自律 Aironet アクセス ポイント Cisco IOS コンフィギュレーション ガイド

Cisco IOS リリース 15.3（3）JBB

初版：2015 年 7 月 29 日

Cisco Systems, Inc.
www.cisco.com

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

Text Part Number:

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

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

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

自律 Aironet アクセス ポイント Cisco IOS コンフィギュレーション ガイド

はじめに

対象読者

このガイドは、自律モードの Cisco Aironet アクセス ポイントをインストールして管理するネットワーキングの専門家を対象にしています。このガイドを読むには、Cisco IOS ソフトウェアの操作経験があり、無線ローカル エリア ネットワークの概念と用語をよく知っている必要があります。

このガイドでは、Cisco Aironet 自律アクセス ポイントの Cisco IOS リリース 15.3(3)JA について説明します。

サポートされているアクセス ポイント プラットフォームは以下のとおりです。

- AP 802
- AP 702I
- AP 700W
- AP 1040
- AP 1140
- AP 1260
- AP 1530
- AP 1550（128 MB のみサポート）
- AP 1570 の比較
- AP 1600
- AP 1700
- AP 2600
- AP 2700
- AP 3500
- AP 3600（AIR-RM3000AC- *x*-K9 802.11ac モジュールはサポートされません）
- AP 3700（AIR-RM3000AC- *x*-K9 802.11ac モジュールはサポートされません）

（注） このガイドには、Lightweight アクセス ポイントについての説明はありません。これらのデバイスの設定方法については、Cisco.com で該当するインストール ガイドおよびコンフィギュレーション ガイドを参照できます。

目的

このガイドには、アクセス ポイントをインストールして、設定するために必要な情報を記載してあります。また、アクセス ポイントで使用するために作成され、変更された Cisco IOS ソフトウェア コマンドを使用する手順について説明します。これらのコマンドの詳細は扱いません。これらのコマンドに関する詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。標準の Cisco IOS ソフトウェア コマンドについては、Cisco.com のホーム ページの [Support] > [Documentation] から入手できる Cisco IOS ソフトウェアのドキュメンテーションを参照してください。

このガイドでは、コマンドライン インターフェイス（CLI）の全機能をカバーしている Access Point Web-based Interface（APWI; アクセス ポイントの Web ベース インターフェイス）の概要についても説明します。このガイドには、APWI ウィンドウのフィールドレベルの説明、および APWI からアクセス ポイントを設定する手順については記載していません。APWI ウィンドウのすべての説明と操作手順については、アクセス ポイントのオンライン ヘルプを参照してください。オンライン ヘルプは、APWI ページの [Help] ボタンをクリックすると表示されます。

設定手順と例

このマニュアルに記載されている手順と例は、Cisco Aironet 3600 シリーズ アクセス ポイントに基づいて文書化されています。

最新の設定例を確認するには、Cisco Tech Zone（https://techzone.cisco.com）にアクセスしてください。Tech Zone の [Navigator] で、[Wireless LAN] > [Autonomous APs (IOS)] の自律（IOS）無線展開に関するナレッジ ベースを参照してください。

（注） Cisco Tech Zone にアクセスするには、Cisco.com のアカウントが必要です。アカウントがない場合は、[Log In] ページで [Register Now] をクリックすると、アカウントを作成できます。

マニュアルの構成

このガイドは次の章にわかれています。

第 1 章「アクセス ポイント機能の概要」では、アクセス ポイントのソフトウェアとハードウェアの機能を挙げ、ネットワークでのアクセス ポイントの役割について説明します。

第 2 章「Web ブラウザ インターフェイスの使用方法」では、Web ブラウザ インターフェイスを使用してアクセス ポイントを設定する方法について説明します。

第 3 章「コマンドライン インターフェイスの使用」では、コマンドライン インターフェイス（CLI）を使用してアクセス ポイントを設定する方法について説明します。

第 4 章「アクセス ポイントの最初の設定」では、新しいアクセス ポイントに基本設定を行う手順について説明します。

第 5 章「アクセス ポイントの管理」では、アクセス ポイントへの不正なアクセスの防止、システムの日時の設定、システム名とプロンプトの設定など、アクセス ポイントを管理する 1 回限りの操作を実行する方法について説明します。

第 6 章「無線の設定」では、無線ネットワーク内での役割、送信電力、チャネル設定など、アクセス ポイント無線の設定方法について説明します。

第 7 章「複数の SSID の設定」では、アクセス ポイントに複数のサービス セット ID（SSID）と複数の基本サービス セット ID（BSSID）を設定して、管理する方法について説明します。アクセス ポイントには最大 16 個の SSID と最大 8 個の BSSID を設定できます。

第 8 章「スパニングツリー プロトコルの設定」では、アクセス ポイント、ブリッジ、またはブリッジ モードで稼働するアクセス ポイントにスパニングツリー プロトコル（STP）を設定する方法について説明します。STP を使用すると、ネットワーク内でのブリッジ ループの発生を防ぐことができます。

第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」では、無線 LAN 用のローカル Remote Authentication Dial-In User Service（RADIUS）サーバとして機能するアクセス ポイントの設定方法について説明します。メインの RADIUS サーバへの WAN 接続に障害が発生した場合、アクセス ポイントはバックアップ サーバとして機能し、無線デバイスを認証します。

第 10 章「WLAN 認証および暗号化の設定」では、認証済みキー管理に必要な暗号スイート、Wired Equivalent Privacy（WEP）、および Message Integrity Check（MIC; メッセージ完全性チェック）、Cisco Message Integrity Check（CMIC）、Temporal Key Integrity Protocol（TKIP）、Cisco Key Integrity Protocol（CKIP）、ブロードキャスト キー ローテーションなどの WEP 機能の設定方法について説明します。

第 11 章「認証タイプの設定」では、アクセス ポイントに認証タイプを設定する方法について説明します。クライアント デバイスは、これらの認証方式を使用してネットワークに接続します。

第 12 章「その他のサービスの設定」では、WDS に参加し、クライアント サービスのローミングで高速な再アソシエーションを可能にしたうえ、無線管理に参加させるためのアクセス ポイントの設定方法について説明します。

第 13 章「RADIUS サーバと TACACS+ サーバの設定」では、RADIUS と Terminal Access Controller Access Control System Plus（TACACS+）を有効にして設定する方法について説明します。RADIUS と TACACS+ は、認証プロセスと許可プロセスに詳細なアカウンティング情報と柔軟な管理制御を提供します。

第 14 章「VLAN の設定」では、有線 LAN で設定された VLAN と相互運用するようにアクセス ポイントを設定する方法について説明します。

第 15 章「QoS の設定」では、Web ブラウザ インターフェイスを使用してアクセス ポイントに MAC アドレス、IP、および EtherType のフィルタを設定して管理する方法について説明します。

第 16 章「フィルタの設定」では、Web ブラウザ インターフェイスを使用してアクセス ポイントに MAC アドレス、IP、および EtherType のフィルタを設定して管理する方法について説明します。

第 17 章「CDP の設定」では、アクセス ポイントに Cisco Discovery Protocol（CDP）を設定する方法について説明します。CDP はすべてのシスコ ネットワーク装置で稼働するデバイス検出プロトコルです。

第 18 章「SNMP の設定」では、アクセス ポイントに簡易ネットワーク管理プロトコル（SNMP）を設定する方法について説明します。

第 19 章「リピータ/スタンバイ アクセス ポイントおよびワークグループ ブリッジ モードの設定」では、アクセス ポイントをホット スタンバイ ユニットまたはリピータ ユニットとして設定する方法について説明します。

第 20 章「ファームウェアと設定の管理」では、フラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、ソフトウェア イメージのアーカイブ（アップロードとダウンロード）方法について説明します。

第 21 章「L2TPv3 over UDP/IP の設定」では、レイヤ 2 トンネリング プロトコル（L2TPv3）を設定する方法について説明します。L2TPv3 は、IP コア ネットワーク上でレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。

第 22 章「Ethernet over GRE の設定」では、Ethernet over GRE（EoGRE）について説明します。EoGRE は、IP コア ネットワーク上で GRE ヘッダーにカプセル化されたレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。

第 23 章「システム メッセージ ロギングの設定」では、アクセス ポイントにシステム メッセージ ロギングを設定する方法について説明します。

第 25 章「その他の AP 固有の設定」では、特定のアクセス ポイントの固有のその他の設定について説明します。

付録 A「プロトコル フィルタ」では、アクセス ポイントでフィルタリングできるプロトコルのリストを示します。

付録 B「サポート対象 MIB」では、アクセス ポイントがこのソフトウェア リリースでサポートする簡易ネットワーク管理プロトコル（SNMP）の管理情報ベース（MIB）のリストを示します。

付録 C「エラー メッセージおよびイベント メッセージ」では、CLI エラー メッセージおよびイベント メッセージのリストを示し、各メッセージの説明とその推奨処置を提示します。

表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ（[ ]）の中の要素は、省略可能です。
- 必ずいずれか 1 つを選択しなければならない要素は、波カッコ（{ }）で囲み、縦棒（|）で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って（[{ | }]）示しています。

対話形式の例では、次の表記法を使用しています。

- 端末セッションおよびシステムの表示は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の `screen` フォント**で示しています。
- 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（< >）で囲んで示しています。

（注）、注意、およびワンポイントアドバイスには、次の表記法および記号を使用しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

ヒント 問題の解決に役立つ情報です。ヒントは、トラブルシューティングの方法や実行すべきアクションを示すものではなくても、役立つ情報を提供している場合があります。

関連資料

- *『Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.3(3)JBB』*
- サポートされるアクセス ポイントごとに、必要に応じて、Cisco.com の対応するサポート ページに以下のタイプのガイドが提供されています。
  - 『Access Point Getting Started Guide』
  - 『Access Point Hardware Installation Guide』(『Getting Started Guide』でハードウェアの設置について説明されていない場合のみ)
  - 『Installation Instructions for Cisco Aironet Power Injectors』
  - 『Access Point Deployment Guide』
  - 『Cisco Aironet 802.11 a/b/g/n/ac Radio Installation and Upgrade Instructions』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

アクセス ポイント機能の概要

Cisco Aironet アクセス ポイント（これ以降は *アクセス ポイント*または略して *AP* と呼ぶ）は、安全で安価な使いやすい無線 LAN ソリューションを提供します。これはモビリティと柔軟性のほかに、ネットワーキングの専門家が必要とする企業クラスの機能を併せ持っています。Cisco IOS ソフトウェアをベースにした管理システムでは、Cisco Aironet アクセス ポイントは、Wi-Fi 認定済みであり、特定のモデルによって、802.11a 準拠、802.11b 準拠、802.11g 準拠、802.11n 準拠、または 802.11ac 準拠の無線 LAN トランシーバになります。

（注） 1530、1700、または 2700 シリーズ AP は、初回の起動時に、統合モードのソフトウェア イメージを使用して起動されます。自律ネットワークに AP を展開するには、AP コンソールまたは Telnet から次のコマンドを使用して、自律モードのソフトウェア イメージで AP を再起動させます。
capwap ap autonomous
AP のソフトウェア イメージの詳細については、「ソフトウェア イメージの操作」（P.20-21）を参照してください。

ワイヤレス デバイスは、コマンドライン インターフェイス（CLI）、ブラウザベースの管理システム、または 簡易ネットワーク管理プロトコル（SNMP）を使用して設定およびモニタできます。

アクセス ポイントの無線

アクセス ポイントは、無線ネットワークと有線ネットワーク間の接続ポイントとして、またはスタンドアロンの無線ネットワークのセントラル ポイントとして機能します。大規模な導入環境では、アクセス ポイントの無線範囲内であれば、無線ユーザは構内を移動しながらシームレスで遮断されないネットワーク アクセスを維持できます。

各アクセス ポイント プラットフォームには、1 台、2 台、または 3 台の無線が含まれます。各アクセス ポイント モデルでサポートされている無線の詳細については、そのモデルに対応する *アクセス ポイント データ シート*を参照してください。

このリリースの新機能およびプラットフォーム

このリリースで追加された新機能および既存の機能に対して行われた更新についての詳細は、次の URL にあるこのリリースの『*Release Notes for Autonomous Cisco Aironet Access Points and Bridges*』を参照してください。

このリリースでサポートされている CLI コマンドを網羅したリストについては、次の URL にあるこのリリースの『*Cisco IOS Command Reference for Autonomous Cisco Aironet Access Points and Bridges*』を参照してください。

（注）　Cisco IOS Release 12.3(2)JA 以降では、プロキシ モバイル IP 機能はサポートされません。

Cisco Aironet 700W シリーズ アクセス ポイントのサポート

- この AP は、802.11n デュアル無線 2 x 2 マルチインプット、マルチアウトプット（MIMO）テクノロジーをサポートしています。AP はアンテナが統合された状態で提供され、802.11a、b、g、n をサポートします。
- サポートされているモデルは 702W です。
- サポートされている動作モードは次のとおりです。
  - ルート
  - ルート ブリッジ
  - 非ルート ブリッジ
  - ワークグループ ブリッジ
  - スキャナ
  - スペクトル
  - リピータ

このアクセス ポイントの詳細については、

http://www.cisco.com/c/en/us/products/wireless/aironet-700w-series/index.html にアクセスしてください。

Cisco Aironet 1570 シリーズ

- この高度なキャリア クラスの屋外アクセス ポイントは、4x4 マルチインプット、マルチアウトプット（MIMO）のスマート アンテナ テクノロジーと 3 空間ストリームをサポートしており、最適なパフォーマンスを実現します。外部アンテナ オプションが統合されたこのアクセス ポイントは、802.11a、b、g、n、ac をサポートしています。
- サポートされているモデルは 1572IC、1572EC および 1572 EAC です。

- サポートされている動作モードは次のとおりです。
  - ルート
  - ルート ブリッジ
  - 非ルート ブリッジ
  - ワークグループ ブリッジ
  - スキャナ
  - スペクトル
  - リピータ

このアクセス ポイントの詳細については、次のページを参照してください。

http://www.cisco.com/go/ap1570

新しい機能とコマンド

Wi-Fi Certified Passpoint

このリリースには、Wi-Fi Certified Passpoint（Hotspot 2.0 とも呼ばれる）の基本サポートが備わっています。

Wi-Fi Certified Passpoint（Hotspot 2.0 とも呼ばれる）は、ホットスポットでのネットワーク アクセスを効率化し、ユーザが接続するたびにネットワークを見つけて認証を行う必要を排除します。Passpoint をサポートしていない Wi-Fi ネットワークでは、ユーザは毎回ネットワークを検索して選択し、アクセス ポイントへの接続を要求する必要があります。また多くの場合、認証クレデンシャルを再入力する必要もあります。Passpoint はそのプロセス全体を自動化し、ホットスポット ネットワークとモバイル デバイスとの間で、最高レベルの WPA2 セキュリティを適用したシームレスな接続を実現します。

現在のリリースでは、自動検出、802.1x 認証、およびセキュア接続がサポートされています。

設定情報については、「802.11u Hotspot および Hotspot 2.0 の設定」（P.12-30）を参照してください。

Cisco Aironet 1600 および 1570 シリーズ アクセス ポイントの Spectrum Expert

このリリースでは、Cisco Aironet 1600 シリーズ アクセス ポイントの Spectrum Expert モードをサポートしています。このモードでは、AP は Cisco Spectrum Expert コンソール（バージョン 4.1 以降）に接続できます。AP を、Cisco Spectrum Expert に接続するために使用する専用スペクトラム センサーとして設定できます。

Cisco Spectrum Expert の詳細については、次の URL にアクセスしてください。

http://www.cisco.com/c/en/us/support/wireless/spectrum-expert/tsd-products-support-series-home.html

Ethernet over GRE（EoGRE）

Ethernet over GRE（EoGRE）は、IP コア ネットワーク上で GRE ヘッダーにカプセル化されたレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。Generic Routing Encapsulation（GRE）は、レイヤ 3 IPv4 またはレイヤ 3 IPv6 アクセス ネットワーク上で仮想ポイントツーポイント リンクに多種多様なネットワーク レイヤ プロトコルをカプセル化するトンネリング プロトコルです。このリリースでは、Ethernet over GRE（EoGRE）設定を提供しています。第 22 章「Ethernet over GRE の設定」を参照してください。

高速ローミング用ワークグループ ブリッジの設定

高速鉄道車両でのローミングなど、高速ローミングのシナリオに対応するワークグループ ブリッジの設定方法の詳細については、「高速ローミングのためのワークグループ ブリッジの設定」（P.19-27）を参照してください。

（注）　高速ローミングのシナリオに対応するワークグループ ブリッジの設定が現在サポートされているのは、Cisco Aironet 3600 および 3700 シリーズ アクセス ポイントのみです。

無線ごとのクライアント数の制限

インターフェイスとのアソシエーションを許可するクライアントの数を設定できるようになりました。「無線ごとのクライアントの制限」（P.6-9）を参照してください。

非ネイティブ VLAN の管理 VLAN としての設定

非ネイティブ VLAN を管理 VLAN として設定する方法については、「管理 VLAN としての非ネイティブ VLAN の設定」（P.14-10）を参照してください。

常に TFTP サーバからコンフィギュレーション ファイルをダウンロードする

NVRAM（フラッシュ）にコンフィギュレーション ファイルが保管されている場合でも、常に TFTP サーバからコンフィギュレーション ファイル（config.txt）をダウンロードするように AP を設定できます。詳細については、「常に TFTP サーバからコンフィギュレーション ファイルをダウンロードする」（P.20-21）を参照してください。

常に TFTP サーバからソフトウェア イメージをダウンロードする

NVRAM（フラッシュ）にコンフィギュレーション ファイルが保管されている場合でも、常に TFTP サーバからソフトウェア イメージ ファイルをダウンロードするように AP を設定できます。詳細については、「常に TFTP サーバからソフトウェア イメージをダウンロードする」（P.20-38）を参照してください。

Cisco Aironet 1570 シリーズ アクセス ポイントのコマンド

Global Positioning System（GPS）モジュールおよび AP 1570 のケーブル モデムをサポートするために、以下のコマンドが導入されました。

コマンド	説明
show cmodemstatus	ケーブル モデムに関する次の情報を表示します。 • ソフトウェア バージョン • AP MAC アドレス • ケーブル モデムの MAC アドレス • イーサネット速度 • イーサネットのステータス • Data Over Cable Service Interface Specification（DOCSIS）登録ステータス • アップストリーム チャネル ステータス • ダウンストリーム チャネル ステータス
show gps location	GPS モジュールからの次の情報を表示します。 • GPS ロケーションの座標 • 収集時刻 • 位置フラグ • 緯度 • 経度 • 高度 • 東への速度 • 北への速度 • 上への速度

管理オプション

ワイヤレス デバイス管理システムは、次のインターフェイスから使用できます。

- Cisco IOS コマンドライン インターフェイス（CLI）。このインターフェイスはコンソール ポートまたは Telnet セッションを通じて使用します。無線デバイスを無線コンフィギュレーション モードにするには、**interface dot11radio** グローバル コンフィギュレーション コマンドを使用します。このマニュアルのほとんどの例は、CLI から引用されています。第 3 章「コマンドライン インターフェイスの使用」に、CLI についての詳細が記載されています。
- Web ブラウザ インターフェイスは、Web ブラウザを介して使用します。第 2 章「Web ブラウザ インターフェイスの使用方法」に、Web ブラウザ インターフェイスについての詳細が記載されています。

- 簡易ネットワーク管理プロトコル(SNMP).SNMP 管理のためのワイヤレス デバイスの設定方法については、第 18 章「SNMP の設定」を参照してください。

クライアント デバイスのローミング

無線 LAN に複数のワイヤレス デバイスがある場合、無線クライアント デバイスは、あるワイヤレス デバイスから別の無線デバイスへとシームレスにローミングできます。ローミング機能は、近接度ではなく、信号の品質に基づきます。クライアントからの信号品質が低下すると、ローミングは別のアクセス ポイントに切り替わります。

クライアント デバイスが近くのアクセス ポイントにローミングせずに、遠くのアクセス ポイントにアソシエートしたままになることを懸念する無線 LAN ユーザがいます。ただし、遠隔のアクセス ポイントへのクライアントの信号が強度に維持され、信号品質が高い場合、クライアントはより近いアクセス ポイントにローミングしません。近接するアクセス ポイントを常にチェックするのは非効率であり、無線のトラフィックの増加により無線 LAN のスループットを低下させます。

無線分散システム(WDS)を提供するデバイスで Cisco Centralized Key Management(CCKM)または 802.11r を使用すると、クライアント デバイスはアクセス ポイント間をすばやくローミングできるため、音声やその他の時間が重要なアプリケーションで、知覚できるほどの遅延は生じません。

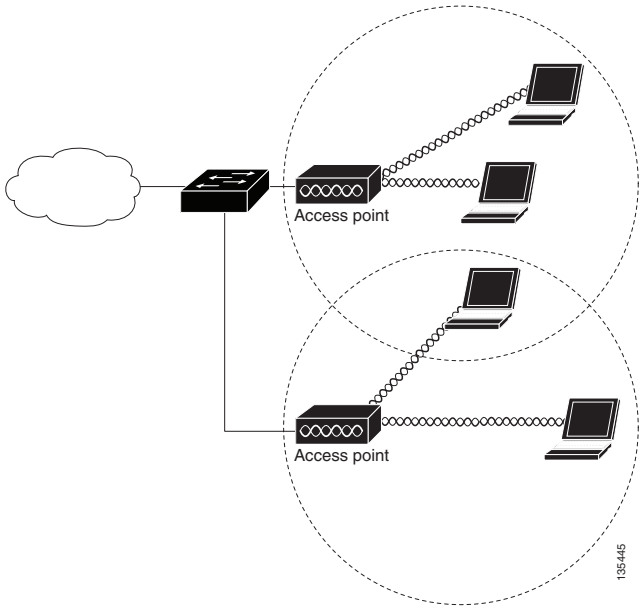
ネットワークの構成例

この項では、一般的な無線ネットワーク構成でのアクセス ポイントの役割について説明します。デフォルトでは、アクセス ポイントは、ワイヤード LAN に接続したルート ユニットとして、または完全なワイヤレス ネットワーク内のセントラル ユニットとして構成されます。アクセス ポイントは、リピータ アクセス ポイント、ブリッジ、およびワークグループとしても設定できます。これらの役割には特定の設定が必要です。

ルート アクセス ポイント

有線 LAN に直接接続されるアクセス ポイントは、無線ユーザへの接続ポイントとして機能します。LAN に複数のアクセス ポイントが接続されている場合、ユーザはネットワークへの接続を維持したまま、構内のエリアをローミングできます。1 つのアクセス ポイントの範囲外に移動したユーザは、自動的に別のアクセス ポイントを経由してネットワークに接続(アソシエート)されます。ローミング プロセスはシームレスで、ユーザには意識されません。図 1-1 は、有線 LAN 上でルート ユニットとして機能するアクセス ポイントを示しています。

図 1-1　有線 LAN 上でルート ユニットとして機能するアクセス ポイント

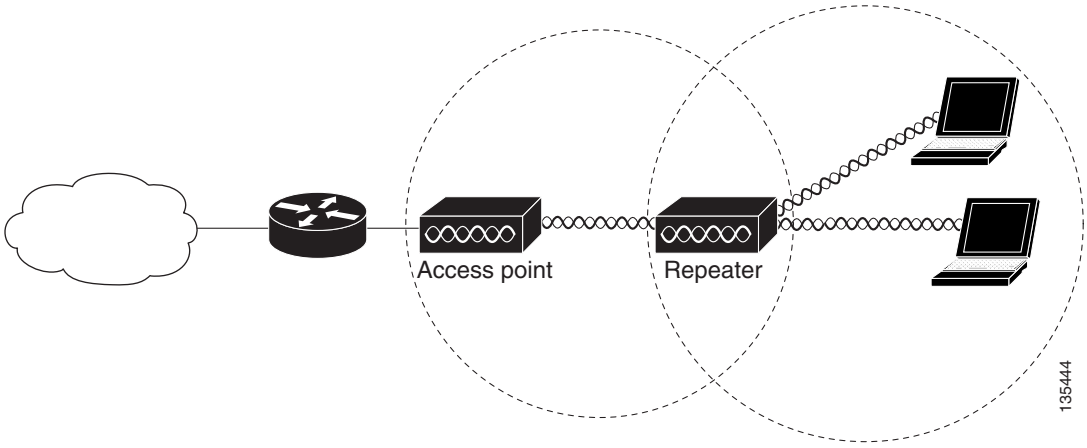


リピータ アクセス ポイント

アクセス ポイントは、インフラストラクチャの範囲を拡張したり、無線通信を妨害する障害を克服したりするスタンドアロン リピータとして設定できます。リピータは、別のリピータや、有線 LAN に接続されているアクセス ポイントにパケットを送信することによって、無線ユーザと有線 LAN との間でトラフィックを転送します。データは、クライアントに最高のパフォーマンスを提供するルートを経由して送信されます。図 1-2 は、リピータとして機能するアクセス ポイントを示しています。アクセス ポイントをリピータとして設定する方法については、「リピータ アクセス ポイントの設定」(P.19-3)を参照してください。

（注） シスコ以外のクライアント デバイスを使用すると、リピータ アクセス ポイントとの通信に問題が生じる可能性があります。

図 1-2　リピータとして機能するアクセス ポイント



ブリッジ

アクセス ポイントは、ルート ブリッジまたは非ルート ブリッジとして設定できます。この役割では、アクセス ポイントは非ルート ブリッジとの無線リンクを確立します。トラフィックはリンク経由で有線 LAN に転送されます。ルート ブリッジおよび非ルート ブリッジの役割を持つアクセス ポイントは、クライアントからのアソシエーションを受け入れるように設定できます。図 1-3 は、クライアントとのルート ブリッジとして設定されたアクセス ポイントを示しています。図 1-4 は、ルート ブリッジおよび非ルート ブリッジとして設定され、いずれもクライアント アソシエーションを受け付ける 2 つのアクセス ポイントを示しています。アクセス ポイントをブリッジとして設定する方法については、「無線ネットワークの役割の設定」(P.6-3)を参照してください。

無線ブリッジがポイントツーマルチポイント構成に使用される場合、ルート ブリッジにアソシエートする非ルート ブリッジの数に応じてスループットは減少します。リンクのデータ レートが 54 Mbps の場合、ポイントツーポイント リンクでの最大スループットは約 25 Mbps です。3 つのブリッジを追加してポイントツーマルチポイント ネットワークを形成すると、スループットは約 12.5Mbps に減少します。

図 1-3　クライアントとのルート ブリッジとして機能するアクセス ポイント

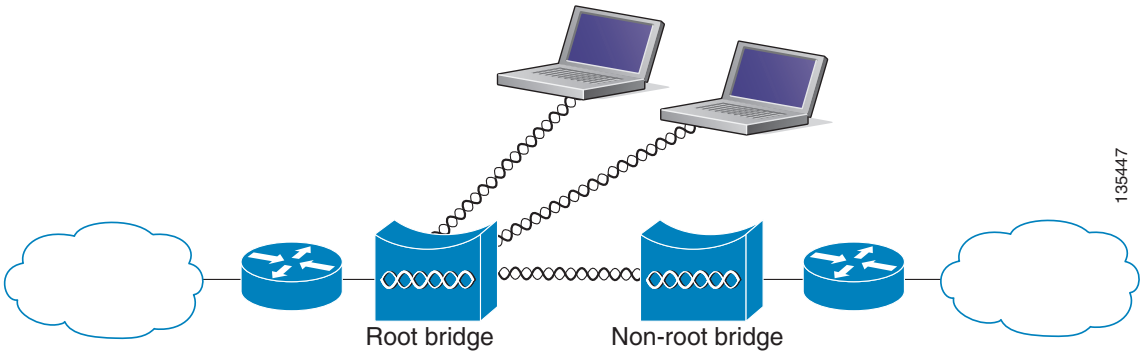
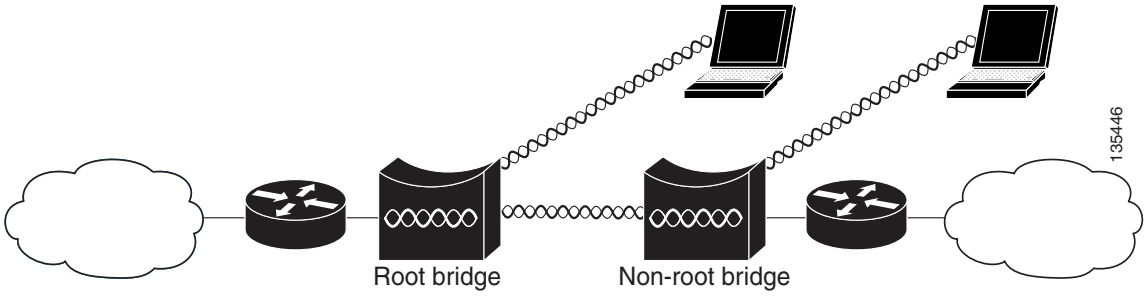


図 1-4　クライアントとのルート ブリッジおよび非ルート ブリッジとして機能するアクセス ポイント



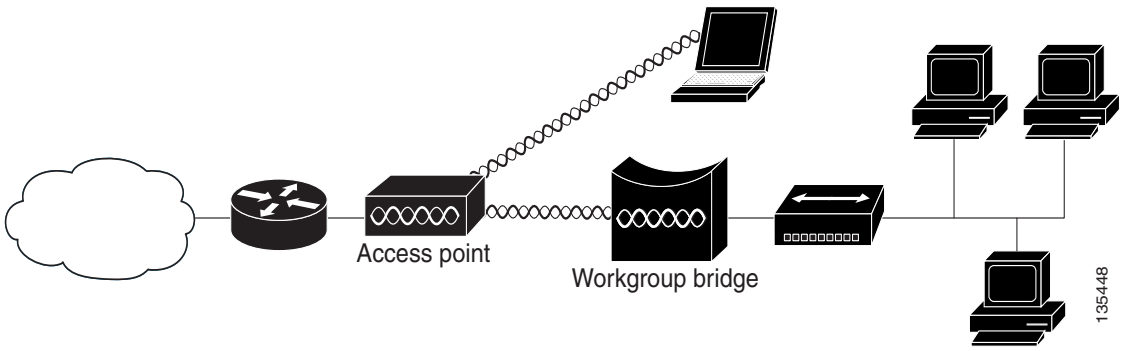
ワークグループ ブリッジ

アクセス ポイントをワークグループ ブリッジとして設定できます。ワークグループ ブリッジ モードのアクセス ポイントは、別のアクセス ポイントにクライアントとしてアソシエートして、イーサネット ポートに接続されたデバイスをネットワークに接続します。たとえば、ネットワーク プリンタのグループを無線で接続する必要がある場合は、プリンタをハブまたはスイッチに接続し、ハブまたはスイッチをアクセス ポイントのイーサネット ポートに接続し、そのアクセス ポイントをワークグループ ブリッジとして設定します。ワークグループ ブリッジはネットワーク上のアクセス ポイントにアソシエートします。

アクセス ポイントに複数の無線がある場合、いずれかの無線がワークグループ ブリッジ モードとして機能できます。

図 1-5 は、ワークグループ ブリッジとして設定されたアクセス ポイントを示しています。アクセス ポイントをワークグループ ブリッジとして設定することについては、「ワークグループ ブリッジ モードの概要」(P.19-14)および「ワークグループ ブリッジ モードの設定」(P.19-20)を参照してください。

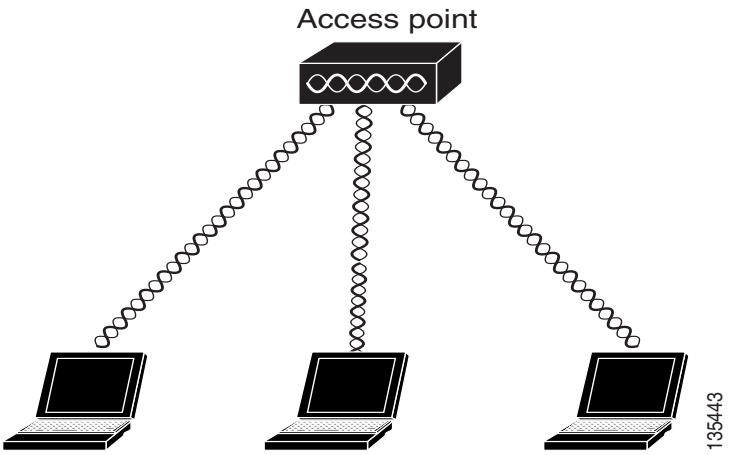
図 1-5　　ワークグループ ブリッジとして機能するアクセス ポイント



全ワイヤレス ネットワークの中央ユニット

完全なワイヤレス ネットワークでは、アクセス ポイントはスタンドアロンのルート ユニットとして機能します。アクセス ポイントは有線 LAN には接続されません。全ステーションをまとめてリンクするハブとして機能します。アクセス ポイントは通信の中心として機能し、無線ユーザの通信範囲を拡張します。図 1-6 は、完全なワイヤレス ネットワークでのアクセス ポイントを示しています。

図 1-6　完全なワイヤレス ネットワークでセントラル ユニットとして機能するアクセス ポイント



CHAPTER 2

Web ブラウザ インターフェイスの使用方法

この章では、ワイヤレス デバイスの設定に使用できる Web ブラウザ インターフェイスについて説明します。

Web ブラウザ インターフェイスには、ワイヤレス デバイスの設定の変更、ファームウェアのアップグレード、およびネットワーク上の他の無線デバイスのモニタと設定に使用する管理ページが含まれます。

（注） ワイヤレス デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 と Mozilla Firefox バージョン 17 と完全に互換性があります。

（注） ワイヤレス デバイスの設定に、CLI と Web ブラウザ インターフェイスの両方を使用することは避けてください。CLI を使用してワイヤレス デバイスを設定した場合、Web ブラウザ インターフェイスでは、設定が正しく表示されない場合があります。しかし、正しく表示されない場合でも、ワイヤレス デバイスは正しく設定されていることがあります。

初めて Web ブラウザ インターフェイスを使用する場合

ワイヤレス デバイスの IP アドレスを使用して、管理システムを参照します。IP アドレスをワイヤレス デバイスに割り当てる方法は、「アクセス ポイントへのログイン」(P.4-3)を参照してください。Web ブラウザ インターフェイスの使用を開始する手順は、次のとおりです。

ステップ 1　ブラウザを起動します。

ステップ 2　アドレス バーにワイヤレス デバイスの IP アドレスを入力し、**Enter** キーを押します。[Summary Status] ページが表示されます。

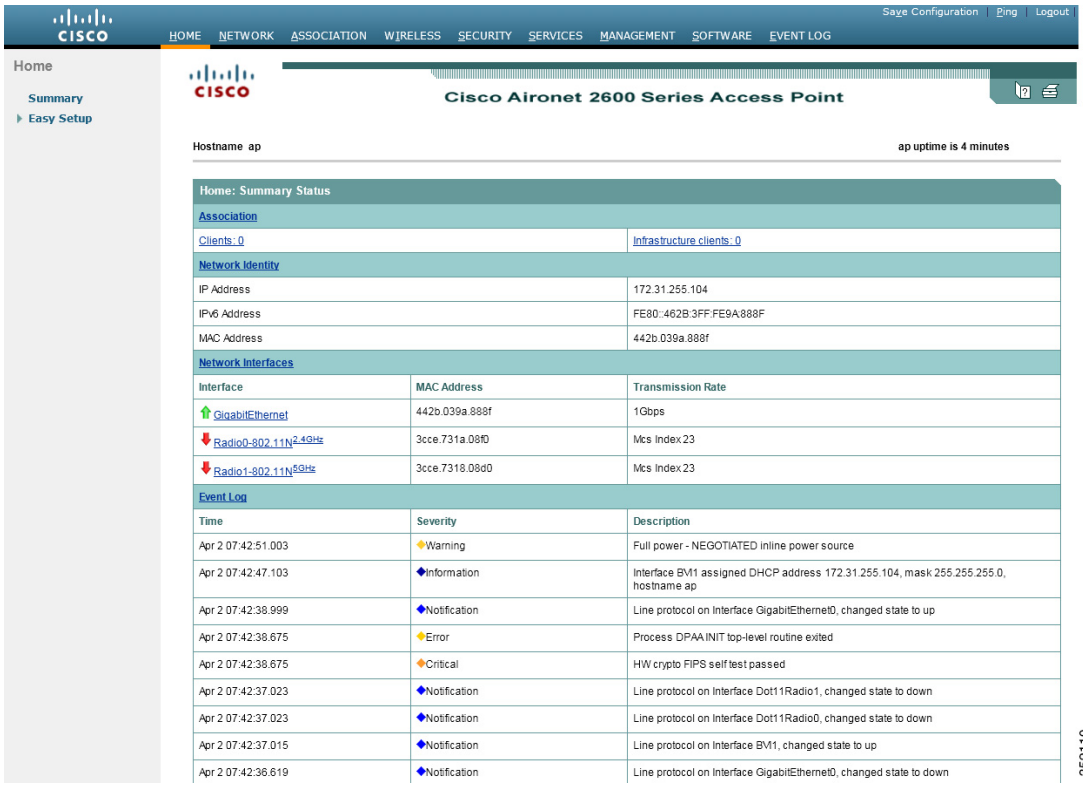
Web ブラウザ インターフェイスの管理ページの使用方法

システム管理ページでの設定情報の表示と保存には、一貫性のある手法が使用されています。ページの上部にあるナビゲーション バーを使用して、メイン メニューのオプションを選択できます。ページの左側にもナビゲーション バーがあります。これは、サブ メニューをナビゲートするために使用します。ナビゲーション バーは他の管理ページへ移動する場合に使用し、設定アクション ボタンは設定の変更を保存またはキャンセルする場合に使用します。

（注）　Web ブラウザの [Back] ボタンをクリックすると前のページに戻りますが、変更内容は保存されないことに留意してください。[Cancel] をクリックすると、ページで行った変更はすべてキャンセルされ、ページの移動は行われません。変更は、[Apply] をクリックした場合にだけ適用されます。

図 2-1 は、Web ブラウザ インターフェイスのホーム ページを示しています。

図 2-1　Web ブラウザ インターフェイスのホーム ページ



アクション ボタンの使用方法

表 2-1は、管理ページに表示されるページ リンクとボタンの一覧を示しています。

表 2-1　管理ページのボタンとリンク

ボタン/リンク	説明
ナビゲーション リンク	
Home	ワイヤレス デバイスにアソシエートされた無線デバイスの数、イーサネットおよび無線インターフェイスのステータス、最近のワイヤレス デバイスの活動リストを示す、ワイヤレス デバイスのステータス ページを表示します。
Easy Setup	システム名、IP アドレス、無線ネットワークでの役割などの基本的な設定を行う [Express Setup] ページを表示します。
Network	無線 LAN のインフラストラクチャ デバイスのリストを表示します。アクセス ポイント インターフェイス(無線とイーサネット)の設定サブメニューがあります。
Association	無線 LAN 上のすべてのデバイスのシステム名、ネットワークでの役割、および親とクライアントの関連性を示すリストを表示します。
Wireless	無線ドメイン サービスの設定とデバイスの要約を表示し、WDS の設定ページへのリンクを示します。

表 2-1　　管理ページのボタンとリンク（続き）

ボタン/リンク	説明
Security	セキュリティ設定の要約を表示し、セキュリティ設定ページへのリンクを提示します。
Services	いくつかの無線デバイス機能のステータスを表示し、Telnet/SSH、CDP、ドメイン ネーム サーバ、フィルタ、QoS、SNMP、SNTP、および VLAN の設定ページへのリンクを示します。
Management	現在のゲスト ユーザのリストを表示し、ゲスト ユーザの設定ページおよび Web 認証ページへのリンクを示します。
Software	無線デバイスで実行されているファームウェアのバージョン番号を表示し、ファームウェアをアップグレードおよび管理するための設定ページへのリンクを示します。
Event Log	無線デバイスのイベント ログを表示し、トラップに含めるイベントの選択、イベントの重大レベルの設定、通知方法の設定を行う設定ページへのリンクを示します。
設定アクション ボタン	
Apply	そのページに加えた変更を保存し、ページをそのまま表示します。
Refresh	ページに表示されるステータス情報または統計を更新します。
Cancel	そのページに加えた変更を廃棄し、ページをそのまま表示します。
Back	そのページに加えた変更を廃棄し、直前のページに戻ります。
Logout	AP 設定を保存せずに AP 設定 Web インターフェイスを終了します。
ping	IPv4 または IPv6 アドレスへの ping を実行します。
Save Configuration	AP の現在の設定を NVRAM に保存します。

入力フィールドの文字制限

Web ブラウザ インターフェイスの入力フィールドで、次の文字を使用することはできません。この制限は、Cisco IOS ソフトウェアを使用するアクセス ポイントのすべてに適用されます。

」
]
+
/

タブ

末尾のスペース

安全なブラウザ利用のための HTTPS の有効化

HTTPS を有効にすることで、アクセス ポイントの Web ブラウザ インターフェイスとの通信を保護できます。HTTPS は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。

（注） HTTPS を有効にすると、ブラウザとアクセス ポイントの接続が解除される可能性があります。接続が解除された場合は、ブラウザのアドレス入力用ボックスの URL を「http://*ip_address*」から「**https://*ip_address***」に変更し、アクセス ポイントに再びログインします。

（注） HTTPS を有効にした場合、大部分のブラウザでは、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を持たないデバイスを参照するたびに、承認を求めるプロンプトが表示されます。承認を求めるプロンプトが表示されないようにするには、次の手順の説明に従って、アクセス ポイントの FQDN を作成します。

FQDN を作成し、HTTPS を有効にする手順は、次のとおりです。

ステップ 1　ブラウザでポップアップ ブロッキング ソフトウェアを使用している場合は、ポップアップ ブロッキング機能を無効にします。

ステップ 2　[Easy Setup] > [Network Configuration] を選択します。

[Network Configuration] ページが表示されます。

ステップ 3　[Host Name] フィールドにアクセス ポイントの名前を入力し、[Apply] をクリックします。

ステップ 4　[Services] > [DNS] ページを選択します。

[Services: DNS - Domain Name Service] ページが表示されます。

ステップ 5　[Domain Name System (DNS)] フィールドで、[Enable] オプション ボタンをクリックします。

ステップ 6　[Domain Name] フィールドに、会社のドメイン名を入力します。

ステップ 7　[Name Server IPv4/IPv6 Addresses] フィールドに、DNS サーバの IP アドレスを 1 つ以上入力します。

ステップ 8　[Apply] をクリックします。

アクセス ポイントの FQDN は、システム名とドメイン名を組み合わせたものです。たとえば、システム名が *ap3600*、ドメイン名が *company.com* の場合、FQDN は *ap3600.company.com* です。

ステップ 9　DNS サーバの FQDN を入力します。

ヒント　DNS サーバがない場合は、ダイナミック DNS サービスを使用してアクセス ポイントの FQDN を登録できます。インターネットで*ダイナミック DNS* を検索し、有料の DNS サービスを見つけてください。

ステップ 10　[Services] > [HTTP] を選択します。

[Services: HTTP - Web Server] ページが表示されます。

ステップ 11　[Web-based Configuration Management] フィールドで、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにします。

ステップ 12　[Domain Name] フィールドにドメイン名を入力し、[Apply] をクリックします。

（注）　HTTPS を有効にすると、自動的に HTTP が無効になります。HTTPS が有効にされた状態で HTTP アクセスを維持するには、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにしてから、[Enable Standard (HTTP) Browsing] チェックボックスをオンにします。標準 HTTP と HTTPS の両方を有効にできますが、いずれか一方のみを有効にすることを推奨します。

警告メッセージが表示され、以降はアクセス ポイントの参照にセキュア HTTP が使用されることが伝えられます。警告メッセージには、*https* を含む新しい URL も表示されます。アクセス ポイントを参照するには、この URL を使用する必要があります。

ステップ 13　警告メッセージ ボックスで [OK] をクリックします。

ブラウザのアドレス入力用ボックスのアドレスが、*http://*<ip-address> から *https://*<ip-address> に変更されます。

ステップ 14　別の警告メッセージが表示され、アクセス ポイントのセキュリティ証明書が、信頼できる認証局によって発行されたものではないことが伝えられます。ただし、この警告メッセージは無視できます。[Continue to this Website（not recommended）] をクリックします。

（注）　次の手順では、Microsoft Internet Explorer を使用していることを前提としています。そうでない場合は、自己署名証明書を使用した Web サイトへのアクセス方法の詳細について、ご使用のブラウザのマニュアルを参照してください。

ステップ 15　アクセス ポイントのログイン ウィンドウが表示されます。アクセス ポイントに再びログインします。デフォルトのユーザ名 は *Cisco*（大文字小文字を区別）、デフォルトのパスワードは *Cisco*（大文字小文字を区別）です。

ステップ 16　アクセス ポイントのセキュリティ証明書を表示するには、アドレス バーの [Certificate error] アイコンをクリックします。

ステップ 17　[View Certificate] をクリックします。

ステップ 18　[Certificate] ウィンドウで、[Install Certificate] をクリックします。
Microsoft Windows の証明書のインポート ウィザードが表示されます。

ステップ 19　[Next] をクリックします。
次に表示される画面では、証明書を保管する場所を確認されます。システムのデフォルトの保管領域を使用することを推奨します。

ステップ 20　[Next] をクリックし、デフォルトの保管領域を承認します。
これで、正常に証明書がインポートされます。

ステップ 21　[Finish] をクリックします。
セキュリティ警告が表示されます。

ステップ 22　[Yes] をクリックします。
インストールが成功したことを示すメッセージ ボックスが表示されます。

ステップ 23　[OK] をクリックします。

CLI の設定例

次の例は、「安全なブラウザ利用のための HTTPS の有効化」(P.2-5) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# hostname ap3600
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

この例では、アクセス ポイントのシステム名は *ap3600*、ドメイン名は *company.com*、DNS サーバの IP アドレスは 10.91.107.18 です。

この例で使用されているコマンドの詳細については、リリース 12.4 の『Cisco IOS Commands Master List』を参照してください。次のリンクをクリックすると、コマンドのマスター リストを参照できます。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124htnml.htm

HTTPS 証明書の削除

HTTPS を有効にすると、アクセス ポイントは証明書を自動的に生成します。ただし、HTTPS を有効にした後でアクセス ポイントの完全修飾ドメイン名 (FQDN) を変更したり、FQDN を追加したりする必要が生じた場合、証明書の削除が必要になることがあります。手順は次のとおりです。

ステップ 1　[Services: HTTP Web Server] ページを表示します。

ステップ 2　[Enable Secure (HTTPS) Browsing] チェックボックスをオフにし、HTTPS を無効にします。

ステップ 3　[Delete Partial SSL certificate] をクリックして証明書を削除します。

ステップ 4　[Apply] をクリックします。アクセス ポイントは、新しい FQDN を使用して新しい証明書を生成します。

HTTPS 証明書を削除する CLI コマンド

グローバル コンフィギュレーション モードでは、次のコマンドを使用して HTTPS 証明書を削除します。

	コマンド	目的
ステップ 1	**no ip http secure-server**	HTTPS を無効にします。
ステップ 2	**crypto key zeroize rsa** *name-of-rsa-key*	HTTP サーバ用の RSA キーを削除します。さらに、削除されるキーを使用して発行されたルータ証明書 (HTTPS 証明書) もすべて削除されます。

オンライン ユーザ ガイドの使用

Web ブラウザ インターフェイスで、ホーム ページの上部にあるヘルプ アイコンをクリックすると、このガイドのオンライン バージョン（『Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points』）にアクセスできます。ガイドをオンラインで表示することも、PDF バージョンのガイドをダウンロードしてオフラインで参照することもできます。オンライン ガイドは定期的に更新されるため、最新の情報を入手できます。

Web ブラウザ インターフェイスの無効化

Web ブラウザ インターフェイスの使用をすべて中止するには、[Services: HTTP-Web Server] ページで [Disable Web-Based Management] チェックボックスをオンにし、[Apply] をクリックします。

Web ブラウザ インターフェイスを再び有効にするには、アクセス ポイントの CLI で次のグローバル コンフィギュレーション コマンドを入力します。

```
ap(config)# ip http server
```

コマンドライン インターフェイスの使用

この章では、ワイヤレス デバイスの設定に使用できる Cisco IOS コマンドライン インターフェイス（CLI）について説明します。

Cisco IOS コマンド モード

Cisco IOS ユーザ インターフェイスには多くのモードがあります。使用できるコマンドの種類は、現在のモードによって異なります。システム プロンプトに疑問符(?)を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

ワイヤレス デバイスでセッションを開始すると、ユーザ モードになります。このモードは、通常、*ユーザ EXEC モード*と呼ばれます。ユーザ EXEC モードでは、Cisco IOS コマンドのサブセットを利用することができます。たとえば、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。ユーザ EXEC コマンドは、ワイヤレス デバイスをリブートするときには保存されません。

すべてのコマンドにアクセスする場合は、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードを開始していなければなりません。

コンフィギュレーション モード(グローバル、インターフェイス、およびライン)を使用して、実行コンフィギュレーションを変更できます。設定を保存した場合はこれらのコマンドが保存され、ワイヤレス デバイスをリブートするときに使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

表 3-1 は主なコマンド モードと、それぞれのモードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法をまとめたものです。表内の例では、ホスト名に *ap* を使用しています。

表 3-1　　コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	ワイヤレス デバイスでセッションを開始します。	`ap>`	**logout** または **quit** を入力します。	このモードは次の場合に使用します。 • ターミナルの設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードで、**enable** コマンドを入力します。	`ap#`	**disable** を入力して終了します。	このモードは、コマンドの確認に使用します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、**configure** コマンドを入力します。	`ap(config)#`	終了して特権 EXEC モードに戻るには、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。	このモードは、ワイヤレス デバイス全体に適用するパラメータを設定する場合に使用します。

表 3-1　　コマンド モードの概要（続き）

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、**interface** コマンドを入力し、インターフェイスを指定します。	`ap(config-if)#`	終了してグローバル コンフィギュレーション モードに戻るには、**exit** を入力します。特権 EXEC モードに戻るには、Ctrl+Z を押すか、**end** を入力します。	このモードは、イーサネットおよび無線インターフェイスのパラメータを設定する場合に使用します。 2.4 GHz 無線および 802.11n 2.4 GHz 無線は無線 0 です。 5 GHz 無線および 802.11n 5 GHz 無線は無線 1 です。

ヘルプの表示

システム プロンプトで疑問符(?)を入力すると、各コマンド モードに使用できるコマンドのリストが表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。表 3-2 を参照してください。

表 3-2　　ヘルプの概要

コマンド	目的
help	コマンド モードのヘルプ システムの簡単な説明を表示します。

*コマンドの先頭部分***?**	特定のストリングで始まるコマンドのリストを表示します。
	次に例を示します。
	`ap# di?`
	`dir  disable  disconnect`

コマンドの先頭部分<Tab>	特定のコマンド名を補完します。
	次に例を示します。
	`ap# sh conf<tab>`
	`ap# show configuration`

?	特定のコマンド モードで使用可能なすべてのコマンドをリストします。 次に例を示します。 `ap> ?`
command **?**	コマンドに関連するキーワードを一覧表示します。 次に例を示します。 `ap> show ?`

*command keyword***?**	キーワードに関連する引数を一覧表示します。
	次に例を示します。
	`ap(config)# cdp holdtime ?`
	`<10-255>  Length of time (in sec) that receiver must keep this packet`

コマンドの短縮形

ワイヤレス デバイスでコマンドが一意に認識される長さまでコマンドを入力します。次の例は、**show configuration** 特権 EXEC コマンドの入力方法を示しています。

```
ap# show conf
```

コマンドの no 形式および default 形式の使用

ほとんどのコンフィギュレーション コマンドに **no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、インターフェイス コンフィギュレーション コマンド **no shutdown** を使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** を指定せずにコマンドを使用すると、ディセーブルにした機能が再びイネーブルになり、また、デフォルトでディセーブルに設定されている機能がイネーブルになります。

コンフィギュレーション コマンドには、*default* 形式もあります。コマンドの default 形式は、コマンドの設定値をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、default 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、default コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

CLI メッセージの概要

表 3-3 は、CLI を使用してワイヤレス デバイスを設定しているときに表示されるエラー メッセージの一部を示しています。

表 3-3　　CLI の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	ワイヤレス デバイスがコマンドとして認識できるだけの長さの文字が入力されていません。	コマンドの後ろに 1 スペース空けて疑問符（**?**）を入力します。 コマンドとともに入力できる利用可能なキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドの後ろに 1 スペース空けて疑問符（**?**）を入力します。 コマンドとともに入力できる利用可能なキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。間違っている箇所をキャレット（^）記号で示しています。	疑問符（**?**）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに入力できる利用可能なキーワードが表示されます。

コマンド履歴の使用方法

CLI は、入力されたコマンドの履歴を保存します。この機能は、アクセス リストなど、長いまたは複雑なコマンドやエントリを呼び出す場合、特に便利です。コマンド履歴機能は、次の項で説明するように要件に合わせてカスタマイズできます。

コマンド履歴バッファ サイズの変更

デフォルトでは、ワイヤレス デバイスは履歴バッファにコマンド ライン 10 行を記録します。特権 EXEC モードで次のコマンドを入力して、現在のターミナル セッションでワイヤレス デバイスが記録するコマンド ライン数を変更します。

```
ap# terminal history [size number-of-lines]
```

範囲は 0 ～ 256 です。

特定のライン上のすべてのセッションでワイヤレス デバイスが記録するコマンド ライン数を設定するには、ライン コンフィギュレーション モードから次のコマンドを入力します。

```
ap(config-line)# history [size number-of-lines]
```

範囲は 0 ～ 256 です。

コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、表 3-4にリストされているいずれかの操作を行います。

表 3-4　　コマンドの呼び出し

操作[1]	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファに保存されているコマンドを、最新のコマンドから順に呼び出します。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	**Ctrl+P** キーまたは↑キーを使用してコマンドを呼び出した後、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
show history	特権 EXEC モードで、直前に入力したいくつかのコマンドを表示します。表示されるコマンドの数は、グローバル コンフィギュレーション コマンド **terminal history** および回線コンフィギュレーション コマンド **history** の設定によって決まります。

1. 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。

現在の端末セッションでこの機能をディセーブルにするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを使用します。

編集機能の使用方法

ここでは、コマンドラインの操作に役立つ編集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。

編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、ディセーブルにできます。

現在の端末セッションで拡張編集モードを再びイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
ap# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
ap(config-line)# editing
```

拡張編集モードをグローバルにディセーブルにするには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
ap(config-line)# no editing
```

キー入力によるコマンドの編集

表 3-5 は、コマンド ラインの編集に必要なキー入力を示しています。

表 3-5　　キー入力によるコマンドの編集

機能	キーストローク[1]	目的
コマンドライン上を移動して、変更または訂正を行います。	**Ctrl+B** キーまたは← キー	カーソルを 1 文字分だけ後ろに戻します。
	Ctrl+F キーまたは→ キー	カーソルを 1 文字分だけ前に進めます。
	Ctrl+A	カーソルをコマンドラインの先頭に移動させます。
	Ctrl+E	カーソルをコマンドラインの末尾に移動させます。
	Esc B	カーソルを 1 ワード分だけ後ろに戻します。
	Esc F	カーソルを 1 ワード分だけ前に進めます。
	Ctrl+T	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
バッファからコマンドを呼び出し、コマンドラインにペーストします。ワイヤレス デバイスは、直前に削除された 10 項目をバッファに入れます。	**Ctrl+Y**	バッファから最新のエントリを呼び出します。
	Esc Y	バッファから次のエントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。**Esc+Y** を 11 回以上押すと、最初のバッファ エントリに戻って表示されます。
不要なエントリを削除します。	**Delete** または **Backspace**	カーソルの左にある文字を消去します。
	Ctrl+D	カーソル位置にある文字を削除します。
	Ctrl+K	カーソル位置からコマンドラインの末尾までの全文字を削除します。
	Ctrl+U または **Ctrl+X**	カーソル位置からコマンドラインの先頭までの全文字を削除します。
	Ctrl+W	カーソルの左にあるワードを消去します。
	Esc D	カーソル位置からワードの末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	**Esc C**	カーソル位置のワードを大文字にします。
	Esc L	カーソル位置のワードを小文字に変更します。
	Esc U	カーソル位置からワードの末尾までの文字を大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	**Ctrl+V** または **Esc Q**	

表 3-5　キー入力によるコマンドの編集（続き）

機能	キーストローク[1]	目的
1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。 （注）　**show** コマンドの出力など、ターミナル画面で表示しきれない行のある出力には、`More` プロンプトが表示されます。`More` プロンプトが表示されている場合は、いつでも **Return** および **Space** バーを使用できます。	**Return**	1 行下へスクロールします。
	Space	1 画面下へスクロールします。
ワイヤレス デバイスから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示する。	**Ctrl+L** または **Ctrl+R**	現在のコマンドラインを再表示します。

1. 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

画面幅よりも長いコマンドラインの編集

画面上で複数行にわたるコマンドに対して折り返し機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。

コマンドの先頭にスクロールして入力内容をチェックするには、**Ctrl+B** キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、**Ctrl+A** を押します。

（注）　矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンド エントリが 1 行分よりも長くなっています。最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号($)は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、**Ctrl+A** を押して全体の構文をチェックし、その後 **Return** キーを押してコマンドを実行してください。行末に表示されるドル記号($)は、その行が右へスクロールされたことを表します。

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。それ以外の幅の場合は、特権 EXEC コマンド **terminal width** を使用してターミナルの幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンド エントリを呼び出して変更できます。前に入力したコマンド エントリの呼び出し方法については、「キー入力によるコマンドの編集」(P.3-7) を参照してください。

show および more コマンド出力の検索およびフィルタリング

show コマンドおよび **more** コマンドの出力を検索してフィルタリングできます。この機能は、大量の出力をソートしたり、表示する必要のない出力を除外したりする場合に便利です。

この機能を使用するには、**show** または **more** コマンドを入力した後、*パイプ*記号(|)、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列(検索またはフィルタの条件)を指定します。

command **|** {**begin** | **include** | **exclude**} *regular-expression*

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

次に、*protocol* が使用されている行だけを出力するように指定する例を示します。

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

CLI のアクセス

ワイヤレス デバイスの CLI は、Telnet またはセキュア シェル(SSH)を使用して開くことができます。

Telnet を使用して CLI を開く

Telnet を使用して CLI を開く手順は、次のとおりです。これらの手順は、Microsoft Windows を実行する PC で Telnet 端末アプリケーションを使用する場合を想定しています。オペレーティング システムの詳細な操作方法については、ご使用の PC の操作マニュアルを確認してください。

ステップ 1　[Start] > [Programs] > [Accessories] > [Telnet] の順に選択します。

[Accessories] メニューに Telnet がない場合は、[Start] > [Run] の順に選択し、入力フィールドに **Telnet** と入力して Enter を押します。

ステップ 2　[Telnet] ウィンドウで、**open** の後にワイヤレス デバイスの IP アドレスを入力し、**Enter** キーを押します。

ステップ 3　ユーザ名とパスワードが要求されたら、管理者のユーザ名とパスワードを入力します。デフォルトのユーザ名は **Cisco**、デフォルトのパスワードは **Cisco** です。デフォルトのイネーブル パスワードも **Cisco** です。ユーザ名とパスワードでは、大文字と小文字が区別されます。

セキュア シェルを使用して CLI を開く

セキュア シェル プロトコルは、ネットワーキング デバイスとの安全なリモート接続を可能にするプロトコルです。セキュア シェル（SSH）は、セッション全体を暗号化することによって、安全なログイン セッションを実現するソフトウェア パッケージです。SSH は、強力な暗号の認証、強力な暗号化、および完全性保護を特長としています。SSH の詳細は、SSH Communications Security, Ltd. のホームページ（http://www.ssh.com/）を参照してください。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。このリリースでは SSH バージョン 1 および 2 がサポートされています。ワイヤレス デバイスの SSH アクセスに関する設定手順の詳細は、「アクセス ポイントのセキュア シェルの設定」（P.5-29）を参照してください。

アクセス ポイントの最初の設定

この章では、最初にワイヤレス デバイス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、ワイヤレス デバイスに付属するクイック スタート ガイドの説明と共通する箇所があります。この章で説明する設定はすべて CLI を使用して実行できますが、ワイヤレス デバイスの Web ブラウザ インターフェイスで初期設定を完了してから、CLI を使用して詳細設定を追加入力する方が簡単な場合があります。

（注） アクセス ポイントの無線インターフェイスはデフォルトで無効になっています。

はじめる前に

ワイヤレス デバイスを設置する前に、使用しているコンピュータがこのワイヤレス デバイスと同じネットワークに接続されていることを確認し、ネットワーク管理者から次の情報を取得してください。

- ワイヤレス デバイスのシステム名
- 大文字と小文字を区別する、無線ネットワークの無線 Service Set Identifier（SSID; サービス セット ID）
- DHCP サーバに接続されていない場合は、ワイヤレス デバイスの一意の IP アドレス（172.17.255.115 など）
- ワイヤレス デバイスが PC と同じサブネット上にない場合、デフォルト ゲートウェイ アドレスとサブネット マスク
- 簡易ネットワーク管理プロトコル（SNMP）コミュニティ名と SNMP ファイル属性（SNMP を使用している場合）
- Cisco IP Setup Utility（IPSU）を使用して、ワイヤレス デバイスの IP アドレスを検索する場合、アクセス ポイントの MAC アドレス。MAC アドレスは、アクセス ポイントの底面ラベルに記載されています（00164625854c など）。

デバイスのデフォルト設定へのリセット

初期設定時に最初からやり直す必要がある場合は、アクセス ポイントをデフォルト設定にリセットすることができます。

MODE ボタンを使用したデフォルト設定へのリセット

（注）　MODE ボタンを使用したデフォルト設定へのリセットは、自律モードのアクセス ポイントにのみ適用されます。Lightweight モードのアクセス ポイントには適用されません。

アクセス ポイントの MODE ボタンを使用して、アクセス ポイント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　アクセス ポイントの電源（外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル）を切ります。

ステップ 2　MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。

ステップ 3　MODE ボタンを押し続けて、ステータス LED がオレンジに変わったら（約 1 ～ 2 秒かかります）ボタンを放します。アクセス ポイントのすべての設定が、デフォルトに戻ります。

GUI を使用したデフォルト設定へのリセット

アクセス ポイントの GUI を使用してデフォルトの設定に戻す手順は、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。
無線デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 と Mozilla Firefox バージョン 17 と完全に互換性があります。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力して、**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 **Cisco** です。

ステップ 4　[Password] フィールドにワイヤレス デバイスのパスワードを入力し、**Enter** を押します。デフォルトのパスワードは **Cisco** です。[Summary Status] ページが表示されます。

ステップ 5　[Software] をクリックして [System Software] 画面を表示します。

ステップ 6　[System Configuration] をクリックして、[System Configuration] 画面を表示します。

ステップ 7　[Reset to Defaults] ボタンをクリックすると、IP アドレスを含むすべての設定がデフォルト値にリセットされます。IP アドレスを除いたすべての設定をデフォルト値にリセットするには、[Reset to Defaults (Except IP)] ボタンをクリックします。

CLI を使用したデフォルト設定へのリセット

注意　デフォルトにリセットまたはソフトウェアをリロードする前に、システム ファイルを削除しないでください。

アクセス ポイントをデフォルト設定および静的 IP アドレスにリセットする場合、*write erase* または *erase /all nvram* コマンドを使用します。静的 IP アドレスなどすべてを消去する場合、上記のコマンドの他に、*erase* および *erase boot static-ipaddr static-ipmask* コマンドを使用します。

特権 EXEC モードからは、CLI を使用して次の手順でアクセス ポイント/ブリッジの設定をデフォルト値にリセットできます。

ステップ 1　**erase nvram** を入力して、スタートアップ コンフィギュレーションを含むすべての NVRAM ファイルを消去します。

（注）　**erase nvram** コマンドでは、静的 IP アドレスは消去されません。

ステップ 2　静的 IP アドレスおよびサブネット マスクを消去するには、次の手順を実行します。それ以外の場合は、ステップ 3 に進みます。

a. **write default-config** と入力します。

ステップ 3　「*Erasing the nvram filesystem will remove all configuration files!Continue? [confirm]*」という CLI メッセージが表示されたら、**Y** と入力します。

ステップ 4　「*Erase of nvram: complete.*」という CLI メッセージが表示されたら、**reload** と入力します。このコマンドにより、オペレーティング システムがリロードされます。

ステップ 5　「*Proceed with reload? [confirm]*」という CLI メッセージが表示されたら、**Y** と入力します。

注意　コンフィギュレーション ファイルの損傷を防ぐため、ブート プロセスは中断しないでください。CLI コンフィギュレーションの変更を続ける前に、アクセス ポイント/ブリッジ Install Mode LED が緑色に点滅するまで待ちます。ロード プロセスが完了すると、「*Line protocal on Interface Dot11Radio0, changed state to up*」という CLI メッセージが表示されます。

ステップ 6　アクセス ポイント/ブリッジがリブートしたら、静的 IP アドレスを割り当てている場合は WEB ブラウザ インターフェイスを使用して、割り当てていない場合は CLI を使用して、アクセス ポイントを再設定できます。

アクセス ポイントは、特権 EXEC モードから、IP アドレスも含めてデフォルト値に設定されています（DHCP を使用して IP アドレスを受信するように設定されます）。アクセス ポイント/ブリッジの新しい IP アドレスを取得するには、*show interface bvi1* CLI コマンドを使用します。

アクセス ポイントへのログイン

ユーザは、次のいずれかの方法を使用してアクセス ポイントにログインできます。

- グラフィカル ユーザ インターフェイス（GUI）
- Telnet（IP アドレスを使用して AP が設定されている場合）
- コンソール ポート

（注）　Cisco Aironet アクセス ポイントのすべてのモデルにコンソール ポートが用意されているわけではありません。アクセス ポイントにコンソール ポートが用意されていない場合は、GUI または Telnet を使用してアクセスしてください。

GUI を使用して AP にログインする方法については、「初めて Web ブラウザ インターフェイスを使用する場合」（P.2-2）を参照してください。

CLI を使用して AP にログインする方法については、「CLI のアクセス」(P.3-9)を参照してください。

コンソール ポートを使用して AP にログインする方法については、「アクセス ポイントへのローカル接続」(P.4-5)を参照してください。

IP アドレスの取得と割り当て

ワイヤレス デバイスの [Express Setup] ページにアクセスするには、次のいずれかの方法でワイヤレス デバイスの IP アドレスを取得するか、割り当てる必要があります。

- アクセス ポイントのコンソール ポートに接続し、静的 IP アドレスを割り当てます。デバイスのコンソール ポートに接続するには、次の項の手順を実行します。
  - 「アクセス ポイントへのローカル接続」(P.4-5)
  - 「1550 シリーズ アクセス ポイントへのローカル接続」(P.4-5)

（注） ターミナル エミュレータ アプリケーションによっては、フロー制御パラメータを Xon/Xoff に設定する必要があります。フロー制御値が none に設定されているためにデバイスのコンソール ポートに接続できない場合は、フロー制御値を Xon/Xoff に変更してみてください。

- IP アドレスを自動的に割り当てるには、DHSP サーバを使用します（使用可能な場合）。次のいずれかの方法により、DHCP によって割り当てられた IP アドレスを検索できます。
  - まず、ワイヤレス デバイスのコンソール ポートに接続し、**show ip interface brief** コマンドを使用して IP アドレスを表示します。

    コンソール ポートに接続するには、「アクセス ポイントへのローカル接続」(P.4-5)の手順に従います。
  - 組織のネットワーク管理者に、ワイヤレス デバイスのメディア アクセス コントロール（MAC）アドレスを知らせます。ネットワーク管理者は、MAC アドレスを使用して DHCP サーバに照会し、IP アドレスを確認します。アクセス ポイントの MAC アドレスは、アクセス ポイントの底面ラベルに記載されています。

デフォルトの IP アドレスの動作

1040、1140、1240、2600 アクセス ポイントをデフォルトの設定で LAN に接続している場合、アクセス ポイントは DHCP サーバに IP アドレスを要求し、アドレスを受信できない場合、要求を無期限に送信し続けます。

アクセス ポイントへのローカル接続

（注）　次の情報は、1550 シリーズ AP を除くすべての AP に適用されます。

アクセス ポイントを（有線 LAN に接続せずに）ローカルに設定する必要がある場合、DB-9 to RJ-45 のシリアル ケーブルを使用して PC をアクセス ポイントのコンソール ポートに接続できます。次の手順に従ってアクセス ポイントのコンソール ポートに接続し、CLI を開きます。

ステップ 1　9 ピンのメスの DB-9 to RJ-45 シリアル ケーブルを、アクセス ポイントの RJ-45 シリアル ポートと、コンピュータの COM ポートに接続します。DB-9 to RJ-45 シリアル ケーブルのシスコ製品番号は AIR-CONCAB1200 です。シリアル ケーブルは、http://www.cisco.com/go/marketplace で注文できます。

ステップ 2　アクセス ポイントと通信できるようにターミナル エミュレータを設定します。ターミナル エミュレータの接続では、9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1 の設定を使用します。フロー制御はなしです。

（注）　xon/xoff フロー制御で正常に機能しない場合は、フロー制御なしを使用してください。

ステップ 3　接続したら、**enter** を押すか、**en** と入力して、コマンド プロンプトを表示します。**enter** を押すと、ユーザ EXEC モードになります。**en** と入力すると、パスワードを入力するよう求められ、パスワードを入力すると特権 EXEC モードになります。デフォルトのパスワードは *Cisco* です。大文字と小文字は区別されます。

（注）　設定の変更が完了したら、アクセス ポイントからシリアル ケーブルを取り外してください。

1550 シリーズ アクセス ポイントへのローカル接続

アクセス ポイントを（有線 LAN に接続せずに）ローカルに設定する必要がある場合、カテゴリ 5 のイーサネット ケーブルを使用して PC を長距離用パワー インジェクタのイーサネット ポートに接続できます。シリアル ポート接続を使用するのと同じように、パワー インジェクタのイーサネット ポートへのローカル接続を使用できます。

（注）　特別なクロス ケーブルを使用しなくても、PC をパワー インジェクタに接続できます。また、ストレート ケーブルまたはクロス ケーブルのいずれも使用できます。

ブリッジをローカルで接続する手順は、次のとおりです。

ステップ 1　使用する PC が IP アドレスを自動的に取得するように設定します。または、アクセス ポイント/ブリッジの IP アドレスと同じサブネット内の IP アドレスを手動で割り当てます。たとえば、アクセス ポイント/ブリッジに IP アドレス 10.0.0.1 を割り当てた場合、PC に IP アドレス 10.0.0.20 を割り当てます。

ステップ 2　パワー インジェクタから電源ケーブルを抜いた状態で、カテゴリ 5 のイーサネット ケーブルを使用して PC をパワー インジェクタに接続します。クロス ケーブルまたはストレート ケーブルのいずれかを使用できます。

（注）　イーサネット ポート 0 を使用して、パワー インジェクタとアクセス ポイント/ブリッジ間で通信が実行されます。イーサネット ポート 0 の設定は何も変更しないようにしてください。

ステップ 3　二重同軸ケーブルで、パワー インジェクタをアクセス ポイント/ブリッジに接続します。

ステップ 4　パワー インジェクタの電源ケーブルを接続して、アクセス ポイント/ブリッジの電源を入れます。

ステップ 5　「基本設定の割り当て」(P.4-6) の手順を実行します。操作を間違えたため、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」(P.4-1) の手順の手順に従ってください。

ステップ 6　アクセス ポイント/ブリッジの設定後、PC からイーサネット ケーブルを抜いて、アクセス ポイントを有線 LAN に接続します。

（注）　PC をアクセス ポイント/ブリッジに接続するか、PC を有線 LAN に再接続する場合は、PC の IP アドレスを解放または更新しなければならない場合があります。ほとんどの PC では、PC をリブートするか、コマンド プロンプト画面で **ipconfig /release** および **ipconfig /renew** コマンドを入力することによって、IP アドレスを解放および更新できます。手順の詳細は、ご使用の PC の操作マニュアルを参照してください。

デフォルトの無線設定

Cisco IOS Release 12.3(8)JA から、アクセス ポイントの無線は無効に設定され、デフォルトの SSID は何も割り当てられていません。これは、権限のないユーザが、デフォルトの SSID を使用してセキュリティを設定していないこのアクセス ポイントからお客様の無線ネットワークにアクセスするのを防ぐための措置です。アクセス ポイントの無線インターフェイスを有効にする前に、SSID を作成する必要があります。

基本設定の割り当て

ワイヤレス デバイスの IP アドレスを決定または割り当てた後、次の手順に従って、このワイヤレス デバイスの [Express Setup] ページにアクセスし、初期設定を行います。

ステップ 1　インターネット ブラウザを開きます。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力して、**Enter** キーを押します。
[Enter Network Password] 画面が表示されます。

ステップ 3　**Tab** を押して、[Username] フィールドの次の [Password] フィールドに進みます。

ステップ 4　大文字/小文字を区別して *Cisco* というパスワードを入力し、**Enter** を押します。
[Summary Status] ページが表示されます。

ステップ 5　[Easy Setup] をクリックします。
[Express Setup] 画面が表示されます。

ステップ 6　[Network Configuration] をクリックします。

ステップ 7　システム管理者から入手した設定を [Network Configuration] に入力します。
設定可能な項目は、次のとおりです。

- [Host Name]：ホスト名は必須設定ではありませんが、ネットワーク上のワイヤレス デバイスを識別するのに役立ちます。ホスト名は、管理システム ページのタイトルに表示されます。

（注）　システム名には、32 文字まで入力することができます。しかし、ワイヤレス デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。異なるワイヤレス デバイスを区別することがクライアント ユーザにとって重要な場合、最初の 15 文字に、システム名の固有の部分を含めてください。

（注）　システム名を変更すると、ワイヤレス デバイスにより無線がリセットされます。この結果、アソシエートされたクライアント デバイスのアソシエーションが解除され、ただちに再アソシエートされます。

- [Server Protocol]：ネットワークの IP アドレスの割り当て方法に対応するオプション ボタンをクリックします。
  - [DHCP]：IP アドレスは、ネットワークの DHCP サーバによって自動的に割り当てられます。
  - [Static IP]：ワイヤレス デバイスでは、[IP Address] フィールドに入力された静的 IP アドレスが使用されます。
- [IP Address]：ワイヤレス デバイスの IP アドレスを割り当てたり、変更したりします。DHCP がネットワークで有効な場合、このフィールドは空白のままにします。

（注）　有線 LAN 上で Web ブラウザ インターフェイスや Telnet セッションを使用してワイヤレス デバイスの設定をしている間にワイヤレス デバイスの IP アドレスが変更されると、そのワイヤレス デバイスへの接続は解除されます。接続が解除された場合は、新しい IP アドレスを使用してワイヤレス デバイスに再接続してください。もう一度、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」（P.4-1）の手順に従ってください。

- [IP Subnet Mask]：IP アドレスが LAN 上で認識されるように、ネットワーク管理者から提供された IP サブネット マスクを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- [Default Gateway]：ネットワーク管理者から提供されたデフォルト ゲートウェイ IP アドレスを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- [IPv6 ProtocolP]：適用するプロトコルに対応する対応するチェックボックスをオンにして、そのプロトコルを指定します。次のオプションを選択できます。
  - DHCP
  - Autoconfig
  - Static IP
- [IPv6 Address]：IPv6 アドレスを入力します。

- [Username]：ネットワークへのアクセスに必要なユーザ名を入力します。
- [Password]：ネットワークへのアクセスに必要なユーザ名に対応するパスワードを入力します。
- [SNMP Community]：ネットワークで SNMP が使用されている場合、ネットワーク管理者により用意された SNMP コミュニティ名を入力して、（同じくネットワーク管理者により用意された）SNMP データの属性を選択します。
- [Current SSID List]（読み取り専用）

ステップ 8　アクセス ポイントでサポートされる無線帯域について、次の [Network Configuration] 設定を入力します。2.4 GHz 無線と 5 GHz の無線には共通して次のオプションがあります。

- [SSID]：[SSID] 入力フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
  - [Broadcast SSID in Beacon]：SSID を指定していないデバイスをアクセス ポイントにアソシエートできるようにするには、このチェックボックスをオンにします。このチェックボックスがオンになっている場合、アクセス ポイントは Broadcast SSID プローブ要求に応答すると共に、ビーコンと併せて自身の SSID をブロードキャストします。SSID をブロードキャストすると、SSID を指定していないデバイスがこの無線デバイスとアソシエートできます。このオプションは、パブリック スペースでゲストやクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしない場合、クライアント デバイスの SSID がこの SSID と一致しない限り、そのクライアント デバイスは無線デバイスとアソシエートできません。無線デバイス ビーコンに組み込める SSID は 1 つだけです。
- [VLAN]：無線の VLAN を有効にするには、[Enable VLAN ID] オプション ボタンをクリックし、VLAN ID を 1 ～ 4095 の範囲で入力します。この VLAN をネイティブ VLAN として指定する場合は、[Native VLAN] チェックボックスをオンにします。VLAN を無効にするには、[No VLAN] オプション ボタンをクリックします。
- [Security]：SSID のセキュリティ設定を選択します。この設定は、[No Security] から [WPA] まで堅牢性の順に並んでいます。[WPA] が最も強力なセキュリティ設定です。[EAP Authentication] または [WPA] を選択する場合は、ネットワーク上の認証サーバの IP アドレス（RADIUS サーバの IP アドレス）と共有秘密（RADIUS サーバ シークレット）を入力します。

（注）　無線 LAN で VLAN を使用しない場合、複数の SSID に割り当てることのできるセキュリティ オプションが制限されます。詳細については、「VLAN の使用」（P.4-12）を参照してください。

  - [No Security]：このセキュリティ設定では、暗号キーやキー管理は使用されず、Open 認証が使用されます。
  - [WEP Key]：このセキュリティ設定では、WEP 暗号化が必須となり、キー管理や Open 認証は使用されません。最大 4 つの WEP キー（つまり、キー 1、2、3、および 4）を指定できます。キーごとに値を入力し、128 ビットまたは 40 ビットのどちらであるかを指定します。
  - [EAP Authentication]：拡張認証プロトコル（EAP）認証では、認証サーバのサービスを通じてデータベースに対して認証されたユーザに無線アクセスを許可します。その上で、認証済みユーザに許可されているトラフィックを暗号化します。LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-GTC、EAP-SIM、およびその他の 802.1x/EAP ベースのプロトコルには、この設定を使用します。この設定では、暗号化必須 WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。

– [WPA]：Wi-Fi Protected Access（WPA）は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可します。その上で、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して、認証済みユーザに許可されている IP トラフィックを暗号化します。このオプションを選択する前に、クライアントが WPA 認定済みであることを確認してください。この設定では、暗号スイート tkip、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。

（注）　ここで使用されるセキュリティ設定の詳細については、「セキュリティ設定の概要」（P.4-11）を参照してください。

- [Role in Radio Network]：ネットワークでのワイヤレス デバイスの役割を示すボタンをクリックします。ワイヤレス デバイスが有線 LAN に接続されている場合は、[Access Point (Root)] を選択します。アクセス ポイントが有線 LAN に接続されていない場合は、[Repeater (Non-Root)] を選択します。Airlink でサポートされている役割は、ルートだけです。無線ネットワークの異なる AP でサポートされる役割の詳細については、「無線ネットワークの役割の設定」（P.6-3）を参照してください。無線ネットワークでは、次の役割が有効です。
  – [Access Point]：ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから無線 LAN までの無線トラフィックを仲介します。この設定は、どのアクセス ポイントにも適用できます。
  – [Repeater]：非ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから、無線 LAN に接続中のルート アクセス ポイントまでの無線トラフィックを仲介します。この設定は、どのアクセス ポイントにも適用できます。
  – [Root Bridge]：非ルート ブリッジとのリンクを確立します。このモードでは、クライアントからのアソシエーションも受け入れます。
  – [Non-Root Bridge]：このモードでは、ルート ブリッジとのリンクを確立します。
  – [Install Mode]：アクセス ポイント/ブリッジを自動インストール モードに指定することで、最適な効率が得られるようにブリッジのリンクを位置合わせして調整できます。
  – [Workgroup Bridge]：ワークグループ ブリッジ モードの場合、アクセス ポイントは、Cisco Aironet アクセス ポイントまたはブリッジにアソシエートするクライアント デバイスとして機能します。他の無線クライアントがルート ブリッジまたはアクセス ポイントにアソシエートされていないと仮定すると、ワークグループ ブリッジは最大 254 のクライアントを持つことができます。
  – [Universal Workgroup Bridge]：アクセス ポイントを、シスコ以外のアクセス ポイントとアソシエートできるワークグループ ブリッジとして設定します。
  – [Client MAC]：ユニバーサル ワークグループ ブリッジに接続されているクライアントのイーサネット MAC アドレス。このフィールドが表示されるのは、ユニバーサル ワークグループ ブリッジ モードの場合のみです。
  – [Scanner]：ネットワーク モニタリング デバイスとして機能します。スキャナ モードでは、アクセス ポイントはクライアントからのアソシエーションを受け入れません。継続的にスキャンを行い、無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセス ポイントは、スキャナとして設定できます。
- [Optimize Radio Network for]：ワイヤレス デバイスの無線の設定済みの設定か、ワイヤレス デバイスの無線のカスタマイズされた設定のいずれかを選択します。
  – [Throughput]：ワイヤレス デバイスで処理されるデータ量が最大限に増えます。ただし、その範囲は縮小される可能性があります。

  - [Range]：ワイヤレス デバイスの範囲が最大限に拡張されます。ただし、スループットは減少する可能性があります。
  - [Default]：アクセス ポイントに使用するデフォルト値のセット。
  - [Custom]：[Network Interfaces] で入力した設定がワイヤレス デバイスに使用されます。[Custom] をクリックすると、次のネットワーク インターフェイスのページに移動します。
- [Aironet Extensions]：無線 LAN 上に Cisco Aironet 無線デバイスしかない場合は、この設定を有効にします。
- [Channel]：無線デバイスの無線のデフォルト チャネル設定は Least Congested です。この場合、無線デバイスは、起動時に最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。
  - 2.4 GHz 無線に対応するオプションは、Least Congested を設定したチャネル 1-2412、チャネル 2-2417、チャネル 3-2422、チャネル 4-2427、チャネル 5-2432、チャネル 6-2437、チャネル 7-2442、チャネル 8-2447、チャネル 9-2452、チャネル 10-2457、チャネル 11-2462 です。
  - 5 GHz 無線に対応するオプションは、動的周波数選択を設定したチャネル 36-5180、チャネル 40-5200、チャネル 44-5220、チャネル 48-5240、チャネル 149-5745、チャネル 153-5765、チャネル 157-5785、チャネル 161-5805、チャネル 165-5825 です。
- [Power]：[Power] ドロップダウン リストから電力レベルを選択します。
  - 2.4 GHz 無線に対応するオプションは、Maximum、22、19、16、13、10、7、および 4 です。
  - 5 GHz 無線に対応するオプションは、Maximum、14、11、8、5、および 2 です。

ステップ 9　[Apply] をクリックして設定値を保存します。

ステップ 10　[Network Interfaces] をクリックして [Network Interfaces Summary] ページを表示します。

ステップ 11　[Radio Interface] をクリックして [Network Interfaces: Radio Status] ページを表示します。

ステップ 12　[Settings] タブをクリックして無線インターフェイスの [Settings] ページを表示します。

ステップ 13　[Enable] をクリックして、無線を有効に設定します。

ステップ 14　[Apply] をクリックします。

これでワイヤレス デバイスは稼働しますが、ネットワークの運用およびセキュリティに関する要件を満たすための追加の設定が必要になる場合があります。設定の完了に必要な情報については、このマニュアルの該当する章を参照してください。

（注）　アクセス ポイントは、工場出荷時の設定に戻すことができます。それには、MODE ボタンを数秒間（ステータス LED がオレンジになるまで）押しながら、電源ジャックを抜いて再び差し込みます。

[Easy Setup] ページのデフォルト設定

表 4-1 は、[Express Setup] ページのデフォルト設定一覧です。

表 4-1　[Express Setup] ページのデフォルト設定

設定	デフォルト
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	デフォルトで DHCP により割り当てられます。アクセス ポイントにおけるデフォルトの IP アドレスの動作については、「デフォルトの IP アドレスの動作」(P.4-4)を参照してください。
IP Subnet Mask	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 255.255.255.224 です。
Default Gateway	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 0.0.0.0 です。
IPv6 Protocol	DHCP および Autoconfig
SNMP Community	defaultCommunity（Read-only）
VLAN	No VLAN
Security	No Security
Role in Radio Network（インストール済みの無線ごとに設定）	Access Point
Optimize Radio Network for	Default
Aironet Extensions	Enable
Channel	Least-Congested（2.4 GHz の場合）および Dynamic Frequency Selection（5 GHz の場合）
Power	Maximum

セキュリティ設定の概要

基本的なセキュリティ設定は、[Easy Setup] > [Radio Configuration] セクションで設定できます。このセクションに提供されているオプションを使用して、固有の SSID を作成し、4 つのセキュリティ タイプのいずれかを割り当てることができます。

ワイヤレス デバイスには最大 16 の SSID を作成できます。作成した SSID は、[Current SSID List] に表示されます。デュアル無線のワイヤレス デバイスでは、デフォルトで、作成した SSID が両方の無線インターフェイスで有効になります。

（注） Cisco IOS Release 12.4(23c)JA および 12.xxx には、デフォルトの SSID は存在しません。クライアント デバイスからアクセス ポイントにアソシエートする前に、SSID を設定しておく必要があります。

SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。

最初の文字として次の文字は使用できません。

- 感嘆符(!)
- ポンド記号(#)
- セミコロン(;)

次の文字は無効とされ、SSID には使用できません。

- プラス記号(+)
- 閉じ大カッコ(])
- スラッシュ(/)
- 引用符(")
- タブ
- 末尾のスペース

VLAN の使用

無線 LAN で VLAN を使用し、VLAN に SSID を割り当てる場合、[Express Security] ページの 4 つのセキュリティ設定のうちのいずれかを使用して複数の SSID を作成できます。ただし、無線 LAN で VLAN を使用しない場合、SSID に割り当てることのできるセキュリティ オプションは制限されます。[Express Security] ページでは暗号化設定と認証タイプがリンクしているためです。VLAN を使用しない場合、暗号化設定(WEP と暗号)が 2.4 GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN をディセーブルにして静的 WEP で SSID を作成すると、WPA 認証を使用する追加の SSID は作成できません。これは、異なる暗号化設定を使用しているからです。SSID のセキュリティ設定が別の SSID と競合していることがわかった場合、1 つ以上の SSID を削除して競合を解消することができます。

SSID のセキュリティ タイプ

表 4-2 は、SSID に割り当てられる 4 つのセキュリティ タイプについて説明しています。

表 4-2　[Express Security Setup] ページのセキュリティ タイプ

セキュリティ タイプ	説明	有効になるセキュリティ機能
No Security	これは安全性が最も低いオプションです。このオプションは、パブリック スペースで使用されている SSID だけに使用し、ネットワークへのアクセスを制限している VLAN に割り当てる必要があります。	なし。

表 4-2　[Express Security Setup] ページのセキュリティ タイプ（続き）

セキュリティ タイプ	説明	有効になるセキュリティ機能
Static WEP Key	このオプションは、[No Security] よりは安全です。ただし、静的 WEP キーは攻撃に対して脆弱です。この設定を行う場合、MAC アドレスに基づいてワイヤレス デバイスへのアソシエーションを制限することを考慮してください（第 16 章「MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止」を参照）。または、ネットワークに RADIUS サーバが存在しない場合、アクセス ポイントをローカルの認証サーバとして使用することを考慮してください（第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照）。	WEP が必須。ワイヤレス デバイス キーに合う WEP キーがないと、この SSID を使用してもクライアント デバイスをアソシエートできません。
EAP Authentication	このオプションでは、802.1X 認証（LEAP、PEAP、EAP-TLS、EAP-FAST、EAP-TTLS、EAP-GTC、EAP-SIM、その他 802.1X/EAP ベースの製品）が有効になります。 この設定では、暗号化必須、WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 を選択します。 ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。802.1X 認証によって動的暗号キーが提供されるため、WEP キーを入力する必要はありません。	必須の 802.1X 認証。この SSID を使用してアソシエートするクライアント デバイスは、802.1X 認証を実行する必要があります。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

表 4-2　[Express Security Setup] ページのセキュリティ タイプ（続き）

セキュリティ タイプ	説明	有効になるセキュリティ機能
WPA	Wi-Fi Protected Access（WPA）は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可し、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して IP トラフィックを暗号化します。 この設定では、暗号スイート、TKIP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 を選択します。 拡張認証プロトコル（EAP）認証の場合と同じように、ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。	WPA 認証が必須。この SSID を使用してアソシエートするクライアント デバイスは、WPA 対応でなければなりません。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

セキュリティ設定の制限事項

[Easy Setup] の [Radio Configuration] セクションでのセキュリティ設定は、基本セキュリティの簡易設定として設計されています。使用可能なオプションは、ワイヤレス デバイスのセキュリティ機能のサブセットです。[Express Security] ページの使用にあたっては、次の制限事項に留意してください。

- [No VLAN] オプションを選択している場合、静的 WEP キーを一度設定することができます。[Enable VLAN] を選択した場合は、静的 WEP キーを無効にする必要があります。
- SSID を編集することはできません。ただし、SSID を削除して再作成することはできます。
- 複数の認証サーバは設定できません。複数の認証サーバを設定する場合は、[Security Server Manager] ページを使用します。
- 複数の WEP キーは設定できません。複数の WEP キーを設定する場合は、[Security Encryption Manager] ページを使用します。
- ワイヤレス デバイス上にすでに設定されている VLAN に SSID を割り当てることはできません。既存の VLAN に SSID を割り当てる場合は、[Security SSID Manager] ページを使用します。
- 同一の SSID 上で認証タイプを組み合わせて設定することはできません（MAC アドレス認証と EAP 認証など）。認証タイプを組み合わせて設定する場合は、[Security SSID Manager] ページを使用します。

CLI の設定例

ここでは、各セキュリティ タイプを使用して SSID を作成するのと同じ働きをする CLI コマンドの例を示します。この項で取り上げる設定例は次のとおりです。

例: 2.4 GHz 無線の [No Security]

次の例は、*no_security_ssid* という名前の SSID を作成し、その SSID をビーコンに組み込んで VLAN 10 に割り当ててから、VLAN 10 をネイティブ VLAN として選択した場合の設定の一部を示しています。

```
!
dot11 ssid no_security_ssid
   vlan 10
   authentication open
   guest-mode
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
ssid no_security_ssid
 !
antenna gain 0
 station-role root
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

例：2.4 GHz 無線の静的 WEP

次の例は、*static_wep_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して VLAN 20 に割り当て、キー スロットとして 3 を選択し、128 ビット キーを入力した場合の設定の一部を示しています。

```
!
dot11 ssid static_wep_ssid
   vlan 20
   authentication open
!
!
!
encryption vlan 20 key 3 size 128bit 7 76031220D71D63394A6BD63DE57F transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 E55F05382FE2064B7C377B164B73 transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio1.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio1.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
```

```
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface GigabitEthernet0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
no bridge-group 20 source-learning
!
interface GigabitEthernet0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
```

例 : [EAP Authentication]

次の例は、*eap_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 30 に割り当てた場合の設定の一部を示しています。

（注） 無線クライアントで EAP-FAST を使用していて、設定の中に Open 認証 + EAP を含めていないと、次の警告メッセージが表示されます。

「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

```
dot11 ssid eap_ssid
   vlan 30
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
dot11 guest
!
username apuser password 7 096F471A1A0A
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
encryption vlan 30 mode wep mandatory
 !
ssid eap_ssid
 !
antenna gain 0
 station-role root
```

```
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
```

```
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 00271A150754
!
bridge 1 route ip
```

例：2.4 GHz 無線の WPA2

次の例は、*wpa_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 40 に割り当てた場合の設定の一部を示しています。

```
aaa new-model
!
aaa group server radius rad_eap
 server name 10.10.11.100
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
!
dot11 ssid wpa_ssid
   vlan 40
   authentication open eap eap_methods
   authentication network-eap eap_methods
    authentication key-management wpa version 2
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
encryption vlan 40 mode ciphers aes-ccm
 !
ssid wpa_ssid
 !
antenna gain 0
 station-role root
```

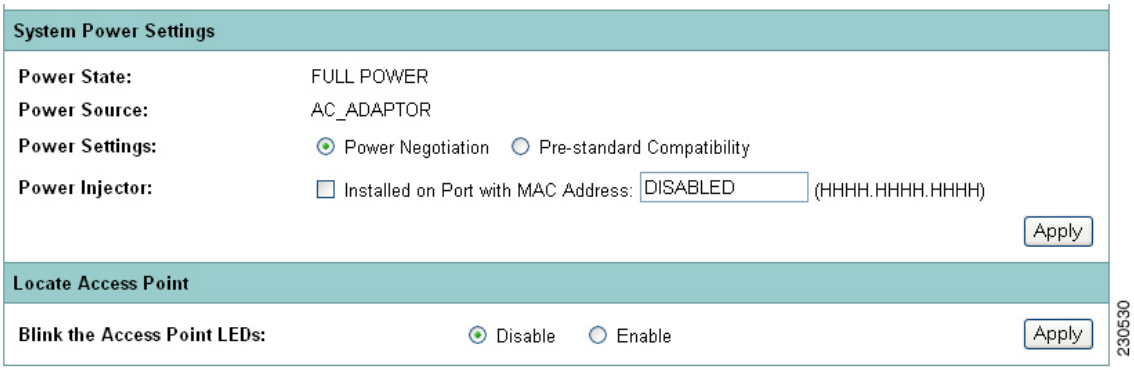
```
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 spanning-disabled
 no bridge-group 40 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
```

```
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 0....F175804
!
```

アクセス ポイントでのシステム電力の設定

AP 1040、AP 802、AP 1140、AP 1550、AP 1600、AP 2600、AP 3500、AP 3600、および AP 1260 は、ユニットの接続先電源が十分に電力を供給していないことを感知すると、無線インターフェイスをディセーブルにします。使用している電源によっては、アクセス ポイントの設定で電源のタイプを入力する必要がある場合があります。Web ブラウザ インターフェイスで [Software] > [System Configuration] ページを選択し、電力オプションを選択します。図 4-1 は、[System Configuration] ページの [System Power Settings] セクションを示しています。

図 4-1　　[System Software: System Configuration] ページの電力オプション



AC 電源アダプタの使用

AC 電源アダプタを使用してアクセス ポイントに電力を供給する場合は、アクセス ポイントの設定を調整する必要はありません。

IEEE 802.3af 電力ネゴシエーションのスイッチ機能の使用

1040、1140、および 1260 アクセス ポイントに Power over Ethernet（PoE）を供給するスイッチを使用していて、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応している場合、[System Software: System Configuration] ページで [Power Negotiation] を選択します。

IEEE 802.3af 電力ネゴシエーションに対応していないスイッチの使用

1040 または 1140 アクセス ポイントに Power over Ethernet（PoE）を供給するスイッチを使用していて、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応していない場合は、[System Software: System Configuration] ページで [Pre-Standard Compatibility] を選択します。

電力インジェクタの使用

電力インジェクタを使用して 1040、1140、または 1260 アクセス ポイントに電力を供給している場合、[System Software: System Configuration] ページで [Power Injector] を選択し、アクセス ポイントを接続しているスイッチ ポートの MAC アドレスを入力します。

dot11 extension power native コマンド

有効になっている場合、**dot11 extension power native** によって、無線で使用中のパワー テーブルが IEEE 802.11 テーブルからネイティブ パワー テーブルへシフトされます。無線装置は、このテーブル値を CISCO-DOT11-1F-MIB の NativePowerTable および NativePowerSupportedTable から取り出します。[Native Power] テーブルは、-1dBm レベルをサポートする Cisco Aironet の無線機器で使用できるよう、電源を -1dBm 近辺に低く設定するよう厳密に設計されています。

802.11ac のサポート

802.11ac は 802.11 の次世代ワイヤレス標準です。高いスループットを実現し、5 GHz 帯域で動作するように設計されています。802.11ac は 3700、2700、および 1700 シリーズ アクセス ポイントでサポートされています。802.11ac 無線が完全に機能するには、802.11n 無線が必要です。802.11n 無線をシャットダウンすると、802.11ac の機能に影響します。

802.11ac のチャネル幅

802.11n 無線と 802.11ac 無線は、同じ帯域で動作します。ただし、802.11n のチャネル帯域幅のほうを低く設定した場合に限り、それぞれのチャネル帯域幅を個別に設定できます。サポートされるチャネル帯域幅の組み合わせの詳細については、表 4-3を参照してください。

表 4-3　　サポートされるチャネル帯域幅の組み合わせ

802.11n のチャネル帯域幅	802.11ac のチャネル帯域幅
20	20
20	40
20	80
40	40
40	80

オフ チャネル スキャンまたは伝送はサポートされません。802.11ac 無線でオフ チャネル スキャン機能を利用するには、802.11n 無線が必要です。

たとえば、80 Mhz のチャネル幅を設定するには次のようにします。

```
ap# configure terminal
ap(config)# interface dot11Radio 1
```

```
ap(config-if)# channel width 80
ap(config-if)# end
```

802.11ac の電源管理

3700、2700、および 1700 の 802.11ac シリーズ アクセス ポイントは、Power over Ethernet（PoE）ソース、ローカル電源、またはパワー インジェクタで電力供給できます。AP が PoE から電力供給される場合、AP にはインライン電源から供給される場合より多くの電力が必要になるため、AP はソース（PoE+（802.3at）または PoE（802.3af））に応じて特定の無線設定を調整します。

たとえば、PoE+（802.3at）から電力供給される 3700 シリーズ AP は両方の無線に 4x4:3 設定を指定します。一方、PoE（802.3af）から電力供給される場合は、両方の無線に 3x3:3 設定を指定します。以下の表を参照してください。

ヒント　たとえば 4x4:3 の無線設定は、4 台のトランスミッタと 4 台のレシーバで 3 つの空間ストリームに対応できることを意味します。

（注）　AP が高電力の PoE または低電力（15.4W）の電源のどちらで動作しているかを判別するには、AP の GUI で [Home] ページを表示します。AP が低電力で動作している場合は、[Home:Summary Status] に次の警告が表示されます。

Due to insufficient inline power.Upgrade inline power source or install power injector.

屋外メッシュ製品を除くすべてのアクセス ポイントは、Power over Ethernet 対応です。Power over Ethernet を使用する無線を 2 台使用するアクセス ポイントは、完全に機能し、すべての機能をサポートします。使用可能なさまざまな電源管理オプションについては、表 4-4を参照してください。

表 4-4　電源に基づくインライン パワー オプション

Power Draw	説明	AP の機能	PoE バジェット（ワット）[1]	802.3af	E-PoE	802.3at PoE+ PWRINJ4
PoE + 802.3at	AP3700 初期状態	4x4:3（2.4/5 GHz）	16.1	No	Yes	Yes
PoE 802.3af	AP3700 初期状態	3x3:3（2.4/5 GHz）	15.4	Yes	該当なし	該当なし
PoE 802.3at	AP2700 初期状態	3x4:3（2.4/5 GHz）および補助イーサネット ポート使用可能	16.8	No	No	Yes
PoE 802.3af	AP2700 初期状態	3x4:3（5 GHz）、2x2:2（2.4 GHz）および補助イーサネット ポート使用可能	15.4	Yes	Yes	該当なし

1. PSE（スイッチまたはインジェクタ）で必要な電力です。

802.11n と 802.11ac は、802.11n に設定された電力レベルを使用します。802.11ac に個別に電力レベルを設定することはできません。

CLI を使用した IP アドレスの割り当て

ワイヤレス デバイスを有線 LAN に接続すると、ワイヤレス デバイスは、自動的に生成される Bridge Virtual Interface（BVI; ブリッジ仮想インターフェイス）を使用してネットワークにリンクします。ネットワークは、ワイヤレス デバイスのイーサネットと無線ポートの IP アドレスを個別に記録せずに、BVI を使用します。

CLI を使用してワイヤレス デバイスに IP アドレスを割り当てる場合、そのアドレスを BVI に割り当てる必要があります。ワイヤレス デバイスの BVI に IP アドレスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface bvi1**	BVI 対応のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	**ip address** *address mask*	BVI に IP アドレスとアドレス マスクを割り当てます。 （注）　Telnet セッションを使用してワイヤレス デバイスに接続している場合は、BVI に新しい IP アドレスを割り当てると、このワイヤレス デバイスへの接続が失われます。Telnet を使用してワイヤレス デバイスの設定を続ける必要がある場合は、新しい IP アドレスで、そのワイヤレス デバイスへの別の Telnet セッションを開始します。

Telnet セッションを使用した CLI へのアクセス

Telnet セッションを使用して CLI にアクセスする手順は、次のとおりです。これらの手順は、Microsoft Windows を実行する PC で Telnet 端末アプリケーションを使用する場合を想定しています。オペレーティング システムの詳細な操作方法については、ご使用の PC の操作マニュアルを確認してください。

ステップ 1　[Start] > [Programs] > [Accessories] > [Telnet] の順に選択します。

[Accessories] メニューに Telnet がない場合は、[Start] > [Run] の順に選択し、入力フィールドに **Telnet** と入力して **Enter** を押します。

ステップ 2　[Telnet] ウィンドウが表示されたら、[Connect] をクリックして、[Remote System] を選択します。

（注）　Windows 2000 では、[Telnet] ウィンドウにドロップダウン リストが表示されません。Windows 2000 で Telnet セッションを起動するには、**open** と入力してから、ワイヤレス デバイスの IP アドレスを入力します。

ステップ 3　[Host Name] フィールドにワイヤレス デバイスの IP アドレスを入力して、[Connect] をクリックします。

802.1X サプリカントの設定

dot1x 認証サーバ/クライアントの関係には、従来、ネットワーク デバイスと PC クライアントがそれぞれ使用されていました。これは、ネットワークへのアクセスに認証が必要なのは PC ユーザであるためです。しかし、無線ネットワークになってから、今までの認証サーバ/クライアントの関係とは違う手法が取り入れられました。まず、プラグが抜かれる可能性や、ネットワーク接続が部外者から使用される可能性がある公衆の場にアクセス ポイントを設置できるようになりました。次に、リピータ アクセス ポイントを無線ネットワークに組み込む場合、そのリピータ アクセス ポイントをクライアントと同様にルート アクセス ポイントで認証させる必要があります。

サプリカントの設定には、次の 2 段階があります。

- クレデンシャル プロファイルを作成して設定する
- このクレデンシャルをインターフェイスまたは SSID に適用する

どちらの手順を先に完了してもかまいませんが、サプリカントを使用する前に完了しておく必要があります。

クレデンシャル プロファイルの作成

特権 EXEC モードから、次の手順に従って 802.1X クレデンシャル プロファイルを作成します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot1x credentials** *profile*	dot1x クレデンシャル プロファイルを作成し、dot1x クレデンシャルのコンフィギュレーション サブモードに入ります。
ステップ 3	**anonymous-id** *description*	(任意):使用する匿名 ID を入力します。
ステップ 4	**description** *description*	(任意):クレデンシャル プロファイルの名称を入力します。
ステップ 5	**username** *username*	認証ユーザ ID を入力します。
ステップ 6	**password {0 | 7 | LINE}**	クレデンシャルに、暗号化されていないパスワードを入力します。 **0**:続けて、暗号化されていないパスワードを入力します。 **7**:続けて、非表示のパスワードを入力します。非表示のパスワードは、すでに保存済みの設定を適用する場合に使用します。 **LINE**:暗号化されていない(クリア テキストの)パスワード。 **(注)**　暗号化されていないテキストとクリア テキストは同じものです。クリア テキストのパスワードの後に 0 を入力してください。または、0 を省略してクリア テキストのパスワードを入力してください。
ステップ 7	**pki-trustpoint** *pki-trustpoint*	(オプション。EAP-TLS だけに使用):デフォルトの PKI トラストポイントを入力します。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

パラメータを無効にするには、**dot1x credentials** コマンドの **no** 形式を使用します。

次に、クレデンシャル プロファイルの作成例を示します。名称を *test*、ユーザ名を *Cisco*、暗号化されていないパスワードを *Cisco* とします。

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
ap(config)# dot1x credentials test
ap(config-dot1x-creden)#username Cisco
ap(config-dot1x-creden)#password Cisco
ap(config-dot1x-creden)#exit
ap(config)#
```

インターフェイスまたは SSID にクレデンシャルを適用する方法

クレデンシャル プロファイルの適用方法は、インターフェイスに対しても SSID に対しても同じです。

クレデンシャル プロファイルを有線ポートに適用する方法

特権 EXEC モードから、次の手順に従ってクレデンシャルをアクセス ポイントの有線ポートに適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet 0**	アクセス ポイントのギガビット イーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 （注）　**interface fa0** を使用してギガビット イーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	**dot1x credentials** *profile name*	すでに作成しておいたクレデンシャル プロファイル名を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例では、アクセス ポイントのギガビット イーサネット ポートに、クレデンシャル プロファイル *test* を適用します。

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
ap(config)#interface Gig0
ap(config-if)#dot1x credentials test
ap(config-if)#end
```

アップリンクに使用する SSID にクレデンシャル プロファイルを適用する方法

無線ネットワーク内にリピータ アクセス ポイントがあり、ルート アクセス ポイントで 802.1X サプリカントを使用している場合、リピータがルート アクセス ポイントとアソシエートして認証に使用する SSID に、802.1X サプリカントのクレデンシャルを適用する必要があります。

特権 EXEC モードから、次の手順に従って、アップリンクに使用する SSID にクレデンシャルを適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid*	802.11 SSID と入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 **（注）**　先頭の文字に !、#、; は使用できません。 +、]、/、"、TAB、末尾のスペースは、SSID で無効な文字です。
ステップ 3	**dot1x credentials** *profile*	設定済みのクレデンシャル プロファイル名を入力します。
ステップ 4	**end**	dot1x クレデンシャルの設定サブモードを終了します。
ステップ 5	**copy running config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例では、*test* という名前のクレデンシャル プロファイルを適用しています。リピータ アクセス ポイント上の適用先 SSID を *testap1* としています。

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

EAP 方式プロファイルの作成と適用

EAP 方式リストを設定して、サプリカントを有効にし、特定の EAP 方式を認識するオプションも用意されています。「802.1X サプリカントの EAP 方式プロファイルの作成と適用」（P.11-20）を参照してください。

IPv6 の設定

IPv6 は、膨大な数のアドレスを提供するために開発された、最新のインターネット プロトコルです。IPv4 では 32 ビットのアドレスが使用されますが、このプロトコルは 128 ビットのアドレスを使用します。

無線ネットワークでの展開では多数の IP 無線デバイスやスマートフォンを使用することから、128 ビットのアドレス形式を使用する IPv6 のアドレス空間では、3.4 x 1038 個のアドレスをサポートできます。

IPv6 アドレスは、x:x:x:x:x:x:x:x のようにコロン(:)で区切られた一連の 16 ビットの 16 進フィールドで表されます。

IPv6 アドレス タイプには、次の 3 つのタイプがあります。

- ユニキャスト

  Cisco IOS ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされます。

  – 集約可能グローバル アドレス

    集約可能グローバル ユニキャスト アドレスは、インターネットの IPv6 部分でグローバルにルーティングおよび到達することができます。これらのグローバル アドレスは、アドレス形式のプレフィックス 001 で識別されます。

  – リンクローカル アドレス

    リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10 (1111 1110 10) を使用して自動的にインターフェイスに設定されます。インターフェイス ID は、Modified EUI-64 形式になります。

- エニーキャストを使用できるのは、ルータだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスには使用しないでください。
- マルチキャスト アドレスは、指定のネットワーク サービスにマルチキャストされるように意図されたフレームを処理するホスト グループの論理 ID です。IPv6 のマルチキャスト アドレスは、プレフィックス FF00::/8 (1111 1111) を使用します。

  IPv6 設定では、次のマルチキャスト グループを使用します。

  – 送信要求ノード マルチキャスト グループ FF02:0:0:0:0:1:FF00::/104
  – 全ノード リンクローカル マルチキャスト グループ FF02::1
  – 全ルータ リンクローカル マルチキャスト グループ FF02::2

表 4-5に、IPv6 アドレスのタイプと形式を示します。

表 4-5　　IPv6 アドレス形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

サポートされるモード

- ルート
- ルート ブリッジ
- 非ルート ブリッジ
- リピータ
- WGB

サポートされないモード

- スペクトル モード
- モニタ モード

IPv6 アドレスを有効にするには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **int bv1**
- ap(config-if)# **ipv6 address**

ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

ステートレス自動設定をイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address autoconfig**

他の IPv6 アドレスをインターフェイスに割り当てることなくリンクローカル アドレスを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address ipv6-address link-local**

サイトローカル アドレスまたはグローバル アドレスをインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

ap(config-if)# **ipv6 address ipv6-address [eui-64]**

（注） オプションの eui-64 キーワードは、アドレスの下位 64 ビットに Modified EUI-64 インターフェイス ID を使用する場合に使用します。

DHCPv6 アドレスの設定

DHCPv6 は、IPv6 ネットワークで動作するために必要な IP アドレス、IP プレフィックス、およびその他のコンフィギュレーションを使用して IPv6 ホストを設定するために使用するネットワーク プロトコルです。DHCPv6 クライアントは、迅速な 2 つのメッセージ交換（送信要求、応答）または通常の 4 つのメッセージ交換（送信要求、アドバタイズ、要求、応答）によって、サーバから設定パラメータを取得します。デフォルトでは、4 つのメッセージ交換が使用されます。rapid-commit オプションをクライアントとサーバの両方でイネーブルにすると、2 つのメッセージ交換が使用されます。

アクセス ポイントの DHCPv6 クライアントをイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

- ap# **conf t**
- ap(config)**# int bv1**
- ap(config)**# ipv6 address dhcp rapid-commit(optional)**

自律 AP は、ステートフルおよびステートレス DHCPv6 アドレッシングの両方をサポートします。

ステートフル アドレッシング

ステートフル アドレッシングでは、DHCP サーバが使用されます。DHCP クライアントはステートフル DHCPv6 アドレッシングを使用して IP アドレスを取得します。

ステートフル アドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config)**# ipv6 address dhcp**

ステートレス アドレッシング

ステートレス アドレッシングでは、DHCP サーバを使用せずに IP アドレスを取得します。DHCP クライアントは、ルータ アドバタイズメントに基づいて、自身の IP アドレスを自動的に設定します。

ステートレス アドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

ap(config)# **ipv6 address autoconfig**

IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、同じネットワーク上のネイバーのリンク層アドレスを決定するために、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用します。

IPv6 ネイバー探索を設定するには、特権 EXEC モードから、次のコマンドを使用します。

コマンド	目的
ipv6 nd ?	ネイバー探索プロトコルを設定します。
ipv6 nd ns-interval *value*	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 インターフェイスに IPv6 ネイバー送信要求の再送信する間隔を設定します。
ipv6 nd reachable-time *value*	リモートの IPv6 ノードに到達可能な時間を設定します。
ipv6 nd dad attempts *value*	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 ユニキャスト IPv6 アドレスで、重複アドレス検出を行う際に連続して送信するネイバー送信要求メッセージの数を設定します。
ipv6 nd dad time *value*	重複アドレス検出の際の IPv6 ネイバー送信要求の送信間隔を設定します。
ipv6 nd autoconfig default-router	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 ネイバー検出によって導出されるデフォルト ルータへのデフォルト ルートを設定します。
ipv6 nd autoconfig prefix	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 次の定期ルータ アドバタイズメントの待機中に遅延を発生させないようにルータ アドバタイズメントの送信要求を行うルータ送信要求メッセージを設定します。
ipv6 nd cache expire *expire-time-in-seconds*	IPv6 ネイバー探索キャッシュ エントリの期限が切れるまでの時間を設定します。
ipv6 nd cache interface-limit size [log rate]	指定したインターフェイスにネイバー探索キャッシュ制限を設定します。
ipv6 nd na glean	このコマンドは、ブリッジ グループ仮想インターフェイス（BVI）に対してのみ有効です。 非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。

コマンド	目的
ipv6 nd nsf {**convergence** *time-in-seconds*| **dad** [**suppress**]| **throttle** *resolutions*}	IPv6 ネイバー探索ノンストップ フォワーディングを設定します。コンバージェンス時間を秒単位で設定したり（10 ～ 600 秒）、重複アドレス検出（DAD）を抑止したり、ノンストップ フォワーディング（NSF）で使用する解決の数を設定したりすることもできます。
ipv6 nd nud limit *limit*	ネイバー到達不能検出（NUD）の再送信回数を設定し、未解決の再送信回数の制限を設定します。
ipv6 nd resolution data limit *limit-in-packets*	キュー内でネイバー探索（ND）解決を待機するデータ パケット数の制限を設定します。
ipv6 nd route-owner	ネイバー探索で学習したルートを「ND」ステータスのルーティング テーブルに挿入し、ND 自動構成動作を有効にします。

IPv6 アクセス リストの設定

IPv6 アクセス リスト（ACL）は、トラフィックをフィルタリングしてルータへのアクセスを制限するために使用します。IPv6 プレフィックスのリストを使用して、ルーティング プロトコル アップデートをフィルタリングします。

アクセス リストをグローバルに設定してインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **ipv6 access-list** *acl-name*

IPv6 アクセス リストの設定には、特権 EXEC モードから、表 4-6に記載されているコマンドを使用できます。

表 4-6　　IPv6 アクセス リストの設定コマンド

コマンド	目的
default	コマンドをデフォルト値に設定します。
deny	拒否するパケットを指定します。
evaluate	アクセス リストを評価します。
exit	アクセス リスト コンフィギュレーション モードを終了します。
no	コマンドを無効にするか、そのデフォルトに設定します。
permit	転送するパケットを指定します。
remark	アクセス リスト エントリのコメントを設定します。
sequence	このエントリのシーケンス番号を設定します。

グローバルに設定された ACL をレイヤ 3 インターフェイスの発信トラフィックと着信トラフィックに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **interface** *interface*
- ap(config)# **ipv6 traffic-filter** *acl-name* **in/out**

RADIUS の設定

RADIUS サーバは、次の 3 つの機能を提供するバックグラウンド プロセスです。

- ネットワークへのアクセスを許可する前に、ユーザを認証する
- 特定のネットワーク サービスに対してユーザを許可する
- 特定のネットワーク サービスの使用状況を把握する

「RADIUS によるアクセス ポイントへのアクセスの制御」(P.5-12) を参照してください。

IPv6 WDS のサポート

WDS およびインフラストラクチャ アクセス ポイントは、WLAN Context Control Protocol (WLCCP) と呼ばれるマルチキャスト プロトコルで通信します。

Cisco IOS Release 15.2(4)JA は、IPv6 アドレスを使用して、WDS とアクセス ポイント間の通信をサポートします。WDS はデュアル スタックで動作します。つまり、IPv4 と IPv6 の両方の登録を受け入れます。

IPv6 WDS AP 登録

最初のアクティブな IPv6 アドレスが WDS の登録に使用されます。表 4-7に、IPv6 WDS AP 登録プロセスでのさまざまなシナリオを示します。

表 4-7　IPv6 WDS-AP 登録

	WDS			AP			
シナリオ	デュアル	IPv6	IPv4	デュアル	IPv6	IPv4	通信モード
1	Yes			yes			IPv6
2	Yes				yes		IPv6
3	Yes					yes	IPv4
4		yes		yes			IPv6
5		yes			yes		IPv6
6		yes				yes	失敗
7			yes	yes			IPv4
8			yes		yes		失敗
9			yes			yes	IPv4

(注)　IPv4 および IPv6 のアクセス ポイント間の 11r ローミングは、MDIE が異なるため、サポートされません。AP および WDS は両方とも、BV1 の最初のアクティブな IPv6 アドレスを使用して登録し、アドバタイズします。リンクローカルは登録に使用されません。

CDPv6 サポート :

CDP は、隣接するネイバーのデバイス ID、機能、MAC アドレス、IP アドレスまたはデュプレックスに関する情報を取得するために使用されるレイヤ 2 プロトコルです。各 CDP 対応デバイスは、隣接するネイバーに自身の情報を送信します。ネイティブ IPv6 の一部として、アクセス ポイントはアドレス TLV の一部と併せて自身の IPv6 アドレスを cdp メッセージで送信すると共に、隣接スイッチから取得した IPv6 アドレス情報を解析します。

次のコマンドは、接続されている IPv6 ネイバーを表示します。

ap# **show cdp neighbors detail**

RA フィルタリング

RA フィルタリングにより、無線クライアントから送信された RA をドロップすることで、IPv6 ネットワークのセキュリティが強化されます。RA フィルタリングは、設定に誤りがあるか、悪意のある IPv6 クライアント（正規の IPv6 ルータよりも優先される高い優先順位が設定されている場合がよくあります）が、ネットワークに接続できないようにします。いずれの場合も、IPv6 RA はある時点でドロップされ、悪意または設定の誤りがある IPv6 デバイスから、他の無線デバイスやアップストリームにある有線ネットワークが保護されます。

ただし、RA フィルタリングはアップリンクの方向ではサポートされません。

アクセス ポイントの自動設定

自律アクセス ポイントの Autoconfig 機能を使用することで、AP は自身の設定を Secure Copy Protocol（SCP）サーバから定期的にダウンロードするようになります。Autoconfig 機能が有効にされている場合、AP は事前に設定された時点でサーバから設定情報ファイルをダウンロードし、その設定を適用します。それと同時に、次回の設定のダウンロードもスケジュールされます。

（注）　設定が最後にダウンロードした設定と変わらない場合、AP はその設定を適用しません。

Autoconfig の有効化

Autoconfig を有効にする手順は次のとおりです。

ステップ 1　設定情報ファイルの準備

ステップ 2　環境変数の有効化

ステップ 3　設定情報ファイルのダウンロードのスケジューリング

設定情報ファイルの準備

Autoconfig 対応の AP は、SCP サーバから構成情報ファイルをダウンロードします。設定情報ファイルは、次の情報が含まれる XML ファイルです。

- 新規スタートアップ コンフィギュレーション。
- 絶対時間および範囲の値。AP は、次回の情報ファイルのダウンロードを、この絶対時間に 0 から範囲値までの間の乱数値を足した時刻にスケジュールします。

設定情報ファイルの形式は次のとおりです。

```
<?xml version="1.0" encoding="UTF-8"?>
<l2tp_cfg>
    <cfg_fetch_start_time>Absolute Time</cfg_fetch_start_time>
    <cfg_fetch_time_range>Random Jitter</cfg_fetch_time_range>
    <cfg_fetch_config>
        <![CDATA[
        <Startup config>
        ]]>
    </cfg_fetch_config>
</l2tp_cfg>
```

以下で、設定情報ファイルで使用される xml タグについて説明します。

XML タグ	目的
cfg_fetch_start_time	このタグには、絶対時間が DAY HH:MM の形式で含まれます。 • DAY には、Sun、Mon、Tue、Wed、Thu、Fri、Sat、All のいずれかを設定できます。 • HH は時間を表します。0 ～ 23 の数値を設定できます。 • MM は分を表します。0 ～ 59 の数値を設定できます。 例:「Sun 10:30」、「Thu 00:00」、「All 12:40」
cfg_fetch_time_range	次回の情報ファイルのダウンロード時刻をランダム化するために、0 からこの値までの間の乱数値が開始時刻に加算されます。
cfg_fetch_config	このタグには、AP の次のスタートアップ コンフィギュレーションが含まれます。

環境変数の有効化

設定情報ファイルを SCP サーバに準備して保管した後は、次の環境変数を設定する必要があります。

環境変数	目的
AUTO_CONFIG_AP_FUNCTIONALITY	Autoconfig を有効にするには、この変数を「YES」に設定する必要があります。
AUTO_CONFIG_USER	SCP サーバにアクセスするためのユーザ名
AUTO_CONFIG_PASSWD	SCP サーバにアクセスするためのパスワード
AUTO_CONFIG_SERVER	SCP サーバのホスト名/IP
AUTO_CONFIG_INF_FILE	SCP サーバからフェッチする設定情報ファイルの名前

環境変数を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

dot11 autoconfig add *environment-variable-name* **val** *value.*
次に例を示します。

```
dot11 autoconfig add AUTO_CONFIG_SERVER val 206.59.246.199
```

設定情報ファイルのダウンロードのスケジューリング

環境変数を設定した後、SCP サーバからの設定情報ファイルのダウンロードをスケジュールする必要があります。手順は次のとおりです。

ステップ 1　AP のクロック時刻を SNTP（Simple Network Time Protocol）サーバに同期させる必要があります。SNTP サーバを設定するには、コマンド **sntp server** *sntp-server-ip* を使用します。ここで、*sntp-server-ip* は SNTP サーバの IP アドレスです。

ステップ 2　AP に正確な時刻を使用させるには、正確なタイム ゾーンを設定する必要があります。それには、コマンド **clock timezone**?*TIMEZONE HH MM* を使用します。

- TIMEZONE はタイム ゾーンの名前です（IST、UTC など）。
- HH はタイムゾーンからの時間のオフセットです。
- MM は、タイムゾーンからの分のオフセットです

ステップ 3　SCP サーバから設定情報ファイルをダウンロードできなかった場合にダウンロードを再試行するまでの時間間隔を設定できます。この再試行間隔を設定するには、コマンド **dot11 autoconfig download retry interval min *MIN* max *MAX*** を使用します。

- MIN は再試行間隔の最小秒数です。
- MAX は再試行間隔の最大秒数です。ダウンロードが失敗するたびに、再試行間隔は 2 倍になります。ただし、再試行間隔が MAX に達すると、再試行は停止されます。

ブート ファイルを使用した Autoconfig の有効化

ブート ファイルで次のコマンドを DHCP IP 設定の一部として指定することでも、Autoconfig を有効にできます。

DHCP/BootTP サーバから返されるブート ファイルには、次の例に示す形式の内容が含まれます。

```
dot11 autoconfig add env var AUTO_CONFIG_AP_FUNCTIONALITY val YES
dot11 autoconfig add env var AUTO_CONFIG_USER val someusername
dot11 autoconfig add env var AUTO_CONFIG_PASSWD val somepasswd
dot11 autoconfig add env var AUTO_CONFIG_SERVER val scp.someserver.com
dot11 autoconfig add env var AUTO_CONFIG_INF_FILE val some_inf_file.xml
sntp server 208.210.12.199
clock timezone IST 5 30
dot11 autoconfig download retry interval min 100 max 400
end
```

Autoconfig ステータスの確認

Autoconfig ステータスを調べるには、**show dot11 autoconfig status** コマンドを使用します。

例

```
AP1600-ATT# show dot11 autoconfig status
Dot11 l2tp auto config is disabled

1600-89-absim# show dot11 autoconfig status
Auto configuration download will occur after
45 seconds

1600-89-absim# show dot11 autoconfig status
Trying to download information file from server
```

Autoconfig のデバッグ

必要に応じて、次のデバッグ コマンドを使用できます。

- Autoconfig ステート マシンの移行を確認するためのデバッグ コマンド:
  Deb dot11 autoconfigsm
- Autoconfig イベントを確認するためのデバッグ コマンド:
  Deb dot11 autoconfigev

アクセス ポイントの管理

この章では、ワイヤレス デバイスの管理方法について説明します。

MODE ボタンの無効化

コンソール ポートを搭載したアクセス ポイントの MODE ボタンは、**[no] boot mode-button** グローバル コンフィギュレーション コマンドで無効にできます。このコマンドを使用するとパスワードによるリカバリを防ぎ、権限のないユーザがアクセス ポイントの CLI にアクセスできないようにします。

注意　このコマンドは、パスワードによるリカバリを無効にします。このコマンドを入力した後、アクセス ポイントの特権 EXEC モードのパスワードを紛失してしまうと、アクセス ポイントの CLI にアクセスし直すには、シスコの Technical Assistance Center（TAC）に連絡する必要があります。

MODE ボタンはデフォルトで有効に設定されています。特権 EXEC モードから、次の手順に従ってアクセス ポイントの MODE ボタンを無効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no boot mode-button**	アクセス ポイントの MODE ボタンを無効にします。
ステップ 3	**end**	**（注）**　この設定は保存する必要はありません。

MODE ボタンのステータスをチェックするには、特権 EXEC モードから **show boot** または **show boot mode-button** コマンドを実行します。設定の実行時には、ステータスが表示されません。**show boot** と **show boot mode-button** コマンドを実行すると、通常次のような応答が表示されます。

```
ap#show boot
BOOT path-list:      flash:/ap3g2-k9w7-mx.152-4.JA1/ap3g2-k9w7-mx.152-4.JA1
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         no
Enable IOS Break:    no
HELPER path-list:
NVRAM/Config file
      buffer size:   32768
      Mode Button:    on
Radio Core TFTP:
ap#
```

（注）　特権 EXEC のパスワードがわかっていれば、グローバル コンフィギュレーション コマンド **boot mode-button** を使用して、MODE ボタンを通常動作に復旧できます。

アクセス ポイントへの不正アクセスの防止

権限のないユーザがワイヤレス デバイスの設定を変更したり、設定情報を表示したりするのを防ぐことができます。通常は、ネットワーク管理者からワイヤレス デバイスへのアクセスを許可し、ローカル ネットワーク内の端末またはワークステーションから接続するユーザのアクセスは制限します。

ワイヤレス デバイスへの不正なアクセスを防ぐには、次のいずれかのセキュリティ機能を設定してください。

- ワイヤレス デバイスでローカルに保存されるユーザ名とパスワードの組み合わせ。この組み合わせによって、各ユーザはワイヤレス デバイスにアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り/書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細については、「ユーザ名とパスワードのペアの設定」（P.5-7）を参照してください。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。ユーザ名とパスワードでは、大文字と小文字が区別されます。

（注）　TAB、?、$、+、および [は、パスワードには無効な文字です。

- RADIUS または TACACS+ セキュリティ サーバのデータベースに集中的に保存されたユーザ名とパスワードの組み合わせ。詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」（P.5-12）および「TACACS+ によるアクセス ポイントへのアクセスの制御」（P.5-18）を参照してください。

特権 EXEC コマンドへのアクセスの保護

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワーク デバイスへのアクセスが制限されます。特権レベルは、ユーザがネットワーク デバイスにログインした後に発行できるコマンドを定義します。

（注）　この項で使用されるコマンドの構文と使用方法の詳細については、リリース 12.3 の『*Cisco IOS Security* Command Reference』を参照してください。

この項では、コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。内容は次のとおりです。

デフォルトのパスワードおよび権限レベル設定

表 5-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 5-1　　デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
ユーザ名とパスワード	デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。
イネーブル パスワードおよび権限レベル	デフォルトのパスワードは *Cisco* です。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードはコンフィギュレーション ファイルで暗号化されます。
イネーブル シークレット パスワードおよび権限レベル	デフォルトのイネーブル パスワードは *Cisco* です。デフォルトはレベル 15 です（特権 EXEC レベル）。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	デフォルトのパスワードは *Cisco* です。パスワードはコンフィギュレーション ファイルで暗号化されます。

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。

（注） グローバル コンフィギュレーション コマンド **no enable password** は、イネーブル パスワードを削除しますが、このコマンドを使用する場合は十分な注意が必要です。イネーブル パスワードを削除すると、EXEC モードからロックアウトされます。

スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトのパスワードは *Cisco* です。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。パスワードに疑問符(?)を含めることができます。その場合はパスワードを作成するとき、疑問符を入力する前に Ctrl キーを押した状態で V キーを押してください。たとえば、パスワード abc?123 を作成する場合は、次のように入力します。 1. **abc** を入力します。 2. **Ctrl+V** を入力します。 3. **?123** を入力します。 enable パスワードの入力を求められたら、疑問符の前で Ctrl+V キーを押す必要はありません。パスワード プロンプトで abc?123 と入力するだけで済みます。 **(注)**　TAB、?、$、+、および [は、パスワードには無効な文字です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。 イネーブル パスワードは暗号化されず、ワイヤレス デバイスのコンフィギュレーション ファイルで読み取ることができます。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます(従来の特権 EXEC モード アクセス)。

```
AP(config)# enable password l1u2c3k4y5
```

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

セキュリティ レベルを強化するために、特にネットワークを超えるパスワードや Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されたパスワードについて、グローバル コンフィギュレーション コマンド **enable password** または **enable secret** を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード（デフォルト設定）または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password}	特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。
	または	または
	enable secret [**level** *level*] {*password* | *encryption-type encrypted*-password}	シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。 • （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 • （任意）*encryption-type* には、タイプ 0 とタイプ 7 の両方を使用できます。暗号化タイプ 0 では、パスワードが暗号化されません。暗号化タイプ 7 では、パスワードが暗号化されます。両方のタイプが指定されると、パスワード文字列は暗号化タイプ 5 に変換されます。これは、シスコ独自の暗号化アルゴリズムです。. **（注）** 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。

	コマンド	目的
ステップ 3	**service password-encryption**	（任意）パスワードを定義するとき、または設定を保存するときに、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の特権レベルの設定」（P.5-9）を参照してください。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

パスワードとレベルを削除するには、**no enable password** [**level** *level*] または**no enable secret** [**level** *level*] グローバル コンフィギュレーション コマンドを使用します。パスワードの暗号化をディセーブルにするには、**no service password-encryption** グローバル コンフィギュレーション コマンドを使用します。

次に、権限レベル 2 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

ユーザ名とパスワードのペアの設定

ユーザ名とパスワードの組み合わせを設定できます。これは、ワイヤレス デバイスでローカルに保存されます。ユーザ名とパスワードの組み合わせは、回線またはインターフェイスに割り当てられ、各ユーザがワイヤレス デバイスにアクセスする際の認証に使用されます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムでは、ログイン ユーザ名とパスワードが要求されます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。

	コマンド	目的
ステップ 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、権限レベル、パスワードを入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password* には、ワイヤレス デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、**no username** *name* グローバル コンフィギュレーション コマンドを使用します。

パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。

（注） ユーザ名は少なくとも 1 つ設定する必要があります。また、ワイヤレス デバイスに対して Telnet セッションを開くように login local を設定する必要があります。**no username** コマンドでユーザ名だけを入力すると、ワイヤレス デバイスからロックアウトされることがあります。

あるいは、ライン コンフィギュレーション コマンド **no login** を使用して、Telnet でのユーザ名の検証を無効にすることもできます。その場合、ユーザ検証を行う AP にログインしてから、**enable password**（または **enable secret**）コマンドで特権 EXEC レベルを取得する必要があります。このレベルを Telnet ラインに対してデフォルトで取得することもできます。それには、コマンド **privilege level 15** を使用します。

（注） no login コマンドと privilege level 15 コマンドの両方を使用すると、AP に接続するすべての Telnet クライアントに AP に対する完全な特権アクセスが割り当てられることになります。

```
ap(config)# line vty 0 4
ap(config-line)# no login
ap(config-line)# privilege level 15
```

複数の特権レベルの設定

デフォルトでは、Cisco IOS ソフトウェアにはユーザ EXEC モードと特権 EXEC モードという 2 つのパスワード セキュリティのモードがあります。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

この項では設定情報を扱います。

- 「コマンドの特権レベルの設定」(P.5-9)
- 「特権レベルへのログインと終了」(P.5-10)

コマンドの特権レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの権限レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure** を、EXEC モードの場合は **exec** を、インターフェイス コンフィギュレーション モードの場合は **interface** を、ライン コンフィギュレーション モードの場合は **line** をそれぞれ入力します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command* には、アクセスを制限したいコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルに対応するイネーブル パスワードを指定します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 **（注）**　TAB、?、$、+、および [は、パスワードには無効な文字です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	入力内容を確認します。 最初のコマンドは、パスワードとアクセス レベルの設定を表示します。2 番目のコマンドは、特権レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip route** コマンドをレベル 15 に設定すると、個別に異なるレベルに設定しない限り、**show** コマンドと **show ip** コマンドも自動的に特権レベル 15 に設定されます。

特定のコマンドについて、デフォルトの権限に戻すには、**no privilege** *mode* **level** *level command* グローバル コンフィギュレーション コマンドを使用します。

configure コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

特権レベルへのログインと終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *level*	指定した権限レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した権限レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

[Easy Setup] の設定

[Easy Setup] を使用すると、一つの画面でネットワークと無線を設定できます。

ネットワーク設定

ネットワーク設定を使用してアクセス ポイントを設定するには、次のフィールドに値を入力します。

- Hostname
- Server protocol（DHCP / Static）
- IP Address
- IP Subnet
- Default Gateway
- IPv6 Protocol（DHCP / Autoconfig / Static IP）
- IPV6 address
- Username
- Password
- SNMP Community
- Current SSID list（アクセス ポイントに設定された SSID リスト）

無線設定

無線設定を使用してアクセス ポイントを設定するには、次のフィールドを設定します。

- [SSID]：32 バイト文字列。
- ビーコン内に指定されたブロードキャスト SSID
- Security
- 無線ネットワークでの役割
  - [Access point]：ルート デバイス。この設定は、どのアクセス ポイントにも適用できます。
  - [Repeater]：非ルート デバイス。この設定も、どのアクセス ポイントにも適用できます。
  - [Root Bridge]：この設定は、どのアクセス ポイントにも適用できます。
  - [Non-Root Bridge]：この設定は、どのアクセス ポイントにも適用できます。
  - [Workgroup Bridge]：この設定は、どのアクセス ポイントにも適用できます。
  - ユニバーサル ワークグループ ブリッジ
  - [Scanner]：アクセス ポイントはネットワーク モニタリング デバイスとして機能します。継続的にスキャンを行い、このモードで無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセス ポイントは、スキャナとして設定できます。
  - [Spectrum]：Spectrum Expert モードの設定を参照してください。
- [Optimize Radio Network]：無線デバイスの無線に対する事前設定を選択するか、設定をカスタマイズできます。
- [Aironet Extensions]：無線 LAN 上に Cisco Aironet 無線デバイスがある場合にのみ、この設定を有効にできます。
- Channel
- Power

工場出荷時設定にアクセス ポイントをリセットするには、[Factory Reset] をクリックします。アクセス ポイントのイメージをリロードするには、[Reboot AP] をクリックします。

Spectrum Expert モードの設定

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセス ポイントでサポートされます。専用スペクトル センサーとして設定すると、Spectrum Expert Connect 自律アクセス ポイントは Cisco Spectrum Expert に接続できます。Spectrum Expert モードは、独立したモードであり、モニタ モードのサブセットではありません。

Spectrum Expert モードを有効にするには、次の手順を実行します。

ステップ 1　[Spectrum Expert] アイコンをクリックします。

ステップ 2　[Network] > [Network Interface] を選択します。

ステップ 3　[Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] をクリックします。

ステップ 4　[Enable] をクリックします。

ステップ 5　[Spectrum] オプション ボタンをクリックします。

ステップ 6　[Apply] をクリックします。

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセス ポイントでサポートされます。

Spectrum Expert の接続の設定

アクセス ポイントを Spectrum Expert として設定するには、次のコマンドを使用します。

- AP(config)**#interface dot11Radio 0**
- AP(config-if)**#station-role spectrum**
- AP(config-if)# **no shutdown**
- AP# **show spectrum status**

Spectrum Expert は、Internet Explorer でのみサポートされます。Spectrum Expert を起動にする前に、次の設定を変更します。

ステップ 1　[Tools] > [Internet options] > [Security] > [custom level] > [ActiveX Controls & plug-ins] > [Initialize and script ActiveX controls not marked as safe for scripting] を選択します。

ステップ 2　[Enable] オプション ボタンをクリックします。

次のポップアップ メッセージは無視できます。

```
Your current security settings put computer at risk.
```

RADIUS によるアクセス ポイントへのアクセスの制御

この項では、Remote Authentication Dial-In User Service（RADIUS）を使用して、ワイヤレス デバイスの管理者アクセス権を制御する手順について説明します。RADIUS をサポートするようにワイヤレス デバイスを設定する手順の詳細は、第 13 章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

RADIUS は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

（注）　この項で使用されるコマンドの構文と使用方法の詳細については、リリース 12.3 の『*Cisco IOS Security Command Reference*』を参照してください。

次の各項で RADIUS の設定について説明します。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI 経由でワイヤレス デバイスにアクセスするユーザを認証できます。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別」（P.13-5）を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** \| *list-name*} ライン コンフィギュレーション コマンドを使用します。

AAA サーバ グループの定義

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようにワイヤレス デバイスを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同一の RADIUS サーバにアカウンティングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、ワイヤレス デバイスが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、ワイヤレス デバイスと RADIUS サーバで動作する RADIUS デーモンの間で使用される認証と暗号キーを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 ワイヤレス デバイスが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な回数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。ワイヤレス デバイス ソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループを、特定のグループ名で定義します。 このコマンドを実行すると、ワイヤレス デバイスはサーバ グループ コンフィギュレーション モードへ移行します。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」（P.5-13）を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server radius** *group-name* グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、ワイヤレス デバイスは異なる 2 つの RADIUS グループ サーバ（*group1* と *group2*）を認識するように設定されます。group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1812 acct-port 1813
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1812 acct-port 1813
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

ユーザー特権アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、ワイヤレス デバイスはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザ プロファイルから取得した情報を使用して、ユーザ セッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

グローバル コンフィギュレーション コマンド **aaa authorization** と **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec group radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

（注）　許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network group radius**	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec group radius**	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、ワイヤレス デバイスを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

RADIUS の設定の表示

RADIUS の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

TACACS+ によるアクセス ポイントへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus（TACACS+）を使用してワイヤレス デバイスの管理者アクセス権を制御する手順について説明します。TACACS+ をサポートするようにワイヤレス デバイスを設定する手順の詳細は、第 13 章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

TACACS+ は詳細なアカウンティング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

（注）　この項で使用されるコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

次の項で TACACS+ の設定について説明します。

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 経由でワイヤレス デバイスにアクセスする管理者を認証できます。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、まずリストの最初の方式を使用してユーザを認証します。その方式が失敗すれば、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** \| *list-name*} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、ワイヤレス デバイスはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザ プロファイルから取得した情報を使用して、ユーザ セッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

グローバル コンフィギュレーション コマンド **aaa authorization** と **tacacs+** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec group tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network group tacacs+**	ネットワーク関連のすべてのサービス要求に対して、ユーザが TACACS+ 許可を受けるようにワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec group tacacs+**	ユーザの TACACS+ 許可でユーザの特権 EXEC アクセス権の有無を判断するように、ワイヤレス デバイスを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

イーサネットの速度およびデュプレックスの設定

ワイヤレス デバイスのイーサネット ポートに速度およびデュプレックスの設定を割り当てることができます。ワイヤレス デバイスのイーサネット ポート上の速度設定とデュプレックス設定のどちらについても、デフォルト設定の **auto** を使用することを推奨します。ワイヤレス デバイスがスイッチからインライン電源を受け取ったときに、速度設定またはデュプレックス設定が変更されるとイーサネット リンクがリセットされ、ワイヤレス デバイスがリブートします。ワイヤレス デバイスの接続先のスイッチのポートが **auto** に設定されていない場合、ワイヤレス デバイスのポートを **half** または **full** に変更してデュプレックスの不一致を修正することができます。これによってイーサネット リンクはリセットされなくなります。ただし、**half** または **full** から **auto** に戻すと、リンクがリセットされ、ワイヤレス デバイスがスイッチからインライン電源を受け取ると、そのワイヤレス デバイスはリブートします。

（注） ワイヤレス デバイスのイーサネット ポート上の速度およびデュプレックスの設定は、ワイヤレス デバイスの接続先のポート上のイーサネット設定と一致させる必要があります。ワイヤレス デバイスの接続先のポート上の設定を変更する場合は、これと一致するようにワイヤレス デバイスのイーサネット ポート上の設定も変更します。

イーサネットの速度とデュプレックスは、デフォルトでは **auto** に設定されています。特権 EXEC モードから、次の手順に従ってイーサネットの速度とデュプレックスを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet0**	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**speed {10 | 100 | 1000 | auto}**	イーサネット速度を設定します。デフォルト設定の **auto** を使用することをお勧めします。
ステップ 4	**duplex { auto | full | half }**	デュプレックス設定を行います。デフォルト設定の **auto** を使用することをお勧めします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス ポイントの無線ネットワーク管理の設定

ワイヤレス デバイスを無線ネットワーク管理に対して有効にできます。無線ネットワーク マネージャ（WNM）は無線 LAN 上のデバイスを管理します。

ワイヤレス デバイスが WNM と対話するように設定するには、次のコマンドを入力します。

```
AP(config)# wlccp wnm ip address ip-address
```

WDS アクセス ポイントと WNM の間の認証ステータスをチェックするには、次のコマンドを入力します。

```
AP# show wlccp wnm status
```

not authenticated、*authentication in progress*、*authentication fail*、*authenticated*、*security keys setup* のいずれかのステータスをとります。

アクセス ポイントのローカル認証および許可の設定

サーバを介さずに AAA を操作できるように設定するには、ローカル モードで AAA を実装するようにワイヤレス デバイスを設定します。ワイヤレス デバイスは、認証と許可を処理します。この設定ではアカウンティング機能は使用できません。

（注） ワイヤレス デバイスを 802.1x 対応のクライアント デバイス用のローカル認証サーバとして設定し、メイン サーバのバックアップを提供したり、RADIUS サーバのないネットワーク上で認証サービスを提供したりできます。ワイヤレス デバイスをローカル認証サーバとして設定する方法の詳細は、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

特権 EXEC モードから、次の手順に従ってローカル AAA にワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカルのユーザ名データベースを使用するようにログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	**aaa authorization exec default local**	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	**aaa authorization network default local**	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 認証を設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 • *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。 • （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type* には、後ろに暗号化されていないパスワードが続くことを指定する場合は **0** を入力します。非表示のパスワードが続くことを指定するには **7** を入力します。 • *password* には、ワイヤレス デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 **（注）** TAB、?、$、+、および [は、パスワードには無効な文字です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

認証キャッシュとプロファイルの設定

認証キャッシュとプロファイル機能を使用すると、アクセス ポイントがユーザのために認証/許可応答をキャッシュできるようになります。このため、次回の認証/許可要求を AAA サーバに送信しなくて済むようになります。

（注） この機能は、アクセス ポイントの Admin 認証だけにサポートされています。

この機能をサポートする次のコマンドが、Cisco IOS Release 12.3(7) に用意されています。

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

（注） これらのコマンドについては、『*Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

次の例は、Admin 認証用に設定したアクセス ポイントの設定例です。認証キャッシュを有効に設定した状態の TACACS+ を使用しています。この例では TACACS サーバを使用していますが、アクセス ポイントは RADIUS を使用して Admin 認証用に設定できます。

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
```

```
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
```

```
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

DHCP サービスを提供するためのアクセス ポイントの設定

次の項では、ワイヤレス デバイスを DHCP サーバとして機能させる方法について説明します。

- 「DHCP サーバの設定」(P.5-26)
- 「DHCP サーバ アクセス ポイントのモニタリングと維持」(P.5-28)

DHCP サーバの設定

デフォルトでは、アクセス ポイントは、ネットワーク上の DHCP サーバから IP 設定を受信するように設定されています。アクセス ポイントを DHCP サーバとして機能するように設定し、IP 設定を、有線 LAN と無線 LAN 両方のデバイスに割り当てることもできます。

（注） アクセス ポイントを DHCP サーバとして設定すると、IP アドレスがそのサブネット上のデバイスに割り当てられます。このデバイスは、サブネット上の他のデバイスと通信しますが、それ以上先とは通信しません。サブネットより先にデータを送信する必要がある場合は、デフォルトのルータを割り当てる必要があります。デフォルト ルータの IP アドレスには、DHCP サーバとして設定したアクセス ポイントと同じサブネット上のものを設定してください。

DHCP 関連のコマンドとオプションの詳細は、リリース 12.3 の『*Cisco IOS IP Configuration Guide*』の「Configuring DHCP」の章を参照してください。「Configuring DHCP」の章を参照するには、次の URL をクリックしてください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

特権 EXEC モードから、次の手順に従って、アクセス ポイントが DHCP サービスを提供するように設定し、デフォルト ルータを指定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp excluded-address** *low_address* [*high_address*]	ワイヤレス デバイスが割り当てるアドレス範囲から、ワイヤレス デバイスの IP アドレスを除外します。IP アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。 ワイヤレス デバイスでは、DHCP アドレス プール サブネット中のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定されます。DHCP サーバがクライアントに割り当てるべきでない IP アドレスを指定する必要があります。 (任意)除外するアドレスの範囲を指定するには、範囲の下限のアドレスの後に、範囲の上限のアドレスを入力します。
ステップ 3	**ip dhcp pool** *pool_name*	DHCP 要求に応じてワイヤレス デバイスが割り当てる IP アドレスのプールの名前を生成し、DHCP コンフィギュレーション モードを開始します。
ステップ 4	**network** *subnet_number* [*mask* | *prefix-length*]	アドレス プールにサブネット番号を割り当てます。ワイヤレス デバイスは、このサブネット内の IP アドレスを割り当てます。 (任意)アドレス プールにサブネット マスクを割り当てるか、アドレス接頭辞を構成するビット数を指定します。接頭辞はネットワーク マスクを割り当てる代替法です。プレフィックス長は、スラッシュ(/)で開始する必要があります。
ステップ 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	ワイヤレス デバイスによって割り当てられた IP アドレスのリース期間を設定します。 • days:日数でリース期間を設定します。 • (任意)hours:時間数でリース期間を設定します。 • (任意)minutes:分数でリース期間を設定します。 • infinite:リース期間を無限に設定します。
ステップ 6	**default-router** *address* [*address2 ... address 8*]	サブネット上の DHCP クライアントに対し、デフォルト ルータの IP アドレスを指定します。求められるのは 1 つの IP アドレスですが、コマンド行 1 行につき最大 8 つまでのアドレスを指定できます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、これらのコマンドの **no** 形式を使用します。

この例では、ワイヤレス デバイスを DHCP サーバとして設定する方法を示しています。IP アドレスの範囲は省略し、デフォルト ルータを割り当てています。

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

DHCP サーバ アクセス ポイントのモニタリングと維持

次の項では、DHCP サーバ アクセス ポイントのモニタと維持に使用できるコマンドについて説明します。

- 「show コマンド」(P.5-28)
- 「clear コマンド」(P.5-29)
- 「debug コマンド」(P.5-29)

show コマンド

DHCP サーバとしてのワイヤレス デバイスに関する情報を表示するには、EXEC モードで表 5-2 中のコマンドを入力します。

表 5-2　DHCP サーバ用の show コマンド

コマンド	目的
show ip dhcp conflict [*address*]	特定の DHCP サーバによって記録されているすべてのアドレス競合のリストを表示します。ワイヤレス デバイスの IP アドレスを入力すると、ワイヤレス デバイスによって記録されている競合が表示されます。
show ip dhcp database [*url*]	DHCP データベースでの最近のアクティビティを表示します。 **（注）** このコマンドは特権 EXEC モードで使用してください。
show ip dhcp server statistics	送受信されたサーバの統計情報やメッセージに関するカウント情報を表示します。

clear コマンド

DHCP サーバ変数を消去するには、特権 EXEC モードで表 5-3 中のコマンドを使用します。

表 5-3　DHCP サーバ用の clear コマンド

コマンド	目的
clear ip dhcp binding { *address* | * }	DHCP データベースから自動アドレス バインディングを削除します。address 引数を指定すると、特定の（クライアント）IP アドレスの自動バインディングが消去されます。アスタリスク（*）を指定すると、すべての自動バインディングが消去されます。
clear ip dhcp conflict { *address* | * }	DHCP データベースのアドレス競合をクリアします。address 引数を指定すると、特定の IP アドレスの競合が消去されます。アスタリスク（*）を指定すると、すべてのアドレスの競合が消去されます。
clear ip dhcp server statistics	すべての DHCP サーバのカウンタを 0 にリセットします。

debug コマンド

DHCP サーバのデバッグを有効にするには、特権 EXEC モードで次のコマンドを使用します。

debug ip dhcp server { **events** \| **packets** \| **linkage** }

ワイヤレス デバイス DHCP サーバのデバッグを無効にするには、このコマンドの **no** 形式を使用します。

アクセス ポイントのセキュア シェルの設定

この項では、セキュア シェル（SSH）機能の設定方法について説明します。

（注）　この項で使用されるコマンドの構文と使用方法の詳細は、『*Cisco IOS Security Command Reference for Release 12.3*』の「Secure Shell Commands」の項を参照してください。

SSH について

SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。SSH には、SSH バージョン 1 と SSH バージョン 2 の 2 種類のバージョンがあります。このソフトウェア リリースでは、どちらの SSH バージョンもサポートします。バージョン番号を指定しないと、アクセス ポイントがデフォルトのバージョン 2 になります。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。SSH 機能では SSH サーバと SSH 統合クライアントを使用します。クライアントは次のユーザ認証方式をサポートしています。

- RADIUS（詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」（P.5-12）を参照してください）
- ローカル認証および許可（詳細については、「アクセス ポイントのローカル認証および許可の設定」（P.5-23）を参照）

SSH の詳細については、次の URL にある『*Secure Shell Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

（注）　このソフトウェア リリースの SSH 機能は IP Security（IPsec）をサポートしていません。

SSH の設定

SSH を設定する前に、Cisco.com から暗号ソフトウェア イメージをダウンロードします。詳細は、このリリースのリリース ノートを参照してください。

SSH の設定方法と SSH 設定の表示方法の詳細については、次の URL にある『*Secure Shell Configuration Guide*』を参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

セキュア コピー プロトコルのサポート

セキュア コピー プロトコル（SCP）は、セキュリティのためにセキュア シェル（SSH）を使用してネットワーク上のホスト間のファイル転送をサポートします。Cisco IOS リリース 15.2(2)JB は、アクセス ポイント自体へのログイン中に、アクセス ポイントとの間の SCP ファイル転送をサポートします。

AAA 認証を使用してデータ転送が制限されます。SCP では、AAA 認証を使用してユーザ名とパスワードを確認して、転送中のデータの完全性と機密性を確保できます。

SSH を設定するには、次のコマンドを使用します。

- **ip hostname**
- **ip domain-name**
- **crypto key generate rsa (512, 1024,2048)**
- **ip SSH version**
- **aaa new-model**
- **aaa authentication login default local**
- **aaa authorization exec default local**
- **username cisco privilege 15 password 0 cisco**

SCP を実行するには、**copy run scp://url** コマンドを使用します。

クライアント ARP キャッシングの設定

アソシエートされたクライアント デバイスの Address Resolution Protocol（ARP; アドレス レゾリューション プロトコル）キャッシュを保持するように、ワイヤレス デバイスを設定できます。ワイヤレス デバイスで ARP キャッシュを保持すると、無線 LAN のトラフィック負荷が軽減されます。ARP キャッシングはデフォルトで無効に設定されています。

ここでは、次の情報について説明します。

クライアント ARP キャッシングの概要

ワイヤレス デバイスでの ARP キャッシングは、クライアント デバイスへの ARP 要求をワイヤレス デバイスで止めることによって、無線 LAN 上のトラフィックを軽減します。ワイヤレス デバイスは、ARP 要求をクライアント デバイスへ転送する代わりに、アソシエートされたクライアント デバイスに代わって ARP 要求に応答します。

ARP キャッシングを無効にすると、ワイヤレス デバイスはすべての ARP 要求をアソシエートされたクライアントに無線ポート経由で転送し、ARP 要求を受け取ったクライアントが応答します。一方、ARP キャッシングを有効にすると、ワイヤレス デバイスはアソシエートされたクライアントに代わって ARP 要求に応答し、クライアントへは要求を転送しません。ワイヤレス デバイスがキャッシュにない IP アドレスに向けた ARP 要求を受け取ると、ワイヤレス デバイスはその要求をドロップして転送しません。ワイヤレス デバイスは、ビーコンに情報エレメントを追加して、バッテリの寿命を延ばすためのブロードキャスト メッセージを安全に無視できることをクライアント デバイスに通知します。

オプションの ARP キャッシング

アクセス ポイントにシスコ製以外のクライアント デバイスがアソシエートされ、そのデバイスがデータを通さない場合、ワイヤレス デバイスがそのクライアントの IP アドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスはワイヤレス デバイスに既知の IP アドレスのクライアントについては、その代理として応答しますが、不明なクライアント宛ての ARP 要求はすべて無線ポートから転送します。アソシエートされた全クライアントの IP アドレスを記憶すると、ワイヤレス デバイスはそれらのアソシエートされたクライアント以外に対する ARP 要求をドロップします。

ARP キャッシングの設定

特権 EXEC モードから、次の手順に従って、アソシエートされたクライアントの ARP キャッシュを保持するようにワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 arp-cache [optional]**	ワイヤレス デバイスでの ARP キャッシングを有効にします。 • （任意）ワイヤレス デバイスが認識している IP アドレスのクライアント デバイスに限って ARP キャッシングを有効にするには、**optional** キーワードを使用します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例に、アクセス ポイントで ARP キャッシングを設定する方法の例を示します。

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

システム日時の管理

ワイヤレス デバイスのシステムの時刻と日付は、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用して自動的に管理することも、ワイヤレス デバイスに時刻と日付を設定して手動で管理することもできます。

（注） この項で使用されるコマンドの構文と使用方法の詳細は、リリース 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報について説明します。

- 「簡易ネットワーク タイム プロトコルの概要」（P.5-32）
- 「SNTP の設定」（P.5-33）
- 「手動での日時の設定」（P.5-33）

簡易ネットワーク タイム プロトコルの概要

簡易ネットワーク タイム プロトコル（SNTP）とは、クライアント専用バージョンの簡易版 NTP です。SNTP は、NTP サーバから時間を受信するだけで、他のシステムに時刻サービスを提供することはできません。通常、SNTP は 100 ミリ秒以内の精度で時刻を提供しますが、NTP のような複雑なフィルタリングや統計メカニズムは提供しません。

SNTP は、設定済みのサーバからパケットを要求して受け入れるように設定するか、任意の送信元から NTP ブロードキャスト パケットを受け入れるように設定できます。複数の送信元が NTP パケットを送信している場合、最適な層にあるサーバが選択されます NTP とストラタムの詳細は、次の URL をクリックしてください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001131

複数のサーバのストラタムが同じだった場合は、ブロードキャスト サーバよりも設定済みサーバが優先されます。これらの両方を満たすサーバが複数ある場合は、時刻パケットを最初に送信したサーバが選択されます。現在選択中のサーバからパケット受信が途絶えたり、または上記の基準に基づいてより最適なサーバが検出されたりしない限り、SNTP が新たにサーバを選択することはありません。

SNTP の設定

SNTP は、デフォルトでディセーブルになっています。アクセス ポイントで SNTP をイネーブルにするには、表 5-4 に示すコマンドのいずれか、または両方をグローバル コンフィギュレーション モードで使用します。

表 5-4　　SNTP コマンド

コマンド	目的
sntp server {*address* | *hostname*} [**version** *number*]	NTP サーバからの NTP パケットを要求するように SNTP を設定します。
sntp broadcast client	任意の NTP ブロードキャストからの NTP パケットを受け入れるように SNTP を設定します。

各 NTP サーバについて、**sntp server** コマンドを 1 回入力します。NTP サーバは、アクセス ポイントからの SNTP メッセージに応答できるよう設定しておく必要があります。

sntp server コマンドと **sntp broadcast client** コマンドの両方を入力した場合、アクセス ポイントはブロードキャスト サーバからの時間を受け付けますが、同一のストラタムと判断して設定済みサーバからの時間の方を優先します。SNTP に関する情報を表示するには、**show sntp** EXEC コマンドを使用します。

手動での日時の設定

他のタイム ソースが使用できない場合は、システムの再起動後、手動で日時を設定できます。時刻は、次にシステムを再起動するまで正確です。手動設定は最後の手段としてのみ使用することを推奨します。ワイヤレス デバイスが同期できる外部ソースがある場合は、システム クロックを手動で設定する必要はありません。

ここでは、次の設定情報について説明します。

システム クロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステム クロックを設定する必要はありません。

システム クロックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のいずれかの書式を使ってシステム クロックを手動で設定します。 • *hh*:*mm*:*ss* には、時刻を時間（24 時間形式）、分、秒で指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day* には、当月の日付で日を指定します。 • *month* には、月を名前で指定します。 • *year* には、年を指定します（常に 4 桁で指定）。
ステップ 2	**show running-config**	入力内容を確認します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次に、システム クロックを手動で 2001 年の 7 月 23 日午後 1 時 32 分に設定する例を示します。

```
AP# clock set 13:32:00 23 July 2001
```

日時設定の表示

日時の設定を表示するには、**show clock [detail]** 特権 EXEC コマンドを使用します。

システム クロックは、信頼性がある（正確であると信じられる）かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミング ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていなければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

show clock の表示の前にある記号は、次の意味があります。

- *:時刻は信頼できません。
- （空白）:時刻は信頼できます。
- .:時刻は信頼できますが、NTP は同期していません。

タイム ゾーンの設定

手動でタイム ゾーンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	タイム ゾーンを設定します。 ワイヤレス デバイスは内部時間を協定世界時（UTC）で維持するため、このコマンドは表示専用で、時刻を手動で設定するときだけに使用されます。 • *zone* には、標準時間が施行されているときに表示されるタイムゾーンの名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC からの時差を入力します。 • （任意）*minutes-offset* には、UTC からの分差を入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

clock timezone グローバル コンフィギュレーション コマンドの**minutes-offset** 変数は、現地のタイム ゾーンと UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域のタイム ゾーン（大西洋標準時（AST））は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは**clock timezone AST -3 30** です。

時刻を UTC に設定するには、**no clock timezone** グローバル コンフィギュレーション コマンドを使用します。

夏時間の設定

毎年特定の曜日に夏時間が開始して終了する地域に夏時間を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで**clock summer-time** *zone* **recurring** を指定すると、夏時間のルールは米国のルールをデフォルトにします。 • *zone* には、夏時間が施行されているときに表示されるタイムゾーンの名前（たとえば PDT）を入力します。 • （任意）*week* には、月の何週目かを指定します（1 ～ 5、または **last**）。 • （任意）*day* には、曜日を指定します（Sunday、Monday など）。 • （任意）*month* には、月を指定します（January、February など）。 • （任意）*hh*:*mm* には、時刻を時間（24 時間形式）と分で指定します。 • （任意）*offset* には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

次に、夏時間が 4 月の第一日曜の 2 時に始まり、10 月の最終日曜の 2 時に終わるように指定する例を示します。

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

ユーザの居住地域の夏時間が定期的なパターンに従わない(次の夏時間のイベントの正確な日時を設定する)場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。 夏時間はデフォルトでディセーブルに設定されています。 • *zone* には、夏時間が施行されているときに表示されるタイム ゾーンの名前(たとえば PDT)を入力します。 • (任意)*week* には、月の何週目かを指定します(1 ～ 5、または **last**)。 • (任意)*day* には、曜日を指定します(Sunday、Monday など)。 • (任意)*month* には、月を指定します(January、February など)。 • (任意)*hh*:*mm* には、時刻を時間(24 時間形式)と分で指定します。 • (任意)*offset* には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** グローバル コンフィギュレーション コマンドを使用します。

次に、夏時間が 2013 年 10 月 12 日の 2 時に始まり、2014 年 4 月 26 日の 2 時に終わるように設定する例を示します。

```
AP(config)# clock summer-time pdt date 12 October 2013 2:00 26 April 2014 2:00
```

HTTP アクセスの定義

デフォルトでは、80 が HTTP アクセスに使用され、ポート 443 が HTTPS アクセスに使用されます。この値は、ユーザがカスタマイズできます。GUI を使用して HTTP アクセスを定義するには、次の手順に従います。

ステップ 1　アクセス ポイントの GUI から、[Services] > [HTTP] の順にクリックします。[Service: HTTP-Web server] 画面が表示されます。

ステップ 2　この画面に、目的の HTTP と HTTPS のポート番号を入力します。このポート番号フィールドに値を入力しないと、デフォルト値が使用されます。

ステップ 3　[Apply] をクリックします。

CLI を使用して HTTP アクセスを定義するには、次の手順に従います。

ステップ 1　AP(config)# **conf t**

ステップ 2　AP(config)# **ip http port** *value*

ステップ 3　AP(config)# **ip http secure-port** *value*

システム名およびプロンプトの設定

ワイヤレス デバイスを識別するシステム名を設定します。デフォルトでは、システム名とプロンプトは *ap* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字をシステム プロンプトとして使用します。大なり記号(>)が追加されます。プロンプトは、システム名が変更されると必ず更新されますが、グローバル コンフィギュレーション コマンド **prompt** を使用して手動でプロンプトを設定している場合は更新されません。

（注）　この項で使用されるコマンドの構文と使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP and IP Routing Command Reference* 』ガイドを参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.5-37)
- 「システム名の設定」(P.5-38)
- 「DNS の概要」(P.5-38)

デフォルトのシステム名およびプロンプトの設定

アクセス ポイントのデフォルトのシステム名とプロンプトは *ap* です。

システム名の設定

手動でシステム名を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *ap* です。 **（注）** システム名を変更する場合、ワイヤレス デバイスの無線はリセットされ、アソシエートしているクライアント デバイスはアソシエーションが解除され、ただちに再アソシエートされます。 **（注）** システム名には、63 文字まで入力することができます。しかし、ワイヤレス デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。クライアント ユーザがアクセス ポイントを区別することが重要な場合、システム名の一意の部分を最初の 15 文字に含めてください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

システム名を設定すると、システム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、グローバル コンフィギュレーション コマンド **no hostname** を使用します。

DNS の概要

ドメイン ネーム システム（DNS）プロトコルは、DNS 分散型データベースを制御し、これによりホスト名を IP アドレスに対応付けできます。ワイヤレス デバイスに DNS を設定すると、**ping**、**telnet**、**connect**、などすべての IP コマンドおよび関連する Telnet サポート操作で、IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP で *com* というドメイン名に分類される商業組織なので、ドメイン名は *cisco.com* となります。このドメイン内のファイル転送プロトコル（FTP）システムなどの個々のデバイスは *ftp.cisco.com* のように識別されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ（またはデータベース）に保存することです。ドメイン名を IP アドレスにマッピングするには、まずホスト名を特定し、ネットワーク上に存在するネーム サーバを指定し、DNS を有効にします。

ここでは、次の設定情報について説明します。

DNS のデフォルト設定

表 5-5 に、DNS のデフォルト設定を示します。

表 5-5　DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	ディセーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

DNS の設定

特権 EXEC モードから、次の手順に従って DNS を使用するようにワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	ソフトウェアが未修飾ホスト名(ドット付き 10 進ドメイン名を含まない名前)を作成するときに使用するデフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名は設定されていませんが、ワイヤレス デバイスの設定が BOOTP または Dynamic Host Configuration Protocol(DHCP)サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります(この情報がサーバに設定されている場合)。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 最大 6 つのネーム サーバを指定できます。各サーバ アドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。ワイヤレス デバイスは、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。

	コマンド	目的
ステップ 4	**ip domain-lookup**	（任意）ワイヤレス デバイスで DNS ベースのホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワイヤレス デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため DNS クエリは作成されません。ピリオド（.）を含まないホスト名を設定すると、名前を IP アドレスにマッピングする DNS クエリが作成される前に、ホスト名の後にピリオドとデフォルトのドメイン名が追加されます。デフォルトのドメイン名は、**ip domain-name** グローバル コンフィギュレーション コマンドによって設定される値です。ホスト名にピリオド（.）が含まれている場合、Cisco IOS ソフトウェアはホスト名にデフォルトのドメイン名を追加せずに、IP アドレスを検索します。

ドメイン名を削除するには、**no ip domain-name** *name* グローバル コンフィギュレーション コマンドを使用します。ネームサーバのアドレスを削除するには、**no ip name-server** *server-address* グローバル コンフィギュレーション コマンドを使用します。ワイヤレス デバイスで DNS を無効にするには、グローバル コンフィギュレーション コマンド **no ip domain-lookup** を使用します。

DNS の設定の表示

DNS 設定情報を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

（注） ワイヤレス デバイスに DNS が設定されている場合、**show running-config** コマンドを実行すると、サーバの名前ではなく IP アドレスが表示される場合があります。

バナーの作成

今日のお知らせ（MOTD）バナーとログイン バナーを設定できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ（差し迫ったシステム シャットダウンの通知など）を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

（注） この項で使用されるコマンドの構文と使用方法の詳細は、リリース 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報について説明します。

バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

MoTD ログイン バナーの設定

ワイヤレス デバイスにログインしたときに画面に表示される 1 行以上の行のメッセージ バナーを作成できます。

MoTD ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner motd** *c message c*	MoTD バナーを指定します。 *c* にはポンド記号(#)など希望する区切り文字を入力し、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message* には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

MoTD バナーを削除するには、**no banner motd** グローバル コンフィギュレーション コマンドを使用します。

次の例は、開始および終了区切り文字にポンド記号(#)を使用して、ワイヤレス デバイスに MOTD バナーを設定する方法を示しています。

```
AP(config)# banner motd #
This is a secure site.Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

次の例は、上記の設定で表示されるバナーを示しています。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site.Only authorized users are allowed.
For access, contact technical support.
```

```
User Access Verification

Password:
```

ログイン バナーの設定

接続したすべての端末に表示されるログイン バナーを設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner login** *c message c*	ログイン メッセージを指定します。 *c* にはポンド記号(#)など希望する区切り文字を入力し、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 *message* には、255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

ログイン バナーを削除するには、**no banner login** グローバル コンフィギュレーション コマンドを使用します。

次の例は、開始および終了区切り文字にドル記号($)を使用して、ワイヤレス デバイスにログイン バナーを設定する方法を示しています。

```
AP(config)# banner login $
Access for authorized users only.Please enter your username and password.
$
AP(config)#
```

自律 Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードする方法

（注）　GUI または CLI を使用して自律アクセス ポイントの Cisco IOS イメージのみをアップグレードする方法については、次の URL を参照してください。
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00809f0e94.shtml.

ネットワーク上で無線 LAN コントローラと通信できるよう、自律 Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードするユーティリティが用意されています。アップグレード ユーティリティの使用方法の詳細については、次の URL にある『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* 』を参照してください。

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

自律アクセス ポイントを Lightweight モードに変換するには、アクセス ポイントに Telnet し、次のコマンドを実行します。

archive download-sw {/overwrite | /reload} tftp: //location/image-name

無線の設定

この章では、ワイヤレス デバイスに無線を設定する手順を説明します。

無線インターフェイスのイネーブル化

ワイヤレス デバイスの無線はデフォルトではディセーブルに設定されています。

（注）　Cisco IOS Release 12.3(8)JA から、デフォルトの SSID は存在しません。無線インターフェイスを有効にする前に、SSID を作成する必要があります。

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid*	SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。
ステップ 3	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11n 2.4 GHz 無線は Radio 0 です。 5 GHz 無線および 802.11n 5 GHz 無線は Radio 1 です。
ステップ 4	**ssid** *ssid*	ステップ 2 で作成した SSID を適切な無線インターフェイスに割り当てます。
ステップ 5	**no shutdown**	無線ポートを有効にします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

無線ポートをディセーブルにするには、**shutdown** コマンドを使用します。

無線ネットワークの役割の設定

表 6-1 は、各デバイスの無線ネットワークの役割を示しています。

表 6-1　　無線ネットワーク設定でのデバイスの役割

無線ネットワークでの役割	AP 1040	AP 1140	AP 1260	AP 1530	AP 1550	AP 1600	AP 1700	AP 2600	AP 3500	AP 3600	AP 3700	AP 700	AP 2700
アクセス ポイント	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
アクセス ポイント（無線シャットダウンにフォールバック）	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
アクセス ポイント（リピータにフォールバック）	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
リピータ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
非ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ワイヤレス クライアントを持つルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
無線クライアントを持つ非ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ワークグループ ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ユニバーサル ワークグループ ブリッジ[1]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
スキャナ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
スペクトル	–	–	–	–	Yes	–	Yes	Yes	Yes	Yes	Yes	–	Yes
インストールするもの [自動 | 非ルート | ルート]	–	–	–	Yes	–	–	–	–	–	–	–	–	–

1. AES-CCM TKIP を使用してユニバーサル ワークグループ ブリッジを設定する場合、非ルート デバイスはルート デバイスとアソシエートするためには、TKIP または AES-CCM TKIP だけを暗号として使用する必要があります。AES-CCM だけで設定した場合、非ルート デバイスはルートとアソシエートできません。この設定により、ルート デバイスと非ルート デバイスの間でマルチキャスト暗号の不一致が発生します。

無線ネットワークでのアクセス ポイントまたはブリッジのロールを設定できます。ルート アクセス ポイントにフォールバック ロールを設定することもできます。ワイヤレス デバイスは、イーサネット ポートがディセーブルになるか、または有線 LAN から切り離されたときに自動的にフォールバック ロール（モード）に移行します。フォールバック ロールとして次の 2 つが挙げられます。

- **Repeater**：イーサネット ポートが無効になった場合、ワイヤレス デバイスはリピータになり、近くのルート アクセス ポイントにアソシエートします。フォールバック リピータがアソシエートするルート アクセス ポイントを指定する必要はありません。リピータは最適な無線接続を提供するルート アクセス ポイントに自動的にアソシエートします。
- **Shutdown**：ワイヤレス デバイスは無線をシャットダウンし、すべてのクライアント デバイスの接続を解除します。

（注） AES-CCM TKIP を使用してユニバーサル ワークグループ ブリッジを設定する場合、非ルート デバイスはルート デバイスとアソシエートするためには、TKIP または AES-CCM TKIP だけを暗号として使用する必要があります。AES-CCM だけで設定した場合、非ルート デバイスはルートとアソシエートできません。この設定により、ルート デバイスと非ルート デバイスの間でマルチキャスト暗号の不一致が発生します。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスの無線ネットワークの役割とフォールバック ロールを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** { **0** | **1** }	次の無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11n 2.4 GHz 無線はインターフェイス 0 です。 5 GHz 無線および 802.11n 5 GHz 無線はインターフェイス 1 です。

	コマンド	目的
ステップ 3	**station-role** **non-root {bridge | wireless-clients}** **repeater** **root {access-point | ap-only | bridge [wireless-clients] |fallback [repeater | shutdown]}** **scanner** **workgroup-bridge** {**multicast | mode** <*client* | *infrastructure*>**| universal** <*Ethernet client MAC address*>}	ワイヤレス デバイスの役割を設定します。 • 役割は、無線クライアントを持つまたは持たない非ルート ブリッジ、リピータ アクセス ポイント、ルート アクセス ポイントまたはブリッジ、スキャナ、またはワークグループ ブリッジに設定します。 • ブリッジ モードの場合、サポートされるブリッジ機能に限り、屋外アクセス ポイント/ブリッジと相互運用します。 • ブリッジ モード無線はポイントツーポイントおよびポイントツーマルチポイント構成をサポートします。 • 非ルート ブリッジとして機能する屋外アクセス ポイント/ブリッジは、非ルート ブリッジのステーション ロールが **non-root wireless clients** に設定されている限り、他の非ルート ブリッジにアソシエートすることができます。 • いずれかの無線がリピータとして設定されると、イーサネット ポートはシャットダウンします。ワークグループ ブリッジまたはリピータとして設定できるのは、アクセス ポイントにつき 1 つの無線だけです。 • **dot11radio 0|1 antenna-alignment** コマンドは、アクセス ポイントがリピータとして設定されるときに使用できます。 • 他の無線クライアントがルート ブリッジまたはアクセス ポイントにアソシエートされていないと仮定すると、ワークグループ ブリッジは最大 254 のクライアントを持つことができます。 • ユニバーサル ワークグループ ブリッジでは、アクセス ポイントをワークグループ ブリッジ モードで設定し、シスコ以外のアクセス ポイントと相互運用できます。イーサネット クライアントの MAC アドレスを入力する必要があります。ワークグループ ブリッジは、設定された MAC アドレスがブリッジ テーブルに存在し、静的エントリでない場合に限り、その MAC アドレスにアソシエートされます。検証に失敗した場合、ワークグループ ブリッジはその BVI の MAC アドレスを使用してアソシエートします。また、ユニバーサル ワークグループ ブリッジの役割では、1 つの有線クライアントだけがサポートされます。 • スパニングツリー プロトコル(STP)は、アクセス ポイントでブリッジ モードで設定できます。 • (任意)ルート アクセス ポイントのフォールバック ロールを選択します。ワイヤレス デバイスのイーサネット ポートが無効になるか、有線 LAN から切断された場合、ワイヤレス デバイスは無線ポートをシャットダウンするか、近くのルート アクセス ポイントにアソシエートしたリピータ アクセス ポイントになります。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

(注)　無線ネットワーク内での役割を非ルート ブリッジまたはワークグループ ブリッジとして有効化し、**no shut** コマンドを使用してインターフェイスを有効化する場合、インターフェイスの物理ステータスおよびソフトウェア ステータスは、相手端末のアクセス ポイントまたはブリッジが起動状態の場合だけ起動状態になります。それ以外の場合、デバイスの物理ステータスだけが起動状態になります。デバイスのソフトウェア ステータスが起動状態になるのは、相手端末のデバイスが設定されて起動しているときだけです。

ユニバーサル ワークグループ ブリッジ モード

ユニバーサル ワークグループ ブリッジの役割を設定する場合は、クライアントの MAC アドレスを含める必要があります。ワークグループ ブリッジがこの MAC アドレスにアソシエートされるのは、MAC アドレスがブリッジ テーブルに存在し、静的エントリでない場合に限られます。検証に失敗した場合、ワークグループ ブリッジはその BVI の MAC アドレスを使用してアソシエートします。ユニバーサル ワークグループ ブリッジ モードでは、ワークグループ ブリッジはイーサネット クライアントの MAC アドレスを使用してシスコまたはシスコ以外のルート デバイスとアソシエートします。ユニバーサル ワークグループ ブリッジは透過的で、管理されません。

(注)　ユニバーサル ワークグループ ブリッジの役割では、1 つの有線クライアントだけがサポートされます。

イーサネット クライアントを無効にし、ユニバーサル ワークグループ ブリッジが独自の BVI アドレスを使用してアクセス ポイントにアソシエートするようにすることによって、復元メカニズムを有効化し、ワークグループ ブリッジを再び管理可能にできます。

「国際線のフライト」シナリオをサポートするために、インターフェイス コマンド **world-mode dot11d country-code** *country* **[indoor | outdoor | both]** にローミング キーワードが追加されています。このキーワードにより、ワークグループ ブリッジはルート アクセス ポイントから認証が取り消されると、パッシブ スキャンを実行します。このコマンドの詳細については、「ワールド モードのイネーブル化とディセーブル化」(P.6-23)を参照してください。

802.11n プラットフォームのポイントツーポイントおよびマルチポイント ブリッジングのサポート

ポイントツーポイントおよびポイントツーマルチポイント ブリッジングはすべての 802.11n アクセス ポイントでサポートされます。5 GHz 帯域は 20 MHz および 40 MHz をサポートし、2.4 GHz 帯域は 20 MHz をサポートします。

次のものはすべての 802.11n アクセス ポイントでサポートされます。

- MIMO、ショートレンジ ブリッジング(キャンパスまたはビルディング間での導入)、1 Km 未満の範囲内でダイポールおよび MIMO アンテナ(ライン オブ サイトおよびショート レンジ)を使用
- 20 MHz および 40 MHz の 802.11n サポート

- ワークグループ ブリッジ（WGB）ショートレンジのサポート
- SISO（Single-In、Single-Out）、1 本の屋外アンテナを使用した MCS 0-7 およびレガシー ブリッジ レート（802.11 a/b/g および 802.11n）

（注）　前述のサポートはショートレンジ リンクでのみサポートされ、AP 1400などのブリッジ製品の置き換えにはなりません。

内部アンテナを持つブリッジ モードの AP モデルでは、次のものはサポートされません。

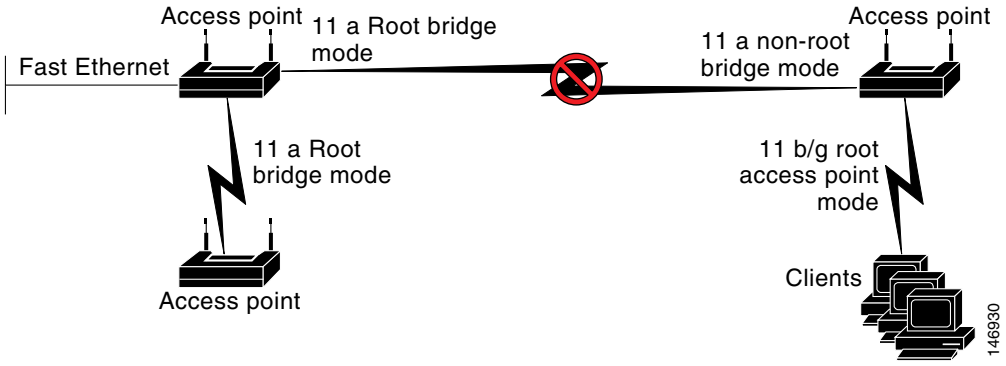
- **distance** コマンド。**distance** コマンドは、屋外での使用が認可されているアクセス ポイントでのみサポートされます。
- 外部アンテナを使用する外部 MIMO ブリッジング。

（注）　ポイントツーマルチポイント ブリッジングでは、ルート ブリッジによる WGB は推奨されません。ポイントツーマルチポイント ブリッジング設定では、WGB はルート AP に関連付ける必要があります。

デュアル無線フォールバックの設定

デュアル無線フォールバック機能を使用すると、アクセス ポイントをネットワーク インフラストラクチャに接続する非ルート ブリッジ リンクがダウンしたとき、クライアントがアクセス ポイントに接続する際に使用するルート アクセス ポイント リンクがシャットダウンするようにアクセス ポイントを設定できます。ルート アクセス ポイント リンクをシャットダウンすると、クライアントは別のアクセス ポイントにローミングを切り替えます。この機能がない場合、クライアントはアクセス ポイントに接続されたままになりますが、ネットワークとデータを送受信できません。

図 6-1　　デュアル無線フォールバック



（注）　この機能はすべてのデュアル無線アクセス ポイントでサポートされます。
この機能はシングル無線アクセス ポイントのフォールバック機能に影響しません。

デュアル無線フォールバックは、次の 3 つの方法で設定できます。

- 無線トラッキング
- ファスト イーサネット トラッキング
- MAC アドレス トラッキング

無線トラッキング

アクセス ポイントのいずれかの無線の状態を追跡またはモニタするようにアクセス ポイントを設定できます。追跡対象の無線がダウンするか無効になると、アクセス ポイントは別の無線をシャットダウンします。追跡対象の無線が起動すると、アクセス ポイントは別の無線をイネーブルにします。

- 無線 0 を追跡するには、無線 1 で次のコマンドを入力してください。

  ```
  # station-role root access-point fallback track d0 shutdown
  ```

- 無線 1 を追跡するには、無線 0 で次のコマンドを入力してください。

  ```
  # station-role root access-point fallback track d1 shutdown
  ```

ファスト イーサネット トラッキング

アクセス ポイントのイーサネット ポートがディセーブルになったり、または有線 LAN から切断されたりしたときにフォールバックするようにアクセス ポイントを設定できます。アクセス ポイントをファスト イーサネット トラッキング用に設定するには、「無線ネットワークの役割の設定」（P.6-3）で説明するようにして行います。

（注）　ファスト イーサネット トラッキングは、リピータ モードをサポートしません。

- ファスト イーサネット トラッキングに対して 802.11n 以外のアクセス ポイントを設定するには、無線インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

  ```
  # station-role root access-point fallback track fa 0
  ```

- ギガビット イーサネット トラッキングに対して 802.11n のアクセス ポイントを設定するには、無線インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

  ```
  # station-role root fallback shutdown
  ```

MAC アドレス トラッキング

非ルート ブリッジまたはワークグループ ブリッジをその MAC アドレスを使用して別の無線でトラッキングすることによって、ルート アクセス ポイントの役割を持つ無線を起動またはダウンするように設定できます。クライアント アクセス ポイントからのアソシエーションが解除されると、ルート アクセス ポイントの無線はダウンします。クライアントがアクセス ポイントと再アソシエートすると、ルート アクセス ポイント無線は起動状態に戻ります。

クライアントがアップストリームの有線ネットワークに接続されている非ルート ブリッジ アクセス ポイントの場合、MAC アドレス トラッキングが最も便利です。

たとえば、MAC アドレスが 12:12:12:12:12:12 の非ルート ブリッジまたはワークグループ ブリッジをトラッキングするには、次のコマンドを入力します。

```
# station-role root access-point fallback track mac-address 12:12:12:12:12:12 shutdown
```

無線ごとのクライアントの制限

インターフェイスにアソシエートされるクライアントの数を設定するには、dot11 無線インターフェイス設定で、コマンド **max-client** *1-255* を使用します。デフォルトでは、この機能はディセーブルになっています。許可されるクライアントの最小数は 1 で、最大数は 255 です。

```
ap(config-if)# max-client 1-255
```

この設定を GUI で行うには、次の手順に従います。

ステップ 1　[Network] > [Network Interfaces] に移動します。

ステップ 2　サイド メニューで、クライアントを制限する無線インターフェイスに応じて、[Dot11 Radio 2.4 GHz] または [Dot11 Radio 5 GHZ] をクリックします。

ステップ 3　無線インターフェイスの設定ページで、[Max-Client] オプションをイネーブルまたはディセーブルにできます。

ステップ 4　[Max-Client] オプションをイネーブルにした場合、[Max-Client] オプションの横にあるテキスト ボックスに、インターフェイスにアソシエートするクライアントの数を指定します。

ステップ 5　[Apply] をクリックします。

無線データ レートの設定

データ レート設定を使用して、ワイヤレス デバイスのデータ転送に使用されるデータ レートを選択します。レートの単位は Megabits per second（Mbps; メガビット/秒）です。ワイヤレス デバイスは、CLI または GUI インターフェイスで設定した最大のデータ レートで転送しようとします。障害や干渉などがある場合、ワイヤレス デバイスはデータ転送が可能な範囲で次に速いレートまで減速されます。各データ レートは、次の 3 つのステートのいずれかに設定できます。

- Basic（GUI では Basic レートを [Required] と表示）：ユニキャストとマルチキャストの両方で、すべてのパケットをこのレートで転送します。ワイヤレス デバイスのデータ レートの少なくとも 1 つは Basic に設定してください。
- Enabled：ワイヤレス デバイスでは、ユニキャスト パケットだけがこのレートで送信され、マルチキャスト パケットは、Basic に設定されているいずれかのデータ レートで送信されます。
- Disabled：ワイヤレス デバイスでは、データはこのレートで送信されません。

（注）　少なくともデータ レートの 1 つは **basic** に設定してください。

Data Rate の設定を使用すると、特定のレートでデータを転送するクライアント デバイスに対応するようにアクセス ポイントを設定できます。2.4 GHz、802.11g 無線を、802.11g クライアント デバイスだけに対応するように設定するには、Orthogonal Frequency Division Multiplexing（OFDM; 直交周波数分割多重方式）データ レート（6、9、12、18、24、36、48、54）を、すべて **Basic** に設定します。

また、範囲またはスループットが最適になるようなデータ レートが自動的に設定されるように、ワイヤレス デバイスを設定することも可能です。データ レート設定に **range** を入力した場合、ワイヤレス デバイスでは 1Mbps レートは Basic に、他のレートは Enabled に設定されます。この range 設定によって、アクセス ポイントではデータ レートについて妥協することでカバレッジ領域を拡大できます。したがって、他のクライアントがアクセス ポイントに接続できるときに接続できないクライアントがいる場合、そのクライアントがアクセス ポイントのカバレッジ領域にいないことが理由の 1 つである場合があります。そのような場合に range オプションを使用すると、カバレッジ領域を拡大するために役立ち、クライアントはアクセス ポイントに接続できる場合があります。通常、スループットと範囲が交換条件となります。(おそらくアクセス ポイントからの距離が原因で)信号が劣化すると、リンクを維持するために(データ レートを下げて)レートが再ネゴシエートされます。これと対照をなすのはスループットを高く設定したリンクで、設定された高いデータ レートを維持できなくなるほど信号が劣化すると、スループットが低下します。または、十分な適用範囲を持つ他のアクセス ポイントが利用できる場合、そのアクセス ポイントにローミングが切り替わります。両者のバランス(スループットと 範囲)は、決定する必要がある設計上の判断の 1 つです。判断を下す際、無線プロジェクトに利用できるリソース、ユーザが渡すトラフィックのタイプ、必要なサービス レベル、そして常に RF 環境の品質が根拠となります。データ レート設定に **throughput** を入力すると、ワイヤレス デバイスではすべてのデータ レートを **basic**(たとえば、2.4 Ghz で 12 のレート、5 GHz で 8 のレート)に設定します。

(注) 802.11b クライアントと 802.11g クライアントが混在する環境の無線ネットワークの場合、1、2、5.5、および 11Mbps のデータ レートが必須(**basic**)に設定され、他のすべてのデータ レートが **enable** に設定されていることを確認します。802.11b アダプタは 802.11g レートを認識せず、接続先のアクセス ポイントで 11Mbps よりも高いデータ レートが必要だと設定されている場合は動作しません。

マルチキャスト フレームと管理フレームを最高の Basic レートで送信するアクセス ポイント

最近のバージョンの Cisco IOS を実行するアクセス ポイントは、設定された最高の Basic レートでマルチキャスト フレームと管理フレームを送受信し、この状況で信頼性の問題が発生することがあります。

LWAPP または自律 IOS を実行するアクセス ポイントは、設定された最低の Basic レートでマルチキャスト フレームと管理フレームを送受信します。これはセルの端に十分なカバレッジを提供するために必要で、マルチキャスト無線送信を受信できないことがある受信応答しないマルチキャスト転送では特に必要です。

マルチキャスト フレームは MAC レイヤで再送信されないため、セルの端のステーションはマルチキャスト フレームを正常に受信できない場合があります。信頼性の高い受信が目的の場合、マルチキャストは低いデータ レートで送信する必要があります。高いデータ レートのマルチキャストをサポートする必要がある場合、セル サイズを縮小して低いデータ レートをすべて無効にすることが役立つ場合があります。

特定の要件に応じて、次の処置が可能です。

- 信頼性を最大限に高めてマルチキャスト データを送信する必要があって、マルチキャストの帯域幅は大きくする必要がない場合、単一の Basic レートを設定し、無線セルの端に到達するために十分な低さにします。
- 特定のスループットを達成するために特定のデータ レートでマルチキャスト データを送信する必要がある場合、そのレートを最高の Basic レートとして設定します。また、マルチキャスト以外のクライアントのカバレッジのために、低い Basic レートを設定することも可能です。

特権 EXEC モードから、次の手順に従って無線データ レートを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線および 2.4 GHz N 無線は Radio 0、5 GHz 無線および 5 GHz N 無線は Radio 1 です。

コマンド	目的
ステップ 3　**speed** 802.11g、2.4 GHz 無線の場合： {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** [**ofdm**] | **default** } 802.11a 5 GHz 無線の場合： {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **ofdm-throughput** | **default**} 802.11n 2.4 GHz 無線の場合： {[**1.0**] [**11.0**] [**12.0**] [**18.0**] [**2.0**] [**24.0**] [**36.0**] [**48.0**] [**5.5**] [**54.0**] [**6.0**] [**9.0**] [**basic-1.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-5.5**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] [**ofdm**] [**only-ofdm**] | **range** | **throughput**} 802.11n 5 GHz 無線の場合： {[**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**6.0**] [**9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] | **range** | **throughput**}	各データ レートを **Basic** または **Enabled** に設定するか、**range** を入力して範囲を最適化するか、あるいは **throughput** を入力してスループットを最適化します。 • （任意）**basic-1.0**、**basic-2.0**、**basic-5.5**、**basic-6.0**、**basic-9.0**、**basic-11.0**、**basic-12.0**、**basic-18.0**、**basic-24.0**、**basic-36.0**、**basic-48.0**、および **basic-54.0** を入力すると、802.11g、2.4 GHz 無線でこれらのデータ レートが **basic** に設定されます。 **（注）** 選択した Basic レートをクライアントがサポートしている必要があります。そうでないと、クライアントはそのワイヤレス デバイスにアソシエートできません。802.11g 無線の Basic データ レートに 12 Mbps 以上を選択した場合、802.11b クライアント デバイスは、ワイヤレス デバイスの 802.11g 無線にアソシエートできません。 **basic-6.0**、**basic-9.0**、**basic-12.0**、**basic-18.0**、**basic-24.0**、**basic-36.0**、**basic-48.0**、および **basic-54.0** を入力すると、5 GHz 無線でこれらのデータ レートが **basic** に設定されます。 （任意）あるいは、**range** または **throughput** または ofdm-throughput（ERP 保護なし）を入力すると、無線範囲またはスループットが自動的に最適化されます。**range** を入力すると、ワイヤレス デバイスは最も低いデータ レートを Basic に設定し、他のレートを **Enabled** に設定します。**throughput** を入力すると、ワイヤレス デバイスはすべてのデータ レートを **basic** に設定します。 （任意）802.11g 無線で、すべての OFDM レート（6、9、12、18、24、36、および 48）を Basic（Required）に設定し、すべての Complementary Code Keying（CCK; 相補コードキー入力）レート（1、2、5.5、および 11）を Disabled に設定するには、**speed throughput ofdm** を入力します。この設定により、802.11b 保護機能がディセーブルとなり、802.11g クライアントに最大のスループットが提供されます。ただし、802.11b クライアントはそのアクセス ポイントにアソシエートできなくなります。 • （任意）**default** を入力すると、データ レートは工場出荷時の設定になります（802.11b 無線ではサポートされていません）。 802.11g 無線では、**default** オプションによって、レート 1、2、5.5、および 11 は Basic に、レート 6、9、12、18、24、36、48、および 54 は Enabled に設定されます。これらのレート設定を使用すると、802.11b および 802.11g の両方のクライアント デバイスをワイヤレス デバイス 802.11g 無線に関連付けできるようになります。 5 GHz 無線では、**default** オプションによって、レート 6.0、12.0、および 24.0 は Basic に、レート 9.0、18.0、36.0、48.0、および 54.0 は Enabled に設定されます。

	コマンド	目的
	speed（続き）	802.11n 2.4 GHz 無線では、**default** オプションによって、レート 1.0、2.0、5.5、および 11.0 が Enabled に設定されます。 802.11n 5 GHz 無線では、**default** オプションによって、6.0、12.0、および 24.0 が Enabled に設定されます。 802.11n 無線のデフォルト MCS レート設定は 0 ～ 15 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定から 1 つ以上のデータ レートを削除する場合は、**speed** コマンドの **no** 形式を使用します。次の例は、設定からデータ レート basic-2.0 と basic-5.5 を削除する方法を示しています。

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# no speed basic-2.0 basic-5.5
ap(config-if)# end
```

MCS レートの設定

Modulation Coding Scheme（MCS; 変調および符号化方式）は、変調順序（BPSK、QPSK、16-QAM、64-QAM）および FEC コード レート（1/2、2/3、3/4、5/6）で構成される PHY パラメータの仕様です。MCS は、802.11n 無線で使用されており、32 個の対称設定を定義します（空間ストリームあたり 8 個）。

- MCS 0 ～ 7
- MCS 8 ～ 15
- MCS 16 ～ 23
- MCS 24 ～ 31

MCS は高いスループットを実現する可能性があるため、重要な設定です。高いスループットのデータ レートは、*MCS*、*帯域幅*、および*ガード間隔*の関数です。802.11 a、b、および g 無線は 20MHz のチャネル幅を使用します。

ヒント　アクセス ポイントに対する MCS インデックス、ガード インターバル（GI）、チャネル幅に基づくデータ レートの最新情報については、Cisco.com サイトの『*Cisco Aironet (AP series name) Series Access Points Data Sheet*』を参照してください。

MCS レートは **speed** コマンドを使用して設定します。次の例は、802.11n 5 GHz 無線の **speed** 設定を示しています。

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 1260test
```

```
!
speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
m0.m1.m2.m3.m4.m8.m9.m10.m11.m12.m13.m14.m15.
```

11ac MCS レートのイネーブル化

MCS レートは **speed** コマンドを使用して設定します。

11ac レートをイネーブルにするには、少なくとも 1 つの基本レートと 1 つの 11n レートをイネーブルにする必要があります。

次の例は、802.11ac 5-GHz 無線の **speed** 設定を示しています。

```
interface Dot11Radio1
!
!
ssid 11ac
!
speed 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
m0.m1.m2.m3.m4.m5.m6.m7.m8.m9.m10.m11.m12.m13.m14.m15.m16.m17.m18.m19.m20.m21.m22.m23.a1ss
9 a2ss9 a3ss9
Channel width 80
```

無線の送信電力の設定

無線の送信電力は、使用するアクセス ポイントに導入されている 1 つ以上の無線のタイプと、アクセス ポイントが動作する規制ドメインに基づきます。アクセス ポイントで使用できる伝送電力と、アクセス ポイントが動作する規制地域について調べるには、デバイスのハードウェア インストレーション ガイドを参照してください。ハードウェア インストレーション ガイドは cisco.com から入手できます。表示およびダウンロードする手順は、次のとおりです。

ステップ 1　http://www.cisco.com を表示します。

ステップ 2　[Technical Support & Documentation] をクリックします。テクニカルサポート リンクのリストを含む小さいウィンドウが表示されます。

ステップ 3　[Technical Support & Documentation] をクリックします。[Technical Support and Documentation] ページが表示されます。

ステップ 4　[Documentation & Tools] セクションで、[Wireless] を選択します。[Wireless Support Resources] ページが表示されます

ステップ 5　[Wireless LAN Access] セクションで、操作するデバイスを選択します。デバイスの概要ページが表示されます。

ステップ 6　[Install and Upgrade] セクションで、[Install and Upgrade Guides] を選択します。デバイスの [Install and Upgrade Guides] ページが表示されます。

ステップ 7　デバイスのハードウェア インストレーション ガイドを選択します。ガイドのホームページが表示されます。

ステップ 8　左のフレームで、[Channels and Antenna Settings] をクリックします。

表 6-2 は、mW と dBm の関係を示しています。

表 6-2　　mW と dBm との変換

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線の伝送電力を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 2.4 GHz 802.11n 無線は 0、5 GHz 802.11n 無線は 1 です。
ステップ 3	**power local** これらのオプションは、802.11a、5-GHz 無線（dBm）、および 2.4-GHz 802.11n 無線（dBM）で利用可能です。 **{22 | 19 | 16 | 13 | 10 | 7 | 4}**	802.11b、2.4 GHz 無線または 5 GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。 **（注）**　規制地域の電力設定について調べるには、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。
ステップ 4	**power local** 次のオプションは、802.11g、2.4 GHz 無線について使用できます。 **power local cck** 設定： { **-1** | **2** | **5** | **8** | **11** | **14** | **17** | **20** | **maximum** } **power local ofdm** 設定： { **-1** | **2** | **5** | **8** | **11** | **14** | **17** |**maximum** } **（注）**　これらのオプションは 802.11n AP では利用できません。	802.11g、2.4 GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。設定は dBm 単位です。 2.4 GHz の 802.11g 無線では、直交周波数分割多重方式（OFDM）と Complementary Code Keying（CCK; 相補コードキー入力）のいずれかの電力レベルを設定できます。CCK 変調は、802.11b デバイスおよび 802.11g デバイスによってサポートされています。OFDM 変調は、802.11g デバイスおよび 802.11a デバイスによってサポートされています。 **（注）**　規制地域の電力設定について調べるには、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。 **（注）**　802.11g 無線の最大送信電力レベルは AP モデルによって異なります。電力レベルについては AP データ シートを参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

電力設定をデフォルトの **maximum** に戻すには、power コマンドの **no** 形式を使用します。

アソシエートしたクライアント デバイスの電力レベルの制限

ワイヤレス デバイスにアソシエートしたクライアント デバイスの電力レベルを制限することもできます。クライアント デバイスがワイヤレス デバイスにアソシエートするとき、ワイヤレス デバイスはクライアントに最大電力レベル設定を送信します。

（注） Cisco AVVID のマニュアルでは、アソシエートされたクライアント デバイスの電力レベルの制限を示すのに Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）という用語を用います。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスにアソシエートするすべてのクライアント デバイスに、最大許可電力設定を指定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 2.4 GHz 802.11n 無線は 0、5 GHz 802.11n 無線は 1 です。
ステップ 3	**power client** これらのオプションは、802.11n 2.4-GHz と 5-GHz クライアント（dBm）の両方で利用可能です。 {*-127 to 127* | **local** | **maximum**}	ワイヤレス デバイスにアソシエートするクライアント デバイスに、許可電力レベルを設定します。次の作業を実行できます。 • -127 ～ 127 dBm の任意の電力レベル値を設定します。 • クライアント電力レベルをアクセス ポイントの電力レベルに設定するには、電力レベルを **local** に設定します。 • クライアント電力を許可される最大値に設定するには、電力レベルを **maximum** に設定します。 **（注）** 規制ドメインで許容される設定は、ここで取り上げる設定と異なる場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アソシエートしたクライアントの最大電力レベルを無効にするには、client power コマンドの **no** 形式を使用します。

（注） アソシエートしたクライアント デバイスの電力レベルを制限する場合は、Aironet 拡張機能をイネーブルにする必要があります。Aironet 拡張機能はデフォルトではイネーブルに設定されています。

無線チャネルの設定

ワイヤレス デバイスの無線のデフォルト チャネル設定は Least Congested です。起動時にワイヤレス デバイスは最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。ワイヤレス デバイスのチャネル設定は、規制ドメインで使用できる周波数に対応します。ドメインで許可されている周波数については、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。

（注） RF 干渉が原因でクライアントが無線からときどき切断されている場所では、チャネル 1（2412）などの別のチャネルで動作するように無線インターフェイスを設定すると干渉を回避できる場合があります。

2.4 GHz 帯チャネル利用帯域幅は、チャネルあたり 22 MHz になります。チャネル 1、6、11 は重複していないため、干渉を起こさずに、同じ圏内に複数のアクセス ポイントを設定できます。802.11b および 802.11g の 2.4GHz 無線はいずれも同じチャネルと周波数を使用します。

5-GHz 無線は、802.11n AP で 5180 ～ 55825 MHz の 9 つのチャネル、1140 シリーズ AP で 5180 ～ 5805 の 8 つのチャネルで動作します。各チャネルは 20 MHz に対応し、チャネルの帯域幅は少しずつ重複しています。最適なパフォーマンスを得るため、互いに近い位置にある無線の場合は、隣接していないチャネル（たとえば、44 と 46）を使用します。

（注） 同じ圏内に多くのアクセス ポイントを設定しすぎると、無線の輻輳が発生し、スループットが減少します。無線のサービス範囲とスループットを最大にするには、慎重なサイト調査を行って、アクセス ポイントの最適な設置場所を決定する必要があります。

チャネル設定は頻繁に変更されるため、このマニュアルには記載されていません。ご使用のアクセス ポイントまたはブリッジのチャネル設定についての最新情報は、『*Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges*』を参照してください。このマニュアルは cisco.com の次の URL から入手できます。

http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html

802.11n のチャネル幅

802.11n では、20 MHz および 40 MHz の両方のチャネル幅が使用可能です。チャネル幅は、2 つの連続する重複しないチャネル（たとえば、5 GHz のチャネル 36 およびチャネル 40）で構成されます。802.11n 無線は、同じ帯域で動作します。ただし、チャネル幅は個別に設定できます。

20MHz チャネルの 1 つは*コントロール チャネル*と呼ばれます。レガシー クライアントおよび 20MHz の高いスループットのクライアントはコントロール チャネルを使用します。ビーコンを送信できるのはこのチャネルだけです。2 番目の 20MHz チャネルは*拡張チャネル* と呼ばれます。40MHz のステーションは、このチャネルとコントロール チャネルを同時に使用できます。

40 MHz チャネルは、チャネルとして指定され、拡張は -1 として指定されます。ここでは、コントロール チャネルはチャネル 40 MHz、拡張チャネルがその下の 36 MHz です。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスのチャネル幅を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11n 2.4 GHz 無線は Radio 0 です。 5 GHz 無線および 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	ワイヤレス デバイス無線のデフォルト チャネルを設定します。起動時に最も混雑の少ないチャネルを探す場合は、**least-congested** を入力します。 使用する帯域幅を指定するには **width** オプションを使用します。このオプションはすべての 802.11n AP で利用できますが、d1（5 GHz）無線のみです。設定は 3 つあります。20、40-above、40-below です。20 を選択すると、チャネル幅が 20 MHz に設定されます。40-above を選択すると、拡張チャネルをコントロール チャネルの上に重ねた状態でチャネル幅が 40 MHz に設定されます。40-below を選択すると、拡張チャネルをコントロール チャネルの下に重ねた状態でチャネル幅が 40 MHz に設定されます。 **（注）** 動的周波数選択（DFS）に関する欧州連合の規制に準拠する 5 GHz の無線については、**channel** コマンドはディセーブルに設定されています。詳細については、「802.11n ガード間隔の設定」（P.6-23）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

動的周波数選択（DFS）

工場出荷時に 5 GHz 無線が設定されている、米国、ヨーロッパ、シンガポール、韓国、日本、イスラエル、および台湾向けのアクセス ポイントは、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動的周波数選択（DFS）の使用を必須とする規制に従うようになりました。アクセス ポイントが特定のチャネルでレーダーを検出すると、そのチャネルを 30 分間使用しないようにします。その他の規制地域向けに設定する無線では、DFS を使用しません。

DFS を有効に設定した 5 GHz 帯無線を 表 6-3 に記載した 15 チャネルのいずれかで動作させると、アクセス ポイントが自動的に DFS を使用して動作周波数を設定します。DFS が有効に設定されると、アクセス ポイントが自身の動作周波数にレーダー信号がないかモニタするようになります。同じチャネルにレーダー信号を検出した場合は、アクセス ポイントが次の処理を実行します。

- チャネル上でそれ以降の伝送をブロックします。
- 省電力モードのクライアントからのキューを消去します。
- 802.11h チャネル切り替えアナウンスメントをブロードキャストします。
- 残りのクライアント デバイスのアソシエーションを解除します。

- Wireless Domain Service（WDS; 無線ドメイン サービス）に参加している場合、周波数を終了する DFS 通知をアクティブな WDS デバイスに送信します。
- 別の 5 GHz チャネルを無作為に選択します。
- 選択したチャネルが 表 6-3 のいずれかのチャネルだった場合は、そのチャネルにレーダー信号がないか 60 秒間スキャンします。
- そのチャネルにレーダー信号がなければ、ビーコンを有効にしてクライアントのアソシエーションを受け入れます。
- WDS に参加している場合、アクティブな WDS デバイスに新しい動作周波数を知らせる DFS 通知を送信します。

（注）　規制要件に従い、一部の地域では、DFS を有効に設定した 5 GHz 帯無線のチャネルを手動で選択できません。この場合、アクセス ポイントが無作為にチャネルを選択します。

DFS が必要なチャネルのすべてのリストを、表 6-3 に示します。

表 6-3　DFS チャネル リスト

チャネル	周波数	チャネル	周波数	チャネル	周波数
52	5260MHz	104	5500MHz	124	5620MHz
56	5280MHz	108	5520MHz	128	5640MHz
60	5300MHz	112	5560MHz	132	5660MHz
64	5320MHz	116	5580MHz	136	5680MHz
100	5500MHz	120	5600MHz	140	5700MHz

自律動作を行うために、DFS では 表 6-3 にリストされているチャネルから無作為にチャネルを選択することが必要です。表 6-3 にリストされていないチャネルは無作為な選択が不要で、手動で設定できます。

動的周波数選択（DFS）が必要なチャネルは 5 GHz の無線設定メニューから手動で選択することができます。DFS チャネルを確認するには、**show controllers d1** コマンドを使用します。

また、手動で非 DFS チャネルを設定する場合の GUI/CLI を使用して、DFS チャネルを選択することもできます。デフォルトのチャネル選択は「DFS」であり、無作為にチャネルが選択されます。

手動で設定された DFS チャネルでレーダーが検出された場合、そのチャネルは自動的に変更され、設定したチャネルには戻りません。

表 6-3 にリストされているチャネルで送信する前に、アクセス ポイント無線は Channel Availability Check（CAC）を実行します。CAC はチャネルに無線信号が存在するかを調べる 60 秒のスキャンです。次のメッセージ例は、CAC スキャンの開始と終了を示すもので、アクセス ポイントのコンソールに表示されます。

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5500 MHz for
60 seconds

*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency
5500 MHz
```

表 6-3 に記載されている DFS チャネルを稼働すると、アクセス ポイントでは、CAC を実行しているため、チャネル上にレーダーがないかどうかを常に監視します。レーダーが検出されると、アクセス ポイントはデータ パケットの転送を 200 ミリ秒間停止し、802.11h チャネル切り替えの通知を含む 5 つのビーコンを同報通信し、アクセス ポイントが使用を開始するチャネル番号を指示します。次のメッセージ例は、レーダーが検出されたときにアクセス ポイント コンソールに表示されます。

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5500 MHz
```

チャネルにレーダーが検出されると、そのチャネルは 30 分間使用できません。アクセス ポイントは、過去 30 分のうちにチャネルにレーダーを検出した各チャネルのフラグを不揮発性ストレージに維持します。30 分が過ぎると、対応するチャネルのフラグがクリアされます。フラグがクリアされる前にアクセス ポイントがリブートすると、チャネルの初期化中に非占有時間が 30 分にリセットされます。

（注） 適法な最大送信電力については、他のチャネルよりも 5 GHz チャネルの方が大きくなるものがあります。無作為に選択した 5 GHz チャネルが電力を制限されていた場合、アクセス ポイントはそのチャネルの電力上限に合うように自動的に送信電力を下げます。

（注） DFS が有効に設定された無線で国番号を設定するには、**world-mode dot11d** *country-code* 設定インターフェイス コマンドを使用することを推奨します。IEEE 802.11h プロトコルでは、アクセス ポイントはビーコンとプローブ応答に国情報エレメント（IE）を含める必要があります。ただしデフォルトでは、IE の国番号は空白に設定されています。**world-mode** コマンドで、国番号 IE を入力してください。

DFS チャネルでのレーダー検出

DFS チャネルでアクセス ポイントがレーダーを検出すると、そのアクセス ポイントはフラッシュ メモリ内にファイルを作成します。このファイルは 802.11a 無線のシリアル番号に基づいたもので、レーダーが検出されたチャネルの番号が記録されています。これは正常な動作です。このファイルは削除しないでください。

CLI コマンド

次の項では、DFS に適用される CLI コマンドを説明します。

DFS が有効に設定されているかどうかの確認

DFS が有効に設定されているかどうかを確認するには、**show controllers dot11radio1** コマンドを使用します。コマンドには、均一拡散（Uniform Spreading）が必須であること、およびレーダーの検出が原因で非占有期間にあるチャネルの表示も含まれます。

次の例は、DFS が有効になっているチャネルで show controller コマンドを実行した時の出力行を示しています。前のパラグラフにリストで表示された内容は、**太字**で記載されています。

```
ap#sh controllers dot11Radio 1
!
interface Dot11Radio1
Radio ElliotNess 5, Base Address f4ea.6710.6590, BBlock version 0.00, Software version
4.10.1
Serial number: FOC16145K24
```

```
Unused dynamic SQRAM memory: 0x00007CB4 (31 KB)
Unused dynamic SDRAM memory: 0x0008E490 (569 KB)
Spectrum FW version: 1.14.2
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: Americas (OFDM) (US) (-A)
Uniform Spreading Required: Yes
Configured Frequency: 0 MHz  Channel 0
Allowed Frequencies: * Dynamic Frequency Selection (DFS) only
         5180( 36)  5200( 40)  5220( 44)  5240( 48) *5260( 52) *5280( 56) *5300( 60)
*5320( 64) *5500(100) *5520(104)
        *5540(108) *5560(112) *5580(116) *5660(132) *5680(136) *5700(140)  5745(149)
5765(153)  5785(157)  5805(161)
         5825(165)
Listen Frequencies:
         5180( 36)  5200( 40)  5220( 44)  5240( 48)  5260( 52)  5280( 56)  5300( 60)
5320( 64)  5500(100)  5520(104)
         5540(108)  5560(112)  5580(116)  5600(120)  5620(124)  5640(128)  5660(132)
5680(136)  5700(140)  5745(149)
         5765(153)  5785(157)  5805(161)  5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0, Interface Flags 20109, Interface Events 0, Mode 9; Beacons are disabled;
Probes are disabled
Configured TxPower:             14 dBm
Allowed Power Levels:           14 11  8  5  2  dBm
Allowed Client Power Levels:    14 11  8  5  2  dBm
Antenna:                        Rx[a b c d ]
                                Tx[a b c d  ofdm all]
                                External
                                Gain [Allowed 12, Reported 0, Configured 0, In Use 12]
(dBi x 2)
```

チャネルの設定

チャネルを設定するには **channel** コマンドを使用します。インターフェイスのコマンドは、特定のチャネル番号を選択して DFS を有効にすることだけをユーザに許可するように変更されています。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio1 dfs**	802.11a 無線のインターフェイス設定を開始します。

	コマンド	目的
ステップ 3	**channel** {*number* | **dfs** |**band** <*1 - 4*>}	*number* には、36 から 5825 のチャネル周波数を入力します。 選択されたチャネルで動的周波数選択を使用するには、**dfs** および次のいずれかの周波数帯を入力します。 1:5.150 ～ 5.250 GHz 2:5.250 ～ 5.350 Ghz 3:5.470 ～ 5.725 GHz 4:5.725 ～ 5.825 GHz DFS だけで選択できるチャネルを設定しようとすると、次のメッセージが表示されます。 `This channel number/frequency can only be used by Dynamic Frequency Selection (DFS)` **（注）** **channel dfs** コマンドは、-P および -Q 規制ドメインではサポートされません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに入力内容を保存します。

次の例では、DFS を使用するように 5 GHz の無線を設定します。

```
ap# configure terminal
ap(config)# interface dot11radio1
ap(config-if)# channel dfs
ap(config-if)# end
```

DFS 選択によるチャネル ブロック

屋内や屋外など特定地域で使用できるチャネルを制限している規制地域の場合、DFS が有効になっている時にアクセス ポイントがそれらを選択しないようチャネルをまとめてブロックすることができます。DFS 選択によってチャネルをまとめてブロックするには、次の設定インターフェイス コマンドを使用してください。

[no] dfs band [1] [2] [3] [4] block

オプション 1、2、3、4 で、ブロック対象のチャネルを指定します。

- **1**:5.150 ～ 5.250 GHz の周波数を指定します。この周波数グループは UNII-1 帯域とも呼ばれています。
- **2**:5.250 ～ 5.350 GHz の周波数を指定します。この周波数グループは UNII-2 帯域とも呼ばれています。
- **3**:5.470 ～ 5.725 GHz の周波数を指定します。この周波数グループは UNII-2 拡張とも呼ばれています。
- **4**:5.725 ～ 5.825 GHz の周波数を指定します。この周波数グループは UNII-3 帯域とも呼ばれています。

次の例は、DFS 中にアクセス ポイントが 5.150 ～ 5.350 GHz の周波数を選択しないようにする方法を示しています。

```
ap(config-if)# dfs band 1 2 block
```

次の例は、DFS について 5.150 ～ 5.350 GHz の周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band 1 2 block
```

次の例は、DFS についてすべての周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band block
```

802.11n ガード間隔の設定

802.11n ガード間隔は、パケット間のナノ秒単位の時間です。短時間（400ns）および長時間（800ns）の 2 つの設定が可能です。

特権 EXEC モードから、次の手順に従って 802.11n ガード間隔を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 | 1}**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 802.11n 2.4 GHz 無線は Radio 0 です。 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**guard-interval {any | long}**	ガード間隔を入力します。 • any では、ショート GI をサポートするクライアントで AP が 400 ns を使用できるようにし、また ショート GI をサポートしないクライアントでは 800 ns を使用できるようにします。つまり、ショート（400ns）またはロング（800ns）いずれかのガード間隔です。 • long では、ロング（800ns）ガード間隔のみを使用できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワールド モードのイネーブル化とディセーブル化

ワイヤレス デバイスで、802.11d ワールド モード、Cisco レガシー ワールド モード、またはワールド モード ローミングをサポートするよう設定できます。ワールド モードをイネーブルにすると、AP はそのビーコンにチャネル キャリア セット情報を追加します。ワールド モードがイネーブルになっているクライアント デバイスは、キャリア セット情報を受信して、それぞれの設定を自動的に調整します。たとえば、日本で主に使用されるクライアント デバイスがイタリアに移され、そこでネットワークに参加した場合、ワールド モードに依存して、そのチャネルと電力の設定を自動的に調整することができます。

ワールド モードはデフォルトではディセーブルに設定されています。

特権 EXEC モードから、次の手順に従ってワールド モードを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0***slot*/*port* | **1**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**world-mode** **dot11d country_code** *code* { **both** | **indoor** | **outdoor** } **world-mode roaming** | **legacy**	ワールド モードを有効にします。 • 802.11d ワールド モードをイネーブルにするには、**dot11d** オプションを入力します。 – **dot11d** オプションを入力する場合、2 文字の ISO 国番号（たとえば、米国の ISO 国番号は **US**）を入力する必要があります。ISO 国番号の一覧は ISO の Web サイトに掲載されています。 – 国番号の後に、ワイヤレス デバイスの配置場所を示すために **indoor**、**outdoor**、または **both** と入力します。 • シスコのレガシー ワールド モードをイネーブルにするには、**legacy** オプションを入力します。 • アクセス ポイントを継続的なワールド モード構成に配置するには、**world-mode roaming** と入力します。 **（注）** レガシー ワールド モードを使用するには、Aironet 拡張機能をイネーブルにする必要がありますが、802.11d ワールド モードではこの拡張機能は不要です。Aironet 拡張機能はデフォルトではイネーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワールド モードを無効にするには、コマンドの **no** 形式を使用します。

short 無線プリアンブルのイネーブル化とディセーブル化

無線プリアンブルは、AP とクライアントが通信を同期するのに役立つフレームの先頭にあるデータのセクションです。無線プリアンブルを long または short に設定できます。

- Short：short プリアンブルを使用すると、スループットのパフォーマンスが向上します。Cisco Aironet 無線 LAN クライアント アダプタは、短いプリアンブルをサポートします。802.11b または 802.11g 認定デバイスはどれも短いプリアンブルをサポートします。ただし、クライアント デバイスによっては、802.11b/g 認定の場合でも、長いプリアンブルを必要とします。
- Long：長いプリアンブルは、レガシー 802.11 のみのデバイス、および最適な運用で長いプリアンブルを予期する一部の 802.11b/g デバイスで使用されます。これらのクライアント デバイスがワイヤレス デバイスにアソシエートしない場合、short プリアンブルを使用する必要があります。

5 GHz 無線では無線プリアンブルに short と long を設定できません。

特権 EXEC モードから、次の手順に従って短い無線プリアンブルを無効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio { 0*slot*/*port* }**	2.4 GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。
ステップ 3	**no preamble-short**	短いプリアンブルを無効にし、長いプリアンブルを有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトでは short プリアンブルがイネーブルに設定されています。short プリアンブルがディセーブルになっている場合、イネーブルにするには **preamble-short** コマンドを使用します。

送受信アンテナの設定

ワイヤレス デバイスがデータの送受信に使用するアンテナを選択できます。受信アンテナと送信アンテナでそれぞれ 3 つのオプションがあります。

- Gain：結果のアンテナ ゲインを dB 単位で設定します。
- Diversity：デフォルト設定。最適な信号を受信するアンテナがワイヤレス デバイスで使用されます。ワイヤレス デバイスに 2 つの固定（取り外し不能）アンテナが使用されている場合は、受信と送信の両方にこの設定を使用します。デバイスに 3 つの取り外し可能アンテナが使用されている場合、この設定を使用して、それらすべてのアンテナを Diversity モードで動作させることが可能です。
- Right：ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの右側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、右にあるのが右側のアンテナになります。
- Middle：無線デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナが無線デバイスの中央コネクタに取り付けられている場合は、この設定を受信だけに使用する必要があります。3 アンテナ構成での送信に使用できるアンテナは、右と左のアンテナです。
- Left：ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの左側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、左にあるのが左側のアンテナになります。
  これは、1600、2600、および 3600 シリーズなどのデュアル アンテナ AP には適用されません。詳細情報については、それぞれのハードウェア ガイドを参照してください。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスがデータの送受信に使用するアンテナを選択します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 802.11n 2.4 GHz 無線は Radio 0 です。 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**antenna again** *dB*	デバイスに接続されたアンテナの結果のゲインを指定します。–128 ～ 128 dB の値を入力します。 **（注）** この設定は無線デバイスの動作に影響せず、ネットワークの管理プラットフォームにデバイスのアンテナ ゲインを通知するだけです。
ステップ 4	**antenna receive** {**diversity** | **left** | **middle** | **right**} **2600 および 3600 シリーズでは、このコマンドは次のとおりです。** **antenna receive** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}	受信アンテナを diversity、left、middle、right、または all に設定します。 **（注）** 2 つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの **diversity** を使用します。1 つのアンテナの場合、アンテナを右側に取り付け、アンテナを **right** に設定します。 2600 および 3600 シリーズの AP では次のようになります。 • a-antenna—to use antenna A • ab-antenna—to use antennas A and B • abc-antenna—to use antennas A, B, and C • abcd-antenna—to use antennas A, B, C, and D
ステップ 5	**antenna transmit** {**diversity** | **left** | **right**} **2600 および 3600 シリーズでは、このコマンドは次のとおりです。** **antenna transmit** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}	送信アンテナを Diversity、Left、Right のいずれかに設定します。 **（注）** 2 つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの **diversity** を使用します。1 つのアンテナの場合、アンテナを右側に取り付け、アンテナを **right** に設定します。 2600 および 3600 シリーズの AP では次のようになります。 • a-antenna—to use antenna A • ab-antenna—to use antennas A and B • abc-antenna—to use antennas A, B, and C • abcd-antenna—to use antennas A, B, C, and D

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Gratuitous Probe Response の有効化と無効化

Gratuitous Probe Response（GPR）は、携帯および WLAN の動作モードをサポートするデュアル モード電話で、バッテリ残量を節約します。GPR は 5 GHz 無線で使用可能で、デフォルトで無効に設定されています。GPR の設定には、次の 2 種類の設定があります。

- Period：（ビーコン間隔と同じように）GPR 伝送間の時間を 10 ～ 255 の Kusec（またはミリ秒）間隔で決定します。
- Speed：GPR の伝送に使用するデータ レートの速度です。

長い期間を選択すると、GPR によって消費される RF 帯域幅の量が減少し、バッテリ寿命が短くなる可能性があります。高い伝送速度を選択すると、消費される帯域幅の量が減少し、代わりにセル サイズが小さくなります。

特権 EXEC モードから、次の手順に従って GPR を有効にし、パラメータを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {1}***slot*/*port*	5 GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。
ステップ 3	**probe-response gratuitous** {**period** | **speed**}	デフォルトの period（10 Kusec）および speed（6.0 Mbps）を使用して Gratuitous Probe Response 機能を有効にします。
ステップ 4	**period** *Kusec*	（任意）10 ～ 255 の範囲の値を入力します。デフォルト値は 10 です。
ステップ 5	**speed** {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] }	（任意）応答速度を Mbps 単位で設定します。デフォルト値は 6.0 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

オプション パラメータのデフォルトを使用したくない場合、次の例に示すようにオプション パラメータを個別に設定したり、または結合して設定したりできます。

```
(config-if)# probe-response gratuitous speed 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

GPR 機能を無効にするには、コマンドの **no** 形式を使用します。

Aironet 拡張機能のディセーブル化およびイネーブル化

デフォルトでは、ワイヤレス デバイスは Cisco Aironet 802.11 拡張機能を使用して Cisco Aironet クライアント デバイスの機能を検出し、ワイヤレス デバイスとアソシエートしたクライアント デバイスとの間での特定の相互作用に必要な機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- ロード バランシング：ワイヤレス デバイスは Aironet 拡張機能を使用して、ネットワークとの最適な接続性を確保できるアクセス ポイントにクライアント デバイスを自動的に誘導します。これは、ユーザ数、ビット エラー レート、信号強度などの要因に基づいて行われます。
- メッセージ完全性チェック（MIC）：暗号化されたパケットへの攻撃（ビットフリップ攻撃）を阻止するために新しく追加された WEP セキュリティ機能。MIC は、ワイヤレス デバイスと、それにアソシエートされたすべてのクライアント デバイスに実装され、数バイトを各パケットに付加することによって、パケットの改ざんを防ぎます。
- Cisco Key Integrity Protocol（CKIP）：IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。標準規格に基づくアルゴリズムである Temporal Key Integrity Protocol（TKIP）では、Aironet 拡張機能を有効にする必要はありません。
- リピータ モード：Aironet 拡張機能はリピータ アクセス ポイントと、それらがアソシエートするルート アクセス ポイントで有効に設定されていなければなりません。
- ワールド モード（レガシーのみ）：レガシー ワールド モードがイネーブルになっているクライアント デバイスは、ワイヤレス デバイスからキャリア セット情報を受信して、それぞれの設定を自動的に調整します。802.11d ワールド モードを使用する場合、Aironet 拡張機能は不要です。
- アソシエートされたクライアント デバイスの電力レベルの制限：クライアント デバイスがワイヤレス デバイスにアソシエートするとき、そのワイヤレス デバイスは最大許可電力レベル設定をクライアントに送信します。

Aironet 拡張機能をディセーブルにすると、上記の機能はディセーブルになりますが、シスコ以外のクライアント デバイスがワイヤレス デバイスにアソシエートしやすくなる場合があります。

Aironet 拡張機能はデフォルトではイネーブルに設定されています。特権 EXEC モードから、次の手順に従って Aironet 拡張機能を無効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port* }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 802.11n 2.4 GHz 無線は Radio 0 です。 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**no dot11 extension aironet**	Aironet 拡張機能を無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Aironet 拡張機能がディセーブルになっている場合、イネーブルにするには **dot11 extension aironet** コマンドを使用します。

イーサネット カプセル化変換方式の設定

フレームには、使用する上位レイヤ プロトコルを指定するフィールドがあります（IP、IPX、ARP など）。このフィールドは、レシーバ ネットワーク スタックでフレームに適切に指示するために、レシーバ レベルで必要です。

プロトコル表示には、主に 2 つの手法があります。

- EtherType：フレームで実行されるプロトコルを示す 16 ビットの値。EtherType はイーサネット 2.0/DIX ネットワークで使用されます。
- LLC/SNAP：802.2 リンク レイヤ プロトコル表示を可能にする 6 バイト ヘッダー。LLC/SNAP は 802.3 および 802.11 ネットワークで使用されます。

アクセス ポイントが EtherType の情報を使用する有線ネットワーク フレームから受信した場合、この EtherType の情報を SNAP/LLC の情報に変換するメカニズムが必要です。2 つの変換方法があります。

- 802.1H：Cisco Aironet 無線製品に対して良好なパフォーマンスを提供します。
- RFC1042：Cisco Aironet 以外の無線機器との良好な相互運用性を確保するには、この設定を使用します。RFC 1042 は、他の無線機器の製造業者によって使用されており、デフォルト設定となっています。これがデフォルト設定です。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 802.11n 2.4 GHz 無線は Radio 0 です。 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**payload-encapsulation** **rfc1042** | **dot1h**	カプセル化変換方式を RFC 1042（**rfc1042**、デフォルト設定）または 802.1h（**dot1h**）に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワークグループ ブリッジへの信頼性のあるマルチキャストの有効化と無効化

Reliable multicast messages from the access point to workgroup bridges 設定は、マルチキャスト メッセージの信頼できる送信を、AP にアソシエートしている最大 20 の Cisco Aironet ワークグループ ブリッジに制限します。デフォルト設定の **disabled** では、マルチキャスト送信の信頼性は低下しますが、ワイヤレス デバイスにアソシエートされるワークグループ ブリッジを増やせます。

通常、アクセス ポイントやブリッジでは、ワークグループ ブリッジはクライアント デバイスとしてではなく、アクセス ポイントやブリッジと同じインフラストラクチャ デバイスとして扱われます。ワークグループ ブリッジがインフラストラクチャ デバイスとして扱われる場合、ワイヤレス デバイスは、アドレス解決プロトコル（ARP）パケットなどのマルチキャスト パケットや一部のブロードキャスト パケットを、確実にワークグループ ブリッジに送信します。

AP は、マルチキャスト アドレスにマルチキャスト フレームを送信し、その後、ワークグループ ブリッジから認識される、ユニキャスト フレームにカプセル化されたマルチキャスト フレームをワークグループ ブリッジに再度送信します。この検証メカニズムにより、無線オーバーヘッドが発生し、アクセス ポイントのスループットが低下します。

信頼性の高いマルチキャスト配信のパフォーマンス コストのため（マルチキャスト パケットが各ワークグループ ブリッジに二重に送信されるので）、ワークグループ ブリッジなどワイヤレス デバイスにアソシエートできるインフラストラクチャ デバイスの数は制限されます。ワイヤレス デバイスへの無線リンクを維持できるワークグループ ブリッジの数を 21 以上にするには、ワイヤレス デバイスがマルチキャスト パケットをワークグループ ブリッジに配信するときの信頼性を低くする必要があります。信頼性が低くなると、ワイヤレス デバイスはマルチキャスト パケットが目的のワークグループ ブリッジに到達したかどうかを確認できなくなるため、ワイヤレス デバイスのカバレッジ領域の端にあるワークグループ ブリッジでは IP 接続が失われる可能性があります。ワークグループ ブリッジをクライアント デバイスとして扱うと、パフォーマンスは向上しますが、信頼性は低くなります。

（注） この機能は、固定型のワークグループ ブリッジでの使用に最適です。モバイル型のワークグループ ブリッジの場合、ワイヤレス デバイスのカバレッジ領域内でマルチキャスト パケットを受信できないスポットに入る可能性があり、この場合、ワイヤレス デバイスにアソシエートされていても接続が失われてしまいます。

Cisco Aironet ワークグループ ブリッジでは、最大 8 つのイーサネット対応デバイスとの無線 LAN 接続を提供します。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

（注） 信頼できるマルチキャスト転送を設定するには、この設定はワークグループ ブリッジではなく、AP で行う必要があります。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 | 1}**	2.4 GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。

	コマンド	目的
ステップ 3	**infrastructure-client**	ワークグループ ブリッジへの信頼性のあるマルチキャスト メッセージを有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

ワークグループ ブリッジへの信頼性のあるマルチキャスト メッセージを無効にするには、コマンドの **no** 形式を使用します。

ワークグループ ブリッジは、マルチキャスト フレームそして同じフレームのユニキャスト フレームを受け取るようになり、レシーバ レベルでフレームの重複が生じて非効率となります。

ワークグループ ブリッジの無線レベルでマルチキャスト フレームまたはユニキャスト コピーだけを考慮するようにワークグループ ブリッジを設定するには、次のコマンドを使用します。

コマンド	目的
station-role workgroup-bridge multicast mode {**client** | **infrastructure**}	次のいずれかを設定できます: • クライアント クライアント モードは、3 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます • インフラストラクチャ インフラストラクチャ モードは、4 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます AP に信頼できるマルチキャストを設定した場合、ワークグループ ブリッジ レベルでインフラストラクチャを使用することが推奨されます。AP に信頼できるマルチキャストを設定しない場合、ワークグループ ブリッジ レベルでクライアントを使用します。

たとえば、次のコマンドはワークグループ ブリッジ レベルでインフラストラクチャを使用します。

```
WGB(config-if)# station-role workgroup-bridge multicast mode infrastructure
```

Public Secure Packet Forwarding のイネーブル化とディセーブル化

Public Secure Packet Forwarding(PSPF)を使用すると、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 デバイスと、同じアクセス ポイントにアソシエートする他のクライアント デバイスとの偶発的なファイル共有や通信を防ぐことができます。PSPF は、クライアント デバイスに LAN におけるインターネット アクセスだけを許可し、その他の権限は与えません。この機能は、空港や大学の構内などに敷設されている公衆ワイヤレス ネットワークに有用です。

(注) 異なるアクセス ポイントにアソシエートするクライアント間での通信を防ぐために、ワイヤレス デバイスを接続するスイッチに保護ポートを設定する必要があります。保護ポートの設定方法については、「保護ポートの設定」(P.6-32)を参照してください。

ワイヤレス デバイス上で CLI コマンドを使用して PSPF をイネーブルまたはディセーブルにするには、ブリッジ グループを使用します。次の文書に、ブリッジ グループに関する詳細な説明と、ブリッジ グループを実装する手順が収められています。

- 『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』。このリンクをクリックすると、「Configuring Transparent Bridging」の章が表示されます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm

PSPF は Web ブラウザ インターフェイスを使用して有効および無効にできます。PSPF 設定は [Radio Settings] ページで行います。

PSPF はデフォルトでディセーブルに設定されています。特権 EXEC モードから、次の手順に従って PSPF を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。 802.11n 2.4 GHz 無線は Radio 0 です。 802.11n 5 GHz 無線は Radio 1 です。
ステップ 3	**bridge-group** *group* **port-protected**	PSPF を有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

PSPF を無効にするには、コマンドの **no** 形式を使用します。

保護ポートの設定

無線 LAN の異なるアクセス ポイントにアソシエートするクライアント デバイス間での通信を防ぐために、無線デバイスを接続するスイッチに保護ポートを設定することができます。また、通信が発生しないようにする AP 同士をつなぐ同じスイッチのポートを分離する必要があります。

特権 EXEC モードから、次の手順に従ってスイッチ上のポートをプロテクテッド ポートとして定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、設定するスイッチポート インターフェイスのタイプと番号を **gigabitethernet0/1** のように入力します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show interfaces** *interface-id* **switchport**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、**no switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。このコマンドは、個別のスイッチ レベルでのみ有効です。これは異なるスイッチに接続された AP は分離しません。このコマンドは、通信が発生しないようにする任意のスイッチのすべての AP のポートで使用できます。また、AP にプライベート VLAN 設定を使用できます。

（注）　無線ドメイン サービス(WDS)を使用する場合、AP と そのWDS と間の通信を遮らないようにします。

プライベート VLAN の設定、保護ポート、およびポート ブロッキングの詳細については、次の URL にある『*Catalyst 3750 Software Configuration Guide*』を参照してください:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750.html

ビーコン間隔と DTIM の設定

ビーコン間隔はアクセス ポイントのビーコン間の時間(キロマイクロ秒)です。1 Kμsec は 1,024 マイクロ秒に相当します。常にビーコン間隔の倍数となるデータ ビーコン レートにより、ビーコンに Delivery Traffic Indication Message(DTIM)が格納される頻度が決定されます。DTIM は、省電力モードのクライアント デバイスに、パケットがクライアント待ちであることを通知します。

たとえば、ビーコン間隔がデフォルト設定の 100 に設定され、DTIM がデフォルト設定の 2 に設定されている場合、AP は DTIM を含むビーコンを 2 ビーコンごと、または 200 Kμsec ごと、または 200 ミリ秒ごとに送信します。1 Kμsec は 1,024 マイクロ秒に相当します。

デフォルトのビーコン間隔は 100、デフォルトの DTIM は 2 です。特権 EXEC モードから、次の手順に従ってビーコン間隔および DTIM を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11n 2.4 GHz 無線は 0 です。 5 GHz 無線および 802.11n 5 GHz 無線は 1 です。
ステップ 3	**beacon period** *value*	ビーコン間隔を 20 ～ 4000 の範囲で設定します。値をキロマイクロ秒で入力します。
ステップ 4	**beacon dtim-period** *value*	DTIM を 1 ～ 100 の範囲で設定します。値をキロマイクロ秒で入力します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

RTS しきい値と再試行回数の設定

Request To Send(RTS; 送信要求)しきい値は、パケットの送信前にワイヤレス デバイスが RTS を発行するときのパケット サイズを決定します。多数のクライアント デバイスがワイヤレス デバイスにアソシエートされているエリアや、クライアントが遠く分散しているために、ワイヤレス デバイスは検知できても、クライアント同士が互いに検知できないエリアでは、RTS しきい値を低く設定すると効果的です。設定値を 0 ～ 23472347 バイトの範囲で入力します。

最大 RTS リトライは、ワイヤレス デバイスが無線を介したパケット送信の試行を中止するまでに RTS を発行する最大回数です。1 ～ 128 の範囲の値を入力します。

すべてのアクセス ポイントおよびブリッジに対するデフォルトの RTS しきい値は 2347、デフォルトの最大 RTS リトライ設定は 3264 です。特権 EXEC モードから、次の手順に従って RTS しきい値と最大 RTS リトライを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**rts threshold** *value*	RTS しきい値を設定します。RTS しきい値は 0 ～ 23472347 の範囲で入力します。
ステップ 4	**rts retries** *value*	最大 RTS リトライ回数を設定します。1 ～ 128 の範囲の値を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

RTS 設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

最大データ パケット再試行回数の設定

最大データ リトライ設定は、ワイヤレス デバイスがパケット送信を放棄し、そのパケットをドロップするまでに行うパケット送信の最大再送回数です。

デフォルト設定は 32 です。特権 EXEC モードから、次の手順に従って最大データ リトライを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**packet retries** *value* [**drop-packet**]	最大データ リトライ回数を設定します。1 ～ 128 の範囲の値を入力します。 drop-packet オプションを使用する場合、デバイスは現在のパケットの送信を停止し、接続を解除せずに、キューにある次のパケットの送信を試みます。 drop-packet オプションを使用しない場合、ワイヤレス デバイスはリンクが使用可能でないと判断して、現在のパケットの送信を停止し、接続を終了します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

フラグメンテーションしきい値の設定

フラグメンテーションしきい値は、断片化されて複数のブロックとして送信されるパケットの最小サイズを決定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。

デフォルト設定は 23382346 バイトです。特権 EXEC モードから、次の手順に従ってフラグメンテーションしきい値を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1***slot*/*port*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 3	**fragment-threshold** *value*	フラグメンテーションしきい値を設定します。2.4 GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。5 GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

802.11g 無線の short スロット時間のイネーブル化

802.11g、2.4 GHz 無線のスループットは、短いスロット時間を有効にすることで向上します。スロット時間を標準の 20 マイクロ秒から 9 マイクロ秒の short スロット時間まで短縮すると、全体のバックオフが減少し、スループットが向上します。バックオフは、スロット時間の倍数であり、LAN 上にパケットを送信するまでにステーションが待機するランダムな長さの時間です。

多くの 802.11g 無線は short スロット時間をサポートしていますが、サポートしていないものもあります。短いスロット時間を有効にした場合、ワイヤレス デバイスは、802.11g、2.4 GHz 無線にアソシエートされたすべてのクライアントが短いスロット時間をサポートしている場合だけこれを使用します。

短いスロット時間は、802.11g、2.4 GHz 無線だけでサポートされています。短いスロット時間は、802.11b クライアントではサポートされていません。短いスロット時間を有効にすると、802.11b クライアントは、AP 無線への参加または AP 無線との通信を行えなくなります。short スロット時間は、デフォルトではディセーブルに設定されています。

無線インターフェイス モードで、次のコマンドを入力して短いスロット時間を有効にします。

```
ap(config-if)# short-slot-time
```

no short-slot-time を入力し、Short スロット時間をディセーブルにします。

キャリア話中検査の実行

キャリア ビジー テストを実行して、ワイヤレス チャネルでの無線活動をチェックします。キャリア ビジー テストでは、キャリア検査を実行して検査結果を表示するまでの約 4 秒間、ワイヤレス デバイスはワイヤレス ネットワーキング デバイスとのアソシエーションをすべて停止します。

特権 EXEC モードで、次のコマンドを入力して、キャリア ビジー テストを実行します。

dot11 *interface-number* **carrier busy**

interface-number については、**dot11radio 0** を入力して、2.4 GHz 無線上の検査を実行するか、**dot11radio 1** を入力して、5 GHz 無線上の検査を実行します。

(注) インターフェイスは、キャリア ビジー テストを実行するためにイネーブルにする必要があります。

show dot11 carrier busy コマンドを入力して、キャリア話中検査結果を再表示します。

```
ap#dot11 dot11Radio 1 carrier busy
ap#show dot11 carrier busy
Frequency  Carrier Busy %
---------  --------------
   5180           2
   5200           0
   5220           2
   5240           1
   5260           1
   5280           0
   5300           1
   5320           0
   5500           0
   5520           0
   5540           0
   5560           0
   5580           0
   5660           0
   5680           0
   5700           0
   5745           0
   5765           0
   5785           0
   5805           0
   5825           0
```

VoIP パケット処理の設定

アクセス ポイントの無線ごとの VoIP パケット処理の質は、ワイヤレス サービス クラス 5（ビデオ）およびワイヤレス サービス クラス 6（音声）の低遅延における 802.11 MAC 動作を強化することで改善できます。

アクセス ポイントの VoIP パケット処理を設定する手順は、次のとおりです。

ステップ 1　ブラウザを使用して、アクセス ポイントにログインします。

ステップ 2　Web ブラウザ インターフェイスの上部にあるタスク メニューで [Services] をクリックします。

ステップ 3　左側のメニューで、[Stream] をクリックします。

[Stream] ページが表示されます。

ステップ 4　設定する無線のタブをクリックします。

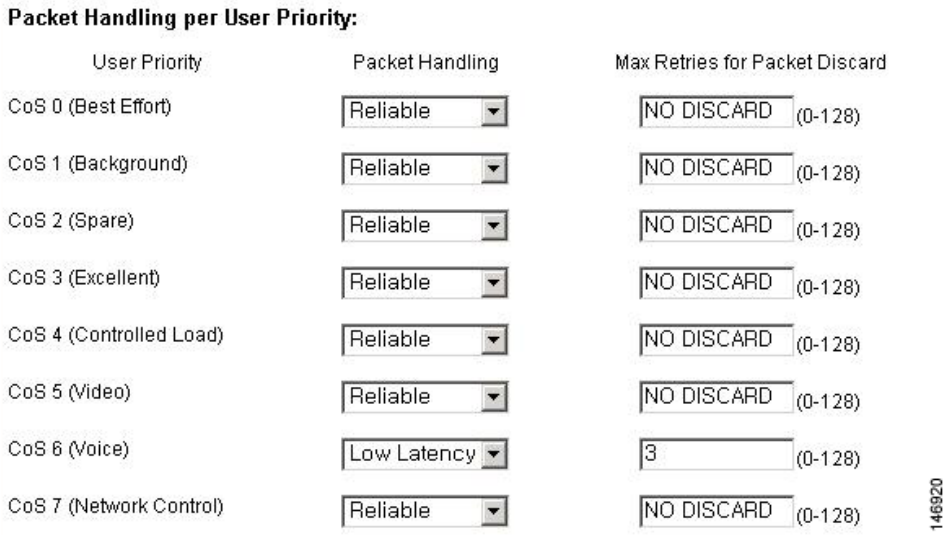
ステップ 5　CoS 5（ビデオ）および CoS 6（音声）の両方のユーザの優先順位について、[Packet Handling] ドロップダウン リストから [Low Latency] を選択し、パケット廃棄の最大リトライ回数の値を、対応するフィールドに入力します。他のキューのパケットはキューが解除され、遅延に影響されやすいデータは他のトラフィックよりも優先して処理されます。

最大再試行回数のデフォルト値は、Low Latency 設定では 3 です（図 6-2）。この値は、損失したパケットを廃棄する前に、アクセス ポイントがパケットを再送信しようとする回数を示します。

（注）　CoS 4（負荷制御）ユーザの優先順位およびその最大再試行回数も設定できます。

ステップ 6　[Apply] をクリックします。

図 6-2　　パケット処理の設定



CLI を使用して VoIP パケット処理を設定することも可能です。CLI を使用して VoIP パケット処理を設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

再試行のレベルを定義すると、それらのフレームを送信する速度も設定できるようになります。これは、ページ下部にある **[Low Latency Packet Rates]** セクションで行えます。各レートを次に設定できます。

- Nominal：AP は、低遅延パケットを送信するときに、このレートを使用します（クライアントの信号レベルに応じて、最初に高速レートを使用）。
- Non-nominal：AP はそのレートを使用しないようにしますが、公称レートが使用できない場合にはこれを使用します。
- Disabled：AP は、そのレートを使用することはありません。

CLI から、次の無線インターフェイス コンフィギュレーション コマンドを使用します（CLI コマンドは GUI ページよりも多くのオプションを提供します）：

packet max-retries *number 1 number 2* **fail-threshold** *number 3 number 4* **priority** *value* **drop-packet**

このコマンドの各項目の意味は以下のとおりです。

- Number 1：特定のプライオリティ レベルで、正しく受信されなかった（確認応答がなかった）パケットの再送信を AP が試みる回数を定義します。number 1 に達すると、AP はパケットをドロップし、（同じ受信者に）次のパケットの送信を試みます。
- Number 3：許容可能なしきい値をフェイル レートが超えたと AP が判断する前に、何回連続して（1 人の受信者に送信された）パケットが失敗できるかを指定します
- Number 2：失敗しきい値を超えた場合でも、AP は失敗したパケットを再送信するできますが、しきい値を超過する前とは試行回数が異なります。これは、number 2 です。たとえば、最初は各パケットを 3 回（number 1）再送信するよう設定できます。その後、AP が一定の数の連続するパケット（たとえば、number 3 として指定する 100）の送信に失敗した場合、条件が劣化しているため、AP が後続の各パケットの再送信を 1 回（number 2）だけ試みるように指定できます。

- Number 4: ターゲット クライアントのアソシエートを解除する前に、number 2 の再送信で、AP がさらにどれだけの連続するパケットの再送信を試みるかを指定します。

例:

```
ap(config-if)# packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

この例では、AP はプライオリティ レベル 6 の各パケットの再送信を 3 回試行します（number one = 3）。連続するパケット 100 個が同じ宛先に対して失敗した場合（number three = 100）、AP はその宛先に対して連続するパケットを 1 度だけ送信します（number two = 0）。同じ宛先に対してさらに 500 のパケットが失敗すると（number four = 500）、AP はそのクライアントを切断します。

GUI を使用する場合、number one は手動で定義します（デフォルト値は 3）。number 2 のデフォルト値は 0、number 3 のデフォルト値は 100、number 4 のデフォルト値は 500 です。これらの数値は CLI から変更できます。

```
ap(config-if)#packet max-retries ?
<0-128>  # packet retries before dropping pkt if first fail-threshold not
           reached


ap(config-if)#packet max-retries 3 ?
<0-128>  # packet retries before dropping pkt if 2nd fail-threshold not
           reached

ap(config-if)#packet max-retries 3 0 ?
fail-threshold  maximum # consecutive dropped packets thresholds

ap(config-if)#packet max-retries 3 0 fa
ap(config-if)#packet max-retries 3 0 fail-threshold ?
<0-1000>  # consecutive dropped packets before switching max-retries
            thresholds

ap(config-if)#packet max-retries 3 0 fail-threshold 100 ?
<0-1000>  number of consecutive dropped packets before disassociating client

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 ?
priority  qos user-priority

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 p
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority ?
<0-7>  qos user-priority number

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 ?
drop-packet  Don't retry pkts, just drop packets when max retries reached

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 d
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

低遅延パケット レートも、公称レートと許可されるレートを定義する次のコマンドを使って、インターフェイス レベルで定義できます。

traffic-stream priority *value* **sta-rates {[***nominal rates***] | [***rates***]}**

```
ap(config-if)# traffic-stream priority 6 sta-rates ?
12.0      Allow 12.0 Mb/s rate
  18.0      Allow 18.0 Mb/s rate
  24.0      Allow 24.0 Mb/s rate
  36.0      Allow 36.0 Mb/s rate
  48.0      Allow 48.0 Mb/s rate
  54.0      Allow 54.0 Mb/s rate
```

```
  6.0       Allow 6.0 Mb/s rate
  9.0       Allow 9.0 Mb/s rate
  nom-12.0  Allow Nominal 12.0 Mb/s rate
  nom-18.0  Allow Nominal 18.0 Mb/s rate
  nom-24.0  Allow Nominal 24.0 Mb/s rate
  nom-36.0  Allow Nominal 36.0 Mb/s rate
  nom-48.0  Allow Nominal 48.0 Mb/s rate
  nom-54.0  Allow Nominal 54.0 Mb/s rate
  nom-6.0   Allow Nominal 6.0 Mb/s rate
  nom-9.0   Allow Nominal 9.0 Mb/s rate
 <cr>
```

例：

```
ap(config-if)# traffic-stream priority 6 sta-rates nom-5.5 nom-11.0 nom-6.0 9.0 nom-12.0
nom-24.0
```

音声キューの場合（具体的には UP 6）、音声キューでパケットを送信するために使用できるレートを決定するために interface コマンドの packet speed を使用できます。

packet speed 5.5 11.0 6.0 9.0 12.0 24.0 priority 6

packet speed コマンドは許可されるレートの定義を主に行うのに対し、traffic-stream priority コマンドは許可されたレートの中で優先されるレートも定義します。音声キューで両方のコマンドを使用する場合、traffic stream priority コマンドで公称として定義されたレートが最初に試され、その後に非公称レートやパケット速度レートが試されます。

ClientLink の設定

Cisco ClientLink（Beam Forming とも呼ばれます）はインテリジェントなビームフォーミング テクノロジーです。RF 信号を 802.11a/g デバイスに送信して、パフォーマンスを 65 % 向上させ、カバレッジを最大 27 % 拡大し、カバレッジ ホールを減少させます。

Cisco ClientLink は、既存の混合クライアント ネットワークの 802.11a/g デバイスと単一トラフィック ストリームのみをサポートする 802.11n クライアントの耐用年数を延長するのに役立ちます。Cisco ClientLink は、802.11n に移行し、種類に関係なく、ネットワーク上のすべてのクライアントで必要な帯域幅およびスループットを確保することを求める組織にとって有益です。

（注） CLientLink バージョン 1 は 802.11 a/g デバイスをサポートし、ClientLink バージョン 2 は単一空間ストリームがある 802.11 a/g デバイスと 802.11n デバイスをサポートします。

（注） 1040、702 シリーズ アクセス ポイントでは、ClientLink はサポートされていません。

CLI を使用した ClientLink の設定

ClientLink を有効にするには、インターフェイス コンフィギュレーション モードの 802.11n 無線インターフェイスで、次の CLI コマンドを入力します。

```
beamform ofdm
```

（注）　現在、ClientLink 設定オプションは、GUI では使用できません。

ClientLink を開始するしきい値を決定するには、次のコマンドを使用します。

ap(config-if)# **beamform rssi** *30to128-rssi-threshold-in-dBm*

ClientLink はデフォルトでは無効に設定されています。詳細は、cisco.com の次の URL を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389.html

無線機能のデバッグ

無線機能のデバッグを開始するには、**debug dot11** 特権 EXEC コマンドを使用します。デバッグ操作を停止するには、このコマンドの **no** 形式を使用します。コマンド構文は次のとおりです。

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map | syslog | virtual-interface}
```

構文は、表 6-4 に示すとおりです。

表 6-4　debug dot11 コマンドの構文

構文	説明
events	無線に関連するすべてのイベントのデバッグをアクティブにします。
packets	送受信された無線パケットのデバッグをアクティブにします。
forwarding	転送された無線パケットのデバッグをアクティブにします。
mgmt	無線アクセス ポイントの管理アクティビティのデバッグをアクティブにします。
network-map	無線アソシエーション管理のネットワーク マップのデバッグをアクティブにします。
syslog	無線システム ログのデバッグをアクティブにします。
virtual interface	無線仮想インターフェイスのデバッグをアクティブにします。

この例では、無線に関連するすべてのイベントのデバッグを開始する方法を示します。

```
AP# debug dot11 events
```

この例では、無線パケットのデバッグを開始する方法を示します。

```
AP# debug dot11 packets
```

この例では、無線システム ログのデバッグを開始する方法を示します。

```
AP# debug dot11 syslog
```

この例では、無線に関連するすべてのイベントのデバッグを停止する方法を示します。

```
AP# no debug dot11 events
```

（注）　デバッグが有効になっていない状態が、コマンドのデフォルトです。

802.11r の設定

802.11r は無線ドメイン サービスを使用して同じサブネット上のアクセス ポイント間で高速ローミングをイネーブルにします。802.11r をイネーブルにすると、モビリティ ドメイン情報要素（MDIE）が AP はビーコンでアドバタイズされます。同じ WDS にアソシエートされたすべての AP で同じ MDIE がアナウンスされます。WDS BVI IP アドレス（IPv4 または IPv6）の最後の 2 バイトは MDIE として使用されます。802.11r 互換性のあるクライアントは、この MDIE を使用して、同じドメインに属していて、高速ローミングが可能な AP を識別します。

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air: クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。これを設定するには、次のコマンドを使用します。
  ap(config-if)**#dot11 dot11r pre-authentication over-air**
- Over-the-DS: クライアントは、現在の AP 経由でターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行され、その後 WDS 経由でターゲット AP に送信されます。これを設定するには、次のコマンドを使用します。
  ap(config-if)**#dot11 dot11r pre-authentication over-ds**

AP 無線では、802.11r サポートをイネーブルにしてローミング ダイアログを無線（デフォルト）で行うか DS 上で行うかを決定し、クライアントがローミング トランザクションを完了するまでに許可される最大時間を設定できます。クライアントがローミング トランザクションを完了するまでに許可される最大時間は、リアソシエーション タイマーと呼ばれます。このタイマーは、攻撃者が多数の 802.11r トランザクションを開き、いずれも完了しないという状態（これにより AP が過負荷状態になる）を防ぐことにより、ネットワークのセキュリティを強化できます。このタイマーは次のコマンドで設定できます。

ap(config-if)**#dot11 dot11r reassociation-time value** *20to1200-timeout-value-in-milli-seconds*

例：DS 上の認証で 802.11r をイネーブルにして、リアソシエーションの時間値を 200 ミリ秒にします。

```
aap(config-if)#dot11 dot11r pre-authentication over-ds
ap(config-if)#dot11 dot11r reassociation-time value 200
```

（注）　ネットワークに導入する前に 802.11r をテストします。一部の非 802.11r クライアントは 802.11r MDIE をサポートせず、802.11r 環境で正しく機能しません。

SSID および無線インターフェイスのトラフィック レート制限の設定

無線クライアント デバイスによる使用帯域幅を制限するには、無線クライアント デバイス間のトラフィック レートを制限できます。このレート制限機能には、次のような特徴があります。

- 各 SSID で設定でき、片方または両方の無線インターフェイスに適用できる
- IPv4 の TCP/UDP にのみ適用される IPv6 トラフィックに対してはサポートされない
- 無線インターフェイスの入力トラフィックおよび出力トラフィックの両方に適用される

レート制限機能は VLAN で利用可能です。同じインターフェイス上で複数の SSID が設定されている場合、VLAN なしではレート制限は設定できません。

複数の SSID の設定については、第 7 章「複数の SSID の設定」を参照してください。

VLAN の詳細については、第 14 章「VLAN の設定」を参照してください。

Quality of Service（QoS）機能の一部として、ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限するレート制限機能があります。詳細については、第 15 章「QoS の設定」を参照してください。

レート制限の設定

レート制限を設定するには、次のコマンドを使用します:
rate-limit {tcp | udp} {input | output} data-rate *rate* **burst-size** *size*。ここで、

- date-rate はデータ転送の平均レートで、キロビット/秒で指定されます。
- burst-size はトラフィックがスロットリングされる前に転送できる合計データです。これはキロビットで指定されます。

これらのパラメータは 8 の倍数の最近値に変換および制限されます。data-rate はキロバイト/秒、burst-size はバイトに変換され、レート制限で考慮されます。

これらのパラメータの機能を理解するために、次の例を考えます。平均データ速度を 10 バイト/秒、バースト サイズを 20 バイトとします。ここで適用されるレート制限は、2 秒間（バースト サイズ/平均レートとして計算）となり、合計データ伝送は 20 バイトを超えることはできません。これにより、平均データ速度が 10 バイト/秒を超えない限り、1 秒あたりにより多くのデータを送信することができます。

GUI 経由で設定するには、[Security] > [SSID Manager] にアクセスします。[Rate Limit Parameters] セクションで、必要に応じて TCP または UDP の入力トラフィックまたは出力トラフィックを制限できます。また、それぞれのレートおよびバースト サイズも指定できます。

レート制限統計情報の表示

レート制限の統計情報を表示するには、任意のインターフェイスに設定された各 SSID について、次のコマンドを使用します:**show interface dot11radio {0 | 1} qos-info**

統計情報カウンタをクリアするには、次のコマンドを使用します:**clear counters dot11Radio {0 | 1}**

GUI 経由でレート制限統計情報を表示するには、[Network] > [Network Interface] > [Radio0-802.11N 2.4 GHz] または [Radio1-802.11N 5 GHz] にアクセスします。統計情報をクリアするには、[Clear] をクリックします。

複数の SSID の設定

この章では、アクセス ポイントで複数のService Set Identifier（SSID）を設定および管理する方法について説明します。

複数の SSID の概要

SSID は、無線ネットワーキング デバイスが無線接続を確立および維持するために使用する、ASCII 文字列です。ネットワークまたはサブネットワーク上の複数のアクセス ポイントは、同じ SSID を使用できます。SSID では大文字と小文字が区別され、最大 32 文字の英数字を使用できます。

アクセス ポイントには、最大 16 の SSID を設定でき、各 SSID に異なる設定を割り当てることができます。すべての SSID は同時にアクティブにできます。つまり、クライアント デバイスは、どの SSID を使用してもアクセス ポイントにアソシエートできます。各 SSID には、次の設定を割り当てることができます。

- VLAN
- クライアント認証の設定

（注） クライアント認証タイプの詳細は、第 11 章「認証タイプの設定」を参照してください。

- クライアントの認証済みキー管理の設定
- AP 認証パラメータの挿入（ブリッジなどの AP 間リンクを使用する場合）
- 管理フレーム保護設定の挿入（802.11w および/または Cisco MFP）
- SSID を使用するクライアント アソシエーションの最大数
- SSID を使用するトラフィックの RADIUS アカウンティング
- ゲスト モード（SSID 文字列をビーコンでブロードキャストするかどうかを定義）
- 古い AP 間認証メソッドの定義（AP 間リンクで PSK または LEAP セキュリティを使用する場合）
- クライアント デバイスから受信したパケットのリダイレクト

ゲスト SSID を設定することで、アクセス ポイント SSID をすべての無線クライアント（該当する SSID に対するプロファイルを持っていないクライアントを含む）に対して表示できます。アクセス ポイントでは、ビーコンでゲスト SSID を示します。ゲスト モードが無効な場合も、AP はゲスト SSID のビーコンを送信しますが、SSID 文字列は示されません。SSID が事前設定されていないクライアントを除外する場合は、ゲスト SSID 機能を無効にします。クライアントはその特定の SSID 文字列を具体的に照会することによって、引き続き SSID を使用できることに注意してください。ブロードキャスト プローブ メッセージを送信するクライアントは、AP 応答で SSID 文字列を受け取りません。また、AP ビーコンの SSID 文字列も表示されません。ゲスト モード SSID の設定方法とゲスト モード SSID の無効化する方法については、「SSID のグローバルな作成」（P.7-3）を参照してください。

アクセス ポイントをリピータまたは非ルート ブリッジとして機能させるには、リピータ側または非ルート ブリッジ側でクレデンシャルを設定し、ルートまたはプライマリ AP でリピータまたは非ルート ブリッジを認証できるようにします。リピータ モードの SSID に認証ユーザ名とパスワードを割り当てると、クライアント デバイス同様、リピータでネットワークへの認証が可能になります。

ネットワークで複数の VLAN を使用する場合は、各 SSID を 1 つの VLAN に割り当てることができます。この割り当てた SSID を使用するクライアント デバイスは、その VLAN にグループ化されます。

複数の SSID の設定

次の項では、複数の SSID の設定情報を説明します。

（注）　SSID をグローバルに設定してから、特定の無線インターフェイスに適用する必要があります。SSID をグローバルに設定するには、「SSID のグローバルな作成」(P.7-3) の手順に従ってください。

SSID のグローバルな作成

Cisco IOS リリースでは、**dot11 ssid** グローバル コンフィギュレーション コマンドを使用して SSID を作成すると、**ssid** 設定インターフェイス コマンドを使用して、特定のインターフェイスにその SSID を割り当てることができます。

グローバル コンフィギュレーション モードで SSID を作成しておき、**ssid** 設定インターフェイス コマンドを実行すると、目的のインターフェイスにその SSID が割り当てられますが、SSID コンフィギュレーション モードにはなりません。SSID をグローバル コンフィギュレーション モードで作成していない場合は、**ssid** コマンドを実行すると、CLI が新しい SSID についての SSID コンフィギュレーション モードとなります。ただし、無線インターフェイスから SSID コンフィギュレーション モードで設定できるパラメータは、SSID グローバル コンフィギュレーション モードで設定できるパラメータより限られてます。

特権 EXEC モードから、次の手順に従って SSID をグローバルに作成します。SSID を作成した後、SSID を特定の無線インターフェイスに割り当てることができます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。 （注）　タブおよび末尾のスペースは、SSID には無効な文字です。
ステップ 3	**authentication client username** *username* **password** *password*	（任意）リピータ モードまたは非ルート ブリッジ モードで LEAP などのレガシー認証システムを使用する場合、アクセス ポイントがネットワークに対する認証で使用する認証ユーザ名とパスワードを設定します。リピータ アクセス ポイントがルート アクセス ポイントまたは別のリピータあるいは非ルート ブリッジにアソシエートするために使用するユーザ名およびパスワードを、SSID に設定します。
ステップ 4	**accounting** *list-name*	（任意）この SSID の RADIUS アカウンティングを有効にします。*list-name* には、アカウンティング方式のリストを指定します。方式のリストについて詳しくは、このリンク http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html をクリックしてください。

	コマンド	目的
ステップ 5	**vlan** *vlan-id*	(任意)ネットワーク上の VLAN に SSID を割り当てます。この SSID を使用してアソシエートするクライアント デバイスは、この VLAN にグループ化されます。同じ VLAN に複数の SSID を割り当てることができますが、同じ SSID を複数の VLAN に割り当てることはできません。
ステップ 6	**guest-mode**	(任意)SSID をアクセス ポイントのゲスト モード SSID として指定します。ビーコンに SSID が含まれるアクセス ポイントは、プローブ要求で SSID を指定していないクライアント デバイスに可視になります。
ステップ 7	**infrastructure-ssid** [**optional**]	このコマンドは、アクセス ポイントとブリッジが互いにアソシエートする際に使用する SSID を制御します。ルート アクセス ポイントでは、インフラストラクチャ SSID を使用してアソシエートができるのは、リピータ アクセス ポイントだけです。ルート ブリッジでは、インフラストラクチャ SSID を使用してアソシエートができるのは、非ルート ブリッジだけです。リピータ アクセス ポイントと非ルート ブリッジは、この SSID を使用してルート デバイスとアソシエートします。 アクセス ポイントとブリッジの GUI では、リピータの役割および非ルート ブリッジの役割にインフラストラクチャ SSID の設定が必要です。ワークグループ ブリッジの役割にインフラストラクチャ SSID を設定する必要はありません。レガシー IOS コードを使用している場合、無線に複数の SSID が設定されていない限り、CLI を使用してデバイスの役割を設定すれば、インフラストラクチャ SSID を設定する必要はありません。複数の SSID が無線に設定されている場合は、infrastructure-ssid コマンドを使用して、非ルート ブリッジがルート ブリッジとの接続に使用する SSID を指定する必要があります。 しかし、12.4(21a)JA1 および 12.3(8)JEC リリース以降では、1 つまたは複数の SSID の有無に関係なく、インフラストラクチャ SSID が設定されない場合、リピータはブリッジとアソシエートしません。
ステップ 8	**interface dot11radio** { **0** | **1** }	SSID の割り当て先とする無線インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 9	**ssid** *ssid-string*	ステップ 2 で作成したグローバル SSID を無線インターフェイスに割り当てます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

（注）　各 SSID に認証タイプを設定する場合は、**ssid** コマンドの認証オプションを使用します。認証タイプの設定方法については、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

（注）　802.11b と 802.11g が同じ 2.4 GHz 帯で動作するため、802.11g 無線にゲストの SSID モードを有効にすると、802.11b 無線にも適用されます。

SSID または SSID 機能を無効にするには、コマンドの **no** 形式を使用します。

次の例は、次の方法を示します。

- SSID の名前の指定
- RADIUS アカウンティングの SSID の設定
- この SSID を使用してアソシエートするクライアント デバイスの最大数を 15 に設定
- SSID の VLAN への割り当て
- SSID の無線インターフェイスへの割り当て

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

グローバルに設定された SSID の表示

グローバルに設定された SSID の設定詳細を表示するには、次のコマンドを使用します。

```
AP# show running-config ssid ssid-string
```

RADIUS サーバを使用した SSID の制限

クライアント デバイスが、不正な SSID を使用してアクセス ポイントにアソシエートするのを防ぐために、RADIUS 認証サーバでクライアントが使用する必要のある、許可された SSID のリストを作成します。

SSID 許可のプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイントにアソシエートします。
2. クライアントは、RADIUS 認証を開始します。

3. RADIUS サーバは、クライアントが使用を許可された SSID のリストを返します。アクセス ポイントは、このリスト内に、クライアントが使用する SSID と一致する SSID があるかどうかをチェックします。次の 3 とおりの結果が予測されます。
   a. クライアントがアクセス ポイントとのアソシエーションに使用した SSID が、RADIUS サーバが返した許可リスト内のエントリに一致する場合、クライアントはすべての認証要件を満たした後にネットワークへのアクセスを許可されます。
   b. アクセス ポイントが、SSID の許可リストにクライアントと一致するエントリを検出できなかった場合は、このクライアントはアソシエーションを解除されます。
   c. RADIUS サーバがクライアントに SSID をまったく返さない場合（リストなし）は、管理者がリストを設定していないことを意味します。この場合、クライアントはアソシエーションと認証の試行を許可されます。

RADIUS サーバの返す SSID の許可リストは、シスコ Vendor-Specific Attribute（VSA; ベンダー固有の属性）の形式です。Internet Engineering Task Force（IETF、インターネット技術特別調査委員会）のドラフト規格では、アクセス ポイントと RADIUS サーバ間で、ベンダー固有の属性（属性 26）を使用してベンダー固有の情報をやり取りする方法を指定しています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は *cisco-avpair* です。RADIUS サーバには、クライアントあたり 0 以上の SSID VSA を指定できます。

次の例では、次の AV ペアにより、ユーザの SSID 許可リストに SSID *batman* が追加されます。

```
cisco-avpair= "ssid=batman"
```

VSA を認識して使用できるようにアクセス ポイントを設定する方法については、「ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定」（P.13-17）を参照してください。

複数の基本 SSID の設定

アクセス ポイントの 802.11a、802.11b、802.11n 無線は、最大 16 の基本 SSID（BSSID）をサポートします。BSSID は、特定の SSID（ネットワーク名）文字列にアソシエートされる無線 MAC アドレスです。

複数の SSID を使用して、それぞれの SSID に一意の DTIM 設定を割り当て、SSID ごとに 1 つのビーコンをブロードキャストします。DTIM を大きな値に設定すると、SSID を使用する省電力モードのクライアント デバイスではバッテリの寿命が延びます。また、複数の SSID をブロードキャストすると、ゲストが無線 LAN にアクセスしやすくなります。

（注）　アクセス ポイントの MAC アドレスに基づいて特定のアクセス ポイントにアソシエートするよう設定していた場合（クライアント デバイス、リピータ、ホット スタンバイ ユニット、ワークグループ ブリッジなど）、複数の BSSID の追加または削除を行うと、無線 LAN 上のデバイスがアソシエーションを損失することがあります。複数の BSSID を追加または削除する際には、特定のアクセス ポイントにアソシエートするよう設定されていたデバイスのアソシエーション状態を確認してください。必要に応じて、アソシエートされていないデバイスを再設定して、BSSID の MAC アドレスを使用するようにします。

複数 BSSID の設定要件

複数の BSSID を設定するには、アクセス ポイントが少なくとも次の要件を満たしている必要があります。

- VLAN が設定されていること。
- アクセス ポイントが Cisco IOS Release 12.3(4)JA 以降を実行していること。
- サポートされる基本 SSID の数を判別するには、**show controllers** *radio_interface* コマンドを入力します。結果に次の行が含まれていれば、その無線は複数の基本 SSID をサポートしています。

  `Number of supported simultaneous BSSID on radio_interface: 16`

複数の BSSID を使用する際のガイドライン

複数の BSSID を設定する際は、次のガイドラインに留意してください。

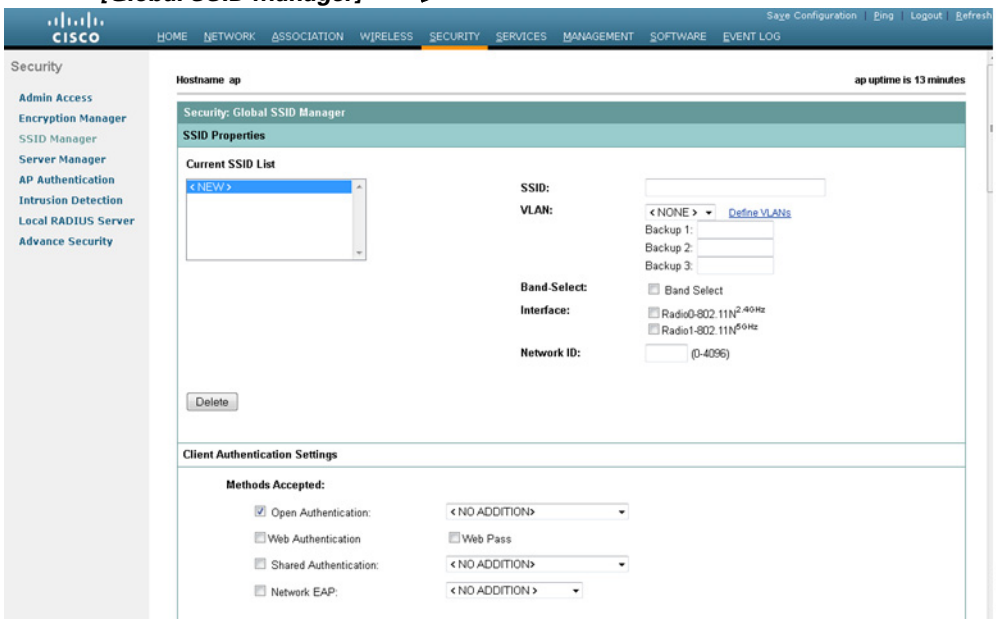
- 複数の BSSID を有効に設定すると、RADIUS サーバによる VLAN 割り当て機能がサポートされなくなります。
- BSSID を有効に設定すると、アクセス ポイントが各 SSID に BSSID を自動的にマッピングします。BSSID を特定の SSID に手動でマッピングすることはできません。
- アクセス ポイントで複数の BSSID を有効にすると、オプションの SSIDL IE には、SSID リストは追加されず、拡張機能だけが追加されます。
- Wi-Fi 認定済みクライアント デバイスであれば、どれでも複数 BSSID を使用したアクセス ポイントにアソシエートできます。
- Wireless Domain Service（WDS; 無線ドメイン サービス）を構成するアクセス ポイントでは、複数の BSSID を有効に設定できます。

複数の BSSID の設定

複数の BSSID（MBSSID）を設定するには、次の手順に従います。

ステップ 1　アクセス ポイントの GUI から、[Global SSID Manager] ページを表示します（GUI ではなく CLI を使用する場合は、この項の最後のCLI の設定例に記載している CLI コマンドを参照してください）。図 7-1 は、[Global SSID Manager] ページの上部を示しています。

図 7-1　[Global SSID Manager] ページ



ステップ 2　[SSID] フィールドに SSID 名を入力します。

ステップ 3　[VLAN] ドロップダウン リストから、SSID を割り当てる VLAN を選択します。

ステップ 4　SSID を有効に設定している無線インターフェイスを選択します。SSID 設定を検証して無線インターフェイスを有効にするまで、SSID はアクティブになりません。

ステップ 5　（任意）[Network ID] フィールドに、SSID のネットワーク ID を入力します。

ステップ 6　このページの [Authentication Settings]、[Authenticated Key Management]、[Accounting Settings] セクションから、認証、認証済みキー管理、アカウンティング設定を SSID に設定します。MBSSID は、SSID でサポートされているすべての認証タイプをサポートします。

ステップ 7　（任意）SSID をビーコンに追加するには、[Multiple BSSID Beacon Settings] セクションで [Set SSID as Guest Mode] チェックボックスをオンにします。

ステップ 8　（任意）この SSID を使用する省電力モードのクライアントのバッテリの寿命を延ばすには、[Set Data Beacon Rate (DTIM)] チェックボックスをオンにして SSID のビーコン レートを入力します。ビーコン レートによって、Delivery Traffic Indicator Message（DTIM）を追加したビーコンをアクセス ポイントが送信する頻度が決まります。

DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが再起動します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。

デフォルトのビーコン レートは 2 に設定されています。つまり、ビーコン 1 つおきに DTIM が追加されます。ビーコン レートは 1 ～ 100 の値で入力します。

（注）　DTIM 期間のカウントを増やすと、マルチキャスト パケットの送信は遅れます。マルチキャスト パケットはバッファリングされるため、DTIM 期間のカウントを大きくするとバッファがオーバーフローする可能性があります。

ステップ 9　[Guest Mode/Infrastructure SSID Settings] セクションで、[Multiple BSSID] を選択します。

ステップ 10　[Apply] をクリックします。

CLI の設定例

次の例は、無線インターフェイスで複数の BSSID を有効に設定する CLI コマンド、*visitor* を呼び出した SSID を作成する CLI コマンド、SSID を BSSID に指定する CLI コマンド、BSSID がビーコンに追加されていることを指定する CLI コマンド、BSSID に DTIM 間隔を設定する CLI コマンド、無線インターフェイスに SSID *visitor* を設定する CLI コマンドを示しています。

```
ap(config)# interface do0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor vlan20
ap(config-ssid)# mbssid guest-mode dtim-period 3
ap(config-ssid)# exit
ap(config)# interface do0
ap(config-if)# ssid visitor
```

また、**dot11 mbssid** グローバル コンフィギュレーション コマンドを使用すると、複数の BSSID をサポートしているすべての無線インターフェイスで、複数の BSSID を同時に有効にすることもできます。

設定済み BSSID の表示

SSID と BSSID の関係、または MAC アドレスを表示するには、**show dot11 bssid** 特権 EXEC コマンドを使用します。次の例はコマンドの出力を示しています。

```
AP1230#show dot11 bssid
Interface     BSSID           Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

SSID に対する IP リダイレクションの割り当て

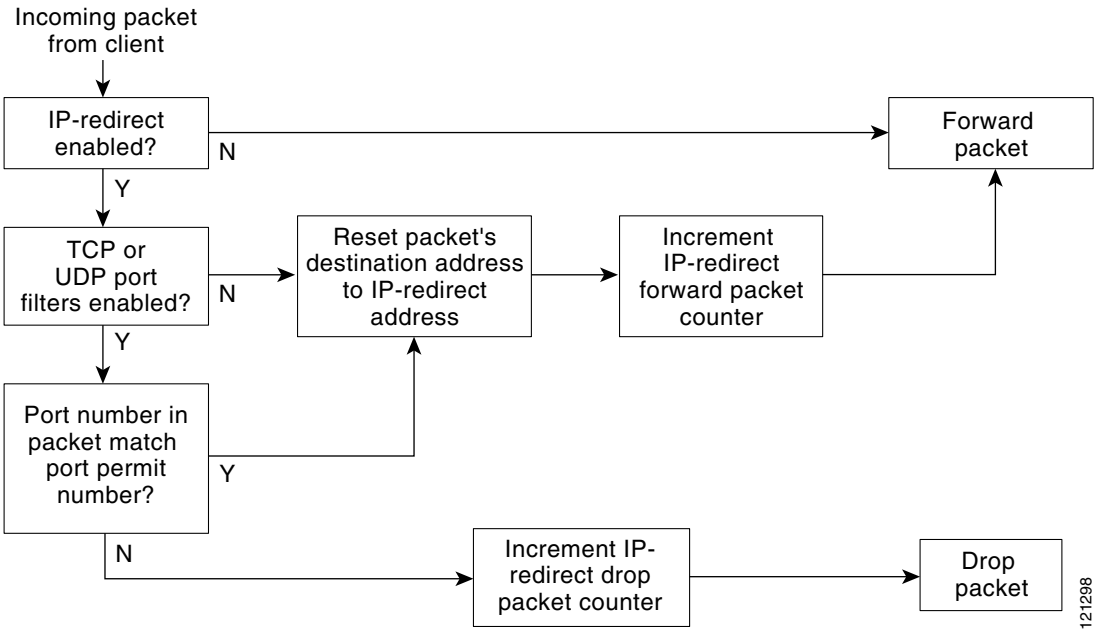
SSID に IP リダイレクションを設定すると、その SSID にアソシエートされたクライアント デバイスからアクセス ポイントに送信されたパケットはすべて、指定した IP アドレスにリダイレクトされます。IP リダイレクションが主に使用されるのは、特定の IP アドレスと通信するように静的に設定され、中央にあるソフトウェア アプリケーションを使用するハンドヘルド デバイスをクライアントとする無線 LAN です。たとえば、小売店や商品倉庫の無線 LAN 管理者は、バーコード スキャナに IP リダイレクションを設定できます。これらすべてのバー コード スキャナでは、同じスキャナ アプリケーションが使用され、すべてのデータは同じ IP アドレスに送信されます。

SSID を使用してアソシエートされているクライアント デバイスからのパケットをすべてリダイレクトできる他、アクセス コントロール リストで定義された特定の TCP ポートや UDP ポート宛てのパケットだけをリダイレクトすることもできます。特定のポート宛てのパケットだけがリダイレクトされるようにアクセス ポイントを設定すると、その SSID を使用しているクライアントからの該当のパケットがアクセス ポイントからリダイレクトされます。また、同じ SSID を使用しているクライアントからのその他のパケットは、アクセス ポイントでドロップされます。

（注） IP リダイレクトが設定された SSID を使用してアソシエートされているクライアント デバイスに対して、アクセス ポイントから ping テストを実行すると、そのクライアントからの応答パケットは、指定した IP アドレスにリダイレクトされ、アクセス ポイントでは受信されません。

図 7-2 は、IP リダイレクトが設定された SSID を使用してアソシエートされているクライアントからのパケットを、アクセス ポイントで受信した場合の処理フローを示しています。

図 7-2　IP リダイレクションの処理フロー



IP リダイレクションを使用する際のガイドライン

IP リダイレクションを使用する際は、次のガイドラインに留意してください。

- クライアント デバイスからブロードキャスト、ユニキャスト、またはマルチキャストで送信された BOOTP/DHCP パケットは、アクセス ポイントからリダイレクトされません。
- 受信パケットに対する ACL フィルタが存在する場合は、IP リダイレクションより優先して適用されます。

IP リダイレクションの設定

特権 EXEC モードから、次の手順に従って SSID に IP リダイレクションを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid-string*	特定の SSID に対するコンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip redirection host** *ip-address*	目的の IP アドレスに対して、IP リダイレクション コンフィギュレーション モードを開始します。ドットを使用して IP アドレスを入力します（例:10.91.104.92）。 リダイレクションの対象となる TCP ポートや UDP ポートを定義したアクセス コントロール リスト（ACL）を指定しない場合は、クライアント デバイスから受信されたパケットはすべてアクセス ポイントからリダイレクトされます。
ステップ 4	**ip redirection host** *ip-address* **access-group** *acl* **in**	（任意）パケットのリダイレクションに適用する ACL を指定します。ACL で定義した特定の UDP ポートまたは TCP ポート宛てに送信されたパケットだけがリダイレクトされます。ACL で定義した設定に一致しない受信パケットはすべて廃棄されます。**in** パラメータを指定すると、アクセス ポイントの受信インターフェイスに ACL が適用されます。

（注）　ACL ロギングは、アクセス ポイントのプラットフォームのブリッジング インターフェイスではサポートされていません。ブリッジング インターフェイスに適用すると、インターフェイスがログ オプションなしで設定されたように動作し、ロギングは実施されません。BVI インターフェイスに別の ACL を使用している限り、ACL ロギングは、BVI インターフェイスで動作します。

次の例は、ACL を適用せずに SSID に IP リダイレクションを設定する方法を示しています。*batman* という SSID にアソシエートされているクライアント デバイスから受信されたパケットはすべて、アクセス ポイントからリダイレクトされます。

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

SSID ビーコンに SSIDL IE を含める

アクセス ポイントは SSID ごとに 1 つのビーコンをブロードキャストします。デフォルトでは、SSID ビーコンのいずれか 1 つだけが、関連する SSID 名を示します。MBSSID 機能が使用されない限り、同じ無線のその他のビーコンでは SSID フィールドが空のままになります。

（注）　アクセス ポイントで複数の BSSID を有効に設定すると、SSIDL IE には、SSID リストは追加されず、拡張機能だけが追加されます。

特権 EXEC モードから、次の手順に従って SSID IE を SSIDL ビーコンに含めます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid-string*	特定の SSID に対するコンフィギュレーション モードを開始します。ゲスト モードに設定された SSID を選択することが推奨されます（つまり、SSID 文字列をビーコンにアドバタイズします）。
ステップ 3	**information-element ssidl** [**advertisement**] [**wps**]	アクセス ポイントの拡張機能をアドバタイズするアクセス ポイント ビーコンに、SSIDL IE を追加します。この拡張機能には、802.1x、Microsoft Wireless Provisioning Services（WPS）のサポートなどがあります。 SSIDL IE に SSID の名前と機能を追加するには、**advertisement** オプションを使用します。SSIDL IE に WPS 機能フラグを設定するには、**wps** オプションを使用します。

SSIDL IE を無効にするには、コマンドの **no** 形式を使用します。デフォルトでは、SSIDL IE は無効になっています。

MBSSID の NAC サポート

ネットワークは、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。これらのセキュリティ脅威によって業務に支障をきたし、ダウンタイムが生じたり、パッチの適用に追われたりすることになります。ネットワークにアクセスしようとするすべての有線/無線デバイスが、企業のセキュリティ ポリシーに適合するように、エンドポイントを視覚化して管理することが必要です。感染したエンドポイントや脆弱なエンドポイントを自動的に検出して切り離し、クリーンな状態にする必要があります。

NAC は、ネットワーク リソースにアクセスするすべての有線/無線のエンドポイント デバイス（PC、ノート パソコン、サーバ、PDA など）が適切にセキュリティ脅威から保護されるよう厳密に設計されています。NAC を使用することにより、企業は、ネットワークに参加するすべてのデバイスを分析して管理できるようになります。すべてのエンドポイント デバイスが企業のセキュリティ ポリシーに準拠し最新のセキュリティ保護策を確実に実行することにより、企業はウイルス感染やネットワークのセキュリティ侵害の経路となりやすいエンドポイント デバイスを大幅に削減または排除できます。

WLAN は、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。NAC アプライアンスも NAC フレームワークも、WLAN クライアントがネットワークにアクセスしようとするときにデバイス セキュリティ ポリシーを施行することで、WLAN をセキュリティ脅威から保護します。これらのソリューションは、ポリシーに準拠しない WLAN クライアントを検疫し、ポリシーに準拠するように修復するサービスを提供しています。

クライアントは、ソフトウェアのバージョンやウイルスのバージョンなどの状態に応じて、別々の VLAN に配置されます。必要なソフトウェアをダウンロードするよう VLAN を設定して、クライアントをネットワークのアクセスに必要なソフトウェアのバージョンにアップグレードします。NAC サポートには 4 つの VLAN が設定されます。そのうちの 1 つは通常の VLAN で、ここには、正しいソフトウェア バージョンを搭載したクライアントが配置されます。その他の VLAN は指定された検疫処理用に確保されています。クライアントがアップグレードされるまで、感染したすべてのクライアントはいずれか 1 つの VLAN に配置されます。

各 SSID では、最大 3 つの VLAN を「有害な」VLAN として設定できます。感染したクライアントは、感染状態に応じて、いずれか 1 つの VLAN に配置されます。クライアントがアソシエーション要求を送信すると、クライアントの感染ステータスをその要求に含めて RADIUS サーバへ送信します。クライアントを特定の VLAN に配置するポリシーのプロビジョニングが RADIUS サーバ上で行われます。

感染したクライアントがアクセス ポイントにアソシエートして RADIUS サーバにそのステートを送信すると、RADIUS サーバは状態に応じてそのクライアントを検疫 VLAN の 1 つに配置します。この VLAN は、dot1x クライアント認証プロセスの途中で、RADIUS サーバの Access Accept 応答内で送信されます。クライアントが健全な状態で、NAC に準拠している場合、RADIUS サーバは通常の VLAN 割り当てを SSID に返し、クライアントは正しい VLAN と BSSID に配置されます。

各 SSID には、通常の VLAN が割り当てられます。通常の VLAN とは、健全なクライアントが配置される VLAN のことです。また、SSID では、ステートに応じてクライアントが配置される検疫 VLAN 対応するバックアップ VLAN を最大 3 つまで設定できます。SSID 用のこれらの VLAN には、SSID の MBSSID によって割り当てた BSSID と同じものを使用します。

設定済み VLAN はそれぞれ異なり、同じ SSID 内で VLAN が重複することはできません。このため、VLAN を設定できるのは 1 つのインターフェイスにつき一度だけで、2 つの異なる SSID で VLAN は使用できません。

検疫 VLAN は、通常の VLAN を設定したインターフェイスで自動的に設定されます。検疫 VLAN は、通常 VLAN と同じ暗号プロパティを継承します。VLAN には、同じキー/認証タイプがあり、検疫 VLAN のキーは自動的に派生します。

Dot11 サブインターフェイスが生成され、dot1q カプセル化 VLAN（設定済み VLAN 数と同数）とともに自動的に設定されます。また、有線側のサブインターフェイスも、ブリッジ グループ設定と併せてギガビット イーサネット 0 サブインターフェイスに自動的に設定されます。

クライアントがアソシエートして RADIUS サーバが有害な状態と判断すると、dot1x 認証の RADIUS 認証応答内でサーバが検疫 NAC の VLAN のいずれかを返します。この VLAN は、クライアントの SSID で設定したバックアップ用 VLAN のうちの 1 つでなければなりません。この VLAN が、すでに設定したバックアップ用 VLAN のうちの 1 つでなければ、クライアントはアソシエートされません。

すべてのバックアップ用 VLAN に対応するデータは、SSID に割り当てられた BSSID を使用して送受信されます。このため、その SSID に対応する BSSID をリッスンしているすべてのクライアント（健全なクライアントおよび有害なクライアント）が再起動します。VLAN が健全か有害かに応じて、使用中のマルチキャスト キーに基づき、クライアントでパケットの復号化が行われます。有線側のトラフィックは、別の VLAN を使用しているため隔離されます。このようにして、感染したクライアントのトラフィックと感染していないクライアントのトラフィックが混在しないようにしています。

次に示すように、**dot11 ssid** <*ssid*> では、これまでの **vlan** <*name*> | <*id*> に、新キーワード **backup** が追加されます。

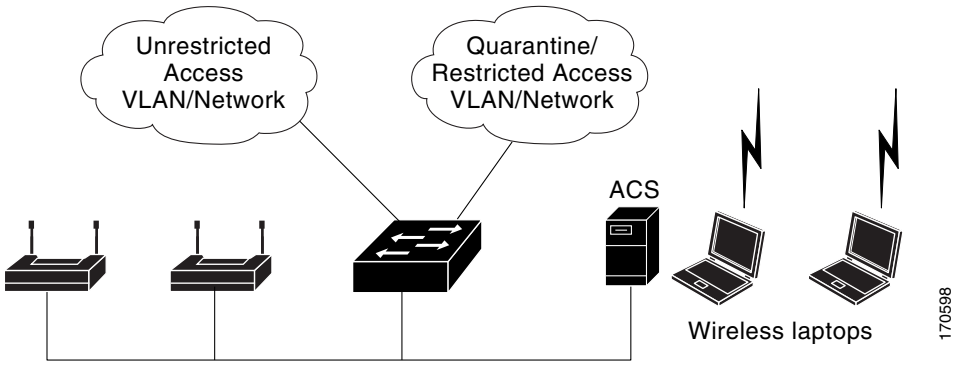
```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```

MBSSID への NAC 設定

（注）　この機能がサポートするのは、VLAN 内のレイヤ 2 モビリティだけです。この機能は、ネットワーク ID を使用するレイヤ 3 モビリティをサポートしません。

（注）　アクセス ポイントで MBSSID の NAC を有効にする前に、NAC が正しく機能するようにしてください。図 7-3 は、一般的なネットワーク設定を示しています。

図 7-3　　一般的な NAC ネットワーク設定



詳細については、シスコ無線ネットワークに NAC を展開する方法のマニュアルを参照してください。

アクセス ポイントの MBSSID に NAC を設定する手順は、次のとおりです。

ステップ 1　図 7-3 に示すように、ネットワークを設定します。

ステップ 2　スタンドアロンのアクセス ポイントと、NAC 対応クライアントの EAP 認証を設定します。

ステップ 3　ポスチャを確認するため、ACS サーバにローカル プロファイルを設定します。

ステップ 4　クライアントが EAP-FAST を使用して正常に認証できるよう、クライアントとアクセス ポイントを設定します。

ステップ 5　クライアントのポスチャが有効であることを確認します。

ステップ 6　認証とポスチャ確認が完了したら、クライアントがアクセス ポイントとアソシエートしていること、クライアントが制限のない VLAN に配置されていることを確認します。

設定例を次に示します。

```
dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
    vlan engg-normal backup engg-infectedauthentication open
    authentication network-eap eap_methods
```

```
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
!
interface Dot11Radio0
!
encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
encryption vlan engg-normal mode ciphers wep40
!
encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
encryption vlan mktg-normal mode ciphers wep40
!
ssid engg
!
ssid mktg
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
```

CHAPTER 8

スパニングツリー プロトコルの設定

この章では、アクセス ポイント/ブリッジにスパニングツリー プロトコル（STP）を設定する方法について説明します。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Access Points and Bridges*』を参照してください。

（注） STP は、アクセス ポイントがブリッジ モードのときだけ使用できます。

スパニングツリー プロトコルの概要

この項では、スパニングツリー機能の仕組みについて説明します。内容は次のとおりです。

STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。スパニングツリーはエンド ステーションに対して透過的に動作するため、エンド ステーションが単一の LAN セグメントに接続されているのか、複数セグメントから成る LAN に接続されているのかを検出することはできません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリー パスを構築する必要があります。スパニングツリー アルゴリズムは、レイヤ 2 ネットワーク全体でループのない最適なパスを計算します。無線アクセス ポイント/ブリッジやスイッチなどのインフラストラクチャ デバイスは、ブリッジ プロトコル データ ユニット(BPDU)というスパニングツリーのフレームを一定間隔で送受信します。デバイスはこれらのフレームを転送せずに、ループのないパスを構成するために使用します。

エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。また、インフラストラクチャ デバイスでも、複数のレイヤ 2 インターフェイス上でエンド ステーションの MAC アドレスを学習する場合があります。このような状況によって、ネットワークが不安定になります。

STP は、レイヤ 2 ネットワーク内のルート ブリッジと、ルートからすべてのインフラストラクチャ デバイスまでのループのないパスでツリーを定義します。

(注) STP の説明において、*ルート*という用語は 2 つの概念を指して使用されます。1 つは、スパニングツリーの中央ポイントとして機能するネットワーク上のブリッジのことで、*ルート ブリッジ*と呼ばれます。もう 1 つは、各ブリッジでルート ブリッジまでの最も効率的なパスを提供するポートのことで、*ルート ポート*と呼ばれます。これらの意味は、ルートおよび非ルートのオプションを持つ無線ネットワーク設定の役割とは区別されます。無線ネットワーク設定の役割がルート ブリッジとなっているブリッジが、必ずしもスパニングツリーのルート ブリッジになるわけではありません。この章では、スパニングツリーのルート ブリッジを*スパニングツリー ルート*と呼びます。

STP は冗長データ パスを強制的にスタンバイ(ブロック)ステートにします。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。

ブリッジ上の 2 つのインターフェイスがループの一部を形成する場合、スパニングツリー ポートの優先順位およびパス コストの設定により、2 つのうちフォワーディング ステートにするインターフェイスと、ブロッキング ステートにするインターフェイスが決まります。ポートの優先順位の値は、ネットワーク トポロジにおけるインターフェイスの位置を表し、その位置がトラフィックを渡すのにどの程度適しているかを示します。パス コスト値はメディアの速度を表します。

アクセス ポイント/ブリッジは、Per-VLAN Spanning Tree（PVST）と VLAN を使用しない単一の 802.1q スパニングツリーの両方をサポートします。アクセス ポイント/ブリッジは、複数の VLAN を 1 つのインスタンスのスパニングツリーにマッピングする 802.1s MST または 802.1d Common Spanning Tree を実行できません。

アクセス ポイント/ブリッジは、設定されているアクティブな VLAN ごとに個別のスパニングツリー インスタンスを保持します。ブリッジの優先順位およびアクセス ポイント/ブリッジの MAC アドレスから成るブリッジ ID は、各インスタンスに関連付けられます。VLAN ごとに、最も小さいアクセス ポイント/ブリッジ ID を持つアクセス ポイント/ブリッジが、その VLAN のスパニングツリー ルートになります。

アクセス ポイント/ブリッジのプロトコル データ ユニット

安定して有効なネットワークのスパニングツリー トポロジは、次の要素によって決まります。

- 各無線アクセス ポイント/ブリッジ上の各 VLAN に関連付けられた固有のアクセス ポイント/ブリッジ ID（無線アクセス ポイント/ブリッジの優先順位および MAC アドレス）
- スパニングツリー ルートまでのスパニングツリー パス コスト
- 各レイヤ 2 インターフェイスに対応付けられたポート ID（ポート プライオリティおよび MAC アドレス）

ネットワーク内のアクセス ポイント/ブリッジに電源が入ると、各アクセス ポイント/ブリッジは STP ルートとして機能します。アクセス ポイント/ブリッジは、イーサネット ポートおよび無線ポートを使用してコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側のアクセス ポイント/ブリッジがスパニングツリー ルートとして識別する無線アクセス ポイント/ブリッジの固有のアクセス ポイント/ブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信側のアクセス ポイント/ブリッジのアクセス ポイント/ブリッジ ID
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

アクセス ポイント/ブリッジは、*上位*の情報（より小さいアクセス ポイント/ブリッジ ID やパス コストなど）を含むコンフィギュレーション BPDU を受信すると、そのポートの情報を保存します。この BPDU をアクセス ポイント/ブリッジのルート ポート上で受信した場合、そのアクセス ポイント/ブリッジが指定アクセス ポイント/ブリッジとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

アクセス ポイント/ブリッジは、そのポートに現在保存されている情報よりも *下位*の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。アクセス ポイント/ブリッジが下位 BPDU を受信した LAN の指定アクセス ポイント/ブリッジである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- スパニングツリー ルートとしてアクセス ポイント/ブリッジが 1 つ選択されます。
- アクセス ポイント/ブリッジごとに（スパニングツリー ルートを除く）ルート ポートが 1 つ選択されます。このポートは、アクセス ポイント/ブリッジからスパニングツリー ルートにパケットを転送するときの最適パス（最小コスト）を提供します。
- スパニングツリー ルートへの最短距離は、パス コストに基づいてアクセス ポイント/ブリッジごとに計算されます。
- LAN セグメントごとに指定アクセス ポイント/ブリッジが選択されます。指定アクセス ポイント/ブリッジは、その LAN からスパニングツリー ルートにパケットを転送するときの最小パス コストを提供します。指定アクセス ポイント/ブリッジを LAN に接続しているポートのことを*指定ポート*と呼びます。
- スパニングツリー インスタンスに含めるインターフェイスが選択されます。ルート ポートおよび指定ポートは、フォワーディング ステートになります。
- スパニングツリーに含まれないすべてのインターフェイスはブロックされます。

スパニングツリー ルートの選択

STP に参加しているレイヤ 2 ネットワークのすべてのアクセス ポイント/ブリッジは、BPDU データ メッセージの交換を通して、ネットワーク内の他のアクセス ポイント/ブリッジに関する情報を集めます。このメッセージ交換により、次の操作が発生します。

- スパニングツリー インスタンスごとに固有のスパニングツリー ルートを選択
- LAN セグメントごとに指定アクセス ポイント/ブリッジを 1 つずつ選択
- 冗長リンクに接続されたレイヤ 2 インターフェイスをブロックすることにより、ネットワーク内のループを排除

VLAN ごとに、アクセス ポイント/ブリッジの優先順位が最も高いアクセス ポイント/ブリッジ（最も小さい数字の優先順位の値）がスパニングツリー ルートとして選択されます。すべてのアクセス ポイント/ブリッジがデフォルトの優先順位（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいアクセス ポイント/ブリッジがスパニングツリー ルートになります。アクセス ポイント/ブリッジの優先順位の値は、アクセス ポイント/ブリッジ ID の最上位ビットに該当します。

アクセス ポイント/ブリッジの優先順位の値を変更すると、アクセス ポイント/ブリッジがルート アクセス ポイント/ブリッジとして選択される確率が変化します。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

スパニングツリー ルートは、スパニングツリー トポロジにおいて論理的な中心に位置します。ネットワーク内のどこからもスパニングツリー ルートに到達する必要のないすべてのパスは、スパニングツリーのブロッキング モードになります。

BPDU には、アクセス ポイント/ブリッジおよび MAC アドレス、アクセス ポイント/ブリッジの優先順位、ポートの優先順位、およびパス コストを含む、送信側アクセス ポイント/ブリッジとそのポートに関する情報が含まれます。STP はこの情報を使用して、ネットワークのスパニングツリー ルートとルート ポート、および各 LAN セグメントのルート ポートと指定ポートを選択します。

スパニングツリー タイマー

表 8-1 で、スパニングツリーのパフォーマンス全体を左右するタイマーについて説明します。

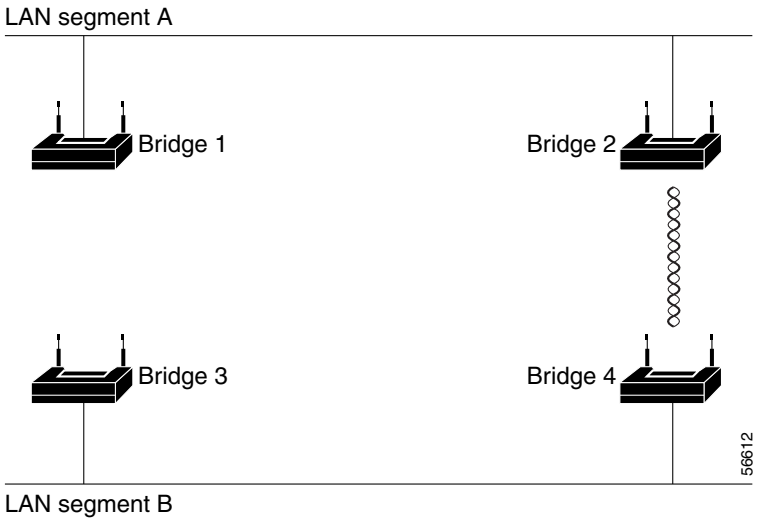
表 8-1　　スパニングツリー タイマー

変数	説明
ハロー タイマー	アクセス ポイント/ブリッジが hello メッセージを他のアクセス ポイント/ブリッジにブロードキャストする頻度が決まります。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートがそれぞれ持続する時間が決まります。
最大エージング タイマー	アクセス ポイント/ブリッジがインターフェイス上で受信したプロトコル情報を保存する時間が決まります。

スパニングツリー トポロジの作成

図 8-1 では、すべてのアクセス ポイント/ブリッジの優先順位がデフォルト（32768）に設定されていて、ブリッジ 4 の MAC アドレスが最も小さいため、ブリッジ 4 がスパニングツリー ルートとして選択されています。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプが原因で、ブリッジ 4 が理想的なスパニングツリー ルートではない場合もあります。理想的なブリッジがスパニングツリー ルートになるように優先順位を上げる（数値を小さくする）ことにより、強制的にスパニングツリーを再計算させて、理想的なブリッジをスパニングツリー ルートとして使用する新しいトポロジを構成します。

図 8-1　　スパニングツリー トポロジ



スパニングツリー インターフェイス ステート

プロトコル情報が無線 LAN を通過する場合、伝播遅延が生じる可能性があります。結果として、その時々やさまざまな場所で、トポロジの変更が行われる場合があります。インターフェイスがスパニングツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータ ループが形成されることがあります。インターフェイスは、LAN 経由で伝播される新しいトポロジ情報を待ってから、フレームの転送を開始しなければなりません。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているアクセス ポイント/ブリッジ上の各インターフェイスは、次のいずれかのステートで存在します。

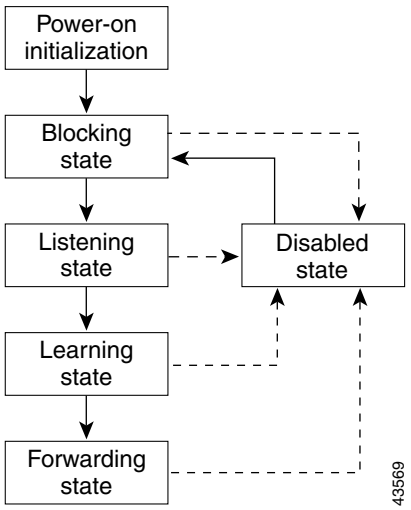
- ブロッキング：インターフェイスはフレーム転送に関与しません。
- リスニング：スパニングツリーでインターフェイスがフレーム転送に参加する必要があると判断された場合、ブロッキング ステートの次に最初に遷移するステート。
- ラーニング：インターフェイスはフレーム転送に関与する準備をしている状態です。
- フォワーディング：インターフェイスはフレームを転送します。
- ディセーブル：インターフェイスはスパニングツリーに含まれません。シャットダウン ポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリー インスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 8-2 に、インターフェイスがステートをどのように移行するかを示します。

図 8-2　　スパニングツリー インターフェイス ステート



アクセス ポイント/ブリッジで STP を有効にすると、イーサネット インターフェイスおよび無線インターフェイスは一度ブロッキング ステートになってから、リスニングおよびラーニングの一時的なステートに遷移します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. インターフェイスをブロッキング ステートに遷移させるプロトコル情報をスパニングツリーが待っている間、そのインターフェイスはリスニング ステートの状態です。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、アクセス ポイント/ブリッジが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

ブロッキング ステート

ブロッキング ステートのインターフェイスは、フレーム転送に参加しません。初期化後、BPDU はアクセス ポイント/ブリッジのイーサネット ポートおよび無線ポートに送信されます。アクセス ポイント/ブリッジは、他のアクセス ポイント/ブリッジと BPDU 交換するまで、最初にスパニングツリー ルートとして機能します。この交換により、ネットワーク内のどのアクセス ポイント/ブリッジがスパニングツリー ルートになるかが決まります。ネットワークにアクセス ポイント/ブリッジが 1 つだけしかない場合、交換は行われず、転送遅延タイマーが切れた後にインターフェイスがリスニング ステートに遷移します。STP を有効にすると、インターフェイスは常にブロッキング ステートから開始されます。

ブロッキング ステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

（注） アクセス ポイント/ブリッジの 1 つのポートがブロックされている場合、ブロードキャスト パケットやマルチキャスト パケットは同じアクセス ポイント/ブリッジ上のフォワーディング ポートに到達するため、ブリッジング ロジックによって、ブロック ポートでパケットがドロップされる前に、一時的にブロック ポートがリスニング ステートに切り替わることがあります。

リスニング ステート

リスニング ステートは、インターフェイスがブロッキング ステートの次に開始する最初のステートです。インターフェイスは、STP によってインターフェイスがフレーム転送に参加する必要があると判断された場合、このステートを開始します。

リスニング ステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

ラーニング ステート

ラーニング ステートのインターフェイスは、フレーム転送に参加する準備を行います。インターフェイスはリスニング ステートからラーニング ステートに移行します。

ラーニング ステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

フォワーディング ステート

フォワーディング ステートのインターフェイスは、フレームを転送します。インターフェイスはラーニング ステートからフォワーディング ステートに移行します。

フォワーディング ステートのインターフェイスは次のように動作します。

- ポート上でのフレームの受信と受信したフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

ディセーブル ステート

ディセーブル ステートのインターフェイスは、フレーム転送にもスパニングツリーにも参加しません。ディセーブル ステートのインターフェイスは動作不能です。

無効のインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信しません。

STP 機能の設定

アクセス ポイント/ブリッジに STP を設定するには、3 つの主要な手順を完了させます。

1. 必要に応じて、インターフェイスおよびサブインターフェイスをブリッジ グループに割り当てます。
2. ブリッジ グループごとに STP を有効にします。
3. ブリッジ グループごとに STP の優先順位を設定します。

次の各項にはスパニングツリーの設定情報が含まれています。

- 「STP のデフォルト設定」(P.8-9)
- 「STP の設定」(P.8-9)
- 「STP の設定例」(P.8-10)

STP のデフォルト設定

STP はデフォルトでは無効に設定されています。表 8-2 に、STP を有効に設定したときのデフォルトの STP 設定を示します。

表 8-2　STP を有効にしたときのデフォルトの STP 値

設定	デフォルト値
ブリッジ プライオリティ	32768
ブリッジの最大経過時間	20
ブリッジの hello タイム	2
ブリッジの転送遅延	15
イーサネット ポートのパス コスト	19
イーサネット ポートの優先順位	128
無線ポートのパス コスト	33
無線ポートの優先順位	128

アクセス ポイント/ブリッジ上の無線インターフェイス、イーサネット インターフェイス、およびネイティブ VLAN は、デフォルトではブリッジ グループ 1 に割り当てられます。STP を有効にして、ブリッジ グループ 1 の優先順位を割り当てると、無線インターフェイス、イーサネット インターフェイス、およびプライマリ VLAN 上で STP が有効になり、これらのインターフェイスはブリッジ グループ 1 に割り当てられている優先順位を採用します。サブインターフェイスのブリッジ グループを作成し、そのブリッジ グループに異なる STP 設定を割り当てることができます。

STP の設定

特権 EXEC モードから、次の手順に従ってアクセス ポイント/ブリッジに STP を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface { dot11radio** *number* **| fastethernet** *number* **|** GigabitEthernet *number*}	無線またはイーサネットのインターフェイスまたはサブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。 ファスト イーサネット インターフェイスは 0 です。
ステップ 3	**bridge-group** *number*	インターフェイスをブリッジ グループに割り当てます。ブリッジ グループには 1 ～ 255 の範囲で番号を付けることができます。
ステップ 4	**no bridge-group** *number* **spanning-disabled**	ブリッジ グループに対して STP を自動的に無効にするコマンドを抑制します。**bridge** ***n*** **protocol ieee** コマンドを入力すると、STP がインターフェイス上で有効になります。

	コマンド	目的
ステップ 5	**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**bridge** *number* **protocol ieee**	ブリッジ グループに対して STP を有効にします。**bridge-group** コマンドを使用して作成するブリッジ グループごとに STP を有効にする必要があります。
ステップ 7	**bridge** *number* **priority** *priority*	（任意）ブリッジ グループに優先順位を割り当てます。優先順位を低くすると、ブリッジがスパニングツリー ルートになる可能性が高くなります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show spanning-tree bridge**	入力内容を確認します。
ステップ 10	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

STP の設定例

次の設定例では、VLAN の使用する場合と使用しない場合それぞれで、ルートおよび非ルートのアクセス ポイント/ブリッジに STP を有効に設定する方法を示します。

- 「VLAN を使用しないルート ブリッジ」(P.8-10)
- 「VLAN を使用しない非ルート ブリッジ」(P.8-11)
- 「VLAN を使用するルート ブリッジ」(P.8-12)
- 「VLAN を使用する非ルート ブリッジ」(P.8-15)

VLAN を使用しないルート ブリッジ

次に、VLAN が設定されていないルート ブリッジに STP を有効に設定する例を示します。

```
hostname master-bridge-south
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid visitor
 !
antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
```

```
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
ssid visitor2
 !
antenna gain 0
 peakdetect
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

VLAN を使用しない非ルート ブリッジ

次に、VLAN が設定されていない非ルート ブリッジに STP を有効に設定する例を示します。

```
hostname client-bridge-north
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
```

```
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid visitor
 !
antenna gain 0
 stbc
 station-role non-root
 bridge-group 1
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
ssid visitor2
 !
antenna gain 0
 peakdetect
 stbc
 station-role non-root
 bridge-group 1
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 path-cost 40
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
End
```

VLAN を使用するルート ブリッジ

次に、VLAN が設定されているルート ブリッジに STP を有効に設定する例を示します。

```
hostname master-bridge-hq
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
```

```
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid vlan1
 !
antenna gain 0
 stbc
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
```

```
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
!
interface GigabitEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 10000
bridge 2 protocol ieee
bridge 3 priority 3100
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

VLAN を使用する非ルート ブリッジ

次に、VLAN が設定されている非ルート ブリッジに STP を有効に設定する例を示します。

```
hostname client-bridge-remote
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
ssid vlan1
 !
antenna gain 0
 stbc
 station-role non-root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 station-role non-root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
```

```
 bridge-group 3 path-cost 500
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface GigabitEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 path-cost 400
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 12000
bridge 2 protocol ieee
bridge 3 priority 2900
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

スパニングツリー ステータスの表示

スパニングツリー ステータスを表示するには、表 8-3 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 8-3　　スパニングツリー ステータス表示用のコマンド

コマンド	目的
show spanning-tree	ネットワークのスパニングツリーに関する情報を表示します。
show spanning-tree blocked-ports	このブリッジのブロック ポートのリストを表示します。
show spanning-tree bridge	このブリッジのステータスおよび設定を表示します。

表 8-3　スパニングツリー ステータス表示用のコマンド （続き）

コマンド	目的
show spanning-tree active	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
show spanning-tree root	スパニングツリー ルートに関する情報の詳細な要約を表示します。
show spanning-tree interface *interface-id*	指定したインターフェイスのスパニングツリー情報を表示します。
show spanning-tree summary [**totals**]	ポート ステートの要約または STP ステート セクションの全行を表示します。

show spanning-tree 特権 EXEC コマンドのその他のキーワードの詳細は、このリリースの『*Cisco Aironet IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

ローカル認証サーバとしてのアクセス ポイントの設定

この章では、アクセス ポイントをローカル認証サーバとして設定して、小規模無線 LAN 用のスタンドアロン認証サーバとして機能させるか、またはバックアップ認証サービスを提供する方法について説明します。アクセス ポイントはローカル認証サーバとして、最大 50 のクライアント デバイスに対して Light Extensible Authentication Protocol（LEAP; 拡張認証プロトコル）認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証、および Media Access Control（MAC; メディア アクセス コントロール）ベースの認証を実行します。

ローカル認証の概要

802.1x 認証を使用すればさらにセキュリティを強化できる小規模な無線 LAN の多くは、RADIUS サーバにアクセスできません。802.1x 認証を使用する多くの無線 LAN でも、アクセス ポイントはクライアント デバイスの認証を、遠隔地にある RADIUS サーバに依存しているため、認証トラフィックは WAN リンクを通過する必要があります。この WAN リンクに不具合が発生した場合、または何らかの理由でアクセス ポイントが RADIUS サーバにアクセスできない場合、クライアント デバイスが必要とする作業が完全にローカルで行えるものであったとしても、このクライアント デバイスは無線ネットワークにアクセスできません。

WAN リンクやサーバが不具合を起こした場合にローカル認証サービスやバックアップ認証サービスを提供するため、アクセス ポイントをローカル認証サーバとして動作するよう設定できます。このように設定したアクセス ポイントは、LEAP 認証、EAP-FAST 認証、または MAC ベースの認証を使用して最大 50 の無線クライアント デバイスを認証できます。このアクセス ポイントは毎秒最大 5 つの認証を実行できます。

ローカル認証サーバのアクセス ポイントはクライアント ユーザ名とパスワードを使って手動で設定します。これは、このアクセス ポイントはメインの RADIUS サーバとデータベースを同期しないからです。また、クライアントが使用できる VLAN や Service Set Identifier（SSID; サービス セット ID）リストを指定することもできます。

（注） 使用している無線 LAN にアクセス ポイントが 1 箇所しかない場合、このアクセス ポイントを 802.1x 認証サーバ、およびローカル認証サーバの両方として設定できます。ただし、ローカル認証サーバとして稼働するアクセス ポイントにアソシエートされているユーザは、アクセス ポイントがクライアント デバイスを認証する際、パフォーマンスが低下することに気づく場合があります。

アクセス ポイントがメイン サーバに到達できない場合には、ローカル認証サーバを使用するように設定できます。または、RADIUS サーバを所有していない場合に、ローカル認証サーバを使用するようにアクセス ポイントを設定したり、アクセス ポイントをメイン認証サーバとして設定したりできます。ローカル認証サーバをメイン サーバのバックアップとして設定する場合、アクセス ポイントは定期的にメイン サーバへのリンクをチェックし、メイン サーバへのリンクが復元された場合は、ローカル認証サーバの使用を自動的に停止します。

注意 認証サーバとして使用するアクセス ポイントには、使用している無線 LAN に関する詳細な認証情報が含まれているため、このアクセス ポイントを物理的に保護して、構成を守る必要があります。

ローカル認証サーバの設定

この項では、アクセス ポイントをローカル認証サーバとして設定する方法について、次の項に分けて説明します。

ローカル認証サーバに対するガイドライン

アクセス ポイントをローカル認証サーバとして設定する場合は、次のガイドラインに従ってください。

- サービスを提供するクライアント デバイスの数が少ないアクセス ポイントを使用します。アクセス ポイントを認証サーバとして使用すると、アソシエートされているクライアント デバイスに対するパフォーマンスが低下します。
- アクセス ポイントを物理的に安全な場所に設置し、設定内容を保護してください。

コンフィギュレーションの概要

ローカル認証サーバの設定は、大きく次の 4 つの手順に分けて実行します。

1. クライアント デバイスを認証するためにローカル認証サーバの使用が許可されているアクセス ポイントのリストをローカル認証サーバに作成します。ローカル認証サーバを使用する各アクセス ポイントは、ネットワーク アクセス サーバ（NAS）です。

   （注）　使用するローカル認証サーバ アクセス ポイントがクライアント デバイスにもサービスを提供する場合は、このローカル認証サーバ アクセス ポイントを NAS として入力する必要があります。クライアントがこのローカル認証サーバ アクセス ポイントとアソシエートしている場合、このアクセス ポイントはクライアント認証のために自分自身を使用します。

2. ローカル認証サーバで、ユーザ グループを作成し、パラメータを各グループに対して適用されるように設定します（任意）。
3. ローカル認証サーバで、ローカル認証サーバが認証を許可された最大 50 の LEAP ユーザ、EAP-FAST ユーザ、または MAC アドレスのリストを作成します。

   （注）　ローカル認証サーバで実行する認証タイプを指定する必要はありません。認証サーバでは、そのユーザ データベースに記録されているユーザについて、LEAP 認証、EAP-FAST 認証、または MAC アドレス認証のいずれかが自動的に実行されます。

4. ローカル認証サーバを使用するアクセス ポイントで、ローカル認証サーバを RADIUS サーバとして入力します。

   （注）　使用するローカル認証サーバ アクセス ポイントがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバの設定時に、このローカル認証サーバを RADIUS サーバとして入力する必要があります。クライアントがこのローカル認証サーバ アクセス ポイントとアソシエートしている場合、このアクセス ポイントはクライアント認証のために自分自身を使用します。

ローカル認証サーバ アクセス ポイントの設定

特権 EXEC モードから、次の手順に従って、アクセス ポイントをローカル認証サーバとして設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	新しいアクセス コントロール コマンドと機能を有効にします。
ステップ 3	**radius-server local**	アクセス ポイントをローカル認証サーバとして有効にし、認証サーバのコンフィギュレーション モードを開始します。
ステップ 4	**nas** *ip-address* **key** *shared-key*	ローカル認証サーバを使用する装置のリストにアクセス ポイントを追加します。ローカル認証サーバとその他のアクセス ポイントの間の認証通信に使用される共有キーとアクセス ポイントの IP アドレスを入力します。ローカル認証サーバを使用するアクセス ポイントで、この共有キーを入力する必要があります。使用するローカル認証サーバがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバ アクセス ポイントを NAS として入力する必要があります。 **（注）** キー ストリングの先頭にある空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 このステップを繰り返して、ローカル認証サーバを使用する各アクセス ポイントを追加します。
ステップ 5	**group** *group-name*	（任意）ユーザ グループ コンフィギュレーション モードを開始して、共有設定を割り当てることができるユーザ グループを設定します。
ステップ 6	**vlan** *vlan*	（任意）ユーザ グループのメンバーが使用する VLAN を指定します。アクセス ポイントにより、グループ メンバーがその VLAN に移動されます。その他の VLAN 割り当ては無効になります。グループに割り当てられる VLAN は 1 つだけです。
ステップ 7	**ssid** *ssid*	（任意）最大 16 個の SSID を入力して、ユーザ グループのメンバーをそれらの SSID に制限します。アクセス ポイントは、クライアントがアソシエートに使用した SSID が、このリスト内の SSID の 1 つと一致するかどうかをチェックします。SSID が一致しない場合、このクライアントのアソシエーションが解除されます。
ステップ 8	**reauthentication time** *seconds*	（任意）アクセス ポイントがグループのメンバーを再認証するまでの秒数を入力します。この再認証により、ユーザには新しい暗号キーが与えられます。デフォルトの設定は 0 です。これは、グループのメンバーを再認証する必要がないことを表しています。

	コマンド	目的
ステップ 9	**block count** *count* **time** { *seconds* | **infinite** }	（任意）パスワード攻撃から保護するために、ここで設定した回数だけ誤ったパスワードが入力されると、一定の期間、そのグループ メンバーをロックアウトできます。 • count：ここで設定した回数だけ誤ったパスワードが入力されると、そのユーザ名がロックアウトされます。 • time：ロックアウトの継続時間を秒単位で指定します。**infinite** と入力した場合、ロックされたユーザ名を管理者が手動で解除する必要があります。クライアント デバイスのロック解除手順については、「ロックされたユーザ名のロック解除」（P.9-10）を参照してください。
ステップ 10	**exit**	グループ コンフィギュレーション モードを終了し、認証サーバ コンフィギュレーション モードに戻ります。
ステップ 11	**user** *username* { **password** | **nthash** } *password* [**group** *group-name*] [**mac-auth-only**]	ローカル認証サーバを使用した認証が許可されている LEAP ユーザおよび EAP-FAST ユーザを入力します。各ユーザについて、ユーザ名とパスワードを入力する必要があります。認証サーバ データベースでよく見かけられる、パスワードの NT 値しかわからない場合は、16 進数のストリングの NT ハッシュを入力することができます。 MAC ベースの認証のためにクライアント デバイスを追加するには、ユーザ名とパスワードの両方にクライアントの MAC アドレスを入力します。このユーザ名とパスワードには、12 桁の 16 進数を入力します。数字の間にピリオドやダッシュは使用しません。たとえば、MAC アドレスが 0009.5125.d02b である場合は、ユーザ名とパスワードの両方に *00095125d02b* と入力します。 ユーザを MAC 認証だけに制限するには、**mac-auth-only** と入力します。 このユーザをユーザ グループに追加するには、グループ名を入力します。グループを指定しない場合、ユーザは特定の VLAN には割り当てられず、再認証するように強制されることはありません。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例は、3 つのユーザ グループと数人のユーザが存在する 3 つのアクセス ポイントによって使用されるローカル認証サーバを設定する方法を表しています。

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
```

```
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group clerks mac-auth-only
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

他のアクセス ポイントがローカル認証サーバを使用するための設定

ローカル認証サーバを、他のサーバを追加するのと同じ方法で、アクセス ポイント上のサーバ リストに追加します。アクセス ポイントに RADIUS サーバを設定する手順の詳細は、第 13 章「RADIUS サーバと TACACS+ サーバの設定」を参照してください。

（注） 使用するローカル認証サーバ アクセス ポイントがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバが自分自身を使用してクライアント デバイスを認証するように設定する必要があります。

ローカル認証サーバを使用するアクセス ポイントで、**radius-server host** コマンドを使用して、ローカル認証サーバを RADIUS サーバとして入力します。アクセス ポイントがサーバの使用を試みる順序は、アクセス ポイント設定でサーバを入力した順序と同じになります。RADIUS を使用するためにアクセス ポイントを初めて設定している場合は、まず、メイン RADIUS サーバを入力し、最後にローカル認証サーバを入力してください。

（注） 認証ポートとして 1812 または 1645 を入力するか、アカウンティング ポートとして 1813 または 1646 を入力する必要があります。ローカル認証サーバは、RADIUS アカウンティング パケットを傍受するために UDP ポート 1813 をモニタします。アカウンティング パケットはローカル認証サーバにより廃棄されますが、サーバがダウンしていると RADIUS クライアントが仮定しないように、確認応答パケットを送り返します。

radius-server deadtime コマンドを使って、アクセス ポイントが応答のなかったサーバへ認証を試みるのを中止する間隔を設定します。これにより、要求がタイムアウトするまで待機しなくても、次に設定されたサーバを試行することができます。dead とマークされているサーバは、指定した期間（分単位）、その他の要求にもスキップされます。この期間は最高 1440 分（24 時間）まで指定できます。

次の例では、2 つのメイン サーバとローカル認証サーバについて、サーバのデッド タイムを 10 分間に設定する方法を示します。

```
AP(config)# aaa new-model
AP(config)# radius server radserv
AP(config-radius-server)# address ipv4 172.10.0.1 auth-port 1000 acct-port 1001
AP(config-radius-server)# key 77654
AP(config)# radius-server deadtime 10
```

この例では、メイン サーバへの WAN リンクに不具合が発生すると、LEAP 対応クライアント デバイスがアソシエートされている場合、アクセス ポイントは次の手順を実行します。

1. 最初のサーバを試し、複数回タイム アウトしたら、最初のサーバを dead とマークします。
2. 2 番目のサーバを試し、複数回タイム アウトしたら、2 番目のサーバを dead とマークします。
3. ローカル認証サーバを試し、正常に処理を終了します。

10 分間の dead-time 間隔中に、他のクライアント デバイスが認証を行う必要がある場合、このアクセス ポイントは最初の 2 台のサーバをスキップして、まず、ローカル認証サーバを試します。デッド タイム間隔後、アクセス ポイントはメイン サーバを使用して認証を試みます。デッド タイムを設定する場合、dead サーバをスキップする必要性と、WAN リンクをチェックする必要性との間でバランスをとり、できるだけ早く、メイン サーバの使用を再開する必要があります。

メイン サーバがダウンしているときに、アクセス ポイントがそのサーバの使用を試みるたびに、認証しようとしているクライアント デバイスが認証タイムアウトを報告する可能性があります。このクライアント デバイスは、メイン サーバがタイムアウトし、アクセス ポイントがローカル認証サーバの使用を試みている場合、再試行し、正常に処理を行います。予想されるサーバ タイムアウトに対応するために、シスコ クライアント デバイス上でタイムアウト値を延長することができます。

アクセス ポイント コンフィギュレーションからローカル認証サーバを削除するには、**no radius server** ***radserv*** グローバル コンフィギュレーション コマンドを使用します。

EAP-FAST の設定

ほとんどの無線 LAN 環境における EAP-FAST 認証では、デフォルトの設定のままで問題ありません。それでも、ネットワークの要件に合わせて、クレデンシャルのタイムアウト値、機関 ID、およびサーバ キーをカスタマイズすることはできます。

PAC の設定

この項では、Protected Access Credential（PAC）を設定する方法について説明します。EAP-FAST クライアント デバイスがローカル認証サーバに対する認証を初めて試みると、ローカル認証サーバではそのクライアントの PAC が生成されます。PAC を手動で生成して、PAC ファイルをクライアントに手動でインポートすることもできます。

PAC の有効期限

PAC に有効期間を設定し、さらにその有効期間が切れた後も暫定的にその PAC を有効にしておく猶予期間を指定できます。デフォルトでは、PAC の有効期間は 2 日（1 日のデフォルト期間プラス 1 日の暫定期間）です。ユーザ グループに対しても有効期限と猶予期間の設定を適用できます。

PAC に有効期限と猶予期間を設定するには、次のコマンドを使用します。

```
AP(config-radsrv-group)# [no] eapfast pac expiry days [grace days]
```

2 ～ 4095 の範囲で日数を入力します。有効期限と猶予期間をリセットして無期限にするには、コマンドの **no** 形式を入力します。

次の例では、ユーザ グループの PAC に 100 日間の有効期限と 2 日間の猶予期間を設定します。

```
AP(config-radsrv-group)# eapfast pac expiry 100 grace 2
```

PAC の手動生成

ローカル認証サーバでは、EAP-FAST クライアントからの要求に応じて、そのクライアントの PAC が自動的に生成されます。しかし、クライアント デバイスによっては、PAC を手動で生成することが必要な場合もあります。コマンドを入力すると、ローカル認証サーバで PAC ファイルが生成され、指定したネットワーク上の場所にそのファイルが書き出されます。ユーザは、その PAC ファイルをクライアントのプロファイルにインポートします。

PAC を手動で生成するには、次のコマンドを使用します。

AP# **radius local-server pac-generate** *username filename* [**password** *password*] [**expiry** *days*]

PAC のファイル名を入力するときは、ローカル認証サーバからその PAC ファイルが書き出される場所へのフル パスを指定します（tftp://172.1.1.1/test/user.pac など）。パスワードはオプションです。指定しなかった場合、CCX クライアントに有効なデフォルトのパスワードが使用されます。失効もオプションです。指定しなかった場合、デフォルトの期間は 1 日です。

次の例では、ローカル認証サーバでユーザ名 *joe* の PAC を生成し、パスワード *bingo* を設定してそのファイルを保護します。さらに、10 日間の有効期限をその PAC に設定して、アドレス 10.0.0.5 の Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに PAC ファイルを書き出します。

```
AP# radius local-server pac-generate tftp://10.0.0.5 joe password bingo expiry 10
```

機関 ID の設定

すべての EAP-FAST 認証サーバは、Authority Identity（AID; 機関 ID）で識別されます。認証対象のクライアントには、ローカル認証サーバからその AID が送信されます。受信したクライアントは、それに一致する AID が自身のデータベースにあるか確認します。送信された AID が確認できない場合、クライアントは新しい PAC を要求します。

ローカル認証サーバに AID を割り当てるには、次のコマンドを使用します。

```
AP(config-radserv)# [no] eapfast authority id identifier

AP(config-radserv)# [no] eapfast authority info identifier
```

identifier には最大 32 桁の 16 進数を設定できます。**eapfast authority id** コマンドにより、認証の際にクライアント デバイスで使用される AID が割り当てられます。

サーバ キーの設定

ローカル認証サーバでは、生成した PAC の暗号化、およびクライアントを認証する際の PAC の復号化にサーバ キーが使用されます。ローカル認証サーバには、プライマリ キーとセカンダリ キーという 2 種類のキーが保持されていますが、PAC の暗号化ではプライマリ キーが使用されます。デフォルトでは、プライマリ キーとしてデフォルト値が使用されます。セカンダリ キーは、設定しない限り、使用されません。

クライアントの PAC を受信したローカル認証サーバは、プライマリ キーを使用してその PAC を復号化しようとします。プライマリ キーによる復号化に失敗した場合、セカンダリ キーが設定されていれば、それを使用して PAC を復号化しようとします。復号化に失敗した認証サーバでは、その PAC は無効として拒否されます。

サーバ キーを設定するには、次のコマンドを使用します。

```
AP(config-radsrv)# [no] eapfast server-key primary {[auto-generate] | [ [0 | 7] key]}

AP(config-radsrv)# [no] eapfast server-key secondary [0 | 7] key
```

キーには、最大 32 桁の 16 進数を設定できます。暗号化されていないキーを入力するには、キーの前に **0** を入力します。暗号化されているキーを入力するには、キーの前に **7** を入力します。ローカル認証サーバをデフォルトの設定にリセットするには、コマンドの **no** 形式を使用します。これにより、プライマリ キーとしてデフォルト値が使用されるようになります。

アクセス ポイントのクロックが原因で発生する PAC の失敗

ローカル認証サーバでは、PAC の生成と PAC の有効性確認の両方でアクセス ポイントのクロックが使用されています。ただし、アクセス ポイントのクロックに依存することで、PAC の失敗が発生することがあります。

NTP サーバから時間設定を取得しているローカル認証サーバのアクセス ポイントの場合、起動してから NTP サーバに同期するまでに若干の時間がかかります。この間、そのアクセス ポイントでは、自身のデフォルトの時間設定が使用されることになります。このときにローカル認証サーバで PAC が生成されていると、NTP サーバから新しい時間設定がアクセス ポイントに取得された場合に、この PAC が期限切れになることがあります。また、アクセス ポイントの起動から NTP 同期までの間に EAP-FAST クライアントが認証を試みると、ローカル認証サーバではそのクライアントの PAC が無効として拒否されることがあります。

さらに、NTP サーバから時間設定を取得していないローカル認証サーバが頻繁にリブートする環境の場合、そのローカル認証サーバで生成された PAC が、有効期限を過ぎても期限切れにならないことがあります。アクセス ポイントのクロックは、アクセス ポイントがリブートするたびにリセットされます。その結果、クロックの経過時間が、PAC の有効期間に達しないことになります。

ローカル認証サーバにおける認証タイプの制限

ローカル認証サーバのアクセス ポイントでクライアント デバイスに対して実行できる認証は、デフォルトで LEAP 認証、EAP-FAST 認証、および MAC ベースの認証です。ただし、ローカル認証サーバが実行できる認証タイプを 1 ～ 2 種類に制限できます。認証サーバの認証タイプを 1 種類に制限するには、次のように認証コマンドの **no** 形式を使用します。

```
AP(config-radsrv)# [no] authentication [eapfast] [leap] [mac]
```

デフォルトではすべての認証タイプが有効なため、コマンドの **no** 形式を使用して認証タイプを無効にします。たとえば、認証サーバで LEAP 認証だけを実行するには、次のコマンドを入力します。

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

ロックされたユーザ名のロック解除

ロックアウト時間が満了する前、またはロックアウト時間が infinite に設定されている場合でもユーザ名のロックを解除できます。ロックされたユーザ名のロックを解除するには、特権 EXEC モードに設定されているローカル認証サーバ上で、次のコマンドを入力します。

AP# clear radius local-server user *username*

ローカル認証サーバ統計情報の表示

特権 EXEC モードで、次のコマンドを入力して、ローカル認証サーバが収集した統計情報を表示します。

AP# show radius local-server statistics

次の例は、ローカル認証サーバ統計情報を示しています。

```
Successes              : 0           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes              : 0           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
Auto provision success : 0           Auto provision failure : 0
PAC refresh            : 0           Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
nicky                             0         0       0
jones                             0         0       0
jsmith                            0         0       0
```

統計情報の最初のセクションは、ローカル認証サーバからの累積統計情報を示しています。

2 番目のセクションは、ローカル認証サーバを使用する権限を持つ各アクセス ポイント（NAS）の統計情報を表示しています。このセクションの EAP-FAST 統計情報には、次の情報が記録されています。

- Auto provision success：自動的に生成された PAC の数
- Auto provision failure：無効なハンドシェイク パケットが原因で、あるいは無効なユーザ名またはパスワードが原因で生成されなかった PAC の数
- PAC refresh：クライアントによって更新された PAC の数
- Invalid PAC received：受信した PAC のうち、期限切れだったもの、認証サーバで復号化できなかったもの、および認証サーバのデータベースに記録されていないクライアント ユーザ名に割り当てられていたものの合計数

この 3 番目のセクションには、個々のユーザの統計情報が表示されます。ユーザがブロックされていて、ロックアウト時間が infinite に設定されている場合、このユーザの統計行の末尾には *blocked* と表示されます。ロックアウト時間が infinite ではない場合、この行の末尾には *Unblocked in x seconds* と表示されます。

ローカル認証サーバ統計情報を 0 にリセットするには、次の特権 EXEC モード コマンドを使用します。

```
AP# clear radius local-server statistics
```

デバッグ メッセージの使用

ローカル認証サーバに対するデバッグ メッセージの表示を制御するには、特権 EXEC モードで次のコマンドを入力します。

```
AP# debug radius local-server { client | eapfast | error | packets}
```

このデバッグ情報を表示するには、次のコマンド オプションを使用します。

- 失敗したクライアント認証に関連するエラー メッセージを表示するには、**client** オプションを使用します。
- EAP-FAST 認証に関連するエラー メッセージを表示するには、eapfast オプションを使用します。特定のデバッグ情報を選択するには、次のサブオプションを使用します。
  - **encryption**：受信されたパケットおよび送信されたパケットの暗号化と複合化に関する情報が表示されます。
  - **events**：すべての EAP-FAST イベントに関する情報が表示されます。
  - **pac**：PAC の生成や検証など、PAC に関連するイベントの情報が表示されます。
  - **pkts**：EAP-FAST クライアントとの間で送受信されたパケットが表示されます。
- ローカル認証サーバに関連するエラー メッセージを表示するには、**error** オプションを使用します。
- 送受信された RADIUS パケットの内容が表示されるようにするには、**packets** オプションを使用します。

WLAN 認証および暗号化の設定

この章では、WLAN を保護するための認証方式および暗号化方式を設定する方法について説明します。

暗号化には、共有キーまたは個々のクライアント キーを使用します。個々のクライアント キーを使用するほうが確実ですが、その場合、キーの管理が必要になります。キーを管理するには、Wi-Fi Protected Access（WPA）バージョン 1 またはバージョン 2 と、Cisco Centralized Key Management（CCKM）認証済みキー管理による暗号スイートを使用します。

暗号化の堅牢性を確保するには、Wired Equivalent Privacy（WEP）を使用します。WEP 機能には、AES、Temporal Key Integrity Protocol（TKIP）、Message Integrity Check（MIC）、およびブロードキャスト キー ローテーションが含まれます。認証には、共有キー（WEP）、事前共有キー（WPAv1 または WPAv2）、個々のクライアント認証（802.1x/EAP）を使用します。

認証および暗号化メカニズムについて

ラジオ局の受信範囲内にいる人すべてが、局の周波数にチューニングして信号を聞くことができるのと同様に、アクセス ポイントの範囲内にあるすべての無線ネットワーキング デバイスは、アクセス ポイントおよび任意の無線クライアントの無線伝送を受信できます。また、アクセス ポイントは一般に有線インフラストラクチャに接続します。アクセス ポイントの無線信号はアクセス ポイントが展開されている施設の壁を越えて伝送できるため、外部ユーザがアクセス ポイントを介して有線インフラストラクチャにアクセスできる場合があります。したがって、WLAN セキュリティは主に次の 2 つの機能によって確保されます。

- ユーザの認証。有効なユーザだけに、アクセス ポイントを介した通信が許可されるようにします。
- 無線通信の暗号化。傍受者がアクセス ポイントやクライアント通信から捕捉した信号を解読できないようにします。

Cisco Aironet アクセス ポイントでは、SSID が直接アクセス ポイントの無線、または AP 無線インターフェイスに設定された VLAN にマッピングされます。暗号化は、無線レベルで設定されるか（無線インターフェイスに VLAN が定義されていない場合）、（無線インターフェイスに 1 つ以上の VLAN が定義されると同時に）VLAN レベルで設定されます。つまり、特定の無線インターフェイスや特定の VLAN で複数の SSID を有効にする場合は、それらすべての SSID が共通の暗号化方式を共有する必要があります。

認証は SSID レベルで設定されます。SSID ごとの異なる認証メカニズムを使用できます。ただし、SSID は VLAN（または無線インターフェイス）にマッピングされるため、SSID レベルで定義された認証メカニズムが、その SSID の VLAN（または無線）レベルで定義されている暗号化メカニズムと互換性があることを確認する必要があります。

無線（または VLAN）レベルで定義する暗号化には、次のいずれかの方式を使用できます。

- 暗号化なし
- オプションの（40 ビット長または 128 ビット長のキーを使用した）静的 WEP 暗号化。WEP をサポートしているクライアントと、暗号化をサポートしていないクライアントの両方が、SSID に参加できます。
- 必須の（40 ビット長または 128 ビット長のキーを使用した）静的 WEP 暗号化。クライアントは静的 WEP 暗号化をサポートしていなければ、SSID に参加できません。
- 40 ビットまたは 128 ビット暗号のキー管理が有効な WEP 暗号化。ユニキャスト WEP キー ローテーション（認証メカニズムが個々のクライアント キー決定に対応する場合）および/またはブロードキャスト キー ローテーション（認証メカニズムが個々のクライアント キー決定に対応する場合）が使用可能になります。
- 暗号 TKIP、CKIP、CMIC、CKIP-CMIC、または AES（認証メカニズムが個々のクライアント キー決定に対応する場合）
- 2 つまたは 3 つの暗号の組み合わせ。
  このタイプの組み合わせは、SSID のセキュリティ レベルを上げる必要がある一方、弱い暗号化方式しかサポートしていないクライアントも引き続きサポートする必要がある場合に使用します。この場合、クライアントは SSID で許可される最も強力な暗号化メカニズムを使用します。ブロードキャスト キーには、すべてのクライアントでサポートされている暗号化メカニズムを使用します。
  サポートされているすべての暗号化方式のうち、最も強力なのは AES-CCMP で、次に TKIP が続きます。WEP は脆弱な暗号化メカニズムと見なされているため、IEEE 802.11 標準で非推奨となっています。
  たとえば、AES+TKIP+WEP 暗号化を定義するとします。この場合、AES をサポートしているクライアントは、ユニキャスト キーの暗号化に AES を使用します。AES はサポートしていないが、TKIP はサポートしているクライアントにはセルへの参加が許可されます。これらの

クライアントはユニキャスト キーの暗号化に TKIP を使用します。WEP のみをサポートしているクライアントにもセルへの参加が許可されます。これらのクライアントはユニキャスト キーの暗号化に WEP を使用します。セルに AES、TKIP、および WEP クライアントが含まれている場合、ブロードキャスト キーには WEP 暗号化が使用されます（WEP がすべてのクライアントでサポートされる唯一の共通の暗号化方式であるため）。セルに AES と TKIP クライアントが含まれていて、WEP クライアントが含まれていない場合、ブロードキャスト キーには TKIP が使用されます（WEP クライアントがセルに参加すると、ブロードキャスト キーの暗号化は WEP に変更されます）。セルに AES クライアントだけが含まれている場合、ブロードキャスト キーには AES が使用されます（TKIP クライアントがセルに参加すると TKIP に変更され、WEP クライアントがセルに参加すると WEP に変更されます）。

（注）　暗号化メカニズムのサポートは、増分式です。WEP をサポートするクライアントは、TKIP や AES をサポートすることもあれば、サポートしないこともあります。ただし、TKIP をサポートするクライアントは、必ず WEP をサポートします。同様に、AES クライアントは必ず TKIP と WEP をサポートします。

各暗号化メカニズムの詳細については、この章の暗号化モードについての項に記載されています。

暗号化は無線または VLAN レベルで設定されます。認証は SSID レベルで設定されます。次のいずれかの認証方式、あるいはこのうちの複数の認証方式を組み合わせて使用できます。

- Open：認証を行わずにアクセス ポイントにアソシエートできます。
- Shared Key：静的 WEP 認証を使用します。
- Network EAP：LEAP を使用します。

（注）　Open モードと Shared Key モードは、どちらも他のモードと組み合わせて使用できます。たとえば、EAP/802.1x と組み合わせると、アクセス ポイントとのアソシエーションが行われた後に認証が行われます。MAC 認証と組み合わせた場合は、アクセス ポイントとのアソシエーションの最終フェーズで認証が行われます。

各認証メカニズムの詳細については、この章の「認証メカニズムについて」の項を参照してください。

さまざまな認証メカニズムと暗号化メカニズムの組み合わせによって、SSID のセキュリティ スキームが変わってきます。次の表に、サポートされる組み合わせまとめます。

SSID 認証	インターフェイス 暗号化	サポートされるセキュリティ
Open	WEP（オプション）	AP は SSID を Open/Open として宣言し、WEP の明示的サポートをブロードキャストしません。ただし、クライアント コンフィギュレーションが WEP 暗号化および/または WEP 認証に設定されている場合、AP はクライアント アソシエーションも受け入れます。WEP を使用するクライアントでこのモードを使用する場合は、WEP キーを定義する必要があります。

SSID 認証	インターフェイス 暗号化	サポートされるセキュリティ
Open	WEP（必須）	AP は SSID を WEP 対応の SSID として宣言します。クライアント コンフィギュレーションが Open/None、WEP 暗号化および/または WEP 認証に設定されている場合、AP はクライアント アソシエーションを受け入れます。アソシエーション フェーズの完了後、トラフィックをアクセス ポイントを介して転送するには、WEP サポートが必須です。WEP を使用するクライアントでこのモードを使用する場合は、WEP キーを定義する必要があります。
Open + MAC	Open 認証でサポートされるすべてのモード	AP とのクライアント アソシエーションの最終フェーズに、クライアント MAC 認証が追加されます（詳細については、「ネットワークに対する MAC アドレス認証」（P.11-6）を参照してください）。
Open + EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	AP とのクライアント アソシエーションの後に、802.1x/EAP 認証が行われます（サポートされる EAP モードは、LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS および EAP-FAST です）。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。
Open + MAC + EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	アクセス ポイントとのクライアント アソシエーションの最終フェーズにクライアント MAC 認証が追加されます。AP とのクライアント アソシエーションの後、802.1x/EAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。

SSID 認証	インターフェイス暗号化	サポートされるセキュリティ
Open + EAP（オプション）	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	EAP に設定されたクライアントは個々の認証を使用し、個々のキーで暗号化を使用します。セキュリティが設定されていないクライアントも、AP とアソシエートできます。このモードは、より強力なセキュリティへの移行メカニズムとして設計されています。ブロードキャスト キーには、すべてのクライアントでサポートされる共通のセキュリティ メカニズムが使用されます。EAP クライアントと Open クライアントの両方がアソシエートされる場合、ブロードキャスト キーは暗号化されません。
共有認証	WEP（オプション）	AP は SSID を WEP 対応の SSID として宣言します。AP は WEP 認証が設定されたクライアントだけを受け入れます。アソシエーション後の WEP 暗号化はサポートされますが、これはオプションです。
共有認証	WEP（必須）	AP は SSID を WEP 対応の SSID として宣言します。AP は WEP 認証が設定されたクライアントだけを受け入れます。アソシエーション後の WEP 暗号化は必須です。
共有認証 + MAC	共有認証でサポートされるすべてのモード	WEP 認証の後、アソシエーションの最終フェーズで MAC 認証が行われます。
共有認証 + EAP	共有認証でサポートされるすべてのモード	WEP 認証の後、AP との Open アソシエーションが行われます。アソシエーションの後、個々のクライアント EAP 認証と個々のキー生成が行われます。
共有認証 + EAP + MAC	共有認証でサポートされるすべてのモード	WEP 認証の後、アソシエーションの最終フェーズで MAC 認証が行われます。アソシエーションの後、個々のクライアント EAP 認証と個々のキー生成が行われます。
Network EAP	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	AP とのクライアント アソシエーションの後、Cisco LEAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。

SSID 認証	インターフェイス 暗号化	サポートされるセキュリティ
Network EAP + MAC	任意の暗号（WEP 40、WEP 128、TKIP、CKIP、CMIC、CKIP-CMIC、TKIP + WEP 40、TKIP + WEP 128、AES-CCMP、AES-CCMP + TKIP、AES-CCMP + TKIP + WEP 40、AES-CCMP + TKIP + WEP 128）	アクセス ポイントとのクライアント アソシエーションの最終フェーズにクライアント MAC 認証が追加されます。AP とのクライアント アソシエーションの後、LEAP を使用した 802.1x/EAP 認証が行われます。このプロセス中に、個々のクライアント キーが生成されます。複数の暗号が許可される場合、クライアントでサポートされる最も強力な暗号を使用してキーが生成されます。ブロードキャスト キーは、すべてのクライアントでサポートされる暗号を使用してすべてのクライアントに転送されます。
Web 認証	いずれか（Any）	Web 認証は、単独で（他の SSID 認証または暗号化を使用せずに）使用することも、他のいずれかの認証および暗号化方式と組み合わせて使用することもできます。

Open との組み合わせで Network EAP 認証を有効にすることができます（EAP、MAC の組み合わせ（つまり、Network EAP または Network EAP + MAC）、Open、Open + EAP、MAC、EAP + MAC を使用するかどうかは問いません）。Network EAP は LEAP を使用しますが、AP 宣言で LEAP フォーマットのサポートが必要です。この特定の宣言フォーマットをサポートしていないクライアントは、（LEAP または別の EAP メカニズムを使用した）Open モードを使用できます。クライアントは常に、アクセス ポイントでサポートされる最も安全な認証メカニズム、および最も強力な暗号化メカニズムの使用を試みます。ただし、（ブリッジまたはワークグループ ブリッジ モードの）クライアント アクセス ポイントは、クライアント サイドで Network EAP より強力な認証メカニズムを使用するように明示的に設定しない限り、デフォルトで Network EAP を使用します。

SSID を設定する際に、暗号を使用すると、各クライアントの個別のキーを管理できます。このキーの管理方法は、SSID の設定時に定義できます。暗号を使用するようにインターフェイスを設定する場合は、SSID の設定時にキー管理も有効にする必要があります。キー管理は「なし」（セキュリティまたは共有キー セキュリティを使用しない場合）、「必須」（暗号を使用する場合）、または「オプション」（Open とオプション EAP、または共有キーとオプション EAP 認証を使用する場合）に設定できます。各種のキー管理モードの詳細については、この章のキー管理に関する項を参照してください。

暗号化モードについて

暗号化はアクセス ポイントのインターフェイス（VLAN または無線）レベルで定義されて、複数の SSID で共通して使用可能になることから、一般に、暗号化を設定してから、SSID とその認証メカニズムを設定します。

ラジオ局の受信範囲内にいる人すべてが、局の周波数にチューニングして信号を聞くことができるのと同様に、アクセス ポイントの範囲内にあるすべての無線ネットワーキング デバイスは、アクセス ポイントの無線伝送を受信できます。通信の暗号化は、攻撃者に対する第一の防衛ラインであるため、シスコでは、無線ネットワークに完全な暗号化を使用することを推奨しています。

802.11 標準で最初に規定された暗号化メカニズムは WEP（Wired Equivalent Privacy）です。WEP 暗号化は、アクセス ポイントとクライアント デバイス間の通信をスクランブルし、通信機密を維持します。802.11 標準では、シスコと一部の他のベンダーが静的 WEP と規定している暗号化を規定しています。このモードでは、WEP キーがクライアントと AP に静的に定義されます。アクセス ポイントとクライアント デバイスはいずれも同じ WEP キーを使用して、無線信号の暗号化および復号化を行います。WEP キーは、ユニキャストおよびマルチキャストの両方のメッセージを暗号化します。ユニキャスト メッセージは、ネットワーク上の 1 つのデバイスだけに送信されます。マルチキャスト メッセージは、ネットワーク上の複数のデバイスに送信されます。

WEP は 802.11 標準で非推奨となっているレガシー プロトコルです。シスコでは可能な場合は常に、これより強力なプロトコル（AES/CCMP など）を使用することを推奨しています。

SSID の認証メカニズムが 802.1x 認証で Extensible Authentication Protocol（EAP）を使用する場合（および WPAv1 または WPAv2 をサポートしていない場合）は、無線ユーザごとに動的 WEP キーを生成できます。動的な WEP キーは、静的な、つまり変化のない WEP キーより安全性が高くなります。不正侵入者は、同じ WEP キーで暗号化されたパケットが多数送られてくるのを待つだけで、WEP キーを割り出す計算を実行し、そのキーを使ってネットワークに侵入できます。動的な WEP キーは頻繁に変化するため、不正侵入者は計算を実行してキーを割り出すことができなくなります。EAP とその他の認証タイプの詳細は、第 11 章「認証タイプの設定」を参照してください。

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。WPA、WPA2、または CCKM を使用する場合は、暗号スイートを使用する必要があります。WEP 暗号化を使用する場合、WEP 暗号化コマンド（暗号コマンド）を使用して WEP を設定するという選択肢があります。WEP 暗号化コマンドを使用すると、認証や暗号化に静的 WEP キーを使用できます。ただし、このモードでは（802.1x を使用した）ユーザごとのセキュア認証を使用できません。暗号スイートは WEP 暗号化を提供すると同時に、個々のユーザ認証とキー管理も使用できるようにするため、シスコでは、CLI で暗号化モードの暗号コマンドを使用するか、あるいは WEP 暗号化コマンドの代わりに Web ブラウザ インターフェイスで暗号ドロップダウン リストを使用して、WEP を有効にすることを推奨しています。ただし、WEP は IEEE で非推奨となっているプロトコルであるため、シスコではクライアント ドライバが他のより強力なセキュリティ メカニズムをサポートしていない場合に限り、WEP を使用するように推奨しています。推奨されるセキュリティは AES-CCMP です。

無線 LAN 上のデータ トラフィックは、次のセキュリティ機能によって保護されます。

- AES-CCMP：米国立標準技術研究所による *FIPS Publication 197* で定義されている高度暗号化規格（AES）に基づいています。AES-CCMP は、128 ビット、192 ビット、および 256 ビットのキーを使用してデータの暗号化および復号化を行う対称ブロック暗号です。AES-CCMP は、WEP 暗号化よりも優れており IEEE 802.11i 規格で定義されています。

（注） 802.11n 改訂は、暗号化なし、または AES-CCMP 暗号化の実装に依存しています。したがって、802.11n 無線では、暗号化なし、または AES-CCMP を設定して 802.11n レートをサポートする必要があります。

- Wired Equivalent Privacy（WEP）：WEP は 802.11 標準暗号アルゴリズムであり、もともとは有線 LAN で可能なレベルのプライバシーを、無線 LAN で実現できるように設計されたものです。しかし、基本の WEP 構造には不備な点があり、侵入者はそれほど苦労することなく機密性を侵害できます。

- Temporal Key Integrity Protocol（TKIP）：TKIP は、WEP を実行するために構築された従来のハードウェア上で、利用可能な最善のセキュリティを達成するように設計された WEP 周辺の一組のアルゴリズムです。TKIP は WEP に対して、次の 4 つの点を改善しています。
  - weak-key（脆弱キー）攻撃を阻止するための、パケットごとの暗号キー混合機能
  - リプレイ攻撃を検知するための、新しい IV キー作成ロジック
  - パケットの送信元と宛先の入れ替え（ビット フリップ攻撃）や変更のような偽造を検出するための *Michael* と呼ばれる暗号メッセージ完全性チェック（MIC）
  - キー更新をほとんど不要にするための IV 長の拡張
- Cisco Key Integrity Protocol（CKIP）：IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。WPA TKIP は、ほとんどの CKIP 実装を置き換えました。
- Cisco Message Integrity Check（CMIC）：TKIP の *Michael* と同様、シスコのメッセージ完全性チェック メカニズムは、偽造攻撃を検出するように設計されています。CMIC を使用するには Cisco CKIP が必要です。
- ブロードキャスト キー ローテーション（グループ キー更新とも呼ばれる）：ブロードキャスト キー ローテーションにより、アクセス ポイントは最良のランダム グループ キーを生成でき、キー管理可能なクライアントすべてを定期的に更新できるようになります。Wi-Fi Protected Access（WPA）も、グループ キー更新の追加オプションを提供します。WPA の詳細は、「WPA キー管理の使用」（P.11-8）を参照してください。

（注） ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理（動的 WEP（802.1x）、EAP を使用した WPA、または事前共有キーなど）を使用する場合のみサポートされます。

（注） 暗号化は、インターフェイスまたは VLAN レベルで設定され、認証はそれぞれの VLAN またはインターフェイスでサポートする SSID ごとに設定されます。このようにして、暗号化と認証が組み合わされます。暗号化と認証の組み合わせの詳細については、第 11 章「認証タイプの設定」を参照してください。

暗号化モードの設定

暗号化は、VLAN または無線インターフェイス レベルで設定されます。有効にする暗号化が、該当する VLAN または無線インターフェイスにマッピングされている SSID で使用する予定の認証メカニズムと互換性があることを確認してください。暗号化と認証方式の互換性の詳細については、認証および暗号化メカニズムについてを参照してください。

（注） WEP、TKIP、MIC、およびブロードキャスト キー ローテーションは、デフォルトで無効に設定されています。

静的WEP キーの作成

（注）　静的 WEP キーの設定は、静的 WEP を使用するクライアント デバイスをアクセス ポイントがサポートしなければならない場合にだけ必要となります。アクセス ポイントにアソシエートするすべてのクライアント デバイスがキー管理（WPA、CCKM、または 802.1x 認証）を使用する場合は、静的 WEP キーを設定する必要はありません。

特権 EXEC モードから、次の手順に従って、WEP キーを作成し、キーのプロパティを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**0** | **7**] [**transmit-key**]	WEP キーを作成し、そのプロパティを設定します。 • （任意）キーを作成する VLAN を選択します。 • この WEP キーを配置するキー スロットの名前を指定します。VLAN ごとに最大 4 つの WEP キーを割り当てることができます。 • キーを入力し、キーのサイズを 40 ビットか 128 ビットのいずれかに設定します。40 ビット キーには、10 の 16 進数が含まれ、128 ビット キーには、26 の 16 進数が含まれています。 • （任意）このコマンドで入力したキー文字列が暗号化された文字列であるか、プレーン テキスト キーであるかどうかを指定します。プレーン テキスト キーは、Enter キーを押すと暗号化されます。 • （任意）このキーを送信キーとして設定します。スロット 1 のキーは、デフォルトで送信キーとなります。 （注）　静的 WEP を MIC（キー ハッシュ）とともに設定する場合、アクセス ポイントおよびアソシエートされているクライアント デバイスは送信キーとして同じ WEP キーを使用する必要があり、そのキーは、アクセス ポイントとクライアントで同じキー スロットに設定されていなければなりません。 （注）　CMIC を使用した静的 WEP の設定はサポートされていません。 （注）　認証済みキー管理などのセキュリティ機能を使用すると、WEP キーの設定を制限できます。WEP キーに影響を与える機能の一覧は、「WEP キーの制限」（P.10-10）を参照してください。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例は、VLAN 22 のスロット 3 に 128 ビット WEP キーを作成し、そのキーを送信キーとして設定する方法を示します。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-if)# end
```

WEP キーの制限

表 10-1 は、それぞれのセキュリティ設定に基づいた WEP キーの制限の一覧を示しています。

表 10-1　WEP キーの制限

セキュリティ設定	WEP キーの制限
CCKM または WPA 認証済みキー管理	キー スロット 1 に WEP キーを設定できません。
LEAP または EAP 認証	キー スロット 4 に WEP キーを設定できません。
40 ビット WEP による暗号スイート	128 ビット キーを設定できません。
128 ビット WEP による暗号スイート	40 ビット キーを設定できません。
TKIP による暗号スイート	WEP キーを設定できません。
TKIP と 40 ビット WEP、または 128 ビット WEP による暗号スイート	WEP キーをキー スロット 1 と 4 に設定できません。
MIC による静的 WEP	アクセス ポイントとクライアント デバイスは、同じ WEP キーを送信キーとして使用する必要があります。また、このキーは、アクセス ポイントとクライアントの両方で同じキー スロットに設定されている必要があります。
ブロードキャスト キー ローテーション	ブロードキャスト キー ローテーションにより、スロット 2 と 3 のキーが上書きされます。 **(注)** ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理(動的 WEP (802.1x)、EAP を使用した WPA、または事前共有キーなど)を使用する場合のみサポートされます。

WEP キーの設定例

表 10-2 は、アクセス ポイントおよびアソシエートされるデバイスで機能する WEP キーの設定例を示しています。

表 10-2　　WEP キーの設定例

キー スロット	アクセス ポイント		アソシエートされるデバイス	
	送信キー	キー値	送信キー	キー値
1	○	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	○	09876543210987654321fedcba
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

アクセス ポイントの WEP キー 1 は送信キーとして選択されているため、アソシエートされるデバイスの WEP キー 1 も同じ内容に設定する必要があります。アソシエートされるデバイスに設定されている WEP キー 4 は、送信キーとして選択されていないため、アクセス ポイントの WEP キー 4 を設定する必要はありません。

（注） MIC を有効にし、静的な WEP を使用する（いずれの EAP 認証も有効にしない）場合は、アクセス ポイントと通信先のデバイスの両方で、データ送信用に同じ WEP キーを使用する必要があります。たとえば、MIC を有効にしたアクセス ポイントでスロット 1 のキーを送信キーとして使用する場合は、そのアクセス ポイントにアソシエートされるクライアント デバイスでも、同じキーをスロット 1 で使用し、これを送信キーとして選択する必要があります。

暗号スイートの有効化

特権 EXEC モードから、次の手順に従って暗号スイートを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。

	コマンド	目的
ステップ 3	**encryption [vlan** *vlan-id***] mode ciphers {aes-ccm | ckip | ckip-cmic | cmic | tkip | wep128 | wep40}**	必要な保護が含まれる暗号スイートを有効にします。表 10-3 は、設定する認証済みキー管理タイプと一致する暗号スイートを選択するためのガイドラインです。 • （任意）暗号タイプを有効にする VLAN を選択します。 • 必要な暗号オプションを選択します。複数の暗号を選択できます。 **（注）** 2 つまたは 3 つの要素で暗号スイートを有効にすると、各クライアントは、インターフェイスで有効にされていて、そのクライアントがサポートする最も強力な暗号化メカニズムを使用します。ブロードキャスト キーは、すべてのクライアントがサポートする要素を使用します。詳細については、認証および暗号化メカニズムについてを参照してください。 **（注）** **ckip** を設定する場合は、Aironet 拡張機能も有効にする必要があります。Aironet 拡張機能を有効にするコマンドは、**dot11 extension aironet** です。 **（注）** 静的 WEP は、**encryption mode wep** コマンドを使用して設定することもできます。ただし、**encryption mode wep** コマンドは、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がキー管理に対応していない場合に限り使用してください。**encryption mode wep** コマンドの詳細は、『*Cisco IOS Command Reference for Cisco Access Points and Bridges*』を参照してください。 **（注）** SSID に（**TKIP + WEP 128** でも **TKIP + WEP 40** でもない）暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。 **（注）** 暗号化モード **TKIP + WEP 128** または **TKIP + WEP 40** を設定するには、WPA キー管理をオプションとして設定する必要があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

暗号スイートを無効にするには、encryption コマンドの **no** 形式を使用します。

WPA または CCKM に一致する暗号スイート

WPA または CCKM 認証済みキー管理を使用するようにアクセス ポイントを設定する場合は、そのタイプの認証キー管理と互換性のある暗号スイートを選択する必要があります。表 10-3 は、WPA および CCKM と互換性のある暗号スイートを示しています。

表 10-3　WPA および CCKM と互換性のある暗号スイート

認証済みキー管理のタイプ	互換性のある暗号スイート
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode aes
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode ciphers eas **（注）** WPA がオプションとして設定されている場合、encryption mode ciphers tkip wep128 および tkip wep-40 だけを使用できます。

（注） キー管理として WPA および CCKM を使用している場合は、tkip および aes の暗号方式だけがサポートされます。キー管理として CCKM だけを使用している場合は、ckip、cmic、ckip-cmic、tkip、wep、および aes の各暗号方式がサポートされます。

（注） SSID に（**TKIP + WEP 128** でも **TKIP + WEP 40** でもない）暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。

WPA の詳細、および認証済みキー管理を設定する手順については、「「WPA キー管理の使用」（P.11-8）」を参照してください。

（注） Wi-Fi 認定アクセス ポイントは、WPA/TKIP 設定をサポートしなくなりました。後方互換性を確保して以前の TKIP 専用デバイスのアソシエーションを可能にするために、TKIP は WPA2/AES との組み合わせでのみ使用できます。WPA バージョン 1 オプションは認証キー管理の wpa cli から削除されたため、このインターフェイスでの TKIP の設定はサポートされません。

ブロードキャスト キー ローテーションの有効化と無効化

ブロードキャスト キー ローテーションは、デフォルトでは無効になっています。

（注）　ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理（動的 WEP（802.1x）、EAP を使用した WPA、または事前共有キーなど）を使用する場合のみサポートされます。

特権 EXEC モードから、次の手順に従ってブロードキャスト キー ローテーションを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 3	**broadcast-key change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	ブロードキャスト キー ローテーションを有効にします。 • ブロードキャスト キーのローテーションの間隔を秒単位で入力します。 • （任意）ブロードキャスト キー ローテーションを有効にする VLAN を入力します。 • （任意）WPA 認証済みキー管理を有効にすると、アクセス ポイントが WPA グループ キーを変更および配布するための条件を追加指定できます。 – Membership termination：アクセス ポイントは、任意の認証済みクライアント デバイスがアクセス ポイントからアソシエーションを解除されたときに、新しいグループ キーを生成、配布します。この機能はアソシエートされたクライアントのグループ キーの機密性を保護します。しかし、ネットワーク上のクライアントが頻繁にローミングする場合、オーバーヘッドが生じる可能性があります。 – Capability change：アクセス ポイントは、最後の非キー管理（静的 WEP）クライアントがアソシエーションを解除されたときに、動的グループ キーを生成、配布します。また、最初の非キー管理（静的 WEP）クライアントが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、アクセス ポイントにアソシエートしている静的 WEP クライアントが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。 認証済みキー管理を有効にする方法の詳細については、第 11 章「認証タイプの設定」を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ブロードキャスト キー ローテーションを無効にするには、encryption コマンドの **no** 形式を使用します。

次の例は、VLAN 22 でブロードキャスト キー ローテーションを有効にし、ローテーション間隔を 300 秒に設定しています。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-if)# end
```

認証タイプの設定

この章では、アクセス ポイントに認証タイプを設定する方法について説明します。

認証タイプの概要

この項ではアクセス ポイントに設定できる認証タイプについて詳しく説明します。認証タイプはアクセス ポイントに設定する Service Set Identifier（SSID; サービス セット ID）に関連付けられます。認証タイプが関連付けられた SSID は、有効な暗号化メカニズムが設定された VLAN または無線インターフェイスに関連付けられます。したがって、SSID に設定する認証方式が、SSID が関連付けられている VLAN または無線インターフェイスに設定されている暗号化方式と互換性を持っていることを確認してください。

詳細については、第 10 章「認証および暗号化メカニズムについて」の項を参照してください。同じアクセス ポイントで異なるタイプのクライアント デバイスを使用する場合は、複数の SSID を設定します。複数の SSID の設定手順の詳細は、第 7 章「複数の SSID の設定」を参照してください。

無線クライアント デバイスがアクセス ポイントを介してネットワークで通信を行うには、Open または Shared キー認証を使用してアクセス ポイントから認証を得る必要があります。最大限のセキュリティを確保するには、MAC アドレス認証または EAP 認証を使用して、ネットワークに対してクライアント デバイスを認証する必要もあります。MAC アドレス認証と EAP 認証は、いずれもネットワーク上の認証サーバに依存します。

認証サーバは AP に設定することも、外部サーバに設定することもできます。クライアント認証プロセスは、次のように設定できます。

1. クライアントの認証は、アクセス ポイントに対して行うことができます（公開キーまたは共有キーを使用）。
2. アソシエーション フェーズでは、オプションで、クライアントの MAC アドレスを使用してクライアントを認証できます。
3. AP とのアソシエーションが完了した後は、オプションで、RADIUS サーバに対してクライアントを認証できます。
4. 個々のクライアント キーの生成および管理には、EAP/802.1x. EAP/802.1x メカニズムを使用できます。

（注） デフォルトでは、アクセス ポイントは service-type 属性を authenticate-only に設定した再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、authenticate-only の service-type 属性をサポートしていないものがあります。ユーザの要件に応じて、service-type 属性を **dot11 aaa authentication attributes service-type login-user** または **dot11 aaa authentication attributes service-type framed-user** に設定してください。デフォルトでは、アクセス要求に応じてサービス タイプ「login」が送信されます。

アクセス ポイントは、複数の認証メカニズム（タイプ）を同時に使用することができます。次の項でそれぞれの認証タイプについて説明します。

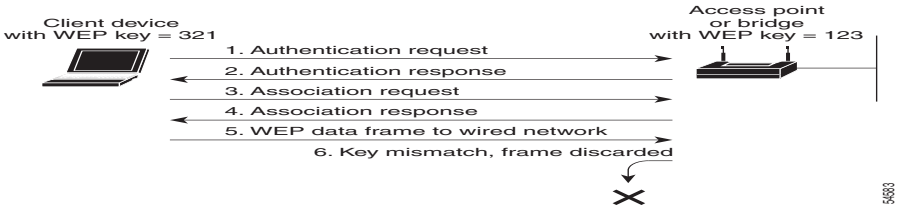
アクセス ポイントに対する Open 認証

Open 認証では、すべてのデバイスに認証およびアクセス ポイントとの通信の試みを許可します。Open 認証を使用すると、すべてのワイヤレス デバイスをアクセス ポイントで認証できます。Open 認証はネットワーク上の RADIUS サーバに依存しません。

Open 認証と WEP 暗号化を使用するシナリオでは、クライアントと AP の WEP が一致しなくても認証は成功します。Open 認証が完了した後は、クライアントはデータ（DHCP 要求を含む）を送信できません。ただし、Open 認証を使用し、暗号化を使用しない場合、ワイヤレス クライアントはアソシエーション フェーズが完了した直後からデータを送信できます。

図 11-1 は、認証を試みるデバイスと、Open 認証を使用しているアクセス ポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセス ポイントのキーと一致しないため、認証はできても、データを転送できません。

図 11-1　　Open 認証のシーケンス



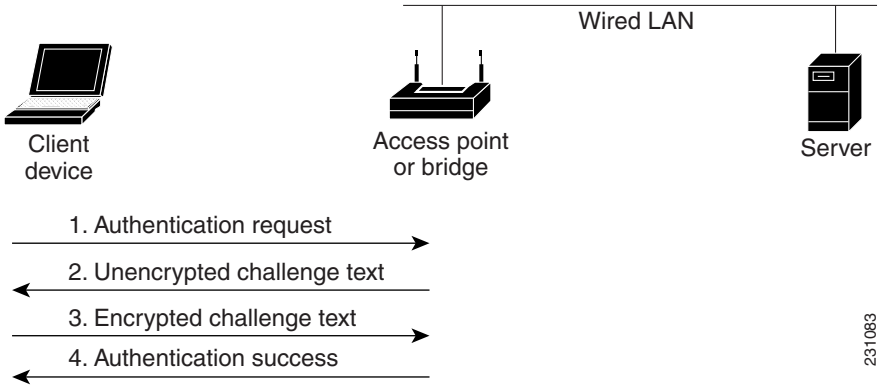
アクセス ポイントに対する WEP Shared Key 認証

シスコでは、802.11 標準で規定されている WEP 認証に準拠するために、Shared Key 認証を提供しています。ただし、Shared Key のセキュリティ上の欠点により、WEP は非推奨となっています。IEEE およびシスコでは、WEP 認証を使用しないよう推奨しています。

Shared Key 認証では、アクセス ポイントが、アクセス ポイントとの通信を試みるすべてのデバイスに、暗号化されていない身元証明要求テキスト ストリングを送信します。認証を求めるデバイスは身元証明要求テキストを暗号化して、アクセス ポイントに返送します。身元証明要求テキストが正しく暗号化されていれば、アクセス ポイントはそのデバイスに認証を許可します。暗号化されていない身元証明要求も暗号化された身元証明要求もモニタできます。しかしそのために、アクセス ポイントは、暗号化前のテキストと暗号化後のテキストを比較して WEP キーを計算する不正侵入者の攻撃に対し、無防備な状態になります。このような弱点により、Shared Key 認証は Open 認証よりも安全性が劣る場合があります。Open 認証と同様に、Shared Key 認証ではネットワーク上の RADIUS サーバは使用されません。

図 11-2 は、認証を試みるデバイスと、Shared Key 認証を使用しているアクセス ポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセス ポイントのキーと一致しているため、認証を受けて通信できます。

図 11-2　Shared Key 認証のシーケンス



ネットワークに対する EAP 認証

この認証タイプは、無線ネットワークに最高レベルのセキュリティを提供します。拡張認証プロトコル（EAP）を使用して EAP 対応の RADIUS サーバと対話することにより、アクセス ポイントは、ワイヤレス クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト キーを派生できるよう支援します。RADIUS サーバはこのキーをアクセス ポイントに送ります。アクセス ポイントはこのキーを、クライアントに対して送受信するすべてのユニキャスト データ信号に使用します。また、アクセス ポイントは、クライアントのユニキャスト キーを使用してブロードキャスト キーを暗号化し、その暗号化したブロードキャスト キーをクライアントに送信します。

このキーは、基礎となるセキュリティ フレームワーク（動的 WEP、WPA または WPA 2 による 802.1X）に応じて、次のように使用されます。

- WEP の場合：アクセス ポイントはこのキーを、クライアントとの間で送受信するすべてのユニキャスト データ信号に直接使用します。
- WPAv1/v2 の場合：このキーは、クライアントとの間で送受信するすべてのユニキャスト データ信号に使用するユニキャスト キーを派生させるために使用されます。

アクセス ポイントとクライアント デバイスで EAP を有効にすると、ネットワークに対する認証は、図 11-3 に示す手順で実行されます。

図 11-3　EAP 認証のシーケンス

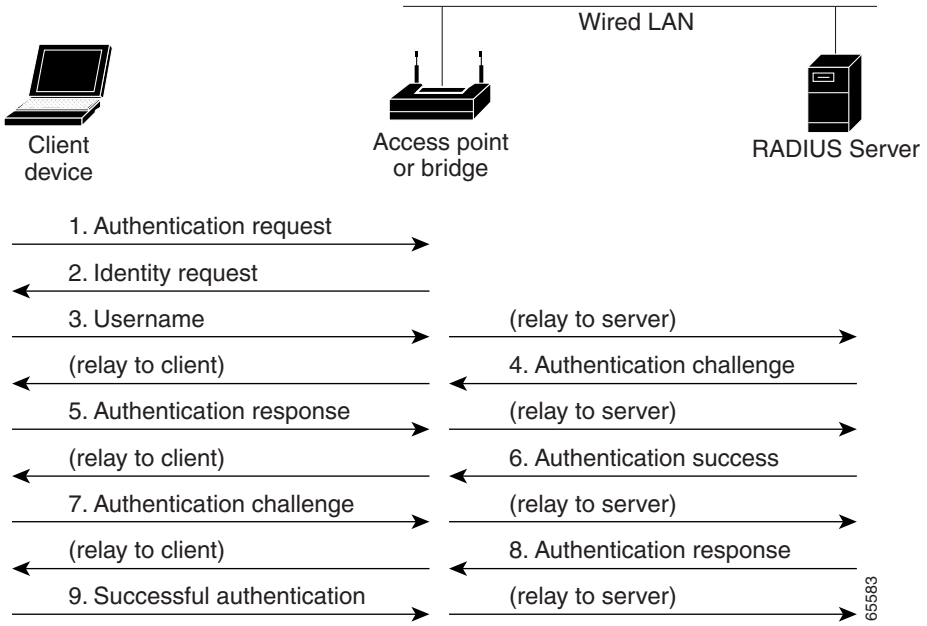


図 11-3 の手順 1 ～ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザまたはマシンによって提供されたクレデンシャルを一方向で暗号化して、認証身元証明要求に対する応答を生成し、その応答を RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が完了すると、RADIUS サーバとクライアントは、クライアントに固有の適切なレベルのネットワーク アクセスを提供する WEP キーまたは Pairwise Master Key（PMK）を決定します。これにより、有線のスイッチド セグメントのセキュリティ レベルは、デスクトップのレベルに近づきます。クライアントはこのキーをロードして、ログイン セッションでの使用に備えます。

ログイン セッション中に、RADIUS サーバは WEP キー（または WPAv1/v2 Pairwise Master Key）を暗号化し、有線 LAN 経由でアクセス ポイントに送信します。AP はこのキーを使用してブロードキャスト キーを暗号化し、暗号化後のブロードキャスト キーをクライアントに送信します。クライアントはこのブロードキャスト キーを同一のユニキャスト キーを使用して復号化します。クライアントとアクセス ポイントは暗号化を有効にし、ユニキャスト キーとブロードキャスト キーを残りのセッションの間、すべての通信に対して使用します。

EAP 認証には複数のタイプがありますが、アクセス ポイントはどのタイプについても同じように機能します。つまり、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。アクセス ポイントで EAP を設定する方法の詳細は、「SSID への認証タイプの割り当て」（P.11-10）を参照してください。

（注） EAP 認証を使用する場合は、Open 認証または Shared Key 認証を選択できますが、この選択は必須ではありません。EAP 認証は、アクセス ポイントとネットワークの両方に対する認証を制御します。

ネットワークに対する MAC アドレス認証

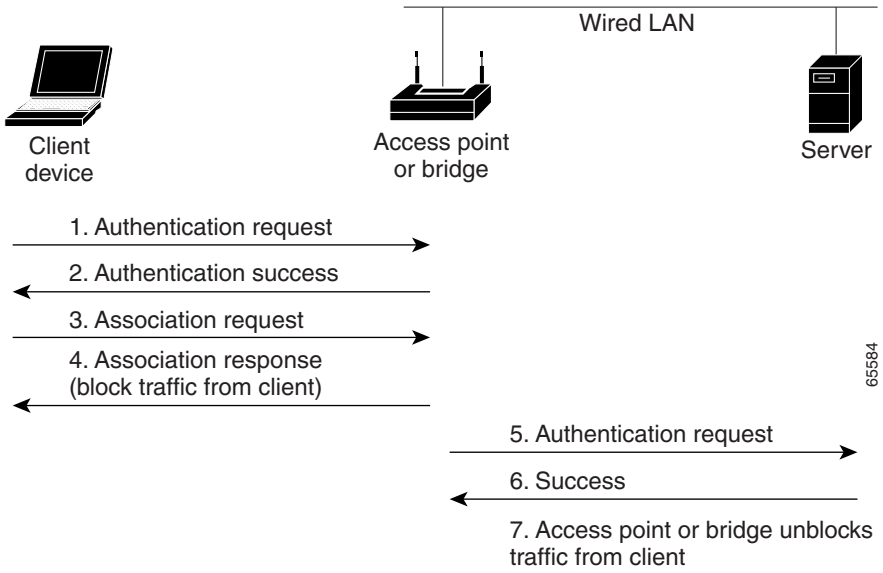
アクセス ポイントは、無線クライアント デバイスの MAC アドレスをネットワーク上の RADIUS サーバに中継します。サーバはそのアドレスを、許可される MAC アドレスのリストと照合します。MAC アドレスは不正侵入者でも偽造できるため、MAC ベースの認証は EAP 認証より安全性が劣ります。ただし、EAP 機能を持たないクライアント デバイスにとって、MAC ベースの認証は 1 つの代替認証方式となります。MAC ベースの認証の有効化の詳細は、「SSID への認証タイプの割り当て」(P.11-10)を参照してください。

ヒント　ネットワークに RADIUS サーバがない場合は、許可される MAC アドレスのリストをアクセス ポイントの [Advanced Security: MAC Address Authentication] ページで作成できます。このリストにない MAC アドレスを持つデバイスは、認証されません。

ヒント　無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。この機能を有効にする手順の詳細は、「MAC 認証キャッシングの設定」(P.11-16)を参照してください。

図 11-4 は、MAC ベースの認証のシーケンスを示しています。

図 11-4　MAC ベースの認証のシーケンス



MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ

MAC ベースの認証と EAP 認証を組み合わせてクライアント デバイスを認証するように、アクセス ポイントを設定できます。この機能を有効にした場合、まず、802.11 Open 認証を使用してアクセス ポイントにアソシエートするクライアント デバイスが MAC 認証を行います。MAC 認証が成功すると、クライアント デバイスはネットワークに接続されます。MAC 認証が失敗した場合、EAP 認証を行います。このような認証の組み合わせを設定する方法の詳細は、「SSID への認証タイプの割り当て」(P.11-10)を参照してください。

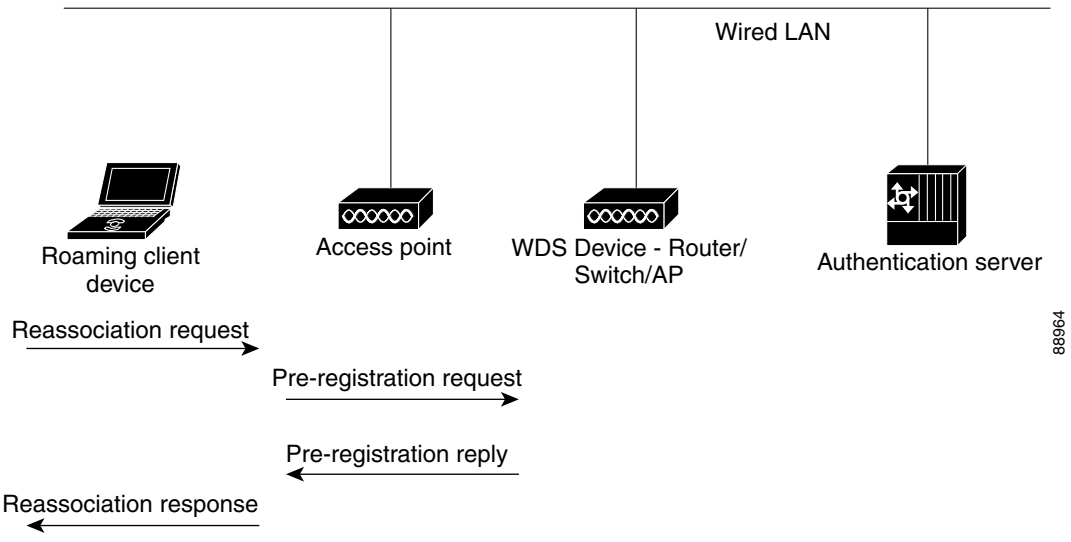
認証されたクライアントの CCKM の利用

Cisco Centralized Key Management（CCKM）を使うと、認証されたクライアント デバイスは、1 つのアクセス ポイントから別のアクセス ポイントへ、再アソシエーションの際にほとんど遅延することなくローミングできます。ネットワーク上のアクセス ポイントは、Wireless Domain Service（WDS; 無線ドメイン サービス）を提供し、サブネット上の CCKM 対応クライアント デバイスに対してセキュリティ クレデンシャルのキャッシュを生成します。WDS アクセス ポイントのクレデンシャルのキャッシュは、CCKM 対応クライアント デバイスが新しいアクセス ポイントにローミングする際、再アソシエーションに必要な時間を大幅に短縮します。クライアント デバイスがローミングすると、WDS アクセス ポイントがクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送し、再アソシエーション プロセスが短縮されて、ローミングするクライアントと新しいアクセス ポイント間での 2 つのパケット交換だけになります。ローミングするクライアントは非常にすばやく再アソシエートするため、音声やその他の時間に敏感なアプリケーションで、知覚できるほどの遅延は生じません。アクセス ポイントで CCKM を有効にする方法の詳細は、「SSID への認証タイプの割り当て」(P.11-10)を参照してください。無線 LAN 上にある WDS アクセス ポイントの設定の詳細は、「アクセス ポイントを潜在的な WDS デバイスとして設定する」(P.12-7)を参照してください。

（注）　RADIUS サーバによる VLAN 割り当て機能は、CCKM を利用した SSID グループのクライアント デバイスに対してはサポートされません。

図 11-5 は、CCKM を使用した再アソシエーション プロセスを示しています。

図 11-5　CCKM を使用したクライアント再アソシエーション



WPA キー管理の使用

WPAv1 は、802.11i 改訂の初期ドラフトに基づく Wi-Fi Alliance 認定です。WPAv1 ではデータ保護に TKIP（Temporal Key Integrity Protocol）を使用します。WPAv2 は、2004 年に発行された 802.11i の最終改訂に基づく Wi-Fi Alliance 認定です。WPAv2 では、AES（Advanced Encryption Standard）と Counter-Mode Cipher Block Chaining（CBC）Message Authentication Code（MAC）プロトコルを使用します。WPAv1 および WPAv2 はいずれも、ホーム タイプの導入には事前共有キー（PSK）を使用した認証を許可し、企業タイプの導入での認証キー管理には 802.1X の使用を許可します。

（注）　WPA では、TKIP の使用を推奨し、AES の使用を許可しています。WPA2 では、AES-CCMP の使用を推奨し、後方互換性を確保するために TKIP の使用を許可しています。シスコおよび Wi-Fi Alliance では、AES と WPAv1 または TKIP と WPAv2 を使用しないよう推奨しています。最も強力なセキュリティは、WPAv2 と AES-CCMP を使用することにより実現できます。クライアントが AES-CCMP で WPAv2 をサポートしていないネットワークでは、WPAv1 と TKIP を使用できます。

クライアントと認証サーバは、WPA（WPAv1 または WPAv2）キー管理を使用して EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

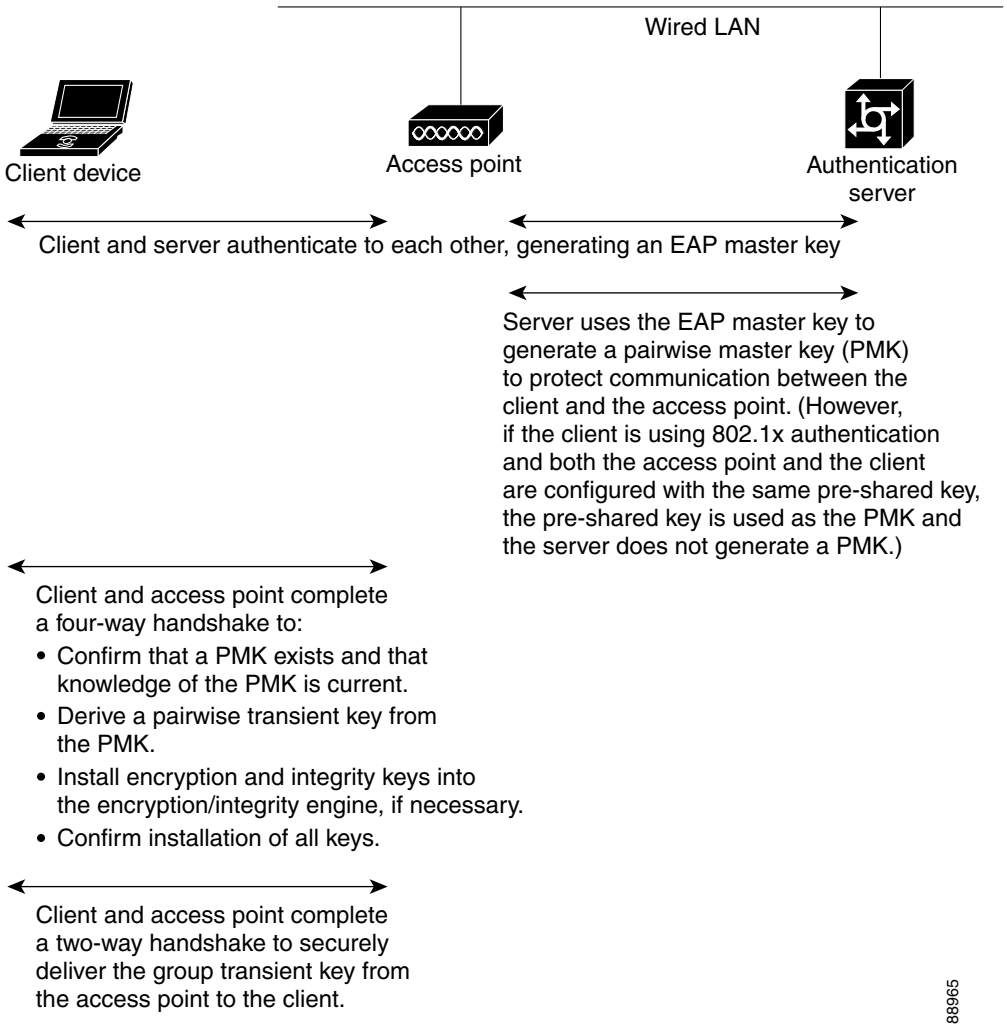
WPA キー管理は、WPA および WPA-Pre-Shared Key（WPA-PSK）の相互に排他的な 2 つの管理タイプをサポートしています。クライアントと認証サーバは、WPA を使用してキーを管理し、EAP 認証方式で相互認証を行い、Pairwise Master Key（PMK）を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセス ポイントに渡します。ただし、そのためには、WPA-PSK を使用してクライアントとアクセス ポイントの両方で事前共有キーを設定し、事前共有キーが PMK として使用されるように設定してください。

（注）　WPA 情報エレメントでアドバタイズされる（さらに 802.11 でのアソシエーション中に決定される）ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセス ポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は許可されていません。このような場合、クライアント デバイスと無線 LAN とのアソシエーションが解除されてしまいます。

WPA キー管理をアクセス ポイントで設定する方法の詳細は、「SSID への認証タイプの割り当て」（P.11-10）を参照してください。

図 11-6 は、WPA キー管理プロセスを示しています。

図 11-6　WPA キー管理プロセス



認証タイプの設定

この項では、認証タイプを設定する方法について説明します。設定タイプはアクセス ポイントの SSID に割り当てます。複数の SSID の設定の詳細は、「複数の SSID の設定」(P.7-3)を参照してください。ここでは、次の内容について説明します。

SSID への認証タイプの割り当て

設定する SSID は、VLAN または無線インターフェイスにマッピングされます。したがって、SSID に定義する認証タイプが、SSID に関連付ける VLAN または無線インターフェイスに定義されている暗号化方式と互換性を持つことを確認してください。詳細については、第 10 章「認証および暗号化メカニズムについて」を参照してください。

特権 EXEC モードから、次の手順に従って SSID に認証タイプを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 一部のクライアントでは、SSID 文字列での特殊文字の使用をサポートしていません。シスコでは、SSID 文字列では文字 !、#、;、+、\、/、" を使用しないよう推奨しています。

	コマンド	目的
ステップ 3	**authentication open** [**mac-address** *list-name* [**alternate**]] [[**optional**] **eap** *list-name*]	(任意)この SSID の認証タイプを Open に設定します。Open 認証では、すべてのデバイスに認証およびアクセス ポイントとの通信の試みを許可します。 • (任意)SSID の認証タイプを MAC アドレス認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に MAC アドレス認証の実行を強制します。*list-name* には、認証方式リストを指定します。 • クライアント デバイスが MAC 認証か EAP 認証を使用してネットワークに接続するのを許可する場合は、**alternate** キーワードを使用します。いずれかの認証を得たクライアントはネットワークとの接続を許可されます。 • (任意)SSID の認証タイプを EAP 認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に EAP 認証の実行を強制します。*list-name* には、認証方式リストを指定します。 クライアント デバイスが Open 認証か EAP 認証を使用してアソシエートおよび認証されるのを許可する場合は、**optional** キーワードを使用します。この設定は、特殊なクライアント アクセシビリティを必要とするサービス プロバイダーが主に使用します。 **(注)** EAP 認証が設定されたアクセス ポイントは、アソシエートするすべてのクライアント デバイスに対して EAP 認証の実行を強制します。EAP を使用しないクライアント デバイスはアクセス ポイントを使用できません。
ステップ 4	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	(任意)SSID の認証タイプを Shared Key に設定します。 **(注)** WEP Shared Key にはセキュリティ上の欠陥があるため、使用しないことを推奨します。 • (任意)SSID の認証タイプを MAC アドレス認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。 • (任意)SSID の認証タイプを EAP 認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。このモードは、EAP に段階的に移行するネットワーク向けに設計されています。EAP をサポートするクライアントは個々のクライアント認証と個々のクライアント キー管理を使用する一方、静的 WEP のみをサポートするクライアントには、静的 WEP を使用したアソシエーションが許可されます。

	コマンド	目的
ステップ 5	**authentication network-eap** *list-name* [**mac-address** *list-name*]	(任意)SSID の認証タイプを Network-EAP に設定します。拡張認証プロトコル(EAP)を使用して、Cisco LEAP をサポートする EAP 互換の RADIUS サーバと対話することにより、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを派生できるよう支援します。 • (任意)SSID の認証タイプを MAC アドレス認証を使用する Network-EAP に設定します。アクセス ポイントにアソシエートするすべてのクライアント デバイスは、MAC アドレス認証の実行が要求されます。list-name には、認証方式リストを指定します。

	コマンド	目的
ステップ 6	**authentication key-management** { [**wpa** [**version** *versionnumber*]] | [**cckm**] } [**optional**]	(任意)SSID の認証タイプを WPA または CCKM、あるいはその両方に設定します。**optional** キーワードを指定すると、WPA(WPAv1 または WPAv2)および CCKM クライアント以外のクライアント デバイスもこの SSID を使用できます。**optional** キーワードを指定しない場合、この SSID を使用できるのは WPA(WPAv1 または WPAv2)または CCKM クライアント デバイスだけになります。 SSID で CCKM を有効にするには、EAP 認証(EAP および/または Network EAP による Open 認証)形式も有効にする必要があります。SSID で CCKM と EAP を有効にすると、LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS、および EAP-FAST を使用するクライアント デバイスは、SSID を使用して認証を行うため、CCKM を使用した高速ローミングによるメリットがもたらされます。 (WPAv1 または WPAv2 による)SSID の WPA キー管理を有効にするには、(さらに MAC 認証を使用するかどうかに関係なく)EAP または Network EAP あるいはその両方による Open 認証も有効にする必要があります。この場合、個々のクライアント認証は EAP を使用して行われ、個々のクライアント Pairwise Master Key(PMK)が定義されます。あるいは、Open 認証を有効にして、WPA 事前共有キーを定義することもできます。この場合、AP およびワイヤレス クライアントは事前共有キーを Pairwise Master Key(PMK)として使用します。 **(注)** CLI から SSID に対して WPA と CCKM の両方を有効にする場合、最初に WPA を入力し、次に CCKM を入力する必要があります(ただし、Web UI では、単純に両方のオプションをオンにします)。WPA ではどのクライアントも認証を試行できますが、CCKM では音声クライアントだけが認証を試行できます。 **(注)** CCKM または WPA を有効にするには、SSID の VLAN に対する暗号化モードを、いずれかの暗号スイート オプションに設定する必要があります。VLAN 暗号化モードの設定方法の詳細は、第 10 章「暗号化モードの設定」を参照してください。 **(注)** 事前共有キーなしで SSID の WPA を有効にすると、キー管理タイプは WPA になります。事前共有キーを設定して SSID の WPA を有効にすると、キー管理タイプは WPA-PSK になります。事前共有キーの設定方法の詳細は、追加の WPA の設定を参照してください。 CCKM およびサブネット コンテキスト マネージャを使うように無線 LAN を設定する方法の詳細については第 12 章「その他のサービスの設定」を参照してください。 (任意)WPA を使用する場合は、サポートする WPA のバージョン(WPAv1 または WPAv2)を指定できます。

	コマンド	目的
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

SSID を無効にする場合、または SSID 機能を無効にする場合は、SSID コマンドの **no** 形式を使用します。

次の例では、SSID *batman* の認証タイプを、CCKM 認証済みキー管理を使用した Network-EAP に設定します。batman SSID を使用するクライアント デバイスは、adam サーバ リストを使って認証します。認証後、CCKM 対応クライアントは CCKM を使って迅速に再アソシエートできます。

```
ap1200# configure terminal
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

レガシー WEP SSID の WPA 移行モードの設定

WPA 移行モードは、レガシー WEP クライアント タイプをサポートする必要がある一方、よりセキュアな認証および暗号化を使用できるようにするための SSID 専用のモードです。この特定のモードでは、次のタイプのクライアント デバイスを使用できます。

- TKIP と認証済みキー管理に対応した WPA クライアント
- 認証済みキー管理には対応しているが TKIP には対応していない 802.1X-2001 クライアント（従来の LEAP クライアント、TLS を使うクライアントなど）
- TKIP にも認証済みキー管理にも対応してない静的 WEP クライアント

これら 3 つのタイプすべてのクライアントが同じ SSID を使用してアソシエートする場合、SSID 用のマルチキャスト暗号スイートは WEP でなければなりません。最初の 2 つのタイプのクライアントだけが同じ SSID を使用する場合、マルチキャスト キーは動的でもかまいませんが、静的 WEP クライアントが SSID を使用する場合、キーは静的でなければなりません。アクセス ポイントは自動的に静的グループ キーおよび動的グループ キー間を切り替えて、アソシエートされているクライアント デバイスに対応することができます。同じ SSID で 3 つのすべてのタイプのクライアントをサポートするには、キー スロット 2 または 3 に静的キーを設定する必要があります。

WPA 移行モードに SSID を設定するには、次の設定を行います。

- WPA（オプション）
- TKIP および 40 ビットまたは 128 ビット WEP を含む暗号スイート
- キー スロット 2 または 3 内の静的 WEP キー

次の例では、WPA 移行モードに移行するために SSID を設定します。

```
ap1200# configure terminal
ap1200(config-if)# ssid migrate
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config)# interface dot11radio 0
```

```
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# end
```

追加の WPA の設定

2 つのオプションの設定を使ってアクセス ポイントに事前共有キーを設定し、グループ キーの更新頻度を調整します。

事前共有キーの設定

8021X/EAP ベース認証を使用できないワイヤレス LAN 上の WPA（WPAv1 または WPAv2）をサポートするには、アクセス ポイント上に事前共有キーを設定する必要があります。事前共有キーを ASCII 文字または 16 進数として入力できます。キーを ASCII 文字として入力する場合は、8 ～ 63 文字を入力します。アクセス ポイントはこのキーを、『*Password-based Cryptography Standard*（RFC2898）』に記載されているプロセスを使用して展開します。キーを 16 進数として入力する場合は、64 桁の 16 進数を入力する必要があります。

グループ キー更新の設定

WPA プロセスの最後の段階で、アクセス ポイントは認証されたクライアント デバイスにグループ キーを配布します。次のオプションの設定を使って、クライアントのアソシエーションとアソシエーション解除をベースにして、グループ キーを変更、配布するようにアクセス ポイントを設定できます。

- Membership-termination：アクセス ポイントは、任意の認証されたデバイスがアクセス ポイントからアソシエーションを解除するときに、新しいグループ キーを生成、配布します。この機能は、アソシエートされているデバイスに対してグループ キーを秘匿しますが、ネットワーク上のクライアントがアクセス ポイント間を頻繁にローミングする場合、オーバーヘッド トラフィックを生む可能性があります。
- 機能の変更：セルのクライアント機能が変更されると、アクセス ポイントは動的グループ キーを生成して配布します。たとえば、AES、TKIP、および WEP を許可するセル内に、現在 AES クライアントだけが含まれている場合、ブロードキャスト キーは AES を使用します。アクセス ポイントは、このセルに初めて TKIP クライアントが参加すると TKIP を使用して新しいブロードキャスト キーを生成し、初めて WEP クライアントが参加すると新しいブロードキャスト キーをブロードキャスト キーを生成します。対称的に、アクセス ポイントは最後の WEP クライアントがセルを離れると新しいブロードキャスト キーを生成します。その時点ですべてのクライアントが AES をサポートしている場合、新しいブロードキャスト キーでは AES が使用されます。一部のクライアントが TKIP を使用し、その他のクライアントが AES を使用する場合（AES クライアントも TKIP をサポートします）、新しいブロードキャスト キーでは TKIP が使用されます。最後の TKIP クライアントがセルを離れ、セル内に AES クライアントだけが残されると、アクセス ポイントは AES を使用して新しいブロードキャスト キーを生成します。

特権 EXEC モードから、次の手順に従って、WPA 事前共有キーとグループ キー更新オプションを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ssid** *ssid-string*	SSID の SSID コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	クライアント デバイス用の事前共有キーを、静的 WEP キーも利用する WPA を使って入力します。 PSK 認証で WPAv1 または WPAv2 を使用するクライアント デバイスの事前共有キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合、アクセス ポイントでキーが拡張されるように最低 8 文字の英数字または記号を入力する必要があります。ASCII 文字は 63 文字まで入力できます。
ステップ 4	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 5	**ssid** *ssid-string*	ステップ 2 で定義した SSID を入力して、選択した無線インターフェイスに SSID を割り当てます。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**broadcast-key** [**vlan** *vlan-id*] { **change** *seconds* } [**membership-termination**] [**capability-change**]	**broadcast key rotation** コマンドを使用して、WPA グループ キーの追加の更新を設定します。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例は、WPA および静的 WEP を使用するクライアント用の事前共有キーを、グループ キー更新オプションとともに設定する方法を示しています。

```
ap# configure terminal
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

MAC 認証キャッシングの設定

無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。クライアント デバイスが認証サーバに対する MAC 認証を実行すると、アクセス ポイントがクライアントの MAC アドレスをキャッシュに追加します。

特権 EXEC モードから、次の手順に従って MAC 認証キャッシングを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 aaa authentication mac-authen filter-cache** [**timeout** *seconds*]	アクセス ポイントでの MAC 認証キャッシングを有効にします。 **timeout** オプションを使用して、キャッシュ内の MAC アドレスのタイムアウト値を設定します。値を 30 ～ 65555 秒の範囲で入力します。デフォルト値は 1800（30 分）です。タイムアウト値を入力すると、MAC 認証キャッシングが自動的に有効になります。
ステップ 3	**exit**	特権 EXEC モードに戻ります。
ステップ 4	**show dot11 aaa authentication mac-authen filter-cache** [*address*]	MAC 認証キャッシュ内のエントリを表示します。特定のクライアントのエントリを表示するには、クライアントの MAC アドレスを追加します。
ステップ 5	**clear dot11 aaa authentication mac-authen filter-cache** [*address*]	キャッシュ内のすべてのエントリをクリアします。キャッシュから特定のクライアントをクリアするには、クライアントの MAC アドレスを追加します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例は、タイムアウトを 1 時間に設定して MAC 認証キャッシングを有効にする方法を示しています。

```
ap# configure terminal
ap(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
ap(config)# end
```

MAC 認証キャッシングを無効にするには、**no** 形式の **dot11 aaa authentication mac-authen filter-cache** コマンドを使用します。次に例を示します。

```
no dot11 aaa authentication mac-authen filter-cache
```

または

```
no wlccp wds aaa authentication mac-authen filter-cache
```

認証のホールドオフ、タイムアウト、間隔の設定

特権 EXEC モードから、次の手順に従って、アクセス ポイントを介して認証を行うクライアント デバイスにホールドオフ時間、再認証間隔、認証タイムアウトを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 holdoff-time** *seconds*	クライアント デバイスが認証失敗の後に次の認証を試みるまでに待機する時間を、秒数で入力します。ホールドオフ期間は、クライアントがログインに 3 回失敗したとき、つまりアクセス ポイントからの認証要求に 3 回応答できなかったときに開始されます。値を 1 ～ 65555 秒の範囲で入力します。
ステップ 3	**dot1x timeout supp-response** *seconds* [local]	認証に失敗するまでにアクセス ポイントがクライアントの EAP/dot1x メッセージ返答を待つ時間を秒数で入力します。値を 1 ～ 120 秒の範囲で入力します。 すでに設定されているタイムアウト値とは別のタイムアウト値を優先して送信するように RADIUS サーバを設定できます。アクセス ポイントが RADIUS サーバの値を無視して、設定された値を使用するように設定するには、**local** キーワードを入力します。 オプションの **no** キーワードを使用すると、タイムアウトが 30 秒のデフォルト状態にリセットされます。
ステップ 4	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 5	**dot1x reauth-period** { *seconds* | **server** }	認証されたクライアントに対して再認証するように強制する前に、アクセス ポイントが待つ間隔を秒数で入力します。 認証サーバが指定した再認証間隔を使用するようにアクセス ポイントを設定する場合は、**server** キーワードを入力します。このオプションを使用する場合は、認証サーバを RADIUS 属性 27、Session-Timeout に設定します。この属性により、セッションまたはプロンプトが終了するまでにクライアントに提供されるサービスの最大秒数が設定されます。サーバは、クライアント デバイスが EAP 認証を実行するときにこの属性をアクセス ポイントに送信します。 **（注）** SSID に MAC アドレス認証と EAP 認証を両方設定した場合、サーバからクライアント デバイスの MAC 認証と EAP 認証両方の Session-Timeout 属性が送信されます。アクセス ポイントでは、クライアントが最後に実行した認証の Session-Timeout 属性が使用されます。たとえば、クライアントが MAC アドレス認証を実行し、次に EAP 認証を実行した場合、アクセス ポイントではサーバの EAP 認証の Session-Timeout 値が使用されます。いずれの Session-Timeout 属性を使用するのかという混乱を避けるため、認証サーバで MAC 認証と EAP 認証の両方に同じ Session-Timeout 値を設定します。
ステップ 6	**countermeasure tkip hold-time** *seconds*	TKIP MIC 障害保持時間を設定します。保持時間は、0 ～ 65535 秒の範囲で指定できます。デフォルトは 60 秒です。 アクセス ポイントが、たとえば 60 秒以内に 2 度の MIC 障害を検出した場合、そのインターフェイス上のすべての TKIP クライアントを保持時間だけブロックします。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

値をデフォルトに戻すには、各コマンドの **no** 形式を使用します。

802.1X サプリカントの EAP 方式プロファイルの作成と適用

この項では、802.1X サプリカントに対応した EAP 方式リストのオプション設定について説明します。EAP 方式プロファイルを設定すると、サプリカントで利用可能な EAP 方式でも、サプリカントがその一部を確認応答しないようにできます。たとえば、RADIUS サーバが EAP-FAST と LEAP をサポートしている場合に、特定の設定下において、サーバは安全性の高い方式ではなく、LEAP を最初に使用する場合があります。優先される EAP 方式リストが定義されていない場合、サプリカントは LEAP をサポートしますが、EAP-FAST などの安全性の高い方式をサプリカントに強制するほうが有益です。

802.1X サプリカントの詳細については、「クレデンシャル プロファイルの作成」(P.4-25)を参照してください。

EAP 方式プロファイルの作成

特権 EXEC モードから、次の手順に従って新しい EAP プロファイルを定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**eap profile** *profile name*	プロファイル名を入力します
ステップ 3	**description**	(任意)EAP プロファイルの説明を入力します
ステップ 4	**method** {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}	許可する 1 つまたは複数の EAP 方式を入力します。 **(注)** EAP-GTC、EAP-MD5、および EAP-MSCHAPV2 は、サブパラメータとして表示されますが、トンネル型 EAP 認証の内部方式として使用され、プライマリ認証方式としては使用されません。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

コマンドを無効にする、またはデフォルトに設定するには、**no** コマンドを使用します。

現在利用可能な(登録済み)EAP 方式を表示するには、**show eap registrations method** コマンドを使用します。

```
ap#show eap registrations method
Registered EAP Methods:
Method  Type            Name
    4     Auth and Peer   MD5
    6     Auth and Peer   GTC
   13     Auth and Peer   TLS
   17     Auth and Peer   LEAP
   25     Auth and Peer   PEAP
   26     Auth and Peer   MSCHAPV2
   43     Auth and Peer   FAST
```

既存の EAP セッションを表示するには、**show eap sessions** コマンドを使用します。

ファスト イーサネット インターフェイスに対する EAP プロファイルの適用

この操作は通常、RADIUS サーバに対して認証する必要があるアクセス ポイントが、接続デバイスの 802.1x 認証を行うように設定されたスイッチ ポートに接続される際に、それらのアクセス ポイントに適用されます。この場合、AP は 802.1X クライアントとして機能するため、認証するクレデンシャルを提供する必要があります。

特権 EXEC モードから、次の手順に従って EAP プロファイルをファスト イーサネット インターフェイスに適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet 0**	アクセス ポイントのファスト イーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。 **interface g0** を使用してファスト イーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	**dot1x eap profile** *profile*	プロファイルの事前設定プロファイル名を入力します。
ステップ 4	**end**	インターフェイス コンフィギュレーション モードを終了します。

アップリンク SSID に対する EAP プロファイルの適用

この操作は通常、無線リンクを介してルート アクセス ポイントまたはルート ブリッジに対して認証される必要がある非ルート ブリッジおよびワークグループ ブリッジに適用されます。特権 EXEC モードから、次の手順に従って EAP プロファイルをアップリンク SSID に適用します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 | 1}**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**ssid** *ssid*	アップリンク SSID を無線インターフェイスに割り当てます。
ステップ 4	**dot1x {credentials | default | eap}**	次のいずれかの値を指定できます。 • credentials: クレデンシャル プロファイルの設定 • default: この SSID のデフォルト値で Dot1x を設定します。 • eap: EAP 固有のパラメータを設定します。
ステップ 5	**dot1x eap profile** *profilename*	プロファイルの事前設定プロファイル名を入力します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy running config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

アクセス ポイントとクライアント デバイスの認証タイプのマッチング

この項で説明する認証タイプを使用する場合は、アクセス ポイントの認証設定がアクセス ポイントにアソシエートするクライアント アダプタの認証設定に一致している必要があります。アクセス ポイントに暗号スイートおよび WEP を設定する手順の詳細は、「暗号化モードの設定」(P.10-8)を参照してください。

表 11-1 は、各認証タイプに必要なクライアントとアクセス ポイントの設定を示しています。

（注） Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** を設定しないと、アクセス ポイントに対して 802.1X 認証を実行しないものもあります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP** 認証と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

表 11-1　クライアントとアクセス ポイントのセキュリティ設定

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
静的 WEP キー（Open 認証）	WEP キーを作成し、Use Static WEP Keys と Open Authentication を有効化	WEP を設定して有効化し、SSID に対して Open 認証を有効化。
静的 WEP キー（Shared Key 認証）	WEP キーを作成し、Use Static WEP Keys と Shared Key Authentication を有効化	WEP を設定して有効化し、SSID に対して Shared Key 認証を有効化。
LEAP 認証	LEAP を有効化	WEP を設定して有効化し、SSID に対して Network-EAP を有効化。[1]

表 11-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
EAP-FAST 認証	EAP-FAST を有効化し、自動プロビジョニングを有効化または Protected Access Credential（PAC）ファイルをインポート	WEP を設定して有効化し、SSID[1] に対して Network-EAP を有効化。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。 「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」 CLI を使用している場合は、次の警告メッセージが表示されます。 「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」
WPA による EAP-FAST 認証	EAP-FAST および Wi-Fi Protected Access（WPA）を有効化し、自動プロビジョニングを有効化または PAC ファイルをインポート。 WPA アクセス ポイントと非 WPA アクセス ポイントの両方にクライアントをアソシエートできるようにするには、両方のアクセス ポイントに対して Allow Association を有効にします。	TKIP を含む暗号スイートの選択、WEP の設定および有効化、SSID に対する Network EAP および WPA の有効化。 **（注）** WPA クライアントおよび非 WPA クライアントの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。
802.1X 認証と CCKM	LEAP を有効化	暗号スイートを選択し、SSID に対して EAP および/または Network EAP による Open 認証および CCKM を有効にします。 **（注）** 802.1X クライアントおよび非 802.1X クライアントの両方で SSID を使用できるようにするには、オプションの CCKM を有効にします。

表 11-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
802.1X 認証と WPA	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対して EAP と WPA による Open 認証を有効化します（EAP による Open 認証に加えて、またはその代わりに Network EAP 認証を有効にすることもできます）。 **（注）** WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
802.1X 認証と WPA-PSK	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対してオプション EAP および WPA による Open 認証を有効化します（オプション EAP による Open 認証に加えて、またはその代わりに、Network-EAP 認証を有効にすることもできます）。WPA 事前共有キーを入力。 802.1x/EAP を使用するクライアントは、個々の WPA PMK を生成します。WPA-PSK を使用するクライアントは、PSK を PMK として使用します。 **（注）** WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
動的 WEP 暗号化による EAP-TLS 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択	WEP を設定して有効化し、SSID に対して EAP と EAP による Open 認証を有効化
動的 WEP 暗号化による EAP-MD5 認証		
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および MD5-Challenge を選択	WEP を設定して有効化し、SSID に対して EAP と Open Authentication を有効化
動的 WEP 暗号化による PEAP 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	WEP を設定して有効化し、SSID に対して必須 EAP と EAP による Open 認証を有効化

表 11-1　クライアントとアクセス ポイントのセキュリティ設定（続き）

セキュリティ機能	クライアントの設定	アクセス ポイントの設定
動的 WEP 暗号化による EAP-SIM 認証		
Windows を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および SIM 認証を選択	完全暗号化による WEP をセットアップして有効化し、SSID に対して必須 EAP と EAP による Open 認証を有効化

1. Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP** 認証と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

ゲスト アクセス管理

ゲスト アクセスでは、ゲストはインターネットと、ホスト エンタープライズのセキュリティを損なうことなくゲスト独自のエンタープライズにアクセスできます。

ゲスト アクセスは、次の方法で許可されます。

- Web 認証（セキュア）
- Web パススルー

Web 認証（セキュア）

Web 認証は、ゲストが有効なユーザ名とパスワードを入力するまで、自律 AP が IP トラフィック（DHCP および DNS 関連のパケット以外）をブロックできるようにするレイヤ 3 セキュリティ機能です。

Web 認証では、各ゲスト用に異なるユーザ名とパスワードを定義する必要があります。ユーザ名とパスワードを使用して、ゲストはローカル RADIUS サーバまたは外部 RADIUS サーバによって認証されます。

Web 認証を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Web Authentication] チェックボックスをオンにします。

特権 EXEC モードから、次のコマンドを使用して Web 認証を有効にします。

- 認証は Web インターフェイスを介してレイヤ 3 で行われます。したがってレイヤ 2 で認証を行う必要はないため、ネットワークのセキュリティ タイプはデフォルトで none に設定されます。ただし、レイヤ 3 セキュリティとレイヤ 2 セキュリティを組み合わせることもできます。Web 認証は、Open 認証でのみサポートされます。暗号化は使用できません。
  - ap(config)# **dot11 ssid guestssid**
  - ap(config-ssid)# **web-auth**
  - ap(config-ssid)# **authentication open**
  - ap(config-ssid)# **exit**

- Web 認証を有効にする場合は、次のようにします。
  - ap(config)# **ip admission name Web_auth proxy http**
  - ap(config)# **interface dot11Radio 0**
  - ap(config-if)# **ip admission Web_auth**

Web パススルー

Web パススルーは、Web 認証と似ています。ただし、ゲストは認証情報を入力する必要はありません。

Web パススルーでは、ゲストがインターネットを初めて使用するとき、使用ポリシー ページにゲストをリダイレクトします。ポリシーを受け入れると、アクセスが許可されます。アクセス ポイントはゲストをポリシー ページにリダイレクトします。

Web 認証を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Web Pass] チェックボックスをオンにします。

特権 EXEC モードから、次のコマンドを使用して、Web パススルーを有効にします。

- ap(config)# **ip admission name Web_passthrough consent**
- ap(config)# **interface dot11Radio 0**
- ap(config-if)# **ip admission Web_passthrough**

（注）　VLAN がない場合に限り、Web 認証または Web パススルーがインターフェイスで動作します。SSID が VLAN にマップされている場合、IP admission Web_auth または IP admission Web_passthrough を VLAN に設定する必要があります。

ゲスト アカウントの作成

新しいゲスト アカウントを作成するには、次の手順を実行します。

ステップ 1　GUI で、アクセス ポイントの [Management] > [Guest Management Services] ページを表示します。

ステップ 2　新しいゲスト アカウントを作成するには、[New] を選択します。

[Webauth] ページが表示されます。

ステップ 3　次の値を入力してください。

- Username
- Password
- Confirm Password
- Lifetime

ステップ 4　システムにパスワードとして自動的にランダム文字列を生成させるには、[Generate Password] チェックボックスをオンにします。または、手動でパスワード値を入力することもできます。

ステップ 5　[Apply] をクリックします。

既存のユーザを削除するには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI の [Guest Management Services] ページを表示します。

ステップ 2　削除するユーザ名を選択します。

ステップ 3　[Delete] をクリックします。

確認メッセージが表示されます。

ステップ 4　[OK] をクリックしてユーザを削除するか、[Cancel] をクリックして変更をキャンセルします。

特権 EXEC モードから、CLI コマンドを使用してゲスト アカウントを作成するには、次のコマンドを使用します。

- ap(config)# **dot11 guest**
- ap(config-guest-mode)# **username Gues-1 lifetime 40 password t_ksdgon**
- ap(config-guest-mode)# **username Gues-2 lifetime 35 password gp2**
- ap(config)# **exit**

ゲスト アクセスは最大で 24 日（35791 分）、最小で 5 分許可されます。

特権 EXEC モードから、ゲスト ユーザを削除するには、次のコマンドを使用します。

ap# **clear dot11 guest-user Gues-1**

特権 EXEC モードから、ゲスト ユーザを表示するには、次のコマンドを使用します。

ap# **show dot11 guest-users**

ゲスト アクセス ページのカスタマイズ

[Webauth Login] ゲスト アクセス ページをカスタマイズして、カスタム ロゴやその他のイメージを表示できます。[Login] ページ、[Success] ページ、[Failure] ページ、[Expired] ページをカスタマイズできます。ページをカスタマイズするには、次の手順に従います。

ステップ 1　カスタマイズしたページに表示するイメージを保存し、Web サーバ上で Web サーバの IP アドレスを ACL 入力/出力リスト許可されるように設定します。

ステップ 2　ページのデフォルト HTML コードをカスタマイズします。

ステップ 3　Web サーバ上のイメージ ファイルのフル パスを指定して、イメージを挿入するようにページのソース コードを編集します。例：<Body background="http://40.40.5.10/image.jpg" width="600" height="600">。ここで、image.jpg ファイルは IP アドレスが 40.40.5.10 の Web サーバ上にあります。

（注）　デフォルト ページの HTML コードを編集する際に、送信関数のコードとユーザ名とパスワードのフィールドのコードは変更しないでください。

ステップ 4　Web サーバにカスタマイズしたページを保存します。

ステップ 5　アクセス ポイントの GUI で、[Management] > [Guest Management Services] ページを表示します。

ステップ 6　[Webauth Login] を選択します。

ステップ 7　Web サーバから、次のページを参照してアップロードします

- [Login] ページ
- [Success] ページ
- [Failure] ページ
- [Expired] ページ

（注）　ゲスト アクセス ログインをカスタマイズする場合、[Login] ページ、[Success] ページ、[Failure] ページ、および [Expired] ページは必ずロードする必要があります。

ステップ 8　ファイル転送方式として FTP または TFTP を選択します。

ステップ 9　[Username] を入力します。

ステップ 10　[Password] を入力します。

ステップ 11　[Allowed-In ACL Name] と [Allowed-Out ACL Name] を入力します。

ステップ 12　変更を保存するには、[Close Window] をクリックします。

あるいは、次の CLI コマンドを使用して、カスタマイズされたゲスト アクセス ページを設定することもできます。編集したすべてのファイルをフラッシュ メモリにコピーします。次に、特権 EXEC モードで、次のコマンドを使用して、すべての編集済みファイルをフラッシュからロードします。

- ap(config)# **ip auth-proxy proxy http login page file flash:web_login.html**
- ap(config)# **ip auth-proxy proxy http success page file flash:web_success.html**
- ap(config)# **ip auth-proxy proxy http failure page file flash:web_fail.html**
- ap(config)# **ip auth-proxy proxy http login expired page file flash:web_logout.html**

ACL で Web サーバの IP アドレス（この場合の IP アドレスは 40.40.5.10）を設定するには、次のコマンドも必要です。特権 EXEC モードから、次の ACL コマンドを使用します。

- ap(config)# **dot11 webauth allowed incoming webauth_acl_in outgoing webaut_acl_out**
- ap(config)# **ip access-list extended webauth_acl_in**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**
- ap(config)# **ip access-list extended webauth_acl_out**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**

（注）　上記のコマンドの acl-in および acl-out は、アクセス リストの名前です。これらの ACL を使用すると、マシンに保存されたイメージ ファイルをダウンロードして Web ページのカスタマイズに使用できます。

デフォルト ページには、ユーザ名、パスワード、[OK] ページだけが表示されます。

ゲスト アクセスは、次をサポートしていません。

- IPv6
- SNMP
- ローミング

その他のサービスの設定

この章では、無線ドメイン サービス（WDS）、クライアント デバイスの高速安全ローミング、無線管理、無線侵入検知サービス（WIDS）、およびその他のサービスのアクセス ポイントを設定する方法について説明します。

WDS の概要

ネットワークに WDS を設定すると、無線 LAN 上のアクセス ポイントは WDS デバイス（WDS デバイスとして設定されたアクセス ポイント、サービス統合型ルータのいずれか）を使用して、特定のサブネット内でクライアント デバイスに高速安全ローミングを提供し、無線管理に参加します。WDS デバイスとして設定されたアクセス ポイントは、最大 60 の参加アクセス ポイントをサポートします。WDS デバイスとして設定されたサービス統合型ルータ（ISR）は、最大 100 の参加アクセス ポイントサポートします。

（注）　単一のアクセス ポイントは、最大 16 個までのモビリティ グループをサポートします。

高速安全ローミングによって、クライアント デバイスがアクセス ポイント間をローミングする際の再認証が迅速化されるため、音声やその他の時間に敏感なアプリケーションにおける遅延を回避できます。

無線管理に参加しているアクセス ポイントは、無線環境に関する情報（潜在的な不正アクセス ポイント、クライアント アソシエーション、アソシエーション解除など）を WDS デバイスに転送します。

WDS デバイスの役割

WDS デバイスは無線 LAN 上で次のようないくつかの作業を実行します。

- WDS 機能をアドバタイズして、無線 LAN に最適な WDS デバイスの選択に参加します。WDS 用に無線 LAN を設定する場合は、1 つのデバイスをメインの WDS 候補として設定し、1 つ以上の追加デバイスをバックアップの WDS 候補として設定します。メインの WDS デバイスがオフラインになったら、バックアップの WDS デバイスの 1 つがその役割を引き継ぎます。
- 有線インターフェイスを使用して、サブネット内の全アクセス ポイントを認証し、それぞれのアクセス ポイントとセキュア通信チャネルを設定します。
- 参加しているアクセス ポイントにアソシエートされているすべての 802.1X 認証クライアント デバイスに対するパススルーとして機能します。
- 動的キーを使用するサブネット中の全クライアント デバイスを登録して、それらに対してセッション キーを設定し、セキュリティ クレデンシャルをキャッシュします。クライアントが WDS デバイスに登録された別のアクセス ポイントにローミングするときは、WDS デバイスがクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送します。

表 12-1 に、WDS デバイスとして設定できるプラットフォーム（アクセス ポイントまたは ISR）でサポートされる参加アクセス ポイント数をリストします。

表 12-1　WDS デバイスでサポートされる参加アクセス ポイント数

WDS デバイスとして設定されたユニット	サポートされる参加アクセス ポイント数
クライアント デバイスからも接続できるアクセス ポイント	30
無線インターフェイスが無効になっているアクセス ポイント	60
サービス統合型ルータ（ISR）	100（ISR プラットフォームに応じて異なる）

WDS デバイスを使用したアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次の動作において WDS デバイスと対話します。

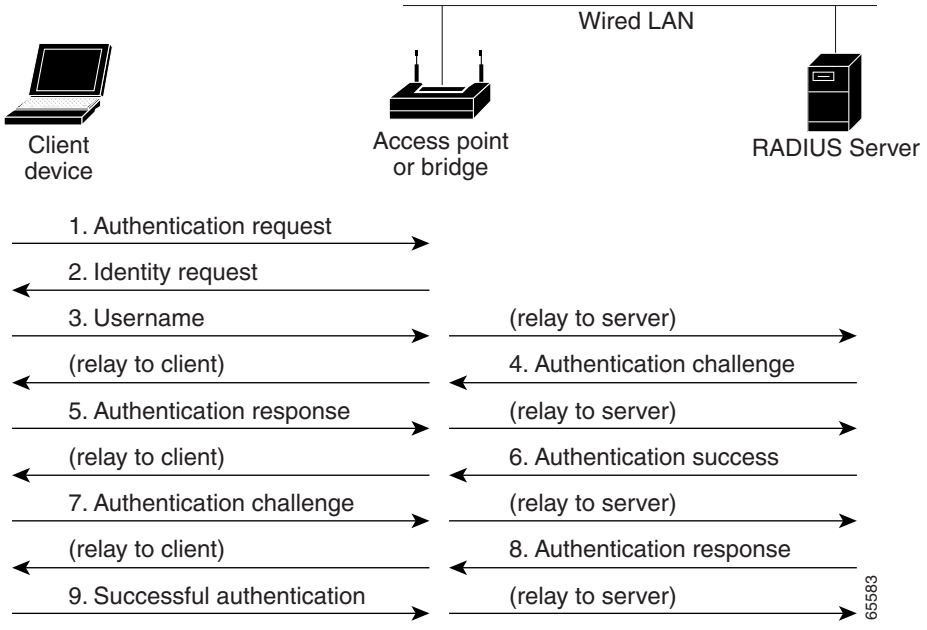
- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。
- 無線データを WDS デバイスに報告します。

高速安全ローミングの概要

多くの無線 LAN 内のアクセス ポイントは、システム全体においてアクセス ポイントからアクセス ポイントへローミングするモバイル クライアント デバイスに対応します。クライアント デバイスで稼働するアプリケーションの中には、異なるアクセス ポイントにローミングする場合に高速な再アソシエーションを必要とするものがあります。たとえば、音声アプリケーションでは、会話の遅延やギャップを防ぐために、シームレスなローミングが必要です。

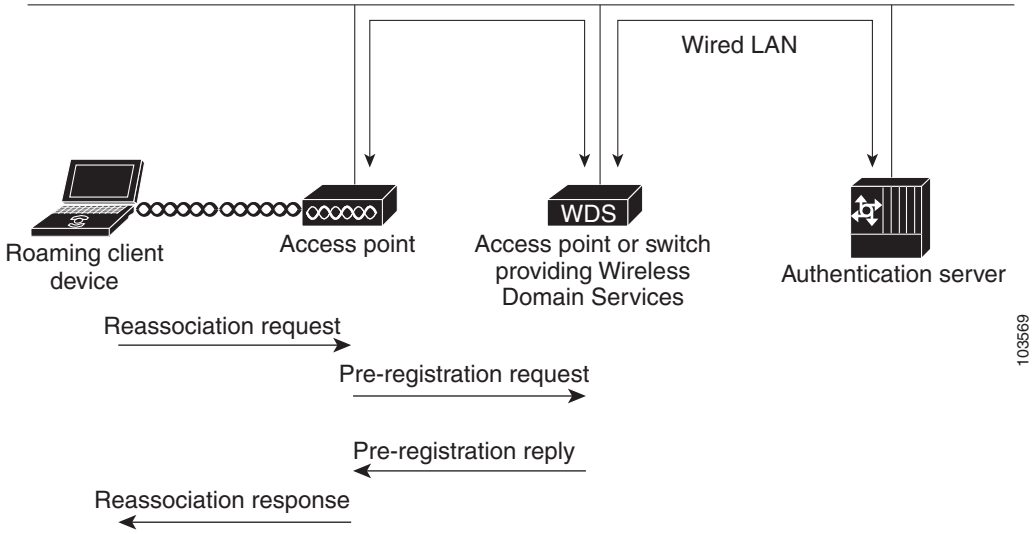
通常稼働時、EAP/802.1x 対応クライアント デバイスは、メイン RADIUS サーバとの通信を含む完全な EAP/802.1x 認証を実行することによって、新しいアクセス ポイントとの間で相互認証を行います（図 12-1 を参照）。

図 12-1　RADIUS サーバを使用したクライアント認証交換の例（LEAP の場合）



無線 LAN に高速安全ローミングを設定すれば、EAP/802.1x 対応のクライアント デバイスはメイン RADIUS サーバを利用することなく、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るようになります。Cisco Centralized Key Management（CCKM）を使用すると、無線ドメイン サービス（WDS）を提供するように設定されているデバイスは、RADIUS サーバの代わりにクライアントを短時間で認証するため、音声などの時間が重要なアプリケーションでは知覚できるほどの遅延は発生しません。図 12-2 は、CCKM を使用したクライアント認証を示しています。

図 12-2　CCKM と WDS アクセス ポイントを使用するクライアント再アソシエーション



WDS デバイスは、無線 LAN 上の CCKM 利用可能クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 利用可能クライアントが、1 つのアクセス ポイントから別のアクセス ポイントへローミングする場合、クライアントが新しいアクセス ポイントへ再アソシエーションの要求を送信し、新しいアクセス ポイントはその要求を WDS デバイスへ中継します。WDS デバイスはクライアントのクレデンシャルを新しいアクセス ポイントに転送し、新しいアクセス ポイントは再アソシエーション応答をクライアントに送信します。クライアントと新しいアクセス ポイントとの間で渡されるパケットは 2 つだけであるため、再アソシエーションの時間が大幅に短縮されます。クライアントは再アソシエーション応答をユニキャスト キーの生成にも使用します。高速安全ローミングをサポートするアクセス ポイントを設定する方法の詳細は、「高速安全ローミングの設定」(P.12-17)を参照してください。

（注） このメカニズムでは、クライアントが AP 間で受け渡しされるクレデンシャルを受け入れる必要もあります。必ず、アクセス ポイントで CCKM を有効にするとともに、ワイヤレス クライアントが、ネットワークで使用されている（CCX を使用する）認証メカニズムに対し CCKM をサポートしていることを確認してください。CCKM をサポートしていない場合、クライアントは高速ローミング メカニズムを拒否し、RADIUS サーバによる再認証を強制する場合があります。
各認証メカニズムに必要な CCX バージョンを調べるには、次の URL にアクセスしてください。
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html
各クライアント タイプでサポートされる CCX バージョンを調べるには、次の URL にアクセスしてください。
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Wireless Intrusion Detection Service の概要

無線 LAN 上に Wireless Intrusion Detection Service（WIDS）を実装すると、アクセス ポイント、およびオプションの（シスコ以外の）WIDS エンジンが同時に動作して、無線 LAN インフラストラクチャ、およびアソシエートされたクライアント デバイスに対する攻撃を探知および防止します。

（シスコ以外の）WIDS エンジンとともに動作する場合、アクセス ポイントは侵入を探知し、無線 LAN を防御するアクションを実行できます。

WIDS の機能は次のとおりです。

- スイッチ ポートのトレースと不正抑制：スイッチ ポートのトレースと抑制では、未知の無線（潜在的な不正デバイス）の無線 MAC アドレスを生成する RF 検出方法を使用します。（シスコ以外の）WIDS エンジンは、無線 MAC アドレスから有線側 MAC アドレスを取り出し、これを使用してスイッチの BRIDGE MIB を検索します。
- 過剰管理フレーム検出：過剰管理フレームは、無線 LAN が攻撃されたことを示します。攻撃者は、無線上で大量の管理フレームを注入し、そのフレームを処理する必要があるアクセス ポイントに大きな負荷を加えることにより、サービス拒絶攻撃を実行する場合があります。スキャン モードのアクセス ポイントとルート アクセス ポイントは、WIDS のフィーチャ セットの一部として無線信号をモニタして、過剰管理フレームを検出します。アクセス ポイントが過剰管理フレームを検出すると、障害を生成して、それを WDS を介して（シスコ以外の）WIDS エンジンに送信します。
- 認証/保護失敗検出：認証/保護失敗検出は、無線 LAN 上での最初の認証フェーズを回避するかまたは、進行中のリンク保護を侵害しようとする攻撃者を探します。これらの検出メカニズムは、次の特定の認証攻撃に対応します。
  - EAPOL フラッド検出
  - MIC/暗号化失敗検出
  - MAC スプーフィング検出
- フレーム キャプチャ モード：フレーム キャプチャ モードでは、スキャナ アクセス ポイントが 802.11 フレームを収集し、ネットワーク上の WIDS エンジンのアドレスに転送します。

（注）　アクセス ポイントの WIDS への参加の設定方法については、「WIDS に参加するようにアクセス ポイントを設定する」（P.12-26）を、アクセス ポイントに対する Management Frame Protection（MFP; 管理フレーム保護）の設定方法については、「管理フレーム保護の設定」（P.12-21）を参照してください。

- 802.11 管理フレーム保護（MFP）：本質的に、無線は正規のデバイスか、不法デバイスであるかを問わず、あらゆるデバイスで傍受および参加が可能なブロードキャスト メディアです。制御/管理フレームは、クライアント ステーションが AP とのセッションを選択および開始する際に使用するため、これらのフレームはオープンである必要があります。管理フレームは暗号化できませんが、偽造から保護する必要があります。MFP は、802.11 管理フレームを完全に保護できる手段です。

WDS の設定

この項では、ネットワーク上で WDS を設定する方法について説明します。この項の構成は、次のとおりです。

WDS のガイドライン

WDS を設定する場合は、次のガイドラインに従います。

- クライアント デバイスも収容している WDS アクセス ポイントでは最大 30 個のアクセス ポイントの参加がサポートされますが、無線を無効にした WDS アクセス ポイントでは、最大 60 個までサポートされます。

  WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャ アクセス ポイントと 1200 個のクライアントがサポートされます。

- リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻る(フォールバックする)設定はしないでください。

WDS の要件

WDS を設定するには、無線 LAN 上に次の項目を含める必要があります。

- 少なくとも 1 つのアクセス ポイントまたはサービス統合型ルータ(ISR)
- 認証サーバ(またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR)

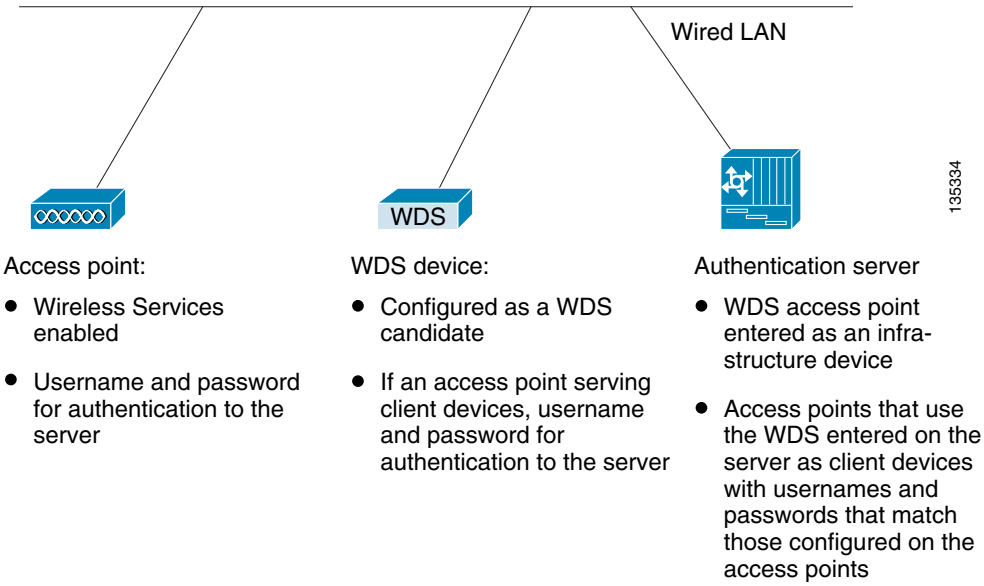
コンフィギュレーションの概要

WDS および高速安全ローミングの設定には、次の 3 つの主要手順を完了する必要があります。

1. アクセス ポイント、ISR、またはスイッチを潜在的な WDS デバイスとして設定します。この項では、アクセス ポイントを WDS デバイスとして設定する方法について説明します。
2. 他のアクセス ポイントが、この WDS デバイスを使用するように設定します。
3. ネットワーク上の認証サーバが WDS デバイスと、WDS デバイスを使用するアクセス ポイントを認証するように設定します。

図 12-3 は、WDS に参加する各デバイスに必要な設定を示しています。

図 12-3　WDS に参加するデバイスの設定



アクセス ポイントを潜在的な WDS デバイスとして設定する

（注） メインの WDS 候補用に、多数のクライアント デバイスを収容する必要のないアクセス ポイントを設定します。クライアント デバイスが WDS アクセス ポイントの起動時にアソシエートした場合、そのクライアントは認証のために数分待たされる可能性があります。

（注） リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また、WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。

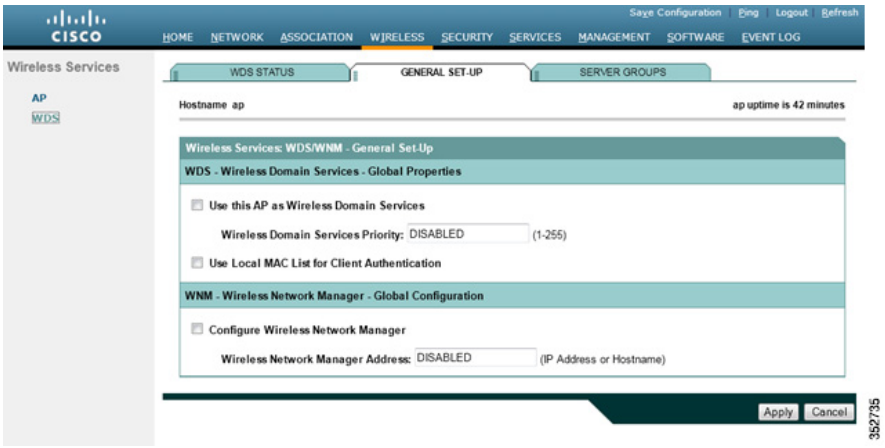
（注） WDS が有効な場合、WDS アクセス ポイントはすべての認証を実行、トラッキングします。したがって、WDS アクセス ポイントでは EAP セキュリティ設定を行う必要があります。アクセス ポイント上での EAP 設定の詳細は、第 11 章「認証タイプの設定」を参照してください。

プライマリ WDS アクセス ポイントとして設定するアクセス ポイント上で、次の手順に従ってメインの WDS 候補としてアクセス ポイントを設定します。

ステップ 1　[Wireless] > [WDS] の順に選択します。

ステップ 2　[General Set-Up] タブをクリックします。

図 12-4　[General Set-Up] の [Hostname ap] ページ



ステップ 3　[***Use this AP as Wireless Domain Services***] チェックボックスをオンにします。

ステップ 4　[Wireless Domain Services Priority] フィールドに 1 ～ 255 の優先順位数を入力して、WDS 候補の優先順位を設定します。
[Wireless Domain Services Priority] フィールド内の数字が最も大きい WDS アクセス ポイント候補が、WDS アクセス ポイントとして機能します。たとえば、1 つの WDS 候補には優先順位に 255 が割り当てられており、もう 1 つの候補には優先順位に 100 が割り当てられている場合は、優先順位が 255 の候補が WDS アクセス ポイントとして機能します。

ステップ 5　(WDS クライアントの場合のみ)WDS デバイスに設定されたローカル アドレス リストに含まれる MAC アドレスを使用してクライアント AP デバイスを認証する場合は、[Use Local MAC List for Client Authentication] チェックボックスをオンにします。
このチェックボックスをオンにしない場合、WDS デバイスは [Server Groups] ページで MAC アドレス認証用に指定したサーバを使用して、MAC アドレスに基づくクライアント認証を行います。

(注)　[Use Local MAC List for Client Authentication] チェックボックスをオンにしても、クライアント デバイスに対して MAC ベースの認証が強制されるわけではありません。サーバベースの MAC アドレス認証に対するローカルの代替方法が提供されるだけです。

ステップ 6　[Apply] をクリックします。

ステップ 7　[Server Groups] タブをクリックして [WDS Server Groups] ページに移動します。

ステップ 8　WDS アクセス ポイントを使用するインフラストラクチャ デバイス(アクセス ポイント)の 802.1x 認証に使用するサーバ グループを作成します。[Server Group Name] フィールドにグループ名を入力します。

ステップ 9　[Priority 1] ドロップダウン リストからプライマリ サーバを選択します (グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります)。

(注)　ネットワーク上に認証サーバが存在しない場合、アクセス ポイントまたは ISR をローカル認証サーバとして設定できます。設定方法の詳細は、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

ステップ 10　（任意）[Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

ステップ 11　[Apply] をクリックします。

ステップ 12　ワイヤレス クライアント デバイス用の 802.1x 認証に使用するサーバのリストを設定します。特定のタイプの認証（EAP、LEAP、その他の EAP タイプ、または MAC ベースなど）を使用するクライアント用の別のリストを指定したり、任意のタイプの認証を使用するクライアント デバイス用のリストを指定したりできます。[Server Group Name] フィールドに、サーバのグループ名を入力します。

[LEAP Authentication] チェックボックスは、特に次に示すシスコ製クライアント向けに用意されています。

- LEAP を使用する Cisco 7920、7921、および 7925 電話
- ワイヤレス クライアント（ワークグループ ブリッジまたは非ルート ブリッジ）として設定され、LEAP 認証を使用する自律 AP

[LEAP Authentication] チェックボックスをオフにすると、これらのクライアント デバイスは、LEAP および WDS サービスを使用してワイヤレス ネットワークに対する認証を実行できなくなります。EAP オプションが選択されている場合、クライアントは他の任意の形式の EAP 認証を使用して接続できます。ただし、これによって、他のクライアント カードやサプリカントの組み合わせが接続できなくなるわけではありません。これらのクライアントは、LEAP を含め、あらゆる形式の EAP 認証に 802.1X 標準を使用するためです。この情報は、シスコ以外のクライアントには適用されません。

ステップ 13　[Priority 1] ドロップダウン リストからプライマリ サーバを選択します（グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります）。

ステップ 14　（任意）[Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

ステップ 15　（任意）[Restrict SSIDs] を選択すると、使用するサーバ グループを、特定の SSID を使用するクライアント デバイスに制限できます。[SSID] フィールドに SSID を入力して、[Add] をクリックします。SSID を削除するには、削除する SSID を [SSID] リスト内で選択して [Remove] をクリックします。

ステップ 16　[Apply] をクリックします。

ステップ 17　EAP 認証用に WDS アクセス ポイントを設定します。EAP の設定方法の詳細については、第 11 章「認証タイプの設定」を参照してください。

（注）　この認証では、デフォルトで LEAP を使用します。WDS サービスを使用するインフラストラクチャ アクセス ポイントは、WDS デバイスを介して認証される必要があります。WDS アクセス ポイントでクライアント デバイスを使用する場合は、「アクセス ポイントを WDS デバイスを使用するように設定する」（P.12-10）の手順に従って、WDS アクセス ポイントが WDS を使用するように設定します。

CLI の設定例

次の例は、「アクセス ポイントを潜在的な WDS デバイスとして設定する」(P.12-7) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

次の例では、サーバ グループ *infra_devices* を使用してインフラストラクチャ デバイスを認証しています。SSID *fred* または *ginger* を使用するクライアント デバイスは、サーバ グループ *client_devices* を使用して認証されます。SSID リストを指定しない場合、すべての SSID が対象になります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

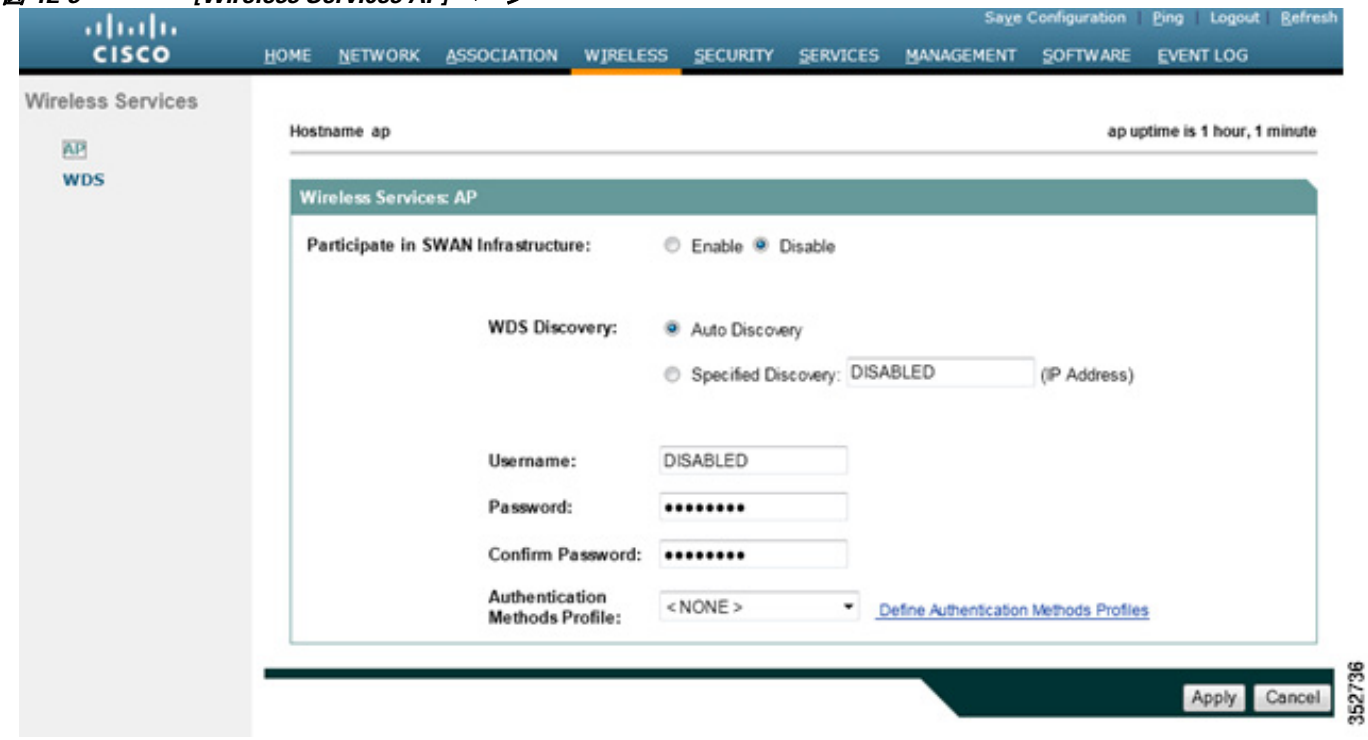
アクセス ポイントを WDS デバイスを使用するように設定する

WDS デバイスを通じて認証し、WDS 内に参加するようにアクセス ポイントを設定する手順は、次のとおりです。

（注） インフラストラクチャ アクセス ポイントが WDS に参加するには、WDS が実行している IOS と同じバージョンを実行する必要があります。

ステップ 1　[Wireless] > [AP] の順に選択します。[Wireless Services AP] ページが表示されます。

図 12-5　[Wireless Services AP] ページ



ステップ 2　AP がクライアント認証で WDS サービスを使用できるように設定するには、[Participate in SWAN Infrastructure] 設定の [Enable] をクリックします。

ステップ 3　（任意）[Specified Discovery] を選択し、入力フィールドに WDS の IP アドレスを入力します。[Specified Discovery] を有効にすると、アクセス ポイントは WDS アドバタイズメントを待たずに、WDS デバイスを使用して即座に認証します。指定した WDS デバイスが応答しない場合、アクセス ポイントは WDS アドバタイズメントを待ちます。

ステップ 4　[Username] フィールドにアクセス ポイントのユーザ名を入力します。このユーザ名は、認証サーバ上でアクセス ポイント用に作成したユーザ名と一致していなければなりません。

ステップ 5　[Password] フィールドにアクセス ポイントのパスワードを入力し、[Confirm Password] フィールドに同じパスワードをもう一度入力します。このパスワード名は、認証サーバ上でアクセス ポイント用に作成したパスワードと一致していなければなりません。このページでユーザ名とパスワードを設定すると、AP は WDS サーバを介した認証に LEAP を使用します。

ステップ 6　（任意）インフラストラクチャ AP の認証を LEAP を使用した WDS で行わず、別の EAP 認証方式（EAP-FAST など）を使用する場合は、[Authentication Methods Profile] ドロップダウン リストから別の認証方式プロファイルを選択します。認証方式プロファイルをまだ定義していない場合は、[Define Authentication Method Profiles] リンクをクリックしてプロファイルを設定してから、[Wireless Services AP] 設定ページに戻ってプロファイルを選択します。新しいプロファイルの作成方法の詳細については、「802.1X サプリカントの EAP 方式プロファイルの作成と適用」（P.11-20）を参照してください。

ステップ 7　[Apply] をクリックします。

WDS と対話するように設定したアクセス ポイントは、自動的に次の手順を実行します。

- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。

CLI の設定例

次の例は、「アクセス ポイントを WDS デバイスを使用するように設定する」（P.12-10）に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 0 wes7win8
AP(config)# wlccp ap eap profile Myfast
AP(config)# end
```

この例では、アクセス ポイントは WDS デバイスと対話できるように設定されており、ユーザ名に *APWestWing*、パスワードに *wes7win8* を使用して認証サーバに対する認証を行います。

オプションの Myfast EAP プロファイルは、LEAP 以外の方式を使用して認証を行うために呼び出されます。この例では、プロファイルは EAP-FAST を使用し、次のように設定されています。

```
ap(config)# eap profile myfast
ap(config-eap-profile)# method fast
ap(config-eap-profile)# end
```

認証サーバ上でクライアントとしてアクセス ポイントを設定するときには、同じユーザ名とパスワードの組み合わせで設定する必要があります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

認証サーバが WDS をサポートするように設定する

WDS デバイスと WDS に参加している全アクセス ポイントは、認証サーバに対する認証を行う必要があります。サーバ上で、アクセス ポイント用のユーザ名とパスワードと、WDS デバイス用のユーザ名とパスワードを設定します。

サーバが Cisco ACS を実行している場合は、次の手順に従ってサーバ上でアクセス ポイントを設定します。

ステップ 1　Cisco Identity Services Engine（ISE）にログインします。

ステップ 2　[Administration] > [Network Resources] > [Network devices] を選択します。
[Network Devices] ページが表示されます。
このページで、WDS を AAA クライアントとして追加できます。

図 12-6　Cisco ISE の [Network Devices] ページ

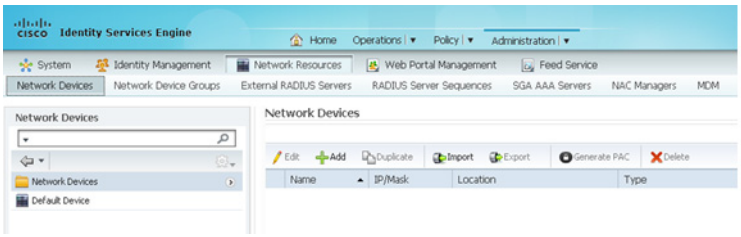
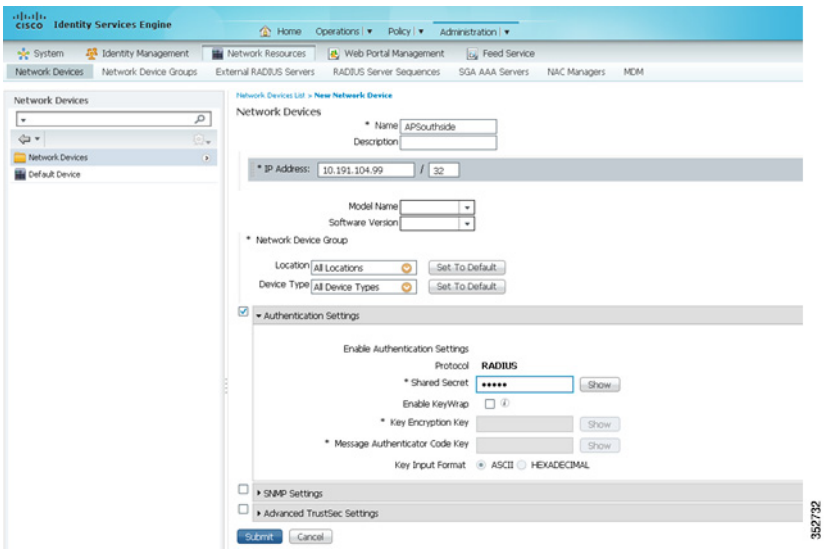


図 12-7　Cisco ISE の [Network Devices] ページの詳細



ステップ 3　[Add] をクリックし、WDS を新しい AAA クライアントとして追加します。

ステップ 4　[Name] フィールドに、WDS デバイス名を入力します。この名前はローカルでのみ有効です。オプションで、WDS デバイスの説明を入力します。

ステップ 5　[IP Address] フィールドに、WDS デバイスの IP アドレスを入力します。
(任意)デバイスのロケーションとデバイス タイプを指定します(これらのカテゴリが ISE に設定されている場合のみ)。

ステップ 6　[Authentication Settings] チェックボックスをオンにします。[Authentication Settings] 領域のフィールドが有効になります。

ステップ 7　RADIUS プロトコルの場合、[Shared Secret] フィールドに共有秘密値を入力します。この値は、ISE を RARIUS サーバとして設定するときに、WDS デバイスでそのとおりに入力されます。

ステップ 8　[Submit] をクリックしてエントリを検証します。

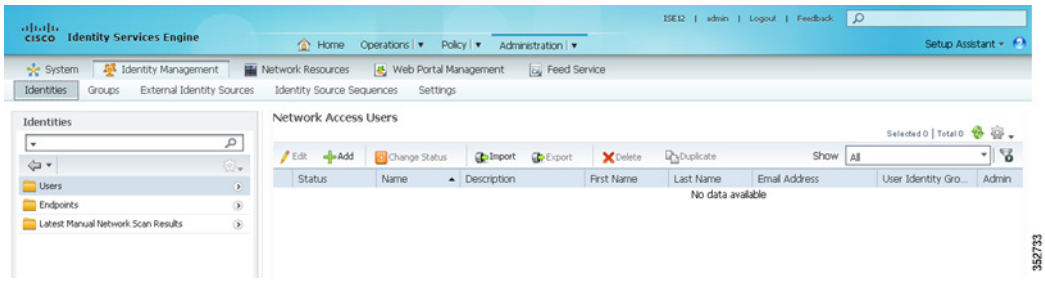
ステップ 9　WDS デバイス候補のそれぞれについて、ステップ 3 からステップ 8 の手順を繰り返します。

ステップ 10　[Administration] > [Identities Management] > [Identities] の順に選択します。
[Network Access Users] ページが表示されます。

(注)　この手順では、ISE 内部データベースにユーザを設定する方法を説明します。ISE では、外部データベースも使用できます。詳細については、ISE ガイドを参照してください。

ステップ 11　[Add] をクリックして、新しいユーザを追加します。

図 12-8　[Network Access Users] ページ



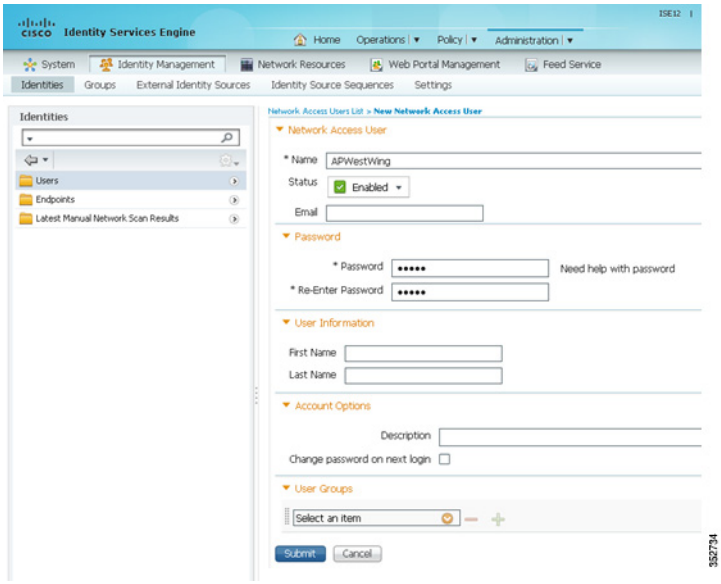
ステップ 12　[Name] フィールドに、WDS へのアクセス ポイント クライアントに設定したユーザ名を入力します。

ステップ 13　[Password] フィールドと [Confirm Password] フィールドに、[Wireless Services AP] ページでアクセス ポイントに対して入力したのとまったく同じパスワードを入力します。

ステップ 14　[Submit] をクリックします。

ステップ 15　WDS デバイスを使用するアクセス ポイントそれぞれに対して、ステップ 11 からステップ 14 の手順を繰り返します。

図 12-9　Cisco ISE の [Network Access Users] ページの詳細



WDS 専用モードの設定

WDS アクセス ポイントは、**wlccp wds mode wds-only** コマンドを使用すれば、WDS 専用モードで稼働できます。このコマンドを発行してリロードすると、アクセス ポイントは WDS 専用モードで機能を開始します。WDS 専用モードでは、dot11 サブシステムが初期化されず、dot11 インターフェイス関連のコマンドが設定できません。WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャ アクセス ポイントと最大 1200 個のクライアントがサポートされます。このコマンドの **no** 形式を使用して、WDS 専用モードをオフにします。WDS アクセス ポイントの実行中モードを表示するには、**show wlccp wds** コマンドを使用します。

WDS アクセス ポイントが AP および WDS の両モードで稼働するように設定するには、**no wlccp wds mode wds-only** コマンドを使用し、さらに **write erase** コマンドを使用してアクセス ポイントをただちにリロードします。アクセス ポイントをリロードすると、dot11 無線サブシステムが初期化されます。アクセス ポイントと WDS は、無線クライアントに直接アソシエートします。このモードの場合、WDS では 20 個の無線クライアントの直接アソシエートに加え、30 個のインフラストラクチャ アクセス ポイントと 600 個のクライアントがサポートされます。

WDS 情報の表示

Web ブラウザのインターフェイスでは、[Wireless Services Summary] ページを使って WDS ステータスの概要を表示します。

特権 EXEC モードの CLI では、次のコマンドを使って、現在の WDS デバイスと CCKM に参加している他のアクセス ポイントについての情報を表示します。

コマンド	説明
show wlccp ap	CCKM に参加する任意のアクセス ポイント上で、このコマンドを使用して、WDS デバイスの MAC アドレス、WDS デバイスの IP アドレス、アクセス ポイントのステート（認証中、認証済み、登録済み）、インフラストラクチャ認証サーバの IP アドレス、クライアント デバイス（MN）認証サーバの IP アドレスを表示できます。
show wlccp wds ap [**cdp-neighbor** | **mac-address** *mac-address* | **order ip**]	WDS デバイスに限り、このコマンドを使って、CCKM に参加するアクセス ポイントに関するキャッシュ情報を表示できます。 • cdp-neighbor：WDS で認証された各 AP によってレポートされた CDP ネイバーを表示します。 • mac-address *mac-address*：入力された MAC アドレスで指定された AP に関する情報のみを表示します。 • order ip：AP の表示順を、AP MAC アドレスによる昇順から AP IP アドレスによる昇順に変更します。

コマンド	説明
show wlccp wds mn [**detail**] [**mac-addr** *mac-address*]	このコマンドを使用して、クライアント デバイスや呼び出されたモバイル ノードに関するキャッシュ情報を表示します。このコマンドは、各クライアントの MAC アドレス、IP 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（cur-AP）、および状態（認証中、認証済み、または登録済み）を表示します。detail オプションを使用して、クライアントの有効期間（クライアントが再認証を必要とするまでの残りの秒数）、SSID、および VLAN ID を表示します。 特定のクライアント デバイスに関する情報を表示するには、**mac-address** オプションを使用します。
show wlccp wds	このコマンドを使用して、アクセス ポイントの IP アドレス、MAC アドレス、優先順位、インターフェイスの状態（管理上スタンドアロン、アクティブ、バックアップ、候補、または WDS 専用）を表示します。 状態がバックアップの場合、コマンドは現在の WDS デバイスの IP アドレス、MAC アドレス、および優先順位も表示します。
show wlccp wds nm	このコマンドを使用して、設定済みのすべてのネットワーク管理プラットフォームと統計情報（送受信メッセージ数、再送信数、ドロップされたメッセージ数）のリストを表示します。
show wlccp wds statistics	このコマンドを使用して、WDS に関する統計情報を表示します。統計情報には、現在の AP カウント、接続された AP での現在のクライアント カウント、AAA 認証試行カウント、AAA 認証成功カウント、AAA 認証失敗カウント、MAC スプーフィング ブロック カウント、AAA 認証なしのローミング カウント（事前共有キーと Open ネットワーク）、完全な AAA 認証を使用したローミング カウント（高速安全ローミングをサポートしていない非 CCX デバイスの場合）、高速安全ローミング カウント、MSC 失敗カウント、KSC 失敗カウントMIC 失敗カウント（WPA/WPA2 リプレイ攻撃の検出）、および RN 不一致カウント（WPA2 不一致の検出）が含まれます。
show wlccp wds aggregator statistics	このコマンドを使用して、参加 AP から収集された無線測定情報（送受信された更新）に関する統計を表示します。

デバッグ メッセージの使用

特権 EXEC モードでは、デバッグ コマンドを使用して、WDS デバイスと対話するデバイス用のデバッグ メッセージの表示を制御します。

コマンド	説明
debug wlccp ap {mn | nm | wds-discovery | state}	このコマンドを使用して、クライアント デバイス（**mn**）、設定済み管理プラットフォーム（**nm**）、WDS 検出プロセス、WDS デバイス（**state**）に対するアクセス ポイントの認証に関連するデバッグ メッセージの表示を有効にします。
debug wlccp dump	このコマンドを使用して、バイナリ形式で送受信された WLCCP パケットのダンプを実行します。
debug wlccp packet	このコマンドを使用して、WDS デバイスとやり取りするパケットの表示をオンにします。
debug wlccp rmlib { errors | packets }	このコマンドを使用して、AP と WDS の間、および（該当する場合は）WDS とネットワーク管理プラットフォームの間で交換された無線測定メッセージのデバッグを有効にします。
debug wlccp wds [aggregator | all | ap | authenticator | mn | nm | recovery | state | statistics]	このコマンドとそのオプションを使用して、WDS デバック メッセージの表示をオンにします。 すべての AP の WDS イベントをデバッグするには、**ap** オプションを使用します。オプションで mac-address を指定して、その特定の AP のイベントをデバッグすることもできます。 すべての WDS イベントをデバッグするには、**all** オプションを使用します。 必要に応じて、**nm** オプションを使用して、ネットワーク管理プラットフォームと交換されたメッセージをデバッグします。 WDS フェールオーバー（正常回復）プロセスをデバッグするには、**recovery** オプションを使用します。 **statistics** オプションを使用して、障害統計情報の表示をオンにします。
debug wlccp wds authenticator {all | dispatcher | mac-authen | process | rxdata | state-machine | txdata}	このコマンドとそのオプションを使用して、認証に関連する WDS デバック メッセージの表示をオンにします。

高速安全ローミングの設定

WDS を設定すると、CCKM 用に設定したアクセス ポイントは、アソシエートされたクライアント デバイスに高速安全ローミングを提供できます。この項では、高速で安全なローミングを無線 LAN 上で設定する方法を説明します。この項の構成は、次のとおりです。

- 高速安全ローミングの要件
- 高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングの要件

高速安全ローミングを設定するには、無線 LAN で次の項目が必要となります。

- WDS デバイスとして設定された 1 つ以上のアクセス ポイントまたは ISR
- WDS に参加するように設定されたアクセス ポイント
- 高速安全ローミング用に設定されたアクセス ポイント
- 認証サーバ（またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR）
- Cisco Aironet クライアント デバイス、または Cisco Compatible Extensions（CCX）バージョン 2 以降と互換性のあるシスコ互換のクライアント デバイス

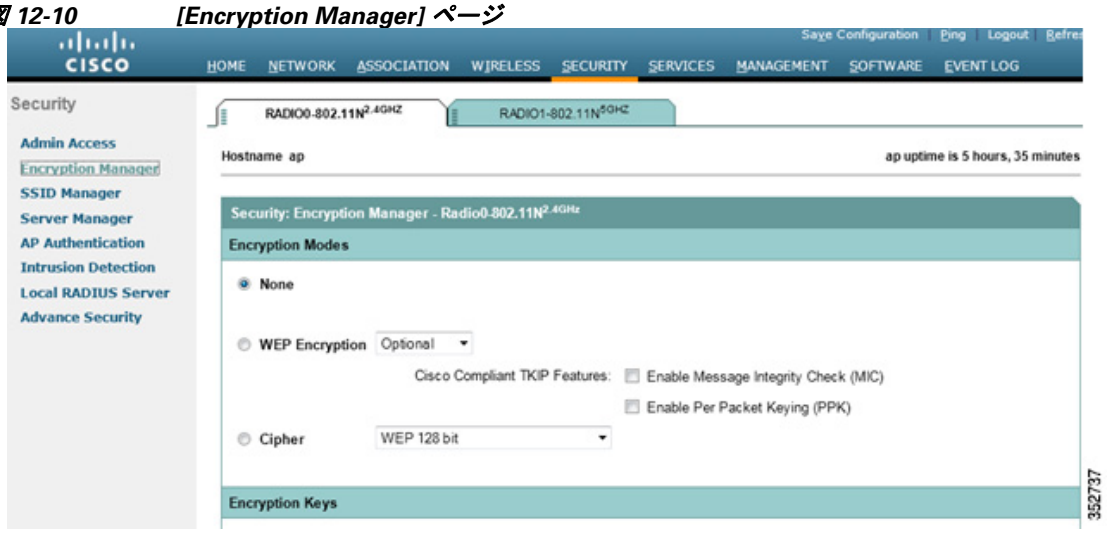
WDS の設定方法については、「WDS の設定」（P.12-6）を参照してください。

高速安全ローミングをサポートするアクセス ポイントの設定

高速安全ローミングをサポートするには、WDS に参加するように無線 LAN 上のアクセス ポイントを設定し、それらのアクセス ポイントでターゲット SSID の CCKM 認証済みキー管理を許可する必要があります。SSID に CCKM 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 GUI で [Encryption Manager] ページを表示します。図 12-10 は、[Encryption Manager] ページの上部を示しています。

図 12-10　[Encryption Manager] ページ



ステップ 2　[Cipher] ボタンをクリックします。

ステップ 3　任意の暗号化メカニズムを設定します。シスコでは WPA2 の使用を推奨しています（WPA2 をサポートしていないレガシー クライアントをサポートする必要がある場合を除く）。暗号化メカニズムを WPA2 に設定するには、[Cipher] ドロップダウン リストから [AES CCMP] を選択します。

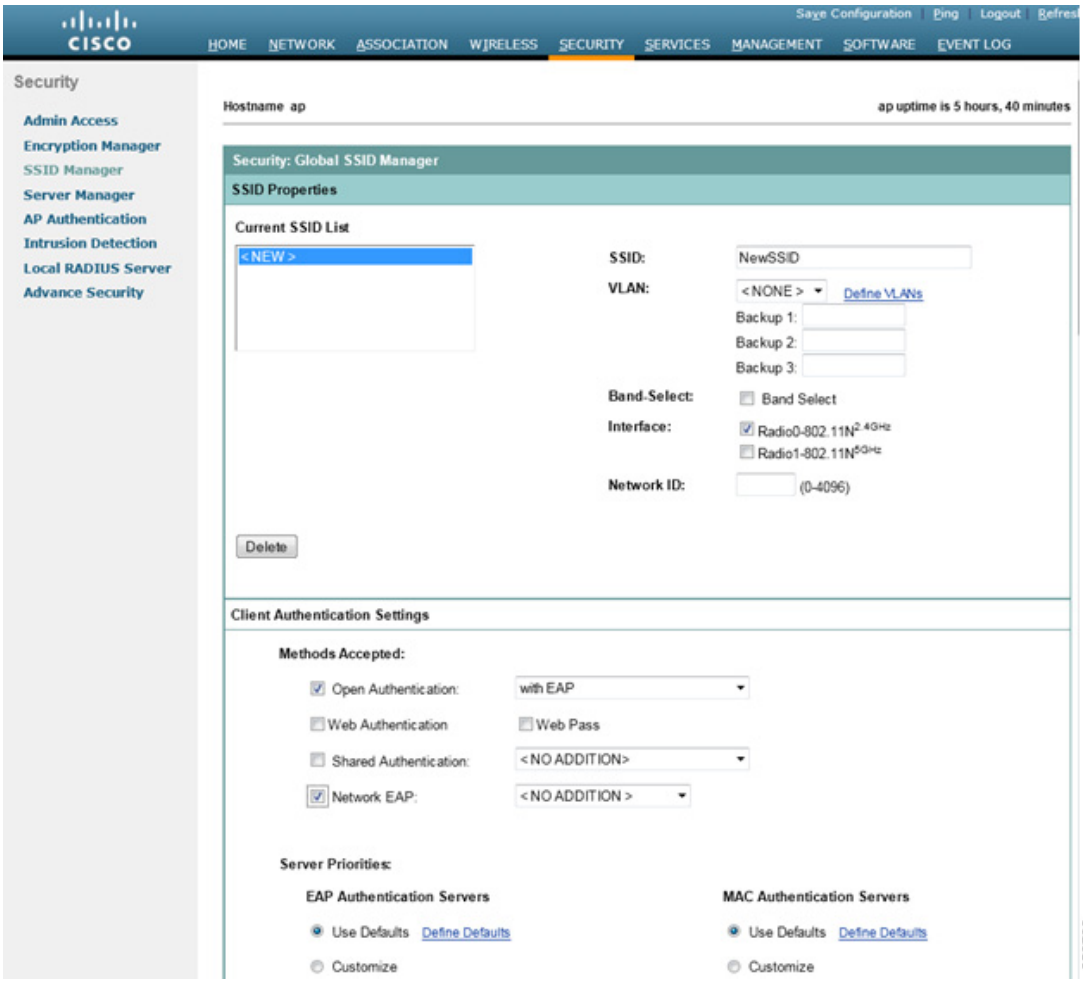
（注）　シスコでは、混合モード（AES CCMP と TKIP または WEP）の設定を推奨していません。これらのモードはネットワークのセキュリティを弱めるため、非推奨となっています。

ステップ 4　[Cipher] ドロップダウン リストから、[CKIP + CMIC] を選択します。

ステップ 5　[Apply] をクリックします。

ステップ 6　[Global SSID Manager] ページを表示します。図 12-11 は、[Global SSID Manager] ページの上部を示しています。

図 12-11　[Global SSID Manager] ページ



ステップ 7　CCKM（高速安全ローミング）をサポートする必要があるターゲット SSID で、次の設定を選択します。

a.　アクセス ポイントに複数の無線インターフェイスが含まれている場合は、SSID が適用されるインターフェイスを選択します。

b.　ネットワーク設定で、サポートする 802.1X/EAP 方式を選択します。Cisco IP 電話 7920、7921、7925、および 7926 で LAP をサポートする場合、およびクライアント アクセス ポイントには [Network EAP] を選択する必要があります。その他すべての EAP タイプ（PEAP、EAP-FAST、または EAP-TLS など）、およびその他すべてのクライアントのすべての EAP タイプ（LEAP を含む）には、[Open Authentication with EAP] を選択する必要があります。

c.　[Key Management] 領域の [Key Management] ドロップダウン リストから、必要に応じて [Mandatory] または [Optional] を選択します。[Mandatory] を選択した場合、CCKM をサポートするクライアントだけが、SSID を使用してアソシエートできます。[Optional] を選択した場合、CCKM クライアントと CCKM をサポートしないクライアントの両方が、SSID を使用してアソシエートできます。

d. [CCKM] チェックボックスをオンにします。

e. AES CCMP 暗号を選択した場合、[Enable WPA] チェックボックスをオンにして、ドロップダウン リストから [WPAv2] オプションを選択します。

ステップ 8　[Apply] をクリックします。

CLI の設定例

次の例は、「高速安全ローミングをサポートするアクセス ポイントの設定」(P.12-18)に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# dot11 ssid NewSSID
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2 cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid NewSSID
AP(config-if)# exit
AP(config)# end
```

この例では、SSID *NewSSID* が CCKM で EAP をサポートするように設定され、AES CCMP 暗号スイートが 2.4 GHz 無線インターフェイスで有効にされます。SSID *NewSSID* は、2.4 GHz 無線インターフェイスで有効にされます。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

802.11r のサポート

802.11r のサポートは、自律アクセス ポイントで提供されます。WGB、非ルート ブリッジ、およびリピータは、802.11r ではサポートされません。これは、クライアントのみをサポートします。

無線ドメイン サービスでは、次のタイプのローミングをサポートします。

- 分散システム（DS）上の Fast Transition
- 無線経由の Fast Transition

802.11r は、Cisco Centralized Key Management（CCKM）および Pairwise Master Key Identifier（PMKID）のローミングとは次のように異なります。

- ローミングする前に最初の認証が行われる
- 無線経由または DS を使用したターゲット AP との認証に既存アクセス ポイントの通信チャネルを使用する

802.11r の有効化

802.11r を有効にするには、次の手順を実行します。

ステップ 1　[Network] > [Network interface] を選択します。

ステップ 2　[Settings] タブをクリックします。

ステップ 3　[Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] を選択します。

ステップ 4　11r 設定の [enable] オプション ボタンをクリックします。

ステップ 5　[over-air] または [over-ds] オプション ボタンをクリックします。

ステップ 6　再アソシエーションの時間を入力します。

値の範囲は 20 ～ 1200 です。

ステップ 7　[Apply] をクリックします。

アクセス ポイントの CLI で 802.11r を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** <*ssid*>	SSID を設定します。
ステップ 3	**authentication key-management wpa version 2 dot11r**	アクセス ポイントに 802.11r を設定します。
ステップ 4	**interface dot11radio** {*0* | *1*}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線は Radio 0、5 GHz 無線は Radio 1 です。
ステップ 5	**dot11 dot11r pre-authentication {over-air | over-ds}**	[over-air] または [over-ds] の移行を有効または無効にします。
ステップ 6	**dot11 dot11r re-association timer** <*value*>	再アソシエーション タイマーを設定します。

管理フレーム保護の設定

管理フレーム保護の動作には WDS が必要です。MFP は、アクセス ポイントおよび WDS で手動で設定できます。

（注）　管理プラットフォームを使用しなければ、MFP は検出した侵入をレポートできないため、有効性が限定されます。

完全に保護するには、MFP アクセス ポイントで Simple Network Transfer Protocol（SNTP）も設定します。

管理フレーム保護

管理フレーム保護は、アクセス ポイントとクライアント ステーション間で転送される管理メッセージにセキュリティ機能を提供します。MFP は、インフラストラクチャ MFP とクライアント MFP の 2 つの機能コンポーネントで構成されます。

インフラストラクチャ MFP は、インフラストラクチャ サポートを提供します。インフラストラクチャ MFP は、不正デバイスおよびサービス拒絶攻撃の検出に有益なブロードキャストおよび誘導された管理フレームに対する Message Integrity Check（MIC; メッセージ完全性チェック）を利用します。クライアント MFP はクライアントをサポートします。クライアント MFP は、WLAN に対する一般的な攻撃の多くを無力化することによって、認証されたクライアントをスプーフィングされたフレームから保護します。

クライアント MFP の概要

クライアント MFP は、アクセス ポイントと CCXv5 対応のクライアント ステーション間で送信されるクラス 3 管理フレームを暗号化し、スプーフィングされたクラス 3 管理フレーム（AP と認証されてアソシエートされたクライアント ステーションとの間で送信される管理フレーム）をドロップすることによって AP とクライアントの両方が予防措置を実行できるようにします。クライアント MFP は、IEEE 802.11i に規定されたセキュリティ メカニズムを使用して、クラス 3 ユニキャスト管理フレームを保護します。再アソシエーション要求の RSNIE で STA によって決定されたユニキャスト暗号スイートによって、ユニキャスト データとクラス 3 管理フレームの両方が保護されます。ワークグループ ブリッジ、リピータ、または非ルート ブリッジ モードのアクセス ポイントでクライアント MFP を使用するには、TKIP または AES-CCMP のいずれかのネゴシエーションが必要です。

ユニキャスト クラス 3 管理フレームは、すでにデータ フレームに使用されている方法と同様にして AES-CCMP または TKIP のいずれかを適用することによって保護されます。クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、自律アクセス ポイントで有効化されます。

ブロードキャスト フレームを使用した攻撃を防ぐため、クライアント MFP 用に設定された 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 管理フレームをいっさい送信しません。クライアント MFP が有効化されている場合、ワークグループ ブリッジ、リピータ、または非ルート ブリッジ モードのアクセス ポイントでは、ブロードキャスト クラス 3 の管理フレームが廃棄されます。

クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、自律アクセス ポイントで有効化されます。

（注） シスコでは、WPA2 を使用すること、および WPA バージョン 2 では TKIP を実装しないことを推奨しています。このモードは非推奨となっているためです。

ルート モードのアクセス ポイントのクライアント MFP

ルート モードの自律アクセス ポイントでは、混合モードのクライアントがサポートされます。CCXv5 に対応し、WPAv2 の暗号スイート AES または TKIP が決定されているクライアントでは、クライアント MFP は有効です。CCXv5 に対応していないクライアントでは、クライアント MFP は無効です。デフォルトでは、クライアント MFP はアクセス ポイント上の特定の SSID に対するオプションで、SSID コンフィギュレーション モードで CLI を使用して有効と無効を切り替えることができます。

特定の SSID に、クライアント MFP を必須とするか、オプションとするかを設定できます。クライアント MFP を必須に設定するには、SSID でキー管理 WPA バージョン 2 を必須に設定します。キー管理が WPAv2 必須に設定されていない場合、エラー メッセージが表示され、CLI コマンドが拒否されます。クライアント MFP を必須として設定したキー管理およびキー管理 WPAv2 を変更しようとすると、エラー メッセージが表示され、CLI コマンドが拒否されます。オプションとして設定されている場合、クライアント MFP は SSID で WPAv2 に対応している場合に限り有効化され、対応していない場合にはクライアント MFP は無効化されます。

クライアント MFP の設定

コマンド	説明
ids mfp client required	この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP を必須として有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。また、このコマンドでは、SSID で WPA バージョン 2 が必須として設定されていることが要求されます。SSID で WPAv2 が必須として設定されていない場合、エラーメッセージが表示され、コマンドが拒否されます。 このコマンドの **no** 形式は、特定の SSID でクライアント MFP を無効にします。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。
ids mfp client optional	この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP をオプションとして有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。クライアント MFP は SSID で WPAv2 に対応している場合に限り、特定の SSID に対して有効化され、対応していない場合にはクライアント MFP は無効化されます。
authentication key management wpa version {1|2}	このコマンドを使用すると、特定の SSID の WPA キー管理に使用される WPA バージョンが明示的に指定されます。

コマンド	説明
dot11 ids mfp {generator | detector}	アクセス ポイントを MFP ジェネレータとして設定します。有効にすると、アクセス ポイントは Message Integrity Check Information Element（MIC IE; メッセージ完全性チェック情報エレメント）を各フレームに追加して、送信する管理フレームを保護します。フレームのコピー、改変、またはリプレイなどの攻撃が仕掛けられた場合、フレームは MIC を無効にし、MFP フレームを検出（検証）するように設定された受信アクセス ポイントのすべてで不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。 アクセス ポイントを MFP ディテクタとして設定します。有効にすると、アクセス ポイントで他のアクセス ポイントから受信した管理フレームが検証されます。有効および予測された MIC IE が含まれないフレームを受信すると、WDS に不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。
sntp server *server IP address*	SNTP サーバの名前または IP アドレスを入力します。
dot11 ids mfp distributor	グローバル コンフィギュレーション モードで、このコマンドを使用して WDS を MFP ディストリビュータとして設定します。有効にすると、WDS では署名キーが管理されます。このキーは MIC IE の作成に使用され、ジェネレータとディストリビュータ間で安全に転送されます。

Dot11Radio インターフェイスで以下の CLI コマンドを使用することで、アクセス ポイント コンソールのクライアント MFP に関する統計情報を表示およびクリアできます。

コマンド	説明
show dot11 ids mfp client statistics	このコマンドを使用すると、Dot11Radio インターフェイスのアクセス ポイント コンソールにクライアント MFP 統計が表示されます。
clear dot11 ids mfp client statistics	このコマンドを使用すると、クライアント MFP 統計がクリアされます。

802.11w による管理フレームの保護

現在の 802.11 標準は、無線リンクの管理および制御に使用するフレーム タイプを定義します。802.11 プロトコルに含まれる管理フレームは、WLAN に最高レベルのセキュリティが使用されている場合でも、認証も暗号化もされません。802.11w は、IEEE 802.11 標準ファミリの管理フレーム保護標準です。

802.11w は 3 種類の新しいセキュリティを提供することにより、管理フレームのセキュリティを向上します。

- データ送信元の信頼性
- リプレイ検出
- 堅牢な管理フレーム保護。

保護できる管理フレームは次のとおりです。

- ディスアソシエーション
- 認証解除
- パブリック アクション フレームを除くロバスト アクション フレーム

802.11w を使用して、アソシエーション要求のリプレイ攻撃を防ぐこともできます。802.11w が提供する保護は、Cisco クライアント MFP が提供する保護とある程度同等です。ただし、802.11w では Cisco インフラストラクチャ MFP と同等のメカニズムを提供していません。

Cisco クライアント MFP を有効にするには、保護対象のクライアントが CCXv5 をサポートすることを確認する必要があります。802.11w を有効にするには、保護対象のクライアントが 802.11w をサポートすることを確認する必要があります。

同じ SSID で Cisco インフラストラクチャ MFP と 802.11w の両方を有効にすることができます。ただし、同じ SSID と同じ無線の両方で Cisco クライアント MFP と 802.11w を有効にすることはできません。

802.11w を有効にするには、次の手順を実行します。

ステップ 1　アクセス ポイントの GUI で [Secuirty] ページを表示します。

ステップ 2　[SSID Manager] を選択します。

ステップ 3　[Client Authenticated Key Management] ページでは、次の操作を実行できます。

- 802.11w をサポートするクライアントだけが SSID に参加できるようにするには、[11w Configuration Required] オプション ボタンをクリックします。
- 802.11w をサポートするクライアントと 802.11w をサポートしないクライアントの両方が SSID に参加できるようにするには、[11w Configuration Optional] オプション ボタンをクリックします。

ステップ 4　[11w Association-comeback] の時間を入力します。

ステップ 5　[11w Saquery-retry] の時間を入力します。

次の CLI コマンドは、アクセス ポイントの 802.11w を有効にするために使用されます。

ap(config-ssid)# **11w-pmf client** *required/optional*

次の CLI コマンドは、アソシエーションのタイム アウトと saquery の再試行間隔を設定するために使用されます。

ap(config-ssid)# **11w-pmf association-comeback** *1000-20000ms*

ap(config-ssid)# **11w-pmf saquery-retry** *100-500ms*

これらのコマンドは任意です。これらのコマンドを使用しない場合、デフォルトの間隔が設定されます。アクセス ポイントに 802.11w を設定するには、MFP クライアントを無効にする必要があります。

（注）　WPAv2/AES は 802.11w では必須です。

（注）　802.11r を有効にすると、CCKM、11r 高速ローミング、DLS、無線測定、およびデュアル パブリック アクション フレーム保護はサポートされなくなります。

無線管理の設定

WDS を使用するように無線 LAN 上のアクセス ポイントを設定すると、アクセス ポイントは WDS デバイスと対話するときに自動的に無線管理における役割を果たします。無線管理の設定を行うには、ネットワーク上の管理プラットフォームと対話するように WDS デバイスを設定します。

WDS デバイスとして設定されたアクセス ポイント上の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　[Wireless Services Summary] ページを表示します。

ステップ 2　[WDS] をクリックして [General Setup] ページを表示します。

ステップ 3　[***Configure Wireless Network Manager***] チェックボックスをオンにします。

ステップ 4　[***Wireless Network Manager IP Address***] フィールドに、ネットワーク上の 管理プラットフォームの IP アドレスを入力します。

ステップ 5　[Apply] をクリックします。WDS アクセス ポイントが管理プラットフォームと対話するように設定されます。

CLI の設定例

次の例は、「無線管理の設定」(P.12-26)に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

この例では、WDS アクセス ポイントは、IP アドレスが 192.250.0.5 の管理プラットフォームと対話できるようになります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

WIDS に参加するようにアクセス ポイントを設定する

WIDS に参加するには、WDS と無線管理に参加するようにアクセス ポイントを設定する必要があります。WDS と無線管理に参加するようにアクセス ポイントを設定するには、「アクセス ポイントを WDS デバイスを使用するように設定する」(P.12-10)と「無線管理の設定」(P.12-26)の手順を実行します。

アクセス ポイントをスキャナ モードに設定する

スキャナ モードの場合、アクセス ポイントは無線活動のチャネルをすべてスキャンし、その活動をネットワーク上の WDS デバイスに報告します。スキャナ アクセス ポイントは、クライアント アソシエーションを受け付けません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに無線ネットワークの役割をスキャナに設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio { 0 | 1 }**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**station role scanner**	アクセス ポイントの役割をスキャナに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。

アクセス ポイントをモニタ モードに設定する

アクセス ポイントをスキャナとして設定すると、モニタ モードでフレームのキャプチャも可能になります。モニタ モードでは、アクセス ポイントは 802.11 フレームをキャプチャし、これをネットワーク上で WIDS エンジンに転送します。アクセス ポイントは、転送するすべての 802.11 フレームに 28 バイトのキャプチャ ヘッダーを追加します。ネットワーク上の WIDS エンジンは、このヘッダー情報を分析に使用します。アクセス ポイントは、キャプチャしたフレームの転送に UDP パケットを使用します。ネットワーク帯域幅を節約するため、複数のキャプチャしたフレームを 1 つの UDP パケットに結合できます。

スキャナ モードでは、アクセス ポイントは無線活動のすべてのチャネルをスキャンします。ただし、モニタ モードの場合、アクセス ポイントは、アクセス ポイント無線が設定されているチャネルだけをモニタします。

（注） アクセス ポイントに 2 つ無線が含まれている場合、インターフェイス上でモニタ モードを設定するには、無線が両方ともスキャナ モードに設定されている必要があります。

特権 EXEC モードから、次の手順に従って 802.11 フレームをキャプチャして転送するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 | 1}**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 3	**monitor frames endpoint ip address** *IP-address* **port** *UDP-port* [**truncate** *truncation-length*]	モニタ モードに無線を設定します。ネットワーク上の WIDS エンジン上で、IP アドレスと UDP ポートを入力します。 • （任意）転送したフレームごとに、バイト単位で最大長を設定します。アクセス ポイントは、この値より長いフレームを切り捨てます。デフォルトの長さは 128 バイトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。

モニタ モード統計の表示

show wlccp ap rm monitor statistics グローバル コンフィギュレーション コマンドを使用して、キャプチャしたフレームの統計を表示します。

次に、コマンドの出力例を示します。

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
====================
WLAN Monitoring           : Enabled
Endpoint IP address       : 10.91.107.19
Endpoint port             : 2000
Frame Truncation Length   : 535 bytes

Dot11Radio 1
====================
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=========================
Total No.of frames rx by DOT11 driver      : 58475
Total No.of Dot11 no buffers               : 361
Total No.of Frames Q Failed                : 0
Current No.of frames in SCAN Q             : 0

Total No.of frames captured                : 0
Total No.of data frames captured           : 425
Total No.of control frames captured        : 1957
Total No.of Mgmt frames captured           : 20287
Total No.of CRC errored frames captured: 0

Total No.of captured frames forwarded      : 23179
Total No.of captured frames forward failed : 0
```

clear wlccp ap rm statistics コマンドを使用して、モニタ モード統計を消去します。

モニタ モード制限の設定

モニタ モードでアクセス ポイントが使用するしきい値を設定できます。しきい値を超えると、アクセス ポイントは、情報をログに記録するかまたは警告を送信します。

認証失敗制限の設定

認証失敗制限を設定すると、*EAPOL フラッディング*と呼ばれるサービス拒絶攻撃からネットワークを保護できます。クライアントとアクセス ポイントとの間で発生する 802.1X 認証により、アクセス ポイント、オーセンティケータ、および EAPOL メッセージングを使用する認証サーバの間に、一連のメッセージが表示されます。通常、RADIUS サーバである認証サーバは、過度に認証が試みられるとすぐに負荷に耐えられなくなります。規制されていない場合、1 台のクライアントからネットワークに影響を与えるほどの認証要求が発生する可能性があります。

モニタ モードでは、アクセス ポイントは 802.1X クライアントがアクセス ポイントを通じて認証を試みる割合をトラッキングします。過度な認証の試みによってネットワークが攻撃される場合、アクセス ポイントは、認証しきい値を超えると警告を発します。

これらの制限はアクセス ポイント上で設定できます。

- アクセス ポイントからの 802.1X の試みの回数
- アクセス ポイント上の秒単位での EAPOL フラッドの期間

アクセス ポイントは、過度の認証の試みを検出すると、この情報を示すための MIB 変数を設定します。

- EAPOL フラッドが検出されました
- 認証の試みの回数
- 認証の試みの回数が最も多いクライアントの MAC アドレス

特権 EXEC モードから、次の手順に従って、アクセス ポイント上の失敗をトリガーする認証制限を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ids eap attempts** *number* **period** *seconds*	認証の試みの回数と、アクセス ポイント上で失敗をトリガーする EAPOL フラッドの秒数を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。

802.11u Hotspot および Hotspot 2.0 の設定

802.11u Hotspot 機能により、IEEE 802.11 デバイスは外部ネットワークと対話できます。この機能はホットスポットやその他のパブリック ネットワークで、サービスがサブスクリプションベースであるか無料であるかを問わずに使用されます。

この機能は、ネットワークの検出や選択を支援し、外部ネットワークから情報を転送できるようにします。アソシエーション前にネットワークに関する情報をステーションに提供します。インターワーキングは、家、企業、およびパブリック アクセスのユーザに役立つだけでなく、製造業者やオペレータが IEEE 802.11 カスタマーに共通のコンポーネントおよびサービスを提供するのにも役立ちます。

802.11u Hotspot を設定する前に、次の条件が満たされていることを確認してください。

- WPA キー管理
- 複数の基本 SSID

802.11u Hotspot および Hotspot 2.0 を設定するには、次の手順に従います。

ステップ 1　ap(config-ssid)# モードを開始します。

ステップ 2　以下のコマンドを入力して、802.11u Hotspot を有効にして、設定します。

a. hotspot dot11u enable

b. hotspot dot11u domain *index domain_name*

c. hotspot dot11u network-type *network_type internet_availabily_status(0 or 1)*

d. hotspot dot11u auth-type *auth_type*

e. hotspot dot11u ipaddr-type *ipv4type ipv6type*

f. hotspot dot11u hessid *h.h.h*

g. hotspot dot11u nai-realm *index* realm-name *name_string*

h. hotspot dot11u nai-realm *index* eap-method *eap-index eap_method*

i. hotspot dot11u nai-realm *index* auth-method *eap-index auth-index auth_type auth_subtype*

j. hotspot dot11u roam-oi *index hex-string isbeacon*

k. hotspot dot11u 3gpp-info *index mobile_country_code mobile_network_code*

例：802.11u Hotspot の有効化

```
ap(config-ssid)# hotspot dot11u enable
ap(config-ssid)# hotspot dot11u domain 1 cisco
ap(config-ssid)# hotspot dot11u network-type  2   1
ap(config-ssid)# hotspot dot11u auth-type  1
ap(config-ssid)# hotspot dot11u ipaddr-type 2 2
ap(config-ssid)# hotspot dot11u hessid 1234.5678.1234
ap(config-ssid)# hotspot dot11u nai-realm 1 realm-name cisco
ap(config-ssid)# hotspot dot11u nai-realm 1 eap-method 1 17
ap(config-ssid)# hotspot dot11u nai-realm 1 auth-method  1 1 1 2
ap(config-ssid)# hotspot dot11u roam-oi 1 004096 1
ap(config-ssid)# hotspot dot11u 3gpp-info 1 123 123
```

ステップ 3　以下のコマンドを入力して、802.11u Hotspot 2.0 を有効にして、設定します。

a. hotspot hs2 enable

b. hotspot hs2 operator-name *index language_code operator_name*

c. hotspot hs2 wan-metrics *link_status symmetric_link_status uplink_speed downlink_speed*

d. hotspot hs2 port-config *ip_protocol port_number port_status*

例：802.11u Hotspot 2.0 の有効化

```
ap(config-ssid)# hotspot hs2 enable
ap(config-ssid)# hotspot hs2 operator-name 1 eng cisco
ap(config-ssid)# hotspot hs2 wan-metrics 1 1 2345 3434
ap(config-ssid)# hotspot hs2 port-config 1 23 34 2
```

ステップ 4　次のグローバル コンフィギュレーション コマンドを入力します。

a. dot11 dot11u ap-venue name *name_string*

b. dot11 dot11u ap-venue type *venue_group venue_type*

例：グローバル コンフィギュレーション コマンド：

```
ap(config)# dot11 dot11u ap-venue name cisco_odc
ap(config)# dot11 dot11u ap-venue type 2 2
```

802.11u Hotspot および Hotspot 2.0 の設定をデバッグするには、コマンド **debug dot11 dot11u** を使用します。

GUI を使用して 802.11u Hotspot や Hotspot 2.0 を有効にして設定するには、[Security] > [Dot11u Manager] に移動します。

RADIUS サーバと TACACS+ サーバの設定

この章では、Remote Authentication Dial-In User Service（RADIUS）と Terminal Access Controller Access Control System Plus（TACACS+）を有効にして設定する方法について説明します。これは、認証プロセスと許可プロセスに詳細なアカウンティング情報と柔軟な管理制御を提供します。RADIUS と TACACS+は AAA を通じて効率化され、AAA コマンド以外では有効に設定できません。

（注） アクセス ポイントをローカル認証サーバとして設定し、メイン サーバのバックアップとして使用したり、RADIUS サーバの存在しないネットワークで認証サービスを提供したりできます。アクセス ポイントをローカル認証サーバとして設定する方法の詳細については、第 11 章「認証タイプの設定」を参照してください。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、リリース 12.2 の『*Cisco IOS Security Command Reference*』を参照してください。

RADIUS の設定と有効化

この項では、RADIUS を設定して有効にする方法について説明します。次の各項で RADIUS の設定について説明します。

RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。RADIUS クライアントは RADIUS をサポートするシスコ デバイス上で動作し、中央 RADIUS サーバに認証要求を送信します。RADIUS サーバには、ユーザ認証情報とネットワーク サービス アクセス情報がすべて格納されます。通常、RADIUS ホストは、シスコ（Cisco Identity Services Engine）、FreeRADIUS、Microsoft、または他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS は、次のようなアクセス セキュリティを必要とするネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。マルチ ベンダーのアクセス サーバを使用する IP ベースのネットワークでは、ダイヤルイン ユーザは Kerberos セキュリティ システムと連携するようにカスタマイズされた RADIUS サーバを通じて認証されます。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。これは、*スマート カード* アクセス コントロール システムを使用するようなアクセス環境です。
- すでに RADIUS を使用中のネットワーク。ネットワークには、RADIUS クライアントを含むシスコ アクセス ポイントを追加できます。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境の場合、RADIUS では、たとえば AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD 接続をサポートしていません。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

RADIUS の動作

無線ユーザが、RADIUS サーバによってアクセス コントロールされるアクセス ポイントにログインして認証を試行する場合、ネットワークの認証は図 13-1に示す手順で実行されます。

図 13-1　EAP 認証のシーケンス

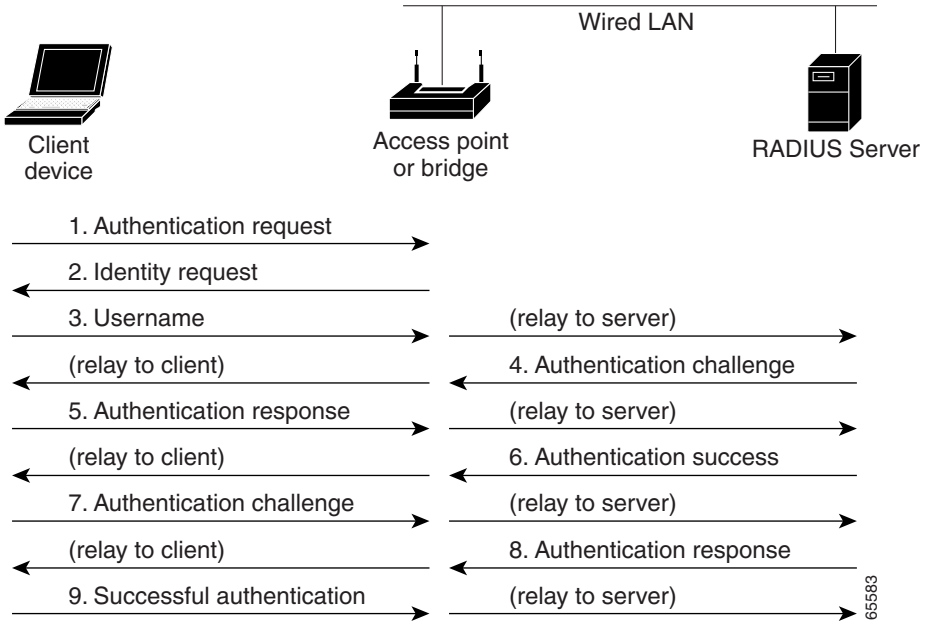


図 13-1 に示すように、まず、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。初期フェーズは 802.11 Open 認証およびアソシエーションです。次に、EAP プロセスが開始します。

AP は無線リンクで EAP/802.1x を使用してクライアントと通信し、RADIUS カプセル化を使用して RADIUS サーバにクライアント メッセージを中継します。クライアントと認証サーバが EAP 方式に同意すると、RADIUS サーバはクライアントに認証身元証明要求を送信します。

一部の EAP 方式でも、クライアントは RADUIS サーバに対して認証を行ってからでないと、サーバから身元証明要求を受け入れることができません。いずれの場合も、クレデンシャル交換は暗号化され、傍受者が読み取ることはできません。

（一方向または双方向の）認証が完了し、WPA/WPA2 が使用されている場合は、RADIUS サーバとクライアントが Pairwise Master Key（PMK）と呼ばれる初期キーを派生させます。クライアントと RADIUS サーバは同じ方式を使用して PKM を派生させるため、派生される PMK は同じです。ただし、PMK は無線リンクでは交換されません。

RADIUS サーバは PMK のコピーを AP に送信します。AP とクライアントは、この PMK を使用してユニキャスト暗号キーを派生させます。クライアント セッション中は、このキーが、クライアントと AP 間での交換を暗号化するために使用されます。AP は、ブロードキャスト キー（セル内のすべてのクライアントにブロードキャストされるトラフィックを暗号化するために使用するキー）をクライアントに通知する際にも、このユニキャスト暗号キーを使用します。

複数の EAP 認証タイプがありますが、どのタイプでもアクセス ポイントは同じように動作します。AP は、無線クライアント デバイスと RADIUS サーバの間で、認証メッセージを中継します。RADIUS サーバを使用したクライアント認証の設定方法の詳細は、「SSID への認証タイプの割り当て」（P.11-10）を参照してください。

RADIUS の設定

この項では、RADIUS をサポートするアクセス ポイントの設定方法について説明します。少なくとも、RADIUS サーバ ソフトウェアを実行するホスト（1 つまたは複数）を特定し、RADIUS 認証方式のリストを定義する必要があります。また、任意で RADIUS 許可およびアカウンティングの方式リストを定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

アクセス ポイントに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして設定する必要があります。

ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」（P.13-4）
- 「RADIUS サーバ ホストの識別」（P.13-5）（必須）
- 「RADIUS ログイン認証の設定」（P.13-7）（必須）
- 「AAA サーバ グループの定義」（P.13-9）（任意）
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」（P.13-11）（任意）
- 「パケット オブ ディスコネクトの設定」（P.13-12）（任意）
- 「RADIUS アカウンティングの起動」（P.13-14）（任意）
- 「すべての RADIUS サーバの設定」（P.13-15）（任意）
- 「すべての RADIUS サーバの設定」（P.13-15）（任意）
- 「ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定」（P.13-16）（任意）
- 「ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定」（P.13-17）（任意）
- 「WISPr RADIUS 属性の設定」（P.13-18）（任意）

（注）　RADIUS サーバの CLI コマンドは、**aaa new-model** コマンドを入力するまで無効になっています。

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてアクセス ポイントにアクセスするユーザを認証できます。

RADIUS サーバ ホストの識別

アクセス ポイントと RADIUS サーバ間の通信には、次のいくつかのコンポーネントを使用します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定のユーザ データグラム プロトコル（UDP）ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号の組み合わせから一意の識別子が作成され、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

（注）　Cisco IOS Release 12.2(8)JA 以降では、RADIUS サーバとアクセス ポイントとの通信に、21645 ～ 21844 の範囲で無作為に選択された UDP ソース ポート番号が使用されます。

同一の RADIUS サーバにアカウンティングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。この例では、最初に設定されたホスト エントリがアカウンティング サービスに失敗すると、アクセス ポイントは同じデバイスに設定された 2 番目のホスト エントリにアカウンティング サービスの提供を求めます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとアクセス ポイントは、共有の身元証明要求テキスト ストリングを使用して、パスワードを暗号化して応答を交換します。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デーモンを実行しているホストと、アクセス ポイントと共有する身元証明要求テキスト（キー）ストリングを指定する必要があります。

タイムアウト、再送信、暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することも、またはグローバル設定とサーバ単位の設定を組み合わせることも可能です。アクセス ポイントと通信するすべての RADIUS サーバにこれらの設定をグローバルに適用するには、3 つの一意なグローバル コンフィギュレーション コマンド（**radius-server timeout**、**radius-server retransmit**、**radius-server key**）を使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。

（注）　アクセス ポイントにグローバル機能とサーバ単位の機能（タイムアウト、再送信、キー コマンド）を同時に設定する場合、サーバ単位のタイマー、再送信、キー値のコマンドがグローバルなタイマー、再送信、キー値のコマンドに優先します。すべての RADIUS サーバに対してこれらの値を設定するには、「すべての RADIUS サーバの設定」（P.13-15）を参照してください。

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようアクセス ポイントを設定できます。詳細については、「AAA サーバ グループの定義」（P.13-9）を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**radius-server** {hostname | ip-address}[**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **（注）** このコマンドは、以前のリリースでサポートされていたものです。次の新しいコマンドの使用が推奨されます。 **radius server** *name* **address** [**IP address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] **address** {**ipv4** *radius-server-IPv4-Address* | **ipv6** *radius-server-IPv6-Address*}	リモート RADIUS サーバ ホストのサーバ名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。（任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout***seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、アクセス ポイントと RADIUS サーバで稼働中の RADIUS デーモンの間で使用される認証と暗号キーを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**dot11 ssid** *ssid-string*	アカウンティングを有効にする必要がある、Service Set Identifier（SSID; サービス セット ID）の SSID コンフィギュレーション モードを開始します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。

	コマンド	目的
ステップ 5	**accounting** *list-name*	この SSID の RADIUS アカウンティングを有効にします。*list-name* には、アカウンティング方式のリストを指定します。方式のリストの詳細は、次の URL をクリックしてください。 http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html （注）　SSID のアカウンティングを有効にするには、SSID 設定に **accounting** コマンドを含める必要があります。URL をクリックすると、SSID コンフィギュレーション モード **accounting** コマンドの詳細が表示されます。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例は、RADIUS アカウンティング用に SSID を設定する方法を示しています。

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

次に、*host1* を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
AP(config)# radius-server host host1
```

（注）　RADIUS サーバ上でも、いくつかの値を設定する必要があります。その設定には、アクセス ポイントの IP アドレスおよびサーバとアクセス ポイントで共有するキー ストリングが含まれます。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。リスト名の詳細については、このリンクをクリックしてください：http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **line**：回線パスワードを認証に使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別」（P.13-5）を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンド	目的
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**radius-server attribute 32 include-in-access-req format** {**%h** | **%i** | **%d**}	(任意)認証用に NAS_ID 属性でシステム名を送信するようにアクセス ポイントを設定します。 • %i:IP アドレス • %h:ホスト名 • %d:ドメイン名
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** \| *list-name*} ライン コンフィギュレーション コマンドを使用します。

AAA サーバ グループの定義

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようアクセス ポイントを設定できます。設定済みのサーバ ホストのサブセットを選択して、それを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

サーバ グループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID(IP アドレスと UDP ポート番号の組み合わせ)を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同一の RADIUS サーバにアカウンティングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。

定義したグループ サーバに特定のサーバを対応付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバ グループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout***seconds* には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、アクセス ポイントと RADIUS サーバで稼働中の RADIUS デーモンの間で使用される認証と暗号キーを指定します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループを、特定のグループ名で定義します。 このコマンドを実行すると、アクセス ポイントはサーバ グループ コンフィギュレーション モードへ移行します。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」(P.13-7)を参照してください。

特定の RADIUS サーバを削除するには、**no radius-server host** {*hostname* | *ip-address*} グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server radius** *group-name* グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、アクセス ポイントは異なる 2 つの RADIUS グループ サーバ(*group1* と *group2*)を認識するように設定されます。group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

(注) RADIUS グループの各 RADUIS サーバ ホストに定義されるポートは、グローバル コンフィギュレーション モードで作成された各 RADIUS サーバ ホスト エントリごとに個別に定義されているポートをオーバーライドします。

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可が有効の場合、アクセス ポイントはユーザのプロファイルから取得した情報を使用してユーザのセッションを設定します。ユーザのプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

(注) この項では、アクセス ポイント管理者向けの許可の設定について説明します。無線クライアント デバイス向けの許可の設定は説明しません。無線クライアント デバイスと無線ネットワーク アクセス許可では、特定の許可プロファイルを RADIUS サーバから返す必要はありません。

グローバル コンフィギュレーション コマンド **aaa authorization** と **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec radius local コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにアクセス ポイントを設定します。
ステップ 3	**aaa authorization exec radius**	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、アクセス ポイントを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

パケット オブ ディスコネクトの設定

Packet of Disconnect（PoD; パケット オブ ディスコネクト）は、ディスコネクト メッセージとも呼ばれています。PoD の詳細は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）Internet Standard RFC 3576 で参照できます。

パケット オブ ディスコネクトは、検出されたセッションを終了させる方式で構成されています。PoD は RADIUS Disconnect_Request パケットであり、RADIUS access_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。

セッションが終了すると、RADIUS サーバは Network Access Server（NAS; ネットワーク アクセス サーバ）（WDS またはアクセス ポイント）に切断メッセージを送信します。802.11 セッションには、Pod 要求で Calling-Station-ID [31] RADIUS 属性（クライアントの MAC アドレス）を指定する必要があります。アクセス ポイントまたは WDS は、関連するセッションのアソシエーションを解除しようとし、次に接続解除応答メッセージを RADIUS サーバに返送します。メッセージ タイプは次のとおりです。

- 40：切断要求
- 41：切断：ACK
- 42：切断：NAK

（注）　PoD 要求の設定法については、ご使用の RADIUS サーバ アプリケーションの資料を参照してください。

（注）　アクセス ポイントは、再アソシエートしようとするクライアントの次の試みを妨害しません。PoD 要求を発行する前にクライアントのアカウントを無効にするのは、セキュリティ管理者の責任です。

（注）　WDS を設定すると、PoD 要求は WDS に対して発行されます。WDS はアソシエーション解除の要求を親アクセス ポイントに転送してから、そのセッションを自身の内部テーブルから削除します。

特権 EXEC モードから、次の手順に従って PoD を設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa pod server** [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] [**clients** *client 1...*] [**ignore** {**server-key** *string...*| **session-key** }] | **server-key** *string...*]}	特定のセッション属性が提供されると、RADIUS サーバからの要求により切断されるユーザ セッションを有効にします。 **port** *port number*：（任意）アクセス ポイントが PoD 要求をリッスンする UDP ポート。デフォルト値は 1700 です。 **auth-type**：このパラメータは、802.11 セッションに対してはサポートされません。 **clients**（任意）：4 台までの RADIUS サーバをクライアントとして指名できます。この設定が存在し、リストにないデバイスからの PoD 要求が発信される場合、拒否されます。 **ignore**（任意）：*server_key* に設定すると、PoD 要求を受信したときに共有の身元証明要求は検証されません。 **session-key**：802.11 セッションに対してはサポートされません。 **server-key**：共有秘密テキスト ストリングを設定します。 *string*：ネットワーク アクセス サーバとクライアント ワークステーション間で共有される事前共有キー。この共有身元証明要求は両方のシステムで同一である必要があります。 （注）　このパラメータ以降に入力されたデータは、共有の身元証明要求ストリングとして扱われます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

CSID 形式の選択

RADIUS パケット内の Called-Station-ID（CSID）および Calling-Station-ID 属性に対する MAC アドレスの形式を選択できます。

Calling-Station-ID [31] RADIUS 属性は無線クライアントの MAC アドレスです。この属性は、たとえばアカウンティングや PoD のために RADIUS サーバに通知しなければならない場合があります。

dot11 aaa csid グローバル コンフィギュレーション コマンドを使用して CSID 形式を選択します。表 13-1 は、対応する MAC アドレスの例付きで示した形式のオプションです。

表 13-1　CSID 形式オプション

オプション	MAC アドレスの例
default	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

デフォルトの CSID 形式に戻すには、**dot11 aaa csid** コマンドで **no** を指定するか、**dot11 aaa csid default** と入力します。

（注）　また **wlccp wds aaa csid** コマンドを使用しても CSID 形式を選択できます。

RADIUS アカウンティングの起動

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形式でユーザ アクティビティを RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アクセス ポイントに送信される属性の詳細なリストについては、「アクセス ポイントが送信する RADIUS 属性」（P.13-20）を参照してください。

Cisco IOS の権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop radius**	ネットワーク関連のすべてのサービス要求について、RADIUS アカウンティングをイネーブルにします。
ステップ 3	**ip radius source-interface bvi1**	アカウンティングの記録として BVI IP アドレスを NAS_IP_ADDRESS 属性で送信するようにアクセス ポイントを設定します。
ステップ 4	**aaa accounting update periodic** *minutes*	アカウンティングの更新間隔を分で入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

すべての RADIUS サーバの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントとすべての RADIUS サーバ間のグローバル通信設定を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server key** *string*	アクセス ポイントとすべての RADIUS サーバ間で使用する共有の身元証明要求テキスト ストリングを指定します。 **(注)** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	アクセス ポイントが RADIUS 要求をサーバに送信して、中止するまでの回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	アクセス ポイントが RADIUS 要求を再送する前に、要求への応答を待機する時間を秒数で指定します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes*	このコマンドは、Cisco IOS ソフトウェアで認証要求に応答しない RADIUS サーバを「dead」とマークして、要求の待機がタイムアウトになる前に、設定された次のサーバを試行する場合に使用します。dead とマークされている RADIUS サーバでは、指定する時間の間(最大 1440 分、24 時間)、追加の要求はスキップされます。 **(注)** このコマンドは、複数の RADIUS サーバを定義するときに必要な設定です。設定しない場合、クライアントの認証が行われません。定義される RADIUS サーバが 1 台の場合、このコマンドはオプションです。
ステップ 6	**radius-server attribute 32 include-in-access-req format %h**	認証時に NAS_ID 属性でシステム名を送信するようにアクセス ポイントを設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定値を確認します。
ステップ 9	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例では、サーバのデッドタイムを 10 分間に指定した 2 つのメイン サーバを設定する方法を示します。

```
ap(config)# aaa new-model
ap(config)# radius server server1
ap(config-radius-server)# address ipv4 172.20.0.1 auth-port 1812 acct-port 1813
ap(config-radius-server)# key 0 cisco
ap(config-radius-server)# exit
ap(config)# radius server server2
ap(config-radius-server)# address ipv4 172.10.0.1 auth-port 1000 acct-port 1001
ap(config-radius-server)# key 0 cisco
ap(config-radius-server)# exit
ap(config)# radius-server deadtime 10
```

再送信、タイムアウト、デッドタイムをデフォルトの設定に戻すには、それぞれのコマンドで **no** 形式を使用します。

ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定

（注） 次の設定は、RADIUS サーバで行います。

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）のドラフト規格では、アクセス ポイントと RADIUS サーバ間で、ベンダー固有の属性（属性 26）を使用してベンダー固有の情報をやり取りする方法を指定しています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートされるオプションはベンダー タイプ 1、名前は *cisco-avpair* です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の許可タイプに使用するシスコのプロトコル属性の値です。*attribute* と *value* は、Cisco TACACS+ 仕様で定義された該当 AV ペアです。*sep* には、必須属性の場合は = を、オプション属性の場合はアスタリスク（*）を指定します。このコマンドにより、TACACS+ 許可で使用できる全機能が RADIUS でも使用できます。

たとえば、次の AV ペアは IP 許可の際（PPP の IPCP アドレス割り当ての際）、シスコの *multiple named ip address pools* 機能を有効にします。

```
cisco-avpair= ”ip:addr-pool=first“
```

次の例は、特権 EXEC コマンドへの即時アクセスを使用して、ユーザがアクセス ポイントからログインする方法を示しています。

```
cisco-avpair= ”shell:priv-lvl=15“
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。ベンダーの ID と VSA についての詳細は、RFC 2138「Remote Authentication Dian-In User Service（RADIUS）」を参照してください。

特権 EXEC モードから、次の手順に従って、VSA を認識して使用するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server vsa send** [**accounting** | **authentication**]	アクセス ポイントが RADIUS IETF 属性 26 で定義された VSA を認識して使用できるようにします。 • (任意)認識されるベンダー固有属性の集合をアカウンティング属性だけに限定するには、**accounting** キーワードを使用します。 • (任意)認識されるベンダー固有属性の集合を認証属性だけに限定するには、**authentication** キーワードを使用します。 キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定値を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

VSA 26 の RADIUS 属性の全リストや VSA 26 の詳細については、次の URL にある RADIUS ガイドを参照してください。
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定

IETF の RADIUS ドラフト規格では、アクセス ポイントと RADIUS サーバの間でベンダー専用の情報を通信する方法を指定していますが、一部のベンダーは RADIUS 属性セットを独自の方法で拡張しています。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

すでに説明したように、ベンダー専用または IETF ドラフト準拠の RADIUS を設定するには、RADIUS サーバ デーモンを実行しているホストと、そのホストがアクセス ポイントを共有する身元証明要求テキストを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ホストがベンダー専用の RADIUS 実装を使用していることを識別します。

	コマンド	目的
ステップ 3	**radius-server key** *string*	アクセス ポイントとベンダー専用の RADIUS サーバ間で使用する共有の身元証明要求テキスト ストリングを指定します。アクセス ポイントと RADIUS サーバは、このテキスト ストリングを使用して、パスワードを暗号化し応答を交換します。 **（注）** キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定値を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** グローバル コンフィギュレーション コマンド を使用します。キーをディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次の例は、ベンダー専用の RADIUS ホストを指定して、アクセス ポイントとサーバ間で秘密キー *rad124* を使用する方法を示しています。

```
AP(config)# radius server Myserver
AP(config-radius-server)# address ipv4 172.20.30.15
AP(config-radius-server)# key 0 rad1234
AP(config-radius-server)# non-standard
```

WISPr RADIUS 属性の設定

Wi-Fi Alliance の『*WISPr Best Current Practices for Wireless Internet Service Provider Roaming*』、および 2010 年に Wireless Broadband Alliance によって *WISPv2* という名前で発行された更新版 *Annex D* に、アクセス ポイントが RADIUS アカウンティングおよび認証要求で送信しなければならない RADIUS 属性がリストされています。現在アクセス ポイントは、WISPr ロケーション名、ISO と International Telecommunications Union（ITU; 国際電気通信連合）の国番号とエリア コード属性だけをサポートしています。**snmp-server location** コマンドと **dot11 location isocc** コマンドを使用して、アクセス ポイントでこれらの属性を設定します。

また、『*WISPr and WISPv2 Best Current Practices for Wireless Internet Service Provider Roaming (WISPr)*』には、RADIUS 認証応答とアカウンティング要求でクラス属性をアクセス ポイントに加えることも指示されています。アクセス ポイントは自動的にクラス属性を加えるため、設定する必要はありません。

ISO と ITU の国番号とエリア コードのリストは、ISO と ITU の Web サイトにあります。Cisco IOS ソフトウェアは、アクセス ポイントで設定された国番号とエリア コードの有効性を確認しません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに WISPr RADIUS 属性を指定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server location** *location*	WISPr の場所名属性を指定します。『*WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*』では、次の形式で場所名を入力することを推奨しています。 *hotspot_operator_name*,*location*
ステップ 3	**dot11 location isocc** *ISO-country-code* **cc** *country-code* **ac** *area-code*	アクセス ポイントがアカウンティング要求と認証要求に加える ISO と ITU の国番号とエリア コードを指定します。 • **isocc** *ISO-country-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ISO 国番号を指定します。 • **cc** *country-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU 国番号を指定します。 • **ac** *area-code*：アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU エリア コードを指定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定値を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例は、WISPr の場所名属性を設定する方法を示しています。

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

次の例は、アクセス ポイントで ISO と ITU のロケーション コードを設定する方法を示しています。

```
ap# dot11 location isocc us cc 1 ac 408
```

次の例は、アクセス ポイントがクライアント デバイスの使用する SSID を追加して場所 ID ストリングをフォーマットする方法を示しています。

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

RADIUS の設定の表示

RADIUS の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

（注）　アクセス ポイントで DNS が設定されている場合、**show running-config** コマンドはサーバの名前の代わりに IP アドレスを表示することがあります。

アクセス ポイントが送信する RADIUS 属性

表 13-2 から 表 13-6 は、アクセス ポイントがクライアントに送信するアクセス要求、アクセス許可、アカウンティング要求パケット中の属性を示しています。

（注）　Wi-Fi アライアンスの資料『*WISPr and WISPv2 Best Current Practices for Wireless Internet Service Provider Roaming (WISPr)*』で推奨されているように、RADIUS アカウンティング要求と認証要求の属性に加えるように、アクセス ポイントを設定できます。詳細は、「WISPr RADIUS 属性の設定」（P.13-18）を参照してください。

表 13-2　　アクセス要求パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier[1]
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

1. 属性 32（include-in-access-req）が設定されている場合、アクセス ポイントは NAS-Identifier を送信します。

表 13-3　　アクセス許可パケットで送信される属性

属性 ID	説明
25	クラス
27	Session-Timeout
64	Tunnel-Type[1]
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA（属性 26）	LEAP session-key
VSA（属性 26）	auth-algo-type
VSA（属性 26）	SSID

1. RFC2868、VLAN オーバーライド番号を定義

表 13-4　アカウンティング要求（開始）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	クラス
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	インターフェイス

表 13-5　アカウンティング要求（更新）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	クラス
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	VLAN-ID
VSA（属性 26）	Connect-Progress
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	インターフェイス

表 13-6　アカウンティング要求（終了）パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	クラス
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA（属性 26）	SSID
VSA（属性 26）	NAS-Location
VSA（属性 26）	Disc-Cause-Ext
VSA（属性 26）	VLAN-ID
VSA（属性 26）	Connect-Progress
VSA（属性 26）	Cisco-NAS-Port
VSA（属性 26）	インターフェイス
VSA（属性 26）	auth-algo-type

（注） デフォルトでは、アクセス ポイントは service-type 属性を authenticate-only に設定した状態で、再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、authenticate-only の service-type 属性をサポートしていないものがあります。ユーザの要件に応じて、service-type 属性を **dot11 aaa authentication attributes service-type login-user** または **dot11 aaa authentication attributes service-type framed-user** に設定してください。デフォルトでは、アクセス要求に応じてサービス タイプ「login」が送信されます。

TACACS+ の設定と有効化

ここでは、次の設定情報について説明します。

TACACS+ の概要

TACACS+ は、アクセス ポイントにアクセスしようとするユーザを集中的に検証するセキュリティ アプリケーションです。RADIUS とは異なり、TACACS+ はアクセス ポイントを介してネットワークにアクセスする無線クライアント デバイスの認証は行いません。

アクセス ポイントに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ(TACACS+ デーモン)が各サービス(認証、許可、およびアカウンティング)を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証:ログインとパスワードのダイアログ、身元証明要求と応答、メッセージのサポートを通じて管理者の認証を完全に制御します。

  認証機能は、管理者との対話を実行できます(たとえば、ユーザ名とパスワードが入力された後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号など、複数の質問でユーザの身元を確認します)。また TACACS+ 認証サービスは、管理者の画面にメッセージを送信できます。たとえば、会社のパスワード エージング ポリシーに従い、パスワードを変更する必要があることをメッセージで管理者に通知することができます。

- 許可:管理者のセッション期間中の管理機能を詳細に制御します。これには自動コマンドの設定、アクセス コントロール、セッション期間、またはプロトコル サポートなどが含まれますが、それに限定されません。また、管理者が TACACS+ 許可機能で実行できるコマンドを強制的に制限できます。

- アカウンティング:課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワーク マネージャはアカウンティング機能を使用して、セキュリティ監査時に管理者アクティビティを追跡したり、またはユーザの課金時に情報を提供できます。アカウンティング レコードには、管理者 ID、開始時間と終了時間、実行されたコマンド、パケット数、バイト数が含まれます。

TACACS+ プロトコルは、アクセス ポイントと TACACS+ デーモンの間で認証を実行します。アクセス ポイントと TACACS+ デーモンの間で実行されるすべてのプロトコル交換が暗号化されるため、認証の機密性を保証します。

アクセス ポイントで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。

TACACS+ の動作

管理者が TACACS+ を使用してアクセス ポイントの認証を受け、簡単な ASCII ログインを試行した場合、次のプロセスが発生します。

1. 接続が確立されると、アクセス ポイントは TACACS+ デーモンに連絡してユーザ名プロンプトを取得し、このプロンプトが管理者に表示されます。管理者がユーザ名を入力すると、アクセス ポイントは TACACS+ デーモンにアクセスしてパスワード プロンプトを取得します。アクセス ポイントは管理者にパスワード プロンプトを表示し、管理者がパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

   TACACS+ を使用してデーモンと管理者との間で会話が続けられ、デーモンは管理者の認証に必要な情報を取得します。デーモンはユーザ名とパスワードの組み合わせを求めるプロンプトを出しますが、たとえばユーザの母親の旧姓など、TACACS でユーザを識別するための必須情報として設定されている他の情報をプロンプトに含めることもできます。

2. アクセス ポイントは最終的に、TACACS+ デーモンから次に示す応答のいずれかを受信します。
   - ACCEPT：管理者が認証され、サービスが開始します。許可を要求するようにアクセス ポイントが設定されている場合、この時点で許可が開始します。
   - REJECT：管理者は認証されません。管理者は TACACS+ デーモンに従ってアクセスが拒否されるか、ログイン シーケンスを再試行するように要求されます。
   - ERROR：デーモンによる認証のある時点、またはデーモンとアクセス ポイント間のネットワーク接続のある時点で、エラーが発生しています。ERROR 応答を受信した場合、通常、アクセス ポイントは、別の方法で管理者の認証を試行します。
   - CONTINUE：管理者は追加の認証情報を要求されます。

   認証の後、アクセス ポイントで許可が有効になっている場合、管理者はさらに許可フェーズに進みます。管理者は TACACS+ 許可に進む前に、まず TACACS+ 認証を完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合、この応答には属性の形でその管理者に EXEC または NETWORK セッションを指示するデータが含まれており、管理者がアクセスできる下記のサービスを決定できます。
   - Telnet、rlogin、または特権 EXEC サービス
   - 接続パラメータ。ホストまたはクライアントの IP アドレス、アクセス リスト、管理者のタイムアウトが含まれます。

「Configuring TACACS+」

この項では、TACACS+ をサポートするアクセス ポイントの設定方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウンティングの方式リストを定義できます。方式リストは管理者アカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して、使用するセキュリティ プロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。このソフトウェアは、リストの先頭の方式を使用して管理者のアカウントを認証、許可、または管理します。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI および Web インターフェイスを介してアクセス ポイントにアクセスする管理者を認証できます。

TACACS+ サーバ ホストの特定および認証キーの設定

認証時に単一サーバまたは AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようにアクセス ポイントを設定できます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	TACACS+ サーバを維持する IP ホスト(1 つまたは複数)を特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • (任意)**port** *integer* には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ～ 65535 です。 • (任意)**timeout** *integer* には、タイム アウトになってアクセス ポイントがエラーを宣言するまでにデーモンからの応答を待機する時間を秒数で指定します。デフォルトは 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • (任意)**key** *string* には、アクセス ポイントと TACACS+ デーモンの間の全トラフィックを暗号化および復号化するための暗号キーを指定します。暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 4	**aaa group server tacacs+** *group-name*	(任意)AAA サーバ グループを、特定のグループ名で定義します。 このコマンドは、アクセス ポイントをサーバ グループサブコンフィギュレーション モードに移行します。
ステップ 5	**server** *ip-address*	(任意)特定の TACACS+ サーバを定義済みのサーバ グループに対応付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。 グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *hostname* グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、**no aaa group server tacacs+** *group-name* グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト(偶然に *default* と名前が付けられている)です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストには、管理者を認証するクエリのシーケンスと認証方式が記述されています。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのどの認証にも失敗する場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースが管理者アクセス権の拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name* には、作成するリストの名前として使用する文字列を指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **line**：回線パスワードを認証に使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	回線または回線セットに対して、認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** \| *list-name*} *method1* [*method2...*] グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication** {**default** \| *list-name*} ライン コンフィギュレーション コマンドを使用します。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可は、管理者が使用できるサービスを制限します。AAA 許可が有効の場合、アクセス ポイントは管理者のプロファイルから取得した情報を使用して管理者のセッションを設定します。管理者のプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。管理者が要求したサービスへのアクセスが許可されるのは、管理者プロファイル内の情報により許可された場合だけです。

tacacs+ キーワードを指定してグローバル コンフィギュレーション コマンド **aaa authorization** を使用すると、管理者のネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

aaa authorization exec tacacs+ local コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

（注） CLI を通してログインした認証済み管理者は、許可が設定されていても許可が省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	ネットワーク関連のすべてのサービス要求に対して、管理者の TACACS+ 許可が受け入れられるようにアクセス ポイントを設定します。
ステップ 3	**aaa authorization exec tacacs+**	管理者の TACACS+ 許可に管理者が特権 EXEC アクセス権を持っているかどうかを判断するように、アクセス ポイントを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* グローバル コンフィギュレーション コマンドを使用します。

また、ユーザ クレデンシャルを使用して TACACS サーバを設定し、TACACS サーバが認証済みユーザの認証プロファイルを返すように設定する必要もあります。プロファイルは、シェル特権レベル 15 のように包括的でコマンドの制限がないプロファイルにも、特定のコマンドのセットまたは低い特権レベルをターゲットとしたより具体的なプロファイルにもできます。

TACACS+ アカウンティングの起動

AAA アカウンティング機能は、管理者がアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形で管理者のアクティビティを TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa accounting network start-stop tacacs+**	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* グローバル コンフィギュレーション コマンドを使用します。

TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

VLAN の設定

この章では、有線 LAN に設定された VLAN を使って動作するようにアクセス ポイントを設定する方法について説明します。

VLAN の概要

VLAN は、物理的または地理的な基準ではなく、機能、プロジェクト チーム、あるいはアプリケーション別に論理的にセグメント化したスイッチド ネットワークです。たとえば、特定の作業グループ チームが使用するワークステーションおよびサーバを、ネットワークへの物理的接続や他のチームと混ざり合っている可能性などにかかわらず、すべて同じ VLAN に接続できます。VLAN によるネットワークの再設定は、デバイスやケーブルを物理的に取り外したり移動したりするのではなく、ソフトウェアを使って行います。

VLAN は、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、1 つのブリッジング ドメインによって接続された、ホストかネットワーク機器（ブリッジやルータなど）のいずれかに該当する複数のエンド システムで構成されます。ブリッジング ドメインは、さまざまなネットワーク機器でサポートされています。たとえば LAN スイッチは、VLAN ごとに異なるグループを使用して、スイッチ間のブリッジング プロトコルを処理します。

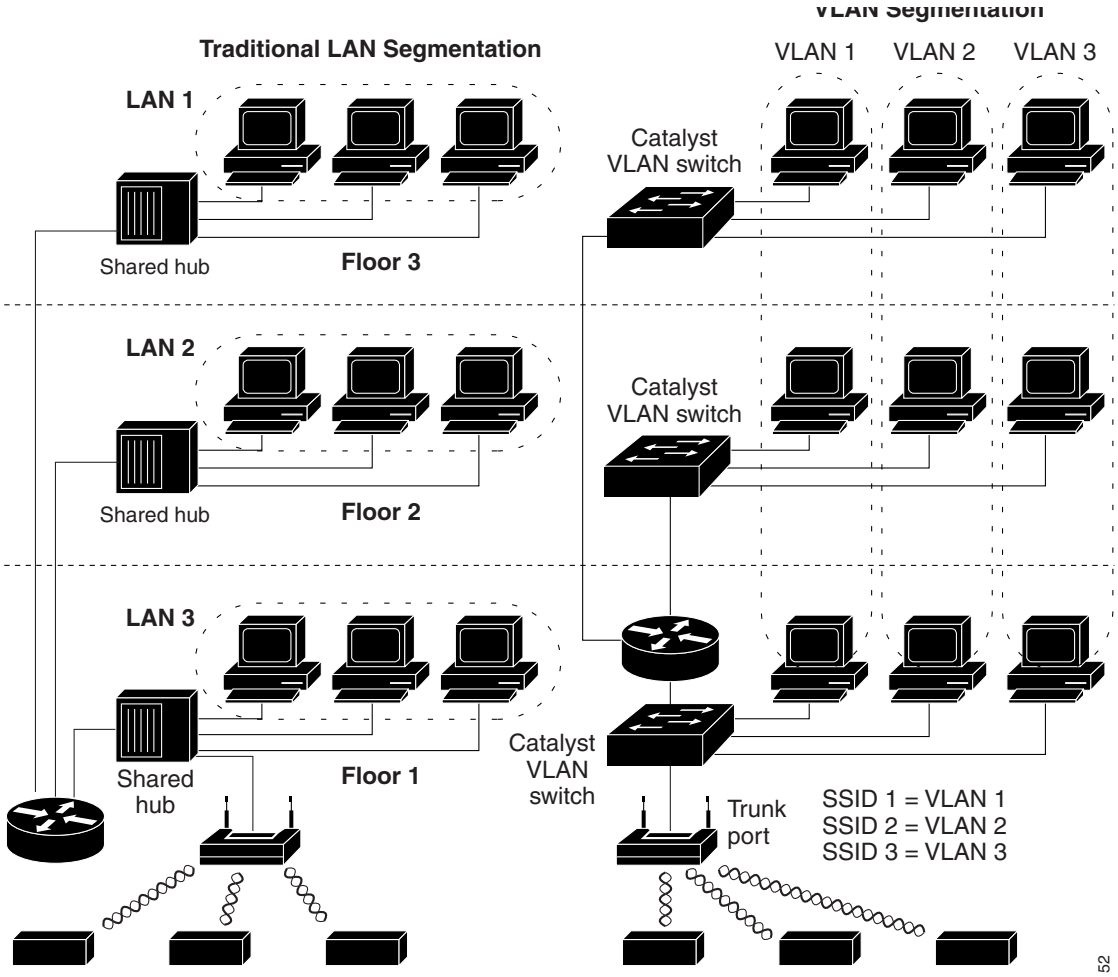
VLAN は、通常は LAN 設定のルータによって提供されるセグメンテーション サービスを提供します。VLAN はスケーラビリティ、セキュリティ、およびネットワーク管理に対応します。スイッチド LAN ネットワークを設計し構築する際は、いくつかの主要な問題を考慮する必要があります。

- LAN セグメンテーション
- セキュリティ
- ブロードキャスト制御
- パフォーマンス
- ネットワーク管理
- VLAN 間の通信

VLAN は、アクセス ポイントに IEEE 802.1Q タグ認識を追加することにより、無線 LAN に拡張することができます。異なる VLAN を宛先とするフレームは、アクセス ポイントによって無線で異なる複数の SSID に送信されます。その VLAN と関連付けられたクライアントだけが、これらのパケットを受信できます。それとは逆に、特定の VLAN にマッピングされている SSID にアソシエートされたクライアントから送信されたパケットは、802.1Q タグが付けられてから、有線ネットワークに転送されます。

図 14-1 は、無線デバイスが接続された状態での、従来の物理的な LAN セグメンテーションと論理的な VLAN セグメンテーションとの違いを示しています。

図 14-1　無線デバイスを使用する LAN セグメンテーションと VLAN セグメンテーション



VLAN の設計と設定の詳細については、次の URL にある『Cisco IOS Switching Services Configuration Guide』を参照してください:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c.html

VLAN への無線デバイスの組み込み

VLAN の基本的な無線コンポーネントは、アクセス ポイントと、無線テクノロジーを使用してアクセス ポイントにアソシエートされるクライアントです。アクセス ポイントは、VLAN が設定されているネットワーク VLAN スイッチに、トランク ポートを介して物理的に接続されています。VLAN スイッチへの物理的な接続には、アクセス ポイントのイーサネット ポートが使用されます。

基本的に、特定の VLAN に接続するようにアクセス ポイントを設定する際に重要なのは、その VLAN を認識するように SSID を設定することです。VLAN は VLAN ID または名前によって識別されるため、アクセス ポイントの SSID が特定の VLAN ID または名前を認識するように設定された場合、VLAN との接続が確立されます。この接続が確立されると、同じ SSID を持つ、アソシエートされた無線クライアント デバイスは、このアクセス ポイントを介して VLAN にアクセ

スできます。VLAN は、有線ネットワークとのやり取りと同様に、クライアントとやり取りしてデータを処理します。アクセス ポイントには最大 16 の SSID を設定できるため、最大 16 の VLAN をサポートできます。

特定の VLAN に複数の SSID を割り当てることができます。ただし、特定の SSID は 1 つの VLAN だけにマッピングできます。また、SSID と VLAN のマッピングは、各インターフェイスに固有である必要があります。

たとえば、SSID1 および SSID2 を設定します。SSID1 を無線 0 の VLANA に割り当てる場合、同じ無線 0 で SSID2 を VLANA に割り当てることはできません。SSID2 は、無線 1 の VLANA に割り当てることができます。また、無線 0 または無線 1、あるいはこの両方で SSID2 を VLANB に割り当てることができます。SSID2 を無線 0 の VLANB に割り当てる場合、SSID2 を無線 1 に割り当てることはできても、VLANB に割り当てることが必須となります。SSID2（または SSID1）を無線 0 の VLANA と無線 1 の VLANB に割り当てることはできません。

VLAN 機能を使用すると、より効率的かつ柔軟に無線デバイスを展開できます。たとえば、ネットワーク アクセスの方法や与えられている権限が多種多様にわたる複数のユーザの個別要件に、1 つのアクセス ポイントで対応できるようになります。VLAN 機能を使用しない場合は、許可されているアクセスの方法や与えられた権限に基づいて多様なユーザに対応するために、複数のアクセス ポイントを設置する必要があります。

無線 VLAN の配備には、2 つの一般的な戦略があります。

- ユーザ グループによるセグメンテーション：無線 LAN のユーザ コミュニティをセグメント化し、各ユーザ グループに異なるセキュリティ ポリシーを適用できます。たとえば、企業環境で、正社員用、パートタイム従業員用、およびゲスト アクセス用の 3 つの有線および無線 VLAN を構築することが可能です。
- デバイス タイプによるセグメンテーション：無線 LAN をセグメント化して、セキュリティ機能の異なる複数のデバイスがネットワークに接続できるようにします。たとえば、一部の無線ユーザのハンドヘルド デバイスは事前共有キー（PSK）セキュリティ メカニズムのみをサポートする一方、他の無線ユーザは 802.1x/EAP を使用する高度なデバイスを使用しているとします。これらのデバイスをグループ化して、個別の VLAN として切り離すことができます。

リピータは VLAN にマッピングされた SSID を繰り返すことができません。ルート アクセス ポイントとリピータを設定する際は、ルート AP 上の SSID とリピータ上の同じ SSID がネイティブ VLAN を使用するようにしてください。ルート AP およびリピータ AP 上の他の SSID は VLAN にマッピングされるように設定することはできますが、これらのタグ付けされた SSID を繰り返すことはできません。

ブリッジと非ルート ブリッジのリンクを設定する際は、ブリッジで使用される SSID からタグを除去する必要があります（つまり、ネイティブ VLAN を使用します）。ルート ブリッジ AP と非ルート ブリッジ AP 両方のその他の SSID が VLAN にマッピングされるように設定することもできます。これらの SSID は、ネイティブ VLAN にアソシエートされた SSID によってルート ブリッジと非ルート ブリッジとの間で転送されます。

VLAN の設定

次の項では、アクセス ポイントに VLAN を設定する方法について説明します。

VLAN の設定

VLAN をサポートするようにアクセス ポイントを設定するプロセスは、次の 3 つの手順で行います。

1. 無線ポートとイーサネット ポートでの VLAN の有効化
   無線ポートとイーサネット ポートで VLAN を有効にすると、アクセス ポイント コンフィギュレーションにも VLAN が作成されます。
2. SSID を作成して VLAN に割り当てます。
3. 特定の無線インターフェイスの VLAN に暗号化設定を割り当てます。

この項では、SSID を VLAN に割り当てる方法、およびアクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にする方法を説明します。SSID に認証タイプを割り当てる手順の詳細は、第 11 章「認証タイプの設定」を参照してください。その他の設定を SSID に割り当てる方法については、第 7 章「複数の SSID の設定」を参照してください。

アクセス ポイントには最大 16 の SSID を設定できるため、LAN に設定される VLAN は、最大 16 までサポートできます。

ステップ 1:無線ポートとイーサネット ポートで VLAN を有効にする

特権 EXEC モードから、次の手順に従って VLAN に SSID を割り当て、アクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio 0.x | 1.x**	無線 VLAN サブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**encapsulation dot1q** *vlan-id* [**native**]	無線インターフェイスで VLAN を有効にします。 (任意)VLAN をネイティブ VLAN に指定します。多くのネットワークではネイティブ VLAN は VLAN 1 です。
ステップ 4	**exit**	グローバル コンフィギュレーション モードに戻ります。

ステップ 2：SSID を作成して VLAN に割り当てる

特権 EXEC モードから、次の手順に従って SSID を VLAN に割り当てます。

	コマンド	目的
ステップ 1	**dot11 ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。 **（注）** 各 SSID に認証タイプを設定する場合は、**ssid** コマンドの認証オプションを使用します。認証タイプの設定方法については、第 11 章「認証タイプの設定」を参照してください。
ステップ 2	**vlan** *vlan-id*	（任意）ネットワーク上の VLAN に SSID を割り当てます。この SSID を使用してアソシエートするクライアント デバイスは、この VLAN にグループ化されます。VLAN ID を 1 ～ 4095 の範囲で入力します。 SSID に割り当てることができる VALN は 1 つだけですが、各 SSID が異なる無線インターフェイスに送信される限り、2 つの SSID を 1 つの VLAN に割り当てることができます。ただし、同じインターフェイスの同じ VLAN に 2 つの SSID を割り当てることはできません。 **ヒント** ネットワークで VLAN 名を使用している場合、アクセス ポイントの VLAN にも名前を割り当てることができます。手順については、「VLAN への名前の割り当て」（P.14-7）を参照してください。
ステップ 3	**exit**	無線インターフェイスのインターフェイス コンフィギュレーション モードに戻ります。

ステップ 3：特定の無線インターフェイスの VLAN に暗号化設定を割り当てる

特権 EXEC モードから、次の手順に従って、特定の無線インターフェイスの VLAN に暗号化設定を割り当てます。

	コマンド	目的
ステップ 1	**interface dot11radio 0 | 1**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 2	**ssid** *ssid-string*	SSID をインターフェイスに割り当てます。
ステップ 3	**encryption vlan** *vlan-id* **{mode | key}**	このインターフェイスにアソシエートされた VLAN の暗号化方式を設定します。詳細については、使用できる方式とキーについて詳しく説明している第 10 章「WLAN 認証および暗号化の設定」を参照してください。

次の例は、下記のことを行う方法を示します。

- 無線ポートとイーサネット ポートで VLAN をネイティブ VLAN として有効にします。
- SSID を VLAN に割り当てます。
- VLAN に AES-CCMP 暗号化方式を割り当てます。
- SSID を無線インターフェイスに割り当てます。

```
ap# configure terminal
ap(config)# interface dot11Radio 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# interface gigabitEthernet 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# dot11 ssid batman
ap(config-ssid)# vlan 31
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
ap(config-if)# encryption vlan 31 mode ciphers aes-ccm
ap(config-if)# ssid batman
ap(config-if)# end
```

VLAN への名前の割り当て

VLAN に ID 番号と名前を割り当てることができます。VLAN 名には、最大 32 文字の ASCII 文字を使用できます。アクセス ポイントでは、各 VLAN 名と ID のペアが表に格納されます。

VLAN 名を使用する際のガイドライン

VLAN 名を使用する際は、次のガイドラインに留意してください。

- VLAN 名の VLAN ID へのマッピングは各アクセス ポイントだけで使用されるため、同じ VLAN 名をネットワーク内の別の VLAN ID に割り当てることができます。

（注） 無線 LAN のクライアントがシームレスなローミングを必要とする場合には、すべてのアクセス ポイントで同じ VLAN ID に対して同じ VLAN 名を割り当てるか、名前を使用せずに VLAN ID だけを使用することを推奨します。

- ID はアクセス ポイントに設定されているすべての VLAN に必要ですが、VLAN 名はオプションです。
- VLAN 名には、最大 32 文字の ASCII 文字を使用できます。ただし、VLAN 名を 1 ～ 4095 の数字にすることはできません。たとえば、*vlan4095* は VLAN 名として有効ですが、*4095* は無効です。アクセス ポイントでは、1 ～ 4095 の数字は VLAN ID 用に予約されています。

VLAN 名の作成

特権 EXEC モードから、次の手順に従って VLAN に名前を割り当てます。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 vlan-name** *name* **vlan** *vlan-id*	VLAN 名を VLAN ID に割り当てます。名前には、最大 32 文字の ASCII 文字を使用できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

VLAN から名前を削除する場合は、コマンドの **no** 形式を使用します。アクセス ポイントに設定されている VLAN 名と ID の組み合わせをすべて表示するには、特権 EXEC コマンド **show dot11 vlan-name** を使用します。

Remote Authentication Dial-In User Service(RADIUS)サーバを使用した VLAN へのユーザの割り当て

ユーザまたはユーザ グループがネットワークから認証を受けたときに、特定の VLAN に割り当てるように RADIUS 認証サーバを設定できます。

(注) WPA または RSN 情報エレメントでアドバタイズされる(さらに 802.11 でのアソシエーション中に決定される)ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセス ポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA、WPA2、および CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は認められていません。このような場合、クライアント デバイスと無線 LAN とのアソシエーションが解除されてしまいます。

VLAN マッピングのプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイントにアソシエートします。
2. クライアントは、RADIUS 認証を開始します。
3. クライアントの認証に成功すると、RADIUS サーバはクライアントを特定の VLAN にマッピングします。この場合、クライアントがアクセス ポイントで使用している SSID に定義された VLAN マッピングは無視されます。サーバがクライアントの VLAN 属性を返さない場合、クライアントはアクセス ポイントでローカルにマッピングされた SSID の指定する VLAN に割り当てられます。

これらは VLAN ID の割り当てに使用される RADIUS ユーザ属性です。各属性はグループ化された関係を特定するため、1 ～ 31 の範囲の共通のタグ値を保有していなければなりません。

- IETF 64（トンネル タイプ）：属性を **VLAN** に設定
- IETF 65（トンネル メディア タイプ）：属性を **802** に設定
- IETF 81（トンネル プライベート グループ ID）：属性を *vlan-id* に設定

アクセス ポイントに設定された VLAN の表示

特権 EXEC モードで、**show vlan** コマンドを使用してアクセス ポイントがサポートする VLAN を表示します。次に、**show vlan** コマンドの出力例を示します。

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Other                                          0                995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                          0                995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                          0                995

   4330 packets, 363704 bytes input
   995 packets, 75675 bytes output

Virtual LAN ID:  31 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.31
Dot11Radio1.31
GigabitEthernet0.31

 This is configured as native Vlan for the following interface(s) :
Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1                 0               5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                 0               5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                 0               5620

   0 packets, 0 bytes input
   5620 packets, 2737560 bytes output

Virtual LAN ID:  34 (IEEE 802.1Q Encapsulation)
```

```
   vLAN Trunk Interfaces:  Dot11Radio0.34
GigabitEthernet0.34

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 34                 0                  0

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 34                 0                  0

   0 packets, 0 bytes input
   0 packets, 0 bytes output

Virtual LAN ID:  35 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   Dot11Radio0.35

   Protocols Configured:   Address:              Received:        Transmitted:

   0 packets, 0 bytes input
   0 packets, 0 bytes output
```

管理 VLAN としての非ネイティブ VLAN の設定

通常は、ネイティブ VLAN が常に管理 VLAN になります。

非ネイティブ VLAN の VLAN ブリッジ グループを 1 に変更する場合を考えます。このような場合、コマンド **dot11 management vlan** *vlanid* を使用することで、非ネイティブ VLAN を管理 VLAN として設定できます。

条件および前提条件

- 非ネイティブ VLAN を管理 VLAN として使用する場合、ネイティブ VLAN を使用できなくなります。
- ワークグループ ブリッジは、この機能でサポートされていません。
- 管理 VLAN を変更する場合、その変更によって、進行中の telnet および GUI ユーザーのすべてのセッションが不安定になるか、中断されます。

設定手順（CLI）

ステップ 1　非ネイティブ VLAN を管理 VLAN として設定するためのコマンドを使用します。

ap(config)# dot11 management vlan *vlanid*

このコマンドを使用する際は、ネイティブ VLAN がないことを確認します。

ステップ 2　メイン インターフェイスまたはネイティブからブリッジ グループ 1 を削除します。

ap(config)# interface d0

ap(config-if)# no bridge-group 1

ステップ 3　ブリッジ グループ 1 を非ネイティブ インターフェイスに設定します。

ap(config-if)# interface 0.5

ap(config-if)# encapsulation dot1q *vlanid*

ap(config-if)# bridge-group 1

ap(config-if)# interface bvi1

ステップ 4　DHCP を設定します。

ap(config-if)# *ip-address* dhcp

設定手順（GUI）

ステップ 1　[Services] > [VLAN] に移動します。

ステップ 2　[Assigned VLANs] セクションの [Current VLAN List] から、管理 VLAN として設定する VLAN を選択します。

ステップ 3　[Management VLAN (If non-native)] チェックボックスをオンにします。

設定を元に戻す手順（CLI）

ステップ 1　管理 VLAN としての非ネイティブ VLAN の設定を解除するためのコマンドを使用します。

ap(config)# no dot11 management vlan *vlanid*

ステップ 2　ブリッジ グループ 1 をメイン インターフェイスまたは別のネイティブ VLAN に移動します。

ステップ 3　ブリッジ グループ 1 を別の非ネイティブ インターフェイスに設定します。

VLAN の設定例

次の例は、VLAN を使用して、大学の構内で無線デバイスを管理する方法を示しています。この例では、有線ネットワークに設定された VLAN を介した 3 つのアクセス レベルが用意されています。

- 管理アクセス：最高のアクセス レベル。ユーザはすべての内部ドライブとファイル、学部のデータベース、トップ レベルの財務情報、およびその他の機密情報にアクセスできます。管理ユーザには、Cisco EAP-FAST を使用した認証が要求されます。
- 教職員アクセス：中級のアクセス レベル。ユーザは学内のイントラネットとインターネット、内部ファイル、および学生のデータベースにアクセスし、人事や給与、その他の教職員関連の資料といった内部情報を参照できます。教職員ユーザには、Cisco PEAP を使用した認証が要求されます。
- 学生アクセス：最も低いアクセス レベル。ユーザは学内のイントラネットおよびインターネットへのアクセス、授業日程の入手、成績の参照、面会の約束など学生に関係のある活動を実行できます。学生は、個人用のスタティック WPA2（事前共有キー）を使用してネットワークに参加できます。

このシナリオでは、各アクセス レベルに 1 つずつ、少なくとも 3 つの VLAN 接続が必要です。アクセス ポイントは最大 16 の SSID を処理できるため、表 14-1 に示す基本設計を使用できます。

表 14-1　アクセス レベルの SSID と VLAN の割り当て

アクセス レベル	SSID	VLAN ID
管理	manage（boss ではない）	01
教職員	teach	02
学生	learn	03

マネージャは SSID manage を使用するように無線クライアント アダプタを設定し、教職員メンバーは SSID teach を使用するようにクライアントを設定し、学生は無線クライアント アダプタを SSID learn を使用するように設定します。これらのクライアントをアクセス ポイントにアソシエートすると、自動的に適切な VLAN を選択します。

この例では、VLAN をサポートするために次の手順を実行します。

1. LAN スイッチのいずれかで、上記の VLAN を設定するか、VLAN 設定を確認します。
2. アクセス ポイントで、各 VLAN に SSID を割り当てます。
3. 各 SSID に認証タイプを割り当てます。
4. アクセス ポイント上のイーサネットおよび dot11radio インターフェイスの両方に対し、VLAN 1 となる管理 VLAN を設定します。この VLAN は、ネイティブ VLAN にする必要があります。
5. アクセス ポイントのイーサネットおよび dot11radio インターフェイスの両方に、VLAN 2 と VLAN 3 を設定します。
6. クライアント デバイスを設定します。

表 14-2 に、この例での 3 つの VLAN の設定に必要な各コマンドを示します。

表 14-2　VLAN のコンフィギュレーション コマンドの例

VLAN 1 の設定	VLAN 2 の設定	VLAN 3 の設定
ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid boss** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid teach** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid learn** ap(config-ssid)# **end**
ap **configure terminal** ap(config) **interface FastEthernet0.1** ap(config-subif) **encapsulation dot1Q 1 native** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.2** ap(config-subif) **encapsulation dot1Q 2** ap(config-subif) **bridge-group 2** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.3** ap(config-subif) **encapsulation dot1Q 3** ap(config-subif) **bridge-group 3** ap(config-subif) **exit**
ap(config)#dot11 ssid manage ap(config-ssid)#vlan 1 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 1 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 2 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 2 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 3 ap(config-ssid)#authentication open ap(config-ssid)#authentication key-management wpa version 2 ap(config-ssid)#wpa-psk ascii 0 Cisco123 ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 3 mode ciphers aes-ccm

表 14-3 は、表 14-2 のコンフィギュレーション コマンドの結果を示しています。アクセス ポイントで実行コンフィギュレーションを表示するには、**show running** コマンドを使用します。

表 14-3　コンフィギュレーション コマンド例の結果

VLAN 1 インターフェイス	VLAN 2 インターフェイス	VLAN 3 インターフェイス
interface Dot11Radio**0**.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled	interface Dot11Radio**0**.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled	interface Dot11Radio**0**.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled
interface gigabitethernet encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface gigabitethernet encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface gigabitethernet encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled

無線インターフェイスのブリッジ グループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

ギガビット イーサネット インターフェイスのブリッジ グループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```

QoS の設定

この章では、アクセス ポイントに Quality of Service（QoS）を設定する方法について説明します。この機能を使用すると、特定のトラフィックを優先的に処理できます。QoS を使用しない場合、パケットの内容やサイズに関係なく、アクセス ポイントは各パケットにベストエフォートでサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

無線 LAN の QoS の概要

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

アクセス ポイントに QoS を設定すると、特定のネットワーク トラフィックを選択して優先順位を付け、輻輳管理と輻輳回避技術を使用して優先的に処理できます。無線 LAN に QoS を実装すると、ネットワークのパフォーマンスを予測可能にして、帯域幅を効果的に使用できます。

QoS を設定する場合、QoS ポリシーを作成して、アクセス ポイントに設定した VLAN に適用します。ネットワークで VLAN を使用しない場合、アクセス ポイントのイーサネット ポートと無線ポートに QoS ポリシーを適用できます。

（注）　QoS を有効にすると、アクセス ポイントでは Wi-Fi Multimedia（WMM）モードがデフォルトで使用されます。WMM については、「Wi-Fi Multimedia モードの使用方法」（P.15-4）を参照してください。

無線 LAN の QoS と有線 LAN の QoS

無線自律アクセス ポイントの QoS 実装は、有線デバイスの QoS 実装とは異なります。

- アクセス ポイントはパケットを分類しません。DSCP 値、クライアント タイプ（セルラー無線など）、または 802.1q か 802.1p タグの優先順位の値に基づいてパケットに優先順位を設定します。
- 内部 DSCP 値を構成しません。IP DSCP、優先順位、プロトコル値をレイヤ 2 Class of Service（COS; サービス クラス）値に割り当てるマッピングだけをサポートします。
- 無線出力ポートで WMM タイプのキューを実行します。
- イーサネット出力ポートで実行するのは、First-in first-out（FIFO; 先入れ先出し）キューイングだけです。
- 802.1Q/P タグ付きパケットだけをサポートします。アクセス ポイントは ISL をサポートしません。
- MQC ポリシーマップの **set cos** アクションだけをサポートします。
- QoS Elements for Wireless Phones 機能が有効な場合、他のクライアントのトラフィックよりも音声クライアントのトラフィック（VoWLAN IP フォンなど）を優先します。
- プロトコル値を 119 に設定したクラスマップ IP プロトコル節を使用して、Spectralink フォンをサポートします。

無線 LAN QoS 実装とシスコの他のネットワーク デバイスの QoS 実装を対比するには、次の URL の『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

無線 LAN への QoS の影響

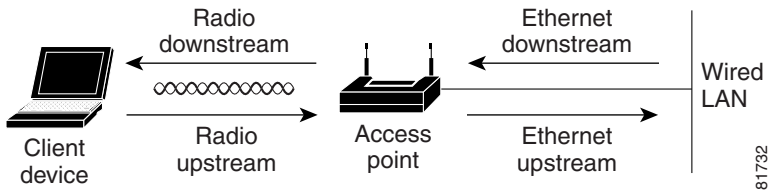
無線 LAN QoS 機能は、IEEE 802.11e の修正に基づいた Wi-Fi Alliance WMM 証明書の実装です。ワイヤレス クライアント認定の WMM は、アップストリーム方向に無線 LAN QoS を実装できます（無線クライアントから AP へ）。クライアント認定の 802.11n または 802.11ac は WMM 認定でもあります。

WMM のクライアント サポート（または未サポート）に関係なく、Cisco アクセス ポイントは WMM をサポートし、ダウンストリーム方向（AP からワイヤレス クライアントへ）またはアップストリーム方向（有線インターフェイスにワイヤレス フレームを転送する場合）にワイヤレス QoS を提供するように設定できます。

他のメディアと同様、負荷の少ない無線 LAN では、QoS の影響に気付かない場合があります。QoS のメリットは無線 LAN の負荷が増加するにしたがって顕著になり、選択されたトラフィック タイプの待ち時間、ジッタ、損失は許容範囲内に維持されます。

無線 LAN の QoS は、アクセス ポイントのダウンストリームを優先します。図 15-1 は、アップストリームとダウンストリームのトラフィック フローを示しています。

図 15-1　アップストリームとダウンストリームのトラフィック フロー



- 無線ダウンストリーム フローは、アクセス ポイントの無線から無線クライアント デバイスに送信されるトラフィックです。このトラフィックは、無線 LAN の QoS の主要な対象です。
- 無線アップストリーム フローは、無線クライアント デバイスからアクセス ポイントに送信されるトラフィックです。各クライアントは、個別にどのような優先順位付けメカニズムをこのトラフィックに使用する必要があるかを決定します。AP はクライアントのアップリンク トラフィックで優先順位付けメカニズムを実行できません。ただし、AP 設定はアップリンク優先順位付けが許可される（WMM が AP SSID でイネーブルの場合）か許可されないか（WMM が AP SSID でディセーブルの場合）を決定します。
- イーサネットのダウンストリーム フローは、スイッチまたはルータからアクセス ポイント上のイーサネット ポートに送信されるトラフィックです。スイッチまたはルータで QoS が有効の場合、スイッチまたはルータはアクセス ポイントへのトラフィックを優先し、レートを制限する場合があります。
- イーサネットのアップストリーム フローは、アクセス ポイントのイーサネット ポートから有線 LAN 上のスイッチまたはルータに送信されるトラフィックです。アクセス ポイントは、有線 LAN に送信するトラフィックの、トラフィック分類に基づく優先付けは行いません。ただし、AP はトラフィック QoS マーキングを維持します。

QoS 設定の優先順位

QoS を有効にすると、アクセス ポイントは各パケットのレイヤ 2 サービス クラス値に基づいて、パケットをキューに置きます。アクセス ポイントは、次の順序で QoS ポリシーを適用します。

1. 分類済みのパケット：アクセス ポイントが QoS 対応スイッチまたはルータからゼロ以外の 802.1 Q/P user_priority 値で分類されたパケットを受信する場合、アクセス ポイントはその分類を使用し、別の QoS ポリシー規則をパケットに適用しません。既存の分類がアクセス ポイントの他のどのポリシーよりも優先されます。

（注）　QoS ポリシーを設定していない場合でも、アクセス ポイントは無線インターフェイスで受信するタグ付け 802.1P パケットを必ず受け入れ、対応する 802.11e ユーザ プライオリティ キューを使用してパケットを地上波で送信します。各キューの送信レートとユニキャスト パケットの再試行回数は、[Streams] ページを使用して設定できます。

2. *QoS Element for Wireless Phones* の設定：*QoS Element for Wireless Phones* 設定を有効にすると、ダイナミック音声分類子は RTP ベース トラフィックのために作成され、これによりセルラー無線のトラフィックが他のクライアントよりも優先されます。さらに、QoS Basic Service Set（QBSS; QoS 基本サービス セット）が、ビーコンとプローブ応答でチャネル ロード情報をアドバタイズするために有効になります。トラフィック負荷に基づき、QBSS 要素を使用してアソシエートするアクセス ポイントを決定する IP フォンもあります。
Cisco IOS コマンド dot11 phone dot11e コマンドを使用して、802.11e/WMM QBSS Load IE をイネーブルにできます。1.05 ファームウェア以前の 7920 フォンは 802.11e QBSS IE をサポートしません。
ネットワーク内のワイヤレス クライアントが主にファームウェア 1.05 以前の 7920 フォンの場合、dot11 phone をイネーブルにします。
ネットワーク内のワイヤレス クライアントが主にファームウェア 1.09 以降の 7920 フォンの場合、または WMM 互換 VoWLAN フォンの場合、コマンド dot11 phone dot11e で IEEE 802.11e 互換 QBSS IE をイネーブルにします。

   次の例は、従来の QBSS Load 要素で IEEE 802.11 セルラー無線のサポートを有効にする方法を示します。

   ```
   AP(config)# dot11 phone
   ```

   次の例は、標準 IEEE 802.11e QBSS Load 要素で IEEE 802.11 フォンのサポートを有効にする方法を示します。

   ```
   AP(config)# dot11 phone dot11e
   ```

   次の例は、IEEE 802.11 電話機のサポートを停止、無効にする方法を示します。

   ```
   AP(config)# no dot11 phone
   ```

3. アクセス ポイントで作成したポリシー：QoS のポリシーを作成して VLAN またはアクセス ポイント インターフェイスに適用すると、この QoS ポリシーはすでに分類済みのパケットと *QoS Element for Wireless Phones* 設定に次いで 3 番目の優先順位になります。
4. VLAN の全パケットに適用されるデフォルト分類：VLAN の全パケットにデフォルトの分類を設定すると、そのポリシーは優先順位リストで 4 番目になります。

Wi-Fi Multimedia モードの使用方法

QoS を有効にすると、アクセス ポイントでは Wi-Fi Multimedia（WMM）モードがデフォルトで使用されます。WMM では、基本的な QoS モードに対して、次のような拡張機能が用意されています。

- アクセス ポイントは、各パケットのサービス クラスをパケットの 802.11 ヘッダーに追加し、このヘッダーを受信ステーションに渡します。
- 各アクセス クラスに 802.11 シーケンス番号が設定されます。このシーケンス番号により、受信側の重複チェック用バッファをオーバーフローさせずに、優先順位の高いパケットが優先順位の低いパケットの再試行を中断できます。

- WPA/WPA2 のリプレイ検出は、アクセス クラスごとに受信側で実行されます。802.11 のシーケンス番号設定と同じく、WPA/WPA2 のリプレイ検出でも、受信ステーションでリプレイをシグナリングせずに、優先順位の高いパケットが優先順位の低いパケットの再試行を中断できます。
- 通常のバックオフ手順で送信するように設定されたトランスミッタは、設定された送信のタイミング（所定のマイクロ秒数）の際に、送信を許可するアクセス クラスに対して保留中のパケットをセットで送信できます。保留中のパケットをセットで送信すると、各パケットがアクセスのためにバックオフを待機する必要がなく、即座にパケットを連続して送信できるため、スループットが向上します。
- U-APSD Power Save が有効になります。

WMM をサポートするクライアント デバイスに送信されたパケットに対して、アクセス ポイントは WMM 拡張機能を適用します。WMM をサポートしないクライアント デバイスに送信されたパケットに対して、アクセス ポイントは基本的な QoS ポリシーを適用します。

CLI を使用して WMM を無効にするには、設定インターフェイス コマンド **no dot11 qos mode wmm** を使用します。Web ブラウザ インターフェイスを使用して WMM を無効にするには、[QoS Advanced] ページで無線インターフェイスのチェックボックスをオフにします。図 15-3 は、[QoS Advanced] ページを示しています。

バンド選択の使用

バンド選択では、SSID が両方の無線で使用可能な場合、セルを結合するデュアル バンド対応無線クライアントをより混雑の少ない 5 GHz 無線に移動することができます。この機能は、ネットワークの全体的なパフォーマンスを向上させます。

バンド選択機能がイネーブルになっている場合、アクセス ポイントはバンド選択がイネーブルになっているすべての SSID で、すべての新しいクライアントに対する 2.4 GHz 無線のプローブ応答を遅らせます。ただし、アクセス ポイントは 5 GHz 無線のプローブ応答は遅延させません。このメカニズムにより、デュアルバンド クライアントは 5 GHz 無線の SSID を先に検出できるため、それらのクライアントは 2.4 Ghz 無線ではなく、AP 5 GHz 無線の SSID にアソシエートされるようにプッシュします。2.4 GHz 専用のクライアントのみが 2.4 GHz 無線となります。

バンド選択を有効にするには、次の手順に従ってください。

ステップ 1　[Security] > [SSID Manager] の順で選択します。

ステップ 2　[NEW] をクリックして、新しい SSID を作成します。

または

[Current SSID] から必要な SSID を選択します。

ステップ 3　[Band Select] オプション ボタンをクリックします。

ステップ 4　[Apply] をクリックします。

（注）　バンド選択機能は、SSID が両方の無線に割り当てられている場合にのみ役立ちます。

クライアントがアクティブにネットワークを検出する場合、そのクライアントは 1 つまたは複数のチャネルでプローブ要求を送ります。通常の動作では、特定のチャネルでプローブ要求のバーストを送信し、応答する AP からの応答を収集し、次のチャネルに移行します。そのため、特定のチャネルで 2 回連続してプローブ要求を受信したとしても必ずしもチャネルで AP の検出を 2 回試みたというわけではなく、バーストによる同じスキャン サイクルの一部である可能性があります。

次の情報を得るために、バンド選択の動作を微調整できます。

- スキャン サイクルの持続期間
- 2.4 GHz チャネルのクライアントと RSSI クライアントからのプローブ要求に AP が応答しないサイクル数
- トリガーするバンド選択メカニズムのタイムアウト。

バンド選択のパラメータの指定では、次の手順に従ってください。

ステップ 1　[Services] > [Band Select] の順で選択します。

ステップ 2　[Band Select] チェックボックスをオンにします。

ステップ 3　次のフィールドに値を入力します。

- [Client-Rssi]: クライアントがバンド選択可能となるための受信信号強度表示（RSSI）の最小値 指定できる範囲は 20 ～ 90 です。
- [Cycle-Count]: アクセス ポイントが無視する 2.4 GHz 帯域のプローブ要求数。
- [Cycle-Threshold (ms)]: アクセス ポイントがクライアントからの各プローブ要求バースト サイクルを受け付けられる時間（ミリ秒）。指定できる範囲は 1 ～ 1000 です。
- [Expire-Dual-Band (secs)]: この時間経過後にデュアル バンド クライアントは新しいクライアントとして宣言され、そのプローブ要求フレームが再度遅延されたり、無視される場合があります。指定できる範囲は 10 ～ 300 です。
- [Expire-Suppression (secs)]: この時間経過後に 2.4 GHz 専用クライアントは新しいクライアントとして宣言され、そのプローブ フレームが再度遅延されたり、無視される場合があります。指定できる範囲は 10 ～ 200 です。

ステップ 4　[Apply] をクリックします。

特権 EXEC モードから、次のコマンドを使用して、アクセス ポイント CLI を利用した BandSelect を設定します。

- ap(config)# **dot11 band-select parameters**
- ap(config-bs-profile)# **cycle-count?**
- ap(config-bs-profile)# **cycle-threshold?**
- ap(config-bs-profile)# **expire-suppression?**
- ap(config-bs-profile)# **expire-dual-band?**
- ap(config-bs-profile)# **client-rssi?**
- ap (config)# **dot11 ssid abcd**
- ap(config-ssid)# **band-select**

QoS の設定

QoS はデフォルトでは無効に設定されています。ただし、無線インターフェイスは、QoS ポリシーを設定していなくても、常にタグ付き 802.1P パケットを優先します。この項では、アクセス ポイントで QoS を設定する方法について説明します。内容は次のとおりです。

設定時の注意事項

アクセス ポイントに QoS を設定する前に、次の情報に注意する必要があります。

- QoS の導入で最も重要なのは、無線 LAN のトラフィックについて十分に把握することです。無線クライアント デバイスで使用するアプリケーション、アプリケーションが遅延の影響を受ける程度、およびアプリケーションに関連するトラフィック量が分かれば、パフォーマンスを向上させるように QoS を設定できます。
- QoS によって無線 LAN の帯域幅が増加することはありません。QoS は、帯域幅の割り当て制御を効率化します。無線 LAN に十分な帯域幅があれば、QoS を設定する必要がない可能性があります。
- **ampdu** コマンドは、802.11n 無線インターフェイスに使用できます。Aggregate MAC protocol data unit（AMPDU; 集合的 MAC プロトコル データ ユニット）は、物理層により単一の PSDU として転送された複数の MPDU を含む構造です。このコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

Web ブラウザ インターフェイスを使用した QoS の設定

この項では、Web ブラウザ インターフェイスを使用する QoS の設定について説明します。

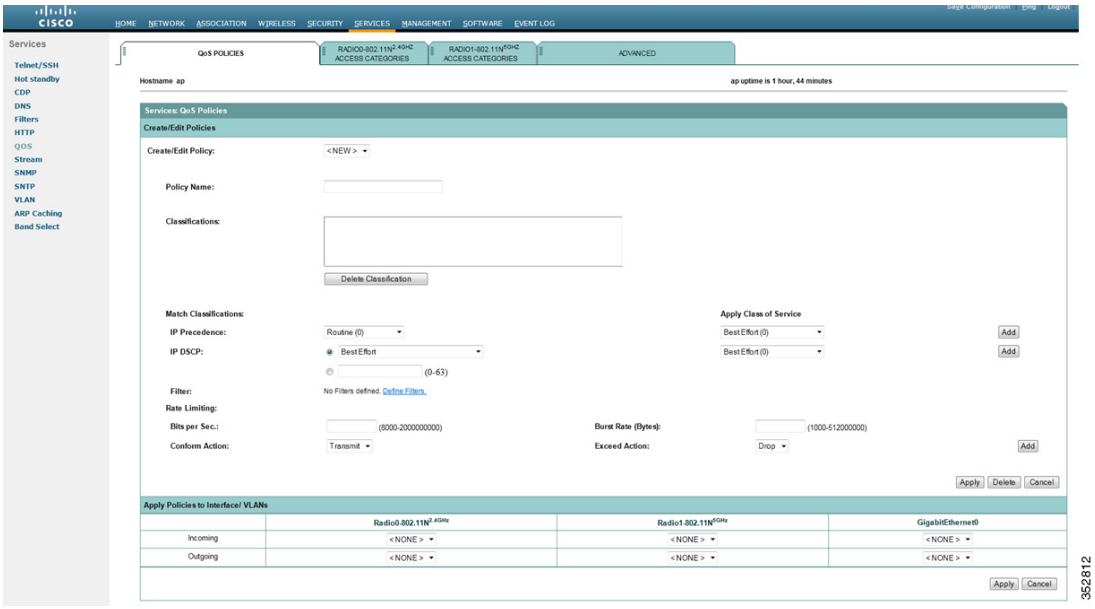
CLI を使用して QoS を設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

QoS を設定する手順は、次のとおりです。

ステップ 1　無線 LAN で VLAN を使用する場合、QoS を設定する前に必要な VLAN がアクセス ポイントに設定されていることを確認します。

ステップ 2　Web ブラウザ インターフェイスの任意のページの上部にある一般メニュー バーで [Services] をクリックします。Services のリストが表示されたら、[QoS] をクリックします。[QoS Policies] ページが表示されます。図 15-2 は、[QoS Policies] ページを示しています。

図 15-2　[QoS Policies] ページ



ステップ 3　[Create/Edit Policy] フィールドで [<NEW>] を選択して、[Policy Name] 入力フィールドに QoS ポリシーの名前を入力します。名前には、最大 25 文字の英数字を使用できます。ポリシー名には空白を入れないでください。

（注）　設定済みの 2 つの QoS ポリシーである WMM と Spectralink を選択することもできます。この 2 つのいずれかを選択すると、デフォルトの分類が自動的に [Classifications] フィールドに入力されます。

ステップ 4　優先順位を設定する必要のあるパケットの [IP header TOS] フィールドに IP 優先情報が含まれている場合には、[IP Precedence] ドロップダウン リストから IP 優先順位の分類を選択します。メニューの選択項目は次のとおりです。

- Routine (0)
- Priority (1)
- Immediate (2)
- Flash (3)
- Flash Override (4)
- Critic/CCP (5)
- Internet Control (6)
- Network Control (7)

ステップ 5　[IP Precedence] メニューで選択したタイプのパケットについて、無線クライアントに送信されるフレームにアクセス ポイントが適用する 802.11e ユーザ プライオリティ値を選択します。アクセス ポイントは [IP Precedence] の選択を 802.11 ユーザ プライオリティ（サービス クラス）の選択に一致させます。[Apply Class of Service]（適用する 802.11e ユーザ プライオリティ値を表す）ドロップダウン リストには次が含まれます。

- Best Effort (0)
- Background (1)

- Spare (2)
- Excellent (3)
- Control Lead (4)
- Video <100ms Latency (5)
- Voice <100ms Latency (6)
- Network Control (7)

ステップ 6　[IP Precedence] の [Class of Services] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。分類を削除するには、削除する分類を選択して、[Classifications] フィールドの横の [Delete] ボタンをクリックします。

ステップ 7　優先設定する必要のあるパケットの [IP header ToS] フィールドに IP 優先情報ではなく IP DSCP 優先情報が含まれている場合には、[IP DSCP] ドロップダウン リストから [IP DSCP] 分類を選択します。メニューの選択項目は次のとおりです。

- Best Effort
- Assured Forwarding — Class 1 Low
- Assured Forwarding — Class 1 Medium
- Assured Forwarding — Class 1 High
- Assured Forwarding — Class 2 Low
- Assured Forwarding — Class 2 Medium
- Assured Forwarding — Class 2 High
- Assured Forwarding — Class 3 Low
- Assured Forwarding — Class 3 Medium
- Assured Forwarding — Class 3 High
- Assured Forwarding — Class 4 Low
- Assured Forwarding — Class 4 Medium
- Assured Forwarding — Class 4 High
- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding（緊急転送）

ステップ 8　[Apply Class of Service] ドロップダウン リストを使用して、[IP DSCP] メニューから選択したタイプのパケットにアクセス ポイントが適用するサービス クラス（つまり 802.11e ユーザ プライオリティ値）を選択します。アクセス ポイントは、IP DSCP の選択内容を選択したサービス クラスに一致させます。

ステップ 9　[IP DSCP] の [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。

ステップ 10　無線 LAN で Spectralink フォン（IP Protocol 119）のパケットを優先設定する必要がある場合、[Apply Class of Service] ドロップダウン リストを使用して、アクセス ポイントが Spectralink フォン パケットに適用するサービス クラスを選択します。アクセス ポイントは、Spectralink フォン パケットを選択したサービス クラスに一致させます。

ステップ 11　IP Protocol 119 の [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。

ステップ 12　フィルタ処理されたパケットに優先順位を割り当てるには、[Filter] ドロップダウン リストを使用してポリシーに追加するフィルタを選択します（アクセス ポイントでフィルタが定義されていない場合、[Filter] ドロップダウン リストの代わりに [Apply Filters] ページへのリンクが表示されます）。たとえば、IP フォンの MAC アドレスを持つ MAC アドレス フィルタの優先順位を高くすることができます。

（注）　QoS で使用するアクセス リストは、ターゲット パケットの優先順位付けにのみ影響し、AP（セキュリティ）フォワーディングの決定には影響しません。

ステップ 13　[Apply Class of Service] ドロップダウン リストを使用して、[Filter] メニューから選択したフィルタに一致するパケットに、アクセス ポイントが適用するサービス クラスを選択します。アクセス ポイントは、フィルタの選択内容を選択したサービス クラスに一致させます。

ステップ 14　フィルタの [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。

ステップ 15　分類をポリシーへ追加したら、[Apply Class of Service] ドロップダウン リストの [Apply] ボタンをクリックします。ポリシーをキャンセルして全フィールドをデフォルトにリセットするには、[Apply Class of Service] ドロップダウン リストの [Cancel] ボタンをクリックします。ポリシー全体を削除するには、[Apply Class of Service] ドロップダウン リストの [Delete] ボタンをクリックします。

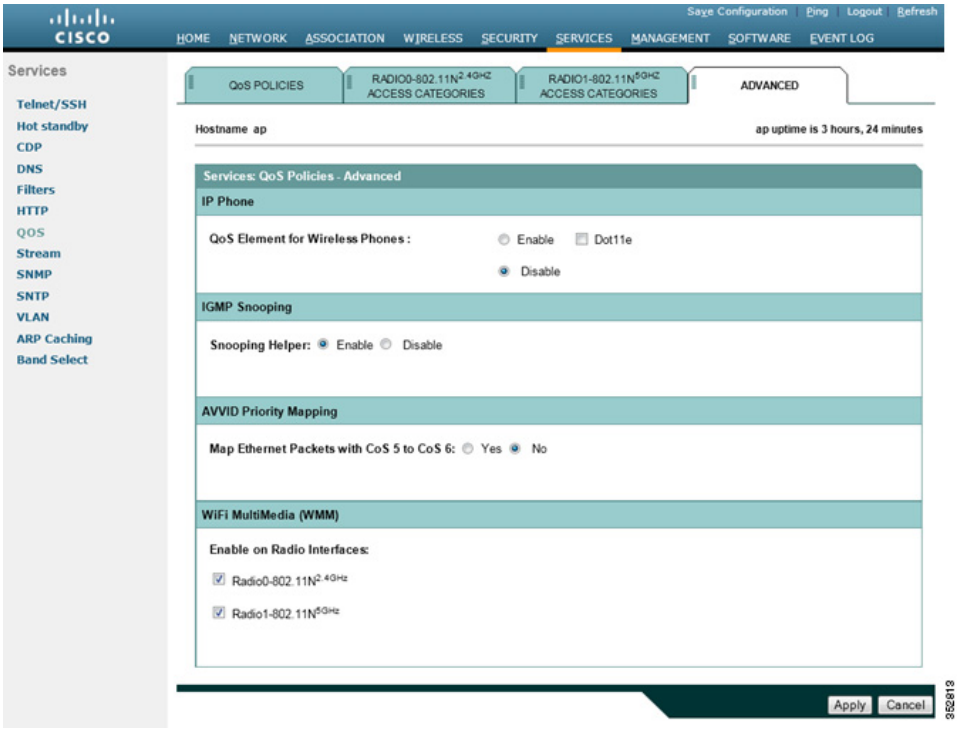
ステップ 16　[Apply Policies to Interface/VLAN] ドロップダウン リストを使用して、アクセス ポイントのイーサネット ポートと無線ポートにポリシーを適用します。アクセス ポイントに VLAN が設定されている場合、各 VLAN の仮想ポートのドロップダウン リストがこのセクションに表示されます。アクセス ポイントに VLAN が設定されていない場合、各インターフェイスのドロップダウン リストが表示されます。

ステップ 17　ページの下にある [Apply] ボタンをクリックして、アクセス ポイントのポートにポリシーを適用します。

[QoS Policies Advanced] ページ

[QoS Policies Advanced] ページ（図 15-3）

図 15-3　[QoS Policies - Advanced] ページ



[Enable the QoS Element for Wireless Phones] オプションを選択して、[Select Enable the QoS Element for Wireless Phones] オプションをクリックし、[Apply] をクリックしてすべての音声パケットに最高の優先順位を指定します。

QoS Element for Wireless Phones

QoS Element for Wireless Phones を有効にすると、QoS を有効にしていなくてもアクセス ポイントは音声パケットに最高の優先順位を指定します。この設定は、QoS ポリシーの設定とは無関係に機能します。

QBSS Load IE の WMM / 802.11e バージョンを使用するには、[dot11e] を選択します。この選択を空白にすると、QBSS Load IE の CCX pre-802.11e バージョンが使用されます。ワイヤレス クライアントが主にファームウェア 1.05 以前の 7920 フォンの場合、802.11e 以前のバージョンを使用します。クライアントが主に WMM 互換クライアントの場合は 802.11e バージョンを使用します。

IGMP スヌーピング

Internet Group Membership Protocol（IGMP）スヌーピングがスイッチでイネーブルになっている場合、スイッチは必要に応じてそのマルチキャスト トラフィックを登録するポートにのみマルチキャスト トラフィックを転送します。その結果、ワイヤレス クライアントが同じスイッチに接続されたアクセス ポイントから別のアクセス ポイントにローミングするとき、スイッチは 2 つ目のアクセス ポイントへのポートでマルチキャスト トラフィックが必要かどうかを認識しません。そのため、クライアントのマルチキャスト セッションは中断されます。アクセス ポイントでの IGMP スヌーピングは、この問題を軽減するのに役立ちます。

アクセス ポイントの IGMP スヌーピング ヘルパーが有効で、クライアントがアクセス ポイント セルに参加すると、アクセス ポイントはすぐに汎用 IGMP クエリを無線 LAN に送信して、クライアントに IGMP メンバーシップ レポートを送信するように求めます。メンバーシップ レポートは有線インターフェイスに転送されます。ネットワーク インフラストラクチャがホストの IGMP メンバーシップ レポートを受け取ると、そのホストのマルチキャスト データ ストリームがアクセス ポイント ポートに配信されることが保証されます。その後、トラフィックは無線インターフェイスにリレーされます。これにより、無線クライアントのマルチキャスト フローはローミング中に中断されません。

インターネット グループ管理プロトコル（IGMP）スヌーピングがスイッチで有効に設定されているときに、クライアントがアクセス ポイント間をローミングする場合、クライアントのマルチキャスト セッションはドロップされます。アクセス ポイントの IGMP スヌーピング ヘルパーが有効な場合、アクセス ポイントは汎用クエリを無線 LAN に送信して、クライアントに IGMP メンバーシップ レポートを送信するように求めます。ネットワーク インフラストラクチャがホストの IGMP メンバーシップ レポートを受け取ると、そのホストのマルチキャスト データ ストリームの配信が保証されます。

IGMP スヌーピング ヘルパーは、デフォルトで有効に設定されています。無効にするには、[QoS Policies - Advanced] ページを表示して [Disable] を選択し、[Apply] をクリックします。

（注）　ホストからの IGMP クエリと応答を処理するマルチキャスト ルータがない場合、アクセス ポイントに **no igmp snooping** が設定されていることが必須となります。IGMP スヌーピングが有効な場合、すべてのマルチキャスト グループ トラフィックが IGMP クエリと応答パケットを送信する必要があります。IGMP クエリまたは応答パケットが検出されない場合、グループのすべてのマルチキャスト トラフィックはドロップされます。

AVVID 優先順位マッピング

802.11e プロトコルは、音声パケットに 6 というユーザ プライオリティ値を割り当てます。Cisco の有線ネットワークは IETF の推奨事項に従って、音声パケットに 5 というサービス クラス値を割り当てます。AVVID プライオリティ マッピングをイネーブルにすると、サービス クラス 5 のイーサネット パケットは、アクセス ポイントの無線と有線の側でやり取りされるときに、サービス クラス 6 にマップされます。この機能を使用すると、アクセス ポイントは、正しい優先順位を音声パケットに適用して Cisco AVVID ネットワークとの互換性を確保します。

AVVID 優先順位マッピングはデフォルトで有効に設定されています。マッピングを無効にするには、[QoS Policies - Advanced] ページを表示して [Map Ethernet Packets with CoS 5 to CoS 6] で [No] を選択し、[Apply] をクリックします。

WiFi Multimedia（WMM）

[Admission Control] チェックボックスを使用すると、アクセス ポイントの無線インターフェイスの WMM サポートをイネーブルまたはディセーブルにできます。デフォルトはイネーブルです。WMM がイネーブルになっている場合、WMM と非 WMM クライアントの両方がアクセス ポイント無線に参加することができます。

（注）　アドミッション コントロール（RADIO1-802.11N2.4GHZ ACCESS CATEGORIES または RADIO1-802.11N5GHZ ACCESS CATEGORIES）を有効にすると、アクセス ポイントにアソシエートされたクライアントは、WMM のアドミッション コントロール プロシージャを完了するまでそのアクセス カテゴリを使用できません。

レート制限

レート制限は、インターフェイスで送受信されるデータのトラフィックを制御します。クラスベースのポリシング機能により、次の動作が実行されます。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- IP precedence 値、IP DiffServ コード ポイント（DSCP）値、および Quality of Service（QoS）グループを設定してパケットにマーク付けをします。

これは、P2MP 設定の場合に、各非ルート ブリッジからルート ブリッジへのアップストリーム トラフィックをレート制限するために使用されます。ダウンストリーム トラフィックのレート制限を行うためには、クラス マップがルート側のルータ/スイッチに適用されます。

（注）　レート制限はイーサネット入力だけに適用できます。

無線アクセス カテゴリの調整

アクセス ポイントは、無線アクセス カテゴリを使用して各パケットのバックオフ時間を計算します。通常、優先順位の高いパケットは、バックオフ時間が短くなります。

[Min and Max Contention Window] フィールドと [Slot Time] フィールドのデフォルト値は、IEEE 802.11 修正で推奨される設定に基づいています。これらの値の詳細については、IEEE 802.11e 修正、7.3.2.27 または 802.11-2012 規格、8.4.2.31（EDCA Parameter Set 要素）を参照してください。

[Radio Access Categories] ページではデフォルト設定を使用することを強く推奨します。これらの値を変更すると、無線 LAN に予期しないトラフィックのブロックが発生しやすくなり、発生したブロックの診断が容易ではない場合もあります。これらの値を変更後にデフォルトにリセットする必要があれば、表 15-1 のデフォルト設定を使用します。

表 15-1 に示された値は 2 の累乗係数です。アクセス ポイントは、次の式を使用して Contention Window の値を計算します。

CW = 2 ** X - 1

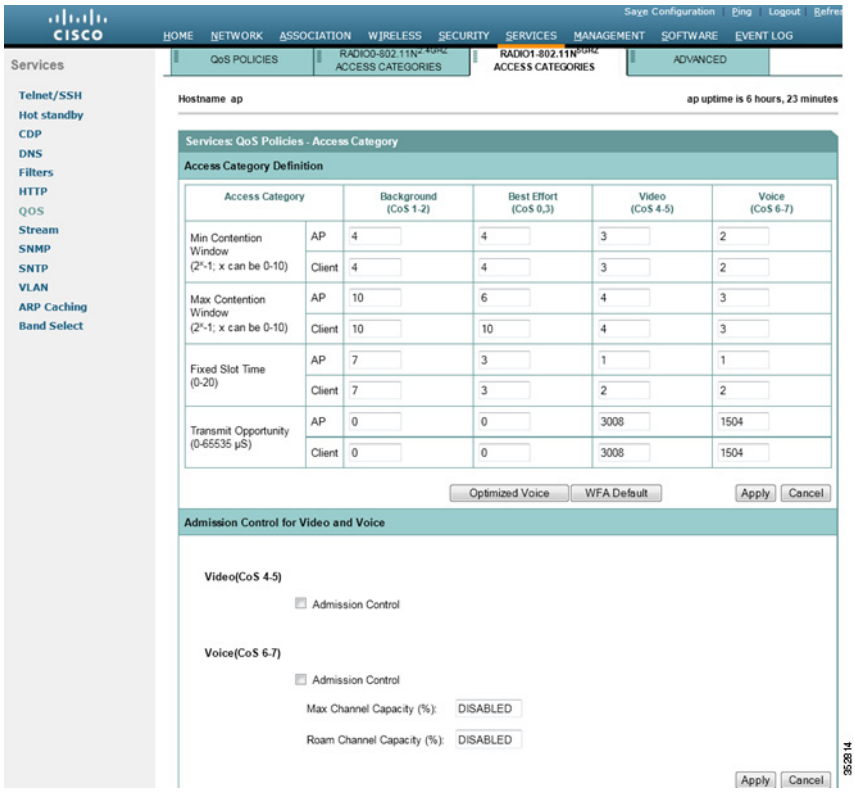
X は 表 15-1 の値です。

表 15-1　QoS 無線アクセス カテゴリのデフォルト

サービス クラス	Min Contention Window		Max Contention Window		Fixed Slot Time		Transmit Opportunity		Admission Control	
	ローカル	Cell	ローカル	Cell	ローカル	Cell	ローカル	Cell	ローカル	Cell
Background	4		10		6		0			
Best Effort	4		10		2		0			
Video <100ms Latency	3		2		1		3008			
Voice <100ms Latency	2		3		1		1504			

図 15-4 は [Radio Access Categories] ページを示しています。デュアル無線アクセス ポイントには、各無線に対して [Radio Access Categories] ページがあります。

図 15-4　[Radio Access Categories] ページ



TCLAS と TSPEC を使用する無線クライアントは、クライアントがトラフィック ストリームを開始する前にアクセス ポイントに送信した ADDTS（add traffic stream 要求）を通してサービス クラスを要求できます。ADDTS は、対象トラフィックとそのトラフィックの予想公称レートについて説明します。

公称レートの設定

アクセス ポイントが WMM クライアントから add traffic stream（ADDTS; トラフィック ストリームの追加）要求を受け取ると、CLI コマンドの **traffic-stream** で定義された公称レートに対する、ADDTS 要求の公称レートまたは最小 PHY レートをチェックします。両者が一致しない場合、アクセス ポイントは ADDTS 要求を拒否します。

[Optimized Voice] 設定（図 15-4 を参照）を選択する場合、次の公称レートが設定されます。

- 5.5Mbps、6.0Mbps、11.0Mbps、12.0Mbps、および 24.0Mbps

traffic-stream コマンドの詳細については、『*Command Reference for Cisco Aironet Access Points and Bridges*』で参照できます。この資料は cisco.com の次の URL から入手できます。

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp3257080

（注）　上記レートは Cisco フォンとほとんどの WMM VoWLAN IP フォンで有効に機能します。例外はサードパーティ製のワイヤレス フォンです。サードパーティのセルラー無線では、公称レートまたは最小 PHY レートが異なっている場合があります。サードパーティのセルラー無線用に追加の公称レートを有効にする必要がある場合があります。

最適化された音声設定

[Admission Control] チェックボックスを使用して、クライアントによるアクセス カテゴリの使用を制御できます。アクセス カテゴリに対するアドミッション コントロールを有効にすると、アクセス ポイントにアソシエートされたクライアントは、WMM のアドミッション コントロール プロシージャを完了するまでそのアクセス カテゴリを使用できません。ただし、このリリースのアクセス ポイントではアドミッション コントロール プロシージャはサポートされないため、[Admission Control] を有効にした場合、クライアントはアクセス カテゴリを使用できません。

コール アドミッション制御の設定

アクセス ポイントの Call Admission Control（CAC; コール アドミッション制御）の設定は次の手順で行います。

1. 無線の設定
2. SSID のアドミッション コントロールの有効化

無線の設定

この項では、アクセス ポイントの無線のアドミッション コントロール設定法について説明します。

コマンドライン インターフェイス（CLI）を使用してアドミッション コントロールを設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

無線のアドミッション コントロールを設定する手順は、次のとおりです。

ステップ 1　設定する無線の [Access Categories] ページをクリックします。

図 15-4 に、[Access Categories] ページの例を示します。

ステップ 2　[Voice(CoS 6-7)] 下の [Admission Control] チェックボックスを選択します。

ステップ 3　音声に使用されるチャネルの最大利用率を [Max Channel Capacity (%)] フィールドに入力します。

ステップ 4　ローミング コールに使用されるチャネルの最大利用率を [Roam Channel Capacity (%)] フィールドに入力します。

このフィールドで指定した値を最大とする、ローミング コールに使用されるチャネルの利用率は、[Max Channel Capacity (%)] フィールドで指定した値から差し引かれます。

たとえば、[Max Channel Capacity (%)] フィールドに 75% と入力し、[Roam Channel Capacity (%)] に 6% と入力したとします。ローミング コールがチャネルの 5% を使用する場合、音声コールはそのチャネルの最大 70% を使用できます（セルのクライアントが開始する新しいコール）。

ステップ 5　リアルタイム ビデオ トラフィック（AC_VO）のコール アドミッション制御を有効にするには、[Video (CoS 5-6)] の下にある [Admission Control] チェックボックスをオンにします。

（注）　この項で設定したアドミッション コントロール設定は、SSID のアドミッション コントロールを有効にするまでは無効です。

SSID のアドミッション コントロールの有効化

この項では、SSID のアドミッション コントロールを有効にする方法について説明します。

コマンドライン インターフェイス（CLI）を使用してアドミッション コントロールを有効にするための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

次の手順に従って SSID のアドミッション コントロールを有効にします。

ステップ 1　[SSID Manager] ページを開きます。

ステップ 2　[SSID] を選択します。

ステップ 3　[General Settings] の下、[Call Admission Control] フィールドの [Enable] を選択します。

アドミッション コントロールのトラブルシューティング

2 つの CLI コマンドを使用して、アドミッション コントロールの問題のトラブルシューティングに役立つ情報を表示できます。

- 無線 0 の現在のアドミッション コントロール設定を表示するには、次のコマンドを入力します。

  ```
  # show dot11 cac int dot11Radio 0
  ```

- 無線 1 の現在のアドミッション コントロール設定を表示するには、次のコマンドを入力します。

  ```
  # show dot11 cac int dot11Radio 1
  ```

- アドミッション コントロールおよび MT の admitted streams についての情報を表示するには、次のコマンドを入力します。

  ```
  # show dot11 traffic-streams
  ```

ストリームの設定

QoS ポリシーは、アクセス ポイントを通過するパケットをマーキングまたは再マーキングします。QoS ポリシーを定義する場合、特定のトラフィックのレート制限を決定することもできます。

ワイヤレス フォンの QoS 要素は、他の考慮事項に関係なく、音声パケットの優先順位を付けることができます。これは上限なしで音声パケットに低遅延設定を適用します。

ストリームの設定は、時間依存のトラフィックに優先順位の技術を適用する 3 つ目の方法で、より高い優先順位（低遅延キュー）で送信するトラフィックを指定して、それらの時間依存のパケットの再試行回数を制限します。ストリームは、他の QoS 設定と組み合わせて使用できます。

これらの機能を設定するには、[Services] > [Streams] のページに進みます（図 15-5 を参照）。

ステップ 1　[Packet Handling per User Priority] セクションから、低遅延キューイング ロジックを実行するユーザ プライオリティ キューを選択します。

- [Reliable] を選択した場合、確認応答がなかったユニキャスト パケットは、宛先（アソシエートされたワイヤレス クライアントまたは接続されたワイヤレス ブリッジ）が到達可能な限り再送されます。確認応答がなかったユニキャスト パケットを再試行する最大回数は無線レベルで決定され、各無線設定セクションの [Settings] タブで最大データ再試行値を設定します。
- [Low Latency] が選択された場合、現在のパケットを廃棄し、次のパケットを送信する前に AP が使用する再試行の回数を設定できます。低遅延のトラフィックの場合、トラフィックのフローを中断するよりもパケットをスキップするほうが推奨されます。[Max Retries for Packet Discard] で、低遅延に設定された対応するユーザ プライオリティについて AP が使用する再試行の最大数を入力します。

ステップ 2　[Apply] をクリックして確認します。

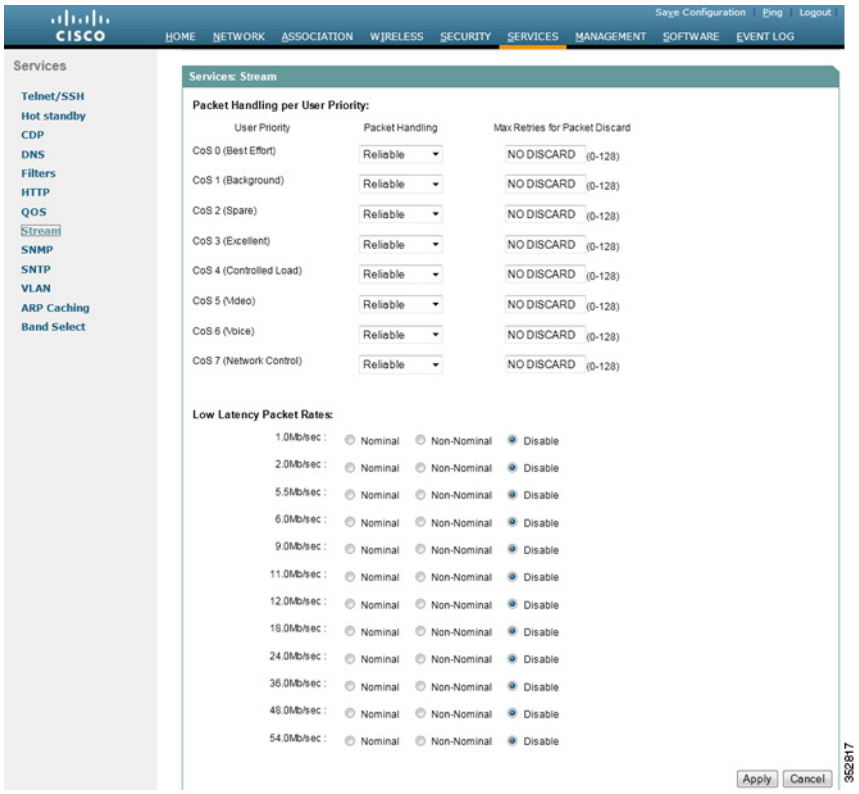
ステップ 3　ページ下部の [Low Latency Packet Rates] セクションで、低遅延キューに設定されたフレームを送信するレートを設定することもできます。

- Nominal：AP は、低遅延パケットを送信するときに、このレートを使用します（クライアントの信号レベルに応じて、最初に高速レートを使用）。
- Non-nominal：AP はそのレートを使用しないようにしますが、公称レートが使用できない場合にはこれを使用します。
- Disabled：AP は、そのレートを使用することはありません。

ステップ 4　[Apply] をクリックして確認します。

CLI を使用してストリームを設定するには、第 6 章「無線の設定」を参照してください。

図 15-5　　ストリーム ページ



フィルタの設定

この章では、Web ブラウザ インターフェイスを使用して、アクセス ポイントに MAC アドレス、IP、および EtherType フィルタを設定し、管理する方法について説明します。

フィルタの概要

プロトコル フィルタ（IP プロトコル、IP ポート、および EtherType）は、アクセス ポイントのイーサネット ポートや無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。プロトコル フィルタは個別に、または複数をまとめて設定することができます。無線クライアント デバイス、または有線 LAN 上のユーザ、あるいはその両方について、プロトコルをフィルタできます。たとえば、アクセス ポイントの無線ポートに SNMP フィルタを設定すると、無線クライアント デバイスはアクセス ポイントで SNMP を使用できなくなります。しかし、有線 LAN からの SNMP アクセスは排除されません。

IP アドレス フィルタや MAC アドレス フィルタによって、特定の IP アドレスや MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。

フィルタの設定には、Web ブラウザ インターフェイスを使用するか、または CLI にコマンドを入力します。

ヒント　アクセス ポイントの QoS ポリシーにフィルタを追加することもできます。QoS ポリシーの設定手順の詳細は、第 15 章「QoS の設定」を参照してください。

（注）　CLI を使用した場合、フィルタに設定できる MAC アドレスは最大 2,048 個です。Web ブラウザ インターフェイスを使用した場合には、フィルタに設定できる MAC アドレスは最大でも 43 個です。

CLI を使用したフィルタの設定

CLI コマンドを使用してフィルタを設定するには、アクセス コントロール リスト（ACL）とブリッジ グループを使用します。

- ブリッジ グループの詳細については、次の URL にある『B*ridging and IBM Networking Configuration Guide*』の「*Configuring Transparent Bridging*」の章を参照してください。
  http://www.cisco.com/c/en/us/td/docs/ios/bridging/configuration/guide/15-s/br-15-s-book/br_transprnt_brdg.html
- アクセス コントロール リスト（ACL）の詳細については、次の URL にある『*Security Configuration Guide*』の「*IP Access List Overview*」の章を参照してください。
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-data-acl-12-4t-book/sec-access-list-ov.html

（注）　ワイヤレス デバイスの設定に、CLI と Web ブラウザ インターフェイスの両方を使用することは避けてください。CLI を使用してワイヤレス デバイスを設定した場合、Web ブラウザ インターフェイスでは、設定が正しく表示されない場合があります。しかし、正しく表示されない場合でも、ワイヤレス デバイスは正しく設定されていることがあります。たとえば、CLI を使用して ACL を設定すると、Web ブラウザ インターフェイスに次のメッセージが表示されることがあります。「Filter 700 was configured on interface Dot11Radio0 using CLI. It must be cleared via CLI to ensure proper operation of the web interface」。このメッセージが表示された場合、ACL を削除するには CLI を使用し、再設定するには Web ブラウザ インターフェイスを使用する必要があります。

Web ブラウザ インターフェイスを使ったフィルタの設定

この項では、Web ブラウザ インターフェイスを使用してフィルタを設定し、有効化する方法について説明します。フィルタを設定し有効化する手順は次の 2 つにわかれます。

1. フィルタの設定ページを使用して、フィルタに名前をつけ、設定します。
2. [Apply Filters] ページを使用して、フィルタを有効化します。

MAC アドレス フィルタの設定と有効化

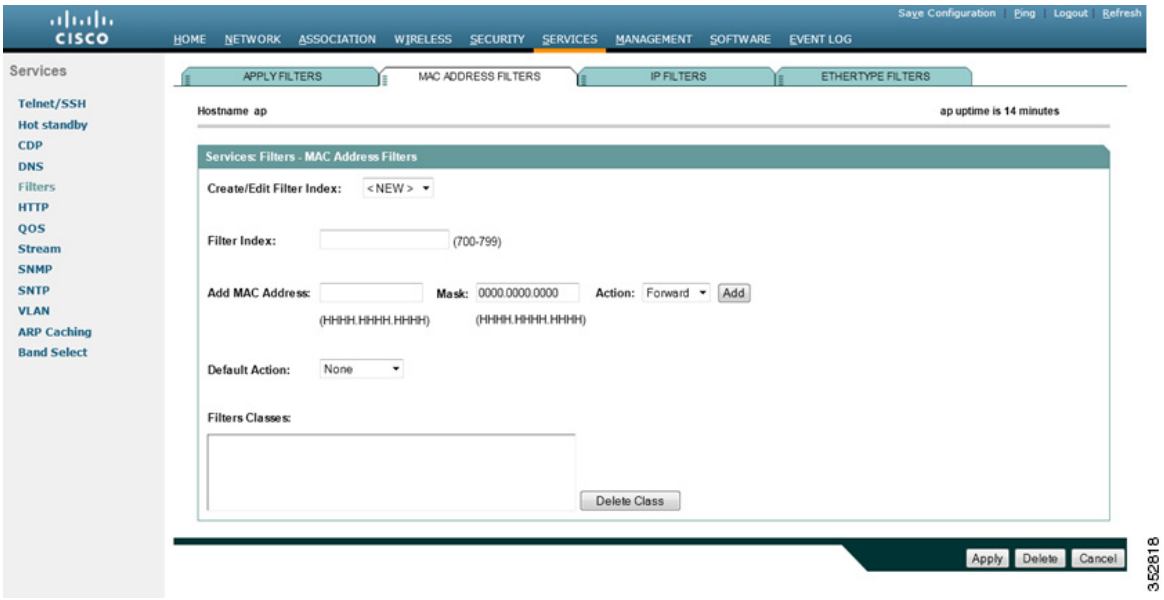
MAC アドレス フィルタによって、特定の MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべての MAC アドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべての MAC アドレスへのトラフィックを排除するフィルタを作成することもできます。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。

（注） CLI を使用して、フィルタリング用に MAC アドレスを設定することができますが、NVRAM の制約があるため、600 を超える MAC フィルタには FTP または TFTP が必要です。Web ブラウザ インターフェイスを使用した場合には、フィルタに設定できる MAC アドレスは最大でも 43 個です。

（注） MAC アドレス フィルタは強力なため、フィルタの設定を間違えると、Telnet を使用して AP に接続している間、アクセス ポイントからロックアウトされる可能性があります。誤ってロックアウトされた場合は、コンソール インターフェイスから CLI を使用してフィルタを無効にしてください。

[MAC Address Filters] ページを使用して、アクセス ポイントの MAC アドレス フィルタを作成します。図 16-1 は、[MAC Address Filters] ページを示しています。

図 16-1　[MAC Address Filters] ページ



次のリンク パスに従って、[Address Filters] ページを表示します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [MAC Address Filters] タブをクリックします。

MAC アドレス フィルタの作成

MAC アドレス フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、[MAC Address Filters] ページを表示します。

ステップ 2　新規 MAC アドレス フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>]（デフォルト）が選択されていることを確認します。フィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ番号を選択します。

ステップ 3　[Filter Index] フィールドで、フィルタに 700 ～ 799 の範囲で番号を付けます。割り当てた番号で、フィルタのアクセス コントロール リスト（ACL）が作成されます。

ステップ 4　[Add MAC Address] フィールドに MAC アドレスを入力します。アドレスは、たとえば、0005.9a39.2110 のように、ピリオドを使って、4 つの英数字からなる 3 つのグループに分けて入力します。

（注）　フィルタを確実に正しく動作させるためには、MAC アドレスで使用する文字はすべて小文字で入力してください。

ステップ 5　[Mask] 入力フィールドには、フィルタが MAC アドレスに対して左から右にチェックするビット数を入力します。たとえば、MAC アドレスと正確に一致させる（すべてのビットをチェックする）には、**0000.0000.0000** と入力します。先頭（最も重みの大きい）8 バイトだけをチェックするには、**0.0.FFFF** と入力します。

ステップ 6　[Action] メニューから [Forward] または [Block] を選択します。

ステップ 7　[Add] をクリックします。追加した MAC アドレスが [Filters Classes] フィールドに表示されます。[Filters Classes] リストから MAC アドレスを削除するには、そのアドレスを選択して [Delete Class] をクリックします。

ステップ 8　このフィルタにさらにアドレスを追加するには、ステップ 4 からステップ 7 を繰り返します。

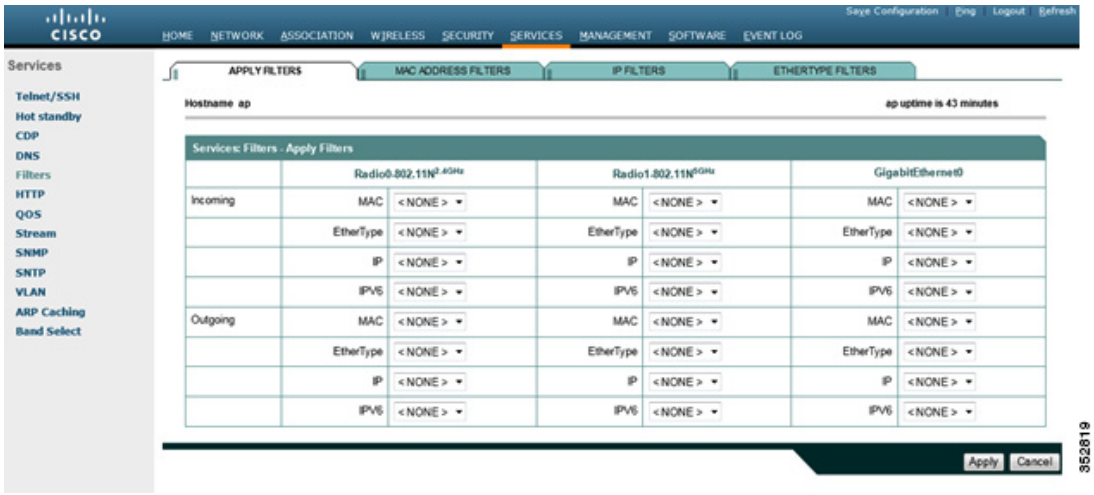
ステップ 9　[Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、複数のアドレスを入力したときに、これらのアドレスすべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。

ヒント　許可された MAC アドレスのリストは、ネットワーク上の認証サーバに作成できます。MAC ベースの認証の使用方法については、「認証タイプの設定」（P.11-10）を参照してください。

ステップ 10　[Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。

ステップ 11　[Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。図 16-2 は、[Apply Filters] ページを示しています。

図 16-2　[Apply Filters] ページ



ステップ 12　[MAC] ドロップダウン リストの 1 つから、フィルタ番号を選択します。フィルタはイーサネット ポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。

ステップ 13　[Apply] をクリックします。選択したポートで、このフィルタが有効化されます。

クライアントがただちにフィルタされない場合は、[System Configuration] ページの [Reload] をクリックして、アクセス ポイントを再起動します。[System Configuration] ページを表示するには、タスク メニューの [Software] をクリックしてから、[System Configuration] をクリックします。

（注）　排除された MAC アドレスを持つクライアント デバイスは、アクセス ポイントを介してデータを送受信できませんが、認証されていないクライアント デバイスとしてアソシエーション テーブルに保持されている場合があります。排除された MAC アドレスを持つクライアント デバイスは、アクセス ポイントによるモニタリングが停止した場合、アクセス ポイントがリブートした場合、またはクライアントが別のアクセス ポイントとアソシエートした場合に、アソシエーション テーブルから消去されます。

MAC アドレス フィルタの作成 - CLI の使用

CLI で MAC アドレス フィルタを作成するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

access-list *number-700-799* **{permit | deny}** *macc-address mask*

次の MAC アドレスのアクセス リストでは、1111.22 で始まる MAC アドレスだけが許可され、その他すべての MAC アドレスはブロックされます。

```
ap(config)# access-list 701 permit 1111.2200.0000   0000.00ff.ffff
ap(config)# access-list 701 deny   0000.0000.0000   ffff.ffff.ffff
```

MAC アドレス アクセス リストをインターフェイスに適用するには、グローバル コンフィギュレーション モードから開始して、次のコマンド シーケンスを使用します。

ステップ 1　**interface** *name*

ステップ 2　**l2-filter bridge-group-acl**

ステップ 3　**bridge-group** *bridge-group-number* **{input-address-list | output-address-list}** *ACL-number*

次の例では、上で作成した MAC アドレス アクセス リスト 701 を受信方向で無線 0 インターフェイスに適用します。ただし、インターフェイスに VLAN は作成しなかったため、ACL はデフォルト ブリッジ グループ 1 に適用されます。

```
ap(config)# interface dot11Radio 0
ap(config-if)# l2-filter bridge-group-acl
ap(config-if)# bridge-group 1 input-address-list 701
```

次の例では、VLAN 33 が作成され、無線 1 にアソシエートされています。一致するブリッジ グループ 33 は無線 1 サブインターフェイス 33 とイーサネット サブインターフェイス 33 の間に作成されました。MAC アドレス フィルタは、発信方向で無線 1 サブインターフェイス 33 に適用されます。

```
ap(config)# interface Dot11Radio1
ap(config-if)# l2-filter bridge-group-acl
ap(config-if)# exit
ap(config)# interface Dot11Radio1.33
ap(config-if)# bridge-group 33 output-address-list 701
```

MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止

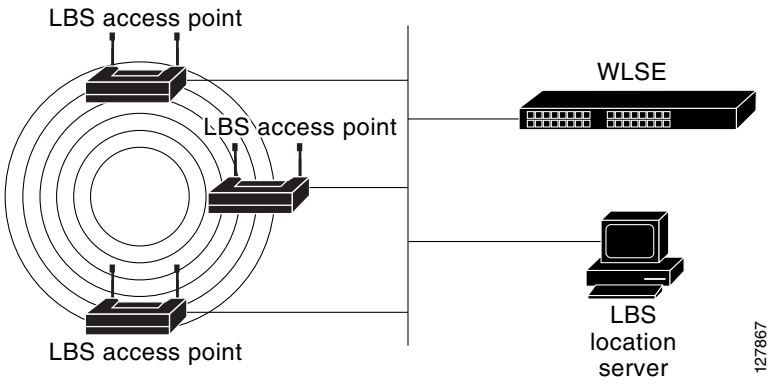
MAC アドレス ACL を使用して、アクセス ポイントへのクライアント アソシエーションを許可または禁止できます。インターフェイスを通過するトラフィックをフィルタする代わりに、ACL を使用して、アクセス ポイントの無線とのアソシエーションをフィルタします。

ACL を使用して、アクセス ポイントの無線へのアソシエーションをフィルタする手順は、次のとおりです。

ステップ 1　「MAC アドレス フィルタの作成」(P.16-4)のステップ 1 ～ 10 に従って、ACL を作成します。アソシエートを許可する MAC アドレスについては、[Action] メニューから [Forward] を選択します。アソシエートを禁止するアドレスについては、[Block] を選択します。[Default Action] メニューから [Block All] を選択します。

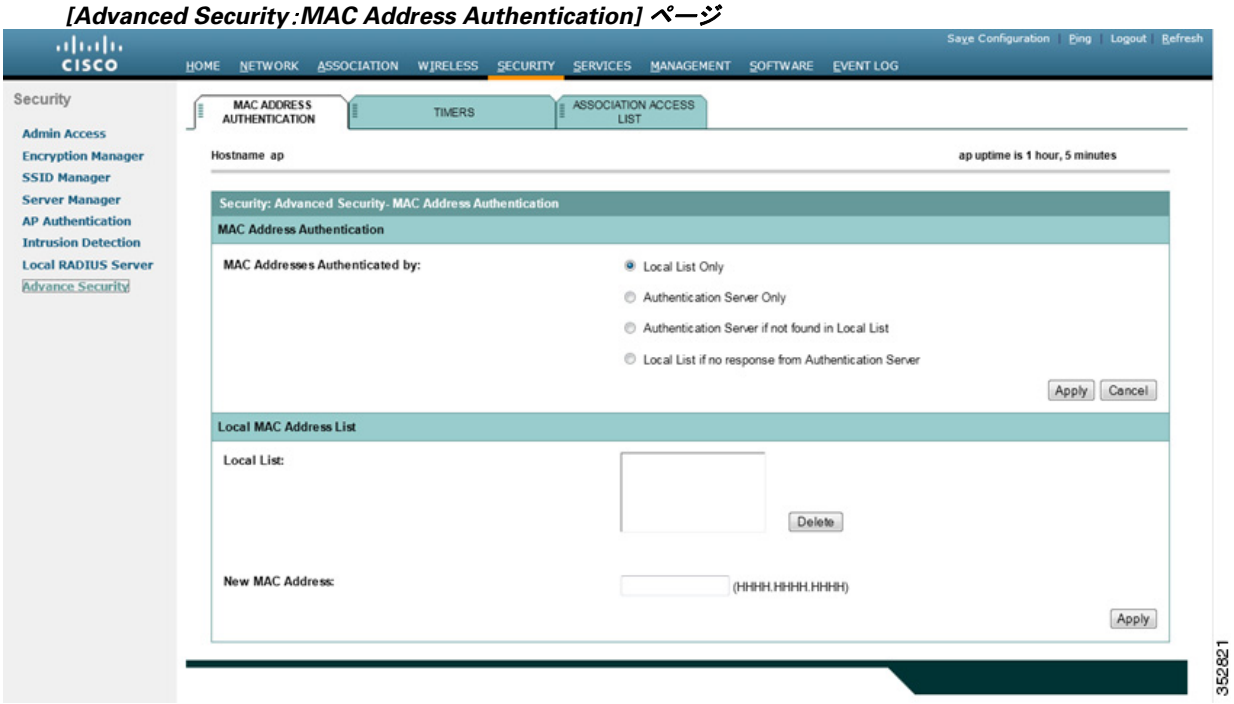
ステップ 2　[Security] をクリックして [Security Summary] ページを表示します。図 16-3 は、[Security Summary] ページを示しています。

図 16-3　[Security Summary] ページ



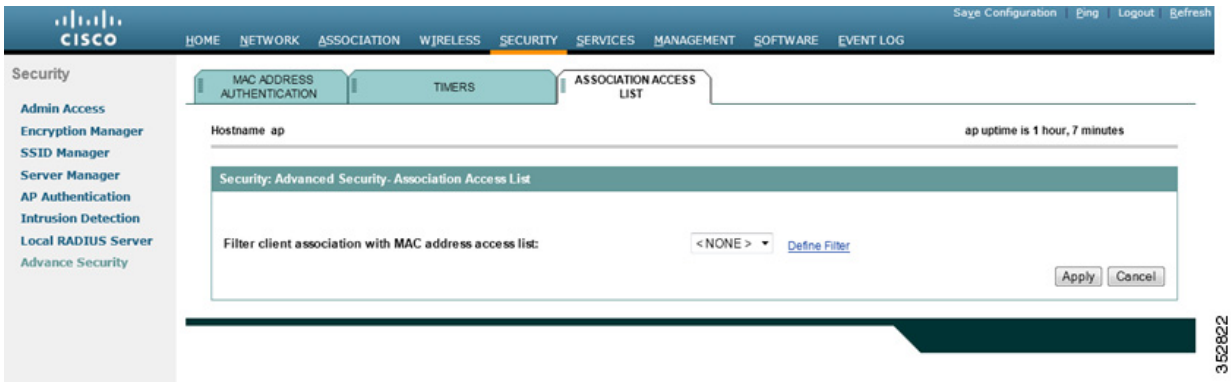
ステップ 3　[Advanced Security] をクリックして、[Advanced Security: MAC Address Authentication] ページを表示します。図 16-4 は、[MAC Address Authentication] ページを示しています。

図 16-4　[Advanced Security:MAC Address Authentication] ページ



ステップ 4　[Association Access List] タブをクリックして [Association Access List] ページを表示します。図 16-5 は [Association Access List] ページを示しています。

図 16-5　[Association Access List] ページ



ステップ 5　ドロップダウン リストから、必要な MAC アドレス ACL を選択します。

ステップ 6　[Apply] をクリックします。

MAC アドレス ACL を使用した CLI によるアクセス ポイントへのクライアント アソシエーションの許可と禁止

CLI でアソシエーション フィルタを作成するには、次の手順を実行します。

ステップ 1　コマンド **access-list** *number-700-799* を使用した MAC アドレス アクセス リストの作成

ステップ 2　グローバル コンフィギュレーション コマンド **dott11 association mac-list** *list-number* を使用して、MAC アドレスをすべての無線ですべてのワイヤレス クライアント アソシエーションのフィルタとして適用します。
MAC アドレス アクセス リストに記載されていないクライアントは、どの AP 無線でも AP SSID にアソシエートすることはできません。

次の例は、グローバル MAC アドレス アソシエーション フィルタとして MAC アドレス アクセス リスト 702 を使用しています。

```
ap(config)# dot11 association mac-list 702
ap(config)# end
```

MAC アドレス認証の設定

インターフェイスに適用された MAC アドレス フィルタは、使用されている SSID に関係なく、そのインターフェイスを介してトラフィックを送信する MAC アドレスをフィルタします。グローバル アソシエーション レベルで適用される MAC アドレス フィルタは、使用中の SSID または SSID にアソシエートされている VLAN やインターフェイスに関係なく、アクセス ポイント SSID にアソシエートすることができる MAC アドレスをフィルタします。

また、ターゲット SSID にアソシエートすることができる MAC アドレスをフィルタするために MAC アドレスを使用することもできます。このプロセスは、MAC アドレス認証と呼ばれます。次の表は、Cisco IOS アクセス ポイントで利用可能な 3 つの MAC アドレス フィルタリング方法を比較しています。

方式	ターゲット	注
インターフェイス MAC アドレス フィルタ	特定のインターフェイスまたは VLAN	ターゲット インターフェイスまたは VLAN にマッピングされたすべての SSID に適用
アソシエーション MAC アドレス	AP、グローバル	AP にアソシエートされているすべてのワイヤレス クライアントのすべての SSID およびすべての VLAN に適用
SSID MAC アドレス認証	特定の SSID	SSID がマッピングされる無線、インターフェイス、VLAN に関係なく特定の SSID に適用

認証に使用される MAC アドレスは、アクセス ポイント ローカル リストまたは認証サーバで確認できます。認証サーバは外部 RADIUS サーバまたは AP 内部 RADIUS サーバを指定できます。

SSID で MAC アドレス認証を使用するように AP を設定するには、次の手順を実行する必要があります。

ステップ 1　MAC アドレス認証のソースを特定します（ローカル リスト、ローカル AP RADIUS サーバ、外部 RADIUS サーバ）。
ローカル RADIUS サーバの AP ローカル リストを使用する場合は、AP で MAC アドレスを作成します（それぞれ RADIUS サーバの AP ローカル リストで）

ステップ 2　定義したメソッドを使用するよう SSID を設定します。

MAC 認証ソースの特定

SSID MAC 認証の MAC アドレス検証のソースを定義するには、[Security] > [Advanced Security] > [MAC Address Authentication] に移動します。

[MAC Address Authentication] タブで、次を実行します。

- ターゲット SSID でクライアント MAC アドレスを認証するためにローカル ページで定義した MAC アドレス リストを専用で使用するには、[Local List Only] オプションをクリックします。
- SSID MAC アドレス認証でローカル MAC アドレス リストをプライマリ MAC アドレス認証メソッドとして使用するとき、MAC アドレス用に外部 RADIUS サーバに作成したリストがローカル リストにない場合は、[Authentication Server if not found in the local list] オプションをクリックします。
- 外部 RADIUS サーバ（またはアクセス ポイント内部 RADIUS サーバ）を主に使用し、外部サーバが応答しない場合にのみ同じページのローカル リストに戻る場合は、[Local list if no response from Authentication server] オプションをクリックします。
- 外部 RADIUS サーバまたは AP 内部 RADIUS サーバのみを使用し、ローカル ページで定義した MAC アドレスは使用しない場合は、[Authentication Server Only] オプションをクリックします。

[Apply] をクリックして選択を確認します。

CLI を使用すると、グローバル コマンド **aaa authentication login mac_methods** を使用して MAC アドレスの検証のソースを特定できます。

次の例では、ローカル リストを使用するように AP を設定し、ローカル リストに MAC アドレスがない場合にのみ rad_mac と呼ばれる RADIUS サーバのグループに戻ります。

```
ap(config)# aaa authentication login mac_methods local group rad_mac
```

RADIUS サーバのグループを作成する方法の詳細については、第 11 章「認証タイプの設定」を参照してください。

ローカル MAC アドレスのリストの使用

SSID MAC アドレスの認証用に MAC アドレス認証ページで定義されている MAC アドレスのリストを使用するには、ターゲット SSID で認証が許可されている MAC アドレスをページの下で入力します（1 つずつ）。

（注） リストはグローバルです。リストで定義された MAC アドレスは、MAC アドレス認証が有効な任意の SSID に参加できます。AP で SSID ごとに異なる MAC アドレスのリストを使用する場合、外部 RADIUS サーバを使用する必要があります。

CLI で、MAC アドレスの認証で使用する MAC アドレスをユーザーとして入力し、パスワードは mac-address を使用します。その後、ユーザーには AP インターフェイスにアクセスしないよう、*exit* 自動コマンドが割り当てられます。次の例では、グローバル リストに MAC アドレス 1111.2222.3333 を作成します。

```
ap(config)# username 111122223333 password 0 111122223333
ap(config)# username 111122223333 autocommand exit
ap(config)# end
```

MAC アドレス認証用の AP 内部 RADIUS サーバの使用

AP 内部 RADIUS サーバ ページで定義された MAC アドレスのリストを使用するには、[Security] > [Local RADIUS Server] > [General Setup] にアクセスします。

[General Setup] ページで、[Enable Authentication Protocols] セクションの [MAC] チェックボックスをオンにして、MAC 認証用のサーバをイネーブルにします。次に [Apply] をクリックして確認します。

AP 内部 RADIUS サーバを使用する場合、AP を RADIUS クライアントとして定義する必要があります。そのためには次を実行します。

ステップ 1　[Network Access Server (AAA Clients)] セクションで、[Network Access Server] フィールドに AP の IP アドレスを入力します。

ステップ 2　[Shared Secret] を入力します。これは AP IP アドレスをソースとするクエリを認証するために使用するパスワードです。[Server Manager] ページで AP を RADIUS サーバとして設定する場合、同じ共有秘密を定義する必要があります。

ステップ 3　[Apply] をクリックして確認します。

CLI コマンドを含め、AP ローカル RADIUS サーバの設定方法の詳細については、第 11 章「認証タイプの設定」を参照してください。

ターゲット SSID で MAC 認証に使用する個別の MAC アドレスを作成するには、[Individual Users] セクションで、次を実行します。

ステップ 1　[Username] および [Password] の両方のフィールドで、区切り文字なしでターゲット MAC アドレスを入力します。

ステップ 2　[MAC authentication only] チェックボックスをオンにします。

ステップ 3　[Apply] をクリックして確認します。

（注）　AP 内部 RADIUS サーバで定義された MAC アドレスはグローバルです。
MAC アドレスの検証に認証サーバを使用するよう AP を設定する場合、MAC 認証およびローカル AP RADIUS サーバを使用するように設定されたすべての SSID はローカル リストを確認します。
SSID MAC 認証のソースとして AP グローバル MAC アドレスのリストを使用することと AP 内部認証サーバを使用することの主な違いは、グローバル リストは MAC アドレス認証を使用するように設定されたすべての SSID に適用されることです。MAC 認証で認証サーバを使用するよう選択する場合、一部の SSID は AP 内部サーバ リストを使用でき、他の SSID は外部 RADIUS サーバ リストを使用できます。

CLI で、ローカル RADIUS サーバ コンフィギュレーション サブモードを開始し、ユーザを作成することにより、MAC アドレス ユーザを追加できます。ユーザ名とパスワードは MAC アドレスで、区切り文字は使用しません。キーワード mac-only を追加して、ユーザが MAC 認証で使用されることを指定します。

次の例では、MAC アドレス ユーザ 333344445555 を作成します。

```
ap(config)# radius-server local
ap(config-radsrv)# user 333344445555 password 0 333344445555 mac-auth-only
ap(config-radsrv)# end
```

AP 内部 RADIUS サーバを使用する場合、[Security] > [Server Manager] ページで、AP を RADIUS サーバとして定義する必要があります。

[Corporate Servers] セクションで、AP に新しいサーバを追加できます。そのためには次を実行します。

ステップ 1　[Server] フィールドに AP の IP アドレスを入力します。

ステップ 2　前のページで AP を RADIUS クライアントとして定義したときに入力したのと同じ [Shared Secret] を入力します。

ステップ 3　[Authentication Port] は 1812 と入力します。

ステップ 4　[Accounting Port] は 1813 と入力します。

ステップ 5　[Apply] をクリックして確認します。

ステップ 6　[Default Server Priorities] セクションで、[MAC Authentication] プライオリティ リストの [Priority 1] フィールドで AP を選択します。

ステップ 7　[Apply] をクリックして確認します。

MAC アドレス認証用の外部 RADIUS サーバの使用

MAC 認証で外部 RADIUS サーバを使用する場合、[Security] > [Server Manager] > [Corporate Servers] セクションに、外部 RADIUS サーバの詳細を入力します。また、[Default Server Priorities] > [MAC Authentication] リストから、少なくとも 1 つのサーバを選択します。

MAC の SSID 認証の設定

MAC アドレスのソースを定義し、MAC アドレスを定義した後（ローカル リストまたは AP 内部 RADIUS サーバを使用する場合）、MAC 認証を使用するようにターゲット SSID を設定する必要があります。そのためには次を実行します。

ステップ 1　[Security] > [SSID Manager] ページにアクセスします。

ステップ 2　新しい SSID を選択または作成します。

ステップ 3　[Client Authentication Settings] セクションで、同意した各認証メソッドのチェックボックスをオンにします。その後、対応するドロップダウン リストから、[With MAC Authentication] を選択します。

ステップ 4　[Security] > [Advanced Security] ページに定義されたデフォルト メソッド、および [Security] > [Server Manager] ページに定義されたデフォルト サーバを使用するには（該当する場合）、[MAC Authentication Servers] セクションで [Use Defaults] オプションをクリックします。
[Security] > [Server Manager] ページで定義されたものとは異なるサーバを使用するには、[Customize] オプションをクリックして、使用するサーバを選択します。
[Customize] オプションは、ローカル リストまたはサーバを使用するかどうかを定義する [Security] > [Advanced Security] ページの設定をオーバーライドすることはありません。内部リストだけを使用するように AP を設定した場合、[SSID] ページの [Customize] オプションを選択しても影響はありません。[Customize] オプションは、MAC サーバが [Security] > [Advanced Security] ページで選択されている場合に、MAC サーバを選択する目的で提供されています。

ステップ 5　[Apply] をクリックして確認します。

Time-Based ACL の作成

Time-based ACL は、一定の時間、有効または無効にできる ACL です。この機能は、特定の種類のトラフィックを許可または拒否するアクセス コントロール ポリシーを定義する柔軟性と堅牢性を提供します。

この例は、CLI で Time-based ACL を設定する方法を説明しています。ここでは、平日の就業時間中、内部から外部への Telnet 接続が許可されています。

（注）　Time-based ACL は、必要に応じて Aironet AP のギガビット イーサネット ポートまたは無線ポートで定義できます。Bridge Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）に適用されることはありません。

次の手順に従って Time-based ACL を作成します。

ステップ 1　CLI で AP にログインします。

ステップ 2　イーサネット インターフェイスまたは無線インターフェイスを介して ACL にアクセスするには、コンソール ポートまたは Telnet を使用します。

ステップ 3　グローバル コンフィギュレーション モードを開始します。

ステップ 4　Time Range を作成します。この例では Test です。

ap(config-time-range)# **time-range Tes**t

ステップ 5　time-range を作成します。

ap(config-time-range)# **time-range periodic weekdays 7:00 to 19:00**

（注）　平日の 7:00 ～ 19:00 時までユーザのアクセスを許可します。

ステップ 6　ACL を作成します。この例では、101:

ap(config)# **ip access-list extended 101**

ap(config-ext-nacl)# **permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test**

（注）　この ACL は、Test で指定した時間範囲の間、ネットワークへの Telnet トラフィックの出入りを許可します。また、AP IP アドレスが 172.16.1.0 サブネットにある場合、平日は AP への Telnet セッションを許可します。

ステップ 7　Time-based ACL をイーサネット インターフェイスに適用します。

ap(config)# **interface gigabitEthernet 0**

ap(config-if)# **ip address 172.16.1.10 255.255.255.0**

ap(config-if)# **ip access-group 101 in**

ACL ロギング

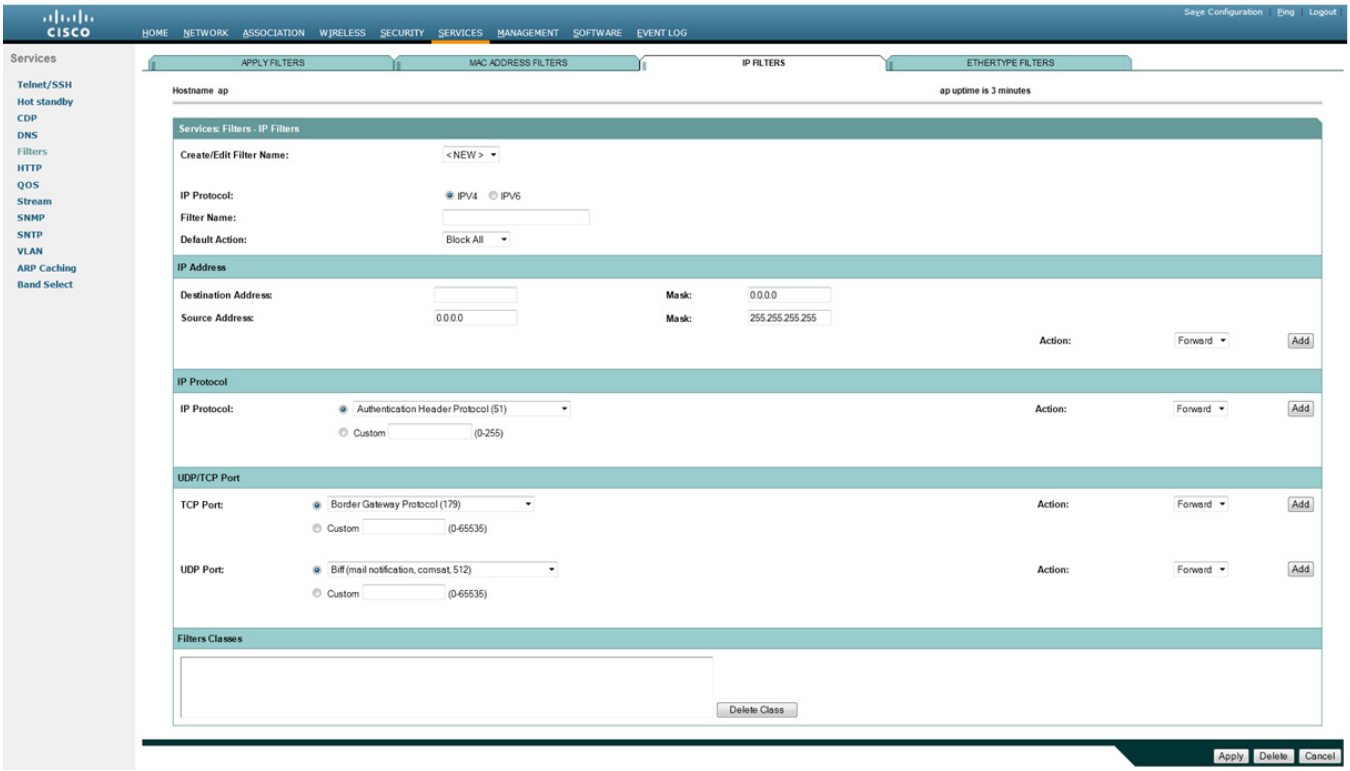
ACL ロギングは、AP プラットフォームのブリッジング インターフェイスではサポートされていません。ブリッジング インターフェイスに適用すると、「log」オプションを指定せずに設定したかのように動作し、ロギングは行われません。ただし、BVI インターフェイスに対しては、独立した ACL が使用される限り、ACL ロギングは行われます。

IP フィルタの設定と有効化

IP フィルタ（IP アドレス、IP プロトコル、および IP ポート）は、アクセス ポイントのイーサネット ポートや無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。また、IP アドレス フィルタを使用して、特定の IP アドレスとの間で送受信されるユニキャスト パケットやマルチキャスト パケットの転送を許可または禁止することができます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。IP フィルタ方法の 1 つ、2 つ、または 3 つすべての要素をすべて含むフィルタを作成できます。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。

[IP Filters] ページを使用して、アクセス ポイントの IP フィルタを作成します。図 16-6 は、[IP Filters] ページを示しています。

図 16-6　　[IP Filters] ページ



[IP Filters] ページは、次のリンク パスに従って表示します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [IP Filters] タブをクリックします。

IP フィルタの作成

IP フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、[IP Filters] ページを表示します。

ステップ 2　新規フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>]（デフォルト）が選択されていることを確認します。既存のフィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ名を選択します。

ステップ 3　[Filter Name] フィールドに、新しいフィルタにつける、わかりやすい名前を入力します。

ステップ 4　フィルタのデフォルト アクションとして、[Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、IP アドレス、IP プロトコル、IP ポートに適用されるフィルタを作成し、これらすべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。

ステップ 5　IP アドレスをフィルタリングするには、[IP Address] フィールドにアドレスを入力します。

（注）　許可された MAC アドレスを除き、すべての IP アドレスへのトラフィックを禁止する場合は、自分の PC のアドレスを許可された MAC アドレスのリストに入力し、アクセス ポイントへの接続が失われないようにします。

ステップ 6　[Mask] フィールドに、この IP アドレスで使用するマスクを入力します。このマスクは、たとえば、172.31.24.10 のように、ピリオドを使って、文字のグループに分けて入力します。マスクに 255.255.255.255 を指定した場合、このアクセス ポイントはすべての IP アドレスを受け付けるようになります。0.0.0.0 を指定した場合、[IP Address] フィールドに入力した IP アドレスと完全に一致するアドレスが検索されます。このフィールドに入力したマスクは、CLI に入力したマスクと同様の動作をします。

ステップ 7　[Action] メニューから [Forward] または [Block] を選択します。

ステップ 8　[Add] をクリックします。追加したアドレスが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからアドレスを削除するには、そのアドレスを選択して [Delete Class] をクリックします。このフィルタにさらにアドレスを追加するには、ステップ 5 からステップ 8 を繰り返します。

フィルタに IP プロトコルや IP ポート要素を追加する必要がない場合は、ステップ 15 にスキップして、アクセス ポイントにフィルタを保存します。

ステップ 9　IP プロトコルをフィルタリングするには、[IP Protocol] ドロップダウン リストから共通プロトコルの 1 つを選択するか、[Custom] オプション ボタンを選択して、既存の ACL 番号を [Custom] フィールドに入力します。ACL 番号を 0 ～ 255 の範囲で入力します。IP プロトコルと対応する識別番号の一覧については、付録 A「プロトコル フィルタ」を参照してください。

ステップ 10　[Action] メニューから [Forward] または [Block] を選択します。

ステップ 11　[Add] をクリックします。追加したプロトコルが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからプロトコルを削除するには、そのプロトコルを選択して [Delete Class] をクリックします。このフィルタにさらにプロトコルを追加するには、ステップ 9 からステップ 11 を繰り返します。

フィルタに IP ポート要素を追加する必要がない場合は、ステップ 15 にスキップして、アクセス ポイントにフィルタを保存します。

ステップ 12　TCP、または UDP ポート プロトコルをフィルタリングするには、[TCP Port]、または [UDP Port] ドロップダウン リストから共通ポート プロトコルの 1 つを選択するか、[Custom] オプション ボタンを選択して、既存のプロトコル番号を [Custom] フィールドの 1 つに入力します。プロトコル番号を 0 ～ 65535 の範囲で入力します。IP ポート プロトコルと対応する識別番号の一覧については、付録 A「プロトコル フィルタ」を参照してください。

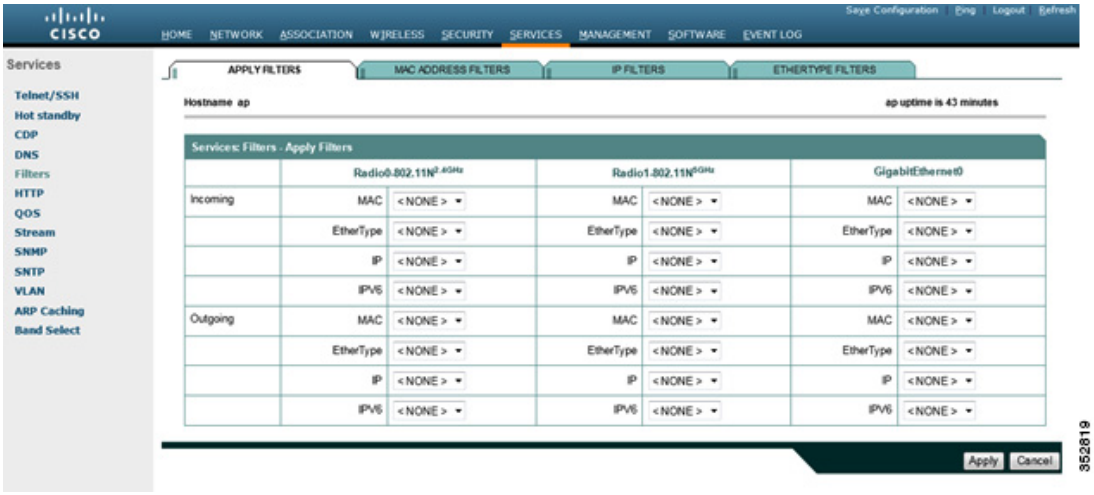
ステップ 13　[Action] メニューから [Forward] または [Block] を選択します。

ステップ 14　[Add] をクリックします。追加したプロトコルが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからプロトコルを削除するには、そのプロトコルを選択して [Delete Class] をクリックします。このフィルタにさらにプロトコルを追加するには、ステップ 12 からステップ 14 を繰り返します。

ステップ 15　フィルタが完成したら、[Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。

ステップ 16　[Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。図 16-7 は、[Apply Filters] ページを示しています。

図 16-7　[Apply Filters] ページ



ステップ 17　IP ドロップダウン リストの 1 つから、フィルタ名を選択します。フィルタはイーサネット ポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。

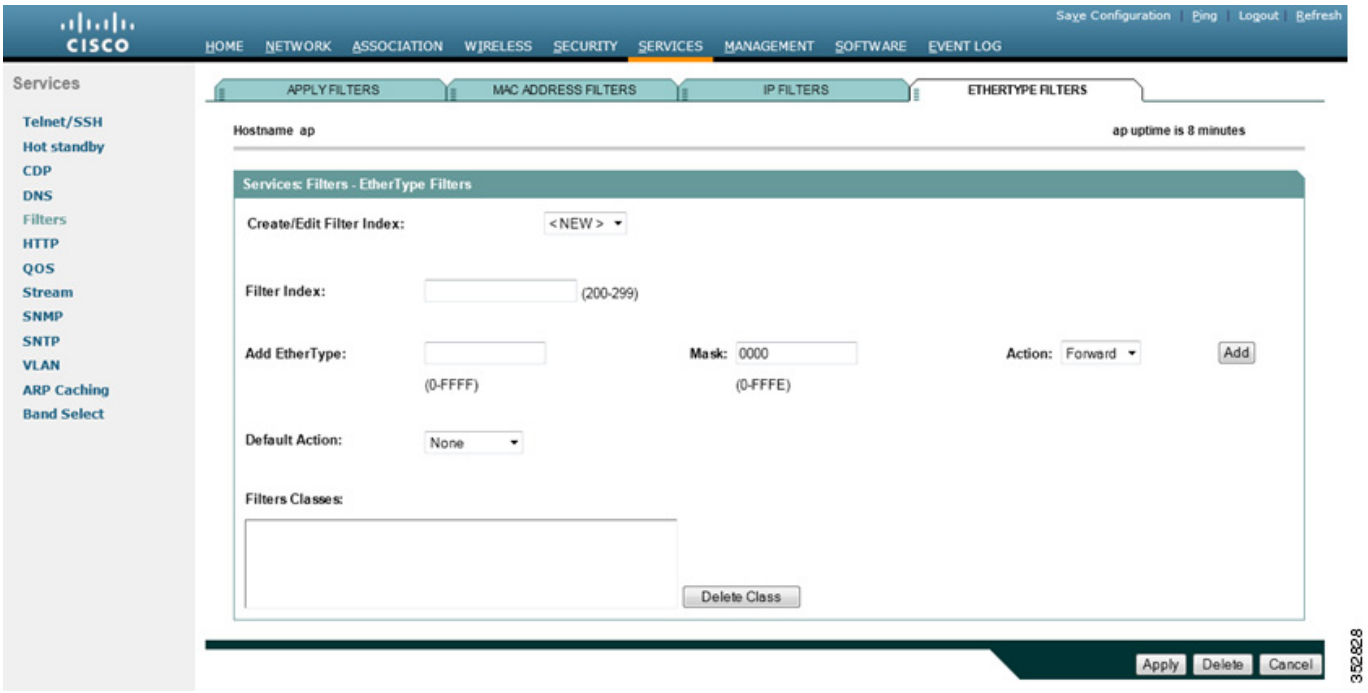
ステップ 18　[Apply] をクリックします。選択したポートで、このフィルタが有効化されます。

EtherType フィルタの設定と有効化

EtherType フィルタは、アクセス ポイントのイーサネット ポートと無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。

[EtherType Filters] ページを使用して、アクセス ポイントの EtherType フィルタを作成します。図 16-8 は、[EtherType Filters] ページを示しています。

図 16-8　[EtherType Filters] ページ



次のリンク パスに従って、[EtherType Filters] ページを表示します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [EtherType Filters] タブをクリックします。

EtherType フィルタの作成

EtherType フィルタを作成する手順は、次のとおりです。

ステップ 1　リンク パスに従って、[EtherType Filters] ページを表示します。

ステップ 2　新規フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>]（デフォルト）が選択されていることを確認します。既存のフィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ番号を選択します。

ステップ 3　[Filter Index] フィールドで、フィルタに 200 ～ 299 の範囲で番号を付けます。割り当てた番号で、フィルタのアクセス コントロール リスト（ACL）が作成されます。

ステップ 4　[Add EtherType] フィールドに EtherType 番号を入力します。プロトコルと対応する識別番号の一覧については、付録 A「プロトコル フィルタ」を参照してください。

ステップ 5　[Mask] フィールドに、この EtherType で使用するマスクを入力します。マスクに **0** を指定した場合、EtherType との正確な一致が必要になります。

ステップ 6　[Action] メニューから [Forward] または [Block] を選択します。

ステップ 7　[Add] をクリックします。追加した EtherType が [Filters Classes] フィールドに表示されます。[Filters Classes] リストから EtherType を削除するには、その EtherType を選択して [Delete Class] をクリックします。このフィルタにさらに Ethertype を追加するには、ステップ 4 からステップ 7 を繰り返します。

ステップ 8　[Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つの EtherType のアクションの逆である必要があります。たとえば、複数の EtherType を入力したときに、これらの Ethertype すべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。

ステップ 9　[Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。

ステップ 10　[Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。

ステップ 11　[EtherType] ドロップダウン リストの 1 つから、フィルタ番号を選択します。フィルタはイーサネット ポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。

ステップ 12　[Apply] をクリックします。選択したポートで、このフィルタが有効化されます。

CDP の設定

この章では、アクセス ポイントに Cisco Discovery Protocol（CDP）を設定する方法について説明します。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco Aironet IOS Command Reference for Access Points and Bridges*』、およびリリース 12.2 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

CDP の概要

Cisco Discovery Protocol（CDP）は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャスト アドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。CDP パケット内の情報は、Cisco Prime Infrastructure2000 などのネットワーク管理ソフトウェアで使用されます。

CDP は、特定のネットワーク デバイスのネイバーについて確認するために、ネットワーク管理で使用されます。アクセス ポイントの無線ポートでは、無線がアクセス ポイントやブリッジなどの他の無線インフラストラクチャ デバイスにアソシエートされている場合だけ CDP が有効です。CDP は、アクセス ポイントに設定された最小の VLAN 番号に送信されます。無線ネットワークで複数の VLAN が使用される場合、設定された最小の VLAN 番号をネイティブ VLAN として使用することを推奨します。

（注）　無線 LAN で最大限のパフォーマンスを得るために、VLAN がアクセス ポイントで有効になっている場合は、すべての無線インターフェイスおよびサブインターフェイスで CDP を無効にします。

CDP の設定

この項では、CDP の設定情報と設定の手順を説明します。

- 「CDP のデフォルト設定」（P.17-2）
- 「CDP 特性の設定」（P.17-2）
- 「CDP のディセーブル化およびイネーブル化」（P.17-3）
- 「インターフェイス上での CDP のディセーブル化およびイネーブル化」（P.17-4）

CDP のデフォルト設定

表 17-1は、デフォルトの CDP 設定を示しています。

表 17-1　CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP 保持時間（パケットの保持時間、秒）	180
CDP タイマー（パケットの送信間隔、秒）	60

CDP 特性の設定

CDP 保持時間（アクセス ポイントが CDP パケットを廃棄するまでの秒数）と CDP タイマー（アクセス ポイントが次の CDP パケットを送信するまでの秒数）を設定できます。

特権 EXEC モードから、次の手順に従って CDP 保持時間と CDP タイマーを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp holdtime** *seconds*	（任意）デバイスから送信された情報を受信側デバイスが廃棄するまで保持する期間を指定します。 有効範囲は 10 ～ 255 秒で、デフォルトは 180 秒です。
ステップ 3	**cdp timer** *seconds*	（任意）CDP 更新の送信頻度（秒）を設定します。 有効範囲は 5 ～ 254 秒で、デフォルトは 60 秒です。
ステップ 4	**cdp advertise-v2**	（任意）CDP がバージョン 2 アドバタイズを送信するように設定します。
ステップ 5	**cdp log mismatch duplex**	（任意）CDP によって生成されたデュプレックス ミスマッチを記録します。
ステップ 6	**cdp source-interface BVI1**	（任意）すべての CDP メッセージで BVI1 インターフェイス IP アドレスを挿入します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

次の例は、CDP 特性を設定し、確認する方法を示しています。

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end

AP# show cdp

Global CDP information:
        Sending a holdtime value of 120 seconds
        Sending CDP packets every 50 seconds
```

その他の CDP **show** コマンドについては、「CDP のモニタおよびメンテナンス」（P.17-5）を参照してください。

CDP のディセーブル化およびイネーブル化

CDP はデフォルトで有効になっています。特権 EXEC モードから、次の手順に従って CDP デバイス検出機能を無効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no cdp run**	CDP をディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

特権 EXEC モードから、次の手順に従って CDP を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**cdp run**	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。

次の例は CDP を有効にする方法を示しています。

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

インターフェイス上での CDP のディセーブル化およびイネーブル化

デフォルトでは、CDP は CDP 情報の送受信がサポートされるすべてのインターフェイスで有効になっています。

特権 EXEC モードから、次の手順に従ってインターフェイス上の CDP を無効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、CDP をディセーブルにするインターフェイスを入力します。
ステップ 3	**no cdp enable**	インターフェイスの CDP をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特権 EXEC モードから、次の手順に従ってインターフェイス上の CDP を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始し、CDP をイネーブルにするインターフェイスを入力します。
ステップ 3	**cdp enable**	ディセーブルになっているインターフェイスの CDP をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

次の例はインターフェイスで CDP を有効にする方法を示しています。

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```

CDP のモニタおよびメンテナンス

デバイス上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
clear cdp counters	トラフィック カウンタをゼロにリセットします。
clear cdp table	ネイバーに関する情報を格納する CDP テーブルを削除します。
show cdp	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を表示します。
show cdp entry *entry-name* [**protocol** | **version**]	特定のネイバーに関する情報を表示します。 アスタリスク(*)を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブルになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
show cdp interface [*type number*]	CDP がイネーブルに設定されているインターフェイスに関する情報を表示します。 表示対象を、インターフェイスのタイプまたは情報が必要なインターフェイスの番号に限定できます(たとえば、**gigabitethernet 0/1** と入力すると、ギガビット イーサネット ポート 1 に関する情報だけが表示されます)。
show cdp neighbors ［*type number*］ [**detail**]	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバーに関する情報を表示します。 表示対象を特定のタイプのネイバーやインターフェイスの番号に限定することも、表示対象を拡大してより詳細な情報を得ることもできます。
show cdp traffic	CDP カウンタ(送受信されたパケット数、チェックサム エラーなど)を表示します。

次に、CDP の **show** 特権 EXEC コマンドの 6 つの出力例を示します。

```
AP# show cdp
Global CDP information:
        Sending CDP packets every 50 seconds
        Sending a holdtime value of 120 seconds

AP# show cdp entry *
-------------------------
Device ID: AP
Entry address(es):
IP address: 10.1.1.66
Platform: cisco WS-C3550-12T,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/2,  Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 129 sec
```

```
Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Experimental Version 12.1(20010612:021
316) [jang-flamingo 120]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 06-Jul-01 18:18 by jang

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010221FF0000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full

-------------------------
Device ID: idf2-1-lab-l3.cisco.com
Entry address(es):
IP address: 10.1.1.10
Platform: cisco WS-C3524-XL,  Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/10
Holdtime : 141 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.1)XP, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 10-Dec-99 11:16 by cchang

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=25, value=0000000
0FFFFFFFF010101FF000000000000000142EFA400FF
VTP Management Domain: ''

AP# show cdp entry * protocol
Protocol information for talSwitch14 :
IP address: 172.20.135.194
Protocol information for tstswitch2 :
IP address: 172.20.135.204
  IP address: 172.20.135.202
Protocol information for tstswitch2 :
IP address: 172.20.135.204
  IP address: 172.20.135.202

AP# show cdp interface
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/4 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
```

```
  Holdtime is 180 seconds
GigabitEthernet0/6 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/7 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/8 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

AP# show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device IDLocal InterfaceHoldtmeCapabilityPlatformPort ID
Perdido2Gig 0/6125R S IWS-C3550-1Gig0/6
Perdido2Gig 0/5125R S IWS-C3550-1Gig 0/5

AP# show cdp traffic
CDP counters :
        Total packets output: 50882, Input: 52510
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 50882, Input: 52510
```

CDP ロギングのイネーブル化

CDP ロギングをイネーブルにできます。CDP で特定されたデュプレックス ミスマッチに関連するエラーをログに記録するには、グローバル コンフィギュレーション コマンド **cdp log mismatch duplex** を使用します。特定のインターフェイスで CDP によって報告されたデュプレックス ミスマッチに関連するエラーをログに記録するには、インターフェイス レベルで同じコマンドを使用します。

次の例では、ギガビット イーサネットのインターフェイスで CDP によって特定されたデュプレックス ミスマッチに関連するエラーのロギングをイネーブルにしますが、無線 0 インターフェイスで CDP によって特定されたデュプレックス ミスマッチに関連するエラーのロギングはディセーブルにします。

```
ap(config)# int gigabitEthernet 0
ap(config-if)# cdp log mismatch duplex
ap(config)# interface dot11Radio 0
ap(config-if)# no cdp log mismatch duplex
ap(config-if)# end
```

CHAPTER 18

SNMP の設定

この章では、アクセス ポイントで簡易ネットワーク管理プロトコル（SNMP）を設定する方法について説明します。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points*』を参照してください。

SNMP の概要

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。SNMP マネージャは、Cisco Prime Infrastructure などのネットワーク管理システム（NMS）に統合できます。エージェントと管理情報ベース（MIB）は、アクセス ポイント上に置かれます。アクセス ポイント上で SNMP を設定する場合、マネージャとエージェント間の関連性を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイス パラメータやネットワーク データの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンク ステータス（アップまたはダウン）、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

この項では、次の概念を説明します。

SNMP バージョン

このソフトウェア リリースでは、次の SNMP バージョンをサポートします。

- SNMPv1：簡易ネットワーク管理プロトコル。RFC 1157 で定義される詳細なインターネット規格。
- SNMPv2C には、次の機能があります。
  - SNMPv2：簡易ネットワーク管理プロトコルのバージョン 2。RFC 1902 ～ 1907 で定義されるドラフト インターネット規格。
  - SNMPv2C：SNMPv2 のコミュニティ ベースの管理フレームワーク。RFC 1901 で定義される試用段階のインターネット プロトコル。
- SNMPv3 には、次の機能があります。
  - SHA および Message Digest 5（MD5; メッセージ ダイジェスト 5）認証プロトコルと DES56 暗号のサポート。
  - 3 つのセキュリティ レベル：認証なしプライバシーなし（NoAuthNoPriv）、認証ありプライバシーなし（AuthNoPriv）、および認証ありプライバシーあり（AuthPriv）。

SNMPv3 は、SNMP 通信に利用できる高度なセキュリティをサポートしています。SNMPv1 と SNMPv2 のコミュニティ ストリングは、暗号化なしのプレーン テキストとして格納、転送されます。SNMPv3 セキュリティ モデルでは、SNMP ユーザはユーザ グループの認証と参加を行います。システム データへのアクセスは、グループに基づいて制限されます。

SNMP エージェントは、管理ステーションでサポートされる SNMP のバージョンを使用するように設定する必要があります。エージェントは複数のマネージャと対話できるため、SNMPv3 プロトコルを使用する管理ステーションや、SNMPv2 または SNMPv1 プロトコルを使用する管理ステーションとの通信をサポートするようにソフトウェアを設定できます。

表 18-1は、アクセス ポイントでサポートされている SNMP のバージョンとセキュリティ レベルを示しています。

表 18-1　SNMP のバージョンとセキュリティ レベル

SNMP バージョン	セキュリティ レベル	認証	暗号化
v1	NoAuthNoPriv	コミュニティ ストリングの一致	なし
v2C	NoAuthNoPriv	コミュニティ ストリングの一致	なし
v3	NoAuthNoPriv	ユーザ名の一致	なし
v3	AuthNoPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	なし
v3	AuthPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	データ暗号規格（DES）56 ビット暗号

SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 18-2 に示す動作を実行します。

表 18-2　SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。[1]
get-bulk-request[2]	テーブル内の複数行など、小さなデータ ブロックを数多く送信する代わりに、大きなブロックでデータを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

1. この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
2. **get-bulk** コマンドは、SNMPv2 に限り機能します。

SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- MIB 変数の取得：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- MIB 変数の設定：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリー トポロジが変更された場合、認証に失敗した場合などがあります。

SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がアクセス ポイントにアクセスするためには、NMS のコミュニティ ストリングの定義が少なくともアクセス ポイントの 3 つのコミュニティ ストリング定義のうち、1 つと一致している必要があります。

（注）　SNMP コミュニティは、SNMPv1 および SNMPv2c で使用されます。SNMPv3 はコミュニティを使用しません。

コミュニティ ストリングの属性は、次のいずれかです。

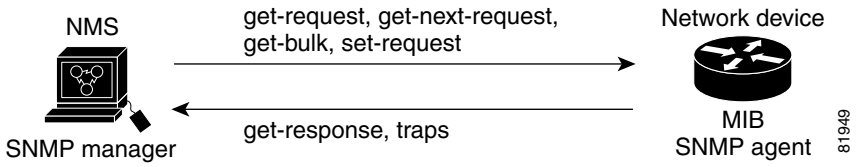
- 読み取り専用：許可された管理ステーションへの読み取りアクセスを、コミュニティ ストリングを除く MIB のすべてのオブジェクトに許可しますが、書き込みアクセスは許可しません。
- 読み取り/書き込み：許可された管理ステーションへの読み取りおよび書き込みアクセスを、MIB のすべてのオブジェクトに許可しますが、コミュニティ ストリングには許可しません。

SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、Cisco Prime Infrastructure ネットワーク管理ソフトウェアがあります。Cisco Prime Infrastructure ソフトウェアは、アクセス ポイント MIB 変数を使用して装置変数を設定し、ネットワーク上の装置をポーリングして特定の情報を取得します。ポーリング結果を表示および解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワーク パフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 18-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャにトラップ（特定のイベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、不適切なユーザ認証、再起動、リンク ステータス（起動または停止）、MAC アドレスの追跡などの、ネットワーク上の状況を SNMP マネージャに警告するメッセージです。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。

図 18-1　SNMP ネットワーク



サポート対象の MIB の詳細、およびアクセス手順については、付録 B「サポート対象 MIB」を参照してください。

SNMP の設定

この項では、アクセス ポイントで SNMP を設定する方法について説明します。内容は次のとおりです。

- 「SNMP のデフォルト設定」(P.18-5)
- 「SNMP エージェントのイネーブル化」(P.18-6)
- 「コミュニティ ストリングの設定」(P.18-6)
- 「SNMP サーバ グループ名の指定」(P.18-8)
- 「SNMP サーバ ホストの設定」(P.18-8)
- 「SNMP サーバ ユーザの設定」(P.18-9)
- 「トラップ マネージャの設定とトラップの有効化」(P.18-9)
- 「エージェント コンタクトおよびロケーションの設定」(P.18-12)
- 「snmp-server view コマンドの使用」(P.18-12)
- 「SNMP での例」(P.18-12)

SNMP のデフォルト設定

表 18-3 に、SNMP のデフォルト設定を示します。

表 18-3　SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル
SNMP コミュニティ ストリング	どのストリングもデフォルトでは設定されていません。しかし、Web ブラウザ インターフェイスを使って SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、*public* コミュニティを生成します。
SNMP トラップ レシーバ	未設定
SNMP トラップ	有効なトラップなし。

SNMP エージェントのイネーブル化

SNMP を有効にするための特定の CLI コマンドはありません。最初に入力したグローバル コンフィギュレーション コマンド **snmp-server** を使用すると、サポートされているバージョンの SNMP が有効になります。

また、Web ブラウザ インターフェイスの [SNMP Properties] ページで SNMP を有効にすることもできます。Web ブラウザ インターフェイスで SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、*public* と呼ばれるコミュニティ ストリングを生成します。

コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングはパスワードと同様に機能し、アクセス ポイント上のエージェントへのアクセスを許可します。

ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限

（注） 現在の Cisco IOS MIB エージェント実装では、デフォルトのコミュニティ ストリングは、インターネット MIB オブジェクト サブツリーに対するものです。IEEE802dot11 は、MIB オブジェクト ツリーの別のブランチのもとにあるため、IEEE802dot11 MIB 上の別のコミュニティ ストリングとビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ ストリングのいずれかを有効にする必要があります。ISO は、IEEE（IEEE802dot11）およびインターネットの共通の親ノードです。この MIB エージェントの動作は、Cisco IOS ソフトウェアを実行していないアクセス ポイントでの MIB エージェントの動作とは異なります。

特権 EXEC モードから、次の手順に従ってアクセス ポイントにコミュニティ ストリングを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	コミュニティ ストリングを設定します。 • *string* には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可するストリングを指定します。任意の長さのコミュニティ ストリングを 1 つまたは複数設定できます。 • （任意）*access-list-number* には、1 ～ 99 および 1300 ～ 1999 の標準 IP アクセス リスト番号を入力します。 • （任意）**view** *mib-view* には、**ieee802dot11** など、このコミュニティがアクセスできる MIB ビューを指定します。IEEE ビューを通じて標準 IEEE 802.11 MIB オブジェクトにアクセスする **snmp-server view** コマンドの使用方法については、「snmp-server view コマンドの使用」（P.18-12）を参照してください。 • （任意）許可された管理ステーションで MIB オブジェクトを取得する場合は、読み取り専用（**ro**）を指定し、許可された管理ステーションを使用して MIB オブジェクトを取得し、修正する場合は、読み取り/書き込み（**rw**）を指定します。デフォルトでは、コミュニティ ストリングはすべてのオブジェクトに対する読み取り専用アクセスを許可します。 **（注）** IEEE802dot11 MIB にアクセスするには、IEEE802dot11 MIB 上の別のコミュニティ ストリングとビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ ストリングを有効にする必要があります。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	（任意）ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。 • *access-list-number* には、ステップ 2 で指定したアクセス リスト番号を入力します。 • **deny** キーワードは、条件が一致した場合にアクセスを拒否します。**permit** キーワードは、条件が一致した場合にアクセスを許可します。 • *source* には、コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。 • （任意）*source-wildcard* には、source に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。 アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティ ストリングをヌル ストリングに設定します(コミュニティ ストリングに値を入力しないでください)。特定のコミュニティ ストリングを削除するには、**no snmp-server community** *string* グローバル コンフィギュレーション コマンドを使用します。

次の例は、コミュニティ ストリング *open* と *ieee* を SNMP に割り当てる方法、両方に対する読み取り/書き込みアクセスを許可する方法、*open* がすべてのオブジェクトのクエリに対するコミュニティ ストリングであることを指定する方法を示します。

```
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```

SNMP サーバ グループ名の指定

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server group [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}][**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	新しい SNMP グループの設定、または SNMP ユーザを SNMP ビューにマップするテーブルの設定を行います。

SNMP サーバ ホストの設定

SNMP トラップ操作の受信者を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server host *host* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	SNMP トラップ操作の受信者を設定します。

SNMP サーバ ユーザの設定

SNMP グループに新しいユーザを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
snmp-server user *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv password*]] [**access** *access-list*]	SNMP グループに新しいユーザを設定します。

トラップ マネージャの設定とトラップの有効化

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにアクセス ポイントが生成するシステム アラートです。デフォルトではトラップ マネージャは定義されておらず、トラップは発行されません。

この Cisco IOS Release を実行するアクセス ポイントには、トラップ マネージャを無制限に設定できます。コミュニティ ストリングの長さは任意です。

表 18-4 は、サポートされるアクセス ポイントのトラップ（通知タイプ）を示しています。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

表 18-4　通知タイプ

通知タイプ	説明
aaa_server	AAA イベントのトラップを有効にします。
authenticate-fail	認証の失敗のトラップを有効にします。
config	SNMP 設定変更のトラップを有効にします。
deauthenticate	クライアント デバイスの認証取り消しのトラップを有効にします。
disassociate	クライアント デバイスのアソシエーション解除のトラップを有効にします。
dot11-qos	QoS 変更のトラップを有効にします。
entity	SNMP のエンティティ変更のトラップを有効にします。
rogue-ap	不正なアクセス ポイントの検出のトラップを有効にします。
snmp	SNMP イベントのトラップを有効にします。
switch-over	切り替えのトラップを有効にします。
syslog	syslog トラップを有効にします。
wlan-wep	WEP トラップを有効にします。
cef	cef トラップを許可します
config-copy	SNMP config-copy トラップを許可します
config-ctid	SNMP config-ctid トラップを許可します
cpu	CPU に関連したトラップを許可します
dot11-mibs	dot11 トラップを許可します

表 18-4　通知タイプ（続き）

通知タイプ	説明
entity	SNMP entity トラップを許可します
l2tun-pseudowire-status	SNMP L2 pseudowire status トラップを許可します
l2tun-session	SNMP L2 session トラップを許可します
syslog	SNMP syslog トラップを許可します
tty	TCP connection トラップを許可します
udp-port	通知ホストの UDP ポート番号です
vrfmib	SNMP vrfmib トラップを許可します

udp-port などの一部の通知タイプは、グローバル コンフィギュレーション コマンド **snmp-server enable** で制御できません。これらの通知タイプは、常に有効です。表 18-4 に示す通知タイプを受信するには、特定のホストに対して **snmp-server host** グローバル コンフィギュレーション コマンドを実行します。

特権 EXEC モードから、次の手順に従ってホストにトラップを送信するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} *community-string* [**udp-port** *port*] *notification-type*	トラップ メッセージの受信側を指定します。 • *host-addr* には、(ターゲットの受信者)ホストの名前またはアドレスを指定します。 • SNMP トラップをホストに送信するには、**traps**(デフォルト)を指定します。SNMP 情報をホストに送信するには、**informs** を指定します。 • サポートする SNMP バージョンを指定します。informs にはバージョン 1(デフォルト)を使用できません。バージョン 3 には、次の 3 つのセキュリティ レベルがあります。 – **auth**:暗号化なしのパケットの認証を指定します。 – **noauth**:パケットの認証と暗号化をしないように指定します。 – **priv**:パケットの認証と暗号化を指定します。 • *community-string* には、通知動作時に送信するストリングを指定します。この文字列は **snmp-server host** コマンドを使用して設定できますが、**snmp-server community** コマンドでこの文字列を定義してから、**snmp-server host** コマンドを使用することを推奨します。 • *notification-type* には、表 18-4(P.18-9) 内のキーワードを使用します。
ステップ 3	**snmp-server enable traps** *notification-types*	アクセス ポイントで特定のトラップの送信を有効にします。トラップのリストは、表 18-4(P.18-9) を参照してください。 複数のタイプのトラップを有効にする場合、各トラップ タイプに **snmp-server enable traps** コマンドを個別に発行します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

指定したホストがトラップを受信しないようにするには、**no snmp-server host** *host* グローバル コンフィギュレーション コマンドを使用します。特定のトラップ タイプをディセーブルにするには、**no snmp-server enable traps** *notification-types* グローバル コンフィギュレーション コマンドを使用します。

エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**snmp-server contact** *text*	システムに関する問い合わせ先を表すストリングを設定します。 次に例を示します。 **snmp-server contact Dial System Operator at beeper 21555.**
ステップ 3	**snmp-server location** *text*	システムのロケーションを表すストリングを設定します。 次に例を示します。 **snmp-server location Building 3/Room 222**
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

snmp-server view コマンドの使用

グローバル コンフィギュレーション モードで **snmp-server view** コマンドを使用して、IEEE ビューおよび dot11 読み取り/書き込みコミュニティ ストリングを通じて、標準 IEEE 802.11 MIB オブジェクトにアクセスします。

次の例は、IEEE ビューと dot11 読み取り/書き込みコミュニティ ストリングを有効にする方法を示しています。

```
AP(config)# snmp-server view ieee ieee802dot11 included
AP(config)# snmp-server community dot11 view ieee RW
```

SNMP での例

次の例は、SNMPv1、SNMPv2C、および SNMPv3 を有効にする方法を示しています。この設定では、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定でアクセス ポイントがトラップを送信することはありません。

```
AP(config)# snmp-server community public
```

次の例は、コミュニティ ストリング *open* と *ieee* を SNMP に割り当てる方法、両方に対する読み取り/書き込みアクセスを許可する方法、*open* が非 IEEE802dot11-MIB オブジェクトのクエリに対するコミュニティ ストリングであり、*ieee* が IEEE802dot11 MIB オブジェクトのクエリに対するコミュニティ ストリングであることを指定する方法を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。また、アクセス ポイントは SNMPv1 を使用してホスト 192.180.1.111 と 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に設定トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c public
AP(config)# snmp-server host 192.180.1.111 version 1 public
AP(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
AP(config)# snmp-server community comaccess ro 4
AP(config)# snmp-server enable traps snmp authentication
AP(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。最初の行で、アクセス ポイントはそれまでに有効になったトラップ以外にエンティティ MIB トラップを送信できます。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドを無効にします。

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted entity
```

次の例は、アクセス ポイントがコミュニティ ストリング *public* を使用して、ホスト *myhost.cisco.com* にすべてのトラップを送信することを有効にする方法を示します。

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com public
```

次の例は、これらの SNMPv3 設定の方法を示しています。

- ビュー名（*iso*）
- IP アドレス *1.4.74.10* のリモート ホストに対して自身を識別するために、このエージェントが使用する SNMP エンジン ID（*1234567890*）
- プライバシー暗号をサポートする SNMPv3 グループ（*admin*）で、このグループのユーザは全員、（*iso*）ビューで定義されているすべてのオブジェクトに対する読み取りおよび書き込みアクセスが許可されています。
- admin グループに属する SNMP ユーザ（*joe*）で、クエリに MD5 認証を使用し、MD5 用のパスワードに *xyz123* を使用し、DES56 データ クエリ暗号を使用し、暗号キーとして *key007* を使用します。
- admin グループに属する SNMP ユーザ（*fred*）で、クエリに MD5 認証を使用し、MD5 用の暗号化されたパスワードに *abc789* を使用し、DES56 データ クエリ暗号を使用し、暗号キーとして *key99* を使用します。

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10 1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read iso write iso
AP(config)# snmp-server user joe admin v3 auth md5 xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3 encrypted auth md5 abc789 priv des56 key99
```

（注）　この例で最後のコマンドを入力すると、**show running-config** コマンドと **show startup-config** コマンドでは、一部の SNMP 設定だけが表示されるようになります。

SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。この表示のフィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

リピータ/スタンバイ アクセス ポイントおよびワークグループ ブリッジ モードの設定

この章では、アクセス ポイントをリピータ、ホット スタンバイ ユニット、またはワークグループ ブリッジとして設定する方法について説明します。

リピータ アクセス ポイントの概要

リピータ アクセス ポイントは有線 LAN には接続されません。インフラストラクチャの範囲を拡大したり、無線通信を妨げる障害物を回避したりするために、有線 LAN に接続されているアクセス ポイントの無線範囲内に配置されます。2.4 GHz 無線または 5 GHz 無線をリピータとして設定できます。2 つの無線を装備したアクセス ポイントでは、1 つの無線しかリピータにすることができません。もう 1 つの無線はシャットダウンするか、ルート、スキャナ、またはスペクトラム無線として設定する必要があります。

リピータは、別のリピータや、有線 LAN に接続されているアクセス ポイントにパケットを送信することによって、無線ユーザと有線 LAN との間でトラフィックを転送します。データは、クライアントに最高のパフォーマンスを提供するルートを経由して送信されます。アクセス ポイントをリピータとして設定した場合、アクセス ポイントのイーサネット ポートはトラフィックを転送しません。

複数のリピータ アクセス ポイントをチェーンとして設定することもできますが、リピータ チェーンの末端のクライアント デバイスのスループットは大幅に低下します。これは、それぞれのリピータが各パケットの受信と再送に同じチャネルを使用する必要があるため、チェーンに追加された各リピータのスループットが半分に減少することによります。

リピータのアクセス ポイントは、最適な接続を確立しているアクセス ポイントにアソシエートします。ただし、リピータがアソシエートするアクセス ポイントを指定することはできます。リピータとルート アクセス ポイント間に静的な特定のアソシエーションを設定すると、リピータのパフォーマンスが向上します。

リピータを設定するには、親（ルート）アクセス ポイントとリピータ アクセス ポイントの両方で Aironet 拡張機能を有効にする必要があります。Aironet 拡張機能はデフォルトで有効になっており、これらを使用すると、アクセス ポイントで、アソシエートされている Cisco Aironet クライアント デバイスの能力がより正確に認識されるようになります。Aironet 拡張機能を無効にすると、アクセス ポイントとシスコ以外のクライアント デバイス間の相互運用性が改善される場合があります。シスコ以外のクライアント デバイスでは、リピータ アクセス ポイントおよびリピータがアソシエートしているルート アクセス ポイントとの通信に問題が生じる場合があります。

SSID をアクセス ポイントとリピータとの間で使用するには、SSID で [Infrastructure SSID] オプションを有効にして、リピータ通信で AP を許可する必要があります。

インフラストラクチャ Service Set Identifier（SSID; サービス セット ID）はネイティブ VLAN に割り当てる必要があります。アクセス ポイントまたはワイヤレス ブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。

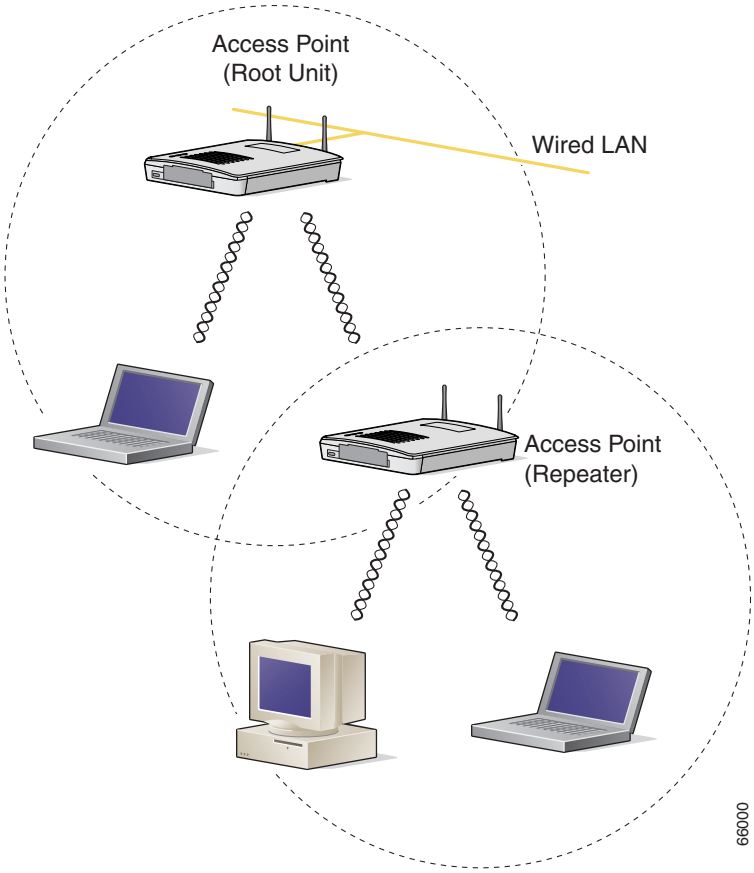
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

（注） アクセス ポイントは、各無線インターフェイスに対して仮想インターフェイスを生成するため、リピータ アクセス ポイントはルート アクセス ポイントに 2 回（実際のインターフェイスに 1 回、仮想インターフェイスに 1 回）アソシエートします。

（注） 無線は、リピータとして機能すると同時に他の SSID をサポートするよう設定することはできません。リピータ無線はネイティブ VLAN だけをリピートすることができます。無線をリピータとして設定した後、ネイティブ VLAN 以外の VLAN にマッピングされた SSID をその無線にマッピングすることはできません。ただし、もう 1 つの無線は複数の SSID と複数の VLAN をサポートするよう設定することができます。

図 19-1 は、リピータとして機能するアクセス ポイントを示しています。

図 19-1　　リピータとしてのアクセス ポイント



リピータ アクセス ポイントの設定

この項では、アクセス ポイントをリピータとして設定する手順について、次の項目で説明します。

- 「デフォルト設定」(P.19-4)
- 「リピータのガイドライン」(P.19-4)
- 「リピータの設定」(P.19-5)
- 「リピータ操作の確認」(P.19-7)
- 「アンテナの位置合わせ」(P.19-7)
- 「リピータの EAP-FAST クライアントとしての設定」(P.19-8)
- 「リピータの WPA2 クライアントとしての設定」(P.19-7)

デフォルト設定

アクセス ポイントは、デフォルトではルート ユニットとして設定されています。表 19-1 は、無線 LAN におけるアクセス ポイントの役割を制御する設定のデフォルト値を示しています。

表 19-1　無線 LAN での役割のデフォルト値

機能	デフォルト設定
ステーションの役割	Root
親	none
拡張機能	Aironet

リピータのガイドライン

リピータ アクセス ポイントを設定する場合は、次のガイドラインに従います。

- 高いスループットを要求しないクライアント デバイスを構成する場合は、リピータを使用します。リピータは無線 LAN のカバレッジ領域を拡大しますが、スループットを大きく減少させます。
- リピータは、それにアソシエートするクライアント デバイスのすべて、または大半が Cisco Aironet クライアントの場合に使用します。他社のクライアントが予想される場合、それらのクライアントが Aironet IE 拡張をサポートすることを確認します。このオプションは、AP とリピータとの間の通信を許可するために SSID で必要です。
- リピータ アクセス ポイントに設定されたデータレートが、親アクセス ポイントのデータ レートと一致しているかどうか確認してください。データ レートの設定については、「無線データ レートの設定」(P.6-9)を参照してください。
- リピータ無線で設定された SSID は、ネイティブ VLAN にマッピングする必要があります。

（注） Cisco IOS ソフトウェアを実行するリピータ アクセス ポイントは、IOS を実行しない親アクセス ポイントにアソシエートできません。

（注） リピータ 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。リピータ アクセス ポイントを WDS 候補として設定しないでください。また、WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。リピータは、必要なときにはいつでも WDS のインフラストラクチャに参加して WDS のクライアントとして機能できます。

（注） リピータの親として指定されているルート アクセス ポイント上で複数の Basic Service Set Identifier（BSSID）が設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のリピータが特定の親にアソシエートするように設定されている場合、親アクセス ポイント上で BSSID を追加または削除するときは、リピータのアソシエーションの状態を確認します。必要に応じて、アソシエートされていないデバイスを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

リピータの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントをリピータとして設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**ssid** *ssid-string*	リピータがルート アクセス ポイントにアソシエートするときに使用する SSID をコールします。次の手順で、この SSID をインフラストラクチャ SSID に指定します。ルート アクセス ポイントにインフラストラクチャ SSID を作成している場合、リピータにも同じ SSID を作成します。 SSID をインフラストラクチャ SSID に指定します。リピータは、この SSID を使用してルート アクセス ポイントにアソシエートします。**optional** キーワードを入力している場合を除き、インフラストラクチャ デバイスはこの SSID を使用して、リピータ アクセス ポイントにアソシエートする必要があります。 インフラストラクチャ Service Set Identifier（SSID; サービス セット ID）はネイティブ VLAN に割り当てる必要があります。アクセス ポイントまたはワイヤレス ブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。 `SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid`
ステップ 4	**station-role repeater**	アクセス ポイントの無線 LAN での役割をリピータに設定します。
ステップ 5	**dot11 extension aironet**	Aironet 拡張機能が無効になっている場合、Aironet 拡張機能を有効にします。

	コマンド	目的
ステップ 6	**parent** {*1-4*} *mac-address* [*timeout*]	(任意) リピータがアソシエートするアクセス ポイントの MAC アドレスを入力します。 • 最大 4 つの親アクセス ポイントの MAC アドレスを入力できます。このポイントには、1 ～ 4 の番号が指定されます。リピータは、必ずその親アクセス ポイントのリストからベストなアクセス ポイントにアソシエートしようとします。リピータは、「タイムアウト」オプションを設定しない限り、親リストにない MAC アドレスにはアソシエートしません。 **(注)** 複数の BSSID が親アクセス ポイント上で設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。 • (任意) タイムアウト値は秒単位で入力できますが、これはどれだけの時間、リピータがその親リストにあるアクセス ポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、リピータは親リストにないアクセス ポイントにアソシエートしようとします。 0 ～ 65535 秒の範囲のタイムアウト値を入力できます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	(任意) コンフィギュレーション ファイルに設定を保存します。

3 つの潜在的な親アクセス ポイントをもつリピータ アクセス ポイントの設定例を次に示します。このアクセス ポイントには、1 ～ 3 の番号が指定されます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-if)# station-role repeater
AP(config-if)# dot11 extension aironet
AP(config-if)# parent 1 0987.1234.h345
AP(config-if)# parent 2 7809.b123.c345
AP(config-if)# parent 3 6543.a456.7421
AP(config-if)# end
```

次の例は、1 つの親を親リストから除く方法を示しています。この例では、親 2 を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに 60 秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

次に、親リストでタイムアウト値をディセーブルにする方法の例を示します。

```
AP(config-if)# no parent timeout
```

アンテナの位置合わせ

アクセス ポイントをリピータとして設定するとき、**dot11 antenna-alignment** CLI コマンドを使用して、アクセス ポイントのアンテナを別のリモート アンテナと位置合わせできます。

コマンドによって位置合わせテストが開始します。無線は親からのアソシエーションが解除され、隣接する無線デバイスをプローブし、受け取る応答の MAC アドレスおよび信号強度を記録します。タイムアウトの後、無線は親と再アソシエートされます。

アンテナ位置合わせテストを実行する手順は、次のとおりです。

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードを開始します。
ステップ 2	**dot11 dot11radio { 0 | 1 } antenna-alignment timeout** *timeout-in-seconds*	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 • 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。 • *timeout-in-seconds*：アンテナ位置合わせテストがタイムアウトする前に実行される時間を秒単位で入力します。デフォルト値は 5 秒です。

show dot11 antenna-alignment コマンドを使用すると、プローブに最後に応答した 10 台のデバイスの MAC アドレスおよび信号レベルをリストします。

リピータ操作の確認

リピータを設定した後、リピータが正しく動作している場合、ルート アクセス ポイントのアソシエーション テーブルで、リピータ アクセス ポイントはルート アクセス ポイントにアソシエートされて表示されます。

リピータの WPA2 クライアントとしての設定

WPA キー管理では暗号化方式を組み合わせて用い、クライアント デバイスとアクセス ポイントとの通信を保護します。リピータ アクセス ポイントを、他の WPA2 対応のクライアント デバイスと同様に、ネットワークで認証されるよう設定できます。

特権 EXEC モードから、次の手順に従ってリピータを WPA2 クライアントとして設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ssid** *ssid-string*	SSID を無線インターフェイスにアソシエートします。
ステップ 3	**authentication open**	SSID 用の open 認証を有効にします。
ステップ 4	**authentication key-management wpa**	SSID 用の WPA 認証済みキー管理を有効にします。

	コマンド	目的
ステップ 5	**infrastructure ssid**	SSID を、リピータが他のアクセス ポイントにアソシエートするために使用する SSID として指定します。
ステップ 6	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	リピータ用に事前共有キーを入力します。 16 進数または ASCII 文字を使用して、キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合は、8 ～ 63 個の ASCII 文字を入力する必要があります。アクセス ポイントがキーを展開します。
ステップ 7	**exit**	SSID 設定サブモードを終了します。
ステップ 8	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 9	**encryption mode ciphers aes-ccm**	無線インターフェイスで AES CCMP 暗号化を有効にします。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

リピータの EAP-FAST クライアントとしての設定

リピータ アクセス ポイントを、他の無線クライアント デバイスと同様に、ネットワークで認証されるよう設定できます。リピータ アクセス ポイントのネットワーク ユーザ名とパスワードを提供すると、ユーザのクレデンシャルを使用して、ルート AP によってネットワークで認証されるようにできます。

リピータを EAP-FAST またはその他の 802.1x/EAP 認証メソッド クライアントとして設定するには、3 つの主要な手順が必要です。

1. 認証サーバでリピータの認証ユーザ名とパスワードを作成します。
2. リピータがアソシエートするルート アクセス ポイントでサポートされるように認証メソッドを設定します。リピータがアソシエートするアクセス ポイントは、親アクセス ポイントと呼ばれます。認証の設定方法については、第 11 章「認証タイプの設定」を参照してください。

（注） リピータ アクセス ポイントでは、親アクセス ポイントで有効にしたものと同じ暗号スイートまたは WEP 暗号化方式と WEP 機能を有効にする必要があります。

3. 選択したメソッドでリピータが 802.1x/EAP クライアントとして機能するように設定します。次に、EAP-FAST コンフィギュレーションの例を示します。

	コマンド	目的
ステップ 1	**eap profile** *profile-name*	使用する認証方式を指定するためにリピータが使用するプロファイルの名前を入力します。
ステップ 2	**method fast**	使用するメソッドとして EAP-FAST を設定します。
ステップ 3	**dot1x credentials** *name*	ワイヤレス インフラストラクチャでの認証にリピータが使用するユーザ クレデンシャルを設定します。
ステップ 4	**username** *user-name*	dot1x クレデンシャル内のユーザ名を設定します。
ステップ 5	**password 0** *password*	リピータがインフラストラクチャで認証されるときに使用するパスワードを設定します。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**dot11 ssid** *ssid-name*	新しい SSID を作成します。
ステップ 8	**authentication open eap eap_methods**	Open+ EAP 認証を許可します（EAP-FAST またはその他）。
ステップ 9	**authentication network-eap eap_methods**	LEAP 認証を許可します。この例では、LEAP は最善の選択肢ではありませんが、LEAP はデフォルトのメソッドです。802.1x/EAP プロセスをトリガーするには、LEP をイネーブルにする必要があります。EAP プロファイルは、どの方式が実際に使用されるかを決定します。
ステップ 10	**authentication key-management wpa version 2**	キー管理を WPA バージョン 2 に設定します。
ステップ 11	**dot1x credentials** *name*	リピータがワイヤレス インフラストラクチャで認証されるときに作成される dot1x クレデンシャルを使用します。dot1x クレデンシャル プロファイルで定義されたクレデンシャルが使用されます。
ステップ 12	**dot1x eap profile EAP-only**	リピータがワイヤレス インフラストラクチャで認証されるときに上記で作成された EAP 専用プロファイルを使用します。eap プロファイルで定義されたメソッド（この例では EAP-FAST）が使用されます。
ステップ 13	**infrastructure ssid** [**optional**]	（任意）SSID を、他のアクセス ポイントおよびワークグループ ブリッジがこのアクセス ポイントにアソシエートするために使用する SSID として指定します。SSID をインフラストラクチャ SSID として指定しない場合、インフラストラクチャ デバイスはどの SSID を使用してもアクセス ポイントにアソシエートできます。SSID をインフラストラクチャ SSID として指定する場合、**optional** キーワードも入力する場合を除き、インフラストラクチャ デバイスはその SSID を使用してアクセス ポイントにアソシエートする必要があります。
ステップ 14	**interface dot11radio** { **0** | **1** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 15	**ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できますが、空白を使用できません。SSID では、大文字と小文字が区別されます。
ステップ 16	**end**	特権 EXEC モードに戻ります。
ステップ 17	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

ホット スタンバイの概要

ホットスタンバイ モードでは、アクセス ポイントが他のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、モニタするアクセス ポイントの近くに配置され、そのアクセス ポイントとまったく同じように設定する必要があります。スタンバイ アクセス ポイントは、モニタするアクセス ポイントにクライアントとしてアソシエートし、イーサネット ポートと無線ポートの両方からそのアクセス ポイントに対して IAPP クエリを送信します。モニタするアクセス ポイントから応答がない場合、スタンバイ アクセス ポイントはオンラインに切り替わり、そのアクセス ポイントの役割をネットワーク上で引き継ぎます。

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。モニタするアクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがネットワークでその役割を引き継ぐ場合、設定のマッチングによりクライアント デバイスは簡単にスタンバイ アクセス ポイントに切り替わります。

スタンバイ アクセス ポイントは、インターフェイスとインターフェイスの関係ではなく、デバイスとデバイスの関係として、別のアクセス ポイントをモニタします。たとえば、スタンバイ アクセス ポイントの 5 GHz 無線はアクセス ポイント alpha 内の 5 GHz 無線をモニタするように設定し、スタンバイの 2.4 GHz 無線はアクセス ポイント bravo 内の 2.4 GHz 無線をモニタするように設定するということはできません。また、デュアル無線のアクセス ポイント内の 1 つの無線をスタンバイ無線として設定し、もう 1 つの無線をクライアント デバイスに対応するように設定することもできません。

ホット スタンバイ モードはデフォルトでは、無効に設定されています。

(注) モニタするアクセス ポイントに障害が発生し、スタンバイ アクセス ポイントがその役割を引き継いだ場合は、モニタするアクセス ポイントを修復または交換する際に、スタンバイ アクセス ポイントのホットスタンバイを再度設定してください。スタンバイ アクセス ポイントは、自動的にはスタンバイ モードに戻りません。

(注) モニタするユニット上の BSSID が追加または削除されると、モニタするアクセス ポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセス ポイント上で BSSID を追加または削除するときに、スタンバイ ユニットの状態を確認します。必要に応じて、スタンバイ ユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

(注) ホット スタンバイは、AP モードに設定されている BR1410 ではサポートされていません。

ホット スタンバイ アクセス ポイントの設定

スタンバイ アクセス ポイントを設定する場合、スタンバイ ユニットがモニタするアクセス ポイントの無線 MAC アドレスを入力する必要があります。2 つの無線でアクセス ポイントをモニタするには、両方の無線の MAC アドレスが必要です。スタンバイ アクセス ポイントを設定する前に、モニタするアクセス ポイントの MAC アドレスを記録してください。

スタンバイ アクセス ポイントでは、モニタするアクセス ポイントのいくつかの主要な設定を複製する必要があります。複製するのは次の設定です。

- プライマリ SSID（およびモニタするアクセス ポイントに設定された追加 SSID）
- デフォルト IP サブネット マスク
- デフォルト ゲートウェイ
- データ レート
- セキュリティ設定
- 認証タイプと認証サーバ
- 無線の設定と状態

スタンバイ アクセス ポイントを設定する前に、モニタするアクセス ポイントを確認し、設定を記録してください。

（注） スタンバイ アクセス ポイントにアソシエートされている無線クライアント デバイスは、ホット スタンバイを設定している間、接続が切断されます。

ヒント スタンバイ アクセス ポイント上でモニタするアクセス ポイントの設定をすばやく複製するには、モニタするアクセス ポイントの設定を保存して、それをスタンバイ アクセス ポイント上にロードします。コンフィギュレーション ファイルのアップロードとダウンロードの方法については、第 20 章「コンフィギュレーション ファイルの操作」を参照してください。

特権 EXEC モードから、次の手順に従ってアクセス ポイントでホット スタンバイ モードを有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**iapp standby** *mac-address*	アクセス ポイントをスタンバイ モードに移行し、モニタするアクセス ポイントの無線の MAC アドレスを指定します。 **（注）** 2 つの無線を装備したアクセス ポイントで 2 つの無線を装備したアクセス ポイントをモニタするように設定する場合、モニタする 2.4 GHz 無線と 5 GHz 無線の両方の MAC アドレスを入力する必要があります。2.4 GHz 無線 MAC アドレスを最初に入力し、次に 5 GHz MAC アドレスが続きます。 **（注）** モニタするユニット上の BSSID が追加または削除されると、モニタするアクセス ポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセス ポイント上で BSSID を追加または削除するときに、スタンバイ ユニットの状態を確認します。必要に応じて、スタンバイ ユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。 **（注）** ホット スタンバイは、AP モードに設定されている BR1410 ではサポートされていません。
ステップ 3	**iapp standby poll-frequency** *seconds*	スタンバイ アクセス ポイントが、モニタするアクセス ポイントの無線ポートとイーサネット ポートに送信するクエリの間隔を秒数で設定します。デフォルトのポーリング周期は 2 秒です。
ステップ 4	**iapp standby timeout** *seconds*	スタンバイ アクセス ポイントが、モニタするアクセス ポイントからの応答を待ち、動作不良だと判断するまでの時間を秒数で設定します。デフォルトのタイムアウト値は 20 秒です。 **（注）** スタンバイ アクセス ポイントとモニタするアクセス ポイントの間のブリッジ パスが 20 秒よりも長い間失われる可能性がある場合（スパニングツリーの再計算中など）、スタンバイ タイムアウトの設定を延長する必要があります。 **（注）** モニタするアクセス ポイントが、最も混雑の少ないチャネルを選択するように設定されている場合、スタンバイ タイムアウトの設定の延長が必要になる場合があります。モニタするユニットが最も混雑の少ないチャネルを選択するまで、最大で 40 秒かかる場合があります。

	コマンド	目的
ステップ 5	**iapp standby primary-shutdown**	(任意)スタンバイ アクセス ポイントが、モニタするアクセス ポイントに Dumb Device Protocol(DDP)メッセージを送信し、スタンバイ ユニットが有効になったときに、モニタするアクセス ポイントの無線を無効にします。この機能によって、モニタするアクセス ポイントにアソシエートされているクライアント デバイスが、障害の発生したユニットにアソシエートしたままになることが回避できます。
ステップ 6	**show iapp standby-parms**	入力内容を確認します。アクセス ポイントがスタンバイ モードの場合、このコマンドにより、モニタするアクセス ポイントの MAC アドレス、ポーリング周期、タイムアウトの値などのスタンバイ パラメータが表示されます。アクセス ポイントがスタンバイ モード以外の場合、*no iapp standby mac-address* が表示されます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

スタンバイ モードを有効にした後、モニタするアクセス ポイントから記録した設定をスタンバイ アクセス ポイントの設定と一致するように変更します。

スタンバイ操作の確認

スタンバイ アクセス ポイントの状態を確認する場合は、次のコマンドを使用します。

show iapp standby-status

このコマンドは、スタンバイ アクセス ポイントのステータスを表示します。表 19-2 は、表示されるスタンバイ ステータス メッセージを示しています。

表 19-2　　スタンバイ ステータス メッセージ

メッセージ	説明
IAPP Standby is Disabled	アクセス ポイントがスタンバイ モードに設定されていません。
IAPP—AP is in standby mode	アクセス ポイントがスタンバイ モードになっています。
IAPP—AP is operating in active mode	スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継いでおり、ルート アクセス ポイントとして機能しています。
IAPP—AP is operating in repeater mode	スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継いでおり、リピータ アクセス ポイントとして機能しています。
Standby status: Initializing	スタンバイ アクセス ポイントが、モニタするアクセス ポイントとのリンク テストを初期化しています。
Standby status: Takeover	スタンバイ アクセス ポイントがアクティブ モードに移行しています。
Standby status: Stopped	スタンバイ モードがコンフィギュレーション コマンドによって停止されました。

表 19-2　スタンバイ ステータス メッセージ（続き）

メッセージ	説明
Standby status: Ethernet Linktest Failed	スタンバイ アクセス ポイントからモニタするアクセス ポイントへのイーサネット リンク テストが失敗しました。
Standby status: Radio Linktest Failed	スタンバイ アクセス ポイントからモニタするアクセス ポイントへの無線リンク テストが失敗しました。
Standby status: Standby Error	未定義のエラーが発生しました。
Standby State: Init	スタンバイ アクセス ポイントが、モニタするアクセス ポイントとのリンク テストを初期化しています。
Standby State: Running	スタンバイ アクセス ポイントがスタンバイ モードで動作しており、モニタするアクセス ポイントへのリンク テストを実行しています。
Standby State: Stopped	スタンバイ モードがコンフィギュレーション コマンドによって停止されました。
Standby State: Not Running	アクセス ポイントはスタンバイ モードではありません。

スタンバイ設定を確認する場合は、次のコマンドを使用します。

show iapp standby-parms

このコマンドは、スタンバイ アクセス ポイントの MAC アドレス、スタンバイ タイムアウト、ポーリング周期の値を表示します。スタンバイ アクセス ポイントが設定されていない場合、次のメッセージが表示されます。

```
no iapp standby mac-address
```

スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継ぐ場合、スタンバイ アクセス ポイントが引き継いだ原因を特定するために **show iapp statistics** コマンドを使用できます。

ワークグループ ブリッジ モードの概要

アクセス ポイントをワークグループ ブリッジ（WGB）として設定できます。ワークグループ ブリッジ（WGB）モードのアクセス ポイントは、別のアクセス ポイントにクライアントとしてアソシエートして、イーサネット ポートに接続されたデバイスをネットワークに接続します。たとえば、ネットワーク プリンタのグループを無線で接続する必要がある場合は、プリンタをハブまたはスイッチに接続し、ハブまたはスイッチをアクセス ポイントのイーサネット ポートに接続し、そのアクセス ポイントをワークグループ ブリッジとして設定します。ワークグループ ブリッジはネットワーク上のアクセス ポイントにアソシエートします。

アクセス ポイントに 2 つの無線がある場合、ワークグループ ブリッジ モードで、2.4 GHz 無線または 5 GHz 無線のいずれかが機能します。一方の無線インターフェイスをワークグループ ブリッジとして設定すると、他方の無線はアップ状態のままになります。ただし、両方の無線が同時にワークグループ ブリッジとして機能するようには設定できません。他方の無線はディセーブル（シャットダウン）にするか、ルート（アクセス ポイントまたはブリッジ）、スキャナ、またはスペクトル モードにできます。

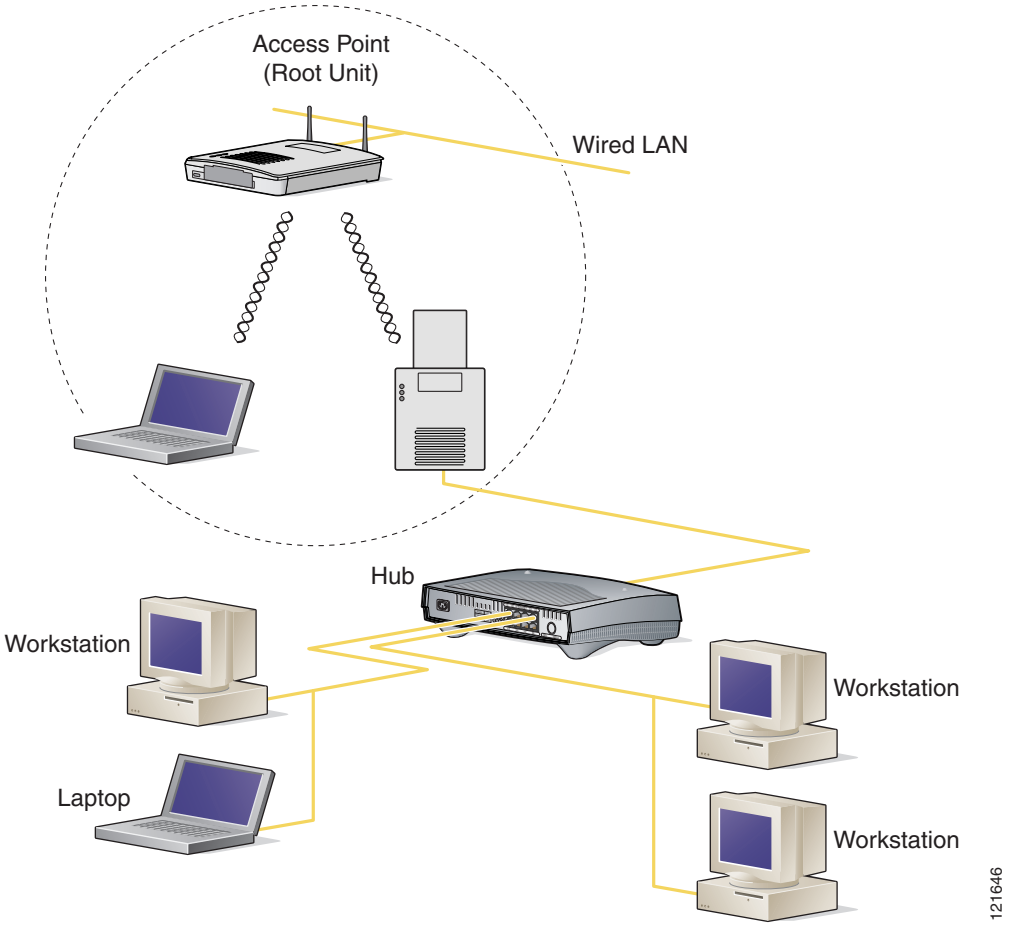
注意　ワークグループ ブリッジ モードのアクセス ポイントでイーサネットポートを有線 LAN に接続すると、ブリッジ ループが発生することがあります。ネットワークのブリッジ ループを防止するには、ワークグループ ブリッジとして設定する前または設定後すぐにワークグループ ブリッジを有線 LAN から切断します。

（注）　ワークグループ ブリッジの親として指定されているルート アクセス ポイント上で複数の BSSID が設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のワークグループ ブリッジが特定の親にアソシエートするように設定されている場合、親アクセス ポイント上で BSSID を追加または削除するときは、ワークグループ ブリッジのアソシエーションの状態を確認します。必要に応じて、ワークグループ ブリッジを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

（注）　ワークグループ ブリッジ モードでのアクセス ポイントは、ブリッジとして機能はしますが、無線範囲が限定されています。ワークグループ ブリッジは、数キロにわたって通信するようにワイヤレス ブリッジを設定できる、**distance** 設定をサポートしていません。

図 19-2 は、ワークグループ ブリッジ モードのアクセス ポイントを示しています。

図 19-2　ワークグループ ブリッジ モードのアクセス ポイント



インフラストラクチャ デバイスまたはクライアント デバイスとしてのワークグループ ブリッジの扱い

ワークグループ ブリッジがアソシエートするアクセス ポイントは、そのワークグループ ブリッジをインフラストラクチャ デバイスまたは単にクライアント デバイスとして扱うことができます。デフォルトでは、アクセス ポイントやブリッジはワークグループ ブリッジをクライアント デバイスとして扱います。

信頼性を向上させるために、ワークグループ ブリッジをクライアント デバイスとしてではなく、アクセス ポイントやブリッジと同じインフラストラクチャ デバイスとして扱うように、アクセス ポイントとブリッジを設定できます。ワークグループ ブリッジがインフラストラクチャ デバイスとして扱われる場合、アクセス ポイントはアドレス解決プロトコル（ARP）パケットなどのマルチキャスト パケットを、確実にワークグループ ブリッジに配信します。ワークグループ ブリッジをインフラストラクチャ デバイスとして扱うようにアクセス ポイントとブリッジを設定するには、設定インターフェイス コマンド **infrastructure-client** を使用します。

ワークグループ ブリッジをクライアント デバイスとして扱うようにアクセス ポイントとブリッジを設定すると、より多くのワークグループ ブリッジが同じアクセス ポイントにアソシエートできます。つまり、より多くのワークグループ ブリッジが、インフラストラクチャ SSID ではない SSID を使用してアソシエートできます。信頼性の高いマルチキャスト配信のパフォーマンス コストのため（マルチキャスト パケットが各ワークグループ ブリッジに二重に送信されるので）、アクセス ポイントまたはブリッジにアソシエートできるワークグループ ブリッジなどのインフラストラクチャ デバイスの数は制限されます。アクセス ポイントにアソシエートできるワークグループ ブリッジの数を 21 以上にするには、アクセス ポイントがマルチキャスト パケットをワークグループ ブリッジに配信するときの信頼性を低くする必要があります。信頼性が低くなると、アクセス ポイントはマルチキャスト パケットが目的のワークグループ ブリッジに到達したかどうか確認できず、アクセス ポイントのカバレッジ領域の端にあるワークグループ ブリッジの有線クライアントは、すべてのマルチキャスト フレームを受信しない可能性があります。ワークグループ ブリッジをクライアント デバイスとして扱うと、パフォーマンスは向上しますが、信頼性は低くなります。ワークグループ ブリッジを単なるクライアント デバイスとして扱うようにアクセス ポイントとブリッジを設定するには、設定インターフェイス コマンド **no infrastructure client** を使用します。これがデフォルト設定です。

ワークグループ ブリッジに接続されたデバイスが、アクセス ポイントまたはブリッジと同等のネットワークに対する信頼性を必要とする場合には、ワークグループ ブリッジをインフラストラクチャデバイスとして使用する必要があります。次の条件を満たす場合には、ワークグループ ブリッジをクライアント デバイスとして使用します。

- 同じアクセス ポイントまたはブリッジに 20 台を超えるワークグループ ブリッジがアソシエートする。
- ワークグループ ブリッジがインフラストラクチャ SSID ではない SSID を使用してアソシエートする。
- ワークグループ ブリッジがモバイルである。

ワークグループ ブリッジがアソシエートされているアクセス ポイントに **(no) infrastructure client** コマンドが入力されることに注意してください。このコマンドは、アクセス ポイントが各マルチキャスト フレームのユニキャスト コピーを追加するために、セル内の各ワークグループ ブリッジへ信頼性のある方式（確認応答のあるユニキャスト）で送信するかどうかを判断します。

インフラストラクチャ クライアントがアクセス ポイントで設定されている場合、各ワークグループ ブリッジはマルチキャスト初期フレームとユニキャスト コピーの両方を受信する可能性があります。両方のフレーム（同じ上位層内容がある）を処理すると、ワークグループ ブリッジでの処理が非効率になります。マルチキャスト フレームを考慮してユニキャスト コピーを破棄するか（デフォルト）、ユニキャスト フレームを考慮してマルチキャスト ソースのフレームを廃棄するようにワークグループ ブリッジを設定できます。ワークグループ ブリッジ無線でこの動作を設定するには、コマンド **station-role workgroup-bridge multicast mode {client | infrastructure}** を使用します。クライアント オプションでは、マルチキャスト フレームを考慮して、ユニキャスト コピーを破棄します。インフラストラクチャ オプションでは、メイン アクセス ポイントのインフラストラクチャ クライアント設定を反映し、マルチキャスト フレームのユニキャスト コピーを考慮してマルチキャスト フレームを処理しないようにワークグループ ブリッジを設定します。

ローミング用ワークグループ ブリッジの設定

デフォルトでは、ワークグループ ブリッジは静的です。そのため、アクセス ポイント SSID にアソシエートされると、他のアクセス ポイントをスキャンしません。

ワークグループ ブリッジがモバイルの場合、親アクセス ポイントやブリッジへのより良好な無線接続をスキャンするように設定できます。ワークグループ ブリッジをモバイル ステーションとして設定するには、次のコマンドを使用します。

ap(config)# **mobile station**

この設定を有効にすると、Received Signal Strength Indicator（RSSI; 受信信号強度表示）の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループ ブリッジは新しい親アソシエーションをスキャンします。これらの基準を使用して、モバイル ステーションとして設定されたワークグループ ブリッジは新しい親アソシエーションを検索し、現在のアソシエーションが失われる前に新しい親にローミングします。モバイル ステーションの設定が無効の場合（デフォルトの設定）、ワークグループ ブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。

ap(config-if)#**mobile station minimum-rate <data rate>**

これは、WGB が新しいローミング イベントをいつ開始するかを制御するための設定可能なパラメータです。この CLI が設定され、現在のデータ レートが設定値より小さい場合、新しいローミング プロセスが開始されます。これにより不要なローミングが減り、所要のレート値が得られます。

また、スキャンの周期を設定することもできます。接続状態が低下した場合、ワークグループ ブリッジは、接続するより良いアクセス ポイントをスキャンします。ワークグループ ブリッジがスキャンによってより良い接続ポイントを見つけられない場合、**mobile station period** *number-of-seconds* コマンドを使って次のスキャン サイクルまでの周期を特定します。

限定チャネル スキャン用のワークグループ ブリッジの設定

鉄道などのモバイル環境では、ワークグループ ブリッジはすべてのチャネルをスキャンする代わりに、限定チャネルのセットのみのスキャンに制限されます。こうすることで、ワークグループ ブリッジのローミングが 1 つのアクセス ポイントから別のアクセス ポイントに切り替わるとき、ハンドオフによる遅延が減少します。ワークグループ ブリッジがスキャンするチャネル数を必要な数に限定することによって、モバイル ワークグループ ブリッジで高速かつスムーズなローミングが可能な継続的な無線 LAN 接続が実現されて維持されます。

限定チャネル セットの設定

この限定チャネル セットは、**mobile station scan <set of channels>** CLI コマンドを使用して設定し、すべてのチャネルまたは指定されたチャネルのスキャンを開始します。設定できるチャネルの最大数に制限はありません。設定できるチャネルの最大数は、無線がサポートできるチャネル数だけに制限されます。スキャンを実行すると、ワークグループ ブリッジは、この限定チャネル セットだけをスキャンします。この限定チャネル機能は、ワークグループ ブリッジが現在アソシエートされているアクセス ポイントから受け取る既知のチャネル リストにも影響します。チャネルが既知のチャネル リストに追加されるのは、チャネルが限定チャネル セットに含まれる場合に限られます。

次の例は、コマンドを使用する方法を示しています。この例では、チャネル 1、6、および 11 がスキャンに指定されています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

no mobile station scan コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

CCX ネイバー リストの無視

さらにワークグループ ブリッジは、AP Adjacent レポートや Enhanced Neighbor List レポートなどの CCX レポートを使用して、既知のチャネル リストを更新します。ただし、ワークグループ ブリッジが限定チャネル スキャンに設定されている場合、CCX レポートを処理して既知のチャネル リストを更新する必要がありません。**mobile station ignore neighbor-list** コマンドを使用して、CCX 近接リスト レポートの処理を無効にします。このコマンドは、ワークグループ ブリッジが限定チャネル スキャンに設定されている場合だけ有効です。次の例は、このコマンドを使用する方法を示しています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

クライアント VLAN の設定

ワークグループ ブリッジのイーサネット ポートに接続されたデバイスをすべて特定の VLAN に割り当てる必要がある場合、接続されたデバイスに対して VLAN を設定できます。ワークグループ ブリッジで、次のコマンドを入力します。

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

ワークグループ ブリッジのイーサネット ポートに接続されたデバイスが、すべてこの VLAN に割り当てられます。

ワークグループ ブリッジの VLAN タギング

ワークグループ ブリッジ（WGB）の VLAN タギング機能を使用すると、Unified WGB ソリューションに対する VLAN 数に基づいた VLAN トラフィックの分離がイネーブルになります。

この機能がイネーブルの場合、VLAN クライアントから無線 LAN コントローラ（WLC）へのパケットの送信中に、WGB が 802.1q ヘッダーを削除します。WGB は、802.1q ヘッダーなしで VLAN クライアントに向かうパケットを取得します。WGB の背後にあるスイッチにフレームを転送する場合は、802.1q ヘッダーを追加するように、WGB コードを変更する必要があります。

WGB は、Internet Access Point Protocol（IAPP）アソシエーション メッセージの有線クライアント VLAN 情報で WLC を更新します。WLC は WGB クライアントを VLAN クライアントとして扱い、送信元 MAC アドレスに基づき正しい VLAN インターフェイスにパケットを転送します。

アップストリーム方向では、WGB はパケットから 802.1q ヘッダーを削除すると同時にパケットを WLC に送信します。ダウンストリーム方向では、WLC は有線クライアントを接続するスイッチにパケットを転送しながら、802.1q タグなしで、そのパケットを WGB に送信します。WGB は、宛先 MAC アドレスに基づき、4 バイトの 802.1q ヘッダーを追加します。（VLAN の詳細については、第 14 章「VLAN の設定」を参照してください）。

次のコマンドを入力して、WGB の VLAN タギングを有効にします。

```
WGB(config)#workgroup-bridge unified-vlan-client ?
       -replicate  Enable WGB broadcast to all vlans
       <cr>
```

ワークグループ ブリッジ モードの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントをワークグループ ブリッジとして設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** | **1**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**station-role workgroup-bridge** [**universal** *mac-address*]	ワークグループ ブリッジに無線の役割を設定します。 (任意) ワークグループ ブリッジとして設定された場合、アクセス ポイントは特定のメッセージをプライマリ アクセス ポイントに送信し、ワークグループ ブリッジ無線経由でリレーされた有線クライアントの MAC アドレスについて通知します。プライマリ アクセス ポイントがシスコのアクセス ポイントでない場合、これらのメッセージは認識されません。 ワークグループ ブリッジがシスコ以外のアクセス ポイントと正常にアソシエートおよび通信できるようにするには、**universal** オプション引数を使用します。このモードでは、1 つの有線クライアントだけがサポートされるという制限があります。 このモードを設定する場合、ワークグループ ブリッジ経由でトラフィックがリレーされる有線クライアントの MAC アドレスを設定する必要があります。プライマリ AP に有線クライアント リストを送信する代わりに、ワークグループ ブリッジは有線クライアントの MAC アドレスを使用してアクセス ポイントに直接アソシエートします。有線クライアントの MAC アドレスがワークグループ ブリッジの MAC アドレス テーブルにない場合、ワークグループ ブリッジは独自の MAC アドレスを使用してアソシエートします。その後、有線クライアントが接続され、MAC アドレスがワークグループ ブリッジ MAC アドレス テーブルに表示されると、WGB は有線クライアントの MAC アドレスを使用してアソシエーションを解除し、再アソシエートします。このプロセスは、無線クライアントと MAC アドレスとの間で固有のマッピングが必要なシスコ以外のアクセス ポイントをサポートします。

	コマンド	目的
ステップ 4	**station-role workgroup-bridge multicast mode {client | infrastructure}**	(任意)プライマリ アクセス ポイントが **infrastructure client** コマンドで設定された場合、マルチキャスト フレームもユニキャスト経由でワークグループ ブリッジに送信されます。このような場合、ユニキャスト経由でリレーされるマルチキャスト フレームには、ヘッダーに次の 4 つの MAC アドレスがあります。ワークグループ ブリッジ ユニキャスト宛先 MAC アドレス、送信アクセス ポイント MAC アドレス、マルチキャスト宛先 MAC アドレス、元の送信者の送信元 MAC アドレス。 元のマルチキャスト フレーム ヘッダーには、マルチキャスト宛先 MAC アドレス、送信アクセス ポイント MAC アドレス、元の送信者の送信元 MAC アドレスの 3 つの MAC アドレスだけが含まれます。 プライマリ アクセス ポイントで **infrastructure client** コマンドを使う場合、ステーション ロール ワークグループ ブリッジ マルチキャスト モード インフラストラクチャを使って、マルチキャスト フレームを無視し、マルチキャスト フレームのリレーされたユニキャスト コピーだけを処理するようワークグループ ブリッジに指示します。ステーション ロール ワークグループ ブリッジ マルチキャスト モード クライアントを使って、標準フレームのみを考慮し、ヘッダーに 4 つの MAC アドレスが表示されるリレーされたフレームは無視するようワークグループ ブリッジに指示します。 • クライアント クライアント モードは、3 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます • インフラストラクチャ インフラストラクチャ モードは、4 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます
ステップ 5	**ssid** *ssid-string*	親アクセス ポイントまたはブリッジにアソシエートするためにワークグループ ブリッジが使用する SSID を指定します。
ステップ 6	**infrastructure-ssid**	SSID をインフラストラクチャ SSID に指定します。 **(注)**　ワークグループ ブリッジは、ルート アクセス ポイントまたはブリッジにアソシエートするために、インフラストラクチャ SSID を使用する必要があります。
ステップ 7	**authentication client username** *username* **password** *password*	(任意)親アクセス ポイントが LEAP 認証を必要とするように設定されている場合、ワークグループ ブリッジが LEAP 認証を実行するときに使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバでワークグループ ブリッジに設定したユーザ名とパスワードに一致する必要があります。
ステップ 8	**exit**	SSID コンフィギュレーション モードを終了し、無線インターフェイス コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 9	**parent** {*1-4*} *mac-address* [*timeout*]	(任意)ワークグループ ブリッジがアソシエートするアクセス ポイントの MAC アドレスを入力します。 • 最大 4 つの親アクセス ポイントの MAC アドレスを入力できます。このポイントには、1 ～ 4 の番号が指定されます。ワークグループ ブリッジは、必ずその親アクセス ポイントのリストからベストなアクセス ポイントにアソシエートしようとします。ワークグループ ブリッジは、「タイムアウト」オプションを設定しない限り、親リストにない MAC アドレスにはアソシエートしません。 **(注)** 複数の BSSID が親アクセス ポイント上で設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。 • (任意)タイムアウト値は秒単位で入力できますが、これはどれだけの時間、ワークグループ ブリッジがその親リストにあるアクセス ポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、ワークグループ ブリッジは親リストにないアクセス ポイントにアソシエートしようとします。 0 ～ 65535 秒の範囲のタイムアウト値を入力できます。
ステップ 10	**mobile station**	(任意)ワークグループ ブリッジをモバイル ステーションとして設定します。 この設定を有効にすると、Received Signal Strength Indicator(RSSI; 受信信号強度表示)の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループ ブリッジは新しい親アソシエーションをスキャンします。この設定が無効の場合(デフォルトの設定)、ワークグループ ブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。
ステップ 11	**mobile station period** *number-of-seconds*	(任意)ワークグループ ブリッジがアソシエートされているアクセス ポイントへの信号が低下した場合、ワークグループ ブリッジは代替アクセス ポイントをスキャンします。このスキャンに失敗した場合(より良い信号のアクセス ポイントが見つからなかった場合)、ここで入力した秒数は次のスキャンの試行までの間隔となります。
ステップ 12	**mobile station minimum-rate** *rate*	(任意)ワークグループ ブリッジが代替アクセス ポイントをスキャンする場合、このコマンドは、ワークグループ ブリッジが代替アクセス ポイントを接続ポイントの候補として考慮するために、新しいアクセス ポイントで達成する必要がある最小データ レートを指定します。
ステップ 13	**mobile station scan**	(任意)ワークグループ ブリッジが代替アクセス ポイントを探すためにスキャンするチャネル リストを制限します。

	コマンド	目的
ステップ 14	**mobile station ignore neighbor-list**	(任意)スキャンされたチャネルのリストを制限するようワークグループ ブリッジが設定されている場合、このコマンドは、候補となるネイバー アクセス ポイントおよびチャネルを示す CCX ネイバー リストのメッセージを無視するようワークグループ ブリッジに指示します。
ステップ 15	**exit**	無線コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 16	**workgroup-bridge client-vlan** *vlan-id*	(任意)ワークグループ ブリッジのイーサネット ポートに接続されたデバイスを割り当てる VLAN を指定します。
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

次の例は、アクセス ポイントをワークグループ ブリッジとして設定する方法を示しています。この例では、ワークグループ ブリッジは設定されたユーザ名とパスワードを使用して LEAP 認証を実行し、イーサネット ポートに接続されたデバイスが VLAN 22 に割り当てられます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# authentication client username wgb1 password cisco123
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# workgroup-bridge client-vlan 22
AP(config)# end
```

次の例は、1 および 2 の番号が指定された親アクセス ポイントを持つワークグループ ブリッジの設定方法を示しています。

```
AP(config-if)# parent 1 0040.9631.81cf
AP(config-if)# parent 2 0040.9631.81da
```

次の例は、1 つの親を親リストから除く方法を示しています。この例では、親 2 を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに 60 秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

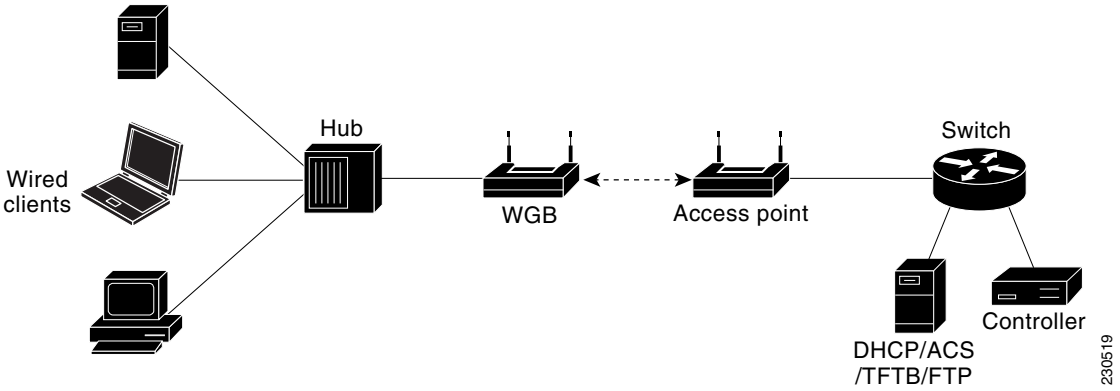
次に、親リストでタイムアウト値をディセーブルにする方法の例を示します。

```
AP(config-if)# no parent timeout
```

Lightweight 環境でのワークグループ ブリッジの使用

アクセス ポイントをワークグループ ブリッジとして動作するように設定することで、アクセス ポイントはワークグループ ブリッジ アクセス ポイントにイーサネットで接続されているクライアントの代理として Lightweight アクセス ポイントへの無線接続を提供できます。ワークグループ ブリッジは、イーサネット インターフェイス側にある有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol（IAPP; インターネット アクセス ポイント プロトコル）メッセージングを使用して、MAC アドレスを Lightweight アクセス ポイントに報告します。この方法によって、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。ワークグループ ブリッジは、Lightweight アクセス ポイントへの単一の接続を確立することで、有線クライアントへの無線アクセス接続を提供します。Lightweight アクセス ポイントはワークグループ ブリッジを無線クライアントとして扱います。

図 19-3　　Lightweight 環境でのワークグループ ブリッジ



（注） Lightweight アクセス ポイントに障害が発生した場合、ワークグループ ブリッジは別のアクセス ポイントへのアソシエートを試行します。

ワークグループ ブリッジを Lightweight 環境で使用する際のガイドライン

ワークグループ ブリッジを Lightweight ネットワークで使用する場合は、次のガイドラインに従います。

- ワークグループ ブリッジは、ワークグループ ブリッジ モードをサポートし、Cisco IOS Release JA 以降（32MB アクセス ポイント）または Cisco IOS Release 12.3(8)JEB 以降（16MB アクセス ポイント）を実行する任意の自律アクセス ポイントを使用できます。これらのアクセス ポイントには、AP1040、AP1140、および AP1260 が含まれます。12.4(3g)JA および 12.3(8)JEB よりも前の Cisco IOS リリースはサポートされません。

（注） アクセス ポイントに 2 つの無線がある場合、1 つだけをワークグループ ブリッジ モードに設定できます。この無線は Lightweight アクセス ポイントへの接続に使用されます。2 番目の無線を無効にすることをお勧めします。

ワークグループ ブリッジでワークグループ 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。

- ワークグループ ブリッジ アクセス ポイント GUI にある [Network] > [Network Interfaces] > [Radio0-802.11N 2.4 GHz / Radio1-802.11N 5 GHz] > [Settings] ページで、無線ネットワークのロールとして [Workgroup Bridge] を選択します。
  または、WGB アクセス ポイント CLI 無線コンフィギュレーション サブモードで、次のコマンドを入力します：**station-role workgroup-bridge**
- ワークグループ ブリッジはクライアント モード（デフォルト値）だけがサポートされます。Lightweight アクセス ポイントは、アソシエートされたワークグループ ブリッジにユニキャスト方式でマルチキャスト フレームをリレーしません。ワークグループ ブリッジのクライアント モードを有効にするには、次のいずれかを実行します。
  - 無線コンフィギュレーション ページで、ワークグループ ブリッジへの信頼性のあるマルチキャスト パラメータで [Disabled] を選択します。
  - 無線コンフィギュレーション サブモードから、次のコマンドを入力します：**no infrastructure client**.
- ワークグループ ブリッジでは次の Lightweight 機能の使用がサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
- ワークグループ ブリッジでは次の Lightweight 機能の使用はサポートされません。
  - Cisco Centralized Key Management（CCKM）
  - ハイブリッド REAP
  - アイドル タイムアウト
  - Web 認証

（注） ワークグループ ブリッジが Web 認証 WLAN にアソシエートする場合、ワークグループ ブリッジは除外リストに追加され、ワークグループ ブリッジの有線クライアントのすべてが削除されます。

- メッシュ ネットワークでは、ワークグループ ブリッジはその役割がルート アクセス ポイントかメッシュ アクセス ポイントかに関係なく、すべてのメッシュ アクセス ポイントにアソシエートできます。
- ワークグループ ブリッジに接続する有線クライアントは、セキュリティが認証されません。その代わり、ワークグループ ブリッジがアソシエートするアクセス ポイントに対してワークグループ ブリッジが認証されます。したがって、ワークグループ ブリッジの有線側は物理的に保護することを推奨します。
- レイヤ 3 ローミングで、ワークグループ ブリッジのローミングが別のコントローラ（外部コントローラなど）に切り替わった後にワークグループ ブリッジ ネットワークに有線クライアントを接続する場合、有線クライアントの IP アドレスはアンカー コントローラだけに表示され、外部コントローラには表示されません。
- ワークグループ ブリッジの記録をコントローラから削除すると、ワークグループ ブリッジの有線クライアントの記録もすべて削除されます。
- ワークグループ ブリッジに接続されている有線クライアントは、ワークグループ ブリッジの QoS および AAA オーバーライド属性を継承します。
- ワークグループ ブリッジに接続されている有線クライアントでは、次の機能がサポートされません。

- MAC フィルタリング
- リンク テスト
- アイドル タイムアウト

- コントローラに何も設定しなくても、ワークグループ ブリッジと Lightweight アクセス ポイントとの通信を有効にできます。ただし、適切な通信を確保するには、ワークグループ ブリッジに設定された SSID およびセキュリティ方式と一致する WLAN をコントローラに作成する必要があります。

サンプル ワークグループ ブリッジ アソシエーションの確認

ワークグループ ブリッジがアクセス ポイントにアソシエートしていることを確認するには、ワークグループ ブリッジで次のコマンドを入力します。

show dot11 association

有線クライアントがトラフィックを長期間送信しない場合、トラフィックがその有線クライアントに連続して送信されている場合でも、ワークグループ ブリッジ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 フローに障害が発生します。トラフィックの損失を避けるには、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。これを行うには、ワークグループ ブリッジで次の IOS コマンドを使用して、ワークグループ ブリッジのエージアウト タイマーを大きな値に設定します。

```
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も大きく設定することをお勧めします。

ワークグループ ブリッジでの VideoStream サポートの有効化

VideoStream は、無線経由でユニキャスト フレームにマルチキャスト フレームを変換することによって、IP マルチキャスト ストリームの信頼性を向上させます。Cisco IOS Release 15.2(2)JA 以降では、ワークグループ ブリッジに接続された有線デバイス向けに VideoStream サポートを提供しています。リリース 15.2(2)JA 以降を実行しているアクセス ポイントに関しては、ワークグループ ブリッジが無線 LAN コントローラ(WLC)のマルチキャスト テーブルに追加され、そのワークグループ ブリッジは VideoStream ユニキャスト フレームをイーサネット マルチキャスト フレームに変換して、それを有線クライアントに送信します。

ワークグループ ブリッジの VideoStream を有効にするには、WLC で次のコマンドを入力します。

config media-stream wired-client enable

高速ローミングのためのワークグループ ブリッジの設定

高速鉄道の車両など、ワークグループ ブリッジ AP の高速ローミングが関係するワイヤレス ネットワークの導入について考えてみます。車両が移動すると、車両のワークグループ ブリッジ AP は 1 つの親 AP(ルート AP)から線路に沿ってマウントされている次の 親 AP に移動します。このようなシナリオでは、約 100 km/h で走行する列車が関係する場合もあり、親 AP は線路で 200～300m の間隔で配置されています。

このようなシナリオでは、次のように設定されていることを確認します。

ワイヤレス コントローラでの 802.11v BSS 遷移

高速ローミングが機能するには、ワイヤレス コントローラで、802.11v BSS 遷移をイネーブルにする必要があります。これにより、ワークグループ ブリッジ AP はアソシエートされた AP(現在の親 AP)からネイバー リストを要求して受信できるようになります。ワークグループ ブリッジ AP はこのリストを使って、次の親 APを見つけるためにスキャンする必要がある一部のチャネルを識別します。

WGB での設定

範囲から遠ざかる際に、現在の親 AP が最適でないことを WGB がどれだけ素早く検出するか、また次の親 AP を検出するためにローミングを開始する必要があることを設定するには、次のコマンドを使用します。

drssi roaming threshold *value* **period** *value* **packet** *value*

このコマンドは次のような特徴を持ちます。

- DRSSI ローミングしきい値は RSSI しきい値です。このしきい値を超える RSSI 値を持つ AP はアソシエーション対象として考慮されません。

  DRSSI ローミングしきい値は、線路上の 2 つの AP の中間点における平均 RSSI レベルよりも約 2 ～ 3 dBm 低くすることが推奨されています。設定済みのしきい値 x は -x dBm に対応します。

- period は、現在の親へのリンクの品質を WGB が評価する頻度を制御します。たとえば、列車が高速で移動している場合、WGB がより頻繁にリンクの品質を評価するように設定します。ただし、速度が遅い場合、WGB はリンクの品質評価の頻繁な計算を回避します。

- packet は、AP とのリンク品質を追跡するために WGB が使用する現在のルート AP のサンプル データ パケットのしきい値です。WGB AP は、ルート AP から最後に受信したデータ パケットの RSSI の継続的な平均を保持します。この継続的な平均がしきい値を下回る場合、WGB はローミングを開始します。たとえば、列車が高速で移動している場合、少数のサンプルを使ってスイッチするタイミングを判断できます。

次の例のように、100 km/h までであれば、DRSSI のローミングしきい値 67、period 値 1、packet 値 20 の設定で問題なく機能します。

```
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#int d0
ap(config-if)#drssi roaming threshold 67 period 1 packet 20
ap(config-if)#end
```

また、次のコマンドを使用して、最後にアソシエートされた AP から受信したネイバー リストのみをスキャンするようワークグループ ブリッジを設定することもできます。
drssi scan-only current-neighbor-list

上記のコマンドをディセーブルにして、ワークグループ ブリッジがネイバー リストを徐々にエージ アウトするようにすることもできます。エージ アウト要因はローミングごとに 1 つずつ削減されます。デフォルトのエージは 2 です。ディセーブルにするには、コマンド **no drssi scan-only current-neighbor-list** を使用します。

debug コマンドおよび show コマンド

WGB で、現在のネイバー リストのテーブルを表示するには、次のコマンドを使用します:
show dot11 bss-trans neighbor-list

WGB で、802.11v BSS 遷移のデバッグをイネーブルにするには、次のコマンドを使用します:
debug dot11 dot11v {detail | errors | all}

CHAPTER 20

ファームウェアと設定の管理

この章では、フラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、およびソフトウェア イメージのアーカイブ（アップロードとダウンロード）方法について説明します。

（注） この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Access Points and Bridges*』、およびリリース 12.4 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

フラッシュ ファイル システムの操作

アクセス ポイントにあるフラッシュ ファイル システムには、ソフトウェア イメージやコンフィギュレーション ファイルを管理しやすくするためのコマンドが用意されています。

フラッシュ ファイル システムは、ファイルを保存できる単独のフラッシュ デバイスです。このフラッシュ デバイスは、*flash:* と呼ばれます。

ここでは、次の情報について説明します。

使用可能なファイル システムの表示

アクセス ポイントで使用可能なファイル システムを表示する場合は、次の例に示すように、特権 EXEC コマンド **show file systems** を使用します。

```
ap# show file systems
File Systems:


       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   arch:
*     31739904      16701952     flash     rw   flash:
      11999232       7754752     flash     rw   ram:
             -             -    opaque     rw   bs:
      31739904      16701952   unknown     rw   zflash:
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
         32768         26572     nvram     rw   nvram:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   tftp:
             -             -    opaque     rw   null:
             -             -    opaque     ro   xmodem:
             -             -    opaque     ro   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
```

表 20-1 は、**show file systems** コマンドのフィールドの詳細を示しています。

表 20-1　　show file systems のフィールドの詳細

フィールド	値
Size(b)	ファイル システムのメモリ サイズ（バイト単位）です。
Free(b)	ファイル システムの空きメモリ サイズ（バイト単位）です。
Type	ファイル システムのタイプです。 **flash**：フラッシュ メモリ デバイス用。 **network**：ネットワーク デバイス用。 **nvram**：Nonvolatile RAM（NVRAM; 不揮発性 RAM）デバイス用。 **opaque**：ファイル システムはローカルに生成された *pseudo* ファイル システム（*system* など）、または brimux などのダウンロード インターフェイスです。 **unknown**：ファイル システムのタイプは不明です。
Flags	ファイル システムの権限です。 **ro**：読み取り専用です。 **rw**：読み取りおよび書き込みです。 **wo**：書き込み専用です。

表 20-1　show file systems のフィールドの詳細 （続き）

フィールド	値
Prefixes	ファイル システムのエイリアスです。 **arch:** **ram:** **bs:** **archive:** **tmpsys:** **xmoem:** **ymodem:** **scp:** **tar:** **https:** **flash:** フラッシュ ファイル システムです。 **ftp:** ファイル転送プロトコル ネットワーク サーバ。ネットワーク デバイス間のファイルの転送に使用されます。 **nvram:** Non-volatile RAM Memory（NVRAM; 不揮発性 RAM メモリ）。 **null:** コピーのヌル宛先です。リモート ファイルをヌルにコピーすると、サイズを確認できます。 **rcp:** Remote Copy Protocol（RCP）ネットワーク サーバです。 **system:** 実行コンフィギュレーションを含むシステム メモリが格納されています。 **tftp:** Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）ネットワーク サーバ。 **zflash:** フラッシュ ファイル システムの内容をミラーリングした、読み取り専用ファイル解凍ファイル システム。

デフォルト ファイル システムの設定

デフォルトのファイル システムとして使用されるファイル システムまたはディレクトリを指定するには、**cd** *filesystem:* 特権 EXEC コマンドを使用します。デフォルト ファイル システムを設定すると、関連するコマンドを実行するときに *filesystem:* 引数を省略できます。たとえば、オプションの *filesystem:* 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイル システムが使用されます。

デフォルトでは、デフォルト ファイル システムは *flash:* です。

cd コマンドで指定された現在のデフォルトのファイル システムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

ファイル システム上のファイル情報の表示

ファイル システムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイル システムに同じ名前のコンフィギュレーション ファイルがまだ格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、別のコマンドで使用するファイル名を確認できます。

ファイル システムのファイルに関する情報を表示するには、表 20-2 に記載された特権 EXEC コマンドのいずれかを使用します。

表 20-2　ファイルに関する情報を表示するためのコマンド

コマンド	説明
dir [**/all**] [*filesystem***:**][*filename*]	ファイル システムのファイル リストを表示します。
show file systems	ファイル システムのファイルごとの詳細を表示します。
show file information *file-url*	特定のファイルに関する情報を表示します。
show file descriptors	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスの **flash:** を使用します。
ステップ 2	**cd** *directory_name*	目的のディレクトリに変更します。
ステップ 3	**pwd**	作業ディレクトリを表示します。

ディレクトリの作成と削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**dir** *filesystem***:**	指定されたファイル システムのディレクトリを表示します。 *filesystem***:** には、システム ボードのフラッシュ デバイスの **flash:** を使用します。
ステップ 2	**mkdir** *directory_name*	新しいディレクトリを作成します。 ディレクトリ名では、大文字と小文字が区別されます。 スラッシュ(/)間に指定できるディレクトリ名は最大 45 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	**dir** *filesystem***:**	設定を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、**delete /force/recursive** *filesystem***:/***file-url* 特権 EXEC コマンドを使用します。

名前で指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

filesystem には、システム ボードのフラッシュ デバイスの **flash:** を使用します。*file-url* には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

注意　ファイルおよびディレクトリが削除された場合、その内容は回復できません。

ファイルのコピー

ファイルをコピー元からコピー先にコピーするには、特権 EXEC コマンド **copy** [**/erase**] *source-url destination-url* を使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドは、現在実行中のコンフィギュレーション ファイルをフラッシュ メモリの NVRAM セクションに保存し、システム初期化の際にコンフィギュレーション ファイルとして使用されるようにします。

（注）　オプションの引数 **/erase** を copy コマンドに追加すると、宛先が上書きされます。宛先に同じ名前のファイルがある場合、そのファイルはコピーされる新しいファイルに置き換えられます。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、および **tftp:** が含まれ、次のような構文で表されます。

- ファイル転送プロトコル（FTP）：**ftp:**[[*//username* [**:***password*]*@location*]*/directory*]*/filename*
- リモート コピー プロトコル（RCP）：**rcp:**[[*//username@location*]*/directory*]*/filename*
- 簡易ファイル転送プロトコル（TFTP）：**tftp:**[[*//location*]*/directory*]*/filename*

ローカルにある書き込み可能なファイル システムには flash: などがあります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ（たとえば、**copy flash: flash:** コマンドは無効）

コンフィギュレーション ファイルによる **copy** コマンドの具体的な使用例については、「コンフィギュレーション ファイルの操作」（P.20-9）を参照してください。

新しいバージョンをダウンロードするか既存のバージョンをアップロードしてソフトウェア イメージをコピーするには、特権 EXEC コマンド **archive download-sw** または **archive upload-sw** を使用します。詳細については、「ソフトウェア イメージの操作」（P.20-21）を参照してください。

ファイルの削除

フラッシュ メモリ デバイス上のファイルが不要になった場合、永続的に削除できます。指定したフラッシュ デバイスからファイルやディレクトリを削除するには、特権 EXEC コマンド **delete** [**/force**] [**/recursive**] [*filesystem***:**]*/file-url* を使用します。

注意　ファイルが削除された場合、その内容は回復できません。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

*filesystem***:** オプションを省略した場合、アクセス ポイントは **cd** コマンドで指定されたデフォルト デバイスを使用します。*file-url* には、削除するファイルのパス（ディレクトリ）および名前を指定します。

次の例は、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する方法を示しています。

```
ap# delete myconfig
```

tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます（次の項を参照）。

tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

archive tar/create *destination-url* **flash:/***file-url*

destination-url には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:/*file-url*
- ファイル転送プロトコル（FTP）の場合、構文は
  ftp:[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** です。
- リモート コピー プロトコル（RCP）の場合、構文は
  rcp:[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** です。
- 簡易ファイル転送プロトコル（TFTP）の場合、構文は
  tftp:[[**//***location*]**/***directory*]**/***tar-filename***.tar** です。

*tar-filename***.tar** は、作成する tar ファイルです。

flash:/*file-url* には、新しい tar ファイルの作成元になるローカル フラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。このコマンドは、ローカル フラッシュ デバイスの *new-configs* ディレクトリの内容を、TFTP サーバの 172.20.10.30 にある *saved.tar* というファイルに書き込みます。

```
ap# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

archive tar/table *source-url*

source-url には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- ファイル転送プロトコル（FTP）の場合、構文は
  ftp:[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** です。
- リモート コピー プロトコル（RCP）の場合、構文は
  rcp:[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** です。
- 簡易ファイル転送プロトコル（TFTP）の場合、構文は
  tftp:[[**//***location*]**/***directory*]**/***tar-filename***.tar** です。

*tar-filename***.tar** は、表示する tar ファイルです。

また、tar ファイルの後にファイルまたはディレクトリのオプション リストを指定すると、ファイルの表示を制限できます。リスト内のファイルだけが表示されます。何も指定しなかった場合、すべてのファイルおよびディレクトリが表示されます。

次の例では、フラッシュ メモリ内にある *ap3g2-k9w7-tar.152-4.JB5.tar* ファイルの内容を表示する方法を示します。

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
ap# archive tar /table flash:ap3g2-k9w7-tar.152-4.JB5.tar
info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
.../...
```

次の例では、*ap3g2-k9w7-mx.152-4.JB5/html* ディレクトリとその内容を表示する方法を示します。

```
ap# archive tar /table flash:/ap3g2-k9w7-tar.152-4.JB5.tar ap3g2-k9w7-mx.152-4.JB5/html
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 bytes)
```

tar ファイルの抽出

フラッシュ ファイル システムのディレクトリに tar ファイルを抽出するには、次の特権 EXEC コマンドを使用します。

archive tar /xtract *source-url* **flash:/***file-url*

source-url には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。
  flash:
- ファイル転送プロトコル（FTP）の場合、構文は
  ftp:[[*//username*[**:***password*]*@location*]**/***directory*]**/***tar-filename***.tar** です。
- リモート コピー プロトコル（RCP）の場合、構文は
  rcp:[[*//username@location*]**/***directory*]**/***tar-filename***.tar** です。
- 簡易ファイル転送プロトコル（TFTP）の場合、構文は
  tftp:[[*//location*]**/***directory*]**/***tar-filename***.tar** です。

*tar-filename***.tar** は、ファイルの抽出元の tar ファイルです。

flash:/*file-url* には、tar ファイルの抽出先であるローカル フラッシュ ファイル システムの場所を指定します。また、tar ファイル内の抽出するファイルまたはディレクトリのオプション リストを指定できます。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。このコマンドは、*new-configs* ディレクトリだけをローカル フラッシュ ファイル システムのルート ディレクトリに抽出します。*saved.tar* ファイルの残りのファイルは無視されます。

```
ap# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、**more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
ap# more tftp://serverA/hampton/savedconfig
!
!Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!

<output truncated>
```

コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説明します。コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。これらのコマンドをより効果的にするために、アクセス ポイントにはシステム ソフトウェアと対話するための最小限のデフォルト実行コンフィギュレーションが含まれています。

TFTP、FTP、RCP サーバのコンフィギュレーション ファイルは、次の理由でアクセス ポイントの実行コンフィギュレーションにコピー（*ダウンロード*）できます。

- バックアップ コンフィギュレーション ファイルを復元するため。
- 別のアクセス ポイントのコンフィギュレーション ファイルを使用するため。たとえば、ネットワークにアクセス ポイントを追加して、そのアクセス ポイントを元のアクセス ポイントと同じように設定できます。新しいアクセス ポイントにファイルをコピーすると、ファイル全体を作り直すことなく関連する部分を変更できます。
- ネットワークにあるすべてのアクセス ポイントに同じコンフィギュレーション コマンドをロードするため。これは、すべてのアクセス ポイントを同じように設定するために行います。

TFTP、FTP、または RCP を使用して、アクセス ポイントのコンフィギュレーション ファイルをファイル サーバにコピー（*アップロード*）できます。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておくと、後でサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。FTP と RCP が組み込まれたプロトコルであり、接続指向型の伝送制御プロトコル/インターネット プロトコル（TCP/IP）スタックを使用しているため、このような改善が可能なのです。

ここでは、次の情報について説明します。

- 「コンフィギュレーション ファイルの作成および使用上の注意事項」（P.20-10）
- 「コンフィギュレーション ファイルのタイプおよび場所」（P.20-10）
- 「テキスト エディタによるコンフィギュレーション ファイルの作成」（P.20-11）
- 「TFTP によるコンフィギュレーション ファイルのコピー」（P.20-11）

コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルの作成によって、アクセス ポイントを設定できます。コンフィギュレーション ファイルには、1 つ以上のアクセス ポイントの設定に必要なコマンドの一部、またはすべてを格納できます。たとえば、同一のハードウェア構成を持つ複数のアクセス ポイントに同一のコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- アクセス ポイントにパスワードが設定されていない場合は、グローバル コンフィギュレーション コマンド **enable secret** *secret-password* を入力して、各アクセス ポイントにパスワードを設定する必要があります。このコマンドには空白行を入力します。パスワードは、クリアテキストとしてコンフィギュレーション ファイルに保存されます。
- パスワードがすでに存在する場合、パスワードの検証に失敗するので、ファイルにグローバル コンフィギュレーション コマンド **enable secret** *secret-password* を入力できません。コンフィギュレーション ファイルにパスワードを入力すると、アクセス ポイントはファイルを実行するときに誤ってコマンドとしてパスワードを実行しようとします。
- 特権 EXEC コマンド **copy** {**ftp:** | **rcp:** | **tftp:**} **system:running-config** は、コマンド ラインでコマンドを入力するのと同じように、アクセス ポイントでコンフィギュレーション ファイルをロードします。アクセス ポイントは、コマンドを追加する前に既存の実行コンフィギュレーションを消去しません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた(コピーされたコンフィギュレーション ファイルが優先する)コンフィギュレーション ファイルが作成されます。

  コンフィギュレーション ファイルをサーバに保存されたファイルの完全なコピーに復元するには、特権 EXEC コマンド **copy** {**ftp:** | **rcp:** | **tftp:**} **nvram:startup-config** を使用して、このコンフィギュレーション ファイルをスタートアップ コンフィギュレーションに直接コピーし、アクセス ポイントをリロードします。

コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2 つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した後、**copy running-config startup-config** 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存され、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに保存されます。

テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

ステップ 1　既存のコンフィギュレーション ファイルをアクセス ポイントからサーバにコピーします。

詳細については、「TFTP によるコンフィギュレーション ファイルのダウンロード」(P.20-12)、「FTP によるコンフィギュレーション ファイルのダウンロード」(P.20-14)、または「RCP によるコンフィギュレーション ファイルのダウンロード」(P.20-18)を参照してください。

ステップ 2　UNIX では vi や emacs、PC ではメモ帳などのテキスト エディタでコンフィギュレーション ファイルを開きます。

ステップ 3　目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出して、新しいファイルに保存します。

ステップ 4　コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ（UNIX ワークステーションの場合は、通常は /tftpboot）にコピーします。

ステップ 5　ファイルに関する権限が world-read に設定されていることを確認します。

TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用したアクセス ポイントの設定、別のアクセス ポイントまたは TFTP サーバからのダウンロードが実行できます。また、コンフィギュレーション ファイルを TFTP サーバにコピー（アップロード）して、格納できます。

ここでは、次の情報について説明します。

- 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-11)
- 「TFTP によるコンフィギュレーション ファイルのダウンロード」(P.20-12)
- 「TFTP によるコンフィギュレーション ファイルのアップロード」(P.20-12)

TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。
- アクセス ポイントに TFTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと TFTP サーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが、TFTP サーバ上の正しいディレクトリにあることを確認します。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。

- アップロード操作でサーバ上の既存のファイルを上書きする場合は、そのファイルに対する適切な権限が設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してアクセス ポイントを設定するには、次の手順に従います。

ステップ 1　コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。

ステップ 2　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-11)を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 3　Telnet セッションでアクセス ポイントにログインします。

ステップ 4　アクセス ポイントを設定するためのコンフィギュレーション ファイルを TFTP サーバからダウンロードします。

TFTP サーバの IP アドレスまたはホスト名と、ダウンロードするファイルの名前を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **system:running-config**
- **copy tftp:**[[[*//location*]*/directory*]*/filename*] **nvram:startup-config**

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-confg* からソフトウェアを設定する例を示します。

```
ap# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
Booting tokyo-confg from 172.16.2.155:!!![OK - 874/16000 bytes]
```

TFTP によるコンフィギュレーション ファイルのアップロード

アクセス ポイントから TFTP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順に従います。

ステップ 1　「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-11)を参照して、TFTP サーバが適切に設定されていることを確認します。

ステップ 2　Telnet セッションでアクセス ポイントにログインします。

ステップ 3　アクセス ポイントの設定を、TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名と、アップロード先のファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:**[[[*//location*]*/directory*]*/filename*]
- **copy nvram:startup-config tftp:**[[[*//location*]*/directory*]*/filename*]

TFTP サーバにファイルがアップロードされます。

次の例は、コンフィギュレーション ファイルをアクセス ポイントから TFTP サーバにアップロードする方法を示しています。

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!![OK]
```

FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは、次のリストで最初に有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- Anonymous

アクセス ポイントは、次のリストで最初に有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- アクセス ポイントが作成するパスワード *username*@*apname.domain*。変数 *username* は現在のセッションと関連付けられたユーザ名、*apname* は設定済みホスト名、*domain* はアクセス ポイントのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

詳細は、ご使用の FTP サーバの資料を参照してください。

ここでは、次の情報について説明します。

- 「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.20-14）
- 「FTP によるコンフィギュレーション ファイルのダウンロード」（P.20-14）
- 「FTP によるコンフィギュレーション ファイルのアップロード」（P.20-15）

FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- アクセス ポイントに FTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと FTP サーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の FTP ユーザ名が、FTP ダウンロードで使用したいユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。
- FTP サーバにコンフィギュレーション ファイルをアップロードする場合、アクセス ポイントのユーザからの書き込み要求を受け付けるように FTP サーバを適切に設定しておく必要があります。

詳細は、ご使用の FTP サーバの資料を参照してください。

FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-14) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	アクセス ポイントでグローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです(ステップ 4からステップ 6を続けます)。
ステップ 4	**ip ftp username** *username*	(任意)デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	(任意)デフォルトのパスワードを変更します。

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*] **system:running-config** または **copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/***filename*] **nvram:startup-config**	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次の例は、コンフィギュレーション ファイル *host1-confg* を IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからコピーし、アクセス ポイントでそのコマンドをロードして実行する方法を示しています。

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* は、IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからアクセス ポイントのスタートアップ コンフィギュレーションにコピーされます。

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.20-14）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。

	コマンド	目的
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4からステップ 6を続けます）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copy system:running-config ftp:**[[[**//**[*username*[**:***password*]@]*location*]**/***directory*]**/***filename*] または **copy nvram:startup-config ftp:**[[[**//**[*username*[**:***password*]@]*location*]**/***directory*]**/***filename*]	FTP を使用して、アクセス ポイントの実行中のコンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定された場所に保存します。

次の例は、実行コンフィギュレーション ファイル *ap2-confg* を、IP アドレス 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリにコピーする方法を示しています。

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-confg
Write file ap2-confg on host 172.16.101.101? [confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101? [confirm]
![OK]
```

RCP によるコンフィギュレーション ファイルのコピー

Remote Copy Protocol（RCP）を使用すると、リモート ホストとアクセス ポイントの間でコンフィギュレーション ファイルを別の方式でダウンロード、アップロード、コピーできます。コネクションレス プロトコルであるユーザ データグラム プロトコル（UDP）を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけでかまいません（ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名（ユーザ名が指定されている場合）
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、**username** コマンドによって認証されている場合、アクセス ポイント ソフトウェアは Telnet ユーザ名をリモート ユーザ名として送信します。
- アクセス ポイント ホスト名。

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

ここでは、次の情報について説明します。

- 「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.20-17）
- 「RCP によるコンフィギュレーション ファイルのダウンロード」（P.20-18）
- 「RCP によるコンフィギュレーション ファイルのアップロード」（P.20-19）

RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- アクセス ポイントに RCP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントとサーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、RCP サーバへの接続を確認します。

- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の RCP ユーザ名が RCP ダウンロードで使用したいユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。
- RCP サーバにファイルをアップロードする場合、アクセス ポイントのユーザからの RCP 書き込み要求を受け付けるようにこのサーバを適切に設定しておく必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、アクセス ポイントに次の設定行が設定されているとします。

```
hostname ap1
ip rcmd remote-username User0
```

アクセス ポイントの IP アドレスが *ap1.company.com* に変換された場合、RCP サーバの User0 の .rhosts ファイルに次の行を追加する必要があります。

```
ap1.company.com ap1
```

詳細は、ご使用の RCP サーバの資料を参照してください。

RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-17) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです(ステップ 4およびステップ 5を続けます)。
ステップ 4	**ip rcmd remote-username** *username*	(任意)リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*] **system:running-config** または **copy rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次の例は、コンフィギュレーション ファイル *host1-confg* を IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからコピーし、アクセス ポイントでそのコマンドをロードして実行する方法を示しています。

```
ap# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-confg* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.20-17）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4およびステップ 5を続けます）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。

	コマンド	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy system:running-config rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*] または **copy nvram:startup-config rcp:**[[[**//**[*username*@]*location*]/*directory*]/*filename*]	RCP を使用して、アクセス ポイントの実行中のコンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコンフィギュレーション ファイルをコピーします。

次の例は、実行コンフィギュレーション ファイル *ap2-confg* を、IP アドレス 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリにコピーする方法を示しています。

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-confg
Write file ap-confg on host 172.16.101.101? [confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101? [confirm]
![OK]
```

設定情報の消去

この項では、設定情報をクリアする方法を説明します。

格納されたコンフィギュレーション ファイルの削除

注意　削除されたファイルは復元できません。

保存されたコンフィギュレーション ファイルをフラッシュ メモリから削除するには、特権 EXEC コマンド **delete flash:***filename* を使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、ファイルを削除するかどうか確認を求めるプロンプトが表示されます。**file prompt** コマンドの詳細については、『*Cisco IOS Command Reference*』ガイドを参照してください。

常に TFTP サーバからコンフィギュレーション ファイルをダウンロードする

NVRAM（フラッシュ）にコンフィギュレーション ファイルが保管されている場合でも、常に TFTP サーバからコンフィギュレーション ファイル（config.txt）をダウンロードするように AP を設定できます。

この設定を行う前に、ルータまたはスイッチ上のアクセス ポイントに、DHCP サーバを使用した自動インストール機能を設定する必要があります。この機能が設定されていないと、以下の設定は有効になりません。

常に TFTP サーバからコンフィギュレーション ファイルをダウンロードするように AP を設定するには、グローバル コンフィギュレーション モードで、コマンド **boot config-skip** を使用します。この設定を無効にするには、コマンド **no boot config-skip** を使用します。デフォルトでは、この機能はディセーブルになっています。

```
ap(config)# boot config-skip
ap(config)# no boot config-skip
```

ブート モードでは、次のコマンドを使用して、この機能を有効または無効にできます。

- 有効にする場合：**ap: set BOOT_CONFIG_SKIP yes**
- 無効にする場合：**ap: set BOOT_CONFIG no**
- 無効にする場合：**ap: unset BOOT_CONFIG_SKIP**

この設定を GUI で行うには、次の手順に従います。

ステップ 1　[Software] > [System Configuration] に移動します。

ステップ 2　[Boot Config Skip] オプションに対して、必要に応じて [Enable] または [Disable] をクリックします。

ステップ 3　[Apply] をクリックします。

ソフトウェア イメージの操作

この項では、システム ソフトウェア、Cisco IOS ソフトウェア、無線ファームウェア、および Web 管理 HTML ファイルを含むソフトウェア イメージ ファイルのアーカイブ（ダウンロードとアップロード）の方法を説明します。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルを、TFTP、FTP、または RCP サーバからダウンロードします。バックアップ用に、アクセス ポイント イメージ ファイルを TFTP、FTP、または RCP サーバにアップロードします。アップロードしたこのイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。FTP と RCP が組み込まれたプロトコルであり、接続指向型の伝送制御プロトコル/インターネット プロトコル（TCP/IP）スタックを使用しているため、このような改善が可能です。

ここでは、次の情報について説明します。

（注）　ソフトウェア イメージとサポートされているアップグレード パスのリストについては、アクセス ポイントのリリース ノートを参照してください。

アクセス ポイントのイメージの場所

Cisco IOS イメージは、バージョン番号を表示したディレクトリに保存されています。サブディレクトリには、Web 管理に必要な HTML ファイルが入っています。イメージは、システム ボードのフラッシュ メモリ（flash:）に格納されています。

特権 EXEC コマンド **show version** を使用して、アクセス ポイントで現在実行中のソフトウェアのバージョンを確認できます。`System image file is...` で始まる行をディスプレイで確認します。この行には、イメージが保存されているフラッシュ メモリ内のディレクトリ名が表示されます。

また、特権 EXEC コマンド **dir** *filesystem*: を使用して、フラッシュ メモリに保存したその他のソフトウェア イメージのディレクトリ名を表示することもできます。

（注）　Cisco Aironet 3600、3700、および 2700 シリーズ AP の Cisco IOS リリース 15.2(4)JB および 12.4(25e)JAO 以降では、新しいイメージがシステム ボードのフラッシュ メモリにダウンロードされると、フラッシュ メモリにあるバックアップ IOS イメージが削除されます。システム ボードのフラッシュ メモリ サイズの合計は 31 MB であり、リカバリ イメージ、新しいイメージ、およびバックアップ イメージを格納するのに十分な領域があるため、このような設計になっています。

サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- *info* ファイル

  info ファイルは、常に tar ファイルの先頭にあり、その tar ファイルに含まれるファイルの情報が入っています。
- Cisco IOS イメージ
- アクセス ポイントの HTTP サーバで要求される Web 管理ファイル
- 無線ファームウェア 5000.img ファイル

- *info.ver* ファイル

  info.ver ファイルは、常に tar ファイルの末尾にあり、info ファイルと同じ情報が入っています。info.ver ファイルは tar ファイルの最後のファイルであるため、このファイルが存在すればイメージ内のすべてのファイルがダウンロードされたことになります。

（注）　tar ファイルには *.tar* 以外の拡張子が付いていることがあります。

TFTP によるイメージ ファイルのコピー

TFTP サーバからアクセス ポイント イメージをダウンロードしたり、アクセス ポイントから TFTP サーバにイメージをアップロードしたりできます。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きできます。

バックアップのために、アクセス ポイントのイメージ ファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.20-23）
- 「TFTP によるイメージ ファイルのダウンロード」（P.20-24）
- 「TFTP によるイメージ ファイルのアップロード」（P.20-25）

TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。
- アクセス ポイントに TFTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと TFTP サーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが、TFTP サーバ上の正しいディレクトリにあることを確認します。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は world-read でなければなりません。
- アップロード操作でサーバ上の既存のファイルを上書きする場合は、そのファイルに対する適切な権限が設定されていることを確認します。ファイルの権限は world-write でなければなりません。

TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 3 を実行します。

	コマンド	目的
ステップ 1		イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-23)を参照して、TFTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**archive download-sw /overwrite /reload tftp:**[[*//location*]*/directory*]*/image-name*	イメージ ファイルを TFTP サーバからアクセス ポイントにダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name* には、ディレクトリ(任意)とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 4	**archive download-sw /leave-old-sw /reload tftp:**[[*//location*]*/directory*]*/image-name*	イメージ ファイルを TFTP サーバからアクセス ポイントにダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name* には、ディレクトリ(任意)とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

（注）　ダウンロードの失敗を回避するには、**archive download-sw /safe** コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセス ポイント モデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュ デバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注）　アクセス ポイント IOS をダウングレードする手順は IOS アップグレードを実行する手順と同じです。アクセス ポイント IOS をダウングレードするには、**archive download-sw /overwrite /reload tftp:**[[*//location*]*/directory*]*/image-name* と入力します。*overwrite* パラメータを指定すると、現在の IOS イメージが消去され、新しくダウングレードされたバージョンの IOS がアクセス ポイントにロードされます。*/reload* オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。

（注）　フラッシュ デバイスに 2 つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの 1 つを上書きする場合、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステム ボードのフラッシュ デバイス（flash:）にインストールされます。イメージは、ソフトウェア バージョンのストリングで名付けられた新しいディレクトリに保存され、新しくインストールされたイメージをポイントするように、システム ブート パス変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem***:/***file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスの **flash:** を使用します。*file-url* には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

TFTP によるイメージ ファイルのアップロード

イメージをアクセス ポイントから TFTP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更*しないでください*。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-23) を参照して、TFTP サーバが適切に設定されていることを確認します。
ステップ 1		Telnet セッションでアクセス ポイントにログインします。
ステップ 2	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name*.**tar**	現在実行中のアクセス ポイント イメージを TFTP サーバにアップロードします。 • *//location* には、TFTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ(任意)およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name*.**tar** は、サーバ上に格納するソフトウェア イメージの名前です。

特権 EXEC コマンド **archive upload-sw** は、info ファイル、Cisco IOS イメージ ファイル、HTML ファイル、および info.ver ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

FTP によるイメージ ファイルのコピー

FTP サーバからアクセス ポイント イメージをダウンロードしたり、アクセス ポイントから FTP サーバにイメージをアップロードしたりできます。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップ用に、アクセス ポイント イメージ ファイルをサーバにアップロードします。アップロードしたイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-26)
- 「FTP によるイメージ ファイルのダウンロード」(P.20-28)
- 「FTP によるイメージ ファイルのアップロード」(P.20-30)

FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名(ユーザ名が指定されている場合)。

- **ip ftp username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- Anonymous

アクセス ポイントは、次のリストで最初に有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password** *password* グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- アクセス ポイントが作成するパスワード *username*@*apname.domain*。変数 *username* は現在のセッションと関連付けられたユーザ名、ap*name* は設定済みホスト名、*domain* はアクセス ポイントのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- アクセス ポイントに FTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと FTP サーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、FTP サーバへの接続を確認します。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の FTP ユーザ名が、FTP ダウンロードで使用したいユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- FTP サーバにイメージ ファイルをアップロードする場合、アクセス ポイントのユーザからの書き込み要求を受け付けるように FTP サーバを適切に設定しておく必要があります。

詳細は、ご使用の FTP サーバの資料を参照してください。

FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ステップ 7 の手順を実行します。現在のイメージを保存するには、ステップ 7 をスキップします。

	コマンド	目的
ステップ 1		「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-26) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4、5、および 6 を参照）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]*@location*]*/directory*] */image-name*.**tar**	イメージ ファイルを FTP サーバからアクセス ポイントにダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-26) を参照してください。 • *@location* には、FTP サーバの IP アドレスを指定します。 • *directory/image-name*.**tar** には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

	コマンド	目的
ステップ 8	**archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]**@***location*]***/directory***] ***/image-name*.tar**	イメージ ファイルを FTP サーバからアクセス ポイントにダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • *//username*[**:***password*] には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-26)を参照してください。 • *@location* には、FTP サーバの IP アドレスを指定します。 • *directory/image-name*.tar には、ディレクトリ(任意)およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

(注) ダウンロードの失敗を回避するには、**archive download-sw /safe** コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセス ポイント モデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュ デバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

(注) フラッシュ デバイスに 2 つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの 1 つを上書きする場合、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステム ボードのフラッシュ デバイス(flash:)にインストールされます。イメージは、ソフトウェア バージョンのストリングで名付けられた新しいディレクトリに保存され、新しくインストールされたイメージをポイントするように、BOOT パスリストが更新されます。ブート属性を表示するには、特権 EXEC モード コマンド **show boot** を使用し、ブート属性を変更するには、グローバル コンフィギュレーション コマンド **boot** を使用します。

ダウンロード プロセス中に古いイメージを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスの **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

FTP によるイメージ ファイルのアップロード

イメージをアクセス ポイントから FTP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

アップロード機能が使用できるのは、Cluster Management Suite（CMS）と関連付けられた HTML ページが既存のイメージとともにインストールされている場合だけです。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」（P.20-14）を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです（ステップ 4からステップ 6を続けます）。
ステップ 4	**ip ftp username** *username*	（任意）デフォルトのリモート ユーザ名を変更します。
ステップ 5	**ip ftp password** *password*	（任意）デフォルトのパスワードを変更します。
ステップ 6	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	**archive upload-sw ftp:**[[*//*[*username*[**:***password*]@]*location*]*/directory*]*/image-name*.**tar**	現在実行中のアクセス ポイント イメージを FTP サーバにアップロードします。 • *//username*:*password* には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-26)を参照してください。 • @*location* には、FTP サーバの IP アドレスを指定します。 • */directory/image-name*.**tar** には、ディレクトリ(任意)およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。*image-name*.**tar** は、サーバ上に格納するソフトウェア イメージの名前です。

archive upload-sw コマンドは、info ファイル、Cisco IOS イメージ ファイル、HTML ファイル、info.ver ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

RCP によるイメージ ファイルのコピー

RCP サーバからアクセス ポイント イメージをダウンロードしたり、アクセス ポイントから RCP サーバにイメージをアップロードしたりできます。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップ用に、アクセス ポイント イメージ ファイルをサーバにアップロードします。アップロードしたこのイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-32)
- 「RCP によるイメージ ファイルのダウンロード」(P.20-33)
- 「RCP によるイメージ ファイルのアップロード」(P.20-35)

RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

RCP によって、リモート ホストとアクセス ポイントの間でイメージ ファイルをダウンロードおよびアップロードする別の方法が提供されます。コネクションレス プロトコルであるユーザ データグラム プロトコル（UDP）を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の copy コマンドは、リモート システム上の rsh サーバ（またはデーモン）を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは rsh をサポートするサーバにアクセスするだけでかまいません（ほとんどの UNIX システムは rsh をサポートしています）。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名（ユーザ名が指定されている場合）。
- **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが入力されている場合）。
- 現在の TTY（端末）プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、**username** コマンドによって認証されている場合、アクセス ポイント ソフトウェアは Telnet ユーザ名をリモート ユーザ名として送信します。
- アクセス ポイント ホスト名。

RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、rsh がサポートされていることを確認します。
- アクセス ポイントに RCP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントとサーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、RCP サーバへの接続を確認します。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の RCP ユーザ名が RCP ダウンロードで使用したいユーザ名であることを確認します。**show users** 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される **ip rcmd remote-username** *username* グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

- RCP サーバにイメージをアップロードする場合、アクセス ポイントのユーザからの RCP 書き込み要求を受け付けるように、このサーバを設定しておく必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の .rhosts ファイルにエントリを追加する必要があります。たとえば、アクセス ポイントに次の設定行が設定されているとします。

```
hostname ap1
ip rcmd remote-username User0
```

アクセス ポイントの IP アドレスが *ap1.company.com* に変換された場合、RCP サーバの User0 の .rhosts ファイルに次の行を追加する必要があります。

```
ap1.company.com ap1
```

詳細は、ご使用の RCP サーバの資料を参照してください。

RCP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ～ 6 の手順を実行します。現在のイメージをそのまま維持するには、ステップ 6 をスキップします。

	コマンド	目的
ステップ 1		「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-32) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 およびステップ 5 を続けます)。
ステップ 4	**ip rcmd remote-username** *username*	(任意) リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 6	**archive download-sw /overwrite /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name*.**tar**]	イメージ ファイルを RCP サーバからアクセス ポイントにダウンロードし、現在のイメージを上書きします。 • **/overwrite** オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • **//***username* には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-32)を参照してください。 • @*location* には、RCP サーバの IP アドレスを指定します。 • **/***directory*/*image-name*.**tar** には、ディレクトリ(任意)およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。
ステップ 7	**archive download-sw /leave-old-sw /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name*.**tar**]	イメージ ファイルを RCP サーバからアクセス ポイントにダウンロードし、現在のイメージを維持します。 • **/leave-old-sw** オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。 • **/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。 • **//***username* には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-32)を参照してください。 • @*location* には、RCP サーバの IP アドレスを指定します。 • **/***directory*]**/***image-name*.**tar** には、ディレクトリ(任意)とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。

（注）　ダウンロードの失敗を回避するには、**archive download-sw /safe** コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセス ポイント モデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュ デバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。

（注）　フラッシュ デバイスに 2 つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの 1 つを上書きする場合、**/overwrite** オプションを指定する必要があります。

/leave-old-sw を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分な余裕がない場合に稼働中のイメージを保存しようとすると、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステム ボードのフラッシュ デバイス（flash:）にインストールされます。このイメージはソフトウェア バージョン ストリングの名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は（**/leave-old-sw** キーワードを指定した場合は）、**delete /force/recursive** *filesystem*:*/file-url* 特権 EXEC コマンドを入力して、そのイメージを削除できます。*filesystem* には、システム ボードのフラッシュ デバイスの **flash:** を使用します。*file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

RCP によるイメージ ファイルのアップロード

イメージをアクセス ポイントから RCP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。

注意　ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

アップロード機能が使用できるのは、Cluster Management Suite（CMS）と関連付けられた HTML ページが既存のイメージとともにインストールされている場合だけです。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.20-32）を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。

	コマンド	目的
ステップ 3	**configure terminal**	グローバル コンフィギュレーション モードを開始します。 この手順が必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4およびステップ 5を続けます）。
ステップ 4	**ip rcmd remote-username** *username*	（任意）リモート ユーザ名を指定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**archive upload-sw rcp:**[[[*//*[*username*@]*location*]*/directory*]*/image-name*.**tar**]	現在実行中のアクセス ポイント イメージを RCP サーバにアップロードします。 • *//username* にはユーザ名を指定します。RCP コピー要求を実行するには、ネットワーク サーバ上でリモート ユーザ名にアカウントを定義する必要があります。詳細については、「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」（P.20-32）を参照してください。 • *@location* には、RCP サーバの IP アドレスを指定します。 • */directory*]*/image-name*.**tar** には、ディレクトリ（任意）およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。 • *image-name*.**tar** は、サーバに保存するソフトウェア イメージの名前です。

特権 EXEC コマンド **archive upload-sw** は、info ファイル、Cisco IOS イメージ ファイル、HTML ファイル、および info.ver ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

Web ブラウザ インターフェイスによるイメージのリロード

アクセス ポイントのイメージ ファイルをリロードするには、Web ブラウザ インターフェイスも使用できます。Web ブラウザ インターフェイスでは、HTTP または TFTP インターフェイスを使用したイメージ ファイルのロードがサポートされています。

（注） ブラウザを使用してイメージ ファイルをリロードする場合、アクセス ポイントの設定は変更されません。

ブラウザ HTTP インターフェイス

HTTP インターフェイスを使用すると、PC 上にあるアクセス ポイント イメージ ファイルを参照し、アクセス ポイントにイメージをダウンロードできます。HTTP インターフェイスを使用する手順は、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。

ステップ 2　ブラウザのアドレス入力用ボックスにアクセス ポイントの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

ステップ 3　[Username] フィールドにユーザ名を入力します。

ステップ 4　[Password] フィールドにアクセス ポイントのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。

ステップ 5　[Software] > [Software Upgrade] を選択します。[HTTP Upgrade] 画面が表示されます。

ステップ 6　[Browse] ボタンをクリックして、PC 内のイメージ ファイルを探します。

ステップ 7　[Upgrade] ボタンをクリックします。

詳細は、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。

ブラウザ TFTP インターフェイス

TFTP インターフェイスを使用すると、ネットワーク デバイスの TFTP サーバを使用してアクセス ポイントのイメージ ファイルをロードできます。TFTP サーバを使用する手順は、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。

ステップ 2　ブラウザのアドレス入力用ボックスにアクセス ポイントの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

ステップ 3　[Username] フィールドにユーザ名を入力します。

ステップ 4　[Password] フィールドにアクセス ポイントのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。

ステップ 5　[Software] > [Software Upgrade] を選択します。[HTTP Upgrade] 画面が表示されます。

ステップ 6　[TFTP Upgrade] タブをクリックします。

ステップ 7　[TFTP Server] 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 8　[Upload New System Image Tar File] フィールドに、アクセス ポイントのイメージ ファイル名を入力します。TFTP サーバのルート ディレクトリ下のサブディレクトリ内にファイルがある場合は、TFTP サーバのルート ディレクトリに対する相対パスとファイル名を指定します。ファイルが TFTP サーバのルート ディレクトリにある場合は、ファイル名だけを入力します。

ステップ 9　[Upgrade] ボタンをクリックします。

詳細については、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。

常に TFTP サーバからソフトウェア イメージをダウンロードする

NVRAM（フラッシュ）にコンフィギュレーション ファイルが保管されている場合でも、常に TFTP サーバからソフトウェア イメージ ファイルをダウンロードするように AP を設定できます。このように設定すると、AP がリロードされたときに、常に TFTP サーバからソフトウェア イメージ ファイルがダウンロードされます。

この設定を行う前に、ルータまたはスイッチ上のアクセス ポイントに、DHCP サーバを使用した自動インストール機能を設定する必要があります。この機能が設定されていないと、以下の設定は有効になりません。

常に TFTP サーバからソフトウェア イメージ ファイルをダウンロードするように AP を設定するには、TFTP サーバに保管されているコンフィギュレーション ファイルに次のコマンドを追加します。

boot sytem ***imagename***

次に例を示します。

```
boot system ap3g1-k9w7-tar.wnbu_bt.0101011010
```

DHCP サーバを使用した自動インストール機能が有効な場合、AP がリロードされるたびに、TFTP IP アドレスおよびコンフィギュレーション ファイル名が取得されます。AP はそのコンフィギュレーション ファイルを TFTP サーバからダウンロードして適用します。コンフィギュレーション ファイルに前述の **boot sytem** コマンドが含まれている場合、AP は TFTP サーバからイメージをダウンロードし、その新しいイメージでリロードします。

（注） TFTP サーバからソフトウェア イメージがダウンロードされるのは、サーバ上のイメージが現在 AP で実行されているイメージと同じではない場合のみです。

例：boot system コマンドを含むコンフィギュレーション ファイル

```
no aaa new-model
led display off
no ip source-route
no ip cef
ip domain name Sardinia
!
dot11 syslog
!
dot11 ssid myssid
!
dot11 ssid mysssid
   authentication open
!
boot system ap1g1-k9w7-tar.v153_80mr.201410081600

interface Dot11Radio0
 no ip address
 !
ssid myssid
 !
antenna gain 0
 packet retries 64 drop-packet
 station-role root
 bridge-group 1
```

```
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
end
```

L2TPv3 over UDP/IP の設定

Layer 2 Tunneling Protocol（L2TPv3）は、IP コア ネットワーク上におけるレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。

L2TPv3 トンネルがエンド ポイント間の制御接続となります。1 つの L2TPv3 トンネルが複数のデータ接続を持つことができ、各データ接続は L2TPv3 セッションと呼ばれます。制御接続は、セッションの確立、維持、および解放に使用されます。各セッションは、一意のセッション ID で識別されます。

イーサネット トラフィックにトンネリング サービスを提供するために、L2TPv3 機能には次のテクノロジーを採用しています。

- L2TPv3
- 疑似回線（PW）テクノロジー

前提条件

L2TPv3 を設定する際の前提条件は次のとおりです。

- L2TP クラスを設定する前に、IP ルーティングを有効にする必要があります。
  IP ルーティングを有効にするコマンドは次のとおりです。

  ip routing

- IP CEF を有効にする必要があります。
  IP CEF を有効にするコマンドは次のとおりです。

  ip cef

- VLAN のサブインターフェイスを作成する必要があります。
  VLAN のサブインターフェイスを作成するコマンドは次のとおりです。

  interface Dot11Radio ***interface number.sub-interface number***

  encapsulation dot1Q ***vlan id***

  bridge-group ***bridge id***

  interface GigabitEthernet0.***sub-interface number***

  encapsulation dot1q ***vlan id***

  bridge-group ***bridge id***

（注）　同じ VLAN ID を持つインターフェイスには、同じブリッジ ID を設定する必要があります。

次はサポートされていません。

- IPv6 アドレスを使用したトンネルの確立
- SNMP および GUI コンフィギュレーション
- 同じ LNS（L2TP ネットワーク サーバ）への複数のトンネル
- 物理インターフェイス（Gig、Dot11 など）での xconnect の設定
- 1.6.1 より前の Prol2tp バージョン（シーケンシングまたは Cookie が有効な場合）
- Xconnect で使用できるのは IPv4 アドレスのみです。FQDN はサポートされません。
- 動的 Cookie 割り当てのみが使用されます。

L2TP クラスの設定

L2TP を設定して、さまざまな疑似回線クラスで継承できる、L2TP コントロール プレーン コンフィギュレーション設定のテンプレートを作成します。次のパラメータを設定できます。

- 認証
- L2TPv3 hello 間隔
- ホスト名
- Cookie の長さ
- ダイジェストの有効化
- L2TPv3 制御パケットの再送信および再試行
- タイムアウト
- 受信ウィンドウ サイズ
- hello 間隔

L2TP クラスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**digest hash** *[MD5, SHA]*	メッセージ ダイジェストを有効にします。
ステップ 2	**receive-window** *size*	制御接続のウィンドウ サイズを受信します。
ステップ 3	**hello** *interval*	2 つの hello メッセージ間の間隔を設定します。
ステップ 4	**cookie size** *cookie size*	Cookie サイズを設定します。有効な値は 4 ～ 8 です。
ステップ 5	**digest secret** *secret*	認証用のシークレットを設定します。
ステップ 6	**retransmit retries** *retries*	応答を受信しない場合に制御メッセージを送信する回数を設定します。
ステップ 7	**retransmit timeout min** *minimum timeout*	再試行間隔の最小タイムアウトを設定します。
ステップ 8	**retransmit timeout max** *maximum timeout*	再試行間隔の最大タイムアウトを設定します。

（注）　複数の L2TP クラスを設定できます。

例

```
ap1# configure terminal
ap1(config)# l2tp-class myl2tpclass
ap1(config-l2tp-class)# hostname myhost1
ap1(config-l2tp-class)# hello 15
ap1(config-l2tp-class)# cookie size 4
ap1(config-l2tp-class)# digest secret cisco
ap1(config-l2tp-class)# retransmit retries 6
ap1(config-l2tp-class)# retransmit timeout 7
ap1(config-l2tp-class)# retransmit timeout max 5
ap1(config-l2tp-class)# retransmit timeout min 1
ap1(config-l2tp-class)# end
```

疑似回線クラスの設定

疑似回線クラスを設定して、レイヤ 2 疑似回線クラスを定義します。擬似回線クラスでは、次の疑似回線パラメータを設定できます。

- カプセル化方式
- l2tp-class
- ローカル インターフェイス
- シーケンシング
- IP 関連のパラメータ（dfbit、tos、ttl など）

疑似回線クラスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**pseudowire-class** *pseudowire class name*	疑似回線クラスの名前を指定します。
ステップ 2	**encapsulation l2tpv3**	L2TPv3 を有効にします。
ステップ 3	**protocol l2tpv3ietf** *l2tp class name*	標準 L2TPv3 を有効にして、L2TP クラスを割り当てます。
ステップ 4	**ip protocol udp**	L2TPv3 over UDP を有効にします。
ステップ 5	**ip local interface** *interface name*	インターフェイスのアドレスを送信元アドレスとして使用します。

例

```
ap1# configure terminal
ap1(config)# pseudowire-class mypwclass
ap1(config-pw-class)# encapsulation l2tpv3
ap1(config-pw-class)# protocol l2tpv3ietf myl2tpclass
ap1(config-pw-class)# ip protocol udp
ap1(config-pw-class)# ip local interface BVI1
ap1(config-pw-class)# end
```

L2TP クラスと疑似回線クラスの関係

複数の疑似回線クラスを設定できます。疑似回線クラスは、使用可能ないずれか 1 つの L2TP クラスを使用して設定できます。Xconnect は、設定済みのいずれか 1 つの疑似回線クラスを使用して設定できます。

次の点に注意してください。

- 疑似回線クラスに割り当てることができる L2TP クラスは 1 つだけです。
- L2TP クラスは複数の疑似回線クラスに割り当てることができます。
- xconnect コマンドには疑似回線クラスが割り当てられるため、1 つの xconnect コマンドには 1 つの疑似回線クラスと 1 つの L2TP クラスがあれば十分です。
- 疑似回線クラスに割り当てられていない L2TP クラスと、xconnect コマンドに割り当てられていない疑似回線クラスは、AP の動作に影響を与えません。
- 疑似回線クラスが割り当てられている L2TP クラスを修正することはできません。修正するには、L2TP クラスに割り当てられた疑似回線クラスを使用しているインターフェイスから、xconnect を除去する必要があります。

トンネル インターフェイスの設定

単一のトンネルをサポートするための新しいインターフェイスです。このインターフェイスに、すべての L2TPv3 トラフィックの xconnect を設定できます。

トンネル インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface VDT** *index*	VDT インターフェイスを指定します。
ステップ 2	**no ip address**	IP アドレスを無効にします。
ステップ 3	**xconnect** *LNS ip* | *vc-id* | **pw-class** *pseudowire class name*	LNS IP を設定して、疑似回線クラスを割り当てます。

VC ID は、ローカルで有効な数値です。すべての xconnect コマンドは、一意の VC ID を使用して設定する必要があります。**xconnect** *VDT index* が設定された SSID のトラフィックは、同じインデックスが設定された VDT インターフェイスを介してトンネリングされます。

例

```
ap1# configure terminal
ap1(config)# interface VDT0
ap1(config-if)# xconnect 100.100.10.2 10 pw-class mypwclass
ap1(config-if)# end
```

トンネル管理インターフェイスの設定

セカンダリ トンネルをサポートするための新しいインターフェイスです。

トンネル管理インターフェイスを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface VDT-Mgmt** index	VDT 管理インターフェイスを指定します。
ステップ 2	**no ip dhcp client request router**	DHCP からのデフォルト ルートを無効にします。
ステップ 3	**ip address** *dhcp* | *ip netmask*	DHCP IP またはスタティック IP を指定します。
ステップ 4	**vdt-mgmt vlan 10**	VLAN ID を設定します。

このインターフェイスにより、トンネルを介して AP にアクセスできます。このインターフェイスは、同じインデックスが設定された VDT インターフェイスにアソシエートされます。このインターフェイスからのトラフィックは、同じインデックスが設定された VDT インターフェイスによって確立されたトンネルを介してトンネリングされます。

（注）　**no ip dhcp client request router** コマンドを使用して DHCP からのデフォルト ルートが無効にされていなければ、デフォルト ルートが 2 つ存在することになるため、通信が失敗します。

例

```
ap1# configure terminal
ap1(config)# interface VDT-Mgmt0
ap1(config-subif)# no ip dhcp client request router
ap1(config-subif)# ip address dhcp
ap1(config-subif)# vdt-mgmt vlan 10
ap1(config)# end
```

SSID とトンネル/Xconnect のマッピング

トンネルを WLAN にマッピングするには、SSID コンフィギュレーションに Xconnect を追加します。

トンネルを VLAN にマッピングするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**dot11 ssid** *ssid*	SSID を指定します。
ステップ 2	**vlan** *vlan id*	VLAN ID を指定します。
ステップ 3	**xconnect** *index of VDT interface*	SSID の L2TPv3 を有効にします。
ステップ 4	**authentication open**	認証のタイプを指定します。

例

```
ap1# configure terminal
ap1(config)# dot11 ssid myssid
ap1(config-ssid)# vlan 10
ap1(config-ssid)# authentication open
ap1(config-ssid)# xconnect 0
ap1(config-ssid)# end
```

TCP MSS 調整の設定

トンネル クライアントの TCP MSS 調整を設定するには、コンフィギュレーション モードで **dot11 l2tp tcp mss** *tcp mss value* コマンドを使用します。

dot11 l2tp tcp mss *tcp mss value*

例

```
ap# configure terminal
ap(config)# dot11 l2tp tcp mss 1360
ap1(config)# end
```

UDP チェックサムの設定

フラグメント化された L2TPv3oUDP データ パケットの UDP チェックサム無視を設定するには、コンフィギュレーション モードで **dot11 l2tpoUdp udp checksum zero** を使用します。

dot11 l2tpoUdp udp checksum zero

（注） このコマンドは、prol2tp サーバが 1.6.1 より前のバージョンである場合に使用します。

例

```
ap# configure terminal
ap(config)# dot11 l2tpoUdp udp checksum zero
ap(config)# end
```

CHAPTER 22

Ethernet over GRE の設定

Ethernet over GRE（EoGRE）は、IP コア ネットワーク上で GRE ヘッダーにカプセル化されたレイヤ 2 パケットのトンネリングを可能にするトンネリング プロトコルです。Generic Routing Encapsulation（GRE）は、レイヤ 3 IPv4 またはレイヤ 3 IPv6 アクセス ネットワーク上で仮想ポイントツーポイント リンクに多種多様なネットワーク レイヤ プロトコルをカプセル化するトンネリング プロトコルです。

前提条件

EoGRE を設定する際の前提条件は次のとおりです。

- IP ルーティングが有効にされている必要があります。IP ルーティングを有効にするためのコマンドは次のとおりです。

  ip routing

- IP CEF が有効にされている必要があります。IP CEF を有効にするためのコマンドは次のとおりです。

  ip cef

- VLAN タグを持つイーサネット フレームをトンネリングする、VLAN のサブインターフェイスを作成する必要があります。VLAN のサブインターフェイスを作成するためのコマンドは次のとおりです。

  interface Dot11Radio *interface number.sub-interface number*

  encapsulation dot1Q *vlan id*

  bridge-group *bridge id*

  interface GigabitEthernet0.*sub-interface number*

  encapsulation dot1Q *vlan id*

  bridge-group *bridge id*

（注） 同じ VLAN ID が設定されたインターフェイスには、同じブリッジ ID を設定する必要があります。

次はサポートされていません。

- SNMP、ACS コンフィギュレーションを使用した GUI
- IPv6 アドレスを使用したトンネルの確立

EoGRE の設定

トンネルのプロファイルを設定して、トンネルを作成するために設定可能なパラメータを定義します。次のパラメータは、dot11 トンネルに設定されます。

- トンネル アドレス モード
- 送信元アドレス
- 宛先アドレス
- 最大セグメント サイズ（MSS）
- 最大伝送ユニット（MTU）
- Type of Service（ToS）または Differentiated Services Code Point（DSCP）

dot11 トンネルのトンネル プロファイルを設定するには、特権 EXEC モードで次の手順に従います。

コマンド	目的
mode [ipv4 | ipv6]	トンネル アドレス モードを IPv4 または IPv6 に設定します。
source *address*	送信元アドレス。デフォルトは AP の BVI アドレスです。
destination *address*	トンネル宛先アドレス
mss *size*	着信/発信 TCP syn および syn/ack パケットの TCP MSS 値を設定します。デフォルトのサイズは 1360 です。
mtu *size*	IP パケットのサイズがこの値より大きい場合、着信 IP パケットはフラグメント化され、ICMP Need Fragmentation エラー メッセージがクライアントに送信されます。デフォルトのサイズは 1400 です。
tos *value*	転送 IP アドレスの ToS または DSCP 値を設定します。デフォルト値は 0 です。

例

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# mode ipv4
ap(config-dot11-tunnel)# destination 1.1.1.1
ap(config-dot11-tunnel)# mss 1360
ap(config-dot11-tunnel)# mtu 1400
ap(config-dot11-tunnel)# tos 5
ap(config-dot11-tunnel)# end
```

SSID のトンネルへのマッピング

トンネルを WLAN にマッピングするには、SSID コンフィギュレーションでコマンド **tunnel** *tunnel_profile* を使用します。

SSID をトンネルにマッピングするには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	**dot11 ssid** *ssid*	SSID を設定します。
ステップ 2	**vlan** *vlan id*	VLAN ID を指定します。
ステップ 3	**tunnel** *tunnel profile*	使用するトンネル プロファイルを指定します。
ステップ 4	**authentication {open | eap }**	認証のタイプを指定します。

例

```
ap(config)# dot11 ssid doc
ap(config-ssid)# tunnel sample
ap(config-ssid)# authentication open
ap(config-ssid)# end
```

EoGRE クライアントの DHCP スヌーピングの設定

DHCP スヌーピングは、信頼できないホストと信頼済み DHCP サーバとの間でファイアウォールのような役割を果たすセキュリティ機能です。AP 上で DHCP スヌーピングを有効にすると、AP は、回線 ID とリモート ID の 2 つのサブオプションを含むリレー エージェント情報オプション（DHCP オプション 82）を挿入します。

（注） DHCP スヌーピングは、デフォルトで無効になっています。

dot11 SSID の EoGRE クライアントの DHCP スヌーピングを有効にするには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	**dhcp-snoop enable**	DHCP スヌーピングを有効にします。 デフォルトでは、DHCP スヌーピングはディセーブルです。
ステップ 2	**dhcp-snoop circuit_id format {ap-mac | client-mac | eth-mac | name | ssid | type | vlan | raw** *word_string***}**	回線 ID として使用する文字列シーケンスの形式を指定します。指定する形式については、「回線 ID およびリモート ID の書式と文字列」（P.22-4）を参照してください。 回線 ID は DHCP パケットに挿入されます。

	コマンド	目的
ステップ 3	**dhcp-snoop circuit_id** *circuit-id-string_sequence*	回線 ID として使用する文字列シーケンスを、設定した形式で指定します。区切り文字を使用して各文字列を区切ります。デフォルトの区切り文字は「;」です。
ステップ 4	**dhcp-snoop remote_id format {ap-mac | client-mac | eth-mac | name | ssid | type | vlan | raw** *word_string***}**	リモート ID として使用する文字列シーケンスの書式を指定する必要があります。指定する値については、「回線 ID およびリモート ID の書式と文字列」（P.22-4）を参照してください。
ステップ 5	**dhcp-snoop remote_id** *remote-id-string_sequence*	リモート ID として使用する文字列シーケンスを、設定した書式で指定する必要があります。区切り文字を使用して各文字列を区切ります。デフォルトの区切り文字は「;」です。

例

```
ap(config)# dot11 ssi
ap(config)# dot11 ssid doc
ap(config-ssid)# dhcp-snoop enable
ap(config-ssid)# dhcp-snoop circuit_id format ap-mac ssid type
ap(config-ssid)# dhcp-snoop circuit_id 00:10:A4:23:B6:C0;xfinityWiFi;s
ap(config-ssid)# dhcp-snoop remote_id format client-mac
ap(config-ssid)# dhcp-snoop remote_id 00:50:24:23:B7:D0
ap(config-ssid)# end
```

その他のコマンド

デフォルトの DHCP スヌーピングのエンコーディングはバイナリです。これを ASCII に設定するには、次のコマンドを使用します。

ap(config-ssid)# **dhcp-snoop encoding ascii**

デフォルトの DHCP スヌーピングの文字列シーケンスの区切り文字は単一の「;」文字です。これを変更するには、次のコマンドを使用します。

ap(config-ssid)# **dhcp-snoop delimiter** *single_character_or_string*

single_character_or_string は、最大 127 文字の長さにできます。

回線 ID およびリモート ID の書式と文字列

回線 ID およびリモート ID に文字列を割り当てる前に、それぞれに文字列シーケンスの書式を指定する必要があります。

書式および文字列には、次の表に記載する 8 つの値のうち、最大 5 つの値を組み合わせることができます。文字列シーケンスを指定する際には、区切り文字で文字列を区切る必要があります。デフォルトの区切り文字は「:」です。

書式	対応する文字列の特性
ap-mac	AP 無線の MAC アドレス
client-mac	クライアント MAC アドレス
eth-mac	AP イーサネット MAC アドレス
name	AP 名
raw *word_string*	任意の文字列。書式コマンドで raw を指定する場合は、入力する文字列も一緒に指定します。
ssid	SSID（Service Set Identifier）
type	SSID の種類。オープン SSID の場合は「o」、セキュア SSID の場合は「s」です。
vlan	VLAN 名

トンネル ゲートウェイ アドレスの冗長性の設定

トンネルの冗長性を設定すると、運用中のゲートウェイ アドレスが失敗または到達不能になった場合、プライマリからセカンダリにスイッチオーバーできるようになります。

冗長性を設定するには、次のパラメータを dot11 トンネルで設定します。

- バックアップ宛先
- バックアップ タイムアウト
- キープアライブ パラメータ

トンネルの冗長アドレスを設定するには、特権 EXEC モードで次の手順に従います。

	コマンド	目的
ステップ 1	**Backup destination** *address*	バックアップの宛先アドレスを指定します。
ステップ 2	**Backup timeout** *seconds*	トンネルをバックアップからプライマリに切り替えるまでの秒数を指定します。
ステップ 3	**Keepalive** *count interval dead-count timeout*	*count* は、各 *interval*（秒数）で送信する ping パケットの数です。 *dead-count* ping が失敗すると、トンネル エンドポイントはデッド状態であるとみなされます。 *timeout* は、AP が pind を送信した後に ping の応答を待機する秒数です。 *count*、*interval*、*dead-count*、*timeout* のデフォルト値は、それぞれ 3、60、3、1 です。

（注）　プライマリからセカンダリ、またはその逆にスイッチオーバーする際は、アソシエートされているクライアントすべてが認証解除され、スイッチオーバー後に再アソシエートされます。
プライマリとセカンダリの両方がダウンすると、トンネルに接続される SSID もダウンします。AP がプライマリ アドレスとセカンダリ アドレスのいずれかに到達可能になると、SSID が有効になり、クライントへの対応を開始します。

例

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# backup destination 2.2.2.2
ap(config-dot11-tunnel)# backup timeout 60
ap(config-dot11-tunnel)# keepalive 3 60 3 3
ap(config-dot11-tunnel)# end
```

CHAPTER 23

システム メッセージ ロギングの設定

この章では、アクセス ポイントにシステム メッセージ ロギングを設定する方法について説明します。

（注） この章で使用されるコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』ガイドを参照してください。

システム メッセージ ロギングの概要

デフォルトでは、アクセス ポイントはシステム メッセージと **debug** 特権 EXEC コマンドからの出力をロギング プロセスに送信します。ロギング プロセスは、ログ メッセージを各宛先（設定に応じて、ロギング バッファ、端末回線、syslog サーバなど）に配信する処理を制御します。ロギング プロセスは、コンソールにもメッセージを送信します。

ロギング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

コンソールと各送信先に表示されるメッセージのタイプを制御する場合、メッセージの重大度レベルを設定できます。ログ メッセージにタイムスタンプを適用したり、syslog 送信元アドレスを設定したりすると、リアルタイムのデバッグと管理を強化できます。

ロギングされたシステム メッセージにアクセスするには、アクセス ポイントのコマンドライン インターフェイス（CLI）を使用するか、適切に設定された syslog サーバに保存します。アクセス ポイントのソフトウェアは、syslog メッセージを内部バッファに保存します。Telnet を通じてアクセス ポイントにアクセスしたり、syslog サーバでログを表示したりすることでシステム メッセージをリモートにモニタできます。

システム メッセージ ロギングの設定

この項では、システム メッセージ ロギングを設定する方法について説明します。内容は次のとおりです。

システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字と 1 つのパーセント記号（%）で構成され、設定されている場合にはその前に、オプションとしてシーケンス番号またはタイムスタンプ情報が付加されます。メッセージは次の形式で表示されます。

seq no:timestamp: %facility-severity-MNEMONIC:description

パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**]、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 23-1 に、Syslog メッセージの要素を示します。

表 23-1　　システム ログ メッセージの要素

要素	説明
seq no:	**service sequence-numbers** グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」(P.23-6)を参照してください。
timestamp のフォーマット： *mm/dd hh:mm:ss* または *hh:mm:ss*（短時間） または *d h*（長時間）	メッセージまたはイベントの日時です。この情報が表示されるのは、グローバル コンフィギュレーション コマンド **service timestamps log [datetime | log]** が設定されている場合だけです。 詳細については、「ログ メッセージのタイムスタンプのイネーブル化とディセーブル化」(P.23-6)を参照してください。
facility	メッセージが参照する機能（SNMP、SYS など）です。ファシリティはハードウェア デバイス、プロトコル、またはシステム ソフトウェアのモジュールである可能性があります。システム メッセージのソースまたは原因を表します。
severity	メッセージの重大度を示す 0 ～ 7 の 1 桁のコードです。重大度の詳細については、表 23-3 (P.23-8)を参照してください。
MNEMONIC	メッセージを一意に示すテキスト ストリングです。
description	レポートされているイベントの詳細を示すテキスト ストリングです。

次の例は、アクセス ポイントの部分的なシステム メッセージを示します。

```
*Mar  1 00:00:29.219: %LINK-6-UPDOWN: Interface GigabitEthernet0, changed state to up
*Mar  1 00:00:29.335: Starting Ethernet promiscuous mode
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
*Apr 13 15:29:28.007: %SYS-5-RESTART: System restarted --
```

システム メッセージ ロギングのデフォルト設定

表 23-2 に、システム メッセージ ロギングのデフォルト設定を示します。

表 23-2　　システム メッセージ ロギングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ロギング	イネーブル
コンソールの重大度	debugging（および数値の低いレベル。表 23-3 (P.23-8) を参照）
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ

表 23-2　システム メッセージ ロギングのデフォルト設定（続き）

機能	デフォルト設定
タイムスタンプ	ディセーブル
同期ロギング	ディセーブル
ロギング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	Local7（表 23-4（P.23-11）を参照）
サーバの重大度	informational（および数値の低いレベル。表 23-3（P.23-8）を参照）

メッセージ ロギングのディセーブル化とイネーブル化

メッセージ ロギングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ロギングをイネーブルにする必要があります。メッセージ ロギングがイネーブルの場合、ログ メッセージはロギング プロセスに送信されます。ロギング プロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

特権 EXEC モードから、次の手順に従ってメッセージ ロギングをディセーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no logging on**	メッセージ ロギングをディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config** または **show logging**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ロギング プロセスを無効にすると、アクセス ポイントの速度が遅くなる場合があります。これはメッセージがコンソールに書き込まれるまで待ってからプロセスで次の動作が行われるためです。ロギング プロセスがディセーブルになると、メッセージは作成されるとすぐにコンソールに表示され、コマンド出力の途中で表示されることが多くなります。

logging synchronous グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。詳細については、「ログ メッセージのタイムスタンプのイネーブル化とディセーブル化」（P.23-6）を参照してください。

メッセージ ロギングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

メッセージ表示宛先デバイスの設定

メッセージ ロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。特権 EXEC モードから、次のコマンドの 1 つ以上を使用してメッセージを受信する場所を指定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging buffered** [*size*] [*level*]	内部バッファへのメッセージを記録します。デフォルトのバッファ サイズは 4096 です。指定できる範囲は 4096 ～ 2147483647 バイトです。レベルには emergencies 0、alerts 1、critical 2、erros 3、warnings 4、notifications 5、informational 6、debugging 7 を指定します。 **（注）** バッファ サイズは大きくしすぎないでください。これは、アクセス ポイントが他の作業の分のメモリを消費してしまうためです。アクセス ポイントのプロセッサの空きメモリを表示する場合は **show memory** 特権 EXEC コマンドを使用します。ただし、この値は使用可能な最大メモリ量です。バッファ サイズをこの数値に設定しないでください。
ステップ 3	**logging** *host*	Syslog サーバ ホストにメッセージを記録します。 *host* には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。 Syslog サーバの設定手順については、「システム ロギング機能の設定」（P.23-10）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**terminal monitor**	現在のセッション中にコンソール以外の端末にメッセージをロギングします。 端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグ メッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

logging buffered グローバル コンフィギュレーション コマンドを実行すると、ログ メッセージが内部バッファにコピーされます。循環バッファであるため、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。最初に表示されるメッセージは、バッファ内で最も古いメッセージです。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。

ログ メッセージのタイムスタンプのイネーブル化とディセーブル化

デフォルトでは、ログ メッセージにはタイムスタンプが設定されていません。

特権 EXEC モードから、次の手順に従ってログ メッセージのタイムスタンプをイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service timestamps log uptime** または **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	ログ タイムスタンプをイネーブルにします。 最初のコマンドにより、ログ メッセージへのタイムスタンプがイネーブルになり、システムがリブートしてからの時間が表示されます。 2 番目のコマンドにより、ログ メッセージへのタイムスタンプがイネーブルになります。選択したオプションに応じて、タイムスタンプに日付、時間（ローカル時間帯を基準、ミリ秒単位）、タイム ゾーン名を指定できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デバッグとログ メッセージの両方に対してタイムスタンプをディセーブルにするには、グローバル コンフィギュレーション コマンド **no service timestamps** を使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
```

ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージが同じタイムスタンプを持つ可能性があるので、シーケンス番号を表示すると確実に 1 つのメッセージを参照できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

特権 EXEC モードから、次の手順に従ってログ メッセージのシーケンス番号をイネーブルにします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**service sequence-numbers**	シーケンス番号をイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

シーケンス番号をディセーブルにするには、**no service sequence-numbers** グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のロギング表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します(表 23-3を参照)。

特権 EXEC モードから、次の手順に従ってメッセージの重大度を定義します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging console** *level*	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します(表 23-3 (P.23-8) を参照)。
ステップ 3	**logging monitor** *level*	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します(表 23-3 (P.23-8) を参照)。
ステップ 4	**logging trap** *level*	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します(表 23-3 (P.23-8) を参照)。 Syslog サーバの設定手順については、「システム ロギング機能の設定」(P.23-10) を参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** または **show logging**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

（注）　*level* を指定すると、この数値以下のレベルのメッセージが出力先に表示されます。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのロギングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 23-3 に *level* キーワードを示します。また、対応する Syslog 定義を、重大度の最も高いものから順に示します。

表 23-3　　メッセージ ロギング level キーワード

level キーワード	レベル	説明	syslog 定義
emergencies	0	システムが不安定	LOG_EMERG
alerts	1	即時処理が必要	LOG_ALERT
critical	2	クリティカルな状態	LOG_CRIT
errors	3	エラー状態	LOG_ERR
warnings	4	警告状態	LOG_WARNING
notifications	5	正常だが注意を要する状態	LOG_NOTICE
informational	6	情報メッセージだけ	LOG_INFO
debugging	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ～ **emergencies** の重大度で表示されます。これらのタイプのメッセージは、アクセス ポイントの機能に影響することを意味しています。
- **debug** コマンドの出力：**debugging** の重大度で表示されます。
- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは情報専用です。アクセス ポイントの機能には影響しません。
- リロード要求と低プロセス スタック メッセージ：**informational** の重大度で表示されます。このメッセージは情報専用です。アクセス ポイントの機能には影響しません。

（注）　認証要求ログ メッセージは syslog サーバにロギングされません。この機能は Cisco Aironet アクセス ポイントでサポートされません。

履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

グローバル コンフィギュレーション コマンド **snmp-server enable trap** を使用して、syslog メッセージ トラップを SNMP ネットワーク管理ステーションへ送信するように設定している場合は、アクセス ポイント履歴テーブルに送信されて保存されるメッセージのレベルを変更できます。また履歴テーブルに保存されるメッセージ数も変更できます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、Syslog トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ（表 23-3（P.23-8）を参照）が、履歴テーブルに 1 つ格納されます。

特権 EXEC モードから、次の手順に従ってレベルと履歴テーブルのサイズのデフォルトを変更します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging history** *level*[1]	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。 *level* キーワードのリストについては、表 23-3（P.23-8）を参照してください。 デフォルトでは、**warnings**、**errors**、**critical**、**alerts**、および **emergencies** のメッセージが送信されます。
ステップ 3	**logging history size** *number*	履歴テーブルに格納できる Syslog メッセージ数を指定します。 デフォルトでは 1 つのメッセージが格納されます。指定範囲は 1 ～ 500 メッセージです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

1. 表 23-3 に、level キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、emergencies は 0 ではなく 1 に、critical は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合）は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのロギングをデフォルトの重大度に戻すには、**no logging history** グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、**no logging history size** グローバル コンフィギュレーション コマンドを使用します。

ロギング レート制限の設定

アクセス ポイントが 1 秒あたりにロギングするメッセージ数への制限を有効にできます。すべてのメッセージ、またはコンソールに送信されるメッセージに対して制限を有効にできます。また特定の重大度のメッセージを制限から除外することを指定できます。

特権 EXEC モードから、次の手順に従ってロギング レート制限を有効にします。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging rate-limit** *seconds* [**all** | **console**] [**except** *severity*]	ロギング レート制限を秒単位で有効にします。 • (任意)すべてのロギング、またはコンソールにロギングされるメッセージにのみ制限を適用します。 • (任意)特定の重大度を制限から除外します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

レート制限を無効にするには、グローバル コンフィギュレーション コマンド **no logging rate-limit** を使用します。

システム ロギング機能の設定

外部デバイスにシステム ログ メッセージを送信する場合は、メッセージを syslog 機能のいずれかから発信されたものとして特定するようにアクセス ポイントを設定できます。

特権 EXEC モードから、次の手順に従ってシステム機能メッセージ ロギングを設定します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**logging** *host*	ホストの IP アドレスを入力して、syslog サーバ ホストにメッセージを記録します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
ステップ 3	**logging trap** *level*	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれより下のレベルのメッセージを受信します。*level* キーワードについては、表 23-3 (P.23-8) を参照してください。
ステップ 4	**logging facility** *facility-type*	Syslog 機能を設定します。*facility-type* キーワードについては、表 23-4 (P.23-11) を参照してください。 デフォルトは **local7** です。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	(任意)コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、**no logging** *host* グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのロギングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを入力します。

表 23-4 に、Cisco IOS ソフトウェアでサポートされているシステム機能を示します。これらの機能に関する詳細情報については、ご使用の Syslog サーバのオペレータ マニュアルを参照してください。

表 23-4　ロギング facility-type キーワード

ファシリティ タイプのキーワード	説明
auth	許可システム
cron	cron 機能
daemon	システム デーモン
kern	カーネル
local0 ～ local7	ローカルに定義されたメッセージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9	システムで使用
sys10	システムで使用
sys11	システムで使用
sys12	システムで使用
sys13	システムで使用
sys14	システムで使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX から UNIX へのコピー システム

ロギング設定の表示

現在のロギング設定とログ バッファの内容を表示する場合は、**show logging** 特権 EXEC コマンドを使用します。ここで示す各フィールドについては、『*Cisco IOS Configuration Fundamentals Command Reference* 』ガイドを参照してください。

ロギング履歴ファイルを表示するには、**show logging history** 特権 EXEC コマンドを使用します。

トラブルシューティング

この章では、ワイヤレス デバイスに発生する可能性のある基本的な問題に対するトラブルシューティングの手順を説明します。トラブルシューティングの最新の詳細情報は、次の URL で、シスコの TAC Web サイト（[Top Issues]、[Wireless Technologies] の順に選択）を参照してください。

http://www.cisco.com/tac

LED インジケータ

使用しているワイヤレス デバイスが通信していない場合は、まずデバイスの LED インジケータを確認して、そのデバイスのステータスを評価します。

LED インジケータの設定は、すべての Cisco Aironet シリーズのアクセス ポイントで同じであるわけではありません。シリーズによって、アクセス ポイントには、1 つのステータス LED インジケータ、または 3 種類のインジケータ（イーサネット LED、ステータス LED、および無線 LED ）があります。LED インジケータの設定情報については、ご使用のアクセス ポイントの *スタートアップ ガイド*、または *ハードウェア設置ガイド*（屋外アクセス ポイント向け）を参照してください。

（注） LED の色の強さや見え方は、装置によって多少異なります。これは想定どおりのことであり、LED メーカーの仕様の正常範囲内であって、不具合ではありません。

電力チェック

パワー インジェクタの LED インジケータをチェックして、アクセス ポイント/ブリッジへの給電を確認できます。

- 緑色は、入力パワーがブリッジに給電されていることを示します。
- 赤色は、過電流または過電圧エラー状況を示します。パワー インジェクタの電源を抜いて、すべての同軸ケーブルで短絡がないことをチェックし、約 1 分間待機してから入力電源をパワー インジェクタに差し込み直します。これで再度 LED が赤色に変わった場合は、テクニカル サポートにお問い合わせください。

  （注） パワー インジェクタが過電流または過電圧状況から回復するには、約 50 秒かかります。

LED がオフの場合は入力パワーが利用できないことを示します。電源モジュールがパワー インジェクタに接続されていること、および AC 電力が使用可能であること、または 12 ～ 40VDC 入力パワーがパワー インジェクタに接続されていることを確認してください。

低電力状態

アクセス ポイントには、48VDC 電源モジュールまたはインライン電源から給電できます。

フル動作には、1040、1140、1260、および 700W シリーズのアクセス ポイントに 12.95 W の電力が必要です。電源モジュールおよび Cisco Aironet パワー インジェクタは、フル動作に必要な電力を給電できますが、インライン電源によっては 12.95 W を給電できないものもあります。また、一部の大電力インライン電源では、すべてのポートに同時に 12.95 W の電力を供給できない場合もあります。

2600、3600、2700、および 3700 シリーズのアクセス ポイントには 18.5 ワットが必要なことから、802.3at または PoE+ が必要です。ただし、各無線モジュールの無線チェーンのいずれかを無効にすることで、これらのアクセス ポイントは 802.3af 電源でも機能します。

（注）　802.3af 準拠スイッチ（シスコ製またはシスコ以外の製品）では、フル動作に十分な電力を供給できます。

（注）　AP2700 または AP3700 が PoE 802.3af 電源を使用して低電力モードで動作しているときには、無線のいずれか 1 つがシャットダウンされます。無線をシャットダウンして節約された分の電力は、動作中の無線に使用されます。その際に、その無線はリセットされます。リセット中は、アソシエートされている WLAN クライアントとの通信が中断されます。リセットされた無線がオンラインに戻ると、WLAN クライアントがその無線に再アソシエートされます。

電源投入時にアクセス ポイントは低電力モードになり（両方の無線が無効になります）、Cisco IOS ソフトウェアがロードされて実行され、電力ネゴシエーションによって十分な電力が利用できるかどうかが判定されます。十分な電力がある場合は、無線がオンになります。それ以外の場合は、過電流状態が発生しないように、アクセス ポイントは無線が無効の状態で低電力モードに保持されます。低電力モードでは、アクセス ポイントのステータス LED の低電力エラー表示が有効化され、ブラウザおよびシリアル インターフェイスに低電力メッセージが表示され、イベント ログ入力が作成されます。

基本設定の確認

無線クライアントとの接続が失われる最も一般的な原因は、基本設定の不一致です。ワイヤレス デバイスでクライアント デバイスとの通信が行われない場合は、この項に記載された項目を確認します。

SSID

ワイヤレス デバイスにアソシエートしようとする無線クライアントは、ワイヤレス デバイスと同じ SSID を使用する必要があります。クライアント デバイスの SSID が無線範囲のワイヤレス デバイスの SSID と一致しない場合、クライアント デバイスはアソシエートしません。

WEP キー

データ送信に使用する WEP キーは、ワイヤレス デバイス、およびにアソシエートするすべての無線デバイスでまったく同じように設定する必要があります。たとえば、クライアント アダプタの WEP Key 3 を 0987654321 に設定し、送信キーとして選択した場合、ワイヤレス デバイスの WEP Key 3 もまったく同じ値に設定する必要があります。ただし、ワイヤレス デバイスでは、Key 3 を送信キーとして使用する必要はありません。

無線デバイスの WEP キーの設定方法については、第 10 章「WLAN 認証および暗号化の設定」を参照してください。

セキュリティ設定

ワイヤレス デバイスによる認証を求める無線クライアントは、そのワイヤレス デバイスで設定されているのと同じセキュリティ オプションをサポートする必要があります。たとえば、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）または Light Extensible Authentication Protocol（LEAP;拡張認証プロトコル）、MAC アドレス認証、Message Integrity Check（MIC; メッセージ完全性チェック）、WEP キー ハッシュ、および 802.1X プロトコル バージョンなどです。

無線クライアントが EAP-FAST 認証を使用している場合は、Open 認証 + EAP を設定する必要があります。Open 認証 + EAP を設定しないと、警告メッセージが表示されます。CLI を使用している場合は、次の警告メッセージが表示されます。

「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

GUI を使用している場合は、次の警告メッセージが表示されます。

「WARNING:
「Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」

無線クライアントがワイヤレス デバイスから認証されない場合には、クライアント アダプタの適切なセキュリティ設定、および現在のワイヤレス デバイスの設定で使用可能なクライアントのアダプタ ドライバおよびファームウェアのバージョンをシステム管理者に問い合わせてください。

デフォルト設定へのリセット

ワイヤレス デバイスの設定に必要なパスワードを忘れてしまった場合は、設定を完全にリセットする必要があることもあります。すべてのアクセス ポイントでは、アクセス ポイントの MODE ボタン、または Web ブラウザ インターフェイスを使用できます。350 シリーズのアクセス ポイントでは、Web ブラウザ インターフェイスまたは CLI を使用します。

（注）　次の手順では、パスワード、WEP キー、IP アドレス、SSID などの *すべての*設定をデフォルトにリセットします。デフォルトのユーザ名とパスワードは両方とも **Cisco** で、大文字と小文字が区別されます。

MODE ボタンの使用

次の手順に従って現在の設定を削除し、MODE ボタンを使用してアクセス ポイントのすべての設定をデフォルトに戻します。

（注）　設定をデフォルトにリセットするには、MODE ボタンを使用する代わりに「Web ブラウザ インターフェイスの使用方法」（P.24-5）の手順または「CLI の使用」（P.24-6）の手順に従います。
350 シリーズのアクセス ポイントでは、MODE ボタンを使用して設定をデフォルトにリセットすることはできません。

ステップ 1　アクセス ポイントの電源(外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル)を切ります。

ステップ 2　MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。

ステップ 3　ステータス LED が青に変わるまで、MODE ボタンを押し続けます。

ステップ 4　アクセス ポイントをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、アクセス ポイントを再設定する必要があります。

（注）　アクセス ポイントは、IP アドレスも含めてデフォルト値に設定されます(DHCP を使用して IP アドレスを受信するように設定されます)。デフォルトのユーザ名とパスワードは **Cisco** で、大文字と小文字が区別されます。

Web ブラウザ インターフェイスの使用方法

Web ブラウザ インターフェイスを使用して、現在の設定を削除してワイヤレス デバイスのすべての設定をデフォルトに戻す手順は、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。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

ステップ 3　[Username] フィールドにユーザ名を入力します。

ステップ 4　[Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。

ステップ 5　[Software] をクリックして [System Software] 画面を表示します。

ステップ 6　[System Configuration] をクリックして、[System Configuration] 画面を表示します。

ステップ 7　[Reset to Defaults] または [Reset to Defaults (Except IP)] ボタンをクリックします。

（注）　静的 IP アドレスを保持する場合は、[Reset to Defaults (Except IP)] を選択します。

ステップ 8　[Restart] をクリックします。システムがリブートします。

ステップ 9　ワイヤレス デバイスをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、ワイヤレス デバイスを再設定する必要があります。デフォルトのユーザ名とパスワードは **Cisco** で、大文字と小文字が区別されます。

CLI の使用

CLI を使用して、現在の設定を削除してワイヤレス デバイスのすべての設定をデフォルトに戻す手順は、次のとおりです。

ステップ 1　Telnet セッションまたはワイヤレス デバイス コンソール ポートへの接続を使用して、CLI を開きます。

ステップ 2　電源を切って再度電源を入れ、ワイヤレス デバイスをリブートします。

ステップ 3　コマンド プロンプトが表示され、ワイヤレス デバイスによってイメージの拡大が開始されるまで、ワイヤレス デバイスのブートを続けます。CLI に次の行が表示されたら、Esc を押します。

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

ステップ 4　ap: プロンプトに対して **flash_init** コマンドを入力し、フラッシュを初期化します。

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

ステップ 5　**dir flash:** コマンドを使用して、フラッシュのコンテンツを表示させ、コンフィギュレーション ファイル config.txt を検索します。

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

ステップ 6　**rename** コマンドを使用して、config.txt ファイルの名前を config.old に変更します。

```
ap: rename flash:config.txt flash:config.old
```

ステップ 7　**reset** コマンドを入力してワイヤレス デバイスをリブートします。

```
ap: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
    using  eeprom values
WRDTR,CLKTR: 0x80000800 0x80000000
RQDC ,RFDC : 0x80000033 0x000001cb
    ddr init done
IOS Bootloader - Starting system.
Xmodem file system is available.
DDR values used from system serial eeprom.
WRDTR,CLKTR: 0x80000800, 0x80000000
RQDC, RFDC : 0x80000033, 0x000001cb
```

ステップ 8　アクセス ポイントでソフトウェアのリブートが終了したら、アクセス ポイントに対して新しい Telnet セッションを開始します。

（注）　ワイヤレス デバイスは、IP アドレス（DHCP を使用して IP アドレスを受信するように設定）およびデフォルトのユーザ名とパスワード（**Cisco**）の設定など、デフォルト値に設定されています。

ステップ 9　IOS ソフトウェアがロードされると、特権 EXEC コマンド **del** を使用してフラッシュから config.old ファイルを削除できます。

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

アクセス ポイントのイメージのリロード

ワイヤレス デバイスでファームウェアの障害が発生した場合は、Web ブラウザ インターフェイスを使用してイメージ ファイルをリロードする必要があります。または、すべてのアクセス ポイントで MODE ボタンを約 30 秒押し続けます。ワイヤレス デバイスのファームウェアが完全に動作している間に、ファームウェア イメージをアップグレードする場合、ブラウザ インターフェイスを使用します。ただし、アクセス ポイントのファームウェア イメージが壊れている場合は MODE ボタンを使用します。

MODE ボタンの使用

すべてのアクセス ポイントでは、MODE ボタンを使用して、ネットワーク上またはアクセス ポイントのイーサネット ポートに接続された PC 上のアクティブな Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバから、アクセス ポイントのイメージ ファイルをリロードできます。

ワイヤレス デバイスの 3 つの LED インジケータが赤色になり、ファームウェア障害、またはファームウェア イメージの破壊が発生した場合、接続した TFTP サーバからイメージをリロードする必要があります。

（注）　その結果、パスワード、セキュリティ設定、ワイヤレス デバイスの IP アドレス、SSID を含むすべての設定がデフォルトにリセットされます。

アクセス ポイントのイメージ ファイルをリロードする手順は、次のとおりです。

ステップ 1　使用する PC は、静的 IP アドレスが 10.0.0.2 ～ 10.0.0.30 の範囲で設定されている必要があります。

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（たとえば、*ap3g2-k9w7-tar.152-4.JB5.tar* など）が格納されていること、および TFTP サーバがアクティブになっていることを確認します。詳細については、「アクセス ポイントのイメージ ファイルの入手」および「TFTP サーバ ソフトウェアの入手」の各項を参照してください。

ステップ 3　TFTP サーバ フォルダのアクセス ポイント イメージ ファイルの名前を変更します。たとえば、イメージ ファイルの名前が **ap3g2-k9w7-tar.152-4.JB5.tar** の場合、ファイル名を **ap3g2-k9w7-tar.default** に変更します。

ステップ 4　Category 5（CAT 5; カテゴリ 5）のイーサネット 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（外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル）を切ります。

ステップ 6　MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。

ステップ 7　MODE ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ～ 30 秒かかります）、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してすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9　アクセス ポイントをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、アクセス ポイントを再設定する必要があります。

Web ブラウザ インターフェイスの使用方法

ワイヤレス デバイスのイメージ ファイルをリロードするには、Web ブラウザ インターフェイスも使用できます。Web ブラウザ インターフェイスでは、HTTP または TFTP インターフェイスを使用したイメージ ファイルのロードがサポートされています。

（注）　ブラウザを使用してイメージ ファイルをリロードする場合、ワイヤレス デバイスの設定は変更されません。

ブラウザ HTTP インターフェイス

HTTP インターフェイスを使用すると、PC にあるワイヤレス デバイスのイメージ ファイルを参照し、ワイヤレス デバイスにイメージをダウンロードできます。HTTP インターフェイスを使用する手順は、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。Microsoft Internet Explorer または Netscape Navigator（バージョン 7.x）を使用する必要があります。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

ステップ 3　[Username] フィールドにユーザ名を入力します。

ステップ 4　[Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。

ステップ 5　[Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。

ステップ 6　[Browse] をクリックして PC 内のイメージ ファイルを検索します。

ステップ 7　[Upload] をクリックします。

詳細は、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。

ブラウザ TFTP インターフェイス

TFTP インターフェイスを使用すると、ネットワーク デバイスの TFTP サーバを使用してワイヤレス デバイスのイメージ ファイルをロードできます。TFTP サーバを使用する手順は、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。

ステップ 2　ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

ステップ 3　[Username] フィールドにユーザ名を入力します。

ステップ 4　[Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。

ステップ 5　[Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。

ステップ 6　[TFTP Upgrade] タブをクリックします。

ステップ 7　[TFTP Server] 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 8　[Upload New System Image Tar File] フィールドに、イメージ ファイル名を入力します。TFTP サーバのルート ディレクトリ下のサブディレクトリ内にファイルがある場合は、TFTP サーバのルート ディレクトリに対する相対パスとファイル名を指定します。ファイルが TFTP サーバのルート ディレクトリにある場合は、ファイル名だけを入力します。

ステップ 9　[Upload] をクリックします。

詳細については、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。

CLI の使用

CLI を使用してワイヤレス デバイスのイメージをリロードする手順は、次のとおりです。ワイヤレス デバイスがブートを開始したら、ブート プロセスを中断させ、ブートローダ コマンドを使用して TFTP サーバからイメージをロードして、ワイヤレス デバイス内のイメージを置き換えます。

（注）　CLI を使用してイメージ ファイルをリロードする場合、ワイヤレス デバイスの設定は変更されません。

ステップ 1　ワイヤレス デバイス コンソール ポートへの接続を使用して、CLI を開きます。

ステップ 2　電源を切って再度電源を入れ、ワイヤレス デバイスをリブートします。

ステップ 3　イメージの拡大が開始されるまで、ワイヤレス デバイスのブートを続けます。CLI に次の行が表示されたら、Esc を押します。

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...################################################################################
################################################################################
################################################################################
####################
```

ステップ 4　ap: コマンド プロンプトが表示されたら、**set** コマンドを入力して、ワイヤレス デバイスに IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを割り当てます。

（注）　**set** コマンドを使用して **IP-ADDR**、**NETMASK**、および **DEFAULT_ROUTER** オプションを入力する場合は、大文字を使用する必要があります。

たとえば、次のように入力します。

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

ステップ 5　**tftp_init** コマンドを入力して、ワイヤレス デバイスを TFTP 用に準備します。

```
ap: tftp_init
```

ステップ 6　**tar** コマンドを入力して、TFTP サーバから新しいイメージをロードおよび拡大します。このコマンドには次の情報を含む必要があります。

- **-xtract** オプション。ロード時にイメージを拡大します。
- TFTP サーバの IP アドレス。
- イメージが格納されている TFTP サーバのディレクトリ。
- イメージの名前。
- イメージの保存先（ワイヤレス デバイスのフラッシュ）。

たとえば、次のように入力します。

```
ap: tar -xtract tftp://192.168.130.222/images/ap3g2-k9w7-tar.152-4.JB5.tar flash
```

ステップ 7　画面の一番下まで出力が表示され、CLI がポーズして --MORE-- と表示されたら、スペースバーを押して続けます。

```
extracting info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/popup_capabilitycodes.shtml.gz (1020 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter.js.gz (1862 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_vlan.js.gz (1459 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_mac_ether.js.gz (1793 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/security.js.gz (962 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/vlan.js.gz (1121 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ssid.js.gz (4286 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/network-if.js.gz (2084 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/dot1x.js.gz (988 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stp.js.gz (957 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_assoc.shtml.gz (5653 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_event-log.shtml.gz (3907 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_home.shtml.gz (7071 bytes)
```

```
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-if.shtml.gz (3565 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-map.shtml.gz (3880 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_services.shtml.gz (3697 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_system-sw.shtml.gz (2888 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_contextmgr.shtml.gz (3834 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ap_title_appname.gif (2092 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/2600_title_appname.gif (2100 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button.gif (1211 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_1st.gif (1171 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_cbottom.gif (318 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_current.gif (1206 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_endcap.gif (878 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_encap_last.gif (333 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_last.gif (386 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_nth.gif (1177 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_dkgreen.gif (869 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_green.gif (879 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_upright.gif (64 bytes)
.../...
```

ステップ 8　**set BOOT** コマンドを入力して、ワイヤレス デバイスがリブートするときに使用するイメージに新しいイメージを指定します。ワイヤレス デバイスによって、イメージと同じ名前のイメージ用ディレクトリが作成されます。このディレクトリをコマンドに含める必要があります。たとえば、次のように入力します。

```
ap: set BOOT flash:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
```

ステップ 9　**set** コマンドを入力して、ブートローダのエントリを確認します。

```
ap: set
BOOT=flash:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

ステップ 10　**boot** コマンドを入力して、ワイヤレス デバイスをリブートします。ワイヤレス デバイスがリブートすると、新しいイメージがロードされます。

```
ap: boot
```

アクセス ポイントのイメージ ファイルの入手

ワイヤレス デバイスのイメージ ファイルは、次の手順に従って Cisco.com から入手できます。

ステップ 1　インターネット ブラウザを使用して、次の URL にあるワイヤレス製品のソフトウェア ダウンロード ページにアクセスします。

http://software.cisco.com/download/navigator.html?mdfid=278875243&i=!h

ステップ 2　Cisco.com サイトにログインします。
ページの右上にある [Log In] をクリックし、CCO ログイン ユーザ名とパスワードを入力します。

ステップ 3　[Select a Product] 領域の右端の列で [Access Points] をクリックします。

ステップ 4　適切なアクセス ポイントをクリックします。

ステップ 5　適切なアクセス ポイント バージョンをクリックします。

ステップ 6　[Autonomous API IOS Software] をクリックします。
利用できるソフトウェア バージョンのリストが表示されます。

ステップ 7　ダウンロードするバージョンを選択します。
選択したバージョンのダウンロード ページが表示されます。

ステップ 8　[Download] をクリックします。[Software Download Rules] ページが表示されます。

ステップ 9　[Software Download Rules] をよく読んで、[Agree] をクリックします。

ステップ 10　お使いのハード ドライブにファイルを保存します。

TFTP サーバ ソフトウェアの入手

TFTP サーバ ソフトウェアは、いくつかの Web サイトからダウンロードできます。次の URL から入手できるシェアウェアの TFTP ユーティリティを推奨します。

http://tftpd32.jounin.net

ユーティリティのインストール方法と使用方法については、Web サイトの指示に従ってください。

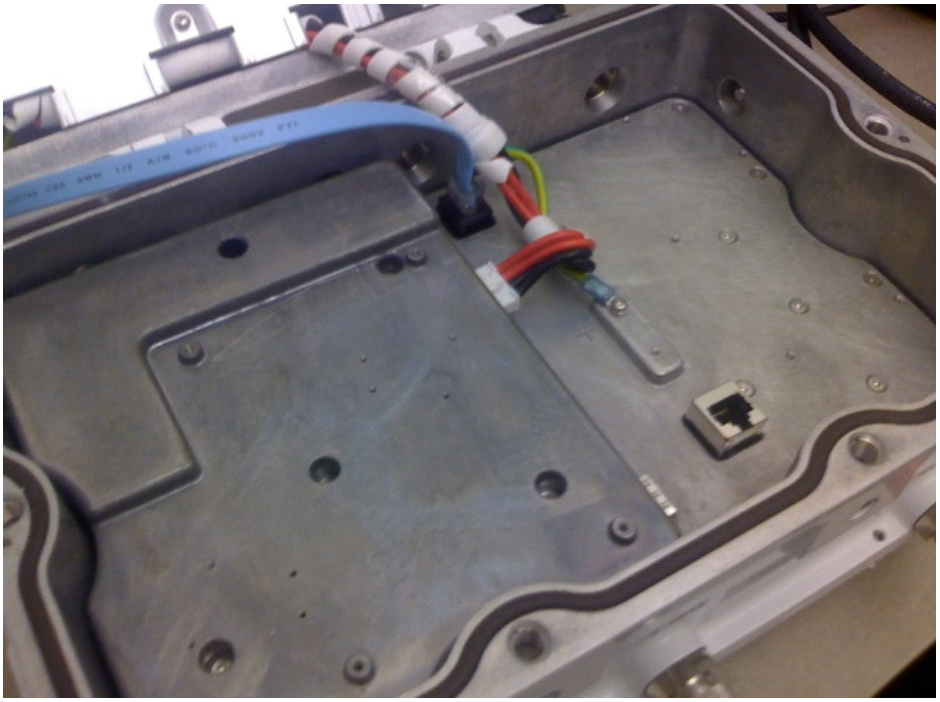
1520 アクセス ポイントでのイメージの復元

1520 アクセス ポイントでイメージを復元するプロセスは、コンソール ポートを持つ IOS アクセス ポイントでのプロセスと同様です。

1520 アクセス ポイントでイメージの復元を実行するには、次の手順に従います。

ステップ 1　アクセス ポイントの電源をオフにした状態で、RJ45 コンソール ケーブルをコンソール ポートに接続します。コンソール ポートは、ユニット内部にある黒いプラスティック製の RJ45 ジャックです。

図 24-1　　コンソール ポートへの RJ45 コンソール ケーブルの接続



ステップ 2　8 データビット、パリティなし、フロー制御なし、9600 bps に対応するようにターミナル エミュレータを設定します。

ステップ 3　アクセス ポイントに電力を供給します。

ステップ 4　ブートローダに「Base Ethernet MAC Address」と表示されたら、Esc キーを押して **ap:** プロンプトを開始します。

```
IOS Bootloader - Starting system.
Xmodem file system is available.
flashfs[0]: 13 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31868928
flashfs[0]: Bytes used: 9721344
flashfs[0]: Bytes available: 22147584
flashfs[0]: flashfs fsck took 20 seconds.
Reading cookie from flash parameter block...done.
Base Ethernet MAC address: 00:1f:27:75:db:00

The system boot has been aborted.The following
commands will finish loading the operating system
software:
    ether_init
    tftp_init
    boot
ap:
```

（注）　**ENABLE_BREAK=no environmental** 変数が設定されている場合、ブートローダにエスケープできません。

ステップ 5　1520 アクセス ポイントの LAN ポート（「PoE In」）と TFTP サーバをケーブルで接続します。たとえば、tftpd32 がインストールされた Windows PC に接続します。

ステップ 6　k9w7 IOS イメージの正常なコピーを TFTP サーバにインストールします。

ステップ 7　静的 IP アドレスで、TFTP サーバの LAN インターフェイスを設定します。たとえば、10.1.1.1 と指定します。

ステップ 8　アクセス ポイントで、次のように入力します。

```
ap: dir flash:
```

新しいコードを保持するのに十分な空きスペースがフラッシュに存在すること（またはフラッシュ ファイル システムが破損しているかどうか）を確認して、次のように入力します。

```
ap: format flash:
```

ステップ 9　TFTP を使用して 1520 アクセス ポイントのフラッシュにイメージをコピーします。

その他の AP 固有の設定

この章では、特定のアクセス ポイントに固有のその他の設定について説明します。

Cisco Aironet 700W シリーズ

700W AP での LAN ポートの使用

Cisco Aironet 700W シリーズのアクセス ポイントには、1 つの 10/100/1000BASE-T PoE アップリンク/WAN ポートと、ワイヤレス デバイスを接続するための 4 つの 10/100/1000BASE-T RJ-45 ローカル イーサネット ポートがあります。4 つのポートは、802.3at イーサネット スイッチ、シスコ パワー インジェクタ AIR-PWRJ4=、またはシスコ電源によって AP に電力が供給されると PoE 出力ポートをとして機能します。

デフォルトでは、4 つのローカル イーサネット ポートはすべて無効です。必要に応じて有効にすることができます。

また、インターフェイス コンフィギュレーション コマンド **vlan** *vlan ID* を使用して、ローカル イーサネット ポートを VLAN ID に設定することもできます。

702W 上の LAN ポートの有効化

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
ap#conf t
Enter configuration commands, one per line.End with CNTL/Z.
```

ステップ 2 LAN ポートを有効にします。

```
ap(config)#lan-Port port-id 1
ap(config-lan-port)#no shutdown
ap(config-lan-port)#end
```

LAN ポートへの VLAN の割り当て

次の例に記載するコマンドを使用します。

```
ap#conf t
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#lan-Port port-id 1
ap(config-lan-port)#vlan 25
ap(config-lan-port)#end
```

LAN ポート設定の確認

次の例に記載するコマンドを使用します。

```
voip#sh lan  config

LAN table entries:

Port    Status       Vlan valid    Vlan Id
  ----    ---------    ----------    -------
  LAN1    DISABLED     25            NA
  LAN2    ENABLED      NO            NA
  LAN3    DISABLED     NO            NA
  LAN4    ENABLED      NO            NA
LAN POE out state = ENABLED
```

ワークグループ ブリッジとしての 700W AP

他のシスコ アクセス ポイントと同じように、702W AP シリーズをワークグループ ブリッジ（WGB）として設定できます。

WGB により、イーサネット対応デバイスの無線インフラストラクチャ接続を実現できます。無線ネットワークに接続するための無線クライアント アダプタを備えていないデバイスは、イーサネット ポート経由で WGB に接続できます。

WGB は、無線 LAN（WLAN）に対して最大 20 台のイーサネット対応デバイスをサポートします。WGB は無線インターフェイスを介してルート AP にアソシエートします。このようにして、有線クライアントが無線ネットワークへのアクセスを取得します。WGB は次のものにアソシエートできます。

- AP
- ルート ブリッジ（AP モード）
- コントローラ（軽量 AP を使用）

Cisco 702W アクセス ポイントが WGB として機能する場合、WGB の背後にある有線イーサネット クライアントを 702W AP 上の LAN または WAN ポートに接続できます。

プロトコル フィルタ

この付録の表では、アクセス ポイントでフィルタの可能なプロトコルを示します。いずれの表でも、「プロトコル」の列にプロトコル名、「別の識別名」の列にプロトコルの別名、「ISO 識別番号」の列にプロトコルの ISO 識別番号を示します。

表 A-1　　Ethertype プロトコル

プロトコル	別の識別名	ISO 識別番号
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX（旧）	—	0x8137
Novell IPX（新）	IPX	0x8138
EAPOL（旧）	—	0x8180
EAPOL（新）	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

表 A-2　　IP プロトコル

プロトコル	別の識別名	ISO 識別番号
dummy	—	0
インターネット制御メッセージ プロトコル(ICMP)	ICMP	1
Internet Group Management Protocol (インターネット グループ管理プロトコル)	IGMP	2
伝送制御プロトコル(TCP)	TCP	6
エクステリア ゲートウェイ プロトコル	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
カプセル化ヘッダー	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

表 A-3　　IP ポート プロトコル

プロトコル	別の識別名	ISO 識別番号
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
シンプル メール転送プロトコル	SMTP mail	25
time	timserver	37
リソース ロケーション プロトコル	RLP	39
IEN 116 Name Server	name	42
whois	nicname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101

表 A-3　　IP ポート プロトコル（続き）

プロトコル	別の識別名	ISO 識別番号
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
ネットワーク タイム プロトコル	ntp	123
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
簡易ネットワーク管理プロトコル	SNMP	161
SNMP トラップ	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
ボーダー ゲートウェイ プロトコル	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201

表 A-3　　IP ポート プロトコル（続き）

プロトコル	別の識別名	ISO 識別番号
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
ルート	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-priveleged	prospero-np	1525
RADIUS	—	1812
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002

サポート対象 MIB

この付録では、アクセス ポイントがこのソフトウェア リリースでサポートする簡易ネットワーク管理プロトコル（SNMP）管理情報ベース（MIB）を示します。Cisco IOS SNMP エージェントは、SNMPv1、SNMPv2、および SNMPv3 をサポートします。

MIB の一覧

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-LBS-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB

- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- CISCO-WDS-INFO-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

FTP による MIB ファイルへのアクセス

FTP を使用して各 MIB ファイルを取得する手順は、次のとおりです。

ステップ 1　FTP を使用してサーバ **ftp.cisco.com** にアクセスします。

ステップ 2　ユーザ名 **anonymous** を使用してログインします。

ステップ 3　パスワードが要求されたら、E メールのユーザ名を入力します。

ステップ 4　`ftp>` プロンプトで、ディレクトリを **/pub/mibs/v1** または **/pub/mibs/v2** に変更します。

ステップ 5　**get** *MIB_filename* コマンドを使用して、MIB ファイルのコピーを入手します。

（注）　シスコの Web サイトでも、MIB に関する情報にアクセスできます。
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

エラー メッセージおよびイベント メッセージ

この付録では、CLI のエラー メッセージおよびイベント メッセージの一覧を示します。

表記法

システム エラー メッセージは、表 C-1 に示す形式で表示されます。

表 C-1　　システム エラー メッセージの形式

メッセージのコンポーネント	説明	例
エラー ID	エラーをカテゴリ分けするストリング。	STATION-ROLE
ソフトウェア コンポーネント	エラーのソフトウェア コンポーネントを識別するためのストリング。	AUTO_INSTALL
重大度	エラーの重大度を示す数値ストリング。	0-LOG-EMERG：緊急事態。何も機能していない 1-LOG-ALERT：ユーザに非常に深刻な問題であることを知らせる 2-LOG-CRIT：深刻で重大なエラーの可能性を警告する 3-LOG-ERR：エラー状態の警告。大半の機能は正常に動作しているが、ユーザは注意を払うべきである 4-LOG-WARNING：必要であれば、無視してもよい警告 5-LOG-NOTICE：ユーザの懸念事項になる可能性のある通告 6-LOG-INFO：情報（深刻ではない） 7-LOG-DEBUG：デバッグ情報（深刻ではない）
動作フラグ	追加処理の表示対象であるコードが内部的に使用。	0：アクション不要を示すフラグ MSG-TRACEBACK：メッセージにトレースバックを含める MSG-PROCESS：メッセージにプロセス情報を含める MSG-CLEAR：問題のある状態が解消されたことを示す MSG-SECURITY：セキュリティ メッセージとして表示する MSG-NOSCAN：EEM パターン スクリーニングを抑制する
%d	整数値。	2450
%e	MAC アドレス。	000b.fcff.b04e
%s	エラーの詳細を示すメッセージ ストリング。	「Attempt to protect port 1640 failed.」
%x	16 進数値。	0x001

ソフトウェア自動アップグレード メッセージ

エラー メッセージ　SW-AUTO-UPGRADE-2-FATAL_FAILURE: Attempt to upgrade software failed, software on flash may be deleted.Please copy software into flash.

説明　ソフトウェアの自動アップグレードに失敗しました。フラッシュのソフトウェアが削除されている可能性があります。ソフトウェアをフラッシュにコピーしてください。

推奨処置　ソフトウェアをコピーしてから装置をリブートしてください。

エラー メッセージ　SW-AUTO-UPGRADE-7-DHCP_CLIENT_FAILURE: “%s”: Auto upgrade of the software failed.

説明　ソフトウェアの自動アップグレードに失敗しました。

推奨処置　Dynamic Host Configuration Protocol（DHCP）クライアントが実行されていることを確認してください。

エラー メッセージ　SW-AUTO-UPGRADE-7-DHCP_SERVER_FAILURE:「“%s”: Auto upgrade of the software failed.」

説明　ソフトウェアの自動アップグレードに失敗しました。

推奨処置　DHCP サーバが正しく設定されていることを確認してください。

エラー メッセージ　SW-AUTO-UPGRADE-7_BOOT_FAILURE:「“%s”: Auto upgrade of the software failed.」

説明　ソフトウェアの自動アップグレードに失敗しました。

推奨処置　装置をリブートしてください。再度メッセージが表示される場合、表示されているエラー メッセージを正確にコピーし、テクニカル サポート担当者に報告してください。

エラー メッセージ　DOT11-4-UPGRADE:「Send your company name and the following report to migrateapj52w52@cisco.com.」The following AP has been migrated from J(j52) to U(w52) Regulatory Domain:AP name AP Model Ethernet MAC %s %s %e \U\Regulatory Doman

説明　J から U への日本の規制分野フィールド アップグレードが完了しました。

推奨処置　なし。

エラー メッセージ　AUTO-INSTALL-4-STATION_ROLE:「“%s”: The radio is operating in automatic install mode.」

説明　自動インストール モードで無線が動作しています。

推奨処置　設定インターフェイス コマンド **station-role** は、無線をインストール モード以外の役割に設定するために使用します。

エラー メッセージ　AUTO-INSTALL-4-IP_ADDRESS_DHCP:「The radio is operating in automatic install mode and has set ip address dhcp.」

説明　無線は自動インストール モードで動作しており、DHCP を介して IP アドレスを受信するように設定されています。

推奨処置　設定インターフェイス コマンド **station-role** は、無線をインストール モード以外の役割に設定するために使用します。

エラー メッセージ　AUTO-INSTALL-6_STATUS:“%s”%s.RSSI=-%d dBm.:「The radio is operating in install mode.」

説明　自動インストール モードで無線が動作しています。

推奨処置　設定インターフェイス コマンド **station-role** は、無線をインストール モード以外の役割に設定するために使用します。

エラー メッセージ　AVR_IMAGE_UPDATE-7-UPDATE_COMPLETE:「The AVR "$d" firmware was successfully updated.」

説明　アクセス ポイント AVR ファームウェアは正常に更新されました。

推奨処置　なし。

エラー メッセージ　AVR_IMAGE_UPDATE-2-UPDATE_FAILURE:「The AVR "$d" firmware is not current.Update error: "$s".」

説明　AVR ファームウェアは最新の状態ではありません。アップデートに失敗しました

推奨処置　エラー メッセージを書き写し、テクニカル サポート担当者に報告してください。

エラー メッセージ　AVR_IMAGE_UPDATE-4-UPDATE_SKIPPED:「AVR "$d" update processing was skipped:"$s".」

説明　エラーのため、AVR アップデートの処理がスキップされました。

推奨処置　なし。

エラー メッセージ　AVR_IMAGE_UPDATE-4-UPDATE_START:「The system is updating the AVR "$d" firmware.Please wait ...」

説明　システムは、AVR ファームウェアをアップデートしています。

推奨処置　なし。

アソシエーション管理メッセージ

エラー メッセージ　DOT11-3-BADSTATE:「%s %s ->%s.」

説明　802.11 アソシエーションと管理では、テーブル方式ステート マシンを使用してアソシエーションのさまざまなステートへの移行を追跡します。ステート移行は、アソシエーションが多くの可能性のあるイベントのいずれかを受け取ったときに起こります。このエラーが発生した場合、移行前のステートでは予測できなかったイベントをアソシエーションが受け取ったことを意味します。

推奨処置　システムは稼働し続けますが、このエラーを発生させたアソシエーションは損失する場合があります。表示されているエラー メッセージを正確にコピーし、サービス担当者に報告してください。

エラー メッセージ　DOT11-6-ASSOC:「Interface %s, Station %s e% %s KEY_MGMT (%s), MSGDEF_LIMIT_MEDIUM.」

説明　表示されているステーションは、表示されているインターフェイスのアクセス ポイントにアソシエートされています。

推奨処置　なし。

エラー メッセージ　DOT11-6-ADD:「Interface %s, Station %e associated to parent %e.」

説明　表示されているステーションは、表示されているインターフェイスの親アクセス ポイントにアソシエートされています。

推奨処置　なし。

エラー メッセージ　DOT11-6-DISASSOC: Interface %s, Deauthenticating Station %e #s

説明　ステーションがアクセス ポイントからアソシエーションを解除されました。

推奨処置　なし。

エラー メッセージ　DOT11-6-ROAMED:「Station %e roamed to %e.」

説明　表示されているステーションは、表示されている新しいアクセス ポイントにローミングしました。

推奨処置　なし。

エラー メッセージ　DOT11-4-ENCRYPT_MISMATCH:「Possible encryption key mismatch between interface %s and station %e.」

説明　表示されているインターフェイスとステーションの暗号化設定が一致していない可能性があります。

推奨処置　このインターフェイスの暗号化設定と、エラーを起こしているステーションの暗号化設定が一致することを確認してください。

エラー メッセージ　DOT11-4-DIVER_USED: Interface $s, Mcs rates 8-15 disabled due to only one transmit or recieve antenna enabled

説明　これらのレートでは、少なくとも 2 つの送受信アンテナを有効にする必要があります。

推奨処置　コンソールまたはシステム ログに出力されたエラー メッセージをそのままコピーします。Output Interpreter（https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl）を使用して、エラーについて調査し、解決を試みます。また、http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl にアクセスして、Bug Toolkit を検索してください。それでもサポートが必要である場合は、インターネット経由で、Technical Assistance Center（http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl）でケースを開くか、シスコのテクニカル サポート担当者に連絡し、収集した情報を報告します。

エラー メッセージ　DOT11-4-NO_HT: Interface %s, Mcs rates disabled on vlan %d due to %s

説明　正しい設定が使用されていなかったため、HT レートを使用できませんでした。

推奨処置　コンソールまたはシステム ログに出力されたエラー メッセージをそのままコピーします。Output Interpreter（https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl）を使用して、エラーについて調査し、解決を試みます。また、http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl にアクセスして、Bug Toolkit を検索してください。それでもサポートが必要である場合は、インターネット経由で、Technical Assistance Center（http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl）でケースを開くか、シスコのテクニカル サポート担当者に連絡し、収集した情報を報告します。

エラー メッセージ　DOT11-4-NO_MBSSID_BACKUP_VLAN: Backup VLANs cannot be configured if MBSSID is not enabled:"$s" not started

説明　VLAN のバックアップを有効にするには、MBSSID モードを設定する必要があります。

推奨処置　このデバイスで MBSSID を設定します。

解凍メッセージ

エラー メッセージ　SOAP-4-UNZIP_OVERFLOW:「Failed to unzip %s, exceeds maximum uncompressed html size.」

説明　HTTP サーバが HTTP GET 要求に対して圧縮ファイルを取り出すことができません。これは、ファイルが圧縮解除プロセスで使用されるバッファよりも大きすぎるためです。

推奨処置　ファイルが有効な HTML ページであることを確認します。有効である場合、圧縮する前のファイルをフラッシュにコピーして、HTTP を通じて取り出します。

システム ログ メッセージ

エラー メッセージ　%DOT11-4-LOADING_RADIO: Interface [chars], loading the radio firmware ([chars])

説明　新しいファームウェアをロードするために、無線が停止されました。

推奨処置　なし。

エラー メッセージ　%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

説明　データ リンク レベル ライン プロトコルの状態が変わりました。

推奨処置　なし。

エラー メッセージ　%SYS-5-RESTART: System restarted --[chars]

説明　リロードまたは再起動が要求されました。

推奨処置　単なる通知メッセージです。なし。

エラー メッセージ　%SYS-5-CONFIG_I: Configured from [chars] by [chars]

説明　ルータの設定が変更されています。

推奨処置　これは単なる通知メッセージです。なし。

エラー メッセージ　%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

説明　表示されているインターフェイスのデータ リンク レベル ライン プロトコルの状態が変わりました。

推奨処置　なし。

エラー メッセージ　%SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start

説明　SNMP サーバがコールド スタートを完了しました。

推奨処置　単なる通知メッセージです。なし。

エラー メッセージ　%SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].

説明　システム クロックが変更されました。

推奨処置　これは単なる情報メッセージです。なし。

802.11 サブシステム メッセージ

エラー メッセージ　DOT11-6-FREQ_USED:「Interface %s, frequency %d selected.」

説明　未使用の周波数をスキャンした後に、表示されたインターフェイスにより、表示された周波数が選択されました。

推奨処置　なし。

エラー メッセージ　DOT11-4-NO-VALID_INFRA_SSID:「No infrastructure SSID configured.%s not started.」

説明　インフラストラクチャ SSID は設定されていませんでした。また、表示されたインターフェイスは開始されていませんでした。

推奨処置　無線の設定に 1 つ以上のインフラストラクチャ SSID を追加します。

エラー メッセージ　DOT11-4-VERSION_UPGRADE:「Interface %d, upgrading radio firmware.」

説明　表示されたインターフェイスの起動時に、アクセス ポイントで誤ったバージョンのファームウェアが見つかりました。無線は要求されたバージョンでロードされます。

推奨処置　なし。

エラー メッセージ　DOT11-2-VERSION_INVALID:「Interface %d, unable to find required radio version %x.%x/ %d/」

説明　表示されたインターフェイスの無線ファームウェアを再フラッシュしているときに、アクセス ポイントが表示された無線ファームウェア（Cisco IOS ソフトウェアに同梱されているもの）のバージョンが誤っていることを検出しました。

推奨処置　なし。

エラー メッセージ　DOT11-3-RADIO_OVER_TEMPERATURE:「Interface %s Radio over temperature detected.」

説明　無線の内部温度が、表示された無線インターフェイスの上限を超えました。

推奨処置　内部温度を下げるために必要な処理を実行してください。この処理は、使用しているインストレーションによって異なります。

エラー メッセージ　DOT11-6-RADIO_TEMPERATURE_NORMAL:「Interface %s radio temperature returned to normal.」

説明　無線の内部温度が、表示された無線インターフェイスの正常な制限範囲内に戻りました。

推奨処置　なし。

エラー メッセージ　DOT11-3-TX_PWR_OUT_OF_RANGE:「Interface %s Radio transmit power out of range.」

説明　送信電力レベルが、表示された無線インターフェイスの正常範囲外にあります。

推奨処置　ネットワークおよびサービスから装置を取り外してください。

エラー メッセージ　DOT11-3-RADIO_RF_LO:「Interface %s Radio cannot lock RF freq.」

説明　無線の Phase Lock Loop（PLL）回線は、表示されたインターフェイスで正しい周波数にロックできません。

推奨処置　ネットワークおよびサービスから装置を取り外してください。

エラー メッセージ　DOT11-3-RADIO_IF_LO:「Interface %s Radio cannot lock IF freq.」

説明　無線の Intermediate Frequency（IF; 中間周波数）PLL は、表示されたインターフェイスで正しい周波数にロックできません。

推奨処置　ネットワークおよびサービスから装置を取り外してください。

エラー メッセージ　DOT11-6-FREQ_SCAN:「Interface %s Scanning frequencies for %d seconds.」

説明　表示されたインターフェイスで Least Congested Frequency のスキャンが開始され、表示された期間、実行されます。

推奨処置　なし。

エラー メッセージ　DOT11-2-NO_CHAN_AVAIL:「Interface %s, no channel available.」

説明　使用可能な周波数がありません。過去 30 分間のうちに、レーダーが検出された可能性があります。

推奨処置　なし。

エラー メッセージ　DOT11-6-CHAN_NOT_AVAIL:「DFS configured frequency %d Mhz unavailable for %d minute(s).」

説明　現在のチャネルでレーダーが検出されました。Dynamic Frequency Selection（DFS; 動的周波数選択）の規制では、このチャネルで 30 秒間、送信しないこととされています。

推奨処置　なし。

エラー メッセージ　DOT11-6-DFS_SCAN_COMPLETE:「DFS scan complete on frequency %d MHz.」

説明　デバイスは、表示された周波数で Dynamic Frequency Selection（DFS; 動的周波数選択）周波数スキャン プロセスを完了しました。

推奨処置　なし。

エラー メッセージ　DOT11-6-DFS_SCAN_START:「DFS: Scanning frequency %d MHz for %d seconds.」

説明　デバイスは、DFS スキャン プロセスを開始しました。

推奨処置　なし。

エラー メッセージ　DOT11-6-DFS_TRIGGERED:「DFS: triggered on frequency %d MHz.」

説明　DFS は、表示された周波数でレーダー信号を検出しました。

推奨処置　なし。このチャネルは Non-Occupancy List に 30 分間載せられ、新しいチャネルが選択されます。

エラー メッセージ　DOT11-4-DFS_STORE_FAIL:「DFS: could not store the frequency statistics.」

説明　DFS 統計情報をフラッシュに書き込むときにエラーが発生しました。

推奨処置　なし。

エラー メッセージ　DOT11-4-NO_SSID:「No SSIDs configured, %d not started.」

説明　すべての SSID が設定から削除されています。無線の実行には SSID が少なくとも 1 つは設定されている必要があります。

推奨処置　アクセス ポイントに 1 つ以上の SSID を設定します。

エラー メッセージ　DOT11-4-NO_SSID_VLAN:「No SSID with VLAN configured.%s not started.」

説明　VLAN 用に設定された SSID はありません。表示されたインターフェイスは開始されていませんでした。

推奨処置　VLAN 1 つにつき、少なくとも 1 つの SSID を設定する必要があります。表示されたインターフェイス上の VLAN に対して、SSID を少なくとも 1 つ追加してください。

エラー メッセージ　DOT11-4-NO_MBSSID_VLAN:「No VLANs configured in MBSSID mode.%s not started.」

説明　MBSSID モードで設定されている VLAN はありません。表示されたインターフェイスは開始されていませんでした。

推奨処置　表示されたインターフェイス設定に、VLAN を持つ SSID を少なくとも 1 つ追加してください。

エラー メッセージ　DOT11-4-NO_MBSSID_SHR_AUTH:「More than 1 SSID with shared authentication method in non-MBSSID mode % is down.」

説明　MBSSID が有効にされていない場合、複数の SSID で認証方式は共有できません。

推奨処置　設定を開くには、Dot11Radio 無線インターフェイスを削除するか、SSID の認証モードを変更します。

エラー メッセージ　DOT114-NO_MBSSID_BACKUP_VLAN:「Backup VLANs cannot be configured if MBSSID is not enabled.%s not started.」

説明　バックアップ VLAN を有効にするには、MBSSID モードを設定する必要があります。

推奨処置　このデバイスで MBSSID を設定します。

エラー メッセージ　IF-4-MISPLACED_VLAN_TAG:「Detected a misplaced VLAN tag on source Interface %.Dropping packet.」

説明　受信された 802.1Q VLAN タグは表示されたインターフェイスで検出されましたが、正しく解析できませんでした。受信されたパケットのカプセル化、またはカプセル化解除は正しく行われていませんでした。

推奨処置　なし。

エラー メッセージ　DOT11-2-FW_LOAD_NET:「Interface %s cannot load on boot.Place image in flash root directory and reload.」

説明　アクセス ポイントをブートしているときには、ネットワークから無線イメージはロードできません。

推奨処置　このイメージを、フラッシュ ファイル システムのルート ディレクトリに格納します。

エラー メッセージ　DOT11-4-FW_LOAD_DELAYED:「Interface %s, network filesys not ready.Delaying firmware (%s) load.」

説明　表示されたインターフェイスに新しいファームウェアをフラッシュしようとしたときに、ネットワーク ファイルシステムが実行されていなかったか、準備ができていませんでした。表示されたファームウェア ファイルのロードが遅れています。

推奨処置　新しいファームウェアのフラッシュを再試行する前に、ネットワークが立ち上がり、準備できていることを確認してください。

エラー メッセージ　DOT11-3-FLASH_UNKNOWN_RADIO:「Interface %s has an unknown radio.」

説明　ユーザが新しいファームウェアを、表示されたインターフェイスにフラッシュしようとしたときに、無線のタイプを判断できませんでした。

推奨処置　システムをリブートし、ファームウェアのアップグレードが完了するかどうかを確認してください。

エラー メッセージ　DOT11-4-UPLINK_ESTABLISHED:「Interface %s associated to AP %s %e %s.」

説明　表示されたリピータは、表示されたルート アクセス ポイントにアソシエートされています。これで、表示されたリピータにクライアントをアソシエートし、トラフィックを通過させることができます。

推奨処置　なし。

エラー メッセージ　DOT11-2-UPLINK_FAILED:「Uplink to parent failed: %s.」

説明　表示された理由で親アクセス ポイントとの接続が失敗しました。アップリンクは接続の試行を停止します。

推奨処置　アップリンク インターフェイスをリセットしてください。それでも問題が解決されない場合は、テクニカル サポートにお問い合わせください。

エラー メッセージ　DOT11-4-CANT_ASSOC:「Interface %, cannot associate %s.」

説明　表示されたインターフェイス デバイスを、表示された親アクセス ポイントにアソシエートできませんでした。

推奨処置　親アクセス ポイントの設定とこの装置の設定が一致していることを確認してください。

エラー メッセージ　DOT11-4-CANT_ASSOC:「Interface Dot11Radio 0, cannot associate.」

説明　親はクライアント MFP をサポートしていません。このエラー メッセージがアクセス ポイントに表示されるのは、ワークグループ ブリッジ、リピータ、または非ルート ブリッジ モードだけです。また、WGB、リピータ、非ルートが Client MFP SD 必須（または、強制）と設定されているが、ルート Client MFP が無効になっている場合に表示されます。

推奨処置　親アクセス ポイントの設定とこの装置の設定が一致していることを確認してください。

エラー メッセージ　DOT11-2-PROCESS_INITIALIZATION_FAILED:「The background process for the radio could not be started: %s」

説明　表示されたインターフェイスで使用されている初期化プロセスが何らかの理由により失敗しました。一時的なエラーである可能性があります。

推奨処置　アクセス ポイントをリロードします。この操作により問題が解決されなかった場合は、電源を再投入します。それでも問題が解決されない場合は、アクセス ポイントのファームウェアを前のバージョンにダウングレードします。

エラー メッセージ　DOT11-2-RADIO_HW_RESET:「Radio subsystem is undergoing hardware reset to recover from problem.」

説明　ソフト リセットでは解決できない修復不可能なエラーが発生しました。

推奨処置　なし。

エラー メッセージ　DOT11-2-RESET_RADIO:「Interface %s, Radio %s, Trying hardware reset on radio.」

説明　ソフトウェア リセットにより無線を起動しようとしましたが、失敗しました。装置の無線すべてをリセットするために、ハードウェア リセットを試行しています。

推奨処置　なし。

エラー メッセージ　DOT11-4-MAXRETRIES:「Packet to client %e reached max retries, removing the client.」

説明　パケット送信試行回数の上限に達したため、クライアントの削除が行われています。このエラー メッセージは、アクセス ポイントが、ある特定の回数、クライアントのポーリングを試みたが、応答を受信できなかったことを表しています。したがって、このクライアントはアソシエーション テーブルから削除されます。この問題は、クライアントとアクセス ポイントがノイズの多い RF 環境で通信を試みたときによく発生します。

推奨処置　この問題を解決するには、アクセス ポイントでキャリア話中検索を実行して、スナップショットの無線スペクトラムにノイズが現れるかどうかを確認します。不要なノイズの軽減を試行します。詳細については、「キャリア話中検査の実行」（P.6-36）の手順を参照してください。1 つのエリアに複数のアクセス ポイントがある場合、チャネル信号や、このエリアを取り囲むエリアにある他の無線デバイスとオーバーラップしている可能性があります。ネットワーク インターフェイスの下のチャネルを変更し、Radio-802.11 を選択します。オーバーラップしないチャネルには、1、6、および 11 の 3 種類があります。

エラー メッセージ　DOT11-4-RM_INCAPABLE:「Interface %s」

説明　表示されたインターフェイスは、無線管理機能をサポートしていません。

推奨処置　なし。

エラー メッセージ　DOT11-4-RM_INCORRECT_INTERFACE:「Invalid interface, either not existing or non-radio.」

説明　無線管理要求により、このインターフェイスは存在しないか、無線インターフェイスではないことが検出されました。

推奨処置　なし。

エラー メッセージ　DOT11-3-POWERS_INVALID:「Interface %s, no valid power levels available.」

説明　無線ドライバは、有効な電力レベル設定を検出できませんでした。

推奨処置　電源および設定を調べ、訂正してください。

エラー メッセージ　DOT11-4-RADIO_INVALID_FREQ:「Operating frequency (%d) invalid - performing a channel scan.」

説明　表示された周波数は、操作には無効です。有効な周波数を選択するためにチャネル スキャンが行われています。

推奨処置　なし。

エラー メッセージ　DOT11-4-RADIO_NO_FREQ:「Interface &s, all frequencies have been blocked, interface not started.」

説明　この操作に対して設定された周波数は無効です。有効な操作周波数を選択するために、チャネル スキャンが行われています。

推奨処置　なし。

エラー メッセージ　DOT11-4-BCN_BURST_NO_MBSSID:「Beacon burst mode is enabled but MBSSID is not enabled, %s is down.」

説明　ビーコン バースト モードは、表示されたインターフェイスで MBSSID が有効にされている場合にだけ有効にできます。

推奨処置　表示されたインターフェイスで MBSSID を有効にするか、ビーコン バーストを無効にしてください。

エラー メッセージ　DOT11-4-BCN_BURST_TOO_MANY_DTIMS:「Beacon burst mode is enabled and there are too many different DTIM periods defined.%s is down.」

説明　ビーコン バースト モードでサポートできるのは最大 4 個の一意の DTIM 値だけです。DTIM 値 1 個につき、最大 4 個の BSS があります。

推奨処置　このインターフェイスで設定されている SSID に対する一意の DTIM 数をより妥当な値に変更します。

エラー メッセージ　DOT11-2-RADIO_INITIALIZATION_ERROR:「The radio subsystem could not be initialized (%s).」

説明　無線サブシステムの初期化を試みているときに、重大なエラーが検出されました。

推奨処置　システムをリロードします。

エラー メッセージ　DOT11-4-UPLINK_NO_ID_PWD:「Interface %s, no username/password supplied for uplink authentication.」

説明　ユーザ名またはパスワード、もしくはその両方の入力に失敗しました。

推奨処置　ユーザ名またはパスワード、もしくはその両方を入力して、もう一度実行してください。

エラー メッセージ　DOT11-5-NO_IE_CFG:「No IEs configured for %s (ssid index %u).」

説明　無線にビーコン、またはプローブ応答を適用しようとしましたが、表示された SSID インデックスではこのビーコン、またはプローブは定義されていませんでした。

推奨処置　IE 設定を確認してください。

エラー メッセージ　DOT11-4-FLASHING_RADIO:「Interface %s, flashing radio firmware (%s).」

説明　表示された新しいファームウェアをロードするために、表示されたインターフェイス無線が停止されました。

推奨処置　なし。

エラー メッセージ　DOT11-4-LOADING_RADIO:「Interface %s, loading the radio firmware (%s).」

説明　表示された新しいファームウェアをロードするために、表示されたインターフェイス無線が停止されました。

推奨処置　なし。

エラー メッセージ　DOT11-2-NO_FIRMWARE:「Interface %s, no radio firmware file (%s) was found.」

説明　新しいファームウェアをフラッシュしようとしましたが、無線のファイルがフラッシュ ファイル システムに見つかりませんでした。または、アクセス ポイントの IOS が破損しています。

推奨処置　装置に誤ったイメージがロードされました。使用している無線のタイプに基づき、正しいイメージを探してください。この問題を解決するために、新しい Cisco IOS イメージを使用して、アクセス ポイントのリロードが必要な場合があります。イメージのリロード手順については、「アクセス ポイントのイメージのリロード」(P.24-7)を参照してください。

アクセス ポイントの IOS が破損している場合は、MODE ボタン方式を使用して、アクセス ポイント イメージをリロードします。「MODE ボタンの使用」(P.24-4)を参照してください。

エラー メッセージ　DOT11-2-BAD_FIRMWARE:「Interface %s, radio firmware file (%s) is invalid.」

説明　新しいファームウェアを、表示されたインターフェイスにフラッシュしようとしたときに、表示された無線ファームウェア ファイルが無効であることがわかりました。

推奨処置　装置が予期している場所に、正しいファームウェア イメージ ファイルが存在することを確認します。

エラー メッセージ　DOT11-2-RADIO_FAILED:「Interface %s, failed - %s.」

説明　表示されたインターフェイスの無線ドライバは重大なエラーを検出しました。表示された理由によりシャットダウンしています。

推奨処置　なし。

エラー メッセージ　DOT11-4-FLASH_RADIO_DONE:「Interface %s, flashing radio firmware completed.」

説明　表示されたインターフェイスの無線ファームウェアのフラッシュが終了しました。この無線は新しいファームウェアで再起動されます。

推奨処置　なし。

エラー メッセージ　DOT11-4-UPLINK_LINK_DOWN:「Interface %s, parent lost: %s.」

説明　表示されたインターフェイス上の親アクセス ポイントへの接続は、表示された理由により失われました。装置は新しい親アクセス ポイントを探そうとしています。

推奨処置　なし。

エラー メッセージ　DOT11-4-CANT_ASSOC: Cannot associate: $s

説明　表示された理由により、装置は親アクセス ポイントとの接続を確立できませんでした。

推奨処置　親アクセス ポイントと装置の基本設定（SSID、WEP など）が一致していることを確認します。

エラー メッセージ　DOT11-4-CLIENT_NOT_FOUND:「Client was not found.」

説明　mic の確認中に、クライアントが見つかりませんでした。

推奨処置　なし。

エラー メッセージ　DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client

説明　クライアントに送信したパケットが何度も正常に届かず、最大再試行回数に達しました。このため、アソシエーション テーブルからこのクライアントが削除されました。

推奨処置　なし。

エラー メッセージ　DOT11-4-BRIDGE_LOOP:「Bridge loop detected between WGB %e and device %e.」

説明　表示されたワークグループ ブリッジは、表示されたイーサネット クライアントのいずれか 1 つのアドレスを報告しましたが、アクセス ポイントではこのアドレスはネットワーク上の別の場所としてすでにマークされています。

推奨処置　アクセス ポイントの GUI において [Associations] ページで [Refresh] をクリックするか、CLI で **clear dot11 statistics** コマンドを入力します。

エラー メッセージ　DOT11-4-ANTENNA_INVALID:「Interface %s, current antenna position not supported, radio disabled.」

説明　表示された AIR-RM21A 無線モジュールは、高ゲイン位置の外部アンテナをサポートしません（高ゲイン位置のアンテナはアクセス ポイントに対して平らに折り返します）。アクセス ポイントは、アンテナが高ゲイン位置にあると自動的に無線を無効にします。

推奨処置　AIR-RM21A 無線モジュールのアンテナを、アクセス ポイントの本体に直角になるように折り返します。

エラー メッセージ　DOT11-6-ANTENNA_GAIN:「Interface %s, antenna position/gain changed, adjusting transmitter power.」

説明　アンテナ ゲインが変更されたため、許可される電力レベルのリストを調節する必要があります。

推奨処置　なし。

エラー メッセージ　DOT11-4-DIVER_USED:「Interface %s Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled.」

説明　リストされているレートでは、少なくとも 2 つの送受信アンテナを有効にする必要があります。

推奨処置　アクセス ポイントに少なくとも 2 つの送受信アンテナを設置し、有効にします。

エラー メッセージ　DOT11-3-RF-LOOPBACK_FAILURE:「Interface %s Radio failed to pass RF loopback test.」

説明　表示されたインターフェイスに対する無線ループバック テストが失敗しました。

推奨処置　なし。

エラー メッセージ　DOT11-3-RF-LOOPBACK_FREQ_FAILURE:「Interface %s failed to pass RF loopback test.」

説明　表示されたインターフェイスに対する、指定された周波数での無線ループバック テストが失敗しました。

推奨処置　なし。

エラー メッセージ　DOT11-7-AUTH_FAILED:「Station %e Authentication failed」

説明　表示されたステーションは、認証に失敗しました。

推奨処置　入力したユーザ名とパスワードが正しいこと、および認証サーバがオンラインであることを確認します。

エラー メッセージ　DOT11-7-CCKM_AUTH_FAILED:「Station %e CCKM authentication failed.」

説明　表示されたステーションは、Cisco Centralized Key Management（CCKM）認証に失敗しました。

推奨処置　WDS アクセス ポイントを使用するように設定されているアクセス ポイントのトポロジが機能していることを確認します。

エラー メッセージ　DOT11-4-CCMP_REPLAY:「AES-CCMP TSC replay was detected on packet (TSC 0x%11x received from &e).」

説明　フレームは、AES-CCMP TSC 再送を示しています。受信パケットにおける AES-CCMP TSC の再送は、ほとんどの場合、アクティブな攻撃を示します。

推奨処置　なし。

エラー メッセージ　DOT11-4-CKIP_MIC_FAILURE:「CKIP MIC failure was detected on a packet (Digest 0x%x) received from %e).」

説明　フレームで、CKIP MIC エラーが検出されました。受信パケットにおける CKIP MIC エラーは、ほとんどの場合、アクティブな攻撃を示します。

推奨処置　なし。

エラー メッセージ　DOT11-4-CKIP_REPLAY:「CKIP SEQ replay was detected on a packet (SEQ 0x&x) received from %e.」

説明　フレームで、CKIP SEQ 再送が検出されました。受信パケットにおける CKIP SEQ の再送は、ほとんどの場合、アクティブな攻撃を示します。

推奨処置　なし。

エラー メッセージ　DOT11-4-TKIP_MIC_FAILURE:「Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key.」

説明　表示されたペア キーを使用してローカルに復号化されたユニキャスト フレーム上で、表示されたステーションから、TKIP Michael MIC の失敗が検出されました。

推奨処置　受信パケットにおける Michael MIC の失敗は、ネットワークがアクティブな攻撃を受けていることを示している可能性があります。無線 LAN から潜在的な不正デバイスを探して削除します。このエラーは、クライアントの設定に誤りがあること、またはクライアントに障害があることを示している可能性もあります。

エラー メッセージ　DOT11-4-TKIP_MIC_FAILURE_REPORT:「Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key」

説明　アクセス ポイントは、表示されたステーションから EAPOL キーを受信しました。このキーは、このアクセス ポイントによって送信されたパケット上で TKIP Michael MIC が失敗したことを、アクセス ポイントに通知しています。

推奨処置　なし。

エラー メッセージ　DOT11-3-TKIP_MIC_FAILURE_REPEATED:「Two TKIP Michael MIC failures were detected within %s seconds on %s interface.The interface will be put on MIC failure hold state for next %d seconds」

説明　表示されたインターフェイスで、表示された時間内に 2 つの TKIP Michael MIC 障害が検出されました。これは通常、ネットワークがアクティブな攻撃を受けていることを示しているため、表示された時間、インターフェイスはホールドされます。このホールド時間中は TKIP 暗号を使用するステーションのアソシエーションが解除され、ホールド時間が終了するまで再アソシエートできません。ホールド時間が終了したら、インターフェイスは通常どおり動作します。

推奨処置　MIC 障害は通常、ネットワークがアクティブな攻撃を受けていることを示しています。無線 LAN から潜在的な不正デバイスを探して削除します。これが偽のアラームで、インターフェイスのホールド時間が長すぎる場合は、**countermeasure tkip hold-time** コマンドを使用してホールド時間を調整します。

エラー メッセージ　DOT11-4-TKIP_REPLAY:「TKIP TSC replay was detected on a packet (TSC 0x%ssx received from %e).」

説明　フレームで、TKIP TSC 再送が検出されました。受信パケットにおける TKIP TSC の再送は、ほとんどの場合、アクティブな攻撃を示します。

推奨処置　なし。

エラー メッセージ　DOT11-4-WLAN_RESOURCE_LIMIT:「WLAN limit exceeded on interface %s and network-id %d.」

説明　このアクセス ポイントの VLAN または WLAN の数が上限の 16 個に達しました。

推奨処置　アクセス ポイントが、割り当てられたネットワーク ID がオンの RADIUS とのアソシエートを試行している場合は、静的 VLAN の設定を解除するか、数を減らします。

エラー メッセージ　SOAP-3-WGB_CLIENT_VLAN_SOAP:「Workgroup Bridge Ethernet client VLAN not configured.」

説明　ワークグループ ブリッジに装着されているクライアント デバイス用に設定されている VLAN がありません。

推奨処置　ワークグループ ブリッジにアタッチされているクライアント デバイスに対応するように VLAN を設定します。

エラー メッセージ　DOT11-4-NO_VLAN_NAME:「VLAN name %s from RADIUS server is not configured for station %e.」

説明　RADIUS サーバにより返された VLAN 名は、アクセス ポイントで設定する必要があります。

推奨処置　アクセス ポイントで VLAN 名を設定します。

エラー メッセージ　DOT11-4-NO_VLAN_ID:「VLAN id %d from Radius server is not configured for station %e.」

説明　RADIUS サーバにより返された VLAN ID は、アクセス ポイントで設定する必要があります。

推奨処置　アクセス ポイントで VLAN ID を設定します。

エラー メッセージ　SOAP-3-ERROR:「Reported on line %d in file %s.%s.」

説明　コントローラ ASIC の表示されたファイル名にある表示された行番号で、内部エラーが発生しました。

推奨処置　なし。

エラー メッセージ　SOAP_FIPS-2-INIT_FAILURE:「SOAP FIPS initialization failure: %s.」

説明　SOAP FIPS 初期化エラー。

推奨処置　なし。

エラー メッセージ　SOAP_FIPS-4-PROC_FAILURE:「SOAP FIPS test failure: %s.」

説明　SOAP FIPS テストの重大なエラー。

推奨処置　なし。

エラー メッセージ　SOAP_FIPS-4-PROC_WARNING:「SOAP FIPS test warning: %s.」

説明　SOAP FIPS テストの重大ではないエラー。

推奨処置　なし。

エラー メッセージ　SOAP_FIPS-2-SELF_TEST_IOS_FAILURE:「IOS crypto FIPS self test failed at %s.」

説明　IOS 暗号化ルーチンでの SOAP FIPS セルフ テストが失敗しました。

推奨処置　IOS イメージをチェックします。

エラー メッセージ　SOAP_FIPS-2-SELF_TEST_RAD_FAILURE:「RADIO crypto FIPS self test failed at %s on interface %s %d.」

説明　無線暗号化ルーチンでの SOAP FIPS セルフ テストが失敗しました。

推奨処置　無線イメージをチェックします。

エラー メッセージ　SOAP_FIPS-2-SELF_TEST_IOS_SUCCESS:「IOS crypto FIPS self test passed.」

説明　SOAP FIPS セルフ テストに合格しました。

推奨処置　なし。

エラー メッセージ　SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS:「RADIO crypto FIPS self test passed on interface %s %d.」

説明　無線インターフェイスでの、SOAP FIPS セルフ テストに合格しました。

推奨処置　なし。

エラー メッセージ　DOT11-6-MCAST_DISCARD:「%s mode multicast packets are discarded in %s multicast mode.」

説明　ワークグループ ブリッジとして設定されているアクセス ポイントは、クライアント モードではインフラストラクチャ モードのマルチキャスト パケットをドロップし、インフラストラクチャ モードではクライアント モードのマルチキャスト パケットをドロップします。

推奨処置　なし。

アクセス ポイント間プロトコル メッセージ

エラー メッセージ　DOT11-6-STANDBY_ACTIVE:「Standby to Active, Reason = %s (%d).」

説明　表示された理由により、アクセス ポイントはスタンバイ モードからアクティブ モードに移行しています。

推奨処置　なし。

エラー メッセージ　DOT11-6-STANDBY_REQUEST:「Hot Standby request to shutdown radios from %e.」

説明　このアクセス ポイントのいずれかの無線インターフェイスでエラーが検出されたため、表示されたスタンバイ アクセス ポイントは、このアクセス ポイントに無線インターフェイスのシャットダウンを要求しました。

推奨処置　なし。

エラー メッセージ　DOT11-6-ROGUE_AP:「Rogue AP %e reported.Reason: %s.」

説明　ステーションは表示された理由で潜在的な不正アクセス ポイントを報告しました。

推奨処置　なし。

ローカル認証サーバ メッセージ

エラー メッセージ　RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]

説明　ローカル Remote Authentication Dial-In User Service（RADIUS）サーバが認証要求を受信しましたが、その要求を転送した Network Access Server（NAS; ネットワーク アクセス サーバ）の IP アドレスを認識していません。

推奨処置　無線 LAN 上のすべてのアクセス ポイントが、ローカル RADIUS サーバで NAS として設定されていることを確認します。

エラー メッセージ　RADSRV-4-NAS_KEYMIS: NAS shared key mismatch.

説明　ローカル RADIUS サーバが認証要求を受信しましたが、メッセージ署名で、共有キーテキストが一致していないことが示されています。

推奨処置　NAS またはローカル RADIUS サーバ上のいずれかで、共有キーの設定を修正します。

エラー メッセージ　RADSRV-4_BLOCKED: Client blocked due to repeated failed authentications

説明　ユーザが、ブロックをトリガーするように設定されている回数の認証に失敗し、アカウントが無効となりました。

推奨処置　**clear radius local-server user** *username* 特権 EXEC コマンドを使用してユーザを解除するか、または、設定したロックアウト時間によってユーザに対するブロックが期限切れとなるようにします。

エラー メッセージ　DOT1X-SHIM-6-AUTH_OK:「Interface %s authenticated [%s].」

説明　802.1x 認証が正常に終了しました。

推奨処置　なし。

エラー メッセージ　DOT1X-SHIM-3-AUTH_FAIL:「Interface %s authentication failed.」

説明　装着されたデバイスの 802.1x 認証に失敗しました。

推奨処置　クライアントおよび RADIUS サーバで、802.1x 認定証の設定をチェックします。

エラー メッセージ　DOT1X-SHIM-3-INIT_FAIL:「Unable to init - %s.」

説明　シム レイヤの初期化中にエラーが発生しました。

推奨処置

エラー メッセージ　DOT1X-SHIM-3-UNSUPPORTED_KM:「Unsupported key management: %X.」

説明　シム レイヤの初期化中にエラーが発生しました。サポートされていないキー管理タイプが検出されました。

推奨処置　なし。

エラー メッセージ　DPT1X-SHIM-4-PLUMB_KEY_ERR:「Unable to plumb keys - %s.」

説明　シム レイヤがキーを調べようとしたときに、予測していなかったエラーが発生しました。

推奨処置　なし。

エラー メッセージ　DOT1X-SHIM-3-PKT_TX_ERR:「Unable to tx packet -%s.」

説明　シム レイヤが dot1x パケットを送信しようとしたときに、予測していなかったエラーが発生しました。

推奨処置　なし。

エラー メッセージ　DOT1X-SHIM-3-ENCAP_ERR:「Packet encap failed for %e.」

説明　シム レイヤが dot1x パケットを送信しようとしたときに、予測していなかったエラーが発生しました。パケットのカプセル化に失敗しました。

推奨処置　なし。

エラー メッセージ　DOT1X-SHIM-3-SUPP_START_FAIL:「Unable to start supplicant on %s.」

説明　表示されたインターフェイスでシム レイヤが dot1x サプリカントを開始しようとしたときに、予測していなかったエラーが発生しました。

推奨処置　なし。

エラー メッセージ　DOT1X-SHIM=3-NO_UPLINK:「No uplink found for %s.」

説明　dot11 インターフェイスで dot1x イベントまたはメッセージを処理している間に、アップリンクが予測されているが見つからないという状況に陥りました。

推奨処置　なし。

エラー メッセージ　Information Group rad_acct: Radius server <ip address> is responding again (previously dead).Error Group acct: No active radius servers found.Id 106

説明　このメッセージは、アクセス ポイントで **radius-server deadtime 10** コマンドが設定されている場合に表示されます。このコマンドは、アクセス ポイントが、応答しないサーバの使用を試行しない期間を設定するためのものです。したがって、要求がタイム アウトするまでに必要な時間を避けて、次の設定済みサーバを試行することができます。dead とマークされている RADIUS サーバは、すべてのサーバが dead とマークされていない限り、指定した期間（分単位）、その他の要求にもスキップされます。デッド タイムを 10 分間に設定するということは、このサーバを 10 分間使用できないことを意味します。

推奨処置　このログを消去する必要がある場合は、このコマンドを無効にします。実際、このメッセージは大きな問題ではありません。単なる情報ログです。

WDS メッセージ

エラー メッセージ　WLCCP-WDS-6-REPEATER_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.

説明　リピータ アクセス ポイントは、WDS をサポートしません。

推奨処置　なし。

エラー メッセージ　WLCCP-WDS-6-PREV_VER_AP: A previous version of AP is detected.

説明　WDS デバイスが、古いバージョンのアクセス ポイントを検出しました。

推奨処置　なし。

エラー メッセージ　WLCCP-AP-6-INFRA: WLCCP Infrastructure Authenticated

説明　アクセス ポイントが、WDS デバイスの認証に成功しました。

推奨処置　なし。

エラー メッセージ　WLCCP-AP-6-STAND_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode

説明　アクセス ポイントが WDS デバイスへの接続を失い、スタンドアロン モードになっています。

推奨処置　なし。

エラー メッセージ　WLCCP-AP-6-PREV_VER_WDS: A previous version of WDS is detected

説明　アクセス ポイントが、古いバージョンの WDS を検出しました。

推奨処置　ネットワーク上で、サポートされていないバージョンの WDS がないかどうかを確認します。

エラー メッセージ　WLCCP-AP-6-UNSUP_VER_WDS: An unsupported version of WDS is detected

説明　アクセス ポイントが、サポートされていないバージョンの WDS を検出しました。

推奨処置　ネットワーク上で、サポートされていないバージョンの WDS がないかどうかを確認します。

エラー メッセージ　WLCCP-NM-3-WNM_LINK_DOWN: Link to WNM is down

説明　ネットワーク マネージャが、keep-active メッセージに応答していません。

推奨処置　ネットワーク マネージャ、またはネットワーク マネージャへのネットワーク パスに問題がないか確認します。

エラー メッセージ　WLCCP-NM-6-WNM_LINK_UP: Link to WNM is up

説明　ネットワーク マネージャが、keep-active メッセージに応答するようになりました。

推奨処置　なし。

エラー メッセージ　WLCCP-NM-6-RESET: Resetting WLCCP-NM

説明　ネットワーク マネージャ IP アドレスの変更、または一時的なリソース不足状態により、WDS ネットワーク マネージャ サブシステムがリセットされた可能性がありますが、間もなく動作は通常の状態に戻ります。

推奨処置　なし。

エラー メッセージ　WLCCP-WDS-3-RECOVER:「%s」

説明　WDS 正常回復エラー。

推奨処置　なし。

ミニ IOS メッセージ

エラー メッセージ　MTS-2-PROTECT_PORT_FAILURE: An attempt to protect port [number] failed

説明　ポートを保護しようとしたときに、初期化に失敗しました。

推奨処置　なし。

エラー メッセージ　MTS-2-SET_PW_FAILURE: Error %d enabling secret password.

説明　ユーザがシークレット パスワードを有効にしようとしたときに、初期化に失敗しました。

推奨処置　なし。

エラー メッセージ　この設定を NVRAM に保存すると、NVRAM の最後に保存されたネットワーク管理やセキュリティ ファイルが破損する可能性があります。Continue?[no]:

説明　この警告メッセージは、アクセス ポイントの CLI 経由で設定変更を保存しようとしたときに、この CLI インターフェイスに表示されます。原因はフラッシュ メモリの容量不足です。無線が故障すると、.rcore ファイルが作成されます。このファイルは、無線にファームウェアまたはハードウェアの問題があることを示しますが、ハードウェアの問題はあまり起こりません。

推奨処置　この警告メッセージが表示されないようにするには、フラッシュ メモリで生成された rcore ファイルを削除します。rcore ファイルの拡張子は .rcore です。このファイルは、無線がある時点でダウンしたことを示しているだけであるため、削除してもかまいません。.rcore ファイルを CLI セッションに次のように表示することができます。

r15_5705_AB50_A8341F30.rcore

アクセス ポイントまたはブリッジについてのメッセージ

エラー メッセージ　APBR-4-SEND_PCKT_FAILED: Failed to Send Packet on port ifDescr (error= errornum)errornum: status error number

HASH(0x2096974)

説明　アクセス ポイント、またはブリッジがパケットの送信に失敗しました。この状態は、外部ノイズまたは干渉がある場合に見られることがあります。

推奨処置　ノイズまたは干渉の発生源をチェックしてください。

エラー メッセージ　APBR-6-DDP_CLNT_RESET: Detected probable reset of hosthost: host MAC address HASH(0x2080f04)

説明　アクセス ポイントまたはブリッジが、別のインフラストラクチャ デバイスの再起動を検出しました。

推奨処置　このメッセージが継続的に表示される場合は、アクセス ポイントをリブートしてください。

Cisco Discovery Protocol メッセージ

エラー メッセージ　CDP_PD-2-POWER_LOW: %s - %s %s (%e)

説明　システムに十分な電力が供給されていません。

推奨処置　インライン パワーの供給源を再設定するか、交換してください。

外部 RADIUS サーバ エラー メッセージ

エラー メッセージ　RADUYS:response-authenticator decrypt fail, paklen 32

説明　このエラー メッセージは、RADIUS サーバとアクセス ポイントの間で、RADIUS 共有キーが一致していないことを示しています。

推奨処置　RADIUS サーバとアクセス ポイントで同じ共有キーが使用されていることを確認してください。

LWAPP エラー メッセージ

エラー メッセージ　LWAPP-3-CDP: Failure sending CDP Update to Controller.Reason "s"

説明　アクセス ポイントの CDP アップデートをコントローラに送信できませんでした。

推奨処置　なし。

エラー メッセージ　LWAPP-3-CLIENTERRORLOG: "s"

説明　このログ メッセージは、LWAPP クライアント エラー イベントを示しています。このメッセージは、LWAPP アクセス ポイントの加入問題をトラブルシューティングしやすくするためにログに記録されています。

推奨処置　なし。

エラー メッセージ　LWAPP-3-CLIENTEVENTLOG: "s"

説明　このログ メッセージは、LWAPP クライアント通知イベントを示しています。このメッセージは、LWAPP アクセス ポイントの加入問題をトラブルシューティングしやすくするためにログに記録されています。

推奨処置　なし。

エラー メッセージ　LWAPP-3-UNSUPPORTEDRM: Got unsupported CCX RM Measurement "s" request "d" from Controller.

説明　コントローラから、サポートされていない CCX 無線管理測定が要求されました。

推奨処置　なし。

エラー メッセージ　LWAPP-5-WRONG_DFS_SLOT: DFS action on non-DFS radio "d"

説明　無線 b/g での DFS 処理

推奨処置　なし。

センサー メッセージ

エラー メッセージ　SENSOR-3-TEMP_CRITICAL: System sensor "d" has exceeded CRITCAL temperature thresholds

説明　環境テストの測定値の 1 つが、最大しきい値を超えています。

推奨処置　指定された状況を解決してください。解決できなかった場合、予防措置として、システムが、システム自身をシャット ダウンすることがあります。原因が温度または電圧にあるかどうかを確認するには、**show environment all** と入力します。これが温度に対する重大な警告である場合は、ルータのファンが動作していること、および部屋の冷却および空調が機能していることを確認してください。この状況により、システムが適切に動作できなくなることがあります。

エラー メッセージ　SENSOR-3-TEMP_NORMAL: "s" temperature sensor is now normal

説明　環境テストの測定値の 1 つが、通常の動作温度を下回っています。

推奨処置　なし。

エラー メッセージ　SENSOR-3-TEMP_SHUTDOWN: Shuting down the system because of dangerously HIGH temperature at sensor "d".

説明　環境テストの測定値の 1 つが、ルータの動作温度環境を超えています。

推奨処置　高温の原因を調べます。

エラー メッセージ　SENSOR-3-TEMP_WARNING: "s" temparature sensor "d" has exceeded WARNING temperature thresholds

説明　環境テストの測定値の 1 つが、警告のしきい値を超えています。

推奨処置　状況を注意深くモニタし、可能であれば、環境を冷却して改善します。

エラー メッセージ　SENSOR-3-VOLT_CRITICAL: System sensor "d" has exceeded CRITCAL voltage thresholds

説明　環境テストの測定値の 1 つが、電圧の最大しきい値を超えています。

推奨処置　指定された状況を解決してください。解決できなかった場合、予防措置として、システムが、システム自身をシャット ダウンすることがあります。原因が電圧にあるかどうかを確認するには、**show environment all** と入力します。この状況により、システムが適切に動作できなくなることがあります。

エラー メッセージ　SENSOR-3-VOLT_NORMAL: System sensor "d"("d") is now operating under NORMAL voltage

説明　測定された環境テスト ポイントの 1 つが、正常な動作温度を下回っています。

推奨処置　なし。

エラー メッセージ　SENSOR-3-VOLT_WARNING: Voltage monitor "d"("d") has exceeded voltage thresholds

説明　電圧テストの測定値の 1 つが、電圧が標準範囲外にあることを示しています。

説明　電源をチェックするか、または TAC にお問い合わせください。

SNMP エラー メッセージ

エラー メッセージ　SNMP-3-AUTHFAILIPV6: Authentication failure for SNMP request from hostUnrecognized format ' %P'

説明　このホストにより、適切に認証されていない SNMP 要求が送信されました。

推奨処置　SNMP 要求で使用されているコミュニティまたはユーザ名がルータで設定されていること確認してください。

エラー メッセージ　SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full

説明　入力キューがいっぱいであるため、SNMP パケットがドロップされました。

推奨処置　コマンド **show snmp** を使用して、ドロップされたパケットの数を確認します。エラー状態が解消されるまで、このデバイスに対する SNMP アクセスをすべて停止します。

エラー メッセージ　SNMP-3-INTERRUPT_CALL_ERR: "s" function, cannot be called from interrupt handler

説明　このメッセージは、この関数に対して、割り込みハンドラからコールが行われたことを示しています。コールが失敗し、デバイスが、malloc コールのスタックの下方でリブートされるため、このようなコールは許可されません。

推奨処置　このメッセージが繰り返し現れる場合は、表示されるとおりに書き写し、テクニカル サポート担当者に報告してください。

エラー メッセージ　SNMP-4-NOENGINEIDV6: Remote snmpEngineID for Unrecognized format ‘ %P’ not found when creating user: “s”

説明　ユーザを作成しようとしましたが、失敗しました。リモート エージェント（または、SNMP マネージャ）のエンジン ID が設定されていなかった可能性があります。

推奨処置　リモート snmpEngineID を設定し、ユーザを再設定します。同じ問題が続く場合は、出力されたエラー メッセージをそのままコピーし、シスコのテクニカル サポートに提出してください。

エラー メッセージ　SNMP_MGR-3-MISSINGHOSTIPV6: Cannot locate information on SNMP informs host:Unrecognized format ‘ %P’

説明　この SNMP の応答要求の宛先となるテーブル エントリが見つかりません。したがって、応答要求型通知はこの宛先に送信されません。

推奨処置　**show snmp host** コマンド、および **show snmp** コマンドを実行します。エラー メッセージ、および show コマンドからの出力を表示されているとおりに書き写し、テクニカル サポート担当者に報告してください。**snmp-server host** コンフィギュレーション コマンドを使用して、応答要求の宛先を削除し、再度追加することにより、この状態が解消されることがあります。解消されない場合は、システムの再ロードが必要になる可能性があります。

SSH エラー メッセージ

エラー メッセージ　SSH-5-SSH2_CLOSE: SSH2 Session from ”%s” (tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’, hmac ’”%s”’ closed

説明　SSH セッションの終了情報

推奨処置　なし - 情報のみのメッセージです。

エラー メッセージ　SSH-5-SSH2_SESSION: SSH2 Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”

説明　SSH セッションの要求情報

推奨処置　なし - 情報のみのメッセージです。

エラー メッセージ　SSH-5-SSH2_USERAUTH: User ’”%s”’ authentication for SSH2 Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”

説明　SSH ユーザ認証ステータス情報

推奨処置　なし - 情報のみのメッセージです。

エラー メッセージ　SSH-5-SSH_CLOSE: SSH Session from “%s”(tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’ closed

説明　SSH セッションの終了情報

推奨処置　なし - 情報のみのメッセージです。

エラー メッセージ　SSH-5-SSH_SESSION: SSH Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”

説明　SSH セッションの要求情報

推奨処置　なし - 情報のみのメッセージです。

エラー メッセージ　SSH-5-SSH_USERAUTH: User ’”%s”’ authentication for SSH Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”

説明　SSH ユーザ認証ステータス情報

推奨処置　なし - 情報のみのメッセージです。