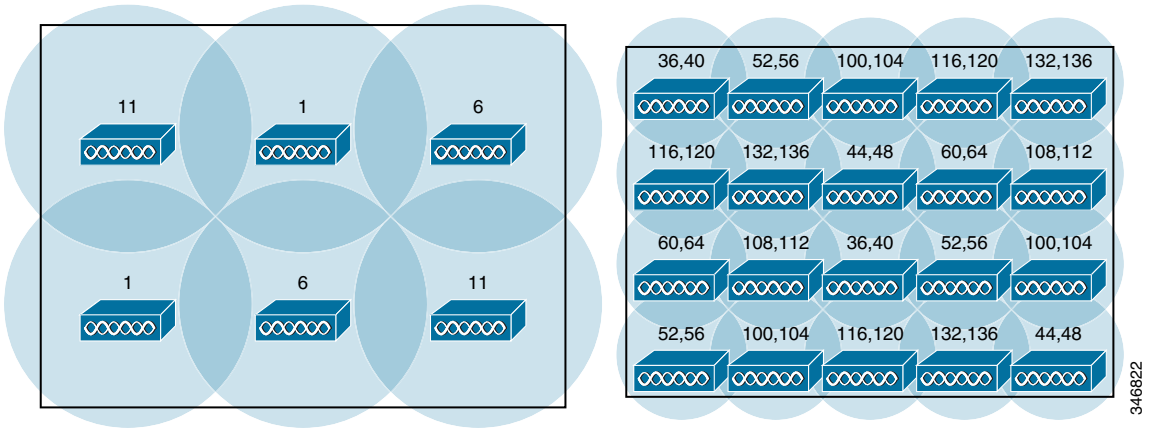


図 3-15 に示すように、デュアルバンド導入方式を実装することもできます。図の左上の部分は 802.11b/g/n だけの導入を示しています。この場合は、3 つのオーバーラップしないチャネル（チャネル 1、6、11）を使用して、相互チャネルの干渉が最小のパターンをマップしています。同じチャネル上にあり、別のアクセス ポイントのカバレッジ パターンとオーバーラップしながら十分な電力レベルで動作している、近くの AP からの干渉のことです。この図には、8 つのオーバーラップしないチャネルを使用した 802.11a/n/ac 導入も示されています。図の右側は、デュアルバンド導入でチャネルをマップする方法を示しています。

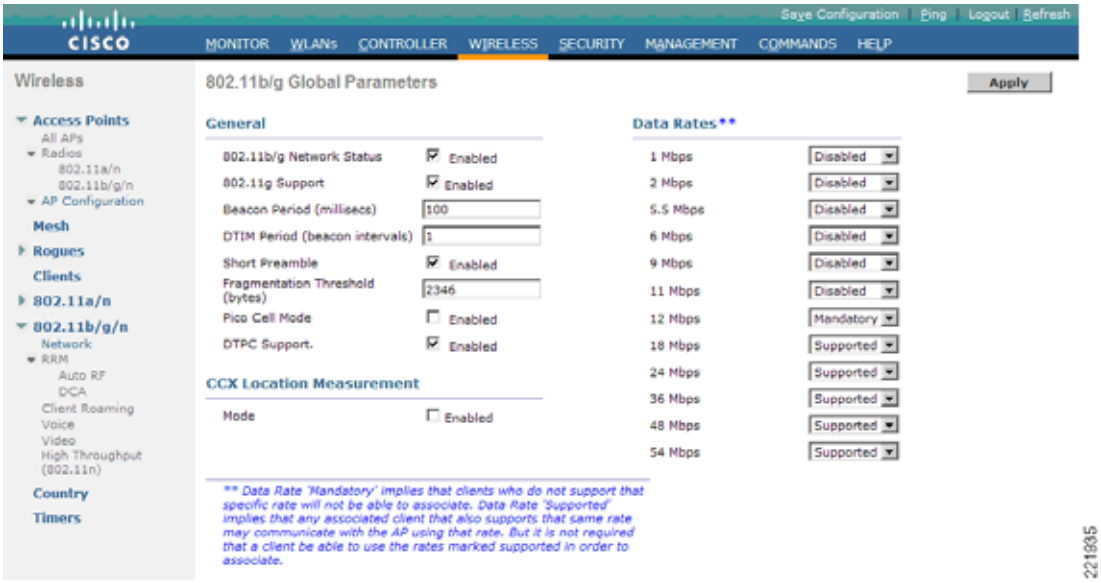
図 3-15　デュアル バンド導入の図



データ レートの選択

図 3-16 は、802.11b/g/n のグローバル パラメータを管理する Cisco WLC ウィンドウのスクリーンショットです。データ レート設定は画面の右側に示されています。

図 3-16　データ レートの割り当て



データ レート モード

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

データ レートは 1 秒あたりのメガビット数で表します。各データ レート モードを Mandatory、Supported、または無効（Disabled）に設定できます。

必須モード（Mandatory）

必須モードでは、ユニキャストとマルチキャストの両方を含むすべてのパケットの伝送を許可します。少なくとも 1 つの AP のデータ レートが必須に設定され、この AP にアソシエートするすべてのクライアントが、ネットワークを使用するための無線でこのデータ レートを物理的にサポートできる必要があります。さらに、AP にアソシエートする無線クライアントについては、最も低い必須データ レートで現在パケットを受信でき、無線が最大の必須データ レートを物理的にサポートしている必要があります。複数のデータ レートが Mandatory に設定されている場合は、マルチキャストおよびブロードキャスト フレームは、アソシエートされているすべてのクライアントで共通の最高の必須伝送レート（すべてのクライアントで最も低い必須受信レート）で送信されます。これにより、すべてのクライアントがブロードキャスト パケットを受信できます。最も低い必須レートは通常、1 Mbps に設定されます。

サポート モード（Supported）

サポート モードでは、ユニキャスト パケットだけの伝送を許可します。AP はこのレートではユニキャスト パケットだけを送信します。マルチキャストおよびブロードキャスト パケットは、必須に設定されているデータ レートのいずれかで送信されます。無線クライアントは常に、可能な最も高いデータ レートで送受信しようとします。無線クライアントは、ユニキャスト パケットを送受信するために、Supported または Mandatory に設定された最も高いデータ レートを AP とネゴシエートします。無線クライアント デバイスは、任意の必須レートまたはネゴシエートしたレートより低いレートでブロードキャストまたはマルチキャスト パケットを受信できます。

無効（Disabled）

AP はこの設定ではデータを送信しません。

最低および最高の必須レートの設定

AP にアソシエートされている複数のクライアントは、干渉、障害物、または AP からの距離に応じて、異なる伝送レートを使用できます。たとえば、802.11b クライアントが AP から離れた場所にあり、それが原因で 1Mbps の速度でしか送受信できない場合、最低必須レートが（図 3-16 を参照）1 Mbps に設定されているため、クライアントは AP にアソシエートできます。54Mbps で AP にアソシエートしている別の 802.11g クライアントについては、すべてのクライアントが受信できる最高必須レートが 1 Mbps であるため、AP はブロードキャストおよびマルチキャストを 1 Mbps で送信します。最低必須レートが 5.5 Mbps に設定された場合、802.11b クライアントは、最低必須レートでブロードキャスト パケットを受信できないため、AP にアソシエートできません。

図 3-16 では、最高必須レートが 11 Mbps に設定されていることに注意してください。最高必須レートは、クライアントの無線が物理的に送信できる必要があるものを AP に示しています。これは、そのレートで実際にパケットを送受信するということではありません。無線が物理的にそのレートをサポートするということです。無線クライアントは、最低必須レートでパケットを受信できるだけで構いません。802.11b デバイスの無線は 11 Mbps で物理的に送信できるため、802.11b デバイスは図 3-16 に示されている AP にアソシエートできます。より高いデータ レート（18 Mbps など）が必須に設定されている場合は、802.11g クライアントだけが AP にアソシエートできます。

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

無線リソース管理（Radio Resource Management）

Cisco WLAN の *スプリット MAC* アーキテクチャ（第 2 章「Cisco Unified Wireless のテクノロジーおよびアーキテクチャ」を参照）では、802.11 のデータと管理プロトコルの処理および AP の機能は、CAPWAP AP と中央集中型 WLC の間で分散されています。具体的には、プローブ応答や MAC レイヤの暗号化など、時間依存型のアクティビティはアクセス ポイントで処理されます。一方システム規模での可視性が必要となるその他すべての機能は、WLC に送信されます。

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

（注）　RF ネットワーク グループ（RF グループ）は、モビリティ グループと同じではありません。モビリティ グループは、ローミング イベントでクライアントが IP アドレスを変更する必要がないように、1 ～ 24 WLC のモビリティ ドメインを定義します。これは、クライアントにサービスする新しい AP を扱う*外部*コントローラに*アンカー*コントローラからクライアント データを転送するための Ethernet over IP トンネルを構築することで実現されます。

リソース管理（RRM）は、RF カバレッジ エリアを管理するために、チャネルおよび電力（それぞれ、動的なチャネル割り当てと動的な送信電力の管理を使用）を調整できます。RRM により、AP の電力レベルは、近隣の AP とのベースラインの信号強度が -65 dBm（設定可能）に保たれるように調整されます（RRM 動作の概要を参照）。RRM は、現在 AP が配置されているチャネルで、近くに干渉源があることが分かると、AP のチャネルを調整します。無線ネットワークの感度およびスループットが最適になるよう、継続的に RF カバレッジを最適化します。

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

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

RRM 動作の概要

WLC でグループ モードが有効の場合、RF グループごとにリーダーを選び、RF ドメインを形成します。リーダーの役割は、WLC のグループからネットワーク全体のネイバー データ パケットを収集し、システム全体の最適なマップのために、チャネル / 電力計算を行うことです。グループ モードが有効でない場合は、コントローラは、CAPWAP 経由で接続されている AP から集められたネイバー データだけに基づいて計算を行い、AP 間の信号を -70 dBm に最適化しようとします。

AP は RRM ネイバー パケットを定期的に、最大電力で送信します。AP はフルパワーで RRM ネイバー データ パケットを定期的に送信します（ネイバー パケットには環境の信号強度および無線要素に関する情報が含まれます）。これらのメッセージには、RF ネットワーク（グループ）名、BSSID、およびタイム スタンプのハッシュであるフィールドが含まれています。AP は、デフォルトの RF ネットワーク名（*RF Network Name*）で送信された RRM ネイバー パケットだけを受信します。

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

表 3-4 は、システム内のデバイスのさまざまな機能の概要を示しています。

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

表 3-4　デバイスの機能

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

RRM は、RRM アルゴリズムとは別個に行われる *不正の検出*（チャネル スキャン）と混同しないでください。AP は、不正な AP のすべての国別チャネルを定期的にスキャン（チャネル スキャン）することによって、不正の検出を実行します。AP は、他のチャネルを 60 ms 以内の周期でリッスンし、*オフチャネル*に切り替えます。この間に収集されたパケット ヘッダーは WLC に送信され、そこで Service Set Identifier（SSID）が不正なクライアント、アドホック クライアント、および干渉する AP をブロードキャストするかどうか、不正な AP を検出するために分析されます。

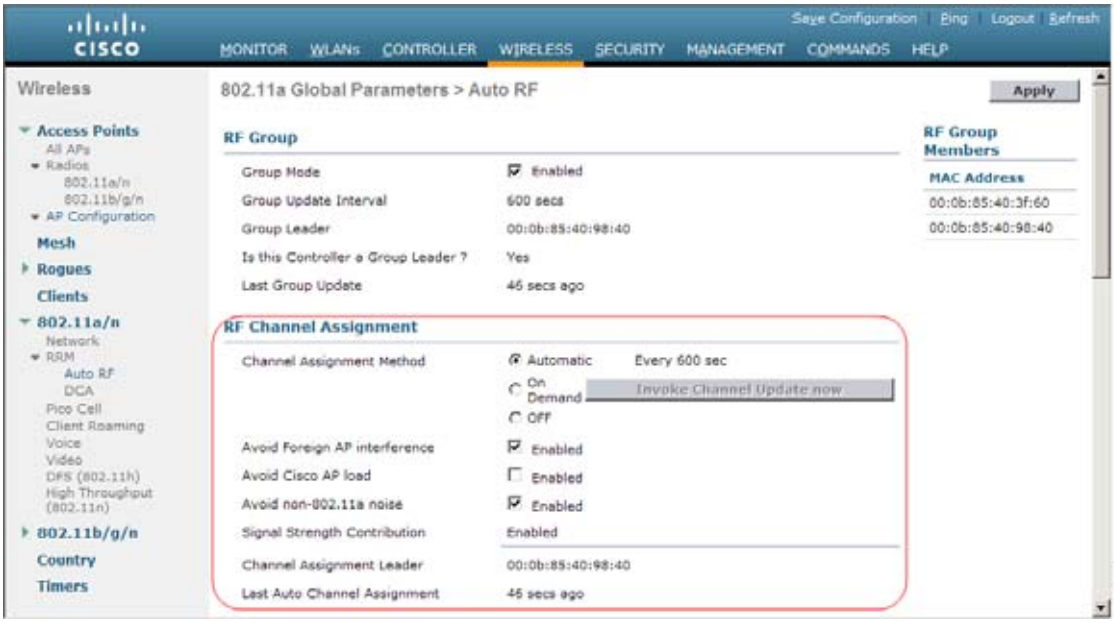
デフォルトでは、各 AP はその時間のオフチャネルの約 0.2 パーセントを費やします。これは、WLAN のパフォーマンスに悪影響を与える可能性のある 2 つの隣接する AP が同時にスキャンを行うことのないように、すべての AP に静的に分散されます。AP が受信したクライアント パケットは、CAPWAP ステータス フィールドが追加されて WLC に転送されます。このフィールドは、パケットの受信時に AP によって受信するされたパケットの RSSI および信号対雑音比（SNR）を含む無線情報を WLC に提供します。

RRM コンフィギュレーションの設定

WLC の *Auto-RF* とも呼ばれる無線リソース管理（RRM）は、チャネル選択のグローバル設定を使用して WLC で有効化または無効化することができます（図 3-14 を参照）。このウィンドウから、AP のチャネルおよび送信電力レベルを手動で設定することもできます。さらに、WLC グローバル Auto-RF コンフィギュレーション ウィンドウから RRM を有効化または無効化できます。RRM が帯域ごとに実効されることに注意してください。5 GHz 帯域の RF グループの計算は、2.4 GHz 帯域の計算とは異なります。

Auto-RF コンフィギュレーション ウィンドウは、3 つのセクションに分かれており、右側のスクロール バーを使用して移動します。最初のセクション（図 3-17 を参照）は、動的なチャネルの割り当てに関する設定です。AP が配置されているチャネルを WLC で自動的に変更できるようにします（詳細については、チャネルの動的割り当てを参照してください）。

図 3-17　Auto-RF（セクション 1）

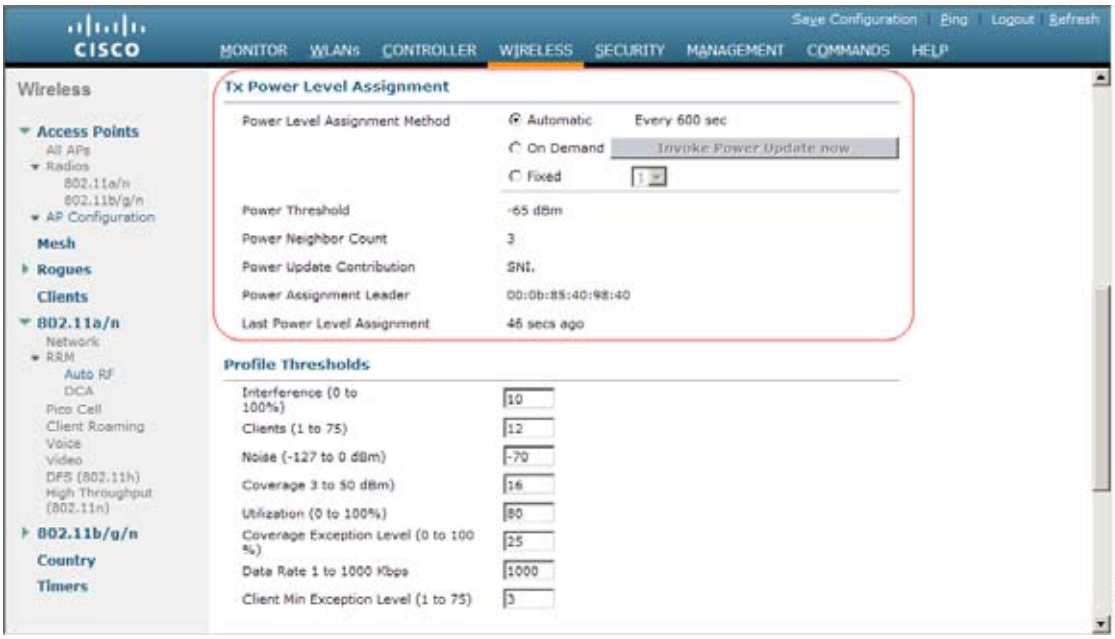


（注）　詳細については、『*Cisco Wireless LAN Controller Configuration Guide*』（http://www.cisco.com/en/US/docs/wireless/controller/7.3/configuration/guide/b_cg73.html）を参照してください。

Auto-RF コンフィギュレーション ウィンドウ最初のグループの [RF Group] は、WLC がグループ内の他の WLC でのダイナミックなグループ化を組み合わせるかどうかを指定するために使用されます。ダイナミックなグループ化は、WLC が、ネイバーではあるがモビリティ グループの別の WLC にアソシエートされている可能性のある AP を確認するのに役立ちます。無効の場合、WLC は把握している（つまり、関連づけられている）アクセス ポイントのパラメータのみ最適化します。グループ リーダーは、選択されたリーダーの MAC アドレスを示します。上部にある [*Controller*] メニューをクリックし、[*Inventory*] を選択して、[WLC Inventory] ウィンドウでコントローラの MAC アドレスを確認できます。

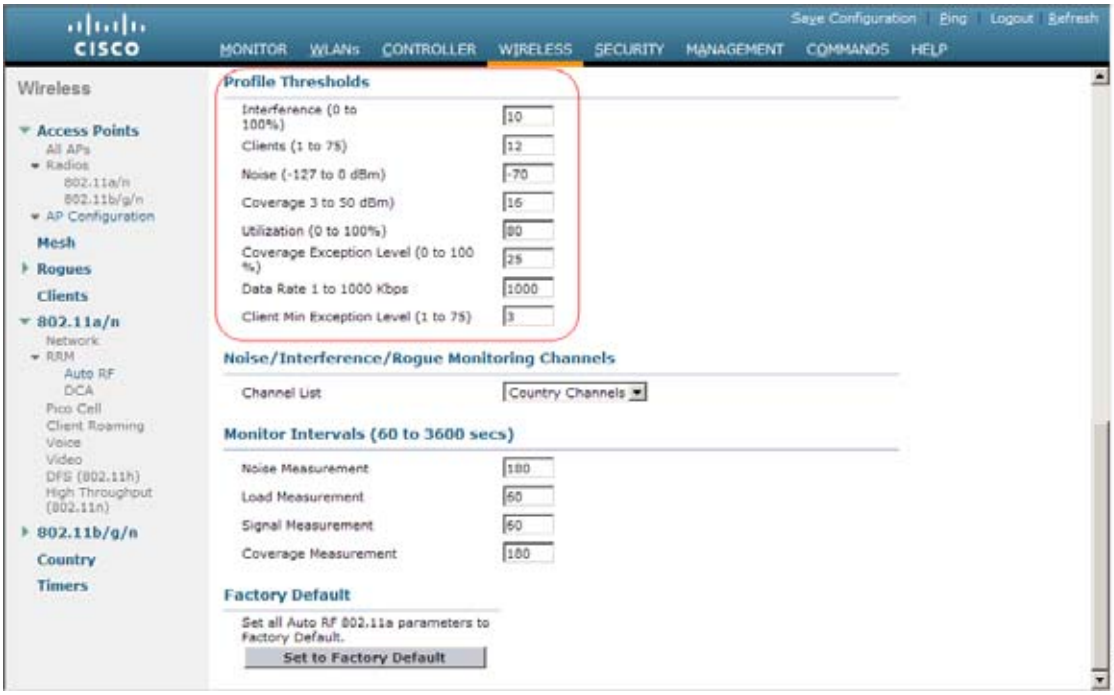
2 番目のセクションは送信（Tx）の電力レベルの割り当て用です（図 3-18 を参照）。電力レベルでは、すべての AP の電力レベルを修正したり、自動調整したりできます。このウィンドウには、AP のネイバーの数と、調整している電力のしきい値も示されます。

図 3-18　Auto-RF（セクション 2）



3 番目のセクション（図 3-19）は、プロファイルのしきい値用です。

図 3-19　Auto-RF（セクション 3）



サンプルの「show ap auto-rf」コマンドの出力

WLC は、AP から渡された情報を分析し、これらのしきい値それぞれについて、パス（pass）またはフェイルのステータスを決定します。これらのパス/フェイルのプロファイルは、**show ap auto-rf** ***radio ap_name*** コマンドの出力によく見られます。このコマンドは、使用される無線から RF 統計情報を表示します。

（注）　**Monitor -> 802.11b/g/n Radios -> Detail** ウィンドウでは、同じ情報をグラフ形式で見ることもできます。

```
show>ap auto-rf 802.11b <access point name>
Number of Slots . . . . . . . . . . . . . . . . . . . . . . 2
AP Name . . . . . . . . . . . . . . . . . . . . . . . . . . <AP name>
MAC Address . . . . . . . . . . . . . . . . . . . . . . . . 00:0b:85:1b:df:c0
Radio Type . . . . . . . . . . . . . . . . . . . . . . . . . RADIO_TYPE_80211b/g
Noise Information
    Noise Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -93 dBm
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -90 dBm
 .
 .
 .
    Channel 11 . . . . . . . . . . . . . . . . . . . . . . -95 dBm
Interference Information
    Interference Profile . . . . . . . . . . . . . . . . . FAILED
    Channel 1 . . . . . . . . . . . . . . . . . . . . . . . -69 dBm @ 31 % busy
    Channel 2 . . . . . . . . . . . . . . . . . . . . . . . -58 dBm @ 26 % busy
 .
 .
 .
    Channel 11. . . . . . . . . . . . . . . . . . . . . . -68 dBm @ 26 % busy
Load Information
    Load Profile . . . . . . . . . . . . . . . . . . . . . PASSED
    Receive Utilization . . . . . . . . . . . . . . . . . . 0 %
    Transmit Utilization . . . . . . . . . . . . . . . . . 0 %
    Channel Utilization . . . . . . . . . . . . . . . . . . 26 %
    Attached Clients . . . . . . . . . . . . . . . . . .  2 clients
Coverage Information
    Coverage Profile . . . . . . . . . . . . . . . . . . .. PASSED
    Failed Clients . . . . . . . . . . . . . . . . . . . . 0 clients
Client Signal Strengths
    RSSI -100 dBm. . . . . . . . . . . . . . . . . . . . . 0 clients
    RSSI -92 dBm . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    RSSI -52 dBm . . . . . . . . . . . . . . . . . . . . . 1 clients
Client Signal To Noise Ratios
    SNR 0 dBm . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 5 dBm . . . . . . . . . . . . . . . . . . . . . .  0 clients
    SNR 10 dBm . . . . . . . . . . . . . . . . . . . . . 0 clients
 .
 .
 .
    SNR 45 dBm . . . . . . . . . . . . . . . . . . . . . 1 clients
Nearby APs
Radar Information
Channel Assignment Information
    Current Channel Average Energy . . . . . . . . . . . . -68 dBm
    Previous Channel Average Energy . . . . . . . . . . . . -51 dBm
```

```
    Channel Change Count . . . . . . . . . . . . . . . . . . . 21
    Last Channel Change Time . . . . . . . . . . . . . . . . . Thu Mar 9 12:18:03 2006
    Recommend Best Channel . . . . . . . . . . . . . . . . . . 11
RF Parameter Recommendations
    Power Level . . . . . . . . . . . . . . . . . . . . . . . . 1
    RTS/CTS Threshold . . . . . . . . . . . . . . . . . . . . . 2347
    Fragmentation Threshold . . . . . . . . . . . . . . . . . . 2346
    Antenna Pattern . . . . . . . . . . . . . . . . . . . . . . 0
```

次の項では、WLC RRM 設定の一部について説明します。

チャネルの動的割り当て

802.11 MAC レイヤでは、キャリア検知多重アクセス / 衝突検出（CSMA/CA）が使用されます。CSMA/CA では、近接する同じチャネル上の 2 つの AP は、無線チャネルを共有するため、異なるチャネルにある 2 つの AP と比較してキャパシティが約半分になります。これは、802.11 MAC では、チャネルがビジー状態であることが検知され、このチャネルが解放されるまで、フレームの送信が延期されることによるものです。802.11 MAC により、そのチャネル自体の AP セルの一部ではないトラフィックの伝送が延期させられた場合は、干渉とみなされます。同一チャネルの別の AP からの干渉は、通常、*同一チャネル干渉*と呼ばれ、大半の 2.4 GHz 802.11 の展開で発生します。これは、オーバーラップしないチャネルが十分ではないため、一部のチャネルのオーバーラップが発生するのを避けることができないからです。設計、計画、および動的な無線管理の目標の 1 つに、同一チャネル オーバーラップを最小限に抑えるということがあります。これにより、同一チャネル干渉が最小になり、AP トラフィックの容量が最大にされます。Cisco Unified Wireless Network では、AP のチャネルを動的に割り当てて、競合を避けることで、この問題および他の同一チャネル干渉の問題に対処します。WLC、つまり指定された WLC（RF グループ リーダー）は、システム全体を認識できるため、チャネルの*再利用*方法を制御し、同一チャネル干渉を最小限に抑えることができます。

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

- ノイズ：ノイズにより、クライアントや AP の信号品質が制限されます。また、ノイズの範囲や周期は、さまざまです。干渉の種類、および干渉が及ぼす影響は多数あります。一例として、ノイズが増加すると、有効なセルのサイズが減少します。WLC は、定期的に、AP の RF 環境を再評価し、チャネルの選択を最適化して、システム全体の容量を維持しつつノイズの原因を回避します。過剰なノイズのためにチャネルが使用できなくなることは避けられます。また、他の無線ネットワークがある場合、WLC は、他のネットワークを補完するために、使用するチャネルを切り替えます。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する WLAN はチャネル 1 または 11 に割り当てられます。これによって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルが使用中で、使用可能なキャパシティがない場合、WLC はこのチャネルを回避することがあります。
- クライアントの負荷：チャネル構造を変更する際には、クライアントの負荷を考慮して、現在 WLAN 上に存在するクライアントへの影響を最小限に抑えるようにします。WLC は、チャネルを最適に割り当てるため、周期的にチャネルの割り当てを監視します。ネットワークのパフォーマンスが大幅に向上する場合や、パフォーマンスが低い AP でパフォーマンスを向上させる場合にだけ、チャネルが変更されます。

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

干渉の検出と回避

Cisco Unified Wireless Network の展開における干渉は、サービスの低下や損失につながる可能性がある同じ周波数帯の不要な RF 信号と定義されます。これらの信号は、特定の電子レンジやコードレス電話などの 802.11 または 802.11 以外の製品が原因となる場合があります。また、場合によっては、アーク溶接やレーダー施設などのさまざまな原因によって電磁干渉（EMI）が発生することもあります。AP は、常にすべてのチャネルをスキャンして干渉の主な原因を調べ、管理リンク インターフェイス（CAPWAP トンネル）経由で得られた情報を定期的に WLC に報告します。

802.11 の干渉の量が、事前に定義されたしきい値に達すると、WLC は、チャネルを再割り当てして干渉が存在するシステムのパフォーマンスを最適化しようと試みます。その場合、隣接する AP が同じチャネルに存在する結果となることがあります。これは、干渉のためにまったく使用できないようなチャネルに存在するよりは、論理的には優れたシナリオです。たとえば、WLC は、近接する AP をチャネル 1 またはチャネル 6 に切り替えることで、チャネル 11 上の不正な AP に応答できます。

送信電力の動的制御

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

RRM アルゴリズムは、ユーザ エクスペリエンスが最適になるように設計されています。たとえば、AP の電力がレベル 4（レベル 1 が最大でレベル 8 が最低）まで下がり、あるユーザの RSSI 値が許容しきい値を下回った場合、そのクライアントに対して最適なエクスペリエンスを提供できるように、AP の電力が増やされます。送信電力の動的制御（DTPC）が有効になっている場合、AP によりチャネルおよび送信電力が、*ビーコン*（チャネル、RF 電力、ネットワーク名などの情報を含む情報要素）に追加されます。DTPC を使用しているクライアント デバイスは、この情報を受信して、自動的に設定を調整します。

カバレッジ ホールの検出と修正

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

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

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

クライアントとネットワークのロード バランシング

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

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

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。

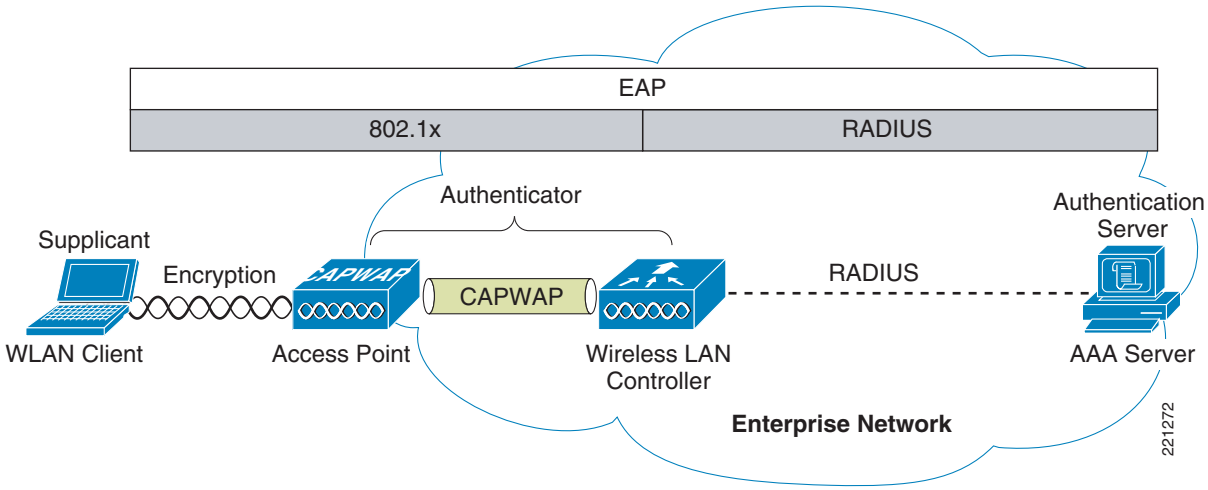
Cisco Unified Wireless Network ソリューションは、IEEE 802.11-2012 標準の基本セキュリティ機能を基盤としています。無線周波数（RF）とネットワーク ベースのセキュリティ機能を強化して全体的なセキュリティを保証します。

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
- 無線アクセスポイント（CAPWAP）プロトコルの管理とプロビジョニング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 AAA（認証、許可、アカウンティング）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行されます。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）
- Wired Equivalent Privacy（WEP）
- シスコの WEP 拡張（Cisco Key Integrity Protocol + Cisco Message Integrity Check）
- Wi-Fi Protected Access（WPA）
- Wi-Fi Protected Access 2（WPA2）
- 拡張ローカル モード（ELM）の Cisco Adaptive Wireless Intrusion Prevention System（wIPS）

シスコの Wired Equivalent Privacy（WEP）Extension

元の 802.11 セキュリティ メカニズムである WEP は*何らか*のレベルのセキュリティを適用するスタティック暗号化方式セキュリティであり、ビジネス コミュニケーションを保証するには不十分であると一般的には見られています。Cisco WLAN 製品では、次のように WEP を拡張することで、その不足に対応しました。

- Cisco Key Integrity Protocol（CKIP）
- Cisco Message Integrity Check（CMIC）

シスコによる WEP の拡張は、Cisco WEP Extension と総称されています。

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ダイナミック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。

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、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 Extesion 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 暗号化の拡張：WPA/WPA2 または WEP TKIP Cisco Key Integrity Protocol（CKIP）、および Cisco Message Integrity Check（CMIC）を介したキー ハッシング（パケットごとのキーイング）およびブロードキャスト キー ローテーション

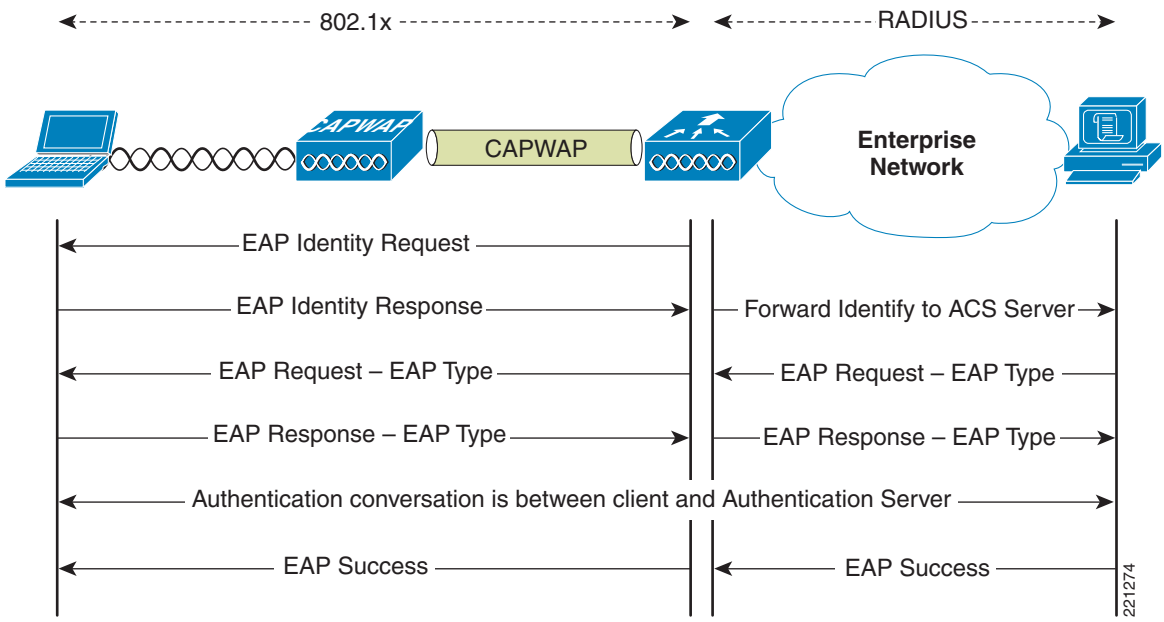
Extensible Authentication Protocol（拡張認証プロトコル）

Extensible Authentication Protocol（EAP）は、転送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かならず使用されます。

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、セキュアな 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、Generic Token Card 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）	あり	あり	あり[1]	あり
ログイン スクリプト（MSFT AD のみ）	あり	あり	一部	あり[2]
パスワード変更（MSFT AD）	あり	あり	あり	該当なし
Microsoft AD データベース サポート	あり	あり	あり	あり
ACS ローカル データベース サポート	あり	あり	あり	あり
LDAP データベース サポート	あり[3]	なし	あり	あり
OTP 認証サポート	あり[4]	なし	あり	なし
RADIUS サーバ証明書は必要か?	なし	あり	あり	あり
クライアント証明書は必要か?	なし	なし	なし	あり
匿名	あり	あり[5]	あり[6]	なし

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

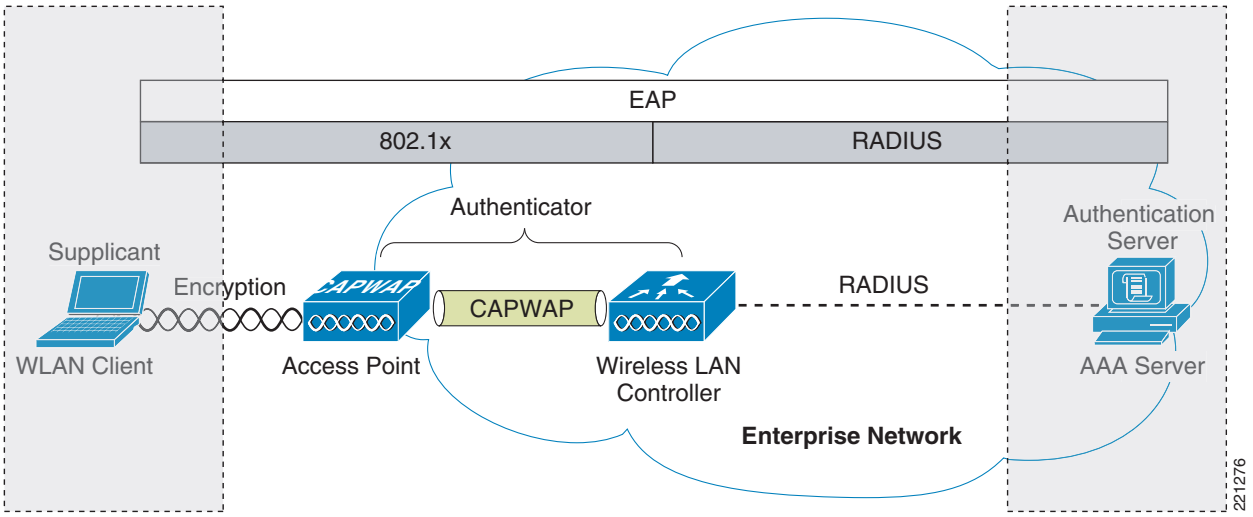
オーセンティケータ

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（VSAs）

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場所



EAP の交換の手順は次のとおりです。

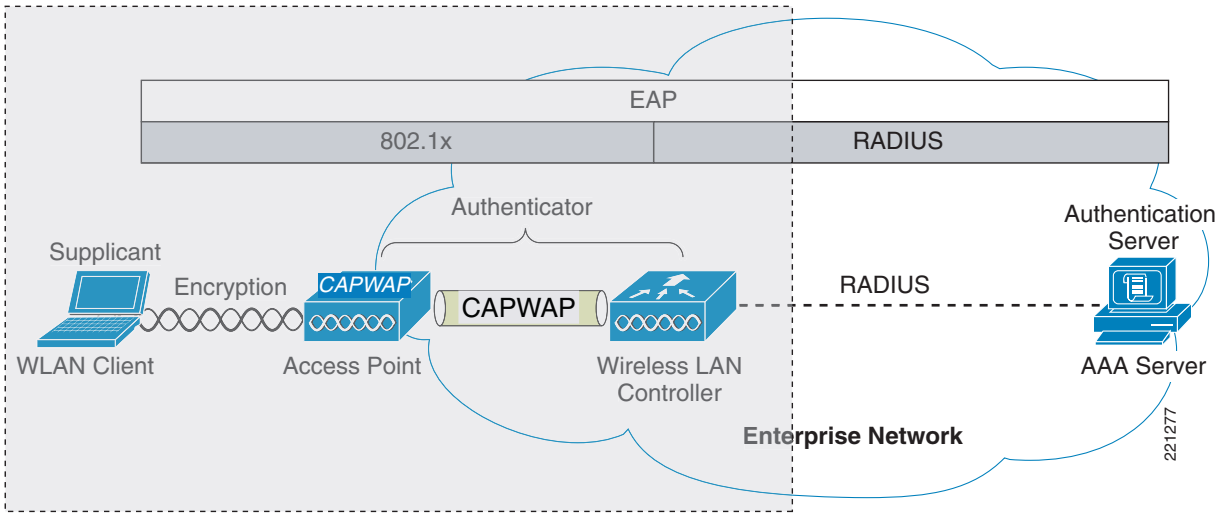
- パケット #1 が、AP によってクライアントに送信されます。このときクライアントの識別情報が要求されます。これにより、EAP 交換が開始されます。
- パケット #2 には、RADIUS サーバに転送されるクライアント ID が含まれています。パケット 2 内のクライアント ID に基づいて、EAP 認証を継続するかどうかを RADIUS サーバが判断します。
- パケット #3 には、認証のための EAP 方式として PEAP を使用する RADIUS サーバ要求が含まれます。実際の要求は、RADIUS サーバで設定された EAP の種類によって異なります。PEAP クライアントが要求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

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 および ISE は、Windows 2000 以降のサーバにインストールされているソフトウェアとして、またはアプライアンスとして入手できます。逆に、認証サーバの役割は、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、特定の WLAN インフラストラクチャ内で実行できます。

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。

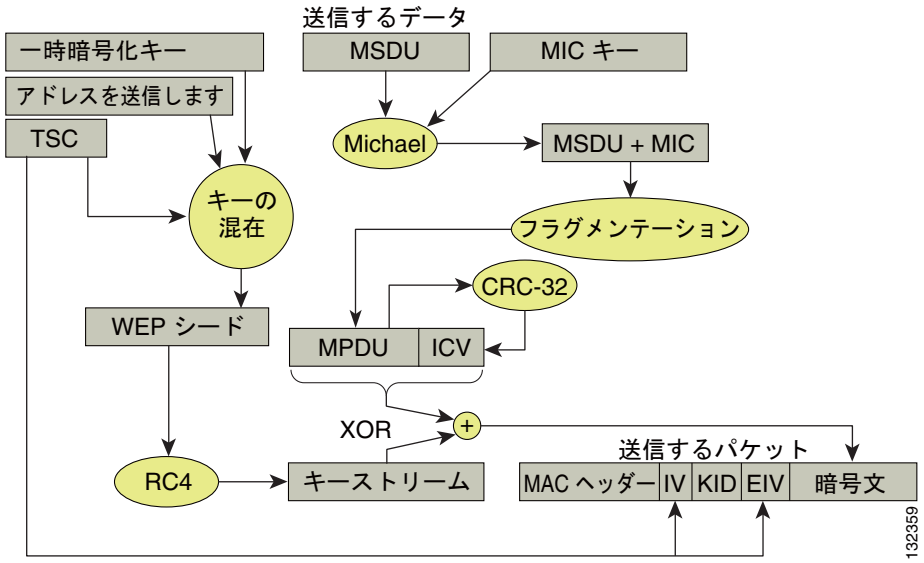
WPA および WPA2 では、暗号キーは Four-Way ハンドシェイク中に取得されます。Four-Way ハンドシェイクについてはこのセクションで後ほど説明します。

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。TKIP は、802.11 の WEP 暗号化方式に関連する元の欠点に対処することによって、旧式の WLAN 機器に対するサポートを提供します。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 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



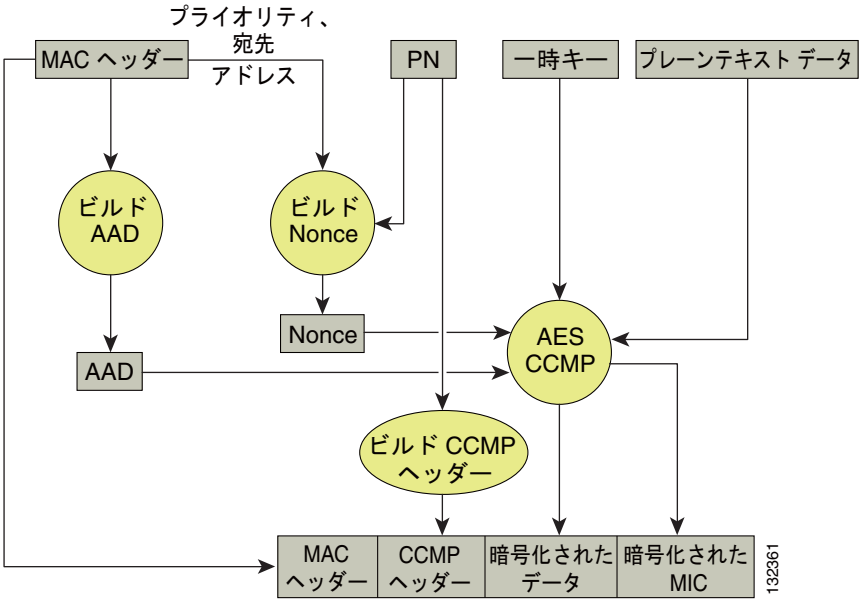
TKIP の主な 2 種類の機能は、MAC Service Data Unit（MSDU）の RC4 暗号化を使用するパケットごとのキーと、暗号化されたパケット内にメッセージ完全性チェック（MIC）を生成することです。パケットごとのキーは、送信アドレス、フレームの初期化ベクトル（IV）、および暗号キーのハッシュです。IV はそれぞれのフレーム送信に従って変化するため、RC4 暗号化に使用されるキーはフレームごとに固有のものです。

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、一時的に WLAN クライアントが切断されたり、60 秒ごとに新しいキーのネゴシエーションを許可されないなどの攻撃を防御する対策が含まれます。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、アンチウイルス機能を無効にすることができます。

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。

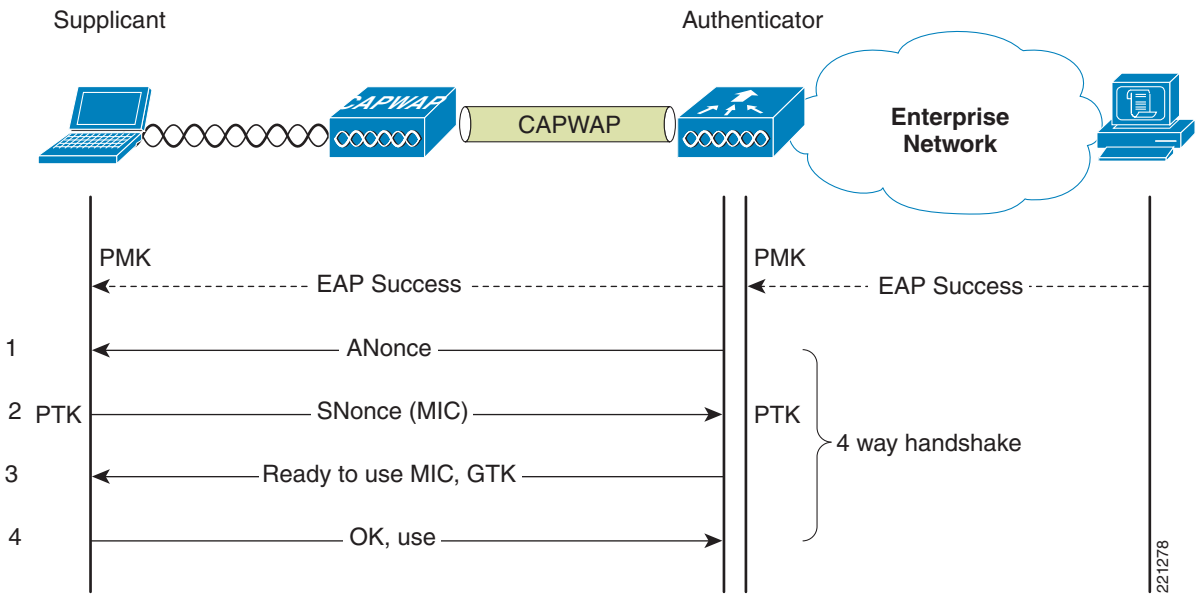
Four-Way ハンドシェイク

Four-Way 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 成功メッセージの中で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 PMK の自分のコピーを生成しているためです。

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-Key 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。
   a. 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-Key フレームを送信します。
   a. オーセンティケータは、ANonce および SNonce から PTK を取得し、EAPOL-Key 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、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-Key フレームを送信します。
4. サプリカントは、一時キーがインストールされていることを確認するための EAPOL-Key フレームを送信します。

図 4-7　Four-Way ハンドシェイク

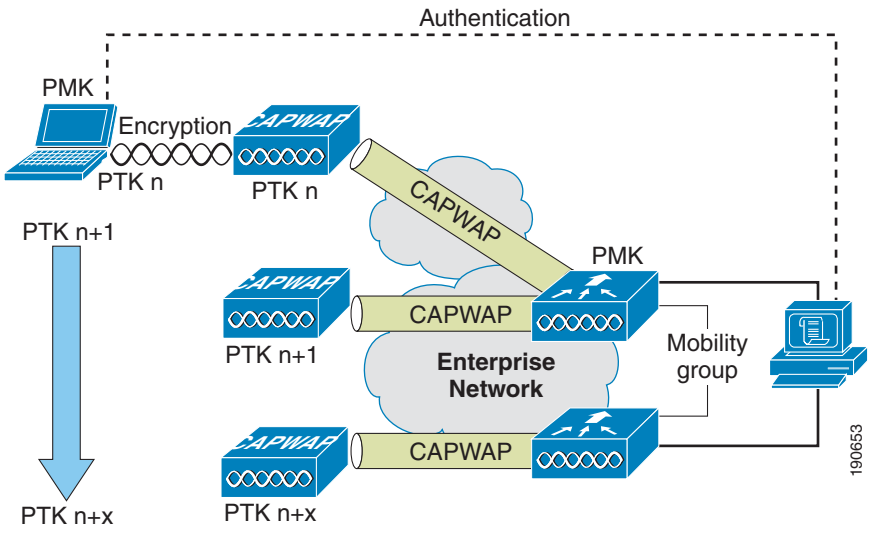


Proactive Key Caching と CCKM

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 クライアントが WPA Four-Way ハンドシェイク プロセスを使用して、その AP との通信のための新しいセッション暗号化キーを安全に取得することができます。

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。

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

Cisco Unified Wireless Network アーキテクチャ

図 4-9 では、CAPWAP AP やメッシュ 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

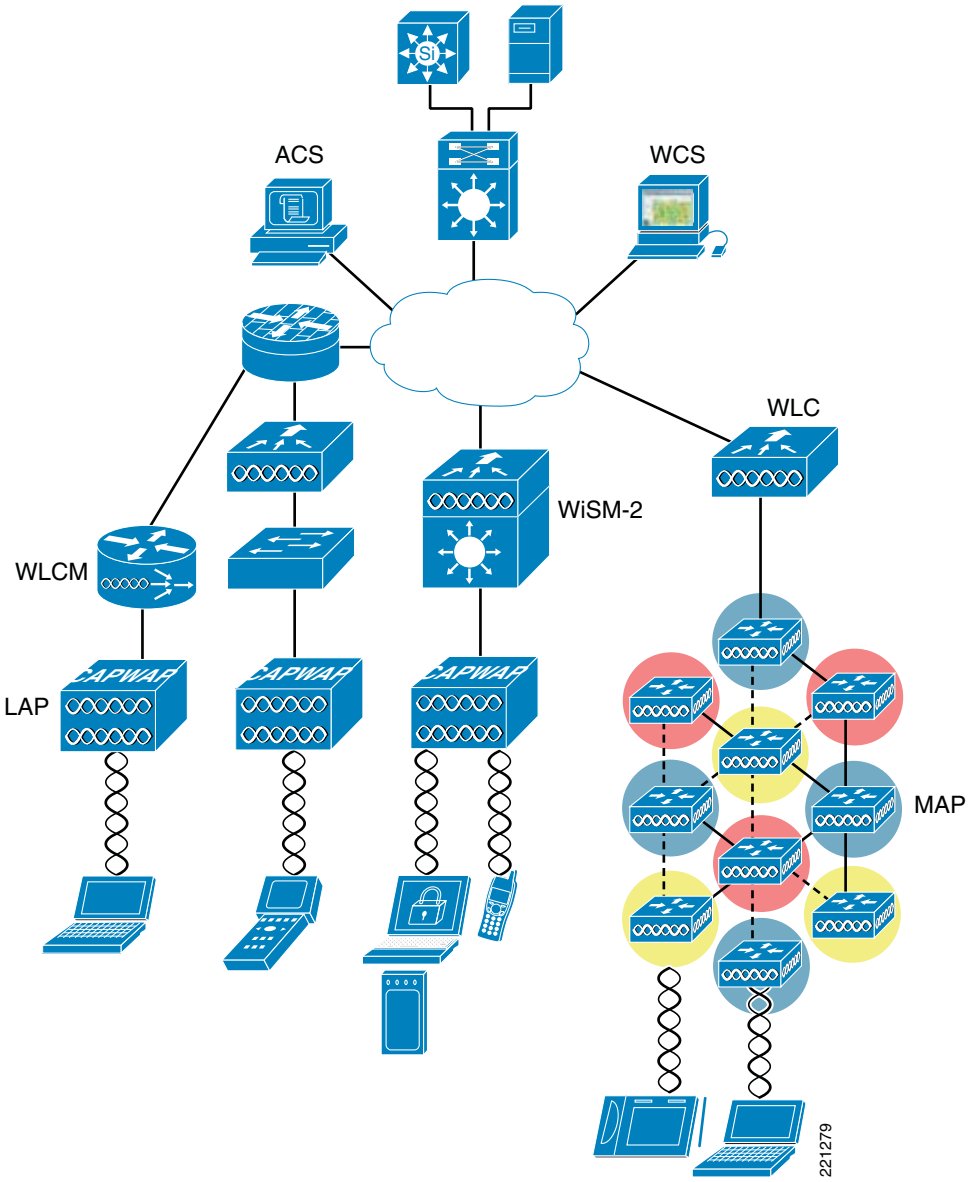
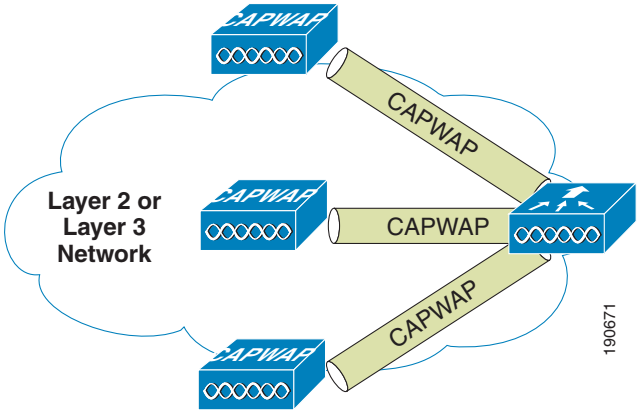


図 4-10 では、アーキテクチャの主要機能の 1 つである、AP がどのように CAPWAP プロトコルを使用して WLC へのトンネル トラフィックと通信するのかについて説明します。

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 からの WLAN クライアント トラフィックのトンネリング
- Cisco Unified Wireless Network の管理に関する 802.11 データの収集

CAPWAP の機能

Control and Provisioning of Wireless Access Points（CAPWAP）は、Lightweight Access Point Protocol（LWAPP）に対する更新です。CAPWAP は多くの AP の管理を WLC でできるようにする、標準かつ相互運用可能なプロトコルです。CAPWAP の機能は次のとおりです。

- シスコの LWAPP 製品から、CAPWAP を使用する次世代のシスコ製品へのアップグレード パス
- RFID リーダーおよび類似のデバイスを管理する機能
- サードパーティのアクセス ポイントと相互運用するコントローラ

LWAPP 対応の AP では、CAPWAP コントローラの discover と join が可能で、CAPWAP コントローラへの移行はシームレスに行われます。たとえば、WLC ディスカバリ処理とファームウェアのダウンロード処理は、CAPWAP および LWAPP で同じです。

覚えておく必要のある重要なポイント

- LWAPP を使用する AP からのトラフィックのみを許容するようにファイアウォールが設定されている場合、CAPWAP を使用する AP からのトラフィックを許容するようにファイアウォールのルールを変更する必要があります。
- CAPWAP UDP ポート 5246 と 5247（LWAPP UDP ポート 12222 と 12223 のように）がイネーブルになっていて、AP のコントローラへの join を妨げる可能性のある中継デバイスによりブロックされていないことを確認してください。
- コントローラと AP 間のコントロール パスにアクセス コントロール リスト（ACL）がある場合、新しいプロトコル ポートをオープンして、アクセス ポイントが阻止されるのを防ぐ必要があります。

AP は、コントローラの宛先ポートに到達するために任意の UDP 送信元ポートを使用します。新しく開封したばかりの AP がある場合、コントローラから CAPWAP イメージをダウンロードする前に LWAPP を使用してコントローラに接続しようとすることがあります。AP は、コントローラから CAPWAP イメージをダウンロードしたら、CAPWAP のみを使用して、コントローラとやり取りします。

（注）　CAPWAP を使用してコントローラへの join を 60 秒間試行した後、AP は LWAPP の使用にフォールバックします。AP は、LWAPP を使用してコントローラを 60 秒以内に検出できないと、CAPWAP を使用してコントローラへの join を再度試行します。AP は、コントローラに join できるまで、CAPWAP と LWAPP を 60 秒ごとに切り替えるこのサイクルを繰り返します。

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 IP（EoIP）上のイーサネットにマッピングすることもできます。

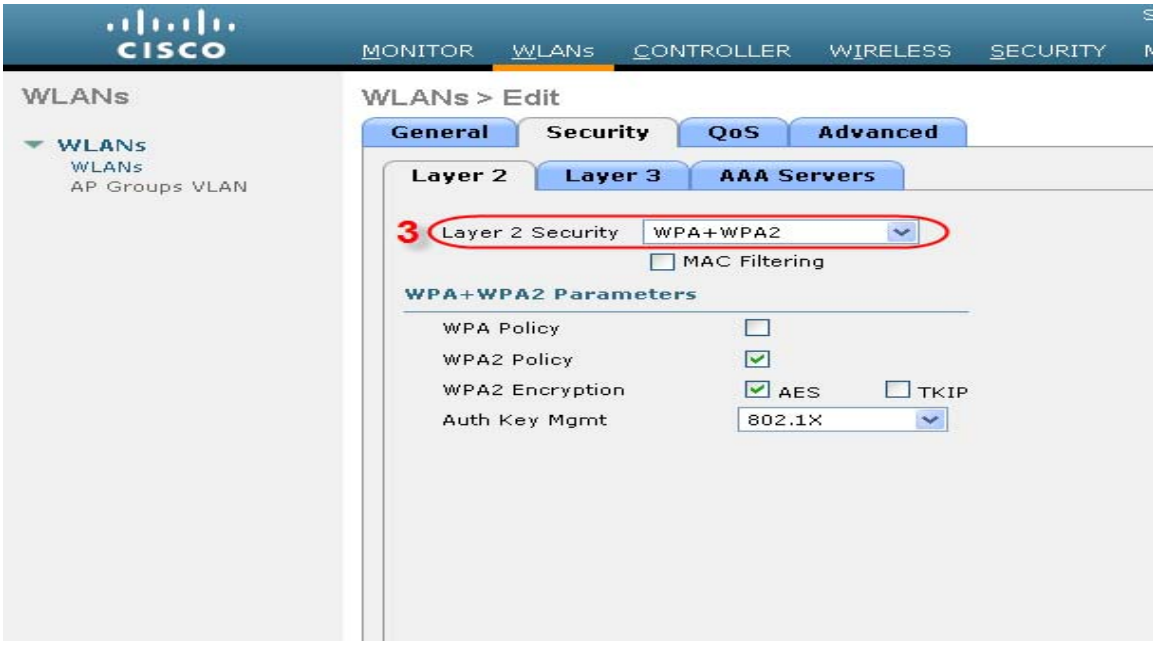
WLAN クライアントが 802.1X を介して認証する場合、dot1q VLAN の割り当ては、認証成功時に WLC に渡される RADIUS 属性を使用して制御されます。

図 4-11 および図 4-12 では、Unified Wireless Network WLAN 設定画面のサブセットを示します。これらの設定画面に表示される主な設定項目は次の 3 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
- セキュリティ方式（図 4-12）

図 4-11　WLAN の [General] タブ

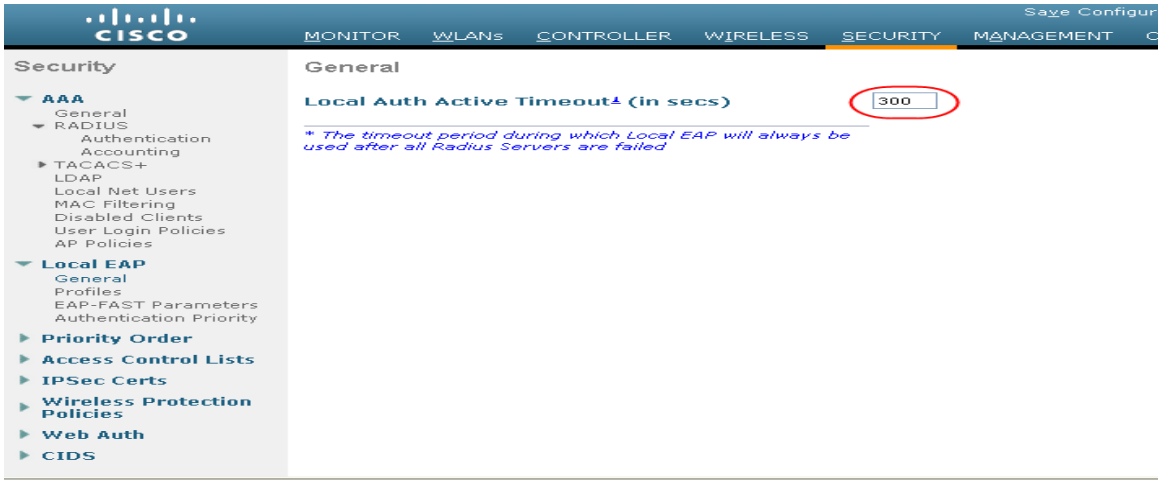
図 4-12　WLAN の [Layer 2 Security] タブ



ローカル EAP 認証

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替えが設定されるまでの遅延は、図 4-13 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。

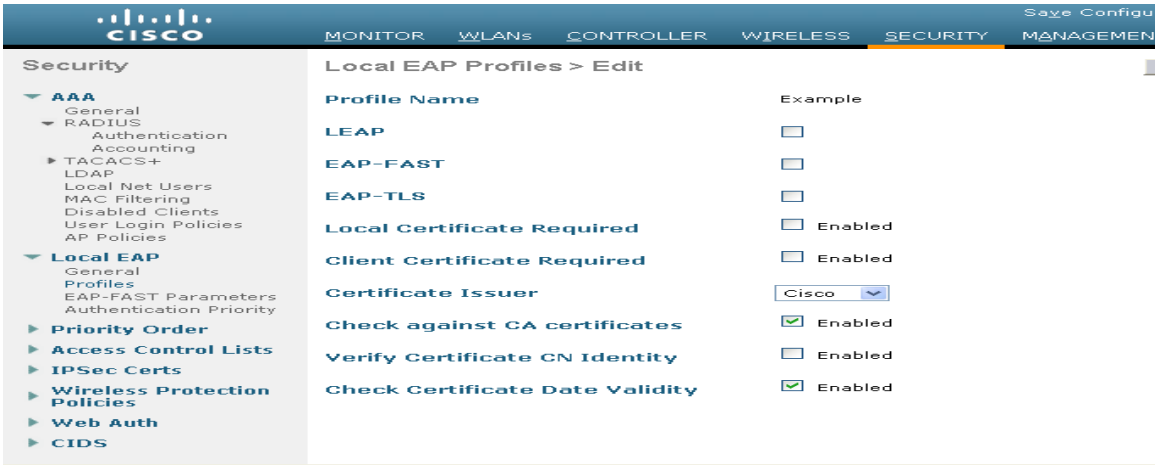
図 4-13　　ローカル認証のタイムアウト



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 4-14 では、ローカル EAP のプロファイルを選択するウィンドウを示します。

図 4-14　　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 4-15 で示すとおりに設定可能です。

図 4-15　　ローカル EAP のプライオリティ

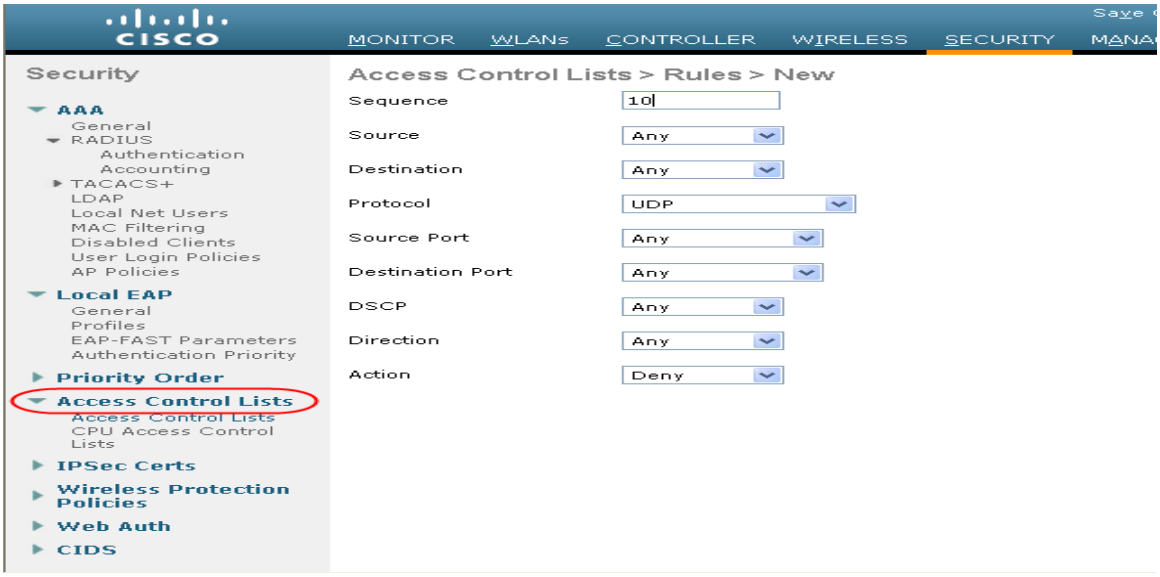
ACL およびファイアウォール機能

WLC では、WLC 上で設定されている任意のインターフェイス用にアクセス コントロール リスト（ACL）を定義できます。また、WLC 自体の CPU 用に ACL を定義することもできます。これらの ACL を使用することで、特定の WLAN にポリシーを適用し、特定のアドレスやプロトコルへのアクセスを制限したり、WLC 自体に追加保護を行ったりすることができます。

インターフェイス ACL は、ACL が適用されているインターフェイスに出入りする WLAN クライアント トラフィックに作用します。CPU ACL は WLC インターフェイスに依存しないため、WLC システムに送受信されるすべてのトラフィックに適用されます。

図 4-16 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 4-16　[ACL Configuration] ページ



DHCP および ARP 保護

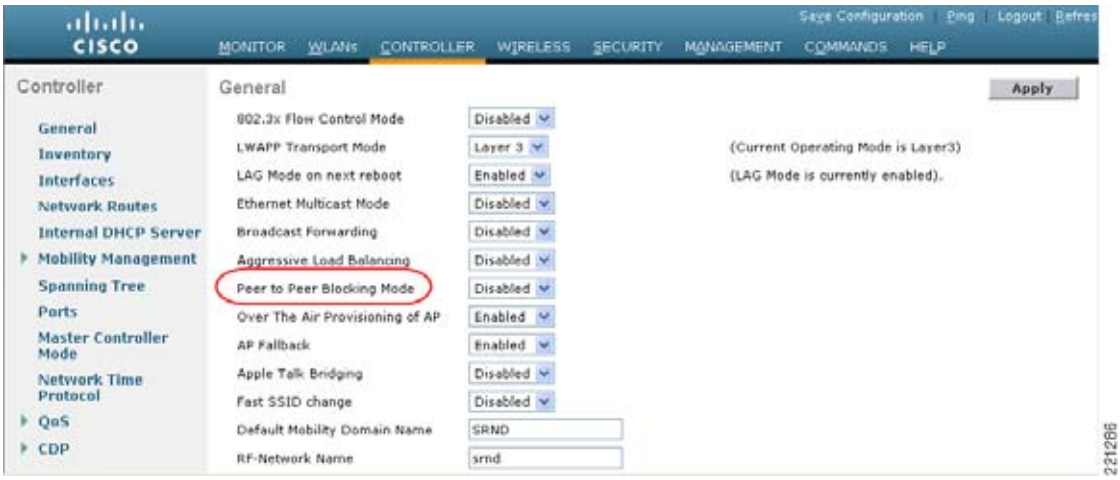
WLC は、WLAN クライアントの DHCP 要求のリレー エージェントとして動作します。その際、WLC は DHCP インフラストラクチャを保護するために、いくつかのチェックを実行します。最も重要なチェックは、DHCP 要求に含まれている MAC アドレスが、要求を送信する WLAN クライアントの MAC アドレスに一致することを確認することです。これにより、WLC 自体のインターフェイスに対する 1 つの DHCP 要求（IP アドレス）に WLAN クライアントを制限し、それによって DHCP 枯渇攻撃を防御します。WLC は、デフォルトでは WLAN クライアントからのブロードキャスト メッセージを WLAN に再転送しないため、WLAN 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 4-17 は、WLC 上でのピアツーピア ブロックの設定画面です。これは WLC のグローバル設定であり、WLC に設定されているすべての WLAN に適用されることに注意してください。

図 4-17　ピアツーピア ブロック



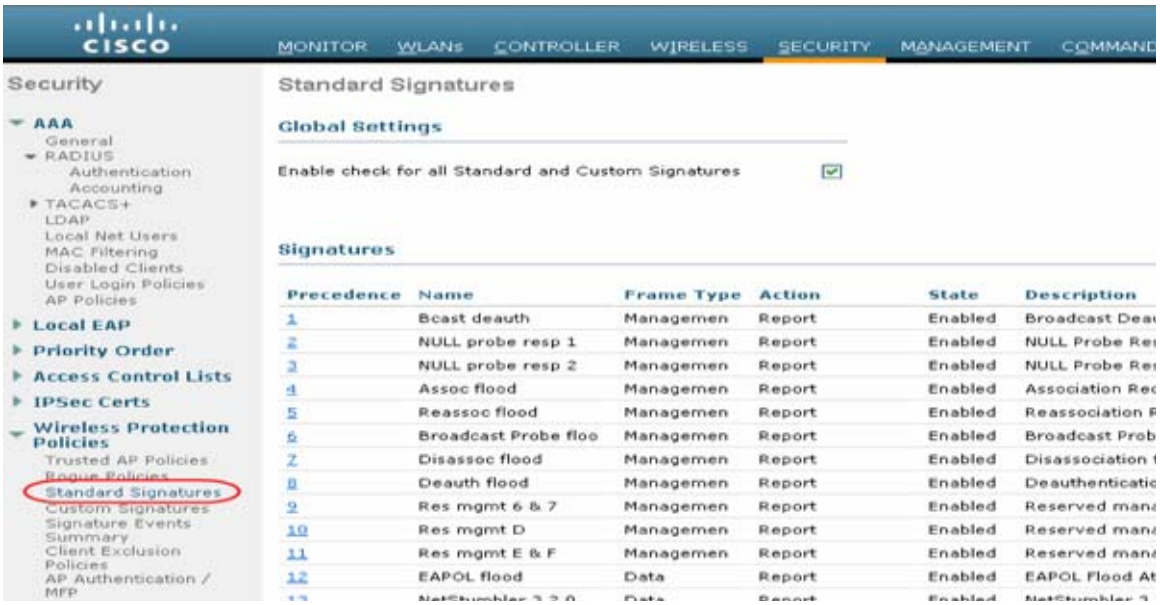
無線 IDS

WLC は、接続された AP すべて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 4-18 は、WLC の [Standard Signatures] ウィンドウです。

図 4-18　標準の WLAN IDS シグニチャ



Cisco Adaptive Wireless Intrusion Prevention System

ELM 機能を備えた Cisco Adaptive Wireless Intrusion Prevention System（wIPS）を使用すれば、モニタリング専用モードまたはオーバーレイ ネットワークを必要とすることなく、展開された AP に総合的なセキュリティ保護を提供できます（図 4-19 を参照）。AP は、セキュリティへの不正なアクセスや侵入、攻撃を防御する必要があります。ネットワーク AP で ELM 機能がイネーブルになっているシスコの wIPS を使用すれば、効果的かつ簡単に無線セキュリティを実装できます。

図 4-19　拡張ローカル モード（ELM）での AP の展開

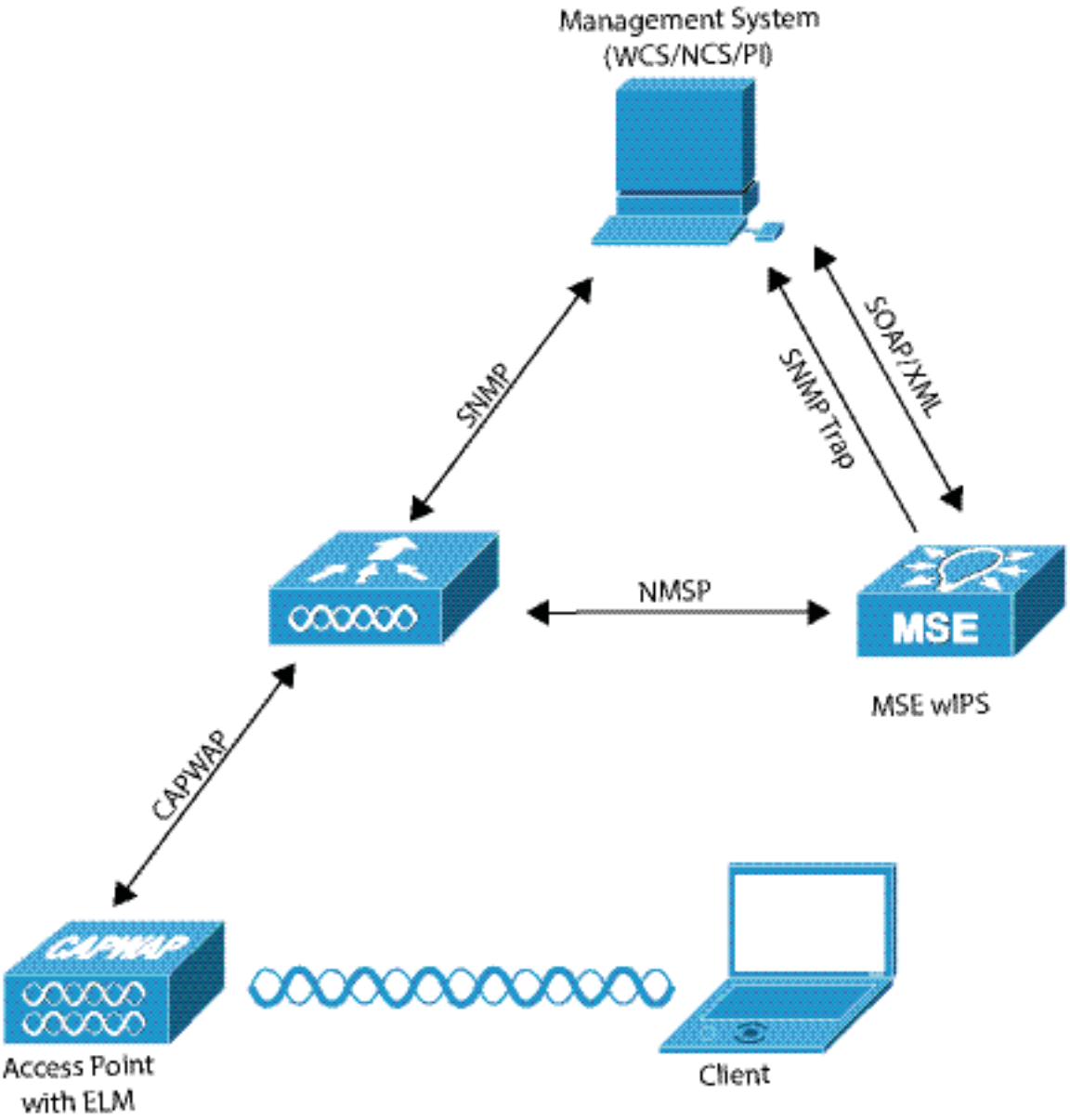


図 4-19 の wIPS 通信プロトコルは次のとおりです。

- CAPWAP：これは、Lightweight Access Point Protocol（LWAPP）の後継プロトコルであり、ELM AP と WLC の間の通信に使用されます。WLC と wIPS との間でアラーム情報が送受信され、他の Cisco Prime Infrastructure 管理システムの構成情報が AP にプッシュされる双方向トンネルを提供します。

（注）　Cisco Prime Infrastructure 管理システムは、以前は Wireless Control System（WCS）と呼ばれていましたが、その後 Network Control System（NCS）に進化しました。わかりやすくするため、これら 3 つすべてを*管理システム（WCS/NCS/PI）*と呼びます。

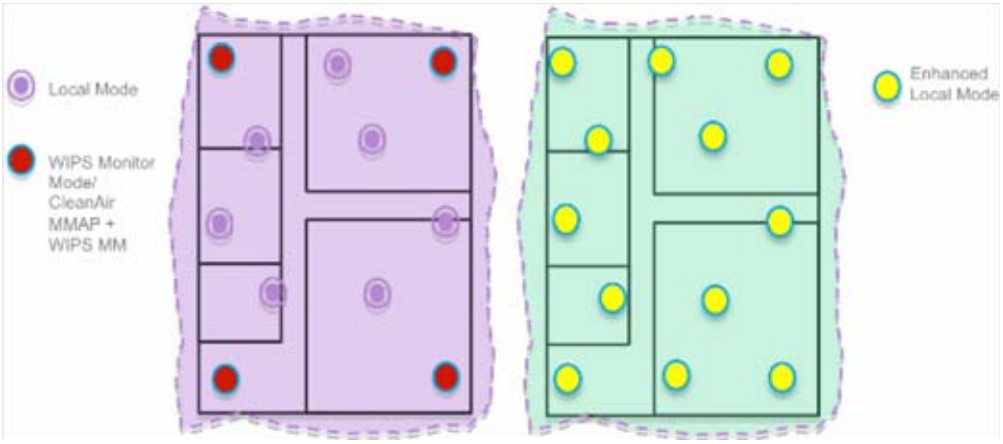
- Network Mobility Services Protocol（NMSP）：この暗号化されたプロトコルは、WLC と管理システム（WCS/NCS/PI）間で通信を行います。wIPS の展開において、このプロトコルは、WLC から wIPS（およびその他の動作しているサービス）へ集約するアラーム情報および、wIPS の設定情報をコントローラにプッシュする経路を提供します。
- SOAP/XML（Simple Object Access Protocol）：管理システム（WCS/NCS/PI）への通信方式。このプロトコルは、モビリティ サービス エンジン（MSE）で稼働する wIPS やその他の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。
- SNMP（簡易ネットワーク管理プロトコル）：MSE から管理システム（WCS/NCS/PI）へ wIPS のアラーム情報を転送するために使用されます。また、WLC から管理システム（WCS/NCS/PI）に不正 AP の情報を伝えるためにも使用されます。

モニタ専用モードと ELM

図 4-20 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 4-20 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 4-20 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 4-20　　モニタ モードと ELM の比較



従来の Adaptive wIPS 展開の場合、5 つそれぞれのローカル モード AP に対して 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。

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そのチャネルに*留まる*時間を、*一時停止*時間といいます。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滞留時間を提供する 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 に関連づけられている場合、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、オフチャネル中の 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 が動作することで効果が増します。したがって、カバレッジの保護を最大にするためにすべてのローカル モードの 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の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。

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。シスコでは、ベスト プラクティスとして、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、CleanAir 操作を補完し、同様のパフォーマンスを実現して、次の既存の CleanAir スペクトラム対応のメリットをモニタ モード AP の展開に提供します。

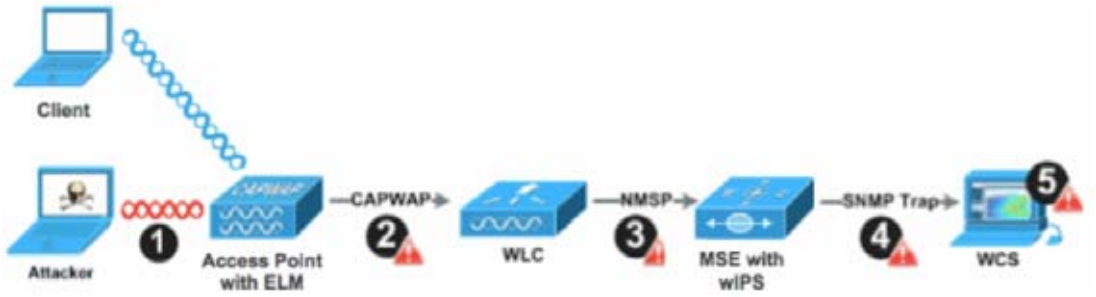
- 専用シリコン レベル RF インテリジェンス
- スペクトラム対応、セルフ ヒーリングおよび自己最適化
- 非標準のチャネル脅威および干渉の検出および緩和
- Bluetooth、マイクロ波、コードレス電話などの非 Wi-Fi 検出
- RF ジャマーなどの RF 層 DOS 攻撃の検出および特定

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。図 4-21 で示すとおり、ELM AP は攻撃を検出した後、管理システム（WCS/NCS/PI）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 に対して発生する
2. ELM 機能を持つ AP の検出が CAPWAP を介して WLC に通知される
3. NMSP を介して MSE に透過的に渡される
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（WCS/NCS/PI）に送信する
5. 管理システム（WCS/NCS/PI）に表示される

図 4-21　　脅威検出のアラーム フロー

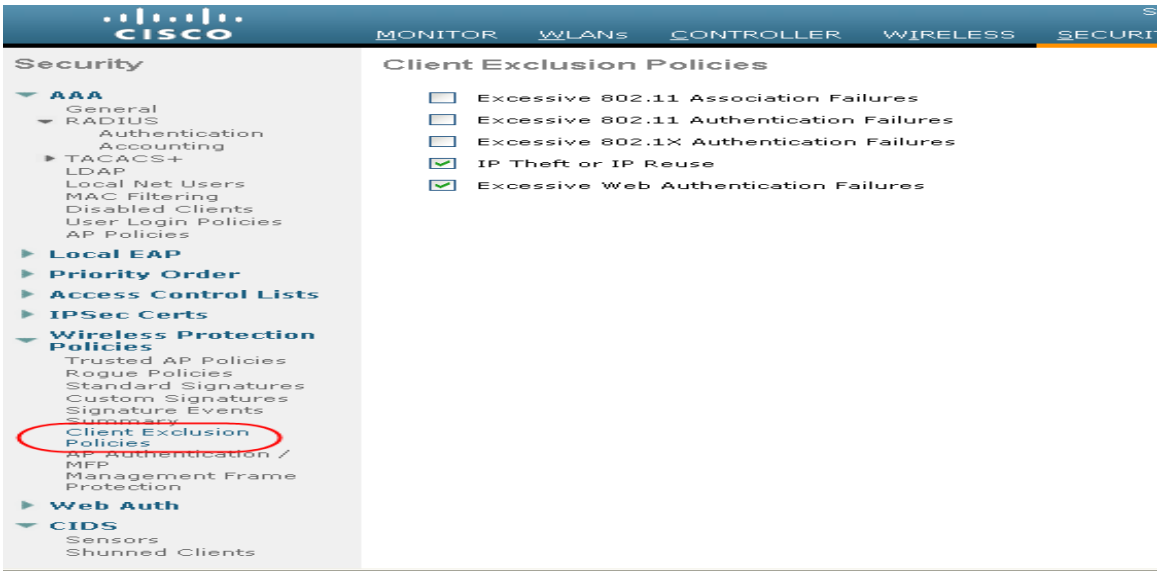


クライアント除外

無線 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 4-22 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
- 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 4-22　クライアント除外ポリシー

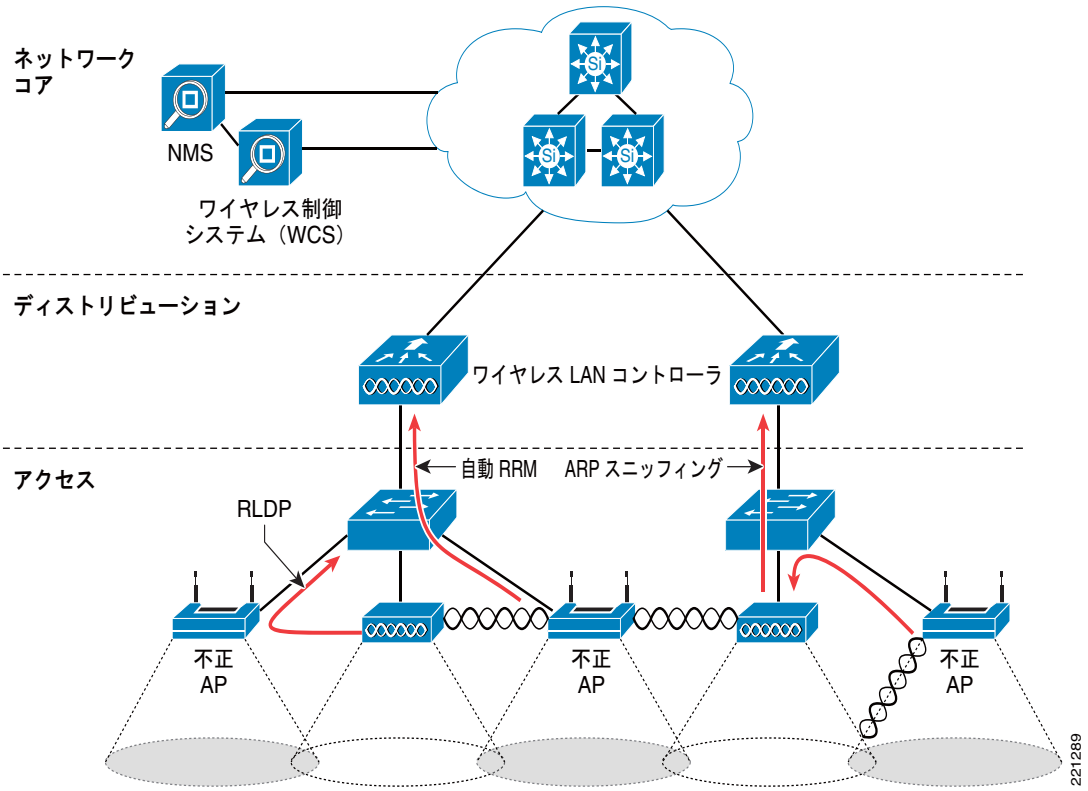


不正 AP

図 4-23 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 4-23　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。

- 標準の AP 導入
- モニタ モードの AP 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）の検出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ていません。

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監視します。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
- 信号対雑音比（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、干渉を監視します。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、または単に近接 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監視したい場合に、最も一般的に使用されるのがモニタ モードです。

ロケーション

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、次の Web ページを参照してください。
http://www.cisco.com/en/US/products/ps6386/index.html

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、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に認識されないため、不正な AP 検知器に代わる手段が必要となります。また、監視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、当該の不正 AP のネットワーク上で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。シスコがソリューションから不正 AP の自動封じ込め機能を削除したのは、これが理由です。

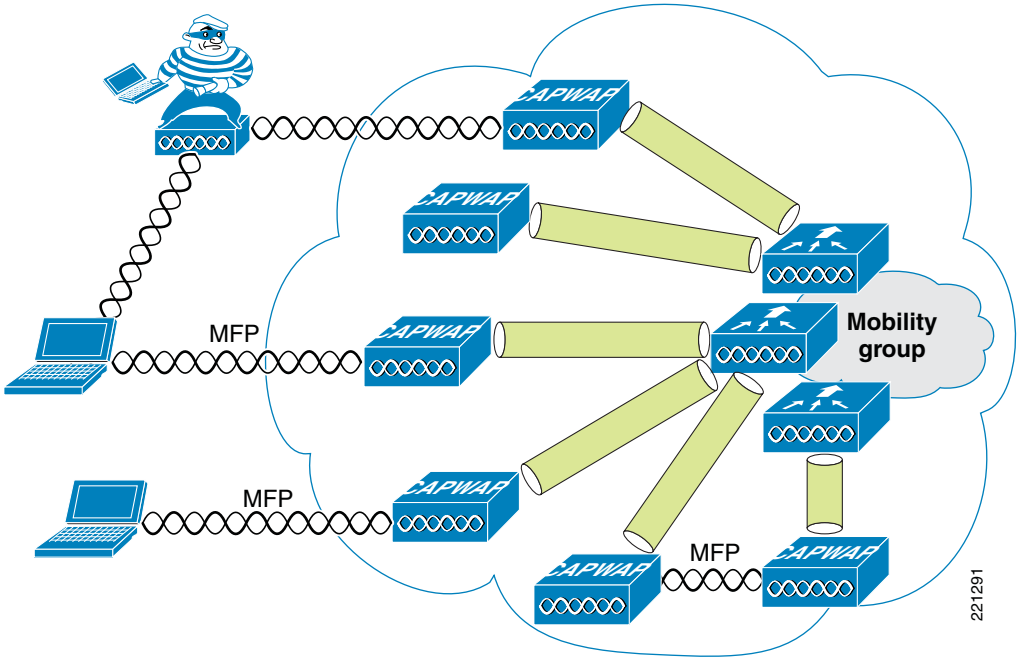
企業の WLAN にも不正 AP クライアントが存在するかどうかを判断するには、クライアントの MAC アドレスと、802.1X 認証中に AAA によって収集された MAC アドレスを比較します。これにより、改ざんされた可能性のある WLAN クライアントやセキュリティ ポリシーに従っていないユーザの識別が可能になります。

管理フレーム保護

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 ハッシュですが、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竄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 4-24）。

図 4-24　管理フレーム保護



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 Extension v5 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 は、次のような利点を提供します。

- 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
- バージョン 12.3(8)/v2.13 のスタンドアロン AP/WDS/WLSE でサポートされる

MFP を有効にするには 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 4-25）、モビリティ グループ内の WLAN で MFP をイネーブルにします（図 4-26）。

図 4-25　コントローラの MFP のイネーブル化

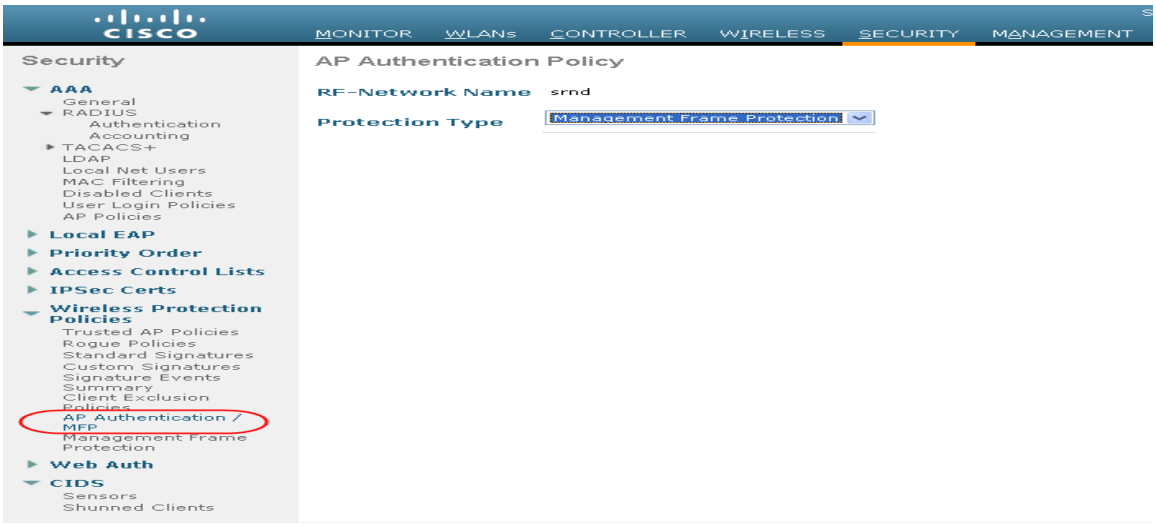
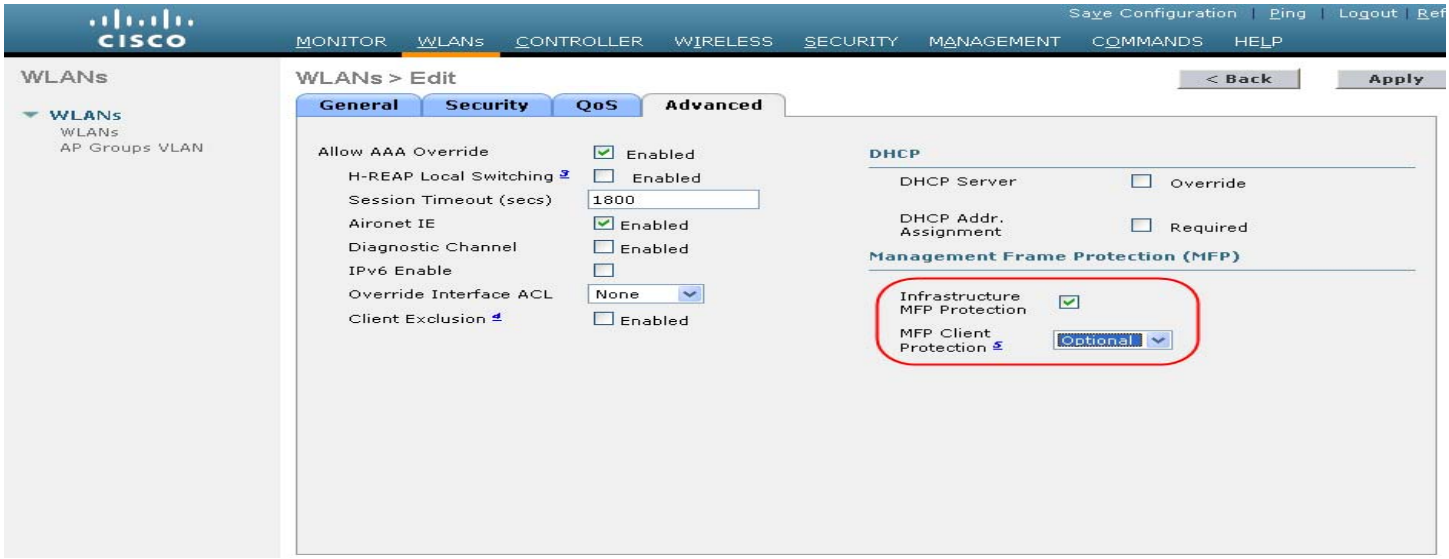


図 4-26　WLAN ごとの MFP のイネーブル化



クライアント管理フレーム保護

Cisco Compatible Extensions v5 の WLAN クライアントでは、MFP をサポートしています。上記の図 4-26 で示したとおり、MFP は WLAN ごとにイネーブルにできます。

WLAN クライアントに MFP を提供する方式は管理フレームで MIC を使用するものであり、AP に使用する方式と基本的に同じです。これにより、信頼済みの管理フレームがクライアントによって識別できるようになります。MIC の暗号キーは、WPA2 認証プロセス中にクライアントに渡されます。クライアント MFP は、WPA2 に対してのみ使用できます。WPA および WPA2 クライアントが同じ WLAN を共有する場合、クライアント MFP は「Optional」に設定する必要があります。

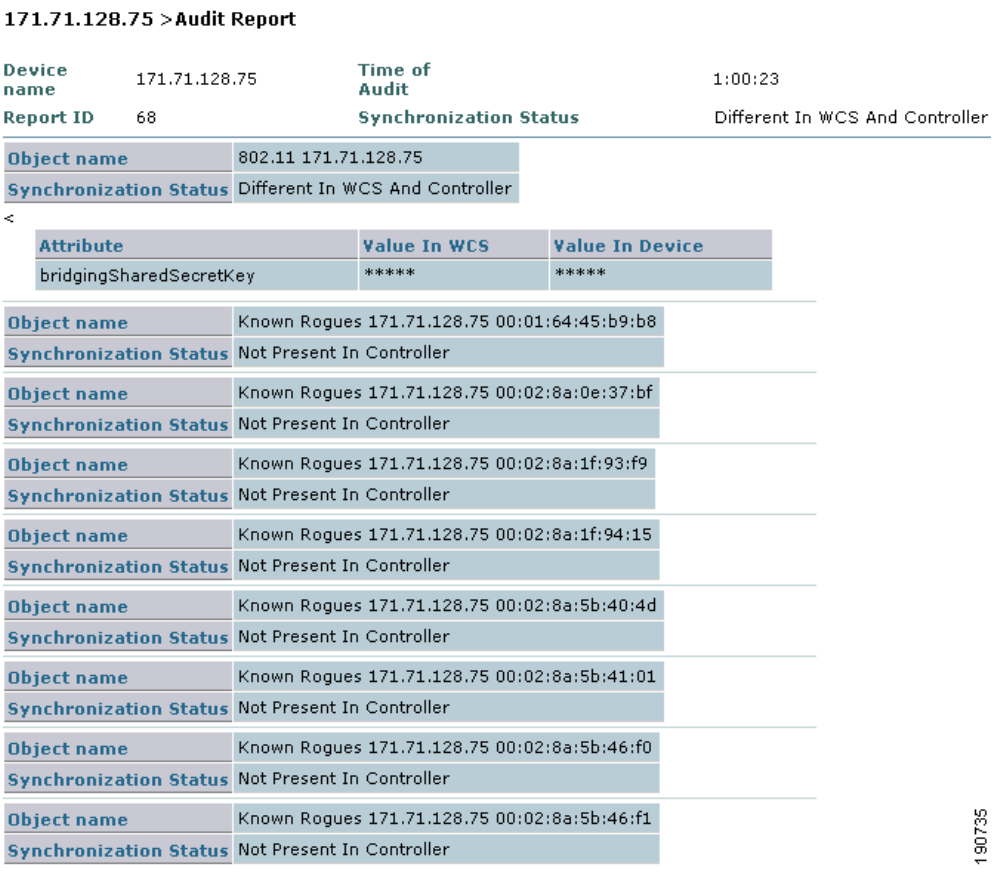
管理システムのセキュリティ機能

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（WCS/NCS/PI）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（WCS/NCS/PI）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 の現在稼働している完全な設定と、管理システム（WCS/NCS/PI）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 4-27）。

図 4-27　監査レポートの例


171.71.128.75 >Audit Report

Device name	171.71.128.75	Time of Audit	1:00:23
Report ID	68	Synchronization Status	Different In WCS And Controller

Object name	802.11 171.71.128.75
Synchronization Status	Different In WCS And Controller

<

Attribute	Value In WCS	Value In Device
bridgingSharedSecretKey	*****	*****

Object name	Known Rogues 171.71.128.75 00:01:64:45:b9:b8
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:0e:37:bf
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:93:f9
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:1f:94:15
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:40:4d
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:41:01
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f0
Synchronization Status	Not Present In Controller

Object name	Known Rogues 171.71.128.75 00:02:8a:5b:46:f1
Synchronization Status	Not Present In Controller

190735

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（NMS）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（WCS/NCS/PI）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（WCS/NCS/PI）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（WCS/NCS/PI）から提供されるレポートの内容は次のようなものです。

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

アーキテクチャの統合

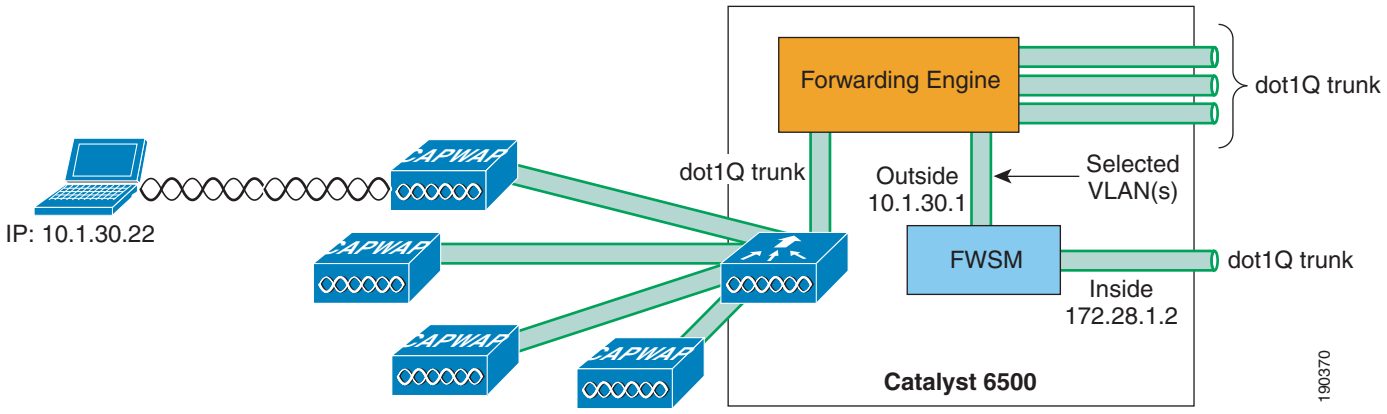
シスコでは、Cisco IOS に組み込まれたもの、サービスまたはネットワーク モジュールに統合されたもの、独立型アプライアンスとして提供されるもの、ソフトウェアとして提供されるものなど、さまざまなセキュリティ サービスを提供しています。

Cisco Unified Wireless Network アーキテクチャでは WLAN クライアントとアップストリームの有線ネットワーク間のレイヤ 2 接続を提供するため、ソリューションへのこれらのセキュリティ サービスの統合が容易になります。これは、クライアント トラフィックと「直列」に並ぶことで機能するアプライアンスやモジュールを、WLAN クライアントと有線ネットワーク間に容易に挿入できることを意味します。たとえば、古い WLSM ベースの展開では、Cisco Firewall Services Module（FWSM）を WLAN が通過するように Cisco 6500 に VRF-Lite を実装する必要がありますが、Cisco Unified WLAN の展開では、WiSM で簡単に WLAN クライアントの VLAN を直接 FWSM にマッピングできます。シスコ ワイヤレス製品の WLAN コントローラのうち、レイヤ 2 で物理/論理インターフェイスに直接 WLAN トラフィックをマッピングできないのは、ISR ベースの WLC モジュールのみです。ISR WLAN モジュールは ISR で利用可能なすべての IOS および IPS 機能にアクセスできますが、ルータの IOS VRF 機能を使用して、WLAN クライアントからの IP トラフィックを特定の ISR サービス モジュールのインターフェイスに送受信する必要があります。

図 4-28 では、WiSM と FWSM モジュールの間でのアーキテクチャの統合の例を示します。この例では、WLAN クライアントは外部ファイアウォール インターフェイスと同じサブネット上にあります。WLAN クライアント トラフィックが両方の方向でファイアウォールを通過することを保証するための、ルーティング ポリシーや VRF 設定は必要ありません。

WLAN の展開と組み合わせて Cisco Network Admission Control（NAC）アプライアンス（旧称 Cisco Clean Access）を実装することで、ネットワークに接続するエンド デバイスが、最新のセキュリティ ソフトウェア要件およびオペレーティング システムのパッチによってコンプライアンスに関する企業ポリシーに従っていることを保証できます。前述した FWSM モジュールのように、Cisco NAC アプライアンスもレイヤ 2 で Cisco Unified Wireless Network アーキテクチャに統合できます。これにより、無線ユーザの VLAN に NAC ポリシーを適用する厳密な管理が可能になります。

図 4-28　ファイアウォール モジュールの統合の例



ネットワーク層との統合が簡単であること以外に、Cisco Unified Wireless Network ソリューションは Cisco IDS の展開と統合されています。これにより、Cisco IDS によってブロックされているクライアントを、Cisco Unified Wireless Network から除外することができます。

Cisco Integrated Security Features

Cisco Integrated Security Features（CISF）は Cisco Catalyst スイッチに入っている機能です。悪意のあるユーザがネットワークへの無線アクセスを取得した後に実行するおそれのあるさまざまな攻撃を防御することができます。このセクションでは、これらの攻撃や、WLC がどのようにこれらの攻撃を防御するか、アクセス スイッチで CISF がイネーブルになっている場合に CISF がどのようにネットワークを保護するかついて説明します。

（注）　ここで述べる攻撃は、CISF がアクセス スイッチでイネーブルになっている場合に防御できるもののみであり、無線ネットワーク上に存在しうるすべての攻撃を総合的に分析することは意図していません。

攻撃のタイプ

攻撃は、有線ネットワークでも無線ネットワークでも発生することがあります。ただし、無線ネットワーク接続の場合、攻撃者はネットワークに物理的に接続しなくても攻撃を確立することができます。WLC および CISF には、次のような攻撃を防ぐために特別に設計された機能があります。

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

MAC フラッディング攻撃

MAC フラッディング攻撃は、スイッチの Content-Addressable Memory（CAM）テーブルに情報を入力して、LAN トラフィックのフラッディングを開始させようとするものです。これらの攻撃は、macof（dsniff パッケージの一部）などのツールによって実行されます。macof は、任意の MAC および IP 送信元アドレスおよび宛先アドレスのフレームのフラッディングを生成するものです。

イーサネット スイッチのレイヤ 2 の学習メカニズムは、パケットの送信元 MAC アドレスに基づいています。ポートで受信した新規の送信元 MAC アドレスそれぞれについて、そのポートと、ポートが属する VLAN の CAM テーブル エントリがスイッチによって作成されます。macof ユーティリティは、これらのエントリを保存するために使用可能なスイッチ上のメモリが有限であれば、通常 10 秒未満で CAM テーブルを一杯にします。CAM テーブルのサイズは有限です。他のエントリが期限切れになる前に十分なエントリが CAM テーブルに入力されると、CAM テーブルが一杯になり、新しいエントリを受信できなくなります。

スイッチの CAM テーブルが一杯になると、CAM テーブルの特定の MAC アドレスのポート番号を特定できないため、着信トラフィックがあるポートすべてがフラッディングされます。スイッチは基本的に、パフォーマンスとセキュリティが損なわれたハブのように機能します。オーバーフローによりローカルの VLAN 内でトラフィックがあふれるため、そのユーザが接続された VLAN 内のトラフィックを侵入者側から見ることができます。

レイヤ 3 では、macof の対象となる任意の IP 送信先では、マルチキャスト アドレス空間も使用します。したがって、Protocol Independent Multicast（PIM）プロセスが偽のルートを処理しようとするため、マルチキャストがオンになっているディストリビューション レイヤ スイッチは高い CPU 利用率を経験することになります。

DHCP の不正サーバ攻撃

DHCP の不正サーバ イベントは、意図的な攻撃の結果である可能性と、ユーザが誤ってネットワーク セグメントに DHCP サーバを持ち込み、誤って IP アドレスを発行しようとした可能性があります。侵入者は DHCP サーバを持ち込み、DNS サーバを示す IP アドレスや、侵入者に制御されているコンピュータに疑いを持つことなくユーザのトラフィックをリダイレクトするデフォルトのゲートウェイを提示することができます。

DHCP 枯渇攻撃

DHCP 枯渇攻撃は、特定のセグメントの DHCP 範囲内にあるアドレスすべてを枯渇させることを意図しています。DHCP が枯渇すると、正規のユーザであっても DHCP を介して要求された IP アドレスが拒否されるため、ネットワークにアクセスできなくなります。Gobbler は、自動 DHCP 枯渇攻撃を実行するパブリック ドメインのハッキング ツールです。DHCP 枯渇は純粋な DoS メカニズムである場合もありますが、悪意のある不正なサーバ攻撃と組み合わせることで、トラフィックを傍受できる悪意のあるコンピュータへトラフィックの方向を変更するために使用される場合もあります。

ARP スプーフィング ベースの中間者攻撃

中間者（MIM）攻撃は、ネットワーク上を移動するデータを悪意のあるユーザが傍受する（あるいは変更する）ネットワーク セキュリティ侵害です。MIM 攻撃では ARP スプーフィングが使用されます。ARP スプーフィングでは、Gratuitous ARP（GARP）要求が悪用され、悪意のあるコンピュータにトラフィックが誤って転送されることで、そのコンピュータが特定の LAN セグメントの IP セッションの「中間者」となります。ARP スプーフィングの実行には、*ettercap*、*dsniff* および *arpspoof* というハッキング ツールが使用されます。特に ettercap は特定の LAN セグメントのすべてのステーションを表示する高度なユーザ インターフェイスであり、さまざまな種類の IP セッションのパスワードを取り込むための高度なパケット キャプチャ機能があります。

IP スプーフィング攻撃

IP スプーフィング攻撃は、他のユーザの IP アドレスをスプーフィングして DoS 攻撃を実行します。たとえば、送信元のセカンド パーティの IP アドレスが攻撃を受けている間に、攻撃者はサード パーティのシステムを ping することができます。ping の応答は、サードパーティ システムからセカンド パーティに転送されます。

無線展開トポロジに対する CISF

このセクションでは、さまざまな Cisco Unified Wireless Network 展開トポロジについて説明します。次のセクションでは、WLC または CISF 機能が無線攻撃をどのように防御するかについて説明します。

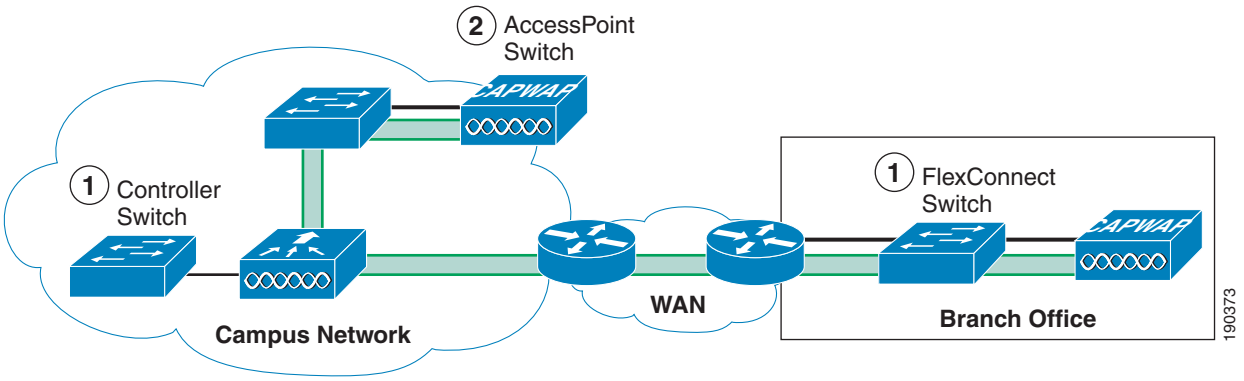
CISF は現在、アクセス ポイント（AP）から直接ではなくアクセス スイッチでのみ利用可能です。したがって、これらの機能の利点は、無線での攻撃者からのトラフィックがスイッチを通過している場合のみ有効です。

Unified Wireless Network ソリューションでは、3 か所をアクセス スイッチとみなすことができるため、アクセス スイッチの定義が若干異なります。

- コントローラ インターフェイスがネットワークで終端するポイント
- CAPWAP AP がネットワークで終端するポイント
- FlexConnect AP がネットワークで終端するポイント

これらのロケーションについて、図 4-29 で示します。

図 4-29　　アクセス スイッチ



CISF に関係する接続は、コントローラのスイッチおよび FlexConnect スイッチです。WLAN トラフィックは AP スイッチ上で終端せず、AP はそのスイッチ ポートに接続されている単一デバイスとして登場するだけで、セキュリティの観点からはアクセス クライアントとみなされるため、AP スイッチについては論じません。

（注）　CAPWAP AP と標準クライアントとの主な違いは、CAPWAP AP の Differentiated Services Code Point（DSCP）値が信頼済みであるという点です。

次のトポロジの対象範囲は、無線ユーザ間の攻撃に限定されています。これは、無線ユーザと有線ユーザが別々のサブネットでサポートされている（シスコのベスト プラクティスで推奨）ためであり、サブネット間の攻撃に関する議論はここの議論の範囲を超えているためです。

次の 3 つのトポロジについて考えます。

- トポロジ 1：攻撃者が接続されている AP と同じ AP にターゲットがアソシエートしている
- トポロジ 2：攻撃者とは別の AP にターゲットがアソシエートしている
- トポロジ 3：攻撃者とは別の AP にターゲットがアソシエートし、この AP が別のコントローラに接続される

1 つ目のトポロジでは、攻撃者とターゲットが両方とも同じ AP に関連付けられ、トラフィックは FlexConnect または WLC でローカルのままであるため、CISF は役に立ちませんが、Cisco Unified Wireless Network のネイティブのセキュリティでこれらの問題に対処できます。2 つ目と 3 つ目は CISF が有効なトポロジです。

さまざまなレベルの承認を必要とする企業の WLAN 展開では、一般的に SSID ごとに複数の VLAN が使用されます。これにより、FlexConnect AP または WLC 上のファスト イーサネット ポートと、アクセス スイッチの対応するポートの間に、802.1q のトランクを設定する必要があります。複数の VLAN が定義されるため、管理者はデータ トラフィックを AP と WLC の管理トラフィックから分離しておくことができます。

企業のセキュリティ ポリシーで、さまざまな種類のユーザに対してさまざまな種類の認証と暗号化が要求される（ゲスト アクセスに対してオープン認証は必要だが暗号化は行わない、従業員に dot1x 認証および強力な暗号化を行うなど）場合もあります。これは、FlexConnect AP または WLC にマルチ SSID および VLAN を定義することで達成されます。

上記の条件から、設定例で使用される設定は、WLC か FlexConnect AP とアクセス スイッチとの間のトランク接続を想定して行われます。

ポート セキュリティの使用による MAC フラッディング攻撃の軽減

ポート セキュリティでは、1 つのポートで許可される MAC アドレスの最大数を設定します。アドレス テーブルにアドレスを、手動、ダイナミックまたはその両方の組み合わせで追加できます。アドレス テーブル内の MAC アドレスの最大数に到達するとハードウェア内でパケットがドロップされ、アドレス テーブル内に MAC アドレスを持たないステーションがトラフィックを送信しようとします。

スイッチのアクセス ポートのポート セキュリティをイネーブルにすると、MAC フラッディング攻撃が停止されます。これは、そのポートで許容される MAC アドレスが制限されるためです。違反に対する対応が**シャットダウン**に設定されている場合、ポートはエラー ディセーブル状態になります。対応が*制限*に設定されている場合、送信元 MAC アドレスが未知のトラフィックはドロップされます。

ワイヤレス ネットワークでのポート セキュリティ

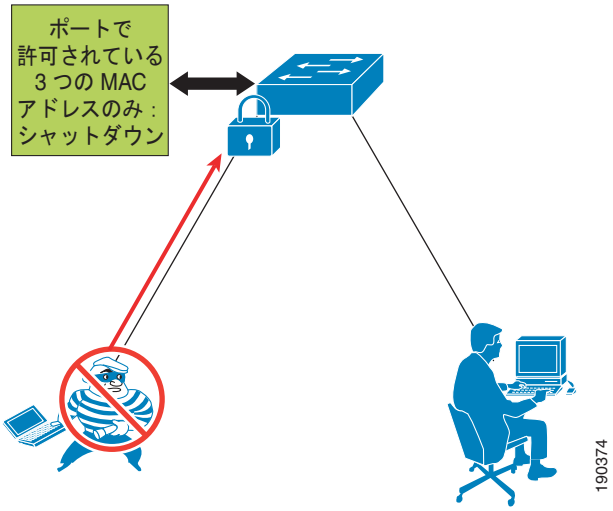
通常、FlexConnect AP や WLC に接続するスイッチ ポートでポート セキュリティをイネーブルにすることは推奨しません。ポート セキュリティを使用するということは、スイッチがそのポートから学習し、許可する MAC アドレスの正確な数が分かるということを暗に意味します。FlexConnect AP や WLC の場合、スイッチが学習したさまざまな送信元 MAC アドレスは通常、無線ユーザに対応します。スイッチ ポートでポート セキュリティを設定すると、有線ネットワーク上にいる特定の数のユーザだけが許可されます。

たとえば、一定の数の MAC しかアクセス ポイントを介してトラフィックを送信できないというセキュリティ ポリシーを設定している会社もあります。この場合、FlexConnect AP や WLC 上の MAC フィルタリングと、スイッチのポート セキュリティを組み合わせることで、選択されたユーザだけが有線ネットワークにアクセスできるようになります。

ただし、通常、会社が WLAN を展開するのは従業員の機動力を高めるためです。このことは、FlexConnect AP や WLC が、それ自体に関連付けられているユーザ数が常にあらかじめ決定されていないということを暗に意味しています。

したがって、AP に接続されているユーザ数を判断できない場合、スイッチ ポートのポート セキュリティをイネーブルにしても、メリットはありません。最悪の場合、違反が発生した場合にポートをシャット ダウンするようなポート セキュリティのポリシーが設定されると、強制的な DoS 攻撃が作成される場合があります。これが発生すると、その AP に接続されたユーザがすべてネットワークから切断されます。図 4-30 では、ポートをロックして SNMP トラップを送信することで無線 MAC フラッディング攻撃を制限するポート セキュリティの使用例を示します。

図 4-30　　ポート セキュリティの使用



ポート セキュリティの有効性

ポート セキュリティが攻撃を阻止するオプションでない場合、無線ユーザが MAC フラッディング攻撃を開始しても成功しません。その理由は、802.11 プロトコル自体にあります。AP とのアソシエーションは MAC ベースで行われます。このことは、AP ブリッジ（トランスレーショナル ブリッジ）のトラフィックが既知のユーザ（既知の MAC）との間で送受信されることを意味します。無線ユーザによって MAC フラッディング攻撃が開始された場合、ランダムに生成された MAC アドレスを持つ、AP に関連していないすべての 802.11 フレームはドロップされます。許可されるフレームは、スイッチがすでに学習していると思われる、悪意のあるユーザの MAC アドレスを持つフレームのみです。このため、アクセス ポイントの基本動作自体によって、スイッチが MAC フラッディング攻撃の被害に遭うことが防止されます。

ポート セキュリティの使用による DHCP 枯渇攻撃の軽減

有線アクセスの場合、ポート セキュリティでは現在、Gobbler などのツールを使用しているスイッチに接続された PC から実行される DHCP 枯渇攻撃を防止できます。攻撃が成功しないのは、ポート セキュリティによる軽減よりも、ツールの機能の制限によるものです。このような攻撃が失敗する理由は、Gobbler が別のソース MAC アドレスを使用して別の DHCP 要求を生成するからであり、ポートの保護によって攻撃を軽減できるからです。

ただし、攻撃者がイーサネット パケット内の MAC アドレスを使用でき、DHCP ペイロード内の MAC アドレス（chaddr フィールドという）を単純に変更した場合、ポート セキュリティでも攻撃は停止されません。この場合、現在可能な対策は、スイッチ ポートの DHCP レート リミッタを使用して攻撃を抑制することのみです。

無線 DHCP 枯渇攻撃

Unified Wireless Network 展開では、DHCP 枯渇攻撃に対する脆弱性は、ユーザ トラフィックを終端する WLC と、ユーザ トラフィックを終端する FlexConnect の間で異なります。

WLC は、DHCP 枯渇攻撃からネットワークを保護します。これは、DHCP 要求を確認することによってクライアントの MAC アドレスが chaddr に一致することが保証されるためです。アドレスが一致しない場合、DHCP 要求はドロップされます。

FlexConnect の場合、ユーザ VLAN はローカルで終端され、DHCP 要求はコントローラを通過せず、chaddr の分析は実行できません。この場合、このアクセス方法には、有線アクセスの場合と同じセキュリティ上の考慮事項が該当します。スマート（無線）攻撃者は、AP にアソシエートしている自分の MAC アドレスを使用してランダムな DHCP 要求を生成し、かどうかを AP に関連付けられただけを使用し、DHCP パケットのペイロード内で MAC アドレスの要求を単純に変更します。このとき、AP 側から見ると、パケットは有効に見えます。これは、信頼済み AP との関連付けに使用される MAC と送信元 MAC が同じであるためです。

DHCP スヌーピングによる不正な DHCP サーバ攻撃の軽減

DHCP スヌーピングは、DHCP スヌーピング バインディング テーブルを構築および維持し、信頼できない DHCP メッセージをフィルタリングすることでセキュリティを確保する DHCP セキュリティ機能です。この機能は、エンドユーザに接続する信頼できないインターフェイスと DHCP サーバまたは別のスイッチに接続する信頼できるインターフェイスとを区別することによって動作します。エンドユーザ ポートは、DHCP 要求のみを送信し、いかなる種類の DHCP トラフィックも送信しないように制限することができます。信頼済みポートではすべての DHCP メッセージの転送が許可されます。DHCP スヌーピング テーブルは VLAN ごとに構築され、クライアントの IP アドレスと MAC アドレスを信頼できないポートに関連付けます。DHCP スヌーピングをイネーブルにすると、非正規の DHCP サーバに接続しているユーザが信頼できない（ユーザ方向の）ポートに接続し、DHCP 要求に応答し始めるのを防止します。

ワイヤレス アクセスの DHCP スヌーピング

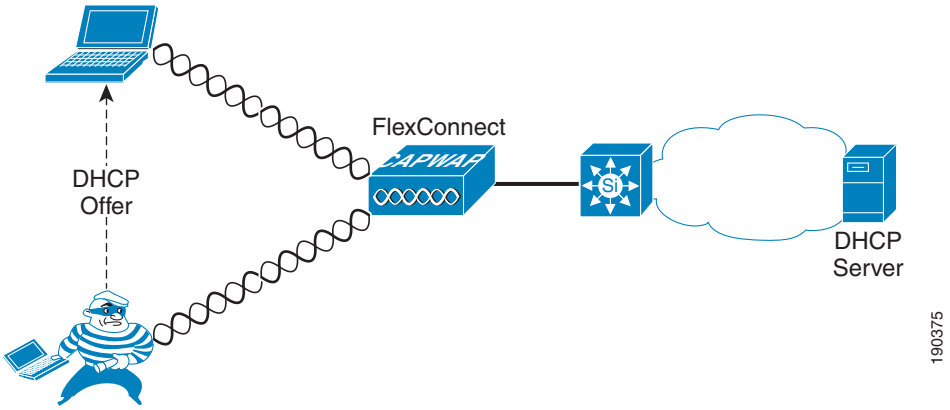
WLC はクライアントからのすべての DHCP 要求を管理し、DHCP リレー エージェントとして機能します。WLAN クライアントからの DHCP 要求は、WLAN に戻るブロードキャストではなく、WLC から設定済みの DHCP サーバへユニキャストされます。これにより、他の WLAN クライアントが不正な DHCP サーバ攻撃から WLC に接続することを防御します。

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

CISF 機能（この場合は DHCP スヌーピング）は AP でなくスイッチに対して実装されるため、不正なサーバからの悪意のあるメッセージを阻止する機能が働くのはスイッチからトラフィックが見える場合のみであることに注意してください。

図 4-31 で、不正な DHCP サーバの攻撃を軽減するための DHCP スヌーピングの使用例および、スイッチで DHCP を保護できるようになる前に攻撃がどのように発生するかを説明します。

図 4-31　不正な DHCP サーバ攻撃に対して使用されるセキュリティ



DHCP スヌーピングの有効性

DHCP スヌーピングは VLAN ごとにイネーブルになっているため、トランク ポートで動作します。異なる VLAN 内のクライアントの特定のトランク ポートで受信される DHCP 要求には、それぞれ異なる DHCP スヌーピング エントリが挿入されます。トランク ポートで DHCP スヌーピングが動作するという事実は非常に重要です。それは、この CISF 機能を、FlexConnect WLC のローカル インターフェイスに複数の SSID と VLAN が設定された WLAN 導入に応用できるためです。攻撃者が同じ WLAN/VLAN にターゲットとして関連付けられているが、経由する FlexConnect WLC は異なっている場合、スイッチによって DHCP スプーフィング攻撃を防御できます。ただし、攻撃者とターゲットが同じ FlexConnect WLC に関連付けられている場合、攻撃はアクセス スイッチを通過しないため、検出されません。

DHCP スヌーピングは、DHCP サーバに対する DHCP 要求を制限するレート制限によって、DHCP サーバ攻撃を防御します。

ダイナミック ARP インスペクションによる中間者攻撃の軽減

ダイナミック ARP インスペクション（DAI）は、アクセス スイッチで VLAN ごとにイネーブルになっています。これにより、ARP 要求や Gratuitous ARP（GARP）を含む応答を、DHCP バインディング テーブル内の DHCP スヌーピングが入力された MAC/IP エントリと比較します。スイッチが ARP メッセージを受信したときに、DHCP バインディング テーブルに一致するエントリがない場合、パケットは廃棄され、ログ メッセージがコンソールに送信されます。

DAI は、ettercap を使用して実行されるような中間者（MIM）攻撃につながる可能性のある ARP ポイズニング攻撃を防止します。ettercap は、悪意のあるユーザからターゲットへ送信された GARP メッセージを停止し、悪意のあるユーザのトラフィックを受信するように ARP テーブルを変更します。ARP メッセージは、攻撃者が接続しているポートで直接フィルタリングされます。

ワイヤレス アクセスに対する DAI

WLC は、WLC 自体に対する DAI と同様の機能を実行することで、MIM 攻撃を防御します。WLC に直接接続している VLAN のアクセス スイッチで DAI をイネーブルにしないでください。これは、WLC が GARP を使用してレイヤ 3 のクライアント ローミングをサポートしているためです。

FlexConnect とアクセス ポイントの間のトランクで設定された各 VLAN の DAI をイネーブルにできます。したがって、FlexConnect 上に複数の SSID と VLAN が存在する無線の展開において DAI は便利です。ただし、FlexConnect での WLC 展開では、DAI 機能の有効性に影響を与えるトポロジが 2 つあります。いずれのトポロジでも、両方の攻撃者が FlexConnect WLC に関連付けられていて、ターゲットにレイヤ 2 で隣接していると仮定しています。

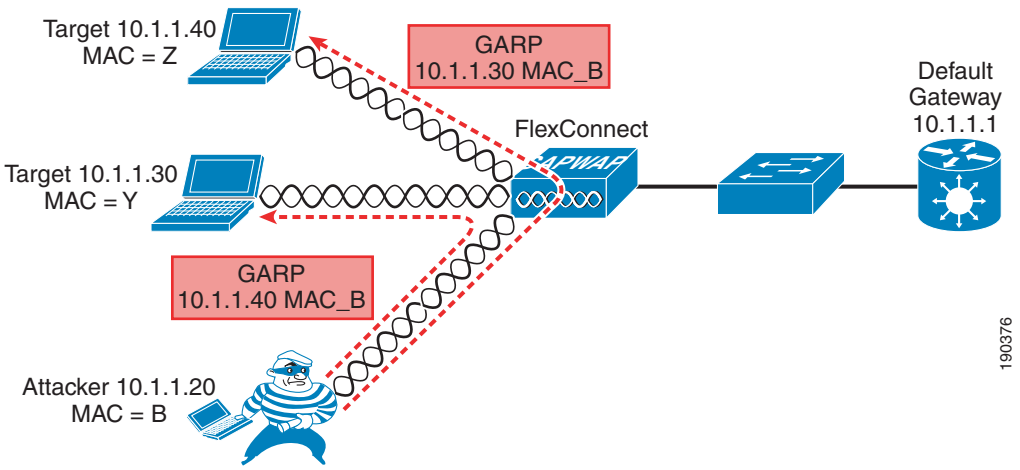
- トポロジ 1：一方のターゲットは無線接続されていて同じ AP に攻撃者として関連付けられているが、もう一方のターゲットはデフォルト ゲートウェイです。これが最も一般的な攻撃です。
- トポロジ 2：両方のターゲットが無線接続されています。

次の例では、攻撃がどのように開始され、停止されるかについて説明します。

- MIM は GARP を使用してデフォルト ゲートウェイと無線ターゲットの ARP テーブル エントリを変更し、攻撃者へトラフィックの方向を変更させようとします。DAI によってデフォルト ゲートウェイに対する GARP がブロックされる場合がありますが、無線ターゲットに対してスプーフィングされた GARP への DAI の影響はありません。これによって MIM 攻撃の影響は限定されますが、完全に MIM 攻撃の影響を防ぐことはできません。
- MIM 攻撃は無線クライアントに GARP を送信します。DAI を実装しているスイッチではこれらの GARP を認識しないため、攻撃を防止することはできません。

図 4-32 では、サブネット上の 2 つの IP 接続ノードに GARP を送信し、2 つのノードの間のトラフィックの方向を変えようとする攻撃メカニズムの例を示します。

図 4-32　　ダイナミック ARP インスペクション



DAI の影響

図 4-32 の例では、攻撃が完全に成功するのは、トラフィックが FlexConnect の WLC に対してローカルのままであり、スイッチを一度も移動しない場合のみです。通常、攻撃者の標的となるトラフィック（パスワードやアカウント情報など）は無線クライアントから有線ネットワーク（サーバまたはインターネット）に移動するため、それほど問題はありません。

デフォルト ゲートウェイと無線クライアントが攻撃対象である例を、半二重 MIM 攻撃と呼ぶことができます。ettercap により、すべてのトラフィックを侵入者に送信するように無線ユーザの ARP テーブルが変更される場合があります。ただし、次の例で示すように、デフォルト ゲートウェイへの GARP の送信はスイッチによって阻止されます。

```
4507-ESE#sh ip arp inspection log
Total Log Buffer Size : 32
```

```
Syslog rate : 5 entries per 1 seconds.
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Wed Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:48 PDT Tue Oct 3 2012) DHCP
Deny
Interface Vlan Sender MAC Sender IP Num of Pkts Reason
---------- ---- -------------- --------------- ----------- ------
Fa3/26 20 00d0.5937.7acc 10.20.1.100 1(11:07:49 PDT Tue Oct 3 2012) DHCP Deny
```

MAC アドレスがログに記録されるため、管理者は攻撃者をアソシエート解除することによって、さらに確実なブロック アクションを実行できます。

DAI が VLAN に設定されている場合、ARP のレート リミッタは、特定のポートからの ARP 要求のフラッディングを防ぐようにグローバルで設定されています。レート リミッタのデフォルト値は 15 パケット/秒（pps）です。この上限に到達すると、スイッチは攻撃を防ぐためにポートをディセーブルにします。この場合、攻撃者が MIM 攻撃を実行するためには、まず他の誰が隣接するレイヤ 2 であるかを見つけ出す必要があります。そのために ettercap は一連の GARP を生成し、サブネット上の各 IP アドレスであると主張します。この方法では、そのアドレスの実際の所有者が応答し、ettercap がテーブルを作成する場合があります。

実験では、ettercap を使用すると即座にこの上限に達し、ポートがシャット ダウンしました。これは、有線トポロジにも当てはまります。無線トポロジでは、AP に接続されたポートをシャット ダウンすると、すべての無線ユーザと外部との接続が失われ、可能性のある MIM 攻撃が DoS 攻撃に変わります。

このような（強制的に DAI をイネーブルにすることで作成される）DoS を回避するため、シスコでは AP に接続されたスイッチのポートで ARP レート リミッタをオフにすることを推奨します。この操作は、次のインターフェイス レベルのコマンドで実行できます。

```
ip arp inspection limit none
```

そのほか、しきい値を 15 pps より大きい値に変更する方法もあります。ただし、攻撃を実行するために使用される特定のツールの実装によって方法が異なるため、これは一般的な解決策ではありません。

IP ソース ガードの使用による IP および MAC スプーフィングの軽減

アクセス スイッチのインターフェイスがイネーブルの場合、IP ソース ガードは、DHCP スヌーピング バインディング テーブルの内容に基づいて、Per-Port アクセス コントロール リスト（PACL）を動的に作成します。この PACL は、DHCP バインディング時に発行された IP アドレスからトラフィックを送信するように強制することで、スプーフィングされた他のアドレスによってトラフィックが転送されるのを防止します。またこれにより、攻撃者が、アドレスを手動で変更したり、アドレスのスプーフィングを行うように設計されたプログラム（hping2 など）を実行したりして、有効なアドレスを偽装す

ることを防止します。この機能には、着信アドレスをフィルタリングするオプション（ポート セキュリティ）があります。ここでも、DHCP スヌーピング バインディング テーブル内の MAC アドレスを使用します。

攻撃者は一般的に、スプーフィングされたアドレスを使用して自分の実際のアイデンティティを非表示にし、DoS 攻撃などのターゲットに対する攻撃を実行します。

無線アクセスに対する IP ソース ガード

無線アクセスの場合には、FlexConnect の WLC にアクセス スイッチを接続するトランク ポート上で IP ソース ガードをイネーブルにできます。これにより、DHCP バインディング テーブル内のエントリと一致しない無線ユーザからのトラフィックをスイッチでフィルタリングできます。

WLC の後ろに設定されている VLAN では、IP ソース ガードをイネーブルにする必要はありません。これは、WLC が同様の機能を実行して、クライアントで使用される IP アドレスが、そのクライアントに割り当てられた IP アドレスであることを保証しているためです。

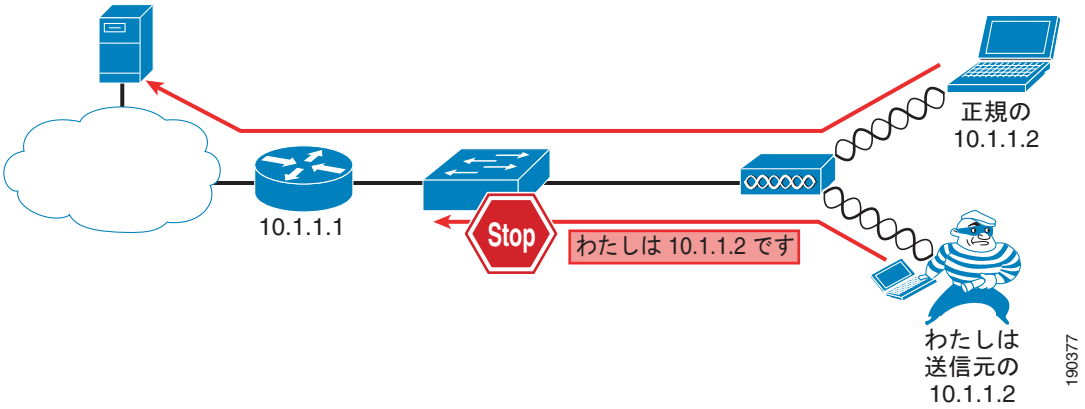
FlexConnect AP（標準の AP とは異なる）では WLAN クライアントの MAC アドレスと IP アドレスとのバインディング関係を検証できないため、FlexConnect の WLC 展開には IP ソース ガードが有利です。

テストでは、次の 2 つのトポロジが考慮されました。

- トポロジ 1：ターゲットが、同じ AP に関連付けられている他の無線ユーザによって表される。
- トポロジ 2：ターゲットが、別の AP に関連付けられた別の無線ユーザである。

図 4-33 は、IP および MAC スプーフィング攻撃を軽減するための IP ソース ガードの使用例です。

図 4-33　IP ソース ガードによる MIM の防止



IP ソース ガードの有効性

IP ソース ガード機能の有効性は、攻撃者がアドレスをどのようにスプーフィングするかと、どのトポロジがテストされるかという 2 つの要因に依存します。

AP へのアソシエーションはクライアントの MAC アドレスに基づくため、未知の送信元 MAC アドレスが指定されたフレームを受信すると、AP はそのフレームをドロップします。IP スプーフィング攻撃を実行する際、攻撃者にできる方法は、自分の MAC アドレスを使用するか、同じ AP に接続されている他のユーザからの MAC アドレスを使用するかです。他のすべての組み合わせ（ランダムな MAC アドレスを使用したり、別の AP に接続されたユーザの MAC アドレスを使用したりするなど）を使用すると、AP がフレームをドロップするため攻撃は失敗します。

攻撃者が自分の MAC アドレスを使用し、IP アドレスはスプーフィングした場合、スイッチでイネーブルになっている IP ソース ガードは、2 つ目トポロジではなく 1 つめのトポロジの攻撃を阻止します。1 つ目のトポロジでは、トラフィックは AP に対してローカルのままなので、CISF 機能は呼び出されません。2 つ目のトポロジでは、悪意のあるユーザによって送信された IP スプーフィングされたパケットのエントリが DHCP スヌーピング テーブルに存在しないため、CISF は正常に攻撃を阻止します。

ただし、攻撃者が同じ AP に接続された他の無線ユーザの MAC アドレスと IP アドレスの両方をスプーフィングできる場合、基本的には別のユーザのアイデンティティを想定しているため、攻撃はトポロジ 1 および 2 で成功します。MAC アドレスと IP アドレスの両方をスプーフィングすることは、暗号化が使用されていないホットスポット環境や、WEP の弱点を悪用した状況であれば現実に可能です。これが、可能な限り強力な暗号の使用をシスコが強く推奨する理由の 1 つです。

ターゲットへの攻撃の概要

表 4-2 では、該当するターゲットへの攻撃、考慮事項および解決策の簡単な要約を示します。

表 4-2　調査結果の概要

ターゲットへの攻撃	適用性	考慮事項	ソリューション
MAC フラッディング	なし	Macof がランダムな MAC アドレスを送信元および宛先として使用する	アソシエーション テーブルに存在しない送信元 MAC からのフレームを AP が廃棄する
DHCP 枯渇	FlexConnect では、ありコントローラが不正な DHCP 要求を廃棄する	要求する MAC が DHCP ペイロード内で送信される	なし - レート制限
不良 DHCP サーバ	FlexConnect では、ありWLAN からの DHCP オファーをコントローラがブロックする	不正な DHCP サーバが無線であることを前提とする	なし
無線クライアント間の MIM	FlexConnect では、ありコントローラが GARP をブロックする	この場合、トラフィックはスイッチを通過しない	なし
異なる AP の無線クライアント間の MIM	FlexConnect では、ありコントローラが GARP をブロックする	ハッカーがトラフィックを妨害できるのは有線に対してのみである	違反のある DAI
無線クライアントと有線クライアントの間の MIM	FlexConnect では、ありサポートされていないコントローラ設定	ハッカーがトラフィックを妨害できるのは有線に対してのみである	違反のある DAI
IP スプーフィング	FlexConnect では、ありコントローラが IP アドレスと MAC アドレスのバインディングをチェックする	アイデンティティのスプーフィングを防止するために無線での暗号化が必要	IP ソース ガード

（注）　有線アクセス上に存在するのは CISF 機能の対象となる攻撃しかないので、攻撃者は常に無線であると想定されますが、ターゲットはそのとき関わっているトポロジによって有線の場合と無線の場合があります。

CHAPTER 5

Cisco Unified Wireless QoS

この章では、WLAN 実装に関連する QoS について説明します。ここでは WLAN QoS 全般について説明します。セキュリティ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、さまざまなネットワーク テクノロジーを介して、選択されたネットワーク トラフィックに差別化サービスを提供するネットワークの機能のことです。QoS テクノロジーには次の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。
- ネットワーク管理者がネットワーク ユーザとのサービス レベル契約（SLA）を制定できます。
- ネットワーク リソースをさらに効率的に共有できるようにし、ミッションクリティカルなアプリケーションの処理を効率化します。
- 時間依存型マルチメディアおよび音声アプリケーションのトラフィックを管理し、このトラフィックがベストエフォート型のデータ トラフィックよりも優先度が高く、帯域幅が大きく、かつ遅延が少なくなるようにします。

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

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

無線 QoS の展開方式

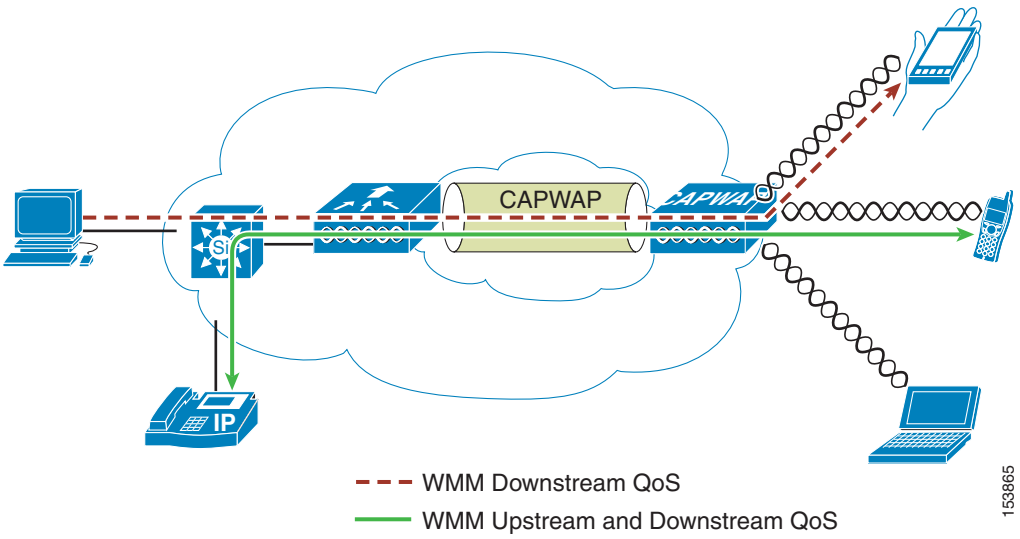
従来、WLAN は主に低帯域幅のデータ アプリケーション トラフィックの伝達に使用されていました。現在では、WLAN は縦方向の環境（小売、金融、教育など）および企業環境に拡張され、時間依存型のマルチメディア アプリケーションと共に高帯域幅のデータ アプリケーションの伝達に使用されています。この要件に対応するために、無線 QoS が必要になりました。

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

Cisco Unified Wireless 製品は、Wi-Fi Alliance が公開した 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 Wireless QoS の展開例を示します。

図 5-1　　QoS の展開例



QoS パラメータ

QoS は、通信の質およびサービスの可用性を反映した通信システムのパフォーマンスの基準として定義されています。サービスの可用性は QoS の重要な要素です。QoS を正しく実装するには、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。

ネットワークの通信の質は、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 の送信の質

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

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 では、*無線アップストリーム*および*無線ダウンストリーム* QoS の定義を示します。

図 5-2　アップストリームおよびダウンストリーム QoS

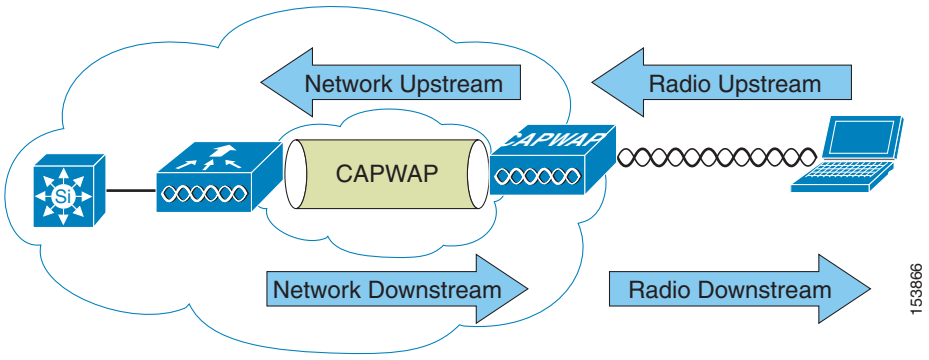


図 5-2 は、以下のことについて示しています。

- *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。クライアントの無線アップストリーム QoS は、クライアントの実装によって異なります。
- *無線アップストリーム* QoS：WLAN クライアントから発信され、AP まで伝送されるトラフィック。WMM では、WMM をサポートする WLAN クライアントのアップストリーム QoS が提供されます。

- *ネットワーク ダウンストリーム*：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。この時点で QoS を適用することで、AP へのトラフィックの優先順位付けと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、その AP のトラフィック分類ルールに従って、AP からアップストリーム ネットワークまでのトラフィックを分類します。

QoS およびネットワークのパフォーマンス

QoS 機能の適用は、負荷の軽いネットワークでは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大するにつれて、QoS 機能がアプリケーションのパフォーマンスに作用し始めます。QoS は、選択されたトラフィック タイプの遅延、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認識されます。クライアントは、アップストリーム伝送に対しても、また AP からのベストエフォート伝送に対しても、他のクライアントと競合します。特定の負荷状況下では、クライアントにアップストリームの輻輳が発生し、AP で QoS 機能を適用しても、QoS 依存型アプリケーションのパフォーマンスが許容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 から自動的に利益を得ているという意味ではありません。WMM の利点を求めるアプリケーションが適切な優先度の分類をそのトラフィックに割り当て、オペレーティング システムはその分類を WLAN インターフェイスに渡す必要があります。VoWLAN 端末などの専用デバイスでは、設計の一部としてこの機能があります。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 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（コンテンション ウィンドウ）。

DCF を 802.11 ネットワークで使用して RF メディアへのアクセスを管理します。802.11e ベースの拡張型分散チャネル アクセス（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

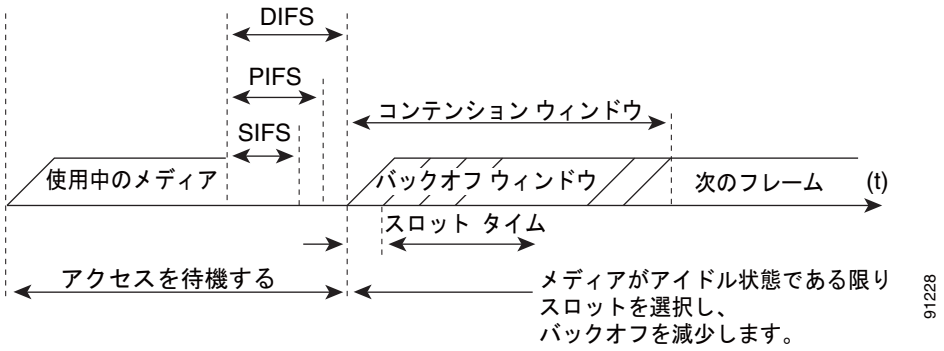
802.11 標準は、フレーム間スペース（IFS）を次のように定義します。

- 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 に対するものです。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 の管理フレームとコンテンションを起こさないフレーム（フレーム シーケンスの一部であるフレーム）では SIFS が使用され、データ フレームでは DIFS が使用されます（図 5-3 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 から最小コンテンション 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」（P.5-6）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 タイム（20 μs）ごとの、ランダム バックオフ番号のデクリメントを開始します。
4. 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、断片化は発生しません。

図 5-4　　分散コーディネーション機能の例

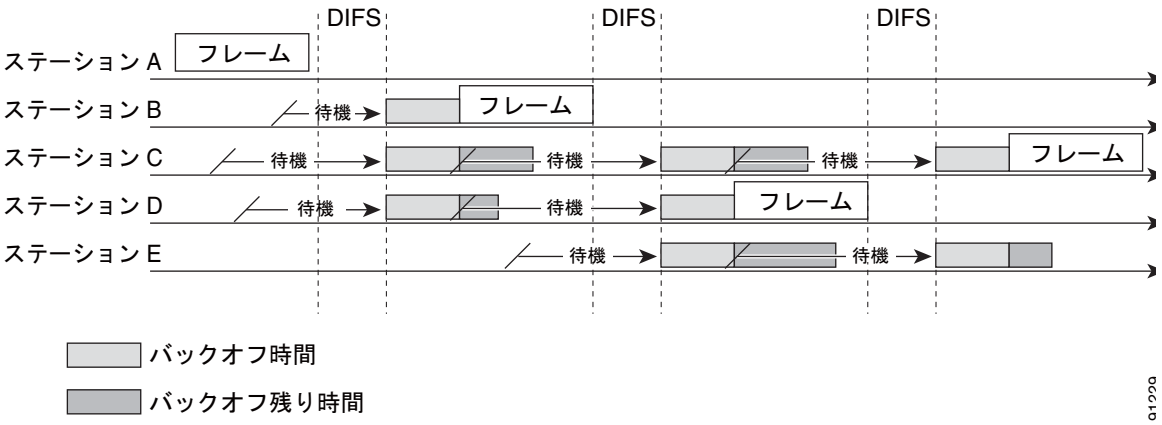


図 5-4 で示している DCF の手順は次のとおりです。

1. ステーション A は正常にフレームを送信します。他の 3 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 タイムごとに 1 度バックオフ カウンタのデクリメントを開始します。
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 の前に 0 に達したので、ステーション B がフレームの送信を開始します。
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しなければなりません。
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 と同様に待機しなければなりません。
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届くと、このプロセスが続行されます。

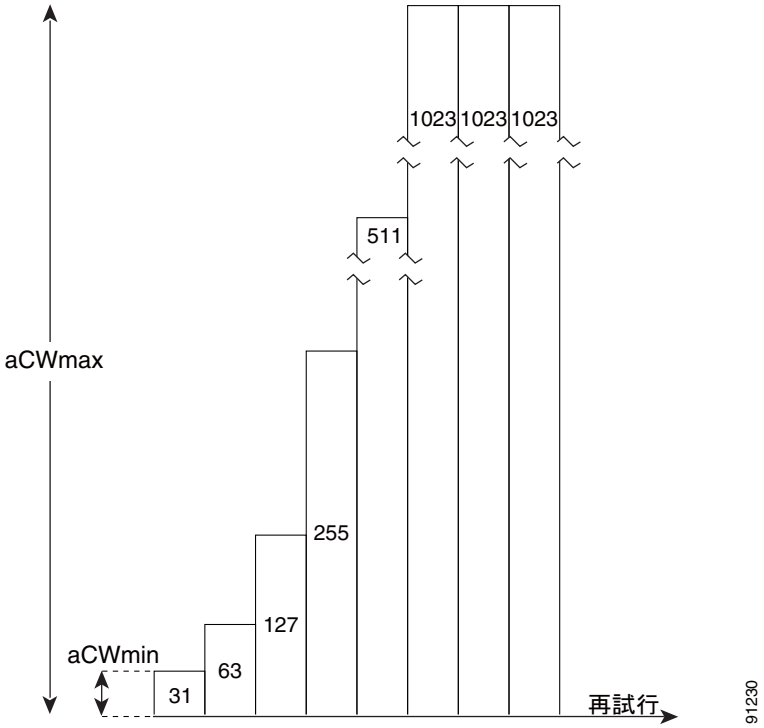
aCWmin、aCWmax および再試行

DCF はコンテンション 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：最小コンテンション ウィンドウ
- aCWmax：最大コンテンション 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やし、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 と同じに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。別の物理レイヤの実装では、値が異なる場合があります。

Wi-Fi Multimedia

この項では、Wi-Fi multimedia（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 草案に述べられている一連の機能に対応した Wi-Fi Alliance の認証です。この認証はクライアントと AP の両方を対象としており、WMM の操作を認定します。WMM は基本的に、802.11e の EDCA コンポーネントの実装です。Wi-Fi の追加認証が、802.11e の別のコンポーネントを対象に計画されています。

WMM の分類

WMM では 802.1P 分類方式（IEEE 802.1D MAC Bridges 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

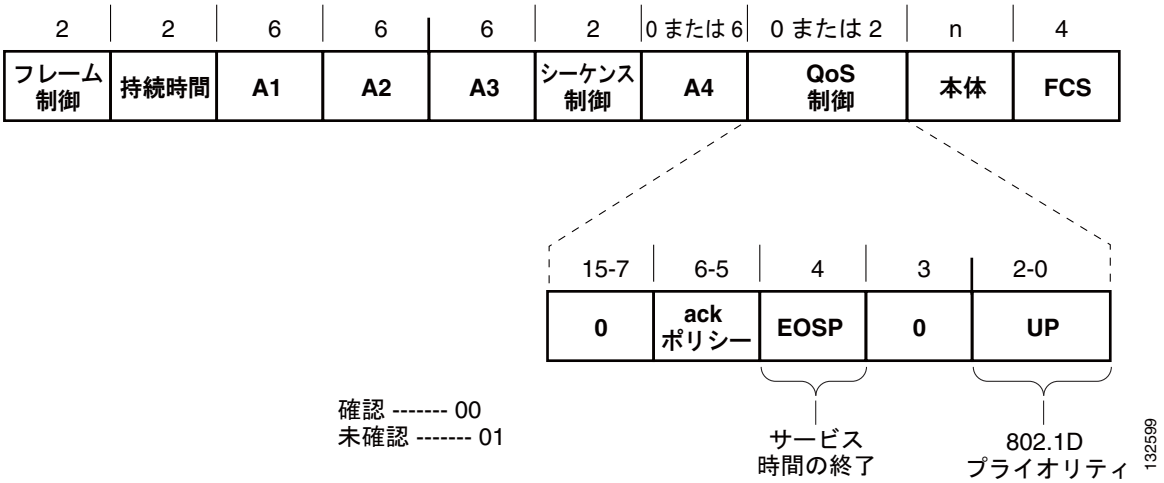
表 5-2 で示すように、これらのアクセス カテゴリは WMM デバイスに必要な 4 つのキュー（「WMM キュー」（P.5-9）を参照）にマッピングします。

表 5-2　　表 2 802.1P および WMM の分類

プライオリティ	802.1P のプライオリティ	802.1P の指定	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
最高	7	NC	

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

図 5-6　WMM フレーム形式



WMM および IEEE 802.11e の分類は、シスコのネットワークで推奨および使用されている、IETF 推奨の分類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、6 つの分類をレイヤ 3 ネットワーク制御に使用できます。両方の標準に準拠するため、Cisco Unified Wireless ソリューションでは、トラフィックが無線と有線の境界を横切る際に、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。4 つの別個のキューが、各アクセス カテゴリに 1 つずつあります。これらのキューはそれぞれ、前述した DCF メカニズムに対するのと同様の方法で無線チャネルを確保するために競います。このとき、各キューには異なる IFS、CWmin、および CWmax の値が使用されます。異なるアクセス カテゴリからの複数のフレームが内部で衝突した場合、優先度の高いフレームが送信され、優先度の低いフレームは、バックオフ パラメータをキューイング メカニズムの外部のフレームと衝突した場合と同様に調整します。このシステムは、拡張型分散チャネル アクセス（EDCA）と呼ばれています。

図 5-7　WMM キュー

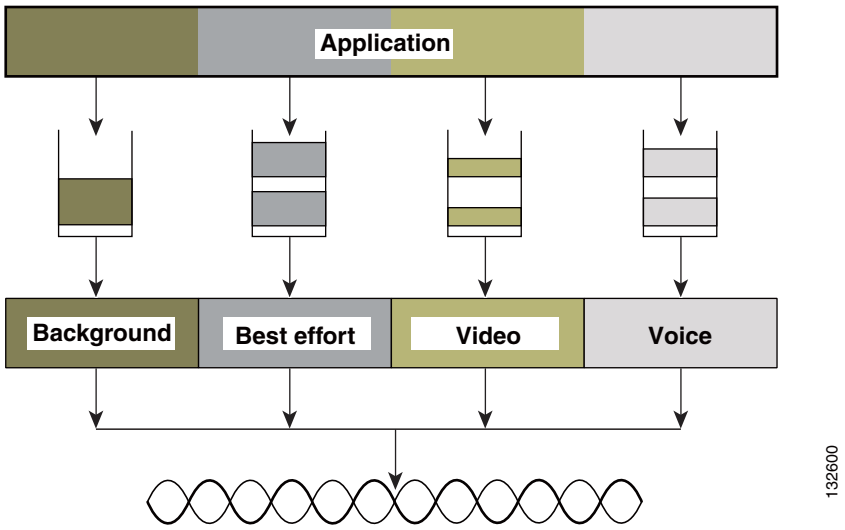
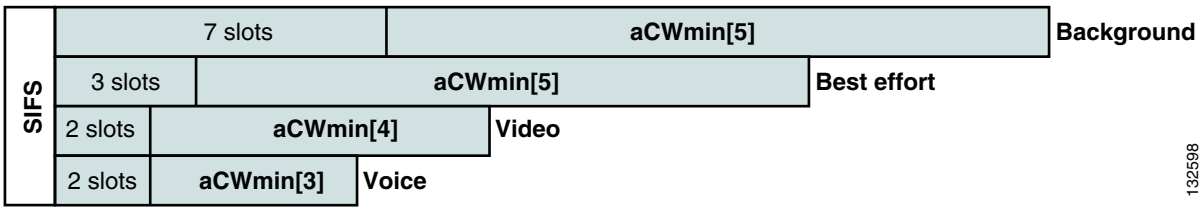


図 5-8 は、EDCF の背後の原則を示しています。ここでは、異なるフレーム間スペースと CWmin および CWmax の値が、トラフィックの分類ごとに適用されています（明確にするため Cwmax は示されていません）。トラフィック タイプが異なると、ランダム バックオフをカウント ダウンする前に別の IFS を待機させることができます。ランダム バックオフ番号の生成に使用される aCW 値も、トラフィックの分類によって異なります。たとえば、音声の CWmin[3] は 23 -1 で、ベストエフォート トラフィックの CWmin[5] は 25 -1 です。優先度が高いトラフィックでは IFS 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高くなります。

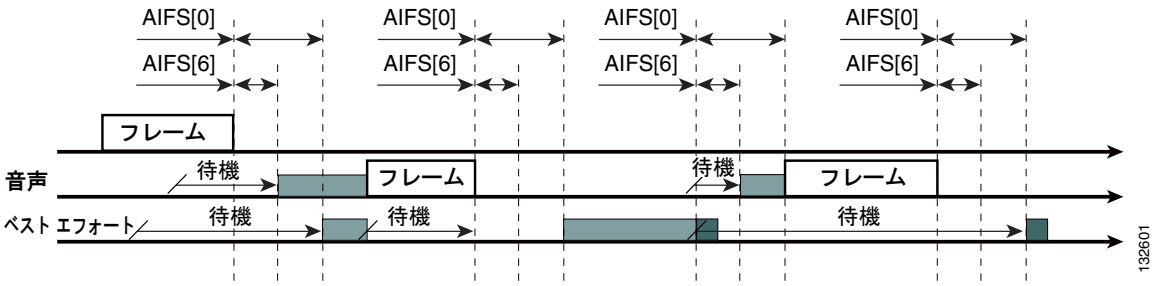
図 5-8　アクセス カテゴリのタイミング



EDCA

図 5-9 は、拡張型分散チャネル アクセス（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 タイムです。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 CWmin 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* （aCQmin+1）- 1	3	0	0

表 5-3　WMM クライアント パラメータ （続き）

AC	CWmin	aCWmax	AIFS[n]	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_VI	（CWmin+1）/2-1	CWmin	1	6.016 ミリ秒	3.008 ミリ秒
AC_VO	（CWmin+1）/4-1	（CWmin+1）/2-1	1	3.264 ミリ秒	1.504 ミリ秒

表 5-4　WMM AP パラメータ

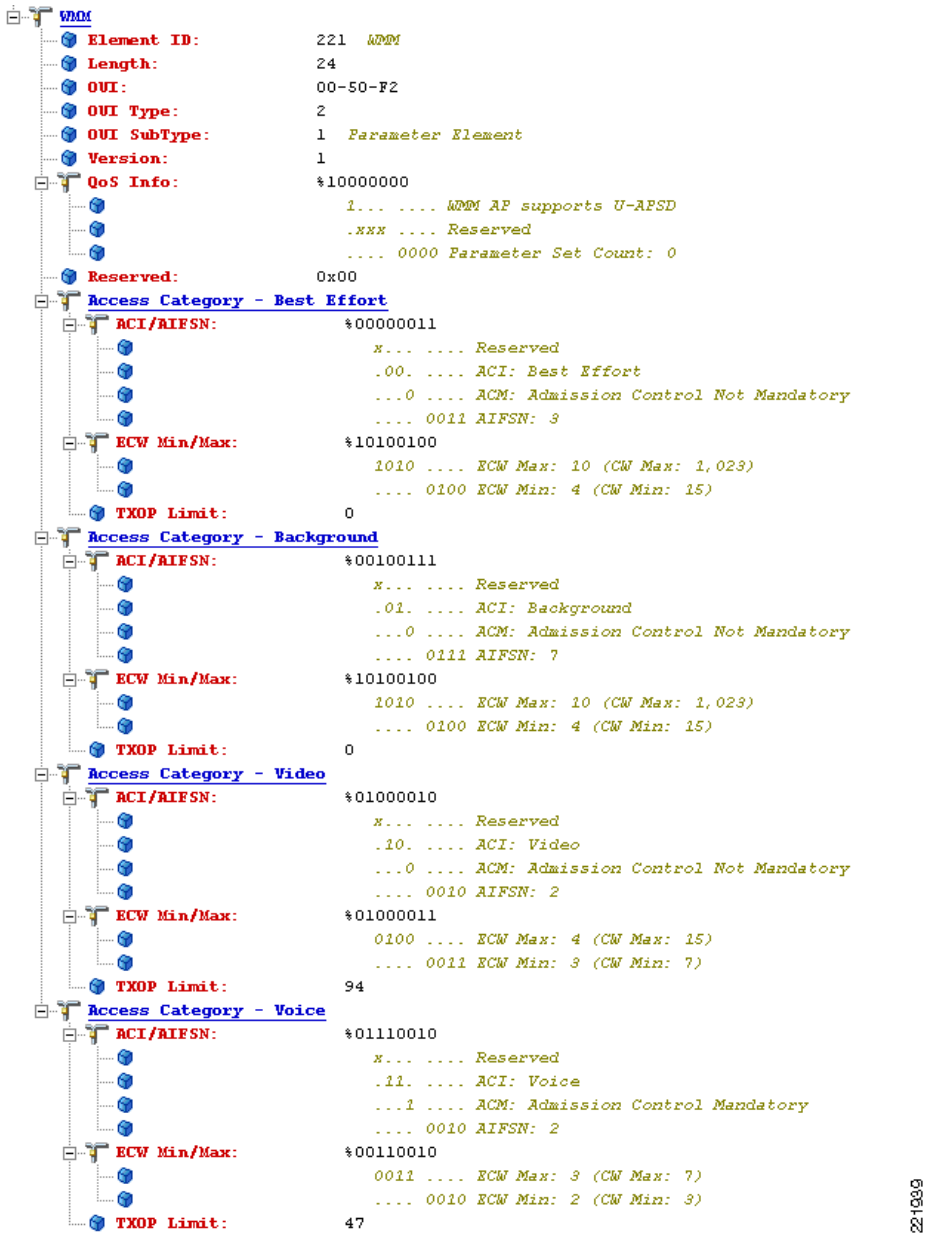
アクセス カテゴリ	CWmin	aCWmax	AIFS[n]	TXOP 制限（802.11b）	TXOP 制限（802.11a/g）
AC_BK	CWmin	aCWmax	7	0	0
AC_BE	CWmin	4*（aCQmin+1）-1	3	0	0
AC_VI	（CWmin+1）/2-1	CWmin	2	6.016 ミリ秒	3.008 ミリ秒
AC_VO	（CWmin+1）/4-1	（CWmin+1）/2-1	2	3.264 ミリ秒	1.504 ミリ秒

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 タイム、バックグラウンド フレームでは 22（7+31/2）スロット タイムです。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（U-APSD）

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。

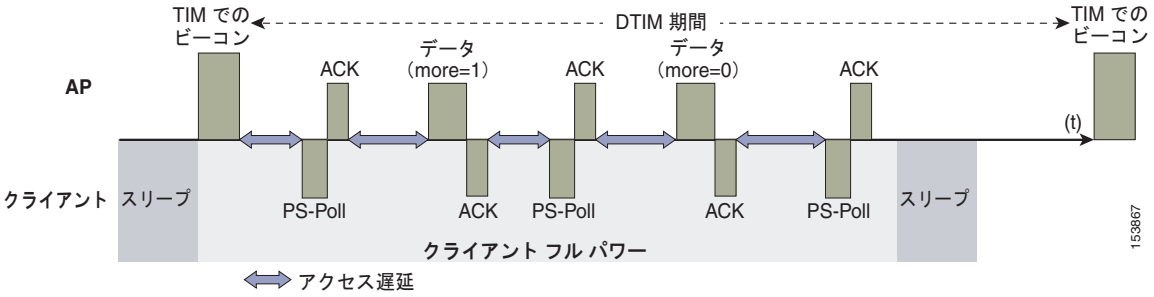
- U-APSD の第 1 の利点は、音声クライアントが AP との間で音声フレームの送受信を同期できることです。そのため、クライアントは音声フレームの各タプルの送受信間に省電力モードになることができます。U-APSD をサポートしているアクセス カテゴリ内で WLAN クライアントからフレームが送信されると、AP はその WLAN クライアントに対してキューイングされているそのアクセス カテゴリのあらゆるデータ フレームの送信を開始します。U-APSD クライアントは、AP からサービス時間終了（EOSP）ビット セットを含むフレームを受信するまで、AP の接続を待機し続けます。EOSP ビット セットによって、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、配信トラフィック通知メッセージ（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リング 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、コールによるコンテンション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



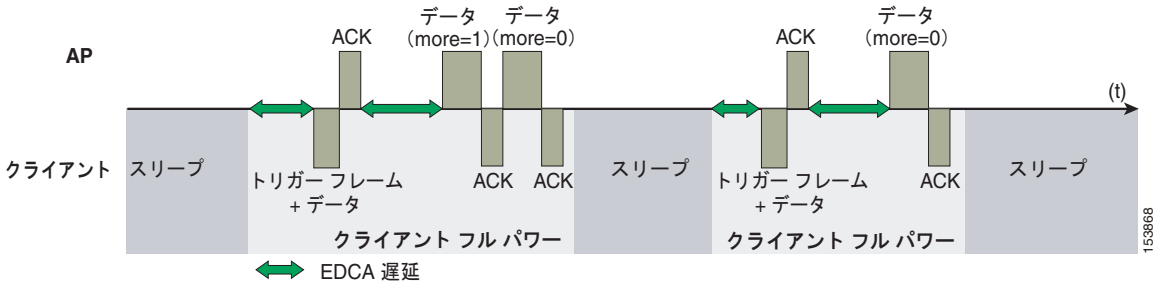
省電力モードにあるクライアントは、まず AP ビーコン内の TIM の存在を介して、AP でデータが待機していることを認識します。クライアントは、そのデータを取得するために AP を省電力ポーリング（PS-Poll）する必要があります。クライアントに送信されたデータが複数のフレームの送信を要求している場合、AP はそのことを送信済みデータ フレーム内に示します。このプロセスでは、クライアントはバッファされたすべてのデータを取得するまで、AP に省電力ポーリングを送信し続ける必要があります。

このことは 2 つの大きな問題点を提示しています。1 つ目の問題は、このプロセスが非常に非効率的で、PS ポーリング以外にも通常のデータ交換を要求し、DCF に関連する標準アクセス遅延を発生するということです。第 2 の問題点は、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さまざまに異なるということです。このことは、音声トラフィックに対してより重大な問題となります。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、音声端末は、音声コールの進行中、省電力モードをフル送信に切り替えて動作を受信します。これにより、許容できる音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、フレームを確認すると、データがキューイングされていることと、接続し続けなくてはならない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。すべての後続のフ

レームは、応答フレームの後で直接送信されます。VoWLAN 実装では、AP でキューイングされている可能性があるフレームは 1 つのみです。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 モードに入ることできます。

図 5-12　U-APSD



この方法は、以前の方式の短所を両方とも克服した、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* * 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 クライアントから AP へ、そのトラフィック要件に関する信号を送信できます。802.11e MAC 定義には、コンテンションベースの 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 使用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（トラフィック ストリームの追加）

Add Traffic Stream（ADDTS）機能は、WLAN クライアントが AP への*アドミッション要求*を実行する際に使用されます。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。

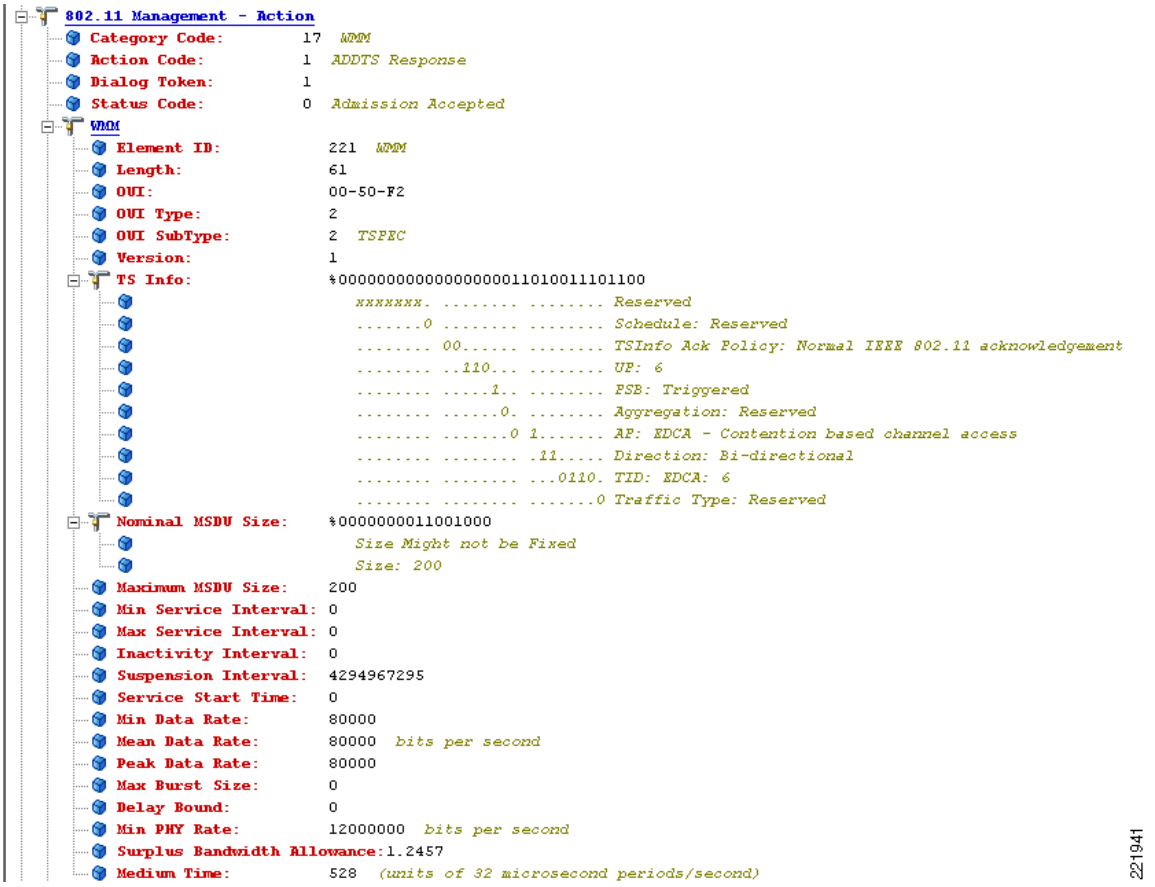
- アソシエーションおよび再アソシエーション メッセージ：ステーションがトラフィック ストリームをアソシエーションの一部として確立しようとすると、アソシエーション メッセージに 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。ステーションが別の AP にローミングすると、再アソシエーション メッセージに 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。

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 端末と 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 端末）。ローミングの際には、TSpec 要求が再アソシエーション要求に追加されます。

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」（P.5-18）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 がイネーブルになっている場合、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 要求のデコード

図 5-14　ADDTS 応答のデコード



WLAN インフラストラクチャ対応の QoS-拡張機能

*Cisco Centralized WLAN アーキテクチャ*には、WMM サポート機能のほかにいくつかの QoS 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 ポリシー
- 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、次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

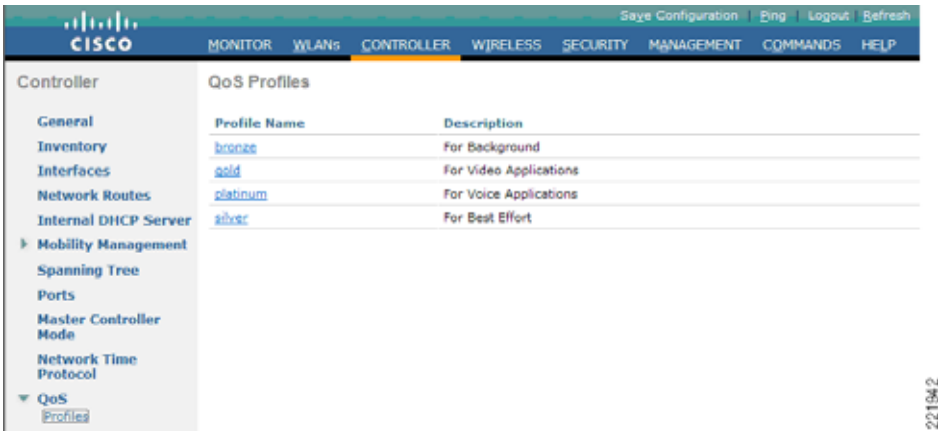
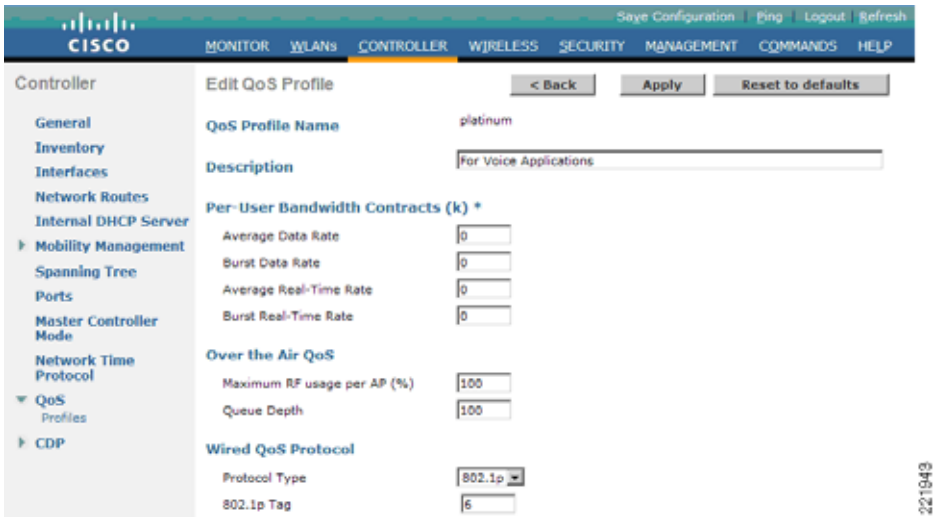


図 5-16 に示すプロファイルごとに、帯域幅の契約、RF 使用制御、および許可された最大の 802.1P 分類を設定できます。

図 5-16　QoS プロファイルの設定



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 802.1P 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

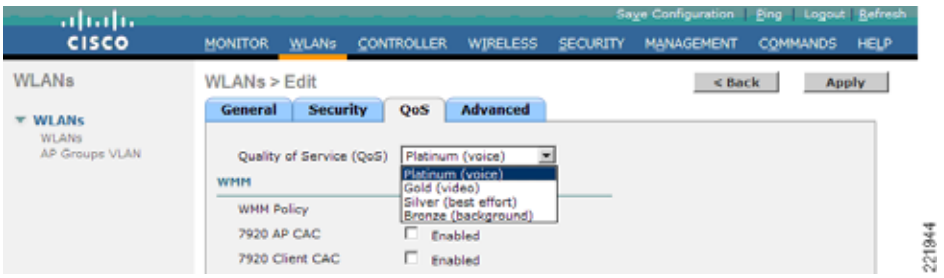
  802.1P 分類によって、そのプロファイルを使用する WLAN で許可される最大 CoS 値が設定されます。

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、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 5-17 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、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 5-17　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 5-18 を参照）。WMM オプションには次のようなものがあります。

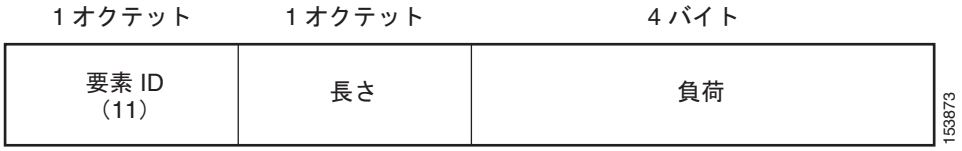
- [Disabled]：WLAN で WMM 機能はアドバタイズされず、WMM ネゴシエーションも許可されません。
- [Allowed]：WLAN で WMM クライアントと WMM 以外のクライアントが許可されます。
- [Required]：WMM 対応クライアントのみをこの WLAN にアソシエートできます。

図 5-18　WLAN WMM ポリシー

Voice over IP 電話

図 5-19 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 5-19　QBSS 情報要素



特定の状況でサポートする必要のある QBSS IE は、次の 3 つです。

- 旧 QBSS：Draft 6（pre-standard）
- 新 QBSS：Draft 13 802.11e（standard）
- 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 5-20 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、アソシエートすべき最良の 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。このサポートには次の機能があります。

- 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 以前の古い 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、および AP CAC 制限のさまざまな組み合わせにより、次のようなさまざまな QBSS IE が送信されます。

- WMM だけがイネーブルの場合、IE 番号 2（802.11e 標準）QBSS Load IE がビーコン応答とプローブ応答で送信されます。
- 7920 クライアント CAC 制限がサポートされる場合、IE 番号 1（以前の標準 QBSS IE）が 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 を使用するので、これらの 3 つの QBSS は相互に排他的です。たとえば、ビーコン応答およびプローブ応答には 1 つの QBSS IE のみを含めることができます。

アドミッション制御パラメータ

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

図 5-20　音声パラメータの設定

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 (%)] 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。

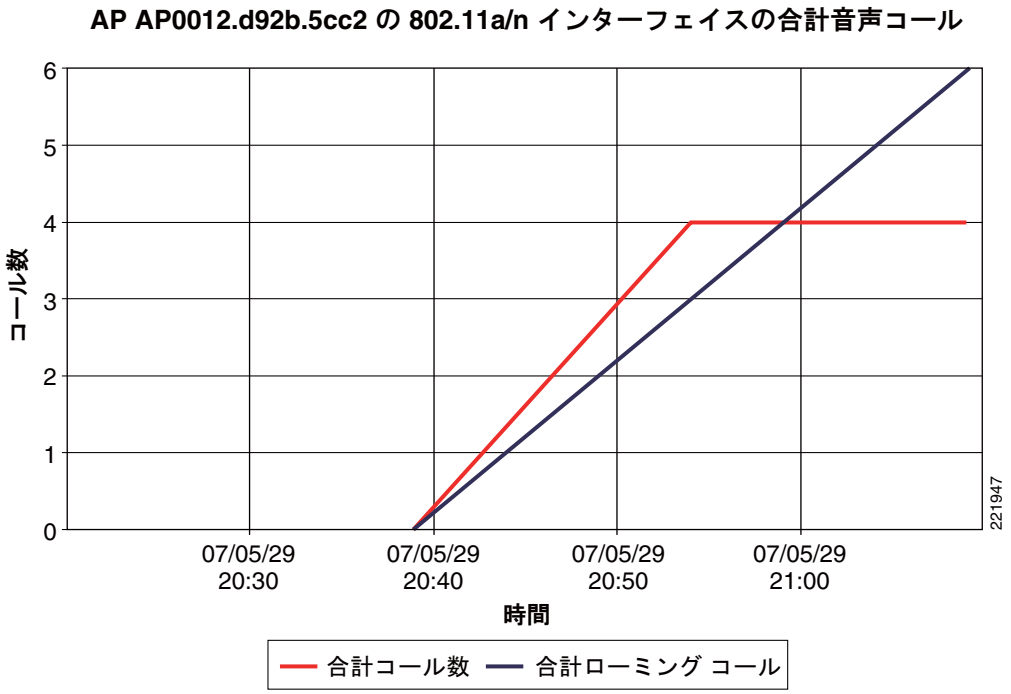
（注）　音声およびビデオの負荷ベースの CAC は非メッシュ AP に適用されます。メッシュ AP の場合は、静的な CAC のみが適用されます。

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 5-20）の [Metrics Collection] オプションで、Cisco Prime Infrastructure で使用するために音声またはビデオ コールでデータを収集するかどうかを指定します。

図 5-21 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）使用できるほか、Cisco Prime Infrastructure でのグラフィック表示やファイルへの書き込みが可能です。

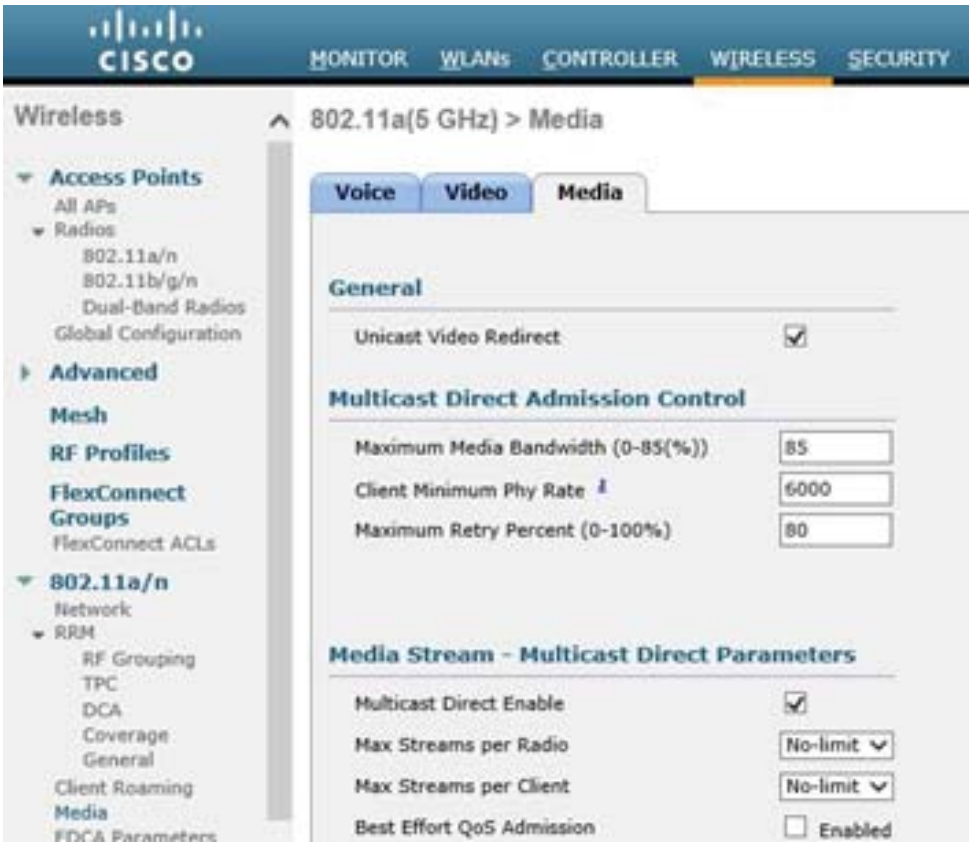
図 5-21　Cisco Prime Infrastructure の音声統計



（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 5-21 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 5-22 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 5-22　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、実行中のビデオ 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 のコンフィギュレーション 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 では、アクセス制御が有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	確立されたトラフィック ストリーム	トラフィック ストリームなし
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ついては、WLAN QoS と共にパケットが送信されます。

表 5-6　ダウンストリーム トラフィック

AC 有効	確立されたトラフィック ストリーム	トラフィック ストリームなし
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。

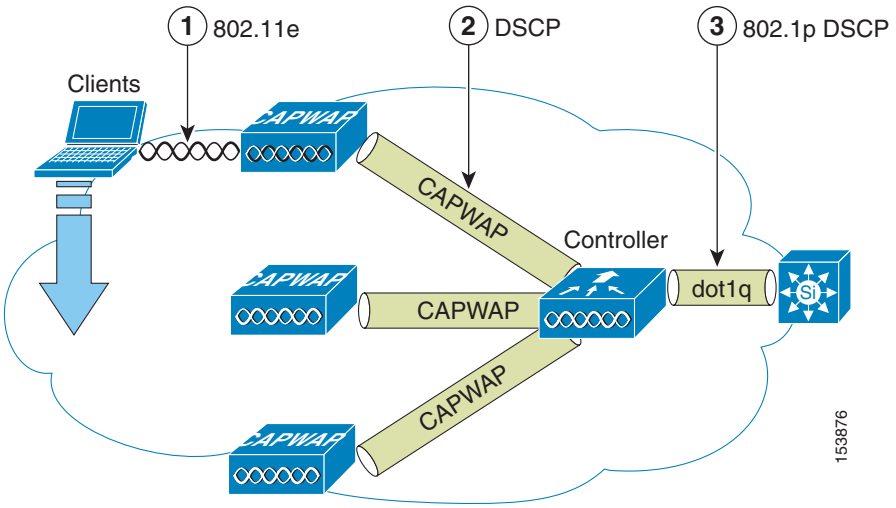
802.11e、802.1P および DSCP のマッピング

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 に行く 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」（P.5-32）を参照）が割り当てられます。

図 5-23 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 5-23　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 を有効化したクライアントは、WLC への CAPWAP パケットに対する該当 DSCP 分類へマップされたフレームの分類が割り当てられています。このマッピングは、QoS ベースラインへの準拠に必要な変更を除いて、IEEE CoS から DSCP へのマッピングの標準に従っています。この DSCP 値は、WLC において、WLC インターフェイスから発信される 802.1Q フレーム上で CoS 値に変換されます。
- WMM 以外のクライアントには、その WLAN のデフォルトの QoS プロファイルに一致するよう設定された 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、CAPWAP パケットの DSCP 値に基づき、含まれている IP パケットの DSCP 値には基づきません。そのため、エンドツーエンドの QoS システムの整備が重要になります。

QoS ベースラインの優先度のマッピング

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	-	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
バックグラウンド	2	0	1
バックグラウンド	4	0	1
バックグラウンド	6	0	1

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 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 は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た 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、アップストリームとダウンストリーム パケットに適用されます。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の場合、AP からのクライアント フレームには CoS マーキングはありません。

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 によりその AP に対して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 に割り当てられた QoS ポリシーに基づきます。

WLC スイッチの設定

WLC 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）か、またはダウンストリーム（AP および WLAN クライアントに送信）です。ダウンストリーム トラフィックは 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開放された 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 上の QoS ポリシーによって制御されます。（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開放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 の設定の CoS を信頼することを選択しています。これは、この場合、WLAN QoS を集中的に管理できるため、WLC 設定の他に WLC スイッチ接続で追加のポリシーを管理する必要がないためです。

```
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 端末をサポートする WLAN では、これらのクライアントの WLAN QoS メカニズムに頼ってください。これらの WLAN には、トラフィック シェーピングも Over-the-Air QoS も適用しないでください。

WLAN 音声とシスコの電話機

Cisco Unified Communications 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

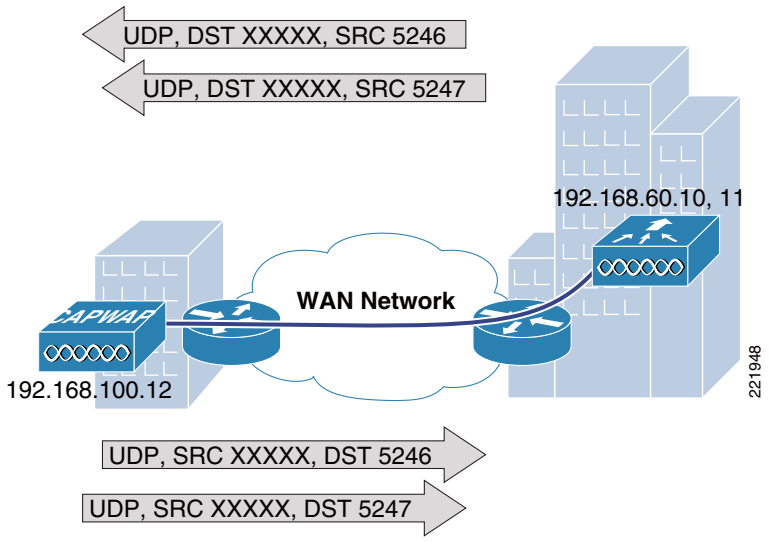
Cisco Jabber の一般的な概要については、次のページを参照してください。

http://www.cisco.com/web/products/voice/jabber.html

WAN 接続を介した CAPWAP

ここでは、図 5-24 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 5-24　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 コントロール トラフィック：UDP ポート 5246 で識別
- CAPWAP 802.11 トラフィック：UDP ポート 5247 で識別

CAPWAP コントロール トラフィック

CAPWAP コントロール 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、WAN からのファイルのダウンロードの影響が最小化されます。

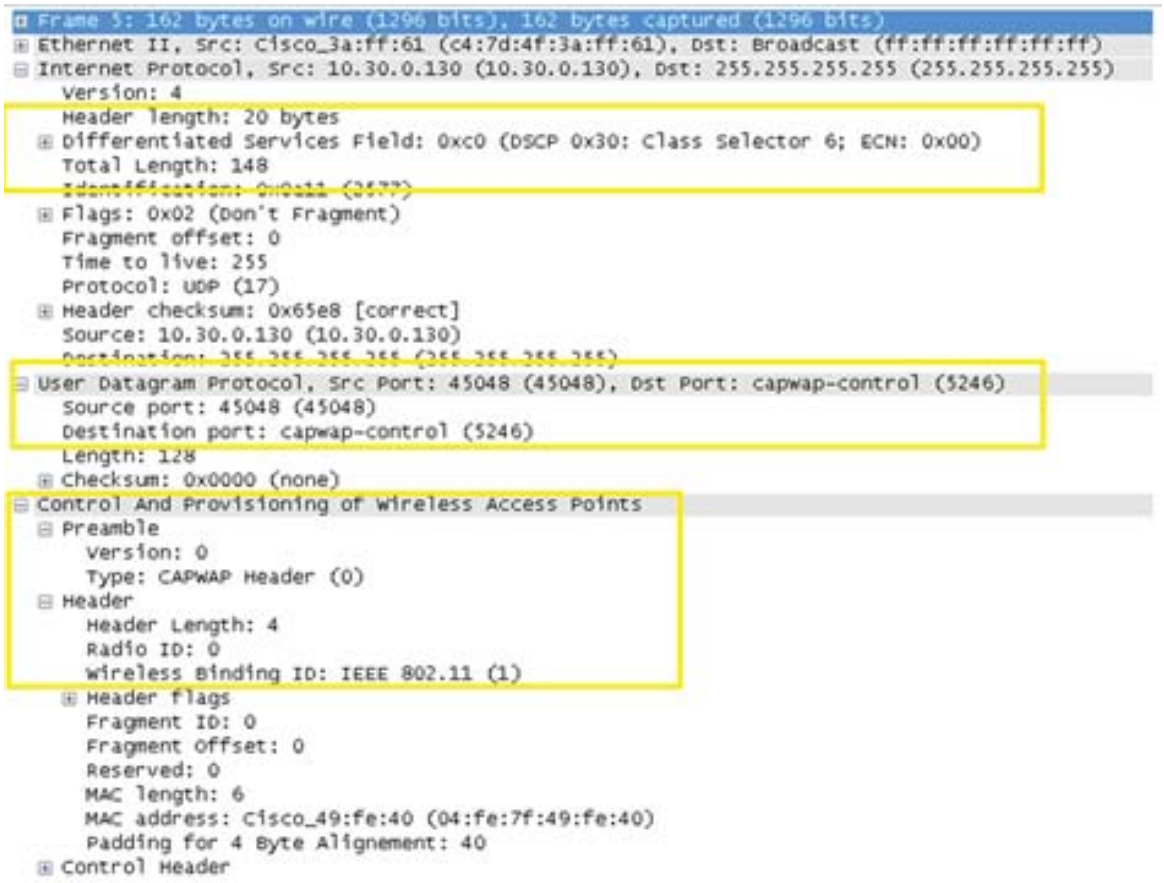
- バックグラウンド トラフィック：WLAN ネットワークのメンバとして動作している CAPWAP AP によって生成されます。たとえば、CAPWAP ハートビート、無線リソース管理（RRM）、不正 AP 測定値などです。バックグラウンド CAPWAP コントロール トラフィックは、CS6 としてマーキングされます。

図 5-24 では、初期 CAPWAP コントロール メッセージの例を示します。初期 CAPWAP コントロール メッセージのリストには、次のものが含まれています。

- CAPWAP discovery メッセージ
- CAPWAP join 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 5-25　WISM-2 での CAPWAP 検出要求



CAPWAP 802.11 トラフィック

CAPWAP 802.11 コントロール 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 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 コントロール 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。これはボーダー ゲートウェイ プロトコル（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 コントロール 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 コントロール トラフィックの負荷に対処する場合のガイドラインとして使用できるルータ設定の例を示します。

この例では、192.168.101.0/24 サブネット上で 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 コントロール トラフィックの DSCP の変更

次の例では、WAN サイトから送られる CAPWAP コントロール トラフィックのレートを制限して、CS6 としてマーキングされたコントール トラフィックがルーティング トラフィックに及ぼす影響を最小化するための設定例を示します。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 コントロール トラフィックが WAN ルーティング プロトコル接続に影響する可能性はほとんどありません。

```
interface Serial0
 ip address 192.168.202.2 255.255.255.252
 rate-limit output access-group 111 8000 3000 6000 conform-action transmit exceed-action
set-dscp-transmit 26
access-list 111 remark 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

CHAPTER 6

Cisco Unified Wireless のマルチキャスト設計

概要

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

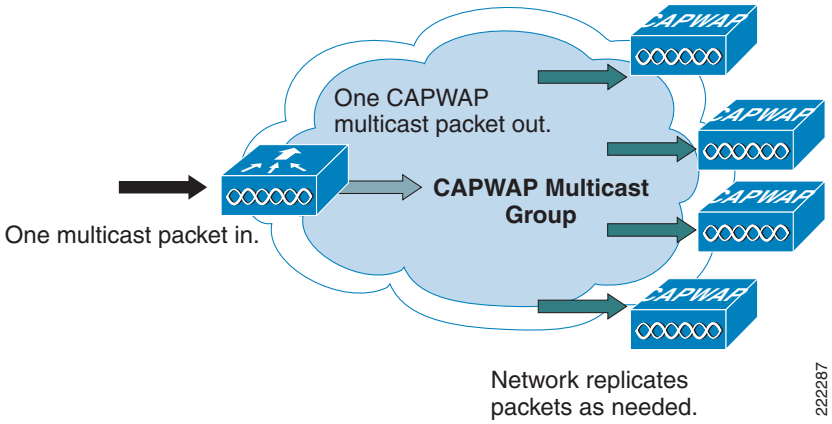
現在、受信先の大規模なグループに宛てた一方向のストリーミングメディア（ビデオなど）には、通常 IP マルチキャストが使用されています。多くのケーブル テレビ局、教育機関、および大企業では、コンテンツの配信のために IP マルチキャストが展開されています。さらに、マルチキャストを使用して音声およびビデオ会議に利用されています。その他、構内および商業ネットワークでマルチキャストが広く使用されている例として、ファイルの配信があります。特に、オペレーティング システムのイメージおよびアップデートをリモート ホストに配信する場合などです。また、金融部門において、株価情報表示および hoot-n-holler 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。

マルチキャスト転送の概要

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

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 の着信 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　　4.1 以前のバージョンでのマルチキャスト転送メカニズム



CAPWAP マルチキャスト グループは実質上、各アクセス ポイントにマルチキャスト パケットを送信するために使用されます。これにより、ネットワーク内のルータは標準のマルチキャスト手法を使用してマルチキャスト パケットを複製し、AP に送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 ルータからの VLAN 上で受信されたマルチキャスト パケットはその種類にかかわらず、HSRP hello パケット、すべてのルータ、EIGRP および PIM マルチキャスト パケットを含め、無線ネットワーク経由で送信されます。

管理者がマルチキャストを有効にして（マルチキャスト モードはデフォルトで無効になっています）、CAPWAP マルチキャスト グループを設定すると、コントローラへの通常の接続プロセス中（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接続し、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 グループに加わるための Internet Group Management Protocol（IGMP）Join 要求が発行されます。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 ステートに対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

- 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、コントローラでは、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 グループに接続されている各アクセス ポイントに配信されます。このときルータでは、マルチキャスト パケットがすべての AP に到達するように、必要に応じて配信時にパケットを複製する通常のマルチキャスト メカニズムが使用されます（図 6-1 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、現在の接続先のコントローラから受信したマルチキャスト パケットだけが処理され、その他のコピーは破棄されます。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。

無線マルチキャスト ローミング

無線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 間の移動時に無線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。

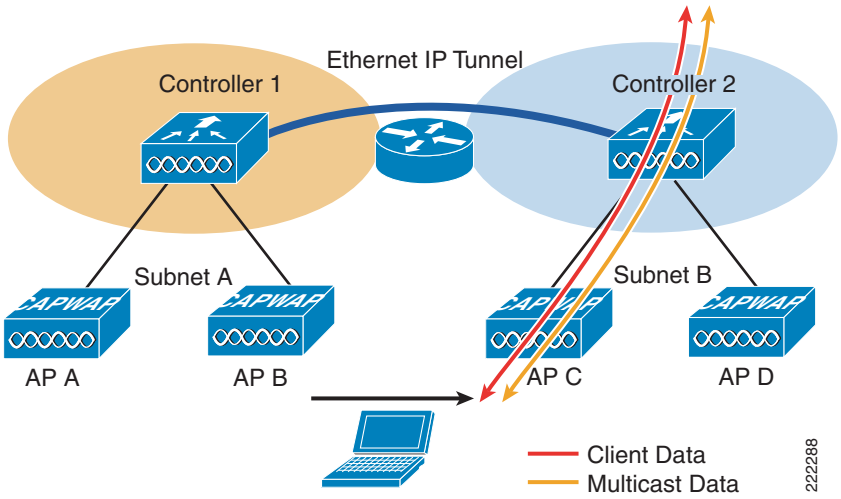
IGMP の基本的な知識は、クライアントのマルチキャスト セッションがネットワーク内を移動するときに何が起こっているかを理解するために重要です。レイヤ 2 ローミングの場合、適切に設定されている外部 AP であればすでにそのマルチキャスト グループに属しており、トラフィックはネットワーク上の別のアンカー ポイントにトンネリングされないため、セッションはそのまま維持されます。レイヤ 3 ローミング環境では仕組みがもう少し複雑で、コントローラに設定したトンネリング モードによって異なっており、ワイヤレス クライアントから送信された IGMP メッセージに影響します。コントローラ上のデフォルトのモビリティ 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 メンバーシップが照会され、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 に関連付けられた外部 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 ストリームに再接続します。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送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

コントローラでは、宛先ポートが 5246、5247、5248 のマルチキャスト グループに送信されるマルチキャスト パケットはすべてブロックされます。また、マルチキャスト グループ アドレスが、コントローラの 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、断片化された 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 断片化と 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、次の手順に従ってください。

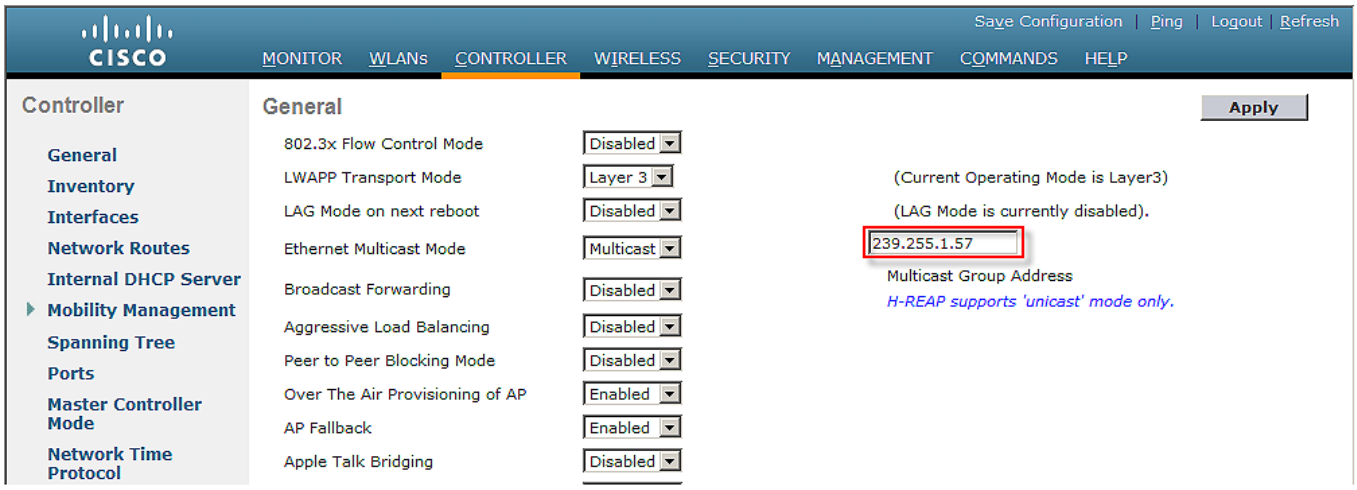
ステップ 1　*マルチキャストが有効なネットワークがある*場合、Ethernet Multicast Mode で [multicast] を選択して、ネットワークでパケットを複製する方法を使用します。

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

ステップ 3　コントローラの全般 Web ページで、CAPWAP トランスポート モードに [Layer 3] が設定されていることを確認します。マルチキャスト パフォーマンス機能は、このモードでのみ動作します。

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

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



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

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

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

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

マルチキャストの配置に関する考慮事項

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無線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

断片化と 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断片化され、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。

これを防止するオプションには次の 2 つがあり、いずれのオプションもそれ自体で効果があります。1 つ目は、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の CAPWAP マルチキャスト グループが同じになる」で、これら 2 つの技術の長所と短所を示します。

図 6-4　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	PRO	CON
すべてのコントローラの CAPWAP マルチキャスト グループが同じになる	追加の断片化保護処理を行う必要がない	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 グループが同じになる

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 予約ポート宛ての着信マルチキャスト パケットをブロックします。予約ポートをブロックすることによって、コントローラはカプセル化された CAPWAP マルチキャスト パケットの断片化パケットの最初の部分をブロックします。ただし、2 つ目のパケットにはポート番号が含まれていないため、2 つ目のパケットは、マルチキャスト グループ アドレス（宛先アドレス）でフィルタするだけでブロックできます。コントローラは、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 グループへ接続するために 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無線マルチキャスト クライアントから送信されているマルチキャスト トラフィックを受信します（送信元アドレスが AP のコントローラの管理アドレスとは異なる場合はドロップします）。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。

（注）　Cisco IOS AP（1240 など）では IGMPv2 を使用し、VxWorks AP（1030 など）では IGMPv1 を使用します。

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 Time To Live フィールドで、**ttl-threshold** コマンドを使用して、Auto-RP の管理用境界を作成していました。この作業は、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、無線 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。

無線クライアント 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、下位の管理用スコープ 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接続できるようになります。

```
mls qos
!
class-map match-all multicast_traffic
  description Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0
  match access-group 101
!
policy-map multicast
 description Rate Limit Multicast traffic to 2.56mps with burst of 12800 bytes
  class multicast_traffic
   police cir 2560000 bc 12800 be 12800 conform-action transmit exceed-action drop
```

```
!
interface Vlan40
 description To Wireless Clients
 ip address 10.20.40.3 255.255.255.0
 ip pim sparse-mode
 ip multicast boundary 1
 ip igmp access-group 30
 standby 40 ip 10.20.40.1
 standby 40 preempt
 service-policy output multicast
!
access-list 1 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
multicast boundary
access-list 1 permit 239.0.0.0 0.127.255.255
!
access-list 30 remark Only Allow IGMP joins to this Multicast Group Range
access-list 30 permit 239.0.0.0 0.127.255.255
!
access-list 101 remark Permit Low Rate Multicast Range of 239.0.0.0 to 239.127.0.0 for
class-map
access-list 101 permit ip any 239.0.0.0 0.127.255.255
```

コントローラの配置がマルチキャスト トラフィック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 は保存できません。マルチキャスト トラフィックが有効になると、トラフィックは HSRP、EIGRP、OSPF、および PIM パケットを含む無線に転送されます。

ここでは、分散型と中央集中型の 2 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/サブネットに接続され、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 に接続されるため、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照会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 に接続されているため、AP 上のマルチキャスト トラフィックの量が軽減されます。WLAN マルチキャスト トラフィックは、WLC の VLAN のクライアント要求によって異なります。表 6-1 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 6-1　中央集中型 WLC 展開および分散型 WLC 展開の長所と短所

導入	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接続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、コントローラに接続されている 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

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 間での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。

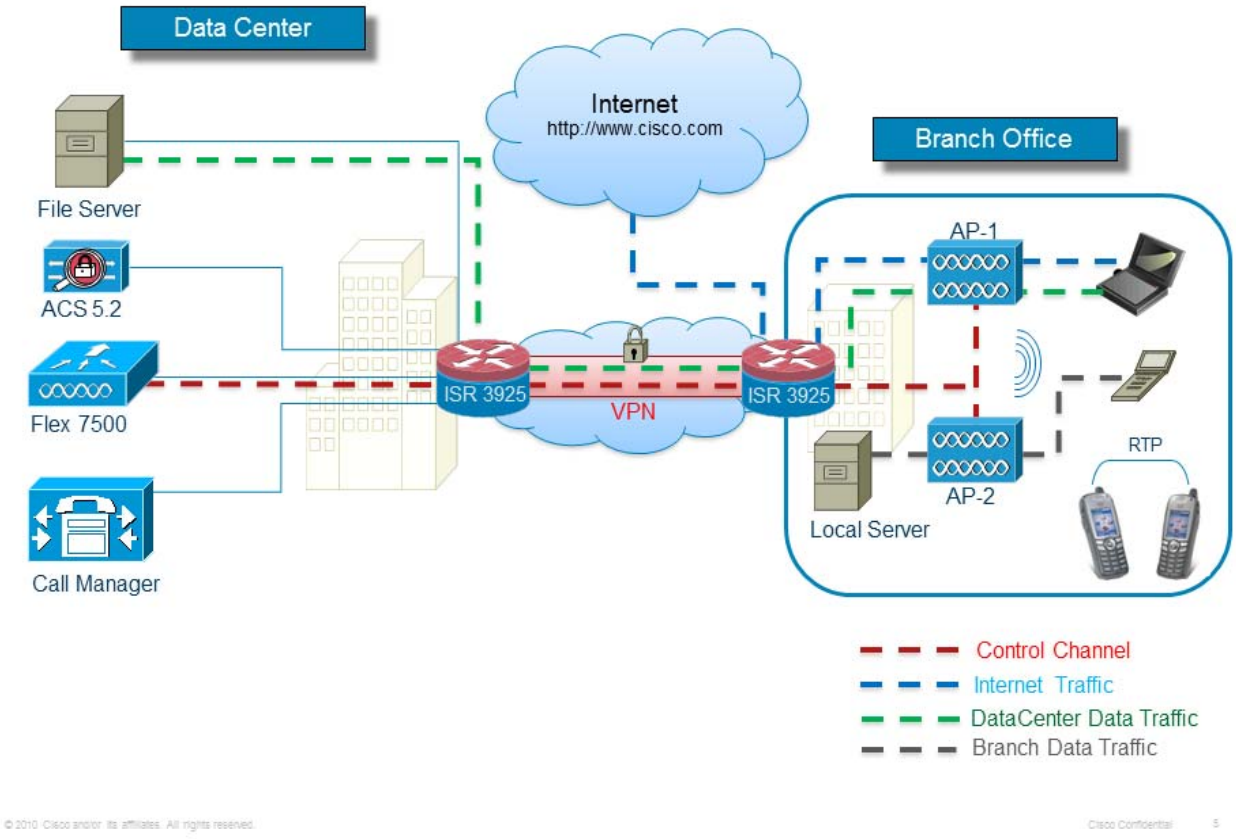
FlexConnect AP を使用すると、WLAN のローカル終端が WLC ではなくネットワーク エッジで可能になり、マルチキャスト動作がそのエッジで制御されます。FlexConnect WLAN が WLC で終端し、マルチキャストがその WLC で有効になっている場合に、FlexConnect ネットワークの場所まで CAPWAP マルチキャストグループを拡張することが許可されているときは、マルチキャストは、その FlexConnect WLAN に配信されます。

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 接続要求を送信できます。

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 のアクセス 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 アーキテクチャ



（注）　FlexConnect 機能マトリクスを表示するには、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。

- 1130AG、1140、1240AG、1040、1250、1260、1600、2600、3600、AP801、3500I、3500E、および AP 1260 アクセス ポイント
- Cisco Flex 7500、Cisco 8500、5500、4400、および 2500 シリーズ コントローラ
- Catalyst 3750G 統合型ワイヤレス LAN コントローラ スイッチ
- Cisco WiSM-2
- サービス統合型ルータ用のコントローラ ネットワーク モジュール
- Cisco 仮想コントローラ

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 台以上の 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を転送します。オフサイト（中央サイト）に送信されるトラフィックは、ブランチのルータによって、標準の IP パケットとして転送されます。AP の制御および管理に関連するすべてのトラフィックは、ワイヤレス アクセス ポイントのコントロールおよびプロビジョニング プロトコル（CAPWAP）経由で別々に中央集中型ワイヤレス LAN コントローラ（WLC）に送信されます。

中央スイッチング

中央スイッチング WLAN は、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、ユーザ トラフィックが WLC 上の動的インターフェイスまたは VLAN にマップされている中央集中型 WLC にトンネリングします。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ブランチ オフィスへの WAN リンクを通じて標準 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 サイトと中央サイト間の WAN リンクが停止した場合などに発生します。

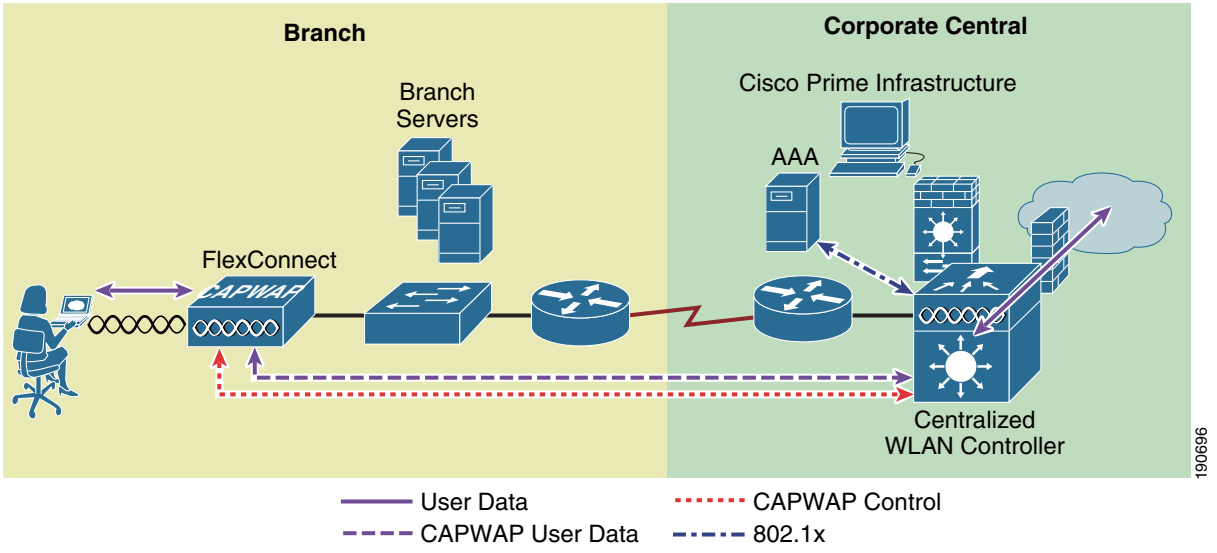
FlexConnect の状態

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



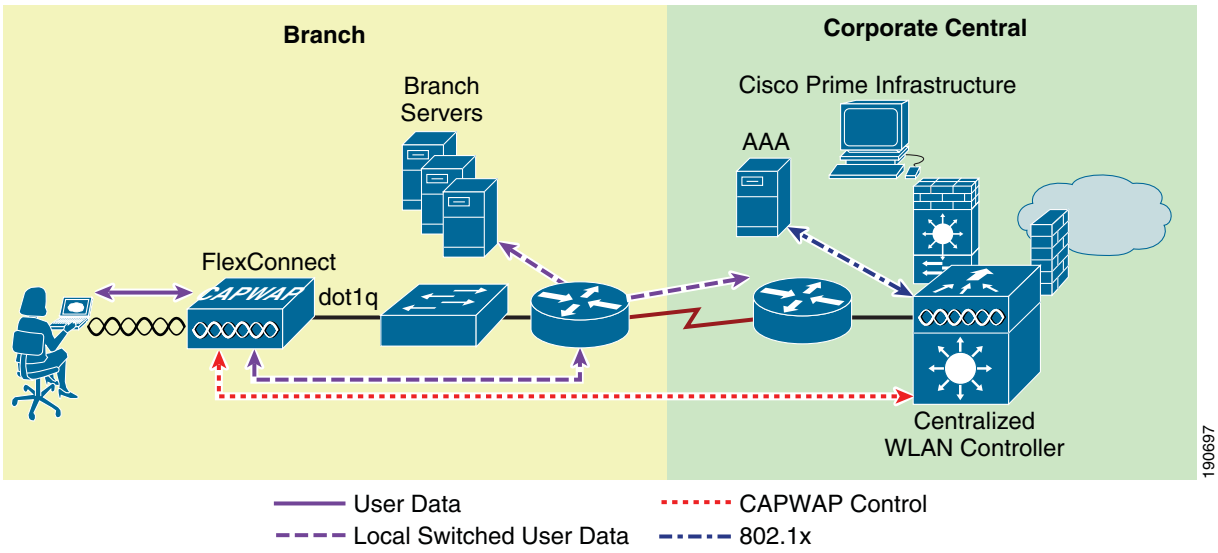
認証ダウン / スイッチング ダウン

中央スイッチング WLAN（上記）は、FlexConnect AP がスタンドアロン モードのときに、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 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。

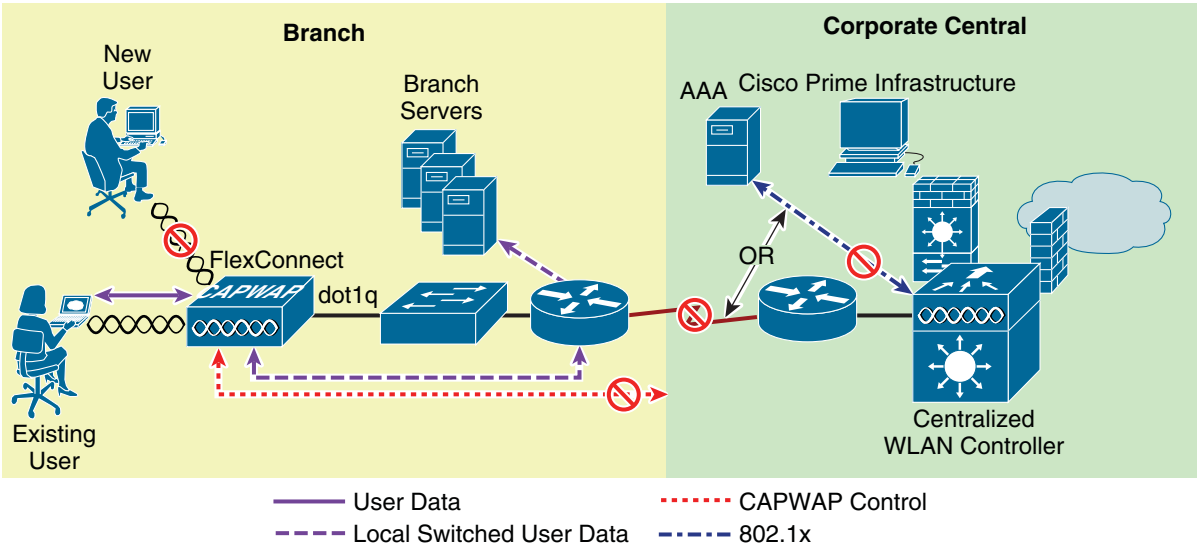
図 7-3　中央認証 / ローカル スイッチング WLAN



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）。

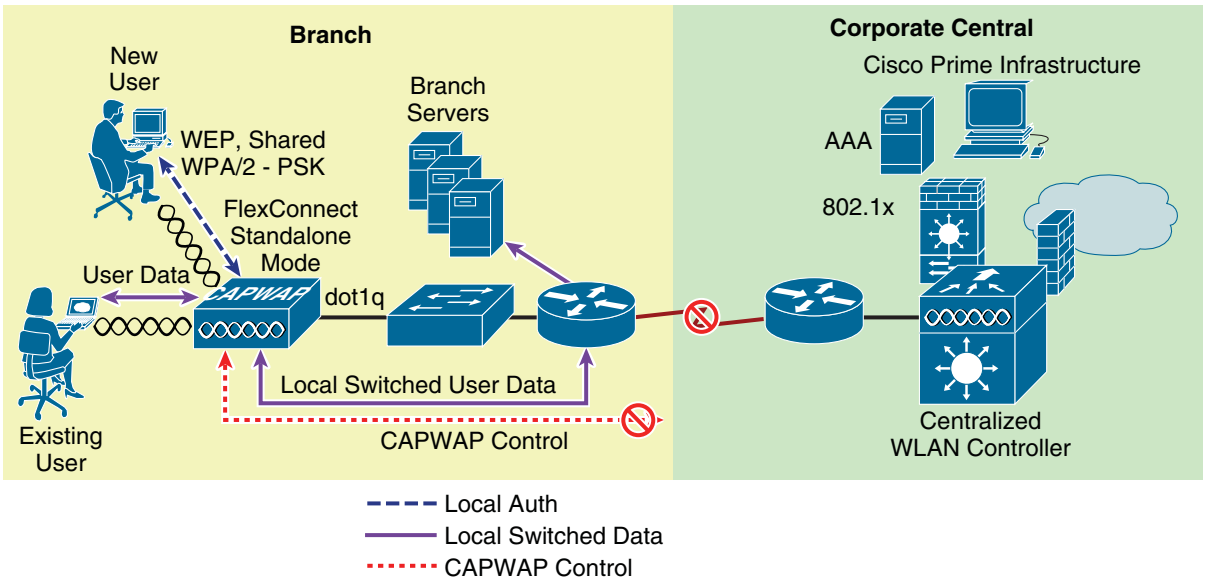
図 7-4　認証ダウン/ローカル スイッチング



ローカル認証/ローカル スイッチング

WLAN がオープン、スタティック WEP、共有、または WPA2 PSK セキュリティ方式を使用している状態です。ユーザ トラフィックはローカルにスイッチングされます。これらのセキュリティ方式だけが、FlexConnect がスタンドアロン モードになったときに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 を使用することができません。

アプリケーション

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

- ブランチのワイヤレス接続
- ブランチのゲスト アクセス
- パブリック WLAN ホットスポット

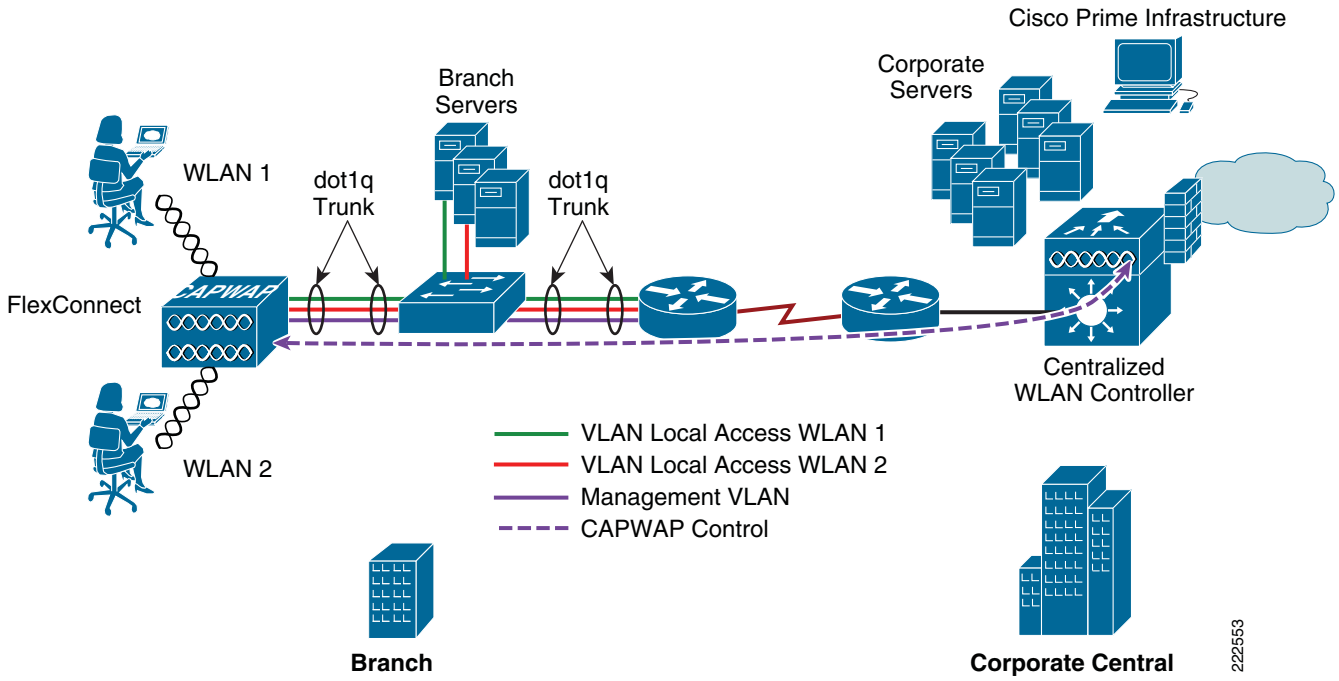
ブランチのワイヤレス接続

FlexConnect は、ワイヤレス ユーザ トラフィックを WAN を経由して中央の 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 コントロール、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 自体は、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

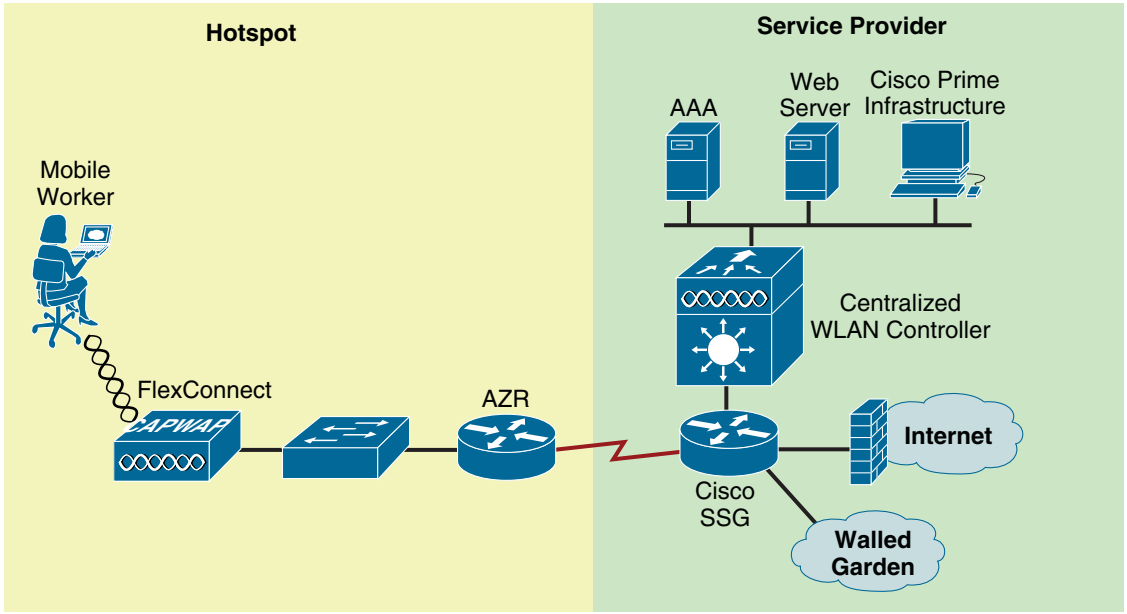


パブリック WLAN ホットスポット

多くのパブリック ホットスポット サービス プロバイダーが複数の SSID/WLAN の実装を始めています。この理由の 1 つは、オペレータが、Web ベースのアクセス用のオープンな認証 WLAN と、より安全なパブリック アクセス用に 802.1x/EAP を使用する別の WLAN を提供することを希望しているためです。

WLAN を個別の VLAN にマップできる 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 に取って代わっています。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



導入に関する考慮事項

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 を予想どおりに機能させるためには、WAN リンク特性に関する次のことに留意してください。

- 遅延：特定の WAN リンクに 100 ミリ秒を超える遅延を与えないように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、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 がスタンドアロン モードに切り替わります（動作モードの定義については、「動作モード」（P.7-4）を参照）。AP 自体は、比較的高い遅延耐性を持っています。ただし、クライアントでは、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。そうでない場合、クライアントは、認証のタイムアウトを待機することになり、それによって、ルーピングなど、その他の予測不可能な動作が発生する可能性があります。
- 帯域幅：所定のロケーションで最大 8 カ所の AP が展開されている場合は、WAN リンクは 128 kbps 以上が必要です。8 カ所を超える AP を展開する場合、比例配分により高い帯域幅が WAN リンクに提供される必要があります。
- 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、AP がスタンドアロン モードのときに、オープン、スタティック WEP および WPA PSK ベースの WLAN など、これらの認証方式を使用するために CAPWAP 接続を必要としない場合にも当てはまります。

- ダイナミック WEP/WPA：これらのキー管理方式の 1 つを使用して 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 展開と同じですが、FlexConnect トポロジ内の動作を除き、WAN 全体にわたるリンク遅延変動が生じる可能性があり、それにより合計ローミング時間に影響する可能性があります。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。

  WLAN が中央にスイッチングされるか、ローカルにスイッチングされるかに関係なく、FlexConnect は PKC をサポートしません。そのため、FlexConnect AP 間をローミングする PKC 対応クライアントは、完全な 802.1x 認証を受けることになります。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なリモート ブランチ ロケーションでは、ローカル WLC（サービス統合型ルータ用の Cisco WLC2100 または NM-WLC）の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、CCKM 対応クライアントのセキュリティ資格情報は WLC にキャッシュされ、モビリティ グループ内の他の AP に転送されます。クライアントが他の AP にローミングおよびアソシエートするとき、その資格情報が AP に転送されるため、2 段階プロセスでクライアントを再びアソシエートして認証できます。これにより、AAA サーバでの完全認証を実行する必要がなくなります。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。
- 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 ルータに対して ARP 要求を実行するまで、クライアントがローミングしたことを認識しません。この動作は、わずかですが、ローミング性能に影響を与える可能性があります。

（注） （所定のローカル スイッチング WLAN 上で）WLAN を異なる VLAN/サブネットにマップする 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 IP アドレスを含むように 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、送信電力制御（TPC）を行うために、最低 4 カ所の 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）トラフィックにローカルで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 タグの dot1p 値をマーク付けします。これはタグ付き VLAN でのみ発生し、ネイティブ VLAN では発生しません。

ダウンストリーム トラフィックの場合、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のフレームにアソシエートされている WMM 値をキューに入れ、マーク付けします。

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

詳細については、第 5 章「Cisco Unified Wireless QoS」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 上で実装することを強く推奨します。適切なプライオリティ キューは、CAPWAP コントロール トラフィックのために予約して、輻輳が原因で接続モードとスタンドアロン モード間を FlexConnect AP が間違って循環しないようにする必要があります。

展開に関する一般的な考慮事項

いずれの WLC 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 合計数によって、FlexConnect AP 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 キャンパス内で AP と同じポリシーを共有せず、各ブランチ ロケーションは、基本的にそれ自体の RF およびモビリティ ドメインです。単一 WLC を複数の論理 RF およびモビリティ ドメインに分割できない場合でも、専用 WLC によって、ブランチ固有の設定およびポリシーを論理的にキャンパスから切り離すことができます。

展開した場合、専用 FlexConnect WLC をメイン キャンパスのものとは異なるモビリティおよび RF ネットワーク名を使用して設定する必要があります。*専用* WLC に接続されたすべての FlexConnect AP は、その RF およびモビリティ ドメインのメンバとなります。

ここでは、auto-RF の観点から、十分な FlexConnect AP が所定のブランチ内に展開されたと想定します（「無線リソース管理」（P.7-11）を参照）。WLC は、各ブランチにアソシエートされている RF カバレッジを自動管理しようとします。

独自のモビリティ ドメインに統合された FlexConnect AP が存在しても、利点（または不都合）はありません。これは、クライアント トラフィックがローカルにスイッチングされるためです。EoIP モビリティ トンネルは、クライアントと FlexConnect AP とのローミングが発生する（同じモビリティ ドメインの）WLC 間で呼び出されません。

専用 WLC が FlexConnect 展開に使用される場合、ネットワークの可用性を確保するためにバックアップ WLC も展開する必要があります。標準の LAP の展開では、指定された WLC とのアソシエーションを強制するために、WLC 優先度を H-REAP に設定する必要があります。

FlexConnect ソリューション

FlexConnect ソリューションでは、次の作業を行うことができます。

- トラフィックの中央集中型制御および管理を行う。
- 各ブランチ オフィスでクライアント データ トラフィックを配信する。
- 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する。

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単一ペイン
- 管理の容易性
- データセンターの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 トラフィックを配信する利点

クライアント データ トラフィックを配信する利点は次のとおりです。

- 完全な WAN リンクの障害発生またはコントローラの使用不能による運用上のダウンタイムなし（サバイバビリティ）。
- WAN リンクの障害発生時のブランチ内のモビリティの復元性。
- ブランチの拡張性の向上。最大 100 カ所の 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。

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非ゲスト クライアントにのみ適用される 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非ゲスト ユーザのレイヤ 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で配信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 認証	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
条件付き 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	外部	許可

Cisco Flex 7500 シリーズ Cloud Controller

Cisco Flex 7500 シリーズ Cloud Controller は、最大 500 カ所のブランチ ロケーションのワイヤレス AP を管理可能です。IT マネージャはデータセンターから、最大 3000 の AP および最大 30,000 のクライアントの設定、管理、およびトラブルシューティングを行うことができます。Cisco Flex 7500 シ

リーズ Cloud Controller は、セキュアなゲスト アクセス、Payment Card Industry（PCI）コンプライアンスのための不正検出、およびブランチ内部（ローカル スイッチング）での Wi-Fi の音声とビデオをサポートします。

Cisco Flex 7500 シリーズ Cloud Controller は、1040、1130、1140、1240、1250、1260、1550、2600、3500、3600、OEAP 600、ISR 881、および ISR 891 の各 AP をサポートします。これらの AP は複数の SSID をサポートします。

表 7-3 では、Flex 7500、WiSM WLC 2、および WLC 5500 シリーズ コントローラ間の拡張性を比較します。

表 7-3　コントローラの拡張性の比較

拡張性	Flex 7500	WiSM-2	WLC 5500
合計アクセス ポイント数	6,000	1000	500
合計クライアント数	64,000	15,000	7,000
FlexConnect の最大グループ数	2,000	100	100
FlexConnect グループあたり最大 AP 数	100	25	25
最大 AP グループ	600	1000	500

動作モード

FlexConnect には、次の 2 種類の動作モードがあります。その内容は次のとおりです。

接続済み：FlexConnect は、その CAPWAP コントロール プレーン（コントローラへの戻り）がアップ状態になっていて、動作しているときに、接続モードにあると見なされます。つまり、WAN リンクはアップ状態になり、期待どおりに動作します。

スタンドアロン：FlexConnect は、コントローラへの戻りの接続がなくなったときにスタンドアロン モードになります。スタンドアロン モードの FlexConnect AP は、電源障害や WAN 障害が発生した場合でも、直前の既知の設定によって動作し続けます。

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。ラウンドトリップ遅延が、データ展開の場合は 300 ミリ秒、データ + 音声展開の場合は 100 ミリ秒を超えない状態で、最小帯域幅の制限を AP あたり 12.8 kbps のままにすることを強く推奨します。（表 7-4 を参照）。最大伝送単位（MTU）は、少なくとも 500 バイトにする必要があります。

表 7-4　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（最大）	ブランチあたりクライアント（最大）
データ	64 kbps	300 ミリ秒	5	25
データ + 音声	128 kbps	100 ms	5	25
モニタ	64 kbps	2 秒	5	該当なし
データ	640 kbps	300 ミリ秒	50	1000

表 7-4　帯域幅の最小値 （続き）

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（最大）	ブランチあたりクライアント（最大）
データ + 音声	1.44 Mbps	100 ms	50	1000
モニタ	640 kbps	2 秒	50	該当なし

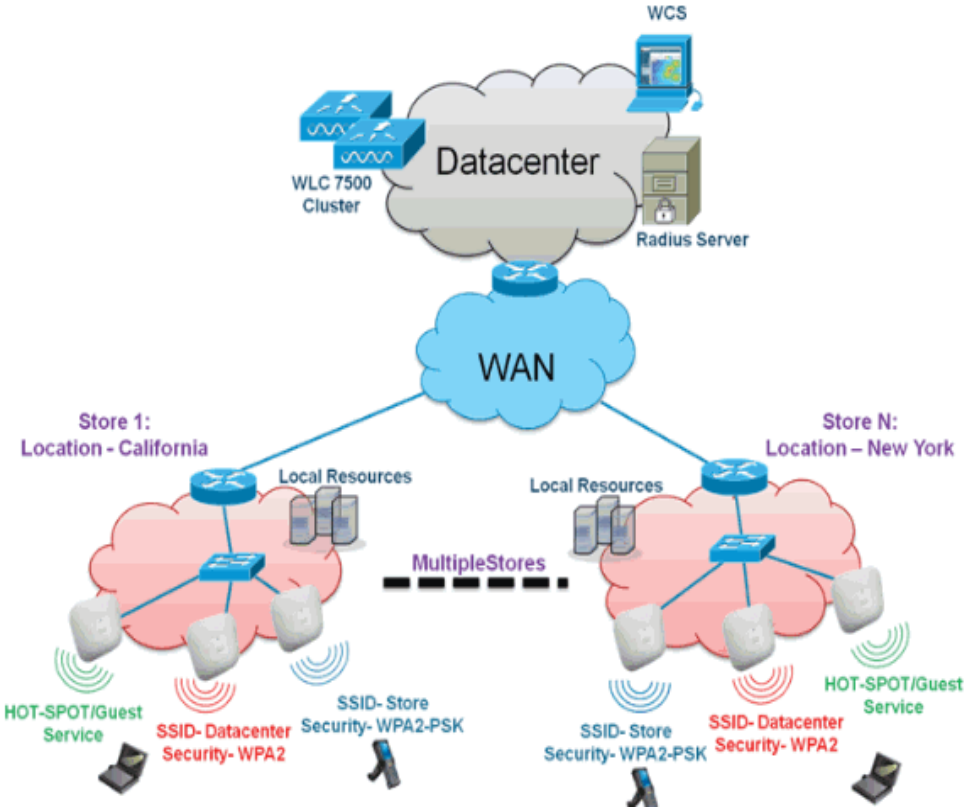
主要な設計要件は次のとおりです。

- 最大 100 カ所の 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。
- 中央集中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

ブランチ ネットワーキング機能とベスト プラクティス

FlexConnect ソリューションは、データセンター内の複雑なセキュリティ、管理、設定、トラブルシューティング処理を仮想化し、これらのサービスを各ブランチに透過的に拡張します。FlexConnect コントローラを使用した展開では、IT の設定、管理がより簡単になりますが、最も重要なことは拡大縮小がより簡単になることです（図 7-8 を参照）。

図 7-8　ワイヤレス ブランチ ネットワークの設計



次の機能とベスト プラクティスが含まれています。

- FlexConnect グループ：ローカル バックアップ Radius、Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミング、ローカル認証の機能を提供します。
- 耐障害性：ワイヤレス ブランチの復元力を高め、運用上のダウンタイムをなくします。
- ELM（Adaptive wIPS 用の拡張ローカル モード）：クライアントにサービスを提供するときに、クライアントのパフォーマンスに影響を与えることなく、Adaptive wIPS 機能を提供します。
- WLAN ごとのクライアント制限：ブランチ ネットワーク上のゲスト クライアントの総数を制限します。
- FlexConnect における AP の自動変換：ブランチの FlexConnect の AP を自動的に変換するための機能。
- ゲスト アクセス：シスコの既存のゲスト アクセス アーキテクチャを FlexConnect で引き続き使用できます。

FlexConnect グループ

各ブランチ サイトの FlexConnect AP は、すべて単一の FlexConnect グループの一部であるため、FlexConnect グループは各ブランチ サイトの構成を簡素化します。

（注）　FlexConnect グループは AP グループに類似していません。

FlexConnect グループは、主に次の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、またはプライマリおよびセカンダリ 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。

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 Store 1 を割り当てます（図 7-8 に示す設定と同様です）。

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。

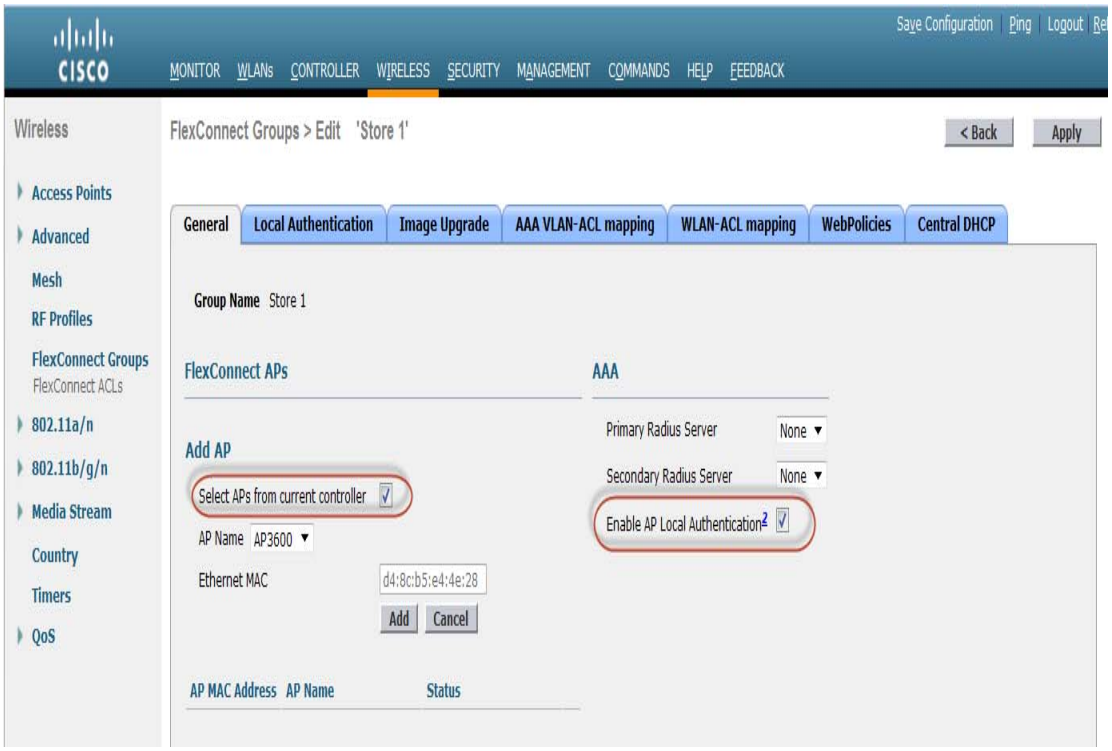
ステップ 5　[Add AP] をクリックします。

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イネーブルにするには、[Enable AP Local Authentication] 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 メニューをイネーブルにするには、[Select APs from current controller] 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 をドロップダウンから選択します。

ステップ 9　AP をドロップダウンから選択した後、[Add] をクリックします。



ステップ 10　ステップ 7 と 8 を繰り返し、この FlexConnect グループ Store 1 にすべての 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] タブ、[Protocols] タブを順にクリックして、[Enable LEAP Authentication] ボックスをオンにします。

ステップ 12　チェックボックスを設定した後、[Apply] をクリックします。

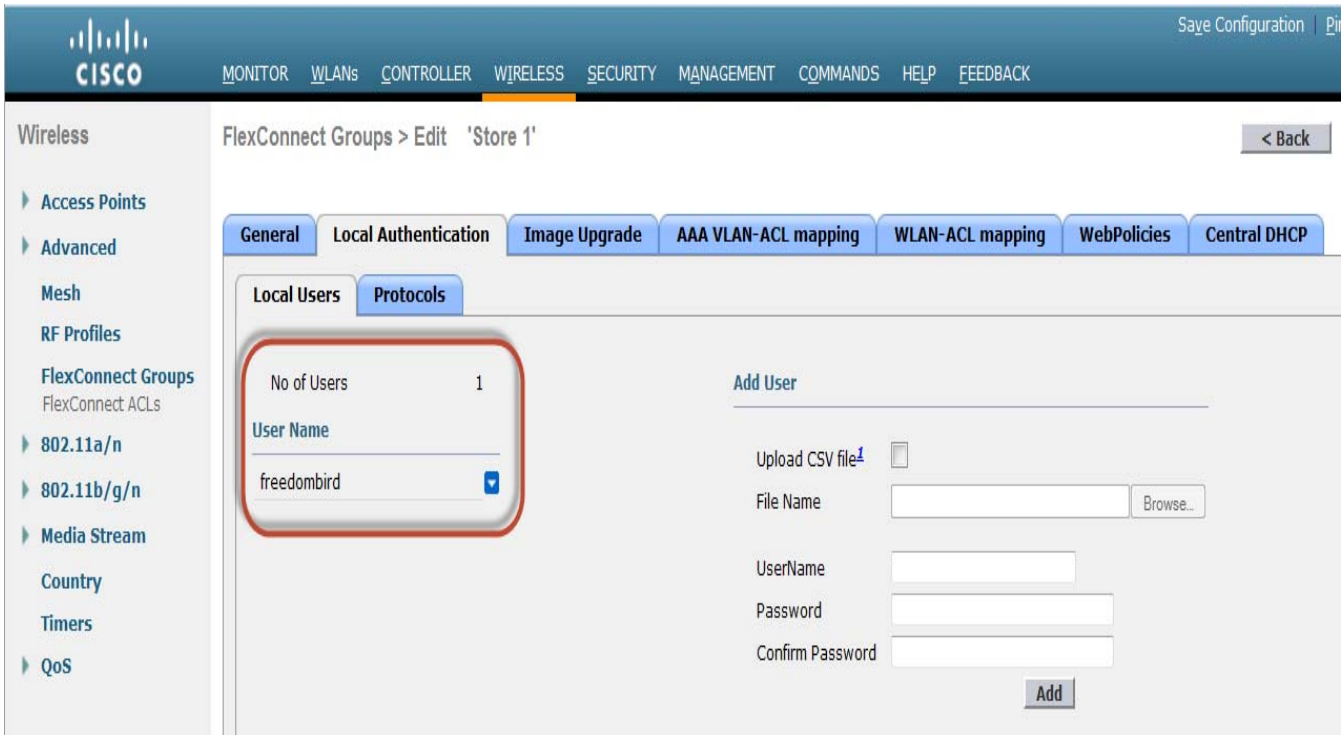
（注）　バックアップ コントローラがある場合は、FlexConnect グループごとに、FlexConnect グループが同じであり、AP の MAC アドレス エントリが含まれていることを確認します。

ステップ 13　[Local Authentication] の [Local Users] をクリックします。

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　ローカル ユーザ名リストがなくなるまでステップ 13 を繰り返します。100 人を超えるユーザの設定や追加はできません。

ステップ 16　ローカル ユーザ情報の入力がすべて完了したら [Apply] をクリックします。ユーザの数を確認します。

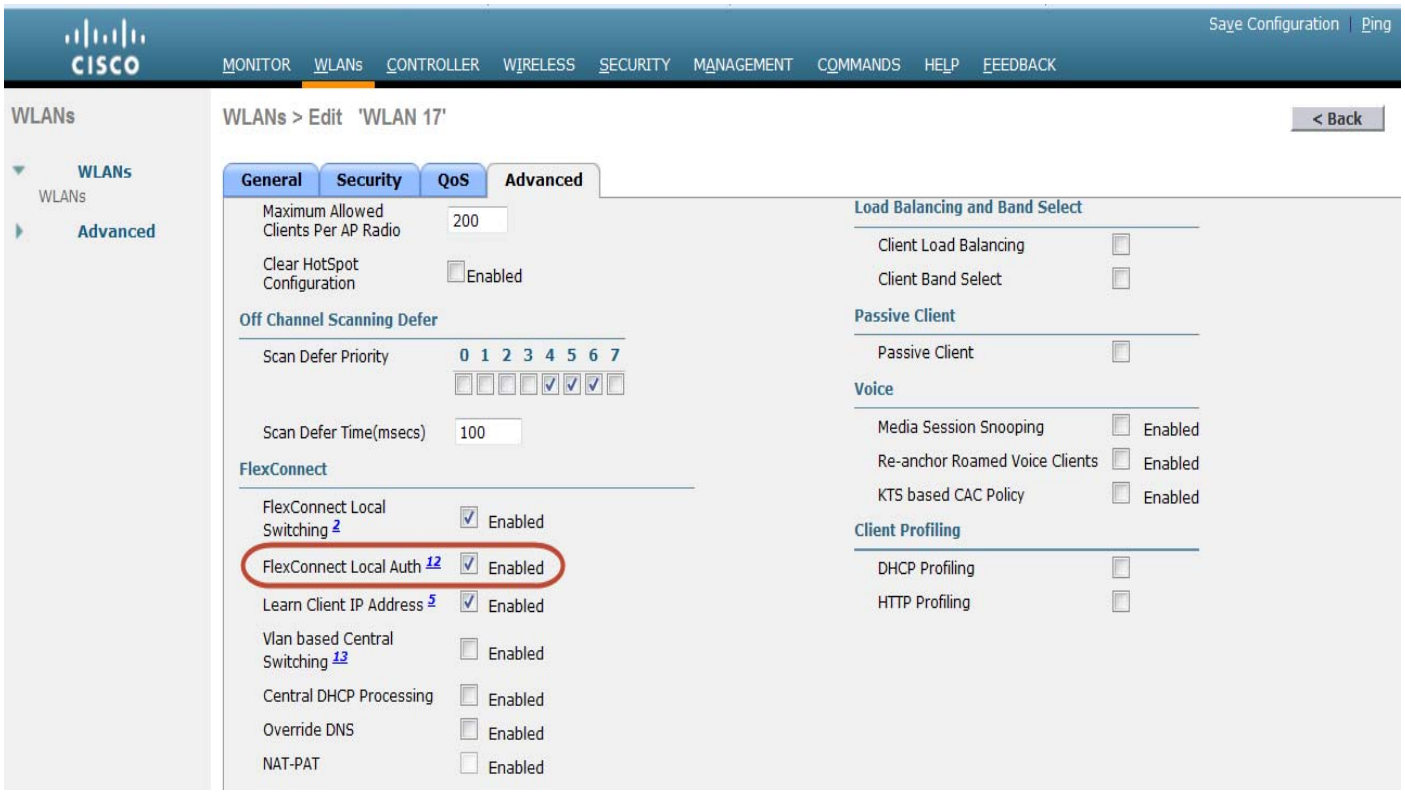


ステップ 17　上部のペインで [WLANs] をクリックします。

ステップ 18　AP グループの作成時に作成された [WLAN ID] の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] の下で、[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イネーブルにするには、[FlexConnect Local Auth] 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した FlexConnect のみでサポートされます。WLAN の下でローカル認証をイネーブルにする前に、必ず FlexConnect グループを作成してください。

CLI を使用した確認

クライアント認証状態とスイッチング モードは、WLC 上で次の CLI コマンドを使用してすばやく確認できます。

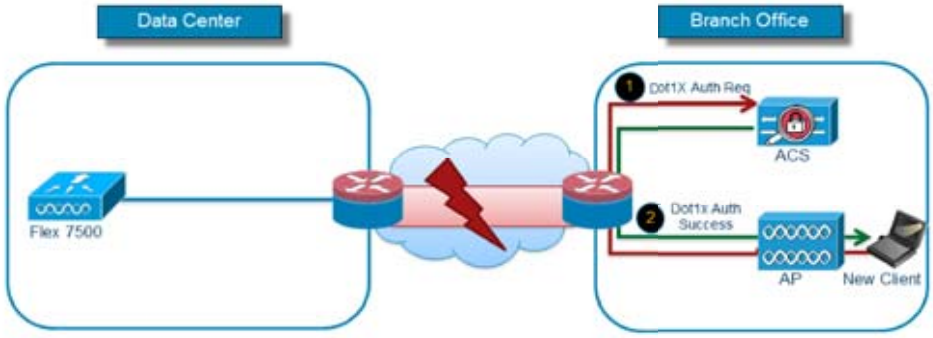
```
(Cisco Controller) >show client detail 00:24:d7:2b:7c:0c
    Client MAC Address.............................00:24:d7:2b:7c:0c
    Client Username................................N/A
    AP MAC Address.................................d0:57:4c:08:e6:70
    Client State...................................Associated
    FlexConnect Data Switching.....................Local
    FlexConnect Authentication.....................Local
```

ローカル認証

図 7-9 に示すように、FlexConnect ブランチ AP がコントローラに接続できない場合でも、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。

言い換えれば、RADIUS/ACS がブランチの中にある場合、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。

図 7-9　　ローカル認証：AP オーセンティケータ



（注）　この機能は、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 グループがバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、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。その後、セカンダリ バックアップ RADIUS サーバを試行し（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。コントローラは、それぞれの FlexConnect アクセス ポイントがコントローラに join すると、ユーザ名とパスワードのスタティック リストをその特定の FlexConnect グループの FlexConnect AP に送信します。グループ内の各 AP は、そのアクセス ポイントにアソシエートされたクライアントのみを認証します。

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際に別のハードウェア デバイスを追加したくない場合です。

CCKM/OKC 高速ローミング

FlexConnect グループは、FlexConnect AP と共に使用する Cisco Centralized Key Management（CCKM）および Opportunistic Key Caching（OKC）高速ローミングで必要となります。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 AP 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。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。

たとえば、300 個の 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して 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。限定されたいくつかの AP からなる FlexConnect グループを作成すれば（たとえば、同じリモート オフィス内の 4 個の AP のグループを作成）、クライアントはその 4 個のアクセス 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 個の AP 間で配布されるのは、クライアントが 1 個の AP 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。

（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あるため、FlexConnect AP 上で特定の WLAN にアソシエーションされたクライアントは、それ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 にアソシエーションする必要があるので、さまざまな制約があります。

7.2 リリースより、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、個別の FlexConnect AP の既存の WLAN-VLAN マッピングを使用するか、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。WLC は、AP でサブインターフェイスを事前作成するために使用されます。

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 について、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 上でイネーブルにする必要があります。
- FlexConnect AP には、ダイナミック 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 から、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（ダイナミック VLAN 割り当て）により、ワイヤレス クライアントが AAA サーバで提供される VLAN に配置されます。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 からマッピングされた VLAN に配置され、トラフィックはその VLAN 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、VLAN が WLC 上に存在する限り、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。

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 コントロールの必要性を満たすメカニズムがあります。FlexConnect ACL を WLC 上で作成し、FlexConnect AP か、AAA オーバーライド VLAN 用の VLAN-ACL マッピングを使用した FlexConnect グループ上に存在する VLAN を使用して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

- コントローラで FlexConnect ACL を作成します。
- 同じことを、AP レベル VLAN ACL マッピングの下で、FlexConnect AP 上に存在する VLAN に適用します。
- VLAN-ACL マッピングの下で、FlexConnect グループに存在する VLAN に適用できます（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

- 最大 512 個の FlexConnect ACL を WLC に対して設定できます。
- 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。
- 最大 16 個の VLAN と 32 個の ACL が FlexConnect AP 上に同時に存在できます。

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、残りのパケットは 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 AP 構成に対するさらなるメリットがあります。

FlexConnect ACL は、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するために、ルールを使用して作成できます。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、残りのトラフィック（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、中央サイトのクライアントにアソシエーションされているサブネットまたは VLAN がローカル サイトに存在しないことを前提としています（つまり、中央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 トンネリング機能は、WAN の帯域幅の使用を避けるために、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ています。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、NAT 操作が実行され、クライアントの送信元 IP アドレスが、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。
- 必要な DHCP を、スプリット トンネリングが設定された WLAN 上でイネーブルに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 ごとか、FlexConnect グループ内のすべての FlexConnect AP に対して、中央の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、これらの設定された WLAN 上のワイヤレス クライアントに送信された場合、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。

耐障害性

FlexConnect の耐障害性を使用すると、FlexConnect AP で次の状態が生じたときに、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です。

- 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 コントローラに切替えるとき。
- プライマリ コントローラとの接続を再確立するとき。

FlexConnect の耐障害性は、ローカル EAP と共に、ネットワーク停止時のゼロ ブランチ ダウンタイムを提供します。この機能はデフォルトでイネーブルになっており、ディセーブルにできません。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

- FlexConnect は、コントローラの設定が変更されない限り、AP が同じコントローラに接続するときにクライアントを切断しません。
- FlexConnect は、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、バックアップ コントローラに接続するときにクライアントを切断しません。
- FlexConnect は、コントローラの設定に変更がない限り、プライマリ コントローラに接続するときに、その無線をリセットしません。

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した FlexConnect のみでサポートされます。
- 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、中央で認証されるクライアントの完全な再認証が必要です。
- 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 ブロック

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。

- [Disabled] : P2P ブロッキングをディセーブルにし、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。
- [Drop] : 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ドロップします。
- [Forward Up-Stream] : 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 上でドロップまたはアップストリーム転送として設定された P2P ブロッキング アクションは、FlexConnect AP でイネーブルにされた P2P ブロッキングとして扱われます。

P2P の制限事項

- FlexConnect では、ソリューション P2P ブロッキング設定を特定の FlexConnect AP または AP のサブセットのみに適用できません。
- 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 にアソシエーション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。FlexConnect ACL は、この制限の回避策として使用できます。

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 はその各有線またはワイヤレス クライアントについて IAPP メッセージを送信し、Flex 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、Flex AP からローカルにスイッチングされます。
- AP がスタンドアロン モードの場合、AP が IAPP メッセージを処理し、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、接続モードに遷移するときに、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遷移するとき、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。WGB の背後にあるクライアントに対する複数 VLAN のサポートは、ローカル スイッチングが設定された WLAN について、FlexConnect AP 上でサポートされていません。
- 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。

注意事項と制約事項

- 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。
- CAPWAP コントロール パケットは、他のすべてのトラフィックに優先する必要があります。
- 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が 300 ミリ秒を達成できない場合は、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含まれています。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、クライアントはシームレスな接続が行われます。
- 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後、AP の無線もリセットされます。
- 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、スタティック 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。
- コントローラの設定は、AP がスタンドアロン モードに移行し、接続モードに戻るまでの時間、変更*しないでください*。同様に、AP がセカンダリ コントローラまたはバックアップ コントローラにフォール バックする場合、プライマリ コントローラとセカンダリ コントローラまたはバックアップ コントローラ間の設定は変更しないでください。
- 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、電流/サポート 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。
- コントローラは、ユニキャスト パケットまたはマルチキャスト パケットの形式でマルチキャスト パケットを AP に送信できます。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 で CCKM 高速ローミングを使用するには、FlexConnect グループを設定する必要があります。
- 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。
- QoS ユーザ単位帯域幅コントラクトは、ローカル モードの中央スイッチング WLAN および AP でのみサポートされます。QoS プロファイルのユーザ単位帯域幅コントラクトは、FlexConnect ローカル スイッチング WLAN ではサポート*されません*。
- ゲスト ユーザ設定は、FlexConnect ローカル スイッチングではサポートされていません。
- 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 ディスカバリ キャッシュ、または 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。

CHAPTER 8

Cisco Wireless Mesh Networking

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

（注） 構成や導入など、Cisco Wireless Mesh Networking の詳細については、『*Cisco Mesh Access Points, Design and Deployment Guide Release 7.3*』を参照してください。URL は次のとおりです。
http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh.html

メッシュ型ネットワーキングでは、Cisco ワイヤレス LAN コントローラ（WLC）との併用で Cisco Aironet 1500 シリーズ屋外メッシュ アクセス ポイント（AP）と屋内メッシュ AP（Cisco Aironet 1040、1130、1140、1240、1250、1260、2600、3500e、3500i、3600e および 3600i シリーズ AP）、および Cisco Prime Infrastructure を採用することで、屋内と屋外の展開の間にスケーラブルな一元管理とモビリティを実現しています。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 AP と Wi-Fi Protected Access 2（WPA2）クライアントの間で高度な暗号化標準（AES）の暗号化を採用することでサポートされています。本書では、屋外ネットワークの設計時に考慮しなければならない無線周波数（RF）コンポーネントの概略についても説明しています。

このマニュアルで説明する機能は、次の製品に該当します。

- Cisco Aironet 1550（1552）シリーズの屋外 802.11n AP
- Cisco Aironet 1520（1522、1524）シリーズの屋外メッシュ AP
- Cisco Aironet 1040、1130、1140、1240、1250、1260、1260、2600、3500e、3500i、3600e、3600i シリーズの屋内メッシュ AP
- Cisco ワイヤレス LAN コントローラのメッシュ機能
- Cisco Prime Infrastructure のメッシュ機能

（注） Cisco Aironet 1505 および 1510 のメッシュ AP は、生産終了のためサポートされていません。

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（AP）は、次の 2 つの方法のいずれかで動作します。

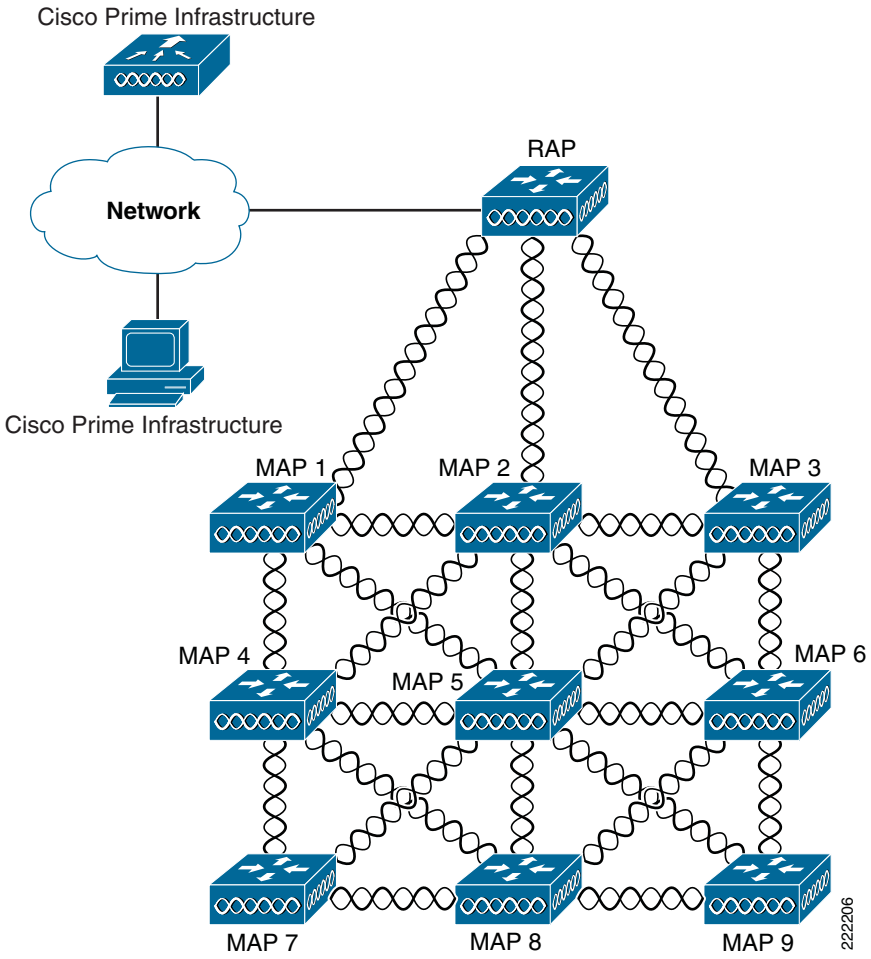
- ルート AP（RAP）
- メッシュ AP（MAP）

MAP はコントローラに無線で接続し、RAP はコントローラに有線で接続します。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 AP を介したコントローラへの最適なパスを決定します。

（注）　すべての AP はメッシュ AP として設定され、出荷されています。Root AP として AP を使用するには、ルート AP にメッシュ AP を再設定します。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 AP があることを確認します。

この図 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 AP のイーサネット ポートで終端します。

メッシュ AP 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 AP 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 AP は、Identity Services Engine（ISE）または証明書付きの拡張認証プロトコル（EAP-FAST）のクライアント認証タイプをサポートする Cisco ACS（4.1 以上）などの RADIUS サーバを使用して、外部から認証できます。

ネットワークのセグメント化

メッシュ AP 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 AP 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 AP から入手できます。このリストでは、AP の各グループでサポートされる 802.11 プロトコルを示します。

- 802.11a/b/g
  - 1130
  - 1240
- 802.11n
  - 1040
  - 1140
  - 1250
  - 1260
- 802.11n+CleanAir
  - 2600
  - 3500e
  - 3500i
  - 3600

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

エンタープライズ 11n メッシュは、802.11n アクセス ポイントで動作するように Cisco Unified Wireless Network 機能に追加された機能拡張です。エンタープライズ 11n メッシュ機能は 802.11n 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。802.11n 屋内 AP は、特定の屋内展開用のデュアル無線 Wi-Fi インフラストラクチャ デバイスです。一方の無線を AP 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。エンタープライズ 11n 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 AP をブリッジ モードに直接指定してオーダーすれば、これらの AP をメッシュ AP として直接使用することもできます。これらの AP がローカル モード（非メッシュ）である場合は、これらの AP 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。特に、展開される AP の量が大きく、AP が従来の非メッシュ ワイヤレス カバレッジに対してローカル モードですでに展開されていると、このシナリオは煩雑になります。

Cisco 屋内メッシュ AP では、次の 2 つの無線が同時に動作します。

- クライアント アクセスに使用される 2.4 GHz の無線
- データ バックホールに使用される 5 GHz の無線

Cisco 屋外メッシュ アクセス ポイント

シスコ屋外メッシュ AP は Cisco Aironet 1500 シリーズの AP で構成されます。1500 シリーズには、1552 11n 屋外メッシュ AP、1522 デュアル ワイヤレス メッシュ AP、および 1524 多重ワイヤレス メッシュ AP が含まれます。1524 には、Public Safety と 1524PS という 2 つのモデルがあります。

（注）　6.0 リリースでは、AP1524SB AP は、A、C、および N のドメインで使用されていました。7.0 リリースでは、AP1524SB アクセス ポイントは -E、-M、-K、-S、-T ドメインでも使用できるようになりました。

Cisco 1500 シリーズ メッシュ AP 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 AP（MAP および RAP）間の通信は、802.11a/n 無線バックホールを介します。一般的に、クライアント トラフィックは、802.11b/g/n 無線（802.11a/n がクライアント トラフィックを受け入れるよう設定することもできます）を介して伝送され、Public Safety トラフィック（AP1524PS のみ）は 4.9 GHz 無線を介して伝送されます。

メッシュ AP は、有線ネットワークに直接接続されていない他の AP の中継ノードとしても動作します。インテリジェントな無線ルーティングは Adaptive Wireless Path Protocol（AWPP）によって提供されます。この Cisco プロトコルを使用すると、各メッシュ AP は、ネイバーを識別し、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数を考慮して各パスのコストを計算することにより、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ます。

AP1500 には、ケーブルモデムありおよびケーブルモデムなしの 2 つの構成モデルがあります。

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

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

AP1500 は、危険な場所用ハードウェア格納ラックに設置できます。危険場所対応の AP1500 は、Class I、Division 2、Zone 2 の危険場所での安全基準を満たしています。

次のモードでは、1520 および 1550 シリーズ AP は非メッシュ モードで動作できます。

- ローカル モード：このモードでは、AP は割り当てられたチャネル上のクライアントを処理できます。180 秒周期で帯域上のすべてのチャネルをモニタ中にも処理が可能です。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 AP 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 と、疑わしい不正クライアントおよび AP の MAC アドレスのリストを渡します。Rogue Detector は ARP パケットを監視します。Rogue Detector はトランク リンクを介して、すべてのブロードキャスト ドメインに接続できます。
- スニファ モード：AP はチャネル上のすべてのパケットをキャプチャし、Wireshark などのパケット アナライザ ソフトウェアを使用してパケットを復号するリモート デバイスに転送します。

Cisco Aironet 1552 メッシュ アクセス ポイント

Cisco Aironet 1550 シリーズの屋外メッシュ AP は、メッシュ ネットワークで使用する目的で設計されたモジュール方式の無線屋外 802.11n アクセス ポイントです。この AP は、ポイントツーマルチポイント メッシュの無線接続およびワイヤレス クライアント アクセスを同時にサポートします。またこの AP は、有線ネットワークに直接接続されていない他の AP の中継ノードとしても動作します。インテリジェントな無線ルーティングは Adaptive Wireless Path Protocol（AWPP）によって提供されます。これにより、AP はネイバー AP を識別し、パスごとに信号の強度とコントローラへのアクセスに必要なホップ カウントについてコストを計算して、有線ネットワークまでの最適なパスをインテリジェントに選択できるようになります。

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

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

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

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

2.4 GHz b/g/n 無線には次の特長があります。

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

5 GHz a/n 無線には次の特長があります。

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

1550 シリーズの AP には次の特長があります。

- 1520 シリーズのモジュール方式をサポートし、無線を柔軟に設定できます。
- 1520 シリーズ AP と完全な相互運用性があります。
- レガシー クライアントとも相互運用性があり、バックホールのパフォーマンスを向上させます。
- AP がローカル モードで設定されている場合は、マルチキャスト VideoStream と HotSpot 2.0 がサポートされます。
- AP1552 は、高品質な VoWLAN コールに対応可能な QoS です。
- 接続されたクライアントに 2.4 GHz から 5 GHz へ移動するように通知する帯域選択がサポートされています。
- AP1552 では、DTLS のサポートにより、ブリッジ モードを除くすべてのサポート対象 AP モードのデータを暗号化できます。
- 5 GHz の無線上で CleanAir をイネーブルにするには、コントローラの GUI で [Wireless] > [Radios] > [802.11a] > [Configure] と移動します。

Cisco Aironet 1522 メッシュ アクセス ポイント

AP1522 メッシュ AP（製品番号 : AIR-LAP1522AG-X-K9、AIR-LAP1522HZ-X-K9、AIR-LAP1522PC-X-K9 2）に、2.4 GHz および 4.9 ～ 5.8 GHz の 2 つの無線が含まれています。2.4 GHz（802.11b/g）の無線はクライアント アクセスに使用し、5 GHz（802.11a）の無線はバックホールとして使用します。7.0.116.0 リリース以降のリリースでは、バックホールに 2.4 GHz を使用できます。この機能は AP1522 にのみ該当します。

5 GHz 無線は、4.9 ～ 5.8 GHz の周波数帯域をカバーする 802.11a 無線で、バックホールとして使用されます。ユニバーサル クライアント アクセス機能がイネーブルになっている場合は、クライアント アクセスにも使用できます。

Cisco 1524SB メッシュ アクセス ポイント

AP1524SB メッシュ AP（製品番号: AIR-LAP1524SB-X-K9 3）には、1 つの 2.4 GHz 無線と 2 つの 5 GHz 無線が含まれています。

2.4 GHz 無線はクライアント アクセス（Public Safety でないトラフィック）用です。2 つの 5 GHz 無線はシリアル バックホールとして機能します（1 つがアップリンク、もう 1 つがダウンリンク）。AP1524SB は線型の展開に適しています。

（注）　6.0 リリースでは、–A ドメイン内の 5 GHz 無線は 5 チャネルの 5.8 GHz 帯域でだけ動作しました。7.0 リリースでは、これらの無線は 5 GHz 帯域全体をカバーします。

各 5 GHz 無線バックホールには別々のバックホール チャネルが設定されます。メッシュ ツリーベース ネットワークでは、ノースバンドとサウスバンドのトラフィック間で同じ共有無線メディアを使用する必要はありません。

RAP の場合、スロット 2 の無線はダウンリンク方向へのバックホールの拡張に使用され、スロット 1 の無線はメッシュではなくクライアント アクセスにだけ使用されます。

MAP の場合、スロット 2 の無線はアップリンク方向へのバックホールに使用され、スロット 1 の無線はダウンリンク方向のバックホールに使用されます。

RAP ダウンリンク（スロット 2）チャネルだけを設定する必要があります。MAP では自動的に、チャネル サブセットからチャネルが選択されます。5.8 GHz 帯域で使用可能なチャネルは、149、153、157、161、および 165 です。

イーサネット ポート

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

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

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

コントローラ CLI では、**show mesh env summary** コマンドを使用してポートのステータスを表示します。4 つのポートの Up または Down（Dn）のステータスは、次の形式で報告されます。

```
port0(PoE-in):port1(PoE-out):port2(cable):port3(fiber)
```

たとえば、次の表示の *rap1522.a380* では、ポート ステータスが *UpDnDnDn* になっています。これは次を意味します。

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

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

1550 シリーズの複数の電源オプション

次の電源オプションがあります。

Power-over-Ethernet（PoE）入力

- パワー インジェクタを使用した 56 VDC（1552E、1552H）
- PoE 入力は 802.3af ではなく、PoE 802.3af 対応イーサネット スイッチでは動作しません

AC 電源

- 100 ～ 480 VAC（47 ～ 63 Hz）：AC または街路灯電源の接続（1552E）
- 100 ～ 240 VAC：AC または街路灯電源の接続（1552H）

外部電源

- 12 VDC：DC 電源ケーブルの接続（全モデル）

内部バッテリ バックアップ（1552E、1552H）

Power-over-Cable（PoC）

- 40 ～ 90 VAC：ケーブル PoC の接続（1552C）

ビデオ カメラなどの IP デバイスに接続するための 802.3af 準拠の PoE 出力（1552E、1552H）

- パワー インジェクタ（PoE-In）を電源として使用する場合は、（PoE 出力）は使用できません

ビデオ カメラなどの IP デバイスに接続するための 802.3af 準拠の PoE 出力（1552E、1552H）

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

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

- AC 電力または PoC 電力
- 外部 12 VDC 電力
- パワー インジェクタ PoE 電力
- 内部バッテリ電力

Cisco ワイヤレス LAN コントローラ

ワイヤレス メッシュ ソリューションは、Cisco 2500、5500、および 8500 シリーズ ワイヤレス LAN コントローラでサポートされます。これらのコントローラについての詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6302/Products_Sub_Category_Home.html.

Cisco Prime Infrastructure

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

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

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

アーキテクチャ

Control And Provisioning of Wireless Access Points

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

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

メッシュ ネットワークの CAPWAP ディスカバリ

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

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

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

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

Adaptive Wireless Path Protocol

Adaptive Wireless Path Protocol（AWPP）は、ワイヤレス メッシュ ネットワー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 AP は、RAP のブリッジ グループ（BGN）の一部である各 MAP 用の RAP に戻る最適なパスを動的に見つけられるようになります。従来のルーティング プロトコルとは異なり、AWPP は RF の詳細を考慮に入れています。

ルートを最適化するため、MAP はネイバー MAP をアクティブに送信要求します。要請メッセージのやり取りの際に、MAP は RAP への接続に使用可能なネイバーをすべて学習し、最適なパスを提供するネイバーを決定して、そのネイバーと同期します。AWPP では、リンクの品質とホップ数に基づいてパスが決定されます。

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

トラフィック フロー

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

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

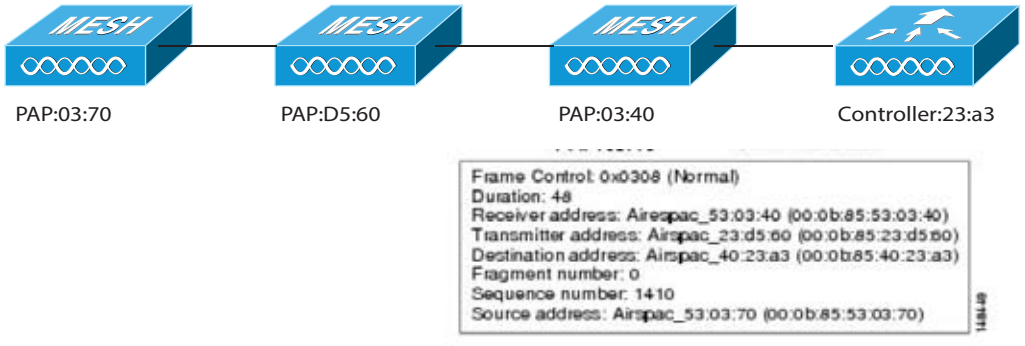
CAPWAP モデルはよく知られており、AWPP は専用プロトコルのため、ワイヤレス メッシュ データ フローについてだけ説明します。ワイヤレス メッシュ データ フローのキーは、メッシュ AP 間で送信される 802.11 フレームのアドレス フィールドです。

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 8-2 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 8-2　　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 AP 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 AP 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。

メッシュ ネイバー、親、および子

メッシュ AP 間の関係は、親、子、またはネイバーです。

- 親 AP 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 AP が選択されます。
- 子の AP は、RAP に戻る最適なルートとして親を選択します。
- ネイバー AP は、他の AP の RF 範囲内にありますが、その容易度の値は親よりも低いため、親や子としては選択されません。

最適な親を選択するための基準

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

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

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

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

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

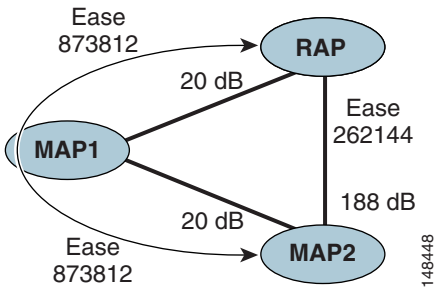
親メッシュ AP は、RAP に戻る最適なパスを提供します。AWPP は、容易度を使用して、最適なパスを判別します。容易度はコストの逆と考えられるため、容易度の高いパスが、パスとして推奨されます。

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 8-3 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 8-3　　親パスの選択



親の決定

親メッシュ AP 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。つまり、次のようになります。

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

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（表示されていません）を使用して通信します。

MAP と RAP の両方共、WLAN クライアント アクセスを提供できますが、RAP の場所がクライアント アクセスの提供には向いていないことがよくあります。3 つすべてのアクセス 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。

ワイヤレス 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。

5 GHz バックホールは、2.4 または 5 GHz 無線をバックホール無線として設定できる 1522 を除くすべてのメッシュ AP で可能です（「拡張機能の設定」を参照）。

ユニバーサル アクセス

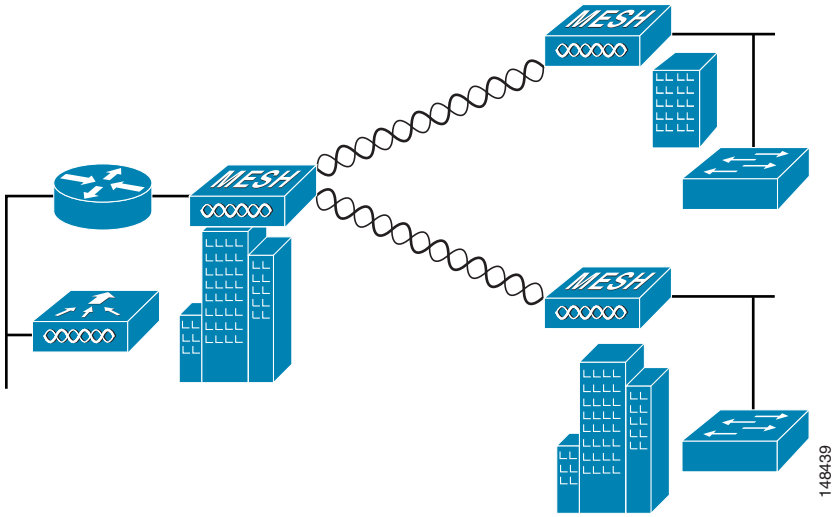
802.11a 無線を介してクライアント トラフィックを受け入れるようメッシュ AP でバックホールを設定できます。この機能は、コントローラの GUI の Backhaul Client Access（[Monitor] > [Wireless]）で識別できます。この機能が無効な場合、バックホール トラフィックは 802.11a または 802.11a/n 無線を介してのみ伝送され、クライアント アソシエーションは 802.11b/g または 802.11b/g/n 無線を介してのみ許可されます。設定の詳細については「拡張機能の設定」を参照してください。

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 8-4 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 8-4　　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 ブリッジングをイネーブルにするには、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。

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 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 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 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）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 カバレッジと必要な 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 1 つのパケットに対して送信される記号の数は、11 Mbps で同じパケットに対して使用される記号の数よりも多くなります。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。シスコの ClientLink テクノロジーは、802.11a/g クライアントが、特にセル境界に近い場合に、最適なレートで動作できるようにすることで、クライアントが混在するネットワークにおける 802.11n の採用に関連する問題を解決します。

高度な信号処理が Wi-Fi チップセットに追加されました。複数の送信アンテナが 802.11a/g クライアントの方向に伝送を収束するために使用され、ダウンリンクの信号対ノイズ比と一定のレンジにおけるデータ レートが増加するため、カバレッジ ホールが減少し、システム全体のパフォーマンスが向上します。このテクノロジーは、クライアントから受信された信号を合成する最適な方法を学習し、この情報を使用してパケットを最適な方法でクライアントに送り返します。このテクニックは、複数入力複数出力（MIMO）ビームフォーミング、送信ビームフォーミング、またはコフェージングとも呼ばれ、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。

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

コントローラの計画

次の項目は、メッシュ ネットワークに必要なコントローラの数に影響します。

- ネットワーク内のメッシュ 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。このネットワークによって、コントローラが、WLAN のパフォーマンスに影響なく、すべての AP から利用できるようになっている場合、AP はすべてのコントローラにわたって最大の効率で等しく分散できます。これに当てはまらない場合で、コントローラがさまざまなクラスタまたは PoP にグループ化されるとき、AP の総数とカバレッジは減少します。
- コントローラごとにサポートされるメッシュ AP（RAP および MAP）の数。

わかりやすくするため、非メッシュ AP をローカル AP と呼びます。

表 8-1　コントローラ モデルによるメッシュ AP のサポート

コントローラ モデル	ローカル AP サポート（非メッシュ）[1]	最大 メッシュ AP サポート
5508[2]	500	500
2504[3]	50	50
WiSM2	500	500

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 の総数です。
2. 5508 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。
3. 2504 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。

（注） メッシュは、Cisco 5508 コントローラで完全にサポートされています。屋内および屋外 AP（AP152X）には基本ライセンス（LIC-CT508-Base）で十分です。WPlus ライセンス（LIC-WPLUS-SW）は、基本ライセンスに含まれます。屋内メッシュ AP には WPlus ライセンスは必要ありません。

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 AP 用

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

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 3500 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、3500、3600）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 および非 Wi-Fi 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 では、空気質指数（AQI）および干渉検出（IDR）というレポートが生成されますが、これらのレポートはコントローラにのみ表示されます。イベント駆動型 RRM（ED-RRM）で実行されるアクションはありません。CleanAir Advisor は、ブリッジ モードの 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、オペレーション的に利点がありますが、その利点は、CAPWAP AP へのリンクのスピードおよびキャパシティ、およびこれらのメッシュ 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 アベイラビリティの増加

「セルの計画と距離」セクションでは、1 平方マイルのワイヤレス メッシュ セルが作成され、組み込まれました。このワイヤレス メッシュ セルは、携帯電話ネットワークの作成に使用されるセルに似た特性を持ちます。より大きなアベイラビリティやキャパシティに対して、同じ物理エリアをカバーするために、（定義された最大セル サイズより）小さいセルが作成される可能性があるからです。このプロセスは、セルに RAP を追加することで行われます。より大きなメッシュ配置と同様、同じチャネルで RAP を使用するか（図 8-5 を参照）、または別のチャネルに置いた RAP を使用するか（図 8-6 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 8-5　同じチャネルでセルごとに 2 つの RAP

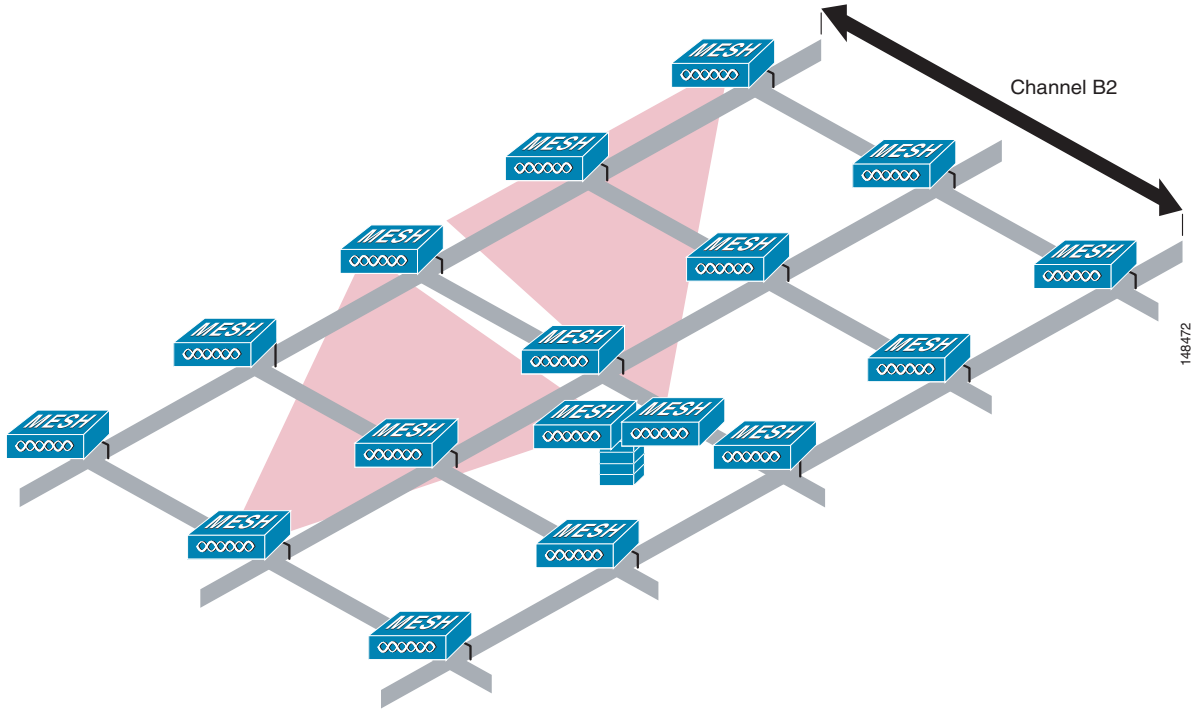
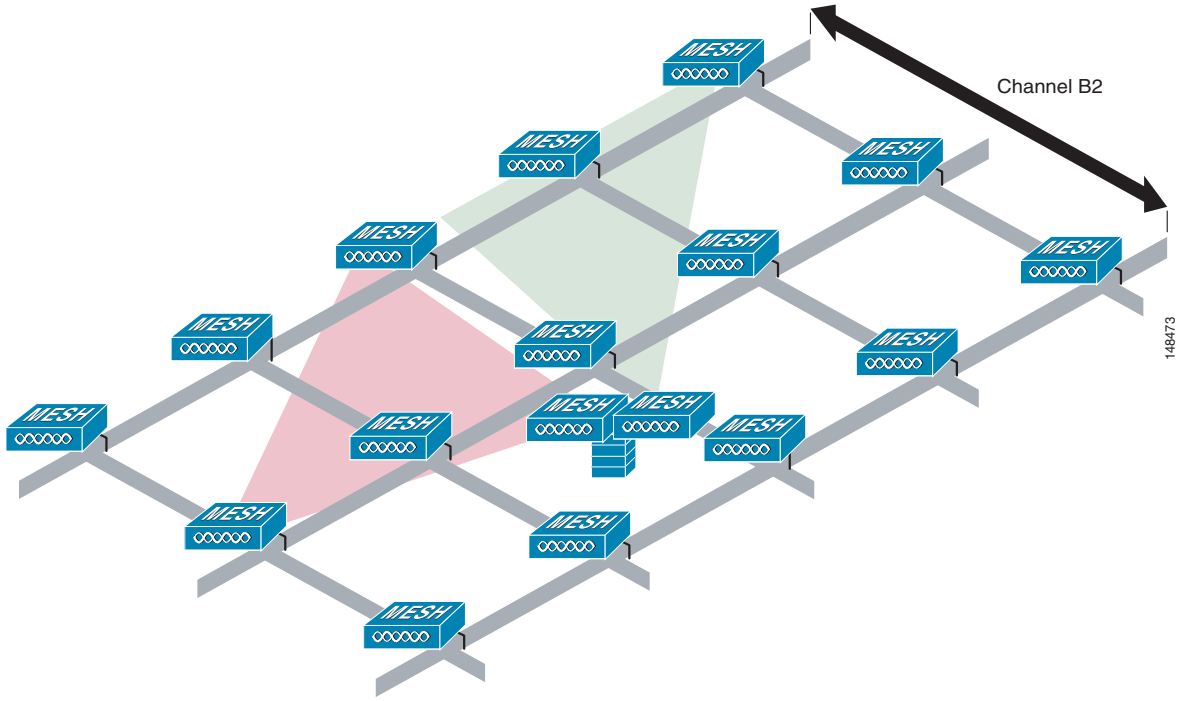


図 8-6　別のチャネルでセルごとに 2 つの RAP



複数の RAP

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

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

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

メッシュ 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、2600、3500e、および 3600 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。

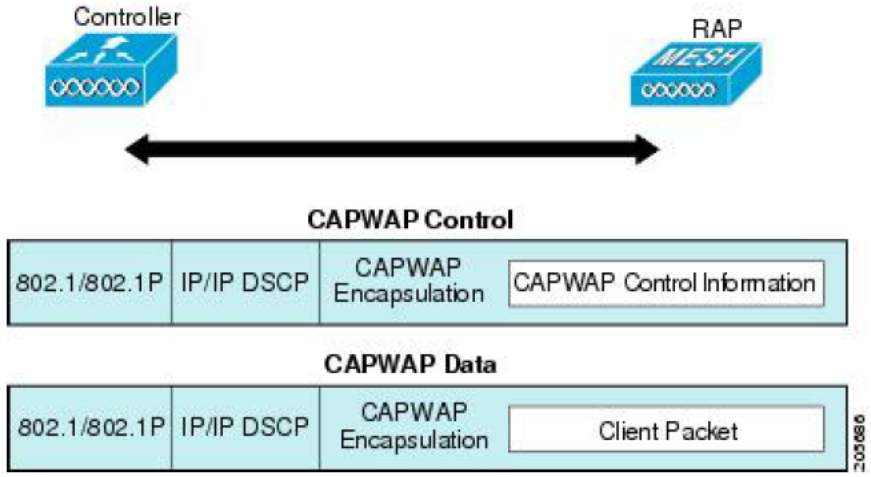
モビリティ グループは、屋外メッシュ ネットワークと屋内 WLAN ネットワークの間で共有できます。1 台のコントローラで、屋内と屋外のメッシュ AP を同時に制御することもできます。同じ WLAN が屋内と屋外の両方のメッシュ AP からブロードキャストされます。

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 8-7 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 8-7　　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。URL は次のとおりです。
http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.3/design/guide/Mesh.html

メッシュ ネットワークへのメッシュ AP の追加

この項では、コントローラがネットワーク内でアクティブで、レイヤ 3 モードで動作していることを前提としています。

（注） メッシュ AP が接続するコントローラ ポートは、タグなしでなければなりません。

メッシュ AP をネットワークに追加する前に、次の作業を行います。

ステップ 1　メッシュ AP の MAC アドレスをコントローラの MAC フィルタに追加します。「MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加」セクションを参照してください。

ステップ 2　メッシュ AP のロール（RAP または MAP）を定義します。「メッシュ アクセス ポイントのロールの定義」セクションを参照してください。

ステップ 3　コントローラでレイヤ 3 が設定されていることを確認します。

ステップ 4　各メッシュ AP のプライマリ、セカンダリ、およびターシャリ コントローラを設定します。バックアップ コントローラを設定します。「バックアップ コントローラの設定」を参照してください。

ステップ 5　外部 RADIUS サーバを使用して、MAC アドレスの外部認証を設定します。「RADIUS サーバを使用した外部認証および許可の設定」を参照してください。

ステップ 6　グローバル メッシュ パラメータを設定します。

ステップ 7　ユニバーサル クライアント アクセスを設定します。

ステップ 8　ローカル メッシュ パラメータを設定します。

ステップ 9　アンテナ パラメータを設定します。

ステップ 10　シリアル バックホールのチャネルを設定します。この手順は、シリアル バックホール AP にのみ適用できます。

ステップ 11　メッシュ AP の DCA チャネルを設定します。

ステップ 12　（必要に応じて）モビリティ グループを設定し、コントローラを割り当てます。

ステップ 13　（必要に応じて）イーサネット ブリッジを設定します。

ステップ 14　イーサネット VLAN タギング ネットワーク、ビデオ、音声などの拡張機能を設定します。

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 ソリューションはソフトフォン アプリケーションで、これらのアプリケーションは一部のハードウェアやオペレーティング システム プラットフォームで使用できます。Cisco Jabber™ 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、ノート PC 用 Jabber の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、次の URL をご覧ください。http://www.cisco.com/web/products/voice/jabber.html

アンテナに関する考慮事項

VoWLAN の多くのネットワーク要件は、アンテナの選択など、WLAN の計画全般にわたって影響を及ぼします。アンテナに関する主な考慮事項は次のとおりです。

- アクセス ポイント（AP）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の天井マウント 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。また、アンテナの放射部分をオープン スペースに配置するため、信号の伝搬と受信を最も効率的に行うことができます。複数のアンテナを内蔵した Cisco AP は設置方法が最も簡単な上、内蔵アンテナにより、大半のインストールに適した下り信号の伝播の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 Multiple Input Multiple Output（MIMO）デュアル バンド、複数エレメント全方向性アンテナとパッチ アンテナを発売しています。これらの複数エレメント アンテナは、最大比合成（MRC）と ClientLink という Cisco AP のテクノロジーを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）クライアント電話パケットを、より強力な単一の信号に結合します。結合された信号では、伝送される電話機のパケットと、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 レートを軽減することです。Cisco の AP では、複数のアンテ

ナと 802.11 ClientLink ロジックを使用して、クライアント電話機に高エネルギー 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。

Cisco では、すべてのアンテナを金属などの高反射面から波長 1 ～ 2 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の間の 1 つまたは複数の波長を分離することにより、AP 無線では送信される電波の受信感度が向上し、無線送信時のヌルの生成を減らすことができます。802.11g/n と 802.11a/n/ac 仕様で使用されている Orthogonal Frequency Division Multiplexing（OFDM）により、リフレクション、ヌル、およびマルチパスに関する問題が軽減されます。ただし、アンテナを適切に配置し、適切なタイプのアンテナを使用すると、より良好な結果が得られます。天井タイルそのものが、天井の上部領域に伝送されカバレッジ 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、次の IEEE レポートをお読みください。

http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=1406225

ClientLink の詳細については、ビーム形成に関する次の IEEE レポートをお読みください。

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4558648&tag=1

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、1 つのタイプですべての用途と場所に適したものはありません。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。URL は次のとおりです。

http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html

シスコでは、ダイポール アンテナを同じ外部アンテナからデュアル（2.4 GHz および 5 GHz）帯域サポートの AP に接続する際に、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）のサポート。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、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ついています。

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、すべて増加を単一の空間ストリームの 802.11n スマート フォンを使用した場合の、カバレッジ セルの全体的なスループットが 2 Mbps 増加します。

一般的な推奨事項

最適な Wi-Fi カバレッジ セルの帯域幅とクライアント アプリケーションのパフォーマンス（あらゆる形式のダイポール アンテナ タイプの場合）のため、シスコでは次のことを推奨します。

- 各 AP 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 に接続されたすべてのアンテナ同士の距離を 2 波長以内にする

AP およびそこ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。これらの推奨事項に従ったアンテナ システムを使用して、そのテクノロジーと AP ハードウェアへの投資を最大限に活用してください。

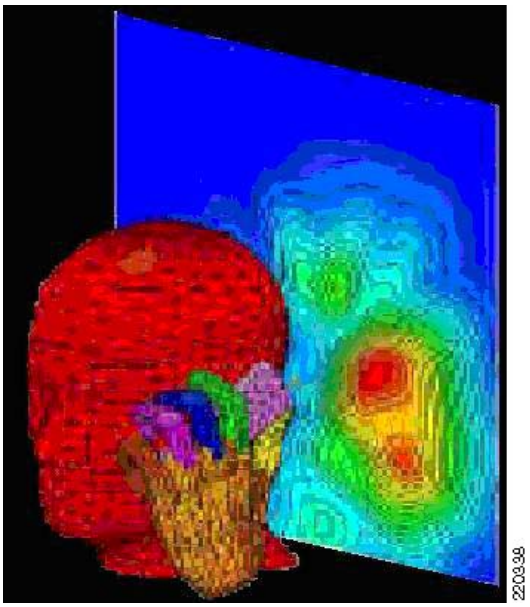
ハイ ゲイン アンテナは信号を水平面に拡散させ、これにより、多くのノイズを拾う大規模セルが作成されます。この結果、信号対雑音比（SNR）が低くなり、パケット エラーの比率が高まります。SNR は次の条件によって定義されます。

- 信号：ある無線から送信され、中断されずに他の無線が受信できる放射エネルギー。すなわち、Wi-Fi では、送信無線によって、受信無線がデコード可能な 802.11 プロトコルのパケットが送信されます。
- ノイズ：受信無線の周波数範囲内の送信エネルギーのうち、その無線でデコードできないもの。

プロトコル パケットとバックグラウンド ノイズ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、高い音声コール キャパシティを維持しつつ、最も低いパケット エラー レートの作成が行われます。

ハイ ゲイン アンテナを使用すると、カバレッジ 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、人間の頭と体が 5dB の信号を減衰させるため、壁面マウント パッチよりも天井マウント アンテナが推奨されます（図 9-3 を参照）。天井マウント アンテナは、多くの壁面マウント アンテナよりも人間の頭と体による減衰を防ぐように、適切に配置されます。

図 9-3　　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。懐中電灯のリフレクタによって電球から放射される光の焦点が合わせられるのと同じです。

WLAN RF 計画の詳細については、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 4dB の信号減衰が起こることがあります。手でアンテナを覆って頭で電話を支えた場合には、9dB の信号減衰が起こることがあります。一般的に、屋内での展開の場合は信号が 9dB 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 コンピュータのゲインは 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、タブレットおよびノート PC 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。スマートフォンやタブレット、ラップトップと AP 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。

チャネル使用率

802.11、802.11b、802.11g、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必要となります。この相互運用性によって、802.11 保護プロトコル ロジックの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 Wi-Fi 帯域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ほかにも多数あります。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使用されていません（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、レーダーが存在しないことが重要となります。したがって、シスコではいずれかの新しいサイトで追加テストを実施し、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確認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、その AP は 200 ミリ秒以内に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 の標準チャネル使用率

Cisco Unified Wireless Network をインストールする前に、チャネル干渉および、AirMagnet や Wild Packets、Cognio などのツールの使用に関して、サイトをテストする必要があります。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*レポートは、次のスペクトルの確認を提供します。

- 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、パケットを送信する前にオープンなタイム 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、無線パケット化されたアロハ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、シスコでは、従来のデバイスがクライアントの構成に含まれていない場合、クライアントを 5 GHz に移動して、2.4 GHz の構成から従来の 1 Mbps および 2 Mbps のデータ レートを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 Federal Communications Commission（FCC）、European Telecommunications Standards Institute（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標準を定めています。5 GHz 帯域の一部は、現在（過去においても）、気象レーダーなど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、FCC は 5.470 ～ 5.725 MHz 帯域をライセンス不要の用途に開放しました。これらの周波数が使用可能になったことにより、*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、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コールの品質に影響する場合があるため、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、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。Spectrum Expert の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/ps9393/index.html

5 GHz 帯域のチャネル

DFS 要件には、従来の UNII-2 チャネル（52 ～ 64）と、8 つの新しい W56 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

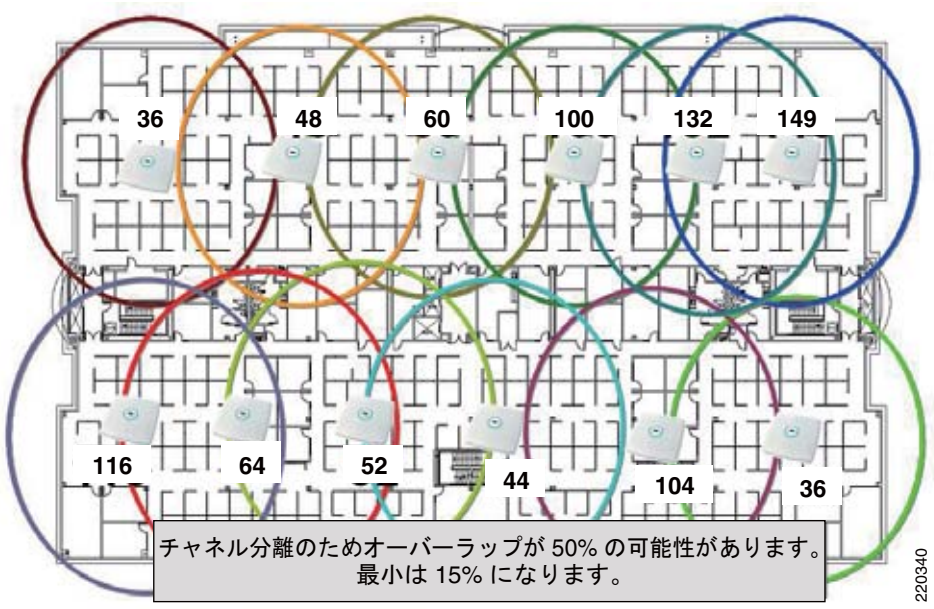
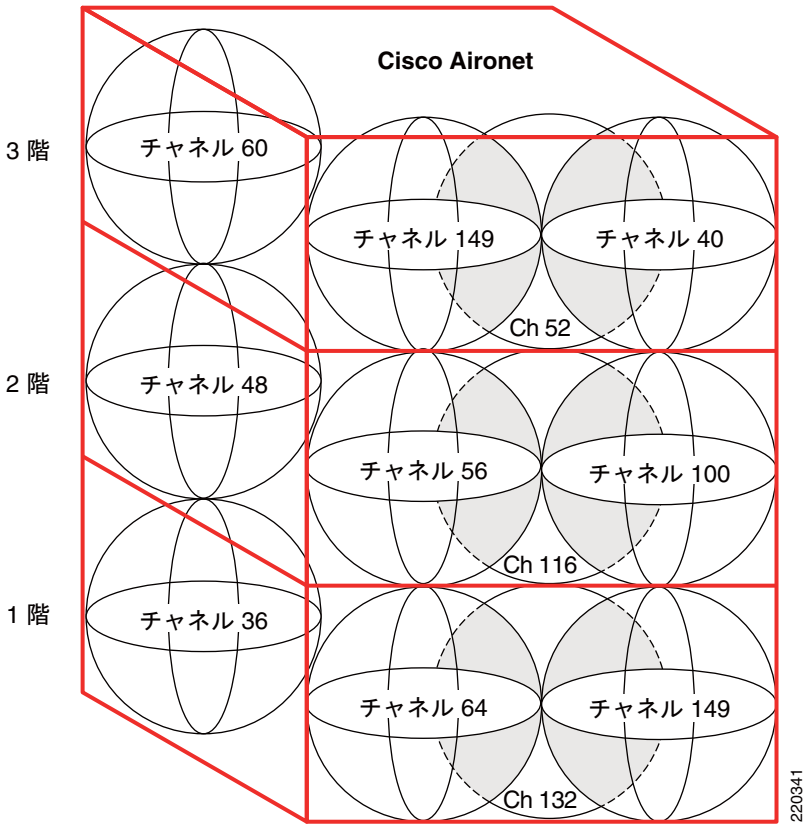


図 9-6 で示すとおり、複数フロア設計では、フロア間で垂直にチャネルを分離して、チャネル相互の干渉を減少させることができます。

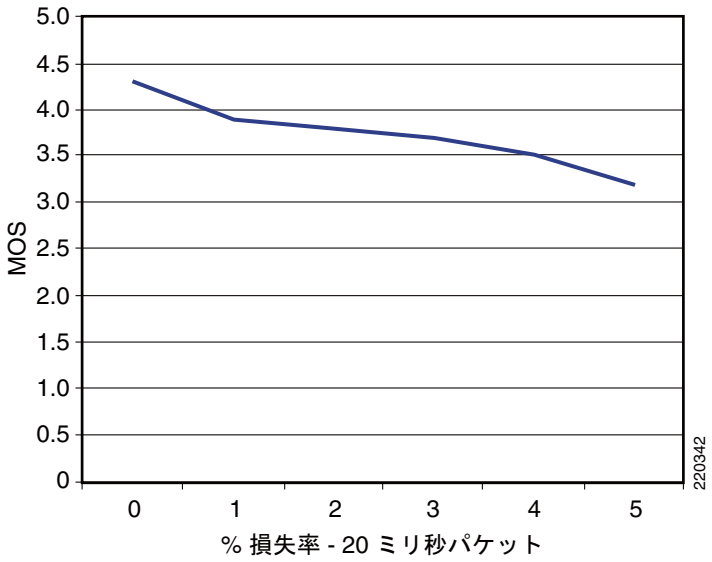
図 9-6　垂直チャネル分離



コール キャパシティ

Wi-Fi チャネルのコール数は、いくつかの要因によって制限されます。まず、AP および VoWLAN クライアントによって使用される RF スペクトラムは、シールド ツイストペア CAT 5 ケーブルなどの電磁干渉からシールドできません。Wi-Fi でセグメンテーションに最も近いのは、チャネル分離です。802.11 のオープンな共有 RF スペクトラムは、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



802.11a では、802.11g と同様、最も低いデータ レート（6 Mbps）によって最も高いカバレッジ範囲が実現します。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、スピーチの質が*一部のユーザにとって満足できる*レベルになった例を示しています。

電話のカバレッジ エリアの境界は、そのカバレッジ エリアの MOS が*非常に満足である*というカテゴリに当てはまる場所です。本書では、カバレッジ エリアの境界を*セルの境界*と呼びます。複数の電話クライアントやデータ クライアント同士の干渉や相互チャネルの干渉、その他の説明のつかない干渉が発生する可能性があるため、音声に対しては、パケット エラー レートが 1% のセルの境界が必要です。セルの境界およびカバレッジ設計については、この章の他のセクションで詳しく定義されています。

802.11 および 802.11b で従来の 2.4 GHz Wi-Fi クライアントをサポートする必要がない場合は、1、2、5.5、および 11 MHz のレートを無効にすることを推奨します。

これらのレートが無効な場合、1 つ以上の 802.11g データ レートを *required* 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。可能であれば、802.11b/g を組み合わせたネットワークよりも 802.11g のみのネットワークが推奨されます。ほとんどのデータ クライアントおよび電話クライアントは、AP からビーコンとプローブ応答でアドバタイズされたデータ レートを認識します。したがって、クライアントは、AP によってアドバタイズされた必須データ レートで、管理、制御、マルチキャスト、およびブロードキャスト パケットを送信します。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。無線受信器は、AP または電話機のいずれかです。SNR はリンクの両方の無線で同じではありません。SNR とマルチパス干渉は、AP およびセルの境界で考慮する必要があります。パス損失は、リンクの両端で同じであると想定できます。

音声アプリケーションに対しては、実際の電話機を使用して、希望するデータ レートでセルの境界を設定することを推奨します。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 リアルタイム転送プロトコル（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、自律 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の境界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、ノート PC 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 の電話のセルの境界の 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

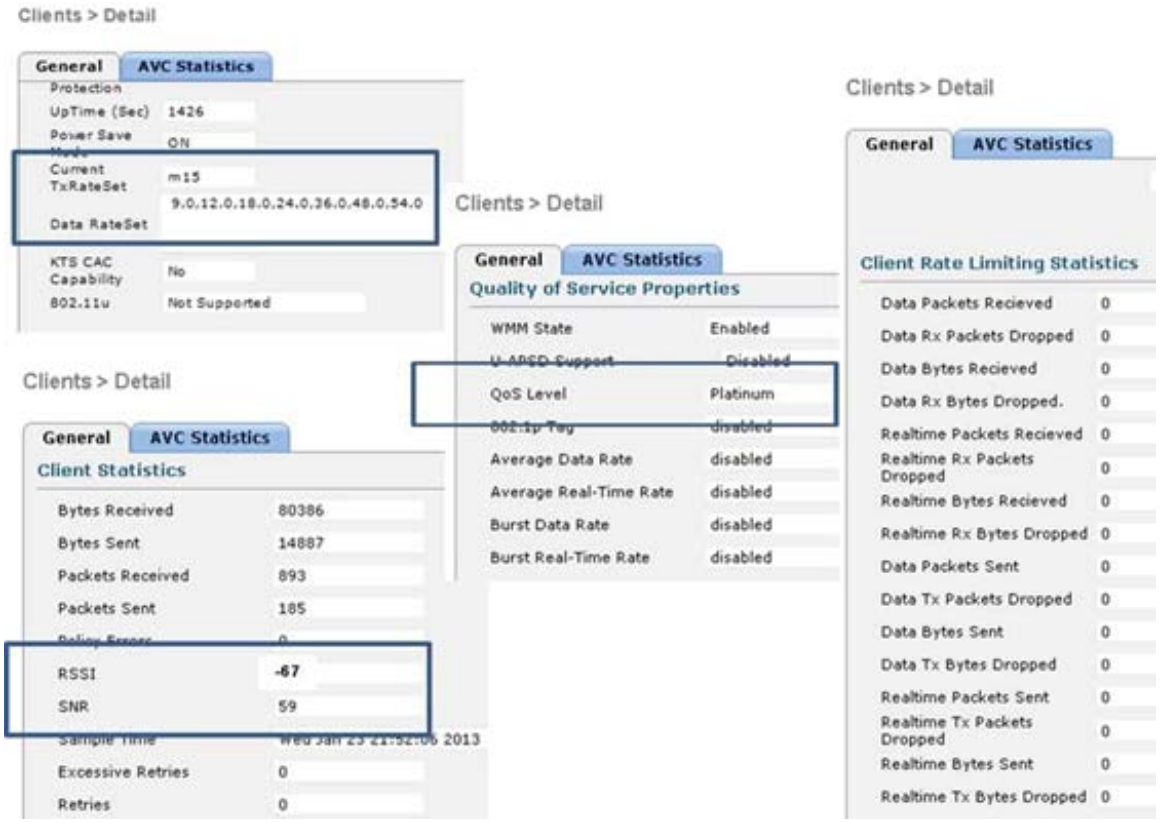
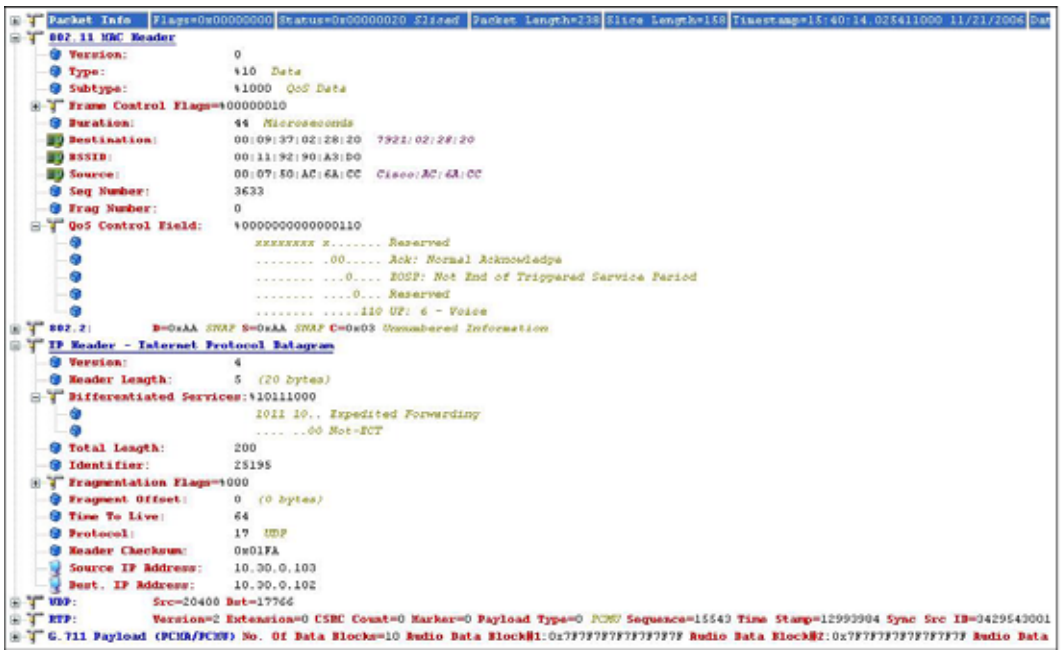


図 9-9 では、デコードされた G.711 オーディオ RTP パケットを示します。Cisco 7960 固定電話から発信されたこのパケットは、AP から VoWLAN のエンドポイントへのダウンストリームです。Over-the-Air QoS マーキングは、802.11e 仕様に従い、QoS ベースライン マーキング 5 からユーザ プライオリティ 6 に変更されます。Cisco 電話のコール統計は、電話機で見ることができます。また、電

話機の IP アドレスを使用して電話機を参照しても見ることができます。セルの境界の 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が効率化されます。

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。パケットは、前のパケットより 5dB 高いか、低い可能性があります。所定の測定場所での平均値が算出されるまでに数分かかることがあります。

AP コール キャパシティ

VoWLAN 展開の計画プロセスの鍵となる部分が、AP ごとの同時音声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 つの電話の間のコールは、2 つのアクティブな音声ストリームとみなされます。

AP の音声ストリーム キャパシティを計画する際は、次の点を考慮してください。

- 無許可の（共有）802.11 チャネルの使用率によって、AP が伝送できる同時音声ストリーム数が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音声ストリーム数が決定されるため、同じチャネルと次のチャネルの分離が非常に重要になります。2 つの AP が同じ場所にあり、同じチャネルで動作していても、音声ストリーム数は 2 倍にはなりません。実際、AP が 1 つの場合よりも音声ストリームが少なくなることがあります。
- セル キャパシティまたは帯域によって、同時に実行可能な音声ストリーム数が決定されます。
- ハンドセットおよび VoWLAN 展開でサポートされている QoS 機能を考慮する必要があります。

- ハンドセットにはさまざまな WLAN QoS 機能があります。これらは WLAN 展開で有効化されている機能に影響を与え、最終的には AP ごとの音声コール キャパシティを決定します。ほとんどの VoWLAN ハンドセットでは、その電話でサポートされる AP ごとのコール数についての指針が示されています。そして、それはハンドセットで最適な QoS 機能を使用でき、チャネル キャパシティにフル アクセスできる最良のケースでの値を示していると考える必要があります。

チャネルでサポート可能な実際の音声ストリーム数は、環境要因やクライアントでの 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。

図 9-10 で、Cisco Compatible Extension 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。

図 9-10　Cisco Compatible Extension VoWLAN 機能

Cisco Compatible Extensions が VoWLAN コールの品質にもたらす利点	
機能	**利点**
EAP タイプに対する CCKM サポート	資格情報がローカルにキャッシュされているとローミングが高速化
不定期自動省電力配信（U-APSD）	より多くのチャネル容量と高いバッテリ残量
TSPEC ベースのコールのアドミッション制御（CAC）	ローミングおよび緊急コール用の管理対象コール キャパシティ
音声メトリック	より多くの情報に基づいた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減少のスキャン
ロード バランシング	AP 間でロード バランスされたコール
送信電力の動的制御（DTPC）	送信する電源をクライアントが学習
アシステッド ローミング	より速いレイヤ 2 ローミング

220352

図 9-10 から、次のことが分かります。

- Cisco Centralized Key Management（CCKM）は Extensible Authentication Protocol（EAP）認証クライアントに高速クライアント ローミングを提供し、これによってコールの質が向上します。
- コール アドミッション制御（CAC）によってコールの質を向上し、E911 およびローミング コール用の帯域予約を作成できます。
- 支援ローミングおよびネイバー リストによって、コールの質が向上し、バッテリの寿命が延びます。
- 音声メトリックは管理に役立ちます。
- 不定期自動省電力配信（U-APSD）および送信電力の動的制御（DTPC）によってバッテリの寿命が延びます。
- 負荷分散および DTPC によってコールの質が向上します。

Cisco Compatible Extensions プログラムでは、サードパーティによる Cisco Aironet 無線インフラストラクチャ製品に対する検証および、サードパーティ企業から発売されている無線クライアント デバイスを提供します。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の主要な要因です。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」を参照してください。

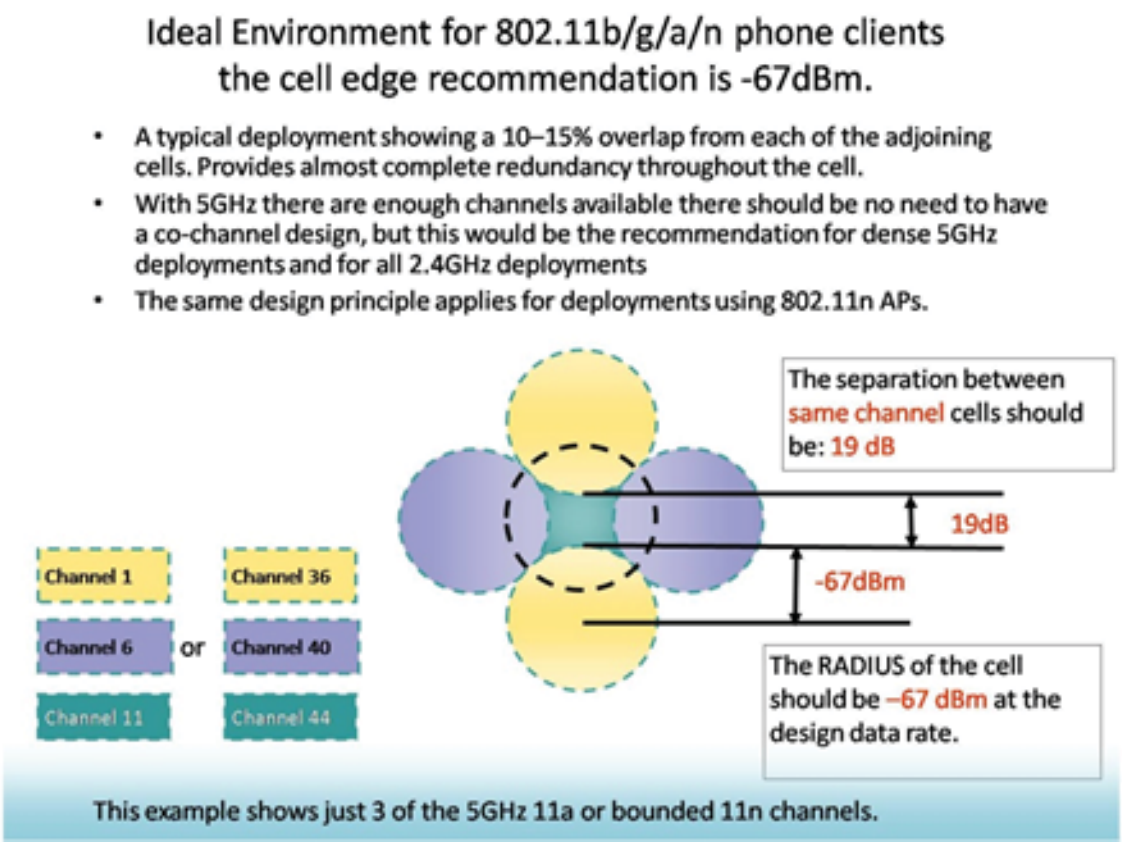
802.11e、WMM、および Cisco Compatible Extensions 仕様では、負荷を分散して、セルが音声ストリームで過負荷にならないようにすることができます。CAC は、コールの再起動のために十分なチャネル キャパシティがあるかどうかを判断します。ない場合、電話は別のチャネルをスキャンします。U-ASPD の主な利点は、WLAN クライアントからのフレームの送信を可能にし、節電のために AP でバッファされるクライアント データ フレームの転送をトリガーすることによる、WLAN クライアントの電力の節約です。[Neighbor List] オプションでは、近隣 AP のチャネル番号とチャネル キャパシティを含むリストが電話に提供されます。これによってコールの質が向上し、高速ローミングが実現し、バッテリの寿命が延びます。

セルの境界の設計

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 9-11 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、その地域のノイズ条件が影響します）。したがって、特定の電話タイプの見込みチャネル カバレッジ エリアを決定する場合は、電話で計測される信号強度とノイズの両方を、AP によって提供されるクライアント統計を使用して検証する必要があります。自律 AP および CAPWAP AP 上でのこれらの値の決定については、図 9-10 を参照してください。

-67dBm という信号強度の測定値は、802.11b 準拠の電話のベンダーで長年にわたって使用されてきました。テストの結果、同じ一般的な測定ルールを 802.11g/n および 802.11a/n 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 9-11　セルの境界の測定



（注）　図 9-11 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。802.11a の 5 GHz 帯域にはチャンネルが 20 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 の両方で、セルの境界を、指定チャネルに必要な最高データ レートでパケット エラー レート 1% が維持されるようなフロア レベルに配置する必要があります。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ノート PC 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。802.11a 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。音声コールのキャパシティは、802.11g および 802.11a の場合と同様、802.11n および 802.11ac とほぼ同じです。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。802.11 仕様の小さいパケット サイズと ACK ロジックにより、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作成されます。ビデオ コールからは、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 セルの境界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。

802.11g および 802.11a 電話クライアントは、最大 54 Mbps のレートを実現できる可能性があります。現在のチップ セットは 54 Mbps をサポートしますが、送信電力の能力はそれぞれ異なります。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、一致する送信電力レベルで確立することを強くお勧めします（「送信電力の動的制御」（P.9-16）を参照）。

特定のデータ レートに対してカバレッジ セルを作成できます。高密度展開や、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、802.11a が推奨されます。802.11a で低いデータ レートを無効にして、データ レート 24 Mbps を *required* に設定し、36 ～ 54 のレートをそのまま有効にしておくことができます。

セルの境界を -67 dBm に設定した後、1% のエラー レートが発生している場所を特定して、SNR 値を確認します。

-67 dBm のセルの境界は、次の手順で決定します。

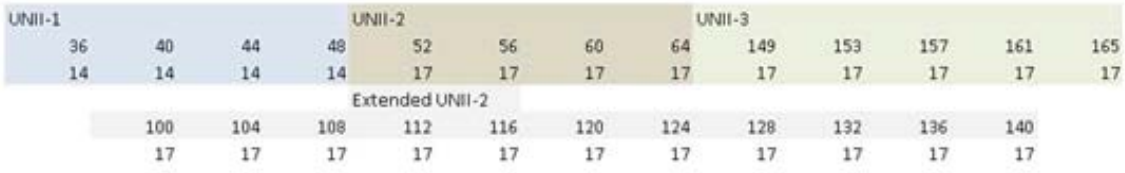
- 電話を、必要な送信電力に設定します。
- AP を、一致する送信電力に設定します。
- AP と必要なアンテナを、電話を使用する場所に配置します。
- アクティブなコールを使用して、または G711 コーデックと同じサイズのパケットを送受信する間に、-67 dBm セル境界への信号レベルを測定します。

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。Cisco Unified Wireless IP Phone のデータ シートは、次の URL で入手できます。

http://www.cisco.com/en/US/products/hw/phones/ps379/index.html.

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 9-12 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 9-12　　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、6dB 単位で変化します。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送信電力が 13 dBm の場合、すべての AP の最大送信電力が 13 dBm であることが推奨されます。したがって、AP の最大送信電力を同じレベルに設定するか、それが不可能であれば、次に大きい送信電力レベルに設定する必要があります。片通話を避けるために、同じ送信電力に設定することが推奨されます。一般的に、AP は電話よりもレシーバの感度およびダイバーシティがすぐれているため、若干低い強度の電話信号を受信できるはずです。同じ送信電力の詳細は、「送信電力の動的制御」（P.9-16）を参照してください。

デュアル バンド カバレッジ セル

第 3 章「WLAN 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。デュアル モード AP において 2.4 GHz チャネルと 5 GHz チャネルの両方で同じセル カバレッジを提供する場合、2.4 GHz チャネルの送信電力は 5 GHz チャネルと同じ（またはそれ以下）である必要があります。多くのサイトでは、SNR 計算式のノイズ レベルは最大で 10dB 低くなります。802.11g 無線のレシーバの感度は一般的に、同じデータ レートの 802.11a 無線よりも 2 dBm 優れています。たとえば、Cisco 7921G のデータ シートでは、データ レート 36 Mbps での受信感度は、802.11g の場合は -78 dBm で、802.11a の場合は -76 dBm となっています。したがって、ノイズ フロアの予想を 10 dB 向上させると、802.11a セルの感度は 8 dBm 向上します。802.11g と 802.11a の間でのパス損失の差異など他にも項目があるため、正比例はしません。ただし、同じカバレッジ セルを希望する場合は、802.11g ネットワークの電力レベルを 11a ネットワークよりも 1 または 2 レベル引き下げる必要があります。

送信電力の動的制御

Cisco Aironet AP ではデフォルトで送信電力の動的制御（DTPC）が有効になっています。DTPC は Cisco WLC によって自動化されていますが、設定は自律 AP 上で行う必要があります。

DTPC の目的は、クライアントの AP と Wi-Fi 無線の間の送信電力の不均衡による片通話の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
- AP でクライアントに知らせるために送信電力をアドバタイズする

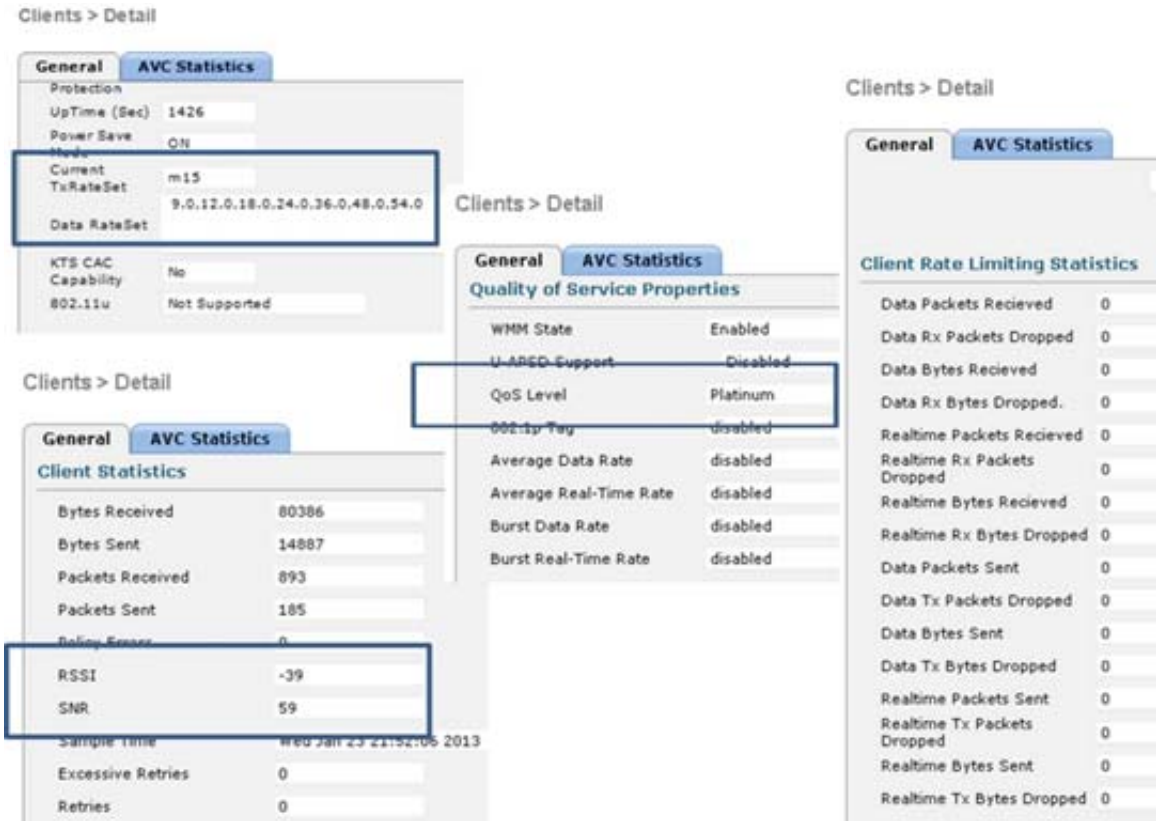
DTPC により、電話の送信電力を AP の送信電力に自動的に一致させることができます。図 9-13 に示す例は、電話の送信電力が 5 mW から 100 mW に変更されることを意味します。

図 9-13　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、クライアントには最小送信電力が要求されません。また、Wi-Fi デバイスが規制で許可された最大送信電力を使用している場合も、ほとんど要求されません。一般的な Wi-Fi デバイスでは、最大送信電力は 100mW 以下です。これは Wi-Fi 仕様によって、AP とクライアントの間での接続中、AP およびクライアントに一致する電力レベルが要求されないためです。短時間でも関

連付けられれば、AP とクライアントが互いのカバレッジ エリアに存在しなくても、引き続き関連付けられる可能性が常にあります。アクティブなコール中にこれが発生すると、音声が失われます。図 9-14 に示すように、アクティブなコール中の送信電力レベルが等しくない場合には、音声が失われます。AP と電話の間の接続の維持に役立つ 802.11 メカニズムはいくつかあり、そのうちの 1 つは低速データ レートをネゴシエートできます。一般的に、低速データ レートの場合には高速データ 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 セルが高いスループットと容量を必要とする場合に、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、Wi-Fi チャネルと 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。

図 9-14　　WLC クライアントの [Detail] ウィンドウ



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 が 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の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 パケットの信号の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の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信号の品質が向上します。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 の残りのカバレッジ エリアの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の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。図 9-14 で示すように、WLC は、電話機が関連付けられた 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、AP でパケットを受信している場合の、電話機が送信したパケットの高度を示します。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、セルの境界（RSSI の推奨値 -67dBm）で、そのパケットが高データ 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の境界については、図 9-11 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であれば、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、お使いの最も弱いスマート フォンやタブレットの最大送信電力 2.4 GHz および 5 GHz に合わせて、最大送信電力 2.4 GHz および 5 GHz を dBm 値に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 4 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、次のページをお読みください。

http://en.wikipedia.org/wiki/IEEE_802.11k-2008

802.11k 仕様については、次のページをお読みください。

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4544755

802.11r 仕様の簡単な説明については、次のページをお読みください。

http://en.wikipedia.org/wiki/IEEE_802.11r-2008

IEEE 802.11r 仕様については、次のページをお読みください。

http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04573292

802.11k および 802.11k 対応のクライアント デバイスは、それ自身が現在関連付けられている AP から近隣の AP（*ネイバー リスト*）の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っています。AP は、同じ WLAN 上にある AP のネイバー リストと共に Wi-Fi チャネル番号を含むアクション 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 フォンが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、無線リソース管理（RRM）を有効にするように WLC を設定することで、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 クライアントがすべての 2.4 GHz と 5 GHz のすべてのチャネルをプローブして AP のローミング先を探す必要はありません。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、クライアントによる決定が向上します。また、各チャネルの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、同じ認証タイプをサポートしています。対象となるのは LEAP、EAP-FAST、EAP-TLS、EAP-TTLS、EAP-SIM、PEAP バージョン 1 および 2 です。このセキュリティ機能により、パケット 4 個のみと引き換えに、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、ローミング後でも、802.11r クライアントでデータ、ビデオ、および音声パケットを認証プロセスの遅延なしで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。このことは、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。

- 自律モードの AP でサポートされない
- ローカル認証 WLAN と中央認証 WLAN 間のローミングがサポートされない

シスコでは 802.11r 仕様を使用することを推奨します。それは、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た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ローカルですが、近接ユーザにも影響する可能性があります。Bluetooth（BT）は、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 9-15 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 802.11g 音声コールから取得したものです。図 9-16 では、Bluetooth ヘッドセットによるジッターも示しています。

図 9-15　一般的な Bluetooth イヤピースの 802.11b/g 2.4 GHz スペクトラムにおける信号パターン

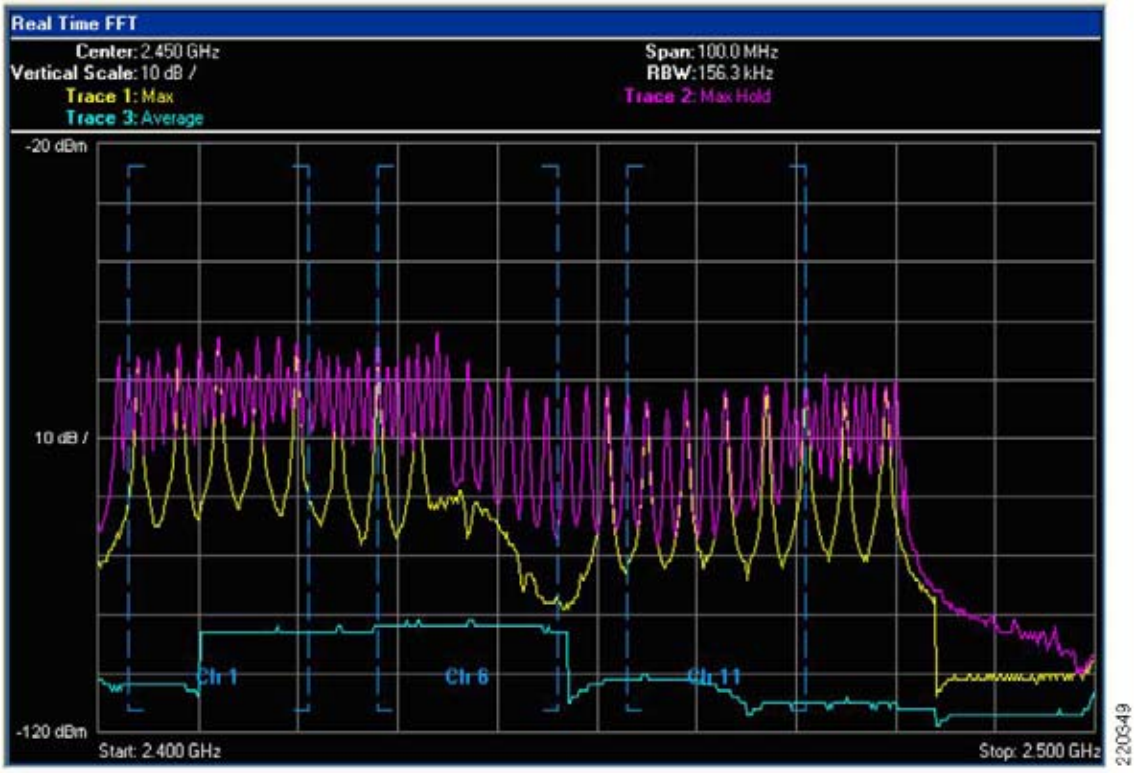
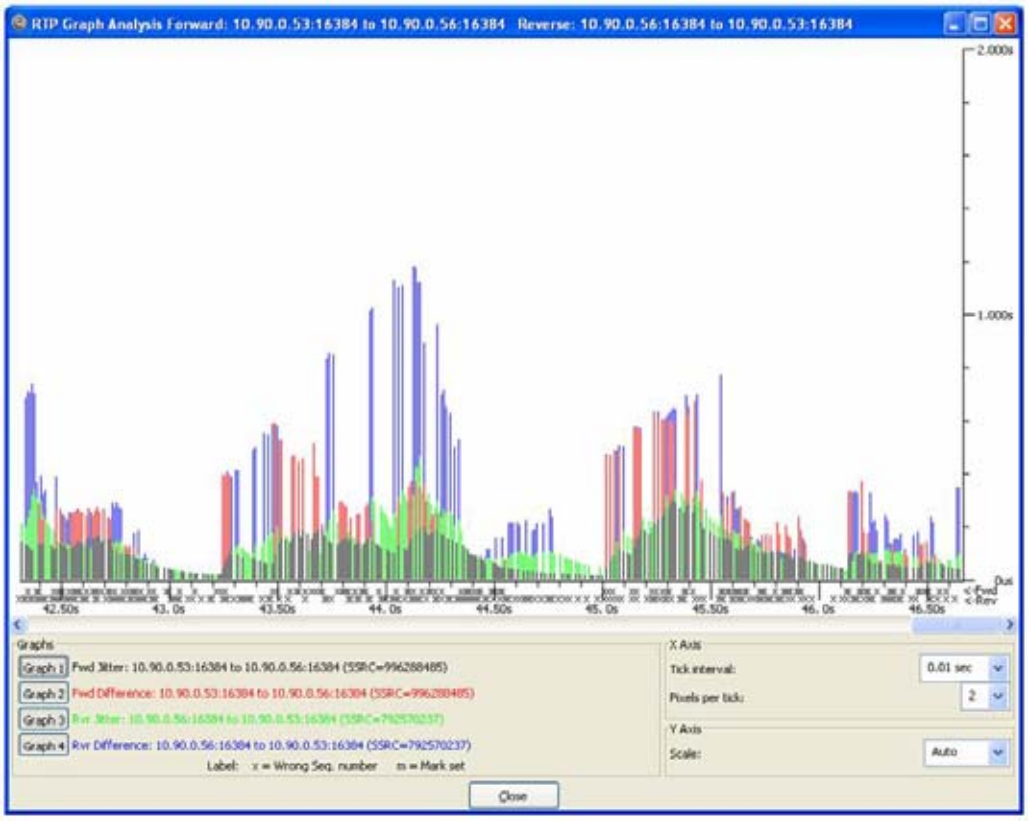


図 9-15 中の**紫色**の線は、最大ホールド回線、すなわちテスト中に到達した最大送信電力を示す回線です。**黄色い**線は、最後のサンプル期間の 10 秒の最大伝送パワーを示しています。**緑色**の線は、テスト期間の平均伝送パワーを示しています。縦の**青い**点線は、オーバーラップしない 3 つの 802.11b/g チャネルである Ch1、Ch6、および Ch11 を分けています。この図は左から右に 2.400 GHz から 2.500 GHz を表します。右端の Ch11 の縦の青い線は、ヨーロッパと日本で使用されている 802.11 スペクトルの部分です。このキャプチャは、北米の規制区域用に設定された 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 802.11g の信号は、混合周波数 22 MHz 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。最大保留回線は、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 802.11g 無線のレベルよりも高いところにあります。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 9-16 で、それぞれ Bluetooth イヤピースを使用する 3 つの同時通話の Ethereal ジッター分析の例を示します。

図 9-16　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 と干渉情報の詳細については、次の IEEE レポートをお読みください。

http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6105779

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 9-17 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 9-17　IEEE 波形シミュレーション

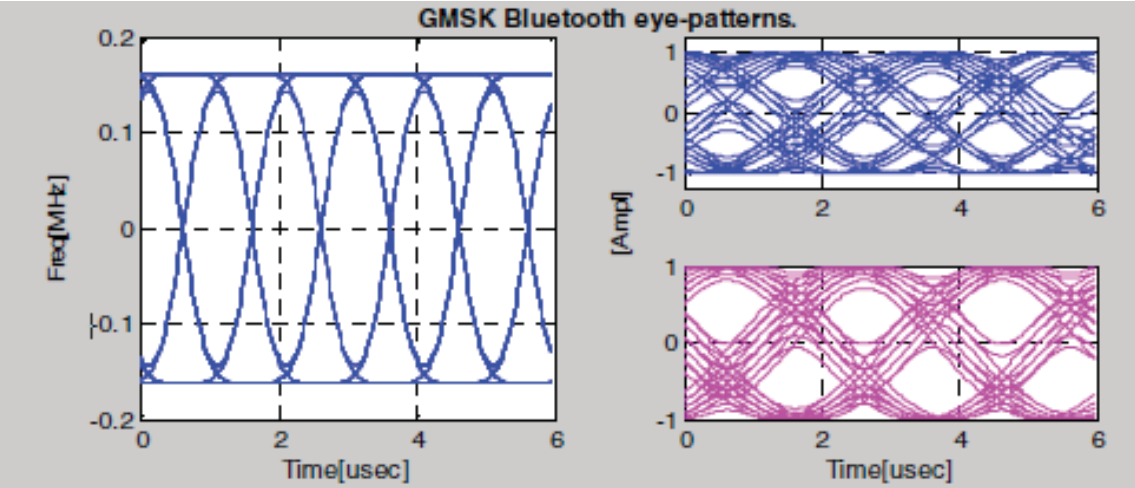


図 9-17 で示すように、ホッピング周期が 625 μ 秒の Bluetooth は、一度に複数の OFDM のパケットが発生した場合に干渉する可能性があります。特に、高速の OFDM モード（パケット長が Bluetooth よりはるかに短い場合）が衝突に関わっている場合にこの傾向が顕著です。

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。

概要

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 URL を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

無線ゲスト アクセスの概要

理想としては、無線ゲスト ネットワークの実装で、企業の既存の無線および有線インフラストラクチャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID：ゲスト アクセスを必要とするあらゆる場所で、キャンパス無線ネットワークを介して実装されます。
- ゲスト トラフィックのセグメンテーション：ゲストの移動場所を制限するために、キャンパス ネットワーク上のレイヤ 2 またはレイヤ 3 での実装テクニックを必要とします。
- アクセス コントロール：キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の使用、または企業ネットワークからインターネットへのゲスト アクセスを制御する外部プラットフォームの実装を伴います。
- ゲスト ユーザ資格情報の管理：スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報を作成できるプロセス。この機能は、アクセス コントロール プラットフォーム内に常駐している場合と、AAA またはその他の管理システムのコンポーネントになっている場合があります。

Cisco Unified Wireless 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が必要となる、プロトコルやセグメンテーション テクニックを追加しなくていいことです。

中央集中型 WLAN アーキテクチャを使用したゲスト アクセス トポロジの例については、図 10-1 を参照してください。

図 10-1　　中央集中型コントローラのゲスト アクセス

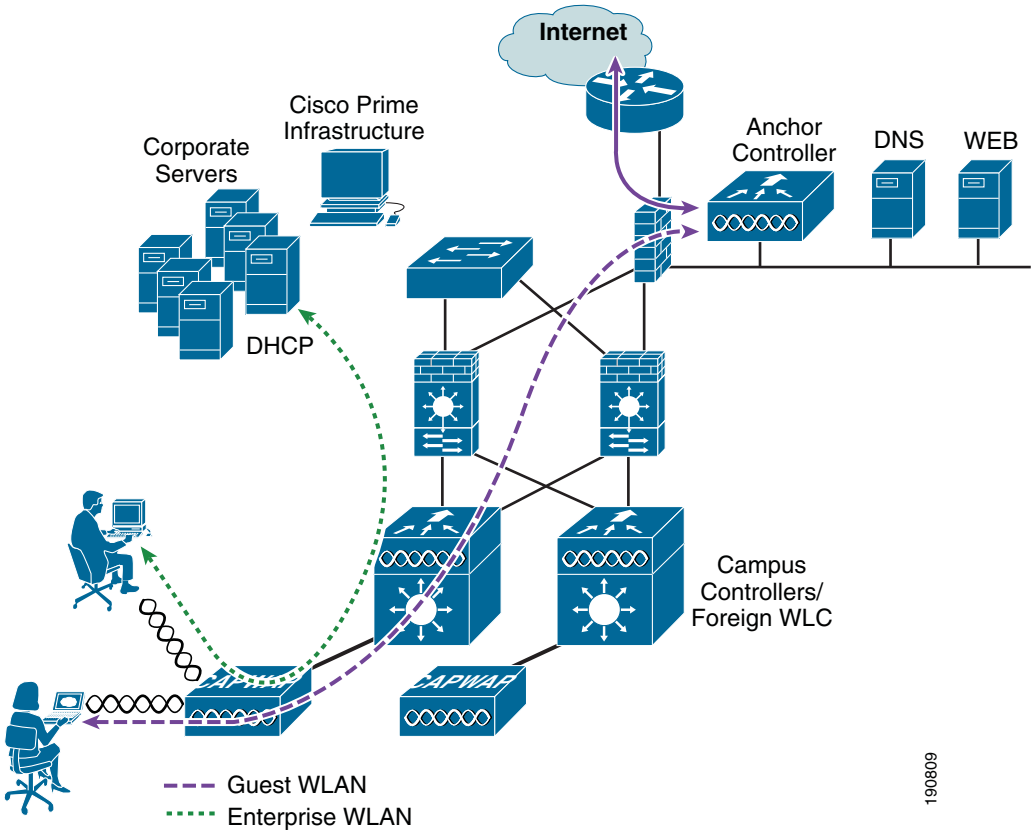


図 10-1 に示すように、アンカー コントローラが企業 DMZ 内に配置され、「アンカー」機能を実行します。アンカー コントローラは、ネットワーク上のその他のキャンパス コントローラを起点とする EoIP トンネルの終端処理に関与します。これらの「外部」コントローラは、企業全体にプロビジョンされたさまざまな WLAN（1 つ以上のゲスト WLAN を含む）の終端、管理、および標準の動作に関与します。ゲスト WLAN は EoIP トンネルを経由してアンカー コントローラに転送されます。具体的には、ゲスト WLAN のデータ フレームが、CAPWAP を使用して AP から外部コントローラにカ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 コントローラ内で構成および実行されます。ただし、これらの機能のうち 1 つまたはすべてを外部で実装するためのオプションがあり、これについてはこの章の後半で説明します。

サポートされ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 6.0 以降を使用した場合）。

- WLC 2504
- WLC 5508
- WiSM-2
- WLC 7500

次の WLC プラットフォームは、アンカー機能に使用 *できません*が、標準のコントローラ展開と指定したアンカー コントローラへのゲスト モビリティ トンネルの起点（外部 WLC）として使用できます。

- サービス統合型ルータ用 Cisco WLAN コントローラ モジュール（ISR-SM）
- Cisco 2504

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、プロビジョンされたゲスト WLAN を 1 つ以上の（アンカー）WLC にマップできます。自動アンカー モビリティによって、ゲスト WLAN と関連するすべてのゲスト トラフィックを、インターネット DMZ に常駐するアンカー コントローラに企業ネットワークを通して透過的に転送できます（図 10-2 を参照）。

図 10-2　自動アンカー EoIP トンネル

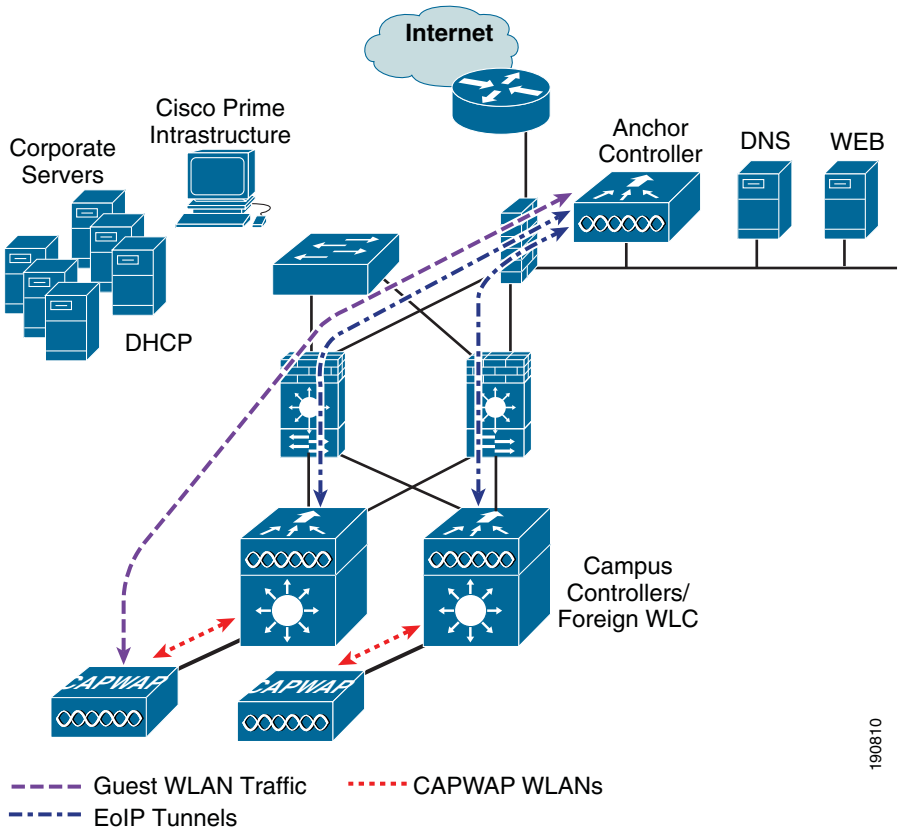
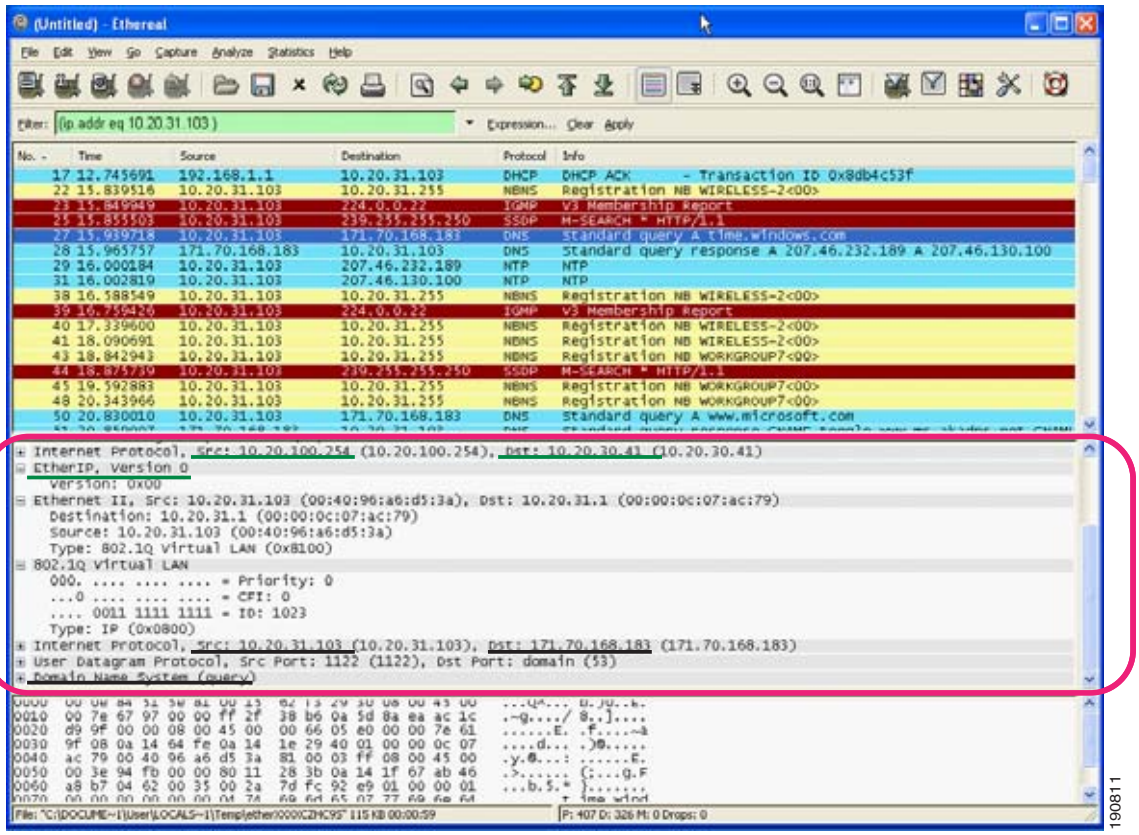


図 10-3 は、ゲスト WLAN がプロビジョンされた外部コントローラとローカル Web 認証を実行しているアンカー コントローラ間の Ethernet in IP トンネル（強調表示部分）のスニファ トレースを示しています。図中の最初の IP 詳細は、外部コントローラとアンカー コントローラ間の Ethernet in IP トンネルを示しています。2 番目の IP 詳細は、ゲスト トラフィックの詳細です（この場合は、DNS クエリー）。

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。

- SNMP 用の TCP 161 と 162
- TFTP 用の UDP 69
- HTTP 用または GUI アクセスの HTTPS 用の TCP 80 または 443
- Telnet 用、または CLI アクセスの SSH 用の TCP 23 または 22

トポロジによっては、ファイアウォールを使用して、外部の脅威からアンカー コントローラを保護できます。

最大のパフォーマンスを引き出すために、また、ネットワーク内の位置決めが推奨されていることから、ゲスト アンカー コントローラをゲスト アクセス機能のサポートに専念させることを強く推奨します。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」（P.10-13）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効率的にサポートするプラットフォームは、Cisco 5508 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 5508 で十分です。

1 台の 5508 シリーズ 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。さらに、5508 コントローラは、同時に最大 7,000 ユーザをサポートし、8 Gbps の転送能力があります。

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。

- Cisco 2504 ワイヤレス LAN コントローラ:4 個の 1 Gbps インターフェイスと 1000 個のゲスト クライアント
- Cisco 5508 ワイヤレス LAN コントローラ（WLC）: 8 Gbps と 7,000 個のゲスト クライアント
- Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM-2）: 20 Gbps と 15,000 個のクライアント
- Cisco 7500 ワイヤレス LAN コントローラ（WLC）: 10 Gbps と 20,000 個のクライアント

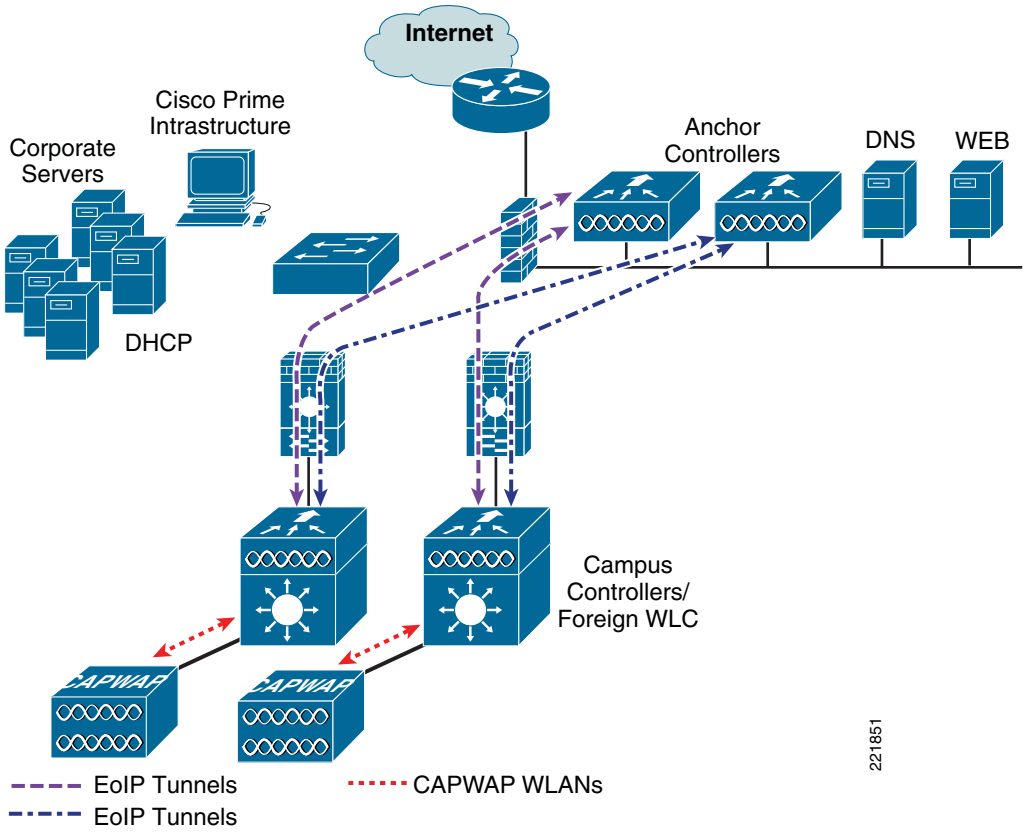
アンカー コントローラの冗長性

Cisco Unified Wireless ソリューション ソフトウェアのリリース 4.1 からは、「ゲスト N+1」冗長性機能が自動アンカー / モビリティ機能に追加されました。この機能には、自動 ping 機能が導入されています。この機能によって、外部コントローラが積極的に ping をアンカー コントローラに送信して、コントロールとデータ パスの接続を確認できます。障害が発生したり、アクティブなアンカーに到達できなくなった場合には、外部コントローラが次のことを行います。

- アンカーが到達できなくなっていることを自動的に検出
- 到達できないアンカーに以前にアソシエートされた無線クライアントを自動的に解除
- 無線クライアントを代替アンカー WLC に自動的に再びアソシエート

ゲスト N+1 冗長性により、所定のゲスト WLAN に 2 つ以上のアンカー WLC を定義できます。図 10-4 は、アンカー コントローラの冗長性を備えた、一般的なゲスト アクセス トポロジを示しています。

図 10-4　ゲスト アンカーの N+1 冗長性を備えたゲスト アクセス トポロジ



ゲスト N+1 冗長性については、次のことに留意してください。

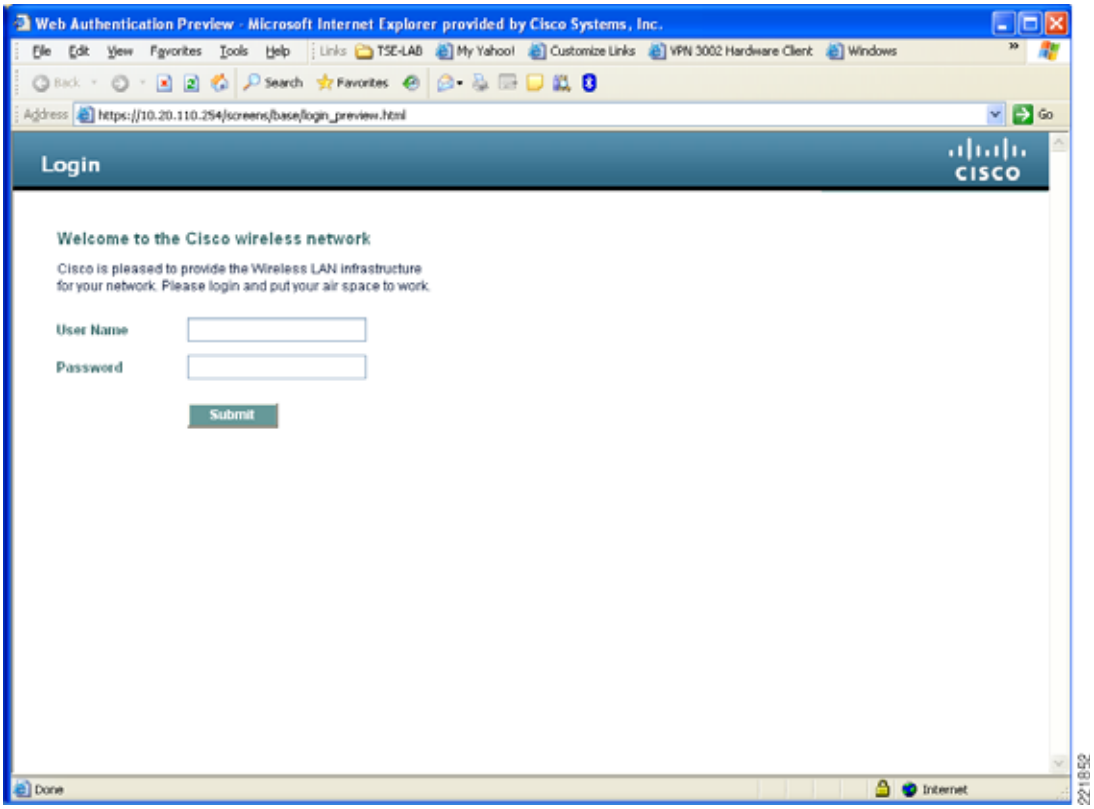
- 所定の外部コントローラの負荷は、ゲスト WLAN に設定されたアンカー コントローラのリスト全体で無線クライアント接続のバランスを取ります。1 つのアンカーを、1 つ以上のセカンダリ アンカーを持つプライマリ アンカーとして指定する方法は、現在のところありません。
- 到達できなくなっているアンカー WLC にアソシエートされた無線クライアントは、WLAN 用に定義された別のアンカーに再びアソシエートされます。これが発生し、Web 認証が使用されている場合には、クライアントは Web ポータル認証ページにリダイレクトされ、資格情報の再送信が要求されます。

（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。

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 Controller プラットフォーム上で使用でき、WLAN がレイヤ 3 Web ポリシーベースの認証用に設定された場合にデフォルトで呼び出されます。

よりカスタマイズされたページが必要な場合は、管理者が、カスタマイズされたページをインポートしてローカルに保存するオプションが用意されています。また、会社で外部 Web サーバを使用する場合は、内部サーバを使用せずに外部サーバにリダイレクトするようにコントローラを設定できます。Web ページの設定に関するガイドラインについては、「ゲスト アクセスの設定」（P.10-13）を参照してください。

ユーザ リダイレクション

たいていの Web ベースの認証システムでは一般的なことですが、ゲスト クライアントを WLC の Web 認証ページにリダイレクトする場合は、ゲスト クライアントが Web ブラウザ セッションを起動して、対象 URL を開く必要があります。リダイレクションが正常に動作するには、次の条件を満たす必要があります。

- DNS 解決：ゲスト アクセス トポロジでは、有効な DNS サーバが DHCP 経由で割り当てられ、認証前のユーザからその DNS サーバへアクセスできるようにする必要があります。クライアントが認証で Web ポリシー WLAN にアソシエートすると、DHCP と DNS を除くすべてのトラフィックがブロックされます。そのため、DNS サーバは、アンカー コントローラから到達可能にする必要があります。トポロジによっては、DNS を許可するためにファイアウォールを通してコンジットを開く必要がある場合と、インターネット境界ルータ上の ACL を変更する必要がある場合があります。

（注） 静的 DNS 設定のクライアントは、設定された DNS サーバがゲスト ネットワークからアクセスできるかどうかによって、機能しない場合があります。

- 解決可能なホームページ URL：ゲスト ユーザのホームページ URL は、DNS によってグローバルに解決可能である必要があります。たとえば、ユーザのホームページが、会社のイントラネットの外側では解決できない社内用ホームページである場合、そのユーザはリダイレクトされません。この場合、ユーザは www.yahoo.com や www.google.com などの一般サイトへの URL を開く必要があります。
- HTTP ポート 80：ユーザのホームページは解決可能ですが、HTTP ポート 80 以外のポート上にある Web サーバに接続された場合、ユーザはリダイレクトされません。また、ユーザが WLC の Web 認証ページにリダイレクトされるには、ポート 80 を使用する URL を開く必要があります。

（注） ポート 80 に加え、コントローラがリダイレクションを監視できるように、追加ポート番号を 1 つ設定するオプションは次のとおりです。この設定は、コントローラの CLI を通してのみ使用可能です。<*controller_name*> config> **network web-auth-port** <*port*>

ゲスト資格情報の管理

ゲスト資格情報は、リリース 4.0 以降の管理システムを使用して、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、管理システム内に限定的な特権アカウントを作成し、ゲスト資格情報を作成する目的の Lobby Ambassador アクセスを許可します。このようなアカウントでは、Lobby Ambassador に許可されている機能は、ゲスト資格情報を作成して、Web ポリシーが WLAN に設定されたコントローラに割り当てることだけです。

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 E メールで送信できるようになります。さらに、「スケジュール」ゲスト テンプレートが使用されると、アクセスが提供される新しい日（間隔）ごとに、資格情報が自動的に E メールで送信されます。

- （ゲスト）WLAN SSID および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、無線ゲストがアソシエートされアクティブな場合は、WLC がトラフィック転送を停止してそのユーザの WEBAUTH_REQD ポリシー状態に戻ります。ゲスト資格情報が（コントローラに）再適用されない場合、そのユーザは二度とネットワークにアクセスすることができません。

（注）　ゲスト資格情報に関連付けられたライフタイム変数は、WLAN セッション タイムアウト変数とは無関係です。WLAN セッション タイムアウトの時間を過ぎてもユーザが接続したままの場合は、認証が解除されます。その後、ユーザは、Web ポータルにリダイレクトされ、資格情報の有効期限が切れていない場合には、再度アクセスするためにログインをやり直す必要があります。面倒な認証のリダイレクトを避けるには、ゲスト WLAN セッション タイムアウト変数を適切に設定する必要があります。

ローカル コントローラのロビー管理者のアクセス

中央集中型 WCS 管理システムが展開されていないか使用できない場合、ネットワーク管理者は、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
- 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
- SSID
- 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」（P.10-10）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] 設定でネットワーク ユーザのチェックボックスがオフになっている場合でも、ネットワーク ユーザ認証をサポートするために使用できます。ただし、これを実現するには、サーバが特定の WLAN の [Security] > [AAA Servers] 設定で明示的に選択されている必要があります。

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。

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 Microsoft ユーザ データベースの使用を検討している場合は、次の Cisco ACS 設定に関する注意事項を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html

特に、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/installation/guide/windows/postin.html#wp1041223

ゲスト パススルー

無線ゲスト アクセスのもう 1 つの形態は、ユーザ認証をすべて省略して、オープン アクセスを可能にすることです。ただし、企業は、アクセスを許可する前に利用規定または免責条項のページをユーザに表示することが必要になる場合があります。そのような場合は、Web ポリシーをパススルーするようにゲスト WLAN を設定できます。このシナリオでは、ゲスト ユーザが、免責情報を含むポータル ページにリダイレクトされます。

また、パススルー モードには、ユーザが接続する前に E メール アドレスを入力するオプションもあります（サンプル ページについては、図 10-6 および図 10-7 を参照）。設定例については、「ゲスト アクセスの設定」（P.10-13）を参照してください。

図 10-6　Welcome AUP ページのパススルー

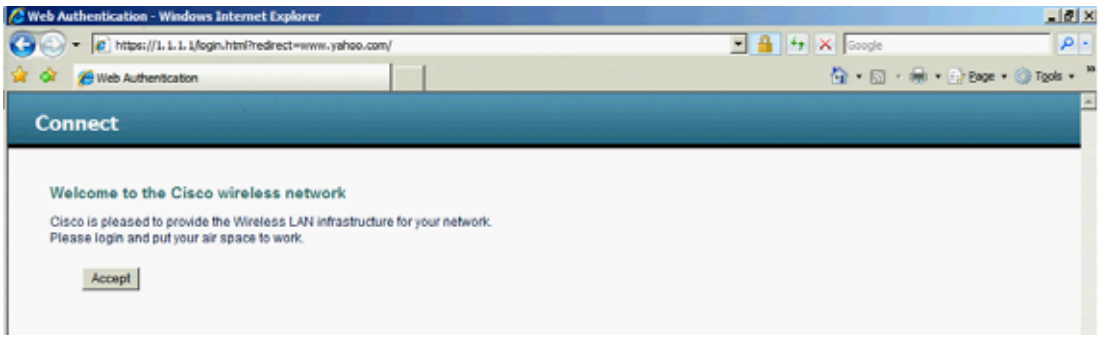


図 10-7　E メールを含むページのパススルー

ゲスト アクセスの設定

この項では、Cisco Unified Wireless 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、次のコントローラの管理 IP アドレスへの HTTPS セッションを開くことによって、確立されます。**https://***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。

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」（P.10-6）を参照してください。

（注）　この項で説明する設定手順は、記載された順序に従って実行することを推奨します。

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」（P.10-6）で説明したように、アンカー WLC は、ゲスト アクセスだけに使用して、社内の LAP の制御および管理には使用しないことを推奨します。

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、1.1.1.1 などのアドレスの仮想 IP を定義するように推奨されています。このアドレスは、同じモビリティ グループのメンバであるすべてのコントローラで同じアドレスにする必要があります。また、仮想インターフェイスは、コントローラがクライアントを Web 認証のためにリダイレクトするときのソース IP アドレスとしても使用されます。

ゲスト VLAN インターフェイスの設定

前述したインターフェイスは、コントローラに関連付けられた動作と管理機能に使用されます。ゲスト アクセス サービスを実装するには、もう 1 つのインターフェイスを定義する必要があります。これは、ゲスト トラフィックをインターネットにルーティングするためのインターフェイスです。「アンカー コントローラの位置決め」（P.10-6）で説明したように、ゲスト インターフェイスは、ファイアウォール上のポートに接続される場合と、インターネット境界ルータ上のインターフェイスに切り替えられる場合があります。

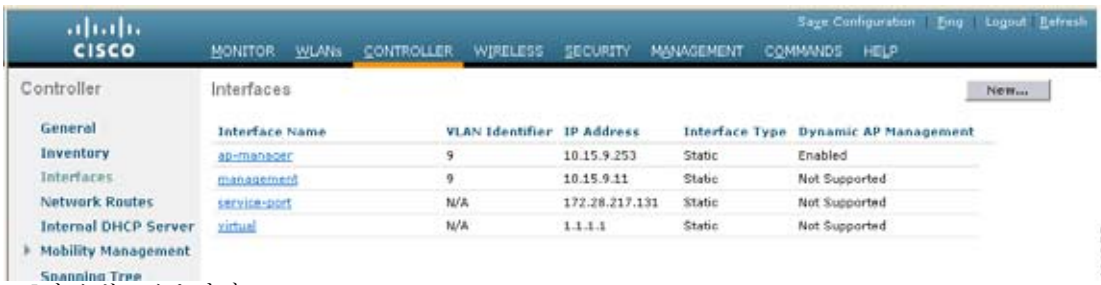
新しいインターフェイスの定義

次の手順を実行して、ゲスト トラフィックをサポートするインターフェイスを定義および設定します。

ステップ 1　[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。

インターフェイス名と VLAN ID の定義

ステップ 4　インターフェイス名と VLAN ID を入力します。（図 10-9 を参照）。

図 10-9　インターフェイス名と VLAN ID

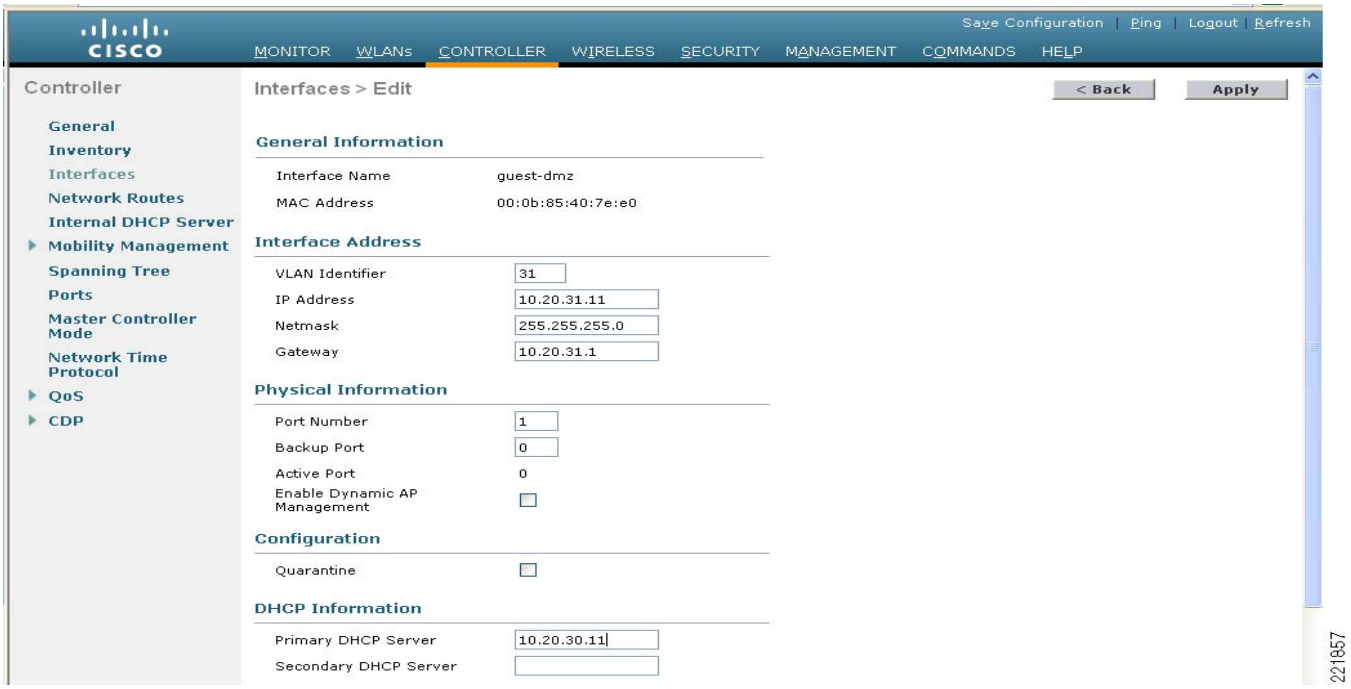
インターフェイス プロパティの定義

ステップ 5　次のプロパティを定義します。

- インターフェイス IP
- マスク
- ゲートウェイ（アンカー コントローラに接続されたファイアウォールまたはネクスト ホップ ルータの場合）
- DHCP サーバ IP（外部 DHCP サーバを使用している場合は、[Primary DHCP Server] フィールドのそのサーバの IP アドレスを使用します）。

  図 10-10 を参照してください。

図 10-10　インターフェイス プロパティの定義



（注）　DHCP サービスをアンカー コントローラ上でローカルに実装する必要がある場合は、[Primary DHCP Server] フィールドにコントローラの管理 IP アドレスを入力します。ゲスト N+1 冗長性が DMZ に実装されている場合、展開されている追加のアンカー WLC ごとに、上記のインターフェイス設定を繰り返します。

モビリティ グループの設定

次のデフォルトのモビリティ グループ パラメータは、標準の中央集中型 WLAN 展開の一部として、外部 WLC に定義しておく必要があります。ゲスト アクセスの自動アンカー モビリティをサポートするには、モビリティ グループ ドメイン名でアンカー WLC も設定する必要があります。

アンカー WLC のデフォルト モビリティ ドメイン名の定義

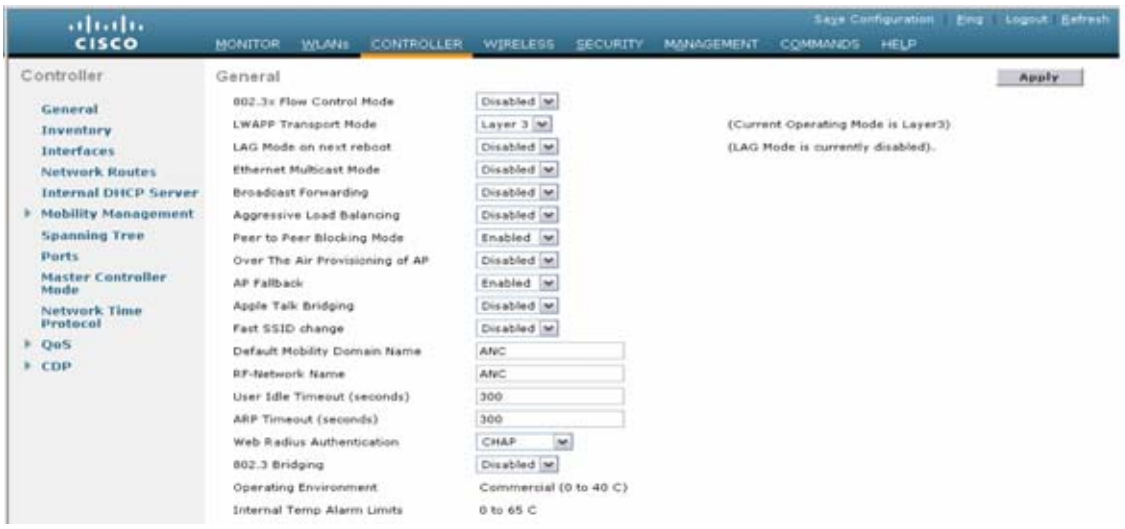
アンカー WLC のデフォルト モビリティ ドメイン名を設定します。アンカーのモビリティ ドメイン名は、外部 WLC に設定した名前と異なる必要があります。以下の例では、企業の無線展開にアソシエートされている WLC（外部コントローラ）は、すべてモビリティ グループ「SRND」のメンバです。一方、ゲスト アンカー WLC は、別のモビリティ グループ名「ANC」で設定されます。これは、企業の無線展開にアソシエートされているプライマリ モビリティ ドメインから、アンカー WLC を論理的に区別しておくために行われます。

ステップ 1　[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 メンバの定義

ゲスト WLAN をサポートする企業での展開内のすべての外部 WLC は、ゲスト アンカー WLC のモビリティ グループ メンバとして定義する必要があります。

ステップ 1　[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の定義

モビリティ グループ メンバとして外部コントローラを追加

ステップ 3　[New] をクリックして、ゲスト アクセス WLAN をサポートする各外部コントローラの MAC と IP アドレスを定義します。（図 10-13 を参照）。

図 10-13　アンカー WLC への外部コントローラの追加

（注）　上に示した図 10-13 の [Group Name] は、外部 WLC の [Default Mobility Domain Name] で設定される名前です。これは、アンカー WLC に使用される名前と異なる必要があります。メンバの IP アドレスと MAC アドレスは、外部 WLC の管理インターフェイスにアソシエートされたアドレスです。ゲスト WLAN をサポートする追加の各外部 WLC に対して、上記の手順を繰り返します。複数のアンカーが展開されている場合（ゲスト N+1 冗長性）、アンカー WLC のデフォルト モビリティ ドメイン名の定義とアンカー WLC のモビリティ グループ メンバの定義の手順を繰り返します。

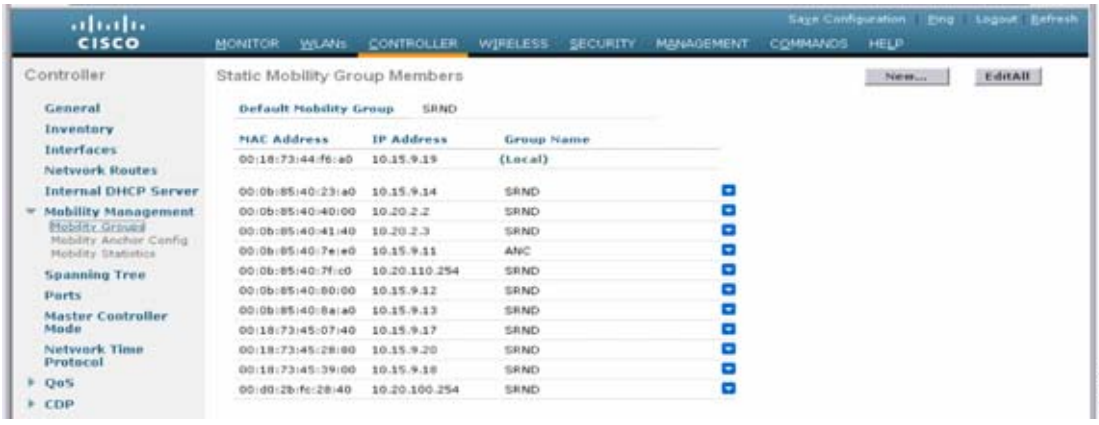
外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加

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 グループのメンバとして定義する必要があります。下の例で、アンカー WLC のグループ名エントリが「ANC」で（「アンカー WLC のモビリティ グループ メンバの定義」（P.10-18）を参照）、企業の無線展開を構成しているもう一方の WLC がモビリティ グループ「SRND」のメンバであることに注意してください。

ステップ 1　[New] をクリックして、アンカー WLC の IP、MAC アドレス、およびグループ名をモビリティ メンバ テーブルに追加します。

ステップ 2　追加の外部コントローラごとにこの手順を繰り返します （図 10-14 を参照）。

図 10-14　外部 WLC へのアンカー コントローラの追加



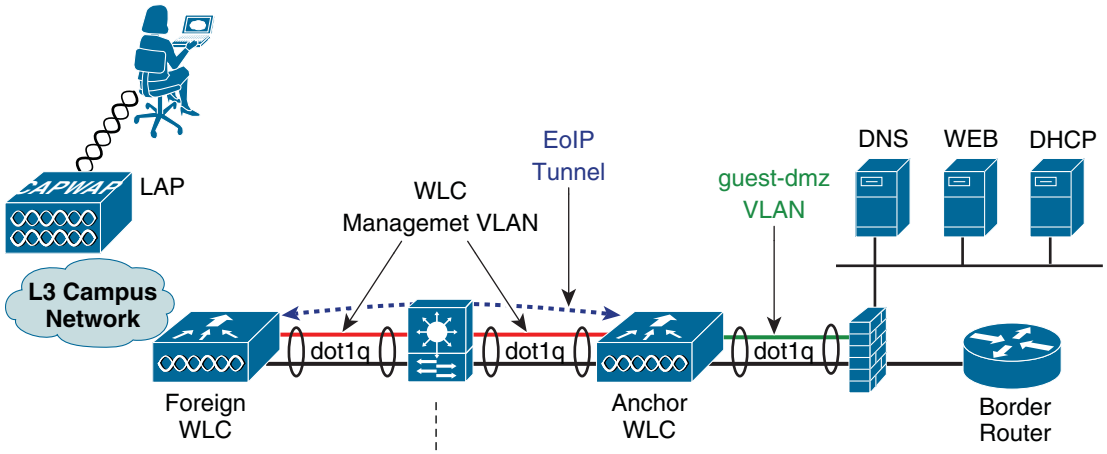
（注）　ゲスト N+1 冗長性機能が展開されている場合、2 つ以上のアンカー WLC エントリが各外部 WLC のモビリティ グループ メンバ リストに追加されます。

ゲスト WLAN の設定

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 にアソシエートされた LAP の管理に使用されない場合でも、アンカー WLC は、ゲスト WLAN を使用して設定する必要があります。なぜならば、アンカー WLC は、WLAN の論理拡張機能で、そこでユーザ トラフィックがアンカー WLC 上のインターフェイス/VLAN に最終的にブリッジされるためです（AP と外部コントローラ間では 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



Foreign WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = 802.11b/g only
Interface = Management
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

Mobility Config
Default Mobility Group Name = **SRND**
Static Mobility Members:
00:0b:85:40:7e:e0 10.15.9.11 ANC

Anchor WLC WLAN Summary
SSID = Guest
WLAN Status = Enabled
Radio Policy = 802.11b/g only
Interface = guest-dmz
Broadcast SSID = Enabled
Layer 2 Security = None
Layer 3 Security = None + Web + Auth
AAA Servers = None
QOS = Bronze (Background)
WMM = Disabled
Advanced = Defaults + DHCP Required

Mobility Config
Default Mobility Group Name = **ANC**
Static Mobility Members:
00:18:73:44:f6:a0 10.15.9.19 SRND

222545

（注）　[WLAN Security]、[QoS]、および [Advanced] 設定タブで定義するパラメータは、アンカーおよび外部コントローラの両方で*同じ設定にする必要があります*。

外部 WLC：ゲスト WLAN の設定

ステップ 1　[WLANs] タブをクリックして、[New] をクリックします。（図 10-16 を参照）。

図 10-16　　ゲスト WLAN の設定

ゲスト WLAN SSID の定義

ステップ 2　将来のゲスト ユーザが、直感的に理解できるか、または認識しやすい SSID を定義します。

コントローラで自動的に VLAN ID を割り当てます。管理者は、他の SSID/WLAN で使用されていなければ、1 ～ 16 の ID を選択できます。

ステップ 3　[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アソシエートされていた無線クライアントのアソシエーション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アソシエートします。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。

a. [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。

b. 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）。

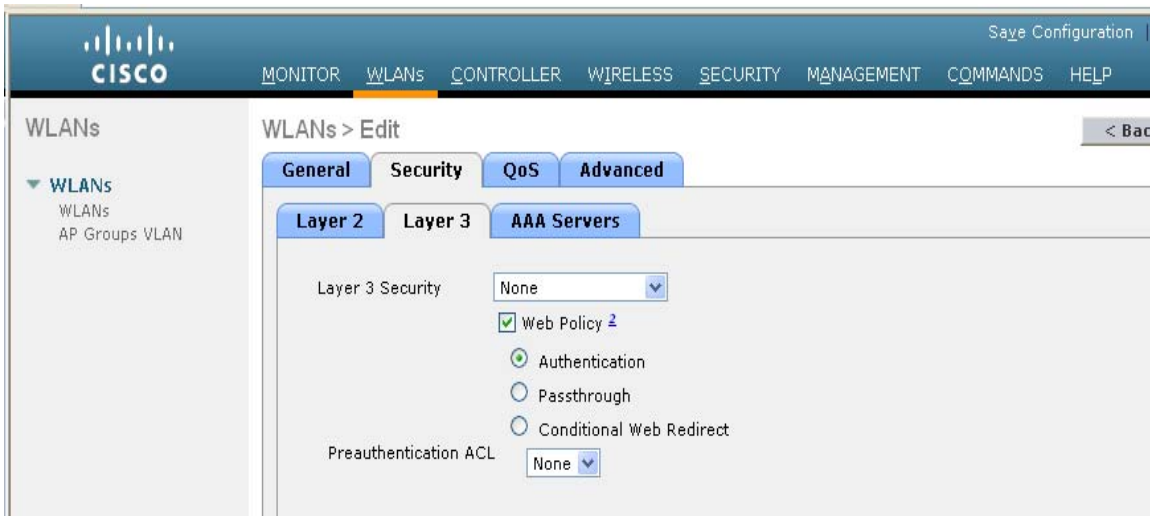
図 10-19　ゲスト WLAN の一般ポリシーの定義

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 10-21 を参照）。

図 10-21　ゲスト WLAN のレイヤ 3 セキュリティ設定



ステップ 6　[Web Policy] チェックボックスをオンにします（追加オプションのリストが表示されます）。

WLC が認証前にクライアント間で DNS トラフィックを受け渡しすることを示す、警告のダイアログ ボックスが表示されます。

ステップ 7　Web ポリシーに [Authentication] または [Pass-through] を選択します（「ゲスト ユーザの認証」（P.10-12）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 10-22 を参照）。

図 10-22　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 10-23 を参照）。

図 10-23　　ゲスト WLAN の高度な設定

ステップ 11　セッション タイムアウトを設定します（オプション）。

（注）　セッション タイムアウトが 0（デフォルト）より大きくなると、有効期限後に強制的に認証が解除され、ユーザは Web ポータルで再認証を要求されます。

ステップ 12　[DHCP Addr. Assignment] を [Required] に設定します。

（注）　ゲスト ユーザが、静的 IP 設定を使用してゲスト ネットワークの使用を試みるのを防ぐため、[DHCP Addr. Assignment] を [Required] に設定することを推奨します。

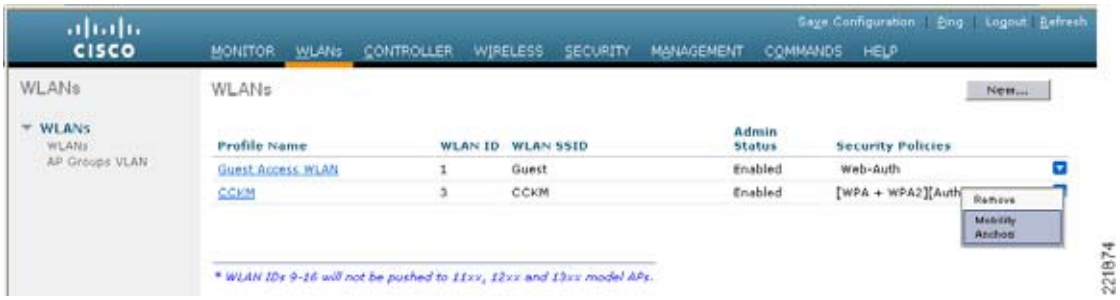
ステップ 13　最後に、[Apply] をクリックします

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 10-24 を参照）。

図 10-24　　WLAN モビリティ アンカー



ステップ 3　[Switch IP Address (Anchor)] プルダウン選択リストで、ネットワーク DMZ 内で展開されたアンカー WLC の管理インターフェイスに対応する IP アドレスを選択します。これは、「外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加」（P.10-19）で設定されたものと同じ IP アドレスです。

ステップ 4　[Mobility Anchor Create] をクリックします （図 10-26 を参照）。

図 10-25　[Switch IP Address (Anchor)] からの管理インターフェイスの選択

図 10-26　WLAN モビリティ アンカーの選択

ゲスト WLAN モビリティ アンカーの確認

設定されると、図 10-27 に示す画面には、ゲスト WLAN に割り当てられたモビリティ アンカー（上記で選択）が表示されます。

図 10-27　ゲスト WLAN モビリティ アンカーの確認

確認作業を容易にするために、ページには、モビリティ トンネル データ パスと CAPWAPP 制御パスがアンカーで設定されているかどうかが表示されます。両方または片方が「down」と表示されている場合には、「ゲスト アクセスのトラブルシューティング」（P.10-57）でトラブルシューティングのヒントを参照してください。右側のプルダウン選択リストには、宛先アンカー WLC に ping を送信するオプションがあります。

ステップ 5　終了する場合は、[Back] をクリックします。

ステップ 6　展開されている追加の各アンカー WLC（ゲスト N+1 冗長性）に対して、上記の手順を繰り返します。

これで、ゲスト WLAN の設定は終了です。ゲスト WLAN をサポートする追加の各外部 WLC に対して、外部 WLC：ゲスト WLAN の設定からゲスト WLAN モビリティ アンカーの確認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。

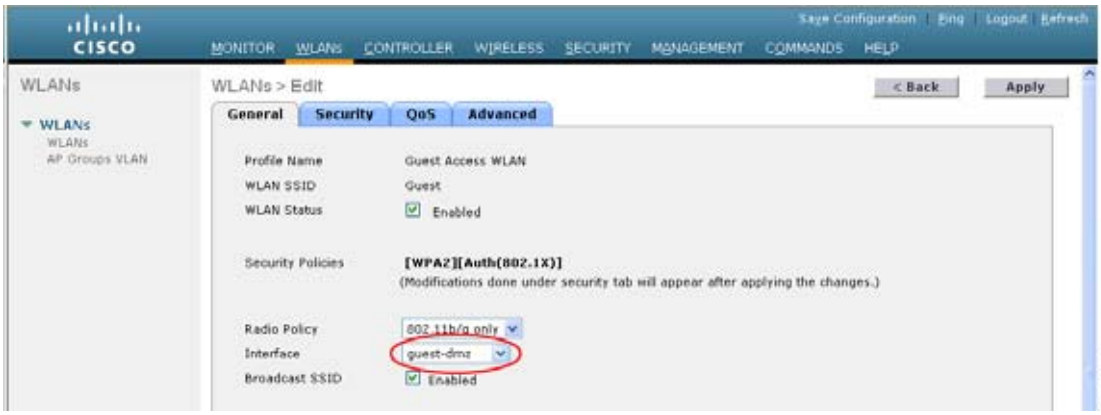
ステップ 1　[WLANs] タブをクリックします。

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 10-28 を参照）。

ステップ 3　[Apply] をクリックします。

図 10-28　アンカー WLC ゲスト WLAN インターフェイスの設定



アンカー WLC：ゲスト WLAN モビリティ アンカーの定義

外部 WLC とは設定が異なる 2 つ目のパラメータは、WLAN モビリティ アンカー設定です。ゲスト WLAN モビリティ アンカーは、アンカー WLC 自体です。

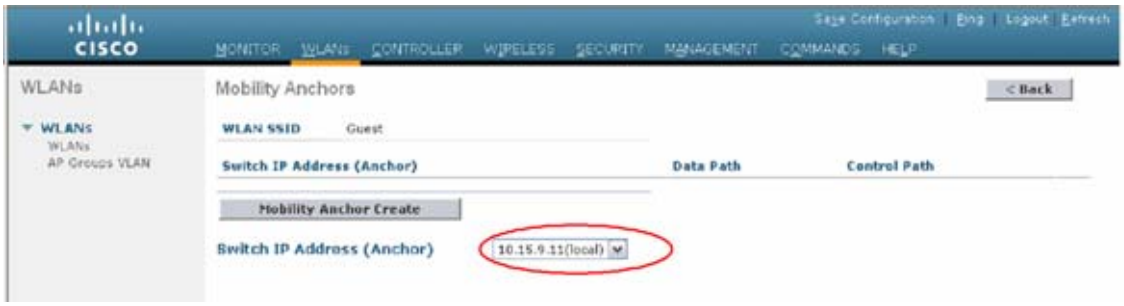
ステップ 1　[WLANs] タブをクリックします。

ステップ 2　ゲスト WLAN を探して、[Mobility Anchors] をクリックします。

ステップ 3　プルダウン選択リストから、アンカー コントローラを表す IP アドレスを選択します。この IP アドレスの隣に「(Local)」と表示されています。

ステップ 4　[Mobility Anchor Create] をクリックします。（図 10-29 を参照）。

図 10-29　ゲスト WLAN モビリティ アンカーの定義



ゲスト WLAN モビリティ アンカーは、*ローカル*であることに注意してください（図 10-30 を参照）。

図 10-30　ゲスト モビリティ アンカーの確認

ゲスト WLAN のモビリティ アンカーはアンカー WLC 自体なので、データとコントロール パスのステータスは常に「up」と表示されます。「up」と表示されない場合、ローカル WLC をアンカーとして [Switch IP Address (Anchor)] ドロップダウン メニューから選択したことを確認します。

ステップ 5　ゲスト N+1 冗長性を実装している場合、展開されている追加のアンカー WLC ごとに WLAN の設定を繰り返します。それ以外の場合、これでゲスト WLAN をアンカー WLC 上で作成するのに必要な設定手順が完了します。

ゲスト アカウント管理

- ゲスト資格情報をローカルのアンカー コントローラ上で管理する場合は、次のいずれかの方法で資格情報を作成して適用できます。
- 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 4.1.83 以降がインストールおよび設定され、Lobby Ambassador のアカウントが作成されているものとします。

（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 10-31 を参照）。

図 10-31　Lobby Ambassador

ログインすると、図 10-32 に示すような画面が表示されます。

図 10-32　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 10-33 を参照）。

図 10-33　ゲスト ユーザ テンプレート オプション

ゲスト ユーザの追加テンプレートの使用

ステップ 1　プルダウン選択リストから、[Add Guest User] を選択して [GO] をクリックします。

ステップ 2　図 10-34 に示すようなテンプレートが表示されます。

図 10-34　　ゲスト ユーザの追加テンプレート

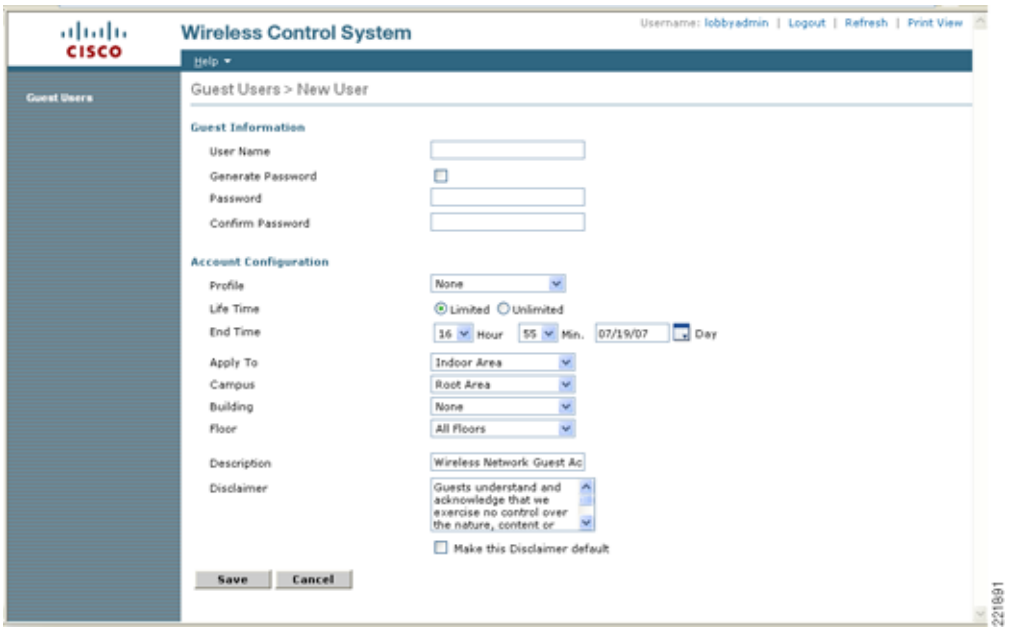
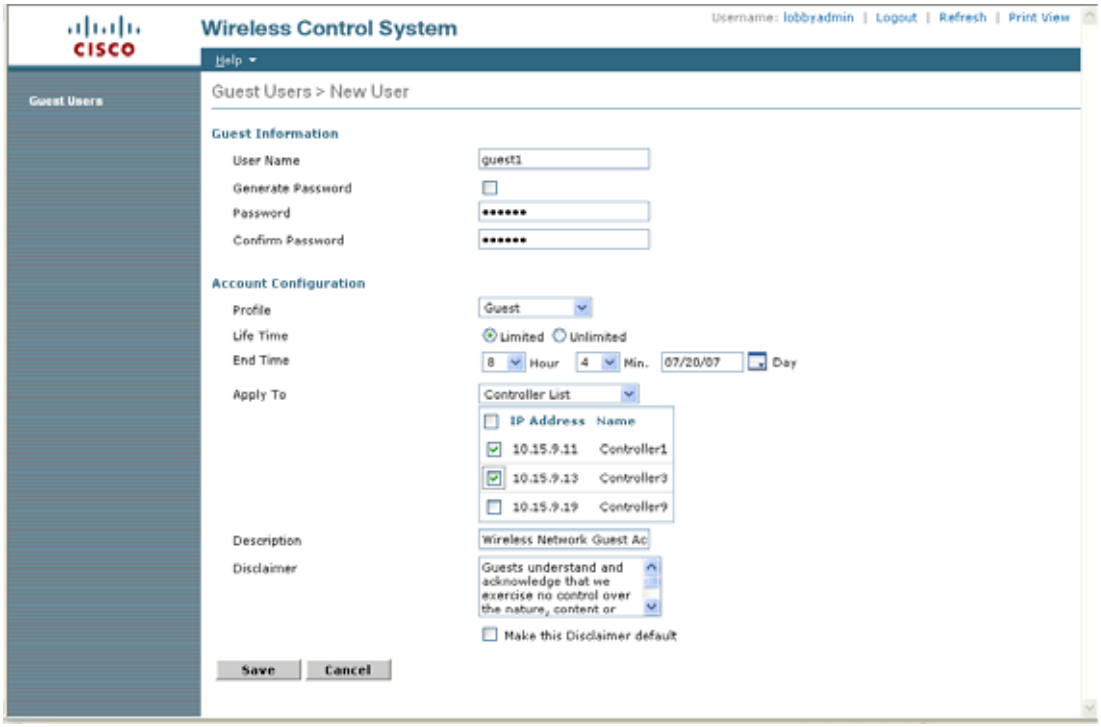


図 10-35 は、ゲスト ユーザ アカウント作成の例を示しています。

図 10-35　ゲスト ユーザ アカウントの作成



ステップ 3　[Guest Information] にユーザ名とパスワードを入力します。

パスワードは大文字と小文字が区別されます。ユーザ名は、24 文字以下に制限されています。管理者には、[Generate Password] チェックボックスを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。

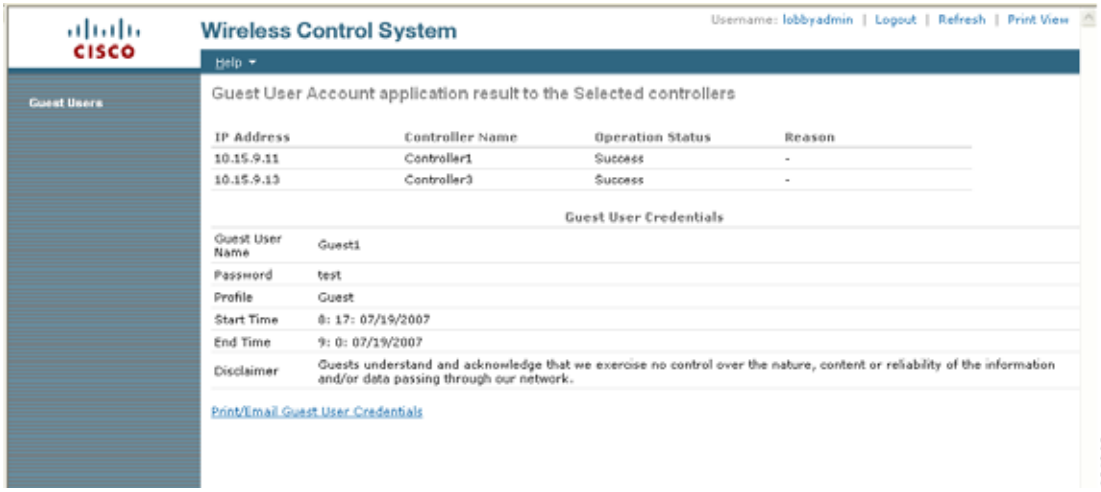
- [Profile]：プルダウン選択リストに、L3 Web ポリシーが設定された WLAN（SSID）のリストが表示されます。
- [Life Time]：[Limited] または [Unlimited] を選択します。
- [End Time]：ゲスト アカウントが [Limited] の場合、資格情報の有効期限が切れる月、日、時刻を選択します。
- [Apply To]：プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。他に表示されるコントローラがありますが、これらは外部 WLC を表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 10-35 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的/地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1）WLAN 展開が管理システム 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 E メールにも含まれ、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。
- [Disclaimer]：ゲスト ユーザに送信できる E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

ステップ 5　完了したら、[Save] をクリックします。図 10-36 に示すサマリ画面が表示され、資格情報がアンカー コントローラに適用されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

図 10-36　ゲスト アカウントの正常な作成



ステップ 6　[Print/Email Guest User Credentials] をクリックします。図 10-37 に示すような画面が表示されます。

図 10-37　ゲスト ユーザ詳細の印刷または E メールでの送信

（注）　ゲスト アカウント情報のユーザへの E メール送信をサポートするように SMTP メール サーバを設定する方法の詳細は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html）を参照してください。

アカウントの詳細を印刷または E メールで送信すると、図 10-38 に示すような画面が表示されます。[User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、[User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択することにより、ゲスト アカウントを削除できます。

図 10-38　Cisco Prime Infrastructure ゲスト ユーザのサマリ

（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は、『Wireless Control System Configuration Guide』（http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html）を参照してください。

図 10-39 は、ゲスト ユーザ テンプレート オプションを示しています。

図 10-39　ゲスト ユーザ テンプレート オプション

ステップ 1　プルダウン選択リストから、[Schedule Guest User] を選択して [Go] をクリックします。

図 10-40 に示すようなテンプレートが表示されます。

図 10-40　ゲスト ユーザのスケジュール テンプレート

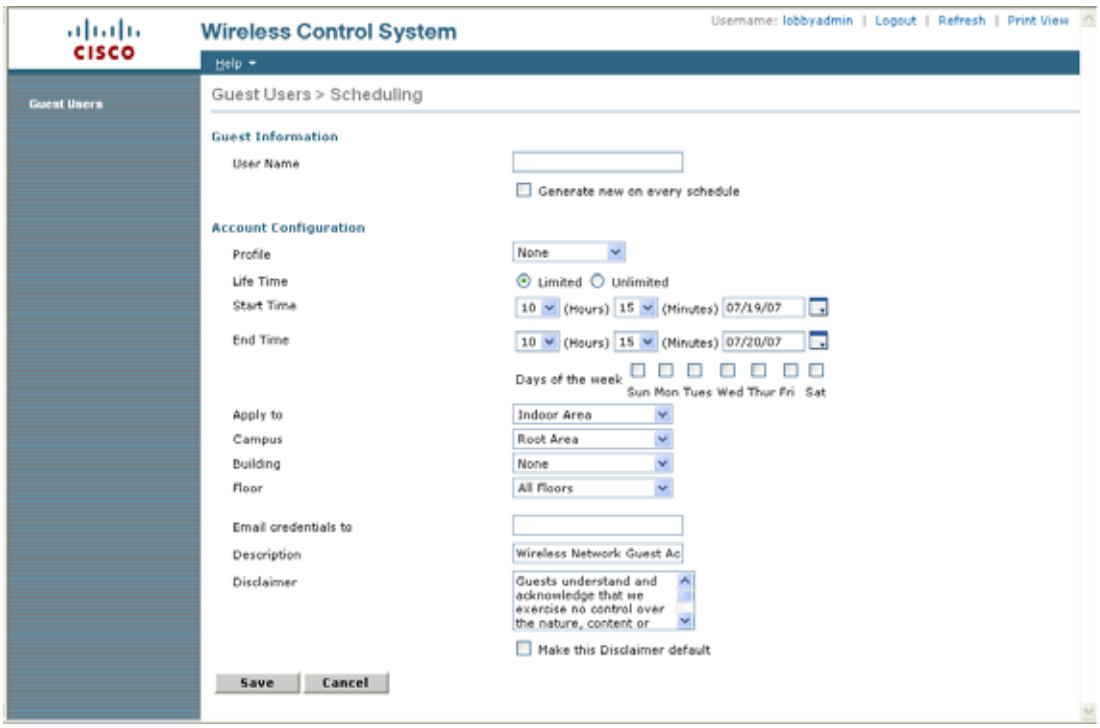
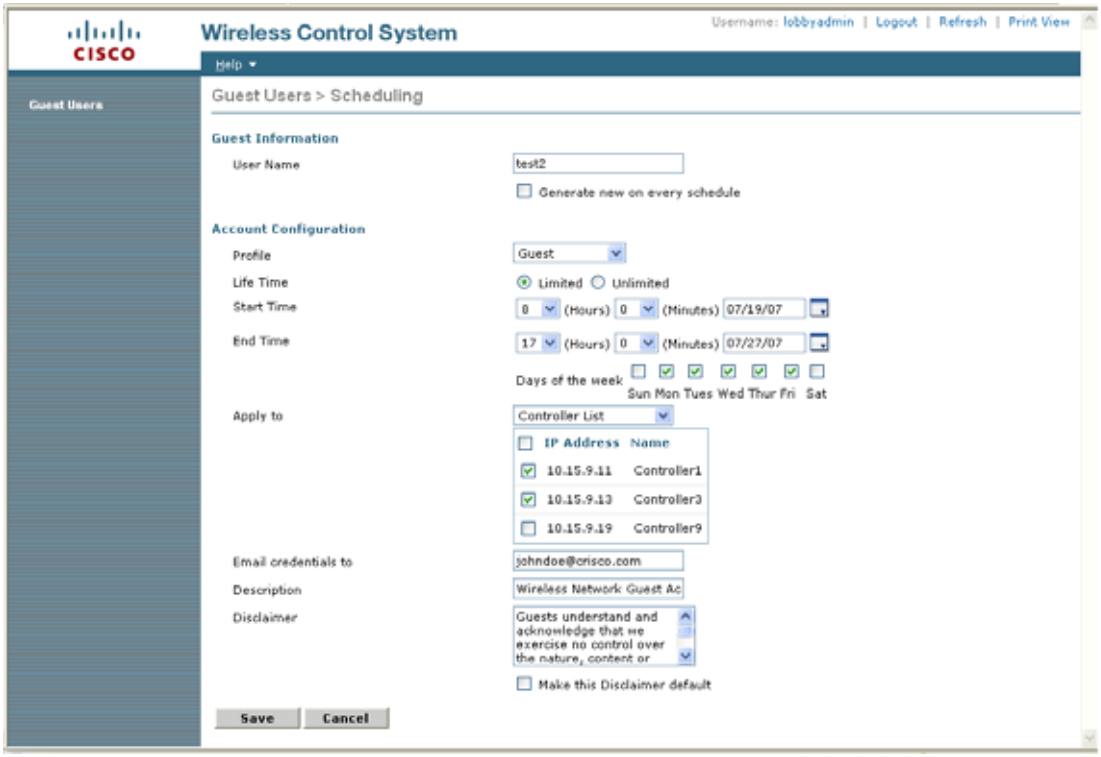


図 10-41 は、ゲスト ユーザ アカウントのスケジュールの作成例を示しています。

図 10-41　　ゲスト ユーザ アカウントのスケジュールの作成



ステップ 2　[Guest Information] にユーザ名を入力します。ユーザ名の長さは、24 文字まで可能です。スケジュールベースのテンプレートを使用する場合、管理者には、アクセスが提供される新しい日ごとに、ユーザ名が自動生成できるように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 ポリシーが設定された WLAN（SSID）のリストが表示されます。
- [Life Time]：[Limited] または [Unlimited] を選択します。
- [Start Time]：アカウントがアクティブになる時刻、月、日を選択します。

（注）　開始時刻は、アカウントが作成される当日に開始することはできません。開始日は、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 E メールで送信され、新しい資格情報が適用可能な WLC に再適用されます。[Days of the Week] が定義されていない場合、開始日時に基づいてアクセスが開始され、終了日時まで常にアクティブになります。

- [Apply To] : プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。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 10-41 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的 / 地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーション ベースのアクセス方法を使用できるのは、1）WLAN 展開が Cisco Prime Infrastructure マッピング データベースに統合されている場合、2）ゲスト WLAN（Web ポリシーが設定された WLAN）がモビリティ アンカーを使用しない場合に限られます。

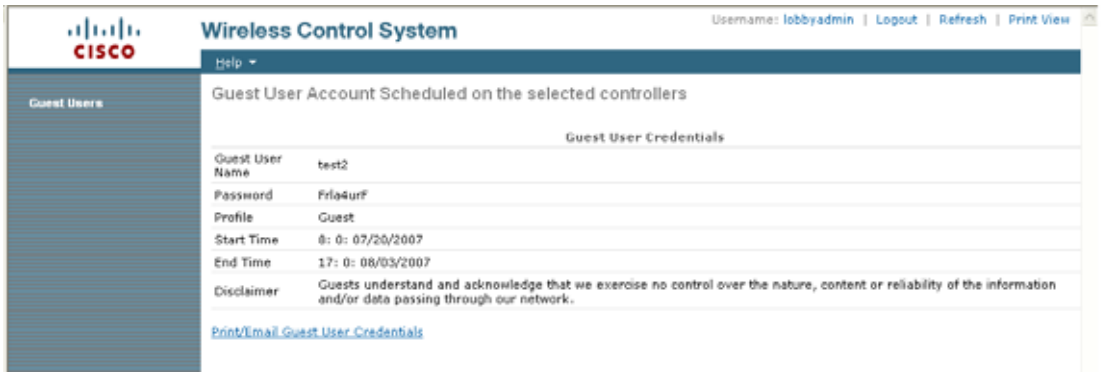
- [E-mail Credentials to] : アカウントを設定するユーザの E メール アドレスを入力します。これは必須フィールドです。

（注）　SMTP メール サーバは、ゲスト アカウント情報の送信に使用できるように、Cisco Prime Infrastructure で設定する必要があります。詳細については、次の項を参照してください。
http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0admin.html

- [Description] : 説明を入力します。説明は、[Security] > [Local Net Users] で資格情報を適用する WLC に表示されます。説明は、ゲストに送信できる E メールにも含まれ、どのような資格情報をネットワークへのアクセスに使用するかを知らせます。
- [Disclaimer] : ゲスト ユーザに送信される E メールで使用され、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。

ステップ 4　完了したら、[Save] をクリックします。図 10-42 に示す画面が表示され、スケジュールされたアカウントが作成されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

図 10-42　スケジュールされたアカウントの正常な作成



ステップ 5　必要に応じて、[Print/Email Guest User Credentials] をクリックします。図 10-43 に示すような画面が表示されます。

図 10-43　ゲスト ユーザ詳細の印刷または E メールでの送信

アカウントの詳細を印刷または E メールで送信すると、図 10-44 に示すようなサマリ画面が表示されます。[User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、[User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択することにより、ゲスト アカウントを削除できます。

図 10-44　Cisco Prime Infrastructure ゲスト ユーザのサマリ

（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」（P.10-6）を参照してください。

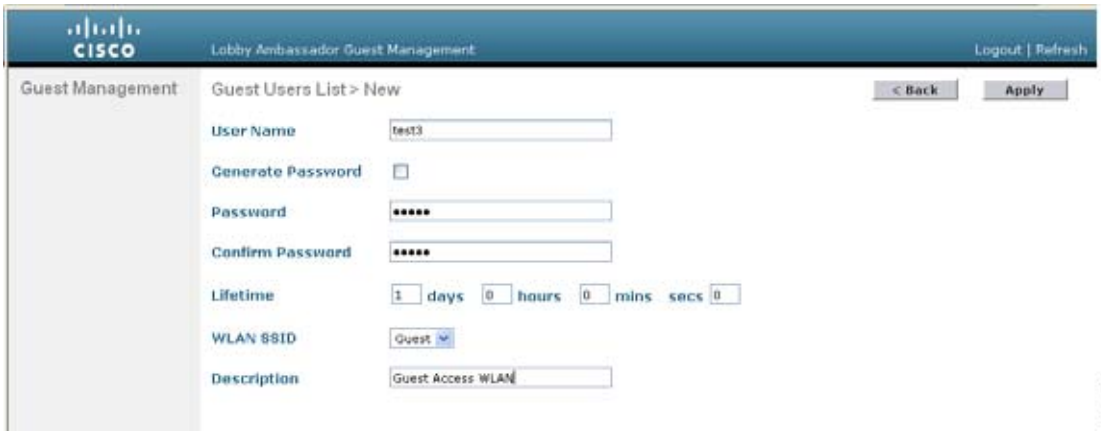
ログインすると、図 10-53 に示すような画面が表示されます。

図 10-45　アンカー コントローラのログイン

ステップ 2　[New] をクリックします。

図 10-46 に示すような画面が表示されます。

図 10-46　ローカル WLC ゲスト資格情報の作成



ステップ 3　ユーザ資格情報を作成するには、次の手順を実行します。

a. ユーザ名とパスワードを入力します（手動または自動）。

b. ゲスト アカウントを適用する WLAN/SSID を選択します。その際、L3 Web ポリシーが設定された WLAN だけが表示されます。

c. 資格情報の有効期間を入力します。

d. ユーザの説明を入力します。

ステップ 4　[Apply] をクリックします。

図 10-47 に示すような画面に、新しく追加されたゲスト ユーザが表示されます。

図 10-47　アンカー WLC ゲスト ユーザのリスト

この画面では、次の機能を実行できます。

- 既存のユーザの編集（右端のリンク。非表示）
- 既存のユーザの削除（右端のリンク。非表示）
- 新規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 512 です。この値は、次の手順を実行することによって変更できます。

ステップ 1　[Security] タブをクリックします。（図 10-48 を参照）。

図 10-48　ユーザ アカウントの最大数の設定

ステップ 2　左側のペインで、AAA プロパティの下の [General] をクリックします。

ステップ 3　ユーザ データベース エントリの最大数を設定します（512 ～ 2,048 の間）。

ステップ 4　[Apply] をクリックします。

最大同時ユーザ ログイン

WWLC 上のローカル ユーザ アカウントの同時ログインの最大数は、設定が可能です。同時ログイン数を無制限にする場合は、値を 0 にします。値を 1 ～ 8 に制限することもできます。ユーザ ログインの最大数は、次の手順で設定されます。

ステップ 1　[Security] タブをクリックします。（図 10-49 を参照）。

図 10-49　　ユーザ ログイン ポリシー

ステップ 2　左ペインで、[AAA] の [User Login Policies] をクリックします。

ステップ 3　同時ユーザ ログインの最大数を設定します（0 ～ 8 の間）。

ステップ 4　[Apply] をクリックします。

ゲスト ユーザの管理に関する注意事項

次の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。

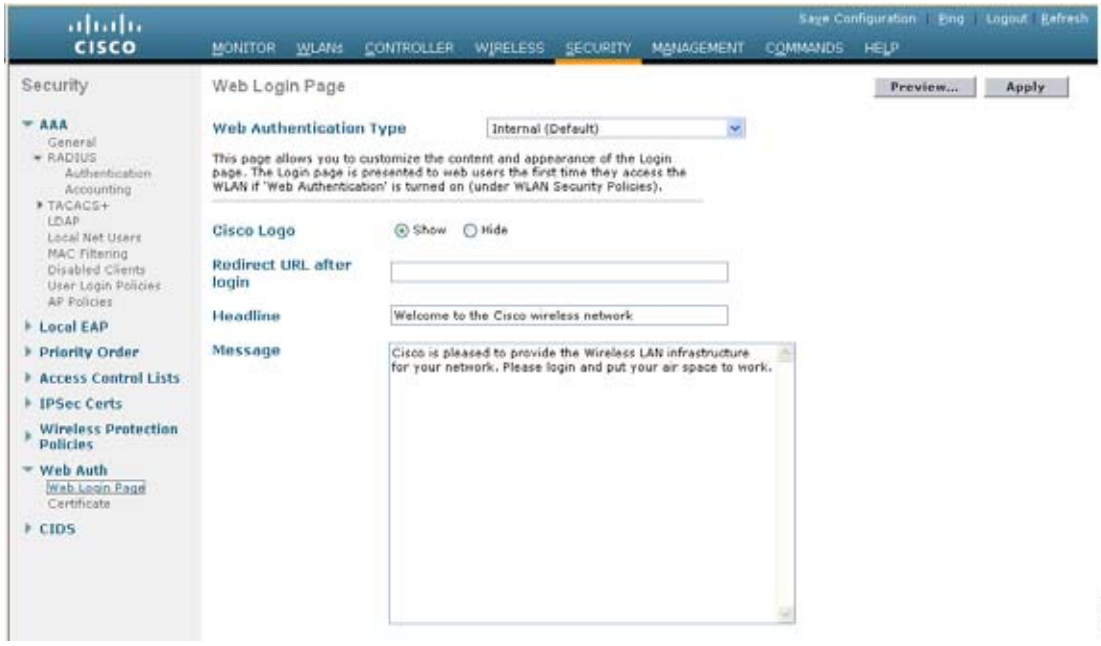
内部 Web ページの管理

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 10-50 に示すような設定画面が表示されます。ポータル ページに表示される見出しとメッセージ情報を変更できます。また、認証後のリダイレクト URL を選択することもできます。

図 10-50　Web ログイン ページ設定画面



ステップ 3　[Apply] をクリックします。

ステップ 4　必要に応じて、[Preview] をクリックして、ユーザに表示されるリダイレクト先のページを確認します。

Web ページのインポート

カスタマイズされた Web ページをダウンロードして、ローカルのアンカー コントローラ上に保存できます。カスタマイズされた Web ページをインポートするには、次の手順を実行します。

ステップ 1　[Commands] タブをクリックします （図 10-51 を参照）。

図 10-51　Web ページのインポート

ステップ 2　[File Type] で [Web Auth Bundle] を選択します。

ステップ 3　ファイルが存在する TFTP サーバの IP アドレスとファイル パスを指定します。

ステップ 4　[Download] をクリックして、ダウンロードを開始します。

Web 認証バンドルをダウンロードする際には、次の点に注意してください。

- プルダウン選択リストから [Web Auth Bundle] を選択して、ファイルがコントローラ上の正しいディレクトリに保存されるようにします。
- [Web Auth Bundle] は、カスタム Web ログイン ページにアソシエートされている、HTML ファイルとイメージ ファイルの **.tar** ファイルである必要があります。ダウンロード後に、WLC によってファイルが untar され、適切なディレクトリに格納されます。
- [Web Auth Bundle]（**.tar** ファイル）は、1MB より大きくてはなりません。
- HTML ログイン ページのファイル名は、**login.html** にする必要があります。

カスタマイズされた Web ページのダウンロードと使用方法の詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcssol.html#wp1065703

インポートした Web 認証ページの選択

コントローラにダウンロードしたカスタマイズ済みの Web 認証ページを使用するには、次の手順を実行します。

ステップ 1　[Security] タブをクリックします。

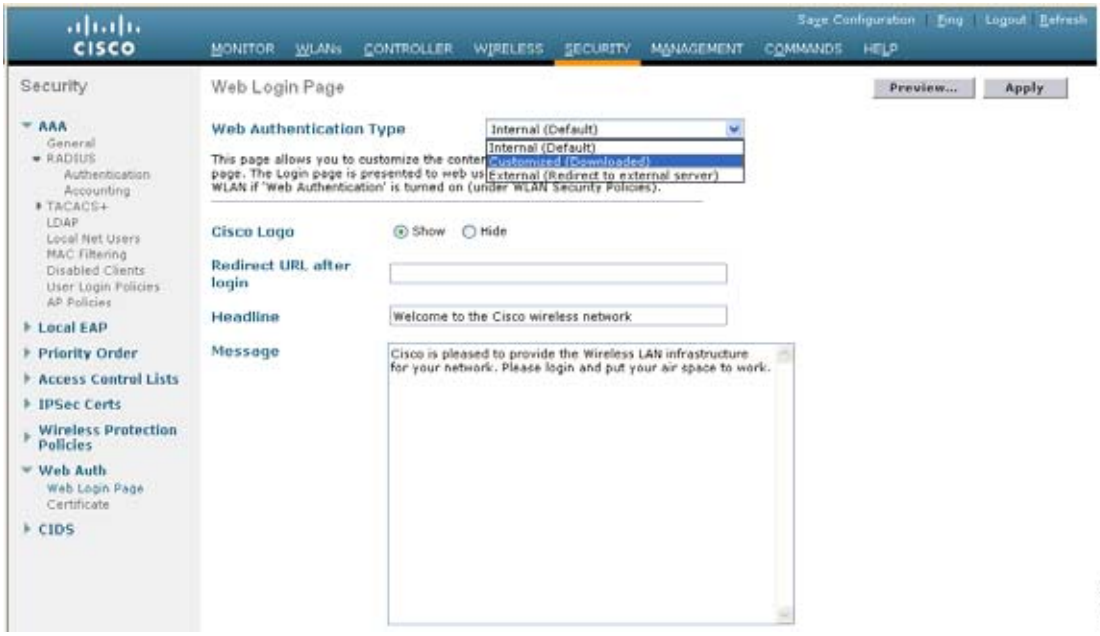
ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。

ステップ 3　[Web Authentication Type] プルダウン選択リストから [Customized (Downloaded)] を選択します。

ステップ 4　[Preview] をクリックして、ダウンロードしたページを表示します。

ステップ 5　最後に、[Apply] をクリックします （図 10-52 を参照）。

図 10-52　インポートした Web 認証ページの選択



内部 Web 証明書の管理

Web 認証ログイン ページでは、ユーザ資格情報を保護するために SSL が使用されます。コントローラでは、簡単な自己署名証明書が使用されます。証明書が自己署名されたものであるため、ゲスト ユーザが図 10-53 に示すような認証ページにリダイレクトされると、次のようなポップアップ アラートが表示されます。

図 10-53　Web 証明書セキュリティ アラート（IE6）

この時点で、[Yes] をクリックして先に進むか、[View Certificate] を選択してそのページを信頼されたサイトとして手動でインストールできます。Web サーバでは、「アンカー WLC の設置およびインターフェイスの設定」（P.10-14）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 アドレスと共に指定する場合は、ホスト名が DNS によって解決されるときに、次の条件を満たすようにする必要があります。

- クライアントが Web 認証ページにリダイレクトされる。
- ユーザが、ホスト名とホスト IP アドレスの矛盾が原因の Web 認証エラーに遭遇しない。

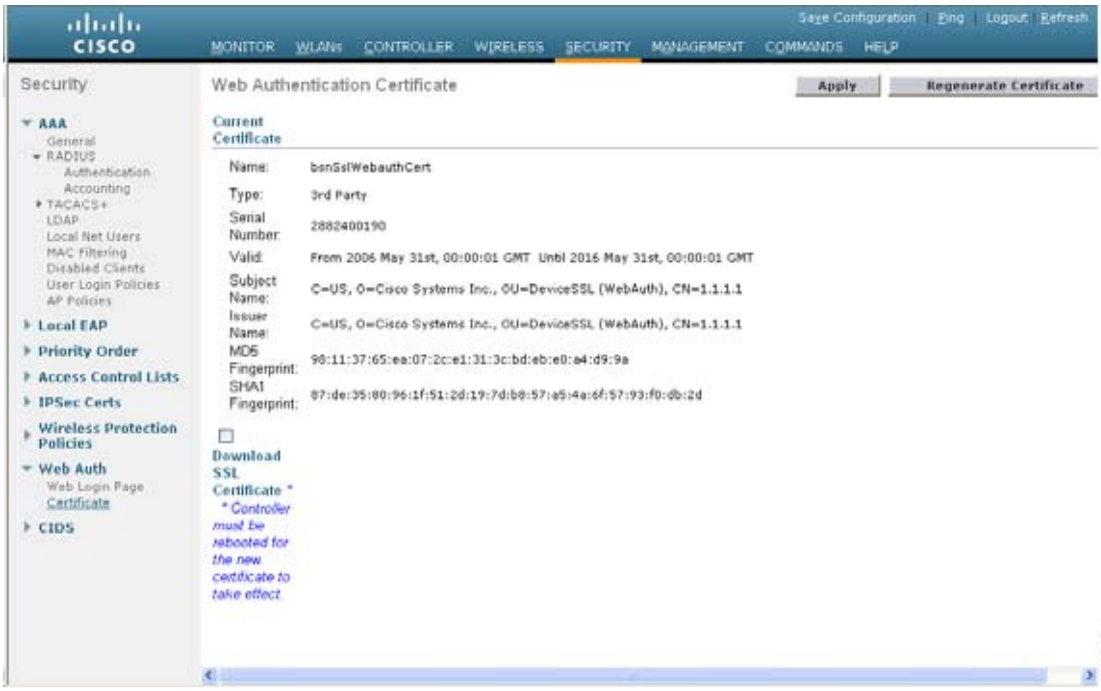
外部 Web 証明書のインポート

信頼できるルート CA によって発行された正式な Web 証明書が必要な場合は、次の手順を実行することによって、コントローラにダウンロードできます。

ステップ 1　[Security] タブをクリックします。

左側のペインで、[Web Auth] をクリックして、[Certificate] をクリックします（図 10-54 を参照）。

図 10-54　外部 Web 証明書のインポート



ステップ 2　[Download SSL Certificate] チェックボックスをオンにします。

ステップ 3　証明書のダウンロードに必要な情報を各フィールドに入力します。

ステップ 4　[Apply] をクリックします。

ステップ 5　証明書をダウンロードしたら、サーバを再起動します。

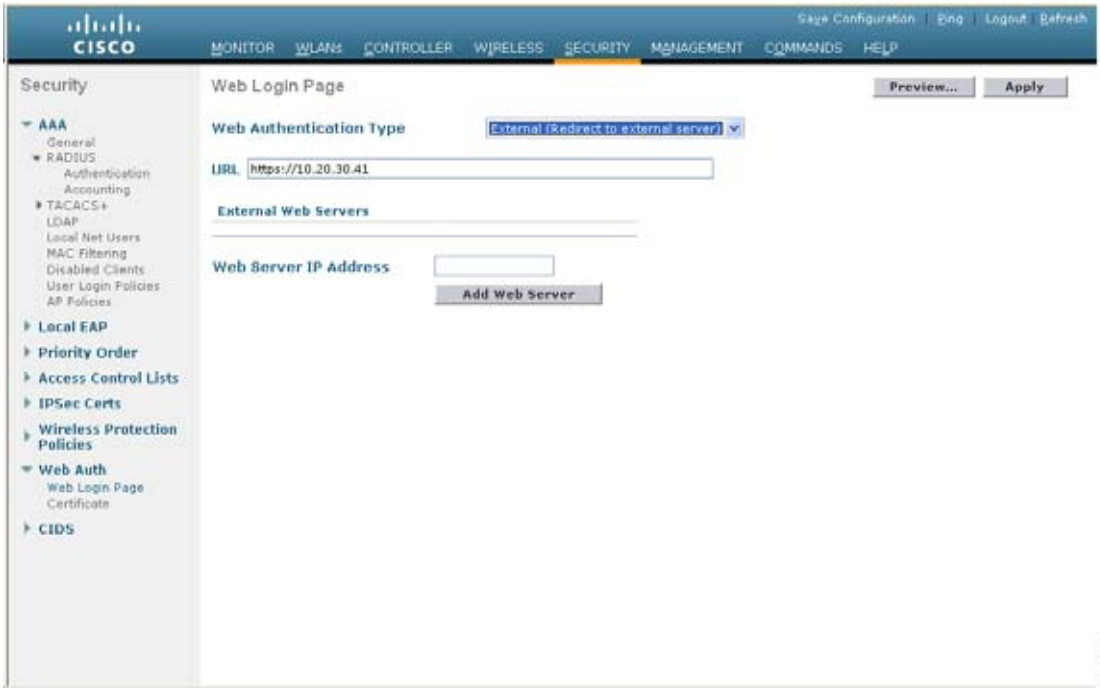
外部 Web リダイレクションのサポート

企業では、有線のゲスト アクセスまたは NAC 機能をサポートする Web ポータル システムがすでに展開されている場合があります。そのような場合は、無線ゲスト ユーザを外部 Web ポータルにリダイレクトするように、アンカー コントローラを次の手順で設定できます。

ステップ 1　[Security] タブをクリックします。

ステップ 2　左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。（図 10-55 を参照）。

図 10-55　外部 Web リダイレクションのサポート



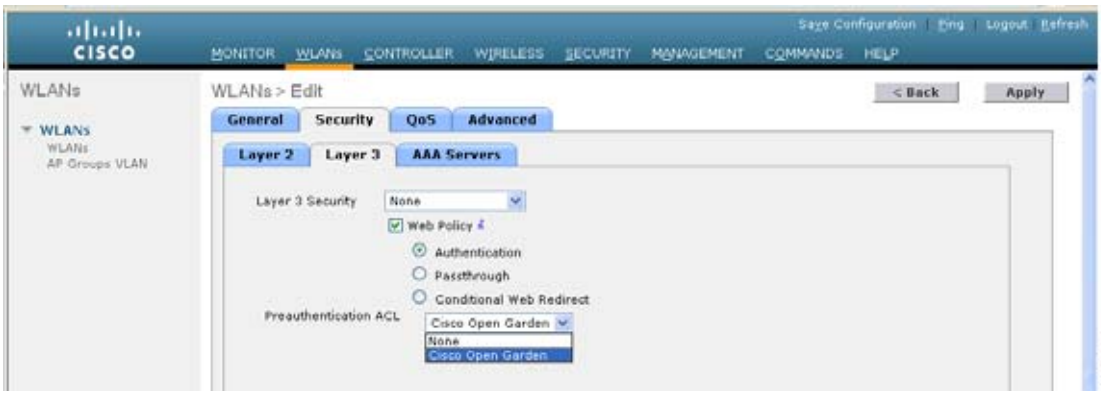
ステップ 3　[Web Server IP] フィールドと [URL] フィールドに入力します。

ステップ 4　[Apply] をクリックします。

アンカー WLC 事前認証 ACL

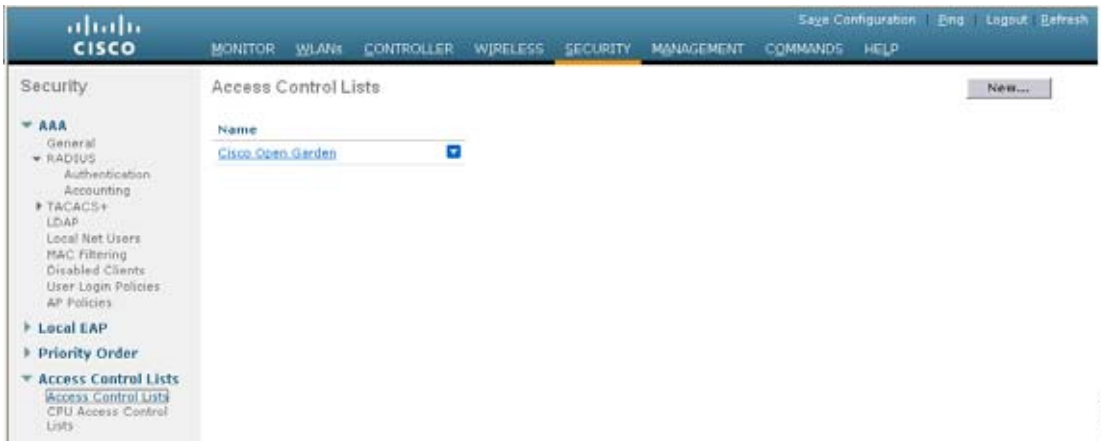
事前認証 ACL は、ゲスト WLAN に適用できます。これにより、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続できます。事前認証 ACL はゲスト WLAN のレイヤ 3 セキュリティ設定で適用されます。有効になっている場合、アンカー WLC 上でのみ実行されます（図 10-56 を参照）。

図 10-56　WLAN 事前認証 ACL



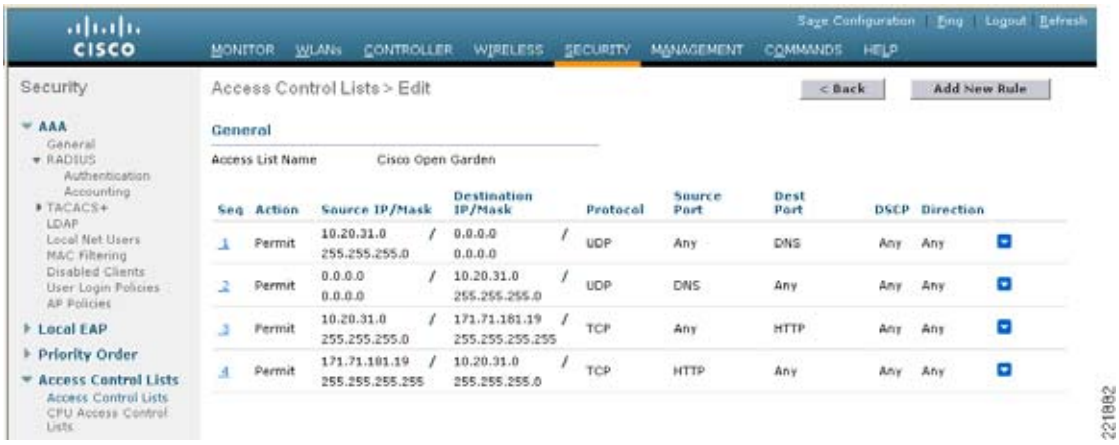
特定の ACL は、[Security] > [Access Control Lists] で設定されます（図 10-57 および図 10-58 を参照）。

図 10-57　WLC アクセス コントロール リスト



（注）　事前認証 ACL が Web 認証ポリシーと共に使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト /URL に解決して接続することができません。

図 10-58　　事前認証 ACL の例



アンカー コントローラ DHCP 設定

アンカー コントローラがゲスト アクセス WLAN の DHCP サービスを管理する場合は、次の手順を実行します。

（注）　アンカー コントローラは、ゲスト N+1 冗長性を実装している場合、DHCP サービスを管理するために使用することはできません。なぜなら、2 つ以上の WLC 間で単一のゲスト VLAN/サブネットのアドレス リースを同期するメカニズムがないからです。

新しい DHCP スコープのアンカー コントローラへの追加

ステップ 1　[Controller] タブをクリックします。

ステップ 2　左側のペインで、[Internal DHCP Server] をクリックします。

ステップ 3　[New] をクリックします。（図 10-59 を参照）。

図 10-59　新しい DHCP スコープの追加

スコープ名の定義

ステップ 4　スコープ名を定義して、[Apply] をクリックします。（図 10-60 を参照）。

図 10-60　スコープ名の定義

ステップ 5　[Scope Name] をクリックして、編集します （図 10-61 を参照）。

図 10-61　DHCP スコープの編集

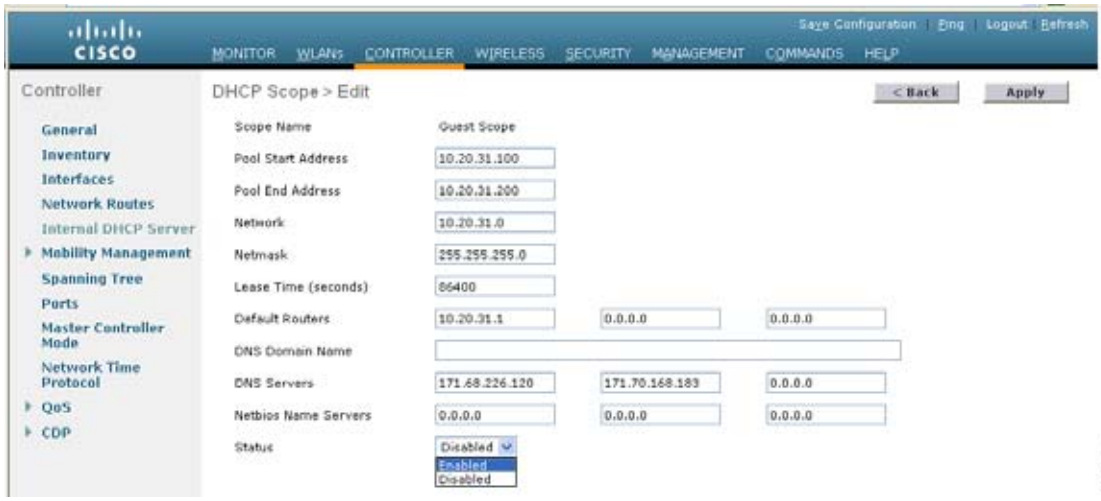
スコープ プロパティの定義

ステップ 6　最低限必要な次の情報を定義します。

- プールの開始と終了
- ネットワーク
- マスク
- デフォルト ルータ
- DNS サーバ

ステップ 7　[Status] として [Enabled] を選択し、[Apply] をクリックします （図 10-62 を参照）。

図 10-62　スコープ プロパティの設定と有効化



外部 RADIUS 認証

ゲスト ユーザの認証で説明したように、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。

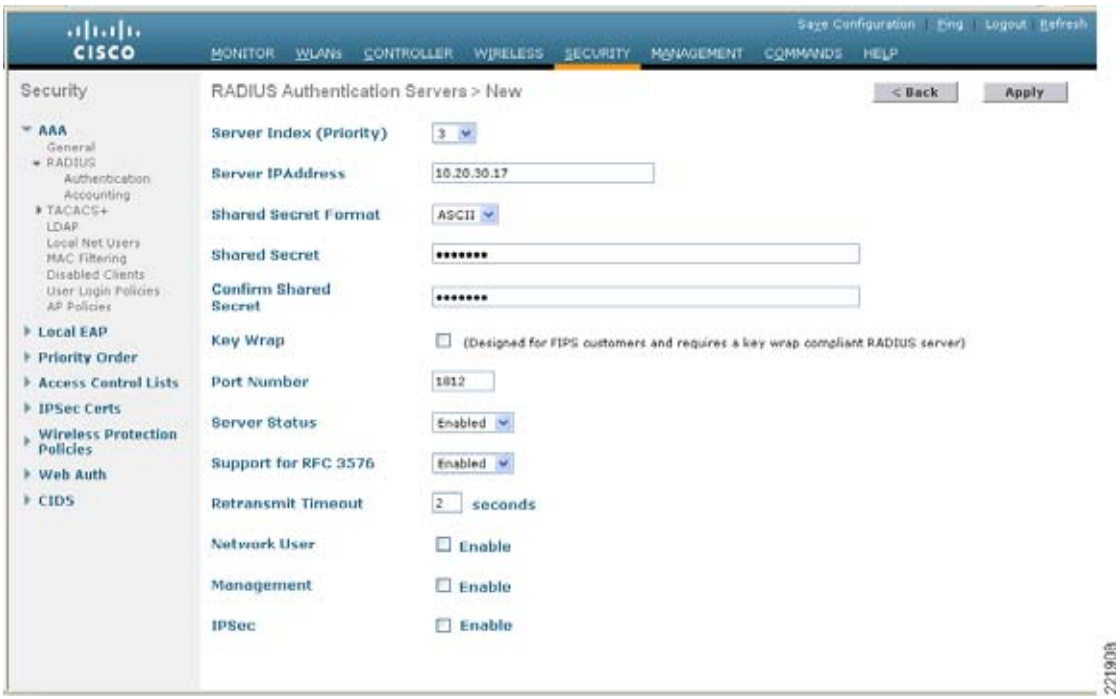
サマリ画面が表示されます （図 10-63 を参照）。

図 10-63　[Summary] 画面

ステップ 2　[New] をクリックします。

図 10-64 に示すような画面が表示されます。

図 10-64　RADIUS サーバ設定の定義



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。

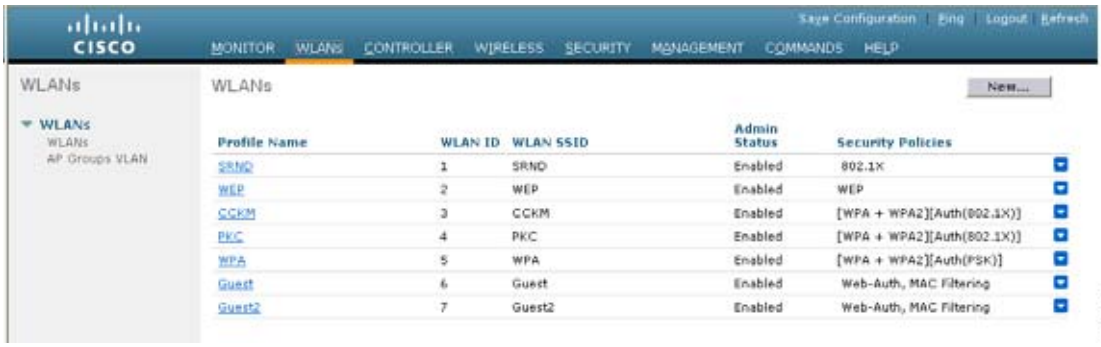
図 10-65 に示すサマリ画面には、新しく追加されたサーバが表示されます。

図 10-65　[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 10-66 に示すような画面が表示されます。

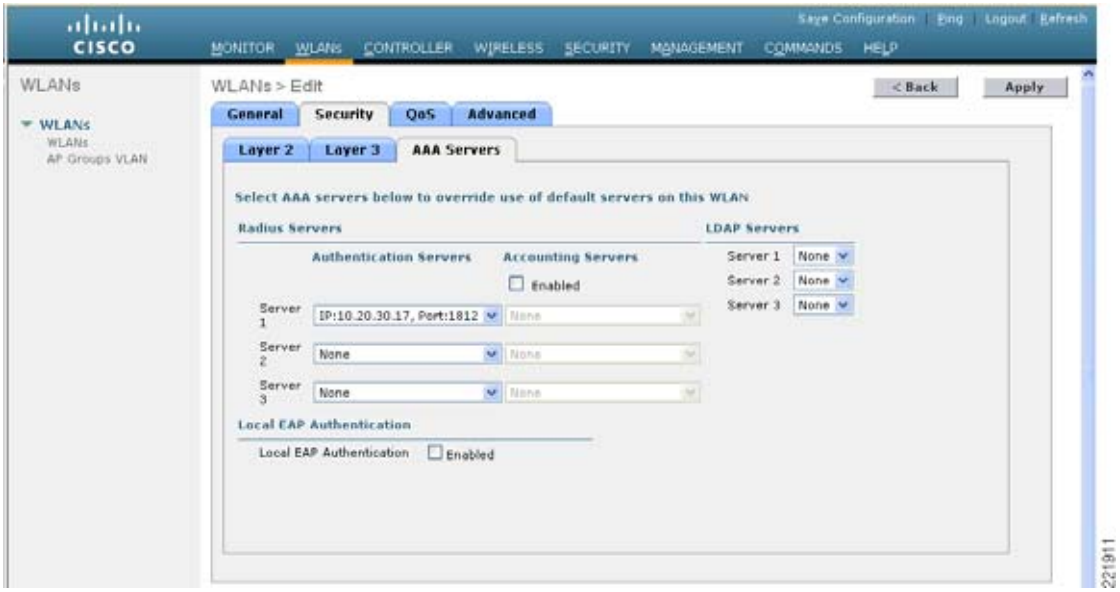
図 10-66　[WLANs] タブ



ステップ 6　ゲスト WLAN を探して、その [Profile Name] をクリックします。

図 10-67 に示すように、ゲスト WLAN の設定画面が表示されます。

図 10-67　ゲスト WLAN の設定画面



ステップ 7　[WLAN Security] タブで [AAA Servers] を選択します。

ステップ 8　[Authentication Servers] のプルダウン選択リストから、Web 認証に使用する RADIUS サーバを選択します。

外部アクセス コントロール

この章で説明した中央集中型ゲスト アクセス トポロジは、Cisco NAC Appliance などの外部アクセス コントロール プラットフォームと統合できます。

このシナリオでは、企業で、有線ゲスト アクセス サービスをサポートするためのアクセス コントロール プラットフォームがインターネットの DMZ に展開されているものとします（図 10-68 を参照）。

図 10-68　外部アクセス コントロールを使用した無線ゲスト アクセス

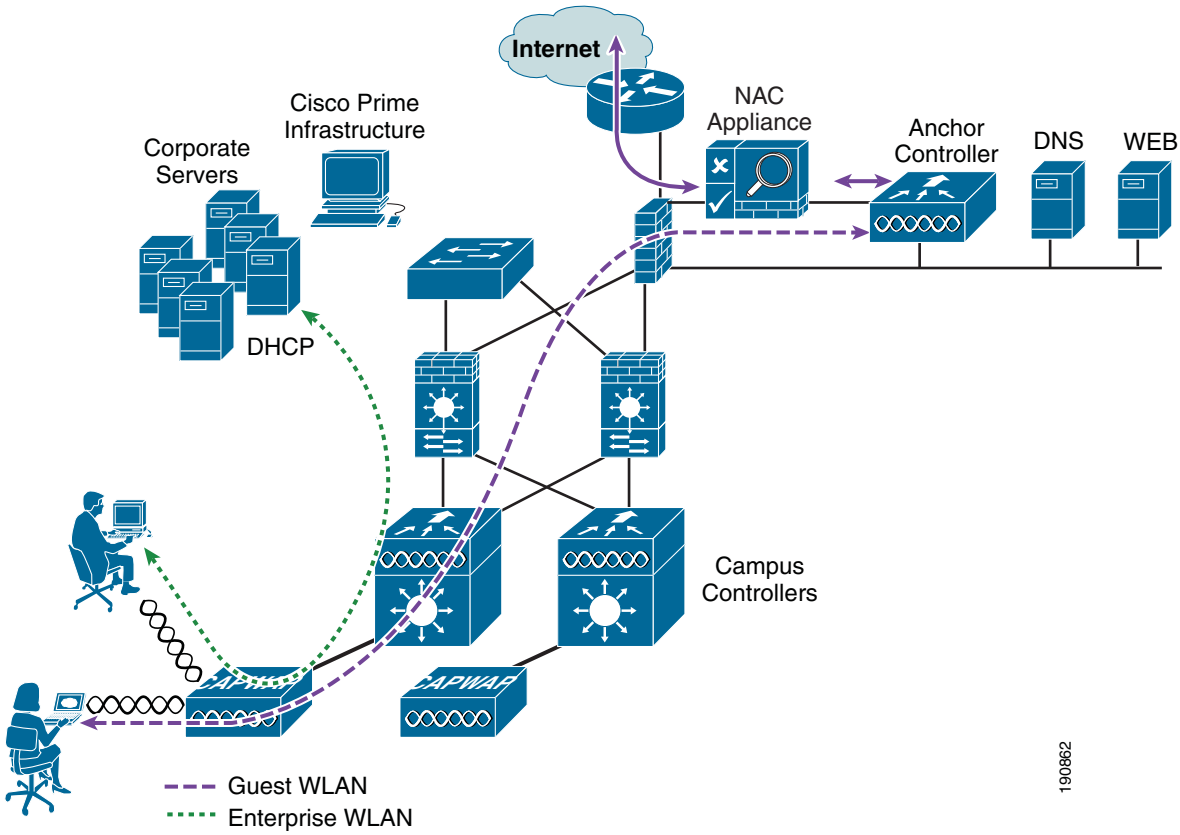


図 10-68 に示すように、無線ゲスト アクセス トポロジは、アンカー コントローラ上のゲスト VLAN インターフェイスが、ファイアウォールや境界ルータに接続する代わりに Cisco NAC Appliance などのアクセス コントロール プラットフォームの inside インターフェイスに接続する点を除いて同じです。

このシナリオでは、NAC Appliance が、リダイレクション、Web 認証、およびその後のインターネットへのアクセスを処理します。キャンパス コントローラとアンカー コントローラは、NAC アプライアンスまたはその他のいくつかのプラットフォームを使用してゲスト アクセスを制御している DMZ に全社的なゲスト WLAN トラフィックをトンネルするためだけに使用されます。

ゲスト WLAN、キャンパス、およびアンカー コントローラの設定は、上記の例と同じです。

唯一の違いは、ゲスト WLAN のセキュリティ設定でレイヤ 3 Web ポリシーが有効になっていない点です（図 10-69 および図 10-70 を参照）。

図 10-69　　ゲスト WLAN のレイヤ 3 セキュリティ ポリシー

図 10-70　　ゲスト WLAN L2 セキュリティ設定

上記の設定では、セキュリティ ポリシーを使用せずに WLAN が設定されます。ゲスト トラフィックは、アンカー コントローラを通過して、Cisco NAC Appliance の inside インターフェイスまたは信頼されていないインターフェイスに到達し、ユーザが認証されるまでブロックされます。

DHCP は、ローカルのコントローラ上でホストするか、外部の NAC Appliance または専用サーバ経由でホストできます。

Cisco NAC Appliance またはその他の外部アクセス コントロール プラットフォーム固有の設定については、この章では説明しません。詳しい設定ガイドラインについては、プラットフォーム固有のマニュアルを参照してください。

ゲスト アクセス機能の確認

ゲスト アクセス サービスは、ユーザが次の条件を満たしている場合に正しく機能します。

- ゲスト WLAN にアソシエートできる。
- DHCP 経由で IP アドレスを受信する。
- ブラウザを開くと、Web 認証ページにリダイレクトされる。
- 資格情報を入力して、インターネット（またはその他の許可されたアップストリーム サービス）に接続する。

ゲスト アクセスのトラブルシューティング

以降の確認作業とトラブルシューティング作業は、次のことを前提としています。

- このソリューションでは、アンカー コントローラ上の Web 認証機能が使用されている。
- ユーザ資格情報が、ローカルのアンカー コントローラ上で作成および保存されている。

次のようなさまざまな症状のトラブルシューティングを実行するには、少なくとも、外部のキャンパス コントローラからアンカー コントローラに ping できる必要があります。それが不可能な場合は、ルーティングを確認します。

その次に、次の高度な ping コマンドを実行できる必要があります。これらのコマンドは、コントローラのシリアル コンソール インターフェイスを通してだけ実行できます。

- **mping** *neighbor WLC ip*

  このコマンドは、CAPWAP 制御チャネルを通して近隣のコントローラに ping します。

- **eping** *neighbor WLC ip*

  このコマンドは、CAPWAP データ チャネルを通して近隣のコントローラに ping します。

標準の ICMP ping が通っても mping が通らない場合は、各 WLC のデフォルトのモビリティ グループ名が同じであることと、各 WLC の IP、MAC、およびモビリティ グループ名がすべての WLC のモビリティ メンバ リストに入力されていることを確認します。

ping と mping は通っても eping が通らない場合は、ネットワークで IP プロトコル 97（Ethernet-over-IP）がブロックされていないことを確認します。

ユーザがゲスト WLAN に接続できない

- ゲスト WLAN をサポートするアンカー コントローラとすべての外部コントローラでゲスト WLAN が有効になっていることを確認します。
- ゲスト WLAN SSID がブロードキャストされていることを確認します。
- クライアント アダプタまたはソフトウェアの設定を確認します。

ユーザが DHCP 経由で IP アドレスを取得できない

- WLAN の設定がアンカー コントローラ上と外部コントローラ上で同じであることを確認します（WLAN インターフェイスおよびモビリティ アンカーを除く。「アンカー WLC 上でのゲスト WLAN の設定」（P.10-28）を参照）。
- ゲスト WLAN がアンカー WLC 上で有効になっていることを確認します。
- アンカー コントローラのゲスト VLAN インターフェイスの設定で、DHCP サーバのアドレスが適切かどうかをチェックします。
  - 外部 DHCP サーバを使用している場合は、IP アドレスが外部サーバのアドレスになっている必要があります。
  - アンカー コントローラから外部 DHCP サーバにアクセスできることを確認します。
  - DHCP サービスにアンカー コントローラを使用している場合は、DHCP サーバの IP アドレスがコントローラの管理 IP アドレスになっている必要があります。
  - コントローラ上で DHCP スコープが設定され有効になっていることを確認します。
  - DHCP スコープのネットワーク マスクとゲスト VLAN インターフェイスのマスクが一致していることを確認します。

– DHCP スコープが、ネットワーク インフラストラクチャに割り当てられたすべてのアドレスと重複していないことを確認します。

ユーザが Web 認証ページにリダイレクトされない

次の解決方法では、ユーザがゲスト WLAN にアソシエートして IP アドレスを取得できることを想定しています。

- 有効な DNS サーバが DHCP を介してクライアントに割り当てられていることを確認します。
- DNS サーバがアンカー コントローラから接続可能なことを確認します。
- Web ブラウザで開かれている URL が解決可能なことを確認します。
- Web ブラウザで開かれている URL が HTTP ポート 80 に接続していることを確認します。

（注）　内部 Web 認証サーバは、80 およびユーザが定義したもう 1 つのポート番号以外のポート上の入力要求をリダイレクトしません（「ユーザ リダイレクション」（P.10-10）参照）。

ユーザが認証されない

- アンカー コントローラ上のユーザ資格情報がアクティブなことを確認します。

  通常は、ゲスト資格情報に対して有効期間が設定されます。資格情報は、期限が切れていると、アンカー コントローラ上の [Security] > [Local Net Users] リストに表示されません。Cisco Prime Infrastructure を使用して、ローカルのコントローラ上でユーザ テンプレートを適用し直すか、ユーザ資格情報を作成し直してください。管理システムを使用したゲスト管理およびゲスト資格情報の管理を参照してください。
- ユーザ パスワードを確認します。

ユーザがインターネットまたはアップストリーム サービスに接続できない

- アンカー コントローラと、アンカー コントローラに接続されているファイアウォールまたは境界ルータ間のルーティングを確認します。
- 必要に応じて、ファイアウォールまたはインターネット境界ルータの NAT 設定を確認します。

システム モニタリング

以降では、トラブルシューティングに役立つ可能性のあるいくつかの監視コマンドについて説明します。

アンカー コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

```
Cisco Controller) >show client summary
Number of Clients................................ 1
MAC Address       AP Name            Status         WLAN  Auth  Protocol  Port
----------------  -----------------  -------------  ----  ----  --------  ----
00:40:96:ac:5f:f8  10.15.9.19         Associated     3     Yes   Mobile    1
```

プロトコルが Mobile になっていることに注目してください。Auth フィールドには、実際のユーザの状態が反映されます。ユーザが Web 認証をパスすると、このフィールドに YES と表示されます。パスしなかった場合は、このフィールドに NO と表示されます。

AP 名にも注目してください。これは、外部コントローラ（起点コントローラ）の管理 IP アドレスです。

サマリ情報に示されたクライアントの MAC アドレスを使用して、詳細を表示します。

```
(Cisco Controller) >show client detail 00:40:96:ac:5f:f8
Client MAC Address.............................. 00:40:96:ac:5f:f8
Client Username ................................ romaxam
AP MAC Address.................................. 00:00:00:00:00:00
Client State.................................... Associated
Wireless LAN Id................................. 3
BSSID........................................... 00:00:00:00:00:02
Channel......................................... N/A
IP Address...................................... 10.20.31.100
Association Id.................................. 0
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 86316
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Anchor
Mobility Foreign IP Address..................... 10.15.9.19
Mobility Move Count............................. 1
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... wlan-user
VLAN............................................ 31
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Not implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 0
      Number of Bytes Sent...................... 0
      Number of Packets Received................ 0
      Number of Packets Sent.................... 0
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... Unavailable
      Signal to Noise Ratio..................... Unavailable
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
```

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を得ることができます （図 10-71 を参照）。

図 10-71　[Anchor WLC Monitor] > [Client Detail]

外部のキャンパス コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

```
(WiSM-slot3-1) >show client summary
Number of Clients.............................. 2
MAC Address       AP Name           Status         WLAN  Auth  Protocol  Port
----------------  ----------------  -------------  ----  ----  --------  ----
00:40:96:ac:5f:f8  AP3_.18e5.7fdc    Associated     1     Yes   802.11g   29
```

アンカー コントローラでは Protocol フィールドが Mobile になっていましたが、同じクライアントに対してこの Protocol フィールドは 802.11g になっていることに注目してください。外部のキャンパス コントローラでは、必ずユーザが Authenticated として表示され、AP name にはクライアントがアソシエートされている実際の AP が反映されます。

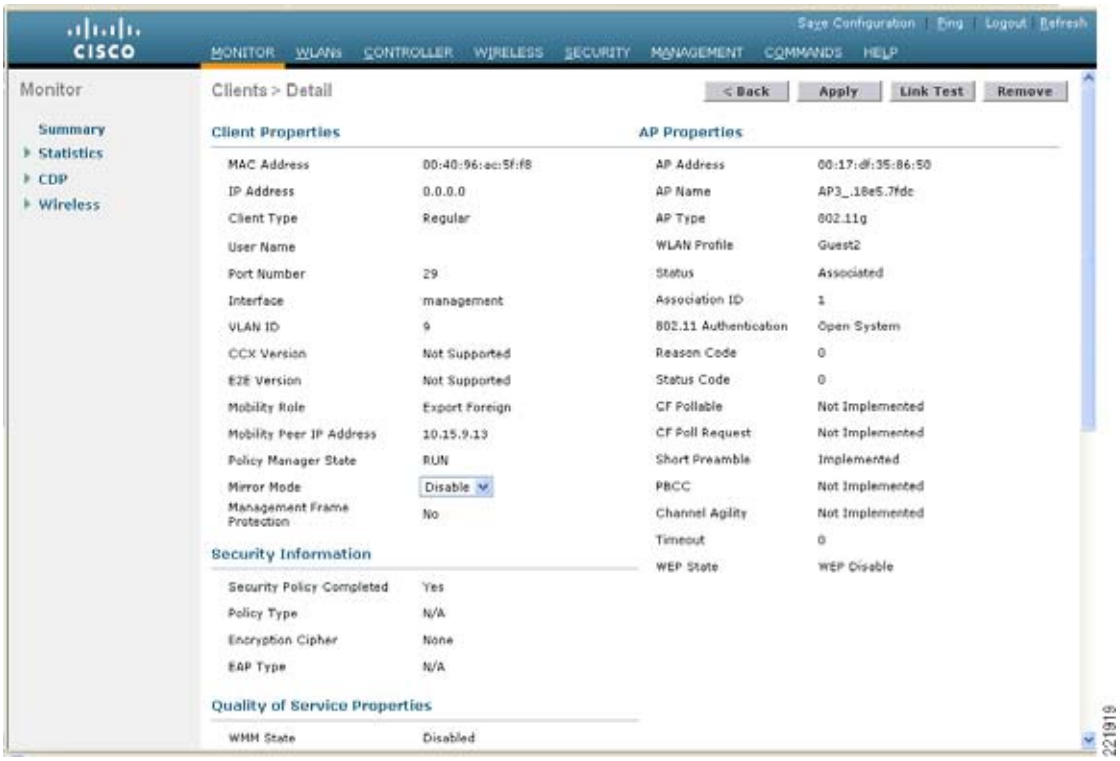
次のコマンドを実行すると、さらに詳しい情報を得られます。

```
(WiSM-slot3-1) >show client detail 00:40:96:ac:5f:f8
Client MAC Address............................. 00:40:96:ac:5f:f8
Client Username ............................... N/A
AP MAC Address................................. 00:17:df:35:86:50
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:17:df:35:86:50
Channel........................................ 11
IP Address..................................... Unknown
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. No CCX support
Mirroring...................................... Disabled
QoS Level...................................... Silver
```

```
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. Export Foreign
Mobility Anchor IP Address...................... 10.15.9.13
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... Yes
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... management
VLAN............................................ 9
Client Capabilities:
      CF Pollable............................... Not implemented
      CF Poll Request........................... Not implemented
      Short Preamble............................ Implemented
      PBCC...................................... Not implemented
      Channel Agility........................... Not implemented
      Listen Interval........................... 0
Client Statistics:
      Number of Bytes Received.................. 308244
      Number of Bytes Sent...................... 700059
      Number of Packets Received................ 2527
      Number of Packets Sent.................... 1035
      Number of Policy Errors................... 0
      Radio Signal Strength Indicator........... -75 dBm
      Signal to Noise Ratio..................... 25 dB
Nearby AP Statistics:
        TxExcessiveRetries: 0
        TxRetries: 0
        RtsSuccessCnt: 0
        RtsFailCnt: 0
        TxFiltered: 0
        TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
      AP3_.18e5.7fdc(slot 0) .....................
antenna0: 37 seconds ago -73 dBm................. antenna1: 4294510568 seconds ago
-128 dBm
```

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を取得できます（図 10-72 を参照）。

図 10-72　[Foreign WLC Monitor] > [Client Detail]



debug コマンド

シリアル コンソールからは、次のデバッグ コマンドも使用できます。

```
debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable
```

Cisco モビリティ サービス エンジン

概要

この章では、Cisco モビリティ サービス エンジン（MSE）を追加し、Cisco Unified Wireless Network で Context Aware Services を実行する場合の設定および展開のガイドラインについて説明します。この章は、次のことを目的としています。

- Cisco モビリティ ソリューションのさまざまな要素およびフレームワークの説明
- 全般的な展開ガイドラインの提供

（注） この章では、MSE および関連コンポーネントの詳細設定は扱いません。これらの情報は、他のドキュメントに含まれています。Context Aware モビリティ サービスの設定および設計に関するドキュメントのリストについては、関連情報を参照してください。適応型 wIPS 設定もこのガイドラインでは扱いません。

背景説明

Cisco MSE では、ワイヤレス LAN コントローラ（WLC）および Cisco Aironet CAPWAP AP を使用して、有線とワイヤレスの両方について、ネットワーク デバイスの物理ロケーションを追跡できます。お客様は、このソリューションによって、クライアント、アクティブ RFID タグ、不正なクライアント、AP などの任意の Wi-Fi デバイスを追跡できます。MSE は、以下の要件を踏まえて設計されました。

- 管理性：Cisco Prime Infrastructure は、MSE の管理および監視に使用されます。さらに、MSE は、ワイヤレス LAN アーキテクチャと直接統合されます。この結果、複数の個別のワイヤレス ネットワークではなく、1 つの統合されたネットワークを管理することができます。
- スケーラビリティ：Cisco MSE シリーズでは、CAS で 25,000 個の要素、wIPS で 5,000 個の AP を同時に追跡できます。CPI では、拡張性を高めるために複数のモビリティ サービス エンジンを管理できます。ワイヤレス LAN コントローラ（WLC）、CPI、および MSE は、拡張性と性能を向上させるために、別々のデバイスを介して実装されます。
- セキュリティ：WLC、CPI、および MSE には、堅牢でセキュアなインターフェイスとデータにアクセスするためのセキュアなプロトコルが用意されています。MSE では、ロケーション情報の履歴を記録しており、この記録は監査証跡および法規制の遵守に使用されます。
- オープンで標準に準拠：MSE には、外部のシステムおよびアプリケーションからアクセスできる SOAP/XML API があり、MSE からのロケーション情報を利用できます。

- ビジネス アプリケーションを容易に展開可能：MSE は、資産の追跡、インベントリ管理、ロケーションに基づくセキュリティ、自動化されたワークフロー管理などの新しいビジネス アプリケーションと統合できます。

概要

Context Aware Service（CAS）は、Wi-Fi 802.11a/b/g/n ネットワークがアクティブな Wi-Fi デバイスを持つ人や物（ワイヤレス クライアントやアクティブ RFID タグ、端末からワイヤレス インフラストラクチャを通じて上流クライアントに送られる関連データなど）の位置を特定できるようにします。適切なライセンスを持つバージョンの CPI を使用して、Cisco MSE を Cisco Unified Wireless Network に追加した場合、MSE では、複数の重要な作業を受け持つことを想定しています。

- 位置決めアルゴリズムの実行
- 調整情報のメンテナンス
- ロケーション通知のトリガーとディスパッチ
- ロケーションの統計情報および履歴の処理
- 地理的な情報、マップ、およびすべてのワイヤレス デバイスの保管

Cisco Prime Infrastructure は MSE とのインターフェイスとなる管理システムで、MSE で提供されるサービスのユーザ インターフェイス（UI）として機能します。メンテナンスおよび診断を目的として、SSH またはコンソール セッションを介して MSE に直接アクセスすることはできますが、オペレータおよびユーザによる MSE とのすべての対話は、通常は、CPI（管理用）またはサードパーティのロケーション クライアント アプリケーションから実行します。

用語

シスコの *中央集中型 WLAN アーキテクチャ*（Cisco Unified Wireless Network の機能アーキテクチャ）および Context Aware ロケーション サービスを使用すると、管理者は、802.11 に基づく任意のデバイスのロケーションや、各デバイスの具体的なタイプまたはステータスを判別できます。クライアント（関連付け、調査などが目的）、不正な AP、不正なクライアント、およびアクティブ タグは、いずれもシステムによって識別され、ロケーションを判別できます。この情報は、イベントの発生から数秒のうちに API で利用できるようになり、履歴の検索やセキュリティ監査のために MSE データベースで保持できます。

Mobility Services Engine

MSE では、一連のモビリティ サービス プログラムをサポートしています。MSE は、オープンなプラットフォームとして設計されており、ネットワーク トポロジと必要なサービスのタイプに基づくさまざまな設定オプションを持つモジュラ形式によって、モビリティ サービス ソフトウェアをサポートします。シスコでは、次のような既存および将来的なソフトウェアをサポートします。

- Context-Aware サービス：これらのプログラムは、ロケーション、温度、アベイラビリティ、使用されているアプリケーションなどの詳細なコンテキスト情報をキャプチャし、ビジネス プロセスに統合されます。Context Aware アプリケーションは、リアルタイム ロケーション、プレゼンス検出、チョークポイントの可視性、テレメトリなどの幅広いロケーション オプションを備えています。拡張受信信号強度表示（RSSI）と到達時間差（TDoA）テクノロジーのサポートにより、さまざまな環境で高い尺度の確度と性能を提供します。

  Context Aware ソフトウェアは、2 つの主要コンポーネントで構成されています。

  - クライアント用 Context Aware Engine：シスコ ロケーション エンジン（RSSI）は、Wi-Fi クライアント、不正なクライアント、不正な AP、および有線クライアントの追跡に使用されます。
  - タグ用 Context Aware Engine：パートナー企業（AeroScout）のロケーション エンジン（RSSI と TDOA の両方）は、Wi-Fi アクティブ RFID タグの追跡に使用されます。

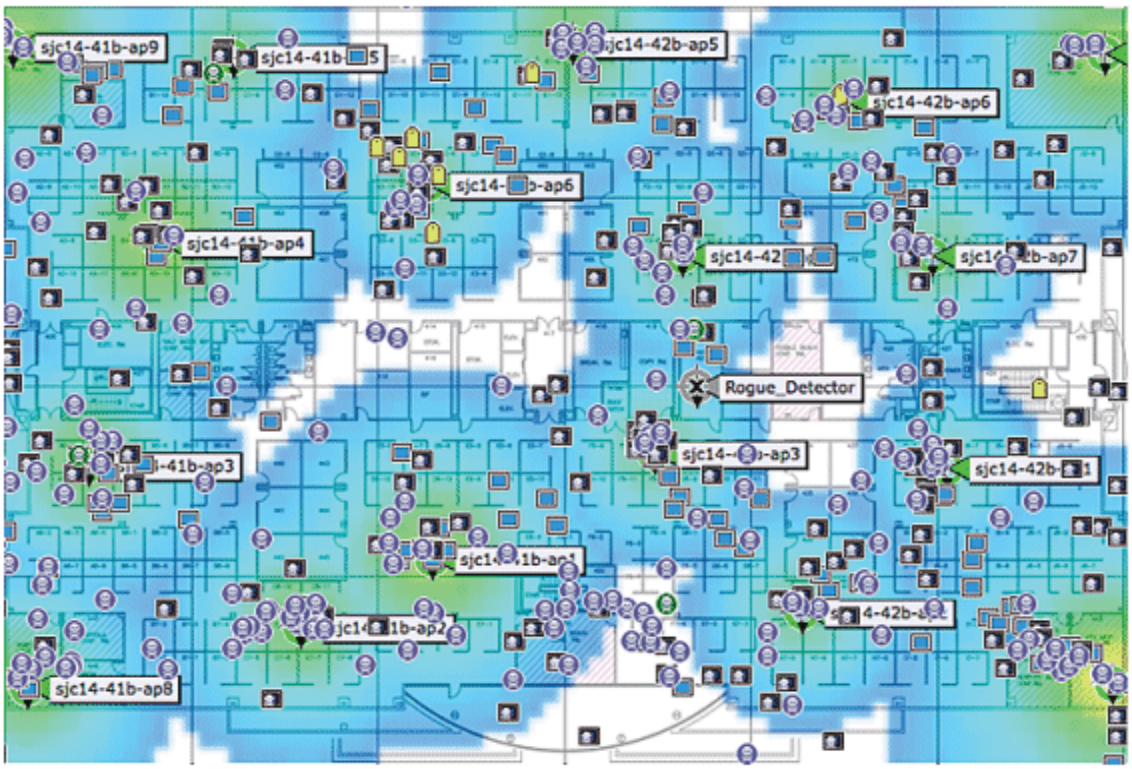
  サードパーティ アプリケーションは、MSE API を介してサポートされます。

- 適応型ワイヤレス侵入防御システム（wIPS）：wIPS ソフトウェアは、ワイヤレスおよび有線ネットワークの脆弱性の監視、アラート、分類、および修復により、モビリティ ネットワークの可視性と包括的な脅威の防止を実現します。
- ネットワーク モビリティ サービス プロトコル：シスコが定義したプロトコルで、WLC と MSE の間の通信を保護するために使用されます。
- Cisco Prime Infrastructure：シスコが開発およびサポートするワイヤレス ネットワーク管理システム。以下の機能を備えています。
  - WLAN の設定
  - WLAN パフォーマンス モニタリング
  - レポート作成（リアルタイムおよび履歴）
  - ネットワークのグラフィカル表示（ワイヤレス LAN コントローラ、AP、クライアントおよびタグ）
- ワイヤレス LAN コントローラ（WLC）：中央集中型 Cisco Unified Wireless Network アーキテクチャおよび制御デバイス。これにより、自律した個別のアクセス ポイントで構成されている従来の 802.11 WLAN インフラストラクチャとは異なり、拡張サービスをサポートするためのアクセス メディアとしてワイヤレスを使用するインテリジェント ネットワークとして、WLAN 全体を運用できます。Cisco Unified Wireless Network では、大量の管理対象エンドポイント（自律 AP）を、1 つ以上の WLC とこれに対応する結合された AP で構成された単一の管理対象システムとしてまとめることで、運営管理が簡素化されます。

  Cisco Unified Wireless Network アーキテクチャでは、AP は *lightweight* です。つまり、WLC から独立して動作できません。AP は通常は*ゼロ タッチ*で展開され、AP の個別の設定は必要ありません。AP では、コントローラ ディスカバリ アルゴリズムによって、1 つ以上の WLC の IP アドレスを学習し、次に join プロセスを通じてコントローラとの信頼関係を確立します。信頼関係が確立されると WLC は AP にファームウェア（必要な場合）および実行時コンフィギュレーションをプッシュします。AP では、設定をローカルに保存しません。
- クライアント：ワイヤレス ネットワーク上のコントローラベースの lightweight AP と関連付けられたすべてのデバイス。
- 不正なアクセス ポイント：検出したワイヤレス LAN モビリティ グループに属していないと判別されたすべての AP。これは、lightweight AP の RF 範囲内にある、このシステム以外のすべての AP で構成されます。これには、有線ネットワーク上の AP や、別の有線ネットワーク上の AP（ネイバーの AP など）を含みます。すべての lightweight AP は、特殊なキーによってビーコン フレームの一部としてハッシュを使用するため、スプーフィングされたインフラストラクチャ AP の場合であっても、不正な AP として識別されます。スプーフィングされた APAP として CPI でフラグが付けられた、正規の AP と誤解されることはありません。
- 不正クライアント：不正な AP に関連付けられたすべてのデバイス。
- アクティブ RFID タグ：Wi-Fi ネットワーク上で検出してロケーションを判別できる Wi-Fi デバイス。Wi-Fi 互換のさまざまなタグが市販されています。タグは、温度と湿度などの動作と環境に関するデータのテレメトリ、コール ボタン、屋内運用と屋外運用、本質的に安全なバージョン、柔軟性のある取り付けオプションなど、さまざまな機能を提供します。

MSE では、最大 25,000 台のデバイス（タグ、クライアント、不正なクライアントおよび AP）を追跡できます。図 11-1 は、CPI に表示されるフロア マップの例で、タグ、クライアント、不正なクライアント、および不正な AP が表示されています。このフロア マップは、MSE で追跡できるデバイス クラスの規模と多様さを示しています。CPI では、検索パラメータを定義して、デバイスのサブセットのみを表示できます。たとえば、医療業務に携わるユーザに対しては、不正なデバイスや、暗号のような MAC アドレスまたは IP アドレスを持つデバイスではなく、わかりやすい識別子の付いた輸液ポンプや心電図装置のみを表示することができます。

図 11-1　　追跡対象デバイスを含む CPI フロア マップ



マップの凡例：

- クライアント：青色の四角形のモニタ
- タグ：黄色の垂直の矩形
- 不正な AP：どくろマーク（赤 = 悪意あり、緑 = 友好、灰色 = 未分類）
- 不正クライアント：どくろマークの付いた青色の四角形のモニタ

技術的な背景情報

Cisco モビリティ ソリューションで Wi-Fi デバイスを追跡するために使用されるテクノロジーは 2 種類あります。

- RSSI：受信信号強度表示
- TDOA：到達時間差

これらのテクノロジーの詳細については、次の Web サイトにある『*Wi-Fi Location-Based Services Design Guide*』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

（注）　このガイドは旧リリース対応ですが、情報は有効です。

RSSI

RSSI は、受信する無線信号の電力によって測定されます。任意のワイヤレス デバイスによって送信されるパケットは、複数の AP（フレームを送信したチャネルをリッスンしている AP であることが前提）で受信されます。AP では、AP で測定した対応する RSSI 情報と一緒に、このパケットをワイヤレス LAN コントローラに転送します。ワイヤレス LAN コントローラでは、さまざまな AP から得たこの情報をデバイスごとに集約します。このデータは、NMSP を介して MSE に転送されます。MSE 上の Context Aware Services では、1 つ以上の WLC から受信した RSSI データを使用して、ワイヤレス デバイスのロケーションを判別します。通常 RSSI は、信号が反射する、屋内や、天井の低い環境で推奨されます。TDOA と異なり、RSSI では AP 間で時間が厳密に同期する必要はありません。さまざまな AP から取得する測定された RSSI 値を使用して、フロア上のさまざまなポイントでデバイスのロケーションの確率が計算されます。この確率に基づいて、ロケーションが推定ロケーションとして返されます。

到達時間差

屋外や、天井の高い屋内環境などの屋外に似た環境でタグを追跡する場合は、デバイス ロケーションを判別する方式として到達時間差（TDOA）メカニズムを推奨します。TDOA では、時刻の同期された 3 台以上の Wi-Fi TDOA 受信機から送信された信号を伝送するときの到達時間に基づいて、WLAN デバイスのロケーションが判別されます。到達時間データが収集されて MSE 上のタグ用 Context Aware Engine に報告され、そこで、複数組の Wi-Fi TDOA 受信機間の到達時間差が計算されます。異なる Wi-Fi TDOA 受信機が特定のメッセージを受信するために必要な時間は、伝送モバイル デバイスと各 TDOA 受信機の間の伝送パスの長さに比例します。このデバイス ロケーション計算メカニズムでは、Wi-Fi TDOA 受信機間の時刻の同期が必要です。

この方式で位置を正確に計算するためには、3 台以上の Wi-Fi TDOA 受信機のセットが必要です。Wi-Fi TDOA 受信機間の距離は、屋内の RSSI による位置決めで必要な AP 間の距離に比べて大きくなります。RSSI 位置決め同様、この方式は単方向通信（タグが通知フレームを伝送し、関連付けは不要）に基づいています。

次の Web サイトにある『*Context Aware Service Software Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/wireless/mse/3350/7.0/CAS/configuration/guide/CAS_70.html

Active RFID Tags

Cisco Compatible Extensions（CCX）準拠のアクティブ RFID タグは、タグから送信されて 802.11 AP で受信されるタグ通知フレームに基づいて、Wi-Fi ネットワーク上で検出されます。タグ通知フレーム レートは、具体的な使用例シナリオに基づいてプログラムできます。通常、タグは、ロケーション アップデートの頻度とバッテリ寿命を最適化するために、3 ～ 5 分おきにタグ通知フレームを送信するように設定されます。コール ボタン機能では、タグ上のプッシュ ボタンに基づいてイベントをトリガーできます。これにより、緊急レポート、部品の補充など拡張機能が実現されます。一部のタグには、複数のコール ボタンが装備されています。2 つ目のコール ボタンは、付加機能用にプログラムできます。タグには、事前にプログラムされており、ワイヤレス ネットワーク インフラストラクチャで受信できるメッセージを保存できます。アクティブ タグの電源として、最長 4 年のバッテリ寿命を持つバッテリが使用されます。バッテリ寿命は、タグ通知フレームの伝送頻度と反復レートなどのタグ設定パラメータの数によって異なります。タグでは、タグのバッテリ レベルを報告でき、電力が低下し

たときはアラートできます。タグには、移動されたときにタグ通知フレームを送信するための内蔵動作センサーも組み込み可能です。このことは、タグが固定されている場合にバッテリ寿命を延ばすために役立ちます。移動のない場合は、送信頻度を低くするようにタグを設定します。

他のロケーションおよびステータスの情報に加えて、周囲温度など、資産の状態を正確に監視する拡張センサー テクノロジーを付加する、別のタグ カテゴリがあります。これらのセンサー タグでは、標準 Wi-Fi ネットワークを使用して、資産のロケーションおよびセンサー データを転送します。専用のセンサー ネットワークを設ける必要はありません。

Wi-Fi タグ用の CCX 仕様に準拠する Wi-Fi RFID タグでは、タグ メッセージ ペイロードの一部として、オプションで、タグ テレメトリ情報をロケーション認識型の Cisco UWN に渡すことができます。テレメトリ情報は、AP が受け取り、WLC が収集します。MSE では、起動時に、タグの測定など、MSE で対象とするすべてのサービスに申し込みます。WLC では、各集約サイクルの終わりに、MSE 通知の送信を続行します。

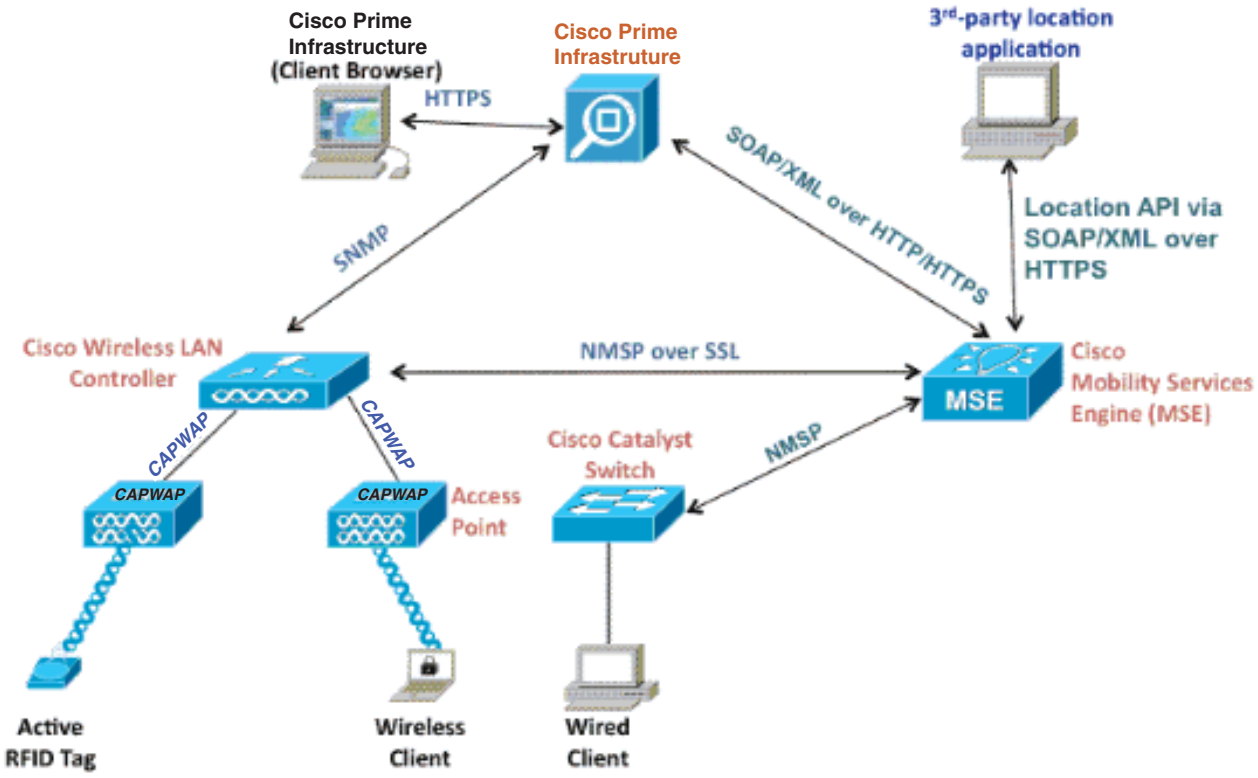
テレメトリ情報は、CCX 互換のタグから送信されて 1 台以上の AP またはロケーション受信機（Wi-Fi TDoA 受信機）、あるいはその両方で受信されます。さらに、このテレメトリ情報は、それぞれが登録されている WLAN コントローラに渡されます。タグが、チャネルごとに複数のフレーム コピー（またはバースト）を送信するよう設定されている場合、コントローラは重複するすべてのタグ テレメトリを削除し、重複を除外したテレメトリ値を MSE に渡します。MSE 内のデータベースに新しいテレメトリ情報が更新され、MSE SOAP/XML API を介してロケーション クライアントに提供されます。

テレメトリ値を渡すタグの場合、NMSP は、複数のタグからのテレメトリ値を同様な方式で効率的に転送するように設計されています。複数のタグからのテレメトリ トラフィックは、NMSP フレーム フラグメンテーションを実行できる各 NMSP エンドポイントを使用して WLC によって集約され、必要に応じて再構成されます。すべてのタグ データは、ノースバウンド通知に含めるテレメトリを含む、コール ボタン、チョーク ポイントなどを検出できます。

システム アーキテクチャ

MSE は、図 11-2 に示すように、シスコの中央集中型ワイヤレス LAN アーキテクチャと統合されます。MSE は、ワイヤレス LAN のデータ パスを外れた場所にあり、NMSP を介して WLC からデータを受信します。Cisco Prime Infrastructure は、MSE の設定に使用されます。いったん設定すれば MSE は、自己完結しています。

図 11-2　　システム アーキテクチャ



Context Aware ソリューションを展開するときは、追跡対象のデバイスのタイプおよび最大デバイス数を考慮する必要があります。個別または同時に追跡するように設定された、5 種類の任意のデバイス タイプ（Wi-Fi クライアント、アクティブ RFID タグ、不正なクライアント、不正な AP、または有線クライアント）を追跡できます。

1 つの MSE は、1 つの CPI のみで管理できます。つまり、単一の MSE は、複数の CPI インスタンスによって管理できません。一方、単一の CPI では、複数の MSE を管理できます。管理対象デバイスの数が 1 つの MSE の容量を超えた場合、複数の独立した MSE の配置が必要になります。拡張用に複数の MSE を展開する機能は、MSE 上で現在サポートされているすべてのサービスに適用されます。Context Aware Service の一環として 1 台の Cisco MSE 3355 で追跡できるデバイスの最大数は、クライアント、アクティブ RFID タグ、不正なクライアント、不正な AP、および有線クライアントを合わせて 25,000 台です。旧モデルの Cisco MSE 3310 が追跡できるデバイスの数は最大 2,000 台ですが、Cisco MSE 3350 は最大 18,000 台のデバイスを追跡できます。管理するデバイスの数が 1 台の MSE ボックスのキャパシティを超える場合は、複数の独立した MSE アプライアンスを配置する必要があります。このためには、場合によっては、特定のコントローラ上に MSE を配置する必要があります。クライアントまたは資産のローミングが物理的に異なるビルやドメインを交差する広大なキャンパスであればなおさらです。この例では、コントローラは、最大 10 台の MSE アプライアンスと通信できます。

Cisco Lightweight AP は、クライアントにサービスを提供するチャネル上のデバイスと、ワイヤレス クライアントにデータ アクセスを提供したままで定期的にバックグラウンド スキャンを実行する場合に、他のすべてのチャネル上のデバイスの両方を検出する、固有のデュアル モードで動作します。収集された未加工ロケーション データは、次に、LWAPP または標準ベースの CAPWAP プロトコルを介して、各 AP からこれに関連付けられた WLC に転送されます。データはセキュアな NMSP 接続を介して WLC と MSE 間で転送されます。

Cisco Prime Infrastructure は、MSE の管理および設定に使用され、追跡対象の Wi-Fi デバイスを表示する、MSE のビジュアルなフロントエンドにもなります。すべてのデバイス（有線およびワイヤレス）の詳細情報および個別のロケーション情報の履歴に、MSE ノースバウンド API によってアクセスできます。CPI では、このインターフェイスを使用して、ロケーション情報の可視化および Context-Aware パラメータの表示と設定を行います。

Cisco モビリティ ソリューションは、2 種類のロケーション エンジンおよび統合された単一の API で構成されています。ロケーション エンジンは次のとおりです。

- クライアント用 Context Aware Engine（Cisco エンジン）：クライアントとタグの両方で使用可能
- タグ用 Context Aware Engine（パートナー製エンジン）：AeroScout ベースのタグ ソリューション

クライアント用 Context Aware Engine は RSSI ベースのソリューションであり、屋内空間（オフィス、病院、その他の天井の低い環境など）で Wi-Fi クライアント デバイスを追跡する場合に適しています。このエンジンは、デフォルトで、すべての Cisco MSE サーバに付属しています。クライアント用 Context Aware Engine の追跡ライセンスはクライアントとタグの間で共有できます。

タグ用 Context Aware Engine では、RSSI ベースと TDOA ベースの両方のエンジンを使用でき、屋内の天井の低い環境（RSSI）、屋内の天井の高い環境（TDOA）、および屋外（TDOA）で Wi-Fi デバイスを追跡する場合に使用することを想定しています。また、このエンジンは、デフォルトで、すべての MSE プラットフォームにインストールされており、ライセンスがイネーブルにされています。タグ用 Context Aware Engine の追跡ライセンスはタグでのみ使用できます。クライアントの追跡にあたって、お客様は以下の追加コンポーネントを購入する必要があります。

- 適切なタグ数を含む MSE 用のタグの追跡ライセンス（TDOA または RSSI）
- Wi-Fi TDOA ロケーション受信機（必要な場合）
- 各 Wi-Fi TDOA 受信機用の LR ライセンス

Cisco MSE を Cisco Unified Wireless Network に追加した場合、MSE では、以下の重要な作業を受け持つことを想定しています。

- 位置決めアルゴリズムの実行
- 調整情報のメンテナンス
- ロケーション通知のトリガーとディスパッチ
- ロケーションの統計情報および履歴の処理

Cisco Prime Infrastructure は MSE サーバの管理プラットフォームで、MSE が提供するサービスのユーザ インターフェイス（UI）です。メンテナンスおよび診断を目的とする場合は、SSH またはコンソール セッションを介して MSE に直接アクセスします。オペレータおよびユーザによる MSE とのすべての対話は、通常は、CPI を介して行われます。Cisco MSE を Cisco Unified Wireless Network アーキテクチャに統合すると、以下の改善点を含むベースレベルのロケーション機能を即座に向上できます。

- 拡張性：Cisco MSE を追加すると、Cisco Unified Wireless Network の拡張性が向上して、一度に 1 つのデバイスを追跡するオンデマンド追跡から、MSE ごとに最大 25,000 台のデバイス（WLAN クライアント、RFID タグ、不正な AP、および不正なクライアント）を同時追跡できるまでに、追跡キャパシティが強化されます。大量のデバイスをサポートする必要のある展開では、1 台以上の CPI サーバの下に追加の MSE アプライアンスを配置して管理できます。
- 履歴および統計のトレンディング：MSE では、クライアントおよびタグのロケーションの統計情報および履歴を記録し、保守します。この情報は、CPI またはサードパーティ ロケーション クライアントを使用して表示できます。この履歴情報は、ロケーション トレンディング、資産損失の調査、RF キャパシティ管理、およびネットワークに関する問題の解決の促進に使用できます。履歴パラメータは、Cisco Prime Infrastructure で設定されます。

関連情報

次の参考資料は、Cisco モビリティ サービス エンジンに関する追加情報を提供します。

- 『*Cisco 3355 Mobility Services Getting Started Guide*』

http://www.cisco.com/en/US/docs/wireless/mse/3355/user/guide/mse_qsgmain.html

- 『*Cisco 3350 Mobility Services Getting Started Guide*』

http://www.cisco.com/en/US/docs/wireless/mse/3350/quick/guide/mse_qsgmain.html

- 『*Cisco 3310 Mobility Services Engine Getting Started Guide*』

http://www.cisco.com/en/US/docs/wireless/mse/3310/quick/guide/MSE3310_GSG.html

- 『*Cisco Mobility Services Engine - Context Aware Mobility Solution Deployment Guide*』

http://www.cisco.com/en/US/products/ps9742/products_tech_note09186a00809d1529.shtml

- 『*Cisco Context Aware Service Configuration Guide*』

http://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch7_CAS.html

- 『*Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide*』

http://www.cisco.com/en/US/docs/wireless/mse/3350/7.3/CAS_Configuration_Guide/Guide/msecg_Overview.html

- 『*Wi-Fi Location-Based Services 4.1 Design Guide*』（旧リリース対応ですが、情報は有効です）

http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/WiFiLBS-DG.html

- モビリティ グループ FAQ

http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a00809a30cc.shtml

関連情報

A

AAA Authentication, Authorization, and Accounting（認証、許可、アカウンティング）

ACS Cisco Access Control Server

AES Advanced Encryption Standard（高度暗号化規格）

AP Access Point（アクセス ポイント）

B

BSSID Basic Service Set Identifier（基本サービス セット識別子）

C

CAM Clean Access Manager

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CCX Cisco Compatible Extensions

CKIP Cisco Key Integrity Protocol

CMIC Cisco Message Integrity Check

CSA Cisco Security Agent

CSSC Cisco Secure Services Client Cisco Key Integrity Protocol（CKIP）および Cisco Message Integrity Check（CMIC）

D

DoS Denial of Service（サービス拒否）

E

EAP Extensible Authentication Protocol

EAP-FAST EAP-Flexible Authentication via Secured Tunnel

EAP-TLS EAP-Transport Layer Security

EIRP Effective Isotropic Radiated Power（実効等方放射電力）

ESSID Extended Service Set Identifier（拡張サービス セット識別子）ー 通常は「SSID」

F

FWSM Firewall Services Module（ファイアウォール サービス モジュール）

I

IDS Intrusion Detection System（侵入検知システム）

IPS Intrusion prevention system（侵入防御システム）

L

LAP LWAPP Access Point（LWAPP アクセス ポイント）

LBS Location-based service（ロケーション ベース サービス）

LWAPP Lightweight Access Point Protocol（Lightweight アクセス ポイント プロトコル）

M

Map Mesh AP（メッシュ AP）

MFP Management frame protection（管理フレーム保護）

MIC Message integrity check（メッセージ整合性チェック）

N

NAC Network Admission Control（ネットワーク アドミッション コントロール）

O

OFDM Orthogonal Frequency Division Multiplexing（直交周波数分割多重方式）

P

PEAP GTC Protected EAP Generic Token Card

PEAP MSCHAP Protected EAP Microsoft Challenge Handshake Authentication Protocol（Microsoft チャレンジ ハンドシェイク認証プロトコル）

PKI Public Key Infrastructure（公開キー インフラストラクチャ）

R

RADIUS Remote Authentication Dial-In User Service（リモート認証ダイヤルイン ユーザ サービス）

RF Radio Frequency（無線周波数）

RFID Radio Frequency（無線周波数）Radio-frequency identification（無線周波数 ID）

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

RSSI Received signal strength indication（受信信号強度表示）

S

SNR Signal-to-noise ratio（信号対雑音比）

SSID IEEE Extended Service Set Identifier（IEEE 拡張サービス セット識別子）

SSO Single sign-on（シングル サインオン）

SVI Switched virtual interfaces（スイッチ仮想インターフェイス）

T

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security

W

WCS Wireless Control System

WEP Wired Equivalent Privacy

Wi-Fi Wi-Fi Alliance のブランド。製品とサービスの相互運用性を IEEE 802.11 テクノロジーに基づいて認定

WiSM	Wireless Services Module
WLAN	Wireless LAN（無線 LAN）
WLC	Wireless LAN Controller（ワイヤレス LAN コントローラ）
WLCM	Wireless LAN Controller Module（ワイヤレス LAN コントローラ モジュール）
WLSM	Wireless LAN Services Module
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access

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