Cisco 880 シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

Text Part Number: OL-22206-02-J

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

本書は、米国シスコ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。

Cisco 880 シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

CONTENTS

はじめに

ここでは、このマニュアルの目的、対象読者、構成、および表記法について説明し、さらに詳細情報が記載されている関連資料を紹介します。ここで説明する内容は、次のとおりです。

目的

このマニュアルでは、Cisco 880 シリーズ サービス統合型ルータ（ISR）の概要と、さまざまな機能を設定する方法について説明します。ご使用のルータ モデルに適用されない情報が記載されている場合もあります。

製品保証、修理、サポートについては、ご購入のルータに付属している『*Readme First for the Cisco 800 Series Integrated Services Routers*』の「Cisco One-Year Limited Hardware Warranty Terms」を参照してください。

対象読者

このガイドは、シスコ製機器のプロバイダーを対象としています。このガイドの内容は、読者が技術的な知識を持ち、Cisco ルータや Cisco IOS ソフトウェアとその機能について熟知していることを前提としています。

マニュアルの構成

このマニュアルは、次の部、章、付録で構成されています。

章	
「製品概要」	ルータのモデルと使用可能なソフトウェア機能の概要を説明します。
「ワイヤレス デバイス概要」	ルータ上のワイヤレス デバイスの概要と、ネットワーク構成の中でのその用途の概要を説明します。
「ルータの基本設定」	ルータの基本的なパラメータを設定するための手順を説明します。
「ワイヤレス デバイスの基本設定」	ワイヤレス デバイスの初期設定手順について説明します。
「無線の設定」	無線の設定の手順を説明します。

表記法

表 1 はこのマニュアルの表記法の一覧です。

表 1　　コマンドの表記法

表記法	説明
太字	コマンドおよびキーワード。
イタリック体	ユーザが値を指定する変数。
[　]	角カッコで囲んで表示される省略可能なキーワードまたは引数。
{**x** | **y** | **z**}	必須キーワードの選択肢は波カッコで囲み、縦棒で区切って示しています。いずれか 1 つを必ず選択します。
`screen フォント`	画面に表示される情報の例を表します。
`太字の screen フォント`	ユーザが入力しなければならない情報を表します。
< >	イタリック体が使用できない場合、パスワード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。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

（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 「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

関連資料

Cisco 880 シリーズ ISR に関する資料には、『*Cisco 880 シリーズ ISR ソフトウェア コンフィギュレーション ガイド*』（本書）のほかに、次のマニュアルがあります。

- *『Readme First for the Cisco 800 Series Integrated Services Routers』*
- *『Regulatory Compliance and Safety Information for Cisco 800 Series and SOHO Series Routers』*
- *『Declarations of Conformity and Regulatory Information for Cisco Access Products with 802.11n Radios』*
- *『Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2』*
- 『*Cisco IOS Release Notes* for Cisco IOS Release 15.1.4 (M)』

必要に応じて、以下のマニュアルもご参照ください。

- *『Cisco System Manager Quick Start Guide』*
- *『Cisco IOS Release 12.4 Quality of Service Solutions Configuration Guide』*
- *『Cisco IOS Security Configuration Guide, Release 12.4』*
- *『Cisco IOS Security Configuration Guide, Release 12.4T』*
- *『Cisco IOS Security Command Reference, Release 12.4』*
- *『Cisco IOS Security Command Reference, Release 12.4T』*
- *『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC』*
- *『Cisco Aironet 1240AG Access Point Support Documentation』*
- *『Cisco 4400 Series Wireless LAN Controllers Support Documentation』*
- *『LWAPP Wireless LAN Controllers』*
- *『LWAPP Wireless LAN Access Points』*
- *『Cisco IOS Release 12.4 Voice Port Configuration Guide』*
- *『SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateway』*
- *『Cisco Software Activation Conceptual Overview』*
- *『Cisco Software Activation Tasks and Commands』*

製品に関する資料の検索方法

Web ブラウザを使用して HTML マニュアルを検索するには、**Ctrl+F**（Windows）または **Cmd+F**（Apple）を使用します。ほとんどのブラウザには、単語単位の検索、大文字と小文字の区別、上または下に向かって検索するためのオプションもあります。

Adobe Reader で PDF を検索するには、基本的な [Find] ツールバー（**Ctrl+F**）を使用するか、[Full Reader Search] ウィンドウ（**Shift+Ctrl+F**）を使用します。1 つのマニュアルの中の単語や語句を検索するには、[Find] ツールバーを使用します。複数の PDF ファイルを一度に検索したり、大文字と小文字の区別などのオプションを変更する場合は、[Full Reader Search] ウィンドウを使用します。Adobe Reader には、PDF マニュアルの検索に関する詳細が記載されたオンライン ヘルプが付属しています。

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

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

製品概要

この章では、Cisco 880 シリーズ Integrated Service Router（ISR; サービス統合型ルータ）で利用できる機能の概要について説明します。この章の内容は次のとおりです。

全般的な機能

Cisco 880 ISR では、20 ユーザ未満の規模の在宅勤務者、リモート オフィス、および小規模オフィスに対して、インターネット、VPN、データ、バックアップの各機能が提供されます。これらのルータは、LAN ポートと WAN ポートの間でのブリッジングおよびマルチプロトコル ルーティング機能を備えており、アンチウイルスなどの高度な機能も提供します。さらに、Cisco 880W シリーズ ISR には、ISR がワイヤレス アクセス ポイントとして機能することを可能にする 802.11b/g/n 無線が組み込まれています。

Cisco 880 シリーズ ISR

Cisco 880 シリーズ ISR は、次のセクションで説明するように、構成が固定のデータ ルータ ファミリです。

また、この構成が固定のデータ ルータ ファミリはデュアルコア インフラストラクチャを使用しています。ホスト ルータ ソフトウェアは第 1 コアで実行され、WLAN AP ソフトウェアは第 2 コアで実行されます。

Cisco 880 シリーズ ISR のモデル

Cisco 880 シリーズ ISR は、データに対応しています。各ルータには WAN ポートが 1 つあります。また、データ バックアップ ポートをほとんどのルータで利用できます。802.11a/n または 802.11b/g/n のオプションは、すべてのモデルで使用できます。

表 1-1 は、Cisco 880 シリーズのデータ ルータのポート設定およびサポートされる WLAN 無線を示します。

表 1-1　Cisco 880 シリーズ データ ISR のポート設定とサポートされる WLAN 無線

モデル	WAN ポート	サポートされる WLAN 無線
C886VA-W-E-K9	ADSL2+ UR2	2.4 GHz
C887VAM-W-E-K9	ADSL2+ Annex M	2.4 GHz
C887VA-W-A-K9	ADSL2+ Annex A	2.4 GHz
C887VA-W-E-K9	ADSL2+ Annex A	2.4 GHz
C887VAGW+7-A-K9	VDSL2/ADSL2	2.4 GHz および 5 GHz
C887VAGW+7-E-K9	VDSL2/ADSL2	2.4 GHz および 5 GHz
C887VA-WD-A-K9	VDSL2/ADSL2	2.4 GHz および 5 GHz
C887VA-WD-E-K9	VDSL2/ADSL2	2.4 GHz および 5 GHz
C881W-A-K9	FE	2.4 GHz
C881W-E-K9	FE	2.4 GHz
C881W-P-K9	FE	2.4 GHz
C881GW+7-A-K9	FE	2.4 GHz および 5 GHz
C881GW+7-E-K9	FE	2.4 GHz および 5 GHz
C881WD-A-K9	FE	2.4 GHz および 5 GHz
C881WD-E-K9	FE	2.4 GHz および 5 GHz
C881GW-S-A-K9	FE	2.4 GHz および 5 GHz
C881GW-V-A-K9	FE	2.4 GHz および 5 GHz

3G 関連製品の詳細については、『*Configuring Cisco EHWIC and 880G for 3G (EV-DO Rev A)*』および『*Configuring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)*』を参照してください。

共通機能

Cisco 880 シリーズ ISR は次の機能をサポートしています。

- 「4 ポート 10/100 FE LAN スイッチ」（P.1-3）
- 「802.11b/g/n 無線 LAN」（P.1-3）
- 「バッテリ バックアップ式リアルタイム クロック」（P.1-3）
- 「Cisco CleanAir テクノロジー」（P.1-3）
- 「DFS（Dynamic Frequency Selection、動的周波数選択）」（P.1-3）
- 「デュアル無線ワイヤレス LAN」（P.1-4）
- 「セキュリティ機能」（P.1-4）

4 ポート 10/100 FE LAN スイッチ

このスイッチは、10/100BASE-T FE LAN、アクセス ポイント、IP 電話に接続するための 4 つのポートを備えています。工場出荷時に、アクセス ポイントまたは電話に電力を供給するための Power over Ethernet（PoE）が 2 つのポートで使用可能となるアップグレードが可能です。

802.11b/g/n 無線 LAN

Cisco 880W シリーズ ISR には、無線 LAN 接続のための、802.11b/g/n 無線モジュールが組み込まれています。このモジュールを使用することで、ルータはローカル インフラストラクチャの中でアクセス ポイントとして機能します。

サポートされる WLAN 無線モジュールの詳細については、表 1-1 を参照してください。

バッテリ バックアップ式リアルタイム クロック

バッテリ バックアップ式 Real-Time Clock（RTC; リアルタイム クロック）は、システムに電源が投入されているときに日付と時刻を提供します。RTC は、ルータに保存された認証局の正当性を検証するために使用されます。

Cisco CleanAir テクノロジー

Cisco CleanAir テクノロジーは、他のシステムが検知不可能な RF 干渉を検出し、その原因を識別してマップ上で特定し、ワイヤレスの受信可能範囲を最適化するための自動調整を行って電波品質を向上する、Cisco Unified Wireless Network のシステム全体に及ぶ機能です。

CleanAir テクノロジーを搭載した Cisco アクセス ポイントは、ミッション クリティカルなモビリティに高性能な 802.11n 接続を提供します。干渉をインテリジェントに回避することによって、アクセス ポイントは 802.11n ネットワークのパフォーマンス保護を提供し、信頼性の高いアプリケーション配信を実現します。

（注）　Cisco CleanAir テクノロジーはデュアル無線アクセス ポイントでのみサポートされます。

詳細については、「*Cisco CleanAir Technology*」を参照してください。

DFS（Dynamic Frequency Selection、動的周波数選択）

工場出荷時に 5 GHz 無線が設定されている、米国およびヨーロッパ向けのアクセス 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っています。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。

DFS 機能は、米国連邦通信委員会（FCC）の保留中の認証により、Cisco 880 シリーズ ISR ではディセーブルになっています。

（注）　DFS 機能はデュアル無線アクセス ポイントでのみサポートされます。

詳細については、「*Dynamic Frequency Selection and IEEE 802.11h Transmit Power Control*」を参照してください。

デュアル無線ワイヤレス LAN

デュアル無線/デュアルバンドの IEEE 802.11n アクセス ポイントを使用して、Cisco 880 シリーズ ISR は、単一デバイスでセキュアな統合アクセス ポイントを提供します。ISR は、自律モードと統合モードの両方をサポートし、802.11a/b/g との下位互換性があります。

ルータは、IEEE 802.11n ドラフト 2.0 をサポートし、スループット、信頼性、および予測可能性を向上させる、複数入力、複数出力（MIMO）テクノロジーを使用します。

Cisco 880 シリーズ ISR の設定の詳細については、「ルータの基本設定」（P.3-1）を参照してください。

セキュリティ機能

Cisco 880 プラットフォームは、次のセキュリティ機能を提供します。

- 侵入防御システム（IPS）
- Dynamic Multipoint VPN（DMVPN）
- IP セキュリティ（IPSec）
- Quality Of Service（QoS）
- ファイアウォール
- URL フィルタリング

ライセンス

Cisco 880 ISR には、ライセンスが付与されたソフトウェアがインストールされています。ソフトウェア機能のアップグレードや、ソフトウェア ライセンスの管理は、*Cisco License Manager* で行われる場合があります。詳細については、『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

新しいルータを注文する際、ソフトウェア イメージとフィーチャ セットを指定できます。イメージとフィーチャ セットはインストールされた状態で出荷されるため、ソフトウェア ライセンスを購入する必要はありません。ソフトウェア ライセンス ファイルは、ルータのフラッシュ メモリに格納されます。

フィーチャ セットの選択

一部のフィーチャ セットはルータに付属しており、ハードウェア プラットフォームにインストールされたソフトウェア ライセンスとともに提供されます。Cisco 880 のライセンスで使用できる機能の一覧については、『*Cisco 880 Series Integrated Services Routers Data Sheet*』を参照してください。ソフトウェア ライセンスのアクティブ化および管理方法の詳細については、Cisco.com の『*Software Activation Configuration Guide*』を参照してください。

次世代 880 SKU Cisco 880 シリーズ ISR プラットフォーム

次に、次世代 Cisco 880 シリーズ ISR プラットフォームに固有の SKU を示します。

C881W および C881WD

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 10/100 FE WAN
- 1 ポートのコンソール/補助ポート
- 1 ポートの外部 USB 2.0
- リアルタイム クロック
- 組み込み WLAN アンテナ（ワイヤレス モデル）

C886VA-W

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 1 ポートのコンソール/補助ポート
- 1 ポートの外部 USB 2.0
- ADSL2+ Annex B
- ISDN バックアップ WAN
- リアルタイム クロック
- 組み込み WLAN アンテナ（ワイヤレス モデル）

C887VAM-W

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 1 ポートのコンソール/補助ポート
- 1 ポートの外部 USB 2.0
- ADSL2+ Annex M
- リアルタイム クロック

- 組み込み WLAN アンテナ（ワイヤレス モデル）

C887VA-W および C887VA-WD

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 1 ポートのコンソール / 補助ポート
- 1 ポートの外部 USB 2.0
- ADSL2+ Annex A
- リアルタイム クロック
- 組み込み WLAN アンテナ（ワイヤレス モデル）

C887VAGW

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 1 ポートのコンソール / 補助ポート
- 1 ポートの外部 USB 2.0
- ADSL2+ Annex A
- リアルタイム クロック
- 組み込み WLAN アンテナ（ワイヤレス モデル）
- SIM カード スロットを 2 つ持つ 3G モデム

C881GW

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 10/100 FE WAN
- SIMM カード スロットを 2 つ持つ 3G モデム
- 1 ポートのコンソール / 補助ポート
- 1 ポートの外部 USB 2.0
- リアルタイム クロック

- 組み込み WLAN アンテナ（ワイヤレス モデル）

C887GW

- 512 MB のメモリ
- 256 MB のフラッシュ
- 4 ポートの 10/100 スイッチ
- 2 ポートの PoE（工場で設定するオプション）
- 1 ポートのコンソール / 補助ポート
- 1 ポートの外部 USB 2.0
- ADSL2+ Annex A
- SIMM カード スロットを 2 つ持つ 3G モデム
- リアルタイム クロック
- 組み込み WLAN アンテナ（ワイヤレス モデル）

3G 関連製品の詳細については、『*Configuring Cisco EHWIC and 880G for 3G (EV-DO Rev A)*』および『*Configuring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)*』を参照してください。

メモリ

表 1-2 に、第 1 コアと第 2 コアのオンボード メモリとフラッシュ サイズを示します。合計 512 MB のメモリと 256 MB のメモリがインストールされていて、次の表で示すようにパーティション化されています。

表 1-2　メモリ仕様

オンボード メモリ	第 1 コア	第 2 コア
512 MB	384 MB	128 MB
フラッシュ サイズ		
256	192	64

LED の概要

表 1-3 に、シャーシの正面（ベゼル側）にあるすべての LED を示します。I/O 側に LED はありません。

表 1-3　インターフェイスごとの LED 定義の概要

LED	色	説明	用途
PWR OK	緑	電源オン OK、ルータ動作可能	消灯 = 電源断 点灯 = 通常動作 点滅 = 起動フェーズ ROM モニタ モード
イーサネット スイッチおよび FE/GE LAN/WAN ポート	緑	イーサネット スイッチ	消灯 = リンクなし 点灯 = リンク 点滅 = TXD/RXD データ
PoE	緑/オレンジ	PoE ステータス	消灯 = 電源オンのデバイスなし、PoE は管理上ディセーブル 緑で点灯 = PD が接続され、電源がオン オレンジで点灯 = PD が電源を遮断、電源供給の異常
xDSL	緑	CD	点灯 = 接続 点滅 = トレーニング
	緑	データ	点滅 = TXD/RXD データ
ISDN データ	緑	リンク	消灯 = 接続なし 点灯 = BRI S/T 接続が確立
	緑	B1 チャネル データ	消灯 = データなし 点滅 = TXD/RXD データ
	緑	B2 チャネル データ	消灯 = データなし 点滅 = TXD/RXD データ

表 1-3　インターフェイスごとの LED 定義の概要 （続き）

LED	色	説明	用途
ワイヤレス /LAN	緑	2.4 GHz 無線	消灯 = 無線が停止（SSID 設定なし） 点灯 = 無線が稼働、SSID 設定済み、ビーコン送信中、クライアント アソシエート済み、送受信中のデータ トラフィックなし 低速点滅 = 無線が稼働（SSID 設定済み、ビーコン送信中） 高速点滅 = 無線が稼働、クライアント アソシエート済み、データ トラフィック送受信中
	緑	5 GHz の無線がサポートされている場合	
	緑	自律モード	消灯 = イーサネット リンクがダウン 点灯 = イーサネット リンクがアップ、トラフィックなし 点滅 = イーサネット リンクがアップ、データ トラフィックあり
		Unified モード	消灯 = イーサネット リンクがダウン 点灯 = イーサネット リンクがアップ、コントローラに接続済み 点滅 = AP がコントローラと通信していない
VPN_OK			消灯 = トンネルなし 点灯 = 1 つ以上のトンネルがアップ
PPP_OK			消灯 = PPP セッションなし 点灯 = 1 つ以上の PPP が確立済み

電源装置

次世代 Cisco 880 ISR プラットフォームでは、SKU に依存する次の電源装置を使用します。

12 VDC の外部電源アダプタ

すべての 86x および 88x モデルで、新しいアース付きの 12 VDC 30 W 外部デスクトップ アダプタを使用できます。1 つのバレル コネクタで、シャーシに接続します。

オンボード 12 VDC 電源装置

PoE ポートには、マザーボード上の 12 VDC から電源が供給されます。

Power over Ethernet インライン パワー オプション

インライン パワーは設定可能なオプションです。PoE が設定されたボックスには、30 W の代わりに 12 VDC 60 W アダプタで電源が供給されます。

サポートされるイメージ

c800-universalk9-mz

このイメージは、c8xx プラットフォームでサポートされるすべての IOS 機能を提供します。

c800-universalk9_npe-mz

このイメージは、VPN ペイロードとセキュアな音声機能をサポートせず、CIS 加盟国に関する重要な考慮事項を満たします。

各イメージのライセンス：

universalk9 イメージ用：

テクノロジー パッケージ ライセンス：

- Advipservices
- advsecurityk9

機能ライセンス：

- ios-ips-update
- SSL_VPN

universalk9_npe イメージ用：

テクノロジー パッケージ ライセンス：

- advipservices_npe
- advsecurity_npe

機能ライセンス：

- ios-ips-ipdate

AP802 でサポートされるイメージ

表 1-4　AP802 でサポートされるイメージ

モード	イメージ
自律	ap802-k9w7-tar
Unified	ap802-k9w8-tar
リカバリ	a802-rcvk9w8-tar

AP802 のサポートに必要なソフトウェアの最小バージョン

表 1-5 に、AP802 をサポートするために必要なソフトウェアの最小バージョンを示します。

表 1-5　AP802 に必要なソフトウェアの最小バージョン

ソフトウェア	AP802 シングル無線	AP802 デュアル無線
ルータ IOS	15.1(4) M1	15.2(4)M1
AP IOS（自律モード）	12.4(25d)JAX	12.4(25d)JAX1
AP IOS（Unified モード）	12.4(23c)JA2	15.2(2)JA
AP IOS（リカバリ モード）	12.4(23c)JA2	15.2(2)JA
WLC	7.0.116.0	7.3.101.0
WCS	7.0.172.0	—
NCS	—	1.2.0.103

CHAPTER 2

ワイヤレス デバイス概要

ワイヤレス デバイス（一般に *アクセス ポイント*として設定されます）は、セキュアでコストが低く使いやすい無線 LAN ソリューションを提供しています。この無線 LAN ソリューションは、企業レベルの機能とネットワーク技術者が要求する機動性および柔軟性を兼ね備えています。ワイヤレス デバイスは、アクセス ポイントとして設定された場合、無線および有線ネットワーク間の接続ポイントまたはスタンドアロン ワイヤレス ネットワークのセンター ポイントとして機能します。大規模なインストールでは、無線範囲内の無線ユーザは、構内を移動できる一方で、シームレスで中断のないネットワーク アクセスを維持できます。

Cisco IOS ソフトウェアをベースにした管理システムを使用し、ワイヤレス デバイスは Wi-Fi CERTIFIED(TM)、802.11b、802.11g および 802.11n に準拠した無線 LAN トランシーバとなります。

ソフトウェア モード

アクセス ポイントには自律イメージが付属し、アクセス ポイントのフラッシュにはリカバリ イメージが付属します。デフォルト モードは自律モードですが、Cisco Unified Wireless モードで動作するようにアクセス ポイントをアップグレードできます。

各モードの詳細は次のとおりです。

- **自律モード：**スタンドアロン ネットワーク コンフィギュレーションをサポートします。このモードでは、すべてのコンフィギュレーション設定がワイヤレス デバイス上にローカルに保存されます。各自律デバイスは起動コンフィギュレーションを独自に読み込んでも、ネットワーク上で緊密に動作できます。
- **Cisco Unified Wireless モード**：Cisco Unified Wireless LAN コントローラと連携して動作します。このモードでは、すべてのコンフィギュレーション情報がコントローラに保存されます。Cisco Unified Wireless LAN アーキテクチャでは、自律モードと対照的に、ワイヤレス デバイスは Lightweight Access Point Protocol（LWAPP）を使用する Lightweight モードで動作します。Lightweight アクセス ポイント（ワイヤレス デバイス）は、コントローラと関連付けられるまでコンフィギュレーションが設定されません。ワイヤレス デバイスのコンフィギュレーションは、ネットワークが起動中および実行中にだけ、コントローラから変更できます。コントローラは、ワイヤレス デバイスのコンフィギュレーション、ファームウェア、802.1x 認証などの制御トランザクションを管理します。すべての無線トラフィックはコントローラを通じてトンネリングされます。

  このネットワーク アーキテクチャ デザインの詳細については、『*Why Migrate to a Cisco Unified Wireless Network?*』を Cisco.com で参照してください。

管理オプション

ワイヤレス デバイスは、ルータ上の Cisco IOS ソフトウェアとは別の、独自のバージョンの Cisco IOS ソフトウェアを実行します。いくつかの異なるツールでアクセス ポイントを設定および監視できます。

- Cisco IOS ソフトウェア CLI
- Simple Network Management Protocol（SNMP）
- Web ブラウザ インターフェイス：
  http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

（注）　Web ブラウザ インターフェイスは、Windows 98、2000 および XP プラットフォーム上の Microsoft Internet Explorer バージョン 6.0、Windows 98、2000、XP および Solaris プラットフォーム上の Netscape バージョン 7.0 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 ツールを同時に使わないでください。CLI を使用してワイヤレス デバイスを設定すると、Web ブラウザ インターフェイスではコンフィギュレーションを正しく表示できない場合があります。このように正確でない情報が表示された場合でも、ワイヤレス デバイスに必ずしも正しくない設定がされたというわけではありません。

interface dot11radio グローバル コンフィギュレーション CLI コマンドを使用して、ワイヤレス デバイスを無線コンフィギュレーション モードにします。

ネットワークの構成例

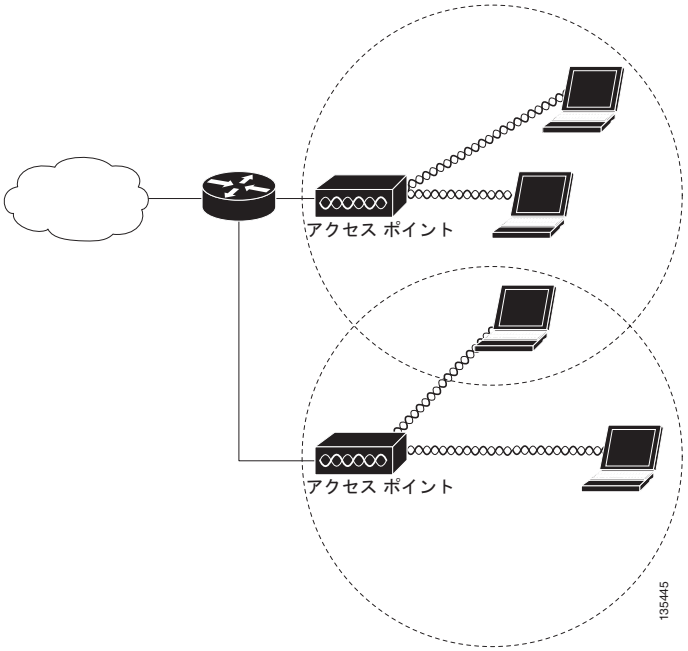
次の一般的なワイヤレス ネットワーク構成のいずれかでアクセス ポイント ロールを設定します。アクセス ポイントのデフォルト コンフィギュレーションは、有線 LAN に接続されているルート ユニット、または完全なワイヤレス ネットワークの中央ユニットにできます。アクセス ポイントはブリッジまたはワークグループのブリッジとしても構成できます。これらの役割には特定の構成が必要になります。次の各ページで例を挙げて説明します。

- 「ルート アクセス ポイント」（P.2-3）
- 「全ワイヤレス ネットワークの中央ユニット」（P.2-4）

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 2-1 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。

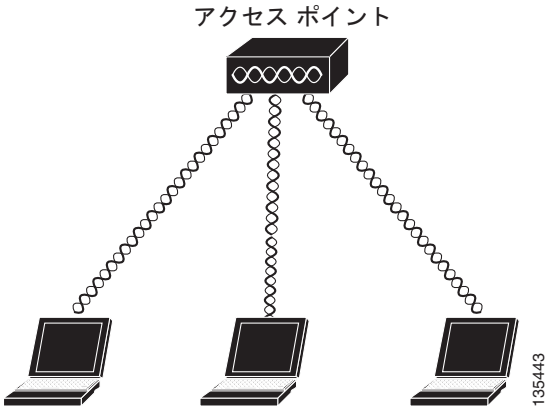
図 2-1　有線 LAN 上でルート ユニットとして機能するアクセス ポイント



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 2-2 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 2-2　　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 3

ルータの基本設定

この章では、Cisco ルータで基本的なパラメータ（グローバル パラメータの設定、ルーティング プロトコル、インターフェイス、およびコマンドライン アクセスなど）を設定する手順について説明します。また、起動時のデフォルト設定についても説明します。

（注） ルータの各モデルは、このマニュアルに記載されている機能の一部をサポートしていない場合があります。特定のルータでサポートされていない機能は、可能な限り明示されています。

この章では、該当するものがある場合には設定例と確認手順が記載されています。

インターフェイス ポート

表 3-1 は、各ルータでサポートされているインターフェイスと装置に表記されているポート ラベルを示しています。

表 3-1　Cisco ルータでサポートされているインターフェイスと対応するポート ラベル

ルータ	インターフェイス	ポート ラベル
Cisco 880	ファスト イーサネット LAN	LAN、FE0–FE3
	ワイヤレス LAN	（表示なし）
Cisco 881、881W、881G、881GW	ファスト イーサネット WAN	WAN、FE4
Cisco 886、886W、886G、886GW	ADSLoverISDN	ADSLoPOTS
Cisco 887、887W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 887V、887VW、887VG、887VGW	VDSL2oPOTS WAN	VDSLoPOTS
Cisco 888、888W	G.SHDSL WAN	G.SHDSL

デフォルト コンフィギュレーション

Cisco ルータを初めて起動すると、一部の基本的な設定はすでに行われています。LAN および WAN インターフェイスはすべて作成されており、コンソール ポートと VTY ポートの設定やネットワーク アドレス変換（NAT）用の内部インターフェイスの割り当てもすでに行われています。初期設定を表示するには、**show running-config** コマンドを使用します（次の Cisco 881W の例を参照してください）。

```
Router# show running-config


User Access Verification

Password:
Router> en
Password:
Router# show running-config
Building configuration...

Current configuration : 986 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$g4y5$NxDeM.0hON6YA51bcfGvN1
enable password ciscocisco
```

```
!
no aaa new-model
!
!
!
!
no ip routing
no ip cef
!
!
!
!
!
multilink bundle-name authe
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface FastEthernet0
!
interface FastEthernet1
 shutdown
!
interface FastEthernet2
 shutdown
!
interface FastEthernet3
 shutdown
!
interface FastEthernet4
 ip address 10.1.1.1 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface wlan-ap0
 description Service Module interface to manage the embedded AP
 ip unnumbered Vlan1
 no cdp enable
 arp timeout 0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
```

```
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 password cisco
 login
 transport input telnet ssh
!
scheduler max-task-time 5000

!
webvpn cef
end

Router#
```

設定に必要な情報

ネットワークを設定する前に、使用するネットワーク構成に基づいて、次の情報の一部またはすべてを収集しておく必要があります。

- インターネット接続を設定する場合、次の情報を収集してください。
  - ユーザのログイン名として割り当てられた PPP クライアント名
  - PPP 認証のタイプ : Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）または Password Authentication Protocol（PAP）
  - ISP アカウントにアクセスするための PPP パスワード
  - DNS サーバの IP アドレスおよびデフォルト ゲートウェイ
- 企業ネットワークへの接続を設定する場合は、ユーザとネットワーク管理者の間で、ルータの WAN インターフェイスに関する次の情報について打ち合わせておく必要があります。
  - PPP 認証のタイプ : CHAP または PAP
  - ルータにアクセスするための PPP クライアント名
  - ルータにアクセスするための PPP パスワード
- IP ルーティングを設定する場合、次の準備が必要です。
  - IP ネットワークのアドレス指定方式を作成します。
  - IP アドレスなどの IP ルーティング パラメータ情報と ATM Permanent Virtual Circuit（PVC; 相手先固定接続）を特定します。通常、これらの PVC パラメータは、Virtual Path Identifier（VPI; 仮想パス識別子）、Virtual Circuit Identifier（VCI; 仮想回線識別子）、およびトラフィック シェーピング パラメータです。
  - サービス プロバイダーから付与された PVC 番号、VPI、および VCI を特定します。
  - PVC ごとに、サポートされている AAL5 カプセル化のタイプを判別します。次のいずれかを指定できます。

    AAL5SNAP : これは、RFC 1483 ルーティングまたは RFC 1483 ブリッジングのいずれかです。RFC 1483 ルーティングの場合、サービス プロバイダーはスタティック IP アドレスを提供する必要があります。ブリッジング RFC 1483 の場合、DHCP を用いて IP アドレスを入手するか、サービス プロバイダーからスタティック IP アドレスを入手することもできます。

AAL5MUX PPP：このタイプでのカプセル化では、PPP 関連設定項目を判別する必要があります。

- ADSL または G.SHDSL 回線を使用して接続する場合、次の準備が必要です。
  - 電話会社と回線契約を結びます。

    ADSL 回線の場合：ADSL シグナリング タイプが DMT（ANSI T1.413 ともいう）または DMT Issue 2 であることを確認します。

    G.SHDSL 回線の場合：G.SHDSL 回線が ITU G.991.2 規格に準拠し、Annex A（北米）または Annex B（欧州）をサポートしていることを確認します。

該当する情報の収集が済んだら、ルータの設定を行うことができます。「コマンドライン アクセスの設定」（P.3-5）から設定を始めてください。

ソフトウェア ライセンスを取得または変更するには、『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

コマンドライン アクセスの設定

ルータへのアクセスを制御するパラメータを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
2. **password** *password*
3. **login**
4. **exec-timeout** *minutes* [*seconds*]
5. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
6. **password** *password*
7. **login**
8. **end**

手順の詳細

	コマンド	目的

ステップ 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	例：
	`Router(config)# line console 0`
	`Router(config-line)#`
		回線コンフィギュレーション モードを開始します。続いて、回線のタイプを指定します。
		この例では、アクセス用にコンソール端末を指定します。

ステップ 2	**password** *password*
	
	例：
	`Router(config)# password 5dr4Hepw3`
	`Router(config-line)#`
		コンソール端末回線に固有のパスワードを指定します。

	コマンド	目的

ステップ 3	**login**
	
	例：
	`Router(config-line)# login`
	`Router(config-line)#`
		端末セッション ログイン時のパスワード チェックをイネーブルにします。

ステップ 4	**exec-timeout** *minutes* [*seconds*]
	
	例：
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		ユーザ入力が検出されるまで EXEC コマンド インタープリタが待機する間隔を設定します。デフォルトは 10 分です。任意で、間隔値に秒数を追加します。
		この例では、5 分 30 秒のタイムアウトを表示します。「0 0」のタイムアウトを入力すると、タイムアウトが発生しません。

ステップ 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	例：
	`Router(config-line)# line vty 0 4`
	`Router(config-line)#`
		リモート コンソール アクセス用の仮想端末を指定します。

ステップ 6	**password** *password*
	
	例：
	`Router(config-line)# password aldf2ad1`
	`Router(config-line)#`
		仮想端末回線に固有のパスワードを指定します。

ステップ 7	**login**
	
	例：
	`Router(config-line)# login`
	`Router(config-line)#`
		仮想端末セッション ログイン時のパスワード チェックをイネーブルにします。

ステップ 8	**end**
	
	例：
	`Router(config-line)# end`
	`Router#`
		回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

例

次の設定は、コマンドライン アクセス コマンドを示します。

「default」と記されているコマンドは入力不要です。これらのコマンドは、**show running-config** コマンドを使用すると、生成されたコンフィギュレーション ファイルに自動的に表示されます。

```
!
line con 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

グローバル パラメータの設定

ルータに選択したグローバル パラメータを設定するには、次の作業を行います。

手順の概要

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *password*
4. **no ip domain-lookup**

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		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（コンソール ポート使用時）。
		リモート端末を使用してルータに接続している場合は、次のコマンドを使用します。
		`telnet router name or address`
		`Login: login id`
		`Password: *********`
		`Router> enable`

ステップ 2	**hostname** *name*
	
	例：
	`Router(config)# hostname Router`
	`Router(config)#`
		ルータ名を指定します。

ステップ 3	**enable secret** *password*
	
	例：
	`Router(config)# enable secret cr1ny5ho`
	`Router(config)#`
		ルータへの不正なアクセスを防止するには、暗号化パスワードを指定します。

ステップ 4	**no ip domain-lookup**
	
	例：
	`Router(config)# no ip domain-lookup`
	`Router(config)#`
		ルータが未知の単語（入力ミス）を IP アドレスに変換しないようにします。

WAN インターフェイスの設定

必要に応じて、次のいずれかの手順を行い、ルータの WAN インターフェイスを設定します。

- 「ファスト イーサネット WAN インターフェイスの設定」（P.3-8）
- 「VDSL2 WAN インターフェイスの設定」（P.3-8）
- 「Cisco Multi Mode 886VA および 887VA ISR での ADSL または VDSL の設定」（P.3-9）
- 「ADSL モードの設定」（P.3-10）

ファスト イーサネット WAN インターフェイスの設定

Cisco 861 または 881 ISR でファスト イーサネット インターフェイスを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **interface** ***type number***
2. **ip address** *ip-address mask*
3. **no shutdown**
4. **exit**

手順の詳細

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		ルータのファスト イーサネット WAN インターフェイス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 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-if)#`
		指定されたファスト イーサネット インターフェイスの IP アドレスおよびサブネット マスクを設定します。

ステップ 3	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		イーサネット インターフェイスをイネーブルにして、インターフェイスの状態を管理上のダウンからアップに変更します。

ステップ 4	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ファスト イーサネット インターフェイスのコンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

VDSL2 WAN インターフェイスの設定

Cisco 887V ISR プラットフォームでは、VDSL2 WAN インターフェイスが使用されます。

（注）　VDSL2 WAN インターフェイスは、レイヤ 2 転送メカニズムとしてイーサネットを使用します。

Cisco 887V ISR で VDSL2 を設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **controller** *vdsl 0*
2. **interface** ***type number***

3. **ip address** *ip-address mask*
4. **shutdown**
5. **no shutdown**
6. **exit**

手順の詳細

	コマンド	目的

ステップ 1	**controller** *vdsl 0*
	
	例：
	`Router# config t`
	`Router(config)# controller vdsl 0`
		コントローラのコンフィギュレーション モードを開始し、コントローラ番号を入力します。
		（注） CPE 側から VDSL2 パラメータを設定する必要はありません。DSLAM 側で特定の VDSL2 設定を実施する必要があります。

ステップ 2	**interface** *type number*
	
	例：
	`Router(config)# interface ethernet 0`
	`Router(config-if)#`
		ルータ上の VDSL WAN インターフェイスを通してイーサネット レイヤ 2 転送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 3	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-if)#`
		インターフェイスに IP アドレスとサブネット マスクを設定します。

ステップ 4	**shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		インターフェイスをディセーブルにします。状態が管理アップから管理ダウンに変化します。

ステップ 5	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		インターフェイスをイネーブルにします。状態が管理ダウンから管理アップに変化します。

ステップ 6	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

Cisco Multi Mode 886VA および 887VA ISR での ADSL または VDSL の設定

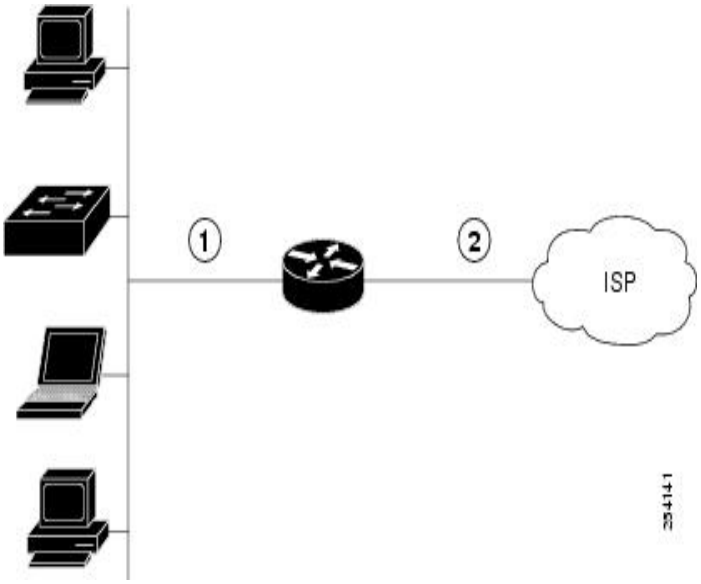
シスコの加入者宅内機器（CPE）886VA および 887VA Integrated Services Router（ISR）は、マルチモードとも呼ばれる、非対称デジタル加入者線（ADSL）1/2/2+ と超高速デジタル加入者線 2（VDSL2）の伝送モードをサポートします。886VA は xDSL over ISDN をサポートし、887VA は xDSL over Plain Old Telephone System（POTS）をサポートします。

デフォルトの CPE 動作モードは auto です。auto モードとは、CPE が Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）に設定されているモード、ADSL1/2/2+ または VDSL2 にトレーニングされるという意味です。

次の例では、DSLAM が ADSL2+ モードまたは VDSL2 で設定されていて、CPE が auto モードで設定されているものとします。

図 3-1 に、ATM WAN またはイーサネット WAN ネットワーク トポロジを示します。

図 3-1　　トポロジの例



1	Fast Ethernet LAN interface	2	ATM WAN interface—ADSL1/2/2+ mode or Ethernet WAN Interface—VDSL2 mode

（注） レイヤ 1 の DSLAM は auto モード用に設定できます。レイヤ 2 の DSLAM は、ATM モードまたは Packet Transfer Mode（PTM）用に設定する必要があります。

（注） Cisco 886VA および 887VA では、最大 4 つの Permanent Virtual Circuit（PVC; 相手先固定接続）が可能です。

ADSL モードの設定

ADSL モードを設定するには、次の作業を行ってください。

- 「ADSL auto モードの設定」（P.3-11）
- 「ADSL モードの CPE およびピアの設定」（P.3-11）
- 「ADSL の設定例」（P.3-13）

- 「ADSL 設定の確認」（P.3-14）
- 「ADSL の CPE からピアへの接続の確認」（P.3-16）

ADSL auto モードの設定

DSL コントローラを auto モードに設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

（注）　ルータを設定する前に、DSLAM を ADSL 1/2//2+ モードに設定します。

手順の概要

1. **controller vdsl** ***slot***
2. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansl}**
3. **end**

手順の詳細

	コマンド	目的

ステップ 1	**controller vdsl** ***slot***
	例：
	`Router (config) #`
	`Controller vdsl 0`
		VDSL コントローラ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 2	**operating mode {auto|adsl1|adsl2|adsl2+|vdsl2|ansl}**
	例：
	`Router (config-controller) #`
	`operating mode`
	`auto`
		動作モードを設定します。デフォルトは auto で、これが推奨されるモードです。

ステップ 3	**end**
	例：
	`Router (config-conroller) #`
	`end`
	`Router`
		コンフィギュレーション モードを終了し、EXEC モードを開始します。

auto で設定した場合は、**show running** コマンドで動作モードが表示されません。

ADSL モードの CPE およびピアの設定

ADSL を設定するとき、ATM メイン インターフェイスまたは ATM サブ インターフェイスは、PVC と IP アドレスで設定する必要があります。必要に応じて、インターフェイスで **no shutdown** コマンドを実行します。

ATM CPE 側の設定

ATM CPE 側を設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **interface** ***type number***
2. **no shutdown**
3. **interface atm0.1 point-to-point**
4. **ip address** *ip-address mask*
5. **pvc [name] vpi/vci**
6. **protocol** *protocol* {*protocol-address* [**virtual-template**] | **inarp**} [[**no**] **broadcast** | **disable-check-subnet** | [**no**] **enable-check-subnet**]
7. **end**

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* 例： `Router (config) # interface atm0`	ATM WAN インターフェイス（ATM0）で、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 shutdown**
	例：
	`Router (config-if) # no shutdown`
	`Router (config-if) #`
		ATM インターフェイスに対する設定変更をイネーブルにします。

ステップ 3	**interface atm0.1 point-to-point**
	例：
	`Router (config-if) # interface ATM0.1`
	`point-to-point`
	`Router (config-subif) #`
		ATM0.1 ポイントツーポイント インターフェイスをイネーブルにします。

ステップ 4	**ip address** *ip-address mask* 例： `Router (config-subif)# ip address 30.0.0.1 255.255.255.0`	IP アドレスとサブネット マスクを入力します。

ステップ 5	**pvc [name] vpi/vci**
	例：
	`Router (config-subif) # pvc 13/32`
	`Router (config-if-atm-vc) #`
		ATM PVC に名前を割り当てるかまたは名前を作成し、ATM 仮想回線コンフィギュレーション モードを開始します。

ステップ 6	**protocol** ***protocol*** {*protocol-address* [**virtual-template**]	**inarp**} [[**no**] **broadcast**	**disable-check-subnet**	[**no**] **enable-check-subnet**]
				例：
				`Router (config-if-atm-vc) #`
				`protocol ip 30.0.0.2 broadcast`
					ATM PVC のスタティック マップを設定します。

ステップ 7	**end**
	例：
	`Router (config-if-atm-vc) # end`
	`Router #`
		コンフィギュレーション モードを終了し、EXEC モードを開始します。

ADSL の設定例

次に、auto モードに設定する一般的な ADSL2+ 設定例を示します。**太字**で表示された箇所が重要です。

```
Router# show running
Building configuration...

Current configuration  :    1250 bytes
!
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level adviperservices
!
!
vtp domain cisco
vtp mode transparet
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet 0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
```

```
 isdn termintation multidrop
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 15/32
  protocol ip 30.0.0.2 broadcast
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-palne
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

ADSL 設定の確認

特権 EXEC モードで **show controller vdsl 0** コマンドを使用して、正しく構成が設定されていることを確認します。**太字**で表示された箇所が重要です。

```
Router# show controller vdsl 0
Controller VDSL 0 is UP


Daemon Status:                Up
                             XTU-R (DS)             XTU-C (US)
chip Vendor ID:               'BDM'                  'BDCM'
Chip Vendor Specific:         0x0000                 0x6110
Chip Vendor Country:          0xB500                 0xB500
```

```
Modem Vendor ID:              'csco'                  'BDCM'
Modem Vendor Specific:        0x4602                  0x6110
Modem Vendor Country:         0xB500                  0xB500
Serial Number Near:           FHK1313227E 887-V2-K 15.1(20100
Serial Number Far:
Modem Version Nead:           15.1(20100426:193435) [changahn
Modem Version Far:            0x6110


Modem Status:                 TC Sync (Showtime!)
DSL Config Mode:              AUTO
Trained Mode:                 G.992.5 (ADSL2+) Annex A
TC Mode:                      ATM
Selftest Result:              0x00
DELT configuration:           disabled
DELT state:                   not running
Trellis:                      ON                      ON
Line Attenuation:             1.0 dB                  1.4 dB
Signal Attenuation:           1.0 dB                  0.0 dB
Noise Margin:                 6.8 dB                  13.6 dB
Atteinable Rate:              25036 kbits/s           1253 kbits/s
Actual Power:                 13.7 dBm                12.3 dBM
Total FECS:                   0                       0
Total ES:                     0                       0
Total SES:                    0                       0
Total LOSS:                   0                       0
Total UAS:                    0                       0
Total LPRS:                   0                       0
Total LOFS:                   0                       0
Total LOLS:                   0                       0
Bit swap:                     163                     7

Full inits:                   32
Failed Full inits:            0
Short inits:                  0
Failed short inits:           0


Firmware          Source          Filename (version)
--------          ------          ------------------
VDSL              embedded        VDSL_LINUX_DEV_01212008 (1)


Modem FW Version:         100426_1053-4.02L.03.A2pv6C030f.d22j
Modem PHY Version:        A2pv6C030f.d22j


                DS Channel1   DS Channel0  US Channel1  US channel0
Speed (kbps):             0         24184            0         1047
Previous Speed:           0         24176            0         1047
Total Cells:              0     317070460            0     13723742
User Cells:               0             0            0            0
Reed-solomon EC:          0             0            0            0
CRC Errors:               0             0            0            0
Header Errors:            0             0            0            0
Interleave (ms):      0.00          0.08         0.00        13.56
Actual INP:           0.00          0.00         0.00         1.80


Training Log:   Stopped
Training Log Filename:  flash:vdsllog.bin
```

ADSL の CPE からピアへの接続の確認

ピアに ping を発行し、CPE からピアへの構成が正しく設定されていることを確認します。

```
Router# ping 30.0.0.2 rep 20

Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 30.0.0.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 20/22/28 ms
Router#
```

ファスト イーサネット LAN インターフェイスの設定

ルータのファスト イーサネット LAN インターフェイスは、デフォルト VLAN の一部として自動的に設定され、個別のアドレスによる設定は行われません。アクセスは VLAN を通じて提供されます。このインターフェイスを別の VLAN に割り当てることが可能です。

無線 LAN インターフェイスの設定

Cisco 880 シリーズ ワイヤレス ルータは、無線 LAN 接続用の統合 802.11n モジュールを備えています。このルータは、ローカル インフラストラクチャのアクセス ポイントとして機能できます。ワイヤレス接続の設定の詳細については、「ワイヤレス デバイスの基本設定」（P.4-1）を参照してください。

ループバック インターフェイスの設定

ループバック インターフェイスは、スタティック IP アドレスのプレースホルダーとして機能し、デフォルトのルーティング情報を提供します。

ループバック インターフェイスを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **exit**

手順の詳細

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface Loopback 0`
	`Router(config-if)#`
		ループバック インターフェイス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 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-if)#`
		ループバック インターフェイスの IP アドレスとサブネット マスクを設定します。

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例

このコンフィギュレーション例のループバック インターフェイスは、仮想テンプレート インターフェイス上の NAT をサポートするために使用されています。この設定例は、スタティック IP アドレスとなる IP アドレス 200.200.100.1/24 を持つファスト イーサネット インターフェイスに設定されるループバック インターフェイスを示します。ループバック インターフェイスは、ネゴシエートされた IP アドレスを持つ virtual-template1 にポイントバックします。

```
!
interface loopback 0
ip address 200.200.100.1 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
!
```

設定の確認

ループバック インターフェイスが正しく設定されたかどうかを確認するには、**show interface loopback** コマンドを入力します。次の例のような確認用の出力が表示されます。

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
```

```
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ping を実行することによって、ループバック インターフェイスを確認する方法もあります。

```
Router# ping 200.200.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

スタティック ルートの設定

スタティック ルートは、ネットワークを介した固定ルーティング パスを提供します。これらは、ルータ上で手動で設定されます。ネットワーク トポロジが変更された場合には、スタティック ルートを新しいルートに更新する必要があります。スタティック ルートは、ルーティング プロトコルによって再配信される場合を除き、プライベート ルートです。

スタティック ルートを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **end**

手順の詳細

	コマンド	目的

ステップ 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
	`Router(config)#`
		IP パケットのスタティック ルートを指定します。
		このコマンドの詳細および設定可能なその他のパラメータについては、『*Cisco IOS IP Routing Protocols Command Reference*』を参照してください。

ステップ 2	**end**
	
	例：
	`Router(config)# end`
	`Router#`
		ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

次の設定例で、スタティック ルートは、ファスト イーサネット インターフェイスで宛先 IP アドレス 192.168.1.0 およびサブネット マスク 255.255.255.0 を持つすべての IP パケットを、IP アドレス 10.10.10.2 を持つ別のデバイスに送信します。具体的には、パケットが設定済みの PVC に送信されます。

「**(default)**」と記されているコマンドの入力は不要です。このコマンドは、**show running-config** コマンドを使用すると、生成されたコンフィギュレーション ファイルに自動的に表示されます。

```
!
ip classless (default)
ip route 192.168.1.0 255.255.255.0 10.10.10.2!
```

設定の確認

スタティック ルーティングが正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、「S」で表されるスタティック ルートを探します。

次のような確認用の出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, FastEthernet0
```

ダイナミック ルートの設定

ダイナミック ルーティングでは、ネットワーク トラフィックまたはトポロジに基づいて、ネットワーク プロトコルがパスを自動調整します。ダイナミック ルーティングの変更は、ネットワーク上の他のルータにも反映されます。

Cisco ルータは、Routing Information Protocol（RIP; ルーティング情報プロトコル）または Enhanced Interior Gateway Routing Protocol（EIGRP）などの IP ルーティング プロトコルを使用して、動的にルートを学習します。いずれかのルーティング プロトコルをルータに設定できます。

- 「Routing Information Protocol の設定」（P.3-20）
- 「拡張インテリア ゲートウェイ ルーティング プロトコルの設定」（P.3-21）

Routing Information Protocol の設定

ルータに RIP ルーティング プロトコルを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **router rip**
2. **version** {**1** | **2**}
3. **network** *ip-address*
4. **no auto-summary**
5. **end**

手順の詳細

	コマンド	作業

ステップ 1	**router rip**
	
	例：
	`Router> configure terminal`
	`Router(config)# router rip`
	`Router(config-router)#`
		ルータ コンフィギュレーション モードを開始します。続いて、ルータの RIP をイネーブルにします。

ステップ 2	**version** {**1**	**2**}
		
		例：
		`Router(config-router)# version 2`
		`Router(config-router)#`
			RIP version 1 または 2 の使用を指定します。

ステップ 3	**network** *ip-address*
	
	例：
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
	`Router(config-router)#`
		直接接続しているネットワークの各アドレスを使用して、RIP を適用するネットワーク リストを指定します。

ステップ 4	**no auto-summary**
	
	例：
	`Router(config-router)# no auto-summary`
	`Router(config-router)#`
		ネットワークレベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。これにより、サブプレフィックス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。

ステップ 5	**end**
	
	例：
	`Router(config-router)# end`
	`Router#`
		ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

次の設定例は、IP ネットワーク 10.0.0.0 および 192.168.1.0 でイネーブルにされる RIP version 2 を示します。

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

```
!
Router# show running-config
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
```

設定の確認

RIP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、「R」で表される RIP ルートを探します。次の例のような確認用の出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0
```

拡張インテリア ゲートウェイ ルーティング プロトコルの設定

ルータに Enhanced Interior Gateway Routing Protocol（EIGRP; 拡張インテリア ゲートウェイ ルーティング プロトコル）を設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **router eigrp** *as-number*
2. **network** *ip-address*
3. **end**

手順の詳細

	コマンド	目的

ステップ 1	**router eigrp** *as-number*
	
	例：
	`Router(config)# router eigrp 109`
	`Router(config)#`
		ルータ コンフィギュレーション モードを開始して、ルータ上で EIGRP をイネーブルにします。Autonomous System（AS; 自律システム）番号は、他の EIGRP ルータへのルートを識別します。また、EIGRP 情報のタグ付けに使用されます。

ステップ 2	**network** *ip-address*
	
	例：
	`Router(config)# network 192.145.1.0`
	`Router(config)# network 10.10.12.115`
	`Router(config)#`
		EIGRP を適用するネットワークのリストを指定します（直接接続されているネットワークの IP アドレスを使用）。

ステップ 3	**end**
	
	例：
	`Router(config-router)# end`
	`Router#`
		ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例

次の設定例は、IP ネットワーク 192.145.1.0 および 10.10.12.115 でイネーブルにされる EIGRP ルーティング プロトコルを示します。EIGRP の自律システム番号として、109 が割り当てられています。

設定を表示するには、特権 EXEC モードで開始し、**show running-config** コマンドを使用します。

```
!
router eigrp 109
    network 192.145.1.0
        network 10.10.12.115
!
```

設定の確認

IP EIGRP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、「D」で表される EIGRP ルートを探します。次のような確認用の出力が表示されます。

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CHAPTER 4

ワイヤレス デバイスの基本設定

この章では、Cisco 880 Series Integrated Services Router（ISR; サービス統合型ルータ）での自律ワイヤレス デバイスの設定方法について説明します。

（注） 自律ソフトウェアを組み込みワイヤレス デバイス上で Cisco Unified ソフトウェアにアップグレードするには、「Cisco Unified ソフトウェアへのアップグレード」（P.4-9）で手順を参照してください。

ワイヤレス デバイスは組み込み型で、接続用の外部コンソール ポートはありません。ワイヤレス デバイスを設定するには、コンソール ケーブルでパーソナル コンピュータをホスト ルータのコンソール ポートに接続して次の手順に従って接続を確立し、ワイヤレス設定を行います。

無線コンフィギュレーション セッションの開始

（注） ルータのセットアップでワイヤレス デバイスを設定する*前*に、後述の手順に従ってルータとアクセス ポイントとの間でセッションを開く必要があります。

以下のコマンドを、グローバル コンフィギュレーション モードでルータの Cisco IOS CLI 上に入力します。

手順の概要

1. **interface wlan-ap0**
2. **ip address *subnet mask***
3. **no shutdown**
4. **interface vlan1**
5. **ip address *subnet mask***
6. **exit**
7. **exit**
8. **service-module wlan-ap 0 session**

手順の詳細

	コマンド	目的

ステップ 1	**interface wlan-ap0**
	
	例：
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		ワイヤレス デバイスへの、ルータのコンソール インターフェイスを定義します。このインターフェイスは、ルータのコンソールとワイヤレス デバイス間の通信に使用します。
		常にポート 0 を使用します。
		次のメッセージが表示されます。
		
		`The wlan-ap 0 interface is used for managing the embedded AP. Please use the` **`service-module wlan-ap 0 session`** `command to console into the embedded AP.`

ステップ 2	**ip address *subnet mask***
	
	例：
	`router(config-if)# ip address 10.21.0.20 255.255.255.0`
	
	`or`
	`router(config-if)# ip unnumbered vlan1`
		インターフェイス IP アドレスとサブネット マスクを指定します。
		（注） この IP アドレスは、**ip unnumbered vlan1** コマンドを使用することで、Cisco ISR に割り当てられた IP アドレスと共有できます。

ステップ 3	**no shutdown** **例：** `router(config-if)# no shutdown`	内部インターフェイス接続を開いた状態を維持するように指定します。

	コマンド	目的
ステップ 4	**interface vlan1** **例：** `router(config-if)# interface vlan1`	データ通信のために、内部 Gigabit Ethernet（GE0; ギガビット イーサネット）0 ポート上で仮想 LAN インターフェイスを別のインターフェイスに指定します。 • Cisco 880 シリーズの ISR では、すべてのスイッチ ポートがデフォルトの vlan1 インターフェイスを継承します。
ステップ 5	**ip address** ***subnet mask*** **例：** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	インターフェイス IP アドレスとサブネット マスクを指定します。

ステップ 6	**exit**
	
	例：
	`router(config-if)# exit`
	`router(config)#`
		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。

ステップ 7	**exit**
	
	例：
	`router(config)# exit`
	`router#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**service-module wlan-ap 0 session**
	
	例：
	`router# service-module wlan-ap0 session`
	`Trying 10.21.0.20, 2002 ... Open`
	
	`ap>`
		ワイヤレス デバイスとルータのコンソール間の接続をオープンにします。

ヒント　ワイヤレス デバイスとのセッションを開始するコンソールに Cisco IOS ソフトウェア エイリアスを作成する場合は、EXEC プロンプトから **alias exec dot11radio service-module wlan-ap 0 session** コマンドを入力します。

セッションの終了

ワイヤレス デバイスとルータのコンソールとの間のセッションを閉じるには、次の手順に従います。

ワイヤレス デバイス

1. **Ctrl+Shift+6**、**x**

ルータ

1. **disconnect** コマンドを入力します。
2. Enter を押します。

無線環境の設定

（注）　ワイヤレス デバイスを初めて設定する場合は、基本のワイヤレス設定の前に、アクセス ポイントとルータとの間でコンフィギュレーション セッションを開始する必要があります。「無線コンフィギュレーション セッションの開始」（P.4-2）を参照してください。

ワイヤレス デバイスのソフトウェアに適合するツールを使用してデバイスを設定します。

- 「Cisco Express 設定」（P.4-4）：ユニファイド ソフトウェア
- 「Cisco IOS コマンドライン インターフェイス」（P.4-5）：自律ソフトウェア

（注）　自律モードでワイヤレス デバイスを実行していて Unified モードにアップグレードするには、「Cisco Unified ソフトウェアへのアップグレード」（P.4-9）でアップグレードの手順を参照してください。

Cisco Unified Wireless ソフトウェアへのアップグレード後、次の URL で Web ブラウザ インターフェイスを使用してデバイスを設定します。
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express 設定

自律ワイヤレス デバイスを設定するには、次の手順に示すように、Web ブラウザ ツールを使用します。

ステップ 1　ワイヤレス デバイスとのコンソール接続を確立し、**show interface bvi1** Cisco IOS コマンドを入力して、ブリッジ グループ仮想インターフェイス（BVI）IP アドレスを取得します。

ステップ 2　ブラウザのウィンドウを開き、ブラウザ ウィンドウのアドレス行にこの BVI IP アドレスを入力します。Enter 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　ユーザ名を入力します。*Cisco* はデフォルトのユーザ名です。

ステップ 4　ワイヤレス デバイスのパスワードを入力します。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。Web ブラウザの設定ページの使用方法の詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS コマンドライン インターフェイス

自律ワイヤレス デバイスを設定するには、Cisco IOS CLI ツールを使用して次の作業を行います。

- 「無線の設定」（P.4-5）
- 「無線セキュリティ設定の実行」（P.4-5）
- 「無線 QoS の設定」（P.4-8）（任意）

無線の設定

自律モードまたは Cisco Unified モードで信号を伝送するために、ワイヤレス デバイスの無線パラメータを設定します。特定の設定手順については、「無線の設定」（P.5-1）を参照してください。

無線セキュリティ設定の実行

- 「認証の設定」（P.4-5）
- 「ローカル認証システムとしてのアクセス ポイント設定」（P.4-6）
- 「WEP および暗号スイートの設定」（P.4-6）
- 「無線 VLAN の設定」（P.4-6）
- 「SSID の割り当て」（P.4-7）

認証の設定

認証の種類は、Service Set Identifiers（SSID; サービス セット識別子）に準拠します。SSID はアクセス ポイントに設定されます。同一のアクセス ポイントを持つ複数の種類のクライアント デバイスで使用するために、複数の SSID を設定します。

アクセス ポイントを介したワイヤレス クライアント デバイスとネットワークとの通信を開始する前に、クライアント デバイスは、公開キーまたは共用キーによる認証によってアクセス ポイントを認証する必要があります。安全性を最大限にするために、クライアント デバイスは MAC アドレスまたは Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証を使用してネットワークも認証する必要があります。いずれの認証タイプもネットワークの認証サーバを信頼します。

認証タイプを選択するには、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html の『*Authentication Types for Wireless Devices*』を参照してください。

最大限のセキュリティ環境を設定するには、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html の『*RADIUS and TACACS+ Servers in a Wireless Environment*』を参照してください。

ローカル認証システムとしてのアクセス ポイント設定

ローカルの認証サービスまたはバックアップ認証サービスを障害が発生した WAN リンクまたはサーバに提供するために、アクセス ポイントをローカルの認証サーバとして機能するように設定できます。アクセス ポイントは、Lightweight Extensible Authentication Protocol（LEAP）認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証または MAC ベースの認証を使用して最大 50 のワイヤレス クライアント デバイスを認証することができます。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 オーセンティケータでのアクセス ポイントの設定は、クライアントのユーザ名とパスワードを使用して手動で行います。これは、ローカル オーセンティケータのデータベースが RADIUS サーバと同期化されないためです。クライアントが使用できる VLAN および SSID のリストを指定できます。

ワイヤレス デバイスにこの機能をセットアップする詳細については、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html
の『*Using the Access Point as a Local Authenticator*』を参照してください。

WEP および暗号スイートの設定

Wired Equivalent Privacy（WEP）暗号はワイヤレス デバイス間での伝送データをスクランブルして、通信機密を保持します。ワイヤレス デバイスおよびそのワイヤレス クライアント デバイスは、同一の WEP キーを使用してデータの暗号化および複合化を行います。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 メッセージとは、ネットワーク上の 1 個のデバイスに向けて送信されるメッセージです。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。

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。Wi-Fi Protected Access（WPA）または Cisco Centralized Key Management（CCKM）をイネーブルにするには、暗号スイートを使用する必要があります。

Temporal Key Integrity Protocol（TKIP）を含む暗号スイートは無線 LAN にとって最適な安全性を提供します。WEP だけしか含まない暗号化スイートでは、最低限のセキュリティしかありません。

暗号化の手順については、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
の『*Configuring WEP and Cipher Suites*』を参照してください。

無線 VLAN の設定

無線 LAN で VLAN を使用し、SSID を VLAN に割り当てると、「セキュリティの種類」（P.4-7）で定義されている 4 種類のセキュリティ設定のいずれかを使用して複数の SSID を作成できます。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、単一のブリッジング ドメインに接続されている複数のエンド システム（ホスト、またはブリッジやブリッジやルータなどのネットワーク装置）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によりサポートされます。ネットワーク機器には、各 VLAN 用の別個のプロトコル グループとともに、ブリッジング プロトコルをそれらの間で動作させる LAN スイッチなどがあります。

無線 VLAN アーキテクチャの詳細については、
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html の
『*Configuring Wireless VLANs*』を参照してください。

（注） 無線 LAN で VLAN を使用*しない*と、SSID に割り当てることができるセキュリティ オプションが制限されます。これは、Express Security ページで暗号化設定と認証タイプが対応付けられているためです。

SSID の割り当て

アクセス ポイントとして機能するワイヤレス デバイスには最大 16 個の SSID を設定できます。また、SSID ごとに一意のパラメータ セットを設定できます。たとえば、ある SSID ではネットワーク アクセスだけを利用者に許可し、別の SSID では認証したユーザであれば機密データへのアクセスを許可するといった利用法が可能です。

複数の SSID の作成の詳細については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html の『*Service Set Identifiers*』を参照してください。

（注） VLAN を使用しない場合、暗号化設定（WEP と暗号）が 2.4GHz 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 がディセーブルの状態でスタティック WEP を使用する SSID を作成した場合は、WPA 認証を使用する SSID を別途作成できません。使用される暗号化設定が異なるためです。ある SSID のセキュリティ設定と、別の SSID の設定が競合していた場合、1 つ以上の SSID を削除して競合を解消できます。

セキュリティの種類

表 4-1 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 4-1　SSID セキュリティの種類

セキュリティ タイプ	説明	有効になるセキュリティ機能
セキュリティなし	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 SSID を使用する場合に限定して使用し、ネットワークへのアクセスを制限する VLAN に割り当てる必要があります。	—
スタティック WEP キー	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。この設定を選択する場合は、MAC アドレス ベースのワイヤレス デバイスへのアソシエートを制限するかどうかを検討してください。詳細については、次の URL の『*Cipher Suites and WEP*』を参照してください。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html または ネットワーク内に RADIUS サーバがない場合、アクセス ポイントをローカル認証サーバとして使用するかを検討してください。 手順については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html の『*Using the Access Point as a Local Authenticator*』を参照してください。	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。

表 4-1　SSID セキュリティの種類 （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
EAP[1] 認証	このオプションは、802.1X 認証（LEAP[2]、PEAP[3]、EAP-TLS[4]、EAP-FAST[5]、EAP-TTLS[6]、EAP-GTC[7]、EAP-SIM[8]、およびその他の 802.1X/EAP ベースの製品）がイネーブルになります。 この設定は、必須の暗号化、WEP、オープン認証プラス EAP、ネットワーク EAP 認証を使用し、キー管理なしで RADIUS サーバ認証ポート 1645 を使用します。 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 によるオープン認証を設定していない場合、以下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[9]	このオプションは、データベース認証されたユーザにワイヤレス アクセスを許可します。アクセスは認証サーバのサービスを通じて行います。ユーザの IP トラフィックは WEP で使用されるものより強力なアルゴリズムで暗号化されます。 この設定では暗号キー、TKIP[10]、オープン認証プラス EAP、ネットワーク EAP 認証、必須のキー管理 WPA、および RADIUS サーバ認証ポート 1645 を使用します。 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 を使用して対応付けを行うクライアント 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 によるオープン認証を設定していない場合、以下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.`

1. EAP = Extensible Authentication Protocol
2. LEAP = Lightweight Extensible Authentication Protocol
3. PEAP = Protected Extensible Authentication Protocol
4. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
5. EAP-FAST = Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
6. EAP-TTLS = Extensible Authentication Protocol-Tunneled Transport Layer Security
7. EAP-GTC = Extensible Authentication Protocol-Generic Token Card
8. EAP-SIM = Extensible Authentication Protocol-Subscriber Identity Module
9. WPA = Wi-Fi Protected Access
10. TKIP = Temporal Key Integrity Protocol

無線 QoS の設定

Quality of Service（QoS）を設定すると、特定のトラフィックを他のトラフィックよりも優先的に処理できます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。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。ワイヤレス デバイスに QoS を設定するには、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html の『*Quality of Service in a Wireless Environment*』を参照してください。

ホット スタンバイ モードでのアクセス ポイントの設定

ホット スタンバイ モードでは、アクセス ポイントは別のアクセス 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、アクセス ポイントのそばに配置され、それを監視します（設定は、このアクセス ポイントとまったく同じにします）。スタンバイ アクセス ポイントは、クライアントとして監視対象のアクセス ポイントとアソシエートします。また監視対象のアクセス ポイントに、イーサネットおよび無線ポートを通して 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）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。モニタ対象アクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがそれを引き継いだ場合、両アクセス ポイントの設定が同一であれば、クライアント デバイスは簡単かつ確実にスタンバイ アクセス ポイントに切り替わることができます。詳細については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html の『*Hot Standby Access Points*』を参照してください。

Cisco Unified ソフトウェアへのアップグレード

アクセス ポイントを Cisco Unified モードで実行するには、次の手順に従ってソフトウェアをアップグレードする必要があります。

- 「アップグレードの準備」（P.4-9）
- 「アップグレードの実行」（P.4-11）
- 「AP ブートローダのアップグレード」（P.4-12）
- 「アクセス ポイントへのソフトウェアのダウンロード」（P.4-12）
- 「アクセス ポイントでのソフトウェア リカバリ」（P.4-13）

ソフトウェア前提条件

- アクセス ポイントが組み込まれた Cisco 880 シリーズ ISR は、ルータが advipservices フィーチャセットと Cisco IOS Release15.2(4)M1 またはそれ以降のバージョンを実行している場合、自律ソフトウェアから Cisco Unified ソフトウェアにアップグレードできます。
- Cisco Unified アーキテクチャの組み込み型アクセス ポイントを使用するには、Cisco Wireless LAN Configuration（WLC）が、シングル無線（Cisco IOS Release 7.0.116.0 またはそれ以降のバージョン）とデュアル無線（Cisco IOS Release 7.2.110.0 またはそれ以降のバージョン）の最小バージョンを実行している必要があります。

アップグレードの準備

アップグレードを準備するには次の作業を行います。

- 「アクセス ポイントの IP アドレスの保護」（P.4-10）
- 「モード設定がイネーブルになっていることの確認」（P.4-10）

アクセス ポイントの IP アドレスの保護

アクセス ポイントの IP アドレスを保護することにより、アクセス ポイントは WLC と通信でき、起動時に Unified イメージをダウンロードできます。ホスト ルータは、DHCP プールを通じてアクセス ポイント DHCP サーバ機能を提供します。このアクセス ポイントは WLC と通信し、DHCP プール コンフィギュレーションのコントローラ IP アドレスのオプション 43 を設定します。以下に設定サンプルを示します。

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex  f104.0a0a.0a0f   (single WLC IP address(10.10.10.15) in hex format)
int vlan1
ip address 60.0.0.1 255.255.255.0
```

WLC 検出プロセスの詳細については、
http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html の『*Cisco Wireless LAN Configuration Guide*』を参照してください。

モード設定がイネーブルになっていることの確認

モード設定がイネーブルになっていることを確認するには、次の手順に従います。

ステップ 1　ルータから WLC サーバに ping を実行し、接続を確認します。

ステップ 2　**service-module wlan-ap 0 session** コマンドを実行し、アクセス ポイントへのセッションを確立します。

ステップ 3　アクセス ポイントが自律起動イメージを動作させているか確認します。

ステップ 4　**show boot** コマンドを入力してアクセス ポイントのモード設定がイネーブルになっていることを確認します。次に、コマンドの出力例を示します。

```
# show boot
BOOT path-list:      flash:ap802-k9w7-mx.124/ap802-k9w7-mx.124
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:          no
Manual Boot:         yes
HELPER path-list:    no
NVRAM/Config file
buffer size:   32768
Mode Button:    on
Radio Core TFTP:
ap#
```

アップグレードの実行

自律ソフトウェアを Cisco Unified ソフトウェアにアップグレードするには、次の手順に従います。

ステップ 1　アクセス ポイントの起動イメージを Cisco Unified アップグレード イメージ（*リカバリ イメージ*とも呼びます）に変更するには、グローバル コンフィギュレーション モードで **service-module wlan-ap 0 bootimage unified** コマンドを実行します。

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

（注）　**service-module wlan-ap 0 bootimage unified** コマンドが実行されない場合、advipservices または advipsevices_npe ソフトウェア ライセンスがイネーブルになっているかどうかを確認してください。

アクセス ポイントの起動イメージのパスを識別するには、アクセス ポイントのコンソールから EXEC モードで **show boot** コマンドを使用します。

```
autonomous-AP# show boot
BOOT path-list: flash:/ap802-rcvk9w8-mx/ap802-rcvk9w8-mx
```

ステップ 2　正規の手順でシャットダウンを行ってアクセス ポイントをリブートし、アップグレード プロセスを完了するには、特権 EXEC モードで **service-module wlan-ap 0 reload** コマンドを実行します。アクセス ポイントとのセッションを確立し、アップグレード プロセスを監視します。

AP から自律モードへアップグレードまたは復帰する際のトラブルシューティング

Q. 私のアクセス ポイントでは、自律ソフトウェアから Cisco Unified ソフトウェアへのアップグレードに失敗し、リカバリ モードに陥ったままになっているようです。どうすればいいでしょうか。

A. アクセス ポイントで自律ソフトウェアから Unified ソフトウェアにアップグレードできなかった場合は、次の操作を実行してください。

- リカバリ イメージを起動する前に、自律アクセス ポイントのスタティック IP アドレスが BVI インターフェイスに設定されていないことを確認します。
- ルータ / アクセス ポイントと WLC 間で ping を実行して、接続が確立されているか確認します。
- アクセス ポイントと WLC クロック（時刻と日付）が正しく設定されているか確認します。

Q. アクセス ポイントが起動を試行しているのですが、何度やってもうまくいきません。どうしてですか。
またアクセス ポイントがリカバリ イメージでスタックしたまま、Unified ソフトウェアにアップグレードしません。どうしてですか。

A. アクセス ポイントでは、起動を試みて失敗したり、リカバリ モードに陥ってしまい、Unified ソフトウェアにアップグレードできない場合があります。このいずれかの状態になった場合は、**service-module wlan-ap0 reset bootloader** コマンドを実行してアクセス ポイントをブートローダに戻し、手動でイメージを復帰させてください。

AP ブートローダのアップグレード

AP802 では、ホスト ルータ イメージの一部としてブートローダを使用できます。ブートローダをアップグレードするには、次の手順を実行します。

ステップ 1　**show platform version** コマンドを使用して、最初のコアで実行されているホスト ルータ イメージにバンドルされている WLAN AP ブートローダを確認します。

```
Router# show platform version
Platform Revisions/Versions :
.
WLAN AP Boot loader (bundled):
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

ステップ 2　ルータと WLAN AP の間でセッションを開きます。

ルータとアクセス ポイントの間でセッションを開く方法については、「無線コンフィギュレーション セッションの開始」（P.4-2）を参照してください。

ステップ 3　WLAN AP ブートローダのバージョンを確認します。

WLAN AP ブートローダでは、**version** コマンドを使用します。

```
ap: version
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

WLAN AP IOS で show version コマンドを使用します。

```
ap# show version
.
BOOTLDR: AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
<snip>
Configuration register is 0xF
```

ステップ 4　次のコマンドを使用してブートローダをアップグレードします。

```
Router# service-module wlan-ap 0 upgrade bootloader
Router# service-module wlan-ap 0 reset
```

アクセス ポイントへのソフトウェアのダウンロード

直前の自律イメージにアクセス ポイントの起動をリセットするには、最初のコアで実行されているホスト ルータで、特権 EXEC モードで **service-module wlan-ap0 bootimage autonomous** コマンドを使用します。自律ソフトウェア イメージをアクセス ポイントにリロードするには、**service-module wlan-ap 0 reload** コマンドを使用します。

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage autonomous
Router(config)# end
Router# write
Router# service-module wlan-ap 0 reload
```

アクセス ポイントでのソフトウェア リカバリ

アクセス ポイントのイメージをリカバリするには、特権 EXEC モードで **service-module wlan-ap0 reset bootloader** コマンドを使用します。このコマンドを使用すると、アクセス ポイントがブートローダに戻り、手動でイメージをリカバリできるようになります。

注意　このコマンドの使用には注意が必要です。この操作では通常のシャットダウンが実行*されない*ことから、実行中のファイル操作に影響が生じる場合があります。このコマンドは、シャットダウンまたは障害状態からリカバリする目的に限り使用してください。

サポートされるイメージ

Cisco ISR 880 シリーズでサポートされるイメージの詳細については、「サポートされるイメージ」（P.1-11）を参照してください。

関連資料

自律およびユニファイド設定手順の詳細については、次のマニュアルを参照してください。

- 「自律モードのマニュアル」—表 4-2
- 「Unified モードのマニュアル」—表 4-3

表 4-2　自律モードのマニュアル

自律モード	リンク	説明
ネットワーク デザイン		
ワイヤレスの概要	ワイヤレス デバイス概要	ネットワークのワイヤレス デバイスの役割について説明します。
『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Versions 12.4(25d)JA and 12.3(8)JEE』	http://www.cisco.com/en/US/docs/wireless/access_point/12.4.25d.JA/Command/reference/cr12425d-preface.html	Cisco Aironet アクセス ポイントとブリッジを設定するための Cisco IOS Release 12.4(25d)JA と Cisco IOS Release 12.3(8)JEE のコマンドについて説明します。
設定		
無線の設定	無線の設定	無線を設定する方法について説明します。
セキュリティ		
『Authentication Types for Wireless Devices』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html	アクセス ポイントに設定されている認証タイプについて説明します。

表 4-2　自律モードのマニュアル （続き）

自律モード	リンク	説明
『RADIUS and TACACS+ Servers in a Wireless Environment』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html	RADIUS[1] および TACACS+[2] のイネーブルと設定の方法、アカウンティング情報の詳細説明、さらに、管理側が行う認証と認証プロセスの柔軟な制御方法について説明します。RADIUS および TACACS+ は、AAA[3] を通じて活用され、AAA コマンドを使用する場合だけイネーブルにできます。
『Using the Access Point as a Local Authenticator』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html	ローカル認証を担当するアクセス ポイントというロールにおいて、ワイヤレス デバイスを使用する方法について説明しています。アクセス ポイントは小規模無線 LAN のスタンドアロン認証システムとして機能するか、またはバックアップ認証サービスを提供します。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。
『Cipher Suites and WEP』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html	WPA[4] および CCKM[5]、WEP[6]、および WEP 機能（AES[7]、MIC[8]、TKIP[9]、およびブロードキャスト キーのローテーションなど）を使用するときに必要な暗号スイートの設定方法について解説します。
『Hot Standby Access Points』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html	ホット スタンバイ ユニットとしてワイヤレス デバイスを設定する方法について説明します。
無線 VLAN の設定	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html	アクセス ポイントが、有線 LAN 上に設定された VLAN と動作するよう設定する方法について説明しています。
『Service Set Identifier』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html	ワイヤレス デバイスは、アクセス ポイントとして最大 16 の SSID[10] をサポートできます。本マニュアルでは、ワイヤレス デバイス上の SSID の設定および管理方法について説明します。

表 4-2　自律モードのマニュアル （続き）

自律モード	リンク	説明
管理		
Quality of Service	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html	シスコのワイヤレス インターフェイスで QoS[11] を設定する方法について説明します。この機能により、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。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。
『Regulatory Domains and Channels』	http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/scg_chanels.html	世界中の規制ドメイン内の Cisco アクセス製品でサポートしている無線チャネルが記載されています。
『System Message Logging』	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html	ワイヤレス デバイスでシステム ロギング メッセージを設定する方法について説明します。

1. RADIUS = リモート認証ダイヤルイン ユーザ サービス
2. TACACS+ = Terminal Access Controller Access Control System Plus
3. AAA = Authentication, Authorization, and Accounting
4. WPA = Wireless Protected Access
5. CCKM = Cisco Centralized Key Management
6. WEP = Wired Equivalent Privacy
7. AES = Advanced Encryption Standard
8. MIC = Message Integrity Check
9. TKIP = Temporal Key Integrity Protocol
10. SSID = サービス セット ID
11. QoS = Quality of Service

表 4-3　Unified モードのマニュアル

ネットワーク デザイン	リンク
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
『Wireless LAN Controller (WLC) FAQ』	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
シングル無線 AP802	
『Cisco Wireles LAN Controller Configuration Guide, Release 7.0.116.0』	http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/cg_controller_setting.html
デュアル無線 AP802	
『Cisco Unified Wireless Network Software Release 7.2.110.0 （7.2 Maintenance Release 1）』	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/product_bulletin_c25-707629.html

CHAPTER 5

無線の設定

ここでは、ワイヤレス デバイスの無線の設定方法について、次の内容で説明します。

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）　ラジオ インターフェイスをイネーブルにする前に、Service Set Identifier（SSID; サービス セット識別子）を作成する必要があります。

アクセス ポイント無線をイネーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **dot11 ssid** *ssid*
3. **interface dot11radio** {**0**}
4. **ssid** *ssid*
5. **no shutdown**
6. **end**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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。 （注）　SSID では、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**}	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。 • 802.11g/n 2.4-GHz および 2.4-GHz は radio 0 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**	無線ポートをイネーブルにします。
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。

ワイヤレス ネットワークでのロールの設定

無線プラットフォームでは、ワイヤレス ネットワークで次のロールを実行します。

- アクセス ポイント
- 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）
- ルート ブリッジ
- 非ルート ブリッジ
- ワイヤレス クライアントを持つルート ブリッジ
- ワイヤレス クライアントを備えていない非ルート ブリッジ

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。Cisco ISR ワイヤレス デバイスのデフォルトのフォールバック ロールは次のとおりです。

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。

ワイヤレス デバイスの無線ネットワーク ロールおよびフォールバック ロールを設定するには、特権 EXEC モードで開始し、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **station-role non-root** {**bridge | wireless-clients**} **root** {**access-point | ap-only | [bridge | wireless-clients] | [fallback | repeater | shutdown]**} **workgroup-bridge** {**multicast | mode** <*client* | *infrastructure*>**| universal** <*Ethernet client MAC address*>}
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz および 2.4-GHz は radio 0 です。
ステップ 3	**station-role** **non-root** {**bridge** | **wireless-clients**} **root** {**access-point** | **ap-only** | **[bridge** | **wireless-clients]** | **[fallback** | **repeater** | **shutdown]**} **workgroup-bridge** {**multicast** | **mode** <*client* | *infrastructure*>| **universal** <*Ethernet client MAC address*>}	ワイヤレス デバイスロールを設定します。 • 有線または無線クライアントを備えた非ルート ブリッジ、ルート アクセス ポイントまたはブリッジ、またはワークグループ ブリッジへのロールを設定します。 （注） **bridge** モードの無線でサポートするには、ポイントツーポイント設定だけです。 （注） **repeater** コマンドおよび **wireless-clients** コマンドは、Cisco 860 シリーズおよび Cisco 880 シリーズの Integrated Services Router ではサポートされません。 （注） **scanner** コマンドは、Cisco 860 シリーズおよび Cisco 880 シリーズの Integrated Services Router ではサポートされません。 • 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。ワークグループ ブリッジは、ルート ブリッジまたはアクセス ポイントに別のワイヤレス クライアントが関連付けられていなければ、最大 25 クライアントを保持できます。
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。

（注） ワイヤレス ネットワークのデバイスのロールをブリッジまたはワークグループ ブリッジとしてイネーブルにし、**no shut** コマンドを使用してインターフェイスをイネーブルにすると、反対側のデバイス（アクセス ポイントまたはブリッジ）が起動している場合にだけ、インターフェイスの物理ステータスとソフトウェア ステータスが起動（動作可能）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。ソフトウェア ステータスは、反対側のデバイスが設定され、準備状態の場合にだけ表示されます。

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。追跡した無線が停止またはディセーブルになった場合、アクセス ポイントにより他の無線がシャットダウンされます。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。

Radio 0 を追跡するには、次のコマンドを入力します。

```
# station-role root access-point fallback track d0 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。ファスト イーサネット トラッキング用にアクセス ポイントを設定する方法については、「ワイヤレス ネットワークでのロールの設定」（P.5-3）を参照してください。

（注）　ファスト イーサネット トラッキングでは、リピータ モードがサポートされていません。

ファスト イーサネット トラッキング用のアクセス ポイントを設定するには、次のコマンドを入力します。

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

MAC アドレス トラッキング

MAC アドレスを使用して別の無線に接続しているクライアント アクセス ポイントをトラッキングし、ルート アクセス ポイントの起動と停止の役割を果たす無線を設定できます。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 のクライアントを追跡するには、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。データ レートの単位は Mbps（メガビット/秒）です。ワイヤレス デバイスでは、常に、最大データ レートでデータ セットを **basic** に転送します。これは、ブラウザ ベース インターフェイスでは、**required** として知られています。障害や干渉などがある場合、ワイヤレス デバイスはデータ送信が可能な範囲での最速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 パケットについては、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。

データ レート設定を使用して、特定のデータ レートで稼働中のサービス クライアント デバイスにアクセス ポイントを設定できます。たとえば、11Mbps サービスでだけ 2.4GHz 無線の転送を設定する場合は、11Mbps レートを **basic** に設定し、他のデータ レートを **disabled** に設定します。ワイヤレス デバイスを 1 および 2 Mbps で稼働するクライアント デバイスにだけサービスを提供するように設定するには、**basic** に 1 および 2 を設定し、データ レートを **disabled** に設定します。802.11g クライアント デバイスにだけサービスを提供するように 2.4GHz、802.11g 無線を設定するには、Orthogonal Frequency Division Multiplexing（OFDM; 直交周波数分割多重方式）のデータ レート（6、9、12、18、24、36、48、54）を、すべて **basic** に設定します。54 Mbps サービスに対応する 5-GHz 無線だけを設定する場合は、54 Mbps レートを **basic** に設定し、他のデータ レートを **disabled** 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** を入力すると、ワイヤレス デバイスにより 1Mbps レートが **basic** に設定され、その他のレートが **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、他のクライアントは接続できるのにアクセス ポイントに接続できないクライアントがある場合は、そのクライアントがアクセス ポイントの適用範囲内に入っていないことが考えられます。このような場合、範囲オプションを使用することにより適用範囲を拡大すると、クライアントがアクセス ポイントに接続できるようになる可能性があります。

通常、スループットと範囲が交換条件となります。信号が低下する（アクセス ポイントからの距離が遠いなどの理由により）と、リンクを維持するためにレートのネゴシエーションをやり直します（この場合は、データ レートが低くなります）。設定されている高データ レートを維持できないほどに信号が低下した場合に、高いスループットに設定したリンクが単純にドロップするか、十分なサービス範囲を持ったアクセス ポイントが利用可能な場合は、そちらにローミングされます。両者のバランス（スループットと 範囲）は、無線プロジェクトで利用可能なリソース、ユーザが使用するトラフィックの種類、必要とされるサービス レベル、そして常に同じですが、RF 環境の質に基づいて行われる設計上の決定事項です。データ レート設定に **throughput** を入力すると、ワイヤレス デバイスにより、4 つのデータ レートすべてが **basic** に設定されます。

（注）　ワイヤレス ネットワークに 802.11b クライアントおよび 802.11g クライアントが混在している環境の場合は、データ レート 1、2、5.5、および 11 Mbps が **required**（**basic**）に設定され、その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必ず確認してください。802.11b アダプタは、接続するアクセス ポイントで 11 Mbps を上回るデータ レートが **required** に設定されていると、54 Mbps データ レートを認識せず、稼働しません。

無線データ レートを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}

3. **speed**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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 および 802.11g/n 2.4-GHz は radio 0 です。

	コマンドまたはアクション	目的
ステップ 3	**speed** 802.11b、2.4GHz 無線の場合： {[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] | **range** | **throughput**} 802.11g、2.4GHz 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 5GHz 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 2.4GHz 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**}	各データ レートを **basic** または **enabled** に設定します。または、**range** を入力して範囲を最適化するか、**throughput** を入力してスループットを最適化します。 • （任意）**1.0**、**2.0**、**5.5**、および **11.0** を入力すると、802.11b、2.4GHz 無線でこれらのデータ レートが **enabled** に設定されます。 **1.0**、**2.0**、**5.5**、**6.0**、**9.0**、**11.0**、**12.0**、**18.0**、**24.0**、**36.0**、**48.0**、および **54.0** を入力すると、802.11g、2.4GHz 無線でこれらのデータ レートが **enabled** に設定されます。 **6.0**、**9.0**、**12.0**、**18.0**、**24.0**、**36.0**、**48.0**、および **54.0** を入力すると、5GHz 無線でこれらのデータ レートが **enabled** に設定されます。 • （任意）**basic-1.0**、**basic-2.0**、**basic-5.5**、および **basic-11.0** を入力すると、802.11b、2.4GHz 無線でこれらのデータ レートが **basic** に設定されます。 **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、2.4GHz 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でサポートする必要がある場合は、ワイヤレス デバイスに関連付けできません。802.11g 無線の basic データ レートに 12Mbps 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 802.11g 無線に関連付けできません。 **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）無線の範囲またはスループットを自動的に最適化するには、**range**、**throughput**、または **ofdm-throughput**（ERP 保護なし）を入力します。**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、その他のレートを **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、すべての CCK 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。

	コマンドまたはアクション	目的
	speed（続き）	• （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、**default** オプションは、レート 1、2、5.5、および 11 を **basic** に、レート 6、9、12、18、24、36、48、および 54 を **enabled** に設定します。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、**default** オプションは、レート 6.0、12.0、および 24.0 を **basic** に、レート 9.0、18.0、36.0、48.0、および 54.0 を **enabled** に設定します。 802.11g/n 2.4 GHz 無線で、**default** オプションは、レート 1.0、2.0、5.5、および 11.0 を **enabled** に設定します。 802.11g/n 5 GHz 無線で、**default** オプションは、レート 6.0、12.0、および 24.0 を **enabled** に設定します。 どちらの 802.11g/n 無線の Modulation Coding Scheme（MCS; 変調符号化方式）インデックス範囲も 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。この例では、データレート **basic-2.0** および **basic-5.5** を設定から削除する方法を示します。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

MCS レートの設定

Modulation Coding Scheme（MCS; 変調符号化方式）は、変調順序（2 位相偏移変調 [BPSK]、4 位相偏移変調 [QPSK]、16- 直交振幅変調 [16-QAM]、64-QAM）から成る PHY パラメータおよび Forward Error Correction（FEC; 前方誤り訂正）コード レート（1/2、2/3、3/4、5/6）の仕様です。MCS は、ワイヤレス デバイス 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

ワイヤレス デバイスでは、MCS 0 ～ 15 をサポートしています。高スループット クライアントでは、少なくとも MCS 0 ～ 7 をサポートします。

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。高スループット データ レートは、*MCS*、*帯域幅*、および*ガード インターバル*の機能です。802.11a、b、および g 無線では、20-MHz チャネル幅を使用しています。表 5-1 は、MCS、ガード インターバル、およびチャネル幅に基づく潜在的なデータ レートを示します。

表 5-1　MCS 設定、ガード インターバル、およびチャネル幅に基づくデータ レート

MCS インデックス	ガード インターバル = 800 ns		ガード インターバル = 400 ns	
	20-MHz チャネル幅 データ レート（Mbps）	40-MHz チャネル幅 データ レート（Mbps）	20-MHz チャネル幅 データ レート（Mbps）	40-MHz チャネル幅 データ レート（Mbps）
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300

レガシー レートは次のとおりです。

5 GHz: 6、9、12、18、24、36、48、および 54 Mbps

2.4 GHz: 1、2、5.5、6、9、11、12、18、24、36、48、および 54 Mbps

MCS レートは **speed** コマンドを使用して設定します。次に、802.11g/n 2.4 GHz 無線の **speed** 設定の例を示します。

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 800test
    !
    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.
```

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 ポイント無線の送信電力を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power local**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# 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**}	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 および 802.11g/n 2.4-GHz は radio 0 です。
ステップ 3	**power local** これらのオプションは、2.4-GHz 802.11n 無線で使用できます（単位は dBm）。 {**8** | **9**| **11** | **14** | **15** | **17** | **maximum**}	規制ドメインにおいて電力レベルが許容範囲内となるように、2.4 GHz 無線に送信電力を設定します。
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。

power local の **no** 形式を使用すると、電力設定をデフォルト設定である **maximum** に戻せます。

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、関連付けされたクライアント デバイスの電力制限を示すために Dynamic Power Control（DPC; 動的電力制限）という用語を使用しています。

ワイヤレス デバイスに関連付けされているすべてのクライアント デバイスの最大使用可能電力設定を指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power client**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz および 2.4-GHz は radio 0 です。
ステップ 3	**power client** 次のオプションは、802.11n、2.4GHz クライアントについて使用できます（単位 dBm）。 {**local** | **8** | **9** | **11** | **14** | **15** | **17** | **maximum**}	ワイヤレス デバイスに関連付けるクライアント デバイスで許可される最大電力レベルを設定できます。 • 電力レベルを **local** に設定すると、クライアントの電力レベルはアクセス ポイントの電力レベルに設定されます。 • 電力レベルを **maximum** に設定すると、クライアントの電力は最大許可電力に設定されます。 （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。

関連付けたクライアントの最大電力レベルをディセーブルにするには、**power client** 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 デバイス無線のデフォルト チャネル設定は least congested です。ワイヤレス デバイスでは、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。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。

2.4GHz 帯チャネル利用帯域幅は、チャネルあたり 22MHz になります。チャネル 1、6、および 11 の帯域は重複しないため、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 無線は同じチャネルと周波数を使用します。

5GHz 無線は、規制ドメインに応じて 5180 ～ 5320MHz の 8 チャネルから、最大 5170 ～ 5850 MHz の 27 チャネルで稼働します。各チャネルの帯域幅は 20 MHz で、それぞれの帯域がわずかに重複しています。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、チャネル 44 と 46）を使用してください。

（注） 同じ圏内に多くのアクセス ポイントが存在すると、スループットの減少の原因となる無線輻輳が発生します。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。

802.11n チャネル幅

802.11n 規格では、隣接する重複しない 2 つのチャネル（たとえば、2.4 GHz チャネル 1 および 6）から成る 20 MHz および 40 Mhz チャネルのどちらも使用できます。

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 20-MHz 高スループット クライアントでは、コントロール チャネルを使用します。このチャネルへ送信できるのはビーコンだけです。もう 1 つの 20MHz チャネルは*拡張チャネル*と呼ばれます。40-MHz ステーションでは、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。

40MHz チャネルは、1,1 のようにチャネルおよび拡張として指定されます。この例で、コントロール チャネルはチャネル 1、拡張チャネルはその上のチャネルです。

ワイヤレス デバイスのチャネル幅を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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** }	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	ワイヤレス デバイスの無線のデフォルト チャネルを設定します。起動時に最も混雑していないチャネルを検索するには、**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、Cisco 800 シリーズ ISR ワイヤレス デバイスで使用できます。使用可能な設定は、**20**、**40-above**、および **40-below** の 3 つです。 – **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、「ワールド モードのイネーブル化とディセーブル化」（P.5-14）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。

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、ワイヤレス デバイスはそのビーコンにチャネル キャリア設定情報を追加します。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。シスコ クライアント デバイスでは、ワイヤレス デバイスが 802.11d を使用しているのか、あるいはシスコ レガシー ワールド モードによりワイヤレス デバイスで使用されているモードに一致するワールド モードを自動的に使用しているのかを検出します。

ワールド モードを常にオンに設定することも可能です。この設定では、基本的にアクセス ポイントが各国間でローミングされ、必要に応じてその設定が変更されます。

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。

ワールド モードをイネーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **world-mode** {**dot11d country_code** *code* {**both** | **indoor** | **outdoor**}| **world-mode roaming** | **legacy**}
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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 モードをイネーブルにします。 • 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。 • **world-mode roaming** オプションを入力し、継続的なワールド モード コンフィギュレーションでアクセス ポイントを配置します。 **（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 モードをディセーブルにするには、**world-mode** 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（ヘッダーと呼ばれる場合もある）は、パケットの先頭にあるデータ部です。ここには、ワイヤレス デバイスとクライアント デバイスのパケットの送受信に必要な情報が含まれています。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。
- Long : long プリアンブルは、ワイヤレス デバイスと初期の Cisco Aironet 無線 LAN アダプタのすべてのモデル間との互換性を確保します。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。

short 無線プリアンブルをディセーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **no preamble-short**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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** }	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 モードを開始します。
ステップ 3	**no preamble-short**	short プリアンブルをディセーブルにし、long プリアンブル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。

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

データの送受信時にワイヤレス デバイスで使用されるアンテナを選択できます。受信アンテナおよび送信アンテナの両方に 3 つのオプションがあります。

- Gain：対称のアンテナ ゲインをデシベル（dB）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。
- 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。
- 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。

データの送受信にワイヤレス デバイスが使用するアンテナを選択するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **gain** *dB*
4. **antenna receive** {**diversity | left | right**}
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**gain** *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。必要に応じて、1.5 などの小数値を使用できます。 **（注）** Cisco 860 および Cisco 880 ISR は、取り外しできない固定アンテナを付けて出荷されています。これらのモデルにアンテナ ゲインを設定できません。
ステップ 4	**antenna receive** {**diversity | left | right**}	受信アンテナを diversity、left、または right 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。
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。

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 デバイスと関連付けられているクライアント デバイス間との特別な相互作用を必要とする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 デバイスでは、Aironet 拡張機能を使用して、クライアント デバイスに対し、ネットワークに対する最適な接続を提供するアクセス ポイントを指示します。この場合、そのような要素の基準となるのは、ユーザ数、ビット誤り率、および信号強度です。
- 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 デバイスおよび関連付けられている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、パケットの不正改ざんを防止します。
- Cisco Key Integrity Protocol（CKIP）：シスコの WEP キー置換技術で、IEEE 802.11i セキュリティ タスク グループにより開示された初期のアルゴリズムに基づいています。標準ベースのアルゴリズムである Temporal Key Integrity Protocol（TKIP; 一時キー整合性プロトコル）の場合は、Aironet 拡張機能をイネーブルにする必要はありません。
- 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。Aironet 拡張機能をディセーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **no dot11 extension aironet**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**no dot11 extension aironet**	Aironet 拡張機能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。

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

ワイヤレス デバイスが 802.3 パケット以外のデータ パケットを受信する場合、カプセル化トランスフォーメーション方式を使用してワイヤレス デバイス パケットを 802.3 にフォーマットする必要があります。この変換方式には次の 2 種類があります。

- 802.1H：この方式では、シスコ無線製品用に最適なパフォーマンスを提供します。
- RFC 1042：この設定を使用すると、非シスコ無線機器との相互運用性が確保されます。RFC1042 は、802.1H ほどの相互運用性は保証されませんが、他のメーカーの無線機器で使用されています。

カプセル化トランスフォーメーション方式を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio {0}**
3. **payload-encapsulation {snap | dot1h}**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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}**	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**payload-encapsulation {snap | dot1h}**	カプセル化トランスフォーメーション方式を RFC 1042（**snap**）または 802.1h（**dot1h**、デフォルト設定）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。

Public Secure Packet Forwarding のイネーブル化とディセーブル化

Public Secure Packet Forwarding（PSPF; パブリック セキュア パケット フォワーディング）では、アクセス ポイントに関連付けられているクライアント デバイスがアクセス ポイントに関連付けられている他のクライアント デバイスと何らかの理由によりファイルを共有したり通信したりしないように防止します。PSPF は、LAN のその他の機能を提供せずにクライアント デバイスに対するインターネット アクセスを提供します。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.5-21）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。ブリッジ グループの詳細な説明とこれらを実装するための手順については、次のリンクの『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』の「Configuring Transparent Bridging」の章を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcftb_ps1835_TSD_Products_Configuration_Guide_Chapter.html

PSPF はデフォルトでディセーブルに設定されています。PSPF をイネーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **bridge-group** *group* **port-protected**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**bridge-group** *group* **port-protected**	PSPF 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。

PSPF をディセーブルにするには、**bridge group** コマンドの **no** 形式を使用します。

保護ポートの設定

使用している無線 LAN の異なるアクセス ポイントに関連付けられているクライアント デバイス間での通信を防止するには、ワイヤレス デバイスが接続されている交換機上で保護ポートを設定する必要があります。

使用している交換機上で保護ポートとしてポートを定義するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport protected**
4. **end**
5. **show interfaces** *interface-id* **switchport**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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 モードを開始します。 • **wlan-gigabitethernet0** など、設定を行う交換機ポート インターフェイスのタイプと番号を入力します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	入力を確認します。
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** コマンドを使用します。

保護ポートとポート ブロッキングの詳細については、次の URL にある『*Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1*』の「Configuring Port-Based Traffic Control」の章を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/3550scg.html

ビーコン間隔と DTIM の設定

ビーコン期間は、アクセス ポイント ビーコン間の時間数をキロマイクロ秒（Kmicrosecs）で表したものです。1 キロマイクロ秒は 1,024 マイクロ秒に相当します。データ ビーコン レートは常にビーコン期間の倍数で、ビーコンにどの程度の頻度で Delivery Traffic Indication Message（DTIM; デリバリー トラフィック インディケーション メッセージ）が含まれるかを決定します。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、ビーコン期間がデフォルトとして 100 に設定されており、データ ビーコン レートが 2 に設定されているとすると、ワイヤレス デバイスでは 200 キロマイクロ秒ごとに DTIM を 1 個含むビーコンを送信します。

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。ビーコン期間および DTIM を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **beacon period** *value*
4. **beacon dtim-period** *value*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**beacon period** ***value***	ビーコン期間を設定します。 • 値をキロマイクロ秒単位で入力します。
ステップ 4	**beacon dtim-period** ***value***	DTIM を設定します。 • 値をキロマイクロ秒単位で入力します。
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 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、パケット送信前にワイヤレス デバイスが RTS を発行するときの基準となるパケット サイズを決定します。多くのクライアント デバイスがワイヤレス デバイスに関連付けられていたり、クライアントが互いに離れていて、ワイヤレス デバイスを検出できても相互に検出できないエリアでは、RTS しきい値設定が小さいほうが便利なことがあります。0 ～ 2347 バイトの範囲で設定を入力できます。

最大 RTS 再試行回数は、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。

どのアクセス ポイントおよびブリッジでもデフォルトの RTS しきい値は 2347 で、デフォルトの最大 RTS 再試行回数の設定は 32 です。

RTS しきい値および最大 RTS 再試行回数を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **rts threshold** *value*
4. **rts retries** *value*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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 および 802.11g/n 2.4-GHz は radio 0 です。
ステップ 3	**rts threshold** *value*	RTS しきい値を設定します。 • RTS しきい値として 0 ～ 2347 を入力します。
ステップ 4	**rts retries** *value*	最大 RTS 再試行回数を入力します。 • 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には、**rts** コマンドの **no** 形式を使用します。

最大データ再試行回数の設定

最大データ再試行回数設定では、ワイヤレス デバイスがパケットを廃棄するまでに、パケット送信を試行する回数を決定します。デフォルト設定は 32 です。

最大データ再試行回数を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **packet retries** *value*
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**packet retries** *value*	最大データ再試行回数を入力します。 • 1 ～ 128 の範囲の値を入力します。
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。

設定をデフォルトにリセットするには、**packet retries** 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 2346 バイトです。

フラグメンテーションしきい値を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **fragment-threshold** *value*
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	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**}	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。 • 802.11g/n 2.4-GHz および 5-GHz は radio 0 です。
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。 • 2.4GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。 • 5GHz 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には、**fragment-threshold** 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の向上に、short スロット時間を使用できます。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。short スロット時間をイネーブルにすると、ワイヤレス デバイスでは、802.11g 2.4-GHz 無線に関連付けられているすべてのクライアントが short スロット時間をサポートしているときにだけ short スロット時間を使用します。

Short スロット時間は、802.11g 2.4-GHz 無線上でだけサポートされています。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 **short-slot-time** コマンドを入力し、short スロット時間をイネーブルにします。

```
ap(config-if)# short-slot-time
```

short スロット時間をディセーブルにするには、**short-slot-time** コマンドの **no** 形式を使用します。

キャリア ビジー テストの実行

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**

2.4 GHz 無線で検査を実行するには、*interface-number* に **dot11radio 0** を入力します。

show dot11 carrier busy コマンドを使用してキャリア ビジー テストの結果を再表示します。

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、Class of Service（CoS; クラス サービス）5（ビデオ）および CoS 6（音声）ユーザ プライオリティの低遅延における 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には、次のステップに従います。

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左側にあるタスク メニューで [Services] をクリックします。

ステップ 3　Services のリストが展開されたら、[Stream] をクリックします。

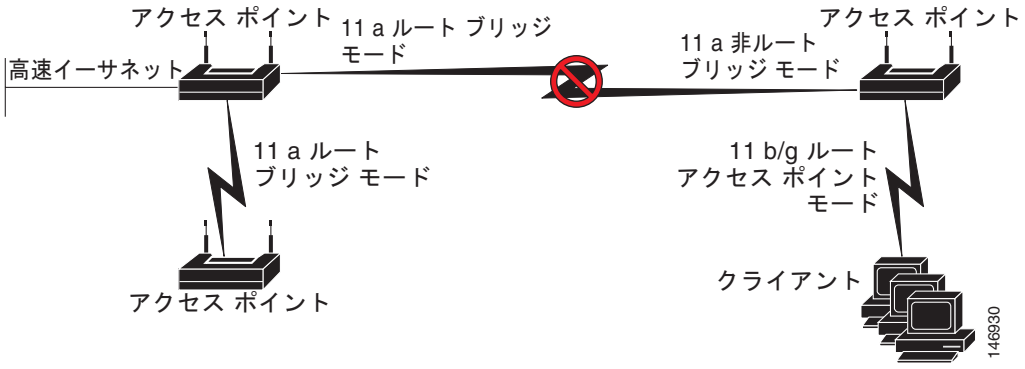
[Stream] ページが表示されます。

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）ユーザ設定のどちらについても、[Packet Handling] ドロップダウン メニューから [Low Latency] を選択し、対応するフィールドにパケット破棄の最大再試行回数の値を入力します。

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 5-1）。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取得しようとする回数を示します。

図 5-1　　パケット処理の設定



（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。

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。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS含む)
電話受付時間 : 平日 10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter/