Cisco Wireless LAN Controller コンフィギュレーション ガイド

Software Release 5.0
February 2008

Text Part Number: OL-15301-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Wireless LAN Controller コンフィギュレーション ガイド

CONTENTS

はじめに

この章では、『Cisco Wireless LAN Controller コンフィギュレーション ガイド Software Release 5.0』の概要について説明します。また、関連資料を紹介し、必要に応じて他の資料や技術サポートを得る方法についても説明します。この章の内容は、次のとおりです。

対象読者

このガイドでは、Cisco Wireless LAN Controller および Cisco Lightweight アクセス ポイントについて説明します。このガイドは、これらのデバイスのインストールと管理を担当するネットワーキングの専門家を対象としています。このガイドを使用するには、無線 LAN の概念および用語を十分に理解している必要があります。

目的

このガイドには、無線 LAN コントローラのセットアップと設定に必要な情報が記載されています。

（注） このバージョンの『Cisco Wireless LAN Controller Configuration Guide』は、コントローラ ソフトウェア リリース 5.0 に特に関連しています。これより古いバージョンのソフトウェアを使用している場合、機能、機能性、および GUI ページの記述はそのソフトウェアとは異なっています。

マニュアルの構成

このガイドは、次の章で構成されています。

第 1 章「概要」：無線 LAN コントローラのネットワークでの役割と機能の概要について説明します。

第 2 章「Web ブラウザと CLI インターフェイスの使用方法」：コントローラの GUI と CLI の使用方法について説明します。

第 3 章「ポートとインターフェイスの設定」：コントローラの物理ポートとインターフェイスについて説明し、それらの設定手順を示します。

第 4 章「コントローラの設定」：コントローラの設定方法について説明します。

第 5 章「セキュリティ ソリューションの設定」：無線 LAN のアプリケーション固有のソリューションを説明します。

第 6 章「WLAN の設定」：システム上で無線 LAN と SSID を設定する方法について説明します。

第 7 章「Lightweight アクセス ポイントの制御」：アクセス ポイントをコントローラに接続する方法、およびアクセス ポイントの設定を管理する方法について説明します。

第 8 章「コントローラ ソフトウェアと設定の管理」：コントローラ ソフトウェアおよび設定のアップグレード方法と管理方法について説明します。

第 9 章「ユーザ アカウントの管理」：ゲスト ユーザ アカウントの作成方法と管理方法、Web 認証プロセス、および Web 認証ログインのカスタマイズ方法について説明します。

第 10 章「Radio Resource Management の設定」：Radio Resource Management（RRM）について、コントローラ上での設定方法も含めて説明します。

第 11 章「モビリティ グループの設定」：モビリティ グループについて、コントローラ上での設定方法も含めて説明します。

第 12 章「Hybrid REAP の設定」：Hybrid REAP、およびこの機能をコントローラ上およびアクセス ポイント上で設定する方法について説明します。

付録 A 「安全上の考慮事項および安全についての警告」：Cisco Unified Wireless Network Solution 製品に適用される安全上の考慮事項と安全についての警告を示します。

付録 B 「適合宣言および規制に関する情報」：Cisco Unified Wireless Network Solution の製品についての適合宣言および規制情報を記載します。

付録 C「エンド ユーザ ライセンス契約および保証」：Cisco Unified Wireless Network Solution 製品に適用されるエンド ユーザ ライセンス契約および保証について説明します。

付録 D 「トラブルシューティング」：コントローラと Lightweight アクセス ポイントの LED パターンに関する情報と、Cisco Unified Wireless Network Solution インターフェイスに表示されるシステム メッセージのリストを示し、コントローラの問題のトラブルシューティングに使用できる CLI コマンドについて説明します。

付録 E 「論理接続図」：FCisco 製品に統合されているコントローラの論理接続図と関連ソフトウェア コマンドを記載します。

表記規則

このマニュアルには、次の表記規則に従って手順および情報が記載されています。

コマンドの説明では次の表記規則を使用します。

- コマンドおよびキーワードは太字で示されています。
- ユーザが値を指定する引数は、イタリック体で示されています。
- 角カッコ（[ ]）は、省略可能の要素を意味します。
- 必須の選択肢は波カッコ（{ }）で囲まれ、各要素は縦棒（|）で区切られています。
- 省略可能な要素内の必須の選択肢は、角カッコ内の波カッコで囲まれ、縦棒（[{ | }]）で区切られています。

対話形式の例では次の表記規則を使用します。

- 端末セッションおよびシステム表示は、`screen` フォントで示されています。
- ユーザが入力する情報は、**太字**で示されています。
- パスワードやタブのように出力されない文字は、山カッコ（< >）で囲んで示されています。

注、注意、およびヒントでは、次の表記規則と記号を使用します。

（注） 読者に留意していただきたいことを示します。「注」には、役立つ助言や、このマニュアルに記述されていない参考資料が示されています。

注意 読者に気を付けていただきたいことを示します。ここに記された注意に従わない場合、ユーザの行為によって機器の損傷やデータの消失が生じる恐れがあります。

警告 **警告マークは危険を示します。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。**

関連資料

Cisco Unified Wireless Network Solution については、併せて次のマニュアルも参照してください。

- 『Quick Start Guide:Cisco 2100 Series Wireless LAN Controllers』
- 『Quick Start Guide:Cisco 4400 Series Wireless LAN Controllers』
- 『Cisco Wireless LAN Controller Command Reference』
- 『Cisco Wireless Control System Configuration Guide』
- 『Quick Start Guide:Cisco Wireless Control System』
- 特定の Lightweight アクセス ポイント用のクイックスタート ガイドとハードウェア インストール ガイド

Cisco Unified Wireless Network Solution のユーザ向けマニュアルを参照するには、次のリンクをクリックしてください。

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

マニュアルの入手、サポート、およびセキュリティのガイドライン

マニュアルの入手、サポートの利用、マニュアルに関するフィードバックの送信方法、セキュリティ ガイドライン、および推奨される全般的なシスコ資料については、毎月更新される『Whats New in Cisco Product Documentation』を参照してください。この文書には、新規追加または改訂されたシスコ技術資料の一覧もあります。URL は次のとおりです。

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

CHAPTER 1

概要

この章では、コントローラのコンポーネントと機能について説明します。この章の内容は、次のとおりです。

Cisco Unified Wireless Network Solution の概要

Cisco Unified Wireless Network（Cisco UWN）Solution は、企業およびサービス プロバイダーに 802.11 無線ネットワーキング ソリューションを提供するように設計されています。Cisco UWN Solution を使用すると、大規模無線 LAN の展開および管理が簡素化され、他に類のないクラス最高のセキュリティ インフラストラクチャを実現できます。オペレーティング システムは、すべてのデータ クライアント、通信、およびシステム管理機能を管理し、Radio Resource Management（RRM）機能を実行します。また、オペレーティング システム セキュリティ ソリューションを使用してシステム全体のモビリティ ポリシーを管理したり、オペレーティング システムのセキュリティ フレームワークを使用してすべてのセキュリティ機能を調整することもできます。

Cisco UWN Solution は、Cisco Wireless LAN Controller とそれにアソシエートされている Lightweight アクセス ポイントで構成されます。これらはオペレーティング システムによって制御され、次のいずれか、またはすべてのオペレーティング システム ユーザ インターフェイスによってすべて同時に管理されます。

- HTTP、HTTPS、またはこれら両方の機能をすべて備えた Web ユーザ インターフェイス。Cisco Wireless LAN Controller によってホストされるこのインターフェイスは、個々のコントローラを設定および監視するときに使用できます。第 2 章を参照してください。
- 全機能を備えた Command-line Interface（CLI; コマンドライン インターフェイス）。個々の Cisco Wireless LAN Controller を設定および監視するときに使用できます。第 2 章を参照してください。
- Cisco Wireless Control System（WCS）。1 つ以上の Cisco Wireless LAN Controller とアソシエートされているアクセス ポイントを設定、監視する場合に使用します。WCS には、大規模システムの監視と制御を容易にするツールが備わっています。WCS は、Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。

（注） WCS ソフトウェア リリース 5.0 は、コントローラ ソフトウェア リリース 5.0 を実行しているコントローラとともに使用する必要があります。前のバージョンの WCS は、コントローラ ソフトウェア リリース 5.0 を実行しているコントローラとともに使用しないでください。

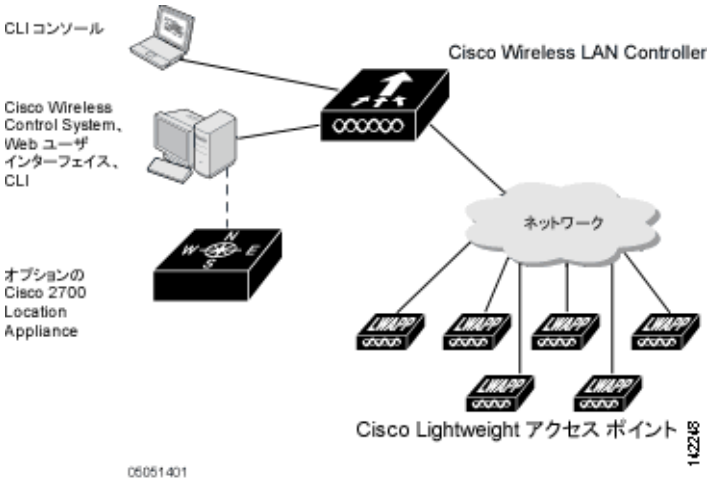
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

Cisco UWN Solution は、クライアント データ サービス、クライアントの監視と制御、およびすべての不正なアクセス ポイントの検出、監視、および阻止機能をサポートします。Cisco UWN Solution では、Lightweight アクセス ポイント、Cisco Wireless LAN Controller、およびオプションの Cisco WCS を使用して、企業とサービス プロバイダーに無線サービスを提供します。

（注） 特に記載されていない限り、以降では、Cisco Wireless LAN Controller を *コントローラ* と呼び、すべての Cisco Lightweight アクセス ポイントを *アクセス ポイント* と呼びます。

図 1-1 は、複数のフロアとビルディングに同時に展開できる Cisco Wireless LAN Solution コンポーネントを示しています。

図 1-1　Cisco UWN Solution コンポーネント



シングルコントローラ展開

スタンドアロンのコントローラでは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートすることができます。サポートされている機能は、次のとおりです。

- ネットワークに追加された Lightweight アクセス ポイントの自動検出と自動設定。
- Lightweight アクセス ポイントの完全制御。
- Lightweight アクセス ポイントに対する最大 16 までの無線 LAN（SSID）ポリシーの完全制御。

（注） LWAPP 有効化アクセス ポイントは、最大 8 つまでの無線 LAN（SSID）ポリシーをサポートします。

- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。ネットワーク機器では、アクセス ポイントに Power over Ethernet を提供してもしなくてもかまいません。

一部のコントローラでは、1 つのネットワークに障害が発生した場合、冗長ギガビット イーサネット接続を使用してこれを迂回します。

（注） 一部のコントローラは、複数の物理ポートを使用して、ネットワークの複数のサブネットに接続できます。この機能は、オペレータが複数の VLAN を別々のサブネットに限定する場合などに役立ちます。

図 1-2 は、一般的なシングルコントローラ展開を示しています。

図 1-2　シングルコントローラ展開

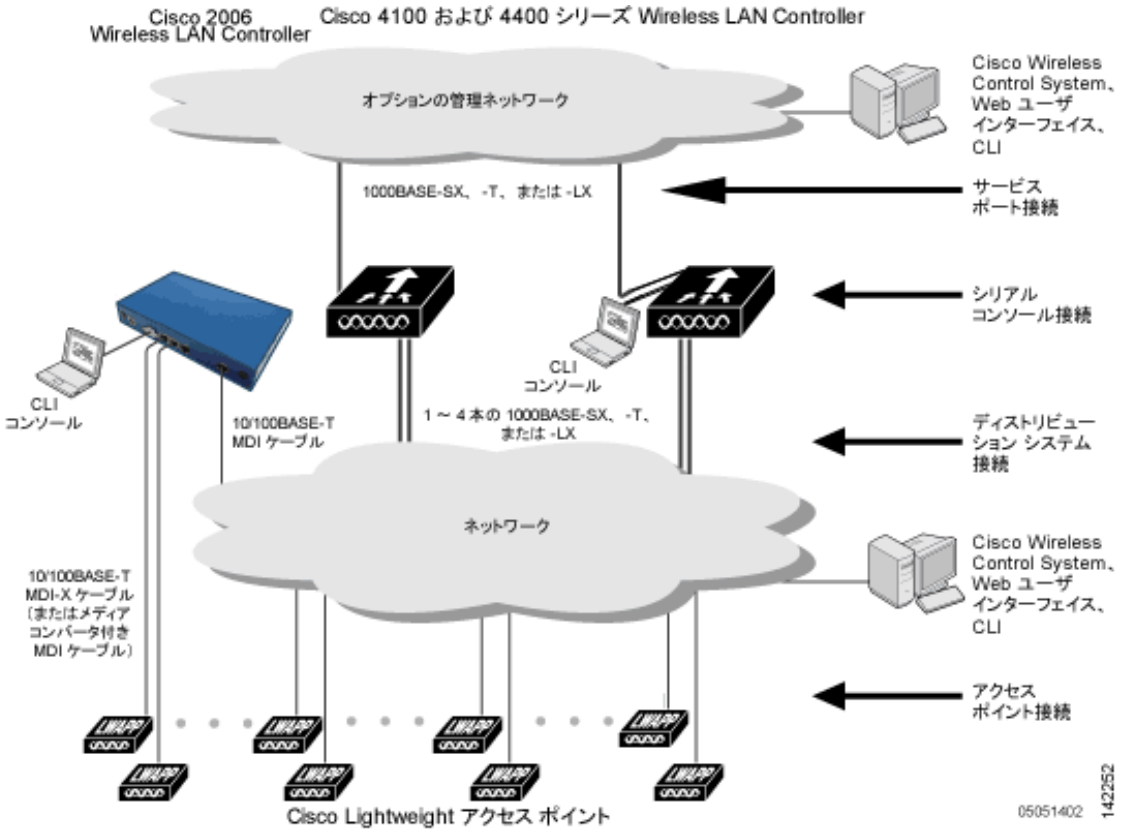
マルチコントローラ展開

すべてのコントローラは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートできます。ただし、Cisco Wireless LAN Solution の全機能が実現されるのは、複数のコントローラが使用されている場合です。マルチ コントローラ システムには、次の追加の機能があります。

- ネットワークに追加された コントローラ の RF パラメータの自動検出と自動設定。
- 同一サブネット（レイヤ 2）でのローミングとサブネット間（レイヤ 3）でのローミング。
- アクセス　ポイントの負荷を減らした任意の冗長コントローラへのアクセス　ポイントの自動フェールオーバー（「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P. 1-19）を参照）。

図 1-3 は、一般的なマルチコントローラ展開を示しています。また、この図では、オプションの専用管理ネットワークと、ネットワークとコントローラ間の 3 つの物理接続タイプも示しています。

図 1-3　一般的なマルチコントローラ展開



オペレーティング システム ソフトウェア

オペレーティング システム ソフトウェアは、Cisco Wireless LAN Controller および Lightweight アクセス ポイントを制御します。このソフトウェアには、オペレーティング システムのセキュリティ機能と Radio Resource Management（RRM）機能がすべて組み込まれています。

オペレーティング システムのセキュリティ

オペレーティング システムのセキュリティ機能は、レイヤ 1、レイヤ 2、およびレイヤ 3 のセキュリティ コンポーネントを、Cisco WLAN Solution 全体を対象とするシンプルな Policy Manager に統合したものです。Policy Manager は、最大 16 の無線 LAN それぞれに対して、独立したセキュリティ ポリシーを作成する管理ツールです（「Cisco UWN Solution 無線 LAN」の項（P. 1-13）を参照）。

802.11 静的 WEP の脆弱性は、次のような強化された業界標準のセキュリティ ソリューションを使用することで克服できます。

- Extensible Authentication Protocol（EAP; 拡張認証プロトコル）使用による 802.1X 動的キー。
- Wi-Fi Protected Access（WPA）動的キー。Cisco WLAN Solution の WPA 実装には、次のものが含まれます。
  - Temporal Key Integrity Protocol（TKIP）+ Message Integrity Code Checksum（Michael）動的キー
  - WEP キー（事前共有キーのパスフレーズの有無を問わない）
- RSN（事前共有キーの有無を問わない）
- Cranite：IPS140-2 準拠パススルー
- オプションの MAC フィルタリング

WEP 問題は、次のような業界標準のレイヤ 3 セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

- パススルー VPN
- Cisco Wireless LAN Solution では、ローカルおよび RADIUS Media Access Control（RADIUS MAC; RADIUS メディア アクセス制御）アドレス フィルタリングがサポートされています。
- Cisco Wireless LAN Solution は、ローカルおよび RADIUS ユーザ / パスワード認証をサポートします。
- また、Cisco Wireless LAN Solution は、手動および自動による無効化を使用して、ネットワーク サービスへのアクセスをブロックします。手動で無効化するときは、オペレータがクライアントの MAC アドレスを使用してアクセスをブロックします。自動による無効化は常にアクティブであり、クライアントが一定の回数の認証を繰り返し試みて失敗すると、オペレーティング システム ソフトウェアにより、オペレータが設定した時間だけネットワーク サービスへのアクセスが自動的にブロックされます。この無効化を使用すると、Brute-Force ログイン アタックを阻止できます。

これらとその他のセキュリティ機能は、業界標準の認可および認証方式を使用して、ビジネスクリティカルな無線 LAN トラフィックに対する最高のセキュリティを実現します。

Cisco WLAN Solution の有線セキュリティ

従来のアクセス ポイント ベンダーの多くは、「オペレーティング システムのセキュリティ」の項（P. 1-6）で説明したような無線インターフェイスのセキュリティ対策に集中的に取り組んでいます。一方、オペレーティング システムには、Cisco Wireless LAN Controller サービス インターフェイス、アクセス ポイントに接続する Cisco Wireless LAN Controller、およびデバイス サービシング時とクライアント ローミング時の Cisco Wireless LAN Controller 間通信をセキュリティで保護するためのセキュリティ機能が組み込まれています。

Cisco Wireless LAN Controller と Lightweight アクセス ポイントには、それぞれ固有の署名付き X.509 証明書が添付されます。この署名付き証明書は、ダウンロードしたコードを読み込む前の検証に使用され、悪意のあるコードがハッカーによって Cisco Wireless LAN Controller や Lightweight アクセス ポイントにダウンロードされることを防ぎます。

また、Cisco Wireless LAN Controller と Lightweight アクセス ポイントでは、ダウンロードしたコードを署名付き証明書を使用して検証してから読み込むことで、ハッカーが Cisco Wireless LAN Controller や Lightweight アクセス ポイントに悪意のあるコードをダウンロードできないようにしています。

レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作

コントローラと Lightweight アクセス ポイント間の LWAPP 通信は、ISO のデータ リンク レイヤ 2 またはネットワーク レイヤ 3 で実行されます。

（注） コントローラ ソフトウェア リリース 5.0 では、レイヤ 3 の LWAPP モードのみがサポートされます。コントローラ ソフトウェア リリース 5.0 にアップグレードする場合、LWAPP モードは、以前にレイヤ 2 に設定されていると、レイヤ 3 に変更されます。

（注） IPv4 ネットワーク レイヤ プロトコルでは、LWAPP コントローラ システムによる転送がサポートされています。IPv6（クライアント用のみ）と Appletalk もサポートされていますが、4400 シリーズ コントローラと Cisco WiSM でのみのサポートとなります。他のレイヤ 3 プロトコル（IPX、DECnet Phase IV、OSI CLNP など）およびレイヤ 2（ブリッジ）プロトコル（LAT および NetBeui など）はサポートされていません。

動作上の要件

レイヤ 2 LWAPP 通信の要件として、Cisco Wireless LAN Controller と Lightweight アクセス ポイントが同一サブネット上のレイヤ 2 デバイスを使用して相互接続されている必要があります。Cisco Wireless LAN Controller と Lightweight アクセス ポイントが異なるサブネット上にあるときは、デバイスはレイヤ 3 モードで動作しなければならないことに注意してください。

レイヤ 3 LWAPP 通信を行う場合、Cisco Wireless LAN Controller と Lightweight アクセス ポイントが同一サブネットにあるときには、それらをレイヤ 2 デバイスを使用して接続します。異なるサブネットにある場合は、レイヤ 3 デバイスを使用して接続します。また、アクセス ポイントの IP アドレスが外部 DHCP サーバを介して静的または動的に割り当てられていることも必要です。

モビリティ グループに属するすべての Cisco Wireless LAN Controller では、同じ LWAPP レイヤ 2 またはレイヤ 3 モードを使用する必要があります。それ以外の場合は、モビリティ ソフトウェアのアルゴリズムが無効になります。

設定上の要件

レイヤ 2 モードで Cisco Wireless LAN Solution を稼働している場合は、レイヤ 2 通信を制御するよう管理インターフェイスを設定する必要があります。

レイヤ 3 モードで Cisco Wireless LAN Solution を稼働させている場合は、Lightweight アクセス ポイントおよびレイヤ 2 モード用に設定された管理インターフェイスを制御するよう AP 管理インターフェイスを設定する必要があります。

Cisco Wireless LAN Controller

Cisco Wireless LAN Controller が複数展開されたネットワークに Lightweight アクセス ポイントを追加する場合、すべての Lightweight アクセス ポイントを、同一サブネット上の 1 つのマスター コントローラにアソシエートさせると便利です。そうすれば、オペレータが複数のコントローラにログインして、新たに追加された Lightweight アクセス ポイントがアソシエートされているコントローラを検索する必要はなくなります。

Lightweight アクセス ポイントを追加するとき、各サブネット内の 1 つのコントローラをマスター コントローラとして割り当てることができます。同一サブネット上のマスター コントローラがアクティブである限り、プライマリ、セカンダリ、およびターシャリ コントローラが割り当てられていない新しいアクセス ポイントはすべて、マスター Cisco Wireless LAN Controller とのアソシエートを自動的に試みます。このプロセスについては、「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P. 1-19）を参照してください。

オペレータは、WCS Web ユーザ インターフェイスを使用して、マスター コントローラを監視し、アクセス ポイントがマスター コントローラにアソシエートするのを確認できます。次に、オペレータは、アクセス ポイント設定を確認して、プライマリ、セカンダリ、ターシャリ コントローラをアクセス ポイントに割り当てて、プライマリ、セカンダリ、またはターシャリ コントローラに再アソシエートするように、アクセス ポイントをリブートします。

（注） Lightweight アクセス ポイントでは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられていない場合、リブート時には必ずマスター コントローラが最初に検索されます。マスター コントローラ経由による Lightweight アクセス ポイントを追加したら、プライマリ、セカンダリ、またはターシャリ コントローラを各アクセス ポイントに割り当ててください。シスコでは、初期設定後にすべてのコントローラのマスター設定を無効にすることを推奨しています。

プライマリ、セカンダリ、ターシャリ コントローラ

マルチコントローラ ネットワークでは、Lightweight アクセス ポイントは同じサブネット上の任意のコントローラにアソシエートできます。確実にすべてのアクセス ポイントを特定のコントローラにアソシエートするために、オペレータは、プライマリ、セカンダリ、およびターシャリ コントローラをアクセス ポイントに割り当てることができます。

用意したアクセス ポイントはネットワークに追加されると、プライマリ、セカンダリ、およびターシャリ コントローラをまず検索してから、使用可能なアクセス ポイント ポートを持つ、最も負荷の少ないコントローラを検索します。詳細は、「Cisco Wireless LAN Controller のフェールオーバーの保護」の項（P. 1-19）を参照してください。

クライアント ロケーション

Cisco Wireless LAN Solution で Cisco WCS を使用する場合、コントローラは、クライアント、不正なアクセス ポイント、不正なアクセス ポイント クライアント、無線周波数 ID（RFID）タグ ロケーションを定期的にチェックし、そのロケーションを Cisco WCS データベースに保存します。ロケーション ソリューションに関する詳細は、『Cisco Wireless Control System Configuration Guide』および『Cisco Location Appliance Configuration Guide』を参照してください。これらのガイドの URL は次のとおりです。

『Cisco Wireless Control System Configuration Guide』

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

『Cisco Location Appliance Configuration Guide』

http://www.cisco.com/en/US/products/ps6386/products_installation_and_configuration_guides_list.html

コントローラ プラットフォーム

コントローラは、802.11a/n プロトコルおよび 802.11b/g/n プロトコルをサポートする、企業向けの高性能無線スイッチング プラットフォームです。Radio Resource Management（RRM）機能が搭載されているオペレーティング システムの制御下でコントローラを稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する Cisco UWN Solution が実現されます。コントローラは、高性能なネットワークおよびセキュリティ ハードウェアを中心に構築されており、他に例のないセキュリティを備えた信頼性の高い 802.11 企業ネットワークが実現します。

- Cisco 2100 シリーズ コントローラ
- Cisco 4400 シリーズ コントローラ
- Catalyst 6500 シリーズ ワイヤレス サービス モジュール（WiSM）
- Cisco 7600 シリーズ ルータ ワイヤレス サービス モジュール（WiSM）
- コントローラ ネットワーク モジュール内蔵の Cisco 28/37/38xx シリーズ サービス統合型ルータ
- Catalyst 3750G 統合型無線 LAN コントローラ スイッチ

最初の 3 つのコントローラはスタンドアロン プラットフォームです。その他の 4 つのコントローラは、シスコのスイッチおよびルータ製品に統合されています。

Cisco 2100 シリーズ コントローラ

Cisco 2100 シリーズ Wireless LAN Controller は、Cisco Lightweight アクセス ポイントおよび Cisco Wireless Control System（WCS）と組み合わせて使用することで、システム全体での無線 LAN 機能を実現します。2100 シリーズ コントローラは、それぞれ最大 6 個の Lightweight アクセス ポイントを制御し、企業の支社展開で一般的なマルチコントローラ アーキテクチャに適しています。小規模から中規模の環境のためのシングル コントローラ展開にも使用できます。

注意　コントローラのコンソール ポートに Power over Ethernet（PoE）ケーブルを接続しないでください。接続すると、コントローラが損傷するおそれがあります。

（注）　アクセス ポイントをコントローラに再接続するときは、20 秒以上待ってから接続してください。待たずに接続すると、コントローラがデバイスを検出できないことがあります。

サポートされない機能

次に示すハードウェア機能は、2100 シリーズ コントローラではサポートされません。

- サービス ポート（専用の帯域外管理 10/100 Mbps イーサネット インターフェイス）

次に示すソフトウェア機能は、2100 シリーズ コントローラではサポートされません。

- VPN 終端（IPSec、L2TP など）
- ゲスト コントローラ トンネルの終端（ゲスト コントローラ トンネルの起点は可能）

- 外部 Web 認証 Web サーバ リスト
- レイヤ 2 LWAPP
- スパニング ツリー
- ポートのミラーリング
- Cranite
- Fortress
- AppleTalk
- QoS ユーザごと帯域幅コントラクト
- IPv6 パススルー
- リンク集約（LAG）

Cisco 4400 シリーズ コントローラ

Cisco 4400 シリーズ Wireless LAN Controller には、4402 と 4404 の 2 つのモデルがあります。4402 では最大 50 個、4404 では最大 100 個の Lightweight アクセス ポイントがサポートされ、大企業や高密度アプリケーションに理想的な LAN 環境が実現されます。

4400 シリーズ コントローラには、1 つまたは 2 つの Cisco 4400 シリーズ電源を装着できます。4400 シリーズ コントローラに 2 つの Cisco 4400 シリーズ電源を装着しておけば、電源が冗長構成になり、一方の電源に障害が発生した場合でも、他方の電源から引き続きコントローラに電力を供給できます。

Catalyst 6500 シリーズ ワイヤレス サービス モジュール

Catalyst 6500 シリーズ Wireless Services Module（WiSM; ワイヤレス サービス モジュール）は、Catalyst 6500 スイッチと 2 つの Cisco 4404 コントローラが統合されたもので、最大 300 個の Lightweight アクセス ポイントをサポートします。スイッチには、スイッチとコントローラを接続する内部ギガバイト イーサネット ポートが 8 個装備されています。スイッチと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。

（注） Catalyst 6509 スイッチのシャーシは、他のサービス モジュールがインストールされていなければ最大 7 個の Cisco WiSM をサポートすることができ、Supervisor 720 がインストールされている Catalyst 6506 は、最大 4 個の Cisco WiSM をサポートできます。その他の Catalyst 6500 シリーズ スイッチのシャーシは、最大 6 個の Cisco WiSM をサポートできます。サービス モジュールが 1 つ以上インストールされている場合、シャーシがサポート可能なサービス モジュールの数は最大 4 個となります（WiSM を含む）。これらの最大設定には、冗長スーパーバイザは使用できません。

詳細は、次のドキュメントを参照してください。

- 『Catalyst 6500 Series Switch Installation Guide』
- 『Catalyst 6500 Series Switch Wireless Services Module Installation and Configuration Note』
- 『Release Notes for Catalyst 6500 Series Switch Wireless LAN Services Module』
- 『Configuring a Cisco Wireless Services Module and Wireless Control System』
- 『Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

Cisco 7600 シリーズ ルータ ワイヤレス サービス モジュール

Cisco 7600 シリーズ ルータ ワイヤレス サービス モジュール（WiSM）は、1 つの Cisco 7600 ルータと 2 つの Cisco 4404 コントローラが統合されたもので、最大 300 個の Lightweight アクセス ポイントをサポートします。ルータには、ルータとコントローラを接続する内部ギガバイト イーサネット ポートが 8 個装備されています。ルータと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。

（注） WiSM は、Cisco IOS Release 12.2(18)SXF5 以降のみを実行する Cisco 7600 シリーズ ルータでサポートされています。

（注） Cisco 7609 ルータのシャーシは、他のサービス モジュールがインストールされていなければ最大 7 個の Cisco WiSM をサポートできます。Cisco 7600 シリーズ ルータのシャーシは、他のサービス モジュールがインストールされていなければ最大 6 個の Cisco WiSM をサポートできます。サービス モジュールが 1 つ以上インストールされている場合、シャーシがサポート可能なサービス モジュールの数は最大 4 個となります（WiSM を含む）。これらの最大設定には、冗長スーパーバイザは使用できません。

詳細は、次のドキュメントを参照してください。

- 『Cisco 7600 Series Router Installation Guide』
- 『Cisco 7600 Series Router Software Configuration Guide』
- 『Cisco 7600 Series Router Command Reference』
- 『Configuring a Cisco Wireless Services Module and Wireless Control System』
- 『Catalyst 6500 Series Switch and Cisco 7600 Series Router Wireless Services Module Installation and Verification Note』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/routers/ps368/tsd_products_support_series_home.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html

http://www.cisco.com/en/US/docs/wireless/technology/wism/installation/note/78_17121.html

Cisco 28/37/38xx シリーズ サービス統合型ルータ

Cisco 28/37/38xx シリーズ サービス統合型ルータは、28/37/38xx ルータと Cisco コントローラ ネットワーク モジュールを統合したもので、ネットワーク モジュールのバージョンに応じて最大 6 個、8 個、または 12 個の Lightweight アクセス ポイントをサポートします。8 個または 12 個のアクセス ポイントをサポート可能なバージョンは、高速プロセッサと大容量のオンボード メモリを備えています。内部ファスト イーサネット ポート（6 アクセス ポイント バージョン）または内部ギガビット イーサネット ポート（8 アクセス ポイントおよび 12 アクセス ポイント バージョン）によって、ルータと統合コントローラが接続されます。ルータと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。詳細は、次のドキュメントを参照してください。

- 『Cisco Wireless LAN Controller Network Module Feature Guide』
- 『Cisco 28/37/38xx Series Hardware Installation Guide』

これらのドキュメントには、次の URL からアクセスできます。

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

（注） Cisco 2801 サービス統合型ルータでは、コントローラ ネットワーク モジュールはサポートされません。

Catalyst 3750G 統合型無線 LAN コントローラ スイッチ

Catalyst 3750G 統合型無線 LAN コントローラ スイッチは、Catalyst 3750 スイッチと Cisco 4400 シリーズ コントローラが統合されたもので、最大 25 個または 50 個の Lightweight アクセス ポイントをサポートします。スイッチには、スイッチとコントローラを接続する内部ギガバイト イーサネット ポートが 2 個装備されています。スイッチと内部コントローラではそれぞれ異なるソフトウェア バージョンが実行されており、これらのソフトウェア バージョンは個別にアップグレードする必要があります。詳細は、次のドキュメントを参照してください。

- 『Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide』
- 『Catalyst 3750 Switch Hardware Installation Guide』
- 『Release Notes for the Catalyst 3750 Integrated Wireless LAN Controller Switch, Cisco IOS Release 12.2(25)FZ』

これらのドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/switches/ps5023/tsd_products_support_series_home.html

Cisco UWN Solution の有線接続

Cisco UWN Solution のコンポーネントは、業界標準のイーサネット ケーブルとコネクタを使用して相互に通信します。ここでは、有線接続について説明します。

- 2100 シリーズ コントローラをネットワークに接続するときは、1 ～ 6 本の 10/100BASE-T イーサネット ケーブルを使用します。
- 4402 コントローラをネットワークに接続するときは、1 ～ 2 本の光ファイバ ギガビット イーサネット ケーブルを使用します。4404 コントローラをネットワークに接続するときは、最大 4 本の光ファイバ ギガビット イーサネット ケーブルを使用します。ギガビット イーサネット接続を冗長化しておけば、ネットワーク上のいずれかの箇所で障害が発生した場合でも、それを迂回できます。
- Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータにインストールされた Wireless Services Module（WiSM）内のコントローラをネットワークに接続するときは、スイッチまたはルータ上のポートを使用します。
- Cisco サービス統合型ルータにインストールされている Wireless LAN Controller ネットワーク モジュールをネットワークに接続するときは、ルータのポートを使用します。
- Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラをネットワークに接続するときは、スイッチのポートを使用します。
- Cisco Lightweight アクセス ポイントをネットワークに接続するときは、10/100BASE-T イーサネット ケーブルを使用します。標準の CAT-5 ケーブルを使用して、Power over Ethernet（PoE）機能が搭載されているネットワーク デバイスから Lightweight アクセス ポイントへ電力を供給することもできます。この電源分配プランを使用すると、個々のアクセス ポイント電源供給と接続用ケーブルにかかるコストを軽減できます。

Cisco UWN Solution 無線 LAN

Cisco UWN Solution では、Lightweight アクセス ポイントについて、最大 16 の無線 LAN を制御できます。各 WLAN には、それぞれ異なる WLAN ID（1 ～ 16）と WLAN SSID（WLAN 名）が割り当てられます。また、一意のセキュリティ ポリシーを割り当てることもできます。ソフトウェア リリース 3.2 以降を使用すると、同じ無線 LAN 上で静的 WEP と動的 WEP の両方を設定できます。

Lightweight アクセス ポイントでは、すべてのアクティブな Cisco UWN Solution 無線 LAN SSID をブロードキャストし、各無線 LAN に定義されているポリシーを適用します。

（注） コントローラが最適な性能と容易な管理で動作できるよう、無線 LAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

Cisco UWN Solution で無線による管理を有効にすると、オペレータは CLI と Telnet、http/https、および SNMP を使用して、有効になった無線 LAN 全体のシステムを管理できるようになります。

無線 LAN の設定については、第 6 章を参照してください。

ID ネットワーキング

コントローラでは、次のパラメータを、特定の無線 LAN にアソシエートしているすべてのクライアントに適用できます。適用可能なパラメータは、QoS、グローバルまたはインターフェイス固有の DHCP サーバ、レイヤ 2 とレイヤ 3 のセキュリティ ポリシー、およびデフォルトのインターフェイス（物理ポート、VLAN、および ACL 割り当てを含む）です。

ただし、MAC フィルタリングを使用するか、または AAA Override パラメータを許可することによって、個々のクライアント（MAC アドレス）にプリセットされている無線 LAN パラメータを無効にすることもできます。たとえば、この設定を使用すると、社内の全クライアントを会社の無線 LAN にログインさせてから、MAC アドレスごとに、異なる QoS、DHCP サーバ、レイヤ 2 とレイヤ 3 のセキュリティ ポリシー、およびインターフェイス設定を使用して、クライアントを接続させることができます。

Cisco UWN Solution オペレータがクライアントに対して MAC フィルタリングを設定するときに、別の VLAN を MAC アドレスに割り当てることができます。そして、このことを利用して、クライアントがオペレーティング システムによって自動的に管理インターフェイスまたはオペレータ定義インターフェイスに再ルーティングされるようにすることができます。インターフェイスはそれぞれ、独自の VLAN、ACL、DHCP サーバ、および物理ポート割り当てが設定されています。この MAC フィルタリングはおおまかな AAA Override として使用でき、通常、いずれも AAA（RADIUS またはその他の）Override より優先されます。

ただし、Allow AAA Override が有効である場合は、MAC アドレスごとに QoS と ACL を返すように、RADIUS（またはその他の AAA）サーバを設定することもできます。Allow AAA Override が有効な場合は、コントローラで設定されている MAC フィルタリング パラメータよりも AAA Override が優先されます。特定の MAC アドレスで使用できる AAA Override がない場合は、コントローラの既存の MAC フィルタリング パラメータがオペレーティング システムによって使用されます。この AAA（RADIUS またはその他の）Override は詳細な AAA Override として使用できますが、Allow AAA Override が有効な場合のみ、MAC フィルタリングより優先されます。

どのような場合でも、Override パラメータ（オペレータ定義のインターフェイスや QoS など）をコントローラの設定で事前に定義しておく必要があります。

いずれの場合も、レイヤ 2 認証が使用されるかレイヤ 3 認証が使用されるかにかかわらず、AAA サーバまたは MAC フィルタリングで指定されている QoS と ACL がオペレーティング システムによって使用されます。

また、MAC フィルタリング、802.1X、または WPA レイヤ 2 認証が設定されている場合、オペレーティング システムが行うのはクライアントをデフォルトの Cisco UWN Solution 無線 LAN VLAN から別の VLAN に移動することだけです。無線 LAN の設定については、第 6 章を参照してください。

Cisco Secure ACS との統合の強化

ID ベースのネットワーキング機能は、認証、認可、アカウンティング（AAA）Override を使用します。次のベンダー固有属性が RADIUS アクセス ポイント メッセージに存在する場合は、値が無線 LAN プロファイルで指定された値を上書きします。

- QoS レベル
- 802.1p 値
- VLAN インターフェイス名
- アクセス コントロール リスト（ACL）名

このリリースでは、IETF RFC 2868（トンネル プロトコル サポートのための RADIUS 属性）で定義されている標準の「RADIUS による VLAN 名 / 番号の割り当て」機能を使用して AAA サーバが VLAN の番号または名前を返せるようにするためのサポートが追加されています。無線クライアントを特定の VLAN に割り当てるために、AAA サーバはアクセス ポイント メッセージ内で次の属性をコントローラに送信します。

- IETF 64（トンネル タイプ）：VLAN
- IETF 65（トンネル メディア タイプ）：802
- IETF 81（トンネル プライベート グループ ID）：VLAN # または VLAN 名文字列

これにより、Cisco Secure ACS はポスチャ分析の結果となりえる VLAN の変更を通信できるようになります。この機能の利点は、次のとおりです。

- Cisco Secure ACS との統合により、インストールとセットアップ時間が短縮されます。
- Cisco Secure ACS は、有線および無線ネットワーク上で円滑に動作します。

この機能は、2100 シリーズと 4400 シリーズのコントローラ、および 1130 シリーズと 1200 シリーズの Lightweight アクセス ポイントをサポートします。

ファイル転送

Cisco UWN Solution のオペレータは、GUI、CLI コマンド、または Cisco WCS を使用して、オペレーティング システムのコード、設定、および証明書ファイルをコントローラにアップロードしたり、コントローラからダウンロードしたりできます。

- CLI　コマンドの使用方法については、「コントローラとのファイルのやり取り」の項（P. 8-9）を参照してください。
- Cisco WCS を使用してソフトウェアをアップグレードする方法については、『Cisco Wireless Control System Configuration Guide』を参照してください。以下の URL をクリックすると、このガイドを参照できます。

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

Power over Ethernet

Lightweight アクセス ポイントは、イーサネット ケーブルを介して、802.3af 準拠の Power over Ethernet（PoE）デバイスから電力供給を受けることができます。これにより、個々のデバイスへの電力供給や、余分な配線、コンジット、コンセントにかかるコストが軽減され、設置時間を短縮できます。PoE 機能を使用すると、設置担当者は、AC コンセントの近くに Cisco 1000 シリーズ Lightweight アクセス ポイントやその他の電力供給を要する装置を取り付ける必要がなくなるため、Cisco 1000 シリーズ Lightweight アクセス ポイントをより柔軟に配置して、最大カバレッジを得ることができます。

PoE を使用している場合、1 本の CAT-5 ケーブルを各 Lightweight アクセス ポイントから PoE 機能が搭載されているネットワーク要素（PoE 電源ハブや、Cisco WLAN Solution シングルライン PoE インジェクタなど）に接続します。PoE 機器で Lightweight アクセス ポイントが PoE 対応であると判断された場合は、使用されていないイーサネット ケーブル ペアを使って、48VDC の電力が Lightweight アクセス ポイントに供給されます。

PoE ケーブルの長さは、100BASE-T 仕様では 100m、10BASE-T 仕様では 200m に制限されています。

Lightweight アクセス ポイントは、802.3af 準拠デバイスまたは外部電源装置から電力供給を受けることができます。

スタートアップ ウィザード

工場出荷の新しいオペレーティング システム ソフトウェアをロードしたり、工場出荷時のデフォルトにリセットした後でコントローラの電源を入れると、起動スクリプトによりスタートアップ ウィザードが実行され、初期設定を要求するプロンプトが表示されます。スタートアップ ウィザードでは次のことを行います。

- コントローラに 32 文字以下のシステム名が付いていることを確認します。
- 管理ユーザ名とパスワードを追加します（それぞれ 24 文字以下）。
- コントローラがサービス ポートを使用して GUI、CLI、または Cisco WCS（直接的にまたは間接的に）と通信できるように設定します。この設定を行うには、有効な IP 設定プロトコル（none または DHCP）を入力し、none の場合は IP アドレスとネットマスクを入力します。サービス ポートを使用しない場合、IP アドレスおよびネットマスクは 0.0.0.0 と入力します。
- コントローラが管理インターフェイスでネットワーク（802.11 ディストリビューション システム）と通信できることを確認します。これは、有効な固定 IP アドレス、ネットマスク、デフォルトのルータ IP アドレス、VLAN 識別子、および物理ポート割り当てを収集することで確認します。
- DHCP サーバの IP アドレスを入力します。これは、クライアント、コントローラ管理インターフェイス、およびオプションでサービス ポート インターフェイスに IP アドレスを指定する際に使用されます。
- LWAPP 転送モードを入力します。詳細は、「レイヤ 2 およびレイヤ 3 の Lightweight Access Point protocol（LWAPP）動作」の項（P. 1-7）を参照してください。
- 仮想ゲートウェイ IP アドレスを収集します。これは、任意の架空、未割り当ての IP アドレス（1.1.1.1 など）で、レイヤ 3 Security Manager と Mobility Manager で使用されます。
- ユーザがモビリティ グループ（RF グループ）名を入力できるようにします。
- 無線 LAN 1 802.11 SSID またはネットワーク名を収集します。
- クライアントが固定 IP アドレスを使用できるようにするかどうかを指定します。Yes に設定すると使い勝手は良くなりますが、セキュリティが低下します（セッションがハイジャックされる可能性がある）。クライアントが自分自身の IP アドレスを指定できるので、DHCP を使用できないデバイスに適した設定です。No に設定すると、使い勝手は悪くなりますが、セキュリティが向上します。また、クライアントが IP アドレスの DHCP を指定する必要があり、XP デバイスに適した設定でもあります。
- スタートアップ ウィザードから RADIUS サーバを設定する場合は、RADIUS サーバの IP アドレス、通信ポート、および秘密鍵の入力を要求します。
- 国コードを収集します。
- 802.11a/n および 802.11b/g/n Lightweight アクセス ポイント ネットワークを有効または無効にします。
- Radio Resource Management（RRM）を有効または無効にします。

スタートアップ ウィザードの使用方法については、「設定 ウィザードの使用方法」の項（P. 4-2）を参照してください。

Cisco Wireless LAN Controller のメモリ

コントローラには 2 種類のメモリがあります。揮発性 RAM には、現在のアクティブなコントローラ設定が保持され、NVRAM（非揮発性 RAM）にはリブート設定が保持されます。コントローラのオペレーティング システムを設定すると、揮発性 RAM の内容が変更されます。したがって、揮発性 RAM の設定を NVRAM に保存し、コントローラが現在の設定でリブートされるようにする必要があります。

次の処理を行うときは、どちらのメモリを編集しているか理解していることが重要となります。

- 設定ウィザードの使用方法
- コントローラの設定のクリア
- 設定の保存
- コントローラのリセット
- CLI からのログアウト

Cisco Wireless LAN Controller のフェールオーバーの保護

各コントローラには、定義された数の Lightweight アクセス ポイント用通信ポートが装備されています。つまり、未使用のアクセス ポイント ポートがある複数のコントローラが同じネットワーク上に展開されている場合、1 つのコントローラが故障すると、ドロップしたアクセス ポイントは、自動的に未使用のコントローラ ポートをポーリングして、そのポートにアソシエートします。

インストール時に、すべての Lightweight アクセス ポイントを専用のコントローラに接続して、最終的な作業として各 Lightweight アクセス ポイントを設定することをお勧めします。この手順では、プライマリ、セカンダリ、ターシャリ コントローラについてそれぞれの Lightweight アクセス ポイントを設定し、設定したモビリティ グループ情報を格納できるようにします。

フェールオーバー回復時に、設定した Lightweight アクセス ポイントが、ローカル DHCP サーバから IP アドレスを取得し（レイヤ 3 動作でのみ）、プライマリ、セカンダリ、ターシャリ コントローラへの接続を試み、次にモビリティ グループ内のその他のコントローラの IP アドレスへの接続を試みます。これにより、アクセス ポイントがブラインド ポーリング メッセージを送信する時間が必要なくなるため、結果的に回復期間が短縮されます。

マルチコントローラ展開では、1 つのコントローラが故障すると、ドロップしたアクセス ポイントが再度ブートされて、Radio Resource Management（RRM）の指示の下で次の処理が行われます。

- ローカル DHCP サーバ（ローカル サブネット上にあるサーバ）の IP アドレスを取得します。
- Lightweight アクセス ポイントは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられている場合、そのコントローラにアソシエートを試みます。
- アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられていない場合、またはプライマリ、セカンダリ、ターシャリ コントローラが使用できない場合には、同一サブネット上のマスター コントローラにアソシエートを試みます。
- アクセス ポイントが同一サブネット上でマスター コントローラを検出できなかった場合は、格納されているモビリティ グループ メンバに IP アドレスで接続を試みます。
- 使用できるモビリティ グループ メンバがない場合、および Lightweight アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられておらず、アクティブなマスター コントローラがない場合、Lightweight アクセス ポイントは、同一サブネット上で最も負荷の少ないコントローラにアソシエートを試み、未使用ポートを使用してそのディスカバリ メッセージに応答します。

つまり、十分なコントローラが展開されている場合には、1 つのコントローラが故障したとしても、アクティブなアクセス ポイントのクライアント セッションがただちにドロップする一方で、ドロップしたアクセス ポイントが別のコントローラの未使用ポートにアソシエートするため、クライアント デバイスはすぐに再アソシエートと再認証を行うことができます。

Cisco Wireless LAN Controller へのネットワーク接続

すべてのコントローラは、動作モードに関係なく、ネットワークを 802.11 ディストリビューション システムとして使用します。コントローラは、イーサネット ポートのタイプや速度に関係なく、関連付けられているコントローラの監視と通信をネットワークを使用して行います。以降の項では、次のネットワーク接続について説明します。

- Cisco 2100 シリーズ Wireless LAN Controller（P. 1-20）
- Cisco 4400 シリーズ Wireless LAN Controller（P. 1-21）

（注） コントローラのポートの設定とコントローラへのインターフェイスの割り当てについては、第 3 章を参照してください。

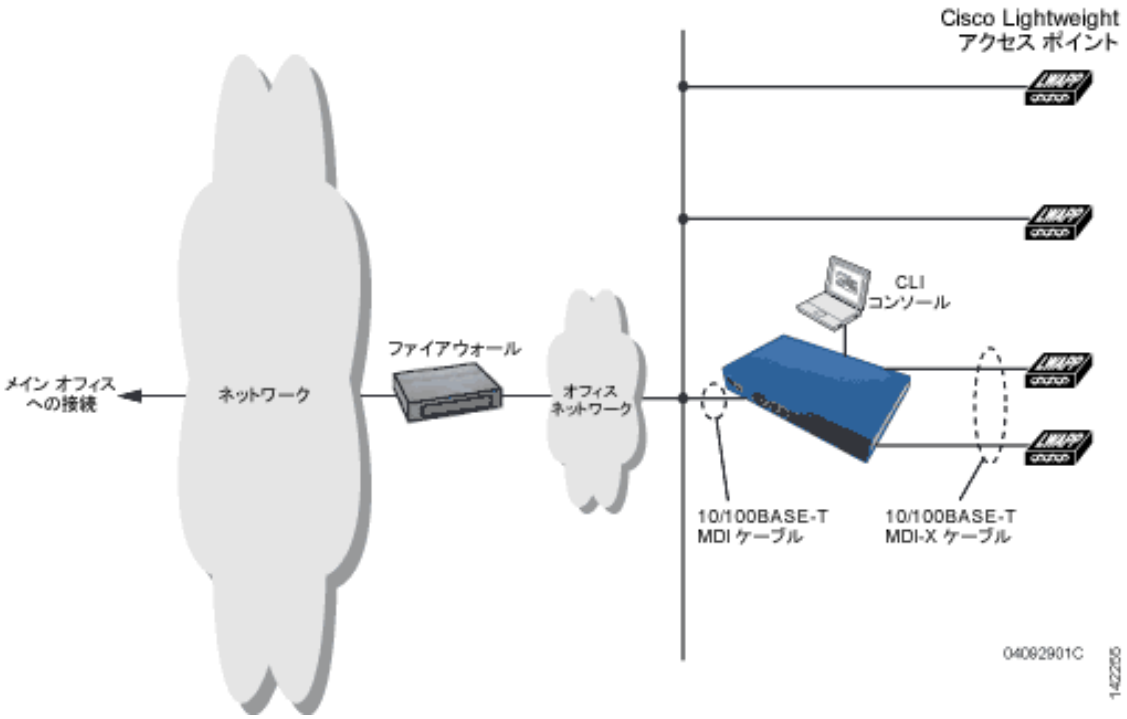
Cisco 2100 シリーズ Wireless LAN Controller

Cisco 2100 シリーズ コントローラでは、ネットワークとの通信に任意の物理データ ポートを 1 つ使用できます。また、ポートの 1 つに論理管理インターフェイスを割り当てることができます。物理ポートについては、次の説明を参照してください。

- 最大 6 本の 10/100BASE-T ケーブルを 2100 シリーズ コントローラ シャーシの 6 つの背面パネル データ ポートに接続できます。2100 シリーズには、2 個の PoE ポートもあります（ポート 7 および 8）。

図 1-4 は、2100 シリーズ コントローラへの接続を示しています。

図 1-4　2100 シリーズ コントローラへの物理ネットワーク接続



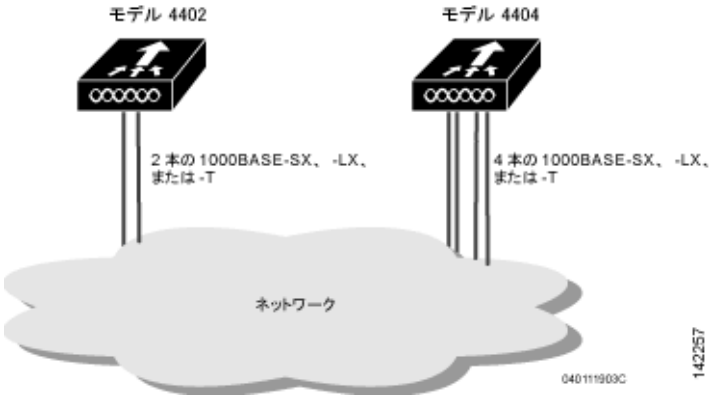
Cisco 4400 シリーズ Wireless LAN Controller

Cisco 4400 シリーズ コントローラは、1 つまたは 2 つの物理データ ポート ペアを使ってネットワークと通信でき、論理管理インターフェイスを物理ポートに割り当てることができます。物理ポートの説明は次のとおりです。

- For the 4402 コントローラでは、次の接続のうち、2 つまでの接続が任意の組み合わせでサポートされます。
  - 1000BASE-T（ギガビット イーサネット、前面パネル、RJ-45 物理ポート、UTP ケーブル）
  - 1000BASE-SX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 850nM（SX）光ファイバ リンク）
  - 1000BASE-LX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 1300nM（LX/LH）光ファイバ リンク）
- 4404 コントローラでは、次の接続のうち、4 つまでの接続が任意の組み合わせでサポートされます。
  - 1000BASE-T（ギガビット イーサネット、前面パネル、RJ-45 物理ポート、UTP ケーブル）
  - 1000BASE-SX（ギガビット イーサネット、前面パネル、LC 物理ポート、LC 物理コネクタを使用したマルチモード 850nM（SX）光ファイバ リンク）
  - 1000BASE-LX（ギガビット イーサネット、前面パネル、LX 物理ポート、LC 物理コネクタを使用したマルチモード 1300nM（LX/LH）光ファイバ リンク）

図 1-5 は、4400 シリーズ コントローラへの接続を示しています。

図 1-5　4402 および 4404 シリーズ コントローラへの物理ネットワーク接続



CHAPTER 2

Web ブラウザと CLI インターフェイスの使用方法

この章では、コントローラの設定に使用する Web ブラウザと CLI インターフェイスについて説明します。この章の内容は、次のとおりです。

Web ブラウザ インターフェイスの使用方法

Web ブラウザ インターフェイス（以降、GUI）は、すべてのコントローラに組み込まれています。最大 5 名のユーザが、コントローラ http または https（http + SSL）管理ページを同時に閲覧して、パラメータを設定し、コントローラとそのアソシエートされているアクセス ポイントの動作ステータスを監視することができます。

（注） Cisco UWN Solution のセキュリティを強化するために、HTTPS インターフェイスを有効にし、HTTP インターフェイスを無効にすることをお勧めします。

GUI を使用する際の注意事項

GUI を使用するときは、次の点に留意してください。

- GUI は、Windows XP SP1 以上または Windows 2000 SP4 以上が動作するコンピュータで使用してください。
- この GUI は、Microsoft Internet Explorer バージョン 6.0 SP1 以上と完全に互換性があります。

（注） Opera、Mozilla、および Netscape はサポートされていません。

（注） Web 認証を使用するには、Microsoft Internet Explorer バージョン 6.0 SP1 以上が必要です。

- サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、サービス ポート インターフェイスの使用をお勧めします。サービス ポート インターフェイスの設定方法については、第 3 章を参照してください。
- GUI のページ上部にある **Help** をクリックすると、オンライン ヘルプが表示されます。オンライン ヘルプを表示するには、ブラウザのポップアップ ブロックを無効にする必要があります。

GUI の表示

GUI を開くには、ブラウザのアドレス行にコントローラの IP アドレスを入力します。セキュリティで保護されている接続の場合は、**https://**<IP アドレス > と入力します。セキュリティの保護が十分でない接続の場合は、**http://**<IP アドレス > と入力します。HTTPS をセットアップする手順は、「GUI を使用した Web およびセキュア Web モードの有効化」の項（P. 2-3）を参照してください。

Web モードおよびセキュア Web モードの有効化

この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。HTTPS を有効化すると、GUI との通信を保護できます。HTTPS では、SSL（Secure Socket Layer）プロトコルを使用することによって、HTTP ブラウザのセッションを保護します。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。また、外部で生成された証明書をダウンロードすることもできます。

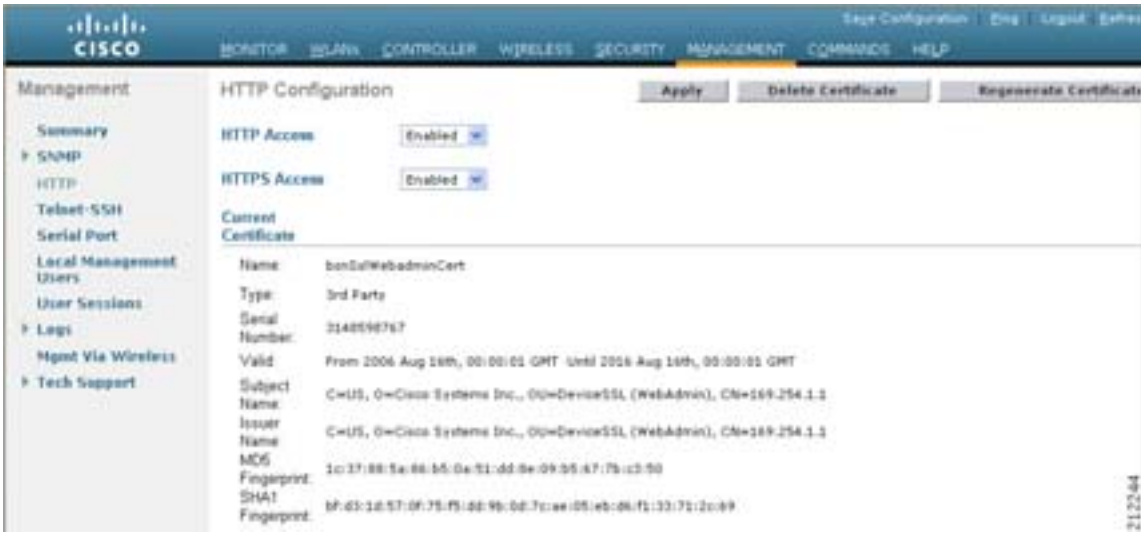
コントローラ GUI または CLI を使用して、Web および セキュア Web モードを設定できます。

GUI を使用した Web およびセキュア Web モードの有効化

コントローラの GUI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　**Management** > **HTTP** の順にクリックして、HTTP Configuration ページを開きます（図 2-1 を参照）。

図 2-1　HTTP Configuration ページ



ステップ 2　Web モードを有効にすると、ユーザが「http://<IP アドレス >」を使用してコントローラ GUI にアクセスできるようになります。そのためには、HTTP Access ドロップダウン ボックスから **Enabled** を選択します。有効にしない場合は、**Disabled** を選択します。デフォルト値は Disabled です。Web モードの接続は、セキュリティで保護されていません。.

ステップ 3　セキュア Web モードを有効にすると、ユーザが「https://<IP アドレス >」を使用してコントローラ GUI にアクセスできるようになります。そのためには、HTTPS Access ドロップダウン ボックスから **Enabled** を選択します。有効にしない場合は、**Disabled** を選択します。デフォルト値は Enabled です。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　ステップ 3 でセキュア Web モードを有効にすると、コントローラはローカル Web アドミニストレーション SSL 証明書を生成して自動的に GUI に適用します。現在の証明書の詳細は、HTTP Configuration ページの中央に表示されます（図 2-1 を参照）。

（注）　独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」の項（P. 2-5）の手順を参照してください。

（注） 必要に応じて、**Delete Certificate** をクリックして現在の証明書を削除し、**Regenerate Certificate** をクリックして新しい証明書を生成するようコントローラで指定できます。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した Web およびセキュア Web モードの有効化

コントローラの CLI を使用して、Web モード、セキュア Web モード、またはその両方を有効にする手順は、次のとおりです。

ステップ 1　Web モードを有効または無効にするには、次のコマンドを入力します。

config network webmode {**enable** | **disable**}

このコマンドにより「http://<IP アドレス >」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は、Disabled です。Web モードの接続は、セキュリティで保護されていません。.

ステップ 2　セキュア Web モードを有効または無効にするには、次のコマンドを入力します。

config network secureweb {**enable** | **disable**}

このコマンドにより「https://<IP アドレス >」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は、Enabled です。セキュア Web モードの接続は、セキュリティで保護されています。

ステップ 3　セキュア Web モードのセキュリティの強化を有効または無効にするには、次のコマンドを入力します。

config network secureweb cipher-option high {**enable** | **disable**}

このコマンドにより、「https://<IP アドレス >」を使用してコントローラの GUI にアクセスできます。ただし、128 ビット（またはそれ以上）の暗号をサポートするブラウザ以外からは、アクセスできません。デフォルト値は無効です。

ステップ 4　コントローラが証明書を生成したことを確認するには、次のコマンドを入力します。

show certificate summary

次のような情報が表示されます。

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

（注） 独自の SSL 証明書をコントローラにダウンロードする場合は、「外部で生成した SSL 証明書のロード」の項（P. 2-5）の手順を参照してください。

ステップ 5　（オプション）新しい証明書を生成する場合は、次のコマンドを入力します。

config certificate generate webadmin

数秒後、コントローラでは、証明書が生成されたことが確認されます。

ステップ 6　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM（不揮発性 RAM）に保存するには、次のコマンドを入力します。

save config

ステップ 7　コントローラをリブートするには、次のコマンドを入力します。

reset system

外部で生成した SSL 証明書のロード

TFTP サーバを使用して、外部で生成された SSL 証明書をコントローラにダウンロードできます。TFTP を使用する際の注意事項は次のとおりです。

- サービス ポート経由で証明書をロードする場合、サービス ポートはルーティングできないため、TFTP サーバはコントローラと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。また、証明書を Distribution System（DS; ディストリビューション システム）のネットワーク ポートでロードすると、TFTP サーバを任意のサブネット上におくこともできます。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

（注）　各 HTTPS 証明書には RSA キーが組み込まれています。キーの長さは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまで対応しています。認証局から新しい証明書を取得する際、証明書に組み込まれた RSA キーの長さが 768 ビットより長いことを確認してください。

GUI を使用した SSL 証明書のロード

コントローラの GUI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　HTTP Configuration ページで、**Download SSL Certificate** チェックボックスをオンにします（図 2-2 を参照）。

図 2-2　HTTP Configuration ページ

ステップ 2　Server IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 3　Maximum Retries フィールドに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。

ステップ 4　Timeout フィールドに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。

ステップ 5　Certificate File Path フィールドに、証明書のディレクトリ パスを入力します。

ステップ 6　Certificate File Name フィールドに、証明書の名前を入力します（*webadmincert_name*.pem）。

ステップ 7　（オプション）Certificate Password フィールドに、パスワードを入力して証明書を暗号化します。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 10　コントローラをリブートして変更内容を有効化するには、**Commands** > **Reboot** > **Reboot** > **Save and Reboot** の順にクリックします。

CLI を使用した SSL 証明書のロード

コントローラの CLI を使用して、外部で生成された SSL 証明書をロードする手順は、次のとおりです。

ステップ 1　パスワードを使用して、.PEM エンコード ファイルで HTTPS 証明書を暗号化します。PEM エンコード ファイルは、Web アドミニストレーション証明書ファイル（*webadmincert_name*.pem）と呼ばれます。

ステップ 2　*webadmincert_name*.pem ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 3　現在のダウンロードの設定を表示するには、次のコマンドを入力してプロンプトに **n** と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename.............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

ステップ 4　次のコマンドを使用して、ダウンロード設定を変更します。

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

ステップ 5　オペレーティング システムが Web アドミニストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、次のコマンドを入力します。

transfer download certpassword *private_key_password*

ステップ 6　現在のダウンロードの設定を確認して証明書とキーのダウンロードを開始するには、次のコマンドを入力して、プロンプトに **y** と応答します。

transfer download start

次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

ステップ 7　リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM に保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラをリブートするには、次のコマンドを入力します。

reset system

CLI の使用方法

Cisco UWN Solution のコマンドライン インターフェイス（CLI）は、すべてのコントローラに組み込まれています。CLI では、VT-100 エミュレータを使用して、個々のコントローラおよび各コントローラにアソシエートされた Lightweight アクセス ポイントをローカルまたはリモートで設定、監視、制御することができます。CLI は簡単なテキスト ベースのツリー構造のインターフェイスで、Telnet 対応ターミナル エミュレータを使用して最大 5 名のユーザがコントローラにアクセスできます。

（注）　特定のコマンドの情報は、『Cisco Wireless LAN Controller Command Reference』を参照してください。

（注）　XML 設定の文字列を CLI コマンドに入力する場合は、文字列を引用符で囲む必要があります。

CLI へのログイン

CLI には、次の 2 つのいずれかの方法でアクセスします。

- コントローラ コンソール ポートへの ASCII シリアル直接接続
- 事前設定されたサービス ポートやディストリビューション システム ポートを使用したイーサネット上のリモート コンソール セッション

CLI にログインする前に、使用する接続の種類に基づいて接続および環境変数を設定しておく必要があります。

ローカル シリアル接続の使用方法

シリアル ポートに接続するには以下が必要です。

- DB-9 シリアル ポートを備えており、ターミナル エミュレーション プログラムを実行しているコンピュータ
- DB-9 オス対メスのヌルモデム シリアル ケーブル

シリアル ポートで CLI にログインする手順は、次のとおりです。

ステップ 1　DB-9 ヌルモデム シリアル ケーブルを使用して、コンピュータをコントローラに接続します。

ステップ 2　以下の設定を使用して、ターミナル エミュレータ セッションを開きます。

- 9600 ボー
- データ ビット 8
- ストップ ビット 1

- パリティなし
- ハードウェア フロー制御なし

ステップ 3　プロンプトで CLI にログインします。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

（注）　コントローラのシリアル ポートは、9600 ボー レートおよび短いタイムアウト用に設定されています。これらの値のいずれかを変更するには、**config serial baudrate** *baudrate* コマンドおよび **config serial timeout** *timeout* コマンドを使用します。**config serial timeout 0** と入力すると、シリアル セッションはタイムアウトしなくなります。

リモート イーサネット接続の使用方法

リモートでコントローラに接続するには、以下が必要です。

- イーサネット ネットワーク上でコントローラにアクセスできるコンピュータ
- コントローラの IP アドレス
- Telnet セッション用のターミナル エミュレーション プログラムまたは DOS シェル

（注）　デフォルトでは、コントローラは Telnet セッションをブロックします。Telnet セッションを有効にするには、シリアル ポートへのローカル接続を使用する必要があります。

リモート イーサネット接続で CLI にログインする手順は、次のとおりです。

ステップ 1　ターミナル エミュレータまたは DOS シェル インターフェイスが、次のパラメータを使用して設定されていることを確認します。

- イーサネット アドレス
- ポート 23

ステップ 2　コントローラの IP アドレスを使用して Telnet を CLI に接続します。

ステップ 3　プロンプトで CLI にログインします。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

CLI からのログアウト

CLI での作業が終わったら、ルート レベルに移動して、**logout** と入力します。揮発性 Random-Access Memory（RAM; ランダムアクセス メモリ）への変更を保存するかどうかを確認するプロンプトが表示されます。

CLI のナビゲーション

CLI のナビゲーションは、5 つのレベルに分かれています。

ルート レベル

レベル 2

レベル 3

レベル 4

レベル 5

CLI にログインしたときは、ルート レベルです。ルート レベルでは、正しいコマンド レベルに移動することなくすべてのコマンドを入力できます。表 2-1 は、CLI のナビゲーションを使用し、共通タスクを実行するためのコマンドの一覧です。

表 2-1　CLI のナビゲーションと共通タスクのコマンド

コマンド	操作
help	ルート レベルの場合、システム全体のナビゲーション コマンドが表示されます。
?	現在のレベルで使用できるコマンドが表示されます。
< コマンド > **?**	指定したコマンドのパラメータが表示されます。
exit	1 つ下のレベルに移動します。
Ctrl+Z	ルート レベルに戻ります。
save config	ルート レベルの場合、使用中のアクティブな RAM への変更を、リブート後も維持されるように不揮発性 RAM（NVRAM）に保存します。
reset system	ルート レベルの場合、ログアウトせずにコントローラをリセットします。

Web ブラウザと CLI インターフェイスの無線接続の有効化

無線クライアントを使用してコントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード以外のすべての管理タスクでサポートされています。

無線クライアント デバイスから GUI や CLI を開く前に、接続が許可されるようにコントローラを設定する必要があります。GUI や CLI への無線接続を有効にする手順は、次のとおりです。

ステップ 1　CLI にログインします。

ステップ 2　**config network mgmt-via-wireless enable** と入力します。

ステップ 3　無線クライアントを使用して、コントローラに接続されている Lightweight アクセス ポイントにアソシエートします。

ステップ 4　無線クライアントで、コントローラの Telnet セッションを開くか、コントローラの GUI を参照します。

ヒント　コントローラの GUI を使用して無線接続を有効にするには、**Management** > **Mgmt Via Wireless** ページをクリックして、**Enable Controller Management to be accessible from Wireless Clients** チェックボックスをオンにします。

CHAPTER 3

ポートとインターフェイスの設定

この章では、コントローラの物理ポートとインターフェイスの概要、およびこれらを設定する手順について説明します。この章の内容は、次のとおりです。

ポートとインターフェイスの概要

コントローラと無線ネットワーク ポートの接続方法を理解するカギとなるのは、ポート、インターフェイス、および WLAN の 3 つの概念です。

ポート

ポートは、コントローラ プラットフォーム上に存在し、接続に使用される物理的実体です。コントローラには、ディストリビューション システム ポートと、サービス ポートの 2 種類があります。各コントローラに用意されているポートは以下の図のとおりです。

(注)　Cisco Integrated Services Router のコントローラ、および Cisco WiSM のコントローラには外部物理ポートはありません。これらをネットワークに接続する場合、ルータ上またはスイッチ上のポートを使用します。

図 3-1　Cisco 2100 シリーズ Wireless LAN Controller のポート

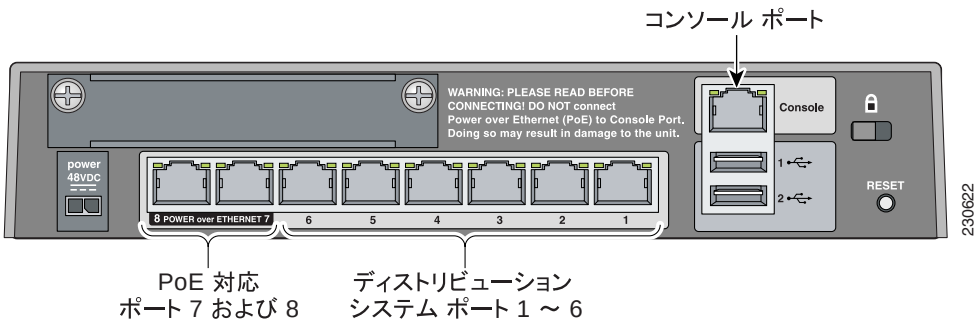
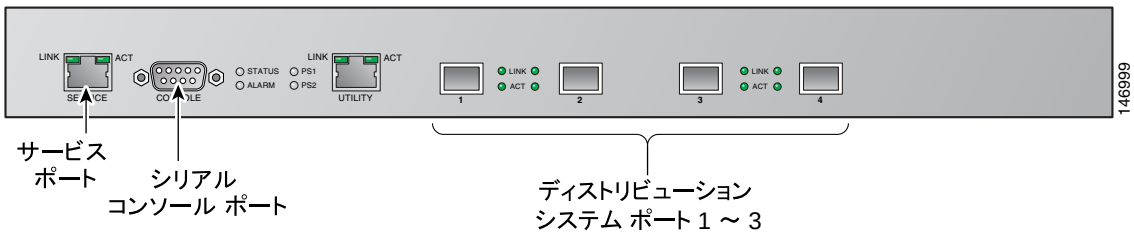


図 3-2　Cisco 4400 シリーズ Wireless LAN Controller のポート



(注)　図 3-2 は Cisco 4404 コントローラです。Cisco 4402 コントローラもこれに類似していますが、ディストリビューション システム ポートの数は 2 つです。図 3-2 でラベルのついていないユーティリティ ポートは、現在動作しません。

図 3-3　Catalyst 3750G 統合型無線 LAN コントローラ スイッチのポート

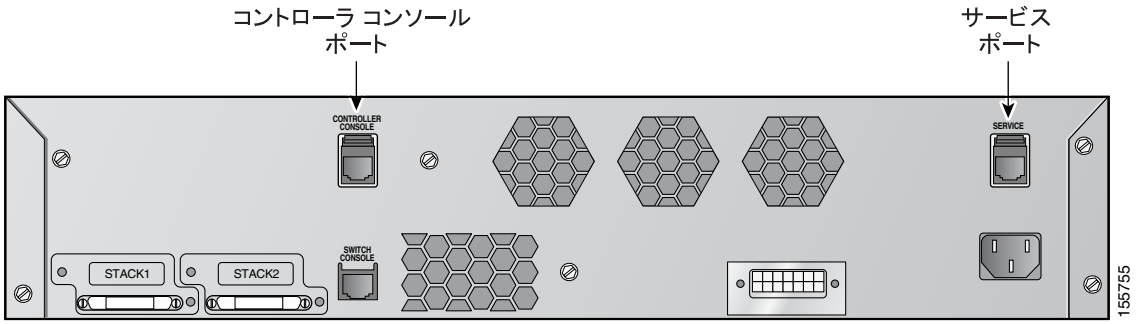


表 3-1 は、1 コントローラあたりのポート数の一覧です。

表 3-1　コントローラ ポート

コントローラ	サービス ポート	ディストリビューション システム イーサネット ポート	シリアル コンソール ポート
2100 シリーズ	なし	8（6 + PoE ポート 2 個）	1
4402	1	2	1
4404	1	4	1
Cisco WiSM	2（ポート 9 および 10）	8（ポート 1 ～ 8）	2
Cisco 28/37/38xx シリーズ サービス統合型ルータに内蔵されたコントローラ ネットワーク モジュール	なし	1	1[1]
Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	1	2（ポート 27 および 28）	1

1. ギガビット イーサネット バージョンのコントローラ ネットワーク モジュールのボー レートは最高 9600bps ですが、ファスト イーサネット バージョンでは 57600bps までサポートされます。

（注） 付録 E には、統合型コントローラの論理接続図および関連するソフトウェア コマンドが記載されています。

ディストリビューション システム ポート

ディストリビューション システム ポートは近接スイッチにコントローラを接続し、これら 2 つのデバイス間のデータ パスとして働きます。

- Cisco 2100 シリーズ コントローラは、8 個の 10/100 銅線イーサネット ディストリビューション システム ポートを持ち、これらのポートを通じて最大 6 個のアクセス ポイントをサポートします。ポート 7 と 8 の 2 つは Power-over-Ethernet（PoE）に対応しており、ポートに接続されたアクセス ポイントに直接電力を供給することができます。

- Cisco 4402 コントローラは、2 つのギガビット イーサネット ディストリビューション システム ポートを持ち、これらはそれぞれ、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。4402-25 モデルおよび 4402-50 モデルでは、合計 25 個または 50 個のアクセス ポイントをコントローラに接続できます。
- Cisco 4404 コントローラは、4 つのギガビット イーサネット ディストリビューション システム ポートを持ち、これらはそれぞれ、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。4404-25 モデル、4404-50 モデル、および 4404-100 モデルでは、合計 25 個、50 個、または 100 個のアクセス ポイントをコントローラに接続できます。

（注） 4402 および 4404 コントローラのギガビット イーサネット ポートは、次の SX/LC/T 小型フォーム ファクタ プラグイン（SFP）モジュールを受け付けます。
- 1000BASE-SX SFP モジュール。LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-LX SFP モジュール。LC 物理コネクタを使用した 1300nM（LX/LH）光ファイバ リンクで 1000Mbps の有線接続をネットワークに提供します。
- 1000BASE-T SFP モジュール。RJ-45 物理コネクタを使用した銅線リンクで 1000Mbps の有線接続をネットワークに提供します。

- Cisco Catalyst 6500 シリーズ スイッチ Wireless Services Module（WiSM; ワイヤレス サービス モジュール）および Cisco 7600 シリーズ ルータ Wireless Services Module（WiSM）には、スイッチまたはルータと統合コントローラを接続する内部ギガビット イーサネット ディストリビューション システム ポートが 8 つあります（ポート 1 ～ 8）。これらの内部ポートは、スイッチまたはルータのバックプレーン上にあり、フロント パネルからは見えません。これらのポートを通じて、最大 300 個のアクセス ポイントをサポートできます。
- Cisco 28/37/38xx シリーズ サービス統合型ルータの内蔵コントローラ ネットワーク モジュールがサポートするアクセス ポイント数は、ネットワーク モジュールのバージョンに応じて最大 6 個、8 個、または 12 個（最大クライアント数はそれぞれ 256、256、350）となります。ネットワーク モジュールは、ルータと統合コントローラを接続するファスト イーサネット ディストリビューション システム ポート（6 アクセス ポイント バージョンの場合）またはギガビット イーサネット ディストリビューション システム ポート（8 アクセス ポイント バージョンまたは 12 アクセス ポイント バージョンの場合）を通じてこれらのアクセス ポイントをサポートします。このポートは、ルータのバックプレーン上にあり、フロント パネルからは見えません。ファスト イーサネット ポートの動作速度は最大 100Mbps、ギガビット イーサネット ポートの動作速度は最大 1Gbps です。
- Catalyst 3750G 統合型無線 LAN コントローラ スイッチには、スイッチと統合コントローラを接続する内部ギガビット イーサネット ディストリビューション システム ポートが 2 つあります（ポート 27 と 28）。これらの内部ポートは、スイッチ バックプレーン上にあり、フロント パネルからは見えません。各ポートでは、最大 48 個のアクセス ポイントを管理できます。ただし、帯域幅の制約により、アクセス ポイントの数は、1 ポートあたり最大 25 個にしておくことをお勧めします。-S25 モデル、および -S50 モデルでは、コントローラの接続に、合計 25 または 50 個のアクセス ポイントが利用できます。

（注） 49 個以上のアクセス ポイントをサポートするように Cisco 4400 シリーズ コントローラを設定するには、「49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定」の項（P. 3-38）を参照してください。

デフォルトでは、各ディストリビューション システム ポートは 802.1Q VLAN トランク ポートです。ポートの VLAN トランク特性は設定できません。

(注)　一部のコントローラは、コントローラのディストリビューション システム ポートすべてを 1 つの 802.3ad ポート チャネルにまとめる Link Aggregation（LAG; リンク集約）をサポートしています。Cisco 4400 シリーズ コントローラは、ソフトウェア リリース 3.2 以降で LAG をサポートし、LAG は Cisco WiSM コントローラ上で自動的に有効になります。詳細は、「リンク集約の有効化」の項（P. 3-33）を参照してください。

サービス ポート

Cisco 4100 および 4400 シリーズ コントローラには、10/100 銅線イーサネット サービス ポートもあります。このサービス ポートは、サービス ポート インターフェイスにより制御され、コントローラのアウトオブバンド管理と、ネットワーク障害時のシステム復旧とメンテナンスのために割り当てられています。また、これは、コントローラがブート モードのときにアクティブな唯一のポートです。このサービス ポートは 802.1Q タグを持つことはできないので、近接スイッチ上のアクセス ポートに接続する必要があります。サービス ポートの使用は任意です。

(注)　このサービス ポートは、Cisco WiSM の 4404 コントローラと Supervisor 720 の間の内部プロトコル通信に使用されます。

(注)　Cisco 2100 シリーズ コントローラ、および Cisco サービス統合型ルータのコントローラには、サービス ポートはありません。

(注)　サービス ポートには自動認識機能が備わっていません。サービス ポートと通信するには、適切なストレートまたはクロス イーサネット ケーブルを使用する必要があります。

インターフェイス

インターフェイスはコントローラ上の論理的実体です。インターフェイスには、IP アドレス、デフォルト ゲートウェイ（IP サブネット用）、プライマリ物理ポート、セカンダリ物理ポート、VLAN 識別子、DHCP サーバなど、複数のパラメータが関連付けられています。

以下の 5 種類のインターフェイスはコントローラで使用できます。これらのうち 4 種類は固定で、セットアップ時に設定されます。

- 管理インターフェイス（固定でセットアップ時に設定。必須）
- AP マネージャ インターフェイス（レイヤ 3 LWAPP を使用する場合。固定でセットアップ時に設定。必須）
- 仮想インターフェイス（固定でセットアップ時に設定。必須）
- サービスポート インターフェイス（固定でセットアップ時に設定。任意）
- 動的インターフェイス（ユーザ定義）

各インターフェイスは少なくとも 1 つのプライマリ ポートにマップされます。一部のインターフェイス（管理および動的）は、オプションのセカンダリ（または、バックアップ）ポートにマップできます。あるインターフェイスのプライマリ ポートに障害が発生すると、このインターフェイスは自動的にバックアップ ポートに移動します。また、複数のインターフェイスを 1 つのコントローラ ポートにマップできます。

(注)　各インターフェイスに対してプライマリ　ポートとセカンダリ　ポートを個別に設定するのではなく、複数のインターフェイスが 1 つのポート チャネルに動的にマップされるようにコントローラを設定する方法については、「リンク集約の有効化」の項（P. 3-33）を参照してください。

管理インターフェイス

管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。管理インターフェイスは、唯一常時「ping 可能」な、コントローラのインバンド インターフェイス IP アドレスを持ちます。コントローラの GUI にアクセスするには、Internet Explorer の Address フィールドに、コントローラの管理インターフェイスの IP アドレスを入力します。

管理インターフェイスは、コントローラと Lightweight アクセス ポイントの間のレイヤ 2 通信にも使用されます。このインターフェイスはディストリビューション システム ポート 1 に割り当てる必要がありますが、必要に応じて、バックアップ ポートにマップしたり、WLAN に割り当てることもできます。これは、AP マネージャ インターフェイスと同じ VLAN または IP サブネットに設定できます。ただし、管理インターフェイスは、次のように、他のディストリビューション システム ポートを通じて通信することも可能です。

- レイヤ 2 ネットワークでメッセージを送信し、すべてのディストリビューション システム ポートを通じて、他のコントローラを自動検出し、通信します。
- レイヤ 2 ネットワーク全体で、Lightweight アクセス ポイント LWAPP ポーリング メッセージを受信し、可能な限り多くの Lightweight アクセス ポイントを自動検出して、アソシエートし、通信を行います。

LWAPP 通信がレイヤ 2（同一サブネット）モードに設定されている場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信と、コントローラとアクセス ポイント間の全通信を制御する管理インターフェイスが 1 つ必要です。LWAPP 通信がレイヤ 3（異なるサブネット）モードに設定されている場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが 1 つと、コントローラとアクセス ポイント間の全通信を制御する AP マネージャ インターフェイスが 1 つ必要です。

(注)　サービス ポートが使用中の場合は、サービス ポート インターフェイスとは異なるスーパーネット上に管理インターフェイスが存在する必要があります。

AP マネージャ インターフェイス

1 つのコントローラに 1 つ以上の AP マネージャ インターフェイスがあります。このインターフェイスは、Lightweight アクセス ポイントがコントローラに接続した後でコントローラとアクセス ポイントの間で行われるすべてのレイヤ 3 通信に使用されます。AP マネージャの IP アドレスは、コントローラからアクセス ポイントへの LWAPP パケットのトンネル発信元、およびアクセス ポイントからコントローラへの LWAPP パケットの宛先として使用されます。

Cisco 4404 および WiSM コントローラの場合は、すべてのディストリビューション システム ポート（1、2、3、および 4）に対して AP マネージャ インターフェイスを設定します。Cisco 4402 コントローラの場合は、ディストリビューション システム ポート 1 および 2 に対して AP マネージャ インターフェイスを設定します。どちらの場合も、静的（または固定）AP マネージャ インターフェイスは必ずディストリビューション システム ポート 1 に割り当てられ、固有の IP アドレスが与えられます。管理インターフェイスと同じ VLAN または IP サブネット上で AP マネージャ インターフェイスを設定すると、アクセス ポイントのアソシエートにおいて最良の結果が得られますが、このような設定は必須ではありません。

（注） LAG が有効化されているときは、AP マネージャ インターフェイスは 1 つだけ存在することができます。LAG が無効の場合は、コントローラの各ポートに対して AP マネージャ インターフェイスを割り当てる必要があります。

（注） 使用可能なディストリビューション システム ポートが 1 つだけの場合は、ディストリビューション システム ポート 1 を使用してください。

AP マネージャ インターフェイスは、どのディストリビューション システム ポートを介して通信するときも、できる限り多くの Lightweight アクセス ポイントのアソシエートおよび通信を行うために、レイヤ 3 ネットワーク全体をリッスンして Lightweight アクセス ポイント（LWAPP）の参加メッセージを検出します。

（注） AP マネージャ インターフェイスに対するポート冗長化はサポートされません。AP マネージャ インターフェイスをバックアップ ポートにマッピングすることはできません。

（注） 複数の AP マネージャ インターフェイスの作成と使用については、「複数の AP マネージャ インターフェイスの使用」の項（P. 3-38）を参照してください。

仮想インターフェイス

仮想インターフェイスは、モビリティ管理、Dynamic Host Configuration Protocol（DHCP）リレー、およびゲスト Web 認証などのレイヤ 3 の組み込みセキュリティをサポートするために使用されます。また、レイヤ 3 Web 認可が有効な場合に証明書のソースを確認するために、レイヤ 3 Security Manager と Mobility Manager で使用される Domain Name System（DNS; ドメイン ネーム システム）ゲートウェイのホスト名も管理します。

具体的には、仮想インターフェイスは主に次の 2 つの役割を果たします。

- その IP アドレスを DHCP サーバから取得する無線クライアントの DHCP サーバ プレースホルダの役割。
- Web Authentication Login ページのリダイレクト アドレスの役割。

（注） Web 認証の詳細は、第 5 章を参照してください。

仮想インターフェイスの IP アドレスは、コントローラと無線クライアントの間の通信でのみ使用されます。ディストリビューション システム ポートから出て、スイッチド ネットワークに入るパケットの発信元アドレスや、宛先アドレスとなることは決してありません。システムを正常に動作させるには、仮想インターフェイスの IP アドレスを設定する必要がありますが（0.0.0.0 は設定できません）、ネットワーク上の他のデバイスは、この仮想インターフェイスと同じアドレスを使用できません。したがって、仮想インターフェイスは、1.1.1.1 など、割り当てられず、使用もされないゲートウェイ IP アドレスを使って設定する必要があります。仮想インターフェイスの IP アドレスは ping できませんし、ネットワーク上のいかなるルーティング テーブルにも存在してはいけません。また、仮想インターフェイスをバックアップ ポートにマップすることもできません。

（注） 同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。設定しなかった場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

サービス ポート インターフェイス

サービス ポート インターフェイスはサービス ポートを介した通信を制御し、サービス ポートに対して静的にマップされます。このインターフェイスは、管理インターフェイス、AP マネージャ インターフェイス、およびその他の動的インターフェイスとは異なるスーパーネット上の IP アドレスを必要とします。また、バックアップ ポートにマップすることはできません。この設定により、コントローラを直接管理したり、10.1.2.x などの専用オペレーティング システム ネットワーク経由で管理したりできるようになり、ネットワーク ダウンタイム時のサービスのアクセスが保証されます。

サービス ポートは DHCP を使用して IP アドレスを取得したり、このポートに固定 IP アドレスを割り当てたりすることはできますが、サービス ポート インターフェイスにデフォルト ゲートウェイを割り当てることはできません。サービス ポートへのリモート ネットワーク アクセスに使用される静的なルートはコントローラを通じて定義できます。

（注） サービス ポート インターフェイスを持つのは Cisco 4400 シリーズのコントローラのみです。

（注） Cisco WiSM コントローラの両方のサービス ポート インターフェイス上に IP アドレスを設定する必要があります。設定しないと、近接スイッチは各コントローラのステータスをチェックできません。

動的インターフェイス

動的インターフェイスは VLAN インターフェイスとも呼ばれ、ユーザによって作成され、無線 LAN クライアントの VLAN に相当する設計になっています。1 つのコントローラで最大 512 個の動的インターフェイス（VLAN）をサポートできます。動的インターフェイスはそれぞれ、個別に設定され、コントローラの任意またはすべてのディストリビューション システム ポートに独立した通信ストリームを設定できます。動的インターフェイスはそれぞれ、コントローラとその他のネットワーク デバイスの間の VLAN などの通信を制御し、このインターフェイスにマップされている WLAN に関連付けられた無線クライアントの DHCP リレーとして働きます。動的インターフェイスは、WLAN、レイヤ 2 管理インターフェイス、およびレイヤ 3 AP マネージャ インターフェイスに割り当てることができます。また、動的インターフェイスをバックアップ ポートにマップすることもできます。

1 つ、または複数の動的インターフェイスをディストリビューション システム ポートに設定できます。また、1 つも設定しなくても問題ありません。ただし、動的インターフェイスはすべて、このポートに設定された他のインターフェイスとは異なる VLAN または IP サブネットに設定する必要があります。ポートにタグが付いていない場合は、動的インターフェイスはすべて、このポートに設定されている他のインターフェイスとは異なる IP サブネットに設定する必要があります。

（注） 動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

WLAN

WLAN は、Service Set Identifier（SSID; サービス セット ID）をインターフェイスにアソシエートします。これは、セキュリティ、Quality of Service（QoS）、無線ポリシーなどその他の無線ネットワーク パラメータを使って設定されます。WLAN は、コントローラ 1 つあたり、最大 16 個のアクセス ポイントを設定できます。

（注） WLAN を設定する手順については、第 6 章を参照してください。

図 3-4 は、ポート、インターフェイス、および WLAN の関係を表しています。

図 3-4　ポート、インターフェイス、および WLAN

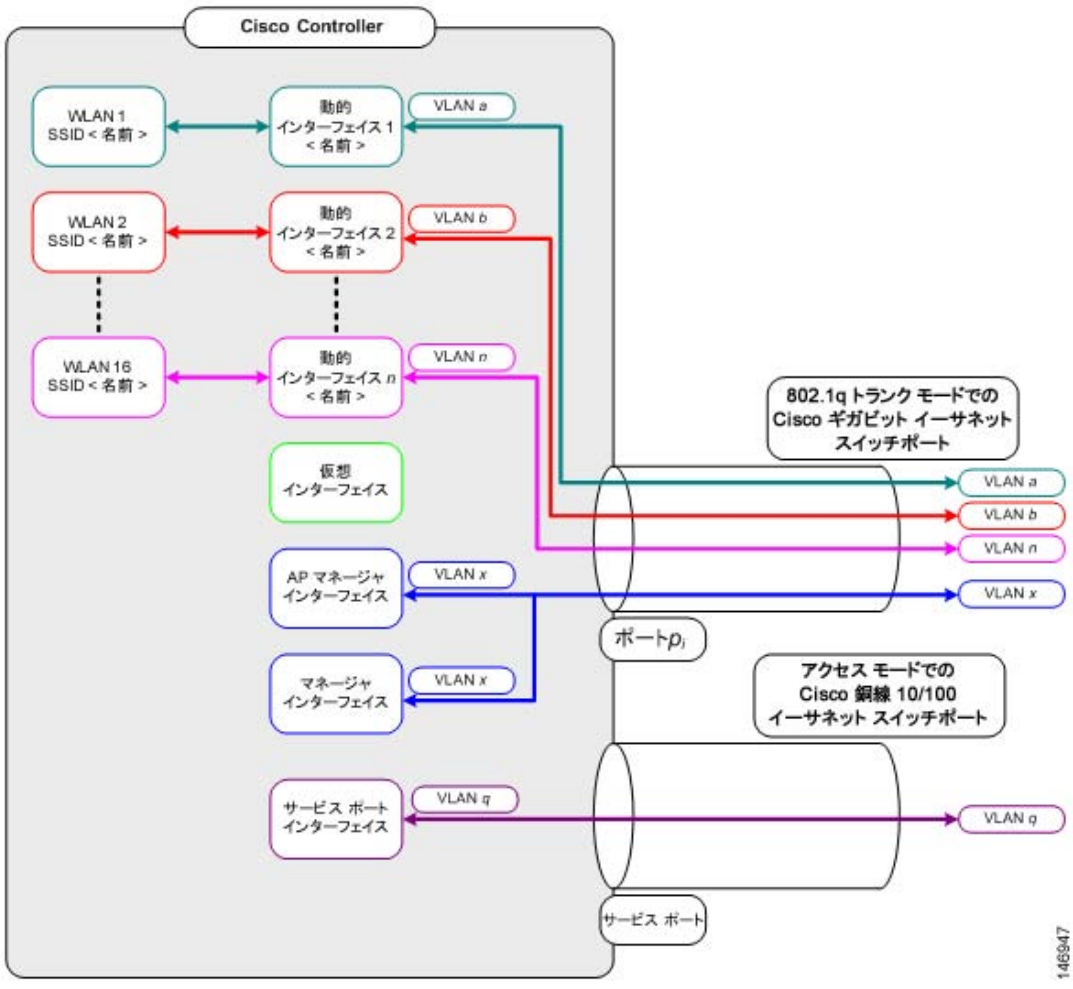


図 3-4 に示すとおり、個々のコントローラ ポート接続は 802.1Q トランクなので、近接スイッチ上ではそのように設定する必要があります。Cisco スイッチでは、802.1Q トランクのネイティブ VLAN にはタグはついていません。したがって、隣接する Cisco スイッチでネイティブ VLAN を使用するためにインターフェイスを設定するには、タグなしになるように、コントローラのインターフェイスを設定する必要があります。

（注） VLAN 識別子の値 0（Controller > Interfaces ページ）は、インターフェイスにタグがつけられていないことを表します。

Cisco スイッチにおいて、デフォルト（タグなし）のネイティブ VLAN は VLAN 1 です。コントローラ インターフェイスがタグ付きとして設定されている（つまり、VLAN 識別子に 0 以外の値が設定されている）場合、ネイティブのタグなし VLAN ではなく、近接スイッチの 802.1Q トランク設定で VLAN を可能にする必要があります。

コントローラでは、タグ付き VLAN のみを使用することをお勧めします。また、近接スイッチからコントローラ ポートへの 802.1Q トランク接続では、関連する VLAN のみを許可するようにしてください。その他の VLAN はすべて無効にするか、スイッチ ポート トランク設定にプルーニングする必要があります。コントローラのパフォーマンスを最適化するには、この慣例は極めて重要です。

（注） コントローラが VLAN トラフィックを正常にルーティングできるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

以下のページに記載された手順に従って、コントローラのインターフェイスやポートを設定してください。

- 管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定（P. 3-11）
- 動的インターフェイスの設定（P. 3-17）
- ポートの設定（P. 3-21）
- リンク集約の有効化（P. 3-33）
- 49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定（P. 3-38）

管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

通常、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを定義するには、スタートアップ ウィザードを使用します。ただし、コントローラが実行されていれば、GUI または CLI のどちらかを介して、インターフェイス パラメータを表示し、設定できます。

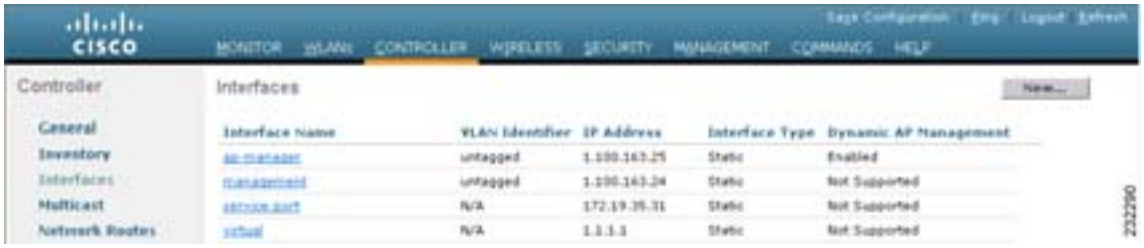
（注） WLAN を DHCP サーバに割り当てるときは、両方が同じサブネット上に存在するようにしてください。同じサブネット上にない場合は、ルータを使用して WLAN と DHCP サーバの間のトラフィックをルーティングする必要があります。

GUI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

GUI を使用して、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1　**Controller** > **Interfaces** の順にクリックして、Interfaces ページを開きます（図 3-5 を参照）。

図 3-5　Interfaces ページ



このページには、現在のコントローラ インターフェイスの設定が表示されます。

ステップ 2　特定のインターフェイスの設定を変更するには、そのインターフェイスの名前をクリックします。このインターフェイスの Interfaces > Edit ページが表示されます。

ステップ 3　各インターフェイス タイプについて、次のパラメータを設定します。

管理インターフェイス

（注） 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューション システムの MAC アドレスが使用されます。

- VLAN 識別子

（注） タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト（ACL）の設定

（注） ACL を作成するには、第 5 章にある手順に従ってください。

AP マネージャ インターフェイス

- VLAN 識別子

（注） タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ

（注） AP マネージャ インターフェイスの IP アドレスは、管理インターフェイスの IP アドレスと異なるものであることが必要です。サブネットは、管理インターフェイスと同じでも同じでなくてもかまいません。ただし、アクセス ポイントのアソシエートにおいて最良の結果を得るには、両方のインターフェイスを同じサブネット上に置くことをお勧めします。

- 物理ポート割り当て
- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト（ACL）の名前

（注） ACL を作成するには、第 5 章にある手順に従ってください。

仮想インターフェイス

- 1.1.1.1 のような、架空、未割り当て、または未使用のゲートウェイ IP アドレス。
- DNS ゲートウェイ ホスト名

（注） 確実に接続と Web 認証が行われるためには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスの DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

サービス ポート インターフェイス

（注）　サービス ポート インターフェイスでは、工場出荷時にコントローラに設定されたサービス ポートの MAC アドレスが使用されます。

- DHCP プロトコル（有効）または
- DHCP プロトコル（無効）および IP アドレスと IP ネットマスク

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 5　仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

CLI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定

この項では、CLI を使用して、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイス パラメータを表示し、設定する手順について説明します。

CLI を使用した、管理インターフェイスの設定

CLI を使用して、管理インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1　**show interface detailed management** と入力し、現在の管理インターフェイスの設定を表示します。

（注）　管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューション システムの MAC アドレスが使用されます。

ステップ 2　ディストリビューション システム通信で管理インターフェイスを使用する WLAN を無効にするには、**config wlan disable** *wlan-number* と入力します。

ステップ 3　次のコマンドを入力し、管理インターフェイスを定義します。

- **config interface address management** *ip-addr ip-netmask gateway*
- **config interface vlan management** {*vlan-id* | **0**}

（注）　タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- **config interface port management** *physical-ds-port-number*
- **config interface dhcp management** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]

- **config interface acl management** *access-control-list-name*

（注） ACL の詳細は、第 5 章を参照してください。

ステップ 4　**save config** と入力して、変更内容を保存します。

ステップ 5　**show interface detailed management** と入力し、変更内容が保存されたかどうか確認します。

CLI を使用した、AP マネージャ インターフェイスの設定

CLI を使用して、AP マネージャ インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1　**show interface summary** と入力し、現在のインターフェイスを表示します。

（注） システムがレイヤ 2 モードで動作している場合は、AP マネージャ インターフェイスは出力に表示されません。

ステップ 2　**show interface detailed ap-manager** と入力し、現在の AP マネージャ インターフェイスの設定を表示します。

ステップ 3　ディストリビューション システム通信で AP マネージャ インターフェイスを使用する WLAN を無効にするには、**config wlan disable** *wlan-number* と入力します。

ステップ 4　次のコマンドを入力し、AP マネージャ インターフェイスを定義します。

- **config interface address ap-manager** *ip-addr ip-netmask gateway*
- **config interface vlan ap-manager** {*vlan-id* | **0**}

（注） タグなし VLAN については **0**、タグ付き VLAN についてはゼロ以外の値を指定します。コントローラでは、タグ付き VLAN のみを使用することをお勧めします。

- **config interface port ap-manager** *physical-ds-port-number*
- **config interface dhcp ap-manager** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- **config interface acl ap-manager** *access-control-list-name*

（注） ACL の詳細は、第 5 章を参照してください。

ステップ 5　**save config** と入力して、変更内容を保存します。

ステップ 6　**show interface detailed ap-manager** と入力し、変更内容が保存されたことを確認します。

CLI を使用した、仮想インターフェイスの設定

CLI を使用して、仮想インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1　**show interface detailed virtual** と入力し、現在の仮想インターフェイスの設定を表示します。

ステップ 2　ディストリビューション システム通信で仮想インターフェイスを使用する WLAN を無効にするには、**config wlan disable** *wlan-number* と入力します。

ステップ 3　次のコマンドを入力し、仮想インターフェイスを定義します。

- **config interface address virtual** *ip-address*

（注）　*ip-address* には、1.1.1.1 など、架空で、割り当てられていない、未使用のゲートウェイ IP アドレスを入力します。

- **config interface hostname virtual** *dns-host-name*

ステップ 4　**reset system** と入力します。NVRAM に設定変更を保存するには、確認のプロンプトで **Y** と入力します。コントローラがリブートします。

ステップ 5　**show interface detailed virtual** と入力し、変更内容が保存されたかどうか確認します。

CLI を使用した、サービス ポート インターフェイスの設定

CLI を使用して、サービス ポート インターフェイス パラメータを表示し、設定する手順は、次のとおりです。

ステップ 1　**show interface detailed service-port** と入力し、現在のサービス ポート インターフェイスの設定を表示します。

（注）　サービス ポート インターフェイスでは、工場出荷時にコントローラに設定されたサービス ポートの MAC アドレスが使用されます。

ステップ 2　次のコマンドを入力し、サービス ポート インターフェイスを定義します。

- DHCP サーバを設定する場合：**config interface dhcp service-port** *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]
- DHCP サーバを無効にする場合：**config interface dhcp service-port none**

- IP アドレスを設定する場合：**config interface address service-port** *ip-addr ip-netmask gateway*

ステップ 3　このサービス ポートは、コントローラの帯域外管理に使用されます。管理ワークステーションがリモート サブネットにある場合、このリモート ワークステーションからコントローラを管理するには、コントローラにルートを追加する必要があります。そのためには、次のコマンドを入力します。

config route *network-ip-addr ip-netmask gateway*

ステップ 4　**save config** と入力して、変更内容を保存します。

ステップ 5　**show interface detailed service-port** と入力し、変更内容が保存されたことを確認します。

動的インターフェイスの設定

この項では、GUI または CLI を使用して動的インターフェイスを設定する手順について説明します。

GUI を使用した動的インターフェイスの設定

GUI を使用して、動的インターフェイスの新規作成や編集を行う手順は、次のとおりです。

ステップ 1　**Controller** > **Interfaces** の順にクリックして、Interfaces ページを開きます（図 3-5 を参照）。

ステップ 2　次のいずれかの操作を行います。

- 新たに動的インターフェイスを作成するには、**New** をクリックします。Interfaces > New ページが表示されます（図 3-6 を参照）。ステップ 3 に進みます。
- 既存の動的インターフェイスの設定を変更するには、インターフェイスの名前をクリックします。そのインターフェイスの Interfaces > Edit ページが表示されます（図 3-7 を参照）。ステップ 5 に進みます。
- 既存の動的インターフェイスを削除するには、そのインターフェイスの青いドロップダウン矢印にカーソルを置いて **Remove** を選択します。

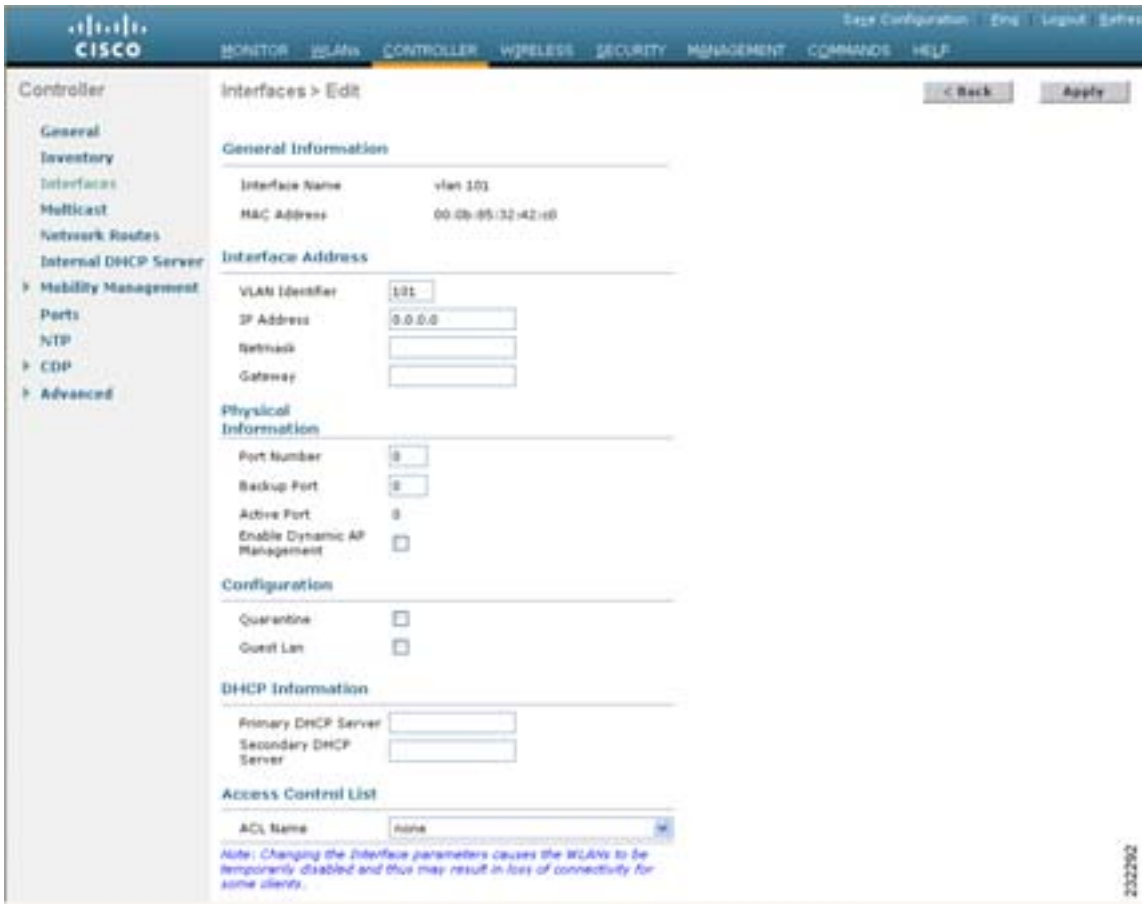
図 3-6　Interfaces > New ページ

ステップ 3　図 3-6 のようにインターフェイス名と VLAN 識別子を入力します。

（注）　VLAN 識別子に対して 0 以外の値を入力します。動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

ステップ 4　**Apply** をクリックして、変更を適用します。Interfaces > New ページが表示されます（図 3-7 を参照）。

図 3-7　Interfaces > Edit ページ



ステップ 5　以下のパラメータを設定します。

- VLAN 識別子
- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- 物理ポート割り当て
- 検疫

（注） **Quarantine** チェックボックスは、この VLAN を正常に動作していない VLAN として設定する場合にオンにします。そうすることにより、WLAN がローカル スイッチングに設定されている場合でも、この VLAN に割り当てられた任意のクライアントのデータ トラフィックがコントローラを経由するようにします。このコマンドを使用するのは一般に、クライアントがアソシエートされるアクセス ポイントが hybrid-REAP アクセス ポイントであり、ネットワーク アクセス コントロール（NAC）を行うようにアクセス ポイントのコントローラが設定されている場合です。hybrid REAP の詳細は、第 12 章を参照してください。

- プライマリ DHCP サーバとセカンダリ DHCP サーバ
- 必要に応じて、アクセス コントロール リスト（ACL）の名前

（注） ACL の詳細は、第 5 章を参照してください。

（注） 適切な動作を保証するには、Port Number パラメータと Primary DHCP Server パラメータを設定する必要があります。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 7　作成または編集する動的インターフェイスそれぞれについて、この手順を繰り返します。

CLI を使用した動的インターフェイスの設定

CLI を使用して動的インターフェイスを設定する手順は、次のとおりです。

ステップ 1　**show interface summary** と入力し、現在の動的インターフェイスを表示します。

ステップ 2　特定の動的インターフェイスの詳細を表示するには、**show interface detailed** *operator_defined_interface_name* と入力します。

ステップ 3　ディストリビューション システム通信に動的インターフェイスを使用する WLAN を無効にするには、**config wlan disable** *wlan_id* と入力します。

ステップ 4　次のコマンドを入力し、動的インターフェイスを設定します。

- **config interface create** *operator_defined_interface_name* {*vlan_id* | ***x***}

（注） VLAN 識別子に対して 0 以外の値を入力します。動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

- **config interface address** *operator_defined_interface_name ip_addr ip_netmask* [*gateway*]
- **config interface vlan** *operator_defined_interface_name* {*vlan_id* | **0**}
- **config interface port** *operator_defined_interface_name physical_ds_port_number*
- **config interface dhcp** *operator_defined_interface_name ip_address_of_primary_dhcp_server* [*ip_address_of_secondary_dhcp_server*]
- **config interface** *operator_defined_interface_name* **quarantine enable**

（注） この VLAN を正常に動作していない VLAN として設定する場合には、このコマンドを使用します。そうすることにより、WLAN がローカル スイッチングに設定されている場合でも、この VLAN に割り当てられた任意のクライアントのデータ トラフィックがコントローラを経由するようにします。このコマンドを使用するのは一般に、クライアントがアソシエートされるアクセス ポイントが hybrid-REAP アクセス ポイントであり、ネットワーク アクセス コントロール（NAC）を行うようにアクセス ポイントのコントローラが設定されている場合です。hybrid REAP の詳細は、第 12 章を参照してください。

- **config interface acl** *operator_defined_interface_name access_control_list_name*

（注） ACL の詳細は、第 5 章を参照してください。

ステップ 5　ディストリビューション システム通信に動的インターフェイスを使用する WLAN を再度有効にするには、**config wlan enable** *wlan_id* と入力します。

ステップ 6　**save config** と入力して、変更内容を保存します。

ステップ 7　**show interface detailed** *operator_defined_interface_name* および **show interface summary** と入力し、変更内容が保存されたかどうか確認します。

（注） 動的インターフェイスを削除するには、**config interface delete** *operator_defined_interface_name* と入力します。

ポートの設定

コントローラのポートは、工場出荷時にあらかじめデフォルト設定が行われていて、追加設定しなくても動作する設計になっています。しかし、必要に応じて、コントローラのポートのステータスを表示し、設定パラメータを編集できます。

GUI を使用してコントローラのポートのステータスを表示し、必要に応じて設定を変更する手順は、次のとおりです。

ステップ 1　**Controller** > **Ports** をクリックして、Ports ページを開きます（図 3-8 を参照）。

図 3-8　Ports ページ

このページには、コントローラのポート別に現在の設定が表示されます。

ステップ 2　特定のポートの設定を変更するには、そのポートの番号をクリックします。Port > Configure ページが表示されます（図 3-9 を参照）。

（注）　管理インターフェイスと AP マネージャ インターフェイスが同じポートにマッピングされており、同じ VLAN のメンバである場合は、これらのインターフェイスのポート マッピングを変更する前に WLAN を無効にする必要があります。管理インターフェイスと AP マネージャ インターフェイスがそれぞれ別の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

（注）　Port > Configure ページで使用できるパラメータの数は、使用しているコントローラの種類によって異なります。たとえば、図 3-9 は Cisco 4400 シリーズのコントローラの例ですが、Cisco 2100 シリーズ コントローラや Cisco サービス統合型ルータのコントローラで設定可能なパラメータはこれよりも少なくなっています。

図 3-9　Ports > Configure ページ

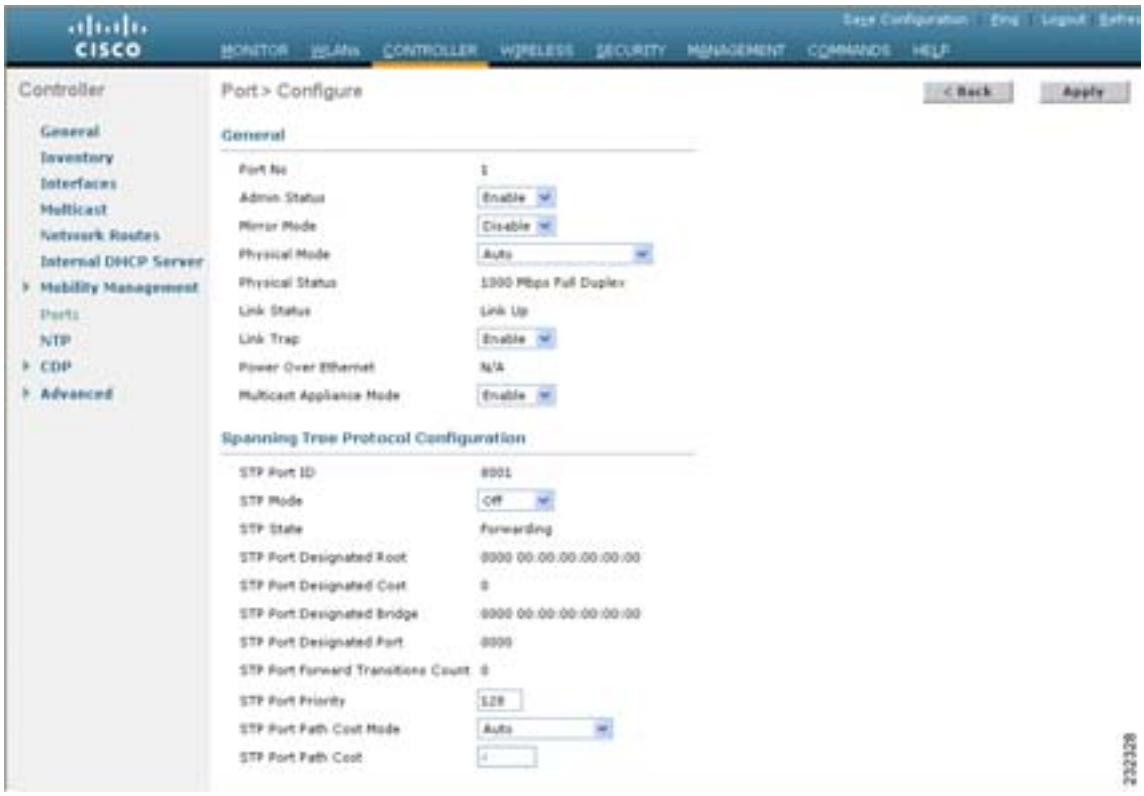


表 3-2 は、現在のポートのステータスを示しています。

表 3-2　ポートのステータス

パラメータ	説明	
Port Number	現在のポートの番号。	
Physical Status	このポートにより使用されているデータ レート。使用可能なデータ レートは、コントローラの種類によって異なります。	
	コントローラ	**使用可能なデータ レート**
	4400 シリーズ	1000 Mbps 全二重
	2100 シリーズ	10 または 100 Mbps、半または全二重
	WiSM	1000 Mbps 全二重
	コントローラ ネットワーク モジュール	100 Mbps 全二重
	Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	1000 Mbps 全二重
Link Status	ポートのリンク ステータス。 **値：**　Link Up、または Link Down	

表 3-2　ポートのステータス（続き）

パラメータ	説明
Power Over Ethernet（PoE）	接続デバイスにイーサネット ケーブル経由で電力を受け取る機能があるかどうかを判断し、受け取ることができる場合は、-48VDC を供給します。 **値：** Enable または Disable **（注）** 古い Cisco アクセス ポイントの中には、コントローラ ポートで有効になっていても、PoE を受け付けないものがあります。このような場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。 **（注）** Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラでは、すべてのポートで PoE がサポートされます。

ステップ 3　表 3-3 は、ポートで設定可能なパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-3　ポート パラメータ

パラメータ	説明
Admin Status	ポートを経由するトラフィックのフローを有効、または無効にします。 **オプション：**Enable または Disable **デフォルト：**Enable **（注）** 管理者がコントローラのポートを無効にしても、ポートのリンク ステータスには影響しません。リンクがダウン状態になるのは、他のシスコ製デバイスによってのみです。ただし、他のシスコ製品では、管理者がポートを無効にするとリンクがダウンします。
Physical Mode	ポートのデータ レートが自動的に設定されるか、ユーザによって指定されるかを表します。サポートされているデータ レートは、コントローラの種類によって異なります。 **デフォルト：**Auto

コントローラ	サポートされているデータ レート
4400 シリーズ	自動、または 1000 Mbps 全二重
2100 シリーズ	自動、または 10 または 100 Mbps、半または全二重
WiSM	自動、または 1000 Mbps 全二重
コントローラ ネットワーク モジュール	自動、または 100 Mbps 全二重
Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	自動、または 1000 Mbps 全二重

表 3-3　ポート パラメータ （続き）

パラメータ	説明
Link Trap	ポートのリンク ステータスが変化したときにポートからトラップが送信されるようにします。 **オプション**：Enable または Disable **デフォルト**：Enable
Multicast Appliance Mode	このポートでマルチキャスト アプライアンス サービスを有効、または無効にします。 **オプション**：Enable または Disable **デフォルト**：Enable

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 6　Ports ページに戻り、変更内容を確認するには、**Back** をクリックします。

ステップ 7　設定するポートそれぞれについて、この手順を繰り返します。

ステップ 8　次の拡張機能を使用できるようにコントローラのポートを設定する必要がある場合は、指定された項を参照してください。

- ポートのミラーリング。次の項を参照してください。
- Spanning Tree Protocol（STP; スパニング ツリー プロトコル）、（P. 3-25）

ポートのミラーリングの設定

ミラー モードでは、特定のクライアント デバイスまたはアクセス ポイントが起点または終点であるトラフィックをすべて別のポートに複製することができます。このモードは、ネットワークで発生している特定の問題を診断するには便利です。このポートは接続にいっさい応答しなくなりますので、ミラー モードは使用されていないポートでのみ有効にしてください。

（注）　WiSM コントローラは、ミラー モードをサポートしません。また、コントローラのサービス ポートをミラーリングされたポートとして使用することもできません。

（注）　コントローラでリンク集約（LAG）が有効になっている場合、ポートのミラーリングはサポートされません。

（注）　ネットワークに問題が発生することがあるので、あるコントローラ　ポートから別のコントローラ ポートへのトラフィックのミラーリングはしないでください。

ポートのミラーリングを有効にする手順は、次のとおりです。

ステップ 1　**Controller** > **Ports** の順にクリックして、Ports ページを開きます（図 3-8 を参照）。

ステップ 2　ミラー モードを有効にする未使用ポートの番号をクリックします。Port > Configure ページが表示されます（図 3-9 を参照）。

ステップ 3　Mirror Mode パラメータを **Enable** に設定します。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　次のいずれかの操作を行います。

- コントローラで選択したポートにトラフィックをミラーリングするクライアント　デバイスを選択する手順は、次のとおりです。
  a. **Wireless** > **Clients** の順にクリックして、Clients ページを開きます。
  b. ミラー モードを有効にするクライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます。
  c. Client Details で、Mirror Mode パラメータを **Enable** に設定します。
- コントローラで選択したポートにトラフィックをミラーリングするアクセス　ポイントを選択する手順は、次のとおりです。
  a. **Wireless** > **All APs** の順にクリックして、All APs ページを開きます。
  b. ミラー　モードを有効にするアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます。
  c. General で、Mirror Mode パラメータを **Enable** に設定します。

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

スパニング ツリー プロトコルの設定

スパニング ツリー プロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正しく動作するには、任意の 2 つのネットワーク デバイス間に存在するアクティブ パスの数は 1 つのみです。STP は、ネットワーク デバイス間のアクティブ パスを一度に 1 つのみ許可しますが、最初のリンクが機能しなくなった場合のバックアップとして冗長リンクを確立します。

スパニング ツリー アルゴリズムによって、レイヤ 2 ネットワークにおける、ループのない最善のパスが計算されます。コントローラやスイッチなどのインフラストラクチャ デバイスは、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）と呼ばれるスパニング ツリー フレームを一定の間隔で送受信します。これらのデバイスは、こうしたフレームを転送せず、ループフリー パスの構築に使用します。

エンド ステーション間に複数のアクティブ パスが存在すると、ネットワーク内でループが発生します。ネットワークにループが存在する場合、エンド ステーションは重複してメッセージを受信する場合があります。また、インフラストラクチャ デバイスが複数のレイヤ 2 インターフェイスにある複数のエンド ステーション MAC アドレスを認識することがあります。これらの条件が重なった結果、ネットワークが不安定になります。

STP は、ルート ブリッジと、レイヤ 2 ネットワークのルートから、すべてのインフラストラクチャ デバイスに向かうループ フリー パスを使用してツリーを定義します。

（注） STP の説明では、*ルート* という用語を、次の 2 つの概念を表す用語として使用しています。1 つは、ネットワーク上でスパニング ツリーの中心点の役割を果たすコントローラで、*ルート ブリッジ*と呼ばれます。もう 1 つは、各コントローラ上にあり、ルート ブリッジに最も効率的なパスを提供するポートで、*ルート ポート*と呼ばれます。スパニング ツリーのルート ブリッジは、*スパニング ツリー ルート*と呼ばれます。

STP によって、冗長データ パスは強制的にスタンバイ（ブロックされた）状態になります。スパニング ツリーのネットワーク セグメントに不具合が発生したときに冗長パスが存在すれば、スパニング ツリー アルゴリズムにより、スパニング ツリー トポロジが再計算され、スタンバイ パスがアクティブ化されます。

コントローラの 2 つのポートがループの一部である場合に、どちらのポートが Forwarding 状態になり、どちらのポートが Blocking 状態になるかは、スパニング ツリー ポートの優先順位とパス コストの設定によって決まります。ポートの優先順位の値は、ネットワーク トポロジ内でのポートの位置と、このポートがどの程度、トラフィックを渡しやすい場所にあるかを表します。パス コストの値は、メディア速度を表します。

コントローラで設定されているアクティブ VLAN ごとに、別のスパニング ツリー インスタンスが保持されます。ブリッジの優先順位とコントローラの MAC アドレスから構成されるブリッジ ID が、各インスタンスに関連付けられます。個々の VLAN については、最も小さなコントローラ ID を持つコントローラが、その VLAN のスパニング ツリー ルートになります。

デフォルトでは、コントローラのディストリビューション システム ポートに対する STP は無効になります。これ以降の項では、GUI、または CLI を使用して、コントローラの STP を設定する手順について説明します。

（注） Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに対する STP は設定できません。

GUI を使用したスパニング ツリー プロトコルの設定

GUI を使用して STP を設定する手順は、次のとおりです。

ステップ 1　**Controller** > **Ports** の順にクリックして、Ports ページを開きます（図 3-8 を参照）。

ステップ 2　STP を設定するポートの番号をクリックします。Port > Configure ページが表示されます（図 3-9 を参照）。このページには、ポートの STP ステータスが表示されます。ここから、STP パラメータを設定できます。

表 3-4 は、現在のポートの STP ステータスを示しています。

表 3-4　ポートのスパニング ツリーのステータス

パラメータ	説明
STP Port ID	STP が有効、または無効になっているポートの番号。
STP State	ポートの現在の STP 状態。これにより、フレームを受信したときのポートのアクションが決まります。 **値：** Disabled、Blocking、Listening、Learning、Forwarding、および Broken
	STP State / **説明**
	Disabled / ポートがシャットダウンされている、リンクがダウンしている、またはこのポートでは STP が有効になっていないため、このポートはスパニング ツリーに参加していません。
	Blocking / このポートはフレーム転送に参加していません。
	Listening / ポートはフレーム転送に参加すべきであると STP が判断したときに、Blocking 状態後に来る最初の変遷状態です。
	Learning / このポートはフレーム転送に参加する準備をしています。
	Forwarding / ポートはフレームを転送します。
	Broken / ポートは正常に機能していません。
STP Port Designated Root	設定 BPDU 内のルート ブリッジを表す一意の ID。
STP Port Designated Cost	指定されたポートのパス コスト。
STP Port Designated Bridge	このポートに対して指定されたブリッジであるとポートがみなしているブリッジの ID。
STP Port Designated Port	このポートに対して指定されたブリッジのポート ID。
STP Port Forward Transitions Count	ポートが Learning 状態から Forwarding 状態に遷移した回数。

ステップ 3　表 3-5 は、ポートで設定可能な STP のパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-5　ポートのスパニング ツリーのパラメータ

パラメータ	説明
STP Mode	このポートに関連付けられている STP 管理モード。 **オプション：**Off、802.1D、または Fast **デフォルト：**Off
	STP Mode / **説明**
	Off / このポートでは STP を無効にします。
	802.1D / このポートがスパニング ツリーに参加できるようにし、リンク状態が Down から Up に変化したときに、すべてのスパニング ツリー状態を確認します。
	Fast / このポートがスパニング ツリーに参加できるようにし、STP モードが 802.1D に設定されているときよりも早くリンク状態が Down から Up に遷移したときに、このポートを Forwarding 状態にします。 **（注）** この状態では、リンクのアップ時に、転送遅延タイマーは無視されます。
STP Port Priority	ネットワーク トポロジ内でのポートの位置と、このポートがどの程度、トラフィックを渡しやすい場所にあるかを表します。 **範囲：** 0 ～ 255 **デフォルト：**128
STP Port Path Cost Mode	STP ポート パス コストは自動的に設定されるか、ユーザにより指定されるかを表します。User Configured を選択する場合、STP Port Path Cost パラメータの値も設定する必要があります。 **範囲：** Auto、または User Configured **デフォルト：**Auto
STP Port Path Cost	トラフィックがポートを通り抜ける速度。このパラメータは、STP Port Path Cost Mode パラメータを User Configured に設定した場合には、必ず設定します。 **オプション：**0 ～ 65535 **デフォルト：**0。リンクがアップしたときに、ポートの速度に合わせてコストが調整されるようになります。 **（注）** 通常、10Mbps のポートには 100 を、100Mbps のポートには 19 を使用します。

ステップ 4　**Apply** をクリックして、変更を適用します。

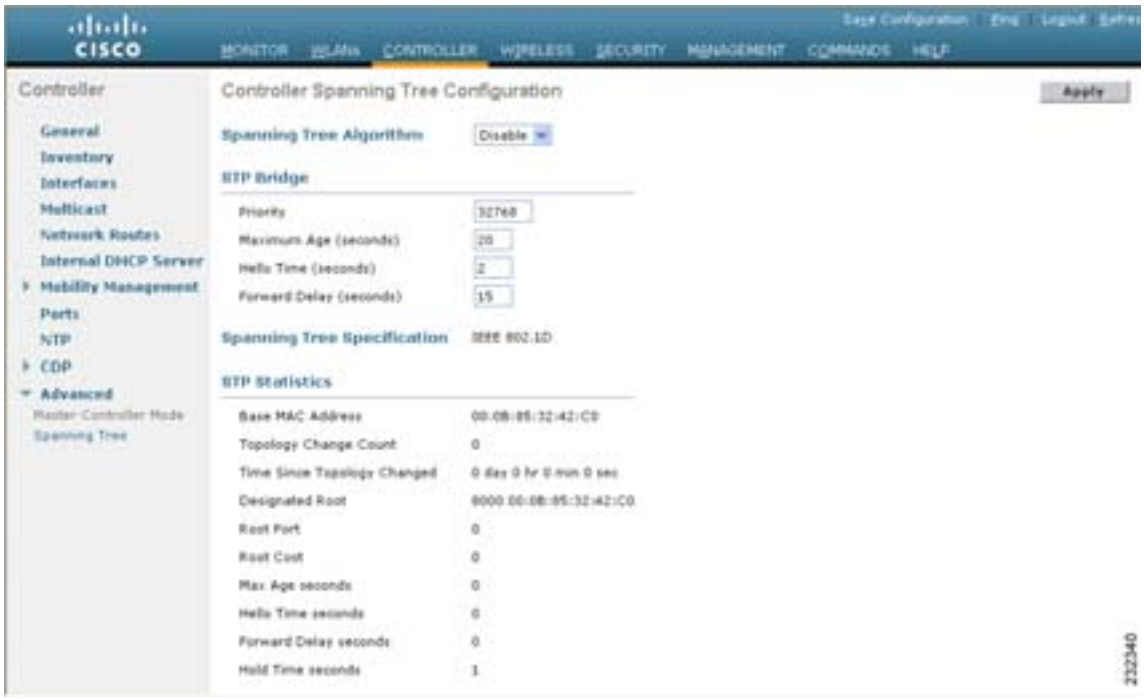
ステップ 5　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 6　Ports ページに戻るには、**Back** をクリックします。

ステップ 7　STP を有効にするポートそれぞれについて、ステップ 2 ～ステップ 6 を繰り返します。

ステップ 8　**Controller** > **Advanced** > **Spanning Tree** の順にクリックして、Controller Spanning Tree Configuration ページを開きます（図 3-10 を参照）。

図 3-10　Controller Spanning Tree Configuration ページ



このページでは、コントローラのスパニング ツリー アルゴリズムの有効化または無効化、その特性の変更、および STP ステータスの表示を行うことができます。表 3-6 は、現在のコントローラの STP ステータスを示しています。

表 3-6　コントローラのスパニング ツリーのステータス

パラメータ	説明
Spanning Tree Specification	このコントローラにより使用されている STP のバージョン。現在、IEEE 802.1D 実装のみ使用可能です。
Base MAC Address	ブリッジを一意に参照する必要がある場合に、このブリッジにより使用される MAC アドレス。このアドレスと dot1dStpPriority を連結することにより、STP で使用される一意のブリッジ識別子が作成されます。
Topology Change Count	管理実体が最後にリセット、または初期化されてから、このブリッジによって検知されたトポロジに対する変更の総数。
Time Since Topology Changed	ブリッジによりトポロジーの変更が検知されてから経過した時間（単位は日、時、分、秒）。
Designated Root	スパニング ツリー ルートのブリッジ識別子。この値は、このノードを起点とする設定 BPDU すべての Root Identifier パラメータとして使用されます。
Root Port	このブリッジからルート ブリッジへの最も低いコスト パスを提供するポートの番号。
Root Cost	このブリッジから見た、ルートへのパスのコスト。

表 3-6　コントローラのスパニング ツリーのステータス （続き）

パラメータ	説明
Max Age (seconds)	任意のポートについて、ネットワークから得られた STP 情報が破棄されるまでの最大経過時間。
Hello Time (seconds)	任意のポートについて、ノードがスパニング ツリーのルートである、またはルートになろうとしているときに、このノードによって行われる設定 BPDU の転送の間隔。これは、このブリッジが現在、実際に使用している値です。
Forward Delay (seconds)	この値は、ポートがスパニング ツリー状態を Forwarding 状態に向かって変化させる速度をコントロールします。この値により、ポートが Forwarding 状態の前に、どのくらい Listening 状態や Learning 状態であるかが決定されます。また、検知されたトポロジの変化が進行中であるときに、フォワーディング データベースの動的エントリすべての時間を経過させるためにも使用されます。 **（注）** これはこのブリッジによって現在、実際に使用されている値です。対照的に、*Stp Bridge Forward Delay* は、このブリッジがルートとなったときに、これを含むその他すべてのブリッジが使用を開始する値です。
Hold Time (seconds)	指定された LAN ポートを通じて行われる設定 BPDU の転送間隔の最小値。 **（注）** Hold Time 期間に転送される設定 BPDU の数は多くても 1 つです。

ステップ 9　表 3-7 は、コントローラで設定可能な STP のパラメータとその説明をまとめたものです。表の指示に従って、必要な変更を行います。

表 3-7　コントローラのスパニング ツリーのパラメータ

パラメータ	説明
Spanning Tree Algorithm	コントローラに対して STP を有効、または無効にします。 **オプション：**Enable または Disable **デフォルト：**Disable
Priority	ネットワーク トポロジ内でのコントローラの位置と、このコントローラがどの程度、トラフィックを渡しやすい場所にあるかを表します。 **範囲：**　0 ～ 65535 **デフォルト：**32768
Maximum Age (seconds)	コントローラが、ポートで受信したプロトコル情報を保管する期間。 **範囲：**　6 ～ 40 秒 **デフォルト：**20 秒

表 3-7　コントローラのスパニング ツリーのパラメータ （続き）

パラメータ	説明
Hello Time (seconds)	コントローラが他のコントローラに Hello メッセージをブロードキャストする期間。 **オプション**：1 ～ 10 秒 **デフォルト**： 2 秒
Forward Delay (seconds)	ポートがフォワーディングを開始する前に、Listening 状態、および Learning 状態でいる期間。 **オプション**：4 ～ 30 秒 **デフォルト**：15 秒

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更を保存します。

CLI を使用したスパニング ツリー プロトコルの設定

CLI を使用して STP を設定する手順は、次のとおりです。

ステップ 1　**show spanningtree port** および **show spanningtree switch** と入力し、現在の STP ステータスを表示します。

ステップ 2　STP が有効な場合は、STP 設定を変更する前に無効にしておく必要があります。**config spanningtree switch mode disable** と入力し、すべてのポートの STP を無効にします。

ステップ 3　次のコマンドのいずれか 1 つを使用して、STP ポートの管理モードを設定します。

- **config spanningtree port mode 802.1d** {*port-number* | **all**}
- **config spanningtree port mode fast** {*port-number* | **all**}
- **config spanningtree port mode off** {*port-number* | **all**}

ステップ 4　次のコマンドのいずれか 1 つを入力し、STP ポートの STP ポート パス コストを設定します。

- **config spanningtree port pathcost** *1-65535* {*port-number* | **all**}：ポートのパス コストを 1 ～ 65535 の範囲で指定します。
- **config spanningtree port mode pathcost auto** {*port-number* | **all**}：STP アルゴリズムによるパス コストの自動割り当てを有効にします。これはデフォルト設定です。

ステップ 5　**config spanningtree port priority** *0-255 port-number* と入力し、STP ポートの優先順位を設定します。デフォルトの優先順位は 128 です。

ステップ 6　必要であれば、**config spanningtree switch bridgepriority** *0-65535* と入力して、コントローラの STP ブリッジ優先順位を設定します。デフォルトのブリッジ優先順位は 32768 です。

ステップ 7　必要であれば、**config spanningtree switch forwarddelay** *4-30* と入力して、コントローラの STP 転送遅延時間（秒）を設定します。デフォルトの転送遅延時間は 15 秒です。

ステップ 8　必要であれば、**config spanningtree switch hellotime** *1-10* と入力して、コントローラの STP ハロー タイム（秒）を設定します。デフォルトのハロー タイムは 2 秒です。

ステップ 9　必要であれば、**config spanningtree switch maxage** *6-40* と入力して、コントローラの STP 最大経過時間を設定します。デフォルトの最大経過時間は 20 秒です。

ステップ 10　ポートの STP 設定を完了したら、**config spanningtree switch mode enable** と入力して、コントローラの STP を有効にします。コントローラによって自動的に論理ネットワーク ループが検出され、冗長ポートが待機状態に設定され、最も効率的なパスウェイでネットワークが構築されます。

ステップ 11　**save config** と入力して、設定を保存します。

ステップ 12　**show spanningtree port** および **show spanningtree switch** と入力し、変更内容が保存されたことを確認します。

リンク集約の有効化

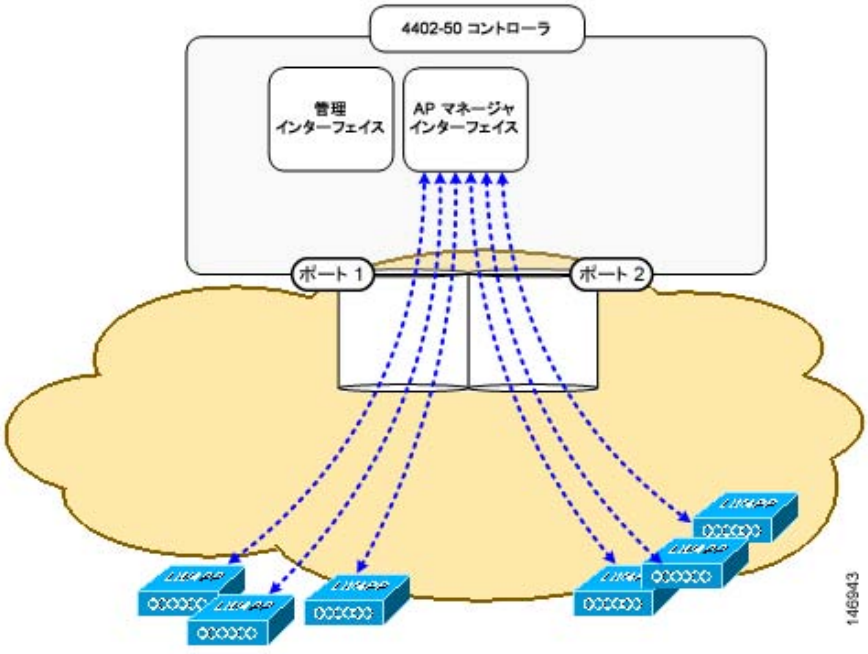
リンク集約（LAG）は、802.3ad ポート集約標準の部分的な実装です。LAG によって、コントローラのすべてのディストリビューション システム ポートが 1 つの 802.3ad ポート チャネルにまとめられるので、コントローラのポートの設定に必要な IP アドレスの数を減らすことができます。LAG が有効である場合、ポートの冗長性は動的に管理され、アクセス ポイントはユーザからは透過的にロード バランシングされます。

Cisco 4400 シリーズ コントローラは、ソフトウェア リリース 3.2 以降で LAG をサポートし、LAG は、Cisco WiSM および Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラ上で自動的に有効になります。LAG を使用していない場合、コントローラ上のディストリビューション システム ポート 1 つにつき、最大 48 個のアクセス ポイントがサポートされます。LAG が有効である場合、4402 コントローラの論理ポートは最大 50 個、4404 コントローラの論理ポートは最大 100 個、各 Cisco WiSM コントローラの論理ポートは最大 150 個のアクセス ポイントをサポートします。

（注） 4404 コントローラの 4 つのポート（または 4402 コントローラの 2 つのポート）をすべて 1 つのリンクにまとめることができます。

図 3-11 は LAG を図示したものです。

図 3-11　リンク集約



LAG を使用すれば、インターフェイスごとにプライマリ ポートとセカンダリ ポートを設定する必要がないので、コントローラ設定も簡単に行えるようになります。いずれかのコントローラ ポートに障害が発生した場合は、他のポートへトラフィックが自動的に移行します。少なくとも 1 つのコントローラ ポートが機能している限り、システムは継続して動作し、アクセス ポイントはネットワークに接続されたままとなります。また、無線クライアントは引き続きデータを送受信します。

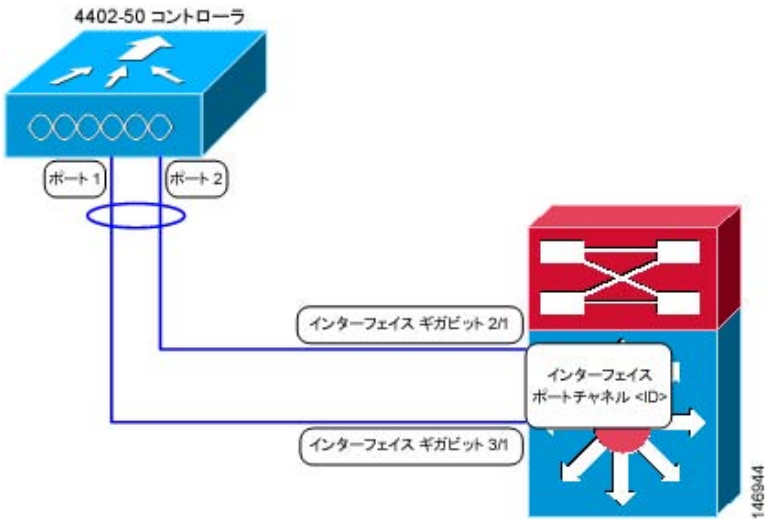
コントローラのポートをまとめるように設定するときに、Catalyst 6500 などのモジュラ スイッチ内の 2 つのモジュールを終端とすることを検討してください。ただし、4400 コントローラの LAG ポートを複数の Catalyst 6500 または 3750G スイッチに接続することはお勧めしません。

単一の Catalyst 6500 スイッチの中の 2 つのモジュールを終端とすることによって冗長化されるので、一方のモジュールに障害が発生してもスイッチとコントローラの間の接続は維持されます。図 3-12 は、この冗長モジュールの使い方を示しています。4402-50 コントローラが Catalyst 6500 内の 2 つのギガビット モジュール（スロット 2 および 3）に接続されています。コントローラのポート 1 は Catalyst 6500 のギガビット インターフェイス 3/1 に接続されており、コントローラのポート 2 はギガビット インターフェイス 2/1 に接続されています。どちらのスイッチ ポートも、同じチャネル グループに割り当てられています。

4404 コントローラまたは WiSM コントローラ モジュールの LAG ポートの接続先である Catalyst 3750G または 6500 のチャネル グループまたは 7600 のチャネル グループで負荷分散が行われているときは、次の点に注意してください。

- LAG を行うには、コントローラと Catalyst スイッチの両方で EtherChannel が「on」モードに設定されている必要があります。
- リンクの両端で EtherChannel が「on」に設定されると、Catalyst スイッチが Link Aggregation Control Protocol（LACP）と Cisco 独自の Port Aggregation Protocol（PAgP）のどちらを使用するように設定されているかは無視されます。コントローラとスイッチの間のチャネル ネゴシエーションは行われないからです。また、LACP と PAgP はコントローラではサポートされません。
- Catalyst スイッチでのロード バランシングは、すべての IP データグラム フラグメントの終点が単一のコントローラ ポートとなるように設定されている必要があります。この推奨事項に従わない場合は、アクセス ポイントのアソシエートの問題が発生することがあります。
- Catalyst スイッチのロード バランシングには、送信元および宛先 IP アドレスに基づく方法（CLI コマンド：**port-channel load-balance** *src_dest_ip*）を使用することをお勧めします。
- 推奨されるロード バランシング方法を Catalyst スイッチ上で設定できない場合は、LAG 接続を単一メンバ リンクとして設定するか、コントローラで LAG を行わないように設定します。

図 3-12　Catalyst 6500 近接スイッチを使ったリンク集約



リンク集約に関するガイドライン

LAG を使用するときには、次の点に留意してください。

- 1 つのコントローラの複数のポートを別々の LAG グループに設定することはできません。1 つのコントローラがサポートする LAG グループは 1 つのみです。したがって、LAG モードのコントローラ 1 つを接続できる隣接デバイスは 1 つのみです。

（注） Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに装備された 2 つの内部ギガビット ポートは、必ず同じ LAG グループに割り当てられます。

- LAG を有効化したときや、LAG の設定に変更を加えたときは、ただちにコントローラをリブートしてください。
- LAG を有効にした場合、必要な論理ポートは 1 つのみであるため、AP マネージャ インターフェイスを 1 つだけ設定できます。LAG を使用する場合は、複数の AP マネージャ インターフェイスのサポートに関する要件はなくなります。
- LAG を有効にした場合、動的 AP マネージャ インターフェイス、およびタグの付いていないインターフェイスはすべて削除されます。同時に、WLAN がすべて無効になり、管理インターフェイスにマップされます。また、管理インターフェイス、静的 AP マネージャ インターフェイス、および VLAN タグ付き動的インターフェイスは、LAG ポートに移されます。
- 複数のタグなしインターフェイスを同じポートに割り当てることはできません。
- LAG を有効にした場合、29 以外のプライマリ ポートを使用してインターフェイスを作成することはできません。
- LAG を有効にした場合、デフォルトでは、すべてのポートが LAG に参加します。したがって、近接スイッチにある接続されたポートすべてについて、LAG を設定する必要があります。
- Cisco WiSM 上で LAG を有効化した場合は、スイッチ上で、コントローラのすべてのポートに対してポート チャネリング / イーサネット チャネリングを有効にする必要があります。
- LAG を有効にした場合、ポートのミラーリングはサポートされません。
- LAG が有効化されているときは、リンクのいずれかがダウンした場合にトラフィックは別のリンクに移されます。
- LAG が有効化されているときは、物理ポートが 1 つでも機能していればコントローラはクライアント トラフィックを通過させることができます。
- LAG が有効化されているときは、アクセス ポイントはスイッチに接続されたままになります。また、ユーザに対するデータ サービスが中断されることはありません。
- LAG が有効化されているときは、各インターフェイスに対してプライマリとセカンダリのポートを設定する必要はなくなります。
- LAG が有効化されているときは、コントローラがパケットを受信したポートと同じポートからパケットが送信されます。アクセス ポイントからの LWAPP パケットがコントローラの物理ポート 1 に入ると、コントローラによって LWAPP ラッパーが除去され、パケットが処理され、物理ポート 1 からネットワークに転送されます。LAG が無効化されている場合は、このようにはならないことがあります。
- LAG を無効化すると、管理、静的 AP マネージャ、および動的の各インターフェイスはポート 1 に移されます。
- LAG を無効にする場合、すべてのインターフェイスについて、プライマリ ポートとセカンダリ ポートを設定する必要があります。
- LAG を無効にする場合、コントローラ上の各ポートについて、AP マネージャ インターフェイスを割り当てる必要があります。
- Cisco 4400 シリーズ コントローラでは、静的リンク集約バンドルが 1 つだけサポートされます。
- 通常、LAG はスタートアップ ウィザードを使って設定されますが、GUI または CLI を使用して、必要なときに有効または無効にすることができます。

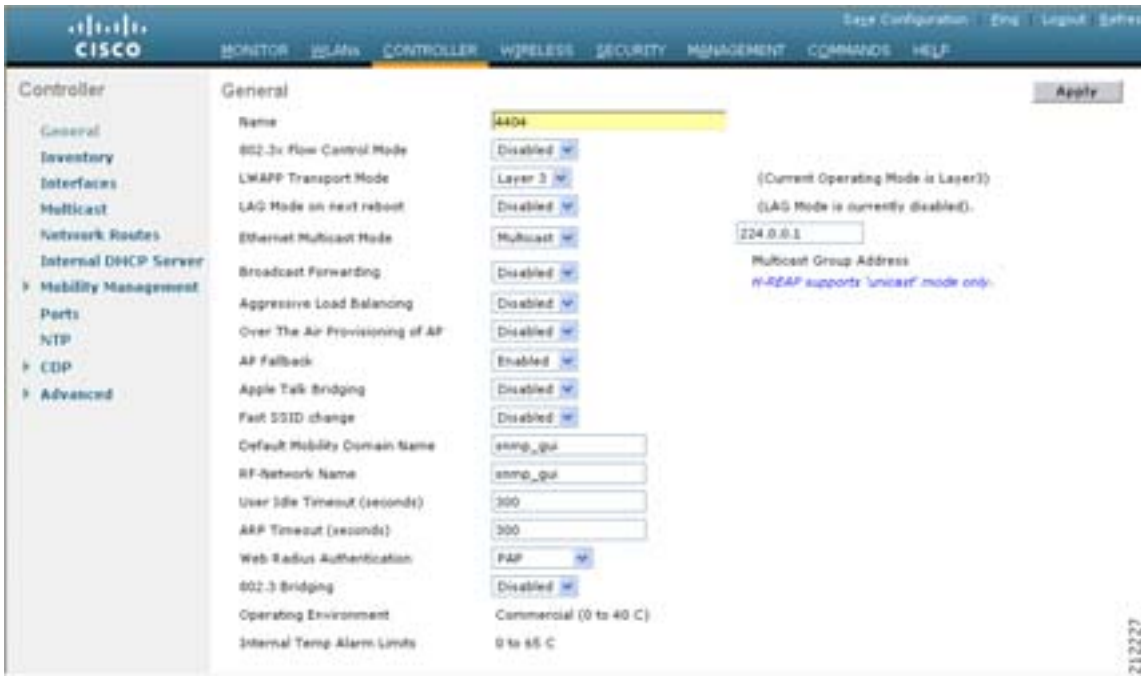
（注） WiSM コントローラおよび Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラでは、LAG はデフォルトで有効化されており、これが唯一のオプションです。

GUI を使用したリンク集約の有効化

GUI を使用して、コントローラで LAG を有効にする手順は、次のとおりです。

ステップ 1　**Controller** > **General** の順にクリックして、General ページを開きます（図 3-13 を参照）。

図 3-13　General ページ



ステップ 2　LAG Mode on Next Reboot パラメータを **Enabled** に設定します。

（注） LAG を無効にするには、**Disabled** を選択します。Cisco 4400 シリーズ コントローラでは LAG はデフォルトで無効化されていますが、Cisco WiSM ではデフォルトで有効化されます。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 5　コントローラをリブートします。

ステップ 6　WLAN を VLAN に割り当てます。

CLI を使ったリンク集約の有効化

CLI を使用して、コントローラで LAG を有効にする手順は、次のとおりです。

ステップ 1　**config lag enable** と入力して、LAG を有効にします。

（注）　LAG を無効にするには、**config lag disable** と入力します。

ステップ 2　**save config** と入力して、設定を保存します。

ステップ 3　コントローラをリブートします。

CLI を使ったリンク集約の確認

LAG の設定を確認するには、次のコマンドを入力します。

show lag summary

次のような情報が表示されます。

```
LAG Enabled
```

LAG をサポートするための隣接デバイスの設定

コントローラの隣接デバイスも、LAG をサポートするように適切に設定する必要があります。

- コントローラが接続されている隣接ポートはそれぞれ、次のように設定します。

```
interface GigabitEthernet <interface id>
switchport
channel-group <id> mode on
no shutdown
```

- 近接スイッチのポート チャネルは、次のように設定します。

```
interface port-channel <id>
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan <native vlan id>
switchport trunk allowed vlan <allowed vlans>
switchport mode trunk
no shutdown
```

49 個以上のアクセス ポイントをサポートするように 4400 シリーズ コントローラを設定

前述のように、4400 シリーズのコントローラは、ポート 1 つにつき、最大 48 個のアクセス ポイントをサポートします。しかし、次のいずれかの方法を使用して、さらに多くのアクセス ポイントをサポートするように 4400 シリーズのコントローラを設定することもできます。

- リンク集約、（P. 3-38）
- 複数の AP マネージャ インターフェイス、（P. 3-38）

使用方法が記されているページの手順に従って操作してください。

コントローラがレイヤ 3 での操作用に設定されている場合、どちらの方法を使用するべきかを判断するポイントは次のとおりです。

- リンク集約では、コントローラのポートはすべて、同一の近接スイッチに接続されている必要があります。近接スイッチがダウンすると、コントローラは接続性を失います
- 複数の AP マネージャ インターフェイスを使用する場合、ポートをさまざまな隣接デバイスへ接続できます。近接スイッチの 1 つがダウンしても、コントローラの接続性は失われません。ただし、ポートの冗長性に不安がある場合、複数の AP マネージャ インターフェイスの使用には、多少の問題があります（詳細は、後述の「複数の AP マネージャ インターフェイスの使用」を参照）。

リンク集約の使用

リンク集約の有効化の詳細と手順は、「リンク集約の有効化」の項（P. 3-33）を参照してください。

（注） リンク集約は、Cisco WiSM および Catalyst 3750G 統合型無線 LAN コントローラ スイッチのコントローラに対して使用可能な唯一の方法です。

複数の AP マネージャ インターフェイスの使用

（注） この方法は、Cisco 4400 シリーズのスタンド アロン コントローラでのみ使用できます。

複数の AP マネージャ インターフェイスを作成すると、インターフェイスはそれぞれ異なるポートにマップされます（図 3-14 を参照）AP マネージャ インターフェイス 2 がポート 2、AP マネージャ インターフェイス 3 がポート 3、AP マネージャ インターフェイス 4 がポート 4 となるように、ポートが順番に設定されている必要があります。

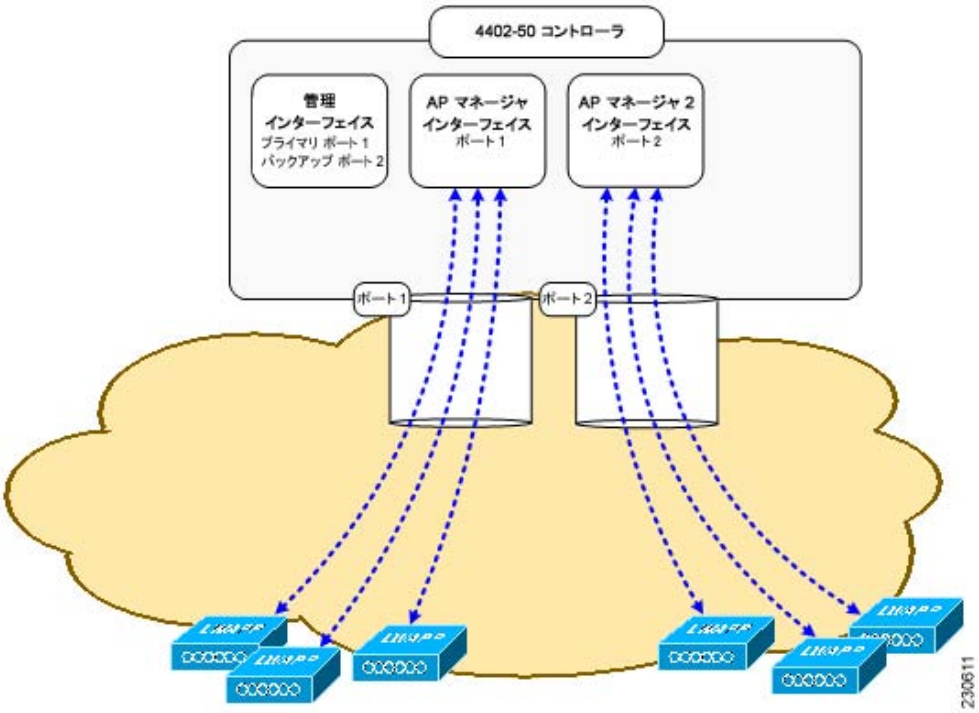
（注） すべての AP マネージャ インターフェイスが同じ VLAN または同じ IP サブネット上になくてもかまいません。また、管理インターフェイスと同じ VLAN または IP サブネットになくても問題はありません。ただし、すべての AP マネージャ インターフェイスが同一の VLAN または IP サブネット上に存在するように設定することをお勧めします。

(注)　コントローラ上の各ポートについて、AP マネージャ インターフェイスを割り当てる必要があります。

アクセス ポイントはコントローラに接続する前に、ディスカバリ要求を送信します。アクセス ポイントは、受信したディスカバリ応答から、コントローラにある AP マネージャ インターフェイスの数と、各 AP マネージャ インターフェイスにあるアクセス ポイントの数を判断します。アクセス ポイントは、通常、最もアクセス ポイント数の少ない AP マネージャに接続します。この方法により、アクセス ポイントの負荷は、複数の AP マネージャ インターフェイスに対して動的に分散されます。

(注)　アクセス ポイントは AP マネージャ インターフェイス全体に、均等に分散されるわけではありませんが、ある程度のロード バランシングは行われます。

図 3-14　2 つの AP マネージャ インターフェイス



複数の AP マネージャ インターフェイスを実装する前に、このことがコントローラのポート冗長性に与える影響を考慮する必要があります。

例：

1. 4402-50 コントローラは最大 50 個のアクセス ポイントをサポートし、ポートを 2 つ持っています。最大数のアクセス ポイントをサポートするには、AP マネージャ インターフェイスを 2 つ作成する必要があります（図 3-14 を参照）。コントローラのポート 1 つあたり 48 個しかアクセス ポイントがサポートされないからです。

2. 4404-100 コントローラは最大 100 個のアクセス ポイントをサポートし、ポートを 4 つ持っています。最大数のアクセス ポイントをサポートするには、AP マネージャ インターフェイスを 3 つまたはそれ以上作成する必要があります（図 3-15 を参照）。いずれかの AP マネージャ インターフェイスのポートで障害が発生した場合は、コントローラによってアクセス ポイントの状態がクリアされるので、通常のコントローラ接続プロセスを使用してコントローラとの通信を再確立するために、アクセス ポイントのリブートが必要になります。この後、コントローラからの LWAPP ディスカバリ応答には、障害を起こした AP マネージャ インターフェイスは含まれなくなります。アクセス ポイントは再度コントローラに接続し、アクセス ポイントの負荷は使用可能な AP マネージャ インターフェイス間に分散されます。

図 3-15　3 つの AP マネージャ インターフェイス

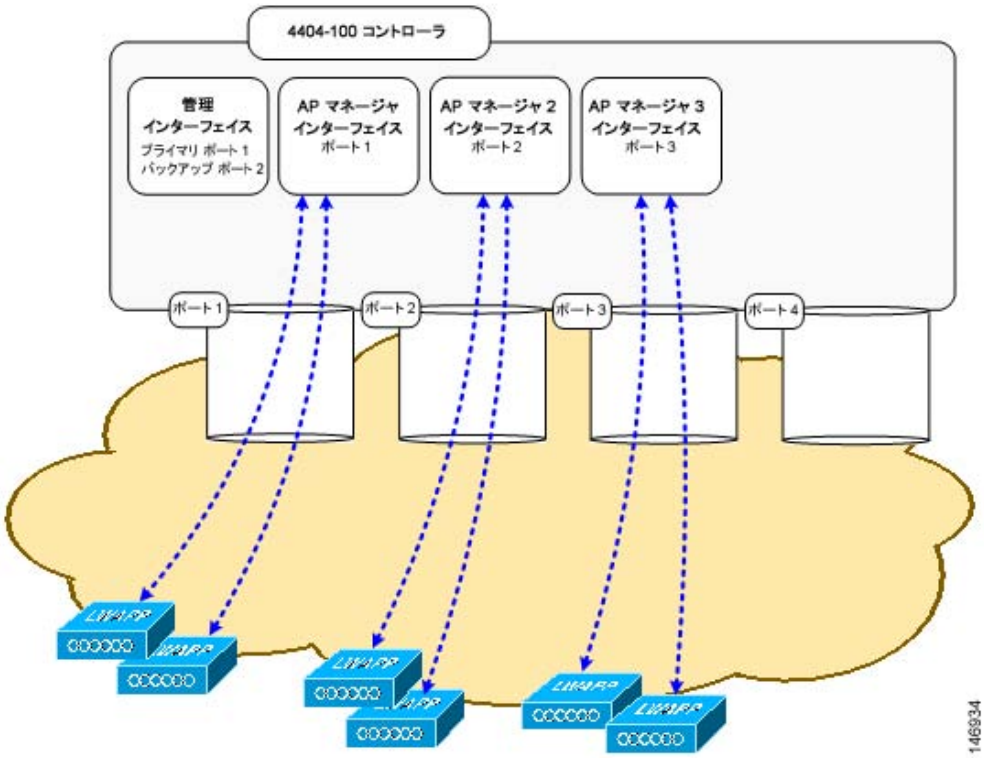
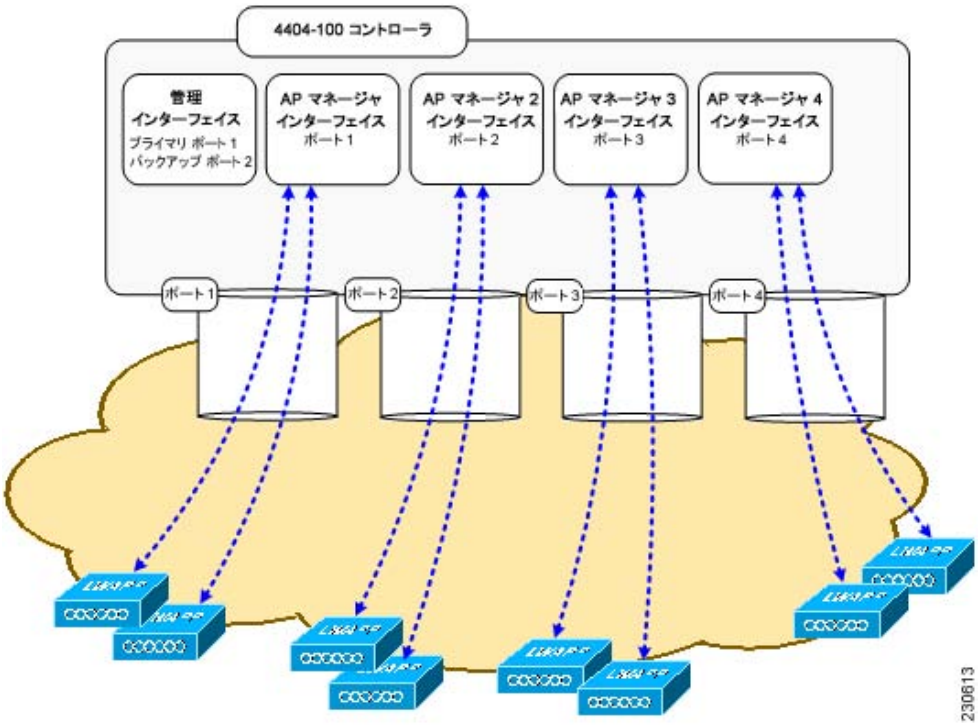


図 3-16 は、4 つの AP マネージャ インターフェイスを使用して、100 個のアクセス ポイントをサポートしている様子を図示したものです。

図 3-16　4 つの AP マネージャ インターフェイス



この設定には、4 つの AP マネージャ インターフェイスすべてにわたって、均等に 100 個のアクセス ポイントをすべてロード バランシングできるという利点があります。AP マネージャ インターフェイスの 1 つで障害が発生しても、このコントローラに接続されているアクセス ポイントはすべて、残り 3 つの使用可能な AP マネージャ インターフェイス間で均等に分散されます。たとえば、AP マネージャ インターフェイス 2 で障害が発生した場合、残りの AP マネージャ インターフェイス（1、3、および 4）はそれぞ約 33 個のアクセス ポイントを管理します。

複数の AP マネージャ インターフェイスを作成する手順は、次のとおりです。

ステップ 1　**Controller** > **Interfaces** の順にクリックして、Interfaces ページを開きます。

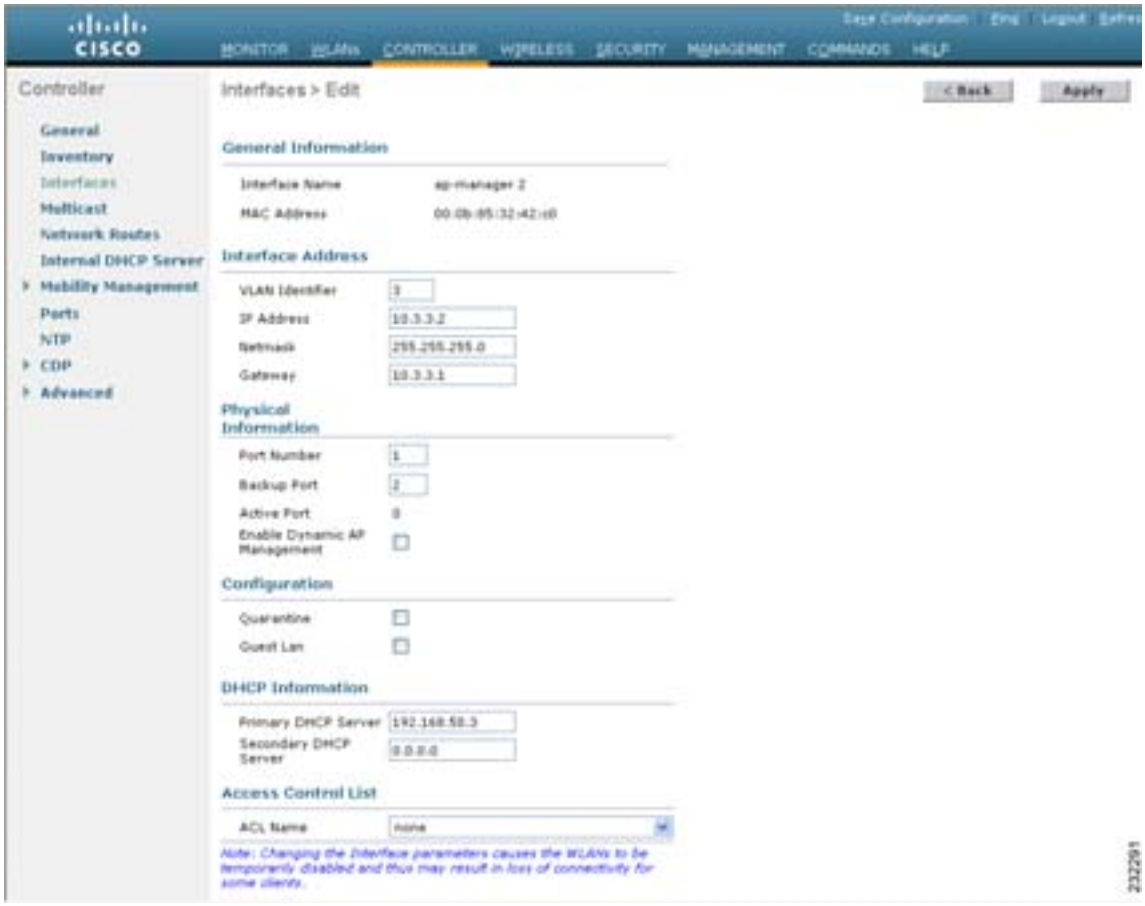
ステップ 2　**New** をクリックします。Interfaces > New ページが表示されます（図 3-17 を参照）。

図 3-17　Interfaces > New ページ

ステップ 3　前述のとおり、AP マネージャ インターフェイスの名前と VLAN 識別子を入力します。

ステップ 4　**Apply** をクリックして、変更を適用します。Interfaces > Edit ページが表示されます（図 3-18 を参照）。

図 3-18　Interfaces > Edit ページ



ステップ 5　適切なインターフェイス パラメータを入力します。

（注）　AP マネージャ インターフェイスのバックアップ ポートは定義しないでください。AP マネージャ インターフェイスに対するポート冗長化はサポートされません。AP マネージャ インターフェイスで障害が発生した場合は、そのインターフェイスを通してコントローラに接続しているすべてのアクセス ポイントが、他の設定済み AP マネージャ インターフェイスに均等に分散されます。

ステップ 6　このインターフェイスを AP マネージャ インターフェイスにするには、**Enable Dynamic AP Management** チェックボックスをオンにします。

ステップ 7　**Save Configuration** をクリックして、設定内容を保存します。

ステップ 8　作成する AP マネージャ インターフェイスそれぞれについて、この手順を繰り返します。

CHAPTER 4

コントローラの設定

この章では、コントローラの設定方法について説明します。この章の内容は、次のとおりです。

設定 ウィザードの使用方法

この項では、最初にコントローラの基本設定を行うとき、または工場出荷時のデフォルトにリセットした後にコントローラの基本設定を行うときの手順について説明します。この章の内容は、コントローラに付属するクイック スタート ガイドの説明と共通する個所があります。

設定ウィザードでは基本的な設定を行います。このウィザードは、Command Line Interface（CLI; コマンドライン インターフェイス）または Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）で実行できます。この項では、CLI でウィザードを実行する方法について説明します。

この項の内容は、次のとおりです。

始める前に

コントローラを設定する前に、次の基本的な設定パラメータを収集しておく必要があります。

- コントローラのシステム名
- サポートされている 802.11 プロトコル：802.11a/n か 802.11b/g/n、または両方
- 管理者のユーザ名およびパスワード（オプション）
- ディストリビューション システム（ネットワーク）ポートの固定 IP アドレス、ネットマスク、およびデフォルトのゲートウェイ IP アドレス
- サービス ポートの固定 IP アドレスおよびネットマスク（オプション）
- ディストリビューション システムの物理ポート（1000BASE-T、1000BASE-SX、または 10/100BASE-T）

（注） 1000BASE-SX コネクタは、LC 物理コネクタを使用した 850nM（SX）光ファイバ リンクで 100/1000Mbps の有線接続をネットワークに提供します。

- ディストリビューション システム ポートの Virtual Local Area Network（VLAN; バーチャル LAN）割り当て（オプション）
- ディストリビューション システム ポートの Web モード設定およびセキュア Web モード設定：有効または無効
- ディストリビューション システム ポートの Spanning Tree Protocol（STP; スパニングツリー プロトコル）：有効 / 無効、各ポートの 802.1D/fast/off モード、各ポートのパス コスト、各ポートの優先順位、ブリッジの優先順位、転送遅延、ハロー タイム、最大経過時間
- WLAN の設定：Service Set Identifier（SSID; サービス セット ID）、VLAN 割り当て、レイヤ 2 セキュリティ設定、レイヤ 3 セキュリティ設定、QoS（Quality of Service）割り当て
- モビリティの設定：モビリティ グループ名（オプション）
- RADIUS 設定
- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）の設定
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバの設定（Cisco サービス統合型ルータにインストールされた無線コントローラ ネットワーク モジュールのウィザードを実行した場合、NTP サーバの設定を求めるプロンプトが表示されます）
- その他のポートおよびパラメータの設定：サービス ポート、Radio Resource Management（RRM）、サードパーティ アクセス ポイント、コンソール ポート、802.3x フロー制御、およびシステム ログ

デフォルト設定へのデバイスのリセット

最初のセットアップ時に、作業を初めからやりなおす必要が生じた場合は、コントローラを工場出荷時のデフォルト設定にリセットできます。

（注） デフォルト設定に戻した後、コントローラにシリアル接続をして、設定ウィザードを実行する必要があります。

CLI を使用したデフォルト設定へのリセット

CLI を使用して設定を工場出荷時のデフォルト設定にリセットする手順は、次のとおりです。

ステップ 1　**reset system** と入力します。変更内容を設定に保存するかどうかを尋ねるプロンプトが表示されたら、**Y** または **N** を入力します。ユニットがリブートします。

ステップ 2　ユーザ名の入力を求められたら、**recover-config** と入力してデフォルトの設定に戻します。コントローラがリブートし、次のメッセージが表示されます。

```
Welcome to the Cisco WLAN Solution Wizard Configuration Tool
```

ステップ 3　設定ウィザードを使用して、設定を入力します。

GUI を使用したデフォルト設定へのリセット

GUI を使用して設定をデフォルト設定に戻す手順は、次のとおりです。

ステップ 1　インターネット ブラウザを開きます。GUI は、Windows プラットフォームで動作する Microsoft Internet Explorer バージョン 6.0 以降に完全に準拠しています。

ステップ 2　ブラウザのアドレス行にコントローラの IP アドレスを入力し、**Enter** キーを押します。Enter Network Password ウィンドウが表示されます。

ステップ 3　User Name フィールドにユーザ名を入力します。デフォルトのユーザ名は *admin* です。

ステップ 4　Password フィールドに無線デバイスのパスワードを入力し、**Enter** キーを押します。デフォルトのパスワードは *admin* です。

ステップ 5　Commands > Reset to Factory Defaults ページを参照します。

ステップ 6　**Reset** をクリックします。プロンプトが表示されるので、リセットの実行を選択します。

ステップ 7　ユニットをリブートします。変更は保存しません。

ステップ 8　設定ウィザードを使用して、設定を入力します。

CLI での設定ウィザードの実行

工場出荷時のデフォルト設定でコントローラをブートすると、bootup スクリプトによって設定ウィザードが実行され、初期設定の入力を求めるプロンプトが表示されます。CLI からこのウィザードを実行して設定を入力する手順は、次のとおりです。

（注） Catalyst 3750G Integrated Wireless LAN Controller Switch でコントローラを設定するには、3750 デバイス マネージャから起動される GUI 設定ウィザードを使用することをお勧めします。手順は、『Catalyst 3750G Integrated Wireless LAN Controller Switch Getting Started Guide』を参照してください。

（注） 利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。

（注） 正しくない応答を入力した場合は、「Invalid Response」などの適切なエラー メッセージがコントローラから返され、ウィザードのプロンプトに戻ります。

（注） 前のコマンド ラインに戻る必要があるときは、ハイフン キーを押してください。

ステップ 1　DB-9 ヌルモデム シリアル ケーブルを使用して、コントローラとコンピュータを接続します。

ステップ 2　以下の設定を使用して、ターミナル エミュレータ セッションを開きます。

- 9600 ボー
- データ ビット 8
- ストップ ビット 1
- パリティなし
- ハードウェア フロー制御なし

ステップ 3　プロンプトで CLI にログインします。デフォルトのユーザ名は *admin*、デフォルトのパスワードは *admin* です。

ステップ 4　必要に応じて、**reset system** と入力してユニットをリブートしてから、ウィザードを開始します。

ステップ 5　システム名を入力します。これは、コントローラに割り当てる名前です。32 文字までの ASCII 文字を入力できます。

ステップ 6　このコントローラに割り当てる管理者のユーザ名およびパスワードを入力します。それぞれ、24 文字までの ASCII 文字を入力できます。デフォルトの管理者ユーザ名およびパスワードは、それぞれ *admin* と *admin* です。

ステップ 7　サービス ポート インターフェイス IP 設定プロトコル（**none** または **DHCP**）を入力します。サービス ポートを使用しない場合、またはサービス ポートに固定 IP アドレスを割り当てる場合は、**none** と入力します。

ステップ 8　手順 7 で **none** と入力したときに、サービス ポートの固定 IP アドレスを入力する必要がある場合は、次の 2 つのプロンプトに対して、サービス ポート インターフェイス IP アドレスとネットマスクを入力します。

ステップ 9　**yes** または **NO** を選択して、Link Aggregation（LAG; リンク集約）を有効または無効にします。LAG の詳細は、第 3 章を参照してください。

ステップ 10　管理インターフェイスの IP アドレスを入力します。

ステップ 11　管理インターフェイス ネットマスクの IP アドレスを入力します。

ステップ 12　デフォルト ルータの IP アドレスを入力します。

ステップ 13　管理インターフェイスの VLAN 識別子（有効な VLAN 識別子またはタグなし VLAN の場合は **0**）を入力します。VLAN 識別子は、スイッチ インターフェイス設定と一致するように設定する必要があります。

ステップ 14　ネットワーク インターフェイス（ディストリビューション システム）の物理ポート番号を入力します。コントローラの場合、設定可能なポートは前面パネル GigE ポートの 1 ～ 4 です。

ステップ 15　クライアント、管理インターフェイス、および使用している場合はサービス ポート インターフェイスに IP アドレスを提供するデフォルト Dynamic Host Configuration Protocol（DHCP）サーバの IP アドレスを入力します。

ステップ 16　アクセス ポイント管理インターフェイスの IP アドレスを入力します。

ステップ 17　コントローラの仮想インターフェイスの IP アドレスを入力します。1.1.1.1 のような、架空の、割り当てられていない IP アドレスを入力する必要があります。

（注）　仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。

ステップ 18　必要に応じて、コントローラを追加するモビリティ グループ /RF グループの名前を入力します。

（注）　ここで入力する名前は、モビリティ グループと RF グループの両方に割り当てられますが、これらのグループは同じではありません。どちらのグループもコントローラの集合を定義するものですが、目的が異なっています。RF グループ内のすべてのコントローラは通常同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラは同じ RF グループに属します。ただし、モビリティ グループはスケーラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現するのに対して、RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現します。詳細は、第 10 章および第 11 章を参照してください。

ステップ 19 **yes** または **no** を入力して、シンメトリック モビリティ トンネリングを有効または無効にします。シンメトリック モビリティ トンネリングを使用すると、任意のサブネット上のルータで Reverse Path Filtering（RPF; 逆方向パス転送）が有効になっている場合、サブネット間のモビリティを継続できるようになります。詳細は、第 11 章を参照してください。

ステップ 20 ネットワーク名または Service Set Identifier（SSID）を入力します。初期 SSID によりコントローラの基本機能が有効になり、コントローラが結合されているアクセス ポイントで無線が有効になります。

ステップ 21 クライアントが独自の IP アドレスを割り当てられるようにする場合は **yes** と入力します。クライアントが DHCP サーバの IP アドレスを使用する必要がある場合は、**no** と入力します。

ステップ 22 RADIUS サーバをここで設定するには、**yes** と入力してから、RADIUS サーバの IP アドレス、通信ポート、および秘密鍵を入力します。それ以外の場合は、**no** と入力します。no を入力した場合は、「Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details」というメッセージが表示されます。

ステップ 23 ネットワークが配置されている国のコードを入力します。使用可能な国コードの一覧を表示するには、**help** と入力します。

（注） 複数の国のアクセス ポイントを 1 つのコントローラで管理する場合は、複数の国コードを入力できます。複数の国コードを入力するには、国コードをカンマで区切ります（「US,CA,MX」など）。設定ウィザードの実行後、コントローラに接続している各アクセス ポイントに特定の国を割り当てる必要があります。手順については、「国コードの設定」の項（P. 7-32）を参照してください。

ステップ 24 Cisco サービス統合型ルータにインストールされた無線コントローラ ネットワーク モジュールのウィザードを実行した場合のみ、NTP サーバの設定を求めるプロンプトが表示されます。コントローラ ネットワーク モジュールにはバッテリがないため、時間設定を保存できません。電源を投入する際に、外部 NTP サーバから時間設定を受信する必要があります。

ステップ 25 **yes** または **no** と入力して、802.11b、802.11a、および 802.11g Lightweight アクセス ポイント ネットワークそれぞれのサポートを有効または無効にします。

ステップ 26 **yes** または **no** と入力して、Radio Resource Management（RRM）自動 RF 機能を有効または無効にします。RRM の詳細は、第 10 章を参照してください。

（注） 自動 RF 機能により、他のコントローラとの RF グループをコントローラで自動生成できるようになります。グループでは、チャネルや送信電力の割り当てなど、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。

コントローラによって設定が保存され、リブートし、ログインのプロンプトが表示されます。デフォルト設定にリセットし、ウィザードに戻るには、**recover-config** と入力します。

設定のないコントローラでの AutoInstall 機能の使用

設定のないコントローラを起動した場合、AutoInstall 機能によって、TFTP サーバから設定ファイルがダウンロードされ、設定がコントローラに自動的にロードされます。

AutoInstall の概要

ネットワーク上に（または WCS フィルタを介して）すでに存在するコントローラに設定ファイルを作成する場合は、TFTP サーバに設定ファイルを配置し、DHCP サーバを設定します。これによって新しいコントローラは IP アドレスと TFTP サーバの情報を取得でき、AutoInstall 機能が新しいコントローラの設定ファイルを自動的に取得できます。

コントローラを起動すると、AutoInstall プロセスが開始されます。設定ウィザードが起動したことが AutoInstall へ通知されないかぎり、コントローラは何も処理しません。設定ウィザードが起動しなければ、コントローラの設定は有効です。

AutoInstall は、設定ウィザードが起動したことを通知されると（つまり、コントローラに設定がないときは）、さらに 30 秒間待機します。この間、ユーザは設定ウィザードからの最初のプロンプトに応答できます。

```
Would you like to terminate autoinstall? [yes]:
```

30 秒の中断タイムアウトが経過すると、AutoInstall は DHCP クライアントを起動します。プロンプトで **Yes** と入力すると、30 秒のタイムアウトが経過した後でも AutoInstall タスクを中断できます。ただし、TFTP タスクがフラッシュをロックしていて、有効な設定ファイルをダウンロードしながらインストールしている場合は、AutoInstall を中断できません。

DHCP による IP アドレスの入手、および TFTP サーバからの設定ファイルのダウンロード

AutoInstall では以下のインターフェイスが使用されます。

- 4400 シリーズ コントローラ
  - eth0：サービス ポート（タグなし）
  - dtl0：NPU を介したギガビット ポート 1（タグなし）
- 2100 シリーズ コントローラ
  - dtl0：FastEthernet ポート 1（タグなし）

AutoInstall は DHCP プロセスが正常に終了するまで、またはユーザが AutoInstall プロセスを停止するまで DHCP サーバから IP アドレスを取得しようとします。DHCP サーバから IP アドレスを正常に取得するための最初のインターフェイスは、AutoInstall タスクに登録されます。このインターフェイスの登録によって、AutoInstall は TFTP サーバ情報の取得と、設定ファイルのダウンロードのプロセスを開始します。

インターフェイスの DHCP IP アドレスを取得した後、AutoInstall はコントローラのホスト名と TFTP サーバの IP アドレスを決定する短い一連のイベントを開始します。この一連のイベントの各段階では、デフォルト情報または暗黙的情報よりも明示的に設定された情報が優先され、明示的 IP アドレスよりも明示的ホスト名が優先されます。

プロセスは次のとおりです。

- DHCP を介して 1 つ以上の Domain Name System（DNS）サーバ IP アドレスが得られると、AutoInstall は /etc/resolv.conf ファイルを作成します。このファイルにはドメイン名、および受信された DNS サーバのリストが含まれます。Domain Name Server オプションでは、DNS サーバのリストが提供され、Domain Name オプションではドメイン名が提供されます。
- ドメイン サーバがコントローラと同じサブネット上にない場合、静的ルート エントリがドメイン サーバごとにインストールされます。これらの静的ルートは、HDCP Router オプションを介して取得されたゲートウェイをポイントします。
- コントローラのホスト名は、次のいずれかの順序で決定されます。
  - DHCP Host Name オプションが受信された場合、この情報（最初のピリオド [.] で切り捨てられる）がコントローラのホスト名として使用されます。
  - DNS の逆ルックアップがコントローラの IP アドレスで実行されます。DNS がホスト名を返すと、（最初のピリオド [.] で切り捨てられた）この名前はコントローラのホスト名として使用されます。
- TFTP サーバの IP アドレスは、次のいずれかの順序で決定されます。
  - AutoInstall が DHCP TFTP Server Name オプションを受信した場合、AutoInstall はこのサーバ名の DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - DHCP Server Host Name（sname）フィールドが有効な場合、AutoInstall はこの sname の DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - AutoInstall が DHCP TFTP Server Address オプションを受信した場合、このアドレスが TFTP サーバの IP アドレスとして使用されます。
  - AutoInstall はデフォルトの TFTP サーバ名（cisco-wlc-tftp）の DNS lookup を実行します。DNS lookup が正常に終了した場合、受信した IP アドレスが TFTP サーバの IP アドレスとして使用されます。
  - DHCP サーバの IP アドレス（siaddr）フィールドがゼロ以外の値である場合、このアドレスは TFTP サーバの IP アドレスとして使用されます。
  - 制限されたブロードキャスト アドレス（255.255.255.255）が TFTP サーバの IP アドレスとして使用されます。
- TFTP サーバがコントローラと同じサブセットにない場合、静的ルート（/32）が TFTP サーバの IP アドレスとしてインストールされます。この静的ルートは、HDCP Router オプションを介して取得されたゲートウェイをポイントします。

（注） コントローラに DHCP を設定する方法の詳細は、「DHCP の設定」の項（P. 6-6）を参照してください。

（注） コントローラに TFTP サーバを設定する方法の詳細は、第 8 章を参照してください。

（注） WCS を介して DHCP サーバと TFTP サーバを設定する方法の詳細は、『Cisco Wireless Control System Configuration Guide, Release 5.0』の第 10 章を参照してください。

設定ファイルの選択

ホスト名と TFTP サーバが決定されると、AutoInstall は設定ファイルのダウンロードを試行します。AutoInstall は DHCP IP アドレスを取得するインターフェイスごとに 3 回の完全なダウンロードを繰り返します。たとえば、4400 シリーズ コントローラが eth0 と dtl0 の両方で DHCP IP アドレスを取得すると、各インターフェイスは設定のダウンロードを試行します。インターフェイスは、3 回の試行後に設定ファイルを正常にダウンロードできない場合、それ以上のダウンロードを試行しません。

正常にダウンロードおよびインストールされた最初の設定ファイルがコントローラのリブートをトリガします。リブート後に、コントローラは新しくダウンロードされた設定を実行します。

AutoInstall は、名前がリストアップされる順番で設定ファイルを検索します。

- DHCP Boot File Name オプションによって提供されるファイル名
- DHCP File フィールドで提供されるファイル名
- *host name*-confg
- *host name*.cfg
- *Base MAC Address*-confg（011.2233.4455-confg など）
- *serial number*-confg
- ciscowlc-confg
- ciscowlc.cfg

AutoInstall は、設定ファイルを見つけるまでは、このリストを介して実行します。登録されているインターフェイスごとにこのリストを 3 回サイクルし、設定ファイルが見つからない場合、実行を停止します。

（注） ダウンロードされる設定ファイルは、完全な設定を行えることもあれば、WCS で管理されるコントローラに十分な程度の情報を持つ最小限の設定のこともあります。完全な設定ファイルは、WCS から直接展開できます。

（注） AutoInstall が TFTP サーバから取得できる設定ファイルの作成とアップロードの詳細は、第 8 章を参照してください。

（注） WCS リリース 5.0 はコントローラに AutoInstall 機能を提供します。WCS 管理者はコントローラのホスト名、MAC アドレス、シリアル番号を含むフィルタを作成し、このフィルタのルールにテンプレートのグループ（設定グループ）を関連付けることができます。WCS は、コントローラの最初の起動時に初期設定をコントローラにコピーします。コントローラが検出された後、WCS は設定グループで定義されているテンプレートをコピーします。AutoInstall の機能と WCS の詳細は、『Cisco Wireless Control System Configuration Guide, Release 5.0』の第 15 章を参照してください。

AutoInstall の操作例

以下は AutoInstall の全プロセスの一例です。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interation 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ===> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==>
'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not
found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)

Resetting system
```

システムの日時の管理

コントローラは、Network Time Protocol（NTP）サーバから日時を取得することや、手動で日時を設定することができます。コントローラ上の時間帯設定の規格には、Greenwich Mean Time（GMT; グリニッジ標準時）が使用されます。

日時を取得するための NTP サーバの設定

各 NTP サーバの IP アドレスは、コントローラ データベースに追加されています。すべてのコントローラは NTP サーバを検索して、リブート時およびユーザ定義ポーリング間隔ごとに（毎日から毎週）、現在時刻を取得できます。

NTP サーバから日時を取得するように設定するコマンドを使用します。

1. コントローラの NTP サーバを指定するには、次のコマンドを入力します。

   config time ntp server *index ip_address*

2. ポーリングの間隔（秒）を指定するには、次のコマンドを入力します。

   config time ntp *interval*

手動による日時の設定

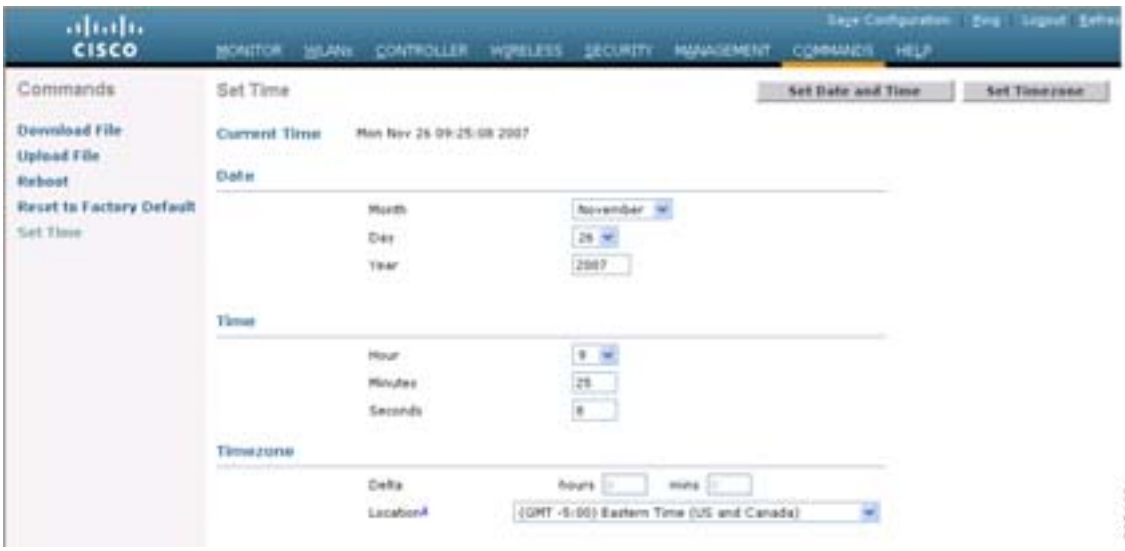
コントローラの GUI または CLI を使用して日時を手動で設定するには、この項の手順に従ってください。

GUI を使用した日時の設定

コントローラの GUI を使用して現地の日時を設定する手順は、次のとおりです。

ステップ 1　**Commands** > **Set Time** の順にクリックして、Set Time ページを開きます（図 4-1 を参照）。

図 4-1　Set Time ページ



現在の日時がページ上部に表示されます。

ステップ 2　Timezone の項の Location ドロップダウン ボックスから現地の時間帯を選択します。

（注）　Daylight Savings Time（DST; 夏時間）を使用する時間帯を選択すると、DST の発生時の時間変更を反映してコントローラが自動的にそのシステム クロックを設定します。米国では、DST は 3 月の第 2 日曜から始まり、11 月の第 1 日曜日で終わります。

（注）　コントローラ GUI に時間帯デルタは設定できません。ただし、コントローラ CLI に設定すると、変更がコントローラ GUI の Delta Hours フィールドと Mins フィールドに反映されます。

ステップ 3　**Set Timezone** をクリックして、変更を適用します。

ステップ 4　Date の項の、Month と Day ドロップダウン ボックスから現在の現地の月と日を選択し、Year フィールドに年を入力します。

ステップ 5　Time の項の Hour ドロップダウン ボックスから現在の現地時間を選択し、Minutes フィールドと Seconds フィールドに分と秒を入力します。

（注）　日時を設定した後に、時間帯のロケーションを変更すると、Time の項の値が更新され、この新しい時間帯のロケーションが反映されます。たとえば、コントローラが東部標準時の正午に設定されていて、時間帯を太平洋標準時に変更すると、時間は自動的に午前 9 時に変更されます。

ステップ 6　**Set Date and Time** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した日時の設定

コントローラの CLI を使用して現地の日時を設定する手順は、次のとおりです。

ステップ 1　コントローラ上の現在の現地日時を GMT で設定するには、次のコマンドを入力します。

config time manual *mm/dd/yy hh:mm:ss*

（注）　時刻を設定する際は、現在の現地時間を GMT で 00:00 ～ 24:00 の値で入力します。たとえば、米国の太平洋標準時刻の午前 8 時の場合は、太平洋標準時の時間帯が GMT より 8 時間遅れているため、16:00 と入力します。

ステップ 2　コントローラに時間帯を設定するには、次のいずれかを実行します。

- 夏時間（DST）が発生時に自動的に設定されるように時間帯ロケーションを設定するには、次のコマンドを入力します。

  config time timezone location *location_index*

  location_index は次のいずれかの時間帯ロケーションの 1 つを表す数字です。

  - 1.（GMT-12:00）国際日付変更線の西側
  - 2.（GMT-11:00）サモア
  - 3.（GMT-10:00）ハワイ
  - 4.（GMT-9:00）アラスカ
  - 5.（GMT-8:00）太平洋標準時（米国およびカナダ）
  - 6.(GMT-7:00)山地標準時(米国およびカナダ)
  - 7.（GMT-6:00）中部標準時（米国およびカナダ）
  - 8.（GMT-5:00）東部標準時（米国およびカナダ）
  - 9.（GMT-4:00）大西洋標準時（カナダ）
  - 10.（GMT-3:00）ブエノスアイレス（アルゼンチン）
  - 11.（GMT-2:00）中央大西洋
  - 12.（GMT-1:00）アゾレス諸島
  - 13.（GMT）ロンドン、リスボン、ダブリン、エジンバラ（デフォルト値）
  - 14.（GMT+1:00）アムステルダム、ベルリン、ローマ、ウィーン
  - 15.（GMT+2:00）エルサレム
  - 16.（GMT+3:00）バクダッド
  - 17.（GMT+4:00）マスカット、アブダビ
  - 18.（GMT+4:30）カブール
  - 19.（GMT+5:00）カラチ、イスラマバード、タシケント
  - 20.（GMT +5:30) コロンボ、コルカタ、ムンバイ、ニューデリー
  - 21.（GMT+5:45）カトマンズ
  - 22.（GMT+6:00）アルマティ、ノボシビルスク
  - 23.（GMT+6:30）ラグーン
  - 24.（GMT+7:00）サイゴン、ハノイ、バンコク、ジャカルタ
  - 25.（GMT+8:00）香港、北京、重慶
  - 26.（GMT+9:00）東京、大阪、札幌
  - 27.（GMT+9:30）ダーウィン
  - 28.（GMT+10:00）シドニー、メルボルン、キャンベラ
  - 29.（GMT+11:00）マガダン、ソロモン諸島、ニューカレドニア
  - 30.（GMT+12:00）カムチャッカ、マーシャル諸島、フィジー

  （注） このコマンドを入力すると、DST に入ったときに、コントローラが自動的にそのシステム クロックを DST に合わせて設定します。米国では、DST は 3 月の第 2 日曜から始まり、11 月の第 1 日曜日で終わります。

- DST が自動的に設定されないように時間帯を手動で設定するには、次のコマンドを入力します。

  config time timezone *delta_hours delta_mins*

delta_hours は GMT と現地の時間単位の時差、*delta_mins* は、GMT と現地の分単位の時差です。

時間帯を手動で設定する際は、現地の現在の時間帯の時差を GMT（+/-）で入力します。たとえば、米国の太平洋標準時は、GMT の時刻より 8 時間遅れています。したがって、-8 と入力します。

（注） 時間帯を手動で設定することで、コントローラ CLI のみで DST が設定されることを回避できます。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　コントローラが現在の現地時間を現地の時間帯で表示していることを確認するには、次のコマンドを入力します。

show time

次のような情報が表示されます。

```
Time..................................... Mon Nov 26 10:25:33 2007

Timezone delta.............................. 0:0
Timezone location........................... (GMT -5:00) Eastern Time (US and
Canada)

NTP Servers
    NTP Polling Interval.....................     86400

     Index              NTP Server
    -------  --------------------------------
       1     19.1.1.1
```

（注） 時間帯ロケーションを設定している場合、Timezone Delta の値は「0:0」に設定されます。時間帯デルタを使用して時間帯を手動で設定している場合、Timezone Location は空白になります。

802.11 帯域の設定

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n（2.4GHz）帯域と 802.11a/n（5GHz）帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n の両方が有効になっています。

GUI を使用した 802.11 帯域の設定

コントローラの GUI を使用して 802.11 帯域を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **Network** の順にクリックして、802.11a（または 802.11b/g）Global Parameters ページを開きます（図 4-2 を参照）。

図 4-2　802.11a Global Parameters ページ

ステップ 2　802.11a または 802.11b/g 帯域を有効にするには、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオンにします。帯域を無効にするには、チェックボックスをオフにします。デフォルト値は有効（enable）です。802.11a 帯域と 802.11b/g 帯域の両方を有効にすることができます。

ステップ 3　ステップ 2 で 802.11b/g 帯域を有効にした場合に、802.11g ネットワークのサポートを有効にするには、**802.11g Support** チェックボックスをオンにします。デフォルト値は有効（enable）です。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。

ステップ 4　アクセス ポイントによる SSID のブロードキャスト レートを指定するには、100 ～ 600 ミリ秒（両端の値を含む）の値を Beacon Period フィールドに入力します。デフォルト値は 100 ミリ秒です。

ステップ 5　断片化するパケットのサイズを指定するには、256 ～ 2346 バイト（両端の値を含む）の値を Fragmentation Threshold フィールドに入力します。接続不良や多くの無線干渉が発生している領域の下位番号を入力します。

ステップ 6　アクセス　ポイントでそれらの領域のチャネルと送信電力レベルをビーコンおよびプローブ応答でアドバタイズできるようにするには、**DTPC Support** チェックボックスをオンにします。有効にしない場合には、このチェックボックスをオフにします。デフォルト値は有効（enable）です。

Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアント デバイスでは、アクセス ポイントからチャネルおよび電力レベル情報を受信し、自動でそれらの設定を調整します。たとえば、主に日本で使用されているクライアント デバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。

（注）　シスコ IOS ソフトウェアを実行しているアクセス ポイントでは、この機能は *ワールド モード*と呼ばれます。

ステップ 7　アクセス ポイントとクライアントとの間のデータ送信レートを指定するには、Data Rates オプションを使用します。次のデータ レートが使用可能です。

- 802.11a：6、9、12、18、24、36、48、および 54Mbps
- 802.11b/g：1、2、5.5、6、9、11、12、18、24、36、48、または 54Mbps

各データ レートに対して、次のオプションのいずれかを選択します。

- **Mandatory**：コントローラ上でアクセス ポイントにアソシエートするには、クライアントでこのデータ レートをサポートしている必要があります。
- **Supported**：このデータ　レートをサポートしているアソシエートされたクライアントは、このレートを使用してアクセス ポイントと通信します。ただし、アソシエートするためにクライアントでこのレートを使用できるようにする必要はありません。
- **Disabled**：通信に使用するデータ レートがクライアントによって指定されます。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した 802.11 帯域の設定

コントローラ CLI を使用して 802.11 帯域を設定する手順は、次のとおりです。

ステップ 1　802.11a 帯域を無効にするには、次のコマンドを入力します。

config 802.11a disable network

（注）　802.11a 帯域を無効にしてから、この項の 802.11a ネットワーク パラメータを設定してください。

ステップ 2　802.11b/g 帯域を無効にするには、次のコマンドを入力します。

config 802.11b disable network

（注） 802.11b 帯域を無効にしてから、この項の 802.11b ネットワーク パラメータを設定してください。

ステップ 3　アクセス ポイントによる SSID のブロードキャスト レートを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

time_unit は、単位時間（TU）でのビーコン間隔です。1 TU は 1024 マイクロ秒です。20 ～ 1000 ミリ秒ごとにビーコンを送信するように、アクセス ポイントを設定できます。

ステップ 4　断片化するパケットのサイズを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **fragmentation** *threshold*

threshold の値は、256 ～ 2346 バイト（両端の値を含む）です。接続不良や多くの無線干渉が発生している領域の下位番号を指定します。

ステップ 5　アクセス　ポイントでその領域のチャネルと送信電力レベルをビーコンおよびプローブ応答でアドバタイズできるようにするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **dtpc** {**enable** | **disable**}

デフォルト値は有効（enable）です。Dynamic Transmit Power Control（DTPC）を使用するクライアント デバイスでは、アクセス ポイントからチャネルおよび電力レベル情報を受信し、自動でそれらの設定を調整します。たとえば、主に日本で使用されているクライアント デバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。

（注） シスコ IOS ソフトウェアを実行しているアクセス ポイントでは、この機能は *ワールド モード*と呼ばれます。

ステップ 6　コントローラとクライアントとの間のデータ送信レートを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

このとき、次のようになります。

- **disabled**：通信に使用するデータ レートがクライアントによって指定されます。
- **mandatory**：コントローラ上でアクセス ポイントにアソシエートするには、クライアントでこのデータ レートをサポートするように指定します。
- **supported**：このデータ　レートをサポートしているアソシエートされたクライアントは、このレートを使用してアクセス ポイントと通信します。ただし、アソシエートするためにクライアントでこのレートを使用できるようにする必要はありません。
- *rate*：データを送信する際のレートです。
  - 6、9、12、18、24、36、48、および 54Mbps（802.11a）
  - 1、2、5.5、6、9、11、12、18、24、36、48、または 54Mbps（802.11b/g）

ステップ 7　802.11a 帯域を有効にするには、次のコマンドを入力します。

config 802.11a enable network

デフォルト値は有効（enable）です。

ステップ 8　802.11b 帯域を有効にするには、次のコマンドを入力します。

config 802.11b enable network

デフォルト値は有効（enable）です。

ステップ 9　802.11g ネットワークのサポートを有効または無効にするには、次のコマンドを入力します。

config 802.11b 11gSupport {enable | disable}

デフォルト値は有効（enable）です。このコマンドは、802.11b 帯域が有効になっている場合のみ使用できます。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。

ステップ 10　変更を保存するには、次のコマンドを入力します。

save config

ステップ 11　802.11a または 802.11b/g 帯域の設定を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b}

次のような情報が表示されます。

```
802.11a Network..............................  Enabled
11nSupport...................................  Enabled
      802.11a Low Band.......................  Enabled
      802.11a Mid Band.......................  Enabled
      802.11a High Band......................  Enabled
802.11a Operational Rates
    802.11a 6M Rate..........................  Mandatory
    802.11a 9M Rate..........................  Supported
    802.11a 12M Rate.........................  Mandatory
    802.11a 18M Rate.........................  Supported
    802.11a 24M Rate.........................  Mandatory
    802.11a 36M Rate.........................  Supported
    802.11a 48M Rate.........................  Supported
    802.11a 54M Rate.........................  Supported
...
Beacon Interval..............................  100
...
Default Channel..............................  36
Default Tx Power Level.......................  1
DTPC Status..................................  Enabled
Fragmentation Threshold......................  2346
...
```

802.11n パラメータの設定

この項では、ネットワーク上の Cisco Aironet 1250 シリーズ アクセス ポイントなどの 802.11n デバイスを管理する手順について説明します。802.11n デバイスでは、2.4GHz 帯域と 5GHz 帯域をサポートしており、高スループット データ レートを提供します。

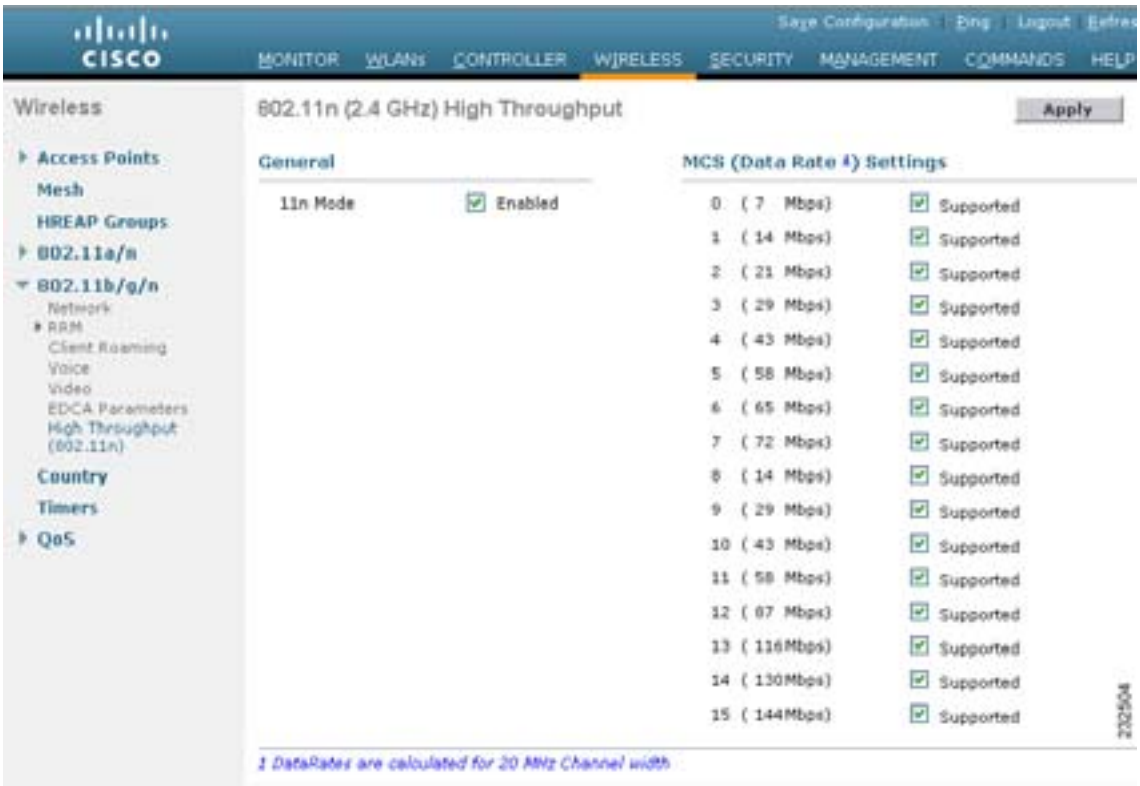
(注)　802.11n 高スループット データ レートは、レイヤ 2 暗号化のない WLAN か、WPA2 暗号化や AES 暗号化が有効になっている WLAN 用の 1250 シリーズ アクセス ポイントでのみ使用可能です。

GUI を使用した 802.11n パラメータの設定

コントローラの GUI を使用して 802.11n パラメータを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **High Throughput (802.11n)** の順にクリックして、802.11n (5 GHz or 2.4 GHz) High Throughput ページを開きます（図 4-3 を参照）。

図 4-3　802.11n (2.4 GHz) High Throughput ページ



ステップ 2　ネットワークでの 802.11n サポートを有効にするには、**11n Mode** チェックボックスをオンにします。デフォルト値は有効（enable）です。

ステップ 3　アクセス ポイントとクライアントとの間でデータを送信する際の Modulation and Coding Scheme（MCS; 変調および符号化方式）のレートを指定するには、目的のレートのチェックボックスをオンにします。20MHz のチャネル幅に対して算出された、下記のデータ レートが使用可能です。

- 0（7Mbps）
- 1（14Mbps）
- 2（21Mbps）
- 3（29Mbps）
- 4（43Mbps）
- 5（58Mbps）
- 6（65Mbps）
- 7（72Mbps）
- 8（14Mbps）
- 9（29Mbps）
- 10（43Mbps）
- 11（58Mbps）
- 12（87Mbps）
- 13（116Mbps）
- 14（130Mbps）
- 15（144Mbps）

選択したレートをサポートしているアソシエートされたクライアントは、それらのレートを使用してアクセス ポイントと通信します。ただし、アソシエートするためにクライアントでこのレートを使用できるようにする必要はありません。MCS 設定では、使用する空間ストリーム数、変調、符号化レート、およびデータ レートの値を定めます。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　設定した 802.11n データ レートを使用するには、WLAN 上で WMM を有効にする必要があります。手順は次のとおりです。

a. **WLANs** をクリックして、WLANs ページを開きます。

b. WMM モードを設定する WLAN の名前をクリックします。

c. WLANs > Edit ページが表示されたら、**QoS** タブをクリックして WLANs > Edit (QoS) ページを開きます。

d. WMM Policy ドロップダウン ボックスから **Required** または **Allowed** 選択して、クライアント デバイスに WMM の使用を要求または許可します。WMM をサポートしていないデバイスは WLAN に接続できません。

（注）　任意の WLAN 上で WMM が 有効になっており、レイヤ 2 LWAPP モードに設定されている場合、アクセス ポイントは、WMM クライアントの QoS 制御フィールドに基づく VLAN ID 0 を使用して、802.1q PRI フィールドにあるそのアクセス ポイントの優先度情報を送信します。レイヤ 3 LWAPP モードでは、この情報は LWAPP パケットの IP ヘッダの DSCP で伝達されます。アクセス ポイントを接続するシスコ以外のアクセス スイッチの中には、VLAN タグの ID 0 を適切に処理しないものもあります。たとえば、そのようなスイッチは、VLAN ID 0 のタグを付けられたパケットをドロップする可能性があり、WMM 有効のアクセス ポイントが レイヤ 2 LWAPP モードでコントローラに接続できなくなり、繰り返しリブートする原因となります。したがって、コントローラがレイヤ 2 モードに設定されていて、かつ WMM が有効な場合は、コントローラに接続できるようにアクセス ポイントをスイッチのトランク ポート上に設置する必要があります。スイッチのトランク ポートへの接続後にアクセス ポイントからコントローラへ接続できない場合は、WMM を使用するためにレイヤ 3 LWAPP モードでコントローラを使用する必要があります。

e. **Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

（注）　アクセス ポイントが 802.11n をサポートしているかどうかを判断するには、802.11a/n（または 802.11b/g/n）Cisco APs > Configure ページか、802.11a/n（または 802.11b/g/n）AP Interfaces > Details ページの 11n Supported フィールドを確認します。

CLI を使用した 802.11n パラメータの設定

コントローラの CLI を使用して 802.11n パラメータを設定する手順は、次のとおりです。

ステップ 1　ネットワークで 802.11n サポートを有効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **11nsupport** {**enable** | **disable**}

ステップ 2　アクセス ポイントとクライアントとの間でデータを送信する際の Modulation and Coding Scheme（MCS）のレートを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}

0 ～ 15 の MCS データ レートの説明については、「GUI を使用した 802.11n パラメータの設定」の項（P. 4-19）を参照してください。

ステップ 3　設定した 802.11n データ レートを使用するには、WLAN 上で WMM を有効にする必要があります。そのためには、次のコマンドを入力します。

config wlan wmm required *wlan_id*

required パラメータは、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。

（注）　任意の WLAN 上で WMM が 有効になっており、レイヤ 2 LWAPP モードに設定されている場合、アクセス ポイントは、WMM クライアントの QoS 制御フィールドに基づく VLAN ID 0 を使用して、802.1q PRI フィールドにあるそのアクセス ポイントの優先度情報を送信します。レイヤ 3 LWAPP モードでは、この情報は LWAPP パケットの IP ヘッダの DSCP で伝達されます。アクセス ポイントを接続するシスコ以外のアクセス スイッチの中には、VLAN タグの ID 0 を適切に処理しないものもあります。たとえば、そのようなスイッチは、VLAN ID 0 のタグを付けられたパケットをドロップする可能性があり、WMM 有効のアクセス ポイントが レイヤ 2 LWAPP モードでコントローラに接続できなくなり、繰り返しリブートする原因となります。したがって、コントローラがレイヤ 2 モードに設定されていて、かつ WMM が有効な場合は、コントローラに接続できるようにアクセス ポイントをスイッチのトランク ポート上に設置する必要があります。スイッチのトランク ポートへの接続後にアクセス ポイントからコントローラへ接続できない場合は、WMM を使用するためにレイヤ 3 LWAPP モードでコントローラを使用する必要があります。

ステップ 4　802.11n パケットに使用する集約方法を指定する手順は、次のとおりです。

a. ネットワークを無効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} disable network

b. 集約方法を指定するには、次のコマンドを入力します。

config {802.11a | 802.11b} 11nsupport a-mpdu tx priority {0-7 | all} {enable | disable}

集約とは、パケットのデータ フレームを別々に送信するのではなく、グループ化するプロセスです。次の 2 つの集約方法が使用可能です。Aggregated MAC Protocol Data Unit（A-MPDU; 集約 MAC プロトコル データ ユニット）および Aggregated MAC Service Data Unit（A-MSDU; 集約 MAC サービス データ ユニット）。A-MPDU はソフトウェアで実行され、A-MSDU はハードウェアで実行されます。

アクセス ポイントからクライアントへのさまざまなタイプのトラフィックに対して集約方法を指定できます。表 4-1 は、トラフィック タイプごとに割り当てる優先レベル（0 ～ 7）を定義しています。

表 4-1　トラフィック タイプの優先レベル

ユーザ優先度	トラフィック タイプ
0	ベスト エフォート
1	バックグラウンド
2	スペア
3	エクセレント エフォート
4	制御された負荷
5	ビデオ、遅延およびジッタは 100 ミリ秒未満
6	音声、遅延およびジッタは 10 ミリ秒未満
7	ネットワーク制御

各優先レベルを個別に設定するか、**all** パラメータを使用して一度にすべての優先レベルを設定できます。**enable** コマンドを使用する場合は、その優先レベルにアソシエートされたトラフィックでは A-MPDU 送信が使用されます。**disable** コマンドを使用する場合は、その優先レベルにアソシエートされたトラフィックでは A-MSDU 送信が使用されます。クライアントに使用される集約方法に適合するように優先レベルを設定してください。デフォルトでは、5 と 6 以外のすべての優先レベルが有効になっています。

c. ネットワークを再度有効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} enable network

ステップ 5　変更を保存するには、次のコマンドを入力します。

save config

ステップ 6　802.11n アクセス ポイントのチャネル帯域幅を設定する手順は、次のとおりです。

a. ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

b. アクセス ポイントを無効にするには、次のコマンドを入力します。

config 802.11a disable *Cisco_AP*

c. アクセス ポイントのチャネルを設定するには、次のコマンドを入力します。

config 802.11a channel ap *Cisco_AP channel*

d. アクセス ポイントの送信電力レベルを設定するには、次のコマンドを入力します。

config 802.11a txpower ap *Cisco_AP power_level*

e. 802.11n をサポートするように設定されている無線のチャネル帯域幅を 20MHz から 40 MHz に変換するには、次のコマンドを入力します。

config 802.11a chan_width *Cisco_AP* {**20** | **40_ABOVE** | **40_BELOW**}

このとき、次のようになります。

- **20** は、デフォルトの 20MHz の帯域幅を指定します。このオプションを使用して、チャネル帯域幅を 40MHz から 20 MHz に戻すことができます。
- **40_ABOVE** は、上位の 20MHz 帯域のセカンダリ チャネルまたは拡張チャネルで 40MHz の帯域幅を指定します。2 つの 20MHz チャネルを組み合わせて、制御メッセージ用に使用される現在のチャネルの上のチャネルで無線ネットワークを作成します。
- **40_BELOW** は、下位の 20MHz 帯域のセカンダリ チャネルまたは拡張チャネルで 40MHz の帯域幅を指定します。2 つの 20MHz チャネルを組み合わせて、制御メッセージ用に使用される現在のチャネルの下のチャネルで無線ネットワークを作成します。

チャネル帯域幅を 20MHz から 40MHz に増やすことにより、無線ネットワークのスループットを向上させることができます。

(注) 802.11n アクセス ポイントは、デフォルトでは 20MHz で動作するように設定されています。40MHz で動作するように設定されている場合は、送信電力とチャネル割り当てが静的に有効でなければなりません。

(注) 40MHz のチャネル帯域幅を使用する場合は、チャネルは 2 つのペアでのみ組み合わせることができます。たとえば、使用できるチャネル 36、40、44、48、52、56、60、および 64 のうち、36 と 40、44 と 48、52 と 56、および 60 と 64 のペアのみが組み合わせ可能となります。802.11a 無線用の現在のチャネルが 40 に設定されており、チャネル帯域幅を ABOVE オプションで 40MHz に設定する場合、コントローラは、組み合わせを壊すことになるためこれを許可しません。BELOW オプションのみ使用可能です。ABOVE オプションを使用する場合は、802.11a 無線でチャネル 36 を使用するように設定する必要があります。

(注) チャネル帯域幅が 40MHz に設定されている場合に、コントローラの GUI 上のチャネル番号を、前述のようなチャネルの組み合わせを壊してしまう設定にしようとすると、エラー メッセージが表示され、チャネルは設定されません。

(注) 深刻な同一チャネル干渉が発生する可能性があるため、2.4GHz 無線では 40MHz チャネルは設定しないようお勧めします。

f. ネットワークを再度有効にするには、次のコマンドを入力します。

config 802.11a enable network

g. アクセス ポイントを再度有効にするには、次のコマンドを入力します。

config 802.11a enable *Cisco_AP*

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　802.11a/n または 802.11b/g/n 帯域の設定を表示するには、次のコマンドを入力します。

show {802.11a | 802.11b}

次のような情報が表示されます。

```
802.11a Network..............................  Enabled
11nSupport...................................  Enabled
      802.11a Low Band.......................  Enabled
      802.11a Mid Band.......................  Enabled
      802.11a High Band......................  Enabled
802.11a Operational Rates
    802.11a 6M Rate..........................  Mandatory
    802.11a 9M Rate..........................  Supported
    802.11a 12M Rate.........................  Mandatory
    802.11a 18M Rate.........................  Supported
    802.11a 24M Rate.........................  Mandatory
    802.11a 36M Rate.........................  Supported
    802.11a 48M Rate.........................  Supported
    802.11a 54M Rate.........................  Supported
802.11n MCS Settings:
MCS 0........................................  Supported
    MCS 1....................................  Supported
    MCS 2....................................  Supported
    MCS 3....................................  Supported
    MCS 4....................................  Supported
    MCS 5....................................  Supported
   MCS 6.....................................  Supported
    MCS 7....................................  Supported
    MCS 8....................................  Supported
    MCS 9....................................  Supported
    MCS 10...................................  Supported
    MCS 11...................................  Supported
    MCS 12...................................  Supported
    MCS 13...................................  Supported
    MCS 14...................................  Supported
  MCS 15.....................................  Supported
802.11n Status:
    A-MPDU Tx ...............................  Enabled
        Priority 0...........................  Enabled
        Priority 1...........................  Enabled
        Priority 2...........................  Enabled
        Priority 3...........................  Enabled
        Priority 4...........................  Enabled
        Priority 5...........................  Disabled
        Priority 6...........................  Disabled
        Priority 7...........................  Enabled
    A-MSDU Tx ...............................  Enabled
     Rifs Tx ................................  Enabled
    Guard Interval ..........................  Short
Beacon Interval..............................  100
CF Pollable mandatory........................  Disabled
CF Poll Request mandatory....................  Disabled
CFP Period...................................  4
CFP Maximum Duration.........................  60
Default Channel..............................  36
Default Tx Power Level.......................  1
DTPC Status..................................Enabled
Fragmentation Threshold......................  2346
Long Retry Limit.............................  4
Maximum Rx Life Time.........................  512
Max Tx MSDU Life Time........................  512
Medium Occupancy Limit.......................  100
```

```
Pico-Cell Status.............................. Disabled
Pico-Cell-V2 Status........................... Disabled
RTS Threshold................................. 2347
Short Retry Limit............................. 7
TI Threshold.................................. -50
Traffic Stream Metrics Status................. Enabled
Expedited BW Request Status................... Disabled
EDCA profile type............................. default-wmm
Voice MAC optimization status................. Disabled
Call Admission Control (CAC) configuration
   Voice AC - Admission control (ACM)............ Enabled
   Voice max RF bandwidth....................... 75
   Voice reserved roaming bandwidth.............. 6
   Voice load-based CAC mode..................... Disabled
   Voice tspec inactivity timeout................ Disabled
   Video AC - Admission control (ACM)............ Enabled
   Voice Stream-Size............................. 84000
   Voice Max-Streams............................. 2
   Video max RF bandwidth........................ Infinite
   Video reserved roaming bandwidth........... 0
```

DHCP プロキシの設定

DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。そのため、少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。

DHCP プロキシがコントローラ上で無効になっている場合は、クライアントとの間で送受信されるそれらの DHCP パケットは、パケットの IP 部分が変更されることなくコントローラによってブリッジされます。クライアントから受信したパケットは LWAPP トンネルから削除され、上流 VLAN 上で送信されます。クライアントへダイレクトされる DHCP パケットは、上流 VLAN 上で受信され、802.11 に変換され、LWAPP トンネルを使用してクライアントへ送信されます。したがって、DHCP プロキシが無効になっている場合は、内部 DHCP サーバは使用できません。DHCP プロキシを無効にする機能により、シスコのネイティブ プロキシ モードの動作をサポートしない DHCP サーバを使用するように構成できます。既存のインフラストラクチャによって必要とされる場合のみ、無効にするようにしてください。

コントローラの CLI を使用して、WLAN ベースではなくグローバル ベースで DHCP プロキシを有効または無効にできます。DHCP プロキシは、デフォルトで有効になっています。

（注） 通信するすべてのコントローラの DHCP プロキシ設定は同じでなければなりません。

（注） DHCP サーバの設定方法については、第 6 章を参照してください。

CLI を使用した DHCP プロキシの設定

コントローラの CLI を使用して DHCP プロキシを設定する手順は、次のとおりです。

ステップ 1　DHCP プロキシを有効または無効にするには、次のコマンドを入力します。

config dhcp proxy {**enable** | **disable**}

ステップ 2　DHCP プロキシの設定を表示するには、次のコマンドを入力します。

show dhcp proxy

次のような情報が表示されます。

```
DHCP Proxy Behavior: enabled
```

管理者のユーザ名とパスワードの設定

（注） コントローラには、パスワード リカバリ メカニズムがありません。WCS を使用してコントローラを管理する場合、コントローラ自体にログインしなくても、WCS からコントローラにアクセスして、新しい admin ユーザを作成できます。ユーザを削除した後、コントローラで設定を保存しなかった場合、コントローラをリブート（パワー サイクリング）すると、削除済みのユーザがまだシステムに存在する状態で、コントローラが起動されます。デフォルトの admin アカウントまたはログオンできる別のユーザ アカウントがない場合、コントローラを工場出荷時のデフォルト設定に戻して、最初から再度設定を行います。または、以前に保存した設定をリロードします。

不正ユーザによるコントローラの再設定や設定情報の閲覧を防止するために、管理者のユーザ名とパスワードを設定することができます。

読み取りと書き込み権限を持つユーザ名とパスワードのペアを作成するには、CLI で **config mgmtuser add** *username password* **read-write** と入力します。読み取り専用権限を持つユーザ名とパスワードのペアを作成するには、CLI で **config mgmtuser add** *username password* **read-only** と入力します。ユーザ名とパスワードは大文字と小文字が区別されます。いずれも、最大 24 文字の ASCII 文字列を使用できます。ユーザ名とパスワードにスペースを使用することはできません。

既存のユーザ名のパスワードを変更するには、**config mgmtuser password** *username new_password* と入力します。

設定済みのユーザの一覧を表示するには、**show mgmtuser** と入力します。

SNMP の設定

GUI を使用してコントローラの SNMP を設定することをお勧めします。CLI を使用する手順は、次のとおりです。

ステップ 1　SNMP コミュニティ名を作成するには、**config snmp community create** *name* と入力します。

ステップ 2　SNMP コミュニティ名を削除するには、**config snmp community delete** *name* と入力します。

ステップ 3　読み取り専用権限を持つ SNMP コミュニティ名を設定するには、**config snmp community accessmode ro** *name* と入力します。読み取りと書き込み権限を持つ SNMP コミュニティ名を設定するには、**config snmp community accessmode rw** *name* と入力します。

ステップ 4　SNMP コミュニティの IP アドレスとサブネット マスクを設定するには、**config snmp community ipaddr** *ip-address ip-mask name* と入力します。

（注）　このコマンドは、SNMP アクセス リストのように動作します。デバイスが、アソシエートされたコミュニティ付きの SNMP パケットを受け入れる IP アドレスを指定します。要求元エンティティの IP アドレスは、その IP アドレスに比較される前にはサブネット マスク付きの ANDed となります。サブネット マスクが 0.0.0.0 に設定されている場合、IP アドレス 0.0.0.0 はすべての IP アドレスに一致します。デフォルト値は 0.0.0.0 です。

（注）　コントローラでは IP アドレス範囲を 1 つだけ使用して、SNMP コミュニティを管理できます。

ステップ 5　コミュニティ名を有効にするには、**config snmp community mode enable** と入力します。コミュニティ名を無効にするには **config snmp community mode disable** と入力します。

ステップ 6　トラップの宛先を設定するには、**config snmp trapreceiver create** *name ip-address* と入力します。

ステップ 7　トラップを削除するには、**config snmp trapreceiver delete** *name* と入力します。

ステップ 8　トラップの宛先を変更するには、**config snmp trapreceiver ipaddr** *old-ip-address name new-ip-address* と入力します。

ステップ 9　トラップを有効にするには、**config snmp trapreceiver mode enable** と入力します。トラップを無効にするには、**config snmp trapreceiver mode disable** と入力します。

ステップ 10　SNMP 接点の名前を設定するには、**config snmp syscontact** *syscontact-name* と入力します。接点の名前には、最大 31 文字の英数字を使用できます。

ステップ 11　SNMP システムの場所を設定するには、**config snmp syslocation** *syslocation-name* と入力します。場所の名前には、最大 31 文字の英数字を使用できます。

ステップ 12　**show snmpcommunity** コマンドおよび **show snmptrap** コマンドを使用して、SNMP トラップおよびコミュニティが正しく設定されていることを確認します。

ステップ 13　**show trapflags** コマンドを使用して、有効または無効にされたトラップフラグを確認します。必要に応じて、**config trapflags** コマンドを使用して、トラップフラグを有効または無効にします。

SNMP コミュニティ文字列のデフォルト値の変更

コントローラは、読み取りと書き込みの SNMP コミュニティ文字列に対して、「public」と「private」という一般的なデフォルト値を持ちます。これらの標準値を使用すると、セキュリティ上のリスクが発生します。したがって、これらの値を変更することを強くお勧めします。

GUI を使用した SNMP コミュニティ文字列のデフォルト値の変更

コントローラの GUI により SNMP コミュニティ文字列のデフォルト値を変更する手順は、次のとおりです。

ステップ 1　SNMP の下で、**Management**、**Communities** の順にクリックします。SNMP v1/v2c Community ページが表示されます（図 4-4 を参照）。

図 4-4　SNMP v1/v2c Community ページ

ステップ 2　Community Name カラムに「public」または「private」が表示される場合は、コミュニティの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** をクリックしてこのコミュニティを削除します。

ステップ 3　**New** をクリックして新しいコミュニティを作成します。SNMP v1/v2c Community > New ページが表示されます（図 4-5 を参照）。

図 4-5　SNMP v1/v2c Community > New ページ

ステップ 4　Community Name フィールドに、16 文字以内の英数字から成る一意の名前を入力します。「public」または「private」を入力しないでください。

ステップ 5　次の 2 つのフィールドには、このデバイスがアソシエートされたコミュニティ付きの SNMP パケットを受け入れる IP アドレスと IP マスクを指定します。

ステップ 6　Access Mode ドロップダウン ボックスから **Read Only** または **Read/Write** を選択して、このコミュニティのアクセス レベルを指定します。

ステップ 7　Status ドロップダウン ボックスから **Enable** または **Disable** を選択して、このコミュニティのステータスを指定します。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、設定を保存します。

ステップ 10　「public」コミュニティまたは「private」コミュニティが SNMP v1/v2c Community ページにまだ表示されている場合には、この手順を繰り返します。

CLI を使用した SNMP コミュニティ文字列のデフォルト値の変更

コントローラの CLI により SNMP コミュニティ文字列のデフォルト値を変更する手順は、次のとおりです。

ステップ 1　このコントローラに対する SNMP コミュニティの最新のリストを表示するには、次のコマンドを入力します。

show snmp community

ステップ 2　SNMP Community Name カラムに「public」または「private」が表示される場合、次のコマンドを入力してこのコミュニティを削除します。

config snmp community delete *name*

name パラメータがコミュニティ名です（この場合、「public」または「private」）。

ステップ 3　新しいコミュニティを作成するには、次のコマンドを入力します。

config snmp community create *name*

name パラメータに、16 文字以内の英数字を入力します。「public」または「private」を入力しないでください。

ステップ 4　このデバイスが、アソシエートされたコミュニティ付きの SNMP パケットを受け入れる IP アドレスを入力するには、次のコマンドを入力します。

config snmp community ipaddr *ip_address ip_mask name*

ステップ 5　このコミュニティのアクセス レベルを指定するには、次のコマンドを入力します。ここで、**ro** は読み取り専用モードで、**rw** は読み書きモードです。

config snmp community accessmode {***ro*** | ***rw***} *name*

ステップ 6　この SNMP コミュニティを有効または無効にするには、次のコマンドを入力します。

config snmp community mode {***enable*** | ***disable***} *name*

ステップ 7　変更を保存するには、**Save Configuration** と入力します。

ステップ 8　「public」または「private」コミュニティ文字列のデフォルト値をまだ変更する必要がある場合には、この手順を繰り返します。

SNMP v3 ユーザのデフォルト値の変更

コントローラは、ユーザ名、認証パスワードおよび SNMP v3 ユーザのプライバシー パスワード用に、デフォルト値の「default」を使用します。これらの標準値を使用すると、セキュリティ上のリスクが発生します。したがって、これらの値を変更することを強くお勧めします。

(注)　SNMP v3 は時間に依存しています。コントローラの時間および時間帯が正確に設定されていることを確認してください。

GUI を使用した SNMP v3 ユーザのデフォルト値の変更

コントローラの GUI により SNMP v3 ユーザのデフォルト値を変更する手順は、次のとおりです。

ステップ 1　**Management** > **SNMP** > **SNMP V3 Users** の順にクリックして、SNMP V3 Users ページを開きます（図 4-6 を参照）。

図 4-6　SNMP V3 Users ページ

ステップ 2　User Name カラムに「default」が表示される場合は、ユーザの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** をクリックしてこの SNMP v3 ユーザを削除します。

ステップ 3　**New** をクリックして新しい SNMP v3 ユーザを追加します。SNMP V3 Users > New ページが表示されます（図 4-7 を参照）。

図 4-7　SNMP V3 Users > New ページ

ステップ 4　User Profile Name フィールドに一意の名前を入力します。「default」を入力しないでください。

ステップ 5　Access Mode ドロップダウン ボックスから **Read Only** または **Read/Write** を選択して、このユーザのアクセス レベルを指定します。デフォルト値は Read Only です。

ステップ 6　Authentication Protocol ドロップダウン ボックスで、目的の認証方式を次のいずれかから選択します。**None**、**HMAC-MD5**（ハッシュ メッセージ認証コード - メッセージ ダイジェスト 5）、または **HMAC-SHA**（ハッシュ メッセージ認証コード - セキュア ハッシュ アルゴリズム）。デフォルト値は HMAC-SHA です。

ステップ 7　Auth Password フィールドと Confirm Auth Password フィールドに、認証に使用する共有秘密鍵を入力します。最低 12 文字の入力が必要です。

ステップ 8　Privacy Protocol ドロップダウン ボックスで、目的の暗号化方式を次のいずれかから選択します。**None**、**CBC-DES**（暗号ブロック連鎖 - デジタル暗号化規格）、または **CFB-AES-128**（暗号フィードバック モード - 高度暗号化規格 -128）。デフォルト値は CFB-AES-128 です。

（注）　CBC-DES 暗号化または CFB-AES-128 暗号化を設定するには、ステップ 6 で認証プロトコルとして HMAC-MD5 か HMAC-SHA を選択しておく必要があります。

ステップ 9　Priv Password フィールドと Confirm Priv Password フィールドに、暗号化に使用する共有秘密鍵を入力します。最低 12 文字の入力が必要です。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、設定を保存します。

CLI を使用した SNMP v3 ユーザのデフォルト値の変更

コントローラの CLI により SNMP v3 ユーザのデフォルト値を変更する手順は、次のとおりです。

ステップ 1　このコントローラに対する SNMP v3 ユーザの最新のリストを表示するには、次のコマンドを入力します。

show snmpv3user

ステップ 2　SNMP v3 User Name カラムに「default」が表示される場合、次のコマンドを入力してこのユーザを削除します。

config snmp v3user delete ***username***

username パラメータが SNMP v3 ユーザ名です（この場合、「default」）。

ステップ 3　新しい SNMP v3 ユーザを作成するには、次のコマンドを入力します。

config snmp v3user create *username* {***ro*** | ***rw***} {***none*** | ***hmacmd5*** | ***hmacsha***} {***none*** | ***des*** | ***aescfb128***} *auth_key encrypt_key*

このとき、次のようになります。

- *username* は、SNMP v3 ユーザ名です。
- **ro** は読み取り専用モード、**rw** は読み書きモードです。
- ***none***、***hmacmd5***、および ***hmacsha*** は、認証プロトコル オプションです。
- **none**、**des**、および **aescfb128** は、プライバシー プロトコル オプションです。
- *auth_key* は、認証用の共有秘密鍵です。
- *encrypt_key* は、暗号化用の共有秘密鍵です。

username、*auth_key*、および *encrypt_key* パラメータに「default」と入力しないでください。

ステップ 4　変更を保存するには、**Save Configuration** と入力します。

アグレッシブなロード バランシングの設定

コントローラでアグレッシブなロード バランシングを有効にすると、LWAPP システムのアクセス ポイント全体にわたって、Lightweight アクセス ポイントで無線クライアントのロード バランシングを実現できます。アグレッシブなロード バランシングを有効にするには、コントローラ GUI または CLI を使用します。

無線クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットがステータス コード 17 の 802.11 応答パケットとともにクライアントに送信されます。このコードは、アクセス ポイントがビジー状態のため、これ以上アソシエーションを承認できないことを示しています。クライアントは次に、別のアクセス ポイントへのアソシエートを試みます。たとえば、ロード バランシングが有効になっていて、クライアント数が 5 クライアントに設定されている場合、6 つめのクライアントがアクセス ポイントへのアソシエートを試みると、クライアントはアクセス ポイントがビジー状態であることを示すステータス コード 17 の 802.11 応答パケットを受信します。

（注） コントローラとともに Cisco 7921 Wireless IP Phone や Cisco 7920 Wireless IP Phone を使用する場合、各コントローラでアグレッシブなロード バランシングが無効化されていることを確認します。無効化されていない場合、電話による初期ローミングが失敗し、オーディオ パスが中断されることがあります。

GUI を使用したアグレッシブなロード バランシングの設定

GUI を使用してアグレッシブなロード バランシングを設定する手順は、次のとおりです。

ステップ 1　**Controller** > **General** の順にクリックして、General ページを開きます。

ステップ 2　Aggressive Load Balancing ドロップダウン ボックスで、**Enabled** または **Disabled** を選択してこの機能を設定します。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用したアグレッシブなロード バランシングの設定

CLI を使用してアグレッシブなロード バランシングを設定する手順は、次のとおりです。

ステップ 1　アグレッシブなロード バランシングを有効または無効にするには、次のコマンドを入力します。

config load-balancing status {**enable** | **disable**}

ステップ 2　アグレッシブなロード バランシングのクライアント数を設定するには、次のコマンドを入力します。

config load-balancing window *clients*

clients パラメータには、0 ～ 20 の値を入力できます。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　設定を確認するには、次のコマンドを入力します。

show load-balancing

次のような情報が表示されます。

```
Aggressive Load Balancing..................... Enabled
Aggressive Load Balancing Window.............. 5 clients
```

802.3X のフロー制御の有効化

802.3X のフロー制御は、デフォルトでは無効にされています。有効にするには、**config switchconfig flowcontrol enable** と入力します。

802.3 ブリッジの設定

コントローラでは、802.3 のフレームおよびそれらを使用するアプリケーションをサポートしています。このようなアプリケーションには、キャッシュ レジスタやキャッシュ レジスタ サーバなどがあります。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

802.3 のフレームのサポートにより、コントローラで、IP 上で実行していないアプリケーションに対して IP 以外のフレームをブリッジできます。この 802.3 Raw のフレーム フォーマットのみ、現在サポートされています。

```
+------------------+--------------------+----------------+-----------------------+

| Destination     | Source             | Total packet | Payload .....
| MAC address   | MAC address    | length          |

+------------------+--------------------+----------------+-----------------------
```

802.3 ブリッジは、ソフトウェア リリース 4.1 以降のコントローラ GUI またはソフトウェア リリース 4.0 以降のコントローラ CLI を使用して設定できます。

（注） Cisco Wireless Control System（WCS）を使用して 802.3 ブリッジを設定することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

GUI を使用した 802.3 ブリッジの設定

コントローラ GUI を使用して 802.3 ブリッジを設定する手順は、次のとおりです。

ステップ 1　**Controller** > **General** の順にクリックして、General ページを開きます（図 4-8 を参照）。

図 4-8　General ページ

ステップ 2　802.3 ブリッジをコントローラで有効にする場合は、802.3 Bridging ドロップダウン ボックスから **Enabled** を選択します。この機能を無効にする場合は、**Disabled** を選択します。デフォルト値は Disabled です。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した 802.3 ブリッジの設定

コントローラ CLI を使用して 802.3 ブリッジを設定する手順は、次のとおりです。

ステップ 1　すべての WLAN の 802.3 ブリッジの現在のステータスを表示するには、次のコマンドを入力します。

show network

ステップ 2　すべての WLAN でグローバルに 802.3 ブリッジを有効または無効にするには、次のコマンドを入力します。

config network 802.3-bridging {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 3　設定を保存するには、次のコマンドを入力します。

save config

マルチキャスト モードの設定

ネットワークでマルチキャストのパケットをサポートする場合は、コントローラで使用するマルチキャストの方法を設定できます。コントローラは次の 2 つのモードでマルチキャストを実行します。

- **ユニキャスト モード**：このモードでは、各マルチキャスト パケットが、コントローラにアソシエートする各アクセス ポイントにコントローラによってユニキャストされます。このモードは非効率的ですが、マルチキャストをサポートしないネットワークでは必要な場合があります。
- **マルチキャスト モード**：このモードでは、コントローラによってマルチキャスト パケットが LWAPP マルチキャスト グループへ送信されます。この方法では、コントローラ プロセッサのオーバーヘッドを軽減して、パケット レプリケーションの作業をネットワークに移動させます。これは、ユニキャストを使った方法より、はるかに効率的です。

マルチキャスト モードを有効にするには、コントローラ GUI または CLI を使用します。

マルチキャスト モードについて

マルチキャスト モードが有効な場合に、コントローラがマルチキャスト パケットを有線 LAN から受信すると、コントローラは LWAPP を使用してパケットをカプセル化し、LWAPP マルチキャスト グループ アドレスへ転送します。コントローラは、必ず管理インターフェイスを使用してマルチキャスト パケットを送信します。マルチキャスト グループのアクセス ポイントはパケットを受け取り、クライアントがマルチキャスト トラフィックを受信するインターフェイスにマップされたすべての BSSID にこれを転送します。アクセス ポイントからは、マルチキャストはすべての SSID に対するブロードキャストのように見えます。

コントローラ ソフトウェア リリース 4.2 以降では、マルチキャスト パケットのダイレクトを向上させるために、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）のスヌーピングを導入しています。この機能が有効になっている場合、コントローラは IGMP レポートをクライアントから収集して処理し、レイヤ 3 マルチキャスト アドレスと VLAN 番号をチェックした後に IGMP レポートから一意な Multicast Group ID（MGID; マルチキャスト グループ ID）を作成し、その IGMP レポートをインフラストラクチャ スイッチへ送信します。コントローラは、クライアントからレポートを受信したインターフェイス アドレスとして、送信元アドレスを持つそれらのレポートを送信します。その上で、コントローラは、アクセス ポイント上でクライアント MAC アドレスを使用してアクセス ポイントの MGID テーブルを更新します。コントローラが特定のマルチキャスト グループのマルチキャスト トラフィックを受信した場合、それをすべてのアクセス ポイントに転送します。ただし、アクティブなクライアントでリッスンしているアクセス ポイント、またはそのマルチキャスト グループへ加入しているアクセス ポイントだけは、その特定の WLAN 上でマルチキャスト トラフィックを送信します。IP パケットは、入力 VLAN および宛先マルチキャスト グループの一意の MGID を使用して転送されます。レイヤ 2 マルチキャスト パケットは、入力インターフェイスの一意の MGID を使用して転送されます。

（注） IGMP スヌーピングは、2100 シリーズ コントローラ、および Cisco サービス統合型ルータの Cisco Wireless LAN Controller Network Module ではサポートされていません。

IGMP スヌーピングが無効になっている場合は、次のようになります。

- コントローラは、マルチキャスト　データをアクセス　ポイントへ送信する際は必ずレイヤ　2 MGID を使用します。作成された各インターフェイスは、1 つのレイヤ 2 MGID を割り当てられます。たとえば、管理インターフェイスの MGID は 0 となります。また、作成された 1 つ目の動的インターフェイスに割り当てられる MGID は 8 となり、動的インターフェイスが作成されるにつれて 1 増えます。
- クライアントからの IGMP パケットはルータへ転送されます。それにより、ルータの IGMP テーブルは、最後のレポータとしてクライアントの IP アドレスで更新されます。

IGMP スヌーピングが有効になっている場合は、次のようになります。

- コントローラは、アクセス ポイントへ送信されるすべてのレイヤ 3 マルチキャスト トラフィックに必ずレイヤ 3 MGID を使用します。すべてのレイヤ 2 マルチキャスト トラフィックについては、引き続き レイヤ 2 MGID を使用します。
- 無線クライアントからの IGMP レポート パケットは、クライアントに対するクエリを生成するコントローラによって消費または吸収されます。ルータによって IGMP クエリが送信されると、コントローラによって、マルチキャスト グループのリスナー IP アドレスとしてインターフェイス IP アドレスを持つ IGMP レポートが送信されます。それにより、ルータの IGMP テーブルは、マルチキャスト リスナーとしてコントローラ IP アドレスで更新されます。
- マルチキャスト　グループをリッスンしているクライアントであるコントローラから別のコントローラへローミングされる場合は、リッスンしているクライアント用のすべてのマルチキャスト グループ情報が、1 番目のコントローラから 2 番目のコントローラへ送信されます。それにより、2 番目のコントローラでは、クライアント用のマルチキャスト グループ情報を直ちに作成できます。2 番目のコントローラでは、クライアントがリッスンしていた全マルチキャスト グループのネットワークに IGMP レポートが送信されます。このプロセスは、クライアントへのマルチキャスト データのシームレスな転送に役立ちます。
- リッスンしているクライアントによって別のサブネットのコントローラにローミングされる場合は、マルチキャスト パケットは、Reverse Path Filtering（RPF; 逆方向パス転送）のチェックを避けるために、クライアントのアンカー コントローラへトンネリングされます。アンカーは、マルチキャスト パケットをインフラストラクチャ スイッチへ転送します。

（注） MGID はコントローラ固有です。2 つの異なるコントローラの同一 VLAN から送られて来る同一マルチキャスト グループのパケットは、2 つの異なる MGID へマップされる可能性があります。

（注） レイヤ 2 マルチキャストが有効になっている場合は、単一の MGID が、1 つのインターフェイスから送られてくるすべてのマルチキャスト アドレスへ割り当てられます（図 4-11 を参照）。

マルチキャスト モードを使用する場合の注意点

ネットワークでマルチキャスト モードを有効にする場合は、以下の点に注意してください。

- Cisco Unified Wireless Network ソリューションでは、特定の目的に対して次の IP アドレス範囲を使用します。マルチキャスト グループを設定する場合は、この範囲を覚えておいてください。
  - 224.0.0.0 ～ 224.0.0.255：予約済みリンクのローカル アドレス
  - 224.0.1.0 ～ 238.255.255.255：グローバル スコープのアドレス
  - 239.0.0.0 ～ 239.255.x.y /16：限定スコープのアドレス
- コントローラのマルチキャスト モードを有効にする場合は、LWAPP マルチキャスト グループ アドレスも設定する必要があります。アクセス ポイントは、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）を使用する LWAPP マルチキャスト グループに加入します。

- Cisco アクセス ポイント 1100、1130、1200、1230、および 1240 は、IGMP バージョン 1、2、および 3 を使用します。
- マルチキャスト モードは、レイヤ 3 の LWAPP モードでのみ動作します。
- Monitor モード、Sniffer モード、または Rogue Detector モードのアクセス ポイントは、LWAPP マルチキャスト グループ アドレスには加入しません。
- コントローラ上で設定されている LWAPP マルチキャスト グループは、コントローラが異なっていれば別のものでなければなりません。
- ネットワークで複数のコントローラを使用する場合は、すべてのコントローラで同じマルチキャスト アドレスが設定されていることを確認してください。
- マルチキャスト モードは、ゲスト トンネリングなどのサブネット間のモビリティ イベントでは動作しません。ただし、RADIUS を使用したインターフェイスの上書き（IGMP スヌーピングが有効になっている場合のみ）またはサイト専用の VLAN（アクセス ポイント グループ VLAN）では動作します。
- コントローラでは、UDP ポート番号 12222、12223、および 12224 へ送信されるマルチキャスト パケットはドロップされます。したがって、これらのポート番号をネットワーク上のマルチキャスト アプリケーションで使用しないように検討してください。
- ネットワーク上のマルチキャスト アプリケーションでは、コントローラで LWAPP マルチキャスト グループ アドレスとして設定されたマルチキャスト アドレスを使用しないようにお勧めします。

GUI を使用したマルチキャスト モードの有効化

コントローラの GUI を使用してマルチキャスト モードを有効にする手順は、次のとおりです。

ステップ 1　**Controller** をクリックして、General ページを開きます（図 4-9 を参照）。

図 4-9　General ページ

ステップ 2　Ethernet Multicast Mode ドロップダウン ボックスで、次のいずれかのオプションを選択します。

- **Disabled**：コントローラでのマルチキャストを無効にします。これはデフォルト値です。
- **Unicast**：ユニキャストを使用するコントローラを設定して、マルチキャスト　パケットを送信します。
- **Multicast**：マルチキャストを使用するコントローラを設定して、マルチキャスト　パケットを LWAPP マルチキャスト グループに送信します。

（注）　Hybrid REAP では、ユニキャスト モードのみがサポートされています。

ステップ 3　ステップ 2 で Multicast を選択した場合は、Multicast Group Address フィールドにマルチキャスト グループの IP アドレスを入力します。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　**Multicast** をクリックして、Multicast ページを開きます（図 4-10 を参照。）

図 4-10　Multicast ページ

ステップ 6　IGMP スヌーピングを有効にするには、**Enable IGMP Snooping** チェックボックスをオンにします。IGMP スヌーピングを無効にするには、チェックボックスをオフのままにします。デフォルト値は無効（disable）です。

ステップ 7　IGMP のタイムアウトを設定するには、30 ～ 300 秒の値を **IGMP Timeout** フィールドに入力します。特定のマルチキャスト グループに対してクライアントが存在するかどうかを確認するために、コントローラから、1 つのタイムアウト値につき 3 つのクエリが *timeout*/3 の間隔で送信されます。コントローラがクライアントからの IGMP レポートを使用して応答を受信しない場合、そのコントローラでは、MGID テーブルのそのクライアントのエントリがタイムアウトになります。特定のマルチキャスト グループに対してクライアントが残っていない場合は、コントローラは IGMP のタイムアウト値が期限切れになるまで待機し、コントローラからその MGID エントリを削除します。一般的な IGMP クエリ（つまり、宛先アドレス 224.0.0.1）がコントローラによって必ず生成され、MGID 値 1 を使用してすべての WLAN 上で送信されます。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更を保存します。

GUI を使用したマルチキャスト グループの表示

コントローラの GUI を使用してマルチキャスト グループを表示する手順は、次のとおりです。

ステップ 1　**Monitor** > **Multicast** の順にクリックします。Multicast Groups ページが表示されます（図4-11 を参照）。

図 4-11　Multicast Groups ページ

このページには、すべてのマルチキャスト グループとそれらに対応する MGID が表示されます。

ステップ 2　特定の MGID（MGID 550 など）のリンクをクリックして、その特定の MGID のマルチキャスト グループに接続されているすべてのクライアントの一覧を表示します。

CLI を使用したマルチキャスト モードの有効化

コントローラの CLI を使用してマルチキャスト モードを有効にする手順は、次のとおりです。

ステップ 1　コントローラ上でマルチキャストを有効または無効にするには、次のコマンドを入力します。

config network multicast global {**enable** | **disable**}

デフォルト値は無効（disable）です。

（注）　**config network broadcast** {**enable** | **disable**} コマンドを使用すると、マルチキャストを同時に有効または無効にしなくても、ブロードキャストを有効または無効にすることができます。このコマンドは、現在コントローラで使用されているマルチキャスト モードを使用して動作します。

ステップ 2　次のいずれかの操作を行います。

a.　ユニキャストを使用してマルチキャスト　パケットを送信するようにコントローラを設定するには、次のコマンドを入力します。

config network multicast mode unicast

b. マルチキャストを使用してマルチキャスト パケットを LWAPP マルチキャスト グループに送信するようにコントローラを設定するには、次のコマンドを入力します。

config network multicast mode multicast *multicast_group_ip_address*

ステップ 3　IGMP スヌーピングを有効または無効にするには、次のコマンドを入力します。

config network multicast igmp snooping {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 4　IGMP のタイムアウト値を設定するには、次のコマンドを入力します。

config network multicast igmp timeout *timeout*

timeout には、30 ～ 300 秒の値を入力できます。特定のマルチキャスト グループに対してクライアントが存在するかどうかを確認するために、コントローラから、1 つのタイムアウト値につき 3 つのクエリが *timeout*/3 の間隔で送信されます。コントローラがクライアントからの IGMP レポートを使用して応答を受信しない場合、そのコントローラでは、MGID テーブルのそのクライアントのエントリがタイムアウトになります。特定のマルチキャスト グループに対してクライアントが残っていない場合は、コントローラは IGMP のタイムアウト値が期限切れになるまで待機し、コントローラからその MGID エントリを削除します。一般的な IGMP クエリ（つまり、宛先アドレス 224.0.0.1）がコントローラによって必ず生成され、MGID 値 1 を使用してすべての WLAN 上で送信されます。

ステップ 5　変更を保存するには、次のコマンドを入力します。

save config

CLI を使用したマルチキャスト グループの表示

コントローラ CLI を使用してマルチキャスト グループを表示するには、次のコマンドを使用します。

- すべてのマルチキャスト グループとそれらに対応する MGID を表示するには、次のコマンドを入力します。

  show network multicast mgid summary

  次のような情報が表示されます。

```
Layer2 MGID Mapping:
--------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       0        0
test                             0        9
wired                            20       8

Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs........................... 1

 Group address    Vlan  MGID
 ---------------  ----  ----
 239.255.255.250  0     550
```

- 特定の MGID でマルチキャスト グループに接続されているすべてのクライアントを表示するには、次のコマンドを入力します。

  show network multicast mgid detail *mgid_value*

  mgid_value パラメータは、550 ～ 4095 の数値です。

  次のような情報が表示されます。

```
Mgid..................................... 550
Multicast Group Address..................... 239.255.255.250
Vlan..................................... 0
Rx Packet Count.......................... 807399588
No of clients............................ 1
Client List.............................
        Client MAC             Expire Time (mm:ss)
        00:13:02:23:82:ad      0:20
```

クライアント ローミングの設定

Cisco UWN Solution は、同じコントローラで管理されている lightweight アクセス ポイント間、同一サブネット上の同じモビリティ グループに属しているコントローラ間、および異なるサブネット上の同じモビリティ グループに属しているコントローラ間において、シームレスなクライアント ローミングをサポートします。また、コントローラ ソフトウェア リリース 4.1 以降では、マルチキャスト パケットでのクライアント ローミングがサポートされています。

GUI または CLI を使用してデフォルトの RF 設定（RSSI、ヒステリシス、スキャンのしきい値、および遷移時間）を調整することで、クライアント ローミングの動作を微調整できます。

コントローラ内ローミング

すべてのコントローラは、同じコントローラで管理されているアクセス ポイント間での同一コントローラ クライアント ローミングをサポートします。セッションはそのまま持続され、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用するため、このローミングはクライアントには透過的に行われます。コントローラには、リレー機能を備えている DHCP 機能があります。同一コントローラ ローミングは、シングルコントローラ展開とマルチコントローラ展開でサポートされています。

コントローラ間ローミング

マルチコントローラ展開では、同一モビリティ グループ内および同一サブネット上のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングもクライアントには透過的に行われます。IP アドレス 0.0.0.0、または自動 IP アドレス 169.254.*.* のクライアントが DHCP Discover を送信するか、オペレータが設定したセッション時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

サブネット間ローミング

同様に、マルチコントローラ展開では、異なるサブネット上の同一モビリティ グループ内のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。IP アドレス 0.0.0.0、または自動 IP アドレス 169.254.*.* のクライアントが DHCP Discover を送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

VoIP による通話ローミング

802.11 voice-over-IP（VoIP）通話は、RF 信号が最も強いアソシエーションを見つけ出すことで、最適な QoS（Quality of Service）と最高のスループットを実現します。Cisco UWN Solution の平均ハンドオーバー遅延時間は 5 ミリ秒以下なので、オープン認証が使用されている場合、20 ミリ秒という最短の VoIP 通話要件や、ローミング ハンドオーバーの遅延時間の短縮は簡単に実現されます。この短い遅延時間は、個々のアクセス ポイントにローミング ハンドオーバーのネゴシエートを許可せずにコントローラによって制御されます。

Cisco UWN Solution では、コントローラが同一のモビリティ グループに属している場合、異なるサブネット上のコントローラによって管理される lightweight アクセス ポイント間での 802.11 VoIP 通話ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、VoIP 通話は同じ DHCP 割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。VoIP 通話 IP アドレス 0.0.0.0、または VoIP 通話自動 IP アドレス 169.254.*.* のクライアントが DHCP Discover を送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、VoIP クライアントの再認証が必要になります。

CCX レイヤ 2 クライアント ローミング

コントローラでは、次の 5 つの CCX レイヤ 2 クライアント ローミング拡張機能がサポートされています。

- **アクセス ポイント経由ローミング**：この機能により、クライアントはスキャン時間を節約できます。CCXv2 クライアントがアクセス ポイントにアソシエートする際、新しいアクセス ポイントに以前のアクセス ポイントの特徴をリストする情報パケットを送信します。各クライアントがアソシエートされていた以前のアクセス ポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセス ポイントをすべてまとめて作成したアクセス ポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセス ポイントのリストには、チャネル、クライアントの現在の SSID をサポートしているネイバー アクセス ポイントの BSSID、およびアソシエーション解除以来の経過時間が含まれています。
- **拡張ネイバー リスト**：この機能は、特に音声アプリケーションのサーバとなる際に、CCX v4 クライアントのローミング能力とネットワーク エッジ パフォーマンスの向上に重点をおいています。アクセス ポイントは、ネイバー リストのユニキャスト更新メッセージを使用して、アソシエートされたクライアントのネイバーに関する情報を提供します。
- **拡張ネイバー リスト要求（E2E）**：End-2-End 仕様は、音声 / ローミング能力の全体的向上のために新しいプロトコルとインターフェイスを定義する、Cisco と Intel の共同プログラムです。これは、CCX 環境の Intel クライアントにのみ適用されます。これにより、Intel クライアントは自由にネイバー リストを要求できるようになります。要求すると、アクセス ポイントはコントローラに要求を転送します。コントローラは要求を受信し、クライアントがアソシエートされているアクセス ポイントに対するネイバーの現在の CCX ローミング サブリストで応答します。

（注） 特定のクライアントが　E2E　をサポートするかどうか確認するには、コントローラの GUI で **Wireless** > **Clients** をクリックし、必要なクライアントの **Detail** リンクをクリックして、Client Properties の下の E2E Version フィールドを確認します。

- **ローミング理由レポート**：この機能により、CCXv4 クライアントは新しいアクセス ポイントにローミングした理由を報告できます。また、ネットワーク管理者はローミング履歴を作成および監視できるようになります。
- **ダイレクトされたローミング要求**：この機能を使用すると、割り当てられているアクセス ポイントとは別のアクセス ポイントの方がクライアントにより優れたサービスを提供できる場合、コントローラはダイレクトされたローミング要求をクライアントに送信できるようになります。この場合、コントローラはクライアントに接続できる最適なアクセス ポイントの一覧を送信します。クライアントはダイレクトされたローミング要求を受け入れることも、無視することもできます。CCX 以外のクライアントおよび CCXv3 以下を実行するクライアントは、どちらの操作も行う必要がありません。この機能を使用するために設定する必要はありません。

コントローラ ソフトウェア リリース 4.2 以降では、CCX バージョン 1 ～ 5 をサポートしています。CCX のサポートは、コントローラ上のすべての WLAN に対して自動的に有効になり、無効にすることはできません。コントローラは、クライアント データベースにクライアントの CCX バージョンを格納し、CCX フレームを生成し、CCX フレームに応答するためにこれを使用します。これらのローミング拡張機能を使用するには、クライアントで CCXv4 か CCXv5（または、アクセス ポイント経由ローミングの場合 CCXv2）がサポートされている必要があります。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

上記に説明するローミング拡張機能は、適切な CCX サポートで自動的に有効化されます。

（注） スタンドアロン モードでの Hybrid-REAP アクセス ポイントでは、CCX レイヤ 2 ローミングはサポートされません。

GUI を使用した CCX クライアント ローミング パラメータの設定

GUI を使用して CCX クライアント ローミング パラメータを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n**（または **802.11b/g/n**）> **Client Roaming** の順にクリックします。802.11a（または 802.11b）> Client Roaming ページが表示されます（図 4-12 を参照）。

図 4-12　802.11a > Client Roaming ページ

ステップ 2　クライアント ローミングに影響を与える RF パラメータを微調整する場合、Mode ドロップダウン ボックスから **Custom** を選択し、ステップ 3 に進みます。RF パラメータをデフォルト値のままにする場合は、**Default** を選択して、ステップ 8 に進みます。

ステップ 3　Minimum RSSI フィールドに、クライアントがアクセス ポイントにアソシエートするために必要な最小の Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）の値を入力します。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。

範囲：-80 ～ -90dBm

デフォルト：-85 dBm

ステップ 4　Hysteresis フィールドに、クライアントがローミングするために必要な近隣のアクセス ポイントの信号強度を示す値を入力します。このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。

範囲：2 ～ 4dB

デフォルト：2dB

ステップ 5　Scan Threshold フィールドに、最小 RSSI を入力します。このしきい値を超えると、クライアントはより適切なアクセス ポイントへのローミングが必要になります。RSSI が指定した値を下回ったときに、クライアントは指定された遷移時間内でより適切なアクセス ポイントにローミングできる必要があります。このパラメータはまた、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

範囲：-70 ～ -77dBm

デフォルト：-72dBm

ステップ 6　Transition Time フィールドに、クライアントのアソシエートされたアクセス ポイントからの RSSI がスキャンのしきい値より低くなった場合に、クライアントがローミングに適した近隣のアクセス ポイントの検出にかけられる最大許容時間を入力します。

Scan Threshold パラメータと Transition Time パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、きわめて高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

範囲：1 ～ 10 秒

デフォルト：5 秒

ステップ 7　**Apply** をクリックして、変更を適用します。

ステップ 8　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 9　別の無線帯域（802.11a または 802.11b/g）についてクライアント ローミングの設定をする場合、この手順を繰り返します。

CLI を使用した CCX クライアント ローミング パラメータの設定

CCX レイヤ 2 クライアント ローミング パラメータを設定するには、次のコマンドを入力します。

config {**802.11a** | **802.11bg**} **l2roam rf-params min-rssi** *rssi_value* **roam-hyst** *hyst_value* **scan-thres** *thres_value* **trans-time** *time_value*

（注）　各 RF パラメータの説明、範囲およびデフォルト値については、「GUI を使用した CCX クライアント ローミング パラメータの設定」の項（P. 4-48）を参照してください。

CLI を使用した CCX クライアント ローミング情報の取得

次のコマンドを使用して、CCX レイヤ 2 クライアント ローミングに関する情報を表示します。

1. 802.11a または 802.11b/g ネットワークのクライアント ローミングに対して設定されている現在の RF パラメータを表示するには、次のコマンドを入力します。

   show {**802.11a** | **802.11b**} **l2roam rf-params**

2. 特定のアクセス ポイントに対する CCX レイヤ 2 クライアント ローミング統計を表示するには、次のコマンドを入力します。

   show {**802.11a** | **802.11b**} **l2roam statistics** *ap_mac*

   このコマンドは、次の情報を提供します。

   - 受信したローミング理由レポートの数
   - 受信したネイバー リスト要求の数
   - 送信したネイバー リスト レポートの数
   - 送信したブロードキャスト ネイバー更新の数

3. 特定のクライアントのローミング履歴を表示するには、次のコマンドを入力します。

   show client roam-history *client_mac*

   このコマンドは、次の情報を提供します。

   - レポートを受信した時刻
   - クライアントが現在アソシエートされているアクセス ポイントの MAC アドレス
   - クライアントが以前アソシエートされていたアクセス ポイントの MAC アドレス
   - クライアントが以前アソシエートされていたアクセス ポイントのチャネル
   - クライアントが以前アソシエートされていたアクセス ポイントの SSID
   - 以前のアクセス ポイントからクライアントがアソシエーション解除した時刻
   - クライアントがローミングする理由

CLI を使用した CCX クライアント ローミング問題のデバッグ

CCX レイヤ 2 クライアント ローミングで問題が発生した場合は、次のコマンドを入力します。

debug l2roam [**detail** | **error** | **packet** | **all]** {**enable** | **disable**}

Quality of Service の設定

Quality of Service（QoS; サービス品質）とは、選択したネットワーク トラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッタおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

コントローラでは次の 4 つの QoS レベルがサポートされています。

- Platinum/Voice：無線の音声用に高品質なサービスを確保します。
- Gold/Video：高品質なビデオ アプリケーションをサポートします。
- Silver/Best Effort：クライアント用に通常の帯域幅をサポートします。これはデフォルト設定です。
- Bronze/Background：ゲスト サービス用に最低帯域幅を提供します。

VoIP クライアントは Platinum、Gold、または Silver に設定する必要がありますが、低帯域幅のクライアントは Bronze に設定することができます。

QoS プロファイルを使用して各 QoS レベルの帯域幅を設定してから、そのプロファイルを WLAN に適用できます。プロファイル設定は、その WLAN にアソシエートされたクライアントに組み込まれます。また、QoS ロールを作成して、通常ユーザとゲスト ユーザに異なる帯域幅レベルを指定できます。QoS プロファイルと QoS ロールを設定するには、この項の手順に従ってください。

Quality of Service プロファイルの設定

Platinum、Gold、Silver、および Bronze QoS プロファイルを有効にするには、コントローラ GUI または CLI を使用します。

GUI を使用した QoS プロファイルの設定

コントローラの GUI を使用して QoS プロファイルを設定する手順は、次のとおりです。

ステップ 1　QoS プロファイルを設定できるように、802.11a および 802.11b/g ネットワークを無効にします。

無線ネットワークを無効にするには、**Wireless > 802.11a/n** または **802.11b/g/n > Network** の順にクリックし、**802.11a (** または **802.11b/g) Network Status** チェックボックスをオフにして、**Apply** をクリックします。

ステップ 2　**Wireless** > **QoS** > **Profiles** の順にクリックして、QoS Profiles ページを開きます。

ステップ 3　設定するプロファイルの名前をクリックして、Edit QoS Profile ページを開きます（図 4-13 を参照）。

図 4-13　Edit QoS Profile ページ

ステップ 4　プロファイルの説明を変更するには、Description フィールドの内容を変更します。

ステップ 5　ユーザごとの TCP トラフィックの平均データ レートを定義するには、Average Data Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、プロファイルに帯域幅の制限を課しません。

ステップ 6　ユーザごとの TCP トラフィックのピーク データ レートを定義するには、Burst Data Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、プロファイルに帯域幅の制限を課しません。

（注）　Burst Data Rate は Average Data Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

ステップ 7　ユーザごとの UDP トラフィックの平均リアルタイム レートを定義するには、Average Real-Time Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、プロファイルに帯域幅の制限を課しません。

ステップ 8　ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義するには、Burst Real-Time Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、プロファイルに帯域幅の制限を課しません。

（注）　Burst Real-Time Rate は Average Real-Time Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

ステップ 9　Maximum RF Usage Per AP フィールドに、ユーザ クラスに与えられている最大帯域幅の割合を入力します。

たとえば、Bronze QoS に 50% を設定する場合、すべての Bronze WLAN ユーザを合わせても、利用可能な RF 帯域幅の 50% 以上を取得できません。実際のスループットは、50% 未満の可能性がありますが、50% を超えることはありません。

ステップ 10　Queue Depth フィールドに、アクセス ポイントがキューに保持するパケットの最大数を入力します。余分なパケットはドロップされます。

ステップ 11　プロファイル内に当てはまるパケットにアソシエートされた優先タグの最大値（0 ～ 7）を定義するには、Protocol Type ドロップダウン ボックスから **802.1p** を選択し、802.1p Tag フィールドに最大優先値を入力します。

タグ付きパケットには、LWAPP データ パケット（アクセス ポイントとコントローラ間）およびコア ネットワークに向けて送信されたパケットが含まれます。

ステップ 12　**Apply** をクリックして、変更を適用します。

ステップ 13　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 14　802.11a および 802.11b/g ネットワークを再度有効にします。

無線ネットワークを有効にするには、**Wireless** > **802.11a/n** または **802.11b/g/n** > **Network** の順にクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオンにして、**Apply** をクリックします。

ステップ 15　QoS プロファイルを WLAN に割り当てるには、「WLAN への QoS プロファイルの割り当て」の項（P. 6-29）の手順に従ってください。

CLI を使用した QoS プロファイルの設定

CLI を使用して Platinum、Gold、Silver、および Bronze QoS プロファイルを設定する手順は、次のとおりです。

ステップ 1　QoS プロファイルを設定できるように、802.11a および 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

config 802.11b disable network

ステップ 2　プロファイルの説明を変更するには、次のコマンドを入力します。

config qos description {bronze | silver | gold | platinum} *description*

ステップ 3　ユーザごとに TCP トラフィックの平均データ レートを Kbps 単位で定義するには、次のコマンドを入力します。

config qos average-data-rate {bronze | silver | gold | platinum} *rate*

（注） *rate* パラメータには、0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS プロファイルに帯域幅の制限を課しません。

ステップ 4　ユーザごとに TCP トラフィックのピーク データ レートを Kbps 単位で定義するには、次のコマンドを入力します。

config qos burst-data-rate {bronze | silver | gold | platinum} *rate*

ステップ 5　ユーザごとに UDP トラフィックの平均リアルタイム レートを Kbps 単位で定義するには、次のコマンドを入力します。

config qos average-realtime-rate {bronze | silver | gold | platinum} *rate*

ステップ 6　ユーザごとに UDP トラフィックのピーク リアルタイム レートを Kbps 単位で定義するには、次のコマンドを入力します。

config qos burst-realtime-rate {bronze | silver | gold | platinum} *rate*

ステップ 7　アクセス ポイントあたりの最大 RF 使用量の割合を指定するには、次のコマンドを入力します。

config qos max-rf-usage {bronze | silver | gold | platinum} *usage_percentage*

ステップ 8　アクセス ポイントがキューに保持するパケットの最大数を指定するには、次のコマンドを入力します。

config qos queue_length {bronze | silver | gold | platinum} *queue_length*

ステップ 9　プロファイル内に当てはまるパケットにアソシエートされた優先タグの最大値（0 ～ 7）を定義するには、次のコマンドを入力します。

config qos **protocol-type** ***{bronze | silver | gold | platinum} dot1p***

config qos dot1p-tag {bronze | silver | gold | platinum} *tag*

ステップ 10　QoS プロファイルを設定できるように、802.11a および 802.11b/g ネットワークを再度有効にするには、次のコマンドを入力します。

config 802.11a enable network

config 802.11b enable network

ステップ 11　QoS プロファイルを WLAN に割り当てるには、「WLAN への QoS プロファイルの割り当て」の項（P. 6-29）の手順に従ってください。

Quality of Service ロールの設定

QoS プロファイルを設定して WLAN に適用すると、その WLAN にアソシエートされたクライアントの帯域幅レベルが制限されます。複数の WLAN を同じ QoS プロファイルにマップできますが、通常ユーザ（従業員など）とゲスト ユーザの間で帯域幅のコンテンションが発生する可能性があります。ゲスト ユーザが通常ユーザと同じレベルの帯域幅を使用しないようにするには、異なる帯域幅コントラクト（恐らく下位）で QoS ロールを作成して、ゲスト ユーザに割り当てます。

コントローラの GUI または CLI を使用して、ゲスト ユーザ用に最大 10 個の QoS ロールを設定できます。

（注） RADIUS サーバ上にゲスト ユーザ用のエントリを作成するように選択し、ゲスト ユーザをコントローラからローカル ユーザ データベースに追加するのではなく、Web 認証が実行される WLAN に対して RADIUS 認証を 有効にする場合は、QoS ロールをその RADIUS サーバ自体に割り当てる必要があります。そのためには、「guest-role」Airespace 属性を、データ型「string」、戻り値「11」で RADIUS サーバに追加する必要があります。この属性は、認証の際にコントローラへ送信されます。RADIUS サーバから返された名前付きのロールがコントローラ上で設定されていることが判明した場合は、認証が正常に完了した後に、そのロールへアソシエートされた帯域幅がゲスト ユーザに対して強制されます。

GUI を使用した QoS ロールの設定

コントローラの GUI を使用して QoS ロールを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **QoS** > **Roles** の順にクリックして、QoS Roles for Guest Users ページを開きます（図 4-14 を参照）。

図 4-14　QoS Roles for Guest Users ページ

このページには、ゲスト ユーザ用の既存の QoS ロールが表示されます。

（注） QoS ロールを削除するには、そのロールの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　新しい QoS ロールを作成するには、**New** をクリックします。QoS Role Name > New ページが表示されます。

ステップ 3　Role Name フィールドに、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください（Contractor、Vendor、など）。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　QoS ロールの帯域幅を編集するには、QoS ロールの名前をクリックします。Edit QoS Role Data Rates ページが表示されます（図 4-15 を参照）。

図 4-15　Edit QoS Role Data Rates ページ

ステップ 6　ユーザごとの TCP トラフィックの平均データ レートを定義するには、Average Data Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS ロールに帯域幅の制限を課しません。

ステップ 7　ユーザごとの TCP トラフィックのピーク データ レートを定義するには、Burst Data Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS ロールに帯域幅の制限を課しません。

（注）　Burst Data Rate は Average Data Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

ステップ 8　ユーザごとの UDP トラフィックの平均リアルタイム レートを定義するには、Average Real-Time Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS ロールに帯域幅の制限を課しません。

ステップ 9　ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義するには、Burst Real-Time Rate フィールドに Kbps の単位でレートを入力します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS ロールに帯域幅の制限を課しません。

（注）　Burst Real-Time Rate は Average Real-Time Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 12　QoS ロールをゲスト ユーザに適用するには、「GUI を使用したローカル ネットワーク ユーザの設定」の項（P. 5-30）の手順に従ってください。

CLI を使用した QoS ロールの設定

コントローラの CLI を使用して QoS ロールを設定する手順は、次のとおりです。

ステップ 1　ゲスト ユーザ用の QoS ロールを作成するには、次のコマンドを入力します。

config netuser guest-role create *role_name*

（注）　QoS ロールを削除するには、次のコマンドを入力します。
config netuser guest-role delete *role_name*

ステップ 2　QoS ロール用の帯域幅コントラクトを設定するには、次のコマンドを入力します。

- **config netuser guest-role qos data-rate average-data-rate** *role_name rate*：ユーザごとの TCP トラフィックの平均データ レートを設定します。
- **config netuser guest-role qos data-rate burst-data-rate** *role_name rate*：ユーザごとの TCP トラフィックのピーク データ レートを設定します。

（注）　Burst Data Rate は Average Data Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

- **config netuser guest-role qos data-rate average-realtime-rate** *role_name rate*：ユーザごとの UDP トラフィックの平均リアルタイム レートを設定します。
- **config netuser guest-role qos data-rate burst-realtime-rate** *role_name rate*：ユーザごとの UDP トラフィックのピーク リアルタイム レートを設定します。

（注）　Burst Real-Time Rate は Average Real-Time Rate 以上に設定する必要があります。そうしないと、QoS ポリシーによって無線クライアントとの間のトラフィックがブロックされることがあります。

（注）　これらの各コマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください（Contractor、Vendor、など）。*rate* パラメータには、0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値 0 は、QoS ロールに帯域幅の制限を課しません。

ステップ 3　ゲスト ユーザに QoS ロールを適用するには、次のコマンドを入力します。

config netuser guest-role apply *username role_name*

たとえば、*Contractor* のロールをゲスト ユーザ *jsmith* に適用するとします。

（注）　ゲスト ユーザに QoS ロールを割り当てない場合、User Details の Role フィールドにロールが「default」のように表示されます。このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

（注）　ゲスト ユーザに QoS ロールを割り当てないようにするには、次のコマンドを入力します。**config netuser guest-role apply** *username* **default**　これで、このユーザは WLAN の QoS プロファイルで定義された帯域幅コントラクトを使用するようになります。

ステップ 4　変更を保存するには、次のコマンドを入力します。

save config

ステップ 5　現在の QoS ロールとそれらの帯域幅パラメータの一覧を表示するには、次のコマンドを入力します。

show netuser guest-roles

次のような情報が表示されます。

```
Role Name..................................... Contractor
     Average Data Rate........................ 10
     Burst Data Rate.......................... 10
     Average Realtime Rate.................... 100
     Burst Realtime Rate...................... 100

Role Name..................................... Vendor
     Average Data Rate........................ unconfigured
     Burst Data Rate.......................... unconfigured
     Average Realtime Rate.................... unconfigured
     Burst Realtime Rate..................... unconfigured
```

音声パラメータとビデオ パラメータの設定

コントローラには、音声またはビデオ、あるいはその両方の品質に影響を及ぼす次の 3 つのパラメータがあります。

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

これらのパラメータはそれぞれ、Cisco Compatible Extensions (CCX) v4 および v5 でサポートされています。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

（注） CCX は、AP1030 ではサポートされません。

音声の品質に関する問題の監視およびレポートには、Traffic Stream Metrics（TSM）を使用します。

Call Admission Control

Call Admission Controll（CAC; コール アドミッション制御）を使用すると、無線 LAN で輻輳が発生する際に、アクセス ポイントで制御された QoS（Quality of Service）を維持できます。CCX v3 で展開される Wi-Fi Multimedia（WMM）プロトコルにより、無線 LAN に輻輳が発生しない限り十分な QoS が保証されます。ただし、異なるネットワーク ロードで QoS を維持するには、CCX v4 で CAC が必要です。帯域幅ベースの CAC と負荷ベースの CAC という 2 種類の CAC が使用できます。

帯域幅ベースの CAC

帯域幅ベースまたは静的な CAC を使用すると、クライアントで新しいコールを受け入れるために必要な帯域幅または共有メディア時間を指定できます。その結果としてアクセス ポイントでは、この特定のコールに対応する能力があるかどうかを決定できます。アクセス ポイントでは、許容される品質でコールの最大数を維持するために、必要であればコールを拒否します。

WLAN の QoS 設定により、帯域幅ベースの CAC サポートのレベルが決定します。音声アプリケーションで帯域幅ベースの CAC を使用するには、WLAN を Platinum QoS に対して設定する必要があります。ビデオア プリケーションで帯域幅ベースの CAC を使用するには、WLAN を Gold QoS に対して設定する必要があります。さらに、WMM が WLAN に対して有効化されているのを確認します。QoS と WMM の設定の手順については、「802.3 ブリッジの設定」の項（P. 4-37）を参照してください。

（注） WMM が有効化されている CCX v4 クライアントに対して Admission Control（ACM; アドミッション コントロール）を有効にする必要があります。そうしない場合、帯域幅ベースの CAC は適切に動作しません。

負荷ベースの CAC

負荷ベースの CAC では、音声アプリケーションに関して帯域幅を消費するすべてのトラフィックの種類（クライアントからのトラフィックなど）、同じチャネルのアクセス ポイントの負荷、および同じ場所に設置されたチャネルの干渉を考慮した測定方法を取り入れます。負荷ベースの CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

負荷ベースの CAC では、アクセス ポイントは RF チャネルの使用状況（つまり、消費された帯域幅の割合）、チャネル干渉、およびアクセス ポイントで許可される追加コールを継続的に測定し、更新します。アクセス ポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、負荷ベースの CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。

（注） 負荷ベースの CAC は Lightweight アクセス ポイントでのみサポートされています。負荷ベースの CAC を無効にすると、アクセス ポイントが帯域幅ベースの CAC を使用するようになります。

Expedited Bandwidth Requests

Expedited Bandwidth Request 機能を使用すると、CCXv5 クライアントは WLAN への緊急の WMM Traffic Specifications（TSPEC）要求（e911 コールなど）を示すことができるようになります。コントローラがこの要求を受信すると、コントローラは、処理中の他の TSPEC コールの質を変えることなく、どうにかして緊急のコールに対応しようとします。

Expedited Bandwidth Requests は、帯域幅ベースの CAC と負荷ベースの CAC の両方に適用できます。Expedited Bandwidth Requests はデフォルトでは無効になっています。この機能が無効の場合、コントローラはすべての緊急の要求を無視し、TSPEC 要求は通常の TSPEC 要求として処理します。

通常の TSPEC 要求と Expedited Bandwidth Requests に対する TSPEC 要求処理の例は、表 4-2 を参照してください。

表 4-2　TSPEC 要求処理の例

CAC モード	音声コールに予約された帯域幅[1]	使用率[2]	通常の TSPEC 要求	Expedited Bandwidth Request を使用した TSPEC
帯域幅ベースの CAC	75%（デフォルト設定）	75% 未満	許可	許可
		75% ～ 90%（音声コール用に予約された帯域幅が消費される）	拒否	許可
		90% 以上	拒否	拒否
負荷ベースの CAC		75% 未満	許可	許可
		75% ～ 85%（音声コール用に予約された帯域幅が消費される）	拒否	許可
		85% 以上	拒否	拒否

1. 帯域幅ベースの CAC の場合、音声コールの帯域幅利用率はアクセス ポイント単位となり、同じチャネルのアクセス ポイントは考慮されません。負荷ベースの CAC の場合、音声コールの帯域幅利用率は、チャネル全体に対して測定されます。
2. 帯域幅ベースの CAC（音声およびビデオに消費された帯域幅）または負荷ベースの CAC（チャネル利用率 [Pb]）

（注） ビデオ ACM が有効になっている場合、TSPEC の Nom-MSDU サイズが 149 より大きい、または平均データ レートが 1Kb/s よりも大きいと、コントローラがビデオ TSPEC を拒否します。

U-APSD

Unscheduled automatic power save delivery（U-APSD）は、モバイル クライアントのバッテリ寿命を延ばす IEEE 802.11e で定義されている QoS 機能です。バッテリ寿命を延ばすだけでなく、この機能は無線メディアで配送されるトラフィック フローの遅延時間を短縮します。U-APSD は、アクセス ポイントでバッファされる個々のパケットをポーリングするようにクライアントに要求しないため、単一のアップリンク トリガ パケットを送信することにより、複数のダウンリンク パケットの送信が許可されます。WMM が有効化されると、U-APSD は自動的に有効化されます。

Traffic Stream Metrics

voice-over-wireless LAN（VoWLAN）展開では、クライアントとアクセス ポイント間のエア インターフェイスでの音声関連のメトリクスの測定には、Traffic Stream Metrics（TSM）が使用されます。TSM ではパケット遅延とパケット損失の両方がレポートされます。管理者は、これらのレポートを調べて劣悪な音声品質の問題を分離できます。

このメトリクスは、CCX v4 以降をサポートするアクセス ポイントとクライアント デバイス間のアップリンク（クライアント側）統計とダウンリンク（アクセス ポイント側）統計の集合から成ります。クライアントが CCX v4 または CCXv5 に準拠していない場合、ダウンリンク統計のみが取得されます。クライアントとアクセス ポイントで、これらのメトリクスが測定されます。アクセス ポイントではまた、5 秒おきに測定値が収集されて、90 秒のレポートが作成された後、レポートがコントローラに送信されます。コントローラでは、アップリンクの測定値をクライアントに基づいて、ダウンリンクの測定値をアクセス ポイントに基づいて整理し、1 時間相当の履歴データを保持します。このデータを格納するには、コントローラでアップリンク メトリクス用に 32MB、ダウンリンク メトリクス用に 4.8MB の追加のメモリが必要となります。

無線帯域別ベースで（たとえば、すべての 802.11a ラジオ）、GUI または CLI により TSM を設定できます。コントローラは、リブート後も持続するように、フラッシュ メモリに設定を保存します。アクセス ポイントにより、コントローラからの設定が受信された後、指定された無線帯域で TSM が有効化されます。

（注） アクセス ポイントでは、ローカル モードと hybrid-REAP モードの両方で TSM がサポートされます。

GUI を使用した音声パラメータの設定

GUI を使用して音声パラメータを設定する手順は、次のとおりです。

ステップ 1　WMM と Platinum QoS レベルに対して WLAN が設定されていることを確認してください。

ステップ 2　WMM が有効になっている WLAN をすべて無効にして、**Apply** をクリックします。

ステップ 3　無線ネットワークを無効にするには、802.11a/n または 802.11b/g/n の下で **Wireless**、**Network** の順にクリックし、802.11a（または 802.11b/g）Network Status チェックボックスをオフにして、**Apply** をクリックします。

ステップ 4　802.11a/n または 802.11b/g/n の **Voice** をクリックします。802.11a（または 802.11b）> Voice Parameters ページが表示されます（図 4-16 を参照）。

図 4-16　802.11a > Voice Parameters ページ

ステップ 5　この無線帯域で帯域幅ベースの CAC 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。デフォルト値は無効（disable）です。

ステップ 6　この無線帯域で負荷ベースの CAC を有効にするには、**Admission Control (ACM)** チェックボックスおよび **Load-based AC** チェックボックスをオンにします。これらのチェックボックスはデフォルトでは、両方とも無効になっています。

ステップ 7　Max RF Bandwidth フィールドに、この無線帯域で音声アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を入力します。クライアントが指定された値に達すると、アクセスポイントではこの無線帯域での新しいコールが拒否されます。

範囲：40 ～ 85%

デフォルト：75%

ステップ 8　Reserved Roaming Bandwidth フィールドに、ローミングする音声クライアント用に割り当てられた最大帯域幅の割合を入力します。コントローラは、ローミングする音声クライアントに対して割り当てられている最大帯域幅から、この割合の帯域幅を予約します。

範囲：0 ～ 25%

デフォルト：6%

ステップ 9　Expedited Bandwidth Requests を有効にするには、**Expedited Bandwidth** チェックボックスをオンにします。デフォルト値は無効（disable）です。

ステップ 10　TSM を有効にするには、**Metrics Collection** チェックボックスをオンにします。デフォルト値は無効（disable）です。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　WMM WLAN すべてを再度有効にして、**Apply** をクリックします。

ステップ 13　無線ネットワークを再度有効にするには、802.11a/n または 802.11b/g/n の下で **Network** をクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオンにし、**Apply** をクリックします。

ステップ 14　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 15　別の無線帯域（802.11a または 802.11b/g）について音声パラメータの設定をする場合、この手順を繰り返します。

GUI を使用したビデオ パラメータの設定

GUI を使用してビデオ パラメータを設定する手順は、次のとおりです。

ステップ 1　WMM と Gold QoS レベルに対して WLAN が設定されていることを確認してください。

ステップ 2　WMM が有効になっている WLAN をすべて無効にして、**Apply** をクリックします。

ステップ 3　無線ネットワークを無効にするには、802.11a または 802.11b/g の下で **Wireless**、**Network** の順にクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオフにして、**Apply** をクリックします。

ステップ 4　802.11a/n または 802.11b/g/n の下の **Video** をクリックします。802.11a（または 802.11b）> Video Parameters ページが表示されます（図 4-17 を参照）。

図 4-17　802.11a > Video Parameters ページ

ステップ 5　この無線帯域でビデオ CAC 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。デフォルト値は無効（disable）です。

ステップ 6　Max RF Bandwidth フィールドに、この無線帯域でビデオ アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を入力します。クライアントが指定された値に達すると、アクセス ポイントではこの無線帯域での新しい要求が拒否されます。

範囲：0 ～ 100%（ただし、音声とビデオを加算した最大 RF 帯域幅が 100% を超えてはなりません）。

デフォルト：0%

（注） このパラメータがゼロ（0）に設定されている場合、コントローラではオペレータが帯域幅の割り当てを行わないと想定されるので、すべての帯域幅の要求が許可されます。

ステップ 7　Reserved Roaming Bandwidth フィールドに、ビデオ クライアントのローミング用に割り当てられた最大帯域幅の割合を入力します。コントローラは、ローミングするビデオ クライアントに対して割り当てられている最大帯域幅から、この割合の帯域幅を予約します。

範囲：0 ～ 25%

デフォルト：0%

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　WMM WLAN すべてを再度有効にして、**Apply** をクリックします。

ステップ 10　無線ネットワークを再度有効にするには、802.11a/n または 802.11b/g/n の下で **Network** をクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオンにし、**Apply** をクリックします。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

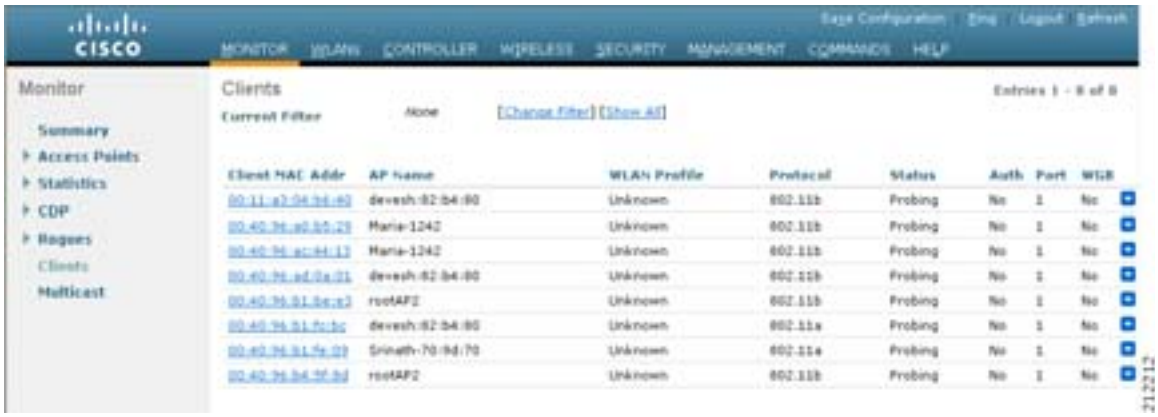
ステップ 12　別の無線帯域（802.11a または 802.11b/g）についてビデオ パラメータの設定をする場合、この手順を繰り返します。

GUI を使用した音声設定とビデオ設定の表示

GUI を使用して音声設定とビデオ設定を表示する手順は、次のとおりです。

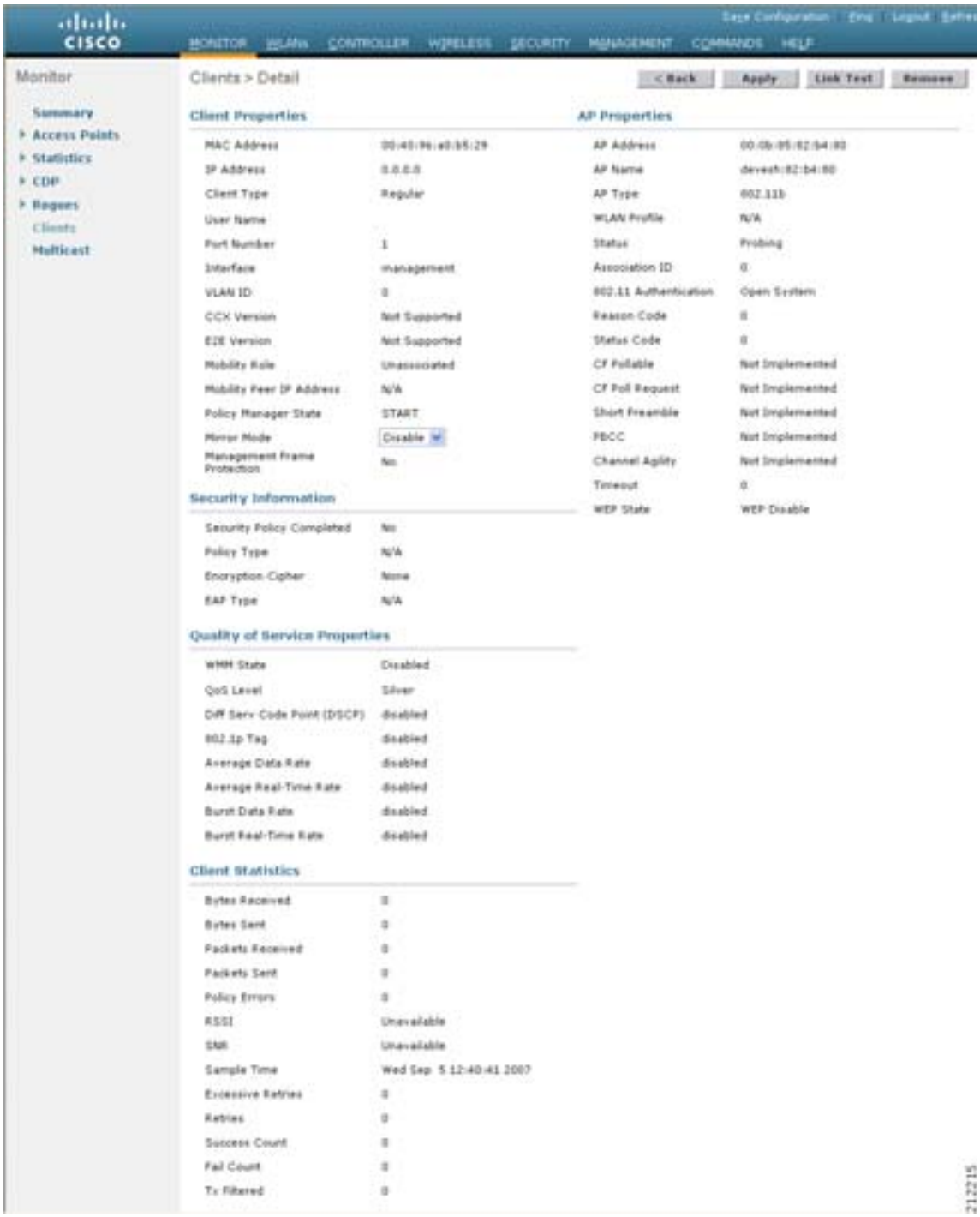
ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます（図 4-18 を参照）。

図 4-18　Clients ページ



ステップ 2　目的のクライアントの MAC アドレスをクリックして、Clients > Detail ページを開きます（図 4-19 を参照）。

図 4-19　Clients > Detail ページ



このページには、Quality of Service Properties の下にこのクライアントの U-APSD ステータス（有効になっている場合）が表示されます。

ステップ 3　Clients ページに戻るには、**Back** をクリックします。

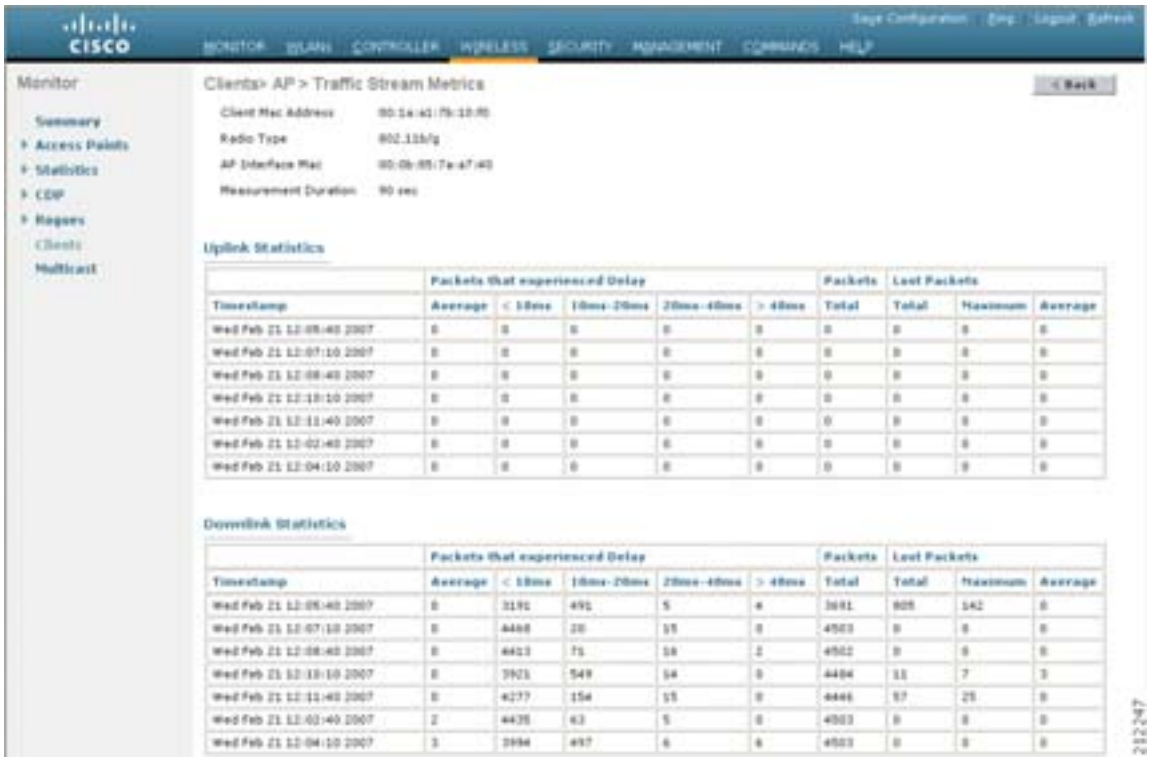
ステップ 4　特定のクライアントと、このクライアントがアソシエートされているアクセス　ポイントに対する TSM 統計を表示する手順は次のとおりです。

a. カーソルを目的のクライアントの青のドロップダウン矢印の上に置いて、**802.11aTSM** または **802.11b/gTSM** を選択します。Clients > AP ページが表示されます（図 4-20 を参照）。

図 4-20　Clients > AP ページ

b. 目的のアクセス ポイントの **Detail** リンクをクリックして、Clients > AP > Traffic Stream Metrics ページを開きます（図 4-21 を参照）。

図 4-21　Clients > AP > Traffic Stream Metrics ページ

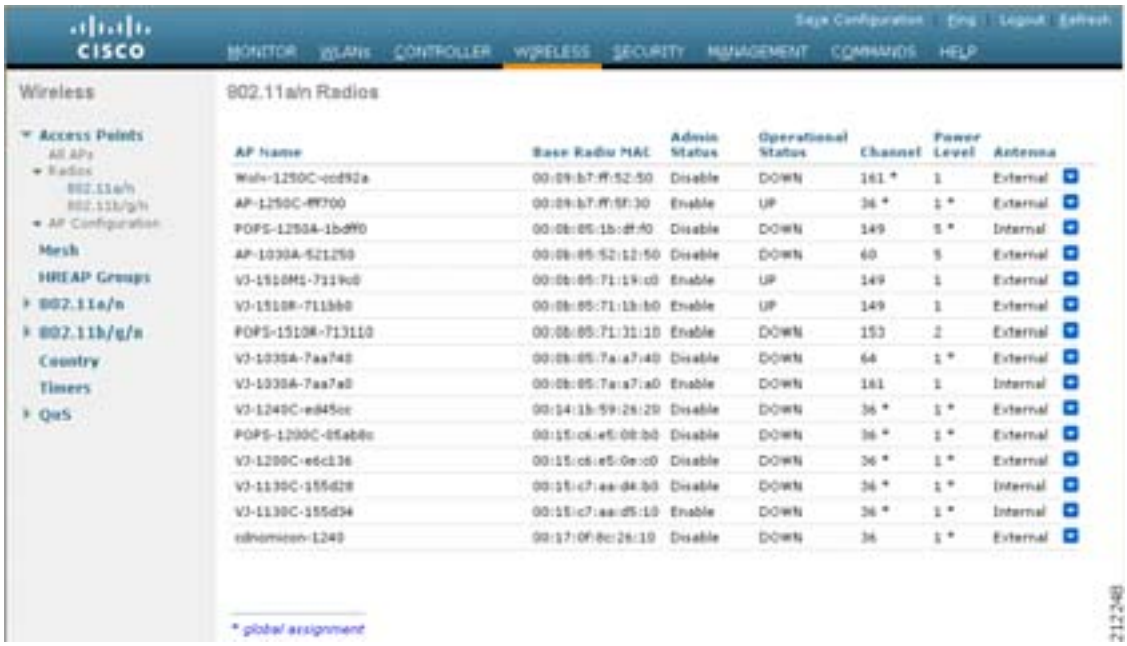


このページには、このクライアントと、このクライアントがアソシエートされているアクセス ポイントの TSM 統計が表示されます。統計は、90 秒間隔で表示されます。timestamp フィールドには、特定の統計収集間隔が表示されます。

ステップ 5　特定のアクセス ポイントと、このアクセス ポイントにアソシエートされている特定のクライアントに対する TSM 統計を表示する手順は次のとおりです。

a. **Wireless** > **Access Points** > **Radios** > **802.11a/n** または **802.11b/g/n** の順にクリックします。802.11a/n Radios ページまたは 802.11b/g/n Radios ページが表示されます（図 4-22 を参照）。

図 4-22　802.11a/n Radios ページ

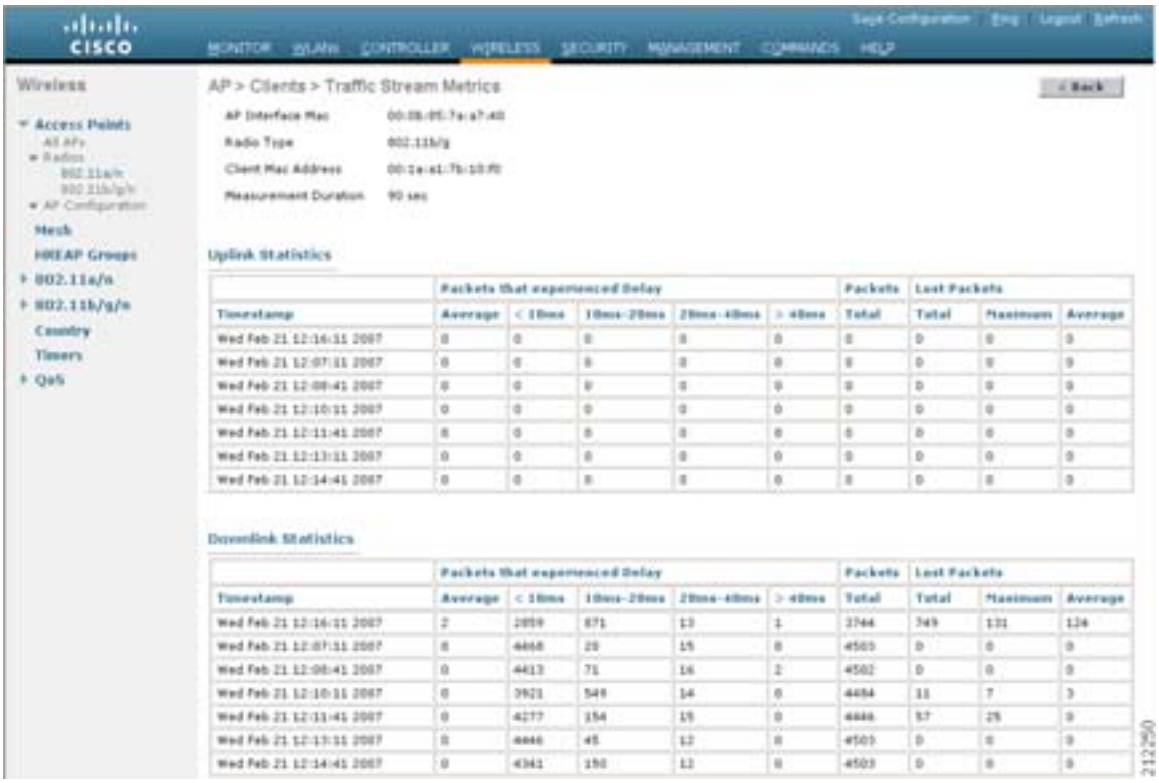


b. カーソルを目的のアクセス ポイントの青のドロップダウン矢印の上に置いて、**802.11aTSM** または **802.11b/gTSM** を選択します。AP > Clients ページが表示されます（図 4-23 を参照）。

図 4-23　AP > Clients ページ

c. 目的のクライアントの **Detail** リンクをクリックして、AP > Clients > Traffic Stream Metrics ページを開きます（図 4-24 を参照）。

図 4-24　AP > Clients > Traffic Stream Metrics ページ



このページには、このアクセス ポイントと、このアクセス ポイントにアソシエートされているクライアントの TSM 統計が表示されます。統計は、90 秒間隔で表示されます。timestamp フィールドには、特定の統計収集間隔が表示されます。

CLI を使用した音声パラメータの設定

CLI を使用して音声パラメータを設定する手順は、次のとおりです。

ステップ 1　コントローラ上に設定されているすべての WLAN を表示するには、次のコマンドを入力します。

show wlan summary

ステップ 2　変更を行う WLAN が WMM に対して設定されており、QoS レベルが Platinum に設定されていることを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

ステップ 3　音声パラメータの変更前に、WMM が有効になっている WLAN をすべて無効にするには、次のコマンドを入力します。

config wlan disable *wlan_id*

ステップ 4　無線ネットワークを無効にするには、次のコマンドを入力します。

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

ステップ 5　設定を保存するには、次のコマンドを入力します。

save config

ステップ 6　802.11a または 802.11b/g ネットワークに対する帯域幅ベースの音声 CAC を有効または無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac voice acm** {**enable** | **disable**}

ステップ 7　802.11a または 802.11b/g ネットワーク上で音声アプリケーション用にクライアントに割り当てられた最大帯域幅の割合を設定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

bandwidth の範囲は 40 ～ 85% で、デフォルト値は 75% です。クライアントが指定された値に達すると、アクセス ポイントではこのネットワーク上の新しいコールが拒否されます。

ステップ 8　音声クライアントのローミング用に割り当てられている最大帯域幅の割合を設定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

bandwidth の範囲は 0 ～ 25% で、デフォルト値は 6% です。コントローラは、ローミングする音声クライアントに対して割り当てられている最大帯域幅から、この割合の帯域幅を予約します。

ステップ 9　アクセス ポイントから受信した TSPEC 無活動タイムアウトを処理または無視するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac voice tspec-inactivity-timeout** {**enable** | **ignore**}

ステップ 10　802.11a または 802.11b/g ネットワークに対する負荷ベースの CAC を有効または無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac voice load-based** {**enable** | **disable**}

ステップ 11　802.11a または 802.11b/g ネットワークに対する Expedited Bandwidth Requests を有効または無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **exp-bwreq** {**enable** | **disable**}

ステップ 12　802.11a または 802.11b/g ネットワークに対する TSM を有効または無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **tsm** {**enable** | **disable**}

ステップ 13　WMM が有効になっている WLAN を再度有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

ステップ 14 無線ネットワークを再度有効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} enable network

ステップ 15 設定を保存するには、次のコマンドを入力します。

save config

CLI を使用したビデオ パラメータの設定

CLI を使用してビデオ パラメータを設定する手順は、次のとおりです。

ステップ 1 コントローラ上に設定されているすべての WLAN を表示するには、次のコマンドを入力します。

show wlan summary

ステップ 2 変更を行う WLAN が WMM に対して設定されており、QoS レベルが Gold に設定されていることを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

ステップ 3 ビデオ パラメータの変更前に、WMM が有効になっている WLAN をすべて無効にするには、次のコマンドを入力します。

config wlan disable *wlan_id*

ステップ 4 無線ネットワークを無効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} disable network

ステップ 5 設定を保存するには、次のコマンドを入力します。

save config

ステップ 6 802.11a または 802.11b/g ネットワークに対するビデオ CAC を有効または無効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} cac video acm {enable | disable}

ステップ 7 802.11a または 802.11b/g ネットワーク上でビデオ アプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定するには、次のコマンドを入力します。

config {802.11a | 802.11b} cac video max-bandwidth *bandwidth*

bandwidth の範囲は 0 ～ 100% で、デフォルト値は 0% です。ただし、音声とビデオを加算した最大 RF 帯域幅が 100% を超えてはなりません。クライアントが指定された値に達すると、アクセス ポイントではこのネットワーク上の新しいコールが拒否されます。

（注） このパラメータがゼロ（0）に設定されている場合、コントローラではオペレータが帯域幅の割り当てを行わないと想定されるので、すべての帯域幅の要求が許可されます。

ステップ 8　音声クライアントのローミング用に割り当てられている最大帯域幅の割合を設定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **cac video roam-bandwidth** *bandwidth*

bandwidth の範囲は 0 ～ 25% で、デフォルト値は 0% です。コントローラは、ローミングするビデオ クライアントに対して割り当てられている最大帯域幅から、この割合の帯域幅を予約します。

ステップ 9　WMM が有効になっている WLAN を再度有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

ステップ 10　無線ネットワークを再度有効にするには、次のコマンドを入力します。

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

ステップ 11　設定を保存するには、次のコマンドを入力します。

save config

CLI を使用した音声設定とビデオ設定の表示

CLI を使用して音声設定とビデオ設定を表示するには、次のコマンドを使用します。

1. 802.11a または 802.11b/g ネットワークに対する CAC 設定を表示するには、次のコマンドを入力します。

   show {**802.11a** | **show 802.11b**}

2. 特定のアクセス ポイントの CAC 統計を表示するには、次のコマンドを入力します。

   show ap stats {**802.11a** | **802.11b**} *ap_name*

   次のような情報が表示されます。

```
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 0
    Total channel MT free..................... 0
    Total voice MT free....................... 0
    Na Direct................................. 0
    Na Roam................................... 0
  Video Bandwidth in use(% of config bw)..... 0
  Total num of voice calls in progress....... 0
  Num of roaming voice calls in progress..... 0
  Total Num of voice calls since AP joined..... 0
  Total Num of roaming calls since AP joined..... 0
  Total Num of exp bw requests received..... 5
  Total Num of exp bw requests admitted..... 2

Num of voice calls rejected since AP joined.... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficient bw....0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate..... 0
  Num of calls rejected due to QoS policy..... 0
```

この例では、「MT」はメディア時間、「Na」は追加コールの数、および「exp bw」は、緊急用帯域幅です。

3. 特定のクライアントの U-APSD 統計を表示するには、次のコマンドを入力します。

   show client detail *client_mac*

4. 特定のクライアントと、このクライアントがアソシエートされているアクセス ポイントに対する TSM 統計を表示するには、次のコマンドを入力します。

   show client tsm {**802.11a** | **802.11b**} *client_mac* [*ap_mac* | **all**]

   オプションの **all** コマンドは、このクライアントがアソシエートされているすべてのアクセス ポイントを表示します。次のような情報が表示されます。

```
AP Interface Mac:                   00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).....................35
       Delay less than 10 ms..............................20
       Delay bet 10 - 20 ms...............................20
       Delay bet 20 - 40 ms...............................20
       Delay greater than 40 ms...........................20
      Total packet Count..................................80
      Total packet lost count (5sec).....................10
      Maximum Lost Packet count(5sec).....................5
      Average Lost Packet count(5secs)....................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).....................35
       Delay less than 10 ms..............................20
       Delay bet 10 - 20 ms...............................20
       Delay bet 20 - 40 ms...............................20
       Delay greater than 40 ms...........................20
      Total packet Count..................................80
      Total packet lost count (5sec).....................10
      Maximum Lost Packet count(5sec).....................5
      Average Lost Packet count(5secs)....................2
```

（注） 統計は、90 秒間隔で表示されます。timestamp フィールドには、特定の統計収集間隔が表示されます。

5. 特定のアクセス ポイントと、このアクセス ポイントにアソシエートされている特定のクライアントに対する TSM 統計を表示する次のコマンドを入力します。

   show ap stats {**802.11a** | **802.11b**} *ap_name* **tsm** [*client_mac* | **all**]

オプションの **all** コマンドは、このアクセス ポイントにアソシエートされているすべてのクライアントを表示します。次のような情報が表示されます。

```
AP Interface Mac:                   00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).............................35
       Delay less than 10 ms......................................20
       Delay bet 10 - 20 ms.......................................20
       Delay bet 20 - 40 ms.......................................20
       Delay greater than 40 ms...................................20
      Total packet Count..........................................80
      Total packet lost count (5sec)..............................10
      Maximum Lost Packet count(5sec).............................5
      Average Lost Packet count(5secs)............................2
```

（注） 統計は、90 秒間隔で表示されます。timestamp フィールドには、特定の統計収集間隔が表示されます。

EDCA パラメータの設定

Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。コントローラの GUI または CLI を使用して EDCA パラメータを設定するには、この項の手順に従ってください。

GUI を使用した EDCA パラメータの設定

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

ステップ 1　無線ネットワークを無効にするには、802.11a または 802.11b/g の下で **Wireless**、**Network** の順にクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオフにして、**Apply** をクリックします。

ステップ 2　802.11a/n または 802.11b/g/n の **EDCA Parameters** をクリックします。802.11a（または 802.11b/g）> EDCA Parameters ページが表示されます（図 4-25 を参照）。

図 4-25　802.11a > EDCA Parameters ページ

ステップ 3　EDCA Profile ドロップダウン ボックスで、次のいずれかのオプションを選択します。

- **WMM**：Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。これはデフォルト値です。音声サービスやビデオのサービスがネットワーク上で展開されない場合に、このオプションを選択します。
- **Spectralink Voice Priority**：Spectralink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。
- **Voice Optimized**：音声用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で Spectralink 以外の音声サービスを展開する場合に、このオプションを選択します。
- **Voice & Video Optimized**：音声とビデオ用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスの両方を展開する場合に、このオプションを選択します。

（注）　ビデオ サービスを展開する場合は、Admission Control（ACM）を無効にする必要があります。

ステップ 4　音声用の MAC の最適化を有効にする場合は、**Enable Low Latency MAC** チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。この機能は、パケットの再送信を制御し、Lightweight アクセス ポイント上で音声パケットを適切にエージングアウトすることより、音声性能を向上させます。したがって、アクセス ポイントごとで提供される音声コール数が高まります。

（注）　WLAN で WMM クライアントが許可されている場合のみ、低遅延 MAC を有効にする必要があります。WMM が有効になっている場合は、低遅延 MAC を任意の EDCA プロファイルと共に使用できます。WMM の有効化の手順については、「QoS Enhanced BSS の設定」の項（P. 6-31）を参照してください。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　無線ネットワークを再度有効にするには、802.11a/n または 802.11b/g/n の下で **Network** をクリックし、**802.11a**（または **802.11b/g**）**Network Status** チェックボックスをオンにし、**Apply** をクリックします。

ステップ 7　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した EDCA パラメータの設定

CLI を使用して EDCA パラメータを設定する手順は、次のとおりです。

ステップ 1　無線ネットワークを無効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} disable network

ステップ 2　設定を保存するには、次のコマンドを入力します。

save config

ステップ 3　特定の EDCA プロファイルを有効にするには、次のコマンドを入力します。

config advanced {802.11a | 802.11b} edca-parameters *?*

? は、次のいずれかです。

- **wmm-default**
- **svp-voice**
- **optimized-voice**
- **optimized-video-voice**

（注）　各オプションの説明については、上記の「GUI を使用した EDCA パラメータの設定」の項を参照してください。

ステップ 4　音声用の MAC 最適化の現在のステータスを表示するには、次のコマンドを入力します。

show {**802.11a** | **802.11b**}

次のような情報が表示されます。

```
Voice-mac-optimization.................Disabled
```

ステップ 5　音声用の MAC 最適化を有効または無効にするには、次のコマンドを入力します。

config advanced {**802.11a** | **802.11b**} **voice-mac-optimization** {**enable** | **disable**}

この機能は、パケットの再送信を制御し、Lightweight アクセス ポイント上で音声パケットを適切にエージングアウトすることより、音声性能を向上させます。したがって、アクセス ポイントごとで提供される音声コール数が高まります。デフォルト値は無効（disable）です。

ステップ 6　無線ネットワークを再度有効にするには、次のコマンドを入力します。

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

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

Cisco Discovery Protocol の設定

Cisco Discovery Protocol（CDP）は、すべてのシスコ製の機器で実行されるデバイス ディスカバリ プロトコルです。CDP を使用して有効化されたデバイスは、近隣のデバイスにその存在を認識させるためにインターフェイスの更新をマルチキャスト アドレスに周期的に送信します。

周期的な送信の間隔のデフォルト値は 60 秒で、アドバタイズされた有効期間のデフォルト値は 180 秒です。プロトコルの第 2 および最新バージョン（CDPv2）では、新しい Time Length Value（TLV）が導入され、従来より迅速なエラー追跡を可能にすることでダウン タイムを減らすレポート メカニズムが備わっています。

CDPv1 および CDPv2 は次のデバイスでサポートされています。

- 2100 および 4400 シリーズ コントローラ

（注） CDP は、Catalyst 3750G Integrated Wireless LAN Controller Switch、Cisco WiSM、および Cisco 28/37/38xx Series Integrated Services Router などの、シスコのスイッチおよびルータと統合されたコントローラではサポートされません。ただし、コントローラに接続されているアクセス ポイントの CDP ネイバーの一覧を表示するには、これらのコントローラで **show ap cdp neighbors** [**detail**] {*Cisco_AP* | **all**} コマンドを使用できます。

- LWAPP 有効化アクセス ポイント
- 2100 シリーズ コントローラへ直接接続されたアクセス ポイント

このサポートにより、ネットワーク管理アプリケーションはシスコのデバイスを検出できるようになります。

次の TLV は、コントローラとアクセス ポイントの両方でサポートされています。

- **Device-ID TLV: 0x0001**：コントローラ、アクセス ポイント、または CDP ネイバーのホスト名。
- **Address TLV: 0x0002**：コントローラ、アクセス ポイント、または CDP ネイバーの IP アドレス。
- **Port-ID TLV: 0x0003**：CDP パケットが送信されるインターフェイス名。
- **Capabilities TLV: 0x0004**：デバイスの機能。コントローラはこの TLV を Host: 0x10 の値で発信し、アクセス ポイントはこの TLV を Transparent Bridge: 0x02 の値で発信します。
- **Version TLV: 0x0005**：コントローラ、アクセス ポイント、または CDP ネイバーのソフトウェア バージョン。
- **Platform TLV: 0x0006**：コントローラ、アクセス ポイント、または CDP ネイバーのハードウェア プラットフォーム。

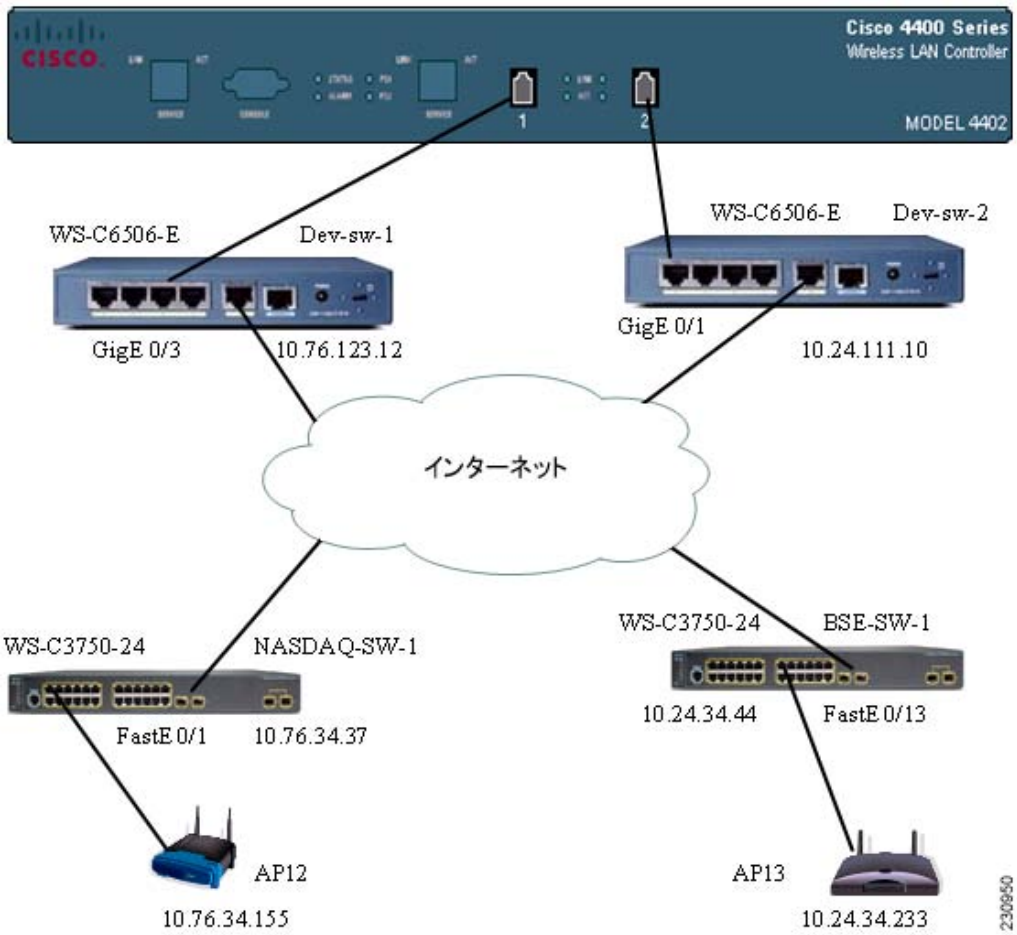
次の TLV は、アクセス ポイントでのみサポートされます。

- **Full/Half Duplex TLV: 0x000b**：CDP パケットが送信されるイーサネット リンクの全二重または半二重モード。この TLV は、2100 シリーズ コントローラに直接接続されたアクセス ポイントではサポートされません。
- **Power Consumption TLV: 0x0010**：アクセス ポイントで消費される電力の最大量。この TLV は、2100 シリーズ コントローラに直接接続されたアクセス ポイントではサポートされません。

コントローラ ソフトウェア リリース 4.1 以降の GUI またはコントローラ ソフトウェア リリース 4.0 以降の CLI を使用して、CDP の設定および CDP 情報の表示を行えます。図 4-26 は、この項の手順を実行する際の参考として使用できる、サンプルのネットワークを示しています。

(注)　CDP 設定をコントローラで変更しても、コントローラに接続されているアクセス ポイントの CDP 設定は変更されません。各アクセス ポイントに対して個別に CDP を有効または無効にする必要があります。

図 4-26　CDP を示したサンプルのネットワーク



GUI を使用した Cisco Discovery Protocol の設定

コントローラ GUI を使用して CDP を設定する手順は、次のとおりです。

ステップ 1　**Controller** > **CDP** > **Global Configuration** の順にクリックして、CDP > Global Configuration ページを開きます（図 4-27 を参照）。

図 4-27　CDP > Global Configuration ページ

ステップ 2　コントローラで CDP を有効にする場合は **CDP Protocol Status** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。

ステップ 3　CDP Advertisement Version ドロップダウン ボックスから、**v1** または **v2** を選択して、コントローラでサポートされている最も新しい CDP バージョンを指定します。デフォルト値は v1 です。

ステップ 4　Refresh-time Interval フィールドで、CDP メッセージが生成される間隔を入力します。範囲は 5 ～ 254 秒で、デフォルト値は 60 秒です。

ステップ 5　Holdtime フィールドに、生成された CDP パッケージで有効時間値としてアドバタイズされる時間を入力します。範囲は 10 ～ 255 秒で、デフォルト値は 180 秒です。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、変更を保存します。

ステップ 8　次のいずれかの操作を行います。

- 特定のアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。
  a. **Wireless** > **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。
  b. 目的のアクセス ポイントのリンクをクリックします。
  c. **Advanced** タブをクリックして、All APs > Details（Advanced）ページを開きます（図 4-28 を参照）。

図 4-28　All APs > Details（Advanced）ページ

d. このアクセス ポイントで CDP を有効にする場合は **Cisco Discovery Protocol** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値は有効（enable）です。

e. **Apply** をクリックして、変更を適用します。

- このコントローラに現在アソシエートされているすべてのアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。

a. **Wireless** > **Access Points** > **AP Configuration** > **CDP Template** の順にクリックして、AP Configuration > CDP Template ページを開きます。

b. コントローラにアソシエートされているすべてのアクセス ポイントで CDP を有効にするには、**CDP State** チェックボックスをオンにします。すべてのアクセス ポイントで CDP を無効にするには、オフにします。デフォルト値はオンです。

c. **Apply to All APs** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更内容を保存します。

GUI を使用した Cisco Discovery Protocol 情報の表示

コントローラ GUI を使用して CDP 情報を表示する手順は、次のとおりです。

ステップ 1　すべてのインターフェイスのすべての CDP ネイバーのリストを確認するには、**Monitor** > **CDP** > **Interface Neighbors** の順にクリックします。CDP > Interface Neighbors ページが表示されます（図 4-29 を参照）。

図 4-29　CDP > Interface Neighbors ページ

このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート
- 各 CDP ネイバーの名前
- 各 CDP ネイバーの IP アドレス
- CDP パケットの送信に各 CDP ネイバーが使用するポート
- 各 CDP ネイバー エントリの有効期間が切れるまでの残り時間（秒）
- 各 CDP ネイバーの機能は、次のように定義されています。R - ルータ、T - 転送ブリッジ、B - ソース ルート ブリッジ、S - スイッチ、H - ホスト、I - IGMP、r - リピータ、M - リモート管理デバイス
- 各 CDP ネイバー デバイスのハードウェア プラットフォーム

ステップ 2　各インターフェイスの CDP ネイバーの詳細情報を表示するには、必要なインターフェイス ネイバーの名前をクリックします。CDP > Interface Neighbors > Detail ページが表示されます（図 4-30 を参照）。

図 4-30　CDP > Interface Neighbors > Detail ページ

このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート

- CDP ネイバーの名前
- CDP ネイバーの IP アドレス
- CDP パケットの送信に CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）
- CDP ネイバーエントリの有効期間が切れるまでの残り時間（秒）
- CDP ネイバーの機能は、次のように定義されています。ルータ、転送ブリッジ、ソース ルータ ブリッジ、スイッチ、ホスト、IGMP、リピータ、またはリモート管理デバイス
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 3　コントローラに接続されているすべてのアクセス ポイントの CDP ネイバーのリストを確認するには、**AP Neighbors** の順にクリックします。CDP AP Neighbors ページが表示されます（図 4-31 を参照）。

図 4-31　CDP AP Neighbors ページ

ステップ 4　特定のアクセス ポイントの CDP ネイバーのリストを確認するには、必要なアクセス ポイントの **CDP Neighbors** リンクをクリックします。CDP > AP Neighbors ページが表示されます（図 4-32 を参照）。

図 4-32　CDP > AP Neighbors ページ

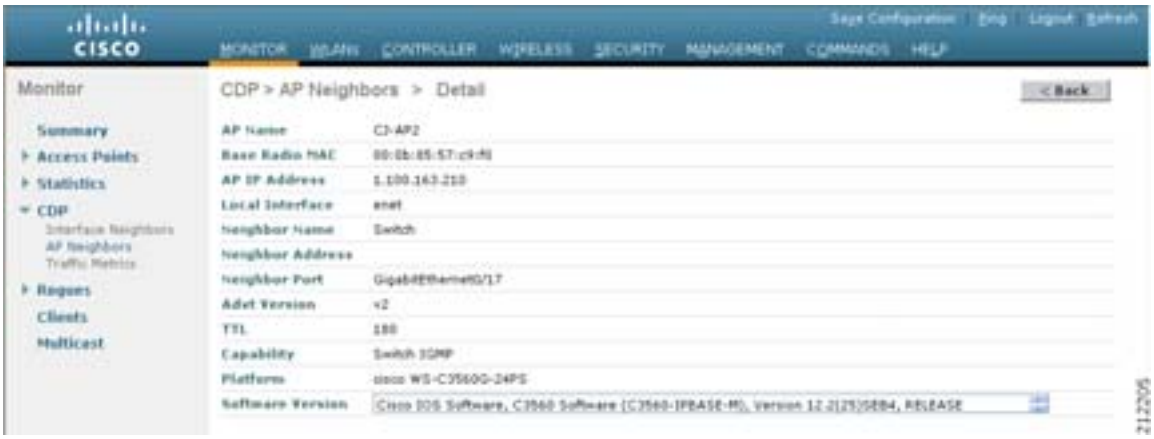
このページには、次の情報が表示されます。

- 各アクセス ポイントの名前
- 各アクセス ポイントの IP アドレス
- 各 CDP ネイバーの名前

- 各 CDP ネイバーの IP アドレス
- 各 CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）

ステップ 5　アクセス ポイントの CDP ネイバーの詳細情報を表示するには、必要なアクセス ポイントの名前をクリックします。CDP > AP Neighbors > Detail ページが表示されます（図 4-33 を参照）。

図 4-33　CDP > AP Neighbors > Detail ページ



このページには、次の情報が表示されます。

- アクセス ポイントの名前
- アクセス ポイントの無線の MAC アドレス
- アクセス ポイントの IP アドレス
- CDP パケットが受信されたインターフェイス
- CDP ネイバーの名前
- CDP ネイバーの IP アドレス
- CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン（v1 または v2）
- CDP ネイバーエントリの有効期間が切れるまでの残り時間（秒）
- CDP ネイバーの機能は、次のように定義されています。R：ルータ、T：転送ブリッジ、B：ソース ルート ブリッジ、S：スイッチ、H：ホスト、I：IGMP、r：リピータ、M：リモート管理デバイス
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 6　CDP のトラフィック情報を表示するには、**Traffic Metrics** をクリックします。CDP > Traffic Metrics ページが表示されます（図 4-34 を参照）。

図 4-34　CDP > Traffic Metrics ページ

このページには、次の情報が表示されます。

- コントローラで受信した CDP パケット数
- コントローラから送信した CDP パケット数
- チェックサム エラーが発生したパケット数
- メモリ不足のためにドロップされたパケット数
- 無効なパケット数

CLI を使用した Cisco Discovery Protocol の設定

コントローラ CLI を使用して CDP を設定するには、次のコマンドを使用します。

1. コントローラで CDP を有効または無効にするには、次のコマンドを入力します。

   config cdp {**enable** | **disable**}

   CDP は、デフォルトで有効になっています。

2. CDP メッセージを生成する間隔を指定するには、次のコマンドを入力します。

   config cdp timer *seconds*

   範囲は 5 ～ 254 秒で、デフォルト値は 60 秒です。

3. 生成された CDP パケットで有効時間値としてアドバタイズされる時間を指定するには、次のコマンドを入力します。

   config cdp holdtime *seconds*

   範囲は 10 ～ 255 秒で、デフォルト値は 180 秒です。

4. コントローラでサポートされる最高の CDP バージョンを指定するには、次のコマンドを入力します。

   config cdp advertise {**v1** | **v2**}

   デフォルト値は v1 です。

5. このコントローラに接続されたすべてのアクセス ポイントで CDP を有効または無効にするには、次のコマンドを入力します。

   config ap cdp {**enable** | **disable**} **all**

   config ap cdp disable all コマンドは、コントローラに接続されているすべてのアクセス ポイントおよび今後接続されるすべてのアクセス ポイントの CDP を無効化します。CDP は、コントローラまたはアクセス ポイントがリブートした後でも、現在および将来のアクセス ポイントの両方で無効化されたままです。CDP を有効にするには、**config ap cdp enable all** と入力します。

(注)　コントローラに接続しているすべてのアクセス ポイントで CDP を有効にした後、下記の 6 のコマンドを使用して個々のアクセス ポイントで CDP を無効にした後再び有効にできます。コントローラに接続されたすべてのアクセス ポイントで CDP を無効にした後、個々のアクセス ポイントで CDP を有効にしてから無効にすることはできません。

6. 特定のアクセス ポイントで CDP を有効または無効にするには、次のコマンドを入力します。

   config ap cdp {**enable** | **disable**} *Cisco_AP*

7. 設定を保存するには、次のコマンドを入力します。

   save config

CLI を使用した Cisco Discovery Protocol 情報の表示

次のコマンドを使用して、コントローラの CDP ネイバーに関する情報を取得します。

1. CDP のステータスを確認し、CDP プロトコル情報を表示するには、次のコマンドを入力します。

   show cdp

2. すべてのインターフェイスのすべての CDP ネイバーのリストを確認するには、次のコマンドを入力します。

   show cdp neighbors [**detail**]

   オプションの **detail** コマンドによって、コントローラの CDP ネイバーの詳細な情報が提供されます。

(注)　このコマンドは、コントローラの CDP ネイバーのみを表示します。コントローラのアソシエート アクセス ポイントの CDP ネイバーは表示されません。アクセス ポイントごとの CDP ネイバーのリストを表示するコマンドは、この後で説明します。

3. データベース内のすべての CDP エントリを表示するには、次のコマンドを入力します。

   show cdp entry all

4. 指定されたポートの CDP トラフィック情報（送受信されるパケット、CRC エラーなど）を表示するには、次のコマンドを入力します。

   show cdp traffic

5. 特定のアクセス ポイントの CDP ステータスを表示するには、次のコマンドを入力します。

   show ap cdp *Cisco_AP*

6. このコントローラに接続されたすべてのアクセス ポイントで CDP ステータスを表示するには、次のコマンドを入力します。

   show ap cdp all

7. 特定のアクセス ポイントのすべての CDP ネイバーのリストを確認するには、次のコマンドを入力します。

   show ap cdp neighbors [**detail**] *Cisco_AP*

(注)　CDP ネイバー情報は変更があった場合にのみ、アクセス ポイントからコントローラに送信されます。

8. コントローラに接続されているすべてのアクセス ポイントのすべての CDP ネイバーのリストを確認するには、次のコマンドを入力します。

   show ap cdp neighbors [**detail**] **all**

   show ap cdp neighbors all と入力すると、次のような情報が表示されます。

```
AP Name AP IP Neighbor Name  Neighbor IP Neighbor Port
-------- -------- -------------  ----------- -------------
AP0013.601c.0a0    10.76.108.123        6500-1   10.76.108.207  GigabitEthernet1/26
AP0013.601c.0b0    10.76.108.111        6500-1   10.76.108.207  GigabitEthernet1/27
AP0013.601c.0c0   10.76.108.125        6500-1    10.76.108.207  GigabitEthernet1/28
```

   show ap cdp neighbors detail all と入力すると、次のような情報が表示されます。

```
AP Name: AP0013.601c.0a0
AP IP Address: 10.76.108.125
----------------------------------
Device ID: 6500-1
Entry address(es): 10.76.108.207
Platform: cisco WS-C6506-E,  Capabilities: Router Switch IGMP
Interface: Port - 1,  Port ID (outgoing port): GigabitEthernet1/26
Holdtime: 157 sec

Version:
Cisco Internetwork Operating System Software  IOS (tm) s72033_rp Software
(s72033_rp-PSV-M), Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support:
http://www.cisco.com/techsupport Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Fri 13-Ma
```

（注） CDP ネイバー情報は変更があった場合にのみ、アクセス ポイントからコントローラに送信されます。

コントローラの CDP デバッグ情報を取得するには、次のコマンドを使用します。

1. CDP パケットに関連したデバッグ情報を取得するには、次のコマンドを入力します。

   debug cdp packets

2. CDP イベントに関連したデバッグ情報を取得するには、次のコマンドを入力します。

   debug cdp events

RFID タグ追跡の設定

コントローラでは、Radio-Frequency Identification（RFID）タグ追跡を設定できます。RFID タグは、小型の無線装置で、位置をリアルタイムで追跡するために資産に取り付けられます。タグはその位置を専用の 802.11 パケットを使用してアドバタイズすることで機能し、パケットは、アクセス ポイント、コントローラ、およびロケーション アプライアンスで処理されます。

コントローラでは、AeroScout、WhereNet、および Pango（InnerWireless）のタグがサポートされています。これらのベンダー企業のタグの一部は、RFID タグの Cisco Compatible Extensions に準拠しています。詳細は、表 4-3 を参照してください。ロケーション アプライアンスは、この CCX 仕様に準拠したタグからテレメトリ情報とチョークポイント情報を受け取ります。

表 4-3　RFID タグ用 Cisco Compatible Extensions の概要

パートナー	AeroScout		WhereNet	Pango（InnerWireless）
製品名	T2	T3	Wheretag IV	V3
テレメトリ				
温度	X	X		X
圧力				
湿度				
状態				
燃料				
量				
距離				
動作検出	X	X		X
パニック ボタンの数	1	2	0	1
改ざん		X	X	X
バッテリー情報	X	X	X	X
複数周波数タグ[1]	X	X	X	

1. チョークポイント システムでは、このタグは同じベンダー製のチョークポイント以外で機能しないことに注意してください。

（注） Network Mobility Services Protocol（NMSP; ネットワーク モビリティ サービス プロトコル）は、ロケーション アプライアンス ソフトウェア リリース 3.0 以降で動作します。NMSP が適切に機能するためには、コントローラおよびロケーション アプライアンスが通信を行う TCP ポート（16113）が、これらの 2 つのデバイス間にあるファイアウォールで開いた（ブロックされていない）状態である必要があります。NMSP および RFID タグの詳細は、『Cisco Location Appliance Configuration Guide, Release 3.0』を参照してください。

シスコ認定タグでは、次の機能がサポートされています。

- **情報通知**：ベンダー固有の情報および緊急情報を表示できます。
- **情報のポーリング**：バッテリのステータスおよびテレメトリ データを監視できます。さまざまな種類のテレメトリ データにより、知覚ネットワークおよび RFID タグの各種アプリケーションに対するサポートを提供します。
- **測定の通知**：ビルディングまたはキャンパス内の重要ポイントにあるチョークポイントに展開できます。決められたチョークポイントの近くに RFID タグが移動すると、タグはそのチョークポイントに対する自分の位置をアドバタイズするパケットの送信を開始します。

サポートされているタグの数は、コントローラ プラットフォームによって異なります。表 4-4 は、コントローラごとにサポートされているタグの数を示しています。

表 4-4　コントローラでサポートされる RFID タグの数

コントローラ	サポートされる RFID タグの数
Cisco WiSM	5000
4404	2500
4402	1250
Catalyst 3750G 統合型無線 LAN コントローラ スイッチ	1250
2106、2006	500
Cisco 28/37/38xx シリーズ サービス統合型ルータに内蔵されたコントローラ ネットワーク モジュール	500

RFID タグ追跡情報は、コントローラ CLI を使用して設定および表示できます。

CLI を使用した RFID タグ追跡の設定

CLI を使用して RFID タグ追跡パラメータを設定する手順は、次のとおりです。

ステップ 1　RFID タグ追跡を有効または無効にするには、次のコマンドを入力します。

config rfid status {**enable** | **disable**}

デフォルト値は有効（enable）です。

ステップ 2　静的なタイムアウト値（60 ～ 7200 秒）を指定するには、次のコマンドを入力します。

config rfid timeout *seconds*

静的なタイムアウト値は、タグの有効期限が切れるまで、コントローラで維持される期間です。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒（ビーコン値の約 3 倍）に設定することをお勧めします。デフォルト値は 1200 秒です。

ステップ 3　特定のタグに対する RFID タグのモビリティを有効または無効にするには、次のコマンドを入力します。

- **config rfid mobility** *vendor_name* **enable**：特定のベンダーのタグに対するクライアント モビリティを有効にします。このコマンドを入力すると、タグが設定を確認またはダウンロードしようとするとき、クライアント モードの DHCP アドレスを取得できなくなります。
- **config rfid mobility** *vendor_name* **disable**：特定のベンダーのタグに対するクライアント モビリティを無効にします。このコマンドを入力した場合、タグは DHCP アドレスを取得できます。タグがあるサブネットから別のサブネットへ移動すると、タグは、アンカー状態を維持するのではなく、新しいアドレスを取得します。

（注）　これらのコマンドは Pango タグに対してのみ使用できます。したがって、*vendor_name* に有効な入力は、すべて小文字の「pango」のみとなります。

CLI を使用した RFID タグ追跡情報の表示

コントローラ CLI を使用して RFID タグ追跡情報を表示するには、次のコマンドを使用します。

1. RFID タグ追跡の現在の設定を確認するには、次のコマンドを入力します。

   show rfid config

   次のような情報が表示されます。

```
RFID Tag data Collection..................... Enabled
RFID timeout................................. 1200 seconds
RFID mobility.............................. Oui:00:14:7e : Vendor:pango
   State:Disabled
```

2. 特定の RFID タグの詳細情報を表示するには、次のコマンドを入力します。

   show rfid detail *mac_address*

   ここで、*mac_address* は、タグの MAC アドレスです。

   次のような情報が表示されます。

```
RFID address................................. 00:12:b8:00:20:52
Vendor....................................... G2
Last Heard................................... 51 seconds ago
Packets Received............................. 2
Bytes Received............................... 324
Cisco Type...................................

Content Header
=================
Version...................................... 1
Tx Power..................................... 12 dBm
Channel...................................... 1
Reg Class.................................... 12
Burst Length................................. 1

CCX Payload
===========
Last Sequence Control........................ 0
Payload length............................... 127
Payload Data Hex Dump

01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03

Nearby AP Statistics:
      lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
      lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

3. コントローラに現在接続されているすべての RFID タグのリストを確認するには、次のコマンドを入力します。

   show rfid summary

   次のような情報が表示されます。

```
Total Number of RFID   : 24
----------------- -------- ----------------- ------ --------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ----------------- ------ --------------------
00:04:f1:00:00:03 Wherenet HReap               -70      151 seconds ago
00:04:f1:00:00:05 Wherenet HReap               -66      251 seconds ago
00:0c:cc:5b:f8:1e Aerosct  HReap               -40        5 seconds ago
00:0c:cc:5c:05:10 Aerosct  HReap               -68       25 seconds ago
00:0c:cc:5c:06:69 Aerosct  HReap               -54        7 seconds ago
00:0c:cc:5c:06:6b Aerosct  HReap               -68      245 seconds ago
00:0c:cc:5c:06:b5 Aerosct  cisco1242           -67       70 seconds ago
00:0c:cc:5c:5a:2b Aerosct  cisco1242           -68       31 seconds ago
00:0c:cc:5c:87:34 Aerosct  HReap               -40        5 seconds ago
00:14:7e:00:05:4d Pango    cisco1242           -66      298 seconds ago
```

4. コントローラにアソシエートされている RFID タグの一覧を確認するには、次のコマンドを入力します。

   show rfid client

   RFID タグがクライアント モードである場合は、次のような情報が表示されます。

```
----------------- -------- --------- ----------------- ------ ----------------
                            Heard
   RFID Mac         VENDOR   Sec Ago    Associated AP    Chnl    Client State
----------------- -------- --------- ----------------- ------ ----------------

00:14:7e:00:0b:b1   Pango      35    AP0019.e75c.fef4   1      Probing
```

   RFID タグがクライアント モードでない場合は、上記のフィールドは空白となります。

CLI を使用した RFID タグ追跡問題のデバッグ

RFID タグ追跡に関する問題が発生した場合は、次のデバッグ コマンドを使用します。

- MAC アドレスのデバッグを設定するには、次のコマンドを入力します。

  debug mac addr *mac_address*

  （注） タグごとにデバッグを実行することをお勧めします。すべてのタグに対してデバッグを有効にすると、コンソールまたは Telnet 画面に非常にたくさんのメッセージが表示されることになります。

- 802.11 RFID タグ モジュールのデバッグを有効または無効にするには、次のコマンドを入力します。

  debug dot11 rfid {**enable** | **disable**}

ロケーション設定の実行および表示

この項では、コントローラ CLI からロケーション設定を実行および表示する手順について説明します。

（注） 監視モードのアクセス ポイントをロケーション目的で使用しないようにしてください。

ロケーション アプライアンス証明書のインストール

自己署名証明書（SSC）は、ロケーション アプライアンス上で必要となります。この証明書はロケーション アプライアンスの MAC アドレスおよび 20 バイトのキーハッシュで構成され、コントローラ上に配置される必要があります。そうでない場合、コントローラによってロケーション アプライアンスが認証されず、接続を確立できません。WCS では、通常は自動で証明書がコントローラに送信されますが、必要に応じて（たとえば、コントローラを WCS に接続しない場合や、WCS でエラーや証明書の不一致が発生した場合）、コントローラ CLI を使用して証明書をコントローラにインストールできます。

（注） WCS でエラーが発生し、ロケーション アプライアンスの証明書をコントローラに送信しないようにする場合は、この手順に従う前に、コントローラとロケーション アプライアンスで時間帯が同期されていることを確認してください。確認は、「コントローラとロケーション アプライアンスの同期化」の項（P. 4-92）の手順に従ってください。

コントローラ上にロケーション アプライアンスの証明書をインストールする手順は、次のとおりです。

ステップ 1　ロケーション アプライアンスの証明書のキーハッシュ値を取得するには、次のコマンドを入力します。

debug pm pki enable

次のような情報が表示されます。

```
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  30820122 300d0609 2a864886 f70d0101
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  01050003 82010f00 3082010a 02820101
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  009a98b5 d2b7c77b 036cdb87 5bd20e5a
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  894c66f4 df1cbcfb fe2fcf01 09b723aa
Thu Oct 11 08:52:26 2007: sshpmGetIssuerHandles: Key Data  5c0917f1 ec1d5061 2d386351 573f2c5e
Thu Oct 11 08:52:30 2007: sshpmGetIssuerHandles: Key Data  b9020301 0001
Thu Oct 11 08:52:30 2007: sshpmGetIssuerHandles: SSC Key Hash is 4869b32638c00ffca88abe9b1a8e0525b9344b8b
```

ステップ 2　コントローラにロケーション アプライアンスの証明書をインストールするには、次のコマンドを入力します。

config auth-list add lbs-ssc *lbs_mac lbs_key*

このとき、次のようになります。

- *lbs_mac* は、ロケーション アプライアンスの MAC アドレスです。
- *lbs_key* は、証明書の 20 バイトのキーハッシュ値です。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　ロケーション　アプライアンス証明書がコントローラ上にインストールされていることを確認するには、次のコマンドを入力します。

show auth-list

次のような情報が表示されます。

```
Authorize APs against AAA ..................... disabled
Allow APs with Self-Signed Certificate (SSC) .... enabled

Mac Addr                  Cert Type    Key Hash
------------------------  ----------   ----------------------------------------
00:13:80:60:48:3e         SSC        ecefbb0622ef76c997ac7d73e413ee499e24769e
```

コントローラとロケーション アプライアンスの同期化

コントローラ ソフトウェア リリース 4.2 以降では、ロケーション アプライアンス（リリース 3.1 以降）がネットワーク上にインストールされている場合は、2 つのシステム間で正しく同期されるように、コントローラ上で時間帯が設定されている必要があります。また、ロケーション アプライアンスのないネットワークに時刻を設定することを強くお勧めします。コントローラ上で時刻と日付を設定する手順については、「システムの日時の管理」の項（P. 4-11）を参照してください。

（注）　時間帯はコントローラとロケーション アプライアンスとで異なる可能性がありますが、時間帯 デルタは GMT に基づいて設定されていなければなりません。

CLI を使用したロケーション設定の表示

コントローラでは、すべての対象クライアント周辺のアクセス ポイントから Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）測定を収集することにより、クライアント デバイスのロケーションを特定します。コントローラは、クライアントおよび RFID タグ両方について、最大 16 のアクセス ポイントからロケーション レポートを取得できます。

コントローラ CLI を使用してロケーション情報を表示するには、次のコマンドを使用します。

1. 現在のロケーション設定値を表示するには、次のコマンドを入力します。

   show location summary

   次のような情報が表示されます。

```
Location Summary :

 Algorithm used:                          Average
 Client RSSI expiry timeout:              150 sec, half life: 60 sec
 Calibrating Client RSSI expiry timeout: 30 sec, half life: 0 sec
 Rogue AP RSSI expiry timeout:            1200 sec, half life: 120 sec
 RFID Tag RSSI expiry timeout:          60 sec, half life: 120 sec
```

2. ロケーションベースの RFID 統計を表示するには、次のコマンドを入力します。

   show location statistics rfid

   次のような情報が表示されます。

```
RFID Statistics

Database Full :          0        Failed Delete:          0
Null Bufhandle:          0        Bad Packet:             0
Bad LWAPP Data:          0        Bad LWAPP Encap:        0
Off Channel:             0        Bad CCX Version:        0
Bad AP Info :            0
Above Max RSSI:          0        Below Max RSSI:         0
Invalid RSSI:            0        Add RSSI Failed:        0
Oldest Expired RSSI:  0         Smallest Overwrite:  0
```

3. ロケーションベースの RFID 統計をクリアするには、次のコマンドを入力します。

   clear location statistics rfid

4. 特定の RFID タグまたはデータベース全体のすべての RFID タグをクリアするには、次のコマンドを入力します。

   clear location rfid {*mac_address* | **all**}

5. クライアントでロケーション表示 (S69) がサポートされているかどうかを表示するには、次のコマンドを入力します。

   show client detail *client_mac*

   ロケーション表示がクライアントでサポートされていて、ロケーション サーバで有効になっている場合、ロケーション サーバは要求に応じてクライアントにそのロケーションを提供できます。CCXv5 クライアントでは、ロケーション表示は自動的に有効になります。

   次のような情報が表示されます。

```
Client MAC Address..............................  00:40:96:b2:a3:44
Client Username ................................  N/A
AP MAC Address..................................  00:18:74:c7:c0:90
Client State....................................  Associated
Wireless LAN Id.................................  1
BSSID...........................................  00:18:74:c7:c0:9f
Channel.........................................  56
IP Address......................................  192.168.10.28
Association Id..................................  1
Authentication Algorithm........................  Open System
Reason Code.....................................  0
Status Code.....................................  0
Session Timeout.................................  0
Client CCX version..............................  5
Client E2E version..............................  No E2E support
Diagnostics Capability..........................  Supported
S69 Capability..................................  Supported
Mirroring.......................................  Disabled
QoS Level.......................................  Silver
...
```

(注) ロケーション サーバでロケーション表示を有効にする手順については、『Cisco Wireless Control System Configuration Guide, Release 5.0』または『Cisco Location Appliance Configuration Guide, Release 4.0』を参照してください。

6. アクティブな Network Mobility Services Protocol（NMSP）接続のステータスを確認するには、次のコマンドを入力します。

   show nmsp status

   次のような情報が表示されます。

```
LocServer IP    TxEchoResp RxEchoReq  TxData  RxData
--------------- ---------- ---------  ------- -------
171.71.132.158   21642       21642  51278   21253
```

7. NMSP カウンタを確認するには、次のコマンドを入力します。

   show nmsp statistics {summary | connection all}

   このとき、次のようになります。

   - **summary** を指定すると、一般的な NMSP カウンタが表示されます。
   - **connection all** を指定すると、その接続固有の NMSP カウンタが表示されます。

   show nmsp statistics summary コマンドに対しては、次のような情報が表示されます。

```
NMSP Global Counters

Client Measure Send Fail:               0
Tag Measure Send Fail:                  0
Rouge AP Measure Send Fail:             0
Rouge Client Measure Send Fail:         0
Client Info Send Fail:                  0
Rouge AP Info Send Fail:                0
Rouge Client Info Send Fail:            0
Send RSSI with no entry:                0
Send too big msg:                       0
Partial SSL write:                      0
Transmit Q full:                        0
Measmt Send Not Called:                 0
Info Send Not Called:                   0
Max Measure Notify Msg:                 0
Max Info Notify Msg:                    0
Max Tx Q Size:                          0
Max Rx Size:                            0
Max Info Notify Q Size:                 0
Max Client Info Notify Delay:           0
Max Rouge AP Info Notify Delay:         0
Max Rouge Client Info Notify Delay:     0
Max Client Measure Notify Delay:        0
Max Tag Measure Notify Delay:           0
Max Rouge AP Measure Notify Delay:      0
Max Rouge Client Measure Notify Delay:  0
Max Client Stats Notify Delay:          0
Max Tag Stats Notify Delay:          0
```

8. NMSP 統計をクリアするには、次のコマンドを入力します。

   clear nmsp statistics

WiSM をサポートする Supervisor 720 の設定

Cisco Catalyst 6500 スイッチまたは Cisco 7600 シリーズ ルータに Wireless Services Module（WiSM; ワイヤレス サービス モジュール）をインストールする場合、WiSM をサポートする Supervisor 720 を設定する必要があります。スーパーバイザによって WiSM が検出されると、Gig*slot*/1 ～ Gig*slot*/8 の範囲で 10 ギガビット イーサネット インターフェイスが作成されます。たとえば、WiSM がスロット 9 にある場合は、スーパーバイザによってインターフェイス Gig9/1 ～ Gig9/8 が作成されます。8 番目までのギガビット イーサネット インターフェイスでは、それぞれ 4 つのインターフェイスを含む 2 つの Etherchannel バンドルにまとめる必要があります。残り 2 つの ギガビット イーサネット インターフェイスは、WiSM 上の各コントローラに 1 つずつ、サービス ポート インターフェイスとして使用されます。WiSM のポートと通信する VLAN を手動で作成する必要があります。

（注） WiSM は、Cisco IOS Release 12.2(18)SXF5 のみを実行する Cisco 7600 シリーズ ルータでサポートされています。

WisM に関する一般的なガイドライン

WiSM をネットワークに追加する場合は、次の点に注意してください。

- コントローラ サービス ポートにつながっているスイッチ ポートやルータ ポートは自動的に設定されます。手動では設定できません。
- コントローラ データ ポートへのスイッチ ポートやルータ ポートは、不要な Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）の送信を避けるため、エッジ ポートとして設定する必要があります。
- コントローラ データ ポートへのスイッチ ポートやルータ ポートには、コントローラとのデータ トラフィックの送受信に必要な設定以外の追加設定（ポート チャネル、Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）の宛先など）を設定しないでください。
- WiSM コントローラはレイヤ 3 の LWAPP モードをサポートしますが、レイヤ 2 の LWAPP モードはサポートしません。

（注） WiSM のポートとインターフェイスの設定方法は、第 3 章を参照してください。

スーパーバイザの設定

スイッチ CLI またはルータ CLI にログオンし、Priveleged Exec モードで開始した後、次の手順に従って WiSM をサポートするスーパーバイザを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル設定モードに移行します。
ステップ 2	**interface** *vlan*	WiSM のデータ ポートと通信する VLAN を作成し、インターフェイス設定モードに移行します。
ステップ 3	**ip address** *ip-address gateway*	IP アドレスとゲートウェイを VLAN に割り当てます。
ステップ 4	**ip helper-address** *ip-address*	ヘルパー アドレスを VLAN に割り当てます。
ステップ 5	**end**	グローバル設定モードに戻ります。

	コマンド	目的
ステップ 6	**wism module** *module_number* **controller** { **1** | **2**} **allowed-vlan** *vlan_number*	指定した WiSM コントローラに対するギガビット ポートチャネル インターフェイスを自動的に作成し、ポートチャネル インターフェイスをトランク ポートとして設定します。また、以前に作成した VLAN を、ポートチャネル トランク上で許可された VLAN として指定します。VLAN トラフィックは、トランク上で WiSM コントローラとスーパーバイザの間を送信されます。
ステップ 7	**wism module** *module_number* **controller** { **1** | **2**} **native-vlan** *vlan_number*	ポートのネイティブな VLAN の場合、WiSM データ ポートとの通信のために以前に作成した VLAN を指定します。
ステップ 8	**interface** *vlan*	WiSM のサービス ポートと通信する VLAN を作成します。
ステップ 9	**ip address** *ip_address gateway*	IP アドレスとゲートウェイを VLAN に割り当てます。
ステップ 10	**end**	グローバル設定モードに戻ります。
ステップ 11	**wism service-vlan** *vlan*	WiSM サービス ポートとの通信に手順 8 ～ 10 で作成した VLAN を設定します。
ステップ 12	**end**	グローバル設定モードに戻ります。
ステップ 13	**show wism status**	WiSM が正常に動作していることを確認します。

（注） Cisco WiSM、Supervisor 720、および 4404 コントローラ間の通信で使用されるコマンドについては、次の URL からアクセスできる『Configuring a Cisco Wireless Services Module and Wireless Control System』を参照してください。
http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html#wp39498

無線 LAN コントローラ ネットワーク モジュールの使用

Cisco サービス統合型ルータにインストールされた無線 LAN Controller Network Module（CNM; コントローラ ネットワーク モジュール）を使用する場合は、次の点に注意してください。

- CNM は IPSec をサポートしていません。CNM と IP セキュリティを使用するには、CNM がインストールされたルータの IP セキュリティを設定します。ルータへの IP セキュリティの設定手順を参照するには、次のリンクをクリックします。

  http://www.cisco.com/en/US/tech/tk583/tk372/tech_configuration_guides_list.html

- CNM にはバッテリがないため、時間設定を保存できません。電源を投入する際に、外部 NTP サーバから時間設定を受信する必要があります。モジュールをインストールする時点で、NTP サーバ情報を求める設定ウィザードのプロンプトが表示されます。

- CNM ブートローダにアクセスするには、ルータから CNM をリセットすることをお勧めします。CNM ユーザ インターフェイスから CNM をリセットすると、ブートローダの使用中にルータが CNM をリセットすることがあります。

  CNM インターフェイスから CNM をリセットした場合、17 分経過した時点で、ルータによって CNM が自動的にリセットされます。CNM ブートローダは Router Blade Configuration Protocol（RBCP）を実行しません。したがって、ルータで実行されている RBCP ハートビートは 17 分後にタイムアウトとなり、その結果、CNM がリセットされます。

  ルータから CNM をリセットした場合、そのルータは RBCP ハートビート交換を停止し、CNM がブートされるまで RBCP を再起動しません。ルータから CNM をリセットするには、ルータ CLI で次のいずれかのコマンドを入力します。

  service-module wlan-controller 1/0 reset（高速イーサネット CNM バージョンの場合）

  service-module integrated-service-engine 1/0 reset（ギガビット イーサネット CNM バージョンの場合）

- Controller Network Module のギガビット イーサネット バージョンは、Cisco IOS Release 12.4(11)T2 以降を実行している Cisco 28/37/38xx シリーズ サービス統合型ルータでサポートされています。

CHAPTER 5

セキュリティ ソリューションの設定

この章では、無線 LAN のセキュリティ ソリューションについて説明します。この章の内容は、次のとおりです。

Cisco UWN Solution のセキュリティ

Cisco UWN Solution セキュリティの内容は、次のとおりです。

セキュリティ概要

Cisco UWN セキュリティ ソリューションは、802.11 アクセス ポイントのセキュリティを構成する潜在的に複雑なレイヤ 1、レイヤ 2、およびレイヤ 3 を 1 つの単純なポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを WLAN 単位でカスタマイズできます。Cisco UWN セキュリティ ソリューションは、単純で、統一された、体系的なセキュリティ管理ツールを提供します。

企業での WLAN 展開の最も大きな障害の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy（WEP）です。低価格のアクセス ポイントの登場も新たな問題であり、それらは企業ネットワークに接続して man-in-the-middle 攻撃や DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。また、次々に追加されるセキュリティ ソリューションの複雑さから、多くの IT マネージャが WLAN セキュリティの最新技術を採用することをためらっています。

レイヤ 1 ソリューション

Cisco UWN セキュリティ ソリューションによって、すべてのクライアントは、アクセスの試行回数をオペレータが設定した回数までに制限されます。クライアントがその制限回数内にアクセスできなかった場合、そのクライアントは、オペレータが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。オペレーティング システムでは、WLAN ごとに SSID ブロードキャストを無効にすることもできます。

レイヤ 2 ソリューション

上位レベルのセキュリティと暗号化が必要な場合、ネットワーク管理者は、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）や Wi-Fi Protected Access（WPA）、および WPA2 など業界標準のセキュリティ ソリューションも実装できます。Cisco UWN Solution の WPA 実装には、Advanced Encryption Standard（AES）動的キー、Temporal Key Integrity Protocol + Message Integrity Code Checksum（TKIP + Michael）動的キー、WEP 静的キーが含まれます。無効化も使用され、オペレータが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ 2 アクセスがブロックされます。

どの無線セキュリティ ソリューションを採用した場合も、コントローラと Lightweight アクセス ポイントとの間のすべてのレイヤ 2 有線通信は、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）トンネルを使用してデータを渡すことにより保護されます。

レイヤ 3 ソリューション

WEP 問題は、パススルー Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のような業界標準のレイヤ 3セキュリティ ソリューションを使用すると、さらに進んだ解決が可能です。

Cisco UWN Solution では、ローカルおよび RADIUS Media Access Control（RADIUS MAC; RADIUS メディア アクセス制御）フィルタリングがサポートされています。このフィルタリングは、802.11 アクセス カード MAC アドレスの既知のリストがある小規模のクライアント グループに適しています。

さらに、Cisco UWN Solution では、ローカルおよび RADIUS ユーザおよびパスワード認証がサポートされています。この認証は、小規模から中規模のクライアント グループに適しています。

統合されたセキュリティ ソリューション

- Cisco UWN Solution オペレーティング システムのセキュリティは、堅牢な 802.1X AAA（認証、認可、アカウンティング）エンジンを中心に構築されており、オペレータは、Cisco UWN Solution 全体にわたってさまざまなセキュリティ ポリシーを迅速に設定および適用できます。
- コントローラおよび Lightweight アクセス ポイントには、システム全体の認証および認可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステム セキュリティが提供されています。
- オペレーティング　システムのセキュリティ　ポリシーは個別の　WLAN　に割り当てられ、Lightweight アクセス ポイントは設定されたすべての WLAN（最大 16）に同時にブロードキャストします。これにより、干渉を増加させ、システム スループットを低下させる可能性があるアクセス ポイントを追加する必要はなくなります。
- オペレーティング システム セキュリティは、RRM 機能を使用して、干渉およびセキュリティ侵犯がないか継続的に空間を監視し、それらを検出したときはオペレータに通知します。
- オペレーティング システム セキュリティは、業界標準の AAA（認証、認可、アカウンティング）サーバで動作し、システム統合が単純で簡単です。

RADIUS の設定

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント / サーバ プロトコルです。このプロトコルは、ローカル認証や TACACS+ 認証と同様に、バックエンドのデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。

（注） 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンド データベースが試行される順序を指定できます。

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUS アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUS アカウンティング サーバが接続不能になった場合、ユーザはセッションを続行できなくなります。

RADIUS では、転送に User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用します。UDP では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

RADIUS 認証サーバおよびアカウンティング サーバは、それぞれ最大 17 台まで設定できます。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

（注） 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。

プライマリ RADIUS サーバ（最も低いサーバ インデックスを持つサーバ）は、コントローラに最も適していると想定されています。プライマリ サーバが応答しなくなると、コントローラは、次にアクティブなバックアップ サーバ（低い方から 2 番目のサーバ インデックスを持つサーバ）に切り替えます。コントローラは、プライマリ RADIUS サーバが回復して応答するようになったときにそのサーバにフォールバックするように設定されているか、使用可能なバックアップ サーバのうちのより適切なサーバにフォールバックするように設定されていない限り、このバックアップ サーバを引き続き使用します。

CiscoSecure Access Control Server（ACS）とコントローラの両方で、RADIUS を設定する必要があります。コントローラは、GUI または CLI のいずれかを使用して設定できます。

ACS 上での RADIUS の設定

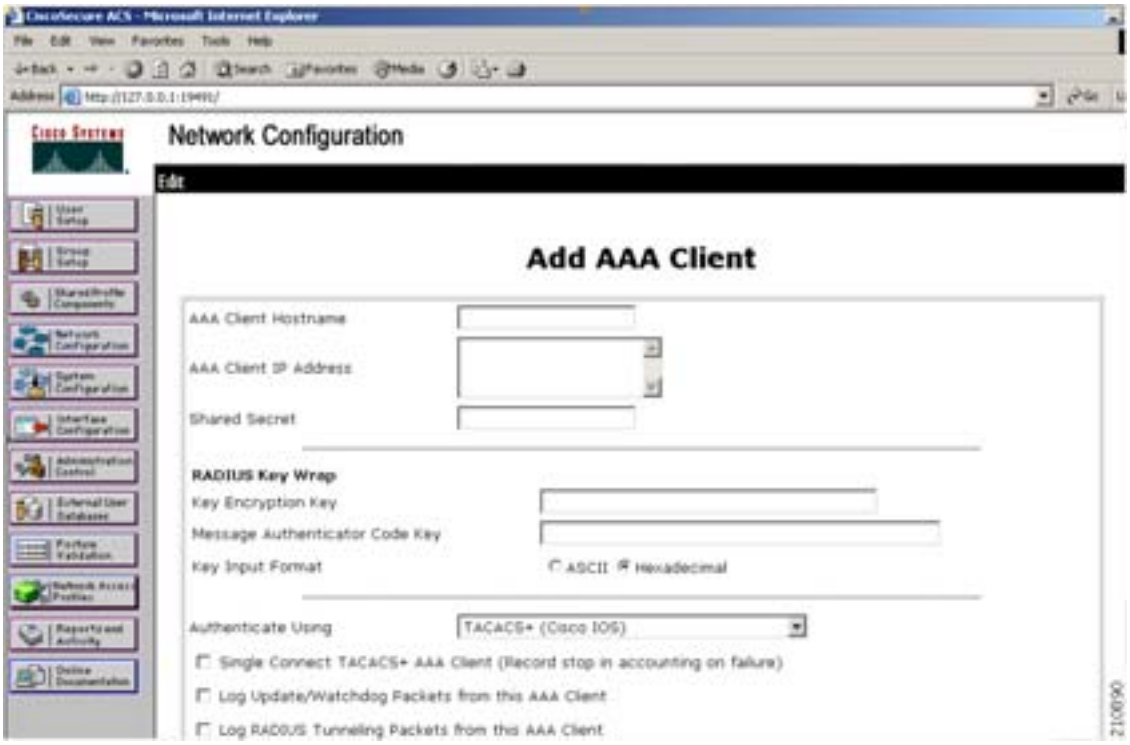
ACS 上で RADIUS を設定する手順は、次のとおりです。

（注） RADIUS は、CiscoSecure ACS バージョン 3.2 以上でサポートされます。この項に示される手順および図は、ACS バージョン 4.1 に関連するもので、他のバージョンでは異なる場合があります。実行中のバージョンの CiscoSecure ACS マニュアルを参照してください。

ステップ 1　ACS のメイン ページで、**Network Configuration** をクリックします。

ステップ 2　AAA Clients の下の **Add Entry** をクリックし、使用しているコントローラをサーバに追加します。Add AAA Client ページが表示されます（図 5-1 を参照）。

図 5-1　CiscoSecure ACS 上の Add AAA Client ページ



ステップ 3　AAA Client Hostname フィールドに、コントローラの名前を入力します。

ステップ 4　AAA Client IP Address フィールドに、コントローラの IP アドレスを入力します。

ステップ 5　Shared Secret フィールドに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注） 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 6　Authenticate Using ドロップダウン ボックスから **RADIUS (Cisco Aironet)** を選択します。

ステップ 7　**Submit + Apply** をクリックして、変更内容を保存します。

ステップ 8　ACS のメイン ページで、**Interface Configuration** をクリックします。

ステップ 9　**RADIUS (Cisco Aironet)** をクリックします。RADIUS (Cisco Aironet) ページが表示されます。

ステップ 10　User Group の **Cisco-Aironet-Session-Timeout** チェックボックスをオンにします。

ステップ 11　**Submit** をクリックして、変更内容を保存します。

ステップ 12　ACS のメイン ページで、**System Configuration** をクリックします。

ステップ 13　**Logging** をクリックします。

ステップ 14　Logging Configuration ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

ステップ 15　ACS のメイン ページで、**Group Setup** をクリックします。

ステップ 16　Group ドロップダウン ボックスから、以前に作成したグループを選択します。

（注）　この手順により、ユーザが割り当てられることになるロールに基づいて、ACS 上のグループにすでにユーザを割り当てていることを確認します。

ステップ 17　**Edit Settings** をクリックします。Group Setup ページが表示されます。

ステップ 18　**Cisco Aironet Attributes** の **Cisco-Aironet-Session-Timeout** チェックボックスをオンにして、編集ボックスにセッション タイムアウト値を入力します。

ステップ 19　RADIUS　認証を使用したコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、Service-Type 属性（006）を設定します。読み取り専用アクセスが必要な場合は **Callback NAS Prompt** に対してこの属性を設定し、読み取りと書き込みの両方の権限が必要な場合は **Administrative** に対して設定してください。この属性を設定しない場合、認証プロセスはコントローラ上での認可エラーなしで正常に完了しますが、認証を再試行するようにプロンプトが表示されることがあります。

（注）　ACS 上で Service-Type 属性を設定する場合は、コントローラの GUI の RADIUS Authentication Servers ページ上にある **Management** チェックボックスを必ずオンにします。詳細は、次の項のステップ 17 を参照してください。

（注）　「アクセス ポイントによって送信される RADIUS 属性」の項（P. 5-16）には、RADIUS 属性の一覧が示されています。この属性は、Access-Request パケットおよび Access-Accept パケットで Lightweight アクセス ポイントからクライアントに送信されます。

ステップ 20　**Submit** をクリックして、変更内容を保存します。

GUI を使用した RADIUS の設定

コントローラの GUI を使用して RADIUS を設定する手順は、次のとおりです。

ステップ 1　**Security** > **AAA** > **RADIUS** の順にクリックします。

ステップ 2　次のいずれかの操作を行います。

- RADIUS サーバを認証用に設定する場合は、**Authentication** をクリックします。
- RADIUS サーバをアカウンティング用に設定する場合は、**Accounting** をクリックします。

（注）　認証およびアカウンティングの設定に使用される GUI ページには、ほとんど同じフィールドが含まれています。そのため、ここでは Authentication ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

RADIUS Authentication（または Accounting）Servers ページが表示されます（図 5-2 を参照）。

図 5-2　RADIUS Authentication Servers ページ

このページには、これまでに設定されたすべての RADIUS サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。
- コントローラが特定のサーバに接続できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Ping** を選択します。

ステップ 3　Call Station ID Type ドロップダウン ボックスから、**IP Address**、**System MAC Address**、または **AP MAC Address** を選択して、送信側の IP アドレス、システムの MAC アドレス、または AP MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定します。

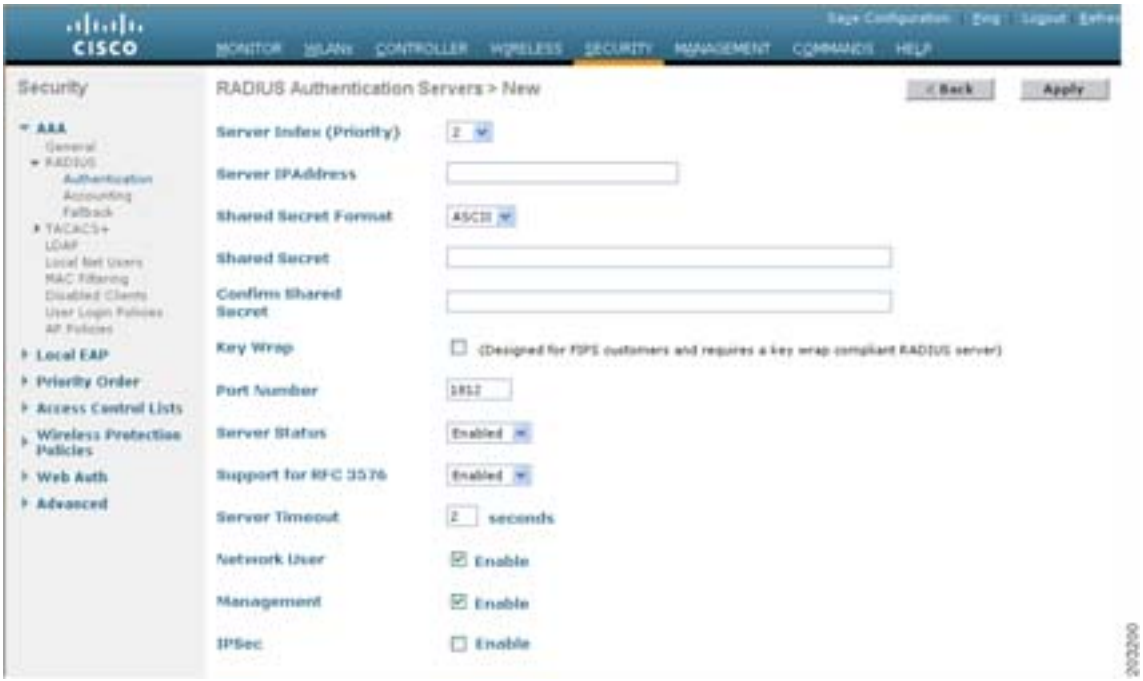
ステップ 4　AES キー ラップ保護を使用して RADIUS からコントローラへのキーの転送を有効にするには、**Use AES Key Wrap** チェックボックスをオンにします。デフォルトではオフになっています。この機能は、FIPS を使用するユーザにとって必要です。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　次のいずれかの操作を行います。

- 既存の RADIUS サーバを編集するには、そのサーバのサーバ インデックス番号をクリックします。RADIUS Authentication（または Accounting）Servers > Edit ページが表示されます。
- RADIUS サーバを追加するには、**New** をクリックします。RADIUS Authentication（または Accounting）Servers > New ページが表示されます（図 5-3 を参照）。

図 5-3　RADIUS Authentication Servers > New ページ



ステップ 7　新しいサーバを追加する場合、Server Index (Priority) ドロップダウン ボックスから数字を選択し、同じサービスを提供するその他の設定済みの RADIUS サーバに対するこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラは、最初のサーバに接続できない場合、必要に応じてリスト内の 2 番目や 3 番目あるいはそれ以降のサーバへの接続を試行します。

ステップ 8　新しいサーバを追加する場合は、Server IP Address フィールドに、RADIUS サーバの IP アドレスを入力します。

ステップ 9　Shared Secret Format ドロップダウン ボックスから、**ASCII** または **Hex** を選択し、コントローラと RADIUS サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は ASCII です。

ステップ 10　Shared Secret フィールドおよび Confirm Shared Secret フィールドに、コントローラとサーバ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 11 新しい RADIUS 認証サーバを設定して AES キー ラップを有効にすると、コントローラと RADIUS サーバ間の共有秘密キーの安全性を高めることができます。そのための手順は、次のとおりです。AES キー ラップは、Federal Information Processing Standards (FIPS) 顧客のために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

a. **Key Wrap** チェックボックスをオンにします。Key Wrap Format ドロップダウン ボックスから **ASCII** または **Hex** を選択し、Key Encryption Key（KEK）または Message Authentication Code Key（MACK）のどちらかの AES キー ラップ キーの形式を指定します。Key Encryption Key (KEK) and Message Authentication Code Key (MACK).

b. Key Encryption Key (KEK) フィールドに、16 バイトの KEK を入力します。

c. Message Authentication Code Key (MACK) フィールドに、20 バイトの KEK を入力します。

ステップ 12 新しいサーバを追加する場合は、Port Number フィールドに、インターフェイス プロトコルに対する RADIUS サーバの UDP ポート番号を入力します。有効な値の範囲は 1 ～ 65535 で、認証用のデフォルト値は 1812、アカウンティング用のデフォルト値は 1813 です。

ステップ 13 Server Status フィールドから **Enabled** を選択してこの RADIUS サーバを有効にするか、**Disabled** を選択して無効にします。デフォルト値は Enabled です。

ステップ 14 新しい RADIUS 認証サーバを設定する場合は、Support for RFC 3576 ドロップダウン ボックスから **Enabled** を選択して RFC 3576 を有効にするか、**Disabled** を選択してこの機能を無効にします。RFC 3576 では、ユーザ セッションへの動的な変更を可能にするよう RADIUS プロトコルが拡張されています。デフォルト値は Enabled です。RFC 3576 では、ユーザの切断およびユーザ セッションに適用される認可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。Disconnect メッセージは、ユーザ セッションをただちに中断させる原因となります。一方、CoA メッセージでは、データ フィルタなどのセッション認可属性が変更されます。

ステップ 15 Server Timeout フィールドに、再送信の間隔（秒数）入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

（注） 再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 16 ネットワーク ユーザ認証（アカウンティング）を有効にする場合は **Network User** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証（アカウンティング）サーバと見なされます。WLAN 上で RADIUS サーバ エントリを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。

ステップ 17 RADIUS 認証サーバを設定するには、**Management** チェックボックスをオンにして管理認証を有効にするか、オフにしてこの機能を無効にします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。

ステップ 18 IP セキュリティ メカニズムを有効にする場合は **IPSec** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルトではオフになっています。

（注） IPSec オプションは、Crypto カードがコントローラに取り付けられている場合に限り表示されます。

ステップ 19 ステップ 18 で IPSec を有効にした場合は、次の手順に従って追加の IPSec パラメータを設定します。

a. IPSec ドロップダウン ボックスから、IP セキュリティで使用する認証プロトコルとして、**HMAC MD5** または **HMAC SHA1** のいずれかのオプションを選択します。デフォルト値は HMAC SHA1 です。

Message Authentication Code（MAC; メッセージ認証コード）は、秘密キーを共有する 2 者間で送信される情報を検証するために使用されます。Hash Message Authentication Codes（HMAC）は、暗号ハッシュ関数に基づくメカニズムであり、任意の反復暗号ハッシュ関数との組み合わせで使用できます。HMAC でハッシュ関数として MD5 を使用するのが HMAC MD5 であり、SHA1 を使用するのが HMAC SHA1 です。また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。

b. IPSec Encryption ドロップダウン ボックスで次のオプションのいずれかを選択して、IP セキュリティ暗号化メカニズムを指定します。

- **DES**：Data Encryption Standard（DES; データ暗号化規格）は、プライベート（秘密）キーを使用するデータ暗号化の方法です。DES では、56 ビットのキーを 64 ビットのデータ ブロックごとに適用します。
- **3DES**：連続して 3 つのキーを適用するデータ暗号化規格ですこれはデフォルト値です。
- **AES CBS**：Advanced Encryption Standard では、128、192、または 256 ビット長のキーを使用して 128、192、または 256 ビット長のデータ ブロックを暗号化します。AES 128 CBC では、Cipher Block Chaining（CBC; 暗号ブロック連鎖）モードで 128 ビットのデータ パスを使用します。

c. IKE Phase 1 ドロップダウン ボックスから、**Aggressive** または **Main** のいずれかのオプションを選択して、Internet Key Exchange（IKE; インターネット キー エクスチェンジ）プロトコルを指定します。デフォルト値は Aggressive です。

IKE Phase 1 は、IKE の保護方法をネゴシエートするために使用されます。Aggressive モードでは、セキュリティ ゲートウェイの ID をクリアで送信するだけで、わずかに高速な接続が確立され、より少ないパケットでより多くの情報が渡されます。

d. Lifetime フィールドに、値（秒単位）を入力してセッションのタイムアウト間隔を指定します。有効な範囲は 1800 ～ 57600 秒で、デフォルト値は 1800 秒です。

e. IKE Diffie Hellman Group ドロップダウン ボックスから、**Group 1 (768 bits)**、**Group 2 (1024 bits)**、または **Group 5 (1536 bits)** のいずれかのオプションを選択して、IKE Diffie Hellman グループを指定します。デフォルト値は Group 1 (768 bits) です。

Diffie Hellman 技術を 2 つのデバイスで使用して共通キーを生成します。このキーを使用すると、値を公開された状態で交換して、同じ共通キーを生成することができます。3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。ただし、Group 1 および Group 2 のキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。

ステップ 20 **Apply** をクリックして、変更を適用します。

ステップ 21 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 22 同じサーバ上または追加の RADIUS サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 23 RADIUS サーバのフォールバック動作を指定する手順は、次のとおりです。

a. **Security** > **AAA** > **RADIUS** > Fallback の順にクリックして、RADIUS > Fallback Parameters ページを開きます（図 5-4 を参照）。

図 5-4　RADIUS > Fallback Parameters ページ

b. Fallback Mode ドロップダウン ボックスから、次のいずれかのオプションを選択します。

- **Off**：RADIUS サーバのフォールバックを無効にします。これはデフォルト値です。
- **Passive**：コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバから（より低いサーバ インデックスを持つ）適切なサーバへの復帰を実行するようにします。コントローラは、ある期間だけすべての非アクティブ サーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。
- **Active**：コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバから（より低いサーバ インデックスを持つ）適切なサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。コントローラは、すべてのアクティブ RADIUS 要求に対して、すべての非アクティブ サーバを無視します。

c. 手順 b. でフォールバック モードを Active にした場合は、非アクティブなサーバ プローブで送信される名前を Username フィールドに入力します。最大 16 文字の英数字を入力できます。デフォルト値は「cisco-probe」です。

d. 手順 b. でフォールバック モードを Active にした場合は、Sec フィールドの Interval にプローブ間隔値（秒単位）を入力します。この間隔は、Passive モードでの非アクティブ時間、および Active モードでのプローブ間隔としての意味を持ちます。有効な範囲は 180 ～ 3600 秒で、デフォルト値は 300 秒です。

ステップ 24 複数のデータベースを設定する際の認証の順序を指定するには、**Security** > **Priority Order** > **Management User** の順にクリックします。Priority Order > Management User ページが表示されます（図 5-5 を参照）。

図 5-5　Priority Order > Management User ページ

ステップ 25　Authentication Priority で、**Radius** または **TACACS+** のどちらかを指定して、コントローラが管理ユーザの認証を試行するときにどちらのサーバが他方に対して優先されるかを指定します。デフォルトで、ローカル データベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは TACACS+ に設定されている場合は TACACS+ サーバに切り替え、RADIUS に設定されている場合は RADIUS サーバに切り替えます。デフォルトの設定はローカル、Radius の順になっています。

ステップ 26　**Apply** をクリックして、変更を適用します。

ステップ 27　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した RADIUS の設定

コントローラの CLI を使用して RADIUS を設定する手順は、次のとおりです。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した RADIUS の設定」の項（P. 5-7）を参照してください。

ステップ 1　送信側の IP アドレス、システムの MAC アドレス、または AP MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定するには、次のコマンドを入力します。

config radius callStationIdType {*ip_address*, *mac_address*, *ap_mac_address*, *ap_macaddr_ssid*}

ステップ 2　RADIUS 認証サーバを設定するには、次のコマンドを使用します。

- **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：RADIUS 認証サーバを追加します。
- **config radius auth keywrap {enable** | **disable}**：AES キー ラップを有効にします。これによって、コントローラと RADIUS サーバ間の共有秘密キーの安全性が高まります。AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。
- **config radius auth keywrap add {ascii** | **hex}** *kek mack index*：AES キー ラップ属性を設定します。
  - *kek* では、16 バイトの Key Encryption Key（KEK）が指定されます。
  - *mack* では、20 バイトの Message Authentication Code Key（MACK）が指定されます。
  - *index* では、AES キー ラップを設定する RADIUS 認証サーバのインデックスが指定されます。
- **config radius auth rfc3576 {enable** | **disable}** *index*：RFC 3576 を有効または無効にします。RFC 3576 では、ユーザ セッションへの動的な変更を可能にするように RADIUS プロトコルが拡張されています。RFC 3576 では、ユーザの切断およびユーザ セッションに適用される認可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。Disconnect メッセージは、ユーザ セッションをただちに中断させる原因となります。一方、CoA メッセージでは、データ フィルタなどのセッション認可属性が変更されます。
- **config radius auth retransmit-timeout** *index timeout*：RADIUS 認証サーバの再送信のタイムアウト値を設定します。

- **config radius auth network** *index* **{enable** | **disable}**：ネットワーク ユーザ認証を有効または無効にします。この機能を有効にすると、ここここで設定するサーバはネットワーク ユーザの RADIUS 認証サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius auth management** *index* **{enable** | **disable}**：管理認証を有効または無効にします。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。
- **config radius auth ipsec** {**enable** | **disable**} *index*：IP セキュリティ メカニズムを有効または無効にします。
- **config radius auth ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*：IP セキュリティに使用する認証プロトコルを設定します。
- **config radius auth ipsec encryption** {**3des** | **aes** | **des** | **none**} *index*：IP セキュリティ暗号化メカニズムを設定します。
- **config radius auth ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *index*：IKE Diffie Hellman グループを設定します。
- **config radius auth ipsec ike lifetime** *interval index*：セッションのタイムアウト間隔を設定します。
- **config radius auth ipsec ike phase1**{**aggressive** | **main**} *index*：Internet Key Exchange（IKE）プロトコルを設定します。
- **config radius auth** {**enable** | **disable**} *index*：RADIUS 認証サーバを有効または無効にします。
- **config radius auth delete** *index*：以前に追加された RADIUS 認証サーバを削除します。

ステップ 3　RADIUS アカウンティング サーバを設定するには、次のコマンドを使用します。

- **config radius acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：RADIUS アカウンティング サーバを追加します。
- **config radius acct server-timeout** *index timeout*：RADIUS アカウンティング サーバの再送信のタイムアウト値を設定します。
- **config radius acct network** *index* **{enable** | **disable}**：ネットワーク ユーザ アカウンティングを有効または無効にします。この機能を有効にすると、ここここで設定するサーバはネットワーク ユーザの RADIUS アカウンティング サーバと見なされます。WLAN 上で RADIUS サーバ エントリを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius acct ipsec** {**enable** | **disable**} *index*：IP セキュリティ メカニズムを有効または無効にします。
- **config radius acct ipsec authentication** {**hmac-md5** | **hmac-sha1**} *index*：IP セキュリティに使用する認証プロトコルを設定します。
- **config radius acct ipsec encryption** {**3des** | **aes** | **des** | **none**} *index*：IP セキュリティ暗号化メカニズムを設定します。
- **config radius acct ipsec ike dh-group** {**group-1** | **group-2** | **group-5**} *index*：IKE Diffie Hellman グループを設定します。
- **config radius acct ipsec ike lifetime** *interval index*：セッションのタイムアウト間隔を設定します。
- **config radius acct ipsec ike phase1**{**aggressive** | **main**} *index*：Internet Key Exchange（IKE）プロトコルを設定します。
- **config radius acct** {**enable** | **disable**} *index*：RADIUS アカウンティング サーバを有効または無効にします。
- **config radius acct delete** *index*：以前に追加された RADIUS アカウンティング サーバを削除します。

ステップ 4　RADIUS サーバのフォールバック動作を設定するには、次のコマンドを入力します。

config radius fallback-test mode {**off** | **passive** | **active**}

- **Off** は、RADIUS サーバのフォールバックを無効にします。
- **Passive** は、コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバから（より低いサーバ インデックスを持つ）適切なサーバへの復帰を実行するようにします。コントローラは、ある期間だけすべての非アクティブ サーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。
- **Active** は、コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバから（より低いサーバ インデックスを持つ）適切なサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。コントローラは、すべてのアクティブ RADIUS 要求に対して、すべての非アクティブ サーバを無視します。

ステップ 5　ステップ 4 で Active モードを有効にした場合は、次のコマンドを入力して追加のフォールバック パラメータを設定します。

- **config radius fallback-test username** *username*：非アクティブなサーバ プローブで送信する名前を指定します。*username* パラメータには、最大 16 文字の英数字を入力できます。
- **config radius fallback-test interval** *interval*：プローブ間隔（秒単位）を指定します。

ステップ 6　変更を保存するには、次のコマンドを入力します。

save config

ステップ 7　複数のデータベースを設定する場合の認証の順序を設定するには、次のコマンドを入力します。

config aaa auth mgmt [**radius** | **tacacs**]

現在の管理認証サーバの順序を表示するには、次のコマンドを入力します。

show aaa auth

次のような情報が表示されます。

```
Management authentication server order:
   1..................................... local
   2..................................... radius
```

ステップ 8　次のコマンドを使用して、RADIUS の統計情報を表示します。

- **show radius summary**：RADIUS サーバと統計情報の概要を表示します。
- **show radius auth statistics**：RADIUS 認証サーバの統計情報を表示します。
- **show radius acct statistics**：RADIUS アカウンティング サーバの統計情報を表示します。
- **show radius rfc3576 statistics**：RADIUS RFC-3576 サーバの概要を表示します。

show radius auth statistics コマンドに対しては、次のような情報が表示されます。

```
Authentication Servers:

Server Index..................................... 1
Server Address................................... 10.91.104.76
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show radius acct statistics コマンドに対しては、次のような情報が表示されます。

```
Accounting Servers:

Server Index..................................... 1
Server Address................................... 10.10.10.1
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 0
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

show radius auth statistics コマンドに対しては、次のような情報が表示されます。

```
RFC-3576 Servers:

Server Index..................................... 1
Server Address................................... 10.91.104.76
Disconnect-Requests.............................. 0
COA-Requests..................................... 0
Retransmitted Requests........................... 0
Malformed Requests............................... 0
Bad Authenticator Requests....................... 0
Other Drops...................................... 0
Sent Disconnect-Ack.............................. 0
Sent Disconnect-Nak.............................. 0
Sent CoA-Ack..................................... 0
Sent CoA-Nak..................................... 0
```

ステップ 9　1 台または複数台の RADIUS サーバの統計情報をクリアするには、次のコマンドを入力します。

clear stats radius {**auth** | **acct**} {*index* | **all**}

ステップ 10　コントローラが RADIUS サーバに接続できることを確認するには、次のコマンドを入力します。

ping *server_ip_address*

アクセス ポイントによって送信される RADIUS 属性

この項の表には、RADIUS 属性が示されています。この属性は、Access-Request パケットおよび Access-Accept パケットで Lightweight アクセス ポイントからクライアントに送信されます。

表 5-1　Access-Request パケットで送信される属性

属性 ID	説明
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type[1]
12	Framed-MTU
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message
243	TPLUS-Role

1. RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は **Callback NAS Prompt** に対してこの属性を設定し、読み取りと書き込みの両方の権限が必要な場合は **Administrative** に対して設定してください。詳細は、「ACS 上での RADIUS の設定」の項のステップ 19 を参照してください。

表 5-2　Access-Accept パケットで受け付けられる属性（シスコ）

属性 ID	説明
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL

（注） シスコ固有の属性 Auth-Algo-Type および SSID はサポートされません。

表 5-3　Access-Accept パケットで受け付けられる属性（標準）

属性 ID	説明
6	Service-Type[1]
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID

1. RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は **Callback NAS Prompt** に対してこの属性を設定し、読み取りと書き込みの両方の権限が必要な場合は **Administrative** に対して設定してください。詳細は、「ACS 上での RADIUS の設定」の項のステップ 19 を参照してください。

（注） メッセージ オーセンティケータはサポートされていません。

表 5-4　Access-Accept パケットで受け付けられる属性（Microsoft）

属性 ID	説明
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

表 5-5　Access-Accept パケットで受け付けられる属性（Airespace）

属性 ID	説明
1	VAP-ID
2	QoS-Level
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name

TACACS+ の設定

Terminal Access Controller Access Control System Plus（TACACS+）とは、コントローラへの管理アクセスを取得しようとするユーザに中央管理されたセキュリティを提供する、クライアント / サーバ プロトコルです。このプロトコルは、ローカルおよび RADIUS に類似したバックエンドのデータベースとして機能します。ただし、ローカルおよび RADIUS では、認証サポートと制限のある認可サポートしか提供されないのに対し、TACACS+ では、次の 3 つのサービスが提供されます。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラで TACACS+ サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。認証サービスおよび認可サービスは、互いに密接に関連しています。たとえば、ローカルまたは RADIUS データベースを使用して認証が実行された場合、認可ではそのローカルまたは RADIUS データベース内のユーザに関連したアクセス権（read-only、read-write、lobby-admin のいずれか）が使用され、TACACS+ は使用されません。同様に、TACACS+ を使用して認証が実行されると、認可は TACACS+ に関連付けられます。

  （注） 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンド データベースが試行される順序を指定できます。

- **認可**：ユーザのアクセス レベルに基づいて、ユーザがコントローラで実行できる処理を決定するプロセス。

  TACACS+ の場合、認可は特定の処理ではなく、権限（またはロール）に基づいて実行されます。利用可能なロールは、コントローラ GUI の次の 7 つのメニュー オプションに対応しています。MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、および COMMANDS です。ロビー アンバサダー権限のみを必要とするユーザは、追加のロールである LOBBY を使用できます。ユーザが割り当てられるロールは、TACACS+ サーバ上で設定されます。ユーザは 1 つまたは複数のロールに対して認可されます。最小の認可は MONITOR のみで、最大は ALL です。ALL では、ユーザは 7 つのメニュー オプションすべてに関連付けられた機能を実行できるよう認可されます。たとえば、SECURITY のロールを割り当てられたユーザは、Security メニューに表示される（または CLI の場合はセキュリティ コマンドとして指定される）すべてのアイテムに対して変更を実行できますユーザが特定のロール（WLAN など）に対して認可されていない場合でも、そのユーザは読み取り専用モード（または関連する CLI の **show** コマンド）で、そのメニュー オプションにアクセスできます。TACACS+ 認可サーバが接続不能または認可不能になった場合、ユーザはコントローラにログインできません。

  （注） ユーザが割り当てられたロールでは許可されていないコントローラ GUI のページに変更を加えようとすると、十分な権限がないことを示すメッセージが表示されます。ユーザが割り当てられたロールでは許可されていないコントローラ CLI コマンドを入力すると、実際にはそのコマンドは実行されていないのに、正常に実行されたというメッセージが表示されます。この場合、次の追加のメッセージが表示され、コマンドを実行するための十分な権限がないことがユーザに通知されます。Insufficient Privilege! Cannot execute command!

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、TACACS+ アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。TACACS+ アカウンティング サーバが接続不能になった場合、ユーザはセッションを妨害されずに続行することはできません。

RADIUS で User Datagram Protocol（UDP; ユーザ データグラム プロトコル）を使用するのとは異なり、TACACS+ では、転送に Transmission Control Protocol（TCP; 転送制御プロトコル）を使用します。1 つのデータベースを維持し、TCP ポート 49 で受信要求をリッスンします。アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

最大 3 台の TACACS+ 認証サーバ、認可サーバ、およびアカウンティング サーバをそれぞれ設定できます。たとえば、1 台の TACACS+ 認証サーバを中央に配置し、複数の TACACS+ 認可サーバを異なる地域に配置できます。同じタイプの複数のサーバを設定していると、最初のサーバで障害が発生したり、接続不能になっても、コントローラは自動的に 2 台目、および必要に応じて 3 台目のサーバを試行します。

（注） 複数の TACACS+ サーバが冗長性のために設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバにおいてユーザ データベースを同一にする必要があります。

CiscoSecure Access Control Server（ACS）とコントローラの両方で、TACACS+ を設定する必要があります。コントローラは、GUI または CLI のいずれかを使用して設定できます。

ACS 上での TACACS+ の設定

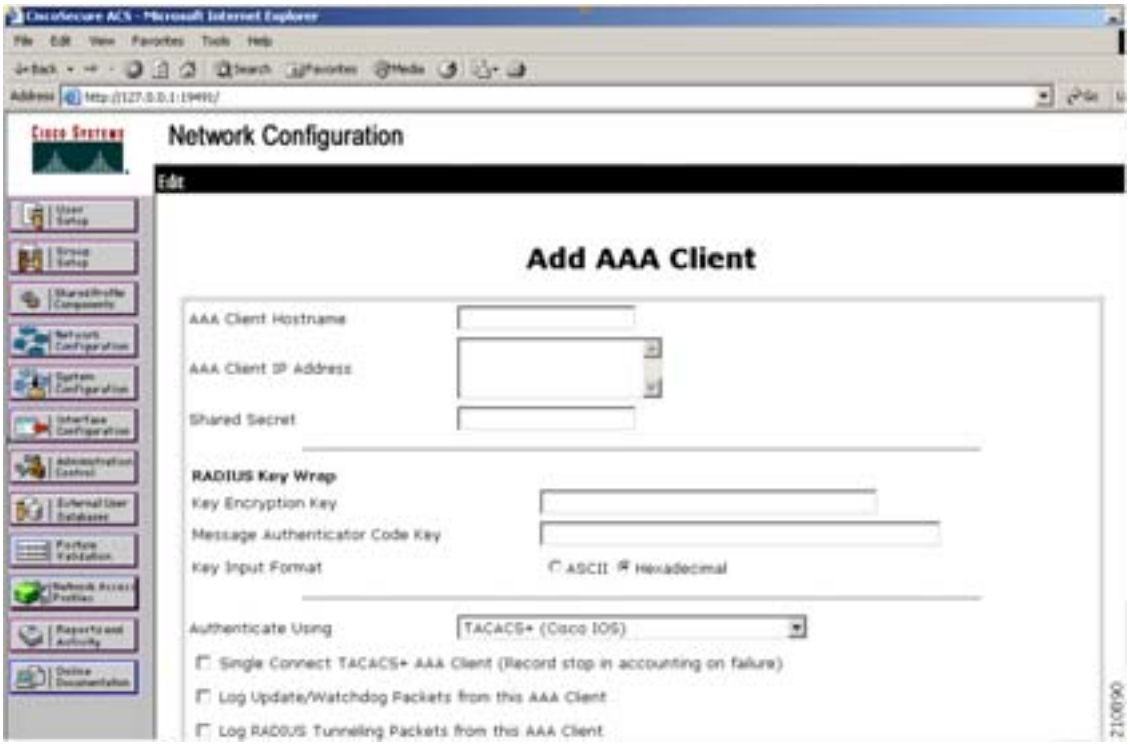
ACS 上で TACACS+ を設定する手順は、次のとおりです。

（注） TACACS+ は、CiscoSecure ACS バージョン 3.2 以上でサポートされます。この項に示される手順および図は、ACS バージョン 4.1 に関連するもので、他のバージョンでは異なる場合があります。実行中のバージョンの CiscoSecure ACS マニュアルを参照してください。

ステップ 1　ACS のメイン ページで、**Network Configuration** をクリックします。

ステップ 2　AAA Clients の下の **Add Entry** をクリックし、使用しているコントローラをサーバに追加します。Add AAA Client ページが表示されます（図 5-6 を参照）。

図 5-6　CiscoSecure ACS 上の Add AAA Client ページ



ステップ 3　AAA Client Hostname フィールドに、コントローラの名前を入力します。

ステップ 4　AAA Client IP Address フィールドに、コントローラの IP アドレスを入力します。

ステップ 5　Shared Secret フィールドに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

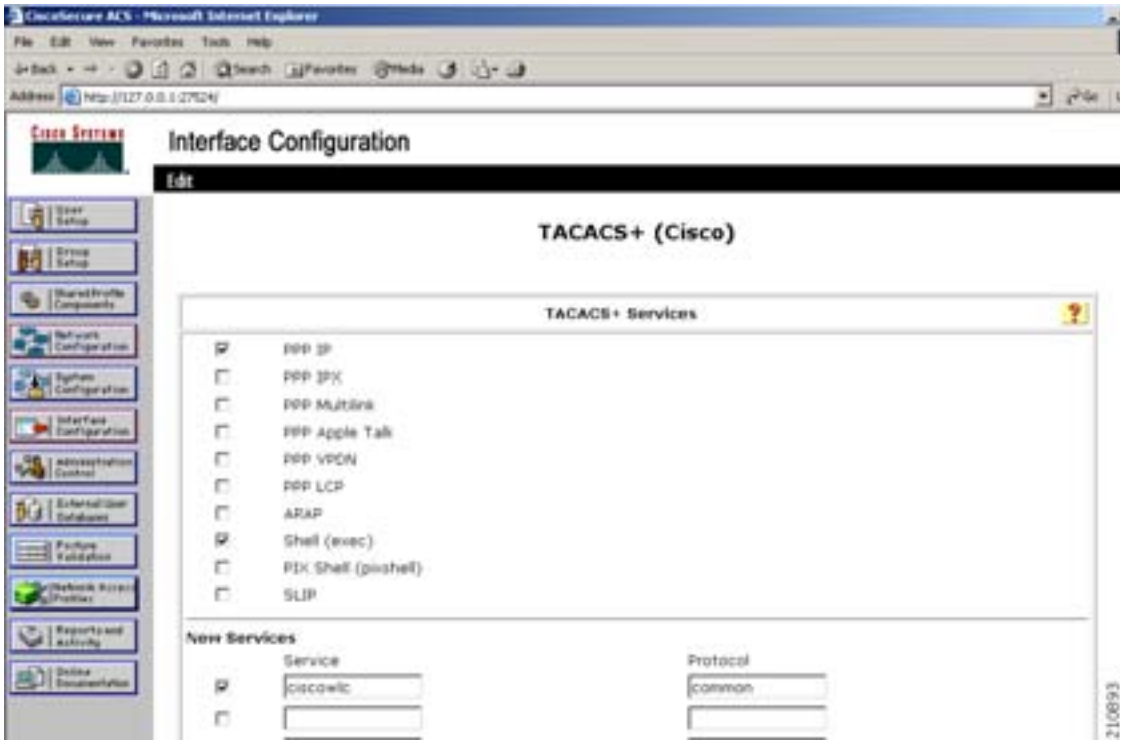
ステップ 6　Authenticate Using ドロップダウン ボックスから **TACACS+ (Cisco IOS)** を選択します。

ステップ 7　**Submit + Apply** をクリックして、変更内容を保存します。

ステップ 8　ACS のメイン ページで、**Interface Configuration** をクリックします。

ステップ 9　**TACACS+ (Cisco IOS)** をクリックします。TACACS+ (Cisco) ページが表示されます（図 5-7 を参照）。

図 5-7　CiscoSecure ACS 上の TACACS+ (Cisco) ページ



ステップ 10　TACACS+ Services の下で、**Shell (exec)** チェックボックスをオンにします。

ステップ 11　New Services の下で、最初のチェックボックスをオンにし、Service フィールドに **ciscowlc** と入力し、Protocol フィールドに **common** と入力します。

ステップ 12　Advanced Configuration Options の下で、**Advanced TACACS+ Features** チェックボックスをオンにします。

ステップ 13　**Submit** をクリックして、変更内容を保存します。

ステップ 14　ACS のメイン ページで、**System Configuration** をクリックします。

ステップ 15　**Logging** をクリックします。

ステップ 16　Logging Configuration ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

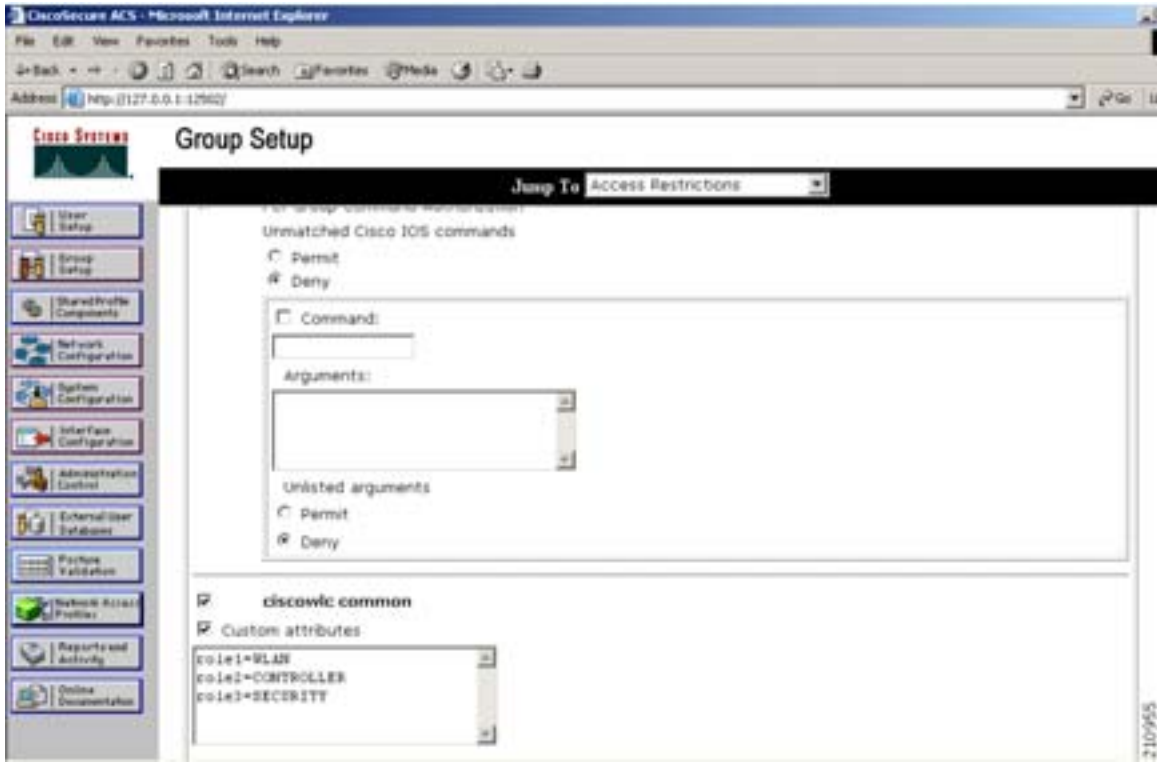
ステップ 17　ACS のメイン ページで、**Group Setup** をクリックします。

ステップ 18　Group ドロップダウン ボックスから、以前に作成したグループを選択します。

（注）　この手順により、ユーザが割り当てられることになるロールに基づいて、ACS 上のグループにすでにユーザを割り当てていることを確認します。

ステップ 19　**Edit Settings** をクリックします。Group Setup ページが表示されます（図 5-8 を参照）。

図 5-8　CiscoSecure ACS 上の Group Setup ページ



ステップ 20　**TACACS+ Settings** の下の **ciscowlc common** チェックボックスをオンにします。

ステップ 21　**Custom Attributes** チェックボックスをオンにします。

ステップ 22　Custom Attributes の下のテキストボックスで、このグループに割り当てるロールを指定します。使用可能なロールは、MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMANDS、ALL、および LOBBY です。前述のように、最初の 7 つのロールは、コントローラ GUI のメニュー オプションに対応しており、これら特定のコントローラ機能へのアクセスを許可します。グループでの必要性に応じて、1 つまたは複数のロールを入力できます。7 つのロールすべてを指定するには ALL を、ロビー アンバサダー ロールを指定するには LOBBY を使用します。次の形式を使用してロールを入力します。

role*x*=*ROLE*

たとえば、特定のユーザ グループに対して WLAN、CONTROLLER、および SECURITY のロールを指定するには、次のテキストを入力します。

```
role1=WLAN
role2=CONTROLLER
role3=SECURITY
```

あるユーザ グループに 7 つのロールすべてに対するアクセスを付与するには、次のテキストを入力します。

```
role1=ALL
```

（注） 必ず上記の形式を使用してロールを入力するようにしてください。ロールはすべて大文字で入力する必要があり、テキスト間にスペースは挿入できません。

（注） MONITOR ロールまたは LOBBY ロールは、その他のロールと組み合わせることはできません。Custom Attributes テキストボックスにこれら 2 つのロールのどちらかを指定すると、追加のロールが指定された場合でも、ユーザには MONITOR または LOBBY 権限のみが付与されます。

ステップ 23　**Submit** をクリックして、変更内容を保存します。

GUI を使用した TACACS+ の設定

コントローラの GUI を使用して TACACS+ を設定する手順は、次のとおりです。

ステップ 1　**Security** > **AAA** > **TACACS+** の順にクリックします。

ステップ 2　次のいずれかの操作を行います。

- TACACS+ サーバを認証用に設定する場合、**Authentication** をクリックします。
- TACACS+ サーバを認可用に設定する場合、**Authorization** をクリックします。
- TACACS+ サーバをアカウンティング用に設定する場合、**Accounting** をクリックします。

（注） 認証、認可、アカウンティングの設定に使用される GUI ページには、すべて同じフィールドが含まれます。そのため、ここでは Authentication ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

TACACS+（Authentication、Authorization、または Accounting）Servers ページが表示されます（図 5-9 を参照）。

図 5-9　TACACS+ Authentication Servers ページ

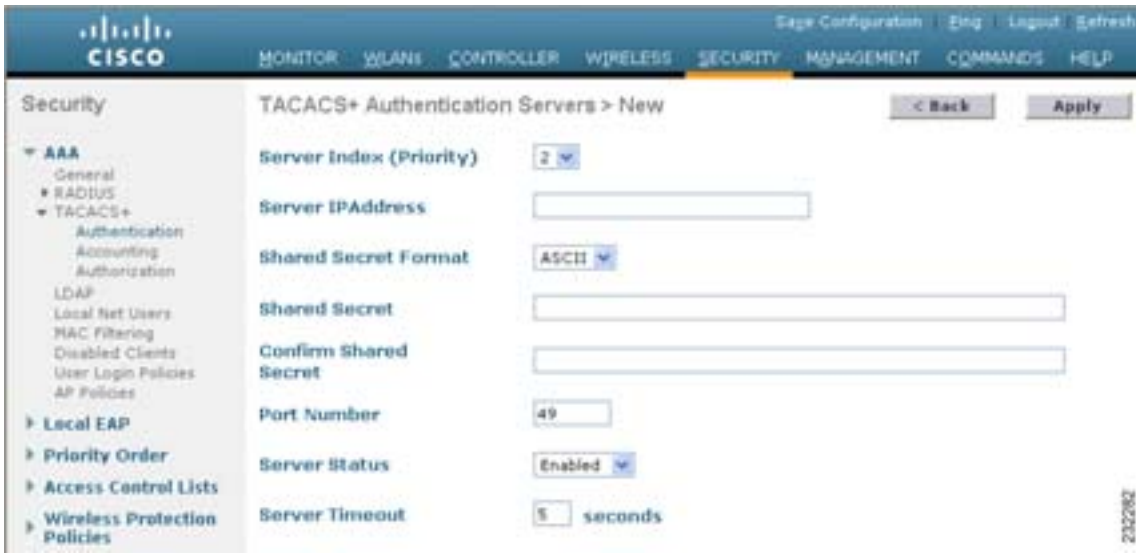
このページでは、これまでに設定されたすべての TACACS+ サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。
- コントローラが特定のサーバに接続できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Ping** を選択します。

ステップ 3　次のいずれかの操作を行います。

- 既存の TACACS+ サーバを編集するには、そのサーバのサーバ インデックス番号をクリックします。TACACS+（Authentication、Authorization、または Accounting）Servers > Edit ページが表示されます。
- TACACS+ サーバを追加するには、**New** をクリックします。TACACS+（Authentication、Authorization、または Accounting）Servers > New ページが表示されます（図 5-10 を参照）。

図 5-10　TACACS+ Authentication Servers > New ページ



ステップ 4　新しいサーバを追加する場合、Server Index (Priority) ドロップダウン ボックスから数字を選択し、同じサービスを提供するその他の設定済みの TACACS+ サーバに対するこのサーバの優先順位を指定します。最大 3 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目および必要に応じて 3 番目のサーバへの接続を試行します。

ステップ 5　新しいサーバを追加する場合は、Server IP Address フィールドに、TACACS+ サーバの IP アドレスを入力します。

ステップ 6　Shared Secret Format ドロップダウン ボックスから、**ASCII** または **Hex** を選択し、コントローラと TACACS+ サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は ASCII です。

ステップ 7　Shared Secret フィールドおよび Confirm Shared Secret フィールドに、コントローラとサーバ間の認証に使用する共有秘密キーを入力します。

（注）　共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 8　新しいサーバを追加する場合は、Port Number フィールドに、インターフェイス プロトコルに対する TACACS+ サーバの TCP ポート番号を入力します。有効な範囲は 1 ～ 65535 で、デフォルト値は 49 です。

ステップ 9　Server Status フィールドから **Enabled** を選択してこの TACACS+ サーバを有効にするか、**Disabled** を選択して無効にします。デフォルト値は Enabled です。

ステップ 10　Server Timeout フィールドに、再送信の間隔（秒数）入力します。有効な範囲は 5 ～ 30 秒で、デフォルト値は 5 秒です。

（注）　再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 13　同じサーバ上で、または追加の TACACS+ サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 14　複数のデータベースを設定する際の認証の順序を指定するには、**Security** > **Priority Order** > **Management User** の順にクリックします。Priority Order > Management User ページが表示されます（図 5-11 を参照）。

図 5-11　Priority Order > Management User ページ

ステップ 15　Authentication Priority で、**Radius** または **TACACS+** のどちらかを指定して、コントローラが管理ユーザの認証を試行するときにどちらのサーバが他方に対して優先されるかを指定します。デフォルトで、ローカル データベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは TACACS+ に設定されている場合は TACACS+ サーバに切り替え、RADIUS に設定されている場合は RADIUS サーバに切り替えます。デフォルトの設定はローカル、Radius の順になっています。

ステップ 16　**Apply** をクリックして、変更を適用します。

ステップ 17　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した TACACS+ の設定

コントローラ CLI を使用して TACACS+ を設定するには、この項のコマンドを使用します。

(注)　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した TACACS+ の設定」の項（P. 5-23）を参照してください。

1. TACACS+ 認証サーバを設定するには、次のコマンドを使用します。
   - **config tacacs auth add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ 認証サーバを追加します。
   - **config tacacs auth delete** *index*：以前に追加された TACACS+ 認証サーバを削除します。
   - **config tacacs auth** {**enable** | **disable**} *index*：TACACS+ 認証サーバを有効または無効にします。
   - **config tacacs auth server-timeout** *index timeout*：TACACS+ 認証サーバの再送信のタイムアウト値を設定します。
2. TACACS+ 認可サーバを設定するには、次のコマンドを使用します。
   - **config tacacs athr add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ 認可サーバを追加します。
   - **config tacacs athr delete** *index*：以前に追加された TACACS+ 認可サーバを削除します。
   - **config tacacs athr** {**enable** | **disable**} *index*：TACACS+ 認可サーバを有効または無効にします。
   - **config tacacs athr server-timeout** *index timeout*：TACACS+ 認可サーバの再送信のタイムアウト値を設定します。
3. TACACS+ アカウンティング サーバを設定するには、次のコマンドを使用します。
   - **config tacacs acct add** *index server_ip_address port#* {**ascii** | **hex**} *shared_secret*：TACACS+ アカウンティング サーバを追加します。
   - **config tacacs acct delete** *index*：以前に追加された TACACS+ アカウンティング サーバを削除します。
   - **config tacacs acct** {**enable** | **disable**} *index*：TACACS+ アカウンティング サーバを有効または無効にします。
   - **config tacacs acct server-timeout** *index timeout*：TACACS+ アカウンティングの再送信のタイムアウト値を設定します。
4. 次のコマンドを使用して、TACACS+ の統計を表示します。
   - **show tacacs summary**：TACACS+ サーバと統計情報の概要を表示します。
   - **show tacacs auth stats**：TACACS+ 認証サーバの統計情報を表示します。
   - **show tacacs athr stats**：TACACS+ 認可サーバの統計情報を表示します。
   - **show tacacs acct stats**：TACACS+ アカウンティング サーバの統計情報を表示します。

たとえば、**show tacacs summary** コマンドに対しては、次のような情報が表示されます。

```
Authentication Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5

Authorization Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5

Accounting Servers

Idx  Server Address    Port    State     Tout
---  ----------------  ------  --------  ----
1    11.11.12.2        49      Enabled   5
2    11.11.13.2        49      Enabled   5
3    11.11.14.2        49      Enabled   5
```

show tacacs auth stats コマンドに対しては、次のような情報が表示されます。

```
Server Index..................................... 1
Server Address................................... 10.10.10.10
Msg Round Trip Time.............................. 0 (1/100 second)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Error Responses.................................. 0
Restart Responses................................ 0
Follow Responses................................. 0
GetData Responses................................ 0
Encrypt no secret Responses...................... 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops.....................................0
```

5. 1 台または複数台の TACACS+ サーバの統計をクリアするには、次のコマンドを入力します。

   clear stats tacacs [**auth** | **athr** | **acct**] {*index* | **all**}

6. 複数のデータベースを設定する場合の認証の順序を設定するには、次のコマンドを入力します。デフォルトの設定はローカル、Radius の順になっています。

   config aaa auth mgmt [**radius** | **tacacs**]

   現在の管理認証サーバの順序を表示するには、次のコマンドを入力します。

   show aaa auth

   次のような情報が表示されます。

```
Management authentication server order:
   1..................................... local
   2..................................... tacacs
```

7. コントローラが確実に TACACS+ サーバに接続できるようにするには、次のコマンドを入力します。

   ping *server_ip_address*

8. TACACS+ のデバッグを有効または無効にするには、次のコマンドを入力します。
   debug aaa tacacs {enable | disable}
9. 変更を保存するには、次のコマンドを入力します。
   save config

TACACS+ 管理サーバのログの表示

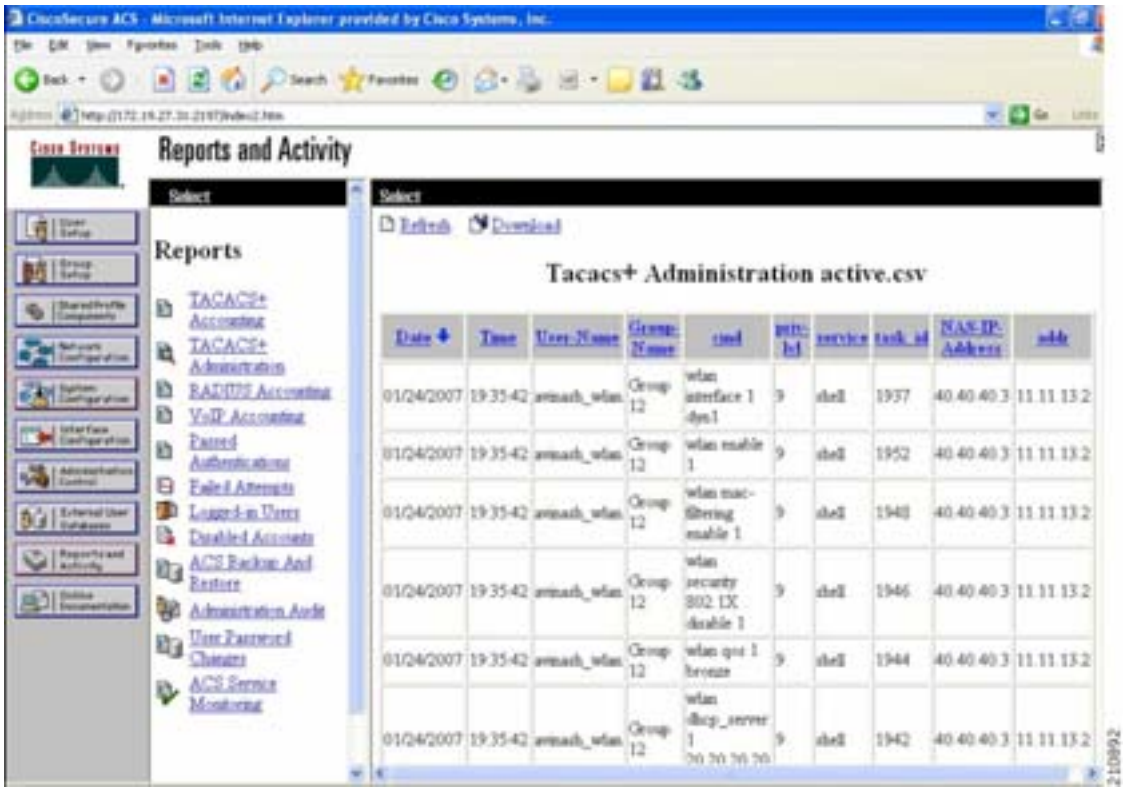
コントローラ上で TACACS+ アカウンティング サーバが設定されている場合、TACACS+ 管理サーバのログを表示する手順は、次のとおりです。

ステップ 1　ACS のメイン ページで、**Reports and Activity** をクリックします。

ステップ 2　**TACACS+ Administration** をクリックします。

ステップ 3　表示するログの日付に対応する .csv ファイルをクリックします。TACACS+ Administration .csv ページが表示されます（図 5-12 を参照）。

図 5-12　CiscoSecure ACS 上の TACACS+ Administration .csv ページ



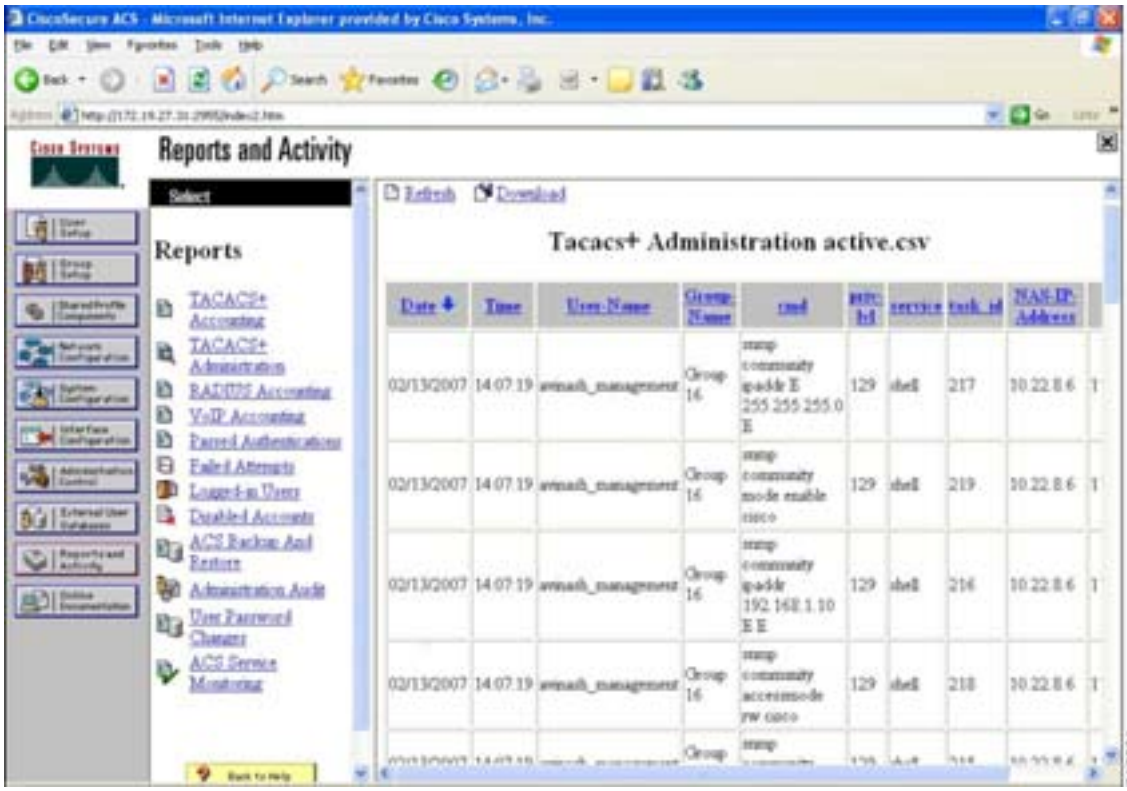
このページには、次の情報が表示されます。

- 処理が実行された日付と時刻
- 処理を実行したユーザの名前と割り当てられたロール
- ユーザが属するグループ

- ユーザが実行した特定の処理
- 処理を実行したユーザの権限レベル
- コントローラの IP アドレス
- 処理が実行されたラップトップまたはワークステーションの IP アドレス

単一の処理（またはコマンド）が、コマンド内のパラメータごとに、複数回ログ記録される場合があります。たとえば、ユーザが **snmp community ipaddr** *ip_address subnet_mask community_name* というコマンドを入力したとします。その場合、ある行では、IP アドレスはログに記録されても、サブネット マスクとコミュニティ名はログに「E」と記録されることがあります。また、別の行では、サブネット マスクはログに記録されても、IP アドレスとコミュニティ名はログに「E」と記録されることがあります。図 5-13 の例の最初の行と 3 番目の行を参照してください。

図 5-13　CiscoSecure ACS 上の TACACS+ Administration .csv ページ



（注） **Refresh** をクリックすると、いつでもこのページを更新できます。

ローカル ネットワーク ユーザの設定

この項では、コントローラ上のローカル ユーザ データベースにローカル ネットワーク ユーザを追加する方法について説明します。ローカル ユーザ データベースには、すべてのローカル ネットワーク ユーザの資格情報（ユーザ名とパスワード）が保存されます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。詳細は、「ローカル EAP の設定」の項（P. 5-39）を参照してください。

（注） コントローラはクライアント情報をまず　RADIUS　認証サーバに渡します。クライアント情報が RADIUS データベースのエントリに一致しない場合は、ローカル ユーザ データベースがポーリングされます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

ローカル ネットワーク ユーザは、GUI または CLI のいずれかを使用して設定できます。

GUI を使用したローカル ネットワーク ユーザの設定

コントローラ GUI を使用してローカル ネットワーク ユーザを設定する手順は、次のとおりです。

ステップ 1　ローカル ユーザ データベースに保存できるローカル ネットワーク ユーザの最大数を指定する手順は、次のとおりです。

a. **Security** > **AAA** > **General** の順にクリックして、General ページを開きます（図 5-14 を参照）。

図 5-14　General ページ

b. Maximum Local Database Entries フィールドに、次回コントローラがリブートした際にローカル ユーザ データベースに追加できるローカル ネットワーク ユーザの最大数の値を入力します。現在設定されている値が、フィールドの右側のカッコ内に表示されます。有効な範囲は 512 ～ 2048 で、デフォルトの設定は 512 です。

c. **Apply** をクリックして、変更を適用します。

ステップ 2　**Security** > **AAA** > **Local Net Users** の順にクリックして、Local Net Users ページを開きます（図 5-15 を参照）。

図 5-15　Local Net Users ページ

このページでは、これまでに設定されたすべてのローカル ネットワーク ユーザが表示されます。すべてのゲスト ユーザと、ゲスト ユーザに割り当てられている QoS ロール（該当する場合）も指定されます。QoS ロールの設定の詳細は、「Quality of Service ロールの設定」の項（P. 4-55）を参照してください。

（注）　既存のユーザを削除するには、そのユーザの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 3　次のいずれかの操作を行います。

- 既存のローカル ネットワーク ユーザを編集するには、そのユーザのユーザ名をクリックします。Local Net Users > Edit ページが表示されます。
- ローカル ネットワーク ユーザを追加するには、**New** をクリックします。Local Net Users > New ページが表示されます（図 5-16 を参照）。

図 5-16　Local Net Users > New ページ

ステップ 4　新しいユーザを追加する場合は、User Name フィールドに、そのローカル ユーザのユーザ名を入力します。最大 24 文字の英数字を入力できます。

（注）　ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

ステップ 5　Password フィールドおよび Confirm Password フィールドに、ローカル ユーザのパスワードを入力します。最大 24 文字の英数字を入力できます。

ステップ 6　新しいユーザを追加する場合、そのユーザがローカル ネットワークにアクセスする時間を制限するには、**Guest User** チェックボックスをオンにします。デフォルトの設定は、オフになっています。

ステップ 7　新しいユーザを追加し、Guest User チェックボックスをオンにした場合は、Lifetime フィールドに、ゲスト ユーザ アカウントをアクティブにする時間（秒単位）を入力します。有効な範囲は 60 ～ 2,592,000（30 日間）秒（両端の値を含む）で、デフォルトの設定は 86,400 秒です。

ステップ 8　Guest User チェックボックスをオンにして新しいユーザを追加するときに、このゲスト ユーザに QoS ロールを割り当てるには、**Guest User Role** チェックボックスをオンにします。デフォルトの設定は、オフになっています。

（注）　ゲスト ユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

ステップ 9　Guest User Role チェックボックスをオンにして新しいユーザを追加する場合は、このゲスト ユーザに割り当てる QoS ロールを Role ドロップダウン ボックスから選択します。

（注）　新しい QoS ロールを作成する手順は、「Quality of Service ロールの設定」の項（P. 4-55）を参照してください。

ステップ 10　WLAN Profile ドロップダウン ボックスから、ローカル ユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である **Any WLAN** を選択すると、ユーザは設定済みのすべての WLAN にアクセスできます。

ステップ 11　Description フィールドに、ローカル ユーザのことを説明したタイトル（「ゲスト ユーザ」など）を入力します。

ステップ 12　**Apply** をクリックして、変更を適用します。

ステップ 13　**Save Configuration** をクリックして、変更を保存します。

CLI を使用したローカル ネットワーク ユーザの設定

コントローラ CLI を使用して ローカル ネットワーク ユーザを設定するには、この項のコマンドを使用します。

（注） CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用したローカル ネットワーク ユーザの設定」の項（P. 5-30）を参照してください。

1. ローカル ネットワーク ユーザを設定するには、次のコマンドを使用します。
   - **config netuser add** *username password* **wlan** *wlan_id* **userType permanent description** *description*：コントローラ上のローカル ユーザ データベースに永久ユーザを追加します。
   - **config netuser add** *username password* {**wlan** | **guestlan**} {*wlan_id* | *guest_lan_id*} **userType guest lifetime** *seconds* **description** *description*：WLAN または有線ゲスト LAN 上のゲスト ユーザを、コントローラのローカル ユーザ データベースに追加します。

     （注） 永久ユーザまたはゲスト ユーザをコントローラからローカル ユーザ データベースに追加する代わりに、RADIUS サーバ上にユーザに対するエントリを作成して Web 認証が実行される WLAN に対して RADIUS 認証を有効にするよう選択できます。

   - **config netuser delete** *username*：コントローラ上のローカル ユーザ データベースからユーザを削除します。

     （注） ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

2. 次のコマンドを使用して、コントローラで設定されたローカル ネットワーク ユーザに関連する情報を表示します。
   - **show netuser detail** *username*：ローカル ユーザ データベース内の特定のユーザの設定を表示します。
   - **show netuser summary**：ローカル ユーザ データベース内のすべてのユーザの一覧を表示します。

   たとえば、**show netuser detail** *username* コマンドに対しては、次のような情報が表示されます。

```
User Name.............................. abc
WLAN Id................................ Any
Lifetime............................... Permanent
Description............................ test user
```

3. 変更を保存するには、次のコマンドを入力します。

   save config

LDAP の設定

この項では、Lightweight Directory Access Protocol（LDAP）サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。LDAP バックエンド データベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとして LDAP を使用する場合があります。詳細は、「ローカル EAP の設定」の項（P. 5-39）を参照してください。

（注） LDAP バックエンド データベースでは、次のローカル EAP 方式がサポートされます。EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。たとえば、Microsoft Active Directory は、平文のパスワードを返さないため、サポートされません。平文のパスワードを返すように LDAP サーバを設定できない場合、LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 はサポートされません。

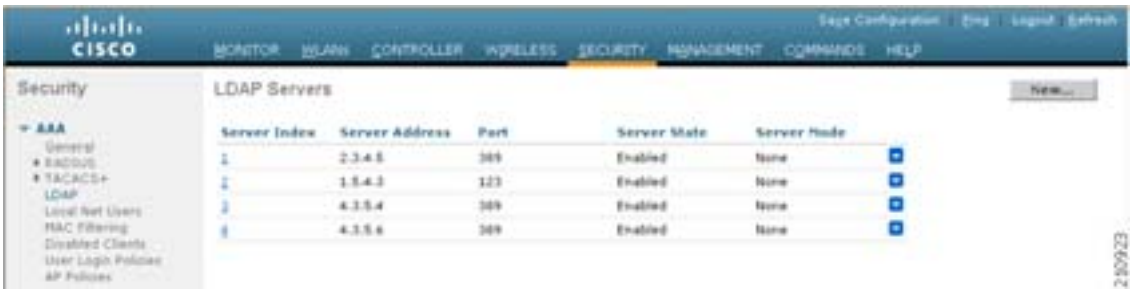
LDAP は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した LDAP の設定

コントローラ GUI を使用して LDAP を設定する手順は、次のとおりです。

ステップ 1　**Security** > **AAA** > **LDAP** の順にクリックして、LDAP Servers ページを開きます（図 5-17 を参照）。

図 5-17　LDAP Servers ページ



このページでは、これまでに設定されたすべての LDAP サーバが表示されます。

- 既存の LDAP サーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。
- コントローラが特定のサーバに接続されるようにするには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、**Ping** を選択します。

ステップ 2　次のいずれかの操作を行います。

- 既存の LDAP サーバを編集するには、そのサーバのインデックス番号をクリックします。LDAP Servers > Edit ページが表示されます。
- LDAP サーバを追加するには、**New** をクリックします。LDAP Servers > New ページが表示されます（図 5-18 を参照）。

図 5-18　LDAP Servers > New ページ

ステップ 3　新しいサーバを追加する場合は、Server Index (Priority) ドロップダウン ボックスから数字を選択し、その他の設定済みの LDAP サーバに対するこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。

ステップ 4　新しいサーバを追加する場合は、Server IP Address フィールドに、LDAP サーバの IP アドレスを入力します。

ステップ 5　新しいサーバを追加する場合は、Port Number フィールドに、LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ～ 65535 で、デフォルト値は 389 です。

ステップ 6　User Base DN フィールドに、すべてのユーザの一覧を含む LDAP サーバ内のサブツリーの Distinguished Name（DN; 認定者名）を入力します。たとえば、ou=organizational unit, .ou=next organizational unit, o=corporation.com のようになります。ユーザを含むツリーがベース DN である場合、**o=***corporation***.com** または **dc=***corporation***,dc=com** と入力します。

ステップ 7　User Attribute フィールドに、ユーザ名を含むユーザ レコード内の属性の名前を入力します。この属性はディレクトリ サーバから取得できます。

ステップ 8　User Object Type フィールドに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザ レコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクト タイプと共有する値があります。

ステップ 9　新しいサーバを追加する場合に、すべての LDAP トランザクションでセキュアな TLS トンネルを使用するには、Server Mode ドロップダウン ボックスから **Secure** を選択します。そうでない場合は、**None** を選択します。これはデフォルト設定です。

ステップ 10　Server Timeout フィールドに、再送信の間隔（秒数）入力します。有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。

ステップ 11　**Enable Server Status** チェックボックスをオンにしてこの LDAP サーバを有効にするか、オフにしてこのサーバを無効にします。デフォルト値は無効です。

ステップ 12　**Apply** をクリックして、変更を適用します。

ステップ 13　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 14　LDAP をローカル EAP 認証のための優先バックエンド データベース サーバとして指定する手順は、次のとおりです。

a. **Security** > **Local EAP** > **Authentication Priority** の順にクリックして、Priority Order > Local-Auth ページを開きます（図 5-19 を参照）。

図 5-19　Priority Order > Local-Auth ページ

b. **LOCAL** を強調表示して、< をクリックし、それを左の User Credentials ボックスに移動します。

c. **LDAP** を強調表示して、> をクリックし、それを右の User Credentials ボックスに移動します。右側の User Credentials ボックスの上部に表示されるデータベースは、ユーザの資格情報を取得する際に使用されます。

（注）　LDAP と LOCAL の両方が右側の User Credentials ボックスに表示され、LDAP が上部で LOCAL が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。LOCAL が上部にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d. **Apply** をクリックして、変更を適用します。

e. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 15　（オプション）特定の LDAP サーバを WLAN に割り当てる手順は、次のとおりです。

a. **WLANs** をクリックして、WLANs ページを開きます。

b. 必要な WLAN のプロファイル名をクリックします。

c. WLANs > Edit ページが表示されたら、**Security** > **AAA Servers** タブをクリックし、WLANs > Edit（Security > AAA Servers）ページを開きます（図 5-20 を参照）。

図 5-20　WLANs > Edit（Security > AAA Servers）ページ

d. LDAP Servers ドロップダウン ボックスから、この WLAN に使用する LDAP サーバを選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位に従って試行されます。

e. **Apply** をクリックして、変更を適用します。

f. **Save Configuration** をクリックして、変更を保存します。

CLI を使用した LDAP の設定

コントローラ CLI を使用して LDAP を設定するには、この項のコマンドを使用します。

（注） CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した LDAP の設定」の項（P. 5-34）を参照してください。

1. LDAP サーバを設定するには、次のコマンドを使用します。

- **config ldap add** *index server_ip_address port# user_dn password base_dn* {**secure**}：LDAP サーバを追加します。
- **config ldap delete** *index*：以前に追加された LDAP サーバを削除します。
- **config ldap** {**enable** | **disable**} *index*：LDAP サーバを有効または無効にします。
- **config ldap retransmit-timeout** *index timeout*：LDAP サーバの再送信の間隔（秒数）を設定します。

2. 次のコマンドを使用すると、LDAP を優先バックエンド データベースとして指定できます。

config local-auth user-credentials ldap

（注）　**config local-auth user-credentials ldap local** と入力すると、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap** と入力すると、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

3. （オプション）特定の LDAP サーバを WLAN に割り当てるには、次のコマンドを使用します。
   - **config wlan ldap add** *wlan_id index*：設定済みの LDAP サーバを WLAN に接続します。
   - **config wlan ldap delete** *wlan_id* **{all |** *index***}**：特定の、またはすべての設定済み LDAP サーバを WLAN から削除します。
4. 設定済みの LDAP サーバに関連する情報を表示するには、次のコマンドを使用します。
   - **show ldap summary**：設定済みの LDAP サーバの概要を表示します。
   - **show ldap detailed** *index*：LDAP サーバの詳細情報を表示します。
   - **show ldap statistics**：LDAP サーバの統計情報を表示します。
   - **show wlan** *wlan_id*：WLAN に適用される LDAP サーバを表示します。

   たとえば、**show ldap summary** コマンドに対しては、次のような情報が表示されます。

```
LDAP Servers
Idx Host IP addr    Port  Enabled
--- --------------- ----- -------
1   10.10.10.10    389    Yes
```

   show ldap statistics コマンドに対しては、次のような情報が表示されます。

```
LDAP Servers
    Server 1..................... 10.10.10.10 389
```

5. コントローラが確実に LDAP サーバに接続できるようにするには、次のコマンドを入力します。

   ping *server_ip_address*
6. 変更を保存するには、次のコマンドを入力します。

   save config
7. LDAP のデバッグを有効または無効にするには、次のコマンドを入力します。

   debug aaa ldap {**enable** | **disable**}

ローカル EAP の設定

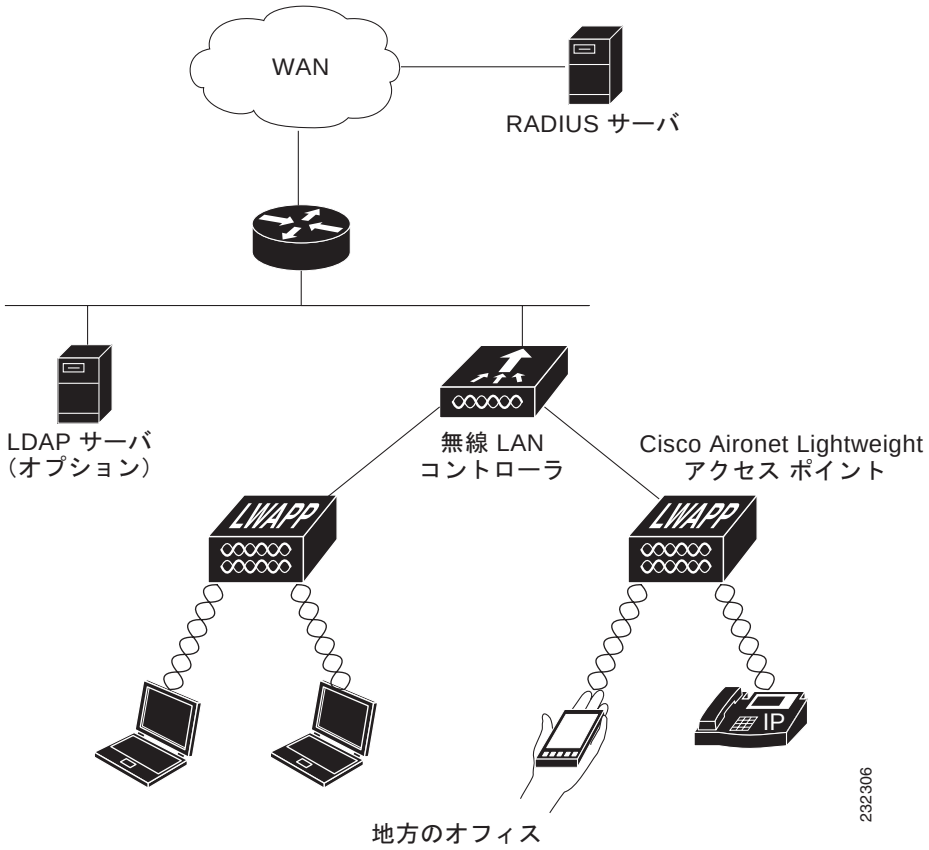
ローカル EAP は、ユーザおよび無線クライアントのローカル認証を可能にする認証方式です。この方式は、バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、無線クライアントへの接続を維持できるように、リモート オフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバへの依存が排除されます。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。ローカル EAP では、コントローラと無線クライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。

（注） LDAP バックエンド データベースでは、次のローカル EAP 方式がサポートされます。EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。たとえば、Microsoft Active Directory は、平文のパスワードを返さないため、サポートされません。平文のパスワードを返すように LDAP サーバを設定できない場合、LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 はサポートされません。

（注） コントローラ上で RADIUS サーバが設定されている場合は、コントローラはまず RADIUS サーバを使用して無線クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番目の RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番目の RADIUS サーバを試行し、次に 4 番目の RADIUS サーバ、その次にローカル EAP を試行します。

図 5-21 は、ローカル EAP を使用したリモート オフィスの例を示しています。

図 5-21　ローカル EAP の例



ローカル EAP は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用したローカル EAP の設定

コントローラの GUI を使用してローカル EAP を設定する手順は、次のとおりです。

ステップ 1　EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA; 認証局）の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。ローカル EAP でこれらのいずれかのタイプの EAP を使用するよう設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。証明書と PAC のインポートの詳細は、第 8 章を参照してください。

ステップ 2　コントローラでローカル　ユーザ　データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。手順については、「ローカル ネットワーク ユーザの設定」の項（P. 5-30）を参照してください。

ステップ 3　コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。手順については、「LDAP の設定」の項（P. 5-34）を参照してください。

ステップ 4　バックエンド データベース サーバからユーザの資格情報が取得される順序を指定する手順は、次のとおりです。

a. **Security** > **Local EAP** > **Authentication Priority** の順にクリックして、Priority Order > Local-Auth ページを開きます（図 5-22 を参照）。

図 5-22　Priority Order > Local-Auth ページ

b. ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を決定します。たとえば、LDAP データベースがローカル ユーザ データベースよりも優先されるようにすることも、または LDAP データベースがまったく考慮されないようにすることもできます。

c. 優先順位を決定したら、目的のデータベースを強調表示します。次に、左と右の矢印および Up ボタンと Down ボタンを使用して、目的のデータベースを右側の User Credential ボックスの上部に移動します。

(注)　LDAP と LOCAL の両方が右側の User Credentials ボックスに表示され、LDAP が上部で LOCAL が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。LOCAL が上部にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

d. **Apply** をクリックして、変更を適用します。

ステップ 5　ローカル EAP タイマーに値を指定する手順は、次のとおりです。

a. **Security** > **Local EAP** > **General** の順にクリックして、General ページを開きます（図 5-23 を参照）。

図 5-23　General ページ

b. Local Auth Active Timeout フィールドに、設定済みの RADIUS サーバのペアによる認証が失敗したあとに、コントローラがローカル EAP を使用して無線クライアントを認証する際の試行時間（秒単位）を入力します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。

c. Identity Request Timeout フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を送信する際の試行時間（秒単位）を入力します。有効な値の範囲は 1 ～ 120 秒で、デフォルトの設定は 1 秒です。

d. Identity Request Max Retries フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。

e. Dynamic WEP Key Index フィールドに、動的 Wired Equivalent Privacy（WEP）に使用するキーインデックスを入力します。デフォルトの設定は 0 です。

f. Request Timeout フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP 要求を送信する際の試行時間（秒単位）を入力します。有効な値の範囲は 1 ～ 120 秒で、デフォルトの設定は 1 秒です。

g. Request Max Retries フィールドに、コントローラがローカル EAP を使用して無線クライアントに EAP 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。

h. **Apply** をクリックして、変更を適用します。

ステップ 6　無線クライアントでサポートされる EAP 認証タイプを指定する、ローカル EAP プロファイルを作成する手順は、次のとおりです。

a. **Security** > **Local EAP** > **Profiles** の順にクリックして、Local EAP Profiles ページを開きます（図 5-24 を参照）。

図 5-24　Local EAP Profiles ページ

このページでは、これまでに設定されたすべてのローカル EAP プロファイルが表示され、そのEAP タイプを指定します。最大 16 個のローカル EAP プロファイルを作成できます。

（注）　既存のプロファイルを削除するには、そのプロファイルの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

b. **New** をクリックして、Local EAP Profiles > New ページを開きます。

c. Profile Name フィールドに、新しいプロファイルの名前を入力し、**Apply** をクリックします。

（注）　プロファイル名には最大 63 文字の英数字を入力できます。スペースは含めないでください。

d. Local EAP Profiles ページが再度表示されたら、新しいプロファイルの名前をクリックします。Local EAP Profiles > Edit ページが表示されます（図 5-25 を参照）。

図 5-25　Local EAP Profiles > Edit ページ

e. **LEAP** チェックボックス、**EAP-FAST** チェックボックス、**EAP-TLS** チェックボックス、**PEAP** チェックボックス（複数可）をオンにし、ローカル認証に使用できる EAP タイプを指定します。

（注） プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、PEAPv1/GTC など）を選択する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注） PEAP チェックボックスをオンにすると、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

f. EAP-FAST を選択し、コントローラ上のデバイスの証明書を認証に使用する場合は、**Local Certificate Required** チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにします。これがデフォルトの設定です。

（注） デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このオプションは EAP-FAST にのみ適用されます。

g. EAP-FAST を選択し、無線クライアントがデバイスの証明書を認証のためにコントローラに送信するようにするには、**Client Certificate Required** チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにします。これがデフォルトの設定です。

（注） クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このオプションは EAP-FAST にのみ適用されます。

h. 証明書を使用する EAP-FAST、EAP-TLS、または PEAP を選択する場合は、シスコが発行する証明書と別のベンダーが発行する証明書のいずれがクライアントに送信されるようにするかを選択します。Certificate Issuer ドロップダウン ボックスから **Cisco** または **Vendor** を選択してください。デフォルトの設定は、Cisco になっています。

i. 証明書を使用する EAP-FAST または EAP-TLS を選択し、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証する場合は、**Check Against CA Certificates** チェックボックスをオンにします。デフォルトの設定は、有効になっています。

j. 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信する証明書内の Common Name（CN; 通常名）をコントローラ上の CA 証明書の CN と照合して検証する場合は、**Verify Certificate CN Identity** チェックボックスをオンにします。デフォルトの設定は、無効になっています。

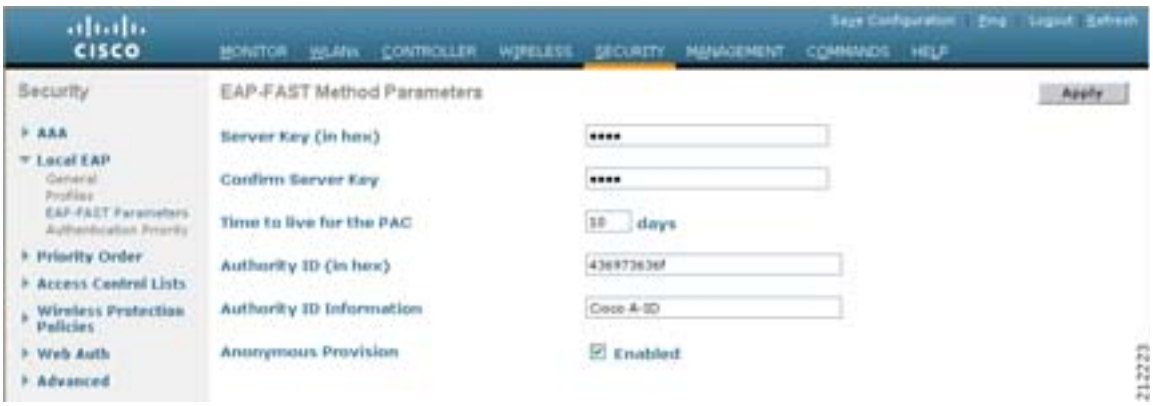
k. 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信するデバイス証明書が現在有効で期限が切れていないことがコントローラで検証されるようにする場合は、**Check Certificate Date Validity** チェックボックスをオンにします。デフォルトの設定は、有効になっています。

l. **Apply** をクリックして、変更を適用します。

ステップ 7　EAP-FAST プロファイルを作成した場合、EAP-FAST パラメータを設定する手順は、次のとおりです。

a. **Security** > **Local EAP** > **EAP-FAST Parameters** の順にクリックして、EAP-FAST Method Parameters ページを開きます（図 5-26 を参照）。

図 5-26　EAP-FAST Method Parameters ページ



b. Server Key フィールドおよび Confirm Server Key フィールドに、PAC の暗号化と暗号化解除に使用するキー（16 進数文字）を入力します。

c. Time to Live for the PAC フィールドに、PAC の有効日数を入力します。有効な範囲は 1 ～ 1000 日で、デフォルトの設定は 10 日です。

d. Authority ID フィールドに、ローカル EAP-FAST サーバの権限識別子を 16 進数文字で入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。

e. Authority ID Information フィールドに、ローカル EAP-FAST サーバの権限識別子をテキスト形式で入力します。

f. 匿名プロビジョニングを有効にするには、**Anonymous Provision** チェックボックスをオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にする場合、PAC は手動でプロビジョニングされる必要があります。デフォルトの設定は、有効になっています。

(注)　ローカル証明書またはクライアント証明書、あるいはその両方が必要で、すべての EAP-FAST クライアントで証明書を使用するよう強制する場合は、**Anonymous Provision** チェックボックスをオフにしてください。

g. **Apply** をクリックして、変更を適用します。

ステップ 8　WLAN 上でローカル EAP を有効にする手順は、次のとおりです。

a. **WLANs** をクリックして、WLANs ページを開きます。

b. 必要な WLAN のプロファイル名をクリックします。

c. WLANs > Edit ページが表示されたら、**Security** > **AAA Servers** タブをクリックし、WLANs > Edit（Security > AAA Servers）ページを開きます（図 5-27 を参照）。

図 5-27　WLANs > Edit（Security > AAA Servers）ページ

d. **Local EAP Authentication** チェックボックスをオンにして、この WLAN に対してローカル EAP を有効にします。

e. EAP Profile Name ドロップダウン ボックスから、この WLAN に使用する EAP プロファイルを選択します。

f. 必要に応じて、LDAP Servers ドロップダウン ボックスから、この WLAN でローカル EAP と共に使用する LDAP サーバを選択します。

g. **Apply** をクリックして、変更を適用します。

ステップ 9　**Save Configuration** をクリックして、変更を保存します。

CLI を使用したローカル EAP の設定

コントローラ CLI を使用してローカル EAP を設定する手順は、次のとおりです。

(注)　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用したローカル EAP の設定」の項（P. 5-40）を参照してください。

ステップ 1　EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority（CA）の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。ローカル EAP でこれらのいずれかのタイプの EAP を使用するよう設定する場合は、適切な証明書と PAC（手動の PAC プロビジョニングを使用する場合）がコントローラにインポートされていることを確認してください。証明書と PAC のインポートの手順については、第 8 章を参照してください。

ステップ 2　コントローラでローカル　ユーザ　データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。手順については、「ローカル ネットワーク ユーザの設定」の項（P. 5-30）を参照してください。

ステップ 3　コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。手順については、「LDAP の設定」の項（P. 5-34）を参照してください。

ステップ 4　ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を指定するには、次のコマンドを入力します。

config local-auth user-credentials {**local** | **ldap**}

(注)　**config local-auth user-credentials ldap local** と入力すると、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap** と入力すると、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

ステップ 5　ローカル EAP タイマーに値を指定するには、次のコマンドを入力します。

- **config local-auth active-timeout** *timeout*：設定済みの RADIUS サーバのペアによる認証が失敗したあとに、コントローラがローカル EAP を使用して無線クライアントを認証する際の試行時間（秒単位）を指定します。有効な範囲は 1 ～ 3600 秒で、デフォルトの設定は 100 秒です。
- **config advanced eap identity-request-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を送信する際の試行時間（秒単位）を指定します。有効な値の範囲は 1 ～ 120 秒で、デフォルトの設定は 1 秒です。
- **config advanced eap identity-request-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ～ 20 回で、デフォルトの設定は 20 回です。

- **config advanced eap key-index** *index*：動的 Wired Equivalent Privacy（WEP）に使用するキー インデックスを指定します。デフォルトの設定は 0 です。
- **config advanced eap request-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに EAP 要求を送信する際の試行時間（秒単位）を指定します。有効な値の範囲は 1 ～ 120 秒で、デフォルトの設定は 1 秒です。
- **config advanced eap request-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに EAP 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ～ 120 回で、デフォルトの設定は 20 回です。
- **config advanced eap identity-request-timeout** *timeout*：コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を指定します。有効な値の範囲は 1 ～ 5 秒で、デフォルトの設定は 1 秒です。
- **config advanced eap eapol-key-retries** *retries*：コントローラがローカル EAP を使用して無線クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ～ 4 回で、デフォルトの設定は 2 回です。
- **config advanced eap max-login-ignore-identity-response** {**enable** | **disable**}：このコマンドを有効にすると、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限できます。同じコントローラ上の異なるデバイス（PDA、ラップトップ、IP 電話など）から最大 8 回ログインできます。デフォルト値は無効（disable）です。

ステップ 6　ローカル EAP プロファイルを作成するには、次のコマンドを入力します。

config local-auth eap-profile add *profile_name*

（注）　プロファイル名にスペースを含めないでください。

（注）　ローカル EAP プロファイルを削除するには、次のコマンドを入力します。**config local-auth eap-profile delete** *profile_name*

ステップ 7　ローカル EAP プロファイルに EAP 方式を追加するには、次のコマンドを入力します。

config local-auth eap-profile method add *method profile_name*

サポートされる方式は、leap、fast、tls、および peap です。

（注）　peap を選択する場合、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。

（注）　プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP　タイプ（証明書を使用する　EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC など）でプロファイルを作成する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。

（注）　ローカル EAP プロファイルから EAP 方式を削除するには、次のコマンドを入力します。**config local-auth eap-profile method delete** *method profile_name*

ステップ 8　EAP-FAST プロファイルを作成した場合に、EAP-FAST パラメータを設定するには、次のコマンドを入力します。

config local-auth method fast *?*

? は、次のいずれかです。

- **anon-prov** {**enable** | **disable**}：コントローラで匿名プロビジョニングが許可されるように設定します。これにより、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。
- **authority-id** *auth_id*：ローカル EAP-FAST サーバの権限識別子を指定します。
- **pac-ttl** *days*：PAC の有効日数を指定します。
- **server-key** *key*：PAC を暗号化および暗号化解除するために使用されるサーバ キーを指定します。

ステップ 9　プロファイルごとに証明書パラメータを設定するには、次のコマンドを入力します。

- **config local-auth eap-profile method fast local-cert** {**enable** | **disable**} *profile_name*：
コントローラ上のデバイスの証明書が認証に必要とされるかどうかを指定します。

（注）　デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile method fast client-cert** {**enable** | **disable**} *profile_name*：
無線クライアントから認証のためのデバイスの証明書をコントローラに送信する必要があるかどうかを指定します。

（注）　クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile cert-issuer {cisco** | **vendor}** *profile_name*：証明書を使用する EAP-FAST、EAP-TLS、または PEAP を指定した場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。
- **config local-auth eap-profile cert-verify ca-issuer** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify cn-verify** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信する証明書内の通常名（CN）をコントローラ上の CA 証明書の CN と照合して検証するかどうかを指定します。
- **config local-auth eap-profile cert-verify date-valid** {**enable** | **disable**} *profile_name*：証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信するデバイスの証明書が現在も有効であり期限が切れていないことがコントローラで検証されるようにするかどうかを指定します。

ステップ 10　ローカル EAP を有効にし、EAP プロファイルを WLAN に接続するには、次のコマンドを入力します。

config wlan local-auth enable *profile_name wlan_id*

（注） WLAN でローカル EAP を無効にするには、次のコマンドを入力します。**config wlan local-auth disable** *wlan_id*

ステップ 11 変更を保存するには、次のコマンドを入力します。

save config

ステップ 12 ローカル EAP に関連する情報を表示するには、次のコマンドを使用します。

- **show local-auth config**：コントローラ上のローカル EAP の設定を表示します。
- **show local-auth statistics**：ローカル EAP の統計情報を表示します。
- **show local-auth certificates**：ローカル EAP で使用可能な証明書を表示します。
- **show local-auth user-credentials**：コントローラがローカル データベースまたは LDAP データベースからユーザの資格情報を取得する際の優先順位を表示します。
- **show advanced eap**：ローカル EAP のタイマーの値を表示します。次のような情報が表示されます。

```
EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries.............. 20
EAP Key-Index for Dynamic WEP................. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)................. 20
EAP-Request Max Retries....................... 20
EAPOL-Key Timeout (seconds)................... 1
EAPOL-Key Max Retries......................... 2
```

- **show wlan** *wlan_id*：特定の WLAN のローカル EAP のステータスを表示します。

たとえば、**show local-auth config** コマンドに対しては、次のような情報が表示されます。

```
User credentials database search order:
   Primary ..................................... Local DB

Configured EAP profiles:
   Name ........................................ fast-cert
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. Yes
       Client certificate required ............. Yes
     Enabled methods ........................... fast
     Configured on WLANs ....................... 1

   Name ........................................ tls
     Certificate issuer ........................ vendor
     Peer verification options:
       Check against CA certificates ........... Enabled
       Verify certificate CN identity .......... Disabled
       Check certificate date validity ......... Enabled
     EAP-FAST configuration:
       Local certificate required .............. No
       Client certificate required ............. No
     Enabled methods ........................... tls
     Configured on WLANs ....................... 2

EAP Method configuration:
   EAP-FAST:
     Server key ................................ <hidden>
     TTL for the PAC ........................... 10
     Anonymous provision allowed ............... Yes
     Accept client on auth prov ................ No
     Authority ID .............................. 436973636f00000000000000000000000
     Authority Information ..................... Cisco A-ID
```

ステップ 13 必要に応じて、次のコマンドを使用してローカル EAP セッションのトラブルシューティングを行います。

- **debug aaa local-auth eap method** {**all** | **errors** | **events** | **packets** | **sm**} {**enable** | **disable**}：ローカル EAP 方式のデバッグを有効または無効にします。
- **debug aaa local-auth eap framework** {**all** | **errors** | **events** | **packets** | **sm**} {**enable** | **disable**}：ローカル EAP フレームワークのデバッグを有効または無効にします。

（注） 上記の 2 つのコマンドでは、**sm** とはステート マシンを指します。

- **clear stats local-auth**：ローカル EAP のカウンタをクリアします。

SpectraLink 社の NetLink 電話用システムの設定

SpectraLink 社の NetLink 電話を Cisco UWN Solution と最適な形で統合するためには、長いプリアンブルを使用できるようにオペレーティング システムを設定する必要があります。無線プリアンブル（ヘッダーとも呼ばれる）とは、パケットの先頭部分のデータ セクションのことであり、ここには、無線デバイスでのパケットの送受信に必要な情報が格納されています。短いプリアンブルの方がスループット パフォーマンスが向上するため、デフォルトではこちらが有効になっています。ただし、SpectraLink 社の NetLink 電話などの一部の無線デバイスでは、長いプリアンブルを使用する必要があります。

長いプリアンブルを有効にするには、次のいずれかの方法を使用します。

- GUI を使用した長いプリアンブルの有効化（P. 5-51）
- CLI を使用した長いプリアンブルの有効化（P. 5-52）

GUI を使用した長いプリアンブルの有効化

GUI を使用して長いプリアンブルを有効化し、無線 LAN 上にある SpectraLink 社の NetLink 電話の動作を最適化する手順は次のとおりです。

ステップ 1　**Wireless** > **802.11b/g/n** > **Network** の順にクリックして、802.11b/g Global Parameters ページを開きます。

ステップ 2　**Short Preamble** チェックボックスがオンの場合は、これ以降の手順に進みます。**Short Preamble** チェックボックスがオフの場合（つまり長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話用に最適化されているため、これ以降の手順を実行する必要はありません。

ステップ 3　**Short Preamble** チェックボックスをオフにして、長いプリアンブルを有効にします。

ステップ 4　**Apply** をクリックして、コントローラの設定を更新します。

（注）　コントローラへの CLI セッションがアクティブでない場合は、CLI セッションを開始してコントローラをリブートし、リブート プロセスを監視することをお勧めします。コントローラがリブートすると GUI が切断されるため、その意味でも CLI セッションは役に立ちます。

ステップ 5　**Commands** > **Reboot** > **Reboot** > **Save and Reboot** の順にクリックして、コントローラをリブートします。次のプロンプトに対し **OK** をクリックします。

```
Configuration will be saved and the controller will be rebooted. Click ok to confirm.
```

コントローラがリブートします。

ステップ 6　コントローラの GUI にもう一度ログインし、コントローラが正しく設定されていることを確認します。

ステップ 7　**Wireless** > **802.11b/g/n** > **Network** の順にクリックして、802.11b/g Global Parameters ページを開きます。**Short Preamble** チェックボックスがオフの場合、コントローラは SpectraLink 社の NetLink 電話用に最適化されています。

CLI を使用した長いプリアンブルの有効化

CLI を使用して長いプリアンブルを有効化し、無線 LAN 上にある SpectraLink 社の NetLink 電話の動作を最適化する手順は次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**show 802.11b** と入力して Short preamble mandatory パラメータをチェックします。短いプリアンブルが有効になっている場合は、以降の手順に進みます。短いプリアンブルが有効な場合、次のように表示されます。

```
Short Preamble mandatory..................... Enabled
```

短いプリアンブルが無効になっている場合（つまり長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話に対して最適化されているため、以降の手順を実行する必要はありません。長いプリアンブルが有効な場合、次のように表示されます。

```
Short Preamble mandatory..................... Disabled
```

ステップ 3　**config 802.11b disable network** と入力して 802.11b/g ネットワークを無効にします。（802.11a ネットワーク上では、長いプリアンブルを有効化できません。）

ステップ 4　**config 802.11b preamble long** と入力して長いプリアンブルを有効にします。

ステップ 5　**config 802.11b enable network** と入力して 802.11b/g ネットワークを再度有効にします。

ステップ 6　**reset system** と入力して、コントローラをリブートします。次のプロンプトに対して **y** と入力します。

```
The system has unsaved changes. Would you like to save them now? (y/n)
```

コントローラがリブートします。

ステップ 7　もう一度 CLI にログインし、**show 802.11b** と入力して次のパラメータを表示し、コントローラが正しく設定されていることを確認します。

```
802.11b Network.............................. Enabled
Short Preamble mandatory..................... Disabled
```

上記のパラメータは、802.11b/g ネットワークが有効になっていて、短いプリアンブルが無効になっていることを示しています。

CLI を使用した Enhanced Distributed Channel Access の設定

次の CLI コマンドを使用すると、802.11 Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータを設定して SpectraLink の電話をサポートできます。

config advanced edca-parameters {**svp-voice** | **wmm-default**}

このとき、次のようになります。

svp-voice は SpectraLink Voice Priority（SVP）パラメータを有効にし、**wmm-default** は Wireless Multimedia（WMM）デフォルト パラメータを有効にします。

（注） このコマンドをコントローラに接続されたすべてのアクセス　ポイントに適用するには、このコマンドを入力した後、802.11b/g ネットワークを無効にし、その後再び有効にしてください。

無線による管理機能の使用

Cisco UWN Solution の無線による管理機能を使用すると、オペレータは、無線クライアントを使用してローカル コントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード（転送）以外のすべての管理タスクに対して使用できます。.

無線による管理機能を使用するには、次のいずれかの方法でコントローラを適切に設定しておく必要があります。

- GUI を使用した無線による管理の有効化（P. 5-54）
- CLI を使用した無線による管理の有効化（P. 5-54）

GUI を使用した無線による管理の有効化

ステップ 1　**Management** > **Mgmt Via Wireless** の順にクリックして、Management Via Wireless ページを開きます。

ステップ 2　**Enable Controller Management to be accessible from Wireless Clients** チェックボックスをオンにして無線による WLAN の管理を有効にするか、オフにしてこの機能を無効にします。デフォルトではオフになっています。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 5　無線クライアント Web ブラウザを使用して、コントローラ管理ポートまたはディストリビューション システム ポート IP アドレスに接続し、コントローラ GUI にログインして、無線クライアントを使用して WLAN を管理できていることを確認します。

CLI を使用した無線による管理の有効化

ステップ 1　CLI で、**show network** コマンドを使用して、Mgmt Via Wireless Interface が Enabled に設定されているか Disabled に設定されているかを確認します。Mgmt Via Wireless Interface が Disabled に設定されている場合は、ステップ 2 に進みます。それ以外の場合は、ステップ 3 に進みます。

ステップ 2　無線による管理を有効にするには、**config network mgmt-via-wireless enable** と入力します。

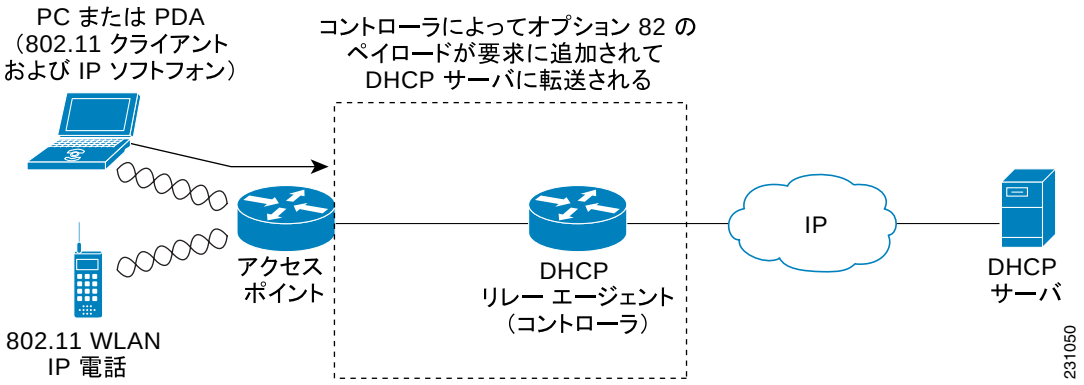
ステップ 3　無線クライアントを使用して、管理対象のコントローラに接続されているアクセス ポイントにアソシエートします。

ステップ 4　**telnet controller-ip-address** と入力して CLI にログインし、無線クライアントを使用して WLAN を管理できることを確認します。

DHCP オプション 82 の設定

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。具体的には、コントローラが DHCP リレイ エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP 要求にオプション 82 情報を追加してから DHCP サーバに転送するように、コントローラを設定することができます。このプロセスの図は、図 5-28 を参照してください。

図 5-28　DHCP オプション 82



アクセス ポイントは、クライアントからのすべての DHCP 要求をコントローラに転送します。コントローラは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。

（注） すでにリレー エージェント オプションが含まれている DHCP パケットは、コントローラでドロップされます。

（注） DHCP オプション 82 は、第 11 章で説明されている自動アンカー モビリティと共に使用することはできません。

次のコマンドを使用して DHCP オプション 82 をコントローラに設定できます。

1. DHCP オプション 82 ペイロードの形式を設定するには、次のコマンドの 1 つを入力します。
   - **config dhcp opt-82 remote-id** *ap_mac*

     このコマンドは DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスを追加します。
   - **config dhcp opt-82 remote-id** *ap_mac:ssid*

     このコマンドは DHCP オプション 82 ペイロードにアクセス ポイントの MAC アドレスと SSID を追加します。
2. コントローラで DHCP オプション 82 を有効または無効にするには、次のコマンドを入力します。

   config interface dhcp ap-manager opt-82 {**enable** | **disable**}

3. コントローラで DHCP オプション 82 のステータスを表示するには、次のコマンドを入力します。

   show interface detailed ap-manager

   次のような情報が表示されます。

```
Interface Name................................. ap-manager
IP Address..................................... 10.30.16.13
IP Netmask..................................... 255.255.248.0
IP Gateway..................................... 10.30.16.1
VLAN........................................... untagged
Active Physical Port........................... LAG (29)
Primary Physical Port.......................... LAG (29)
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.1.0.10
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Enabled
ACL............................................ Unconfigured
AP Manager..................................... Yes
```

アクセス コントロール リストの設定と適用

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、または無線クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは Central Processing Unit（CPU; 中央処理装置）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

または、Web 認証用に事前認証 ACL を作成することもできます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。

（注） 2100 シリーズのコントローラ、または Cisco 28/37/38xx Series Integrated Services Router 内のコントローラ ネットワーク モジュールと共に外部の Web サーバを使用している場合には、WLAN 上でサーバに対する事前認証 ACL を設定する必要があります。

最大で 64 の ACL を定義することができ、各 ACL に最大 64 のルール（またはフィルタ）を設定できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが 1 つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。

（注） すべての ACL には、暗黙的に最後のルールとして「すべてのルールを拒否」が適用されます。パケットがどのルールとも一致しない場合、コントローラによってドロップされます。

ACL は、GUI または CLI のいずれかを使用して設定および適用できます。

GUI を使用したアクセス コントロール リストの設定

コントローラ GUI を使用して ACL を設定する手順は、次のとおりです。

ステップ 1　**Security** > **Access Control Lists** > **Access Control Lists** の順にクリックして、Access Control Lists ページを開きます（図 5-29 を参照）。

図 5-29　Access Control Lists ページ

このページでは、このコントローラに設定されたすべての ACL が表示されます。

（注） 既存の ACL を削除するには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　パケットがコントローラ上で設定されている ACL のいずれかに一致しているかどうかを確認する場合は、**Enable Counters** チェックボックスをオンにして、**Apply** をクリックします。それ以外の場合は、このチェックボックスをオフのままにします（デフォルト値）。この機能は、システムのトラブルシューティングを実行する際に役立ちます。

（注） ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、**Clear Counters** を選択します。

（注） ACL カウンタは、次のコントローラ上でのみ使用可能です。4400 シリーズ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチ。

ステップ 3　新しい ACL を追加するには、**New** をクリックします。Access Control Lists > New ページが表示されます（図 5-30 を参照）。

図 5-30　Access Control Lists > New ページ

ステップ 4　Access Control List Name フィールドに新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 5　**Apply** をクリックします。Access Control Lists ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6　Access Control Lists > Edit ページが表示されたら、**Add New Rule** をクリックします。Access Control Lists > Rules > New ページが表示されます（図 5-31 を参照）。

図 5-31　Access Control Lists > Rules > New ページ

ステップ 7　この ACL にルールを設定する手順は、次のとおりです。

a. コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは 1 ～ 64 の順にリストされます。Sequence フィールドに値（1 ～ 64）を入力し、この ACL に定義された他のルールとの順序関係を明確にします。

（注） ルール 1 ～ 4 がすでに設定されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加したり、変更した場合には、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ、自動的に 6 および 7 へと番号が変更されます。

b. Source ドロップダウン ボックスから、これらオプションの 1 つを選択して、この ACL を適用するパケットのソースを指定します。

- **Any**：任意のソース（これは、デフォルト値です）。
- **IP Address**：特定のソース。このオプションを選択した場合、編集ボックスに、ソースの IP アドレスとネットマスクを入力します。

c. Destination ドロップダウン ボックスから、これらオプションの 1 つを選択して、この ACL を適用するパケットの宛先を指定します。

- **Any**：任意の宛先（これは、デフォルト値です）。
- **IP Address**：特定の宛先。このオプションを選択した場合、編集ボックスに、宛先の IP アドレスとネットマスクを入力します。

d. Protocol ドロップダウン ボックスから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコル オプションは次のとおりです。

- **Any**：任意のプロトコル（これは、デフォルト値です）
- **TCP**：Transmission Control Protocol
- **UDP**：ユーザ データグラム プロトコル
- **ICMP**：インターネット制御メッセージ プロトコル
- **ESP**：IP Encapsulating Security Payload
- **AH**：認証ヘッダー

- **GRE**：総称ルーティング カプセル化
- **IP in IP**：Internet Protocol（IP; インターネット プロトコル）内 IP。IP-in-IP パケットを許可または拒否します。
- **Eth Over IP**：Ethernet-over-Internet プロトコル
- **OSPF**：Open Shortest Path First
- **Other**：その他の Internet Assigned Numbers Authority（IANA）プロトコル

（注） **Other** を選択する場合は、Protocol 編集ボックスに目的のプロトコルの番号を入力します。次の URL で、使用可能なプロトコルと対応する番号の一覧にアクセスできます。http://www.iana.org/assignments/protocol-numbers

（注） コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。

e. 前の手順で TCP または UDP を選択すると、Source Port および Destination Port の 2 つのパラメータも追加で表示されます。これらパラメータを使用すれば、特定のソース ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、ネットワーキング スタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、telnet、ssh、http などの特定のアプリケーション用に指定されています。

f. DSCP ドロップダウン ボックスから、これらオプションの 1 つを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。DSCP は、インターネット上のサービスの質を定義するのに使用できる IP ヘッダ フィールドです。

- **Any**：任意の DSCP（これは、デフォルト値です）
- **Specific**：DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

g. Direction ドロップダウン ボックスから、これらオプションの 1 つを選択して、この ACL を適用するトラフィックの方向を指定します。

- **Any**：任意の方向（これは、デフォルト値です）
- **Inbound**：クライアントから
- **Outbound**：クライアントへ

（注） この ACL をコントローラ CPU に適用することを計画している場合は、**Any** または **Inbound** を選択してください。これは、CPU ACL は、CPU から送信されたパケットではなく、CPU に送信されたパケットのみに適用されるためです。

h. Action ドロップダウン ボックスから、**Deny** を選択してこの ACL でパケットがブロックされるようにするか、**Permit** を選択してこの ACL でパケットが許可されるようにします。デフォルト値は Deny です。

i. **Apply** をクリックして、変更を適用します。Access Control Lists > Edit ページが再表示され、この ACL のルールが示されます。図 5-32 を参照してください。

図 5-32　Access Control Lists > Edit ページ

Deny Counters フィールドには、パケットが明示的拒否 ACL ルールに一致した回数が表示されます。Number of Hits フィールドには、パケットが ACL ルールに一致した回数が表示されます。これらのフィールドを有効にするには、Access Control Lists ページ上で ACL カウンタを有効にする必要があります。

（注） ルールを編集する場合は、希望のルールのシーケンス番号をクリックし、Access Control Lists > Rules > Edit ページを開きます。ルールを削除するには、目的のルールの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

j. この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 8　**Save Configuration** をクリックして、変更を保存します。

ステップ 9　さらに ACL を追加するにはこの手順を繰り返します。

GUI を使用したアクセス コントロール リストの適用

コントローラ GUI を使用して ACL を適用するには、次の項の指示に従ってください。

- インターフェイスへのアクセス コントロール リストの適用（P. 5-61）
- コントローラ CPU へのアクセス コントロール リストの適用（P. 5-63）
- WLAN へのアクセス コントロール リストの適用（P. 5-64）
- WLAN への事前認証アクセス コントロール リストの適用（P. 5-64）

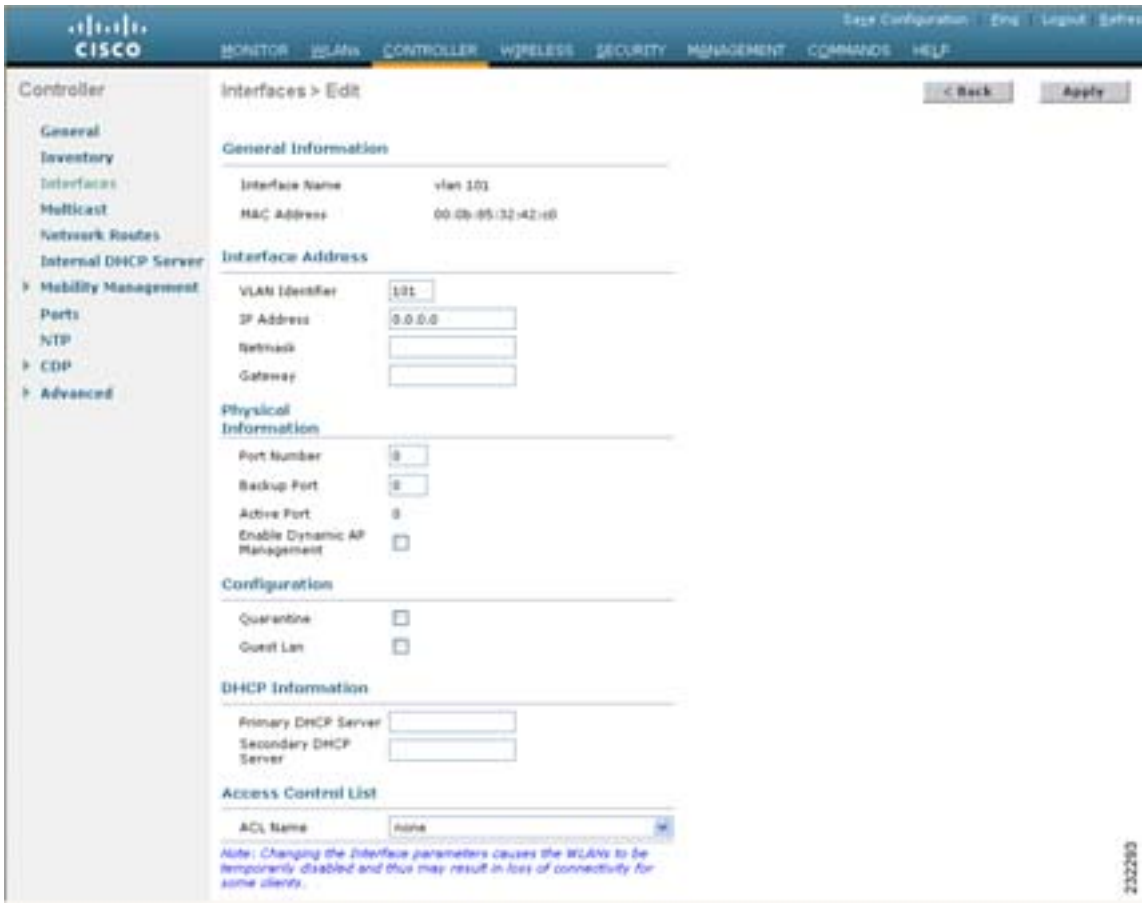
インターフェイスへのアクセス コントロール リストの適用

コントローラの GUI を使用して管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスに ACL を適用する手順は、次のとおりです。

ステップ 1　**Controller** > **Interfaces** の順にクリックします。

ステップ 2　必要なインターフェイスの名前をクリックします。そのインターフェイスの Interfaces > Edit ページが表示されます（図 5-33 を参照）。

図 5-33　Interfaces > Edit ページ



ステップ 3　ACL Name ドロップダウン ボックスから必要な ACL を選択し、**Apply** をクリックします。デフォルト値は None です。

（注）　コントローラ インターフェイスの設定の詳細は、第 3 章を参照してください。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

コントローラ CPU へのアクセス コントロール リストの適用

コントローラの GUI を使用して、コントローラの CPU に ACL を適用し、CPU へのトラフィックを制御する手順は、次のとおりです。

ステップ 1　**Security** > **Access Control Lists** > **CPU Access Control Lists** を選択します。CPU Access Control Lists ページが表示されます（図 5-34 を参照）。

図 5-34　CPU Access Control Lists ページ

ステップ 2　**Enable CPU ACL** チェックボックスをオンにして、指定した ACL でコントローラの CPU へのトラフィックを制御できるようにするか、チェックボックスをオフにして CPU ACL の機能を無効にし、CPU にすでに適用されている ACL をすべて削除します。デフォルトではオフになっています。

ステップ 3　ACL Name ドロップダウン ボックスから、コントローラの CPU へのトラフィックを制御する ACL を選択します。デフォルト値は None で、CPU ACL 機能は無効にされています。CPU ACL Enable チェックボックスをオンにして、None を選択すると、ACL を選択する必要があることを示すエラーメッセージが表示されます。

（注）　このパラメータは、CPU ACL Enable チェックボックスをオンにした場合のみ使用できます。

ステップ 4　CPU ACL Mode ドロップダウン ボックスから、コントローラの CPU への転送が制限されるトラフィックのタイプ（有線、無線、または両方）を選択します。デフォルト値は Wired です。

（注）　このパラメータは、CPU ACL Enable チェックボックスをオンにした場合のみ使用できます。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

WLAN へのアクセス コントロール リストの適用

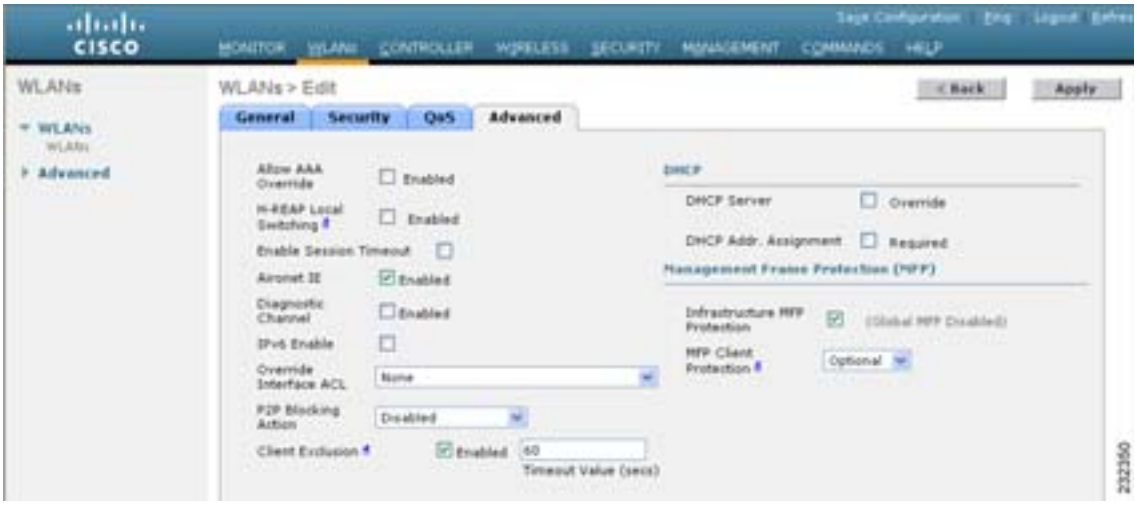
コントローラの GUI を使用して ACL を WLAN に適用する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Advanced** タブをクリックして、WLANs > Edit (Advanced) ページを開きます（図 5-35 を参照）。

図 5-35　WLANs > Edit (Advanced) ページ



ステップ 4　Override Interface ACL ドロップダウン ボックスから、この WLAN に適用する ACL を選択します。選択した ACL は、インターフェイスに設定されたすべての ACL を上書きします。デフォルト値は None です。

（注）　WLAN の設定の詳細は、第 6 章を参照してください。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

WLAN への事前認証アクセス コントロール リストの適用

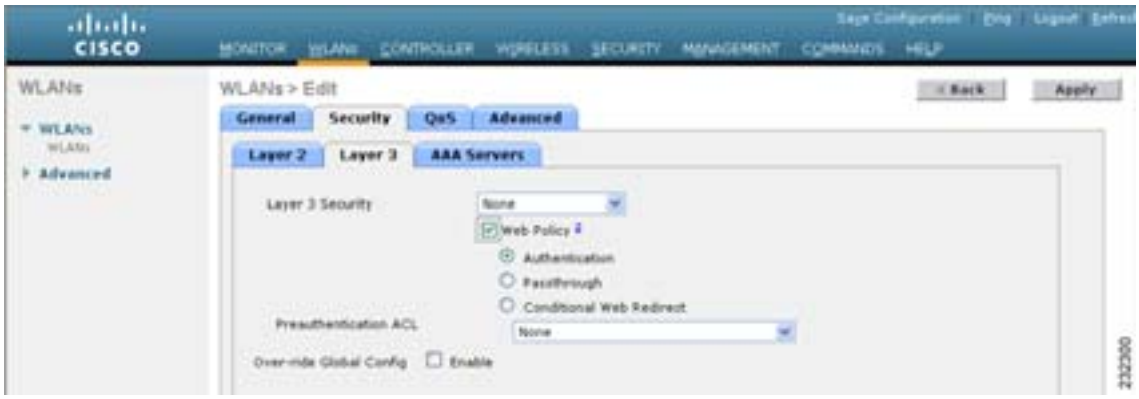
コントローラの GUI を使用して事前認証 ACL を WLAN に適用する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Security** タブおよび **Layer 3** タブをクリックして、WLANs > Edit（Security > Layer 3）ページを開きます（図 5-36 を参照）。

図 5-36　WLANs > Edit（Security > Layer 3）ページ



ステップ 4　**Web Policy** チェックボックスをオンにします。

ステップ 5　Preauthentication ACL ドロップダウン ボックスから必要な ACL を選択し、**Apply** をクリックします。デフォルト値は None です。

（注）　WLAN の設定の詳細は、第 6 章を参照してください。

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

CLI を使用したアクセス コントロール リストの設定

コントローラ CLI を使用して ACL を設定する手順は、次のとおりです。

ステップ 1　コントローラ上に設定されているすべての ACL を表示するには、次のコマンドを入力します。

show acl summary

次のような情報が表示されます。

```
ACL Counter Status         Enabled
-------------------------------------
ACL Name                    Applied
------------------------- -----------
acl1                          Yes
acl2                          Yes
acl3                         Yes
```

ステップ 2　特定の ACL の詳細情報を表示するには、次のコマンドを入力します。

show acl detailed *acl_name*

次のような情報が表示されます。

```
            Source          Destination        Source Port Dest Port
I Dir IP Address/Netmask IP Address/Netmask Prot    Range Range   DSCP Action Counter
- --- ------------------ ------------------ ---- ----------- -------- ----- ------
-------
1 Any 0.0.0.0/0.0.0.0   0.0.0.0/0.0.0.0   Any    0-65535  0-65535  0    Deny    0
2 In  0.0.0.0/0.0.0.0   200.200.200.0/     6     80-80    0-65535  Any  Permit  0
                        255.255.255.0

DenyCounter :     0
```

Counter フィールドはパケットが ACL ルールに一致する場合に毎回増分され、DenyCounter フィールドはパケットがいずれのルールにも一致しない場合に毎回増分されます。

ステップ 3　コントローラの ACL カウンタを有効または無効にするには、次のコマンドを入力します。

config acl counter {**start** | **stop**}

（注）　ACL の現在のカウンタをクリアする場合は、次のコマンドを入力します。
clear acl counters *acl_name*

（注）　ACL カウンタは、次のコントローラ上でのみ使用可能です。4400 シリーズ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチ。

ステップ 4　新しい ACL を追加するには、次のコマンドを入力します。

config acl create *acl_name*

acl_name パラメータには、最大 32 文字の英数字を入力できます。

ステップ 5　ACL に新しいルールを追加するには、次のコマンドを入力します。

config acl rule add *acl_name rule_index*

ステップ 6　ACL ルールを設定するには、次のコマンドを入力します。

config acl rule {

action *acl_name rule_index* {**permit** | **deny**} |

change index *acl_name old_index new_index* |

destination address *acl_name rule_index ip_address netmask* |

destination port range *acl_name rule_index start_port end_port* |

direction *acl_name rule_index* {**in** | **out** | **any**} |

dscp *acl_name rule_index dscp* |

protocol *acl_name rule_index protocol* |

source address *acl_name rule_index ip_address netmask* |

source port range *acl_name rule_index start_port end_port* |

swap index *acl_name index_1 index_2*}

ルール パラメータの説明については、「GUI を使用したアクセス コントロール リストの設定」の項（P. 5-57）のステップ 7 を参照してください。

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

（注）　ACL を削除するには、**config acl delete** *acl_name* を入力します。ACL ルールを削除するには、**config acl rule delete** *acl_name rule_index* を入力します。

CLI を使用したアクセス コントロール リストの適用

コントローラ CLI を使用して ACL を適用する手順は、次のとおりです。

ステップ 1　次のいずれかの操作を行います。

- 管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスに ACL を適用するには、次のコマンドを入力します。

  config interface acl {**management** | **ap-manager** | *dynamic_interface_name*} *acl_name*

  （注）　インターフェイスに適用されている ACL を表示するには、**show interface detailed** {**management** | **ap-manager** | *dynamic_interface_name*} と入力します。インターフェイスに適用されている ACL を削除するには、**config interface acl** {**management** | **ap-manager** | *dynamic_interface_name*} **none** と入力します。

  コントローラ インターフェイスの設定の詳細は、第 3 章を参照してください。

- ACL をデータ パスに適用するには、次のコマンドを入力します。

  config acl apply *acl_name*

- ACL をコントローラの CPU に適用して、CPU に転送されるトラフィックのタイプ（有線、無線、または両方）を制限するには、次のコマンドを入力します。

  config acl cpu *acl_name* {**wired** | **wireless** | **both**}

  （注）　コントローラ CPU に適用されている ACL を表示するには、**show acl cpu** と入力します。コントローラ CPU に適用されている ACL を削除するには、**config acl cpu none** と入力します。

- ACL を WLAN に適用するには、次のコマンドを入力します。
  config wlan acl *wlan_id acl_name*

（注） WLAN に適用されている ACL を表示するには、**show wlan** *wlan_id* と入力します。WLAN に適用されている ACL を削除するには、**config wlan acl** *wlan_id* **none** と入力します。

- 事前認証 ACL を WLAN に適用するには、次のコマンドを入力します。
  config wlan security web-auth *acl* *wlan_id acl_name*
  WLAN の設定の詳細は、第 6 章を参照してください。

ステップ 2　設定を保存するには、次のコマンドを入力します。

save config

管理フレーム保護の設定

Management Frame Protection（MFP; 管理フレーム保護）では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。コントローラ ソフトウェア リリース 4.0 は、インフラストラクチャ MFP のみをサポートするのに対し、コントローラ ソフトウェア リリース 4.1 以降は、インフラストラクチャとクライアント MFP の両方をサポートします。

- **インフラストラクチャ MFP**：DoS 攻撃を引き起こしたり、ネットワーク上で過剰なアソシエーションやプローブを生じさせたり、不正アクセス ポイントとして介入したり、QoS と無線測定フレームへの攻撃によりネットワーク パフォーマンスを低下させたりする敵対者を検出することにより、管理フレームを保護します。インフラストラクチャ MFP はまた、フィッシング インシデントの効果的かつ迅速な検出 / 報告手段を提供します。

  インフラストラクチャ MFP は特に、アクセス ポイントによって送信され（クライアントによって送信されたのではなく）、次にネットワーク内の他のアクセス ポイントによって検証される管理フレームに、Message Integrity Check Information Element（MIC IE; メッセージ整合性情報要素）を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- **クライアント MFP**：認証されたクライアントをスプーフィング フレームからシールドし、無線 LAN に対する多数の共通の攻撃が威力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを劣化させます。

  クライアント MFP は特に、アクセス ポイントと CCXv5 クライアント間で送受信される管理フレームを暗号化します。これにより、アクセス ポイントとクライアントの両方で、スプーフィングされたクラス 3 管理フレーム（つまり、アクセス ポイントと認証され関連付けられたクライアント間でやり取りされる管理フレーム）をドロップすることにより、予防措置をとることができます。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS（WMM）アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP は、最も一般的な種類のサービス拒否攻撃から、クライアントとアクセス ポイント間のセッションを保護します。また、セッションのデータ フレームに使用されているのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

  クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしており、TKIP または AES-CCMP のいずれかを使用して WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用されます。CCKM およびコントローラのモビリティ管理は、レイヤ 2 およびレイヤ 3 の高速ローミングのために、アクセス ポイント間でセッション キーを分散するのに使用されます。

（注） ブロードキャスト フレームを使用した攻撃を防ぐため、CCXv5 をサポートするアクセス ポイントでは、ブロードキャスト クラス 3 管理フレーム（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントおよびアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄する必要があります。

インフラストラクチャ MFP は、クライアント MFP 対応でないクライアントに送信された無効なユニキャスト フレームと、無効なクラス 1 およびクラス 2 管理フレームを引き続き検出および報告するため、クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足するものであると言えます。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- **管理フレーム保護**：アクセス ポイントでは、送信される管理フレームが、各フレームに MIC IE を追加することによって保護されます。フレームのコピー、変更、リプレイが試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。
- **管理フレーム検証**：アクセス ポイントでは、インフラストラクチャ MFP によって、ネットワークの他のアクセス ポイントから受信する各管理フレームが検証されます。MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの有効な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能できるように、すべてのコントローラはネットワーク タイム プロトコル（NTP）で同期化されている必要があります。
- **イベント報告**：アクセス ポイントで異常が検出されるとコントローラに通知されます。コントローラでは、受信した異常イベントが集計され、その結果が SNMP トラップを使用してネットワーク管理システムに報告されます。

（注） スタンドアロン モードの Hybrid REAP アクセス ポイントで生成されるエラー レポートは、コントローラに転送することはできず、ドロップされます。

（注） クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効にされ、グローバルに無効化できます。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント認証が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はグローバルに無効になります。インフラストラクチャ MFP がグローバルに有効化されると、選択した WLAN に対してシグニチャの生成（MIC を送信フレームに追加する）を無効にでき、選択したアクセス ポイントに対して検証を無効にできます。

クライアント MFP は、WPA2 に対して設定された WLAN 上でデフォルトで有効にされています。選択した WLAN 上で、無効にすることも、必須にすることも（この場合 MFP をネゴシエートするクライアントのみがアソシエーションを許可されます）できます。

MFP は、GUI または CLI のいずれを使用しても設定できます。

MFP の使用に関するガイドライン

MFP を使用する際のガイドラインは次のとおりです。

- MFP は、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。
- Lightweight アクセス ポイントでは、ローカル モードおよび監視モードで、およびアクセス ポイントがコントローラに接続されているときは Hybrid REAP モードで MFP がサポートされます。ローカル モード、Hybrid REAP モード、およびブリッジ モードで、MFP がサポートされます。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでの使用のみがサポートされています。
- クライアント MFP が無効にされているか、オプションである場合は、非 CCXv5 クライアントは WLAN にアソシエートできます。

GUI を使用した MFP の設定

コントローラ GUI を使用して MFP を設定する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **AP Authentication/MFP** の順にクリックします。AP Authentication Policy ページが表示されます（図 5-37 を参照）。

図 5-37　AP Authentication Policy ページ

ステップ 2　コントローラでインフラストラクチャ MFP をグローバルに有効化するには、Protection Type ドロップダウン ボックスから **Management Frame Protection** を選択します。

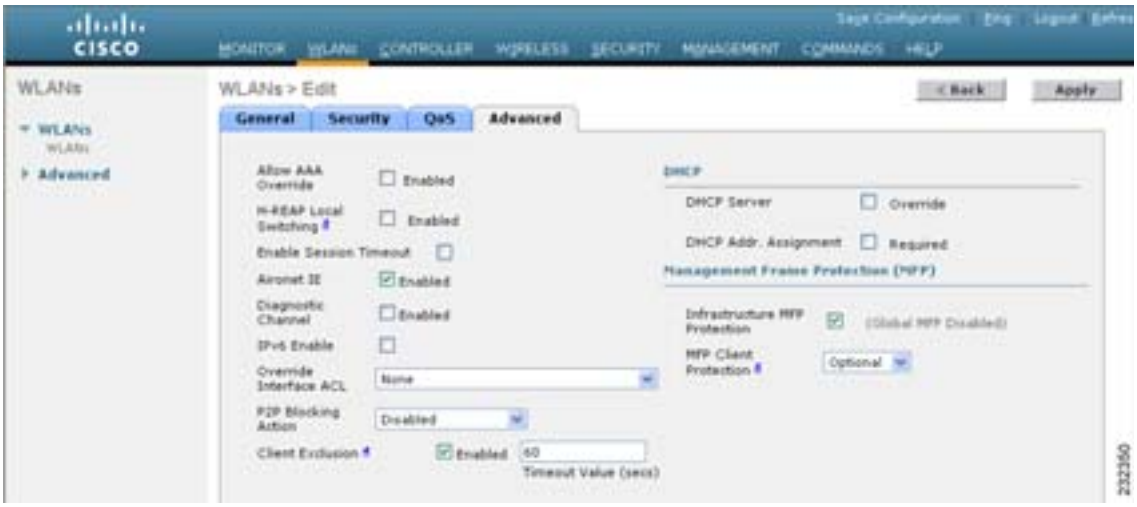
ステップ 3　**Apply** をクリックして、変更を適用します。

（注）　複数のコントローラがモビリティ グループに含まれている場合は、インフラストラクチャ MFP に対して設定されているモビリティ グループ内のすべてのコントローラ上で、Network Time Protocol（NTP）サーバを設定する必要があります。

ステップ 4　コントローラで MFP をグローバルで有効化した後、特定の WLAN に対してインフラストラクチャ MFP 保護の無効化や再有効化を行う手順は、次のとおりです。

a. **WLANs** をクリックします。
b. 必要な WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。
c. **Advanced** をクリックします。WLANs > Edit (Advanced) ページが表示されます（図 5-38 を参照）。

図 5-38　WLANs > Edit (Advanced) ページ



d. **Infrastructure MFP Protection** チェックボックスをオフにしてこの WLAN に対して MFP を無効にするか、このチェックボックスをオンにしてこの WLAN に対して MFP を有効にします。デフォルト値は有効（enable）です。グローバル MFP が無効にされている場合、チェックボックスの右側のカッコ内に注意が表示されます。

e. MFP Client Protection ドロップダウン ボックスから、**Disabled**、**Optional**、または **Required** を選択します。デフォルト値は Optional です。Required を選択した場合、MFP がネゴシエートされている場合（つまり、WPA2 がコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 に対して設定されている場合）のみ、クライアントはアソシエーションを許可されます。

f. **Apply** をクリックして、変更を適用します。

ステップ 5　コントローラでインフラストラクチャ MFP をグローバルで有効化した後、特定のアクセス ポイントに対してインフラストラクチャ MFP 検証の無効化や再有効化を行う手順は、次のとおりです。

a. **Wireless** > **Access Points** の順にクリックして、All APs ページを開きます。

b. 目的のアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます。

c. General で、**MFP Frame Validation** チェックボックスをオフにしてこのアクセス ポイントに対して MFP を無効にするか、このチェックボックスをオンにしてこのアクセス ポイントに対して MFP を有効にします。デフォルト値は有効（enable）です。グローバル MFP が無効にされている場合、チェックボックスの右側のカッコ内に注意が表示されます。

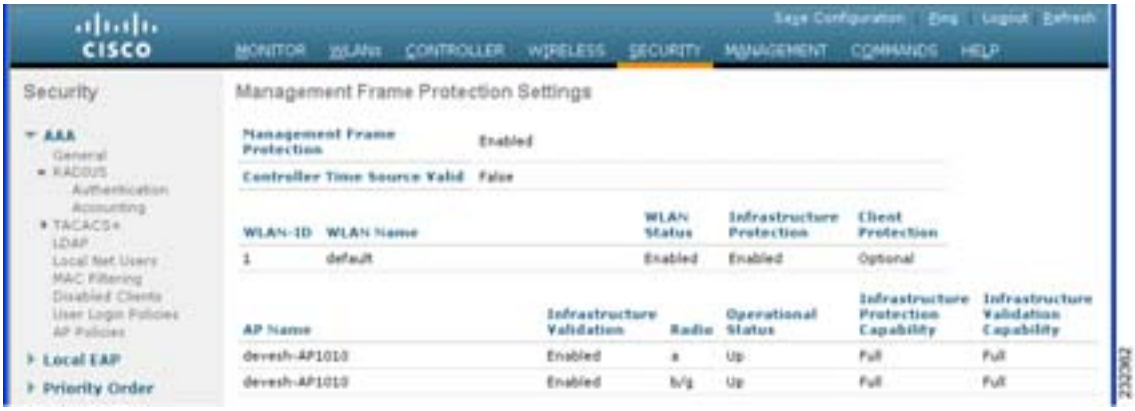
d. **Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、設定を保存します。

GUI を使用した MFP 設定の表示

コントローラの現在のグローバル MFP の設定を表示するには、**Security** > **Wireless Protection Policies** > **Management Frame Protection** の順にクリックします。Management Frame Protection Settings ページが表示されます（図 5-39 を参照）。

図 5-39　Management Frame Protection Settings ページ



このページでは、次の MFP 設定が表示されます。

- Management Frame Protection フィールドは、インフラストラクチャ MFP がコントローラでグローバルに有効化されているかどうかを示します。
- Controller Time Source Valid フィールドは、コントローラの時刻が（時刻を手動で入力することにより）ローカルで設定されているか、外部ソース（NTP サーバなど）を通して設定されているかを示します。時刻が外部ソースにより設定されている場合、このフィールドの値は「True」です。時刻がローカルで設定されている場合、このフィールドの値は「False」です。時刻ソースは、モビリティ グループ内の複数のコントローラのアクセス ポイント間の管理フレーム上のタイムスタンプの検証に使用されます。
- Infrastructure Protection フィールドは、インフラストラクチャ MFP が個別の WLAN に対して有効化されているかどうかを示します。
- Client Protection フィールドは、クライアント MFP が個別の WLAN に対して有効化されているかどうかと、オプションまたは必須のいずれであるかを示します。
- Infrastructure Validation フィールドは、インフラストラクチャ MFP が個別のアクセス ポイントに対して有効化されているかどうかを示します。

CLI を使用した MFP の設定

コントローラ CLI を使用して MFP を設定するには、次のコマンドを使用します。

1. コントローラでインフラストラクチャ MFP をグローバルに有効または無効にするには、次のコマンドを入力します。

   config wps mfp infrastructure {**enable** | **disable**}

2. WLAN で MFP シグニチャの生成を有効または無効にするには、次のコマンドを入力します。

   config wlan mfp infrastructure protection {**enable** | **disable**} *wlan_id*

（注） シグニチャの生成は、インフラストラクチャ MFP がグローバルに有効にされている場合のみ、アクティブ化されます。

3. アクセス ポイントでインフラストラクチャ MFP 検証を有効または無効にするには、次のコマンドを入力します。

   config ap mfp infrastructure validation {**enable** | **disable**} *Cisco_AP*

   (注) MFP 検証は、インフラストラクチャ MFP がグローバルに有効にされている場合のみ、アクティブ化されます。

4. 特定の WLAN でクライアント MFP シグニチャを有効または無効にするには、次のコマンドを入力します。

   config wlan mfp client {**enable** | **disable**} *wlan_id* [**required**]

   クライアント MFP を有効にしてオプションの **required** パラメータを使用すると、MFP がネゴシエートされている場合のみ、クライアントはアソシエーションを許可されます。

CLI を使用した MFP 設定の表示

コントローラの CLI を使用して MFP の設定を表示するには、次のコマンドを使用します。

1. コントローラの現在の MFP の設定を表示するには、次のコマンドを入力します。

   show wps mfp summary

   次のような情報が表示されます。

```
Global Infrastructure MFP state.... Enabled
Controller Time Source Valid....... False

 WLAN       Infra.      Client
WLAN ID  WLAN Name Status     Protection  Protection
-------  ---------- -------- ----------  -----------
1        test1     Enabled  Disabled  Disabled
2        open      Enabled  Enabled    Required
3        testpsk    Enabled   *Enabled   Optional but inactive (WPA2 not
configured)

  Infra.             Operational     --Infra. Capability--
AP Name  Validation  Radio  State           Protection  Validation
-------- ----------- -----  -----------  ----------- -----------
mapAP   Disabled    a   Up              Full        Full
     b/g   Up              Full        Full
rootAP2  Enabled    a    Up              Full        Full
     b/g   Up              Full        Full
HReap   *Enabled   b/g   Up     Full        Full
     a      Down      Full        Full
```

2. 特定の WLAN の現在の MFP 設定を表示するには、次のコマンドを入力します。

   show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.......................... 1
Profile Name............................. test1
Network Name (SSID)...................... test1
Status................................... Enabled
MAC Filtering............................ Disabled
Broadcast SSID........................... Enabled
...
Local EAP Authentication................. Enabled (Profile 'test')
Diagnostics Channel...................... Disabled
Security

   802.11 Authentication:................ Open System
   Static WEP Keys....................... Disabled
   802.1X................................ Enabled
        Encryption:...................... 104-bit WEP
   Wi-Fi Protected Access (WPA/WPA2)..... Disabled
   CKIP ................................. Disabled
   IP Security........................... Disabled
   IP Security Passthru.................. Disabled
   Web Based Authentication.............. Disabled
   Web-Passthrough....................... Disabled
   Conditional Web Redirect.............. Disabled
   Auto Anchor........................... Enabled
   Cranite Passthru...................... Disabled
   H-REAP Local Switching................ Disabled
   Infrastructure MFP protection..... Enabled
   Client MFP............................ Required
...
```

3. 特定のアクセス ポイントの現在の MFP 設定を表示するには、次のコマンドを入力します。

   show ap config general *AP_name*

   次のような情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... ap:52:c5:c0
AP Regulatory Domain............................. 80211bg: -N 80211a: -N
Switch Port Number .............................. 1
MAC Address...................................... 00:0b:85:52:c5:c0
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.67.73.33
IP NetMask....................................... 255.255.255.192
...
AP Mode ......................................... Local
Remote AP Debug ................................. Disabled
S/W  Version .................................... 4.0.2.0
Boot  Version ................................... 2.1.78.0
Mini IOS Version ................................      --
Stats Reporting Period .......................... 180
LED State........................................ Enabled
ILP Pre Standard Switch.......................... Disabled
ILP Power Injector............................... Disabled
Number Of Slots.................................. 2
AP Model......................................... AP1020
AP Serial Number................................. WCN09260057
AP Certificate Type.............................. Manufacture Installed
Management Frame Protection Validation .......... Enabled
```

4. 特定のクライアントでクライアント MFP が有効にされているかどうかを表示するには、次のコマンドを入力します。

   show client detail *client_mac*

```
Client MAC Address.............................. 00:14:1c:ed:34:72
...
Policy Type..................................... WPA2
Authentication Key Management................... PSK
Encryption Cipher............................... CCMP (AES)
Management Frame Protection..................... Yes
...
```

5. コントローラの MFP 統計を表示するには、次のコマンドを入力します。

   show wps mfp statistics

   次のような情報が表示されます。

(注) 実際に攻撃が進行中でない限り、このレポートにデータは含まれません。ここに示すさまざまなエラーの種類の例は、図示のみを目的としています。この表は 5 分ごとにクリアされ、データはネットワーク管理ステーションに転送されます。

```
BSSID             Radio Validator AP Last Source Addr  Found  Error Type Count Frame Types
----------------- ----- ------------ ----------------- ------ ------------ ----- -------
00:0b:85:56:c1:a0  a    jatwo-1000b 00:01:02:03:04:05 Infra  Invalid MIC 183  Assoc Req
                                                                             Probe Req
                                                                             Beacon
                                                    Infra  Out of seq     4  Assoc Req
                                                    Infra  Unexpected MIC 85 Reassoc Req
                                                    Client Decrypt err  1974 Reassoc Req
                                                                             Disassoc
                                                    Client Replay err     74 Assoc Req
                                                                             Probe Req
                                                                             Beacon
                                                    Client Invalid ICV   174 Reassoc Req
                                                                             Disassoc
                                                    Client Invalid header174 Assoc Req
                                                                             Probe Req
                                                                             Beacon
                                                    Client Brdcst disass 174 Reassoc Req
                                                                             Disassoc
00:0b:85:56:c1:a0  b/g  jatwo-1000b 00:01:02:03:04:05 Infra  Out of seq  185 Reassoc Resp
                                                    Client Not encrypted 174 Assoc Resp
                                                                             Probe Resp
```

CLI を使用した MFP に関する問題のデバッグ

MFP に関する問題が発生した場合は、次のコマンドを使用します。

- **debug wps mfp** *?*{**enable** | **disable**}

  ? は、次のいずれかです。

  client：クライアントの MFP メッセージのデバッグについて設定します。

  lwapp：コントローラとアクセス ポイント間の MFP メッセージのデバッグについて設定します。

  detail：MFP メッセージの詳細なデバッグについて設定します。

  report：MFP レポートのデバッグについて設定します。

  mm：MFP モビリティ（コントローラ間）メッセージのデバッグについて設定します。

クライアント除外ポリシーの設定

特定の条件下で、コントロール GUI を使用してクライアントを除外するようにコントローラを設定する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **Client Exclusion Policies** の順にクリックして、Client Exclusion Policies ページを開きます。

ステップ 2　指定された条件においてコントローラでクライアントを除外するには、これらのいずれかのチェックボックスをオンにします。各除外ポリシーのデフォルト値は有効（enable）です。

- **Excessive 802.11 Association Failures**：クライアントは、802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- **Excessive 802.11 Authentication Failures**：クライアントは、802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- **Excessive 802.1X Authentication Failures**：クライアントは、802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- **IP Theft or IP Reuse**：IP アドレスが他のデバイスにすでに割り当てられている場合、クライアントは除外されます。
- **Excessive Web Authentication Failures**：クライアントは、Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ID ネットワーキングの設定

この項では、ID ネットワーキング機能とその設定方法、およびさまざまなセキュリティ ポリシーに対して予想される動作について説明します。

ID ネットワーキングの概要

ほとんどの無線 LAN システムの場合、各 WLAN に静的なポリシーがあり、SSID が設定されているすべてのクライアントに適用されます。これは強力な方式ですが、クライアントに複数の Quality Of Service（QoS）およびセキュリティ ポリシーを適用するには、そのクライアントに複数の SSID を設定する必要があるために、限界がありました。

これに対して Cisco Wireless LAN Solution は、ID ネットワーキングをサポートしています。これは、ネットワークが 1 つの SSID をアドバタイズできるようにすると同時に、特定のユーザに対して、ユーザ プロファイルに基づいて異なる QoS またはセキュリティ ポリシーの適用を可能にするものです。ID ネットワーキングを使用して制御できるポリシーには、次のものがあります。

- Quality Of Service。RADIUS Access Accept に QoS-Level 値が指定されている場合、WLAN プロファイルで指定された QoS 値が上書きされます。
- ACL。RADIUS Access Accept に ACL 属性が指定されている場合、システムでは ACL-Name が認証後にクライアント ステーションに適用されます。これにより、そのインターフェイスに割り当てられている ACL がすべて上書きされます。
- VLAN。VLAN Interface-Name または VLAN-Tag が RADIUS Access Accept に存在する場合は、クライアントが特定のインターフェイス上に配置されます。

（注）　VLAN 機能は、MAC フィルタリング、802.1X、および WPA のみをサポートします。Web 認証または IPSec はサポートしません。

- トンネル属性。

（注）　この項で後述する他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

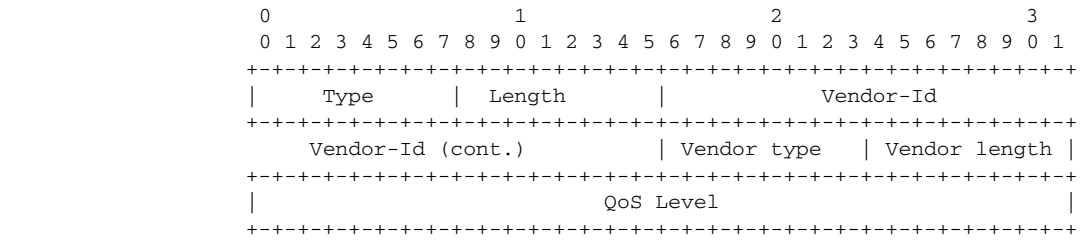
オペレーティング システムのローカル MAC フィルタ データベースは、インターフェイス名を含むように拡張され、ローカル MAC フィルタで、クライアントが割り当てられるインターフェイスを指定できるようになりました。別の RADIUS サーバも使用できますが、その RADIUS サーバは Security メニューを使用して定義する必要があります。

ID ネットワーキングで使用される RADIUS 属性

この項では、ID ネットワーキングで使用される RADIUS 属性について説明します。

QoS-Level

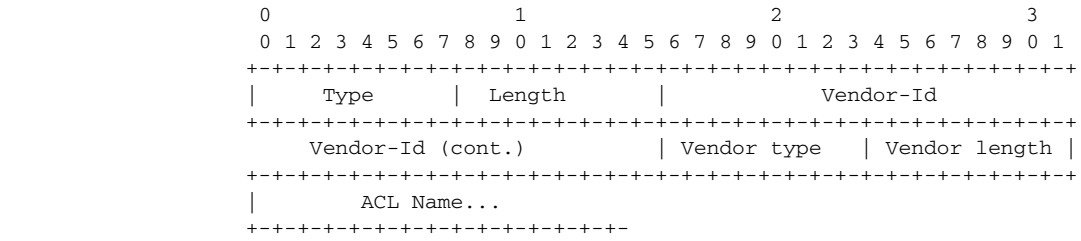
この属性は、スイッチング ファブリック内および空間経由のモバイル クライアントのトラフィックに適用される Quality of Service レベルを示します。この例は、QoS-Level 属性フォーマットの要約を示しています。フィールドは左から右に伝送されます。



- Type - 26（ベンダー固有）
- Length - 10
- Vendor-Id - 14179
- Vendor type - 2
- Vendor length - 4
- Value - 3 オクテット：
  - 0 - Bronze（バックグラウンド）
  - 1 - Silver（ベストエフォート）
  - 2 - Gold（ビデオ）
  - 3 - Platinum（音声）

ACL-Name

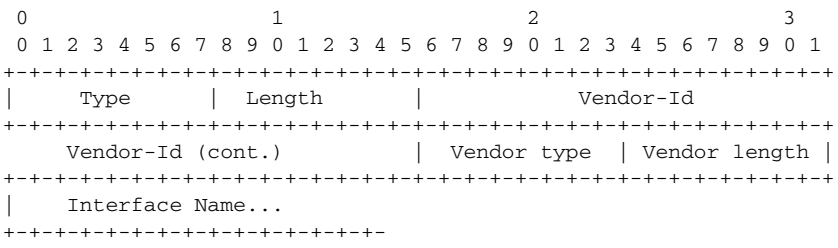
この属性は、クライアントに適用される ACL 名を示します。ACL-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。



- Type - 26（ベンダー固有）
- Length - >7
- Vendor-Id - 14179
- Vendor type - 6
- Vendor length - >0
- Value - クライアントに対して使用する ACL の名前を含む文字列

Interface-Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。Interface-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。



- Type - 26（ベンダー固有）
- Length - >7
- Vendor-Id - 14179
- Vendor type - 5
- Vendor length - >0
- Value - クライアントが割り当てられるインターフェイスの名前を含む文字列

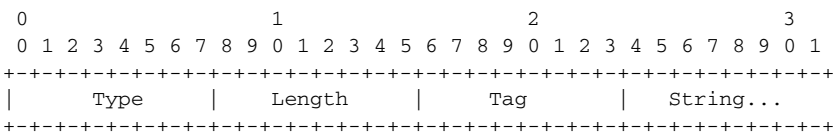
（注） この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

VLAN-Tag

この属性は、特定のトンネル セッションのグループ ID を示し、Tunnel-Private-Group-ID 属性とも呼ばれます。

この属性は、トンネルの発信側が、特定の接続からグループを事前に判別できる場合は Access-Request パケットに含めることができ、このトンネル セッションを特定のプライベート グループに属するものとして処理する場合は Access-Accept パケットに含める必要があります。プライベート グループは、トンネル セッションを特定のユーザのグループと関連付けるために使用できます。たとえば、未登録の IP アドレスが特定のインターフェイスを通過するようにするルーティングを容易にするために使用できます。Start と Stop のいずれかの値を持つ Acct-Status-Type 属性を含み、かつトンネル セッションに関連する Accounting-Request パケットには、プライベート グループを含める必要があります。

Tunnel-Private-Group-ID 属性形式の要約を次に示します。フィールドは左から右に伝送されます。



- Type - 81（Tunnel-Private-Group-ID 用）
- Length - >= 3
- Tag - Tag フィールドは、長さが 1 オクテットで、同じパケット内の、同じトンネルを示す属性をグループ化するために使用されます。Tag フィールドの値が 0x00 より大きく、0x1F 以下である場合、（いくつかの選択肢のうちの）この属性が属するトンネルを示すと解釈されます。Tag フィールドが 0x1F より大きい場合、後続の String フィールドの最初のバイトとして解釈されます。
- String - このフィールドは必須です。グループはこの String フィールドによって表されます。グループ ID の形式に制約はありません。

トンネル属性

(注)　この項の他の RADIUS 属性（QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag）のいずれかを返す場合、トンネル属性も返す必要があります。

RFC2868 では、認証と認可に使用される RADIUS トンネル属性が定義されています。RFC2867 では、アカウンティングに使用されるトンネル属性が定義されています。IEEE 802.1X Authenticator がトンネリングをサポートしている場合は、認証の結果としてサプリカントに対して強制的なトンネルをセットアップできます。

これは、特に、認証の結果に基づいて IEEE8021Q で定義されている特定のバーチャル LAN（VLAN）にポートを配置できるようにする場合に適しています。たとえば、これを使用すると、無線ホストが大学のネットワーク内で移動するときに同じ VLAN 上にとどまれるようになります。

RADIUS サーバは、一般的に、Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。ただし、IEEE 802.1X Authenticator も、Access- Request 内にトンネル属性を含めることによってサプリカントに割り当てる VLAN に関するヒントを提供できます。

VLAN 割り当てのために、次のトンネル属性が使用されます。

- Tunnel-Type=VLAN（13）
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

VLANID は 12 ビットであり、1 ～ 4094（両端の値を含む）の値をとることに注意してください。Tunnel-Private-Group-ID は、RFC2868 で定義されているように String 型なので、IEEE 802.1X で使用するために VLANID 整数値は文字列としてエンコードされます。

トンネル属性が送信されるときは、Tag フィールドに値が含まれている必要があります。RFC2868 の第 3.1 項には次のように明記されています。

- この Tag フィールドは長さが 1 オクテットであり、同じパケット内で同じトンネルを示す属性をグループ化する方法を提供することを目的としています。このフィールドの有効な値は、0x01 ～ 0x1F（両端の値を含む）です。この Tag フィールドが使用されない場合は、ゼロ（0x00）である必要があります。
- Tunnel-Client-Endpoint、Tunnel-Server-Endpoint、Tunnel-Private-Group-ID、Tunnel-Assignment-ID、Tunnel-Client-Auth-ID、または Tunnel-Server-Auth-ID 属性（ただし Tunnel-Type、Tunnel-Medium-Type、Tunnel-Password、Tunnel-Preference は含まない）で使用する場合、0x1F より大きい Tag フィールドは、次のフィールドの最初のオクテットと解釈されます。
- 代替トンネル タイプが提供されない場合（たとえば、トンネリングはサポートしているが VLAN はサポートしていない IEEE 802.1X Authenticator の場合）、トンネル属性に必要なのは 1 つのトンネルを指定することのみです。したがって、VLANID を指定することのみが目的の場合、すべてのトンネル属性の Tag フィールドをゼロ（0x00）に設定する必要があります。代替トンネル タイプが提供される場合は、0x01 ～ 0x1F のタグ値を選択する必要があります。

AAA Override の設定

WLAN の Allow AAA Override オプションを使用すると、WLAN で ID ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、QoS、および ACL を適用できます。

AAA Override を許可する設定の多くは、RADIUS サーバで実行されます。RADIUS サーバでは、コントローラに返すようにする上書きプロパティで、Access Control Server（ACS）を設定する必要があります。

コントローラでは、GUI または CLI を使用して、Allow AAA Override 設定パラメータを有効にするだけです。このパラメータを有効にすることにより、コントローラで RADIUS サーバから返される属性を受け入れるようになります。次にコントローラはそれらの属性をクライアントに適用します。

正しい QoS 値を取得するための RADIUS サーバ ディクショナリ ファイルの更新

Steel-Belted RADIUS（SBR）、FreeRadius、または同等の RADIUS サーバを使用している場合、AAA オーバーライド機能を有効化した後、クライアントが正しい QoS 値を取得できないことがあります。ディクショナリ ファイルの編集を可能にするこれらのサーバについて、正しい QoS 値（Silver = 0、Gold = 1、Platinum = 2、Bronze = 3）を反映させてファイルを更新する必要があります。そのための手順は、次のとおりです。

（注） この問題は、Cisco Secure Access Control Server（ACS）には適用されません。

ステップ 1　SBR サービス（または他の RADIUS サービス）を停止します。

ステップ 2　次のテキストを、ciscowlan.dct として Radius_Install_Directory\Service フォルダに保存します。

```
################################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
################################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level         Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze  3
VALUE Aire-QoS-Level Silver   0
VALUE Aire-QoS-Level Gold     1
VALUE Aire-QoS-Level Platinum 2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

################################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
################################################################################
```

ステップ 3　dictiona.dcm ファイルを（同じディレクトリに）開いて、行「@ciscowlan.dct.」を追加します。

ステップ 4　dictiona.dcm ファイルを保存して閉じます。

ステップ 5　vendor.ini ファイルを（同じでディレクトリに）開いて、次のテキストを追加します。

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id             =
```

ステップ 6　vendor.ini ファイルを保存して閉じます。

ステップ 7　SBR サービス（または他の RADIUS サービス）を起動します。

ステップ 8　SBR アドミニストレータ（または他の RADIUS アドミニストレータ）を起動します。

ステップ 9　RADIUS クライアントを追加します（まだ追加されていない場合）。Make/Model ドロップダウン ボックスから **Cisco WLAN Controller** を選択します。

GUI を使用した AAA Override の設定

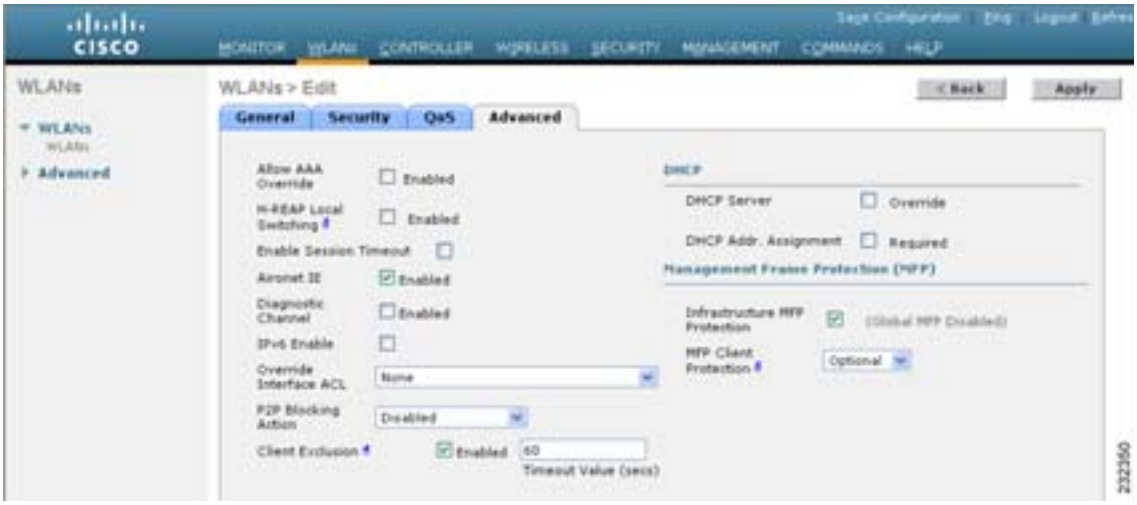
コントローラ GUI を使用して AAA Override を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　設定する WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。

ステップ 3　**Advanced** タブをクリックして、WLANs > Edit (Advanced) ページを開きます（図 5-40 を参照）。

図 5-40　WLANs > Edit (Advanced) ページ



ステップ 4　AAA Override の検証を有効にする場合は **Allow AAA Override** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値は無効です。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

CLI を使用した AAA Override の設定

コントローラ CLI を使用して AAA Override を有効または無効にするには、次のコマンドを使用します。

config wlan aaa-override {**enable** | **disable**} *wlan_id*

wlan_id には、1 ～ 16 の ID を入力します。

不正なデバイスの管理

この項では、不正なデバイスに対するセキュリティ ソリューションについて説明します。不正なデバイスとは、ネットワーク内で管理対象のアクセス ポイントによって検出される、システムに属していない不明なアクセス ポイントまたはクライアントのことです。

問題

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連の Clear To Send （CTS; クリア ツー センド）フレームを送信できるようになります。アクセス ポイントになりすましてこの CTS フレームが送信され、特定のクライアントには伝送を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。したがって、無線 LAN サービス プロバイダーは、境域からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、許可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正なアクセス ポイントは、企業のファイアウォールの背後にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯につながる恐れがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセス ポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

不正なデバイスの検出

コントローラでは、すべての近隣のアクセス ポイントが継続的に監視されます。また、不正なアクセス ポイントおよびクライアントが自動的に検出されて、それらの情報が収集されます。コントローラで不正なアクセス ポイントが検出されると、Rogue Location Discovery Protocol （RLDP; 不正ロケーション検出プロトコル）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

コントローラは、すべてのアクセス ポイント上で、または monitor（リッスン専用）モードに設定されたアクセス ポイント上でのみ RLDP を使用できるように設定できます。この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じたり、一定のデータ アクセス ポイント機能に影響を与えたりすることなく、監視を行えるようになります。すべてのアクセス ポイントで RLDP を使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラでは常に RLDP 動作に対してモニタ アクセス ポイントが選択されます。

（注） RLDP は、Cisco Autonomous 不正アクセス ポイントでの使用がサポートされていません。これらのアクセス ポイントでは、RLDP クライアントによって送信された DHCP Discover 要求が破棄されます。また、不正なアクセス ポイント チャンネルから Dynamic Frequency Selection（DFS; 動的周波数選択）が要求された場合、RLDP はサポートされません。

不正なアクセス ポイントの分類

コントローラ ソフトウェア リリース 5.0 では、不正なアクセス ポイントの分類および報告機能が強化されており、不正なアクセス ポイントがユーザ定義のルールに従って特定の不正の状態に分類され、ある状態から別の状態に自動的に移行できるようになっています。以前のリリースでは、MAC アドレスまたは BSSID によってソートされた不正なアクセス ポイントが 1 ページにまとめてコントローラに表示されていました。このリリースでは、不正なアクセス ポイントを Friendly、Malicious、または Unclassified に分類してコントローラに表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての不明なアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、未分類のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態のみのすべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にそのルールが適用されます。

（注） ルール　ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

1. コントローラは、不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれていることを確認できると、そのアクセス ポイントを Friendly に分類します。
2. 不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正の状態の分類ルールを適用します。
3. 不正なアクセス ポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセス ポイントを自動的に分類しません。不正なアクセス ポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセス ポイントを自動的に分類し直します。
4. コントローラは、優先度の一番高いルールを適用します。不正なアクセス ポイントがルールで指定された条件に一致すると、コントローラはそのアクセス ポイントをルールに設定された分類タイプに基づいて分類します。
5. 不正なアクセス ポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセス ポイントを Unclassified に分類します。
6. コントローラは、すべての不正なアクセス ポイントに対して上記の手順を繰り返します。
7. 不正なアクセス ポイントがネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的に Malicious に分類します。その後、不正なアクセス ポイントを手動で阻止することができますが、その場合は不正の状態が Contained に変更されます。不正なアクセス ポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのセス ポイントを手動で阻止できるようになります。
8. アクセス ポイントは、必要に応じて、異なる分類タイプや不正の状態に手動で移動できます。

表 5-6 には、特定の分類タイプの不正なアクセス ポイントに適用される不正の状態を示してあります。

表 5-6　分類マッピング

ルール ベースの分類タイプ	不正の状態
Friendly	• Internal：不明なアクセス ポイントがネットワーク内に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、Internal に設定します。たとえば、ラボ ネットワーク内のアクセス ポイントなどです。 • External：不明なアクセス ポイントがネットワーク外に存在し、WLAN のセキュリティに脅威を与えない場合、手動で Friendly、External に設定します。たとえば、近所のコーヒー ショップ設置されているアクセス ポイントなどです。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。
Malicious	• Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Threat：不明なアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：不明なアクセス ポイントが阻止されています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。
Unclassified	• Pending：最初の検出で、不明なアクセス ポイントは 3 分間 Pending 状態に置かれます。この間に、管理対象のアクセス ポイントでは、不明なアクセス ポイントがネイバー アクセス ポイントであるかどうかが判定されます。 • Alert：不明なアクセス ポイントがネイバー リストまたはユーザが設定した危険性のない MAC のリストに記載されていない場合、そのアクセス ポイントは Alert に移動されます。 • Contained：不明なアクセス ポイントが阻止されています。 • Contained Pending：不明なアクセス ポイントが Contained とマークされましたが、リソースを使用できないため対処が遅れています。

コントローラ ソフトウェア リリース 5.0 にアップグレードした場合は、不正なアクセス ポイントの分類と状態は次のように再設定されます。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

前述のように、コントローラでは、ユーザ定義のルールに基づいて不明なアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。または、不明なアクセス ポイントを異なる分類タイプと不正の状態に手動で移動できます。表 5-7 には、不明なアクセス ポイントの分類タイプや不正の状態がどのように遷移するよう設定可能であるかを示してあります。

表 5-7　設定可能な分類タイプ / 不正の状態の遷移

遷移前	遷移後
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

不正の状態が Contained の場合、不正なアクセス ポイントの分類タイプを変更する前に、そのアクセス ポイントが阻止されないようにする必要があります。不正なアクセス ポイントを Malicious から Unclassified に移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

WCS 相互作用

WCS ソフトウェア リリース 5.0 でも、ルール ベースの分類がサポートされています。WCS では、コントローラ上で設定された分類ルールが使用されます。次のイベント後に、コントローラから WCS にトラップが送信されます。

- 最初に不明なアクセス ポイントが Friendly に移動した場合に、不正の状態が Alert であると、コントローラから WCS にトラップが送信されます。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが移動した場合、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正なアクセス ポイントに関して、コントローラから WCS にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

RLDP の設定

RLDP を設定するには、コントローラの GUI または CLI を使用します。

GUI を使用した RLDP の設定

コントローラの GUI を使用して RLDP を設定する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **Rogue Policies** > **General** の順にクリックして、Rogue Policies ページを開きます（図 5-41 を参照）。

図 5-41　Rogue Policie ページ

ステップ 2　Rogue Location Discovery Protocol ドロップダウン ボックスから、次のオプションのいずれかを選択します。

- **Disable**：すべてのアクセス ポイント上で RLDP を無効にします。これはデフォルト値です。
- **All APs**：すべてのアクセス ポイント上で RLDP を有効にします。
- **Monitor Mode APs**：監視モードのアクセス ポイント上でのみ RLDP を有効にします。

ステップ 3　Expiration Timeout for Rogue AP and Rogue Client Entries フィールドに、不正なアクセス ポイントとクライアント エントリの期限が切れてリストから削除されるまでの秒数を入力します。有効な範囲は 240 ～ 3600 秒で、デフォルト値は 1200 秒です。

（注）　不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

ステップ 4　必要に応じて、**Validate Rogue Clients Against AAA** チェックボックスをオンにし、AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントかどうかを検証します。デフォルトではオフになっています。

ステップ 5　必要に応じて、**Detect and Report Ad-Hoc Networks** チェックボックスをオンにして、アドホック不正検出および報告を有効にします。デフォルト値はオンです。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した RLDP の設定

コントローラの CLI を使用して RLDP を設定する手順は、次のとおりです。

ステップ 1　RLDP を有効、無効、または開始するには、次のコマンドを入力します。

- **config rogue ap rldp enable alarm-only**：すべてのアクセス ポイント上で RLDP を有効にします。

- **config rogue ap rldp enable alarm-only** *monitor_ap_only*：監視モードのアクセス ポイント上でのみ RLDP を有効にします。
- **config rogue ap rldp initiate** *rogue_mac_address*：特定の不正なアクセス ポイント上で RLDP を開始します。
- **config rogue ap rldp disable**：すべてのアクセス ポイント上で RLDP を無効にします。

ステップ 2　不正なアクセス ポイントとクライアント エントリの期限が切れてリストから削除されるまでの秒数を指定するには、次のコマンドを入力します。

config rogue ap timeout *seconds*

*秒数*の有効な値の範囲は 240 ～ 3600 秒（両端の値を含む）で、デフォルト値は 1200 秒です。

（注）　不正なアクセス ポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

ステップ 3　アドホック不正検出および報告を有効または無効にするには、次のコマンドを入力します。

config rogue adhoc {**enable** | **disable**}

ステップ 4　AAA サーバまたはローカル データベースを有効または無効して、不正なクライアントが有効なクライアントかどうかを検証するには、次のコマンドを入力します。

config rogue client aaa {**enable** | **disable**}

ステップ 5　変更を保存するには、次のコマンドを入力します。

save config

不正分類ルールの設定

コントローラの GUI または CLI を使用して、1 つのコントローラにつき最大 64 の不正分類ルールを設定できます。

GUI を使用した不正分類ルールの設定

コントローラの GUI を使用して不正分類ルールを設定する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **Rogue Policies** > **Rogue Rules** の順にクリックして、Rogue Rules ページを開きます（図 5-42 を参照）。

図 5-42　Rogue Rules ページ

すでに作成されているすべてのルールが優先順位に従って一覧表示されます。各ルールの名前、タイプ、およびステータスが表示されます。

（注）　ルールを削除するには、そのルールの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** をクリックします。

ステップ 2　新しいルールを作成する手順は、次のとおりです。

a. **Add Rule** をクリックします。Add Rule のセクションがページ上部に表示されます。

b. Rule Name フィールドに、新しいルールの名前を入力します。名前にはスペースを含めないでください。

c. Rule Type ドロップダウン ボックスで、**Friendly** または **Malicious** を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。

d. **Add** をクリックして既存のルール リストにこのルールを追加するか、**Cancel** をクリックしてこの新しいルールを破棄します。

ステップ 3　ルールを編集する手順は、次のとおりです。

a. 編集するルールの名前をクリックします。Rogue Rule > Edit ページが表示されます（図 5-43 を参照）。

図 5-43　Rogue Rule > Edit ページ

b. Type ドロップダウン ボックスで、**Friendly** または **Malicious** を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。

c. Match Operation フィールドで、次のいずれかを選択します。

- **Match All**：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定されたすべての条件を満たしている必要があります。それによって、そのルールに従ってルールの分類タイプが不正なアクセス ポイントに適用されます。
- **Match Any**：このルールが有効な場合、検出された不正なアクセス ポイントは、ルールで指定された条件のいずれかを満たす必要があります。これにより、ルールが満たされ、ルールの分類タイプが不正なアクセス ポイントに適用されます。これはデフォルト値です。

d. このルールを有効にするには、**Enable Rule** チェックボックスをオンにします。デフォルトではオフになっています。

e. Add Condition ドロップダウン ボックスで、不正なアクセス ポイントが満たす必要がある次の条件から 1 つまたは複数を選択し、**Add Condition** をクリックします。

- **SSID**：不正なアクセス ポイントには、特定のユーザ設定 SSID が必要です。このオプションを選択する場合は、User Configured SSID フィールドに SSID を入力して、**Add SSID** をクリックします。

（注） SSID を削除するには、SSID を強調表示して **Remove** をクリックします。

- **RSSI**：不正なアクセス ポイントには、Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）の最小値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、Minimum RSSI フィールドに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50dBm（両端の値を含む）で、デフォルト値は 0dBm です。
- **Duration**：不正なアクセス　ポイントが最小期間で検出される必要があります。このオプションを選択する場合は、Time Duration フィールドに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。
- **Client Count**：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、Minimum Number of Rogue Clients フィールドに不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
- **No Encryption**：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。このオプションに関して、これ以外の設定を行う必要はありません。

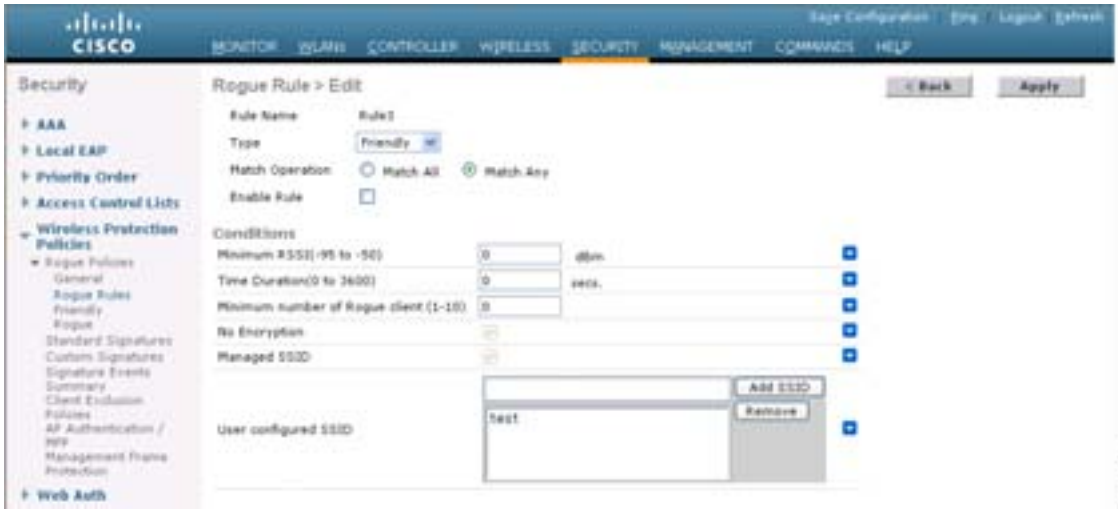
（注） WCS では、「オープン認証」としてこのオプションが参照されます。

- **Managed SSID**：不正なアクセス ポイントの管理対象 SSID （WLAN に対して設定された SSID）がコントローラで認識されている必要があります。このオプションに関して、これ以外の設定を行う必要はありません。

（注） SSID および管理対象 SSID の 2 つのリストは相互に排他的であるため、SSID および管理対象 SSID の条件を Match All 操作で使用することはできません。Match All を使用してルールを定義し、これら 2 つの条件を設定した場合は、いずれかの条件が満たされないので、不正なアクセス ポイントが Friendly または Malicious に分類されることはありません。

1 つのルールにつき最大 6 つの条件を追加できます。条件を追加すると、Conditions のセクションに表示されます（図 5-44 を参照）。

図 5-44　Rogue Rule > Edit ページ



（注） 条件を削除するには、その条件の青いドロップダウンの矢印の上にカーソルを置いて、**Remove** をクリックします。

f. **Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 5　不正分類ルールを適用する順序を変更する場合の手順は、次のとおりです。

a. **Back** をクリックして、Rogue Rules ページに戻ります。

b. **Change Priority** をクリックして、Rogue Rules > Priority ページにアクセスします（図 5-45 を参照）。

図 5-45　Rogue Rules > Priorit ページ

不正ルールが優先順位に従って Change Rules Priority 編集ボックスに表示されます。

c. 優先順位を変更するルールを強調表示し、**Up** をクリックしてリスト内の順位を上げるか、**Down** をクリックしてリスト内の順位を下げます。

d. 目的の順位になるまで、ルールを上または下に移動し続けます。

e. **Apply** をクリックして、変更を適用します。

ステップ 6　不正なアクセス ポイントを Friendly に分類して危険性のない MAC アドレスのリストに追加する場合の手順は、次のとおりです。

a. **Security** > **Wireless Protection Policies** > **Rogue Policies** > **Friendly Rogue** の順にクリックして、Friendly Rogue > Create ページにアクセスします（図 5-46 を参照）。

図 5-46　Friendly Rogue > Create ページ

b. MAC Address フィールドに、危険性のない不正なアクセス ポイントの MAC アドレスを入力します。

c. **Apply** をクリックして、変更を適用します。

d. **Save Configuration** をクリックして、変更内容を保存します。このアクセス ポイントは、コントローラの、危険性のないアクセス ポイントのリストに追加され、Friendly Rogue APs ページに表示されます。

CLI を使用した不正分類ルールの設定

コントローラの CLI を使用して不正分類ルールを設定する手順は、次のとおりです。

ステップ 1　ルールを作成するには、次のコマンドを入力します。

config rogue rule add ap priority *priority* **classify** {**friendly** | **malicious**} *rule_name*

（注）　後からこのルールの優先順位を変更し、それに伴ってリスト内の他のルールの順番を変更する場合は、次のコマンドを入力します。**config rogue rule priority** *priority rule_name*
後からこのルールの分類を変更する場合は、次のコマンドを入力します。**config rogue rule classify** {**friendly** | **malicious**} *rule_name*

（注）　すべての不正分類ルール、または特定のルールを削除するには、次のコマンドを入力します。**config rogue rule delete** {**all** | *rule_name*}

ステップ 2　すべてのルールまたは特定のルールを無効にするには、次のコマンドを入力します。

config rogue rule disable {**all** | *rule_name*}

（注）　ルールの属性を変更する前にルールを無効にする必要があります。

ステップ 3　不正なアクセス ポイントが満たす必要があるルールに条件を追加するには、次のコマンドを入力します。

config rogue rule condition ap set *condition_type condition_value rule_name*

condition_type は、次のいずれかです。

- **ssid**：不正なアクセス ポイントには、特定の SSID が必要です。コントローラによって管理されない SSID を追加する必要があります。このオプションを選択する場合は、*condition_value* パラメータに SSID を入力します。SSID はユーザ設定の SSID リストに追加されます。

  （注）　ユーザ設定の SSID リストからすべての SSID または特定の SSID を削除するには、次のコマンドを入力します。**config rogue rule condition ap delete ssid** {**all** | *ssid*} *rule_name*

- **rssi**：不正なアクセス ポイントには、最小の RSSI 値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition_value* パラメータに最小 RSSI 値を入力します。有効な値の範囲は -95 ～ -50dBm（両端の値を含む）で、デフォルト値は 0dBm です。
- **duration**：不正なアクセス ポイントが最小期間で検出される必要があります。このオプションを選択する場合は、*condition_value* パラメータに最小検出期間の値を入力します。有効な値の範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。

- **client-count**：不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition_value* パラメータに不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。
- **no-encryption**：不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。このオプションには *condition_value* パラメータは必要ありません。
- **managed-ssid**：不正なアクセス ポイントの SSID がコントローラで認識されている必要があります。このオプションには *condition_value* パラメータは必要ありません。

（注） 1 つのルールにつき最大 6 つの条件を追加できます。ルールからすべての条件または特定の条件を削除するには、次のコマンドを入力します。**config rogue rule condition ap delete** {**all** | *condition_type*} *condition_value rule_name*.

ステップ 4　検出された不正なアクセス ポイントで、そのルールで指定された条件のすべてまたはいずれかが満たされ、ルールに従ってそのアクセス ポイントにルールの分類タイプが適用されるようにする必要があるかどうかを指定するには、次のコマンドを入力します。

config rogue rule match {**all** | **any**} *rule_name*

ステップ 5　すべてのルールまたは特定のルールを有効にするには、次のコマンドを入力します。

config rogue rule enable {**all** | *rule_name*}

（注） 変更を有効にするには、ルールを有効にする必要があります。

ステップ 6　新しい危険性のないアクセス ポイント エントリを危険性のない MAC アドレスのリストに追加したり、リストから既存の危険性のないアクセス ポイント エントリを削除したりするには、次のコマンドを入力します。

config rogue ap friendly {**add** | **delete**} *ap_mac_address*

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　コントローラ上に設定されている不正分類ルールを表示するには、次のコマンドを入力します。

show rogue rule summary

次のような情報が表示されます。

```
Priority Rule Name  State      Type        Match  Hit Count
-------- ---------- -------- ------------ ------ ---------
1        Rule1      Disabled   Friendly      Any   0
2        Rule2      Enabled    Malicious     Any  339
3       Rule3      Disabled   Friendly     Any   0
```

ステップ 9　特定の不正分類ルールの詳細情報を表示するには、次のコマンドを入力します。

show rogue rule detailed *rule_name*

次のような情報が表示されます。

```
Priority.................................... 2
Rule Name................................... Rule2
State....................................... Enabled
Type.........................................Malicious
Match Operation............................. Any
Hit Count................................... 352
Total Conditions............................ 6
Condition 1
    type.................................... Client-count
    value................................... 10
Condition 2
    type.................................... Duration
    value (seconds)......................... 2000
Condition 3
    type.................................... Managed-ssid
    value................................... Enabled
Condition 4
    type.................................... No-encryption
    value................................... Enabled
Condition 5
    type.................................... Rssi
    value (dBm)............................. -50
Condition 6
    type.................................... Ssid
    SSID Count.............................. 1
    SSID 1.................................. test
```

不正なデバイスの表示および分類

コントローラの GUI または CLI を使用して、不正なデバイスを表示し、コントローラによって実行されるべき処理を決定することができます。

GUI を使用した不正なデバイスの表示および分類

コントローラの GUI を使用して、不正なデバイスを表示および分類する手順は、次のとおりです。

ステップ 1　**Monitor** > **Rogues** の順にクリックします。

ステップ 2　次のオプションをクリックすると、コントローラで検出された各タイプの不正なアクセス ポイントを表示できます。

- **Friendly APs**
- **Malicious APs**
- **Unclassified APs**

次のようなページが表示されます（図 5-47 を参照）。

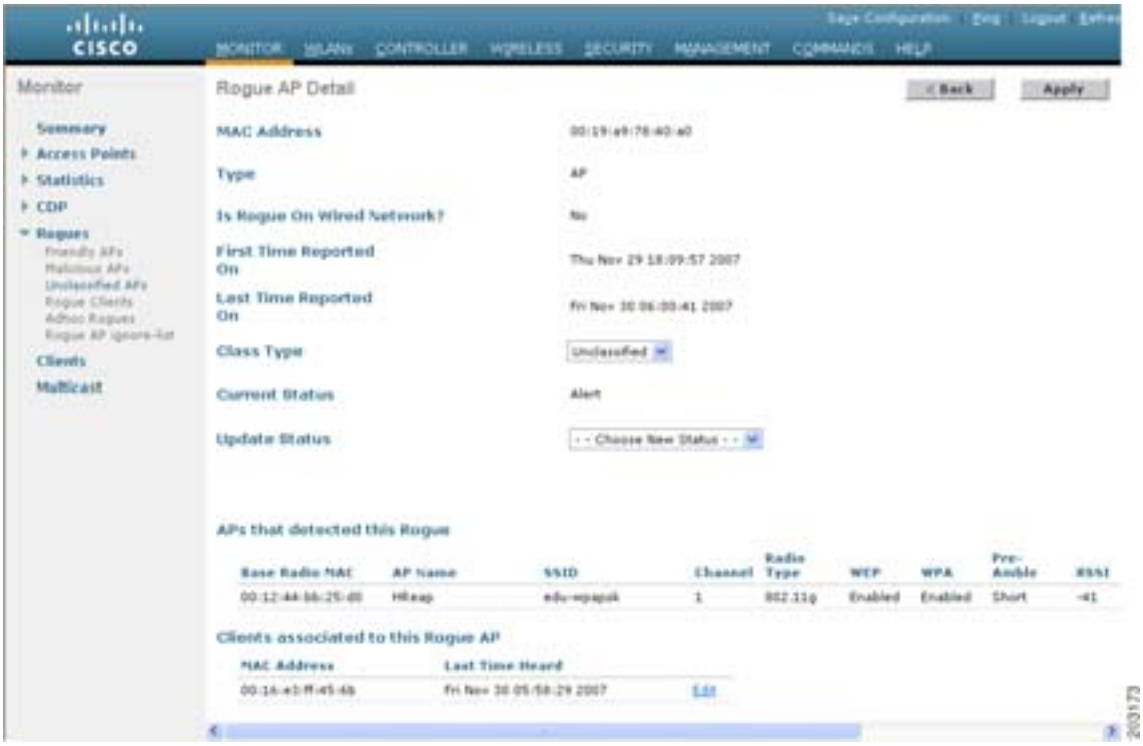
図 5-47　Friendly Rogue APs ページ

Friendly Rogue APs ページ、Malicious Rogue APs ページ、および Unclassified Rogue APs ページには、次の情報が表示されます。不正なアクセス ポイントの MAC アドレスと SSID、不正なアクセス ポイントに接続されたクライアント数、不正なアクセス ポイントが検出された無線の数、および不正なアクセス ポイントの現在のステータス。

（注）　これらのいずれかのページから不正なアクセス ポイントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、**Remove** をクリックします。

ステップ 3　不正なアクセス ポイントの詳細を取得するには、アクセス ポイントの MAC アドレスをクリックします。Rogue AP Detail ページが表示されます（図 5-48 を参照）。

図 5-48　Rogue AP Detail ページ



このページには、次の情報が表示されます。不正なデバイスの MAC アドレス、不正なデバイス（アクセス ポイントなど）のタイプ、不正なデバイスが有線ネットワーク上にあるかどうか、不正なデバイスが最初および最後に報告された日時、およびデバイスの現在のステータス。

ステップ 4　Class Type フィールドには、この不正なアクセス ポイントの現在の分類が表示されます。

- **Friendly**：ユーザ定義の Friendly ルールと一致した不明なアクセス ポイント、または既知の不正なアクセス ポイント。危険性のないアクセス ポイントは阻止することができません。
- **Malicious**：ユーザ定義の Malicious ルールと一致した不明なアクセス ポイント、またはユーザが Friendly または Unclassified 分類タイプから手動で移動した不明なアクセス ポイント。

（注） アクセス ポイントが Malicious に分類されると、その後でそのアクセス ポイントにルールを適用することはできなくなります。また、別の分類タイプに移動することもできません。危険性のあるアクセス ポイントを Unclassified 分類タイプに移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。

- **Unclassified**：ユーザ定義の Friendly または Malicious ルールと一致しない不明なアクセス ポイント。未分類のアクセス ポイントは阻止することができます。また、このアクセス ポイントは、ユーザ定義のルールに従って自動的に、またはユーザが手動で、Friendly または Malicious 分類タイプに移動できます。

このデバイスの分類を変更するには、Class Type ドロップダウン ボックスから別の分類を選択します。

（注） 不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントは移動できません。

ステップ 5　Update Status ドロップダウン ボックスから、次のオプションの 1 つを選択して、この不正なアクセス ポイントに対するコントローラの応答方法を指定します。

- **Internal**：コントローラはこの不正なアクセス ポイントを信頼します。このオプションは、Class Type が Friendly に設定されている場合に使用できます。
- **External**：コントローラはこの不正なアクセス ポイントの存在を認識します。このオプションは、Class Type が Friendly に設定されている場合に使用できます。
- **Contain**：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。このオプションは、Class Type が Malicious または Unclassified に設定されている場合に使用できます。
- **Alert**：コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されます。このオプションは、Class Type が Malicious または Unclassified に設定されている場合に使用できます。

ページの下部には、この不正なアクセス ポイントが検出されたアクセス ポイントと、アクセス ポイントにアソシエートされた任意のクライアントの両方に関する情報が提供されます。クライアントの詳細を表示するには、**Edit** をクリックして Rogue Client Detail ページを開きます。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 8　コントローラに接続された不正なクライアントを表示するには、**Rogue Clients** をクリックします。Rogue Clients ページが表示されます。このページには、次の情報が表示されます。不正なクライアントの MAC アドレス、不正なクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID、不正なクライアントが検出された無線の数、不正なクライアントが最後に報告された日時、および不正なクライアントの現在のステータス。

ステップ 9　不正なクライアントの詳細情報を参照するには、そのクライアントの MAC アドレスをクリックします。Rogue Client Detail ページが表示されます（図 5-49 を参照）。

図 5-49　Rogue Client Detail ページ

このページには、次の情報が表示されます。不正なクライアントの MAC アドレス、このクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID および IP アドレス、不正なクライアントが最初および最後に報告された日時、および不正なクライアントの現在のステータス。

ステップ 10　Update Status ドロップダウン ボックスから、次のオプションの 1 つを選択して、この不正なクライアントに対するコントローラの応答方法を指定します。

- **Contain**：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- **Alert**：コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されます。

ページの下部には、この不正なクライアントが検出されたアクセス ポイントに関する情報が提供されます。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　必要に応じて、**Ping** をクリックすることによって、このクライアントへのコントローラの接続をテストできます。

ステップ 13　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 14　コントローラによって検出されたアドホック不正を表示するには、**Adhoc Rogues** をクリックします。Adhoc Rogue ページが表示されます（図 5-50 を参照）。

図 5-50　Adhoc Rogue ページ

このページには、次の情報が表示されます。MAC アドレス、BSSID、アドホック不正の SSID、アドホック不正が検出された無線の数、アドホック不正の現在のステータス。

ステップ 15　アドホック不正の詳細情報を参照するには、その不正の MAC アドレスをクリックします。Adhoc Rogue Detail ページが表示されます（図 5-51 を参照）。

図 5-51　Adhoc Rogue Detail ページ

このページには、次の情報が表示されます。アドホック不正の MAC アドレスおよび BSSID、不正が最初および最後に報告された日時、および不正の現在のステータス。

ステップ 16 Update Status ドロップダウン ボックスから、次のオプションの 1 つを選択して、このアドホック不正に対するコントローラの応答方法を指定します。

- **Contain**：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- **Alert**：コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されます。
- **Internal**：コントローラはこの不正なアクセス ポイントを信頼します。
- **External**：コントローラはこの不正なアクセス ポイントの存在を認識します。

ステップ 17 Maximum Number of APs to Contain the Rogue ドロップダウン ボックスから、**1**、**2**、**3**、または **4** のオプションの 1 つを選択して、このアドホック不正を阻止するために使用するアクセス ポイントの最大数を指定します。

ページの下部には、このアドホック不正が検出されたアクセス ポイントに関する情報が提供されます。

ステップ 18 **Apply** をクリックして、変更を適用します。

ステップ 19 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 20 無視するように設定された任意のアクセス ポイントを表示するには、**Rogue AP Ignore-List** をクリックします。Rogue AP Ignore-List ページが表示されます（図 5-52 を参照）。

図 5-52　Rogue AP Ignore-List ページ

このページには、無視するように設定されている任意のアクセス ポイントの MAC アドレスが表示されます。不正無視リストには、WCS ユーザが WCS マップに手動で追加した任意の Autonomous アクセス ポイントのリストが含まれています。コントローラでは、これらの Autonomous アクセス ポイントが、WCS によって管理されていても不正と見なされます。不正無視リストを使用すると、コントローラでこれらのアクセス ポイントを無視できます。このリストは次のように更新されます。

- コントローラは、不正レポートを受信すると、不明なアクセス ポイントが不正無視アクセス ポイント リストに存在するかどうかを確認します。
- 不明なアクセス ポイントが不正無視リストに存在する場合、コントローラはこのアクセス ポイントを無視して他の不正なアクセス ポイントの処理を続けます。

- 不明なアクセス ポイントが不正無視リストにない場合、コントローラは WCS にトラップを送信します。WCS は、Autonomous アクセス ポイント リストでこのアクセス ポイントを発見すると、このアクセス ポイントを不正無視リストに追加するようコントローラにコマンドを送信します。このアクセス ポイントは、今後の不正レポートで無視されるようになります。
- ユーザが WCS から Autonomous アクセス ポイントを削除すると、WCS はこのアクセス ポイントを不正無視リストから削除するようにコントローラにコマンドを送信します。

CLI を使用した不正デバイスの表示および分類

コントローラの CLI を使用して、不正デバイスを表示および分類するには、次のコマンドを入力します。

1. コントローラによって検出されたすべての不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap summary

   次のような情報が表示されます。

```
Rogue Location Discovery Protocol..... Enabled
Rogue AP timeout..................................... 1200

MAC Address        Classification     # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0a:b8:7f:08:c0  Friendly           0     0         Not Heard
00:0b:85:01:30:3f  Malicious          1     0         Fri Nov 30 11:30:59 2007
00:0b:85:63:70:6f  Malicious          1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf Malicious         1   0   Fri Nov 30 11:23:12 2007
...
```

2. コントローラによって検出された危険性のない不正なアクセス　ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap friendly summary

   次のような情報が表示されます。

```
Number of APs..................................... 1

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- --------------------------
00:0a:b8:7f:08:c0  Internal           1   0        Tue Nov 27 13:52:04 2007
```

3. コントローラによって検出された危険性のある不正なアクセス　ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap malicious summary

   次のような情報が表示されます。

```
Number of APs..................................... 264

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- -----------------------
00:0b:85:01:30:3f  Alert              1     0         Fri Nov 30 11:20:01 2007
00:0b:85:63:70:6f  Alert              1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf  Alert              1     0         Fri Nov 30 11:23:12 2007
00:0b:85:63:cd:dd  Alert              1     0         Fri Nov 30 11:27:03 2007
00:0b:85:63:cd:de  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:cd:df Alert         1 0   Fri Nov 30 11:26:50 2007
...
```

4. コントローラによって検出された未分類の不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

   show rogue ap unclassified summary

   次のような情報が表示されます。

```
Number of APs.................................. 164

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- ----------------------
00:0b:85:63:cd:bd  Alert              1     0         Fri Nov 30 11:12:52 2007
00:0b:85:63:cd:e7  Alert              1     0         Fri Nov 30 11:29:01 2007
00:0b:85:63:ce:05  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:ce:07 Alert         1  0         Fri Nov 30 11:26:23 2007
...
```

5. 特定の不正なアクセス ポイントの詳細情報を表示するには、次のコマンドを入力します。

   show rogue ap detailed *ap_mac_address*

   次のような情報が表示されます。

```
Rogue BSSID.................................... 00:0b:85:63:d1:94
Is Rogue on Wired Network...................... No
Classification.................................Unclassified
State.......................................... Alert
First Time Rogue was Reported.................. Fri Nov 30 11:24:56 2007
Last Time Rogue was Reported................... Fri Nov 30 11:24:56 2007
Reported By
    AP 1
        MAC Address............................ 00:12:44:bb:25:d0
        Name................................... HReap
        Radio Type............................. 802.11g
        SSID................................... edu-eap
        Channel................................ 6
        RSSI................................... -61 dBm
        SNR.................................... -1 dB
        Encryption............................. Enabled
        ShortPreamble.......................... Enabled
        WPA Support............................ Disabled
        Last reported by this AP.............. Fri Nov 30 11:24:56 2007
```

6. 不正なアクセス　ポイントにアソシエートされているすべての不正なクライアントのリストを表示するには、次のコマンドを入力します。

   show rogue ap clients *ap_mac_address*

   次のような情報が表示されます。

```
MAC Address        State              # APs  Last Heard
-----------------  ------------------ ----- -------------------------
00:bb:cd:12:ab:ffAlert 1Fri Nov 30 11:26:23 2007
```

7. コントローラによって検出されたすべての不正なクライアントのリストを表示するには、次のコマンドを入力します。

   show rogue client summary

   次のような情報が表示されます。

```
Validate rogue clients against AAA.............. Disabled

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- ----------------------
00:0a:8a:7d:f5:f5  Alert              1     Mon Dec  3 21:56:36 2007
00:18:ba:78:c4:44  Alert              1     Mon Dec  3 21:59:36 2007
00:18:ba:78:c4:d1  Alert              1     Mon Dec  3 21:47:36 2007
00:18:ba:78:ca:f8 Alert         1  Mon Dec  3 22:02:36 2007
...
```

8. 特定の不正なクライアントの詳細情報を表示するには、次のコマンドを入力します。

   show rogue client detailed *client_mac_address*

   次のような情報が表示されます。

```
Rogue BSSID..................................... 00:0b:85:23:ea:d1
State........................................... Alert
First Time Rogue was Reported................... Mon Dec  3 21:50:36 2007
Last Time Rogue was Reported.................... Mon Dec  3 21:50:36 2007
Rogue Client IP address......................... Not known
Reported By
    AP 1
        MAC Address............................. 00:15:c7:82:b6:b0
        Name.................................... AP0016.47b2.31ea
        Radio Type.............................. 802.11a
        RSSI.................................... -71 dBm
        SNR..................................... 23 dB
        Channel................................. 149
        Last reported by this AP.............. Mon Dec  3 21:50:36 2007
```

9. コントローラによって検出されたすべてのアドホック不正のリストを表示するには、次のコマンドを入力します。

   show rogue adhoc summary

   次のような情報が表示されます。

```
Detect and report Ad-Hoc Networks.............. Enabled

Client MAC Address  Adhoc BSSID         State    # APs   Last Heard
------------------  ------------------  ----------- -------
------------------------
00:bb:cd:12:ab:ffsuperAlert 1 Fri Nov 30 11:26:23 2007
```

10. 特定のアドホック不正の詳細情報を表示するには、次のコマンドを入力します。

    show rogue adhoc detailed *rogue_mac_address*

    次のような情報が表示されます。

```
Adhoc Rogue MAC address......................... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID............................... 02:61:ce:8e:a8:8c
State........................................... Alert
First Time Adhoc Rogue was Reported............. Tue Dec 11 20:45:45 2007
Last Time Adhoc Rogue was Reported.............. Tue Dec 11 20:45:45 2007
Reported By
    AP 1
        MAC Address............................. 00:14:1b:58:4a:e0
        Name.................................... AP0014.1ced.2a60
        Radio Type.............................. 802.11b
        SSID.................................... rf4k3ap
        Channel................................. 3
        RSSI.................................... -56 dBm
        SNR..................................... 15 dB
        Encryption.............................. Disabled
        ShortPreamble........................... Disabled
        WPA Support............................. Disabled
Last reported by this AP.............. Tue Dec 11 20:45:45 2007
```

11. 無視するように設定されている不正なアクセス ポイントのリストを表示するには、次のコマンドを入力します。

    show rogue ignore_list

    次のような情報が表示されます。

```
MAC Address
------------------
10:bb:17:cc:01:ef
```

(注)　不正無視アクセス ポイント リストの詳細は、「GUI を使用した不正なデバイスの表示および分類」の項（P. 5-97）のステップ 20 を参照してください。

12. 不正なアクセス ポイントを Friendly に分類するには、次のコマンドを入力します。

config rogue ap classify friendly state {**internal** | **external**} *ap_mac_address*

このとき、次のようになります。

- **internal** は、コントローラがこの不正なアクセス ポイントを信頼することを表しています。
- **external** は、コントローラがこの不正なアクセス ポイントの存在を認識することを表しています。

(注)　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Friendly クラスに移動することはできません。

13. 不正なアクセス ポイントに Malicious のマークを付けるには、次のコマンドを入力します。

config rogue ap classify malicious state {**alert** | **contain**} *ap_mac_address*

このとき、次のようになります。

- **contain** は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。
- **alert** は、コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されることを表しています。

(注)　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Malicious クラスに移動することはできません。

14. 不正なアクセス ポイントに Unclassified のマークを付けるには、次のコマンドを入力します。

config rogue ap classify unclassified state {**alert** | **contain**} *ap_mac_address*

(注)　不正なアクセス ポイントの現在の状態が Contain である場合、そのアクセス ポイントを Unclassified クラスに移動することはできません。

15. 不正なクライアントに対するコントローラの応答方法を指定するには、次のコマンドを入力します。

- **config rogue client alert** *client_mac_address*：コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されます。
- **config rogue client contain** *client_mac_address*：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。

16. アドホック不正に対するコントローラの応答方法を指定するには、次のコマンドを入力します。
    - **config rogue adhoc alert** *rogue_mac_address*：コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されます。
    - **config rogue adhoc contain** *rogue_mac_address*：コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
    - **config rogue adhoc external** *rogue_mac_address*：コントローラによって、このアドホック不正の存在が認識されます。
17. 変更を保存するには、次のコマンドを入力します。

    save config

IDS の設定

Cisco Intrusion Detection System/Intrusion Prevention System（CIDS/IPS; 侵入検知システム / 侵入防御システム）は、特定のクライアントに関わる攻撃がレイヤ 3 ～ レイヤ 7 で検出されたとき、これらクライアントによる無線ネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア / アドウェア、ネットワーク ウィルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。IDS 攻撃を検出するには 2 つの方法があります。

- IDS センサー。次の項を参照してください。
- IDS シグニチャ。（P. 5-113）を参照してください。

IDS センサーの設定

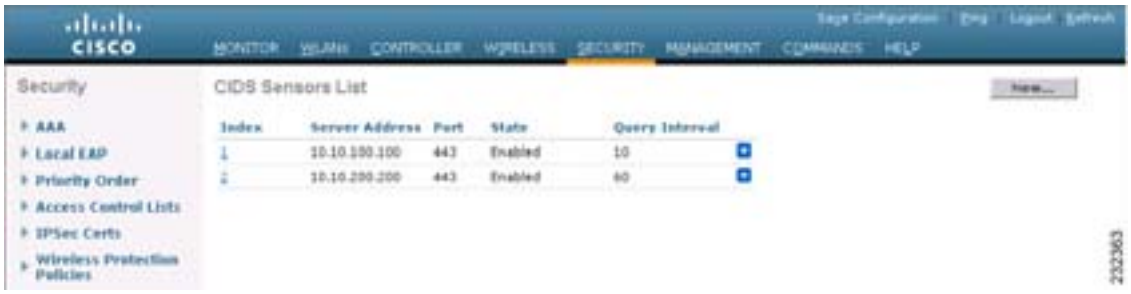
ネットワークのさまざまなタイプの IP レベル攻撃を検出するように、IDS センサーを設定することができます。センサーで攻撃が特定されたら、違反クライアントを回避するよう、コントローラに警告することができます。新しく IDS センサーを追加したときは、コントローラをその IDS センサーに登録し、回避クライアントのリストをセンサーから取得できるようにします。IDS センサー登録 は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した IDS センサーの設定

コントローラの GUI を使用して IDS センサーを設定する手順は、次のとおりです。

ステップ 1　**Security** > **Advanced** > **CIDs** > **Sensors** の順にクリックして、CIDS Sensors List ページを開きます（図 5-53 を参照）。

図 5-53　CIDS Sensors List ページ

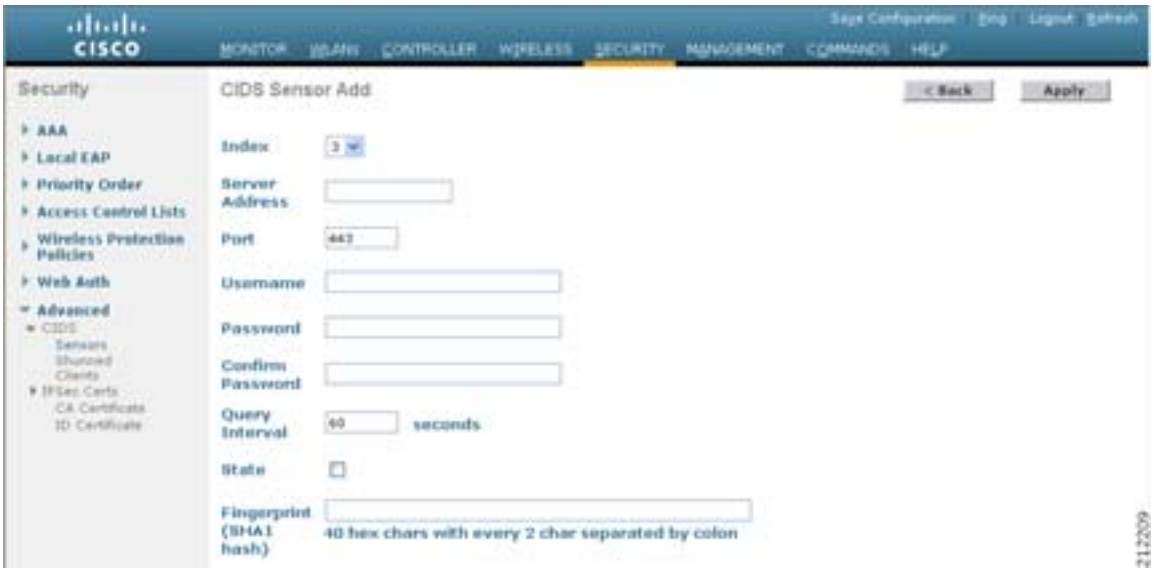


このページでは、このコントローラに設定されたすべての IDS センサーが表示されます。

（注）　既存のセンサーを削除するには、そのセンサーの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　IDS センサーをリストに追加するには、**New** をクリックします。CIDS Sensors Add ページが表示されます（図 5-54 を参照）。

図 5-54　CIDS Sensors Add ページ



ステップ 3　コントローラでは最大 5 つの IPS センサーをサポートします。Index ドロップダウン ボックスから数字（1 ～ 5）を選択し、コントローラで IPS センサーが検索される順序を決定します。たとえば、1 を選択した場合には、コントローラは最初にこの IPS センサーを検索します。

ステップ 4　Server Address フィールドに、IDS サーバの IP アドレスを入力します。

ステップ 5　Port フィールドには、コントローラと IDS センサーとの通信に使用される HTTPS ポートの数が設定されます。センサーはデフォルトで 443 を使用して通信するので、このパラメータを 443 に設定することをお勧めします。

デフォルト：443

範囲：1 ～ 65535

ステップ 6　Username フィールドで、コントローラが IDS センサーの認証に使用するユーザ名を入力します。

（注）　このユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 7　Password フィールドと Confirm Password フィールドに、コントローラが IDS センサーの認証に使用するパスワードを入力します。

ステップ 8　Query Interval フィールドに、コントローラが IDS サーバーで IDS イベントを検索する間隔（秒単位）を入力します。

デフォルト：60 秒

範囲：10 ～ 3600 秒

ステップ 9　**State** チェックボックスをオンにしてコントローラをこの IDS センサーに登録するか、このチェックボックスをオフにして登録を解除します。デフォルト値は無効です。

ステップ 10　Fingerprint フィールドに、40 桁の 16 進数文字のセキュリティ キーを入力します。このキーは、センサーの有効性の確認、およびセキュリティ攻撃の防止に使用されます。

（注）　キー内に 2 バイト間隔で現れるコロン（:）を含めないようにしてください。たとえば、AA:BB:CC:DD の代わりに、AABBCCDD と入力します。

ステップ 11　**Apply** をクリックします。CIDS Sensors List ページのセンサーのリストに新しい IDS センサーが表示されます。

ステップ 12　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した IDS センサーの設定

コントローラの CLI を使用して IDS センサーを設定する手順は、次のとおりです。

ステップ 1　IDS センサーを追加するには、次のコマンドを入力します。

config wps cids-sensor add *index ids_ip_address username password*

index パラメータは、コントローラで IPS センサーが検索される順序を決定します。コントローラでは最大 5 つの IPS センサーをサポートします。数字（1 ～ 5）を選択してこのセンサーの優先順位を決定します。たとえば、1 を入力した場合には、コントローラは最初にこの IPS センサーを検索します。

（注）　ユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

ステップ 2　（オプション）コントローラが IDS センサーとの通信に使用する HTTPS ポートの数を指定するには、このコマンドを入力します。

config wps cids-sensor port *index port_number*

port-number パラメータには、1 ～ 65535 の値を入力することができます。デフォルト値は 443 です。この手順はオプションであり、デフォルト値の 443 の使用をお勧めします。センサーはデフォルトでこの値を使用して通信します。

ステップ 3　コントローラが IDS イベントについて IDS センサーを検索する間隔を指定するには、次のコマンドを入力します。

config wps cids-sensor interval *index interval*

interval パラメータには、10 ～ 3600 秒の値を入力することができます。デフォルト値は 60 秒です。

ステップ 4　センサーの有効性の確認に使用する 40 桁の 16 進数文字のセキュリティ キーを入力するには、このコマンドを入力します。

config wps cids-sensor fingerprint *index* **sha1** *fingerprint*

センサーのコンソール上で、**show tls fingerprint** と入力することにより、フィンガープリントの値を取得できます。

（注）　キー内にコロン（:）が 2 バイト間隔で現れるようにしてください（たとえば、AA:BB:CC:DD）。

ステップ 5　IDS センサーへのこのコントローラの登録を有効または無効にするには、次のコマンドを入力します。

config wps cids-sensor {**enable** | **disable**} *index*

ステップ 6　設定を保存するには、次のコマンドを入力します。

save config

ステップ 7　IDS センサー設定を表示するには、次のコマンドの 1 つを入力します。

- **show wps cids-sensor summary**
- **show wps cids-sensor detail** *index*

2 つ目のコマンドは、1 つ目のコマンドよりも詳細な情報を提供します。

ステップ 8　IDS センサー設定に関連したデバッグ情報を取得するには、次のコマンドを入力します。

debug wps cids enable

（注）　センサーの設定を削除または変更するには、まず、**config wps cids-sensor disable** *index* と入力して設定を無効にする必要があります。その後、センサーを削除するには、**config wps cids-sensor delete** *index* と入力します。

回避クライアントの表示

IDS センサーは、疑わしいクライアントを検出すると、コントローラにこのクライアントを回避するよう警告します。回避エントリは、同じモビリティ グループ内のすべてのコントローラに配信されます。回避すべきクライアントが現在、このモビリティ グループ内のコントローラに接続されている場合、アンカー コントローラはこのクライアントを動的除外リストに追加し、外部コントローラはクライアントを切り離します。次回、このクライアントがコントローラに接続を試みた場合、アンカー コントローラはハンドオフを拒否し、外部コントローラにクライアントを除外することを通知します。モビリティ グループの詳細は、第 11 章 を参照してください。

GUI または CLI により、IDS センサーが回避すべきと特定したクライアントのリストを表示できます。

GUI を使用した 回避クライアントの表示

コントローラの GUI を使用し、IDS センサーによって回避すべきであると判断されたクライアントのリストを表示する手順は、次のとおりです。

ステップ 1　**Security** > **Advanced** > **CIDS** > **Shunned Clients** の順にクリックします。CIDS Shun List ページが表示されます（図 5-55 を参照）。

図 5-55　CIDS Shun List ページ

このページには、各回避クライアントの IP アドレスと MAC アドレス、IDS センサーの要求に応じてコントローラがクライアントのデータ パケットをブロックする期間、およびクライアントを発見した IDS センサーの IP アドレスが表示されます。

ステップ 2　必要に応じてリストを削除、およびリセットするには、**Re-sync** をクリックします。

CLI を使用した 回避クライアントの表示

コントローラの CLI を使用し、IDS センサーによって回避すべきであると判断されたクライアントのリストを表示する手順は、次のとおりです。

ステップ 1　回避すべきクライアントのリストを表示するには、次のコマンドを入力します。

show wps shun-list

ステップ 2　コントローラに対し、このモビリティ グループ内の他のコントローラの回避リストと同期をとるよう強制するには、次のコマンドを入力します。

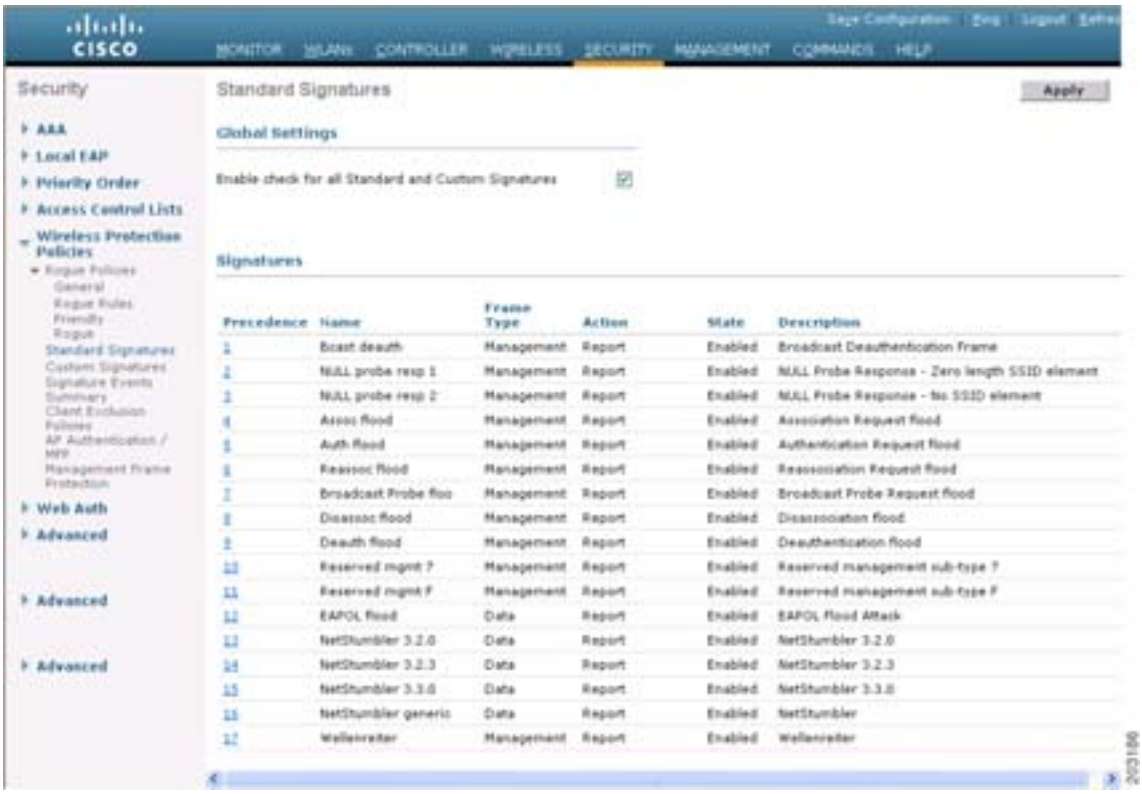
config wps shun-list re-sync

IDS シグニチャの設定

コントローラ上で、IDS シグニチャ、すなわち、受信 802.11 パケットにおけるさまざまなタイプの攻撃を特定するのに使用されるビット パターンのマッチング ルールを設定することができます。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレーム上でシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が開始されます。

Standard Signatures ページに示すように、シスコでは、コントローラ上で 17 の標準シグニチャをサポートしています（図 5-56 を参照）。

図 5-56　Standard Signatures ページ



これらのシグニチャは 6 つの主要なグループに分かれます。初めの 4 つのグループには管理シグニチャが含まれており、後の 2 つのグループにはデータ シグニチャが含まれます。

- **Broadcast deauthentication frame signatures**：ブロードキャスト認証解除フレーム攻撃において、ハッカーは別のクライアントのブロードキャスト MAC 宛先アドレスに対して 802.11 認証解除フレームを送信します。この攻撃は、宛先クライアントをアクセス ポイントからアソシエート解除および切断する原因となります。この処理が繰り返されると、クライアントで DoS 攻撃が発生します。ブロードキャスト認証解除フレーム シグニチャ（優先 1）を使用してそのような攻撃が検出されると、アクセス ポイントでは、シグニチャの特性と一致するクライアント送信ブロードキャスト認証解除フレームがリッスンされます。アクセス ポイントは、そのような攻撃を検出すると、コントローラに警告を送ります。システムの設定に応じて、危険性のあるデバイスが阻止され、そのデバイスの信号が認証されたクライアントに干渉しないようにされるか、コントローラからシステム管理者に、これ以上の操作を行わないよう即時に警告が転送されるか、または、その両方が実行されます。

- **NULL probe response signatures**：NULL プローブ応答攻撃において、ハッカーは無線クライアント アダプタに NULL プローブ応答を送信します。結果として、クライアント アダプタがロックされます。NULL プローブ応答シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは無線クライアントを特定し、コントローラに警告を送ります。NULL プローブ応答には、次のものがあります。
  - NULL probe resp 1（優先 2）
  - NULL probe resp 2（優先 3）
- **Management frame flood signatures**：管理フレーム フラッド攻撃において、ハッカーはアクセス ポイントに大量の 802.11 管理フレームを送り付けます。その結果、アソシエートされたすべてのクライアントに対するサービスが拒絶されるか、アクセス ポイントへのアソシエートが試行され続けます。この攻撃は、アソシエーション要求、認証要求、再アソシエーション要求、プローブ要求、アソシエーション解除要求、認証解除要求、予約管理サブタイプなど、さまざまなタイプの管理フレームを使用して実行されます。

  管理フレーム フラッド シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントによって、シグニチャのすべての特性と一致する管理フレームが特定されます。これらのフレームの頻度が、シグニチャで設定された頻度の値より大きくなると、これらのフレームを受信するアクセス ポイントによってアラームがトリガーされます。コントローラではトラップが生成され、WCS に転送されます。

  管理フレーム フラッド シグニチャには、次のものがあります。
  - Assoc flood（優先順位 4）
  - Auth flood（優先順位 5）
  - Reassoc flood（優先順位 6）
  - Broadcast probe flood（優先順位 7）
  - Disassoc flood（優先順位 8）
  - Deauth flood（優先順位 9）
  - Reserved mgmt 7（優先順位 10）
  - Reserved mgmt F（優先順位 11）

  予約管理フレーム シグニチャ 7 および F は、将来使用するために予約されています。
- **Wellenreiter signature**：Wellenreiter は、無線 LAN スキャンおよびディスカバリ ユーティリティです。これを使用すると、アクセス ポイントおよびクライアントに関する情報が漏洩してしまう可能性があります。Wellenreiter シグニチャ（優先順位 17）を使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定し、コントローラに警告を送ります。
- **EAPOL flood signature**：EAPOL フラッド攻撃において、ハッカーは 802.1X 認証要求を含む EAPOL フレームを大量に発生させます。結果として、802.1X 認証サーバはすべての要求に応答できなくなり、有効なクライアントに正常な認証応答を送信できなくなります。そして、その影響を受けるすべてのクライアントに対するサービスが拒絶されます。EAPOL フラッド シグニチャ（優先順位 12）を使用してそのような攻撃が検出されると、アクセス ポイントは EAPOL パケットの最大許容数を超えるまで待機します。次に、コントローラに警告を送り、適切な緩和措置を実行します。
- **NetStumbler signatures**：NetStumbler は、無線 LAN スキャン ユーティリティです。これによって、アクセス ポイントのブロードキャスト関連情報（動作チャネル、RSSI 情報、アダプタ製造業者名、SSID、WEP ステータス、GPS が接続された NetStumbler を実行するデバイスの経度と緯度など）が報告されます。NetStumbler は、アクセス ポイントに対する認証とアソシエーションを正常に完了すると、次の文字列のデータ フレーム（NetStumbler のバージョンによって異なる）を送信します。

バージョン	文字列
3.2.0	「Flurble gronk bloopit, bnip Frundletrune」
3.2.3	「All your 802.11b are belong to us」
3.3.0	ホワイト スペースを送信

NetStumbler シグニチャを使用してそのような攻撃が検出されると、アクセス ポイントは危険性のあるデバイスを特定してコントローラに警告を送ります。NetStumbler シグニチャには、次のものがあります。

- NetStumbler 3.2.0（優先順位 13）
- NetStumbler 3.2.3（優先順位 14）
- NetStumbler 3.3.0（優先順位 15）
- NetStumbler generic（優先順位 16）

コントローラ上にはデフォルトで標準シグニチャ ファイルが存在します。このシグニチャ ファイルをコントローラからアップロードすることも、カスタム シグニチャ ファイルを作成してコントローラにダウンロードすることも、または標準シグニチャ ファイルを修正してカスタム シグニチャ ファイルを作成することもできます。シグニチャは、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した IDS シグニチャの設定

コントローラ GUI を使用してシグニチャを設定する手順は、次のとおりです。

- IDS シグニチャのアップロードまたはダウンロード。（P. 5-115）
- IDS シグニチャの有効化または無効化。（P. 5-117）
- IDS シグニチャ イベントの表示。（P. 5-119）

GUI を使用した IDS シグニチャのアップロードまたはダウンロード

コントローラの GUI を使用して IDS シグニチャをアップロードまたはダウンロードする手順は、次のとおりです。

ステップ 1　必要に応じて、独自のカスタム シグニチャ ファイルを作成します。

ステップ 2　Trivial File Transfer Protocol（TFTP）サーバが使用可能であることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション　システム　ネットワーク　ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

ステップ 3　カスタム シグニチャ ファイル（*.sig）をダウンロードする場合は、ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 4　**Commands** をクリックして、Download File to Controller ページを開きます（図 5-57 を参照）。

図 5-57　Download File to Controller ページ

ステップ 5　次のいずれかの操作を行います。

- カスタム シグニチャ ファイルをコントローラにダウンロードする場合は、Download File to Controller ページの File Type ドロップダウン ボックスから **Signature File** を選択します。
- 標準シグニチャ ファイルをコントローラからアップロードする場合は、Upload File from Controller ページで **Upload File** をクリックしてから、File Type ドロップダウン ボックスから **Signature File** を選択します。

ステップ 6　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 7　シグニチャ ファイルをダウンロードする場合は、Maximum Retries フィールドにコントローラによるシグニチャ ファイルのダウンロードの最大試行回数を入力します。

範囲：1 ～ 254

デフォルト：10

ステップ 8　シグニチャ ファイルをダウンロードする場合は、シグニチャ ファイルのダウンロードの試行時にコントローラがタイムアウトするまでの時間（秒単位）を Timeout フィールドに入力します。

範囲：1 ～ 254 秒

デフォルト：6 秒

ステップ 9　File Path フィールドに、ダウンロードまたはアップロードするシグニチャ ファイルのパスを入力します。デフォルト値は「/」です。

ステップ 10　File Name フィールドに、ダウンロードまたはアップロードするシグニチャ ファイルの名前を入力します。

（注）　コントローラは、シグニチャのアップロード時に、ユーザが指定した基本名に「_std.sig」および「_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの*両方*を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に ids1_std.sig と ids1_custom.sig を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で ids1_custom.sig を変更し（必ず「Revision = custom」を設定してください）、自動的にダウンロードすることもできます。

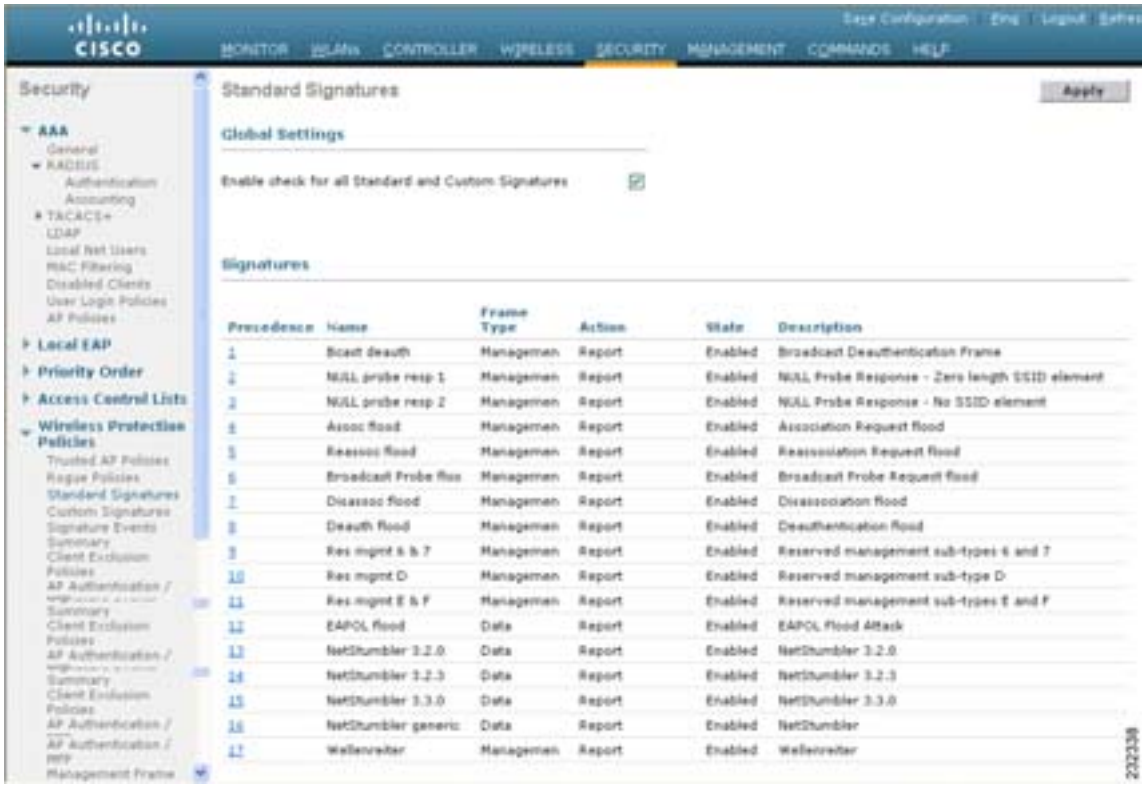
ステップ 11　**Download** をクリックしてシグニチャ ファイルをコントローラにダウンロードするか、**Upload** をクリックしてシグニチャ ファイルをコントローラからアップロードします。

GUI を使用した IDS シグニチャの有効化または無効化

コントローラ GUI を使用して IDS シグニチャを有効化または無効化する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **Standard Signatures** または **Custom Signatures** の順にクリックします。Standard Signatures ページ（図 5-58 を参照）、または Custom Signatures ページが表示されます。

図 5-58　Standard Signatures ページ



Standard Signatures ページには、現在コントローラ上に存在する Cisco 提供のシグニチャのリストが表示されます。Custom Signatures ページには、現在コントローラ上に存在する、ユーザ提供のシグニチャのリストが表示されます。このページには、各シグニチャについて次の情報が表示されます。

- コントローラがシグニチャ チェックをする順序、または優先順位。
- シグニチャ名。シグニチャが検出しようとする攻撃タイプを明示するもの。
- シグニチャがセキュリティ攻撃を検出するフレーム タイプ。フレーム タイプとしては、データおよび管理があります。
- シグニチャが攻撃を検出したとき、コントローラが行うべき処理。処理としては、None と Report があります。
- シグニチャの状態。セキュリティ攻撃を検出するために、シグニチャが有効化されているかどうかを示すもの。

- シグニチャが検出しようとする攻撃のタイプの説明。

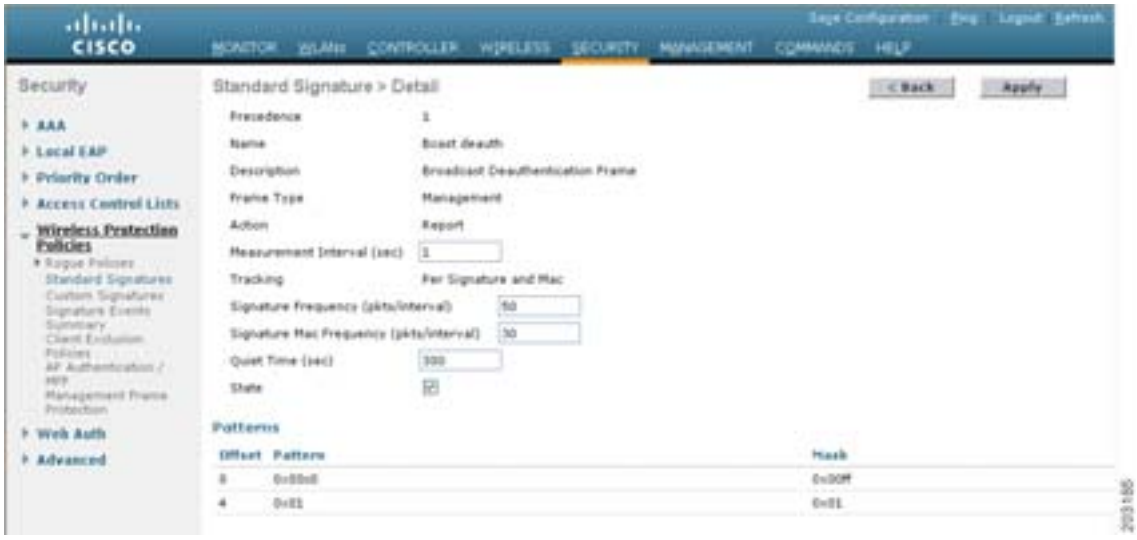
ステップ 2　次のいずれかの操作を行います。

- すべてのシグニチャ（標準およびカスタムの両方）について、それぞれ状態を Enabled に設定して有効にしておく場合には、Standard Signatures ページまたは Custom Signatures ページの上部の **Enable Check for All Standard and Custom Signatures** チェックボックスをオンにします。デフォルト値は、有効になっています（オンになっています）。シグニチャが有効化されると、コントローラに接続されたアクセス ポイントでは、受信した 802.11 データまたは管理フレーム上でシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。
- コントローラ上のすべてのシグニチャ（標準およびカスタムの両方）を無効にしておく場合には、**Enable Check for All Standard and Custom Signatures** チェックボックスをオフにします。このチェックボックスをオフにすると、たとえ個別のシグニチャの状態が Enabled に設定されている場合でも、すべてのシグニチャが無効になります。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　個別のシグニチャを有効化または無効化するには、そのシグニチャの優先順位番号をクリックします。Standard Signature（または Custom Signature）> Detail ページが表示されます（図 5-59 を参照）。

図 5-59　Standard Signature > Detail ページ



このページには、Standard Signatures ページおよび Custom Signatures ページとほぼ同じ情報が表示されますが、次のような詳細も提供します。

- アクセス　ポイントによるシグニチャ分析およびコントローラへの結果報告に使用される追跡方法。次の値が設定可能です。
  - Per Signature：シグニチャ分析とパターン マッチングにおける追跡および報告は、シグニチャ別およびチャネル別に実行されます。
  - Per MAC：シグニチャ分析とパターン マッチングにおける追跡と報告は、個々のクライアント MAC アドレスに対してチャネル別に実行されます。
  - Per Signature and MAC：シグニチャ分析とパターン マッチングにおける追跡と報告は、シグニチャ別 / チャネル別、および MAC アドレス別 / チャネル別の両方で実行されます。
- セキュリティ攻撃の検出に使用されるパターン。

ステップ 5　Measurement Interval フィールドに、シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を入力します。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値はシグニチャによって異なります。

ステップ 6　Signature Frequency フィールドに、攻撃が検出される前に個々のアクセス ポイント レベルで特定されるべき、1 間隔あたりの一致するパケット数を入力します。有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 7　Signature MAC Frequency フィールドに、攻撃が検出される前に個々のアクセス ポイントでクライアント別に特定されるべき、1 間隔あたりの一致するパケット数を入力します。有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 8　Quiet Time フィールドに、個々のアクセス ポイント レベルで攻撃が検出されない状態が経過して、アラームを停止できるようになるまでの時間（秒単位）を入力します。有効な値の範囲は 60 ～ 32,000 秒で、デフォルト値はシグニチャによって異なります。

ステップ 9　**State** チェックボックスをオンにし、このシグニチャを有効にしてセキュリティ攻撃を検出するか、オフにしてこのシグニチャを無効にします。デフォルト値は、有効になっています（オンになっています）。

ステップ 10　**Apply** をクリックして、変更を適用します。Standard Signatures ページまたは Custom Signatures ページに、シグニチャの更新された状態が反映されます。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

GUI を使用した IDS シグニチャ イベントの表示

コントローラ GUI を使用してシグニチャ イベントを表示する手順は、次のとおりです。

ステップ 1　**Security** > **Wireless Protection Policies** > **Signature Events Summary** の順にクリックします。Signature Events Summary ページが表示されます（図 5-60 を参照）。

図 5-60　Signature Events Summary ページ

このページには有効化されたシグニチャによって検出された攻撃の数が表示されます。

ステップ 2　特定のシグニチャによって検出された攻撃の詳細を表示するには、そのシグニチャのシグニチャ タイプのリンクをクリックします。Signature Events Detail ページが表示されます（図 5-61 を参照）。

図 5-61　Signature Events Detail ページ

このページには、次の情報が表示されます。

- 攻撃者として特定されたクライアントの MAC アドレス
- アクセス ポイントが攻撃の追跡に使用する方法
- 攻撃が検出されるまでに特定された 1 秒当たりのマッチング パケットの数
- 攻撃が検出されたチャネル上のアクセス ポイント数
- アクセス ポイントが攻撃を検出した日時

ステップ 3　特定の攻撃の詳細を表示するには、その攻撃の **Detail** リンクをクリックします。Signature Events Track Detail ページが表示されます（図 5-62 を参照）。

図 5-62　Signature Events Track Detail ページ

このページには、次の情報が表示されます。

- 攻撃を検出したアクセス ポイントの MAC アドレス
- 攻撃を検出したアクセス ポイントの名前
- アクセス ポイントが攻撃の検出に使用した無線のタイプ（802.11a または 802.11b/g）
- 攻撃が検出された無線チャネル
- アクセス ポイントから攻撃が報告された日時

CLI を使用した IDS シグニチャの設定

コントローラの CLI を使用して IDS シグニチャを設定する手順は、次のとおりです。

ステップ 1　必要に応じて、独自のカスタム シグニチャ ファイルを作成します。

ステップ 2　TFTP サーバが使用可能であることを確認します。「GUI を使用した IDS シグニチャのアップロードまたはダウンロード」の項（P. 5-115）のステップ 2 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 3　カスタム シグニチャ ファイル（*.sig）を TFTP サーバ上のデフォルト ディレクトリに移動します。

ステップ 4　ダウンロード モードまたはアップロード モードを指定するには、**transfer** {**download** | **upload**} **mode tftp** と入力します。

ステップ 5　ダウンロードまたはアップロードするファイルのタイプを指定するには、**transfer** {**download** | **upload**} **datatype signature** と入力します。

ステップ 6　TFTP サーバの IP アドレスを指定するには、**transfer** {**download** | **upload**} **serverip** *tftp-server-ip-address* と入力します。

（注）　TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

ステップ 7　ダウンロードまたはアップロードのパスを指定するには、**transfer** {**download** | **upload**} **path** *absolute-tftp-server-path-to-file* と入力します。

ステップ 8　ダウンロードまたはアップロードするファイルを指定するには、**transfer** {**download** | **upload**} **filename** *filename.sig* と入力します。

（注）　コントローラは、シグニチャのアップロード時に、ユーザが指定した基本名に「_std.sig」および「_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの*両方*を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に ids1_std.sig と ids1_custom.sig を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で ids1_custom.sig を変更し（必ず「Revision = custom」を設定してください）、自動的にダウンロードすることもできます。

ステップ 9　**transfer** {**download** | **upload**} **start** と入力し、プロンプトに **y** と応答して現在の設定を確認し、ダウンロードまたはアップロードを開始します。

ステップ 10　シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を指定するには、次のコマンドを入力します。

config wps signature interval *signature_id interval*

ここで、*signature_id* は、シグニチャを一意に識別するために使用する数字です。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値はシグニチャによって異なります。

ステップ 11 攻撃が検出される前に個々のアクセス ポイント レベルで特定されるべき、1 間隔あたりの一致するパケット数を指定するには、次のコマンドを入力します。

config wps signature frequency *signature_id frequency*

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 12 攻撃が検出される前に個々のアクセス ポイントでクライアント別に特定されるべき、1 間隔あたりの一致するパケット数を指定するには、次のコマンドを入力します。

config wps signature mac-frequency *signature_id mac_frequency*

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

ステップ 13 個々のアクセス ポイント レベルで攻撃が検出されない状態が経過して、アラームを停止できるようになるまでの時間（秒単位）を指定するには、次のコマンドを入力します。

config wps signature quiet-time *signature_id quiet_time*

有効な値の範囲は 60 ～ 32,000 秒で、デフォルト値はシグニチャによって異なります。

ステップ 14 個別のシグニチャを有効または無効にするには、次のコマンドを入力します。

config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

ステップ 15 変更を保存するには、次のコマンドを入力します。

save config

ステップ 16 必要に応じて、特定のシグニチャまたはすべてのシグニチャをデフォルト値にリセットできます。そのためには、次のコマンドを入力します。

config wps signature reset {*signature_id* | **all**}

（注） シグニチャは、コントローラの CLI を使用してのみデフォルト値にリセットできます。

CLI を使用した IDS シグニチャ イベントの表示

コントローラの CLI を使用してシグニチャ イベントを表示するには、次のコマンドを使用します。

1. コントローラ上にインストールされているすべての標準シグニチャとカスタム シグニチャを表示するには、次のコマンドを入力します。

   show wps signature summary

   次のような情報が表示されます。

```
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 50 pkts/interval
Signature Mac Frequency.......................... 30 pkts/interval
Interval......................................... 1 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast Deauthentication Frame
Patterns:
                0(Header):0x00c0:0x00ff
   4(Header):0x01:0x01
```

2. 有効化されたシグニチャによって検出された攻撃の数を表示するには、次のコマンドを入力します。

   show wps signature events summary

   次のような情報が表示されます。

```
Precedence Signature Name     Type   # Events
---------- ------------------ -----   -----------
1 Bcast deauth    Standard  2
2 NULL probe resp 1  Standard    1
```

3. 特定の標準シグニチャまたはカスタム　シグニチャによって検出された攻撃の詳細を表示するには、次のコマンドを入力します。

   show wps signature events {**standard** | **custom**} *precedence#* **summary**

   次のような情報が表示されます。

```
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. Standard
Number of active events..................... 2

Source MAC Addr   Track Method  Frequency No. APs Last Heard
----------------- ------------  --------- -------- ------------------------
00:01:02:03:04:01 Per Signature   4        3  Tue Dec 6 00:17:44 2005
00:01:02:03:04:01 Per Mac        6  2  Tue Dec 6 00:30:04 2005
```

4. アクセス ポイントによってシグニチャ別 / チャネル別ベースで追跡される攻撃の詳細を表示するには、次のコマンドを入力します。

   show wps signature events {**standard** | **custom**} *precedence#* **detailed per-signature** *source_mac*

5. アクセス ポイントによって個別クライアント ベース（MAC アドレス）で追跡される攻撃の詳細を表示するには、次のコマンドを入力します。

   show wps signature events {**standard** | **custom**} *precedence#* **detailed per-mac** *source_mac*

次のような情報が表示されます。

```
Source MAC..................................... 00:01:02:03:04:01
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Track.......................................... Per Mac
Frequency...................................... 6
Reported By
AP 1
MAC Address.............................. 00:0b:85:01:4d:80
Name..................................... Test_AP_1
Radio Type............................... 802.11bg
Channel.................................. 4
Last reported by this AP................. Tue Dec 6 00:17:49 2005
AP 2
MAC Address.............................. 00:0b:85:26:91:52
Name..................................... Test_AP_2
Radio Type............................... 802.11bg
Channel.................................. 6
        Last reported by this AP.................Tue Dec 6 00:30:04 2005
```

最大ローカル データベース エントリの設定

コントローラの GUI または CLI を使用して、ユーザ認証情報を格納するために使用する最大ローカル データベース エントリを指定できます。データベース内の情報は、コントローラの Web 認証機能と連係して使用されます。

GUI を使用した最大ローカル データベース エントリの設定

GUI を使用して最大ローカル データベース エントリを使用するようコントローラを設定する手順は、次のとおりです。

ステップ 1　**Security** > **AAA** > **General** の順にクリックして、General ページを開きます（図 5-63 を参照）。

図 5-63　General ページ

ステップ 2　Maximum Local Database Entries フィールドに、必要な最大値（次回のコントローラのリブート時の）を入力します可能な値の範囲は 512 ～ 2048 です（これには任意の設定された MAC フィルタ エントリも含まれます）。デフォルト値は 2048 です。現在の値がフィールドの右側のカッコ内に表示されます。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、設定内容を保存します。

CLI を使用したローカル データベース エントリの最大数の指定

CLI を使用して、ローカル データベース エントリの最大数を設定するには、次のコマンドを入力します。

config database size *max_entries*

CHAPTER 6

WLAN の設定

この章では、Cisco UWN Solution のために最大 16 の WLAN を設定する方法について説明します。この章の内容は、次のとおりです。

WLAN の概要

Cisco UWN Solution では、Lightweight アクセス ポイントについて、最大 16 の WLAN を制御できます。各 WLAN には、それぞれ異なる WLAN ID（1 ～ 16）と WLAN SSID（WLAN 名）が割り当てられます。また、一意のセキュリティ ポリシーを割り当てることもできます。

Lightweight アクセス ポイントでは、Cisco UWN ソリューションのアクティブな WLAN SSID がすべてブロードキャストされ、各 WLAN に定義されているポリシーが適用されます。

（注） コントローラが VLAN トラフィックを正常にルーティングできるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

WLAN の設定

次の項では、WLAN を設定する方法について説明します。

WLAN の作成

この項では、コントローラの GUI または CLI を使用して最大 16 の WLAN を作成する手順について説明します。

異なる Service Set Identifier（SSID; サービス セット ID）または同じ SSID で WLAN を設定できます。SSID は、コントローラがアクセスする必要がある特定の無線ネットワークを識別します。同じ SSID で WLAN を作成すると、同じ無線 LAN 内で異なるレイヤ 2 セキュリティ ポリシーを割り当てることができます。同じ SSID を持つ WLAN を区別するには、各 WLAN に対して一意のプロファイル名を作成する必要があります。

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。利用できるレイヤ 2 セキュリティ ポリシーは次のとおりです。

- なし（オープン WLAN）
- 静的 WEP または 802.1X

（注） 静的 WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、静的 WEP と 802.1X の両方を使用できません。

- CKIP
- WPA/WPA2

（注） 同じ SSID を持つ複数の WLAN で WPA と WPA2 の両方を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する WPA/TKIP でそれぞれ設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES でそれぞれ設定することができます。

GUI を使用した WLAN の作成

GUI を使用して WLAN を作成する手順は、次のとおりです。

ステップ 1　**Wireless** > **WLANs** の順にクリックして、WLANs ページを開きます（図 6-1 を参照）。

図 6-1　WLANs ページ

このページでは、コントローラ上で現在設定されているすべての WLAN が表示されます。図 6-1 は、同じ SSID を使用している複数の WLAN を示しています。特に、「user」という名前の 2 つの SSID が示されていますが、プロファイル名が異なります（user1 と user2）。セキュリティ ポリシーも異なることに注意してください。

（注） WLAN を削除するには、その WLAN の青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　新しい WLAN を作成するには、**New** をクリックします。WLANs > New ページが表示されます（図 6-2 を参照）。

図 6-2　WLANs > New ページ

ステップ 3　Type ドロップダウン ボックスから、**WLAN** を選択して WLAN を作成します。

（注）　有線ゲスト ユーザ用にゲスト LAN を作成する場合は、**Guest LAN** を選択し、「有線ゲスト アクセスの設定」の項（P. 9-26）の手順に従ってください。

ステップ 4　Profile Name フィールドに、この WLAN に割り当てるプロファイル名に対する最大 32 文字の英数字を入力します。プロファイル名は一意にする必要があります。

ステップ 5　WLAN SSID フィールドに、この WLAN に割り当てる SSID に対する最大 32 文字の英数字を入力します。

ステップ 6　**Apply** をクリックして、変更を適用します。WLANs > Edit ページが表示されます（図 6-3 を参照）。

（注）　編集する WLAN の名前をクリックすることにより、WLAN ページから WLANs > Edit ページにアクセスすることもできます。

図 6-3　WLANs > Edit ページ

ステップ 7　General タブ、Security タブ、QoS タブおよび Advanced タブ上でパラメータを使用してこの WLAN を設定します。WLAN の特定の機能を設定する手順については、この章の後の項を参照してください。

ステップ 8　General タブの **Status** チェックボックスをオンにして、この WLAN を有効にします。WLAN に対する設定変更が終了するまで、チェックボックスをオフにしておいてください。

ステップ 9　**Apply** をクリックして、変更を適用します。

ステップ 10　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した WLAN の作成

CLI を使用して WLAN を作成するには、次のコマンドを使用します。

1. 既存の WLAN のリストを表示して、有効か無効かを確認するには、次のコマンドを入力します。

   show wlan summary

2. 新しい WLAN を作成するには、次のコマンドを入力します。

   config wlan create *wlan_id profile_name ssid*

   （注） *ssid* を指定しない場合、*profile_name* パラメータがプロファイル名と SSID の両方に対して使用されます。

   （注） 設定ウィザードで WLAN 1 を作成した場合、これは有効モードで作成されています。設定が完了するまでは、無効にしてください。**config wlan create** コマンドを使用して WLAN を新しく作成する場合は、無効モードで作成されます。この場合は、設定が完了するまで無効のままにします。

   （注） 有線ゲスト ユーザ用にゲスト LAN を作成する場合は、「有線ゲスト アクセスの設定」の項（P. 9-26）の手順に従ってください。

3. WLAN を無効にするには（たとえば、WLAN に任意の変更を行う前）、次のコマンドを入力します。

   config wlan disable *wlan_id*

   （注） 管理インターフェイスと AP マネージャ インターフェイスが同じポートにマッピングされており、同じ VLAN のメンバである場合は、これらのインターフェイスのポートマッピングを変更する前に WLAN を無効にする必要があります。管理インターフェイスと AP マネージャ インターフェイスがそれぞれ別の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

4. WLAN を有効にするには（たとえば、WLAN に対する変更が終了した後）、次のコマンドを入力します。

   config wlan enable *wlan_id*

5. WLAN を削除するには、次のコマンドを入力します。

   config wlan delete *wlan_id*

DHCP の設定

WLAN では、同じ Dynamic Host Configuration Protocol (DHCP) サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

内部 DHCP サーバ

コントローラには、内部 DHCP サーバが含まれます。このサーバは、一般的に、DHCP サーバを持たない支社で使用されます。無線ネットワークには、通常、コントローラと同じ IP サブネット上にある 10 個以下のアクセス ポイントが含まれます。内部サーバは、無線クライアント、ダイレクトコネクト アクセス ポイント、管理インターフェイス上のアプライアンスモード アクセス ポイント、およびアクセス ポイントからリレーされた DHCP 要求に対して DHCP アドレスを提供します。Lightweight アクセス ポイントのみサポートされています。内部 DHCP サーバを使用する場合は、コントローラの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、DNS、プライミング、または無線検出などの別の方法を使用してコントローラの管理インターフェイスの IP アドレスを見つける必要があります。

（注） アクセス ポイントがコントローラを見つける方法の詳細は、第 7 章または次の URL からアクセスできる『Controller Deployment Guide』を参照してください。
http://www.cisco.com/en/US/products/ps6366/prod_technical_reference_list.html

外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対しては DHCP リレーとして機能し、クライアントに対しては DHCP サーバとして機能するように設計されています。つまり、各コントローラは、DHCP サーバにとっての DHCP リレー エージェントとなります。これはコントローラが、無線クライアントに対しては、仮想 IP アドレスでの DHCP サーバとして機能することも意味します。

コントローラは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、コントローラ内、コントローラ間、およびサブネット間でのクライアント ローミング時に、各クライアントに対して同じ IP アドレスが保持されます。

DHCP の割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することが推奨されます。

インターフェイスごとの割り当て

個々のインターフェイスに DHCP サーバを割り当てることができます。管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスはプライマリおよびセカンダリ DHCP サーバに設定でき、サービス ポート インターフェイスは DHCP サーバを有効または無効にするように設定できます。

（注） コントローラのインターフェイスの設定方法については、第 3 章を参照してください。

WLAN ごとの割り当て

WLAN で DHCP サーバを定義することもできます。このサーバは、WLAN に割り当てられたインターフェイス上の DHCP サーバのアドレスを無効にします。

セキュリティ上の考慮事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。この要件を適用するためには、すべての WLAN を DHCP Addr. Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Addr. Assignment Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得する必要があります。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントの DHCP プロキシとして動作するコントローラが、DHCP トラフィックを監視します。

（注） 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。無線による管理の設定方法については、「無線による管理機能の使用」の項（P. 5-54）を参照してください。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr. Assignment Required を無効に設定して WLAN を作成できます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

また、DHCP Addr. Assignment Required を無効に設定し、DHCP サーバの IP アドレス を 0.0.0.0 に指定した WLAN を別に作成することもできます。このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの WLAN は、無線接続による管理をサポートしていないことに注意してください。

（注） DHCP プロキシをグローバルに設定する方法については、第 4 章を参照してください。

この項では、DHCP の設定を GUI で行う場合と CLI で行う場合の両方の手順を説明します。

GUI を使用した DHCP の設定

GUI を使用して DHCP を設定する手順は、次のとおりです。

ステップ 1　WLAN に割り当てられる管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスにプライマリ DHCP サーバを設定するには、「GUI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定」の項（P. 3-11）または「GUI を使用した動的インターフェイスの設定」の項（P. 3-17）の手順に従います。

（注） 内部 DHCP サーバを使用する場合は、コントローラの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

ステップ 2　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 3　インターフェイスを割り当てる WLAN のプロファイル名をクリックします。WLANs > Edit (General) ページが表示されます。

ステップ 4　General タブの **Status** チェックボックスをオフにし、**Apply** をクリックして WLAN を無効にします。

ステップ 5　WLAN のプロファイル名を再度クリックします。

ステップ 6　General タブの **Interface** ドロップダウン ボックスから、この WLAN で使用するプライマリ DHCP サーバを設定したインターフェイスを選択します。

ステップ 7　**Advanced** タブをクリックして、WLANs > Edit (Advanced) ページを開きます。

ステップ 8　WLAN 上で、WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを無効にする DHCP サーバを定義する場合、**DHCP Server Override** チェックボックスをオンにして、**DHCP Server IP Addr** 編集ボックスに目的の DHCP サーバの IP アドレスを入力します。チェックボックスはデフォルトでは、無効になっています。

（注）　DHCP を設定する際、DHCP サーバを無効にするのではなく、特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することが推奨されます。

ステップ 9　すべてのクライアントが DHCP サーバから IP アドレスを取得するよう設定するには、**DHCP Addr. Assignment Required** チェックボックスをオンにします。この機能が有効になっている場合、固定 IP アドレスを持つクライアントはネットワーク上で許可されません。デフォルト値は無効です。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　General タブの **Status** チェックボックスをオンにし、**Apply** をクリックして WLAN を再度有効にします。

ステップ 12　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した DHCP の設定

CLI を使用して DHCP を設定する手順は、次のとおりです。

ステップ 1　WLAN に割り当てられる管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスにプライマリ DHCP サーバを設定するには、「CLI を使用した、管理、AP マネージャ、仮想、およびサービス ポートの各インターフェイスの設定」の項（P. 3-13）または「CLI を使用した動的インターフェイスの設定」の項（P. 3-19）の手順に従います。

ステップ 2　WLAN を無効するには、次のコマンドを入力します。

config wlan disable *wlan_id*

ステップ 3　この WLAN で使用するプライマリ DHCP サーバを設定したインターフェイスを指定するには、次のコマンドを入力します。

config wlan interface *wlan_id interface_name*

ステップ 4　WLAN 上で、WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを無効にする DHCP サーバを定義するには、次のコマンドを入力します。

config wlan dhcp_server *wlan_id dhcp_server_ip_address*

（注）　DHCP を設定する際、DHCP サーバを無効にするのではなく、特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することが推奨されます。オーバーライド機能を有効にした場合、**show wlan** コマンドを使用して DHCP サーバが WLAN に割り当てられていることを確認できます。

ステップ 5　WLAN を再度有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

DHCP スコープの設定

コントローラには組み込みの DHCP リレー エージェントがあります。ただし、ネットワーク管理者が別個の DHCP サーバを持たないネットワーク セグメントを求める場合、コントローラに IP アドレスとサブネット マスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのコントローラには、それぞれある範囲の IP アドレスを指定する複数の DHCP スコープを設定できます。

DHCP スコープは内部 DHCP が機能するために必要となります。コントローラで DHCP が定義された後、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをコントローラの管理インターフェイスにポイントできます。コントローラの GUI または CLI を使用して、最大 16 の DHCP スコープを設定できます。

GUI を使用した DHCP スコープの設定

GUI を使用して DHCP スコープを設定する手順は、次のとおりです。

ステップ 1　**Controller** > **Internal DHCP Server** をクリックして、DHCP Scopes ページを開きます（図 6-4 を参照）。

図 6-4　DHCP Scopes ページ

このページには、これまでに設定されたすべての DHCP スコープが表示されます。

（注） 既存の DHCP スコープを削除するには、その スコープの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　新しい DHCP スコープを追加するには、**New** をクリックします。DHCP Scope > New ページが表示されます。

ステップ 3　Scope Name フィールドに、新しい DHCP スコープの名前を入力します。

ステップ 4　**Apply** をクリックします。DHCP Scopes ページが再度表示されたら、新しいスコープの名前をクリックします。DHCP Scope > Edit ページが表示されます（図 6-5 を参照）。

図 6-5　DHCP Scope > Edit ページ

ステップ 5　Pool Start Address フィールドに、クライアントに割り当てられた範囲の開始 IP アドレスを入力します。

（注） このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。

ステップ 6　Pool End Address フィールドに、クライアントに割り当てられた範囲の終了 IP アドレスを入力します。

（注） このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。

ステップ 7　Network フィールドに、この DHCP スコープの対象となるネットワークの名前を入力します。これは、Interfaces ページで設定されている、ネットマスクが適用された管理インターフェイスが使用する IP アドレスです。

ステップ 8　Netmask フィールドに、すべての無線クライアントに割り当てられたサブネット マスクを入力します。

ステップ 9　Lease Time フィールドに、IP アドレスをクライアントに対して許可する時間（0 ～ 65536 秒）を入力します。

ステップ 10　Default Routers フィールドに、コントローラに接続しているオプション ルータの IP アドレスを入力します。各ルータには、DHCP フォワーディング エージェントを含める必要があります。これにより、単一コントローラで複数のコントローラのクライアントを処理できます。

ステップ 11　DNS Domain Name フィールドに、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションの Domian Name System （DNS）ドメイン名を入力します。

ステップ 12　DNS Servers フィールドに、オプションの DNS サーバの IP アドレスを入力します。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。

ステップ 13　Netbios Name Servers フィールドに、Windows Internet Naming Service（WINS）サーバなど、オプションの Microsoft NetBIOS ネーム サーバの IP アドレスを入力します。

ステップ 14　Status ドロップダウン ボックスから、**Enabled** を選択してこの DHCP スコープを有効にするか、または **Disabled** を選択して無効にします。

ステップ 15　**Apply** をクリックして、変更を適用します。

ステップ 16　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した DHCP スコープの設定

CLI を使用して DHCP スコープを設定する手順は、次のとおりです。

ステップ 1　DHCP スコープを作成するには、次のコマンドを入力します。

config dhcp create-scope *scope*

（注）　DHCP スコープを削除するには、次のコマンドを入力します。**config dhcp delete-scope** *scope*.

ステップ 2　クライアントに割り当てられた範囲の開始および終了 IP アドレスを指定するには、次のコマンドを入力します。

config dhcp address-pool *scope start end*

（注）　このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。

ステップ 3　この DHCP スコープの対象となるネットワーク（ネットマスクが適用された管理インターフェイスによって使用される IP アドレス）およびすべての無線クライアントに割り当てられたサブネットマスクを指定するには、次のコマンドを入力します。

config dhcp network *scope network netmask*

ステップ 4　クライアントに IP アドレスを許容する時間（0 ～ 65536 秒）を指定するには、次のコマンドを入力します。

config dhcp lease *scope lease_duration*

ステップ 5　コントローラに接続されているオプション ルータの IP アドレスを指定するには、次のコマンドを入力します。

config dhcp default-router *scope router_1* [*router_2*] [*router_3*]

各ルータには、DHCP フォワーディング エージェントを含める必要があります。これにより、単一コントローラで複数のコントローラのクライアントを処理できます。

ステップ 6　1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションの Domian Name System（DNS）ドメイン名を指定するには、次のコマンドを入力します。

config dhcp domain *scope domain*

ステップ 7　オプションの DNS サーバの IP アドレスを指定するには、次のコマンドを入力します。

config dhcp dns-servers *scope dns1* [*dns2*] [*dns3*]

各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。

ステップ 8　Windows Internet Naming Service（WINS）サーバなど、オプションの Microsoft NetBIOS ネーム サーバの IP アドレスを指定するには、次のコマンドを入力します。

config dhcp netbios-name-server *scope wins1* [*wins2*] [*wins3*]

ステップ 9　この DHCP スコープを有効または無効にするには、次のコマンドを入力します。

config dhcp {**enable** | **disable**} *scope*

ステップ 10　変更を保存するには、次のコマンドを入力します。

save config

ステップ 11　設定されている DHCP スコープのリストを表示するには、次のコマンドを入力します。

show dhcp summary

次のような情報が表示されます。

```
Scope Name           Enabled          Address Range
Scope 1               No          0.0.0.0 -> 0.0.0.0
Scope 2               No          0.0.0.0 -> 0.0.0.0
```

ステップ 12 特定のスコープの DHCP 情報を表示するには、次のコマンドを入力します。

show dhcp *scope*

次のような情報が表示されます。

```
Enabled..................................... No
Lease Time.................................. 0
Pool Start.................................. 0.0.0.0
Pool End.................................... 0.0.0.0
Network..................................... 0.0.0.0
Netmask..................................... 0.0.0.0
Default Routers............................. 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain..................................
DNS......................................... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers........................ 0.0.0.0 0.0.0.0 0.0.0.0
```

WLAN の MAC フィルタリングの設定

クライアント認可または管理者認可に MAC フィルタリングを使用する場合は、WLAN レベルで先に有効にしておく必要があります。任意の WLAN でローカル MAC アドレス フィルタリングを使用する予定がある場合は、この項のコマンドを使用して WLAN の MAC フィルタリングを設定します。

MAC フィルタリングの有効化

WLAN 上で MAC フィルタリングを有効にするには、次のコマンドを使用します。

- **config wlan mac-filtering enable** *wlan_id* コマンドを入力して、MAC フィルタリングを有効にします。
- **show wlan** コマンドを入力して、WLAN の MAC フィルタリングが有効になっていることを確認します。

MAC フィルタリングを有効にすると、WLAN に追加した MAC アドレスにのみ WLAN への接続が許可されます。追加されていない MAC アドレスは、WLAN への接続が許可されません。

ローカル MAC フィルタの作成

コントローラには MAC フィルタリング機能が組み込まれています。これは、RADIUS 認可サーバで提供されるものとよく似ています。

WLAN MAC フィルタに MAC アドレスを追加するには、次のコマンドを使用します。

- **show macfilter** コマンドを入力して、WLAN に割り当てられている MAC アドレスを表示します。
- **config macfilter add** *mac_addr wlan_id* コマンドを入力して、MAC アドレスを WLAN MAC フィルタに割り当てます。
- **show macfilter** コマンドを入力して、WLAN に割り当てられている MAC アドレスを確認します。

無効なクライアントのタイムアウトの設定

無効なクライアントに対してタイムアウトを設定できます。アソシエートしようとした際に認証で 3 回失敗したクライアントは、それ以降のアソシエーションの試みでは自動的に無効にされます。タイムアウト期間が経過すると、クライアントは認証の再試行を許可され、アソシエートすることができます。このとき、認証に失敗すると再び排除されます。無効なクライアントに対してタイムアウトを設定するには、次のコマンドを使用します。

- 無効なクライアントのタイムアウトを設定するには、**config wlan blacklist** *wlan_id timeout* コマンドを入力します。**1** ～ **65,535** 秒のタイムアウトを入力するか、または **0** を入力して永続的にクライアントを無効にします。
- 現在のタイムアウトを確認するには、**show wlan** コマンドを使用します。

インターフェイスへの WLAN の割り当て

WLAN をインターフェイスに割り当てるには、次のコマンドを使用します。

- 次のコマンドを入力して、WLAN をインターフェイスに割り当てます。
  config wlan interface {*wlan_id* | **foreignAp**} *interface_id*
  - WLAN を特定のインターフェイスに割り当てるには、*interface_id* オプションを使用します。
  - サードパーティ アクセス ポイントを使用するには、**foreignAp** オプションを使用します。
- インターフェイスの割り当てステータスを確認するには、**show wlan summary** コマンドを入力します。

DTIM 期間の設定

802.11a/n ネットワークおよび 802.11b/g/n ネットワークの場合、Lightweight アクセス ポイントは、Delivery Traffic Indication Map（DTIM）と同期する一定間隔でビーコンをブロードキャストします。アクセス ポイントでビーコンがブロードキャストされると、DTIM 期間で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャスト データが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11a/n または 802.11b/g/n のネットワークのビーコン期間が 100ms で DTIM 値が 1 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 5 回送信します。ブロードキャスト フレームおよびマルチキャスト フレームの頻度を考慮して、VoIP を含むアプリケーションに適したいずれかの設定を使用できます。

ただし、802.11a/n または 802.11b/g/n のすべてのクライアントで省電力モードが有効になっている場合は、DTIM 値を最大 255 まで設定できます（ブロードキャスト フレームおよびマルチキャスト フレームは 255 回のビーコンで 1 回送信）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100ms で DTIM 値が 100 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒おきに送信するので、省電力クライアントを再起動してブロードキャストとマルチキャストをリッスンするまでのスリープ時間が長くなり、結果的にバッテリー寿命が長くなります。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。省電力クライアントをサポートしている 802.11a/n ネットワークおよび 802.11b/g/n ネットワークでは、DTIM 値を小さく設定ことをお勧めします。

コントローラ ソフトウェア リリース 5.0 では、特定の WLAN 上の 802.11a/n および 802.11b/g/n 無線ネットワークの DTIM 期間を設定できます。以前のソフトウェア リリースでは、DTIM 期間は無線ネットワークごとにのみ設定され、WLAN ごとに設定できませんでした。この変更により、各 WLAN に異なる DTIM 期間を設定できるようになりました。たとえば、音声 WLAN とデータ WLAN に異なる DTIM 値を設定できます。

（注） コントローラ ソフトウェアをリリース 5.0 にアップグレードすると、無線ネットワークに対して設定されていた DTIM 期間が、そのコントローラのすべての既存の WLAN にコピーされます。

GUI を使用した DTIM 期間の設定

GUI を使用して WLAN の DTIM 期間を設定する次の手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

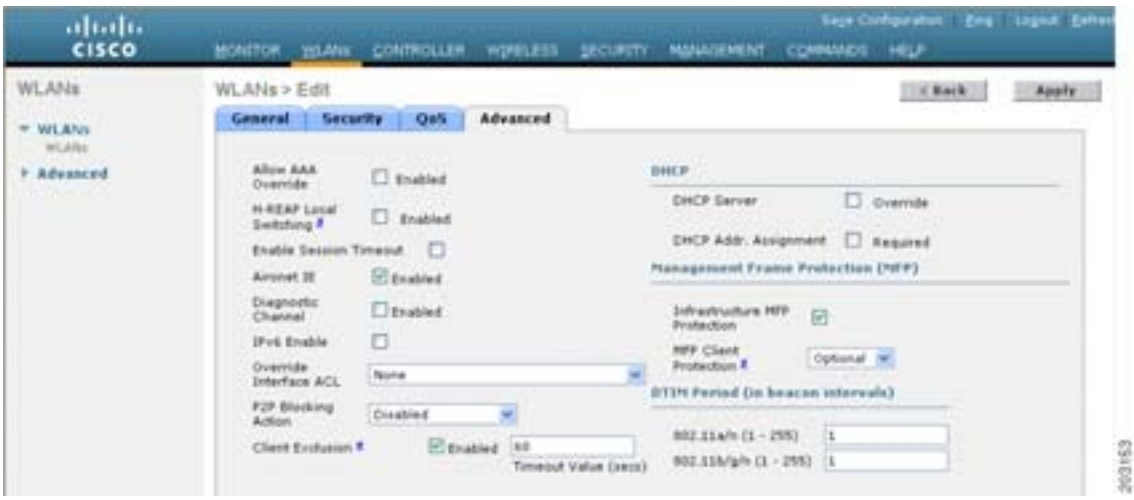
ステップ 2　DTIM 期間を設定する WLAN の名前をクリックします。

ステップ 3　**Status** チェックボックスをオフにしてこの WLAN を無効にします。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　**Advanced** タブをクリックして、WLANs > Edit (Advanced) ページを開きます（図 6-6 を参照）。

図 6-6　WLANs > Edit (Advanced) ページ



ステップ 6　DTIM Period の下の 802.11a/n フィールドと 802.11b/g/n フィールドに 1 ～ 255 までの値を入力します。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。

ステップ 7　**Apply** をクリックして、変更を適用します。

ステップ 8　**General** タブをクリックして、WLANs > Edit (General) ページを開きます。

ステップ 9　**Status** チェックボックスをオンにしてこの WLAN を再度有効にします。

ステップ 10　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した DTIM 期間の設定

CLI を使用して WLAN の DTIM 期間を設定する手順は、次のとおりです。

ステップ 1　WLAN を無効するには、次のコマンドを入力します。

config wlan disable *wlan_id*

ステップ 2　特定の WLAN 上の 802.11a/n または 802.11b/g/n の無線ネットワークのいずれかに DTIM 期間を設定するには、次のコマンドを入力します。

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

dtim の値は、1 ～ 255（両端の値を含む）です。デフォルト値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）です。

ステップ 3　WLAN を再度有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

ステップ 4　変更を保存するには、次のコマンドを入力します。

save config

ステップ 5　DTIM 期間を確認するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

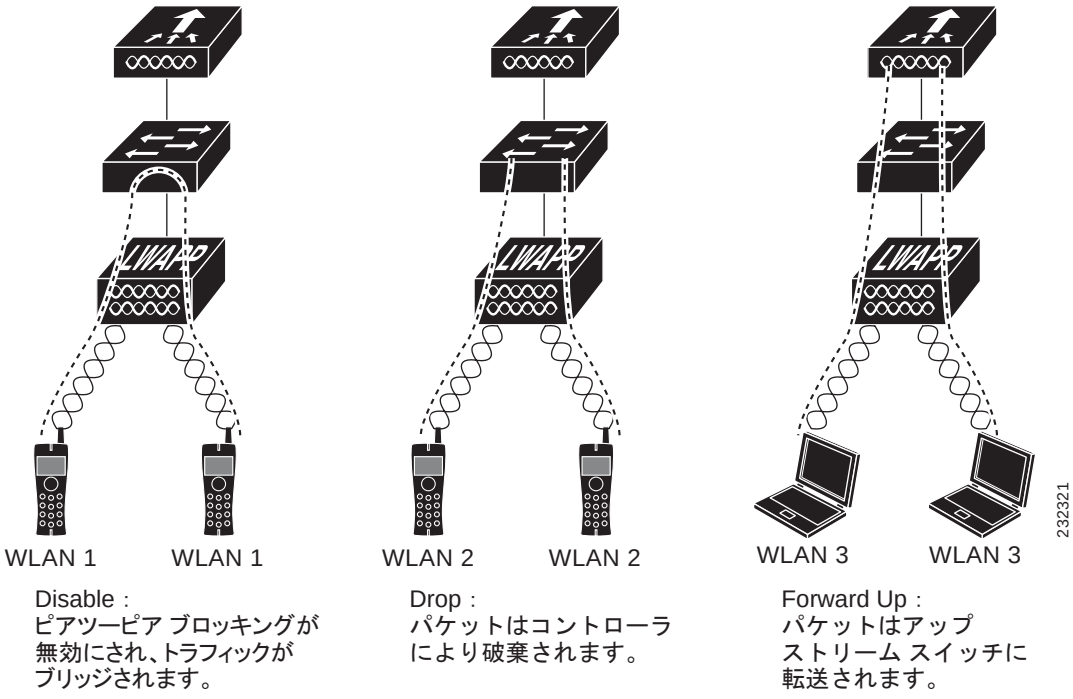
```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Enabled
...
DTIM period for 802.11a radio..................... 1
DTIM period for 802.11b radio..................... 1
Local EAP Authentication..................... Disabled
...
```

ピアツーピア ブロッキングの設定

4.2 以前のコントローラのソフトウェア リリースでは、ピアツーピア ブロッキングはすべての WLAN 上のすべてのクライアントにグローバルに適用され、それによって同じ VLAN 上の 2 つのクライアント間のトラフィックが、コントローラでブリッジされるのではなく、アップストリーム VLAN に転送されていました。この動作の結果、スイッチはパケットを受け取ったのと同じポートからパケットを転送しないため、通常アップストリーム スイッチでトラフィックがドロップされます。

コントローラのソフトウェア リリース 4.2 以降では、ピアツーピア ブロッキングが個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。4.2 以降では、トラフィックがダイレクトされる方法をより詳細に制御することもできます。たとえば、トラフィックがコントローラ内でローカルにブリッジされたり、コントローラによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。図 6-7 は、各オプションを示しています。

図 6-7　ピアツーピア ブロッキングの例



ピアツーピア ブロッキングを使用する際のガイドライン

ピアツーピア ブロッキングを使用する場合には、次のガイドラインに従ってください。

- 4.2 以前のコントローラのソフトウェア リリースでは、コントローラはアドレス解決プロトコル（ARP）要求ストリームを転送します（他のすべてのトラフィックと同様）。コントローラのソフトウェア リリース 4.2 以降では、ARP 要求は、ピアツーピア ブロッキングに設定された動作に従ってダイレクトされます。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- ローカルにスイッチされる Hybrid REAP WLAN およびスタンドアロン モードでの Hybrid REAP アクセス ポイントは、ピアツーピア ブロッキングをサポートしません。

- 以前のリリースから、グローバル ピアツーピア ブロッキングをサポートしているコントローラ ソフトウェア リリース 4.2 以降にアップグレードすると、各 WLAN はトラフィックをアップストリーム VLAN に転送するピアツーピア ブロッキング処理で設定されます。

GUI を使用したピアツーピア ブロッキングの設定

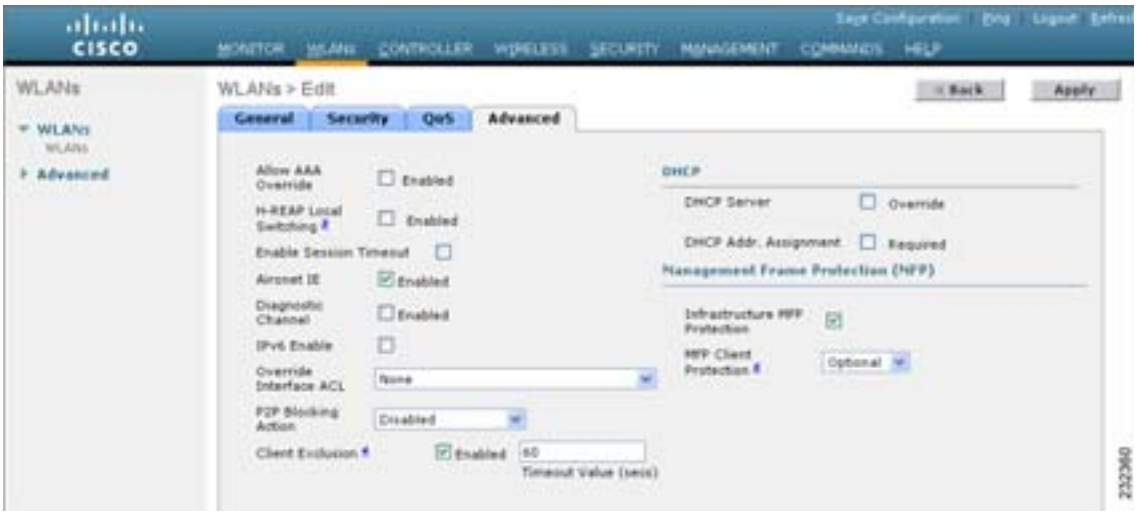
GUI を使用して WLAN のピアツーピア ブロッキングを設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　ピアツーピア ブロッキングを設定する WLAN の名前をクリックします。

ステップ 3　**Advanced** タブをクリックして、WLANs > Edit (Advanced) ページを開きます（図 6-8 を参照）。

図 6-8　WLANs > Edit (Advanced) ページ



ステップ 4　P2P Blocking ドロップダウン ボックスから、次のオプションのいずれかを選択します。

- **Disabled**：ピアツーピア　ブロッキングを無効にして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。これはデフォルト値です。

（注）　コントローラ内の VLAN でトラフィックがブリッジされることはありません。

- **Drop**：コントローラでパケットを破棄するようにします。
- **Forward-UpStream**：パケットがアップストリーム VLAN に転送されるようにします。コントローラ上のデバイスに応じて、パケットに関して実行される処理が決まります。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

CLI を使用したピアツーピア ブロッキングの設定

CLI を使用して WLAN のピアツーピア ブロッキングを設定する手順は、次のとおりです。

ステップ 1　WLAN のピアツーピア ブロッキングを設定するには、次のコマンドを入力します。

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

（注）　各パラメータの詳細は、上記の「GUI を使用したピアツーピア ブロッキングの設定」の項を参照してください。

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

ステップ 3　WLAN のピアツーピア ブロッキングのステータスを参照するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.............................. 1
Profile Name................................. test
Network Name (SSID).......................... test
Status....................................... Enabled
...
...
...
Peer-to-Peer Blocking Action................. Disabled
Radio Policy................................. All
Local EAP Authentication..................... Disabled
```

レイヤ 2 セキュリティの設定

この項では、WLAN にレイヤ 2 セキュリティ設定を割り当てる方法について説明します。

（注）　Microsoft Wireless Configuration Manager と 802.1X を使用しているクライアントは、40 ビットまたは 104 ビットのキーの長さに対して設定された WLAN を使用する必要があります。128 ビットのキーの長さに対して設定すると、アソシエートできても、認証できないクライアントとなります。

静的 WEP キー

コントローラでは、アクセス ポイント上で静的 WEP キーを制御できます。WLAN の静的 WEP を設定するには、次のコマンドを使用します。

- 802.1X 暗号化を無効にするには、次のコマンドを入力します。
  config wlan security 802.1X disable *wlan_id*
- 40/64 ビット、104/128 ビット、または 128/152 ビット WEP キーを設定するには、次のコマンドを入力します。

config wlan security static-wep-key encryption *wlan_id* {**40** | **104** | **128**} {**hex** | **ascii**} *key key_index*

- 40/64 ビット、104/128 ビット、または 128/152 ビット暗号化を指定するには、**40**、**104**、または **128** オプションを使用します。デフォルトの設定は、104/128 です。
- WEP キーの文字形式を指定するには、**hex** または **ascii** オプションを使用します。
- 40 ビット /64 ビット WEP キーの場合は 10 桁の 16 進数（0 ～ 9、a ～ f、または A ～ F の組み合わせ）または印刷可能な 5 つの ASCII 文字、104 ビット /128 ビット キーの場合は 26 桁の 16 進数または 13 の ASCII 文字、128 ビット /152 ビット キーの場合は 32 桁の 16 進数または 16 の ASCII 文字を入力します。
- **1** ～ **4** のキー インデックス（キー スロットとも呼ばれます）を入力します。

802.1X 動的キーおよび認可

コントローラでは、アクセス ポイント上で Extensible Authentication Protocol（EAP; 拡張認証プロトコル）を使用する 802.1X 動的 WEP キーを制御できます。また、WLAN の 802.1X 動的キー設定をサポートしています。

（注） Lightweight アクセス ポイントと無線クライアントで LEAP を使用するには、CiscoSecure Access Control Server（ACS）を設定する際に RADIUS サーバ タイプとして **Cisco-Aironet** を選択することを確認します。

- 各 WLAN のセキュリティ設定を確認するには、**show wlan** *wlan_id* と入力します。新しい WLAN のデフォルトのセキュリティ設定は、動的キーが有効な 802.1X です。レイヤ 2 の堅牢なポリシーを維持するには、802.1X を WLAN 上で設定したままにします。
- 802.1X 認証を無効または有効にするには、次のコマンドを使用します。

  config wlan security 802.1X {**enable** | **disable**} *wlan_id*

  802.1X 認証を有効にした後、コントローラから、無線クライアントと認証サーバとの間で EAP 認証パケットが送信されます。このコマンドにより、すべての EAP タイプのパケットは、コントローラとの送受信が可能になります。
- WLAN の 802.1X の暗号化レベルを変更するには、次のコマンドを使用します。

  config wlan security 802.1X encryption *wlan_id* [**40** | **104** | **128**]

  - 40/64 ビット暗号化を指定するには、40 オプションを使用します。
  - 104/128 ビット暗号化を指定するには、104 オプションを使用します。（これは、デフォルトの暗号化設定です）。
  - 128/128 ビット暗号化を指定するには、128 オプションを使用します。

静的 WEP と動的 WEP の両方をサポートする WLAN の設定

静的 WEP キーをサポートする WLAN は 4 つまで設定できます。また、これらすべての静的 WEP WLAN に動的 WEP も設定できます。静的 WEP と動的 WEP を両方サポートする WLAN を設定する際の留意事項は次のとおりです。

- 静的 WEP キーおよび動的 WEP キーは、同じ長さである必要があります。
- 静的 WEP と動的 WEP の両方をレイヤ 2 セキュリティ ポリシーとして設定する場合は、他のセキュリティ ポリシーを指定できません。つまり、Web 認証を設定できません。ただし、静的 WEP と動的 WEP のいずれかをレイヤ 2 セキュリティ ポリシーとして設定する場合は、Web 認証を設定できます。

WPA1 と WPA2

Wi-Fi 保護アクセス（WPA または WPA1）および WPA2 は、無線 LAN システム用のデータ保護とアクセス コントロールを提供する Wi-Fi Alliance の規格ベースのセキュリティ ソリューションです。WPA1 は、IEEE 802.11i 規格に準拠していますが、規格の承認前に実装されたものです。これに対して、WPA2 は、承認された IEEE 802.11i 規格が Wi-Fi Alliance によって実装されています。

WPA1 のデフォルトでは、データの保護に Temporal Key Integrity Protocol（TKIP）および Message Integrity Check（MIC）が使用されますが、WPA2 では Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用したより強力な Advanced Encryption Standard 暗号化アルゴリズム（AES-CCMP）が使用されます。WPA1 および WPA2 のデフォルトでは、両方とも 802.1X を使用して認証キー管理を行います。ただし、次に説明する PSK、CCKM、および 802.1X+CCKM の各オプションも利用できます。

- **802.1X**：IEEE によって定義された無線 LAN セキュリティの規格。*802.1X for 802.11*、または単に *802.1X* と呼ばれます。802.1X をサポートするアクセス ポイントは、無線ネットワークを介して通信を行う相手となる無線クライアントおよび認証サーバ（RADIUS サーバなど）との間のインターフェイスとして機能します。802.1X が選択されている場合は、802.1X クライアントのみがサポートされます。
- **PSK**：PSK（*WPA 事前共有キー*または *WPA パスフレーズ*とも呼ばれます）を選択した場合は、事前共有キー（またはパスフレーズ）を設定する必要があります。このキーは、クライアントと認証サーバの間で Pairwise Master Key（PMK; ペアワイズ マスター キー）として使用されます。
- **CCKM**：Cisco Centralized Key Management（CCKM）では、迅速なキーの再生成技術を使用しています。この技術を使用すると、クライアントは、通常 150 ミリ秒（ms）以下で、コントローラを経由せずにあるアクセス ポイントから別のアクセス ポイントにローミングできます。CCKM により、クライアントが新しいアクセス ポイントと相互に認証を行い、再アソシエーション時に新しいセッション キーを取得するために必要な時間が短縮されます。CCKM の迅速かつ安全なローミングでは、無線 VoIP、Enterprise Resource Planning（ERP）、Citrix ベースのソリューションなどの時間依存型のアプリケーションにおいて、認識できるほどの遅延は発生しません。CCKM は、CCXv4 に準拠する機能です。CCKM が選択されている場合は、CCKM クライアントのみがサポートされます。

（注） コントローラ ソフトウェア リリース 4.2 以降では、CCX バージョン 1 ～ 5 をサポートしています。CCX のサポートは、コントローラ上のすべての WLAN に対して自動的に有効になり、無効にすることはできません。コントローラは、クライアント データベースにクライアントの CCX バージョンを格納し、これを使用してクライアントの機能を制限します。CCKM を使用するには、クライアントで CCXv4 または v5 をサポートする必要があります。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

- **802.1X+CCKM**：通常の動作状態の間、802.1X　が有効になっているクライアントは、主要な RADIUS サーバとの通信を含む完全な 802.1X 認証を実行することにより、新しいアクセス ポイントとの相互認証を行います。ただし、802.1X および CCKM の迅速で安全なローミング用に WLAN を設定した場合、CCKM が有効になっているクライアントは、RADIUS サーバに対して再認証せずに、あるアクセス ポイントから別のアクセス ポイントに安全にローミングを行います。このオプションが選択されている場合、CCKM クライアントと非 CCKM クライアントの両方がサポートされるため、802.1X+CCKM はオプションの CCKM とみなされます。

単一の WLAN では、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM のクライアントに接続を許可できます。このような WLAN 上のすべてのアクセス ポイントは、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM の情報要素をビーコン応答とプローブ応答でアドバタイズします。WPA1 または WPA2、あるいは両方を有効にした場合は、データ トラフィックを保護するために設計された 1 つまたは 2 つの*暗号方式*（暗号化アルゴリズム）を有効にすることもできます。

具体的には、WPA1 または WPA2、あるいはその両方に対して、AES または TKIP、またはその両方を有効にすることができます。TKIP は WPA1 のデフォルト値で、AES は WPA2 のデフォルト値です。

WPA1 と WPA2 は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した WPA1 と WPA2 の設定

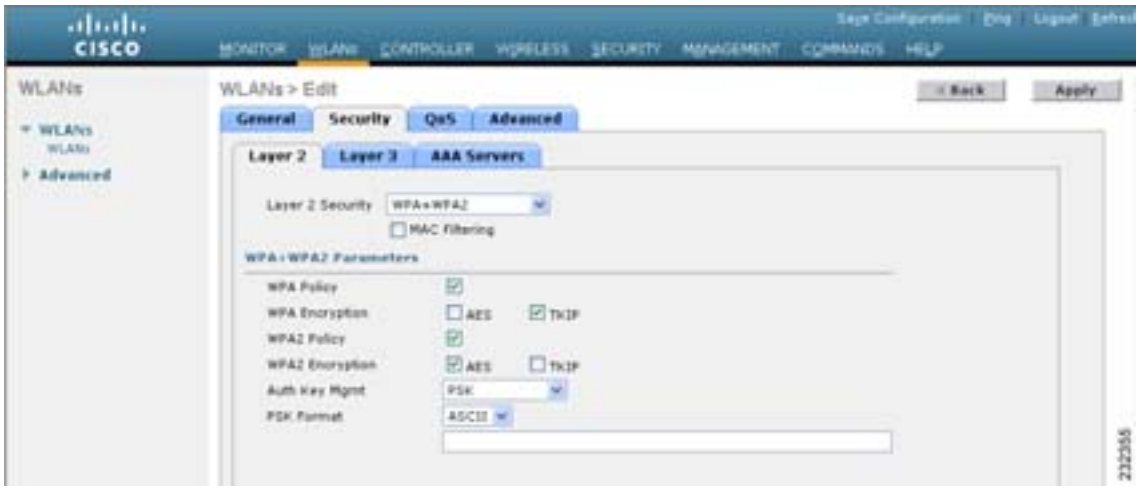
コントローラ GUI を使用して WLAN の WPA1 と WPA2 を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Security** タブおよび **Layer 2** タブをクリックして、WLANs > Edit（Security > Layer 2）ページを開きます（図 6-9 を参照）。

図 6-9　WLANs > Edit（Security > Layer 2）ページ



ステップ 4　Layer 2 Security ドロップダウン ボックスから **WPA+WPA2** を選択します。

ステップ 5　WPA+WPA2 Parameters で、**WPA Policy** チェックボックスをオンにして WPA1 を有効にするか、**WPA2 Policy** チェックボックスをオンにして WPA2 を有効にするか、または両方のチェックボックスをオンにして WPA1 と WPA2 を両方有効にします。

（注）　WPA1 および WPA2 のデフォルト値は、両方とも無効になっています。WPA1 と WPA2 を両方とも無効のままにすると、アクセス ポイントは、ステップ 7 で選択する認証キー管理方式に対してのみ情報要素をビーコンおよびプローブ応答でアドバタイズします。

ステップ 6　WPA1、WPA2、またはその両方に対して、AES データ暗号化を有効にする場合は **AES** チェックボックスをオンにし、TKIP データ暗号化を有効にする場合は **TKIP** チェックボックスをオンにします。WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。

ステップ 7　Auth Key Mgmt ドロップダウン ボックスから、次のいずれかのキー管理方式を選択します。**802.1X**、**CCKM**、**PSK**、または **802.1X+CCKM**.

ステップ 8　ステップ 7 で PSK を選択した場合は、PSK Format ドロップダウン ボックスから **ASCII** または **HEX** を選択し、空のフィールドに事前共有キーを入力します。WPA の事前共有キーには、8 ～ 63 個の ASCII テキスト文字、または 64 桁の 16 進数文字が含まれている必要があります。

ステップ 9　**Apply** をクリックして、変更を適用します。

ステップ 10　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した WPA1 と WPA2 の設定

コントローラ CLI を使用して WLAN の WPA1 と WPA2 を設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 2　次のコマンドを入力して、WLAN に対して WPA を有効または無効にします。

config wlan security wpa {**enable** | **disable**} *wlan_id*

ステップ 3　次のコマンドを入力して、WLAN に対して WPA1 を有効または無効にします。

config wlan security wpa wpa1 {**enable** | **disable**} *wlan_id*

ステップ 4　次のコマンドを入力して、WLAN に対して WPA2 を有効または無効にします。

config wlan security wpa wpa2 {**enable** | **disable**} *wlan_id*

ステップ 5　次のコマンドを入力して WPA1 または WPA2 に対して AES または TKIP データ暗号化を有効または無効にします。

- **config wlan security wpa wpa1 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*
- **config wlan security wpa wpa2 ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。

ステップ 6　次のコマンドを入力して、802.1X、PSK、または CCKM の認証キー管理を有効または無効にします。

config wlan security wpa akm {**802.1X** | **psk** | **cckm**} {**enable** | **disable**} *wlan_id*

デフォルト値は 802.1X です。

ステップ 7　ステップ 6 で PSK を有効にした場合は、次のコマンドを入力して事前共有キーを指定します。

config wlan security wpa akm psk set-key {**ascii** | **hex**} *psk-key wlan_id*

WPA の事前共有キーには、8 ～ 63 個の ASCII テキスト文字、または 64 桁の 16 進数文字が含まれている必要があります。

ステップ 8　ステップ 6 で CCKM を有効にした場合、必要に応じて、PMK キャッシュ ライフタイム タイマーを使用して、クライアントでの再認証をトリガします。タイマーは、AAA サーバから受信したタイムアウト値または WLAN のセッション タイムアウト設定に基づきます。タイマーが切れるまでに残されている時間を確認するには、次のコマンドを入力します。

show pmk-cache all

次のような情報が表示されます。

```
PMK-CCKM Cache
                          Entry
Type        Station       Lifetime   VLAN Override        IP Override
------  ------------------ --------   ------------------   ---------------
CCKM    00:07:0e:b9:3a:1b  150                         0.0.0.0
```

ステップ 9　次のコマンドを入力して WLAN を有効にします。

config wlan enable *wlan_id*

ステップ 10　次のコマンドを入力して、設定を保存します。

save config

CKIP

Cisco Key Integrity Protocol（CKIP）は、IEEE 802.11 メディアを暗号化するためのシスコ独自のセキュリティ プロトコルです。CKIP では、インフラストラクチャ モードでの IEEE 802.11 セキュリティを強化するために、キーの置換、メッセージの整合性チェック（MIC）、およびメッセージ シーケンス番号が使用されています。ソフトウェア リリース 4.0 以降では、静的キーを使用した CKIP をサポートしています。この機能を正常に動作させるには、WLAN に対して Aironet 情報要素（IE）を有効にする必要があります。

Lightweight アクセス ポイントは、ビーコンおよびプローブ応答パケットに Aironet IE を追加し、CKIP ネゴシエーション ビット [キー置換およびマルチモジュラ ハッシュ メッセージ整合性チェック（MMH MIC）] の一方または両方を設定することにより、CKIP のサポートをアドバタイズします。キー置換は、基本の暗号キーおよび現在の初期ベクトル（IV）を使用して新しいキーを作成するデータ暗号化技術です。MMH MIC では、ハッシュ関数を使用してメッセージ整合性コードを計算することにより、暗号化されたパケットでのパケット改ざん攻撃を回避します。

WLAN で指定された CKIP の設定は、アソシエートを試みるすべてのクライアントに必須です。WLAN で CKIP のキー置換および MMH MIC の両方が設定されている場合、クライアントは両方をサポートする必要があります。WLAN でこれらの機能の一方のみが設定されている場合、クライアントはこの CKIP 機能のみをサポートするだけでかまいません。

CKIP では、5 バイトおよび 13 バイトの暗号キーは 16 バイトのキーに拡張される必要があります。キーを拡張するためのアルゴリズムは、アクセス ポイントで発生します。キーは、長さが 16 バイトに達するまで、そのキー自体に繰り返し追加されます。Lightweight アクセス ポイントはすべて CKIP をサポートしています。

CKIP は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した CKIP の設定

コントローラ GUI を使用して WLAN の CKIP を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Advanced** タブをクリックします。

ステップ 4　**Aironet IE** チェックボックスをオンにして、この WLAN に対する Aironet IE を有効にし、**Apply** をクリックします。

ステップ 5　**General** タブをクリックします。

ステップ 6　**Status** チェックボックスがオンになっている場合は、これをオフにしてこの WLAN を無効にし、**Apply** をクリックします。

ステップ 7　**Security** タブおよび **Layer 2** タブをクリックして、WLANs > Edit（Security > Layer 2）ページを開きます（図 6-10 を参照）。

図 6-10　WLANs > Edit（Security > Layer 2）ページ

ステップ 8　Layer 2 Security ドロップダウン ボックスから **CKIP** を選択します。

ステップ 9　CKIP Parameters で、Key Size ドロップダウン ボックスから CKIP 暗号キーの長さを選択します。

範囲：Not Set、40 bits、または 104 bits

デフォルト：Not Set

ステップ 10　Key Index ドロップダウン ボックスからこのキーに割り当てる番号を選択します。キーは、最高 4 つまで設定できます。

ステップ 11 Key Format ドロップダウン ボックスから **ASCII** または **HEX** を選択し、Encryption Key フィールドに暗号キーを入力します。40 ビットのキーには、5 個の ASCII テキスト文字または 10 桁の 16 進数文字が含まれている必要があります。104 ビットのキーには、13 個の ASCII テキスト文字または 26 桁の 16 進数文字が含まれている必要があります。

ステップ 12 この WLAN に対して MMH MIC データ保護を有効にする場合は、**MMH Mode** チェックボックスをオンにします。デフォルト値は、無効になっています（オフになっています）。

ステップ 13 この形式の CKIP データ保護を有効にする場合は、**Key Permutation** チェックボックスをオンにします。デフォルト値は、無効になっています（オフになっています）。

ステップ 14 **Apply** をクリックして、変更を適用します。

ステップ 15 **General** タブをクリックします。

ステップ 16 **Status** チェックボックスをオンにしてこの WLAN を有効にします。

ステップ 17 **Apply** をクリックして、変更を適用します。

ステップ 18 **Save Configuration** をクリックして、変更を保存します。

CLI を使用した CKIP の設定

コントローラ CLI を使用して WLAN の CKIP を設定する手順は、次のとおりです。

ステップ 1 次のコマンドを入力して WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 2 次のコマンドを入力して、この WLAN に対して Aironet IE を有効にします。

config wlan ccx aironet-ie enable *wlan_id*

ステップ 3 次のコマンドを入力して WLAN に対して CKIP を有効または無効にします。

config wlan security ckip {**enable** | **disable**} *wlan_id*

ステップ 4 次のコマンドを入力して、WLAN に対して CKIP の暗号キーを指定します。

config wlan security ckip akm psk set-key *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key_index*

ステップ 5 次のコマンドを入力して WLAN に対して CKIP の MMH MIC を有効または無効にします。

config wlan security ckip mmh-mic {**enable** | **disable**} *wlan_id*

ステップ 6 次のコマンドを入力して WLAN に対して CKIP のキー置換を有効または無効にします。

config wlan security ckip kp {**enable** | **disable**} *wlan_id*

ステップ 7　次のコマンドを入力して WLAN を有効にします。

config wlan enable *wlan_id*

ステップ 8　次のコマンドを入力して、設定を保存します。

save config

レイヤ 3 セキュリティの設定

この項では、コントローラ上の WLAN に対してレイヤ 3 セキュリティを設定する方法について説明します。

（注） Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）と IPSec は、ソフトウェア リリース 4.0 以降を実行しているコントローラでサポートされていません。

VPN パススルー

GUI を使用した VPN パススルーの設定

コントローラの GUI を使用して WLAN の VPN パススルーを設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　VPN パススルーを設定する WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。

ステップ 3　**Security** タブおよび **Layer 3** タブをクリックして、WLANs > Edit（Security > Layer 3）ページを開きます（図 6-11 を参照）。

図 6-11　WLANs > Edit（Security > Layer 3）ページ

ステップ 4　Layer 3 Security ドロップダウン ボックスから **VPN Pass-Through** を選択します。

ステップ 5　VPN Gateway Address フィールドに、クライアントにより開始され、コントローラを通過した VPN トンネルを終端しているゲートウェイ ルータの IP アドレスを入力します。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、設定内容を保存します。

CLI を使用した VPN パススルーの設定

コントローラ CLI を使用して WLAN の VPN パススルーを設定するには、次のコマンドを入力します。

- **config wlan security passthru** {**enable** | **disable**} *wlan_id gateway*

  gateway には、VPN トンネルを終端している IP アドレスを入力します。
- パススルーが有効になっていることを確認するには、**show wlan** コマンドを入力します。

Web 認証

コントローラで IPSec または VPM パススルーが有効になっていない場合、WLAN では Web 認証を使用できます。Web 認証は、セットアップも使用方法も簡単で、SSL とともに使用することで WLAN 全体のセキュリティを向上させることができます。

（注）　Web 認証はレイヤ 2 セキュリティ ポリシー（オープン認証、オープン認証 + WEP、WPA-PSK）でのみサポートされています。802.1X での使用はサポートされていません。

（注）　Web 認証は HTTP 経由のみがサポートされています。HTTPS はサポートされていません。Web 認証はコントローラの管理ログインに関連付けられているため、管理用 HTTPS ログインを無効にして、管理用 HTTP のみを有効にする必要があります。

（注）　WLAN の Web 認証を有効にする場合、コントローラが無線クライアントで送受信されるトラフィックを転送することを示すメッセージが認証前に表示されます。シスコでは、DNS トラフィックを規制し、DNS トンネリング攻撃を検出および予防するために、ゲスト VLAN の背後にファイアウォールまたは Intrusion Detection System（IDS; 侵入検知システム）を設置することをお勧めします。

GUI を使用した Web 認証の設定

コントローラ GUI を使用して WLAN の Web 認証を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　Web 認証を設定する WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。

ステップ 3　**Security** タブおよび **Layer 3** タブをクリックして、WLANs > Edit（Security > Layer 3）ページを開きます。

ステップ 4　**Web Policy** チェックボックスをオンにします。

ステップ 5　**Authentication** オプションが選択されていることを確認します。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、設定内容を保存します。

CLI を使用した Web 認証の設定

コントローラ CLI を使用して WLAN の Web 認証を設定するには、次のコマンドを入力します。

- **config wlan security web** {**enable** | **disable**} *wlan_id*
- Web 認証が有効になっていることを確認するには、**show wlan** コマンドを入力します。

WLAN への QoS プロファイルの割り当て

Cisco UWN Solution の WLAN は、4 レベルの QoS をサポートしています。Platinum（音声）、Gold（ビデオ）、Silver（ベスト エフォート）、Bronze（バックグラウンド）です。デフォルトは Silver です。音声転送 WLAN で Platinum QoS を使用するよう設定したり、低帯域幅 WLAN で Bronze QoS を使用するよう割り当てたり、その他すべてのトラフィックに残りの QoS レベルを割り当てたりすることができます。

WLAN QoS レベルは、無線トラフィックの特定の 802.11e User Priority（UP）を定義します。この UP は、WMM 以外の有線トラフィックの優先順位を導出すると同時に、さまざまな優先レベルの WMM トラフィックを管理する際の上限値としても機能します。アクセス ポイントは、表 6-1 の値に従ってこの QoS プロファイル固有の UP を使用することで、無線 LAN 上で確認可能な IP DSCP 値を導出します。

表 6-1　アクセス ポイントの QoS 変換値

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

表 6-1　アクセス ポイントの QoS 変換値（続き）

AVVID 802.1p 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
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

コントローラの GUI または CLI を使用して、WLAN に QoS プロファイルを割り当てることができます。

GUI を使用した WLAN への QoS プロファイルの割り当て

コントローラの GUI を使用して WLAN へ QoS プロファイルを割り当てる手順は、次のとおりです。

ステップ 1　まだ設定していない場合は、「GUI を使用した QoS プロファイルの設定」の項（P. 4-51）の指示に従って 1 つ以上の QoS プロファイルを設定してください。

ステップ 2　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 3　QoS プロファイルを割り当てる WLAN の名前をクリックします。

ステップ 4　WLANs > Edit ページが表示されたら、**QoS** タブをクリックします。

ステップ 5　Quality of Service（QoS）ドロップダウン ボックスから、次のいずれかを選択します。

- Platinum（音声）
- Gold（ビデオ）
- Silver（ベスト エフォート）
- Bronze（バックグラウンド）
- Silver（ベスト エフォート）がデフォルト値です。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した WLAN への QoS プロファイルの割り当て

コントローラ CLI を使用して WLAN へ QoS プロファイルを割り当てる手順は、次のとおりです。

ステップ 1　まだ設定していない場合は、「CLI を使用した QoS プロファイルの設定」の項（P. 4-53）の指示に従って 1 つ以上の QoS プロファイルを設定してください。

ステップ 2　QoS プロファイルを WLAN に割り当てるには、次のコマンドを入力します。

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}

Silver がデフォルト値です。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　QoS を WLAN に適切に割り当てたことを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist.................................... Disabled
Session Timeout.................................. 0
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... 1.100.163.24
DHCP Address Assignment Required................. Disabled
Quality of Service.............................. Silver (best effort)
WMM.............................................. Disabled
...
```

QoS Enhanced BSS の設定

QoS Enhansed Basis Service Set（QBSS）情報要素（IE）により、アクセス ポイントはそのチャネル使用率を無線デバイスに通知できます。チャネル使用率が高いアクセス ポイントではリアルタイム トラフィックを効率的に処理できないため、7921 または 7920 電話では、QBSS 値を使用して、他のアクセス ポイントにアソシエートするべきかどうかが判断されます。次の 2 つのモードで QBSS を有効にできます。

- 802.11E QBSS 規格を満たすデバイス（Cisco 7921 IP Phone など）をサポートしている、Wi-Fi Multimedia（WMM）モード
- 802.11b/g ネットワーク上で Cisco 7920 IP Phone をサポートしている 7920 サポート モード

  7920 サポート モードには、次の 2 つのオプションが含まれています。

  - Call Admission Controll（CAC; コール アドミッション制御）がクライアント デバイス上で設定され、クライアント デバイスによってアドバタイズされている必要がある 7920 電話のサポート（通常、旧式の 7920 電話）
  - CAC がアクセス ポイント上で設定され、アクセス ポイントによってアドバタイズされている必要がある 7920 電話のサポート（通常、新式の 7920 電話）

    アクセス ポイントで制御される CAC が有効になっている場合、アクセス ポイントは、シスコが所有する CAC Information Element（IE; 情報要素）を送信し、標準の QBSS IE を送信しません。

コントローラの GUI または CUI を使用して QBSS を設定できます。デフォルトで、QBSS は無効になっています。

QBSS を設定する際のガイドライン

WLAN で QBSS を設定する場合には、次のガイドラインに従ってください。

- 7920 電話は、CAC 機能が制限された、非 WMM 電話です。電話は、アソシエート先のアクセス ポイントのチャネル使用率を確認し、それをアクセス ポイントによりビーコンされたしきい値と比較します。チャネル使用率がしきい値より低い場合は、7920 は電話をかけます。対照的に、7921 電話は、完全な機能を備えた WMM 電話で、Traffic Specifications（TSPEC）を使用して、電話をかける前に音声キューにアクセスします。7921 電話は、負荷ベースの CAC と適切に連動します。負荷ベースの CAC では、音声に取り分けられたチャネルの割合を使用して、それに応じて通話を制限しようとします。

  7921 電話は WMM をサポートし、7920 電話はサポートしないため、これらの電話を混合環境で使用する場合に両方の電話を適切に設定していないと、キャパシティと音声品質の問題が生じる可能性があります。7921 および 7920 電話の両方を有効にして同じネットワーク上で共存させるには、負荷ベースの CAC と 7920 AP CAC の両方がコントローラで有効にされ、WMM Policy が Allowed に設定されていることを確認してください。7921 ユーザより、7920 ユーザの方が多い場合に、これは特に重要になります。

（注） 負荷ベースの CAC の詳細および設定の手順は、第 4 章を参照してください。

7921 および 7920 Wireless IP Phone を使用する際の追加のガイドライン

Cisco 7921 および 7920 Wireless IP Phone をコントローラで使用する場合は、次のガイドラインに従ってください。

- 各コントローラで、アグレッシブなロード バランシングが無効にされている必要があります。無効化されていない場合、電話による初期ローミングが失敗し、オーディオ パスが中断されることがあります。
- Dynamic Transmit Power Control（DTPC）情報要素（IE）が、**config 802.11b dtpc enable** コマンドを使用して有効にされている必要があります。DTPC IE は、アクセス ポイントがその送信電力で情報をブロードキャストすることを可能にする、ビーコンおよびプローブの情報要素です。7921 または 7920 電話は、この情報を使用して、その送信電力を、アソシエート先のアクセス ポイントと同じレベルに自動的に調整します。このようにして、両方のデバイスが同じレベルで送信するようになります。
- 7921 と 7920 電話のおよびコントローラの両方で、Cisco Centralized Key Management（CCKM）高速ローミングがサポートされます。
- WEP を設定する際、コントローラおよび 7921 または 7920 電話によって、用語上の違いがあります。7921 または 7920 で 128 ビット WEP を使用する場合は、コントローラを 104 ビットに設定してください。
- スタンドアロンの 7921 電話では、負荷ベースの CAC が有効にされ、また WLAN 上で WMM Policy が Required に設定されている必要があります。

GUI を使用した QBSS の設定

コントローラの GUI を使用して QBSS を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　WMM モードを設定する WLAN の名前をクリックします。

ステップ 3　WLANs > Edit ページが表示されたら、**QoS** タブをクリックして WLANs > Edit（Qos）ページを開きます（図 6-12 を参照）。

図 6-12　WLANs > Edit（QoS）ページ

ステップ 4　7291 電話および WMM 規格を満たすその他のデバイスに対して WMM モードを有効にするかどうかに応じて、WMM Policy ドロップダウン ボックスから次のオプションのいずれかを選択してください。

- **Disabled**：WLAN 上で WMM を無効にします。これはデフォルト値です。
- **Allowed**：WLAN 上でクライアント デバイスに WMM の使用を許可します。
- **Required**：クライアント デバイスで WMM の使用を必須にします。WMM をサポートしていないデバイスは WLAN に接続できません。

（注）　任意の WLAN 上で WMM が 有効になっており、レイヤ 2 LWAPP モードに設定されている場合、アクセス ポイントは、WMM クライアントの QoS 制御フィールドに基づく VLAN ID 0 を使用して、802.1q PRI フィールドにあるそのアクセス ポイントの優先度情報を送信します。レイヤ 3 LWAPP モードでは、この情報は LWAPP パケットの IP ヘッダの DSCP で伝達されます。アクセス ポイントを接続するシスコ以外のアクセス スイッチの中には、VLAN タグの ID 0 を適切に処理しないものもあります。たとえば、そのようなスイッチは、VLAN ID 0 のタグを付けられたパケットをドロップする可能性があり、WMM 有効のアクセス ポイントが レイヤ 2 LWAPP モードでコントローラに接続できなくなり、繰り返しリブートする原因となります。したがって、コントローラがレイヤ 2 モードに設定されていて、かつ WMM が有効な場合は、コントローラに接続できるようにアクセス ポイントをスイッチのトランク ポート上に設置する必要があります。スイッチのトランク ポートへの接続後にアクセス ポイントからコントローラへ接続できない場合は、WMM を使用するためにレイヤ 3 LWAPP モードでコントローラを使用する必要があります。

ステップ 5　アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、**7920 AP CAC** チェックボックスをオンにします。デフォルトではオフになっています。

ステップ 6　クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、**7920 Client CAC** チェックボックスをオンにします。デフォルトではオフになっています。

（注）　WLAN 上で、WMM モードおよびクライアントで制御される CAC モードの両方を有効にすることはできません。

ステップ 7　**Apply** をクリックして、変更を適用します。

ステップ 8　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した QBSS の設定

コントローラの CLI を使用して QBSS を設定する手順は、次のとおりです。

ステップ 1　QBSS サポートを追加する WLAN の ID 番号を決定するには、次のコマンドを入力します。

show wlan summary

ステップ 2　WLAN を無効するには、次のコマンドを入力します。

config wlan disable *wlan_id*

ステップ 3　7921 電話および WMM 規格を満たすその他のデバイスで WMM モードを設定するには、次のコマンドを入力します。

config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

このとき、次のようになります。

- **disabled** パラメータは、WLAN 上で WMM モードを無効にします。
- **allowed** パラメータは、WLAN 上でクライアント デバイスに WMM の使用を許可します。
- **required** パラメータは、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。

（注）　任意の WLAN 上で WMM が 有効になっており、レイヤ 2 LWAPP モードに設定されている場合、アクセス ポイントは、WMM クライアントの QoS 制御フィールドに基づく VLAN ID 0 を使用して、802.1q PRI フィールドにあるそのアクセス ポイントの優先度情報を送信します。レイヤ 3 LWAPP モードでは、この情報は LWAPP パケットの IP ヘッダの DSCP で伝達されます。アクセス ポイントを接続するシスコ以外のアクセス スイッチの中には、VLAN タグの ID 0 を適切に処理しないものもあります。たとえば、そのようなスイッチは、VLAN ID 0 のタグを付けられたパケットをドロップする可能性があり、WMM 有効のアクセス ポイントが レイヤ 2 LWAPP モードでコントローラに接続できなくなり、繰り返しリブートする原因となります。したがって、コントローラがレイヤ 2 モードに設定されていて、かつ WMM が有効な場合は、コントローラに接続できるようにアクセス ポイントをスイッチのトランク ポート上に設置する必要があります。スイッチのトランク ポートへの接続後にアクセス ポイントからコントローラへ接続できない場合は、WMM を使用するためにレイヤ 3 LWAPP モードでコントローラを使用する必要があります。

ステップ 4　クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

config wlan 7920-support client-cac-limit {**enable** | **disable**} *wlan_id*

（注）　WLAN 上で、WMM モードおよびクライアントで制御される CAC モードの両方を有効にすることはできません。

ステップ 5　アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

ステップ 6　WLAN を再度有効にするには、次のコマンドを入力します。

config wlan enable *wlan_id*

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　WLAN が有効にされており、かつ Dot11-Phone Mode (7920) フィールドが互換モードに設定されていることを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

IPv6 ブリッジの設定

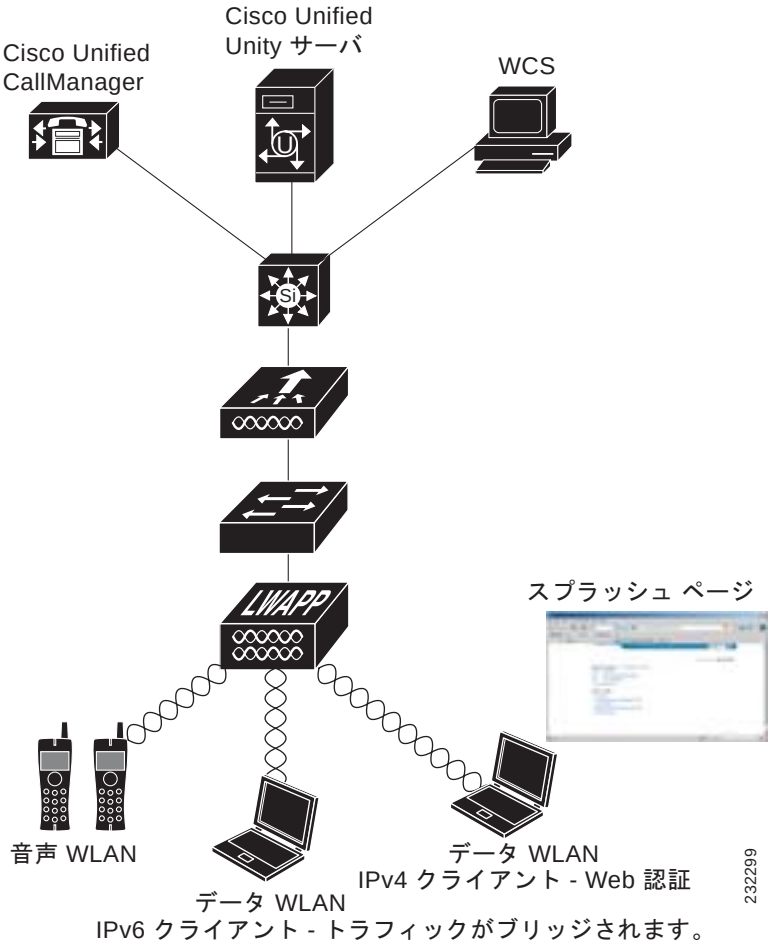
インターネット プロトコル バージョン 6（IPv6）は、プロトコルの TCP/IP スイートのバージョン 4（IPv4）の後継となることを意図された次世代のネットワーク レイヤ インターネット プロトコルです。この新しいバージョンでは、一意なグローバル IP アドレスを必要とするユーザとアプリケーションを収容するためのインターネット グローバル アドレス空間が拡張されています。IPv6 は、128 ビットの発信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。コントローラの GUI または CLI のいずれかを使用して、WLAN を IPv6 ブリッジ用に設定するには、この項の手順に従ってください。

IPv6 ブリッジを使用する際のガイドライン

IPv6 ブリッジを使用する場合には、次のガイドラインに従ってください。

- IPv6 ブリッジは、次のコントローラでのみサポートされます。4400 シリーズのコントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチ。
- IPv6 ブリッジを有効にするには、レイヤ 3 セキュリティが *None* に設定されている必要があります。
- 中央スイッチングを使用する Hybrid REAP は IPv6 ブリッジとの共用がサポートされています。ローカル スイッチングを使用する Hybrid REAP はサポートされていません。
- 自動アンカー モビリティは、IPv6 ブリッジと共には使用できません。
- シンメトリック モビリティ トンネリングが有効にされている場合は、クライアントとの間のすべての IPv4 トラフィックは双方向でトンネルされますが、IPv6 クライアント トラフィックはローカルでブリッジされます。
- コントローラ ソフトウェア リリース 4.2 以降では、同じ WLAN 上で IPv6 ブリッジと IPv4 Web 認証を有効にできます。この組み合わせは、以前はサポートされていませんでした。コントローラは WLAN 上のすべてのクライアントからの IPv6 トラフィックをブリッジするのに対し、IPv4 トラフィックは通常の Web 認証プロセスを経由します。コントローラは、IPv4 クライアントの Web 認証が完了する前でも、クライアントがアソシエートするとすぐに IPv6 のブリッジを開始します。IPv6 ブリッジおよび Web 認証が有効にされている場合に、WLAN 上でその他のレイヤ 2 またはレイヤ 3 セキュリティ ポリシー設定はサポートされません。図 6-13 は、IPv6 ブリッジおよび IPv4 Web 認証が同じ WLAN 上で使用される方法を示しています。

図 6-13　IPv6 ブリッジおよび IPv4 Web 認証



（注） コントローラの GUI と CLI の両方にある Security Policy Completed フィールドには、Web 認証が完了するまで、「No for IPv4 (bridging allowed for IPv6)」と表示されます。このフィールドは、GUI の Clients > Detail ページまたは **show client detail** CLI コマンドを使用して表示できます。

GUI を使用した IPv6 ブリッジの設定

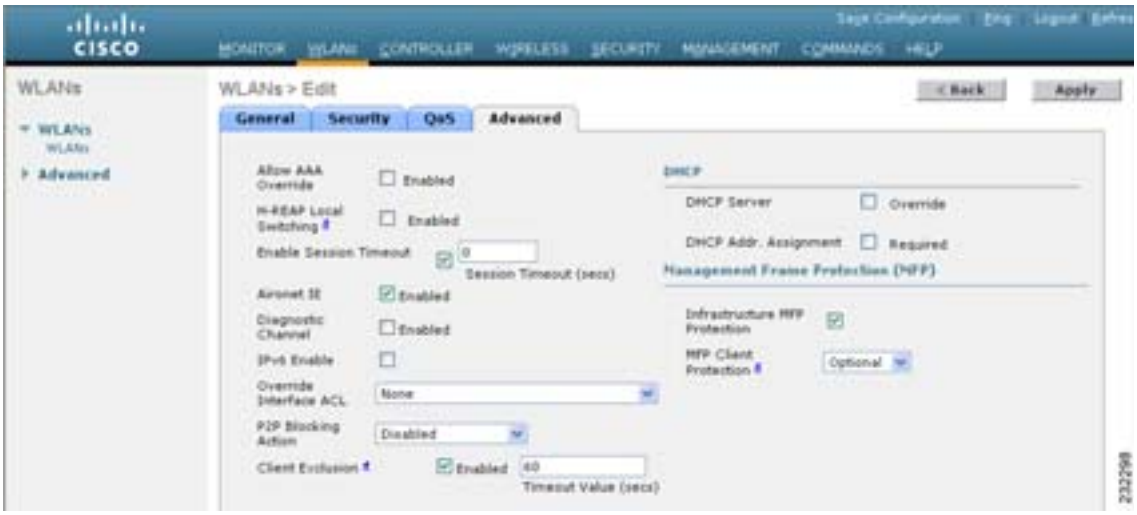
GUI を使用して WLAN の IPv6 ブリッジを設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Advanced** タブをクリックして、WLANs > Edit（Advanced tab）ページを開きます（図 6-14 を参照）。

図 6-14　WLANs > Edit（Advanced）ページ



ステップ 4　この WLAN に接続するクライアントで、IPv6 パケットを受け入れるようにする場合は、**IPv6 Enable** チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフのままにします（デフォルト値）。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

CLI を使用した IPv6 ブリッジの設定

CLI を使用して WLAN の IPv6 ブリッジを設定するには、次のコマンドを入力します。

config wlan IPv6support {**enable** | **disable**} *wlan_id*

デフォルト値は無効です。

Cisco Client Extensions の設定

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードバーティ製クライアント デバイスは、シスコ製のアクセス ポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、迅速なローミング、優れた電源管理などの、他のクライアント デバイスがサポートしていないシスコの機能もサポートできるようになります。

コントローラ ソフトウェアのリリース 4.2 以降では、CCX バージョン 1 ～ 5 をサポートしています。これにより、コントローラおよびそのアクセス ポイントは、CCX をサポートするサードパーティ製のクライアント デバイスと無線で通信できるようになります。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。ただし、WLAN ごとに特定の CCX の機能を設定することができます。この機能は、Aironet 情報要素（IE）です。

Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの番号などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラは、Aironet IEs 0x85 および 0x95（コントローラの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション要求に格納して送信します。

GUI または CLI のいずれかを使用して CCX Aironet IE 機能を使用するように WLAN を設定したり、特定のクライアント デバイスでサポートされる CCX のバージョンを確認するには、この項の手順に従ってください。

（注） CCX は、AP1030 ではサポートされません。

GUI を使用した CCX Aironet IE の設定

GUI を使用して WLAN の CCX Aironet IE を設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックして、WLANs > Edit ページを開きます。

ステップ 3　**Advanced** タブをクリックして、WLANs > Edit（Advanced tab）ページを開きます（図 6-14 を参照）。

ステップ 4　この WLAN で Aironet IE のサポートを有効にする場合は、**Aironet IE** チェックボックスをオンにします。有効にしない場合には、このチェックボックスをオフにします。デフォルト値は、有効になっています（オンになっています）。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

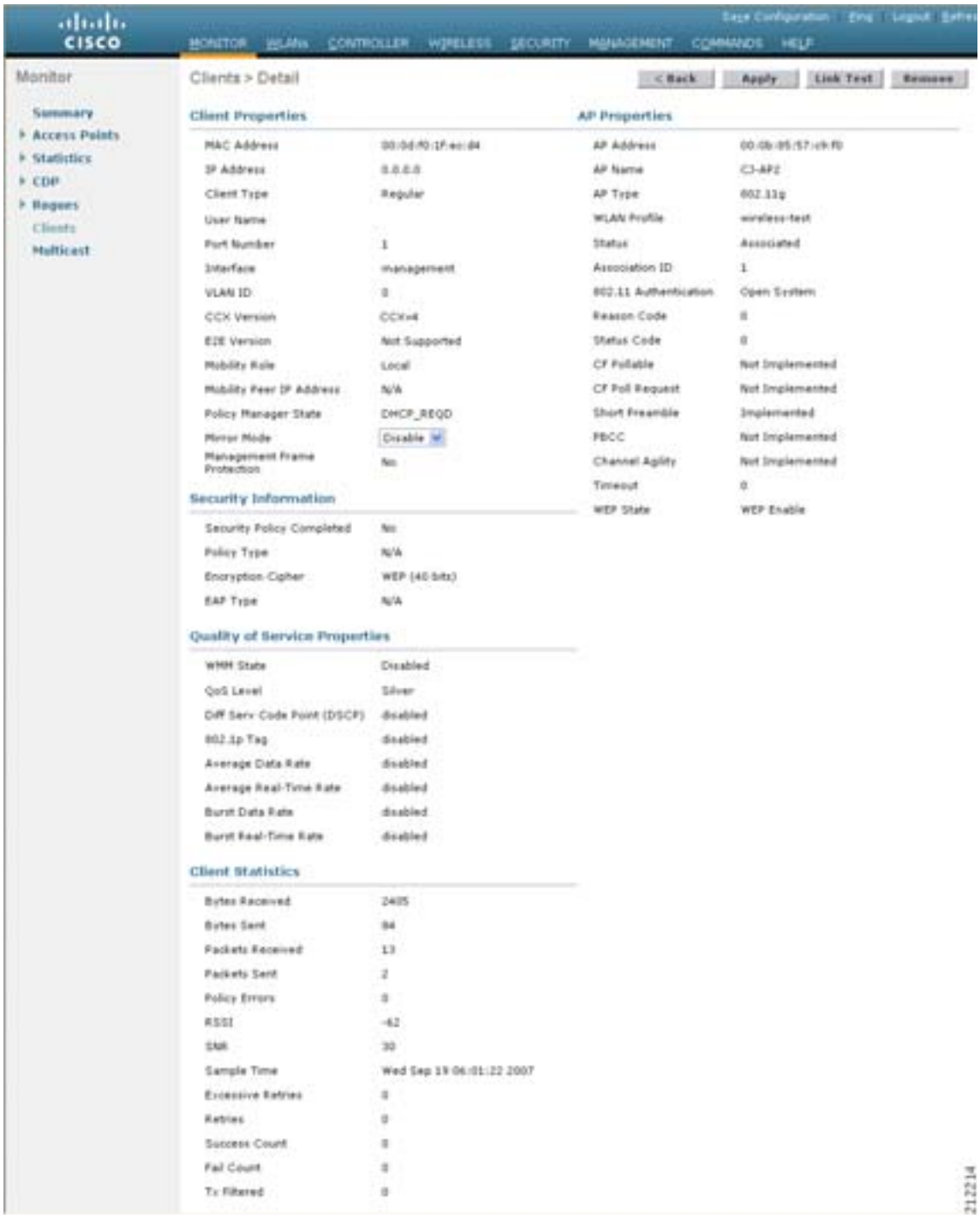
GUI を使用したクライアントの CCX バージョンの表示

クライアント デバイスは、アソシエーション要求パケットに CCX バージョンを格納してアクセス ポイントに送信します。コントローラは、クライアントの CCX バージョンをデータベースに格納し、これを使用してこのクライアントの機能を制限します。たとえば、クライアントが CCX バージョン 2 をサポートしている場合、コントローラは、CCX バージョン 4 の機能を使用することをクライアントに許可しません。GUI を使用して特定のクライアント デバイスでサポートされている CCX バージョンを表示する手順は、次のとおりです。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます。

ステップ 2　必要なクライアント デバイスの MAC アドレスをクリックして、Clients > Detail ページを開きます（図 6-15 を参照）。

図 6-15　Clients > Detail ページ



CCX Version に、このクライアント デバイスでサポートされる CCX バージョンが表示されます。クライアントで CCX がサポートされていない場合は、*Not Supported* が表示されます。

ステップ 3　前の画面に戻るには、**Back** をクリックします。

ステップ 4　他のクライアント デバイスでサポートされる CCX バージョンを表示するには、この手順を繰り返します。

CLI を使用した CCX Aironet IE の設定

特定の WLAN の Aironet IE のサポートを有効または無効にするには、次のコマンドを入力します。

config wlan ccx aironet-ie {**enable** | **disable**} *wlan_id*

デフォルト値は有効（enable）です。

CLI を使用したクライアントの CCX バージョンの表示

特定のクライアント デバイスでサポートされる CCX バージョンを表示するには、次のコマンドを入力します。

show client detail *client_mac*

WLAN オーバーライドの設定

デフォルトで、アクセス ポイントはコントローラ上のすべての定義済みの WLAN を送信します。ただし、WLAN オーバーライド オプションを使用して、送信される WLAN、およびアクセス ポイントごとに設定しない WLAN を選択できます。たとえば、WLAN オーバーライドを使用して、ゲスト WLAN がネットワークのどこで送信するかを制御できます。また、ネットワークの一定のエリアで特定の WLAN を無効にするためにも使用できます。

GUI を使用した WLAN オーバーライドの設定

特定のアクセス ポイントの WLAN オーバーライド オプションを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **Radios** > **802.11a/n** または **802.11b/g** の順にクリックして、802.11a/n（または 802.11b/g）Radios ページを開きます。

ステップ 2　カーソルを目的のアクセス ポイントの青のドロップダウン矢印の上に置いて、**Configure** を選択します。802.11a/n（または 802.11b/g）Cisco APs > Configure ページが表示されます（図 6-16 を参照）。

図 6-16　802.11a/n Cisco APs > Configure ページ

ステップ 3　WLAN Override ドロップダウン ボックスから **Enable** を選択して、このアクセス ポイントの WLAN オーバーライド機能を有効にするか、**Disable** を選択してこの機能を無効にします。

ステップ 4　ステップ 3 で WLAN オーバーライド機能を有効にした場合、アクセス ポイントでブロードキャストする WLAN のチェックボックスをオンにします。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

CLI を使用した WLAN オーバーライドの設定

コントローラの CLI を使用して特定のアクセス ポイントの WLAN オーバーライド機能を設定するには、次のコマンドを使用します。

1. 特定のアクセス ポイントで WLAN オーバーライド機能を有効または無効にするには、次のコマンドを入力します。

   config ap wlan {**enable** | **disable**} {**802.11a** | **802.11b**} *Cisco_AP*

2. 送信する WLAN を定義するには、次のコマンドを入力します。

   config ap wlan add {**802.11a** | **802.11b**} *wlan_id Cisco_AP*

アクセス ポイント グループの設定

一般的な展開では、WLAN 上のすべてのユーザはコントローラ上の 1 つのインターフェイスにマップされます。したがって、その WLAN にアソシエートされたすべてのユーザは、同じサブネットまたは VLAN 上にあります。ただし、複数のインターフェイス間で負荷を分散するか、*アクセス ポイント グループ*（以前は *サイト特定の VLAN* と呼ばれていました）を作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループ ユーザへと負荷を分配するために、このデフォルトの WLAN 設定を無効にできます。さらに、図 6-17 の例で示すように、ネットワーク管理を簡素化するために、これらのアクセス ポイント グループを別個の VLAN で設定できます。

（注）　VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト（ACL）を定義する必要があります。

（注）　アクセス ポイント グループ VLAN 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。ただし、クライアントがあるアクセス ポイントから別のアクセス ポイントにローミングする場合、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

図 6-17　アクセス ポイント グループ

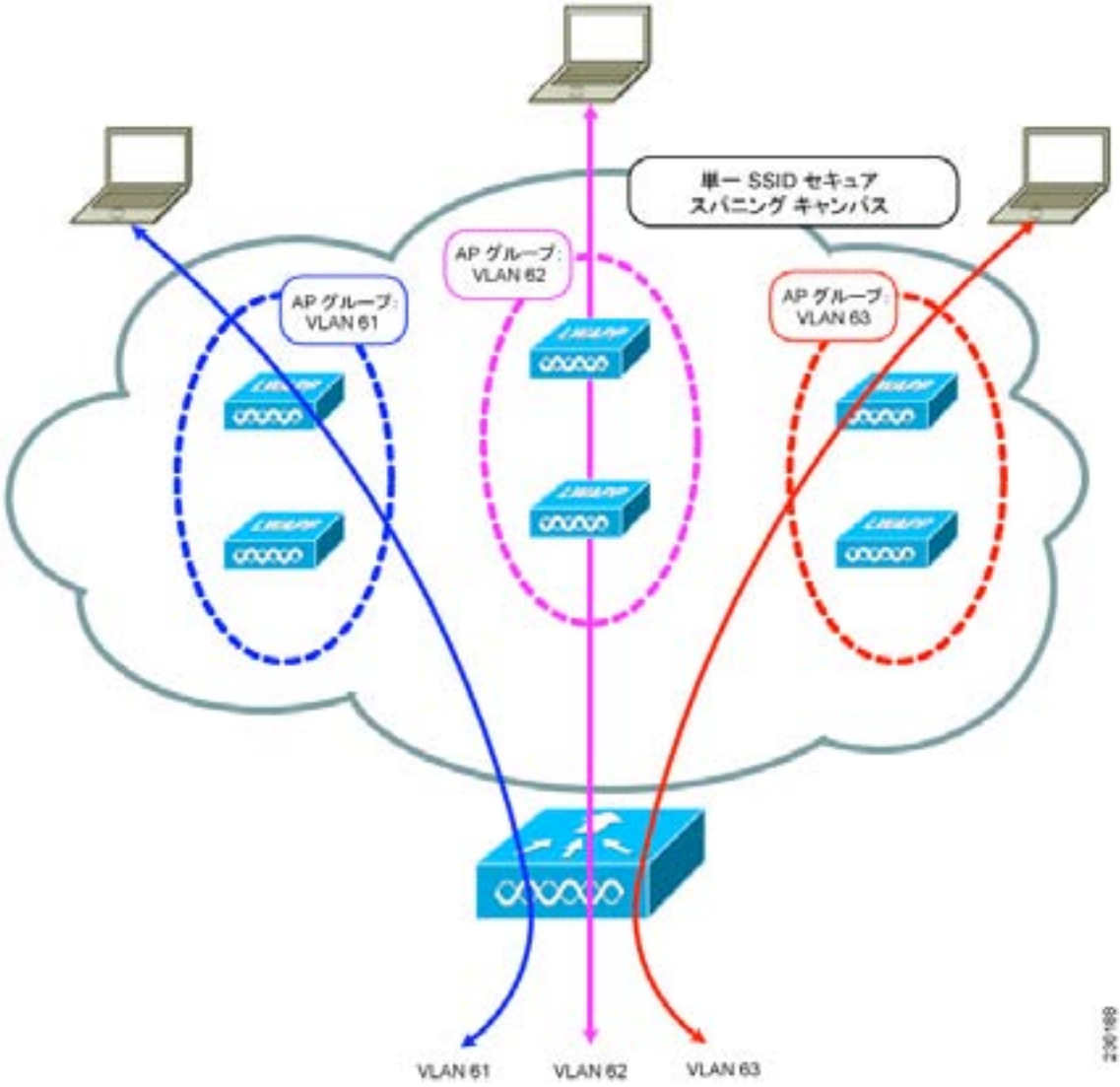


図 6-17 では、3 つの設定された動的インターフェイスが、3 つの異なる VLAN（VLAN 61、VLAN 62、および VLAN 63）にマップされています。3 つのアクセス ポイント グループが定義されており、各グループは異なる VLAN のメンバですが、すべてのグループが同じ SSID のメンバとなっています。無線 SSID 内のクライアントには、そのアクセス ポイントがメンバとなっている VLAN サブネットから IP アドレスが割り当てられています。たとえば、アクセス ポイント グループ VLAN 61 のメンバであるアクセス ポイントにアソシエートする任意のユーザには、そのサブネットから IP アドレスが割り当てられます。

図 6-17 の例では、コントローラはアクセス ポイント間のローミングをレイヤ 3 ローミング イベントとして内部で処理します。こうすることで、WLAN クライアントは元の IP アドレスを保持します。

アクセス ポイント グループを設定するには、次のトップレベルの手順に従います。

1. 適切な動的インターフェイスを設定し、必要な VLAN にマップします。

   たとえば、図 6-17 でネットワークを実装するには、コントローラ上で VLAN 61、62、および 63 に対する動的インターフェイスを作成します。動的インターフェイスの構成方法の詳細は、第 3 章を参照してください。

2. アクセス ポイント グループを作成します。「アクセス ポイント グループの作成」の項（P. 6-43）を参照してください。

3. 適切なアクセス ポイント グループにアクセス ポイントを割り当てます。「アクセス ポイントのアクセス ポイント グループへの割り当て」の項（P. 6-45）を参照してください。

アクセス ポイント グループの作成

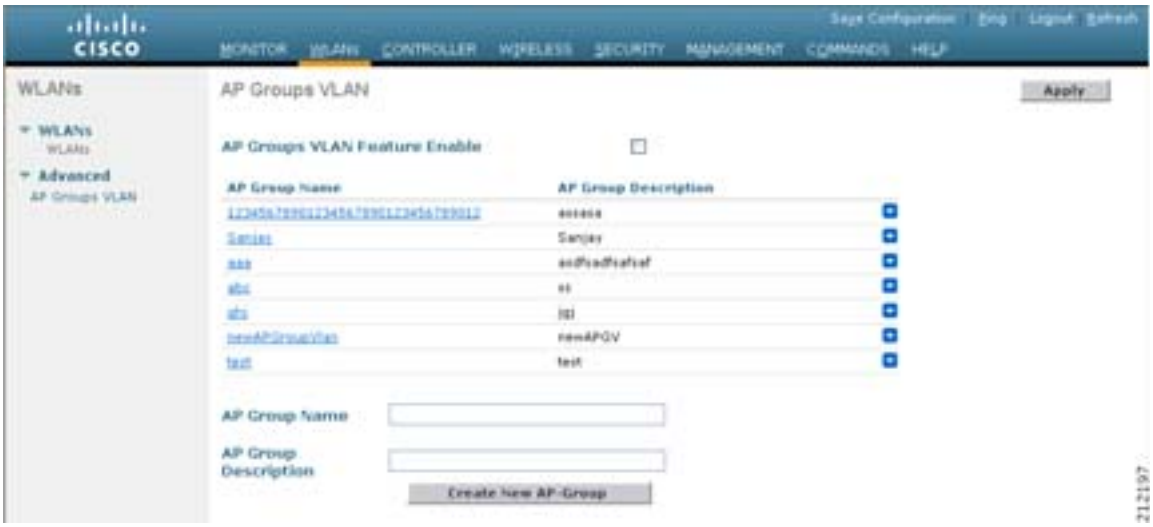
すべてのアクセス ポイントがコントローラに接続された後は、アクセス ポイント グループを作成して、各グループを 1 つまたは複数の WLAN に割り当てることができます。また、WLAN とインターフェイスのマッピングを定義する必要があります。

GUI を使用したアクセス ポイント グループの作成

コントローラ GUI を使用してアクセス ポイント グループを作成する手順は、次のとおりです。

ステップ 1　**WLANs** > **Advanced** > **AP Groups VLAN** の順にクリックして、AP Groups VLAN ページを開きます（図 6-18 を参照）。

図 6-18　AP Groups VLAN ページ



ステップ 2　**AP Groups VLAN Feature Enable** チェックボックスをオンにしてこの機能を有効にします。デフォルトではオフになっています。

ステップ 3　AP Group Name フィールドに、グループの名前を入力します。

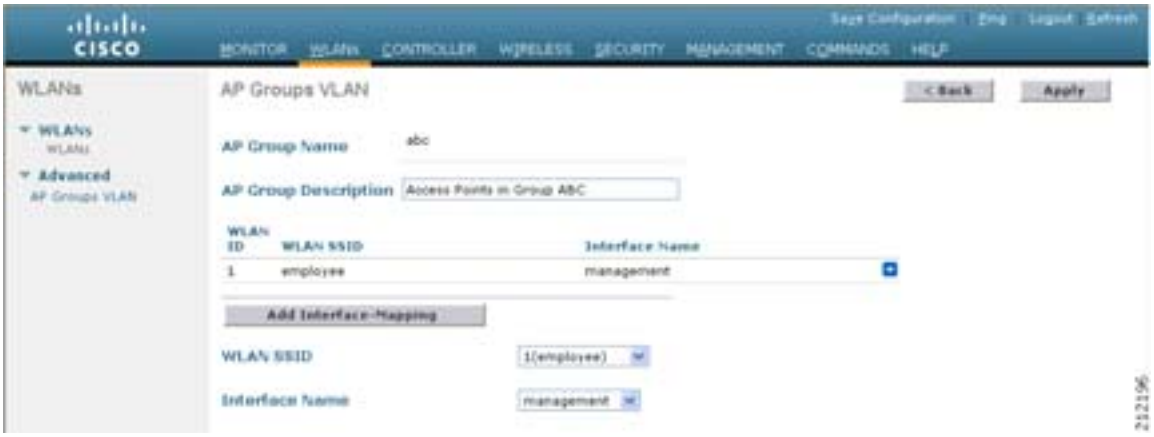
ステップ 4　AP Group Description フィールドに、グループの説明を入力します。

ステップ 5　**Create New AP-Group** をクリックしてグループを作成します。新しく作成されたアクセス ポイント グループがページの中央に表示されます。

（注）　このグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 6　この新しいグループを編集するには、グループの名前をクリックします。異なるフィールドを含む AP Groups VLAN ページが再度表示されます（図 6-19 を参照）。

図 6-19　AP Groups VLAN ページ



ステップ 7　アクセス ポイント グループを WLAN にマップするには、WLAN SSID ドロップダウン ボックスからその ID を選択します。

ステップ 8　アクセス ポイント グループをインターフェイスにマップするには、Interface Name ドロップダウン ボックスから必要なインターフェイスを選択します。

ステップ 9　**Add Interface-Mapping** をクリックして、WLAN とインターフェイスのマッピングをグループに追加します。新しく作成されたインターフェイスのマッピングがページの中央に表示されます。

（注）　このマッピングを削除するには、そのマッピングの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 10　さらにインターフェイス マッピングを追加するには、ステップ 7 ～ ステップ 9 を繰り返します。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　さらにアクセス ポイント グループを追加するには、ステップ 3 ～ ステップ 11 を繰り返します。

ステップ 13　**Save Configuration** をクリックして、変更を保存します。

CLI を使用したアクセス ポイント グループの作成

CLI を使用してアクセス ポイント グループを作成するには、次のコマンドを入力します。

config ap group-name *group_name*

アクセス ポイントのアクセス ポイント グループへの割り当て

アクセス ポイント グループを作成した後、コントローラ GUI または CLI を使用して、アクセス ポイントをこれらのグループに割り当てます。

GUI を使用したアクセス ポイントのアクセス ポイント グループへの割り当て

GUI を使用してアクセス ポイントをアクセス ポイント グループに割り当てる手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。

ステップ 2　グループを割り当てるアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます。

ステップ 3　**Advanced** タブをクリックして、All APs > Details（Advanced）ページを開きます（図 6-20 を参照）。

図 6-20　All APs > Details (Advanced) ページ

ステップ 4　AP Group Name ドロップダウン ボックスから必要なアクセス ポイント グループを選択します。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用したアクセス ポイントのアクセス ポイント グループへの割り当て

CLI を使用してアクセス ポイントをアクセス ポイント グループに割り当てるには、次のコマンドを入力します。

config ap group-name *group_name ap_name*

802.1X 認証を使用した Web リダイレクトの設定

802.1X 認証が正常に完了した後に、ユーザを特定の Web ページにリダイレクトするように WLAN を設定できます。Web リダイレクトを設定して、ユーザにネットワークへの部分的または全面的なアクセス権を与えることができます。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。RADIUS サーバー上で、リダイレクト先のページとリダイレクトが発生する条件を指定できます。条件には、ユーザのパスワードの有効期限が近づいている場合、または使用を継続するためにユーザが料金を支払う必要がある場合などがあります。

RADIUS サーバが Cisco AV-pair "url-redirect" を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。サーバが Cisco AV-pair "url-redirect-acl" も返す場合は、指定されたアクセス コントロール リスト（ACL）が、このクライアントの事前認証 ACL としてインストールされています。クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。

指定された URL （たとえば、パスワードの変更、請求書の支払い）でクライアントが特定の操作を完了すると、クライアントの再認証が必要になります。RADIUS サーバが "url-redirect" を返さない場合、クライアントは完全に認証されたと見なされ、トラフィックの送信が許可されます。

（注） 条件付き Web リダイレクト機能は、802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上で条件付き Web リダイレクトを設定できます。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークに完全にアクセスできます。RADIUS サーバでリダイレクト ページを指定できます。RADIUS サーバが Cisco AV-pair "url-redirect" を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。クライアントは、この段階で完全に認証され、RADIUS サーバが "url-redirect" を返さなくても、トラフィックを渡すことができます。

（注） スプラッシュ ページ Web リダイレクト機能は、802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上でスプラッシュ ページ Web リダイレクトを設定できます。

RADIUS サーバの設定

RADIUS サーバを設定する手順は、次のとおりです。

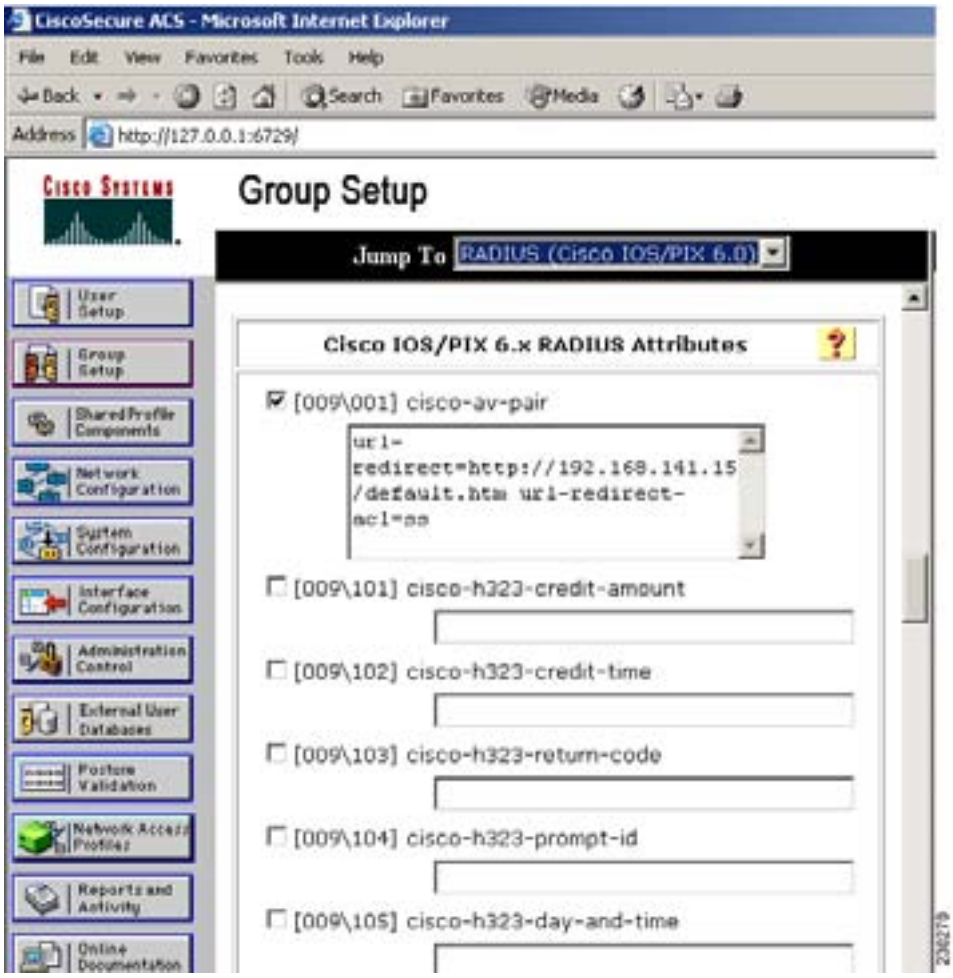
（注） 次の手順は、CiscoSecure ACS 固有の手順ですが、その他の RADIUS サーバでも同様の手順を使用します。

ステップ 1　CiscoSecure ACS メイン メニューから、**Group Setup** をクリックします。

ステップ 2　**Edit Settings** をクリックします。

ステップ 3　Jump To ドロップダウン ボックスから **RADIUS (Cisco IOS/PIX 6.0)** を選択します。図 6-21 に示すウィンドウが表示されます。

図 6-21　ACS サーバの設定



ステップ 4　**[009\001] cisco-av-pair** チェックボックスをオンにします。

ステップ 5　[009\001] cisco-av-pair 編集ボックスに次の Cisco AV ペアを入力して、ユーザをリダイレクトする URL を指定するか、条件付 Web リダイレクトを設定する場合は、ダイレクトが発生する条件をそれぞれ指定します。

url-redirect=http://*url*

url-redirect-acl=*acl_name*

GUI を使用した Web リダイレクトの設定

コントローラの GUI を使用して条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを設定する手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　必要な WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。

ステップ 3　**Security** タブおよび **Layer 2** タブをクリックして、WLANs > Edit（Security > Layer 2）ページを開きます。

ステップ 4　Layer 2 Security ドロップダウン ボックスから **802.1X** または **WPA+WPA2** を選択します。

ステップ 5　802.1X または WPA+WPA に対して任意の追加パラメータを設定します。

ステップ 6　**Layer 3** タブをクリックして、WLANs > Edit（Security > Layer 3）ページを開きます（図 6-22 を参照）。

図 6-22　WLANs > Edit（Security > Layer 3）ページ

ステップ 7　Layer 3 Security ドロップダウン ボックスから **None** を選択します。

ステップ 8　**Web Policy** チェックボックスをオンにします。

ステップ 9　条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを有効化するオプションとして、**Conditional Web Redirect** または **Splash Page Web Redirect** のいずれかを選択します。デフォルトでは、両方のパラメータが無効になっています。

ステップ 10　ユーザをコントローラ外部のサイトにリダイレクトする場合、Preauthentication ACL ドロップダウン リストから RADIUS サーバ上で設定された ACL を選択します。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した Web リダイレクトの設定

コントローラの CLI を使用して条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを設定する手順は、次のとおりです。

ステップ 1　条件付き Web リダイレクトを有効または無効にするには、次のコマンドを入力します。

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

ステップ 2　スプラッシュ ページ Web リダイレクトを有効または無効にするには、次のコマンドを入力します。

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

ステップ 3　設定を保存するには、次のコマンドを入力します。

save config

ステップ 4　特定の WLAN の Web リダイレクト機能の状態を表示するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
...
```

WLAN ごとのアカウンティング サーバの無効化

この項では、WLAN 上のすべてのアカウンティング サーバを無効にする手順について説明します。アカウンティング サーバを無効にすると、すべてのアカウンティング動作が無効となり、コントローラが WLAN に対するデフォルトの RADIUS サーバにフォールバックしなくなります。

RADIUS 認証サーバのすべてのアカウンティング サーバを無効にする手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　変更する WLAN のプロファイル名をクリックします。WLANs > Edit ページが表示されます。

ステップ 3　**Security** タブおよび **AAA Servers** タブをクリックして、WLANs > Edit（Security > AAA Servers）ページを開きます（図 6-23 を参照）。

図 6-23　WLANs > Edit（Security > AAA Servers）ページ

ステップ 4　Accounting Servers の **Enabled** チェックボックスをオフにします。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

CHAPTER 7

Lightweight アクセス ポイントの制御

この章では、Cisco Lightweight アクセス ポイントをコントローラに接続する方法、およびアクセス ポイントの設定を管理する方法について説明します。この章の内容は、次のとおりです。

コントローラ ディスカバリのプロセス

Cisco Lightweight アクセス ポイントは、Lightweight アクセス ポイント プロトコル（LWAPP）を使用して、コントローラとネットワーク上にある別の Lightweight アクセス ポイントとの間の通信を行います。LWAPP の環境では、LWAPP ディスカバリ メカニズムによりコントローラが検出され、そのコントローラに LWAPP 接続要求が送信されます。コントローラは、アクセス ポイントに LWAPP 接続応答を送信してアクセス ポイントにコントローラへの接続を許可します。アクセス ポイントがコントローラに接続する際、設定、ファームウェア、コントロール トランザクション、およびデータ トランザクションはコントローラが管理します。

（注） 1100 および 1300 シリーズ アクセス ポイントをコントローラに接続する前に、ソフトウェア リリース 4.0.155.0 以上をコントローラにインストールする必要があります。1120 および 1310 アクセス ポイントは、ソフトウェア リリース 4.0.155.0 以前ではサポートされていません。

（注） アクセス ポイント名にスペースが含まれていると、Cisco コントローラで CLI を使用してアクセス ポイントの情報を編集または検索できません。

（注） コントローラが現在時刻に設定されていることを確認します。コントローラの時計が遅れている場合、アクセス ポイントをコントローラに接続できないことがあります。これはその時刻の証明書が有効ではない可能性があるからです。

コントローラは Lightweight アクセス ポイントがネットワーク上でアクティブになる前に検出する必要があります。Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。

- **Layer 3 LWAPP ディスカバリ**：アクセス ポイントとは異なるサブネット上で行われ、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。
- **Layer 2 LWAPP ディスカバリ**：アクセス ポイントと同一のサブネット上で行われ、アクセス ポイントとコントローラ間の通信用 MAC アドレスを持つカプセル化されたイーサネット フレームが使用されます。レイヤ 2 LWAPP ディスカバリは、レイヤ 3 の環境には適しません。
- **Over-the-air provisioning（OTAP）**：この機能は Cisco 4400 シリーズ コントローラでサポートされています。この機能がコントローラで有効になっている場合、アソシエートされたすべてのアクセス ポイントが無線 LWAPP ネイバー メッセージを送信し、新しいアクセス ポイントがこれらのメッセージからコントローラの IP アドレスを受信します。この機能はデフォルトでは無効になっています。すべてのアクセス ポイントをインストールする際には無効のままにしておいてください。
- **ローカルに保存されているコントローラの IP アドレス ディスカバリ**：アクセス ポイントがすでにコントローラにアソシエートされている場合、プライマリ、セカンダリおよびターシャリ コントローラの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。コントローラの IP アドレスを今後の展開のためにアクセス ポイントに保存するこのプロセスは、*アクセス ポイントのプライミング*と呼ばれています。
- **DHCP サーバのディスカバリ**：この機能は DHCP オプション 43 を使用して、アクセス ポイントへのコントローラ IP アドレスを提供します。シスコ スイッチは、通常この機能に使用される DHCP サーバ オプションをサポートします。DHCP オプション 43 に関する詳細は、「DHCP オプション 43 の使用」の項（P. 7-14）を参照してください。

- **DNS ディスカバリ**：アクセス ポイントは、Domain Name Server（DNS; ドメイン ネーム サーバ）を介してコントローラを検出できます。アクセス ポイントがコントローラを検出するには、CISCO-LWAPP-CONTROLLER.*localdomain* への応答としてコントローラの IP アドレスを返すように DNS を設定する必要があります。この *localdomain* は、アクセス ポイントのドメイン名です。アクセス ポイントは DHCP サーバから IP アドレスと DNS 情報を受け取ると、DNS に問い合わせて CISCO-LWAPP-CONTROLLER.*localdomain* を解決します。DNS がコントローラ IP アドレスのリストを送信すると、アクセス ポイントはディスカバリ要求をコントローラに送信します。

アクセス ポイントのコントローラへの接続の確認

コントローラを交換する場合、アクセス ポイントが新しいコントローラに接続していることを確認する必要があります。

GUI を使用したアクセス ポイントのコントローラへの接続の確認

アクセス ポイントが新しいコントローラに接続していることを確認する手順は、次のとおりです。

ステップ 1　次の手順に従って、新しいコントローラをマスター コントローラとして設定します。

a. **Controller** > **Advanced** > **Master Controller Mode** の順にクリックし、Master Controller Configuration ページを開きます。

b. **Master Controller Mode** チェックボックスをオンにします。

c. **Apply** をクリックして、変更を適用します。

d. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 2　（オプション）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。この手順の詳細は、ネットワーク管理者に問い合わせてください。

ステップ 3　アクセス ポイントを再起動します。

ステップ 4　すべてのアクセス ポイントが新しいコントローラに接続された後で、そのコントローラがマスター コントローラとして機能しないように設定するには、Master Controller Configuration ページで **Master Controller Mode** チェックボックスをオフにします。

CLI を使用したアクセス ポイントのコントローラへの接続の確認

アクセス ポイントが新しいコントローラに接続していることを確認する手順は、次のとおりです。

ステップ 1　新しいコントローラをマスター コントローラとして設定するには、次のコマンドを入力します。

config network master-base enable

ステップ 2　（オプション）ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。この手順の詳細は、ネットワーク管理者に問い合わせてください。

ステップ 3　アクセス ポイントを再起動します。

ステップ 4　すべてのアクセス ポイントが新しいコントローラに接続された後で、そのコントローラがマスター コントローラとして機能しないように設定するには、次のコマンドを入力します。

config network master-base disable

アクセス ポイントのグローバル資格情報の設定

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトのイネーブル パスワード *Cisco* が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、**show** および **debug** コマンドを実行することができますが、これはセキュリティに対する脅威です。不正アクセスを防止し、ユーザがアクセス ポイントのコンソール ポートから設定コマンドを実行できるようにするには、デフォルトのイネーブル パスワードを変更する必要があります。

5.0 以前のコントローラ ソフトウェア リリースでは、現在、コントローラに接続されているアクセス ポイントについてのみ、アクセス ポイント イネーブル パスワードを設定できます。コントローラ ソフトウェア リリース 5.0 では、グローバル ユーザ名、パスワード、およびイネーブル パスワードを設定し、アクセス ポイントがコントローラに接続するときに継承させることができます。これには、コントローラに現在接続されているすべてのアクセス ポイントおよび今後接続されるすべてのアクセス ポインがすべて含まれます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブル パスワードを特定のアクセス ポイントに割り当てることができます。

また、コントローラ ソフトウェア リリース 5.0 では、アクセス ポイントをコントローラに接続した後で、アクセス ポイントによりコンソール ポートのセキュリティが有効化され、このアクセス ポイントのコンソール ポートにログインしようとすると、必ずユーザ名とパスワードを求めるプロンプトが表示されます。ログインすると、非特権モードに入るので、特権モードを使用するには、イネーブル パスワードを入力する必要があります。

（注）　コントローラ ソフトウェア リリース 5.0 のこれらの機能は、1100 シリーズを除く、Lightweight モードに変換されたアクセス ポイントすべてでサポートされています。VxWorks アクセス ポイントはサポートされていません。

コントローラで設定したグローバル資格情報はコントローラやアクセス ポイントをリブートした後でも保持されます。この情報が上書きされるのは、アクセス ポイントを、グローバル ユーザ名およびパスワードが設定された新しいコントローラに接続した場合のみです。グローバル資格情報を使って新しいコントローラを設定しなかった場合、このアクセス ポイントは最初のコントローラに設定されているグローバル ユーザ名とパスワードをそのまま保持します。

（注）　アクセス ポイントにより使用される資格情報は常に把握している必要があります。そうしないと、アクセス ポイントのコンソール ポートにログインできなくなることがあります。必要に応じて、アクセス ポイント設定をクリアして、アクセス ポイントのユーザ名とパスワードをデフォルト設定に戻すこともできます。

GUI 設定ウィザードを使用して、コントローラ ソフトウェアをリリース 5.0 にアップグレードすると、コントローラへの接続時にアクセス ポイントによって継承されるグローバル資格情報を設定するためのプロンプトが表示されます。コントローラの GUI または CLI を使用してこの設定を行うには、以下の項のいずれかに記載されている手順に従ってください。

GUI を使用した、アクセス ポイントのグローバル資格情報の設定

コントローラの GUI を使用して、コントローラに接続するアクセス ポイントのグローバル資格情報を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **AP Configuration** > **AP Credentials** の順にクリックして、AP Configuration > AP Credentials ページを開きます（図 7-1 を参照）。

図 7-1　AP Configuration > AP Credentials ページ

ステップ 2　Username フィールドに、コントローラに接続するすべてのアクセス ポイントによって継承されるユーザ名を入力します。

ステップ 3　Password フィールドに、コントローラに接続するすべてのアクセス ポイントによって継承されるパスワードを入力します。

ステップ 4　Enable Password フィールドに、コントローラに接続するすべてのアクセス ポインによって継承されるイネーブル パスワードを入力します。

ステップ 5　**Apply to All APs** をクリックして、グローバル ユーザ名、パスワード、およびイネーブル パスワードを、コントローラに現在接続されているアクセス ポイント、および今後接続されるすべてのアクセス ポイントに送信します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 7　必要に応じて、特定のアクセス　ポイントに対するグローバル資格情報を無効にし、このアクセス ポイントに独自のユーザ名、パスワード、およびイネーブル パスワードを割り当てることを選択できます。手順は次のとおりです。

a. **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。

b. グローバル資格情報を無効にするアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます（図 7-2 を参照）。

図 7-2　All APs > Details ページ

c. AP Credentials の下にある **Override Global Credentials** チェックボックスをオンにし、このアクセス ポイントがコントローラからグローバル ユーザ名、パスワード、イネーブル パスワードを継承しないようにします。デフォルトではオフになっています。

d. Username、Password、および Enable Password フィールドに、このアクセス ポイントに割り当てる一意のユーザ名、パスワード、およびイネーブル パスワードを入力します。

（注） 入力した情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

e. **Apply** をクリックして、変更を適用します。

f. **Save Configuration** をクリックして、変更内容を保存します。

（注） このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、**Override Global Credentials** チェックボックスをオフにします。

CLI を使用した、アクセス ポイントのグローバル資格情報の設定

コントローラの CLI を使用して、コントローラに接続するアクセス ポイントのグローバル資格情報を設定する手順は、次のとおりです。

ステップ 1　コントローラに現在接続されているアクセス　ポイント、および今後接続されるすべてのアクセス ポイントについて、グローバル ユーザ名、パスワード、およびイネーブル パスワードを設定するには、次のコマンドを入力します。

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

ステップ 2　必要に応じて、特定のアクセス　ポイントに対するグローバル資格情報を無効にし、このアクセス ポイントに独自のユーザ名、パスワード、およびイネーブル パスワードを割り当てることを選択できます。そのためには、次のコマンドを入力します。

config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

このコマンドに入力した資格情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに接続された場合でも保持されます。

（注）　このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、次のコマンドを入力します。**config ap mgmtuser delete** *Cisco_AP* このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　コントローラに接続するすべてのアクセス ポイントに対して、グローバル資格情報が設定されていることを確認するには、次のコマンドを入力します。

show ap summary

次のような情報が表示されます。

```
Number of APs.................................... 1
Global AP User Name.............................. globalap

AP Name  Slots  AP Model           Ethernet MAC       Location         Port  Country
-------- ------ ------------------ ------------------ ------------------ ----
-------
HReap      2    AIR-AP1131AG-N-K9 00:13:80:60:48:3e  default location  1     US
```

（注）　グローバル資格情報が設定されていない場合、Global AP User Name フィールドには「Not Configured」と表示されます。

ステップ 5　特定のアクセス　ポイントのグローバル資格情報の設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

（注） アクセス ポイントの名前では、大文字と小文字が区別されます。

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... HReap
...
AP User Mode..................................... AUTOMATIC
AP User Name..................................... globalap
...
```

（注） AP User Mode フィールドには、グローバル資格証明を使用するようにこのアクセス ポイントが設定されている場合は「Automatic」と表示され、このアクセス ポイントに対してグローバル資格証明が無効にされている場合は「Customized」と表示されます。

Cisco Aironet メッシュ アクセス ポイント

コントローラ ソフトウェア リリース 5.0 は、Cisco Aironet メッシュ アクセス ポイントの使用に対してはサポートされていません。メッシュ アクセス ポイントとサポートされているソフトウェア リリースの詳細は、次の URL のメッシュ アクセス ポイントのユーザ向けマニュアルを参照してください。http://www.cisco.com/en/US/products/ps6548/tsd_products_support_series_home.html

Autonomous アクセス ポイントの Lightweight モードへの変換

アップグレード変換ツールを使用して、Cisco Aironet 1100、1130AG、1200、1240AG、および 1300 シリーズの Autonomous アクセス ポイントを Lightweight モードに変換できます。これらのいずれかのアクセス ポイントを Lightweight モードに変換した場合、アクセス ポイントはコントローラと通信し、コントローラから設定とソフトウェア イメージを受信します。

自律アクセス ポイントの Lightweight モードへの変換の手順については、『Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode』を参照してください。このドキュメントには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00804fc3dc.html

Lightweight モードに変換したアクセス ポイントの使用に関するガイドライン

Lightweight モードに変換された自律アクセス ポイントを使用する場合は、次のガイドラインに従ってください。

- 変換したアクセス ポイントは、2006、4400、WiSM コントローラのみをサポートします。Autonomous アクセス ポイントを Lightweight モードに変換した場合、そのアクセス ポイントは、Cisco 2006 シリーズ コントローラ、4400 シリーズ コントローラ、または Cisco WiSM のコントローラとのみ通信できます。
- Lightweight モードに変換したアクセス ポイントは、Wireless Domain Service（WDS; 無線ドメイン サービス）をサポートしません。変換したアクセス ポイントは、Cisco 無線 LAN コントローラとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、コントローラが WDS に相当する機能を提供します。
- コントローラ ソフトウェア リリース 4.2 以降では、すべての Cisco Lightweight アクセス ポイントで無線ごとに 16 の BSSID とアクセス ポイントごとに合計 16 の無線 LAN がサポートされます。以前のリリースでは、無線ごとに 8 の BSSID と、アクセス ポイントごとに合計 8 の無線 LAN がサポートされました。変換したアクセス ポイントがコントローラにアソシエートすると、1 ～ 16 の ID を持つ無線 LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、レイヤ 2 LWAPP をサポートしません。Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネット ブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。
- アクセス ポイントを Lightweight モードに変換した後、コンソール ポートは、そのアクセス ポイントへの読み取り専用アクセスを提供します。
- 1130AG アクセス ポイントと 1240AG アクセス ポイントは、hybrid REAP モードをサポートします。詳細は、第 12 章を参照してください。
- アップグレード変換ツールが自己署名証明書（SSC）のキーハッシュを追加するのは、Cisco WiSM の 1 つのコントローラに対してのみです。変換が完了した後で、そのコントローラから別のコントローラへ SSC キーハッシュをコピーして、それを Cisco WiSM の別のコントローラに追加します。SSC キーハッシュをコピーするには、コントローラ GUI の AP Policies ページを開き（**Security** > **AAA** > **AP Policies**）、AP Authorization List の SHA1 Key Hash カラムから SSC キーハッシュをコピーします（図 7-3 を参照）。次に、もう 1 つのコントローラの GUI を使用して同じページを開き、キーハッシュを Add AP to Authorization List の SHA1 Key Hash フィールドに貼り付けます。複数の Cisco WiSM がある場合には、WCS を使用して SSC キーハッシュをすべてのコントローラにコピーします。

Lightweight モードから Autonomous モードへの復帰

アップグレード ツールで Autonomous アクセス ポイントを Lightweight モードに変換した後、Autonomous モードをサポートする Cisco IOS リリース（Cisco IOS リリース 12.3(7)JA 以前）をロードすることによって、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがコントローラにアソシエートされている場合、コントローラを使用して Cisco IOS リリースをロードすることができます。アクセス ポイントがコントローラにアソシエートされていない場合、TFTP を使用して Cisco IOS リリースをロードすることができます。いずれの方法でも、ロードする Cisco IOS リリースを含む TFTP サーバにアクセス ポイントがアクセスできなければなりません。

コントローラを使用した前のリリースへの復帰

無線 LAN コントローラを使用して Lightweight モードから自律モードに戻す手順は、次のとおりです。

ステップ 1　アクセス ポイントがアソシエートしているコントローラで CLI にログインします。

ステップ 2　次のコマンドを入力します。

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

ステップ 3　アクセス ポイントがリブートするまで待ち、CLI または GUI を使用してアクセス ポイントを再設定します。

MODE ボタンと TFTP サーバを使用した前のリリースへの復帰

アクセス ポイントの MODE（Reset）ボタンを使用して TFTP サーバから Cisco IOS リリースをロードし、Lightweight モードから Autonomous モードに復帰する手順は次のとおりです。

ステップ 1　TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定する必要があります。

ステップ 2　PC の TFTP サーバ フォルダにアクセス ポイントのイメージ ファイル（1200 シリーズ アクセス ポイントの場合は、*c1200-k9w7-tar.123-7.JA.tar* など）があり、TFTP サーバがアクティブ化されていることを確認します。

ステップ 3　1200 シリーズ アクセス ポイントの場合は、TFTP サーバ フォルダにあるアクセス ポイントのイメージ ファイル名を **c1200-k9w7-tar.default** に変更します。

ステップ 4　カテゴリ 5（CAT5）イーサネット ケーブルを使用して PC をアクセス ポイントに接続します。

ステップ 5　アクセス ポイントの電源を切ります。

ステップ 6　**MODE** ボタンを押しながら、アクセス ポイントの電源を再投入します。

（注） アクセス ポイントの MODE ボタンを有効にしておく必要があります。アクセス ポイントの MODE ボタンのステータスを確認するには、「Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化」の項（P. 7-20）の手順に従ってください。

ステップ 7　**MODE** ボタンを押し続け、ステータス LED が赤に変わったら（約 20 ～ 30 秒）、MODE ボタンを放します。

ステップ 8　アクセス ポイントがリブートするまで待ちます（すべての LED が緑に変わった後、ステータス LED が緑に点滅します）。

ステップ 9　アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセス ポイントの認可

アクセス ポイントに製造元がインストールした証明書（MIC）があるかないかに応じて、コントローラでは自己署名証明書（SSC）を使用してアクセス ポイントが認証されるか、RADIUS サーバに認可情報が送信されるかのいずれかとなります。

SSC を使用したアクセス ポイントの認可

Lightweight アクセス ポイント プロトコル（LWAPP）は、アクセス ポイントとコントローラの両方の X.509 証明書を必要とするセキュアなキーの配布によって、アクセス ポイントとコントローラ間の制御通信を保護します。LWAPP は、X.509 証明書の事前プロビジョニングに依存しています。2005 年 7 月 18 日より前に出荷された Cisco Aironet アクセス ポイントには MIC がありません。このため、これらのアクセス ポイントでは Lightweight モードで動作するようにアップグレードされた場合、SSC が作成されます。コントローラは特定のアクセス ポイントの認証についてローカル SSC を許可するようにプログラムされており、これらの認証要求を RADIUS サーバに転送しません。これは、許容できるセキュアな動作です。

MIC を使用したアクセス ポイントの認可

RADIUS サーバによって、MIC を使用してアクセス ポイントを認可するようにコントローラを設定できます。コントローラでは、情報を RADIUS サーバに送信する際、アクセス ポイントの MAC アドレスがユーザ名とパスワードの両方に使用されます。たとえば、アクセス ポイントの MAC アドレスが 000b85229a70 の場合、コントローラでアクセス ポイントを認可する際に使用されるユーザ名もパスワードも 000b85229a70 になります。

（注） アクセス ポイントの MAC アドレスではパスワードが強力性に欠けるという点は、問題にはなりません。コントローラでは RADIUS サーバを介したアクセス ポイントの認可の前に、MIC を使用してアクセス ポイントが認証されるためです。MIC の使用により、強力に認証されます。

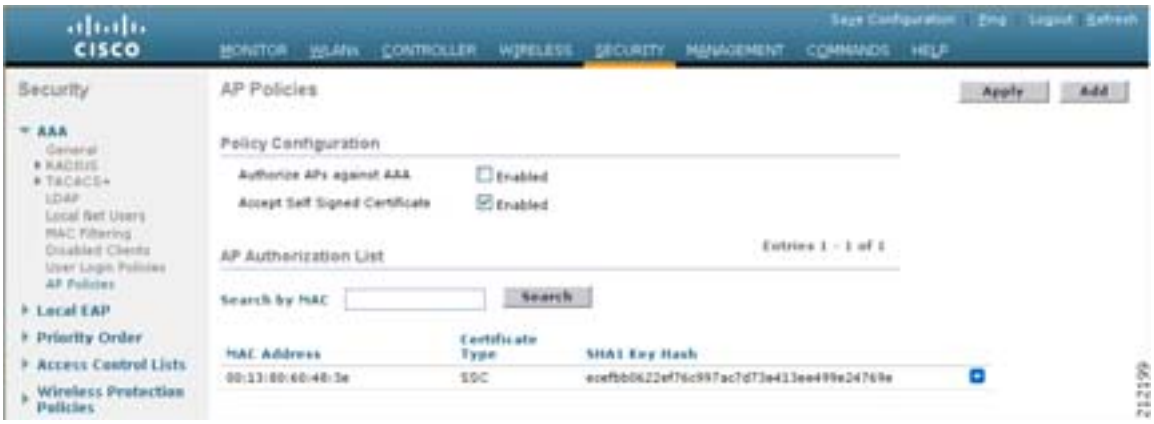
（注） MAC アドレスを RADIUS AAA サーバのアクセス ポイントの認証に対するユーザ名とパスワードに使用する場合には、同じ AAA サーバをクライアント認証に使用しないでください。

GUI を使用したアクセス ポイントの認可

コントローラの GUI を使用してアクセス ポイントを認可する手順は、次のとおりです。

ステップ 1　**Security** > **AAA** > **AP Policies** の順にクリックして、AP Policies ページを開きます（図 7-3 を参照）。

図 7-3　AP Policies ページ



ステップ 2　アクセス ポイントを認可する際に AAA RADIUS サーバを使用する場合には、**Authorize APs Against AAA** チェックボックスをオンにします。

ステップ 3　アクセス ポイントを認可する際に SSC を使用する場合には、**Authorize Self Signed Certificate (SSC)** チェックボックスをオンにします。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　アクセス ポイントをコントローラの認可リストに追加する手順は、次のとおりです。

a. **Add** をクリックして、Add AP to Authorization List 領域にアクセスします。
b. MAC Address フィールドに、アクセス ポイントの MAC アドレスを入力します。
c. Certificate Type ドロップダウン ボックスから、**MIC** または **SSC** を選択します。
d. **Add** をクリックします。アクセス ポイントが認可リストに表示されます。

（注） アクセス ポイントを認可リストから削除するには、そのアクセス ポイントの青いドロップダウン矢印にカーソルを置いて **Remove** を選択します。

（注） 特定のアクセス ポイントを 認可リストで検索するには、Search by MAC フィールドにアクセス ポイントの MAC アドレスを入力して **Search** をクリックします。

CLI を使用したアクセス ポイントの認可

コントローラの CLI を使用してアクセス ポイントを認可する手順は、次のとおりです。

ステップ 1　アクセス ポイントの認可ポリシーを設定にするには、次のコマンドを入力します。

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

ステップ 2　アクセス ポイントを認可リストに追加するには、次のコマンドを入力します。

config auth-list add {**mic** | **ssc**} *ap_mac* [*ap_key*]

ap_key は 20 バイトすなわち 40 桁のオプション キーハッシュ値です。

（注） アクセス ポイントを認可リストから削除するには、次のコマンドを入力します。
config auth-list delete *ap_mac*

ステップ 3　アクセス ポイントの認可リストを表示にするには、次のコマンドを入力します。

show auth-list

次のような情報が表示されます。

```
Authorize APs against AAA ..................... enabled
Allow APs with Self-Signed Certificate (SSC) .... enabled

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ----------------------------------------
00:0b:85:57:c9:f0         MIC
00:13:80:60:48:3e       SSC          ecefbb0622ef76c997ac7d73e413ee499e24769e
```

DHCP オプション 43 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセス ポイントの DHCP Vendor Class Identifier（VCI; ベンダー クラス ID）文字列に基づいてオプションを返すようにプログラムする必要があります（DHCP オプション 60）。表 7-1 は、Lightweight モードで動作可能な Cisco アクセス ポイントの VCI 文字列を示しています。

表 7-1　Lightweight アクセス ポイントの VCI 文字列

アクセス ポイント	VCI 文字列
Cisco Aironet 1130 シリーズ	Cisco AP c1130
Cisco Aironet 1200 シリーズ	Cisco AP c1200
Cisco Aironet 1240 シリーズ	Cisco AP c1240

TLV ブロックの形式は次のとおりです。

- Type（タイプ）：0xf1（十進数 241）
- Length（長さ）：コントローラ IP アドレスの数 * 4
- Value（値）：コントローラの管理インターフェイスの IP アドレス リスト

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品マニュアルを参照してください。『Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントの接続プロセスのトラブルシューティング

アクセス ポイントがコントローラへの接続を失敗するのは、保留中の RADIUS の認可、コントローラで有効になっていない自己署名証明書、アクセス ポイントとコントローラ間の規制区域の不一致などの多くの原因が考えられます。リリース 4.2 以前のコントローラ ソフトウェアでは、アクセス ポイントでコントローラの接続の問題がある場合、コンソール ポートを使用してアクセス ポイントにアクセスし、エラー メッセージを確認するか、コントローラ上でさまざまな LWAPP デバッグ コマンドを有効にすること以外、その詳細を知る方法はありません。そのようなタスクは、多数のアクセス ポイントが配備され、コントローラの接続にほとんど問題がない場合、コントローラのパフォーマンスに影響を与えることがあります。この状況で LWAPP デバッグ コマンドが有効になっていると、コントローラは LWAPP エラー メッセージで一杯になり、接続不能になります。

この状況を避け、アクセス ポイントの接続の問題を改善するために、コントローラ ソフトウェア リリース 4.2 以降を使用すると、すべての LWAPP 関連のエラーを syslog サーバに送信するように設定できます。すべての LWAPP エラー メッセージを syslog サーバ自体で表示できるため、デバッグ コマンドをコントローラで有効にする必要はありません。

アクセス ポイントの状態は、コントローラがアクセス ポイントから LWAPP 接続要求を受信するまでは、コントローラ上に保持されません。したがって、特定のアクセス ポイントからの LWAPP のディスカバリ要求が拒否された理由を判断するのは難しいことがあります。そのような接続の問題をコントローラで LWAPP デバッグ コマンドを有効にせずトラブルシューティングするために、コントローラはディスカバリ メッセージを送信してきたすべてのアクセス ポイントの情報を収集し、このコントローラに正常に接続したアクセス ポイントの情報を保持します。

コントローラは、LWAPP ディスカバリ要求をコントローラに送信した各アクセス ポイントの接続関連の情報をすべて収集します。収集は、アクセス ポイントから受信した最初のディスカバリ メッセージで始まり、コントローラからアクセス ポイントへ送信された最後の設定ペイロードで終わります。

接続関連の情報を表示できるアクセス ポイントの数は、次のとおりです。

- 4400 シリーズのコントローラ、Cisco WiSM、および Catalyst 3750G Integrated Wireless LAN Controller Switch については、最大 300 のアクセス ポイント
- 2100 シリーズ コントローラのプラットフォームおよび Cisco 28/37/38xx Series Integrated Services Routers 内の Controller Network Module によりサポートされたアクセス ポイントの最大 3 倍のアクセス ポイント

コントローラが最大数のアクセス ポイントの接続関連情報を維持している場合、それ以上のアクセス ポイントの情報は収集されません。

デフォルトでは、次の条件のいずれかと一致している場合、1 つのアクセス ポイントからすべての syslog メッセージが IP アドレス 255.255.255.255 に送信されます。

- ソフトウェア リリース 4.2 以降を稼動するアクセス ポイントが、新たに配備されている。
- ソフトウェア リリース 4.2 以前を稼動する既存アクセス ポイントが、4.2 以降のリリースにアップグレードされている。
- ソフトウェア リリース 4.2 以降を稼動する既存アクセス ポイントが、設定クリア後にリセットされている。

以上のいずれかの条件と一致しているのにアクセス ポイントがコントローラに接続されない場合には、DHCP サーバを設定し、サーバ上のオプション 7 を使用して syslog サーバの IP アドレスをアクセス ポイントに戻すこともできます。それにより、アクセス ポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

アクセス ポイントが現在コントローラに接続されていなければ、そのアクセス ポイントの CLI を使用して syslog サーバの IP アドレスを設定することもできます。関連コマンドは、**lwapp ap log-server** *syslog_server_IP_address* です。

アクセス ポイントが最初にコントローラに接続される際に、コントローラはグローバルな syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセス ポイントにコピーします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセス ポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントは同じコントローラに接続されたままで、コントローラ上のグローバル syslog サーバの IP アドレスの設定が **config ap syslog host global** *syslog_server_IP_address* コマンドを使用して変更された。この場合、コントローラは新しいグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントは同じコントローラに接続されたままで、特定の syslog サーバの IP アドレスが **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* コマンドを使用してコントローラ上のアクセス ポイントに対して設定された。この場合、コントローラは新しい特定の syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントはコントローラから接続を切断されており、syslog サーバの IP アドレスが **lwapp ap log-server** *syslog_server_IP_address* コマンドを使用して、アクセス ポイントの CLI から設定された。このコマンドは、アクセス ポイントが他のコントローラに接続されていない場合に限り機能します。
- アクセス ポイントがコントローラから接続を切断され、別のコントローラに接続されている。この場合、新しいコントローラはそのグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存されます。アクセス ポイントはその syslog サーバの IP アドレスに接続できれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

アクセス ポイントの syslog サーバを設定して、アクセス ポイントの接続情報をコントローラの CLI 以外では表示しないようにできます。

アクセス ポイントの Syslog サーバの設定

コントローラの CLI を使用してアクセス ポイントの syslog サーバを設定する手順は、次のとおりです。

ステップ 1　次のいずれかの操作を行います。

- このコントローラに接続するすべてのアクセス ポイントに対して、グローバルな syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host global *syslog_server_IP_address*

  （注） デフォルトでは、グローバル syslog サーバの IP アドレスは、すべてのアクセス ポイントに対して 255.255.255.255 です。アクセス ポイントが syslog サーバ常駐のサブネットに接続できることを確認してから、コントローラの syslog サーバを設定してください。アクセス ポイントがこのサブネットに接続できない場合には、そのアクセス ポイントは syslog メッセージを送信できません。

- 特定のアクセス ポイントの syslog サーバを設定するには、次のコマンドを入力します。

  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  （注） デフォルトでは、各アクセス ポイントの syslog サーバの IP アドレスは 0.0.0.0 で、これは未設定であることを示しています。デフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスが、アクセス ポイントにコピーされます。

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

ステップ 3　コントローラに接続するすべてのアクセス ポイントに対して、グローバルな syslog サーバを表示するには、次のコマンドを入力します。

show ap config global

次のような情報が表示されます。

```
AP global system logging host..................... 255.255.255.255
```

ステップ 4　特定のアクセス ポイントの syslog サーバの設定を表示するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

アクセス ポイントの接続情報の表示

LWAPP ディスカバリ要求をコントローラに少なくとも 1 回送信したアクセス ポイントの接続の統計は、アクセス ポイントがリブートまたは切断されても、コントローラ上に維持されます。これらの統計は、コントローラがリブートされた場合のみ削除されます。

次の CLI コマンドを使用して、アクセス ポイントの接続情報を表示します。

- コントローラに接続されているまたは接続を試行した、すべてのアクセス ポイントの MAC アドレスを表示するには、次のコマンドを入力します。

  show ap join stats summary all

  次のような情報が表示されます。

```
Number of APs.................................................. 3

00:0b:85:1b:7c:b0.............................................. Joined
00:12:44:bb:25:d0.............................................. Joined
00:13:19:31:9c:e0.............................................. Not joined
```

- 特定アクセス ポイントの最新接続エラーの詳細を表示するには、次のコマンドを入力します。

  show ap join stats summary *ap_mac*

  ap_mac は、802.11 無線インターフェイスの MAC アドレスです。

（注） 802.11 無線インターフェイスの MAC アドレスを取得するには、アクセス ポイントの CLI に次のコマンドを入力します。**show interfaces Dot11Radio 0**

次のような情報が表示されます。

```
Is the AP currently connected to controller..... No
Time at which the AP joined this controller last time...... Aug 21 12:50:36.061
Type of error that occurred last.......................... Lwapp join request
rejected
Reason for error that occurred last....................... RADIUS authorization
 is pending for the AP
Time at which the last join error occurred.............. Aug 21 12:50:34.374
```

- 特定アクセス ポイントで収集されたすべての接続関連の統計を表示するには、次のコマンドを入力します。

  show ap join stats detailed *ap_mac*

  次のような情報が表示されます。

```
Discovery phase statistics
- Discovery requests received.............................. 2
- Successful discovery responses sent...................... 2
- Unsuccessful discovery request processing................ 0
- Reason for last unsuccessful discovery attempt........... Not applicable
- Time at last successful discovery attempt................ Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt.............. Not applicable

Join phase statistics
- Join requests received................................... 1
- Successful join responses sent........................... 1
- Unsuccessful join request processing..................... 1
- Reason for last unsuccessful join attempt................ RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..................... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt................... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received.......................... 1
- Successful configuration responses sent.................. 1
- Unsuccessful configuration request processing............ 0
- Reason for last unsuccessful configuration attempt....... Not applicable
- Time at last successful configuration attempt............ Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt.......... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure............... Not applicable

Last AP disconnect details
- Reason for last AP connection failure.................... Not applicable

Last join error summary
- Type of error that occurred last......................... Lwapp join request
rejected
- Reason for error that occurred last...................... RADIUS authorization
 is pending for the AP
- Time at which the last join error occurred............... Aug 21 12:50:34.374
```

Lightweight モードに変換したアクセス ポイントへのコントローラを使用したデバッグ コマンドの送信

Lightweight モードに変換したアクセス ポイントにコントローラがデバッグ コマンドを送信できるようにするには、次のコマンドを入力します。

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

この機能を有効にした場合、コントローラは変換したアクセス ポイントに文字列としてデバッグ コマンドを送信します。Cisco IOS ソフトウェアを Lightweight モードで実行する Cisco Aironet アクセス ポイントがサポートしている任意のデバッグ コマンドを送信することができます。

変換したアクセス ポイントからコントローラへのクラッシュ情報の送信

変換したアクセス ポイントが予期せずリブートした場合、アクセス ポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルが保存されます。リブート後、アクセス ポイントはリブートの理由をコントローラに送信します。クラッシュにより装置がリブートした場合、コントローラは既存の LWAPP メッセージを使用してクラッシュ ファイルを取得し、コントローラのフラッシュ メモリにそれを保存します。クラッシュ情報コピーは、コントローラがアクセス ポイントからそれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

変換したアクセス ポイントからコントローラへの無線コア ダンプの送信

変換したアクセス ポイントの無線モジュールがコア ダンプを生成した場合、アクセス ポイントは無線クラッシュ発生時にローカル フラッシュ メモリ上に無線のコア ダンプ ファイルを保存します。また、無線がコア ダンプ ファイルを生成したことを知らせる通知メッセージをコントローラに送信します。コントローラはネットワーク管理者に警告するトラップを送信し、管理者はアクセス ポイントから無線コア ファイルを受信することができます。

取得したコア ファイルはコントローラのフラッシュに保存されます。このファイルを TFTP 経由で外部サーバにアップロードし、分析に使用することができます。コア ファイルは、コントローラがアクセス ポイントからそれを取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

CLI を使用して無線のコア ダンプ ファイルを取得する手順は、次のとおりです。

ステップ 1　アクセス ポイントからコントローラに無線のコア ダンプ ファイルを転送するには、次のコマンドを入力します。

config ap crash-file get-radio-core-dump *slot Cisco_AP*

slot パラメータには、クラッシュした無線のスロット ID を入力します。

ステップ 2　ファイルがコントローラにダウンロードされたことを確認するには、次のコマンドを入力します。

show ap crash-file

次のような情報が表示されます。

```
Local Core Files:
lrad_AP1130.rdump0   (156)
```

カッコ内の数字は、ファイルのサイズを示します。コア ダンプ ファイルを使用できる場合、サイズはゼロより大きくなければなりません。

ステップ 3　ファイルをコントローラから TFTP サーバに転送するには、次のコマンドを入力します。

transfer upload datatype radio-core-dump

transfer upload filename *filename*

transfer upload serverip *tftp_server_ip*

transfer upload start

変換したアクセス ポイントからのメモリ コア ダンプの有効化

デフォルトでは、Lightweight モードに変換したアクセス ポイントは、コントローラにメモリ コア ダンプを送信しません。この機能を有効にするには、次のコマンドを入力します。

config ap core-dump enable *tftp-server-ip-address filename* {**compress** | **uncompress**} {*ap-name* | **all**}

- *tftp-server-ip-address* には、アクセス ポイントがコア ファイルを送信する TFTP サーバの IP アドレスを入力します。アクセス ポイントは TFTP サーバに到達可能でなければなりません。
- *filename* には、アクセス ポイントがコア ファイルのラベル付けに使用するファイル名を入力します。

- 圧縮したコア ファイルを送信するようにアクセス ポイントを設定するには、**compress** を入力します。圧縮しないコア ファイルを送信するようにアクセス ポイントを設定するには、**uncompressed** を入力します。
- *ap-name* には、特定のアクセス ポイントの名前を入力します。Lightweight モードに変換したすべてのアクセス ポイントからのメモリ コア ダンプを有効にするには、**all** を入力します。

変換したアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には違いがあります。

- コントローラでは、AP Summary ページに変換されたアクセス ポイントのイーサネット MAC アドレスのリストを表示します。
- AP Detail ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストを表示します。
- Radio Summary ページには、変換されたアクセス ポイントのリストを無線 MAC アドレスによって表示します。

Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化

Lightweight モードに変換したアクセス ポイントの Reset ボタンを無効化することができます Reset ボタンは、アクセス ポイントの外面に MODE と書かれたラベルが付けられています。

次のコマンドを使用すると、あるコントローラにアソシエートしている変換されたアクセス ポイントの 1 つまたはすべての Reset ボタンを無効または有効にできます。

config ap reset-button {**enable** | **disable**} {*ap-name* | **all**}

変換されたアクセス ポイントの Reset ボタンは、デフォルトでは有効になっています。

Lightweight モードに変換したアクセス ポイントの固定 IP アドレスの設定

Lightweight モードに変換したアクセス ポイントがコントローラにアソシエートした後、次のコマンドを入力してアクセス ポイントに固定 IP アドレスを設定します。

config ap static-ip enable *ap-name ip-address mask gateway*

（注） アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォール バックします。アクセス ポイントが DHCP アドレスにフォール バックすると、アクセス ポイントがフォールバック IP アドレスを使用していることが **show ap config general** *ap-name* CLI コマンドによって適切に表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであるとは識別しません。

サイズの大きなアクセス ポイントのイメージのサポート

コントローラ ソフトウェア リリース 5.0 では、リカバリ イメージを自動的に削除して十分なスペースを作ることで、サイズの大きなアクセス ポイントのイメージにアップグレードできます。この機能は、8MB のフラッシュを備えたアクセス ポイントにのみ影響を及ぼします（1100、1200、および 1310 シリーズ アクセス ポイント）。すべての比較的新しいアクセス ポイントには、8MB を超える大型フラッシュが備わっています。

（注） 2007 年 8 月現在で、サイズの大きなアクセス ポイントのイメージはありませんでしたが、新機能が追加され、アクセス ポイントのイメージ サイズはこれからも拡大し続けます。

リカバリ イメージによって、イメージのアップグレード時にアクセス ポイントのパワーサイクリングを行っても使用できる、バックアップ イメージが提供されます。アクセス ポイントでリカバリの必要を避ける最善の方法は、システムのアップグレード時にアクセス ポイントのパワーサイクリングを避けることです。サイズの大きなアクセス ポイントのイメージへのアップグレードの際にパワーサイクリングが発生した場合、TFTP リカバリの手順を使用してアクセス ポイントを回復できます。

TFTP リカバリを実行する手順は、次のとおりです。

ステップ 1　必要なリカバリ イメージを Cisco.com（c1100-rcvk9w8-mx、c1200-rcvk9w8-mx、または c1310-rcvk9w8-mx）からダウンロードし、お使いの TFTP サーバのルート ディレクトリにインストールします。

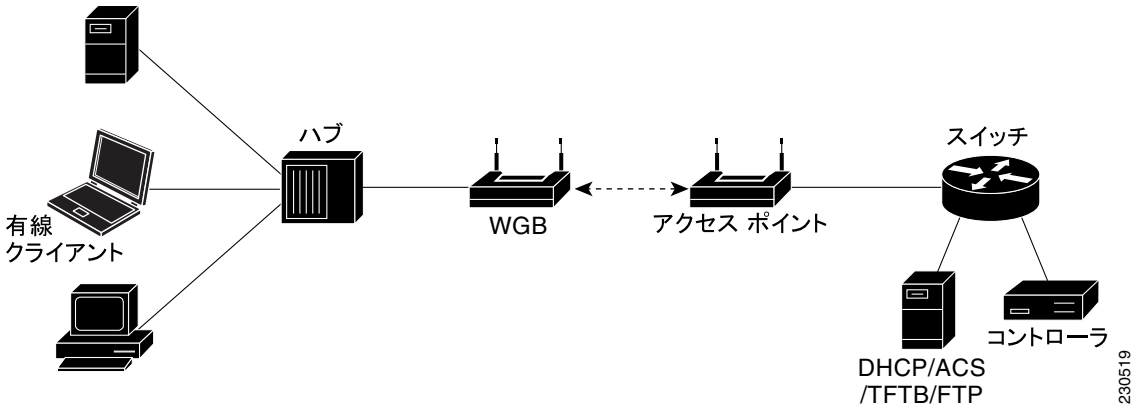
ステップ 2　TFTP サーバをターゲットのアクセス ポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセス ポイントは TFTP イメージから起動し、次にコントローラに接続してサイズの大きなアクセス ポイントのイメージをダウンロードし、アップグレード手順を完了します。

ステップ 3　アクセス ポイントが回復したら、TFTP サーバを削除できます。

Cisco ワークグループ ブリッジ

ワークグループ ブリッジ（WGB）は、Autonomous IOS アクセス ポイント上で設定でき、イーサネットで WGB アクセス ポイントに接続されたクライアントの代わりに Lightweight アクセス ポイントに無線で接続を提供するモードです。イーサネット インターフェイス上の有線クライアントの MAC アドレスを記憶し、それを Internet Access Point Protocol（IAPP）メッセージングを使用して Lightweight アクセス ポイントに報告することで、WGB は単一の無線セグメントを介して有線ネットワークに接続します。WGB は、単一の無線接続を Lightweight アクセス ポイントに確立して、有線クライアントに無線で接続できるようになります。Lightweight アクセス ポイントは、WGB を無線クライアントとして処理します。図 7-4 の例を参照してください。

図 7-4　WGB の例



（注） Lightweight アクセス ポイントが機能しない場合には、WGB は別のアクセス ポイントへのアソシエーションを試行します。

WGB の使用に関するガイドライン

ネットワークで WGB を使用する場合には、次のガイドラインに従ってください。

- ワークグループ ブリッジ モードをサポートし、Cisco IOS リリース 12.4（3g）JA 以降（32 MB のアクセス ポイント上の）または Cisco IOS リリース 12.3（8）JEB 以降（16 MB のアクセス ポイント上の）を稼動している自律アクセス ポイントであれば、WGB を構成できます。これらのアクセス ポイントには、AP1120、AP1121、AP1130、AP1231、AP1240、および AP1310 があります。12.4（3g）JA および 12.3（8）JEB 以前の Cisco IOS リリースは、サポートされていません。

（注） アクセス ポイントに 2 つの無線がある場合、1 つのみをワークグループ ブリッジ モード対応に設定できます。この無線を使用して、Lightweight アクセス ポイントに接続します。もう一方の無線を無効にしておくことをお勧めします。

（注） コントローラは Cisco WGB 製品のみをサポートしています。Linksys および OEM WGB デバイスはサポートされていません。Cisco Wireless Unified Solution では Linksys WET54G および WET11B イーサネット ブリッジはサポートされていませんが、次のガイドラインに従った場合、Wireless Unified Solution 設定でこれらのデバイスを使用できるようになります。
1. WET54G または WET11B にデバイスを 1 つのみ接続する。
2. 接続されたデバイスをクローンするために、WET54G または WET11B で MAC クローン機能を有効化する。
3. WET54G または WET11B に接続されたデバイスに最新のドライバおよびファームウェアをインストールする。このガイドラインは JetDirect プリンタでは特に重要です。初期のファームウェア バージョンは DHCP で問題を起こす可能性があるからです。
注：これらのデバイスは Cisco Wireless Unified Solution ではサポートされていないので、これらに関連する問題のトラブルシューティングは、シスコのテクニカル サポートでは役に立ちません。

WGB 上でワークグループ ブリッジ モードを有効にするには、次のいずれかを実行します。

- WGB アクセス ポイントの GUI で、Settings > Network Interfaces ページの無線ネットワークのロールに対する **Workgroup Bridge** を選択します。
- WGB アクセス ポイントの CLI で、次のコマンドを入力します。**station-role workgroup-bridge**

（注） 「WGB 設定例」の項（P. 7-25）の WGB アクセス ポイントの設定サンプルを参照してください。

- WGB は Lightweight アクセス ポイントにのみアソシエートできます。
- クライアント モード（デフォルト値）の WGB のみがサポートされています。インフラストラクチャ モードの WGB はサポートされていません。WGB 上でクライアント モードを有効にするには、次のいずれかを実行します。
  - WGB アクセス ポイントの GUI で、Reliable Multicast to WGB パラメータに対して **Disabled** を選択します。
  - WGB アクセス ポイントの CLI で、次のコマンドを入力します。**no infrastructure client**

（注） VLAN と WGB の共用はサポートされていません。

（注） 「WGB 設定例」の項（P. 7-25）の WGB アクセス ポイントの設定サンプルを参照してください。

- 次の機能は、WGB との共用がサポートされています。
  - Guest N+1 redundancy
  - Local EAP
- 次の機能は、WGB との共用がサポートされていません。
  - Cisco Centralized Key Management（CCKM）
  - Hybrid REAP

- Idle timeout
- Web 認証

（注） WGB が Web 認証 WLAN にアソシエートしている場合、その WGB は除外リストに追加され、その WGB 有線クライアントすべてが削除されます。

- WGB に接続している有線クライアントは、セキュリティについて認証されません。代わりに WGB が、アソシエートしているアクセス ポイントに対して認証されます。そのため、WGB の有線サイドを物理的に保護することをお勧めします。
- レイヤ 3 のローミングでは、WGB が別のコントローラ（外部コントローラなどに）にローミングした後で、有線クライアントをその WGB ネットワークに接続すると、有線クライアントの IP アドレスはアンカー コントローラにのみ表示され、外部コントローラには表示されません。
- 有線クライアントが長期間にわたってトラフィックを送信しない場合には、トラフィックが継続的にその有線クライアントに送信されていても、WGB はそのクライアントをブリッジ テーブルから削除します。その結果、有線クライアントへのトラフィック フローは機能しなくなります。このトラフィック損失を避けるには、次の IOS コマンドを WGB で使用して WGB の エージングアウト タイマの値を大きく設定することで、有線クライアントがブリッジ テーブルから削除されないようにします。

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

  bridge-group-number の値は 1 ～ 255、*seconds* の値は 10 ～ 1,000,000 秒です。*seconds* パラメータを有線クライアントのアイドル時間の値より大きく設定することをお勧めします。
- WGB レコードをコントローラから削除すると、すべての WGB 有線クライアントのレコードも削除されます。
- WGB に接続された有線クライアントは、WGB の QoS および AAA Override 属性を継承します。
- 次の機能は、WGB に接続された有線クライアントにはサポートされていません。
  - MAC filtering
  - Link tests
  - Idle timeout
- WGB が Lightweight アクセス ポイントと通信できるようにするために、コントローラで設定する必要はありません。ただし、適切な通信を確保するために、コントローラに WLAN を作成して SSID と WGB で設定したセキュリティ方式を一致させる必要があります。

WGB 設定例

これは、40 ビットの WEP キーを持つ静的 WEP を使用して設定した、WGB アクセス ポイントの設定例です。

```
ap#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#dot11 ssid WGB_with_static_WEP
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface  dot11Radio 0
ap(config)#station-role workgroup-bridge
ap(config-if)#encry mode wep 40
ap(config-if)#encry key 1 size 40 0 1234567890
ap(config-if)#WGB_with_static_WEP
ap(config-if)#end
```

この WGB がアクセス ポイントにアソシエートしていることを確認するには、WGB に次のコマンドを入力します。

show dot11 association

次のような情報が表示されます。

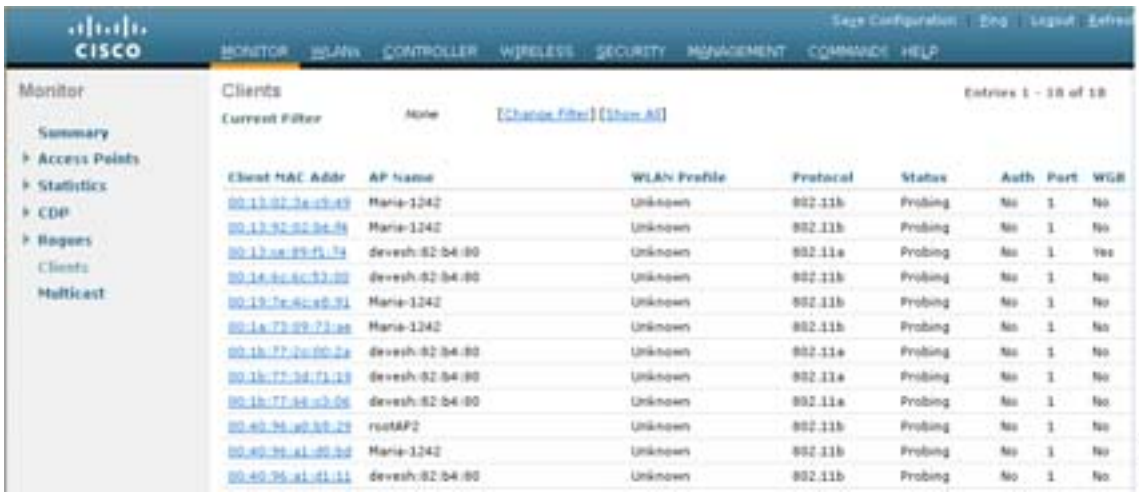
```
ap#show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

GUI を使用したワークグループ ブリッジのステータスの表示

コントローラの GUI を使用して WGB のステータスをネットワークで表示する手順は、次のとおりです。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます（図 7-5 を参照）。

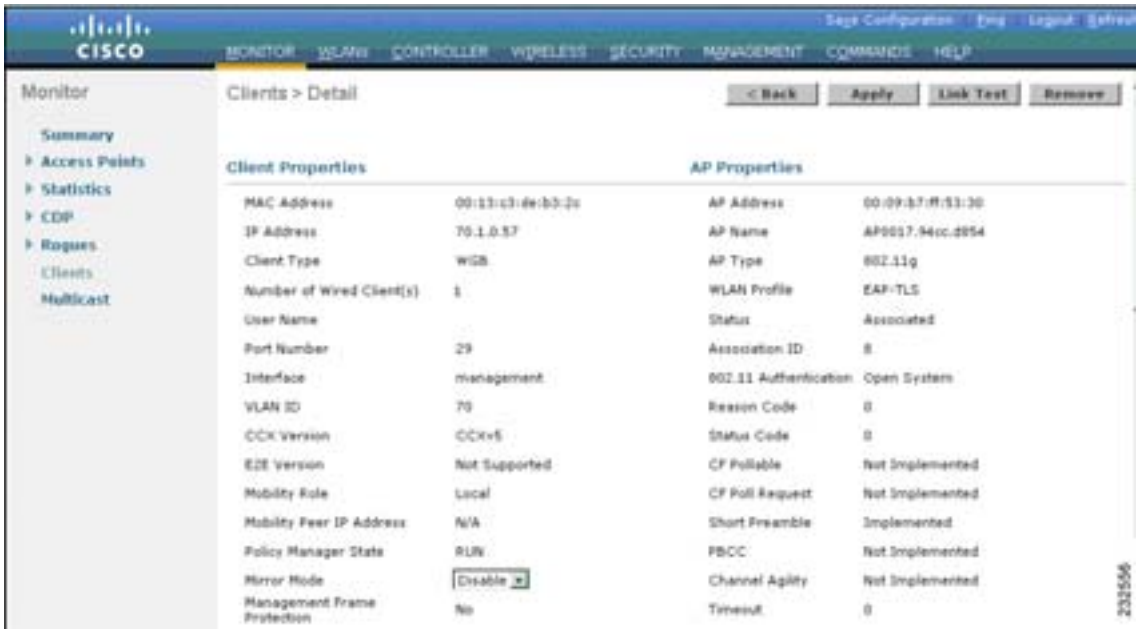
図 7-5　Clients ページ



このページの右側の WGB フィールドには、ネットワーク上の各クライアントについてワークグループ ブリッジであるかどうかが示されています。

ステップ 2　目的のクライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます（図 7-6 を参照）。

図 7-6　Clients > Detail ページ



このクライアントがワークグループ ブリッジの場合、Client Properties 下の Client Type フィールドに「WGB」が表示され、Number of Wired Client(s) フィールドにこの WGB に接続されている有線クライアントの番号が表示されます。

ステップ 3　特定の WGB に接続された有線クライアントの詳細を表示する手順は、次のとおりです。

a.　Clients > Detail ページで **Back** をクリックして、Clients ページに戻ります。

b.　カーソルを目的の WGB の青のドロップダウン矢印の上に置いて、**Show Wired Clients** を選択します。WGB Wired Clients ページが表示されます（図 7-7 を参照）。

図 7-7　WGB Wired Clients ページ

（注）　特定のクライアントを無効にしたり、削除する場合には、カーソルを目的のクライアントの青のドロップダウン矢印の上に置いて、**Remove** または **Disable** を選択します。

c. 目的のクライアントの MAC アドレスをクリックすると、この特定のクライアントに関する詳細が表示されます。Clients > Detail ページが表示されます（図 7-8 を参照）。

図 7-8　Clients > Detail ページ

Client Properties 下の Client Type フィールドには「WGB Client」と表示され、このページの他のフィールドにはこのクライアントに関するその他の情報が記載されています。

CLI を使用したワークグループ ブリッジのステータスの表示

コントローラ CLI を使用して WGB のステータスをネットワークで表示する手順は、次のとおりです。

ステップ 1　WGB をネットワークで表示するには、次のコマンドを入力します。

show wgb summary

次のような情報が表示されます。

```
Number of WGBs..................................... 1

MAC Address        IP Address AP Name  Status  WLAN  Auth  Protocol  Clients
-----------------  ---------  -------- ------  ----  ----- --------- --------
00:0d:ed:dd:25:82  10.24.8.73      a1   Assoc   3     Yes   802.11b   1
```

ステップ 2　特定の WGB に接続された有線クライアントの詳細を表示するには、次のコマンドを入力します。

show wgb detail *wgb_mac_address*

次のような情報が表示されます。

```
Number of wired client(s): 1

MAC Address         IP Address AP Name  Mobility   WLAN   Auth
------------------- ---------- -------- ---------  ----- -----
00:0d:60:fc:d5:0b   10.24.8.75   a1      Local      3     Yes
```

CLI を使用した WGB 問題のデバッグ

WGB に関する問題が発生した場合には、この項のコマンドを使用します。

1. IAPP メッセージ、エラー、およびパケットのデバッグを有効にするには、次のコマンドを入力します。
   - **debug iapp all enable**：IAPP メッセージのデバッグを有効にします。
   - **debug iapp error enable**：IAPP エラー イベントのデバッグを有効にします。
   - **debug iapp packet enable**：IAPP パケットのデバッグを有効にします。
2. ローミングの問題が発生した場合には、次のコマンドを入力します。

   debug mobility handoff enable
3. IP 割り当ての問題が発生し、DHCP が使用されている場合には、次のコマンドを入力します。
   - **debug dhcp message enable**
   - **debug dhcp packet enable**
4. IP 割り当ての問題が発生し、固定 IP が使用されている場合には、次のコマンドを入力します。
   - **debug dot11 mobile enable**
   - **debug dot11 state enable**

バックアップ コントローラの設定

中央ロケーションにある単一のコントローラは、アクセス ポイントでローカルのプライマリ コントローラを失った場合にバックアップとして機能できます。中央および地域のコントローラは、同じモビリティ グループに存在する必要があります。コントローラの CLI を使用して、ネットワークのアクセス ポイントのプライマリ、セカンダリ、ターシャリのコントローラを指定できます。コントローラ ソフトウェア リリース 4.2 では、バックアップ コントローラの IP アドレスを指定できます。これにより、アクセス ポイントはモビリティ グループ外のコントローラをフェールオーバーできます。

コントロール ソフトウェア リリース 5.0 では、プライマリおよびセカンダリ バックアップ コントローラとともに、高速ハートビート タイマーおよびプライマリ ディスカバリ要求タイマーを設定することもできます。コントローラの障害検出時間を削減するには、ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの時間が来ると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。

（注） 高速ハートビート タイマーは、ローカル モードまたは hybrid-REAP モードのアクセス ポイントにのみ設定できます。

アクセス ポイントはバックアップ コントローラのリストを維持し、リスト上の各エントリに対して定期的にプライマリ ディスカバリ要求を送信します。アクセス ポイントがコントローラから新しいディスカバリ応答を受信すると、バックアップ コントローラのリストが更新されます。プライマリ ディスカバリ要求に 2 回連続で応答できなかったコントローラはすべて、リストから削除されます。アクセス ポイントのローカル コントローラに障害が発生した場合、プライマリ、セカンダリ、ターシャリ、プライマリ バックアップ、セカンダリ バックアップの順に、バックアップ コントローラ リストから使用可能なコントローラが選択されます。アクセス ポイントはバックアップ リストで使用可能な最初のコントローラからのディスカバリ応答を待機し、プライマリ ディスカバリ要求タイマーで設定された時間内に応答を受信した場合は、このコントローラを接続します。制限時間に達すると、アクセス ポイントはコントローラを接続できないとみなし、リストで次に使用可能なコントローラからのディスカバリ応答を待ちます。

これらの機能は、現在、コントローラの CLI を介してのみサポートされています。

CLI を使用したバックアップ コントローラの設定

バックアップ コントローラはアクセス ポイントごと、またはコントローラごとに設定できます。CLI を使用して、特定のアクセス ポイントのプライマリ、セカンダリ、およびターシャリのコントローラ、および特定のコントローラのプライマリおよびセカンダリ バックアップ コントローラを設定する手順は、次のとおりです。

ステップ 1　特定のアクセス ポイントのプライマリ コントローラを設定するには、次のコマンドを入力します。

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

（注） このコマンドの *controller_ip_address* パラメータおよびそれに続く 2 つのコマンドはオプションです。バックアップ コントローラが、アクセス ポイントが接続されている（プライマリ コントローラ）モビリティ グループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。各コマンドで、*controller_name* および *controller_ip_address* は同じプライマリ、セカンダリ、またはターシャリ コントローラに属す必要があります。そうでない場合、アクセス ポイントはバックアップ コントローラに接続できません。

ステップ 2　特定のアクセス ポイントのセカンダリ コントローラを設定するには、次のコマンドを入力します。

config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 3　特定のアクセス ポイントのターシャリ コントローラを設定するには、次のコマンドを入力します。

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 4　特定のコントローラのプライマリ バックアップ コントローラを設定するには、次のコマンドを入力します。

config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

ステップ 5　特定のコントローラのセカンダリ バックアップ コントローラを設定するには、次のコマンドを入力します。

config advanced backup-controller secondary *backup_controller_name backup_controller_ip_address*

（注） プライマリ、またはセカンダリ バックアップ コントローラ エントリを削除するには、コントローラの IP アドレスとして 0.0.0.0 を入力します。

ステップ 6　ローカル、hybrid-REAP、またはすべてのアクセス ポイントで 高速ハートビート タイマーを有効または無効にするには、次のコマンドを入力します。

config advanced timers ap-fast-heartbeat {**local** | **hreap** | **all**} {**enable** | **disable**} *interval*

ここで、**all** はローカルおよび hybrid-REAP アクセス ポイントの両方を表します。また、*interval* には 1 ～ 10 秒の値（両端の値を含む）を指定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が削減されます。デフォルト値は無効（disable）です。

ステップ 7　アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定にするには、次のコマンドを入力します。

config advanced timers ap-primary-discovery-timeout *interval*

interval の値は、30 ～ 3600 秒です。デフォルト値は 120 秒です。

ステップ 8　変更を保存するには、次のコマンドを入力します。

save config

ステップ 9　アクセス ポイントの設定を表示にするには、次のコマンドを入力します。

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

show ap config general *Cisco_AP* コマンドに対しては、次のような情報が表示されます。

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.133
...
Primary Cisco Switch Name....................... 1-4404
Primary Cisco Switch IP Address.................. Not Configured
Secondary Cisco Switch Name..................... 2-4404
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name...................... 1-4404
Tertiary Cisco Switch IP Address................ Not Configured
...
```

show advanced backup-controller コマンドに対しては、次のような情報が表示されます。

```
AP primary Backup Controller ................... controller 10.10.10.10
AP secondary Backup Controller ................ 0.0.0.0
```

show advanced timers コマンドに対しては、次のような情報が表示されます。

```
Authentication Response Timeout (seconds)........ 50
Rogue Entry Timeout (seconds).................... 1300
AP Heart Beat Timeout (seconds).................. 30
AP Discovery Timeout (seconds)................... 10
AP Local mode Fast Heartbeat (seconds)........... 3 (enable)
AP Hreap mode Fast Heartbeat (seconds)........... 3 (enable)
AP Primary Discovery Timeout (seconds)........... 120
```

国コードの設定

コントローラおよびアクセス ポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセス ポイント内の無線は、工場で特定の規制区域に割り当てられています（ヨーロッパの場合には E など）。しかし、国コードを使用すると、稼動する特定の国を指定できます（フランスの場合には FR、スペインの場合には ES など）。国コードを設定すると、各無線のブロードキャスト周波数帯、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

通常、コントローラごとに 1 つの国コードを設定します。この国コードでは、そのコントローラの物理的な場所とそのアクセス ポイントが一致している必要があります。ただし、コントローラ ソフトウェア リリース 4.1 以降では、コントローラごとに 20 の国コードを設定できます。これによって、複数の国がサポートされ、1 つのコントローラからさまざまな国にあるアクセス ポイントを管理できます。

（注） コントローラはさまざまな規制区域（ドメイン）でさまざまなアクセス ポイントをサポートしていますが、同一の規制区域については 1 つのアクセス ポイントにすべての無線を設定する必要があります。たとえば、米国（-A）の規制区域に対して Cisco 1231 アクセス ポイントの 802.11b/g 無線を設定し、イギリス（-E）の規制区域に対して 802.11a 無線を設定してはなりません。設定した場合、コントローラのアクセス ポイントに選択した規制区域に応じて、コントローラはアクセス ポイントの無線のどちらか 1 つだけをオンにします。したがって、アクセス ポイントの無線の両方には必ず同じ国コードを設定してください。

製品ごとにサポートされている国コードの一覧は、www.ciscofax.com または http://www.cisco.com/application/pdf/en/us/guest/products/ps5861/c1650/cdccont_0900aecd80537b6a.pdf を参照してください。

複数の国コードの設定に関するガイドライン

複数の国コードを設定する場合には、次のガイドラインに従ってください。

- 複数の国コード機能を使用している場合、同じ RF グループに接続する予定のすべてのコントローラは、同じ国で構成された一連の国々を同じ順序で設定する必要があります。
- 複数の国コードを設定し、Radio Resource Management（RRM）自動 RF 機能を有効にしている場合には、自動 RF 機能はすべての設定済みの国で合法的なチャネルのみ、およびすべての設定済みの国に共通の最低電力レベルに制限されます。アクセス ポイントは常にすべての合法的な周波数を使用できますが、共通でないチャネルは手動でのみ割り当てることができます。

  （注） アクセス ポイントが既に規制の電力レベルより高く設定されていたり、手動入力で設定されている場合には、電力レベルはそのアクセス ポイントが割り当てられている特定の国によってのみ制限されます。

- 複数の国コードを設定する際に、802.11a 無線をサポートしない国があったり、802.11a 無線の共通チャネルがない場合には、802.11a ネットワークはすべての国に対して無効になります。

コントローラ GUI または CLI を使用して国コードを設定することもできます。

GUI を使用した国コードの設定

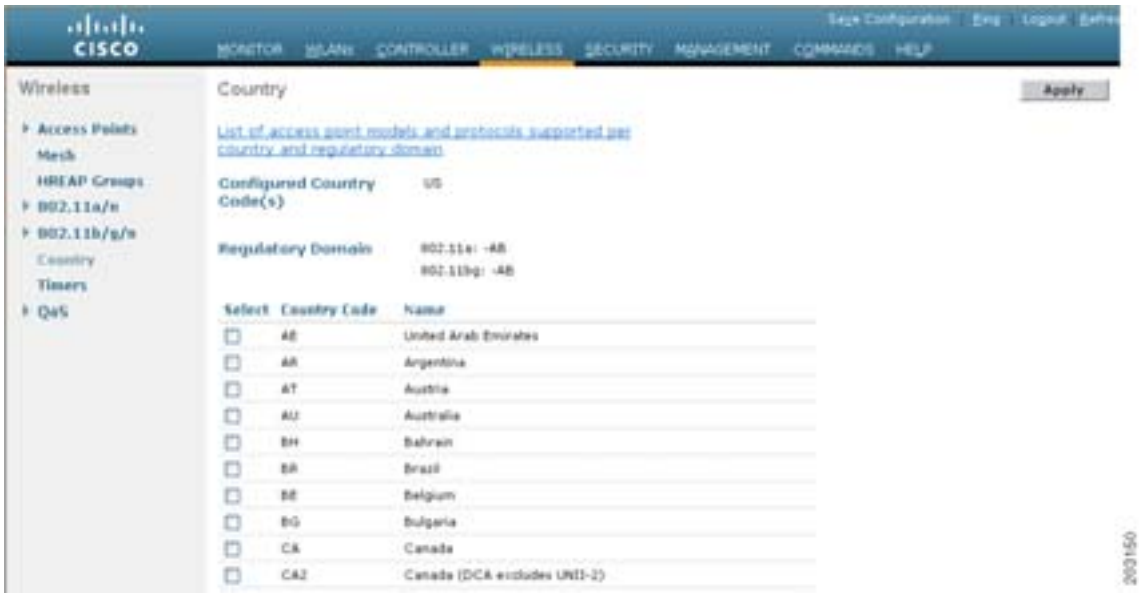
GUI を使用して国コードを設定する手順は、次のとおりです。

ステップ 1　802.11a および 802.11b/g ネットワークを無効にする手順は、次のとおりです。

a. **Wireless** > **802.11a/n** > **Network** の順にクリックします。
b. **802.11a Network Status** チェックボックスをオフにします。
c. **Apply** をクリックして、変更を適用します。
d. **Wireless** > **802.11b/g/n** > **Network** の順にクリックします。
e. **802.11b/g Network Status** チェックボックスをオフにします。
f. **Apply** をクリックして、変更を適用します。

ステップ 2　**Wireless** > **Country** の順にクリックして、Country ページを開きます（図 7-9 を参照）。

図 7-9　Country ページ



ステップ 3　アクセス ポイントがインストールされている各国のチェックボックスをオンにします。

ステップ 4　ステップ 3 で複数のチェックボックスをオンにした場合、RRM チャネルと電力レベルが共通のチャネルと電力レベルに制限されることを記載したメッセージが表示されます。**OK** をクリックして続行するか、**Cancel** をクリックして操作をキャンセルします。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　ステップ 3 で複数の国コードを選択した場合、各アクセス ポイントが国に割り当てられます。各アクセス ポイントに対して選択されたデフォルトの国を表示し、必要に応じて異なる国を選択する手順は、次のとおりです。

（注） 国コードを設定から削除する場合、削除する国に現在割り当てられているアクセス ポイントはリブートし、コントローラに再接続される際に、必要に応じて残りの国のいずれかに再割り当てされます。

a. 次のいずれかの操作を行います。

- 802.11a および 802.11b/g ネットワークを無効のままにします。
- 802.11a および 802.11b/g ネットワークを再び有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。アクセス ポイントを無効にするには、**Wireless** > **Access Points** > **All APs** の順にクリックし、目的のアクセス ポイントのリンクをクリックして、Admin Status ドロップダウン ボックスで **Disable** を選択し、**Apply** をクリックします。

b. **Wireless** > **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。

c. 目的のアクセス ポイントのリンクをクリックします。

d. All APs > Details ページが表示されたら、**Advanced** タブをクリックして All APs > Details（Advanced）ページを開きます（図 7-10 を参照）。

図 7-10　All APs > Details（Advanced）ページ

e. このアクセス ポイントのデフォルトの国が Country Code ドロップダウン ボックスに表示されます。アクセス ポイントが表示された国以外でインストールされている場合には、ドロップダウン ボックスから正しい国を選択します。ドロップダウン ボックスに記載される国コードは、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制区域に適合します。

f. **Apply** をクリックして、変更を適用します。

g. コントローラに接続されたすべてのアクセス ポイントを特定の国に割り当てるには、この手順を繰り返します。

h. 手順 a. で無効にしたアクセス ポイントを再び有効にします。

ステップ 7　ステップ 6 で 802.11a および 802.11b/g ネットワークを再び有効にしなかった場合には、有効にします。

ステップ 8　**Save Configuration** をクリックして、設定内容を保存します。

CLI を使用した国コードの設定

CLI を使用して国コードを設定する手順は、次のとおりです。

ステップ 1　使用可能な国コードをすべて表示するには、次のコマンドを入力します。

show country supported

ステップ 2　802.11a および 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

config 802.11b disable network

ステップ 3　アクセス　ポイントがインストールされた国の国コードを設定するには、次のコマンドを入力します。

config country *code1*[,*code2*,*code3*,...]

複数の国コードを入力する場合には、各国コードをカンマで区切ります（**config country US,CA,MX** など）。次のような情報が表示されます。

```
Changing country code could reset channel configuration.
If running in RFM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) y
```

ステップ 4　決定を確認するプロンプトが表示されたら、**Y** を入力します。次のような情報が表示されます。

```
Configured Country..................................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
--More-- or (q)uit
            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . . C C C C x
```

ステップ 5　国コードの設定を確認するには、次のコマンドを入力します。

show country

ステップ 6　コントローラに設定された国コードの使用可能なチャネルの一覧を表示するには、次のコマンドを入力します。

show country channels

次のような情報が表示されます。

```
Configured Country............................ Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6

            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . C C C C x
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

ステップ 8　アクセス ポイントが割り当てられた国を表示するには、次のコマンドを入力します。

show ap summary

次のような情報が表示されます。

```
Number of APs.................................. 2

AP Name  Slots  AP Model          Ethernet MAC        Location          Port    Country
-------- ------ ----------------- -----------------  ----------------  -------
--------
ap1        2   AP1030            00:0b:85:5b:8e:c0  default location     1     US
ap2        2   AIR-AP1242AG-A-K9  00:14:1c:ed:27:fe  default location     1     US
```

ステップ 9　複数の国コードをステップ 3 で入力してある場合には、次の手順に従って特定の国への各アクセス ポイントを割り当てます。

a. 次のいずれかの操作を行います。

- 802.11a および 802.11b/g ネットワークを無効のままにします。
- 802.11a および 802.11b/g ネットワークを再び有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。そのネットワークを再び有効にするには、次のコマンドを入力します。

  config 802.11a enable network

  config 802.11b enable network

  アクセス ポイントを無効にするには、次のコマンドを入力します。

  config ap disable *ap_name*

b. アクセス ポイントを特定の国に割り当てるには、次のコマンドを入力します。

config ap country *code* {*ap_name* | **all**}

選択した国コードが、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制区域に適合していることを確認します。

（注） ネットワークを有効にしてアクセス ポイントを無効にしてから、**config ap country** *code* **all** コマンドを実行すると、指定した国コードが無効にしたアクセス ポイントにのみ設定されます。他のアクセス ポイントは、すべて無視されます。

たとえば、**config ap country mx all** と入力した場合、次のような情報が表示されます。

```
To change country code: first disable target AP(s) (or disable all networks).
  Changing the country may reset any customized channel assignments.
  Changing the country will reboot disabled target AP(s).

 Are you sure you want to continue? (y/n) y

AP Name  Country  Status
---------  --------  --------
ap2  US  enabled (Disable AP before configuring country)
ap1    MX  changed (New country configured, AP rebooting)
```

c. 手順 a. で無効にしたアクセス ポイントを再び有効にするには、次のコマンドを入力します。

config ap enable *ap_name*

ステップ 10　802.11a および 802.11b/g ネットワークをステップ 9 で再び有効にしなった場合には、ここで有効にするために次のコマンドを入力します。

config 802.11a enable network

config 802.11b enable network

ステップ 11　設定を保存するには、次のコマンドを入力します。

save config

アクセス ポイントの -J 規制区域から -U 規制区域への移行

日本政府は、5 GHz 無線周波スペクトルの規制を変更しました。これらの規制によって、802.11a 5-GHz 無線のフィールドがアップグレードできるようになりました。日本では、3 セットの周波数が許可されています。

- J52 = 34（5170 MHz）、38（5190 MHz）、42（5210 MHz）、46（5230 MHz）
- W52 = 36（5180 MHz）、40（5200 MHz）、44（5220 MHz）、48（5240 MHz）
- W53 = 52（5260 MHz）、56（5280 MHz）、60（5300 MHz）、64（5320 MHz）

シスコでは、これらの周波数セットを次の規制区域にまとめました。

- -J 規制区域 = J52
- -P 規制区域 = W52 + W53
- -U 規制区域 = W52

規制区域とは、シスコが世界の周波数の規制を論理的なグループにまとめたものです。たとえば、ヨーロッパの大半の国は -E 規制区域に入ります。シスコのアクセス ポイントは工場で特定の規制区域向けに設定され、この移行プロセス以外によって変更されることはありません。規制区域は無線ごとに割り当てられるので、アクセス ポイントの 802.11a および 802.11b/g 無線は別々の区域に割り当てられることがあります。

（注） コントローラとアクセス　ポイントは、その国で使用できるように設計されていない場合、正しく動作しない場合があります。たとえば、部品番号が AIR-AP1030-A-K9（米国の規制区域に含まれている）のアクセス ポイントは、オーストラリアでは使用できません。その国の規制区域に適合したコントローラとアクセス ポイントを購入することを常に確認してください。

日本の規制では、アクセス ポイントの無線を -J 区域から -U 区域へ移行するようにプログラムされた規制区域が許可されています。日本市場向けの新しいアクセス ポイントには、-P 規制区域に対応した設定の無線が含まれています。-J 無線は、現在販売されていません。現在お使いの -J 無線が新しい -P 無線と共に 1 つのネットワーク内で動作することを確認するには、お使いの -J 無線を -U 区域に移行する必要があります。

国コードは、前の項で説明したように、各国で合法的に使用できるチャネルを定義します。日本で使用できる国コードは、次のとおりです。

- JP：コントローラに接続できるのは、-J 無線のみです。
- J2：コントローラに接続できるのは、-P 無線のみです。
- J3：-U 周波数を使用しますが、-U 無線および -P 無線の両方をコントローラに接続できます。

（注） 移行した後は、J3　国コードを使用する必要があります。お使いのコントローラでソフトウェア リリース 4.1 以降が動作している場合には、前の項で説明したように複数の国コード機能を使用して、J2 と J3 の両方を選択できます。したがって、手動で -P 無線を設定して J3 で対応していないチャネルを使用できます。

日本の規制区域のアクセス ポイントでサポートされているチャネルと電力レベルの一覧については、『Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points』マニュアルを参照してください。

移行に関するガイドライン

アクセス ポイントを -U 規制区域に移行する場合には、次のガイドラインに従ってください。

- 移行できるのは、-J 規制区域および Airespace AS1200 アクセス ポイントをサポートする Cisco Aironet 1130、1200、および 1240 Lightweight アクセス ポイントのみです。その他のアクセス ポイントは移行できません。
- お使いのコントローラとすべてのアクセス ポイントでは、ソフトウェア リリース 4.1 以上またはソフトウェア リリース 3.2.193.0 が動作している必要があります。

（注） ソフトウェア リリース 4.0 はサポートされていません。アクセス ポイントの移行にソフトウェア リリース 3.2.193.0 を使用した場合、ソフトウェア リリース 4.0 にアップグレードできません。アップグレードできるのは、ソフトウェア リリース 4.1 以降または 3.2 ソフトウェアの後続リリースのみです。

- お使いのコントローラを最後にブートしたときに、1 つまたは複数の日本の国コード（JP、J2、または J3）を設定しているはずです。
- -J 規制区域をコントローラに接続するよう設定したアクセス ポイントが、少なくとも 1 つは必要です。
- アクセス ポイントを -U 規制区域から -J 区域へ移行しなおすことはできません。日本政府は、移行の反転を違法であると規定しています。

（注） アクセス ポイントの移行をやり直すことはできません。アクセス ポイントを移行したら、ソフトウェア リリース 4.0 に戻ることはできません。移行済みのアクセス ポイントでは、ソフトウェア リリース 4.0 下の 802.11a 無線が機能できなくなります。

アクセス ポイントの -U 規制区域への移行

コントローラ CLI を使用して、アクセス ポイントを -J 規制区域から -U 規制区域へ移行する手順は、次のとおりです。このプロセスは、コントローラ GUI を使用して実行することはできません。

ステップ 1　ネットワーク内のどのアクセス ポイントが移行できるかを決定するには、次のコマンドを入力します。

show ap migrate

次のような情報が表示されます。

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "J"Reg. Domain

No APs have already been migrated.
```

ステップ 2　802.11a および 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config 802.11a disable network

config 802.11b disable network

ステップ 3　アクセス ポイントの国コードを変更して J3 へ移行するには、次のコマンドを入力します。

config country J3

ステップ 4　アクセス ポイントがリブートして、コントローラに再接続するのを待機します。

ステップ 5　アクセス ポイントを -J 規制区域から -U 規制区域に移行するには、次のコマンドを入力します。

config ap migrate j52w52 {**all** | *ap_name*}

次のような情報が表示されます。

```
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory
Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
Send the AP list and your company name to: migrateapj52w52@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)
```

ステップ 6　移行の決定を確認するプロンプトが表示されたら、**Y** を入力します。

ステップ 7　すべてのアクセス ポイントがリブートして、コントローラに再接続するまで待機します。このプロセスは、アクセス ポイントによっては最長 15 分かかる場合があります。AP1130、AP1200、および AP1240 は 2 回リブートします。それ以外のアクセス ポイントは 1 回リブートします。

ステップ 8　すべてのアクセス ポイントの移行を確認するには、次のコマンドを入力します。

show ap migrate

次のような情報が表示されます。

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9ap1240      "U"Reg. Domain
```

ステップ 9　802.11a および 802.11b/g ネットワークを再び有効にするには、次のコマンドを入力します。

config 802.11a enable network

config 802.11b enable network

ステップ 10　会社名を記載した E メールと移行済みのアクセス ポイントの一覧を、次のメール アドレスへ送信します。migrateapj52w52@cisco.com。ステップ 8 の **show ap migrate** コマンドからの出力を切り取って、電子メールに貼り付けることをお勧めします。

動的周波数選択

Cisco UWN Solution は、無線デバイスがレーダー信号を検出して干渉しないようにする Dynamic Frequency Selection（DFS; 動的周波数選択）の使用を必須とする規制に準拠しています。

5GHz の無線を使用する Lightweight アクセス ポイントが表 7-2 に示す 15 チャネルのいずれかで動作している場合、アクセス ポイントがアソシエートするコントローラは、自動的に DFS を使用して動作周波数を設定します。

DFS 対応の 5GHz 無線用のチャネルを手動で選択した場合、コントローラはそのチャネルでのレーダー アクティビティを 60 秒間チェックします。レーダー アクティビティが検出されない場合、アクセス ポイントは選択されたチャネル上で動作します。選択されたチャネルでレーダー アクティビティが検出された場合、コントローラは自動的に別のチャネルを選択し、30 分後にアクセス ポイントは選択されたチャネルを再試行します。

（注） レーダーが DFS 有効チャネルで検出された後、30 分間は使用できません。

（注） Rogue Location Detection Protocol（RLDP; 不正ロケーション検出プロトコル）は、表 7-2 に示すチャネルではサポートされていません。

（注） 一部の 5GHz チャネルの有効な最大送信電力は、他のチャネルよりも大きくなります。電力が制限されている 5GHz チャネルをランダムに選択した場合、コントローラはそのチャネルの電力制限に合うように送信電力を下げます。

表 7-2　DFS が自動的に有効化される 5GHz チャネル

52（5260MHz）	104（5520MHz）	124（5620MHz）
56（5280MHz）	108（5540MHz）	128（5640MHz）
60（5300MHz）	112（5560MHz）	132（5660MHz）
64（5320MHz）	116（5580MHz）	136（5680MHz）
100（5500MHz）	120（5600MHz）	140（5700MHz）

DFS の使用時、コントローラはレーダー信号の動作周波数を監視します。チャネルでレーダー信号が検出された場合、コントローラは次の手順を実行します。

- アクセス ポイント チャネルを、それ以前の 30 分間にレーダー アクティビティが見られないチャネルに変更します。（レーダー イベントは、30 分後にクリアされます。）コントローラは、ランダムにチャネルを選択します。
- 選択されたチャネルが表 7-2 に示したチャネルのいずれかである場合、新しいチャネルでレーダー信号を 60 秒間スキャンします。新しいチャネルでレーダー信号が検出されない場合、コントローラはクライアントのアソシエーションを承認します。
- レーダー アクティビティが見られたチャネルをレーダー チャネルとして記録し、そのチャネルでのアクティビティを 30 秒間回避します。
- トラップを生成し、ネットワーク マネージャに警告します。

アクセス ポイント上での Location Optimized Monitor Mode（LOMM）の設定

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセス ポイント無線用の 2.4GHz 帯域内で最高 4 つのチャネルで Location Optimized Monitor Mode（LOMM）を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャネル（チャネル 1、6、11 など）のみをスキャンすることができます。

コントローラの GUI または CLI 使用して、監視モード用アクセス ポイントを設定し、このアクセス ポイント無線で LOMM を有効化できます。

GUI を使用した、アクセス ポイント上での Location Optimized Monitor Mode（LOMM）の設定

GUI を使用して LOMM を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。

ステップ 2　監視モードを有効にするアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます。

ステップ 3　AP Mode ドロップダウン ボックスから **Monitor** を選択します。

ステップ 4　**Apply** をクリックして、変更を適用します。

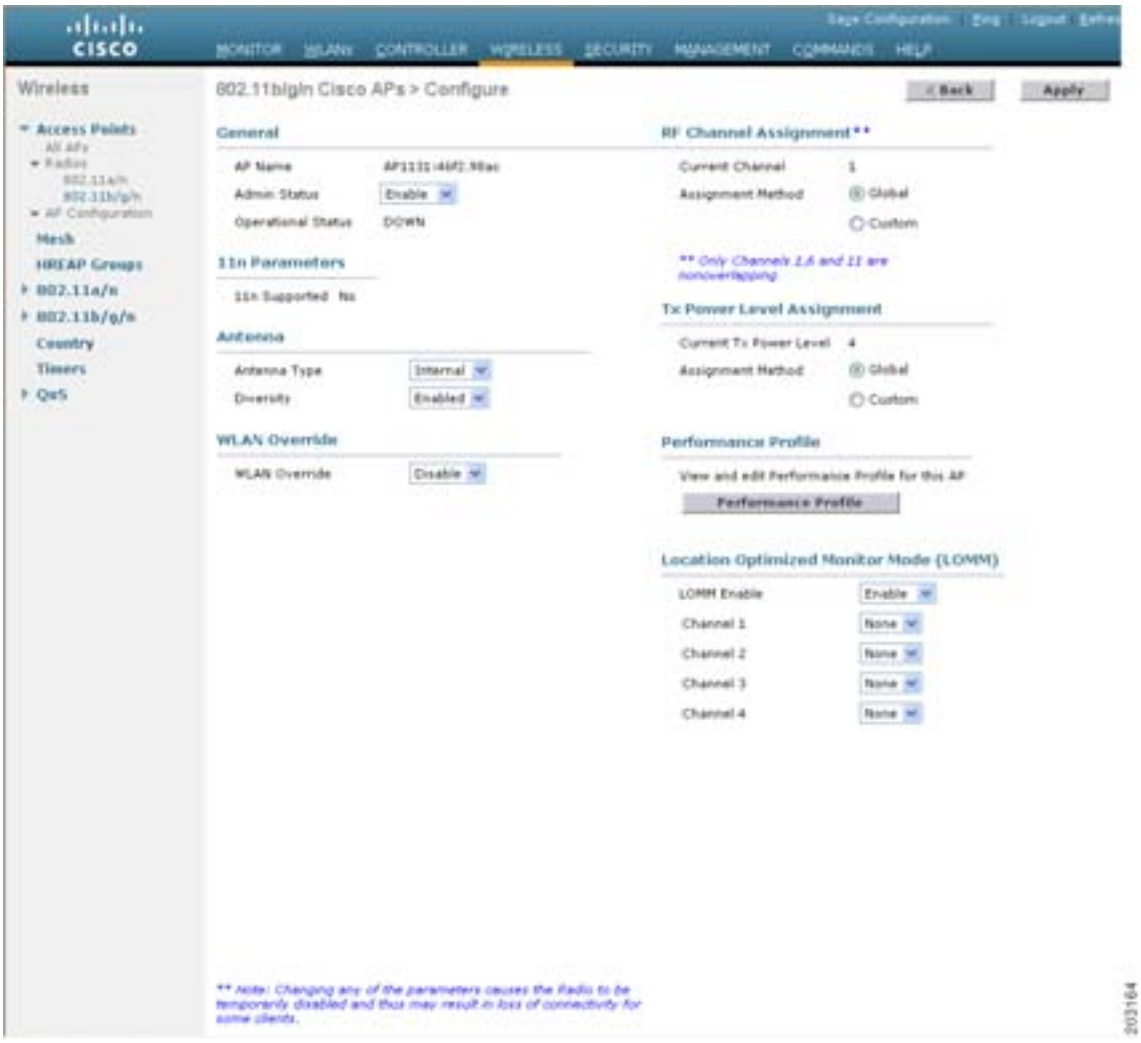
ステップ 5　アクセス ポイントをリブートするという警告が表示されたら、**OK** をクリックします。

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

ステップ 7　**Wireless** > **Access Points** > **Radios** > **802.11b/g/n** の順にクリックして、802.11b/g/n Radios ページを開きます。

ステップ 8　カーソルを目的のアクセス ポイントの青のドロップダウン矢印の上に置いて、**Configure** を選択します。802.11b/g/n Cisco APs > Configure ページが表示されます（図 7-11 を参照）。

図 7-11　802.11b/g/n Cisco APs > Configure ページ



ステップ 9　アクセス ポイント無線を無効化するには、Admin Status ドロップダウン ボックスから **Disable** を選択し、**Apply** をクリックします。

ステップ 10　無線で LOMM を有効化するには、LOMM Enable ドロップダウン ボックスから **Enable** を選択します。

ステップ 11　4 つの Channel ドロップダウン ボックスから、RFID タグの監視対象となるチャネルを選択します。

（注）　タグの監視対象となるチャネルは少なくとも 1 つ設定する必要があります。

ステップ 12　**Apply** をクリックして、変更を適用します。

ステップ 13　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 14　アクセス ポイント無線を再度有効化するには、Admin Status ドロップダウン ボックスから **Enable** を選択し、**Apply** をクリックします。

ステップ 15　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した、アクセス ポイント上での Location Optimized Monitor Mode（LOMM）の設定

コントローラの CLI を使用して LOMM を設定する手順は、次のとおりです。

ステップ 1　監視モード用のアクセス ポイントを設定にするには、次のコマンドを入力します。

config ap mode monitor *Cisco_AP*

ステップ 2　アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。

ステップ 3　変更を保存するには、次のコマンドを入力します。

save config

ステップ 4　アクセス ポイント無線を無効にするには、次のコマンドを入力します。

config 802.11b disable *Cisco_AP*

ステップ 5　このアクセス ポイントで LOMM を有効にし、RFID タグを監視するためのチャネルを 4 つまで割り当てるには、次のコマンドを入力します。

config location 802.11b monitor enable *Cisco_AP channel1 channel2 channel3 channel4*

（注）　米国では、*channel* 変数に 1 から 11 までの任意の値を割り当てられます。その他の国ではさらに多くのチャネルがサポートされています。少なくともチャネルを 1 つ割り当てる必要があります。

（注）　LOMM を無効するには、次のコマンドを入力します。**config location 802.11b monitor disable** *Cisco_AP*.

ステップ 6　アクセス ポイント無線を再度有効にするには、次のコマンドを入力します。

config 802.11b enable *Cisco_AP*

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

ステップ 8　現在の LOMM 構成のステータスを表示するには、次のコマンドを入力します。

show location monitor summary

次のような情報が表示されます。

```
Summary of Location Optimized Monitor Mode(LOMM) AP
AP Name             Ethernet MAC        Status      LOMM Channels
------------------ -------------------- ----------  ----------------
AP1131:46f2.98ac    00:16:46:f2:98:ac   Enabled     1, 6, NA, NA
```

コントローラとアクセス ポイント上の一意のデバイス ID の取得

一意のデバイス ID（UDI）標準は、すべてのシスコ製ハードウェア製品ファミリにわたって、一意に製品を識別するので、ビジネスおよびネットワーク操作を通じてシスコ製品を識別および追跡し、資産運用システムを自動化できます。この標準は、すべての電子的、物理的、および標準のビジネス コミュニケーションにわたって一貫性があります。UDI は、次の 5 つのデータ要素で構成されています。

- 注文可能な製品 ID（PID）
- 製品 ID のバージョン（VID）
- シリアル番号（SN）
- エンティティ名
- 製品の説明

UDI は、工場出荷時にコントローラと Lightweight アクセス ポイントの EEPROM に記録されます。UDI は、GUI または CLI のいずれかを使用して取得できます。

GUI を使用したコントローラとアクセス ポイントの一意のデバイス ID の取得

GUI を使用してコントローラとアクセス ポイントの UDI を取得する手順は、次のとおりです。

ステップ 1　**Controller** > **Inventory** の順にクリックして、Inventory ページを開きます（図 7-12 を参照）。

図 7-12　Inventory ページ

このページには、コントローラ UDI の 5 つのデータ要素が表示されています。

ステップ 2　**Wireless** をクリックして、All APs ページを開きます。

ステップ 3　目的のアクセス ポイントの名前をクリックします。

ステップ 4　All APs > Details ページが表示されたら、**Inventory** タブをクリックして All APs > Details（Advanced）ページを開きます（図 7-13 を参照）。

図 7-13　All APs > Details（Inventory）ページ

このページには、アクセス ポイントのコンポーネント情報が表示されます。

CLI を使用したコントローラとアクセス ポイントの一意のデバイス ID の取得

次のコマンドを入力して、CLI を使用してコントローラとアクセス ポイントの UDI を取得します。

- **show inventory**：コントローラの UDI 文字列を表示します。次のような情報が表示されます。

```
NAME: "Chassis"    , DESCR: "Cisco Wireless Controller"
PID: WS-C3750G-24PS-W24,  VID: V01,  SN: FLS0952H00F
```

- **show inventory ap** *ap_id*：指定したアクセス ポイントの UDI 文字列を表示します。

リンク テストの実行

リンク テストを使用して、2 つのデバイス間の無線リンクの質を決定します。リンク テストの際には、要求と応答の 2 種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なフィールドを記入して、応答タイプ セットを使用して送信者にパケットを返信します。

クライアントからアクセス ポイント方向の無線リンクの質は、送信電力の非対称なディストリビューションによってアクセス ポイントからクライアント方向の質とは異なり、両サイドで感度を受け取る可能性があります。2 種類のリンク テスト（ping テストおよび CCX リンク テスト）を実行できます。

*ping リンク テスト*では、コントローラはクライアントからアクセス ポイント方向でのみリンクの質をテストできます。アクセス ポイントで受信された ping パケットの RF パラメータは、クライアントからアクセス ポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

*CCX リンク テスト*では、コントローラはアクセス ポイントからクライアント方向でもリンクの質をテストできます。コントローラは、リンク テストの要求をクライアントに発行し、クライアントは応答パケットで受信した要求パケットの RF パラメータ［Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）、Signal-to-Noise Ratio（SNR; 信号対雑音比）など］を記録します。リンク テストの要求ロールと応答ロールの両方を、アクセス ポイントとコントローラに実装します。したがって、アクセス ポイントまたはコントローラが CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始でき、同様に CCX v4 クライアントまたは v5 クライアントもアクセス ポイントまたはコントローラに対してリンク テストを開始できます。

コントローラでは、CCX リンク テストに対する下記のリンクの質のメトリックが両方向で表示されます（アウト : アクセス ポイントからクライアント、イン : クライアントからアクセス ポイント）。

- RSSI の形式の信号強度（最小、最大、および平均）
- SNR の形式の信号の質（最小、最大、および平均）
- 再試行されたパケットの合計数
- 単一パケットの最大再試行回数
- 消失パケット数
- 正常に送信されたパケットのデータ レート

コントローラは、方向とは無関係に次のメトリックを表示します。

- リンク テストの要求 / 応答の往復時間（最小、最大、および平均）

コントローラ ソフトウェアでは、CCX バージョン 1 ～ 5 がサポートされています。CCX のサポートは、コントローラ上のすべての WLAN に対して自動的に有効になり、無効にすることはできません。コントローラでは、クライアント データベースにクライアントの CCX バージョンが格納されます。このクライアントの機能を制限するには、これを使用します。クライアントが CCX v4 または v5 をサポートしていない場合、コントローラはクライアント上で ping リンク テストを実行します。クライアントが CCX v4 または v5 をサポートしている場合、コントローラはクライアント上で CCX リンク テストを実行します。クライアントが CCX リンク テストの間にタイムアウトになった場合、コントローラは ping リンク テストに自動的に切り替わります。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

（注）　CCX は、AP1030 ではサポートされません。

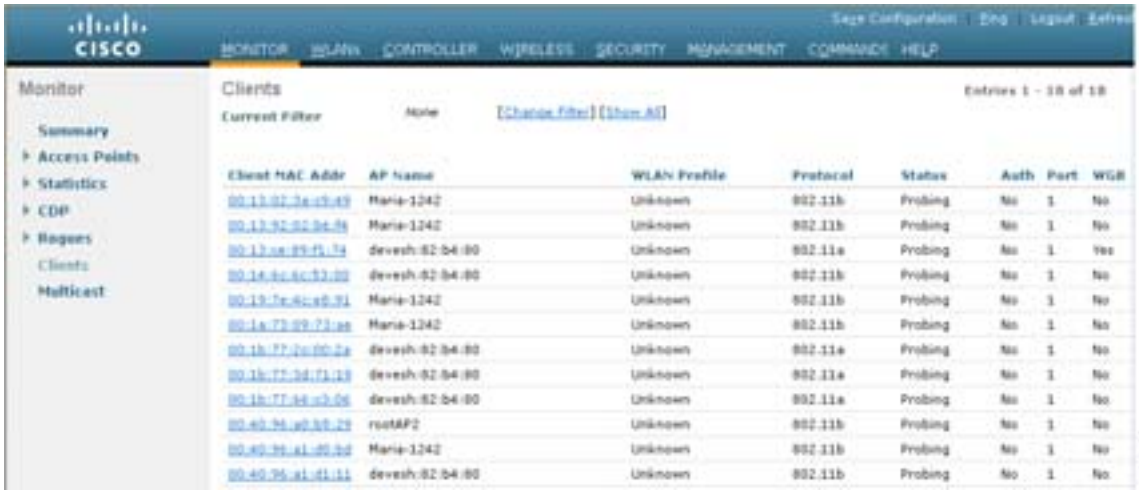
この項の手順に従って、GUI または CLI のいずれかを使用してリンク テストを実行します。

GUI を使用したリンク テストの実行

次の手順に従って、GUI を使用してリンク テストを実行します。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます（図 7-14 を参照）。

図 7-14　Clients ページ



ステップ 2　カーソルを目的のクライアントの青のドロップダウン矢印の上に置いて、**LinkTest** を選択します。リンク テストのページが表示されます（図 7-15 参照）。

（注）　目的のクライアントの MAC アドレスをクリックしてから、Clients > Detail ページの上部にある **Link Test** ボタンをクリックしても、このページにアクセスできます。

図 7-15　Link Test ページ

このページには、CCX リンク テストの結果が表示されます。

（注） クライアントおよびコントローラ（またはそのいずれか）が CCX v4 以降をサポートしていない場合、コントローラは代わりにクライアント上で ping リンク テストを実行し、さらに制限のあるリンク テスト ページが表示されます。

ステップ 3　**OK** をクリックして、Link Test ページを終了します。

CLI を使用したリンク テストの実行

CLI を使用してリンク テストを実行するコマンドは、次のとおりです。

1. リンク テストを実行するには、次のコマンドを入力します。

   linktest *ap_mac*

   コントローラとテストするクライアントの両方で CCX v4 以降を有効化すると、次のような情報が表示されます。

```
CCX Link Test to 00:0d:88:c5:8a:d1.
     Link Test Packets Sent..................................... 20
     Link Test Packets Received................................. 10
     Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
     Link Test Packets round trip time (min/max/average)......... 5ms/20ms/15ms
     RSSI at AP (min/max/average).............................
-60dBm/-50dBm/-55dBm
     RSSI at Client (min/max/average)........................
-50dBm/-40dBm/-45dBm
     SNR at AP (min/max/average)................................ 40dB/30dB/35dB
     SNR at Client (min/max/average)............................ 40dB/30dB/35dB
     Transmit Retries at AP (Total/Maximum)..................... 5/3
     Transmit Retries at Client (Total/Maximum).................. 4/2
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M
108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0   18
0
     Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M
108M
     Packet Count:   0     0     0    0    0    0   0   0     0     2    0    8
0
```

   CCX v4 以降がコントローラまたはテストするクライアントのいずれかで無効化されている場合には、表示される情報が少なくなります。

```
Ping Link Test to 00:0d:88:c5:8a:d1.
        Link Test Packets Sent.......................... 20
        Link Test Packets Received..................... 20
        Local Signal Strength.......................... -49dBm
        Local Signal to Noise Ratio.................... 39dB
```

2. CCX リンク テストおよび ping テストの両方に使用できるリンク テスト パラメータを調整するには、config モードから次のコマンドを入力します。

   config > **linktest frame-size** *size_of_link-test_frames*

   config > **linktest num-of-frame** *number_of_link-test_request_frames_per_test*

Power over Ethernet の設定

LWAPP 有効化アクセス ポイント（AP1131、AP1242 など）が Cisco pre-Intelligent Power Management（pre-IPM）スイッチに接続された電源インジェクタで電源を供給されている場合、*インライン電源*とも呼ばれる Power over Ethernet（PoE）を設定する必要があります。PoE は、GUI または CLI のいずれかを使用して設定できます。

GUI を使用した Power over Ethernet の設定

コントローラ GUI を使用して PoE を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **All APs** の順にクリックし、目的のアクセス ポイントの名前をクリックします。

ステップ 2　All APs > Details ページが表示されたら、**Advanced** タブをクリックして All APs > Details（Advanced）ページを開きます（図 7-16 を参照）。

図 7-16　All APs > Details（Advanced）ページ

ステップ 3　次のいずれかの操作を行います。

- アクセス　ポイントが高出力のシスコ　スイッチで電源を供給されている場合、**Pre-Standard State** チェックボックスをオンにします。これらのスイッチは従来の 6 W 以上の電力を供給しますが、Intelligent Power Management（IPM）機能をサポートしません。次のスイッチが該当します。
  - WS-C3550、WS-C3560、WS-C3750
  - C1880
  - 2600, 2610, 2611, 2621, 2650, 2651,
  - 2610XM、2611XM、2621XM、2650XM、2651XM、2691
  - 2811, 2821, 2851,
  - 3620、3631-telco、3640、3660
  - 3725, 3745,
  - 3825、3845
- 上記のリストに記載されていない電源インジェクタまたはスイッチで電源を供給されている場合、**Pre-Standard State** チェックボックスをオフにします。

ステップ 4　付属のスイッチが IPM をサポートしておらず、電源インジェクタが使用されている場合、**Power Injector State** チェックボックスをオンにします。付属のスイッチが IPM をサポートしている場合、このチェックボックスをオンにする必要はありません。

ステップ 5　前の手順で Power Injector State チェックボックスをオンにした場合、**Power Injector Selection** パラメータが表示されます。電源インジェクタを不注意でバイパスした場合には、このパラメータによってスイッチ ポートを突発的に過負荷にしないよう保護できます。ドロップダウン ボックスから次のオプションのいずれかを選択して、必要な保護のレベルを指定します。

- **Installed**：現在接続されているスイッチ ポートの MAC アドレスを点検して記憶し、電源インジェクタが接続されていることを想定します。ネットワークに従来のシスコ 6 W スイッチが装備されていて、再配置されたアクセス ポイントを強制的にダブルチェックしたときに発生する可能性のある過負荷を避けたい場合に、このオプションを選択します。

（注）　アクセス ポイントが再配置されるたびに、新しいスイッチ ポートの MAC アドレスは記憶した MAC アドレスとの一致に失敗し、アクセス ポイントは低電力モードのままになります。その場合、電源インジェクタの存在を物理的に検証し、このオプションを再選択して新しい MAC アドレスを記憶させます。

- **Override**：このオプションにより、アクセス ポイントは最初に MAC アドレスの一致を検証しなくても、高電力モードで稼動できます。ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されていない場合には、このオプションを選択できます。このオプションのメリットは、アクセス ポイントを再配置した場合、設定しなおさずに高電力モードで稼動を継続できることです。このオプションのデメリットは、アクセス ポイントが直接 6 W スイッチへ接続されていると、過負荷が発生することです。
- **Foreign**：このオプションにより、Injector Switch MAC Address パラメータを表示します。Injector Switch MAC Address パラメータは、記憶した MAC アドレスを手動で変更できるようにします。接続スイッチ ポートの MAC アドレスが分かっていて、Installed オプションを使用して自動的に検出しない場合に、このオプションを選択します。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　**Save Configuration** をクリックして、設定を保存します。

CLI を使用した Power over Ethernet の設定

コントローラ CLI を使用して PoE を設定するには、次のコマンドを使用します。

1. **config ap power injector enable ap installed**

   ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、このコマンドをお勧めします。アクセス ポイントは、電源インジェクタがこの特定のスイッチ ポートに接続されていることを記憶します。アクセス ポイントを再配置する場合、新しい電源インジェクタの存在を検証した後で、このコマンドを再発行する必要があります。

(注)　このコマンドを発行する前に、CDP が有効化されていることを確認します。有効になっていない場合、このコマンドは失敗します。CDP を有効化する方法は、前の項を参照してください。

2. **config ap power injector enable ap override**

   このコマンドにより安全確認の必要がなくなり、アクセス ポイントをどのスイッチ ポートにも接続できるようになります。ネットワークに、12 W アクセス ポイントは直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されていない場合には、このコマンドを使用できます。アクセス ポイントは、電源インジェクタが常に接続されていることを前提としています。アクセス ポイントを再配置した場合も、電源インジェクタの存在が前提となったままです。

点滅する LED の設定

コントローラ ソフトウェア リリース 4.0 以降では、アクセス ポイントの LED を点滅させて、その場所を示すことができます。すべての IOS Lightweight アクセス ポイントがこの機能をサポートしています。

次のコマンドを使用して、LED の点滅をコントローラの Privileged Exec モードから設定します。

(注)　コマンドがコントローラで入力されたか TELNET/SSH CLI セッションで入力されたかに関係なく、これらのコマンドの出力はコントローラ コンソールへのみ送信されます。

1. コントローラを有効にして、コマンドを CLI からアクセス ポイントへ送信するには、次のコマンドを入力します。

   debug ap enable *Cisco_AP*

2. 特定のアクセス ポイントの LED を指定した秒数間点滅させるには、次のコマンドを入力します。

   debug ap command "led flash *seconds***"** *Cisco_AP*

   seconds パラメータには、1 ～ 3600 秒の値を入力できます。

3. 特定のアクセス ポイントの LED 点滅を無効にするには、次のコマンドを入力します。

   debug ap command "led flash disable" *Cisco_AP*

   このコマンドは、LED 点滅を直ちに無効化します。たとえば、前のコマンドを実行してから（60 秒に設定した *seconds* パラメータを使用して）わずか 20 秒で LED 点滅を無効にした場合、アクセス ポイントの LED は直ちに点滅を停止します。

クライアントの表示

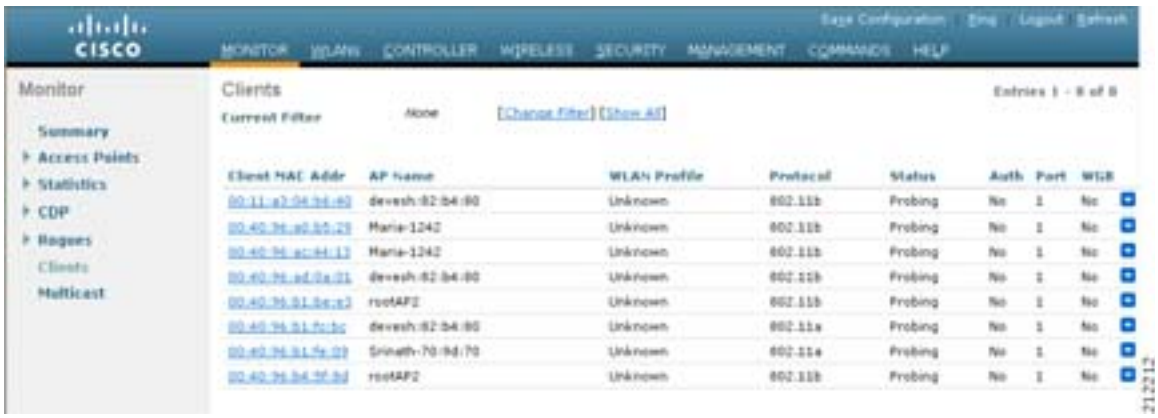
コントローラの GUI または CLI を使用してコントローラのアクセス ポイントにアソシエートされているクライアントに関する情報を表示できます。

GUI を使用したクライアントの表示

GUI を使用して、クライアントの情報を表示する手順は、次のとおりです。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます（図 7-17 を参照）。

図 7-17　Clients ページ



このページには、コントローラのアクセス ポイントにアソシエートされたすべてのクライアントのリストが表示されています。それには、各クライアントに関する次の情報が記載されています。

- クライアントの MAC アドレス
- クライアントがアソシエートされているアクセス ポイントの名前
- クライアントが使用する WLAN の名前
- クライアントのタイプ（802.11a、802.11b、802.11g、または 802.11n）

（注）　802.11n クライアントが 802.11n を有効にした 802.11a 無線にアソシエートされている場合、クライアントのタイプは 802.11n(5) と表示されます。802.11n クライアントが 802.11n を有効にした 802.11b/g 無線にアソシエートされている場合、クライアントのタイプは 802.11n(2.4) と表示されます。

- クライアント接続のステータス
- クライアントの認可ステータス
- クライアントがアソシエートされているアクセス ポイントのポート数
- クライアントが WGB かどうかの表示

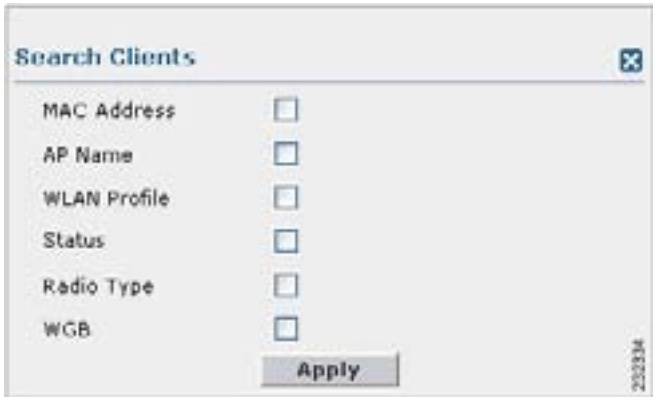
（注）　WGB ステータスの詳細は、「Cisco ワークグループ ブリッジ」の項（P. 7-22）を参照してください。

（注） クライアントを削除したり無効にする場合には、カーソルをそのクライアントの青のドロップダウン矢印の上に置いて、**Remove** または **Disable** を選択します。クライアントとアクセス ポイントの間の接続をテストするには、そのクライアントの青いドロップダウンの矢印の上にカーソルを置いて、**Link Test** を選択します。

ステップ 2　フィルタを作成して、特定の基準（MAC アドレス、ステータス、無線のタイプなど）を満たすクライアントのみを表示する手順は、次のとおりです。

a. **Change Filter** をクリックして、Search Clients ページを開きます（図 7-18 を参照）。

図 7-18　Search Clients ページ



b. 次のチェックボックスの 1 つまたは複数をオンにして、クライアントを表示する際に使用する基準を指定します。

- **MAC Address**：クライアントの MAC アドレスを入力します。

（注） MAC Address フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、MAC Address フィルタは自動的に無効になります。

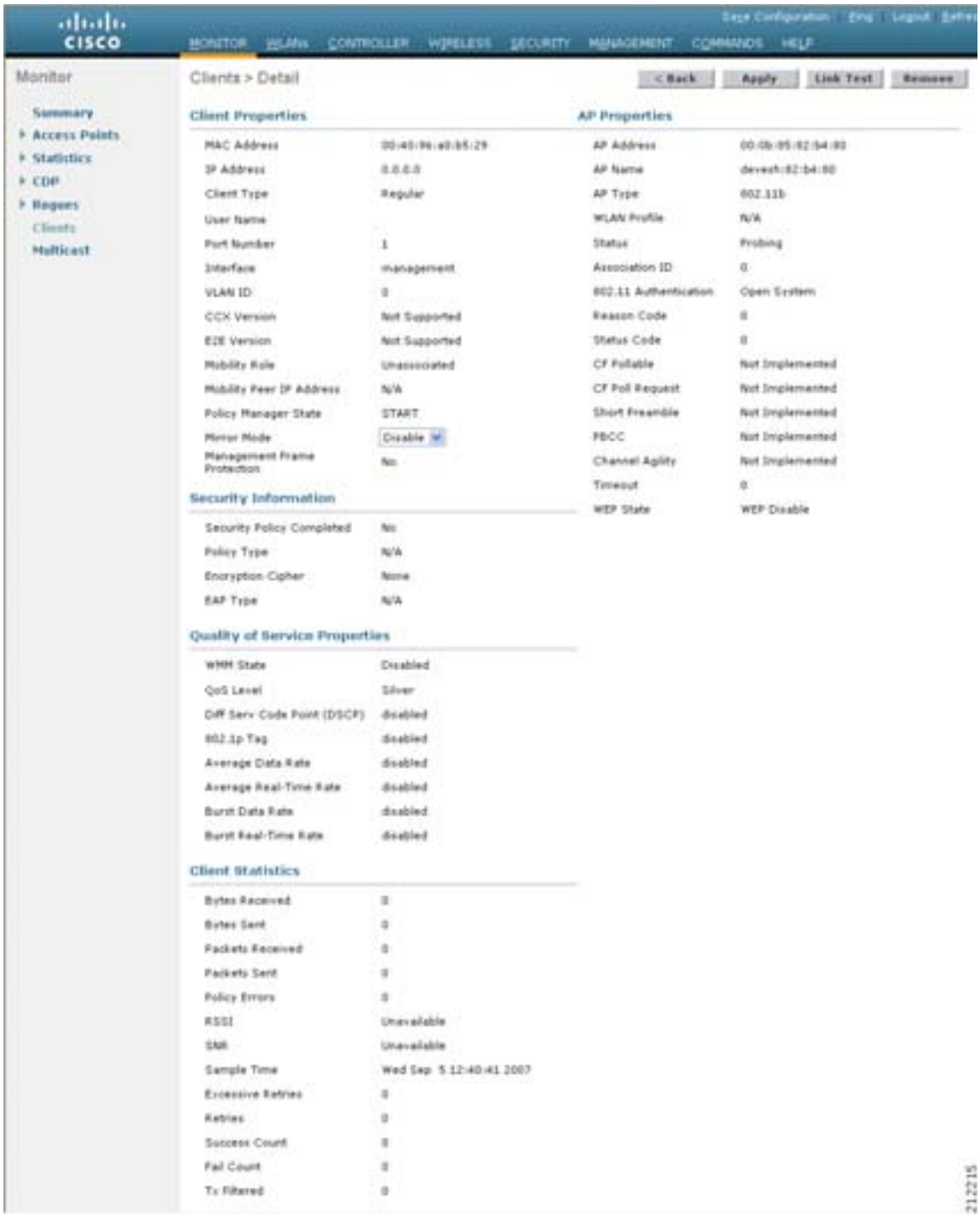
- **AP Name**：アクセス ポイントの名前を入力します。
- **WLAN Profile**：WLAN の名前を入力します。
- **Status**：**Associated**、**Authenticated**、**Excluded**、**Idle**、または **Probing** チェックボックス（複数可）をオンにします。
- **Radio Type**：**802.11a**、**802.11b**、**802.11g**、**802.11n**、または **Mobile** を選択します。
- **WGB**：コントローラのアクセス ポイントにアソシエートされた WGB クライアントを表示します。

c. **Apply** をクリックして、変更を適用します。Clients ページの上部にある Current Filter パラメータは、現在適用されているフィルタを示しています。

（注） フィルタを削除してクライアント リスト全体を表示するには、**Show All** をクリックします。

ステップ 3　特定のクライアントの詳細情報を表示するには、クライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます（図 7-19 を参照）。

図 7-19　Clients > Detail ページ



このページには、次の情報が表示されます。

- クライアントの一般的なプロパティ
- クライアントのセキュリティ設定
- クライアントの QoS のプロパティ

- クライアントの統計
- クライアントがアソシエートされているアクセス ポイントのプロパティ

CLI を使用したクライアントの表示

次の CLI コマンドを使用して、クライアント情報を表示します。

- 特定のアクセス ポイントにアソシエートされたクライアントを表示するには、次のコマンドを入力します。

  show client ap {**802.11a** | **802.11b**} *Cisco_AP*

  次のような情報が表示されます。

```
MAC Address         AP Id   Status          WLAN Id Authenticated
-----------------   ------  -------------   ---------  -------------
00:13:ce:cc:8e:b8   1     Associated      1          No
```

- コントローラのアクセス ポイントにアソシエートされたクライアントの概要を表示するには、次のコマンドを入力します。

  show client summary

  次のような情報が表示されます。

```
Number of Clients.............................. 6

MAC Address       AP Name           Status        WLAN Auth Protocol Port Wired
----------------- ----------------- ------------- ---- ---- -------- ---- -----

00:13:ce:cc:8e:b8 Maria-1242        Probing       N/A  No   802.11a 1    No
00:40:96:a9:a0:a9 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:ac:44:13 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:b1:fe:06 CJ-AP1            Probing       N/A  No   802.11a 1    No
00:40:96:b1:fe:09 CJ-AP1         Probing    N/A  No   802.11a 1    No
```

- 特定のクライアントの詳細情報を表示するには、次のコマンドを入力します。

  show client detail *client_mac*

  次のような情報が表示されます。

```
Client MAC Address............................. 00:40:96:b2:a3:44
Client Username ............................... N/A
AP MAC Address................................. 00:18:74:c7:c0:90
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:18:74:c7:c0:9f
Channel........................................ 56
IP Address..................................... 192.168.10.28
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. 5
Client E2E version............................. No E2E support
Diagnostics Capability......................... Supported
S69 Capability................................. Supported
Mirroring...................................... Disabled
QoS Level...................................... Silver
...
```

CHAPTER 8

コントローラ ソフトウェアと設定の管理

この章では、コントローラにおける設定とソフトウェア バージョンの管理方法について説明します。この章の内容は、次のとおりです。

コントローラ ソフトウェアのアップグレード

コントローラのソフトウェアをアップグレードすると、コントローラのアソシエート アクセス ポイントも自動的にアップグレードされます。アクセス ポイントがソフトウェアをロードしている場合、アクセス ポイントの各 LED は連続して点滅します。最大 10 個のアクセス ポイントをコントローラから同時にアップグレードできます。

注意　このプロセスの実行時に、コントローラまたは任意のアクセス ポイントの電源を切らないでください。電源を切ると、ソフトウェア イメージが破損する場合があります。多数のアクセス ポイントを含むコントローラをアップグレードするには、ネットワークのサイズにもよりますが、最大で 30 分かかる場合があります。ただし、ソフトウェア リリース 4.0.206.0 以降でサポートされている場合、同時にアップグレードされるアクセス ポイント数が増加したため、アップグレードの時間が大幅に短縮されました。アクセス ポイントの電源は入れたままにしておく必要があります。また、アップグレード時にコントローラをリセットしてはなりません。

コントローラ ソフトウェアのアップグレードに関するガイドライン

ソフトウェア リリース 5.0 にコントローラをアップグレードする前に、次のガイドラインに従ってください。

  - ソフトウェアのアップグレードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。
  - コントローラ ソフトウェア リリース 5.0 は、32MB よりサイズが大きいので、TFTP サーバで 32MB より大きいファイルがサポートされていることを確認する必要があります。このサイズのファイルをサポートする TFTP サーバとして、tftpd32、および WCS 内の TFTP サーバがあります。5.0 コントローラ ソフトウェアをダウンロードする際に TFTP サーバでこのサイズのファイルがサポートされていない場合、次のエラー メッセージが表示されます。「TFTP failure while storing in flash」
  - サービス ポート経由でアップグレードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
  - ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
  - サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

- お使いのコントローラでソフトウェア リリース 3.2.195.10（またはそれ以降の 3.2 リリース）、4.0.206.0（またはそれ以降の 4.0 リリース）、4.1.171.0（またはそれ以降の 4.1 リリース）、または 4.2.61.0（またはそれ以降の 4.2 リリース) が動作している場合には、コントローラをソフトウェア リリース 5.0 に直接アップグレードできます。お使いのコントローラで以前の 3.2 または 4.0 リリースが動作している場合には、コントローラを中間リリースにアップグレードしてから 5.0 にアップグレードしてください。表 8-1 には、ソフトウェア リリース 5.0 をダウンロードする前にアップグレードする必要のあるパスが記載されています。

（注）　お使いのコントローラで現在動作しているソフトウェア　　リリースを確認するには、**Monitor** をクリックして、コントローラの GUI 上で Controller Summary の下にある Software Version フィールドを見るか、コントローラの CLI に **show sysinfo** と入力してください。

表 8-1　コントローラ ソフトウェア リリース 5.0 へのアップグレード パス

現在のソフトウェア リリース	5.0 ソフトウェアへのアップグレード パス
3.2.78.0	5.0 へアップグレードする前に、4.0.206.0 以降の 4.0 リリースへアップグレードします。
3.2.116.21	
3.2.150.10	
3.2.171.6	
3.2.193.5	
3.2.195.10 以降の 3.2 リリース	5.0 へ直接アップグレードできます。
4.0.155.5	5.0 へアップグレードする前に、4.0.206.0 以降の 4.0 リリースへアップグレードします。
4.0.179.11	
4.0.206.0 以降の 4.0 リリース	5.0 へ直接アップグレードできます。
4.1.171.0 以降の 4.1 リリース	5.0 へ直接アップグレードできます。
4.2.61.0 以降の 4.2 リリース	5.0 へ直接アップグレードできます。

（注） 中間ソフトウェアリリースにコントローラをアップグレードする場合、5.0 ソフトウェアをインストールする前に、コントローラに接続されているすべてのアクセス ポイントが中間リリースにアップグレードされるまで待ってください。大規模なネットワークでは、各アクセス ポイントでソフトウェアをダウンロードするのに多少時間がかかる場合があります。

- コントローラに Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルもインストールすることをお勧めします。ブート ソフトウェアの欠陥はこのファイルにより解決され、このファイルはコントローラが適切に動作していることを確認する際に必要です。ER.aes ファイルはすべてのコントローラのプラットフォームにインストールできます。

（注） ブートローダは、2106 コントローラではアップグレードできません。

（注） ER.aes ファイルは、コントローラ ソフトウェア ファイルに依存しません。どのコントローラ ソフトウェア ファイルも、すべての ER.aes ファイルで動作させることができます。ただし、最新のブート ソフトウェア ファイル（5.0 ER.aes）をインストールすると、新旧ブート ソフトウェア ER.aes ファイルすべてに含まれるブート ソフトウェアの修正を確実にインストールできます。

注意 あるリリースから別のリリースへダウングレードする必要がある場合、現在のリリースからの設定が失われる可能性があります。回避策として、バックアップ サーバに保存されている以前のコントローラ設定ファイルをリロードするか、コントローラを再設定する方法があります。

GUI を使用したコントローラ ソフトウェアのアップグレード

GUI を使用してコントローラ ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1　コントローラ設定ファイルをサーバにアップロードしてバックアップします。

（注）　コントローラの設定ファイルをバックアップしてから、コントローラ ソフトウェアをアップグレードするよう強くお勧めします。バックアップしない場合には、コントローラを手動で設定してください。

ステップ 2　802.11a および 802.11b/g ネットワークを無効にします。

ステップ 3　コントローラ上のすべての WLAN を無効にします。

ステップ 4　Software Center on Cisco.com から 5.0 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルを取得する手順は、次のとおりです。

a. 次の URL をクリックして、Software Center にアクセスします。
   http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml
b. **Wireless Software** をクリックします。
c. **Wireless LAN Controllers** をクリックします。
d. **Standalone Controllers**、**Wireless Integrated Routers**、または **Wireless Integrated Switches** をクリックします。
e. コントローラの名前をクリックします。
f. **Wireless LAN Controller Software** をクリックします。
g. コントローラ ソフトウェア リリースをクリックします。
h. ファイル名（*filename*.aes）をクリックします。
i. **Download** をクリックします。
j. シスコのエンド ユーザ ソフトウェアのライセンス契約を読んでから、**Agree** をクリックします。
k. お使いのハード ドライブにファイルを保存します。
l. 手順 a. ～ k. を繰り返し、残りのファイル（5.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイル）をダウンロードします。

ステップ 5　コントローラ ソフトウェア ファイル（*filename*.aes）および Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルを TFTP サーバのデフォルト ディレクトリにコピーします。

ステップ 6　**Commands** > **Download File** の順にクリックして、Download File to Controller ページを開きます（図 8-1 を参照）。

図 8-1　Download File to Controller ページ

ステップ 7　File Type ドロップダウン ボックスから、**Code** を選択します。

ステップ 8　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 9　Maximum Retries フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を Maximum Retries フィールドに、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を Timeout フィールドに入力します。

ステップ 10　File Path フィールドに、ソフトウェアのディレクトリ パスを入力します。

ステップ 11　File Name フィールドに、コントローラ ソフトウェア ファイル（*filename*.aes）の名前を入力します。

ステップ 12　**Download** をクリックして、ソフトウェアをコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 13　ステップ 6 ～ ステップ 12 を繰り返し、残りのファイル（5.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイル）をダウンロードします。

ステップ 14　ダウンロードが完了した後、**Reboot** の順にクリックします。

ステップ 15　変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。

ステップ 16　**OK** をクリックし、変更内容を確定してコントローラをリブートします。

ステップ 17　コントローラのリブート後、WLAN を再び有効にします。

ステップ 18　802.11a および 802.11b/g ネットワークを再度有効にします。

ステップ 19　必要な場合、最新の設定ファイルをコントローラにリロードします。

ステップ 20　5.0 コントローラ ソフトウェアがコントローラにインストールされたことを確認するには、コントローラの GUI の **Monitor** をクリックして Controller Summary の下の Software Version フィールドを見ます。

ステップ 21 Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルがコントローラにインストールされていることを確認するには、コントローラの CLI に **show sysinfo** コマンドを入力して Bootloader Version フィールドを見ます。

（注） このコマンドを使用して 2106 を除くすべてのコントローラのブートローダのバージョンを確認できます。2106 コントローラでは、ブートローダをアップグレードできません。

CLI を使用したコントローラ ソフトウェアのアップグレード

CLI を使用してコントローラ ソフトウェアをアップグレードする手順は、次のとおりです。

ステップ 1 コントローラ設定ファイルをサーバにアップロードしてバックアップします。

（注） コントローラの設定ファイルをバックアップしてから、コントローラ ソフトウェアをアップグレードするよう強くお勧めします。バックアップしない場合には、コントローラを手動で設定してください。

ステップ 2 802.11a および 802.11b/g ネットワークを無効にします。

ステップ 3 コントローラ上のすべての WLAN を無効にします（**config wlan disable** *wlan_id* コマンドを使用）。

ステップ 4 Software Center on Cisco.com から 5.0 コントローラ ソフトウェアおよび Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルを取得する手順は、次のとおりです。

a. 次の URL をクリックして、Software Center にアクセスします。
   http://www.cisco.com/kobayashi/sw-center/sw-wireless.shtml
b. **Wireless Software** をクリックします。
c. **Wireless LAN Controllers** をクリックします。
d. **Standalone Controllers**、**Wireless Integrated Routers**、または **Wireless Integrated Switches** をクリックします。
e. コントローラの名前をクリックします。
f. **Wireless LAN Controller Software** をクリックします。
g. コントローラ ソフトウェア リリースをクリックします。
h. ファイル名（*filename*.aes）をクリックします。
i. **Download** をクリックします。
j. シスコのエンド ユーザ ソフトウェアのライセンス契約を読んでから、**Agree** をクリックします。
k. お使いのハード ドライブにファイルを保存します。
l. 手順 a. ～ k. を繰り返し、残りのファイル（5.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイル）をダウンロードします。

ステップ 5　コントローラ ソフトウェア ファイル（*filename*.aes）および Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルを TFTP サーバのデフォルト ディレクトリにコピーします。

ステップ 6　コントローラの CLI にログインします。

ステップ 7　**ping** *server-ip-address* を入力して、コントローラが TFTP サーバと通信できることを確認します。

ステップ 8　**transfer download start** コマンドを入力し、プロンプトに **n** と応答して現在のダウンロード設定を表示します。次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Code
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename............................ xxx.aes

Are you sure you want to start? (y/n) n
Transfer Canceled
```

ステップ 9　必要に応じて、次のコマンドを入力して、ダウンロードの設定を変更します。

transfer download mode tftp

transfer download datatype code

transfer download serverip *tftp-server-ip-address*

transfer download filename *filename*

transfer download path *tftp-server-path-to-file*

（注）　TFTP サーバ上のパス名は、サーバのデフォルト ディレクトリまたはルート ディレクトリに対して相対的です。たとえば、Solarwinds TFTP サーバの場合、このパスは "/" となります。

ステップ 10　**transfer download start** と入力して、更新後の設定を表示します。プロンプトに **y** と応答して、現在のダウンロード設定を確認し、ソフトウェアのダウンロードを開始します。次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Code
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename............................ xxx.aes

Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
TFTP receive complete... extracting components.
Writing new bootloader to flash.
Making backup copy of RTOS.
Writing new RTOS to flash.
Making backup copy of Code.
Writing new Code to flash.
TFTP File transfer operation completed successfully.
  Please restart the switch (reset system) for update to complete.
```

ステップ 11　ステップ 8 ～ ステップ 11 を繰り返し、残りのファイル（5.0 コントローラ ソフトウェアまたは Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイル）をダウンロードします。

ステップ 12　**reset system** と入力して不揮発性 NVRAM に対するコードのアップデートを保存し、コントローラをリブートします。コントローラのブートアップ プロセスが完了します。

ステップ 13　**config wlan enable** *wlan_id* と入力して、WLAN を再度有効にします。

ステップ 14　802.11a および 802.11b/g ネットワークを再度有効にします。

ステップ 15　必要な場合、最新の設定ファイルをコントローラにリロードします。

ステップ 16　5.0 コントローラ ソフトウェアがコントローラにインストールされたことを確認するには、**show sysinfo** と入力して Product Version フィールドを見ます。

ステップ 17　Cisco Unified Wireless Network Controller Boot Software 5.0 ER.aes ファイルがコントローラにインストールされていることを確認するには、**show sysinfo** と入力して Bootloader Version フィールドを見ます。

（注）　このコマンドを使用して 2106 を除くすべてのコントローラのブートローダのバージョンを確認できます。2106 コントローラでは、ブートローダをアップグレードできません。

コントローラとのファイルのやり取り

コントローラには、さまざまなファイルをアップロードまたはダウンロードするための組み込みユーティリティがあります。コントローラ GUI または CLI を使用してファイルをインポートするには、次の項の指示に従ってください。

デバイスの証明書のダウンロード

各無線デバイス（コントローラ、アクセス ポイント、およびクライアント）には独自のデバイスの証明書があります。たとえば、コントローラには、Cisco によりインストールされたデバイスの証明書が付属しています。この証明書は、ローカル EAP 認証時に無線クライアントの認証を行うために、EAP-FAST（PAC を使用していない場合）、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用されます。ただし、ご自身のベンダー固有のデバイスの証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

（注） ローカル EAP の設定の詳細は、「ローカル EAP の設定」の項（P. 5-39）を参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、ベンダー固有のデバイスの証明書をコントローラにダウンロードします。ただし、開始する前に、証明書のダウンロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション　システム　ネットワーク　ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

（注） コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

GUI を使用したデバイスの証明書のダウンロード

GUI を使用してコントローラにデバイスの証明書をダウンロードする手順は、次のとおりです。

ステップ 1　デバイスの証明書を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 2　**Commands** > **Download File** の順にクリックして、Download File to Controller ページを開きます（図 8-2 を参照）。

図 8-2　Download File to Controller ページ

ステップ 3　File Type ドロップダウン ボックスから、**Vendor Device Certificate** を選択します。

ステップ 4　Certificate Password フィールドに、証明書を保護するために使用されたパスワードを入力します。

ステップ 5　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 6　Maximum Retries フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが証明書のダウンロードを試行する最大回数を Maximum Retries フィールドに、証明書のダウンロードを試行する時間の合計（秒単位）を Timeout フィールドに入力します。

ステップ 7　File Path フィールドに、証明書のディレクトリ パスを入力します。

ステップ 8　File Name フィールドに、証明書の名前を入力します。

ステップ 9　**Download** をクリックして、デバイスの証明書をコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 10　ダウンロードが完了した後、**Commands** > **Reboot** > **Reboot** をクリックします。

ステップ 11　変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。

ステップ 12　**OK** をクリックし、変更内容を確定してコントローラをリブートします。

CLI を使用したデバイスの証明書のダウンロード

CLI を使用してコントローラにデバイスの証明書をダウンロードする手順は、次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**transfer download datatype eapdevcert** と入力します。

ステップ 3　**transfer download certpassword** *password* と入力します。

ステップ 4　**transfer upload serverip** *tftp-server-ip-address* と入力します。

ステップ 5　**transfer download filename** *filename*.pem と入力します。

ステップ 6　**transfer download start** と入力して更新した設定を表示し、現在のダウンロード設定を確認するプロンプトが表示されたら **y** と応答して、ダウンロード プロセスを開始します。このダウンロード コマンドの出力例は、次のとおりです。

```
Mode..................................... TFTP
Data Type................................ Vendor Dev Cert
TFTP Server IP........................... 10.10.10.4
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /tftpboot/username/
TFTP Filename............................ filename.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use the new certificate.
```

ステップ 7　**reset system** と入力して、コントローラをリブートします。

ステップ 8　コントローラがリブートしたら、**show certificates local-auth** と入力して証明書がインストールされていることを確認します。

CA 証明書のダウンロード

コントローラとアクセス ポイントには、デバイスの証明書の署名と確認に使用される Certificate Authority（CA; 認証局）の証明書があります。コントローラには、Cisco によりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時に無線クライアントの認証を行うために、EAP-FAST（PAC を使用していない場合）、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用できます。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。

（注）　ローカル EAP の設定の詳細は、「ローカル EAP の設定」の項（P. 5-39）を参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、CA 証明書をコントローラにダウンロードします。ただし、開始する前に、証明書のダウンロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション　システム　ネットワーク　ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。

- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

（注） コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

GUI を使用した CA 証明書のダウンロード

GUI を使用してコントローラに CA 証明書をダウンロードする手順は、次のとおりです。

ステップ 1　CA 証明書を TFTP サーバ上のデフォルト ディレクトリにコピーします。

ステップ 2　**Commands** > **Download File** の順にクリックして、Download File to Controller ページを開きます（図 8-3 を参照）。

図 8-3　Download File to Controller ページ

ステップ 3　File Type ドロップダウン ボックスから、**Vendor CA Certificate** を選択します。

ステップ 4　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 5　Maximum Retries フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが証明書のダウンロードを試行する最大回数を Maximum Retries フィールドに、証明書のダウンロードを試行する時間の合計（秒単位）を Timeout フィールドに入力します。

ステップ 6　File Path フィールドに、証明書のディレクトリ パスを入力します。

ステップ 7　File Name フィールドに、証明書の名前を入力します。

ステップ 8　**Download** をクリックして、CA 証明書をコントローラへダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 9　ダウンロードが完了した後、**Commands** > **Reboot** > **Reboot** をクリックします。

ステップ 10　変更を保存するように求めるプロンプトが表示されたら、**Save and Reboot** をクリックします。

ステップ 11　**OK** をクリックし、変更内容を確定してコントローラをリブートします。

CLI を使用した CA 証明書のダウンロード

CLI を使用してコントローラに CA 証明書をダウンロードする手順は、次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**transfer download datatype eapcacert** と入力します。

ステップ 3　**transfer download serverip** *tftp-server-ip-address* と入力します。

ステップ 4　**transfer download filename** *filename*.pem と入力します。

ステップ 5　**transfer download start** と入力して更新した設定を表示し、現在のダウンロード設定を確認するプロンプトが表示されたら **y** と応答して、ダウンロード プロセスを開始します。このダウンロード コマンドの出力例は、次のとおりです。

```
Mode..................................... TFTP
Data Type................................ Vendor CA Cert
TFTP Server IP........................... 10.10.10.4
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /tftpboot/username/
TFTP Filename............................ filename.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
Reboot the switch to use the new certificate.
```

ステップ 6　**reset system** と入力して、コントローラをリブートします。

ステップ 7　コントローラがリブートしたら、**show certificates local-auth** と入力して証明書がインストールされていることを確認します。

PAC のアップロード

Protected Access Credential（PAC）は、自動的または手動でプロビジョニングされる資格情報で、EAP-FAST 認証時にローカル EAP 認証で相互認証を実行するために使用されます。手動の PAC プロビジョニングが有効になっている場合、PAC ファイルはコントローラ上で手動で生成されます。

（注）　ローカル EAP の設定の詳細は、「ローカル EAP の設定」の項（P. 5-39）を参照してください。

この項の手順に従って、GUI または CLI のいずれかを使用して、コントローラから PAC を生成してロードします。ただし、開始する前に、PAC アップロードに TFTP サーバを使用できることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でアップロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション　システム　ネットワーク　ポートを経由してアップロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

GUI を使用した PAC のアップロード

GUI を使用してコントローラから PAC をアップロードする手順は、次のとおりです。

ステップ 1　**Commands** > **Upload File** をクリックして、Upload File from Controller ページを開きます（図 8-4 を参照）。

図 8-4　Upload File from Controller ページ

ステップ 2　File Type ドロップダウン ボックスから、**PAC (Protected Access Credential)** を選択します。

ステップ 3　User フィールドに、PAC を使用するユーザ名を入力します。

ステップ 4　Validity フィールドに、PAC が有効である日数を入力します。デフォルトの設定は、ゼロ（0）です。

ステップ 5　Password フィールドおよび Confirm Password フィールドに、PAC を保護するためのパスワードを入力します。

ステップ 6　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 7　File Path フィールドに、PAC のディレクトリ パスを入力します。

ステップ 8　File Name フィールドに、PAC ファイルの名前を入力します。PAC ファイルには .pac 拡張子が付いています。

ステップ 9　**Upload** をクリックして、コントローラから PCA をアップロードします。アップロードのステータスを示すメッセージが表示されます。

ステップ 10　無線クライアントの手順に従って、クライアント デバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。

CLI を使用した PAC のアップロード

CLI を使用してコントローラから PAC をアップロードする手順は、次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**transfer upload datatype pac** と入力します。

ステップ 3　**transfer upload pac** *username validity password* と入力します。

ステップ 4　**transfer upload serverip** *tftp-server-ip-address* と入力します。

ステップ 5　**transfer upload filename** *manual*.pac と入力します。

ステップ 6　**transfer upload start** と入力して更新した設定を表示し、現在の設定を確認するプロンプトが表示されたら **y** と応答して、アップロード プロセスを開始します。このコマンドの出力例は、次のとおりです。

```
Mode..................................... TFTP
TFTP Server IP........................... 10.10.10.4
TFTP Path................................ /tftpboot/username/
TFTP Filename............................ manual.pac
Data Type................................ PAC
PAC User................................. username
PAC Validity............................. 10 days
PAC Password............................. password

Are you sure you want to start? (y/N) y

PAC transfer starting.

File transfer operation completed successfully.
```

ステップ 7　無線クライアントの手順に従って、クライアント デバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。

設定ファイルのアップロードおよびダウンロード

お使いのコントローラのソフトウェアをアップグレードする前に、コントローラの設定ファイルをサーバにアップロードして保存することをお勧めします。その上で新しいコントローラ ソフトウェアをインストールすると、設定ファイルをコントローラにダウンロードできます。

（注） コントローラの設定ファイルをコントローラのソフトウェアのアップグレード前に保存してない場合は、手動でコントローラを再設定する必要があります。

コントローラ ソフトウェア リリース 4.2 以降では、コントローラのブートアップ設定ファイルがバイナリ形式ではなく、Extensible Markup Language（XML; 拡張マークアップ言語）形式で保存されます。したがって、ソフトウェア リリース 4.2 以降が稼動しているコントローラにバイナリの設定ファイルをダウンロードすることはできません。ただし、以前のソフトウェア リリースを 4.2 以降にアップグレードする際には、設定ファイルが移行されて XML に変換されます。

（注） 設定ファイルを変更しないようにしてください。設定ファイルを変更してからそのファイルをコントローラへダウンロードすると、コントローラがリブートしながら設定パラメータをデフォルト値に戻す際に、コントローラは巡回冗長検査（CRC）エラーを表示します。

設定ファイルのアップグレード

GUI または CLI のいずれかを使用して、設定ファイルをアップロードできます。

GUI を使用した設定ファイルのアップロード

コントローラ GUI を使用して設定ファイルをアップロードする手順は、次のとおりです。

ステップ 1　**Commands** > **Upload File** の順にクリックして、Upload File from Controller ページを開きます（図 8-5 を参照）。

図 8-5　Upload File from Controller ページ

ステップ 2　File Type ドロップダウン ボックスから **Configuration** を選択します。

ステップ 3　暗号化を有効にするには、**Configuration File Encryption** チェックボックスをオンにして暗号キーを入力します。

ファイルの暗号化により、設定ファイルが TFTP サーバを介してアップロードされる際に、データは確実に暗号化されます。

ステップ 4　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 5　File Path フィールドに、設定ファイルのディレクトリ パスを入力します。

ステップ 6　File Name フィールドに、設定ファイルの名前を入力します。

ステップ 7　**Upload** をクリックし、設定ファイルを TFTP サーバにアップロードします。アップロードのステータスを示すメッセージが表示されます。

CLI を使用した設定ファイルのアップロード

コントローラ CLI を使用して 設定ファイルをアップロードする手順は、次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**transfer upload datatype config** と入力します。

ステップ 3　設定ファイルを暗号化する手順は、次のとおりです。

a. **transfer encrypt enable** と入力します。
b. **transfer encrypt set-key** *key* と入力します。

ステップ 4　**transfer upload serverip** *tftp-server-ip-address* と入力します。

ステップ 5　**transfer upload path** *path* と入力します。

ステップ 6　**transfer upload filename** *filename* と入力します。

ステップ 7　**transfer upload start** と入力して更新した設定を表示し、現在の設定を確認するプロンプトが表示されたら **y** と応答して、アップロード プロセスを開始します。このコマンドの出力例は、次のとおりです。

```
Mode............................................. TFTP
TFTP Server IP................................... 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

************************************************
***  WARNING: Config File Encryption Disabled  ***
************************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

設定ファイルのダウンロード

GUI または CLI のいずれかを使用して、設定ファイルをダウンロードできます。

GUI を使用した設定ファイルのダウンロード

コントローラの GUI を使用して 設定ファイルをダウンロードする手順は、次のとおりです。

ステップ 1　**Commands** > **Download File** の順にクリックして、Download File to Controller ページを開きます（図 8-6 を参照）。

図 8-6　Download File to Controller ページ

ステップ 2　File Type ドロップダウン ボックスから **Configuration** を選択します。

ステップ 3　Configuration File Encryption Key フィールドに、ファイルがダウンロードされる際に設定ファイルのデータを暗号化する暗号キーを入力します。

ステップ 4　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 5　Maximum Retries フィールドの 10 回の再試行および Timeout フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、必要に応じてその値を変更できます。そのためには、TFTP サーバが設定ファイルのダウンロードを試行する最大回数を Maximum Retries フィールドに、設定ファイルのダウンロードを試行する時間の合計（秒単位）を Timeout フィールドに入力します。

ステップ 6　File Path フィールドに、設定ファイルのディレクトリ パスを入力します。

ステップ 7　File Name フィールドに、設定ファイルの名前を入力します（*filename*）。

ステップ 8　**Download** をクリックして、ファイルをコントローラへダウンロードします。ダウンロードのステータスを示したメッセージが表示され、コントローラが自動的にリブートされます。

CLI を使用した設定ファイルのダウンロード

コントローラの CLI を使用して 設定ファイルをコントローラへダウンロードする手順は、次のとおりです。

ステップ 1　コントローラの CLI にログインします。

ステップ 2　**transfer download datatype config** と入力します。

ステップ 3　設定ファイルを暗号化する手順は、次のとおりです。

a. **transfer encrypt enable** と入力します。
b. **transfer encrypt set-key** *key* と入力します。

ステップ 4　**transfer download serverip** *tftp-server-ip-address* と入力します。

ステップ 5　**transfer download path** *path* と入力します。

ステップ 6　**transfer download filename** *filename* と入力します。

ステップ 7　**transfer download start** と入力して更新した設定を表示し、現在のダウンロード設定を確認するプロンプトが表示されたら **y** と応答して、ダウンロード プロセスを開始します。このダウンロード コマンドの出力例は、次のとおりです。

```
Mode............................................. TFTP
TFTP Server IP................................... 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

***********************************************
***  WARNING: Config File Encryption Disabled  ***
***********************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

設定の保存

コントローラには 2 種類のメモリが搭載されています。揮発性 RAM と NVRAM です。アクティブな揮発性 RAM からの不揮発性 RAM への設定の変更は、次のコマンドのいずれかを使用することで、いつでも保存できます。

- **save config** コマンドを使用します。このコマンドにより、コントローラをリセットせずに、揮発性 RAM から NVRAM に設定を保存できます。
- **reset system** コマンドを使用します。CLI から、コントローラをリブートする前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。
- **logout** コマンドを使用します。CLI から、ログアウトの前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。

コントローラ設定のクリア

NVRAM のアクティブな設定をクリアする手順は、次のとおりです。

ステップ 1　**clear config** と入力し、操作を確認するプロンプトが表示されたら、**y** と入力します。

ステップ 2　**reset system** と入力します。確認のプロンプトで **n** と入力すると、設定の変更を保存せずにリブートされます。コントローラをリブートすると、設定ウィザードが自動的に起動されます。

ステップ 3　「設定 ウィザードの使用方法」の項（P. 4-2）の指示に従って、初期設定を行います。

コントローラ設定の消去

コントローラ設定をデフォルト設定にリセットする手順は、次のとおりです。

ステップ 1　**reset system** と入力します。確認のプロンプトで **y** と入力して、設定変更を NVRAM に保存します。コントローラがリブートします。

ステップ 2　ユーザ名の入力を求められたら、**recover-config**　と入力してデフォルトの設定に戻します。コントローラをリブートすると、設定ウィザードが自動的に起動されます。

ステップ 3　「設定 ウィザードの使用方法」の項（P. 4-2）の指示に従って、初期設定を行います。

コントローラのリセット

次の 2 つの方法のいずれかを使用して、コントローラをリセットして、CLI コンソールにリブート処理を表示することができます。

- コントローラを一度オフにし、再びオンにします。
- CLI で **reset system** と入力します。確認のプロンプトで **y** と入力して、設定変更を NVRAM に保存します。コントローラがリブートします。

コントローラがリブートすると、CLI コンソールに次のリブート情報が表示されます。

- システムの初期化。
- ハードウェア設定の検証。
- マイクロコードのメモリへのロード。
- オペレーティング システム ソフトウェアのロードの検証。
- 保存されている設定による初期化。
- ログイン プロンプトの表示。

CHAPTER 9

ユーザ アカウントの管理

この章では、ゲスト ユーザ アカウントの作成および管理方法、Web 認証プロセス、および、Web 認証ログイン ページのカスタマイズ手順について説明します。この章の内容は、次のとおりです。

ゲスト ユーザ アカウントの作成

コントローラは、WLAN 上でゲスト ユーザ アクセスを提供できます。ゲスト ユーザ アカウント作成の最初の手順では、ロビー アンバサダー アカウントとしても知られる、ロビー管理者アカウントを作成します。このアカウントを作成すると、ロビー アンバサダーはゲスト ユーザ アカウントをコントローラ上で作成および管理できます。ロビー アンバサダーは、ゲスト アカウントを管理するために使用する Web ページのみの設定権限やアクセスを制限します。

ロビー アンバサダーは、ゲスト ユーザ アカウントを利用できる時間を指定できます。指定した時間を経過すると、ゲスト ユーザ アカウントは、自動的に無効になります。

ローカル ユーザ データベースは、最大エントリ数が 2048 に制限され、デフォルト値は、512 エントリです（Security > General ページ）。データベースは、ローカル管理ユーザ（ロビー アンバサダーを含む）、ネット ユーザ（ゲスト ユーザを含む）、MAC フィルタ エントリ、および無効になったクライアントで共有します。これらを合わせて、設定済みのデータベース容量を超えることはできません。

ロビー アンバサダー アカウントの作成

GUI または CLI を使用して、コントロール上にロビー アンバサダー アカウントを作成することができます。

GUI を使用したロビー アンバサダー アカウントの作成

コントローラ GUI を使用してロビー アンバサダー アカウントを作成する手順は、次のとおりです。

ステップ 1　**Management** > **Local Management Users** の順にクリックして、Local Management Users ページを開きます（図 9-1 を参照）。

図 9-1　Local Management Users ページ

このページは、ローカル管理ユーザの名前やアクセス権限の一覧表示です。

（注）　コントローラから任意のユーザ アカウントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。ただし、デフォルトの管理ユーザを削除すると、GUI および CLI によるコントローラへのアクセスは両方とも禁止されます。したがって、デフォルトのユーザを削除する前に、管理権限（ReadWrite）を持つユーザを作成しなければなりません。

ステップ 2　ロビー アンバサダー アカウントを作成するには、**New** をクリックします。Local Management Users > New ページが表示されます（図 9-2 を参照）。

図 9-2　Local Management Users > New ページ

ステップ 3　User Name フィールドに、ロビー アンバサダー アカウントのユーザ名を入力します。

（注）　管理ユーザ名は、すべて単一データベース内に保存されるため、一意である必要があります。

ステップ 4　Password フィールドおよび Confirm Password フィールドに、ロビー アンバサダー アカウントのパスワードを入力します。

（注）　パスワードは大文字と小文字が区別されます。

ステップ 5　User Access Mode ドロップダウン ボックスから **LobbyAdmin** を選択します。このオプションを使用すると、ロビー アンバサダーでゲスト ユーザ アカウントを生成できます。

（注）　**ReadOnly** オプションでは、読み取り専用の権限を持つアカウントを作成し、**ReadWrite** オプションでは、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。

ステップ 6　**Apply** をクリックして、変更を適用します。ローカル管理ユーザのリストに、新しいロビー アンバサダー アカウントが表示されます。

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用したロビー アンバサダー アカウントの作成

コントローラ CLI を使用してロビー アンバサダー アカウントを作成するには、以下のコマンドを入力します。

config mgmtuser add *lobbyadmin_username lobbyadmin_pwd* **lobby-admin**

(注) **lobby-admin** を **read-only** に置き換えると、読み取り専用の権限を持つアカウントを作成します。**lobby-admin** を **read-write** に置き換えると、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。

ロビー アンバサダーとしてのゲスト ユーザ アカウントの作成

ロビー アンバサダーは、次の手順に従ってゲスト ユーザ アカウントを作成します。

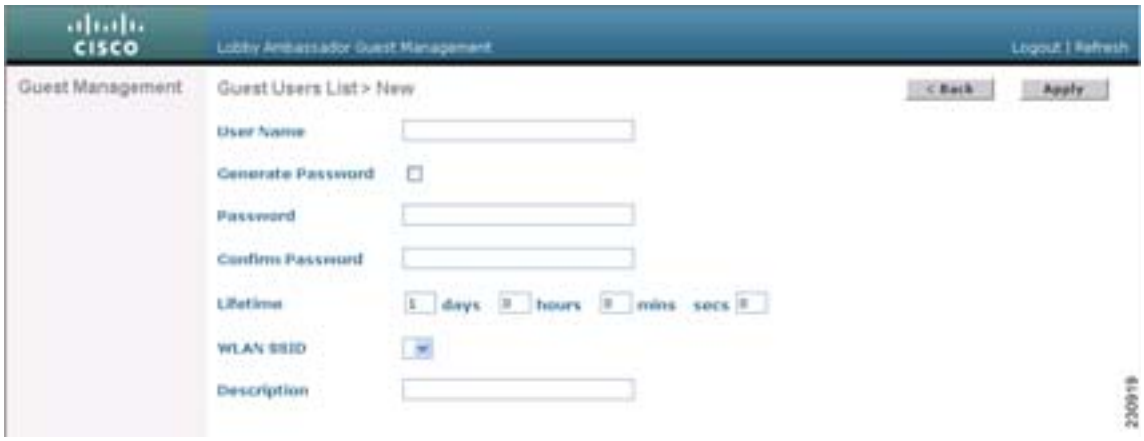
(注) ロビー アンバサダーは、コントローラの CLI インタフェースにアクセスできないため、コントローラの GUI からのみゲスト ユーザ アカウントを作成できます。

ステップ 1　上記の「ロビー アンバサダー アカウントの作成」の項で指定されたユーザ名およびパスワードを使用して、ロビー アンバサダーとしてコントローラにログインします。Lobby Ambassador Guest Management > Guest Users List ページが表示されます（図 9-3 を参照）。

図 9-3　Lobby Ambassador Guest Management > Guest Users List ページ

ステップ 2　**New** をクリックして、ゲスト ユーザ アカウントを作成します。Lobby Ambassador Guest Management > Guest Users List > New ページが表示されます（図 9-4 を参照）。

図 9-4　Lobby Ambassador Guest Management > Guest Users List > New ページ



ステップ 3　User Name フィールドに、ゲスト ユーザの名前を入力します。最大 24 文字を入力することができます。

ステップ 4　次のいずれかの操作を行います。

- このゲスト　ユーザ用のパスワードを自動的に生成する場合は、**Generate Password** チェック ボックスを選択します。生成されたパスワードは、Password フィールドおよび Confirm Password フィールドに自動的に入力されます。
- このゲスト ユーザ用にパスワードを作成する場合は、**Generate Password** チェック ボックスを選択せずに、Password フィールドおよび Confirm Password フィールドの両方にパスワードを入力します。

（注）　パスワードは最大 24 文字まで含めることができ、大文字と小文字が区別されます。

ステップ 5　Lifetime ドロップダウン ボックスから、このゲスト ユーザ アカウントをアクティブにする時間（日数、時間数、分数、秒数）を選択します。4 つのフィールド値をすべてゼロ（0）にすると、永久アカウントとなります。

デフォルト：1 日

範囲：5 分から 30 日

（注）　小さい方の値、またはゲスト アカウントが作成された WLAN であるゲスト WLAN のセッション タイムアウトが、優先します。たとえば、WLAN セッションのタイムアウトが 30 分でも、ゲスト アカウントのライフタイムが 10 分の場合、アカウントはゲスト アカウントの失効に従い、10 分で削除されます。同様に、WLAN セッションがゲスト アカウントのライフタイムより前にタイムアウトする場合、クライアントは、再認証を要求するセッション タイムアウトを繰り返すことになります。

（注） ゼロ以外の値がライフタイムに設定されているゲスト ユーザ アカウントの値は、アカウントがアクティブになっている間、いつでも別の値に変更できます。しかし、ゲスト ユーザ アカウントを永久アカウントにするため、または、永久アカウントをゲスト アカウントにするためには、そのアカウントを削除してから再度アカウントを作成しなければなりません。

ステップ 6　WLAN SSID ドロップダウン ボックスから、ゲスト ユーザが使用する SSID を選択します。リストアップされた WLAN のみにレイヤ 3 の Web 認証が設定されています。

（注） 潜在的な競合を阻止するために、システム管理者が特定のゲスト WLAN を作成することをお勧めします。ゲスト アカウントの有効期限が切れ、RADIUS サーバ上でアカウント名が競合し、両アカウントとも同じ WLAN 上にある場合、両アカウントにアソシエートしているユーザのアソシエートが解除されてから、ゲスト アカウントが削除されます。

ステップ 7　Description フィールドに、ゲスト ユーザ アカウントの説明を入力します。最大 32 文字を入力することができます。

ステップ 8　**Apply** をクリックして、変更を適用します。新しいゲスト ユーザ アカウントが、Guest Users List ページのゲスト ユーザ リストに表示されます（図 9-5 を参照）。

図 9-5　Lobby Ambassador Guest Management > Guest Users List ページ

このページから、すべてのゲスト ユーザ アカウント、それぞれの WLAN SSID およびライフタイムを表示できます。また、ゲスト ユーザ アカウントを編集、または削除することができます。ゲスト ユーザ アカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

ステップ 9　新しいゲスト ユーザ アカウントを作成するには、この手順を繰り返します。

ゲスト ユーザ アカウントの表示

ロビー アンバサダーがゲスト ユーザ アカウントを作成後、システム管理者は、コントローラの GUI または CLI からそれらのアカウントを表示できます。

GUI を使用したゲスト アカウントの表示

コントローラ GUI を使用してゲスト ユーザ アカウントを表示するには、**Security** > **AAA** > **Local Net Users** をクリックします。Local Net Users ページが表示されます（図 9-6 を参照）。

図 9-6　Local Net Users ページ

このページから、システム管理者はすべてのローカル ネット ユーザ アカウント（ゲストユーザアカウントを含む）を表示し、必要に応じて編集または削除することができます。ゲスト ユーザ アカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

CLI を使用したゲスト アカウントの表示

コントローラ CLI を使用して、すべてのローカル ネット ユーザ アカウント（ゲスト ユーザ アカウントを含む）を表示するには、次のコマンドを入力します。

show netuser summary

Web 認証プロセス

Web 認証は、レイヤ 3 セキュリティ機能です。これにより、コントローラは、クライアントが有効なユーザ名およびパスワードを正しく提供しない限り、そのクライアントに対する IP トラフィック（DHCP 関連パケットを除く）を許可しません。Web 認証を使用してクライアントを認証する場合、各クライアントのユーザ名とパスワードを定義する必要があります。クライアントは、無線 LAN に接続する際に、ログイン ページの指示に従ってユーザ名とパスワードを入力する必要があります。

Web 認証が（レイヤ 3 セキュリティ下で）有効になっている場合、ユーザが、最初にある URL にアクセスしようとした際に、Web ブラウザにセキュリティ警告が表示されることがあります。図 9-7 は一般的なセキュリティ警告を示しています。

図 9-7　一般的な Web ブラウザ セキュリティ警告ウィンドウ

ユーザが **Yes** をクリックして続行した後、（または、クライアントのブラウザにセキュリティ警告が表示されない場合）、Web 認証システムのログイン ページが表示されます（図 9-8 を参照）。

セキュリティ警告が表示されないようにするために、次の手順を実行できます。

ステップ 1　Security Alert ページで **View Certificate** をクリックします。

ステップ 2　**Install Certificate** をクリックします。

ステップ 3　Certificate Import Wizard が表示されたら、**New** をクリックします。

ステップ 4　**Place all certificates in the following store** を選択して、**Browse** をクリックします。

ステップ 5　Select Certificate Store ページの下部で、**Show Physical Stores** チェック ボックスをオンにします。

ステップ 6　**Trusted Root Certification Authorities** フォルダを展開して、**Local Computer** を選択します。

ステップ 7　**OK** をクリックします。

ステップ 8　**Next** > **Finish** の順にクリックします。

ステップ 9　「The import was successful」というメッセージが表示されたら、**OK** をクリックします。

ステップ 10　コントローラの自己署名証明書の issuer フィールドは空白であるため、Internet Explorer を開いて、**Tools** > **Internet Options** > **Advanced** の順にクリックし、Security の下の **Warn about Invalid Site Certificates** チェック ボックスをオフにして、**OK** をクリックします。

ステップ 11　PC をリブートします。次回 Web 認証を試みるときには、ログイン ページが表示されます（図 9-8 を参照）。

図 9-8　デフォルトの Web 認証ログイン ページ

デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- デフォルトのログイン ページ
- デフォルトのログイン ページの変更バージョン
- 外部の Web サーバに設定する、カスタマイズされたログイン ページ
- コントローラにダウンロードする、カスタマイズされたログイン ページ

「Web 認証ログイン ページの選択」の項（P. 9-11）には、Web 認証ログイン ページの表示方法を選択する手順が記載されています。

Web 認証ログイン ページで、ユーザが有効なユーザ名とパスワードを入力し、**Submit** をクリックすると、Web 認証システムは、ログインに成功したことを示すページを表示し、認証されたクライアントは要求した URL にリダイレクトされます。図 9-9 は一般的なログイン成功ページを示しています。

図 9-9　ログイン成功ページ

デフォルトのログイン成功ページには、仮想ゲートウェイ アドレスの URL（https://1.1.1.1/logout.html）が表示されます。コントローラの仮想インターフェイスに設定した IP アドレスは、ログイン ページのリダイレクト アドレスとして機能します（仮想インターフェイスの詳細は、第 3 章を参照）。

Web 認証ログイン ページの選択

この項では、Web 認証ログイン ページの内容および外観を指定する手順を説明します。いずれかの項の手順に従って、コントローラ GUI または CLI を使用して Web 認証ログイン ページを選択します。

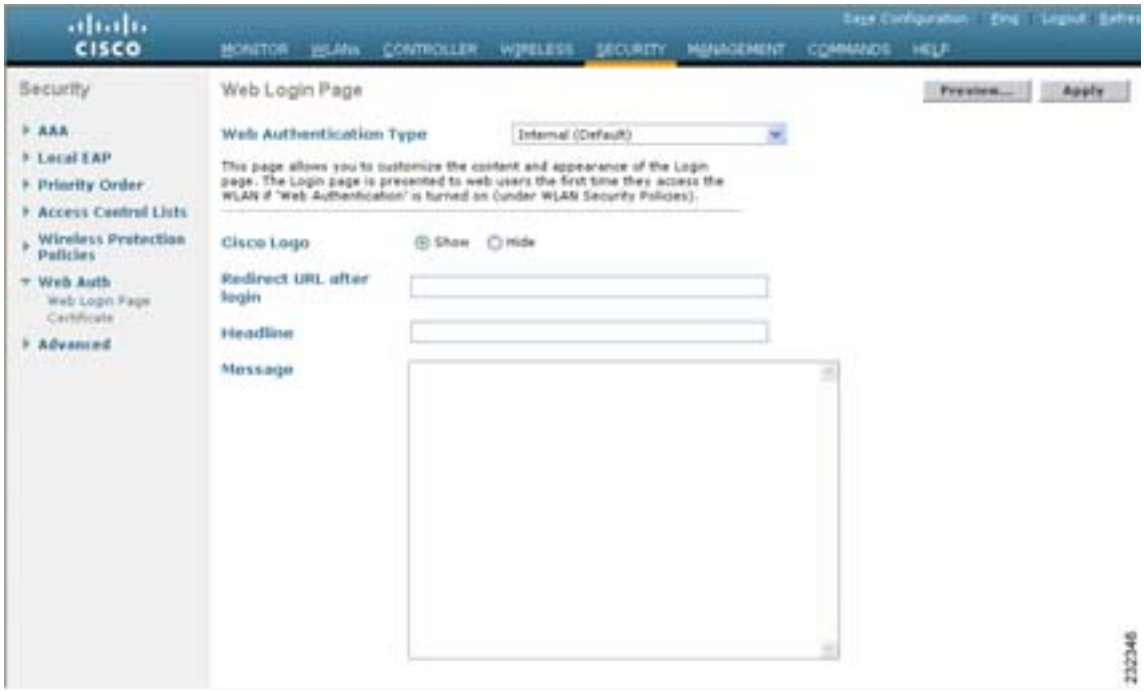
デフォルトの Web 認証ログイン ページの選択

デフォルトの Web 認証ログイン ページをそのまま使用する場合（図 9-8 を参照）、または、多少変更を加えて使用する場合、次の GUI または CLI 手順の指示に従ってください。

GUI を使用したデフォルト Web 認証ログイン ページの選択

ステップ 1　**Security** > **Web Auth** > **Web Login Page** の順にクリックして、Web Login ページを開きます（図 9-10 を参照）。

図 9-10　Web Login ページ



ステップ 2　Web Authentication Type ドロップダウン ボックスから **Internal (Default)** を選択します。

ステップ 3　デフォルトの Web 認証ログイン ページをそのまま使用する場合、ステップ 8 に進みます。デフォルトのログイン ページを変更する場合、ステップ 4 に進みます。

ステップ 4　デフォルト ページの右上に表示されている Cisco ロゴを非表示にするには、Cisco Logo **Hide** オプションを選択します。それ以外の場合は、**Show** オプションをクリックします。

ステップ 5　ログイン後にユーザを特定の URL（会社の URL など）にダイレクトさせる場合、Redirect URL After Login フィールドに必要な URL （www.AcompanyBC.com など）を入力します。最大 254 文字を入力することができます。

ステップ 6　ログイン ページで独自のヘッドラインを作成する場合、Headline フィールドに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。

ステップ 7　ログイン ページで独自のメッセージを作成する場合、Message フィールドに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　**Preview** をクリックして、Web 認証ログイン ページを表示します。

ステップ 10　ログイン ページの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。納得いかない場合は、納得する結果を得られるように必要に応じて上記手順を繰り返します。

CLI を使用したデフォルトの Web 認証ログイン ページの選択

ステップ 1　デフォルトの Web 認証タイプを指定するには、次のコマンドを入力します。

config custom-web webauth_type internal

ステップ 2　デフォルトの Web 認証ログイン ページをそのまま使用する場合、ステップ 7 に進みます。デフォルトのログイン ページを変更する場合、ステップ 3 に進みます。

ステップ 3　デフォルトのログイン ページの右上に表示されている Cisco ロゴの表示/非表示を切り替えるには、次のコマンドを入力します。

config custom-web weblogo {**enable** | **disable**}

ステップ 4　ユーザをログイン後に特定の URL （会社の URL など）にダイレクトさせる場合、次のコマンドを入力します。

config custom-web redirecturl *url*

URL には最大 130 文字を入力することができます。リダイレクト先をデフォルトの設定に戻すには、**clear redirecturl** と入力します。

ステップ 5　ログイン ページで独自のヘッドラインを作成する場合、次のコマンドを入力します。

config custom-web webtitle *title*

最大 130 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。ヘッドラインをデフォルトの設定に戻すには、**clear webtitle** と入力します。

ステップ 6　ログイン ページで独自のメッセージを作成する場合、次のコマンドを入力します。

config custom-web webmessage *message*

最大 130 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。メッセージをデフォルトの設定に戻すには、**clear webmessage** と入力します。

ステップ 7　**save config** と入力して、設定を保存します。

ステップ 8　独自のロゴを Web 認証ログイン ページにインポートする場合、次の手順に従ってください。

a. Trivial File Transfer Protocol（TFTP）サーバがダウンロードのために使用可能であることを確認します。TFTP サーバをセットアップする際の注意事項は次のとおりです。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバと WCS 内蔵型 TFTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP サーバは Cisco WCS と同じコンピュータ上で実行できません。

b. **ping ip-address** を入力して、コントローラが TFTP サーバと通信可能であることを確認します。

c. TFTP サーバのデフォルト ディレクトリにロゴ ファイル（.jpg、.gif、または .png 形式）を移動します。ファイル サイズは 30KB 以内です。うまく収まるようにするには、ロゴは、横 180 ピクセル X 縦 360 ピクセル前後の大きさにします。

d. ダウンロード モードを指定するには、**transfer download mode tftp** と入力します。

e. ダウンロードするファイルのタイプを指定するには、**transfer download datatype image** と入力します。

f. TFTP サーバの IP アドレスを指定するには、**transfer download serverip** *tftp-server-ip-address* と入力します。

（注） TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

g. ダウンロード パスを指定するには、**transfer download path** *absolute-tftp-server-path-to-file* と入力します。

h. ダウンロードするファイルを指定するには、**transfer download filename** {*filename.jpg* | *filename.gif* | *filename.png*} と入力します。

i. **transfer download start** と入力して更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。次のような情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Login Image
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename............................ <filename.jpg|.gif|.png>
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

j. **save config** と入力して、設定を保存します。

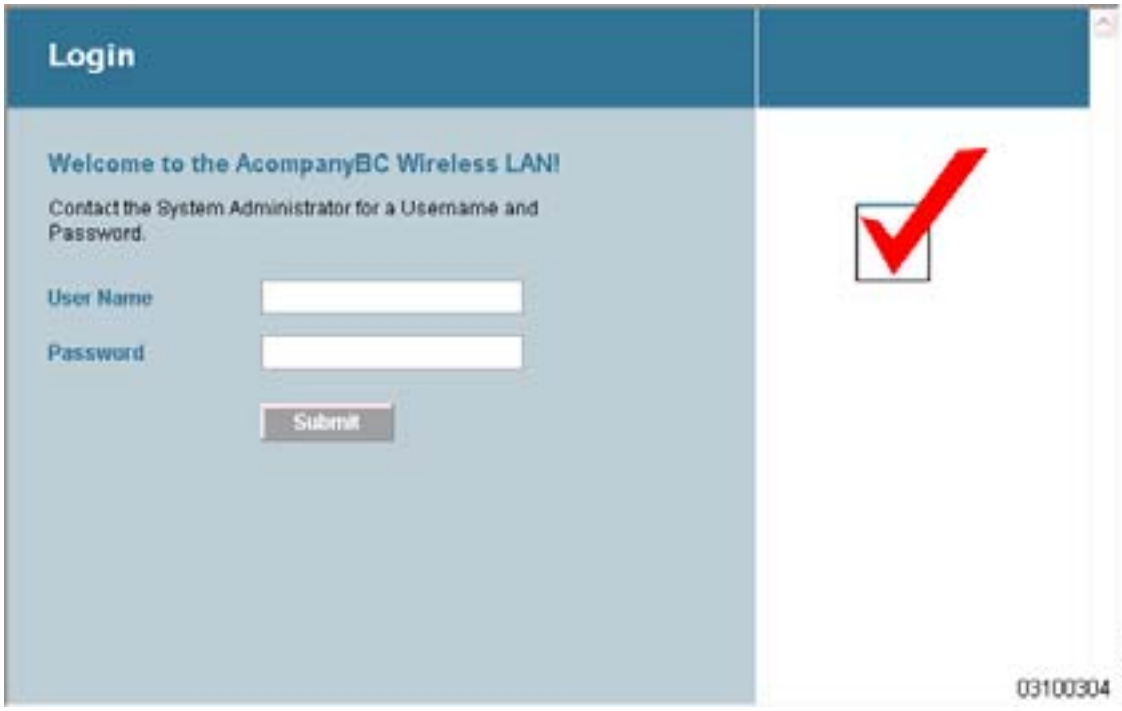
（注） Web 認証ログイン ページからロゴを削除するには、**clear webimage** と入力します。

ステップ 9　「CLI を使用した、Web 認証ログイン ページの設定の確認」の項（P. 9-22）の指示に従って、設定を確認します。

変更されたデフォルトの Web 認証ログイン ページの例

図 9-11 は、デフォルトの Web 認証ログイン ページを変更した例を示しています。

図 9-11　変更されたデフォルトの Web 認証ログイン ページの例



このログイン ページは、次の CLI コマンドを使用して作成されます。

config custom-web weblogo disable

config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!

config custom-web webmessage Contact the System Administrator for a Username and Password.

transfer download start

```
Mode..................................... TFTP
Data Type................................ Login Image
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ /
TFTP Filename............................ Logo.gif
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

config custom-web redirecturl http://www.AcompanyBC.com

show custom-web

```
Cisco Logo.............. Disabled
CustomLogo.............. 00_logo.gif
Custom Title............ Welcome to the AcompanyBC Wireless LAN!
Custom Message ......... Contact the System Administrator for a Username and
Password.
Custom Redirect URL..... http://www.AcompanyBC.com
Web Authentication Mode..... Disabled
Web Authentication URL..... Disabled
```

カスタマイズされた Web 認証ログイン ページの作成

この項では、カスタマイズされた Web 認証ログイン ページの作成について説明します。作成後は、外部 Web サーバからアクセスできるようになります。

Web 認証ログイン ページのテンプレートを次に示します。カスタマイズされたページを作成する際に、モデルとして使用できます。

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
      var link = document.location.href;
      var searchString = "redirect=";
      var equalIndex = link.indexOf(searchString);
      var redirectUrl = "";
      var urlStr = "";
      if(equalIndex > 0) {
            equalIndex += searchString.length;
            urlStr = link.substring(equalIndex);
            if(urlStr.length > 0){
               redirectUrl += urlStr;
               if(redirectUrl.length > 255)
                   redirectUrl = redirectUrl.substring(0,255);
               document.forms[0].redirect_url.value = redirectUrl;
           }
      }

      document.forms[0].buttonClicked.value = 4;
      document.forms[0].submit();
```

```
}

function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
      //alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      //document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your
part.");
      }
      else if(args.statusCode == 2){
        alert("You are not configured to authenticate against web portal. No further
action is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the
username is already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }

}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="http://1.1.1.1/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username"
SIZE="25" MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password"
name="password" SIZE="25" MAXLENGTH="24">
</td>
</tr>
```

```
<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

ユーザのインターネット ブラウザがカスタマイズされたログイン ページにリダイレクトされるときに、次のパラメータが URL に追加されます。

- **ap_mac**：無線ユーザがアソシエートされているアクセス ポイントの MAC アドレス。
- **switch_url**：ユーザの資格情報を記録するコントローラの URL。
- **redirect**：認証に成功した後、ユーザがリダイレクトされる URL。
- **statusCode**：コントローラの Web 認証サーバから戻されるステータス コード。
- **wlan**：無線ユーザがアソシエートされている WLAN SSID。

使用可能なステータス コードは次のとおりです。

- ステータス コード 1："You are already logged in. No further action is required on your part."（すでにログインしています。これ以上の操作は不要です。）
- ステータス コード 2："You are not configured to authenticate against web portal. No further action is required on your part."（Web ポータルに対して認証するように設定されていません。これ以上の操作は不要です。）
- ステータス コード 3："The username specified cannot be used at this time. Perhaps the username is already logged into the system?"（指定されたユーザ名は、今回使用できません。ユーザ名はすでにログインされている可能性があります。）
- ステータス コード 4："You have been excluded."（除外されています。）
- ステータス コード 5："The User Name and Password combination you have entered is invalid. Please try again."（入力したユーザ名とパスワードの組み合わせが無効です。再入力してください。）

（注） 詳細は、次の URL にある『External Web Authentication with Wireless LAN Controllers Configuration Example』を参照してください。
http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

外部 Web サーバでカスタマイズされた Web 認証ログイン ページの使用

外部 Web サーバでカスタマイズされた Web 認証ログイン ページを使用する場合、次の GUI または CLI 手順の指示に従ってください。この機能を有効にすると、ユーザは、外部 Web サーバ上のカスタマイズされたログイン ページへダイレクトされます。

（注） 外部 Web サーバに対して、事前認証アクセス コントロール リスト（ACL）を WLAN 上で設定してから、Security Policies > Web Policy on the WLANs > Edit ページで、WLAN 事前認証 ACL としてその ACL を選択する必要があります。ACL の詳細は、第 5 章を参照してください。

GUI を使用した、外部 Web サーバでカスタマイズされた Web 認証ログイン ページの選択

ステップ 1　**Security** > **Web Auth** > **Web Login Page** の順にクリックして、Web Login ページを開きます（図 9-12 を参照）。

図 9-12　Web Login ページ

ステップ 2　Web Authentication Type ドロップダウン ボックスから **External (Redirect to external server)** を選択します。

ステップ 3　URL フィールドに、Web サーバ上でカスタマイズされた Web 認証ログイン ページの URL を入力します。最大 252 文字を入力することができます。

ステップ 4　Web Server IP Address フィールドに、Web サーバの IP アドレスを入力します。Web サーバは、コントローラ サービス ポート ネットワークとは異なるネットワーク上に存在しなくてはなりません。

ステップ 5　**Add Web Server** をクリックします。このサーバは、外部 Web サーバ リスト上に表示されます。

ステップ 6　**Apply** をクリックして、変更を適用します。

ステップ 7　ログイン ページの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。

CLI を使用した、外部 Web サーバでカスタマイズされた Web 認証ログイン ページの選択

ステップ 1　Web 認証タイプを指定するには、次のコマンドを入力します。

config custom-web webauth_type external.

ステップ 2　Web サーバ上でカスタマイズされた Web 認証ログイン ページの URL を指定するには、次のコマンドを入力します。

config custom-web ext-webauth-url *url*

URL には最大 252 文字を入力することができます。

ステップ 3　Web サーバの IP アドレスを指定するには、次のコマンドを入力します。

config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

ステップ 4　**save config** と入力して、設定を保存します。

ステップ 5　「CLI を使用した、Web 認証ログイン ページの設定の確認」の項（P. 9-22）の指示に従って、設定を確認します。

カスタマイズされた Web 認証ログイン ページのダウンロード

Web 認証ログイン ページに使用するページやイメージ ファイルを .tar ファイルに圧縮してコントローラへダウンロードできます。これらのファイルは、*webauth bundle* と呼ばれています。ファイルの最大許容サイズは、非圧縮の状態で 1 MB です。.tar ファイルがローカル TFTP サーバからダウンロードされる際、コントローラのファイル システムには、展開済みファイルとして取り込まれます。

（注）　webauth bundle を GNU に準拠していない .tar 圧縮アプリケーションでロードすると、コントローラはこの bundle のファイルを解凍できず、「Extracting error」および「TFTP transfer failed」というエラー メッセージが表示されます。このため、PicoZip など GNU 標準に準拠するアプリケーションを使用して、webauth bundle の .tar ファイルを圧縮することをお勧めします。

カスタマイズされたログイン ページを作成する際のガイドラインは、次のとおりです。

- ログイン ページの名前を「login.html」とします。コントローラは、この名前に基づき Web 認証 URL を作成します。webauth bundle の展開後にこのファイルが見つからない場合、bundle は破棄され、エラー メッセージが表示されます。
- ユーザ名とパスワードの両方に入力フィールドを提供する。
- リダイレクト先の URL を元の URL から抽出後、非表示入力アイテムとして保持する。
- 元の URL からアクション URL を抽出して、ページに設定する。
- リターン ステータス コードをデコードするスクリプトを提供する。
- メインページで使用されるすべてのパス（たとえば、イメージへの参照など）が相対タイプであることを確認する。

サンプルのログイン ページを Cisco WCS からダウンロードし、カスタマイズの足がかりとして利用できます。手順は、『Cisco Wireless Control System Configuration Guide, Release 5.0』の「Using Templates」の章の「Downloading a Customized Web Auth Page」を参照してください。

カスタマイズされた Web 認証ログイン ページをコントローラにダウンロードする場合、次の GUI または CLI 手順の指示に従ってください。

GUI を使用した、Web 認証ログイン ページのダウンロード

ステップ 1　ファイルのダウンロードで TFTP サーバを使用できることを確認します。「CLI を使用したデフォルトの Web 認証ログイン ページの選択」の項（P. 9-12）のステップ 8 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 2　ログイン ページが含まれる .tar ファイルを TFTP サーバのデフォルトディレクトリに移動します。

ステップ 3　**Commands** > **Download File** の順にクリックして、Download File to Controller ページ（図 9-13 を参照）を開きます。

図 9-13　Download File to Controller ページ

ステップ 4　File Type ドロップダウン ボックスから、**Webauth Bundle** を選択します。

ステップ 5　IP Address フィールドに、TFTP サーバの IP アドレスを入力します。

ステップ 6　Maximum Retries フィールドに、コントローラによる .tar ファイルのダウンロードの最大試行回数を入力します。

範囲：1 ～ 254

デフォルト：10

ステップ 7　Timeout フィールドに、コントローラによる *.tar ファイルのダウンロード試行がタイムアウトするまでの時間（秒数）を入力します。

範囲：1 ～ 254 秒

デフォルト：6 秒

ステップ 8　File Path フィールドに、ダウンロードする .tar ファイルのパスを入力します。デフォルト値は「/」です。

ステップ 9　File Name フィールドに、ダウンロードする .tar ファイルの名前を入力します。

ステップ 10　**Download** をクリックして、.tar ファイルをコントローラへダウンロードします。

ステップ 11　**Security** > **Web Auth** > **Web Login Page** の順にクリックして、Web Login ページを開きます。

ステップ 12　Web Authentication Type ドロップダウン ボックスから **Customized (Downloaded)** を選択します。

ステップ 13　**Apply** をクリックして、変更を適用します。

ステップ 14　**Preview** をクリックして、カスタマイズされた Web 認証ログイン ページを表示します。

ステップ 15　ログイン ページの内容と外観に満足したら、**Save Configuration** をクリックして変更を保存します。

CLI を使用した、Web 認証ログイン ページのダウンロード

ステップ 1　ファイルのダウンロードで TFTP サーバを使用できることを確認します。「CLI を使用したデフォルトの Web 認証ログイン ページの選択」の項（P. 9-12）のステップ 8 にある TFTP サーバのセットアップのガイドラインを参照してください。

ステップ 2　ログイン ページが含まれる .tar ファイルを TFTP サーバのデフォルトディレクトリに移動します。

ステップ 3　ダウンロード モードを指定するには、**transfer download mode tftp** と入力します。

ステップ 4　ダウンロードするファイルのタイプを指定するには、**transfer download datatype webauthbundle** と入力します。

ステップ 5　TFTP サーバの IP アドレスを指定するには、**transfer download serverip** *tftp-server-ip-address* と入力します。

（注）　TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ（/）を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

ステップ 6　ダウンロード パスを指定するには、**transfer download path** *absolute-tftp-server-path-to-file* と入力します。

ステップ 7　ダウンロードするファイルを指定するには、**transfer download filename** *filename.tar* と入力します。

ステップ 8　**transfer download start** と入力して更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

ステップ 9　Web 認証タイプを指定するには、**config custom-web webauth_type customized** と入力します。

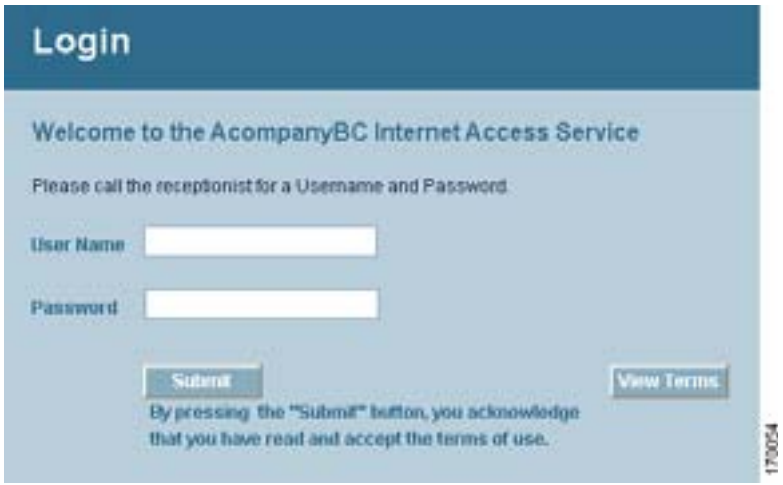
ステップ 10　**save config** と入力して、設定を保存します。

ステップ 11　「CLI を使用した、Web 認証ログイン ページの設定の確認」の項（P. 9-22）の指示に従って、設定を確認します。

カスタマイズされた Web 認証ログイン ページの例

図 9-14 は、カスタマイズされた Web 認証ログイン ページの例を示しています。

図 9-14　カスタマイズされた Web 認証ログイン ページの例



CLI を使用した、Web 認証ログイン ページの設定の確認

show custom-web と入力して、Web 認証ログイン ページに対する変更を確認します。次の例は、構成設定がデフォルト値に設定されている際に表示する情報を示します。

```
Cisco Logo..................................... Enabled
CustomLogo..................................... Disabled
Custom Title................................... Disabled
Custom Message................................. Disabled
Custom Redirect URL............................ Disabled
Web Authentication Mode........................ Disabled
Web Authentication URL......................... Disabled
```

This example shows the information that appears when the configuration settings have been modified:

```
Cisco Logo..................................... Disabled
CustomLogo..................................... 00_logo.gif
Custom Title................................... Welcome to the AcompanyBC Wireless
LAN!
Custom Message................................. Contact the System Administrator for a
                                                Username and Password.
Custom Redirect URL............................ http://www.AcompanyBC.com
Web Authentication Mode........................ Internal
Web Authentication URL.......................... Disabled
```

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

ユーザに対して、WLAN ごとに異なる Web 認証ログイン ページ、ログイン失敗ページ、ログアウト ページを表示できます。この機能を使用すると、ゲスト ユーザや組織内のさまざまな部署の従業員など、さまざまなネットワーク ユーザに対し、ユーザ固有の Web 認証ページを表示できます。

すべての Web 認証タイプ（Internal、Exterenal、Customized）で異なるログイン ページを使用できます。ただし、Web 認証タイプで Customized を選んだ場合に限り、異なるログイン失敗ページとログアウト ページを指定できます。

GUI を使用した、WLAN ごとのログイン ページ、ログイン失敗ページ、ログアウト ページの割り当て

コントローラの GUI を使用して WLAN に Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる手順は、次のとおりです。

ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　Web ログイン ページ、ログイン失敗ページ、またはログアウト ページを割り当てる WLAN のプロファイル名をクリックします。

ステップ 3　**Security** > **Layer 3** の順にクリックします。

ステップ 4　**Web Policy** と **Authentication** が選択されていることを確認します。

ステップ 5　Web 認証ページに設定されているグローバル認証設定を無効にするには、**Override Global Config** チェック ボックスをオンにします。

ステップ 6　Web Auth Type ドロップダウン ボックスが表示されたら、次のオプションのいずれかを選択して、無線ゲスト ユーザ用の Web 認証ページを定義します。

- **Internal**：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **Customized**：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン ボックスが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン ボックスで **None** を選択します。

（注）　これらオプションのログイン　ページ、ログイン失敗ページ、ログアウト　ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。カスタム ページをダウンロードする詳細は、「カスタマイズされた Web 認証ログイン ページのダウンロード」の項（P. 9-19）を参照してください。

- **External**：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、URL フィールドに外部サーバの URL も入力する必要があります。

  WLANs > Edit（Security > AAA Servers）ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 7　ステップ 6 で、Web 認証タイプとして External を選択した場合は、**AAA Servers** をクリックして、ドロップダウン ボックスから最大 3 つまでの RADIUS サーバおよび LDAP サーバを選択してください。

（注）　RADIUS および LDAP の外部サーバは、WLANs > Edit（Security > AAA Servers）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。RADIUS Authentication Servers ページと LDAP Servers ページでこれらのサーバを設定できます。

ステップ 8　Web 認証で接続するサーバの優先順位を指定する手順は、次のとおりです。デフォルトでは、ローカル、Radius、LDAP の順になっています。

a. Up ボタンと Down ボタンの隣にあるボックスで、最初に接続するサーバの種類（Local、Radius、LDAP）を強調表示します。
b. 希望のサーバ タイプがボックスの一番上に表示されるように **Up** ボタンおよび **Down** ボタンをクリックします。
c. < 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。
d. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 9　**Apply** をクリックして、変更を適用します。

ステップ 10　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した、WLAN ごとのログイン ページ、ログイン失敗ページ、ログアウト ページの割り当て

コントローラの CLI を使用して、WLAN に Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる手順は、次のとおりです。

ステップ 1　Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる WLAN の ID 番号を決定するには、次のコマンドを入力します。

show wlan summary

ステップ 2　カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに無線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して Web 認証ページのファイル名および表示する WLAN を指定します。

- **config wlan custom-web login-page** *page_name wlan_id*：指定した WLAN に対するカスタマイズしたログイン ページを定義します。
- **config wlan custom-web loginfailure-page** *page_name wlan_id*：指定した WLAN に対するカスタマイズしたログイン失敗ページを定義します。

（注）　コントローラのデフォルトのログイン失敗ページを使用するには、次のコマンドを入力します。**config wlan custom-web loginfailure-page none** *wlan_id*

- **config wlan custom-web logout-page** *page_name wlan_id*：指定した WLAN に対するカスタマイズしたログアウト ページを定義します。

（注）　コントローラのデフォルトのログアウト ページを使用するには、次のコマンドを入力します。**config wlan custom-web logout-page none** *wlan_id*

ステップ 3　Web ログイン ページにアクセスする前に無線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

ステップ 4　Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

サーバの Web 認証は、デフォルトではローカル、Radius、LDAP の順になっています。

（注）　すべての外部サーバをコントローラで事前に設定しておく必要があります。RADIUS Authentication Servers ページと LDAP Servers ページでこれらを設定できます。

ステップ 5　無線ゲスト ユーザ用の Web 認証ページを定義するには、次のコマンドを入力します。

config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

このとき、次のようになります。

- **Internal** は、コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** は、ステップ 2 で設定したカスタム Web ログイン ページを表示します。

（注）　ログイン失敗ページとログアウト ページは常にカスタマイズされているため、ステップ 5 で Web 認証タイプを定義する必要はありません。

- **external** は、ステップ 3 で設定された URL にユーザをリダイレクトします。

ステップ 6　グローバル カスタム Web 設定ではなく、WLAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

config wlan custom-web global disable *wlan_id*

（注）　**config wlan custom-web global enable** *wlan_id* コマンドを入力すると、カスタム Web 認証がグローバル レベルで設定されます。

ステップ 7　変更を保存するには、次のコマンドを入力します。

save config

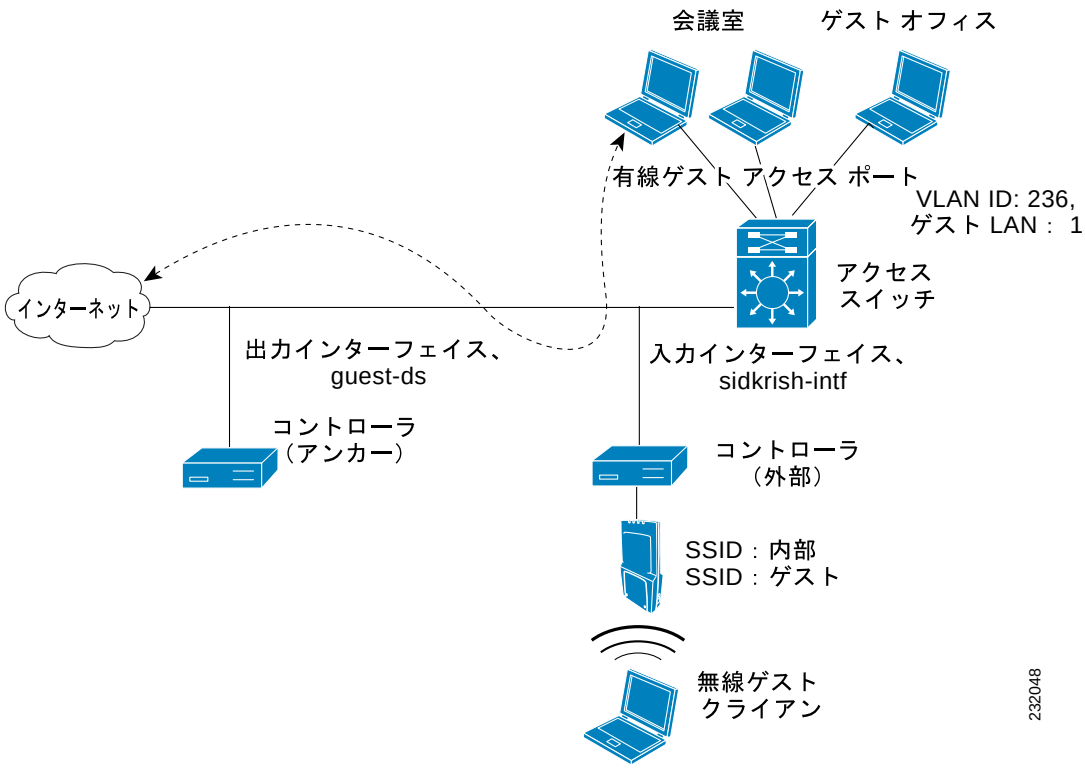
有線ゲスト アクセスの設定

有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスからまたは会議室の特定のポートを介して利用することもできます。無線ゲスト ユーザ アカウントと同様に、有線ゲスト アクセス ポートは、ロビー アンバサダー機能を使用してネットワークに追加されます。

有線ゲスト アクセスは、スタンドアロン設定または、アンカー コントローラと外部コントローラの両方を使用するデュアル コントローラ設定で設定できます。この後者の設定は、有線ゲスト アクセス トラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必要ありません。

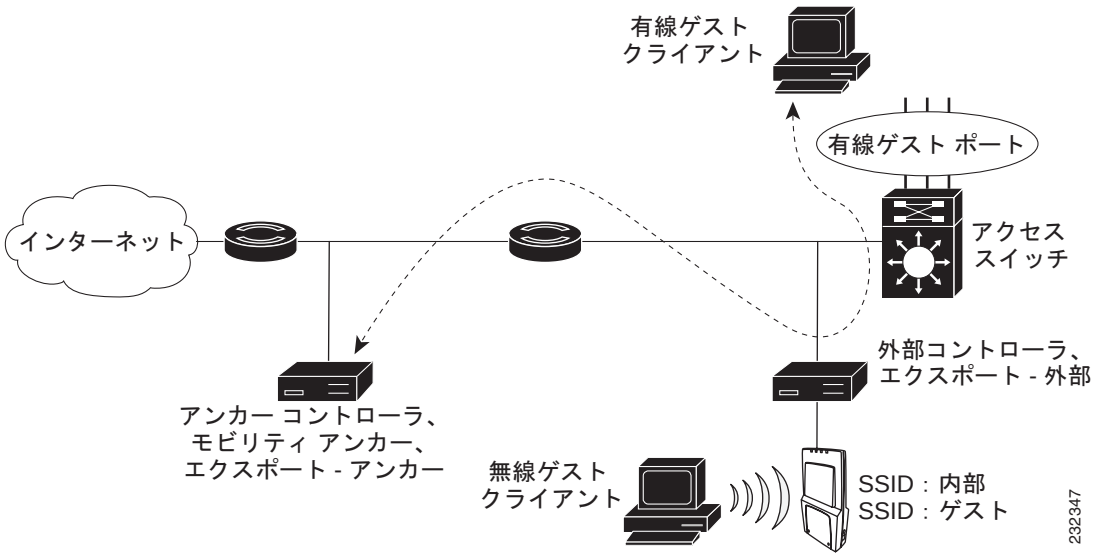
有線ゲスト アクセス ポートは最初、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセス トラフィック用の VLAN インターフェイスで設定されているスイッチ ポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。図 9-15 を参照してください。

図 9-15　1 つのコントローラを使用した有線ゲスト アクセスの例



2 つのコントローラが使用されている場合、有線ゲスト トラフィックをアクセス スイッチから受信する外部コントローラは、アンカー コントローラへそのトラフィックを転送します。このトラフィックを処理するために、外部コントローラとアンカー コントローラとの間で双方向 EoIP トンネルが確立されます。図 9-16 を参照してください。

図 9-16　2 つのコントローラを使用した有線ゲスト アクセスの例



（注） 2 つのコントローラが展開されるとき、有線ゲスト アクセスはアンカーと外部アンカーによって管理されますが、有線ゲスト アクセス クライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。

（注） QoS ロールと帯域幅コントラクトを設定することにより、ネットワーク内の有線ゲスト ユーザに割り当てられている帯域幅の量を指定できます。これらの機能の設定の詳細は、「Quality of Service ロールの設定」の項（P. 4-55）を参照してください。

設定の概要

無線ネットワーク上で有線ゲスト アクセスを設定する手順は、次のとおりです。

1. 有線ゲスト ユーザ アクセス用の動的インターフェイス（VLAN）を設定します。
2. ゲスト ユーザ アクセス用の有線 LAN を作成します。
3. コントローラを設定します。
4. アンカー コントローラを設定します（別のコントローラでトラフィックを終端する場合）。
5. ゲスト LAN 用のセキュリティを設定します。
6. 設定を確認します。

設定のガイドライン

ネットワーク上で有線ゲスト アクセスを使用するには、次のガイドラインに従ってください。

- 有線ゲスト アクセスは、次のコントローラ上でのみサポートされています。4400 シリーズのコントローラ、Cisco WiSM、および Catalyst 3750G 統合型無線 LAN コントローラ スイッチ。
- 有線ゲスト アクセス インターフェイスは、タグ付きである必要があります。
- 有線ゲスト アクセス ポートは、外部コントローラと同じレイヤ 2 ネットワークになければなりません。
- コントローラ上で、最大 5 つの有線ゲスト アクセス LAN を設定できます。
- 有線ゲスト アクセス クライアントに対して、レイヤ 3 Web 認証と Web パススルーがサポートされています。レイヤ 2 セキュリティはサポートされていません。

GUI を使用した有線ゲスト アクセスの設定

コントローラの GUI を使用して、ネットワーク上で有線ゲスト ユーザ アクセスを設定する手順は、次のとおりです。

ステップ 1　有線ゲスト ユーザ アクセス用の動的インターフェイスを作成するために、**Controller** > **Interfaces** の順にクリックします。Interfaces ページが表示されます。

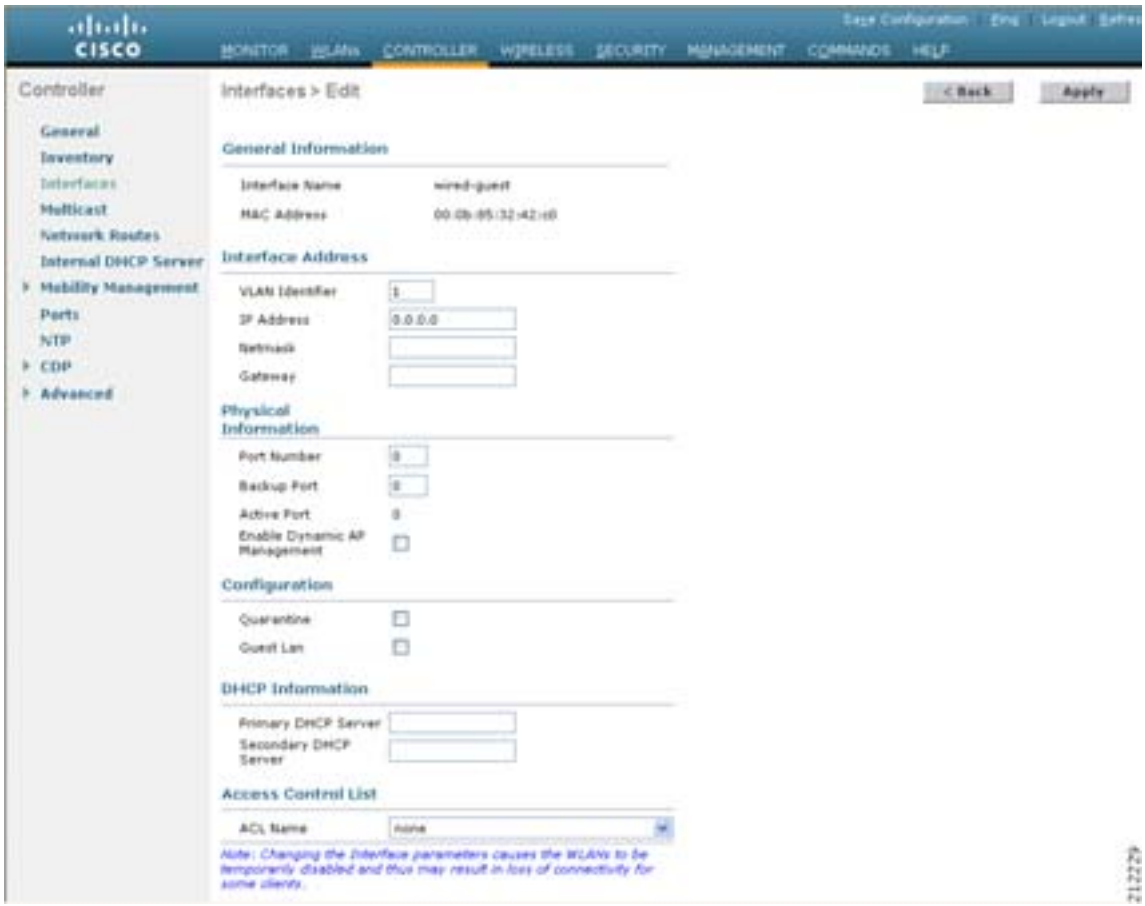
ステップ 2　**New** をクリックして、Interfaces > New ページを開きます。

ステップ 3　新しいインターフェイスの名前と VLAN ID を入力します。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　Interfaces > Edit ページで、インターフェイスの IP アドレス、ネットマスク、およびゲートウェイ アドレスを入力します（図 9-17 を参照）。

図 9-17　Interfaces > Edit ページ



ステップ 6　Port Number フィールドに、有効なポート番号を入力します。0 ～ 25（両端の値を含む）の数値を入力できます。

ステップ 7　**Guest LAN** チェックボックスをオンにします。

ステップ 8　プライマリ DHCP サーバの IP アドレスを入力します。

ステップ 9　**Apply** をクリックして、変更を適用します。

ステップ 10　ゲスト ユーザ アクセス用に有線 LAN を作成するために、**WLANs** をクリックします。

ステップ 11　WLANs ページで、**New** をクリックします。WLANs > New ページが表示されます（図 9-18 を参照）。

図 9-18　WLANs > New ページ

ステップ 12　Type ドロップダウン ボックスから、**Guest LAN** を選択します。

ステップ 13　Profile Name フィールドに、ゲスト LAN を識別する名前を入力します。スペースを使用しないでください。

ステップ 14　WLAN SSID フィールドに、ゲスト LAN を識別する SSID を入力します。スペースを使用しないでください。

ステップ 15　**Apply** をクリックして、変更を適用します。WLANs > Edit ページが表示されます（図 9-19 を参照）。

図 9-19　WLANs > Edit ページ

ステップ 16　Status パラメータに対する **Enabled** チェックボックスをオンにします。

ステップ 17　Web 認証（Web-Auth）は、デフォルトのセキュリティ ポリシーです。これを Web パススルーに変更する場合は、ステップ 18 とステップ 19 を終了してから、**Security** タブをクリックします。

ステップ 18　Ingress Interface ドロップダウン ボックスから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセス スイッチを経由して、有線ゲスト クライアントとコントローラとの間のパスを提供します。

ステップ 19　Egress Interface ドロップダウン ボックスから、インターフェイスの名前を選択します。この WLAN は、有線ゲスト クライアント トラフィックのコントローラから送信されるパスを提供します。

（注）　設定でコントローラが 1 つしかない場合は、Egress Interface ドロップダウン ボックスから **management** を選択します。

ステップ 20　認証方式を変更する（たとえば、Web 認証から Web パススルーへ）場合、**Security** > **Layer 3** の順にクリックします。WLANs > Edit (Security > Layer 3) ページが表示されます（図 9-20 を参照）。

図 9-20　WLANs > Edit（Security > Layer 3）ページ

ステップ 21　Layer 3 Security ドロップダウン ボックスから、次のいずれかを選択します。

- **None**：レイヤ 3 セキュリティが無効になっています。
- **Web Authentication**：無線ネットワークに接続する際に、ユーザにユーザ名とパスワードの入力を求めます。これはデフォルト値です。
- **Web Passthrough**：ユーザがユーザ名とパスワードを入力せずに、ネットワークにアクセスすることを許可します。

ステップ 22　Web パススルー オプションを選択する場合、**Email Input** チェックボックスが表示されます。ユーザがネットワークに接続を試みているときに、電子メール アドレスの入力を求める場合、このチェックボックスをオンにします。

ステップ 23　Web Login ページに設定されているグローバル認証設定を無効にするには、**Override Global Config** チェック ボックスをオンにします。

ステップ 24　Web Auth Type ドロップダウン ボックスが表示されたら、次のオプションのいずれかを選択して、有線ゲスト ユーザ用の Web 認証ページを定義します。

- **Internal**：コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **Customized**：カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウン ボックスが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン ボックスで **None** を選択します。

（注）　これらのオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- **External**：認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、URL フィールドに外部サーバの URL も入力する必要があります。

  WLANs > Edit（Security > AAA Servers）ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 25 ステップ 24 で、Web 認証タイプとして External を選択した場合は、**AAA Servers** をクリックして、ドロップダウン ボックスから最大 3 つまでの RADIUS サーバおよび LDAP サーバを選択してください。

（注） RADIUS および LDAP の外部サーバは、WLANs > Edit（Security > AAA Servers）ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。RADIUS Authentication Servers ページと LDAP Servers ページでこれらのサーバを設定できます。

ステップ 26 Web 認証で接続するサーバの優先順位を指定する手順は、次のとおりです。デフォルトでは、ローカル、Radius、LDAP の順になっています。

a. Up ボタンと Down ボタンの隣にあるボックスで、最初に接続するサーバの種類（Local、Radius、LDAP）を強調表示します。
b. 希望のサーバ タイプがボックスの一番上に表示されるように **Up** ボタンおよび **Down** ボタンをクリックします。
c. < 矢印をクリックして、そのサーバ タイプを左側の優先順位ボックスに移動します。
d. この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 27 **Apply** をクリックして、変更を適用します。

ステップ 28 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 29 2 番目の（アンカー）コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

CLI を使用した有線ゲスト アクセスの設定

コントローラの CLI を使用して、ネットワーク上で有線ゲスト ユーザ アクセスを設定する手順は、次のとおりです。

ステップ 1 有線ゲスト ユーザのアクセス用の動的インターフェイス（VLAN）を作成するには、次のコマンドを入力します。

config interface create *interface_name vlan_id*

ステップ 2 リンク集約トランクが設定されていない場合、次のコマンドを入力して、物理ポートをインターフェイスにマップします。

config interface port *interface_name primary_port* {*secondary_port*}

ステップ 3 ゲスト LAN VLAN を有効または無効にするには、次のコマンドを入力します。

config interface guest-lan *interface_name* {**enable** | **disable**}

この VLAN は、ステップ 5 で作成した ingress インターフェイスに後でアソシエートされます。

ステップ 4　有線クライアント トラフィックを作成してインターフェイスにアソシエートさせるには、次のコマンドを入力します。

config guest-lan create *guest_lan_id interface_name*

ゲスト LAN ID は、1 ～ 5（両端の値を含む）にする必要があります。

（注）　有線ゲスト LAN を削除するには、次のコマンドを入力します。**config guest-lan delete** *guest_lan_id*

ステップ 5　レイヤ 2 アクセス スイッチ経由で有線ゲスト クライアントとコントローラ間のパスを提供する、有線ゲスト VLAN の ingress インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan ingress-interface *guest_lan_id interface_name*

ステップ 6　コントローラから有線ゲスト トラフィックを送信する egress インターフェイスを設定するには、次のコマンドを入力します。

config guest-lan interface *guest_lan_id interface_name*

（注）　有線ゲスト トラフィックが別のコントローラで終端する場合は、終点の（アンカー）コントローラに対してステップ 4 とステップ 6 を繰り返し、起点の（外部）コントローラに対してステップ 1 ～ ステップ 5 を繰り返します。さらに、両方のコントローラに対して次のコマンドを設定します。
config mobility group anchor add {**guest-lan** *guest_lan_id* | **wlan** *wlan_id*} *IP_address*

ステップ 7　有線ゲスト LAN のセキュリティ ポリシーを設定するには、次のコマンドを入力します。

config guest-lan security {**web-auth enable** *guest_lan_id* | **web-passthrough enable** *guest_lan_id*}

（注）　Web 認証はデフォルト設定です。

ステップ 8　有線ゲスト LAN を有効または無効にするには、次のコマンドを入力します。

config guest-lan {**enable** | **disable**} *guest_lan_id*

ステップ 9　カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに有線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して、Web 認証ページのファイル名および表示するゲスト LAN を指定します。

- **config guest-lan custom-web login-page** *page_name guest_lan_id*：Web ログイン ページを定義します。
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id*：Web ログイン失敗ページを定義します。

（注） コントローラのデフォルトのログイン失敗ページを使用するには、次のコマンドを入力します。**config guest-lan custom-web loginfailure-page none** *guest_lan_id*

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*：Web ログアウト ページを定義します。

（注） コントローラのデフォルトのログアウト ページを使用するには、次のコマンドを入力します。**config guest-lan custom-web logout-page none** *guest_lan_id*

ステップ 10 有線ゲスト ユーザが Web ログイン ページにアクセスする前に有線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

ステップ 11 ローカル（コントローラ）または外部（RADIUS、LDAP）の Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

サーバの Web 認証は、デフォルトではローカル、Radius、LDAP の順になっています。

（注） すべての外部サーバをコントローラで事前に設定しておく必要があります。RADIUS Authentication Servers ページまたは LDAP Servers ページでこれらを設定できます。

ステップ 12 有線ゲスト ユーザー用の Web ログイン ページを定義するには、次のコマンドを入力します。

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

このとき、次のようになります。

- **Internal** は、コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
- **customized** では、ステップ 9 で設定したカスタム Web ページ（ログイン ページ、ログイン失敗ページ、またはログアウト ページ）が表示されます。
- **external** は、ステップ 10 で設定された URL にユーザをリダイレクトします。

ステップ 13 グローバル カスタム Web 設定ではなく、ゲスト LAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

config guest-lan custom-web global disable *guest_lan_id*

（注） **config guest-lan custom-web global enable** *guest_lan_id* コマンドを入力すると、カスタム Web 認証がグローバル レベルで設定されます。

ステップ 14 変更を保存するには、次のコマンドを入力します。

save config

（注） 設定された Web 認証ページの情報は、**show run-config** コマンドおよび **show running-config** コマンドの両方に表示されます。

ステップ 15 特定のゲスト LAN に対するカスタマイズ Web 認証設定を表示するには、次のコマンドを入力します。

show custom-web {**all** | **guest-lan** *guest_lan_id*}

（注） 内部の Web 認証が設定されていると、Web Authentication Type は、外部（コントローラ レベル）またはカスタマイズ（WLAN プロファイル レベル）ではなく内部として表示されます。

show custom-web all コマンドに対しては、次のような情報が表示されます。

```
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. None
Web Authentication Type.............              External
External Web Authentication URL............      http:\\9.43.0.100\login.html

External Web Server list
Index IP Address
----- ---------------
1       9.43.0.100
2       0.0.0.0
3       0.0.0.0
4       0.0.0.0
5       0.0.0.0
...
20      0.0.0.0

Configuration Per Profile:

WLAN ID: 1
    WLAN Status.................................. Enabled
    Web Security Policy.......................... Web Based Authentication
    Global Status................................ Disabled
    WebAuth Type................................. Customized
    Login Page................................... login1.html
    Loginfailure page name....................... loginfailure1.html
    Logout page name............................. logout1.html

WLAN ID: 2
WLAN Status.................................. Enabled
    Web Security Policy.......................... Web Based Authentication
    Global Status................................ Disabled
    WebAuth Type................................. Internal
    Loginfailure page name....................... None
    Logout page name............................. None
```

```
WLAN ID: 3
WLAN Status..................................... Enabled
    Web Security Policy........................... Web Based Authentication
    Global Status................................. Disabled
    WebAuth Type.................................. Customized
    Login Page.................................... login.html
    Loginfailure page name........................ LF2.html
    Logout page name.............................. LG2.html
```

show custom-web guest-lan *guest_lan_id* コマンドに対しては、次のような情報が表示されます。

```
Guest LAN ID: 1
Guest LAN Status.............................. Disabled
Web Security Policy........................... Web Based Authentication
Global Status................................. Enabled
WebAuth Type.................................. Internal
Loginfailure page name........................ None
Logout page name.............................. None
```

ステップ 16　ローカル インターフェイスの要約を表示するには、次のコマンドを入力します。

show interface summary

次のような情報が表示されます。

```
Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
ap-manager                       1    untagged 1.100.163.25    Static  Yes    No

management                       1    untagged 1.100.163.24    Static  No     No

service-port                     N/A  N/A      172.19.35.31    Static  No     No

virtual                          N/A  N/A      1.1.1.1         Static  No     No

wired                            1    20       10.20.20.8      Dynamic No     No

wired-guest                      1  236     10.20.236.50   Dynamic No    Yes
```

（注）　この例の有線ゲスト LAN のインターフェイス名は、*wired-guest*、その VLAN ID は 236 です。

ステップ 17 詳細なインターフェイス情報を表示するには、次のコマンドを入力します。

show interface detailed *interface_name*

次のような情報が表示されます。

```
Interface Name................................. wired-guest
MAC Address.................................... 00:11:92:ff:e7:eb
IP Address..................................... 10.20.236.50
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 10.50.236.1
VLAN........................................... 236
Quarantine-vlan................................ no
Active Physical Port........................... LAG (29)
Primary Physical Port.......................... LAG (29)
Backup Physical Port........................... Unconfigured
Primary DHCP Server............................ 10.50.99.1
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
AP Manager..................................... No
Guest Interface.............................. Yes
```

ステップ 18 特定の有線ゲスト LAN の設定を表示するには、次のコマンドを入力します。

show guest-lan *guest_lan_id*

次のような情報が表示されます。

```
Guest LAN Identifier........................... 1
Profile Name................................... guestlan
Network Name (SSID)............................ guestlan
Status......................................... Enabled
AAA Policy Override............................ Disabled
Number of Active Clients....................... 1
Exclusionlist Timeout.......................... 60 seconds
Session Timeout................................ Infinity
Interface...................................... wired
Ingress Interface.............................. wired-guest
WLAN ACL....................................... unconfigured
DHCP Server.................................... 10.20.236.90
DHCP Address Assignment Required............... Disabled
Quality of Service............................. Silver (best effort)
Security
    Web Based Authentication..................... Enabled
    ACL.......................................... Unconfigured
    Web-Passthrough.............................. Disabled
    Conditional Web Redirect..................... Disabled
    Auto Anchor.................................. Disabled
Mobility Anchor List
GLAN ID IP Address Status
------- --------------- ------
```

（注） **show guest-lan summary** と入力して、コントローラ上で設定されているすべての有線ゲスト LAN を表示します。

ステップ 19 有線ゲスト LAN クライアントを有効または無効にするには、次のコマンドを入力します。

show client summary guest-lan

次のような情報が表示されます。

```
Number of Clients.............................. 1
MAC Address        AP Name Status     WLAN  Auth Protocol  Port Wired
------------------ ------- ---------- ----- ----- --------- ----- ------
00:16:36:40:ac:58   N/A   Associated   1    No    802.3     1    Yes
```

ステップ 20 特定のクライアントの詳細情報を表示するには、次のコマンドを入力します。

show client detail *client_mac*

次のような情報が表示されます。

```
Client MAC Address............................. 00:40:96:b2:a3:44
Client Username ............................... N/A
AP MAC Address................................. 00:18:74:c7:c0:90
Client State................................... Associated
Wireless LAN Id................................ 1
BSSID.......................................... 00:18:74:c7:c0:9f
Channel........................................ 56
IP Address..................................... 192.168.10.28
Association Id................................. 1
Authentication Algorithm....................... Open System
Reason Code.................................... 0
Status Code.................................... 0
Session Timeout................................ 0
Client CCX version............................. 5
Client E2E version............................. No E2E support
Diagnostics Capability......................... Supported
S69 Capability................................. Supported
Mirroring...................................... Disabled
QoS Level...................................... Silver
...
```

CHAPTER 10

Radio Resource Management の設定

この章では、Radio Resource Management（RRM）とコントローラにおけるその設定方法について説明します。この章の内容は、次のとおりです。

Radio Resource Management の概要

Radio Resource Management（RRM）ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは、次の情報についてそのアソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- **トラフィックの負荷**：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- **干渉**：他の 802.11 発信元から送られてくるトラフィック量。
- **ノイズ**：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- **カバレッジ**：接続されているすべてのクライアントの Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）と Signal-to-Noise Ratio（SNR; 信号対雑音比）。
- **その他の**：近くにあるアクセス ポイントの数。

RRM は、この情報を使用して、最も効率がよくなるように 802.11 RF ネットワークを定期的に再設定できます。そのために、RRM では次の機能を実行します。

- 無線リソースの監視
- 送信電力の動的制御
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正
- クライアントとネットワークのロード バランシング

無線リソースの監視

RRM は、ネットワークに追加された新しいコントローラや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に分散して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントは、使用国で有効なすべての 802.11a/b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントは、これらのチャネルのノイズや干渉を監視する際、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 過去 100 ミリ秒の間にパケットが音声キューに入っていた場合、アクセス ポイントはオフチャネルになりません。

デフォルトでは、各アクセス ポイントがオフチャネルになるのはその時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。そのため管理者は、すべてのアクセス ポイントを監視でき、ネットワークの可視性が向上します。

送信電力の動的制御

コントローラは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。通常は、電力を低く維持することでキャパシティを増やし、干渉を減らします。コントローラは、最適な -65dBm 以上の電力がある上位 4 つのネイバーが認識されるようにアクセス ポイントを調整します。

送信電力制御アルゴリズムでは、アクセス ポイントの電力を減らすことしかできません。ただし、次に説明するカバレッジ ホール アルゴリズムではアクセス ポイントの電力を増やすことで、カバレッジ ホールを埋めることができます。たとえば、障害が発生したアクセス ポイントが検出されると、カバレッジ ホール アルゴリズムによって周囲のアクセス ポイントの電力が自動的に増やされて、カバレッジの消失によって生じたギャップが埋められます。

（注） 送信電力レベルについては、ステップ 4（P. 10-28）を参照してください。

チャネルの動的割り当て

同じチャネル上の 2 つの隣接するアクセス ポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突が発生すると、アクセス ポイントではデータがまったく受信されません。この動作は問題になることがあります。たとえば、誰かがカフェで E メールを読むことで、近隣の会社のアクセス ポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル 1 を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。コントローラは、アクセス ポイント チャネルを動的に割り当てて衝突を回避し、キャパシティとパフォーマンスを改善することで、この問題に対処します。それによって、チャネルは「再利用」され、希少な RF リソースが浪費されるのを防ぐことができます。つまり、チャネル 1 はカフェから離れた別のアクセス ポイントに割り当てられます。これは、チャネル 1 をまったく使用しないよりも効果的です。

コントローラによるチャネルの動的割り当て機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、1 や 2 など、802.11b/g 帯域の 2 つのオーバーラップするチャネルでは、両方が同時に 11/54Mbps を使用することはできません。コントローラは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離し、この問題を防ぎます。

コントローラは、さまざまなリアルタイムの RF 特性を検証して、チャネルの割り当てを効率的に処理します。次のような RF 特性があります。

- **アクセス ポイントの受信エネルギー**：各アクセス ポイントとその近隣のアクセス ポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- **ノイズ**：ノイズによって、クライアントおよびアクセス　ポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザ エクスペリエンスが低下します。コントローラでは、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- **802.11 干渉**：干渉とは、不正アクセス ポイントや近隣の無線ネットワークなど、無線 LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。定義済みの設定可能なしきい値（デフォルトは 10% です）を 802.11 干渉の量が超えると、アクセス ポイントからコントローラにアラートが送信されます。その場合、コントローラでは、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステム パフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネ

ルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

また、他の無線ネットワークがある場合、コントローラは、他のネットワークを補足するようにチャネルの使用を転換します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、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。チャネルにキャパシティがほとんど残っていない場合、コントローラはそのチャネルを回避できます。オーバーラップしないすべてのチャネルが使用される非常に高密度の展開では、コントローラでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。

- **利用率**：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリング エリアを比較して）一部のアクセス ポイントが他のアクセス ポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。これによってコントローラは、最も低いパフォーマンス（および利用率）が報告されているアクセス ポイントを改善するようにチャネルを割り当てることができます。
- **負荷**：チャネル構造を変更する際には、負荷を考慮して、現在無線 LAN 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。このメトリックによって、すべてのアクセス ポイントの送信パケットおよび受信パケットの数が追跡されて、アクセス ポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセス ポイントを回避し、別のアクセス ポイントにアソシエートします。

コントローラは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、ソフト決定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。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、上下のフロアにあるアクセス ポイントが全体的な無線 LAN 設定において主要な役割を果たします。

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出するように設計されています。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたしきい値を下回る Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）レベルで Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからコントローラに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。コントローラでは、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジ ホールの場合、コントローラでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジ ホールがコントローラによって解消されることはありません。ダウンストリームの送信電力を増加させても、アップストリームのパフォーマンスの低さを改善することは不可能であり、ネットワーク内の干渉を増加させる可能性があるからです。

（注） 管理者は、Cisco Wireless Control System（WCS）を使用して、カバレッジ ホールの場所を表示できます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

クライアントとネットワークのロード バランシング

RRM は、各コントローラにレポートするようにグループ化された Lightweight アクセス ポイント間で、新しいクライアントをロード バランシングします。RRM により、一部の登録者を近くのアクセス ポイントへ自動的にアソシエートして、すべてのクライアントのスループットを高めることができます。したがって、会議室や講堂など、多数のクライアントが 1 か所に集中する場合は、この機能が特に重要になります。コントローラでは、すべてのアクセス ポイントにおけるクライアントの負荷についての集中ビューが提供されます。この情報に基づいて、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できます。また、既存のクライアントを新しいアクセス ポイントに配置して、無線 LAN のパフォーマンスを向上させることもできます。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。

（注） クライアントのロード バランシングは、1 つのコントローラのみで動作します。マルチコントローラ環境では動作しません。

RRM の利点

RRM によって、最適なキャパシティ、パフォーマンス、および信頼性を備えたネットワークが構築されると同時に、面倒な履歴データの解釈と個々の Lightweight アクセス ポイントの再設定にかかる負担を避けることができます。また、一過性でトラブルシューティングが困難なノイズや干渉の問題を確認するために常時ネットワークを監視する必要がなくなります。最終的には、RRM によって、クライアントは Cisco Unified Wireless Network 経由による、シームレスで円滑な接続を利用できるようになります。

RRM では、配備されているネットワーク（802.11a および 802.11b/g）ごとに監視と制御が実施されます。つまり、無線タイプ（802.11a および 802.11b/g）ごとに RRM アルゴリズムが実行されます。RRM では、測定とアルゴリズムの両方が使用されます。RRM による測定については、監視間隔を使用して調整できます。ただし、RRM を無効にすることはできません。一方 RRM アルゴリズムは自動的に有効になりますが、チャネルや電力の割り当てを静的に設定することで無効にすることができます。RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。

（注） 過去 100 ミリ秒の間に音声トラフィックがあった場合、トラフィックが Platinum QoS キューに残っている各アクセス ポイントでは RRM 測定が延期されます。

RF グループの概要

RF グループは、RF ドメインとも呼ばれ、802.11 ネットワークごとに RRM による計算の調整を行うコントローラのクラスタです。802.11 ネットワーク タイプごとに RF グループが存在します。コントローラを RF グループにクラスタ化することで、複数のコントローラに RRM アルゴリズムを拡張できます。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。RRM アルゴリズムでは、コントローラで設定されて各アクセス ポイントに送信される共有秘密が使用されます。同じ秘密を共有するアクセス ポイントは、相互から送信されたメッセージを検証できます。検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが -80dBm 以上の信号強度で受信すると、コントローラによって RF グループが動的に生成されます。

（注） RF グループとモビリティ グループは、どちらもコントローラのクラスタを定義するという点では同じですが、用途に関しては異なります。この 2 つの概念がよく混同されるのは、スタートアップ ウィザードでモビリティ グループ名と RF グループ名が同じ名前に設定されるためです。さらにほとんどの場合、RF グループ内のすべてのコントローラが同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラが同じ RF グループに属します。ただし、RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現します。モビリティ グループの詳細は、第 11 章を参照してください。

RF グループ リーダー

RF グループのメンバーによって、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 グループ リーダーが選ばれます。RF グループ リーダーは動的に選択されます。ユーザが選択することはできません。また、RF グループ リーダーは、RRM アルゴリズム計算に基づいて、いつでも変更できます。

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て、マスター電力を算出し、チャネル計画を作成します。RRM のアルゴリズムでは、すべてのアクセス ポイント間の信号強度を約 -65dBm に最適化し、同じ 802.11 チャネルの干渉とコンテンション、および 802.11 以外の干渉を回避するよう試みられます。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、最適な電力およびチャネル計画が動的に策定されます。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合い間に、RF グループ リーダーは各 RF グループ メンバーにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。

（注） 複数の監視間隔を使用することもできます。詳細は、「RRM の設定」の項（P. 10-12）を参照してください。

RF グループ名

コントローラには RF グループ名が設定されます。この RF グループ名は、そのコントローラに結合されているすべてのアクセス ポイントに送信され、アクセス ポイントでは、この名前がハッシュ MIC をネイバー メッセージで生成するための共有秘密として使用されます。RF グループを作成するには、グループに含めるすべてのコントローラに同じ RF グループ名を設定すればよいだけです。RF グループには、最大 20 のコントローラと 1000 のアクセス ポイントを含めることができます。

コントローラに結合されているアクセス ポイントが別のコントローラ上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらのコントローラに同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

RF グループの設定

この項では、GUI または CLI を使用して RF グループを設定する手順について説明します。

（注） 通常、RF グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて変更できます。

（注） 複数の国コード機能を使用している場合、同じ RF グループに接続する予定のすべてのコントローラは、同じ国で構成された一連の国々を同じ順序で設定する必要があります。

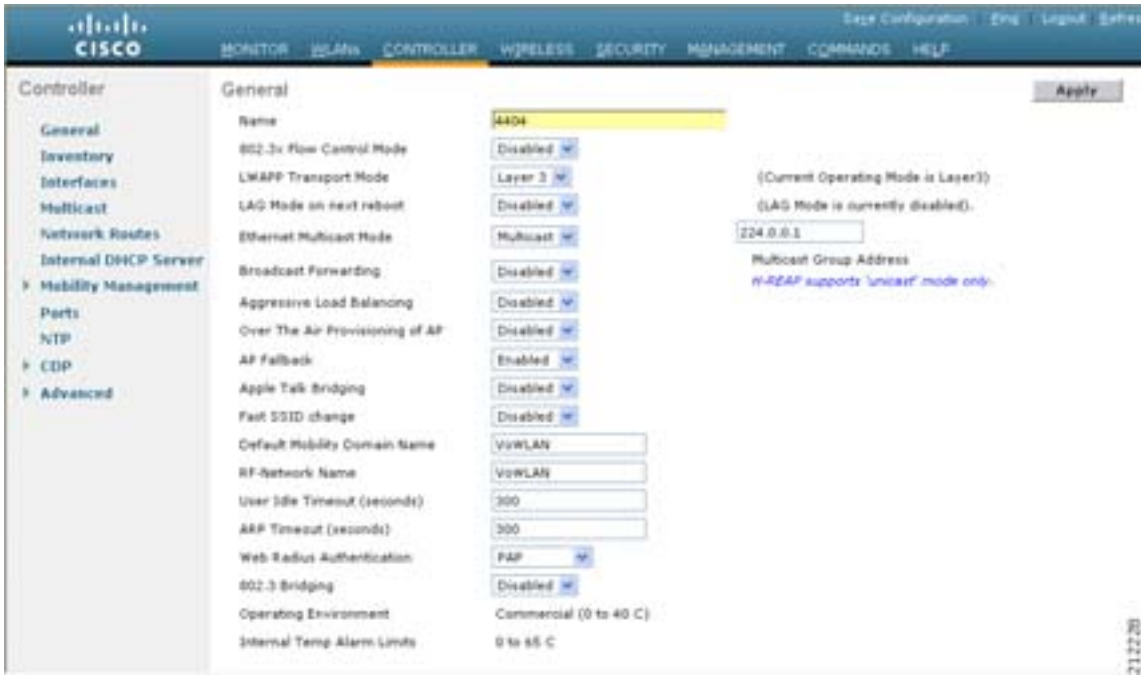
（注） Cisco Wireless Control System（WCS）を使用して RF グループを設定することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

GUI を使用した RF グループの設定

GUI を使用して RF グループを作成する手順は、次のとおりです。

ステップ 1　**Controller** > **General** の順にクリックして、General ページを開きます（図 10-1 を参照）。

図 10-1　General ページ



ステップ 2　RF-Network Name フィールドに RF グループの名前を入力します。名前には、19 文字以内の ASCII 文字を使用できます。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 5　RF グループに含める各コントローラについて、この手順を繰り返します。

CLI を使用した RF グループの設定

CLI を使用して RF グループを設定する手順は、次のとおりです。

ステップ 1　**config network rf-network-name** *name* と入力して、RF グループを作成します。

（注）　グループ名として 19 文字以内の ASCII 文字を入力します。

ステップ 2　**show network** と入力して、RF グループを表示します。

ステップ 3　**save config** と入力して、設定を保存します。

ステップ 4　RF グループに含める各コントローラについて、この手順を繰り返します。

RF グループ ステータスの表示

この項では、GUI または CLI を使用して RF グループのステータスを表示する手順について説明します。

（注） Cisco Wireless Control System（WCS）を使用して RF グループのステータスを表示することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

GUI を使用した RF グループ ステータスの表示

GUI を使用して RF グループのステータスを表示する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **RF Grouping** の順にクリックして、802.11a（または 802.11b/g）RRM > RF Grouping ページを開きます（図 10-2 を参照）。

図 10-2　802.11a > RRM > RF Grouping ページ

このページには、RF グループの詳細が示されます。具体的には、グループ情報の更新間隔（デフォルトでは 600 秒）、RF グループ リーダーの MAC アドレス、この特定のコントローラがグループ リーダーであるかどうか、グループ情報の最終更新時間、およびすべてのグループ メンバーの MAC アドレスです。

（注） **Group Mode** チェックボックスを使用して設定する自動 RF グループ化は、デフォルトで有効になっています。このパラメータの詳細は、「GUI を使用した RF グループ モードの設定」の項（P. 10-12）を参照してください。

ステップ 2　必要に応じて、選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

CLI を使用した RF グループ ステータスの表示

CLI を使用して RF グループのステータスを表示する手順は、次のとおりです。

ステップ 1　**show advanced 802.11a group** と入力して、802.11a RF ネットワークの RF グループ リーダーであるコントローラを表示します。次のような情報が表示されます。

```
Radio RF Grouping
      802.11a Group Mode.............................. AUTO
      802.11a Group Update Interval................... 600 seconds
      802.11a Group Leader............................ 00:16:9d:ca:d9:60
     802.11a Group Member........................... 00:16:9d:ca:d9:60
      802.11a Last Run................................ 594 seconds ago
```

このテキストは、RF グループの詳細を示しています。具体的には、このコントローラで自動 RF グループ化が有効かどうか、グループ情報の更新間隔（デフォルトでは 600 秒）、RF グループ リーダーの MAC アドレス、この特定のコントローラの MAC アドレス、およびグループ情報の最終更新時間です。

（注）　グループ リーダーとグループ メンバーの MAC アドレスが同じ場合、そのコントローラは現在、グループ リーダーです。

ステップ 2　**show advanced 802.11b group** と入力して、802.11b/g RF ネットワークの RF グループ リーダーであるコントローラを表示します。

RRM の設定

コントローラで事前設定された RRM 設定は、ほとんどの展開向けに最適化されています。ただし、GUI または CLI を使用して、コントローラの RRM 設定パラメータをいつでも変更できます。

（注） RF グループの一部であるコントローラ上、または RF グループの一部でないコントローラ上で、これらのパラメータを設定できます。

（注） RRM パラメータは、RF グループ内のすべてのコントローラで同じ値に設定する必要があります。RF グループ リーダーは、いつでも変更できます。RRM パラメータの異なる RF グループ メンバがある場合は、グループ リーダーが変更されると、異なる結果が生じることがあります。

GUI を使用した RRM の設定

コントローラの GUI を使用して設定できる RRM パラメータは、RF グループ モード、送信電力の制御、チャネルの動的割り当て、カバレッジ ホールの検出、プロファイルしきい値、監視チャネル、および監視間隔です。これらのパラメータを設定するには、次の項の指示に従ってください。

GUI を使用した RF グループ モードの設定

コントローラの GUI を使用して RF グループ モードを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **RF Grouping** の順にクリックして、802.11a（または 802.11b/g）RRM > RF Grouping ページを開きます（図 10-2 を参照）。

ステップ 2　**Group Mode** チェックボックスをオンにして、このコントローラが RF グループに参加できるようにするか、またはオフにしてこの機能を無効化します。この機能を有効にすると、コントローラによって、他のコントローラを含む RF グループが自動的に生成されます。グループでは、グループの RMM パラメータの設定を最適化するためのリーダーが動的に選ばれます。無効にすると、コントローラは、自動 RF グループ化に参加せずに、コントローラに直接接続されているアクセス ポイントを最適化します。デフォルト値はオンです。

（注） コントローラが自動 RF グループ化に関連するように設定することをお勧めします。RRM の設定を無効にする際には、自動 RF グループ化への参加を無効にする必要はありません。手順については、「RRM の無効化」の項（P. 10-26）を参照してください。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

GUI を使用した送信電力の制御の設定

コントローラの GUI を使用して送信電力の動的制御を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **TPC** の順にクリックして、802.11a（または 802.11b/g）> RRM > Tx Power Control (TPC) ページを開きます（図 10-3 を参照）。

図 10-3　802.11a > RRM > Tx Power Control (TPC) ページ

ステップ 2　Power Level Assignment Method ドロップダウン ボックスから次のオプションのいずれかを選択して、コントローラの動的電力割り当てモードを指定します。

- **Automatic**：コントローラによって、結合されているすべてのアクセス ポイントの送信電力が定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- **On Demand**：コントローラによって、結合されているすべてのアクセス ポイントの送信電力が定期的に評価されます。ただし、**Invoke Power Update Now** をクリックした場合のみ、必要に応じて電力が更新されます。

（注）　**Invoke Power Update Now** をクリックしても、すぐに送信電力の評価と更新が行われるわけではありません。次の間隔（600 秒）まで待機します。この値は設定可能です。

- **Fixed**：コントローラによって、結合されているアクセス ポイントの送信電力が評価されたり、必要に応じて更新されたりすることはありません。電力レベルは、ドロップダウン ボックスから選択した固定値に設定されます。

（注）　送信電力レベルには、mW や dBm による値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な送信電力レベルについては、ステップ 4（P. 10-28）を参照してください。

（注）　最適なパフォーマンスを確保するには、Automatic 設定を使用することをお勧めします。コントローラのチャネルおよび電力の動的設定を無効にする必要がある場合、手順については「コントローラにおけるチャネルおよび電力の動的割り当てのグローバルな無効化」の項（P. 10-30）を参照してください。

このページには、次のような送信電力レベルのパラメータの設定も表示されますが、これらは設定できません。

- **Power Threshold**：RRM で、アクセス ポイントの電力を減らすかどうかを判断する際に使用される切断信号レベルです。このパラメータのデフォルト値は -65 dBm です。まれに、アクセス ポイントが送信する電力レベルが必要以上に高い (または低い) 場合は、コントローラ CLI を使用して変更できます。CLI コマンドについては、「CLI を使用した RRM の設定」の項（P. 10-20）を参照してください。
- **Power Neighbor Count**：送信電力制御アルゴリズムを実行するためにアクセス ポイントに必要なネイバーの最小数です。
- **Power Assignment Leader**：電力レベルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- **Last TPC Iteration**：RRM が現在の送信電力レベルの割り当てを最後に評価した時間です。

ステップ 3　**Apply** をクリックして、変更を適用します。

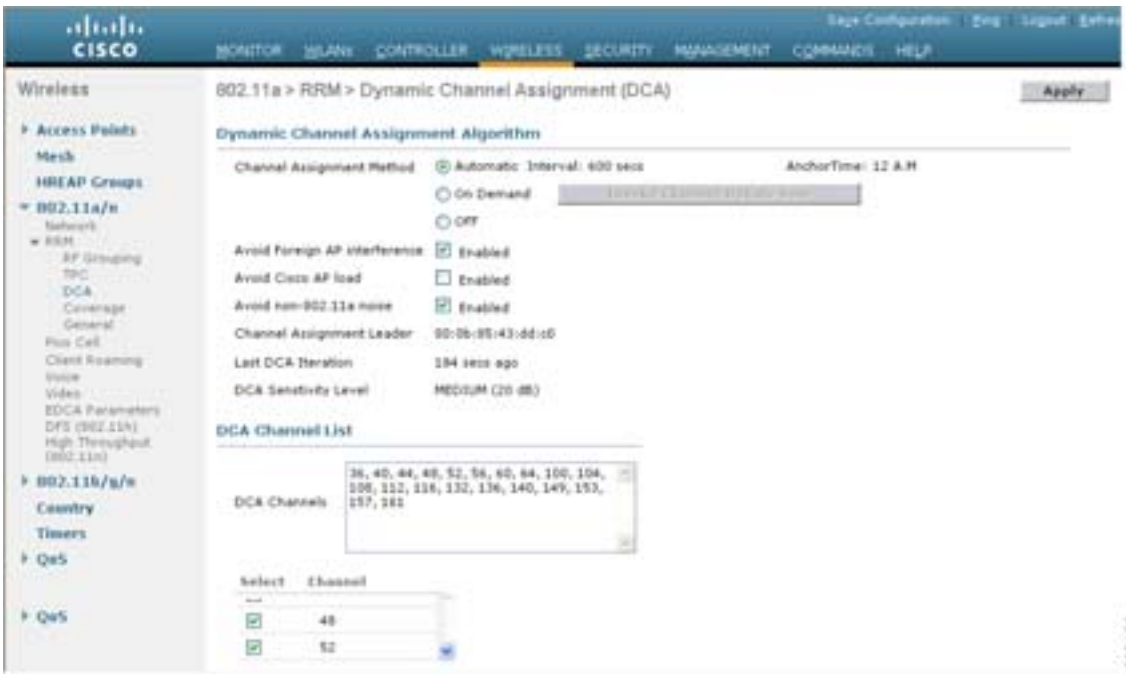
ステップ 4　**Save Configuration** をクリックして、変更内容を保存します。

GUI を使用したチャネルの動的割り当ての設定

RRM スキャンに使用されるチャネルが動的チャネル割り当て（DCA）アルゴリズムで選択される際に考慮されるチャネルを、コントローラの GUI を使用して指定する手順は、次のとおりです。この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャネルがサポートされないことがわかっている場合に役立ちます。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **DCA** の順にクリックして、802.11a（または 802.11b/g）> RRM > Dynamic Channel Assignment (DCA) ページを開きます（図 10-4 を参照）。

図 10-4　802.11a > RRM > Dynamic Channel Assignment (DCA) ページ



ステップ 2　Channel Assignment Method ドロップダウン ボックスから次のオプションのいずれかを選択して、コントローラの DCA モードを指定します。

- **Automatic**：コントローラによって、結合されているすべてのアクセス ポイントのチャネル割り当てが定期的に評価され、必要に応じて更新されます。これはデフォルト値です。
- **On Demand**：コントローラによって、結合されているすべてのアクセス ポイントのチャネル割り当てが定期的に評価されます。ただし、**Invoke Channel Update Now** をクリックした場合のみ、必要に応じてチャネルが再割り当てされます。

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

- **OFF**：コントローラによって、結合されているアクセス ポイントのチャネル割り当てが評価されたり、必要に応じて更新されたりすることはありません。

（注）　最適なパフォーマンスを確保するには、Automatic 設定を使用することをお勧めします。コントローラのチャネルおよび電力の動的設定を無効にする必要がある場合、手順については「コントローラにおけるチャネルおよび電力の動的割り当てのグローバルな無効化」の項（P. 10-30）を参照してください。

Interval フィールドには、設定されている DCA アルゴリズムの実行頻度が表示されます。デフォルト値は 600 秒です。Anchor Time フィールドには、設定されている DCA アルゴリズムの開始時刻が表示されます。範囲は、午前 12:00 ～ 午後 11:00 です。

（注）　間隔とアンカー時間は、コントローラ CLI を使用して設定できます。詳細は、「CLI を使用した RRM の設定」の項（P. 10-20）を参照してください。

ステップ 3　**Avoid Foreign AP Interference** チェックボックスをオンにすると、コントローラの RRM アルゴリズムで、Lightweight アクセス ポイントにチャネルを割り当てるときに、外部アクセス ポイント（無線ネットワークに含まれないもの）からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、外部アクセス ポイントに近いチャネルをアクセス ポイントが回避するようにチャネル割り当てを調整できます。デフォルト値はオンです。

ステップ 4　**Avoid Cisco AP Load** チェックボックスをオンにすると、コントローラの RRM アルゴリズムで、チャネルを割り当てるときに、無線ネットワーク内の Cisco Lightweight アクセス ポイントからの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、トラフィックの負荷が高いアクセス ポイントに適切な再利用パターンを割り当てることができます。デフォルトではオフになっています。

ステップ 5　**Avoid Non-802.11a (802.11b) Noise** チェックボックスをオンにすると、コントローラの RRM アルゴリズムで、Lightweight アクセス ポイントにチャネルを割り当てるときに、ノイズ（802.11 以外のトラフィック）が考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、電子レンジなど、アクセス ポイント以外を原因とする重大な干渉があるチャネルをアクセス ポイントに回避させることができます。デフォルト値はオンです。

このページには、次のようなチャネル パラメータの設定も表示されますが、これらは設定できません。

- **Channel Assignment Leader**：チャネルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- **Last DCA Iteration**：RRM が現在のチャネル割り当てを最後に評価した時刻です。
- **DCA Sensitivity Level**：設定されている DCA 感度設定（低、中、高）。チャネルを変更するかどうかを判断する際に、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度が、この設定によって決定されます。

（注） **config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}** CLI コマンドを使用して DCA 感度レベルを設定できます。詳細は、「CLI を使用した RRM の設定」の項（P. 10-20）を参照してください。

ステップ 6　DCA Channel List の選択時に、DCA Channels フィールドには、現在選択されているチャネルが表示されます。チャネルを選択するには、Select カラムでそのチャネルのチェックボックスをオンにします。チャネルの選択を解除するには、チャネルのチェックボックスをオフにします。

範囲：
802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165、190、196
802.11b/g：1、2、3、4、5、6、7、8、9、10、11

デフォルト：
802.11a：36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161
802.11b/g：1、6、11

ステップ 7　**Apply** をクリックして、変更を適用します。

ステップ 8　**Save Configuration** をクリックして、変更内容を保存します。

（注） DCA アルゴリズムによってチャネルが変更された理由を参照するには、**Monitor** をクリックして、次に Most Recent Traps で **View All** をクリックします。トラップにより、チャネルが変更された無線の MAC アドレス、前のチャネルと新規のチャネル、変更された理由、変更前後のエネルギー、変更前後のノイズ、変更前後の干渉が示されます。

GUI を使用したカバレッジ ホールの検出の設定

コントローラの GUI を使用してカバレッジ ホールの検出を有効にする手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **Coverage** の順にクリックして、802.11a（または 802.11b/g）> RRM > Coverage ページを開きます（図 10-5 を参照）。

図 10-5　802.11a > RRM > Coverage ページ

ステップ 2　カバレッジ ホールの検出を有効にする場合は **Enable Coverage Hole Detection** チェックボックスをオンにします。この機能を無効にする場合は、オフにします。カバレッジ ホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいてコントローラが自動的に判断します。デフォルト値はオンです。

ステップ 3　Data RSSI フィールドに、アクセス ポイントで受信されたデータ パケットの最小の受信信号強度インジケータ（RSSI）を入力します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は -60 ～ -90dBm で、デフォルト値は -80dBm です。アクセス ポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔でコントローラにレポートされます。

ステップ 4　Voice RSSI フィールドに、アクセス ポイントで受信された音声パケットの最小の受信信号強度インジケータ（RSSI）を入力します。入力する値は、ネットワーク内のカバレッジ ホールを特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は -60 ～ -90dBm で、デフォルト値は -75dBm です。アクセス ポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔でコントローラにレポートされます。

ステップ 5　Min Failed Client Count per AP フィールドに、RSSI 値がデータ RSSI または音声 RSSI のしきい値以下であるアクセス ポイント上のクライアントの最小数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 6　Coverage Exception Level per AP フィールドに、信号レベルが低くなっているにもかかわらず別のアクセス ポイントにローミングできない、アクセス ポイント上のクライアントの割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、Failed Packet Count および Failed Packet Percentage（コントローラの CLI を使用して設定可能。（P. 10-22）を参照）に設定された値を超える場合、クライアントは事前アラーム状態と判断されます。コントローラでは、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールが区別され、ローミング ロジックが不完全なクライアントが除外されます。90 秒間で失敗したクライアントの数と割合の両方が、Min Failed Client Count per AP および Coverage Exception Level per AP フィールドに入力された値を満たすか超えている場合、カバレッジ ホールが検出されます。コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、適切な場合は、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。

ステップ 7　**Apply** をクリックして、変更を適用します。

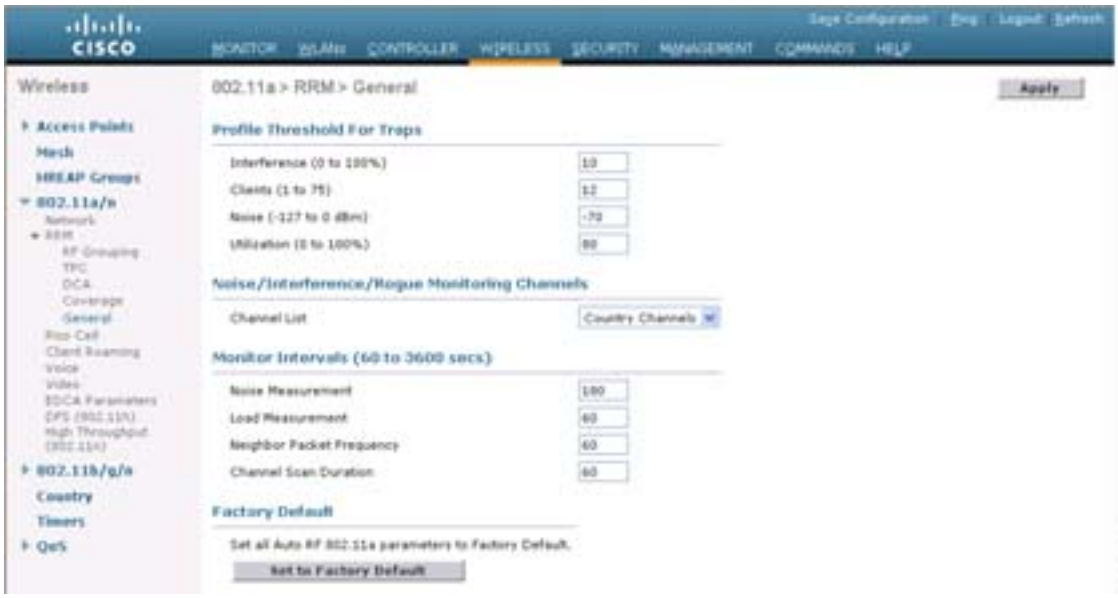
ステップ 8　**Save Configuration** をクリックして、変更内容を保存します。

GUI を使用した RRM プロファイルしきい値、監視チャネル、および監視間隔の設定

コントローラの GUI を使用して RRM プロファイルしきい値、監視チャネル、および監視間隔を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **General** の順にクリックして、802.11a（または 802.11b/g）> RRM > General ページを開きます（図 10-6 を参照）。

図 10-6　802.11a > RRM > General ページ



ステップ 2　アラームに使用されるプロファイルしきい値を設定する手順は、次のとおりです。

（注）　プロファイルしきい値は、RRM アルゴリズムの機能には関係ありません。これらのしきい値パラメータに設定された値を超えると、Lightweight アクセス ポイントからコントローラに SNMP トラップ（またはアラート）が送信されます。

a. Interference フィールドに、1 つのアクセス ポイントにおける干渉（無線ネットワーク外の発信元からの 802.11 トラフィック）の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 10% です。

b. Clients フィールドに、1 つのアクセス ポイントにおけるクライアントの数を入力します。有効な範囲は 1 ～ 75 で、デフォルト値は 12 です。

c. Noise フィールドに、1 つのアクセス ポイントにおけるノイズ（802.11 以外のトラフィック）のレベルを入力します。有効な値の範囲は -127 ～ 0dBm で、デフォルト値は -70dBm です。

d. Utilization フィールドに、1 つのアクセス ポイントで使用されている RF 帯域の割合を入力します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 80% です。

ステップ 3　Channel List ドロップダウン ボックスから次のオプションのいずれかを選択して、アクセス ポイントで RRM によるスキャンに使用されるチャネルのセットを指定します。

- **All Channels**：選択した無線でサポートされているすべてのチャネルで、RRM によるチャネル スキャンが実行されます。使用国で有効でないチャネルも対象となります。
- **Country Channels**：使用国内の D チャネルのみで、RRM によるチャネル スキャンが実行されます。これはデフォルト値です。
- **DCA Channels**：DCA アルゴリズムによって使用されるチャネル セットのみで、RRM によるチャネル スキャンが実行されます。デフォルトでは、使用国で有効な、オーバーラップしないすべてのチャネルが対象となります。ただし、必要に応じて、DCA で使用するチャネル セットを指定できます。指定するには、「GUI を使用したチャネルの動的割り当ての設定」の項（P. 10-14）の手順に従ってください。

ステップ 4　監視間隔を設定する手順は、次のとおりです。

a. Noise Measurement フィールドに、アクセス ポイントでノイズや干渉が測定される間隔（秒）を入力します。有効な範囲は 60 ～ 3600 秒で、デフォルト値は 180 秒です。

b. Load Measurement フィールドに、アクセス ポイントでチャネルの負荷に関する情報が収集される頻度（秒）を入力します。収集された情報は、DCA アルゴリズムに取り込まれます。有効な値の範囲は 60 ～ 3600 秒で、デフォルト値は 60 秒です。

c. Neighbor Packet Frequency フィールドに、アクセス ポイントで信号強度が測定される間隔、およびネイバー パケット（メッセージ）が送信されて最終的にネイバー リストが構築される間隔を秒単位で入力します。有効な値の範囲は 60 ～ 3600 秒で、デフォルト値は 60 秒です。

d. Channel Scan Duration フィールドに、無線帯域内の各チャネルでスキャンを実行する時間間隔の合計（秒）を入力します。スキャン プロセス全体の所要時間はチャネル、無線ごとに 50 分であり、Channel Scan Duration に指定された間隔で実行されます。各チャネルをリッスンするための所要時間は、50 分のスキャン時間（設定不可）とスキャン対象チャネル数によって決まります。たとえば、米国では、11 個の 802.11b/g チャネルがすべて、デフォルトの 180 秒の間隔で、50 分間ずつスキャンされます。したがって、各スキャン チャネルで 16 秒ごとに 50 分がリッスンに費やされます（180/11 = ～ 16 秒）。スキャン プロセス全体に割り当てられている時間。スキャンが実行される間隔は、Channel Scan Duration パラメータによって決まります。有効な値の範囲は 60 ～ 3600 秒で、802.11a 無線のデフォルト値は 60 秒、802.11b/g 無線のデフォルト値は 180 秒です。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

（注）　コントローラの　RRM　関連パラメータをすべて工場出荷時のデフォルト値に戻す場合は、**Set to Factory Default** をクリックします。

CLI を使用した RRM の設定

コントローラの CLI を使用して RRM を設定する手順は、次のとおりです。

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

config {**802.11a** | **802.11b**} **disable**

ステップ 2　送信電力の制御に関して設定するには、次のいずれかの操作を行います。

- すべての 802.11a または 802.11b/g 無線の送信電力が定期的に RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **txPower global auto**
- すべての 802.11a または 802.11b/g 無線の送信電力が一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **txPower global once**
- デフォルトの送信電力設定 -65dBm を手動で変更するには、次のコマンドを入力します。

  config advanced {**802.11a** | **802.11b**} **tx-power-control-thresh** *threshold*

  threshold は、-50 ～ -80dBm の値です。この値を -50 ～ -65dBm の範囲で増やすと、アクセス ポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。

  多数のアクセス ポイントを使用しているアプリケーションでは、しきい値を -75dBm または -80dBm に減らして、無線クライアントが認識可能な BSSID（アクセス ポイント）やビーコンの数を少なくするとよいでしょう。一部の無線クライアントは多数の BSSID や高速ビーコンを処理できない場合があり、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

（注）　詳細は、「GUI を使用した送信電力の制御の設定」の項（P. 10-13）の Power Threshold についての説明を参照してください。

ステップ 3　チャネルの動的割り当て（DCA）を設定するには、次のいずれかの操作を行います。

- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャネルが RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **channel global auto**
- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャネルが一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

config {802.11a | 802.11b} channel global once

- RRM を無効にし、すべてのチャネルをデフォルト値に設定するには、次のコマンドを入力します。

  config {802.11a | 802.11b} channel global off

- DCA に使用するチャネル セットを指定するには、次のコマンドを入力します。

  config advanced {802.11a | 802.11b} channel {add | delete} *channel_number*

  コマンドごとに 1 つのチャネル番号のみを入力できます。このコマンドは、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャネルがサポートされないことがわかっている場合に役立ちます。

ステップ 4　追加の DCA パラメータを設定するには、次のコマンドを使用します。

- **config advanced {802.11a | 802.11b} channel dca anchor-time** *value*：DCA アルゴリズムの開始時刻を指定します。*value* は、午前 12:00 ～ 午後 11:00 の時刻を表す、0 ～ 23（両端の値を含む）の数値です。
- **config advanced {802.11a | 802.11b} channel dca interval** *value*：DCA アルゴリズムの実行が許可される頻度を指定します。*valu* には、時間単位で 1、2、3、4、6、8、12、または 24 のいずれかの値を指定するか、デフォルト値の 10 分（すなわち 600 秒）を示す 0 を指定します。
- **config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}**：DCA アルゴリズムでチャネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する感度を指定します。
  - **low** の場合、環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
  - **medium** の場合、環境の変化に対する DCA アルゴリズムの感度は中程度です。
  - **high** の場合、環境の変化に対する DCA アルゴリズムの感度が高くなります。

  DCA の感度のしきい値は、次のように、無線帯域によって異なります（表 10-1 を参照）。

表 10-1　DCA の感度のしきい値

	2.4GHz での DCA の感度のしきい値	5GHz での DCA の感度のしきい値
High	5dB	5dB
Medium	15dB	20dB
Low	30dB	35dB

- **config advanced {802.11a | 802.11b} channel foreign {enable | disable}**：チャネル割り当てにおける外部アクセス ポイントの干渉の回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel load {enable | disable}**：チャネル割り当てにおける負荷の回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel noise {enable | disable}**：チャネル割り当てにおけるノイズの回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel update**：すべてのシスコ アクセス ポイントのチャネル選択の更新を開始します。

ステップ 5　カバレッジ ホールの検出を設定するには、次のコマンドを使用します。

- **config advanced {802.11a | 802.11b} coverage {enable | disable}**：カバレッジ ホールの検出を有効または無効にします。カバレッジ ホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいてコントローラが自動的に判断します。デフォルト値は有効（enable）です。

- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*：アクセス ポイントによって受信されるパケットの受信信号強度インジケータ（RSSI）の最小値を指定します。入力する値は、ネットワーク内のカバレッジ ホール（またはカバレッジが不完全な領域）を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータ キューまたは音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は -60 ～ -90dBm で、データ パケットのデフォルト値は -80dBm、音声パケットのデフォルト値は -75dBm です。アクセス ポイントでは、RSSI が 5 秒おきに測定され、それらが 90 秒間隔でコントローラにレポートされます。
- **config advanced** {**802.11a** | **802.11b**} **coverage level global** *clients*：RSSI 値がデータ RSSI または音声 RSSI のしきい値以下であるアクセス ポイント上のクライアントの最小数を指定します。有効な範囲は 1 ～ 75 で、デフォルト値は 3 です。
- **config advanced** {**802.11a** | **802.11b**} **coverage exception global** *percent*：信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないアクセス ポイント上のクライアントの割合を指定します。有効な値の範囲は 0 ～ 100% で、デフォルト値は 25% です。
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **packet-count** *packets*：アップリンク データまたは音声パケットの最小失敗回数のしきい値を指定します。有効な値の範囲は 1 ～ 255 パケットで、デフォルト値は 10 パケットです。
- **config advanced** {**802.11a** | **802.11b**} **coverage** {**data** | **voice**} **fail-rate** *percent*：アップリンク データまたは音声パケットの失敗率のしきい値を指定します。有効な値の範囲は 1 ～ 100% で、デフォルト値は 20% です。

（注） 5 秒間で失敗したパケットの数と割合の両方が、**packet-count** および **fail-rate** コマンドに入力された値を超える場合、クライアントは事前アラーム状態と判断されます。コントローラでは、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールが区別され、ローミング ロジックが不完全なクライアントが除外されます。90 秒間で失敗したクライアントの数と割合の両方が、**coverage level global** および **coverage exception global** コマンドで入力された値を満たすか超えている場合、カバレッジ ホールが検出されます。コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、適切な場合は、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。

ステップ 6　次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

config {**802.11a** | **802.11b**} **enable**

（注） 802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 7　次のコマンドを入力して、設定を保存します。

save config

CLI を使用した RRM 設定の表示

802.11a および 802.11b/g のその他の RRM 設定を表示するには、次のコマンドを使用します。

show advanced {**802.11a** | **802.11b**} *?*

? は、次のいずれかです。

- **ccx** {**global** | *Cisco_AP*}：CCX RRM 設定を表示します。

```
802.11a Client Beacon Measurements:
    disabled
```

- **channel**：チャネル割り当ての設定および統計情報を表示します。

```
Automatic Channel Assignment
  Channel Assignment Mode....................... AUTO
  Channel Update Interval....................... 600 seconds
  Anchor time (Hour of the day)................. 0
  Channel Update Contribution................... SNI.
  Channel Assignment Leader..................... 00:0b:85:43:dd:c0
  Last Run...................................... 426 seconds ago

  DCA Sensitivity Level: ..................... MEDIUM (20 dB)
  Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List.................. 36,40,44,48,52,56,60,64,100,
    ............................................ 104,108,112,116,132,136,140,
    ............................................ 149,153,157,161
  Auto-RF Unused Channel List................. 165,190,196
```

- **coverage**：カバレッジ ホールの検出の設定および統計に関する情報を表示します。

```
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode.......... Enabled
  802.11a Coverage Voice Packet Count........... 10 packets
  802.11a Coverage Voice Packet Percentage...... 20%
  802.11a Coverage Voice RSSI Threshold......... -75 dBm
  802.11a Coverage Data Packet Count............ 10 packets
  802.11a Coverage Data Packet Percentage....... 20%
  802.11a Coverage Data RSSI Threshold.......... -80 dBm
  802.11a Global coverage exception level....... 25%
  802.11a Global client minimum exception lev. 3 clients
```

- **logging**：RF イベント ログおよびパフォーマンス ログを表示します。

```
RF Event and Performance Logging
  Channel Update Logging........................ Off
  Coverage Profile Logging...................... Off
  Foreign Profile Logging....................... Off
  Load Profile Logging.......................... Off
  Noise Profile Logging......................... Off
  Performance Profile Logging................... Off
  TxPower Update Logging..................... Off
```

- **monitor**：シスコの無線監視に関する情報を表示します。

```
Default 802.11a AP monitoring
  802.11a Monitor Mode.......................... enable
  802.11a Monitor Channels...................... Country channels
  802.11a AP Coverage Interval.................. 180 seconds
  802.11a AP Load Interval...................... 60 seconds
  802.11a AP Noise Interval..................... 180 seconds
  802.11a AP Signal Strength Interval......... 60 seconds
```

- **profile** {**global** | *Cisco_AP*}：アクセス ポイントのパフォーマンス プロファイルを表示します。

```
Default 802.11a AP performance profiles
  802.11a Global Interference threshold......... 10%
  802.11a Global noise threshold................. -70 dBm
  802.11a Global RF utilization threshold........ 80%
  802.11a Global throughput threshold............ 1000000 bps
  802.11a Global clients threshold............. 12 clients
```

- **receiver**：802.11a または 802.11b/g 受信装置の設定および統計情報を表示します。

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 15
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 2
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Enabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Enabled
 TxStomp  : Wrong BSSID Data Only Status......... Enabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
 RxAbort  : Low RSSI Threshold................... 0
 RxAbort  : Wrong BSSID Status................... Disabled
 RxAbort  : Wrong BSSID Data Only Status......... Disabled
 ---------------------------------------....
 pico-cell-V2 parameters in dbm units:...........

 RxSensitivity: Min,Max,Current RxSense Thres.... 0,0,0
 CCA Threshold: Min,Max,Current Clear Channel.... 0,0,0
Tx Pwr: Min,Max,Current Transmit Power for A.... 0,0,0
 ---------------------------------------....
```

- **summary**：802.11a または 802.11b/g アクセス ポイントの設定および統計情報を表示します。

```
AP Name                          Channel     TxPower Level
-------------------------------- ----------- -------------
AP1242.47b2.31f6                    132*           1*
AP0016.47b2.31ea                    132*           1*
AP1131:46f2.98ac        64*           1*
```

- **txpower**：送信電力割り当ての設定および統計情報を表示します。

```
Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Threshold....................... -65 dBm
  Transmit Power Neighbor Count.................. 3 APs
  Transmit Power Update Contribution............. SNI.
  Transmit Power Assignment Leader............... 00:0b:85:43:dd:c0
  Last Run....................................... 360 seconds ago
```

CLI を使用した RRM の問題のデバッグ

RRM の動作のトラブルシューティングおよび検証には、以下のコマンドを使用します。

debug airewave-director *?*

? は、次のいずれかです。

- **all**：すべての RRM ログのデバッグを有効にします。
- **channel**：RRM チャネル割り当てプロトコルのデバッグを有効にします。
- **detail**：RRM 詳細ログのデバッグを有効にします。
- **error**：RRM エラー ログのデバッグを有効にします。
- **group**：RRM グループ プロトコルのデバッグを有効にします。
- **manager**：RRM マネージャのデバッグを有効にします。
- **message**：RRM メッセージのデバッグを有効にします。
- **packet**：RRM パケットのデバッグを有効にします。
- **power**：RRM 電力割り当てプロトコルのデバッグとカバレッジ ホールの検出を有効にします。
- **profile**：RRM プロファイル イベントのデバッグを有効にします。
- **radar**：RRM レーダー検出 / 回避プロトコルのデバッグを有効にします。
- **rf-change**：RRM RF 変更のデバッグを有効にします。

RRM の無効化

展開方法によっては、シスコから提供されている RRM アルゴリズムを使用するよりも、チャネルや送信電力の設定を静的にアクセス ポイントに割り当てる方が適している場合があります。通常、これは厳しい RF 環境や一般的でない展開に該当し、カーペットを敷いた一般的なオフィスには該当しません。

（注） チャネルおよび電力レベルを静的にアクセス　ポイントに割り当てる場合や、チャネルおよび電力の動的割り当てを無効にする場合でも、自動 RF グループ化を使用して不要な不正デバイス イベントを回避することが必要です。

チャネルおよび電力の動的割り当てをコントローラでグローバルに無効にすることも、チャネルおよび電力の動的割り当てを有効にしたまま、アクセス ポイント無線ごとにチャネルおよび電力を静的に設定することもできます。次のいずれかの項に記載された手順に従ってください。

- アクセス ポイント無線へのチャネルおよび送信電力設定の静的割り当て（P. 10-26）
- コントローラにおけるチャネルおよび電力の動的割り当てのグローバルな無効化（P. 10-30）

（注） コントローラ上のすべてのアクセス　ポイント無線に適用されるグローバルなデフォルトの送信電力パラメータをネットワーク タイプごとに指定できますが、チャネルの動的割り当てを無効にした場合は、アクセス ポイント無線ごとにチャネルを設定する必要があります。また、グローバルな送信電力を有効にしておく代わりに、アクセス ポイントごとに送信電力を設定することもできます。

（注） Cisco Wireless Control System（WCS）を使用して RRM を無効にすることもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

アクセス ポイント無線へのチャネルおよび送信電力設定の静的割り当て

この項では、GUI または CLI を使用してチャネルおよび電力設定を静的に割り当てる手順について説明します。

（注） 相互に隣接するアクセス　ポイントには、オーバーラップしない別のチャネルを割り当てることをお勧めします。米国のオーバーラップしないチャネルは、802.11a ネットワークでは 36、40、44、48、52、56、60、64、149、153、157、および 161、802.11b/g ネットワークでは 1、6、および 11 です。

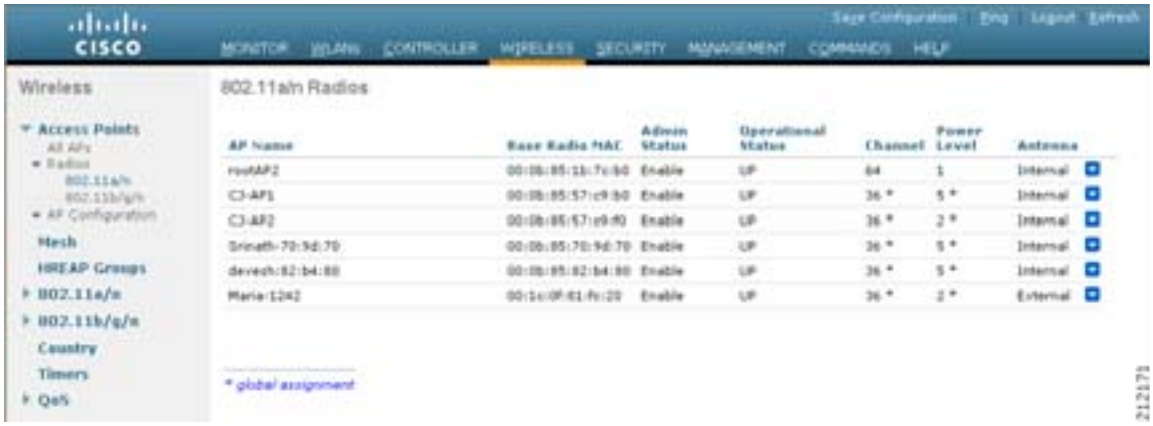
（注） 相互に隣接するすべてのアクセス ポイントを最大電力レベルに割り当てないようお勧めします。

GUI を使用したチャネルおよび送信電力設定の静的割り当て

GUI を使用して、アクセス ポイント無線ごとにチャネルや電力の設定を静的に割り当てる手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **Radios** > **802.11a/n** または **802.11b/g/n** の順にクリックして、802.11a/n（または 802.11b/g/n）Radios ページを開きます（図 10-7 を参照）。

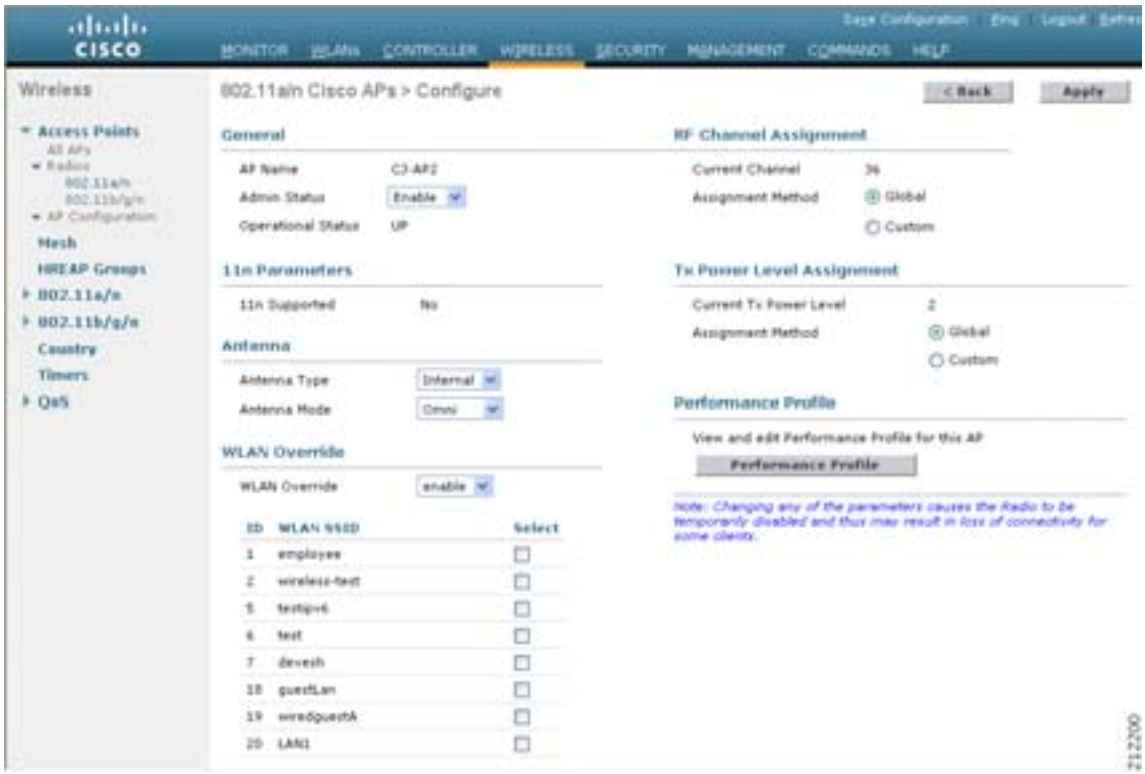
図 10-7　802.11a/n Radios ページ



このページには、コントローラに結合されているすべての 802.11a/n または 802.11b/g/n アクセス ポイント無線とその現在の設定が表示されます。

ステップ 2　無線設定を変更するアクセス ポイントの青いドロップダウンの矢印の上にカーソルを置いて、**Configure** を選択します。802.11a/n（または 802.11b/g/n）Cisco APs > Configure ページが表示されます（図 10-8 を参照）。

図 10-8　802.11a/n Cisco APs > Configure ページ



ステップ 3　RF チャネルをアクセス ポイント無線に割り当てるには、RF Channel Assignment の Assignment Method で **Custom** を選択し、ドロップダウン ボックスからチャネルを選択します。

ステップ 4　送信電力レベルをアクセス ポイント無線に割り当てるには、Tx Power Level Assignment の Assignment Method で **Custom** を選択し、ドロップダウン ボックスから送信電力レベルを選択します。

送信電力レベルには、mW 単位または dBm 単位の値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な電力レベルの数は、アクセス ポイント モデルによって異なります。ただし、電力レベル 1 は常に各国番号の設定で有効な最大電力レベルで、それ以降の各電力レベルは前の電力レベルの 50% を表します。たとえば、1 = 特定の規制区域の最大電力レベル、2 = 50% の電力、3 = 25% の電力、4 = 12.5% の電力となります。

（注）　各規制区域でサポートされている最大送信電力レベルについては、お使いのアクセス ポイントのハードウェア インストレーション ガイドを参照してください。また、サポートされている電力レベルの数については、お使いのアクセス ポイントのデータ シートを参照してください。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、アクセス ポイント無線の変更内容を保存します。

ステップ 7　静的なチャネルおよび電力レベルを割り当てる各アクセス ポイント無線について、この手順を繰り返します。

CLI を使用したチャネルおよび送信電力設定の静的割り当て

CLI を使用して、アクセス ポイント無線ごとにチャネルや電力の設定を静的に割り当てる手順は、次のとおりです。

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

config {**802.11a** | **802.11b**} **disable**

ステップ 2　特定のアクセス ポイントで使用するチャネルを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **channel** *Cisco_AP channel*

例：802.11a チャネル 36 を AP1 のデフォルト チャネルとして設定するには、次のコマンドを入力します。
config 802.11a channel AP1 36

ステップ 3　特定のアクセス ポイントで使用する送信電力レベルを指定するには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **txPower** *Cisco_AP power_level*

例：802.11a AP1 の送信電力を電力レベル 2 に設定するには、次のコマンドを入力します。
config 802.11a txPower AP1 2

送信電力レベルには、mW や dBm による値の代わりに整数値が割り当てられます。この整数は、アクセス ポイントが展開されている規制区域によって異なる電力レベルに対応します。使用可能な電力レベルの数は、アクセス ポイント モデルによって異なります。ただし、電力レベル 1 は常に各国番号の設定で有効な最大電力レベルで、それ以降の各電力レベルは前の電力レベルの 50% を表します。たとえば、1 = 特定の規制区域の最大電力レベル、2 = 50% の電力、3 = 25% の電力、4 = 12.5% の電力となります。

（注）　各規制区域でサポートされている最大送信電力レベルについては、お使いのアクセス ポイントのハードウェア インストレーション ガイドを参照してください。また、サポートされている電力レベルの数については、お使いのアクセス ポイントのデータ シートを参照してください。

ステップ 4　次のコマンドを入力して、設定を保存します。

save config

ステップ 5　静的なチャネルおよび電力レベルを割り当てる各アクセス ポイント無線について、ステップ 2 からステップ 4 を繰り返します。

ステップ 6　次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

config {802.11a | 802.11b} enable

（注）　802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 7　次のコマンドを入力して、設定を保存します。

save config

コントローラにおけるチャネルおよび電力の動的割り当てのグローバルな無効化

この項では、GUI または CLI を使用してチャネルおよび電力の動的割り当てを無効にする手順について説明します。

GUI を使用したチャネルおよび電力の動的割り当ての無効化

GUI を使用してチャネルおよび電力の動的割り当てを無効にする手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **RRM** > **Auto RF** の順にクリックして、802.11a（または 802.11b/g）Global Parameters > Auto RF ページを開きます（図 10-2 を参照）。

ステップ 2　チャネルの動的割り当てを無効にするには、RF Channel Assignment で **Off** を選択します。

ステップ 3　電力の動的割り当てを無効にするには、Tx Power Level Assignment で **Fixed** を選択し、ドロップダウン ボックスからデフォルトの送信電力レベルを選択します。

（注）　送信電力レベルについては、ステップ 4（P. 10-28）を参照してください。

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 6　無線ごとにチャネルおよび電力のデフォルト設定を無効にする場合は、コントローラに結合されている各アクセス ポイント無線にチャネルおよび電力の静的設定を割り当てます。

ステップ 7　必要に応じて、選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

CLI を使用したチャネルおよび電力の動的割り当ての無効化

すべての 802.11a または 802.11b/g 無線について RRM を無効にする手順は、次のとおりです。

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

config {**802.11a** | **802.11b**} **disable**

ステップ 2　次のコマンドを入力して、すべての 802.11a または 802.11b/g 無線について RRM を無効にし、すべてのチャネルをデフォルト値に設定します。

config {**802.11a** | **802.11b**} **channel global off**

ステップ 3　次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

config {**802.11a** | **802.11b**} **enable**

（注）　802.11g ネットワークを有効にするには、**config 802.11b enable** コマンドの後に **config 802.11b 11gSupport enable** と入力します。

ステップ 4　次のコマンドを入力して、設定を保存します。

save config

RF グループ内の不正アクセス ポイント検出の有効化

コントローラの RF グループを作成したら、コントローラに接続されているアクセス ポイントを、不正なアクセス ポイントを検出するように設定する必要があります。すると、アクセス ポイントによって、近隣のアクセス ポイントのメッセージ内のビーコン / プローブ応答フレームがチェックされ、RF グループの認証 IE（Information Element; 情報要素）と一致するものが含まれているかどうかが確認されます。チェックが正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルはコントローラに送信されます。

GUI を使用した RF グループ内の不正アクセス ポイントの検出の有効化

コントローラの GUI を使用して RF グループ内の不正アクセス ポイントの検出を有効にする手順は、次のとおりです。

ステップ 1　RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。

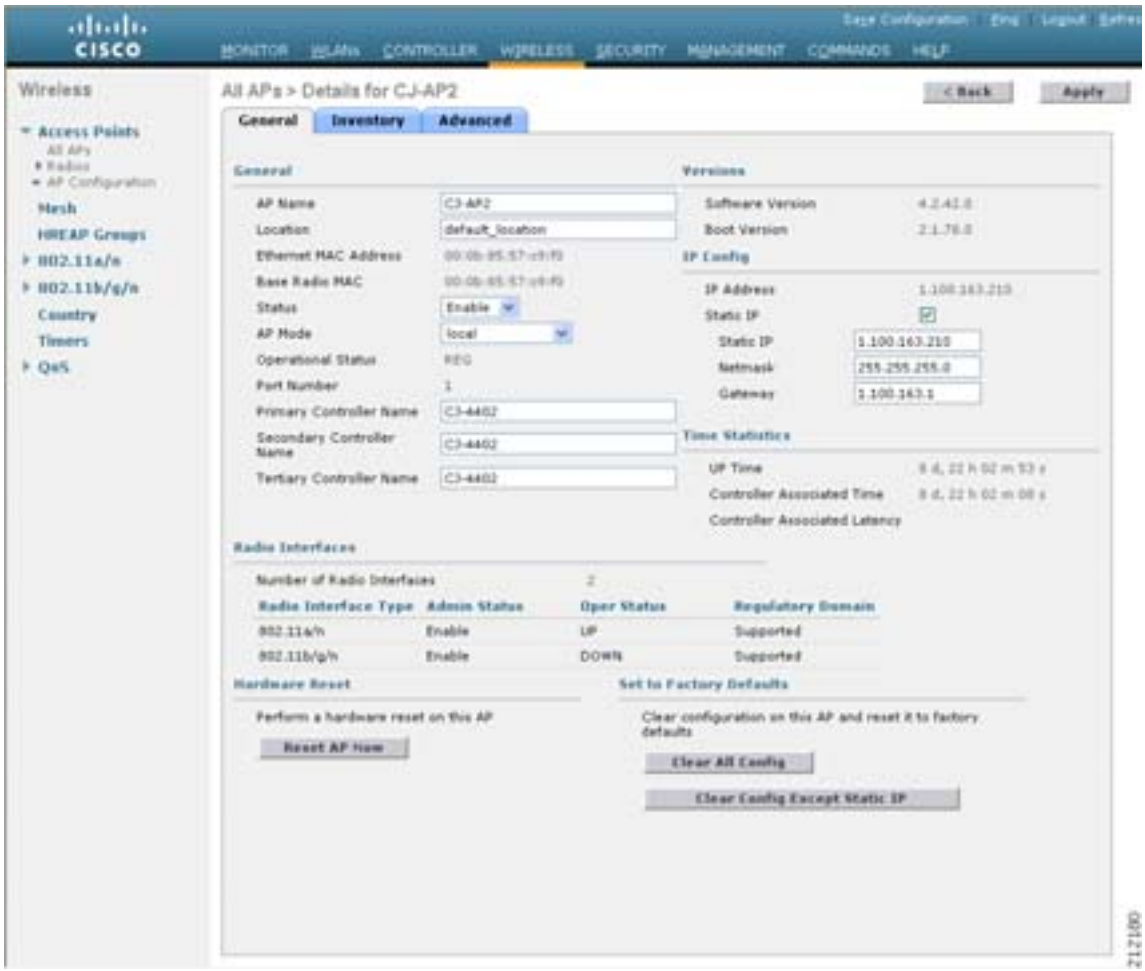
（注）　この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。各コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

ステップ 2　**Wireless** をクリックして、All APs ページを開きます（図 10-9 を参照）。

図 10-9　All APs ページ

ステップ 3　アクセス ポイントの名前をクリックして、All APs > Details ページを開きます（図 10-10 を参照）。

図 10-10　All APs > Details ページ



ステップ 4　AP Mode ドロップダウン ボックスから **local** または **monitor** を選択し、**Apply** をクリックして変更を適用します。

ステップ 5　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 6　コントローラに接続されているすべてのアクセス ポイントについて、ステップ 2 からステップ 5 を繰り返します。

ステップ 7　**Security** > **Wireless Protection Policies** > **AP Authentication/MFP** の順にクリックして、AP Authentication Policy ページを開きます（図 10-11 を参照）。

図 10-11　AP Authentication Policy ページ

このコントローラが属する RF グループの名前は、ページの上部に表示されます。

ステップ 8　Protection Type ドロップダウン ボックスから **AP Authentication** を選択して、不正アクセス ポイントの検出を有効にします。

ステップ 9　Alarm Trigger Threshold 編集ボックスに数値を入力して、不正アクセス ポイントに関するアラームがいつ生成されるようにするかを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

（注）　しきい値の有効範囲は 1 ～ 255 で、デフォルト値は 1 です。障害アラームを回避するには、しきい値を高い値に設定してください。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 12　RF グループ内のすべてのコントローラについて、この手順を繰り返します。

（注）　不正アクセス ポイントの検出が有効になっていないコントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

CLI を使用した RF グループ内の不正アクセス ポイントの検出の有効化

コントローラの CLI を使用して RF グループ内の不正アクセス ポイントの検出を有効にする手順は、次のとおりです。

ステップ 1　RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。

（注）　この名前は、すべてのビーコン フレーム内の認証 IE を検証するために使用されます。各コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

ステップ 2　**config ap mode local** *Cisco_AP* または **config ap mode monitor** *Cisco_AP* と入力して、この特定のアクセス ポイントを local（通常）モードまたは monitor（リッスン専用）モードに設定します。

ステップ 3　**save config** と入力して、設定を保存します。

ステップ 4　コントローラに接続されているすべてのアクセス ポイントについて、ステップ 2 とステップ 3 を繰り返します。

ステップ 5　**config wps ap-authentication** と入力して、不正アクセス ポイントの検出を有効にします。

ステップ 6　**config wps ap-authentication** *threshold* と入力して、不正アクセス ポイントに関するアラームがいつ生成されるようにするかを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

（注）　しきい値の有効範囲は 1 ～ 255 で、デフォルト値は 1 です。障害アラームを回避するには、しきい値を高い値に設定してください。

ステップ 7　**save config** と入力して、設定を保存します。

ステップ 8　RF グループ内のすべてのコントローラについて、ステップ 5 からステップ 7 を繰り返します。

（注）　不正アクセス ポイントの検出が有効になっていないコントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

CCX 無線管理機能の設定

クライアント ロケーションの計算に影響を与える次の 2 つのパラメータを設定できます。

- 無線測定要求
- ロケーション調整

これらのパラメータは、Cisco Client Extensions（CCX）v2 以降でサポートされており、参加する CCX クライアントのロケーションの正確性と適時性を強化するよう設計されています。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

ロケーション機能が適切に動作するように、アクセス ポイントを normal、monitor、または hybrid-REAP モードに設定する必要があります。ただし、hybrid-REAP モードの場合は、アクセス ポイントをコントローラに接続する必要があります。

（注） CCX は、AP1030 ではサポートされません。

無線測定要求

この機能が有効な場合、Lightweight アクセス ポイントは、CCXv2 以降を実行しているクライアントに、ブロードキャスト無線測定要求メッセージを発行します。Lightweight アクセス ポイントは、すべての SSID に対し、それぞれ有効になった無線インターフェイスを使用して、一定の設定間隔でこれらのメッセージを送信します。802.11 無線測定の実行プロセスでは、測定要求に指定されているすべてのチャネル上の CCX クライアントが 802.11 ブロードキャスト プローブ要求を送信します。Cisco Loaction Appliance は、アクセス ポイントで受信されたこれらの要求に基づいてアップリンク測定を使用し、すばやく正確にクライアント ロケーションを計算します。測定するクライアントのチャネルを指定する必要はありません。コントローラ、アクセス ポイント、およびクライアントによって、使用するチャネルが自動的に特定されます。

コントローラ ソフトウェア リリース 4.1 以降では、無線測定機能が拡張されたため、アクセス ポイントの観点だけでなくクライアントの観点での無線環境に関する情報もコントローラで取得できるようになりました。この場合、アクセス ポイントは、ユニキャスト無線測定要求を特定の CCXv4 または v5 クライアントに対して発行します。クライアントは、さまざまな測定レポートをアクセス ポイントおよびコントローラに返します。これらのレポートには、無線環境に関する情報と、クライアントのロケーションを解釈するために使用されるデータが含まれています。アクセス ポイントおよびコントローラが無線測定要求およびレポートで過負荷状態になるのを防ぐため、各アクセス ポイントのクライアント数は 2 つのみとし、各コントローラでサポートされるクライアント数は最大で 20 までとします。特定のアクセス ポイントまたはクライアントの無線測定要求の状態および特定のクライアントに対する無線測定レポートは、コントローラ CLI で確認できます。

コントローラ ソフトウェア リリース 4.1 以降では、Location Appliance の機能も向上しており、ロケーションベースのサービスと呼ばれる新しい CCXv4 機能によりデバイスのロケーションを正確に解釈できます。コントローラは、特定の CCXv4 または v5 クライアントにパス損失要求を発行します。クライアントが応答する場合、クライアントはコントローラにパス損失測定レポートを送信します。これらのレポートには、クライアントのチャネルおよび送信電力が含まれます。

（注） CCX 以外のクライアントおよび CCXv1 クライアントでは、CCX 測定要求を無視するため、これらのクライアントは無線測定アクティビティには参加しません。

ロケーション調整

たとえば、クライアント調整が実行される場合など、より厳密な追跡が必要な CCX クライアントの場合、アクセス ポイントからこれらのクライアントに対して、一定の設定間隔で、また CCX クライアントが新しいアクセス ポイントにローミングした場合は常に、ユニキャスト測定要求を送信させるようにコントローラを設定できます。このような特定の CCX クライアントに対するユニキャスト要求は、すべてのクライアントに送信されるブロードキャスト測定要求より頻繁に送信できます。ロケーション調整を CCX 以外のクライアントおよび CCXv1 クライアントに設定すると、それらのクライアントは設定された間隔で強制的にアソシエート解除され、ロケーション測定が生成されます。

GUI を使用した CCX 無線管理の設定

コントローラの GUI を使用して CCX 無線管理を設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **802.11a/n** または **802.11b/g/n** > **Network** の順にクリックします。802.11a（または 802.11b/g）Global Parameters ページが表示されます（図 10-12 を参照）。

図 10-12　802.11a Global Parameters ページ

ステップ 2　CCX Location Measurement の下にある **Mode** チェックボックスをオンにして、CCX 無線管理をグローバルに有効にします。このパラメータによって、このコントローラに接続されているアクセス ポイントから、CCXv2 以降を実行しているクライアントに対してブロードキャスト無線測定要求が発行されます。デフォルト値は、無効になっています（オフになっています）。

ステップ 3　前の手順で Mode チェックボックスを選択した場合、Interval フィールドに値を入力して、アクセス ポイントによるブロードキャスト無線測定要求の発行間隔を指定します。

範囲：60 ～ 32400 秒

デフォルト：60 秒

ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　**Save Configuration** をクリックして、設定内容を保存します。

ステップ 6　次の「CLI を使用した CCX 無線管理の設定」の項のステップ 2 に従って、アクセス ポイントのカスタマイズを有効にします。

（注）　特定のアクセス ポイントの CCX 無線管理を有効にするには、アクセス ポイントのカスタマイズを有効にする必要があります。これは、コントローラの CLI を使用してのみ実行できます。

ステップ 7　必要に応じて、もう一方の無線帯域（802.11a または 802.11b/g）について、この手順を繰り返します。

CLI を使用した CCX 無線管理の設定

コントローラの CLI を使用して CCX 無線管理を有効にする手順は、次のとおりです。

ステップ 1　CCX 無線管理をグローバルに有効にするには、次のコマンドを入力します。

config advanced {**802.11a** | **802.11b**} **ccx location-meas global enable** *interval_seconds*

interval_seconds パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワークでこのコントローラに接続されているすべてのアクセス ポイントから、CCX v2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。

ステップ 2　アクセス ポイントのカスタマイズを有効にするには、次のコマンドを入力します。

- **config advanced** {**802.11a** | **802.11b**} **ccx customize** *Cisco_AP* {**on** | **off**}

  このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントの CCX 無線管理機能が有効または無効になります。
- **config advanced** {**802.11a** | **802.11b**} **ccx location-meas ap** *Cisco_AP* **enable** *interval_seconds*

  interval_seconds パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントから、CCX v2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。

ステップ 3　特定のクライアントのロケーション調整を有効または無効にするには、次のコマンドを入力します。

config client location-calibration {**enable** | **disable**} *client _mac interval_seconds*

（注）　1 つのコントローラにつき最大 5 つのクライアントに対して、ロケーション調整を設定できます。

ステップ 4　設定を保存するには、次のコマンドを入力します。

save config

CLI を使用した CCX 無線管理情報の取得

次のコマンドを使用して、コントローラの CCX 無線管理に関する情報を取得します。

1. 802.11a または 802.11b/g ネットワークでこのコントローラに接続されているすべてのアクセス ポイントの CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

   show advanced {802.11a | 802.11b} ccx global

2. 802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントの CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

   show advanced {802.11a | 802.11b} ccx ap *Cisco_AP*

3. 特定のアクセス ポイントの無線測定要求の状態を表示するには、次のコマンドを入力します。

   show ap ccx rm *Cisco_AP* **status**

   次のような情報が表示されます。

```
A Radio

  Beacon Request.............................. Enabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Disabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5

B Radio

  Beacon Request.............................. Disabled
  Channel Load Request........................ Enabled
  Frame Request............................... Disabled
  Noise Histogram Request..................... Enabled
  Path Loss Request........................... Disabled
  Interval.................................... 60
  Iteration................................... 5
```

4. 特定のクライアントの無線測定要求の状態を表示するには、次のコマンドを入力します。

   show client ccx rm *client_mac* **status**

   次のような情報が表示されます。

```
Client Mac Address.......................... 00:40:96:ae:53:b4
Beacon Request.............................. Enabled
Channel Load Request........................ Disabled
Frame Request............................... Disabled
Noise Histogram Request..................... Disabled
Path Loss Request........................... Disabled
Interval.................................... 5
Iteration................................... 3
```

5. 特定のクライアントの無線測定レポートを表示するには、次のコマンドを入力します。

   - **show client ccx rm** *client_mac* **report beacon**：特定のクライアントのビーコン レポートを表示します。

- **show client ccx rm** *client_mac* **report chan-load**：特定のクライアントのチャネル負荷レポートを表示します。
- **show client ccx rm** *client_mac* **report noise-hist**：特定のクライアントのノイズヒストグラムレポートを表示します。
- **show client ccx rm** *client_mac* **report frame**：特定のクライアントのフレーム レポートを表示します。

6. ロケーション調整が設定されているクライアントを表示するには、次のコマンドを入力します。

   show client location-calibration summary

7. クライアントを検出した各アクセス ポイントの両方のアンテナについてレポートされる RSSI を表示するには、次のコマンドを入力します。

   show client detail *client_mac*

CLI を使用した CCX 無線管理問題のデバッグ

CCX 無線管理に関する問題が発生した場合は、次のコマンドを使用します。

1. CCX ブロードキャスト測定要求アクティビティをデバッグするには、次のコマンドを入力します。

   debug airewave-director message {**enable** | **disable**}

2. クライアント ロケーション調整アクティビティをデバッグするには、次のコマンドを入力します。

   debug ccxrm [**all** | **error** | **warning** | **message** | **packet** | **detail** {**enable** | **disable**}]

3. CCX 無線測定レポート パケットは、Inter-Access Point Protocol（IAPP）パケットでカプセル化されます。したがって、前の **debug ccxrm** コマンドでデバッグできない場合は、次のコマンドを入力すると IAPP レベルでデバッグできます。

   debug iapp error {enable | disable}

4. 転送されたプローブとそれに含まれている両アンテナの RSSI の出力をデバッグするには、次のコマンドを入力します。

   debug dot11 load-balancing

ピコ セル モードの設定

大規模なマルチセル高密度無線ネットワークでは、帯域幅の理想累積負荷を処理するための多数のアクセス ポイントを含むサイトを実装しながら、アクセス ポイント間のコンテンションを減らし、サービスの質を維持することは、難しい場合があります。RF チャネルのキャパシティを最適化し、ネットワーク全体のパフォーマンスを向上させるには、コントローラ GUI または CLI を使用して高密度（またはピコ セル）モード パラメータを設定します。

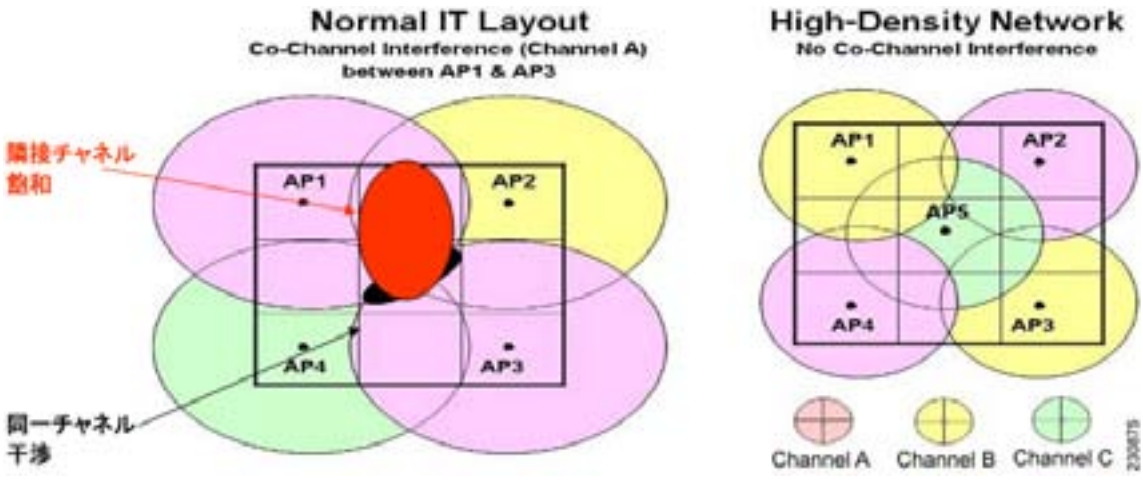
これらのパラメータを使用すると、特定のコントローラに登録されているすべてのアクセス ポイント全体に対して、受信装置の感度のしきい値、Clear Channel Assessment（CCA）の感度のしきい値、および送信電力の値を適用できます。高密度をサポートするクライアントから高密度対応アクセス ポイントにアソシエートするとき、これらの間では、アクセス ポイントでアドバタイズされた受信感度のしきい値、CCA 感度のしきい値、および送信電力の値に従うようクライアントに指示する、特定の 802.11 情報要素（IE）が交換されます。これらの 3 つのパラメータは、アクセス ポイントおよびクライアントがパケットの転送に利用できるチャネルとして見なす前に受信信号強度を調整することで、有効なセルのサイズを減らします。すべてのアクセス ポイントおよびクライアントが高密度領域でこのような方法を使用して信号標準を上げると、アクセス ポイントは互いに干渉したり、環境の信号や遠くの不正信号によって過負荷になることなく、近接して展開されます。

高密度対応無線ネットワークの利点は、次のとおりです。

- 利用可能な帯域をより有効に活用できる
- クライアントの総スループットまたは平方メートルあたりのスループットの大幅な増加
- 無線 LAN のキャパシティの大幅な増加
- キャパシティの線形拡大
- 干渉を発生させることなく WiFi を送信できるようにすることで、干渉への耐性が増加

図 10-13 は、高密度ネットワークの例を示しています。

図 10-13　高密度ネットワークの例



ピコ セル モードの使用に関するガイドライン

ピコ セル モードを使用する際の注意事項は次のとおりです。

- 高密度ネットワークは、Cisco Lightweight アクセス ポイントと、Intel PRO/Wireless 3945ABG および Intel Wireless WiFi Link 4965AG クライアントを使用しているノートブックでサポートされています。

- ピコ セル モード バージョン 2 を使用するには、Intel クライアントの WMM Policy が Allowed に設定されている必要があります。
- 高密度ネットワークをサポートするには、クライアントとアクセス ポイントの両方が高密度対応として設定されている必要があります。高密度に対応したデバイスと高密度に対応していないデバイスを同じネットワーク内で混在させないでください。
- 高密度アクセス ポイントは、専用コントローラに接続されている必要があります。
- ピコ セル モード パラメータを調整すると、次の RRM の値が自動的に変わります。
  - Power Level Assignment Method パラメータの Fixed オプションのデフォルト値（802.11a または 802.11b > RRM > Tx Power Control (TPC) ページ）には、ピコ セルの Transmit Power パラメータに指定した電力設定が反映されます。
  - Power Threshold パラメータのデフォルト値（802.11a または 802.11b > RRM > Tx Power Control (TPC) ページ）には、ピコ セルの CCA Sensitivity Threshold パラメータに指定した値が反映されます。

GUI を使用したピコ セル モードの設定

コントローラ GUI を使用してピコ セル モードを設定する手順は、次のとおりです。

ステップ 1　ピコ セル モード パラメータを変更する前に、802.11a または 802.11b/g ネットワークを無効にします。そのためには、**Wireless** > **802.11a/n**（または **802.11b/g/n**）> **Network** の順にクリックし、**802.11a Network Status**（または **802.11b/g Network Status**）チェックボックスをオフにします。

ステップ 2　**Wireless** > **802.11a/n**（または **802.11b/g/n**）> **Pico Cell** の順にクリックして、802.11a（または 802.11b/g）> Pico Cell ページを開きます（図 10-14 を参照）。

図 10-14　802.11a > Pico Cell ページ

ステップ 3　Pico Cell Mode ドロップダウン ボックスのオプションをいずれか 1 つ選択します。

- **Disable**：ピコ セル モードを無効にします。これはデフォルト値です。
- **V1**：ピコ セル モード バージョン 1 を有効にします。このオプションは、従来の Airespace 製品（シスコが Airespace を買収する前にリリースされた製品）で使用するためのものです。シスコでは、ピコ セル モードを有効化する場合は、V2 を選択することをお勧めします。
- **V2**：ピコ セル モード バージョン 2 を有効にします。このオプションは、ピコ セル モード パラメータを調整して、すべてのクライアントが高密度をサポートしている高密度領域におけるネットワーク パフォーマンスを最適化する場合に選択します。

ステップ 4　ステップ 3 で V2 を選択した場合、802.11a（または 802.11b/g）> Pico Cell ページには、3 つの設定可能なフィールドが表示されます。Rx Sensitivity Threshold、CCA Sensitivity Threshold、および Transmit Power です（図 10-15 を参照）。

図 10-15　Pico Cell Mode V2 のパラメータが表示された 802.11a > Pico Cell ページ

表 10-2 の情報を参考に、これらのパラメータの値を必要に応じて調整します。

（注） これらのパラメータのデフォルト値は、ほとんどのアプリケーションに適しています。このため、シスコではデフォルト値を使用することをお勧めします。

表 10-2　Pico Cell Mode V2 のパラメータ

パラメータ	説明
Rx Sensitivity Threshold	802.11a または 802.11b/g 無線の受信装置の感度に対する現在の値、最小値、および最大値（単位は dBm）を指定します。現在の値は、受信装置の感度をローカル無線で設定します。最小値および最大値は、Inter-Access Point Protocol（IAPP）高密度レポートに含めるためにのみ使用されます。 **デフォルト：**-65dBm（現在値）、-127dBm（最小値）、および 127dBm（最大値）
CCA Sensitivity Threshold	高密度セルのすべての無線に対する Clear Channel Assessment（CCA）の感度のしきい値を指定します。802.11a または 802.11b/g の受信装置は、現在値でプログラムされます。最小値および最大値は、IAPP レポートでのアドバタイズに使用されます。 **デフォルト：**-65dBm（現在値）、-127dBm（最小値）、および 127dBm（最大値）
Transmit Power	アクセス ポイントおよびクライアントの 802.11a または 802.11b/g 無線の両方で使用される高密度送信電力を指定します。 **デフォルト：**10dBm（現在値）、-127dBm（最小値）、および 127dBm（最大値）

（注） 図 10-15 および表 10-2 の最小値と最大値は、クライアントに対する範囲を示すためにのみ使用されます。アクセス ポイントでは使用されません。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　802.11a または 802.11b/g ネットワークを再度有効にします。そのためには、**Wireless** > **802.11a/n**（または **802.11b/g/n**）> **Network** の順にクリックし、**802.11a Network Status**（または **802.11b/g Network Status**）チェックボックスをオンにします

ステップ 7　**Save Configuration** をクリックして、変更内容を保存します。

（注）　ピコ セル モード パラメータの値を変更した場合、後からデフォルト値にリセットするには、**Reset to Defaults**、**Apply** の順にクリックします。

CLI を使用したピコ セル モードの設定

（注）　CLI コマンドで使用されるパラメータの説明およびデフォルト値については、「GUI を使用したピコ セル モードの設定」の項（P. 10-42）を参照してください。

ステップ 1　ピコ セル モード パラメータを変更する前に、802.11a または 802.11b/g ネットワークを無効にするには、次のコマンドを入力します。

config {**802.11a** | **802.11b**} **disable**

ステップ 2　ピコ セル モードを有効にするには、次のコマンドのいずれかを入力します。

- **config** {**802.11a** | **802.11b**} **picocell enable**：ピコ セル モード バージョン 1 を有効にします。このコマンドは、特定のアプリケーションで使用します。ピコ セル モードを有効にする場合は、**config** {**802.11a** | **802.11b**} **picocell-V2 enable** コマンドを使用することをお勧めします。
- **config** {**802.11a** | **802.11b**} **picocell-V2 enable**：ピコ セル モード バージョン 2 を有効にします。このコマンドは、ピコ セル モード パラメータを調整して、高密度領域におけるネットワーク パフォーマンスを最適化する場合に使用します。

ステップ 3　ステップ 2 でピコ セル モード バージョン 2 を有効にした場合は、次の手順に従って受信感度のしきい値、CCA 感度のしきい値、および送信電力のパラメータを設定します。

a. 受信感度のしきい値を設定するには、次のコマンドを入力します。

   config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 rx_sense_threshold** *min max current*

b. CCA の感度のしきい値を設定するには、次のコマンドを入力します。

   config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 cca_sense_threshold** *min max current*

c. 送信電力を設定するには、次のコマンドを入力します。

   config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 sta_tx_pwr** *min max current*

ステップ 4　ステップ 2 でピコ セル モード バージョン 2 を有効にした場合、ユニキャスト IAPP 高密度フレーム要求を特定のクライアントに送信するには、次のコマンドを入力します。

config advanced {**802.11a** | **802.11b**} **receiver pico-cell-V2 send_iapp_req** *client_mac*

ステップ 5　802.11a または 802.11b/g ネットワークを再び有効にするには、次のコマンドを入力します。

config {802.11a | 802.11b} enable

ステップ 6　設定を保存するには、次のコマンドを入力します。

save config

CLI を使用したピコ セル モードの問題のデバッグ

ピコ セル モードに関する問題が発生した場合は、次のコマンドを使用します。

1. ピコ セル モードの現在のステータスを表示するには、次のコマンドを入力します。

   show {802.11a | 802.11b}

   次のような情報が表示されます。

```
802.11a Network.................................. Disabled
11nSupport....................................... Disabled
      802.11a Low Band........................... Enabled
      802.11a Mid Band........................... Enabled
      802.11a High Band.......................... Enabled
...
Pico-Cell Status................................. Disabled
Pico-Cell-V2 Status.......................... Enabled
```

2. ピコ セル モード コマンドで設定された受信装置のパラメータを表示するには、次のコマンドを入力します。

   show advanced {802.11a | 802.11b} receiver

   次のような情報が表示されます。

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 30
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 30
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Disabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Disabled
 TxStomp  : Wrong BSSID Data Only Status......... Disabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
 RxAbort  : Low RSSI Threshold................... 30
 RxAbort  : Wrong BSSID Status................... Disabled
 RxAbort  : Wrong BSSID Data Only Status......... Disabled
 ----------------------------------------------....
 pico-cell-V2 parameters in dbm units:
 RxSensitivity: Min,Max,Current RxSense Thres.... -127,127,-65
 CCA Threshold: Min,Max,Current Clear Channel.... -127,127,-65
Tx Pwr: Min,Max,Current Transmit Power for A..... -127,127,10
 ----------------------------------------------....
```

3. ノイズおよび干渉に関する情報、カバレッジ情報、クライアントの信号強度と信号対雑音比、および近くにあるアクセス ポイントを表示するには、次のコマンドを入力します。

   show ap auto-rf {**802.11a** | **802.11b**} *Cisco_AP*

   次のような情報が表示されます。

```
Number Of Slots.................................. 2
AP Name.......................................... AP1242.47b2.31f6
MAC Address...................................... 00:16:47:b2:31:f6
  Radio Type..................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile................................ PASSED
  Interference Information
    Interference Profile......................... PASSED
  Load Information
    Load Profile................................. PASSED
    Receive Utilization.......................... 0 %
    Transmit Utilization......................... 0 %
    Channel Utilization.......................... 0 %
    Attached Clients............................. 0 clients
  Coverage Information
    Coverage Profile............................. PASSED
    Failed Clients............................... 0 clients
  Client Signal Strengths
    RSSI -100 dbm................................ 0 clients
    RSSI  -92 dbm................................ 0 clients
    RSSI  -84 dbm................................ 0 clients
RSSI  -76 dbm................................ 0 clients
    RSSI  -68 dbm................................ 0 clients
    RSSI  -60 dbm................................ 0 clients
    RSSI  -52 dbm................................ 0 clients
  Client Signal To Noise Ratios
    SNR    0 dB.................................. 0 clients
    SNR    5 dB.................................. 0 clients
    SNR   10 dB.................................. 0 clients
    SNR   15 dB.................................. 0 clients
    SNR   20 dB.................................. 0 clients
    SNR   25 dB.................................. 0 clients
    SNR   30 dB.................................. 0 clients
    SNR   35 dB.................................. 0 clients
    SNR   40 dB.................................. 0 clients
    SNR   45 dB.................................. 0 clients
  Nearby APs
  Radar Information
  RF Parameter Recommendations
    Power Level.................................. 0
    RTS/CTS Threshold............................ 0
    Fragmentation Threshold...................... 0
    Antenna Pattern.............................. 0
```

CHAPTER 11

モビリティ グループの設定

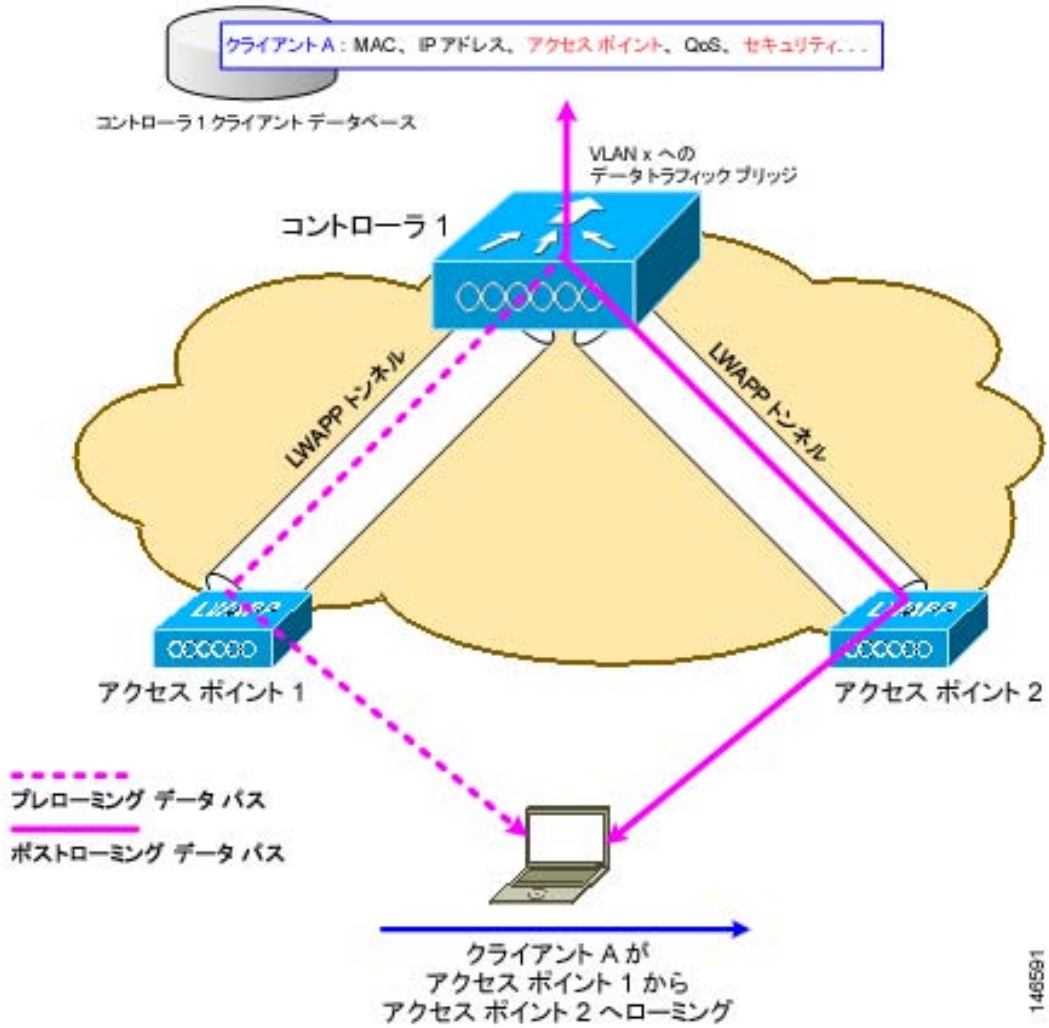
この章では、モビリティ グループについておよびモビリティ グループのコントローラ上での設定方法を説明します。この章の内容は、次のとおりです。

モビリティの概要

モビリティ、すなわちローミングは、できるだけ遅れることなく、確実かつスムーズに、あるアクセス ポイントから別のアクセス ポイントへアソシエーションを維持する無線 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にモビリティが動作する方法について説明します。

ある無線クライアントがアクセス ポイントにアソシエートして認証すると、アクセス ポイントのコントローラは、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配置します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセス ポイントが含まれます。. コントローラはこの情報を使用してフレームを転送し、無線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 11-1 には、2 つのアクセス ポイントが同一のコントローラに接続されている場合の両アクセス ポイント間における無線クライアント ローミングの様子が示されています。

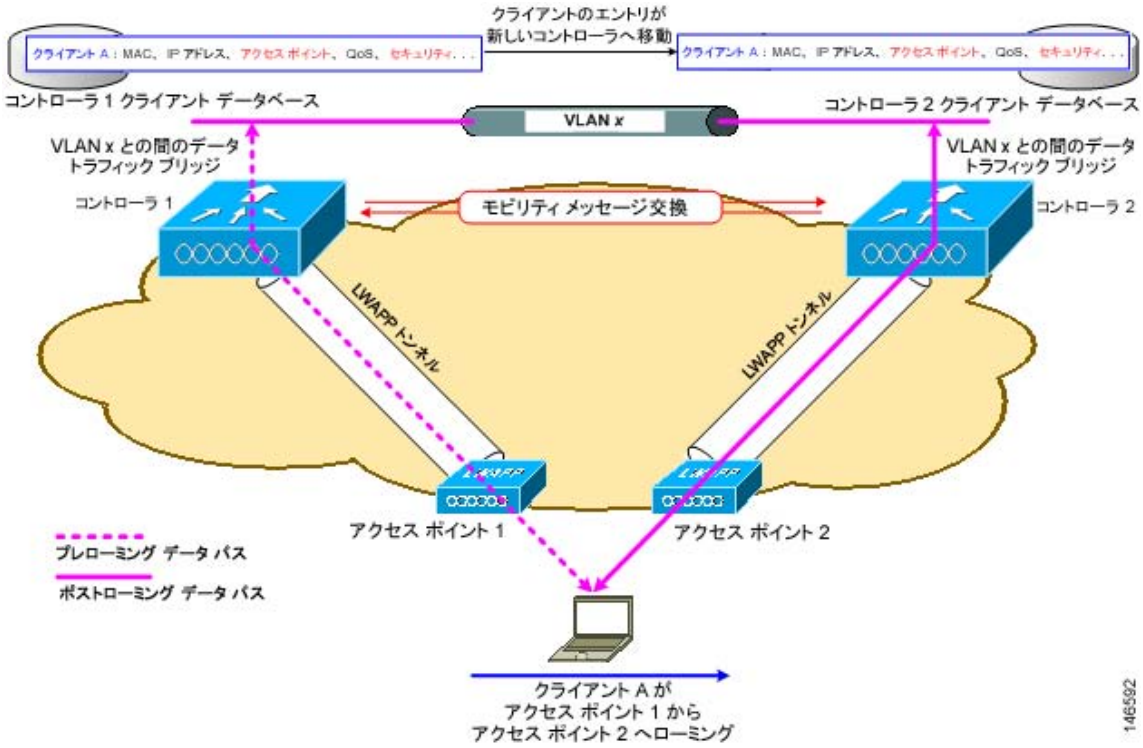
図 11-1　コントローラ内ローミング



無線クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセス ポイントで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アクセス ポイントから別のコントローラに接続されたアクセス ポイント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 11-2 は、コントローラの無線 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表したものです。

図 11-2　コントローラ間ローミング

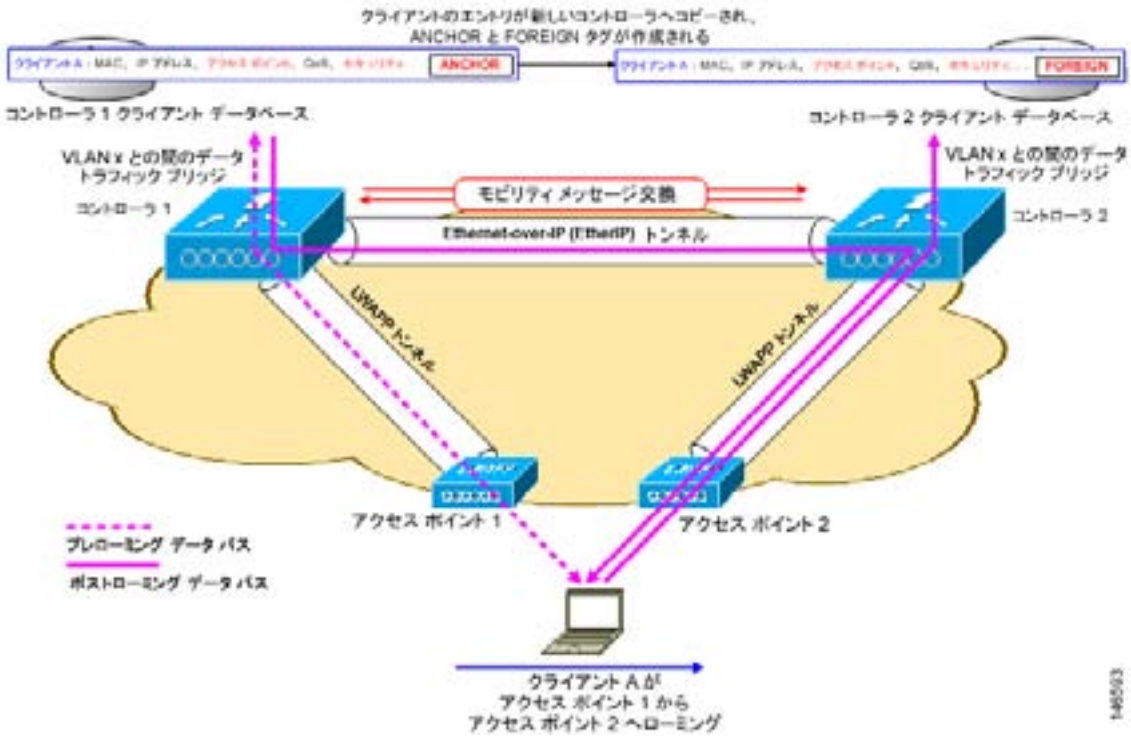


クライアントが新たなコントローラに接続されたアクセス ポイントへアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

（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に認証を完了します。

図 11-3 は、コントローラの無線 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表したものです。

図 11-3　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 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に「外部」エントリのマークが付けられます。ローミングは無線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のあと、無線クライアントに出入りするデータは非対称トラフィック パスで転送されます。クライアントからネットワークへのトラフィックは、外部コントローラでネットワークへ直接転送されます。クライアントへのトラフィックはアンカー コントローラに達し、ここで EtherIP トンネルの外部コントローラへ転送されます。外部コントローラは、そのデータをクライアントへ転送します。無線クライアントが新たな外部コントローラへローミングする場合、クライアントのデータベース エントリは元の外部コントローラから新しい外部コントローラへ移動されますが、元のアンカー コントローラは常に保持されます。クライアントは元のコントローラに返されると、再びローカルになります。

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所定の位置に設定しないでおく必要があります。そのように設定してない場合、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） 現時点では、サブネット間ローミングの際にマルチキャスト　トラフィックは通過できません。この点を考慮して、サブネット間ネットワークの設計には Push-to-Talk を使用する際にマルチキャスト トラフィックを送信する必要のある Spectralink の電話を組み込まないようにします。

(注)　コントローラ間ローミングもサブネット間ローミングも、コントローラを同一のモビリティ グループ内に設置する必要があります。モビリティ グループの説明と設定の手順については、次の 2 項を参照してください。

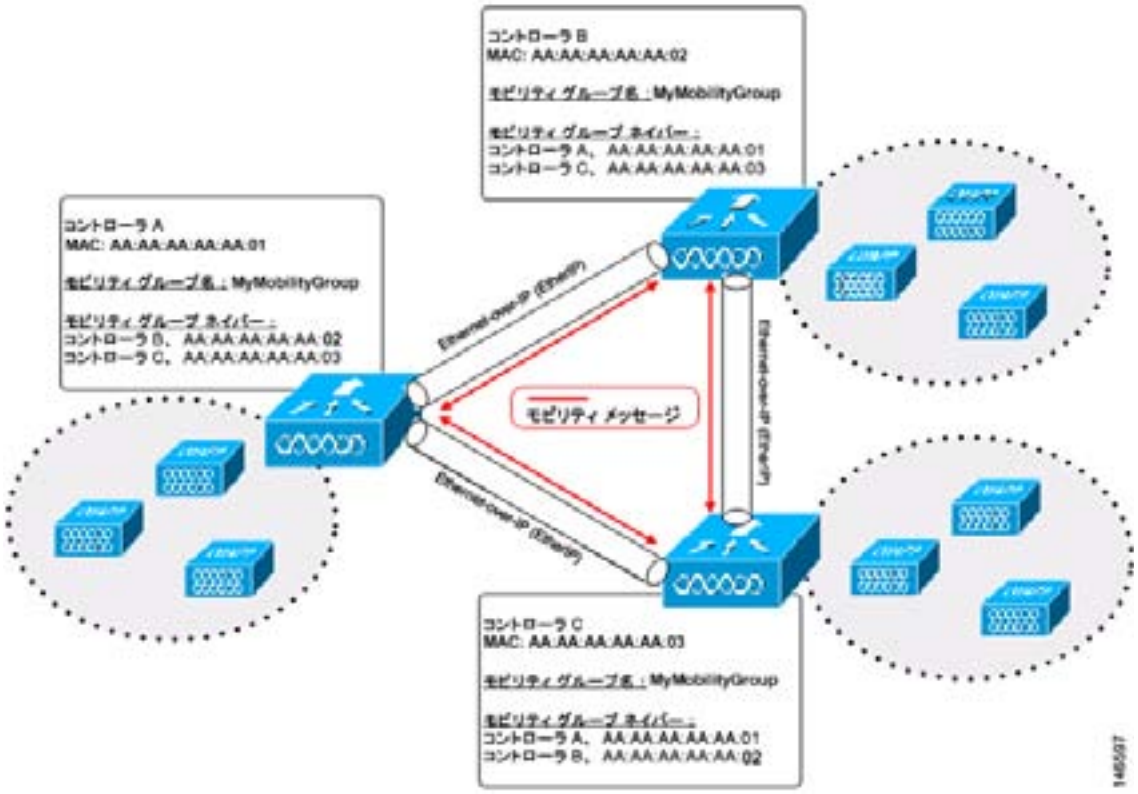
モビリティ グループの概要

コントローラのセットをモビリティ グループとして設定することで、コントローラのグループ内でクライアントのローミングをスムーズに行うことができるようになります。モビリティ グループを作成すると、ネットワーク内で複数のコントローラを有効化して、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータ トラフィックを転送できるようになります。コントローラは、クライアント デバイスのコンテキストと状態およびコントローラのロード情報を共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。

(注)　クライアントでは、モビリティ グループ間のローミングは行われません。

図 11-4 には、モビリティ グループの例が示されています。

図 11-4　シングル モビリティ グループ



図示したように、各コントローラはモビリティ グループの別メンバーのリストを使用して設定されています。新たなクライアントがコントローラに追加されると、コントローラはユニキャスト メッセージをそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。コントローラ間のすべてのモビリティ メッセージ交換が 16666 ポートの UDP パケットで実行されます。IPSec 暗号化もコントローラ間モビリティ メッセージに対して設定されます。この場合は、16667 ポートが使用されます。

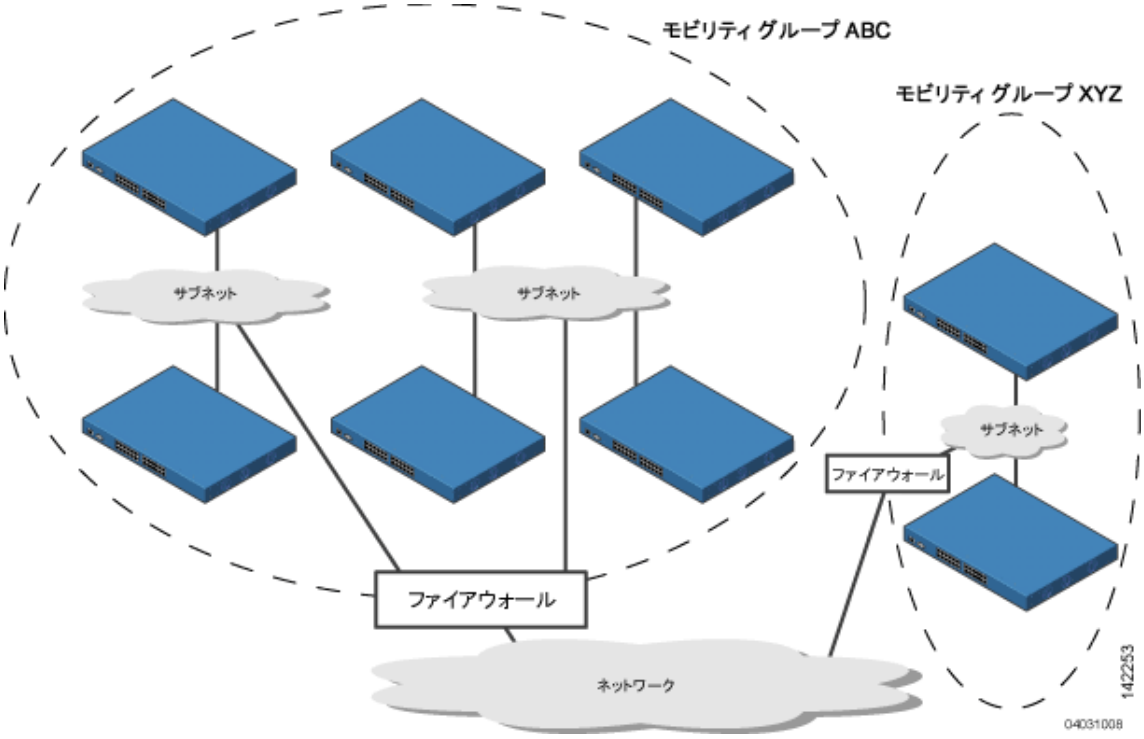
1 つのモビリティ グループには、任意のタイプのコントローラを最大 24 まで追加できます。モビリティ グループでサポートされたアクセス ポイントの数は、そのグループのコントローラの数とタイプでバインドされます。

例：

1. 4404-100 コントローラは、最大 100 個のアクセス ポイントをサポートします。したがって、24 個の 4404-100 コントローラで構成されているモビリティ グループは、最大 2400 個のアクセス ポイント（24 * 100 = 2400 アクセス ポイント）をサポートします。
2. 4402-25 コントローラは最大 25 個のアクセス ポイントをサポートし、4402-50 コントローラは最大 50 個のアクセス ポイントをサポートします。したがって、12 個の 4402-25 コントローラと 12 個の 4402-50 コントローラで構成されたモビリティ グループは最大 900 個のアクセス ポイント（12 * 25 + 12 * 50 = 300 + 600 = 900 アクセス ポイント）をサポートします。

モビリティ グループによって、同じ無線ネットワーク内で異なるモビリティ グループ名を異なるコントローラに割り当て、1 つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。図 11-5 には、2 つのコントローラのグループに異なるモビリティ グループ名を作成した結果が示されています。

図 11-5　2 つのモビリティ グループ



ABC モビリティ グループのコントローラは、そのアクセス ポイントと共有サブネットを使用して相互に認識しあい、通信します。ABC モビリティ グループのコントローラは、異なるモビリティ グループの XYZ コントローラを認識せず、通信を行いません。同様に、XYZ モビリティ グループのコントローラは、ABC モビリティ グループのコントローラを認識せず、通信を行いません。この機能により、ネットワークでのモビリティ グループの切り離しが確実に行われます。

（注） クライアントは、異なるモビリティ グループのアクセス ポイントを認識できれば、そのアクセス ポイント間のローミングを行うことがあります。しかし、そのセッションの情報は異なるモビリティ グループのコントローラ間では実行されません。

モビリティ グループにコントローラを追加するタイミングの判断

ネットワーク内の無線クライアントが、あるコントローラに接続したアクセス ポイントから、別のコントローラに接続したアクセス ポイントへローミングできるとしたら、どちらのコントローラも同じモビリティ グループに属しているはずです。

モビリティ グループ内でのメッセージング

コントローラでは、モビリティ メッセージを他のメンバ コントローラに送信することにより、クライアントにサブネット間モビリティが提供されます。同じモビリティ グループに最大 24 のメンバを持つリスト内に最大 72 のメンバを持つことができます。コントローラ ソフトウェア リリース 5.0 では、モビリティ メッセージングに対して 2 つの改良が行われました。どちらも、モビリティ メンバの全リストにメッセージを送信する場合に役立ちます。

- Mobile Announce メッセージを、まず同じグループ内に送信してから、リスト内の他のグループに送信する

  コントローラは、新しいクライアントがアソシエートされるたびに、モビリティ リスト内のメンバに Mobile Announce メッセージを送信します。5.0 以前のコントローラ ソフトウェア リリースでは、コントローラは所属グループに関係なく、このメッセージをリスト内のすべてのメンバに送信します。しかし、コントローラ ソフトウェア リリース 5.0 では、コントローラは自分と同じグループ（ローカル グループ）に属するメンバに対してのみメッセージを送信し、その後、再試行を送信しながら、他のメンバをすべて加えます。

- ユニキャストではなくマルチキャストを使用して Mobile Annouce メッセージを送信する

  5.0 以前のコントローラ ソフトウェア リリースでは、コントローラはユニキャスト モードを使用して、すべてのモビリティ メッセージを送信しますが、これには、すべてのモビリティ メンバにメッセージのコピーを送信する必要があります。多くのメッセージ（Mobile Announce、PMK Update、AP List Update、IDS Shun など）はグループ内のすべてのメンバに向けられたものなので、この動作は効率的ではありません。コントローラ ソフトウェア リリース 5.0 では、マルチキャストを使用して Mobile Announce メッセージを送信するようにコントローラを設定できます。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティ メンバすべてを含むマルチキャスト グループに宛てて送られます。マルチキャスト メッセージングを最大限生かすには、グループ メンバすべてに対してこの機能を有効化または無効化することをお勧めします。

NAT デバイスでのモビリティ グループの使用

コントローラ ソフトウェア リリース 4.2 以前では、同じモビリティ グループ内のコントローラ間のモビリティは、コントローラのいずれかが Network Address Translation（NAT; ネットワーク アドレス変換）デバイスの背後にある場合には機能しません。この動作により、1 台のコントローラがファイアウォールの外側にあると考えられるゲストのアンカー機能では、問題が発生します。

モビリティ メッセージのペイロードは、ソース コントローラに関する IP アドレス情報を伝達します。この IP アドレスは、IP ヘッダのソース IP アドレスで検証されます。この動作により、NAT デバイスがネットワークに導入されるときに問題が発生します。これは、IP ヘッダ内でソース IP アドレスが変更されるためです。したがって、ゲスト WLAN 機能では、NAT デバイス経由でルーティングされているモビリティ パケットはすべて、IP アドレスの不一致のためにドロップされます。

コントローラ ソフトウェア リリース 4.2 以降では、ソース コントローラの MAC アドレスを使用するようにモビリティ グループの検索が変更されています。NAT デバイスのマッピングに従ってソース IP アドレスが変更されるため、要求元のコントローラの IP アドレスを取得するために応答が送信される前に、モビリティ グループのデータベースが検索されます。これは、要求元のコントローラの MAC アドレスを使用して実行されます。

NAT が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからからコントローラに送信される IP アドレスを入力します。さらに、PIX などのファイアウォールを使用している場合には、ファイアウォールで次のポートが開いていることを確認します。

- UDP 16666：トンネル コントロール トラフィック用
- UDP 16667：暗号化トラフィック用
- IP Protocol 97：ユーザのデータ トラフィック用
- UDP 161 および 162：SNMP

（注） コントローラ間のクライアント モビリティは、自動アンカー モビリティ（*ゲスト トンネリング*とも呼ばれる）またはシンメトリック モビリティ トンネリングが有効になっている場合にのみ機能します。アシンメトリック トンネリングは、モビリティ コントローラが NAT デバイスの背後にある場合にはサポートされません。これらのモビリティ オプションの詳細は、「自動アンカー モビリティの設定」および「シンメトリック モビリティ トンネリングの設定」の項を参照してください。

図 11-6 は、NAT デバイスを使用したモビリティ グループの設定の例を示しています。この例では、すべてのパケットが NAT デバイスを通過します（つまり、送信元から宛先、およびその逆方向に送信されるパケット）。図 11-7 は、2 台の NAT デバイスを使用したモビリティ グループの設定の例を示しています。この例では、送信元とゲートウェイとの間に 1 台の NAT デバイスを使用し、宛先とゲートウェイとの間にもう 1 台の NAT デバイスを使用しています。

図 11-6　1 台の NAT デバイスを使用したモビリティ グループの設定

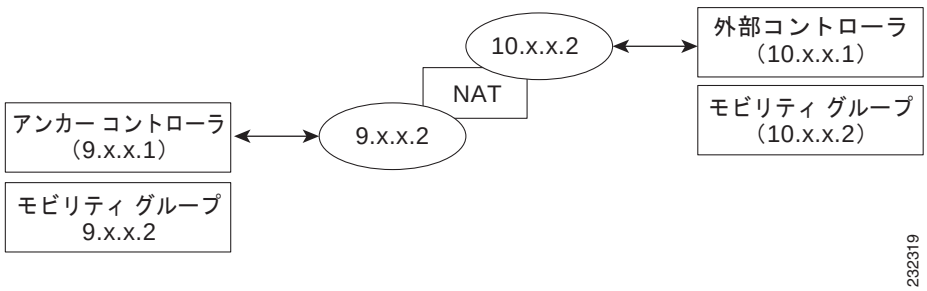
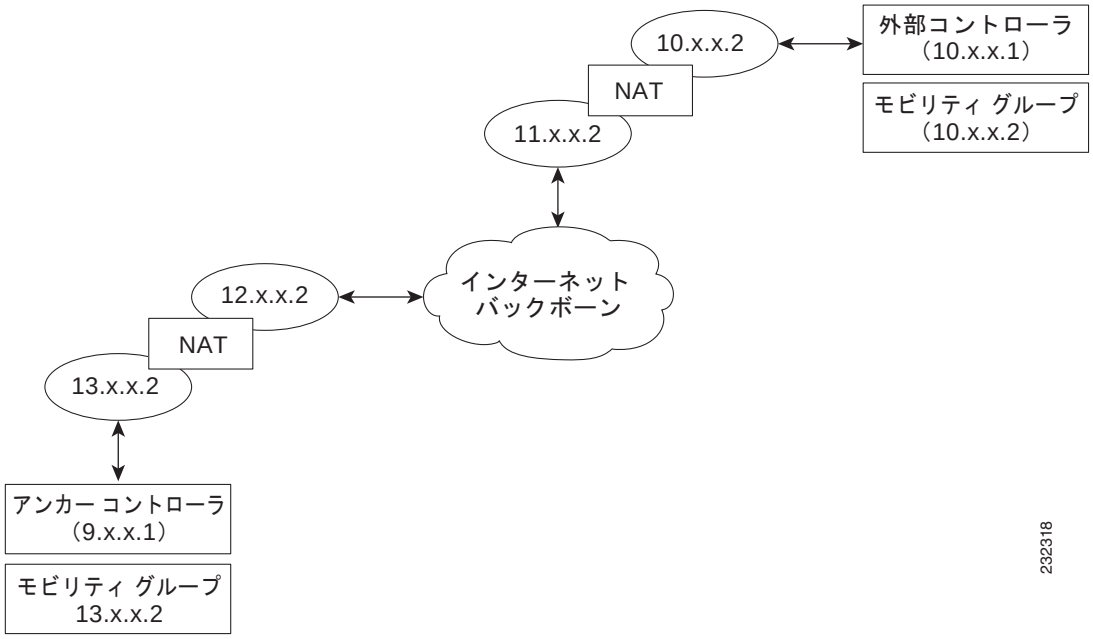


図 11-7　2 台の NAT デバイスを使用したモビリティ グループの設定



モビリティ グループの設定

この項では、GUI または CLI を使用してコントローラのモビリティ グループを設定する手順について説明します。

（注） Cisco Wireless Control System（WCS）を使用してモビリティ グループを設定することもできます。手順については、『Cisco Wireless Control System Configuration Guide』を参照してください。

必須条件

コントローラをモビリティ グループに追加する前に、グループに追加するコントローラすべてについて、次の要件が満たされていることを確認する必要があります。

- すべてのコントローラは、同じ LWAPP 転送モード（レイヤ 2 またはレイヤ 3）で設定されている必要があります。

（注） Controller > General ページで LWAPP 転送モードを確認し、必要に応じて LWAPP 転送モードに変更できます。

- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。

（注） コントローラを ping すると、IP 接続を確認できます。

- すべてのコントローラは、同じモビリティ グループ名で設定する必要があります。

（注） 通常、モビリティ グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて、Controller > General ページの Default Mobility Domain Name フィールドで変更できます。モビリティ グループ名では、大文字と小文字が区別されます。

（注） Cisco WiSM の場合、300 のアクセス ポイント間のルーティングをスムーズにするために両方のコントローラを同じモビリティ グループ名で設定してください。

- すべてのコントローラは、同じバージョンのコントローラ ソフトウェアが動作している必要があります。
- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。

（注） 必要に応じて、仮想インターフェイス IP アドレスを変更するには、Controller > Interfaces ページで仮想インターフェイス名を編集します。コントローラの仮想インターフェイスの詳細は、第 3 章を参照してください。

（注） モビリティ グループ内のすべてのコントローラが同じ仮想インターフェイスを使用していない場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

- モビリティ グループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他の全モビリティ グループ メンバの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。

（注） モビリティ グループに追加する他のコントローラの MAC アドレスと IP アドレスは、各コントローラの GUI の Controller > Mobility Groups ページにあります。

- サード パーティのファイアウォール、Cisco PIX、または Cisco ASA を使用してモビリティ グループを設定する際に、セキュア モビリティ グループを使用していない場合は、ポート 16666、16667、12222、および 12223、IP プロトコル 50 および 97、および UDP ポート 500 を開く必要があります。Encapsulating Security Payload（ESP）を採用したセキュリティ モビリティ グループを使用している場合は、UDP ポート 500 を開くことにより、Internet Security Association and Key Management Protocol（ISAKMP）がファイアウォールを通過できるようにする必要があります。また、IP プロトコル 50 を使用して、暗号化されたデータがファイアウォールを通過できるようにする必要もあります。ポート 16666 および 16667 上のモビリティ データは ESP でカプセル化されます。したがって、ポート 16666 と 16667 を許可するように ACL を作成する必要はありません。これは、これらのポートがすでに ESP 内でカプセル化されているからです。

（注） ファイアウォール上では Port Address Translation（PAT; ポート アドレス変換）は実行できません。1 対 1 の Network Address Translation（NAT; ネットワーク アドレス変換）を設定する必要があります。

モビリティ グループを設定するための GUI の使用

GUI を使用してモビリティ グループを設定する手順は、次のとおりです。

（注） CLI を使用してモビリティ グループを設定する場合は、「モビリティ グループを設定するための CLI の使用」の項（P. 11-16）を参照してください。

ステップ 1　**Controller** > **Mobility Management** > **Mobility Groups** の順にクリックして、Static Mobility Group Members ページを開きます（図 11-8 を参照）。

図 11-8　Static Mobility Group Members ページ

このページでは、Default Mobility Group フィールドにモビリティ グループ名が表示され、現在モビリティ グループのメンバである各コントローラの MAC アドレスと IP アドレスが示されます。最初のエントリはローカル コントローラで、これを削除することはできません。

（注） モビリティ　グループからいずれかのリモート　コントローラを削除するには、そのコントローラの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　次のいずれかを実行して、コントローラをモビリティ グループに追加します。

- コントローラを 1 つだけ追加する場合、または別々に複数のコントローラを追加する場合、**New** をクリックしてステップ 3 に進みます。
- 複数のコントローラを追加する場合、それらを一括で追加するには、**EditAll** をクリックしてステップ 4 へ進みます。

（注） EditAll オプションを使用すると、現在のモビリティ グループ メンバのすべての MAC アドレスと IP アドレスを入力した後で、すべてのエントリをモビリティ グループの 1 つのコントローラから別のコントローラにコピーして貼り付けることができます。

ステップ 3　Mobility Group Member > New ページが表示されます（図 11-9 を参照）。

図 11-9　Mobility Group Member > New ページ

次の手順に従って、コントローラをモビリティ グループに追加します。

a. Member IP Address フィールドに、追加するコントローラの管理インターフェイスの IP アドレスを入力します。

（注） Network Address Translation（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

b. Member MAC Address フィールドに、追加するコントローラの MAC アドレスを入力します。

c. Group Name フィールドに、モビリティ グループ名を入力します。

（注） モビリティ グループ名では、大文字と小文字が区別されます。

d. **Apply** をクリックして、変更を適用します。新しいコントローラが、Static Mobility Group Members ページのモビリティ グループ メンバのリストに追加されます。

e. **Save Configuration** をクリックして、変更内容を保存します。

f. 手順 a. ～ 手順 e. を繰り返して、すべてのコントローラをモビリティ グループに追加します。

g. モビリティ グループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティ グループ内のすべてのコントローラでは、他のすべてのモビリティ グループ メンバの MAC アドレスと IP アドレスについて設定する必要があります。

ステップ 4 The Mobility Group Members > Edit All ページ（図 11-10 を参照）に現在モビリティ グループにあるすべてのコントローラの MAC アドレス、IP アドレス、およびモビリティ グループ名（オプション）が表示されます。コントローラのリストは、先頭にローカルのコントローラが表示され、1 行に 1 つずつ表示されます。

（注） 必要に応じて、リストのコントローラを編集または削除できます。

図 11-10　Mobility Group Member > Edit All ページ

次の手順に従って、さらにコントローラをモビリティ グループに追加します。

a. 編集ボックス内をクリックして、新たな行を開始します。

b. MAC アドレス、管理インターフェイスの IP アドレス、および追加するコントローラのモビリティ グループ名を入力します。

（注） これらの値は 1 行に入力し、1 つまたは 2 つのスペースで区切ってください。

（注） モビリティ グループ名では、大文字と小文字が区別されます。

c. モビリティ グループに追加するコントローラごとに、手順 a. および手順 b. を繰り返します。

d. 編集ボックス内のエントリ全体を強調表示して、コピーします。

e. **Apply** をクリックして、変更を適用します。新しいコントローラが、Static Mobility Group Members ページのモビリティ グループ メンバのリストに追加されます。

f. **Save Configuration** をクリックして、変更内容を保存します。

g. リストをモビリティ グループ内の他のすべてのコントローラの Mobility Group Members > Edit All ページにある編集ボックスに貼り付けて、**Apply** と **Save Configuration** をクリックします。

ステップ 5　**Multicast Messaging** をクリックして、Mobility Multicast Messaging ページを開きます（図 11-11 を参照。）

図 11-11　Mobility Multicast Messaging ページ

現在、設定されているモビリティ グループすべての名前がページの中央に表示されます。

ステップ 6　Mobility Multicast Messaging ページで、**Enable Multicast Messaging** チェック ボックスをオンにすると、Mobile Announce メッセージをモビリティ メンバに送信するために、コントローラでマルチキャスト モードを使用できるようになります。このチェック ボックスをオフにしておくと、Mobile Announce メッセージはユニキャスト モードで送信されます。デフォルトではオフになっています。

ステップ 7　前の手順でマルチキャスト メッセージングを有効化した場合は、Local Group Multicast IP Address フィールドに、ローカル モビリティ グループのマルチキャスト グループ IP アドレスを入力します。このアドレスは、マルチキャスト モビリティ メッセージングに使用されます。

（注） マルチキャスト メッセージングを使用するには、ローカル モビリティ グループの IP アドレスを設定する必要があります。

ステップ 8　**Apply** をクリックして、変更を適用します。

ステップ 9　必要に応じて、モビリティ リスト内にあるローカル以外のグループのマルチキャスト グループ IP アドレスを設定することもできます。このためには、ローカル以外のモビリティ グループの名前をクリックして、Mobility Multicast Messaging > Edit ページ（図 11-12 を参照）を開き、Multicast IP Address フィールドにローカル以外のモビリティ グループのマルチキャスト グループ IP アドレスを入力します。

（注） ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャスト モードでモビリティ メッセージを送信します。

図 11-12　Mobility Multicast Messaging > Edit ページ

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

モビリティ グループを設定するための CLI の使用

CLI を使用してモビリティ グループを設定する手順は、次のとおりです。

ステップ 1　現在のモビリティ設定を確認するには、次のコマンドを入力します。

show mobility summary

次のような情報が表示されます。

```
Symmetric Mobility Tunneling (current) ..... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... snmp_gui
Multicast Mode ..... Disabled
Mobility Domain ID for 802.11r..... 0x66bd
Mobility Keepalive Interval..... 10
Mobility Keepalive Count..... 3
Mobility Group Members Configured..... 3
Mobility Control Message DSCP Value..... 0

Controllers configured in the Mobility Group
 MAC Address        IP Address       Group Name Multicast IP Status
 00:0b:85:32:42:c0 1.100.163.24     snmp_gui     0.0.0.0     Up
 00:cc:11:ee:1b:10 10.100.100.1    VoWLAN        0.0.0.0     Control and Data Path
Down
 11:22:11:33:11:44 1.2.3.4         test          0.0.0.0     Control and Data Path
Down
```

ステップ 2　モビリティ グループを作成するには、次のコマンドを入力します。

config mobility group domain *domain_name*

（注）　グループ名には、最大 31 文字の ASCII 文字列を使用できます。大文字と小文字が区別されます。モビリティ グループ名には、スペースは使用できません。

ステップ 3　グループ メンバを追加するには、次のコマンドを入力します。

config mobility group member add *mac_address ip_address*

（注）　Network Address Translation（NAT）が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティ グループ内のコントローラ間でモビリティが失敗します。

（注）　グループ メンバを削除するには、**config mobility group member delete** *mac_address* と入力します。

ステップ 4　マルチキャスト モビリティ モードを有効または無効にするには、次のコマンドを入力します。

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

ここで、*local_group_multicast_address* は、ローカル モビリティ グループのマルチキャスト グループ IP アドレスです。このアドレスは、マルチキャスト モビリティ メッセージングに使用されます。

マルチキャスト モビリティ モードを有効にした場合、Mobile Announce メッセージはマルチキャスト モードでローカル グループに送信されます。マルチキャスト モビリティ モードを無効にした場合、Mobile Announce メッセージはユニキャスト モードでローカル グループに送信されます。デフォルト値は無効です。

ステップ 5　必要に応じて、モビリティ リスト内にあるローカル以外のグループのマルチキャスト グループ IP アドレスを設定することもできます。そのためには、次のコマンドを入力します。

config mobility group multicast-address *group_name IP_address*

ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャスト モードでモビリティ メッセージを送信します。

ステップ 6　モビリティ設定を確認するには、次のコマンドを入力します。

show mobility summary

ステップ 7　設定を保存するには、次のコマンドを入力します。

save config

ステップ 8　モビリティ　グループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティ グループ内のすべてのコントローラでは、他のすべてのモビリティ グループ メンバの MAC アドレスと IP アドレスについて設定する必要があります。

ステップ 9　モビリティ メッセージのマルチキャスト使用のデバッグを有効または無効にするには、次のコマンドを入力します。

debug mobility multicast {**enable** | **disable**}

モビリティ グループの統計の表示

コントローラの GUI から次の 3 種類のモビリティ グループの統計を表示できます。

- Global Mobility Statistics：すべてのモビリティ トランザクションに影響します。
- Mobility Initiator Statistics：モビリティ イベントを開始するコントローラによって生成されます。
- Mobility Responder Statistics：モビリティ イベントに応答するコントローラによって生成されます。

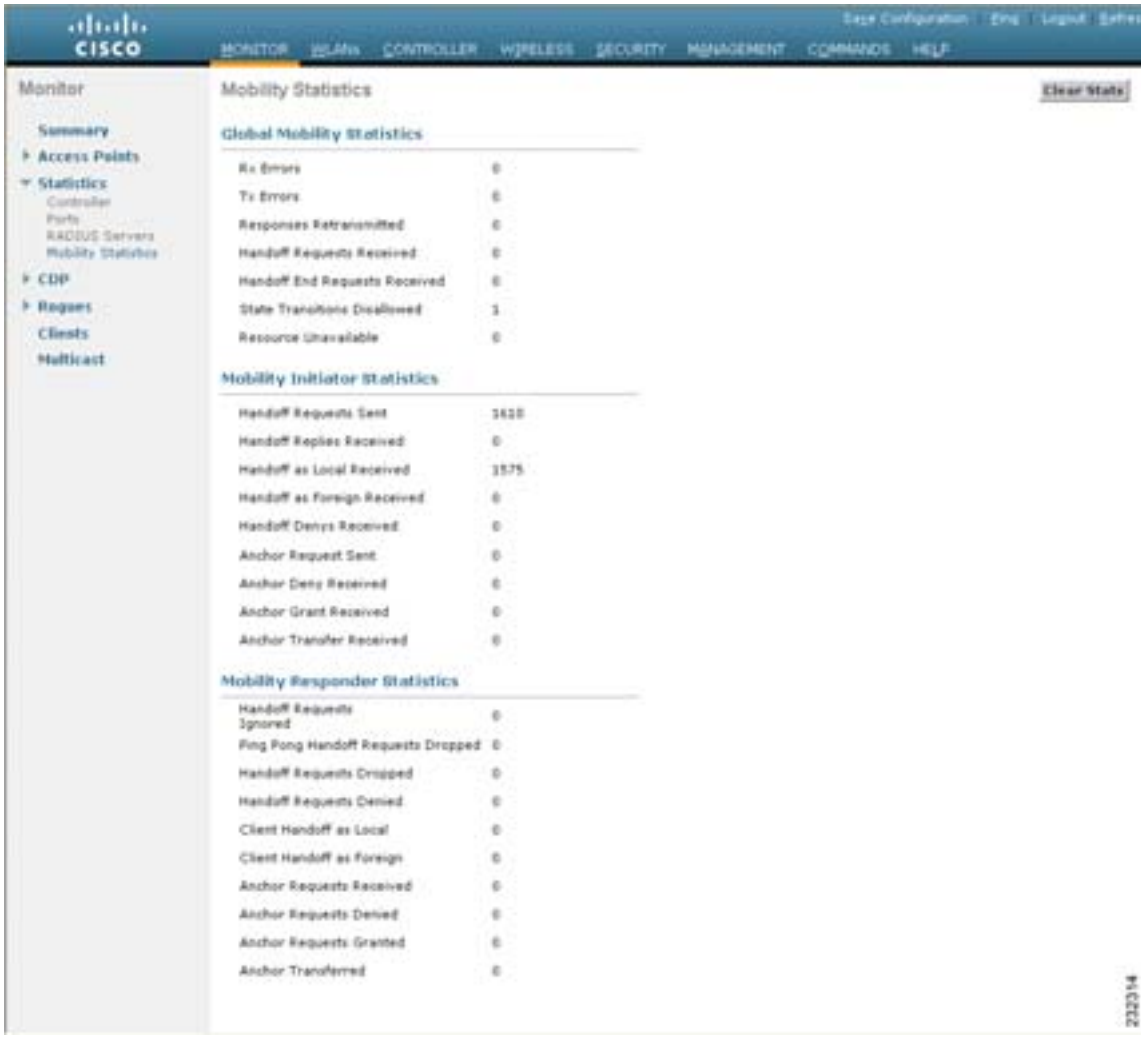
コントローラの GUI または CLI を使用して、モビリティ グループの統計を表示できます。

GUI を使用したモビリティ グループの統計の表示

コントローラの GUI を使用して、モビリティ グループの統計を表示する手順は、次のとおりです。

ステップ 1　**Monitor** > **Statistics** > **Mobility Statistics** の順にクリックして、Mobility Statistics ページを開きます（図 11-13 を参照）。

図 11-13　Mobility Statistics ページ



ステップ 2　各統計の説明については、表 11-1 を参照してください。

表 11-1　モビリティの統計

パラメータ	説明
Global Mobirity Statistics	
Rx Errors	短すぎるパケットや不正な形式などの、一般的なプロトコル パケット受信エラー。
Tx Errors	パケット転送失敗など、一般的なプロトコル パケット転送エラー。
Responses Retransmitted	モビリティ プロトコルで UDP が使用されているときに応答が受信されない場合には、複数回にわたって要求が再送信されます。ネットワークの遅延または処理の遅延のため、応答側が最初に要求に応答した後に、1 回以上の再試行要求を受信する場合があります。このフィールドには、応答が再送信された回数が表示されます。
Handoff Requests Received	ハンドオフ要求が受信、無視または応答された合計回数。
Handoff End Requests Received	ハンドオフ終了要求が受信された合計回数。これらの要求は、クライアント セッションの終了について通知するために、アンカー コントローラまたは外部コントローラによって送信されます。
State Transitions Disallowed	Policy Enforcement Module（PEM；ポリシー施行モジュール）がクライアントの状態の遷移を拒否しました。通常、その結果としてハンドオフが中断されます。
Resource Unavailable	バッファなどの必要なリソースが使用できませんでした。その結果としてハンドオフが中断されます。
Mobility Initiator Statistics	
Handoff Requests Sent	コントローラにアソシエートされ、モビリティ グループに通知されているクライアントの数。
Handoff Replies Received	送信された要求に応答して受信されている、ハンドオフ応答の数。
Handoff as Local Received	クライアント セッション全体が転送されているハンドオフの数。
Handoff as Foreign Received	クライアント セッションが別の場所でアンカーされたハンドオフの数。
Handoff Denys Received	拒否されたハンドオフの数。
Anchor Request Sent	スリーパーティ（外部から外部）ハンドオフ用に送信されたアンカー要求の数。ハンドオフが別の外部コントローラから受信され、新しいコントローラがクライアントを移動させるためのアンカーを要求しています。
Anchor Deny Received	現在のアンカーによって拒否されたアンカー要求の数。
Anchor Grant Received	現在のアンカーによって許可されたアンカー要求の数。
Anchor Transfer Received	現在のアンカー上でセッションを閉じ、要求元にアンカーを送り返したアンカー要求の数。
Mobility Responder Statistics	
Handoff Requests Ignored	コントローラにそのクライアントが認識されていなかったために無視された、ハンドオフ要求またはクライアント通知の数。

表 11-1　モビリティの統計 （続き）

パラメータ	説明
Ping Pong Handoff Requests Dropped	ハンドオフ期間が短すぎた（3 秒）ために拒否されたハンドオフ要求の数。
Handoff Requests Dropped	クライアントについての認識が不完全であるか、パケットの問題が原因でドロップされたハンドオフ要求の数。
Handoff Requests Denied	拒否されたハンドオフ要求の数。
Client Handoff as Local	クライアントがローカル ロールにある間に送信されたハンドオフ応答の数。
Client Handoff as Foreign	クライアントが外部ロールにある間に送信されたハンドオフ応答の数。
Anchor Requests Received	受信したアンカー要求の数。
Anchor Requests Denied	拒否されたアンカー要求の数。
Anchor Requests Granted	許可されたアンカー要求の数。
Anchor Transferred	クライアントが外部コントローラから現在のアンカーとして同じサブネット上のコントローラに移動したために、転送されたアンカーの数。

ステップ 3　現在のモビリティ統計をクリアする場合は、**Clear Stats** をクリックします。

CLI を使用したモビリティ グループの統計の表示

コントローラの CLI を使用して、モビリティ グループの統計を表示する手順は、次のとおりです。

ステップ 1　モビリティ グループの統計を表示するには、次のコマンドを入力します。

show mobility statistics

ステップ 2　各統計の説明については、表 11-1 を参照してください。

ステップ 3　現在のモビリティ統計をクリアする場合は、次のコマンドを入力します。

clear stats mobility

自動アンカー モビリティの設定

無線 LAN 上でローミング クライアントの負荷分散とセキュリティを向上させるために、自動アンカー モビリティ（*ゲスト トンネリング*とも呼ばれる）を使用できます。通常のローミング状態では、クライアント デバイスは無線 LAN に接続され、最初に接触するコントローラにアンカーされます。クライアントが異なるサブネットにローミングする場合、クライアントのローミング先のコントローラは、アンカー コントローラを備えたクライアントの外部セッションを設定します。ただし、自動アンカー モビリティ機能を使用して、無線 LAN 上のクライアントのアンカー ポイントとしてコントローラまたはコントローラのセットを指定できます。

自動アンカー モビリティ モードでは、モビリティ グループのサブセットは WLAN のアンカー コントローラとして指定されます。クライアントのネットワークへのエントリ ポイントに関係なく、この機能を使用して WLAN を単一のサブネットに制限できます。それにより、クライアントは企業全体にわたりゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、自動アンカー モビリティで地理的負荷分散も提供でき、WLAN のホーム コントローラのセットを効果的に作成できます。モバイル クライアントがたまたま最初に接触するコントローラにアンカーされるのではなく、特定の圏内にあるアクセス ポイントを制御するコントローラにモバイル クライアントをアンカーできます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モビリティ グループのすべてのコントローラ上で同じセットのアンカー コントローラを設定する必要があります。

クライアントが WLAN のモビリティ アンカーとして設定されていないモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカル セッションが作成され、コントローラが同じモビリティ グループの別のコントローラに通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカー コントローラに接触して、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティ トンネルを介してカプセル化され、アンカー コントローラに送信されます。ここでカプセルを解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカー コントローラに受信され、EtherIP を使用してモビリティ トンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

4.1 以前のコントローラのソフトウェア リリースでは、モビリティ グループ内に到着不能になったコントローラがあるかどうか自動で判断する方法はありませんでした。そのため、到着不能なアンカー コントローラに外部コントローラが新たなクライアント要求を送信し続け、セッションがタイムアウトするまでクライアントがこの到着不能なコントローラに接続し続けることがありました。このコントローラのソフトウェア リリース 4.1 以降では、モビリティ グループのメンバ同士が ping 要求をお互いに送信し合い、データを確認してそのデータのパスを管理することで、到着不能なメンバがいないかを調べてクライアントを再ルーティングできます。それぞれのアンカー コントローラに送信する ping 要求の数と間隔は、設定可能です。この機能には、ゲスト トンネリングのほか、通常のモビリティでモビリティをフェールオーバーできるよう、ゲスト N+1 冗長性が備わっています。

ゲスト N+1 冗長性を利用すると、到着不能なアンカーを検出できます。到着不能なアンカー コントローラが検出されると、このコントローラに接続していたすべてのクライアントが認証解除され、すぐに別のコントローラに接続できるようになります。この機能は、モビリティ フェールオーバーによって通常のモビリティ クライアントにも使用されます。この機能によって、モビリティ グループのメンバは到着不能なメンバを検出してクライアントを再ルーティングできます。

(注)　2100 シリーズ コントローラは、WLAN のアンカーとして指定できません。ただし、2100 シリーズ コントローラ上に作成された WLAN に 4400 シリーズ コントローラをアンカーとして指定できます。

(注)　IPSec および L2TP レイヤ 3 セキュリティ ポリシーは、モビリティ アンカーで設定された WLAN には使用できません。

自動アンカー モビリティを使用する際のガイドライン

自動アンカー モビリティを設定するためのガイドラインは、次のとおりです。

- コントローラを WLAN のモビリティ アンカーとして指定するには、そのコントローラをモビリティ グループ メンバ リストに追加する必要があります。
- WLAN のモビリティ アンカーとして、複数のコントローラを設定できます。
- WLAN のモビリティ アンカーを設定する前に、WLAN を無効にする必要があります。
- 自動アンカー モビリティは、Web 認可をサポートしていますが、その他のレイヤ 3 セキュリティ タイプをサポートしていません。
- 外部コントローラ上の WLAN とアンカー コントローラ上の WLAN は、両方ともモビリティ アンカーを使用して設定する必要があります。アンカー コントローラ上で、アンカー コントローラ自体をモビリティ アンカーとして設定します。外部コントローラ上で、アンカーをモビリティ アンカーとして設定します。
- 自動アンカー モビリティは、DHCP オプション 82 と共には使用できません。
- ゲスト N+1 冗長性とモビリティ フェールオーバー機能にファイアウォールを組み合わせて使用する場合は、以下のポートに空きがあることを確認してください。
  - UDP 16666：トンネル コントロール トラフィック用
  - UDP 16667：暗号化トラフィック用
  - IP Protocol 97：ユーザのデータ トラフィック用
  - UDP 161 および 162：SNMP

GUI を使用した自動アンカー モビリティの設定

GUI を使用して WLAN の新たなモビリティ アンカーを作成するには、次の手順に従って操作します。

(注)　CLI を使用して自動アンカー モビリティを設定する場合は、「自動アンカー モビリティを設定するための CLI の使用」の項（P. 11-24）を参照してください。

ステップ 1　モビリティ グループ内に到着不能なアンカー コントローラがないかを検出するには、次の手順でコントローラを設定してください。

a. **Controller** > **Mobility Management** > **Mobility Anchor Config** の順にクリックして、Mobility Anchor Config ページを開きます（図 11-14 を参照）。

図 11-14　Mobility Anchor Config ページ

b. Keep Alive Count フィールドに、そのアンカーが到着不能と判断するまでにアンカー コントローラに ping 要求を送信する回数を入力します。有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。

c. Keep Alive Interval フィールドには、アンカー コントローラに送信する各 ping 要求の所要時間を秒単位で入力します。有効な範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。

d. **Apply** をクリックして、変更を適用します。

ステップ 2　**WLANs** をクリックして、WLANs ページを開きます（図 11-15 を参照。）

図 11-15　WLANs ページ

ステップ 3　目的の WLAN または有線ゲスト LAN の青のドロップダウン矢印をクリックして、**Mobility Anchors** を選択します。Mobility Anchors ページが表示されます（図 11-16 を参照）。

図 11-16　Mobility Anchors ページ

このページには、すでにモビリティ アンカーとして設定されているコントローラが一覧表示されるほか、そのデータと管理パスの現状が表示されます。モビリティ グループ内のコントローラは、well-known UDP ポート上で管理情報をお互いに通信し合い、Ethernet-over-IP（EoIP）トンネルを通じてデータ トラフィックを交換します。具体的には、mpings を送信して、モビリティ制御パケットの到着可能性を管理インターフェイスのモビリティ UDP ポート 16666 によってテストします。また、epings を送信して、モビリティ データ トラフィックを管理インターフェイスの EoIP ポート 97 によってテストします。Control Path フィールドは、mpings が通過した（up）か通過しなかった（down）かを表示します。Data Path フィールドは、epings が通過した（up）か通過しなかった（down）かを表示します。Data Path フィールドまたは Control Path フィールドに「down」が表示された場合は、モビリティ アンカーが到着できず、接続できないと考えられます。

ステップ 4　モビリティ アンカーに指定されたコントローラの IP アドレスを、Switch IP Address （Anchor）ドロップダウン ボックスで選択します。

ステップ 5　**Mobility Anchor Create** をクリックします。選択したコントローラが、この WLAN または有線ゲスト LAN のアンカーになります。

（注）　WLAN または有線ゲスト LAN のモビリティ アンカーを削除するには、アンカーの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 6　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 7　ステップ 4 およびステップ 6 を繰り返し、他のコントローラをこの WLAN または有線ゲスト LAN のモビリティ アンカーとして設定します。

ステップ 8　モビリティ グループのすべてのコントローラに同じセットのモビリティ アンカーを設定します。

自動アンカー モビリティを設定するための CLI の使用

これらのコマンドで、CLI を使用して自動アンカー モビリティを設定します。

（注）　CLI コマンドで使用されるパラメータの有効範囲およびデフォルト値については、「GUI を使用した自動アンカー モビリティの設定」の項（P. 11-22）を参照してください。

1. コントローラを設定して、モビリティ グループ内のモビリティ グループ メンバ（アンカー コントローラなど）の中に到着不能のものがないかどうかを検出するには、以下のコマンドを入力します。
   - **config mobility group keepalive count** *count*：そのメンバが到着不能と判断されるまでにモビリティ グループ メンバに送信する ping 要求の回数。有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。
   - **config mobility group keepalive interval** *seconds*：モビリティ グループ メンバに送信する各 ping 要求の所要時間（秒単位）。有効な範囲は 1 ～ 30 秒で、デフォルト値は 10 秒です。
2. **config {wlan | guest-lan} disable {***wlan_id* | *guest_lan_id***}** と入力し、モビリティ アンカーを設定している WLAN または有線ゲスト LAN を無効にします。

3. WLAN または有線ゲスト LAN の新たなモビリティ アンカーを作成するには、次のコマンドのいずれかを入力します。
   - **config mobility group anchor add {wlan | guest-lan} {***wlan_id* | *guest_lan_id***}** *anchor_controller_ip_address*
   - **config {wlan | guest-lan} mobility anchor add {***wlan_id* | *guest_lan_id***}** *anchor_controller_ip_address*

（注） *wlan_id* または *guest_lan_id* は、存在しているが無効になっており、*anchor_controller_ip_address* は、デフォルトのモビリティ グループのメンバである必要があります。

（注） WLAN または有線ゲスト LAN の自動アンカー モビリティは、最初のモビリティ アンカーを設定する際に有効になります。

4. WLAN または有線ゲスト LAN のモビリティ アンカーを削除するには、次のコマンドのいずれかを入力します。
   - **config mobility group anchor delete {wlan | guest-lan} {***wlan_id* | *guest_lan_id***}** *anchor_controller_ip_address*
   - **config {wlan | guest-lan} mobility anchor delete {***wlan_id* | *guest_lan_id***}** *anchor_controller_ip_address*

（注） *wlan_id* または *guest_lan_id* は存在し、無効になっている必要があります。

（注） 最後のアンカーを削除すると、自動アンカー モビリティ機能が無効化され、新たなアソシエーションに対して通常のモビリティがレジュームされます。

5. 設定を保存するには、次のコマンドを入力します。

   save config

6. 特定の WLAN または有線ゲスト LAN のモビリティ アンカーとして設定されたコントローラのリストとステータスを表示するには、次のコマンドを入力します。

   show mobility anchor {**wlan** | **guest-lan**} {*wlan_id* | *guest_lan_id*}

（注） *wlan_id* パラメータと *guest_lan_id* パラメータはオプションであり、リストを特定の WLAN またはゲスト LAN のアンカーに制限します。システムのすべてのモビリティ アンカーを表示するには、**show mobility anchor** と入力します。

たとえば、**show mobility anchor** コマンドに対しては、次のような情報が表示されます。

```
Mobility Anchor Export List
WLAN IDIP AddressStatus
110.50.234.2UP
110.50.234.6UP
210.50.234.2UP
210.50.234.3CNTRL_DATA_PATH_DOWN

GLAN IDIP AddressStatus
110.20.100.2UP
210.20.100.3UP
```

Status フィールドには、次のうちいずれかの値が表示されます。

- UP：コントローラは到達可能で、データを渡すことができます。
- CNTRL_PATH_DOWN：mpings の送信に失敗しました。この制御パスでは到達できず、障害が発生すると考えられます。
- DATA_PATH_DOWN：epings の送信に失敗しました。この制御パスでは到達できず、障害が発生すると考えられます。
- CNTRL_DATA_PATH_DOWN：mpings と epings の両方の送信に失敗しました。この制御パスでは到達できず、障害が発生すると考えられます。

7. すべてのモビリティ グループ メンバのステータスを確認するには、次のコマンドを入力します。

show mobility summary

次のような情報が表示されます。

```
Mobility Keepalive interval..................... 10
Mobility Keepalive count........................ 3
Mobility Group members configured............... 3

Controllers configured in the mobility group
MAC AddressIP AddressGroup NameStatus
00:0b:85:32:b1:80  10.10.1.1localUp
00:0b:85:33:a1:7010.1.1.2localData Path Down
00:0b:85:23:b2:3010.20.1.2localUp
```

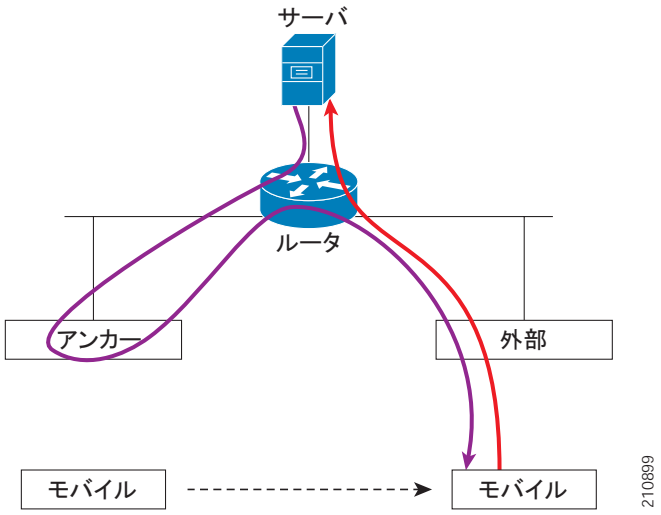
8. モビリティの問題のトラブルシューティングを行うには、以下のコマンドを入力します。

- **debug mobility handoff** {**enable** | **disable**}：モビリティのハンドオフ問題をデバッグします。
- **debug mobility keep-alive** {**enable** | **disable**} **all**：すべてのモビリティ アンカーの keepalive パケットをダンプします。
- **debug mobility keep-alive** {**enable** | **disable**} *IP_address*：特定のモビリティ アンカーの keepalive パケットをダンプします。

シンメトリック モビリティ トンネリングの設定

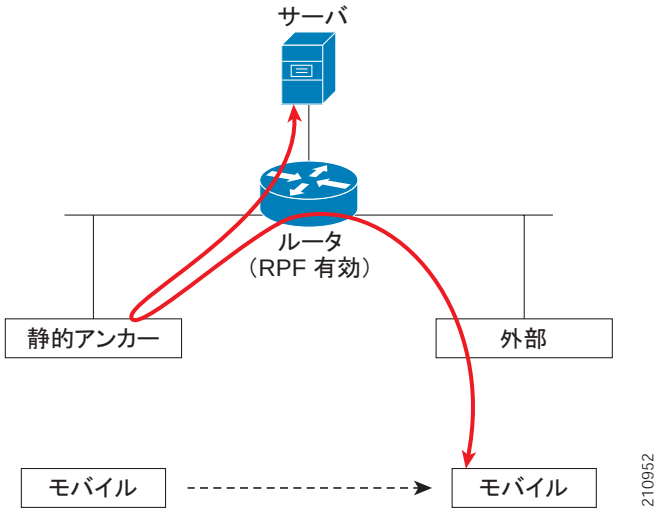
無線 LAN 内でアクセス ポイントから別のアクセス ポイントへクライアント ローミングを実現するため、本コントローラにはサブネット間のモビリティが備わっています。図 11-17 に示すとおり、このモビリティは非対称のため、有線ネットワークへのクライアント トラフィックは外部コントローラから直接ルーティングされます。

図 11-17　アシンメトリック トンネリングまたは単一指向性トンネリング



この仕組みでは、上流のルータに Reverse Path Filtering（RPF; 逆方向パス転送）が有効に設定されている場合、切断されます。この場合、RPF チェックによって、ソース アドレスに戻るパスとパケットの着信先パスを一致させるため、クライアント トラフィックがルータでドロップされます。この問題はコントローラのソフトウェア リリース 4.1 以降では解決され、シンメトリック モビリティ トンネリングがモバイル クライアントでサポートされるようになりました。シンメトリック モビリティ トンネリングを有効に設定すると、図 11-18 に示すように、すべてのクライアント トラフィックがアンカー コントローラに送信され、RPF チェックを正常に通過します。

図 11-18　シンメトリック モビリティ トンネリングまたは双方向性トンネリング



ソース IP アドレスがパケットの受信先サブネットと一致しないため、クライアント パケット パス内のファイアウォール設置でパケットがドロップされる場合は、シンメトリック モビリティ トンネリングも有効に設定してください。シンメトリック モビリティ トンネリングは、GUI または CLI のどちらを使用しても設定できます。

（注） 自動アンカー モビリティを使用中の場合、2100 シリーズ コントローラは WLAN のアンカーとして指定できませんが、シンメトリック モビリティ トンネリングではアンカーとして指定して、外部コントローラからトンネルされている上流のクライアント データ トラフィックを処理して転送できます。

（注） シナリオを混同しないよう、シンメトリック モビリティ トンネリングにはモビリティ グループ内のすべてのコントローラで同じ設定を共有するようにしてください。

（注） アンカー コントローラ上のアクセス ポイント グループ VLAN が、外部コントローラ上の WLAN インターフェイス VLAN とは異なる場合は、シンメトリック モビリティ トンネリングを有効化する必要があります。それ以外の場合、モビリティ イベント中に、クライアント トラフィックが誤った VLAN に送信される可能性があります。

シンメトリック モビリティ トンネリングを設定するための GUI の使用

コントローラ GUI を使用してシンメトリック モビリティ トンネリングを設定する手順は、次のとおりです。

ステップ 1　**Controller** > **Mobility Management** > **Mobility Anchor Config** の順にクリックして、Mobility Anchor Config ページを開きます（図 11-19 を参照）。

図 11-19　Mobility Anchor Config ページ

ステップ 2　このコントローラにシンメトリック モビリティ トンネリングを有効に設定するには、**Symmetric Mobility Tunneling Mode** チェックボックスをオンにし、この機能を無効に設定するにはチェックボックスをオフにします。デフォルトではオフになっています。

（注）　シンメトリック モビリティ トンネリングは、本コントローラをリブートしないと有効または無効に設定されません。このパラメータの現在の状態は、チェックボックスの右横にカッコで囲まれて表示されています（例：currently enabled または currently disabled）。

ステップ 3　**Apply** をクリックして、変更を適用します。

ステップ 4　設定内容を保存するようメッセージが表示されたら **OK** をクリックして、本コントローラをリブートして変更内容を反映させます。

ステップ 5　**Save Configuration** をクリックして、変更を保存します。

ステップ 6　設定内容を保存するか確認メッセージが表示されたら、**Yes** をクリックします。

ステップ 7　ここでコントローラをリブートするには、**Commands** > **Reboot** をクリックしてから、**Reboot** をクリックします。

ステップ 8　モビリティ グループ内のすべてのコントローラで、シンメトリック モビリティ トンネリングには同じ設定を必ず共有してください。

シンメトリック モビリティ トンネリングを設定するための CLI の使用

コントローラ CLI を使用してシンメトリック モビリティ トンネリングを設定する手順は、次のとおりです。

ステップ 1　シンメトリック モビリティ トンネリングを有効または無効にするには、次のコマンドを入力します。

config mobility symmetric-tunneling {**enable** | **disable**}

ステップ 2　変更内容を反映するようコントローラをリブートするには、次のコマンドを入力します。

reset system

ステップ 3　シンメトリック モビリティ トンネリングのステータスを確認するには、次のコマンドを入力します。

show mobility summary

次のような情報が表示されます。

```
Symmetric Mobility Tunneling (current) ..... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... User1
Mobility Keepalive interval..... 10
Mobility Keepalive count..... 3
Mobility Group members configured..... 7

Controllers configured in the Mobility Group
MAC Address          IP Address    Group Name      Status
00:0b:85:32:b0:80    10.28.8.30       User1        Up
00:0b:85:47:f6:00    10.28.16.10      User1        Up
00:16:9d:ca:d8:e0    10.28.32.10      User1        Up
00:18:73:34:a9:60    10.28.24.10      <local>      Up
00:18:73:36:55:00    10.28.8.10       User1        Up
00:1a:a1:c1:7c:e0    10.28.32.30      User1        Up
00:d0:2b:fc:90:20    10.28.32.61      User1           Control and Data Path Down
```

（注） 画面には、シンメトリック モビリティ トンネリングの現在のステータスと、リブート後のこの機能のステータスの両方が表示されます。

ステップ 4　モビリティ グループ内のすべてのコントローラで、シンメトリック モビリティ トンネリングには同じ設定を必ず共有してください。

モビリティ ping テストの実行

同じモビリティ グループに属するコントローラは、well-known UDP ポート上で情報を制御し、Ethernet-over-IP（EoIP）トンネルを通じてデータ トラフィックを交換することにより、お互いに通信します。UDP と EoIP は信頼できる転送メカニズムではないため、モビリティ コントロール パケットまたはデータ パケットがモビリティ ピアに配信される保証はありません。ファイアウォールによる UDP ポートや EoIP パケットのフィルタリング、あるいはルーティングの問題のために、モビリティ パケットが転送中に消失する可能性があります。

コントローラ ソフトウェア リリース 4.0 以降を使用すると、モビリティ ping テストを実行することにより、モビリティ通信環境をテストできます。これらのテストを使用して、モビリティ グループ（ゲスト コントローラを含む）のメンバ間の接続を検証できます。次の 2 つの ping テストが利用できます。

- **UDP 上でのモビリティ ping**：このテストは、モビリティ UDP ポート 16666 上で実行されます。管理インターフェイス上でモビリティ コントロール パケットに到達できるかどうかをテストします。
- **EoIP 上のモビリティ ping**：このテストは EoIP 上で実行されます。管理インターフェイス上で、モビリティ データ トラフィックをテストします。

各コントローラにつき、実行できるモビリティ ping テストは 1 度に 1 回だけです。

（注） これらの ping テストは、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）ベースではありません。「ping」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。

コントローラ CLI を使用してモビリティ ping テストを実行するには、次のコマンドを使用します。

1. 2 つのコントローラ間でモビリティ UDP コントロール パケット通信をテストするには、次のコマンドを入力します。

   mping *mobility_peer_IP_address*

   mobility_peer_IP_address パラメータは、モビリティ グループに属するコントローラの IP アドレスにする必要があります。

2. 2 つのコントローラ間でモビリティ EoIP データ パケット通信をテストするには、次のコマンドを入力します。

   eping *mobility_peer_IP_address*

   mobility_peer_IP_address パラメータは、モビリティ グループに属するコントローラの IP アドレスにする必要があります。

3. モビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

   config logging buffered debugging

   show logging

   UDP 上のモビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

   debug mobility handoff enable

   （注） トラブルシューティングを行う際には、Ethereal トレース キャプチャを使用することをお勧めします。

CHAPTER 12

Hybrid REAP の設定

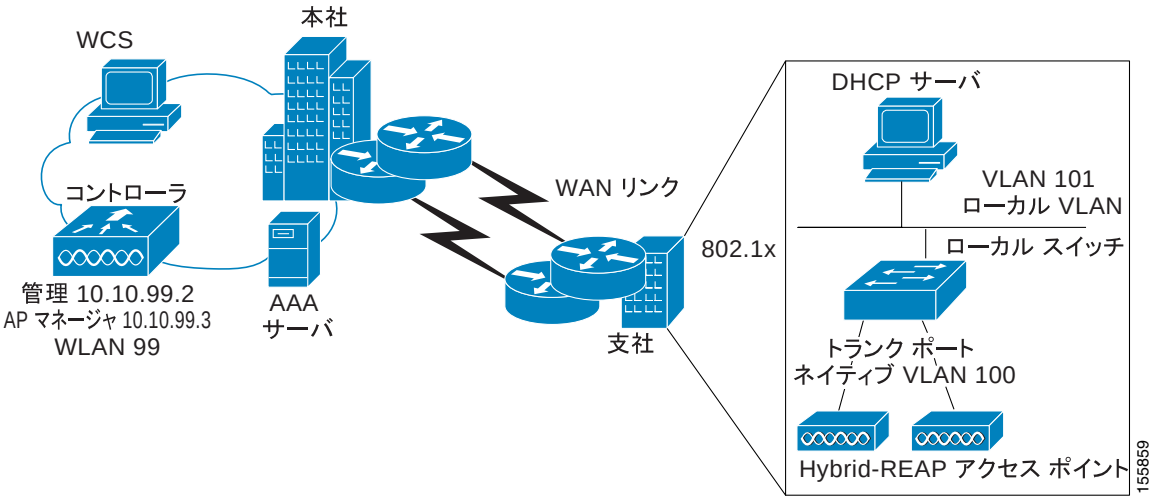
この章では、Hybrid REAP、およびこの機能をコントローラとアクセス ポイント上で設定する方法について説明します。この章の内容は、次のとおりです。

Hybrid REAP の概要

Hybrid REAP は、支社またはリモート オフィスでの展開のための無線ソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリア ネットワーク）経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。Hybrid REAP アクセス ポイントは、コントローラへの接続が失われた場合、クライアント データ トラフィックをローカルにスイッチして、ローカルにクライアント認証を行うことができます。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。

Hybrid REAP は、1130AG アクセス ポイント、1240AG アクセス ポイント、および 1250 アクセス ポイントと、2100 および 4400 シリーズのコントローラ、Catalyst 3750G 統合型無線 LAN コントローラ スイッチ、Cisco WiSM、サービス統合型ルータのコントローラ ネットワーク モジュールでのみサポートされます。図 12-1 は、一般的な Hybrid REAP 展開を示しています。

図 12-1　Hybrid REAP の展開



Hybrid REAP アクセス ポイントは、1 ロケーションにつき何台でも展開できます。ただし、帯域幅は最低でも 128 kbps を維持しながら、ラウンドトリップ遅延は 100 ミリ秒を超えてはならず、Maximum Transmission Unit（MTU; 最大伝送ユニット）は 500 バイトを下回ってはなりません。

Hybrid REAP の認証プロセス

Hybrid REAP アクセス ポイントがブートされると、コントローラを検索します。コントローラが見つかると、コントローラに接続し、最新のソフトウェア イメージと設定をコントローラからダウンロードして、無線を初期化します。スタンドアロン モードで使用するために、不揮発性メモリにダウンロードした設定を保存します。

Hybrid REAP アクセス ポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- DHCP サーバからアクセス ポイントに IP アドレスが割り当てられている場合、通常の LWAPP ディスカバリ プロセス [レイヤ 3 ブロードキャスト、over-the-air provisioning（OTAP）、DNS、または DHCP オプション 43] を介してコントローラを発見できます。

（注）　OTAP は、購入後初のブート時には動作しません。

- アクセス ポイントに静的 IP アドレスが割り当てられている場合は、DHCP オプション 43 以外の方法の LWAPP ディスカバリ プロセスを使用してコントローラを検出できます。アクセス ポイントでレイヤ 3 ブロードキャストまたは OTAP を使用してコントローラを検出できない場合は、DNS 名前解決の使用をお勧めします。DNS の場合、DNS サーバを認識している静的 IP アドレスを持つ任意のアクセス ポイントは、最低 1 つのコントローラを見つけることができます。
- LWAPP ディスカバリ メカニズムが使用可能でないリモート ネットワークからアクセス ポイントによりコントローラを見つける場合、プライミングを使用できます。この方法を使用すると、アクセス ポイントの接続先のコントローラを（アクセス ポイントの CLI により）指定できます。

（注）　アクセス ポイントによるコントローラ検出方法の詳細は、第 7 章、または次の URL からアクセスできるコントローラ展開ガイドを参照してください。
http://wnbu-tme/docs/Controller_DG_1.3_External.pdf

Hybrid REAP アクセス ポイントがコントローラに到達できるとき（*接続モード*と呼ばれます）、コントローラはクライアント認証を支援します。Hybrid REAP アクセス ポイントがコントローラにアクセスできないとき、アクセス ポイントはスタンドアロン モードに入り、独自にクライアントを認証します。

（注）　アクセス ポイント上の LED は、デバイスが異なる Hybrid REAP モードに入るときに変化します。LED パターンの情報については、アクセス ポイントのハードウェア インストール ガイドを参照してください。

クライアントが Hybrid REAP アクセス ポイントにアソシエートするとき、アクセス ポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアント データ パケットをローカルにスイッチする（ローカル スイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータ パケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：コントローラがクライアント認証を処理し、すべてのクライアント データはコントローラにトンネルを通じて戻されます。この状態は接続モードでのみ有効です。
- **中央認証、ローカル スイッチング**：コントローラがクライアント認証を処理し、Hybrid REAP アクセス ポイントがデータ パケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードと共に設定コマンドを送信し、Hybrid REAP アクセス ポイントに対して、ローカルにデータ パケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。
- **ローカル認証、ローカル スイッチング**：Hybrid REAP アクセス ポイントがクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。この状態はスタンドアロン モードでのみ有効です。

- **認証ダウン、スイッチング ダウン**：WLAN が既存クライアントをアソシエート解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：WLAN が認証を試みる新しいクライアントをすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答を送信し続けます。この状態はスタンドアロン モードでのみ有効です。

Hybrid REAP アクセス ポイントがスタンドアロン モードに入ると、オープン、共有、WPA-PSK、または WPA2-PSK 認証に対して設定されている WLAN は、「ローカル認証、ローカル スイッチング」状態に入り、新しいクライアント認証を続行します。コントローラ ソフトウェア リリース 4.2 以降では、これは 802.1X、WPA-802.1X、WPA2-802.1X、または CCKM 用に設定された WLAN でも同様です。ただし、これらの認証タイプでは外部の RADIUS サーバが設定されている必要があります。その他の WLAN は、「認証ダウン、スイッチング ダウン」状態（WLAN が中央スイッチングに対して設定されている場合）または「認証ダウン、ローカル スイッチング」状態（WLAN がローカル スイッチングに対して設定されている場合）のいずれかに入ります。

（注） 前述のように、802.1X EAP 認証をサポートするには、スタンドアロン モードの Hybrid REAP アクセス ポイントでは、クライアントを認証するためにそのアクセス ポイント独自の RADIUS サーバが必要となります。このバックアップ RADIUS サーバは、コントローラによって使用されるサーバである場合もそうでない場合もあります。コントローラの CLI を使用してバックアップ RADIUS サーバを個々の Hybrid REAP アクセス ポイントに対して設定するか、GUI または CLI のどちらかを使用して Hybrid REAP グループに対して設定することができます。個々のアクセス ポイント用に設定されたバックアップ サーバでは、Hybrid REAP グループに対する RADIUS サーバ設定は上書きされます。

Hybrid REAP アクセス ポイントがスタンドアロン モードに入ると、中央でスイッチされる WLAN 上にあるすべてのクライアントをアソシエート解除します。Web 認証 WLAN の場合は既存クライアントはアソシエート解除されませんが、Hybrid REAP アクセス ポイントはアソシエートされているクライアントの数がゼロ（0）に達すると、ビーコン応答の送信を停止します。また、Web 認証 WLAN にアソシエートしている新しいクライアントにアソシエート解除メッセージを送信します。Network Access Control（NAC; ネットワーク アクセス コントロール）や Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティは無効化され、アクセス ポイントからコントローラへの Intrusion Detection System（IDS; 侵入検知システム）レポートは送信されなくなります。さらに、ほとんどの Radio Resource Management（RRM）機能（ネイバー ディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバー リストの使用、不正阻止および検出）は無効化されます。ただし、Hybrid REAP アクセス ポイントは、スタンドアロン モードで動的周波数選択をサポートします。

（注） コントローラが NAC に対して設定されている場合、クライアントはアクセス ポイントが接続モードにある場合にのみアソシエートできます。NAC が有効化されている場合、正常に動作しない（または検疫された）VLAN を作成する必要があります。これは、WLAN がローカル スイッチングに対して設定されている場合でも VLAN に割り当てられている任意のクライアントのデータ トラフィックがコントローラを経由するようにするためです。クライアントが検疫 VLAN に割り当てられると、クライアントのすべてのデータ パケットは中央でスイッチされます。検疫 VLAN の作成については、「動的インターフェイスの設定」の項（P. 3-17）を参照してください。

Hybrid REAP アクセス ポイントは、スタンドアロン モードに入った後も、クライアントの接続を維持します。ただし、アクセス ポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

Hybrid REAP のガイドライン

Hybrid REAP を使用するときには、次の点に留意してください。

- Hybrid REAP アクセス ポイントは、静的 IP アドレスまたは DHCP アドレスのいずれかで展開できます。DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセス ポイントの IP アドレスを提供できる必要があります。
- Hybrid REAP 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 Maximum Transmission Unit（MTU; 最大伝送ユニット）WAN リンクをサポートします。
- ラウンドトリップ遅延は、アクセス ポイントとコントローラ間で 100 ミリ秒（ms）を超えてはならず、LWAPP コントロール パケットはすべてのその他のトラフィックよりも優先される必要があります。
- 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 パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。Hybrid REAP モードで、アクセス ポイント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。
- CCKM 高速ローミングを Hybrid REAP アクセスポイントで使用するには、Hybrid REAP グループを設定する必要があります。詳細は、「Hybrid REAP グループの設定」の項（P. 12-17）を参照してください。
- Hybrid-REAP アクセス ポイントは 1 対 1 の Network Address Translation（NAT; ネットワーク アドレス変換）設定をサポートします。また、真のマルチキャストを除くすべての機能に対して、Port Address Translation（PAT; ポート アドレス変換) をサポートします。マルチキャストは、ユニキャスト オプションを使用して設定する場合、NAT 境界全体にわたってサポートされます。NAT と PAT は Hybrid REAP アクセス ポイント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。
- VPN、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプがアクセス ポイントでローカルにアクセス可能であれば、ローカルにスイッチされるトラフィックに対してサポートされます。
- Hybrid-REAP アクセス ポイントは、複数の SSID をサポートします。詳細は、「CLI を使用した WLAN の作成」の項（P. 6-5）を参照してください。
- Hybrid REAP アクセス ポイントのプライマリ コントローラとセカンダリ コントローラでは、同じ設定をする必要があります。設定が異なると、アクセス ポイントはその設定を失い、特定の機能（WLAN の無効化、AP グループ VLAN、静的チャネル番号など）が正しく動作しないことがあります。さらに、Hybrid REAP アクセス ポイントの SSID とそのインデックス番号は、両方のコントローラで複製してください。

Hybrid REAP の設定

Hybrid REAP を設定するには、提供される順に次の項の指示に従ってください。

リモート サイトでのスイッチの設定

リモート サイトでスイッチを準備する手順は、次のとおりです。

ステップ 1　スイッチ上のトランクまたはアクセス ポートに、Hybrid REAP に対して有効化されるアクセス ポイントを接続します。

（注）　次の設定例は、スイッチ上のトランクに接続されている Hybrid REAP アクセス ポイントを示します。

ステップ 2　Hybrid REAP アクセス ポイントをサポートするようにスイッチを設定するには、次の設定例を参照してください。

この設定例では、Hybrid REAP アクセス ポイントは、ネイティブ VLAN 100 でトランク インターフェイス FastEthernet 1/0/2 に接続されています。このアクセス ポイントは、ネイティブ VLAN 上で IP 接続を必要とします。リモート サイトには、VLAN 101 上にローカル サーバとリソースがあります。スイッチ内の両方の VLAN に対して、DHCP プールがローカル スイッチ内に作成されます。最初の DHCP プール（ネイティブ）は、Hybrid REAP アクセス ポイントによって使用され、2 番目の DHCP プール（ローカル スイッチ）は、ローカルにスイッチされている WLAN にアソシエートするときにクライアントによって使用されます。設定例の太字のテキストは、これらの設定を示します。

（注）　この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに収まる必要があります。

ローカル スイッチ設定例：

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Hybrid REAP に対するコントローラの設定

この項では、GUI または CLI を使用して Hybrid REAP コントローラを設定する手順について説明します。

GUI を使用した、Hybrid REAP に対するコントローラの設定

Hybrid REAP のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。GUI を使用してこれらの WLAN のコントローラを設定するには、この項の手順に従ってください。この手順では、次の 3 つの WLAN を例として使用します。

WLAN	Security	スイッチング	インターフェイス マッピング（VLAN）
employee	WPA1+WPA2	中央	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2 (PSK)	Local	101（ローカルにスイッチされる VLAN）
guest-central	Web 認証	中央	management（中央でスイッチされる VLAN）

（注）　CLI を使用して Hybrid REAP のコントローラを設定する場合は、「CLI による Hybrid REAP のコントローラの設定」の項（P. 12-11）を参照してください。

ステップ 1　中央でスイッチされる WLAN を作成する手順は次のとおりです。例では、これは最初の WLAN（employee）です。

a. **WLANs** をクリックして WLANs ページを開きます。

b. **New** をクリックして WLANs > New ページを開きます（図 12-2 を参照）。

図 12-2　WLANs > New ページ

c. Type ドロップダウン ボックスから、**WLAN** を選択します。

d. Profile Name フィールドで、WLAN に一意のプロファイル名を付けます。

e. WLAN SSID フィールドに WLAN の名前を入力します。

f. **Apply** をクリックして、変更を適用します。WLANs > Edit ページが表示されます（図 12-3 を参照）。

図 12-3　WLANs > Edit ページ

g. WLANs タブ > Edit タブの各設定から、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security タブ > Layer 2 タブから Layer 2 Security に **WPA1+WPA2** を選択してから、WPA1+WPA2 パラメータを設定する必要があります。

（注）　General タブの **Status** チェックボックスをオンにして、この WLAN を必ず有効化するようにしてください。

（注） NAC が有効化されているときに、検疫 VLAN を作成し、この WLAN に対して検疫 VLAN を使用する場合には、General タブの Interface ドロップダウン ボックスから選択することを確認してください。また、Advanced タブの **Allow AAA Override** チェックボックスをオンにして、コントローラが検疫 VLAN 割り当てをチェックするように確認してください。

h. **Apply** をクリックして、変更を適用します。

i. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 2　ローカルにスイッチされる WLAN を作成する手順は次のとおりです。例では、これは 2 番目の WLAN（employee-local）です。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN には「employee-local」という名前が付けられています。

b. WLANs > Edit ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security タブ > Layer 2 タブから Layer 2 Security に **WPA1+WPA2** を選択してから、WPA1+WPA2 パラメータを設定する必要があります。

（注） General タブの **Status** チェックボックスをオンにして、この WLAN を必ず有効化するようにしてください。さらに、Advanced タブの **H-REAP Local Switching** チェックボックスをオンにして、ローカル スイッチングを確実に有効化してください。ローカル スイッチングを有効化すると、この WLAN をアドバタイズするすべての Hybrid REAP アクセス ポイントは、データ パケットを（コントローラへトンネリングする代わりに）ローカルにスイッチできます。

（注） Hybrid REAP アクセス ポイントの場合、H-REAP ローカル スイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。これは、SSID 別、Hybrid REAP アクセス ポイント別に容易に変更できます。Hybrid REAP 以外のアクセス ポイントでは、すべてのトラフィックがコントローラへトンネリングで戻され、VLAN タギングは各 WLAN のインターフェイス マッピングによって要求されます。

c. **Apply** をクリックして、変更を適用します。

d. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 3　ゲスト アクセスに使用される中央スイッチの WLAN も作成する場合は、次の手順に従ってください。例では、これは 3 番目の WLAN（guest-central）です。中央サイトからの保護されていないゲスト トラフィックに対する企業データ ポリシーを施行できるように、ゲスト トラフィックをコントローラにトンネリングする必要のある場合があります。

（注） 第 9 章は、ゲスト ユーザ アカウントの作成に関する詳細について説明します。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN には「employee-local」という名前が付けられています。

b. WLANs > Edit ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security > Layer 2 タブと Security > Layer 3 タブから Layer 2 Security および Layer 3 Security の両方に **None** を選択し、**Web Policy** チェックボックスをオンにして、Layer 3 タブで **Authentication** が選択されていることを確認する必要があります。

（注） 外部 Web サーバを使用している場合には、WLAN 上でサーバに対する事前認証 Access Control List（ACL; アクセス コントロール リスト）を設定し、Layer 3 タブでこの ACL を WLAN 事前認証 ACL として選択する必要があります。ACL の詳細は、第 5 章を参照してください。

（注） General タブの **Status** チェックボックスをオンにして、この WLAN を必ず有効化するようにしてください。

c. **Apply** をクリックして、変更を適用します。

d. **Save Configuration** をクリックして、変更内容を保存します。

e. ゲスト ユーザがこの WLAN に初めてアクセスするときに表示されるログイン ページのコンテンツと外観をカスタマイズする場合は、第 5 章の指示に従ってください。

f. この WLAN にローカル ユーザを追加するには、**Security** > **AAA** > **Local Net Users** をクリックしてください。

g. Local Net Users ページが表示されたら、**New** をクリックします。Local Net Users > New ページが表示されます（図 12-4 を参照）。

図 12-4　Local Net Users > New ページ

h. User Name フィールドと Password フィールドに、ローカル ユーザのユーザ名とパスワードを入力します。

i. Confirm Password フィールドに、パスワードを再度入力します。

j. **Guest User** チェックボックスをオンにして、このローカル ユーザ アカウントを有効にします。

k. Lifetime フィールドに、このユーザ アカウントをアクティブにする時間（秒数）を入力します。

l. Guest User チェックボックスをオンにして新しいユーザを追加するときに、このゲスト ユーザに QoS ロールを割り当てるには、**Guest User Role** チェックボックスをオンにします。デフォルトの設定は、オフになっています。

（注）　ゲスト ユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

m. Guest User Role チェックボックスをオンにして新しいユーザを追加する場合は、このゲスト ユーザに割り当てる QoS ロールを Role ドロップダウン ボックスから選択します。新しい QoS ロールを作成する手順は、「Quality of Service ロールの設定」の項（P. 4-55）を参照してください。

n. WLAN Profile ドロップダウン ボックスから、ローカル ユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である **Any WLAN** を選択すると、ユーザは設定済みのすべての WLAN にアクセスできます。

o. Description フィールドに、ローカル ユーザを説明するタイトル（「ゲスト ユーザ」など）を入力します。

p. **Apply** をクリックして、変更を適用します。

q. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 4　「Hybrid REAP のアクセス ポイントの設定」の項（P. 12-12）へ移動して、Hybrid REAP に対する最大 6 台までのアクセス ポイントを設定します。

CLI による Hybrid REAP のコントローラの設定

次のコマンドを使用して、Hybrid REAP のコントローラを設定します。

- **config wlan h-reap local-switching** *wlan_id* **enable**：ローカル スイッチングに対して WLAN を設定します。
- **config wlan h-reap local-switching** *wlan_id* **disable**：中央スイッチングに対して WLAN を設定します。これはデフォルト値です。

（注）　「Hybrid REAP のアクセス ポイントの設定」の項（P. 12-12）へ移動して、Hybrid REAP に対する最大 6 台までのアクセス ポイントを設定します。

次のコマンドを使用して、Hybrid REAP 情報を取得します。

- **show ap config general** *Cisco_AP*：VLAN 設定を表示します。
- **show wlan wlan_id**：WLAN がローカルにスイッチされているか、中央でスイッチされているかを表示します。
- **show client detail** *client_mac*：クライアントがローカルにスイッチされているか、中央でスイッチされているかを表示します。

次のコマンドを使用して、デバッグ情報を取得します。

- **debug lwapp events enable**：LWAPP イベントに関するデバッグ情報を提供します。
- **debug lwapp error enable**：LWAPP エラーに関するデバッグ情報を提供します。
- **debug pem state enable**：Policy Manager ステート マシンに関するデバッグ情報を提供します。
- **debug pem events enable**：Policy Manager イベントに関するデバッグ情報を提供します。
- **debug dhcp packet enable**：DHCP パケットに関するデバッグ情報を提供します。
- **debug dhcp message enable**：DHCP エラー メッセージに関するデバッグ情報を提供します。

Hybrid REAP のアクセス ポイントの設定

この項では、コントローラの GUI または CLI を使用して Hybrid REAP のアクセス ポイントを設定する手順について説明します。

GUI を使用した Hybrid REAP のアクセス ポイントの設定

コントローラの GUI を使用して Hybrid REAP のアクセス ポイントを設定する手順は、次のとおりです。

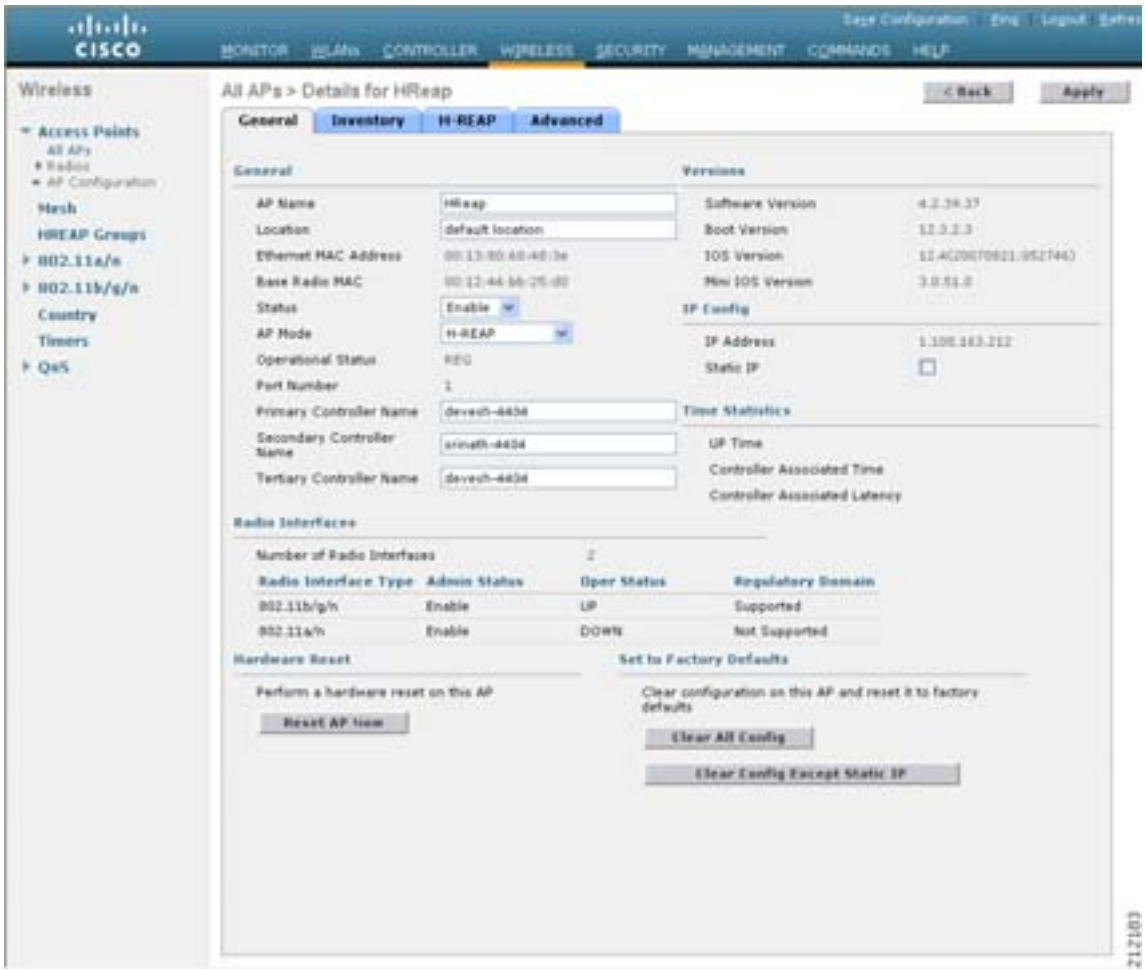
ステップ 1　アクセス ポイントが物理的にネットワークに追加されていることを確認します。

ステップ 2　**Wireless** をクリックして、All APs ページを開きます（図 12-5 を参照）。

図 12-5　All APs ページ

ステップ 3　目的のアクセス ポイントの名前をクリックします。All APs > Details（General）ページが表示されます（図 12-6 を参照）。

図 12-6　All APs > Details (General) ページ



ステップ 4　このアクセス ポイントに対して Hybrid REAP を有効にするには、AP Mode ドロップダウン ボックスから **H-REAP** を選択します。

（注）　Inventory タブの最後のパラメータは、このアクセス ポイントを Hybrid REAP に対して設定できるかどうかを示します。1130AG アクセス ポイント、1240AG アクセス ポイント、および 1250 アクセス ポイントのみが、Hybrid REAP をサポートしています。

ステップ 5　**Apply** をクリックして変更を適用し、アクセス ポイントをリブートさせます。

ステップ 6　**H-REAP** タブをクリックして、All APs > Details（H-REAP)）ページを開きます（図 12-7 を参照)。

図 12-7　All APs > Details (H-REAP) ページ

アクセス ポイントが Hybrid REAP グループに属している場合は、HREAP Group Name フィールドにグループ名が表示されます。

ステップ 7　**VLAN Support** チェックボックスをオンにし、**Native VLAN ID** フィールドにリモート ネットワーク上のネイティブ VLAN の数（100 など）を入力します。

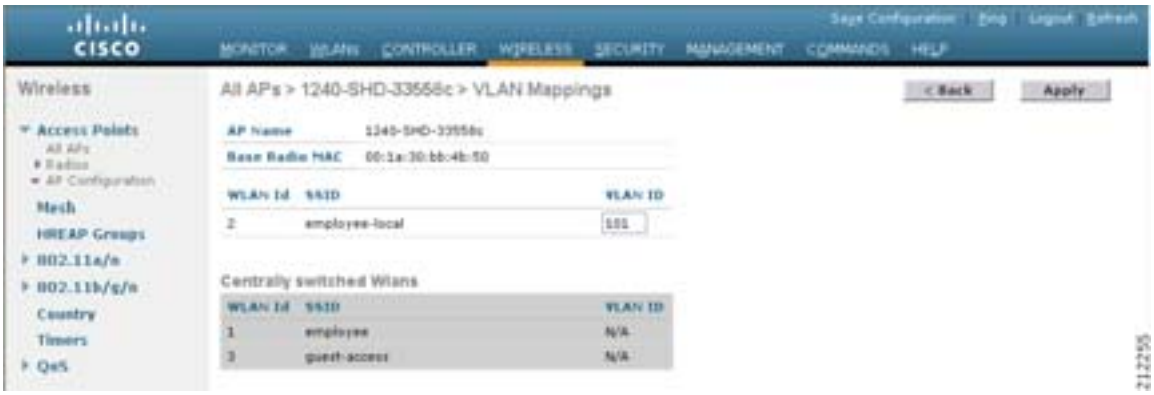
（注）　デフォルトで、VLAN は Hybrid REAP アクセス ポイント上では有効化されていません。Hybrid REAP が有効化されると、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。この設定はアクセス ポイントで保存され、接続応答が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 となります。VLAN が有効化されたドメインで、Hybrid REAP アクセス ポイントごとにネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。

ステップ 8　**Apply** をクリックして、変更を適用します。イーサネット ポートがリセットされる間、アクセス ポイントは一時的にコントローラへの接続を失います。

ステップ 9　同じアクセス ポイントの名前をクリックしてから、**H-REAP** タブをクリックします。

ステップ 10　**VLAN Mappings** をクリックして、All APs > *Access Point Name* > VLAN Mappings ページを開きます（図 12-8 を参照）。

図 12-8　All APs > Access Point Name > VLAN Mappings ページ



ステップ 11 ローカル スイッチング（この例では、VLAN 101）を行っているときにクライアントが IP アドレスを取得する VLAN の数を VLAN ID フィールドに入力します。

ステップ 12 **Apply** をクリックして、変更を適用します。

ステップ 13 **Save Configuration** をクリックして、変更内容を保存します。

ステップ 14 リモート サイトで、Hybrid REAP に対して設定が必要なその他すべてのアクセス ポイントについて、この手順を繰り返します。

CLI を使用した Hybrid REAP に対するアクセス ポイントの設定

次のコマンドを使用して、Hybrid REAP に対するアクセス ポイントを設定します。

- **config ap mode h-reap** *Cisco_AP*：このアクセス ポイントに対する Hybrid REAP を有効化します。
- **config ap h-reap radius auth set** {**primary** | **secondary**} *ip_address auth_port secret Cisco_AP*：特定の Hybrid REAP アクセス ポイントに対してプライマリまたはセカンダリの RADIUS サーバを設定します。

（注） スタンドアロン モードでは、Session Timeout RADIUS 属性のみがサポートされています。その他のすべての属性や RADIUS アカウンティングはサポートされていません。

（注） Hybrid REAP アクセス ポイントに対して設定されている RADIUS サーバを削除するには、次のコマンドを入力します。**config ap h-reap radius auth delete** {**primary** | **secondary**} *Cisco_AP*

- **config ap h-reap vlan wlan** *wlan_id vlan-id Cisco_AP*：VLAN ID をこの Hybrid REAP アクセス ポイントに割り当てることができます。デフォルトで、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。
- **config ap h-reap vlan** {**enable** | **disable**} *Cisco_AP*：この Hybrid REAP アクセス ポイントに対して VLAN タギングを有効化または無効化します。デフォルトで、VLAN タギングは有効化されていません。VLAN タギングが Hybrid REAP アクセス ポイント上で有効化されると、ローカル スイッチングに対する WLAN は、コントローラで割り当てられている VLAN を継承します。
- **config ap h-reap vlan native** *vlan-id Cisco_AP*：この Hybrid REAP アクセス ポイントに対するネイティブ VLAN を設定できます。デフォルトで、VLAN はネイティブ VLAN に設定されています。（VLAN タギングが有効化されているとき）Hybrid REAP アクセス ポイントごとにネイティブ VLAN を 1 つ設定する必要があります。アクセス ポイントが接続されているスイッチ ポートに、対応するネイティブ VLAN も設定されていることを確認します。Hybrid REAP アクセス ポイントのネイティブ VLAN 設定と、アップストリーム スイッチポートのネイティブ VLAN が一致しない場合、アクセス ポイントではコントローラとの間のパケット送受信ができません。

Hybrid REAP アクセス ポイント上で次のコマンドを使用して、ステータス情報を取得します。

- **show lwapp reap status**：Hybrid REAP アクセス ポイントのステータス（connected または standalone）を表示します。
- **show lwapp reap association**：このアクセス ポイントおよび SSID にアソシエートされているクライアントのリストを表示します。

Hybrid REAP アクセス ポイント上で次のコマンドを使用して、デバッグ情報を取得します。

- **debug lwapp reap**：一般的な Hybrid REAP アクティビティを表示します。
- **debug lwapp reap mgmt**：クライアント認証メッセージとアソシエーション メッセージを表示します。
- **debug lwapp reap load**：Hybrid REAP アクセス ポイントがスタンドアロン モードでブートされるときに役立つ、ペイロード アクティビティを表示します。
- **debug dot11 mgmt interface**：802.11 管理インターフェイス イベントを表示します。
- **debug dot11 mgmt msg**：802.11 管理メッセージを表示します。
- **debug dot11 mgmt ssid**：SSID 管理イベントを示します。
- **debug dot11 mgmt state-machine**：802.11 ステート マシンを表示します。
- **debug dot11 mgmt station**：クライアント イベントを表示します。

クライアント デバイスの WLAN への接続

「Hybrid REAP に対するコントローラの設定」の項（P. 12-7）で作成した WLAN に接続するためのプロファイルを作成するには、クライアント デバイスで次の手順に従ってください。

例では、クライアント上で 3 つプロファイルを作成することになります。

1. 「employee」WLAN へ接続するには、PEAP-MSCHAPV2 認証で WPA/WPA2 を使用するクライアント プロファイルを作成します。クライアントは認証されると、コントローラの管理 VLAN から IP アドレスを取得します。
2. 「local-employee」WLAN へ接続するには、WPA/WPA2 認証を使用するクライアント プロファイルを作成します。クライアントは認証されると、ローカル スイッチ上の VLAN 101 から IP アドレスを取得します。
3. 「guest-central」WLAN へ接続するには、オープン認証を使用するクライアント プロファイルを作成します。クライアントは認証されると、アクセス ポイントにとってローカルのネットワーク上にある VLAN 101 から、IP アドレスを取得します。クライアントが接続すると、ローカル ユーザは、Web ブラウザに任意の http アドレスを入力できます。ユーザは、Web 認証プロセスを完了するために、自動的にコントローラへダイレクトされます。Web ログイン ページが表示されると、ユーザはユーザ名とパスワードを入力します。

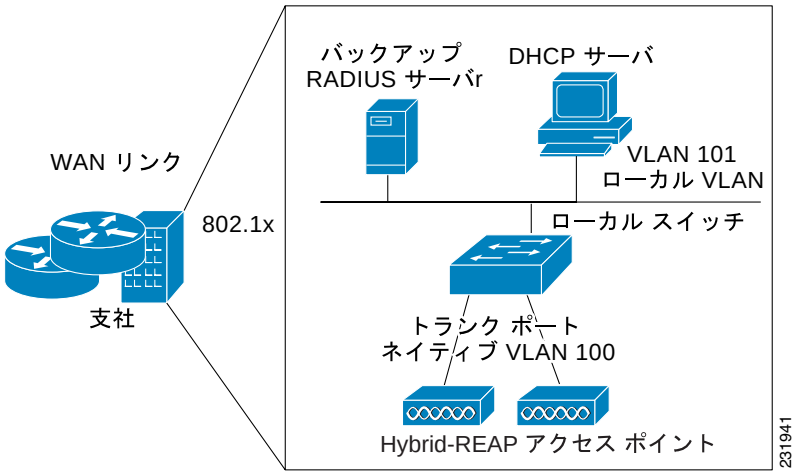
クライアントのデータ トラフィックがローカルに、または中央でスイッチされていることを確認するには、コントローラの GUI で、**Monitor** > **Clients** をクリックし、必要なクライアントの **Detail** リンクをクリックして、AP Properties の下の Data Switching パラメータを確認します。

Hybrid REAP グループの設定

Hybrid REAP アクセス ポイントをより体系化し管理しやすくするには、Hybrid REAP グループを作成して特定のアクセス ポイントをそれらに割り当てます。コントローラごとに、25 個までのアクセス ポイントを含む Hybrid REAP グループを最大 20 個設定できます。

グループ内のすべての Hybrid REAP アクセス ポイントは、同じ WLAN、バックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。この機能は、リモート オフィス内や建物のフロア上に複数の Hybrid REAP アクセス ポイントがあり、それらすべてを一度に設定する場合に役立ちます。たとえば、各アクセス ポイント上で同じサーバの設定を行なうのではなく、Hybrid REAP グループに対してバックアップ RADIUS サーバを設定することができます。図 12-9 は、支社でのバックアップ RADIUS サーバを備えた Hybrid REAP グループの一般的な展開を示しています。

図 12-9　Hybrid REAP グループの展開



Hybrid REAP グループとバックアップ RADIUS サーバ

スタンドアロン モードの Hybrid REAP アクセス ポイントが完全な 802.1X 認証を実行して RADIUS サーバをバックアップできるようにコントローラを設定できます。プライマリ RADIUS サーバを設定することも、プライマリとセカンダリの両方の RADIUS サーバを設定することもできます。

Hybrid REAP グループと CCKM

Hybrid REAP グループは、Hybrid REAP アクセス ポイントと共に使用する CCKM 高速ローミングで必要となります。CCKM 高速ローミングは、無線クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、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アクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。Hybrid REAP アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM 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 個のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。限られた数のアクセス ポイントから成る Hybrid REAP グループを作成する場合（たとえば、リモート オフィス内の 4 つのアクセス ポイントにグループを作成するとします）、クライ

アントはそれら 4 つのアクセス ポイント間でのみローミングし、クライアントがアクセス ポイントから別のアクセス ポイントへアソシエートするときだけ、それら 4 つのアクセス ポイント間で CCKM キャッシュが分散されます。

(注)　Hybrid REAP アクセス ポイントと Hybrid REAP 以外のアクセス ポイントとの間の CCKM 高速ローミングはサポートされていません。CCKM の設定方法については、「WPA1 と WPA2」の項（P. 6-21）を参照してください。

Hybrid REAP グループとローカル認証

スタンドアロン モードの Hybrid REAP アクセス ポイントが最大 20 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、Hybrid REAP アクセス ポイントがコントローラに接続する際に、ユーザ名とパスワードの静的リストを各 Hybrid REAP アクセス ポイントに送信します。グループ内の各アクセス ポイントは、そのグループにアソシエートされたクライアントのみを認証します。

この機能は、Autonomous アクセス ポイント ネットワークから LWAPP Hybrid REAP アクセス ポイント ネットワークに移行する顧客で、かつ、より大きなユーザ データベースを保持する必要もなく、Autonomous アクセス ポイントで使用できる RADIUS サーバの機能の代わりに別のハードウェア デバイスを追加することもない顧客に最適です。

(注)　この機能は、Hybrid REAP 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。Hybrid REAP 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、Hybrid REAP アクセス ポイントは、まずプライマリ バックアップ RADIUS サーバ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（プライマリに接続できない場合）、最後に Hybrid REAP アクセス ポイント自身の認証を試行します（プライマリとセカンダリの両方に接続できない場合）。

コントローラの GUI または CLI を使用して Hybrid REAP グループを設定するには、この項の手順に従ってください。

GUI を使用した Hybrid REAP グループの設定

コントローラの GUI を使用して Hybrid REAP グループを設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **HREAP Groups** の順にクリックして、HREAP Groups ページを開きます（図12-10 を参照）。

図 12-10　HREAP Groups ページ

このページでは、これまでに作成されたすべての Hybrid REAP グループが表示されます。

（注）　既存のグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 2　新しい Hybrid REAP グルーを作成するには、**New** をクリックします。

ステップ 3　HREAP Groups > New ページが表示されたら、新しいグループの名前を Group Name フィールドに入力します。最大 32 文字の英数字を入力できます。

ステップ 4　**Apply** をクリックして、変更を適用します。新しいグループが HREAP Groups ページに表示されます。

ステップ 5　グループのプロパティを編集するには、目的のグループの名前をクリックします。HREAP Groups > Edit（General）ページが表示されます（図 12-11 を参照）。

図 12-11　HREAP Groups > Edit（General）ページ

ステップ 6　プライマリ RADIUS サーバをこのグループに対して設定する場合（たとえば、アクセス ポイントで 802.1X 認証を使用している場合）、Primary RADIUS Server ドロップダウン リストから目的のサーバを選択します。それ以外の場合は、そのフィールドの設定をデフォルト値の None のままにします。

ステップ 7　セカンダリ RADIUS サーバをこのグループに対して設定する場合、Secondary RADIUS Server ドロップダウン リストからサーバを選択します。それ以外の場合は、そのフィールドの設定をデフォルト値の None のままにします。

ステップ 8　アクセス ポイントをグループに追加するには、**Add AP** をクリックします。追加のフィールドが「Add AP」の下にあるページに表示されます（図 12-12 を参照）。

図 12-12　HREAP Groups > Edit（General）ページ

ステップ 9　次のいずれかの操作を行います。

- このコントローラに接続するアクセス　ポイントを選択するには、**Select APs from Current Controller** チェックボックスをオンにし、AP Name ドロップダウン ボックスからアクセス ポイントの名前を選択します。

（注）　このコントローラ上でアクセス　ポイントを選択する場合は、不一致が起こらないように、アクセス ポイントの MAC アドレスが自動的に Ethernet MAC フィールドに入力されます。

- 別のコントローラに接続するアクセス ポイントを選択するには、**Select APs from Current Controller** チェックボックスをオフのままにし、そのアクセスポイントの MAC アドレスを Ethernet MAC フィールドに入力します。

（注）　グループ内の Hybrid REAP アクセス ポイントを別のコントローラに接続する場合は、すべてのコントローラが同じモビリティ グループに属している必要があります。

ステップ 10　**Add** をクリックして、アクセス ポイントをこの Hybrid REAP グループに追加します。アクセス ポイントの MAC アドレス、名前、およびステータスがページ下部に表示されます。

（注）　アクセス ポイントを削除するには、そのアクセス ポイントの青いドロップダウンの矢印の上にカーソルを置いて、**Remove** を選択します。

ステップ 11　**Apply** をクリックして、変更を適用します。

ステップ 12　Hybrid REAP グループにアクセス ポイントをさらに追加する場合は、ステップ 9 ～ ステップ 11 を繰り返します。

ステップ 13　Hybrid REAP グループのローカル認証を有効にする手順は、次のとおりです。

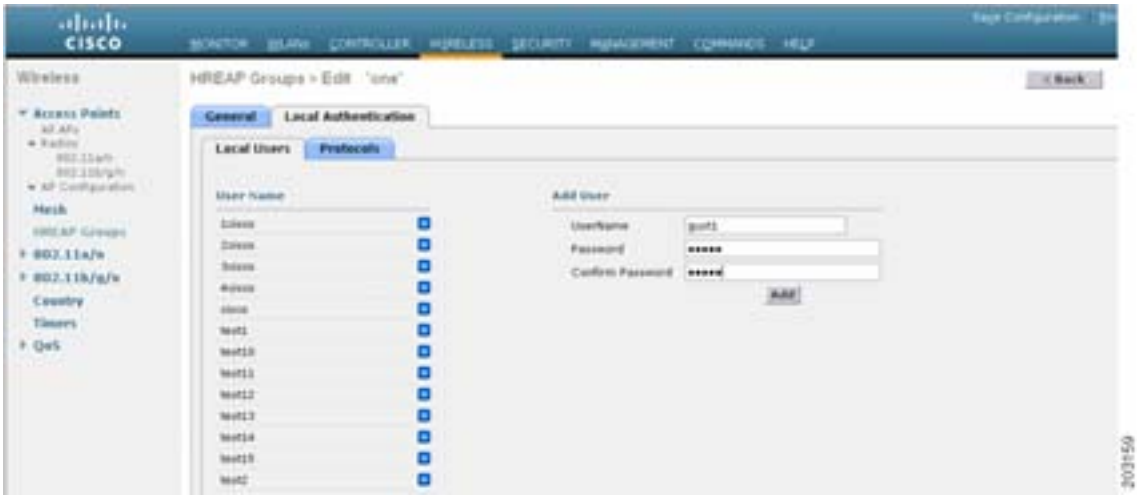
a. Primary RADIUS Server パラメータと Secondary RADIUS Server パラメータが **None** に設定されていることを確認します。

b. **Enable AP Local Authentication** チェックボックスをオンにして、この Hybrid REAP グループに対してローカル認証を有効にします。デフォルトではオフになっています。

c. **Apply** をクリックして、変更を適用します。

d. **Local Authentication** タブをクリックして、HREAP Groups > Edit（Local Authentication > Local Users）ページを開きます（図 12-13 を参照）。

図 12-13　HREAP Groups > Edit（Local Authentication > Local Users）ページ



e. UserName フィールドに LEAP または EAP-EAST を使用して認証できるクライアントのユーザ名を入力します。

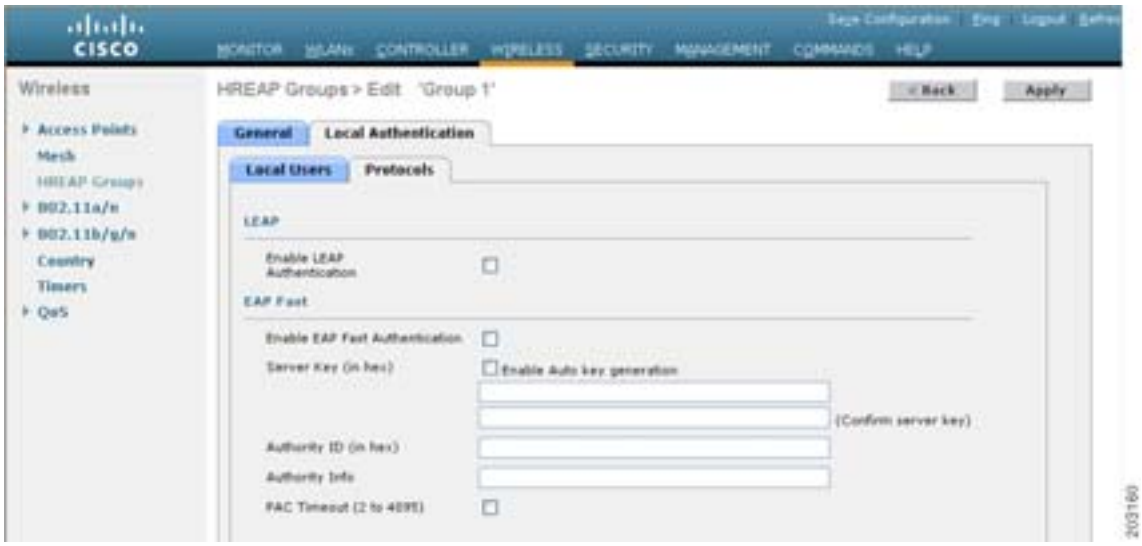
f. Password フィールドおよび Confirm Password フィールドに、前の手順で指定したクライアントのパスワードを入力します。

g. **Add** をクリックして、サポートされているローカル ユーザのリストに、このクライアントを追加します。クライアント名が「User Name」見出しの下のページの左側に表示されます。

h. **Apply** をクリックして、変更を適用します。

i. **Protocols** タブをクリックして、HREAP Groups > Edit（Local Authentication > Protocols）ページを開きます（図 12-14 を参照）。

図 12-14　HREAP Groups > Edit（Local Authentication > Protocols）ページ



j. Hybrid REAP アクセス ポイントで LEAP を使用しているクライアントを認証できるようにするには、**Enable LEAP Authentication** チェックボックスをオンにして、手順 p. に進みます。

k. Hybrid REAP アクセス ポイントで EAP-FAST を使用しているクライアントを認証できるようにするには、**Enable EAP-FAST Authentication** チェックボックスをオンにして次の手順に進みます。デフォルトではオフになっています。

l. Protected Access Credential（PAC）をプロビジョニングする方法に応じて、以下のいずれかを実行します。

- 手動の PAC プロビジョニングを使用するには、Server Key フィールドおよび Confirm Server Key フィールドに、PAC の暗号化と暗号化解除に使用するサーバ キーを入力します。このキーには 32 桁の 16 進数文字を使用します。
- PAC プロビジョニング中に PAC を持たないクライアントに PAC を自動的に送信できるようにするには、**Enable Auto Key Generation** チェック ボックスをオンにします。

m. Authority ID フィールドに、EAP-FAST サーバの権限識別子を 32 桁の 16 進数文字で入力します。

n. Authority Info フィールドに、EAP-FAST サーバの権限識別子をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。

o. PAC タイムアウト値を指定するには、**PAC Timeout** チェックボックスをオンにして、PAC が編集ボックスに表示される秒数を入力します。デフォルトではオフになっています。入力できる有効な範囲は 2 ～ 4095 秒です。

p. **Apply** をクリックして、変更を適用します。

ステップ 14　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 15　Hybrid REAP グループをさらに追加する場合は、この手順を繰り返します。

(注)　個々のアクセス ポイントが Hybrid REAP グループに属しているかどうかを確認するには、**Wireless** > **Access Points** > **All APs** > 目的のアクセス ポイントの名前 > **H-REAP** タブをクリックします。アクセス ポイントが Hybrid REAP グループに属している場合は、HREAP Group Name フィールドにグループ名が表示されます。

CLI を使用した Hybrid REAP グループの設定

コントローラ CLI を使用して Hybrid REAP グループを設定する手順は、次のとおりです。

ステップ 1　Hybrid REAP グループを追加または削除するには、次のコマンドを入力します。

config hreap group *group_name* {**add** | **delete**}

ステップ 2　プライマリまたはセカンダリの RADIUS サーバを Hybrid REAP グループに対して設定するには、次のコマンドを入力します。

config hreap group *group_name* **radius server** {**add** | **delete**} {**primary** | **secondary**} *server_index*

ステップ 3　アクセス ポイントを Hybrid REAP グループに追加するには、次のコマンドを入力します。

config hreap group *group_name* **ap** {**add** | **delete**} *ap_mac*

ステップ 4　Hybrid REAP グループのローカル認証を設定する手順は、次のとおりです。

a. Hybrid REAP グループにプライマリおよびセカンダリの RADIUS サーバが設定されていないことを確認します。

b. この Hybrid REAP グループのローカル認証を有効または無効にするには、次のコマンドを入力します。

config hreap group *group_name* **radius ap** {**enable** | **disable**}

c. LEAP または EAP-FAST を使用して認証できるクライアントのユーザ名とパスワードを入力するには、次のコマンドを入力します。

config hreap group *group_name* **radius ap user add** *username* **password** *password*

d. Hybrid REAP アクセス ポイントで LEAP を使用しているクライアントの認証を有効にするには、または無効にするには、次のコマンドを入力します。

config hreap group *group_name* **radius ap leap** {**enable** | **disable**}

e. Hybrid REAP アクセス ポイントで EAP-FAST を使用しているクライアントの認証を有効にするには、または無効にするには、次のコマンドを入力します。

config hreap group *group_name* **radius ap eap-fast** {**enable** | **disable**}

f. PAC をプロビジョニングする方法に応じて、次のいずれかのコマンドを入力します。

- **config hreap group** *group_name* **radius ap server-key** *key*：PAC の暗号化と暗号化解除に使用するサーバ キーを指定します。キーは 32 桁の 16 進数文字である必要があります。
- **config hreap group** *group_name* **radius ap server-key auto**：プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにします。

g. EAP-FAST サーバの権限識別子を指定するには、次のコマンドを入力します。

config hreap group *group_name* **radius ap authority id** *id*

id は 32 桁の 16 進数文字です。

h. EAP-FAST サーバの権限識別子をテキスト形式で指定するには、次のコマンドを入力します。

config hreap group *group_name* **radius ap authority info** *info*

info は 32 桁までの 16 進数文字です。

i. PAC が表示される秒数を指定するには、次のコマンドを入力します。

config hreap group *group_name* **radius ap pac-timeout** *timeout*

timeout は 2 ～ 4095 秒までの値（両端の値を含む）、または 0 です。デフォルト値 0 を指定すると、PAC タイムアウトは無効になります。

ステップ 5　変更を保存するには、次のコマンドを入力します。

save config

ステップ 6　Hybrid REAP グループの最新のリストを表示するには、次のコマンドを入力します。

show hreap group summary

次のような情報が表示されます。

```
HREAP Group Summary: Count 2

Group Name      # Aps
Group 1         1
Group 2         1
```

ステップ 7　特定の Hybrid REAP グループの詳細を表示するには、次のコマンドを入力します。

show hreap group detail *group_name*

次のような情報が表示されます。

```
Number of Ap's in Group: 3

00:1d:45:12:f2:24    AP1240.EW3.f224  Joined
00:1d:45:12:f7:12    AP1240.10.f712     Joined
00:1d:a1:ed:9f:84    AP1131.23.9f84     Joined


Group Radius Servers Settings:
 Primary Server Index.......................... Disabled
 Secondary Server Index........................ Disabled

Group Radius AP Settings:
AP RADIUS server............ Enabled
EAP-FAST Auth............... Enabled
LEAP Auth................... Enabled
Server Key Auto Generated... No
Server Key..................     <hidden>
Authority ID................ 436973636f00000000000000000000000
Authority Info.............. Cisco A_ID
PAC Timeout................. 0
Number of User's in Group: 20

                  1cisco                    2cisco
                  3cisco                    4cisco
                   cisco                     test1
                  test10                    test11
                  test12                    test13
                  test14                    test15
                   test2                     test3
                   test4                     test5
                   test6                     test7
                 test8                   test9
```

APPENDIX A

安全上の考慮事項および安全についての警告

この付録では、Cisco Unified Wireless Network ソリューション製品に適用される安全上の考慮事項と安全についての警告の翻訳を示します。この付録で説明する安全上の考慮事項と安全についての警告は、次のとおりです。

安全上の考慮事項

Cisco UWN Solution 製品をインストールする際は、次のガイドラインに従ってください。

- Cisco Lightweight アクセスポイントは、外部アンテナポートの有無にかかわらず、IEEE 802.3af で定義された環境 A における設置のみを目的としています。相互接続機器はすべて、アソシエートされた LAN 接続も含めて、同じ建物内に収容する必要があります。
- オプションの外部アンテナポートが装備されている Lightweight アクセスポイントでは、すべての外部アンテナとその配線が完全に屋内に設置されていることを確認してください。これらの Lightweight アクセスポイントとそのオプションの外部アンテナは、屋外での使用に適しません。
- プレナムに設置された Lightweight アクセスポイントは、安全規制に適合するよう Power over Ethernet （PoE）を使用して電源を投入してください。
- すべての Cisco Wireless LAN Controller について、ラックに設置した場合の温度上昇を考慮に入れて、周囲温度が 0 ℃ ～ 40 ℃ であることを確認してください。
- 複数の Cisco Wireless LAN Controller を機器ラックに取り付ける場合は、ラック内のすべての機器が安全に稼働可能な定格電源が使用されていることを確認してください。
- Cisco Wireless LAN Controller は、完全にアースされていることを確認してから機器ラックに取り付けてください。
- Lightweight アクセスポイントは、National Electrical Code の 300.22.C 項、Canadian Electrical Code、Part 1、C22.1 の 2-128、12-010（3)、および 12-100 の各項目に準拠しており、空間での使用に適しています。

警告の定義

警告　**安全上の重要な注意事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

クラス 1 レーザー製品についての警告

（注）　1000BASE-SX および 1000BASE-LX SFP モジュールには、EN 60825-1+A1+A2 に従ってクラス 1 レーザー（Laser Klasse 1）が装備されています。

警告　**クラス 1 レーザー製品です。**

アース導体についての警告

警告　この装置はアース接続する必要があります。アース導体を破損しないよう注意し、アース導体を正しく取り付けないまま装置を稼動させないでください。アース接続が適正であるかどうか分からない場合には、電気検査機関または電気技術者に相談してください。

筐体のラックへの設置と保守作業についての警告

警告　この装置をラックに設置したり保守作業を行ったりするときは、人身事故を防ぐため、システムが安定しているかどうかを十分に確認する必要があります。次の注意事項に従ってください。

- ラックにこの装置を単独で設置する場合は、ラックの一番下に設置します。
- ラックに別の装置がすでに設置されている場合は、最も重量のある装置を一番下にして、重い順に下から上へ設置します。
- ラックに安定器具が付属している場合は、その安定器具を取り付けてから、装置をラックに設置するか、またはラック内の装置の保守作業を行ってください。

バッテリの取り扱いについての警告

警告　不適切なバッテリに交換すると、爆発の危険性があります。製造元が推奨するものと同じまたは同等のバッテリだけを使用してください。使用済みのバッテリは、製造元が指示する方法に従って処分してください。

装置の設置についての警告

警告　この装置の設置、交換、保守は、訓練を受けた相応の資格のある人が行ってください。

複数の電源についての警告

警告　この装置には、複数の電源が接続されている場合があります。装置の電源を完全にオフにするには、すべての電源を切断する必要があります。

APPENDIX B

適合宣言および規制に関する情報

この付録には、Cisco UWN Solution の製品についての適合宣言および規制に関する情報を記載します。

この付録の内容は、次のとおりです。

Lightweight アクセス ポイントの規制に関する情報

この項には、Lightweight アクセス ポイントの規制に関する情報が記載されています。記載されている情報は次のとおりです。

製造業者による連邦通信委員会への適合宣言

モデル：

AIR-AP1010-A-K9、AIR-AP1020-A-K9、AIR-AP1030-A-K9

FCC 認証番号：

LDK102057

製造業者：

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

このデバイスは Part 15 の規定に準拠しています。動作は次の 2 つの条件を前提としています。

1. このデバイスにより有害な干渉を発生しない。
2. このデバイスは、予想外の動作を引き起こす可能性のある干渉を含め、受信した干渉をすべて受け入れる。

この機器は、FCC 規定の Part 15 に基づくクラス B デジタル デバイスの制限に準拠していることがテストによって確認済みです。制限は、住宅地で機器を使用した場合に有害な干渉が起きないようにするための、一定の保護を目的としたものです。この機器は無線周波エネルギーを発生、使用、および放射するため、取り扱い説明書に従わずに設置および使用した場合は有害な干渉を引き起こすことがあります。ただし、説明書に従った場合にも、干渉が絶対に起きないことを保証するものではありません。この機器によってラジオやテレビの受信に干渉が発生する場合は（機器をオン / オフすることで確認できます）、次のいずれかの方法で干渉をなくすようにしてください。

- 受信アンテナの向きや設置場所を変える。
- 機器とラジオ / テレビの位置を離す。

- ラジオ / テレビが接続されている回路とは別の回路のコンセントに機器を接続する。
- 販売店またはラジオやテレビの専門技術者に問い合せる。

注意　FCC 規定 Part 15 に適合した無線デバイスは、一体型アンテナを使用した場合、当該周波数で動作する他のデバイスと干渉のない状態で動作します。シスコによる明確な許可なしに製品への変更を行った場合、ユーザはこのデバイスの使用を禁止されることがあります。

注意　5.15 ～ 5.25GHz 帯域内（5GHz 無線チャネル 34 ～ 48）では、同じチャネルの Mobile Satellite System（MSS）への有害な干渉を削減するため、Unlicensed National Information Infrastructure（U-NII）デバイスの使用は屋内に制限されています。

カナダ通信省

モデル：

AIR-AP1010-A-K9、AIR-AP1020-A-K9、AIR-AP1030-A-K9

認証番号：

2461B-102057

カナダの適合宣言

このクラス B デジタル装置は、Canadian Interference-Causing Equipment Regulations のすべての要件を満たしています。

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

このデバイスは、カナダ産業省のクラス B の制限に適合しています。動作は次の 2 つの条件を前提としています。

1. このデバイスにより有害な干渉を発生しない。
2. このデバイスは、予想外の動作を引き起こす可能性のある干渉を含め、受信した干渉をすべて受け入れる。

Cisco Aironet の 2.4GHz アクセス ポイントは 2.4GHz スペクトル拡散方式のデバイスに関する RSS-210 の要件を満たし、Cisco Aironet の 54Mbp/5GHz アクセスポイントは 5GHz スペクトル拡散方式のデバイスに関する RSS-210 の要件を満たしています。部分的または完全に屋外で動作するシステムでこのデバイスを使用する場合、ユーザはカナダの規定に従ってそのシステムの免許を取得しなければならないことがあります。詳細は、各地域のカナダ産業省管轄部局にお問い合せください。

欧州共同体、スイス、ノルウェー、アイスランド、およびリヒテンシュタイン

モデル：

AIR-AP1010-E-K9、AIR-AP1020-E-K9、AIR-AP1030-E-K9

R&TTE 指令（1999/5/EC）に関する適合宣言

English:	この機器は、R&TTE 指令（1999/5/EC）の基本要件およびその他の関連規定に適合しています。

2.4GHz 無線には次の規格が適用されています。

- 無線：　EN 300.328-1、EN 300.328-2
- EMC：　EN 301.489-1、EN 301.489-17
- 安全性：　EN 60950

（注） この機器は、EU および EFTA 加盟国での使用を意図しています。屋外での使用については、一定の周波数に制限される場合や、免許が必要な場合があります。詳細は、Cisco Corporate Compliance にお問い合せください。

54Mbps の 5GHz アクセスポイントには次の規格が適用されています。

- 無線：　EN 301.893
- EMC：　EN 301.489-1、EN 301.489-17
- 安全性：　EN 60950

2.4GHz 無線および 5GHz 無線（54Mbps）のアクセスポイントには、次の CE マークが付けられています。

CE ⓘ

RF 被曝に関する適合宣言

無線は、無線周波数電磁場における人体の被曝に関する FCC ガイドライン（Evaluating Compliance with FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields）に定義された、無線周波デバイスによる RF 被曝の影響に関する CFR 47 第 2.1091、2.1093 および 15.247（b）（4）項の要件を満たすことが判明しています。機器は人体から 20cm 以上離して設置する必要があります。

アクセス ポイントは、アクセス ポイントで使用されている FCC の認可を受けたその他の室内 / 屋外アンテナから最低でも 20cm は離して設置する必要があります。FCC の認可を受けていないアンテナまたはトランスミッタを、アクセス ポイントと同じ場所に設置することはできません。アクセス ポイントと同じ場所に設置された 2.4GHz 一体型アンテナと 5GHz 一体型アンテナは、最低でも 8cm は離す必要があり、同時伝送時には該当する FCC RF 被曝制限に適合します。

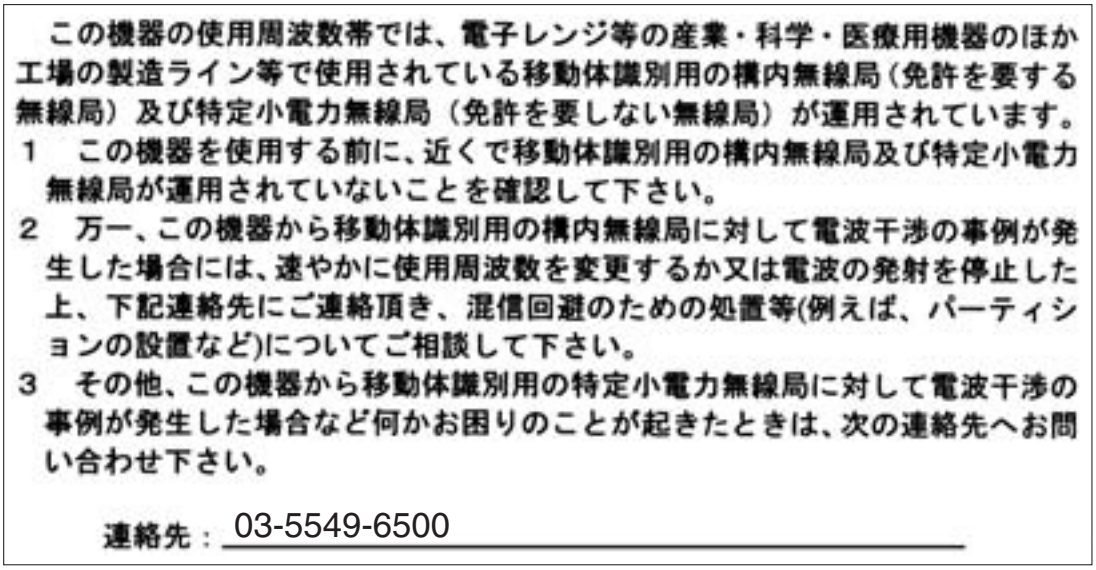
（注） ダイバーシティ用のデュアル アンテナは、同じ場所への設置とは見なされません。

Cisco Aironet アクセス ポイントの使用に関するガイドライン（日本）

この項では、日本で Cisco Aironet アクセス ポイントを使用する際に干渉を防ぐためのガイドラインを示します。

モデル：

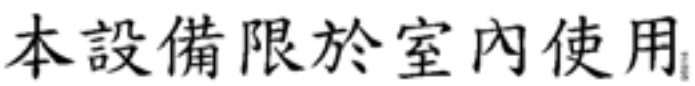
AIR-AP1010-J-K9、AIR-AP1020-J-K9、AIR-AP1030-J-K9



（Cisco Aironet アクセス ポイントに関する行政規定（台湾）

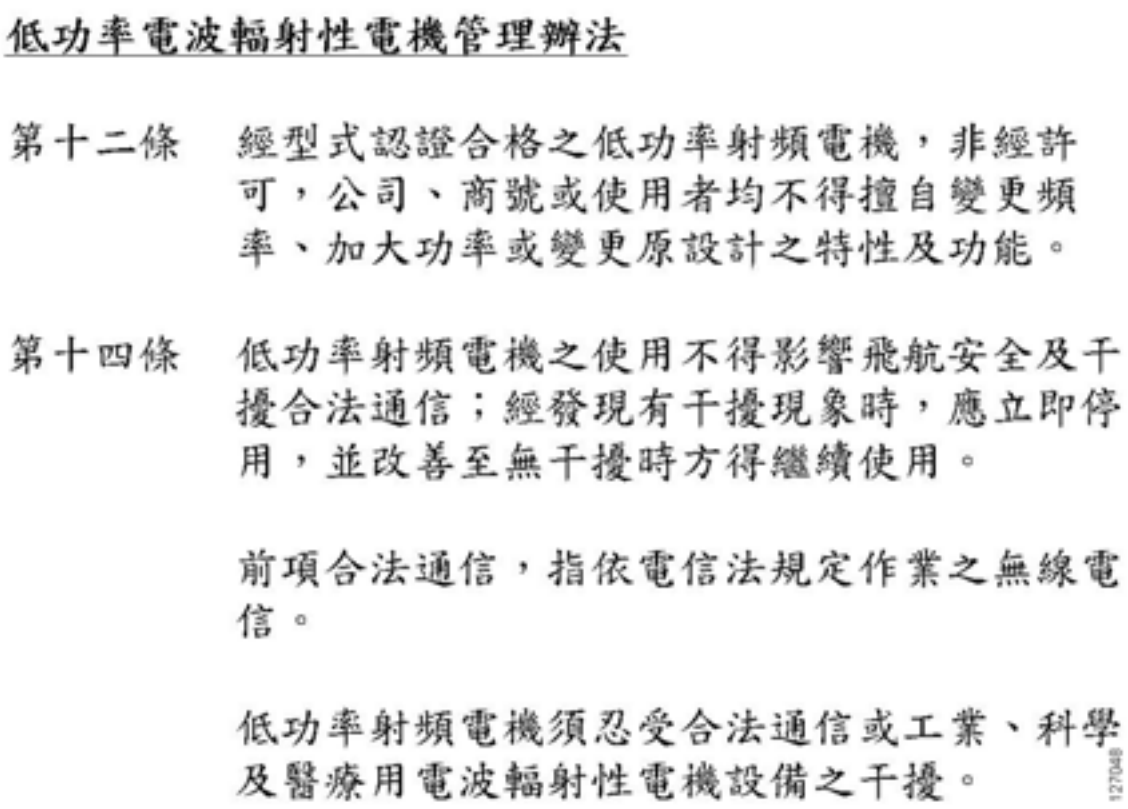
この項では、台湾における Cisco Aironet アクセス ポイントの使用に関する行政規定を示します。

IEEE 802.11a 無線のアクセス ポイント



この機器の使用は室内に制限されます。

すべてのアクセス ポイント



低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

低電力無線周波デバイスに関する行政規定

第 12 項

すでに形式承認されている低電力無線周波デバイスについては、企業、事業体、またはユーザによる周波数の変更、消費電力の増大、本来の機能の変更は認められていません。

第 14 項

低電力無線周波デバイスを使用する場合は、航空機の安全や認可された無線局に対する有害な干渉を発生しないという条件に従わなければなりません。干渉が発生した場合、ユーザはデバイスの使用をただちに停止する必要があり、干渉がなくなるまで使用を再開できません。

認可された無線局とは、電信法の規定に従って提供されている無線通信サービスのことです。

低電力無線周波デバイスの動作は、認可された無線局からの発信、別の送信アンテナ（故意による場合と故意でない場合のいずれも含む）、工業、科学、医療用（ISM）機器、または付帯する送信アンテナにより発生する干渉の影響を受ける可能性があります。

適合宣言

この製品に関するすべての適合宣言は、次のサイトに掲載されています。

http://www.ciscofax.com

Cisco 2100 シリーズ Wireless LAN Controller に関する FCC 規定について

この機器は、FCC 規定の Part 15 に基づくクラス B デジタル デバイスの制限に準拠していることがテストによって確認済みです。この制限は、住宅に設置した場合に有害な干渉が起きないようにするためのものです。この機器は無線周波エネルギーを発生、使用、および放射するため、取り扱い説明書に従わずに設置および使用した場合は、無線通信に有害な干渉を起こすことがあります。しかし、いかなる特定の設置条件でも干渉が起きないことを保証するものではありません。この機器によってラジオやテレビの受信に有害な干渉が発生する場合は（機器の電源をオン / オフするとわかります）、次の 1 つ以上の方法で干渉をなくすようにしてください。

- 受信アンテナの向きや設置場所を変える。
- 機器と受信装置の距離を広げる。
- 受信装置が接続されている回路とは別の回路のコンセントに機器を接続する。
- 販売店またはラジオやテレビの専門技術者に問い合わせる。[cfr reference 15.105]

4400 シリーズ Wireless LAN Controller に関する FCC 規定について

Cisco 4400 シリーズ Wireless LAN Controller は、FCC 規定の Part 15 に基づくクラス A デジタル デバイスの制限に準拠していることがテストによって確認済みです。この制限は、機器を商業環境で動作させた場合に有害な干渉が起きないようにするための、一定の保護を目的としたものです。この機器は無線周波エネルギーを発生、使用、および放射するため、取り扱い説明書に従って設置または使用しなかった場合には、無線通信に有害な干渉を起こすことがあります。また、この機器を住宅地で使用すると有害な干渉を起こすことがあり、その場合、ユーザの負担で干渉をなくす必要があります。

APPENDIX C

エンド ユーザ ライセンス契約および保証

この付録では、Cisco UWN Solution 製品に適用されるエンド ユーザ ライセンス契約および保証について説明します。

- Cisco 2100 シリーズ Wireless LAN Controller
- Cisco 4400 シリーズ Wireless LAN Controller
- Cisco Wireless Services Module （ワイヤレス サービス モジュール）

この付録の内容は、次のとおりです。

エンド ユーザ ライセンス契約

重要：本エンド ユーザ ライセンス契約をよくお読みください。シスコのソフトウェアまたはシスコが提供するソフトウェアをダウンロード、インストール、または使用することにより、お客様は本ライセンス契約に同意したものと見なされます。

お客様が本ライセンス契約に記載されているすべての条項に同意される場合のみ、シスコは本ソフトウェアのライセンスをお客様に許諾いたします。本ソフトウェアのダウンロード、インストール、または本ソフトウェアを内蔵する機器の使用により、お客様およびお客様が代表する企業体（以下、総称して「お客様」）は本契約に法的に拘束されます。本契約のいずれかの条項に同意されない場合は、シスコでは本ソフトウェアのライセンスを許諾いたしかねますので、本ソフトウェアのダウンロード、インストール、使用を行わないでください。この場合、お客様は、本ソフトウェアを返却して代金の全額払い戻しを受けるか、または本ソフトウェアが他の製品の一部として供給された場合には当該製品全体を返却して代金の全額払い戻しを受けることができます。返却および代金払い戻しの有効期限は、シスコまたはシスコにより認定されたリセラーから本ソフトウェアを購入後 30 日間であり、お客様が最初のエンド ユーザ購入者である場合にのみ適用されます。

(a) お客様とシスコとの間にお客様による本ソフトウェアの使用に関する署名済みの契約が別途存在する場合、または (b) インストールまたはダウンロード プロセスの一部としてソフトウェアに「クリック合意」ライセンス契約が別途含まれている場合を除き、本エンド ユーザ ライセンス契約（以下「契約」）の以下の条項が、お客様の本ソフトウェアへのアクセスおよび使用に対して適用されます。上記契約の条項に対立する内容が含まれている場合、契約の優先順位は（1）署名済みの契約、(2）クリック合意契約、(3）本エンド ユーザ ライセンス契約の順とします。

ライセンス。シスコシステムズ、またはシスコに代わりソフトウェアのライセンスを許諾するその関連子会社（以下「シスコ」）は、お客様に対し、本契約の条件に従うことを条件とし、お客さまが規定のライセンス料を支払ったソフトウェアおよび資料をお客様の社内業務目的で使用するための非独占的かつ譲渡不能なライセンスを許諾します。「資料」とは、特に本ソフトウェアに関して（ユーザ マニュアル、テクニカル マニュアル、トレーニング資料、仕様などに）記載されている情報のことであり、シスコから（CD-ROM、オンラインなどの）何らかの方法でソフトウェアとともに提供されます。

お客様が本ソフトウェアを使用するためのライセンスは、単一のハードウェア シャーシまたはカード、あるいは、シスコが同意済みの適用可能な発注書に記載された、お客様がシスコに支払った規定のライセンス料に相当する数のエージェント、同時ユーザ、セッション、IP アドレス、ポート、シート、サーバ、またはサイトに制限され、お客様はこれを超えてソフトウェアを使用しないものとします。

関連資料に明示されていない限り、お客様は本ソフトウェアを、お客様が所有または貸借している、お客様の社内業務目的に使用されるシスコ機器に内蔵されたものとして、かかるシスコ機器での実行、または（関連資料によってシスコ以外の機器へのインストールが許可されている場合には）かかるシスコ機器と通信のみを目的として使用するものとします。注：シスコがライセンス料を徴収しない評価版またはベータ版については、上記のライセンス料の支払い要件は適用されません。

一般的な制限。本契約は、ソフトウェアおよび資料の使用許諾であり、所有権を譲渡するものではありません。すべてのソフトウェアおよび資料の所有権はシスコが保有しています。お客様は、ソフトウェアおよび資料には、個々のプログラムの固有の内部設計と構造、関連インターフェイス情報などの、シスコおよびそのサプライヤ、またはライセンサの企業秘密が含まれていることを認めるものとします。したがって、本契約で明示的に規定されている場合を除き、お客様は、以下の行為を行う権利はなく、また以下の行為を行わないことに同意するものとします。

(i)　他者等へのお客様のライセンス権利の譲渡または二次ライセンスの付与、あるいは未承諾または中古のシスコ機器での本ソフトウェアの使用。お客様は、かかる譲渡、二次ライセンスの付与、または使用は無効であることを認めるものとします。

(ii)　本ソフトウェアに対するエラー修正またはその他の変更および改変、本ソフトウェアに基づく派生著作権物の作成、または第三者への当該行為の許可。

(iii)　本ソフトウェアを、リバース エンジニアリング、逆コンパイル、復号化、逆アセンブル、またはその他の方法により、判読可能な形式に変換すること。ただし、この制限にかかわらず、適用される法律により明示的に許可されている場合を除きます。

(iv)　シスコの書面による許可なく、サービス ビューロ、タイム シェアリング、またはその他の方法により、第三者へのサービス提供を目的として本ソフトウェアを使用、または使用を許可すること。

(v)　シスコの書面による事前の同意なしに、本ソフトウェアおよび資料に含まれる企業秘密を第三者に対して開示、提供、またはその他の何らかの方法により公開すること。お客様は、かかる企業秘密を保護するための妥当なセキュリティ対策を講ずるものとします。

(vi)　本ソフトウェアを採用した再販目的のソフトウェアアプリケーションの開発のための本ソフトウェアの使用。

シスコは、法律により求められている範囲内で、お客様からの書面による依頼に応じて、本ソフトウェアと独自に開発された他のプログラムとの互換性を実現するために必要なインターフェイス情報を、シスコが妥当と見なす料金が支払われた場合にお客様に提供するものとします。お客様は、当該情報について厳重な秘密保持義務を負うものとし、シスコが当該情報を提供する際には、適用される条件に従って当該情報を使用するものとします。お客様は、本契約で特に許可されている場合を除き、その他の知的所有権に対する暗黙の使用許諾は付与されていません。

ソフトウェアのアップグレードおよび追加の複製物。本契約で言及する「ソフトウェア」には、シスコまたは認定されたシスコのリセラーからお客様に提供されたコンピュータ プログラム（ファームウェアを含む）と、シスコまたは認定されたシスコのリセラーからお客様にライセンス許諾または提供された本ソフトウェアのアップグレード版、アップデート版、バグ修正版、または修正版（以下、総称して「アップグレード」）、またはバックアップ コピーが含まれ、本契約の条件が適用されるものとします。本契約の他の規定に関係なく、下記の条項が適用されます。（1）お客様が、かかる追加の複製物またはアップグレードの取得時に、オリジナルのソフトウェアの有効なライセンスを保持し、アップグレードまたは追加の複製物に対する妥当な料金を支払っている場合を除き、お客様にはいかなる追加の複製物またはアップグレードを使用するライセンスまたは権利もなく、（2）アップグレードの使用は、お客様が最初のエンド ユーザ購入者または賃借者であるか、またはアップグレードされるソフトウェアに対して有効なライセンスを保持しているシスコ機器に限定され、（3）追加の複製物の作成および使用は、必要なバックアップ用途のみに限定されます。

所有権の表示。お客様は、いかなる形式であれ、本ソフトウェアのすべての複製物について、あらゆる著作権およびその他の所有権の表示を、それらの著作権およびその他の所有権の表示が本ソフトウェアに含まれているのと同じ形式かつ方法で保持し、複製することに同意します。本契約で明示的に認可されている場合を除き、お客様は、シスコから事前に書面による許可を得ることなく、本ソフトウェアの複製物を作成しないものとします。

オープン ソース コンテンツ。お客様は、本ライセンス契約の添付書類、本ソフトウェアの README ファイル、または資料のいずれかに別途規定されたライセンスおよび著作権要件の下で、本ソフトウェアにはオープン ソースまたは公開されたコンテンツが含まれていることを認めるものとします。お客様は、かかる別途規定されたライセンスおよび著作権の要件に従うことに同意するものとします。

第三者受益。特定のシスコまたはシスコの関連サプライヤは、本契約の第三者受益対象です。本契約の条件は、シスコのサプライヤの利益のために明示的に規定され、法的強制力を持っています。ただし、これは当該代理店がお客様と契約関係にない場合です。シスコのサプライヤには下記が含まれますが、これに限定されません。（a）Hifn, Inc.（750 University Avenue, Los Gatos, California に本社を置くデラウェア法人）。（b）Wind River Systems, Inc. およびそのサプライヤ。お客様に提供される資料が今後更新される際に、サプライヤが追加される可能性があります。

期間および終了。本契約、および本契約内で許諾されているライセンスは、終了時に至るまで有効です。お客様は、本ソフトウェアと資料のすべての複製物を廃棄することにより、本契約およびライセンスをいつでも終了させることができます。本契約に基づくお客様のライセンス権利は、お客様が本契約のいずれかの規定に従わない場合、シスコからの通告なしに、ただちに終了します。お客様が本ソフトウェアをライセンス制限に違反して使用した場合には、シスコおよびそのサプライヤは、差し止めによる救済を受ける権利も有します。お客様は、本契約の終了時に、お客様が保有または管理する本ソフトウェアおよび資料のすべての複製物を廃棄する必要があります。お客様のあらゆる守秘義務、あらゆる責任制限、および保証の放棄と制限はすべて、本契約終了後も存続するものとします。さらに、「米国政府機関がエンド ユーザ購入者である場合」および「限定保証の記述とエンド ユーザ ライセンス契約に適用される一般条項」の各項の規定についても、本契約終了後も存続するものとします。

お客様の記録。お客様は、シスコとその独立会計士に対して、お客様の通常の営業時間中にお客様の帳簿、記録、財務諸表を査察し、本契約の条項に従っていることを確認する権利を認めるものとします。かかる査察において本契約に従っていないことが明らかになった場合は、お客様はただちにシスコに対して、妥当なライセンス料と査察に要した相応の経費を支払うものとします。

輸出。本ソフトウェアおよび資料は、技術データを含め、米国輸出管理法とその関連法規を含む米国輸出規制法の対象となります。また、他国の輸出入規制の対象になることがあります。お客様は、かかる規制のすべてを厳密に遵守することに同意し、また、本ソフトウェアおよび資料を輸出、再輸出、または輸入するためのライセンスを取得する責任があることを認めるものとします。お客様がかかる制限に従わない場合は、本契約に対する重大な違反と見なされます。

米国政府機関がエンド ユーザ購入者である場合。本ソフトウェアおよび資料は、Federal Acquisition Regulation（FAR; 連邦調達規則）（以下「FAR」）(48 C.F.R.) 2.101 で定義される「商用品目」に分類されます。これは、「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」で構成されます（当該用語は FAR 12.212 で使用されています）。FAR 12.212 および DoD FAR 補則 227.7202-1 ～ 227.7202-4 に一致している場合は、本エンド ユーザ ライセンス契約が含まれる契約にこれと異なるその他の FAR または契約条項があったとしても、お客様が政府機関のエンド ユーザに提供可能であり、本契約書が直接適用される場合に政府機関のエンド ユーザが入手するのは、本エンド ユーザ ライセンス契約で規定された権利のみが認められた本ソフトウェアおよび資料になります。ソフトウェアと資料のいずれか、または両方を使用することにより、政府機関は、本ソフトウェアと資料が「商用コンピュータ ソフトウェア」および「商用コンピュータ ソフトウェア関連資料」であることに同意し、この契約書に規定されている権利および制限に同意したことになります。

限定保証

Cisco 2100 シリーズ Wireless LAN Controller、Cisco 4400 シリーズ Wireless LAN Controller のハードウェア、および Cisco Wireless Services Modules。シスコシステムズ、または本製品を販売するシスコシステムズの関連子会社（以下「シスコ」）は、お客様への出荷日から（シスコのリセラーが販売した場合は、シスコが最初に出荷した日から 90 日以内から）90 日間に限り、通常の使用において本ハードウェアに材質上および製造上の欠陥がないことを保証します。シスコからの本製品の出荷日は、本製品出荷時の梱包材に記載されています。この限定保証は、本製品の最初のユーザに対してのみ適用されます。この限定保証に基づくお客様への唯一の救済として、シスコおよびサプライヤの全責任において、シスコまたはそのサービス センターによる、任意での保証期間内における交換品の出荷が行われます。交換品は、保証カードがある場合は記載された交換手順に従って出荷され、保証カードがない場合は、www.cisco.com/en/US/products/prod_warranties_listing.html に記載された方法で出荷されます。あるいは、お客様への本ハードウェアの提供者に本ハードウェアが返却される場合は、支払い済みの購入代金、運送料、および保険料が返金されます。ハードウェアの交換時に使用されるシスコの交換部品は、新しい部品あるいはそれと同等の部品です。本契約でのシスコの義務は、シスコまたはそのサービス センターにおけるその当時の最新の Return Material Authorization（RMA）手順に従って欠陥のあったハードウェアが返却されることが条件となります。

ソフトウェア。シスコは、お客様への出荷日から（認定されたシスコのリセラーが販売した場合は、シスコが最初に出荷した日から 90 日以内から）、（a）90 日後、または（b）本製品に保証カードが添付されておりソフトウェアの保証期間が記載されている場合はその保証期間、のいずれか長い方の期間内で、（a）通常の使用においては、本ソフトウェアの提供媒体に材質上および製造上の欠陥がないこと、および（b）本ソフトウェアが公示仕様に実質的に適合していること、を保証します。シスコからの本製品の出荷日は、本製品出荷時の梱包材に記載されています。上記の場合を除き、本ソフトウェアは「現状のまま」提供されます。この限定保証は、オリジナル ライセンスを付与されているお客様に対してのみ適用されます。この限定保証に基づくお客様への唯一の救済として、シスコとそのサプライヤ、およびライセンサの全責任において、シスコまたはお客様への本ソフトウェアの提供者に報告（あるいは、要求に応じて返却）があった場合に、シスコは本ソフトウェアの修理、交換、または返金を任意で行います。シスコは、本ソフトウェアにエラーが発生しないこと、またはお客様が本ソフトウェアを支障または障害なく使用できることを保証しません。また、日々新たな方法によるネットワークへの侵入や攻撃が試みられるため、シスコは本ソフトウェア、あるいは本ソフトウェアが使用される機器、システム、またはネットワークがかかる侵入または攻撃を受けないことを保証しません。

制約事項。本保証は、本ソフトウェア、本製品、または本ソフトウェアの使用が許可されているその他の機器が、（a）シスコまたはシスコにより認定された販売代理店以外で改変された場合、（b）シスコが提供する説明書に従ってインストール、運用、修理、または保守されなかった場合、（c）過剰な物理的または電気的負荷、誤使用、不注意、または事故による障害を受けた場合、または（d）シスコが購入代金やライセンス料を徴収しないベータ版、評価版、試験版、またはデモンストレーション版用としてライセンス供与されている場合、には適用されません。

保証の放棄

本保証に明記されている場合を除き、商品性、特定目的に対する適合性、非侵害、良好な品質、不干渉、情報内容の正確性に関する黙示保証 / 条項、または取引の過程、慣例、慣習、または取引慣行で発生する黙示保証 / 条項を含みこれらに限定されない、一切の明示または黙示の条項、表明、および保証は、適用される法で許可される範囲において除外され、シスコおよびそのサプライヤとライセンサによって明示的に放棄されます。除外されない黙示保証については、明示されている保証期間内に限られます。州または司法管轄区域によっては、黙示保証の有効期間を限定することが許可されていないため、お客様に上記の制限が適用されない場合があります。この保証はお客様に

特別な法的権利を付与するものであり、お客様は司法管轄区によって異なるその他の権利を有する場合もあります。この放棄と除外は、上記の明示の保証がその本来の目的を達成できない場合であっても適用されるものとします。

限定保証の説明およびエンド ユーザ ライセンス契約に適用される一般条項

責任の放棄。本契約に記載されている救済の本来の目的を達成不可能であったかどうかにかかわらず、シスコおよびそのサプライヤは、すべての収益および利益の損失、データの損失または損傷、業務の中断、資本の喪失、または特殊、間接的、派生的、偶発的、または懲罰的な損害に対して、損害発生の原因を問わず、かつ責任の根拠、あるいは本ソフトウェアの使用または本ソフトウェアが使用不可能なことが原因で発生したかどうかにかかわらず、シスコまたはその販売代理店、あるいはライセンサがかかる損害の可能性を通知されていた場合であっても、一切責任を負いません。シスコおよびそのサプライヤ、またはライセンサのお客様に対する責任は、契約の記載、不法行為（過失を含む）、保証の不履行その他の有無を問わず、クレームを生じた本ソフトウェアに対してお客様が支払った金額を超えないものとし、本ソフトウェアが別の製品に組み込まれている場合は、かかる別製品に支払った金額を超えないものとします。州または司法管轄区域によっては、結果的または偶発的な損害の制限または除外が許可されていないため、お客様に上記の制限が適用されない場合があります。

お客様は、お客様が本ソフトウェアまたはシスコが提供するその他の製品またはサービスを受け入れたかどうかにかかわらず、本契約に記載されている責任の制限および放棄が適用されることに同意するものとします。お客様は、シスコが本契約に記載されている保証の放棄および責任の制限をよりどころとして価格を設定し、本契約を結んでいること、同様のことが当事者間のリスク配分（契約上の救済における本来の目的を達成することができず、結果的に損害が生じるリスクを含む）に反映され、当事者間での取引の基本を成すことを認め、これに同意するものとします。

保証およびエンド ユーザ ライセンス契約は、法規または法的原則の選択を参照または適用することなく、カリフォルニア州の法律に準拠し、これによって解釈されます。国際物品売買契約に関する国連条約は適用されないものとします。本契約の一部が無効または施行不能になったとわかった場合も、本契約における他の条項は完全に効力を保持するものとします。本契約に明記されている場合を除き、本契約は、本ソフトウェアおよび資料のライセンスに関する当事者間の完全な合意を成すものとし、発注書等に相反する条件または追加条項が含まれている場合は、それらの条件はすべて除外され、本契約が優先されます。本契約は英語で記述されており、当事者は英語版に適用されることに同意するものとします。特定の国において適用される保証またはライセンス条件と、上記情報の翻訳については、Cisco Legal Department（300 E. Tasman Drive, San Jose, California 95134）にお問い合せください。

表示

次の表示は、本ソフトウェア ライセンスに関するものです。

OpenSSL/OpenSSL プロジェクト

この製品には、OpenSSL ツールキットで使用される OpenSSL プロジェクト（http://www.openssl.org/）によって開発されたソフトウェアが含まれています。

本製品には、Eric Young（eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれます。

本製品には、Tim Hudson（tjh@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれます。

ライセンスについて

OpenSSL ツールキットはデュアル ライセンス下にあります。つまり、OpenSSL ライセンスと元の SSLeay ライセンスの両方の条件がこのツールキットには適用されます。実際のライセンスに関する記述は、以下を参照してください。両方のライセンスは、実際的には BSD スタイルのオープン ソース ライセンスです。OpenSSL のライセンスに関しては、openssl-core@openssl.org にお問い合わせください。

OpenSSL ライセンス：

Copyright 1998-2007 The OpenSSL Project. All rights reserved.

ソースコード形式であれバイナリ形式であれ、変更の有無に関わらず、以下の条件を満たす限りにおいて、再配布および使用を許可します。

1. ソース コード形式で再配布する場合、上記の著作権表示、本条件書、および下記の免責事項を記載する必要があります。
2. バイナリ形式で再配布する場合、上記の著作権表示、本条件書、および下記の免責事項を、配布物とともに提供される文書とその他の資料のいずれかまたは両方に記載する必要があります。
3. 本ソフトウェアの機能または使用について言及しているすべての広告資料には、次の通知を表示する必要があります。「この製品には、OpenSSL ツールキットにおける使用のため、OpenSSL プロジェクト（http://www.openssl.org/）によって開発されたソフトウェアが含まれています。」
4. 「OpenSSL Toolkit」および「OpenSSL Project」の名前は、事前の書面による許可なしに、本ソフトウェアから派生した製品を推奨または宣伝するために使用することはできません。書面による許可については openssl-core@openssl.org にお問い合わせください。
5. 本ソフトウェアから派生した製品には、事前の書面による許可なしに、「OpenSSL」という名称を使用したり、また製品名に「OpenSSL」を含めたりすることはできません。
6. いかなる形式の再配布にも次の通知を含める必要があります。

   「この製品には、OpenSSL　ツールキットにおける使用のため、OpenSSL　プロジェクト（http://www.openssl.org/）によって開発されたソフトウェアが含まれています。」

本ソフトウェアは、OpenSSL PROJECT によって「現状のまま」提供され、一切の明示または黙示の保証（商品性の黙示保証および特定目的に対する適合性を含むがこれに限定されない）は放棄されます。OpenSSL プロジェクトもまたはその寄与者も、本ソフトウェアの使用から生じた直接的、間接的、偶発的、特殊、懲罰的、または派生的な損害（代替品または代替サービスの調達、使用機会、データ、または利益の損失、あるいは業務の中断を含むがこれに限定されない）について、損害発生の原因を問わず、かつ責任の根拠が契約であるか厳格責任であるか、不法行為（過失等を含む）であるかを問わず、かかる損害の可能性を通知されていた場合であっても、一切責任を負いません。

本製品には、Eric Young （eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれます。本製品には、Tim Hudson （tjh@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれます。

元の SSLeay ライセンス：

Copyright 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

本パッケージは、Eric Young （eay@cryptsoft.com）によって作成された SSL 実装です。

実装は、Netscapes SSL に適合するように作成されました。

このライブラリは商用および非商用の使用に対して無料ですが、次の条件を順守する必要があります。次の条件は、この配布に見られるすべてのコード、SSL コードだけでなく、RC4、RSA、lhash、DES などのコードにも適用されます。この配布に含まれている SSL 文書は、所有者が Tim Hudson （tjh@cryptsoft.com）である場合を除き、同じ著作権条項による適用を受けます。

著作権は Eric Young にあるため、コードの著作権表示を削除することはできません。このパッケージが製品で使用される場合は、使用されるライブラリは作成者である Eric Young に帰属を与える必要があります。帰属については、プログラムの起動時のテキスト メッセージまたはパッケージに同梱の文書（オンラインまたはテキスト）で表すことができます。

ソースコード形式であれバイナリ形式であれ、変更の有無に関わらず、以下の条件を満たす限りにおいて、再配布および使用を許可します。

1. ソース コード形式で再配布する場合、上記の著作権表示、本条件書、および下記の免責事項を記載する必要があります。
2. バイナリ形式で再配布する場合、上記の著作権表示、本条件書、および下記の免責事項を、配布物とともに提供される文書とその他の資料のいずれかまたは両方に記載する必要があります。
3. 本ソフトウェアの機能または使用について言及しているすべての広告資料には、次の通知を表示する必要があります。

   本製品には、Eric Young （eay@cryptsoft.com）によって作成された暗号化ソフトウェアが含まれます。

   ライブラリから使用されるルーチンが暗号化に関連しない場合、「暗号化」という言葉は省略できます。
4. Windows に特定のコード（またはその派生）を apps のディレクトリ（アプリケーション コード）から含める場合、次の通知を明示する必要があります。「この製品には Tim Hudson （tjh@cryptsoft.com）によって作成されたソフトウェアが含まれます。」

本ソフトウェアは Eric Young によって「現状のまま」提供され、一切の明示または黙示の保証（商品性の黙示保証および特定目的に対する適合性を含むがこれに限定されない）は放棄されます。作成者もまたはその寄与者も、本ソフトウェアの使用から生じた直接的、間接的、偶発的、特殊、懲罰的、または派生的な損害（代替品または代替サービスの調達、使用機会、データ、または利益の損失、あるいは業務の中断を含むがこれに限定されない）について、損害発生の原因を問わず、かつ責任の根拠が契約であるか厳格責任であるか、不法行為（過失等を含む）であるかを問わず、かかる損害の可能性を通知されていた場合であっても、一切責任を負いません。

このコードの公開バージョンまたは派生バージョンにおいて、ライセンスおよび配布条件を変更することはできません。つまり、このコードを別の配布ライセンス（GNU パブリック ライセンスを含む）下にコピーして配置することはできません。

APPENDIX D

トラブルシューティング

この付録では、Cisco Unified Wireless Network Solution インターフェイスに表示されるシステム メッセージのリストと、コントローラと Lightweight アクセス ポイントの LED パターンに関する情報を示し、コントローラのトラブルシューティングに使用できる CLI コマンドについて説明します。この章の内容は、次のとおりです。

LED の解釈

コントローラの LED の解釈

LED パターンの情報については、特定のコントローラのクイック スタート ガイドを参照してください。これらのガイドには、次の URL からアクセスできます。

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

Lightweight アクセス ポイント LED の解釈

LED パターンの情報については、特定のアクセス ポイントのハードウェア インストレーション ガイドを参照してください。これらのガイドには、次の URL からアクセスできます。

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

システム メッセージ

表 D-1 は、一般的なシステム メッセージとその説明の一覧です。システム メッセージの一覧は、『Cisco Wireless LAN Controller System Message Guide, Release 5.0』を参照してください。

表 D-1　システム メッセージとその説明

エラー メッセージ	説明
apf_utils.c 680:Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	クライアントは保護ビットが 0 に設定された、セキュリティが有効になっている WLAN 上でアソシエーション要求を送信しています（アソシエーション要求の Capability フィールドで）。設計されたとおりに、コントローラはアソシエーション要求を却下し、クライアントにはアソシエーション エラーが表示されます。
dtl_arp.c 480:Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	コントローラの Network Processing Unit（NPU）はタイムアウト メッセージを CPU に送信し、特定のクライアントがタイムアウトまたは期限切れであることを知らせます。これは通常、CPU が内部データベースから無線クライアントを削除したことを NPU に通知していない場合に起こります。クライアントは NPU データベースにとどまるため、ネットワーク プロセッサで期限切れになり、CPU に通知されます。CPU はデータベースにないクライアントを検出して、このメッセージを送信します。
STATION_DISASSOCIATE	クライアントが使用を意図的に中断したか、サービスの中断を受けた可能性があります。
STATION_DEAUTHENTICATE	クライアントが使用を意図的に中断したか、認証上の問題があることを示しています。
STATION_AUTHENTICATION_FAIL	設定の有効性、キーの不一致、またはその他の問題を確認します。
STATION_ASSOCIATE_FAIL	Cisco Radio 上の負荷または信号の品質に問題がないか確認します。
LRAD_ASSOCIATED	アソシエートされた Lightweight アクセス ポイントがこのコントローラで管理されるようになりました。
LRAD_DISASSOCIATED	Lightweight アクセス ポイントが他のコントローラにアソシエートされているか、完全に接続不可能になっている可能性があります。
LRAD_UP	Lightweight アクセス ポイントは正常に動作しています。処理は必要ありません。
LRAD_DOWN	Lightweight アクセス ポイントに問題があるか、管理上無効にされています。
LRADIF_UP	Cisco Radio は稼働状態です。
LRADIF_DOWN	Cisco Radio に問題があるか、管理上無効にされています。
LRADIF_LOAD_PROFILE_FAILED	クライアント密度がシステムのキャパシティを超えている可能性があります。
LRADIF_NOISE_PROFILE_FAILED	802.11 以外のノイズが設定しきい値を超えました。
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 干渉がチャネル上のしきい値を超えました。チャネルの割り当てを確認してください。

表 D-1　システム メッセージとその説明（続き）

エラー メッセージ	説明
LRADIF_COVERAGE_PROFILE_FAILED	カバレッジ ホールの可能性が検出されました。Lightweight アクセス ポイント履歴を調べて、一般的な問題がないかどうかを確認し、必要に応じて Lightweight アクセス ポイントを追加してください。
LRADIF_LOAD_PROFILE_PASSED	負荷がしきい値の制限内に戻りました。
LRADIF_NOISE_PROFILE_PASSED	検出されたノイズがしきい値より小さくなりました。
LRADIF_INTERFERENCE_PROFILE_PASSED	検出された干渉がしきい値より小さくなりました。
LRADIF_COVERAGE_PROFILE_PASSED	不良電波を受信しているクライアント数はしきい値内です。
LRADIF_CURRENT_TXPOWER_CHANGED	情報メッセージです。
LRADIF_CURRENT_CHANNEL_CHANGED	情報メッセージです。
LRADIF_RTS_THRESHOLD_CHANGED	情報メッセージです。
LRADIF_ED_THRESHOLD_CHANGED	情報メッセージです。
LRADIF_FRAGMENTATION_THRESHOLD_ CHANGED	情報メッセージです。
RRM_DOT11_A_GROUPING_DONE	情報メッセージです。
RRM_DOT11_B_GROUPING_DONE	情報メッセージです。
ROGUE_AP_DETECTED	セキュリティ上の問題がある可能性があります。マップと傾向を使用して調べてください。
ROGUE_AP_REMOVED	不正なアクセス ポイントのタイムアウトが検出されました。ユニットがシャットダウンしたか、カバレッジ領域外に移動しました。
AP_MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセス ポイント数がシステムのしきい値を超えました。
LINK_UP	肯定的な確認メッセージです。
LINK_DOWN	ポートに問題があるか、管理上無効にされています。
LINK_FAILURE	ポートに問題があるか、管理上無効にされています。
AUTHENTICATION_FAILURE	セキュリティ違反の試行が検出されました。調査してください。
STP_NEWROOT	情報メッセージです。
STP_TOPOLOGY_CHANGE	情報メッセージです。
IPSEC_ESP_AUTH_FAILURE	WLAN IPSec の設定を確認してください。
IPSEC_ESP_REPLAY_FAILURE	IP アドレスのスプーフィング試行がないかどうか確認してください。
IPSEC_ESP_POLICY_FAILURE	WLAN とクライアントの間で IPSec 設定が矛盾していないかどうか確認してください。
IPSEC_ESP_INVALID_SPI	情報メッセージです。
IPSEC_OTHER_POLICY_FAILURE	WLAN とクライアントの間で IPSec 設定が矛盾していないかどうか確認してください。
IPSEC_IKE_NEG_FAILURE	WLAN とクライアントの間で IPSec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_SUITE_NEG_FAILURE	WLAN とクライアントの間で IPSec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_INVALID_COOKIE	情報メッセージです。

表 D-1　システム メッセージとその説明（続き）

エラー メッセージ	説明
RADIOS_EXCEEDED	サポートされている Cisco Radio の最大数を超えました。同じレイヤ 2ネットワークでコントローラの障害を調べるか、別のコントローラを追加してください。
SENSED_TEMPERATURE_HIGH	ファン、空調、その他の冷却装置を確認してください。
SENSED_TEMPERATURE_LOW	室温が低くないか、低温の原因が他にないかどうかを調べてください。
TEMPERATURE_SENSOR_FAILURE	温度センサーを至急交換してください。
TEMPERATURE_SENSOR_CLEAR	温度センサーは正常に動作しています。
POE_CONTROLLER_FAILURE	ポートを確認してください。深刻な障害が検出されました。
MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセス ポイント数がシステムのしきい値を超えました。
SWITCH_UP	コントローラは SNMP のポーリングに応答しています。
SWITCH_DOWN	コントローラは SNMP のポーリングに応答していません。コントローラと SNMP の設定を確認してください。
RADIUS_SERVERS_FAILED	RADIUS とコントローラの間のネットワーク接続を確認してください。
CONFIG_SAVED	実行中の設定はフラッシュに保存されました。設定はリブート後にアクティブになります。
MULTIPLE_USERS	同じユーザ名の別のユーザがログインしています。
FAN_FAILURE	コントローラの温度を監視して、オーバーヒートしないようにしてください。
POWER_SUPPLY_CHANGE	電源が故障していないか確認してください。
COLD_START	コントローラはリブートされた可能性があります。
WARM_START	コントローラはリブートされた可能性があります。

CLI を使用したトラブルシューティング

お使いのコントローラで問題が発生した場合には、この項のコマンドを使用して情報を収集し、問題をデバッグすることができます。

1. **show process cpu**：システム内で各タスクが使用している CPU の現状を表示します。このコマンドは、タスクの中に CPU を独占して別のタスクの実行を妨げているものがないかどうか調べる際に役立ちます。

   次のような情報が表示されます。

```
Name                Priority      CPU Use     Reaper
 reaperWatcher       ( 3/124)     0 %       (  0/  0)%   I
 osapiReaper          (10/121)    0 %       (  0/  0)%   I
 TempStatus          (255/  1)    0 %      (  0/  0)%   I
 emWeb               (255/  1)    0 %     (  0/  0)%   T 300
 cliWebTask          (255/  1)    0 %     (  0/  0)%   I
 UtilTask            (255/  1)    0 %      (  0/  0)%   T 300
```

   上の例のフィールドの説明は、次のとおりです。

   - Name フィールドは、CPU が実行対象としているタスクです。
   - Priority フィールドは、次の 2 種類の値を示しています。1）実際のファンクション コールから生成されたタスクの最初の優先順位。2）システムの各優先順位で割ったタスクの優先順位。
   - CPU Use フィールドは、それぞれのタスクの CPU 利用率です。
   - Reaper フィールドは、次の 3 種類の値を示しています。1）ユーザ モードの操作でそのタスクが予定されている所要時間。2）システム モードの操作でそのタスクが予定されている所要時間。3）そのタスクが Reaper タスク モニタで監視されているかどうか（監視されている場合は「T」で表示）。タスクが Reaper タスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。

   （注） CPU 総利用率を % で表示するには、**show cpu** コマンドを入力してください。

2. **show process memory**：システム内で各プロセスが割り当てているメモリと、割り当て解除されているメモリの現状を表示します。

   次のような情報が表示されます。

```
Name                Priority     BytesInUse  BlocksInUse  Reaper
 reaperWatcher       ( 3/124)     0           0         (  0/  0)%   I
 osapiReaper          (10/121)    0        0 (  0/  0)%   I
 TempStatus          (255/  1)    308         1         (  0/  0)%   I
 emWeb               (255/  1)    294440       4910   (  0/  0)%  T 300
 cliWebTask          (255/  1)    738         2 (  0/  0)%   I
 UtilTask            (255/  1)    308         1 (  0/  0)%  T 300
```

   上の例のフィールドの説明は、次のとおりです。

   - Name フィールドは、CPU が実行対象としているタスクです。
   - Priority フィールドは、次の 2 種類の値を示しています。1）実際のファンクション コールから生成されたタスクの最初の優先順位。2）システムの各優先順位で割ったタスクの優先順位。
   - BytesInUse フィールドは、ダイナミック メモリの割り当てでそのタスクに使用される実際のバイト数です。
   - BlocksInUse フィールドは、そのタスクを実行する際に割り当てられる連続メモリです。

- Reaper フィールドは、次の 3 種類の値を示しています。1）ユーザ モードの操作でそのタスクが予定されている所要時間。2）システム モードの操作でそのタスクが予定されている所要時間。3）そのタスクが Reaper タスク モニタで監視されているかどうか（監視されている場合は「T」で表示）。タスクが Reaper タスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。

3. **show tech-support**：現在の設定内容、最新のクラッシュ ファイル、CPU 利用率、メモリ利用率など、システムの状態についての一連の情報を表示します。

4. **show running-config**：コントローラの現在の設定内容がすべて表示されます。アクセス ポイントの設定は表示されません。このコマンドで表示されるのは、ユーザが設定した値だけです。システムから設定されたデフォルト値は表示されません。このコマンドは **show run-config** コマンドとは違い、現在の設定内容の一部と多数のダイナミック情報を出力しません。その代わり **show running-config** コマンドでは、コントローラの設定内容をコマンド形式の平文で出力します。

   以下は、その出力例です。

```
radius auth add 1 10.50.3.104 1812 ascii ****


radius backward compatibility enable

radius admin-authentication disable

radius cred-cache enable

radius callStationIdType macAddr


radius acct retransmit-timeout 1 4

radius acct network 1 disable

radius auth rfc3576 enable 1

radius auth retransmit-timeout 1 6

radius auth network 1 disable

radius auth management 1 disable

radius auth ipsec enable
```

（注） 平文でパスワードを表示するには、**config passwd-cleartext enable** と入力してください。このコマンドを実行するには、管理者のパスワードを入力する必要があります。このコマンドは、このセッションに限り有効です。リブート後は、保存されません。

（注） このコマンドの出力をアップロードする際に、TFTP　は使用できません。この出力は、必要に応じてカット & ペーストしてください。

システム ロギングとメッセージ ロギングの設定

システム ロギングを使用すると、コントローラのシステム イベントを最大 3 台のリモート syslog サーバにログできるようになります。syslog メッセージはコントローラに設定されている syslog サーバごとにログされるため、コントローラは各 syslog メッセージのコピーを送信します。複数のサーバに syslog メッセージを送信できるため、1 台の syslog サーバが一時的に使用できなくなってもメッセージが失われることがありません。メッセージ ロギングを使用すると、システム メッセージをコントローラのバッファまたはコンソールにログできるようになります。

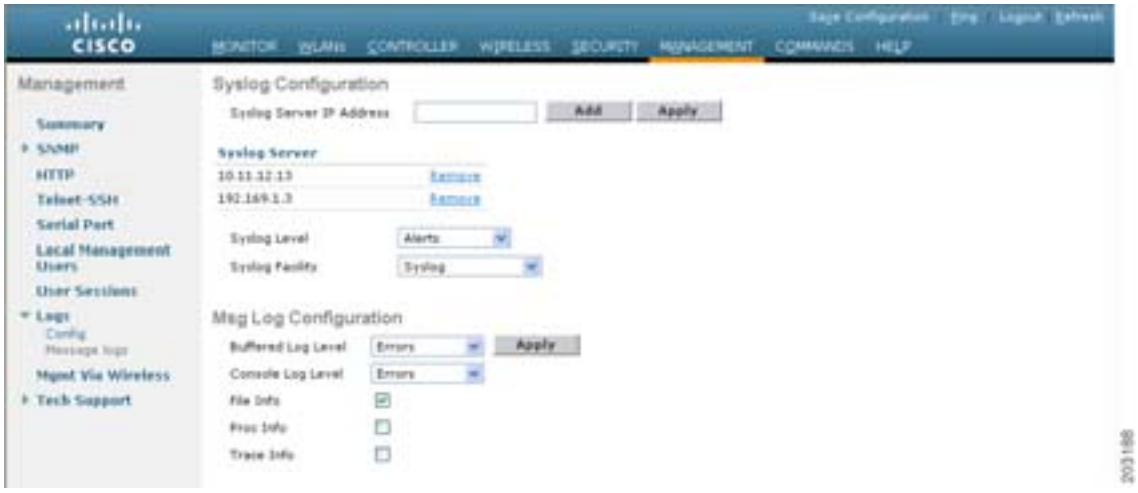
システム ロギングとメッセージ ロギングを設定するには、コントローラ GUI または CLI を使用します。

GUI を使用したシステム ロギングとメッセージ ロギングの設定

GUI を使用してシステム ロギングとメッセージ ロギングを設定する手順は、次のとおりです。

ステップ 1　**Management** > **Logs** > **Config** の順にクリックします。Syslog Configuration ページが表示されます（図 D-1 を参照）。

図 D-1　Syslog Configuration ページ



ステップ 2　Syslog Server IP Address フィールドに、syslog メッセージの送信先となるサーバの IP アドレスを入力し、**Add** をクリックします。コントローラには最大 3 台の syslog サーバを追加できます。このフィールドの下には、すでにコントローラに追加されている syslog サーバのリストが表示されます。

（注）　コントローラから syslog サーバを削除するには、目的のサーバの右側の **Remove** をクリックします。

ステップ 3　syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、Syslog Level ドロップダウン ボックスから次のいずれかのオプションを選択します。

- **Emergencies** = 重大度レベル 0
- **Alerts** = 重大度レベル 1（デフォルト値）
- **Critical** = 重大度レベル 2
- **Errors** = 重大度レベル 3
- **Warnings** = 重大度レベル 4
- **Notifications** = 重大度レベル 5
- **Informational** = 重大度レベル 6
- **Debugging** = 重大度レベル 7

syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

ステップ 4　syslog サーバに送信する syslog メッセージのファシリティを設定するには、Syslog Facility ドロップダウン ボックスから次のいずれかのオプションを選択します。

- **Kernel** = ファシリティ レベル 0
- **User Process** = ファシリティ レベル 1
- **Mail** = ファシリティ レベル 2
- **System Daemons** = ファシリティ レベル 3
- **Authorization** = ファシリティ レベル 4
- **Syslog** = ファシリティ レベル 5（デフォルト値）
- **Line Printer** = ファシリティ レベル 6
- **USENET** = ファシリティ レベル 7
- **Unix-to-Unix Copy** = ファシリティ レベル 8
- **Cron** = ファシリティ レベル 9
- **FTP Daemon** = ファシリティ レベル 11
- **System Use 1** = ファシリティ レベル 12
- **System Use 2** = ファシリティ レベル 13
- **System Use 3** = ファシリティ レベル 14
- **System Use 4** = ファシリティ レベル 15
- **Local Use 0** = ファシリティ レベル 16
- **Local Use 1** = ファシリティ レベル 17
- **Local Use 2** = ファシリティ レベル 18
- **Local Use 3** = ファシリティ レベル 19
- **Local Use 4** = ファシリティ レベル 20
- **Local Use 5** = ファシリティ レベル 21
- **Local Use 6** = ファシリティ レベル 22
- **Local Use 7** = ファシリティ レベル 23

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　コントローラのバッファとコンソールに対するロギング　メッセージの重大度レベルを設定するには、Buffered Log Level および Console Log Level ドロップダウン リストから次のいずれかのオプションを選択します。

- **Emergencies** = 重大度レベル 0

- **Alerts** = 重大度レベル 1
- **Critical** = 重大度レベル 2
- **Errors** = 重大度レベル 3（デフォルト値）
- **Warnings** = 重大度レベル 4
- **Notifications** = 重大度レベル 5
- **Informational** = 重大度レベル 6
- **Debugging** = 重大度レベル 7

ロギング レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 7　ソース ファイルの情報をメッセージ ログに含める場合は、**File Info** チェック ボックスをオンにします。デフォルト値は有効（enable）です。

ステップ 8　プロセス情報をメッセージ ログに含める場合は、**Proc Info** チェック ボックスをオンにします。デフォルト値は無効（disable）です。

ステップ 9　トレースバック情報をメッセージ ログに含める場合は、**Trace Info** チェック ボックスをオンにします。デフォルト値は無効（disable）です。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更を保存します。

GUI を使用したメッセージ ログの表示

コントローラの GUI を使用してメッセージ ログを表示するには、**Management** > **Logs** > **Message Logs** の順にクリックします。Message Logs ページが表示されます（図 D-2 を参照）。

図 D-2　Message Logs ページ

（注）　コントローラから現在のメッセージ ログをクリアするには、**Clear** をクリックします。

CLI を使用したシステム ロギングとメッセージ ロギングの設定

CLI を使用してシステム ロギングとメッセージ ロギングを設定する手順は、次のとおりです。

ステップ 1　システム ロギングを有効化し、syslog メッセージの宛先 syslog サーバの IP アドレスを設定するには、次のコマンドを入力します。

config logging syslog host *server_IP_address*

コントローラには最大 3 台の syslog サーバを追加できます。

（注）　コントローラから syslog サーバを削除するには、次のコマンドを入力します。
config logging syslog host *server_IP_address* **delete**

ステップ 2　syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、次のコマンドを入力します。

config logging syslog level *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注）　代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注）　syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

ステップ 3　syslog サーバへ発信する syslog メッセージのファシリティを設定するには、次のコマンドを入力します。

config logging syslog facility *facility_code*

facility_code は、次のいずれかです。

- authorization = 認可システム。ファシリティ レベル = 4。
- auth-private = 認可システム（プライベート）。ファシリティ レベル = 10。
- cron = cron/at ファシリティ。ファシリティ レベル = 9。
- daemon = システム デーモン。ファシリティ レベル = 3。
- ftp = FTP デーモン。ファシリティ レベル = 11。
- kern = カーネル。ファシリティ レベル = 0。
- local0 = ローカル使用。ファシリティ レベル = 16。
- local1 = ローカル使用。ファシリティ レベル = 17。
- local2 = ローカル使用。ファシリティ レベル = 18。
- local3 = ローカル使用。ファシリティ レベル = 19。
- local4 = ローカル使用。ファシリティ レベル = 20。
- local5 = ローカル使用。ファシリティ レベル = 21。
- local6 = ローカル使用。ファシリティ レベル = 22。
- local7 = ローカル使用。ファシリティ レベル = 23。
- lpr = ライン プリンタ システム。ファシリティ レベル = 6。
- mail = メール システム。ファシリティ レベル = 2。
- news = USENET ニュース。ファシリティ レベル = 7。
- sys12 = システム使用。ファシリティ レベル = 12。
- sys13 = システム使用。ファシリティ レベル = 13。
- sys14 = システム使用。ファシリティ レベル = 14。
- sys15 = システム使用。ファシリティ レベル = 15。
- syslog = syslog 自体。ファシリティ レベル = 5。
- user = ユーザ プロセス。ファシリティ レベル = 1。
- uucp = UNIX 間コピー システム。ファシリティ レベル = 8。

ステップ 4　コントローラのバッファとコンソールに対するロギング　メッセージの重大度レベルを設定するには、次のコマンドを入力します。

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注） 代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注） ロギング　レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 5　コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging fileinfo {**enable** | **disable**}

デフォルト値は有効（enable）です。

ステップ 6　コントローラがメッセージ ログ内にプロセス情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging procinfo {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 7　コントローラがメッセージ ログ内にトレースバック情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging traceinfo {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 8　メッセージ ログのタイムスタンプを有効または無効にするには、次のコマンドを入力します。

config service timestamps log {**datetime** | **uptime** | **disable**}

このとき、次のようになります。

- **datetime** = メッセージ ログは、標準の日付と時刻でタイムスタンプされます。
- **uptime** = メッセージ ログは、コントローラが最後にリセットされてからの時間でタイムスタンプされます。
- **disable** = メッセージ ログはタイムスタンプされません。

ステップ 9　変更を保存するには、次のコマンドを入力します。

save config

CLI を使用したシステム ログとメッセージ ログの表示

ロギング パラメータとバッファの内容を表示するには、次のコマンドを入力します。

show logging

次のような情報が表示されます。

```
Logging to buffer :
- Logging filter level..................................... errors
- Number of lines logged.................................... 1000
- Number of lines dropped................................... 2752
Logging to console :
- Logging filter level..................................... errors
- Number of lines logged.................................... 0
- Number of lines dropped................................... 3752
Logging to syslog :
- Logging filter level..................................... alerts
- Syslog facility........................................... syslog
- Number of lines logged.................................... 0
- Number of lines dropped................................... 3752
- Number of remote syslog hosts............................. 2
  - Host 0................................................. 10.11.12.1
  - Host 1................................................. 192.169.1.3
  - Host 2................................................. Not Configured
Logging of traceback....................................... Enabled
- Traceback logging level.................................. debugging
Logging of process information............................. Enabled
Logging of source file informational....................... Enabled
Timestamping of messages................................... Enabled
- Timestamp format......................................... Date and Time

Logging buffer (1000 logged, 2752 dropped)

Nov 14 13:27:32.308 mm_listen.c:5246 MM-3-INVALID_PKT_RECVD: Received an invalid
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.
Nov 14 13:27:21.204 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding join request
from AP 00:13:19:31:9c:e0
Nov 14 13:27:21.203 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free public key for
AP 00:13:19:31:9c:e0
Nov 14 13:27:21.203 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request does not
contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Nov 14 13:27:16.189 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding join request
from AP 00:13:19:31:9c:e0
Nov 14 13:27:16.189 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free public key for
AP 00:13:19:31:9c:e0
Nov 14 13:27:16.188 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request does not
contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Previous message occurred 2 times.
Nov 14 13:27:03.659 mm_listen.c:5246 MM-3-INVALID_PKT_RECVD: Received an invalid
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.
...
```

CCXv5 クライアント デバイスのトラブルシューティング

コントローラでは、CCXv5 クライアントとの通信に関する問題のトラブルシューティングのために設計された 3 つの機能がサポートされています。診断チャネル、クライアント レポート、およびローミング診断とリアルタイム診断です。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

（注）　これらの機能は、CCXv5 クライアントでのみサポートされています。CCX 以外のクライアントでの使用や、以前のバージョンの CCX を実行するクライアントでの使用はサポートされていません。

診断チャネル

診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。クライアントに発生している通信の問題の原因を特定するために、定義済みのテストのセットを使用してクライアントとアクセス ポイントをテストし、その後、ネットワーク上でクライアントを動作させるための修正措置を行うことができます。診断チャネルを有効にするには、コントローラの GUI や CLI を使用します。また、診断テストを実行するには、コントローラの CLI や WCS を使用します。

クライアント レポート

クライアント レポート プロトコルは、クライアント情報を交換するためにクライアントとアクセス ポイントによって使用されます。クライアント レポートは、クライアントがアソシエートするときに自動で収集されます。クライアント のアソシエート後は、いつでもコントローラの GUI や CLI を使用してクライアント レポート要求を任意の CCXv5 クライアントに送信できます。クライアント レポートには次の 4 種類があります。

- Client profile：クライアントの設定に関する情報を示します。
- Operating parameters：クライアントの現在の動作モードの詳細を示します。
- Manufacturers information：使用している無線 LAN クライアント アダプタに関するデータを示します。
- Client capabilities：クライアントの機能に関する情報を示します。

ローミング診断とリアルタイム診断

ローミング ログとリアルタイム ログ、および統計を使用して、システムの問題を解決できます。イベント ログにより、クライアント デバイスの動作を識別および追跡できるようになります。これは、WLAN 上に存在する可能性がある問題を診断する際に特に役立ちます。イベント ログはイベントのログを示し、アクセス ポイントへそれらをレポートします。イベント ログには次の 3 つのカテゴリがあります。

- Roaming ログ：このログは、指定されたクライアントのローミング イベントの履歴を示します。クライアントは、ローミングの失敗や成功などの直近のローミング イベントを最低 5 つ以上保持します。
- Robust Security Network Association（RSNA; ロバスト セキュリティ ネットワーク アソシエーション）ログ：このログは、指定されたクライアントの認証イベントの履歴を示します。クライアントは、失敗や成功などの直近の認証イベントを最低 5 つ以上保持します。
- Syslog：このログは、クライアントの内部システム情報を示します。たとえば、802.11 の動作、システムの動作などに関する問題を示します。

統計レポートは、クライアントの 802.1X とセキュリティの情報を示します。クライアント のアソシエート後は、いつでもコントローラの CLI を使用してイベント ログおよび統計の要求を任意の CCXv5 クライアントに送信できます。

GUI を使用した診断チャネルの設定

コントローラの GUI を使用して診断チャネルを設定する手順は、次のとおりです。

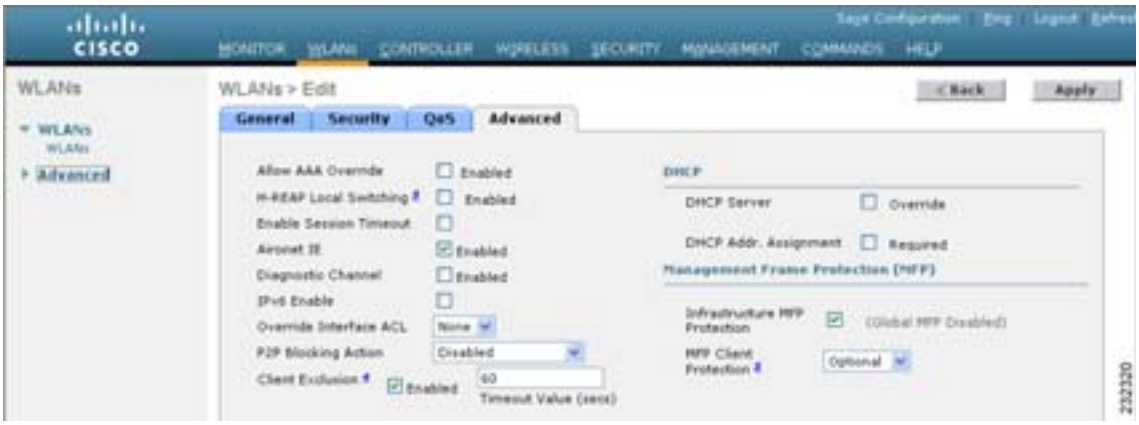
ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　新しい WLAN を作成するか、既存の WLAN のプロファイル名をクリックします。

（注）　診断テストを実行するための新しい WLAN を作成することをお勧めします。

ステップ 3　WLANs > Edit ページが表示されたら、**Advanced** タブをクリックして WLANs > Edit（Advanced）ページを開きます（図 D-3 を参照）。

図 D-3　WLANs > Edit（Advanced）ページ



ステップ 4　この WLAN 上で診断チャネルでのトラブルシューティングを有効にする場合は、**Diagnostic Channel** チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。

（注）　クライアント上で診断テストを開始するには、CLI を使用します。詳細は、「CLI を使用した診断チャネルの設定」の項（P. D-16）を参照してください。

ステップ 5　**Apply** をクリックして、変更を適用します。

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

CLI を使用した診断チャネルの設定

コントローラの CLI を使用して診断チャネルを設定する手順は、次のとおりです。

ステップ 1　特定の WLAN 上で診断チャネルでのトラブルシューティングを有効にするには、次のコマンドを入力します。

config wlan diag-channel {**enable** | **disable**} *wlan_id*

ステップ 2　変更されたかどうかを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. Infinity
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Enabled
...
```

ステップ 3　DHCP テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dhcp-test *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 4　デフォルト ゲートウェイの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx default-gw-ping *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 5　DNS サーバの IP アドレスの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dns-ping *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 6　DNS 名前解決テストを特定のホスト名に対して実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dns-resolve *client_mac_address host_name*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 7　アソシエーション テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-association *client_mac_address ssid bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

ステップ 8　802.1X テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-dot1x *client_mac_address profile_id bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

ステップ 9　プロファイルのリダイレクト テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-profile *client_mac_address profile_id*

profile_id は、クライアント レポートが有効になっているクライアント プロファイルのものでなければなりません。

（注）　ユーザは親の WLAN へリダイレクトされます。他のプロファイルへはリダイレクトされません。表示されるプロファイルは、ユーザの親のプロファイルのみとなります。ただし、親 WLAN のプロファイルには、診断する子 WLAN を 1 つ持つことができます。

ステップ 10　テストを中断またはクリアする必要がある場合は、次のコマンドを使用します。

- 現在のテストを中断する要求をクライアントに送信するには、次のコマンドを入力します。
  config client ccx test-abort *client_mac_address*
  保留にできるテストは一度に 1 つだけのため、このコマンドは現在保留中のテストを中断します。
- コントローラ上のテスト結果をクリアするには、次のコマンドを入力します。
  config client ccx clear-results *client_mac_address*

ステップ 11 クライアントにメッセージを送信するには、次のコマンドを入力します。

config client ccx send-message *client_mac_address message_id*

message_id は、次のいずれかです。

- 1 = SSID が無効です。
- 2 = ネットワーク設定が無効です。
- 3 = WLAN の信頼性に矛盾があります。
- 4 = ユーザの資格情報が正しくありません。
- 5 = サポートに問い合わせてください。
- 6 = 問題は解決されました。
- 7 = 問題は解決されていません。
- 8 = 後でもう一度試してください。
- 9 = 示された問題を修正してください。
- 10 = ネットワークによってトラブルシューティングが拒否されました。
- 11 = クライアント レポートを取得しています。
- 12 = クライアント ログを取得しています。
- 13 = 取得が完了しました。
- 14 = アソシエーション テストを開始しています。
- 15 = DHCP テストを開始しています。
- 16 = ネットワーク接続テストを開始しています。
- 17 = DNS ping テストを開始しています。
- 18 = 名前解決テストを開始しています。
- 19 = 802.1X 認証テストを開始しています。
- 20 = クライアントを特定のプロファイルへリダイレクトしています。
- 21 = テストが完了しました。
- 22 = テストに合格しました。
- 23 = テストに合格しませんでした。
- 24 = 診断チャネル動作をキャンセルするか WLAN プロファイルを選択して通常の動作を再開します。
- 25 = クライアントによってログの取得が拒否されました。
- 26 = クライアントによってクライアント レポートの取得が拒否されました。
- 27 = クライアントによってテスト要求が拒否されました。
- 28 = ネットワーク（IP）設定が無効です。
- 29 = ネットワークに関する既知の機能停止または問題があります。
- 30 = 定期的なメンテナンスの時期です。
- 31 = WLAN のセキュリティ方式が正しくありません。
- 32 = WLAN の暗号化方式が正しくありません。
- 33 = WLAN の認証方式が正しくありません。

ステップ 12 最新のテストのステータスを確認するには、次のコマンドを入力します。

show client ccx last-test-status *client_mac_address*

デフォルト ゲートウェイの ping テストに対しては、次のような情報が表示されます。

```
Test Type..................................... Gateway Ping Test
Test Status................................... Pending/Success/Timeout

Dialog Token.................................. 15
Timeout....................................... 15000 ms
Request Time.................................. 1329 seconds since system boot
```

ステップ 13 最新のテスト応答のステータスを確認するには、次のコマンドを入力します。

show client ccx last-response-status *client_mac_address*

802.1X 認証 テストに対しては、次のような情報が表示されます。

```
Test Status................................... Success

Response Dialog Token......................... 87
Response Status............................... Successful
Response Test Type............................ 802.1x Authentication Test
Response Time................................. 3476 seconds since system boot
```

ステップ 14 最新の合格診断テストの結果を確認するには、次のコマンドを入力します。

show client ccx results *client_mac_address*

802.1X 認証 テストに対しては、次のような情報が表示されます。

```
dot1x Complete................................ Success
EAP Method.................................... *1,Host OS Login Credentials
dot1x Status.................................. 255
```

ステップ 15 前回のテストでクライアントが取得した関連データ フレームを確認するには、次のコマンドを入力します。

show client ccx frame-data *client_mac_address*

次のような情報が表示されます。

```
LOG Frames:

Frame Number:..................................... 1
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 863954us
Frame Length:..................................... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd bd b0  ............D...
00000010: 00 12 44 bd bd b0 f0 af  43 70 00 f2 82 01 00 00  ..D.....Cp......
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 32 33 2d  31 30 00 00 00 00 00 00  ...AP23-10......
00000050: 00 00 00 00 00 00 26 96  06 00 40 96 00 ff ff dd  ......&...@.....
00000060: 18 00 50 f2 01 01 00 00  50 f2 05 01 00 00 50 f2  ..P.....P.....P.
00000070: 05 01 00 00 40 96 00 28  00 dd 06 00 40 96 01 01  ....@..(....@...

00000080: 00 dd 05 00 40 96 03 04  dd 16 00 40 96 04 00 02  ....@......@....
00000090: 07 a4 00 00 23 a4 00 00  42 43 00 00 62 32 00 00  ....#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd  18 00 50 f2 02 01 01 82  ...@......P.....
000000b0: 00 03 a4 00 00 27 a4 00  00 42 43 5e 00 62 32 2f  .....'...BC^.b2/

LOG Frames:

Frame Number:..................................... 2
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 878289us
Frame Length:..................................... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 0d ed c3 a0 22  ..............."
00000010: 00 0d ed c3 a0 22 00 bd  4d 50 a5 f7 78 08 00 00  ....."..MP..x...
00000020: 64 00 01 00 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 84 00 0f 00 ff  l...............
00000040: 03 19 00 72 6f 67 75 65  2d 74 65 73 74 31 00 00  ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96  06 00 40 96 00 10 00 dd  ......#...@.....
00000060: 06 00 40 96 01 01 00 dd  05 00 40 96 03 04 dd 05  ..@.......@.....
00000070: 00 40 96 0b 01 dd 18 00  50 f2 02 01 01 81 00 03  .@......P.......

00000080: a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 d2  ...'...BC^.b2/..
00000090: b4 ab 84                                          ...

LOG Frames:

Frame Number:..................................... 3
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 881513us
Frame Length:..................................... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd 80 30  ............D..0
00000010: 00 12 44 bd 80 30 60 f7  46 c0 8b 4b d1 05 00 00  ..D..0`.F..K....
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 00 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 34 30 2d  31 37 00 00 00 00 00 00  ...AP40-17......
00000050: 00 00 00 00 00 00 26 dd  18 00 50 f2 01 01 00 00  ......&...P.....
00000060: 50 f2 05 01 00 00 50 f2  05 01 00 00 40 96 00 28  P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01  00 dd 05 00 40 96 03 04  ....@.......@...

00000080: dd 16 00 40 96 04 00 05  07 a4 00 00 23 a4 00 00  ...@........#...
00000090: 42 43 00 00 62 32 00 00  dd 05 00 40 96 0b 01 dd  BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85  00 03 a4 00 00 27 a4 00  ..P..........'..
000000b0: 00 42 43 5e 00 62 32 2f  00 0b 9a 1d 6f           .BC^.b2/....o
...
```

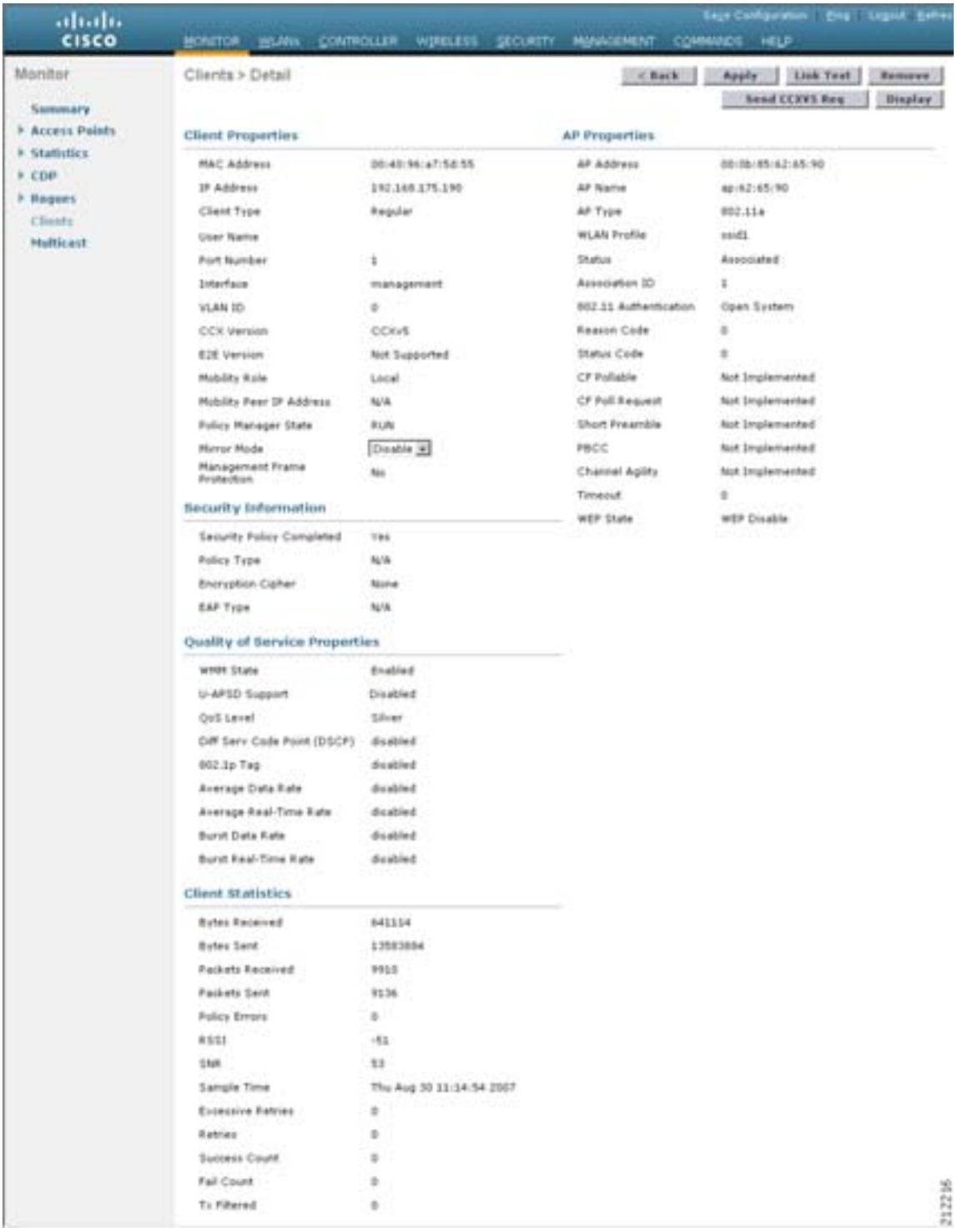
GUI を使用したクライアント レポートの設定

コントローラの GUI を使用してクライアント レポートを設定する手順は、次のとおりです。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます。

ステップ 2　目的のクライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます（図 D-4 を参照）。

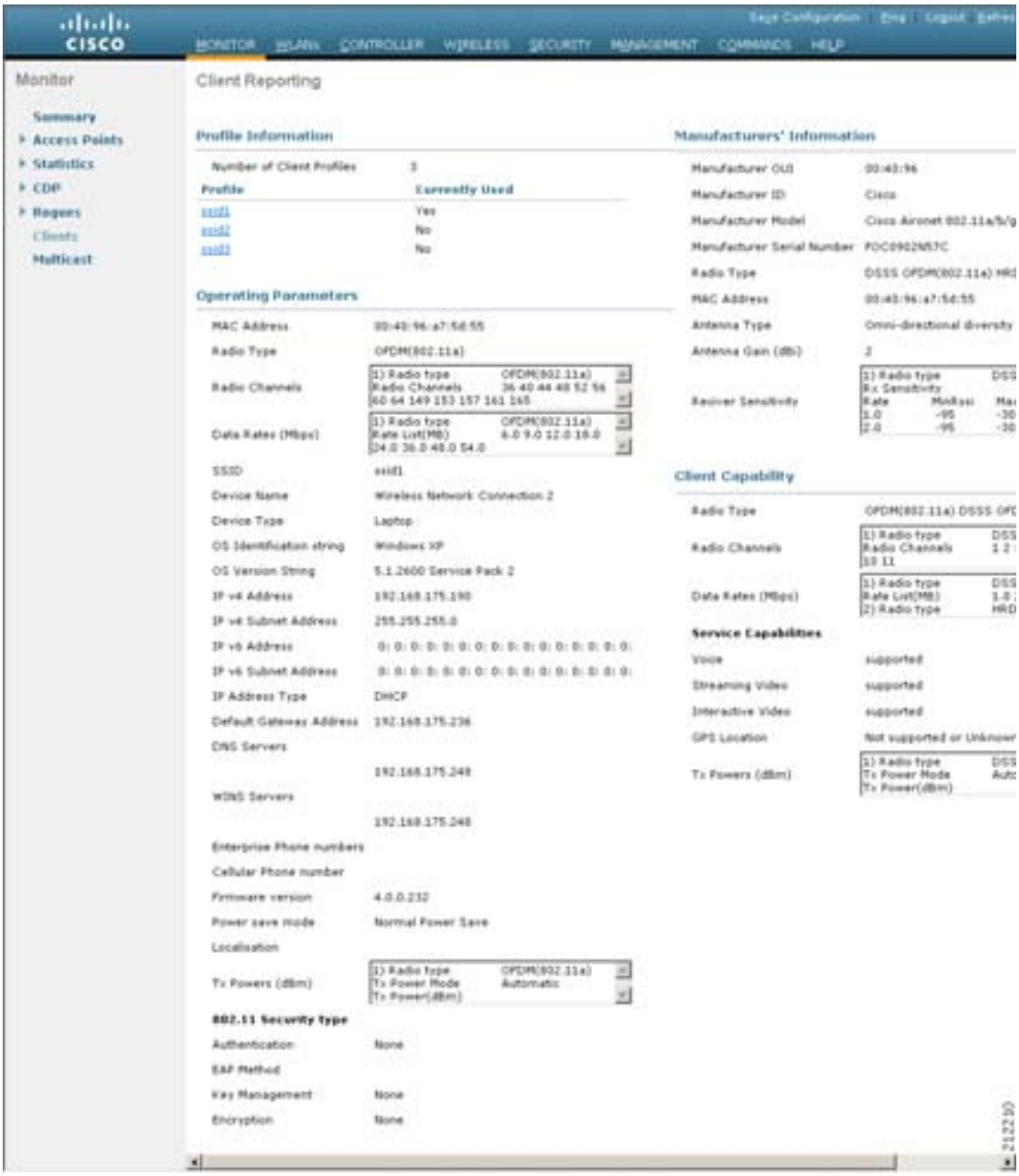
図 D-4　Clients > Detail ページ



ステップ 3　レポート要求をクライアントに送信するには、**CCXv5 Req** ボタンをクリックします。

ステップ 4　クライアントのパラメータを表示するには、**Display** をクリックします。Client Reporting ページが表示されます（図 D-5 を参照）。

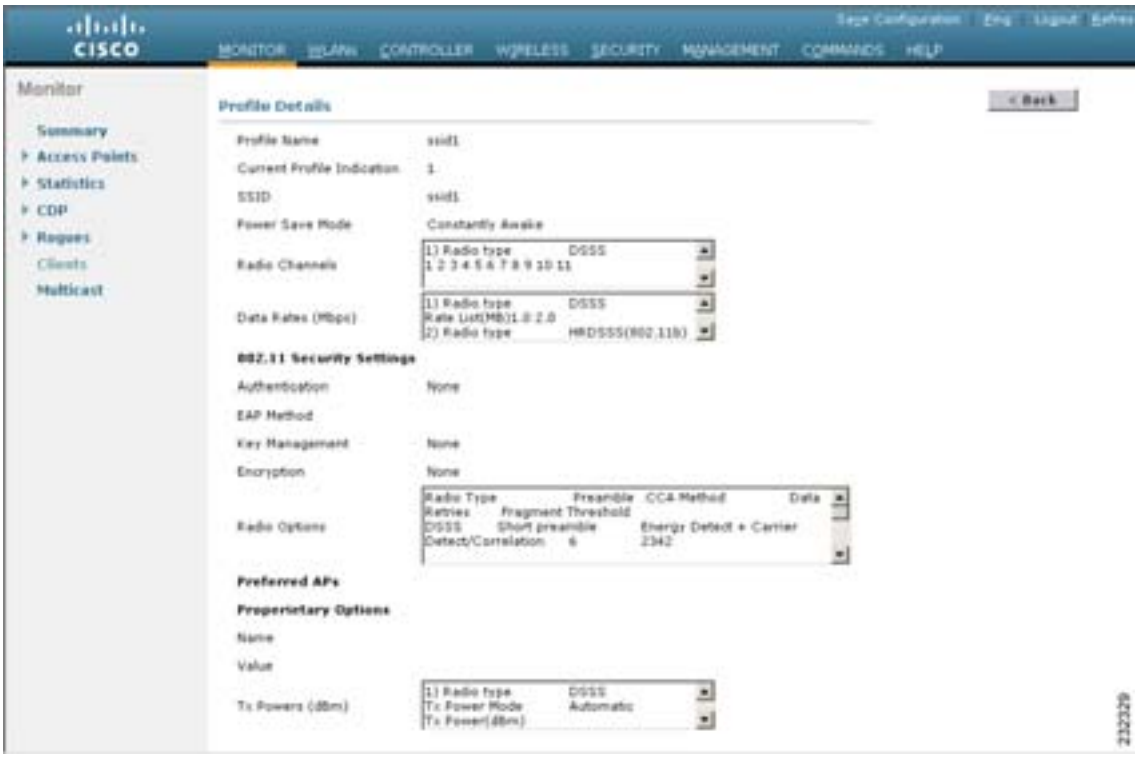
図 D-5　Client Reporting ページ



このページには、クライアント プロファイルおよび現在それらが使用されているかどうかが表示されます。クライアントの動作パラメータ、製造元、および機能に関する情報も表示されます。

ステップ 5　目的のクライアント プロファイルのリンクをクリックします。Profile Details ページが表示されます（図 D-6 を参照）。

図 D-6　Profile Details ページ



このページには、SSID、省電力モード、無線チャネル、データ レート、802.11 セキュリティ設定などのクライアント プロファイルの詳細が表示されます。

CLI を使用したクライアント レポートの設定

コントローラの CLI を使用してクライアント レポートを設定する手順は、次のとおりです。

ステップ 1　クライアント プロファイルを送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-profiles *client_mac_address*

ステップ 2　現在の動作パラメータを送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-operating-parameters *client_mac_address*

ステップ 3　製造元の情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-manufacturer-info *client_mac_address*

ステップ 4　機能情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-client-capability *client_mac_address*

ステップ 5　クライアント レポートの情報をクリアするには、次のコマンドを入力します。

config client ccx clear-reports *client_mac_address*

ステップ 6　クライアント プロファイルを表示するには、次のコマンドを入力します。

show client ccx profiles *client_mac_address*

次のような情報が表示されます。

```
Number of Profiles.............................. 1
Current Profile................................. 1

Profile ID...................................... 1
Profile Name.................................... wifiEAP
SSID............................................ wifiEAP
Security Parameters[EAP Method,Credential]..... EAP-TLS,Host OS Login Credentials
Auth Method..................................... EAP
Key Management................................. WPA2+CCKM
Encryption...................................... AES-CCMP
Power Save Mode................................. Constantly Awake
Radio Configuration:
Radio Type...................................... DSSS
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 1.0 2.0

Radio Type...................................... HRDSSS(802.11b)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 5.5 11.0

Radio Type...................................... ERP(802.11g)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Radio Type...................................... OFDM(802.11a)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
Radio Channels................................ 36 40 44 48 52 56 60 64 149 153 157
161 165
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0
```

ステップ 7　クライアントの動作パラメータを表示するには、次のコマンドを入力します。

show client ccx operating-parameters *client_mac_address*

次のような情報が表示されます。

```
Client Mac..................................... 00:40:96:b2:8d:5e
Radio Type..................................... OFDM(802.11a)

Radio Type..................................... OFDM(802.11a)
  Radio Channels............................... 36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Power Save Mode................................ Normal Power Save
SSID........................................... wifi
Security Parameters[EAP Method,Credential]..... None
Auth Method.................................... None
Key Management................................. None
Encryption..................................... None
Device Name.................................... Wireless Network Connection 15
Device Type.................................... 0
OS Id.......................................... Windows XP
OS Version..................................... 5.1.2600 Service Pack 2
IP Type........................................ DHCP address
IPv4 Address................................... Available
IP Address..................................... 70.0.4.66
Subnet Mask.................................... 255.0.0.0
Default Gateway................................ 70.1.0.1
IPv6 Address................................... Not Available
IPv6 Address.................................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0: 0:
IPv6 Subnet Mask............................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0: 0:
DNS Servers.................................... 103.0.48.0
WINS Servers...................................
System Name.................................... URAVAL3777
Firmware Version............................... 4.0.0.187
Driver Version................................. 4.0.0.187
```

ステップ 8　クライアントの製造元情報を表示するには、次のコマンドを入力します。

show client ccx manufacturer-info *client_mac_address*

次のような情報が表示されます。

```
Manufacturer OUI.............................. 00:40:96
Manufacturer ID............................... Cisco
Manufacturer Model............................ Cisco Aironet 802.11a/b/g Wireless
Adapter
Manufacturer Serial........................... FOC1046N3SX
Mac Address................................... 00:40:96:b2:8d:5e
Radio Type.................................... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Antenna Type.................................. Omni-directional diversity
Antenna Gain.................................. 2 dBi

Rx Sensitivity:
Radio Type.................................... DSSS
Rx Sensitivity ............................... Rate:1.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:2.0 Mbps, MinRssi:-95,
MaxRssi:-30
Radio Type.................................... HRDSSS(802.11b)
Rx Sensitivity ............................... Rate:5.5 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:11.0 Mbps, MinRssi:-95,
MaxRssi:-30
Radio Type.................................... ERP(802.11g)
Rx Sensitivity ............................... Rate:6.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:9.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:12.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:18.0 Mbps, MinRssi:-95,
MaxRssi:-30
```

ステップ 9　クライアントの機能情報を表示するには、次のコマンドを入力します。

show client ccx client-capability *client_mac_address*

（注）　このコマンドは、機能の現在の設定ではなく、クライアントで使用可能な機能を表示します。

次のような情報が表示されます。

```
Service Capability..............................  Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type.....................................  DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)

Radio Type.....................................  DSSS
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  1.0 2.0

Radio Type.....................................  HRDSSS(802.11b)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  5.5 11.0

Radio Type.....................................  ERP(802.11g)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Radio Type.....................................  OFDM(802.11a)
  Radio Channels...............................  36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0
```

CLI を使用したローミング診断とリアルタイム診断の設定

コントローラの CLI を使用してローミング診断とリアルタイム診断を設定する手順は、次のとおりです。

ステップ 1　ログ要求を送信するには、次のコマンドを入力します。

config client ccx log-request *log_type client_mac_address*

log_type は、roam、rsna、または syslog です。

ステップ 2　ログ応答を表示するには、次のコマンドを入力します。

show client ccx log-response *log_type client_mac_address*

log_type は、roam、rsna、または syslog です。

log_type が roam であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 13s 322396us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3125(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 16s 599006us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3235(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 19s 882921us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3234(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 08s 815477us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:d2, Transition Time=3281(ms)
                          Transition Reason: First association to WLAN
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 26s 637084us
                          Source BSSID=00:0b:85:81:06:d2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3313(ms)
```

log_type が rsna であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246578us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246625us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 01s 624375us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                        RSNA Result: Success
```

log_type が syslog であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278987us
                          Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278990us
                          Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278993us
                          Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278996us
                          Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279000us
                          Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279003us
                          Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279009us
                          Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279012us
                          Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory
elements missing in the OID response'
```

ステップ 3　統計の要求を送信するには、次のコマンドを入力します。

config client ccx stats-request *measurement_duration stats_name client_mac_address*

stats_name は、dot11 または security です。

ステップ 4　統計応答を表示するには、次のコマンドを入力します。

show client ccx stats-report *client_mac_address*

次のような情報が表示されます。

```
Measurement duration = 1

     dot11TransmittedFragmentCount       = 1
     dot11MulticastTransmittedFrameCount = 2
     dot11FailedCount                    = 3
     dot11RetryCount                     = 4
     dot11MultipleRetryCount             = 5
     dot11FrameDuplicateCount            = 6
     dot11RTSSuccessCount                = 7
     dot11RTSFailureCount                = 8
     dot11ACKFailureCount                = 9
     dot11ReceivedFragmentCount          = 10
     dot11MulticastReceivedFrameCount    = 11
     dot11FCSErrorCount                  = 12
     dot11TransmittedFrameCount        = 13
```

デバッグ ファシリティの使用方法

デバッグ ファシリティにより、コントローラの CPU とやり取りするすべてのパケットを表示できるようになります。受信したパケット、送信したパケット、またはその両方に対して有効にできます。デフォルトでは、デバッグ ファシリティによって受信されたすべてのパケットが表示されます。それらを表示する前に、アクセス コントロール リスト（ACL）を定義してパケットをフィルタリングすることもできます。ACL に渡されないパケットは、表示されずに破棄されます。

各 ACL には、動作（許可、拒否、無効化）、およびパケットの適合に使用する 1 つまたは複数のフィールドが含まれます。デバッグ ファシリティでは、次のレベルおよび値で動作する ACL が提供されます。

- ドライバ ACL
  - NPU のカプセル化の種類
  - ポート
- Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）
  - 宛先ポート（該当する場合）
- EoIP payload Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- EoIP payload IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）
  - 宛先ポート（該当する場合）
- LWAPP payload 802.11 header ACL
  - 宛先アドレス
  - 送信元アドレス
  - BSSID
  - SNAP ヘッダの種類
- LWAPP payload IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）

— 宛先ポート（該当する場合）

各レベルにおいて、複数の ACL を定義できます。パケットと一致する最初の ACL が、選択された ACL となります。

デバッグ ファシリティを使用する手順は、次のとおりです。

ステップ 1　デバッグ ファシリティを有効にするには、次のコマンドを入力します。

debug packet logging enable {**rx** | **tx** | **all**} *packet_count display_size*

このとき、次のようになります。

- **rx** の場合は受信したすべてのパケット、**tx** の場合は送信したすべてのパケット、**all** の場合は受信と送信の両方のパケットが表示されます。
- *packet_count* は、ログするパケットの最大数です。1 ～ 65535 の値をパケット数として入力できます。また、デフォルト値は 25 パケットです。
- *display_size* は、パケットを印刷する際の表示バイト数です。デフォルトでは、全パケットが表示されます。

（注）　デバッグ ファシリティを無効にするには、次のコマンドを入力します。**debug packet logging disable**

ステップ 2　パケットをログする ACL を設定するには、次のコマンドを使用します。

- **debug packet logging acl driver** *rule_index action npu_encap port*

  このとき、次のようになります。
  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *npu_encap* では、パケットのフィルタリング方法を定める、NPU のカプセル化の種類を指定します。指定可能な値には、dhcp、dot11-mgmt、dot11-probe、dot1x、eoip-ping、iapp、ip、lwapp、multicast、orphan-from-sta、orphan-to-sta、rbcp、wired-guest などがあります。
  - *port* は、パケットの送受信のための物理ポートです。
- **debug packet logging acl eth** *rule_index action dst src type vlan*

  このとき、次のようになります。
  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *dst* は、宛先の MAC アドレスです。
  - *src* は、送信元の MAC アドレスです。
  - *type* は、2 バイト タイプのコード（IP の場合は 0x800、ARP の場合は 0x806 など）です。このパラメータには、「ip」（0x800 の代わり）や「arp」（0x806 の代わり）などのいくつかの一般的な文字列値も使用できます。
  - *vlan* は、2 バイトの VLAN ID です。
- **debug packet logging acl ip** *rule_index action src dst proto src_port dst_port*

  このとき、次のようになります。
  - *proto* は、数値または getprotobyname() で認識される任意の文字列です。コントローラでは、次の文字列がサポートされています。ip、icmp、igmp、ggp、ipencap、st、tcp、egp、pup、udp、hmp、xns-idp、rdp、iso-tp4、xtp、ddp、idpr-cmtp、rspf、vmtp、ospf、ipip、および encap。

- *src_port* は、2 バイトの UDP/TCP 送信元ポート（telnet、23 など）か「any」です。コントローラでは、数値または getservbyname() によって認識される任意の文字列を受け付けます。コントローラでは、次の文字列がサポートされています。tcpmux、echo、discard、systat、daytime、netstat、qotd、msp、chargen、ftp-data、ftp、fsp、ssh、telnet、smtp、time、rlp、nameserver、whois、re-mail-ck、domain、mtp、bootps、bootpc、tftp、gopher、rje、finger、www、link、kerberos、supdup、hostnames、iso-tsap、csnet-ns、3com-tsmux、rtelnet、pop-2、pop-3、sunrpc、auth、sftp、uucp-path、nntp、ntp、netbios-ns、netbios-dgm、netbios-ssn、imap2、snmp、snmp-trap、cmip-man、cmip-agent、xdmcp、nextstep、bgp、prospero、irc、smux、at-rtmp、at-nbp、at-echo、at-zis、qmtp、z3950、ipx、imap3、ulistserv、https、snpp、saft、npmp-local、npmp-gui、および hmmp-ind。
- *dst_port* は、2 バイトの UDP/TCP 宛先ポート（telnet、23 など）か「any」です。コントローラでは、数値または getservbyname() によって認識される任意の文字列を受け付けます。コントローラでは、*src_port.* の場合と同じ文字列がサポートされています。

- **debug packet logging acl eoip-eth** *rule_index action dst src type vlan*
- **debug packet logging acl eoip-ip** *rule_index action src dst proto src_port dst_port*
- **debug packet logging acl lwapp-dot11** *rule_index action dst src bssid snap_type*

  このとき、次のようになります。
  - *bssid* は、Basic Service Set Identifier（BSSID; 基本サービス セット ID）です。
  - *snap_type* は、イーサネットの種類です。
- **debug packet logging acl lwapp-ip** *rule_index action src dst proto src_port dst_port*

（注） 設定されているすべての ACL を削除するには、次のコマンドを入力します。**debug packet logging acl clear-all**

ステップ 3　デバッグ出力の形式を設定するには、次のコマンドを入力します。

debug packet logging format {**hex2pcap** | **text2pcap**}

デバッグ ファシリティでは、hex2pcap と text2pcap という 2 つの出力形式がサポートされています。IOS によって使用される標準の形式では hex2pcap の使用がサポートされており、HTML フロントエンドを使用してデコードできます。text2pcap オプションは、一連のパケットを同一のコンソール ログ ファイルからデコードできるように代案として提供されます。図 D-7 は hex2pcap の出力例を示し、図 D-8 は text2pcap の出力例を示します。

図 D-7　Hex2pcap の出力例

```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B0540 08C0000C 316E7F00 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 ADBD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
```

212236

図 D-8　Text2pcap の出力例

```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
```

232343

ステップ 4　パケットが表示されない理由を判断するには、次のコマンドを入力します。

debug packet error {**enable** | **disable**}

ステップ 5　パケットのデバッグのステータスを表示するには、次のコマンドを入力します。

show debug packet

次のような情報が表示されます。

```
Status..................................... disabled
Number of packets to display..................... 25
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

無線スニファの設定

コントローラでは、アクセス ポイント をネットワーク「スニファ」として設定できます。スニファは、特定のチャネル上のすべてのパケットを取り出して、パケット アナライザ ソフトウェアを実行しているリモート マシンに転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。スニファを使用すると、ネットワーク アクティビティを監視して記録し、問題を検出できます。

サポートされている主なサードパーティ製のネットワーク アナライザ ソフトウェア アプリケーションは、次のとおりです。

- Wildpackets Omnipeek または Airopeek（http://www.wildpackets.com）
- AirMagnet Enterprise Analyzer（http://www.airmagnet.com）
- Wireshark（http://www.wireshark.org）

無線スニファの必須条件

無線スニファを実行するには、次のハードウェアとソフトウェアが必要です。

- **専用アクセス ポイント**：スニファとして設定された アクセス ポイント は、同時にネットワーク上の無線アクセス サービスとして機能することはできません。カバレッジの障害を防ぐために、既存の無線ネットワークの一部ではない アクセス ポイント を使用してください。
- **リモート監視デバイス**：アナライザ ソフトウェアを実行できるコンピュータ。
- **Windows XP** または **Linux オペレーティング システム**：コントローラは、Windows XP と Linux のいずれのマシンでもスニファをサポートしています。
- **ソフトウェア**および**関連ファイル、プラグイン、**または**アダプタ**：アナライザ ソフトウェアによっては、スニファを有効にするために特殊なファイルが必要となる場合があります。
  - **Omnipeek** または **Airopeek**：http://www.wildpackets.com にアクセスし、手順に従ってソフトウェアを購入、インストール、および設定してください。
  - **AirMagnet**：http://www.airmagnet.com/products/ea_cisco/#top にアクセスし、手順に従ってソフトウェアを購入、インストール、および設定してください。
  - **Wireshark**：http://tools.cisco.com/support/downloads にアクセスし、手順に従って使用しているオペレーティング システム用の Wireshark と適切なインストール ウィザードをダウンロードしてください。

GUI を使用した、アクセス ポイントのスニファの設定

コントローラの GUI を使用して、アクセス ポイント上でスニファを有効化して設定する手順は、次のとおりです。

ステップ 1　**Wireless** > **Access Points** > **All APs** の順にクリックして、All APs ページを開きます。

ステップ 2　スニファとして設定するアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます（図 D-9 を参照）。

図 D-9　All APs > Details ページ

ステップ 3　AP Mode ドロップダウン ボックスから **Sniffer** を選択します。

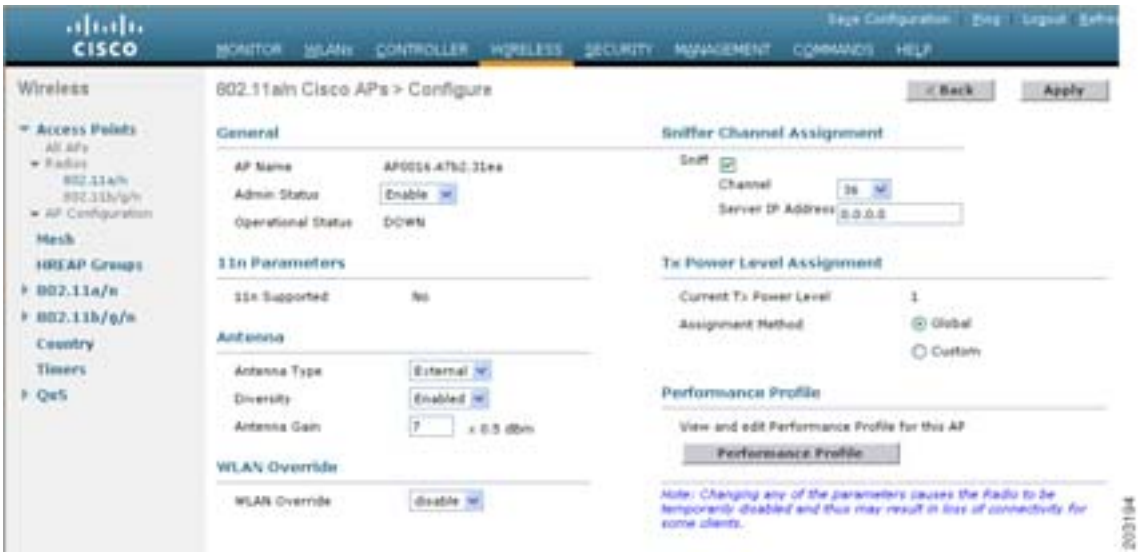
ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　アクセス ポイントをリブートするという警告が表示されたら、**OK** をクリックします。

ステップ 6　**Wireless** > **Access Points** > **Radios** > **802.11a/n**（または **802.11b/g/n**）の順にクリックして、802.11a/n（または 802.11b/g/n）Radios ページを開きます。

ステップ 7　カーソルを目的のアクセス ポイントの青のドロップダウン矢印の上に置いて、**Configure** を選択します。802.11a/n（または 802.11b/g/n）Cisco APs > Configure ページが表示されます（図 D-10 を参照）。

図 D-10　802.11b/g/n Cisco APs > Configure ページ



ステップ 8　このアクセス ポイントでスニファを有効にする場合は、**Sniff** チェック ボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルトではオフになっています。

ステップ 9　ステップ 8 でスニファを有効にした場合は、次の手順に従ってください。

a. Channel ドロップダウン ボックスから、アクセス ポイントがパケットに対してスニファするチャネルを選択します。

b. Server IP Address フィールドに、Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスを入力します。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した、アクセス ポイントのスニファの設定

コントローラの CLI を使用して、アクセス ポイント上でスニファを有効にする手順は、次のとおりです。

ステップ 1　アクセス ポイントをスニファとして設定するには、次のコマンドを入力します。

config ap mode sniffer *Cisco_AP*

Cisco_AP はスニファとして設定されるアクセス ポイントです。

ステップ 2　アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。アクセス ポイントはスニファ モードでリブートします。

ステップ 3　アクセス ポイントでスニファを有効にするには、次のコマンドを入力します。

config ap sniff {802.11a | 802.11b} enable *channel server_IP_address Cisco_AP*

このとき、次のようになります。

- *channel* はアクセス ポイントがパケットに対してスニファする無線チャンネルです。デフォルト値は 36（802.11a/n）と 1（802.11b/g/n）です。
- *server_IP_address* は Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスです。
- *Cisco_AP* はスニファとして設定されるアクセス ポイントです。

（注）　アクセス ポイントでスニファを無効にするには、次のコマンドを入力します。
config ap sniff {802.11a | 802.11b} disable *Cisco_AP*

ステップ 4　変更を保存するには、次のコマンドを入力します。

save config

ステップ 5　アクセス ポイントのスニファ設定を表示するには、次のコマンドを入力します。

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

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 17
Cisco AP Name.................................... AP1131:46f2.98ac
...
AP Mode ......................................... Sniffer
Public Safety ................................... Global: Disabled, Local: Disabled
Sniffing ........................................ No
...
```

Telnet または SSH を使用したアクセス ポイントのトラブルシューティング

コントローラは、Telnet プロトコルまたは Secure Shell（SSH）プロトコルを使用した Lightweight アクセス ポイントのトラブルシューティングをサポートしています。これらのプロトコルを使用すると、特にアクセス ポイントがコントローラに接続できない場合に、デバッグを簡単に行うことができます。

- 潜在的な競合やネットワーク セキュリティの脅威を避けるため、Telnet または SSH セッションを有効にしている間は次のコマンドを使用できません。**config terminal**、**telnet**、**ssh**、**rsh**、**ping**、**traceroute**、**clear**、**clock**、**crypto**、**delete**、**fsck**、**lwapp**、**mkdir**、**radius**、**release**、**reload**、**rename,renew**、**rmdir**、**save**、**set**、**test**、**upgrade**。
- Telnet または SSH セッション中に使用できる主なコマンドは次のとおりです。**debug**、**disable**、**enable**、**help**、**led**、**login**、**logout**、**more**、**no debug**、**show**、**systat**、**undebug**、**where**。

コントローラの CLI を使用して、Lightweight アクセス ポイント上で Telnet または SSH を有効にする手順は、次のとおりです。

ステップ 1　アクセス ポイントで Telnet または SSH の接続を有効にするには、次のコマンドを入力します。

config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

（注）　アクセス ポイントで Telnet または SSH の接続を無効にするには、次のコマンドを入力します。
config ap {**telnet** | **ssh**} **disable** *Cisco_AP*

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

ステップ 3　アクセス ポイントで Telnet または SSH が有効になっているかどうかを確認するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask....................................... 255.255.248.0
Gateway IP Addr.................................. 10.22.8.1
Domain.......................................
Name Server...................................
Telnet State..................................... Enabled
Ssh State........................................ Enabled
...
```

APPENDIX E

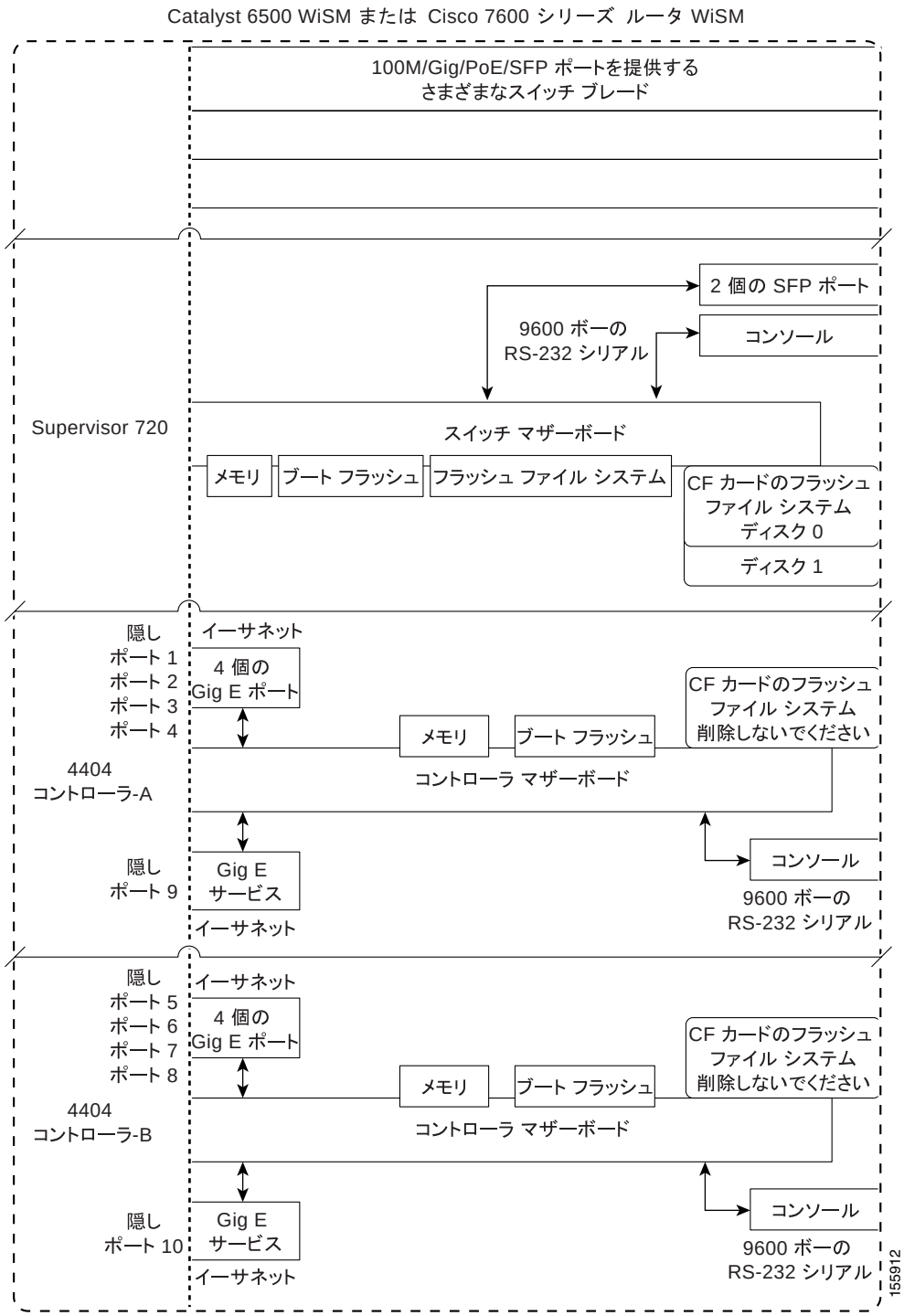
論理接続図

この付録には、統合コントローラの論理接続図および関連するソフトウェア コマンドが記載されています。この章の内容は、次のとおりです。

この項には、他のシスコ製品に統合されたコントローラ、特に、Catalyst 3750G 統合型無線 LAN コントローラ スイッチ、Cisco WiSM、および Cisco 28/37/38xx シリーズ サービス統合型ルータの論理接続図が記載されています。これらの図は、スイッチまたはルータ、およびコントローラとの間の内部接続を示しています。また、デバイス間の通信に使用されるソフトウェア コマンドも記載されています。

Cisco WiSM

図 E-1　Cisco WiSM の論理接続図

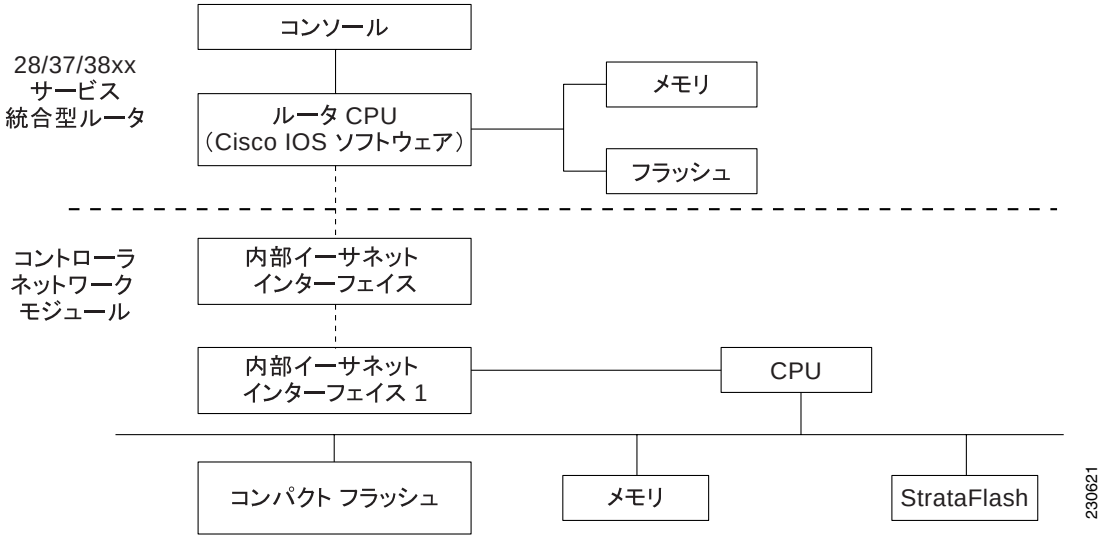


Cisco WiSM、Supervisor 720、および 4404 コントローラ間の通信で使用されるコマンドについては、次の URL からアクセスできる『Configuring a Cisco Wireless Services Module and Wireless Control System』を参照してください。

http://www.cisco.com/en/US/docs/wireless/technology/wism/technical/reference/appnote.html#wp39498

Cisco 28/37/38xx サービス統合型ルータ

図 E-2　Cisco 28/37/38xx サービス統合型ルータの論理接続図



次のコマンドは、28/37/38xx サービス統合型ルータおよびコントローラ ネットワーク モジュール間の通信で使用されます。これらは、ルータから起動されます。このコマンドは、ネットワーク モジュールのバージョンによって異なります。

次のコマンドは、ルータおよびファスト イーサネット バージョンのコントローラ ネットワーク モジュール間の通信で使用されます。

- **interface wlan-controller** *slot/unit*（サブインターフェイスをサポートする場合は、**dot1q encap** を追加）
- **show interfaces wlan-controller** *slot/unit*
- **show controllers wlan-controller** *slot/unit*
- **test service-module wlan-controller** *slot/unit*
- **test HW-module wlan-controller** *slot/unit* **reset** {**enable** | **disable**}
- **service-module wlan-controller** *slot/port* {**reload** | **reset** | **session** [**clear**] | **shutdown** | **status**}

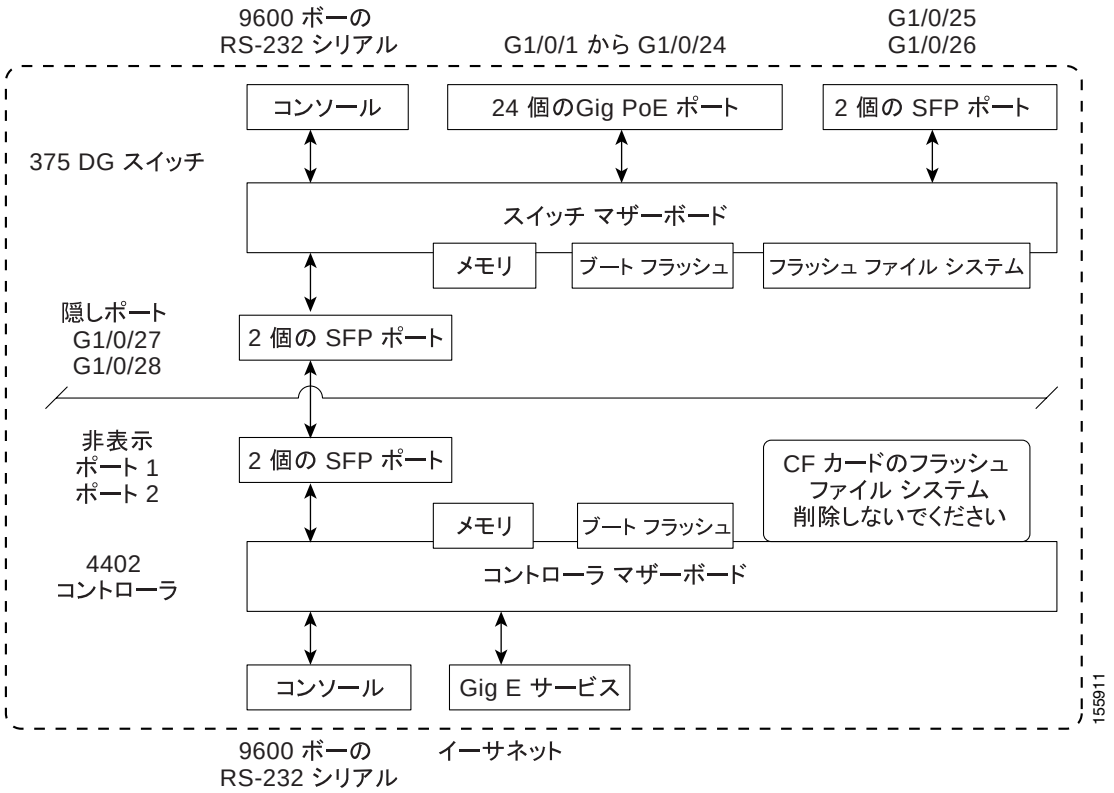
次のコマンドは、ルータおよびギガビット イーサネット バージョンのコントローラ ネットワーク モジュール間の通信で使用されます。

- **interface integrated-service-engine** *slot/unit*（サブインターフェイスをサポートする場合は、**dot1q encap** を追加）
- **show interfaces integrated-service-engine** *slot/unit*
- **show controllers integrated-service-engine** *slot/unit*
- **test service-module integrated-service-engine** *slot/unit*
- **test HW-module integrated-service-engine** *slot/unit* **reset** {**enable** | **disable**}
- **service-module integrated-service engine** *slot/port* {**reload** | **reset** | **session** [**clear**] | **shutdown** | **status**}

(注)　詳細は、『Cisco Wireless LAN Controller Network Module Feature Guide』を参照してください。このドキュメントには、次の URL からアクセスできます。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124limit/124x/124xa2/boxernm.htm#wp2033271

Catalyst 3750G 統合型無線 LAN コントローラ スイッチ

図 E-3　Catalyst 3750G 統合型無線 LAN コントローラ スイッチの論理接続図



次のコマンドは、Catalyst 3750G スイッチと 4402 コントローラ間の通信で使用されます。

ログイン コマンド

次のコマンドは、スイッチからコントローラへの Telnet セッションを開始するために使用します。

session *switch_number* **processor 1**

スタック内には複数のスイッチが存在することがあるため、*switch_number* パラメータを使用して、このセッションのスタック内のコントローラにダイレクトされるスイッチを示します。セッションが確立されたら、コントローラの CLI と対話します。**exit** を入力すると、セッションが終了し、スイッチの CLI に戻ります。

表示コマンド

次のコマンドは、内部コントローラのステータスを表示するために使用します。これらは、スイッチから起動されます。

- **show platform wireless-controller** *switch_number* **summary**

  次のような情報が表示されます。

```
Switch  Status  State
1       up      operational
2       up      operational
```

- **show platform wireless-controller** *switch_number* **status**

  次のような情報が表示されます。

```
Switch  Service IP      Management IP   SW Version      Status
------+---------------+---------------+---------------+-------
 1      127.0.1.1       70.1.30.1       4.0.52.0        operational
 2      127.0.1.2       70.1.31.1       4.0.45.0        operational
```

- **show platform wireless-controller** *switch_number* **management-info**

```
sw vlan ip                  gateway         http https mac            version
1  0    70.1.30.1/16        70.1.1.1        1    1     0016.9dca.d963 4.0.52.0
2  0    70.1.31.1/16        70.1.1.1        0    1     0016.9dca.dba3 4.0.45.0
```

デバッグ コマンド

Wireless Control Protocol（WCP）は、スイッチとコントローラの間で実行される内部キープアライブ プロコトルです。このプロトコルにより、スイッチは、コントローラの状態を管理できます。このプロトコルは、UDP を使用し、2 つの内部ギガビット ポート上で実行されますが、内部 VLAN 4095 を作成してコントロール トラフィックをデータ トラフィックから区別します。20 秒ごとに、スイッチは、キープアライブ メッセージをコントローラに送信します。コントローラが 16 回の連続したキープアライブ メッセージに応答しなかった場合、スイッチは、コントローラがアクティブではないことを宣言し、リセット信号を送信してコントローラをリブートします。

次のコマンドは、内部コントローラの状態を監視するために使用します。

このコマンドは、コントローラから起動されます。

- **debug wcp** *?*

  ? は、次のいずれかです。

  packet：WCP パケットをデバッグします。

  events：WCP イベントをデバッグします。

  次のような情報が表示されます。

```
Tue Feb  7 23:30:31 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:30:31 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:31 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:51 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:30:51 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:30:51 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:31:11 2006: Received WCP_MSG_TYPE_REQUEST
Tue Feb  7 23:31:11 2006: Received WCP_MSG_TYPE_REQUEST,of type WCP_TLV_KEEP_ALIVE
Tue Feb  7 23:31:11 2006: Sent WCP_MSG_TYPE_RESPONSE,of type WCP_TLV_KEEP_ALIVE
```

このコマンドは、スイッチから起動されます。

- **debug platform wireless-controller** *switch_number ?*

  ? は、次のいずれかです。

  all：すべて

  errors：エラー

  packets：WCP パケット

  sm：ステート マシン

  wcp：WCP プロトコル

リセット コマンド

次の 2 つのコマンドは、スイッチからコントローラをリセットするために使用します（示されている順序で使用します）。これらのコマンドは、現時点ではまだ使用できませんが、今後のリリースでサポートされる予定です。

- **test wireless-controller stop** *switch_number*
- **test wireless-controller start** *switch_number*

（注） コントローラへの直接コンソール接続は、PC でハードウェア フロー制御が有効になっている場合は動作しません。ただし、スイッチのコンソール ポートは、ハードウェア フロー制御が有効になっている状態でも動作します。

INDEX

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

て

と

な

に

ね

ほ

ま

み

む

め

ろ

わ