Cisco 860、Cisco 880 および Cisco 890 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

OL-18906-06-J

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

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

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

Cisco 860、Cisco 880 および Cisco 890 シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

CONTENTS

はじめに

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

目的

このマニュアルでは、Cisco 860、Cisco 880、および Cisco 890 シリーズ サービス統合型ルータ（ISR）の概要と、さまざまな機能を設定する方法について説明します。ご使用のルータ モデルに適用されない情報が記載されている場合もあります。

保証、サービス、サポート情報については、ルータに付属する『*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

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

マニュアルの構成

このマニュアルは、次の部、章、付録で構成されています。

概要 / はじめに	
「製品概要」	ルータのモデルと使用可能なソフトウェア機能の概要を説明します。
「ワイヤレス デバイス概要」	ルータ上のワイヤレス デバイスの概要と、ネットワーク構成の中でのその用途の概要を説明します。
「ルータの基本設定」	ルータの基本的なパラメータを設定するための手順を説明します。
ルータの設定	
「バックアップ データ回線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。
「無線デバイスの管理」	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。
イーサネットおよび DSL アクセス用のルータの設定	
「PPP over Ethernet と NAT の設定」	Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。
「PPP over ATM と NAT の設定」	Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。
「DHCP および VLAN による LAN の設定」	各ルータは Dynamic Host Configuration Protocol（DHCP）を使用して、このようなネットワーク上にある各ノードに対して、IP 設定の自動割り当てをイネーブルにできます。
「Easy VPN および IPSec トンネルを使用した VPN の設定」	Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できるバーチャル プライベート ネットワーク（VPN）の作成の概要について説明します。

その他の情報	
「展開シナリオ」	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伝送制御プロトコル（TCP）ポート番号を示します。

表記法

これらのマニュアルでは、手順や情報を示すために、表 1 の表記法を使用しています。

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引数。
[　]	角カッコで囲んで表示される省略可能なキーワードまたは引数。
{**x** | **y** | **z**}	必須キーワードの選択肢は波カッコで囲み、縦棒で区切って示しています。いずれか 1 つを選択しなければなりません。
`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。
<　>	イタリック体が使用できない場合、パスワードのように出力されない文字は、山カッコで囲んで示しています。
[　]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

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

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

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 および Cisco 890 シリーズ ISR ソフトウェア コンフィギュレーション ガイド*』（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, Cisco 880, and Cisco 890 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*』
- 『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』
- 『*Cisco IOS Release Notes* for Cisco IOS Release 12.4(15)XZ』

必要に応じて、以下のマニュアルもご参照ください。

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

製品に関する資料の検索方法

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

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

マニュアルの入手方法およびテクニカル サポート

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

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

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

CHAPTER 1

製品概要

この章では、Cisco 860、Cisco 880、および Cisco 890 シリーズ サービス統合型ルータ（ISR）で利用できる機能の概要について説明します。この章の内容は次のとおりです。

全般的な機能

Cisco 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

ここでは、次の項目について説明します。

Cisco 860 シリーズ ISR の機能

Cisco 860 シリーズ ISR は、10/100 ファスト イーサネット（FE）または ADSL2 over POTS WAN 接続のいずれかを提供する固定構成データ ルータです。

次の機能は、すべての Cisco 860 シリーズ ISR でサポートされます。

- 「802.11n ワイヤレス LAN オプション」（P.1-2）

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 860VAE シリーズ ISR の機能

ここでは、Cisco 860VAE シリーズ ISR の機能について説明します。

- 「一般的な機能」（P.1-2）
- 「インターフェイス」（P.1-3）
- 「IOS イメージ」（P.1-4）

一般的な機能

表 1-1 では、Cisco 860VAE シリーズ ルータの一般的な機能について説明します。

表 1-1　Cisco 860VAE シリーズ ISR の一般的な機能

機能	利点
パフォーマンスの向上	• パフォーマンスは、セキュア、同時データ、音声、ビデオ、およびワイヤレスの各サービスの実行中に、ブロードバンド ネットワークの速度を使用できるようにします。
セキュア ルータを使用したセキュリティおよび QoS	• 10 個のトンネルを使用した IPSec および Easy VPN • BGP • MAC フィルタリングおよびポート セキュリティ • LLQ および WFQ を含む QoS 機能 • NBAR および DiffServ
最新技術の xDSL	• 最新の ADSL2+/VDSL2 規格を含む最新技術の xDSL 機能 • 改善された相互運用性と WW SP で展開されるさまざまな DSLAM

表 1-1　Cisco 860VAE シリーズ ISR の一般的な機能 （続き）

機能	利点
ScanSafe Web フィルタリング	• 望ましくない Web コンテンツからネットワークとスタッフを保護 • 娯楽サーフィンに費やされる時間の制限によって生産性を向上 • 帯域幅の輻輳を減少してネットワーク リソースを最適化 • 包括的なレポートを使用したオンライン アクティビティのモニタリング
IPv6 のサポート	• 最新の IP アドレッシング規格をサポート
WAN ダイバーシティ	• GE + DSL マルチ モード VDSL2 と ADSL 1、2、および 2+ • 同じボックス内の複数の WAN オプションを使用した、さまざまな展開の一貫した設定
4 ポート 10/100 Mbps の管理対象スイッチ セキュア ルータ用の GE ポート × 1	• ネットワーク エッジとしてポートを指定する機能により、在宅勤務者の自宅またはスモール オフィス内で複数のデバイスを接続。 • VLAN は、ネットワーク リソースのセキュアな分割を実現します。
CON/AUX ポート	• 1 つのデュアルパーパス ポートが、管理またはバックアップのアクセス ポイントにコンソールまたは外部モデムへの直接接続を提供
リアルタイム クロック	• 組み込みリアルタイム クロックが、ロギングおよびデジタル証明書などの正確なタイムスタンプを必要とするアプリケーションの正確な日時を維持

インターフェイス

表 1-2 では、Cisco 860VAE シリーズ ルータのインターフェイスについて説明します。

表 1-2　Cisco 860VAE シリーズ ISR のインターフェイス

インターフェイス	モデル			
	866VAE	867VAE	866VAE-K9	867VAE-K9
4 つの FE[1] スイッチ ポート	x	x	x	x
1 つの GE[2] スイッチ ポート	—	—	x	x
1 つの GE WAN ポート	x	x	x	x
1 つの VDSL/ADSL over POTS ポート	—	x	—	x
1 つの VDSL/ADSL over ISDN ポート	x	—	x	—

1. FE = Fast Ethernet（ファスト イーサネット）
2. GE = Gigabit Ethernet（ギガビット イーサネット）

（注）　Cisco 866VAE、867VAE、866VAE-K9 および 867VAE-K9 ルータにはそれぞれ 2 つの WAN ポートがあります。2 ポートの 1 つだけがいつでもアクティブにできます。

IOS イメージ

表 1-3 では、Cisco 860VAE シリーズ ルータに含まれる IOS イメージについて説明します。

表 1-3　Cisco 860VAE シリーズ ISR の IOS イメージ

IOS イメージ	モデル			
	866VAE	867VAE	866VAE-K9	867VAE-K9
c860vae-ipbasek9-mz	x	x	—	—
c860vae-advsecurityk9-mz	—	—	x	x
c860vae-advsecurityk9_npe-mz	—	—	x	x

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.1-4）
- 「共通機能」（P.1-6）
- 「音声機能」（P.1-7）

Cisco 880 シリーズ ISR のモデル

Cisco 880 シリーズ ISR は、データと音声に対応しています。各ルータには WAN ポートが 1 つあります。また、音声をサポートするルータには Foreign Exchange Station（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。すべてのモデルで、802.11b/g/n オプションが利用できます。

表 1-4 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 1-4　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	—	—
881-V	FE	—	—
881G および 881GW	FE	—	x
886 および 886W	ADSL2oPOTS	x	—

表 1-4　Cisco 880 シリーズ データ ISR のポート構成 （続き）

モデル	WAN ポート	バックアップ	
		データ ISDN	データ 3G
886G および 886GW	ADSL2oPOTS	—	x
887 および 887W	ADSL2oPOTS	x	—
887G および 887GW	ADSL2oPOTS	—	x
887-VA-V	VDSL2oPOTS	x	x
887V および 887VW	VDSL2oPOTS	x	—
887VG および 887VGW	VDSL2oPOTS	—	x
888 および 888W	G.SHDSL	x	—
888G および 888GW	G.SHDSL	—	x
888E および 888EW	EFM over G.SHDSL	x	—
C888EA-K9	マルチモード	x	—

表 1-5 に、Cisco 880 シリーズ音声ルータのポート構成を示します。

表 1-5　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 C888SRSTW	G.SHDSL	4	—	x
C888ESRST および C888ERSTW	EFM over G.SHDSL	4	—	4

表 1-6 に、Cisco 881-V、Cisco887VA-V および Cisco 887VA-V-W ルータのポート構成を示します。

表 1-6　Cisco 880 シリーズ データおよび音声 ISR のポート構成

モデル	WAN ポート	FXS 音声ポート	PSTN BRI	WLAN	バックアップ	
					PSTN FXO	データ（ISDN）
C881-V	FE	4	2	—	1	—
C887VA-V	VDSL2/ADSL2	4	2	—	—	x
C887VA-V-W	VDSL2/ADSL2	4	2	x	—	x

Cisco 887 VA-V および Cisco 881-V ルータにより、FXS または BRI 音声ポート（Cisco 881-V ルータは、バックアップ FX0 ポートもサポートします）を使用できる柔軟性が提供されますが、ルータがサポートする同時コール数はコーデックの複雑度設定によって制限されます。コーデックの複雑度設定が高複雑度に対して行われている場合、ルータがサポートするコール数が少なくなります。表 1-7 は、各コーデックの複雑度設定に対してルータでサポートされる同時コールの数を表します。セキュア コールをサポートするためにコーデックの複雑度を設定しても、次の番号に影響しません。

表 1-7　サポートされる同時コール数

	柔軟な複雑度	中複雑度	高複雑度
C881-V	9	8	6
C887VA-V	8	8	6
C887VA-V-W	8	8	6

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.1-6）
- 「802.11n ワイヤレス LAN オプション」（P.1-6）
- 「リアルタイム クロック」（P.1-6）
- 「セキュリティ機能」（P.1-6）

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、無線 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

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）
- ファイアウォール
- URL フィルタリング

音声機能

Cisco 880 音声およびデータ プラットフォーム（C880SRST、C880SRSTW、C881-V、C887 VA-V、および C887VA-V-W）では、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
- C880SRST および C880SRSTW の WAN 障害時は、PSTN に接続された Foreign Exchange Office（FXO）または BRI バックアップ ポートへの SRST フェールオーバーをサポート
- SRST と CME のサポートは、ユーザ ライセンスが必要（C881-V、C887VA-V および C887VA-V-W ルータでは 5 ユーザ ライセンスだけがサポートされます）
- 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。これらのルータには、ギガ ビット イーサネット WAN ポートおよびデータ バックアップ ポートがあります。

表 1-8 に、Cisco 890 シリーズ ISR のポート構成を示します。

表 1-8　Cisco 890 シリーズ ISR のポート構成

		データ バックアップ		
モデル	**WAN ポート**	**FE**	**V.92**	**ISDN**
891 および 891W	GE	x	x	—
892 および 892W	GE	x	—	x
892F および 892F-W	GE[1] または SFP[2]	x	—	x

1. GE 銅ポート
2. SFP ポートはファイバを使用した GE をサポートします。サポートされる SFP の全リストについては、Cisco.com の Cisco 892F ISR データ シートを参照してください。

サポートされる機能は次のとおりです。

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に、4 つのポートで PoE を提供するアップグレードを使用できます。

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

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）
- 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、ライセンスされたソフトウェアが付属しています。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、『*Software Activation On Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

新しいルータを注文する際、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。

（注）　Cisco 860VAE にライセンスは必要ではありません。

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 プラットフォームのソフトウェア ライセンスで使用できる機能の一覧については、『*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 ライセンスをアクティブにして管理する方法の詳細については、『*Cisco IOS Software Activation Tasks and Commands*』を参照してください。

CHAPTER 2

ワイヤレス デバイス概要

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

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

ソフトウェア モード

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

各モードの詳細は次のとおりです。

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

  このネットワーク アーキテクチャの設計の詳細については、Cisco.com の『*Why Migrate to a Cisco Unified Wireless Network?*』を参照してください。

管理オプション

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

- Cisco IOS ソフトウェア CLI
- Simple Network Management Protocol（SNMP）
- Web ブラウザ インターフェイス

（注）　CLI および Web ブラウザ ツールを同時に使用しないでください。CLI を使用してワイヤレス デバイスを設定すると、Web ブラウザ インターフェイスではコンフィギュレーションを正しく表示できない場合があります。

無線デバイスを無線コンフィギュレーション モードにするには、グローバル コンフィギュレーション モードから **interface dot11radio** コマンドを使用します。

ネットワークの構成例

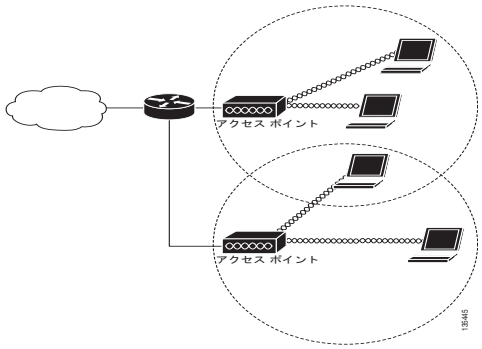
次の一般的なワイヤレス ネットワーク構成のいずれかでアクセス ポイント ロールを設定します。デフォルトでは、アクセス ポイントは、ワイヤード LAN に接続したルート ユニットとして、または完全なワイヤレス ネットワーク内のセントラル ユニットとして構成されます。アクセス ポイントはブリッジまたはワークグループのブリッジとしても構成できます。これらの役割には特定の構成が必要になります。次の各ページで例を挙げて説明します。

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

ルート アクセス ポイント

有線 LAN に直接接続されるアクセス ポイントは、無線ユーザへの接続ポイントとして機能します。LAN に複数のアクセス ポイントが接続されている場合、ユーザはネットワークへの接続を維持したまま、構内のエリアをローミングできます。1 つのアクセス ポイントの範囲外に移動したユーザは、自動的に別のアクセス ポイントを経由してネットワークに接続（アソシエート）されます。ローミング プロセスはシームレスで、ユーザには意識されません。図 2-1 は、有線 LAN 上でルート ユニットとして機能するアクセス ポイントを示しています。

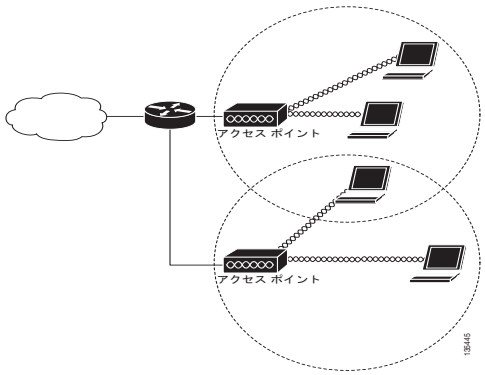
図 2-1　有線 LAN 上でルート ユニットとして機能するアクセス ポイント



全ワイヤレス ネットワークの中央ユニット

完全なワイヤレス ネットワークでは、アクセス ポイントはスタンドアロンのルート ユニットとして機能します。アクセス ポイントは有線 LAN には接続されません。全ステーションをまとめてリンクするハブとして機能します。アクセス ポイントは通信の中心として機能し、無線ユーザの通信範囲を拡張します。図 2-2 は、完全なワイヤレス ネットワークでのアクセス ポイントを示しています。

図 2-2　完全なワイヤレス ネットワークでセントラル ユニットとして機能するアクセス ポイント



CHAPTER 3

ルータの基本設定

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

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

この章では、該当するものがある場合には設定例と確認手順が記載されています。

グローバル コンフィギュレーション モードにアクセスする方法の詳細については、「グローバル コンフィギュレーション モードの開始」（P.A-6）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　Cisco ルータでサポートされているインターフェイスと対応するポート ラベル

ルータ	インターフェイス	ポート ラベル
LAN ポート		
Cisco 860、Cisco 880、および Cisco 890 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 866VAE、867VAE	イーサネット LAN	LAN、FE0-FE3
Cisco 866VAE-K9、867VAE-K9	イーサネット LAN	LAN、GE0、FE0-FE3
WAN ポート		
Cisco 861、861W、881、881W、881G、881GW、881-V	ファスト イーサネット WAN	WAN、FE4
Cisco 867、867W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 886、886W、886G、886GW	ADSL2oISDN WAN	ADSLoPOTS
Cisco 887、887W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 887V、Cisco 887VW、887VG、887VGW	VDSL2oPOTS WAN	VDSLoPOTS
Cisco 867VA、887VA、887VA-M、887VA-V、887VA-V-W	VDSL/ADSLoPOTS WAN	VDSL/ADSLoPOTS
Cisco 888、888W	G.SHDSL WAN	G.SHDSL
Cisco 891、892	ファスト イーサネット WAN	FE8
	ギガビット イーサネット WAN	WAN GE 0
Cisco 866VAE、867VAE	ギガビット イーサネット WAN	WAN GE0
Cisco 866VAE-K9、867VAE-K9	ギガビット イーサネット WAN	WAN GE1
Cisco 866VAE、866VAE-K9	VDSL/ADSLoISDN WAN	VDSL/ADSL OVER ISDN
Cisco 867VAE、867VAE-K9	VDSL/ADSLoPOTS WAN	VDSL/ADSL OVER POTS

デフォルト コンフィギュレーション

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

```
Router# show running-config


User Access Verification

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

Current configuration : 986 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$g4y5$NxDeM.0hON6YA51bcfGvN1
enable password ciscocisco
!
no aaa new-model
!
!
!
!
no ip routing
no ip cef
!
!
!
!
!
multilink bundle-name authe
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface FastEthernet0
!
interface FastEthernet1
 shutdown
```

```
!
interface FastEthernet2
 shutdown
!
interface FastEthernet3
 shutdown
!
interface FastEthernet4
 ip address 10.1.1.1 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface wlan-ap0
 description Service Module interface to manage the embedded AP
 ip unnumbered Vlan1
 no cdp enable
 arp timeout 0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 password cisco
 login
 transport input telnet ssh
!
scheduler max-task-time 5000

!
webvpn cef
end

Router#
```

設定に必要な情報

ネットワークを設定する前に、使用するネットワーク構成に基づいて、次の情報を収集します。

- インターネット接続を設定する場合、次の情報を収集してください。
  - ユーザのログイン名として割り当てられた PPP クライアント名

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

    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。

適切な情報を収集したら、「コマンドライン アクセスの設定」（P.3-5）のタスクからルータの完全な設定を行います。

作業内容に応じて、次のマニュアルを参照します。

- 音声機器を接続する場合は、『*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は、『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

コマンドライン アクセスの設定

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **例：** `Router(config)# line console 0` `Router(config-line)#`	回線コンフィギュレーション モードを開始します。続いて、回線のタイプを指定します。 この例では、アクセス用にコンソール端末を指定します。
ステップ 2	**password** *password* **例：** `Router(config)# password 5dr4Hepw3` `Router(config-line)#`	コンソール端末回線に固有のパスワードを指定します。
ステップ 3	**login** **例：** `Router(config-line)# login`	端末セッション ログイン時のパスワード チェックをイネーブルにします。
ステップ 4	**exec-timeout** *minutes* [*seconds*] **例：** `Router(config-line)# exec-timeout 5 30`	ユーザ入力が検出されるまで EXEC コマンド インタープリタが待機する間隔を設定します。デフォルトは 10 分です。任意で、間隔値に秒数を追加します。 この例では、5 分 30 秒のタイムアウトを表示します。「0 0」のタイムアウトを入力すると、タイムアウトが発生しません。
ステップ 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **例：** `Router(config-line)# line vty 0 4`	リモート コンソール アクセス用の仮想端末を指定します。
ステップ 6	**password** *password* **例：** `Router(config-line)# password aldf2ad1`	仮想端末回線に固有のパスワードを指定します。

	コマンド	目的
ステップ 7	**login** **例：** `Router(config-line)# login`	仮想端末セッション ログイン時のパスワード チェックをイネーブルにします。
ステップ 8	**end** **例：** `Router(config-line)# end` `Router#`	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

例

次の設定は、コマンドライン アクセス コマンドを示します。

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

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

グローバル パラメータの設定

ルータに選択したグローバル パラメータを設定するには、次の作業を行います。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# 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（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`	ルータ名を指定します。
ステップ 3	**enable secret** *password* **例：** `Router(config)# enable secret cr1ny5ho`	ルータへの不正なアクセスを防止するには、暗号化パスワードを指定します。
ステップ 4	**no ip domain-lookup** **例：** `Router(config)# no ip domain-lookup`	ルータが未知の単語（入力ミス）を IP アドレスに変換しないようにします。

WAN インターフェイスの設定

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

- 「ファスト イーサネット WAN インターフェイスの設定」（P.3-9）
- 「メディア タイプの設定」（P.3-10）
- 「ギガビット イーサネット WAN インターフェイスの設定」（P.3-10）
- 「V.92 モデム インターフェイスの設定」（P.3-11）
- 「VDSL2 WAN インターフェイスの設定」（P.3-12）
- 「Cisco 860VAE および 880VA マルチモード ISR の ADSL または VDSL の設定」（P.3-14）
- 「シームレス レート適応の設定」（P.3-16）
- 「UBR+ の設定」（P.3-16）
- 「ADSL モードの設定」（P.3-17）
- 「VDSL モードの設定」（P.3-24）
- 「CLI を使用したトレーニング ログの設定」（P.3-35）
- 「ATM モードでの G.SHDSL WAN インターフェイスの設定」（P.3-37）
- 「EFM モードでの G.SHDSL WAN インターフェイスの設定」（P.3-41）
- 「セル ワイヤレス WAN インターフェイスの設定」（P.3-41）
- 「Cisco 860VAE ISR での WAN モードの設定」（P.3-53）

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。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface fastethernet 4`	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`	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`	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。

（注）　Cisco IOS Release 15.1 (3) T では、インターフェイスモードに **batch** コマンドが導入されました。パケットがより効率的なキャッシュ使用率でバッチで処理されるため、インターフェイスのバッチがイネーブルの場合、CPU 使用率の低下を確認できます。

メディア タイプの設定

Cisco 892F ISR でギガビット イーサネット インターフェイスを設定する前に、まず SFP または RJ-45 としてメディア タイプを選択する必要があります。

メディア タイプを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **media-type** {**sfp** | **rj45**}
3. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface gigabitethernet 0`	ルータのギガビット 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	**media-type** {**sfp**	**rj45**} **例：** `Router(config-if)# media-type sfp` または `Router(config-if)# media-type rj45`	SFP の物理接続を指定します。 または RJ-45 の物理接続を指定します。
ステップ 3	**exit** **例：** `Router(config-if)# exit` `Router(config)#`	ギガビット 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 モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

ギガビット イーサネット WAN インターフェイスの設定

Cisco 891、892、または 860VAE ISR のギガビット イーサネット（GE）WAN 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 モードで次の手順を行います。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface gigabitethernet 1` `Router(config-if)#`	ルータのギガビット 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`	指定したギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 3	**no shutdown** **例：** `Router(config-if)# no shutdown`	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)#`	ギガビット 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 モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

V.92 モデム インターフェイスの設定

Cisco 891 ISR には、V.92 モデムバックアップ インターフェイスがあります。この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 モードで次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **encapsulation** *ppp*
4. **dialer in-band**
5. **dialer string** *dial-string*
6. **dialer-group** *group-number*
7. **async mode dedicated**
8. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface async 1`	ルータの V.92 WAN インターフェイス（シリアル 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`	指定された V.92 インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 3	**encapsulation** *ppp* **例：** `Router(config-if)# encapsulation ppp`	シリアル インターフェイスのポイントツーポイント プロトコル（PPP）に対するカプセル化方式を設定します。
ステップ 4	**dialer in-band** **例：** `Router(config-if)# dialer in-band`	ダイヤルオンデマンド ルーティング（DDR）をサポートするように指定します。
ステップ 5	**dialer string** *dial-string* **例：** `Router(config-if)# dialer string 102`	インターフェイスからコールを発信するときに使用する文字列（電話番号）を指定します。
ステップ 6	**dialer-group** *group-number* **例：** `Router(config-if)# dialer-group 1`	インターフェイスを、指定したダイヤル アクセス グループに属するように設定します。
ステップ 7	**async mode dedicated** **例：** `Router(config-if)# async mode dedicated`	シリアル ライン インターネット プロトコル（SLIP）または PPP カプセル化を使用して、専用非同期モードに回線を配置します。
ステップ 8	**exit** **例：** `Router(config-if)# exit` `Router(config)#`	V.92 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、グローバル コンフィギュレーション モードに戻ります。

VDSL2 WAN インターフェイスの設定

Cisco 887V ISR プラットフォームでは、VDSL2 WAN インターフェイスが使用されます。VDSL2 WAN インターフェイスは、レイヤ 2 転送メカニズムとしてイーサネットを使用することに注意してください。

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

手順の概要

1. **controller** *vdsl 0*
2. **interface** *type number*
3. **ip address** *ip-address mask*
4. **shutdown**
5. **no shutdown**
6. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**controller** *vdsl 0* **例：** `Router(config)# controller vdsl 0`	コントローラのコンフィギュレーション モードを開始し、コントローラ番号を入力します。 **（注）** CPE 側から VDSL2 パラメータを設定する必要はありません。DSLAM 側で特定の VDSL2 設定を実施する必要があります。
ステップ 2	**interface** *type number* **例：** `Router(config)# interface ethernet 0`	ルータ上の VDSL WAN インターフェイスを通してイーサネット レイヤ 2 転送のコンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	インターフェイスに IP アドレスとサブネット マスクを設定します。
ステップ 4	**shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをディセーブルにします。状態が管理アップから管理ダウンに変化します。
ステップ 5	**no shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。状態が管理ダウンから管理アップに変化します。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

Cisco 860VAE および 880VA マルチモード ISR の ADSL または VDSL の設定

ここでは、次の項目について説明します。

Cisco 860VAE、886VA、および 887VA マルチモード ISR の概要

シスコの加入者宅内機器（CPE）である Cisco 866VAE、867VAE、866VAE-K9、867VAE-K9、886VA および 887VA サービス統合型ルータ（ISR）は、非対称デジタル加入者線（ADSL）1/2/2+、およびマルチモードと呼ばれる超高速デジタル加入者線 2（VDSL2）転送モードをサポートします。

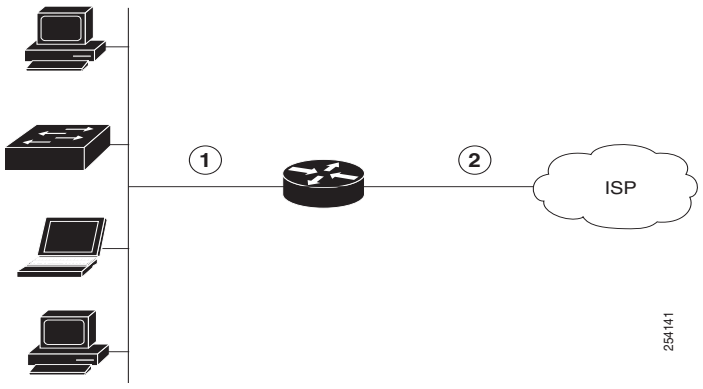
（注）　866VAE および 886VA は、ISDN 経由の xDSL をサポートします。867VAE および 887VA は、従来のアナログ電話回線（POTS）経由の xDSL をサポートします。

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

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

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

図 3-1　トポロジの例



1	ファスト イーサネット LAN インターフェイス または ギガビット イーサネット LAN インターフェイス	2	ATM WAN インターフェイス：ADSL 1/2/2+ モード または イーサネット WAN インターフェイス：VDSL2 モード

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

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

（注）　Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ISR には、最大 2 つの PVC を設定できます。

Over POTS VDSL2/ADSL マルチモード Annex A SKU での ADSL2/2+ Annex M モード

Annex M は、ダウンストリーム周波数範囲から 32 の追加トーンを「借りる」ことで、アップストリーム帯域幅を 2 倍にする G.992.3 規格の拡張です。この機能は、サービス プロバイダーが、最大 2 Mbps のデータレートで ADSL2 および ADSL2+ サービスの対称データレートを提供できるようにします。

Cisco IOS Release 15.2(1)T では、Cisco 887VA プラットフォームで Annex A データ構造を、Cisco 887VA-M プラットフォームで Annex M データ構造をイネーブルにするサポートが追加されます。この機能を使用することで、Annex A と Annex M の両方の構造を同じプラットフォームで実行できます。ただし、デバイスに対して最適化されていない Annex のパフォーマンス トレードオフが存在します。この機能の実装によって、Annex A のプラットフォームでサポートされるモードは Annex M のプラットフォーム（887VA-M および EHWIC-1DSL-VA-M）でサポートされるモードと同じです。デジタル加入者線アクセス マルチプレクサ（DSLAM）が Annex M をサポートしている場合、Annex M モードは、Annex A モードよりも優先されます。

（注）　Cisco 867VAE と 867VAE-K9 では、Cisco IOS Release 15.1(4)M2 または 15.2(2)T 以降がこの機能を使用する必要があります。

Annex A プラットフォームでの Annex M データ構造の設定については、「Over POTS VDSL2/ADSL マルチモード Annex A SKU の ADSL2/2+ Annex M モードのイネーブル化」（P.3-30）を参照してください。

シームレス レート適応の設定

ADSL 接続は、クロストーク、ノイズ マージンの変化、温度変化、または干渉などの複数の理由によってドロップされる場合があります。ADSL2 は、データ レートをリアルタイムに適応することで、こうした問題に対処しています。シームレス レート適応（SRA）により、ADSL2 システムはサービスの中断またはビット エラーなしで、動作中に接続のデータ レートを変更できます。

（注）　これらの機能は、866VAE、867VAE、866VAE-K9、および 867VAE-K9 では使用できません。

SRA の設定については、「シームレス レート適応のイネーブル化」（P.3-31）を参照してください。

UBR+ の設定

UBR は、通常、ファイル転送や電子メールなどのデータ通信アプリケーションに対して使用されます。UBR はベスト エフォート サービスであり、階層の最下位レイヤのサービス クラスです。許可されている実際の帯域幅は保証されません。したがって、UBR 仮想回線（VC）は、セルが送信元から宛先に移動する場合に発生する、多数のセル ドロップまたは大きなセル転送遅延による影響を受けます。UBR は、セル遅延変動許容値（CDVT）の限度を持たない単なるベスト エフォート サービスです。

UBR+ はシスコが開発した特別な ATM サービス クラスです。UBR は、ピーク セル レート（PCR）だけを定義します。ただし、UBR+ は最低保証セル レート（MCR）および（スイッチでの）セル遅延変動許容値（CDVT）を定義します。

（注）　Cisco IOS バージョン 15.2(1)T 以降では、UBR+ は Cisco マルチモード 886VA および 887VA ルータと互換性があります。

（注）　これらの機能は、866VAE、867VAE、866VAE-K9、および 867VAE-K9 では使用できません。

UBR+ の設定の詳細については、「UBR+ の設定」（P.3-33）を参照してください。

ADSL モードの設定

設定作業

ADSL モードを設定するには、次の作業を行います。

- 「ADSL auto モードの設定」（P.3-17）
- 「ADSL モードの CPE およびピアの設定」（P.3-18）
- 「ADSL 設定の確認」（P.3-22）
- 「ADSL の CPE からピアへの接続の確認」（P.3-24）

ADSL auto モードの設定

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

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

手順の概要

1. **enable**
2. **configure terminal**
3. **controller vdsl** *slot*
4. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | {ansi |etsi}}**

（注）　ANSI オプションは、POTS をサポートするモデルにのみ使用できます。ETSI オプションは、ISDN をサポートするモデルにのみ使用できます。

5. **end**

手順の詳細

	コマンド	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトにパスワードを入力します。
ステップ 2	**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 3	**controller vdsl** *slot* **例：** `Router(config)# controller vdsl 0`	VDSL コントローラのコンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	**operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansi}** **例：** `Router(config-controller)# operating mode auto`	動作モードを設定します。デフォルトは auto で、これが推奨されるモードです。 **（注）** auto で設定した場合、**show running** コマンドでは動作モードが表示されません。
ステップ 5	**end** **例：** `Router(config-controller)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。 **（注）** Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 で adsl または vdsl にモードを変更した場合はリロードが必要です。

ADSL モードの CPE およびピアの設定

ADSL を設定するときは、ATM メイン インターフェイスまたは ATM サブインターフェイスを PVC および IP アドレスを使用して設定する必要があり、必要な場合、インターフェイスで **no shutdown** コマンドを実行します。

手順の概要

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

手順の詳細

ATM CPE 側の設定

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

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface atm0` `Router(config-if)#`	ATM WAN インターフェイス（ATM0）で、コンフィギュレーション モードを開始します。
ステップ 2	**no shutdown** **例：** `Router(config-if)# no shutdown` `Router(config-if)#`	ATM インターフェイスに対する設定変更をイネーブルにします。
ステップ 3	**interface atm0.1 point-to-point** **例：** `Router(config-if)# interface ATM0.1 point-to-point` `Router(config-subif)#`	ATM0.1 ポイントツーポイント インターフェイスをイネーブルにします。
ステップ 4	**ip address** *ip-address mask* **例：** `Router(config-subif)# ip address 30.0.0.1 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 5	**pvc [name] vpi/vci** **例：** `Router(config-subif)# pvc 13/32` `Router(config-if-atm-vc)#`	ATM PVC に名前を割り当てるかまたは名前を作成し、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 6	**protocol** *protocol* {*protocol-address* **[virtual-template] | inarp} [[no] broadcast | disable-check-subnet | [no] enable-check-subnet]** **例：** `Router(config-if-atm-vc)# protocol ip 30.0.0.2 broadcast`	ATM PVC のスタティック マップを設定します。
ステップ 7	**end** **例：** `Router(config-if-atm-vc)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。

ATM ピア側の設定

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

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface atm0`	ATM WAN インターフェイス（ATM0）で、コンフィギュレーション モードを開始します。
ステップ 2	**no shutdown** **例：** `Router(config-if)# no shutdown`	ATM インターフェイスに対する設定変更をイネーブルにします。
ステップ 3	**interface atm0.1 point-to-point** **例：** `Router(config-if)# interface ATM0.1 point-to-point`	ATM0.1 ポイントツーポイント インターフェイスをイネーブルにします。
ステップ 4	**ip address** *ip-address mask* **例：** `Router(config-subif)# ip address 30.0.0.2 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 5	**pvc [name] vpi/vci** **例：** `Router(config-subif)# pvc 13/32`	ATM PVC に名前を割り当てるかまたは名前を作成し、ATM 仮想回線コンフィギュレーション モードを開始します。
ステップ 6	**protocol** *protocol {protocol-address* **[virtual-template] | inarp} [[no] broadcast | disable-check-subnet | [no] enable-check-subnet]** **例：** `Router(config-if-atm-vc)# protocol ip 30.0.0.1 broadcast`	ATM PVC のスタティック マップを設定します。
ステップ 7	**end** **例：** `Router(config-if-atm-vc)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。

ADSL の設定例

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

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


Current configuration : 1250 bytes
!
```

```
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 15/32
  protocol ip 30.0.0.2 broadcast
!
!
```

```
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

ADSL 設定の確認

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

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


Daemon Status:           Up


                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x6110
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x6110
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    FHK1313227E 887-V2-K 15.1(20100
Serial Number Far:
Modem Version Near:    15.1(20100426:193435) [changahn
Modem Version Far:     0x6110

Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.992.5 (ADSL2+) Annex A
```

```
TC Mode:                 ATM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Trellis:                 ON                      ON
Line Attenuation:         1.0 dB                  1.4 dB
Signal Attenuation:       1.0 dB                  0.0 dB
Noise Margin:             6.8 dB                 13.6 dB
Attainable Rate:        25036 kbits/s           1253 kbits/s
Actual Power:            13.7 dBm               12.3 dBm
Total FECS:             0                       0
Total ES:               0                       0
Total SES:              0                       0
Total LOSS:             0                       0
Total UAS:              0                       0
Total LPRS:             0                       0
Total LOFS:             0                       0
Total LOLS:             0                       0
Bit swap:               163                     7

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


Firmware        Source          File Name (version)
--------        ------          -------------------
VDSL            embedded        VDSL_LINUX_DEV_01212008 (1)


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


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


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

ADSL の CPE からピアへの接続の確認

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

```
Router# ping 30.0.0.2 rep 20

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

VDSL モードの設定

設定作業

VDSL モードを設定するには、次の作業を行います。

- 「VDSL auto モードの設定」（P.3-24）
- 「VDSL モードの CPE およびピアの設定」（P.3-25）
- 「VDSL 設定の確認」（P.3-28）
- 「VDSL の CPE からピアへの接続の確認」（P.3-30）

VDSL auto モードの設定

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

（注）　ルータを設定する前に VDSL2 モードで DSLAM を設定します。

手順の概要

1. **controller vdsl** *slot*
2. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | {ansi |etsi}}**

   （注）　ANSI オプションは、POTS をサポートするモデルにのみ使用できます。ETSI オプションは、ISDN をサポートするモデルにのみ使用できます。

3. **end**

手順の詳細

	コマンド	目的
ステップ 1	**controller vdsl** *slot* **例：** `Router(config)# controller vdsl 0`	VDSL コントローラのコンフィギュレーション モードを開始します。
ステップ 2	**operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansi}** **例：** `Router(config-controller)# operating mode auto`	動作モードを設定します。デフォルトは auto で、これが推奨されるモードです。 **（注）** auto で設定した場合、**show running** コマンドでは動作モードが表示されません。
ステップ 3	**end** **例：** `Router(config-controller)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。 **（注）** Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 でモードを変更した場合は、リロードが必要です。

VDSL モードの CPE およびピアの設定

VDSL を設定する場合は ethernet 0 インターフェイスを設定し、必要に応じて **no shutdown** コマンドを実行します。グローバル コンフィギュレーション モードで開始します。

VDSL CPE 側の設定

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface ethernet0`	イーサネット インターフェイス 0 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 90.0.0.1 255.255.255.0`	IP アドレスとサブネット マスクを入力します。
ステップ 3	**no shutdown** **例** `Router(config-if)# no shutdown`	IP アドレスとサブネット マスクに対して設定変更をイネーブルにします。
ステップ 4	**end** **例** `Router(config-if)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。

VDSL ピア側の設定

VDSL ピア側を設定するには、グローバル コンフィギュレーション モードで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 ethernet0`	イーサネット インターフェイス 0 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 90.0.0.2 255.255.255.0`	IP アドレスとサブネット マスクを設定します。
ステップ 3	**no shutdown** **例** `Router(config-if)# no shutdown`	IP アドレスとサブネット マスクに対して設定変更をイネーブルにします。
ステップ 4	**end** **例** `Router(config-if)# end` `Router#`	コンフィギュレーション モードを終了し、EXEC モードを開始します。

VDSL の設定例

次に、VDSL の設定の一般的な出力例を示します。**太字**で表示された箇所が重要です。

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


Current configuration : 1250 bytes
!
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level advipservices
!
!
vtp domain cisco
vtp mode transparent
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet0
 ip address 30.0.0.1 255.255.255.0
 no fair-queue
!
interface BRI
 no ip address
 encapsulation hdlc
 shutdown
 isdn termination multidrop
!
```

```
interface ATM0
 no ip address
 shutdown
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

VDSL 設定の確認

特権 EXEC モードから **show controller vdsl 0** コマンドを使用して、設定が正しく行われていることを確認します。**太字**で表示された箇所が重要です。

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


Daemon Status:           Up


                       XTU-R (DS)              XTU-C (US)

Chip Vendor ID:        'BDCM'                   'BDCM'
Chip Vendor Specific:  0x0000                   0x0000
Chip Vendor Country:   0xB500                   0xB500
Modem Vendor ID:       'CSCO'                   'BDCM'
Modem Vendor Specific: 0x4602                   0x0000
Modem Vendor Country:  0xB500                   0xB500
Serial Number Near:    FHK1313227E 887-V2-K 15.1(20100
Serial Number Far:
Modem Version Near:    15.1(20100426:193435) [changahn
```

```
Modem Version Far:     0x0000


Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.993.2 (VDSL2) Profile 12a
TC Mode:                 PTM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Trellis:                 ON                      OFF
Line Attenuation:         1.0 dB                  0.0 dB
Signal Attenuation:       1.0 dB                  0.0 dB
Noise Margin:            12.0 dB                  9.5 dB
Attainable Rate:        87908 kbits/s           50891 kbits/s
Actual Power:            13.5 dBm                 8.9 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   0.9     2.3     N/A     7.2     2.9     7.0     N/A
Signal Attenuation(dB): 0.9     2.3     N/A     N/A     2.3     6.6     N/A
Noise Margin(dB):       14.5    9.3     N/A     N/A     N/A     N/A     N/A
Total FECS:             0                        0
Total ES:               0                        0
Total SES:              0                        0
Total LOSS:             0                        0
Total UAS:              0                        0
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0
Bit swap:               1                        0


Full inits:             33
Failed full inits:      0
Short inits:            0
Failed short inits:     0


Firmware        Source          File Name (version)
--------        ------          -------------------
VDSL            embedded        VDSL_LINUX_DEV_01212008 (1)


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


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):               0           84999             0             48968
Previous Speed:             0           24184             0              1047
Reed-Solomon EC:            0               0             0                 0
CRC Errors:                 0               0             0                 0
Header Errors:              0               0             0                 0
Interleave (ms):         0.00            6.00          0.00              0.00
Actual INP:              0.00            0.00          0.00              0.00


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


Router#
```

VDSL の CPE からピアへの接続の確認

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

```
Router# ping 30.0.0.2 rep 20

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

Over POTS VDSL2/ADSL マルチモード Annex A SKU の ADSL2/2+ Annex M モードのイネーブル化

Over POTS VDSL2/ADSL マルチ モード Annex A SKU で ADSL2/2+ Annex M モードをイネーブルにするには、次の手順を実行します。

（注） この機能には、Cisco IOS Release 15.2(1)T 以降が必要になります。

（注） Cisco 867VAE と 867VAE-K9 では、Cisco IOS Release 15.1(4)M2 または 15.2(2)T 以降がこの機能を使用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **controller vdsl** *0*
4. **operating mode {adsl1** | **adsl2 [***annex a* | *annex m***]** | **adsl2+ [***annex a* | *annex m***]**| **ansi** | **auto**| **vdsl2 }**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトにパスワードを入力します。
ステップ 2	**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。

	コマンドまたはアクション	目的
ステップ 3	**controller vdsl** *0*	VDSL コントローラのコンフィギュレーション モードを開始します。
ステップ 4	**operating mode {adsl1** | **adsl2 [***annex a* | *annex m***]** | **adsl2+ [***annex a* | *annex m***]** | **ansi** | **auto| vdsl2}** **例：** `Router(config-controller)# operating mode adsl2+ annex m`	**asdl1**：ITU G.992.1 Annex A のフルレート モードでの動作を設定します。 **adsl2**：ADSL2 動作モード（ITU G.992.3 Annex A、Annex L、Annex M）での動作を設定します。Annex 動作モードが選択されていない場合は、Annex A、Annex L、Annex M がイネーブルになります。最終的なモードは、DSL アクセス マルチプレクサ（DSLAM）でのネゴシエーションによって決まります。 **adsl2+**：ADSL2+ モード（ITU G.992.5 Annex A および AnnexM）での動作を設定します。Annex A 動作モードが選択されていない場合は、Annex と Annex M の両方がイネーブルになります。最終的なモードは、DSLAM とのネゴシエーションによって決まります。 **ansi**：ANSI フルレート モード（ANSI T1.413）でルータが動作するように設定します。 **auto**：デフォルト設定。DSLAM が、「使用上のガイドライン」に記載されている順序で自動的に DSL 動作モードを選択するようにルータを設定します。サポートされているすべてのモードがイネーブルになります。 **vdsl2**：ITU G.993.2 モードでの動作を設定します。 *annex a, m*：（任意）annex オプションが指定されていない場合、Annex A と Annex M の両方がイネーブルになります。最終的なモードは、デジタル加入者線アクセス マルチプレクサ（DSLAM）とのネゴシエーションによって決まります。

シームレス レート適応のイネーブル化

SRA をイネーブルにするには、次の手順を実行します。

（注） SRA モードはデフォルトでディセーブルです。

（注） SRA には Cisco IOS Release 15.2(1)T 以降が必要です。

（注） これらの機能は、現在のところ Cisco 866VAE、867VAE、866VAE-K9、または 867VAE-K9 では使用できません。

手順の概要

SRA は次の手順でイネーブルおよびディセーブルにできます。

1. **enable**
2. **configure terminal**
3. **controller vdsl** *x/y/z*
4. **sra**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • プロンプトにパスワードを入力します。
ステップ 2	**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 3	**controller vdsl** *x/y/z* **例：** `Router(config)# controller vdsl 0/0/0`	コントローラ コンフィギュレーション モードを開始します。グローバル コンフィギュレーション モードで、controller vdsl コマンドを使用します。このコマンドには、no 形式はありません。 *x*：ネットワーク モジュールを定義します。 *y*：スロット番号を定義します。 *z*：ポート番号を定義します。
ステップ 4	**sra** **例：** `router(config-controller)# sra`	SRA モードをイネーブルにします。 SRA を無効にするには、コマンドの no 形式を使用します。

シームレス レート適応の例

次の例では、VDSL 回線の SRA をイネーブルします。

```
!
!
!
rotuer>enable
router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
router(config)# controller vdsl 0
router(config-controller)# sra
router(config-controller)# end
router#
!
!
!
```

UBR+ の設定

UBR+ を設定するには、次の手順を実行します。

（注）　Cisco IOS Release 15.2(1)T 以降のリリースでは、Cisco 886VA、887VA および 887VA-M ルータ上で UBR+ を実行する必要があります。

（注）　これらの機能は、現在のところ Cisco 866VAE、867VAE、866VAE-K9、または 867VAE-K9 では使用できません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ubr+** *output-pcr output-mcr* [**input-pcr**] [**input-mcr**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトにパスワードを入力します。
ステップ 2	**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 3	**ubr+** *output-pcr output-mcr* [**input-pcr**] [**input-mcr**] **例：** `Router(config-if-vc)# ubr+ 10000 3000 9000 1000`	未指定ビット レート（UBR）の Quality of Service（QoS）を設定し、ATM 相手先固定接続（PVC）、PVC 範囲、相手先選択接続（SVC）、仮想回線（VC）クラス、または VC バンドル メンバの出力ピーク セル レートと出力最小保証セル レートを指定します。 UBR+ パラメータを削除するには、このコマンドの **no** 形式を使用します。 *output-pcr*：kbps 単位の出力ピーク セル レート（PCR）。 *output-mcr*：Kbps 単位の出力最小保証セル レート。 **input-pcr**：（SVC の場合だけはオプション）kbps 単位の入力 PCR。この値が省略された場合は、input-pcr は、output-pcr と等しくなります。 **input-mcr**：（SVC の場合だけはオプション）kbps 単位の入力最小保証セル レート。この値が省略された場合は、input-mcr は、output-mcr と等しくなります。

UBR+ の例

次に、DSL ライン上に UBR+ PVC を設定する例を示します。

```
interface atm 0/0
 pvc 4/100
  ubr+ 2304 2304
```

次の例では、ATM PVC の output-pcr 引数に 100,000 kbps を、output-mcr 引数に 3,000 kbps を指定しています。

```
pvc 1/32
 ubr+ 100000 3000
```

次の例では、ATM SVC の output-pcr、output-mcr、input-pcr、および input-mcr 引数に、それぞれ、10,000 kbps、3,000 kbps、9,000 kbps、および、1,000 kbps を指定しています。

```
svc lion nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 ubr+ 10000 3000 9000 1000
```

トラブルシューティング

Cisco 886VA および 887VA のトラフィックを確認する新しいコマンドはありません。便利なコマンドとして、次の **show** コマンドが挙げられます。

- **show interface Ethernet0**
- **show interface ATM0**
- **show interface summary**
- **show controller vdsl 0**
- **show controller atm0**
- **show controller vdsl 0 datapath**
- **show atm pvc**

また、「Cisco 860, Cisco 880, and Cisco 890 Series Integrated Services Routers Software Configuration Guide, Troubleshooting」も役に立ちます。

CLI を使用したトレーニング ログの設定

Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ISR で **debug vdsl 0 training log** を使用してトレーニング ログの取得をを開始すると、トレーニング ログファイルが開きます。生成されたメッセージがローカルにバッファされ、間隔あたり 5k バイトのトレーニング ログファイルに書き込まれます。トレーニング ログの取得機能をサポートする以前のソフトウェア バージョンと同様に、メッセージはすべて一度に書き込まれるわけではありません。

（注）　Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ISR の最大ログ容量は 8MB（約 1 時間）です。このため、全体のログ収集が 8MB を超えると、ログの取得が自動的に終了します。

（注）　Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ISR は、継続的なトレーニング ログの自動停止機能をサポートしていません。

トレーニング ログの取得

デフォルトでは、トレーニング ログは flash:vdsllog.bin に保存されます。

トレーニング ログの取得を開始するには、**debug vdsl 0 training log** コマンドを使用します。

```
Router# debug vdsl 0 training log
Router#
```

次の確認が表示されます。

```
Training log generation started for VDSL 0
```

トレーニング ログの取得の停止

トレーニング ログの取得を停止するには、**no debug vdsl 0 training log** コマンドを使用します。

```
Router# no debug vdsl 0 training log
Router#
```

次の確認が表示されます。

```
Training Log file for VDSL written to flash:vdsllog.bin
```

トレーニング ログのステータスおよびファイルの場所の表示

トレーニング ログのステータスおよびファイルの場所を表示するには、**show controller vdsl 0** コマンドを使用します。

```
Router# show controller vdsl 0
Router#
```

次の確認が表示されます。

```
Controller VDSL 0 is UP

Daemon Status:           NA

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0x938C
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x938C
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    GMH1049001M 867VAE-K 15.1(20110
Serial Number Far:
Modem Version Near:    15.1(20110422:230431) [suguraja
Modem Version Far:     0x938C

Modem Status:            TC Sync (Showtime!)
DSL Config Mode:         AUTO
Trained Mode:            G.992.5 (ADSL2+) Annex A
TC Mode:                 ATM
```

```
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Trellis:                 ON                        ON
Line Attenuation:         0.0 dB                    0.0 dB
Signal Attenuation:       0.0 dB                    0.0 dB
Noise Margin:            16.0 dB                   14.6 dB
Attainable Rate:        28516 kbits/s             1222 kbits/s
Actual Power:             7.0 dBm                  12.4 dBm
Total FECS:             3                         0
Total ES:               0                         0
Total SES:              0                         0
Total LOSS:             0                         0
Total UAS:              147                       147
Total LPRS:             0                         0
Total LOFS:             0                         0
Total LOLS:             0                         0
Bit swap:               0                         0

Full inits:             1
Failed full inits:      0
Short inits:            0
Failed short inits:     0

Firmware        Source          File Name (version)
--------        ------          -------------------
VDSL            embedded         (0)

Modem FW  Version:      23a
Modem PHY Version:      A2pv6C032b.d23a


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):               0           24543             0              1020
Previous Speed:             0               0             0                 0
Total Cells:                0        87837567             0           3652502
User Cells:                 0               0             0                 0
Reed-Solomon EC:            0               3             0                 0
CRC Errors:                 0               0             0                 0
Header Errors:              0               0             0                 0
Interleave (ms):       0.00            15.00          0.00              3.76
Actual INP:            0.00            57.00          0.00              0.50

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

ATM モードでの 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 モードで次の手順を実行します。

手順の概要

1. **controller dsl** *slot/port*
2. **mode atm**
3. **line-term cpe**
4. **line-mode 4 wire standard**
5. **line-rate** {**auto** | *rate*}

6. **interface atm** *interface-number*
7. **ip-address** *ip-address*
8. **load-interval** *seconds*
9. **no atm ilmi-keepalive** [*seconds*]
10. **pvc** [*name*] *vpi/vci*
11. **protocol** *protocol protocol-address* **broadcast**
12. **encapsulation** *encapsulation-type*

手順の詳細

	コマンド	目的
ステップ 1	**controller dsl** *slot/port* **例：** `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	**mode atm** **例：** `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	**line-term cpe** **例：** `Router(config-ctrl)# line-term cpe`	CPE をイネーブルにします。
ステップ 4	**line-mode 4 wire standard** **例：** `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	**line-rate** {**auto** | *rate*} **例：** `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 kbps 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、回線レートよりも 8 Kbps 低くなります。
ステップ 6	**interface atm** *interface-number* **例：** `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	**ip-address** *ip-address* **例：** `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。

	コマンド	目的
ステップ 8	**load-interval** *seconds* **例：** `Router(config-ctrl)# load-interval 3`	負荷の間隔値を割り当てます。
ステップ 9	**no atm ilmi-keepalive** [*seconds*] **例：** `Router(config-ctrl)# no atm ilmi-keepalive0`	統合ローカル管理インターフェイス（ILMI）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	**pvc** [*name*] *vpi/vci* **例：** `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、デフォルトのカプセル化は AAL5+LLC/SNAP です。
ステップ 11	**protocol** *protocol protocol-address* **broadcast** **例：** `Router(config-ctrl)# protocol ip 10.10.10.2 broadcast`	IP 接続をイネーブルにし、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	**encapsulation** [*encapsulation-type*] **例：** `Router(config-ctrl)# encapsulation aal5snap`	ATM アダプテーション層（AAL）と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 running** 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# show running
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
 !
```

EFM モードでの G.SHDSL WAN インターフェイスの設定

Cisco 888E ISR で G.SHDSL を設定するには、次の URL で『Configuring Cisco G.SHDSL EFM HWICs in Cisco Routers』を参照してください。

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_HWICS.html

セル ワイヤレス WAN インターフェイスの設定

Cisco 880 シリーズ ISR は、Global System for Mobile Communications（GSM）および符号分割多重接続（CDMA）ネットワークを介して使用する、第 3 世代（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一覧については、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 の説明に従い、信号強度について LED をチェックする必要があります。
- Cisco IOS リリース 12.4(15)XZ 以降の Cisco IOS ソフトウェアを理解する必要があります。Cisco 3G ワイヤレス サポートについては、Cisco IOS のマニュアル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
  - アクセス ポイント ネーム（APN）
- 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
P3G 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
	グリーンの点灯	高 RSSI（–69 dBm 以上）
	グリーンが素早く（16 Hz）点滅	中 RSSI（–89 ～ –70 dBm）
	グリーンがゆっくり（1 Hz）点滅	低～中 RSSI（–99 ～ –90 dBm）、信頼できる接続の最小レベル
	Off	低 RSSI（–100 dBm 未満）

1. 3G RSSI = 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左右されます。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 モデムの活性挿抜（OIR）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ムと交換するには、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** コマンドの出力には、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** コマンドを使用すると次のメッセージが表示され、他のすべての show コマンドを使用すると空の出力が表示されます。

  ```
  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有効になりません。次のメッセージは、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した場合に表示されます。

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

- 取り外されたモデムとは別のタイプのモデムを取り付けた場合は、設定を変更して、システムをリロードしなければなりません。

データ アカウントのプロビジョニング

（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、次の手順を実行します。

- 「信号の強さとサービスの可用性」（P.3-44）
- 「GSM モデム データ プロファイルの設定」（P.3-45）
- 「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.3-46）

信号の強さとサービスの可用性

モデムの信号の強さとサービスの可用性を確認するには、特権 EXEC モードで次のコマンドを使用します。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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	**show cellular 0 hardware** **例：** `Router# show cellular 0 hardware`	セルラー モデム ハードウェア情報を表示します。
ステップ 3	**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。
ステップ 4	**show cellular 0 radio** **例：** `Router# show cellular 0 radio`	無線信号の強さを示します。 **（注）** 安定した信頼性の高い接続には、RSSI が -90 dBm を超える必要があります。
ステップ 5	**show cellular 0 profile** **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。

	コマンドまたはアクション	目的
ステップ 6	**show cellular 0 security** **例：** `Router# show cellular 0 security`	SIM およびモデムのロック ステータスに関するセキュリティ情報を示します。
ステップ 7	**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 プロファイルを作成するには、特権 EXEC モードで **cellular 0 gsm profile create** <*profile number*> <*apn*> <*authentication*> <*username*> <*password*> コマンドを入力します。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。

例

```
Router# cellular 0 gsm profile create 3 apn.com chap GSM GSMPassword
```

表 3-3 は、モデム データ プロファイルのパラメータのリストです。

表 3-3　モデム データ プロファイルのパラメータ

profile number	作成するプロファイルの番号。最大 16 個のプロファイルを作成できます。
apn	アクセス ポイント名。この情報はサービス プロバイダーから取得する必要があります。
authentication	CHAP、PAP などの認証タイプ。
username	サービス プロバイダーから提供されるユーザ名。
password	サービス プロバイダーから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わせて、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
- 電波によるサービス提供（OTASP）を使用したアクティベーション

表 3-4 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 プロセスのリストです。

表 3-4　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. OTASP = Over the Air Service Provisioning（電波によるサービス提供）
2. IOTA = Internet Over the Air（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 committed 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

電波によるサービス提供（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。

router # **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 committed 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。

手順の概要

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。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	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	**interface cellular 0** **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。
ステップ 3	**encapsulation ppp** **例：** `Router (config-if)# encapsulation ppp`	専用非同期モード用または Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）用の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	**ppp chap hostname** *host* **例：** `Router (config-if)# ppp chap hostname host@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、通信事業者から提供されたユーザ名に一致する必要があります。GSM だけに適用されます。
ステップ 5	**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 パスワードを指定します。これは、通信事業者から提供されたパスワードに一致する必要があります。
ステップ 6	**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	**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 コマンド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。セルラー インターフェイスの例については、「基本セルラー インターフェイスの設定」（P.3-52）を参照してください。

DDR の設定

セルラー 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。

手順の概要

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**
    または
    chat-script *script name* **""** **"ATDT*777***profile number#*" **TIMEOUT** *timeout value* **CONNECT**
14. **interface cellular 0**
15. **dialer string** *string*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface cellular 0** **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 3	**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	**dialer idle-timeout** *seconds* **例：** `Router (config-if)# dialer idle-timeout 30`	回線切断後のアイドル時間を秒単位で指定します。
ステップ 5	**dialer string** *string* **例：** `Router (config-if)# dialer string gsm`	ダイヤルする番号または文字列を指定します。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	**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	**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	**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`	関係するトラフィックのダイヤラ リストを作成し、プロトコル全体に対してアクセスを許可します。
ステップ 9	**ip access-list** *access list number* **permit** *ip source address* **例：** `Router (config)# ip access list 1 permit any`	関係するトラフィックを定義します。
ステップ 10	**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	**script dialer** *regexp* **例：** `Router (config-line)# script-dialer gsm`	デフォルト モデムのチャット スクリプトを指定します。

	コマンドまたはアクション	目的
ステップ 12	**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	GSM の場合： **chat-script** *script name* **"" "ATDT*99*** *profile number#***" TIMEOUT** *timeout value* **CONNECT** CDMA の場合： **chat-script** *script name* **"" "ATDT*777*** *profile number#***" TIMEOUT** *timeout value* **CONNECT** **例：** `Router (config)# chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT"`	GSM の回線を設定します。 CDMA の回線を設定します。 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	**interface cellular 0** **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。
ステップ 15	**dialer string** *string* **例：** `Router (config)# dialer string gsm`	ダイヤラ スクリプトを指定します（**chat script** コマンドを使用して定義されます）。

データ専用転送モード（DDTM）の設定

データ専用転送モード（DDTM）がディセーブルの場合、CDMA モデムでは、データ送信は、着信音声コールによって中断されます。DDTM モードをイネーブルにして、モデムが着信音声コールを無視するように設定できます。

CDMA モデムの DDTM をイネーブルにするには、コンフィギュレーション モードで **cdma ddtm** コマンドを使用します。

このコマンドは、デフォルトでイネーブルになっています。**no cdma ddtm** コマンドを使用して、この機能をディセーブルにできます。

（注） DDTM がイネーブルの場合、音声コールだけが MC5728v モデムに対してブロックされます。AC597E、MC5725 および MC5727 では、着信 SMS メッセージがブロックされます。

セル ワイヤレス インターフェイスの設定例

ここでは、次の設定例について説明します。

- 「基本セルラー インターフェイスの設定」（P.3-52）
- 「セルラー インターフェイスを介するトンネルの設定」（P.3-53）

基本セルラー インターフェイスの設定

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
```

セルラー インターフェイスを介するトンネルの設定

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
```

Cisco 860VAE ISR での WAN モードの設定

Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ルータは、WAN リンクとして GE インターフェイスまたは DSL インターフェイスを使用するように設定できます。DSL は、Cisco 866VAE、Cisco 867VAE、Cisco 866VAE-K9、および Cisco 867VAE-K9 ルータ起動時のデフォルト WAN インターフェイスです。

ルータの起動後は、**wan mode** コマンドを使用して目的の WAN インターフェイスを選択できます。WAN モードがイーサネットとして設定されている場合、ATM0 と Ethernet0 インターフェイスの両方がシャットダウン状態になります。DSL インターフェイスのいずれかで **no shutdown** コマンドを入力しても、「***WAN interface is Ethernet***」というメッセージが表示されて拒否されます。同様に、WAN モードが DSL の場合、GE WAN インターフェイスはシャットダウン状態となり、**no shutdown** コマンドを入力しても「***WAN interface is DSL***」というメッセージが表示されて拒否されます。

（注）　ルータは、GE および DSL インターフェイスを同時にイネーブルにすることをサポートしていません。

DSL から Ethernet インターフェイス、またはその逆に切り替えるには、**wan mode dsl | ethernet** コマンドを使用します。

ここでは、次の内容について説明します。

- 「WAN モードのイネーブル化」（P.3-54）
- 「WAN モード設定の表示」（P.3-54）

WAN モードのイネーブル化

WAN モードを選択してイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **show running-configuration**
3. **wan mode {dsl | ethernet}**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトにパスワードを入力します。
ステップ 2	**show running-configuration** **例：** `Router# show running-configuration`	起動時にデフォルト エントリを表示します。
ステップ 3	**wan mode {dsl | ethernet}** **例：** `Router(config)# wan mode dsl`	目的の WAN モードを選択します。
ステップ 4	**exit** **例：** `Router(config)# exit` `Router#`	コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。

WAN モード設定の表示

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 866VAE ルータの例を参照してください）。

（注） Cisco ルータは、初期設定の完了後の起動シーケンス中に WAN モードを表示します。

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

Current configuration : 1195 bytes
!
! Last configuration change at 13:27:25 UTC Wed Feb 24 2010
version 15.2
no service pad
service timestamps debug datetime msec localtime show-timezone
```

```
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
enable password lab
!
no aaa new-model
wan mode ethernet
no ipv6 cef
!
!
!
!
!
ip cef
!
crypto pki token default removal timeout 0
!
!
!
!
!
!
controller VDSL 0
 shutdown
!
!
!
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 202.0.0.1 255.255.255.0
 pvc 0/202
 !
!
interface Ethernet0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
!
interface FastEthernet1
 no ip address
!
interface FastEthernet2
 no ip address
!
interface FastEthernet3
 no ip address
!
interface GigabitEthernet0
 ip address 1.0.0.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
scheduler allocate 60000 1000
!
end

Router#
```

ファスト イーサネット LAN インターフェイスの設定

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

無線 LAN インターフェイスの設定

Cisco 860、Cisco 880、および Cisco 890 シリーズ無線ルータには、ワイヤレス LAN 接続用に 802.11n モジュールが内蔵されています。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ーとして機能し、デフォルトのルーティング情報を提供します。

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**interface** *loopback 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。 *number*：ループ バック インターフェイスの番号。
ステップ 2	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	ループバック インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 3	**exit** **例：** `Router(config-if)# exit` `Router(config)#`	ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例

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

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

設定の確認

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

```
Router# show interface loopback 0
Loopback 0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

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

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

スタティック ルートの設定

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

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **例：** `Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`	IP パケットのスタティック ルートを指定します。 このコマンドの詳細および設定可能なその他のパラメータについては、『*Cisco IOS IP Routing Protocols Command Reference*』を参照してください。
ステップ 2	**end** **例：** `Router(config)# end` `Router#`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

スタティック ルーティングの一般的な説明については、「概要」（P.B-1）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。具体的には、パケットが設定済みの PVC に送信されます。

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

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

設定の確認

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

次のような確認用の出力が表示されます。

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

Gateway of last resort is not set

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

ダイナミック ルートの設定

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

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

- 「ルーティング情報プロトコルの設定」（P.3-60）
- 「拡張インテリア ゲートウェイ ルーティング プロトコルの設定」（P.3-62）

ルーティング情報プロトコルの設定

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

手順の概要

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

手順の詳細

	コマンド	タスク
ステップ 1	**router rip** **例：** `Router(config)# router rip` `Router(config-router)#`	ルータ コンフィギュレーション モードを開始します。続いて、ルータの RIP をイネーブルにします。
ステップ 2	**version** {**1**	**2**} **例：** `Router(config-router)# version 2`	RIP version 1 または 2 の使用を指定します。
ステップ 3	**network** *ip-address* **例：** `Router(config-router)# network 192.168.1.1` `Router(config-router)# network 10.10.7.1`	直接接続しているネットワークの各アドレスを使用して、RIP を適用するネットワーク リストを指定します。

	コマンド	タスク
ステップ 4	**no auto-summary** **例：** `Router(config-router)# no auto-summary`	ネットワーク レベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。これにより、サブプレフィクス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。
ステップ 5	**end** **例：** `Router(config-router)# end` `Router#`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

RIP に関する一般情報については、「RIP」（P.B-3）を参照してください。

例

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

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

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

設定の確認

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

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

Gateway of last resort is not set

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

拡張インテリア ゲートウェイ ルーティング プロトコルの設定

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**router eigrp** *as-number* **例：** `Router(config)# router eigrp 109`	ルータ コンフィギュレーション モードを開始します。続いて、ルータの EIGRP をイネーブルにします。Autonomous System（AS; 自律システム）番号は、他の EIGRP ルータへのルートを識別します。また、EIGRP 情報のタグ付けに使用されます。
ステップ 2	**network** *ip-address* **例：** `Router(config)# network 192.145.1.0` `Router(config)# network 10.10.12.115`	EIGRP を適用するネットワークのリストを指定します（直接接続されているネットワークの IP アドレスを使用）。
ステップ 3	**end** **例：** `Router(config-router)# end` `Router#`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

EIGRP の概要については、「EIGRP」（P.B-3）を参照してください。

例

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

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

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

設定の確認

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

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

Gateway of last resort is not set

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

CHAPTER 4

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 サービス統合型ルータ（ISR）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。

この章の内容は、次のとおりです。

認証、許可、アカウンティング

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 コントロールを設定する主要なフレームワークを提供します。認証は、ログインおよびパスワード ダイアログ、確認要求および応答、メッセージングのサポート、暗号化（選択するセキュリティ プロトコルに応じて）など、ユーザを識別するための方法を提供します。許可は、1 回限りの許可や各サービスに対する許可、各ユーザに対するアカウント リストおよびプロファイル、ユーザ グループのサポート、IP、インターネットワーク パケット交換（IPX）、AppleTalk リモート アクセス（ARA）、および Telnet のサポートなど、リモート アクセスをコントロールするための方法を提供します。アカウンティングで、ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。

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を管理します。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 サーバ間の通信を確立するための手段となります。

AAA サービスの設定およびサポートされるセキュリティ プロトコルの詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T*』で次の項を参照してください。

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

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃に悪用される可能性のある一般的な IP サービスをディセーブルにし、攻撃を受けたときはネットワークの防御に役立つ IP サービスおよび機能をイネーブルにできます。この IP サービスは、1 つのコマンドですべてを同時にディセーブル/イネーブルにすることにより、ルータ上のセキュリティ設定を大幅に簡易化しています。AutoSecure 機能の詳細については、「*AutoSecure*」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、標準版または拡張版のどちらかに設定されます。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 リストでは、宛先および送信元の両方を指定できます。また、各プロトコルを指定して、通過を許可または拒否することができます。

アクセス リストの作成の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Access Control Lists (ACLs)」を参照してください。

アクセス リストは、一般的なタグによってコマンドがバインドされる一連のコマンドです。タグは、番号または名前のどちらかです。表 4-1 は、アクセス リストの設定に使用するコマンドのリストです。

表 4-1　アクセス リストのコンフィギュレーション コマンド

ACL タイプ	コンフィギュレーション コマンド
番号形式	
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*]
名前形式	
標準	**ip access-list standard** *name* followed by **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、精緻化、管理するには、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』の「Access Control Lists (ACLs)」を参照してください。

- IP アクセス リストの作成とインターフェイスへの適用
- 「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」
- IP アクセス リストの精緻化
- 「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、一般的な名前または番号にバインドされている一連のアクセス リストの定義のことです。このグループは、インターフェイスを設定するときに、インターフェイスに対してイネーブルにされます。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 リストの定義の順序は重要です。パケットは、最初のアクセス リストから順に照合されます。一致するものがない場合（つまり、許可または拒否が発生しない場合）は、次のアクセス リストに照合され、さらに次のアクセス リストへと順に進められます。
- パケットが許可または拒否される前に、すべてのパラメータがアクセス リストに一致する必要があります。
- すべてのシーケンスの末尾には、暗黙的に「deny all」が付きます。

アクセス グループの設定および管理の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』を参照してください。

Cisco IOS ファイアウォールの設定

Cisco IOS ファイアウォールでは、ステートフルなファイアウォールを設定できます。ステートフルなファイアウォールでは、パケットが内部的に検査され、ネットワーク接続の状態がモニタされます。アクセス リストは各パケットに基づいたトラフィックの許可または拒否に制限され、パケットの流れには基づいていないため、ステートフルなファイアウォールの方が静的アクセス リストよりも優れてい

ます。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、アプリケーション層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、検証するプロトコルを指定します。

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

指定し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インスペクションで検出された場合、ダイナミック アクセス リストが作成され、リターン トラフィックの通過を許可します。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。タイムアウト値が指定値に達すると、ダイナミック アクセス リストが削除され、後続のパケット（有効なパケットの場合もある）が許可されなくなります。

複数のステートメントで同一のインスペクション名を使用して、1 つのルール セットにまとめてください。ファイアウォールにインターフェイスを設定するときに、**ip inspect inspection-name {in | out}** コマンドを使用して、このルール セットを設定の別の場所でアクティブ化できます。

Cisco IOS ファイアウォールの設定の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』を参照してください。

また、Cisco IOS ファイアウォールは、Session Initiated Protocol（SIP; セッション開始プロトコル）アプリケーションでの音声セキュリティを提供するようにも設定できます。SIP インスペクションは、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、『*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 では、「シグネチャ」を使用して、ネットワーク トラフィック内における誤使用の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。

- アラームを送信する
- 不審なパケットを廃棄する
- 接続を再設定する
- 攻撃者の発信元 IP アドレスからのトラフィックを一定時間拒否する
- シグニチャが見つかった接続のトラフィックを一定時間拒否する

Cisco IOS IPS の設定の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane, Release 12.4T*』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、許可または拒否する Web サイトのカテゴリを選択し、ISR 上で URL フィルタリングを準備します。各カテゴリの URL のチェックには、サードパーティが保守する外部サーバが使用されています。ポリシーの許可および拒否は、ISR 上で保守されています。サービスは加入ベースで提供され、各カテゴリの URL はサードパーティ ベンダーによってメンテナンスされています。

URL フィルタリングの設定の詳細については、『*Subscription-based Cisco IOS Content Filtering guide*』を参照してください。

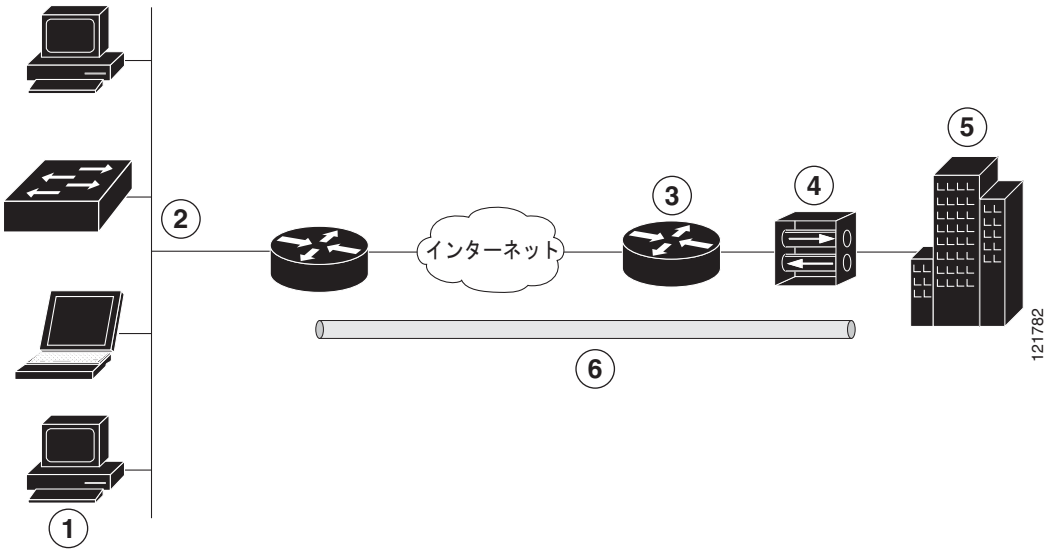
VPN の設定

VPN 接続は、インターネットなどのパブリック ネットワーク上の 2 台のネットワーク間の安全な接続を提供します。Cisco 860 および Cisco 880 シリーズ ISR は、サイト間およびリモート アクセスの 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、企業ネットワークにログインする際にリモート クライアントによって使用されます。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 コンフィギュレーションでは、Cisco Easy VPN および IP Security（IPSec）トンネルを使用して、リモート クライアントとコーポレート ネットワーク間の接続を設定および保護します。図 4-1 は、一般的な構成例を示します。

図 4-1　IPSec トンネルを使用したリモート アクセス VPN



1	リモート ネットワークで接続されたユーザ
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 アドレスが 210.110.101.1 の Cisco VPN 3000 コンセントレータなど）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN クライアント機能は、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業の大部分を排除します。このプロトコルでは、ほとんどの 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、インターネット ネーミング サービス（WINS）サーバ アドレス、スプリットトンネリング フラグなど）を、VPN サーバ（IPSec サーバとして機能している Cisco VPN 3000 シリーズ コンセントレータなど）に定義することできます。

Cisco Easy VPN サーバ対応のデバイスでは、PC 上で Cisco Easy VPN リモート ソフトウェアを実行しているモバイルおよびリモート作業者が開始した VPN トンネルを終了できます。Cisco Easy VPN サーバ対応のデバイスでは、リモート ルータを Cisco Easy VPN リモート ノードとして動作させることができます。

Cisco Easy VPN クライアント機能は、クライアント モードとネットワーク拡張モードの 2 つのモードのいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、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 ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

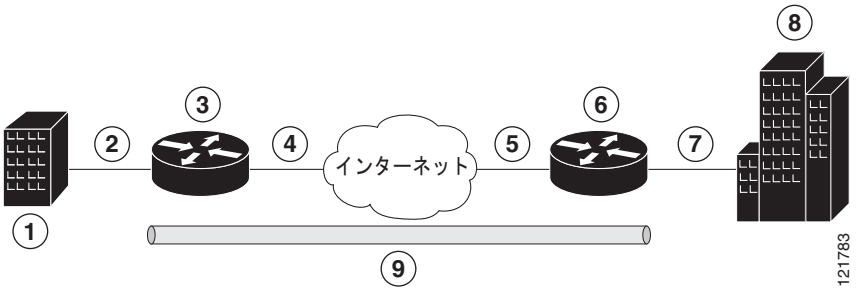
（注） Cisco Easy VPN クライアント機能に設定できるのは、1 つの宛先ピアだけです。アプリケーションで複数の VPN トンネルを作成する必要がある場合、手動でクライアントおよびサーバ側の両方に IPSec VPN および Network Address Translation/Peer Address Translation（NAT/PAT; ネットワーク アドレス変換 / ピア アドレス変換）パラメータを設定する必要があります。

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 サーバの設定手順については、「*Easy VPN Server*」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 および Generic Routing Encapsulation（GRE; 汎用ルーティング カプセル化）プロトコルを使用して、ブランチ オフィスとコーポレート ネットワーク間の接続を保護します。図 4-2 は、一般的な構成例を示します。

図 4-2　IPSec トンネルおよび GRE を使用したサイト間の VPN



1	複数の LAN および VLAN を使用しているブランチ オフィス
2	ファスト イーサネット LAN インターフェイス（NAT 用の内部インターフェイス、アドレスは 192.165.0.0/16）
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 イーサネットまたは ATM インターフェイス（NAT 用の外部インターフェイス、アドレスは 200.1.1.1）
5	LAN インターフェイス（外部インターフェイス アドレスは 210.110.101.1）：インターフェイスに接続
6	VPN クライアント：企業ネットワークへのアクセスを制御する別のルータ
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	コーポレート 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 設定の詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity, Release 12.4T*』を参照してください。

設定例

各例では、「IPSec トンネル上での VPN の設定」（P.4-8）の手順を使用して IPSec トンネル上に VPN を設定します。次に、リモート アクセス設定およびサイト間設定の具体的な手順を順番に説明します。

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 モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

VPN コンフィギュレーション情報は、両方のエンドポイントに設定する必要があります。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、およびネットワーク アドレス変換（NAT）などです。

- 「IPSec トンネル上での VPN の設定」（P.4-8）
- 「Cisco Easy VPN リモート コンフィギュレーションの作成」（P.4-17）
- 「サイト間 GRE トンネルの設定」（P.4-19）

IPSec トンネル上での VPN の設定

IPSec トンネル上に VPN を設定するには、次の作業を行います。

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー交換）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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp policy** *priority*
2. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
3. **hash** {**md5** | **sha**}
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **group** {**1** | **2** | **5**}
6. **lifetime** *seconds*
7. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**crypto isakmp policy** *priority* **例：** `Router(config)# crypto isakmp policy 1`	IKE ネゴシエーション時に使用される IKE ポリシーを作成します。プライオリティ番号の範囲は 1 ～ 10000 で、プライオリティが最も高いのは 1 です。 また、Internet Security Association Key and Management Protocol（ISAKMP; インターネット セキュリティ アソシエーション キーおよび管理）ポリシー 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	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} **例：** `Router(config-isakmp)# encryption 3des`	IKE ポリシーに使用される暗号化アルゴリズムを指定します。 この例では、168 ビット Data Encryption Standard（DES; データ暗号化規格）を指定します。
ステップ 3	**hash** {**md5** | **sha**} **例：** `Router(config-isakmp)# hash md5`	IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。 この例では、Message Digest 5（MD5）アルゴリズムを指定します。デフォルトは、Secure Hash 標準（SHA-1）です。
ステップ 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**} **例：** `Router(config-isakmp)# authentication pre-share`	IKE ポリシーに使用される認証方式を指定します。 この例では、事前共有キーを指定します。
ステップ 5	**group** {**1** | **2** | **5**} **例：** `Router(config-isakmp)# group 2`	IKE ポリシーに使用される 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`	IKE セキュリティ アソシエーション（SA）のライフタイムを指定します。 指定できる値は 60 ～ 86400 です。
ステップ 7	**exit** **例：** `Router(config-isakmp)# exit`	ISAKMP ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp client configuration group** {**group-name** | **default**}
2. **key** *name*
3. **dns** *primary-server*
4. **domain** *name*
5. **exit**
6. **ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]

手順の詳細

	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`	リモート クライアントにダウンロードされる属性を含む IKE ポリシー グループを作成します。 また、ISAKMP グループ ポリシー 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	**key** *name* **例：** `Router(config-isakmp-group)# key secret-password`	グループ ポリシーの IKE 事前共有キーを指定します。
ステップ 3	**dns** *primary-server* **例：** `Router(config-isakmp-group)# dns 10.50.10.1`	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。 **（注）** グループの Windows インターネット ネーミング サービス（WINS）サーバを指定するには、**wins** コマンドを使用します。
ステップ 4	**domain** *name* **例：** `Router(config-isakmp-group)# domain company.com`	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)#`	ISAKMP グループ ポリシー 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。
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`	グループのローカル アドレス プールを指定します。 このコマンドの詳しい説明およびその他の設定可能な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。

クリプト マップへのモード設定の適用

クリプト 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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

手順の詳細

	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`	クリプト 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 ポリシーのキー ルックアップ（IKE クエリ）をイネーブルにします。
ステップ 2	**crypto map** *tag* **client configuration address** [**initiate**	**respond**] **例：** `Router(config)# crypto map dynmap client configuration address respond`	リモート クライアントからのモード設定要求にルータが応答するように設定します。

ポリシー ルックアップのイネーブル化

AAA 経由でポリシー ルックアップ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 モードから始め、次の手順を実行します。

手順の概要

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

手順の詳細

	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`	AAA アクセス コントロール 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`	選択したユーザのログイン時の AAA 認証を指定し、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を使用します。 **（注）** RADIUS サーバも使用できます。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』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`	PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに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を使用します。 **（注）** RADIUS サーバも使用できます。詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』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 username1 password 0 password1`	ユーザ名をベースとした認証システムを構築します。

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、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IKE のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用してデータ フローを保護することに合意します。

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が含まれているトランスフォーム セットが検出された場合は、両方のピアの設定の一部として選択され、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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec profile** *profile-name*
2. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
3. **crypto ipsec security-association lifetime** {**seconds** *seconds* \| **kilobytes** *kilobytes*}

手順の詳細

	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`	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。
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`	トランスフォーム セット（IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ）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 Configuration Guide: Secure Connectivity, Release 12.4T*』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`	IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。

IPSec 暗号方式およびパラメータの設定

ダイナミック クリプト マップ ポリシーでは、ルータがすべてのクリプト 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 ピアからの新規の SA 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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
3. **reverse-route**
4. **exit**
5. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

手順の詳細

	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`	ダイナミック クリプト マップ エントリを作成し、クリプト 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`	クリプト 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`	クリプト 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。
ステップ 4	**exit** **例：** `Router(config-crypto-map)# exit`	クリプト マップ 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 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`	クリプト マップ プロファイルを作成します。

物理インターフェイスへのクリプト マップの適用

クリプト マップは、IPSec トラフィックが通過する各インターフェイスに適用されている必要があります。物理インターフェイスにクリプト マップを適用することにより、ルータがすべてのトラフィックを SA データベースに照合するようになります。デフォルト設定では、ルータはリモート サイト間に送信されるトラフィックを暗号化して、安全な接続を提供します。ただし、パブリック インターフェイスでは他のトラフィックの通過を許可し、インターネットへの接続を提供しています。

インターフェイスにクリプト 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 モードから始め、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **crypto map** *map-name*
3. **exit**

手順の詳細

	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`	クリプト 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`	クリプト 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)#`	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。

次の作業

Cisco Easy VPN リモート コンフィギュレーションを作成する場合は、「Cisco Easy VPN リモート コンフィギュレーションの作成」（P.4-17）を参照してください。

IPSec トンネルおよび GRE を使用してサイト間 VPN を作成する場合は、「サイト間 GRE トンネルの設定」（P.4-19）を参照してください。

Cisco Easy VPN リモート コンフィギュレーションの作成

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 コンフィギュレーションを作成するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec client ezvpn** *name*
2. **group** *group-name* **key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **network extension plus**}
5. **exit**
6. **crypto isakmp keepalive** *seconds*
7. **interface** *type number*
8. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
9. **exit**

手順の詳細

	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`	Cisco Easy VPN リモート コンフィギュレーションを作成します。続いて、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`	VPN 接続の IPSec グループおよび IPSec キー値を指定します。

	コマンドまたはアクション	目的
ステップ 3	**peer** {*ipaddress* | *hostname*} **例：** `Router(config-crypto-ezvpn)# peer 192.168.100.1`	VPN 接続のピア IP アドレスまたはホスト名を指定します。 • ホスト名を指定できるのは、ルータから DNS サーバを介してホスト名解決を行える場合だけです。 **（注）** このコマンドを使用して、バックアップとして使用する複数のピアを設定します。1 つのピアがダウンすると、次に使用可能なピアを用いて Easy VPN トンネルが確立されます。プライマリ ピアが再起動すると、プライマリ ピアを用いてトンネルが再確立されます。
ステップ 4	**mode** {**client** | **network-extension** | **network extension plus**} **例：** `Router(config-crypto-ezvpn)# mode client`	VPN 動作モードを指定します。
ステップ 5	**exit** **例：** `Router(config-crypto-ezvpn)# exit`	Cisco Easy VPN リモート 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。
ステップ 6	**crypto isakmp keepalive** *seconds* **例：** `Router(config)# crypto isakmp keepalive 10`	デッド ピア検出メッセージがイネーブルになります。 • *seconds*：メッセージの間隔を設定します。範囲は 10 ～ 3600 です。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface fastethernet 4`	Cisco Easy VPN リモート コンフィギュレーション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。 **（注）** ATM WAN インターフェイスを使用し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`	WAN インターフェイスに Cisco Easy VPN リモート コンフィギュレーションを割り当てます。 • このコマンドにより、ルータは VPN 接続に必要な NAT またはポート アドレス変換（PAT）とアクセス リスト設定を自動的に作成します。
ステップ 9	**exit** **例：** `Router(config-crypto-ezvpn)# exit`	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。

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 ファイルの一部を示します。

```
!
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
!
```

サイト間 GRE トンネルの設定

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。

手順の概要

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

4. **tunnel destination** *default-gateway-ip-address*
5. **crypto map** *map-name*
6. **exit**
7. **ip access-list** {**standard** | **extended**} *access-list-name*
8. **permit** *protocol source source-wildcard destination destination-wildcard*
9. **exit**

手順の詳細

	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`	トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**ip address** *ip-address mask* **例：** `Router(config-if)# 10.62.1.193 255.255.255.252`	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`	GRE トンネルに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`	GRE トンネルに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`	トンネルにクリプト マップを割り当てます。 **（注）** 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 ルートは、サイト間の接続を確立するために設定しておく必要があります。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	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。
ステップ 7	**ip access-list** {**standard**	**extended**} *access-list-name* **例：** `Router(config)# ip access-list extended vpnstatic1`	クリプト 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。

	コマンドまたはアクション	目的
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`	発信インターフェイスでは GRE トラフィックだけが許可されるように指定します。
ステップ 9	**exit** **例：** `Router(config-acl)# exit` `Router(config)#`	ACL 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。

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 5

バックアップ データ回線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 サービス統合型ルータ（ISR）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 ポートおよび補助ポートは、同じ物理 RJ-45 ポートにあります。したがって、2 ポートを同時にアクティブにすることはできません。必要な機能をイネーブルにするには、CLI を使用する必要があります。

Cisco 892F ISR には、銅線接続をサポートするギガ ビット イーサネット（GE）ポートまたはファイバ接続をサポートをサポートする Small Form-factor Pluggable（SFP）ポートがあり、ネットワークがダウンした場合のフェールオーバー冗長性に設定できます。

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 5-1 では、ポートの指定とともに Cisco 880 および Cisco 890 シリーズ ISR のバックアップ インターフェイスを示します。これらのインターフェイスの基本設定は、第 3 章「ルータの基本設定」の「WAN インターフェイスの設定」（P.3-8）に示します。

表 5-1　　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	V.92
881G、886G、887G、887VG、888G	—	Yes	—
886、886VA、887、887V、888、888E	Yes	—	—
891	—	—	Yes
892、892F	Yes	—	—

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。

手順の概要

1. **interface** *type number*
2. **backup interface** *interface-type interface-number*
3. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface atm 0`	バックアップ用に設定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。 このインターフェイスは、シリアル、ISDN、または非同期の可能性があります。 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`	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。

セルラー 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

必要な場合にプライマリ接続をモニタし、セルラー インターフェイスでバックアップ接続を開始する場合、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：スタンバイの状態のまま待機し、プライマリ インターフェイス回線プロトコルがダウンと認識されると、アップ状態になります。「バックアップ インターフェイスの設定」（P.5-2）を参照してください。
- ダイヤラ ウォッチ：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.5-4）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する経路に、プライマリ接続のアドミニストレーティブ ディスタンスよりも大きいアドミニストレーティブ ディスタンスがあり、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 テーブルには存在しません。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.5-5）を参照してください。

（注） セルラー インターフェイスおよびその他の非同期シリアル インターフェイスのバックアップ 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、インターフェイスを設定して 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必要があります。ダイヤラ マップなどの、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、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。

手順の概要

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*

   または

   dialer group *dialer group number*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *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	**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	**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`	監視されるすべての IP アドレスのリストを定義します。

	コマンドまたはアクション	目的
ステップ 5	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**} **例：** `Router(config)# dialer-list 2 protocol ip permit`	関係するトラフィックのダイヤラ リストを作成し、プロトコル全体に対してアクセスを許可します。
ステップ 6	**ip access-list** *access-list-number* **permit** *ip source address* **例：** `Router(config)# access list 2 permit 10.4.0.0`	関係するトラフィックを定義します。 IP ネットワークへのトラフィック送信を回避するには、**access list permit all** コマンドは使用しないでください。これによって、コールが強制的に終了される場合があります。
ステップ 7	**interface cellular** *0* **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。
ステップ 8	**dialer string** *string* または **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 スクリプトを指定します（**chat script** コマンドを使用して定義されます）。 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 classless がイネーブルにされていることを確認してください。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	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	**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、設定されているアドミニストレーティブ ディスタンスを使用して、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ときだけバックアップ インターフェイスを使用するするよう、バックアップ インターフェイスを通したルートのアドミニストレーティブ ディスタンスをより高く設定する必要があります。

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 ネットワークまたは CDMA ネットワークで NAT および IPsec を設定したバックアップとして 3G ワイヤレス モデムを設定する方法の例を示します。

（注） 送受信速度は設定できません。実際のスループットは、セルラー ネットワーク サービスによって異なります。

```
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
```

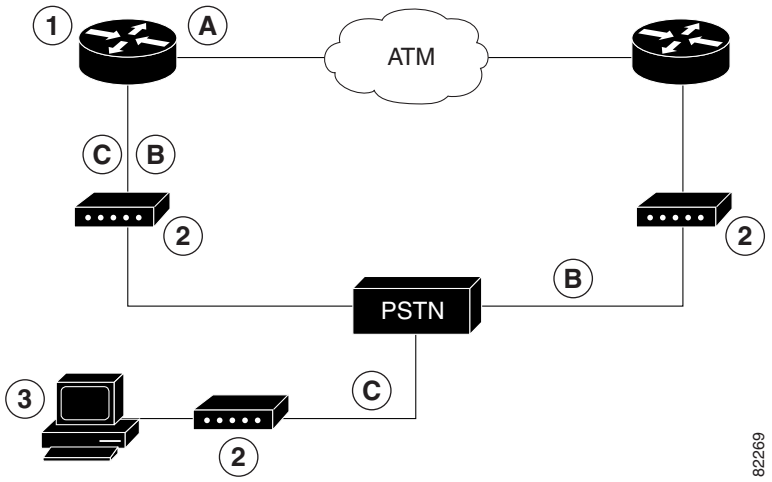
```
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line 3
 exec-timeout 0 0
 script dialer gsm                                    *** or cdma ***
 login
 modem InOut
 no exec
line vty 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インターネット サービス プロバイダー（ISP）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。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 ルートを提供するため、ダイヤル バックアップ機能を追加できます。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 5-1 は、リモート管理アクセスおよびプライマリ WAN 回線にバックアップを提供する場合に使用するネットワーク コンフィギュレーションを示しています。

図 5-1　　補助ポートによるダイヤル 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 プロバイダーへのプライマリ接続です。
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 コンフィギュレーションへの変更または更新を可能にするダイヤルイン アクセスとして機能します。

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。

手順の概要

1. **ip name-server** *server-address*
2. **ip dhcp pool** *name*
3. **exit**
4. **chat-script** *script-name expect-send*
5. **interface** *type number*
6. **exit**

7. **interface** *type number*
8. **dialer watch-group** *group-number*
9. **exit**
10. **ip nat inside source {list** *access-list-number*} {**interface** *type number* | **pool** *name*} **[overload]**
11. **ip route** *prefix mask* {***ip-address*** | ***interface-type interface-number*** [***ip-address***]}
12. **access-list** *access-list-number* **{deny | permit}** *source* **[***source-wildcard***]**
13. **dialer watch-list** *group-number* {**ip** *ip-address address-mask* | **delay route-check initial** *seconds*}
14. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
15. **modem enable**
16. **exit**
17. **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
18. **flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}

手順の詳細

	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`	ISP DNS IP アドレスを入力します。 **ヒント** 可能な場合は、複数のサーバ アドレスを追加できます。
ステップ 2	**ip dhcp pool** *name* **例：** `Router(config)# ip dhcp pool 1`	ルータ上に DHCP アドレス プールを作成します。続いて、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* 引数は、ストリングまたは整数にすることができます。 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 モードで使用できるサンプル コマンドについては、「例」（P.5-13）を参照してください。
ステップ 3	**exit** **例：** `Router(config-dhcp)#exit`	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`	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を使用して PSTN に接続されたモデムで通話します。

	コマンド	目的
ステップ 5	**interface** *type number* **例：** `Router(config)# interface Async 1`	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 モードで使用できるサンプル コマンドについては、「例」（P.5-13）を参照してください。
ステップ 6	**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 7	**interface** *type number* **例：** `Router(config)# interface Dialer 3`	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`	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`	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`	内部インターフェイス上のダイナミック 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`	ダイヤラ インターフェイスにポイントする IP ルートをデフォルト ゲートウェイとして設定します。
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示す拡張アクセス リストを定義します。
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`	ピアへのルートが存在するかどうかにより、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。

	コマンド	目的
ステップ 14	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*] **例：** `Router(config)# line console 0`	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`	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`	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`	補助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 18	**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]} **例：** `Router(config)# flowcontrol hardware`	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
```

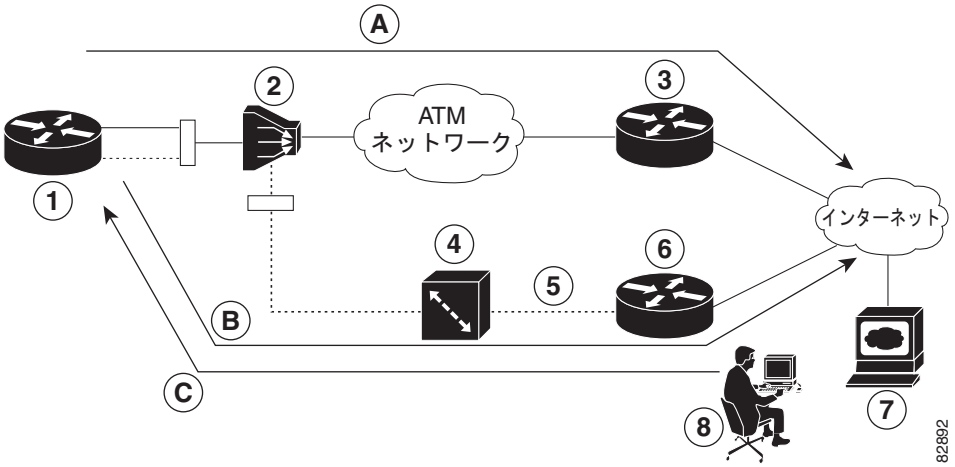
```
!
! Dial backup and remote management physical interface.
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 async default routing
 async dynamic routing
 async mode dedicated
 ppp authentication pap callin
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 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 ポート経由でのデータ回線バックアップおよびリモート管理の設定

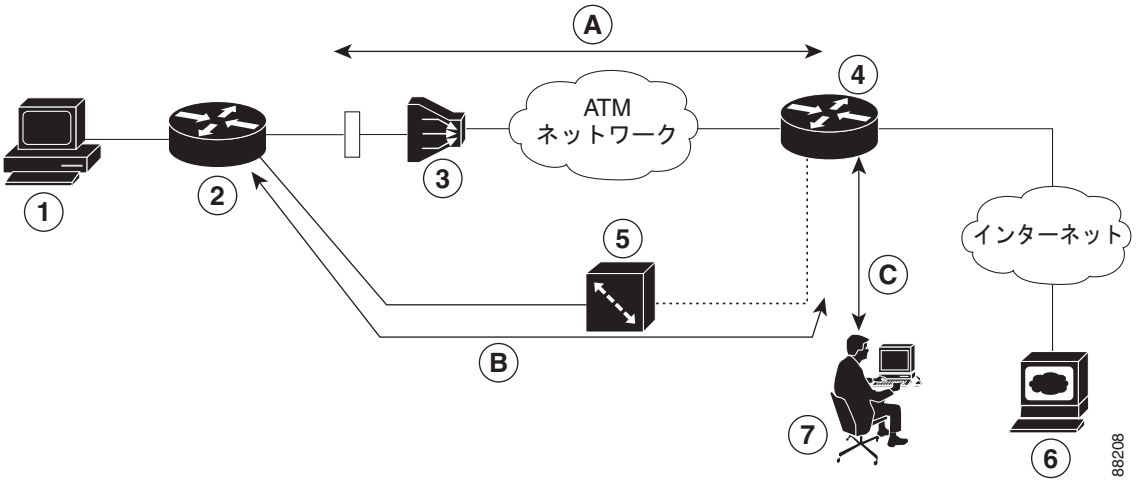
Cisco 880 シリーズ ルータは、リモート管理に ISDN S/T ポートを使用できます。図 5-2 および 図 5-3 は、プライマリ WAN 回線のリモート管理アクセスおよびバックアップを実現する 2 種類の典型的なネットワーク コンフィギュレーションを示します。図 5-2 の場合、ダイヤル バックアップ リンクは加入者宅内機器（CPE）のスプリッタ、デジタル加入者線アクセス マルチプレクサ（DSLAM）、およびセントラル オフィス（CO）のスプリッタを経由して ISDN 交換機に接続されます。図 5-3 では、ダイヤル バックアップ リンクは、ルータから ISDN 交換機に直接接続されます。

図 5-2　　CPE スプリッタ、DSLAM、および CO スプリッタを経由するデータ回線バックアップ



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）経由のダイヤル 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 リンクとして機能します。
3	ATM アグリゲータ		
4	ISDN スイッチ		
5	ISDN	**C**	プライマリ DSL リンクがダウンした場合に、ISDN インターフェイスから管理者にリモート管理機能を提供します。Cisco IOS コンフィギュレーションへの変更または更新を可能にするダイヤルイン アクセスとして機能します。
6	ISDN ピア ルータ		
7	Web サーバ		
8	管理者	**—**	—

図 5-3　ルータから ISDN スイッチへの直接接続データ回線バックアップ



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）経由のダイヤル 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 リンクとして機能します。
3	DSLAM		
4	アグリゲータ		
5	ISDN スイッチ	C	プライマリ DSL リンクがダウンした場合に、ISDN インターフェイスから管理者にリモート管理機能を提供します。Cisco IOS コンフィギュレーションへの変更または更新を可能にするダイヤルイン アクセスとして機能します。
6	Web サーバ		
7	管理者		

ルータの ISDN S/T ポート経由でダイヤル バックアップおよびリモート管理を設定するには、次の手順を実行します。

- ISDN 設定の構成
- アグリゲータおよび ISDN ピア ルータの設定

ISDN 設定の構成

（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。

バックアップ インターフェイスとして使用するルータ ISDN インターフェイスを設定するには、グローバル コンフィギュレーション モードから始めて次の手順を実行します。

手順の概要

1. **isdn switch-type** *switch-type*
2. **interface** *type number*

3. **encapsulation** *encapsulation-type*
4. **dialer pool-member** *number*
5. **isdn switch-type** *switch-type*
6. **exit**
7. **interface dialer** *dialer-rotary-group-number*
8. **ip address negotiated**
9. **encapsulation** *encapsulation-type*
10. **dialer pool** *number*
11. **dialer string** *dial-string*#[**:***isdn-subaddress*]
12. **dialer-group** *group-number*
13. **exit**
14. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | *access-group*}

手順の詳細

	コマンド	目的
ステップ 1	**isdn switch-type** *switch-type* **例：** `Router(config)# isdn switch-type basic-net3`	ISDN スイッチ タイプを指定します。 この例では、豪州、欧州、および英国で使用するスイッチ タイプを指定しています。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`	ISDN BRI 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`	BRI0 インターフェイスのカプセル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`	ダイヤラ プールの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`	ISDN スイッチ タイプを指定します。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	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。

	コマンド	目的
ステップ 7	**interface dialer** *dialer-rotary-group-number* **例：** `Router(config)# interface dialer 0`	ダイヤラ インターフェイス（番号 0 ～ 255）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`	インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。ピアから IP アドレスを取得します。
ステップ 9	**encapsulation** *encapsulation-type* **例：** `Router(config-if)# encapsulation ppp`	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`	使用するダイヤラ プールを指定します。 この例では、BRI0 の dialer pool-member 値は 1 なので、dialer pool 1 という設定により dialer 0 インターフェイスが BRI0 インターフェイスに対応付けられます。
ステップ 11	**dialer string** *dial-string*#[**:***isdn-subaddress*] **例：** `Router(config-if)# dialer string 384040`	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`	ダイヤラ グループ（1 ～ 10）にダイヤラ インターフェイスを割り当てます。
ステップ 13	**exit** **例：** `Router(config-if)# exit`	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`	指定したインターフェイス ダイヤラ グループ経由で転送する対象パケット用のダイヤラ リストを作成します。 この例では、dialer-list 1 が dialer-group 1 に対応します。 このコマンドの詳しい説明およびその他の設定可能な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

ISDN ピア ルータは、ISDN インターフェイスを装備し、公衆 ISDN ネットワーク経由で Cisco ルータの ISDN インターフェイスに到達可能なルータです。ISDN ピア ルータは、ATM ネットワークがダウンした場合、Cisco ルータにインターネット アクセスできるようになります。

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。

```
! 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!
```

ギガビット イーサネット フェールオーバー メディアの設定

Cisco 892F ルータには、銅線接続をサポートするギガ ビット イーサネット（GE）ポートまたはファイバ接続をサポートする Small Form-factor Pluggable（SFP）ポートがあります。ネットワークがダウンした場合に、フェールオーバー冗長性を保つようメディアを設定できます。

プライマリおよびセカンダリ フェールオーバー メディアを GE-SFP ポートに割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **hostname** *name*
2. **enable secret** *password*
3. **interface gigabitethernet** *slot/port*
4. **media-type** {**sfp | rj45**} **auto-failover**
5. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**hostname** *name* **例：** `Router(config)# hostname Router`	ルータ名を指定します。
ステップ 2	**enable secret** *password* **例：** `Router(config)# enable secret cr1ny5ho`	ルータへの不正なアクセスを防止するには、暗号化パスワードを指定します。
ステップ 3	**interface gigabitethernet** *slot/port* **例：** `Router(config)# interface gigabitethernet 0/1`	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 4	**media-type {sfp | rj45} auto-failover** **例：** `Router(config-if)# media-type sfp auto-failover` または `Router(config-if)# media-type rj45 auto-failover`	SFP のあるポートを SFP から RJ-45 への自動フェールオーバーのプライマリ メディアとして設定します。 または RJ-45 のあるポートを RJ-45 から SFP への自動フェールオーバーのプライマリ メディアとして設定します。

	コマンド	目的
ステップ 5	**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。

Auto-Detect

Auto-Detect 機能は、media-type が設定されていない場合にイネーブルにされます。この機能により、どのメディアが接続されているか自動的に検出され、リンクが稼動します。両方のメディアが接続されている場合、最初に稼動したメディアのリンクが稼動します。

（注） Auto-Detect 機能は、1000 Base SFP だけで動作します。この機能は、100 Base SFP を検出しません。

Auto-Detect 機能を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface gigabitethernet** *slot/port*
2. **no media-type**
3. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**interface gigabitethernet** *slot/port* **例：** `Router(config)# interface gigabitethernet 0/1`	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	**no media-type** **例：** `Router(config-if)# no media-type` `GigabitEthernet0/1: Changing media to UNKNOWN.` `You may need to update the speed and duplex settings for this interface.`	Auto-Detect をイネーブルにします。1000Base SFP が接続されている場合、速度とデュプレックスは自動的に 1000 および全二重に設定されます。速度とデュプレックス オプションは使用できません。RJ45 接続は、速度 1000 および全二重の場合だけ動作します。SFP が接続されていない場合、RJ45 メディアにはすべての速度およびデュプレックスが使用できます。 **（注）** Auto-Detect 機能は、1000Base SFP だけで動作します。この機能は 100Base SFP を検出しません。
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、グローバル コンフィギュレーション モードに戻ります。

CHAPTER 6

イーサネット スイッチの設定

この章では、次の設定作業の概要について説明します。

- Cisco 860、880、および 890 サービス統合型ルータ（ISR）の 4 ポート ファスト イーサネット（FE）スイッチ
- Cisco 860VAE-K9 のギガビット イーサネット（GE）スイッチ
- Cisco 860 および Cisco 880 シリーズ ISR で内蔵ワイヤレス アクセス ポイントを提供するギガビット イーサネット（GE）スイッチ

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。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。

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。

この章の内容は、次のとおりです。

スイッチ ポートの番号付けと命名

Cisco 860、880、および 890 ISR のポートは、次のように番号が割り当てられています。

- Cisco 860、880、および 890 ISR の FE スイッチのポートには FE0 ～ FE3 の番号が付けられています。
- 860VAE-K9 の GE スイッチのポートには GE0 という番号が付けられます。
- Cisco 860 および Cisco 880 シリーズ ISR で内蔵ワイヤレス アクセス ポイントを提供する GE スイッチのポートには、Wlan-GigabitEthernet0 という名前と番号が付けられます。

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」（P.6-2）
- 「インライン パワー」（P.6-2）
- 「レイヤ 2 イーサネット スイッチング」（P.6-3）
- 「802.1x 認証」（P.6-3）
- 「スパニング ツリー プロトコル」（P.6-3）
- 「Cisco Discovery Protocol」（P.6-3）
- 「スイッチド ポート アナライザ」（P.6-3）
- 「IGMP スヌーピング」（P.6-3）
- 「ストーム制御」（P.6-4）

VLAN および VLAN Trunk Protocol

VLAN および VLAN トランク プロトコル（VTP）の概念については、次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。回路上に電力がある場合、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 スイッチングの詳細については、次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 認証については、次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

（注）　スイッチのトランク インターフェイス モードでの **authentication** コマンドは NEAT 機能に対してイネーブルにされます。これは、Cisco IOS Release 15.2T で使用可能です。

スパニング ツリー プロトコル

スパニング ツリー プロトコルについては、次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（データリンク層）上で動作します。CDP を使用することにより、ネットワーク管理アプリケーションで、既知装置のネイバーであるシスコ製の装置、特に下位レイヤのトランスペアレント プロトコルを実行しているネイバーを検索することができます。ネットワーク管理アプリケーションは CDP によって、近接装置の装置タイプおよび SNMP エージェント アドレスを学習できます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべての LAN および WAN メディア上で動作します。CDP を設定した各デバイスは、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。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つ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 アナライザの詳細については、次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 スヌーピングについては、次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、ソース フィルタリングのサポートを提供します。これにより、マルチ キャストのレシーバ ホストは、レシーバ ホストがマルチキャスト トラフィックを受信するグループ、およびこのトラフィックが予期されるソースから、ルータに対して信号を送信することができます。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 ホストが存在する場合に、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。

ストーム制御

ストーム制御については、次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

SNMP MIB の概要

簡易ネットワーク管理プロトコル（SNMP）の開発と使用は MIB を中心とします。SNMP MIB は抽象的なデータベースで、管理アプリケーションが特定の形式で読み取りおよび変更できる、情報の概念的な仕様です。これは、情報が同じ形式で管理対象システムに保持されているという意味は含まれません。SNMP エージェントでは、管理対象システムの内部データ構造と形式、および MIB 用に定義された外部データ構造と形式の間で変換が行われます。

SNMP MIB は、概念的には、概念上のテーブルを使用するツリー構造です。Cisco レイヤ 2 スイッチング インターフェイス MIB については、「レイヤ 2 イーサネット スイッチングの BRIDGE-MIB」（P.6-4）で詳しく説明します。このツリー構造に対して、MIB という用語は 2 つの意味で使用されます。MIB の定義の 1 つとして、実際には MIB ブランチであることが挙げられ、伝送メディアやルーティング プロトコルなど、通常はテクノロジーの 1 つの側面に関する情報が含まれます。この意味で使用される MIB は、正確には MIB モジュールと呼ばれ、通常は 1 つのドキュメントで定義されます。MIB の他の定義はこのようなブランチの集合です。このような集合体は、たとえば、該当のエージェントによって実装されたすべての MIB モジュール、または、SNMP で定義された MIB モジュールの全体の集まりで構成されます。

MIB は、オブジェクトと呼ばれる、データの個々の項目に分岐されるツリーです。オブジェクトは、たとえば、カウンターまたはプロトコルのステータスです。MIB オブジェクトも、変数と呼ばれることがあります。

レイヤ 2 イーサネット スイッチングの BRIDGE-MIB

レイヤ 2 イーサネットスイッチング インターフェイス BRIDGE-MIB は Cisco 887、880、および 890 プラットフォームでサポートされます。BRIDGE-MIB により、ユーザはイーサネット スイッチ モジュールのメディア アクセス コントロール（MAC）アドレスとスパニング ツリー情報を把握することができます。ユーザは、SNMP プロトコルを使用して MIB エージェントを照会し、MAC アドレスなどのイーサネット スイッチ モジュールの詳細や、各インターフェイスおよびプロトコル情報に関する詳細を取得できます。

ブリッジ MIB はレイヤ 2 BRIDGE-MIB 情報を取得するために次のアプローチを使用します。

- コミュニティ ストリングに基づくアプローチ

- コンテキストに基づくアプローチ

コミュニティ ストリングに基づくアプローチでは、VLAN ごとに、1 個のコミュニティ ストリング作成されます。クエリに基づいて、各 VLAN MIB が表示されます。

BRIDGE-MIB の詳細情報を取得するには、コンフィギュレーション モードで **snmp-server community public RW** コマンドを使用します。

```
Router(config)# snmp-server community public RW
```

SNMP BRIDGE-MIB の詳細をクエリするには、次の構文を使用します。

```
snmpwalk -v2c <ip address of the ISR, …>  public .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@2 .1.3.6.1.2.1.17
snmpwalk -v2c <ip address of the ISR, …>  public@3 .1.3.6.1.2.1.17
```

（注） VLAN「x」を作成すると、論理エンティティ public@x が追加されます。パブリック コミュニティについてクエリを実行すると、レイヤ 3 MIB が表示されます。public@x についてクエリを実行すると、VLAN「x」のレイヤ 2 MIB が表示されます。

コンテキストに基づくアプローチでは、レイヤ 2 インターフェイスの値を表示するために、SNMP コンテキスト マッピング コマンド使用されます。各 VLAN はコンテキストにマッピングされます。ユーザがコンテキストを使用してクエリを実行すると、MIB は、コンテキストにマッピングされた特定の VLAN のデータを表示します。このアプローチでは、各 VLAN はコンテキストに手動でマッピングされます。

BRIDGE-MIB の詳細情報を取得するには、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。

```
Router(config)# Routersnmp-server group public v2c context bridge-group
Router(config)# snmp-server community public RW
Router(config)# snmp-server community private RW
Router(config)# snmp-server context bridge-group
Router(config)# snmp mib community-map public context bridge-group
```

SNMP BRIDGE-MIB の詳細をクエリするには、次の構文を使用します。

```
snmpwalk -v2c <ip address of the ISR, …>  public@1 .1.3.6.1.2.1.17 ?L2-MIB
snmpwalk -v2c <ip address of the ISR, …>  private .1.3.6.1.2.1.17?L3-MIB
```

（注） パブリック コミュニティについてクエリすると、レイヤ 2 MIB が表示されます。レイヤ 3 MIB に対してプライベート グループを使用します。

BRIDGE-MIB の詳細を設定および取得する方法の詳細については、次を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094a9b.shtml#brgmib

MAC アドレス通知

MAC アドレス通知では、スイッチに MAC アドレス アクティビティを保存することでネットワーク上のユーザを追跡できます。スイッチが MAC アドレスを学習または削除した場合は、常に SNMP 通知を生成して NMS に送信することができます。ネットワークから多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減

できます。MAC 通知履歴テーブルは、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、動的でセキュアな MAC アドレスについて生成されます。自己アドレス、マルチキャスト アドレス、またはその他のスタティック アドレスについては、イベントは生成されません。

MAC アドレス通知の設定の詳細については、次を参照してください。

http://www1.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.2_25_see/configuration/guide/swadmin.html#wp1102213

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

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 の VLAN をサポートし、860VAE シリーズ ISR は 5 つの VLAN をサポートします。Cisco 880 シリーズ ISR は 8 の VLAN をサポートします。

（注）　Cisco 866VAE-K9 および 867VAE-K9 ルータには 4 つのファスト イーサネット（FE）スイッチング ポートと 1 つのギガビット イーサネット（GE）スイッチング ポートがあります。

FE および GE スイッチ ポートの 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。

手順の概要

1. **interface** *type number*
2. **shutdown**
3. **switchport access vlan** *vlan_id*
4. **no shutdown**
5. **end**

手順の詳細

	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 fastethernet0`	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** **例：** `Router(config-if)# shutdown`	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。
ステップ 3	**switchport access vlan** *vlan_id* **例：** `Router(config-if)# switchport access vlan 2`	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 4	**no shutdown** **例：** `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。状態が管理ダウンから管理アップに変化します。
ステップ 5	**end** **例：** `Router(config-if)# 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

無線 AP の GE ポートと GE ESW ポートの VLAN

GE ポートはルータの組み込みアクセス ポイントだけを提供する内部インターフェイスであるため、X が 1 以外の場合は、**switchport access vlan X** 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、グローバル 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。

手順の概要

1. **interface** *type number*
2. **switchport mode trunk**
3. **switchport access vlan** *vlan_id*

手順の詳細

	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 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 2	**switchport mode trunk** **例：** `Router(config-if)# switchport mode trunk`	ポートをトランク モードにします。
ステップ 3	**switchport access vlan** *vlan_id* **例：** `Router(config-if)# switchport access vlan 2`	（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 ポートに基づく認証を設定する方法の詳細については、次を参照してください。

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

このマニュアルには、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

このマニュアルには、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 テーブル操作を設定する方法については、次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

このマニュアルには、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。 **maximum** キーワードを指定すると、ダイナミック 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

このマニュアルには、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

スイッチド ポート アナライザ（SPAN）セッションを設定する方法については、次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

このマニュアルには、次の情報が含まれています。

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

インターフェイスでの電力管理の設定

アクセス ポイントまたは Cisco IP Phone のインライン パワーを設定する方法については、次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 スイッチングを設定する方法については、次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#wp1048610

このマニュアルには、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

IGMP スヌーピングの設定

IGMP スヌーピングを設定する方法については、次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

このマニュアルには、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 Release 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を設定する方法については、次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

このマニュアルには、次の情報が含まれています。

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

個別の音声およびデータ サブネットの設定

個別の音声およびデータ サブネットの設定方法については、次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
このマニュアルには、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 サービス統合型ルータ（ISR）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。
- C881-V には 4FXS ポート、2 基の BRI ポートおよび 1 基のバックアップ FXO ポートが装備されています。
- C887VA-V と C887VA-V-W には 4FXS ポートおよび 2 基の BRI ポートが装備されています。

この章の構成は、次のとおりです。

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

モデル番号	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）
C881-V	2	4	1（FXO ポート）
C887VA-V	2	4	—
C887VA-V-W	2	4	—

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。

- 「SIP」（P.7-2）
- 「MGCP」（P.7-3）
- 「H.323」（P.7-3）

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。SIP 検査機能（SIP パケット検査、および小さな穴を検知する機能）、プロトコル確認機能、アプリケーション セキュリティを提供します。ユーザは、SIP トラフィックに適用するポリシー、セキュリティ チェック、および不要なメッセージのフィルタリング

を細かく制御できます。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。

MGCP

Media Gateway Control Protocol（MGCP）RFC 2705 は、Voice over IP（VoIP）を含むマルチメディア アプリケーション作成の集中化アーキテクチャを定義します。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 コンフィギュレーションの情報については、『*Cisco IOS MGCP and Related Protocols Configuration Guide*』の「*Basic MGCP Configuration*」の章の「*Configuring an RGW*」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）
- 「SCCP 制御のアナログ ポートと追加機能」（P.7-4）

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*」

SCCP 制御のアナログ ポートと追加機能

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。サポートする機能は次のとおりです。

- 可聴メッセージ待機表示

- コール転送オプション
- コール パークおよびコール 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
- 三者電話会議
- リダイヤル
- スピード 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 Gateway*」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.7-5）
- 「T.38 ファクス 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, Modem, and Text Services over IP Configuration 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, Modem, and Text Services over IP Configuration 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, Modem, and Text Services over IP Configuration Guide*』の「*Configuring T.37 Store-and-Forward Fax*」の章を参照してください。

T.38 ファクス 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, Modem, and Text Services over IP Configuration 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 の一般的な情報については、『*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*」
- 主要な SRST 機能のコンフィギュレーションについては、『*Cisco Unified SRST System Administrator Guide*』の次の章を参照してください。
  - 「*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 固有の SRST の情報については、『*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、「*4.1 Features*」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、モニタ、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。

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 Cisco サービス統合型ルータ（ISR）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 ソフトウェアへのアップグレード」（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。

無線コンフィギュレーション セッションの開始

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface wlan-ap0** **例：** `Router(config)# interface wlan-ap0` `Router(config-if)#`	ワイヤレス デバイスへの、ルータのコンソール インターフェイスを定義します。 • このインターフェイスは、ルータのコンソールとワイヤレス デバイス間の通信に使用します。 （注）　常にポート 0 を使用します。 • 次のメッセージが表示されます。 `The wlan-ap 0 interface is used for managing the embedded AP. Please use the` **`service-module wlan-ap 0 session`** `command to console into the embedded AP.`
ステップ 2	**ip address** *subnet mask* **例：** `Router(config-if)# ip address 10.21.0.20 255.255.255.0` または `Router(config-if)# ip unnumbered vlan1`	インターフェイス IP アドレスとサブネット マスクを指定します。 （注）　この IP アドレスは、**ip unnumbered vlan1** コマンドを使用することで、Cisco ISR に割り当てられた IP アドレスと共有できます。
ステップ 3	**no 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。

	コマンドまたはアクション	目的
ステップ 4	**interface vlan1** **例：** `Router(config-if)# interface vlan1`	データ通信のために、内部 Gigabit Ethernet（GE0; ギガビット イーサネット）0 ポート上で仮想 LAN インターフェイスを別のインターフェイスに指定します。 • Cisco 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。
ステップ 5	**ip address** *subnet mask* **例：** `Router(config-if)# ip address 10.10.0.30 255.255.255.0`	インターフェイス IP アドレスとサブネット マスクを指定します。
ステップ 6	**exit** **例：** `Router(config-if)# exit` `Router(config)#`	インターフェイス コンフィギュレーション モードを終了し、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 7	**exit** **例：** `Router(config)# exit` `Router#`	グローバル コンフィギュレーション モードを終了します。
ステップ 8	**service-module wlan-ap 0 session** **例：** `Router# service-module wlan-ap0 session` `Trying 10.21.0.20, 2002 ... Open` `ap>`	ワイヤレス デバイスとルータのコンソール間の接続をオープンにします。

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

セッションの終了

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

ワイヤレス デバイス

1. **Control-Shift-6 x**

ルータ

2. **disconnect**
3. Enter キーを 2 回押します。

無線環境の設定

（注）　ワイヤレス デバイスを初めて設定する場合は、基本のワイヤレス設定の前に、アクセス ポイントとルータとの間でコンフィギュレーション セッションを開始する必要があります。「無線コンフィギュレーション セッションの開始」（P.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.8-5）：自律ソフトウェア
- 「Cisco Express 設定」（P.8-4）：ユニファイド ソフトウェア

（注）　自律モードから Unified モードにアップグレードするには、アップグレード手順について、「Cisco Unified ソフトウェアへのアップグレード」（P.8-9）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 ブラウザのツールを使って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 設定

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 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方法の詳細については、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）
- 「無線セキュリティ設定の実行」（P.8-5）
- 「無線 QoS 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。

無線セキュリティ設定の実行

- 「認証の設定」（P.8-5）
- 「WEP および暗号スイートの設定」（P.8-6）
- 「無線 VLAN の設定」（P.8-6）

認証の設定

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

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

認証タイプを選択するには、次の URL で『*Authentication Types for Wireless Devices*』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、次の URL で『*RADIUS and TACACS+ Servers in a Wireless Environment*』を参照してください。

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html

ローカル認証システムとしてのアクセス ポイント設定

ローカルの認証サービスまたはバックアップ認証サービスを障害が発生した WAN リンクまたはサーバに提供するために、アクセス ポイントをローカルの認証サーバとして機能するように設定できます。アクセス ポイントは、Lightweight Extensible Authentication Protocol（LEAP）認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）認証または MAC ベースの認証を使用して最大 50 のワイヤレス クライアント デバイスを認証することができます。このアクセス ポイントは毎秒最大 5 つの認証を実行できます。

ローカル オーセンティケータでのアクセス ポイントの設定は、クライアントのユーザ名とパスワードを使用して手動で行います。これは、ローカル オーセンティケータのデータベースが RADIUS サーバと同期化されないためです。クライアントが使用できる VLAN および SSID のリストを指定できます。

このロールの無線デバイスの設定に関する詳細については、次の URL で『*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

WEP および暗号スイートの設定

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

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された、暗号と完全性アルゴリズムのセットです。Wi-Fi Protected Access（WPA）または Cisco Centralized Key Management（CCKM）を有効にするには、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無線 LAN にとって最適な安全性を提供します。WEP だけしか含まない暗号化スイートでは、最低限のセキュリティしかありません。

暗号化の手順については、次の URL で『*Configuring WEP and Cipher Suites*』を参照してください。

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

無線 VLAN の設定

無線 LAN で VLAN を使用し、SSID を VLAN に割り当てると、「セキュリティの種類」（P.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、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、単一のブリッジング ドメインに接続されている複数のエンド システム（ホスト、またはブリッジやブリッジやルータなどのネットワーク装置）で構成されます。ブリッジング ドメインは、さまざまなネットワーク機器によりサポートされます。ネットワーク機器には、各 VLAN 用の別個のプロトコル グループとともに、ブリッジング プロトコルをそれらの間で動作させる LAN スイッチなどがあります。

無線 VLAN アーキテクチャの詳細については、次の URL で『*Configuring Wireless VLANs*』を参照してください。

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

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

SSID の割り当て

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

複数の SSID の作成の詳細については、次の URL で『*Service Set Identifiers*』を参照してください。

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

Read VLAN を使用しない場合、暗号化設定（WEP と暗号）が 2.4GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN がディセーブルの状態でスタティック WEP を使用する SSID を作成した場合は、WPA 認証を使用する SSID を別途作成できません。使用される暗号化設定が異なるためです。SSID のセキュリティ設定が別の SSID の設定と競合する場合、競合を解消するために 1 つ以上の SSID を削除します。

セキュリティの種類

表 8-1 は、SSID に割り当てられる 4 つのセキュリティ タイプについて説明しています。

表 8-1　SSID セキュリティの種類

セキュリティ タイプ	説明	有効になるセキュリティ機能
セキュリティなし	これは安全性が最も低いオプションです。このオプションは、パブリック スペースで SSID を使用する場合に限定して使用し、ネットワークへのアクセスを制限する VLAN に割り当てる必要があります。	なし。
スタティック WEP キー	このオプションは、「セキュリティなし」よりは安全です。ただし、スタティック WEP キーは攻撃に対して脆弱です。この設定を行う場合は、MAC アドレスに基づいてワイヤレス デバイスにアソシエーションを制限する必要があります。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html の『*Cipher Suites and WEP*』を参照してください。 または ネットワーク内に RADIUS サーバがない場合、アクセス ポイントをローカル認証サーバとして使用するかを検討してください。 手順については、 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html の『*Using the Access Point as a Local Authenticator*』を参照してください。	WEP が必須。ワイヤレス デバイス キーに合う WEP キーがないと、この SSID を使用してもクライアント デバイスをアソシエートできません。

表 8-1　SSID セキュリティの種類 （続き）

セキュリティ タイプ	説明	有効になるセキュリティ機能
EAP[1] 認証	このオプションは、802.1X 認証（LEAP[2]、PEAP[3]、EAP-TLS[4]、EAP-FAST[5]、EAP-TTLS[6]、EAP-GTC[7]、EAP-SIM[8]、およびその他の 802.1X/EAP ベースの製品）がイネーブルになります。 この設定は、必須の暗号化、WEP、オープン認証プラス EAP、ネットワーク EAP 認証を使用し、キー管理なしで RADIUS サーバ認証ポート 1645 を使用します。 ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。802.1x 認証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がありません。	必須の 802.1X 認証。この SSID を使用してアソシエートするクライアント デバイスは、802.1X 認証を実行する必要があります。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
WPA[9]	このオプションは、データベース認証されたユーザにワイヤレス アクセスを許可します。アクセスは認証サーバのサービスを通じて行います。ユーザの IP トラフィックは WEP で使用されるものより強力なアルゴリズムで暗号化されます。 この設定では暗号キー、TKIP[10]、オープン認証プラス EAP、ネットワーク EAP 認証、必須のキー管理 WPA、および RADIUS サーバ認証ポート 1645 を使用します。 EAP 認証の場合と同じように、ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。	WPA 認証が必須。この SSID を使用して対応付けを行うクライアント デバイスは WPA 対応でなければなりません。 ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP によるオープン認証を設定していない場合、以下の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`

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

無線 QoS の設定

Quality of Service（QoS）を設定することで、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。信頼性、遅延限度、またはスループットに関して保証することなく、パケットを送信します。ワイヤレス デバイスに QoS を設定するには、http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html の『*Quality of Service in a Wireless Environment*』を参照してください。

ホット スタンバイ モードでのアクセス ポイントの設定

ホット スタンバイ モードでは、アクセス ポイントは別のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、アクセス ポイントのそばに配置され、それをモニタします（設定は、このアクセス ポイントとまったく同じにします）。スタンバイ アクセス ポイントは、クライアントとしてモニタ対象のアクセス ポイントとアソシエートします。またモニタ対象のアクセス ポイントに、イーサネットおよび無線ポートを通して Internet Access Point Protocol（IAPP; インターネット アクセス ポイント プロトコル）クエリを送信します。モニタするアクセス ポイントから応答がない場合、スタンバイ アクセス ポイントはオンラインに切り替わり、そのアクセス ポイントの役割をネットワーク上で引き継ぎます。

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。モニタ対象アクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがそれを引き継いだ場合、両アクセス ポイントの設定が同一であれば、クライアント デバイスは簡単かつ確実にスタンバイ アクセス ポイントに切り替わることができます。詳細については、次の URL で『*Hot Standby Access Points*』を参照してください。

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

Cisco Unified ソフトウェアへのアップグレード

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

- 「アップグレードの準備」（P.8-9）
- 「アップグレードの実行」（P.8-10）
- 「アクセス ポイントへのソフトウェアのダウンロード」（P.8-11）
- 「アクセス ポイントでのソフトウェア リカバリ」（P.8-12）

ソフトウェア前提条件

- アクセス ポイントが組み込まれた Cisco 890 シリーズ ISR は、IP Base フィーチャ 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、advipservices フィーチャ 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 DHCP サーバ機能を提供します。このアクセス ポイントは WLC と通信し、DHCP プール コンフィギュレーションのコントローラ IP アドレスのオプション 43 を設定します。次の例は、設定サンプルを示しています。

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

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

モード設定がイネーブルになっていることの確認

モードの設定が有効になっていることを確認するには、次の手順を実行します。

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

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

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

ステップ 4　**show boot** コマンドを入力してアクセス ポイントのモード設定がイネーブルになっていることを確認します。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　グレースフル 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。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 プロセスをモニタします。

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 設定」（P.8-4）を参照してください。

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

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

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

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

A. アクセス ポイントでは、起動を試みて失敗したり、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 ポイントへのソフトウェアのダウンロード

アクセス ポイントの起動イメージ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 リカバリ

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。このコマンドを使用すると、アクセス ポイントがブートローダに戻り、手動でイメージをリカバリできるようになります。

注意　このコマンドの使用に当たっては、十分注意してください。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 デザイン	リンク
ワイヤレスの概要	第 2 章「ワイヤレス デバイス概要」
設定	**リンク**
無線の設定	第 9 章「無線の設定」
セキュリティ	**リンク**
『Authentication Types for Wireless Devices』	本マニュアルでは、アクセス ポイントに設定する認証の種類について説明しています。 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
『Using the Access Point as a Local Authenticator』	本マニュアルでは、ローカル認証を担当するアクセス ポイントというロールにおいて、無線デバイスを使用する方法について説明しています。アクセス ポイントは小規模無線 LAN のスタンドアロン認証システムとして機能するか、あるいはバックアップ認証サービスを提供します。ローカル認証を担当するアクセス ポイントは、LEAP、EAP-FAST および MAC ベースの認証を最大 50 個のクライアント デバイスに対して実行します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.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 デザイン	リンク
『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 キー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』	本マニュアルでは、ホット スタンバイ ユニットとしてワイヤレス デバイスを設定する方法を説明しています。 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 Identifier』	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。本マニュアルでは、ワイヤレス デバイス上の SSID の設定および管理方法について説明します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
管理	**リンク**
アクセス ポイントの管理	第 10 章「無線デバイスの管理」
Quality of Service	このマニュアルは、ユーザのシスコ無線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。この機能により、別のトラフィックを犠牲にして特定のトラフィックを優先させることができます。QoS がない場合、デバイスは各パケットに最善のサービスを提供します（パケットの内容やサイズは問いません）。信頼性、遅延限度、またはスループットに関して保証することなく、パケットを送信します。 http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html
『Regulatory Domains and Channels』	本マニュアルには、世界中の規制ドメイン内の Cisco アクセス製品でサポートしている無線チャネルが記載されています。 http://www.cisco.com/en/US/customer/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
『System Message Logging』	本マニュアルでは、ユーザのワイヤレス デバイス上でシステム メッセージ ロギングを設定する方法について説明しています。 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 デザイン	リンク
『Why Migrate to the Cisco Unified Wireless Network?』	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
『Wireless LAN Controller (WLC) FAQ』	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
『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

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はディセーブルに設定されています。

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

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

手順の概要

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

手順の詳細

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

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

ワイヤレス ネットワークでのロールの設定

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

- アクセス ポイント
- アクセス ポイント（無線シャットダウンにフォールバック）
- ルート ブリッジ
- 非ルート ブリッジ
- ワイヤレス クライアントを持つルート ブリッジ
- ワイヤレス クライアントを備えていない非ルート ブリッジ

ルート アクセス ポイントにフォールバック ロールを設定することもできます。ワイヤレス デバイスは、イーサネット ポートがディセーブルになるか、または有線 LAN から切り離されたときに自動的にフォールバック ロール（モード）に移行します。Cisco ISR ワイヤレス デバイスのデフォルトのフォールバック ロールは次のとおりです。

Shutdown：ワイヤレス デバイスは無線をシャットダウンし、すべてのクライアント デバイスの接続を解除します。

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**station-role** **non-root** {**bridge** | **wireless-clients**} **root** {**access-point** | **ap-only** | **[bridge** | **wireless-clients]** | **[fallback** | **repeater** | **shutdown]**} **workgroup-bridge** {**multicast** | **mode** <*client* | *infrastructure*>| **universal** <*Ethernet client MAC address*>}	ワイヤレス デバイスロールを設定します。 • 有線または無線クライアントを備えた非ルート ブリッジ、ルート アクセス ポイントまたはブリッジ、またはワークグループ ブリッジへのロールを設定します。 （注） **bridge** モードの無線でサポートするには、ポイントツーポイント設定だけです。 （注） **repeater** コマンドおよび **wireless-clients** コマンドは、Cisco 860 シリーズおよび Cisco 880 シリーズのサービス統合型ルータ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 シリーズのサービス統合型ルータではサポートされません。 • いずれかの無線がリピータとして設定されると、イーサネット ポートはシャットダウンします。ワークグループ ブリッジまたはリピータとして設定できるのは、アクセス ポイントにつき 1 つの無線だけです。ワークグループ ブリッジは、ルート ブリッジまたはアクセス ポイントに別のワイヤレス クライアントが関連付けられていなければ、最大 25 クライアントを保持できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

無線トラッキング

アクセス ポイントのいずれかの無線の状態を追跡またはモニタするようにアクセス ポイントを設定できます。追跡した無線が停止またはディセーブルになった場合、アクセス ポイントにより他の無線がシャットダウンされます。追跡対象の無線が起動すると、アクセス ポイントは別の無線をイネーブルにします。

Radio 0 を追跡するには、次のコマンドを入力します。

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

ファスト イーサネット トラッキング

アクセス ポイントのイーサネット ポートがディセーブルになったり、または有線 LAN から切断されたりしたときにフォールバックするようにアクセス ポイントを設定できます。ファスト イーサネット トラッキング用にアクセス ポイントを設定する方法については、「ワイヤレス ネットワークでのロールの設定」（P.9-3）を参照してください。

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

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

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

MAC アドレス トラッキング

MAC アドレスを使用して別の無線に接続しているクライアント アクセス ポイントをトラッキングし、ルート アクセス ポイントの起動と停止の役割を果たす無線を設定できます。クライアントとアクセス ポイントのアソシエーションが解除されると、ルート アクセス ポイントの無線はダウンします。クライアントがアクセス ポイントと再アソシエートすると、ルート アクセス ポイント無線は起動状態に戻ります。

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

たとえば、MAC アドレスが 12:12:12:12:12:12 のクライアントを追跡するには、次のコマンドを入力します。

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

無線データ レートの設定

データ レート設定を使用して、ワイヤレス デバイスのデータ転送に使用されるデータ レートを選択します。データ レートの単位は Mbps（メガビット/秒）です。ワイヤレス デバイスでは、常に、最大データ レートでデータ セットを **basic** に転送します。これは、ブラウザ ベース インターフェイスでは、**required** として知られています。障害や干渉などがある場合、ワイヤレス デバイスはデータ送信が可能な範囲での最速レートまで減速されます。各データ レートは、次の 3 つのステートのいずれかに設定できます。

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

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

データ レート設定を使用して、特定のデータ レートで稼動中のサービス クライアント デバイスにアクセス ポイントを設定できます。たとえば、11Mbps サービスでだけ 2.4GHz 無線の転送を設定する場合は、11Mbps レートを **basic** に設定し、他のデータ レートを **disabled** に設定します。ワイヤレス デバイスを 1 および 2 Mbps で稼動するクライアント デバイスにだけサービスを提供するように設定するには、**basic** に 1 および 2 を設定し、データ レートを **disabled** に設定します。802.11g クライアント デバイスにだけサービスを提供するように 2.4GHz、802.11g 無線を設定するには、Orthogonal Frequency Division Multiplexing（OFDM; 直交周波数分割多重方式）のデータ レート（6、9、12、18、24、36、48、54）を、すべて **basic** に設定します。54 Mbps サービスに対応する 5-GHz 無線だけを設定する場合は、54 Mbps レートを **basic** に設定し、他のデータ レートを **disabled** に設定します。

また、範囲またはスループットが最適になるようなデータ レートが自動的に設定されるように、ワイヤレス デバイスを設定することも可能です。データ レート設定に **range** を入力すると、ワイヤレス デバイスにより 1Mbps レートが **basic** に設定され、その他のレートが **enabled** に設定されます。この range 設定によって、アクセス ポイントではデータ レートを下げることでカバレッジ領域を拡大できます。したがって、他のクライアントは接続できるのにアクセス ポイントに接続できないクライアントがある場合は、そのクライアントがアクセス ポイントの適用範囲内に入っていないことが考えられます。このような場合、範囲オプションを使用することにより適用範囲を拡大すると、クライアントがアクセス ポイントに接続できるようになる可能性があります。

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

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

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

手順の概要

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

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

手順の詳細

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

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

	コマンドまたはアクション	目的
	speed（続き）	5 GHz 無線で、**default** オプションは、レート 6.0、12.0、および 24.0 を **basic** に、レート 9.0、18.0、36.0、48.0、および 54.0 を **enabled** に設定します。 802.11g/n 2.4 GHz 無線で、**default** オプションは、レート 1.0、2.0、5.5、および 11.0 を **enabled** に設定します。 802.11g/n 5 GHz 無線で、**default** オプションは、レート 6.0、12.0、および 24.0 を **enabled** に設定します。 どちらの 802.11g/n 無線の Modulation Coding Scheme（MCS; 変調符号化方式）インデックス範囲も 0 ～ 15 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定から 1 つ以上のデータ レートを削除するには、**speed** コマンドの **no** 形式を使用します。この例では、データレート **basic-2.0** および **basic-5.5** を設定から削除する方法を示します。

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

MCS レートの設定

Modulation Coding Scheme（MCS; 変調符号化方式）は、変調順序（2 位相偏移変調 [BPSK]、4 位相偏移変調 [QPSK]、16- 直交振幅変調 [16-QAM]、64-QAM）から成る PHY パラメータおよび Forward Error Correction（FEC; 前方誤り訂正）コード レート（1/2、2/3、3/4、5/6）の仕様です。MCS は、ワイヤレス デバイス 802.11n 無線で使用されており、32 個の対称設定を定義します（空間ストリームあたり 8 個）。

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

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

MCS は高いスループットを実現する可能性があるため、重要な設定です。高スループット データ レートは、*MCS*、*帯域幅*、および*ガード インターバル*の機能です。802.11a、b、および g 無線では、20-MHz チャネル幅を使用しています。表 9-1 は、MCS、ガード インターバル、およびチャネル幅に基づく潜在的なデータ レートを示します。

表 9-1　MCS 設定、ガード インターバル、およびチャネル幅に基づくデータ レート

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

レガシー レートは次のとおりです。

5 GHz: 6、9、12、18、24、36、48、および 54 Mbps

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

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

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 800test
    !
    speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4.
    m8. m9. m10. m11. m12. m13. m14. m15.
```

無線の送信電力の設定

無線の送信電力は、使用するアクセス ポイントに導入されている 1 つ以上の無線のタイプと、アクセス ポイントが動作する規制ドメインに基づきます。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 2.4-GHz および 802.11g/n 2.4-GHz は radio 0 です。
ステップ 3	**power local** これらのオプションは、2.4-GHz 802.11n 無線で使用できます（単位は dBm）。 {**8** | **9**| **11** | **14** | **15** | **17** | **maximum**}	規制ドメインにおいて電力レベルが許容範囲内となるように、2.4 GHz 無線に送信電力を設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

アソシエートしたクライアント デバイスの電力レベルの制限

ワイヤレス デバイスにアソシエートしたクライアント デバイスの電力レベルを制限することもできます。クライアント デバイスがワイヤレス デバイスにアソシエートするとき、ワイヤレス デバイスはクライアントに最大電力レベル設定を送信します。

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz および 2.4-GHz は radio 0 です。
ステップ 3	**power client** 次のオプションは、802.11n、2.4GHz クライアントについて使用できます（単位 dBm）。 {**local** | **8** | **9** | **11** | **14** | **15** | **17** | **maximum**}	ワイヤレス デバイスに関連付けるクライアント デバイスで許可される最大電力レベルを設定できます。 • 電力レベルを **local** に設定すると、クライアントの電力レベルはアクセス ポイントの電力レベルに設定されます。 • 電力レベルを **maximum** に設定すると、クライアントの電力は最大許可電力に設定されます。 **（注）** 規制ドメインで許容される設定は、ここで取り上げる設定と異なる場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

関連付けたクライアントの最大電力レベルをディセーブルにするには、**power client** コマンドの **no** 形式を使用します。

（注） アソシエートしたクライアント デバイスの電力レベルを制限する場合は、Aironet 拡張機能をイネーブルにする必要があります。Aironet 拡張機能はデフォルトではイネーブルに設定されています。

無線チャネルの設定

ワイヤレス デバイス無線のデフォルト チャネル設定は least congested です。ワイヤレス デバイスでは、起動時に最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。ワイヤレス デバイスのチャネル設定は、規制ドメインで使用できる周波数に対応します。ドメインで許可されている周波数については、アクセス ポイントのハードウェア インストレーション ガイドを参照してください。

2.4GHz 帯チャネル利用帯域幅は、チャネルあたり 22MHz になります。チャネル 1、6、および 11 の帯域は重複しないため、干渉を起こさずに、同じ圏内に複数のアクセス ポイントを設定できます。802.11b および 802.11g の 2.4GHz 無線は同じチャネルと周波数を使用します。

5GHz 無線は、規制ドメインに応じて 5180 ～ 5320MHz の 8 チャネルから、最大 5170 ～ 5850 MHz の 27 チャネルで稼動します。各チャネルの帯域幅は 20 MHz で、それぞれの帯域がわずかに重複しています。最適なパフォーマンスを得るため、互いに近い位置にある無線の場合は、隣接していないチャネル（たとえば、チャネル 44 と 46）を使用してください。

（注） 同じ圏内に多くのアクセス ポイントが存在すると、スループットの減少の原因となる無線輻輳が発生します。無線のサービス範囲とスループットを最大にするには、慎重なサイト調査を行って、アクセス ポイントの最適な設置場所を決定する必要があります。

802.11n チャネル幅

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

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

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** }	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	ワイヤレス デバイスの無線のデフォルト チャネルを設定します。起動時に最も混雑していないチャネルを検索するには、**least-congested** を入力します。 • 使用する帯域幅を指定するには **width** オプションを使用します。このオプションは、Cisco 800 シリーズ ISR ワイヤレス デバイスで使用できます。使用可能な設定は、**20**、**40-above**、および **40-below** の 3 つです。 – **20** を選択すると、チャネル幅が 20 MHz に設定されます。 – **40-above** を選択すると、拡張チャネルをコントロール チャネルの上に重ねた状態でチャネル幅が 40 MHz に設定されます。 – **40-below** を選択すると、拡張チャネルをコントロール チャネルの下に重ねた状態でチャネル幅が 40 MHz に設定されます。 **（注）** 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 5GHz の無線については、**channel** コマンドはディセーブルに設定されています。詳細については、「ワールド モードのイネーブル化とディセーブル化」（P.9-14）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワールド モードのイネーブル化とディセーブル化

ワイヤレス デバイスで、802.11d ワールド モード、Cisco レガシー ワールド モード、またはワールド モード ローミングをサポートするよう設定できます。ワールド モードをイネーブルにすると、ワイヤレス デバイスはそのビーコンにチャネル キャリア設定情報を追加します。ワールド モードがイネーブルになっているクライアント デバイスは、キャリア セット情報を受信して、それぞれの設定を自動的に調整します。たとえば、日本で主に使用されるクライアント デバイスがイタリアに移され、そこでネットワークに参加した場合、ワールド モードに依存して、そのチャネルと電力の設定を自動的に調整することができます。シスコ クライアント デバイスでは、ワイヤレス デバイスが 802.11d を使用しているのか、あるいはシスコ レガシー ワールド モードによりワイヤレス デバイスで使用されているモードに一致するワールド モードを自動的に使用しているのかを検出します。

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

ワールド モードはデフォルトではディセーブルに設定されています。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**world-mode** {**dot11d country_code** *code* {**both** | **indoor** | **outdoor**} | **world-mode roaming** | **legacy**}	ワールド モードをイネーブルにします。 • 802.11d ワールド モードをイネーブルにするには、**dot11d** オプションを入力します。 – **dot11d** オプションを入力する場合、2 文字の ISO 国番号（たとえば、米国の ISO 国番号は **US**）を入力する必要があります。ISO 国番号の一覧は ISO の Web サイトに掲載されています。 – 国番号の後に、ワイヤレス デバイスの配置場所を示すために **indoor**、**outdoor**、または **both** と入力します。 • シスコのレガシー ワールド モードをイネーブルにするには、**legacy** オプションを入力します。 • **world-mode roaming** オプションを入力し、継続的なワールド モード コンフィギュレーションでアクセス ポイントを配置します。 **（注）** レガシー ワールド モードを使用するには、Aironet 拡張機能をイネーブルにする必要がありますが、802.11d ワールド モードではこの拡張機能は不要です。Aironet 拡張機能はデフォルトではイネーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワールド モードをディセーブルにするには、**world-mode** コマンドの **no** 形式を使用します。

short 無線プリアンブルのイネーブル化とディセーブル化

無線プリアンブル（ヘッダーと呼ばれる場合もある）は、パケットの先頭にあるデータ部です。ここには、ワイヤレス デバイスとクライアント デバイスのパケットの送受信に必要な情報が含まれています。無線プリアンブルを long または short に設定できます。

- Short : short プリアンブルを使用すると、スループットのパフォーマンスが向上します。
- Long : long プリアンブルは、ワイヤレス デバイスと初期の Cisco Aironet 無線 LAN アダプタのすべてのモデル間との互換性を確保します。これらのクライアント デバイスがワイヤレス デバイスにアソシエートしない場合、short プリアンブルを使用する必要があります。

5GHz 無線では無線プリアンブルに short と long を設定できません。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0** }	2.4-GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no preamble-short**	short プリアンブルをディセーブルにし、long プリアンブルをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

デフォルトでは short プリアンブルがイネーブルに設定されています。short プリアンブルがディセーブルになっている場合、イネーブルにするには **preamble-short** コマンドを使用します。

送受信アンテナの設定

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

- Gain : 対称のアンテナ ゲインをデシベル（dB）で設定します。

- Diversity：デフォルト設定。最適な信号を受信するアンテナがワイヤレス デバイスで使用されます。ワイヤレス デバイスに 2 つの固定（取り外し不能）アンテナが使用されている場合は、受信と送信の両方にこの設定を使用します。
- Right：ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの右側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、右にあるのが右側のアンテナになります。
- Left：ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの左側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、左にあるのが左側のアンテナになります。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**gain** *dB*	デバイスに接続されたアンテナの結果のゲインを指定します。 • –128 ～ 128 dB の値を入力します。必要に応じて、1.5 などの小数値を使用できます。 **（注）** Cisco 860 および Cisco 880 ISR は、取り外しできない固定アンテナを付けて出荷されています。これらのモデルにアンテナ ゲインを設定できません。
ステップ 4	**antenna receive** {**diversity	left	right**}	受信アンテナを diversity、left、または right に設定します。 **（注）** 2 つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの **diversity** を使用します。1 つのアンテナの場合、アンテナを右側に取り付け、アンテナを **right** に設定します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Aironet 拡張機能のディセーブル化およびイネーブル化

デフォルトでは、ワイヤレス デバイスは Cisco Aironet 802.11 拡張機能を使用して、Cisco Aironet クライアント デバイスの機能を検出し、ワイヤレス デバイスと関連付けられているクライアント デバイス間との特別な相互作用を必要とする機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- ロード バランシング：ワイヤレス デバイスでは、Aironet 拡張機能を使用して、クライアント デバイスに対し、ネットワークに対する最適な接続を提供するアクセス ポイントを指示します。この場合、そのような要素の基準となるのは、ユーザ数、ビット誤り率、および信号強度です。
- Message Integrity Check（MIC; メッセージ完全性チェック）：暗号化されたパケットへの攻撃（ビットフリップ攻撃）を阻止するために新しく追加された WEP セキュリティ機能。MIC は、ワイヤレス デバイスおよび関連付けられているすべてのクライアント デバイスに実装され、数バイトを各パケットに付加することによって、パケットの不正改ざんを防止します。
- Cisco Key Integrity Protocol（CKIP; シスコ キー整合性プロトコル）：シスコの WEP キー置換技術で、IEEE 802.11i セキュリティ タスク グループにより開示された初期のアルゴリズムに基づいています。標準ベースのアルゴリズムである Temporal Key Integrity Protocol（TKIP; 一時キー整合性プロトコル）の場合は、Aironet 拡張機能をイネーブルにする必要はありません。
- ワールド モード（レガシーのみ）：レガシー ワールド モードがイネーブルになっているクライアント デバイスは、ワイヤレス デバイスからキャリア セット情報を受信して、それぞれの設定を自動的に調整します。802.11d ワールド モードを使用する場合、Aironet 拡張機能は不要です。
- アソシエートされたクライアント デバイスの電力レベルの制限：クライアント デバイスがワイヤレス デバイスにアソシエートするとき、そのワイヤレス デバイスは最大許可電力レベル設定をクライアントに送信します。

Aironet 拡張機能をディセーブルにすると、上記の機能はディセーブルになりますが、シスコ以外のクライアント デバイスがワイヤレス デバイスにアソシエートしやすくなる場合があります。

Aironet 拡張機能はデフォルトではイネーブルに設定されています。Aironet 拡張機能をディセーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0}**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**no dot11 extension aironet**	Aironet 拡張機能をディセーブルにします。

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

Aironet 拡張機能がディセーブルになっている場合、イネーブルにするには **dot11 extension aironet** コマンドを使用します。

イーサネット カプセル化変換方式の設定

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

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**payload-encapsulation** {**snap** | **dot1h**}	カプセル化トランスフォーメーション方式を RFC 1042（**snap**）または 802.1h（**dot1h**、デフォルト設定）に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

Public Secure Packet Forwarding（PSPF; パブリック セキュア パケット フォワーディング）では、アクセス ポイントに関連付けられているクライアント デバイスがアクセス ポイントに関連付けられている他のクライアント デバイスと何らかの理由によりファイルを共有したり通信したりしないように防止します。PSPF は、LAN のその他の機能を提供せずにクライアント デバイスに対するインターネット アクセスを提供します。この機能は、空港や大学の構内などに敷設されている公衆ワイヤレス ネットワークに有用です。

（注）　異なるアクセス ポイントにアソシエートするクライアント間での通信を防ぐために、ワイヤレス デバイスを接続するスイッチに保護ポートを設定する必要があります。保護ポートの設定方法については、「保護ポートの設定」（P.9-21）を参照してください。

ワイヤレス デバイス上で CLI コマンドを使用して PSPF をイネーブルまたはディセーブルにするには、ブリッジ グループを使用します。次の文書に、ブリッジ グループに関する詳細な説明と、ブリッジ グループを実装する手順が収められています。

- 『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』。次のリンクをクリックすると、「Configuring Transparent Bridging」の章を参照できます。

  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に設定されています。PSPF をイネーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**bridge-group** *group* **port-protected**	PSPF をイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

保護ポートの設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。 • **wlan-gigabitethernet0** など、設定を行う交換機ポート インターフェイスのタイプと番号を入力します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、**no switchport protected** コマンドを使用します。

保護ポートとポート ブロッキングについての詳細は、『*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。次のリンクをクリックすると上記のガイドを参照できます。

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

ビーコン間隔と DTIM の設定

ビーコン期間は、アクセス ポイント ビーコン間の時間数をキロマイクロ秒（Kmicrosecs）で表したものです。1 キロマイクロ秒は 1,024 マイクロ秒に相当します。データ ビーコン レートは常にビーコン期間の倍数で、ビーコンにどの程度の頻度で Delivery Traffic Indication Message（DTIM; デリバリー トラフィック インディケーション メッセージ）が含まれるかを決定します。DTIM は、省電力モードのクライアント デバイスに、パケットがクライアント待ちであることを通知します。

たとえば、ビーコン期間がデフォルトとして 100 に設定されており、データ ビーコン レートが 2 に設定されているとすると、ワイヤレス デバイスでは 200 キロマイクロ秒ごとに DTIM を 1 個含むビーコンを送信します。

デフォルトのビーコン間隔は 100、デフォルトの DTIM は 2 です。ビーコン期間および DTIM を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**beacon period** *value*	ビーコン期間を設定します。 • 値をキロマイクロ秒単位で入力します。
ステップ 4	**beacon dtim-period** *value*	DTIM を設定します。 • 値をキロマイクロ秒単位で入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RTS しきい値と再試行回数の設定

Request to Send（RTS; 送信要求）しきい値は、パケット送信前にワイヤレス デバイスが RTS を発行するときの基準となるパケット サイズを決定します。多くのクライアント デバイスがワイヤレス デバイスに関連付けられていたり、クライアントが互いに離れていて、ワイヤレス デバイスを検出できても相互に検出できないエリアでは、RTS しきい値設定が小さいほうが便利なことがあります。0 ～ 2347 バイトの範囲で設定を入力できます。

最大 RTS 再試行回数は、ワイヤレス デバイスが無線を介したパケット送信の試行を中止するまでに RTS を発行する最大回数です。1 ～ 128 の範囲の値を入力します。

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 2.4-GHz および 802.11g/n 2.4-GHz は radio 0 です。
ステップ 3	**rts threshold** *value*	RTS しきい値を設定します。 • RTS しきい値として 0 ～ 2347 を入力します。
ステップ 4	**rts retries** *value*	最大 RTS 再試行回数を入力します。 • 1 ～ 128 の範囲の値を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

RTS 設定をデフォルトにリセットするには、**rts** コマンドの **no** 形式を使用します。

最大データ再試行回数の設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**packet retries** *value*	最大データ再試行回数を入力します。 • 1 ～ 128 の範囲の値を入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトにリセットするには、**packet retries** コマンドの **no** 形式を使用します。

フラグメンテーションしきい値の設定

フラグメンテーションしきい値は、パケットのフラグメント化（ブロックではなく断片化して送信）のサイズを決定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。デフォルト設定は 2346 バイトです。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio** {**0**}	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 • 802.11g/n 2.4-GHz および 5-GHz は radio 0 です。
ステップ 3	**fragment-threshold** *value*	フラグメンテーションしきい値を設定します。 • 2.4GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。 • 5GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	(任意）コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトにリセットするには、**fragment-threshold** コマンドの **no** 形式を使用します。

802.11g 無線の short スロット時間のイネーブル化

802.11g 2.4-GHz 無線のスループットの向上に、short スロット時間を使用できます。スロット時間を標準の 20 マイクロ秒から 9 マイクロ秒の short スロット時間まで短縮すると、全体のバックオフが減少し、スループットが向上します。バックオフは、スロット時間の倍数であり、LAN 上にパケットを送信するまでにステーションが待機するランダムな長さの時間です。

多くの 802.11g 無線は short スロット時間をサポートしていますが、サポートしていないものもあります。short スロット時間をイネーブルにすると、ワイヤレス デバイスでは、802.11g 2.4-GHz 無線に関連付けられているすべてのクライアントが short スロット時間をサポートしているときにだけ short スロット時間を使用します。

Short スロット時間は、802.11g 2.4-GHz 無線上でだけサポートされています。short スロット時間は、デフォルトではディセーブルに設定されています。

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

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

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

キャリア ビジー テストの実行

キャリア ビジー テストを実行して、ワイヤレス チャネルでの無線活動をチェックします。キャリア ビジー テストでは、キャリア検査を実行して検査結果を表示するまでの約 4 秒間、ワイヤレス デバイスはワイヤレス ネットワーキング デバイスとのアソシエーションをすべて停止します。

特権 EXEC モードで、次のコマンドを入力して、キャリア ビジー テストを実行します。

dot11 *interface-number* **carrier busy**

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

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

VoIP パケット処理の設定

アクセス ポイントの無線ごとの VoIP パケット処理の質は、Class of Service（CoS; クラス サービス）5（ビデオ）および CoS 6（音声）ユーザ プライオリティの低遅延における 802.11 MAC 動作を強化することで改善できます。

アクセス ポイントの VoIP パケット処理を設定するには、次のステップに従います。

ステップ 1　ブラウザを使用して、アクセス ポイントにログインします。

ステップ 2　Web ブラウザ インターフェイスの左側にあるタスク メニューで [Services] をクリックします。

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

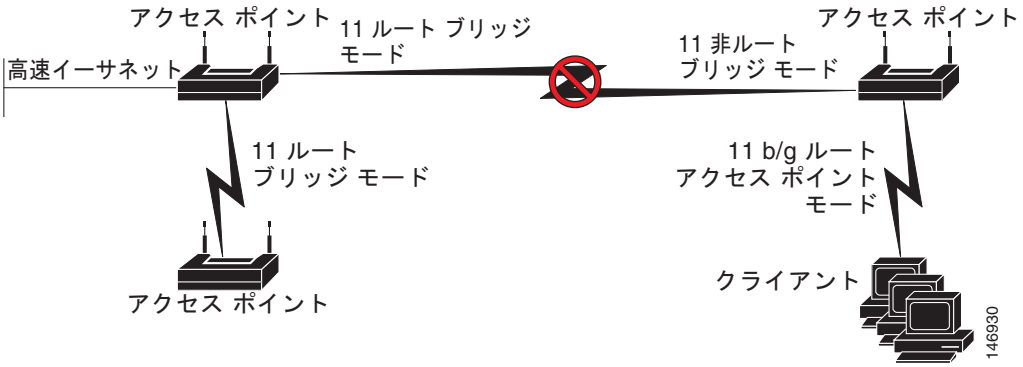
[Stream] ページが表示されます。

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）および CoS 6（音声）ユーザ設定のどちらについても、[Packet Handling] ドロップダウン メニューから [Low Latency] を選択し、対応するフィールドにパケット破棄の最大再試行回数の値を入力します。

最大再試行回数のデフォルト値は、Low Latency 設定では 3 です（図 1）。この値は、損失したパケットを廃棄する前に、アクセス ポイントがパケットを取得しようとする回数を示します。

図 1　　パケット処理の設定



（注）　CoS 4（負荷制御）ユーザの優先順位およびその最大再試行回数も設定できます。

ステップ 6　[Apply] をクリックします。

CLI を使用して VoIP パケット処理を設定することも可能です。CLI を使用して VoIP パケット処理を設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

CHAPTER 10

無線デバイスの管理

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。

無線デバイスへのアクセスのセキュリティ保護

アクセス ポイントのハードウェアおよびソフトウェアの管理

無線デバイスの通信管理

モード ボタン機能のディセーブル化

無線デバイスの MODE ボタンをディセーブルにするには、**[no] boot mode-button** コマンドを使用します。

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

（注）　無線デバイスをリブートするには、ルータの Cisco IOS CLI から **service-module wlan-ap reset** コマンドを使用してください。このコマンドの詳細については、「無線デバイスのリブート」（P.10-22）を参照してください。

MODE ボタンはデフォルトでイネーブルに設定されています。アクセス ポイントの MODE ボタンをディセーブルにするには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **no boot mode-button**
3. **end**

手順の詳細

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

モード ボタンのステータスを確認するには、特権 EXEC モードで **show boot** または **show boot mode-button** コマンドを実行します。設定の実行時には、ステータスが表示されません。**show boot** および **show boot mode-button** コマンドを実行すると、通常は次のような応答が表示されます。

```
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 パスワードがわかっていれば、**boot mode-button** コマンドを使用して、モード ボタンを通常動作に復旧できます。

アクセス ポイントへの不正アクセスの防止

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

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

- ワイヤレス デバイスでローカルに保存されるユーザ名とパスワードの組み合わせ。このペアによって、各ユーザは、ワイヤレス デバイスにアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り / 書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細については、「ユーザ名とパスワードのペアの設定」（P.10-8）を参照してください。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。ユーザ名とパスワードでは、大文字と小文字が区別されます。

  （注）　TAB、?、$、+、および [は、パスワードに無効な文字です。

- ユーザ名と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一元的に保管されます。詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」（P.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

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

（注）　ここで使用す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 ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。内容は次のとおりです。

- 「デフォルト パスワードと特権レベルの設定」（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.10-4）
- 「暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護」（P.10-6）
- 「ユーザ名とパスワードのペアの設定」（P.10-8）
- 「複数の特権レベルの設定」（P.10-9）

デフォルト パスワードと特権レベルの設定

表 10-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 10-1　デフォルト パスワードと特権レベル

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

スタティック イネーブル パスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。

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

特権 EXEC モードから静的 enable パスワードを設定または変更するには、次のステップを実行します。

手順の概要

1. **configure terminal**
2. **enable password** *password*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**enable password** *password*	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 • デフォルトのパスワードは *Cisco* です。 • *password* : 1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。スペースを使用できますが、先頭のスペースは無視されます。パスワードには疑問符（?）を含めることができます。その場合はパスワードを作成するときに、疑問符を入力する前に Ctrl キーを押した状態で V キーを押してください。たとえば、パスワード abc?123 を作成する場合は、次のように入力します。 **1.** **abc** と入力します。 **2.** Crtl+V キーを押します。 **3.** **?123** と入力します。 • イネーブル パスワードを入力するよう求められた場合は Ctrl+V キーを入力する必要はありません。パスワード プロンプトで **abc?123** と入力します。 **（注）** TAB、?、$、+、および [は、パスワードに無効な文字です。
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**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例は、enable パスワードを *l1u2c3k4y5* に変更する方法を示しています。このパスワードは暗号化されず、レベル 15 へのアクセス（標準の特権 EXEC モード アクセス）を可能にします。

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

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特にネットワーク間を行き交う、または TFTP サーバに保存されるパスワードに対してセキュリティ レイヤを追加するには、グローバル コンフィギュレーション モードで **enable password** コマンドまたは **enable secret** コマンドのいずれかを使用できます。いずれのコマンドを使用しても、ユーザが特権 EXEC モード（デフォルト）にアクセスするために、または指定した特権レベルにアクセスするために入力が必要な暗号化パスワードを設定できます。

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

enable secret コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。これら 2 つのコマンドを同時に有効にすることはできません。

enable パスワードおよび enable secret パスワードに暗号化を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **enable password** [**level** *level*] {*password* | *encryption-type encrypted*-**password**}
   または
   enable secret [**level** *level*] {*password* | *encryption-type encrypted*-**password**}
3. **service password-encryption**
4. **end**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password}	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。
	または	または
	enable secret [**level** *level*] {*password* | *encryption-type encrypted*-password}	シークレット パスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。 • *level*：（任意）範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です（特権 EXEC モード権限）。 • *password*：1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。スペースを使用できますが、先頭の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。 • *encryption-type*：（任意）5 だけを入力してください。シスコ独自の暗号化アルゴリズムを使用できます。暗号化タイプを指定する場合は、別のアクセス ポイントの無線デバイスの設定からコピーした暗号化パスワードを指定する必要があります。 **（注）** 暗号化タイプを指定し、クリア テキスト パスワードを入力した場合は特権 EXEC モードを再開できません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。
ステップ 3	**service password-encryption**	（任意）パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。 暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したら、特権レベルにアクセスする必要のあるユーザだけにパスワードを通知してください。さまざまなレベルにアクセス可能なコマンドを指定する場合は、グローバル コンフィギュレーション モードで **privilege level** コマンドを使用します。詳細については、「複数の特権レベルの設定」（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すると、ユーザ名パスワード、認証キー パスワード、特権コマンド パスワード、コンソール パスワード、および仮想端末の回線パスワードを含む、すべてのパスワードに適用されます。

パスワードとレベルを削除するには、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 に対して暗号化パスワード *1FaD0$Xyti5Rkls3LoyxzS8* を設定する例を示します。

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

ユーザ名とパスワードのペアの設定

ワイヤレス デバイスでローカルに保存されるユーザ名とパスワードの組み合わせを設定します。ユーザ名とパスワードのペアは回線またはインターフェイスに割り当てられ、これらのペアにより、各ユーザはワイヤレス デバイスにアクセスする前に認証されます。特権レベルを定義したら、ユーザ名とパスワードの各ペアに特定の特権レベルを（対応する権限とともに）指定します。

ログイン ユーザ名とパスワードを要求するユーザ名ベースの認証システムを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
3. **login local**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	各ユーザのユーザ名、特権レベル、およびパスワードを入力します。 • *name*：1 語でユーザ ID を指定します。スペースや引用符は使用できません。 • *level*：（任意）ユーザがアクセス権を取得した後に持つ特権レベルを指定します。範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type*：暗号化されていないパスワードが続くことを指定する場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • *password*：ワイヤレス デバイスにアクセスするためにユーザが入力する必要があるパスワード。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。
ステップ 3	**login local**	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
ステップ 4	**end**	特権 EXEC 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 5	**show running-config**	入力を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

特定のユーザに対して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、パスワードを指定しない接続を許可するには、回線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 つ設定する必要があります。また、ワイヤレス デバイスとの Telnet セッションを開くように login local を設定する必要があります。ユーザ名が 1 つだけの場合にそのユーザ名を入力しないと、ワイヤレス デバイスからロックアウトされることがあります。

複数の特権レベルの設定

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

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。**configure** コマンドへのアクセスを制限する場合は、レベル 3 のセキュリティを割り当て、制限されたユーザのグループにそのパスワードを配布できます。

この項では、設定情報について説明します。

- 「コマンドの特権レベルの設定」（P.10-9）
- 「特権レベルへのログインと終了」（P.10-11）

コマンドの特権レベルの設定

コマンド モードに特権レベルを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **privilege** *mode* **level** *level command*
3. **enable password level** *level password*
4. **end**
5. **show running-config**
   または
   show privilege
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**privilege** *mode* **level** *level command*	コマンドの特権レベルを設定します。 • *mode*：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** と入力します。 • *level*：範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって許可されるアクセス レベルです。 • *command*：アクセスが制限されるコマンドを指定します。
ステップ 3	**enable password level** *level password*	特権レベルの enable パスワードを指定します。 • *level*：範囲は 0 ～ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。 • *password*：1 ～ 25 文字の英数字の文字列。文字列を数字で始めることはできません。大文字と小文字が区別されます。スペースを使用できますが、先頭の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 [は、パスワードに無効な文字です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	入力を確認します。 **show running-config** コマンドを実行すると、パスワードとアクセス レベルの設定が表示されます。 **show privilege** コマンドを実行すると、特権レベルの設定が表示されます。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

特定のコマンドの特権をデフォルトに戻すには、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。

次の例は、**configure** コマンドを特権レベル 14 に設定し、ユーザがレベル 14 のコマンドを使用する場合に入力するパスワードとして *SecretPswd14* を定義する方法を示しています。

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

特権レベルへのログインと終了

指定された特権レベルにログインする、あるいは指定された特権レベルを終了するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **enable** *level*
2. **disable** *level*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** *level*	指定された特権レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した特権レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

RADIUS によるアクセス ポイントへのアクセスの制御

ここでは、Remote Authentication Dial-In User Service（RADIUS）を使用して、ワイヤレス デバイスの管理者アクセス権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手順の詳細については、『*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 を使用すると、アカウンティングの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。RADIUS は、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）を通じて効率化され、AAA コマンドでだけイネーブルにできます。

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

次の各項で RADIUS の設定について説明します。

- 「RADIUS のデフォルト設定」（P.10-12）
- 「RADIUS ログイン認証の設定」（P.10-12）（必須）
- 「AAA サーバ グループの定義」（P.10-14）（任意）
- 「ユーザの特権アクセスとネットワーク サービスに対する RADIUS 許可の設定」（P.10-16）（任意）
- 「RADIUS の設定の表示」（P.10-17）

RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトでディセーブルです。

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

RADIUS ログイン認証の設定

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

方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方式が失敗した場合に認証用のバックアップ システムが確実に機能します。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、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証に失敗した場合、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からユーザ アクセスを拒否する応答があった場合には、許可プロセスが停止し、それ以上の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで開始し、次のステップに従います。この手順は必須です。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name*：作成するリストの名前を指定する文字列。 • *method1...*：認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **radius**：RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細については、『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章にある「Identifying the RADIUS Server Host」を参照してください。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成したデフォルト リストが使用されます。 • *list-name*：**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**	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、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 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、回線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

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようにワイヤレス デバイスを設定できます。設定済みのサーバ ホストの一部を選択して、それらを特定のサービスに使用します。サーバ グループは、選択されたサーバ ホストの IP アドレスのリストを含むグローバルなサーバ ホスト リストとともに使用されます。

各ホストのエントリが一意の識別情報（IP アドレスと UDP ポート番号の組み合わせ）を持っていれば、同一のサーバに対する複数のホスト エントリをサーバ グループに含めることができます。これにより、特定の AAA サービスを提供する RADIUS ホストとして、異なるポートを個別に定義できます。同じ RADIUS サーバに同一のサービス（アカウンティングなど）を実行する 2 つの異なるホスト エントリを設定すると、2 番目に設定されたホスト エントリが最初のホスト エントリのフェールオーバー時のバックアップとして機能します。

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

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

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **radius-server host** {***hostname*** | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaa group server radius** *group-name*
5. **server** *ip-address*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**
9. RADIUS ログイン認証をイネーブルにします。

手順の詳細

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

	コマンドまたはアクション	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。 • **auth-port** *port-number*：（任意）認証要求用のユーザ データグラム プロトコル（UDP）の宛先ポートを指定します。 • **acct-port** *port-number*：（任意）アカウンティング要求のための UDP 宛先ポートを指定します。 • **timeout** *seconds*：（任意）再送信する前に、ワイヤレス デバイスが RADIUS サーバの応答を待機する間隔。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドによる設定を上書きします。**radius-server host** コマンドでタイムアウトを設定しない場合は、**radius-server timeout** コマンドの設定が使用されます。 • **retransmit** *retries*：（任意）サーバが応答しない、または応答が遅い場合に RADIUS の要求をサーバに再送信する回数。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数を指定しない場合、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • **key** *string*：（任意）ワイヤレス デバイスと RADIUS サーバで実行されている RADIUS デーモン間で使用される認証および暗号キーを指定します。 **（注）** このキーはテキスト文字列で、RADIUS サーバで使用される暗号キーと一致する必要があります。キーは常に **radius-server host** コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 ワイヤレス デバイスが単一の IP アドレスに関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な回数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。ワイヤレス デバイス ソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーをそれぞれ設定してください。
ステップ 4	**aaa group server radius** *group-name*	グループ名を指定して AAA サーバ グループを定義します。 このコマンドを実行すると、ワイヤレス デバイスはサーバ グループ コンフィギュレーション モードへ移行します。

	コマンドまたはアクション	目的
ステップ 5	**server** *ip-address*	特定の RADIUS サーバを定義済みのサーバ グループと関連付けます。 • AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。 • グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。
ステップ 9	RADIUS ログイン認証をイネーブルにします。	『*Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*』の「Configuring Radius and TACACS+ Servers」の章にある「Configuring RADIUS Login Authentication」を参照してください。

指定された 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。設定リストからサーバ グループを削除するには、グローバル コンフィギュレーション モードで **no 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 デバイスは異なる 2 つの RADIUS グループ サーバ（*group1* と *group2*）を認識するように設定されます。Group1 には、同じ RADIUS サーバで同じサービス用に設定された異なる 2 つのホスト エントリがあります。2 番目のホスト エントリは、最初のエントリに対してフェールオーバー 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
```

ユーザの特権アクセスとネットワーク サービスに対する 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 デバイスはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザのプロファイルから取得した情報を使用して、ユーザ セッションを設定します。ユーザが要求したサービスにアクセスを許可されるのは、ユーザ プロファイルによって許可された場合だけです。

グローバル コンフィギュレーション モードで **aaa authorization** コマンドに **radius** キーワードを使用すると、特権 EXEC モードへのユーザのネットワーク 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 コマンドを実行すると、次の許可パラメータが設定されます。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。

- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

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

特権 EXEC アクセスおよびネットワーク サービスに RADIUS 許可を指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa authorization network radius**
3. **aaa authorization exec radius**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

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

許可をディセーブルにするには、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 の設定の表示

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+ によるアクセス ポイントへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus（TACACS+）を使用してワイヤレス デバイスの管理者アクセス権を制御する手順について説明します。TACACS+ をサポートするようにワイヤレス デバイスを設定する手順の詳細については、『*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を提供し、認証と許可のプロセスを柔軟に管理します。AAA により TACACS+ が容易になります。また、TACACS+ をイネーブルにするには AAA コマンドを実行する必要があります。

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

次の各項で TACACS+ の設定について説明します。

- 「TACACS+ のデフォルト設定」（P.10-18）
- 「TACACS+ ログイン認証の設定」（P.10-18）
- 「特権 EXEC アクセスおよびネットワーク サービスに対する TACACS+ 許可の設定」（P.10-20）
- 「TACACS+ 設定の表示」（P.10-21）

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されます。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI を通じてワイヤレス デバイスにアクセスしている管理者を認証できます。

TACACS+ ログイン認証の設定

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

方式リストには、ユーザの認証に使用する、順序と認証方式が記述されています。認証に使用するセキュリティ プロトコルを 1 つまたは複数指定できるため、最初の方式が失敗した場合に認証用のバックアップ システムが確実に機能します。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、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証に失敗した場合、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からユーザ アクセスを拒否する応答があった場合には、許可プロセスが停止し、それ以上の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで開始し、次のステップに従います。この手順は必須です。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]
5. **login authentication** {**default** | *list-name*}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login** {**default** | *list-name*} ***method1*** [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが指定*されなかった*場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name*：作成するリストの名前を指定する文字列。 • *method1...*：認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 次のいずれかの方式を選択します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。グローバル コンフィギュレーション モードで **username** *password* コマンドを使用します。 • **tacacs+**：TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* : **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。

	コマンドまたはアクション	目的
ステップ 7	**show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、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 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、回線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 サービスに対する TACACS+ 許可の設定

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

グローバル コンフィギュレーション モードで **aaa authorization** コマンドに **tacacs+** キーワードを使用すると、特権 EXEC モードへのユーザ 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、次の許可パラメータを設定します。

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

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

TACACS+ 許可を特権 EXEC アクセスおよびネットワーク サービスに指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa authorization network tacacs+**
3. **aaa authorization exec tacacs+**
4. **end**
5. **show running-config**
6. **show running-config**

手順の詳細

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

許可をディセーブルにするには、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+ サーバの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、次のタスクを実行するための手順について説明します。

- 「無線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.10-21）
- 「無線デバイスのリブート」（P.10-22）
- 「無線デバイスのモニタリング」（P.10-22）

無線デバイスの工場出荷時のデフォルト設定へのリセット

無線デバイスのハードウェアおよびソフトウェアを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　データを紛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回復する場合は、**service-module wlan-ap0 reset** コマンドだけを使用してください。

無線デバイスのリブート

グレースフル シャットダウンを実行し、無線デバイスをリブートするには、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** と入力してキャンセルします。

自律モードでリロード コマンドを実行すると、リブートする前に設定が保存されます。リブートの試行が成功しない場合は、次のメッセージが表示されます。

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

通常、リロード機能は、Lightweight Access Point Protocol（LWAPP）モードで動作しているときには、Wireless LAN Controller（WLC; ワイヤレス LAN コントローラ）で処理されます。**service-module wlan-ap0 reload** コマンドを入力すると、次のメッセージと共にプロンプトが表示されます。

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

Still want to proceed? [yes]
```

無線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をモニタリングするためのコマンドについて説明します。

- 「無線デバイスの統計情報の表示」（P.10-22）
- 「無線デバイスのステータスの表示」（P.10-22）

無線デバイスの統計情報の表示

無線デバイスの統計情報を表示するには、特権 EXEC モードで **service-module wlan-ap0 statistics** コマンドを使用します。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
```

無線デバイスのステータスの表示

無線デバイスのステータスおよび設定情報を表示するには、特権 EXEC モードで **service-module wlan-ap0 status** コマンドを使用します。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.
```

システム日時の管理

ワイヤレス デバイスのシステムの日付と時刻は、Simple Network Time Protocol（SNTP）を使用して自動的に管理する、あるいはワイヤレス デバイスに日付と時刻を設定して手動で管理できます。

（注）　ここで使用す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。

この項で説明する設定情報は次のとおりです。

簡易ネットワーク タイム プロトコルの概要

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

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

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

複数のサーバのストラタムが同じだった場合は、ブロードキャスト サーバよりも設定済みサーバが優先されます。これらの両方を満たすサーバが複数ある場合は、時刻パケットを最初に送信したサーバが選択されます。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ている場合や、上記の基準に基づいてより最適なサーバが検出された場合に限り、SNTP は新しいサーバを選択します。

SNTP の設定

SNTP は、デフォルトでディセーブルになっています。アクセス ポイントで SNTP をイネーブルにするには、表 10-2 に示すコマンドのいずれか、または両方をグローバル コンフィギュレーション モードで使用します。

表 10-2　　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 サーバからの NTP パケットを受け入れるように SNTP を設定します。

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

sntp server コマンドと **sntp broadcast client** コマンドの両方を入力した場合、アクセス ポイントはブロードキャスト サーバからの時間を受け入れますが、ストラタムが等しい場合は、設定済みのサーバからの時間を優先します。SNTP に関する情報を表示するには、**show sntp** EXEC コマンドを使用します。

手動での日時の設定

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

ここでは、次の設定情報について説明します。

- 「システム クロックの設定」（P.10-24）
- 「日時設定の表示」（P.10-25）
- 「タイム ゾーンの設定」（P.10-25）
- 「夏時間の設定」（P.10-26）

システム クロックの設定

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

システム クロックを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **clock set** *hh*:*mm*:*ss day month year*
   または
   clock set *hh*:*mm*:*ss month day year*
2. **show running-config**
3. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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*：時間（24 時間形式）、分、秒を指定します。指定された時刻は、設定されたタイム ゾーンに基づきます。 • *day*：月の日で日付を指定します。 • *month*：フル ネームで月を指定します。 • *year*：4 桁（短縮なし）で年を指定します。
ステップ 2	**show running-config**	入力を確認します。
ステップ 3	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

日時設定の表示

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

show clock の表示の前にある記号は、次の意味があります。

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

タイム ゾーンの設定

タイム ゾーンを手動で設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **clock timezone** *zone hours-offset* [*minutes-offset*]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	時間帯を設定します。 **（注）** ワイヤレス デバイスは、協定世界時（UTC）で内部時刻を保持します。このコマンドは、手動で時刻を設定したときに表示目的でだけ使用します。 • *zone*：標準時が適用されているときに表示されるタイム ゾーンの名前を入力します。デフォルトの設定は UTC です。 • *hours-offset*：UTC からのオフセット時間数を入力します。 • *minutes-offset*：（任意）UTC からのオフセット分数を入力します。
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**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

グローバル コンフィギュレーション モードでの *clock timezone* コマンドの **minutes-offset** 変数は、ローカル タイム ゾーンの UTC との時差が 1 時間のパーセンテージである場合に使用できます。たとえば、大西洋沿岸のカナダの一部地域のタイム ゾーン（AST）は UTC-3.5 です。3 は 3 時間を、.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、特定の日付（曜日）に開始および終了するサマー タイム（夏時間）を設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **clock summer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**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設定されています。パラメータなしで **clock summer-time** *zone* **recurring** を指定すると、夏時間のルールは米国のルールをデフォルトにします。 • *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • *week*：（任意）月の週（1 ～ 5 または **last**）を指定します。 • *day*：（任意）曜日（日曜日など）を指定します。 • *month*：（任意）月（January など）を指定します。 • *hh*:*mm*：（任意）時間と分で時刻（24 時間形式）を指定します。 • *offset*：（任意）夏時間中に追加する分数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

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

ユーザの居住地域のサマー タイムが定期的なパターンで実施されていない場合は、特権 EXEC モードでから、次のステップを実行して、次回のサマー タイム イベントの正確な日付と時刻を設定してください。

手順の概要

1. **configure terminal**
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*]]
3. **end**
4. **show running-config**

5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**clock summer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]]	最初の日付で夏時間開始の日付を、2 番めの日付で終了の日付を設定します。
	または	夏時間はデフォルトでディセーブルに設定されています。
	clock summer-time *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	• *zone*：夏時間が有効な場合に表示される時間帯名（PDT など）を指定します。 • *week*：（任意）月の週（1 ～ 5 または **last**）を指定します。 • *day*：（任意）曜日（日曜日など）を指定します。 • *month*：（任意）月（January など）を指定します。 • *hh*:*mm*：（任意）時間と分で時刻（24 時間形式）を指定します。 • *offset*：（任意）夏時間中に追加する分数を指定します。デフォルト値は 60 です。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

サマー タイム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 日の 2 時に始まり、2001 年 4 月 26 日の 2 時に終わるように設定する例を示します。

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

システム名およびプロンプトの設定

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

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

（注）　ここで使用す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、次の設定情報について説明します。

デフォルトのシステム名とプロンプトの設定

デフォルトのアクセス ポイントのシステム名とプロンプトは *ap* です。

システム名の設定

システム名を手動で設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **hostname** *name*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**hostname** *name*	手動でシステム名を設定します。 デフォルト設定は *ap* です。 （注）　システム名を変更する場合、ワイヤレス デバイスの無線はリセットされ、アソシエートしているクライアント デバイスはアソシエーションが解除され、ただちに再アソシエートされます。 （注）　システム名には、63 文字まで入力することができます。しかし、ワイヤレス デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。装置同士を区別することがクライアント ユーザにとって重要な場合、システム名の一意の部分が最初の 15 文字に表示されるようにしてください。

	コマンドまたはアクション	目的
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	入力を確認します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

システム名を設定すると、その名前がシステムプロンプトとしても使用されます。

ホスト名をデフォルトに戻すには、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 の概要

DNS プロトコルは、ドメイン ネーム システム（DNS）を制御します。DNS とは分散型データベースであり、ホスト名を IP アドレスにマッピングできます。ワイヤレス デバイス に DNS を設定すると、**ping**、**telnet**、**connect**、および関連する Telnet サポート操作などの、すべての IP コマンドでホスト名の代わりに IP アドレスを使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP では *com* ドメイン名で識別される民間組織です。このためドメイン名は *cisco.com* です。このドメイン内にあるファイル転送プロトコル（FTP）システムなどの個々のデバイスは *ftp.cisco.com* のように識別されます。

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

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」（P.10-30）
- 「DNS の設定」（P.10-31）
- 「DNS 設定の表示」（P.10-32）

DNS のデフォルト設定

表 10-3 に、デフォルトの DNS 設定を示します。

表 10-3　DNS のデフォルト設定

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

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 モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **ip domain-name** *name*
3. **ip name-server** *server-address1* [*server-address2 ... server-address6*]
4. **ip domain-lookup**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip domain-name** *name*	非完全修飾ホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにソフトウェアが使用する、デフォルトのドメイン名を定義します。 ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 ブート時にはドメイン名が設定されませんが、ワイヤレス デバイスの設定が BOOTP または DHCP サーバから行われている場合、デフォルトのドメイン名前が BOOTP あるいは DHCP サーバによって設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。 最大 6 つのネーム サーバを指定できます。各サーバのアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。ワイヤレス デバイスは、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合は、バックアップ サーバにクエリが送信されます。
ステップ 4	**ip domain-lookup**	（任意）ワイヤレス デバイスで DNS ベースのホスト名からアドレスへの変換を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。 ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式（DNS）を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	**end**	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show running-config**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ワイヤレス デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため、DNS クエリは発生しません。ピリオド（.）なしでホスト名を設定すると、ピリオドと、それに続くデフォルトのドメイン名がホスト名に追加され、その後で DNS クエリが行われて、名前が IP アドレスにマッピングされます。デフォルトのドメイン名前は、グローバル コンフィギュレーション モードで **ip domain-name** コマンドによって設定される値です。ホスト名にピリオド（.）が含まれている場合は、Cisco IOS ソフトウェアはホスト名にデフォルトのドメイン名を追加せずに、IP アドレスを検索します。

ドメイン名を削除するには、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）　ワイヤレス デバイスに DNS が設定されている場合、**show running-config** コマンドを実行すると、サーバの名前ではなく IP アドレスが表示されます。

バナーの作成

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

ログイン バナーも接続されたすべての端末に表示されます。これは MOTD バナーの後、ログイン プロンプトの前に表示されます。

（注）　ここで使用す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、次の設定情報について説明します。

- 「バナーのデフォルト設定」（P.10-32）
- 「MOTD ログイン バナーの設定」（P.10-33）
- 「ログイン バナーの設定」（P.10-34）

バナーのデフォルト設定

MOTD およびログイン バナーは設定されていません。

MOTD ログイン バナーの設定

ワイヤレス デバイスにログインしたときに画面に表示される 1 行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 モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **banner motd** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

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

MOTD バナーを削除するには、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。

次の例は、ワイヤレス デバイスに MOTD バナーを設定する方法を示しています。ポンド記号（#）は開始および終了の区切り文字として次のように使用されています。

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

次の例では、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

接続したすべての端末に表示されるログイン バナーを設定できます。このバナーは MOTD バナーの後、ログイン プロンプトの前に表示されます。

ログイン バナーを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **banner login** *c message c*
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

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

ログイン バナーを削除するには、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。

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

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

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 1000Mbps の速度とデュプレックス設定だけをサポートし、このインターフェイスは常にアップになっています。ワイヤレス デバイスがスイッチからインライン パワーを受け取ったときに、速度設定またはデュプレックス設定が変更されるとイーサネット リンクがリセットされ、ワイヤレス デバイスがリブートします。

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

イーサネットの速度とデュプレックスは、デフォルトでは **auto** に設定されています。イーサネット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、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface fastethernet0**
3. **speed** {**10** | **100** | **auto**}
4. **duplex** {**auto** | **full** | **half**}
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface fastethernet0**	設定インターフェイス モードを開始します。
ステップ 3	**speed** {**10** | **100** | **auto**}	イーサネット速度を設定します。 **（注）** デフォルト設定の **auto** を使用することをお勧めします。
ステップ 4	**duplex** {**auto** | **full** | **half**}	デュプレックス設定を設定します。 **（注）** 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**	入力を確認します。
ステップ 7	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

アクセス ポイントの無線ネットワーク管理の設定

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

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

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

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

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

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

アクセス ポイントのローカル認証および許可の設定

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

（注） ワイヤレス デバイスを 802.1x 対応のクライアント デバイス用のローカル認証サーバとして設定し、メイン サーバのバックアップを提供したり、RADIUS サーバのないネットワーク上で認証サービスを提供したりできます。ワイヤレス デバイスをローカル認証サーバとして設定する詳細な手順については、Cisco.com の『*Using the Access Point as a Local Authenticator*』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/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 モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication login default local**
4. **aaa authorization exec local**
5. **aaa authorization network local**
6. **username** *name* [**privilege** *level*] {**password** *encryption-type password*}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカル ユーザ名データベースを使用するログイン認証を設定します。**default** キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	**aaa authorization exec local**	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	**aaa authorization network local**	ネットワーク関連のすべてのサービス要求に対してユーザ 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、ユーザ名ベースの認証システムを設定します。 このコマンドをユーザごとに繰り返し入力します。 • *name*：1 語でユーザ ID を指定します。スペースや引用符は使用できません。 • *level*：（任意）ユーザがアクセス権を取得した後に持つ特権レベルを指定します。範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type*：暗号化されていないパスワードが続くことを指定する場合は **0** を入力します。暗号化されたパスワードが後ろに続く場合は **7** を指定します。 • *password*：ワイヤレス デバイスへのアクセス権を取得するためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ～ 25 文字で指定し、スペースを含めることができます。また、パスワードは、**username** コマンドの最後のオプションとして指定する必要があります。 **（注）** TAB、?、$、+、および [は、パスワードに無効な文字です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、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。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。

認証キャッシュとプロファイルの設定

認証キャッシュとプロファイル機能により、アクセス ポイントがユーザの認証応答および許可応答をキャッシュできるようになります。このため、これ以降認証および許可要求を AAA サーバに送信しなくても済みます。

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

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

cache expiry
cache authorization profile
cache authentication profile
aaa cache profile

（注）　これらのコマンドについては、『*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。

次の例は、Admin 認証用に設定したアクセス ポイントの設定例です。許可キャッシュをイネーブルにした状態で TACACS+ を使用しています。この例では、TACACS サーバを使用していますが、アクセス ポイントは RADIUS を使用して Admin 認証用に設定できます。

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
```

```
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
```

```
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

DHCP サービスを提供するためのアクセス ポイントの設定

次の項では、ワイヤレス デバイスを DHCP サーバとして機能するように設定する方法について説明します。

- 「DHCP サーバの設定」（P.10-40）
- 「DHCP サーバ アクセス ポイントのモニタリングと維持」（P.10-42）

DHCP サーバの設定

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

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

DHCP 関連のコマンドとオプションの詳細については、次の URL で『*Cisco IOS IP Addressing Services Configuration Guide, Release 12.4*』の DHCP の部分を参照してください。

http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

DHCP サービスを提供するようにアクセス ポイントを設定し、デフォルトのルータを指定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **ip dhcp excluded-address** *low_address* [*high_address*]
3. **ip dhcp pool** *pool_name*
4. **network** *subnet_number* [*mask* | *prefix-length*]
5. **lease** {*days* [*hours*] [*minutes*] | **infinite**}
6. **default-router** *address* [*address2 ... address 8*]
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `AP# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip dhcp excluded-address** *low_address* [*high_address*]	ワイヤレス デバイスが割り当てるアドレス範囲からワイヤレス デバイスの IP アドレスを除外します。 • IP アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。 • ワイヤレス デバイスは、DHCP アドレス プール サブネット内のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定します。DHCP サーバがクライアントに割り当てない IP アドレスを指定する必要があります。 • （任意）除外するアドレスの範囲を入力するには、範囲の下限のアドレスの後に、範囲の上限のアドレスを入力します。
ステップ 3	**ip dhcp pool** *pool_name*	DHCP 要求に応じてワイヤレス デバイスが割り当てる IP アドレスのプールの名前を作成して、DHCP コンフィギュレーション モードを開始します。
ステップ 4	**network** *subnet_number* [*mask*	*prefix-length*]	アドレス プールにサブネット番号を割り当てます。ワイヤレス デバイスは、このサブネット内の IP アドレスを割り当てます。 （任意）アドレス プール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。プレフィクスはネットワーク マスクを割り当てる代替法です。プレフィクス長は、スラッシュ（/）で開始する必要があります。

	コマンドまたはアクション	目的
ステップ 5	**lease** {*days* [*hours*] [*minutes*] | **infinite**}	ワイヤレス デバイスによって割り当てられた IP アドレスのリース期間を設定します。 • *days*：リース期間（日数）。 • *hours*：（任意）リース期間（時間数）。 • *minutes*：（任意）リース期間（分数）。 • **infinite**：リース期間を無期限に設定します。
ステップ 6	**default-router** *address* [*address2 ... address 8*]	サブネット上の DHCP クライアントに対してデフォルト ルータの IP アドレスを指定します。 **（注）** 求められるのは 1 つの IP アドレスですが、コマンド行 1 行につき最大 8 つまでのアドレスを指定できます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	入力を確認します。
ステップ 9	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

次の例では、ワイヤレス デバイスを DHCP サーバとして設定し、IP アドレスの範囲を除外し、さらにデフォルト ルータを割り当てる方法を示します。

```
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と維持

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

- 「show コマンド」（P.10-42）
- 「clear コマンド」（P.10-43）
- 「debug コマンド」（P.10-43）

show コマンド

DHCP サーバとしてのワイヤレス デバイスに関する情報を表示するには、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 サーバ用の show コマンド

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

clear コマンド

DHCP サーバ変数を消去するには、特権 EXEC モードで表 10-5 のコマンドを使用します。

表 10-5　DHCP サーバ用の clear コマンド

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

debug コマンド

DHCP サーバ デバッグをイネーブルにするには、次のコマンドを特権 EXEC モードで使用します。

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

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

アクセス ポイントのセキュア シェルの設定

ここでは、セキュア シェル（SSH）機能を設定する方法について説明します。

（注）　この章で使用す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」を参照してください。

SSH の概要

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

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

- RADIUS（詳細については、「RADIUS によるアクセス ポイントへのアクセスの制御」（P.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、「アクセス ポイントのローカル認証および許可の設定」（P.10-36）を参照してください）

SSH に関する詳細については、『*Cisco IOS Security Configuration Guide for Release 12.4*』のパート 5「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 から暗号ソフトウェア イメージをダウンロードします。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 を設定し、SSH の設定を表示する方法については、次の URL で『*Cisco IOS Security Configuration Guide for Release 12.4*』のパート 6「Other Security Features」を参照してください。

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

関連付けられたクライアント装置のアドレス解決プロトコル（ARP）キャッシュを保持するように、ワイヤレス デバイスを設定できます。ワイヤレス デバイスで ARP キャッシュを保持すると、無線 LAN のトラフィック負荷が軽減されます。ARP キャッシングはデフォルトで無効に設定されています。

ここでは、次の情報について説明します。

- 「クライアント ARP キャッシングの概要」（P.10-45）
- 「ARP キャッシングの設定」（P.10-45）

クライアント ARP キャッシングの概要

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

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

オプションの ARP キャッシング

シスコ製以外のクライアント装置がアクセス ポイントに関連付けられ、その装置にデータを渡していない場合、ワイヤレス デバイスがクライアント IP アドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスは、ワイヤレス デバイスに既知の IP アドレスを持つクライアントに代わって応答しますが、不明なクライアント宛ての ARP 要求を無線ポートから転送します。アソシエートされた全クライアントの IP アドレスを記憶すると、ワイヤレス デバイスはそれらのアソシエートされたクライアント以外に対する ARP 要求をドロップします。

ARP キャッシングの設定

関連付けられたクライアントの ARP キャッシュを保持するようにワイヤレス デバイスを設定するには、特権 EXEC モードで開始し、次のステップに従います。

手順の概要

1. **configure terminal**
2. **dot11 arp-cache** [**optional**]
3. **end**
4. **show running-config**
5. **copy running-config startup-config**

手順の詳細

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

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

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

ポイントツーマルチポイント ブリッジングにおける複数の VLAN とレート制限の設定

この機能は、ポイントツーマルチポイント ブリッジングを変更したもので、複数の VLAN で動作しながら、各 VLAN のトラフィック レートを制御できるように設定するものです。

（注） レート制限ポリシーは、非ルート ブリッジでのファスト イーサネット入力ポートにだけ適用できます。

通常、複数の VLAN をサポートしていると、別々の VLAN 上にある各リモート サイトで、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、各サイトへのトラフィックを分離して制御することができます。レート制限機能により、リモート サイトがリンク帯域幅全体のうち指定された量を超える帯域幅が消費されないようになります。アップリンク トラフィックだけは、非ルート ブリッジのファスト イーサネット入力ポートを使用して管理できます。

クラスベースのポリシング機能を使用すると、レート制限を指定して、これを非ルート ブリッジのイーサネット インターフェイスの入力に適用できます。イーサネット インターフェイスの入力にレートを適用すると、すべての受信イーサネット パケットが設定したレートに適合します。

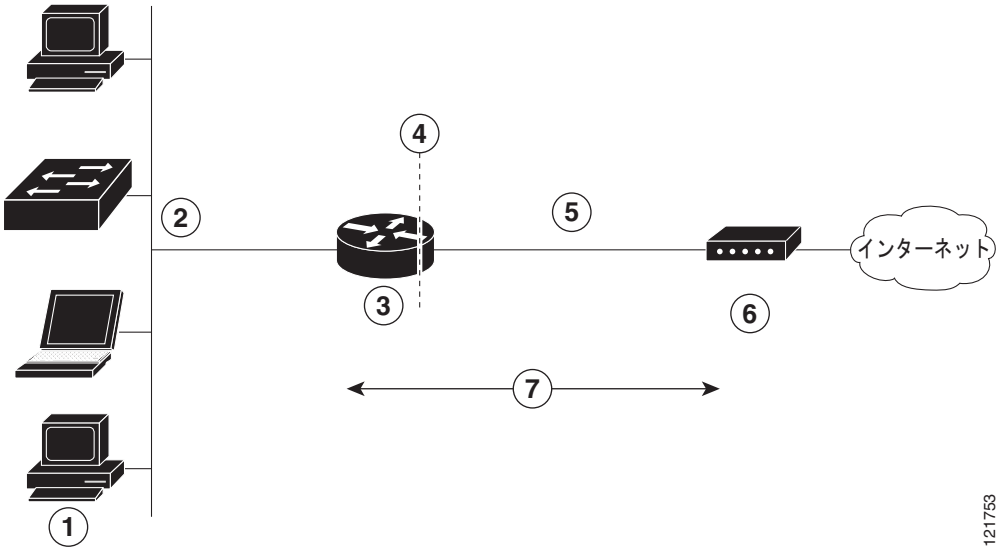
CHAPTER 11

PPP over Ethernet と NAT の設定

この章では、Cisco 860、Cisco 880、および Cisco 890 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。

ルータの背後の LAN には、複数の PC を接続できます。これらの PC からのトラフィックは PPPoE セッションに送信する前に暗号化やフィルタリングなどを行うことができます。図 11-1 に、Cisco ルータに PPPoE クライアントと NAT が設定された一般的な配置シナリオを示します。

図 11-1　PPP over Ethernet と NAT



1	複数のネットワーク デバイス：デスクトップ、ラップトップ PC、スイッチ
2	ファスト イーサネット LAN インターフェイス（NAT の内部インターフェイス）
3	PPPoE クライアント（Cisco 860、Cisco 880、または Cisco 890 ルータ）
4	NAT が実行されるポイント
5	ファスト イーサネット WAN インターフェイス（NAT 用の外部インターフェイス）
6	ケーブル モデムまたはインターネットに接続している他のサーバ
7	クライアントと PPPoE サーバ間の PPPoE セッション

PPPoE

ルータ上の PPPoE クライアント機能により、イーサネット インターフェイスでの PPPoE クライアント サポートが可能になります。仮想アクセスのクローニングには、ダイヤラ インターフェイスを使用する必要があります。イーサネット インターフェイスには、複数の PPPoE クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

PPPoE セッションが Cisco 860 または Cisco 880 ISR によってクライアント側で開始されます。確立された PPPoE クライアント セッションは、次のいずれかの方法で終了できます。

- **clear vpdn tunnel pppoe** コマンドを入力する。PPPoE クライアント セッションが終了し、PPPoE クライアントはただちにセッションの再確立を試みます。セッションがタイムアウトした場合にも、この動作が発生します。
- **no pppoe-client dial-pool** *number* コマンドを入力して、セッションをクリアする。PPPoE クライアントは、セッションの再確立を試みません。

NAT

NAT（Cisco ルータの端に点線で表示）は、2 つのアドレス指定ドメインと内部送信元アドレスを示します。送信元リストには、パケットがネットワークをどのように通過するかが定義されます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定
- イーサネット WAN インターフェイスの設定
- ダイヤラ インターフェイスの設定
- ネットワーク アドレス変換の設定

この設定タスクの結果を示す例は「設定例」（P.11-9）に示されています。

バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定

バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）を設定すると、複数のクライアントが 1 つの IP アドレスを使用してルータを介して通信できるようになります。

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

手順の概要

1. **vpdn enable**
2. **vpdn-group** *name*
3. **request-dialin**
4. **protocol** {**l2tp** | **pppoe**}
5. **exit**
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vpdn enable** **例：** `Router(config)# vpdn enable`	ルータで VPDN をイネーブルにします。
ステップ 2	**vpdn-group** *name* **例：** `Router(config)# vpdn-group 1`	VPDN グループを作成し、カスタマーまたは VPDN プロファイルに関連付けます。
ステップ 3	**request-dialin** **例：** `Router(config-vpdn)# request-dialin`	ダイヤリング方向を示す request-dialin VPDN サブグループを作成し、トンネルを開始します。
ステップ 4	**protocol** {**l2tp** | **pppoe**} **例：** `Router(config-vpdn-req-in)# protocol pppoe`	VPDN サブグループが確立できるセッションのタイプを指定します。
ステップ 5	**exit** **例：** `Router(config-vpdn-req-in)# exit`	request-dialin VPDN グループのコンフィギュレーション モードを終了します。
ステップ 6	**exit** **例：** `Router(config-vpdn)# exit`	VPDN 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。

イーサネット WAN インターフェイスの設定

このシナリオでは、PPPoE クライアント（Cisco ルータ）が、内部および外部インターフェイスの 10/100/1000 Mbps イーサネット インターフェイスと通信します。

ファスト イーサネット WAN 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 モードで次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **pppoe-client dial-pool-number** *number*
3. **no shutdown**
4. **exit**

手順の詳細

	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` または `Router(config)# interface gigabitethernet 4`	WAN 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	**pppoe-client dial-pool-number** *number* **例：** `Router(config-if)# pppoe-client dial-pool-number 1`	PPPoE クライアントを設定し、クローニングに使用するダイヤラ インターフェイスを指定します。
ステップ 3	**no shutdown** **例：** `Router(config-if)# no shutdown`	ファスト イーサネット インターフェイスとそれに対して行った設定変更をイネーブルにします。
ステップ 4	**exit** **例：** `Router(config-if)# exit`	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。

イーサネット運用管理およびメンテナンス

イーサネット運用管理およびメンテナンス（OAM）は、イーサネット メトロポリタン エリア ネットワーク（MAN）およびイーサネット WAN の設置、モニタリング、トラブルシューティングのためのプロトコルで、開放型システム間相互接続（OSI）モデルのデータ リンク層の新しいオプション サブレイヤを使用します。このプロトコルによって提供される OAM の機能には、ディスカバリ、リンク モニタリング、リモート障害検知、リモート ループバック、および Cisco Proprietary Extension（シスコ独自の拡張機能）があります。

イーサネット OAM の設定および構成情報については、次の URL で『*Using Ethernet Operations, Administration, and Maintenance*』を参照してください。

http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/ce_oam_ps10591_TSD_Products_Configuration_Guide_Chapter.html

ダイヤラ インターフェイスの設定

ダイヤラ インターフェイスは、デフォルトのルーティング情報、カプセル化プロトコル、および使用するダイヤラ プールなど、クライアントからのトラフィックを処理する方法を示します。ダイヤラ インターフェイスは、仮想アクセスのクローニングにも使用されます。ファスト イーサネット インターフェイスには、複数の PPPoE クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

ファスト イーサネット LAN インターフェイスのダイヤラ インターフェイスの 1 つをルータで設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface dialer** *dialer-rotary-group-number*
2. **ip address negotiated**
3. **ip mtu** *bytes*
4. **encapsulation** *encapsulation-type*
5. **ppp authentication** {*protocol1* [*protocol2...*]}
6. **dialer pool** *number*
7. **dialer-group** *group-number*
8. **exit**
9. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
10. **ip route** *prefix mask* {*interface-type interface-number*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface dialer** *dialer-rotary-group-number* **例：** `Router(config)# interface dialer 0`	ダイヤラ インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。 • 範囲は 0 ～ 255 です。
ステップ 2	**ip address negotiated** **例：** `Router(config-if)# ip address negotiated`	インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。
ステップ 3	**ip mtu** *bytes* **例：** `Router(config-if)# ip mtu 1492`	IP Maximum Transmission Unit（MTU; 最大伝送ユニット）のサイズを設定します。 • デフォルトの最小値は 128 バイトです。イーサネットの最大値は 1492 バイトです。
ステップ 4	**encapsulation** *encapsulation-type* **例：** `Router(config-if)# encapsulation ppp`	送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。

	コマンドまたはアクション	目的
ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]} **例：** `Router(config-if)# ppp authentication chap`	PPP 認証方式を Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）に設定します。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 6	**dialer pool** *number* **例：** `Router(config-if)# dialer pool 1`	特定の宛先サブ ネットワークへの接続に使用するダイヤラ プールを指定します。
ステップ 7	**dialer-group** *group-number* **例：** `Router(config-if)# dialer-group 1`	ダイヤラ グループにダイヤラ インターフェイスを割り当てます。 • 指定できる範囲は 1 ～ 10 です。 **ヒント** ダイヤラ グループを使用して、ルータへのアクセスを制御します。
ステップ 8	**exit** **例：** `Router(config-if)# exit`	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 モードに戻ります。
ステップ 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**} **例：** `Router(config)# dialer-list 1 protocol ip permit`	ダイヤラ リストを作成し、ダイヤル グループを関連付けます。パケットは、指定されたインターフェイス ダイヤラ グループを通じて転送されます。 このコマンドの詳しい説明およびその他の設定可能な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。
ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*} **例：** `Router(config)# ip route 10.10.25.2 255.255.255.255 dialer 0`	ダイヤラ 0 インターフェイスのデフォルト ゲートウェイに IP ルートを設定します。 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 Command Reference, Volume 2; Routing Protocols*』を参照してください。

ネットワーク アドレス変換の設定

ネットワーク アドレス変換（NAT）は、ダイヤラ インターフェイスによって割り当てられたグローバル アドレスを使用して、標準のアクセス リストに一致するアドレスからのパケットを変換します。内部インターフェイスを介してルータに到達したパケット、ルータから発信されたパケット、またはその両方のパケットについて、可能なアドレス変換がアクセス リストで確認されます。NAT には、スタティック アドレス変換もダイナミック アドレス変換も設定できます。

外部ファスト イーサネット WAN インターフェイスをダイナミック NAT で設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. **ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
3. **interface** *type number*
4. **ip nat** {**inside** | **outside**}
5. **no shutdown**
6. **exit**
7. **interface** *type number*
8. **ip nat** {**inside** | **outside**}
9. **no shutdown**
10. **exit**
11. **access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **例：** `Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0`	NAT 用のグローバル IP アドレスのプールを作成します。
ステップ 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**] **例：** `Router(config)# ip nat inside source list 1 interface dialer 0 overload` または `Router(config)# ip nat inside source list acl1 pool pool1`	内部インターフェイス上のダイナミック アドレス変換をイネーブルにします。 最初の例は、アクセス リスト *1* で許可されたアドレスが、ダイヤラ インターフェイス *0* に指定されているいずれかのアドレスに変換されることを示しています。 次の例は、アクセス リスト *acl1* で許可されたアドレスが、NAT プール *pool1* に指定されたいずれかのアドレスに変換されることを示しています。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface vlan 1`	NAT の内部インターフェイスにする VLAN（ファスト イーサネット LAN インターフェイス（FE0–FE3）が存在する）に対して、コンフィギュレーション モードを開始します。
ステップ 4	**ip nat** {**inside** | **outside**} **例：** `Router(config-if)# ip nat inside`	指定の VLAN インターフェイスを NAT の内部インターフェイスとして識別します。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 5	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	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。

	コマンドまたはアクション	目的
ステップ 7	**interface** *type number* **例：** `Router(config)# interface fastethernet 4`	NAT の外部インターフェイスとするファスト イーサネット WAN インターフェイス（FE4 または NAT）に対して、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 nat** {**inside** | **outside**} **例：** `Router(config-if)# ip nat outside`	指定の WAN インターフェイスを NAT の外部インターフェイスとして識別します。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 9	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。
ステップ 10	**exit** **例：** `Router(config-if)# exit`	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。
ステップ 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **例：** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	変換が必要なアドレスを示す標準アクセス リストを定義します。 **（注）**　その他のアドレスはすべて、暗黙的に拒否されます。

（注）　仮想テンプレート インターフェイスとともに NAT を使用するには、ループ バック インターフェイスを設定する必要があります。ループバック インターフェイスの設定の詳細については、第 3 章「ルータの基本設定」を参照してください。

NAT コマンドの詳細については、Cisco NX-OS Release 4.1 のマニュアル セットを参照してください。NAT の概要については、付録 A「Cisco IOS ソフトウェアの基礎知識」を参照してください。

設定例

次の設定例は、この章で説明した PPPoE シナリオのコンフィギュレーション ファイルの一部を示しています。

VLAN インターフェイスの IP アドレスは 192.168.1.1、サブネット マスクは 255.255.255.0 です。NAT は内部と外部に設定されています。

（注）　「**(default)**」のマークが付いているコマンドは、**show running-config** コマンドを実行すると自動的に生成されます。

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
interface FastEthernet 4
no ip address
no ip directed-broadcast (default)
ip nat outside
pppoe enable group global
pppoe-client dial-pool-number 1
no sh
!
interface dialer 0
ip address negotiated
ip mtu 1492
encapsulation ppp
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
ip classless (default)
ip route 10.10.25.2 255.255.255.255 dialer 0
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0
ip nat inside source list acl1 pool pool1
!
```

設定の確認

PPPoE クライアントと NAT の設定を確認するには、特権 EXEC モードで **show ip nat statistics** コマンドを使用します。次の例のような確認用の出力が表示されます。

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet4
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

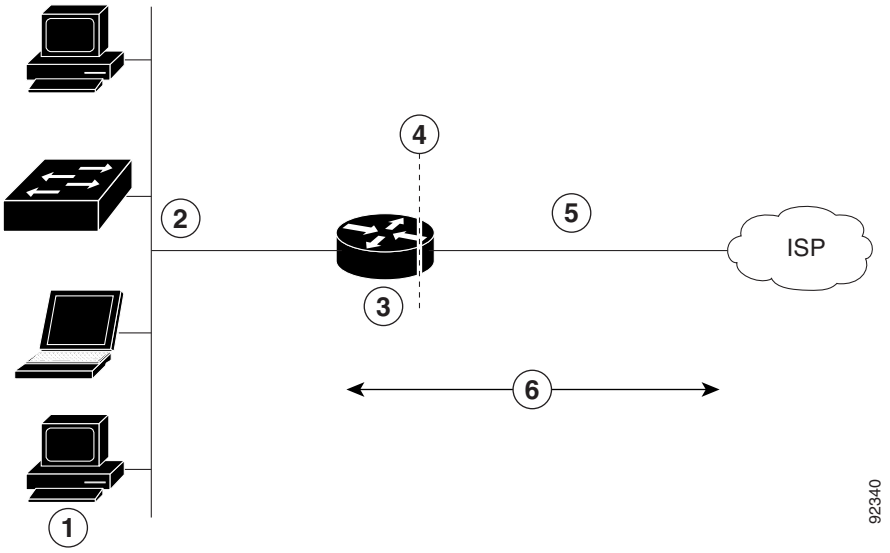
CHAPTER 12

PPP over ATM と NAT の設定

この章では、Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）およびネットワーク アドレス変換（NAT）の概要について説明します。

ルータの背後の LAN には、複数の PC を接続できます。PC からのトラフィックに対しては、PPPoA セッションに送信する前に暗号化やフィルタリングなどを行うことができます。PPP over ATM により、ダイヤル ネットワークのような簡素化されたアドレス処理と単純なユーザ検証がネットワーク ソリューションで実現します。図 12-1 に、Cisco ルータに PPPoA クライアントと NAT を設定する一般的な配置シナリオを示します。このシナリオでは、ATM 接続に単一のスタティック IP アドレスを使用しています。

図 12-1　PPP over ATM と NAT



1	複数のネットワーク接続デバイス（デスクトップ、ラップトップ PC、スイッチ）を使用するスモール ビジネス
2	ファスト イーサネット LAN インターフェイス（NAT の内部インターフェイス、192.168.1.1/24）
3	PPPoA クライアント
4	NAT が実行されるポイント
5	ATM WAN インターフェイス（NAT の外部インターフェイス）
6	ISP でのクライアントと PPPoA サーバ間の PPPoA セッション

このシナリオでは、ファスト イーサネット LAN の小規模企業またはリモート ユーザは、Cisco 860 および Cisco 880 シリーズ ISR の xDSL WAN インターフェイスを使用してインターネット サービス プロバイダー（ISP）に接続できます。

ファスト イーサネット インターフェイスが LAN 経由でデータ パケットを伝送し、ATM インターフェイスの PPP 接続にオフロードします。ATM トラフィックはカプセル化されて、xDSL インターフェイスで送信されます。ISP への接続には、ダイヤラ インターフェイスが使用されます。

PPPoA

ルータ上の PPPoA クライアント機能により、ATM インターフェイスでの PPPoA クライアント サポートが可能になります。仮想アクセスのクローニングには、ダイヤラ インターフェイスを使用する必要があります。イーサネット インターフェイスには、複数の PPPoA クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

PPPoA セッションは、Cisco 860 または Cisco 880 シリーズ ルータによってクライアント側で開始されます。

NAT

NAT（Cisco ルータの端に点線で表示）は、2 つのアドレス指定ドメインと内部送信元アドレスを示します。送信元リストには、パケットがネットワークをどのように通過するかが定義されます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- ダイヤラ インターフェイスの設定
- ATM WAN インターフェイスの設定
- DSL シグナリング プロトコルの設定
- ネットワーク アドレス変換の設定

この設定タスクの結果を示す例は「設定例」（P.12-9）に示されています。

ダイヤラ インターフェイスの設定

ダイヤラ インターフェイスは、デフォルトのルーティング情報、カプセル化プロトコル、および使用するダイヤラ プールなど、クライアントからのトラフィックを処理する方法を示します。また、仮想アクセスのクローニングにも使用されます。イーサネット インターフェイスには、複数の PPPoA クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

ルータ上の ATM インターフェイスに対してダイヤラ 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 モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**interface dialer** *dialer-rotary-group-number* **例：** `Router(config)# interface dialer 0`	ダイヤラ インターフェイス（番号 0 ～ 255）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 negotiated** **例：** `Router(config-if)# ip address negotiated`	ダイヤラ インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。
ステップ 3	**ip mtu** *bytes* **例：** `Router(config-if)# ip mtu 4470`	IP Maximum Transmission Unit（MTU; 最大伝送ユニット）のサイズを設定します。デフォルトの最小値は 128 バイトです。ATM の最大値は、4470 バイトです。
ステップ 4	**encapsulation** *encapsulation-type* **例：** `Router(config-if)# encapsulation ppp`	送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。
ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]} **例：** `Router(config-if)# ppp authentication chap`	PPP 認証方式を設定します。 例では、Challenge Handshake Authentication Protocol（CHAP）が適用されます。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 6	**dialer pool** *number* **例：** `Router(config-if)# dialer pool 1`	特定の宛先サブネットワークへの接続に使用するダイヤラ プールを指定します。
ステップ 7	**dialer-group** *group-number* **例：** `Router(config-if)# dialer-group 1`	ダイヤラ グループ（1 ～ 10）にダイヤラ インターフェイスを割り当てます。 **ヒント** ダイヤラ グループを使用して、ルータへのアクセスを制御します。
ステップ 8	**exit** **例：** `Router(config-if)# exit`	ダイヤラ 0 インターフェイスの設定を終了します。

	コマンド	目的
ステップ 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**} **例：** `Router(config)# dialer-list 1 protocol ip permit`	ダイヤラ リストを作成し、ダイヤル グループを関連付けます。パケットは、指定されたインターフェイス ダイヤラ グループを通じて転送されます。 このコマンドの詳しい説明およびその他の設定可能な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。
ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*} **例：** `Router(config)# ip route 10.10.25.2 0.255.255.255 dialer 0`	ダイヤラ 0 インターフェイスのデフォルト ゲートウェイに IP ルートを設定します。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS IP Command Reference, Volume 1 of 4: Routing Protocols*』を参照してください。

ダイヤラ インターフェイスまたはダイヤラ プールを追加する必要がある場合は、この手順を繰り返します。

ATM WAN インターフェイスの設定

ATM 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 モードで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 atm 0`	ATM インターフェイス（ルータの背面に ADSLoPOTS または G.SHDSL というラベルがあります）に対するインターフェイス コンフィギュレーション モードを開始します。 **（注）** このインターフェイスは、ルータの基本設定時に初期設定されています。「WAN インターフェイスの設定」（P.3-8）を参照してください。
ステップ 2	**pvc** *vpi/vci* **例：** `Router(config-if)# pvc 8/35`	ルータが通信する各エンド ノード（最大 10 台）用に ATM PVC を作成します。ATM 仮想回線コンフィギュレーション モードを開始します。 PVC が定義されると、AAL5SNAP カプセル化がデフォルトで定義されます。この設定を変更するには、ステップ 3 に示すように **encapsulation** コマンドを使用します。VPI および VCI 引数は同時に 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。

	コマンド	目的
ステップ 3	**encapsulation** {**aal5auto** | **aal5autoppp** **virtual-template** *number* [**group** *group-name*] | **aal5ciscoppp virtual-template** *number* | **aal5mux** *protocol* | **aal5nlpid** | **aal5snap**} **例：** `Router(config-if-atm-vc)# encapsulation aal5mux ppp dialer`	PVC のカプセル化タイプを指定し、ダイヤラ インターフェイスに戻ります。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。
ステップ 4	**dialer pool-member** *number* **例：** `Router(config-if-atm-vc)# dialer pool-member 1`	ダイヤラ プロファイル ダイヤリング プールのメンバーとして、ATM インターフェイスを指定します。プール番号は 1 ～ 255 の範囲内にする必要があります。
ステップ 5	**no shutdown** **例：** `Router(config-if-atm-vc)# no shutdown`	ATM インターフェイスに対するインターフェイスおよび設定の変更をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config-if)# exit` `Router(config)#`	ATM インターフェイスに対するコンフィギュレーション モードを終了します。

DSL シグナリング プロトコルの設定

DSL シグナリングは、ISP への接続用に ATM インターフェイスに設定する必要があります。Cisco 887 および Cisco 867 ISR は、POTS 経由の ADSL シグナリングをサポートし、Cisco 886 ISR は、ISDN 経由の ADSL シグナリングをサポートします。Cisco 888 ISR は、G.SHDSL をサポートします。

ADSL の設定

表 12-1 には、ADSL シグナリングのデフォルト設定を示します。

表 12-1　ADSL のデフォルト設定

属性	説明	デフォルト値
動作モード	ATM インターフェイスの Digital Subscriber Line（DSL; デジタル加入者線）の動作モードを指定します。 • ADSL over POTS : ANSI または ITU フル レート、または自動選択。 • ADSL over ISDN : ITU フル レート、ETSI、または自動選択。	Auto
マージン損失	マージン損失の発生可能回数を指定します。	—
トレーニング ログ	トレーニング ログの有効化と無効化を切り替えます。	Disabled

これらの設定を変更する場合は、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

- **dsl operating-mode**（ATM インターフェイス コンフィギュレーション モードから）
- **dsl lom** *integer*
- **dsl enable-training-log**

これらのコマンドの詳細については、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。

設定の確認

設定に誤りがないことを確認するには、特権 EXEC モードで **show dsl interface atm** コマンドを使用します。

```
Router# show dsl interface atm 0
ATM0
Alcatel 20190 chipset information
                ATU-R (DS)                      ATU-C (US)
Modem Status:    Showtime (DMTDSL_SHOWTIME)
DSL Mode:        ITU G.992.5 (ADSL2+) Annex A
ITU STD NUM:     0x03                            0x2
Chip Vendor ID:  'STMI'                          'BDCM'
Chip Vendor Specific:  0x0000                    0x6193
Chip Vendor Country:   0x0F                      0xB5
Modem Vendor ID: 'CSCO'                          '    '
Modem Vendor Specific: 0x0000                    0x0000
Modem Vendor Country:  0xB5                      0x00
Serial Number Near:
Serial Number Far:
Modem VerChip ID:        C196 (3)
DFE BOM:         DFE3.0 Annex A (1)
Capacity Used:   82%                             99%
Noise Margin:    12.5 dB                          5.5 dB
Output Power:    11.5 dBm                        12.0 dBm
Attenuation:      5.5 dB                          0.0 dB
FEC ES Errors:    0                               0
ES Errors:        1                              287
SES Errors:       1                               0
LOSES Errors:     1                               0
UES Errors:       0                              276233
Defect Status:   None                            None
Last Fail Code:  None
Watchdog Counter: 0x56
Watchdog Resets: 0
Selftest Result: 0x00
Subfunction:     0x00
Interrupts:      4147 (0 spurious)
PHY Access Err:  0
Activations:     3
LED Status:      ON
LED On Time:     100
LED Off Time:    100
Init FW:         init_AMR-4.0.015_no_bist.bin
Operation FW:    AMR-4.0.015.bin
FW Source:       embedded
FW Version:      4.0.15

                 DS Channel1      DS Channel0   US Channel1       US Channel0
Speed (kbps):              0            19999             0              1192
Cells:                     0                0             0           1680867
```

```
Reed-Solomon EC:          0                 0             0                  0
CRC Errors:               0                 0             0                326
Header Errors:            0                 0             0                131
Total BER:                0E-0           65535E-0
Leakage Average BER:      0E-0           65535E-255
Interleave Delay:         0                 36            0                 11
                        ATU-R (DS)      ATU-C (US)
Bitswap:                enabled           enabled
Bitswap success:          0                 0
Bitswap failure:          0                 0

LOM Monitoring : Disabled


DMT Bits Per Bin
000: 0 0 0 0 F F F F F F F F F F F F
010: 0 0 3 0 F F F F F F F F F F F F
020: F F F F F F F F F F F F F F F F
....
DSL: Training log buffer capability is not enabled
Router#
```

ネットワーク アドレス変換の設定

ネットワーク アドレス変換（NAT）は、ダイヤラ インターフェイスによって割り当てられたグローバル アドレスを使用して、標準のアクセス リストに一致するアドレスからのパケットを変換します。内部インターフェイスを介してルータに到達したパケット、ルータから発信されたパケット、またはその両方のパケットについて、可能なアドレス変換がアクセス リストで確認されます。NAT には、スタティック アドレス変換もダイナミック アドレス変換も設定できます。

外部 ATM WAN インターフェイスにダイナミック NAT を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **例：** `Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.255.0`	NAT 用のグローバル IP アドレスのプールを作成します。
ステップ 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**] **例 1：** `Router(config)# ip nat inside source list 1 interface dialer 0 overload` または **例 2：** `Router(config)# ip nat inside source list acl1 pool pool1`	内部インターフェイス上のダイナミック アドレス変換をイネーブルにします。 最初の例は、アクセス リスト *1* で許可されたアドレスが、ダイヤラ インターフェイス *0* に指定されているいずれかのアドレスに変換されることを示しています。 次の例は、アクセス リスト *acl1* で許可されたアドレスが、NAT プール *pool1* に指定されたいずれかのアドレスに変換されることを示しています。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 3	**interface** *type number* **例：** `Router(config)# interface vlan 1`	NAT の内部インターフェイスにする VLAN（ファスト イーサネット LAN インターフェイス（FE0–FE3）が存在する）に対して、コンフィギュレーション モードを開始します。
ステップ 4	**ip nat** {**inside** | **outside**} **例：** `Router(config-if)# ip nat inside`	ファスト イーサネット LAN インターフェイスを内部インターフェイスとして、NAT を適用します。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 5	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。

	コマンド	目的
ステップ 6	**exit** **例：** `Router(config-if)# exit`	ファスト イーサネット インターフェイスに対する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	**interface** *type number* **例：** `Router(config)# interface atm 0`	NAT の外部インターフェイスにする ATM WAN インターフェイス（ATM0）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 8	**ip nat** {**inside** | **outside**} **例：** `Router(config-if)# ip nat outside`	指定の WAN インターフェイスを NAT の外部インターフェイスとして識別します。 このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。
ステップ 9	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。
ステップ 10	**exit** **例：** `Router(config-if)# exit`	ATM インターフェイスに対するコンフィギュレーション モードを終了します。
ステップ 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **例：** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	変換が必要なアドレスを許可する標準アクセス リストを定義します。 **（注）**　その他のアドレスはすべて、暗黙的に拒否されます。

（注） NAT を仮想テンプレート インターフェイスで使用する場合は、ループバック インターフェイスを設定する必要があります。ループバック インターフェイスの設定については、第 3 章「ルータの基本設定」を参照してください。

NAT コマンドの詳細については、Cisco NX-OS Release 4.1 のマニュアル セットを参照してください。

設定例

次の設定例は、この章で説明した PPPoA シナリオにおけるクライアントのコンフィギュレーション ファイルの一部を示します。

VLAN インターフェイスの IP アドレスは 192.168.1.1、サブネット マスクは 255.255.255.0 です。NAT は内部と外部に設定されています。

（注）「**(default)**」のマークが付いているコマンドは、**show running-config** コマンドを実行すると自動的に生成されます。

```
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly (default)
!
interface ATM0
 no ip address
 ip nat outside
 ip virtual-reassembly
 no atm ilmi-keepalive
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless (default)
!
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255
ip nat inside source list 1 interface Dialer0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit

ip route 10.10.25.2 0.255.255.255 dialer 0
!
```

設定の確認

PPPoA クライアントと NAT の設定を確認するには、特権 EXEC モードで **show ip nat statistics** コマンドを使用します。次の例のような確認用の出力が表示されます。

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  ATM0
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

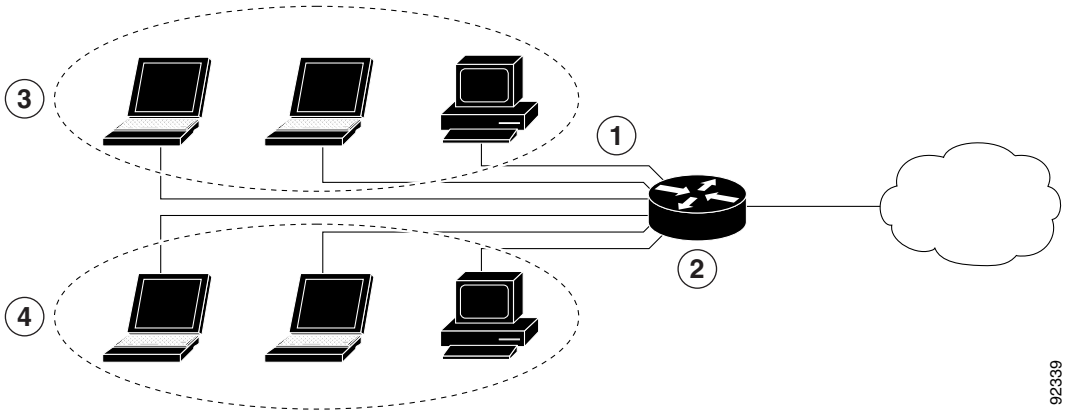
CHAPTER 13

DHCP および VLAN による LAN の設定

Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）は、両方の物理 LAN および VLAN のクライアントをサポートします。各ルータは Dynamic Host Configuration Protocol（DHCP）を使用して、このようなネットワーク上にある各ノードに対して、IP 設定の自動割り当てをイネーブルにできます。

図 13-1 に、ルータおよび 2 つの VLAN を介して接続された 2 つの物理 LAN の一般的な構成例を示します。

図 13-1　Cisco ルータで DHCP が設定された物理および仮想 LAN



1	ファスト イーサネット LAN（複数のネットワーク デバイス）
2	インターネットに接続されたルータおよび DHCP サーバ（Cisco 860 および 880 シリーズ アクセス ルータ）
3	VLAN 1
4	VLAN 2

DHCP

DHCP は、RFC 2131 に説明されているように、アドレス割り当てにクライアント/サーバ モデルを採用しています。管理者は、Cisco 800 シリーズ ルータを DHCP サーバとして動作するように設定できます。この場合、IP アドレスの割り当てと他の TCP/IP 関連の設定情報をワーク ステーションに提供します。DHCP を使用すると、IP アドレスを各クライアントに手動で割り当てるという作業を省くことができます。

DHCP サーバの設定では、サーバのプロパティ、ポリシーおよび DHCP オプションを設定する必要があります。

（注）　サーバのプロパティを変更する場合には、Network Registrar データベースからのコンフィギュレーション データでサーバを毎回リロードする必要があります。

VLAN

Cisco 860 および 880 シリーズ アクセス ルータは VLAN を設定できる 4 つのファスト イーサネット ポートをサポートします。

VLAN によって、ユーザの物理的な配置または LAN 接続に関係なく、ネットワークをユーザの論理グループに分割して、まとめることができます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- DHCP の設定
- VLAN の設定

（注）　この章の各手順では、ルータの基本機能、NAT による PPPoE または PPPoA をすでに設定していることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 3 章「ルータの基本設定」、第 11 章「PPP over Ethernet と NAT の設定」、および第 12 章「PPP over ATM と NAT の設定」を参照してください。

DHCP の設定

DHCP 用にル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 モードで次の手順を実行します。

手順の概要

1. **ip domain name** *name*
2. **ip name-server** *server-address1* [*server-address2...server-address6*]
3. **ip dhcp excluded-address** *low-address* [*high-address*]
4. **ip dhcp pool** *name*
5. **network** *network-number* [*mask* | *prefix-length*]
6. **import all**
7. **default-router** *address* [*address2...address8*]
8. **dns-server** *address* [*address2...address8*]
9. **domain-name** *domain*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip domain name** *name* **例：** `Router(config)# ip domain name smallbiz.com` `Router(config)#`	未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにルータが使用する、デフォルトのドメインを特定します。
ステップ 2	**ip name-server** *server-address1* [*server-address2...server-address6*] **例：** `Router(config)# ip name-server 192.168.11.12` `Router(config)#`	名前およびアドレス解決に使用する 1 つ以上の Domain Name System（DNS; ドメイン ネーム システム）サーバのアドレスを指定します。
ステップ 3	**ip dhcp excluded-address** *low-address* [*high-address*] **例：** `Router(config)# ip dhcp excluded-address 192.168.9.0`	DHCP サーバが DHCP クライアントに割り当ててはいけない IP アドレスを指定します。 この例では、ルータのアドレスを除外します。
ステップ 4	**ip dhcp pool** *name* **例：** `Router(config)# ip dhcp pool dpool1` `Router(config-dhcp)#`	ルータ上に DHCP アドレス プールを作成します。続いて、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* 引数は、ストリングまたは整数にすることができます。
ステップ 5	**network** *network-number* [*mask* | *prefix-length*] **例：** `Router(config-dhcp)# network 10.10.0.0 255.255.255.0` `Router(config-dhcp)#`	DHCP アドレス プールのサブネット番号（IP）アドレスを定義します（任意でマスクを入力します）。
ステップ 6	**import all** **例：** `Router(config-dhcp)# import all` `Router(config-dhcp)#`	ルータ データベースの DHCP 部分に DHCP オプション パラメータをインポートします。
ステップ 7	**default-router** *address* [*address2...address8*] **例：** `Router(config-dhcp)# default-router 10.10.10.10` `Router(config-dhcp)#`	DHCP クライアントのデフォルト ルータを最大 8 つまで指定します。
ステップ 8	**dns-server** *address* [*address2...address8*] **例：** `Router(config-dhcp)# dns-server 192.168.35.2` `Router(config-dhcp)#`	DHCP クライアントが使用できる DNS サーバを最大 8 つまで指定します。

	コマンドまたはアクション	目的
ステップ 9	**domain-name** *domain* **例：** `Router(config-dhcp)# domain-name cisco.com` `Router(config-dhcp)#`	DHCP クライアントのドメイン名を指定します。
ステップ 10	**exit** **例：** `Router(config-dhcp)# exit` `Router(config)#`	DHCP 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 モードを開始します。

設定例

次の設定例は、この章で説明してきた DHCP 設定のコンフィギュレーション ファイルの一部を示します。

```
ip dhcp excluded-address 192.168.9.0
!
ip dhcp pool dpool1
   import all
   network 10.10.0.0 255.255.255.0
   default-router 10.10.10.10
   dns-server 192.168.35.2
   domain-name cisco.com
!
ip domain name smallbiz.com
ip name-server 192.168.11.12
```

DHCP 設定の確認

DHCP 設定を表示するには、次のコマンドを使用します。

- **show ip dhcp import** : DHCP サーバ データベースにインポートされたオプションのパラメータを表示します。
- **show ip dhcp pool** : DHCP アドレス プールに関する情報を表示します。
- **show ip dhcp server statistics**:アドレス プールおよびバインディングの数などの DHCP サーバ統計情報を表示します。

```
Router# show ip dhcp import
Address Pool Name: dpool1

Router# show ip dhcp pool
Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0
```

```
Router# show ip dhcp server statistics
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

VLAN の設定

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

手順の概要

1. **vlan** *vlan_id*
2. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**vlan** *vlan_id* **例：** `Router(config)# vlan 2`	VLAN を追加します（識別番号の範囲は 1 ～ 4094）。
ステップ 2	**exit** **例：** `Router(config)# exit`	VLAN データベースを更新し、管理ドメイン全体にデータベースを伝搬して、特権 EXEC モードに戻ります。

VLAN へのスイッチ ポートの割り当て

VLAN にスイッチ ポートを割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface** *switch port id*
2. **switchport access vlan** *vlan-id*
3. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface** *switch port id* **例：** `Router(config)# interface FastEthernet 2` `Router(config-if)#`	VLAN に割り当てるスイッチ ポートを指定します。
ステップ 2	**switchport access vlan** *vlan-id* **例：** `Router(config-if)# switchport access vlan 2` `Router(config-if)#`	VLAN にポートを割り当てます。
ステップ 3	**end** **例：** `Router(config-if)# end` `Router#`	インターフェイス モードを終了し、特権 EXEC モードに戻ります。

VLAN コンフィギュレーションの確認

VLAN コンフィギュレーションを表示するには、次のコマンドを使用します。

- **show**：VLAN データベース モードから入力します。設定されたすべての VLAN の設定情報の概要を表示します。
- **show vlan-switch**：特権 EXEC モードから入力します。設定されたすべての VLAN の詳細情報を表示します。

```
Router# vlan database
Router(vlan)# show

  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003
```

```
  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500

  VLAN ISL Id: 3
    Name: red-vlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100003
    State: Operational
    MTU: 1500

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

  VLAN ISL Id: 1005
    Name: trnet-default
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

Router# show vlan-switch

VLAN Name                             Status    Ports
```

```
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0, Fa1, Fa3
2    VLAN0002                         active    Fa2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

CHAPTER 14

Easy VPN および IPSec トンネルを使用した VPN の設定

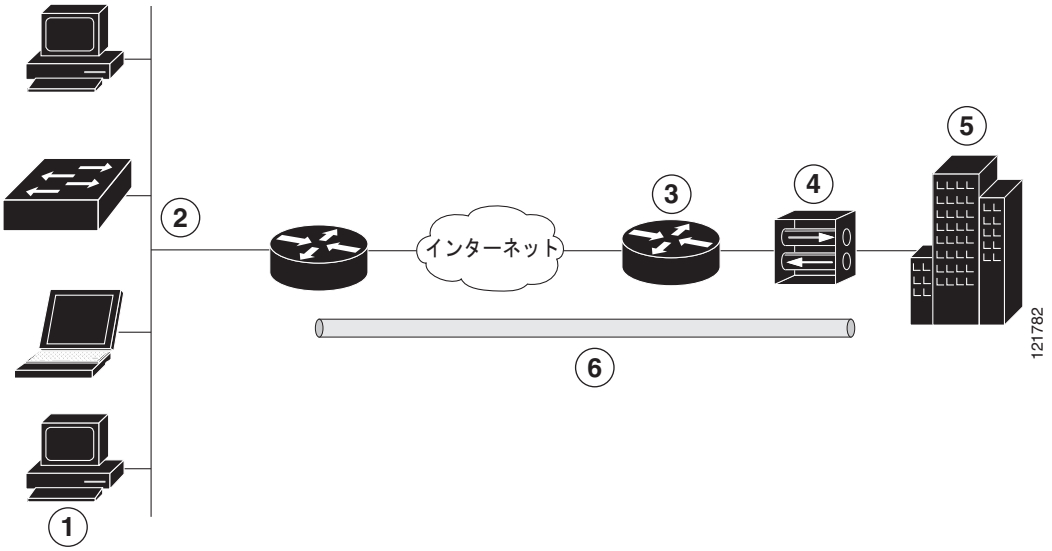
この章では、Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できる仮想プライベート ネットワーク（VPN）の作成の概要について説明します。

Cisco ルータと他のブロードバンド デバイスは、インターネットへの高パフォーマンスな接続を提供しますが、多くのアプリケーションでは、高レベルの認証を実行し、2 つの特定のエンドポイント間でデータを暗号化する VPN 接続のセキュリティも必要です。

サイト間とリモート アクセスの 2 種類の VPN がサポートされます。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、企業ネットワークにログインする際にリモート クライアントによって使用されます。

この章の例は、Cisco Easy VPN と IPSec トンネルを使用してリモート クライアントと企業ネットワーク間の接続を設定し、セキュアにするリモート アクセス VPN の構成を示しています。図 14-1 は、一般的な構成例を示します。

図 14-1　IPSec トンネルを使用したリモート アクセス VPN



1	リモート、ネットワークで接続されたユーザ
2	VPN クライアント：Cisco 860 および Cisco 880 シリーズ ISR
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
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN

Cisco Easy VPN クライアント機能を使用し、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業が大幅に削減されます。このプロトコルでは、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、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、ほとんどの VPN パラメータを IPSec サーバとして機能している VPN サーバで定義できます。

Easy VPN サーバ対応のデバイスでは、PC 上で Cisco Easy VPN リモート ソフトウェアを実行しているモバイルおよびリモート作業者が開始した VPN トンネルを終了できます。Easy VPN サーバ対応のデバイスでは、リモート ルータを Easy VPN リモート ノードとして動作させることができます。

Cisco Easy VPN クライアント機能は、クライアント モードとネットワーク拡張モードの 2 つのモードのいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、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では、中央サイトのユーザはクライアント 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 860 および 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 ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

（注）　Cisco Easy VPN クライアント機能で設定できるのは、1 つの宛先ピアだけです。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、手動でクライアントおよびサーバ側の両方に 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 / ピア アドレス変換）パラメータを設定する必要があります。

設定作業

このネットワーク シナリオのルータを設定するには、次の作業を実行します。

- IKE ポリシーの設定
- グループ ポリシー情報の設定
- クリプト マップへのモード設定の適用
- ポリシー ルックアップのイネーブル化
- IPSec トランスフォームおよびプロトコルの設定
- IPSec 暗号方式およびパラメータの設定
- 物理インターフェイスへのクリプト マップの適用
- Easy VPN リモート コンフィギュレーションの作成

この設定タスクの結果を示す例は「設定例」（P.14-13）で提供されます。

（注）　この章の手順では、基本的なルータ機能と、NAT、DCHP、および VLAN を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 3 章「ルータの基本設定」、第 11 章「PPP over Ethernet と NAT の設定」、第 12 章「PPP over ATM と NAT の設定」および第 13 章「DHCP および VLAN による LAN の設定」を参照してください。

（注）　この章の例は、Cisco 870 シリーズ ルータのエンドポイント設定だけを示しています。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 モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー交換）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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp policy** *priority*
2. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
3. **hash** {**md5** | **sha**}
4. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
5. **group** {**1** | **2** | **5**}

6. **lifetime** *seconds*
7. **exit**

手順の詳細

	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 ネゴシエーション時に使用される IKE ポリシーを作成します。プライオリティ番号の範囲は 1 ～ 10000 で、プライオリティが最も高いのは 1 です。 また、Internet Security Association Key and Management Protocol（ISAKMP; インターネット セキュリティ アソシエーション キーおよび管理）ポリシー 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	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**} **例：** `Router(config-isakmp)# encryption 3des` `Router(config-isakmp)#`	IKE ポリシーに使用される暗号化アルゴリズムを指定します。 この例では、168 ビット Data Encryption Standard（DES; データ暗号化規格）を指定します。
ステップ 3	**hash** {**md5** | **sha**} **例：** `Router(config-isakmp)# hash md5` `Router(config-isakmp)#`	IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。 この例では、Message Digest 5（MD5）アルゴリズムを指定します。デフォルトは、Secure Hash 標準（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 ポリシーに使用される認証方式を指定します。 この例では、事前共有キーを指定します。
ステップ 5	**group** {**1** | **2** | **5**} **例：** `Router(config-isakmp)# group 2` `Router(config-isakmp)#`	IKE ポリシーに使用される 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 セキュリティ アソシエーション（SA）のライフタイムを指定します。 • 指定できる値は 60 ～ 86400 です。
ステップ 7	**exit** **例：** `Router(config-isakmp)# exit` `Router(config)#`	ISAKMP ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto isakmp client configuration group** {**group-name** | **default**}
2. **key** *name*
3. **dns** *primary-server*
4. **domain** *name*
5. **exit**
6. **ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]

手順の詳細

	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含む IKE ポリシー グループを作成します。 また、ISAKMP グループ ポリシー 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	**key** *name* **例：** `Router(config-isakmp-group)# key secret-password` `Router(config-isakmp-group)#`	グループ ポリシーの IKE 事前共有キーを指定します。
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。 **（注）** グループの Windows インターネット ネーミング サービス（WINS）サーバを指定するには、**wins** コマンドを使用します。
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。

	コマンドまたはアクション	目的
ステップ 5	**exit** **例：** `Router(config-isakmp-group)# exit` `Router(config)#`	ISAKMP ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。
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。 このコマンドの詳しい説明およびその他の設定可能な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。

クリプト マップへのモード設定の適用

クリプト 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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto map** *map-name* **isakmp authorization list** *list-name*
2. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]

手順の詳細

	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)#`	クリプト 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 ポリシーのキー ルックアップ（IKE クエリ）をイネーブルにします。
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ルータが応答するように設定します。

ポリシー ルックアップのイネーブル化

AAA 経由でポリシー ルックアップ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 モードから始め、次の手順を実行します。

手順の概要

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]
4. **username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}

手順の詳細

	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 コントロール 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)#`	選択したユーザのログイン時の AAA 認証を指定し、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を使用します。 **（注）** RADIUS サーバを使用することもできます。詳細については、『*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)#`	PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに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を使用します。 **（注）** RADIUS サーバを使用することもできます。詳細については、『*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)#`	ユーザ名をベースとした認証システムを構築します。

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、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IKE のネゴシエーション中に、ピアは特定のトランスフォーム セットを使用してデータ フローを保護することに合意します。

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 セットが検出された場合、そのトランスフォーム セットが選択され、両方のピアの設定の一部として、保護する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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
2. **crypto ipsec security-association lifetime** {**seconds** *seconds* \| **kilobytes** *kilobytes*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**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 プロトコルとアルゴリズムの有効な組み合わせ）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 2	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*} **例：** `Router(config)# crypto ipsec security-association lifetime seconds 86400` `Router(config)#`	IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。 詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

（注） 手動で確立したセキュリティ アソシエーションの場合は、ピアとのネゴシエーションが存在しないため、両方に同じトランスフォーム セットを指定する必要があります。

IPSec 暗号方式およびパラメータの設定

ダイナミック クリプト マップ ポリシーでは、ルータがすべてのクリプト 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 ピアからの新規の SA 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 モードから始め、次の手順を実行します。

手順の概要

1. **crypto dynamic-map** *dynamic-map-name dynamic-seq-num*
2. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
3. **reverse-route**
4. **exit**
5. **crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

手順の詳細

	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 クリプト マップ エントリを作成し、クリプト 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)#`	クリプト 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)#`	クリプト 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。
ステップ 4	**exit** **例：** `Router(config-crypto-map)# exit` `Router(config)#`	クリプト マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 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)#`	クリプト マップ プロファイルを作成します。

物理インターフェイスへのクリプト マップの適用

クリプト マップは、IP Security（IPSec; IP セキュリティ）トラフィックが通過する各インターフェイスに適用されている必要があります。物理インターフェイスにクリプト マップを適用することにより、ルータがすべてのトラフィックを SA データベースに照合するようになります。デフォルト設定では、

ルータはリモート サイト間に送信されるトラフィックを暗号化して、安全な接続を提供します。ただし、パブリック インターフェイスでは他のトラフィックの通過を許可し、インターネットへの接続を提供しています。

インターフェイスにクリプト 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 モードから始め、次の手順を実行します。

手順の概要

1. **interface** *type number*
2. **crypto map** *map-name*
3. **exit**

手順の詳細

	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)#`	クリプト 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)#`	クリプト 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)#`	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。

Easy VPN リモート コンフィギュレーションの作成

IPSec リモート ルータとして機能するルータは、Easy VPN リモート コンフィギュレーションを作成し、発信インターフェイスに割り当てる必要があります。

リモート コンフィギュレーションを作成するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec client ezvpn** *name*
2. **igroup** *group-name* **key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **network extension plus**}
5. **exit**

6. **interface** *type number*
7. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
8. **exit**

手順の詳細

	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 コンフィギュレーションを作成します。続いて、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 接続の IPSec グループおよび IPSec キー値を指定します。
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、ルータから DNS サーバを介してホスト名解決を行える場合だけです。
ステップ 4	**mode** {**client** | **network-extension** | **network extension plus**} **例：** `Router(config-crypto-ezvpn)# mode client` `Router(config-crypto-ezvpn)#`	VPN 動作モードを指定します。
ステップ 5	**exit** **例：** `Router(config-crypto-ezvpn)# exit` `Router(config)#`	Cisco Easy VPN リモート 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。
ステップ 6	**interface** *type number* **例：** `Router(config)# interface fastethernet 4` `Router(config-if)#`	Cisco Easy VPN リモート コンフィギュレーション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。 **（注）** ATM WAN インターフェイスを使用しているルータの場合、このコマンドは **interface atm 0** になります。

	コマンドまたはアクション	目的
ステップ 7	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **例：** `Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside` `Router(config-if)#`	WAN インターフェイスに Cisco Easy VPN リモート コンフィギュレーションを割り当てます。 このコマンドにより、ルータは VPN 接続に必要な NAT またはポート アドレス変換（PAT）とアクセス リスト設定を自動的に作成します。
ステップ 8	**exit** **例：** `Router(config-crypto-ezvpn)# 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。

Easy VPN の設定の検証

```
Router# show crypto ipsec client ezvpn


Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

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 ファイルの一部を示します。

```
!
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
!
```

CHAPTER 15

シスコのマルチモード G.SHDSL EFM/ATM の設定

この章では、最初のマイル（EFM）/非同期転送モード（ATM）WAN ポートで、シスコのマルチモード 4 ペア G.SHDSL イーサネットを設定する方法を説明するマニュアルへのリンクを提供します。この機能は、Cisco C888-EA-K9 固定サービス統合型ルータ（ISR）によって提供されます。

次のガイドは、拡張された高速 WAN インターフェイス カード（EHWIC）および C888-EA-K9 ルータを含む複数の製品について、この機能を説明しています。

『*Configuring Cisco Multimode G.SHDSL EFM/ATM in Cisco ISR G2*』（次の URL で入手可能）

http://www.cisco.com/en/US/docs/routers/access/interfaces/software/feature/guide/GSHDSL_EFM_ATM_HWICS.html

CHAPTER 16

展開シナリオ

ここでは、Cisco 860、Cisco 880、および Cisco 890 シリーズ サービス統合型ルータ（ISR）の一般的な展開シナリオについて説明します。

構成例について

この章では、Cisco ISR の一般的な構成例について説明します。また、新機能に関する情報を示しながら各シナリオの高レベルな概要を提供します。

Cisco ISR の主な機能は次のとおりです。

- 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 5 章「バックアップ データ回線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 フィーチャ 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 フィーチャ 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、PoE 機能が含まれます。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。

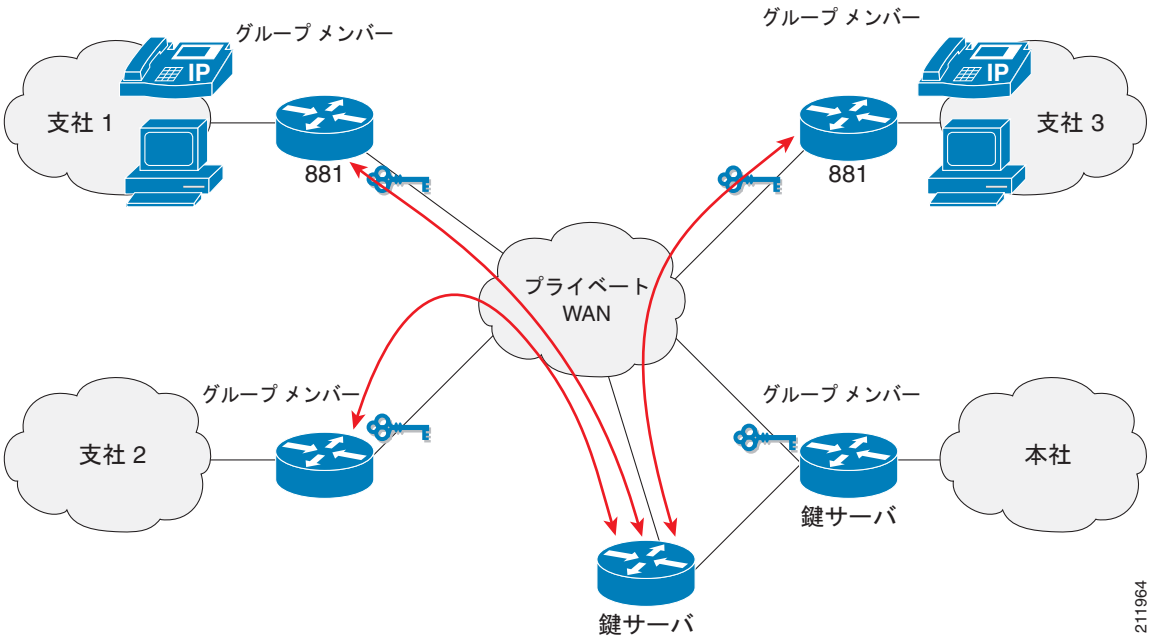
エンタープライズ スモール ブランチ

図 16-1 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層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 Firewall（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）

図 16-1　エンタープライズ スモール ブランチ

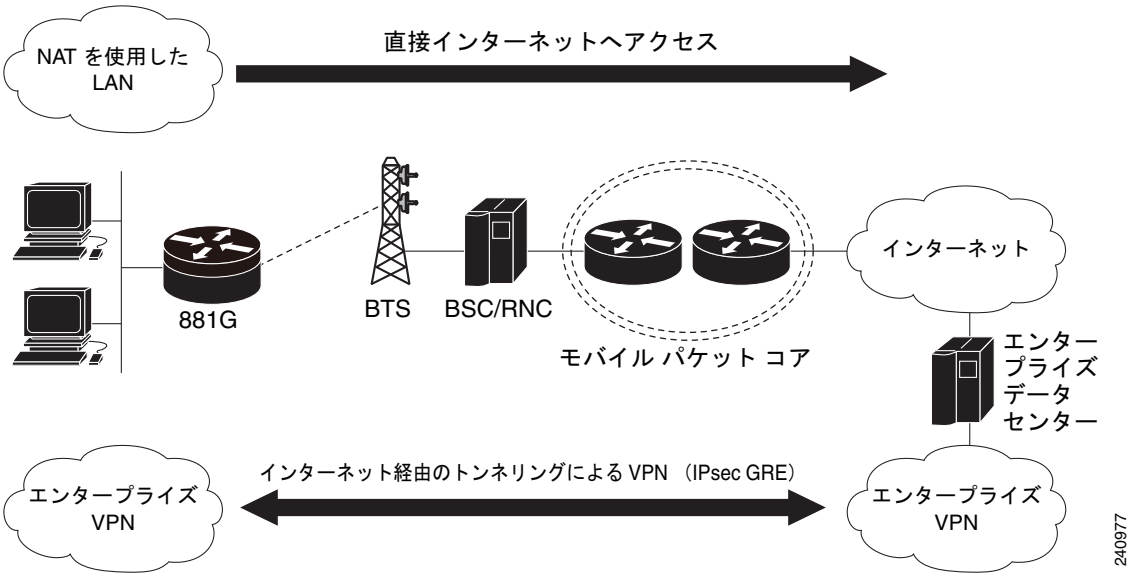


3G を使用したインターネット サービスと IPSec VPN

図 16-2 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、ネットワーク アドレス変換（NAT）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 16-2　　3G を使用したインターネット サービスと IPSec VPN



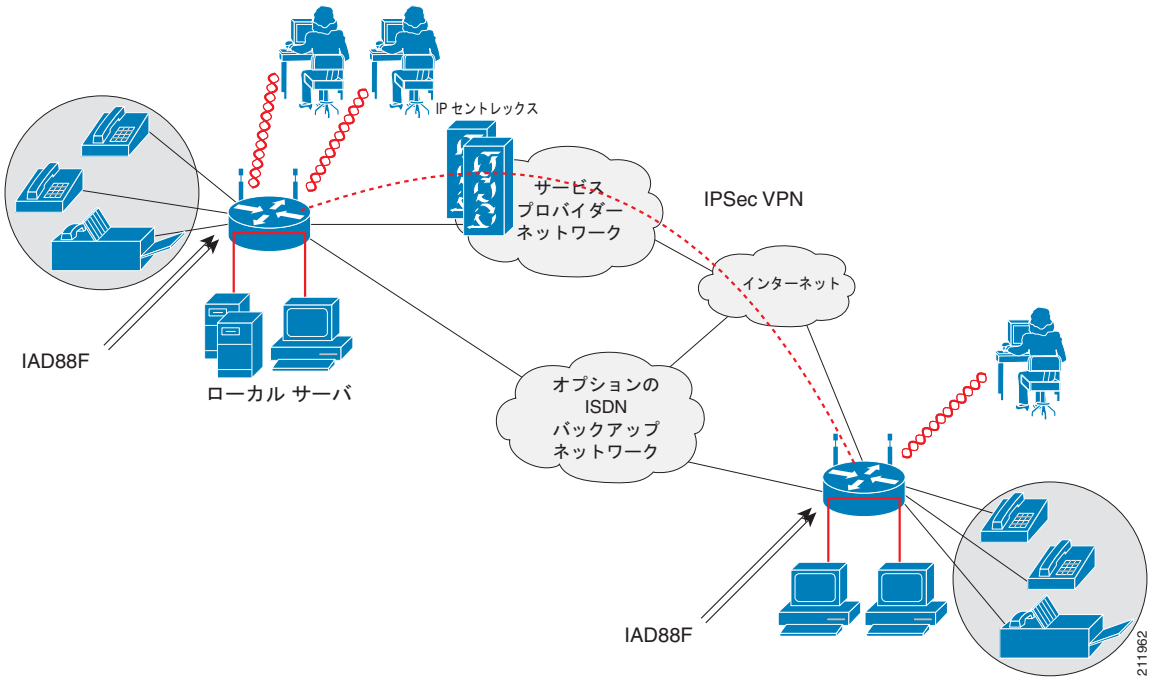
小規模から中規模のビジネス構成（SMB）アプリケーション

図 16-3 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。
- インラインの侵入防御システム（IPS）保護は、セキュリティを強化する、Cisco Self-Defending Network のコアとなる側面です。Cisco IOS IPS は、インテリジェンスな機能によってネットワーク自体を保護し、不正または有害なトラフィックを正確にリアル タイムで分類、識別し、停止またはブロックします。
- 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 16-3　　小規模から中規模のビジネス



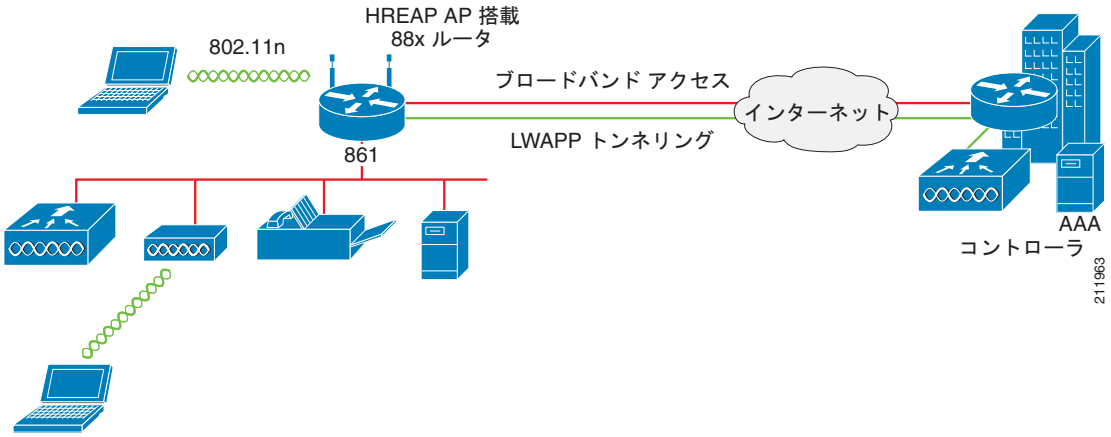
LWAPP を使用したエンタープライズ ワイヤレス構成

図 16-4 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。

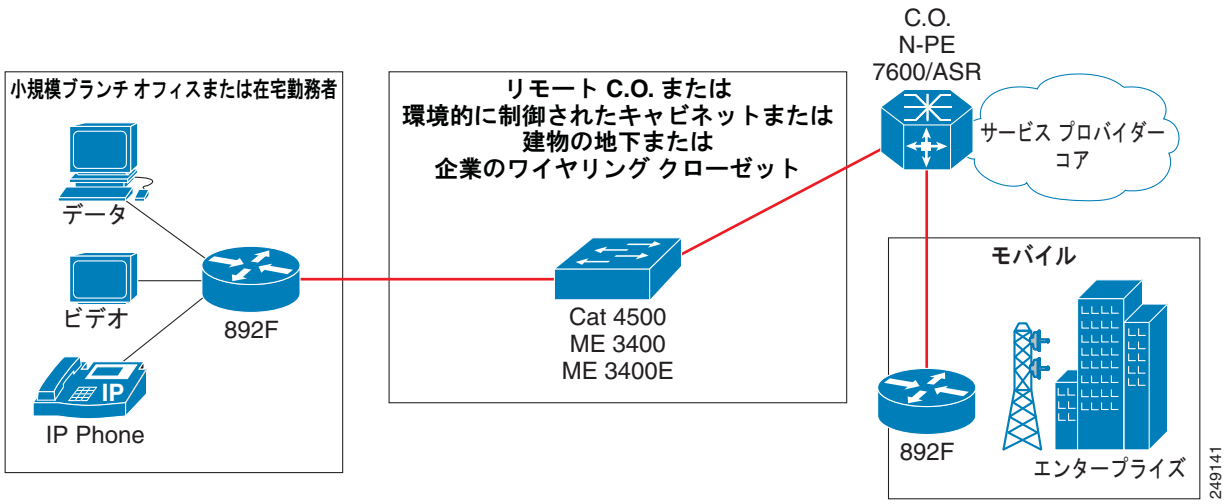
図 16-4　　LWAPP を使用したワイヤレス LAN



企業の小規模ブランチ オフィスへの展開

図 16-5 は、SFP ポートを通じてギガ ビット イーサネット ファイバ接続を使用する小規模なブランチ オフィスまたは在宅勤務者の展開を示しています。

図 16-5　　企業の小規模ブランチ オフィスへの展開



CHAPTER 17

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。この章の内容は、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.xvi）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の内容
- ソフトウェアのタイプとバージョン番号

- ハードウェアを受け取った日付
- 問題点の要約
- 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。点灯していない場合は、ルータが DSL アクセス マルチプレクサ（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。
- 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 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。
- Cisco 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る。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。点灯していない場合は、ルータが DSL アクセス マルチプレクサ（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 接続で問題が発生した場合は、次の状態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、ルータのハードウェア ガイドを参照してください。

- VDSL2 LED CD ライトが点灯している。点灯していない場合は、ルータが DSL アクセス マルチプレクサ（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、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 シグナリング 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。使用するコマンドは、次のとおりです。

controller vdsl 0 firmware *flash:<firmware file name>*

このコマンドにより、ファームウェア ファイルを VDSL モデムのチップセットにロードします。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。

（注） Cisco 860VAE シリーズ ISR では、新しい VDSL ファームウェアがロードされる前に、ルータがリロードされる（IOS のリロード）必要があります。

コマンドが存在しない場合、または指定されたファームウェアが破損または使用不可の場合は、デフォルトのファームウェア ファイル *flash:vdsl.bin* の存在と破損状態がチェックされます。その後で、このファイル内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。

（注） IOS リロード後に新しい VDSL ファームウェアのロードに失敗した場合、Cisco 860VAE シリーズ ISR は起動時に失敗の原因を表示します。

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 17-1 では、コマンド出力のメッセージを示しています。

例 17-1　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 17-2　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 17-3　　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 17-1 に、**show interfaces** コマンドの出力を示します。

表 17-1　　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。
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。

表 17-1　show interfaces コマンド出力の説明 （続き）

出力	原因
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

特定の PVC が使用中であるかどうかを判別するには、**ping atm interface** コマンドを使用します。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 17-4 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 17-4　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 17-5 を参照）。

例 17-5　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 17-2 は、コマンド出力で表示されるフィールドの一部です。

表 17-2　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を指定します。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; 物理層インターフェイス 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 17-6 に出力例を示します。

例 17-6　　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 17-7 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 17-8 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 17-7　　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 17-8　　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）の番号

vc *vpi/vci number*　ATM PVC の VPI/VCI の値

例 17-9 に、**debug atm packet** コマンドの出力例を示します。

例 17-9　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 17-3 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 17-3　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。

失われたパスワードの復旧

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、プロンプトに **no** で応答します。

```
Press RETURN to get started!
```

ステップ 6　Return 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　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 terminal** コマンドを実行します。

```
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　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 terminal** コマンドを実行します。

```
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。

Cisco Configuration Professional Express

ケーブルを接続してルータの電源を入れた後で、Cisco CP Express という Web ベースのアプリケーションを使用して、ルータを初期設定してください。

Cisco CP Express でルータを設定する手順については、『*Cisco CP Express User's Guide*』を参照してください。

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「ルータの基本設定」
- 第 16 章「展開シナリオ」

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 Release 12.3 のマニュアルを参照してください。

表 A-2　コマンド モードの概要

モード	アクセス方法	プロンプト	モードの終了および開始	モードの用途
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。	このモードは次の場合に使用します。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードから **enable** コマンドを入力します。	`Router#`	• ユーザ EXEC モードに戻る場合は、**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。	このモードは次の場合に使用します。 • 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」（P.A-5）の手順 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)#`	• 特権 EXEC モードに戻る場合は、**exit** または **end** コマンドを入力するか、**Ctrl+Z** 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 • 回線の設定

表 A-2　コマンド モードの概要 （続き）

モード	アクセス方法	プロンプト	モードの終了および開始	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードから（**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)#`	• グローバル コンフィギュレーション モードに戻る場合は、**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)#`	• グローバル コンフィギュレーション モードに戻る場合は、**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。
回線の設定	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)#`	• グローバル コンフィギュレーション モードに戻る場合は、**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。	このモードを使用して、端末回線のパラメータを設定します。

ヘルプの表示

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。どちらのパスワードでも、先頭文字に数字は使用できません。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　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 terminal** コマンドを実行します。

```
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　CLI の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	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）。 コマンドとともに入力できる利用可能なキーワードが表示されます。
`% Incomplete command.`	コマンドに必須のキーワードまたは値が、一部入力されていません。	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）。 コマンドとともに入力できる利用可能なキーワードが表示されます。
`% Invalid input detected at '^' marker.`	コマンドの入力ミスです。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。

コンフィギュレーションの変更の保存

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 を押すか、または対象の保存先ファイル名を入力して Enter 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。設定が保存されると、次のメッセージが表示されます。

```
Building configuration...
Router#
```

サマリー

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。以下に留意してください。

- コマンドの入力支援として、疑問符（**?**）と矢印キーを使用できます。

- 各コマンド モードは、一定のコマンド セットに制限されています。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。
- 機能を無効にするには、コマンドの前に **no** キーワードを入力します（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「ルータの基本設定」および第 16 章「展開シナリオ」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 Cisco 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 16 章「展開シナリオ」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、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層で最も一般的な伝送制御プロトコル/インターネット プロトコル（TCP/IP）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; ルーティング情報プロトコル）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; ルーティング情報プロトコル）
- Enhanced Interior Gateway Routing Protocol（Enhanced IGRP; 拡張 IGRP）

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 カウントが 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層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層アドレス 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; チャレンジ ハンドシェイク認証プロトコル）

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）

非同期転送モード（ATM）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、相手先固定接続（PVC）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 アダプテーション層）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、送信時に上位層情報をセルに分割し、受信時にセルを再び組み立てます。

Cisco 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、アドミニストレーティブ ディスタンスがダイナミック 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 ルートにアドミニストレーティブ ディスタンスを設定すると、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モニタ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、Cisco 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、Cisco 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ユーザ データグラム プロトコル（UDP）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）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 テクニックがすべてのネットワーク ルータに適しているわけではありません。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 専用アクセス レート（CAR）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、リソース予約プロトコル（RSVP）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。完全プライオリティ 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、ファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムの起動を助けます。ROM モニタを使用して、忘れてしまったパスワードの回復やコンソール ポートでの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、ROM モニタがルータを実行します。

この付録の構成は、次のとおりです。

ROM モニタの開始

ROM モニタを使用するには、端末または PC をコンソール ポート経由でルータに接続している必要があります。

次に再起動するときは ROM モニタ モードで起動するようにルータを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードを開始します。 プロンプトに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 レジスタ値でルータを再起動します。ルータは ROM モニタ モードのままで、Cisco IOS ソフトウェアは起動されません。 設定値が 0x0 である限り、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。 再起動したルータは ROM モニタ モードになります。新しく行が増えるごとにプロンプトの数字が増加します。

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、次のように、使用できるコマンドおよびオプションの一覧が表示されます。

```
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
```

860VAE ISR の ROM モニタ コマンド

Cisco 866VAE、867VAE、866VAE-K9 および 867VAE-K9 ISR は、次の ROM モニタ コマンドをサポートします。ROM モニタ プロンプトに **?** または **help** を入力すると、次のように、使用できるコマンドおよびオプションの一覧が表示されます。

```
rommon 1 > ?
alias              set and display aliases command
boot               boot up an external process
confreg            configuration register utility
delete             Delete file(s)-delete <filenames ...>
dev                List the device table
dir                List files in directories-dir <directory>
format             Format a filesystem-format <filessystem>
help               monitor builtin command help
history            monitor command history
meminfo            main memory information
repeat             repeat a monitor command
reset              system reset
set                display the monitor variables
showmon            display currently selected ROM monitor
sync               write monitor environment to NVRAM
tftpdnld           tftp image download
unalias            unset an alias
unset              unset a monitor variable
```

コマンドの大文字と小文字は区別されます。端末上で Break キーを押すとコマンドを停止できます。PC を使用している場合、Ctrl キーと Break キーを同時に押すと、ほとんどの端末エミュレーション プログラムはコマンドを停止します。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、一般的に使用される 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 **?**	使用できるすべての ROM モニタ コマンドを表示します。
-?	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`

表 C-1　一般的な ROM モニタ コマンド （続き）

コマンド	説明
reset または **i**	ルータをリセットまたは初期化します。電源投入時と同様の動作が行われます。
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)`
ブート 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ディザスタ リカバリ

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 ソフトウェアのコマンドライン インターフェイス（CLI）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、このコマンドはディザスタ リカバリの場合にだけ使用してください。

TFTP ダウンロードのコマンド変数

ここでは、ROM モニタ モードで設定し、TFTP ダウンロード プロセスで使用す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。

必須の変数

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*

オプションの変数

次の変数は、**tftpdnld** コマンドを使用する前に各コマンドで設定できます。

変数	コマンド
ファイル ダウンロードの進行状況をどのように表示するかを設定します。 0：進行状況は表示されません。 1：感嘆符（!!!）でファイル ダウンロードの進行状況を表示します。これはデフォルトの設定です。 2：ファイル ダウンロードの処理中に詳細な進行状況を表示します。例を示します。 • 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。デフォルト値は 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。デフォルトは 2,400 秒（40 分）です。	**TFTP_TIMEOUT=** *time*
ダウンロードされたイメージに対してルータがチェックサム テストを実行するかどうか。 1：チェックサム テストを実行します。 0：チェックサム テストを実行しない	**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** 変数は任意です。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
```

ルータが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 Non-Volatile RAM（NVRAM; 不揮発性 RAM）にあり、他の Cisco ルータと同じ機能を持っています。ROM モニタからでも、オペレーティング システム ソフトウェアからでも、仮想コンフィギュレーション レジスタの表示および変更ができます。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 レジスタの手動での変更

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 >
```

値は常に 16 進数と見なされます。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、ルータをリセットまたは再起動するまでは有効になりません。

コンフィギュレーション レジスタのプロンプトでの変更

confreg コマンドを引数なしで入力すると、仮想コンフィギュレーション レジスタの内容と、各ビットの意味を指定することによって内容を変更するための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、ルータをリセットまたは再起動するまでは有効になりません。

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、Cisco IOS イメージをルータ コンソール ポート経由で 115,200 bps でダウンロードする場合は、PC のシリアル ポートで 16550 汎用非同期送受信器（UART）が使用されていることを確認します。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	オプション。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 ビットの CRC です。
y	オプション。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。各プロトコルの相違は次のとおりです。 • Xmodem は 128 ブロックの転送サイズをサポートします。Ymodem は 1024 ブロックの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となるデバイスによっては、この機能が Xmodem でサポートされないことがあります。
r	オプション。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、フラッシュ メモリにイメージをロードします。
x	オプション。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。ルータに認識させるために、コンフィギュレーション ファイル名は *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。

デフォルトのボー レートを変更した場合は、端末のボー レートをコンフィギュレーション レジスタに指定されたボー レートに戻すことを指示するメッセージがエラー メッセージに続いて表示されます。

デバッグ コマンド

ROM モニタのほとんどのデバッグ コマンドは、Cisco IOS ソフトウェアがクラッシュまたは停止した場合にだけ機能します。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."
```

次に、ROM モニタのデバッグ コマンドを示します。

- **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、イメージを中止した理由、最大 8 フレームのスタック ダンプ、および例外が発生したアドレス（例外がある場合）などが含まれます。

```
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。ルータの次のリセット時または電源の再投入時に、コンフィギュレーション レジスタの値は 0x2101 になります。

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伝送制御プロトコル（TCP）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	—	未割り当て
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	日時
15	NETSTAT	Who is up または NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	キャラクタ ジェネレータ
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	シンプル メール転送プロトコル
37	TIME	時刻
39	RLP	リソース ロケーション プロトコル
42	NAMESERVER	ホストネーム サーバ
43	NICNAME	名前
49	LOGIN	ログイン ホスト プロトコル
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	トリビアル ファイル転送プロトコル
75	—	任意のプライベート ダイヤルアウト 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	ネットワーク インターフェイス カード（NIC）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	ルーティング情報プロトコル
525	Timed	タイム サーバ