Cisco 860 および 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

Cisco 860 and Cisco 880 Series Integrated Services Routers Software Configuration Guide

Text Part Number: OL-18906-01-J

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

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

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

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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

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

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

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

Cisco 860 および 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
© 2008, 2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2008–2010, シスコシステムズ合同会社 .
All rights reserved.

CONTENTS

OL-18906-01-J i

はじめに

ここでは、このマニュアルの目的、対象読者、構成、表記方法について説明するとともに、追加の情報が記載されている関連マニュアルについて説明します。この章の内容は次のとおりです。

目的

このマニュアルでは、Cisco 860、Cisco 880、および Cisco 890 シリーズ Integrated Services Router（ISR; サービス統合型ルータ）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。一部の情報は、特定のルータ モデルに該当しない場合があります。

保証、サービス、サポート情報については、ルータ付属の『*Readme First for the Cisco 800 Series Integrated Services Routers*』の「Cisco One-Year Limited Hardware Warranty Terms」のセクションを参照してください。

対象読者

このマニュアルは、技術的な知識を持ち、シスコのルータと Cisco IOS ソフトウェアおよび機能について熟知しているシスコ機器プロバイダーを対象にしています。

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。

概要 / はじめに	
製品の概要	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 デバイスの概要	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。
基本的なルータの設定	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。
ルータの設定	
バックアップ データ ラインおよびリモート管理の設定	リモート管理機能とバックアップ データ回線接続を設定するための手順について説明します。
セキュリティ機能の設定	ルータで設定可能なセキュリティ機能を実装するための手順について説明します。
イーサネット スイッチの設定	ルータの 4 ポート ファスト イーサネット スイッチの設定作業の概要について説明します。
音声機能の設定	音声設定のための手順が記載された参考資料を示します。
ワイヤレス デバイスの設定と管理	
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	ワイヤレス デバイスの無線設定を行う方法について説明します。
ワイヤレス デバイスの管理	ワイヤレス デバイスの管理のさまざまな側面について説明します。
追加情報	
構成例	Cisco 860、Cisco 880、および Cisco 890 シリーズ ISR の一般的な構成例をいくつか示します。
トラブルシューティング	発生する可能性がある問題を切り分けるのに役立つ情報を提供します。
参考資料（付録）	
付録 A「Cisco IOS ソフトウェアの基礎知識」	Cisco IOS ソフトウェアを使用してルータを設定するための方法を説明します。
付録 B「概要」	Internet Service Provider（ISP; インターネット サービス プロバイダー）またはネットワーク管理者がシスコのルータを設定する際に役立つ機能の概要について説明します。
付録 C「ROM モニタ」	シスコの ROM モニタ ファームウェアを使用する方法について説明します。
付録 D「共通ポート割り当て」	現在割り当てられている Transmission Control Protocol（TCP; 伝送制御プロトコル）ポート番号を示します。

表記法

これらのマニュアルでは、表 1 に示す表記法を使用して説明および情報を表示しています。

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。
[　]	省略可能なキーワードまたは引数は、角カッコ内に示しています。
{**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 つを選択する必要があります。
`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の例です。
<　>	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、追加の情報やマニュアルの参照先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。

ワンポイントアドバイス　「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

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 860, Cisco 880, and Cisco 890 Series ISR Software Configuration Guide*』（このマニュアル）に加えて、Cisco 860、Cisco 880、および Cisco 890 シリーズ ISR には次のマニュアルがあります。

- 『*Readme First for the Cisco 800 Series Integrated Services Routers*』
- 『*Cisco 860 and Cisco 880 Series Integrated Services Routers Hardware Installation Guide*』
- 『*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*』
- 『*Cisco Software Licensing Feature Guide*』
- 『*Cisco IOS Release Notes* for Cisco IOS Release 12.4(15)XZ』

必要に応じて次のマニュアルも参照してください。

- 『*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 Gateways*』
- 『*Cisco Software Activation Conceptual Overview*』
- 『*Cisco Software Activation Tasks and Commands*』

シスコのマニュアルの検索方法

ブラウザを使用して Hyper Text Markup Language（HTML）マニュアルを検索するには、Ctrl+F（Windows の場合）または Cmd+F（Apple の場合）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。

PART 1

概要 / はじめに

CHAPTER 1

製品の概要

この章では、Cisco 860、Cisco 880、および Cisco 890 シリーズ Integrated Services 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。

全般的な説明

Cisco 860、Cisco 880、および Cisco 890 シリーズ ISR は、企業の在宅勤者や、ユーザが 20 人未満のリモート オフィスおよびスモール オフィスに対し、インターネット、VPN、音声、データ、およびバックアップ機能を提供します。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。また、Cisco 860W、Cisco 880W、および Cisco 890W シリーズ ISR には、802.11n ワイヤレス LAN オプションがあり、ISR がワイヤレス アクセス ポイントとしての機能を果たすことができます。

Cisco 860 シリーズ ISR

Cisco 860 シリーズ ISR は、構成が固定されたデータ ルータです。次の 3 つのモデルがあり、それぞれ単一の WAN 接続が可能です。

- Cisco 861 および Cisco 861W：Fast Ethernet（FE; ファスト イーサネット）WAN 接続
- Cisco 866：VDSL2 Annex B、DSL over ISDN WAN 接続
- Cisco 867：VDSL2 Annex A、DSL over POTS WAN 接続

次の機能は 3 種類のモデルすべてでサポートされています。

4 ポート 10/100 FE LAN スイッチ

このスイッチは、10/100BASE-T（10/100 Mbps）ファスト イーサネット（FE）LAN またはアクセス ポイントに接続するための 4 つのポートを備えています。

セキュリティ機能

Cisco 860 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。

- IPsec
- ファイアウォール

802.11n ワイヤレス LAN オプション

Cisco 861W ISR には、ワイヤレス LAN 接続のための 802.11b/g/n シングル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。

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および音声ルータ ファミリです。

- 「Cisco 880 シリーズ ISR のモデル」（P.1-2）
- 「共通機能」（P.1-3）
- 「音声機能」（P.1-4）

Cisco 880 シリーズ ISR のモデル

このファミリは、異なる WAN 接続を提供する複数のグループにわかれています。

- Cisco 881 グループ：FE WAN 接続
- Cisco 887V グループ：VDSL2oPOTS WAN 接続
- Cisco 888 グループ：G.SHDSL 2 線式または 4 線式 WAN 接続

Cisco 881 および 888 グループには、次の 3 つのモデルがあります。

- Cisco 880：基本的なデータ ルータ
- Cisco 880G：セルラー データ バックアップを備えたデータ ルータ
- Cisco C880SRST：Survivable Remote Site Telephony（SRST）機能を備えた在宅勤務者向け音声ルータ

Cisco 887 グループは、基本的なデータ ルータだけで構成されます。

各ルータには WAN ポートが 1 つあります。また、音声ルータには、FXS または BRI 音声ポートがあります。また、データまたは音声バックアップ ポートは、ほとんどのルータで利用できます。Cisco 880G ルータには、セルラー バックアップのための市販の第 3 世代（3G）ワイヤレス インターフェイス カードが付属しています。

表 1-1 に、Cisco 880 シリーズ データ ルータのポート構成を示します。

表 1-1　Cisco 880 シリーズ データ ISR のポート構成

モデル	WAN ポート	バックアップ	
		データ ISDN	データ 3G
881 および 881W	FE		
881G および 881GW	FE		x
887V	VDSL2oPOTS	x	
888 および 888W	G.SHDSL	x	
888G および 888GW	G.SHDSL		x

表 1-2 に、Cisco 880 シリーズ音声ルータのポート構成を示します。

表 1-2　Cisco 880 シリーズ音声 ISR のポート構成

モデル	WAN ポート	FXS 音声ポート	バックアップ	
			PSTN FXO	PSTN BRI
C881SRST および C881SRSTW	FE	4	x	
C888SRST および C888CRSTW	G.SHDSL	4		x

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）
- 「802.11n ワイヤレス LAN オプション」（P.1-3）
- 「リアルタイム クロック （RTC）」（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。また、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。

802.11n ワイヤレス LAN オプション

Cisco 880W シリーズ ISR には、ワイヤレス LAN 接続のための、802.11b/g/n シングル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。

リアルタイム クロック（RTC）

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。

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。

- Intrusion Prevention System（IPS; 侵入防御システム）
- Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）
- IPsec
- Quality of service（QoS; サービス品質）
- ファイアウォール
- URL フィルタリング

音声機能

Cisco 880 音声プラットフォーム（C880SRST および C880SRSTW）は、次の音声機能をサポートします。

- シグナリング プロトコル：Session Initiation Protocol（SIP）、Media Gateway Control Protocol（MGCP）、H323
- これらのシグナリング プロトコルのための Real-time transfer protocol（RTP）、Cisco RTP（cRTP）、Secure RTP（SRTP）
- FAX パススルー、Cisco FAX リレー、T37 FAX Store-and-Forward、および T.38 FAX リレー（T.38 ゲートウェイ制御 MGCP FAX リレーを含む）
- Dual Tone MultiFrequency（DTMF; デュアルトーン多重周波数）リレー：OOB および RFC2833
- 無音圧縮とコンフォート ノイズ
- G.711（a-law および u-law）、G.729A、G.729AB、G.729、G.729B、G.726
- WAN 障害の場合の、Foreign Exchange Office（FXO）または PSTN に接続された BRI バックアップ ポートへの SRST フェールオーバーのサポート
- FXS 上の Direct Inward Dialing（DID; ダイヤルイン）

Cisco 890 シリーズ ISR

Cisco 890 シリーズ ISR は、構成が固定されたデータ ルータです。2 つのモデルがあり、それぞれ単一のギガビット イーサネット WAN 接続が可能です。データ バックアップ ポートも使用できます。

表 1-3　Cisco 890 シリーズ ISR のポート構成

モデル	WAN ポート	データ バックアップ		
		FE	V.92	ISDN
891 および 891W	GE	x	x	
892 および 892W	GE	x		x

次の機能がサポートされます。

- 「8 ポート 10/100 FE LAN スイッチ」（P.1-5）
- 「802.11n ワイヤレス LAN オプション」（P.1-5）
- 「リアルタイム クロック（RTC）」（P.1-5）
- 「セキュリティ機能」（P.1-6）

8 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 8 つのポートを備えています。また、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 4 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。

802.11n ワイヤレス LAN オプション

Cisco 890W シリーズ ISR には、ワイヤレス LAN 接続のための 802.11b/g/n および 802.11a/n デュアル無線モジュールが組み込まれています。これら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。

リアルタイム クロック（RTC）

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。

セキュリティ機能

Cisco 890 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。

- Intrusion Prevention System（IPS; 侵入防御システム）
- Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）
- IPsec
- Quality of service（QoS; サービス品質）
- ファイアウォール
- URL フィルタリング

ライセンス

Cisco 860、Cisco 880、および Cisco 890 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 Licensing Manager* を通じて行います。詳細については、Cisco.com にある『*Software Activation On Cisco Integrated Services Routers*』を参照してください。

新しいルータを注文する際、必要なソフトウェア イメージとフィーチャ セットを指定します。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 860、Cisco 880、および Cisco 890 プラットフォームでソフトウェア ライセンスとともに使用できるフィーチャの一覧については、『*Cisco 860 Data Sheet*』、『*Cisco 880 Data Sheet*』、および『Cisco 890 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と管理方法の詳細については、Cisco.com にある『*Cisco IOS Software Activation Tasks and Commands*』を参照してください。

CHAPTER 2

ワイヤレス デバイスの概要

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ワイヤレス LAN ソリューションを提供しています。このワイヤレス 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。アクセス ポイントとして設定されると、ワイヤレス デバイスはワイヤレス ネットワークとワイヤード ネットワークと間の接続ポイントとして機能したり、スタンドアロンのワイヤレス 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、無線範囲内のワイヤレス ユーザは、ファシリティ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。無線範囲内のワイヤレス ユーザは、ファシリティ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 ソフトウェアに基づいた管理システムでは、ワイヤレス デバイスとは Wi-Fi CERTIFIED(TM)、802.11 準拠、802.11b 準拠、802.11g 準拠、および 802.11n 準拠のワイヤレス LAN トランシーバです。

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回復イメージが付属します。デフォルトのモードは Autonomous ですが、アクセス ポイントは Cisco ユニファイド ワイヤレス モードで動作するようにアップグレードできます。

次に、各モードについて説明します。

- **Autonomous モード**：スタンドアロンのネットワーク構成をサポートし、すべての設定はワイヤレス デバイスでローカル管理されます。自律デバイスは、それぞれ自身の初期設定をロードできる一方で、ネットワークとの密接な関係を保ちながら動作します。
- **Cisco Unified Wireless モード**：Cisco Unified Wireless LAN コントローラと連動し、すべての構成情報はコントローラの内部に保持されます。Cisco Unified Wireless LAN アーキテクチャでは、ワイヤレス デバイスは、Leightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）を使用する Lightweight モードで動作します（Autonomous モードとは対照的）。Lightweight アクセス ポイントつまりワイヤレス デバイスには、コントローラに関連付けられない限り、設定はありません。ワイヤレス デバイスの設定は、ネットワーキングが稼動している場合に限り、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 デバイスの設定、ファームウェア、および 802.1x 認証などの制御トランザクションを管理します。すべてのワイヤレス トラフィックはコントローラによってトンネリングされます。

  このネットワーク アーキテクチャ設計の詳細については、Cisco.com の「*Why Migrate to a Cisco Unified Wireless Network?*」を次の URL から参照してください。
  http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_white_paper0900aecd804f19e3_ps6305_Products_White_Paper.html

管理オプション

ワイヤレス デバイスは、ルータ上で動作する Cisco IOS ソフトウェアとは異なる独自のバージョンの Cisco IOS ソフトウェアを実行します。アクセス ポイントは、次のようなツールで設定したり監視したりできます。

- Cisco IOS ソフトウェアの Command-Line Interface（CLI; コマンドライン インターフェイス）
- 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、XP の各プラットフォームで稼動する Microsoft Internet Explorer バージョン 6.0 と完全な互換性があります。また、Windows 98、2000、XP、および Solaris の各プラットフォームで稼動する Netscape バージョン 7.0 とも完全な互換性があります。

（注） CLI 用ツールと Web ブラウザ用ツールを同時に使用してワイヤレス デバイスを設定しないでください。CLI を使用してワイヤレス デバイスを設定すると、設定に関する正確でない説明が Web ブラウザのインターフェイスに表示される場合があります。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。

ワイヤレス デバイスを無線コンフィギュレーション モードにするには、**interface dot11radio** global コンフィギュレーション CLI コマンドを使用します。

ネットワーク構成の例

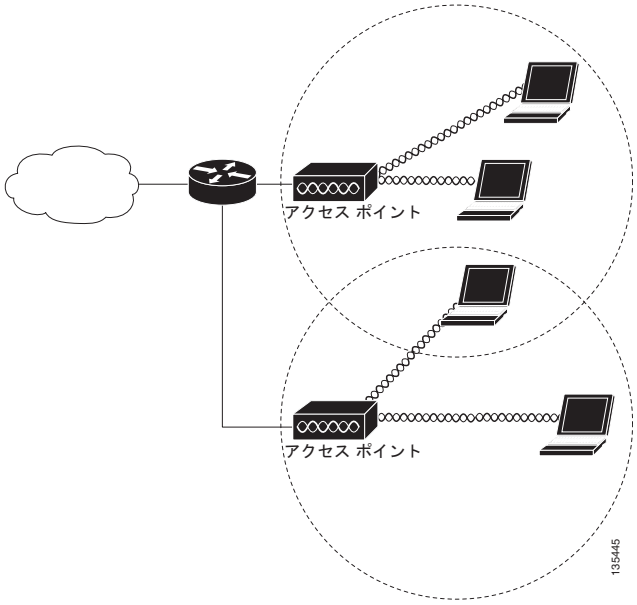
このような一般的なワイヤレス ネットワーク構成にアクセス ポイントの役割を設定します。デフォルトでは、アクセス ポイントは、ワイヤード LAN に接続したルート ユニットとして、または完全なワイヤレス ネットワーク内のセントラル ユニットとして構成されます。アクセス ポイントはブリッジまたはワークグループのブリッジとしても構成できます。これらの役割には特定の構成が必要になります。次の各ページで例を挙げて説明します。

- 「ルート アクセス ポイント」（P.3）
- 「完全なワイヤレス ネットワークでのセントラル ユニット」（P.4）

ルート アクセス ポイント

ワイヤード LAN に直接接続されるアクセス ポイントは、ワイヤレス 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移動することができます。1 つのアクセス ポイントの範囲から外れたユーザは、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（関連付け）されます。このローミング処理は、ユーザにとってシームレスでしかも透過的に行われます。図 1 に、ワイヤード LAN 上でルート ユニットとして機能するアクセス ポイントを示します。

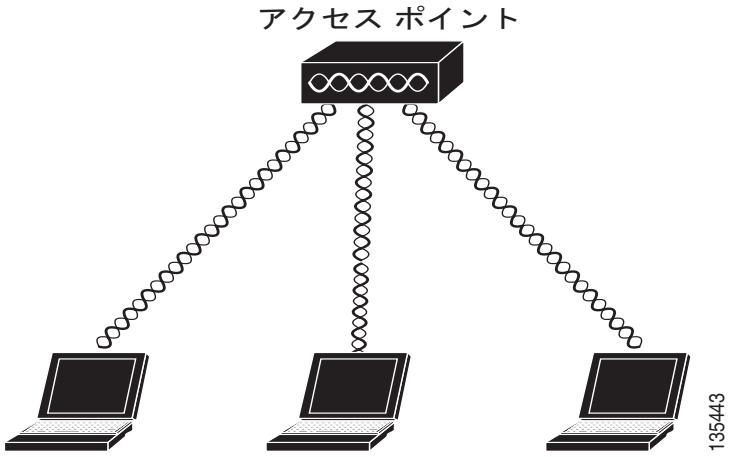
図 1　　ワイヤード LAN 上でルート ユニットとして機能するアクセス ポイント



完全なワイヤレス ネットワークでのセントラル 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。このアクセス ポイントはワイヤード LAN には接続されず、すべての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。つまり、このアクセス ポイントは通信の中心点として動作し、ワイヤレス ユーザの通信範囲を拡張します。図 2 に、完全なワイヤレス ネットワークでのアクセス ポイントを示します。

図 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

基本的なルータの設定

この章では、シスコ 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。

グローバル コンフィギュレーション モードの利用の詳細については、付録 A「Cisco IOS Basic Skills」の「グローバル コンフィギュレーション モードの開始」の項を参照してください。

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　シスコ 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 860 シリーズ、Cisco 880 シリーズ	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 861、861W、881、881W	ファスト イーサネット WAN	WAN、FE4
Cisco 888、888W	G.SHDSL WAN	G.SHDSL

デフォルト設定

シスコ 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 Network Address Translation（NAT; ネットワーク アドレス変換）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）または Password Authentication Protocol（PAP）
  - Internet Service Provider（ISP; インターネット サービス プロバイダー）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。次のようなものがあります。

    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。

音声機器に接続する場合：

- 『*Cisco IOS Voice Port Configuration Guide*』を参照してください。

ソフトウェア ライセンスを取得または変更する場合：

- 『*Software Activation On Cisco Integrated Services Routers*』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、次の作業を行います。

	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)#`
		ライン コンフィギュレーション モードを開始し、ライン タイプを指定します。
		この例では、アクセス用のコンソール端末を指定しています。

ステップ 2	**password** *password*
	
	例：
	`Router(config)# password 5dr4Hepw3`
	`Router(config-line)#`
		コンソール端末ラインの一意なパスワードを指定します。

ステップ 3	**login**
	
	例：
	`Router(config-line)# login`
	`Router(config-line)#`
		端末セッション ログインでパスワード 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)#`
		EXEC コマンド インタープリタがユーザ入力を待機する時間を設定します。デフォルトは 10 分です。秒単位の時間を任意に設定することもできます。
		この例では、タイムアウト時間が 5 分 30 秒であることを示しています。タイムアウト時間を 0 0 に設定すると、タイムアウトは無効になります。

	コマンド	目的

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)#`
		仮想端末ラインの一意な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 ログインでパスワード 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#`
		ライン 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 コマンドを示すものです。

「default」のマークが付いているコマンドは入力する必要がありません。これらのコマンドは、**show running-config** コマンドを使用した場合に生成される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。

	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)#`
		ルータへの不正アクセスを防ぐための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)#`
		ルータが知らない語句（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

Cisco 860 および Cisco 880 シリーズ ISR は、WAN 接続用にそれぞれ 1 つのインターフェイスを持っています。

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）
- 「G.SHDSL WAN インターフェイスの設定」（P.3-9）
- 「セル ワイヤレス WAN インターフェイスの設定」（P.3-12）

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、次の作業を行います。

	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。

G.SHDSL WAN インターフェイスの設定

Cisco 888 ISR で G.SHDSL 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、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# controller dsl 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。
ステップ 2	`Router(config-ctrl)# mode atm`	ATM カプセル化をイネーブルにし、論理 ATM インターフェイス 0 を作成します。
ステップ 3	`Router(config-ctrl)# line-term cpe`	CPE をイネーブルにします。
ステップ 4	`Router(config-ctrl)# line-mode 4 wire standard`	4 線式動作をイネーブルにします。
ステップ 5	`Router(config-ctrl)# line-rate 4608`	SHDSL ポートの DSL ライン レートを指定します。範囲は、192 ～ 2312 kb/s です。デフォルトは、**auto**（SHDSL ポートおよび DSLAM 間でネゴシエートされます）です。 **（注）** 逆側の DSL アップリンクで設定されている DSL ライン レートが異なる場合、実際の DSL ライン レートは、常に、低い方のレートになります。 **（注）** 最大ピーク セル レートは、ライン レートより 8 kb/s 低くなります。
ステップ 6	`Router(config-ctrl)# interface atm0`	インターフェイス ATM 0 の ATM コンフィギュレーションモードを開始します。
ステップ 7	`Router(config-ctrl)#ip-address IP-address`	DSL ATM インターフェイスに IP アドレスを割り当てます。
ステップ 8	`Router(config-ctrl)#load-interval 3`	

	コマンド	目的
ステップ 9	`Router(config-ctrl)# no atm ilmi-keepalive0`	（任意）Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）キープアライブをディセーブルにします。 秒数を指定せずに ILMI キープアライブをイネーブルにした場合、デフォルトで、間隔は 3 秒になります。
ステップ 10	`Router(config-ctrl)# pvc 0/35`	atm-virtual-circuit（interface-atm-vc）コンフィギュレーション モードを開始し、名前（任意）および VPI/VCI 番号を割り当て、新しい ATM PVC を設定します。 デフォルトのトラフィック シェーピングは UBR です。デフォルトのカプセル化は AAL5+LLC/SNAP です。
ステップ 11	`Router(config-ctrl)# protocol ip 10.10.10.2 broadcast`	（任意）IP 接続をイネーブルし、VC のポイントツーポイント IP アドレスを作成します。
ステップ 12	`Router(config-ctrl)# encapsulation aal5snap`	（任意）ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化タイプを設定します。 • **aal2** キーワードを AAL2 に使用します。 • **aal5ciscoppp** キーワードを Cisco PPP over AAL5 に使用します。 • **aal5mux** キーワードを AAL5+MUX に使用します。 • **aal5nlpid** キーワードを AAL5+NLPID に使用します。 • **aal5snap** キーワードを AAL5+LLC/SNAP（デフォルト）に使用します。

例

次の設定例は、4 線式標準 G.SHDSL 設定を示しています。

```
!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
```

```
 isdn termination multidrop
!
!
interface ATM0
 ip address 10.10.10.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 0/35
  protocol ip 10.10.10.2 broadcast
  encapsulation aal5snap
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
 shutdown
!
interface Vlan1
 ip address 2.15.15.26 255.255.255.0
!
ip forward-protocol nd
ip route 223.255.254.254 255.255.255.255 Vlan1
no ip http server
no ip http secure-server
!
```

設定の確認

ルータが正しく設定されているかどうかを確認するには、**show run** コマンドを入力して、コントローラ DSL およびインターフェイス ATM0 パラメータを調べます。

```
Router#sh run
Building configuration...

Current configuration : 1298 bytes
!
.......

!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 dsl-mode shdsl symmetric annex B
 line-rate 4608
!
!
interface ATM0
 ip address 10.10.10.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 0/31
  protocol ip 10.10.10.5 broadcast
  encapsulation aal5snap
 !
```

セル ワイヤレス WAN インターフェイスの設定

Cisco 881G および 888G ISR は、Global System for Mobile Communications（GSM）および Code Division Multiple Access（CDMA; 符号分割多重接続）ネットワークを介して使用する、Third Generation（3G）ワイヤレス インターフェイスを提供します。このインターフェイスは、34-mm PCMCIA スロットです。

その主な用途は、重要なデータ アプリケーションのバックアップ データ リンクとしての WAN 接続です。ただし、3G ワイヤレス インターフェイスは、ルータのプライマリ WAN 接続としても機能できます。

3G セル ワイヤレス インターフェイスを設定するには、次の注意事項および手順に従ってください。

3G ワイヤレス インターフェイスの設定に関する要件

次に、3G ワイヤレス インターフェイスの設定に関する要件を示します。

- 通信事業者のワイヤレス サービスが必要です。また、ルータが物理的に配置されるネットワーク カバレッジも必要です。サポートされている通信事業者の詳細リストについては、次の URL のデータ シートを参照してください。

  http://www.cisco.com/en/US/prod/routers/networking_solutions_products_genericcontent0900aecd80601f7e.html

- ワイヤレス サービス プロバイダーとのサービス プランに契約し、そのサービス プロバイダーから SIM カード（GSM モデムだけ）を取得する必要があります。
- 表 3-2 の信号強度を参照して、LED をチェックしなければなりません。
- Cisco IOS ソフトウェアの Cisco 3G ワイヤレス サポートの Cisco IOS リリース 12.4(15)XZ 以降を十分に理解している必要があります（Cisco IOS 資料を参照してください）。
- GSM データ プロファイルを設定するには、サービス プロバイダーから次の情報を取得する必要があります。
  - ユーザ名
  - パスワード
  - Access Point Name（APN; アクセス ポイント ネーム）
- 手動でアクティブにするために CDMA データ プロファイルを設定するには、サービス プロバイダーから次の情報を取得する必要があります。
  - Master Subsidy Lock（MSL）番号
  - Mobile Directory Number（MDN）
  - Mobile Station Identifier（MSID）
  - Electronic Serial Number（ESN）

表 3-2　前面パネル LED の信号強度表示

LED	LED カラー	信号強度
3G RSSI[1]	オレンジ	使用できるサービスがなく、RSSI が検出されません
	グリーンが点灯	高速 RSSI（-69 dBm 以上）
	グリーンが素早く（16 Hz）点滅	中速 RSSI（-89 ～ -70 dBm）
	グリーンがゆっくり（1 Hz）点滅	低～中速 RSSI（-99 ～ -90 dBm）、信頼できる接続の最小レベル
	消灯	低速 RSSI（-100 dBm 未満）

1. 3G 受信信号強度表示

セル ワイヤレス インターフェイスの設定に関する制約事項

Cisco 3G ワイヤレス インターフェイスの設定には、次の制約事項があります。

- データ接続は、3G ワイヤレス インターフェイスだけから行うことができます。リモート ダイヤルインはサポートされていません。
- ワイヤレス通信共通の性質により、スループットは、ネットワークでのアクティブ ユーザの数や輻輳の量により異なります。
- セル ネットワークの遅延は、優先ネットワークの場合よりも大きくなります。遅延レートは、テクノロジーおよび通信事業者により異なります。ネットワーク輻輳が発生している場合、遅延が大きくなることがあります。
- VoIP は現在サポートされていません。
- 通信事業者のサービス条件に含まれるいずれの制約事項も Cisco 3G ワイヤレス インターフェイスに適用されます。
- Cisco 880G ISR は、3G モデムの Online Insertion and Removal（OIR; 活性挿抜）をサポートしません。モデムをモデム タイプが同じ別のモデルと交換するには、モデムを交換する前に、Cisco CLI を使用して、セル インターフェイスで **shutdown** コマンドを入力します。
- 3G モデルが取り外されても、**show interface cellular 0**、**show run** および **show version** 出力に、セル インターフェイスに関する情報が表示されます。**show interface** コマンドは、次のメッセージを表示します。その他のすべてのコマンドは空の出力を表示します。

  ```
  3G Modem not inserted
  ```

- 3G モデムが取り外されている状態でセル インターフェイスを設定できます。ただし、3G モデムが取り付けられるまで、設定は有効になりません。モデムが取り付けられていない状態でセル インターフェイスを設定しようとすると、次のメッセージが表示されます。

  ```
  Router(config)#interface cellular 0
  Warning: 3G Modem is not inserted
  Configuration will not be effective until modem is inserted
  ```

- 取り外したモデムとタイプが異なるモデムを取り付ける場合、設定を変更し、システムをリロードしなければなりません。

データ アカウント プロビジョニング

（注）　モデムをプロビジョニングするには、サービス プロバイダーとのアクティブ ワイヤレス アカウントが必要です。SIM カードを GSM 3G ワイヤレス カードに挿入する必要があります。

データ アカウントをプロビジョニングするには、次の手順を行います。

- 「信号強度およびサービス アベイラビリティの確認」（P.3-14）
- 「GSM モデル データ プロファイルの設定」（P.3-15）
- 「CDMA モデム アクティベーションおよびプロビジョニング」（P.3-16）

信号強度およびサービス アベイラビリティの確認

モデムの信号強度およびサービス アベイラビリティを確認するには、特権 EXEC モードで、次のコマンドを使用します。

手順概要

1. **show cellular 0 network**
2. **show cellular 0 hardware**
3. **show cellular 0 connection**
4. **show cellular 0 radio**
5. **show cellular 0 profile**
6. **show cellular 0 security**
7. **show cellular 0 all**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	Router# **show cellular 0 network** **例：** Router# show cellular *0* network	通信事業者ネットワーク、セル サイト、および使用可能なサービスに関する情報を表示します。
ステップ 2	Router# **show cellular 0 hardware** **例：** Router# show cellular 0 hardware	セル モデム ハードウェア情報を表示します。
ステップ 3	Router# **show cellular 0 connection** **例：** Router# show cellular 0 connection	現在アクティブな接続状態およびデータの統計情報を表示します。

	コマンドまたはアクション	目的
ステップ 4	Router# **show cellular 0 radio** **例：** Router# show cellular 0 radio	ラジオ信号強度を示します。 **（注）** 接続が安定し信頼できる状態であるには RSSI が -90 dBm 以上でなければなりません。
ステップ 5	Router# **show cellular 0 profiles** **例：** Router# show cellular 0 profile	作成されたモデム データ プロファイルに関する情報を示します。
ステップ 6	Router# **show cellular 0 security** **例：** Router# show cellular *0* security	SIM およびモデム ロック ステータスなど、モデルのセキュリティ情報を示します。
ステップ 7	Router# **show cellular 0 all** **例：** Router# show cellular 0 all	モデムに関する統合情報を示します。たとえば、作成されたプロファイル、ラジオ信号強度、ネットワーク セキュリティなどです。

GSM モデル データ プロファイルの設定

新しいモデム データ プロファイルを設定または作成するには、特権 EXEC モードで、次のコマンドを入力します。

手順概要

1. **cellular gsm profile create** <*profile number*> <*apn*> <*authentication*> <*username*> <*password*>

詳細手順

コマンドまたはアクション	目的
Router# **cellular 0 gsm profile create** <*profile number*> <*apn*> <*authentication*> <*username*> <*password*> **例：** Router# cellular 0 gsm profile create 3 apn.com chap GSM GSMPassword	新しいモデム データ プロファイルを作成します。コマンド パラメータの詳細については、表 3-3 を参照してください。

次の表は、モデム データ プロファイル パラメータのリストを示します。

表 3-3　　モデム データ プロファイル パラメータ

profile number	作成するプロファイルの番号。最大 16 のプロファイルを作成できます。
apn	アクセス ポイント ネーム。この情報をサービス プロバイダーから取得する必要があります。
authentication	認証のタイプ。たとえば、CHAP、PAP です。
Username	サービス プロバイダーにより提供されるユーザ名。
Password	サービス プロバイダーにより提供されるパスワード。

CDMA モデム アクティベーションおよびプロビジョニング

アクティベーション手順は、通信事業者により異なります。通信事業者に問い合せて、次のいずれかの手順を実行してください。

- 手動によるアクティベーション
- 地上波サービス プロビジョニングを使用したアクティベーション

次の表は、さまざまなワイヤレス通信事業者によりサポートされているアクティベーションおよびプロビジョニング プロセスのリストを示します。

アクティベーションおよびプロビジョニング プロセス	通信事業者
MDN、MSID、MSL を使用した手動によるアクティベーション	Sprint
OTASP[1] アクティベーション	Verizon Wireless
データ プロファイル リフレッシュ用 IOTA[2]	Sprint

1. 地上波サービス プロビジョニング
2. インターネット地上波

手動によるアクティベーション

（注） この手順を開始する前に、有効な Mobile Directory Numner（MDN）、Mobile Subsidy Lock（MSL）、および Mobile Station Identifier（MSID）情報を通信事業者から取得しておく必要があります。

モデム プロファイルを手動で設定するには、EXEC モードから、次のコマンドを使用します。

cellular 0 cdma activate manual mdn msid sid nid msl

アクティブ化される前に、モデル データ プロファイルのプロビジョニングが、Internet Over the Air（IOTA; インターネット地上波）プロセスを介して行われます。IOTA プロセスは、**cellular cdma activate manual** コマンドを使用すると自動的に開始されます。

次に、このコマンドの出力例を示します。

```
router# cellular 0 cdma activate manual 1234567890 1234567890 1234 12 12345
NAM 0 will be configured and will become Active
Modem will be activated with following Parameters
MDN :1234567890; MSID :1234567890; SID :1234; NID 12:
Checking Current Activation Status
Modem activation status: Not Activated
```

```
Begin Activation
Account activation - Step 1 of 5
Account activation - Step 2 of 5
Account activation - Step 3 of 5
Account activation - Step 4 of 5
Account activation - Step 5 of 5
Secure Commit Result: Succeed
Done Configuring - Resetting the modem
The activation of the account is Complete
Waiting for modem to be ready to start IOTA
Beginning IOTA
router#
*Feb  6 23:29:08.459: IOTA Status Message Received. Event: IOTA Start, Result: SUCCESS
*Feb  6 23:29:08.459: Please wait till IOTA END message is received
*Feb  6 23:29:08.459: It can take up to 5 minutes
*Feb  6 23:29:27.951: OTA State = SPL unlock, Result = Success
*Feb  6 23:29:32.319: OTA State = Parameters commited to NVRAM, Result = Success
*Feb  6 23:29:40.999: Over the air provisioning complete; Result:Success
*Feb  6 23:29:41.679: IOTA Status Message Received. Event: IOTA End, Result: SUCCESS
```

IOTA Start および IOTA End には、結果の出力として「SUCCESS」と示されていなければなりません。エラー メッセージが表示された場合、**cellular cdma activate iota** コマンドを使用して個別に IOTA を実行できます。

通信事業者により、データ プロファイルの定期的なリフレッシュが要求されることがあります。データ プロファイルをリフレッシュするには、次のコマンドを使用します。

cellular cdma activate iota

Over-the-Air Service Provisioning を使用したアクティベーション

Over-the-Air Service Provisioning（OTASP）のプロビジョニングおよびアクティベーションを行うには、EXEC モードから、次のコマンドを使用します。

cellular 0 cdma activate otasp phone_number

（注）　このコマンドで使用する電話番号は、通信事業者から取得する必要があります。標準の OTASP 発番号は *22899 です。

次に、このコマンドの出力例を示します。

```
router# cellular 0 cdma activate otasp  *22899
Beginning OTASP activation
OTASP number is *22899
steelers_c881G#
OTA State = SPL unlock, Result = Success
router#
OTA State = PRL downloaded, Result = Success
OTA State = Profile downloaded, Result = Success
OTA State = MDN downloaded, Result = Success
OTA State = Parameters commited to NVRAM, Result = Success
Over the air provisioning complete; Result:Success
```

セル インターフェイスの設定

セル インターフェイスを設定するには、特権 EXEC モードから、次のコマンドを入力します。

手順概要

1. **configure terminal**
2. **interface cellular 0**
3. **encapsulation ppp**
4. **ppp chap hostname** <*host*>
5. **ppp chap password 0** <*password*>
6. **asynchronous mode interactive**
7. **ip address negotiated**

（注） この手順で使用する PPP Challenge Handshake Authentication Protocol（CHAP）認証パラメータは、通信事業者により提供され、GSM プロファイル下だけで設定されているユーザ名およびパスワードと同じでなければなりません。CDMA では、ユーザ名またはパスワードは必要ありません。

詳細手順

	コマンドまたはアクション	目的
ステップ 1	`Router# configure terminal` **例：** `Router# configure terminal`	端末からグローバル 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	`Router(config)# interface cellular 0`
	
	例：
	`Router (config)# interface cellular 0`
		セル インターフェイスを指定します。

ステップ 3	`Router(config-if)# encapsulation ppp`
	
	例：
	`Router (config-if)# encapsulation ppp`
		専用非同期モードまたは Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）に設定されているインターフェイスの PPP カプセル化を指定します。

ステップ 4	`Router(config-if)# ppp chap hostname` <*hostname*> **例：** `Router (config-if)# ppp chap hostname cisco@wwan.ccs`	インターフェイス固有の Challenge Handshake Authentication Protocol（CHAP）ホスト名を定義します。これは、通信事業者により提供されるユーザ名と一致しなければなりません。GSM だけに適用されます。
ステップ 5	`Router(config-if)# ppp chap password 0` <*password*> **例：** `Router (config-if)# ppp chap password 0 cisco`	インターフェイス固有の CHAP パスワードを定義します。これは、通信事業者により提供されるパスワードと一致しなければなりません。

	コマンドまたはアクション	目的
ステップ 6	Router(config-if)# **asynchronous mode interactive** **例：** Router (config-if)# asynchronous mode interactive	ラインを専用非同期ネットワーク モードから対話モードに戻して、特権 EXEC モードで、**slip** および **ppp** コマンドをイネーブルにします。
ステップ 7	Router(config-if)# **ip address negotiated** **例：** Router (config-if)# ip address negotiated	特定のインターフェイスの IP アドレスが PPP および IPCP アドレス ネゴシエーションを介して取得されることを指定します。

（注）　セル インターフェイスでスタティック IP アドレスが必要な場合、アドレスは、**ip address negotiated** として設定できます。Internet Protocol Control Protocol（IPCP; インターネット プロトコル コントロール プロトコル）を介して、ネットワークにより、正しいスタティック IP アドレスがデバイスに割り当てられるようになります。トンネル インターフェイスが **ip address unnumbered** <*cellular interface*> で設定されている場合、実際のスタティック IP アドレスは、**ip address negotiated** でなく、セル インターフェイス下で設定されなければなりません。セル インターフェイスの設定例については、「セル インターフェイスの基本設定」（P.3-22）を参照してください。

DDR の設定

セル インターフェイスのダイヤルオンデマンド ルーティング（DDR）を設定するには、次の手順を実行します。

手順概要

1. **configure terminal**
2. **interface cellular 0**
3. **dialer in-band**
4. **dialer idle-timeout** <*seconds*>
5. **dialer string** <*string*>
6. **dialer group** <*number*>
7. **exit**
8. **dialer-list** <*dialer-group*> **protocol** <*protocol-name*> {**permit** | **deny** | **list** <access-list-number> | **access-group**}>
9. **ip access-list <*access list number*> permit** <*ip source address*>
10. **line 3**
11. **script dialer** <*regexp*>
12. **exit**
13. **chat-script** <*script name*> ”” “**ATDT*99***<*profile number*>#” **TIMEOUT** <*timeout value*> **CONNECT**
14. **interface cellular 0**
15. **dialer string** <*string*>

詳細手順

	コマンドまたはアクション	目的
ステップ 1	Router# **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	Router(config)# **interface cellular 0** **例：** Router (config)# interface cellular 0	セル インターフェイスを指定します。
ステップ 3	Router(config-if)# **dialer in-band** **例：** Router (config-if)# dialer in-band	DDR をイネーブルにし、インバンド ダイヤリングに指定されたシリアル インターフェイスを設定します。
ステップ 4	Router(config-if)# **dialer idle-timeout** *<seconds>* **例：** Router (config-if)# dialer idle-timeout 30	回線が切断されるまでのアイドル時間を秒単位で指定します。
ステップ 5	Router(config-if)# **dialer string** *<string>* **例：** Router (config-if)# dialer string gsm	ダイヤルする番号またはストリングを指定します。チャット スクリプトの名前をここで使用します。
ステップ 6	Router(config-if)# **dialer-group** *<number>* **例：** Router (config-if)# dialer-group 1	特定のインターフェイスが属するダイヤラ アクセス グループの番号を指定します。
ステップ 7	Router(config-if)# **exit** **例：** Router (config-if)# exit	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 8	Router(config)# **dialer-list** *<dialer-group>* **protocol** *<protocol-name>* {**permit** | **deny** | **list** <access-list-number> | **access-group**}> **例：** Router (config)# dialer-list 1 protocol ip list 1	対象トラフィックのダイヤラ リストを作成して、すべてのプロトコルへのアクセスを許可します。
ステップ 9	Router(config)# **ip access-list** *<access list number>* **permit** *<ip source address>* **例：** Router (config)# ip access list 1 permit any	対象トラフィックを定義します。

	コマンドまたはアクション	目的
ステップ 10	Router(config)# **line 3** **例：** Router (config-line)# line 3	ライン コンフィギュレーション モードを指定します。これは常に 3 です。
ステップ 11	Router(config-line)**script dialer** *<regexp>* **例：** Router (config-line)# script-dialer gsm	デフォルト モデム チャット スクリプトを指定します。
ステップ 12	Router(config-line)**exit** **例：** Router (config-line)# exit	ライン コンフィギュレーション モードを終了します。
ステップ 13	For GSM: Router(config)# **chat-script** *<script name>* ”” **“ATDT*99*** *<profile number>* **#” TIMEOUT** *<timeout value>* **CONNECT** For CDMA: Router(config)# **chat-script** <script name> "" **"ATDT*777*** <profile number> **#" TIMEOUT** <timeout value> **CONNECT** **例：** Router (config)# chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT“	ラインが GSM 用です。 ラインが CDMA 用です。 ダイヤラが開始されるときの Attention Dial Tone（ATDT）コマンドを定義します。
ステップ 14	Router(config)# **interface cellular 0** **例：** Router (config)# interface cellular 0	セル インターフェイスを指定します。
ステップ 15	Router(config-if)# **dialer string** *<string>* **例：** Router (config)# dialer string gsm	ダイヤラ スクリプト（**chat script** コマンドを使用して定義されます）を指定します。

セル ワイヤレス インターフェイスの設定例

ここでは、次の設定例を示します。

- 「セル インターフェイスの基本設定」（P.3-22）
- 「セル インターフェイス設定を介したトンネル」（P.3-23）

セル インターフェイスの基本設定

次に、プライマリ WAN 接続として使用される gsm セル インターフェイスを設定する例を示します。これは、デフォルト ルートとして設定されます。

```
chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT"

!
interface Cellular0
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer string gsm
 dialer-group 1
 async mode interactive
 ppp chap hostname cisco@wwan.ccs
 ppp chap password 0 cisco
 ppp ipcp dns request
!

ip route 0.0.0.0 0.0.0.0 Cellular0
!
!
access-list 1 permit any
dialer-list 1 protocol ip list 1
!
line 3
 exec-timeout 0 0
 script dialer gsm
 login
 modem InOut
```

次に、プライマリとして使用される cdma セル インターフェイスを設定する例を示します。これは、デフォルト ルートとして設定されます。

```
chat-script cdma "" "ATDT#777" TIMEOUT 60 "CONNECT"

!
interface Cellular0
 ip address negotiated
 encapsulation ppp
 dialer in-band
 dialer string cdma
 dialer-group 1
 async mode interactive
 ppp chap password 0 cisco
!

ip route 0.0.0.0 0.0.0.0 Cellular0
!
!
access-list 1 permit any
dialer-list 1 protocol ip list 1
!
line 3
 exec-timeout 0 0
 script dialer cdma
 login
 modem InOut
```

セル インターフェイス設定を介したトンネル

次に、トンネル インターフェイスが **ip address unnumbered** <*cellular interface*> コマンドで設定される場合のスタティック IP アドレスを設定する例を示します。

```
interface Tunnel2
 ip unnumbered Cellular0
 tunnel source Cellular0
 tunnel destination 128.107.248.254

interface Cellular0
 bandwidth receive 1400000
 ip address 23.23.0.1 255.255.0.0
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string dial<carrier>
 dialer-group 1
 async mode interactive
 no ppp lcp fast-start
 ppp chap hostname <hostname>        *** gsm only ***
 ppp chap password 0 <password>
 ppp ipcp dns request

! traffic of interest through the tunnel/cellular interface
ip route 10.10.0.0 255.255.0.0 Tunnel2
```

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。必要に応じて、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。VLAN 作成の詳細については、第 6 章「イーサネット スイッチの設定」を参照してください。

ワイヤレス LAN インターフェイスの設定

Cisco 861W ISR および Cisco 880W シリーズ ISR は、ワイヤレス LAN 接続の統合 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、第 8 章「ワイヤレス デバイスの基本設定」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、次の手順を実行します。

	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 アドレスおよびサブネット 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

設定例のループバック 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で Network Address Translation（NAT; ネットワーク アドレス変換）をサポートするために使用されます。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。このループバック 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 を指します。

```
!
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ているかどうかを確認するには、**show interface loopback** コマンドを入力します。確認出力は、次の例のように表示されます。

```
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
```

インターフェイスに対して ping を実行してループバック インターフェイスを確認することもできます。

```
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 ルートを使用すると、ネットワーク内で固定ルーティング パスを利用できます。スタティック ルートは、ルータ上で手動で設定します。ネットワーク トポロジーが変化した場合には、新しいルートを使用してスタティック ルートを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、プライベートなルートです。

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、次の手順を実行します。

	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 モードに戻ります。

スタティック ルーティングの一般的な説明については、付録 B「フローティング スタティック ルート」を参照してください。

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。これらのパケットは設定された PVC へ送信されています。

「**default**」のマークが付いているコマンドは入力する必要がありません。このコマンドは、**show running-config** コマンドを使用した場合に生成される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ている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 ルートを調べます。

確認出力は、次のように表示されます。

```
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 プロトコルは、ネットワーク トラフィックまたはネットワーク トポロジーに基づき自動的にパスを調整します。ダイナミック ルートの変更は、ネットワーク上の他のルータと共有されます。

シスコ ルータは、Routing Information Protocol（RIP）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。ルータでは RIP または EIGRP のいずれかのルーティング プロトコルを設定できます。

- 「Routing Information Protocol の設定」（P.3-28）
- 「Enhanced Interior Gateway Routing Protocol の設定」（P.3-29）

Routing Information Protocol の設定

ルータ上で 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、次の作業を行います。

	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、ルータ上で 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 バージョン 1 または 2 を使用することを指定します。

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)#`
		RIP 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各ネットワークのネットワーク アドレスを使用）。

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。その結果、サブプレフィクス ルーティング情報がクラスフル ネットワーク境界を超えて伝送されます。

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 モードに戻ります。

RIP に関する一般的な説明については、付録 B「RIP」を参照してください。

例

次に、IP ネットワーク 10.0.0.0 および 192.168.1.0 で RIP バージョン 2 をイネーブルにする設定例を示します。

この設定を参照するには、特権 EXEC モードから、**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 が正しく設定されている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 ルートを調べます。確認出力は、次の例のように表示されます。

```
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
```

Enhanced Interior Gateway Routing Protocol の設定

Enhanced Interior Gateway Routing Protocol GRP（EGRP）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、次の作業を行います。

	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。自律システム番号は、他の EIGRP ルータへのルートを表し、EIGRP 情報のタグ付けに使用されます。

	コマンド	目的

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 モードに戻ります。

EIGRP の概要については、付録 B「EIGRP」を参照してください。

例

次に、IP ネットワーク 192.145.1.0 および 10.10.12.115 で EIGRP ルーティング プロトコルをイネーブルにする設定例を示します。EIGRP 自律システム番号は、109 に設定されています。

この設定を参照するには、特権 EXEC モードから、**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 が正しく設定されている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 ルートを調べます。確認出力は、次の例のように表示されます。

```
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
```

PART 2

ルータの設定

CHAPTER 4

バックアップ データ ラインおよびリモート管理の設定

この章では、次の項で、バックアップ データ ラインおよびリモート管理の設定について説明します。

Cisco 880 シリーズ Integrated Services Router（ISR; サービス統合型ルータ）は、WAN のダウンタイムを削減するバックアップ データ ラインとのバックアップ データ接続をサポートします。

（注） ビデオ バックアップは、ルータ モデル C881SRST および C888SRST で使用できます。ビデオ バックアップの設定については、第 7 章「音声機能の設定」を参照してください。

Cisco 880 ISR は、次のようにリモート管理機能をサポートします。

- 任意の Cisco 880 シリーズ ISR の AUX ポートを使用
- Cisco 880 シリーズ ISR の ISDN S/T ポートを使用

（注） Cisco 880 シリーズ ISR では、コンソール ポートおよび AUX ポートは、同じ物理 RJ-45 ポートにあります。そのため、これら 2 つのポートを同時にアクティブにできません。Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して、目的の機能をイネーブルにする必要があります。

バックアップ インターフェイスの設定

プライマリ インターフェイスがダウンしていることをルータが検出した場合、バックアップ インターフェイスはイネーブルになっています。指定された期間中にプライマリ接続が復旧した場合、バックアップ インターフェイスがディセーブルになります。

バックアップ インターフェイスがスタンバイ モードから起動した場合も、ルータはそのバックアップ インターフェイスに関する指定されたトラフィックを受信しない限り、バックアップ インターフェイスをイネーブルにしません。

表 4-1 に、各 Cisco 880 ISR で使用できるバックアップ インターフェイス、およびポート指定を示します。これらのインターフェイスの基本設定は、第 3 章「基本的なルータの設定」の「WAN インターフェイスの設定」（P.3-7）に示します。

表 4-1　モデル番号およびデータ ライン バックアップ機能

ルータ モデル番号	ISDN	3G
881G	—	あり
888G	—	あり
888	あり	—

ルータでバックアップ 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、次の作業を行います。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface atm 0`
	`Router(config-if)#`
		バックアップの設定を行うインターフェイスで、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。
		
		ここで指定できるのは、シリアル インターフェイス、ISDN インターフェイス、または非同期インターフェイスです。
		
		この例では、ATM WAN 接続のバックアップ インターフェイスを設定しています。

ステップ 2	**backup interface** *interface-type interface-number*
	
	例：
	`Router(config-if)# backup interface bri 0`
	`Router(config-if)#`
		インターフェイスをセカンダリ、つまりバックアップ インターフェイスとして割り当てます。
		
		ここで指定できるインターフェイスは、シリアル インターフェイスまたは非同期インターフェイスです。たとえば、シリアル 0 インターフェイスのバックアップとしてシリアル 1 インターフェイスを設定できます。
		
		この例では、ATM 0 インターフェイスのバックアップ インターフェイスとして BRI インターフェイスを設定しています。

ステップ 3	**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。

セル ダイヤルオンデマンド ルーティング バックアップの設定

プライマリ接続を監視し、必要に応じてセル インターフェイスを介してバックアップ接続を開始するには、ルータは、次のいずれかの方法を使用できます。

- バックアップ インターフェイス：プライマリ インターフェイス ライン プロトコルが停止していることが検出されてから、起動されるまで、スタンバイ モードを維持するバックアップ インターフェイス。「バックアップ インターフェイスの設定」（P.4-1）を参照してください。
- ダイヤラ ウォッチ：ダイヤラ ウォッチは、ダイヤル バックアップとルーティング機能を統合するバックアップ機能です。「ダイヤラ ウォッチを使用した DDR バックアップの設定」（P.4-3）を参照してください。
- フローティング スタティック ルート：バックアップ インターフェイスを介したルートの管理距離は、プライマリ接続ルートよりも長いため、プライマリ インターフェイスがダウンするまで、ルーティング テーブルに格納されません。プライマリ インターフェイスがダウンすると、フローティング スタティック ルートが使用されます。「フローティング スタティック ルートを使用した DDR バックアップの設定」（P.4-5）を参照してください。

（注）　セル インターフェイスのバックアップ インターフェイスおよびその他の任意の非同期シリアル インターフェイスは設定できません。

ダイヤラ ウォッチを使用した DDR バックアップの設定

ダイヤラ ウォッチを開始するには、Dial-On-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）およびバックアップを実行するインターフェイスを設定する必要があります。ダイヤラ マップなど、DDR 機能の従来の DDR コンフィギュレーション コマンドを使用します。バックアップ インターフェイスでダイヤラ ウォッチをイネーブルにして、ダイヤラ リストを作成するには、インターフェイス コンフィギュレーション モードで、次のコマンドを使用します。

手順概要

1. **configure terminal**
2. **interface** *type number*
3. **dialer watch group** *group-number*
4. **dialer watch-list** *group-number* **ip** *ip-address address-mask*
5. **dialer-list** <*dialer-group*> **protocol** <*protocol name*> {**permit** | **deny** | **list** <*access list number*> | **access-group**}
6. **ip access-list** <*access list number*> **permit** <*ip source address*>
7. **interface cellular** *0*
8. **dialer string** <*string*>

詳細手順

	コマンドまたはアクション	目的
ステップ 1	Router# **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	Router(config)# **interface** *type number* **例：** Router (config)# interface ATM0	インターフェイスを指定します。
ステップ 3	Router(config-if)**# dialer watch-group** *group-number* **例：** Router(config-if)# dialer watch-group 2	バックアップ インターフェイスでダイヤラ ウォッチをイネーブルにします。
ステップ 4	Router(config)# **dialer watch-list** *group-number* **ip** *ip-address address-mask* **例：** Router(config-if)# dialer watch-list 2 ip 10.4.0.254 255.255.0.0	ウォッチ対象のすべての IP アドレスのリストを定義します。
ステップ 5	Router(config)# **dialer-list** *<dialer-group>* **protocol** *<protocol-name>* {**permit** | **deny** | **list** <access-list-number> | **access-group**}> **例：** Router(config)# dialer-list 2 protocol ip permit	対象トラフィックのダイヤラ リストを作成して、すべてのプロトコルへのアクセスを許可します。
ステップ 6	Router(config)# **ip access-list** *<access list number>* **permit** *<ip source address>* **例：** Router(config)# access list 2 permit 10.4.0.0	対象トラフィックを定義します。 **access list permit all** コマンドを使用して、トラフィックの IP ネットワークへの送信を回避しないでください。このようにすると、コールが終了することがあります。

	コマンドまたはアクション	目的
ステップ 7	Router(config)# **interface cellular** *0* **例：** Router (config)# interface cellular 0	セル インターフェイスを指定します。
ステップ 8	Router(config-if)# **dialer string** <*string*> または Router(config-if)# **dialer group** <*dialer group number*> **例：** Router (config-if)# dialer string cdma *** cdma *** または Router (config-if)# dialer group 2 *** gsm ***	CDMA だけ。ダイヤラ スクリプト（**chat script** コマンドを使用して定義されます）を指定します。 GSM だけ。ダイヤラ リストをダイヤラ インターフェイスにマッピングします。

フローティング スタティック ルートを使用した DDR バックアップの設定

フローティング スタティック デフォルト ルートをセカンダリ インターフェイスで設定するには、グローバル コンフィギュレーション モードから、次のコマンドを使用します。

（注） ルータで IP クラスがイネーブルになっていることを確認してください。

手順概要

1. **configure terminal**
2. **ip route** *network-number network-mask* {ip address | interface} [administrative distance] [**name** *name*]

詳細手順

	コマンドまたはアクション	目的
ステップ 1	Router# **configure terminal** **例：** Router# configure terminal	端末からグローバル 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	Router(config)# **ip route** *network-number network-mask* {ip-address | interface} [administrative distance] [**name** name] **例：** Router (config)# ip route 0.0.0.0 Dialer 2 track 234	指定されたインターフェイスを介して設定されている管理距離でフローティング スタティック ルートを確立します。 プライマリ インターフェイスがダウンした場合だけバックアップ インターフェイスが使用されるように、バックアップ インターフェイスのルートに設定する管理距離は長くしてください。

NAT および IPsec 設定でのバックアップとしてのセル ワイヤレス モデム

次に、GSM または CDMA のいずれかのネットワークの NAT および IPsec で 3G ワイヤレス モデムを設定する例を示します。

（注） 受信および送信速度は設定できません。実際のスループットは、セル ネットワーク サービスにより異なります。

```
Current configuration : 3433 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
!
!
no aaa new-model
!
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key gsm address 128.107.241.234              *** or cdma ***
!
!
crypto ipsec transform-set gsm ah-sha-hmac esp-3des        *** or cdma ***
!
crypto map gsm1 10 ipsec-isakmp                            *** or cdma1 ***
 set peer 128.107.241.234
 set transform-set gsm                                     *** or cdma ***
 match address 103
!
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool gsmpool                                        *** or cdmapool ***
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"        *** or cdma ***
!
```

```
!
archive
 log config
  hidekeys
!
!
controller DSL 0
 mode atm
 line-term cpe
 line-mode 4-wire standard
 line-rate 4608
!
!
!
!
interface ATM0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 backup interface Cellular0
 ip nat outside
 ip virtual-reassembly
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Cellular0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string gsm                                        *** or cdma ***
 dialer-group 1
 async mode interactive
 no ppp lcp fast-start
 ppp chap hostname chunahayev@wwan.ccs
 ppp chap password 0 B7uhestacr
 ppp ipcp dns request
 crypto map gsm1                                        *** or cdma1 ***
!
interface Vlan1
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
```

```
!
interface Dialer2
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@dsl.com
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto map gsm1                                          *** or cdma1 ***
!
ip local policy route-map track-primary-if
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0 254
no ip http server
no ip http secure-server
!
!
ip nat inside source route-map nat2cell interface Cellular0 overload
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 2 permit 10.4.0.0 0.0.255.255
access-list 3 permit any
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 209.131.36.158
access-list 103 permit ip host 166.136.225.89 128.107.0.0 0.0.255.255
access-list 103 permit ip host 75.40.113.246 128.107.0.0 0.0.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0
!
!
control-plane
!
```

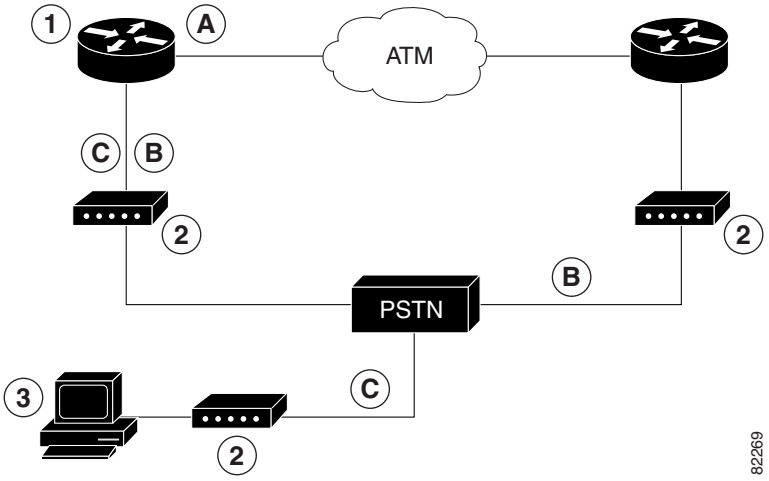
```
!
line con 0
 no modem enable
line aux 0
line 3
 exec-timeout 0 0
 script dialer gsm                                    *** or cdma ***
 login
 modem InOut
 no exec
line vty 0 4
 login
!
scheduler max-task-time 5000

!
webvpn cef
end
```

コンソール ポートまたは AUX ポートを使用したダイヤル バックアップおよびリモート管理の設定

Cisco 880 シリーズ ISR などの加入者宅内機器と Internet Service Provider（ISP; インターネット サービス プロバイダー）が接続されている場合、IP アドレスは動的にルータに割り当てられます。また、中央管理機能を使用して、ルータのピアによって割り当てられることもあります。ダイヤル バックアップ機能を追加すると、プライマリ回線に障害が発生した場合に、フェールオーバー ルートを使用できます。Cisco 880 シリーズ ISR では、AUX ポートを使用してダイヤル バックアップおよびリモート管理を行うことができます。

図 4-1 は、リモート管理アクセスおよびプライマリ WAN 回線のバックアップに使用するネットワーク設定を示しています。

図 4-1　　AUX ポートを使用したダイヤル バックアップおよびリモート管理



1	Cisco 880 シリーズ ルータ	**A**	メイン WAN リンク（インターネット サービス プロバイダーとのプライマリ接続）
2	モデム	**B**	ダイヤル バックアップ（プライマリ回線がダウンした場合に Cisco 880 ルータのフェールオーバー リンクとして機能）
3	PC	**C**	リモート管理（Cisco IOS の設定の変更または更新が可能なダイヤルイン アクセスとして機能）

これらのルータでダイヤル バックアップおよびリモート管理を設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンド	目的

ステップ 1	**ip name-server** *server-address*
	
	例：
	`Router(config)#ip name-server 192.168.28.12`
	`Router(config)#`
		ISP DNS IP アドレスを入力します。
		
		ヒント 複数のサーバ アドレスが存在する場合には、それらのアドレスも追加できます。

ステップ 2	**ip dhcp pool** *name*
	
	例：
	`Router(config)#ip dhcp pool 1`
	`Router(config-dhcp)#`
		ルータ上に DHCP アドレス プールを作成し、DHCP プール コンフィギュレーション モードを開始します。*name* 引数には、ストリングまたは整数を使用できます。
		
		• DHCP アドレス プールを設定します。DHCP プール コンフィギュレーション モードで使用可能なサンプル コマンドについては、「例」（P.4-13）を参照してください。

ステップ 3	**exit**
	
	例：
	`Router(config-dhcp)#exit`
	`Router(config)#`
		config-dhcp モードを終了し、グローバル コンフィギュレーション モードに切り替えます。

ステップ 4	**chat-script** *script-name expect-send*
	
	例：
	`Router(config)# chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102 T" TIMEOUT 45 CONNECT \c`
	`Router(config)#`
		ダイヤルオンデマンド ルーティング（DDR）で使用するチャット スクリプトを設定し、モデムのダイヤリングおよびリモート システムへのログインを行うコマンドを使用します。定義されたスクリプトは、PSTN に接続されているモデム経由でコールする場合に使用されます。

ステップ 5	**interface** *type number*
	
	例：
	`Router(config)# interface Async 1`
	`Router(config-if)#`
		非同期インターフェイスのコンフィギュレーション モードを作成および開始します。
		
		非同期インターフェイスを設定します。非同期インターフェイス コンフィギュレーション モードで使用可能なサンプル コマンドについては、「例」（P.4-13）を参照してください。

	コマンド	目的

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

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)# interface Dialer 3`
	`Router(config-if)#`
		ダイヤラ インターフェイスのコンフィギュレーション モードを作成および開始します。

ステップ 8	**dialer watch-group** ***group-number***
	
	例：
	`Router(config-if)# dialer watch-group 1`
	`Router(config-if)#`
		ウォッチ リストのグループ番号を指定します。

ステップ 9	**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 10	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**] **例：** `Router(config)# ip nat inside source list 101 interface Dialer 3 overload`	内部のインターフェイスでダイナミック アドレス変換をイネーブルにします。

ステップ 11	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		デフォルト ゲートウェイとしてダイヤラ インターフェイスを示すように、IP ルートを設定します。

ステップ 12	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **例：** `Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255 any`	変換が必要なアドレスを指定する拡張アクセス リストを定義します。

	コマンド	目的

ステップ 13	**dialerwatch-list** ***group-number*** {**ip** *ip-address address-mask* | **delay route-check initial** *seconds*}
	
	例：
	`Router(config)# dialer watch-list 1 ip 22.0.0.2 255.255.255.255`
	`Router(config)#`
		ピアへのルートが存在するかどうかに基づいて、プライマリ リンクのステータスを評価します。アドレス 22.0.0.2 は ISP のピア IP アドレスです。

ステップ 14	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
	
	例：
	`Router(config)# line console 0`
	`Router(config-line)#`
		ライン 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 15	**modem enable**
	
	例：
	`Router(config-line)# modem enable`
	`Router(config-line)#`
		ポートをコンソールから AUX ポート機能に変更します。

ステップ 16	**exit**
	
	例：
	`Router(config-line)# 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 17	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
	
	例：
	`Router(config)# line aux 0`
	`Router(config)#`
		AUX 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 18	**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}
	
	例：
	`Router(config)# flowcontrol hardware`
	`Router(config)#`
		ハードウェア信号フロー制御をイネーブルにします。

例

次の設定例では、ATM インターフェイスの IP アドレスを、PPP および Internet Protocol Control Protocol（IPCP; インターネット プロトコル コントロール プロトコル）アドレス ネゴシエーションおよびコンソール ポートを介したダイヤル バックアップによって指定します。

```
!
ip name-server 192.168.28.12
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool 1
 import all
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
! Need to use your own correct ISP phone number.
modemcap entry MY-USER_MODEM:MSC=&F1S0=1
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102\T"
TIMEOUT 45 CONNECT \c
!
!
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
! Dial backup and remote management physical interface.
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 async default routing
 async dynamic routing
 async mode dedicated
 ppp authentication pap callin
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
 pppoe-client dial-pool-number 1
!
dsl operating-mode auto
!
! Primary WAN link.
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username account password 7 pass
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
```

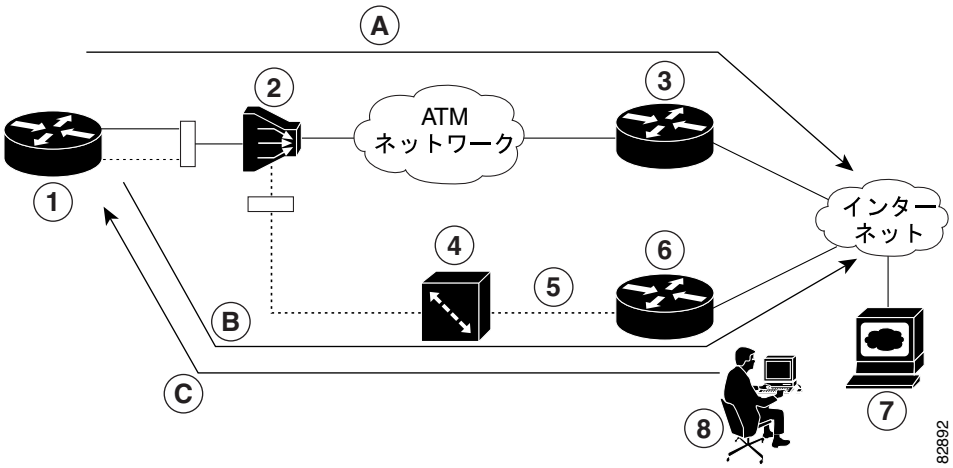
```
! Dialer backup logical interface.
interface Dialer3
 ip address negotiated
 ip nat outside
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool 3
 dialer idle-timeout 60
 dialer string 5555102 modem-script Dialout
 dialer watch-group 1
!
! Remote management PC IP address.
peer default ip address 192.168.2.2
no cdp enable
!
! Need to use your own ISP account and password.
ppp pap sent-username account password 7 pass
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
! IP NAT over Dialer interface using route-map.
ip nat inside source route-map main interface Dialer1 overload
ip nat inside source route-map secondary interface Dialer3 overload
ip classless
!
! When primary link is up again, distance 50 will override 80 if dial backup
! has not timed out. Use multiple routes because peer IP addresses are alternated
! among them when the CPE is connected.
ip route 0.0.0.0 0.0.0.0 64.161.31.254 50
ip route 0.0.0.0 0.0.0.0 66.125.91.254 50
ip route 0.0.0.0 0.0.0.0 64.174.91.254 50
ip route 0.0.0.0 0.0.0.0 63.203.35.136 80
ip route 0.0.0.0 0.0.0.0 63.203.35.137 80
ip route 0.0.0.0 0.0.0.0 63.203.35.138 80
ip route 0.0.0.0 0.0.0.0 63.203.35.139 80
ip route 0.0.0.0 0.0.0.0 63.203.35.140 80
ip route 0.0.0.0 0.0.0.0 63.203.35.141 80
ip route 0.0.0.0 0.0.0.0 Dialer1 150
no ip http server
ip pim bidir-enable
!
! PC IP address behind CPE.
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 103 permit ip 192.168.0.0 0.0.255.255 any
!
! Watch multiple IP addresses because peers are alternated
! among them when the CPE is connected.
dialer watch-list 1 ip 64.161.31.254 255.255.255.255
dialer watch-list 1 ip 64.174.91.254 255.255.255.255
dialer watch-list 1 ip 64.125.91.254 255.255.255.255
!
! Dial backup will kick in if primary link is not available
! 5 minutes after CPE starts up.
dialer watch-list 1 delay route-check initial 300
dialer-list 1 protocol ip permit
!
```

```
! Direct traffic to an interface only if the dialer is assigned an IP address.
route-map main permit 10
 match ip address 101
 match interface Dialer1
!
route-map secondary permit 10
 match ip address 103
 match interface Dialer3
!
! Change console to aux function.
line con 0
 exec-timedout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 ! To enable and communicate with the external modem properly.
 script dialer Dialout
 modem InOut
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
scheduler max-task-time 5000
end
```

ISDN S/T ポートを使用したデータ ライン バックアップおよびリモート管理の設定

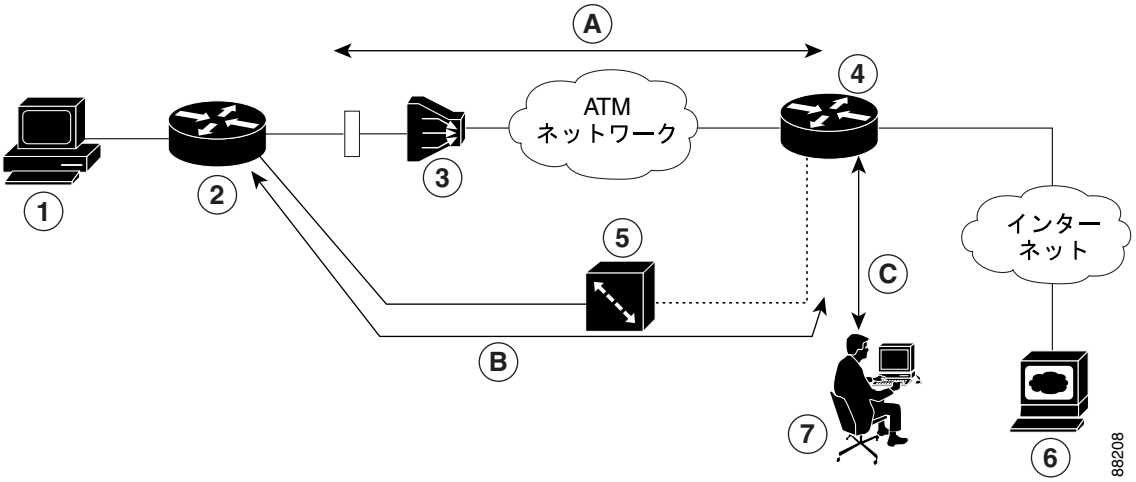
Cisco 880 シリーズ ルータは、リモート管理に ISDN S/T ポートを使用できます。図 4-2 および図 4-3 は、リモート管理アクセスおよびプライマリ WAN 回線のバックアップに使用する 2 つの一般的なネットワーク構成を示しています。図 4-2 の場合、ダイヤル バックアップ リンクは Customer Premises Equipment（CPE; 加入者宅内機器）のスプリッタ、Digital Subscriber Line Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）、および Central Office（CO; セントラル オフィス）のスプリッタを経由して ISDN 交換機に接続されます。図 4-3 では、ダイヤル バックアップ リンクは、ルータから ISDN 交換機に直接接続されます。

図 4-2　CPE スプリッタ、DSLAM、および CO スプリッタを経由したデータ ライン バックアップ



1	Cisco 880 シリーズ ルータ	**A**	プライマリ DSL インターフェイス、FE インターフェイス（Cisco 881 ルータ）
2	DSLAM	**B**	ISDN インターフェイス（ISDN S/T ポート）を介したダイヤル バックアップおよびリモート管理（プライマリ回線がダウンした場合にフェールオーバー リンクとして機能）
3	ATM アグリゲータ		
4	ISDN 交換機		
5	ISDN	**C**	プライマリ DSL リンクがダウンした場合の、ISDN インターフェイスを介した管理者によるリモート管理機能（Cisco IOS 設定の変更または更新が可能なダイヤルイン アクセスとして機能）
6	ISDN ピア ルータ		
7	Web サーバ		
8	管理者	**—**	—

図 4-3　ルータから ISDN 交換機に直接接続されたデータ ライン バックアップ



1	PC	A	プライマリ DSL インターフェイス
2	Cisco 880 シリーズ ISR	B	ISDN インターフェイス（ISDN S/T ポート）を介したダイヤル バックアップおよびリモート管理（プライマリ回線がダウンした場合にフェールオーバー リンクとして機能）
3	DSLAM		
4	アグリゲータ		
5	ISDN 交換機	C	プライマリ DSL リンクがダウンした場合の、ISDN インターフェイスを介した管理者によるリモート管理機能（Cisco IOS 設定の変更または更新が可能なダイヤルイン アクセスとして機能）
6	Web サーバ		
7	管理者		

ルータの ISDN S/T ポートを介したダイヤル バックアップおよびリモート管理を設定するには、次の作業を行います。

- ISDN の設定
- アグリゲータおよび ISDN ピア ルータの設定

ISDN の設定

（注）　バックアップ インターフェイスおよびフローティング スタティック ルート方式を使用してバックアップ ISDN 回線を起動するには、対象トラフィックが存在していなければなりません。ダイヤラ ウォッチを使用してバックアップ ISDN 回線を起動する場合は、対象トラフィックが存在しなくても構いません。

ルータの ISDN インターフェイスをバックアップ インターフェイスとして設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンド	目的

ステップ 1	**isdn switch-type** ***switch-type***
	
	 例：
	 `Router(config)# isdn switch-type basic-net3`
	 `Router(config)#`
		ISDN スイッチ タイプを指定します。
		
		 この例では、オーストラリア、欧州、および英国で使用されているスイッチ タイプを指定します。サポートされている他のスイッチ タイプの詳細については、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

ステップ 2	**interface** ***type number***
	
	 例：
	 `Router(config)# interface bri 0`
	 `Router(config-if)#`
		ISDN Basic Rate Interface（BRI; 基本速度インターフェイス）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 3	**encapsulation** *encapsulation-type*
	
	 例：
	 `Router(config-if)#encapsulation ppp`
	 `Router(config-if)#`
		BRI0 インターフェイスの暗号化タイプを設定します。

ステップ 4	**dialer pool-member** *number*
	
	 例：
	 `Router(config-if)# dialer pool-member 1`
	 `Router(config-if)#`
		ダイヤラ プール メンバーシップを指定します。

ステップ 5	**isdn switch-type** ***switch-type***
	
	 例：
	 `Router(config-if)# isdn switch-type basic-net3`
	 `Router(config-if)#`
		ISDN スイッチ タイプを指定します。

	コマンド	目的

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、グローバル コンフィギュレーション モードに切り替えます。

ステップ 7	**interface dialer** *dialer-rotary-group-number*
	
	例：
	`Router(config)# interface dialer 0`
	`Router(config-if)#`
		ダイヤラ インターフェイス（0 ～ 255 の番号を指定）を作成し、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 8	**ip address negotiated**
	
	例：
	`Router(config-if)# ip address negotiated`
	`Router(config-if)#`
		PPP/IPCP（インターネット プロトコル コントロール プロトコル）アドレス ネゴシエーションを使用してインターフェイスの IP アドレスを取得するように設定します。IP アドレスはピアから取得されます。

ステップ 9	**encapsulation** *encapsulation-type*
	
	例：
	`Router(config-if)# encapsulation ppp`
	`Router(config-if)#`
		インターフェイスのカプセル化タイプを PPP に設定します。

ステップ 10	**dialer pool** *number*
	
	例：
	`Router(config-if)# dialer pool 1`
	`Router(config-if)#`
		使用するダイヤラ プールを指定します。
		この例の場合、BRI0 のダイヤラ プールメンバーの値が 1 であるため、dialer pool 1 の設定によって、ダイヤラ 0 インターフェイスと BRI0 インターフェイスが関連付けられます。

ステップ 11	**dialer string** *dial-string#*[**:***isdn-subaddress*]
	
	例：
	`Router(config-if)# dialer string 384040`
	`Router(config-if)#`
		ダイヤルする電話番号を指定します。

ステップ 12	**dialer-group** *group-number*
	
	例：
	`Router(config-if)# dialer group 1`
	`Router(config-if)#`
		ダイヤラ インターフェイスをダイヤラ グループ（1 ～ 10）に割り当てます。

	コマンド	目的

ステップ 13	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ダイヤラ 0 のインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに切り替えます。

ステップ 14	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}
	
	例：
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		特定のインターフェイス ダイヤラ グループを介して転送される対象パケットについて、ダイヤラ リストを作成します。
		
		この例の場合、ダイヤラ リスト 1 はダイヤラ グループ 1 に対応します。
		
		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 Dial Technologies Command Reference*』を参照してください。

アグリゲータおよび ISDN ピア ルータの設定

通常、アグリゲータはシスコ ルータの ATM PVC が終端するコンセントレータ ルータです。次の設定例では、アグリゲータは、PPPoE サーバとして設定されます。

ISDN ピア ルータは、ISDN インターフェイスを備え、パブリック ISDN ネットワークを介して通信し、シスコ ルータの ISDN インターフェイスに到達することができる任意のルータです。ISDN ピア ルータを使用すると、ATM ネットワークのダウンタイム時に、シスコ ルータからインターネットにアクセスすることができます。

```
! This portion of the example configures the aggregator.
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
 protocol pppoe
 virtual-template 1
!
interface Ethernet3
 description “4700ref-1”
 ip address 40.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Ethernet4
 ip address 30.1.1.1 255.255.255.0
 media-type 10BaseT
!
interface Virtual-Template1
 ip address 22.0.0.2 255.255.255.0
 ip mtu 1492
 peer default ip address pool adsl
!
interface ATM0
 no ip address
 pvc 1/40
 encapsulation aal5snap
 protocol pppoe
```

```
!
no atm limi-keepalive
!
ip local pool adsl 22.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 22.0.0.1 50
ip route 0.0.0.0 0.0.0.0 30.1.1.2.80

! This portion of the example configures the ISDN peer.
isdn switch-type basic-net3
!
interface Ethernet0
 ip address 30.1.1.2 255.0.0.0
!
interface BRI0
 description “to 836-dialbackup”
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type basic-net3
!
interface Dialer0
 ip address 192.168.2.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer string 384020
 dialer-group 1
 peer default ip address pool isdn
!
ip local pool isdn 192.168.2.1
ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.2.1
ip route 40.0.0.0 255.0.0.0 30.1.1.1
!
dialer-list 1 protocol ip permit
!
```

CHAPTER 5

セキュリティ機能の設定

この章では、Cisco 860 および Cisco 880 シリーズ Integrated Services Routers（ISR; サービス統合型ルータ）で設定可能な特定のセキュリティ機能を実装するシスコの主要なフレームワークである Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）の概要について説明します。

この章で説明する内容は、次のとおりです。

AAA

AAA のネットワーク セキュリティ サービスは、ルータ上でアクセス制御を設定するための主要なフレームワークを提供します。認証は、ユーザを識別する手段を提供します。これには、ログインおよびパスワード ダイアログ、チャレンジ/応答、メッセージ サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などがあります。許可は、リモート アクセス制御の手段を提供します。これには、一時的な許可またはサービスごとの許可、ユーザ単位のアカウント リストおよびプロファイル、ユーザ グループのサポート、および IP、Internetwork Packet Exchange（IPX）、AppleTalk Remote Access（ARA）、Telnet のサポートなどがあります。アカウンティングは、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数などの課金、監査、および報告に使用するセキュリティ サーバ情報の収集および送付を行う手段を提供します。

AAA は RADIUS、TACACS+、または Kerberos などのプロトコルを使用してセキュリティ機能の管理を行います。ルータがネットワーク アクセス サーバとして機能している場合、AAA はネットワーク アクセス サーバと RADIUS、TACACS+、または Kerberos セキュリティ サーバ間で通信を確立する手段となります。

AAA サービスの設定およびサポートされているセキュリティ プロトコルの詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』で次の各セクションを参照してください。

- 「Configuring Authentication」
- 「Configuring Authorization」
- 「Configuring Accounting」
- 「Configuring RADIUS」
- 「Configuring TACACS+」
- 「Configuring Kerberos」

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃の対象になる可能性のある一般的な IP サービスを無効にして、攻撃時のネットワークの防御に役立つ IP サービスと機能を有効します。これらの IP サービスは、コマンドを 1 回使用するだけで一度に無効および有効に設定されるため、ルータのセキュリティ設定が大幅に簡素化されます。AutoSecure 機能の詳細については、http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123_1/ftatosec.htm の *AutoSecure* 機能のマニュアルを参照してください。

アクセス リストの設定

アクセス リスト ACL は、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上でネットワーク トラフィックの許可または拒否を行います。アクセス リストは、標準アクセス リストまたは拡張アクセス リストとして設定します。標準アクセス リストは、指定された送信元からのパケットの通過を許可または拒否します。拡張アクセス リストの場合は、宛先と送信元の両方を指定でき、個別のプロトコルの通過を許可または拒否するように指定できます。

アクセス リストの作成の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html で『*Cisco IOS Release 12.4 Security Configuration Guide*』の「Access Control Lists: Overview and Guidelines」のセクションを参照してください。

アクセス リストは、共通のタグを使用して結合された一連のコマンドです。タグは番号または名前のいずれかです。表 5-1 は、アクセス リストの設定に使用するコマンドを示しています。

表 5-1　アクセス リストの設定コマンド

ACL タイプ	設定コマンド
番号指定	
標準	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
拡張	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]
名前指定	
標準	**ip access-list standard** *name* **deny** {*source* | *source-wildcard* | **any**}
拡張	**ip access-list extended** *name* **{permit** | **deny}** *protocol* {*source-addr*[*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

アクセス リストを作成、改良、および管理するには、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Traffic Filtering, Firewalls, and Virus Detection」で次の各セクションを参照してください。

- 「Creating an IP Access List and Applying It to an Interface」
- 「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」
- 「Refining an IP Access List」
- 「Displaying and Clearing IP Access List Data Using ACL Manageability」

アクセス グループ

アクセス グループとは、共通の名前または番号を使用して統合された一連のアクセス リスト設定です。アクセス グループは、インターフェイスの設定時にインターフェイスに対してイネーブルになります。アクセス グループを作成する際には、次の点に注意します。

- アクセス リスト設定の順序は重要です。パケットはシーケンスの最初のアクセス リストと比較されます。一致しない場合（許可または拒否のいずれでもない場合）、パケットは次のアクセス リストと比較され、以降は同様に処理されます。
- パケットを許可または拒否するには、すべてのパラメータがアクセス リストと一致する必要があります。
- すべてのシーケンスの最後には暗黙的な「deny all」が存在しています。

アクセス グループの設定および管理の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html の『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」のセクションを参照してください。

Cisco IOS ファイアウォールの設定

Cisco IOS ファイアウォールを使用すると、パケットを内部で検査し、ネットワーク接続の状態を監視するステートフルなファイアウォールを設定できます。ステートフル ファイアウォールは、スタティックなアクセス リストよりも優れています。アクセス リストは、パケットのストリームに基づくのではなく、個別のパケットに基づいてトラフィックを許可または拒否するだけだからです。また、Cisco IOS ファイアウォールはパケットの検査を行うため、アプリケーション レイヤのデータを調べてトラフィックの許可または拒否を判断できます。スタティックなアクセス リストでは、このような検査を行うことはできません。

Cisco IOS ファイアウォールを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用して、検査するプロトコルを指定します。

ip inspect name *inspection-name protocol* **timeout** *seconds*

検査によって指定されたプロトコルがファイアウォールを通過していることが検出されると、ダイナミックなアクセス リストが作成されて、戻りトラフィックの通過が許可されます。timeout パラメータでは、ルータを通過する戻りトラフィックが存在しない場合にダイナミック アクセス リストをアクティブにしておく時間を指定します。所定のタイムアウト値が経過すると、ダイナミック アクセス リストは削除されるため、後続のパケット（通常、有効なパケット）は許可されません。

複数のステートメントで同じ検査名を使用すると、それらは 1 つのルール セットにまとめられます。コンフィギュレーションの別の場所でこのルールを有効にするには、ファイアウォールのインターフェイスを設定する際に **ip inspect inspection-name in | out** コマンドを使用します。

Cisco IOS ファイアウォールの設定の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html で『*Cisco IOS Release 12.4 Security Configuration Guide*』の「Cisco IOS Firewall Overview」のセクションを参照してください。

Cisco IOS ファイアウォールは、Session Initiated Protocol（SIP）アプリケーションのボイス セキュリティを提供するように設定することもできます。SIP 検査は、プロトコルの適合性およびアプリケーションの保護に加え、基本的な検査機能（SIP パケット検査およびピンホールの開きの検出）が提供されます。詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html で、「Cisco IOS Firewall: SIP Enhancements: ALG and AIC」を参照してください。

Cisco IOS IPS の設定

Cisco 880 シリーズ ISR で利用可能な Cisco IOS Intrusion Prevention System（IPS; 侵入防御システム）テクノロジーは、セキュリティ ポリシーに違反したり、不正なネットワーク動作を示したりするパケットおよびフローに適切に対処することによって、境界部分のファイアウォール保護を強化します。

Cisco IOS IPS は、「シグネチャ」を使用してネットワーク トラフィックの悪用パターンを検出します。Cisco IOS IPS は、インライン型の侵入検知装置として機能し、ルータを通過するパケットおよびセッションを監視して、既知の IPS シグニチャとの比較を行います。Cisco IOS IPS は、不審な動作を検出すると、ネットワーク セキュリティが破られる前に対処してイベントを記録します。また、設定に応じて、次のいずれかを行います。

- アラームの送信
- 疑わしいパケットの破棄
- 接続のリセット
- 攻撃者のソース IP アドレスからのトラフィックを一定の期間拒否する
- シグネチャが確認された接続のトラフィックを一定の期間拒否する

Cisco IOS IPS の設定の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html で『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Configuring Cisco IOS Intrusion Prevention System (IPS)」のセクションを参照してください。

URL フィルタリング

Cisco 860 シリーズおよび Cisco 880 シリーズ ISR には、URL フィルタリングに基づいたカテゴリがあります。ユーザは、許可またはブロックする Web サイトのカテゴリを選択することで、ISR で URL フィルタリングをプロビジョニングします。サード パーティで管理されている外部のサーバを使用して、それぞれのカテゴリの URL を調べます。許可ポリシーおよび拒否ポリシーは ISR で保守管理します。サービスは加入ベースで、各カテゴリの URL はサード パーティのベンダーが保守管理します。

URL フィルタリングの詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_url_filtering.html の「Subscription-based Cisco IOS Content Filtering」を参照してください。

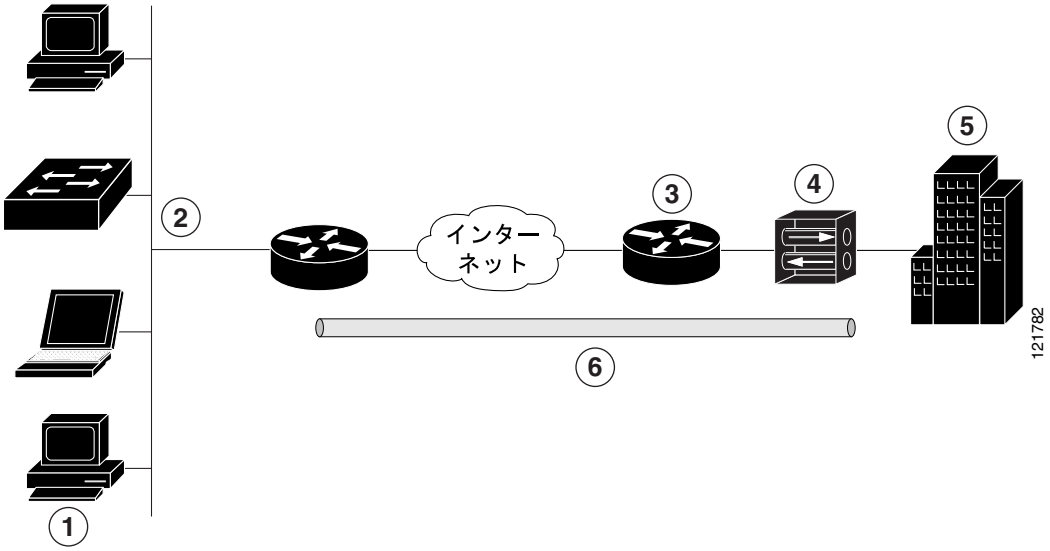
VPN の設定

Virtual Private Network（VPN; 仮想私設網）接続を使用すると、インターネットなどのパブリック ネットワーク上で 2 つのネットワーク間のセキュアな接続を実現できます。Cisco 860 および Cisco 880 シリーズ ISR は、サイト間 VPN およびリモート アクセス VPN の 2 種類の VPN をサポートしています。サイト間 VPN は、ブランチ オフィスとコーポレート オフィスを接続する場合などに使用します。リモート アクセス VPN は、リモート クライアントが企業ネットワークにログインする場合に使用します。リモート アクセス VPN およびサイト間 VPN の両方についてこのセクションで 2 つの例を挙げて説明します。

リモート アクセス VPN

リモート アクセス VPN の設定では、Cisco Easy VPN および IP Security（IPSec）トンネリングを使用して、リモート クライアントと企業のネットワーク間の接続を設定および保護します。図 5-1 は、一般的なネットワーク構成例を示しています。

図 5-1　IPSec トンネルを使用したリモート アクセス VPN



1	リモート ネットワークに接続されたユーザ
2	VPN クライアント：Cisco 880 シリーズ アクセス ルータ
3	ルータ：本社オフィスへのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ（外部インターフェイス アドレスを 210.110.101.1 に設定した Cisco VPN 3000 コンセントレータなど）
5	本社オフィス（ネットワーク アドレス 10.1.1.1 を使用）
6	IPSec トンネル

Cisco Easy VPN クライアントの機能を使用すると、Cisco Unity Client プロトコルを実行して、面倒な設定作業の多くを省略することができます。このプロトコルを使用すると、大半の VPN パラメータ（内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、Windows Internet Naming Services（WINS）サーバ アドレス、およびスプリットトンネリング フラグなど）を VPN サーバ（IPSec サーバとして動作する Cisco VPN 3000 シリーズ コンセントレータなど）で定義できます。

Cisco Easy VPN サーバ対応デバイスは、PC 上で Cisco Easy VPN リモート ソフトウェアを使用しているモバイル ユーザやリモート ユーザが起動した VPN トンネルを終端できます。Cisco Easy VPN サーバ対応装置により、リモート ルータが Easy VPN リモート ノードとして機能することができます。

Cisco Easy VPN クライアントの機能は、クライアント モードまたはネットワーク拡張モードのいずれかのモードで設定できます。クライアント モードはデフォルト設定です。クライアント モードを使用すると、クライアント サイトのデバイスだけが中央サイトにあるリソースにアクセスできます。クライアント サイトにあるリソースは、中央サイトでは利用できません。ネットワーク拡張モードを使用すると、（VPN 3000 シリーズ コンセントレータが配置された）中央サイトのユーザがクライアント サイトのネットワーク リソースにアクセスできます。

IPSec サーバが設定されている場合は、サポート対象の Cisco 880 シリーズ ISR といった IPSec クライアント上で最小限の設定を行うことにより、VPN 接続を作成できます。IPSec クライアントが VPN トンネル接続を開始すると、IPSec サーバは IPSec クライアントに IPSec ポリシーを設定し、対応する VPN トンネル接続を作成します。

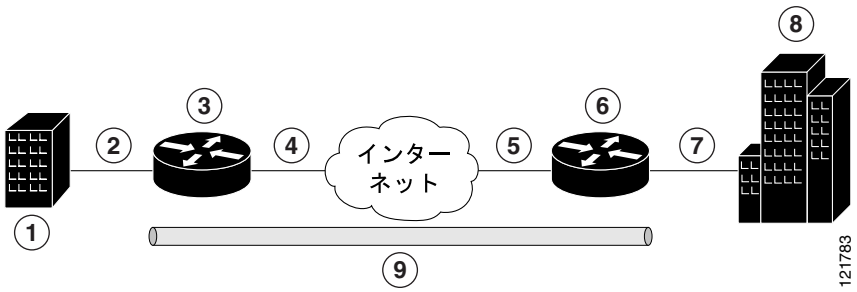
（注） Cisco Easy VPN クライアントの機能は、宛先ピアを 1 つだけ使用する構成をサポートしています。アプリケーションで複数の VPN トンネルを作成する必要がある場合には、クライアントとサーバの両方で IPSec VPN および Network Address Translation/Peer Address Translation（NAT/PAT; ネットワーク アドレス変換 / ポート アドレス変換）パラメータを手動で設定する必要があります。

Cisco 860 および Cisco 880 シリーズ ISR は、Cisco Easy VPN サーバとして動作するように設定することもでき、この機能を使用すると、許可された Cisco Easy VPN クライアントは接続されたネットワークに対してダイナミックな VPN トンネルを確立できます。Cisco Easy VPN サーバの設定の詳細については、http://www.cisco.com/en/US/docs/ios/12_2t/12_2t8/feature/guide/ftunity.html の「*Easy VPN Server*」の機能のマニュアルを参照してください。

サイト間 VPN

サイト間 VPN の設定では、IPSec トンネルと Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）プロトコルを使用して、ブランチ オフィスと企業ネットワーク間の接続を保護します。図 5-2 は、一般的なネットワーク構成例を示しています。

図 5-2　IPSec トンネルおよび GRE によるサイト間 VPN



1	複数の LAN および VLAN を持つブランチ オフィス
2	ファスト イーサネット LAN インターフェイス：アドレス 192.165.0.0/16（NAT の内部インターフェイス）
3	VPN クライアント：Cisco 860 または Cisco 880 シリーズ ISR
4	ファスト イーサネット ATM インターフェイス：アドレス 200.1.1.1（NAT の内部インターフェイス）

5	LAN インターフェイス：インターネットと接続（外部インターフェイス アドレス 210.110.101.1）
6	VPN クライアント：もう 1 つのルータ（企業ネットワークへのアクセスを制御）
7	LAN インターフェイス：企業ネットワークと接続（内部インターフェイス アドレス 10.1.1.1）
8	本社オフィス ネットワーク
9	GRE を使用した IPSec トンネル

IPSec および GRE の設定の詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.html で『*Cisco IOS Release 12.4T Security Configuration Guide*』の「Configuring Security for VPNs with IPSec」の章を参照してください。

設定例

設定例ではいずれも「IPSec トンネル上での VPN の設定」（P.5-7）の手順を使用して、IPSec トンネル上に VPN を設定します。その後、リモート アクセス設定、サイト間設定という順にそれぞれの特定の手順を行います。

この章の設定例は、Cisco 860 および Cisco 880 の ISR のエンドポイント設定にだけ適用されます。いずれの VPN 接続も、両端のエンドポイントが適切に機能するように設定されている必要があります。他のルータ モデルで VPN を設定するために、必要に応じてソフトウェア設定マニュアルを参照してください。

VPN の設定情報は、両端のエンドポイントに設定される必要があります。設定する必要のあるパラメータは、内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、および Network Address Translation（NAT; ネットワーク アドレス変換）などです。

- 「IPSec トンネル上での VPN の設定」（P.5-7）
- 「Cisco Easy VPN リモート設定の作成」（P.5-14）
- 「GRE トンネルでの Site-to-Site の設定」（P.5-17）

IPSec トンネル上での VPN の設定

次の作業を行って IPSec トンネル上で VPN を設定します。

- 「IKE ポリシーの設定」（P.5-8）
- 「グループ ポリシー情報の設定」（P.5-9）
- 「暗号マップに対するモード設定の適用」（P.5-10）
- 「ポリシー検索のイネーブル化」（P.5-10）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.5-11）
- 「IPSec 暗号方式およびパラメータの設定」（P.5-12）
- 「暗号マップの物理インターフェイスへの適用」（P.5-13）
- 「次の作業」（P.5-14）

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット鍵交換）ポリシーを設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp policy** *priority*
	
	例：
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		IKE ネゴシエーションで使用する IKE ポリシーを作成します。プライオリティは 1 ～ 10000 の番号（1 が最高）です。
		このとき、Internet Security Association and Key Management Protocol（ISAKMP）ポリシー コンフィギュレーション モードが開始されます。

ステップ 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	
	例：
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する暗号化アルゴリズムを指定します。
		例では、168 ビットの Data Encryption Standard（DES; データ暗号規格）が指定されています。

ステップ 3	**hash** {**md5** | **sha**}
	
	例：
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		IKE ポリシーで使用するハッシュ アルゴリズムを指定します。
		例では、Message Digest 5（MD5）アルゴリズムが指定されています。デフォルトは Secure Hash standard（SHA-1）です。

ステップ 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	
	例：
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する認証方式を指定します。
		例では、事前共有鍵が指定されています。

ステップ 5	**group** {**1** | **2** | **5**}
	
	例：
	`Router(config-isakmp)# group 2`
	`Router(config-isakmp)#`
		IKE ポリシーで使用する Diffie-Hellman グループを指定します。

ステップ 6	**lifetime** *seconds*
	
	例：
	`Router(config-isakmp)# lifetime 480`
	`Router(config-isakmp)#`
		IKE Security Association（SA; セキュリティ アソシエーション）のライフタイム（60 ～ 86400 秒）を指定します。

ステップ 7	**exit**
	
	例：
	`Router(config-isakmp)# exit`
	`Router(config)#`
		IKE ポリシーのコンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに切り替えます。

グループ ポリシー情報の設定

グループ ポリシーを設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	
	例：
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		リモート クライアントにダウンロードされる属性を格納する IKE ポリシー グループを作成します。
		このとき、Internet Security Association Key and Management Protocol（ISAKMP）グループ ポリシー コンフィギュレーション モードが開始されます。

ステップ 2	**key** *name*
	
	例：
	`Router(config-isakmp-group)# key secret-password`
	`Router(config-isakmp-group)#`
		グループ ポリシーの IKE 事前共有鍵を指定します。

ステップ 3	**dns** *primary-server*
	
	例：
	`Router(config-isakmp-group)# dns 10.50.10.1`
	`Router(config-isakmp-group)#`
		グループのプライマリ Domain Name System（DNS; ドメイン ネーム システム）サーバを指定します。
		wins コマンドを使用して、グループの Windows Internet Naming Service（WINS）サーバを指定することもできます。

ステップ 4	**domain** *name*
	
	例：
	`Router(config-isakmp-group)# domain company.com`
	`Router(config-isakmp-group)#`
		グループのドメイン メンバーシップを指定します。

ステップ 5	**exit**
	
	例：
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		IKE グループ ポリシーのコンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに切り替えます。

ステップ 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]
	
	例：
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		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 Dial Technologies Command Reference*』を参照してください。

暗号マップに対するモード設定の適用

暗号マップにモード設定を適用するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto map** *map-name* **isakmp authorization list** *list-name*
	
	例：
	`Router(config)# crypto map dynmap isakmp authorization list rtr-remote`
	`Router(config)#`
		暗号マップにモード設定を適用し、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバからのグループ ポリシーの鍵検索（IKE 要求）を有効にします。

ステップ 2	**crypto map** *tag* **client configuration address** [**initiate** | **respond**]
	
	例：
	`Router(config)# crypto map dynmap client configuration address respond`
	`Router(config)#`
		リモート クライアントからのモード設定要求に応答するようにルータを設定します。

ポリシー検索のイネーブル化

AAA によるポリシー検索をイネーブルにするには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**aaa new-model**
	
	例：
	`Router(config)# aaa new-model`
	`Router(config)#`
		AAA アクセス制御モデルをイネーブルにします。

ステップ 2	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
	
	例：
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		特定のユーザに関するログイン時の AAA 認証を設定し、使用する方式を指定します。
		
		この例では、ローカル認証データベースが使用されます。ここで RADIUS サーバを使用することもできます。詳しくは、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的

ステップ 3	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
	
	例：
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		すべてのネットワーク関連サービス要求（PPP など）に関する AAA 許可を設定し、許可方式を指定します。
		
		この例では、ローカル許可データベースが使用されます。ここで RADIUS サーバを使用することもできます。詳しくは、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 4	**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}
	
	例：
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		ユーザ名に基づく認証システムを確立します。
		
		この例では、ユーザ名 *Cisco* と暗号化パスワード *Cisco* を指定しています。

IPSec トランスフォームおよびプロトコルの設定

トランスフォーム セットは、セキュリティ プロトコルとアルゴリズムの特定の組み合わせです。IKE ネゴシエーションの実行時に、両ピアはデータ フローを保護するために特定のトランスフォーム セットの使用に同意します。

IKE ネゴシエーションの実行時に、両ピアは、複数のトランスフォーム セットから両ピアに共通するトランスフォームを検索します。このようなトランスフォームを含むトランスフォーム セットが見つかると、そのセットが選択され、両ピアのコンフィギュレーションの一部として、そのセットが保護対象トラフィックに適用されます。

IPSec トランスフォーム セットおよびプロトコルを指定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec profile** *profile-name*
	
	例：
	`Router(config)# crypto ipsec profile pro1`
	`Router(config)#`
		トンネルに暗号化が適用されるように IPSec プロファイルを設定します。

	コマンドまたはアクション	目的

ステップ 2	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	
	例：
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		トランスフォーム セット（IPSec セキュリティ プロトコルおよびアルゴリズムの使用可能な組み合わせ）を定義します。
		
		有効なトランスフォームおよび組み合わせの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
	
	例：
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		IPSec セキュリティ アソシエーション（SA）のネゴシエート時に使用されるグローバル ライフタイムの値を指定します。
		
		詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

IPSec 暗号方式およびパラメータの設定

ダイナミック暗号マップ ポリシーは、ルータがすべての暗号マップ パラメータ（IP アドレスなど）を認識していない場合でも、リモート IPSec ピアからの新しいセキュリティ アソシエーションのネゴシエーション要求を処理します。

IPSec 暗号方式を設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
	
	例：
	`Router(config)# crypto dynamic-map dynmap 1`
	`Router(config-crypto-map)#`
		ダイナミック暗号マップ エントリを作成して、暗号マップ コンフィギュレーション モードを開始します。
		
		このコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 2	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
	
	例：
	`Router(config-crypto-map)# set transform-set vpn1`
	`Router(config-crypto-map)#`
		暗号マップ エントリで使用可能なトランスフォーム セットを指定します。

ステップ 3	**reverse-route**
	
	例：
	`Router(config-crypto-map)# reverse-route`
	`Router(config-crypto-map)#`
		暗号マップ エントリの送信元プロキシ情報を作成します。
		
		詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]
	
	例：
	`Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`
	`Router(config)#`
		暗号マップ プロファイルを作成します。

暗号マップの物理インターフェイスへの適用

暗号マップは、IPSec トラフィックが流れる各インターフェイスに適用する必要があります。物理インターフェイスに暗号マップを適用すると、ルータはすべてのトラフィックをセキュリティ アソシエーション データベースに対して評価するようになります。デフォルト設定の場合、ルータは接続を保護するためにリモート サイト間で送信されるトラフィックを暗号化します。この場合、パブリック インターフェイスを使用して、他のトラフィックの伝送やインターネットとの接続を利用することが可能です。

インターフェイスに暗号マップを適用するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		暗号マップを適用する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 2	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		暗号マップをインターフェイスに適用します。
		
		このコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

次の作業

Cisco Easy VPN リモート設定を作成している場合は、「Cisco Easy VPN リモート設定の作成」（P.5-14）の作業を行います。

IPSec トンネルおよび GRE を使用したサイト間 VPN を作成している場合は、「GRE トンネルでの Site-to-Site の設定」（P.5-17）の作業を行います。

Cisco Easy VPN リモート設定の作成

Cisco Easy VPN クライアントとして機能するルータでは、Cisco Easy VPN リモートの設定を作成して、発信インターフェイスにこの設定を関連付ける必要があります。

リモートの設定を作成するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec client ezvpn** *name*
	
	例：
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Cisco Easy VPN リモートの設定を作成し、Cisco Easy VPN リモート 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	**group** *group-name* **key** *group-key*
	
	例：
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		VPN 接続用の IPSec グループおよび IPSec キーの値を指定します。

ステップ 3	**peer** {*ipaddress* | *hostname*}
	
	例：
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		VPN 接続のピア IP アドレスまたはホスト名を指定します。
		（注） ホスト名を指定できるのは、ルータが DNS サーバを使用してホスト名を解決できる場合だけです。
		（注） このコマンドを使用して両ピアをバックアップとして使用するように設定します。一方のピアがダウンすると、利用可能な 2 番目のピアで Easy VPN トンネルが確立されます。最初のピアが復旧したら、トンネルは最初のピアで再確立されます。

ステップ 4	**mode** {**client** | **network-extension** | **network extension plus**}
	
	例：
	`Router(config-crypto-ezvpn)# mode client`
	`Router(config-crypto-ezvpn)#`
		VPN の動作モードを指定します。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

ステップ 6	**crypto isakmp keepalive** *seconds*
	
	例：
	`Router(config-crypto-ezvpn)# crypto isakmp keepalive 10`
	`Router(config)#`
		不能になったピアの検出メッセージをイネーブルにします。メッセージの時間間隔は、10 ～ 3600 の *seconds* 単位で指定します。

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定を適用するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
		（注） ATM WAN インターフェイスを備えているルータの場合、このコマンドは **interface atm 0** になります。

ステップ 8	**crypto ipsec client ezvpn** *name* [***outside*** | ***inside***]
	
	例：
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定を WAN インターフェイスに関連付けます。これにより、ルータは VPN 接続に必要な NAT または Port Address Translation（PAT; ポート アドレス変換）、およびアクセス リストの設定を自動的に作成します。

ステップ 9	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

設定例

次の設定例は、この章で説明した VPN および IPSec トンネルのコンフィギュレーション ファイルの一部です。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

crypto ipsec client ezvpn ezvpnclient
    connect auto
    group 2 key secret-password
    mode client
    peer 192.168.100.1
!

interface fastethernet 4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

GRE トンネルでの Site-to-Site の設定

GRE トンネルを設定するには、グローバル コンフィギュレーション モードから、次の作業を行います。

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface tunnel 1`
	`Router(config-if)#`
		トンネル インターフェイスを作成し、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 2	**ip address** ***ip-address mask***
	
	例：
	`Router(config-if)# 10.62.1.193 255.255.255.252`
	`Router(config-if)#`
		トンネルにアドレスを割り当てます。

ステップ 3	**tunnel source** *interface-type number*
	
	例：
	`Router(config-if)# tunnel source fastethernet 0`
	`Router(config-if)#`
		GRE トンネルに対するルータの送信元エンドポイントを指定します。

ステップ 4	**tunnel destination** *default-gateway-ip-address*
	
	例：
	`Router(config-if)# tunnel destination 192.168.101.1`
	`Router(config-if)#`
		GRE トンネルに対するルータの宛先エンドポイントを指定します。

ステップ 5	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		トンネルに暗号マップを割り当てます。
		
		（注） サイト間で接続を確立するには、トンネル インターフェイスへのダイナミック ルーティングまたはスタティック ルートを設定する必要があります。詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

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、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的

ステップ 7	**ip access-list** {**standard** | **extended**} *access-list-name*
	
	例：
	`Router(config)# ip access-list extended vpnstatic1`
	`Router(config-acl)#`
		暗号マップで使用される名前付き ACL の ACL コンフィギュレーション モードを開始します。

ステップ 8	**permit** *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`
	`Router(config-acl)#`
		発信インターフェイス上で GRE トラフィックだけを許可するように設定します。

ステップ 9	**exit**
	
	例：
	`Router(config-acl)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

設定例

次の設定例は、前述の各項で説明した GRE トンネルによる VPN のコンフィギュレーション ファイルの一部です。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username cisco password 0 cisco
!
interface tunnel 1
    ip address 10.62.1.193 255.255.255.252

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
!
```

```
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPsec tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Defines encryption and transform set for the IPsec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPsec tunnel.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
! VLAN 1 is the internal home network.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Inspection examines outbound traffic.
 crypto map static-map
 no cdp enable
!
! FE4 is the outside or Internet-exposed interface
interface fastethernet 4
 ip address 210.110.101.21 255.255.255.0
 ! acl 103 permits IPsec traffic from the corp. router as well as
 ! denies Internet-initiated traffic inbound.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Applies the IPsec tunnel to the outside interface.
!
! Utilize NAT overload in order to make best use of the
! single address provided by the ISP.
ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
```

```
!
! acl 102 associated addresses used for NAT.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
! acl 103 defines traffic allowed from the peer for the IPsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! Allow ICMP for debugging but should be disabled because of security implications.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.
! acl 105 matches addresses for the IPsec tunnel to or from the corporate network.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
```

CHAPTER 6

イーサネット スイッチの設定

この章では、Cisco 860 および Cisco 880 シリーズ Integrated Services Router（ISR; サービス統合型ルータ）上に組み込まれているワイヤレス アクセス ポイントに対してサービスを提供する、4 ポート Fast Ethernet（FE; ファスト イーサネット）スイッチと、Gigabit Ethernet（GE; ギガビット イーサネット）スイッチの設定作業の概要について説明します。

FE スイッチは、10/100Base T レイヤ 2 ファスト イーサネット スイッチです。スイッチ上の異なる VLAN の間のトラフィックは、Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を使用し、ルータ プラットフォームを通じてルーティングされます。

GE スイッチは 1000Base T レイヤ 2 ギガビット イーサネット スイッチであり、ルータとそれに組み込まれているワイヤレス アクセス ポイントの間の内部インターフェイスです。

どのスイッチ ポートも、他のシスコ イーサネット スイッチに接続するためのトランキング ポートとして設定できます。

オプションの電源モジュールを Cisco 880 シリーズ ISR に追加することで、IP 電話や外外部アクセス ポイント用に、FE ポートのうちの 2 つにインライン パワーを供給できます。

この章で説明する内容は、次のとおりです。

スイッチ ポートの番号付けと命名

FE スイッチ上のポートには、番号 FE0 ～ FE3 が付与されています。GE スイッチ上のポートには、Wlan-GigabitEthernet0 という名前と番号が付けられています。

FE スイッチの制限事項

FE スイッチには次の制限事項があります。

- FE スイッチのポートを、ルータのファスト イーサネット オンボード ポートに接続してはなりません。
- Cisco 880 シリーズ ISR では、インライン パワーは FE スイッチ ポート FE0 および FE1 でだけサポートされています。Cisco 860 シリーズ ISR では、インライン パワーはサポートされていません。
- VTP プルーニングはサポートされていません。
- FE スイッチは、最大 200 個の安全な MAC アドレスをサポートできます。

イーサネット スイッチについて

イーサネット スイッチを設定するには、次の概念について理解する必要があります。

VLAN および VLAN Trunk Protocol

VLAN および VLAN Trunk Protocol（VTP）については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1047027

インライン パワー

Cisco 860 シリーズ ISR では、インライン パワーはサポートされていません。Cisco 880 シリーズ ISR では、FE スイッチ ポート FE0 および FE1 上で、シスコ IP 電話または外部アクセス ポイントにインライン パワーを供給できます。

FE スイッチ上の検出メカニズムにより、シスコの装置に接続されているかどうかが判別されます。スイッチは、回線に電力が供給されていないことを検知すると、電力を供給します。回線に電力が供給されている場合、スイッチは電力を供給しません。

シスコの装置に電力を供給しないようにスイッチを設定したり、検出メカニズムをディセーブルにすることができます。

FE スイッチは、IEEE 802.3af に準拠する受電装置もサポートしています。

レイヤ 2 イーサネット スイッチング

レイヤ 2 イーサネット スイッチングの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048478

802.1x 認証

802.1x 認証の概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051006

スパニング ツリー プロトコル

スパニング ツリー プロトコルの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1048458

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）は、シスコ製のすべてのルータ、ブリッジ、アクセス サーバ、スイッチで、レイヤ 2（データ リンク レイヤ）上で動作します。CDP を使用すると、ネットワーク管理アプリケーションが、既知の装置のネイバ（特に、下位レイヤの透過的なプロトコルが動作するネイバ）であるシスコ製の装置を検出することができます。CDP を使用すると、ネットワーク管理アプリケーションは、隣接する装置の種類と SNMP エージェント アドレスを学習することができます。この機能により、アプリケーションは、隣接する装置に SNMP クエリーを送信できます。

CDP は、Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）をサポートするすべての LAN および WAN メディアで動作します。CDP が設定されている各装置は、マルチキャスト アドレスに対して定期的にメッセージを送信します。各装置は、SNMP メッセージを受信できるアドレスを 1 つ以上アドバタイズします。アドバタイズには、存続可能時間（ホールドタイム情報）も含まれています。これは、受信側の装置が CDP 情報を破棄せずに保持する時間の長さを示します。

スイッチド ポート アナライザ

スイッチド ポート アナライザの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053663

IGMP スヌーピング

IGMP スヌーピングの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1053727

IGMP バージョン 3

Cisco 880 シリーズ ISR は、IGMP スヌーピングのバージョン 3 をサポートしています。

IGMPv3 は、発信元フィルタリングをサポートしています。これを使用すると、マルチキャスト レシーバー ホストは、マルチキャスト トラフィックの受信元のグループと、どの発信元からのトラフィックを待っているかをルータに知らせることができます。Cisco ISR 上で IGMP スヌーピングとともに IGMPv3 機能を有効にすることで、Basic IGMPv3 Snooping Support（BISS）が提供されます。BISS では、IGMPv3 ホストの存在の下で、マルチキャスト トラフィックの制約されたフラッディングが可能になります。このサポートは、トラフィックを、IGMPv2 スヌーピングが IGMPv2 ホストで行うのとほぼ同じポート セットに制約します。制約されたフラッディングでは、宛先マルチキャスト アドレスだけが考慮されます。

ストーム コントロール

ストーム コントロールの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1051018

フォールバック ブリッジング

フォールバック ブリッジングの概念については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt1636nm.html#wp1054833

イーサネット スイッチの設定方法

イーサネット スイッチの設定作業については、以降のセクションを参照してください。

- 「VLAN の設定」（P.6-5）
- 「レイヤ 2 インターフェイスの設定」（P.6-6）
- 「802.1x 認証の設定」（P.6-6）
- 「スパニング ツリー プロトコルの設定」（P.6-7）
- 「MAC テーブルの操作の設定」（P.6-7）
- 「Cisco Discovery Protocol の設定」（P.6-8）
- 「スイッチド ポート アナライザ（SPAN）の設定」（P.6-8）
- 「インターフェイス上での電源管理の設定」（P.6-8）
- 「IP マルチキャスト レイヤ 3 スイッチングの設定」（P.6-9）
- 「IGMP スヌーピングの設定」（P.6-9）
- 「ポート単位のストーム制御の設定」（P.6-9）
- 「フォールバック ブリッジングの設定」（P.6-10）
- 「独立した音声サブネットとデータ サブネットの設定」（P.6-10）
- 「スイッチの管理」（P.6-10）

VLAN の設定

ここでは、VLAN の設定方法について説明します。Cisco 860 シリーズ ISR は 2 つ の VLAN をサポートしており、Cisco 880 シリーズ ISR は 8 つの VLAN をサポートしています。

FE ポート上の VLAN

VLAN を設定するには、コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface fe** *port*	設定対象のファスト イーサネット ポートを選択します。
ステップ 2	**shutdown**	（任意）インターフェイスをシャットダウンし、設定が完了するまでトラフィックが流れないようにします。
ステップ 3	**switchport**	ファスト イーサネット ポートでレイヤ 2 スイッチングを設定します。 **（注）** ファスト イーサネット ポートをレイヤ 2 ポートとして設定するには、**switchport** コマンドをキーワードなしで実行してから、他のキーワード付きの switchport コマンドを実行する必要があります。このコマンドは、シスコ デフォルト VLAN を作成します。 この設定は、デフォルトのトランキング管理モードを **switchport mode dynamic desirable** に設定し、トランク カプセル化を **negotiate** に設定します。 デフォルトでは、作成されるすべての VLAN がデフォルト トランクに追加されます。
ステップ 4	**switchport access vlan** *vlan_id*	追加の VLAN のインスタンスを作成します。*vlan_id* に指定できる値の範囲は 2 ～ 4094 ですが、値 1002 と 1005 は予約されています。
ステップ 5	**no shutdown**	インターフェイスをアクティブにします。
ステップ 6	**end**	コンフィギュレーションモードを終了します。

詳細については、次の URL の情報を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/layer2.html

GE ポート上の VLAN

GE ポートはルータの組み込みアクセス ポイントだけにサービスを提供する内部インターフェイスであるため、X に 1 以外を指定した **switchport access vlan X** コマンドだけでは設定できません。ただし、トランク モードで設定することはできます。そのためには、コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface** *Wlan-GigabitEthernet0*	設定対象のギガビット イーサネット ポートを選択します。
ステップ 1	**switchport mode trunk**	ポートをトランク モードにします。
ステップ 1	**switchport access vlan** *vlan_id*	（任意）ポートがトランク モードになったら、1 以外の VLAN 番号を割り当てることができます。

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスの設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1047041

この URL には、次の情報が含まれています。

- Configuring a range of interfaces
- Defining a range macro
- Configuring Layer 2 optional interface features

802.1x 認証の設定

802.1x ポートベース認証の設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/ht_8021x.html

この URL には、次の情報が含まれています。

- Understanding the default 802.1x configuration
- Enabling 802.1x Authentication
- Configuring the switch-to-RADIUS-server comunication
- Enabling periodic reauthentication
- Changing the quiet period
- Changing the switch-to-client retransmission time
- Setting the switch-to-client frame-retransmission number
- Enabling multiple hosts
- Resetting the 802.1x configuration to default values
- Displaying 802.1x statistics and status

スパニング ツリー プロトコルの設定

スパニング ツリー プロトコルの設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1047906

この URL には、次の情報が含まれています。

- Enabling spanning tree
- Configuring spanning tree port priority
- Configuring spanning tree port cost
- Configuring the bridge priority of a VLAN
- Configuring the Hello Time
- Configuring the forward-delay time for a VLAN
- Configuring the maximum aging time for a VLAN
- Disabling spanning tree

MAC テーブルの操作の設定

MAC テーブルの操作の設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048223

この URL には、次の情報が含まれています。

- Enabling known MAC address traffic
- Creating a static entry in the MAC address table
- Configuring the aging timer
- Verifying the aging time

ポート セキュリティ

既知の MAC アドレス トラフィックのイネーブル化に関するトピックでは、ポート セキュリティを扱います。ポート セキュリティには、スタティックなポート セキュリティとダイナミックなポート セキュリティがあります。

スタティックなポート セキュリティでは、指定したスイッチ ポートを通じてアクセスすることを許可する装置を、ユーザが指定できます。指定は、許可する装置の MAC アドレスを MAC アドレス テーブルに格納することで、手動で行います。スタティックなポート セキュリティは、MAC アドレス フィルタリングとも呼ばれます。

ダイナミックなポート セキュリティもこれに似ています。ただし、装置の MAC アドレスを指定する代わりに、ポート上で許可する装置の最大数を指定します。指定した最大数が手動で指定した MAC アドレスの数よりも大きい場合、スイッチは、指定された最大値になるまで、MAC アドレスを自動的に学習します。指定した最大数がスタティックに指定されている MAC アドレスの数よりも小さい場合は、エラー メッセージが生成されます。

スタティックまたはダイナミックなポート セキュリティを指定するには、次のコマンドを使用します。

コマンド	目的
Router(config)# **mac-address-table secure** [*<mac-address>* | **maximum** *maximum addresses*] **fastethernet** *interface-id* [**vlan** *<vlan id>*]	*<mac-address>* を指定すると、スタティックなポート セキュリティがイネーブルになります。キーワード **maximum** を使用すると、ダイナミックなポート セキュリティがイネーブルになります。

Cisco Discovery Protocol の設定

Cisco Discovery Protocol（CDP）の設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048365

この URL には、次の情報が含まれています。

- Enabling CDP
- Enabling CDP on an interface
- Monitoring and maintaining CDP

スイッチド ポート アナライザ（SPAN）の設定

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）セッションの設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048473

この URL には、次の情報が含まれています。

- Configuring the SPAN sources
- Configuring SPAN destinations
- Verifying the SPAN session
- Removing sources or destinations from a SPAN session

インターフェイス上での電源管理の設定

アクセス ポイントまたはシスコ IP 電話向けにインライン パワーを設定する方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048551

IP マルチキャスト レイヤ 3 スイッチングの設定

IP マルチキャスト レイヤ 3 スイッチングの設定方法については、下記の URL を参照してください。この URL には、次の情報が含まれています。

- Enabling IP multicast routing globally
- Enabling IP protocol-independent multicast (PIM) on Layer 3 interfaces
- Verifying IP multicast Layer 3 hardware switching summary
- Verifying the IP multicast routing table

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048610

IGMP スヌーピングの設定

IGMP スヌーピングの設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1048777

この URL には、次の情報が含まれています。

- Enabling or disabling IGMP snooping
- Enabling IGMP immediate-leave processing
- Statically configuring an interface to join a group
- Configuring a multicast router port

IGMP バージョン 3

Cisco IOS リリース 12.4(15)T で IGMPv3 機能をサポートするため、キーワード **groups** および **count** が **show ip igmp snooping** コマンドに追加されました。また、**show ip igmp snooping** コマンドの出力に、IGMP スヌーピング グループに関するグローバル情報が含まれるように変更されました。**show ip igmp snooping** コマンドを **groups** キーワードとともに使用すると、すべての VLAN に対して IGMP スヌーピングによって学習されたマルチキャスト テーブルが表示されます。また、**show ip igmp snooping** コマンドを、**groups** キーワード、**vlan-id** キーワード、*vlan-id* 引数とともに使用すると、特定の VLAN に対して IGMP スヌーピングによって学習されたマルチキャスト テーブルが表示されます。**show ip igmp snooping** コマンドを **groups** キーワードおよび **count** キーワードとともに使用すると、IGMP スヌーピングによって学習されたマルチキャスト グループの数が表示されます。

ポート単位のストーム制御の設定

ポート単位のストーム制御の設定方法については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049009

この URL には、次の情報が含まれています。

- Enabling per-port storm-control
- Disabling per-port storm-control

フォールバック ブリッジングの設定

フォールバック ブリッジングの設定方法については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049176
この URL には、次の情報が含まれています。

- Understanding the default fallback bridging configuration
- Creating a bridge group
- Preventing the forwarding of dynamically learned stations
- Configuring the bridge table aging time
- Filtering frames by a specific MAC address
- Adjusting spanning-tree parameters
- Monitoring and maintaining the network

独立した音声サブネットとデータ サブネットの設定

独立した音声サブネットとデータ サブネットの設定方法については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049866

スイッチの管理

スイッチの管理については、次の URL を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t8/feature/guide/esw_cfg.html#wp1049978
この URL には、次の情報が含まれています。

- Adding Trap Managers
- Configuring IP Information
- Enabling Switch Port Analyzer
- Managing the ARP Table
- Managing the MAC Address Tables
- Removing Dynamic Addresses
- Adding Secure Addresses
- Configuring Static Addresses
- Clearing all MAC Address Tables

CHAPTER 7

音声機能の設定

この章では、Cisco 880 シリーズ Integrated Services Routers（ISR; サービス統合型ルータ）での音声機能の設定について説明します。次の ISR には音声ゲートウェイの機能があります。

- C881SRST および C888SRST : 4 基の FXS ポートと 1 基の音声バックアップ ポート
  - C881SRST ISR には 1 基の FXO 音声バックアップ ポートが装備されています。
  - C888SRST ISR には 1 基の BRI 音声バックアップ ポートが装備されています。

この章では、次の内容について説明します。

ボイス ポート

アナログ音声ポート（Foreign Exchange Station（FXS）ポート）は、パケットベース ネットワークのルータを 2 線式または 4 線式のテレフォニー ネットワークに接続します。2 線式ではアナログ電話または FAX デバイスに、4 線式では PBX にそれぞれ接続します。

デジタル音声ポートは、ISDN Basic Rate Interface（BRI; 基本速度インターフェイス）ポートです。

アナログおよびデジタルの音声ポートの割り当て

アナログおよびデジタルの音声ポートの割り当ては型番によって異なります。表 7-1 に、Cisco 880 シリーズ ISR およびその音声ポートの割り当ての一覧を示します。

表 7-1　Cisco 880 シリーズ ISR の音声ポートの割り当て

型番	デジタル（BRI）ポート番号	アナログ（FXS）ポート番号	バックアップ用音声ポート番号
C881SRST	—	0 ～ 3	4（FXO ポート）
C888SRST	—	0 ～ 3	4（BRI ポート）

音声ポートの設定

アナログおよびデジタルの音声ポートを設定するには、次の資料を参照してください。

- 「*Configuring Analog Voice Ports*」
- 「*Basic ISDN Voice Interface Configuration*」

コール制御プロトコル

Cisco 880 シリーズ ISR 音声ゲートウェイ モデルでは、次のコール制御プロトコルをサポートしています。

- 「Session Initiation Protocol（SIP）」（P.7-2）
- 「Media Gateway Control Protocol（MGCP）」（P.7-3）
- 「H.323」（P.7-3）

Session Initiation Protocol（SIP）

Session Initiation Protocol（SIP）は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）（IETF RFC 2543）が規定した、ピアツーピアのマルチメディア シグナリング プロトコルです。Session Initiation Protocol は、ASCII ベースです。このプロトコルは HTTP と同様、既存の IP プロトコル（DNS や SDP）を再利用してメディアのセットアップとティアダウンを提供します。詳細については、『*Cisco IOS SIP Configuration Guide, Release 4T*』を参照してください。

SIP を使用したルータ設定の詳細は、『*Cisco IOS SIP Configuration Guide, Release 4T*』の「*Basic SIP Configuration*」の章を参照してください。

Cisco 880 シリーズ ISR 音声ゲートウェイでは、Cisco IOS ファイアウォール内で SIP の機能を拡張することで音声セキュリティを提供しています。プロトコルの適合性およびアプリケーション保護の機能に加え、SIP 検査機能（SIP パケット検査およびピンホールの開きの検出）が提供されます。ユーザは、ポリシーをより詳細に制御したり、SIP トラフィックにセキュリティ チェックを適用したりできます。また、不要なメッセージをフィルタリングで除去することもできます。詳細については、http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_sip_alg_aic.html で、「Cisco IOS Firewall: SIP Enhancements: ALG and AIC」を参照してください。

Media Gateway Control Protocol（MGCP）

Media Gateway Control Protocol（MGCP）RFC 2705 は、Voice over IP（VoIP）を含むマルチメディア アプリケーションを作成する集中型のアーキテクチャを定義しています。詳細については、『*Cisco IOS MGCP and Related Protocols Configuration Guide*』を参照してください。

Cisco 880 シリーズ音声ゲートウェイ ISR は、主に、MGCP を使用する Residential Gateway（RGW; レジデンシャル ゲートウェイ）として設定されます。レジデンシャル ゲートウェイの設定情報については、『*Cisco IOS MGCP and Related Protocols Configuration Guide*』の章「*Basic MGCP Configuration*」の「*Configuring an RGW*」のセクションを参照してください。

H.323

国際電気通信連合勧告 H.323 では、Voice over IP（VoIP）を含むマルチメディア アプリケーションの作成用の分散アーキテクチャについて定義しています。H.323 の詳細については、『*Cisco IOS H.323 Configuration Guide, Release 12.4T*』を参照してください。

ルータ設定の詳細については、『*Cisco IOS H.323 Configuration Guide, Release 12.4T*』の「*Configuring H.323 Gateways*」の章を参照してください。

ダイヤル ピアの設定

ダイヤル ピアの設定は、ダイヤル プランの実装と IP ネットワークを通じた音声サービスの提供において非常に重要です。ダイヤル ピアを使用することで、コールの発信元と宛先のエンドポイントを識別し、コール接続の各コール レッグに適用される特性を定義します。ルータの設定情報については、『*Dial Peer Configuration on Voice Gateway Routers*』を参照してください。

その他の音声機能

Cisco 880 シリーズの音声ゲートウェイ ISR では、次の音声機能をサポートしています。

- 「Real-Time Transport Protocol」（P.7-3）
- 「デュアル トーン多重周波数リレー」（P.7-4）
- 「CODEC」（P.7-4）
- 「補助機能付き SCCP 制御のアナログ ポート」（P.7-5）

Real-Time Transport Protocol

Real-Time Transport Protocol（RTP）は、リアルタイムでデータを伝送するアプリケーションにエンドツーエンドのネットワーク転送機能を提供します。

Cisco Real-Time Transport Protocol（cRTP）は RTP プロトコルを使用してシスコ特有のペイロード タイプを転送します。

Secure Real-Time Transport Protocol（SRTP）は、暗号化、認証、再送保護を提供する RTP プロファイルを定義します。

RTP は主に DTMF リレーで使用され、ダイヤル ピア構成で設定されます。RTP ペイロード タイプの設定については、『*Dial Peer Configuration on Voice Gateway Routers*』の「*Dual-Tone Multifrequency Relay*」のセクションを参照してください。

SIP 制御下のプラットフォームでの SRTP 設定については、『*Cisco IOS SIP Configuration Guide, Release 4T*』の「*Configuring SIP Support for SRTP*」の章を参照してください。

MGCP 制御下のプラットフォームでの RTP 設定については、『*Cisco IOS MGCP and Related Protocols Configuration Guide*』の章「*Basic MGCP Configuration*」の「*Configuring an RGW*」のセクションを参照してください。

デュアル トーン多重周波数リレー

Dual Tone Multi Frequency（DTMF; デュアル トーン多重周波数）リレーでは、ローカルの VoIP ゲートウェイが DTMF ディジットを待ち受け、受信したディジットを RTP パケットまたは H.245 パケットのいずれかによって未圧縮でリモートの VoIP ゲートウェイに送信します。受信したリモートの VoIP ゲートウェイはこの DTMF ディジットを再生成します。この方法により、圧縮によるディジットの欠落を防ぐことができます。DTMF リレーの設定については、『*Dial Peer Configuration on Voice Gateway Routers*』の「*Dual-Tone Multifrequency Relay*」のセクションを参照してください。

コール制御プロトコルに特定の DTMF の設定については、次の各トピックを参照してください。

- 「*Configuring SIP DTMF Features*」
- 「*Configuring DTMF Relay*（H.323）」
- 「*Configuring Global MGCP Parameters*」

CODEC

Cisco 880 シリーズ音声ゲートウェイ ルータでは、次の CODEC がサポートされています。

- G.711（a-law および mu-law）
- G.726
- G.729、G.729A、G.729B、G.729AB

CODEC の詳細については、次のマニュアルを参照してください。

- 『*Dial Peer Configuration on Voice Gateway Routers*』の付録「*Dial Peer Configuration Examples*」
- 『*Cisco IOS SIP Configuration Guide, Release 4T*』
- 『*Cisco IOS H.323 Configuration Guide*』
- 「*Configuring Global MGCP Parameters*」

補助機能付き SCCP 制御のアナログ ポート

Cisco 880 シリーズ音声ゲートウェイ ISR では、Cisco Skinny Client Control Protocol（SCCP）をサポートします。このプロトコルは、Cisco Unified Communications Manager または Cisco Unified Communications Manager Express システムで制御されるアナログ音声ポートの補助機能を提供します。次の機能がサポートされます。

- 可聴メッセージ待機指示
- コール転送オプション
- コール パーク / ピックアップ オプション
- コール転送
- コール ウェイティング
- 発信者 ID
- 3 者参加の電話会議
- リダイヤル
- 短縮ダイヤル オプション

サポートされる機能とその設定の詳細については、「*SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*」を参照してください。

FAX サービス

Cisco 880 シリーズの音声ゲートウェイ ISR では、次の FAX サービスをサポートしています。

- 「FAX パススルー」（P.7-5）
- 「Cisco FAS リレー」（P.7-5）
- 「T.37 ストアアンドフォワード FAX」（P.7-6）
- 「T.38 FAX リレー」（P.7-6）

FAX パススルー

FAX パススルーは、IP を介して FAX を送信する最もシンプルな方法ですが、Cisco FAX リレーほどは信頼性が高くありません。詳細については、『*Cisco IOS Fax and Modem Services over IP Application Guide*』の「*Configuring Fax Pass-Through*」の章を参照してください。

Cisco FAS リレー

Cisco FAX リレーは、シスコ独自の FAX 方式であり、デフォルトでオンになります。Cisco FAX リレーは、T.30 変調信号を IP ゲートウェイを通じて H.323 ネットワークまたは SIP ネットワークでリアルタイムにリレーできます。詳細については、『*Cisco IOS Fax and Modem Services over IP Application Guide*』の「*Configuring Cisco Fax Relay*」の章を参照してください。

T.37 ストアアンドフォワード FAX

T.37 ストアアンドフォワード FAX メカニズムでは、FAX メッセージを H.323 ネットワークまたは SIP ネットワークで保管および転送できます。詳細については、『*Cisco IOS Fax and Modem Services over IP Application Guide*』の「*Configuring T.37 Store-and-Forward Fax*」の章を参照してください。

T.38 FAX リレー

T.38 FAX リレーは、FAX 信号のリアルタイムのリレーに対し、ITU 仕様に準拠したメカニズムを提供します。MGCP ネットワークでは、ゲートウェイ制御による T.38 FAX リレーを実行できます。詳細については、『*Cisco IOS Fax and Modem Services over IP Application Guide*』の「*Configuring T.38 Fax Relay*」の章を参照してください。

Unified Survival Remote Site Telephony（Unified SRST）

Unified Survival Remote Site Telephony（Unified SRST）機能を持つ Cisco 880 シリーズ音声ゲートウェイ ISR には、次のものがあります。

- Cisco C881SRST
- Cisco C888SRST

Unified SRST は、ネットワーク障害を自動検出し、ルータの自動設定処理を開始します。Unified SRST は、IP 電話と FXS 電話に冗長性を提供して、電話システムの操作性を確保します。

在宅勤務者のサイトに接続するすべての IP 電話とアナログ電話は、Cisco Unified Communications Manager を使用する本社オフィスのコール制御システムで制御されます。WAN の障害時は、すべての電話が在宅勤務者のルータにより本社に SRST モードで登録され、すべての着信ダイヤルと発信ダイヤルは PSTN（バックアップ Foreign Exchange Office（FXO）または BRI ポート）に経路選択されます。WAN 接続が復旧すると、プライマリ Cisco Unified Communications Manager クラスタへの通信に自動的に戻ります。

Cisco 880 シリーズ SRST 音声ゲートウェイ ISR では、Direct Inward Dialing（DID; ダイヤルイン）がサポートされています。

Unified SRST に関する全般的な説明については、『*Cisco Unified SRST System Administrator Guide*』を参照してください。Cisco Unified SRST については、「*Overview*」の章で説明しています。

- H.323 および MGCP のコール制御プロトコルと SRST との関連付けの方法については、『*Cisco Unified SRST System Administrator Guide*』の「*Overview*」の章で、次の各トピックを参照してください。
  - H.323 の場合：「*Cisco Unified SRST Description*」
  - MGCP の場合：「*MGCP Gateways and SRST*」

- 主な SRST 機能の設定については、『*Cisco Unified SRST System Administrator Guide*』の次の各章に説明があります。
  - 「*Setting Up the Network*」
  - 「*Setting Up Cisco Unified IP Phones*」
  - 「*Setting Up Call Handling*」
  - 「*Configuring Additional Call Features*」
  - 「*Setting Up Secure SRST*」
  - 「*Integrating Voice Mail with Cisco Unified SRST*」

SIP 特有の SRST については、『*Cisco Unified SIP SRST System Administrator Guide*』を参照してください。SIP SRST 機能を設定するには、「*Cisco Unified SIP SRST 4.1*」の章を参照してください。

音声設定の確認

次の手順で音声ポートの設定を確認します。

- 『*Cisco IOS Voice Port Configuration Guide*』の「*Verifying Analog and Digital Voice Port Configurations*」
- 『*Cisco IOS Voice Port Configuration Guide*』の「*Verify BRI Interfaces*」

SRST を確認、監視、および管理する場合は、「*Monitoring and Maintaining Cisco Unified SRST*」を参照してください。

PART 3

ワイヤレス デバイスの設定と管理

CHAPTER 8

ワイヤレス デバイスの基本設定

このモジュールは、次の Integrated Services Routers（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。

- Cisco 860 シリーズ
- Cisco 880 シリーズ
- Cisco 890 シリーズ

（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 ソフトウェアのアップグレード」（P.8-9）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。

ワイヤレス 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。

ルータの Cisco IOS コマンドライン インターフェイス（CLI）から次のコマンドをグローバル コンフィギュレーション モードで入力します。

	コマンド	目的

ステップ 1	**interface wlan-ap0**
	
	例：
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		ルータのコンソール インターフェイスをワイヤレス デバイスに定義します。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 を使用してください。
		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`
		インターフェイスの IP アドレスおよびサブネット マスクを指定します。
		
		（注）　**ip unnumbered vlan1** コマンドを使用すると、IP アドレスをシスコ サービス統合型ルータに割り当てられている IP アドレスと共用できます。

ステップ 3	**no shut** **例：** `router(config-if)# no shut`	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。
ステップ 4	**interface vlan1** **例：** `router(config-if)# interface vlan1`	内部ギガビット イーサネット 0（GE 0）ポートから他のインターフェイスへのデータ通信に、仮想 LAN インターフェイスを使用するように指定します。 Cisco 860 シリーズ、Cisco 880 シリーズ、および Cisco 890 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。

	コマンド	目的
ステップ 5	**ip address** *subnet mask* **例：** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	インターフェイスの IP アドレスおよびサブネット 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で接続を開きます。

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。このコマンドを入力すると、Cisco IOS ソフトウェアの **dot11 radio** レベルに自動的にスキップします。

セッションを閉じる

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. **Control-Shift-6 x**

ルータ

2. 通信を切断します。
3. **Enter** キーを 2 回押します。

ワイヤレス設定

（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。「ワイヤレス コンフィギュレーション セッションの開始」（P.8-2）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 IOS コマンドライン インターフェイス」（P.8-4）：自律ソフトウェア
- 「Cisco Express のセットアップ」（P.8-4）：ユニファイド ソフトウェア

（注）　Autonomous 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 ソフトウェアのアップグレード」（P.8-9）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終了後、Web ブラウザのインターフェイスでデバイスを設定します。手順については次の URL を参照してください。
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express のセットアップ

Unified 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、Bridge-Group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）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 キーを押します。[Enter Network Password] ウィンドウが表示されます。

ステップ 3　ユーザ名を入力します。デフォルトのユーザ名は *Cisco* です。

ステップ 4　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に関する詳細については、次の URL を参照してください。
http://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.8-5）
- 「ワイヤレス セキュリティの設定」（P.8-5）
- 「ワイヤレス サービス品質の設定」（P.8-8）（任意）

無線の設定

Autonomous 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、第 9 章「無線の設定」を参照してください。

ワイヤレス セキュリティの設定

認証の設定

認証のタイプは、アクセス ポイントに設定される Service Set Identifiers（SSID; サービス セット ID）に対応しています。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、公開鍵または共用鍵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、次のシスコの URL で Cisco.com の『*Authentication Types for Wireless Devices*』のマニュアルを参照してください。

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html

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 Cisco.com で『*RADIUS and TACACS+ Servers in a Wireless Environment*』のマニュアルを参照してください。

ローカル オーセンティケータとしてのアクセス ポイントの設定

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。アクセス ポイントは毎秒最大 5 回の認証を行います。

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 のリストも設定可能です。

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 Cisco.com で『*Using the Access Point as a Local Authenticator*』のマニュアル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。ワイアレス デバイスとそのワイヤレス クライアント デバイスは同じ WEP キーを使用してデータの暗号化と復号化を行います。WEP キーはユニキャスト とマルチキャストの両方のメッセージを暗号化します。ユニキャスト メッセージは、ネットワーク上の 1 つのデバイスだけに送信されます。マルチキャスト メッセージは、ネットワーク上の複数のデバイスに送信されます。

暗号スイートは、ワイヤレス LAN 上の無線通信を保護するように設計された暗号化と安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）を有効にするには、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ワイヤレス LAN にとって最適な安全性を提供します。WEP だけを含む暗号スイートは、安全性が最も劣ります。

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 Cisco.com で『*Configuring WEP and Cipher Suites*』のマニュアルを参照してください。

ワイヤレス VLAN の設定

ワイヤレス LAN で VLAN を使用し、SSID を VLAN に割り当てると、「セキュリティ タイプ」（P.8-7）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、定義済みのスイッチ セット内のブロードキャスト 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。このブリッジング ドメインはネットワーク装置のさまざまな部分でサポートされています。たとえば、相互にブリッジング プロトコルを稼動する LAN スイッチは、VLAN ごとに個別のプロトコル グループが 1 つあります。

ワイヤレス 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
Cisco.com で『*Configuring Wireless VLANs*』のマニュアルを参照してください。

（注） ワイヤレス 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
Cisco.com で『*Service Set Identifiers*』のマニュアルを参照してください。

お読みください VLAN を使用しない場合は、2.4-GHz 無線などのインターフェイスに暗号化設定（WEP および暗号）が適用されます。1 つのインターフェイスに複数の暗号化設定を使用できません。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。SSID のセキュリティ設定が他の SSID の設定と競合する場合は、SSID を 1 つまたは複数削除して競合が生じないようにします。

セキュリティ タイプ

表 8-1 に、SSID に割り当てることができる 4 つのセキュリティ タイプを示します。

表 8-1　SSID セキュリティのタイプ

セキュリティ タイプ	説明	イネーブル化されたセキュリティ機能
セキュリティなし	セキュリティが一番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。	なし。
スタティック WEP キー	セキュリティなしよりもセキュリティが高いオプションです。ただし、スタティック WEP キーは攻撃に対して脆弱です。このオプションを設定する場合は、MAC アドレスに基づいてワイヤレス デバイスとのアソシエーションを制限することを検討してください。設定の手順については、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html の Cisco.com で『*Cipher Suites and WEP*』のマニュアルを参照してください。 または ネットワークに RADIUS サーバが配置されていない場合は、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こと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 Cisco.com で『*Using the Access Point as a Local Authenticator*』のマニュアルを参照してください。	必須の WEP。クライアント デバイスは、ワイヤレス デバイス キーに一致する WEP キーなしでは、この SSID を使用して対応付けできません。

表 8-1　SSID セキュリティのタイプ （続き）

セキュリティ タイプ	説明	イネーブル化されたセキュリティ機能
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、鍵管理なしで RADIUS サーバ認証ポート 1645 を使用します。 ネットワークの認証サーバ（サーバ認証ポート 1645）に関する IP アドレスおよび共有シークレットの入力が必要となります。802.1X 認証ではダイナミック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。クライアント デバイスがこの SSID を使用して対応付けを行う場合、802.1X 認証を実行する必要があります。 EAP-FAST を使用して無線クライアントが認証されるように設定している場合、EAP のオープン認証も設定する必要があります。オープン認証を EAP で設定しないと、次の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
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 認証と同様、ネットワークの認証サーバ（サーバ認証ポート 1645）に IP アドレスおよび共有シークレットを入力する必要があります。	必須の WPA 認証。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。 EAP-FAST を使用して無線クライアントが認証されるように設定している場合、EAP のオープン認証も設定する必要があります。オープン認証を EAP で設定しないと、次の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`

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

ワイヤレス サービス品質の設定

サービス品質（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 を設定しない場合、デバイスは、パケットのコンテンツやサイズに関係なくすべてのパケットにベストエフォートのサービスを提供します。この場合のパケット送信では、信頼性、遅延限度、スループットのいずれも保証されません。ワイヤレス デバイスのサービス品質（QoS）に設定するには、URL http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html の『*Quality of Service in a Wireless Environment*』のマニュアルを参照してください。

ホット スタンバイ モードのアクセス 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。このスタンバイ アクセス ポイントは、監視するアクセス ポイントの近くに配置され、監視対象のアクセス ポイントとまったく同じ設定が行われます。スタンバイ アクセス ポイントは監視対象のアクセス ポイントに対するクライアントとして対応付けられ、イーサネットと無線ポートを介して 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）要求を送信します。監視対象のアクセス ポイントが応答に失敗した場合は、スタンバイ アクセス ポイントがオンラインになり、監視対象のアクセス ポイントのネットワークでの立場を引き継ぎます。

スタンバイ アクセス ポイントの設定は、監視対象のアクセス ポイントの設定と IP アドレス以外は同一にする必要があります。監視対象のアクセス ポイントがオフラインになり、ネットワークでの立場をスタンバイ アクセス ポイントが引き継いだ場合、両者の設定が同じであるため、クライアント デバイスはスタンバイ アクセス ポイントに容易にスイッチできます。詳細については、Cisco.com の http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html で『*Hot Standby Access Points*』のマニュアルを参照してください。

Cisco Unified ソフトウェアのアップグレード

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.8-9）
- 「アップグレードの実行」（P.8-11）
- 「アクセス ポイントでのソフトウェアのダウングレード」（P.8-12）
- 「アクセス ポイントでのソフトウェアの回復」（P.8-12）

ソフトウェアの前提条件

- アクセス ポイントが組み込まれた Cisco 890 シリーズ ISR は、ルータが IP Base 機能セットと Cisco IOS 12.4(22)YB ソフトウェア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。
- 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 機能セットと Cisco IOS 12.4(20)T ソフトウェア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 アーキテクチャの中で組み込み型アクセス ポイントを使用するには、バージョン 5.1 以降のシスコ Wireless LAN Configuration（WLC）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.8-10）
- 「モード設定がイネーブルになっていることの確認」（P.8-10）

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 ポイントに DHCP サーバ機能を提供します。次に、アクセス ポイントは WLC と通信を行って、DHCP プール設定でオプション 43 をコントローラの IP アドレスにセットアップします。設定例は次のとおりです。

```
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.com で『*Cisco Wireless LAN Configuration Guide*』のマニュアル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

次の手順を行います。

1. ルータから WLC に ping を送信して IP 接続が確立されていることを確認します。
2. **service-module wlan-ap 0 session** コマンドを入力してアクセス ポイントへのセッションを確立します。
3. アクセス ポイントで自律起動イメージを実行していることを確認します。
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、このコマンドの出力例を示します。

```
Autonomous-AP#show boot
BOOT path-list:      flash:ap801-k9w7-mx.124-10b.JA3/ap801-k9w7-mx.124-10b.JA3
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
buffer size:   32768
Mode Button:    on
```

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（*回復イメージ*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# conf terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

（注）　**service-module wlan-ap 0 bootimage unified** コマンドを実行しても正しく処理されない場合は、ソフトウェア ライセンスがまだ有効であるか確認してください。

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:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

ステップ 2　正規の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、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 reload** コマンドを実行します。その後、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。

GUI の設定ページを使用したワイヤレス デバイスのセットアップの詳細については、「Cisco Express のセットアップ」（P.8-4）を参照してください。

アップグレードのトラブルシューティングまたは AP の Autonomous モードへの復帰

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、回復モードに陥ったままになっているようです。次にどのような作業が必要でしょうか。

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。

- 回復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.　私のアクセス ポイントでは、何度試みても起動できません。何が原因でしょうか。
私のアクセス ポイントは回復イメージのままになってしまい、Unified ソフトウェアにアップグレードできません。何が原因でしょうか。

A.　アクセス ポイントでは、起動を試みて失敗したり、回復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。

アクセス ポイントでのソフトウェアのダウングレード

アクセス ポイント BOOT を直前の自律イメージにリセットするには、グローバル コンフィギュレーション モードで **service-module wlan-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。

アクセス ポイントでのソフトウェアの回復

アクセス ポイントにイメージを回復するには、グローバル コンフィギュレーション モードで **service-module wlan-ap0 reset bootloader** コマンドを使用します。このコマンドは手動でイメージを回復するためにアクセス ポイントをブートローダに戻します。

注意　このコマンドを使用するときは注意が必要です。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回復する目的に限り使用してください。

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。

- シスコの自律ソフトウェアのマニュアル—表 8-2
- Cisco Unified ソフトウェアのマニュアル—表 8-3

表 8-2　シスコの自律ソフトウェアのマニュアル

ネットワーク設計	**リンク先**
ワイヤレスの概要	第 2 章「ワイヤレス デバイスの概要」
設定	**リンク先**
無線の設定	第 9 章「無線の設定」
セキュリティ	**リンク先**
『Authentication Types for Wireless Devices』	このマニュアルは、アクセス ポイントに設定する認証タイプについて解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
『RADIUS and TACACS+ Servers in a Wireless Environment』	このマニュアルは、RADIUS および TACACS+ 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[1] 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。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html

表 8-2　シスコの自律ソフトウェアのマニュアル （続き）

ネットワーク設計	リンク先
『Using the Access Point as a Local Authenticator』	このマニュアルは、アクセス ポイントを小規模のワイヤレス LAN に対するスタンドアロンのオーセンティケータとして使用したり、バックアップ認証サービスを提供したりといった、ローカル オーセンティケータとして機能するようにワイヤレス デバイスを使用する方法について解説します。アクセス ポイントはローカル オーセンティケータとして、最大 50 のクライアント デバイスに対し、LEAP 認証、EAP-FAST 認証、および MAC ベースの認証を実施します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html
『Cipher Suites and WEP』	このマニュアルは、WPA および CCKM[2]、WEP、および WEP 機能（AES[3]、MIC[4]、TKIP、およびブロードキャスト鍵のローテーションなど）を使用するために必要な暗号スイートの設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
『Hot Standby Access Points』	このマニュアルは、ワイヤレス デバイスをホットスタンバイ ユニットとして設定する方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html
『Configuring Wireless VLANs』	このマニュアルは、ワイヤード LAN に設定された VLAN とともにアクセス ポイントを使用するための設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html
『Service Set Identifiers』	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 をサポートできます。このマニュアルは、ワイヤレス デバイスで SSID を設定および管理する方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
管理	**リンク先**
アクセス ポイントの管理	第 10 章「ワイヤレス デバイスの管理」
『Quality of Service』	このマニュアルは、ユーザのシスコ ワイヤレス インターフェイスでの QoS の設定方法について解説します。この機能を使用すると、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 を設定しない場合、デバイスは、パケットのコンテンツやサイズに関係なくすべてのパケットにベストエフォートのサービスを提供します。この場合のパケット送信では、信頼性、遅延限度、スループットのいずれも保証されません。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html

表 8-2　シスコの自律ソフトウェアのマニュアル （続き）

ネットワーク設計	リンク先
『Regulatory Domains and Channels』	このマニュアルは、シスコのアクセス製品でサポートされている世界の規制区域内の無線チャネルを一覧表示します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
『System Message Logging』	このマニュアルは、ワイヤレス デバイスへのシステム メッセージ ロギングの設定方法について解説します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html

1. AAA = Authentication, Authorization, and Accounting
2. CCKM = Cisco Centralized Key Management
3. AES = Advanced Encryption Standard
4. MIC = Message Integrity Check

表 8-3　Cisco Unified ソフトウェアのマニュアル

ネットワーク設計	リンク先
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_white_paper0900aecd804f19e3_ps6305_Products_White_Paper.html
『LWAPP[1] Wireless LAN Controllers』	http://www.cisco.com/en/US/products/ps6366/index.html
『LWAPP Wireless LAN Access Points』	http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6306/prod_white_paper0900aecd802c18ee_ps6366_Products_White_Paper.html
『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC』	http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr2410b.html
『Cisco Aironet 1240AG Access Point Support Documentation』	http://www.cisco.com/en/US/docs/wireless/access_point/1240/quick/guide/ap1240qs.html
『Cisco 4400 Series Wireless LAN Controllers Support Documentation』	http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html

1. LWAPP = Lightweight Access Point Protocol

CHAPTER 9

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ディセーブルです。

（注）　無線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 ID）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 モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 ssid** *ssid*	SSID を入力します。SSID は、最大 32 文字の英数字です。SSID 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。2.4 GHz 無線および 802.11g/n 2.4 GHz 無線は、無線 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）入力内容をコンフィギュレーション ファイルに保存します。

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

無線ネットワークの役割の設定

ワイヤレス ネットワークでの無線の役割は、次のとおりです。

- 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対するフォールバック）
- 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 クライアントを持つ非ルート ブリッジ

ルート アクセス ポイントにはフォールバック ロールを設定することもできます。イーサネット ポートがディセーブルになるか、ワイヤード LAN から切断された場合、ワイヤレス デバイス は、自動的にフォールバック ロールを受け持ちます。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 デバイスとの関連付けを解除します。

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 モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11g/n 2.4 GHz 無線は、無線 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 デバイスの役割を設定します。 • ワイヤレス クライアントを持つ非ルート ブリッジ、ワイヤレス クライアントを持たない非ルート ブリッジ、ルート アクセス ポイント、ルート ブリッジ、またはワークグループ ブリッジのいずれかの役割を設定します。 （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。 • イーサネット ポートは、無線のうちいずれでもリピータとして設定されると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、最大 25 個のクライアントを含めることができます。これ以外のワイヤレス クライアントをルート ブリッジまたはルート アクセス ポイントに関連付けないことを前提としています。
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）入力内容をコンフィギュレーション ファイルに保存します。

（注）　無線ネットワークでデバイスの役割をブリッジ/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的な状態およびソフトウェアの状態は起動の状態（動作可能）になります。それ以外の場合は、デバイスの物理的な状態だけが起動になります。反対側のデバイスが設定され動作可能になると、ソフトウェアの状態が起動になります。

無線トラッキング

アクセス ポイントを設定して、いずれかの無線の状態をトラッキングまたは監視できます。トラッキング対象の無線が停止またはディセーブルになっている場合、アクセス ポイントは他の無線をシャットダウンします。トラッキング対象の無線が開始された場合、アクセス ポイントは他の無線をイネーブルにします。

- 無線 0 をトラッキングするには、次のコマンドを入力します。

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

ファスト イーサネットのトラッキング

イーサネット ポートがディセーブルになるか、ワイヤード LAN から切断された場合に、フォールバックするアクセス ポイントを設定できます。「無線ネットワークの役割の設定」（P.9-2）で説明されているように、ファスト イーサネットをトラッキングするアクセス ポイントを設定します。

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

- ファスト イーサネットをトラッキングするアクセス 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-Address のトラッキング

別の無線のクライアント アクセス ポイントを MAC アドレスを使用してトラッキングすることで、ルート アクセス ポイントの役割を持つ無線を開始または停止するように設定できます。クライアントがアクセス ポイントへの関連付けを解除した場合、ルート アクセス ポイントの無線は停止します。クライアントがアクセス ポイントに再び関連付けた場合、ルート アクセス ポイントの無線は開始されます。

MAC アドレスのトラッキングは、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た非ルート ブリッジのアクセス ポイントである場合に最も役立ちます。

たとえば、MAC アドレスが 12:12:12:12:12:12 のクライアントをトラッキングするには、次のコマンドを入力します。

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

無線データ レートの設定

データ レート設定を使用して、ワイヤレス デバイスがデータ送信に使用するデータ レートを選択できます。レートの単位は、メガビット/秒（Mb/s）です。ワイヤレス デバイスは常に、**basic**（ブラウザベースのインターフェイスでは [required] ともいいます）に設定された最大データ レートでの送信を試行します。妨害や干渉がある場合、ワイヤレス デバイスは、データ送信可能な最大レートまでレートを落とします。データ レートはそれぞれ、次の 3 つの状態のいずれかに設定できます。

- basic（GUI では basic レートは [Required] と表示されます）：ユニキャストおよびマルチキャストはどちらも、すべてのパケットをこのレートで送信できます。ワイヤレス デバイスのデータ レートのうち少なくとも 1 つは、basic に設定する必要があります。

- enabled : ワイヤレス デバイスは、このレートでユニキャスト パケットだけを送信し、マルチキャスト パケットは basic に設定されたうちのいずれかのデータ レートで送信します。
- disabled : ワイヤレス デバイスは、このレートでデータを送信しません。

（注）　データ レートの少なくとも 1 つは、**basic** に設定する必要があります。

データ レート設定を使用して、特定のデータ レートで動作するクライアント デバイスに提供するアクセス ポイントを設定できます。たとえば、11 Mb/s のサービス専用に 2.4 GHz 無線を設定し、11 Mb/s レートを **basic** に、その他のデータ レートを **disabled** に設定します。1 Mb/s および 2 Mb/s で動作するクライアント デバイスだけを扱うようにワイヤレス デバイスを設定するには､1 Mb/s および 2 Mb/s を **basic** に、その他のデータ レートは **disabled** に設定します。802.11g クライアント デバイスだけを扱うように 2.4 GHz の 802.11g 無線を設定するには、任意の Orthogonal Frequency Division Multiplexing（OFDM; 直交周波数分割多重方式）データ レート（6、9、12、18、24、36、48、54）を **basic** に設定します。54 Mb/s のサービス専用に 5 GHz 無線を設定するには、54 Mb/s レートを **basic** に、その他のデータ レートを **disabled** に設定します。

データ レートを自動的に設定して範囲またはスループットを最適化するように、ワイヤレス デバイスを設定できます。データ レートの設定で **range** を入力すると、ワイヤレス デバイスは、1 Mb/s レートを **basic** に、その他のレートを **enabled** に設定します。範囲を設定すると、データ レートを下げてバランスを取ることで、アクセス ポイントのカバレッジ領域を拡張できます。したがって、他のクライアントからは接続可能なアクセス ポイントに接続できないクライアントがある場合、そのクライアントは、アクセス ポイントのカバレッジ領域外にいる可能性があります。このような場合、range オプションを使用することで、カバレッジ領域を拡張できるようになり、クライアントがアクセス ポイントに接続できる場合があります。通常は、スループットと範囲の兼ね合いです。信号が劣化すると（可能性としては、アクセス ポイントからの距離による要因で）、リンクを維持するために（データ レートを下げて）レートは再びネゴシエートされます。スループットが高く設定されたリンクは、設定された高いデータ レートを持続できなくなるほど信号が劣化すると単純に落ちるか、または、十分なカバレッジを持つ別のアクセス ポイントが使用可能な場合にはそれにローミングします。両者（スループットと範囲）のバランスは、ワイヤレスの計画、ユーザが使用しているトラフィックの種類、求められるサービス レベル、そして常に上げられる Radio Frequency（RF）環境の品質に対して、使用可能なリソースに基づいて行うべき設計上の判断です。データ レートの設定で **throughput** を入力すると、ワイヤレス デバイスは、4 つすべてのデータ レートを **basic** に設定します。

（注）　ワイヤレス ネットワークに 802.11b クライアントと 802.11g クライアントが混在する環境がある場合は、データ レート 1、2、5.5、および 11 Mb/s が **required**（**basic**）に設定されていて、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確認します。802.11b アダプタは、接続しているアクセス ポイントで 11 Mb/s を上回るデータ レートが **required** に設定されている場合、54 Mb/s データ レートを認識せず動作しません。

無線のデータ レートを設定するには、特権 EXEC モードを開始して次の手順に従ってください。

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

	コマンド	目的
ステップ 3	**speed** 802.11b、2.4 GHz 無線： {[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] | **range** | **throughput**} 802.11g、2.4 GHz 無線： {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** [**ofdm**] | **default**} 802.11a 5 GHz 無線： {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **ofdm-throughput** | **default**} 802.11n 2.4 GHz 無線： {[**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、2.4 GHz 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、2.4 GHz 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、5 GHz 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、2.4-GHz 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、2.4 GHz 無線でこれらのデータ レートが **basic** に設定されます。 **（注）** 選択した basic レートをクライアントがサポートする必要がある場合、そのクライアントはワイヤレス デバイスに関連付けられません。802.11g 無線で basic データ レートに 12 Mb/s 以上を選択した場合、802.11b クライアント デバイスは、ワイヤレス デバイスの 802.11g 無線に関連付けられません。 **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。これを設定すると、802.11b の保護機構はディセーブルになり、802.11g クライアントに対して最大スループットが提供されます。ただし、これにより、802.11b クライアントがアクセス ポイントに関連付けられなくなります。

	コマンド	目的
	speed（続き）	• （任意）データ レートを工場出荷時の設定に戻すには、**default** を入力します（802.11b 無線ではサポートされません）。 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。これらのレートを設定すると、802.11b と 802.11g の両方のクライアント デバイスがワイヤレス デバイスの 802.11g 無線に関連付けられます。 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 無線でも Modulation Coding Scheme（MCS）インデックスの範囲は、0 ～ 15 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

設定から 1 つ以上のデータ レートを削除するには、**speed** コマンドの **no** 形式を使用します。次に、設定からデータ レート **basic-2.0** および **basic-5.5** を削除する例を示します。

```
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）は、変調命令（Binary Phase Shift Keying [BPSK; 2 位相偏移変調]、Quaternary Phase Shift Keying [QPSK; 4 位相偏移変調]、16-Quadrature Amplitude Modulation [16-QAM; 16 直交振幅変調]、64-QAM）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）で構成される PHY パラメータの仕様です。MCS は、ワイヤレス デバイスの 802.11n 無線で使用され、次の 32 個の対称設定（空間ストリームごとに 8 個の設定）を定義します。

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

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

MCS によってスループットが向上する可能性があるため、MCS は重要な設定です。高スループットのデータ レートは、*MCS*、*帯域幅*、および*ガード インターバル*に依存します。802.11a、b、および g の無線では、20 MHz のチャネル幅を使用します。表 1 に、MCS、ガード インターバル、およびチャネル幅に基づき見込まれるデータ レートを示します。

表 1　　MCS 設定、ガード インターバル、チャネル幅を基にしたデータ 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（Mb/s）	40 MHz チャネル幅 データ レート（Mb/s）	20 MHz チャネル幅 データ レート（Mb/s）	40 MHz チャネル幅 データ レート（Mb/s）
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

従来のレートは次のとおりです。

5 GHz : 6、9、12、18、24、36、48、および 54 Mb/s

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

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.
```

無線の伝送パワーの設定

無線の伝送パワーは、無線の種類またはアクセス ポイントにインストールされている無線、およびその無線が動作する規制地域に基づいています。

アクセス ポイントの無線に伝送パワーを設定するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4 GHz 無線および 802.11g/n 2.4 GHz 無線は、無線 0 です。
ステップ 3	**power local** 次のオプションは、2.4 GHz 802.11n 無線に使用できます（dBm 単位）。 {**8** | **9**| **11** | **14** | **15** | **17** | **maximum**}	規制地域において電力レベルが許容範囲内となるように、2.4 GHz 無線に伝送パワーを設定します。
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）入力内容をコンフィギュレーション ファイルに保存します。

電力設定を **maximum** のデフォルト設定に戻すには、**power local** コマンドの **no** 形式を使用します。

関連付けたクライアント デバイスの電力レベルの制限

ワイヤレス デバイスに関連付けるクライアント 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 デバイスに関連付けると、ワイヤレス デバイスは、最大電力レベルの設定をクライアントに送信します。

（注）　Cisco AVVID のマニュアルでは、Dynamic Power Control（DPC）の用語を用いて、関連付けたクライアント デバイスの電力レベルを制限することを指します。

ワイヤレス デバイスに関連付けるすべてのクライアント デバイスで最大許容電力の設定を指定するには、特権 EXEC モードを開始して次の手順に従います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface 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 無線および 802.11g/n 2.4 GHz 無線は、無線 0 です。

	コマンド	目的
ステップ 3	**power client** 次のオプションは、802.11n 2.4 GHz クライアントで使用できます（dBm 単位）： {**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 デバイスに最大許容電力レベルを設定します。 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がアクセス 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が最大許容電力に設定されます。 **（注）** 規制地域により設定できる内容は、ここで示した設定とは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）入力内容をコンフィギュレーション ファイルに保存します。

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） 関連付けたクライアント デバイスの電力レベルを制限するには、Aironet 拡張機能をイネーブルにする必要があります。Aironet 拡張機能はデフォルトでイネーブルです。

無線チャネルの設定

ワイヤレス デバイスの無線のデフォルト チャネル設定は、least-congested です。ワイヤレス デバイスは、起動時に最も混雑していないチャネルをスキャンして選択します。ただし、サイト調査後も可能な限り一貫性のあるパフォーマンスを得るために、各アクセス ポイントにスタティック チャネル設定を割り当て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、規制地域において使用可能な周波数に相当します。各地域で使用でき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。

2.4 GHz の各チャネルは 22 MHz の範囲です。チャネル 1、6、および 11 の帯域は重複しないため、干渉を受けず複数のアクセス ポイントを同じ近辺に設定できます。802.11b および 802.11g の 2.4 GHz 無線は、同じチャネルと同じ周波数を使用します。

5 GHz 無線は、5180 ～ 5320 MHz の 8 チャネルで動作し、規制地域によっては、5170 ～ 5850 MHz の最大 27 チャネルで動作します。各チャネルは 20 MHz の範囲で、チャネルの帯域は少しずつ重複しています。最適なパフォーマンスを得るには、互いに近接する無線の場合は隣り合っていないチャネル（たとえば、チャネル 44 と 46 を使用するなど）を使用します。

（注） 同じ近辺に存在するアクセス ポイントが多すぎると、スループットを低下させる無線の輻輳が発生する場合があります。サイト調査を慎重に行って、無線のカバレッジとスループットが最大になるようにアクセス ポイントの最適な配置を決定してください。

802.11n チャネル幅

802.11n 標準では、重複せず連続する 2 つのチャネル（たとえば、2.4 GHz のチャネル 1 と 6）から成る 20 MHz と 40 MHz の両方のチャネル幅を使用できます。

20 MHz チャネルのうち片方のチャネルは、*制御チャネル*と呼ばれます。従来のクライアントおよび 20 MHz の高スループットのクライアントは、制御チャネルを使用します。このチャネルで送信するのはビーコンだけです。もう一方の 20 MHz チャネルは、*拡張チャネル*と呼ばれます。40 MHz のステーションでは、このチャネルと制御チャネルを同時に使用できます。

40 MHz チャネルは、1.1 のようにチャネルと拡張を表現して指定されます。この例では、制御チャネルはチャネル 1 で、その上に拡張チャネルがあります。

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 モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** }	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、無線 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 シリーズの 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、制御チャネルよりも上に拡張チャネルが設定されて、チャネル幅が 40 MHz に設定されます。 • **40-below** を選択すると、制御チャネルよりも下に拡張チャネルが設定されて、チャネル幅が 40 MHz に設定されます。 **（注）** 5 GHz 無線については、Dynamic Frequency Selection（DFS; 動的周波数選択）に関する欧州連合の規制に準拠するため、**channel** コマンドはディセーブルです。詳細については、「ワールド モードのイネーブル化およびディセーブル化」（P.9-12）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）入力内容をコンフィギュレーション ファイルに保存します。

ワールド モードのイネーブル化およびディセーブル化

802.11d のワールド モード、シスコ従来のワールド モード、およびワールド モード ローミングに対応するように、ワイヤレス デバイスを設定できます。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、チャネル キャリア設定情報をビーコンに追加します。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、キャリア設定情報を受信し、各自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。シスコのクライアント デバイスは、ワイヤレス デバイスが 802.11d を使用しているのか、シスコ従来のワールド モードを使用しているのかを検出し、ワイヤレス デバイスで使用されているモードと一致するワールド モードを自動的に使用します。

ワールド モードを常にオンにするように設定することもできます。この設定では、アクセス ポイントは基本的に各国間でローミングし、必要に応じて設定を変更します。

ワールド モードはデフォルトでディセーブルです。

ワールド モードをイネーブルにするには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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は、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 サイトで確認できます。 – 国番号の後に、**indoor**、**outdoor**、または **both** を入力して、ワイヤレス デバイスの配置を指定する必要があります。 • シスコ従来のワールド モードをイネーブルにするには、**legacy** オプションを入力します。 • アクセス ポイントを継続的にワールド モードに設定するには、**world-mode roaming** オプションを入力します。 **（注）** 従来のワールド モードを使用する場合は、Aironet 拡張機能をイネーブルにする必要がありますが、802.11d ワールド モードの場合、Aironet 拡張機能は不要です。Aironet 拡張機能はデフォルトでイネーブルです。
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）入力内容をコンフィギュレーション ファイルに保存します。

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。

短い無線プリアンブルのディセーブル化とイネーブル化

無線プリアンブル（ヘッダーとも呼ばれます）は、ワイヤレス デバイスおよびクライアント デバイスがパケットを送受信する際に必要な情報を含む、パケットの先頭にあるデータの一部です。無線プリアンブルを long または short に設定できます。

- short：短いプリアンブルを設定すると、スループットのパフォーマンスが向上します。
- long：長いプリアンブルを設定すると、ワイヤレス デバイスと Cisco Aironet Wireless LAN アダプタのすべての初期モデルとの互換性が確保されます。これらのクライアント デバイスがワイヤレス デバイスに関連付けない場合は、短いプリアンブルを使用する必要があります。

5 GHz 無線には、短い無線プリアンブルも長い無線プリアンブルも設定できません。

短い無線プリアンブルをディセーブルにするには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 }**	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**	短いプリアンブルをディセーブルにし、長い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）入力内容をコンフィギュレーション ファイルに保存します。

短いプリアンブルはデフォルトでイネーブルです。短いプリアンブルがディセーブルの場合にイネーブルにするには、**preamble-short** コマンドを使用します。

送受信アンテナの設定

ワイヤレス デバイスがデータの送受信に使用するアンテナを選択できます。受信アンテナおよび送信アンテナのどちらにも次の 3 つのオプションがあります。

- gain：結果として得られたアンテナ ゲインをデシベル（dB）単位で設定します。
- diversity：このデフォルト設定では、ワイヤレス デバイスが最適な信号を受信するアンテナを使用します。ワイヤレス デバイスに 2 つの固定（取り外し不可）のアンテナがある場合、送受信両方にこの設定を使用する必要があります。
- right：ワイヤレス デバイスに取り外し可能なアンテナがあり、高ゲイン アンテナをワイヤレス デバイスの右側のコネクタに取り付けている場合、送受信両方にこの設定を使用する必要があります。右側のアンテナとは、ワイヤレス デバイスの背面パネルの向かって右側にあります。
- left：ワイヤレス デバイスに取り外し可能なアンテナがあり、高ゲイン アンテナをワイヤレス デバイスの左側のコネクタに取り付けている場合、送受信両方にこの設定を使用する必要があります。左側のアンテナとは、ワイヤレス デバイスの背面パネルの向かって左側にあります。

ワイヤレス デバイスでデータの送受信に使用するアンテナを選択するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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、無線 0 です。
ステップ 3	**gain** *dB*	デバイスに取り付けられたアンテナの結果として得られる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 などの小数点以下の値も使用できます。 **（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）** アンテナを 2 台使用して最適なパフォーマンスを得るには、受信アンテナの設定をデフォルトの **diversity** の設定のまま使用してください。アンテナが 1 台の場合、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	**antenna transmit** {**diversity** | **left** | **right**}	送信アンテナを diversity、left、または right に設定します。 **（注）** アンテナを 2 台使用して最適なパフォーマンスを得るには、受信アンテナの設定をデフォルトの **diversity** の設定のまま使用してください。アンテナが 1 台の場合、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 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）入力内容をコンフィギュレーション ファイルに保存します。

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たクライアント デバイス間で特定の対話に必要な機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- ロード バランシング：ワイヤレス デバイスは Aironet 拡張機能を使用して、ユーザ数、ビット誤り率、および信号強度などの要因に基づいて、ネットワークへの最適な接続を提供するアクセス ポイントにクライアント デバイスを接続させます。
- Message Integrity Check（MIC; メッセージ完全性チェック）：MIC は、ビットフリップ攻撃という暗号化パケットへの攻撃を防ぐ追加の WEP セキュリティ機能です。MIC は、ワイヤレス デバイスおよび関連付けたすべてのクライアント デバイスに実装されていて、パケットが改ざんされていないことを証明するための数バイトを各パケットに追加します。
- Cisco Key Integrity Protocol（CKIP）：シスコの WEP キー置換技術は、IEEE 802.11i セキュリティ タスク グループによって発表された初期アルゴリズムに基づいています。標準に基づくアルゴリズムである Temporal Key Integrity Protocol（TKIP）では、Aironet 拡張機能をイネーブルにする必要はありません。
- ワールド モード（従来のワールド モードだけ）：従来のワールド 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、キャリア設定情報をワイヤレス デバイスから受信し、各自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。
- 関連付けたクライアント 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 デバイスに関連付けると、ワイヤレス デバイスは、そのクライアントに最大許容電力レベルの設定を送信します。

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、場合によっては、シスコ以外のクライアント デバイスによるワイヤレス デバイスへの関連付け機能が改善されることがあります。

Aironet 拡張機能はデフォルトでイネーブルです。Aironet 拡張機能をディセーブルにするには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0}**	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、無線 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）入力内容をコンフィギュレーション ファイルに保存します。

Aironet 拡張機能がディセーブルの場合に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 パケットを受信した場合、ワイヤレス デバイスは、カプセル化変換方式を使用してそのパケットを 802.3 パケットに変換する必要があります。変換方式には次の 2 種類があります。

- 802.1H：この方式では、シスコのワイヤレス製品に最適なパフォーマンスを提供します。
- RFC 1042：シスコ 以外のワイヤレス機器との相互運用性を確保するには、この設定を使用します。RFC 1042 は、802.1H の相互運用性の利点は提供しませんが、他の製造元のワイヤレス機器で使用されます。

カプセル化変換方式を設定するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0}**	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、無線 0 です。
ステップ 3	**payload-encapsulation {snap | dot1h}**	カプセル化変換方式を 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）入力内容をコンフィギュレーション ファイルに保存します。

Public Secure Packet Forwarding のイネーブル化およびディセーブル化

Public Secure Packet Forwarding（PSPF）を使用して、アクセス ポイントに関連付けたクライアント デバイスが、アクセス ポイントに関連付けた別のクライアント デバイスと不注意にファイルを共有したり、通信したりすることを防ぎます。PSPF では、クライアント デバイスへのインターネット アクセスを提供します。LAN の他の機能は提供しません。この機能は、空港や大学構内などで敷設されている公衆無線ネットワークで役立ちます。

（注）　異なるアクセス ポイントに関連付けたクライアント間での通信を防ぐには、ワイヤレス デバイスが接続されているスイッチに保護ポートを設定する必要があります。保護ポートの設定手順については、「保護ポートの設定」（P.9-17）を参照してください。

ワイヤレス デバイスで Command-line Iinterface（CLI: コマンドライン インターフェイス）を使用して、PSPF をイネーブルおよび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 グループの詳細と実装手順については、次のマニュアルで確認できます。

- 『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』。「Configuring Transparent Bridging」の章を参照するには、次のリンクをクリックします。
  http://www.cisco.com/en/US/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です。PSPF をイネーブルにするには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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、無線 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）入力内容をコンフィギュレーション ファイルに保存します。

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

ワイヤレス LAN 上で異なるアクセス ポイントに関連付けたクライアント デバイス間での通信を防ぐには、ワイヤレス デバイスが接続されたスイッチの保護ポートを設定する必要があります。

スイッチのポートを保護ポートとして定義するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。**wlan-gigabitethernet0** など、設定するスイッチ ポート インターフェイスのタイプと番号を入力します。
ステップ 3	**switchport protected**	保護ポートにするインターフェイスを設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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。

保護ポートおよびポート ブロッキングの詳細については、『*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。このガイドを参照するには、次のリンクをクリックします。

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

ビーコン期間および DTIM の設定

ビーコン期間は、アクセス ポイントのビーコン間の時間（キロマイクロ秒）です。1 キロマイクロ秒は、1,024 マイクロ秒です。データ ビーコン レートは常にビーコン期間の倍数となり、ビーコンが Delivery Traffic Indication Message（DTIM）を含む頻度を決定します。DTIM は、パケットが待っている省電力のクライアント デバイスを示します。

たとえば、ビーコン期間がデフォルト設定の 100 で設定されていて、データ ビーコン レートがデフォルト設定の 2 で設定されている場合、ワイヤレス デバイスは、200 キロマイクロ秒ごとに DTIM を含むビーコンを送信します。

デフォルトのビーコン期間は 100 で、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 モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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、無線 0 です。
ステップ 3	**beacon period** ***value***	ビーコン期間を設定します。値は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。値は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）入力内容をコンフィギュレーション ファイルに保存します。

送信要求（RTS）しきい値およびリトライ回数の設定

Request To Send（RTS; 送信要求）しきい値は、ワイヤレス デバイスがパケットを送信する前に RTS を発行するときのパケット サイズを決定します。RTS しきい値を小さく設定すると、多数のクライアント デバイスがワイヤレス デバイスに関連付けられている領域、またはクライアントが遠く離れていて、このワイヤレス デバイスしか検出されず、互いに検出できない領域では有用な場合があります。設定は 0 ～ 2347 バイトの範囲で入力できます。

最大 RTS リトライ回数は、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 の値を入力します。

すべてのアクセス ポイントおよびブリッジのデフォルトの RTS しきい値は 2347 で、デフォルトの最大 RTS リトライ回数の設定は 32 です。

RTS しきい値および最大 RTS リトライ回数を設定するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線および 802.11g/n 2.4 GHz 無線は、無線 0 です。
ステップ 3	**rts threshold** *value*	RTS しきい値を設定します。RTS しきい値を 0 ～ 2347 の範囲で入力します。
ステップ 4	**rts retries** *value*	最大 RTS リトライ回数を設定します。1 ～ 128 の値を入力します。
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）入力内容をコンフィギュレーション ファイルに保存します。

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 リトライ回数の設定

最大データ リトライ回数の設定は、ワイヤレス デバイスがパケットをドロップ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 リトライ回数を設定するには、特権 EXEC モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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、無線 0 です。
ステップ 3	**packet retries** *value*	最大データ リトライ回数を設定します。1 ～ 128 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）入力内容をコンフィギュレーション ファイルに保存します。

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、パケットを断片化する（ひとかたまりで送信するのではなく複数に分けて送信する）ときのサイズを決定します。通信状態の悪い領域や無線の干渉が非常に多い場所では、低い設定を使用します。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 モードを開始して次の手順に従ってください。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	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 の 2.4 GHz 無線および 5 GHz 無線は、無線 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。2.4 GHz 無線の場合は、256 ～ 2346 バイトの値を入力します。5 GHz 無線の場合は、256 ～ 2346 バイトの値を入力します。
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）入力内容をコンフィギュレーション ファイルに保存します。

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 無線の短いスロット時間のイネーブル化

短いスロット時間をイネーブルにして、802.11g 2.4 GHz 無線のスループットを上げることができます。スロット時間を標準の 20 マイクロ秒から 9 マイクロ秒の短いスロット時間にすると、全体のバックオフが減少するため、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、ステーションが LAN 上でパケットを送信するまで待機するランダムな長さの時間です。

短いスロット時間は、802.11g 無線の多くでサポートされていますが、一部サポートしていないものもあります。短いスロット時間をイネーブルにした場合、ワイヤレス デバイスが短いスロット時間を使用するのは、802.11g 2.4 GHz 無線に関連付けたすべてのクライアントが短いスロット時間をサポートしているときだけです。

短いスロット時間をサポートするのは、802.11g 2.4 GHz 無線だけです。短いスロット時間はデフォルトでディセーブルです。

短いスロット時間をイネーブルにするには、無線インターフェイス モードで **short-slot-time** コマンドを入力します。

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

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

キャリア話中検査の実行

キャリア話中検査を実行して、ワイヤレス チャネルの無線活動をチェックできます。キャリア話中検査の際、ワイヤレス デバイスは、キャリア検査を実施してその検査結果を表示するまでの 4 秒間は、ワイヤレス ネットワーキング デバイスとのすべての関連付けを破棄します。

キャリア話中検査を実行するには、特権 EXEC モードでこのコマンドを入力します。

```
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。

キャリア話中検査の結果を再表示するには、**show dot11 carrier busy** コマンドを使用します。

VoIP パケット処理の設定

Class of Service（CoS; サービス クラス）5（ビデオ）および CoS 6（音声）のユーザ優先順位に対して遅延がより短くなるように 802.11 MAC 動作を向上させることで、アクセス ポイントの無線あたりの VoIP パケット処理の品質を高めることができます。

アクセス ポイントの VoIP パケット処理を設定するには、次の手順に従ってください。

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　サービスのリストが展開されたら、[Stream] をクリックします。

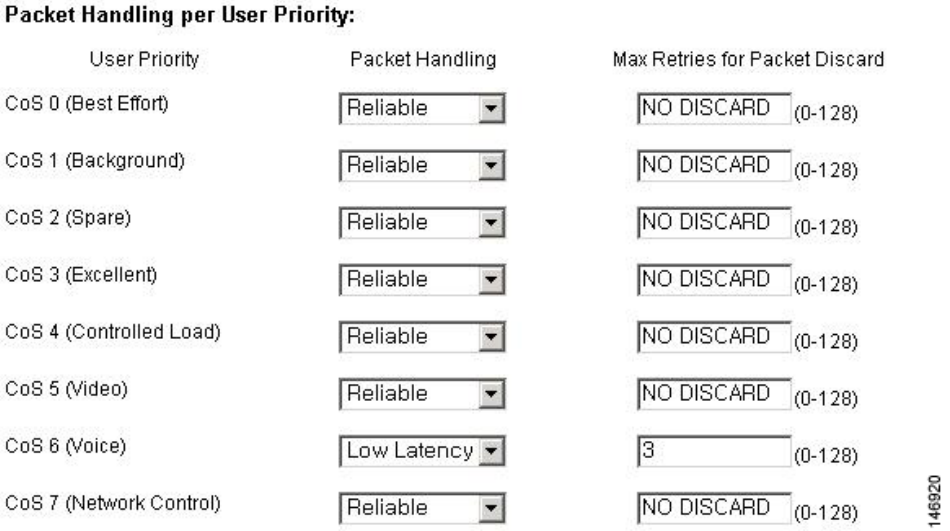
[Stream] ページが表示されます。

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）と CoS 6（音声）のユーザ優先順位の両方に、[Packet Handling] ドロップダウン メニューから [Low Latency] を選択し、パケット破棄までの最大リトライ回数を該当フィールドに入力します。

最大リトライ回数のデフォルト値は、[Low Latency] の設定で 3 です（図 1）。この値は、アクセス ポイントが損失パケットを破棄するまでに検索を試行する回数を示します。

図 1　　パケット処理設定



（注） CoS 4（制御された負荷）のユーザ優先順位およびその最大リトライ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できます。CLI を使用して VoIP パケット処理を設定するための Cisco IOS コマンドの一覧については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

CHAPTER 10

ワイヤレス デバイスの管理

このモジュールでは、次のワイヤレス デバイス管理タスクについて説明します。

ワイヤレス デバイスへのアクセスのセキュリティ強化

アクセス ポイント ハードウェアおよびソフトウェアの管理

ワイヤレス デバイス通信の管理

モード ボタン機能のディセーブル化

[no] boot mode-button コマンドを使用して、ワイヤレス デバイスのモード ボタンをディセーブルにすることができます。

注意　このコマンドを使用すると、パスワード回復がディセーブルになります。このコマンドを入力した後で、アクセス ポイントの特権 EXEC モード パスワードを紛失した場合、Cisco Technical Assistance Center（TAC）に問い合せて、アクセス ポイント Command Line Interface（CLI; コマンドライン インターフェイス）へのアクセスを再び取得する必要があります。

（注）　ワイヤレス デバイスを再起動するには、ルータの Cisco IOS CLI から **service-module wlan-ap reset** コマンドを使用します。このコマンドについては、「ワイヤレス デバイスの再起動」（P.10-19）を参照してください。

モード ボタンは、デフォルトでイネーブルにされています。アクセス ポイントのモード ボタンをディセーブルにするには、特権 EXEC モードから、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**no boot mode-button**	アクセス ポイントのモード ボタンをディセーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。 **（注）**　コンフィギュレーションを保存する必要はありません。

特権 EXEC モードで **show boot** または **show boot mode-button** コマンドを実行して、モード ボタンのステータスをチェックできます。ステータスは、実行コンフィギュレーションには表示されません。次に、**show boot** および **show boot mode-button** コマンドに対する通常の応答を示します。

```
ap# show boot
BOOT path-list: flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap#show boot mode-button
on
ap#
```

（注）　特権 EXEC パスワードを認識している限り、**boot mode-button** コマンドを使用して、モードボタンを通常の動作に戻すことができます。

アクセス ポイントへの不正アクセスの防止

不正ユーザが、ワイヤレス デバイスを再設定したり、設定情報を表示したりできないように防止できます。通常、ネットワーク管理者は、ワイヤレス デバイスにアクセスでき、ローカル ネットワーク内から端末またはワークステーションを介して接続するユーザにアクセスを制限します。

ワイヤレス デバイスへの不正アクセスを防止するには、次のいずれかのセキュリティ機能を設定します。

- ワイヤレス デバイスにローカルで保存される、ユーザ名およびパスワードのペア。これらのペアは、ユーザのワイヤレス デバイスへのアクセスを許可する前に、各ユーザを認証します。また、特定の権限レベル（読み取り専用または読み取り / 書き込み）を各ユーザ名とパスワードのペアに割り当てることができます。詳細については、「ユーザ名およびパスワードのペアの設定」（P.10-8）を参照してください。デフォルトのユーザ名は、*Cisco* です。デフォルトのパスワードは、*Cisco* です。ユーザ名およびパスワードは、大文字と小文字が区別されます。

  （注）　TAB、?、$、+ および [の文字は、パスワードには無効な文字です。

- ユーザ名およびパスワードのペアは、セキュリティ サーバのデータベースに中央で保存されます。詳細については、「RADIUS でのアクセス ポイント アクセスの制御」（P.10-11）を参照してください。

特権 EXEC コマンドへのアクセスの保護

ネットワークの端末アクセス制御を提供する簡単な方法は、パスワードを使用して、権限レベルを割り当てることです。パスワード保護は、ネットワークまたはネットワーク デバイスへのアクセスを制限します。権限レベルは、ユーザがネットワーク デバイスにログインした後で使用できるコマンドを定義します。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference for Release 12.4*』を参照してください。

ここでは、コンフィギュレーション ファイルおよび特権 EXEC コマンドへのアクセスを制御する方法について説明します。また、このコンフィギュレーションについても説明します。

- 「デフォルト パスワードおよび権限レベルの設定」（P.10-4）
- 「スタティック イネーブル パスワードの設定または変更」（P.10-5）
- 「暗号化によるイネーブル パスワードおよびイネーブル シークレット パスワードの保護」（P.10-6）
- 「ユーザ名およびパスワードのペアの設定」（P.10-8）
- 「複数の権限レベルの設定」（P.10-9）

デフォルト パスワードおよび権限レベルの設定

表 1 に、デフォルト パスワードおよび権限レベルのコンフィギュレーションを示します。

表 1　　デフォルトのパスワードおよび権限レベル

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。

（注）　グローバル コンフィギュレーション モードで、**no enable password** コマンドを使用すると、イネーブル パスワードを削除できますが、このコマンドを使用する場合は十分に注意してください。イネーブル パスワードを削除すると、特権 EXEC モードからロックされます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	新しいパスワードを定義するか、特権 EXEC モードにアクセスするための既存のパスワードを変更します。 デフォルトのパスワードは、*Cisco* です。 *password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行スペースは無視されます。パスワードを作成する場合、疑問符の前にキーの組み合わせを指定すると、疑問符（?）文字を含めることができます。たとえば、abc?123 というパスワードを作成する場合、次のようにします。 **1.** **abc** を入力します。 **2.** **Crtl-V** を入力します。 **3.** **?123** を入力します。 イネーブル パスワードを入力するプロンプトが表示された場合、疑問符の前に Ctrl-V を付ける必要はありません。パスワード プロンプトには、**abc?123** とだけ入力できます。 （注）　TAB、?、$、+ および [の文字は、パスワードには無効な文字です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

イネーブル パスワードは、暗号化されず、ワイヤレス デバイスのコンフィギュレーション ファイルに読み込むことができます。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは、暗号化されず、レベル 15（標準特権 EXEC モード アクセス）のアクセスを提供します。

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

暗号化によるイネーブル パスワードおよびイネーブル シークレット パスワードの保護

セキュリティを強化するには、特に、ネットワークを介するパスワード、または TFTP サーバに保存されるパスワードのセキュリティを強化するには、グローバル コンフィギュレーション モードで、**enable password** または **enable secret** コマンドのいずれかを使用できます。これらのコマンドを同じことを実行します。つまり、ユーザが特権 EXEC モード（デフォルト）を開始するときに入力しなければならない暗号化されたパスワード、または指定する任意の権限レベルを確立できます。

改善された暗号化アルゴリズムが使用されるため、**enable secret** コマンドを使用することをお勧めします。

enable secret コマンドを設定する場合、**enable password** コマンドより優先されます。これら 2 つのコマンドが同時に有効になることはありません。

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化を設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password}	新しいパスワードを定義するか、特権 EXEC モードにアクセスするための既存のパスワードを変更します。
	または	または
	enable secret [**level** *level*] {*password* | *encryption-type encrypted*-password}	元に戻すことができない暗号方式を使用して保存される、シークレット パスワードを定義します。 • （任意）*level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。デフォルトのレベルは 15 です（特権 EXEC モード権限）。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。 • （任意）*encryption-type* には、シスコ社製暗号アルゴリズムである、タイプ 5 だけを使用できます。暗号タイプを指定する場合、暗号化されたパスワードを提供する必要があります。暗号化されたパスワードは、別のアクセス ポイント ワイヤレス デバイス コンフィギュレーションからコピーします。 **（注）** 暗号タイプを指定して、クリア テキスト パスワードを入力した場合、特権 EXEC モードを再び開始できません。暗号化されたパスワードを損失した場合、いかなる方法でも回復できません。

	コマンド	目的
ステップ 3	**service password-encryption**	（任意）パスワードが定義されるか、コンフィギュレーションが書き込まれるときに、パスワードを暗号化します。 暗号化により、パスワードは、コンフィギュレーション ファイルで読み取ることができなくなります。
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）入力内容をコンフィギュレーション ファイルに保存します。

イネーブル パスワードとイネーブル シークレット パスワードが両方定義されている場合、ユーザは、イネーブル シークレット パスワードを開始する必要があります。

level キーワードを使用して、特定の権限レベルのパスワードを定義します。レベルを指定して、パスワードを設定したら、このレベルでアクセスする必要があるユーザだけに、設定したパスワードを提供します。グローバル コンフィギュレーション モードで、**privilege level** コマンドを使用して、さまざまなレベルでアクセス可能なコマンドを指定します。詳細については、「複数の権限レベルの設定」（P.10-9）を参照してください。

パスワード暗号化をイネーブルにした場合、これは、ユーザ名パスワード、認証鍵パスワード、特権コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

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

次に、権限レベル 2 の暗号化されたパスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

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

ユーザ名およびパスワードのペアの設定

ワイヤレス デバイスにローカルで保存される、ユーザ名およびパスワードのペアを設定できます。これらのペアは、ラインまたはインターフェイスに割り当てられ、ユーザがワイヤレス デバイスにアクセスできるようになる前に各ユーザを認証します。権限レベルを定義した場合、各ユーザ名およびパスワードのペアに、特定の権限レベル（および関連する権利と権限）を割り当てることもできます。

ログイン ユーザ名およびパスワードを要求する、ユーザ名に基づいた認証システムを確立するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、権限レベル、およびパスワードを入力します。 • *name* には、ユーザ ID を 1 単語で指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセス権を取得した後の権限レベルを指定します。範囲は、0 ～ 15 です。レベル 15 は、特権 EXEC モード アクセスを提供します。レベル 1 は、ユーザ EXEC モード アクセスを提供します。 • *encryption-type* には、暗号化されていないパスワードを使用する場合は 0 を入力します。非表示パスワードを使用する場合は 7 を入力します。 • *password* には、ワイヤレス デバイスへのアクセス権を取得するときにユーザが入力する必要があるパスワードを指定します。パスワードは、1 ～ 25 文字でなければなりません。スペースを含めることができます。また、パスワードは、**username** コマンドで指定される最後のオプションでなければなりません。
ステップ 3	**login local**	ログイン時にローカル パスワード チェックをイネーブルにします。認証は、手順 2 で指定したユーザ名に基づいて行われます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

パスワード チェックをディセーブルにし、パスワードなしで接続を許可するには、グローバル コンフィギュレーション モードで、**no login** コマンドを使用します。

（注） ユーザ名は少なくとも 1 つ設定しなければなりません。また、login local を設定して、ワイヤレス デバイスに Telnet セッションを開かなければなりません。only username にユーザ名を入力しない場合、ワイヤレス デバイスからロックされます。

複数の権限レベルの設定

デフォルトでは、Cisco IOS ソフトウェアは、ユーザ EXEC および特権 EXEC の 2 つのパスワード セキュリティ モードを提供します。各モードのコマンドの階層レベルは 16 まで設定できます。複数のパスワードを設定すると、ユーザのさまざまなセットに指定コマンドへのアクセスを許可できます。

たとえば、多数のユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 セキュリティを割り当て、このレベル 2 セキュリティ パスワードを幅広く配布します。ただし、**configure** コマンドへのアクセスをさらに制限する場合、レベル 3 セキュリティを割り当て、そのパスワードを、より限定したユーザ グループに配布します。

ここでは、次の設定情報について説明します。

- 「コマンドの権限レベルの設定」（P.10-9）
- 「権限レベルへのログインおよび終了」（P.10-10）

コマンドの権限レベルの設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの権限レベルを設定します。 • *mode* には、グローバル コンフィギュレーション モードの場合は **configure**、EXEC モードの場合は **exec**、インターフェイス コンフィギュレーション モードの場合は **interface**、ライン コンフィギュレーション モードの場合は **line** を入力します。 • *level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードにより許可されるアクセスのレベルです。 • *command* には、アクセスを制限するコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルのイネーブル パスワードを指定します。 • *level* の範囲は 0 ～ 15 です。レベル 1 は、通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字のストリングを指定します。このストリングの最初に数値は使用できません。また、大文字と小文字が区別されます。ストリングにはスペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。 **（注）** TAB、?、$、+ および [の文字は、パスワードには無効な文字です。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config** または **show privilege**	入力内容を確認します。 **show running-config** コマンドは、パスワードおよびアクセス レベル コンフィギュレーションを表示します。 **show privilege** コマンドは、権限レベル コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

コマンドを権限レベルに設定すると、構文がそのコマンドのサブセットであるすべてのコマンドも、そのレベルに設定されます。たとえば、**show ip route** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、個別に別のレベルに設定していない限り、自動的に権限レベル 15 に設定されます。

特定のコマンドのデフォルト権限に戻すには、グローバル コンフィギュレーション モードで、**no privilege** *mode* **level** *level command* コマンドを使用します。

次に、**configure** コマンドを権限レベル 14 に設定し、ユーザがレベル 14 コマンドを使用するときに入力しなければならないパスワードとして *SecretPswd14* を定義する例を示します。

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

権限レベルへのログインおよび終了

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

	コマンド	目的
ステップ 1	**enable** *level*	指定された権限レベルにログインします。 *level* の範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定された権限レベルを終了します。 *level* の範囲は 0 ～ 15 です。

RADIUS でのアクセス ポイント アクセスの制御

ここでは、Remote Authentication Dial-In User Service（RADIUS）を使用して、ワイヤレス デバイスへの管理者アクセスを制御する方法について説明します。RADIUS をサポートするようにワイヤレス デバイスを設定する方法の詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章を参照してください。

RADIUS は、詳細なアカウンティング情報、および認証や認可プロセスを介した柔軟な管理制御を提供します。RADIUS は、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）により促進され、AAA コマンドを介してだけイネーブルにできます。

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

ここでは、RADIUS 設定について説明します。

- 「デフォルトの RADIUS 設定」（P.10-11）
- 「RADIUS ログイン認証の設定」（P.10-11）（必須）
- 「AAA サーバ グループの定義」（P.10-13）（任意）
- 「ユーザ権限アクセスおよびネットワーク サービスの RADIUS 許可の設定」（P.10-15）（任意）
- 「RADIUS 設定の表示」（P.10-16）

デフォルトの RADIUS 設定

RADIUS および AAA は、デフォルトでディセーブルにされています。

セキュリティの欠落を避けるため、ネットワーク管理アプリケーションを介して RADIUS を設定できません。イネーブルにされている場合、RADIUS は、コマンドライン インターフェイス（CLI）を介してワイヤレス デバイスにアクセスするユーザを認証できます。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義して、そのリストをさまざまなインターフェイスに適用します。認証方式のリストは、実行される認証のタイプ、およびそれらが実行される順序を定義します。これは、定義される認証方式が実行される前に、特定のインターフェイスに適用しなければなりません。唯一の例外は、デフォルトの認証方式リストです（この名前は *default* です）。デフォルトの認証方式リストは、名前付き認証方式リストが明示的に定義されているインターフェイスを除く、すべてのインターフェイスに自動的に適用されます。

認証方式リストは、ユーザの認証に使用される順序と認証方式を記述します。最初の方式が失敗した場合の認証にバックアップ システムが使用されるように、認証に 1 つ以上のセキュリティ プロトコルを指定できます。ソフトウェアは、リストの最初の方式を使用して、ユーザを認証します。この方式が応答しない場合、ソフトウェアは、方式リストの次の認証方式を選択します。このプロセスは、リストの認証方式との通信に成功するまで、または定義されているすべての方式が失敗するまで、続けられます。このサイクルのいずれかの時点で認証が失敗した場合、つまり、セキュリティサーバまたはローカル ユーザ名データベースが、ユーザ アクセスを拒否することで応答した場合、認証プロセスは停止し、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードから、次の作業を行います。これは必須手順です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • 名前付きリストが **login authentication** コマンドで指定されていないときに使用されるデフォルト リストを作成するには、デフォルト状況で使用される方式リストが後に続く **default** キーワードを使用します。デフォルト方式リストは、すべてのインターフェイスに自動的に適用されます。 • *list-name* には、作成するリストに名前を付ける文字ストリングを指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。認証の追加方式は、直前の方式からエラーが返された場合だけ使用されます。失敗した場合は、使用されません。 次のいずれかの方式を選択します。 • **local**：認証のローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力しなければなりません。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバを設定しなければなりません。詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章の「Identifying the RADIUS Server Host」の項を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始して、認証リストを適用するラインを設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストをラインまたはラインのセットに適用します。 • **default** を指定する場合、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

AAA サーバ グループの定義

ワイヤレス デバイスを設定して、AAA サーバ グループを使用し、認証に既存のサーバ ホストをまとめることができます。設定されているサーバ ホストのサブセットを選択して、特定のサービスでこれらを使用する必要があります。サーバ グループは、グローバル サーバ ホスト リストで使用されます。このリストは、選択されたサーバ ホストの IP アドレスを示します。

サーバ グループには、各エントリの ID（IP アドレスと UDP ポート番号の組み合わせ）が一意な場合、同じサーバの複数のホスト エントリを含めることもできます。これにより、異なるポートを、特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。同じサービス（アカウンティングなど）の同じ RADIUS サーバで 2 つの異なるホスト エントリを設定する場合、2 番目に設定されるホスト エントリは、最初のホスト エントリのフェールオーバー バックアップとして機能します。

server グループ サーバ コンフィギュレーションコマンドを使用して、特定のサーバと定義済みグループ サーバを関連付けます。サーバをその IP アドレスで識別するか、オプションの **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを識別できます。

AAA サーバ グループを定義して、特定の RADIUS サーバをこれに関連付けるには、特権 EXEC モードから、次の作業を行います。

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

	コマンド	目的
ステップ 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、ワイヤレス デバイスが再転送前に RADIUS サーバの応答を待機する時間を指定します。範囲は、1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンド設定を上書きします。**radius-server host** コマンドで timeout が設定されていない場合、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合、またはサーバの応答が遅い場合に RADIUS 要求がサーバに再送信される回数を指定します。範囲は、1 ～ 1000 です。**radius-server host** コマンドで retransmit 値が設定されていない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドが使用されます。 • （任意）**key** *string* には、ワイヤレス デバイス、および RADIUS サーバで実行している RADIUS デーモン間で使用される認証と暗号キーを指定します。 **（注）** このキーは、RADIUS サーバで使用される暗号鍵と一致しなければならないテキスト ストリングです。常に、**radius-server host** コマンドの最後の項目としてキーを設定します。先行スペースは無視されますが、鍵の中間および後続のスペースは使用されます。キーにスペースを含める場合、引用符がキーの一部でない限り、引用符でキーを囲まないでください。 単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにワイヤレス デバイスを設定するには、各 UDP ポート番号が異なるように、このコマンドを必要なだけ使用します。ワイヤレス デバイス ソフトウェアは、指定されている順序でホストを検索します。特定の RADIUS ホストで使用する timeout、retransmit、および encryption key の値を設定します。
ステップ 4	**aaa group server radius** *group-name*	AAA サーバ グループをグループ名で定義します。 このコマンドは、ワイヤレス デバイスをサーバ グループ コンフィギュレーション モードにします。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバと定義済みサーバ グループと関連付けます。AAA サーバ グループの各 RADIUS サーバでこの手順を繰り返します。 グループの各サーバは、手順 2 で事前に定義されている必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章の「Configuring RADIUS Login Authentication」の項を参照してください。

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

次の例では、ワイヤレス デバイスは、2 つの異なる RADIUS グループ サーバ（*group1* および *group2*）を認識するように設定されます。group1 には、同じサービスに設定されている同じ RADIUS サーバに 2 つの異なるホスト エントリがあります。2 つめのホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

ユーザ権限アクセスおよびネットワーク サービスの RADIUS 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可がイネーブルの場合、ワイヤレス デバイスは、ユーザのプロファイルから受け取った情報を使用します。これは、ローカル ユーザ データベースまたはセキュリティ サーバにあり、ユーザ セッションを設定します。ユーザには、ユーザ プロファイルにより許可されている場合だけ、要求されたサービスのアクセス権が付与されます。

グローバル コンフィギュレーション モードで、**radius** キーワードを指定した **aaa authorization** コマンドを使用して、ユーザの特権 EXEC モードへのネットワーク アクセスを制限するパラメータを設定できます。

aaa authorization exec radius コマンドは、これらの authorization パラメータを設定します。

- 認証が RADIUS を使用して実行された場合、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証が RADIUS を使用して実行されなかった場合、ローカル データベースを使用します。

（注） 許可は、許可が設定されている場合でも CLI レベルを介してログインする認証ユーザにバイパスされます。

特権 EXEC アクセスおよびネットワーク サービスに RADIUS 許可を指定する場合、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network radius**	すべてのネットワーク関連サービス要求に対して、ユーザ RADIUS 許可にワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec radius**	ワイヤレス デバイスをユーザ RADIUS 許可に設定して、ユーザが特権 EXEC アクセス権を持つかどうかを決めます。 **exec** キーワードは、ユーザ プロファイル情報（**autocommand** 情報など）を返す場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

RADIUS 設定の表示

RADIUS 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。

TACACS+ でのアクセス ポイント アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）を使用して、ワイヤレス デバイスへの管理者アクセスを制御する方法について説明します。TACACS+ をサポートするようにワイヤレス デバイスを設定する方法の詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章を参照してください。

TACACS+ は、詳細なアカウンティング情報、および認証や認可プロセスを介した柔軟な管理制御を提供します。TACACS+ は、AAA により促進され、AAA コマンドを介してだけイネーブルにできます。

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

ここでは、TACACS+ 設定について説明します。

- 「デフォルトの TACACS+ 設定」（P.10-16）
- 「TACACS+ ログイン認証の設定」（P.10-17）
- 「特権 EXEC アクセスおよびネットワーク サービスの TACACS+ 許可の設定」（P.10-18）
- 「TACACS+ 設定の表示」（P.10-19）

デフォルトの TACACS+ 設定

TACACS+ および AAA は、デフォルトでディセーブルにされています。

セキュリティの欠落を避けるため、ネットワーク管理アプリケーションを介して TACACS+ を設定できません。イネーブルにされている場合、TACACS+ は、CLI を介してワイヤレス デバイスにアクセスする管理者を認証できます。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義して、そのリストをさまざまなインターフェイスに適用します。認証方式のリストは、実行される認証のタイプ、およびそれらが実行される順序を定義します。これは、定義される認証方式が実行される前に、特定のインターフェイスに適用しなければなりません。唯一の例外は、デフォルトの認証方式リストです（この名前は *default* です）。デフォルトの認証方式リストは、名前付き認証方式リストが明示的に定義されているインターフェイスを除く、すべてのインターフェイスに自動的に適用されます。

認証方式リストは、ユーザの認証に使用される順序と認証方式を記述します。最初の方式が失敗した場合の認証にバックアップ システムが使用されるように、認証に 1 つ以上のセキュリティ プロトコルを指定できます。ソフトウェアは、リストの最初の方式を使用して、ユーザを認証します。この方式が応答しない場合、ソフトウェアは、方式リストの次の認証方式を選択します。このプロセスは、リストの認証方式との通信に成功するまで、または定義されているすべての方式が失敗するまで、続けられます。このサイクルのいずれかの時点で認証が失敗した場合、つまり、セキュリティサーバまたはローカル ユーザ名データベースが、ユーザ アクセスを拒否することで応答した場合、認証プロセスは停止し、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードから、次の作業を行います。これは必須手順です。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • 名前付きリストが **login authentication** コマンドで指定されていないときに使用されるデフォルト リストを作成するには、デフォルト状況で使用される方式リストが後に続く **default** キーワードを使用します。デフォルト方式リストは、すべてのインターフェイスに自動的に適用されます。 • *list-name* には、作成するリストに名前を付ける文字ストリングを指定します。 • *method1...* には、認証アルゴリズムが試行する実際の方式を指定します。認証の追加方式は、直前の方式からエラーが返された場合だけ使用されます。失敗した場合は、使用されません。 次のいずれかの方式を選択します。 • **local**：認証のローカル ユーザ名データベースを使用します。データベースにユーザ名情報を入力しなければなりません。**username** *password* コマンドをグローバル コンフィギュレーション モードで使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、TACACS+ サーバを設定しなければなりません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始して、認証リストを適用するラインを設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストをラインまたはラインのセットに適用します。 • **default** を指定する場合、**aaa authentication login** コマンドで作成したデフォルト リストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。

	コマンド	目的
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力内容を確認します。
ステップ 8	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

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

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可がイネーブルの場合、ワイヤレス デバイスは、ユーザ プロファイルから受け取った情報を使用します。これは、ローカル ユーザ データベースまたはセキュリティ サーバにあり、ユーザ セッションを設定します。ユーザには、ユーザ プロファイルの情報により許可されている場合だけ、要求されたサービスのアクセス権が付与されます。

グローバル コンフィギュレーション モードで、**tacacs+** キーワードを指定した **aaa authorization** コマンドを使用して、ユーザの特権 EXEC モードへのネットワーク アクセスを制限するパラメータを設定できます。

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

- 認証が TACACS+ を使用して実行された場合、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証が TACACS+ を使用して実行されなかった場合、ローカル データベースを使用します。

（注） 許可は、許可が設定されている場合でも CLI レベルを介してログインする認証ユーザにバイパスされます。

特権 EXEC アクセスおよびネットワーク サービスに TACACS+ 許可を指定する場合、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authorization network tacacs+**	すべてのネットワーク関連サービス要求に対して、ユーザ TACACS+ 許可にワイヤレス デバイスを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ワイヤレス デバイスをユーザ TACACS+ 許可に設定して、ユーザが特権 EXEC アクセス権を持つかどうかを決めます。 **exec** キーワードは、ユーザ プロファイル情報（**autocommand** 情報など）を返す場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

TACACS+ 設定の表示

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

ワイヤレス ハードウェアおよびソフトウェアの管理

ここでは、次の作業の実行について説明します。

- 「ワイヤレス デバイスの工場出荷時のデフォルト設定へのリセット」（P.10-19）
- 「ワイヤレス デバイスの再起動」（P.10-19）
- 「ワイヤレス デバイスのモニタリング」（P.10-20）

ワイヤレス デバイスの工場出荷時のデフォルト設定へのリセット

ワイヤレス デバイス ハードウェアおよびソフトウェアをその工場出荷時のデフォルト設定にリセットするには、ルータの Cisco IOS 特権 EXEC モードで、**service-module wlan-ap0 reset default-config** コマンドを使用します。

注意　データを損失することがあるため、シャットダウンまたは障害状態からの回復には、**service-module wlan-ap0 reset** コマンドだけを使用してください。

ワイヤレス デバイスの再起動

正規の手順でシャットダウンを実行し、ワイヤレス デバイスを再起動するには、ルータの Cisco IOS 特権 EXEC モードで、**service-module wlan-ap0 reload** コマンドを使用します。確認プロンプトで、**Enter** キーを押してアクションを確認するか、**n** を入力してキャンセルします。

自律モードで実行している場合、reload コマンドを使用する、再起動前に設定が保存されます。これに失敗した場合、次のメッセージが表示されます。

```
Failed to save service module configuration.
```

Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）モードで実行している場合、reload 機能は、通常、Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）により扱われます。**service-module wlan-ap0 reload** コマンドを入力した場合、次のメッセージが表示されます。

```
The AP is in LWAPP mode. Reload is normally handled by WLC controller.

Still want to proceed? [yes]
```

ワイヤレス デバイスのモニタリング

ここでは、ルータのハードウェアのモニタリング用のコマンドについて説明します。

- 「ワイヤレス デバイス統計情報の表示」（P.10-20）
- 「ワイヤレス デバイス ステータスの表示」（P.10-20）

ワイヤレス デバイス統計情報の表示

特権 EXEC モードで、**service-module wlan-ap0 statistics** コマンドを使用すると、ワイヤレス デバイス統計情報を表示できます。次に、このコマンドの出力例を示します。

```
  CLI reset count = 0
  CLI reload count = 1
  Registration request timeout reset count = 0
  Error recovery timeout reset count = 0
  Module registration count = 10

The last IOS initiated event was a cli reload at *04:27:32.041 UTC Fri Mar 8 2007
```

ワイヤレス デバイス ステータスの表示

特権 EXEC モードで、**service-module wlan-ap0 status** コマンドを使用すると、ワイヤレス デバイスのステータスおよびその設定情報を表示できます。次に、このコマンドの出力例を示します。

```
Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 2
Service Module is in Steady state
Service Module reset on error is disabled
Getting status from the Service Module, please wait..

Image path = flash:c8xx_19xx_ap-k9w7-mx.acregr/c8xx_19xx_ap-k9w7-mx.acre
gr
System uptime = 0 days, 4 hours, 28 minutes, 5 seconds
Router#d was introduced for embedded wireless LAN access points on Integrated Services
Routers.
```

システムの時刻と日付の管理

Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用して、自動的に、またはワイヤレス デバイスの時刻と日付を設定して、手動で、ワイヤレス デバイスのシステムの時刻と日付を管理できます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*』を参照してください。

ここでは、次の設定情報を示します。

- 「簡易ネットワーク タイム プロトコルについて」（P.10-21）
- 「SNTP の設定」（P.10-21）
- 「時刻および日付の手動設定」（P.10-22）

簡易ネットワーク タイム プロトコルについて

簡易ネットワーク タイム プロトコル（SNTP）は、NTP の簡素化されたクライアント専用バージョンです。SNTP は、NTP サーバから時刻を受信できるだけで、時刻サービスを他のシステムに提供できません。SNTP は、通常、100 ミリ秒以内の正確な時刻を提供しますが、NTP の複雑なフィルタリングおよび統計メカニズムは提供しません。

設定済みサーバにパケットを要求してこれを受信する、または任意のソースから NTP ブロードキャスト パケットを受信するように、SNTP を設定できます。複数のソースが NTP パケットを送信する場合、最適な層のサーバが選択されます。NTP および層の詳細については、次の URL をクリックしてください。

http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075

複数のサーバが同じ層にある場合、ブロードキャスト サーバよりも、設定済みサーバが優先されます。これらの両方を満たすサーバが複数ある場合、時刻パケットを最初に送信したサーバが選択されます。SNTP が新しいサーバを選択するのは、クライアントが現在選択されているサーバからパケットの受信を停止した場合、または（上記の条件に従って）SNTP がより最適なサーバを検出した場合だけです。

SNTP の設定

SNTP は、デフォルトでディセーブルにされています。SNTP をアクセス ポイントでイネーブルにするには、グローバル コンフィギュレーション モードで、表 2 にリストされているコマンドのいずれか、または両方を使用します。

表 2　　SNTP コマンド

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

sntp server コマンドは、各 NTP サーバに一度入力します。NTP サーバは、アクセス ポイントから SNTP メッセージに応答するように設定する必要があります。

sntp server コマンドおよび **sntp broadcast client** コマンドの両方を入力した場合、アクセス ポイントは、ブロードキャスト サーバから時刻を受信しますが、層が同じ場合、設定済みサーバからの時刻を優先します。SNTP の情報を表示するには、**show sntp** EXEC コマンドを使用します。

時刻および日付の手動設定

他の時刻ソースを使用できない場合、システムを再起動してから時刻と日付を手動で設定できます。次にシステムが再起動されるまで、正確な時刻に維持されます。手動での設定は最後の手段とすることをお勧めします。ワイヤレス デバイスが同期化できる外部ソースがある場合、システム クロックを手動で設定する必要はありません。

ここでは、次の設定情報を示します。

システム クロックの設定

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

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

	コマンド	目的
ステップ 1	**clock set** *hh*:*mm*:*ss day month year* または **clock set** *hh*:*mm*:*ss month day year*	次のいずれかの形式を使用して、システム クロックを手動で設定します。 • *hh*:*mm*:*ss* には、時間（24 時間形式）、分、秒で時刻を指定します。指定された時刻は、設定されている時間帯に関連します。 • *day* には、日付を月の日付で指定します。 • *month* には、月をその完全な名前で指定します。 • *year* には、年度を 4 桁（省略形ではなく）で指定します。
ステップ 2	**show running-config**	入力内容を確認します。
ステップ 3	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

次に、システム クロックを 2001 年 7 月 23 日、1:32 p.m. に手動で設定する例を示します。

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

時刻と日付の設定の表示

時刻と日付の設定を表示するには、特権 EXEC モードで、**show clock** [**detail**] コマンドを使用します。

システム クロックは、時刻が信頼できるか（正確か）どうかを示す *authoritative* フラグを保持します。システム クロックが、NTP などのタイミング ソースにより設定されている場合、フラグが設定されます。時刻が信頼できない場合、これは、表示目的だけに使用されます。ピアの時刻が無効な場合、クロックが信頼でき、*authoritative* フラグが設定されるまで、このフラグにより、両ピアがクロックと同期化しないようになります。

次に、**show clock** 表示の前に付いているシンボルの意味を示します。

- *****：時刻は信頼できません。
- （ブランク）：時刻は信頼できます。
- **.**：時刻は信頼できますが、NTP は同期化されません。

時間帯の設定

時間帯を手動で設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [***minutes-offset***]	時間帯を設定します。 ワイヤレス デバイスは、Universal Time Coordinated（UTC; 協定世界時）で内部時刻を保持するため、時刻が手動で設定される場合、このコマンドは、表示目的だけに使用されます。 • *zone* には、表示時刻が有効な場合に表示される時間帯の名前を入力します。デフォルトは UTC です。 • *hours-offset* には、UTC からの時間オフセットを入力します。 • （任意）*minutes-offset* には、UTC からの分オフセットを入力します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

グローバル コンフィギュレーション モードの **clock timezone** コマンドの *minutes-offset* 変数は、現地時間帯と UTC との差が分単位である場合に使用できます。たとえば、Atlantic Canada（AST）の一部の地区の時間帯は、UTC-3.5 です。ここで、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは、**clock timezone AST -3 30** です。

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

夏時間の設定

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	毎年指定された日に開始および終了する夏時間を設定します。 夏時間は、デフォルトでディセーブルにされています。パラメータを指定せずに、**clock summer-time** *zone* **recurring** を指定する場合、夏時間の規則は米国の規則をデフォルトにします。 • *zone* には、夏時間が施行されているときに表示される時間帯の名前（たとえば、PDT）を指定します。 • （任意）*week* には、月の何週目か（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（たとえば、Sunday）を指定します。 • （任意）*month* には、月（たとえば、January）を指定します。 • （任意）*hh*:*mm* には、時間および分で時刻（24 時間形式）を指定します。 • （任意）*offset* には、サマー タイム中に追加する時間を分単位で指定します。デフォルトは 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地時間帯を基準にしています。開始時刻は、標準時刻を基準にしています。終了時間は夏時間を基準にしています。開始月が、終了月前の場合、システムでは、南半球であると想定されます。

次に、夏時間が、4 月の第一日曜日の 02:00 から始まり、10 月の最後の日曜日の 02:00 に終わるように指定する例を示します。

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

現地の夏時間が、定期的なパターンに従わない（次の夏時間のイベントの正確な日付および時刻を設定する）場合、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または **clock summer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	夏時間が最初の日付で開始し、2 番目の日付で終了するように設定します。 夏時間は、デフォルトでディセーブルにされています。 • *zone* には、夏時間が施行されているときに表示される時間帯の名前（たとえば、PDT）を指定します。 • （任意）*week* には、月の何週目か（1 ～ 5 または **last**）を指定します。 • （任意）*day* には、曜日（たとえば、Sunday）を指定します。 • （任意）*month* には、月（たとえば、January）を指定します。 • （任意）*hh*:*mm* には、時間および分で時刻（24 時間形式）を指定します。 • （任意）*offset* には、サマー タイム中に追加する時間を分単位で指定します。デフォルトは 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

clock summer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番めの部分では終了時期を指定します。すべての時刻は、現地時間帯を基準にしています。開始時刻は、標準時刻を基準にしています。終了時間は夏時間を基準にしています。開始月が、終了月前の場合、システムでは、南半球であると想定されます。

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

次に、夏時間が 2000 年 10 月 12 日 02:00 に始まり、2001 年 4 月 26 日 02:00 に終了するよう設定する例を示します。

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名およびプロンプトの設定

識別できるようにワイヤレス デバイスのシステム名を設定します。デフォルトでは、システム名およびプロンプトは *ap* です。

システム プロンプトを設定しない場合、システム名の最初の 20 文字がシステム プロンプトとして使用されます。大なりシンボル（>）が追加されます。グローバル コンフィギュレーション モードで **prompt** コマンドを使用してプロンプトを手動で設定しない限り、プロンプトは、システム名が変更された場合に必ず更新されます。

（注） ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』および『*Cisco IOS IP Addressing Services Command Reference*』を参照してください。

ここでは、次の設定情報を示します。

- 「デフォルトのシステム名およびプロンプト設定」（P.10-26）
- 「システム名の設定」（P.10-26）
- 「DNS について」（P.10-27）

デフォルトのシステム名およびプロンプト設定

デフォルトのアクセス ポイント システム名およびプロンプトは *ap* です。

システム名の設定

システム名を手動で設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	システム名を手動で設定します。 デフォルト設定は、*ap* です。 **（注）** システム名を変更すると、ワイヤレス デバイス ラジオがリセットされ、関連付けられているクライアント デバイスの関連付けが解除され、その後すぐに再び関連付けられます。 **（注）** システム名は最高 63 文字まで入力できます。ただし、ワイヤレス デバイスがそれ自体をクライアント デバイスに識別する場合、システム名の最初の 15 文字だけ使用します。クライアント ユーザがデバイス間を区別することが重要な場合、システム名の一意の部分が最初の 15 文字になるようにしてください。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

システム名を設定する場合、名前は、システム プロンプトとしても使用されます。

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

DNS について

DNS プロトコルは、ホスト名を IP アドレスにマッピングできる分散データベースである、Domain Name System（DNS; ドメイン ネーム システム）を制御します。ワイヤレス デバイスで DNS を設定する場合、**ping**、**telnet**、**connect**、および関連する Telnet サポート操作など、すべての IP コマンドで、IP アドレスの代わりにホスト名を使用できます。

IP は、位置やドメインによってデバイスを識別できる階層ネーミング スキームを定義します。ドメイン名は、デリミタとしてピリオド（.）を使用して結合されます。たとえば、Cisco Systems は、IP が *com* ドメイン名により識別される営利団体であるため、そのドメイン名は *cisco.com* です。このドメインの、File Transfer Protocol（FTP; ファイル転送プロトコル）システムなど、特定のデバイスは、*ftp.cisco.com* として識別されます。

ドメイン名を追跡するため、IP は、IP アドレスにマッピングされる名前のキャッシュ（またはデータベース）を保持する、ドメイン ネーム サーバの概念を定義します。ドメイン名を IP アドレスにマッピングするには、ホスト名を識別し、ネットワークに存在するネーム サーバを指定し、DNS をイネーブルにする必要があります。

ここでは、次の設定情報を示します。

- 「デフォルトの DNS 設定」（P.10-27）
- 「DNS の設定」（P.10-28）
- 「DNS 設定の表示」（P.10-29）

デフォルトの DNS 設定

表 10-3 では、デフォルトの DNS 設定を示しています。

表 10-3　デフォルトの DNS 設定

機能	デフォルト設定
DNS enable state	ディセーブル。
DNS default domain name	設定されていません。
DNS servers	ネーム サーバ アドレスは設定されていません。

DNS の設定

DNS を使用するようにワイヤレス デバイスを設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	完全修飾でないホスト名（ドット付き 10 進表記ドメイン名を使用しない名前）を完成させるためにソフトウェアが使用するデフォルト ドメイン名を定義します。 未修飾名とドメイン名を区切る最初のピリオドを含めないでください。 起動時、ドメイン名は設定されません。ただし、ワイヤレス デバイス設定が BOOTP または DHCP サーバに渡される場合、デフォルト ドメイン名が BOOTP または DHCP サーバにより設定されることがあります（この情報でサーバが構成された場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	1 つ以上のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。 ネーム サーバは 6 台まで指定できます。スペースでサーバ アドレスを区切ります。最初に指定されるサーバは、プライマリ サーバです。ワイヤレス デバイスは、DNS 要求を最初にプライマリ サーバに送信します。この要求に失敗すると、バックアップ サーバに要求が送信されます。
ステップ 4	**ip domain-lookup**	（任意）ワイヤレス デバイスでの DNS に基づいたホスト名からアドレスへの変換をイネーブルにします。この機能は、デフォルトでイネーブルにされています。 ネットワーク デバイスが、名前割り当てを制御しないネットワークのデバイスとの接続を要求する場合、グローバル インターネット ネーミング スキーム（DNS）を使用して、デバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

ワイヤレス デバイス IP アドレスをそのホスト名として使用する場合、IP アドレスが使用され、DNS 要求は発生しません。ピリオド（.）を含まないホスト名を設定する場合、名前を IP アドレスにマッピングする DNS 要求が行われる前に、デフォルト ドメイン名が続くピリオドが、ホスト名に追加されます。デフォルト ドメイン名は、グローバル コンフィギュレーション モードで **ip domain-name** コマンドを設定される値です。ホスト名にピリオド（.）が含まれる場合、Cisco IOS ソフトウェアは、デフォルト ドメイン名をホスト名に追加せずに、IP アドレスを参照します。

ドメイン名を削除するには、グローバル コンフィギュレーション モードで、**no ip domain-name** *name* コマンドを使用します。ネーム サーバ アドレスを削除するには、グローバル コンフィギュレーション モードで、**no ip name-server** *server-address* コマンドを使用します。ワイヤレス デバイスで DNS をディセーブルにするには、グローバル コンフィギュレーション モードで、**no ip domain-lookup** コマンドを使用します。

DNS 設定の表示

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

（注）　DNS がワイヤレス デバイスで設定されている場合、**show running-config** コマンドを使用すると、サーバの名前ではなく、IP アドレスが表示されることがあります。

バナーの作成

Message-of-The-Day（MOTD）およびログイン バナーを設定できます。MOTD バナーは、接続されるすべての端末にログイン時に表示されます。これは、すべてのネットワーク ユーザに影響を与えるメッセージ（間もなくシステムがシャットダウンされるなど）を送信する場合に便利です。

ログイン バナーも接続されているすべての端末に表示されます。これは、MOTD バナーが表示されてから、ログイン プロンプトが表示されるまでに表示されます。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ここでは、次の設定情報を示します。

- 「デフォルトのバナー設定」（P.10-29）
- 「Message-of-the-Day ログイン バナーの設定」（P.10-29）
- 「ログイン バナーの設定」（P.10-30）

デフォルトのバナー設定

MOTD およびログイン バナーは設定されていません。

Message-of-the-Day ログイン バナーの設定

ワイヤレス デバイスへのログインが発生したときに画面に表示される単一または複数行のメッセージ バナーを作成できます。

MOTD ログイン バナーを設定するには、特権 EXEC モードから、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner motd** *c message c*	Message-of-the-Day を指定します。 *c* には、シャープ記号（#）などの必要なデリミタを入力し、**Enter** キーを押します。デリミタは、バナー テキストの開始および終了を示します。終了デリミタの後の文字は廃棄されます。 *message* には、最高 255 文字のバナー メッセージを入力します。メッセージでデリミタを使用できません。

	コマンド	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

次に、ワイヤレス デバイスの MOTD バナーを設定する例を示します。シャープ記号（#）は、開始および終了デリミタとして使用されます。

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

次の例では、直前の設定のバナーを示します。

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

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

User Access Verification

Password:
```

ログイン バナーの設定

接続されているすべての端末に表示されるログイン バナーを設定できます。このバナーは、MOTD バナーが表示されてから、ログイン プロンプトが表示されるまでに表示されます。

ログイン バナーを設定するには、特権 EXEC モードから、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**banner login** *c message c*	ログイン メッセージを指定します。 *c* には、シャープ記号（#）などの必要なデリミタを入力し、**Enter** キーを押します。デリミタは、バナー テキストの開始および終了を示します。終了デリミタの後の文字は廃棄されます。 *message* には、最高 255 文字のログイン メッセージを入力します。メッセージでデリミタを使用できません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

次に、ドル記号（$）を開始および終了デリミタとして使用して、ワイヤレス デバイスのログイン バナーを設定する例を示します。

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

イーサネットの速度およびデュプレックスの設定

Cisco 1941-W ISR インターフェイスは、デフォルトで 1000 Mbps 速度およびデュプレックス設定だけをサポートします。インターフェイスは常に稼動しています ワイヤレス デバイスがスイッチからインライン電力を受け取る場合、イーサネット リンクをリセットする速度またはデュプレックス設定を変更すると、ワイヤレス デバイスが再起動されます。

（注） ワイヤレス デバイス イーサネット ポートの速度またはデュプレックス設定は、ワイヤレス デバイスが接続されているポートのイーサネット設定と一致しなければなりません。ワイヤレス デバイスが接続されているポートの設定を変更する場合、ワイヤレス デバイス イーサネット ポートの設定もこれに一致するように変更します。

イーサネットの速度およびデュプレックスは、デフォルトで **auto** に設定されています。イーサネットの速度およびデュプレックスを設定するには、特権 EXEC モードから、次の作業を行います。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface fastethernet0**	コンフィギュレーション インターフェイス モードを開始します。
ステップ 3	**speed** {**10** | **100** | **auto**}	イーサネットの速度を設定します。デフォルト設定の **auto** を使用することをお勧めします。
ステップ 4	**duplex** {**auto** | **full** | **half**}	デュプレックスを設定します。デフォルト設定の **auto** を使用することをお勧めします。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	入力内容を確認します。
ステップ 7	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

ワイヤレス ネットワーク管理のアクセスポイントの設定

ワイヤレス デバイスをワイヤレス ネットワーク管理でイネーブルにできます。Wireless Network Manager（WNM; 無線ネットワーク マネージャ）は、ワイヤレス LAN のデバイスを管理します。

次のコマンドを入力して、WNM と相互作用するようにワイヤレス デバイスを設定します。

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

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

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

可能なステータスは、*not authenticated*、*authentication in progress*、*authentication fail*、*authenticated* および *security keys setup* です。

ローカル認証および許可のアクセス ポイントの設定

ローカル モードで AAA を実装するようにワイヤレス デバイスを設定して、サーバなしで動作するように AAA を設定できます。ワイヤレス デバイスは、認証および許可を扱います。この設定ではアカウンティングは使用できません。

（注）　ワイヤレス デバイスを 802.1x 対応クライアント デバイスのローカル オーセンティケータとして設定し、メイン サーバのバックアップを提供、または RADIUS サーバなしでネットワークの認証サービスを提供できます。ローカル オーセンティケータとしてワイヤレス デバイスを設定する方法の詳細については、Cisco.com 上のマニュアル『*Using the Access Point as a Local Authenticator*』を参照してください。
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

ワイヤレス デバイスをローカル AAA に設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ログイン認証を設定して、ローカル ユーザ名データベースを使用します。**default** キーワードは、ローカル ユーザ データベース認証をすべてのインターフェイスに適用します。
ステップ 4	**aaa authorization exec local**	ユーザ AAA 許可を設定して、ローカル データベースをチェックすることでユーザが EXEC シェルの実行を許可されるかどうかを決定します。
ステップ 5	**aaa authorization network local**	すべてのネットワーク関連サービス要求に対して、ユーザ AAA 許可を設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースを入力し、ユーザ名に基づいた認証システムを確立します。 このコマンドを各ユーザに繰り返します。 • *name* には、ユーザ ID を 1 単語で指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセス権を取得した後の権限レベルを指定します。範囲は、0 ～ 15 です。レベル 15 は、特権 EXEC モード アクセスを提供します。レベル 0 は、ユーザ EXEC モード アクセスを提供します。 • *encryption-type* には、暗号化されていないパスワードを使用する場合は **0** を入力します。非表示パスワードを使用する場合は **7** を入力します。 • *password* には、ワイヤレス デバイスへのアクセス権を取得するときにユーザが入力する必要があるパスワードを指定します。パスワードは、1 ～ 25 文字でなければなりません。スペースを含めることができます。また、パスワードは、**username** コマンドで指定される最後のオプションでなければなりません。 **（注）**　TAB、?、$、+ および [の文字は、パスワードには無効な文字です。
ステップ 7	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

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

認証キャッシュおよびプロファイルの設定

認証キャッシュおよびプロファイル機能を使用すると、アクセス ポイントでユーザの認証および許可応答をキャッシュに入れることができます。これにより、これ以降の認証および許可要求を AAA サーバに送信しなくて済みます。

（注）　アクセス ポイントでは、この機能は、Admin 認証だけでサポートされます。

この機能をサポートする次のコマンドは、Cisco IOS リリース 12.3(7) に含まれています。

cache expiry
cache authorization profile
cache authentication profile
aaa cache profile

（注）　これらのコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, Versions 12.4(10b)JA and 12.3(8)JEC*』を参照してください。

次に、許可キャッシュがイネーブルにされている、TACACS+ を使用した Admin 認証に設定されたアクセス ポイントの設定例を示します。この例は、TACACS サーバに基づいていますが、アクセス ポイントは、RADIUS を使用した Admin 認証に設定できます。

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

```
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
```

```
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

DHCP サービスを提供するアクセス ポイントの設定

次の項では、DHCP サーバとして機能するようにワイヤレス デバイスを設定する方法について説明します。

DHCP サーバの設定

デフォルトでは、アクセス ポイントは、ネットワークの DHCP サーバから IP 設定を受け取るように設定されています。また、アクセス ポイントを DHCP サーバとして機能するように設定して、IP 設定を有線およびワイヤレスの両方の LAN に割り当てることもできます。

（注）　アクセス ポイントを DHCP サーバとして設定する場合、IP アドレスは、そのサブネットのデバイスに割り当てられます。デバイスは、サブネット外ではなく、サブネット上の他のデバイスと通信します。データをサブネット外に渡す必要がある場合、デフォルト ルータを割り当てる必要があります。デフォルト ルータの IP アドレスは、DHCP サーバとして設定されているアクセス ポイントと同じサブネットになければなりません。

DHCP 関連のコマンドおよびオプションの詳細については、『*Cisco IOS IP Addressing Services Configuration Guide, Release 12.4*』の DHCP パートを参照してください。DHCP パートを参照するには、次の URL をクリックしてください。

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

アクセス ポイントを設定して、DHCP サービスを提供し、デフォルト ルータを指定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp excluded-address** *low_address* [*high_address*]	ワイヤレス デバイスが割り当てるアドレスの範囲からワイヤレス デバイス IP アドレスを除外します。10.91.6.158 のように 4 つの文字グループで IP アドレスを入力します。 ワイヤレス デバイスは、DHCP アドレス プール サブネットのすべての IP アドレスが、DHCP クライアントへの割り当てに使用できると想定します。そのため、DHCP サーバがクライアントへの割り当てに使用しない IP アドレスを指定する必要があります。 （任意）除外されたアドレスの範囲を入力するには、範囲のロー エンドのアドレスを入力し、その後で範囲のハイ エンドのアドレスを入力します。
ステップ 3	**ip dhcp pool** *pool_name*	DHCP 要求に応答してワイヤレス デバイスが割り当てる IP アドレスのプールの名前を作成し、DHCP コンフィギュレーションモードを開始します。

	コマンド	目的
ステップ 4	**network** *subnet_number* [*mask* | *prefix-length*]	アドレス プールのサブネット番号を割り当てます。ワイヤレス デバイスは、このサブネット内で IP アドレスを割り当てます。 （任意）アドレス プールのサブネット マスクを割り当てるか、アドレス プレフィクスを構成するビット数を指定します。このプレフィクスは、ネットワーク マスクを割り当てる代替方法です。プレフィクス長の前には、スラッシュ（/）を付ける必要があります。
ステップ 5	**lease** {*days* [*hours*] [*minutes*] | **infinite**}	ワイヤレス デバイスにより割り当てられる IP アドレスのリース期間を設定します。 • days：リース期間を日数で設定します。 • （任意）hours：リース期間を時間単位で設定します。 • （任意）minutes：リース期間を分単位で設定します。 • infinite：リース期間を無限に設定します。
ステップ 6	**default-router** *address* [*address2 ... address 8*]	サブネットの DHCP クライアントのデフォルト ルータの IP アドレスを指定します。ただし、IP アドレスが必要な場合、1 つのコマンド最高 8 つのアドレスを指定できます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力内容を確認します。
ステップ 9	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

これらのコマンドの **no** 形式を使用すると、デフォルト設定に戻すことができます。

次に、ワイヤレス デバイスを DHCP サーバとして設定する、IP アドレスの範囲を除外する、デフォルト ルータを割り当てる例を示します。

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

DHCP サーバ アクセス ポイントのモニタリングおよび保守

次の例では、DHCP サーバ アクセス ポイントのモニタリングおよび保守に使用できるコマンドについて説明します。

show コマンド

DHCP サーバとしてのワイヤレス デバイスの情報を表示するには、特権 EXEC モードで、表 10-4 のコマンドを入力します。

表 10-4　DHCP サーバの show コマンド

コマンド	目的
show ip dhcp conflict [*address*]	特定の DHCP サーバにより記録されるすべてのアドレス衝突のリストを表示します。ワイヤレス デバイス IP アドレスを入力して、ワイヤレス デバイスにより記録される衝突を表示します。
show ip dhcp database [*url*]	DHCP データベースの最近のアクティビティを表示します。 **（注）**　このコマンドは、特権 EXEC モードで使用します。
show ip dhcp server statistics	サーバ統計情報および送受信されたメッセージのカウント情報を表示します。

clear コマンド

DHCP サーバ変数をクリアするには、特権 EXEC モードで、表 10-5 のコマンドを使用します。

表 10-5　DHCP サーバの clear コマンド

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

debug コマンド

DHCP サーバ デバッグをイネーブルにするには、特権 EXEC モードで、次のコマンドを使用します。

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

このコマンドの **no** 形式を使用すると、ワイヤレス デバイス DHCP サーバのデバッグをディセーブルにできます。

セキュア シェルのアクセス ポイントの設定

ここでは、Secure Shell（SSH; セキュア シェル）機能の設定について説明します。

（注）　ここで使用されているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference for Release 12.4*』の「Secure Shell Commands」の項を参照してください。

SSH について

SSH は、レイヤ 2 またはレイア 3 デバイスへの安全なリモート接続を提供するプロトコルです。SSH バージョン 1 と SSH バージョン 2 の 2 つの SSH バージョンがあります。このソフトウェア リリースは、これら両方の SSH バージョンをサポートしています。バージョン番号を指定しない場合、アクセス ポイントでは、デフォルトで、バージョン 2 が使用されます。

SSH は、デバイスが認証されるときに強力な暗号化を提供することで、Telnet よりも安全なリモート接続を提供します。SSH 機能には、SSH サーバおよび SSH 統合クライアントがあります。クライアントは、次のユーザ認証方式をサポートしています。

- RADIUS（詳細について、「RADIUS でのアクセス ポイント アクセスの制御」（P.10-11）を参照してください）
- ローカル認証および許可（詳細については、「ローカル認証および許可のアクセス ポイントの設定」（P.10-32）を参照してください）

SSH の詳細については、『*Cisco IOS Security Configuration Guide for Release 12.4*』の第 5 部「Other Security Features」を参照してください。

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

SSH の設定

SSH を設定する前に、Cisco.com から暗号化されたソフトウェア イメージをダウンロードしてください。詳細については、このリリースのリリース ノートを参照してください。

SSH の設定および SSH 設定の表示については、『*Cisco IOS Security Configuration Guide for Release 12.4*』の第 6 部「Other Security Features」を参照してください。これは、次のリンクの Cisco.com から利用できます。

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html

クライアント ARP キャッシングの設定

関連するクライアント デバイスの Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシュを保守するようにワイヤレス デバイスを設定できます。ワイヤレス デバイスで ARP キャッシュを保守すると、ワイヤレス LAN のトラフィック負荷を軽減できます。ARP キャッシングは、デフォルトでディセーブルにされています。

ここでは、この情報について説明します。

クライアント ARP キャッシングについて

ワイヤレス デバイスの ARP キャッシングにより、ワイヤレス デバイスのクライアント デバイスの ARP 要求を停止することでワイヤレス LAN のトラフィックが軽減されます。ARP 要求をクライアント デバイスに転送せずに、ワイヤレス デバイスは、関連付けられているクライアント デバイスに代わり要求に応答します。

ARP キャッシングがディセーブルの場合、ワイヤレス デバイスは、関連付けられているクライアントにラジオ ポートを介してすべての ARP 要求を転送します。ARP 要求を受け取るクライアントはこれに応答します。ARP キャッシングがイネーブルの場合、ワイヤレス デバイスは、関連付けられているクライアントの ARP 要求に応答し、要求をクライアントに転送しません。ワイヤレス デバイスが、キャッシュにない IP アドレスの ARP 要求を受け取ると、ワイヤレス デバイスは、その要求をドロップし、これを転送しません。そのビーコンで、ワイヤレス デバイスは、クライアント デバイスにバッテリ寿命を延ばすためにブロードキャスト メッセージを安全に無視できることを通知する情報要素を含んでいます。

オプション ARP キャッシング

シスコ以外のクライアント デバイスがアクセス ポイントに関連付けられていて、データを受け渡さない場合、ワイヤレス デバイス は、クライアント IP アドレスを認識できない場合があります。このような状況がワイヤレス LAN で頻繁に発生する場合、オプション ARP キャッシングをイネーブルにできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスは、IP アドレスがワイヤレス デバイスに認識されているクライアントに代わって応答しますが、そのラジオ ポートから、認識されていないクライアントへの ARP 要求を転送します。ワイヤレス デバイスが、関連付けられているすべてのクライアントの IP アドレスを学習すると、関連付けられているクライアントに送信されない ARP 要求をドロップします。

ARP キャッシングの設定

関連付けられているクライアントの ARP キャッシングを保守するようにワイヤレス デバイスを設定するには、特権 EXEC モードから、次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**dot11 arp-cache** [**optional**]	ワイヤレス デバイスで ARP キャッシングをイネーブルにします。 • （任意）**optional** キーワードを使用して、IP アドレスがワイヤレス デバイスに認識されているクライアント デバイスだけで ARP キャッシングをイネーブルにします。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力内容を確認します。
ステップ 5	**copy running-config startup-config**	（任意）入力内容をコンフィギュレーション ファイルに保存します。

次に、ARP キャッシングをアクセス ポイントで設定する例を示します。

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

ポイントツーマルチポイント ブリッジの複数の VLAN およびレート制限の設定

この機能は、各 VLAN でのトラフィック レートを制御できる機能により、複数の VLAN で動作するように、ポイントツーマルチポイント ブリッジをどのように設定できるかを変更します。

（注）　レート制限ポリシーは、非ルート ブリッジのファスト イーサネット入力ポートだけに適用できます。

通常、複数の VLAN サポートにより、ユーザは、個々の VLAN に各リモート サイトがある、リモート サイトでのポイントツーマルチポイント ブリッジ リンクを設定できます。この設定では、トラフィックを各サイトに分割し制御できます。レート制限を設定すると、全体のリンク帯域幅の消費量が指定量を超えるリモート サイトがなくなります。非ルート ブリッジのファスト イーサネット入力ポートを使用して、アップリンク トラフィックだけを制御できます。

クラスベースのポリシー機能を使用することで、レート制限を指定して、非ルート ブリッジのイーサネット インターフェイスの入力できます。イーサネット インターフェイスの入力でレートを提供すると、すべての着信イーサネット パケットが設定レートに準拠するようになります。

PART 4

追加情報

CHAPTER 11

構成例

この章では、Cisco 860 シリーズおよび 880 シリーズ Integrated Services Router（ISR; サービス統合型ルータ）の一般的ないくつかの構成例について説明します。

構成例について

この章では、Cisco 860 シリーズおよび Cisco 880 シリーズ ISR の一般的な構成例を挙げ、各構成例の概要を説明するとともに、新機能に関する情報の参照先を示します。

Cisco 860 シリーズおよび Cisco 880 シリーズ ISR の主な機能には、次のものがあります。

- 3G ワイヤレス データ接続のバックアップ（一部の Cisco 880 シリーズ ISR）
- 音声機能（一部の Cisco 880 シリーズ ISR）
- 組み込み型ワイヤレス デバイス（オプション）
- Power over Ethernet（すべての Cisco 880 シリーズ ISR）

3G ワイヤレス バックアップ

一部の Cisco 880 シリーズ ISR には、3G ワイヤレス データ バックアップ機能が搭載されています。詳細については、第 4 章「バックアップ データ ラインおよびリモート管理の設定」を参照してください。

音声

一部の Cisco 880 シリーズ ISR には、音声機能が搭載されています。詳細については、『*Cisco IOS Voice Configuration Library*』を参照してください。

組み込み型ワイヤレス デバイス

- Cisco 860 シリーズ、Cisco 880 シリーズ、および Cisco 890 ISR には、独自のバージョンの Cisco IOS ソフトウェアが稼動する、オプションのワイヤレス デバイスがあります。
  - アクセス ポイントが組み込まれた Cisco 890 シリーズ ISR は、ルータが IP Base 機能セットと Cisco IOS 12.4(22)YB ソフトウェア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。
  - 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 機能セットと Cisco IOS 12.4(20)T ソフトウェア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。
  - アクセス ポイントが組み込まれた Cisco 860 シリーズ ISR は、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せん。

（注）　Cisco Unified アーキテクチャの中で組み込み型アクセス ポイントを使用するには、バージョン 5.1 以降のシスコ Wireless LAN Configuration（WLC）を実行している必要があります。

アップグレード情報については、第 8 章「ワイヤレス デバイスの基本設定」を参照してください。

Power Over Ethernet

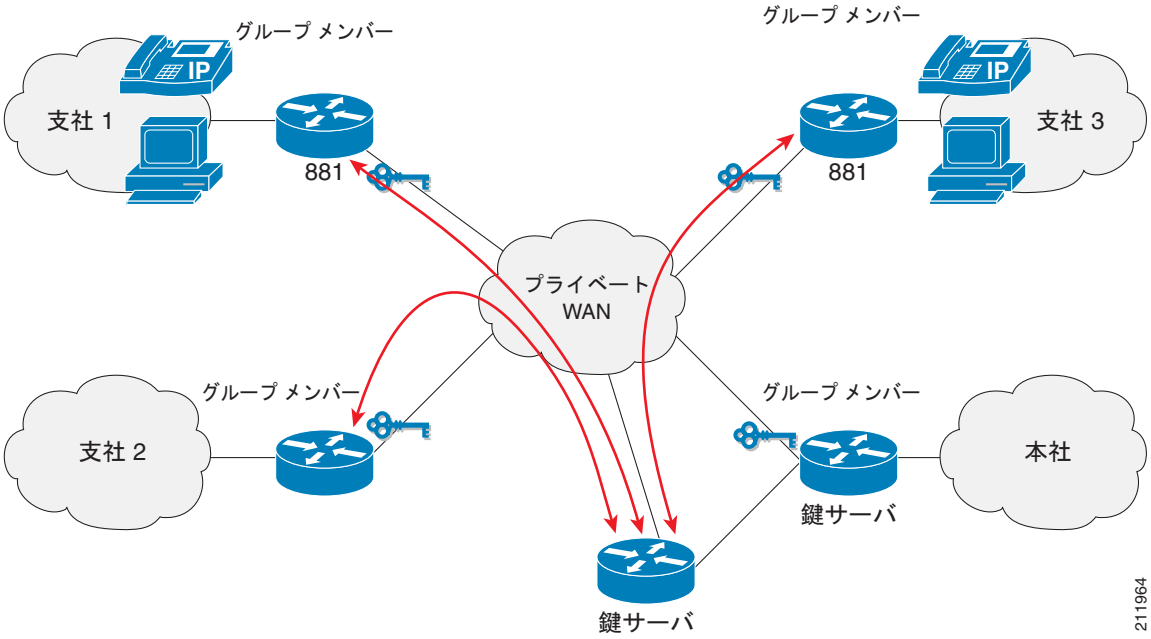
すべての Cisco 880 シリーズ ISR には、Power Over Ethernet（PoE）機能が搭載されています。詳細については、『*Cisco 860 Series, Cisco 880 Series, and Cisco 890 Series Integrated Services Routers Hardware Installation Guide*』を参照してください。

エンタープライズ スモール ブランチ

図 11-1 に、次のテクノロジーと機能を使用したエンタープライズ スモール ブランチ構成を示します。

- 非常にスケーラブルで安全なブランチ接続のための、Group Encrypted Transport VPN（GETVPN）
- ネットワーク接続の最前線の安全を確保し、ネットワークおよびアプリケーション レイヤの保護をエンタープライズ ネットワークに提供する、Cisco IOS Fiwawall（FW; ファイアウォール）ポリシー
- 音声アプリケーションおよびマルチキャスト アプリケーション
- 重要なアプリケーションに優先度を設定し、遅延に敏感なアプリケーションやミッションクリティカル アプリケーションを適切な時間内に配送する Quality of service（QoS; サービス品質）

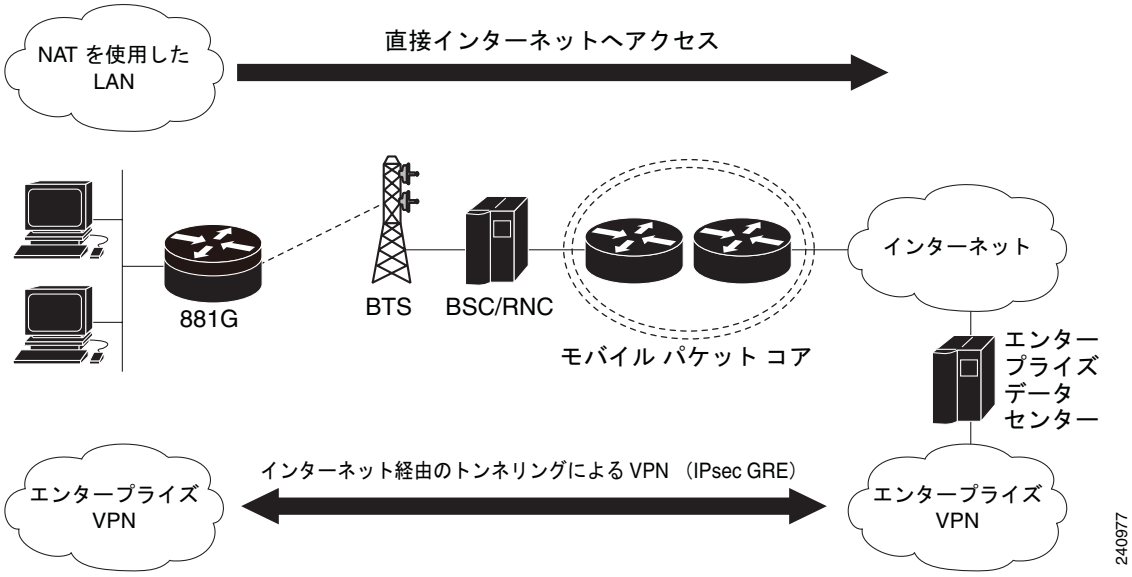
図 11-1　　エンタープライズ スモール ブランチ



3G を使用したインターネット サービスと IPSec VPN

図 11-2 に、エンタープライズ データ センターと通信するために、バックアップ アプリケーションとプライマリ アプリケーションの両方で 3G ワイヤレス テクノロジーを使用した、リモート オフィス構成を示します。Cisco 880 シリーズ ISR では、Network Address Translation（NAT; ネットワーク アドレス変換）を使用して直接インターネットにアクセスできるのに加え、公衆インターネット経由で安全かつプライベートに通信するため、IP Security および Generic Routing Encapsulation（IPSec+GRE; IPS + 総称ルーティング カプセル化）を使用した、トンネリングによる Virtual Private Network（VPN; 仮想私設網）サービスを提供できます。

図 11-2　　3G を使用したインターネット サービスと IPSec VPN

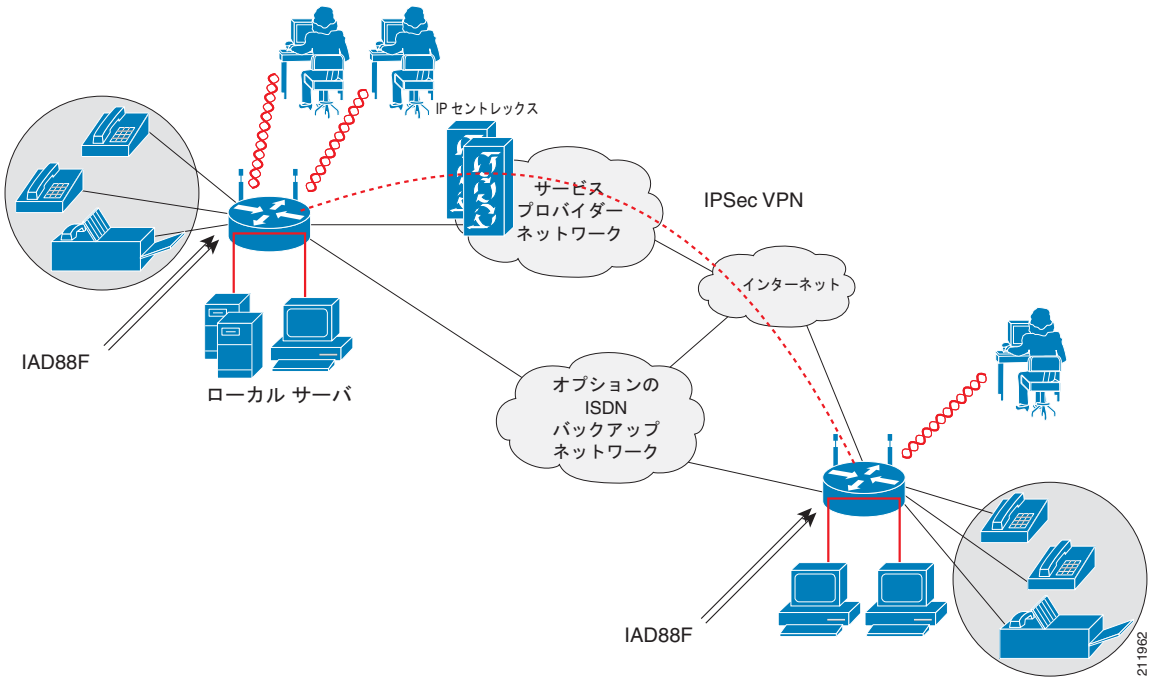


小規模から中規模のビジネス構成（SMB）アプリケーション

図 11-3 に、次のテクノロジーと機能を各ブランチ オフィスで使用した、小規模から中規模のビジネス構成を示します。

- リモート オフィスと在宅勤務者のための安全な VPN を簡単に実現するための、Easy VPN と Virtual Tunnel Interface（VTI）。
- セキュリティのためのディープ パケット インスペクション ファイアウォール。ファイアウォールは、第 1 レベルのアクセス チェックを行います。ファイアウォールは、侵入防御、暗号化、エンドポイント セキュリティなどの他のセキュリティ テクノロジーとともに動作し、包括的な多層防御によるエンタープライズ セキュリティ システムを提供します。
- インライン Intrusion Prevention Systems（IPS; 侵入防御システム）保護は、さらなるセキュリティを提供し、Cisco Self-Defending Network（SDN; 自己防衛型ネットワーク）の中核をなします。Cisco IOS IPS は、実世界の悪意のあるトラフィックまたは有害なトラフィックを正確に分類、識別、停止または遮断するための知能により、ネットワークが自身を防御するのに役立ちます。
- QoS は、遅延に敏感なアプリケーションやミッションクリティカル アプリケーションを適切な時間内に配送します。
- ISDN 接続によるバックアップは、プライマリ サービス プロバイダー リンクが障害になった場合の、ネットワークの冗長性を提供します。
- 既存のアナログ音声と FAX 機能のサポート。

図 11-3　　小規模から中規模のビジネス

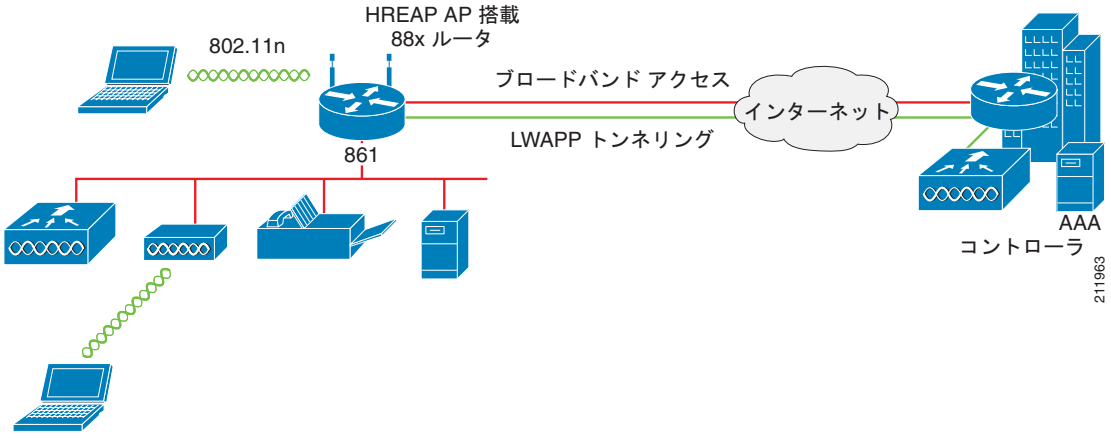


LWAPP を使用したエンタープライズ ワイヤレス構成

図 11-4 に、Lightweight Access Point Protocol（LWAPP; Lightweight アクセス ポイント プロトコル）と次のテクノロジーおよび機能を使用した、エンタープライズ ワイヤレス LAN 構成を示します。

- ブロードバンド インターネット アクセスと中央サイトへの VPN 接続。
- Hybrid Remote Edge Access Point（H-REAP; ハイブリッド リモート エッジ アクセス ポイント）は、リモート オフィスおよびブランチ オフィスに対してワイヤレス LAN サービスを提供します。それぞれの場所でワイヤレス LAN コントローラを使用する必要はありません。HREAP を使用すると、ローカルでのトラフィックのブリッジ、WAN 上でのトラフィックのトンネリング、Service Set Identifier（SSID; サービス セット ID）ごとの LWAPP 上でのトラフィックのトンネリングが可能です。
- Cisco Wireless Control System（WCS）を使用したダイナミックな RF 管理。
- 組み込み型アクセス ポイントと外部アクセス ポイントを組み合わせることができる機能。

図 11-4　　LWAPP を使用したワイヤレス LAN



CHAPTER 12

トラブルシューティング

この章では、問題を切り分けたり、問題の原因がそのルータにないことを判断する方法について説明します。この章で説明する内容は、次のとおりです。

はじめに

ソフトウェアに関する不具合のトラブルシューティングを行う前に、ライトブルーのコンソール ポートを使用して端末または PC をルータに接続してください（接続方法については、「関連資料」（P.xv）にあるマニュアルを参照してください）。接続した端末または PC を使用して、ルータからのステータス メッセージの確認やコマンドの入力といったトラブルシューティング作業を行います。

また、Telnet を使用してリモートから各インターフェイス（イーサネット、ADSL、または電話）にアクセスすることもできます。Telnet オプションを使用する方法では、インターフェイスが稼動していることが前提になります。

代理店に連絡する前に

問題の原因が見つからない場合は、製品を購入した代理店に連絡し、指示を求めてください。代理店に連絡する前に、次の情報を用意してください。

- シャーシのタイプとシリアル番号
- 保守契約または保証内容
- ソフトウェアのタイプおよびバージョン番号
- ハードウェアを受け取った日付
- 問題の概要
- 問題箇所を特定するために行った手順の概要

ADSL のトラブルシューティング

ADSL 接続に問題が起こった場合は、次のことを確認してください。

- ADSL 回線が接続されており、ピン 3 とピン 4 を使用している。ADSL 接続の詳細については、ご使用のルータのハードウェア ガイドを参照してください。
- ADSL CD LED がオンになっている。オンになっていない場合、ルータは DSL Access Multiplexer（DSLAM）に接続されていない可能性があります。ADSL LED の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- Asynchronous Transfer Mode（ATM; 非同期転送モード）の適切な Virtual Path Identifier（VPI; 仮想パス識別子）/Virtual Circuit Identifier（VCI; 仮想回線識別子）が使用されている。
- DSLAM は Discrete Multi-Tone（DMT; ディスクリート マルチトーン）Issue 2 をサポートしている。
- シスコ ルータに接続している ADSL ケーブルは、10 BASE-T カテゴリ 5、Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを使用する必要があります。通常の電話用のケーブルを使用すると、回線エラーが起こる場合があります。

Symmetrical High-Data-Rate Digital Subscriber Line（SHDSL）のトラブルシューティング

Cisco 888 ルータでは、Symmetrical High-Data-Rate Digital Subscriber Line（SHDSL）が利用できます。SHDSL 接続に問題が起こった場合は、次のことを確認してください。

- SHDSL 回線が接続されており、ピン 3 とピン 4 を使用している。G.SHDSL 接続の詳細については、ご使用のルータのハードウェア ガイドを参照してください。
- G.SHDSL LED がオンになっている。オンになっていない場合、ルータは DSL Access Multiplexer（DSLAM）に接続されていない可能性があります。G.SHDSL LED の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- 非同期転送モード（ATM）の適切な 仮想パス識別子 / 仮想回線識別子（VPI/VCI）が使用されている。
- DSLAM が G.SHDSL シグナリング プロトコルをサポートしている。

SHDSL のコンフィギュレーションを確認するには、EXEC モードで **show controllers dsl 0** コマンドを使用します。

VDSL2 のトラブルシューティング

Cisco 887 ルータでは、Very-high-data-rate Digital Subscriber Line 2（VDSL2）が利用できます。VDSL2 接続に問題が起こった場合は、次のことを確認してください。

- VDSL2 回線が接続されており、ピン 3 とピン 4 を使用している。VDSL2 接続の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- VDSL2 LED がオンになっている。オンになっていない場合、ルータは DSL Access Multiplexer（DSLAM）に接続されていない可能性があります。VDSL2 LED の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- DSLAM が VDSL2 信号プロトコルをサポートしている。

VDSL2 のコンフィギュレーションを確認するには、EXEC モードで **show controllers vdsl 0** コマンドを使用します。**debug vdsl 0 daemon state** コマンドを使用すると、VDSL2 トレーニングの状態遷移を表示するデバッグ メッセージが有効になります。

VDSL ファームウェア ファイルに問題がある場合は、リロードまたはアップグレードすることができます。Cisco IOS イメージのアップグレードは必要ありません。ファームウェア ファイルを VDSL モデム チップセットにロードするには、コマンド

controller vdsl 0 firmware *flash:<firmware file name>*

を使用します。次に、コントローラの vdsl 0 インターフェイスで、**shutdown/no shutdown** コマンドを入力します。この後、新しいファームウェアがダウンロードされ、VDSL2 回線のトレーニングが開始されます。

コマンドが存在しない場合や、指定した名前のファームウェア ファイルが壊れているか存在しない場合は、デフォルトのファームウェア ファイル *flash:vdsl.bin* が存在し壊れていないことが確認されます。その後、このファイルの中のファームウェアがモデム チップセットにダウンロードされます。

show interfaces トラブルシューティング コマンド

すべての物理ポート（イーサネット、ファスト イーサネット、および ATM）およびルータ上の論理インターフェイスの状態を表示するには、**show interfaces** コマンドを使用します。表 12-1 では、コマンド出力のメッセージを示しています。

例 12-1　　イーサネットまたはファスト イーサネット インターフェイスのステータス表示

```
Router# show interfaces ethernet 0 **similar output for show interfaces fastethernet 0
command **
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.0c13.a4db
(bia0010.9181.1281)
Internet address is 170.1.4.101/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255., txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
```

例 12-2　　ATM インターフェイスのステータス表示

```
Router# show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 14.0.0.16/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

例 12-3　　ダイヤラ インターフェイスのステータス表示

```
Router# show interfaces dialer 1
Dialer 1 is up, line protocol is up
    Hardware is Dialer interface
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
        255/255. txload 1/255, rxload 1/255
    Encapsulation PPP, loopback not set
    Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

表 12-1 に、**show interfaces** コマンドの出力を示します。

表 12-1　　show interfaces コマンド出力の説明

出力	原因
ATM インターフェイスの場合	
ATM 0 is up, line protocol is up	ATM 回線はアップで、正しく動作しています。
ATM 0 is down, line protocol is down	• ATM インターフェイスは **shutdown** コマンドによってディセーブルにされています。 または • ATM 回線はダウンしています。ADSL ケーブルが切断されたか、間違ったタイプのケーブルが ATM ポートに接続されている可能性があります。
ATM 0.*n* is up, line protocol is up	指定された ATM サブインターフェイスはアップで、正しく動作しています。

表 12-1　show interfaces コマンド出力の説明 （続き）

出力	原因
ATM 0.*n* is administratively down, line protocol is down	指定された ATM サブインターフェイスは **shutdown** コマンドによってディセーブルにされています。
ATM 0.*n* is down, line protocol is down	指定された ATM サブインターフェイスはダウンしています。ATM 回線が（サービス プロバイダーによって）切断された可能性があります。
イーサネットまたはファスト イーサネット インターフェイスの場合	
Ethernet/Fast Ethernet *n* is up, line protocol is up	指定されたイーサネットまたはファスト イーサネット インターフェイスはネットワークに接続されており、正しく動作しています。
Ethernet/Fast Ethernet *n* is up, line protocol is down	指定されたイーサネットまたはファスト イーサネット インターフェイスは正しく設定され、イネーブルになっていますが、イーサネット ケーブルは LAN から切断されている可能性があります。
Ethernet/Fast Ethernet *n* is administratively down, line protocol is down	指定されたイーサネットまたはファスト イーサネット インターフェイスは **shutdown** コマンドによりディセーブルになっており、インターフェイスは切断されています。
ダイヤラ インターフェイスの場合	
Dialer *n* is up, line protocol is up	指定されたダイヤラ インターフェイスはアップで、正しく動作しています。
Dialer *n* is down, line protocol is down	• これは標準メッセージであり、設定の誤りを示しているとは限りません。 または • 指定されたダイヤラ インターフェイスに問題がある場合、このメッセージはインターフェイスが動作していないことを意味する可能性があります。これには、インターフェイスが **shutdown** コマンドでダウン状態になっている、または ADSL ケーブルが接続されていない、などの理由が考えられます。

ATM トラブルシューティング コマンド

ATM インターフェイスのトラブルシューティングを行うには、次のコマンドを使用します。

- ping atm interface コマンド
- show atm interface コマンド
- debug atm コマンド

ping atm interface コマンド

ping atm interface コマンドを使用して、特定の PVC が使用中であるかどうかを判別することができます。このコマンドを使用する際にルータで PVC を設定する必要はありません。例 12-4 は、PVC 8/35 が使用中であるかどうかを判別するためにこのコマンドを使用する例を示しています。

例 12-4　　PVC が使用中かどうかの特定

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

このコマンドは、5 つの OAM F5 ループバック パケットを DSLAM（セグメント OAM パケット）へ送信します。PVC が DSLAM で設定されている場合、ping は成功します。

PVC がアグリゲータで使用中であるかどうかをテストするには、次のコマンドを入力します。

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

このコマンドはエンドツーエンド OAM F5 パケットを送信します。このパケットは、アグリゲータによりエコーバックされます。

show atm interface コマンド

ATM インターフェイスについての ATM 固有の情報を表示するには、特権 EXEC モードで **show atm interface atm 0** コマンドを使用します（例 12-5 を参照）。

例 12-5　ATM インターフェイスに関する情報の確認

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0

Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
Avail bw = 640
Config. is ACTIVE
```

表 12-2 は、コマンド出力で表示されるフィールドの一部です。

表 12-2　show atm interface コマンド出力の説明

フィールド	説明
ATM interface	インターフェイス番号。Cisco 860 および Cisco 880 シリーズ アクセス ルータの場合は常に 0 です。
AAL enabled	イネーブルの AAL のタイプ。Cisco 860 および Cisco 880 シリーズ アクセス ルータは AAL5 をサポートしています。
Maximum VCs	インターフェイスがサポートする仮想接続の最大数。
Current VCCs	アクティブな Virtual Channel Connection（VCC; 仮想チャネル接続）の数。
Maximum Transmit Channels	伝送チャネルの最大数。
Max Datagram Size	最大データグラム内で設定されたバイトの最大数。
PLIM Type	Physical Layer Interface Module（PLIM; 物理レイヤ インターフェイス モジュール）タイプ。

debug atm コマンド

ネットワークのコンフィギュレーションに関する問題のトラブルシューティングを行うには、**debug** コマンドを使用します。**debug** コマンドでは、問題の解決に役立つさまざまな情報が表示されます。

debug コマンドを使用する場合の注意事項

正しい結果を得るために、debug コマンドを使用する前に次の注意事項をよく確認してください。

- debug コマンドはすべて特権 EXEC モードで実行します。
- デバッグ メッセージをコンソールに表示するには、**logging console debug** コマンドを入力します。
- ほとんどの **debug** コマンドは引数を使用しません。
- デバッグ機能をディセーブにするには、**undebug all** コマンドを使用します。
- ルータで Telnet セッション中に **debug** コマンドを使用する場合は、**terminal monitor** コマンドを使用します。

注意　デバッグにはルータ CPU プロセスの中で高いプライオリティを与えられているため、デバッグを実行するとルータが使用不能になる場合があります。そのため、特定の問題のトラブルシューティングを行う場合にだけ **debug** コマンドを使用してください。ネットワーク上の他のアクティビティが影響を受けないよう、ネットワーク トラフィックが少ないときに debug コマンドを使用することを推奨します。

debug コマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

debug atm errors コマンド

ATM エラーを表示するには、**debug atm errors** コマンドを使用します。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。例 12-6 に出力例を示します。

例 12-6　ATM エラーの確認

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

debug atm events コマンド

ATM インターフェイス プロセッサで発生したイベントを表示して、ATM ネットワークの問題点を診断するには、**debug atm events** コマンドを使用します。このコマンドは、ネットワークの安定性についての全体像を表示します。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

インターフェイスが電話会社の Digital Subscriber Line Access Multiplexer（DSLAM）とうまく通信できた場合、モデム状態は 0x10 です。インターフェイスが DSLAM と通信していない場合、モデム状態は 0x8 です。例 12-7 に、アップでトレーニングに成功した ADSL 回線を示します。例 12-8 に、正常に通信していない ADSL 回線を示します。モデムの状態が 0x10 になっていないことに注意してください。

例 12-7　　ATM インターフェイス プロセッサ イベントの表示：正常

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

例 12-8　　ATM インターフェイス プロセッサ イベントの表示：不良

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

debug atm packet コマンド

debug atm packet コマンドは、着信および送信パケットのすべてのプロセス レベル ATM パケットを表示する場合に使用します。パケットが受信された場合、または送信が試行された場合、出力報告情報はオンラインです。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

注意　**debug atm packet** コマンドは、処理するすべてのパケットについて、かなりの量の出力を生成します。他のシステム アクティビティが影響を受けないよう、ネットワーク トラフィックが少ない場合にだけ使用してください。

コマンド構文は次のとおりです。

debug atm packet [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

no debug atm packet [**interface atm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

これらのキーワードの定義は、次のとおりです。

interface atm *number*　（任意）ATM インターフェイスまたはサブインターフェイス番号

vcd *vcd-number*　（任意）Virtual Circuit Designator（VCD; 仮想回線識別子）の番号

vc *vpi/vci number*　ATM PVC の VPI/VCI の値

例 12-9 に、**debug atm packet** コマンドの出力例を示します。

例 12-9　ATM パケット処理の確認

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

表 12-3 に、**debug atm packet** コマンド出力で表示されるフィールドの一部を示します。

表 12-3　debug atm packet コマンド出力の説明

フィールド	説明
ATM0	パケットを生成しているインターフェイス。
(O)	出力パケット。(I) は、受信パケットを意味します。
VCD: 0x*n*	このパケットに対応付けられる仮想回線。*n* は値です。
VPI: 0x*n*	このパケットの仮想パス識別子。*n* は値です。
DM: 0x*n*	記述子モード ビット。*n* は値です。
Length: *n*	ATM ヘッダーを含むパケットの全長（バイト単位）。

ソフトウェア アップグレード方法

Cisco 860 および Cisco 880 シリーズ サービス統合型ルータのソフトウェアは、次の方法でアップグレードできます。

- 既存の Cisco IOS ソフトウェア イメージの実行中に、LAN または WAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ブート イメージ（ROM モニタ）の実行中に、LAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ROM モニタ モードで新しいソフトウェア イメージをコンソール ポート経由でコピーします。
- ROM モニタ モードで、TFTP サーバにロードされたソフトウェア イメージからルータを起動します。この方法を使用するには、TFTP サーバがルータと同じ LAN 上にある必要があります。

パスワードの回復

イネーブル パスワードまたはイネーブル シークレット パスワードを回復するには、次の作業を行います。

1. コンフィギュレーション レジスタの変更
2. ルータのリセット
3. パスワードのリセットと変更の保存（イネーブル シークレット パスワードを忘れた場合だけ）
4. コンフィギュレーション レジスタ値のリセット

（注） パスワードを回復できるのは、コンソール ポートを使用してルータに接続している場合だけです。Telnet セッション経由では実行できません。

ヒント イネーブル シークレット パスワードの変更方法のさらに詳しい情報については、Cisco.com の「Hot Tips」を参照してください。

コンフィギュレーション レジスタの変更

コンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ 1　ルータの CONSOLE ポートに、ASCII 端末または端末エミュレーション プログラムが稼動している PC を接続します。

ステップ 2　端末を 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビットに設定します。

ステップ 3　特権 EXEC プロンプト（*router_name* #）に、**show version** コマンドを入力すると、現在のコンフィギュレーション レジスタ値が表示されます（次の出力例の末尾の太字部分を参照）。

```
Router# show version
Cisco IOS Software, C880 Software (C880-ADVENTERPRISEK9-M), Version 12.3(nightly
.PCBU_WIRELESS041110) NIGHTLY BUILD, synced to haw_t_pi1_pcbu HAW_T_PI1_PCBU_200
40924
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 11-Nov-04 03:37 by jsomebody

ROM: System Bootstrap, Version 1.0.0.6(20030916:100755) [jsomebody],
 DEVELOPMENT SOFTWARE

Router uptime is 2467 minutes
System returned to ROM by power-on
System image file is "flash:c880-adventerprisek9-mz.pcbu_wireless.041110"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
use. Delivery of Cisco cryptographic products does not imply
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 877 (MPC8272) processor (revision 0x00) with 59392K/6144K bytes of memory.

Processor board ID
MPC8272 CPU Rev: Part Number 0xC, Mask Number 0x10
4 FastEthernet interfaces
1 ATM interface
1 802.11 Radio
128K bytes of non-volatile configuration memory.
20480K bytes of processor board System flash (Intel Strataflash)

Configuration register is 0x2102
```

ステップ 4　コンフィギュレーション レジスタの設定値を記録しておきます。

ステップ 5　ブレークの設定（コンフィギュレーション レジスタのビット 8 の値で示されます）をイネーブルにするには、特権 EXEC モードで **config-register 0x01** コマンドを使用します。

- ブレーク イネーブル：ビット 8 が 0 に設定されています。
- ブレーク ディセーブル（デフォルトの設定）：ビット 8 が 1 に設定されています。

ルータのリセット

ルータをリセットする手順は、次のとおりです。

ステップ 1　ブレークがイネーブルになっている場合は、ステップ 2 に進みます。ブレークがディセーブルになっている場合は、ルータの電源をオフ（O）にしてから 5 秒後に、再びオン（|）にします。その後 60 秒以内に、**Break** キーを押します。端末に ROM モニタ プロンプトが表示されます。ステップ 3 に進みます。

（注）　一部の端末では、キーボードに *Break* というラベルの付いたキーがあります。使用するキーボードに Break キーがない場合は、端末に付属のマニュアルを参照して、ブレーク信号の送信方法を確認してください。

ステップ 2　**break** を押します。端末に次のプロンプトが表示されます。

```
rommon 2>
```

ステップ 3　**confreg 0x142** を入力して、コンフィギュレーション レジスタをリセットします。

```
rommon 2> confreg 0x142
```

ステップ 4　**reset** コマンドを入力して、ルータを初期化します。

```
rommon 2> reset
```

ルータの電源が一度オフになってからオンになり、コンフィギュレーション レジスタが 0x142 に設定されます。ルータはブート ROM システム イメージを使用します。その状況はシステム コンフィギュレーション ダイアログで示されます。

```
--- System Configuration Dialog ---
```

ステップ 5　次のメッセージが表示されるまで、各プロンプトに **no** を入力します。

```
Press RETURN to get started!
```

ステップ 6　**Enter** キーを押します。次のプロンプトが表示されます。

```
Router>
```

ステップ 7　**enable** コマンドを入力して、イネーブル モードを開始します。コンフィギュレーション変更は、イネーブル モードでだけ行うことができます。

```
Router> enable
```

プロンプトが特権 EXEC プロンプトに変わります。

```
Router#
```

ステップ 8　**show startup-config** コマンドを入力すると、コンフィギュレーション ファイルに保存されているイネーブル パスワードが表示されます。

```
Router# show startup-config
```

イネーブル パスワードを回復する場合には、「パスワードのリセットと変更の保存」に示す手順は実行しないでください。代わりに、「コンフィギュレーション レジスタ値のリセット」に記載されている手順を実行して、パスワード回復作業を行ってください。

イネーブル シークレット パスワードを回復しているときには、**show startup-config** コマンド出力には表示されません。次の「パスワードのリセットと変更の保存」に記載されている手順を実行して、パスワード回復作業を完了させてください。

パスワードのリセットと変更の保存

パスワードをリセットして、変更を保存するには、次の作業を実行します。

ステップ 1　**configure terminal** コマンドを入力して、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。

```
Router# configure terminal
```

ステップ 2　**enable secret** コマンドを入力して、ルータのイネーブル シークレット パスワードをリセットします。

```
Router(config)# enable secret password
```

ステップ 3　**exit** を入力して、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。

```
Router(config)# exit
```

ステップ 4　設定変更を保存します。

```
Router# copy running-config startup-config
```

コンフィギュレーション レジスタ値のリセット

パスワードの回復または再設定を行った後にコンフィギュレーション レジスタをリセットするには、次の作業を行います。

ステップ 1　**configure terminal** コマンドを入力して、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。

```
Router# configure terminal
```

ステップ 2　**configure register** コマンドと、記録しておいた元のコンフィギュレーション レジスタ値を入力します。

```
Router(config)# config-reg value
```

ステップ 3　**exit** を入力して、コンフィギュレーション モードを終了します。

```
Router(config)# exit
```

（注）　忘れたイネーブル パスワードを回復する前に使用していたコンフィギュレーションに戻るには、コンフィギュレーションの変更を保存せずに、ルータを再起動してください。

ステップ 4　ルータを再起動し、回復したパスワードを入力します。

SDM を使用したルータの管理

Cisco SDM ツールは無料のソフトウェア コンフィギュレーション ユーティリティで、Cisco 860 および Cisco 880 シリーズ アクセス ルータをサポートしています。Cisco SDM は Web ベースの GUI を備えており、次の機能を利用することができます。

- 簡単なセットアップ
- 高度な設定
- ルータ セキュリティ
- ルータ モニタ

PART 5

参考資料（付録）

APPENDIX A

Cisco IOS ソフトウェアの基礎知識

Cisco IOS ソフトウェアの使用方法について理解しておくと、ルータの設定を効率的に行うことができます。この付録では、次の内容で基礎知識について説明します。

すでに Cisco IOS ソフトウェアを理解している場合は、次の章に進んでください。

- 第 3 章「基本的なルータの設定」
- 第 11 章「構成例」

PC からのルータの設定

コンソール ポート経由で接続された PC からルータを設定するには、端末エミュレーション ソフトウェアを使用します。PC はこのソフトウェアを使用して、ルータにコマンドを送信します。表 A-1 に、実行しているオペレーティング システムに応じて使用できる一般的な種類の端末エミュレーション ソフトウェアをいくつか示します。

表 A-1　端末エミュレーション ソフトウェアの種類

PC オペレーティング システム	端末エミュレーション ソフトウェア
Windows 95、Windows 98、Windows 2000、Windows NT、Windows XP	HyperTerm（Windows ソフトウェアに組み込まれています）、ProComm Plus
Windows 3.1	Terminal（Windows ソフトウェアに組み込まれています）
Macintosh	ProComm、VersaTerm

端末エミュレーション ソフトウェアを使用して、PC に接続されているルータの設定を変更できます。PC がルータと対話できるようにするため、ソフトウェアを次の標準 VT-100 エミュレーション設定に合わせて設定してください。

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

この設定は、ご使用のルータのデフォルト設定に一致する必要があります。ルータのボー、データ ビット、パリティ、またはストップ ビットの設定を変更するには、ROM モニタのパラメータを再設定する必要があります。詳細については、付録 C「ROM モニタ」を参照してください。ルータ フロー制御設定を変更するには、グローバル コンフィギュレーション モードで **flowcontrol** コマンドを使用します。

ルータを設定するためにグローバル コンフィギュレーション モードを開始する手順については、この章で後述する「グローバル コンフィギュレーション モードの開始」を参照してください。

コマンド モードの概要

ここでは、Cisco IOS コマンド モードの構造について説明します。コマンド モードは、それぞれ固有の Cisco IOS コマンド群をサポートしています。たとえば、**interface** *type number* コマンドを使用できるのは、グローバル コンフィギュレーション モードだけです。

次に示す Cisco IOS コマンド モードは、階層構造になっています。ルータ セッションを開始した時点では、ユーザ EXEC モードが有効です。

- ユーザ EXEC
- 特権 EXEC
- グローバル コンフィギュレーション

表 A-2 では、このマニュアルで使用されるコマンド モードについて、各モードへのアクセス方法を、各モードのプロンプトについて、モードを終了したり、別のモードを開始したりする方法を説明します。各モードでは、設定するルータの要素がそれぞれ異なるため、モードの切り替えを頻繁に行わなければならない場合があります。特定のモードで使用できるコマンドの一覧を表示するには、プロンプトで疑問符（?）を入力します。各コマンドの詳細（構文も含む）については、Cisco IOS リリース 12.3 のマニュアルを参照してください。

表 A-2　コマンド モードの要約

モード	アクセス方式	プロンプト	モードの終了および開始	モードの説明
ユーザ EXEC	ルータ セッションを開始します。	`Router>`	ルータ セッションを終了するには、**logout** コマンドを入力します。	このモードを使用するのは、次のような場合です。 • 端末の設定値を変更する。 • 基本的なテストを実行する。 • システム情報を表示する。
特権 EXEC	ユーザ EXEC モードから **enable** コマンドを入力します。	`Router#`	• 終了してユーザ EXEC モードに戻るには、**disable** コマンドを入力します。 • グローバル コンフィギュレーション モードを開始するには、**configure** コマンドを入力します。	このモードを使用するのは、次のような場合です。 • ルータの動作パラメータを設定する。 • このマニュアルで説明されている確認手順を実行する。 ルータ コンフィギュレーションに対する不正な変更を防ぐため、「イネーブル シークレット パスワードおよびイネーブル パスワード」の手順（P.A-5）に説明されているようにパスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードから **configure** コマンドを入力します。	`Router (config)#`	• 終了して特権 EXEC モードに戻るには、**exit** コマンドまたは **end** コマンドを入力するか、**Ctrl+Z** キーを押します。 • インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを入力します。	このモードは、ルータにグローバルに適用するパラメータを設定する目的で使用します。 このモードからは次のモードにアクセスできます。 • インターフェイス コンフィギュレーション • ルータ コンフィギュレーション • ライン コンフィギュレーション

表 A-2　コマンド モードの要約 （続き）

モード	アクセス方式	プロンプト	モードの終了および開始	モードの説明
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードから（**interface atm 0** など特定のインターフェイスを指定して）**interface** コマンドを入力します。	`Router (config-if)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** キーを押します。 • サブインターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを使用してサブインターフェイスを指定します。	このモードは、ルータのイーサネット インターフェイスおよびシリアル インターフェイスまたはサブインターフェイスのパラメータを設定する目的で使用します。
ルータ コンフィギュレーション	グローバル コンフィギュレーション モードから、**router** コマンドを入力し、続けて **router rip** などの適切なキーワードを入力します。	`Router (config-router)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** キーを押します。	このモードは、IP ルーティング プロトコルを設定する目的で使用します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードから、**line 0** などの目的のライン番号とオプションのライン タイプを指定して **line** コマンドを入力します。	`Router (config-line)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** キーを押します。	このモードは、端末回線のパラメータを設定する目的で使用します。

ヘルプの利用方法

コマンド入力の補助手段として、疑問符（?）および矢印キーを使用できます。

疑問符を入力すると、そのコマンド モードで使用できるコマンドの一覧が表示されます。

```
Router> ?
access-enable  Create a temporary access-list entry
access-profile Apply user-profile to interface
clear          Reset functions
.
.
.
```

コマンドの先頭の数文字を入力し、続けて（スペースを入れずに）疑問符を入力すると、完全なコマンドが表示されます。

```
Router> sh?
* s=show set show slip systat
```

コマンドを入力し、続けてスペース 1 つと疑問符を入力すると、コマンド変数の一覧が表示されます。

```
Router> show ?
.
.
.
clock      Display the system clock
dialer     Dialer parameters and statistics
exception  exception information
.
.
.
```

上矢印キーを押すと、直前に入力したコマンドが再表示されます。上矢印キーを押し続けると、さらに前に入力したコマンドにさかのぼって、順に表示されます。

イネーブル シークレット パスワードおよびイネーブル パスワード

デフォルトでは、ルータはパスワード保護なしで出荷されます。特権 EXEC コマンドの多くは動作パラメータの設定に使用されるため、これらのコマンドをパスワードで保護して、不正使用を防止する必要があります。

パスワードの設定には、次の 2 つのコマンドを使用します。

- **enable secret** *password*：非常に安全な、暗号化パスワード
- **enable** *password*：やや安全性の低い、暗号化されていないローカル パスワード

enable パスワードおよび **enable secret** パスワードは、各種権限レベル（0 ～ 15）へのアクセスを制御します。**enable** パスワードはローカルで使用することを前提としているため、暗号化されません。**enable secret** パスワードは、ネットワークで使用すること、つまり、ネットワークを超えてパスワードを使用したり、TFTP サーバにパスワードを保管したりする環境での使用を前提としています。**enable secret** パスワードまたは **enable** パスワードは、特権 EXEC モード コマンドが利用できる権限レベル 1 で使用する必要があります。

最大限のセキュリティを確保するには、これらのパスワードを別々のものにする必要があります。セットアップ時に両方のパスワードに同じ文字列を入力すると、ルータはそのパスワードを受け付けますが、異なったパスワードにするように指示する警告メッセージが表示されます。

enable secret パスワードには、1 ～ 25 文字の英数字（大文字および小文字）を指定できます。**enable** パスワードには、任意の文字数で英数字（大文字および小文字）を指定できます。どちらの場合も、先頭の文字に数字を使用できません。パスワードにはスペースも使用できます。たとえば、*two words* は有効なパスワードです。先行スペースは無視されますが、後続スペースは認識されます。

グローバル コンフィギュレーション モードの開始

ルータのコンフィギュレーションを変更するには、グローバル コンフィギュレーション モードを使用する必要があります。ここでは、ルータのコンソール ポートに接続された端末または PC を使用して、グローバル コンフィギュレーション モードを開始する手順について説明します。

グローバル コンフィギュレーション モードを開始する手順は、次のとおりです。

ステップ 1　ルータの起動後に、**enable** コマンドまたは **enable secret** コマンドを入力します。

```
Router> enable
```

ステップ 2　ルータにイネーブル パスワードを設定している場合は、プロンプトに対してそのパスワードを入力します。

イネーブル パスワードは、入力しても画面に表示されません。次に、特権 EXEC モードを開始する例を示します。

```
Password: enable_password
Router#
```

プロンプトにシャープ記号（#）が表示されることにより、特権 EXEC モードが開始されたことがわかります。この時点でルータ コンフィギュレーションの変更を行うことができます。

ステップ 3　**configure terminal** コマンドを入力して、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。

```
Router# configure terminal
Router(config)#
```

この時点でルータ コンフィギュレーションの変更を行うことができます。

コマンドの使用方法

ここでは、Command-line Interface（CLI: コマンドライン インターフェイス）で Cisco IOS コマンドを入力するときに役立つヒントをいくつか紹介します。

コマンドの短縮形

コマンドを入力する際、ルータが一意のコマンドとして認識できる文字数だけを入力すれば十分です。次に、**show version** コマンドを入力する例を示します。

```
Router # sh v
```

コマンドの取り消し

特定の機能を無効にする（入力したコマンドを取り消す）には、ほとんどの場合、該当するコマンドの前にキーワード **no** を入力します（例：**no ip routing**）。

コマンドライン エラー メッセージ

CLI を使用してルータを設定する際に、表示される可能性のあるエラー メッセージを表 A-3 に示します。

表 A-3　一般的な CLI エラー メッセージ

エラー メッセージ	意味	解決方法
`% Ambiguous command: "show con"`	ルータがコマンドとして認識できる十分な文字数を入力していません。	再度コマンドを入力し、続けて疑問符（**?**）を入力します（コマンドと疑問符の間にはスペースは入れません）。 そのコマンドとともに入力できるキーワードが表示されます。
`% Incomplete command.`	このコマンドに必要なすべてのキーワードまたは値を入力していません。	再度コマンドを入力し、続けて疑問符（**?**）を入力します（コマンドと疑問符の間にはスペースは入れません）。 そのコマンドとともに入力できるキーワードが表示されます。
`% Invalid input detected at '^' marker.`	入力したコマンドが不正です。エラーのある位置に、カレット記号（^）が表示されます。	疑問符（**?**）を入力して、このコマンド モードで使用できるコマンドをすべて表示します。

設定変更の保存

コンフィギュレーションの変更内容を Nonvolatile RAM（NVRAM; 不揮発性 RAM）に保存して、システムの再ロード時または停電時に消失しないようにするには、**copy running-config startup-config** コマンドを入力する必要があります。次に、このコマンドを使用して変更を保存する例を示します。

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

デフォルトの保存先ファイル名である **startup-config** をそのまま使用する場合は、*Enter* キーを押すか、または対象の保存先ファイル名を入力して **Enter** キーを押します。

コンフィギュレーションが NVRAM に保存されるまでに、1 ～ 2 分を要する場合があります。コンフィギュレーションが保存されると、次のメッセージが表示されます。

```
Building configuration...
Router#
```

要約

以上、Cisco IOS ソフトウェアの基本事項について学習したため、ルータの設定作業を開始することができます。次の内容を忘れないでください。

- コマンド入力の補助手段として、疑問符（**?**）および矢印キーを使用できます。
- コマンド モードごとに、使用できるコマンドが限られています。コマンドの入力に問題が生じたときは、プロンプトを確認したあと、疑問符（**?**）を入力して、使用できるコマンドの一覧を表示してください。間違ったコマンド モードを使用しているか、構文が不正である可能性があります。
- 特定の機能を無効にするには、該当するコマンドの前にキーワード **no** を入力します（例：**no ip routing**）。
- コンフィギュレーションの変更内容は NVRAM に保存して、システムの再ロード時または停電時に消失しないようにします。

次の作業

ルータを設定するには、第 3 章「基本的なルータの設定」および第 11 章「構成例」を参照してください。

APPENDIX B

概要

この付録では、インターネット サービス プロバイダーまたはネットワーク管理者がシスコ ルータを設定する際に役立つ機能の概要について説明します。一般的なネットワーク構成を再検討するには、第 11 章「構成例」を参照してください。

この付録に記載されている内容は、次のとおりです。

ADSL

ADSL は、データと音声の両方を同一回線を介して伝送するためのテクノロジーです。ADSL のパケットベース ネットワーク テクノロジーを使用すると、Network Service Provider（NSP; ネットワーク サービス プロバイダー）のセントラル オフィスとカスタマー サイト間のローカル ループ（「ラスト マイル」）、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

シリアル回線またはダイヤルアップ回線と比較した ADSL の利点は、常時接続状態になり、ダイヤルアップ回線または専用線に比べて帯域幅が増え、コストが低下することです。ADSL テクノロジーは非対称的であり、カスタマー サイトから NSP のセントラル オフィス方向での帯域幅よりも、セントラル オフィスからカスタマー サイト方向での帯域幅を大きくすることができます。この非対称性と常時

アクセス（コール セットアップが不要）を組み合わせることにより、ADSL はインターネットとイントラネットへのアクセス、ビデオ オン デマンド、およびリモート LAN アクセスに最適な手段になります。

SHDSL

SHDSL は、データと音声の両方を同一回線を介して伝送するための、G.SHDSL（G.991.2）標準に基づくテクノロジーです。SHDSL のパケットベース ネットワーク テクノロジーを使用すると、ネットワーク サービス プロバイダー（NSP）のセントラル オフィスとカスタマー サイト間で、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

G.SHDSL 装置は、セントラル オフィスおよびリモート端末からの到達距離を約 26,000 フィート（7925 m）に拡張することができます（72 kbps ～ 2.3 Mbps の対称的なデータ速度の場合）。また、より低速でリピートすることができるため、到達距離は事実上、無制限になります。

SHDSL テクノロジーは対称的であり、NSP のセントラル オフィスとカスタマー サイト間の両方向の帯域幅を同じにすることができます。この対称性と常時アクセス（コール セットアップが不要）を組み合わせることにより、SHDSL は LAN アクセスに最適な手段になります。

ネットワーク プロトコル

ネットワーク プロトコルを使用すると、送信元から特定の宛先に、LAN または WAN リンクを介してデータを渡すことができます。ネットワーク プロトコルには、ネットワークを介してデータを送信するための最適パスが格納されたルーティング アドレス テーブルが組み込まれています。

IP

インターネットワーク レイヤで最も一般的な Transmission Control Protocol/Internet Protocol（TCP; 伝送制御プロトコル/IP; インターネット プロトコル）は IP です。IP は、すべての TCP/IP ネットワークに基本的なパケット配信サービスを提供します。IP プロトコルは、物理ノード アドレスの他に、IP アドレスと呼ばれる論理ホスト アドレス システムを実装します。IP アドレスは、インターネットワーク以上のレイヤで、装置を特定したり、インターネットワーク ルーティングを実行するために使用されます。Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用すると、IP は指定の IP アドレスと一致する物理アドレスを識別できるようになります。

IP 以外のレイヤ内のすべてのプロトコルでは、データを配信するために IP を使用しています。つまり、最終宛先に関係なく、送受信される TCP/IP データはすべて IP を通過します。

IP はコネクションレス プロトコルであるため、データを伝送する前に、制御情報（*ハンドシェイク*）を交換してエンドツーエンド接続を確立することはありません。対照的に、コネクション型プロトコルはリモート コンピュータと制御情報を交換して、データ受信準備が完了したことを確認してから、データを送信します。ハンドシェイクに成功した場合は、コンピュータによって接続が確立されています。コネクション型サービスが必要な場合、IP は他のレイヤ内のプロトコルによって接続を確立します。

Internetwork Packet Exchange（IPX）は、動的なディスタンス ベクタ ルーティング プロトコルである Routing Information Protocol（RIP）を使用して、ルーティング情報を交換します。RIP については、この後で詳細に説明します。

ルーティング プロトコルのオプション

ルーティング プロトコルには次のものがあります。

- Routing Information Protocol（RIP）
- Enhanced Interior Gateway Routing Protocol（EIGRP）

RIP と EIGRP には、いくつか異なる点があります（表 B-1 を参照）。

表 B-1　RIP と EIGRP の比較

プロトコル	最適なトポロジ	メトリック	ルーティング アップデート
RIP	15 ホップ以内のトポロジに適しています。	ホップ カウント。最大ホップ カウントは 15 です。最良ルートは、ホップ カウントが最小のルートです。	デフォルトで 30 秒間隔。この間隔を変更することもできますし、RIP のトリガ拡張機能を使用することもできます。
EIGRP	宛先までのホップ数が 16 以上の、大規模なトポロジに適しています。	距離情報。後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準にします。	hello パケットが 5 秒間隔で送信されます。さらに、宛先のステートが変化した時点で差分更新が送信されます。

RIP

RIP は IP に関連するプロトコルで、インターネット上のルーティング プロトコル トラフィックとして幅広く使用されます。RIP は、ディスタンス ベクタ ルーティング プロトコルです。つまり、ルート選択のためのメトリックとして距離（ホップ カウント）を使用します。*ホップ カウント*は、パケットが宛先に到達するために経由しなければならないルータ数です。たとえば、あるルートのホップ カウントが 2 である場合、パケットを宛先に送るには 2 台のルータを経由しなければなりません。

デフォルトでは、RIP のルーティング アップデートは 30 秒おきにブロードキャストされます。ルーティング アップデートをブロードキャストする間隔は、ユーザ側で再設定することができます。さらに、RIP のトリガ拡張機能を使用して、ルーティング データベースが更新されたときにだけルーティング アップデートを送信するように設定することもできます。RIP のトリガ拡張機能については、Cisco IOS 12.3 のマニュアルを参照してください。

EIGRP

EIGRP は、シスコ独自仕様による高度なディスタンス ベクタおよびリンク ステート ルーティング プロトコルであり、距離（ホップ カウント）よりも洗練されたメトリックに基づいてルートを選択します。EIGRP は、後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準とするメトリックを使用します。特定の宛先への後継ルータが存在しないにもかかわらず、近接ルータが宛先をアドバタイズしている場合、ルータはルートを再計算しなければなりません。

EIGRP が稼動する各ルータは、5 秒おきに hello パケットを送信して、近接ルータに自らが動作していることを知らせます。所定時間内に hello パケットを送信しないルータがあれば、EIGRP は宛先のステートに変化があったと見なし、差分更新を送信します。

EIGRP は IP をサポートするため、マルチプロトコル ネットワーク環境で 1 つのルーティング プロトコルを使用して、ルーティング テーブルのサイズおよびルーティング情報の量を最小限に抑えることができます。

PPP 認証プロトコル

Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）は、ポイントツーポイント リンクを介して送信されるネットワーク レイヤ プロトコル情報をカプセル化します。

本来、PPP はポイントツーポイント リンクを介して IP トラフィックを転送するためのカプセル化プロトコルとして開発されました。また、IP アドレスの割り当てと管理、非同期（スタート/ストップ）カプセル化とビット型同期カプセル化、ネットワーク プロトコルの多重化、リンク コンフィギュレーション、リンク品質テスト、エラー検出、およびネットワーク レイヤ アドレス ネゴシエーションやデータ圧縮ネゴシエーションなどのオプションのネゴシエーション機能に関する標準も、PPP によって確立されました。上記機能をサポートするために、PPP には拡張可能な Link Control Protocol（LCP）および Network Control Protocol（NCP）ファミリーが備わっており、これらによってオプションの設定パラメータおよびファシリティをネゴシエートします。

PPP の最新の実装では、PPP セッションを認証するためのセキュリティ認証プロトコルが 2 つサポートされています。

- Password Authentication Protocol（PAP）
- Challenge Handshake Authentication Protocol（CHAP）

通常、PPP と PAP または CHAP 認証の組み合わせは、接続されているリモート サイトを中央サイトに通知する場合に使用されます。

PAP

PAP は双方向のハンドシェイクを使用して、ルータ間のパスワードを検証します。PAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。PPP リンクが確立された後、リモート オフィス ルータは、本社オフィス ルータが認証を受け付けるまで、設定されているユーザ名およびパスワードの送信を繰り返します。

PAP の特徴は、次のとおりです。

- 認証のパスワード部分は、リンク上をクリア テキストで送信されます（スクランブル処理または暗号化は行われません）。
- PAP では、プレイバック攻撃または反復的な総当り攻撃からの保護機能が提供されません。
- 認証試行の頻度およびタイミングは、リモート オフィス ルータが制御します。

CHAP

CHAP は 3 ウェイ ハンドシェイクを使用して、パスワードを検証します。CHAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク　トポロジを例にとります。

PPP リンクが確立された後、本社オフィス ルータはリモート オフィス ルータに対し、チャレンジ メッセージを送信します。リモート オフィス ルータは可変の値で応答します。本社オフィス ルータは、独自に計算した値と照らし合わせて、この応答をチェックします。両方の値が一致していれば、本社オフィス ルータは認証を受け付けます。リンクを確立した後は、いつでも認証プロセスを繰り返すことができます。

CHAP の特徴は、次のとおりです。

- 認証プロセスでは、パスワードではなく、可変のチャレンジ値を使用します。
- CHAP は、一意の予測不可能な可変のチャレンジ値の使用により、プレイバック攻撃から保護します。チャレンジの反復により、1 回の攻撃にさらされる時間を限定します。
- 認証試行の頻度およびタイミングは、本社オフィス ルータが制御します。

（注）　2 つのプロトコルのうち、より安全性の高い CHAP の使用を推奨します。

TACACS+

Cisco 860 および Cisco 880 シリーズ ルータは、Telnet を介して Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。TACACS+ は、リモート アクセス認証およびイベント ロギングなどの関連ネットワーク セキュリティ サービスを提供するシスコ独自の認証プロトコルです。ユーザ パスワードは、個々のルータではなく中央のデータベースで管理されます。TACACS+ は、ルータごとに設定された、別個のモジュールである Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）ファシリティもサポートします。

ネットワーク インターフェイス

ここでは、Cisco 860 および Cisco 880 シリーズ ルータがサポートするネットワーク インターフェイス プロトコルについて説明します。サポートされるネットワーク インターフェイス プロトコルは、次のとおりです。

- イーサネット
- ATM（DSL 用）

イーサネット

イーサネットは、Carrier Sense Multiple Access Collision Detect（CSMA/CD; キャリア検知多重アクセス/衝突検知）を使用してデータおよび音声パケットを WAN インターフェイスに送信するベースバンド LAN プロトコルです。この用語は、通常、すべての CSMA/CD LAN を表します。イーサネットは、散発的な、場合によっては大量のトラフィックが発生するネットワーク内で機能するように設計されました。IEEE 802.3 仕様は、本来のイーサネット テクノロジーに基づいて、1980 年に開発されました。

イーサネット CSMA/CD メディアアクセス プロセスでは、CSMA/CD LAN 上のすべてのホストはいつでもネットワークにアクセスできます。データを送信する前に、CSMA/CD ホストはネットワークを通過するトラフィックを待ち受けます。データを送信するホストは、トラフィックが検出されなくなるまで待機してから、データを送信します。イーサネットでは、ネットワーク上をデータが流れていない場合、ネットワーク上のすべてのホストがデータを送信できます。トラフィックを待ち受けていた 2 台のホストがトラフィックを検出せず、同時にデータを送信すると、衝突が発生します。衝突が発生すると両方の送信内容が破壊されるため、ホストは後で再送信する必要があります。衝突したホストがいつ再送信を行うかは、アルゴリズムによって決まります。

ATM（DSL 用）

Asynchronous Transfer Mode（ATM; 非同期転送モード）は、音声、データ、ビデオ、画像など複数のトラフィック タイプをサポートする、高速な多重化およびスイッチング プロトコルです。

ATM は、ネットワークのすべての情報をスイッチングおよび多重化する固定長セルで構成されます。ATM 接続は、単に宛先ルータまたはホストに情報を転送するために使用されます。ATM ネットワークは、帯域幅を幅広く利用できる LAN と考えられます。コネクションレス型である LAN と異なり、ATM を使用してユーザに LAN 環境を提供するには、特定の機能が必要となります。

各 ATM ノードは、ATM ネットワーク内の通信する必要があるすべてのノードに対して、接続を個別に確立する必要があります。このような接続はすべて、Permanent Virtual Circuit（PVC; 相手先固定接続）によって確立されます。

PVC

PVC はリモート ホストとルータ間の接続です。PVC は、ルータが通信する ATM エンド ノードごとに確立されます。PVC の作成時に確立される PVC の特性は、ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化タイプによって設定されます。AAL は、ユーザ情報をセルに変換する方法を定義します。AAL は、送信時に上位レイヤ情報をセルに分割し、受信時にセルを再び組み立てます。

シスコ ルータは AAL5 形式をサポートしています。AAL5 は、AAL3/4 よりもオーバーヘッドが少なく、エラー検出および訂正機能が優れている最新のデータ トランスポート サービスを提供します。AAL5 は通常、Variable Bit Rate（VBR; 可変ビット レート）トラフィックおよび Unspecified Bit Rate（UBR; 未指定ビット レート）トラフィックを対象とします。

ATM カプセル化は、特定のプロトコル ヘッダーによりデータをラップする機能です。接続しているルータのタイプにより、ATM PVC カプセル化タイプが決まります。

ルータがサポートする ATM PVC カプセル化タイプは、次のとおりです。

- LLC/SNAP（RFC 1483）
- VC-MUX（RFC 1483）
- PPP（RFC 2364）

各 PVC は、宛先ノードへの完全な、独立したリンクと見なされます。ユーザは必要に応じて、接続間でデータをカプセル化できます。ATM ネットワークは、データの内容を無視します。必要となるのは、特定の AAL 形式に従って、ルータの ATM サブシステムにデータを送信することだけです。

ダイヤラ インターフェイス

ダイヤラ インターフェイスは、PVC に PPP 機能（認証方法や IP アドレス割り当て方法など）を割り当てます。PPP over ATM を設定する場合に使用します。

ダイヤラ インターフェイスは、すべての物理インターフェイスから独立して設定し、必要に応じて動的に適用することができます。

ダイヤル バックアップ

ダイヤル バックアップを使用すると、ユーザはバックアップ モデム回線接続を設定できるようになるため、WAN のダウンタイムが短縮されます。Cisco IOS ソフトウェアのダイヤル バックアップ機能を起動するために、以下を使用できます。

- バックアップ インターフェイス
- フローティング スタティック ルート
- ダイヤラ ウォッチ

バックアップ インターフェイス

バックアップ インターフェイスは、WAN ダウンタイムなど、自らが起動する特定の環境が発生するまで、アイドル状態にとどまるインターフェイスです。バックアップ インターフェイスとして設定できるのは、Basic Rate Interface（BRI; 基本速度インターフェイス）などの物理インターフェイス、またはダイヤラ プールで使用されるように割り当てられたバックアップ ダイヤラ インターフェイスです。プライマリ回線が起動している場合、バックアップ インターフェイスはスタンバイ モードです。スタンバイ モードのバックアップ インターフェイスは、イネーブルになるまで、事実上のシャットダウン状態です。バックアップ インターフェイスに関連付けられたルートは、ルーティング テーブルに格納されません。

バックアップ インターフェイス コマンドは、インターフェイスが物理的にダウンしていることを識別したルータによって異なるため、通常は、ISDN BRI 接続、非同期回線、および専用線をバックアップするために使用されます。プライマリ回線に障害が発生すると、上記接続に対するインターフェイスがダウンして、バックアップ インターフェイスがこれらの障害をただちに識別します。

フローティング スタティック ルート

フローティング スタティック ルートは、管理距離がダイナミック ルートよりも長いスタティック ルートです。スタティック ルートに管理距離を設定すると、スタティック ルートの優先度をダイナミック ルートよりも小さくすることができます。この方法では、ダイナミック ルートが使用可能な場合、スタティック ルートは使用されません。ただし、ダイナミック ルートが失われると、スタティック ルートが引き継ぎ、この代替ルートを通してトラフィックを送信できます。この代替ルートに Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）インターフェイスが使用されている場合は、DDR インターフェイスをバックアップ インターフェイスとして使用できます。

ダイヤラ ウォッチ

ダイヤラ ウォッチは、ダイヤル バックアップとルーティング機能を統合するバックアップ機能です。ダイヤラ ウォッチを使用すると、中央ルータにおいて発信コールをトリガするトラフィックを定義しなくても、信頼できる接続を確立できます。したがって、ダイヤラ ウォッチは対象トラフィックに関する条件がない正規の DDR と見なすことができます。プライマリ インターフェイスを定義するウォッチ対象ルートを設定することにより、ウォッチ対象ルートの追加および削除にともない、プライマリ インターフェイスのステータスを監視し追跡することができます。

ウォッチ対象ルートを削除すると、ダイヤラ ウォッチはウォッチ中のいずれかの IP アドレスまたはネットワークに対して、有効なルートが少なくとも 1 つ存在するかどうかを確認します。有効なルートが存在しない場合、プライマリ回線はダウンしており、使用不可能であると見なされます。定義済みのウォッチ対象 IP ネットワークの少なくとも 1 つに有効なルートが存在し、このルートがダイヤラ ウォッチに設定されたバックアップ インターフェイス以外のインターフェイスを示している場合、プライマリ リンクは起動していると見なされ、ダイヤラ ウォッチはバックアップ リンクを起動しません。

NAT

Network Address Translation（NAT; ネットワーク アドレス変換）はプライベートにアドレス指定されたネットワークから、インターネットなどの登録済みネットワークにアクセスするためのメカニズムを提供します。サブネット アドレスが登録されている必要はありません。このメカニズムにより、ホスト番号の再設定は不要になり、複数のイントラネットで同じ IP アドレス範囲を使用できます。

NAT は、*内部ネットワーク*（登録されていない IP アドレスを使用するネットワーク）と*外部ネットワーク*（グローバルに一意な IP アドレスを使用するネットワーク [この場合はインターネット]）の境界に配置されたルータに設定されます。NAT は内部ローカル アドレス（内部ネットワークのホストに割り当てられた登録されていない IP アドレス）をグローバルに一意な IP アドレスに変換してから、パケットを外部ネットワークに送信します。

NAT が設定されている場合、内部ネットワークは既存のプライベート アドレスまたは古い形式のアドレスを引き続き使用します。これらのアドレスが有効なアドレスに変換された後、パケットは外部ネットワークに転送されます。変換機能は標準ルーティングと互換性があります。この機能が必要となるのは、内部ネットワークと外部ドメインを接続しているルータだけです。

変換はスタティックにもダイナミックにも行えます。スタティック アドレス変換は、内部ネットワークと外部ドメインの 1 対 1 のマッピングを確立します。ダイナミック アドレス変換は、変換されるローカル アドレスと、外部アドレスの割り当て元となるアドレス プールとを指定することによって、定義されます。割り当ては番号順に行われ、連続するアドレス ブロックからなる複数のプールを定義できます。

NAT を使用すると、外部へのアクセスが必要なすべてのホストにアドレスを再指定する必要がなくなるため、時間が短縮され、コストが削減されます。また、アプリケーション ポートレベルの多重化によって、アドレスも節約されます。NAT が設定されていると、内部ホストはすべての外部通信に対して、1 つの登録済み IP アドレスを共有できます。このタイプの設定では、多数の内部ホストをサポートするために必要な外部アドレスが比較的少なくてすむため、IP アドレスが節約されます。

内部ネットワークのアドレス指定方式は、インターネット内で割り当てられた登録済みアドレスと競合することがあります。したがって、NAT は重複ネットワークごとに個別のアドレス プールを使用して、適切に変換することができます。

Easy IP（フェーズ 1）

Easy IP（フェーズ 1）機能は、ネットワーク アドレス変換と PPP/Internet Protocol Control Protocol（IPCP; インターネット プロトコル コントロール プロトコル）を組み合わせた機能です。この機能を使用すると、シスコ ルータは、独自の登録済み WAN インターフェイス IP アドレスを中央サーバから自動的にネゴシエートし、すべてのリモート ホストがこの単一の登録済みアドレスを使用してインターネットにアクセスできるようにします。Easy IP（フェーズ 1）では、Cisco IOS ソフトウェアに組み込まれた既存のポートレベル多重化 NAT 機能が使用されるため、リモート LAN 上の IP アドレスはインターネットから参照できません。

Easy IP（フェーズ 1）機能は、NAT と PPP/IPCP を組み合わせた機能です。NAT が設定されているルータは、LAN 装置で使用される登録されていない IP アドレスを、ダイヤラ インターフェイスで使用されるグローバルに一意な IP アドレスに変換します。複数の LAN 装置でグローバルに一意な同一 IP アドレスを使用する機能は、*オーバーローディング*といいます。NAT は、内部ネットワーク（登録されていない IP アドレスを使用するネットワーク）と外部ネットワーク（グローバルに一意な IP アドレスを使用するネットワーク [この場合はインターネット]）の境界に配置されたルータに設定されます。

PPP/IPCP が設定されている場合、シスコ ルータは、Internet Service Provider（ISP; インターネット サービス プロバイダー）ルータからダイヤラ インターフェイス用のグローバルに一意な（登録済み）IP アドレスを自動的にネゴシエートします。

Easy IP（フェーズ 2）

Easy IP（フェーズ 2）機能は、Dynamic Host Configuration Protocol（DHCP）サーバとリレーを組み合わせた機能です。DHCP は、IP ネットワーク上の装置（DHCP クライアント）が DHCP サーバ内の設定情報を要求できるようにするためのクライアント/サーバ プロトコルです。DHCP は必要に応じて、中央プールのネットワーク アドレスを割り当てます。DHCP は、一時的にネットワークに接続されるホストに IP アドレスを割り当てる場合や、永久的な IP アドレスが不要なホスト グループ間で、限られた IP アドレス プールを共有する場合に便利です。

DHCP を使用すると、ユーザはクライアントごとに IP アドレスを手動で設定する必要がなくなります。

DHCP では、ルータが DHCP クライアントからの User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ブロードキャスト（IP アドレス要求を含む）を転送するように設定します。DHCP には、自動化を促進しネットワーク管理の問題を減少させるために、次の機能が備わっています。

- 各コンピュータ、プリンタ、および共有ファイル システムの手動設定が不要
- 2 つのクライアントで同じ IP アドレスが同時に使用される状況を防止
- 中央サイトからの設定が可能

QoS

ここでは、Quality of Service（QoS; サービス品質）パラメータについて説明します。具体的な内容は、次のとおりです。

- IP precedence
- PPP フラグメンテーションおよびインターリーブ
- CBWFQ
- RSVP
- 低遅延キューイング（LLQ）

QoS は、ATM、イーサネットおよび IEEE 802.1 ネットワーク、これらの基本テクノロジーの一部またはすべてを使用した IP ルーテッド ネットワークなど、さまざまなテクノロジーを介して、選択されたネットワーク トラフィックに対し、より優れたサービスを提供するためのネットワーク機能です。QoS の主な目的は、専用帯域幅の確保、ジッタおよび遅延の制御（一部のリアルタイム トラフィックおよび対話型トラフィックで必要）、および損失特性の改善です。QoS テクノロジーは、キャンパス、WAN、およびサービス プロバイダー ネットワークの今後のビジネス用途に対応するための基本的な構成単位を提供します。

音声ネットワークのパフォーマンスを高めるには、VoIP が稼動しているルータだけでなく、ネットワーク全体に QoS を設定する必要があります。すべての QoS 技術が、あらゆるネットワーク ルータに適しているとは限りません。ネットワーク内のエッジ ルータとバックボーン ルータは、必ずしも同じ動作をするわけではありません。同様に、実行する QoS の作業もそれぞれ異なる場合があります。リアルタイム音声トラフィックに対応するように IP ネットワークを設定するには、ネットワーク内のエッジ ルータとバックボーン ルータの両方の機能を検討する必要があります。

QoS ソフトウェアを使用すると、複雑なネットワークにおいて、さまざまなネットワーク アプリケーションおよびトラフィック タイプを制御し、予測どおりに処理することができます。ほとんどすべてのネットワークは、小規模企業ネットワーク、インターネット サービス プロバイダー、エンタープライズ ネットワークのいずれであるかに関係なく、QoS を利用して効率を最適化できます。

IP precedence

IP precedence を使用すると、最大 6 つのサービス クラスにトラフィックを分類できます（他の 2 つのクラスは、内部ネットワーク用に予約されています）。ネットワークに適用されたキューイング テクノロジーは、この信号を使用して処理を促進することができます。

ポリシーベース ルーティングや Committed Access Rate（CAR; 専用アクセス レート）などの機能を使用すると、拡張アクセスリスト分類に基づいて優先順位を設定できます。これにより、アプリケーションまたはユーザ別、宛先および送信元サブネット別など、優先順位をきわめて柔軟に割り当てることができます。通常、この機能は可能な限りネットワーク（または管理ドメイン）のエッジ付近に配備されるため、これ以降のネットワーク要素は決定されたポリシーに基づいてサービスを提供できます。

オプションの信号方式を使用している場合は、ホストまたはネットワーク クライアントに IP precedence を設定することもできます。IP precedence を使用すると、既存ネットワーク キューイング メカニズム（Class-Based Weighted Fair Queuing [CBWFQ; クラス ベース WFQ] など）を使用して、サービス クラスを確立できます。既存アプリケーションの変更の必要性や複雑なネットワーク要件はありません。

PPP フラグメンテーションおよびインターリーブ

マルチクラス マルチリンク PPP インターリーブにより、大きいパケットをマルチリンクでカプセル化し、リアルタイム音声トラフィックの遅延条件を満たす小さいパケットに分割することができます。もともと小さいリアルタイム パケットは、マルチリンクでカプセル化されず、大きいパケットのフラグメントの合間に伝送されます。インターリーブ機能はさらに、小型で遅延に敏感なパケット用に特殊な送信キューを提供するので、そのようなパケットを他のフローより先に送信できます。インターリーブ機能は、他のベスト エフォート型トラフィックに使用される低速リンク上で、遅延に敏感な音声パケットに遅延限度を設定します。

マルチリンク PPP インターリーブは、通常、CBWFQ および RSVP または IP precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、マルチリンク PPP インターリーブおよび CBWFQ を使用します。音声パケットにプライオリティを設定する場合は、Resource Reservation Protocol（RSVP; リソース予約プロトコル）または IP precedence を使用します。

CBWFQ

通常、CBWFQ はマルチリンク PPP インターリーブおよび RSVP または IP precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、CBWFQ とマルチリンク PPP を組み合わせて使用します。音声パケットにプライオリティを設定する場合は、RSVP または IP precedence を使用します。

ATM キューと Cisco IOS キューの 2 つのキューイング レベルがあります。CBWFQ は Cisco IOS キューに適用されます。PVC が作成されると、First-in first-out（FIFO; 先入れ先出し）Cisco IOS キューが自動的に作成されます。CBWFQ を使用してクラスを作成し、それらを PVC に関連付けると、クラスごとにキューが作成されます。

CBWFQ により、キューに十分な帯域幅が確保され、トラフィックは予測どおりのサービスを受けます。小容量トラフィック ストリームが優先されます。大容量トラフィック ストリームに残りの容量が分配され、同等または比例配分された帯域幅が与えられます。

RSVP

RSVP を使用すると、ルータはインターフェイス上に十分な帯域幅を確保して、信頼性および品質性能を高めることができます。RSVP により、エンド システムはネットワークに特定の QoS を要求できます。リアルタイム音声トラフィックには、ネットワークの一貫性が不可欠です。一貫した QoS が得られなかった場合、リアルタイム トラフィックにジッタ、帯域幅不足、遅延変動、または情報損失が生じる可能性があります。RSVP は、最新のキューイング メカニズムと連動します。予約がどのように実行されるかは、インターフェイス キューイング メカニズム（CBWFQ など）に依存します。

RSVP は、PPP、HDLC、および同様なシリアル回線インターフェイス上で適切に動作します。マルチアクセス LAN 上では、適切に動作しません。RSVP は、パケット フローに関するダイナミック アクセス リストと同様のものと考えることができます。

ネットワークに次の条件が存在する場合は、RSVP を設定して QoS を保証する必要があります。

- 小規模な音声ネットワークの実装
- 2 Mbps 未満のリンク
- 使用率の高いリンク
- 可能なかぎり最良の音質を必要とする場合

低遅延キューイング（LLQ）

Low Latency Queuing（LLQ; 低遅延キューイング）は、リアルタイム トラフィック用の低遅延完全優先送信キューを提供します。完全優先キューを使用すると、（他のキュー内のパケットがキューから取り出される前に）最初に遅延に敏感なデータをキューから取り出して送信することにより、遅延に敏感なデータを他のトラフィックよりも優先的に処理することができます。

アクセス リスト

基本的な標準アクセス リストおよびスタティック拡張アクセス リストを使用すると、**permit** コマンドにキーワードを指定して、セッション フィルタリングと同様の処理を行うことができます。指定されたキーワードは、ACK または RST ビットが設定されているかどうかに基づいて、TCP パケットをフィルタリングします （ACK または RST ビットが設定されているパケットはセッション内の最初のパケットではないため、このパケットは確立されたセッションに属します）。このフィルタ基準は、インターフェイスに永久的に適用されるアクセス リストの一部になります。

APPENDIX C

ROM モニタ

ROM モニタ ファームウェアは、ルータの電源投入時またはリセット時に実行され、プロセッサ ハードウェアの初期設定およびオペレーティング システム ソフトウェアの起動を補助します。ROM モニタを使用すると、忘れたパスワードの回復、コンソール ポートを介したソフトウェアのダウンロードなど、特定の設定作業を実行することができます。ルータに Cisco IOS ソフトウェア イメージがロードされていない場合、ルータは ROM モニタによって稼動されます。

この付録の内容は、次のとおりです。

ROM モニタの起動

ROM モニタを使用するには、コンソール ポートを介してルータに接続された端末または PC を使用する必要があります。

次の再起動時に、ROM モニタ モードで起動するようにルータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードを開始します。 プロンプトが表示された場合は、パスワードを入力します。
ステップ 2	**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 3	**config-reg 0x0**	コンフィギュレーション レジスタをリセットします。

	コマンド	目的
ステップ 4	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**reload**	新しいコンフィギュレーション レジスタ値を使用して、ルータを再起動します。ルータでは引き続き ROM モニタが稼動します。Cisco IOS ソフトウェアは起動されません。 設定値が 0x0 の場合は、コンソールから手動でオペレーティング システムを起動する必要があります。この付録のコマンドの説明の **boot** コマンドを参照してください。 ルータを再起動すると、ROM モニタ モードになります。新しい行ごとに、プロンプトの数字は増加します。

ワンポイント アドバイス　ルータを再起動してから 60 秒間は、コンフィギュレーション レジスタで Break（システム割り込み）がオフに設定されていても、Break が常に有効となります。再起動から 60 秒間のあいだに Break キーを押すと、ROM モニタのプロンプトに割り込むことができます。

ROM モニタ コマンド

ROM モニタ プロンプトに **?** または **help** を入力すると、ROM モニタに、次のように、使用できるコマンドとオプションのリストが表示されます。

```
rommon 1 > ?
alias              set and display aliases command
boot               boot up an external process
break              set/show/clear the breakpoint
confreg            configuration register utility
cont               continue executing a downloaded image
context            display the context of a loaded image
cookie             display contents of cookie PROM in hex
copy               Copy a file-copy [-b <buffer_size>] <src_file> <dst_file>
delete             Delete file(s)-delete <filenames ...>
dir                List files in directories-dir <directory>
dis                display instruction stream
dnld               serial download a program module
format             Format a filesystem-format <filessystem>
frame              print out a selected stack frame
fsck               Check filesystem consistency-fsck <filesystem>
help               monitor builtin command help
history            monitor command history
meminfo            main memory information
mkdir              Create dir(s)-mkdir <dirnames ...>
more               Concatenate (type) file(s)-cat <filenames ...>
rename             Rename a file-rename <old_name> <new_name>
repeat             repeat a monitor command
reset              system reset
rmdir              Remove a directory
set                display the monitor variables
stack              produce a stack trace
sync               write monitor environment to NVRAM
sysret             print out info from last system return
tftpdnld           tftp image download
unalias            unset an alias
unset              unset a monitor variable
xmodem             x/ymodem image download
```

コマンドは、大文字と小文字が区別されます。端末の Break キーを押すことにより、コマンドを中止することができます。PC 上で一般的な端末エミュレーション プログラムを使用している場合は、Ctrl キーと Break キーを同時に押すと、コマンドが中止します。別のタイプの端末エミュレータまたは端末エミュレーション ソフトウェアを使用している場合は、製品のマニュアルに記載された Break コマンドの送信方法を参照してください。

コマンドの説明

表 C-1 に、最も一般的な ROM モニタ コマンドを示します。

表 C-1　一般的な ROM モニタ コマンド

コマンド	説明
help または **?**	使用可能なすべての ROM モニタ コマンドの概要を表示します。

-?	次のような、コマンド構文に関する情報を表示します。
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	
	このコマンドの出力は、**xmodem** ダウンロード コマンドの出力とわずかに異なります。
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

reset または **i**	電源投入時のように、ルータをリセットして、初期化します。

dir *device***:**	指定したデバイス（フラッシュ メモリ ファイルなど）上のファイルがリストされます。
	`rommon 4 > dir flash:`
	`Directory of flash:/`
	`2 -rwx 10283208 <date> c880-advsecurityk9-mz`
	`9064448 bytes available (10289152 bytes used)`

boot コマンド	ROM モニタの boot コマンドを詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Guide*』を参照してください。
b	フラッシュ メモリ内の最初のイメージをブートします。
b flash: [*filename*]	フラッシュ メモリの最初のパーティションからイメージを直接ブートします。ファイル名を入力しないと、フラッシュ メモリ内の最初のイメージがブートされます。

TFTP ダウンロードによる障害の回復

ルータに新しいソフトウェアをロードするには、通常、Cisco IOS ソフトウェアの Command-Line Interface（CLI; コマンドライン インターフェイス）から **copy tftp flash** 特権 EXEC コマンドを実行します。ただし、ルータが Cisco IOS ソフトウェアをブートできない場合は、ROM モニタ モード中に新しいソフトウェアをロードすることができます。

ここでは、リモート TFTP サーバからルータのフラッシュ メモリに Cisco IOS ソフトウェア イメージをロードする方法について説明します。**tftpdnld** コマンドを実行すると、ルータに新しいソフトウェア イメージをダウンロードする前にフラッシュ メモリ内のすべての既存データが消去されるため、このコマンドは障害回復の場合にだけ使用してください。

TFTP ダウンロード コマンドの変数

ここでは、ROM モニタ モードで設定できるシステム変数、および TFTP ダウンロード プロセス中に使用されるシステム変数について説明します。必須変数とオプション変数があります。

（注）　ここに記載されたコマンドは大文字と小文字の区別があり、表記どおり正確に入力する必要があります。

必須変数

tftpdnld コマンドを使用する前に、次のコマンドを使用して、次に示す変数を設定する必要があります。

変数	コマンド
ルータの IP アドレス	**IP_ADDRESS=** ***ip_address***
ルータのサブネット マスク	**IP_SUBNET_MASK=** *ip_address*
ルータのデフォルト ゲートウェイの IP アドレス	**DEFAULT_GATEWAY=** *ip_address*
ソフトウェアのダウンロード元となる TFTP サーバの IP アドレス	**TFTP_SERVER=** *ip_address*
ルータにダウンロードするファイル名	**TFTP_FILE=** *filename*

オプション変数

tftpdnld コマンドを使用する前に、次のコマンドを使用して、次に示す変数を設定します。

変数	コマンド
ファイル ダウンロードの進行状況の表示方法を設定します。 0：進行状況は表示されません。 1：ファイル ダウンロードが進行中であることを示す感嘆符（!!!）が表示されます。これがデフォルトの設定です。 2：ファイル ダウンロード プロセス中に、次のような詳細な進行状況が表示されます。 • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received.MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*
ルータが ARP および TFTP ダウンロードを試行する回数です。デフォルトの設定は 7 です。	**TFTP_RETRY_COUNT=** *retry_times*
ダウンロード プロセスがタイムアウトするまでの時間（秒）です。デフォルト値は 2,400 秒（40 分）です。	**TFTP_TIMEOUT=** *time*
ルータがダウンロードイメージにチェックサム テストを実行するかどうかを指定します。 1：チェックサム テストを実行します。 0：チェックサム テストを実行しません。	**TFTP_CHECKSUM=***setting*

TFTP ダウンロード コマンドの使用

TFTP を使用してファイルをダウンロードするには、ROM モニタ モードで次の手順を実行します。

ステップ 1　適切なコマンドを使用して、上記のすべての必須変数およびオプション変数を入力します。

ステップ 2　次のように、**tftpdnld** コマンドを入力します。

```
rommon 1 > tftpdnld -r
```

（注）　**-r** 変数はオプションです。この変数を入力すると、新しいソフトウェアがダウンロードされ、ブートされますが、ソフトウェアはフラッシュ メモリに保存されません。次回に **reload** を入力した場合は、フラッシュ メモリ内のイメージを使用することができます。

次のような出力が表示されます。

```
IP_ADDRESS: 10.3.6.7
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 10.3.0.1
TFTP_SERVER: 192.168.254.254
TFTP_FILE: c880-advsecurityk9-mz
Do you wish to continue? y/n:  [n]:
```

ステップ 3　継続する場合は、出力内の質問に対して **y** を入力します。

```
Do you wish to continue? y/n:  [n]:y
```

ルータは新しいファイルのダウンロードを開始します。

誤って y を入力した場合、**Ctrl+C** または **Break** を入力するとフラッシュ メモリを消去する前に転送を止めることができます。

コンフィギュレーション レジスタ

仮想コンフィギュレーション レジスタは Nonvolatile RAM（NVRAM; 不揮発性 RAM）内にあり、他のシスコ製ルータと同じ機能を持ちます。仮想コンフィギュレーション レジスタの設定は、ROM モニタまたはオペレーティングシステム ソフトウェアから表示したり、変更することができます。ROM モニタ内でコンフィギュレーション レジスタを変更するには、レジスタ値を 16 進形式で入力するか、ROM モニタ プロンプトを使用して各ビットを設定します。

コンフィギュレーション レジスタの手動変更

ROM モニタから仮想コンフィギュレーション レジスタを手動で変更するには、**confreg** コマンドを入力し、続けて新しいレジスタ値を 16 進数で入力します（次の例を参照）。

```
rommon 1 > confreg 0x2101


You must reset or power cycle for new config to take effect
rommon 2 >
```

指定値は、常に 16 進数として解釈されます。新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットするか再起動しない限り有効になりません。

プロンプトを使用したコンフィギュレーション レジスタの変更

引数を指定しないで **confreg** コマンドを入力すると、仮想コンフィギュレーション レジスタの内容が表示され、各ビットの意味と、設定を変更するかどうかを問い合せるプロンプトが表示されます。

いずれの場合も、新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットするか再起動しない限り有効になりません。

次に、**confreg** コマンドの入力例を示します。

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

コンソール ダウンロード

ROM モニタ機能の 1 つであるコンソール ダウンロードを使用すると、ルータ コンソール ポートを介して、ソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードすることができます。ダウンロードされたファイルは、ミニフラッシュ メモリ モジュールまたはメイン メモリに保存されて実行されます（イメージ ファイルの場合だけ）。

TFTP サーバにアクセスできない場合は、コンソール ダウンロードを使用してください。

（注） コンソール ポートを介してソフトウェア イメージまたはコンフィギュレーション ファイルをルータにダウンロードする場合は、ROM モニタの **dnld** コマンドを使用する必要があります。

（注）　PC を使用して、ルータ コンソール ポートを介して 115,200 bps の速度で Cisco IOS イメージをダウンロードする場合は、PC のシリアル ポートに 16550 Universal Asynchronous Transmitter/Receiver（UART）が使用されていることを確認してください。PC のシリアル ポートに 16550 UART が使用されていない場合は、コンソール ポートを介して Cisco IOS イメージをダウンロードするときに、38,400 bps 以下の速度を使用することを推奨します。

コマンドの説明

xmodem コンソール ダウンロード コマンドの構文および説明を、次に示します。

xmodem [-cyrx] *destination_file_name*

c	（任意）パケット検証に CRC-16 エラー チェックを使用して、ダウンロードを実行します。デフォルトは 8 ビット CRC です。
y	（任意）Ymodem プロトコルを使用してダウンロードを実行するように、ルータに指示します。デフォルトは Xmodem プロトコルです。これらのプロトコルは、次の点が異なります。 • Xmodem は 128 ブロック転送サイズをサポートします。Ymodem は 1024 ブロック転送サイズをサポートします。 • Ymodem は、各パケットの検証に CRC-16 エラー チェックを使用します。ソフトウェアのダウンロード元装置によって、Xmodem がこの機能に対応するかどうかが決まります。
r	（任意）イメージは DRAM にロードされ、実行されます。デフォルトでは、イメージはフラッシュ メモリにロードされます。
x	（任意）イメージは DRAM にロードされますが、実行されません。
destination_file_name	システム イメージ ファイルまたはシステム コンフィギュレーション ファイルの名前です。ルータにコンフィギュレーション ファイル名を認識させるには、ファイル名を *router_confg* にする必要があります。

次の手順に従って、Xmodem を実行します。

ステップ 1　Xmodem を実行するローカル ドライブに、イメージ ファイルを移動します。

ステップ 2　**xmodem** コマンドを入力します。

エラー レポート

ROM モニタのコンソール ダウンロードは、コンソールを使用してデータ転送を行うため、データ転送中にエラーが発生した場合、エラー メッセージがコンソール上に表示されるのはデータ転送が終了してからです。

ボーレートがデフォルト レートから変更されている場合は、エラー メッセージの後に、コンフィギュレーション レジスタで指定されたボーレートに端末を戻すように伝えるメッセージが表示されます。

debug コマンド

ROM モニタ デバッグ コマンドを使用するのは、通常、Cisco IOS ソフトウェアがクラッシュしたり、中断された場合だけです。デバッグ コマンドの入力時に Cisco IOS クラッシュ情報が得られない場合は、次のエラーメッセージが表示されます。

```
"xxx: kernel context state is invalid, can not proceed."
```

ROM モニタ デバッグ コマンドは次のとおりです。

- **stack** または **k**：スタック トレースが生成されます。次に例を示します。

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**：プロセッサのコンテキストが表示されます。次に例を示します。

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**：個々のスタック フレームが表示されます。
- **sysret**：最後に起動したシステム イメージからの戻り情報が表示されます。この情報には、イメージの停止理由、8 フレームまでのスタックダンプ、例外が生じている場合の例外発生アドレスが含まれています。次に例を示します。

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**：メイン メモリのサイズ（バイト）、開始アドレス、および使用可能範囲、パケット メモリの開始ポイントとサイズ、NVRAM のサイズが表示されます。次に例を示します

```
rommon 9> meminfo
Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
IO (packet) memory size: 5 percent of main memory.
NVRAM size: 32KB
```

ROM モニタの終了

ルータの起動時または再ロード時に Cisco IOS イメージをフラッシュ メモリから起動させるには、コンフィギュレーション レジスタ値を 0x2 ～ 0xF に設定する必要があります。

次に、コンフィギュレーション レジスタをリセットして、ルータがフラッシュ メモリに格納された Cisco IOS イメージを起動するように設定する例を示します。

```
rommon 1 > confreg 0x2101
```

新しい設定を有効にするには、リセットまたは電源のオフ/オンを行う必要があります。

```
rommon 2 > boot
```

ルータは、フラッシュ メモリ内の Cisco IOS イメージを起動します。次回にルータをリセットするか、またはいったん電源を切ってから再投入すると、コンフィギュレーション レジスタは 0x2101 に変更されます。

APPENDIX D

共通ポート割り当て

表 D-1 に、現在割り当てられている Transmission Control Protocol（TCP; 伝送制御プロトコル）ポート番号を示します。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）でも、可能な限り同じ番号が使用されています。

表 D-1　　現在割り当てられている TCP および UDP ポート番号

ポート	キーワード	説明
0	—	予約済み
1 ～ 4	—	割り当てなし
5	RJE	リモート ジョブ入力
7	ECHO	エコー
9	DISCARD	廃棄
11	USERS	アクティブ ユーザ
13	DAYTIME	デイタイム
15	NETSTAT	Who is up または NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	Character generator
20	FTP-DATA	ファイル転送プロトコル（データ）
21	FTP	ファイル転送プロトコル
23	TELNET	端末接続
25	SMTP	Simple Mail Transport Protocol
37	TIME	時間
39	RLP	Resource Location Protocol
42	NAMESERVER	ホストネーム サーバ
43	NICNAME	Who is
49	LOGIN	Login Host Protocol
53	DOMAIN	ドメイン ネーム サーバ
67	BOOTPS	ブートストラップ プロトコル サーバ
68	BOOTPC	ブートストラップ プロトコル クライアント

表 D-1　現在割り当てられている TCP および UDP ポート番号 （続き）

ポート	キーワード	説明
69	TFTP	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）
75	—	任意のプライベート ダイアルアウト サービス
77	—	任意のプライベート RJE サービス
79	FINGER	Finger
95	SUPDUP	SUPDUP プロトコル
101	HOST NAME	Network Interface Card（NIC; ネットワーク インターフェイス カード）ホスト ネーム サーバ
102	ISO-TSAP	ISO-Transport Service Access Point（TSAP）
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	Sun Microsystems のリモート プロシージャ コール
113	AUTH	認証サービス
117	UUCP-PATH	UNIX-to-UNIX Copy Protocol（UUCP; UNIX 間コピー プログラム）パス サービス
119	NNTP	Usenet Network News Transfer Protocol
123	NTP	ネットワーク タイム プロトコル
126	SNMP	簡易ネットワーク管理プロトコル
137	NETBIOS-NS	NetBIOS ネーム サービス
138	NETBIOS-DGM	NetBIOS データグラム サービス
139	NETBIOS-SSN	NetBIOS セッション サービス
161	SNMP	簡易ネットワーク管理プロトコル
162	SNMP-TRAP	簡易ネットワーク管理プロトコル トラップ
512	rexec	UNIX のリモート実行（制御）
513	TCP：rlogin UDP：rwho	TCP：UNIX リモート ログイン UDP：UNIX ブロードキャスト ネーム サービス
514	TCP：rsh UDP：syslog	TCP：UNIX リモート シェル UDP：システム ログ
515	Printer	UNIX ライン プリンタ リモート スプーリング
520	RIP	Routing Information Protocol
525	Timed	タイム サーバ