Cisco 800 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

初版：2009 年 01 月 01 日

最終更新：2016 年 12 月 30 日

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

【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。

目 次

はじめに

ここでは、このマニュアルの対象読者、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。

対象読者

このマニュアルでは、Cisco 810、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。

このガイドは、シスコ製機器の販売者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。

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

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
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。
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。
レイヤ 3 インターフェイスでのイーサネット CFM と Y.1731 パフォーマンス モニタリングの設定, （89 ページ）	ネットワーク インターフェイス デバイスの機能、イーサネット データ プレーン ループバック、IEEE 接続障害管理、および Y.1731 パフォーマンス モニタリングを設定する手順について説明します。
電力管理の設定	電源管理と Power over Ethernet（PoE）の設定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。
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。
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。
シリアル インターフェイスの設定	WAN アクセスと集約、レガシー プロトコル トランスポート、ダイヤル アクセス サーバについて説明します。
ワイヤレス デバイスの設定	ワイヤレス デバイス、無線設定、WLAN、およびワイヤレス デバイスの管理の初期設定の手順について説明します。
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。
『Configuring PPP over ATM with NAT』	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。
4G LTE ワイヤレス WAN	4G LTE と 3G 携帯電話ネットワークについて説明します。

章	説明
DHCP および VLAN による LAN の設定	各ルータは Dynamic Host Configuration Protocol（DHCP）を使用することで、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有効にできます。
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。
シスコのマルチモード G.SHDSL EFM/ATM の設定	シスコのマルチモード 4 ペア G.SHDSL の設定について説明します。
展開シナリオ	Cisco 860、Cisco 880、および Cisco 890 シリーズ ISR の一般的な展開シナリオ例をいくつか示します。
Cisco 800 シリーズ ルータの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。
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。
概要	インターネット サービス プロバイダー（ISP）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。
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。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、**^D** または **Ctrl+D** というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。

表記法	説明
Italic フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
太字の courier フォント	太字の courier フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。
[x | y]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	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。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注）	「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。
ヒント	「問題解決に役立つ情報」です。
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	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	**「警告」の意味です。人身事故を予防するための注意事項が記述されています。**

関連資料

本マニュアルに加えて、Cisco 810、Cisco 860、Cisco 880 および Cisco 890 シリーズ ISR マニュアル セットには、以下のマニュアルが含まれます。

- 『*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』

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*』

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。

第 1 章

製品概要

この章では、Cisco 810、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。

Cisco 800 シリーズ ISR について

Cisco 860、Cisco 880、および Cisco 890 シリーズ ISR は、企業の在宅勤務者、ユーザが 20 人未満のリモート オフィスおよび小規模オフィスにインターネット、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 810 シリーズ ISR は、企業の在宅勤務者、ユーザが 20 人未満のリモート オフィス、および小規模オフィスにインターネット、VPN、データ、バックアップの各機能を提供するほか、マシン間接続を提供します。Cisco 810 シリーズ ISR には、Cisco 812 シリーズ ISR と Cisco 819 シリーズ ISR の 2 つの異なるシリーズがあります。Cisco 812 ISR は、ギガビット イーサネット（GE）、セルラー（3G）インターフェイスを介する WAN 接続、および WLAN をサポートします。Cisco 819 ISR は、4 つの 10/100 ファスト イーサネット（FE）、1 つのギガビット イーサネット（GE）、シリアルおよびセルラー（3G、4G）インターフェイスを介する WAN 接続、および WLAN を提供する固定構成のデータ ルータです。

Cisco 860 シリーズ ISR

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。

ここでは、次の内容について説明します。

Cisco 860 シリーズ ISR の機能

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。

Cisco 860 シリーズ ISR の 4 ポート 10/100 FE LAN スイッチ

4 ポート 10/100 FE LAN 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。

Cisco 860 シリーズ ISR のセキュリティ機能

Cisco 860 ISR 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

Cisco 860 シリーズ ISR の 802.11n 無線 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。

Cisco 860 VAE シリーズ ルータの一般的な機能

表 1：Cisco 860VAE シリーズ ISR の一般的な機能, （3 ページ） 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*：*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 • WW SP で展開されているさまざまな DSLAM との相互運用性の向上
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 サポート	• 最新の IP アドレッシング規格をサポート

機能	利点
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

Cisco 860 VAE シリーズ ISR のインターフェイス

表 2：Cisco 860VAE シリーズ ISR のインターフェイス，（4 ページ） 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 *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 FE[1] スイッチ ポート	○	○	○	○

1 GE[2] スイッチ ポート	—	—	○	○
1 つの GE WAN ポート	○	○	○	○
1 つの VDSL/ADSL over POTS ポート	—	○	—	○
1 つの VDSL/ADSL over ISDN ポート	○	—	○	—

1 FE = ファスト イーサネット
2 GE = 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。

表 3：C860VAE シリーズ ISR のインターフェイス，（5 ページ） では、C860VAE 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 *3*：*C860VAE* 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		
	C867VAE	C866VAE-K9	C867VAE-K9
3 FE[3] スイッチ ポート	○	○	○
2 GE[4] スイッチ ポート	○	○	○
1 つの GE WAN ポート	○	○	○
1 つの VDSL/ADSL over POTS ポート	○	—	○
1 つの VDSL/ADSL over ISDN ポート	—	○	—

3 FE = ファスト イーサネット
4 GE = ギガビット イーサネット

表 4：C860VAE-W シリーズ ISR のインターフェイス，（6 ページ） では、C860VAE 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 *4*：*C860VAE-W* 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			
	C866VAE-W-E-K9	C867VAE -W-E-K9	C867VAE -W-A-K9	C867VAE -POE-W-A-K9
3 FE[5] スイッチポート	○	○	○	○
2 GE[6] スイッチポート	○	○	○	○
1 つの GE WAN ポート	○	○	○	○
1 つの VDSL/ADSL over POTS ポート	—	○	○	○
1 つの VDSL/ADSL over ISDN ポート	○	—	—	—

5 FE = ファスト イーサネット
6 GE = ギガビット イーサネット

Cisco 860 VAE シリーズ ISR の IOS イメージ

表 5：Cisco 860VAE シリーズ ISR の IOS イメージ，（6 ページ） 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 *5*：*Cisco 860VAE* シリーズ *ISR* の *IOS* イメージ

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

表 6：C860VAE シリーズ ISR の IOS イメージ，（7 ページ） 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 *6*：*C860VAE* シリーズ *ISR* の *IOS* イメージ

IOS イメージ	モデル		
	C867VAE	C866VAE-K9	C867VAE-K9
c860vae-ipbasek9-mz	○	—	—
c860vae-advsecurityk9-mz	—	○	○
c860vae-advsecurityk9_npe-mz	—	○	○

表 7：C860VAE-W シリーズ ISR の IOS イメージ，（7 ページ） 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 *7*：*C860VAE-W* シリーズ *ISR* の *IOS* イメージ

IOS イメージ	モデル			
	C866VAE-W-E-K9	C867VAE -W-E-K9	C867VAE -W-A-K9	C867VAE -POE-W-A-K9
c860vaew-advsecurityk9-mz	○	○	○	○
c860vaew-advsecurityk9_npe-mz	○	○	○	○

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、構成が固定されたデータおよび音声ルータのファミリです。

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 8：Cisco 880 シリーズ データ ISR のポート構成, （8 ページ） に、Cisco 880 シリーズ データ ISR のポート構成を示します。

表 *8*：*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	—	○
886 および 886W	ADSL2oPOTS	○	—
886G および 886GW	ADSL2oPOTS	—	○
887 および 887W	ADSL2oPOTS	○	—
887G および 887GW	ADSL2oPOTS	—	○
887-VA-V	VDSL2oPOTS	○	○
887V および 887VW	VDSL2oPOTS	○	—
887VG および 887VGW	VDSL2oPOTS	—	○
888 および 888W	G.SHDSL	○	—
888G および 888GW	G.SHDSL	—	○
888E および 888EW	EFM over G.SHDSL	○	—
C888EA-K9	マルチモード	○	—

表 9：Cisco 880 シリーズ音声 ISR のポート構成, （8 ページ） に、Cisco 880 シリーズ音声 ISR のポート構成を示します。

表 *9*：*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	○	—
C888SRST および C888SRSTW	G.SHDSL	4	—	○
C888ESRST および C888ERSTW	EFM over G.SHDSL	4	—	4

表 10：Cisco 880 シリーズ データおよび音声 ISR のポート構成, （9 ページ） に、Cisco 881-V、Cisco887VA-V および Cisco 887VA-V-W シリーズ ISR のポート構成を示します。

表 *10*：*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	—	—	○
C887VA-V-W	VDSL2/ADSL2	4	2	○	—	○

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 11：Cisco 880 シリーズ データおよび音声 ISR でサポートされている同時通話数, （9 ページ） 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 *11*：*Cisco 880* シリーズ データおよび音声 *ISR* でサポートされている同時通話数

モデル	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

Cisco 880 シリーズ ISR の一般的な機能

Cisco 880 シリーズ ISR は次の機能をサポートしています。

Cisco 880 シリーズ ISR の 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。

Cisco 880 シリーズ ISR の 802.11n 無線 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。

Cisco 880 シリーズ ISR のリアルタイム クロック

リアルタイム クロック（RTC）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。

（注） Cisco 881V シリーズ ルータは、クロック ソースとして BRI2 をサポートしていません。クロック ソースとしてサポートしているのは BRI1 のみです。クロック ソースとして BRI2 を設定する場合、ルータは LINK DOWN メッセージを表示します。

Cisco 880 シリーズ ISR のセキュリティ機能

Cisco 880 ISR は、次のセキュリティ機能を提供します。

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

Cisco 880 シリーズ ISR の音声機能

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）、メディア ゲートウェイ コントロール プロトコル（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）
- デュアルトーン多重周波数（DTMF）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 上のダイヤルイン（DID）

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 12：Cisco 890 シリーズ ISR のポート構成，（11 ページ） に、Cisco 890 シリーズ ISR のポート構成を示します。

表 *12*：*Cisco 890* シリーズ *ISR* のポート構成

モデル	WAN ポート	データ バックアップ		
		FE	V.92	ISDN
891 および 891W	GE	○	○	—
892 および 892W	GE	○	—	○
892F および 892F-W	GE[7]、または SFP[8]	○	—	○

7 GE 銅線ポート
8 SFP ポートはファイバ接続で GE をサポート。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。

Cisco 890 シリーズ ISR でサポートされている機能には次のものがあります。

Cisco 890 シリーズ ISR の 8 ポート 10/100 FE LAN スイッチ

8 ポート 10/100 FE LAN 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。

Cisco 890 シリーズ ISR の 802.11n 無線 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。

Cisco 890 シリーズ ISR のリアルタイムク ロック

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

Cisco 890 シリーズ ISR のセキュリティ機能

Cisco 890 ISR は、次のセキュリティ機能を提供します。

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

Cisco 810 シリーズ ISR

このセクションでは、Cisco 810 シリーズ ISR によってサポートされている機能に関する情報を提供します。Cisco 810 シリーズ ISR には、Cisco 812 シリーズ ISR と Cisco 819 シリーズ ISR の 2 つの異なるシリーズがあります。

ここでは、次の内容について説明します。

Cisco 812 シリーズ ISR の機能

ここでは、Cisco 812 シリーズ ISR でサポートされるソフトウェア、プラットフォームおよびセキュリティ機能を示します。

（注） WAAS-Express 機能はサポートされていません。この機能は、以後の IOS リリースでの 3G および 4G インターフェイスにサポートされます。

Cisco 812 シリーズ ISR の 3G 機能

第 3 世代（3G）は、成長を促進し、帯域幅を増やし、より広範なアプリケーションをサポートするモバイル テクノロジー標準の世代です。Cisco 812 シリーズ ISR では、次の 3G 機能がサポートされています。

- モデム制御および管理
- 非同期転送（AT）コマンド セット
- Wireless Host Interface Protocol（WHIP）
- アウトオブバンド モデムの制御およびステータスのための Control and Status（CNS）
- Diagnostic Monitor（DM）ロギング
- アカウントのプロビジョニング
- モデム ファームウェアのアップグレード
- SIM のロックおよびロック解除
- MEP のロック解除
- OMA-DM の有効化、音声開始データ コールバック
- デュアル SIM カード スロット
- リンクの永続性
- SMS サービス
- Global Positioning System（GPS）サービス

- 3G MIB

Cisco 812 シリーズ ISR の WLAN 機能

ワイヤレス ローカルエリア ネットワーク（WLAN）は、ビルや敷地内の有線 LAN を交換するのではなく、頻繁に増強して、柔軟なデータ通信システムを実装します。WLAN では、無線周波数を使用して、データを無線で送受信し、有線接続の必要性を最小限にします。

Cisco 812 ISR は、次の WLAN 機能をサポートします。

Cisco 812 シリーズ ISR のデュアル無線

Cisco 802 アクセス ポイント（AP802）は、Cisco 812 ISR 上の統合アクセス ポイントです。アクセス ポイントは、無線ネットワークと有線ネットワーク間の接続ポイントとして、またはスタンドアロンの無線ネットワークのセンター ポイントとして機能する無線 LAN トランシーバです。大規模なインストールでは、複数のアクセス ポイントで提供されるローミング機能により、ネットワークへのアクセスを中断させることなく維持しながら、無線ユーザがファシリティ全体を自由に移動できます。

AP802 デュアル無線には、802.11b、802.11g、および 802.11n で使用されている 2.4 GHz と、802.11a および 802.11n で使用される 5 GHz の両方での接続に対応可能な、2 種類のワイヤレス無線があります。

Cisco 812 ISR のすべての WLAN トラフィックはイーサネット WAN または 3G インターフェイスを通過します。AP802 デュアル無線は、次の SKU でサポートされます。

- C812G-CIFI+7-E-K9
- C812G-CIFI+7-N-K9
- C812G-CIFI-V-A-K9
- C812G-CIFI-S-A-K9

Cisco 812 シリーズ ISR の CleanAir テクノロジー

CleanAir は、802.11n のパフォーマンスを保護するため、インテリジェントに無線周波数（RF）を回避する新しいワイヤレス テクノロジーです。詳細については、「Cisco CleanAir Technology」を参照してください。この機能は、WLAN サポートを含むすべての SKU でサポートされています。

Cisco 812 シリーズ ISR の動的周波数選択

動的周波数選択（DFS）は、802.11a の干渉から保護する必要があるレーダー信号を検出し、検出時に 802.11a の動作周波数をレーダー システムと干渉しない周波数に切り替える処理です。送信電力を規制要件と範囲情報に適合させるため、送信電力制御（TPC）が使用されます。

（注） DFS 機能は、FCC 認証を保留している FCC SKU に対してはディセーブルです。詳細については、「Dynamic Frequency Selection and IEEE 802.11h Transmit Power Control」を参照してください。

Cisco 812 シリーズ ISR のプラットフォーム機能

Cisco 812 ISR のすべてのプラットフォーム機能については、「Platform Features」を参照してください。

Cisco 812 シリーズ ISR のイーサネット WAN インターフェイス機能を使用した TFTP

TFTP ダウンロードの詳細については、「Disaster Recovery with TFTP Download」を参照してください。

（注） Cisco 812 ISR には、唯一のイーサネット インターフェイスとして GE インターフェイスがあります。このため、ポート番号は TFTP 接続に対して ROMmon で自動的に設定されます。

Cisco 812 シリーズ ISR の SKU 情報

Cisco 812 シリーズ ISR ルータに使用できる SKU については、次のリンクを参照してください。

http://www.cisco.com/en/US/docs/routers/access/800/812/hardware/install/guide/overview.html#wp1057240
Cisco 812 シリーズの SKU 情報

Cisco 819 シリーズ ISR の機能

ここでは、Cisco 819 シリーズ ISR でサポートされるソフトウェア、プラットフォームおよびセキュリティ機能を示します。

（注） WAAS-Express 機能はサポートされていません。この機能は、以後の IOS リリースでの 3G および 4G インターフェイスにサポートされます。

Cisco 819 シリーズ ISR の G 機能

Cisco 819 シリーズ ISR ルータでは、次の 3G 機能がサポートされています。

- モデム制御および管理
- 非同期転送（AT）コマンド セット

- Wireless Host Interface Protocol（WHIP）
- アウトオブバンド モデムの制御およびステータスのための Control and Status（CNS）
- Diagnostic Monitor（DM）ロギング
- アカウントのプロビジョニング
- モデム ファームウェアのアップグレード
- SIM のロックおよびロック解除
- MEP のロック解除
- OMA-DM アクティベーション
- デュアル SIM カード スロット
- リンクの永続性
- SMS サービス
- Global Positioning System（GPS）サービス
- 3G MIB

Cisco 819 シリーズ ISR の WLAN 機能

Cisco 819 シリーズ ISR は次の WLAN 機能をサポートしています。

- デュアル無線
- CleanAir テクノロジー
- Dynamic Frequency Selection（動的周波数選択）

Cisco 819 シリーズ ISR の 4G LTE 機能

Cisco 819 シリーズ ISR は次の 4G LTE 機能をサポートしています。

- IPv4 ベアラー
- MIPv4、NEMOv4、RFC 3025
- LTE UE インターフェイス背後の IPv4 サブネット
- 4G LTE および 3G サービス間のシームレスなハンドオフを可能にする Evolved High-Rate Packet Data（EHRPD）（C819(H)G-4G-V-K9 のみ）
- LTE および EHRPD ネットワーク間のシームレスなハンドオフ（C819(H)G-4G-V-K9 のみ）
- LTE サービスからのフォールバック オプションとして UMTS サービスのサポート（C819(H)G-4G-A-K9 および C819(H)G-4G-G-K9 のみ）

- LTE と UMTS サービス間のシームレスなハンドオフ（C819(H)G-4G-A-K9 および C819(H)G-4G-G-K9 のみ）
- Qualcomm の診断モニタ ポートへのリモート アクセス
- ワイヤレス設定 FOTA を含む OTA-DM（C819(H)G-4G-V-K9 のみ）
- モデムのプロビジョニングのためのミニ USB タイプ 2 コネクタ

Cisco 819 シリーズ ISR のプラットフォーム機能

Cisco 819 シリーズ ISR プラットフォーム機能の完全なリストについては、「Platform Features for Cisco 819 ISRs」を参照してください。

Cisco 819 シリーズ ISR のセキュリティ機能

Cisco 819 ISR は、次のセキュリティ機能を提供します。

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

Cisco 819 シリーズ ISR の SKU 情報

Cisco 819 シリーズ ISR ルータに使用できる SKU については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/800/hardware/installation/guide/800HIG/prodoverview.html#pgfId-1146483

Cisco 800 シリーズ ISR のライセンス

Cisco 810、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。

Cisco 800 シリーズ ISR の機能セットの選択

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 810、Cisco 860、Cisco 880、および Cisco 890 プラットフォームのソフトウェア ライセンスで利用できる機能の一覧については、Cisco 812 データ シート、Cisco 819 データ シート、Cisco 860 データ シート、Cisco 880 データ シート、および Cisco 890 データ シート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。

第 2 章

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 モードのアクセス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」の項を参照してください。

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 モードのアクセス方法の詳細については、A-5 ページの「グローバル コンフィギュレーション モードの開始」の項を参照してください。

インターフェイス ポート

表 13：Cisco 860、880、および 890 シリーズ ルータでサポートされているインターフェイスと関連付けられているポート ラベル，（20 ページ） に、Cisco 860、880 と 890 シリーズ ルータでサポートされているインターフェイス、および各インターフェースに関連付けられている機器上のポート ラベルを一覧表示します。

表 *13*：*Cisco 860*、*880*、および *890* シリーズ ルータでサポートされているインターフェイスと関連付けられているポート 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
	Wireless LAN（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

ルータ	インターフェイス	ポート ラベル
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

表 ***14*** : ***Cisco 810*** シリーズ ***ISR*** でサポートされているインターフェイスとポート ラベル

ルータ	インターフェイス	ポート ラベル
Cisco 819 シリーズ ルータ	4 ポート ファスト イーサネット LAN	LAN、FE0–FE3
	ギガビット イーサネット WAN	GE WAN 0
	シリアル（Serial）	シリアル（Serial）
	3G ポート プロビジョニング用ミニ USB	3G RSVD
	コンソール/Aux ポート	CON/AUX
Cisco 812 シリーズ ルータ	ギガビット イーサネット WAN	GE WAN 0
	3G ポート プロビジョニング用ミニ USB	3G RSVD
	コンソール/Aux ポート	CON/AUX

デフォルト設定

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、**showrunning-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：チャレンジ ハンドシェイク認証プロトコル（CHAP）またはパスワード認証プロトコル（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。次のいずれかを指定できます。

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

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

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

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

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

- 3G を設定している場合：
  - Cisco 819 ISR で通信事業者からのサービスを使用可能でなければなりません。また、ルータが物理的に置かれているネットワーク 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、「Cisco 3G Wireless Connectivity Solutions」のデータシートを参照してください。
  - ワイヤレス サービス プロバイダーのサービス プランに登録し、SIM カードを取得する必要があります。
  - SIM カードを取り付けてから 3G Cisco 819 ISR を設定する必要があります。SIM カードの取り付け方法については、Cisco 800 シリーズの『Configuring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)』を参照してください。
  - Cisco 819 ISR の 3G を設定する前に必要なアンテナを取り付ける必要があります。アンテナの設置方法については、表 15：アンテナの設置手順, （25 ページ）を参照してください。

表 *15*：アンテナの設置手順

アンテナ	アンテナの設置手順
3G-ANTM1919D	『Cisco Multiband Swivel-Mount Dipole Antenna (3G-ANTM1919D)』を参照。http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/antdi806.html
3G-ANTM1916-CM	『Cisco Multiband Omnidirectional Ceiling Mount Antenna (3G-ANTM1916-CM)』を参照。
3G-AE015-R（アンテナの拡張）	『Cisco Single-Port Antenna Stand for Multiband TNC Male-Terminated Portable Antenna (Cisco 3G-AE015-R)』を参照。
3G-AE010-R（アンテナの拡張）	『Cisco Single-Port Antenna Stand for Multiband TNC Male-Terminated Portable Antenna (Cisco 3G-AE015-R)』を参照。http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/antex15r.html このドキュメントは、3G-AE015-R と 3G-AE010-R の両方を対象にしています。この 2 つの製品はケーブルの長さのみが異なります。
3G-ANTM-OUT-OM	『Cisco 3G Omnidirectional Outdoor Antenna (3G-ANTM-OUT-OM)』を参照。
3G-ANTM-OUT-LP	『Cisco Multiband Omnidirectional Panel-Mount Antenna (3G-ANTM-OUT-LP)』を参照。
3G-ACC-OUT-LA	『Cisco 3G Lightning Arrestor (3G-ACC-OUT-LA)』を参照。
4G-ANTM-OM-CM	『Cisco 4G Indoor Ceiling-Mount Omnidirectional Antenna (4G-ANTM-OM-CM)』を参照。

- ◦表 2-1 に説明したように、信号の受信状況について LED を確認する必要があります。
  ◦Cisco IOS ソフトウェアに精通している必要があります。Cisco 3G のサポートについては、リリース 12.4(15)T またはそれ以降の Cisco IOS マニュアルを参照してください。
  ◦3G データ プロファイルを設定するには、サービス プロバイダーからユーザ名、パスワード、およびアクセス ポイント名（APN）を取得する必要があります。

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, （26 ページ）のタスクから始めて、ルータですべての設定を行います。

- 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

	コマンドまたはアクション	目的
ステップ 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number* 例： `Router(config)# line console 0`	ライン 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-line)# password 5dr4Hepw3`	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。

	コマンドまたはアクション	目的
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。 この例は 5 分 30 秒のタイムアウトを示しています。「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。
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`	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。

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. **configureterminal**
2. **hostname** *name*
3. **enablesecret** *password*
4. **noipdomain-lookup**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configureterminal**
	例：
	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： 例： `Router(config)# hostname Router`	ルータ名を指定します。
ステップ 3	**enablesecret** *password* 例： 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	**noipdomain-lookup** 例： 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

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. **ipaddressip-addressmask**
3. **noshutdown**
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`	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	**ipaddressip-addressmask** 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	**noshutdown** 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`	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。

次の作業

（注） Cisco IOS リリース 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。パケットがバッチで処理されるとキャッシュ使用の効率性が高まるため、インターフェイスのバッチ処理が有効な場合は、CPU 使用率が低下しているのがわかる場合があります。

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

	コマンドまたはアクション	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`
		
		例：
		`OR`
		
		例：
		`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`	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. **ipaddressip-addressmask**
3. **noshutdown**
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 gigabitethernet 1`	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	**ipaddressip-addressmask** 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	**noshutdown** 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`
	
	例：
	`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. **ipaddressip-addressmask**
3. **encapsulation** *ppp*
4. **dialerin-band**
5. **dialerstring** *dial-string*
6. **dialer-group** *group-number*
7. **asyncmodededicated**
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	**interface** type number 例： 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	**ipaddressip-addressmask** 例： 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： 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	**dialerin-band** 例： 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。

	コマンドまたはアクション	目的
ステップ 5	**dialerstring** *dial-string* 例： 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： 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	**asyncmodededicated** 例： 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：
	例：
	`Router(config-if)# exit`
	例：
	`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. **ipaddressip-addressmask**
4. **shutdown**
5. **noshutdown**
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	**controller** *vdsl 0* 例： 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： 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	**ipaddressip-addressmask** 例： 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： 例： `Router(config-if)# 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。

	コマンドまたはアクション	目的
ステップ 5	**noshutdown** 例： 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： 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、次の内容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。

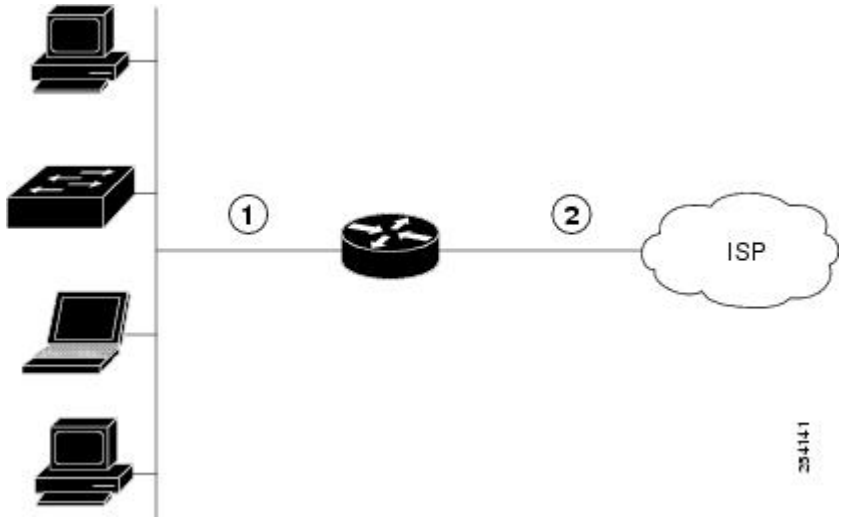
（注） 866VAE および 886VA は、ISDN 経由の xDSL をサポートします。867VAE および 887VA は、従来のアナログ電話回線（POTS）経由の xDSL をサポートします。

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 1：トポロジの例, （36 ページ） 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 *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 リリース 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 リリース 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, （51 ページ）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, （52 ページ）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，（53 ページ）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

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}**
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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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： 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 4	operating mode **{auto|adsl1|adsl2|adsl2+|vdsl2|ansi}** 例： 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：
	
	例：
	
	`Router(config-controller)# end`
	
	例：
	
	`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。

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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	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`
	
	例：
	
	`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`	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。

	コマンドまたはアクション	目的
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。

手順の概要

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

手順の詳細

	コマンドまたはアクション	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。

	コマンドまたはアクション	目的
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`	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

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}**
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	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。

	コマンドまたはアクション	目的
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

	コマンドまたはアクション	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。

	コマンドまたはアクション	目的
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`	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。

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

	コマンドまたはアクション	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。

	コマンドまたはアクション	目的
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`	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

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

（注） Cisco 867VAE と 867VAE-K9 では、Cisco IOS リリース 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。

Over POTS VDSL2/ADSL マルチモード Annex A SKU の ADSL2/2+ Annex M モードの設定

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。 • パスワードを入力します（要求された場合）。
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 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、および 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、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。

	コマンドまたはアクション	目的
		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：デフォルトの設定。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

1. **enable**
2. **configure terminal**
3. **controllervdsl** *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。 • パスワードを入力します（要求された場合）。
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	**controllervdsl** *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。

設定例：シームレス レート適応

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。 • パスワードを入力します（要求された場合）。
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、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、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』の「Troubleshooting」の項も役に立ちます。

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 **debugvdsl0traininglog** を使用してトレーニング ログの取得を開始すると、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. **controllerdsl** *slot/port*
2. **modeatm**
3. **line-termcpe**
4. **line-mode4wirestandard**
5. **line-rate**{**auto** |*rate*}
6. **interfaceatm** *interface-number*
7. **ip-address** *ip-address*
8. **load-interval** *seconds*
9. **noatmilmi-keepalive**[*seconds*]
10. **pvc** [*name*] *vpi/vci*
11. **protocol** *protocol protocol-address* **broadcast**
12. **encapsulation** [*encapsulation-type]*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**controllerdsl** *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	**modeatm** 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-termcpe** 例： `Router(config-ctrl)# line-term cpe`	CPE をイネーブルにします。
ステップ 4	**line-mode4wirestandard** 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。

	コマンドまたはアクション	目的
		（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	**interfaceatm** *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。
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	**noatmilmi-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。

	コマンドまたはアクション	目的
		• aal5snap キーワードを AAL5+LLC/SNAP（デフォルト）に使用します。

設定例：G.SHDSL WAN インターフェイスの設定

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
!
```

G.SHDSL WAN インターフェイス設定の確認

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 にある『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 シリーズおよび Cisco 810 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、Cisco 880 シリーズ用の 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 16：前面パネル LED の信号強度表示，（62 ページ）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 NX-OS リリース 4.1 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 *16*：前面パネル *LED* の信号強度表示

LED	LED カラー	信号強度
P3G RSSI[9]	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
	グリーンに点灯	高速 RSSI（-69 dBm 以上）
	グリーンが素早く（16 Hz）点滅	中速 RSSI（-89 ～ -70 dBm）
	グリーンがゆっくり（1 Hz）点滅	低～中速 RSSI（-99 ～ -90 dBm）、信頼できる接続の最小レベル
	消灯	低速 RSSI（-100 dBm 未満）

9 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連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の確認

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。

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

（注） Cisco 867VAE と 867VAE-K9 では、Cisco IOS リリース 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. **showcellular0network**
2. show cellular 0 hardware
3. show cellular 0 connection
4. **showcellular0radio**
5. **showcellular0profile**
6. **showcellular0security**
7. **showcellular0all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showcellular0network** 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	**showcellular0radio** 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。

	コマンドまたはアクション	目的
ステップ 5	**showcellular0profile** 例： `Router# show cellular 0 profile`	作成されたモデム データ プロファイルに関する情報を示します。
ステップ 6	**showcellular0security** 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	**showcellular0all** 例： `Router# show cellular 0 all`	モデムに関する統合情報を示します。たとえば、作成されたプロファイル、ラジオ信号強度、ネットワーク セキュリティなどです。

GSM モデル データ プロファイルの設定

新しいモデム データ プロファイルを設定、または作成するには、特権 EXEC モードで **cellular0gsmprofilecreate<profilenumber><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 17：モデム データ プロファイルのパラメータ，（65 ページ）を参照してください。

例

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

表 17：モデム データ プロファイルのパラメータ，（65 ページ） 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 *17*：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。
認証	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 18：CDMA モデム アクティベーションおよびプロビジョニング, （66 ページ） 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 *18*：*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[10] Activation	Verizon Wireless
IOTA[11]（データ プロファイル リフレッシュ用）	Sprint

10 OTASP = Over the Air Service Provisioning（電波によるサービス提供）
11 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、インターネット地上波（IOTA）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
```

セルラー 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。

（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。

手順の概要

1. configure terminal
2. **interfacecellular0**
3. **encapsulationppp**
4. **pppchaphostname** ホスト
5. **pppchappassword** 0 password
6. **asynchronousmodeinteractive**
7. **ipaddressnegotiated**

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	**interfacecellular0** 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	**encapsulationppp** 例： `Router (config-if)# encapsulation ppp`	専用非同期モード用またはダイヤルオンデマンドルーティング（DDR）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	**pppchaphostname** ホスト 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。

	コマンドまたはアクション	目的
ステップ 5	**pppchappassword** 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	**asynchronousmodeinteractive** 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	**ipaddressnegotiated** 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。

次の作業

（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。インターネット プロトコル コントロール プロトコル（IPCP）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，（73 ページ）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. **configureterminal**
2. **interfacecellular0**
3. **dialerin-band**
4. **dialeridle-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. GSM の場合：
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	**configureterminal** 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	**interfacecellular0** 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	**dialerin-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	**dialeridle-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。

	コマンドまたはアクション	目的
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。
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：	GSM の回線を設定します。

	コマンドまたはアクション	目的

	例：
	`chat-script script name ”” “ATDT*99* profile number#” TIMEOUT timeout value CONNECT`
	例：
	`For CDMA:`
	例：
	`chat-script` *script name* `""` `"ATDT*777*` *profile number*`#"` `TIMEOUT` *timeout value* `CONNECT`
	例：
	`Router (config)# chat-script gsm "" "ATDT*98*2#" TIMEOUT 60 "CONNECT"`
		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 **cdmaddtm** 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

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ときに、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
```

セルラー ネットワーク用デュアル SIM の Cisco 819 シリーズ ISR での設定

デュアル SIM 機能は、2 つのセルラー ネットワーク間の自動スイッチおよびフェールオーバーを Cisco 819 ISR に実装します。この機能は、プライマリ スロットである SIM スロット 0 とセカンダリ（フェールオーバー）スロットであるスロット 1 を使用して、デフォルトでイネーブルになっています。

（注） 4G LTE セルラー ネットワークのデュアル SIM 機能を設定する方法については、『Cisco 4G LTE ソフトウェア インストール ガイド』を参照してください。

次のコマンドを使用して、デュアル SIM 機能を設定できます。

コマンド	構文	説明
gsm failovertimer	**gsm failovertimer <1-7>**	フェールオーバー タイマーを分単位で設定します。
gsm sim authenticate	**gsm sim authenticate <0,7> <pin> slot <0-1>**	SIM CHV1 コードを確認します。
gsm sim max-retry	**gsm sim max-retry <0-65535>**	フェールオーバー リトライの最大回数を指定します。デフォルト値は 10 です。
gsm sim primary slot	**gsm sim primary slot <0-1>**	プライマリ スロットの割り当てを変更します。
gsm sim profile	**gsm sim profile <1-16> slot <0-1>**	SIM プロファイルを設定します。

次の点に注意してください。

- 自動スイッチおよびフェールオーバーを機能させるには、**gsmsimprofile** コマンドを使用して、スロット 0 および 1 に SIM プロファイルを設定します。
- 動作スイッチおよびフェールオーバーを機能させるには、特定のプロファイル番号なしのチャット スクリプトを設定します。
- SIMプロファイルが設定されていない場合、プロファイル#1がデフォルトで使用されます。
- GSM フェールオーバー タイマーが設定されていない場合、デフォルトのフェールオーバーのタイムアウトは 2 分です。
- GSM SIM プライマリ スロットが設定されていない場合、デフォルトのプライマリ SIM はスロット 0 です。

次に、SIM スイッチオーバーのタイムアウト時間を 3 分に設定する例を示します。

```
router(config-controller)# gsm failovertimer 3
```

次に、暗号化されていないピンを使用して認証する例を示します。

router(config-controller)# **gsmsimauthenticate01234slot0**

次に、SIM スイッチオーバーのリトライ最大回数を 20 に設定する例を示します。

router(config-controller)# **gsmsimmax-retry20**

次に、プライマリ スロットとして SIM スロット 1 を設定する例を示します。

```
router(config-controller)# gsm sim primary slot 1
```

次に、プロファイル 10 を使用するように、スロット 0 の SIM カードを設定する例を示します。

```
router(config-controller)# gsm sim profile 10 slot 0
```

手動で SIM を切り替えるには、次のコマンドを実行します。

コマンド	構文	説明
cellular GSM SIM	**cellular GSM SIM {lock | unlock}**	SIMをロックまたはロック解除します。
gsm sim	**cellular <unit> gsm sim [lock | unlock] <pin>**	gsm SIMをロックまたはロック解除します。
gsm sim unblock	**cellular <unit> gsm sim unblock <puk> <newpin>**	gsm SIMのブロックを解除します。
gsm sim change-pin	**cellular <unit> gsm sim change-pin <oldpin> <newpin>**	SIM の PIN を変更します。
gsm sim activate slot	**cellular <unit> gsm sim activate slot <slot_no>**	GSM SIM をアクティブにします。

次のコマンドは、強制的にモデムを SIM1 に接続します。

```
Router# cellular
0
 gsm sim activate
slot 1
```

プッシュ ボタンを使用したイメージおよび Config の復元のための Cisco 819 Series ISR ルータの設定

プッシュ ボタン機能は Cisco 819 ISR で使用できます。ルータの前面パネルのリセット ボタンは、この機能をイネーブルにします。

この機能を使用するには、次の手順を実行します。

手順の概要

1. 電源プラグを外します。
2. ルータの前面パネルのリセット ボタンを押します。
3. リセット ボタンを押しながら、システムの電源を投入します。

手順の詳細

ステップ 1 電源プラグを外します。

ステップ 2 ルータの前面パネルのリセット ボタンを押します。

ステップ 3 リセット ボタンを押しながら、システムの電源を投入します。
システム LED が 4 回点滅し、ルータがボタンの押下を受け入れていることを示します。

次の作業

このボタンの使用は、ROMMON の初期化中にのみ有効です。ウォーム リブート中にこのボタンを押しても、パフォーマンスには影響しません。表 19：ROMMON の初期化中のプッシュ ボタンの機能，（77 ページ） に、ROMMON の初期化中にボタンが押された場合の高レベルの機能を示します。

表 *19* : ***ROMMON*** の初期化中のプッシュ ボタンの機能

ROMMON の動作	IOS の動作
• デフォルトのボー レートを使用してブートします。 • 自動ブートを実行します。 • コンパクト フラッシュで *.default イメージを使用可能な場合はロードします。 （注） *.defaultイメージを使用できない場合は、ROMMONはフラッシュ上の最初のCisco IOSイメージを使用して起動されます。 デフォルトイメージの名前の例： c800-universalk9-mz.SPA.default c-800-universalk9_npe-mz.151T.default image.default （注） *.cfg オプションを含むコンフィギュレーション ファイルを 1 つだけ使用できます。複数のファイルが存在する場合は、不確かな動作上の反応が現れます。	*.cfg という設定が NVRAM ストレージまたはフラッシュ ストレージで使用できる場合、IOS は元の設定のバックアップを実行し、この設定を使用して起動されます。 （注） *.cfg オプションを含むコンフィギュレーション ファイルを 1 つだけ使用できます。複数のファイルが存在する場合は、不確かな動作上の反応が現れます。

ルータの現在のブートアップ モードを表示するには、show platform コマンドを使用します。次の項では、ボタンが押されていないときと、ボタンが押されたときの出力例を示します。

ボタンが押されていないときの出力：例

```
router# show platform boot-record
Platform Config Boot Record :
============================
Configuration Register at boot time : 0x0
Reset Button Status at Boot Time    : Not Pressed
Startup-config Backup Status at Boot: No Status
Startup-config(backup file)location : No Backup
Golden config file at location      : No Recovery Detected
Config Recovery Status              : No Status
```

ボタンが押されたときの出力：例

```
router# show platform boot-record


Platform Config Boot Record :
============================
Configuration Register at boot time : 0x0
Reset Button Status at Boot Time    : Pressed
```

```
Startup-config Backup Status at Boot: Ok
Startup-config(backup file)location : flash:/startup.backup.19000716-225840-UTC
Golden config file at location      : flash:/golden.cfg
Config Recovery Status              : Ok
```

WLAN AP のプッシュ ボタン

前面パネルのボタンが押されると、WLAN AP はイメージと設定の両方の復元を実行します。

イメージの復元を実行する場合、WLANはブートローダに移行し、ユーザがブートローダプロンプトからイメージをダウンロードできるようになります。

```
To perform configuration recovery, WLAN AP will overwrite the contents of flash:/config.txt
 with the contents of flash:/cpconfig-ap802.cfg file if available in flash drive. Otherwise,
 flash:/config.txt will be deleted.
```

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。いずれかの DSL インターフェイスで **noshutdown** コマンドを入力すると、*WAN interface is Ethernet* というメッセージが表示されてコマンドは拒否されます。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 ダウン状態になり、**noshutdown** コマンドは *WAN interface is DSL* というメッセージを表示して拒否されます。

（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からイーサネットインターフェイスに、またはその逆に切り替えるには、**wanmodedsl|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

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. **showrunning-configuration**
3. **wanmode{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。 • パスワードを入力します（要求された場合）。
ステップ 2	**showrunning-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	**wanmode{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`
	例：
	`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、**showrunning-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、を参照してください。イーサネット スイッチの設定, （181 ページ）

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、ワイヤレス デバイスの設定を参照してください。ワイヤレス デバイスの設定, （229 ページ）

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** *loopback number*
2. **ipaddress** *ip-address mask*
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** *loopback number* 例： `Router(config)# interface Loopback 0`	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	**ipaddress** *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`
	
	例：
	
	`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。

設定例：ループバック インターフェイスの設定

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. **iproute** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **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	**iproute** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}	IP パケットのスタティック ルートを指定します。

	コマンドまたはアクション	目的
	例： `Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`	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`	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。

次の作業

スタティック ルーティングの一般的な情報については、B-1 ページの「概念」セクション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)」と示されているコマンドは、入力する必要はありません。このコマンドは、**showrunning-config** コマンドの使用時に生成されるコンフィギュレーション ファイルに自動的に表示されます。

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

スタティック ルーティングの設定確認

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

Routing Information Protocol の設定

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. **configureterminal**
2. **routerrip**
3. **version** {**1** | **2**}
4. **network** *ip-address*
5. **noauto-summary**
6. **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	**configureterminal** 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	**routerrip** 例： `Router(config)# router rip`	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 3	**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。

	コマンドまたはアクション	目的
ステップ 4	**network** *ip-address* 例： `Router(config-router)# network 192.168.1.1`	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。
ステップ 5	**noauto-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、サブプレフィックス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。
ステップ 6	**end** 例： `Router(config-router)# end`	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。

次の作業

RIP の一般的な情報については、B-3 ページの「RIP」セクションを参照してください。

設定例：ダイナミック ルーティング プロトコルの設定

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。

この設定を表示するには、特権 EXEC モードで **showrunning-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
!
```

RIP の設定確認

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
```

Enhanced Interior Gateway Routing Protocol 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. **routereigrp** *as-number*
2. **network** *ip-address*
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	**routereigrp** *as-number* 例： 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。自律システム（AS）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：
	
	例：
	`Router(config)# network 192.145.1.0`
	
	例：
	`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： 例： `Router(config-router)# end`	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。

	コマンドまたはアクション	目的
	例： `Router#`	

次の作業

EIGRP の概念に関する一般的な情報については、B-3 ページの「拡張 IGRP」を参照してください。

設定例：EIGRP

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

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

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

EIGRP 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
```

第 3 章

レイヤ 3 インターフェイスでのイーサネット CFM と Y.1731 パフォーマンス モニタリングの設定

この章では、ネットワーク インターフェイス デバイスの機能、イーサネット データ プレーン ループバック、IEEE 接続障害管理、および Y.1731 パフォーマンス モニタリングを設定する手順について説明します。

EVC ブリッジ ドメイン（BD）およびこれがサポートする機能の設定については、「イーサネット仮想コネクション ブリッジ ドメインの設定」を参照してください。

この章の内容は、次のとおりです。

L3インターフェイスでのネットワークインターフェイスデバイスの設定

ネットワーク インターフェイス デバイス（NID）を設定すると、ネットワークに NID ハードウェアが含まれていなくても、ルータで NID 機能をサポートできるようになります。この機能は、顧客構内設備（CPE）と NID 機能を 1 つの物理的なデバイスに結合します。NID 機能を設定する利点は次のとおりです。

- 物理的なデバイスを使わなくて済む。
- 管理型 CPE 機能セットと NID 要件の両方をサポートする。

（注） この機能は、*advipservices* ライセンス モジュールを購入している場合にのみサポートされます。Cisco ISR および Cisco ISR G2 プラットフォームでのソフトウェア アクティベーション ライセンスの管理については、http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html を参照してください。

NID の設定

次の手順では、NID を設定する方法について説明します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacegigabitethernet** *slot/port*
4. **port-tagging**
5. **encapsulationdot1q** *vlan-id*
6. **setcos** *cos-value*
7. **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	**enable** 例： `Router>enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet** *slot/port* 例： `Router(config)#interface gigabitethernet 0/2`	インターフェイスを指定し、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 4	**port-tagging** 例： `Router(config-if)#port-tagging`	パケットが属する仮想ローカル エリア ネットワーク（VLAN）を特定するために、パケットヘッダーに VLAN ID を挿入します。

	コマンドまたはアクション	目的
ステップ 5	**encapsulationdot1q** *vlan-id* 例： `Router(config-if-port-tagging)#encapsulation dot1q 10`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 6	**setcos** *cos-value* 例： `Router(config-if-port-tagging)#set cos 6`	レイヤ 2 サービス クラス（CoS）値を発信パケットの最後に設定します。
ステップ 7	**end** 例： `Router(config-if-port-tagging)#end`	インターフェイス コンフィギュレーション モードを終了します。

設定例

この設定は、NID を設定する方法を示しています。

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitethernet 0/2
Router(config-if)#port-tagging
Router(config-if-port-tagging)#encapsulation dot1q 10
Router(config-if-port-tagging)#set cos 6
Router(config-if-port-tagging)#end
```

NID の設定の確認

次のコマンドを使用して、ポート タギング セッションを確認できます。

- **showrunint**
- **ping**

ポート タグング セッションを表示するには、**showrunint** コマンドを使用します。

```
Router#show run int gi0/2
Building configuration...
Current configuration : 10585 bytes
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 port-tagging
  encapsulation dot1q 10
  set cos 6
```

```
  exit
end
!
interface GigabitEthernet0/2.1101
encapsulation dot1Q 100
ip address 132.1.101.4 255.255.255.0
!
interface GigabitEthernet0/2.1102
encapsulation dot1Q 100
ip address 132.1.102.4 255.255.255.0
!
```

設定されているポート タギングとの接続を確認するには、**ping** コマンドを使用します。

```
Router#ping
 132.1.101.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 132.1.101.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
router#
```

NID 設定のトラブルシューティング

表 20：NID の設定の debug コマンド, （92 ページ） に、NID 機能に関連する問題のトラブルシューティングを行う debug コマンドの一覧を示します。

Cisco IOS マスター コマンド一覧は以下にあります。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

注意 CPU プロセスでは、デバッグ出力に高いプライオリティが割り当てられるため、デバッグ出力によってルータのパフォーマンスが低下したり、ルータが使用できなくなったりすることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。

（注） 次の表に記載されている debug コマンドのいずれかを実行する前に、必ず **loggingbuffereddebugging** コマンドを実行し、**nologgingconsole** コマンドを使用してコンソールのデバッグ ロギングをオフにしてください。

表 *20*：*NID* の設定の *debug* コマンド

debug コマンド	目的
debugethernetnidconfiguration	設定関連の問題のデバッグを有効にする。
debugethernetnidpacketegress	出力側でパケット処理（VLAN タグの付加）のデバッグを有効にする。

debug コマンド	目的
debugethernetnidpacketingress	入力側でパケット処理（VLAN タグの除去）のデバッグを有効にする。

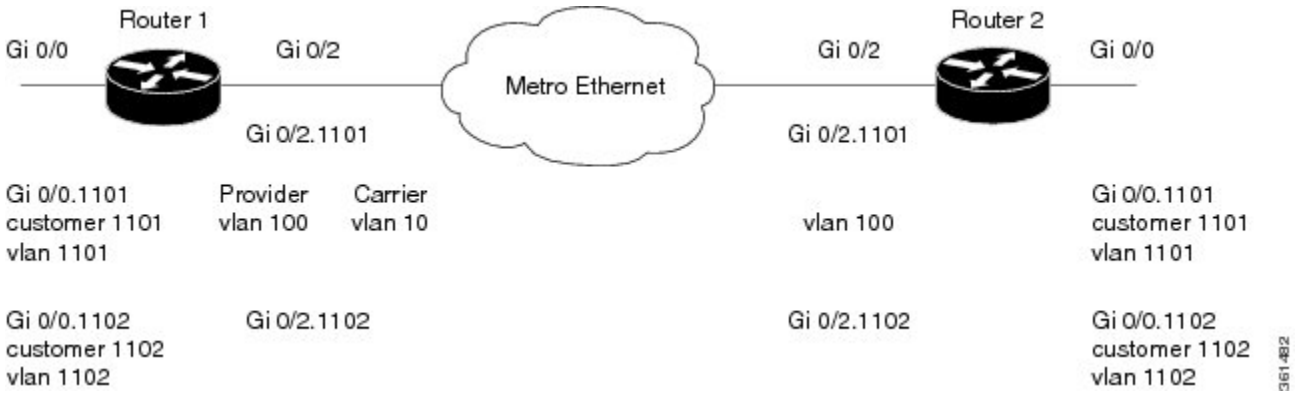
イーサネット データ プレーン ループバック

イーサネット データ プレーン ループバック機能は、イーサネット ポートのスループットをリモートでテストするための手段を提供します。フレーム損失なしでフレーム転送の最大速度を確認できます。

（注） この機能は、*advipservices* ライセンス モジュールを購入している場合にのみサポートされます。Cisco ISR および Cisco ISR G2 プラットフォームでのソフトウェア アクティベーション ライセンスの管理については、http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html を参照してください。

（注） 内部イーサネット データ プレーン ループバックはサポートされていません。

図 4-1 は、イーサネット データ プレーン ループバックを設定するサンプル トポロジを示します。



イーサネット データ プレーン ループバックの設定に関する制約事項

レイヤ 3 インターフェイスにイーサネット データ プレーン ループバックを設定する際は、ここに一覧されているガイドラインに従い、制約事項に注意してください。

- L3 dot1q サブインターフェイスおよび（タグなし）メイン インターフェイスでの外部ループバック（ケーブル側から受け取るパケット）のみがサポートされています。

- MAC スワップを実行するには、ループ バックされるパケットで宛先アドレスと発信元アドレスを入れ替える必要があります。発信先アドレスがブロードキャストまたはマルチキャストの場合、MAC アドレスはループ バックされるパケットの発信元アドレスとして使用されます。
- ループバックは、ライン レートでの動作がサポートされています。
- サブインターフェイスでは、タグなしフレームはサポートされません。ただし、*dot1q* および *qinq* のフレームは、サブインターフェイスでサポートされます。
- メイン インターフェイスでは、*dot1ad* はサポートされません。ただし、タグなしフレームは、メイン インターフェイスでサポートされます。
- 単一の VLAN はサブインターフェイスのフィルタリング オプションとしてサポートされていますが、VLAN リストと VLAN 範囲はサポートされません。
- メイン インターフェイスでは、MAC アドレスのみがフィルタリング オプションとしてサポートされています。
- フィルタリング オプションで、宛先 MAC を inner VLAN や outer VLAN と組み合わせることはできません。
- L3 と L4 のループバックはサポートされていません。送信元と宛先の IP アドレスまたは送信元と宛先のポートはスワップされません。
- 接続障害管理（CFM）パケットは、データ プレーン ループバック設定に対して透過的であり、ループ バックすることはできません。
- ループバックが設定されているケーブルの反対側から到着するパケットおよび同じ宛先MACアドレスを持つパケットは破棄されます。
- 受信するブロードキャストおよびマルチキャストIPフレームのブロードキャストおよびマルチキャスト IP アドレスは、イニシエータに送り返すときにフレームの送信元 IP アドレスとして使用できません。このような場合、イニシエータに送り返すときのフレームには、サブインタ フェースの IP アドレスが送信元 IP アドレスとして使用されます。

外部イーサネット データ プレーン ループバックの設定

レイヤ 3 のメイン インターフェイスおよびサブインターフェイスでは、外部イーサネット データ プレーン ループバックを設定できます。

次に、シングルおよびダブル タギングを使用してサブインターフェイス上に外部イーサネット データ プレーン ループバックを設定する方法を示します。（メイン インターフェイス上に外部イーサネット データ プレーン ループバックを設定する手順も、この手順と同様です。）

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacegigabitethernet** *slot/port.sub-port*
4. 次のいずれかを実行します。
   - **encapsulationdot1q** *vlan-id*
   - **encapsulationdot1q** *vlan-id***second-dot1q** *inner vlan-id*
5. **ethernetloopbackpermitexternal**
6. **end**
7. **ethernetloopbackstartlocalinterfacegigabitethernet** *slot/port.sub-port***externaltimeout** *none*
8. **ethernetloopbackstoplocalinterfacegigabitethernet** *slot/port.sub-port***id** *session-id*
9. **showethernetloopbackactive**

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。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**interfacegigabitethernet** *slot/port.sub-port* 例： `Router(config)#interface gigabitethernet 0/2.1101`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかを実行します。 • **encapsulationdot1q** *vlan-id* • **encapsulationdot1q** *vlan-id***second-dot1q** *inner vlan-id* 例： `Router(config-subif)#encapsulation dot1q 100` または	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。 ダブル タギングの場合は、**second-dot1q** キーワードおよび *inner vlan-id* 引数を使用して VLAN タグを指定します。

	コマンドまたはアクション	目的
	例： `Router(config-subif)#encapsulation dot1q 100 second-dot1q 1101`	
ステップ 5	**ethernetloopbackpermitexternal** 例： `Router(config-subif)#ethernet loopback permit external`	サブインターフェイス上にイーサネット外部ループバックを設定します。
ステップ 6	**end** 例： `Router(config-subif)#end`	サブインターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**ethernetloopbackstartlocalinterfacegigabitethernet** *slot/port.sub-port***externaltimeout** *none* 例： `Router#ethernet loopback start local interface gigabitethernet 0/2.1101 external timeout none`	サブインターフェイス上でイーサネット外部ループバックを開始します。 タイムアウトに *none* を入力し、ループバックのタイムアウト期間をなしにします。
ステップ 8	**ethernetloopbackstoplocalinterfacegigabitethernet** *slot/port.sub-port***id** *session-id* 例： `Router#ethernet loopback stop local interface gigabitethernet 0/2.1101 id 1`	サブインターフェイス上でイーサネット外部ループバックを停止します。 停止するループバック セッションを指定するために、ループバック セッションIDの値を入力します。
ステップ 9	**showethernetloopbackactive** 例： `Router#show ethernet loopback active`	情報を表示し、ループバック セッションが終了したかどうかを確認します。

イーサネット データ プレーン ループバックの設定例

次の例は、シングル タギングを使用してイーサネット データ プレーン ループバックを設定する方法を示しています。

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100
```

```
Router(config-subif)#ethernet loopback permit external
Router(config-subif)#end
```

次の例は、ダブル タギングを使用してイーサネット データ プレーン ループバックを設定する方法を示しています。

```
Router>enable
Router#configure terminal
Router(config)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100 second-dot1q 1101
Router(config-subif)#ethernet loopback permit external
Router(config-subif)#end
```

次の例は、イーサネット データ プレーン ループバックを開始する方法を示しています。

```
Router#ethernet loopback start local interface gigabitethernet 0/2.1101 external timeout
none
This is an intrusive loopback and the packets matched with the service will not be able to
 pass through. Continue? (yes/[no]):
Enter yes to continue.
```

次の例は、イーサネット データ プレーン ループバックを停止する方法を示しています。

```
Router#ethernet loopback stop local interface gigabitethernet 0/2.1101 id 1
Router#*Oct 21 10:16:17.887: %E_DLB-6-DATAPLANE_LOOPBACK_STOP: Ethernet Dataplane Loopback
 Stop on interface GigabitEthernet0/2 with session id 1
Router#show ethernet loopback active
Total Active Session(s): 0
Total Internal Session(s): 0
Total External Session(s): 0
```

イーサネット データ プレーン ループバックの設定の確認

イーサネットデータプレーンループバックの設定を確認するには、次のコマンドを使用します。

- **showethernetloopbackpermitted**
- **showethernetloopbackactive**

インターフェイスごとのループバック機能を表示するには、**show ethernet loopback permitted** コマンドを使用します。

```
Router#show ethernet loopback permitted
------------------------------------------------------------------------------
Interface                               SrvcInst Direction
Dot1q/Dot1ad(s)                         Second-Dot1q(s)
------------------------------------------------------------------------------
Gi0/2.1101                              N/A      External
100                                     1101
```

サブインターフェイス上のアクティブなループバック セッションの概要を表示するには、**showethernetloopbackactive** コマンドを使用します。

```
Router#show ethernet loopback active
Loopback Session ID     : 1
Interface               : GigabitEthernet0/2.1101
Service Instance        : N/A
Direction               : External
Time out(sec)           : none
Status                  : on
Start time              : *10:17:46.930 UTC Mon Oct 21 2013
Time left               : N/A
```

```
Dot1q/Dot1ad(s)          : 100
Second-dot1q(s)          : 1101
Source Mac Address       : Any
Destination Mac Address  : Any
Ether Type               : Any
Class of service         : Any
Llc-oui                  : Any
Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1
```

メイン インターフェイス上のアクティブなループバック セッションの概要を表示するには、**showethernetloopbackactive** コマンドを使用します。

```
Router#show ethernet loopback permitted
Loopback Session ID      : 1
Interface                : GigabitEthernet0/2
Service Instance         : N/A
Direction                : External
Time out(sec)            : none
Status                   : on
Start time               : *10:14:23.507 UTC Mon Oct 21 2013
Time left                : N/A
Dot1q/Dot1ad(s)          : 1-100
Second-dot1q(s)          : 1-1101
Source Mac Address       : Any
Destination Mac Address  : Any
Ether Type               : Any
Class of service         : Any
Llc-oui                  : Any
Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1
```

イーサネット データ プレーン ループバックの設定のトラブルシューティング

表 21：イーサネット データ プレーン ループバックの設定の debug コマンド, （99 ページ） に、イーサネット データ プレーン ループバック機能に関連する問題のトラブルシューティングを行う debug コマンドの一覧を示します。Cisco IOS マスター コマンド一覧は以下にあります。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

注意 CPUプロセスでは、デバッグ出力に高いプライオリティが割り当てられるため、デバッグ出力によってルータのパフォーマンスが低下したり、ルータが使用できなくなったりすることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。

（注） 次の表に記載されている debug コマンドのいずれかを実行する前に、必ず **loggingbuffereddebugging** コマンドを実行し、**nologgingconsole** コマンドを使用してコンソールのデバッグ ロギングをオフにしてください。

表 *21*：イーサネット データ プレーン ループバックの設定の *debug* コマンド

debug コマンド	目的
debugelb-pal-pdall	イーサネット データ プレーン ループバックの設定に関するすべてのデバッグ情報を表示する。
debugelb-pal-pderror	イーサネット データ プレーン ループバックの設定エラーに関するデバッグ情報を表示する。
debugelb-pal-pdevent	イーサネット データ プレーン ループバックの設定の変更に関するデバッグ情報を表示する。

ルーテッド ポートとポート MEP での CFM のサポート

IEEE 接続障害管理（CFM）は、サービスごとのエンドツーエンド イーサネット レイヤの運用、管理およびメンテナンス（OAM）のプロトコルです。CFM には、大規模イーサネット メトロポリタンエリア ネットワーク（MAN）および WAN の予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。

（注） この機能は、*advipservices* ライセンス モジュールを購入している場合にのみサポートされます。Cisco ISR および Cisco ISR G2 プラットフォームでのソフトウェア アクティベーション ライセンスの管理については、http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html を参照してください。

イーサネット CFM の設定に関する制約事項

- 特定のドメインを設定する必要があります。設定しない場合、エラー メッセージが表示されます。
- 同じメンテナンス レベルの複数のドメイン（異なるドメイン名）を設定できます。ただし、1 つのドメイン名に複数のメンテナンス レベルを関連付けることはできません。

イーサネット CFM（ポート MEP）の設定

ポート メンテナンス エンド ポイント（MEP）でイーサネット CFM を設定して有効化するには、以下の手順を完了します。

手順の概要

1. **enable**
2. **configureterminal**
3. **ethernetcfmieee**
4. **ethernetcfmglobal**
5. **ethernetcfmdomain** *domain-name***level** *value*
6. **service** *service-name***port**
7. **continuity-checkinterval** *value*
8. **end**
9. **configureterminal**
10. **interfacegigabitethernet** *slot/port*
11. **ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name*
12. **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	**enable** 例： `Router>enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**ethernetcfmieee** 例： `Router(config)#ethernet cfm ieee`	CFM の IEEE バージョンをイネーブルにします。
ステップ 4	**ethernetcfmglobal** 例： `Router(config)#ethernet cfm global`	ルータの CFM 処理をグローバルにイネーブルにします。
ステップ 5	**ethernetcfmdomain** *domain-name***level** *value* 例： `Router(config-ecfm)#ethernet cfm domain carrier level 2`	指定されたレベルで CFM メンテナンス ドメインを定義し、イーサネット CFM コンフィギュレーション モードにします。 **level** には、0 ～ 7 の任意の値を指定できます。

	コマンドまたはアクション	目的
ステップ 6	**service** *service-name***port** 例： `Router(config-ecfm)#service carrier port`	インターフェイス上でサービスを作成し、*config-ecfm-srv* サブモードを設定します。
ステップ 7	**continuity-checkinterval** *value* 例： `Router(config-ecfm-srv)#continuity-check interval 100m`	設定した間隔での Continuity Check メッセージの送信を有効にします。
ステップ 8	**end** 例： `Router(config-ecfm-srv)#end`	ルータを特権 EXEC モードに戻します。
ステップ 9	**configureterminal** 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 10	**interfacegigabitethernet** *slot/port* 例： `Router(config)#interface gigabitethernet 0/2`	インターフェイスを指定し、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 11	**ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name* 例： `Router(config-if)#ethernet cfm mep domain carrier mpid 44 service carrier`	ポートをメンテナンス ドメインに設定し、MEP として定義します。 （注） **domain** および **service** の値は、CFM に設定されている値と同じにする必要があります。
ステップ 12	**end** 例： `Router(config-if-ecfm-mep)#end`	ルータを特権 EXEC モードに戻します。

イーサネット CFM（ポート MEP）の設定例

次の例は、ポート MEP にイーサネット CFM を設定する方法を示しています。

```
Router>enable
Router#configure terminal
```

```
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config-ecfm)#ethernet cfm domain carrier level 2
Router(config-ecfm)#service carrier port
Router(config-ecfm-srv)#continuity-check interval 100m
Router(config-ecfm-srv)#end
Router#configure terminal
Router(config)#interface gigabitethernet
 0/2
Router(config-if)#ethernet cfm mep domain
carrier
 mpid 44 service
carrier
Router(config-if-ecfm-mep)#end
```

ポート MEP のイーサネット CFM の設定の確認

ポート MEP に設定されているイーサネット CFM を確認するには、次のコマンドを使用します。

- **showethernetcfmdomain**
- **showethernetcfmmaintenance-pointslocal**
- **showethernetcfmmaintenance-pointsremote**
- **pingethernetmpid** *mpid-value* **domain** *domain-name* **service** *service-name* cos *value*
- **traceroutеethernetmpid** *mpid-value* **domain** *domain-name* **service** *service-name*
- **showethernetcfmerrorconfiguration**

CFM メンテナンス ドメインの詳細を表示するには、**show ethernet cfm domain** コマンドを使用します。

```
Router#show ethernet cfm domain carrier
Domain Name: carrier
Level: 2
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Port none Dwn Y  100ms  Disabled    Disabled   100    Static  carrier
Router#
```

ルータにローカルに設定されている MEP を表示するには、**showethernetcfmmaintenance-pointslocal** コマンドを使用します。次に、**showethernetcfmmaintenance-pointslocal** コマンドの出力例を示します。

```
Router#show ethernet cfm maintenance-points local

Local MEPs:
--------------------------------------------------------------------------------
MPID Domain Name                                Lvl   MacAddress     Type  CC
Ofld Domain Id                                  Dir   Port           Id
     MA Name                                          SrvcInst       Source
     EVC name
--------------------------------------------------------------------------------
44   carrier                                    2     5657.a844.04fa Port  Y
No   carrier                                    Down  Gi0/2          none
     carrier                                          N/A            Static
     N/A
Total Local MEPs: 1
Local MIPs: None
```

リモート メンテナンス ポイント ドメイン、またはレベルに関する情報を表示するには、**showethernetcfmmaintenance-pointsremote** コマンドを使用します。次の例では、通信事業者、プロバイダー、顧客のメンテナンス ポイント ドメインが設定されています。

```
On router 1:
Router1#show ethernet cfm maintenance-points remote

-------------------------------------------------------------------------------
MPID  Domain Name                                MacAddress          IfSt  PtSt
 Lvl  Domain ID                                  Ingress
 RDI  MA Name                                    Type Id             SrvcInst
      EVC Name                                                       Age
      Local MEP Info
-------------------------------------------------------------------------------
43    carrier                                    5657.a86c.fa92      Up    N/A
 2    carrier                                    Gi0/2
 -    carrier                                    Port none           N/A
      N/A                                                            0s
      MPID: 44 Domain: carrier MA: carrier
33    Provider                                   5657.a86c.fa92      Up    Up
 5    Provider                                   Gi0/2.100
 -    Provider                                   Vlan 100            N/A
      N/A                                                            0s
      MPID: 34 Domain: Provider MA: Provider
3101  customer                                   5657.a86c.fa92      Up    Up
 7    customer                                   Gi0/2.1101
 -    customer1101                               S,C  100,1101       N/A
      N/A                                                            0s
      MPID: 4101 Domain: customer MA: customer1101
3102  customer                                   5657.a86c.fa92      Up    Up
 7    customer                                   Gi0/2.1102
 -    customer1102                               S,C  100,1102       N/A
      N/A                                                            0s
      MPID: 4102 Domain: customer MA: customer1102
Total Remote MEPs: 4
```

リモート メンテナンス ポイント ドメインを表示するには、**showethernetcfmmaintenance-pointsremote** コマンドを使用します。

```
On router 1:
Router1#show ethernet cfm maintenance-points remote domain carrier service carrier
-------------------------------------------------------------------------------
MPID  Domain Name                                MacAddress          IfSt  PtSt
 Lvl  Domain ID                                  Ingress
 RDI  MA Name                                    Type Id             SrvcInst
      EVC Name                                                       Age
      Local MEP Info
-------------------------------------------------------------------------------
43    carrier                                    5657.a86c.fa92      Up    Up
 2    carrier                                    Gi0/2
 -    carrier                                    S,C  100,1101       N/A
      N/A                                                            0s
      MPID: 44 Domain: carrier MA: carrier
Total Remote MEPs: 1
```

On router 2:

```
Router2#show ethernet cfm maintenance-points remote domain carrier service carrier
-------------------------------------------------------------------------------
MPID  Domain Name                                MacAddress          IfSt  PtSt
 Lvl  Domain ID                                  Ingress
 RDI  MA Name                                    Type Id             SrvcInst
      EVC Name                                                       Age
      Local MEP Info
-------------------------------------------------------------------------------
44    carrier                                    5657.g945.04fa      Up    Up
 2    carrier                                    Gi0/2
 -    carrier                                    S,C  100,1101       N/A
```

```
      N/A                                                                 0s
      MPID: 43 Domain: carrier MA: carrier
```

ループバック メッセージ（LBM）およびループバック リプライ（□□□）がルータ間で正しく送受信されているかどうかを確認するには、**ping** コマンドを使用します。

```
Router1#ping ethernet mpid 44 domain carrier service carrier cos 5

Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 5657.a86c.fa92, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router1#
```

イーサネット CFM トレースルート メッセージを送信するには、**traceroute** コマンドを使用します。

```
Router#traceroute ethernet mpid 44 domain carrier service carrier
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to 5657.a86c.fa92 on Domain carrier, Level 2, service carrier
Traceroute sent via Gi0/2
B = Intermediary Bridge
! = Target Destination
* = Per hop Timeout
-------------------------------------------------------------------------------
                              MAC      Ingress        Ingr Action  Relay Action
  Hops   Host              Forwarded   Egress         Egr Action   Previous Hop
-------------------------------------------------------------------------------
! 1                   5657.a86c.fa92 Gi0/2          IngOk        RlyHit:MEP
                     Not Forwarded                               5657.g945.04fa
Router#
```

イーサネット CFM の設定（シングルタグ付きパケット）

以下の手順を実行し、シングルタグ付きパケットにイーサネット CFM を設定して有効にします。

手順の概要

1. **enable**
2. **configureterminal**
3. **ethernetcfmieee**
4. **ethernetcfmglobal**
5. **ethernetcfmdomain** *domain-name***level** *value*
6. **service** *service-name***vlan** *vlan-id***directiondown**
7. **continuity-check**
8. **interfacegigabitethernet** *slot/port*
9. **ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name*
10. **interfacegigabitethernet** *slot/port.subinterface*
11. **encapsulationdot1q** *vlan-id*
12. **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	**enable** 例： `Router>enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**ethernetcfmieee** 例： `Router(config)#ethernet cfm ieee`	CFM の IEEE バージョンをイネーブルにします。
ステップ 4	**ethernetcfmglobal** 例： `Router(config)#ethernet cfm global`	ルータの CFM 処理をグローバルにイネーブルにします。
ステップ 5	**ethernetcfmdomain** *domain-name***level** *value* 例： `Router(config)#ethernet cfm domain customer level 7`	指定されたレベルで CFM メンテナンス ドメインを定義し、イーサネット CFM コンフィギュレーション モードにします。 **level** には、0 ～ 7 の任意の値を指定できます。
ステップ 6	**service** *service-name***vlan** *vlan-id***directiondown** 例： `Router(config-ecfm)#service customer1101 vlan 100 direction down`	CFM サービス コンフィギュレーション モードを開始します。 **vlan**：VLAN を指定します。
ステップ 7	**continuity-check** 例： `Router(config-ecfm-srv)#continuity-check`	Continuity Check メッセージの送信を有効にします。
ステップ 8	**interfacegigabitethernet** *slot/port* 例： `Router(config-ecfm-srv)#interface gigabitethernet 0/2`	インターフェイスを指定し、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。

	コマンドまたはアクション	目的
ステップ 9	**ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name* 例： `Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101`	ポートをメンテナンス ドメインに設定し、MEP として定義します。 （注） **domain** および **service** の値は、CFM に設定されている値を同じにする必要があります。
ステップ 10	**interfacegigabitethernet** *slot/port.subinterface* 例： `Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**encapsulationdot1q** *vlan-id* 例： `Router(config-subif)#encapsulation dot1q 100`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。
ステップ 12	**end** 例： `Router(config-subif)#end`	ルータを特権 EXEC モードに戻します。

イーサネット CFM の設定例（シングルタグ付きパケット）

次の例は、シングルタグ付きパケットにイーサネット CFM を設定する方法を示しています。

```
Router>enable
Router#configure terminal
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config)#ethernet cfm domain customer level 7
Router(config-ecfm)#service customer1101 vlan 100 direction down
Router(config-ecfm-srv)#continuity-check
Router(config)#interface gigabitethernet
 0/2
Router(config-if)#ethernet cfm mep domain customer mpid 100 service
customer1101
Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1
Router(config-subif)#encapsulation dot1q 100
Router(config-subif)#end
```

シングルタグ付きパケットのイーサネット CFM の設定の確認

シングルタグ付きパケットに設定されているイーサネット CFM を確認するには、次のコマンドを使用します。

- **showethernetcfmdomain**
- **showethernetcfmmaintenance-pointslocal**
- **showethernetcfmmaintenance-pointsremote**
- **showethernetcfmerrorconfiguration**

ネットワークに設定されているメンテナンス ポイント ドメインを表示するには、**showethernetcfmdomain** コマンドを使用します。次の例では、顧客、企業、通信事業者のメンテナンス ポイント ドメインが設定されています。

```
Router#show ethernet cfm domain
Domain Name: customer
Level: 7
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 100  Dwn Y  10s    Disabled    Disabled   100    Static  customer1101
Domain Name: enterprise
Level: 6
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 110  Dwn Y  10s    Disabled    Disabled   100    Static  custservice
Domain Name: carrier
Level: 2
Total Services: 1
  Services:
  Type Id   Dir CC CC-int Static-rmep Crosscheck MaxMEP Source  MA-Name
  Vlan 200  Dwn Y  10s    Disabled    Disabled   100    Static  carrier
Router#
```

ローカルMEPを表示するには、**showethernetcfmmaintenance-pointslocal** コマンドを使用します。次に、**showethernetcfmmaintenance-pointslocal** コマンドの出力例を示します。

```
Router#show ethernet cfm maintenance-points local
-------------------------------------------------------------------------------
MPID Domain Name                                Lvl   MacAddress     Type  CC
Ofld Domain Id                                  Dir   Port           Id
     MA Name                                          SrvcInst       Source
     EVC name
-------------------------------------------------------------------------------
100  customer                                   7     70ca.9b4d.a400 Vlan  Y
No   customer                                   Down  Gi0/2          100
     customer1101                                     N/A            Static
     N/A
400  enterprise                                 6     70ca.9b4d.a400 Vlan  I
No   enterprise                                 Down  Gi0/1          110
     custservice                                      N/A            Static
     N/A
44   carrier                                    2     70ca.9b4d.a400 Vlan  N
No   carrier                                    Down  Gi0/2          200
     carrier                                          N/A            Static
     N/A
Total Local MEPs: 3
Local MIPs: None
Router#
```

リモート メンテナンス ポイント ドメイン、またはレベルに関する情報を表示するには、**showethernetcfmmaintenance-pointsremote** コマンドを使用します。

```
The following example displays the continuity check messages exchanged between remote MEPs:
On router 1:
Router1#show ethernet cfm maintenance-points remote
-------------------------------------------------------------------------------------------
MPID Domain Name             MacAddress           IfSt               PtSt
```

```
 Lvl Domain                  Ingress
 RDI MA                      Type Id             SrvcInst
     EVC Name                                    Age
     Local MEP Info
------------------------------------------------------------------------------------------
110  customer               70ca.9b4d.a400      Up                  Up
 7   customer               Gi0/2
 -   customer1101           Vlan 100            N/A
     N/A                                        12s
     MPID: 100 Domain: customer MA: customer1101
410  enterprise             70ca.9b4d.a400      Up                  Up
 6   enterprise             Gi0/1
 -   custservice            Vlan 110            N/A
     N/A                                        12s
     MPID: 400 Domain: enterprise MA: custservice
43   carrier                70ca.9b4d.a400      Up                  Up
 2   carrier                Gi0/2
 -   carrier                Vlan 200            N/A
     N/A                                        12s
     MPID: 44  Domain: carrier MA: carrier
Total Remote MEPs: 3
Router1#
```

ルータ 2:

```
Router2#show ethernet cfm maintenance-points remote
------------------------------------------------------------------------------------------
MPID Domain Name            MacAddress          IfSt              PtSt
 Lvl Domain                 Ingress
 RDI MA                     Type Id             SrvcInst
     EVC Name                                   Age
     Local MEP Info
------------------------------------------------------------------------------------------
100  customer               0026.99f7.0b41      Up                  Up
 7   customer               Gi0/2
 -   customer1101           Vlan 100            N/A
     N/A                                        2s
     MPID: 110 Domain: customer MA: customer1101
400  enterprise             0026.99f7.0b41      Up                  Up
 6   enterprise             Gi0/1
 -   custservice            Vlan 110            N/A
     N/A                                        2s
     MPID: 410 Domain: enterprise MA: custservice
44   carrier                0026.99f7.0b41      Up                  Up
 2   carrier                Gi0/2
 -   carrier                Vlan 200            N/A
     N/A                                        2s
     MPID: 43  Domain: carrier MA: carrier
Total Remote MEPs: 3
Router2#
```

イーサネット CFM 設定エラー（ある場合）を表示するには、**showethernetcfmerrorconfiguration** コマンドを使用します。次に、**showethernetcfmerrorconfiguration** コマンドの出力例を示します。

```
Router#show ethernet cfm error configuration
------------------------------------------------------------------------------
CFM Interface      Type  Id       Level    Error type
------------------------------------------------------------------------------
Gi0/2              S,C   100      5        CFMLeak
```

イーサネット CFM の設定（ダブルタグ付きパケット）

以下の手順を実行し、ダブルタグ付きパケットにイーサネット CFM を設定して有効にします。

手順の概要

1. **enable**
2. **configureterminal**
3. **ethernetcfmieee**
4. **ethernetcfmglobal**
5. **ethernetcfmdomain** *domain-name***level** *0 to 7*
6. **service** *service-name***vlan** *vlan-id***inner-vlan** *inner vlan-id***directiondown**
7. **continuity-check**
8. **interfacegigabitethernet** *slot/port*
9. **ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name*
10. **interfacegigabitethernet** *slot/port.subinterface*
11. **encapsulationdot1q** *vlan-id***second-dot1q** *inner vlan-id*
12. **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	**enable** 例： `Router>enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**ethernetcfmieee** 例： `Router(config)#ethernet cfm ieee`	CFM の IEEE バージョンをイネーブルにします。
ステップ 4	**ethernetcfmglobal** 例： `Router(config)#ethernet cfm global`	ルータの CFM 処理をグローバルにイネーブルにします。
ステップ 5	**ethernetcfmdomain** *domain-name***level** *0 to 7* 例： `Router(config-ecfm)#ethernet cfm domain customer level 7`	指定されたレベルで CFM メンテナンス ドメインを定義し、イーサネット CFM コンフィギュレーション モードにします。 **level** には、0 ～ 7 の任意の値を指定できます。

	コマンドまたはアクション	目的
ステップ 6	**service** *service-name***vlan** *vlan-id***inner-vlan** *inner vlan-id***directiondown** 例： `Router(config-ecfm)#service customer1101 vlan 100 inner-vlan 30 direction down`	CFM サービス コンフィギュレーション モードを開始します。 パラメータは次のとおりです。 • **vlan**：VLAN を指定します。 • **inner-vlan**：**inner-vlan** キーワードおよび *inner vlan-id* 引数で、ダブルタグ付きパケットに VLAN タグを指定します。
ステップ 7	**continuity-check** 例： `Router(config-ecfm-srv)#continuity-check`	Continuity Check メッセージの送信を有効にします。
ステップ 8	**interfacegigabitethernet** *slot/port* 例： `Router(config-ecfm-srv)#interface gigabitethernet 0/2`	インターフェイスを指定し、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 9	**ethernetcfmmepdomain** *domain-name***mpid** *mpid-value***service** *service-name* 例： `Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101`	ポートをメンテナンス ドメインに設定し、MEP として定義します。 （注） **domain** および **service** の値は、CFM に設定されている値と同じにする必要があります。 **MPID**：メンテナンス エンドポイント識別子を指定します。
ステップ 10	**interfacegigabitethernet** *slot/port.subinterface* 例： `Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1101`	サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**encapsulationdot1q** *vlan-id***second-dot1q** *inner vlan-id* 例： `Router(config-subif)#encapsulation dot1q 100 second-dot1q 30`	カプセル化形式を IEEE 802.1Q（dot1q）と定義し、VLAN 識別子を指定します。 **second-dot1q** キーワードおよび *inner vlan-id* 引数を使用して、VLAN タグを指定します。
ステップ 12	**end** 例： `Router(config-subif)#end`	ルータを特権 EXEC モードに戻します。

イーサネット CFM の設定例（ダブルタグ付きパケット）

次の例は、ダブルタグ付きパケットにイーサネット CFM を設定する方法を示しています。

```
Router>enable
Router#configure terminal
Router(config)#ethernet cfm ieee
Router(config)#ethernet cfm global
Router(config-ecfm)#ethernet cfm domain customer level 7
Router(config-ecfm)#service customer1101 vlan 100 inner-vlan 30 direction down
Router(config-ecfm-srv)#continuity-check
Router(config-ecfm-srv)#interface gigabitethernet
 0/2
Router(config-if)#ethernet cfm mep domain customer mpid 100 service customer1101
Router(config-if-ecfm-mep)#interface gigabitethernet 0/2.1101
Router(config-subif)#encapsulation dot1q 100 second-dot1q 30
Router(config-subif)#end
```

ダブルタグ付きパケットのイーサネット CFM の設定の確認

ダブルタグ付きパケットに設定されているイーサネットCFMを確認するには、次のコマンドを使用します。

- **showethernetcfmmaintenance-pointslocal**
- **showethernetcfmmaintenance-pointsremote**
- **pingethernetmpid** *mpid-value***domain** *domain-name***service** *service-name***cos** *value*
- **tracerouteethernetmpid** *mpid-value***domain** *domain-name***service** *service-name*
- **showethernetcfmerrorconfiguration**

ローカルMEPを表示するには、**showethernetcfmmaintenance-pointslocal** コマンドを使用します。次に、**showethernetcfmmaintenance-pointslocal** コマンドの出力例を示します。

```
Router#show ethernet cfm maintenance-points local
-------------------------------------------------------------------------------
MPID Domain Name          MacAddress                IfSt                    PtSt
 Lvl Domain ID           Ingress
 RDI MA Name              Type Id                   SrvcInst
     EVC Name                              Age
     Local MEP Info
-------------------------------------------------------------------------------
100  customer             8843.e154.6f01            Up                      Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30              N/A
     N/A                                   58s
     MPID: 100 Domain: customer MA: customer1101
Router#
```

リモート メンテナンス ポイント ドメインを表示するには、**showethernetcfmmaintenance-pointsremote** コマンドを使用します。次の例では、顧客、通信事業者、企業のメンテナンス ポイント ドメインが設定されています。

On router 1:

```
Router1#show ethernet cfm maintenance-points remote
-------------------------------------------------------------------------------
MPID Domain Name          MacAddress                IfSt                    PtSt
 Lvl Domain ID           Ingress
 RDI MA Name              Type Id                   SrvcInst
     EVC Name                                      Age
     Local MEP Info
-------------------------------------------------------------------------------
110  customer             8843.e154.6f01            Up                      Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30              N/A
     N/A                                           58s
     MPID: 100 Domain: customer MA: customer1101
43   carrier              8843.e154.6f01            Up                      Up
 2   carrier              Gi0/2.2
 -   carrier              S, C 50, 20               N/A
     N/A                                           58s
     MPID: 44 Domain: carrier MA: carrier
410  enterprise           8843.e154.6f01            Up                      Up
 6   enterprise           Gi0/1.1
 -   custservice          S, C 200, 70              N/A
     N/A                                           58s
     MPID: 400 Domain: enterprise MA: custservice
Router1#
```

On router 2:

```
Router2#show ethernet cfm maintenance-points remote
-------------------------------------------------------------------------------
MPID Domain Name          MacAddress                IfSt                    PtSt
 Lvl Domain ID           Ingress
 RDI MA Name              Type Id                   SrvcInst
     EVC Name                                      Age
     Local MEP Info
-------------------------------------------------------------------------------
100  customer             0026.99f7.0b41            Up                      Up
 7   customer             Gi0/2.1101
 -   customer1101         S, C 100, 30              N/A
     N/A                                           40s
     MPID: 110 Domain: customer MA: customer1101
44   carrier              0026.99f7.0b41            Up                      Up
 2   carrier              Gi0/2.2
 -   carrier              S, C 50, 20               N/A
     N/A                                           40s
     MPID: 43 Domain: carrier MA: carrier
400  enterprise           0026.99f7.0b41            Up                      Up
 6   enterprise           Gi0/1.1
 -   custservice          S, C 200, 70              N/A
     N/A                                           40s
     MPID: 410 Domain: enterprise MA: custservice
Router2#
```

イーサネット CFM ループバック メッセージがルータ間で正しく送受信されるかどうかを確認するには、**ping** コマンドを使用します。

```
Router#ping ethernet mpid 100 domain customer service customer1101  cos 5

Type escape sequence to abort.
Sending 5 Ethernet CFM loopback messages to 8843.e154.6f01, timeout is 5 seconds:!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Router#
Use the traceroute
 command to send the Ethernet CFM traceroute messages:
Router#traceroute ethernet mpid 100 domain customer service customer1101
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds
Tracing the route to 8843.e154.6f01 on Domain customer, Level 7, service customer1101, vlan
 100 inner-vlan 30
Traceroute sent via Gi0/2.1101
B = Intermediary Bridge
```

```
! = Target Destination
* = Per hop Timeout
------------------------------------------------------------------------------
                              MAC      Ingress        Ingr Action  Relay Action
  Hops    Host             Forwarded   Egress         Egr Action   Previous Hop
------------------------------------------------------------------------------
! 1                    8843.e154.6f01 Gi0/2.1101 IngOk        RlyHit:MEP
                      Not Forwarded                              5657.a86c.fa92
```

イーサネット CFM 設定エラー（ある場合）を表示するには、**showethernetcfmerrorconfiguration** コマンドを使用します。次に、**showethernetcfmerrorconfiguration** コマンドの出力例を示します。

```
Router#show ethernet cfm error configuration
------------------------------------------------------------------------------
CFM Interface      Type  Id         Level    Error type
------------------------------------------------------------------------------
Gi0/2              S,C   100,30     5        CFMLeak
Gi0/2              S,C   100,30     1        CFMLeak
```

イーサネット CFM の設定のトラブルシューティング

表 22：イーサネット CFM の設定の debug コマンド，（113 ページ） に、イーサネット CFM の設定に関連する問題のトラブルシューティングを行う debug コマンドの一覧を示します。

Cisco IOS マスター コマンド一覧は以下にあります。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

注意 CPU プロセスでは、デバッグ出力に高いプライオリティが割り当てられるため、デバッグ出力によってルータのパフォーマンスが低下したり、ルータが使用できなくなったりすることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。

（注） 次の表に記載されている debug コマンドのいずれかを実行する前に、必ず **loggingbuffereddebugging** コマンドを実行し、**nologgingconsole** コマンドを使用してコンソールのデバッグ ロギングをオフにしてください。

表 *22*：イーサネット *CFM* の設定の *debug* コマンド

debug コマンド	目的
debugethernetcfmall	すべてのイーサネット CFM デバッグ メッセージを有効にする。
debugethernetcfmdiagnostic	イーサネット CFM の一般的なイベントまたはパケット関連のイベントのローレベル診断デバッグを有効にする。

debug コマンド	目的
debugethernetcfmerror	イーサネット CFM エラーのデバッグを有効にする。
debugethernetcfmpackets	イーサネットCFMメッセージパケットのデバッグを有効にする。
debugecfmpalall	すべてのイーサネット CFM プラットフォームイベントのデバッグ メッセージを有効にする。
debugecfmpalapi	すべてのイーサネット CFM プラットフォームAPIイベントに関するデバッグ メッセージを表示する。
debugecfmpalcommon	すべてのイーサネット CFM プラットフォーム共通イベントに関するデバッグ メッセージを表示する。
debugecfmpalecfmpal	すべてのイーサネット CFM プラット フォームイベントのデバッグを有効にする。
debugecfmpalepl	すべてのイーサネット CFM プラットフォームエンドポイント リスト（EPL）イベントのデバッグを有効にする。
debugecfmpalisr	すべてのイーサネット CFM プラットフォーム割り込みサービス要求（ISR）イベントのデバッグを有効にする。

ルーテッドポート（L3サブインターフェイス）でのY.1731 パフォーマンス モニタリングのサポート

Y.1731 パフォーマンス モニタリング（PM）では、イーサネットのフレーム遅延、フレーム遅延変動、フレーム損失、フレーム スループット測定など、標準的なイーサネット PM 機能が提供されます。これらの測定はITU-T Y-1731 標準で規定され、メトロ イーサネット フォーラム（MEF）標準グループによって認定されています。

（注） この機能は、*advipservices* ライセンス モジュールを購入している場合にのみサポートされます。Cisco ISR および Cisco ISR G2 プラットフォームでのソフトウェア アクティベーション ライセンスの管理については、http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html を参照してください。

フレーム遅延

イーサネット フレーム遅延測定を使用して、フレーム遅延とフレーム遅延変動を測定します。イーサネット フレーム遅延は、遅延測定メッセージ（DMM）法を使用して測定します。

双方向遅延測定の設定に関する制約事項

双方向遅延測定を設定する際は、ここに記載するガイドラインと制約事項に従ってください。

- Y.1731 PM 測定は、ポイントツーポイント ネットワーク トポロジでのみ動作します。
- 遅延測定用のクロックの粒度は秒単位とナノ秒単位です。
- CFM Y.1731 パケットは、最大 2 つの VLAN タグで動作します。VLAN タグが 3 つ以上になると、予期しない動作が生じる場合があります。また、CFM Y.1731 パケットはタグなしのケースでは動作しません。

双方向遅延測定の設定

次に、双方向遅延測定を設定する方法を示します。以下の手順には、シングルとダブル タギングの両方の方法が含まれています。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipsla** *operation number*
4. 次のいずれかを実行します。
   - **ethernety1731delay** *DMM***domain** *value***vlan** *vlan-id***mpid** *value***cos** *value***sourcempid** *value*
   - **ethernety1731delay** *DMM***domain** *value***vlan** *vlan-id***inner-vlan** *inner vlan-id***mpid** *value***cos** *value***sourcempid** *value*
5. **aggregateinterval** *seconds*
6. **exit**
7. **ipslaschedule** *operation number***life** *value forever***start-time** *value*
8. **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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configureterminal** 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	**ipsla** *operation number* 例： `Router(config)# ip sla 1101`	IP SLA 設定を有効にします。 *operation-number*：設定する IP SLA 動作。

ステップ 4	次のいずれかを実行します。
	• **ethernety1731delay** *DMM***domain** *value***vlan** *vlan-id***mpid** *value***cos** *value***sourcempid** *value*
	• **ethernety1731delay** *DMM***domain** *value***vlan** *vlan-id***inner-vlan** *inner vlan-id***mpid** *value***cos** *value***sourcempid** *value*
	
	例：
	
	`Router(config-ip-sla)# ethernet y1731 delay DMM domain customer vlan 100 mpid 3101 cos 1 source mpid 4101`
	または
	
	例：
	
	`Router(config-ip-sla)# ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101 mpid 3101 cos 1 source mpid 4101`
		双方向遅延測定を設定します。
		（注） シングル タギングとダブル タギングの両方がサポートされています。
		パラメータは次のとおりです。
		• **delay**：遅延分散パラメータを指定します。
		（注） サポートされている遅延分散パラメータはDMMのみです。
		• **vlan**：VLAN を指定します。
		• **inner-vlan**：**inner-vlan** キーワードおよび *inner vlan-id* 引数で、ダブルタグ付きパケットにVLANタグを指定します。
		• **cos**：CoS を指定します。値は 0 ～ 7 の間の任意の数値に設定できます。
		（注） ダブルタグ付きパケットの場合は、**cos** の値が外部タグに指定する値に対応します。
		• **mpid**：宛先 MPID を指定します。
		• **source**：送信元 MPID を指定します。

ステップ 5	**aggregateinterval** *seconds* 例： `Router(config-sla-y1731-delay)# aggregate interval 30`	Y.1731 引数パラメータを設定します。ここで、**aggregateinterval** はパケットを送信する間隔です。 *seconds*：時間の長さを秒単位で指定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-sla-y1731-delay)# exit`	ルータ 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	**ipslaschedule** *operation number***life** *value forever***start-time** *value* 例： `Router(config)#ip sla schedule 1101 life forever start-time now`	双方向遅延測定をスケジュールします。 • **life**：実行する期間（秒単位）を指定します。この値は *forever* にも設定できます。 • **start-time**：開始する時間を指定します。選択できるオプションは、*after*、*hh:mm*、*hh:mm:ss*、*now* および *pending* です。
ステップ 8	**end** 例： `Router(config)#end`	ルータ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

双方向遅延測定の設定例

次の例は、シングル タギングを使用して双方向遅延測定を設定する方法を示しています。

```
router>enable
router#configure terminal
router(config)#ip sla
 1101
router(config-ip-sla)#ethernet y1731 delay DMM domain customer vlan 100 mpid 3101 cos 1
router(config-sla-y1731-delay)#aggregate interval 30
router(config-sla-y1731-delay)#exit
router(config)#ip sla schedule 1102 life forever start-time now
router(config)#end
```

次の例は、ダブル タギングを使用して双方向遅延測定を設定する方法を示しています。

```
router>enable
router#configure terminal
router(config)#ip sla
 1101
router(config-ip-sla)#ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101
mpid 3101 cos 1 source mpid 4101
router(config-sla-y1731-delay)#aggregate interval 30
router(config-sla-y1731-delay)#exit
router(config)#ip sla
 schedule 1101 life forever start-time now
router(config)#end
```

双方向遅延測定の設定の確認

次のコマンドを使用して、パフォーマンスモニタリング セッションを確認します。

- **showrun|secipsla**
- **showipslasummary**
- **showipslastatistics** *entry-number*
- **showipslaconfiguration** *entry-number*
- **showethernetcfmpmsessionsummary**
- show ethernet cfm pm session detail *session-id*
- show ethernet cfm pm session db *session-id*

上記コマンドの出力例を次に示します。

```
Router#show run | sec ip sla
ip sla auto discovery
ip sla 1101
 ethernet y1731 delay DMM domain customer vlan 100 inner-vlan 1101 mpid 3101 cos
 1 source mpid 4101
ip sla schedule 1101 life forever start-time now
Router#show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*1101        y1731-delay Domain:customer V -           OK          27 seconds ag
                         lan:100 CVlan:110                         o
                         1 Mpid:3101
Router#show ip sla statistics

IPSLAs Latest Operation Statistics
IPSLA operation id: 1101
Delay Statistics for Y1731 Operation 1101
Type of operation: Y1731 Delay Measurement
Latest operation start time: *10:43:12.930 UTC Mon Oct 21 2013
Latest operation return code: OK
Distribution Statistics:
Interval
 Start time:  *10:43:12.930 UTC Mon Oct 21 2013
 Elapsed time: 15 seconds
 Number of measurements initiated: 7
 Number of measurements completed: 7
 Flag: OK
Router#show ip sla configuration 1101
IP SLAs Infrastructure Engine-III
Entry number: 1101
Owner:
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: DMM
Domain: customer
Vlan: 100
CVlan: 1101
Target Mpid: 3101
Source Mpid: 4101
CoS: 1
   Max Delay: 5000
   Request size (Padding portion): 64
```

```
   Frame Interval: 1000
   Clock: Not In Sync
Threshold (milliseconds): 5000
Schedule:
   Operation frequency (seconds): 30  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Statistics Parameters
  Frame offset: 1
  Distribution Delay Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation Two-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Aggregation Period: 30
History
  Number of intervals: 2
Router#show ethernet cfm pm session summary
Number of Configured Session : 150
Number of Active Session: 2
Number of Inactive Session: 148
Router#
Router(config)#show ethernet cfm pm session detail 0
Session ID: 0
Sla Session ID: 1101
Level: 7
Service Type: S,C
Service Id: 100,1101
Direction: Down
Source Mac: 5352.a824.04fr
Destination Mac: 5067.a87c.fa92
Session Version: 0
Session Operation: Proactive
Session Status: Active
MPID: 4101
Tx active: yes
Rx active: yes
RP monitor Tx active: yes
RP monitor Rx active: yes
Timeout timer: stopped
Last clearing of counters: *00:00:00.000 UTC Mon Jan 1 1900
DMMs:
   Transmitted: 117
DMRs:
   Rcvd: 117
1DMs:
   Transmitted: 0
   Rcvd: 0
LMMs:
   Transmitted: 0
LMRs:
   Rcvd: 0
VSMs:
   Transmitted: 0
VSRs:
   Rcvd: 0
SLMs:
   Transmitted: 0
SLRs:
   Rcvd: 0
Test ID 0
Router1#
Router#show ethernet cfm pm session db 0
-------------------------------------------------------------------------------
      TX Time FWD                   RX Time FWD
      TX Time BWD                   RX Time BWD             Frame Delay
      Sec:nSec                      Sec:nSec                 Sec:nSec
```

```
---------------------------------------------------------------------------
Session ID: 0
***************************************************************************
3591340722:930326034            3591340663:866791722
3591340663:866898528            3591340722:930707484            0:274644
***************************************************************************
3591340723:927640626            3591340664:864091056
3591340664:864182604            3591340723:927976302            0:244128
***************************************************************************
3591340724:927640626            3591340665:864091056
3591340665:864167346            3591340724:927961044            0:244128
***************************************************************************
3591340725:927671142            3591340666:864121572
3591340666:864213120            3591340725:928006818            0:244128
***************************************************************************
3591340726:927655884            3591340667:864106314
3591340667:864197862            3591340726:927991560            0:244128
***************************************************************************
3591340727:927732174            3591340668:864167346
3591340668:864533538            3591340727:928327236            0:228870
***************************************************************************
3591340728:927655884            3591340669:864121572
3591340669:864197862            3591340728:928006818            0:274644
***************************************************************************
3591340729:927671142            3591340670:864121572
3591340670:864197862            3591340729:927991560            0:244128
***************************************************************************
```

双方向遅延測定の設定のトラブルシューティング

表 23：双方向遅延測定の設定の debug コマンド, （121 ページ） に、双方向遅延測定の設定に関連する問題のトラブルシューティングを行う debug コマンドの一覧を示します。

Cisco IOS マスター コマンド一覧は以下にあります。

http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html
http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html provides more information about these commands.

（注） CPUプロセスでは、デバッグ出力に高いプライオリティが割り当てられるため、デバッグ出力によってルータのパフォーマンスが低下したり、ルータが使用できなくなったりすることがあります。したがって、debug コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。

（注） 次の表に記載されている debug コマンドのいずれかを実行する前に、必ず **logging buffered debugging** コマンドを実行し、**no logging console** コマンドを使用してコンソールのデバッグ ロギングをオフにしてください。

表 *23*：双方向遅延測定の設定の *debug* コマンド

debug コマンド	目的
debug epmpal all	すべてのイーサネット パフォーマンス モニタリング（PM）イベントのデバッグを有効にする。
debug epmpal api	イーサネット PM API イベントのデバッグを有効にする。
debug epmpal rx	イーサネット PM パケット受信イベントのデバッグを有効にする。
debug epmpal tx	イーサネット PM パケット送信イベントのデバッグを有効にする。

第 4 章

電力管理の設定

この章では、これらの機能をサポートしているルータ モデルの電源管理および Power over Ethernet（PoE）について説明します。サポートされている機能については、該当するルータ モデルのマニュアルを参照してください。

EnergyWise による電力使用のモニタリング

Cisco EnergyWise は、ネットワーク デバイスとネットワークに接続しているデバイスの電力消費量のモニタと管理を行います。EnergyWise テクノロジーの使用については、次の設定ガイドを参照してください。

『Cisco EnergyWise Configuration Guide』

Power over Ethernet の設定

有効/無効を切り替えるには、**powerinline** コマンドを使用します。また、Power over Ethernet（PoE）を確認するには、**showpowerinline** コマンドを使用します。

（注） Power over Ethernet は、C867VAE-POE-W-A-K9 モデルで利用可能で、FE0 ポート、60 W 電源を使用します。

Power over Ethernet の有効化/無効化

ファスト イーサネット（FE）ポート 0 で Power over Ethernet（PoE）を有効/無効にするには、**powerinline** コマンドを使用します。特権 EXEC モードで次の手順を実行します。

手順の概要

1 **configureterminal**
2 **interfacefastethernet0**
3 **powerinline{auto|never}**
4 **end**

手順の詳細

手順の概要

1. Router# **configureterminal**
2. Router(config)# **interfacefastethernet0**
3. Router(config-if)# **powerinline{auto|never}**
4. Router(config-if)# **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	Router# **configureterminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Router(config)# **interfacefastethernet0**	ファスト イーサネット（FE）0 のインターフェイス。 （注） C867VAE-POE-W-A-K9 は、FE0 インターフェイスでのみ Power over Ethernet をサポートします。
ステップ 3	Router(config-if)# **powerinline{auto|never}**	ポートにインライン パワーを自動的に供給するように設定するには、**auto** を使用します。 ポートでのインラインパワーを無効にするには、**never** を使用します。
ステップ 4	Router(config-if)# **end** 例： `Router#`	設定モードを終了します。

インターフェイス上の Power over Ethernet 設定の確認

FE0 ポート上の電力設定を確認するには、**showpowerinline** コマンドを使用します。

```
Router# show power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
INT-PS           0        18.000     6.300         PS GOOD
Interface   Config   Device   Powered    PowerAllocated
---------   ------   ------   -------    --------------
Fa0         auto     Cisco    On         6.300 Watts
```

第 5 章

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認証、許可、アカウンティング（AAA）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、およびアカウンティング

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』（http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_4T/sec_securing_user_services_12.4t_book.html）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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）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。以下の表は、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 *24*：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	

ACL タイプ	コンフィギュレーション コマンド
規格	**access-list1-99**} {**permit**| **deny**} *source-addr [source-mask]*
拡張	**access-list100-199**} {**permit**|**deny**} *protocol source-addr [source-mask] destination-addr [destination-mask]*
名前形式	
規格	**ipaccess-liststandard** *name***deny** {*source*	*source-wildcard*	**any**}
拡張	**ipaccess-listextended** *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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）の「Access Control Lists (ACLs)」を参照してください。

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

アクセス グループ

アクセス グループとは、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、暗黙の「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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）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。

ipinspectname *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、**ipinspectinspection-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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）を参照してください。

また、Cisco IOS ファイアウォールは、セッション開始プロトコル（SIP）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 インスペクション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 侵入防御システム（IPS）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」を使用して攻撃を特定し、ネットワーク トラフィック内における悪用パターンを検出します。Cisco IOS IPS は、インライン型の侵入検知装置として機能し、ルータを通過するパケットおよびセッションを監視して、既知の IPS シグニチャとの比較を行います。Cisco IOS IPS は、不審な動作を検出すると、ネットワーク セキュリティが破られる前に対処してイベントを記録します。また、設定に応じて、次のいずれかを行います。

- アラームを送信する
- 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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html）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、カテゴリ ベースの URL フィルタリング機能があります。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』（http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_url_filtering.html）を参照してください。

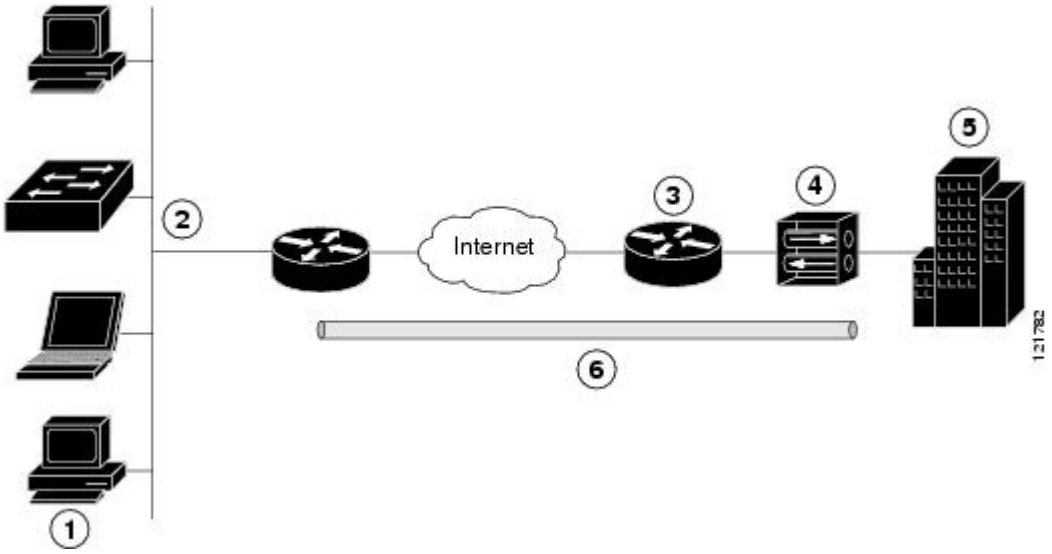
VPN の設定

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。

Remote Access 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。以下の図は、一般的な展開シナリオです。

図 *2*：*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 VPN 終端装置など）
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、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、Windows インターネット ネーム 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、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の VPN サーバに定義することができます。

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。

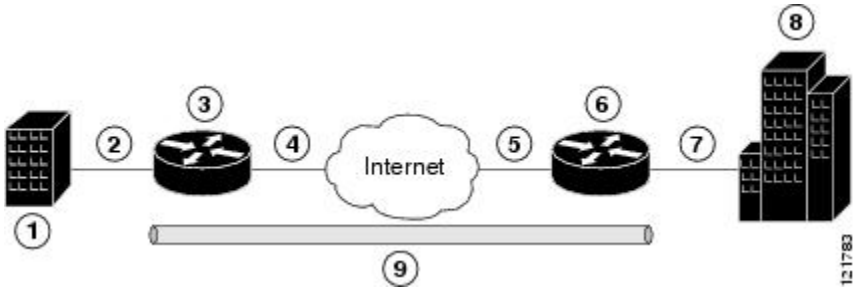
（注） Cisco Easy VPN クライアント機能で設定できるのは、1 つの宛先ピアだけです。アプリケーションで複数の VPN トンネルを作成する必要がある場合、手動でクライアントおよびサーバ側の両方に IPSec VPN およびネットワーク アドレス変換/ピア アドレス変換（NAT/PAT）パラメータを設定する必要があります。

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ます。これにより、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、http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/configuration-professional/112037-easyvpn-router-config-ccp-00.html 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 および汎用ルーティング カプセル化（GRE）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。以下の図は、一般的な展開シナリオです。

図 *3*：*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』（http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/12-4t/secon-12-4t-library.html）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, （133 ページ）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 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

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

インターネット キー交換（IKE）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. **cryptoisakmppolicy** *priority*
2. **encryption{des|3des|aes|aes192|aes256}**
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	**cryptoisakmppolicy** *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、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（ISAKMP）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|aes192|aes256}** 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 データ暗号規格（DES）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**}	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。

	コマンドまたはアクション	目的
	例： `Router(config-isakmp)# authentication pre-share`	
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. **cryptoisakmpclientconfigurationgroup** {**group-name**|**default**}
2. **key** *name*
3. **dns** *primary-server*
4. **domain** *name*
5. **exit**
6. **iplocalpool**{**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	**cryptoisakmpclientconfigurationgroup** {**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。

	コマンドまたはアクション	目的
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 ドメイン ネーム システム（DNS）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	**iplocalpool**{**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. **cryptomap** *map-name***isakmpauthorizationlist** *list-name*
2. **cryptomap** *tag***clientconfigurationaddress[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	**cryptomap** *map-name***isakmpauthorizationlist** *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、認証、許可、アカウンティング（AAA）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	**cryptomap** *tag***clientconfigurationaddress[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 ルックアップの有効化

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. **aaanew-model**
2. **aaaauthenticationlogin{default|** *list-name} method1 [method2...***]**
3. **aaaauthorization{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	**aaanew-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。

	コマンドまたはアクション	目的
ステップ 2	**aaaauthenticationlogin{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 12.4T』および『Cisco IOS Security Command Reference』を参照してください。
ステップ 3	**aaaauthorization{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 12.4T』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. **cryptoipsecprofile** *profile-name*
2. **cryptoipsectransform-set** *transform-set-name transform1 [transform2] [transform3] [transform4]*
3. **cryptoipsecsecurity-associationlifetime**{**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	**cryptoipsecprofile** *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	**cryptoipsectransform-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	**cryptoipsecsecurity-associationlifetime**{**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. **cryptodynamic-map** *dynamic-map-name dynamic-seq-num*
2. **settransform-set** *transform-set-name [transform-set-name2...transform-set-name6]*
3. **reverse-route**
4. **exit**
5. **cryptomap** *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	**cryptodynamic-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	**settransform-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。
ステップ 5	**cryptomap** *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. **cryptomap** *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	**cryptomap** *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

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, （141 ページ）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, （143 ページ）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. **cryptoipsecclientezvpn** *name*
2. **group** *group-name***key** *group-key*
3. **peer***{ipaddress | hostname}*
4. **mode** {**client**|**network-extension**|**networkextensionplus**}
5. **exit**
6. **cryptoisakmpkeepalive** *seconds*
7. **interface** *type number*
8. **cryptoipsecclientezvpn***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	**cryptoipsecclientezvpn** *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。
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。

	コマンドまたはアクション	目的
		（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**|**networkextensionplus**} 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	**cryptoisakmpkeepalive** *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 **interfaceatm0** になります。
ステップ 8	**cryptoipsecclientezvpn***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。

次の作業

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. **ipaddress** *ip-address mask*
3. **tunnelsource** *interface-type number*
4. **tunneldestination** *default-gateway-ip-address*
5. **cryptomap** *map-name*
6. **exit**
7. **ipaccess-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	**ipaddress** *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	**tunnelsource** *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	**tunneldestination** *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	**cryptomap** *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。

	コマンドまたはアクション	目的
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	**ipaccess-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。
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。

次の作業

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
```

第 6 章

セキュア ストレージの設定

この章の内容は、次のとおりです。

セキュア ストレージについて

セキュア ストレージ機能では、重要な設定情報を暗号化して保護できます。VPN、IPSec とその他の非対称キーペア、事前共有秘密、タイプ 6 のパスワード暗号化キーおよび特定のクレデンシャルを暗号化します。インスタンス固有の暗号キーは、危険にさらされることを防ぐためにハードウェアのトラスト アンカーに保管されます。

デフォルトでは、この機能はハードウェアのトラスト アンカーを備えたプラットフォームで有効です。この機能は、ハードウェアのトラスト アンカーがないプラットフォームではサポートされません。

サポートされるプラットフォーム

Cisco IOS リリース 15.6(3)M1 以降、次のプラットフォームでセキュア ストレージがサポートされています。

表 *25*：セキュア ストレージがサポートされているプラットフォーム

PID
C881-K9
C886VA-K9
C886VAJ-K9
C887VA-K9
C887VAM-K9
C888-K9
C891F-K9
C891FW-A-K9
C891FW-E-K9
C841M-4X/K9
C841M-8X/K9
C897VAB-K9
C891-24X-K9

セキュア ストレージの有効化

はじめる前に

デフォルトでは、この機能はプラットフォームで有効です。この手順は、無効になっているプラットフォームで使用します。

手順の概要

1. Config terminal
2. service private-config-encryption
3. do write memory

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例： `router#config terminal`	コンフィギュレーション モードを開始します。
ステップ 2	service private-config-encryption 例： `router(config)# service private-config-encryption`	プラットフォームでセキュリティ ストレージ機能を有効にします。
ステップ 3	do write memory 例： `router(config)# do write memory`	private-config ファイルを暗号化し、暗号化フォーマットで保存します。

次に、セキュア ストレージをイネーブルにする例を示します。

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

セキュア ストレージの無効化

はじめる前に

プラットフォームでセキュア ストレージ機能を無効にするには、次のタスクを実行します。

手順の概要

1. Config terminal
2. no service private-config-encryption
3. do write memory

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例： `router#config terminal`	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	no service private-config-encryption 例： `router(config)# no service private-config-encryption`	プラットフォームでセキュリティ ストレージ機能を無効にします。
ステップ 3	do write memory 例： `router(config)# do write memory`	private-config ファイルを復号し、プレーン フォーマットで保存します。

次に、セキュア ストレージをディセーブルにする例を示します。

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

暗号化のステータスの確認

暗号化のステータスを確認するには、**show parser encrypt file status** コマンドを使用します。次のコマンド出力は、機能は利用できるが、ファイルが暗号化されていないことを示します。ファイルは「プレーン テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

次のコマンド出力は、機能は有効で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

プラットフォーム ID の確認

標準の PEF 形式で SUDI 証明書を表示するには、show platform sudi certificate コマンドを使用します。コマンド出力から、プラットフォーム ID を簡単に確認できます。

コマンド出力にある最初の証明書は Cisco Root CA 2048 で、2 番目はシスコの下位 CA（ACT2 SUDI CA）です。3 番目は SUDI 証明書です。

```
router#show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
```

```
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFtolYYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE1MTExNDA5MzMzN1oXDTI1
MTExNDA5MzMzN1owczEsMCoGA1UEBRMjUElEOldTLUMzNjUwLTEyWDQ4VVEgU046
RkRPMTk0NkJHMDUxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRl
IFNVREkxGTAXBgNVBAMTEFdTLUMzNjUwLTEyWDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC6SARWyImWrRV/x7XQogAE+02WmzKki+4arMVBvl9o
GgvJfkoJDdaHOROSUkEE3qXtd8N3lfKy3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6dl
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F2O7
GEzb/WkO5NLexznef2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTMp1/k/TVaIepEGZuWM3hxdUZjkNGG1c1m+oB8vLX3UlSL76sDBBoiaprD
rjXBgBIozyFW8tTjh50jMDG84hKD5s31ifOe4KpqEcnVAgMBAAGjbzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQID
oDUTM0NoaXBJRD1VWUpOTlZJMENBUkhVM1Z1SUVSbFl5QXlPQ0F4TXpvek5Ub3lN
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtM8vdlf+p1WKSKX1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1ljuLHyMFTC+945F9RfA
eAuVWVb5A9dnGL8MssBJe2lVSnZwrWkT1EIdxLYrTiPAQHtll6CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNBH1uI7c2S1qlwk4WWZ6xxci+lhaQnIG
pWzapaiAYL1XrcBz4KwFc1ZZpQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICTAE
Signature version: 1
Signature:
405C70D802B73947EDBF8D0D2C8180F10D4B3EF9694514219C579D2ED52F7D583E0F40813FC4E9F549B2EB1C21725F7C
B1C79F98271E47E780E703E67472380FB52D4963E1D1FB9787B38E28B8E696570A180B7A2F131B1F174EA79F5DB4765DF67386126D8
9E07EDF6C26E0A81272EA1437D03F2692937082756AE1F1BFAFBFACD6BE9CF9C84C961FACE9FA0FE64D85AE4FA086969D0702C536ABD
B8FBFDC47C14C17D02FEBF4F7F5B24D2932FA876F56B4C07816270A0B4195C53D975C85AEAE3A74F2DBF293F52423ECB7B853967080A
9C57DA3E4B08B2B2CA623B2CBAF7080A0AEB09B2E5B756970A3A27E0F1D17C8A243
```

プラットフォームイメージの旧バージョンへのダウングレード

セキュアストレージがサポートされていない旧バージョンにプラットフォームイメージをダウングレードする場合は、サポートされているバージョンでこの機能を事前に無効にする必要があります。セキュア ストレージを無効にするには、セキュア ストレージの無効化, （149 ページ）を参照してください。

旧バージョンにダウングレードする前にこの機能を無効にしないと、private-config ファイルが暗号化形式になります。ファイルが暗号化形式になっていることを示す、次の Syslog メッセージが生成されます。

%PARSER-4-BADCFG: Unexpected end of configuration file.

ファイルが「プレーン テキスト」の場合、Syslog メッセージは生成されません。

第 7 章

バックアップ データ回線およびリモート管理の設定

Cisco 819 シリーズおよび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、を参照してください。 音声機能の設定，（197 ページ）

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。

- 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

Cisco 819 ISR は、任意の Cisco 819 シリーズ ISR の AUX ポートによるリモート管理機能をサポートします。

（注） Cisco 819 シリーズおよび Cisco 880 シリーズ ISR では、コンソール ポートおよび AUX ポートは、同じ RJ-45 物理ポートにあります。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。

（注） 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を構成できます。

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。

- 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，162 ページ
- 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，168 ページ
- 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，175 ページ
- サード パーティ製 SFP の設定，178 ページ

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。

以下の表には、Cisco 810、Cisco 880 および Cisco 890 シリーズ ISR のバックアップ インターフェイスとポートの指定をまとめています。これらのインターフェイスの基本設定をに示します。WAN インターフェイスの設定，（28 ページ）

表 *26*：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	—	—
819		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. **backupinterface** *interface-type interface-number*
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 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	**backupinterface** *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監視し、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，（154 ページ）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，（156 ページ）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。浮動スタティック ルートを使用した DDR バックアップの設定, （158 ページ）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ダイヤルオンデマンドルーティング（DDR）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。

または

dialergroup *dialer group number*

手順の概要

1. **configureterminal**
2. **interface** *type number*
3. **dialerwatch-group** *group-number*
4. **dialerwatch-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. **ipaccess-list** *access-list-number* **permit** *ip source address*
7. **interfacecellular 0**
8. 次のいずれかを実行します。
   - **dialerstring** *string*
   - または
   - **dialergroup** *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	**configureterminal** 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	**dialerwatch-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	**dialerwatch-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。
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	**ipaccess-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	**interfacecellular 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	次のいずれかを実行します。 • **dialerstring** *string*	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。

	コマンドまたはアクション	目的

	• または
	• **dialergroup** *dialer group number*
	
	例：
	`Router (config-if)# dialer string cdma *** cdma ***`
	または
	`Router (config-if)# dialer group 2 *** gsm ***`	

浮動スタティック 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. **configureterminal**
2. **iproute** *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	**configureterminal** 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	**iproute** *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、浮動スタティック 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

	コマンドまたはアクション	目的
		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
```

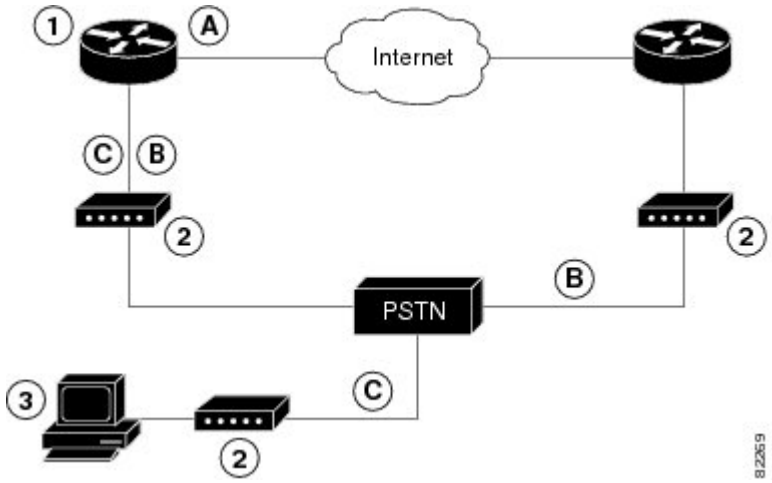
```
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@dsl.com
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto map gsm1                                          *** or cdma1 ***
!
ip local policy route-map track-primary-if
ip forward-protocol 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 または Cisco 819 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。

以下の図は、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 *4*：*AUX* 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	Modem	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. **ipname-server** *server-address*
2. **ipdhcppool** *name*
3. **exit**
4. **chat-script** *script-name expect-send*
5. **interface** *type number*
6. **exit**
7. **interface** *type number*
8. **dialerwatch-group** *group-number*
9. **exit**
10. **ipnatinsidesource{list** *access-list-number*}**{interface** *type number* |**pool***name*}**[overload]**
11. **iproute** *prefix mask {ip-address* | *interface-type interface-number [ip-address]*
12. **access-list** *access-list-number*{**deny**|**permit}** *source [source-wildcard]*
13. **dialerwatch-list** *group-number* {**ip***ip-address address-mask*| **delayroute-checkinitial** *seconds*
14. **line** [**aux**|**console**|**tty**|**vty**] *line-number [ending-line-number*]
15. **modemenable**
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

	コマンドまたはアクション	目的
ステップ 1	**ipname-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。

	コマンドまたはアクション	目的
ステップ 2	**ipdhcppool** *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、PPP および IPCP アドレス ネゴシエーションとダイヤル バックアップにより ATM インターフェイスの IP アドレスを指定する例, （166 ページ）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。

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、PPP および IPCP アドレス ネゴシエーションとダイヤル バックアップにより ATM インターフェイスの IP アドレスを指定する例, （166 ページ）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。

	コマンドまたはアクション	目的
ステップ 8	**dialerwatch-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	**ipnatinsidesource{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	**iproute** *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*| **delayroute-checkinitial** *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。
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。

	コマンドまたはアクション	目的
ステップ 15	**modemenable** 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。

PPP および IPCP アドレス ネゴシエーションとダイヤル バックアップにより ATM インターフェイスの IP アドレスを指定する例

次の設定例では、ATM インターフェイスの IP アドレスを、PPP およびインターネット プロトコル コントロール プロトコル（IPCP）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
```

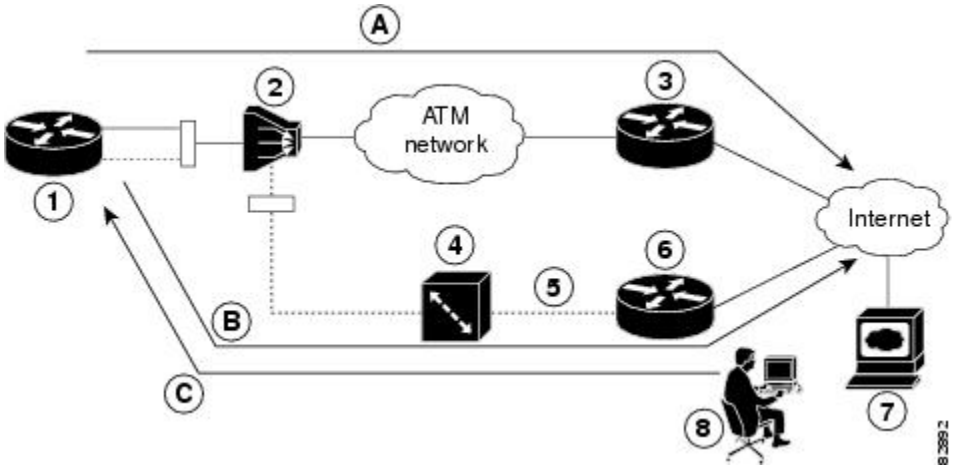
```
ip route 0.0.0.0 0.0.0.0 Dialer1 150
no ip http server
ip pim bidir-enable
!
! PC IP address behind CPE.
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 103 permit ip 192.168.0.0 0.0.255.255 any
!
! Watch multiple IP addresses because peers are alternated
! among them when the CPE 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 ルータではリモート管理に ISDN S/T ポートを使用できます。図 5：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，（169 ページ） および図 6：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，（170 ページ）は、プライマリ WAN 回線のリモート管理アクセスと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：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，（169 ページ）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 6：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, （170 ページ）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。

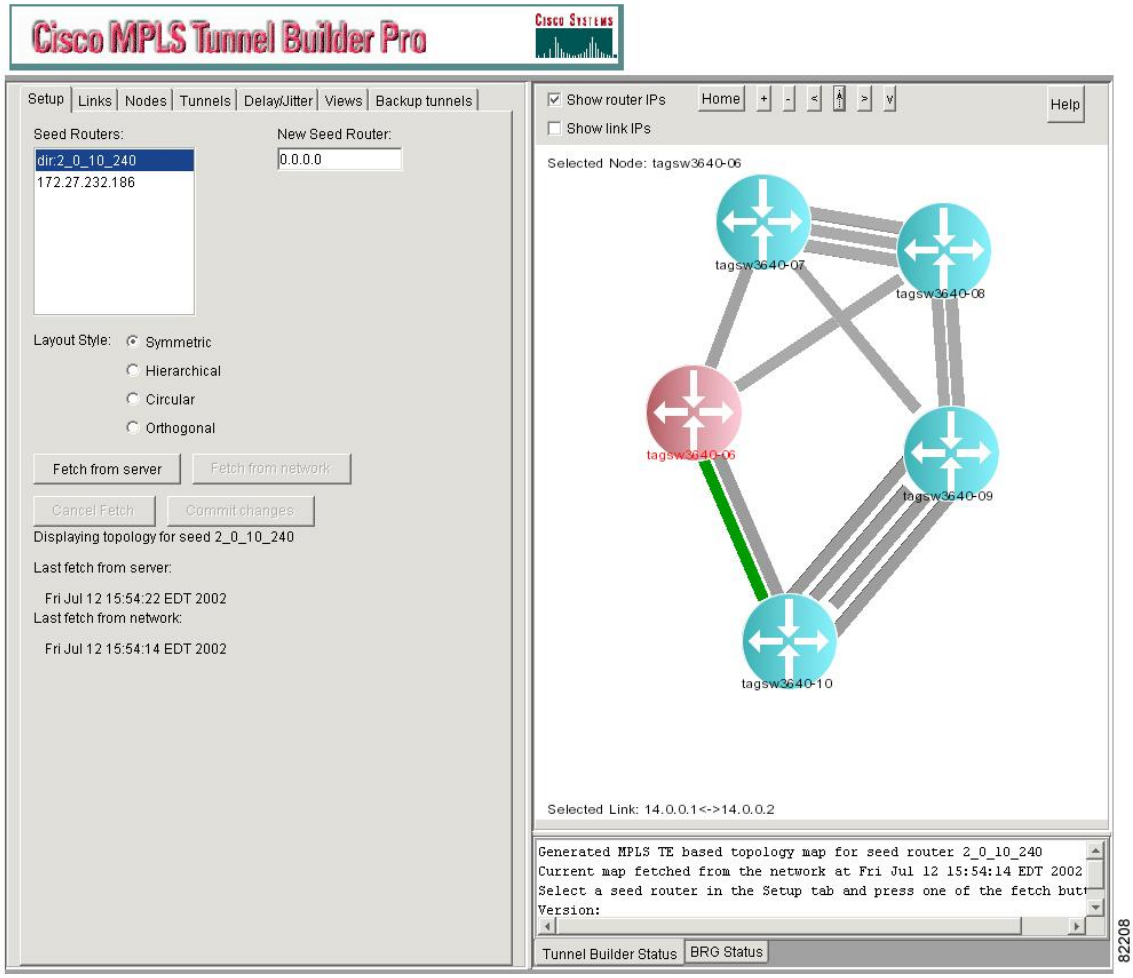
図 *5*：*CPE* スプリッタ、*DSLAM*、および *CO* スプリッタを経由するデータ回線バックアップ



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 *6* : 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, （171 ページ）
- アグリゲータおよび ISDN ピア ルータの設定, （174 ページ）

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. **isdnswitch-type** *switch-type*
2. **interface** *type number*
3. **encapsulation** *encapsulation-type*
4. **dialerpool-member** *number*
5. **isdnswitch-type** *switch-type*
6. **exit**
7. **interfacedialer** *dialer-rotary-group-number*
8. **ipaddressnegotiated**
9. **encapsulation** *encapsulation-type*
10. **dialerpool** *number*
11. **dialerstring** *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

	コマンドまたはアクション	目的
ステップ 1	**isdnswitch-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。サポートされるその他のスイッチ 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	**dialerpool-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。

	コマンドまたはアクション	目的
ステップ 5	**isdnswitch-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。
ステップ 7	**interfacedialer** *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	**ipaddressnegotiated** 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	**dialerpool** *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	**dialerstring** *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。

	コマンドまたはアクション	目的
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 Cisco 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. **enablesecret** *password*
3. **interfacegigabitethernet** *slot/port*
4. **media-type {sfp|rj45}auto-failover**
5. **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	**hostname** *name* 例： `Router(config)# hostname Router`	ルータ名を指定します。
ステップ 2	**enablesecret** *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	**interfacegigabitethernet** *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。

ステップ 5	**exit**
	例：
	`Router(config-if)# exit`
	または
	`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 の設定

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、リンクが稼働します。両方のメディアが接続されている場合、最初に稼働したメディアのリンクが稼働します。

（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. **interfacegigabitethernet** *slot/port*
2. **nomedia-type**
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	**interfacegigabitethernet** *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	**nomedia-type**
	
	例：
	`Router(config-if)# no media-type`
	`GigabitEthernet0/1: Changing media to UNKNOWN.`
	場合によっては、このインターフェイスの速度およびデュプレックス設定を更新する必要があります。
		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。

サードパーティ製 SFP の設定

Cisco の認証を得ていない Small Form-Factor Pluggable（SFP）は、サードパーティ製 SFP と呼ばれます。Cisco の承認取得済みとは、Cisco 製品との厳しい試験をクリアし、100% の互換性が保証されている SFP であることを意味します。

サードパーティ製 SFP は、Cisco 承認済みベンダー リスト（AVL）に記載されていない企業が製造しています。現在、Cisco ISR G2 ルータは、Cisco の承認取得済みの SFP のみをサポートします。リリース 15.3(2)T 以降の Cisco ISR G2 ルータは、サードパーティ製 SFP を認識します。

（注） サードパーティ製 SFP は Cisco の検証を受けていないため、Cisco はサードパーティ製 SFP に対するサポートを一切提供しません。

（注）
- 2 つの速度設定で、100BASE SFP と 1000BASE SFP のみをサポートします。
- 100BASE SFP では 100 Mbps
- 1000BASE SFP では 1000 Mbps
- 次のルータおよびモジュールのみ、サードパーティ SFP をサポートします。
- Cisco 2921 Integrated Services Router
- Cisco 2951 Integrated Services Router
- Cisco 3900 Integrated Services Router
- Cisco 3900E シリーズ サービス統合型ルータ
- Cisco 892-F ギガビット イーサネット セキュリティ ルータ
- Cisco 898-EA ギガビット イーサネット セキュリティ ルータ
- EHWIC-1GE-SFP

手順の概要

1. **enable**
2. **configureterminal**
3. **serviceunsupported-transceiver**
4. **interface type** *slot/subslot/port number*
5. **media-typesfp**
6. **speed** *value*
7. **shutdown**
8. **noshutdown**
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	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**serviceunsupported-transceiver** 例： `Router(config)# service unsupported-transceiver`	サードパーティ SFP のサポートを有効にします。
ステップ 4	**interface type** *slot/subslot/port number* 例： `Router(config)# interface ethernet 0/3/0`	設定するインターフェイスを選択します。
ステップ 5	**media-typesfp** 例： `Router(config-if)# media-type sfp`	メディア タイプを SFP に変更します。
ステップ 6	**speed** *value* 例： `Router(config-if)# speed 100`	インターフェイス速度を設定します。 （注） 100BASE SFP では、速度を 100Mbps のみに設定します。同様に、1000BASE SFP では、速度を 1000Mbps のみに設定します。
ステップ 7	**shutdown** 例： `Router(config-if)# 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 8	**noshutdown** 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。

	コマンドまたはアクション	目的

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

サード パーティ製 SFP の設定例

次の例は、Cisco ISR G2 シリーズ ルータにサード パーティ製 SFP を設定する方法を示しています。

```
Router# configure terminal
Router(config-if)# service unsupported-transceiver
Router(config)# interface ethernet 0/3/0
Router(config-if)# media-type sfp
Router(config-if)# speed 100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

第 8 章

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、スイッチ仮想インターフェイス（SVI）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。

スイッチ ポート モード

リリース 15.7 (3)M 以前では、Cisco 800 シリーズ ルータのスイッチ ポートのデフォルト モードはアクセスでした。デフォルト スイッチ ポート モード（アクセス）のコマンドは次の通りです：**switchport mode access**

リリース 15.7 (3)M 以降では、デフォルトのスイッチ ポート モードはダイナミック トランキングです。ダイナミック トランキング モードのスイッチ ポートにより、スイッチは反対側にある通信スイッチが接続を確立しようとするリンクのタイプに基づいて、トランク、またはアクセス モードを動的に切り替えることができます。デフォルト スイッチ ポート モード（ダイナミック トランキング）のコマンドは次のとおりです。 **switchport mode dynamic auto**

リリース 15.7(3)M 以降では、次の CLI を使用する方法でも Cisco 800 シリーズ ルータのスイッチ ポートを設定できます。 **switchport mode dynamic desirable**

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 でのみ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

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 トランク プロトコル

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 フォン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は、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 に準拠する受電デバイスもサポートしています。

802.1X 認証の設定

IEEE 802.1x ポート ベース認証は、一般的にアクセス可能なポートから認証されていないクライアントが LAN に接続しないように規制する、クライアント/サーバ ベースのアクセス コントロールおよび認証プロトコルを規定しています。認証サーバがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN サービスにアクセスできるようにします。クライアントが認証されるまで、IEEE 802.1x アクセス コントロールでは、クライアントの接続先であるポートを介して、Extensible Authentication Protocol over LAN（EAPOL）、Cisco Discovery Protocol（CDP）、およびスパニングツリー プロトコル（STP）トラフィックだけが許可されます。認証後、通常のトラフィックをポート経由で送受信できます。

IEEE 802.1x 認証では、ネットワーク内のデバイスにそれぞれ固有の役割があります。

- サプリカント：LAN およびスイッチ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります（サプリカントはクライアントと呼ばれることもあります）。
- サプリカント：LAN およびスイッチ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります（サプリカントはクライアントと呼ばれることもあります）。

- 認証サーバ：サプリカントの実際の認証を実行する装置。認証サーバはサプリカントの識別情報を確認し、そのサプリカントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをルータに通知します。ネットワーク アクセス デバイス（この例では Cisco ISR ルータ）は、サプリカントと認証サーバ間で認証メッセージを透過的に渡し、サプリカントと認証サーバ間で認証プロセスが実行されます。サプリカントと認証サーバ（RADIUS サーバ）間で使用される EAP 方式が決定されます。EAP 拡張機能を搭載した RADIUS セキュリティ システムは、Cisco Secure Access Control Server バージョン 3.0 以降で使用できます。RADIUS はクライアントおよびサーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。
- オーセンティケータ：サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するルータ。ルータは、サプリカントと認証サーバ間で仲介装置として動作し、サプリカントからの ID 情報を要求し、その情報を認証サーバで確認し、応答をサプリカントにリレーします。ルータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

802.1x ポートベース認証の設定方法に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/15-mt/sec-user-8021x-15-mt-book/config-ieee-802x-pba.html

スパニングツリー プロトコルの設定

スパニングツリー プロトコル（STP）は、ネットワーク内のループを回避しながらパスを冗長化するためのレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークの正常な動作を実現するには、どの 2 つのステーション間でもアクティブ パスを 1 つにする必要があります。エンド ステーション間に複数のアクティブ パスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンド ステーションにメッセージが重複して到着する可能性があります。また、スイッチも複数のレイヤ 2 インターフェイスのエンド ステーション MAC アドレスを学習する可能性が出てきます。このような状況によって、ネットワークが不安定になります。スパニングツリーの動作は透過的であり、エンドステーション側で、単一LANセグメントに接続されているのか、複数セグメントからなるスイッチドLANに接続されているのかを検出することはできません。

STP は、スパニングツリー アルゴリズムを使用し、スパニングツリーのルートとして冗長接続ネットワーク内のスイッチを 1 つ選択します。スパニングツリー アルゴリズムは、アクティブ トポロジでのポートの役割に基づいて各ポートに役割を割り当てることにより、スイッチド レイヤ 2 ネットワーク上で最良のループフリー パスを算出します。

- ルート：スパニングツリー トポロジに対して選定される転送ポート
- 指定：各スイッチド LAN セグメントに対して選定される転送ポート
- 代替：スパニングツリーのルート ブリッジへの代替パスとなるブロック ポート
- バックアップ：ループバック コンフィギュレーションのブロック ポート

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、

指定スイッチを意味します。スパニング ツリーは、冗長データ パスを強制的にスタンバイ（ブロック）ステートにします。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的にブリッジ プロトコル データ ユニット（BPDU）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポートプライオリティ、パスコストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

スイッチの 2 つのポートがループの一部になっている場合、スパニングツリー ポート プライオリティとパスコストの設定値によって、どちらのポートをフォワーディング ステートにするか、どちらをブロッキング ステートにするかが制御されます。スパニングツリー ポート プライオリティ値は、ネットワーク トポロジにおけるポートの位置とともに、トラフィック転送におけるポートの位置がどれだけ適切であるかを表します。パス コストの値は、メディアの速度を表します。

STP の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/swstp.html

例：スパニングツリー プロトコルの設定
次に、ギガビット イーサネット インターフェイスのスパニングツリー ポート プライオリティの設定の例を示します。ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# spanning-tree vlan 1 port-priority 64
Router(config-if)# end
```

ギガビット イーサネット インターフェイスのスパニングツリー ポート コストを変更する方法の例を示します。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング ステートにするインターフェイスを選択します。

```
Router#configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# spanning-tree cost 18
Router(config-if)# end
```

VLAN 10 のブリッジ プライオリティを 33792 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 priority 33792
Router(config)# end
```

VLAN 10 の hello タイムを 4 秒に設定する例を示します。hello タイムはルート スイッチがコンフィギュレーション メッセージを生成する間隔です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 hello-time 4
Router(config)# end
```

転送遅延時間を設定する例を示します。転送遅延時間は、スパニングツリーラーニング ステートおよびリスニング ステートからフォワーディング ステートに移行するまでに、インターフェイスが待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 forward-time 21
Router(config)# end
```

スパニング ツリーの最大エージング インターバルの設定の例を示します。最大エージング タイムは、再構成を試行するまでにスイッチがスパニングツリーコンフィギュレーションメッセージを受信せずに待機する秒数です。

```
Router# configure terminal
Router(config)# spanning-tree vlan 20 max-age 36
Router(config)# end
```

スイッチを VLAN 10 のルート ブリッジとして設定し、ネットワークの直径を 4 に設定する例を示します。

```
Router# configure terminal
Router(config)# spanning-tree vlan 10 root primary diameter 4
Router(config)# exit
```

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 クエリーを送信できます。

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 ホストの存在の下で、マルチキャスト トラフィックの制約されたフラッディングが可能になります。このサポートは、トラフィックを、IGMPv2 スヌーピングが IGMPv2 ホストで行うのとほぼ同じポート セットに制約します。制約されたフラッディングでは、宛先マルチキャスト アドレスだけが考慮されます。

Storm Control

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,（187 ページ）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すると常に、SNMP 通知を生成して NMS に送信させることができます。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

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 accessvlan** *vlan_id*
4. **noshutdown**
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 accessvlan** *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 ～ 1005 は予約されています。
ステップ 4	**noshutdown** 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`	設定モードを終了します。

次の作業

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、**switchportaccessvlanX** コマンドだけでは設定できません。ただし、トランク モードで設定することはできます。そのためには、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. **switchportmodetrunk**
3. **switchportaccessvlan** *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	**switchportmodetrunk** 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	**switchportaccessvlan** *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

（注） authentication timer reauthenticate seconds コマンドを使用して、イーサネット スイッチ ポートにローカル セッションのタイム アウトが設定されている場合、ポートのみ、承認ユーザに対して再認証されます。ユーザに中央 Web 認証（CWA）のログイン ページは表示されません。ユーザが中央 Web 認証（CWA）で再認証される必要がある場合は、authentication timer reauthenticate server seconds コマンドを使用します。

スパニングツリー プロトコルの設定

スパニング ツリー プロトコル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
- hello タイムの設定
- 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-tablesecure** [*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源管理の設定

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 での IGMPv3 機能のサポートにより、**groups** および **count** キーワードが **showipigmpsnooping** コマンドに追加され、**showipigmpsnooping** 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なりました。すべての VLAN に対する IGMP スヌーピングで学習したマルチキャスト テーブルを表示するには、**showipigmpsnooping** コマンドに **groups** キーワードを指定し、特定の VLAN に対する IGMP スヌーピングで学習したマルチキャスト テーブルを表示するには、**showipigmpsnooping** コマンドに、**groups** キーワード、**vlan-id** キーワード、*vlan-id* 引数を指定して使用します。IGMP スヌーピングで学習したマルチキャスト グループの数を表示するには、**showipigmpsnooping** コマンドに **groups** および **count** キーワードを指定して使用します。

ポート単位のストーム コントロールの設定

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

第 9 章

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。

音声ポート

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 基本速度インターフェイス（BRI）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 27：Cisco 880 シリーズ ISR の音声ポートの割り当て，（198 ページ） 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 *27*：*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

SIP

Session Initiation Protocol（SIP）は、インターネット技術特別調査委員会（IETF）（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』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 12.4T』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 パケットインスペクション、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、『Cisco IOS Firewall: SIP Enhancements: ALG and AIC』を参照してください。

MGCP

メディア ゲートウェイ コントロール プロトコル（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 を使用するレジデンシャル ゲートウェイ（RGW）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。

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 ピアでの設定

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

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

デュアル トーン多重周波数（DTMF）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』

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
- 短縮ダイヤル オプション

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

FAX サービス

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

FAX パススルー

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 Fax Relay

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 T.38 Fax Relay」の章を参照してください。

T.37 Store-and-Forward 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 FAX リレー

T.38 FAX リレーは、FAX 信号のリアルタイムのリレーに対し、ITU 仕様に準拠したメカニズムを提供します。MGCP ネットワークでは、ゲートウェイ制御による T.38 FAX リレーを実行できます。詳細については、『Cisco IOS Fax, 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、ダイヤルイン（DID）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、次の各項を参照してください。

SIP 固有の SRST の情報については、『Cisco Unified 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。

- 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。

第 10 章

シリアル インターフェイスの設定

この章では、シリアル インタ フェース管理の設定について説明します。

シリアル インターフェイスの設定

Cisco 819 サービス統合型ルータ（ISR）は、同期（デフォルト）および非同期のシリアルインターフェイス プロトコルをサポートします。

Cisco 819 ISR のシリアル インターフェイスを設定すると、WAN アクセス、レガシー プロトコル転送、コンソール サーバおよびダイヤル アクセス サーバなどのアプリケーションをイネーブルにすることができます。また、リモート ネットワーク管理、外部ダイヤル モデム アクセス、低密度 WAN アグリゲーション、レガシー プロトコル転送および高ポート密度のサポートをイネーブルにします。

シリアル インターフェイスにより、次の機能が実現されます。

- WAN アクセスおよびアグリゲーション
- レガシー プロトコル転送
- ダイヤル アクセス サーバ

シリアル インターフェイスを使用して、リモート サイトの WAN アクセスを提供できます。最大 8 Mbps のシリアル速度のサポートの場合、低密度および中密度の WAN アグリゲーションに理想的です。

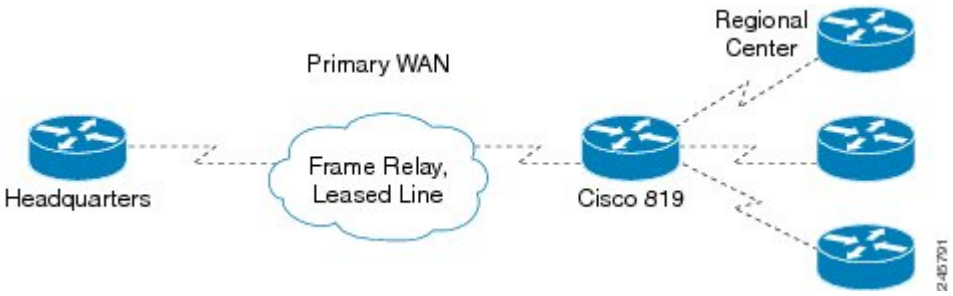
図 *7*：*WAN* コンセントレーション

レガシー プロトコル転送

シリアルおよび同期/非同期ポートは、TCP/IP ネットワーク全体での理想的なレガシー トラフィックの転送に適していて、ネットワーク コンバージェンスを容易にします。Cisco IOSR ソフトウェアでサポートされるレガシー プロトコルには、次のものが含まれます。

- 同期データ リンク制御（SDLC）プロトコル
- バイナリ同期通信プロトコル（Bisync）
- X.25 プロトコル

図 *8*：ネットワーク コンバージェンス



Cisco 819 シリーズ ISR は、シスコ スマート シリアル コネクタを使用します。サポートされているケーブルを以下の表に示します。

表 *28*：*Cisco 819 ISR* のスマート シリアル ケーブル

製品番号	ケーブル タイプ	長さ	コネクタ タイプ
CAB-SS-V35MT	V.35 DTE	10 フィート（3m）	オス型
CAB-SS-V35FC 10 フィート（3m）メス型	V.35 DCE	10 フィート（3m）	メス型
CAB-SS-232MT	EIA/TIA-232 DTE	10 フィート（3m）	オス型

製品番号	ケーブル タイプ	長さ	コネクタ タイプ
CAB-SS-232FC	EIA/TIA-232 DTE	10 フィート（3m）	メス型
CAB-SS-449MT	EIA/TIA-449 DTE	10 フィート（3m）	オス型
CAB-SS-449FC	EIA/TIA-449 DTE	10 フィート（3m）	メス型
CAB-SS-X21MT	X.21 DTE	10 フィート（3m）	オス型
CAB-SS-X21FC	X.21 DTE	10 フィート（3m）	メス型
CAB-SS-530MT	EIA/TIA-530 DTE	10 フィート（3m）	オス型
CAB-SS-530AMT	EIA/TIA-232 DTE	10 フィート（3m）	オス型

シリアル 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。

シリアル インターフェイスを設定するには、次の概念を理解しておく必要があります。

Cisco HDLC カプセル化

Cisco ハイレベル データリンク コントローラ（HDLC）は、HDLC を使用して、同期シリアル リンクでデータを送信するためのシスコ独自のプロトコルです。また、Cisco HDLC は、シリアル リンクのキープアライブを維持するシリアルラインアドレス解決プロトコル（SLARP）と呼ばれる単純な制御プロトコルも提供します。Cisco HDLC は、効率的なパケットの説明およびエラー制御を行う、オープン システム インターコネクション（OSI）スタックのレイヤ2（データリンク）におけるデフォルトのデータ カプセル化のデフォルト プロトコルです。

（注） Cisco HDLC は、シリアル インターフェイスのデフォルトのカプセル化タイプです。

シリアル インターフェイスでのカプセル化が HDLC から他のカプセル化タイプに変更されると、主要なインターフェイスに設定されたシリアル サブインターフェイスは、新しく変更されたカプセル化を引き継ぎますが、削除されません。

Cisco HDLC では、キープアライブ タイマー, （209 ページ）で説明するように、キープアライブを使用してリンク ステートをモニタします。

PPP のカプセル化

PPP は、同期シリアル リンクでデータを送信するために使用される標準プロトコルです。また、PPP は、リンクのプロパティをネゴシエートするリンク制御プロトコル（LCP）も提供します。LCP は、エコー要求および応答を使用して、リンクの継続的なアベイラビリティをモニタリングします。

（注） インターフェイスに PPP カプセル化が設定されている場合、リンクがダウンしたと宣言され、エコー応答（ECHOREP）を受信せずに 5 回のエコー要求（ECHOREQ）パケットが送信された後、完全な LCP ネゴシエーションが再開されます。

PPP は、リンク上で動作するデータ プロトコルのプロパティをネゴシエートする、次の Network Control Protocol（NCP）を提供します。

- IP のプロパティをネゴシエートする IP コントロール プロトコル（IPCP）
- MPLS のプロパティをネゴシエートするマルチプロトコル ラベル スイッチング コントロール プロセッサ（MPLSCP）
- CDP のプロパティをネゴシエートする Cisco Discovery Protocol コントロール プロセッサ（CDPCP）
- IP バージョン 6（IPv6）のプロパティをネゴシエートする IPv6CP
- OSI のプロパティをネゴシエートするオープン システム インターコネクション コントロール プロセッサ（OSICP）

PPP は、キープアライブ タイマー, （209 ページ）の説明にあるように、キープアライブを使用してリンク ステートをモニタリングします。

PPP は次の認証プロトコルをサポートします。これらのプロトコルでは、接続によるデータ トラフィックのフローを許可する前にそのアイデンティティを証明するために、リモート デバイスが必要です。

- チャレンジ ハンドシェイク認証プロトコル（CHAP）：CHAP は、リモート デバイスにチャレンジ メッセージを送信します。リモート デバイスは、共有秘密を使用してチャレンジの値を暗号化し、暗号化された値とその名前を応答メッセージでローカル ルータに戻します。ローカル ルータは、リモート デバイスの名前をローカル ユーザ名またはリモート セキュリティ サーバ データベース内に保存された関連秘密に一致させようとします。保存された秘密を使用して、元のチャレンジを暗号化し、暗号化された値が一致していることを確認します。
- Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）：MS-CHAP は CHAP の Microsoft バージョンです。CHAP の標準バージョンと同様に、MS-CHAP は PPP 認証に使用されます。この場合、認証は、Microsoft Windows NT または Microsoft Windows 95 を使用す

るパーソナル コンピュータとネットワーク アクセス サーバとして機能する Cisco ルータまたはアクセス サーバの間で行われます。

- パスワード認証プロトコル（PAP）：PAP 認証では、ローカル ユーザ名データベース内またはリモートセキュリティ サーバデータベース内の一致するエントリに照らし合わせてチェックする名前とパスワードを送信するために、リモート デバイスが必要です。

シリアルインターフェイスでCHAP、MS-CHAP、およびPAPをイネーブルにするには、インターフェイス コンフィギュレーション モードで **pppauthentication** コマンドを使用します。

（注） PPP をイネーブル化またはディセーブル化しても、リモート デバイスに対してローカル ルータ自身を識別させる機能は影響を受けません。

マルチリンク PPP

マルチリンク PPP（MLPPP）は、Cisco 819 ISR シリアル インターフェイスでサポートされています。MLPPPは、複数の物理リンクを1つの論理リンクに組み合わせる方式を提供します。MLPPPを実装することによって、複数のPPPシリアル インターフェイスを1つのマルチリンク インターフェイスに組み合わせます。MLPPPは、複数のPPPリンクでデータグラムの断片化、再編成、および配列を行います。

MLPPPは、QoSを除くPPPシリアルインターフェイスでサポートされる同じ機能を提供します。また、次の追加機能も提供します。

- 128 バイト、256 バイト、および 512 バイトのフラグメント サイズ
- 長いシーケンス番号（24 ビット）
- 失われたフラグメントの検出タイムアウト期間（80 ms）
- 最小アクティブ リンクの設定オプション
- マルチリンク インターフェイスでの LCP エコー要求および応答のサポート
- フル T1 および E1 フレームおよび非フレーム リンク

キープアライブ タイマー

シスコ キープアライブは、リンク ステートをモニタリングする場合に便利です。キープアライブは、キープアライブ タイマーの値によって決定される頻度で、定期的にピアに送信され、ピアから受信されます。受け入れ可能なキープアライブがピアから受信されない場合、リンクはダウン状態に移行します。ピアから受け入れ可能なキープアライブが受信されるか、キープアライブがディセーブルになると、リンクはすぐにアップ状態に移行します。

（注） **keepalive** コマンドは、HDLC または PPP カプセル化を使用するシリアル インターフェイスに適用されます。フレーム リレー カプセル化を使用するシリアル インターフェイスには適用されません。

各カプセル化タイプでは、ピアによって無視される特定の数のキープアライブがシリアル インターフェイスのダウン状態への移行をトリガーします。HDLC カプセル化の場合、無視されるキープアライブが 3 つあると、インターフェイスがダウン状態になります。PPP カプセル化の場合、無視されるキープアライブが 5 つあると、インターフェイスがダウン状態になります。ECHOREQ パケットは、LCP ネゴシエーションが完了した場合（LCP が開いている場合など）に限り、送信されます。

LCP が ECHOREQ パケットをピアに送信する頻度を設定するには、インターフェイス コンフィギュレーション モードで **keepalive** コマンドを使用します。システムを 10 秒のデフォルト キープアライブ インターバルに戻すには、**keepalive** コマンドに **no** キーワードを指定して使用します。キープアライブをディセーブルにするには、**keepalive** disable コマンドを使用します。PPP と Cisco HDLC の両方で、キープアライブ 0 はキープアライブをディセーブルにし、**showrunning-config** コマンドの出力に **keepalivedisable** としてレポートされます。

LCP がピアで動作していて、ECHOREQ パケットを受信すると、キープアライブがピアでイネーブルかどうかに関係なく、ECHOREP パケットで応答します。

キープアライブは、2 つのピアの間で独立しています。一方のピアの端ではキープアライブをイネーブルにし、もう一方の端ではディセーブルにすることができます。キープアライブがローカルでディセーブルの場合でも、LCP は受信する ECHOREQ パケットに ECHOREP パケットで応答します。同様に、LCP は、それぞれの端のキープアライブの期間が異なる場合でも機能します。

フレーム リレーのカプセル化

シリアル インターフェイスでフレーム リレー カプセル化がイネーブルの場合、インターフェイスの設定は階層型になっており、次の要素で構成されます。

- シリアル メイン インターフェイスは、物理インターフェイスおよびポートで構成されます。Cisco HDLC および PPP カプセル化接続をサポートするシリアル インターフェイスを使用していない場合、シリアル メイン インターフェイスの下に相手先固定接続（PVC）があるサブインターフェイスを設定する必要があります。フレーム リレー接続は、PVC でのみサポートされます。
- シリアル サブインターフェイスは、シリアル メイン インターフェイスの下に設定されます。シリアル サブインターフェイスは、シリアル サブインターフェイスの下に PVC を設定するまで、トラフィックをアクティブに伝送しません。レイヤ 3 の設定は、一般的にサブインターフェイス上で行われます。
- シリアル インターフェイスでのカプセル化が HDLC から他のカプセル化タイプに変更されると、主要なインターフェイスに設定されたシリアル サブインターフェイスは、新しく変更されたカプセル化を引き継ぎますが、削除されません。

- ポイントツーポイント PVC は、シリアル サブインターフェイスの下に設定されます。メイン インターフェイスの下にPVCを直接設定できません。1つのサブインターフェイスに対して 1 つのポイントツーポイント PVC を設定できます。PVC はあらかじめ定義された回線パスを使用し、パスが中断されるとエラーが発生します。PVCは、どちらかの設定から回線を削除しない限り、アクティブな状態に保たれます。シリアル PVC での接続は、フレーム リレー カプセル化だけをサポートします。

（注） 親インターフェイスの管理状態は、サブインターフェイスとその PVC の状態を決定します。親インターフェイスまたはサブインターフェイスの管理状態が変わると、その親インターフェイスまたはサブインターフェイスの下に設定されたすべての子PVCの管理状態も変わります。

シリアル インターフェイスにフレーム リレーの暗号化を設定するには、**encapsulation(FrameRelayVC-bundle)** コマンドを使用します。

フレーム リレー インターフェイスは、次の 2 つのタイプのカプセル化フレームをサポートします。

- Cisco（デフォルト）
- IETF

PVC に Cisco または IETF カプセル化を設定するには、PVC コンフィギュレーション モードで **encap** コマンドを使用します。PVC にカプセル化のタイプが明示的に設定されていない場合、その PVC は、メイン シリアル インターフェイスからカプセル化のタイプを引き継ぎます。

（注） Cisco カプセル化は、MPLS に設定されたシリアル メイン インターフェイスで必要です。IETF カプセル化は、MPLS ではサポートされていません。

インターフェイスにフレーム リレーのカプセル化を設定する前に、そのインターフェイスから以前のレイヤ 3 のすべての設定が除去されていることを確認する必要があります。たとえば、メイン インターフェイスの下に直接設定されている IP アドレスがないことを確認する必要があります。IP アドレスが直接設定されていると、メイン インターフェイスの下で行われたフレーム リレー設定が実行できなくなります。

フレーム リレー インターフェイスでの LMI

ローカル管理インターフェイス（LMI）プロトコルは、PVC の追加、削除、およびステータスをモニタリングします。また、LMI は、フレーム リレーUNI インターフェイスを形成するリンクの完全性を確認します。デフォルトでは、**cisco** LMI はすべての PVC でイネーブルです。

LMI のタイプが **cisco**（デフォルトの LMI タイプ）である場合、1 つのインターフェイスでサポートできる PVC の最大数は、メイン インターフェイスの MTU サイズに関連しています。カードまたは SPA でサポートされる PVC の最大数を計算するには、次の公式を使用します。

(MTU - 13)/8 = PVC の最大数

（注） シリアル インターフェイスでの **mtu** コマンドのデフォルト設定は 1504 バイトです。したがって、**cisco** LMI が設定されたシリアル インターフェイスでサポートされる PVC のデフォルト数は 186 です。

シリアル インターフェイスの設定

ここでは、次のタスクについて説明します。

同期シリアル インターフェイスの設定

同期シリアル インターフェイスは、さまざまなシリアル ネットワーク インターフェイス カードまたはシステムでサポートされています。このインターフェイスは、T1（1.544 Mbps）と E1（2.048 Mbps）の速度での全二重方式の動作をサポートします。

同期シリアル インターフェイスを設定するには、次の項で説明する作業を実行します。一覧内の各作業は、必須と任意に分けています。

この章で説明する設定作業の例については、インターフェイスの有効化設定の例, （227 ページ）を参照してください。

同期シリアル インターフェイスの指定

同期シリアル インターフェイスを指定し、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 モードで次のいずれかのコマンドを使用します。

コマンド	目的
`Router(config)#` **interface serial** *0*	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。

同期シリアル カプセル化の指定

デフォルトでは、同期シリアル回線は、ウィンドウイングまたは再送信を行わずにハイレベル データ リンク制御（HDLC）の同期フレーム構成およびエラー検出機能を提供する HDLC シリアル カプセル化方式を使用します。同期シリアル インターフェイスは、次のシリアル カプセル化方式をサポートします。

- HDLC
- フレーム リレー
- PPP

- 同期データ リンク制御（SDLC）
- SMDS
- Cisco Serial Tunnel（STUN）
- Cisco Bisync Serial Tunnel（BSTUN）
- X.25 ベースのカプセル化

カプセル化方式を定義するには、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。

コマンド	目的
`Router(config-if)#` **encapsulation** {**hdlc** | **frame-relay** | **ppp** | **sdlc-primary** | **sdlc-secondary** | **smds** | **stun** | **x25** | **bstun**}	同期シリアル カプセル化を設定します。

（注） フレーム リレー カプセル化には、**physical-layerasync** コマンドを使用できません。

カプセル化の方式は、Cisco IOS ソフトウェアで設定するプロトコルまたはアプリケーションのタイプに応じて設定されます。

- PPP については、「Configuring Media-Independent PPP and Multilink PPP」で説明しています。
- その他のカプセル化方式は、プロトコルまたはアプリケーションについて説明するそれぞれの文書および章で定義されています。また、シリアル カプセル化方式については、『Cisco IOS Interface and Hardware Component Command Reference』の **encapsulation** コマンドの箇所で説明しています。

デフォルトでは、同期インターフェイスは全二重方式で動作します。半二重モードの SDLC インターフェイスを設定するには、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ます。

コマンド	目的
`Router(config-if)#` **half-duplex**	半二重モードの SDLC インターフェイスを設定します。

バイナリ同期通信（Bisync）は、半二重プロトコルです。各ブロックの送信は明示的に確認されます。同期送信に関連する問題を回避するには、プライマリおよびセカンダリ ステーションの暗黙のロールがあります。ブロック レシーブ タイムアウトの期間内にセカンダリからの応答がない場合、プライマリは最後のブロックを再び送信します。

全二重方式のシリアル インターフェイスを設定するには、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ます。

コマンド	目的
`Router(config-if)#` **full-duplex**	スイッチドRTS信号を使用して、インターフェイスがBisyncを実行できるように指定します。

PPP の設定

PPP を設定するには、「Configuring Media-Independent PPP and Multilink PPP」を参照してください。

Bisync の設定

Cisco 819 ISR の同期シリアル ポート アダプタの Bisync 機能を設定するには、「Block Serial Tunneling (BSTUN) Overview」を参照してください。ここに挙げたすべてのコマンドは、Cisco 891 ISR の同期シリアル ポート アダプタに適用されます。インターフェイス番号を指定するすべてのコマンド構文は、Cisco 891 ISRの **slot/port** 構文をサポートします。

HDLC データの圧縮の設定

HDLC カプセル化を使用するシリアル インターフェイスでは、ポイントツーポイント ソフトウェア圧縮を設定できます。損失のないデータ圧縮によって、HDLC フレームのサイズが減少します。使用される圧縮アルゴリズムは、Stacker（LZS）アルゴリズムです。

圧縮はソフトウェアで行われ、システム パフォーマンスに大いに影響を与える可能性があります。CPU ロードが 65% を超える場合、圧縮をディセーブルにすることを推奨します。CPU ロードを表示するには、**showprocesscpu** EXEC コマンドを使用します。

トラフィックの大部分がすでに圧縮されたファイルである場合、圧縮を使用しないでください。

HDLC で圧縮を設定するには、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ます。

手順の概要

1. **encapsulationhdlc**
2. **compressstac**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encapsulationhdlc** 例： `Router(config-if)# encapsulation hdlc`	シリアル回線の 1 つのプロトコルのカプセル化をイネーブルにします。
ステップ 2	**compressstac** 例： `Router(config-if)# compress stac`	圧縮をイネーブルにします。

NRZI ライン コーディング フォーマットの使用

NonReturn-to-Zero（NRZ）および NonReturn-to-Zero Inverted（NRZI）フォーマットは、Cisco 819 シリアル ポートでサポートされます。

NRZ と NRZI は、一部の環境でのシリアル接続で必要なライン コーディング フォーマットです。NRZ 符号化が最も一般的です。NRZI 符号化は、主に IBM 環境での EIA/TIA-232 接続で使用されます。

すべてのシリアルインターフェイスのデフォルト設定は、NRZフォーマットです。デフォルトは **nonrzi-encoding** です。

NRZI フォーマットをイネーブルにするには、インターフェイス コンフィギュレーション モードで次のいずれかのコマンドを使用します。

手順の概要

1. 次のいずれかを実行します。
   - **nrzi-encoding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	次のいずれかを実行します。 • **nrzi-encoding**	NRZI符号化フォーマットをイネーブルにします。 ルータの NRZI 符号化フォーマットをイネーブルにします。

	コマンドまたはアクション	目的

	例：
	`Router(config-if)# nrzi-encoding`
	`Router(config-if)# nrzi-encoding [mark]`	

内部クロックのイネーブル化

DTEが送信クロックを戻さない場合、ルータで次のインターフェイス コンフィギュレーション コマンドを使用して、内部で生成されたクロックをシリアル インターフェイスでイネーブルにします。

手順の概要

1. **transmit-clock-internal**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**transmit-clock-internal** 例： `Router(config-if)# transmit-clock-internal`	内部で生成されたクロックをシリアル インターフェイスでイネーブルにします。

送信クロック信号の反転

長いケーブルまたはTxC信号（送信エコー クロック回線、TXCEまたはSCTEクロックとしても知られています）を送信していないケーブルを使用するシステムは、速い伝送速度で動作する場合に、エラー率が高くなる可能性があります。たとえば、PA-8TおよびPA-4T+同期シリアル ポート アダプタのインターフェイスが多数のエラーパケットを報告している場合、位相偏移が問題である可能性があります。クロック信号を反転させると、この偏移を修正できます。クロック信号を反転させるには、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. **inverttxclock**
2. **invertrxclock**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**inverttxclock** 例： `Router(config-if)# invert txclock`	インターフェイスのクロック信号を反転させます。
ステップ 2	**invertrxclock** 例： `Router(config-if)# invert rxclock`	T1/E1 インターフェイスを使用しない UIO シリアル インターフェイスの RX クロックのフェーズを反転させます。

送信遅延の設定

シリアル インターフェイスで、一部のホストが受信するよりも速くバックツーバック データ パケットを送信できます。パケット送信後の最小デッドタイムを指定し、この条件を除去できます。この設定は、MCI および SCI インターフェイス カードのシリアル インターフェイスと HSSI または MIP で使用できます。インターフェイス コンフィギュレーション モードで、システムに応じて次のいずれかのコマンドを使用します。

コマンド	目的
`Router(config-if)#` **transmitter-delay** *microseconds*	MCI および SCI 同期シリアル インターフェイスに送信遅延を設定します。
`Router(config-if)#` **transmitter-delay** *hdlc-flags*	HSSI または MIP に送信遅延を設定します。

DTR 信号パルシングの設定

すべてのシリアル インターフェイスに、パルシング データ ターミナル レディ（DTR）信号を設定できます。シリアル回線プロトコルがダウンした場合（同期ずれなどの原因による）、インターフェイス ハードウェアはリセットされ、DTR 信号は少なくとも指定された間隔で非アクティブになります。この機能は、DTR 信号のトグリングによって同期をリセットする暗号化デバイスまたは他の同様のデバイスの処理に役立ちます。DTR 信号パルシングを設定するには、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ます。

コマンド	目的
`Router(config-if)#` **pulse-time** *seconds*	DTR 信号パルシングを設定します。

回線アップ/ダウン インジケータとしての DCD の無視と DSR のモニタリング

デフォルトでは、シリアル インターフェイスが DTE モードで動作しているとき、回線アップ/ダウンインジケータとして、データ キャリア検出（DCD）信号をモニタリングします。デフォルトでは、DCE デバイスは DCD 信号を送信します。DTE インターフェイスは、DCD 信号を検出すると、インターフェイスの状態をアップ状態に変更します。

一部の構成（SDLC マルチドロップ環境など）では、DCE デバイスは、インターフェイスの活動を妨げる DCD 信号ではなく、データ セット レディ（DSR）信号を送信します。インターフェイスが回線アップ/ダウン インジケータとして DCD 信号ではなく DSR 信号をモニタリングするように設定するには、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ます。

手順の概要

1. **ignore-dcd**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ignore-dcd** 例： `Router(config-if)# ignore-dcd`	シリアル インターフェイスが回線アップ/ダウン インジケータとして DSR 信号をモニタリングするように設定します。

次の作業

⚠

注意 この機能が必要かどうかきちんと確認できる場合を除いて、このコマンドの使用には注意してください。インターフェイスの実際の状態が表示されなくなります。実際にはインターフェイスがダウンしているのに、表示を見るだけではわからない場合があります。

シリアル ネットワーク インターフェイス モジュールのタイミングの指定

Cisco 819 シリーズ ISR では、シリアル ネットワーク インターフェイス モジュールのタイミング信号の設定を指定できます。ボードが DCE として動作していて、DTE が端末タイミング（SCTE または TT）を提供する場合、DCE が DTE から SCTE を使用するように設定できます。回線が高速および長距離で動作している場合、この方法によって、クロックに対するデータの位相偏移が妨げられます。

DCEがDTEからSCTEを使用するように設定するには、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ます。

手順の概要

1. **dce-terminal-timingenable**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**dce-terminal-timingenable** 例： `Router(config-if)# dce-terminal-timing enable`	DCE が DTE から SCTE を使用するように設定します。

シリアル ネットワーク インターフェイス モジュールのタイミングの指定

ボードが DTE として動作している場合、DTE がデータを送信するために使用する DCE から得られる TXC クロック信号を反転できます。DCE が DTE から SCTE を受信できず、データが高速で動作し、送信回線が長い場合、クロック信号を反転させます。この場合も、クロックに対するデータの位相偏移が妨げられます。

ルータがTXCクロック信号を反転させるようにインターフェイスを設定するには、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ます。

手順の概要

1. **dte-invert-txc**

手順の詳細

	コマンドまたはアクション	目的
ステップ1	**dte-invert-txc** 例： `Router(config-if)# dte-invert-txc`	TXC クロック信号を反転させるタイミング設定を指定します。

低速シリアル インターフェイスの設定

この項では、低速シリアルシリアル インターフェイスを設定する方法について説明します。次の項で構成されています。

設定例については、低速シリアル インターフェイスの例, （227 ページ）を参照してください。

半二重 DTE および DCE ステート マシン

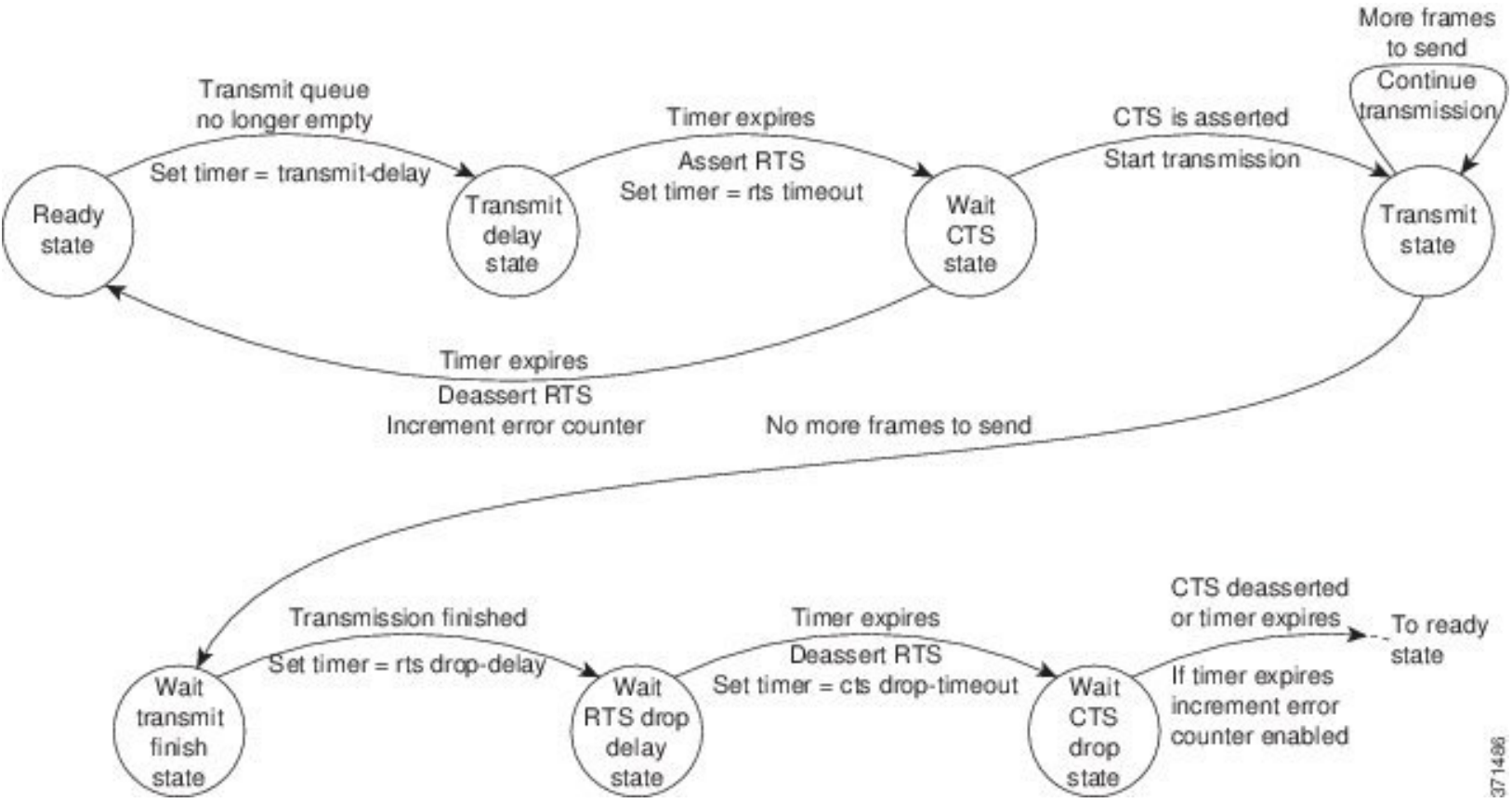
次の項では、半二重 DTE 送受信ステート マシンと半二重 DCE 送受信ステート マシンとの間の通信について説明します。

半二重 DTE ステート マシン

以下の図に示すように、低速インターフェイス用の半二重DTE送信ステートマシンは、休止時は準備状態のままです。送信のためにフレームが使用可能な場合、ステート マシンは送信遅延状態になり、**half-duplextimertransmit-delay** コマンドで定義された時間にわたって待ち状態になりま

す。デフォルトは 0 ミリ秒です。送信遅延は、半二重リンクをデバッグし、バックツーバック フレームを処理できない低速レシーバを補助するために使用されます。

図 *9*：半二重 *DTE* 送信ステート マシン



定義されたミリ秒（ms）の間、アイドル状態になった後で、ステート マシンにより、送信要求（RTS）信号がアサートされ、DCE がクリア ツー セント（CTS）待ち状態に変わって CTS がアサートされます。**half-duplextimerrts-timeout** コマンドで設定された値でタイムアウト タイマーが開始されます。デフォルトは 3 ms です。CTS がアサートされる前にタイムアウト タイマーの期限が切れた場合、ステート マシンは準備状態に戻り、RTS のアサートが解除されます。タイマーが切れる前に CTS がアサートされると、ステート マシンは送信のステートになり、フレームを送信します。

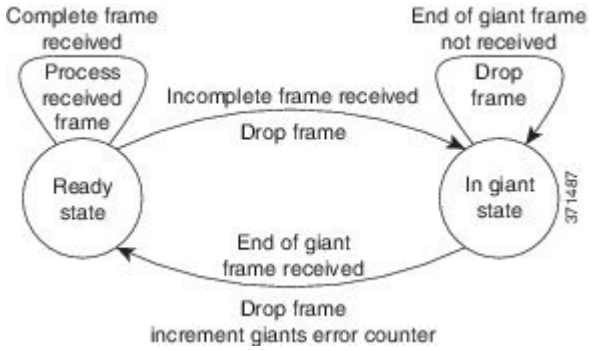
送信するフレームがなくなると、ステート マシンは送信完了待ち状態に変わります。マシンでは、シリアル コントローラが空になるまで FIFO 送信を待ち、**half-duplextimerrts-drop-delay** インターフェイス コマンドによって定義された値で遅延タイマーが開始され、RTS ドロップ待ち遅延状態に変わります。

RTS ドロップ待ち遅延状態のタイマーの期限が切れると、ステート マシンでは、RTS のアサートが解除され、CTS ドロップ待ち状態に変わります。**half-duplextimercts-drop-timeout** インターフェイス コマンドで設定された値でタイムアウト タイマーが開始され、ステート マシンでは、CTS のアサート解除を待ちます。デフォルトは 250 ms です。CTS 信号のアサートが解除されるか、ま

たは、タイムアウトタイマーの期限が切れると、ステートマシンは準備状態に戻ります。CTSのアサートが解除される前にタイマーの期限が切れると、エラーカウンタの値が増加します。この値は、該当のシリアルインターフェイスで**showcontrollers**コマンドを実行すると表示できます。

以下の図に示すように、低速インターフェイス用の半二重DTE受信ステートマシンはアイドル状態にあり、準備状態でフレームを受信します。巨大フレームは、サイズが最大伝送単位（MTU）を超えるすべてのフレームです。巨大フレームの先頭を受信すると、ステート マシンは巨大状態に代わり、巨大フレームの末尾を受信するまで、フレーム フラグメントは廃棄されます。この時点で、ステート マシンは準備状態に戻り、次のフレームの到達を待ちます。

図 *10*：半二重 *DTE* 受信ステート マシン



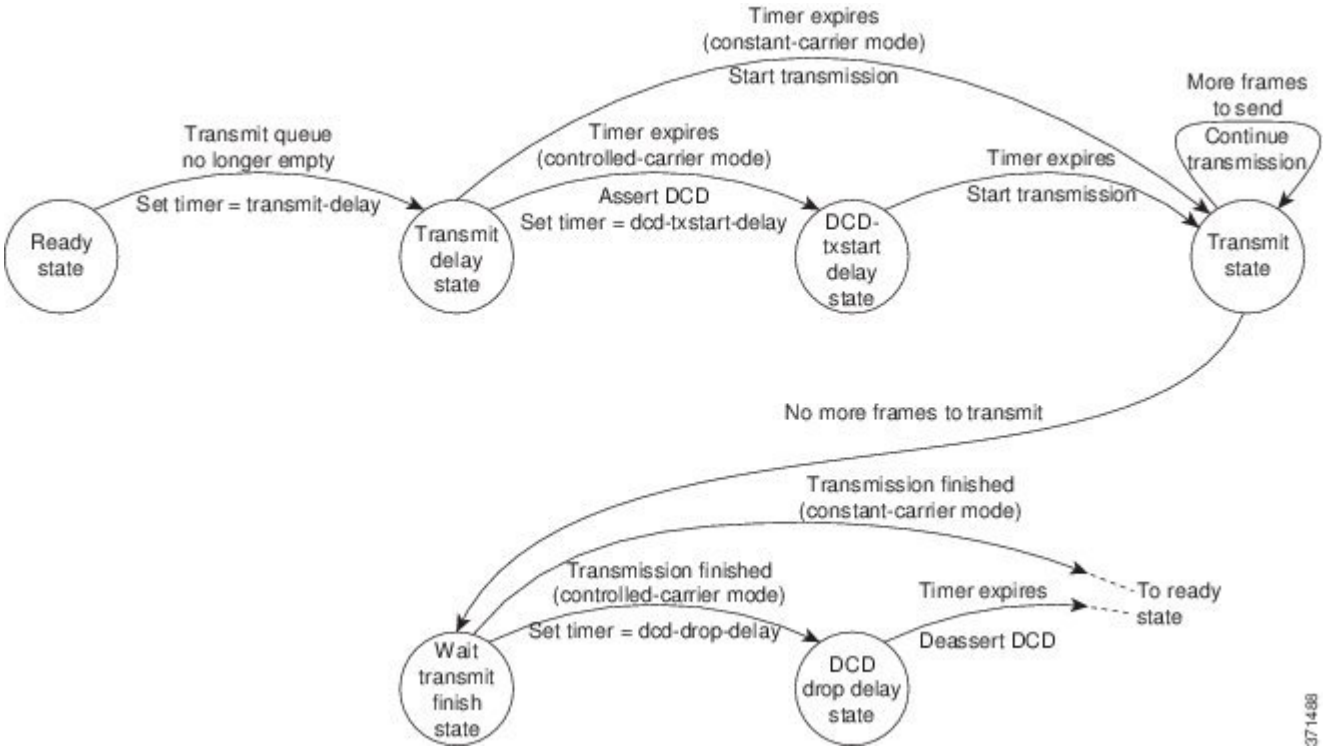
巨大フレームを受信すると、エラーカウンタの値が増やされます。エラーカウンタを表示するには、該当するシリアル インターフェイスで **showinterfaces** コマンドを使用します。

半二重 DCE ステート マシン

以下の図で説明されているように、DCE モードの低速シリアル インターフェイスでは、半二重DCE送信ステートマシンは休止時、準備状態でアイドルになっています。出力キューが空ではなくなったときなど、シリアルインターフェイスで送信にフレームを使用できる場合、ステートマシンではタイマーが開始され（**half-duplextimertransmit-delay** コマンドのミリ秒単位の値に基づいて）、送信遅延状態に変わります。DTE送信状態のマシンと同様、送信遅延状態により、フレームの送信間の遅延を設定するオプションが与えられます。たとえば、この機能を使用すると、高速に継続されて複数フレームが受信されるときに、データを損失した低速レシーバを補うことができます。デフォルトの **transmit-delay** 値は 0 ms です。0 以外の遅延値を指定するには、

half-duplextimertransmit-delay インターフェイス コンフィギュレーション コマンドを使用します。

図 *11*：半二重 *DCE* 送信ステート マシン



送信遅延状態の後の次の状態は、インターフェイスが固定キャリア モード（デフォルト）か制御キャリア モードかで異なります。

インターフェイスが固定キャリア モードの場合、次の状態を経過します。

1. **transmit-delay** タイマーの期限が切れると、ステート マシンは送信状態になります。送信するフレームがなくなるまで、ステート マシンは送信状態のままになります。
2. 送信するフレームがなくなると、ステート マシンは、送信完了待ち状態に変わります。これは、送信 FIFO が空になるのを待つ状態です。
3. FIFO が空になると、DCE が準備状態に戻り、出力キューに次のフレームが表示されるのを待ちます。

インターフェイスが制御キャリア モードの場合、インターフェイスでは、データ キャリア検出（DCD）信号を使用してハンドシェイクが実行されます。このモードでは、インターフェイスがアイドル状態で、送信するものがない場合に、DCDのアサートが解除されます。送信ステートマシンは、次の状態を経過します。

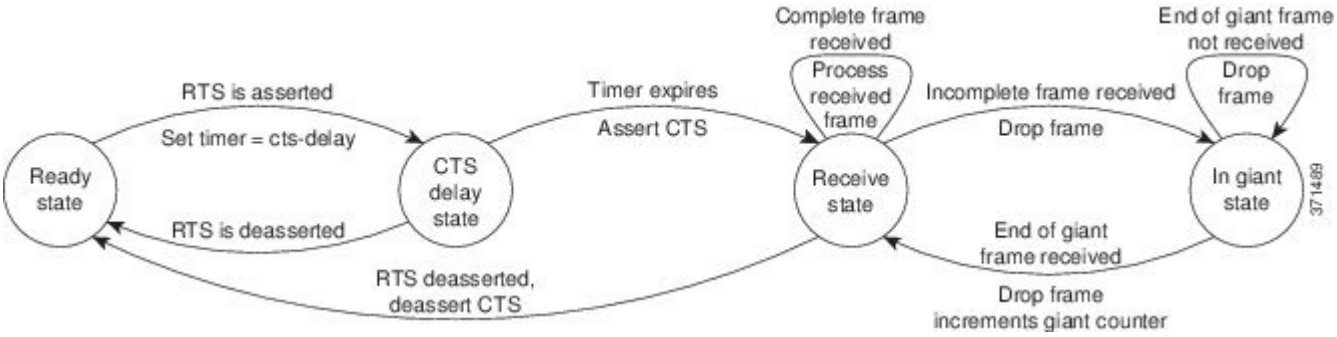
1. **transmit-delay** タイマーの期限が切れると、DCE によって DCD がアサートされ、DCD-txstart 遅延状態に移行し、DCD のアサーションと送信の開始との間の時間に遅延が生じるようになります。タイマーは、**dcd-txstart-delay** コマンドを使用して指定された値に基づいて、開始されます。（このタイマーのデフォルト値は 100 ms です。遅延値を指定するには、

half-duplextimerdcd-txstart-delay インターフェイス コンフィギュレーション コマンドを使用します）

2. この遅延タイマーの期限が切れると、ステートマシンが送信状態になり、送信するフレームがなくなるまでフレームが送信されます。
3. DCE によって最後のフレームが送信されると、送信完了待ち状態になります。これは、送信 FIFO が空になり、最後のフレームがワイヤに送信されるのを、待つ状態です。次に、DCE では、**dcd-drop-delay** コマンドを使用して値を指定することによって、遅延タイマーが開始されます。（このタイマーのデフォルト値は 100 ms です。遅延値を指定するには、**half-duplextimerdcd-drop-delay** インターフェイス コンフィギュレーション コマンドを使用します）
4. DCE は、DCD ドロップ待ち遅延状態に変わります。この状態によって、最後のフレームの送信と、DCE 送信の制御キャリア モードでの DCD のアサーション解除との間での、時間の遅延が発生します。
5. タイマーの期限が切れると、DCE によって DCD のアサートが解除され、準備状態に戻って、そのインターフェイス上で送信するフレームが存在するまでそこに残ります。

以下の図で示すように、半二重 DCE 受信ステート マシンは休止時、準備状態でアイドルになっています。DTE によって RTS がアサートされると、この状態から変化します。応答で、**cts-delay** コマンドを使用して指定された値に基づいて、DCE によってタイマーが開始されます。一部の DTE インターフェイスでは、この遅延が想定されているため、このタイマーによって、CTS のアサーションが遅延されます（このタイマーのデフォルト値は 0 ms です。遅延値を指定するには、**half-duplextimercts-delay** インターフェイス コンフィギュレーション コマンドを使用します）。

図 *12*：半二重 *DCE* 受信ステート マシン



タイマーの期限が切れると、DCE ステート マシンによって CTS がアサートされ、受信状態に変わります。受信するフレームが存在するまで、受信状態のままになります。巨大フレームの先頭を受信すると、巨大状態に代わり、巨大フレームのすべてのフレームが廃棄され続けて、受信状態に戻ります。

DTE によって RTS のアサートが解除されるときに、準備状態に戻ります。RTS のアサーション解除に対する DCE の応答によって、CTS のアサートが解除され、準備状態に戻ります。

低速シリアル インターフェイスを固定キャリア モードに設定

低速シリアル インターフェイスを制御キャリア モードから固定キャリア モードに戻すには、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. **nohalf-duplexcontrolled-carrier**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**nohalf-duplexcontrolled-carrier** 例： `Router(config-if)# no half-duplex controlled-carrier`	低速シリアル インターフェイスを固定キャリア モードに設定します。

半二重タイマーの調整

半二重タイマーのパフォーマンスを最適化するには、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。

コマンド	目的
`Router(config-if)#` **half-duplex timer** {**cts-delay** *value* | **cts-drop-timeout** *value* | **dcd-drop-delay** *value* | **dcd-txstart-delay** *value* | **rts-drop-delay** *value* | **rts-timeout** *value* | **transmit-delay** *value* }	半二重タイマーを調整します。

タイマー調整コマンドを使用すると、半二重ステート マシンのタイミングを調整し、使用している半二重環境の特定の要件に合わせることができます。

half-duplextimer コマンドとそのオプションによって、高速シリアル インターフェイスでのみ使用可能な次の 2 つのタイマー調整コマンドが置き換えられることに注意してください。

- **sdlccts-delay**
- **sdlcrts-timeout**

同期モードと非同期モードの切り替え

低速シリアル インターフェイスのモードを同期または非同期のいずれかに指定するには、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ます。

手順の概要

1. **physical-layer{sync|async}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**physical-layer{sync|async}** 例： `Router(config-if)# physical-layer sync`	低速インターフェイスのモードを同期または非同期のいずれかに指定します。

同期モードと非同期モードの切り替え

このコマンドは、Cisco 2520 ルータから Cisco 2523 ルータで使用可能な低速シリアル インターフェイスにのみ適用されます。

（注） シリアル インターフェイス上で非同期モードから同期モードに変更するときには、インターフェイスの状態は、デフォルトで、ダウン状態になります。次にインターフェイスをアップ状態にするには、**noshutdown** オプションを使用する必要があります。

同期モードでは、低速シリアル インターフェイスによって、次の 2 つのコマンドを除く、高速シリアル インターフェイスで使用可能なすべてのインターフェイス コンフィギュレーション コマンドがサポートされます。

- **sdlccts-delay**
- **sdlcrts-timeout**

非同期モードにした場合、低速シリアル インターフェイスによって、標準非同期インターフェイスで使用可能なすべてのコマンドがサポートされます。デフォルトは同期モードです。

（注） このコマンドを使用した場合、物理レイヤのコマンドのため、**showrunning-config** および **showstartup-config** コマンドの出力には表示されません。

Cisco 2520 ルータから Cisco 2523 ルータで低速シリアル インターフェイスのデフォルト モード（同期）に戻るには、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. **nophysical-layer**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**nophysical-layer** 例： `Router(config-if)# no physical-layer`	インターフェイスを、そのデフォルト モードである同期モードに戻します。

インターフェイスの有効化設定の例

次に、シリアル インターフェイスのインターフェイス設定を開始する例を示します。PPP カプセル化がシリアル インターフェイス 0 に割り当てられます。

```
interface serial 0
 encapsulation ppp
```

同じコマンドでもルータになると、たとえば PPP カプセル化をスロット 1 のポート 0 に割り当てるため、次のようになります。

```
interface serial 1/0
 encapsulation ppp
```

次の例では、lass というアドレス プールを使用するインターフェイス 7 を除くすべてのインターフェイス上で、デフォルト アドレス プールが使用されるよう、アクセス サーバを設定する方法を示します。

```
ip address-pool local
ip local-pool lass 172.30.0.1
 async interface
 interface 7
 peer default ip address lass
```

低速シリアル インターフェイスの例

ここでは、低速シリアル インターフェイスの次の設定例について説明します。

同期モードまたは非同期モードの例

次に、低速シリアル インターフェイスを同期モードから非同期モードに変更する例を示します。

```
interface serial 2
 physical-layer async
```

次に、低速シリアル インターフェイスを、非同期モードからデフォルトの同期モードに戻す例を示します。

```
interface serial 2
 physical-layer sync
```

または

```
interface serial 2
 no physical-layer
```

次に、一般的な非同期インターフェイス コンフィギュレーション コマンドの一部の例を示します。

```
interface serial 2
 physical-layer async
 ip address 10.0.0.2 255.0.0.0
 async default ip address 10.0.0.1
 async mode dedicated
 async default routing
```

次に、インターフェイスが同期モードにある場合に使用可能な、一般的な同期シリアル インターフェイス コンフィギュレーション コマンドの一部の例を示します。

```
interface serial 2
 physical-layer sync
 ip address 10.0.0.2 255.0.0.0
 no keepalive
 ignore-dcd
 nrzi-encoding
 no shutdown
```

半二重タイマーの例

次に、cts-delay タイマーを 1234 ms に設定し、transmit-delay タイマーを 50 ms に設定する例を示します。

```
interface serial 2
 half-duplex timer cts-delay 1234
 half-duplex timer transmit-delay 50
```

第 11 章

ワイヤレス デバイスの設定

この章では、ワイヤレス デバイスの初期設定、無線設定、WLAN、およびワイヤレス デバイスの管理の手順について説明します。この章は、以下の内容で構成されています。

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。大規模インストールにおいて、アクセス ポイントの無線の範囲内にいる無線ユーザは、シームレスで中断のないネットワーク アクセスを維持したまま、ファシリティ全体でローミングできます。

ワイヤレス デバイスは、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、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。

ワイヤレス デバイスのソフトウェア 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 アクセス ポイント プロトコル（LWAPP）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。

Cisco Unified Wireless モードの詳細については、http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_white_paper0900aecd804f19e3_ps6305_Products_White_Paper.htmlを参照してください。

ワイヤレス デバイスの管理オプション

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

- Cisco IOS ソフトウェア CLI
- 簡易ネットワーク管理プロトコル（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。

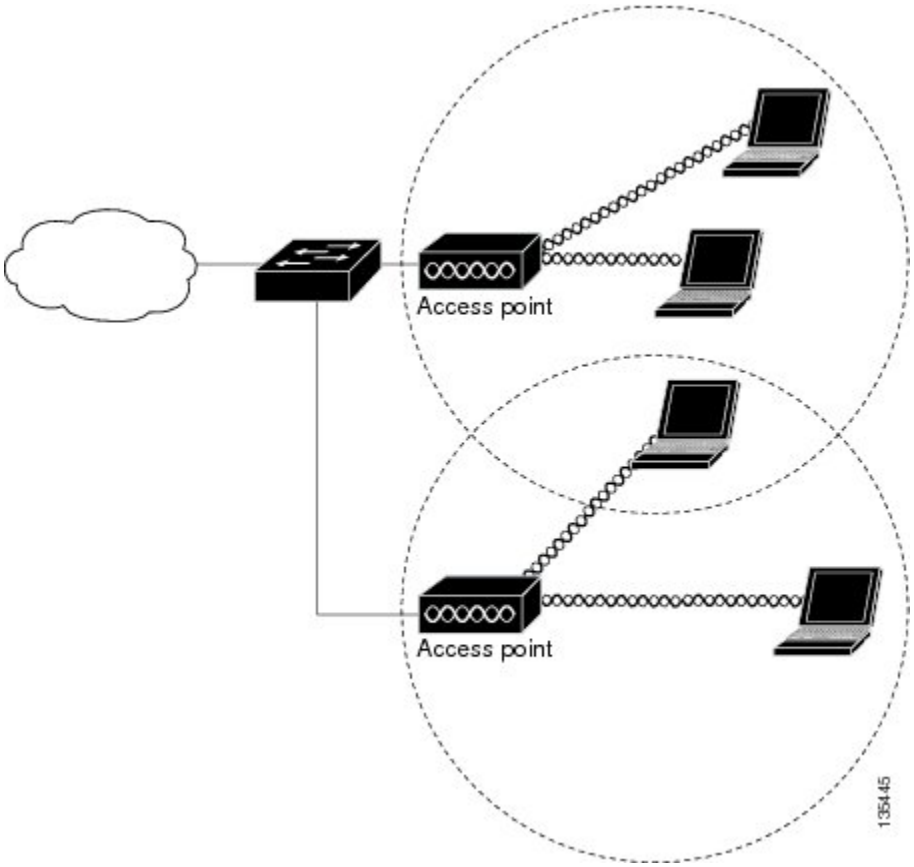
ワイヤレス デバイスを無線コンフィギュレーション モードにするには、**global** コンフィギュレーション モードから **interfacedot11radio** コマンドを使用します。ネットワークの構成例

これら一般的なワイヤレス ネットワーク構成のいずれかにアクセス 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、有線 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

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 13：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，（231 ページ） 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。

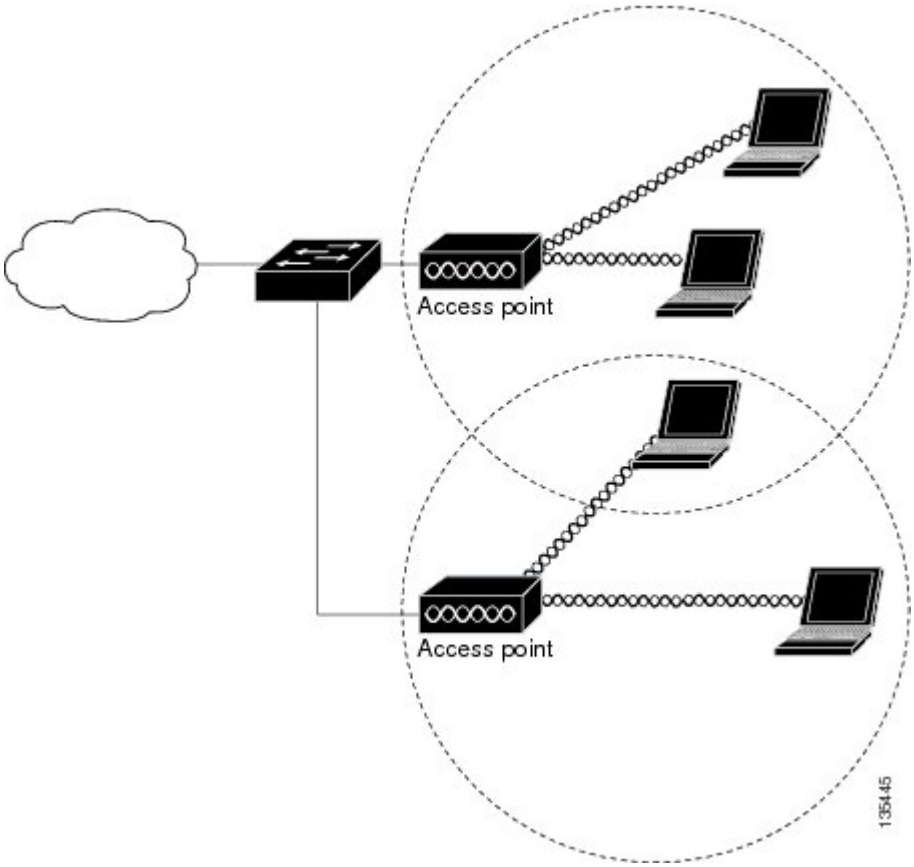
図 *13*：有線 *LAN* 上でルート ユニットとして機能するアクセス ポイント



完全なワイヤレス ネットワークでのセントラル ユニット

完全なワイヤレス ネットワークでは、アクセス ポイントはスタンドアロンのルート ユニットとして機能します。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 14：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，（232 ページ） 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 *14*：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



Cisco ScanSafe

Cisco サービス統合型ルータ G2（ISR G2）ファミリは、ファイアウォール、侵入防御と VPN を含む複数のセキュリティ サービスを提供します。これらのセキュリティ機能は、Web セキュリティのための Cisco ScanSafe、およびハードウェアやクライアント ソフトウェアの追加を必要としない Web フィルタリング ソリューションを使用する Cisco ISR Web セキュリティによって強化されました。

Cisco ScanSafe を使用する Cisco ISR Web セキュリティにより、ブランチ オフィスでインテリジェントに Web トラフィックをクラウドにリダイレクトし、ユーザ Web トラフィックへのきめ細かなセキュリティと受け入れやすい使用ポリシーを適用できます。このソリューションでは、市場をリードする Web セキュリティをすぐに展開し、帯域幅、費用、およびリソースを節約しながら、ウイルスなどの Web ベースの脅威から簡単にブランチ オフィスのユーザを保護できます。

詳細については、『Cisco ISR Web Security with Cisco ScanSafe Solution Guide』を参照してください。

イーサネット WAN インターフェイスを使用した TFTP のサポート

Trivial File Transfer Protocol（TFTP）は、その簡易性から注目すべきファイル転送プロトコルです。これは一般に、ローカル環境内のマシン間で設定またはブート ファイルを自動転送するために使用されます。

Cisco ISR 819H ISR は、10 Mbps のデータ転送速度をサポートするイーサネット WAN インターフェイスを使用した TFTP をサポートします。

詳細については、「TFTP ダウンロード コマンドの使用」セクションを参照してください。

（注） この機能は、ROMMON バージョン 15.2(2r)T 以降のすべての Cisco 819 ISR でサポートされます。

（注） スイッチ ポートを使用する TFTP ダウンロードは Cisco 819HGW SKU でのみサポートされます。

Cisco 819 シリーズ ISR の LED

LED は、ルータの前面パネルにあります。表 29：Cisco 819 シリーズ ISR の 3G LED の説明，（234 ページ） に、Cisco 819 ISR の 3G LED について説明します。

表 *29*：*Cisco 819* シリーズ *ISR* の *3G LED* の説明

LED	色	説明
SYS	黄色	FPGA のダウンロードが完了しました。
	グリーン（点滅）	ROMMON が稼働しています。
	グリーン（点灯）	IOS が稼働しています。
	グリーン（ブートアップ時に 4 回点滅）	リセット ボタンがブートアップ中に押されました。
	消灯	電源投入後、FPGA がダウンロードされている場合（ROMMON 時）。
ACT	グリーン	FE スイッチ ポート、GE WAN ポート、3G セルラー インターフェイスおよびシリアル インターフェイス上のネットワーク アクティビティ。
	消灯	ネットワーク アクティビティはありません。
WWAN	グリーン	モジュールの電源が投入されていて、接続されているが、送受信していません。
	グリーン（ゆっくり点滅）	モジュールの電源が投入されていて、接続を検索しています。
	グリーン（速く点滅）	モジュールは送信中または受信中です。
	消灯	モジュールの電源が入っていません。

LED	色	説明
GPS	グリーン（点灯）	独立型 GPS。
	グリーン（ゆっくり点滅）	GPS が取得中です。
	黄色（点灯）	アシスト型 GPS。
	黄色（ゆっくり点滅）	アシスト型GPS が取得中です。
	消灯	GPS は設定されていません。
RSSI	グリーン（点灯）	信号 > – 60 非常に強い信号
	緑色（4 回点滅した後、長い一時停止）	信号 <= –60 ～ 74 強い信号
	グリーン（2 回点滅した後、長い一時停止）	信号 <= –75 ～ -89 適正な信号
	グリーン（1 回点滅した後、長い一時停止）	信号 <= –90 ～ -109 最低限の信号
	消灯	信号 <= –110 使用不可能な信号
SIM[12]、[13]	グリーン/黄色（1 回グリーン点滅した後、2 回黄色点滅が続く）	スロット 0 の SIM はアクティブで、スロット 1 の SIM はアクティブではありません。
	黄色/緑色（1 回黄色点滅した後、2 回緑色点滅が続く）	スロット 1 の SIM はアクティブで、スロット 0 の SIM はアクティブではありません。
	消灯/緑色（2 回緑色点滅した後、一時停止）	スロット 0 に SIM がなく、スロット 1 に SIM があります。
	緑色/消灯（ゆっくり 1 回緑色点滅した後、一時停止）	スロット 0 に SIM があり、スロット 1 に SIM がありません。
	消灯/消灯	いずれかのスロットに SIM がありません。

LED	色	説明
3G	1 回緑色点滅した後、一時停止	1xRTT、EGPRS、GPRS サービスの場合。
	2 回緑色点滅した後、一時停止	EVDO、EVDO/1xRTT、UMTS の場合。
	3 回緑色点滅した後、一時停止	EVDO/1xRTT RevA、HSPA、HSUPA/HSDPA の場合。
	グリーン（点灯）	HSPA PLUS の場合。

12 Verizon および Sprint EVDO のモデムには適用されません。

13 2 つの SIM のステータスを示す LED が 1 つのみあります。1 回の点滅パターンはスロット 0 の SIM のステータスを表し、その後に 2 回の点滅パターンが続いてスロット 1 の SIM のステータスを表します。

ルータの LED のステータスを確認するには、次の show コマンドを使用します。

- **showplatformled**（すべての LED）
- **showcontrollercellular0**（3G LED）

次に、show platform led コマンドの出力例と LED ステータスを示します。

```
Router# show platform led
LED STATUS:
==========
LEDS   :  SYSTEM   WWAN           RSSI            GPS
STATUS:   GREEN    GREEN          GREEN(2 BLINK)  OFF
LEDS   :  ACTIVITY   SIM(slot0  / slot1)          3G
STATUS:   OFF            GREEN  / YELLOW          GREEN
LAN PORTS       :  FE0      FE1      FE2      FE3
LINK/ENABLE LED :  OFF      OFF      OFF      OFF
SPEED LED       :  Unknown  Unknown  Unknown  Unknown
PORT            :  GE-WAN0
LINK/ENABLE LED :  OFF
SPEED LED       :  Unknown
```

次に、3G LED ステータスを表示する show controllers cellular コマンドの出力例を示します。

```
Router# show controllers cellular 0
Interface Cellular0
3G Modem-QuadBand HSPA+R7/HSPA/UMTS QuadBand EDGE/GPRS Global and GPS,
Cellular modem configuration:
----------------------------
GSM-Carrier Type  : Cellular GSM Global.
SKU (PRI) Value: 9900198    .
Modem is recognized as valid
manufacture id:  0x00001199     product id: 0x000068A3
Sierra Wireless Mini Card MC8705 HSPA+R7 modem.
Cellular Dual SIM details:
----------------------------
SIM 0 is present
SIM 0 is active SIM
Modem Management Statistics
----------------------------
Modem resets = 2
Last known modem state = 'application' mode
Packets sent = 2508, Packets received = 44621, Packets pending = 0
```

```
DIP MDM link status retry count = 0 pdp context = 0
DIP MDM link up pending = 0 pdp context = 0
IDB Cellular0: DIP profile id = 255
RSSI LED    : 3-blink Green      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Service LED : 3-blink Green      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
SIM LED     : Slot0 - Green;    Slot1 - Off    <<<<<<<<<<<<<<<<<<<<<<<<
GPS LED     : Off                <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
GPS NMEA port = Disabled   (Stream OFF)
DM port = Disabled
    :
    :
    :
B
```

Cisco 800 シリーズ ISR の基本的なワイヤレス設定

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
- Cisco 810 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, （246 ページ）の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、次の手順に従って接続を確立して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**setup,** でワイヤレス設定を行う前に、手順 1 と 2 を実行してルータとアクセス ポイント間でセッションを開始する必要があります。

（注） リリース 15.5(03)M06 より前のリリースでは、手順 1 と 2 は必要ありません。

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. **line** *line number*
2. **transport input all**
3. **interfacewlan-ap0**
4. **ip address** サブネット マスク
5. **noshut**
6. **interfacevlan1**
7. **ip address** サブネット マスク
8. **exit**
9. **exit**
10. **service-modulewlan-ap0session**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**line** *line number* 例： `Router(config)# line 2`	設定する回線を指定し、ラインコンフィギュレーション コレクション モードを開始します。 （注） リリース 15.5(03)M06 より前のリリースでは、この手順は必要ありません。
ステップ 2	**transport input all** 例： `Router(config)# transport input all`	デバイスまたはインターフェイスをドメインに指定されたゲートウェイとして割り当てます。 （注） リリース 15.5(03)M06 より前のリリースでは、この手順は必要ありません。
ステップ 3	**interfacewlan-ap0** 例： `Router(config)# interface wlan-ap0`	ルータのコンソールインターフェイスをワイヤレスデバイスに定義します。 • このインターフェイスは、ルータのコンソールとワイヤレス デバイス間の通信に使用します。 （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.`

	コマンドまたはアクション	目的
ステップ 4	**ip address** サブネット マスク 例： `Router(config-if)# ip address 10.21.0.20 255.255.255.0`	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。 （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 5	**noshut** 例： `Router(config-if)# no shut`	内部インターフェイス接続を開いた状態を維持するように指定します。
ステップ 6	**interfacevlan1** 例： `Router(config-if)# interface vlan1`	データ通信のために、内部ギガビット イーサネット（GE0）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 7	**ip address** サブネット マスク 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 8	**exit**
	
	例：
	
	`Router(config-if)# exit`
	
	例：
	
	`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 9	**exit**
	
	例：
	
	`Router(config)# exit`
	
	例：
	
	`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。

	コマンドまたはアクション	目的

ステップ 10	**service-modulewlan-ap0session**
	
	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。

次の作業

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には、EXEC プロンプトから **aliasexecdot11radioservice-modulewlan-ap0session** 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 **dot11radio** 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間のセッションを閉じるには、ワイヤレスデバイス上で control+shift+6 および x を使用し、ルータで **disconnect** コマンドを入力して enter 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，（237 ページ）を参照してください。

使用しているソフトウェアに応じて、次のツールのいずれかを使用してワイヤレス 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，（241 ページ）：自律ソフトウェア
- Cisco Express 設定，（241 ページ）：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、手順についてCisco Unified ソフトウェアへのアップグレード, （246 ページ）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、Web ブラウザ ツールを使用して、次の手順を実行します。

1. ワイヤレス デバイスとコンソール接続を確立し、**showinterfacebvi1CiscoIOS** コマンドを入力して、ブリッジグループ仮想インターフェイス（BVI）IP アドレスを取得します。
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。
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。
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

自律モードまたは Cisco Unified モードで信号を伝送するために、ワイヤレス デバイスの無線パラメータを設定します。特定の設定手順については、無線の設定, （252 ページ）を参照してください。

無線セキュリティ設定の実行

この項では、次の設定作業について説明します。

認証の設定

認証の種類は、サービス セット識別子（SSID）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 アドレスまたは拡張認証プロトコル（EAP）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/SecurityAuthentication Types.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 の設定と SSID の割り当て

無線 LAN で VLAN を使用し、SSID を VLAN に割り当てると、表 30：SSID セキュリティの種類,（244 ページ）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。

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

（注） VLAN を使用しない場合、暗号化設定（WEP と暗号）が 2.4GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN が無効な状態で、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 タイプ

表 30：SSID セキュリティの種類, （244 ページ） 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 *30*：*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、[No Security] よりは安全です。ただし、静的 WEP キーは攻撃に対して脆弱です。この設定を行う場合は、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。『*Cipher Suites and WEP*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html）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、『*Using the Access Point as a Local Authenticator*』（http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html）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。

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[14] 認証	このオプションは、802.1X認証を有効にします（LEAP[15]、PEAP[16]、EAP-TLS[17]、EAP-FAST[18]、EAP-TTLS[19]、EAP-GTC[20]、EAP-SIM[21]、およびその他の802.1X/EAP ベースの製品）。 この設定は、必須の暗号化、WEP、オープン認証プラスEAP、ネットワーク EAP 認証を使用し、キー管理なしで RADIUS サーバ認証ポート 1645 を使用します。 ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。802.1X認証によって動的暗号キーが提供されるため、WEP キーを入力する必要はありません。	必須の 802.1X 認証。この SSID を使用してアソシエートするクライアントデバイスは、802.1X認証を実行する必要があります。 ワイヤレス クライアントでEAP-FASTを使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAPによるオープン認証を設定していない場合、以下の警告メッセージが表示されます。 `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
WPA[22]	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、暗号化暗号、TKIP[23]、オープン認証と EAP、ネットワーク EAP 認証、キー管理（WPA 必須）、RADIUS サーバ認証ポート 1645 を使用します。 拡張認証プロトコル（EAP）認証の場合と同じように、ネットワーク上の認証サーバのIPアドレスと共有秘密キーを入力する必要があります（サーバ認証ポート 1645）。	WPA 認証が必須。この SSID を使用して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.`

14 EAP = Extensible Authentication Protocol
15 LEAP = Lightweight Extensible Authentication Protocol
16 PEAP = Protected Extensible Authentication Protocol
17 EAP-TLS = Extensible Authentication Protocol—Transport Layer Security
18 EAP-FAST = Extensible Authentication Protocol—Flexible Authentication via Secure Tunneling

19 EAP-TTLS = Extensible Authentication Protocol—Tunneled Transport Layer Security
20 EAP-GTC = Extensible Authentication Protocol—Generic Token Card
21 EAP-SIM = Extensible Authentication Protocol—Subscriber Identity Module
22 WPA = Wi-Fi Protected Access
23 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、スイッチはパケットを送信します。ワイヤレス デバイスに QoS を設定するには、以下にある『*Quality of Service 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/QualityOfService.html.

ホット スタンバイ モードでのアクセス ポイントの設定

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

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。監視対象アクセス 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。

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

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。

設定例：アクセス ポイントの IP アドレスの保護

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、『Cisco Wireless LAN Configuration Guide』を参照してください（http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html）。

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。

1. ルータから WLC サーバに ping を実行し、接続を確認します。
2. **service-modulewlan-ap0session** コマンドを入力し、アクセス ポイントへのセッションを確立します。
3. アクセス ポイントが自律起動イメージを動作させているか確認します。
4. show boot コマンドを入力してアクセス ポイントのモード設定がイネーブルになっていることを確認します。

```
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。

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（回復イメージともいう）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-modulewlan-ap0bootimageunified** コマンドを使用します。

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

（注） **service-modulewlan-ap0bootimageunified** コマンドが正しく機能しない場合は、ソフトウェア ライセンスが有効かどうか確認してください。

（注） 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特権 EXEC モードで **showboot** コマンドを使用します。

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-modulewlan-ap0reload** 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。

（注） 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, （241 ページ）を参照してください。

APを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

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。

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。このいずれかが発生する場合は、**service-modulewlan-ap0resetbootloader** コマンドを使用し、イメージを手動で回復できるようにアクセス ポイントをブートローダに戻します。

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-modulewlan-ap0bootimageautonomous** 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-modulewlan-ap0reload** 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 ポイントのイメージをリカバリするには、グローバル コンフィギュレーション モードで **service-modulewlan-ap0resetbootloader** コマンドを使用します。このコマンドを使用すると、アクセス ポイントがブートローダに戻り、手動でイメージをリカバリできるようになります。

注意 このコマンドの使用には注意が必要です。この操作では通常のシャットダウンが実行されないことから、実行中のファイル操作に影響が生じる場合があります。このコマンドは、シャットダウンまたは障害状態から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。

表 *31*：シスコの自律ソフトウェアのマニュアル

トピック	リンク
ワイヤレスの概要	ワイヤレス デバイス概要，（229 ページ）
無線の設定	無線の設定，（252 ページ）
『*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

トピック	リンク
『*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[24] 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。 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
『*Cipher Suites and WEP*』	本マニュアルでは、WPA および CCKM[25] を使用するのに必要な暗号スイートや WEP を設定する方法、および AES[26]、MIC[27]、TKIP、ブロードキャスト キー ローテーションなどの WEP 機能を設定する方法について説明します。 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

トピック	リンク
『*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
アクセス ポイントの管理	無線デバイスの管理, （334 ページ）
QoS	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、スイッチは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

24 AAA = 認証、認可、アカウンティング。
25 CCKM = Cisco Centralized Key Management
26 AES = Advanced Encryption Standard
27 MIC = メッセージ整合性チェック

表 *32*：*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

ネットワーク デザイン	リンク
『*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

無線の設定

ここでは、ワイヤレス デバイスに無線設定を行う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。

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、サービス セット識別子（SSID）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. **copyrunning-configstartup-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。 （注） 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。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**copyrunning-configstartup-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。

無線ネットワーク内のワイヤレス デバイスのロール

ワイヤレス デバイスは、無線ネットワーク内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 ロールはシャット ダウンです。つまり、ワイヤレス デバイスは、その無線をシャット ダウンし、すべてのクライアント デバイスの関連付けを解除します。

無線ネットワーク内のワイヤレス デバイスのロールの設定

ワイヤレス デバイスの無線ネットワーク ロールおよびフォールバック ロールを設定するには、特権 EXEC モードで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. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0}**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 802.11g/n 2.4 GHz および 2.4 GHz は radio 0 です。
ステップ 3	**station-role non-root {bridge | wireless-clients} root {access-point | ap-only | [bridge | wireless-clients] | [fallback | repeater | shutdown]} workgroup-bridge {multicast | mode { client | infrastructure} | universal** *Ethernet-client-MAC-address* **}**	ワイヤレス デバイスのロールを設定します。 • ワイヤレス クライアントがある、またはない非ルート 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 ブリッジにロールを設定します。 （注） ブリッジモード無線はポイントツーポイント構成だけをサポートします。 （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。

	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	**copyrunning-configstartup-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。

次の作業

（注） 無線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。

デュアル無線フォールバックの設定

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

デュアル無線フォールバックは、次の 3 つの方法で設定できます。

無線トラッキング

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、無線ネットワーク内のワイヤレス デバイスのロール，（253 ページ）を参照してください。

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

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

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

MAC アドレス トラッキング

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

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

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

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

無線データ レートの概要

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 デバイスは常に **basic** に設定された最大データ レートで転送しようとします。なお、ブラウザベースのインターフェイスでは、basic は **required** と呼ばれます。障害や干渉がある場合、ワイヤレス デバイスはデータ伝送が可能である最も高いデータ レートに引き下げます。各データ レートは、次の 3 つのステートのいずれかに設定できます。

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

• Disabled：ワイヤレス デバイスでは、データはこのレートで送信されません。

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

データ レート設定を使用して、特定のデータ レートで稼働中のサービス クライアント デバイスにアクセス ポイントを設定できます。たとえば、11 Mbps サービスにのみ 2.4 GHz 無線を設定するには、11 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。1 Mbps および 2 Mbps でデータを転送するクライアント デバイスだけに対応するようにワイヤレス デバイスを設定するには、1 Mbps および 2 Mbps を **basic,** に設定し、その他のデータ レートは **disabled** に設定します。2.4 GHz、802.11g 無線を、802.11g クライアント デバイスだけに対応するように設定するには、Orthogonal Frequency Division Multiplexing（OFDM：直交周波数分割多重方式）データ レート（6、9、12、18、24、36、48、54）を、すべて **basic** に設定します。54 Mbps サービスにのみ 5 GHz 無線を設定するには、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は 1 Mbs レートを **basic** に設定し、他のレートを **enabled** に設定します。この range 設定によって、アクセスポイントではデータ レートについて妥協することでカバレッジ領域を拡大できます。したがって、他のクライアントは接続できるのにアクセス ポイントに接続できないクライアントがある場合は、そのクライアントがアクセス ポイントの適用範囲内に入っていないことが考えられます。このような場合、範囲オプションを使用することにより適用範囲を拡大すると、クライアントがアクセス ポイントに接続できるようになる可能性があります。

通常、スループットと範囲が交換条件となります。信号が低下する（アクセス ポイントからの距離が遠いなどの理由により）と、リンクを維持するためにレートのネゴシエーションをやり直します（この場合は、データ レートが低くなります）。設定されている高データ レートを維持できないほどに信号が低下した場合に、高いスループットに設定したリンクが単純にドロップするか、十分なサービス範囲を持ったアクセス ポイントが利用可能な場合は、そちらにローミングされます。設計する際は、この 2 つ（スループットと範囲）のバランスを、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、そして当然ながら RF 環境の質に基づいて考える必要があります。データ レート設定に **throughput** を入力すると、ワイヤレス デバイスは 4 つすべてのデータ レートを **basic** に設定します。

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

無線データ レートの設定

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**
   - 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}
4. **end**
5. **copyrunning-configstartup-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	**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：	各データ レートを basic または enabled に設定します。または、range を入力して範囲を最適化するか、throughput を入力してスループットを最適化します。 • （任意）1.0、2.0、5.5、および 11.0 を入力すると、802.11b、2.4 GHz 無線でこれらのデータ レートが enabled に設定されます。

	コマンドまたはアクション	目的
	{[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}**	1.0、2.0、5.5、6.0、9.0、11.0、12.0、18.0、24.0、36.0、48.0、および 54.0 を入力すると、802.11g、2.4 GHz 無線でこれらのデータ レートが enabled に設定されます。 6.0、9.0、12.0、18.0、24.0、36.0、48.0、および 54.0 を入力すると、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、2.4 GHz 無線でこれらのデータ レートが basic に設定されます。 basic-1.0、basic-2.0、basic-5.5、basic-6.0、basic-9.0、basic-11.0、basic-12.0、basic-18.0、basic-24.0、basic-36.0、basic-48.0、および basic-54.0 を入力すると、802.11g、2.4 GHz 無線でこれらのデータ レートが basic に設定されます。 （注） 選択した basic レートをクライアント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 12 Mbps 以上を選択した場合、802.11b クライアント デバイスは、ワイヤレス デバイスの 802.11g 無線に関連付けできません。 basic-6.0、basic-9.0、basic-12.0、basic-18.0、basic-24.0、basic-36.0、basic-48.0、および basic-54.0 を入力すると、5 GHz 無線でこれらのデータ レートが basic に設定されます。 • （任意）範囲、またはスループットを自動的に最適化するには、range または throughput、あるいは **{[1.0] [11.0] [2.0] [5.5] [basic-1.0] [basic-11.0] [basic-2.0] [basic-5.5] | range | throughput}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** に設定し、他のレートを enabled に設定します。throughput を入力すると、ワイヤレス デバイスはすべてのデータ レートを basic に設定します。 （任意）802.11g 無線で、すべての OFDM レート（6、9、12、18、24、36、および 48）を **basic**（**required**）に設定し、すべての 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）。

	コマンドまたはアクション	目的
		802.11g 無線では、default オプションによって、レート 1、2、5.5、および 11 は **basic** に、レート 6、9、12、18、24、36、48、および 54 は **enabled** に設定されます。これらのレート設定によって、802.11b および 802.11g の両方のクライアント デバイスが、ワイヤレス デバイスの 802.11g 無線にアソシエートできます。 5-GHz 無線では、default オプションによって、レート 6.0、12.0、および 24.0 は **basic** に、レート 9.0、18.0、36.0、48.0、および 54.0 は **enabled** に設定されます。 802.11g/n 2.4-GHz 無線では、default オプションによって、レート 1.0、2.0、5.5、および 11.0 が **enabled** に設定されます。 802.11g/n 5-GHz 無線では、default オプションによって、レート 6.0、12.0、および 24.0 が **enabled** に設定されます。 どちらの 802.11g/n 無線の変調符号化方式（MCS）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	**copyrunning-configstartup-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。

設定例：無線データ レートの設定

次に、コンフィギュレーションからデータ レート **basic-2.0** および **basic-5.5** を設定する方法を示します。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

MCS レートの設定

変調符号化方式（MCS）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 パラメータおよび前方誤り訂正（FEC）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 3 つで決まります。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 33：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，（261 ページ） は、MCS、ガード インターバル、およびチャネル幅に基づいた可能なデータ レートを示したものです。

表 *33*：*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

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		
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				

設定例：MCS レート

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. **configureterminal**
2. **interfacedot11radio{0}**
3. **power local**
4. **end**
5. **copyrunning-configstartup-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	**configureterminal** 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	**interfacedot11radio{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**
	
	例：
	`These options are available for the 2.4-GHz 802.11n radio (in dBm):`
	
	例：
	`{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。
		（注） 電力の設定をデフォルト設定の最大に戻すには、**powerlocal** コマンドの no 形式を使用します。

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

アソシエートしたクライアント 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動的電力制限（DPC）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 モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface dot11radio {0}**
3. **power client**
4. **end**
5. **copyrunning-configstartup-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**
	例：
	`These options are available for 802.11n 2.4-GHz clients (in dBm):`
	`{local | 8 | 9 | 11 | 14 | 15 | 17 | maximum}`
		ワイヤレス デバイスにアソシエートするクライアント デバイスに、最大許可電力レベルを設定します。
		• 電力レベルを local に設定すると、クライアントの電力レベルはアクセス 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	**copyrunning-configstartup-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。

次の作業

アソシエートしたクライアントの最大電力レベルを無効にするには、**powerclient** コマンドの no 形式を使用します。

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

無線チャネルの設定

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

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

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

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

802.11n 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。

20 MHz 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 20 MHz 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 チャネル幅の設定

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 モードで次の手順を実行します。

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. **copyrunning-configstartup-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**、40-below の 3 つです。 **40-below:** ◦ **20** を選択すると、チャネル幅が 20 MHz に設定されます。 ◦ **40-above** を選択すると、拡張チャネルをコントロール チャネルの上に重ねた状態でチャネル幅が 40 MHz に設定されます。 ◦ **40-below** を選択すると、拡張チャネルをコントロール チャネルの下に重ねた状態でチャネル幅が 40 MHz に設定されます。 （注） 動的周波数選択（DFS）に関する欧州連合の規制に準拠する 5 GHz の無線については、channel コマンドはディセーブルに設定されています。詳細については、「ワールド モードのイネーブル化とディセーブル化, （267 ページ）」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	**copyrunning-configstartup-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

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ワイヤレスデバイスを設定できます。ワールドモードをイネーブルにすると、ワイヤレスデバイスはそのビーコンにチャネルキャリアセット情報を追加します。ワールドモードがイネーブルになっているクライアントデバイスは、キャリアセット情報を受信して、それぞれの設定を自動的に調整します。たとえば、日本で主に使用されるクライアントデバイスがイタリアに移され、そこでネットワークに参加した場合、ワールド モードに依存して、そのチャネルと電力の設定を自動的に調整することができます。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 モードのイネーブル化

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. **copyrunning-configstartup-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**	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。

	コマンドまたはアクション	目的
	| outdoor} | world-mode roaming | legacy}	◦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	**copyrunning-configstartup-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。

次の作業

ワールド モードを無効にするには、**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 Cisco Aironet 無線 LAN アダプタのすべての初期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、短いプリアンブルは使用しないようにします。

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

short 無線プリアンブルのディセーブル化

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. **copyrunning-configstartup-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。 （注） 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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-configstartup-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。

次の作業

送受信アンテナ

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 4 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）アンテナがある場合は、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あり、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。

送受信アンテナの設定については、次の項を参照してください。

送受信アンテナの設定

ワイヤレス デバイスがデータの送受信に使用するアンテナを選択するには、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. **interface dot11radio {0 }**
3. **gain dB**
4. **antenna receive {diversity | left | right}**
5. **end**
6. **copyrunning-configstartup-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。

	コマンドまたはアクション	目的
		（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	**copyrunning-configstartup-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 デバイスとアソシエートしたクライアント デバイスとの間の特定の相互作用に必要な機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- ロード バランシング：ワイヤレス デバイスでは、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 エラー レート、および信号強度です。
- メッセージ整合性チェック（MIC）：暗号化されたパケットへの攻撃（ビットフリップ攻撃）を阻止するために新しく追加された WEP セキュリティ機能。MIC は、ワイヤレス デバイスおよび関連付けられているすべてのクライアント デバイスに実装され、数バイトを各パケットに付加することによって、パケットの不正改ざんを防止します。
- 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 エラー レート、および信号強度です。
- Cisco Key Integrity Protocol（CKIP）：シスコの WEP キー置換技術で、IEEE 802.11i セキュリティ タスク グループにより開示された初期のアルゴリズムに基づいています。標準ベースのアルゴリズムである一時キー整合性プロトコル（TKIP）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 拡張機能のディセーブル化

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. **copyrunning-configstartup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface dot11radio {0 }**	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 802.11g/n 2.4-GHz 無線は radio 0 です。
ステップ 3	**no dot11 extension aironet**	Aironet 拡張機能をディセーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-configstartup-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。

次の作業

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 カプセル化トランスフォーメーション方式

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。

イーサネット カプセル化トランスフォーメーション方式の設定方法については、次の項を参照してください。

イーサネット カプセル化トランスフォーメーション方式の設定

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. **copyrunning-configstartup-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。

	コマンドまたはアクション	目的
ステップ 5	**copyrunning-configstartup-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

パブリック セキュア パケット フォワーディング（PSPF）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、関連資料, （249 ページ）を参照してください。

ワイヤレス デバイス上で CLI コマンドを使用して PSPF をイネーブルまたはディセーブルにするには、ブリッジグループを使用します。ブリッジグループおよびそれらを実装する手順の詳細については、次のリンクを参照してください。

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

Public Secure Packet Forwarding の設定

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. **copyrunning-configstartup-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	**copyrunning-configstartup-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。

次の作業

PSPF を無効にするには、**bridgegroup** 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スイッチ上で保護ポートを設定する必要があります。

使用しているスイッチ上で保護ポートとしてポートを定義するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **interface** *interface-id*
3. **switchportprotected**
4. **end**
5. **showinterfaces** *interface-id***switchport**
6. **copyrunning-configstartup-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	**configureterminal**	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、設定を行うスイッチ ポート インターフェイスのタイプと番号を入力します。
ステップ 3	**switchportprotected**	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	**showinterfaces** *interface-id***switchport**	入力を確認します。
ステップ 6	**copyrunning-configstartup-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。

次の作業

保護ポートを無効にするには、**noswitchportprotected** 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

ビーコン周期と DTIM

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周期の倍数で、ビーコンにどの程度の頻度で Delivery Traffic Indication Message（DTIM）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、ビーコン周期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。

ビーコン周期と DTIM の設定については、次のセクションを参照してください。

ビーコン周期と DTIM の設定

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. **copyrunning-configstartup-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	**copyrunning-configstartup-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 しきい値とリトライ回数

送信要求（RTS）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るエリアや、クライアントが互いに離れているためワイヤレス デバイスのみ検

出できてクライアント同士は検出できないエリアでは、RTS しきい値設定を低くすると便利なことがあります。設定値を 0 ～ 2347 バイトの範囲で入力します。

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

すべてのアクセス ポイントおよびブリッジに対するデフォルトの RTS しきい値は 2347、デフォルトの最大 RTS リトライ回数設定は 32 です。

RTS しきい値とリトライ回数の設定

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. **copyrunning-configstartup-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 しきい値は 0 ～ 2347 の範囲で入力します。
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	**copyrunning-configstartup-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。

次の作業

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

最大データ リトライ回数

最大データ リトライ回数設定では、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の設定

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. **configureterminal**
2. **interfacedot11radio{0}**
3. **packetretries** *value*
4. **end**
5. **copyrunning-configstartup-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	**configureterminal**	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	**interfacedot11radio{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	**packetretries** *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。 （注） 設定をデフォルトにリセットするには、**packetretries** コマンドの no 形式を使用します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-configstartup-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。

次の作業

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。

フラグメントしきい値の設定

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. **configureterminal**
2. **interfacedot11radio{0}**
3. **fragment-threshold** *value*
4. **end**
5. **copyrunning-configstartup-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	**configureterminal**	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	**interfacedot11radio{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。 （注） 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。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copyrunning-configstartup-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。

次の作業

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 チャネルでの無線アクティビティをチェックします。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。

キャリア ビジー テストの結果を再表示するには、**showdot11carrierbusy** コマンドを使用します。

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、クラス サービス（CoS）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。

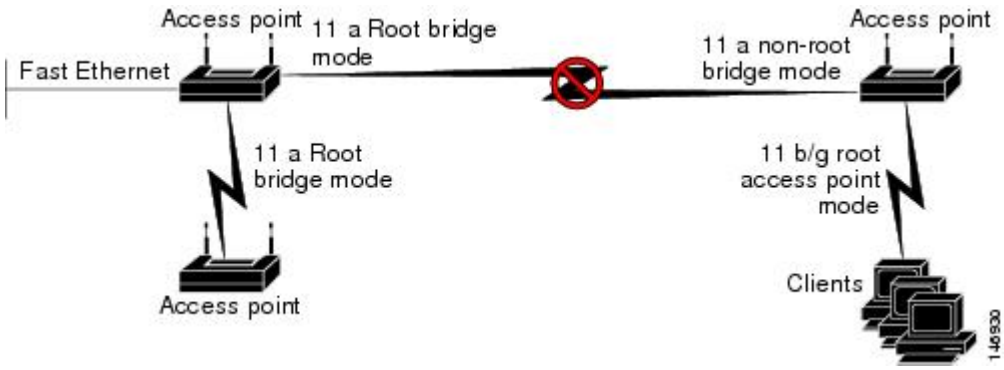
1. ブラウザを使用して、アクセス ポイントにログインします。
2. Web ブラウザ インターフェイスの左側にあるタスク メニューで [**Services**] をクリックします。

3 Services のリストが展開されたら、[**Stream**] をクリックします。
[Stream] ページが表示されます。

4 設定する無線のタブをクリックします。

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。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 *15*：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。

6 [**Apply**] をクリックします。

WLAN の設定

ここでは、Cisco 810、860、880、890 シリーズ ルータのワイヤレス LAN（WLAN）の設定タスクについて説明します。この章の内容は次のとおりです。

（注） このセクションは、C866VAE-K9、C867VAE、および C867VAE-K9 SKU には該当しません。これらの SKU は、WLAN をサポートしていません。

Web ベース インターフェイスを使用した WLAN の設定

ワイヤレス LAN（WLAN）の情報を表示して設定を行うには、Web ベースのインターフェイスを使用します。CLI ベースの WLAN インターフェイスについては、CLI ベース インターフェイスを使用した WLAN の設定，（291 ページ）を参照してください。

Web ベースの WLAN インターフェイスへの接続

Web ベースの WLAN インターフェイスに接続するには、Web ブラウザでアドレス http://10.10.10.2 を開きます。

デフォルトのクレデンシャルでログインします。

ユーザ名: **admin**

パスワード: **admin**

（注） デフォルトの WLAN クレデンシャルを使用すると、初回ログイン時、パスワードを変更するようにユーザにプロンプトが表示されます。

Web ベースのインターフェイスにアクセスするためのアドレス

Web ベースのインターフェイスにアクセスするためのアドレスを変更できます。Web ベース インターフェイスへのアクセスの設定, （284 ページ）を参照してください。

DHCP サーバ設定

デフォルトでは、DHCP サーバは設定されません。Cisco IOS CLI を使用して VLAN 1 に DHCP パラメータを設定します。

サブネット

ルータを含むLAN内のデバイスからインターフェイスに接続します。デバイスは、ルータにアクセスするために設定されたサブネット内に存在する必要があります。デフォルトのサブネット マスクは 255.255.255.0 です。

デバイス情報の表示

左側のパネルで、[**DeviceInfo**] -> [**Summary**] の順にクリックし、次のデバイス情報を表示する [Device Info] ページを開きます。

- ドライバのアップグレードまたはトラブルシューティングに必要なハードウェアおよびドライバ情報

接続統計情報の表示

左側のパネルで、[**DeviceInfo**] -> [**Statistics**] の順にクリックし、送受信したパケットの統計情報を表示する [Statistics - WLAN] ページを開きます。ページが自動的に更新されます。

Web ベース インターフェイスへのアクセスの設定

左側のパネルで、[**DeviceInfo**] -> [**NetworkInterface**] の順にクリックし、Web ベースのインターフェイスへのアクセスを設定できる [Network Interface Setup] ページを開きます。

このページには、Web ベースのインターフェイスへのアクセスに使用する IP アドレスおよびサブネット マスクが表示されます。Web ベースのインターフェイスにアクセスするための新しい IP アドレスとサブネット マスクを入力できます。デフォルトの値は次のとおりです。

IP: **10.10.10.2**

サブネットマスク： **255.255.255.248**

（注） IPv4 値のみを入力します。IPv6 はサポートされていません。

（注） IP アドレスを別のサブネットに変更するには、VLAN 1 も同じサブネット上に存在するように変更する必要があります。

（注） Webベースのインターフェイスは、同じサブネット内のデバイスからのみアクセスできます。

基本的なワイヤレス設定

左側のパネルで、[**Wireless**] -> [**Basic**] の順にクリックし、ワイヤレス LAN（WLAN）のオプションを設定できる [Wireless - Basic] ページを開きます。

Main SSID

[Wireless - Basic] ページの上部にある以下のオプションは、メイン SSID（Service Set Identification）に適用されます。

- Enable Wireless：WLAN 機能を有効/無効にします。
- Hide Access Point：SSID の非表示は簡単なセキュリティ対策になり、許可されていないユーザによるネットワーク アクセスの防止に役立ちます。この機能が有効な場合、WLAN アクセス ポイントの SSID はブロードキャストされないため、ワイヤレス スヌーピングがさらに難しくなります。
- Clients Isolation：特定の SSID に接続されているワイヤレス クライアントが同じ SSID に接続されている他のワイヤレス クライアントと通信しないようにします。
- Disable WMM Advertise：WMM（WiFi Multimedia）機能を無効にします。WMM 機能は、メディア トラフィックに優先順位を付けてメディア伝送を改善します。
- Enable Wireless Multicast Forwarding（WMF）：Wireless Multicast Forwarding（WMF）機能を有効にします。

- SSID：WLAN のアクセスに使用するメイン SSID。同じ SSID を使用して WLAN に接続されているデバイスは、同じドメイン内で動作します。メイン SSID を無効にする唯一の方法は、WLAN を完全に無効にすることです。
- BSSID：メイン SSID の MAC アドレス。有効な SSID ごとに個別の BSSID があります。
- Max Clients：メイン SSID に接続できるクライアントの最大数を設定します。デフォルト値：16、推奨最大値：16、理論上の最大値：128

ゲスト SSID

[Wireless - Basic] ページの下部にある表は、ゲスト デバイスを WLAN に接続するためのゲスト SSID を示しています。ゲスト SSID ごとに、メイン SSID と同様のオプションを設定できます。

デフォルトの SSID 値

デフォルトの SSID 値は次のとおりです。

- メイン SSID：Cisco860
- ゲスト SSID 1：Cisco860_Guest1
- ゲスト SSID 2：Cisco860_Guest2
- ゲスト SSID 3：Cisco860_Guest3

（注） デフォルトでは、メイン SSID が有効、ゲスト SSID は無効です。

セキュリティの設定

左側のパネルで、[**Wireless**] -> [**Security**] の順にクリックし、各アクセス ポイントのセキュリティ設定を表示する [Wireless - Security] ページを開きます。

以下の手順を実行し、アクセス ポイントにセキュリティ設定を行います。

1. [Select SSID] ドロップダウン リストで、設定する SSID を選択します。
2. ドロップダウン リストを使用して、SSID のネットワーク認証オプションを選択します。認証の種類を選択すると、認証の種類に固有の追加オプションが表示されます。

（注） デフォルトで、ネットワーク認証はオープン、WEP 暗号化は各 SSID に対して無効です。

3. [**Apply/Save**] をクリックします。

MAC フィルタリングの設定

左側のパネルで、[**Wireless**] -> [**MACFilter**] の順にクリックし、デバイス MAC アドレスに従って特定の SSID にアクセスを制限できる [Wireless - MAC Filter] ページを開きます。

SSID ごとに MAC アドレスを指定し、MAC アドレスを許可、または拒否できます。デフォルトでは、すべての SSID に対して MAC 制限機能は無効です。

SSID に MAC フィルタリングを設定するには、次の手順を実行します。

1. [Select SSID] ドロップダウン リストで、設定する SSID を選択します。
2. リストに MAC アドレスを追加するには、[**Add**] をクリックしてアドレスを入力します。
3. MACアドレスをリストから削除するには、アドレスの[Remove]チェック ボックスを選択し、[**Remove**] をクリックします。
4. 以下のオプションから、MAC 制限モードを選択します。
   - Disabled：機能は無効です。
   - Allow：指定された MAC アドレスを持つデバイスに接続を許可します。
   - Deny：指定された MAC アドレスを持つデバイスの接続を拒否します。

高度なワイヤレス設定

左側のパネルで、[**Wireless**] > [**Advanced**] の順にクリックし、表 34：高度な WLAN, （286 ページ）で説明されている高度なワイヤレス LAN（WLAN）機能を設定できる [Wireless - Advanced] ページを開きます。

表 *34*：高度な *WLAN*

オプション	説明
帯域	周波数帯域。これは 2.4 GHz にプリセットされています。
チャネル	無線チャネル。デフォルトではチャネルを自動的に設定しますが、特定のチャネルを選択することもできます。チャネルオプションは地理的地域によって異なります。
Auto Channel Timer (min)	（チャネルが [Auto] に設定されている場合に有効） 最善のチャネルを判断するために再度スキャニングを開始する前に待機する分数。 範囲：1 ～ 35791394 分
802.11n/EWC	802.11n サポートを有効/無効にします。
802.11n Rate	（802.11n/EWC は [Auto] に設定する必要があります） 802.11n のレートを設定します。

オプション	説明
802.11n Protection	（802.11n/EWC は [Auto] に設定する必要があります） RTS/CTS 保護を設定します。
Support 802.11n Client Only	（802.11n/EWC は [Auto] に設定する必要があります） 802.11n 以外はサポートを無効にします。
RIFS Advertisement	（802.11n/EWC は [Auto] に設定する必要があります） RIFS（Reduced Inter-Frame Space）アドバタイズメントを有効/無効にします。
RX Chain Power Save	（802.11n/EWC は [Auto] に設定する必要があります） 省電力モードを有効/無効にします。
RX Chain Power Save Quiet Time	（802.11n/EWC は [Auto] に設定する必要があり、[RX Chain Power Save] は有効に設定する必要があります） 省電力モードに移行する前に待機する時間間隔（秒）。 範囲は 0 ～ 2147483647 秒です。
RX Chain Power Save PPS	（802.11n/EWC は [Auto] に設定する必要があり、[RX Chain Power Save] は有効に設定する必要があります） PPS（1秒あたりのパケット数）しきい値。PPS がしきい値を下回ると、ルータは [RX Chain Power Save Quiet Time] フィールドに設定されている秒数後に省電力モードになります。 範囲：0 ～ 2147483647（1 秒あたりのパケット数）
54g Rate	（802.11n/EWC は [Disabled] に設定する必要があり、802.11n Rate は [Use 54g Rate] に設定する必要があります） 54g レートを設定します。

オプション	説明
Multicast Rate	マルチキャスト パケットの送信/受信レート。 （注） 802.11n/EWC が [Disabled] で、[54g Mode] が [802.11b Only] に設定されている場合、オプションは異なります。
Basic Rate	ワイヤレスクライアントがサポートするデータレート。
Fragmentation Threshold	超過するとデータが断片化される最大パケットサイズ（バイト）。 範囲：256 ～ 2346 バイト
RTS Threshold	CTS 保護メカニズムをトリガーする RTS のしきい値。アクセスポイントがしきい値より大きいパケットを送信する場合、これによってCTS保護モードがトリガーされます。 範囲：0 ～ 2347 バイト
DTIM Interval	Delivery Traffic Indication Message（DTIM）間隔は、ビーコンフレームに含める情報で、次に予定されているバッファ データが AP にあることをクライアントに知らせます。間隔はビーコンの数で指定します。たとえば、DTIM 間隔を 2 に設定すると、クライアントは 2 ビーコンごとにウェイク アップし、AP 上にバッファ データがないかチェックします。 範囲：1 ～ 255 ビーコン
ビーコン間隔（Beacon Interval）	ビーコン送信間の時間の長さ。 範囲：1 ～ 65535 ミリ秒
Global Max Clients	APに接続できるクライアントの最大数の上限。各 SSID の「最大クライアント」設定で、この制限を超えることはできません。 範囲：1 ～ 128、デフォルト値：16、推奨最大値：16、理論上の最大値：128
送信電力	送信電力のレベルを設定します。
WMM（Wi-Fi Multimedia）	WMM 機能、802.11 の Quality of Service（QoS）機能を有効/無効にします。

オプション	説明
WMM No Acknowledgement	（WMM（Wi-Fi マルチメディア）は [Enabled] または [Auto] に設定する必要があります） WMM No Acknowledgement を有効/無効にします。
WMM APSD	（WMM（Wi-Fi マルチメディア）は [Enabled] または [Auto] に設定する必要があります） WMM Automatic Power Save Delivery 機能を有効/無効にします。 （注） WMM が [Auto] モードの場合、WMM APSD は [Enabled] に設定し、クライアントが省電力モードを使用できるようにする必要があります。WMM が「有効」モードの場合、クライアントは WMM APSD が「有効」または「無効」かどうかに関係なく、省電力モードを使用できます。
54g Mode	（802.11n/EWC は [Disabled] に設定する必要があります） 54g モードを設定します。
54g Protection	（802.11n/EWC は [Disabled] に設定する必要があります） このフィールドを [Auto] に設定すると、RTS/CTS 保護メカニズムが有効になります。
Preamble Type	（802.11n/EWC は [Disabled] に設定する必要があります）54g Mode は [54g Auto] または [802.11b only] のいずれかに設定する必要があります。 AP-to-WLAN クライアント通信に使用する CRC（巡回冗長検査）ブロックの長さを指定します。

ステーション情報

左側のパネルで、**[Wireless] -> [StationInfo]** の順にクリックし、ワイヤレス LAN（WLAN）に対して認証されているクライアント、および各クライアントの状態を表示する [Wireless - Authenticated Stations] ページを開きます。

Web ベースのインターフェイスに接続するパスワードの設定

左側のパネルで、[**Management**] をクリックし、管理者パスワードを設定できる [Access Control - Passwords] ページを開きます。

ユーザ名は、**admin** でなければなりません。パスワードは、このページにある手順に従って変更できます。デフォルトのパスワードは **admin** です。

（注） 管理者アカウントには、ルータ設定に関して無制限の権限があります。

（注） WLAN 設定をデフォルトに戻すには、Cisco IOS CLI を使用して、フラッシュ メモリから wlconfig.txt ファイルを削除します。

ワイヤレス LAN の構成をファイルに保存する

左側のパネルで、[**Configuration**] -> [**Backup**] の順にクリックし、ワイヤレスの構成をまとめた設定ファイルを保存します。ファイルは、GUI のアクセスに使用しているワークステーションにローカルに保存されます。保存されている設定をローカル ファイルからロードする方法については、無線 LAN の設定ファイルの読み込み, （290 ページ）を参照してください。

無線 LAN の設定ファイルの読み込み

左側のパネルで、[**Configuration**] -> [**Update**] の順にクリックし、GUI へのアクセスに使用するワークステーションから、無線 LAN を構成するための設定ファイルを読み込みます。

注意 設定ファイルを読み込むとルータが再起動されるため、現在アクティブな接続が中断されます。

設定ファイルをローカルに保存する方法については、ワイヤレス LAN の構成をファイルに保存する, （290 ページ）を参照してください。

（注） 設定ファイルは、複数の異なるルータに特定の設定を読み込むのに使用できます。

デフォルト設定の復元

左側のパネルで、[**Configuration**] -> [**RestoreDefault**] の順にクリックし、ワイヤレス LAN 設定をデフォルトに復元します。

注意 デフォルト設定を復元するとルータが再起動されるため、現在アクティブな接続が中断されます。

CLI ベース インターフェイスを使用した WLAN の設定

ワイヤレス LAN（WLAN）の情報を表示して設定を行うには、CLI ベースのインターフェイスを使用します。Web ベースの WLAN インターフェイスについては、Web ベース インターフェイスを使用した WLAN の設定, （282 ページ）を参照してください。

次の項を参照してください。

WLAN CLI インターフェイス

WLAN CLI インターフェイスは、IOS の CLI インターフェイスに似ています。

CLI インターフェイスを開始すると、次のようにプロンプトが表示されます。

ap#

Cisco IOS と同様に、プロンプトはコマンドモードを示します。たとえば、**configureterminal** コマンド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と、プロンプトは以下に変わります。

ap(config)#

特定のモードを終了するには、**exit** コマンドを使用します。

次に例を示します。

ap(config)# **exit**

ap#

WLAN CLI のコマンド情報の表示

疑問符（**?**）を入力すると、使用可能なコマンド オプションに関する情報が表示されます。この機能では、コマンドと関連するコマンド オプションに関する情報に簡単にアクセスできます。

例：WLAN CLI のコマンド情報の表示

インターフェイス コンフィギュレーション モードで、**?** をプロンプトで入力すると、このモードで使用できるコマンドが表示されます。

```
ap(config-if)# ?
        exit                    Exit from config-if mode
        ip                      Interface Internet Protocol config commands
        no                      Negate a command or set its defaults
        shutdown                Shutdown the interface
```

以下に示すように SSID コンフィギュレーション モードで、**encryptionmodewep?** を入力すると、**encryptionmodewep** コマンドで WEP 暗号化モードを設定する際に選択できるオプションが表示されます。

```
ap(config-ssid)# encryption mode wep ?
        current-key              Network Key to use
        encryption-strength      Encryption strength
        key                      Set encryption keys
        <cr>
```

このコマンドには、3 つの引数（*current-key*、*encryption-strength*、*key*）を入力できます。<cr> オプションは、オプションを追加しなくても単独で **encryptionmodewep** を使えることを示します。この例で、引数を追加せずにコマンドを入力すると、WEP 暗号化が有効になります。

WLAN CLI インターフェイスへの接続

WLAN CLI に接続するには、次の手順を実行します。

1. Cisco IOS コマンド ラインから目的の IP アドレスを指定して、ループバック インターフェイスを作成します。Cisco IOS でのループバック インターフェイスの作成については、「*Cisco IOS Master Commands List*」（http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html）を参照してください。
2. ループバック インターフェイスに指定されている IP アドレスとポート 2002 に Telnet で接続します。
3. プロンプトが表示されたらログインします。
   ルータに、WLAN CLI インターフェイス プロンプトが表示されます。

（注） デフォルトのログイン クレデンシャルは、ユーザ名：**admin** パスワード：**admin** です。初回ログイン時に、デフォルトのパスワードを変更するように指示されます。

例：ループバック インターフェイスの設定

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface loopback 0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# end
```

例：ループバック インターフェイス経由の Telnet による WLAN CLI へのアクセス

```
Router# telnet 1.1.1.1 2002
Trying 1.1.1.1, 2002 ... Open
Connecting to AP console, enter Ctrl-^ followed by x,
then "disconnect" to return to router prompt
ap#
```

WLAN CLI インターフェイスの終了

WLAN CLI を終了し、Cisco IOS CLI プロンプトに戻るには、**CTRL-SHIFT-6**、次に **x**、さらに [**disconnect**] を押します。

Web ベース インターフェイスの IP アドレスの設定

デフォルトでは、Web ベースの WLAN インターフェイスへのアクセスに IP アドレス 10.10.10.2 が使用されます。

Web ベースのインターフェイスへのアクセスに使われるブリッジ インターフェイスの IP アドレスを変更するには、以下の手順を実行します。

手順の概要

1. **configureterminal**
2. **interfaceBVI1**
3. **ipaddress** *IP-address subnet-mask*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configureterminal**
	
	例：
	`ap# configure terminal`
	
	例：
	`ap(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**interfaceBVI1** 例： `ap(config)# interface BVI 1`	インターフェイス番号
ステップ 3	**ipaddress** *IP-address subnet-mask* 例： `ap(config-if)# ip address 10.10.10.2 255.255.255.248`	新しい IP アドレスとサブネット マスクを設定します。 （注） IPv4 アドレスのみを使用します。 ヒント 設定した IP アドレスを表示するには、**showinterfacesBVI1** コマンドを使用します（BVI 1 インターフェイスの詳細の表示，（329 ページ）を参照）。

WLAN のイネーブル化およびディセーブル化

デフォルトで、WLAN 機能は有効です。

WLAN を有効、または無効にするには、グローバル コンフィギュレーション モードで次の手順を実行します。

WLAN を無効にするには、**shutdown**、有効にするには **noshutdown** を使います。

手順の概要

1. **interfaceDot11Radio0**
2. **[no]shutdown**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)# interface Dot11Radio 0`	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]shutdown** 例： `ap(config-if)# no shutdown`	**shutdown**：WLAN をディセーブルにします。 **noshutdown**：WLAN をイネーブルにします。

メイン SSID の設定

メイン SSID の名前を変更するには、以下の手順を実行します。

手順の概要

1. **configureterminal**
2. **dot11ssid** *SSID-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	**configureterminal**
	例：
	`ap# configure terminal`
	例：
	`ap(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**dot11ssid** *SSID-name* 例： `ap(config)# dot11 ssid mainssid`	*SSID-name*：メイン SSID。SSID は最大 32 文字まで使用できます。 この例での新しい SSID は mainssid です。

ゲスト SSID の設定

ゲスト SSID の名前を変更するには、以下の手順を実行します。

手順の概要

1. **configureterminal**
2. **dot11guest-ssid** *guest-SSID-number SSID-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	**configureterminal**
	例：
	`ap# configure terminal`
	例：
	`ap(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**dot11guest-ssid** *guest-SSID-number SSID-name* 例： `ap(config)# dot11 guest-ssid 1 guest1`	*guest-SSID-number*：設定するゲスト SSID を 1、2、または 3 で指定します。 *SSID-name*：新しい SSID。SSID は最大 32 文字まで使用できます。

	コマンドまたはアクション	目的
		この例では、1 番のゲスト SSID に、新しい SSID として **guest1** を指定しています。

ゲスト SSID の有効化と無効化

ゲスト SSID を有効、または無効にするには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） メイン SSID は無効にできません。ゲスト SSID は有効/無効にできます。デフォルトでは、ゲスト SSID は無効です。

手順の概要

1. **interfaceDot11Radio0**
2. **[no]guest-ssid** *guest-SSID-number SSID-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	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	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]guest-ssid** *guest-SSID-number SSID-name* 例： `ap(config-if)#` **guest-ssid 1 guestssid1**	*guest-SSID-number* および *SSID-name* で指定したゲスト SSID を有効にします。 • *guest-SSID-number*：設定するゲスト SSID を 1、2、または 3 で指定します。 • *SSID-name*：ゲスト SSID の名前。間違った SSID を入力すると、エラー メッセージが表示されます。 （注） このコマンドの **no** 形式は、指定したゲスト SSID を無効にします。

アクセス ポイントの非表示

SSID を非表示、または表示するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） SSID（アクセス ポイント）を非表示にする方法は簡単なセキュリティ対策になり、許可されていないユーザによるネットワーク アクセスの防止に役立ちます。SSID を非表示にすると、SSID はブロードキャストされないため、ワイヤレス スヌーピングがさらに難しくなります。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]hide-ap**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**[no]hide-ap** 例： `ap(config-ssid)#` **hide-ap**	前の手順で指定した SSID を非表示にします。 （注） このコマンドの **no** 形式は、指定した SSID を表示します。

クライアント アイソレーションの有効化と無効化

特定の SSID に対してクライアント アイソレーションを有効または無効にするには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） クライアントアイソレーションは、特定のSSIDに接続されているワイヤレスクライアントが同じ SSID に接続されている他のワイヤレス クライアントと通信しないようにします。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]isolate-clients**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**[no]isolate-clients** 例： `ap(config-ssid)#` **isolate-clients**	前の手順で指定した SSID にクライアント アイソレーションを有効にします。 このコマンドの **no** 形式は、指定した SSID に対してクライアント アイソレーションを無効にします。

WMM アドバタイズの有効化と無効化

特定のSSIDに対してWiFi Multimedia（WMM）アドバタイズを有効、または無効にするには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） WiFi Multimedia（WMM）アドバタイズ機能は、メディア トラフィックに優先順位を付けてメディア伝送を向上させます。WMM アドバタイズは、デフォルトで有効です。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]disable-wmm**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**[no]disable-wmm** 例： `ap(config-ssid)#` **disable-wmm**	前の手順で指定した SSID に対して WMM アドバタイズ機能を無効にします。 このコマンドの **no** 形式は、指定した SSID に対して WMM アドバタイズ機能を無効にします。 （注） WMM アドバタイズは、デフォルトで有効です。

Wireless Multicast Forwarding（WMF）の有効化と無効化

特定の SSID に対して Wireless Multicast Forwarding（WMF）を有効、または無効にするには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） WMF 機能は、マルチキャスト トラフィックのパフォーマンスを向上させます。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]wmf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**[no]wmf** 例： `ap(config-ssid)#` **wmf**	前の手順で指定した SSID に WMF 機能を有効にします。 このコマンドの **no** 形式は、指定した SSID に対して WMF 機能を無効にします。

クライアントのグローバル最大数の設定

AP に接続できるクライアントのグローバル最大数を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **global-max-clients** *number-of-clients*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `ap#` **configure terminal** 例： `ap(config)#`	コンフィギュレーション モードに入ります。 （注） 設定タスクを完了してからコンフィギュレーション モードを終了するには、**exit** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 2	**global-max-clients** *number-of-clients* 例： `ap(config)#` **global-max-clients 32**	AP に接続できるクライアントの最大数を設定します。 *number-of-lines* の範囲：1 ～ 128 クライアント

SSID のクライアントの最大数の設定

クライアントの最大数を設定するには、グローバルコンフィギュレーションモードで次の手順を実行します。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **max-associations** *number-of-clients*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**max-associations** *number-of-clients* 例： `ap(config-ssid)#` **max-associations 24**	前の手順で指定した SSID のクライアント最大数を設定します。 *number-of-clients*：範囲は 1 ～ 128 で、デフォルト値は 16 です。

認証オプションの設定

特定の SSID に対して認証オプションを設定するには、**authentication** コマンドを使用します。デフォルトでは、ネットワーク認証はオープンです。

認証オプションを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **authentication***authentication-options*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**authentication***authentication-options* 例： `ap(config-ssid)#` **authentication open**	前の手順で指定した SSID に認証オプションを設定します。表 35：認証コマンドのオプション，（302 ページ）で、**authentication** コマンドのオプションについて説明します。 デフォルトの認証オプションは、**open** です。

次の作業

表 35：認証コマンドのオプション，（302 ページ） で、**authentication** コマンドのオプションについて説明します。

表 *35*：認証コマンドのオプション

オプション	構文	説明
オープン認証	**open**	オープン認証を設定します。

オプション	構文	説明
共有認証	**shared** `ap(config-ssid)#` **authentication shared**	共有認証を設定します。
802.1x オプション		
認証サーバ ポート	**802.1xauth-port** *port-number* `ap(config-ssid)#` **authentication 802.1x auth-port 2000**	RADIUS 認証サーバに UDP ポートを定義します。 範囲：0 ～ 65535 デフォルト：1812
RADIUS キー	**802.1xkey** *encryption-key* `ap(config-ssid)#` **authentication 802.1x key ABC123ABC1**	サーバごとの暗号キーを定義します。 暗号化されていない（クリアテキスト）形式でサーバ キーを入力します。
RADIUS サーバ アドレス	**802.1xserver** *server-IP-address* `ap(config-ssid)#` **authentication 802.1x server 10.1.1.1**	RADIUS サーバを指定します。
WPA 認証		
認証サーバ ポート	**WPAauth-port** *port-number* `ap(config-ssid)#` **authentication WPA auth-port 2000**	RADIUS 認証サーバに UDP ポートを定義します。 範囲：0 ～ 65535 デフォルト：1812
RADIUS キー	**WPAkey** *encryption-key* `ap(config-ssid)#` **authentication WPA key ABC123ABC1**	サーバごとの暗号キーを定義します。 暗号化されていない（クリアテキスト）形式でサーバ キーを入力します。
WPA グループ キー再生成間隔	**WPArekey-interval***seconds* `ap(config-ssid)#` **authentication WPA rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。
RADIUS サーバ アドレス	**WPAserver** *server-IP-address* `ap(config-ssid)#` **authentication WPA server 10.1.1.1**	RADIUS サーバを指定します。
WPA-PSK 認証		

オプション	構文	説明
WPA/WAPI passphrase	**WPA-PSKpassphrase** *password* `ap(config-ssid)#` **authentication WPA-PSK passphrase MyPaSsWoRd**	WPA-PSK のパスフレーズ。 クリアテキスト/非暗号化 WPA パスフレーズを入力します。 範囲：8 ~ 63 の ASCII 文字または 64 桁の 16 進数
WPA グループ キー再生成間隔	**WPA-PSKrekey-interval** *seconds* `ap(config-ssid)#` **authentication WPA-PSK rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。
WPA2 認証		
認証サーバ ポート	**WPA2auth-port** *port-number* `ap(config-ssid)#` **authentication WPA2 auth-port 2000**	RADIUS 認証サーバに UDP ポートを定義します。 範囲：0 ～ 65535 デフォルト：1812
RADIUS キー	**WPA2key** *encryption-key* `ap(config-ssid)#` **authentication WPA2 key ABC123ABC1**	サーバごとの暗号キーを定義します。 暗号化されていない（クリアテキスト）形式でサーバキーを入力します。
WPA2 事前認証	**WPA2preauth** `ap(config-ssid)#` **authentication WPA2 preauth** `ap(config-ssid)#` **no authentication WPA2 preauth**	WPA2 事前認証を有効にします。 このコマンドの**no**形式を使用すると、事前認証が無効になります。
ネットワーク再認証間隔	**WPA2reauth-interval***seconds* `ap(config-ssid)#` **authentication WPA2 reauth-interval 604800**	WPA2 再認証の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、再認証間隔を 1 週間（604800 秒）に設定します。

オプション	構文	説明
WPA グループ キー再生成間隔	**WPA2rekey-interval** *seconds* `ap(config-ssid)#` **authentication WPA2 rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。
RADIUS サーバ アドレス	**WPA2server** *server-IP-address* `ap(config-ssid)#` **authentication WPA2 server 10.1.1.1**	RADIUS サーバを指定します。
WPA2-PSK 認証		
WPA/WAPI パスフレーズ	**WPA2-PSKpassphrase** *password* `ap(config-ssid)#` **authentication WPA2-PSK passphrase MyPaSsWoRd**	WPA2-PSK のパスフレーズ。 クリアテキスト/非暗号化 WPA パスフレーズを入力します。 範囲：8 ~ 63 の ASCII 文字または 64 桁の 16 進数
WPA-PSK グループ キー再生成間隔	**WPA2-PSKrekey-interval***seconds* `ap(config-ssid)#` **authentication WPA2-PSK rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。
Mixed WPA2/WPA Authentication		
認証サーバ ポート	**Mixed-WPA2-WPAauth-port** *port-number* `ap(config-ssid)#` **authentication Mixed-WPA2-WPA auth-port 2000**	RADIUS 認証サーバに UDP ポートを定義します。 範囲：0 ～ 65535 デフォルト：1812
RADIUS キー	**Mixed-WPA2-WPAkey** *encryption-key* ap(config-ssid)# **authentication Mixed-WPA2-WPAkey ABC123ABC1**	サーバごとの暗号キーを定義します。 暗号化されていない（クリアテキスト）形式でサーバキーを入力します。

オプション	構文	説明
WPA2 事前認証	**Mixed-WPA2-WPApreauth** `ap(config-ssid)#` **authentication Mixed-WPA2-WPA preauth** `ap(config-ssid)#` **no authentication Mixed-WPA2-WPA preauth**	WPA2 事前認証を有効にします。 このコマンドの**no**形式を使用すると、事前認証が無効になります。
ネットワーク再認証	**Mixed-WPA2-WPAreauth-interval** `ap(config-ssid)#` **authentication Mixed-WPA2-WPA reauth-interval 604800**	WPA2 再認証の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、再認証間隔を 1 週間（604800 秒）に設定します。
WPA グループ キー再生成間隔	**Mixed-WPA2-WPArekey-interval** *seconds* `ap(config-ssid)#` **authentication Mixed-WPA2-WPA rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。
RADIUS サーバ アドレス	**Mixed-WPA2-WPAserver***server-IP-address* `ap(config-ssid)#` **authentication Mixed-WPA2-WPA server 10.1.1.1**	RADIUS サーバを指定します。
Mixed WPA2/WPA-PSK Authentication		
パスフレーズ	**Mixed-WPA2-WPA-PSKpassphrase** *password* `ap(config-ssid)#` **authentication Mixed-WPA2-WPA-PSK passphrase MyPaSsWoRd**	WiFi 保護アクセスの事前共有パスフレーズ。 クリアな WPA パスフレーズを入力します。 範囲：8 ~ 63 の ASCII 文字または 64 桁の 16 進数
WPA グループ キー再生成間隔	**WPA2-PSKrekey-interval** *seconds* `ap(config-ssid)#` **authentication Mixed-WPA2-WPA-PSK rekey-interval 604800**	認証キー再生成の間隔を秒数で定義します。 範囲：0 ～ 2147483647（秒） この例は、キー再生成間隔を 1 週間（604800 秒）に設定します。

暗号化オプションの設定

特定の SSID に暗号化オプションを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **encryptionmode***encryption-options*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**encryptionmode***encryption-options* 例： `ap(config-ssid)#` **encryption mode wep**	前の手順で指定した SSID に暗号化オプションを設定します。表 36：暗号化コマンドのオプション，（307 ページ） で、**encryptionmode** コマンドのオプションについて説明します。

次の作業

表 36：暗号化コマンドのオプション，（307 ページ） で、**encryptionmode** コマンドのオプションについて説明します。

表 *36*：暗号化コマンドのオプション

オプション	Syntax	説明
WEP 暗号化オプション		

オプション	Syntax	説明
Enable/Disable WEP encryption	**[no]encryptionmodewep** `ap(config-ssid)#` **encryption mode wep** `ap(config-ssid)#` **no encryption mode wep**	WEP 暗号化をイネーブルにします。このコマンドの**no**形式を使用すると、WEP 暗号化がディセーブルになります。 （注） WEP 暗号化のデフォルト設定は、選択された認証オプションによって異なります。Open authentication：デフォルトでは無効です。Shared：デフォルトで有効です。無効にできません。802.1 x：-デフォルトで有効です。無効にできません。WPA、WPA-PSK、WPA2、WPA2-PSK、Mixed WPA2/WPA、Mixed WPA2/WPA-PSK：デフォルトでは無効です。有効にできません。
Encryption strength	**wepencryption-strength[64bit|128bit]** `ap(config-ssid)#` **encryption mode wep encryption-strength 64bit**	WEP 暗号化の強度を構成します。 **64bit**：64 ビット キーを指定します。 **128bit**：128 ビット キーを指定します。
Current network key	**wepcurrent-key** *key-number* `ap(config-ssid)#` **encryption mode wep current-key 1**	4 つの異なるネットワーク キーを設定できます。このコマンドは、現在使用するキーを特定します。 *key-number*の範囲：1 ~ 4
Network key	**wepkey** *key-number key* `ap(config-ssid)#` **encryption mode wep key 1 54321**	ネットワーク キーを設定します。 *key-number*の範囲：1 ~ 4 *key*： • 64 ビット キーの場合： 5 個の ASCII 文字または 10 桁の 16 進数 • 128 ビット キーの場合： 13 個の ASCII 文字または 26 桁の 16 進数

オプション	Syntax	説明
WPA/WAPI 暗号化オプション		
AES	**aes** `ap(config-ssid)#` **encryption mode aes**	暗号化モードを AES に設定します。 （注） AES は WPA、WPA-PSK、WPA2、WPA2-PSK、Mixed WPA2/WPA、Mixed WPA2/WPA-PSK でのみサポートされています。
TKIP+AES	**tkip+aes** `ap(config-ssid)#` **encryption mode tkip+aes**	暗号化モードを TKIP+AES に設定します。 （注） TKIP + AES は WPA、WPA-PSK、WPA2、WPA2-PSK、Mixed WPA2/WPA、Mixed WPA2/WPA-PSK でのみサポートされています。

MACアドレス フィルタ アクセス リストの設定

MAC アドレスをアクセスリストに追加するか、または MAC アドレスをアクセスリストから削除するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]access-list** *MAC-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	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名

	コマンドまたはアクション	目的
ステップ 2	**[no]access-list** *MAC-address* 例： `ap(config-ssid)#` **access-list AB:12:CD:34:EF:56** 例： `ap(config-ssid)#` **no access-list AB:12:CD:34:EF:56**	前の手順で指定した SSID のアクセス リストに MAC アドレスを追加します。 *MAC-address*：HH:HH:HH:HH:HH:HH の形式の16 進数 （注） このコマンドの **no** 形式は、アクセス リストから MAC アドレスを削除します。

MAC アドレス フィルタ モードの設定

MAC アドレス アクセス リスト モードを選択するには、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. **dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name*
2. **[no]mac-filter-mode[allow|deny]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot11{ssid|guest-ssid}**[*guest-SSID-number*]*SSID-name* 例： `ap(config)#` **dot11 guest-ssid 1 guestssid1**	特定の SSID に対して、SSID コンフィギュレーション モードを開始します。ap(config-ssid) プロンプトは、SSID コンフィギュレーション モードを示します。 • **ssid**：メイン SSID • **guest-ssid**：ゲスト SSID • *guest-SSID-number*：ゲスト SSID 番号。これは、**guest-ssid** オプションでのみ使用します。 • *SSID-name*：SSID 名
ステップ 2	**[no]mac-filter-mode[allow|deny]** 例： `ap(config-ssid)#` **mac-filter-mode allow**	MAC アドレス フィルタ機能のモードを設定します。 • **allow**：アクセス リスト上の MAC アドレスに接続を許可する

	コマンドまたはアクション	目的
	例： 	• **deny**：アクセス リスト上の MAC アドレスの接続を拒否する

無線チャネルの設定

チャネル オプションを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **channel{***channel-number***|least-congested}[timer** *minutes-before-next-scan***]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**channel{***channel-number***|least-congested}[timer** *minutes-before-next-scan***]** 例： `ap(config-if)#` **channel least-congested timer 60**	特定の無線チャネルを手動で設定します。または自動スキャンを選択し、自動スキャニング タイマーを設定します。 • *channel-number*：特定のチャネルを設定します。チャネル番号の範囲は米国モデルで 1 ~ 11、ヨーロッパ モデルで 1 ～ 13 です。 • **least-congested**：least congested チャネルに自動スキャニングを設定します。**least-congested** オプションを使用して、最善のチャネルのスキャニングを再度始めるまでに待機する分数を指定します。 • *minutes-before-next-scan*：自動スキャニングのタイマーを設定します。範囲は 1 ～ 35791394 です。

802.11n オプションの設定

802.11n オプションを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **[no]dot11n**
3. **dot11nrate**
4. **[no]dot11nprotection**
5. **[no]dot11nn-client-only**
6. **[no]dot11nrifs**
7. **[no]dot11n[rx-pwr-save|rx-pwr-savequiet-time** *seconds*|**pps** *pps-value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**[no]dot11n**	802.11n 無線オプションを設定します。
ステップ 3	**dot11nrate**	C802.11n のレートを設定します。 • レート範囲：0 ～ 15。表 37：802.11n のレート オプション，（313 ページ） に、レート値ごとの 802.11n のレートについて説明します。 • **54g**：54g レートを使用します。 • **auto**：自動的にレートを選択します。
ステップ 4	**[no]dot11nprotection**	802.11n 保護を有効にします。
ステップ 5	**[no]dot11nn-client-only**	802.11n クライアント専用モードを有効にします。これは 802.11n を使用するクライアントに WLAN を制限します。

	コマンドまたはアクション	目的
		（注） 802.11n クライアント専用オプションが有効な場合、クライアントは WEP セキュリティ設定を使用して SSID に接続することはできません。クライアントが SSID に接続できるようにするには、SSID セキュリティ設定を変更して WEP が設定されないようにします。または、WEP 以外のセキュリティ設定を使用する方法でも、クライアントは SSID に接続できます。
ステップ 6	**[no]dot11nrifs**	RIFS（Reduced Inter-Frame Space）アドバタイズメントを有効にします。
ステップ 7	**[no]dot11n[rx-pwr-save|rx-pwr-savequiet-time** *seconds*|**pps** *pps-value*]	RX Chain Power Save を有効にします。 • *seconds*：RX Chain Power Save 待機時間（省電力モードになる前に待機する時間間隔）を設定します。範囲は 0 ～ 2147483647 です。 • *pps-value*：秒あたりの RX Chain Power Save パケット（PPS）のしきい値を設定します。範囲は毎秒 0 ～ 2147483647 パケットです。

次の作業

表 37：802.11n のレート オプション，（313 ページ） に、802.11n のレート オプションについて説明します。これは、**dot11n** *rate* コマンドで指定します。

表 *37*：*802.11n* のレート オプション

値	レート
0	MCS インデックス 0、6.5 Mbps
1	MCS インデックス 1、13 Mbps
2	MCS インデックス 2、19.5 Mbps
3	MCS インデックス 3、26 Mbps
4	MCS インデックス 4、39 Mbps
5	MCS インデックス 5、52 Mbps
6	MCS インデックス 6、58.5 Mbps

値	レート
7	MCS インデックス 7、65 Mbps
8	MCS インデックス 8、13 Mbps
9	MCS インデックス 9、26 Mbps
10	MCS インデックス 10、39 Mbps
11	MCS インデックス 11、52 Mbps
12	MCS インデックス 12、78 Mbps
13	MCS インデックス 13、104 Mbps
14	MCS インデックス 14、117 Mbps
15	MCS インデックス 15、130 Mbps

54g モードの設定

54g モードを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **54g-mode[auto|dot11b-only|lrs|performance]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)# interface Dot11Radio 0`	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**54g-mode[auto|dot11b-only|lrs|performance]** 例： `ap(config-if)# 54g-mode auto`	54g モードを設定します。 • **auto**：54g auto モード。802.11b、802.11g、および 54g クライアントを受け入れます。このオプションには、最も広範囲な互換性があります。

	コマンドまたはアクション	目的
		• **dot11b-only**：802.11b クライアントのみを受け入れます。 • **lrs**：54g LRS（Limited Rate Support）。従来の 802.11b クライアントをサポートするために用意されています。 • **performance**：54g Performance モード。54g クライアントのみを受け入れ、54g 認証装置で最速のパフォーマンスを提供します。

54g プリアンブル タイプの設定

54g プリアンブル 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 モードで以下の手順を実行します。

（注） プリアンブル タイプは、802.11n が無効（**nodot11n**）で、54g モードが **auto** または **dot11b-only** のいずれかである場合のみ設定できます。

手順の概要

1. **interfaceDot11Radio0**
2. **54g-mode{auto|dot11b-only}preamble{short|long}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)# interface Dot11Radio 0`	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。

ステップ 2	**54g-mode{auto|dot11b-only}preamble{short|long}**
	例：
	`ap(config-if)# 54g-mode auto preamble long`
	例：
	`ap(config-if)# 54g-mode dot11b-only preamble short`
		54g プリアンブル タイプを設定します。
		• **short**：短いプリアンブル。802.11b クライアントがない場合、プリアンブル タイプを **short** に設定するとパフォーマンスが向上します。
		• **long**：長いプリアンブル。802.11g と 802.11b の両方がある場合は、プリアンブル タイプを **long** に設定します。

	コマンドまたはアクション	目的
		• **54g-mode** は、**auto** または **dot11b-only** のいずれかである必要があります。

54g レートの設定

54g 転送速度を設定するには、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。

（注） 54g レートは、802.11n レートが 54g レートを使うように設定されている場合（**dot11nrate54g**）、または 802.11n が無効の場合（**nodot11n**）のみ設定できます。

手順の概要

1. **interfaceDot11Radio0**
2. **54g-rate**{*Mbps-rate*|**auto**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**54g-rate**{*Mbps-rate*|**auto**} 例： `ap(config-if)#` **54g-rate 54** 例：	54g モードの速度を設定します。 • *Mbps-rate*：速度を Mbps で指定します。以下の値を指定できます。 • 1 • 2 • 5.5 • 6 • 9 • 11 • 12

	コマンドまたはアクション	目的
		• 18 • 24 • 36 • 48 • 54 • **auto**：54g レートを自動的に設定します。

54g 保護の設定

54g 保護を設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） 54g 保護は、802.11n が無効になっている場合にのみ設定できます。

手順の概要

1. **interfaceDot11Radio0**
2. **54g-protection**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**54g-protection** 例： `ap(config-if)#` **54g-protection**	54g 保護を有効にします。 • **54g-protection**：RTS/CTS 保護メカニズムを有効にします。 • **no54g-protection**：54g 保護を無効にします。

マルチキャスト レートの設定

マルチキャスト転送速度を設定するには、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. **interfaceDot11Radio0**
2. **multicast-rate{***Mbps-rate***|auto}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**multicast-rate{***Mbps-rate***|auto}** 例： `ap(config-if)#` **multicast-rate 54** 例： `ap(config-if)#` **multicast-rate auto**	マルチキャスト レートを設定します。 *Mbps-rate*：速度を Mbps で指定します。以下の値を指定できます。 • 1 • 2 • 5.5 • 6 • 9 • 11 • 12 • 18 • 24 • 36 • 48 • 54 **auto**：マルチキャスト レートを自動的に設定します。 （注） 802.11n が無効で（**nodot11n**）、54g モードが 802.11b のみに設定されている（**54g-modedot11b-only**）場合、許容される速度は自動、1、2、5.5、11 Mbps のみになります。その他の速度を設定しようとすると、警告メッセージが表示されます。

	コマンドまたはアクション	目的

基本レートの設定

ワイヤレス クライアントでサポートするデータ レートである基本転送速度を設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **basic-rate{1|2|all|default}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**basic-rate{1|2|all|default}** 例： `ap(config-if)#` **basic-rate 2** 例： `ap(config-if)#` **basic-rate all**	基本レートを設定します。 • **1**：1 および 2 Mbps • **2**：1、2、5.5、6、11、12、および 24 Mbps • **all**：すべてのレート • **default**：1、2、5.5、および 11 Mbps

フラグメンテーションしきい値の設定

このサイズを超えるとデータが断片化される最大パケット サイズ（バイト）としてのフラグメンテーションしきい値を設定するには、グローバルコンフィギュレーションモードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **fragment-threshold***threshold-in-bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイスモードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**fragment-threshold***threshold-in-bytes* 例： `ap(config-if)#` **fragment-threshold 2346**	フラグメンテーションしきい値をバイト単位で設定します。 *threshold-in-bytes* の範囲：256 ～ 2346 バイト デフォルト値は 2346 です。

RTS しきい値の設定

送信要求（RTS）しきい値を設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

（注） アクセス ポイントがしきい値より大きなパケットを送信する場合、CTS（clear-to-send）保護モードがトリガーされます。

手順の概要

1. **interfaceDot11Radio0**
2. **rts-threshold** *threshold-in-bytes*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイスモードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**rts-threshold** *threshold-in-bytes* 例： `ap(config-if)#` **rts-threshold 2347**	RTS しきい値をバイトで設定します。 *threshold-in-bytes*：範囲は 0 ～ 2347 バイトです。デフォルト値は 2347 です。

DTIM 間隔の設定

Delivery Traffic Indication Message（DTIM）間隔を設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **dtim-interval** *number-of-beacons*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**dtim-interval** *number-of-beacons* 例： `ap(config-if)#` **dtim-interval 255**	DTIM 間隔を設定します。これはビーコン フレームに含める情報で、次に予定されているバッファ データが AP にあることをクライアントに知らせます。 *number-of-beacons*：範囲は 1 ～ 255 ビーコンです。 デフォルト値は 1 です。

ビーコン間隔の設定

ビーコン間隔を設定するには、グローバルコンフィギュレーションモードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **beacon-interval***number-of-milliseconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイスモードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**beacon-interval***number-of-milliseconds* 例： `ap(config-if)#` **beacon-interval 65535**	ビーコン間隔を設定します。 *number-of-milliseconds*：範囲は 1 ～ 65535 ミリ秒（ms）です。デフォルト値は 100 ミリ秒です。

無線送信電力の設定

WLAN の無線送信電力を設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **tx-pwr***power-percentage*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**tx-pwr***power-percentage* 例： `ap(config-if)#` **tx-pwr 60**	送信電力を最大電力のパーセンテージで設定します。 *power-percentage*：電力のパーセンテージを指定します。以下の値を指定できます。 • 20 • 40 • 60 • 80

	コマンドまたはアクション	目的
		• 100

WMM オプションの設定

WiFi Multimedia（WMM）オプションを設定するには、グローバル コンフィギュレーション モードで以下の手順を実行します。

手順の概要

1. **interfaceDot11Radio0**
2. **[no]wmm[auto|no-ack|apsd]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interfaceDot11Radio0** 例： `ap(config)#` **interface Dot11Radio 0**	無線インターフェイス モードを開始します。プロンプトは ap(config-if) になります。
ステップ 2	**[no]wmm[auto|no-ack|apsd]** 例： `ap(config-if)#` **wmm**	WMM を有効、または無効にします。 • auto：WMM を auto モードに設定します。 • no-ack：WMM に no-acknowledgement を設定します。 • apsd：WMM に対して Automatic Power Save Delivery（APSD）モードを有効にします。 （注） WMM が「自動」モードの場合、WMM APSD は「有効」に設定し、クライアントが省電力モードを使用できるようにする必要があります。WMM が「有効」モードの場合、クライアントは WMM APSD が「有効」または「無効」かどうかに関係なく、省電力モードを使用できます。

現在の CLI 値とキーワードの表示

現在の CLI 値とキーワードを表示するには、**showap-config** コマンドを使用します。

手順の概要

1. **showap-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	**showap-config** 例： `ap#` **show ap-config**	現在の CLI 値とキーワードを表示します。

次の作業

設定例：現在の CLI 値とキーワードの表示

この例では、現在の CLI 値とキーワードを表示します。

```
ap# show ap-config
global-max-clients 16
dot11 ssid Cisco860
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit
dot11 guest-ssid 1 Cisco860_Guest1
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit
dot11 guest-ssid 2 Cisco860_Guest2
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
no encryption mode wep
exit
dot11 guest-ssid 3 Cisco860_Guest3
no isolate-clients
no wmf
max-associations 16
no hide-ap
no disable-wmm
no mac-filter-mode
authentication open
```

```
no encryption mode wep
exit
interface Dot11Radio 0
no shutdown
ssid Cisco860
no guest-ssid 1 Cisco860_Guest1
no guest-ssid 2 Cisco860_Guest2
no guest-ssid 3 Cisco860_Guest3
dot11n
channel least-congested timer 15
dot11n rate auto
dot11n protection
no dot11n n-client-only
dot11n rifs
no dot11n rx-pwr-save
dot11n rx-pwr-save quiet-time 10
dot11n rx-pwr-save pps 10
54g-rate auto
multicast-rate auto
basic-rate default
fragment-threshold 2346
rts-threshold 2347
dtim-interval 1
beacon-interval 100
tx-pwr 100
wmm
no wmm no-ack
wmm apsd
exit
interface BVI 1
ip address 10.10.10.2  255.255.255.248
no shutdown
exit
```

現在のチャネルと電源に関する情報の表示

現在のチャネルと電源に関する情報を表示するには、**showcontrollersDot11Radio0** コマンドを使用します。

手順の概要

1. **showcontrollersDot11Radio0**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showcontrollersDot11Radio0** 例： `ap# show controllers Dot11Radio 0`	現在のチャネルと電源に関する情報を表示します。

次の作業

例

```
ap# show controllers Dot11Radio 0
interface Dot11Radio0
Beacon Interval(ms)                 : 100
DTIM Interval(beacon)               :   1
Power Control:          On, HW
Current Channel:        11
BSS Channel:            11
BSS Local Max:          30.0 dBm
BSS Local Constraint:   0.0 dB
Channel Width:          20MHz
User Target:            31.75 dBm
SROM Antgain 2G:        2.0 dB
SROM Antgain 5G:        2.0 dB
SAR:                    -
Current rate:           [MCS15] ht mcs 15 Tx Exp 0 BW 20 sgi
Regulatory Limits:
Rate                   Chains 20MHz
DSSS                    1     19.0
OFDM                    1     13.50
MCS0_7                  1     13.50
VHT8_9SS1               1     -
DSSS_MULTI1             2     -
OFDM_CDD1               2     10.50
MCS0_7_CDD1             2     10.50
VHT8_9SS1_CDD1          2     -
MCS0_7_STBC             2     10.50
VHT8_9SS1_STBC          2     -
MCS8_15                 2     10.50
VHT8_9SS2               2     -
DSSS_MULTI2             3     -
OFDM_CDD2               3     -
MCS0_7_CDD2             3     -
VHT8_9SS1_CDD2          3     -
MCS0_7_STBC_SPEXP1      3     -
VHT8_9SS1_STBC_SPEXP1   3     -
MCS8_15_SPEXP1          3     -
VHT8_9SS2_SPEXP1        3     -
MCS16_23                3     -
VHT8_9SS3               3     -
Core Index:             0
Board Limits:
Rate                   Chains 20MHz
DSSS                    1     17.50
OFDM                    1     17.50
MCS0_7                  1     17.50
VHT8_9SS1               1     -
DSSS_MULTI1             2     17.50
OFDM_CDD1               2     17.50
MCS0_7_CDD1             2     17.50
VHT8_9SS1_CDD1          2     -
MCS0_7_STBC             2     17.50
VHT8_9SS1_STBC          2     -
MCS8_15                 2     17.50
VHT8_9SS2               2     -
DSSS_MULTI2             3     -
OFDM_CDD2               3     -
MCS0_7_CDD2             3     -
VHT8_9SS1_CDD2          3     -
MCS0_7_STBC_SPEXP1      3     -
VHT8_9SS1_STBC_SPEXP1   3     -
MCS8_15_SPEXP1          3     -
VHT8_9SS2_SPEXP1        3     -
MCS16_23                3     -
VHT8_9SS3               3     -
Power Targets:
Rate                   Chains 20MHz
DSSS                    1     16.0
```

```
OFDM                    1     12.0
MCS0_7                  1     12.0
VHT8_9SS1               1      8.0
DSSS_MULTI1             2      8.0
OFDM_CDD1               2      9.0
MCS0_7_CDD1             2      9.0
VHT8_9SS1_CDD1          2      8.0
MCS0_7_STBC             2      9.0
VHT8_9SS1_STBC          2      8.0
MCS8_15                 2      9.0
VHT8_9SS2               2      8.0
DSSS_MULTI2             3     -
OFDM_CDD2               3     -
MCS0_7_CDD2             3     -
VHT8_9SS1_CDD2          3     -
MCS0_7_STBC_SPEXP1      3     -
VHT8_9SS1_STBC_SPEXP1   3     -
MCS8_15_SPEXP1          3     -
VHT8_9SS2_SPEXP1        3     -
MCS16_23                3     -
VHT8_9SS3               3     -
Maximum Power Target among all rates:   16.0  16.0
Last est. power                     :   0.0  15.75
Power Target for the current rate   :   16.0  16.0
Last adjusted est. power            :   0.0  15.75
Power Percentage                    :   100
Channel Status:
No scan in progress.
current mac channel     11
target channel  11
```

現在関連付けられているクライアントの表示

現在関連付けられているクライアントを表示するには、**showdot11associations** コマンドを使用します。

手順の概要

1. **showdot11associations**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showdot11associations** 例： `ap# show dot11 associations`	現在関連付けられているクライアントを表示します。

次の作業

例：現在関連付けられているクライアントの表示

```
ap# show dot11 associations
Authenticated       Associated      Authorized       Interface
AA:BB:CC:11:22:33   yes             no               Dot11Radio0
```

SSID と BSSID のマッピングの表示

各 SSID には BSSID が関連付けられています。SSID と BSSID のマッピングを表示するには、**showdot11bssid** コマンドを使用します。

手順の概要

1. **showdot11bssid**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showdot11bssid** 例： `ap# show dot11 bssid`	SSID と BSSID のマッピングを表示します。

次の作業

例：SSID と BSSID のマッピングの表示

```
ap# show dot11 bssid
Interface       BSSID               Guest           SSID
Dot11Radio0     A4:93:4C:01:7A:9A   No              Cisco860
Dot11Radio0     A4:93:4C:01:7A:9B   Yes             Cisco860_Guest1
Dot11Radio0     A4:93:4C:01:7A:9C   Yes             Cisco860_Guest2
Dot11Radio0     A4:93:4C:01:7A:9D   Yes             Cisco860_Guest3
```

Tx/Rx 統計情報の表示

Dot11Radio 0 インターフェイスに関する現在の送信/受信（tx/rx）統計情報を表示するには、**showdot11statistics** コマンドを使用します。

手順の概要

1. **showdot11statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showdot11statistics** 例： `ap# show dot11 statistics`	Dot11Radio 0 インターフェイスの現在の tx/rx 統計情報を表示します。

次の作業

例：**Tx/Rx 統計情報の表示**

```
ap# show dot11 statistics
            rx bytes    rx pkts    rx errs  rx drops  tx bytes    tx pkts    tx errs  tx drops
Dot11Radio0        0          0          0         0     12824         94          0         0
```

BVI 1 インターフェイスの詳細の表示

BVI 1 インターフェイスの詳細を表示するには、**showinterfacesBVI1** コマンドを使用します。詳細にはルータの IP アドレスが含まれます。

ヒント　ルータにアクセスするために使用する IP アドレスを変更した後、このコマンドを使用して変更を確認できます。Web ベース インターフェイスの IP アドレスの設定, （293 ページ）を参照してください。

手順の概要

1. **showinterfacesBVI1**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showinterfacesBVI1** 例： `ap# show interfaces BVI 1`	現在の BVI 1 インターフェイスの詳細を表示します。

次の作業

例：BVI 1 インターフェイスの詳細の表示

```
This example displays BVI 1 interface details.
ap# show interfaces BVI 1
BVI1
          Link encap:Ethernet  HWaddr AA:11:BB:22:CC:33
          inet addr:10.10.10.2  Bcast:10.10.10.7  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:260 multicast:86 unicast:0 broadcast:174
          RX errors:0 dropped:0 overruns:0 frame:0
          TX packets:21 multicast:0 unicast:21 broadcast:0
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:0
          RX bytes:46642 (45.5 KiB) TX bytes:1260 (1.2 KiB)
          RX multicast bytes:32164 (31.4 KiB) TX multicast bytes:0 (0.0 B)
```

Dot11Radio 0 インターフェイス情報の表示

Dot11Radio 0 インターフェイス情報を表示するには、**showinterfacesDot11Radio0** コマンドを使用します。

手順の概要

1. **showinterfacesDot11Radio0**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showinterfacesDot11Radio0** 例： `ap# show interfaces Dot11Radio 0`	現在の Dot11Radio 0 インターフェイス情報を表示します。

例：Dot11Radio 0 インターフェイス情報の表示

この例では、Dot11Radio 0 インターフェイス情報が表示されます。

```
ap# show interfaces Dot11Radio 0
Dot11Radio0
          Link encap:Ethernet  HWaddr AA:11:BB:22:CC:33
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 multicast:0 unicast:0 broadcast:0
          RX errors:0 dropped:0 overruns:0 frame:160876
          TX packets:267 multicast:86 unicast:0 broadcast:181
          TX errors:0 dropped:0 overruns:0 carrier:0 collisions:0
          txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:52150 (50.9 KiB)
          RX multicast bytes:0 (0.0 B) TX multicast bytes:0 (0.0 B)
          Interrupt:15 Base address:0x4000
```

すべてのインターフェイスに関する概要の表示

すべてのインターフェイスに関する概要を表示するには、**showipinterfacebrief** コマンドを使用します。

手順の概要

1. **showipinterfacebrief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showipinterfacebrief** 例： `ap# show ip interface brief`	すべてのインターフェイスに関する概要を表示します。

次の作業

例：すべてのインターフェイスに関する概要の表示

出力の [Method] 列には、ユーザが設定したインターフェイスか、DHCP が設定したインターフェイスかが表示されます。

```
ap# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Dot11Radio0                unassigned      YES NVRAM  up                    up
BVI1                       10.10.10.2      YES NVRAM  up                    up
```

CPU 統計情報の表示

CCPU 使用率の統計情報を表示するには、**showprocessescpu** コマンドを使用します。

手順の概要

1. **showprocessescpu**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showprocessescpu** 例： `ap# show processes cpu`	CPU 使用率の統計情報を表示します。

例：**CPU** 統計情報の表示

```
ap# show processes cpu
CPU:   0% usr   0% sys   0% nic  90% idle   0% io   0% irq   9% sirq
```

メモリ使用量の概要の表示

現在のメモリ使用量の詳細を表示するには、**showmemorysummary** コマンドを使用します。

手順の概要

1. **showmemorysummary**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**showmemorysummary** 例： `ap# show memory summary`	現在のメモリ使用量の詳細が表示されます。

次の作業

例：メモリ使用量の概要の表示

ap# **showmemorysummary**

Total(kB) Used(kB) Free(kB)

Processor 88052 44212 43840

アドレスの ping

特定のアドレスの接続をテストするには、**ping** コマンドを使用します。

手順の概要

1. **ping**{*IP-address*| *hostname*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ping**{*IP-address*| *hostname*} 例： `ap#` **ping 10.0.0.0**	指定した IP アドレスまたはホスト名への接続をテストします。 アドレスを指定した **ping** コマンドを入力すると、小さなデータグラムの複数の伝送についてラウンド トリップ時間がミリ秒単位で示されます。 アドレスを指定せずに **ping** コマンドを入力すると、コマンドはインタラクティブ モードで開始されるため、ターゲットのアドレス、伝送の繰り返し回数、データグラムのサイズを入力できます。

管理者パスワードの変更

管理者パスワードを変更するには、**password** コマンドを使用します。

（注） デフォルトのログイン クレデンシャルは、ユーザ名：**admin** パスワード：**admin** です。初回ログイン時に、デフォルトのパスワードを変更するように指示されます。

手順の概要

1. **password** *old-password new-password confirm-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	**password** *old-password new-password confirm-password* 例： `ap#` **password admin AbCdE123# AbCdE123#**	管理者パスワードを変更します。新しいパスワードは、確認のために2回入力する必要があるため注意してください。

画面上の行数の設定

画面に表示する行数を設定するには、**terminallength** コマンドを使用します。

手順の概要

1. **terminallength***number-of-lines*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminallength***number-of-lines* 例： `ap#` **terminal length 40**	画面に表示する行数を設定します。 *number-of-lines* の範囲：0 ～ 512 値0を指定すると、表示は停止せずにスクロールします。

次の作業

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

この項では、次に示すワイヤレス デバイスへのアクセスを保護するタスクの実行について説明します。

MODE ボタン機能のディセーブル化

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） ワイヤレス 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，（355 ページ）を参照してください。

MODE ボタンはデフォルトで有効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 モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **nobootmode-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	**configureterminal**	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	**nobootmode-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。

MODE ボタンのステータスの表示

MODE 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、MODE ボタンを通常動作に復旧できます。

アクセス ポイントへの不正アクセスの防止

権限のないユーザがワイヤレス デバイスの設定を変更したり、設定情報を表示したりするのを防ぐことができます。通常は、ワイヤレス デバイスへのアクセスは、ネットワーク管理者とローカル 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に制限します。

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。

（注） TAB、?、$、+、および [は、パスワードに無効な文字です。

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 Configuration Fundamentals Command Reference for Release 12.4*』を参照してください。

この項では、コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。次の設定情報が含まれています。

デフォルト パスワードと特権レベルの設定

表 38：デフォルト パスワードと特権レベル，（336 ページ） に、デフォルトのパスワードおよび特権レベルの設定を示します。

表 *38*：デフォルト パスワードと特権レベル

Privilege Level	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。

Privilege Level	デフォルト設定
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 **noenablepassword** コマンドを実行すると、イネーブル 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. **configureterminal**
2. **enablepassword** *password*
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-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	**configureterminal**	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	**enablepassword** *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。

	コマンドまたはアクション	目的
		• *password*：1 ～ 25 文字の英数字の文字列。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。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	**showrunning-config**	入力を確認します。
ステップ 5	**copyrunning-configstartup-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。

次の作業

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 ファイル内で読み取ることができます。

設定例：スタティック イネーブル パスワードの変更

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

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。

（注） **enablesecret** コマンドを使用することが推奨されます。機能が向上した暗号化アルゴリズムが使用されるためです。**enablesecret** コマンドを設定する場合、**enablepassword** 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。

手順の概要

1. **configureterminal**
2. • **enablepassword** [**level** *level*] {*password* | *encryption-type encrypted-password*
   または
   • **enablesecret** [**level** *level*] {*password* | *encryption-type encrypted-password*
3. **servicepassword-encryption**
4. **end**
5. **copyrunning-configstartup-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	**configureterminal**	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	• **enablepassword** [**level** *level*] {*password* | *encryption-type encrypted-password* または • **enablesecret** [**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 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。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。 • *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 ポイントのワイヤレス 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	**servicepassword-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。

	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	**copyrunning-configstartup-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。

設定例：イネーブル シークレット パスワード

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 デバイスに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. **configureterminal**
2. **username** *name* [**privilege** *level*] {**password** *encryption-type password* }
3. **loginlocal**
4. **end**
5. **showrunning-config**
6. **copyrunning-configstartup-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	**configureterminal**	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。スペースと引用符は使用できません。

	コマンドまたはアクション	目的
		• *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。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type*：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	**loginlocal**	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。
ステップ 5	**showrunning-config**	入力を確認します。
ステップ 6	**copyrunning-configstartup-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。

次の作業

（注） ユーザ名は少なくとも 1 つ設定する必要があります。また、ワイヤレス デバイスに対して Telnet セッションを開くように login local を設定する必要があります。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。

複数の権限レベルの設定

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

たとえば、多くのユーザに **clearline** コマンドへのアクセスを許可する場合は、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を扱います。

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. **configureterminal**
2. **privilege** *mode***level** *level command*
3. **enablepasswordlevel** *level password*
4. **end**
5. • **showrunning-config**
   または
   • **showprivilege**
6. **copyrunning-configstartup-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	**configureterminal**	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** を入力します。 • *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	**enablepasswordlevel** *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。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。

	コマンドまたはアクション	目的
		（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	• **showrunning-config** または • **showprivilege**	入力を確認します。 **showrunning-config** コマンドは、パスワードとアクセス レベルの設定を表示します。 **showprivilege** コマンドは、特権レベルの設定を表示します。
ステップ 6	**copyrunning-configstartup-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。

複数の権限レベルの設定

（注） コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**showiproute** コマンドをレベル 15 に設定すると、**show** コマンドと **showip** コマンドは、異なるレベルに個別に設定しない限り、権限レベルは自動的に 15 に設定されます。あるコマンドの権限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 **noprivilege** *mode* **level** *level command* コマンドを使用します。

権限レベルへのログインおよび終了

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

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*：指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した権限レベルを終了します。

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詳しい手順については、『Cisco IOS Software Configuration Guide』で Cisco Aironet アクセス ポイントについて参照してください。

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、認証、許可、アカウンティング（AAA）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。

RADIUS の設定作業については、以降の項で説明します。

RADIUS 設定

RADIUSおよびAAAは、デフォルトではディセーブルに設定されています。セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてワイヤレス デバイスにアクセスしているユーザを認証できます。

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。その方式が応答に失敗すると、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。

RADIUS ログイン認証の設定

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. **configureterminal**
2. **aaanew-model**
3. **aaaauthenticationlogin{default|***list-name* } *method1* [*method2...*
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*
5. **loginauthentication** {**default** | *list-name*
6. **end**
7. **showrunning-config**
8. **copyrunning-configstartup-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	**configureterminal**	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	**aaanew-model**	AAA をイネーブルにします。
ステップ 3	**aaaauthenticationlogin{default|***list-name* } *method1* [*method2...*	ログイン認証方式リストを作成します。 • **loginauthentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name*：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」セクションを参照してください。

	コマンドまたはアクション	目的
ステップ 4	**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	**loginauthentication** {**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、**aaaauthenticationlogin** 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*：**aaaauthenticationlogin** 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	**showrunning-config**	入力を確認します。
ステップ 8	**copyrunning-configstartup-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。

次の作業

AAA サーバ グループの定義

AAA サーバ グループを使用して認証用に既存のサーバ ホストをグループ化するように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関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。サーバをIPアドレスで特定することも、任意指定の**auth-port** および**acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定することもできます。

AAA サーバ グループの設定

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

手順の概要

1. **configureterminal**
2. **aaanew-model**
3. **radius-serverhost** {*hostname* | *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
4. **aaagroupserverradius** *group-name*
5. **server** *ip-address*
6. **end**
7. **showrunning-config**
8. **copyrunning-configstartup-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	**configureterminal**	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	**aaanew-model**	AAA をイネーブルにします。
ステップ 3	**radius-serverhost** {*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-servertimeout** 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-serverhost** コマンドでタイムアウトが設定されていない場合、**radius-servertimeout** 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-serverhost** コマンドに再送信の値が設定されていない場合、**radius-serverretransmit** 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）RADIUS サーバ上で動作する RADIUS デーモンとワイヤレス デバイスの間で使用する認証および暗号キーを指定します。

	コマンドまたはアクション	目的
		（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。必ず **radius-serverhost** コマンドで、最終項目として key を設定してください。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、および暗号キーの値をそれぞれ設定してください。
ステップ 4	**aaagroupserverradius** *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。
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	**showrunning-config**	入力を確認します。
ステップ 8	**copyrunning-configstartup-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。

次の作業

RADIUS ログイン認証を有効にします。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「Configuring RADIUS Login Authentication」の項を参照してください。

設定例：*AAA* グループ

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 イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 許可は、ユーザが使用できるサービスを制限します。AAA 許可が有効の場合、ワイヤレス デバイスはユーザのプロファイルから取得した情報を使用してユーザのセッションを設定します。ユーザのプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。ユーザ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。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータは、グローバル コンフィギュレーション モードで **aaaauthorization** コマンドに **radius** キーワードを指定して設定できます。

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。

ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

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. **configureterminal**
2. **aaaauthorizationnetworkradius**
3. **aaaauthorizationexecradius**
4. **end**
5. **showrunning-config**
6. **copyrunning-configstartup-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	**configureterminal**	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	**aaaauthorizationnetworkradius**	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	**aaaauthorizationexecradius**	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	**showrunning-config**	入力を確認します。
ステップ 6	**copyrunning-configstartup-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。

次の作業

認証を無効にするには、グローバル コンフィギュレーション モードで **noaaaauthorization** {**network** | **exec**} *method1* コマンドを使用します。

RADIUS の設定の表示

RADIUS 設定情報を表示するには、特権 EXEC モードで **showrunning-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詳しい手順については、『*Cisco IOS Software Configuration Guide*』で Cisco Aironet アクセス ポイントについて参照してください。

TACACS+ は、認証および認可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

（注） こ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+ の設定情報について説明します。

TACACS+ のデフォルト設定

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

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 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。

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。その方式が応答に失敗すると、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。

TACACS+ ログイン認証の設定

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. **configureterminal**
2. **aaanew-model**
3. **aaaauthenticationlogin{default|** *list-name* } *method1* [*method2...*
4. **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*
5. **loginauthentication** {**default** | *list-name*
6. **end**
7. **showrunning-config**
8. **copyrunning-configstartup-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	**configureterminal**	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	**aaanew-model**	AAA をイネーブルにします。
ステップ 3	**aaaauthenticationlogin{default|** *list-name* } *method1* [*method2...*	ログイン認証方式リストを作成します。 • **loginauthentication** コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。 • *list-name*：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	**loginauthentication** {**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、**aaaauthenticationlogin** 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*：**aaaauthenticationlogin** 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	**showrunning-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copyrunning-configstartup-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。

次の作業

AAA をディセーブルにするには、**noaaanew-model** コマンドをグローバル コンフィギュレーション モードで使用します。AAA 認証をディセーブルにするには、**noaaaauthenticationlogin** {default | *list-name* } *method1* [*method2...*] コマンドをグローバル コンフィギュレーション モードで使用します。ログインに対してTACACS+認証をディセーブルにするか、またはデフォルト値に戻すには、**nologinauthentication** {**default** | *list-name* } コマンドをグローバル コンフィギュレーション モードで使用します。

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

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可が有効の場合、ワイヤレス デバイスはユーザのプロファイルから取得した情報を使用してユーザのセッションを設定します。ユーザのプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータは、グローバル コンフィギュレーション モードで **aaaauthorization** コマンドに **tacacs+** キーワードを指定して設定できます。

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

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

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

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. **configureterminal**
2. **aaaauthorizationnetworktacacs+**
3. **aaaauthorizationexectacacs+**
4. **end**
5. **showrunning-config**
6. **copyrunning-configstartup-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	**configureterminal**	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	**aaaauthorizationnetworktacacs+**	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	**aaaauthorizationexectacacs+**	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	**showrunning-config**	入力を確認します。
ステップ 6	**copyrunning-configstartup-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。

次の作業

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 **showtacacs** コマンドを使用します。

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

ここでは、次のタスクの実行について説明します。

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

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-modulewlan-ap0resetdefault-config** コマンドを使用します。

注意 データを消失する可能性があるため、**service-modulewlan-ap0reset** 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。

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-modulewlan-ap0reload** コマンドを使用します。確認プロンプトで、**Enter** を押してアクションを確認するか、**n** を入力してキャンセルします。

自律モードでリロード 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、ワイヤレス LAN コントローラ（WLC）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、ルータ上のハードウェアをモニタリングし、無線デバイスの統計情報および無線デバイスのステータスを表示するコマンドについて説明します。

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-modulewlan-ap0statistics** 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** コマンドを実行します。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。

Simple Network Time Protocol の概要

簡易ネットワーク タイム プロトコル（SNTP）とは、クライアント専用バージョンの簡易版 NTP です。SNTP は、NTP サーバから時間だけを受信します。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、最適な層にあるサーバが選択されますNTP とストラタムの詳細は、次の URL をクリックしてください。

http://www.cisco.com/en/US/docs/ios/12_1/configfun/configuration/guide/fcd303.html#wp1001075
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 39：SNTP コマンド，（357 ページ）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 *39*：*SNTP* コマンド

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

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

sntp server コマンドと sntp broadcast client コマンドの両方を入力した場合、アクセス ポイントはブロードキャスト サーバからの時間を受け入れますが、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。

日付と時刻の手動設定

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 デバイスを同期できる外部ソースがある場合は、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、タイム ゾーン、夏時間を設定するオプションがあります。

日時の設定

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

（注） 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。

手順の概要

1. **clockset** *hh*:*mm*:*ss day month year*
2. **clocktimezone** *zone hours-offset minutes-offset*
3. **clocksummer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]
4. • **clocksummer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]]
   または
   • **clocksummer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]
5. **end**
6. **showrunning-config**
7. **copyrunning-configstartup-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	**clockset** *hh*:*mm*:*ss day month year* 例： **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、秒単位で時刻を指定します。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*：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	**clocktimezone** *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。グローバル コンフィギュレーション モードでの **clocktimezone** コマンドの *minutes-offset* 変数は、ローカル タイム ゾーンと 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。
ステップ 3	**clocksummer-time** *zone* **recurring** [*week day month hh*:*mm week day month hh*:*mm* [*offset*]]	（任意）毎年指定した日に開始および終了するように夏時間を設定します。

	コマンドまたはアクション	目的
		clocksummer-time グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。 夏時間はデフォルトで無効に設定されています。パラメータなしで **clocksummer-time** *zone* **recurring** を指定すると、夏時間のルールは米国のルールにデフォルト設定されます。 • *zone*：夏時間が有効な場合に表示されるタイム ゾーンの名前（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。デフォルトは 60 です。
ステップ 4	• **clocksummer-time** *zone* **date** [*month date year hh*:*mm month date year hh*:*mm* [*offset*]] または • **clocksummer-time** *zone* **date** [*date month year hh*:*mm date month year hh*:*mm* [*offset*]]	（任意）定期的なパターンがない場合の夏時間を設定します。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。**clocksummer-time** グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイム ゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。 夏時間はデフォルトで無効に設定されています。 • *zone*：夏時間が有効な場合に表示されるタイム ゾーンの名前（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。デフォルトは 60 です。

	コマンドまたはアクション	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**showrunning-config**	入力を確認します。
ステップ 7	**copyrunning-configstartup-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。

次の作業

（注） 日時の設定を表示するには、特権 EXEC モードで **showclock** [**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 クロックがタイミング ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていなければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。**showclock** の表示の前にある記号は、次の意味があります。

設定例: 日付と時刻

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
```

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
```

システム名とプロンプトの設定

識別するためのシステム名をワイヤレス デバイス上に設定します。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 文字がシステム プロンプトとして使用されます。大なり記号（>）が追加されます。プロンプトは、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設定しない限り、システム名が変更されると必ず更新されます。

（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』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。

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. **configureterminal**
2. **hostname** *name*
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-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	**configureterminal**	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、関連付けられているクライアントデバイスは関連付けが解除され、ただちに再度関連付けられます。 （注） システム名には、63 文字まで入力することができます。ただし、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。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**showrunning-config**	入力を確認します。
ステップ 5	**copyrunning-configstartup-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。

DNS について

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 デバイス上に DNS を設定すると、**ping**、**telnet**、**connect** などのすべての IP コマンドや、関連する Telnet サポート操作時に、IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できます。ドメイン名は、ピリオド（.）を区切り文字として使用して構成されています。たとえば、シスコは、IP では *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。このドメイン内の File Transfer Protocol（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

表 40：DNS のデフォルト設定, （362 ページ） に、デフォルトの DNS 設定を示します。

表 *40*：*DNS* のデフォルト設定

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

DNS の設定

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 モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **ipdomain-name** *name*
3. **ipname-server** *server-address1* [*server-address2 ... server-address6*
4. **ipdomain-lookup**
5. **end**
6. **showrunning-config**
7. **copyrunning-configstartup-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	**configureterminal**	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	**ipdomain-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	**ipname-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 サーバに DNS クエリーを送信します。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	**ipdomain-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。

	コマンドまたはアクション	目的
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**showrunning-config**	入力を確認します。
ステップ 7	**copyrunning-configstartup-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。

次の作業

ワイヤレス デバイスの IP アドレスをそのホスト名として使用する場合は、IP アドレスが使用され、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クエリーが行われ、名前を IP アドレスにマッピングします。デフォルトのドメイン名は、グローバル コンフィギュレーション モードで **ipdomain-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 **noipdomain-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 **noipname-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 **noipdomain-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 **showrunning-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る場合があります。

バナーの作成

Message-of-The-Day（MoTD）バナーおよびログイン バナーを作成できます。デフォルトでは、MOTD とログインバナーは設定されていません。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。

Message-of-the-Day 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. **configureterminal**
2. **bannermotd** *c message c*
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-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	**configureterminal**	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	**bannermotd** *c message c*	MoTD を指定します。 • *c*：ポンド記号（#）など希望する区切り文字を入力し、**Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 • *message*：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	**showrunning-config**	入力を確認します。
ステップ 5	**copyrunning-configstartup-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。

例：MOTD バナーの設定

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. **configureterminal**
2. **bannerlogin** *c message c*
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-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	**configureterminal**	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	**bannerlogin** *c message c*	ログイン メッセージを指定します。 • *c*：ポンド記号（#）など希望する区切り文字を入力し、**Return** キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。 • *message*：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	**showrunning-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 5	**copyrunning-configstartup-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。

設定例：ログイン バナー

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、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)#
```

無線デバイスの通信管理

ここでは次の作業について説明します。

イーサネットの速度およびデュプレックスの設定

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。

（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。

手順の概要

1. **configureterminal**
2. **interfacefastethernet0**
3. **speed{10|100|auto}**
4. **duplex{auto|full|half}**
5. **end**
6. **showrunning-config**
7. **copyrunning-configstartup-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	**configureterminal**	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	**interfacefastethernet0**	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	**showrunning-config**	入力を確認します。
ステップ 7	**copyrunning-configstartup-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 デバイスで無線ネットワーク管理を有効にできます。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。

次のコマンドを入力し、WNM と対話するようにワイヤレス デバイスを設定します。

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

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

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

ステータスは、not authenticated、authentication in progress、authentication fail、authenticated、security keys setup のいずれかになります。

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。この場合、ワイヤレスデバイスは認証および許可の処理を行います。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 モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **aaanew-model**
3. **aaaauthenticationlogindefaultlocal**
4. **aaaauthorizationexeclocal**
5. **aaaauthorizationnetworklocal**
6. **username** *name* [**privilege** *level*] {**password** *encryption-type password*
7. **end**
8. **showrunning-config**
9. **copyrunning-configstartup-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	**configureterminal**	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	**aaanew-model**	AAA をイネーブルにします。
ステップ 3	**aaaauthenticationlogindefaultlocal**	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	**aaaauthorizationexeclocal**	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	**aaaauthorizationnetworklocal**	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。 ユーザごとにコマンドを繰り返し入力します。

	コマンドまたはアクション	目的
		• *name*：1 語でユーザ ID を指定します。スペースと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。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • *encryption-type*：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を指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、**username** コマンドの最後のオプションとして指定します。 （注） TAB、?、$、+、および [は、パスワードに無効な文字です。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**showrunning-config**	入力を確認します。
ステップ 9	**copyrunning-configstartup-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。

次の作業

（注） AAA をディセーブルにするには、**noaaanew-model** コマンドをグローバル コンフィギュレーション モードで使用します。認証を無効にするには、グローバル コンフィギュレーション モードで **noaaaauthorization** {**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。

- **cacheexpiry**
- **cacheauthorizationprofile**
- **cacheauthenticationprofile**
- **aaacacheprofile**

（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。

設定例：認証キャッシュとプロファイルの設定

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

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 にある『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
http://www.cisco.com/en/US/docs/ios/ipaddr/configuration/guide/iad_dhcp_rdmp_ps6350_TSD_Products_Configuration_Guide_Chapter.html

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

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. **configureterminal**
2. **ipdhcpexcluded-address** *low_address*[*high_address*]
3. **ipdhcppool** *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. **showrunning-config**
9. **copyrunning-configstartup-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	**configureterminal** 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	**ipdhcpexcluded-address** *low_address*[*high_address*]	ワイヤレス デバイスが割り当てるアドレス範囲からワイヤレス デバイスの IP アドレスを除外します。 • IP アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。 • ワイヤレス デバイスでは、DHCP アドレス プール サブネット中のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定されます。DHCP サーバがクライアントに割り当てない 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	**ipdhcppool** *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、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 プレフィックスを構成するビット数を指定します。接頭辞はネットワーク マスクを割り当てる代替法です。プレフィックス長は、スラッシュ（/）で開始する必要があります。
ステップ 5	**lease**{days [hours] [minutes] | **infinite**}	ワイヤレス デバイスによって割り当てられた IP アドレスのリース期間を設定します。 • *days*：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。

	コマンドまたはアクション	目的
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**showrunning-config**	入力を確認します。
ステップ 9	**copyrunning-configstartup-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。

次の作業

設定例：DHCP サーバの設定

次の例では、ワイヤレス デバイスを DHCP サーバとして設定する方法、IP アドレスの範囲を除外する方法、およびデフォルト 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 ポイントの監視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

DHCP サーバとして使用しているワイヤレス デバイスに関する情報を表示するには、表 41：DHCP サーバ用の show コマンド, （375 ページ）にあるコマンドを特権 EXEC モードで入力します。

表 *41*：*DHCP* サーバ用の *show* コマンド

コマンド	目的
showipdhcpconflict [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で記録された競合を表示するには、ワイヤレス デバイスの IP アドレスを入力します。
showipdhcpdatabase [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。

コマンド	目的
showipdhcpserverstatistics	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、表 42：DHCP サーバ用の clear コマンド, （376 ページ）にあるコマンドを特権 EXEC モードで使用します。

表 *42*：*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。
clearipdhcpconflict {address | *}	DHCP データベースのアドレス競合をクリアします。address 引数を指定すると、特定の IP アドレスの競合が消去されます。アスタリスク（*）を指定すると、すべてのアドレスの競合が消去されます。
clearipdhcpserverstatistics	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 デバイスの 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、SSH 機能を設定する方法について説明します。

（注） この項で使用されるコマンドの構文と使用方法の詳細は、『*Cisco IOS Security Command Reference for Release 12.4*』の「*Secure Shell Commands*」の項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。

SSH の詳細については、『*Cisco IOS Security Configuration Guide for Release 12.4*』の「*Other Security Features*」のパート 5 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 にある、『*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

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

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、関連付けられたクライアント デバイスに代わって ARP 要求に応答します。

ARP キャッシングを無効にすると、ワイヤレス デバイスはすべての ARP 要求を無線ポート経由で関連付けられたクライアントに転送します。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関連付けら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 デバイスは、キャッシュにない IP アドレス宛ての ARP 要求を受け取ると、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、バッテリの寿命を延ばすためにブロードキャスト メッセージを安全に無視できることをクライアント デバイスに通知します。

アクセスポイントにシスコ製以外のクライアントデバイスが関連付けられ、そのデバイスがデータを通さない場合、ワイヤレスデバイスはそのクライアントのIPアドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスは、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要求は無線ポートから転送します。ワイヤレスデバイスは、関連付けられている全クライアントのIPアドレスを学習すると、それら関連付けられたクライアント宛て以外の ARP 要求をドロップします。

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 モードで次の手順を実行します。

手順の概要

1. **configureterminal**
2. **dot11arp-cache[optional]**
3. **end**
4. **showrunning-config**
5. **copyrunning-configstartup-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	**configureterminal**	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	**dot11arp-cache[optional]**	ワイヤレスデバイス上でARPキャッシングを有効にします。 （任意）ワイヤレス デバイスが 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	**showrunning-config**	入力を確認します。

	コマンドまたはアクション	目的
ステップ 5	**copyrunning-configstartup-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。

次の作業

例：ARP キャッシュの設定

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。

第 12 章

PPP over Ethernet と NAT の設定

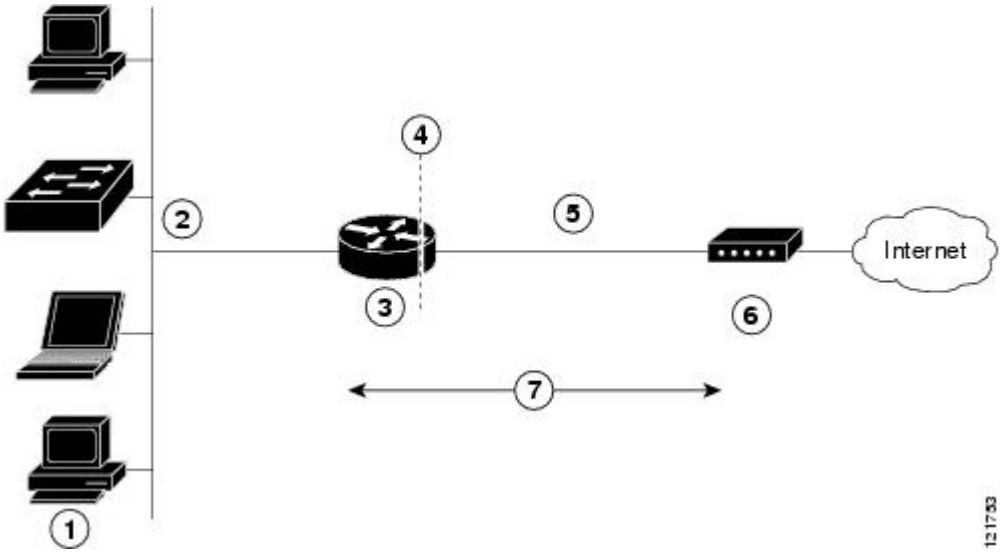
この章では、Cisco 819、Cisco 860、Cisco 880、および Cisco 890 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。

概要

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 16：PPP over

Ethernet と NAT に、Cisco ルータに PPPoE クライアントと NAT を設定する一般的な展開シナリオを示します。

図 16：*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 ISR
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 819、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。
- セッションをクリアする **nopppoe-clientdial-pool** *number* コマンドを入力する。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。

この設定タスクの結果を示す例は、設定例, （391 ページ）にあります。

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. **vpdnenable**
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	**vpdnenable** 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 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-clientdial-pool-number** *number*
3. **noshutdown**
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`
	or
	
	例：
	`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-clientdial-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	**noshutdown** 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。

次の作業

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、『Carrier Ethernet Configuration Guide』の「Using Ethernet Operations, Administration, and Maintenance」を参照してください。

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. **interfacedialer** *dialer-rotary-group-number*
2. **ipaddressnegotiated**
3. **ipmtu** *bytes*
4. **encapsulation** *encapsulation-type*
5. **pppauthentication** {*protocol1* [*protocol2...*]}
6. **dialerpool** *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. **iproute***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	**interfacedialer** *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。

	コマンドまたはアクション	目的
ステップ 2	**ipaddressnegotiated** 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	**ipmtu** *bytes* 例： `Router(config-if)# ip mtu 1492`	IP 最大伝送単位（MTU）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。
ステップ 5	**pppauthentication** {*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。 このコマンドと設定可能な追加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	**dialerpool** *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。

	コマンドまたはアクション	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	**iproute***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。

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. **ipnatpool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. 次のいずれかを実行します。
   - **ipnatinsidesource{list** *access-list-number*}{**interface** *type number* |**pool***name*}**[overload]**
   - `Router(config)# ip nat inside source list 1 interface dialer 0 overload`
   - `Router(config)# ip nat inside source list acl1 pool pool1`
3. interface type number
4. **ipnat** {**inside** | **outside**}
5. **noshutdown**
6. **exit**
7. interface type number
8. **ipnat** {**inside** | **outside**}
9. **noshutdown**
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	**ipnatpool** *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	次のいずれかを実行します。 • **ipnatinsidesource{list** *access-list-number*}{**interface** *type number* |**pool***name*}**[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。 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。

	コマンドまたはアクション	目的
	• Router(config)# ip nat inside source list 1 interface dialer 0 overload • Router(config)# ip nat inside source list acl1 pool pool1	2番目の例は、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。
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	**ipnat** {**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。
ステップ 5	**noshutdown** 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。
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	**ipnat** {**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。
ステップ 9	**noshutdown** 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。

	コマンドまたはアクション	目的
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。

次の作業

（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については、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 の概念の概要については、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） **showrunning-config** コマンドを実行すると、「(default)」でマークされたコマンドが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
```

第 13 章

『Configuring PPP over ATM with NAT』

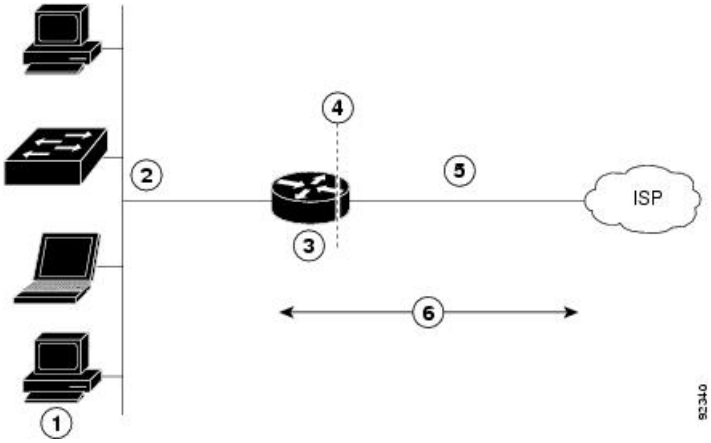
この章では、Cisco 860 および Cisco 880 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）およびネットワーク アドレス変換（NAT）の概要について説明します。

概要

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 17：PPP over ATM と NAT，（394 ページ） に、Cisco ルー

タに PPPoA クライアントと NAT を設定する一般的な展開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 *17*：*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, （395 ページ）
- ATM WAN インターフェイスの設定, （397 ページ）
- DSL シグナリング プロトコルの設定, （399 ページ）
- ネットワーク アドレス変換の設定, （401 ページ）

この設定タスクの結果を示す例は、設定例, （403 ページ）にあります。

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。

手順の概要

1. **interfacedialer** *dialer-rotary-group-number*
2. **ipaddressnegotiated**
3. **ipmtubytes**
4. **encapsulation** *encapsulation-type*
5. **pppauthentication** {*protocol1* [*protocol2...*]}
6. **dialerpoolnumber**
7. **dialer-group** *group-number*
8. **exit**
9. **dialer-list** *dialer-group***protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
10. **iproute** *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	**interfacedialer** *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	**ipaddressnegotiated** 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	**ipmtubytes** 例： `Router(config-if)# ip mtu 4470`	IP 最大伝送単位（MTU）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	**pppauthentication** {*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	**dialerpoolnumber** 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。

	コマンドまたはアクション	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	**iproute** *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。

次の作業

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。

手順の概要

1. interface type number
2. **pvc** *vpi/vci*
3. **encapsulation{aal5auto|aal5autoppp virtual-template** *number***[group** *group-name***]|aal5ciscopppvirtual-template** *number***|aal5mux** *protocol***|aal5nlpid|aal5snap}**
4. **dialerpool-member** *number*
5. **noshutdown**
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	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, （28 ページ）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。ステップ 3 に示すように、これを変更するには **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。
ステップ 3	**encapsulation{aal5auto|aal5autoppp virtual-template** *number*[**group** *group-name*]|**aal5ciscopppvirtual-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	**dialerpool-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	**noshutdown** 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。

	コマンドまたはアクション	目的

ステップ 6	**exit**
	
	例：
	`Router(config-if)# exit`
	
	例：
	`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 43：ADSL のデフォルト設定, （399 ページ）に、ADSL シグナリングのデフォルト設定を示します。

表 *43*：*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。	自動
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。	無効

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。

- **dsloperating-mode**（ATM インターフェイス コンフィギュレーション モード）
- **dsllom** 整数
- **dslenable-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 **showdslinterfaceatm** 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。

手順の概要

1. **ipnatpool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
2. 次のいずれかを実行します。
   - **ipnatinsidesource{list** *access-list-number*}{**interface** *type number* |**pool***name*}**[overload]**
   - **例 1**：

     ```
     Router(config)# ip nat inside source list 1 interface dialer
         0 overload
     ```

   - **例 2**：

     ```
     Router(config)# ip nat inside source list acl1 pool pool1
     ```

3. interface type number
4. **ipnat{inside|outside}**
5. **noshutdown**
6. **exit**
7. interface type number
8. **ipnat{inside|outside}**
9. **noshutdown**
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	**ipnatpool** *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	次のいずれかを実行します。
	• **ipnatinsidesource{list** *access-list-number*}**{interface** *type number* |**pool***name*}**[overload]**
	• **例 1**：
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	• **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。
		2 番目の例は、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。

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	**ipnat{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。
ステップ 5	**noshutdown** 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 インターフェイスに対するコンフィギュレーション モードを終了します。

	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 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	**ipnat{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。
ステップ 9	**noshutdown** 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。

次の作業

（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、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） **showrunning-config** コマンドを実行すると、「(default)」でマークされたコマンドが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
!
```

NAT の設定の確認

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
```

第 14 章

環境および電源管理

この章では、環境と電源管理機能について説明します。

環境および電源管理

Cisco 819 サービス統合型ルータは、環境温度を監視し、30 秒ごとに温度を記録するために本体にセンサーを搭載しています。ルータのシャーシの四隅に 1 つずつ、4 つのセンサーがあります。さらにシステム アンビエント センサーおよび 3G センサーがあります。

コーナー センサーは次のメッセージを表示します。

- コンソールへのエラー メッセージ：温度範囲が設定されている温度しきい値を外れると、モニタにエラー メッセージを表示します。ルータの異なる SKU ごとに違う温度範囲が設定されています。
  - Cisco 819G（非強化）：0 ～ 60 °C
  - Cisco 819HG（強化）：–25 ～ 75 °C
- SNMP トラップ：syslog メッセージは、温度が指定範囲外の場合に作成されます。
- サーバの「Call Home」機能：サーバの CallHome 機能が有効化されているため、非常に高温または低温になった場合に、Cisco TAC に問い合わせることができます。

コーナー センサーに加えて、システム周囲センサーと 3G センサーでも 30 秒おきに温度をブート フラッシュ メモリに記録されます。

温度が上限しきい値を超えたり、下限しきい値を下回ったりすると、温度情報が不揮発性メモリ領域に保存され、この出力の一部として表示されます。

ルータの動作温度を確認するには、show environment コマンドを使用します。または最後に装置の電力使用量および電力消費量を表示するには、このコマンドを使用できます。

次に、show environment コマンドの出力例を示します。

```
router# show environment

SYSTEM WATTAGE
===============
 Board Power consumption is: 4.851 W
 Power Supply Loss:  1.149 W
 Total System Power consumption is: 6.000 W
REAL TIME CLOCK BATTERY STATUS
==============================
 Battery OK (checked at power up)
TEMPERATURE STATUS
==================
 Sensor                Current                       High/Low
 Name                  Temperature    Status         Threshold
 --------------------- -------------- -------------- ---------
 Sensor 1              36             Normal         60/0
 Sensor 2              34             Normal         60/0
 Sensor 3              40             Normal         60/0
 Sensor 4              38             Normal         60/0
 System Ambient Sensor 35             Normal         60/0
 3G Modem Sensor       33             Normal         85/0
 Environmental information last updated 00:00:26 ago
```

（注） モデムの温度が、非強化バージョンの場合は85度まで、強化バージョンでは90度まで上がると、警告メッセージが表示されます。温度が108度を超えた場合、ルータは自動的にシャットダウンします。

Cisco EnergyWise サポート

Cisco 819 ISR には、電力消費を減らすためのハードウェアおよびソフトウェア機能があります。ハードウェア機能としては、高性能 AC 電源および RAM 選択やクロック ゲーティングなど、省電力機能を内蔵した電気部品があります。詳細については、『Cisco 819 Integrated Services Router Hardware Installation Guide』を参照してください。

ソフトウェア機能には、未使用のモジュールの電源を切り、ルータのモジュールおよび周辺機器への未使用のクロックをディセーブルにする電力効率管理機能である Cisco EnergyWise があります。

Cisco 819 ISR で EnergyWise をサポートするには、Cisco IOS Release 15.0(1)M 以降を実行している必要があります。詳細な設定手順は以下に記載されています。

『Cisco EnergyWise Configuration Guide, EnergyWise Phase 1』および『Cisco EnergyWise Configuration Guide, EnergyWise Phase 2』

第 15 章

4G LTE ワイヤレス WAN

Cisco 4G LTE（Fourth-Generation Long-Term Evolution）WWAN（Wireless WAN）は、DSL やフレーム リレーに代わり、安全性が高くシンプルでコスト効率の高い WAN を提供します。地上ブロードバンド サービス（ケーブル、DSL、T1）が利用できない地域や、設備投資が高額となる地域では、4G LTE WWAN 接続が現実的な選択肢です。Cisco 819 シリーズ 4G LTE ISR、Cisco C880 シリーズ 4G LTE ISR、Cisco C890 シリーズ 4G LTE ISR は、4G LTE と 3 G 携帯電話ネットワークをサポートし、Cisco 880G シリーズ ISR は、3G 携帯電話ネットワークをサポートします。

Cisco 800 シリーズ ISR での 4G LTE のサポート

Cisco IOS リリース 15.2(4)M1 より、Cisco 819 シリーズ 4G LTE ISR ではマルチモード 4G LTE 機能がサポートされます。Cisco C880 シリーズ 4G LTE ISR と Cisco C890 シリーズ 4G LTE ISR も、Cisco IOS リリース 15.4(3)T より 4G LTE 機能をサポートします。Cisco 819 シリーズ 4G LTE ISR、Cisco C880 シリーズ 4G LTE ISR、Cisco C890 シリーズ 4G LTE ISR は、次のモードをサポートします。

- 4G LTE：4G LTE モバイル仕様では、マルチメガビットの帯域幅、より効率的な無線ネットワーク、遅延の減少、改善されたモビリティが提供されます。LTE ソリューションは新しい携帯電話ネットワークを対象とします。これらのネットワークは、最初にダウンリンクで最大 100 Mb/s のピーク レートを、アップリンクで最大 50 Mb/s のピーク レートをサポートします。これらのネットワークのスループットは既存の 3G ネットワークよりも大きくなります。
- 3G Evolution High-Speed Packet Access（HSPA/HSPA+）モード：HSPA は UMTS ベースの 3G ネットワークです。これは、ダウンロードおよびアップロード速度の向上のため、High-Speed Downlink Packet Access（HSDPA）および High-Speed Uplink Packet Access（HSUPA）データをサポートします。Evolution High-Speed Packet Access（HSPA+）は、Multiple Input/Multiple Output（MIMO）アンテナ機能をサポートします。

- 3G Evolution-Data Optimized（EVDO または DOrA）：EVDO は、無線信号を介したデータのワイヤレス伝送、特にブロードバンド インターネット アクセスの 3G 通信規格です。DOrA は EVDO Rev-A を参照します。EVDO は、個々のユーザのスループットおよびシステム全体のスループットの両方を最大化するために、符号分割多重接続（CDMA）や時分割多重アクセス（TDMA）などの多重化技術を使用します。

Cisco 800 シリーズ 4G LTE ISR の設定方法

Cisco 819 シリーズ 4G LTE ISR、Cisco C880 シリーズ 4G LTE ISR、および Cisco C890 シリーズ 4G LTE ISR の 4G LTE 機能を設定する方法については、『Cisco 4G LTE ソフトウェア インストール ガイド』を参照してください。

（注） Cisco 800 シリーズ 4G LTE ISR では、すべてのコマンドに対してスロット「0」を使用します。

Cisco 800 シリーズ 4G LTE ISR の設定例

次に、Cisco 800 シリーズ 4G LTE ISR のセルラー インターフェイスを設定する例を示します。

例：基本のセルラー設定

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

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
!
controller Cellular 0
!
!
interface Cellular0
ip address negotiated
encapsulation slip
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
async mode interactive
routing dynamic
!
dialer-list 1 protocol ip permit
!
line 3
script dialer lte
modem InOut
no exec
transport input all
transport output all
!
```

例：外部ダイヤラ インターフェイスを使用しない dialer-watch の設定

次に、外部ダイヤラ インターフェイスを使用しないダイヤラウォッチを設定する例を示します。太字テキストはダイヤラウォッチに固有の重要なコマンドを示します。

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
interface Cellular0
ip address negotiated
encapsulation slip
dialer in-band
dialer string LTE
dialer watch-group 1
async mode interactive
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
!
ip route 0.0.0.0 0.0.0.0 cellular 0
line 3
script dialer LTE
modem InOut
no exec
transport input all
transport output all
```

例：外部ダイヤラ インターフェイスを使用する dialer-persistent の設定

次に、外部ダイヤラ インターフェイスを使用する dialer-persistent を設定する例を示します。太字テキストは dialer-persistent に固有の重要なコマンドを示します。

```
interface Cellular0
ip address negotiated
encapsulation slip
dialer in-band
dialer pool-member 1
async mode interactive
routing dynamic
interface Dialer1
ip address negotiated
encapsulation slip
dialer pool 1
dialer idle-timeout 0
dialer string lte
dialer persistent
dialer-group 1
!
dialer-list 1 protocol ip permit
ip route 0.0.0.0 0.0.0.0 dialer 1
line 3
script dialer lte
modem InOut
no exec
transport input all
transport output all
```

例：セルラー インターフェイスの設定を介した GRE トンネル

次に、GRE トンネル インターフェイスが ip address unnumbered cellular interface で設定されている場合に、スタティック IP アドレスを設定する例を示します。

（注） GRE トンネルの設定は、サービス プロバイダーが LTE インターフェイスのパブリック IP アドレスを提供している場合にだけサポートされます。

（注） プライベート IP アドレスを使用するサービス プロバイダーの場合、ポイントツーポイント スタティック GRE トンネルの一方のエンドをプライベート IP アドレスに、もう一方のエンドをパブリック IP アドレスに設定することはできません。

```
interface Tunnel2
ip unnumbered <internal LAN interface GE0/0 etc.>
tunnel source Cellular0
tunnel destination a.b.c.d
interface Cellular0
ip address negotiated
encapsulation slip
no ip mroute-cache
dialer in-band
dialer string lte
dialer-group 1
async mode interactive
! traffic of interest through the tunnel/cellular interface
ip route x.x.x.x 255.0.0.0 Tunnel2
! route for the tunnel destination via cellular
ip route a.b.c.d 255.255.255.255 cellular 0
```

モデム ファームウェアのアップグレード

Cisco 800 シリーズ 4G LTE ISR のモデム ファームウェアをアップグレードする方法については、『Cisco 4G LTE ソフトウェア インストール ガイド』の「モデム ファームウェアのアップグレード」の項を参照してください。

トラブルシューティング

Cisco 800 シリーズ 4G LTE ISR のトラブルシューティングの手順については、『Cisco 4G LTE ソフトウェア インストール ガイド』の「トラブルシューティング」の項を参照してください。

Cisco 880G シリーズ ISR での 3G のサポート

第 3 世代（3G）ワイヤレス WAN（WWAN）オプションが組み込まれた Cisco 880G シリーズ サービス統合型ルータ（ISR）は、安全なデータ通信のためのコラボレーション ビジネス ソリューションを小企業および企業に提供します。

Cisco 880G シリーズ ISRS が対応している 3G 標準は次のとおりです。

- HSPA+、HSPA、UMTS、EDGE、および GPRS をサポートする、第 3 世代パートナー プロジェクト（3GPP）に基づいた GMS および UMTS モデル。
  Cisco 880G シリーズ ISR に 3G HSPA または HSPA+ を設定する方法については、次のリンクを参照してください。

- http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwls_hspa.html
- http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwlsgsm.html

- EVDO、EVDO Rev A モードをサポートする、3GPP2 に基づく CDMA モデル。
  Cisco 880G シリーズ ISR に EVDO を設定する方法については、次のリンクを参照してください。
  - http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwls_evdo.html
  - http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/mrwlcdma.html

サポートされている Cisco 880G シリーズ モデルの詳細については、以下にある Cisco 880G シリーズ ISR データ シートを参照してください：

http://www.cisco.com/en/US/prod/collateral/routers/ps380/ps10082/data_sheet_c78-682548.html

第 16 章

DHCP および VLAN による LAN の設定

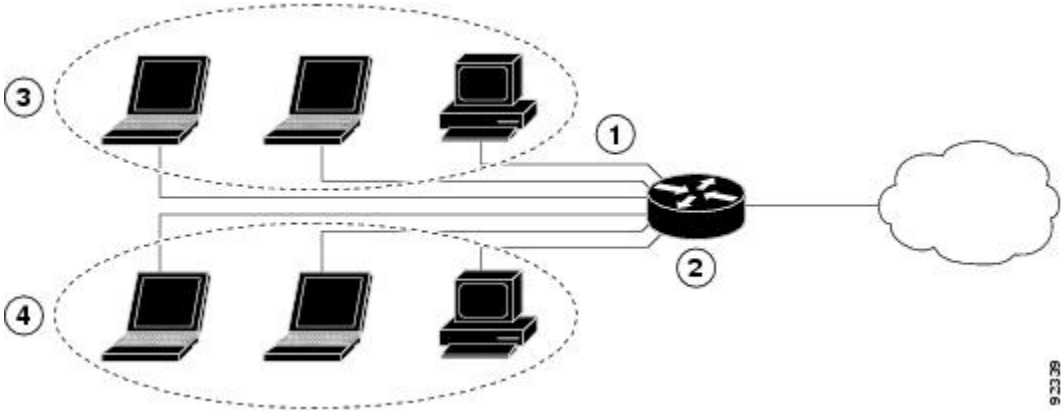
Cisco 819、Cisco 860、および Cisco 880 サービス統合型ルータ（ISR）は、物理 LAN および仮想 LAN（VLAN）の両方でクライアントをサポートします。

DHCP および VLAN による LAN の設定

Cisco 819、Cisco 860、および Cisco 880 サービス統合型ルータ（ISR）は、物理 LAN および仮想 LAN（VLAN）の両方で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。

以下の図に、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 *18*：*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ている、Cisco 819、Cisco 860、Cisco 880 ISR などのルータと DHCP サーバ
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。

（注） Cisco 800 シリーズ ルータは、DHCP スヌーピングをサポートしません。

VLANs

Cisco 819、Cisco 860、Cisco 880 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、ユーザの物理的な場所または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。

DHCP および 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、「ルータの基本設定」、およびEasy VPN および IPSec トンネルを使用した VPN の設定, （421 ページ）を参照してください。

DHCP の設定

DHCP 動作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 モードから始め、次の手順を実行します。

手順の概要

1. **ipdomainname** *name*
2. **ipname-server** *server-address1 [server-address2...server-address6]*
3. **ipdhcpexcluded-address** *low-address [high-address]*
4. **ipdhcppool** *name*
5. **network** *network-number [mask| prefix-length]*
6. **importall**
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	**ipdomainname** *name* 例： `Router(config)# ip domain smallbiz.com`	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	**ipname-server** *server-address1 [server-address2...server-address6]* 例： `Router(config)# ip name-server192.168.11.12`	名前およびアドレス解決に使用する 1 つ以上のドメイン ネーム システム（DNS）サーバのアドレスを指定します。

	コマンドまたはアクション	目的
ステップ 3	**ipdhcpexcluded-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	**ipdhcppool** *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`	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	**importall** 例： `Router(config-dhcp)# import all`	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`	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`	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。
ステップ 9	**domain-name** *domain* 例： `Router(config-dhcp)#domain-name cisco.com`	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`	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：DHCP

次の設定例は、この章で説明したDCHP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。

- **showipdhcpimport**：DHCPサーバデータベースにインポートされたオプション パラメータを表示します。
- **showipdhcppool**：DHCP アドレス プールに関する情報を表示します。
- **showipdhcpserverstatistics**：アドレス プール数、バインディング数などの DHCP サーバの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 モードから始め、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 t`
	`Router(config)#vlan 2`
		VLAN 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	**exit** 例： `Router(config-vlan)#exit`	VLAN データベースを更新し、それを管理ドメイン全体に伝播して、グローバル コンフィギュレーション モードに戻ります。

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. **switchportaccessvlan** *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`	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	**switchportaccessvlan** *vlan-id* 例： `Router(config-if)# switchport access vlan 2`	VLAN にポートを割り当てます。
ステップ 3	**end** 例： `Router(config-if)#end`	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 設定の確認

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
```

第 17 章

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 819、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。

Easy VPN および IPSec トンネルを使用した VPN の設定

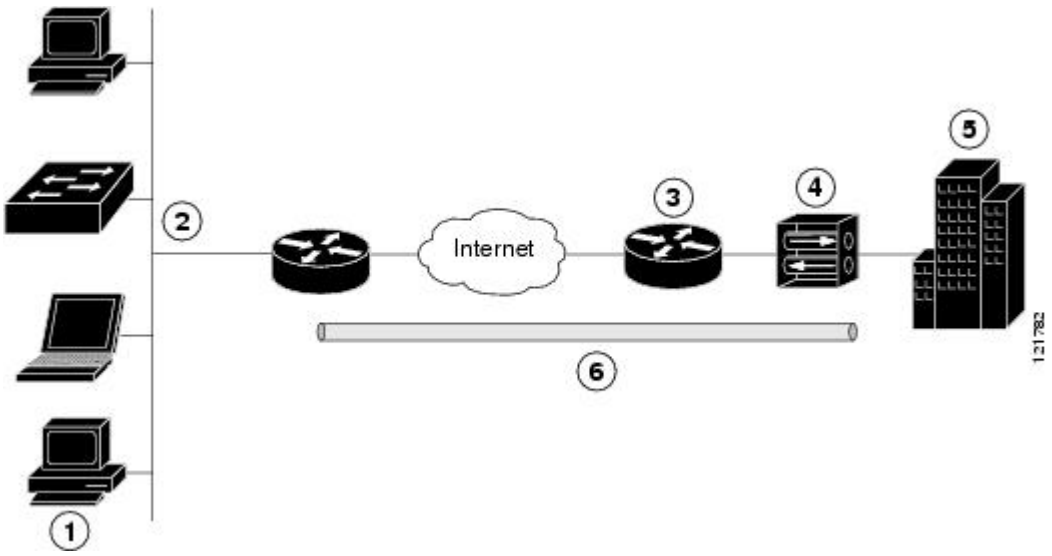
Cisco ルータと他のブロードバンド デバイスは、インターネットへの高パフォーマンスな接続を提供しますが、多くのアプリケーションでは、高レベルの認証を実行し、2 つの特定のエンドポイント間でデータを暗号化する VPN 接続のセキュリティも必要です。

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。

Easy VPN および IPSec トンネルを使用した VPN の設定

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。以下の図は、一般的な導入シナリオです。

図 *19*：*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 および IPSec トンネルを使用した VPN の設定

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 819、Cisco 860、および Cisco 880 シリーズ ISR などの 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 およびネットワーク アドレス変換/ピア アドレス変換（NAT/PAT）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, （424 ページ）
- グループ ポリシー情報の設定, （425 ページ）
- クリプト マップへのモード設定の適用, （427 ページ）
- ポリシー ルックアップの有効化, （427 ページ）
- IPSec トランスフォームおよびプロトコルの設定, （428 ページ）
- IPSec 暗号方式およびパラメータの設定, （430 ページ）
- 物理インターフェイスへのクリプト マップの適用, （431 ページ）
- Easy VPN リモート コンフィギュレーションの作成, （432 ページ）

この設定タスクの結果を示す例は、VPN および IPSec の設定例, （434 ページ）をご覧ください。

（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、ご使用のルータに合わせて、「ルータの基本設定」、「PPP over Ethernet と NAT の設定」、「『Configuring PPP over ATM with NAT』」、およびDHCP および VLAN による LAN の設定, （413 ページ）を参照してください。

（注） この章の例は、Cisco 819、860 および 880 シリーズ ルータのエンドポイント設定のみを示しています。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

インターネット キー交換（IKE）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. **cryptoisakmppolicy** *priority*
2. **encryption{des|3des|aes|aes192|aes256}**
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	**cryptoisakmppolicy** *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、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（ISAKMP）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|aes192|aes256}** 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 データ暗号規格（DES）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。

	コマンドまたはアクション	目的
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. **cryptoisakmpclientconfigurationgroup** {**group-name** | **default**}
2. **key** *name*
3. dns *primary-server*
4. **domain** *name*
5. **exit**
6. **iplocalpool**{**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	**cryptoisakmpclientconfigurationgroup** {**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`	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 ドメイン ネーム システム（DNS）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 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	**iplocalpool**{**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. **cryptomap** *map-name***isakmpauthorizationlist** *list-name*
2. **cryptomap** *tag***clientconfigurationaddress[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	**cryptomap** *map-name***isakmpauthorizationlist** *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、認証、許可、アカウンティング（AAA）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	**cryptomap** *tag***clientconfigurationaddress[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 ルックアップの有効化

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. **aaanew-model**
2. **aaaauthenticationlogin{default|** *list-name***}** *method1***[***method2...***]**
3. **aaaauthorization{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	**aaanew-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	**aaaauthenticationlogin{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 3	**aaaauthorization{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`	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. **cryptoipsectransform-set***transform-set-name transform1 [transform2] [transform3] [transform4]*
2. **cryptoipsecsecurity-associationlifetime***{***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	**cryptoipsectransform-set***transform-set-name transform1 [transform2] [transform3] [transform4]* 例： `Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac` 例：	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	**cryptoipsecsecurity-associationlifetime***{***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。

次の作業

（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. **cryptodynamic-map** *dynamic-map-name dynamic-seq-num*
2. **settransform-set***transform-set-name [transform-set-name2...transform-set-name6]*
3. **reverse-route**
4. **exit**
5. **cryptomap** *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	**cryptodynamic-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	**settransform-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。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		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	**cryptomap** *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、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. **cryptomap** *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	**cryptomap** *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。

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. **cryptoipsecclientezvpn** *name*
2. **group** *group-name***key** *group-key*
3. **peer** {*ipaddress* | *hostname*}
4. **mode** {**client** | **network-extension** | **networkextensionplus**}
5. **exit**
6. **interface** *type number*
7. **cryptoipsecclientezvpn***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	**cryptoipsecclientezvpn** *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** | **networkextensionplus**}
	
	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 **interfaceatm0** になります。

	コマンドまたはアクション	目的

ステップ 7	**cryptoipsecclientezvpn***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
```

VPN および IPSec の設定例

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
!
```

第 18 章

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

第 19 章

VDSL2 ボンディングとシングルワイヤ ペアの設定

VDSL2（Very-high-bit-rate Digital Subscriber Line 2）ボンディングは、キャパシティを増やすか、または銅線ネットワークのリーチを拡張するために2つの銅線ペアを結合します。顧客にとっては、より長いループで、データ レートと操作が強化されることになります。シングルワイヤ ペアでは、回線 0 にプロファイル 8a ～ 17a および ADSL、回線 1 にプロファイル 8a ～ 30a を設定できます。VDSL2 ボンディングとシングルワイヤ ペアは、**C897VAB-K9** シリーズ ルータでサポートされます。

この章の内容は、次のとおりです。

制約事項

Cisco 800 シリーズ ルータには、VDSL2 ボンディングについて次の制約事項があります。

- VDSL2 ボンディングは、C897VAB-K9 シリーズ ルータでのみサポートされます。
- C897VAB-K9 がボンディング用 SKU であっても、ボンディングはデフォルトの設定ではありません。ADSL モードと VDSL シングルワイヤ モードは、デフォルト設定でサポートされています。ボンディングは、**line-mode bonding** コマンドを使用して有効にします。
- **no line-mode bonding** および **default line-mode bonding** コマンドは、回線 0 の設定をデフォルト設定である「シングルワイヤ」に変更します。

- line-mode の設定は、動作モードを変更するたびにルータから削除されます。新しい動作モードでは、コマンドを再度実行してボンディングを設定する必要があります。

auto モードのボンディングの設定

ボンディングは、**auto** モード、または **VDSL2** のいずれかで設定できます。デフォルト設定は **auto** です。

auto モードでボンディングを設定するには以下のタスクを実行します。

手順の概要

1. **configure terminal**
2. **controller VDSL** *slot*
3. **operating mode** *mode*
4. **line-mode bonding**
5. **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	**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）。
ステップ 2	**controller VDSL** *slot* 例： `router(config)# controller vdsl 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。
ステップ 3	**operating mode** *mode* 例： `router(config)# operating mode auto`	動作モードを指定します。動作モードは **auto** です。
ステップ 4	**line-mode bonding** 例： `router(config-controller)# line-mode bonding`	CPE でボンディング モードを有効にします。
ステップ 5	**exit** 例： `router(config-controller)# exit`	コントローラ コンフィギュレーション モードを終了します。

VDSL2 モードでのボンディングの設定

VDSL2 モードでボンディングを設定するには以下のタスクを実行します。

手順の概要

1. **configure terminal**
2. **controller VDSL** *slot*
3. **operating mode** *mode*
4. **line-mode bonding**
5. **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	**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）。
ステップ 2	**controller VDSL** *slot* 例： `router(config)# controller vdsl 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。
ステップ 3	**operating mode** *mode* 例： `router(config)# operating mode vdsl2`	動作モードを指定します。動作モードは VDSL2 です。
ステップ 4	**line-mode bonding** 例： `router(config-controller)# line-mode bonding`	CPE でボンディング モードを有効にします。
ステップ 5	**exit** 例： `router(config-controller)# exit`	コントローラ モードを終了します。

回線 0 のシングルワイヤ ペアの設定

回線 0 にシングルワイヤ ペアを設定するには、以下のタスクを実行します。

手順の概要

1. **configure terminal**
2. **controller VDSL** *slot*
3. **line-mode single-wire line** *line-number*
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	**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）。
ステップ 2	**controller VDSL** *slot* 例： `router(config)# controller vdsl 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。
ステップ 3	**line-mode single-wire line** *line-number* 例： `router(config-controller)# line-mode single-wire line 0`	シングルワイヤ（ボンディングなし）モードで、回線 0 上の 8a ～ 17a のプロファイルおよび ADSL を有効にします。
ステップ 4	**exit** 例： `router(config-controller)# exit`	コントローラ コンフィギュレーション モードを終了します。

回線 1 のシングルワイヤ ペアの設定

回線 1 にシングルワイヤ ペアを設定するには、以下のタスクを実行します。

手順の概要

1. **configure terminal**
2. **controller VDSL** *slot*
3. **line-mode single-wire line** *line-number* [profile 30a]
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	**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）。
ステップ 2	**controller VDSL** *slot* 例： `router(config)# controller vdsl 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。
ステップ 3	**line-mode single-wire line** *line-number* [profile 30a] 例： `router(config-controller)# line-mode single-wire line 1 profile 30a`	シングルワイヤ（ボンディングなし）モードで、回線 1 のプロファイル 8a ～ 30a を有効にします。プロファイル 30 a を指定しない場合、その回線ではプロファイル 8a ～ 17a が有効になります。
ステップ 4	**exit** 例： `router(config-controller)# exit`	コントローラ モードを終了します。

設定例

ボンディングを auto モードで有効にする例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config)# operating mode auto
router(config-controller)# line-mode bonding
router(config-controller)# exit
```

次に、VDSL2 ボンディングを有効にする例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config)# operating mode vdsl2
router(config-controller)# line-mode bonding
router(config-controller)# exit
```

次に、ボンディングを削除する例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config)# no operating mode
router(config-controller)# no line-mode bonding
router(config-controller)# exit
```

次に、回線 0 でプロファイル 8a から 17a を有効にする例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
```

```
router(config-controller)# line-mode single-wire line 0
router(config-controller)# exit
```

次に、回線 1 でプロファイル 30a を有効にする例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config-controller)# line-mode single-wire line 1 profile 30a
router(config-controller)# exit
```

次に、回線 1 からプロファイル 30a を削除する例を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config-controller)# no line-mode single-wire line 1
router(config-controller)# exit
```

第 20 章

Cisco IOx の設定

Cisco IOx は、エンドツーエンドアプリケーションイネーブルメントプラットフォームであり、さまざまなプラットフォームで構成される Cisco ネットワーク全体で、アプリケーションのタイプに関係なく、統一された一貫した方法のアプリケーション ホスティング機能を提供します。IOx プラットフォームにより、開発、配布、導入、ホスティング、モニタリング、管理を含むアプリケーションのライフ サイクル全体を管理することができます。この章では、Cisco 819 と 800M シリーズのルータに Cisco IOx を設定する方法について説明します。

この章の内容は、次のとおりです。

Cisco IOx の設定

お使いのデバイスにアプリケーションを展開する前に、IOx を設定する必要があります。Cisco 800 シリーズ ルータで、IOS イメージはコア 1、IOx はコア 2 で実行されます。IOx の設定には、お使いのデバイスのコア 2 で IOx フレームワークを有効にする作業が含まれます。

（注） デバイスに IOx を設定するには、前提条件として IOx をサポートする IOS イメージが必要です。IOS イメージは 15.5(1)T 以降である必要があります。

次のタスクを実行して、IOx を設定します。

ステップ 1 特権 EXEC プロンプトで configure terminal コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

ステップ 2 interface コマンドを入力します。インターフェイス タイプ、スロット番号、ポート番号を指定し、設定するインターフェイスを特定します。ここで設定するインターフェイスは、ギガビットイーサネットのような物理的なインターフェイスです。このインターフェイスをコア 1 およびコア 2 の外部接続用に設定します。

```
Router(config)#interface GigabitEthernet0
Router(config-if)#
```

ステップ 3 インターフェイスに **IP アドレス**と**サブネット マスク**を割り当てます。**no shutdown** を入力し、インターフェイスを有効にします。**ip nat outside** を入力し、インターフェイスが外部ネットワークに接続するように指定します。**Exit** を入力して、インターフェイス モードを終了します。

```
Router(config-if)#ip address 172.x.x.x 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
```

ステップ 4 ip route コマンドを入力し、インターフェイス間でスタティック ルートを確立します。ip default-gateway コマンドを入力し、デフォルト ゲートウェイを指定します。

```
Router(config)#ip route 0.0.0.0 0.0.0.0 172.x.x.x
Router(config)#ip default-gateway 172.x.x.x
```

ステップ 5 interface コマンドを入力し、ルータのコア 1 およびコア 2 が通信できるようにする内部インターフェイスを指定します。インターフェイス名は、Cisco 819 シリーズ ルータの場合は **ethernet1**、Cisco 800 M シリーズ ルータの場合は **ethernet0**/1 にします。このインターフェイスには、他の名前を使用しないでください。このインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。**ip nat inside** を入力し、インターフェイスが内部ネットワークに接続されていることを指定します（ネットワークは NAT 変換を行う）。Exit を入力して、インターフェイス モードを終了します。

```
Router(config)#interface ethernet1
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
```

ステップ 6 iox コマンドを入力し、IOx コンフィグレーション モードを開始します。

```
Router(config)#iox
Router(config-iox)#
```

ステップ 7 **ホスト**の **IP アドレス**および**デフォルト ゲートウェイ**を設定します。デフォルト ゲートウェイの IP アドレスと先に設定した **ethenet1** の IP アドレスは同じにする必要があります。Exit を入力して、IOx モードを終了します。

```
Router(config-iox)host ip address 192.168.3.2 255.255.255.0
Router(config-iox)host ip default-gateway 192.168.3.1
Router(config-iox)exit
```

ステップ 8 次に、アプリケーション トラフィックに NAT ルールを設定する必要があります。ip nat inside source list overload コマンドを入力します。このコマンドは、ルータで多数のローカル アドレスに 1 つのグローバル アドレスを使用できるようにします。オーバーロードを設定すると、各内部ホストの TCP または UDP ポート番号により、同じローカル IP アドレスを使用している複数の会話が区別されるようになります。発信元アドレスを持ち、アクセス リストを渡すパケットは、名前付きプールにあるグローバル アドレスを使用して動的に変換されます。ip access-list standard コマンドを入力し、標準の IP アクセス リストを指定します。permit コマンドを入力し、名前付きプールからのパケットを許可します。

```
Router(config)#ip nat inside source list NAT_ACL interface GigabitEthernet0 overload
Router(config)#ip access-list standard NAT_ACL
Router(config-std-nacl)#permit 192.168.0.0 0.0.1.255
Router(config-std-nacl)#exit
```

ステップ 9 最後に、ブラウザ トラフィックを IOS 経由でセカンド コア Web サーバに 8443 ポートを使用して振り向けるように PAT エントリを指定します。

```
Router(config)#ip nat inside source static tcp 192.168.3.2 8443 interface gigabitEthernet0 8443
```

設定例

次に、3 つの異なるユース ケースの例を示します。

- ネットワークのエッジにあるルータ（イーサネットによる開発者モード）
- ネットワークの真中にあるルータ（イーサネットによる据え置き型）
- ネットワークの真中にあるルータ（セルラーによるモバイル型）

イーサネットによる開発者モード

このシナリオでは、次のようになります。

- ルータは実際のルーティングには使用されません。ルータはネットワークのエッジにあります。
- このモードは、外部のネットワークにアクセスするアプリケーションだけが必要なユーザに適しています。
- アプリケーションは NAT の背後あります。このため、ローカル IP アドレスを割り当てる DHCP プールを IOS に設定します。

次のタスクを実行して、IOx を設定します。

ステップ 1 特権 EXEC プロンプトで configure terminal コマンドを入力して、グローバル コンフィギュレーション モードを開始します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

ステップ 2 最初に、アプリケーションと通信する **VirtualPortGroup** インターフェイスを設定します。interface コマンドを入力し、セカンド コアで実行する単独の IOx アプリケーションの仮想インターフェイスを指定します。このインターフェイスは、アプリケーション トラフィックをルーティングします。インターフェイスの名前は **virtualportgroup0** にしてください。このインターフェイスには、他の名前を使用しないでください。仮想インターフェイスに **IP アドレス**と**サブネット マスク**を割り当てます。ip nat inside コマンドを入力し、インターフェイスが内部ネットワークに接続されていることを指定します（ネットワークは NAT 変換を行う）。

```
Router(config)#interface VirtualPortGroup0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
```

ステップ 3 IOS に DHCP ネットワーク プールを設定します。このプールからアプリケーションは DHCP 経由で IP アドレスを取得します。割り当てに使用しないアドレスを指定します。

```
Router(config)#ip dhcp excluded-address 192.168.1.0 192.168.1.5
```

ステップ 4 ネットワークに DHCP プールを設定します（この場合 192.168.1.0/24）。

```
Router(config)#ip dhcp pool iox-apps
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#domain-name sample.com
Router(dhcp-config)#dns-server 171.70.168.183
Router(dhcp-config)#option 42 ip 171.68.38.65 172.x.x.x
Router(dhcp-config)#exit
```

option 42 コマンドは NTP サーバの詳細をアプリケーションに送信します。IP アドレス 171.68.38.65 はパブリック NTP サーバの IP アドレス、172.x.x.x は GE0 インターフェイスの IP アドレスです。

ステップ 5 最後に、ntp マスター コマンドを使用して、バックアップ用にローカル NTP サーバを設定します。

```
Router(config)#ntp master
Router(config)#exit
```

アプリケーションは、日時の同期にタイムサーバを使用します。NTP サーバはルータに対してローカル、またはパブリックです。サーバがルータに対してローカルの場合、最初にルータを設定する必要があります。コマンドは ntp master です。EXEC モードで clock read-calendar コマンドを使用し、ルータのクロックとハードウェアのクロックを同期します（まだの場合）。

イーサネットによる固定型

このシナリオでは、次のようになります。

- ルータは実際のルーティングに使用されます。ルータはネットワークの真中にあります。
- このモードは、外部のネットワークにアクセスする、または外部のネットワークからアクセス可能なアプリケーションが必要なユーザに適しています。
- アプリケーションは NAT の背後にありません。
- VirtualPortGroup は、外部インターフェイスの IP アドレスを借用します。これにより、ルータの外部から到達できるようになります。
- アプリケーションは、VirtualPortGroup 経由で DHCP 要求を中継することで、外部の DHCP サーバからインターフェイスの IP アドレスを取得します。また、外部の IP アドレスも取得します。

次のタスクを実行して、IOx を設定します。

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	特権 EXEC プロンプトで configure terminal コマンドを入力して、グローバル コンフィギュレーション モードを開始します。	`Router# configure terminal`
		`Enter configuration commands, one per line. End with CNTL/Z.`
		`Router(config)#`

ステップ 2	アプリケーションと通信する VirtualPortGroup インターフェイスを設定します。このシナリオでは DHCP サーバは外部になるため、VirtualPortGroup に IP ヘルパー アドレスを設定する必要があります。	`Router(config)#interface VirtualPortGroup0`
		`Router(config-if)#ip unnumbered GigabitEthernet0`
		`Router(config-if)#ip helper-address 1.100.30.114`
		`Router(config-if)#no shutdown`
		`Router(config-if)#exit`
		`Router(config)#exit`

セルラーによるモバイル型

このシナリオでは、次のようになります。

- ルータはセルラー接続性を備えたモバイル型です（WAN リンクのみ）。
- VirtualPortGroup とアプリケーションは NAT の背後にあり、セルラー インターフェイスの IP アドレスをオーバーロードします。
- アプリケーションは、内部の DHCP から IP アドレスを取得します。

- アプリケーション管理モデルは、携帯電話サービス プロバイダーに登録している IP アドレスの種類がパブリックとプライベートのどちらかによって異なります。

このモードでは、次のようになります。

- GigabitEthernet インターフェイスの代わりに、WAN リンクとしてセルラー インターフェイスを設定します。
- デフォルト ルート、NAT アドレス オーバーロード、PAT に対して、参照をセルラー インターフェイス（GigabitEthernet ではなく）に変更します。
- VirtualPortGroup に専用の IP アドレスを割り当てます。
- アプリケーションに、ローカルの DHCP プールを設定します。

次のタスクを実行して、IOx を設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ダイヤラの開始時に、Cellular modem AT コマンドを定義します。	`Router#config terminal` `Router(config)#chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"`

ステップ 2	セルラー コントローラを設定します。	`Router(config)#controller cellular 0`
		`Router(config-controller)#lte gps mode standalone`
		`Router(config-controller)#lte gps nmea ip`
		`Router(config-controller)#lte modem link-recovery rssi onset-threshold -110`
		`Router(config-controller)#lte modem link-recovery monitor-timer 20`
		`Router(config-controller)#lte modem link-recovery wait-timer 10`
		`Router(config-controller)#lte modem link-recovery debounce-count 5`

ステップ 3	セルラー インターフェイスを設定します。	`Router(config-controller)#interface cellular 0`
		`Router(config-if)#ip address negotiated`
		`Router(config-if)#ip nat outside`
		`Router(config-if)#ip virtual-reassembly in`
		`Router(config-if)#encapsulation slip`
		`Router(config-if)#load-interval 30`
		`Router(config-if)#dialer in-band`
		`Router(config-if)#dialer idle-timeout 0`
		`Router(config-if)#dialer string lte`
		`Router(config-if)#dialer-group 1`
		`Router(config-if)#no peer default ip address`
		`Router(config-if)#async mode interactive`
		`Router(config-if)#routing dynamic`
		`Router(config-if)#exit`

ステップ 4	関係するトラフィックに関するDDRにダイヤラ リストを作成します。	`Router(config)#dialer-list 1 protocol ip permit`

ステップ 5	最後に、回線設定（常に回線3を使用）を指定し、デフォルトのモデム チャット スクリプトを定義します。	`Router(config)#line 3`
		`Router(config-line)#script dialer lte`
		`Router(config-line)#modem inout`

セルラー IP アドレス タイプ

ユーザがセルラーサービスに登録すると、デフォルトでは、サービスプロバイダーがプライベートIPアドレスを割り当てます。ただし、パブリックアドレスを選択する方法もあります。いずれの場合もほぼ同じ IOS の設定が機能しますが、以下の表でこの 2 つの主な違いと IOx アプリケーションへの影響について説明します。

表 *44* : セルラー *IP* アドレス タイプ

	パブリック IP アドレス	プライベート IP アドレス
ルーティング	インターネット スペースでルーティング可能。	アドレスはプロバイダーのドメイン専用のため、インターネット スペースでルーティングできるようにするには、パブリック アドレスに変換する必要があります。
可用性とコスト	可用性および追加料金については、ご利用のローカル プロバイダーに確認してください。	ほとんどのプロバイダーが共通の規定を提供。

スタティックとダイナミック	スタティック。	通常はダイナミック。これはルータがセルラーネットワークに接続し直すたびに（ルータのリロード後やセルラーインターフェイスのリセット後など）、ほとんどの場合はアドレスが変更されることを意味します。

IOx アプリケーション管理	Stationary Ethernet モードと同じ。	

			ルータはプロバイダーの NAT の背後にあるため、ユーザがルータの Web サーバポートにアクセスすることはできません。このため、アプリケーションは IOS 仮想サービス CLI を使用して、ルータのコンソールポート経由、または LAN スイッチポート経由でローカルでのみ管理できま

		す。

Local Manager の Web インターフェイスへのアクセス

ルータに IOx を設定すると、IOx アプリケーションを管理するための Web インターフェイスにアクセスできます。ルータのギガビットイーサネットインターフェイスの IP アドレスを使用して、Web URL が生成されます。たとえば、GE インターフェイスの IP アドレスが 172.x.x.x の場合、Local Manager の Web URL は https:// 172.x.x.x:8443 になります。

自分のユーザ名とパスワードを使用して、Local Manager にログインします。ユーザ名とパスワードは、ルータへのログインに使用したユーザ名とパスワードに対して認証されます。Web インターフェイスにアクセスするには、**privilege 15** が必要です。次に、ルータで **privilege 15** を有効にする例を示します。

username *username* **privilege 15 password 0** *password*

Local Manager にログインし、デバイス（819 および 800M）を追加します。

NTP サーバの設定

すべての IOx コンポーネント（ルータ、アプリケーション、Fog Director など）が同じ NTP サーバと同期するように NTP サーバを設定します。これにより、IOS と IOx は必ず同じ日時を使用します。次の設定を使用します。

```
ntp update-calendar
ntp server 10.64.58.50
```

ブリッジ モードおよび NAT ネットワーキング モードを使用してインストールしたアプリケーションに対する IOS NAT の設定

ブリッジまたは NAT ネットワーキング モードを使用して App をインストールした場合は、IOS 側の対応する NAT の設定を行う必要があります。

App は、IOS 上に構成されている DHCP サーバから IP アドレスを取得します。

ブリッジ モード：

- App のインストール時にブリッジモードを選択します（Local Manager または Fog Director）。
- FD または LM のデバイス詳細ページでは以下がわかります。
  - App に割り当てられている IP アドレス
  - App に要求された TCP および UDP ポート

- App に要求されたポートに対応する内部および外部ポート番号

次にブリッジ モードの App の例を示します。

- PaaS App がポート TCP:9000 および UDP:12000 を package.yaml でリクエストしている。
- IOS に設定されている DHCP サーバからこの App に割り当てられた IP は 192.168.1.46 である。
- 内部と外部の両方のポート番号が同じになる。

IOS 側で次の NAT 設定を実行し、App に到着するトラフィックに備える必要があります。

```
ip nat inside source static tcp 192.168.1.46 9000 interface gabitEthernet0 9000
ip nat inside source static udp 192.168.1.46 12000 interface gigabitEthernet0 12000
```

センサーは TCP / UDP トラフィックを次の IP に送信する必要があります。

TCP ポート：<Router_Wan_IP>:9000
UDP ポート：<Router_Wan_IP>:12000

これは以下に変換されます。

TCP ポート：192.168.1.46:9000
UDP ポート：192.168.1.46:12000

NAT モード：

App が NAT モードでインストールされている場合は、次の設定を実行する必要があります。

- App のインストール時に FD または LM で NAT モードを選択します。
- IOx は IOx 内の DHCP サーバから IP アドレスを提供します。
- CAF は、192.168.223.x の範囲の DHCP IP アドレスを提供します。
- CAF は、App に要求されたポートに対応する内部および外部ポートを提供します。
- FD または LM のデバイス詳細ページでは以下がわかります。
  - App に割り当てられている IP アドレス
  - App に要求された TCP および UDP ポート
  - App に要求されたポートに対応する内部および外部ポート番号
  - 外部と内部のポート番号は異なります。

NAT モードで、IOx/GOS の開始時に割り当てられる IOx svcbr_0 IP アドレス（192.168.1.6）に対する NAT ルールを設定する必要があります。

TCP：< Router_Wan_ip >: 40000
UDP：< Router_Wan_ip >: 42000

これは以下に変換されます。

192.168.1.6:40000
192.168.1.6:42000

さらに、次の App IP に変換されます。

192.223.1.10:9000
192.223.1.10:12000

IOS 側で次の NAT 設定を実行します。

```
ip nat inside source static tcp 192.168.1.6 40000 interface gabitEthernet0 40000
ip nat inside source static udp 192.168.1.6 42000 interface gabitEthernet0 42000
```

ゲスト シリアルの設定

この機能により、インストールされている IOx アプリケーションは、ルータのシリアル インターフェイスにアクセスできます。この設定は、すべてのアプリケーションで必要な設定ではないためオプションです。

次に、Cisco 819 ルータのシリアル ポート s0 をゲストに接続する方法の例を示します。

```
interface serial0
physical-layer async
vrf forwarding internal-score-vrf
no ip address
encapsulation raw-tcp
end
line 7
raw-socket tcp client 192.168.3.2 32000
```

raw-socket tcp client コマンドで、192.168.3.2 はホスト Linux の IP アドレスであり、32000 はシリアル TCP ポートです。

Cisco 800M シリーズ ルータで、インターフェイス名は、モジュール スロットによって **serial0/0/0** または **serial0/1/0** のいずれかになります。

次に、Cisco 800M シリーズ ルータの slot 0 に取り付けられているモジュールを設定する方法の例を示します。

```
interface Serial0/0/0
physical-layer async
no ip address
encapsulation raw-tcp
!
line 3
raw-socket tcp client 192.168.3.2 32000
```

次に、Cisco 800M シリーズ ルータの slot 1 に取り付けられているモジュールを設定する方法の例を示します。

```
interface Serial0/1/0
physical-layer async
no ip address
encapsulation raw-tcp
end
line 19
raw-socket tcp client 192.168.3.2 32001
```

（注） Cisco 819 のシリアル インターフェイス **s0** に関連付けられている非同期回線は 7 です。Cisco 800M ルータのシリアル インターフェイス **s0/0/0** および **s0/1/0** に関連付けられている非同期回線はそれぞれ 3 と 19 です。

非同期回線はデフォルトで、9600 ボー、パリティなし、1 ストップ ビットに設定されます。すべての TTY 端末設定は、IOS で非同期回線として設定する必要があります。次の例は、ボー レートを 115Kbps に変更する方法を示しています。

```
line 7
raw-socket tcp client 192.168.3.2 32000
stopbits 1
speed 115200

819-42#show line 7
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
      7 TTY 115200/115200-    -      -    -    -      0       0     0/0     Se0

Line 7, Location: "", Type: ""
```

Cisco IOx のアップグレード

IOx は IOS を変更せずに個別にアップグレードできます。次に、IOx をアップグレードする方法を示します。

```
Router#configure terminal
Router#iox
 host ip address 192.168.3.2 255.255.255.0
 host ip default-gateway 192.168.3.1
 host boot flash:p1021_c800.xxxxx.bin   <<<<<<<<<<< new image for IOX
Router#write
Router#reload
```

トラブルシューティング

このセクションでは、IOS と IOx のトラブルシューティングの方法について説明します。

IOS のデバッグ

IOS をデバッグするには、次のコマンドを使用します。

表 *45* : *IOS* のデバッグ コマンド

コマンド	説明	例

debug iox config level error	IOx の設定エラーをデバッグします。	`Router#debug iox config level error`
		`*Oct 7 08:30:27.951 PDT:`
		`if_c800_iox_infra_cli_handler.c ::`
		`debug_iox_configuration_command_han`
		`dler() : 242 - Changed`
		`configuration debug level to 3`
		`iox_819_2#`
		`iox_819_2#`
		`iox_819_2#conf t`
		`Enter configuration commands, one`
		`per line. End with CNTL/Z.`
		`iox_819_2(config)#iox`
		`iox_819_2(config-iox)#host ip add`
		`192.168.100.2 255.255.255.0`
		`iox_819_2(config-iox)#`
		`*Oct 7 08:30:44.043 PDT:`
		`if_c800_iox_trans_mgr.c ::`
		`iox_create_transaction() : 50 -`
		`Created transaction: tid=14,`
		`pid=155`
		`*Oct 7 08:30:44.043 PDT:`
		`if_c800_iox_cli_handler.c ::`
		`cfg_iox_host_ip_address_cmd_handler`
		`() : 387 - host ip address entered`
		`address: 192.168.100.2 mask:`
		`255.255.255.0`
		`*Oct 7 08:30:44.043 PDT:`
		`if_c800_iox_cli_handler.c ::`
		`iox_validate_host_ip_address() :`
		`309 - All checks passed`
		`.....`

debug iox config level debug	IOx の設定をデバッグします。	`Router#debug iox config level debug`
		`iox_819_2#conf t`
		`Enter configuration commands, one`
		`per line. End with CNTL/Z.`
		`iox_819_2(config)#iox`
		`iox_819_2(config-iox)#host ip`
		`default-gateway 192.168.100.1`
		`% configuration failure: host ip`
		`default-gateway`
		`iox_819_2(config-iox)#`
		`*Oct 7 08:35:10.231 PDT:`
		`SCORE_ERR:`
		`score_ipc_send_msg_socket 394 Send`
		`failed, socket down`
		`*Oct 7 08:35:10.231 PDT:`
		`if_c800_iox_cli_handler.c ::`
		`cfg_iox_host_default_gateway_cmd_ha`
		`ndler() : 645 - Sending host ip`
		`message unsuccessful`

debug iox config level warning	IOx の設定の警告をデバッグします。	

		Router#debug iox config level warning iox_819_2#conf t Enter configuration commands, one per line. End with CNTL/Z. iox_819_2(config)#iox iox_819_2(config-iox)#host ip default-gateway 192.168.100.1 % configuration failure: host ip default-gateway iox_819_2(config-iox)# *Oct 7 08:37:06.067 PDT: SCORE_ERR: score_ipc_send_msg_socket 394 Send failed, socket down *Oct 7 08:37:06.067 PDT: if_c800_iox_cli_handler.c :: cfg_iox_host_default_gateway_cmd_handler() : 645 - Sending host ip message unsuccessful
debug iox host-agent level error	このコマンドは、IOS 側で IOx の設定の問題が生じている場合に使用します。これにより、IOS と IOx フレームワーク間のメッセージングをモニタできます。これは、IOS の設定/メッセージングのデバッグを行うものであり、一般には IOx プラットフォームのデバッグ レベルを変更するものではありません。	Router#debug iox host-agent level error Oct 23 22:37:40.598: if_c800_iox_trans_mgr.c :: iox_create_transaction() : 50 - Created transaction: tid=2, pid=103 *Oct 23 22:37:40.598: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - **********[IOS-DUMP]********** *Oct 23 22:37:40.598: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - 00 0F 00 06 00 00 00 02 07 01 00 08 01 03 *Oct 23 22:37:40.598: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - ********** *Oct 23 22:37:40.598: if_c800_iox_ipc_utils.c :: iox_msg_send() : 137 - Pid: 103 Sending iox message to Score *Oct 23 22:37:40.598: if_c800_iox_cli_handler.c :: iox_cli_wait_for_response() : 207 - CLI is waiting for response - pid: 103 *Oct 23 22:37:40.810: if_c800_iox_ipc_main.c :: iox_recv_msg_from_ioxhad() : 35 - **********[IOS-DUMP]********** *Oct 23 22:37:40.810: if_c800_iox_ipc_main.c :: iox_recv_msg_from_ioxhad() : 35 - 00 10 00 03 00 00 00 02 00 01 00 *Oct 23 22:37:40.810: if_c800_iox_ipc_main.c :: iox_recv_msg_from_ioxhad() : 35 - **********
debug iox host-agent level debug	IOx ホスト エージェントをデバッグします。	

		Router#debug iox host-agent level debug *Oct 7 08:43:04.727 PDT: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - **********[IOS-DUMP]********** *Oct 7 08:43:04.727 PDT: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - 00 0F 00 06 00 00 00 14 07 01 00 08 01 03 *Oct 7 08:43:04.727 PDT: if_c800_iox_infra_cli_handler.c :: set_debug_level() : 151 - ********** *****
debug iox host-agent level warning	IOx ホスト エージェントの警告をデバッグします。	Router#debug iox host-agent level warning
reset iox	IOx フレームワークをリセットします。	Router#reset iox *Oct 23 22:41:05.406: if_c800_iox_trans_mgr.c :: iox_create_transaction() : 50 - Created transaction: tid=4, pid=103 *Oct 23 22:41:05.406: if_c800_iox_infra_cli_handler.c :: exec_iox_infra_command_handler() : 298 - **********[IOS-DUMP]********** *Oct 23 22:41:05.406: if_c800_iox_infra_cli_handler.c :: exec_iox_infra_command_handler() : 298 - 00 11 00 03 00 00 00 04 07 01 01 *Oct 23 22:41:05.406: if_c800_iox_infra_cli_handler.c :: exec_iox_infra_command_handler() : 298 - ********** ***** *Oct 23 22:41:05.406: if_c800_iox_ipc_utils.c :: iox_msg_send() : 137 - Pid: 103 Sending iox message to Score % Couldn't process IOx Infrastructure response
show raw-socket tcp sessions	raw ソケット セッションのステータスを表示します。	Router#show raw-socket tcp sessions ---------- ---------- TCP Sessions ---------- ---------- interface tty socket mode local_ip_addr local_port dest_ip_addr dest_port up_time idle_time/timeout vrf_name Se0 7 0 client 10.10.10.1 34383 10.10.10.2 32000 00:00:10 00:00:10 /5 min internal-score-vrf
show raw-socket tcp statistic	raw ソケットの統計情報を表示します。	

		Router# show raw-socket tcp statistic ---------- ---------- Network-Serial Statistics ---------- ---------- Interface tty sessions network_in_bytes network_out_bytes network_to_tty_frames tty_to_network_frames vrf_name Se0 7 1 6 6 1 1 internal-score-vrf ---------- CEF Connections Statistics ---------- tty_id network_in_frames network_in_bytes network_out_frames network_out_bytes 0 0 0 0 0 0 0 0 0 0
show virtual-service detail	アプリケーション固有の情報を表示します。	

		Router# show virtual-service detail name APP Virtual service APP detail State : Activated Package information Name : APP Path : flash:/iox/tmp/APP.ova Application Name : KVM1_Application Installed version : 2.0 Description : KVM1 Linux Test Distro Signing Key type : Unsigned Method : SHA-1 Licensing Name : kvm1_license Version : 3.3 Activated profile name: Resource reservation Disk : 16 MB Memory : 256 MB CPU : 55% system CPU VCPUs : 1 (sockets:1 cores:1 threads:1) Attached devices Type Name Alias ---------- NIC dp_1_0 net1 Serial/shell serial0 Disk shared_moun Network interfaces MAC address Attached to interface ---------- 52:54:11:11:00:FE VirtualPortGroup0 Resource admission (without profile) : passed Disk space : 16MB Memory : 256MB CPU : 55% system CPU VCPUs : 1 (sockets:1 cores:1 threads:1)
show virtual-service global	仮想サービスのグローバル情報を表示します。	

		Router# show virtual-service global Virtual Service Global State and Virtualization Limits: Infrastructure version : 1.7 Total virtual service installed : 1 Total virtual service activated : 1 Maximum VCPUs per virtual service : 1 Machine types supported : KVM Machine types disabled : LXC Resource virtualization limits: Name Quota Committed Available ----------
show virtual-service list	アプリケーションを一覧します。	Router# show virtual-service list Virtual Service List: Name Status Package Name ----------
show virtual-service profile	アプリケーション プロファイルに関する情報を表示します。	Router# show virtual-service profile
show virtual-service utilization	アプリケーションの使用率に関する情報を表示します。	Router# show virtual-service utilization name APP Virtual-Service Utilization: CPU Utilization: Requested Application Utilization: 55 % Actual Application Utilization: 1 % (30 second average) CPU State: R : Running Memory Utilization: Memory Allocation: 262144 Kb Memory Used: 262144 Kb Network Utilization: Name: dp_1_0, Alias: net1 RX Packets: 16 TX Packets: 24 RX Bytes: 2416 TX Bytes: 6624 RX Errors: 0 TX Errors: 0 Storage Utilization: Name: shared_mount, Alias: Capacity(1K blocks): 16384 Used(1K blocks): 20 Available(1K blocks): 16364 Usage: 1 %
virtual-service connect name *appname* **console**		Router# virtual-service connect name sensorbot console

	IOx アプリケーションが実行されている VM 環境のコンソールに接続します。	

CAF のログ設定の有効化

CAF のログ設定を使用すると、App ライフ サイクルの問題をデバッグできます。デフォルトでは、ログ設定は [INFO] に設定されます。Fog Director または Local Manager を使用して、CAF 設定を [debug] に設定します。

アプリケーション固有のデバッグ

IOx の管理者は、Local Manager を使用して App コンソールにアクセスできます。App コンソールにアクセスするには、Local Manager にログインし、[Apps] > [Manage] > [App-info] の順に移動して、次の SSH コマンドを入力します。

```
ssh -p {SSH_PORT} -i net_bridge.pem appconsole@10.78.106.163
```

SSH_PORT は、管理者が IOS NAT ルールで設定しているポート番号に置き換えます。たとえば、GOS に割り当てられている IP アドレスが 192.168.1.6 で、IOS 上に設定されている NAT ルールが SSH に 2222 までを許可している場合、最終的な App コンソール アクセス コマンドは以下になります。

```
ssh -p 2222 -i net_bridge.pem appconsole@10.78.106.163
```

よくある問題

問題： Fog Director に追加したデバイスが表示されません。Fog Director の [Last Heard] 列に、「connection timed out or no route to host」と表示されます。

解決策：この問題は、ルータの WAN IP アドレスが Fog Director から到達できないために生じます。到達可能性の問題を修正し、すべての必要な設定が正しく行われていることを確認してください。

問題： ルータの WAN IP アドレスは到達可能ですが、Fog Director にデバイスが表示されません。

解決策：この問題のトラブルシューティングでは、以下を実行します。

- 必要な NAT ルールが ポート 8443 に対して有効になっているかどうかを確認します。次の例は NAT ルールを示しています。

  ```
  ip nat inside source list NAT_ACL interface gigabitEthernet0 overload
  ip nat inside source static tcp 192.168.1.6 8443 interface gigabitEthernet0 8443
  ```

- GIG5 が起動しているかどうかを確認します。
- GOS/IOx が起動して稼働しているかどうか、DHCP サーバから IP アドレスを取得しているかどうかを確認します。
- 8443 について、WAN IP から GOS SVCbr_0 IP アドレスへの NAT 変換が行われているかどうか確認します。

  ```
  829-163#show ip nat translations
  Pro Inside global         Inside local          Outside local         Outside global
  tcp 10.78.106.163:2222    192.168.1.6:22        ---                   ---
  tcp 10.78.106.163:8443    192.168.1.6:8443     10.232.26.200:57639   10.232.26.200:57639
  ```

シリアル データ トラフィックに関する問題

次のコマンドを使用して、シリアルデータ トラフィックの問題のトラブルシューティングを実行します。

表 *46*：シリアル データ トラフィックの問題に関するデバッグ コマンド

コマンド	説明	例

show interface serial	シリアルインターフェイスの設定と統計情報を表示します。	`Router# show interface serial`
		`erial0 is up, line protocol is up`
		`Hardware is Serial in async mode`
		`MTU 1500 bytes, BW 9 Kbit/sec,`
		`DLY 100000 usec,`
		`reliability 255/255, txload`
		`1/255, rxload 1/255`
		`Encapsulation RAW-TCP, loopback`
		`not set`
		`Keepalive not set`
		`DTR is pulsed for 5 seconds on`
		`reset`
		`Last input never, output never,`
		`output hang never`
		`Last clearing of "show interface"`
		`counters 5d21h`
		`Input queue: 0/75/0/0`
		`(size/max/drops/flushes); Total`
		`output drops: 0`
		`Queueing strategy: fifo`
		`Output queue: 0/10 (size/max)`
		`30 second input rate 0 bits/sec,`
		`0 packets/sec`
		`30 second output rate 0 bits/sec,`
		`0 packets/sec`
		`391 packets input, 3247 bytes,`
		`0 no buffer`
		`Received 0 broadcasts (0 IP`
		`multicasts)`
		`0 runts, 0 giants, 0 throttles`
		`1 input errors, 0 CRC, 1`
		`frame, 0 overrun, 0 ignored, 0`
		`abort`
		`395 packets output, 3160`
		`bytes, 0 underruns`
		`0 output errors, 0 collisions,`
		`0 interface resets`
		`0 unknown protocol drops`
		`0 output buffer failures, 0`
		`output buffers swapped out`
		`0 carrier transitions`
		`DCD=up DSR=up DTR=up RTS=up`
		`CTS=up`

debug raw-socket tcp packet **raw ソケット ドライバパケットをデバッグします。**	IOS とホスト Linux のシリアルデータ フローをモニタします。 （注） これは、コンソールの全パケットの内容をダンプします。コンソールのロギングをオフにして、コンソールからデバッグメッセージがフラッディングするのを避けることができます。	

		Router# debug raw-socket tcp packet *Oct 23 18:52:25.912: [From Network]<-- received 8 bytes on socket 0 from 192.168.3.2 port 32000 *Oct 23 18:52:25.912: 010300000002C40B *Oct 23 18:52:25.912: [To Serial]<-- sending 8 bytes from socket 0 to interface 7 *Oct 23 18:52:25.912: rawsocket_async_output[tty 7]: Received 8 byte from socket... *Oct 23 18:52:25.912: [Socket --> Async] 01 03 00 00 00 02 C4 0B *Oct 23 18:52:25.948: [Async --> Socket] tty(7) Received 9 byte from serial... *Oct 23 18:52:25.948: [Async --> Socket] 01 03 04 89 2F 80 4F C1 92 *Oct 23 18:52:25.948: [From Serial]--> received 9 bytes from interface 7 tty 7 *Oct 23 18:52:25.948: 010304892F804FC192 *Oct 23 18:52:25.948: [To Network]--> dispatched 9 bytes on socket 0 to ip 192.168.3.2 port 32000

シリアル デバイスが接続されているかどうか、およびデバイス上のシリアル ポートが同じボーレートを共有しているかどうかを確認します。

第 21 章

展開シナリオ

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）の一般的な展開シナリオについて説明します。

展開シナリオについて

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（任意）
- 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、「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 ソフトウェアが稼働する、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、「ワイヤレス デバイスの設定」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。

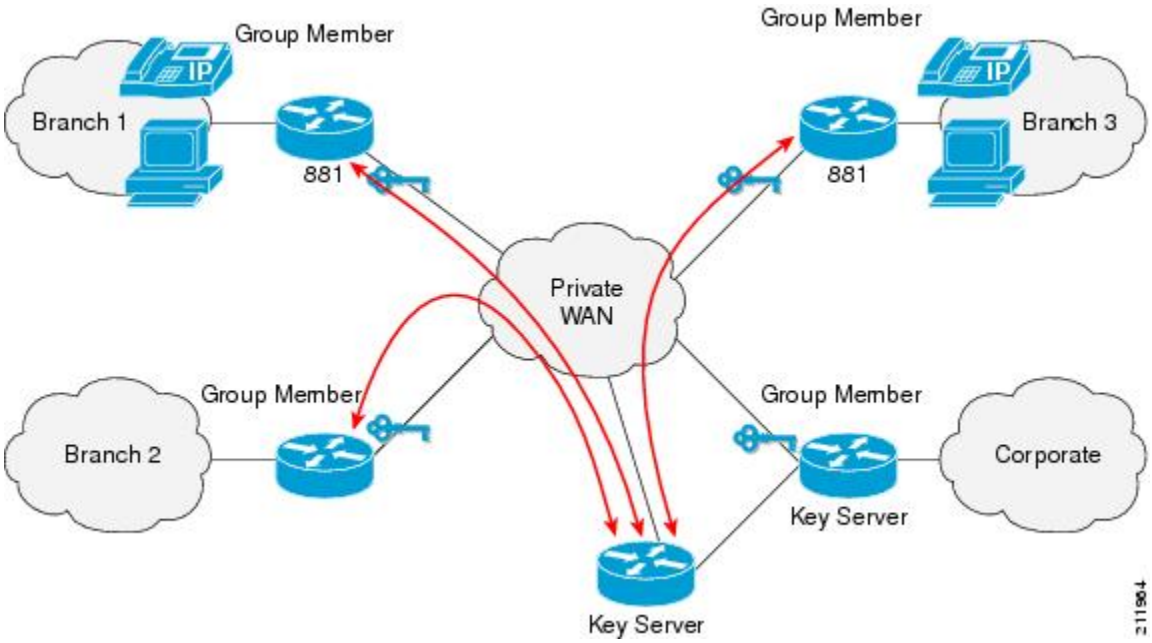
エンタープライズ スモール ブランチ

以下の図に、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 ファイアウォール（FW）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 *20*：エンタープライズ スモール ブランチ

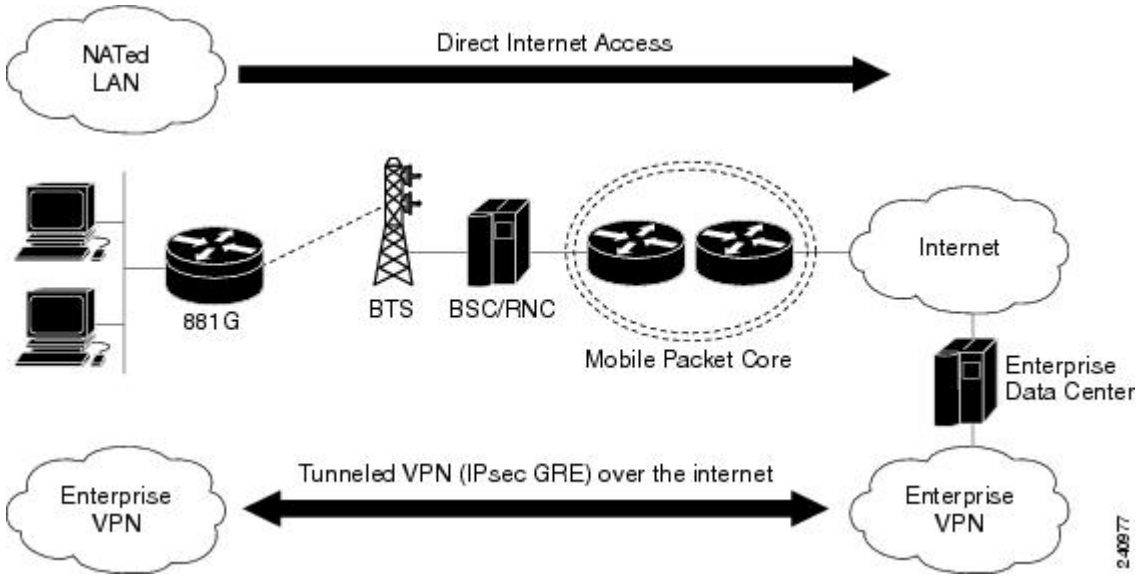


3G を使用したインターネット サービスと IPSec VPN

以下の図に、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 *21*：*3G* を使用したインターネット サービスと *IPSec VPN*



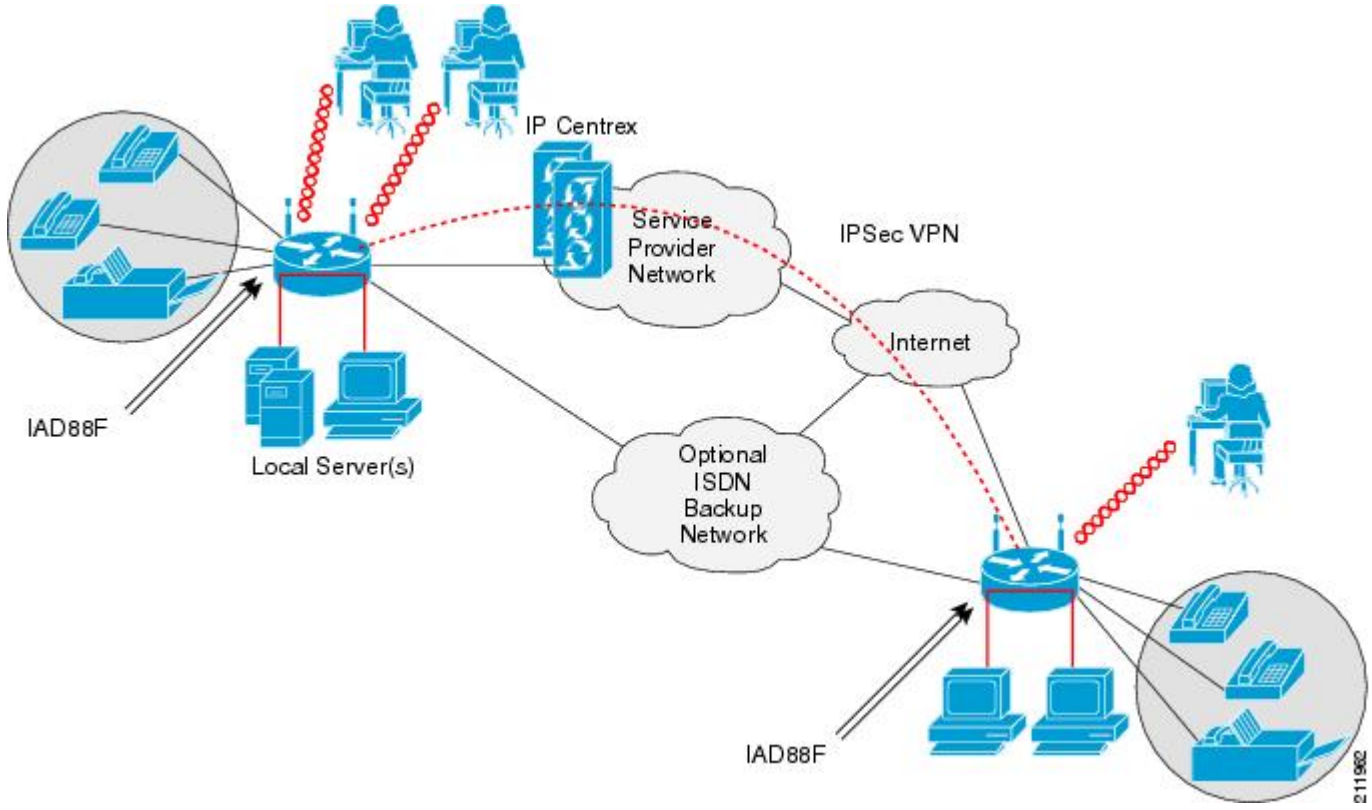
SMB アプリケーション

次の図は、以下のテクノロジーと機能を各ブランチ オフィスで使用する小規模から中規模のビジネスでの展開（SMB）を示しています。

- 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 *22*：小規模から中規模のビジネス



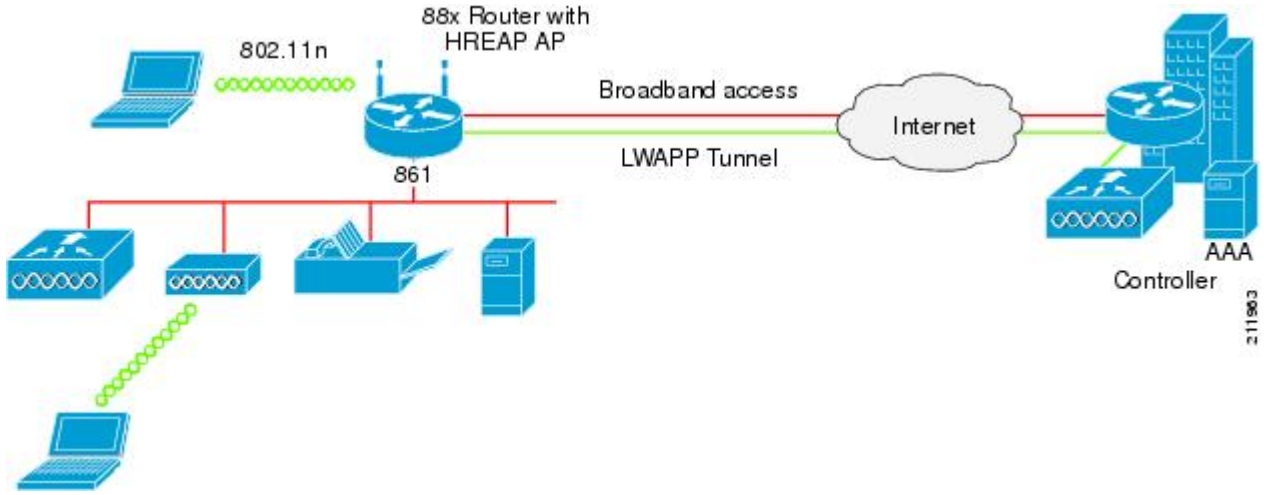
LWAPP を使用したエンタープライズ ワイヤレス構成

以下の図に、Lightweight アクセス ポイント プロトコル（LWAPP）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。
- ハイブリッド リモート エッジ アクセス ポイント（H-REAP）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、サービス セット ID（SSID）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。

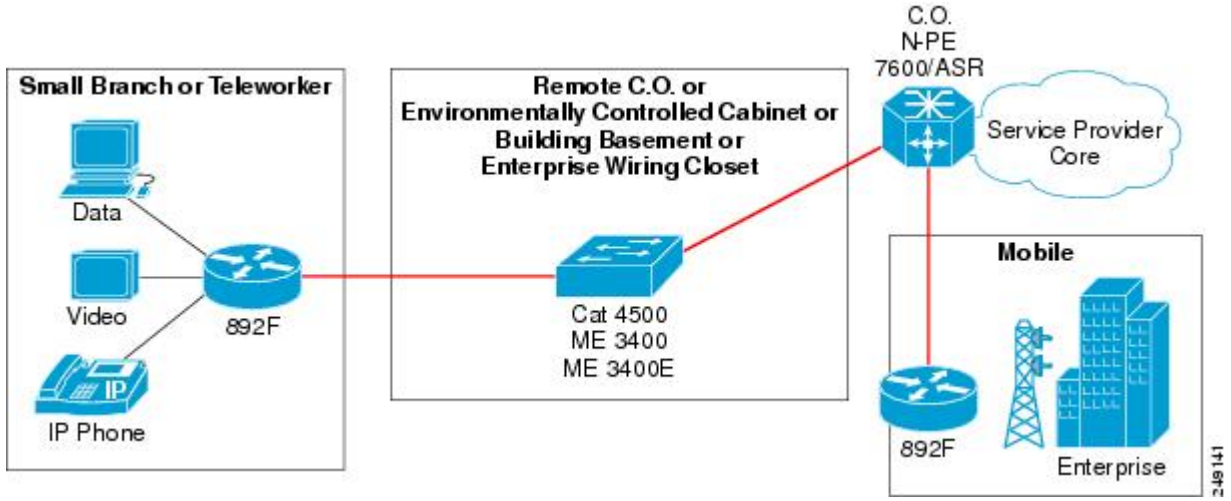
図 *23*：*LWAPP* を使用したワイヤレス *LAN*



企業の小規模ブランチ オフィスへの展開

以下の図は、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 *24*：企業の小規模ブランチ オフィスへの展開



第 22 章

Cisco 800 シリーズ ルータの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。

使用する前に

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した端末またはPCを使用してルータのステータス メッセージを表示し、コマンドを入力して問題のトラブルシューティングを実行できます。

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働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
- メンテナンス契約書または保証情報
- 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設置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（VPI）/仮想回線識別子（VCI）が使用されている。
- DSLAM はディスクリート マルチトーン（DMT）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、シールドなしツイストペア（UTP）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。

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設置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 の設定を表示するには、EXEC モードで **showcontrollersdsl0** 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設置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 の設定を表示するには、EXEC モードで **showcontrollersvdsl0** コマンドを使用します。debug vdsl 0 daemon state コマンドを使用して、VDSL2 トレーニングの状態遷移を表示するデバッグ メッセージを有効にできます。

VDSL ファームウェア ファイルに問題がある場合は、Cisco IOS イメージをアップグレードせずに、リロードまたはアップグレードできます。使用するコマンドは、次のとおりです。

controllervdsl0firmware *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 ファイル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、**showinterfaces** コマンドを使用します。表 47：show interfaces コマンド出力の説明，（481 ページ）は、コマンド出力のメッセージを示します。

次の例は、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状態を表示する方法を示しています。

```
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)
```

次の例は、ATM インターフェイスの状態を表示する方法を示しています。

```
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
```

次の例は、ダイヤラ インターフェイスの状態を表示する方法を示しています。

```
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
```

以下の表に、**show interfaces** コマンドの出力について説明します。

表 *47* : ***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。
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。

出力	原因
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

特定の PVC が使用中であるかどうかを判別するには、**pingatminterface** 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。以下に、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ます。

次の例は、PVC が使用中かどうかを確認する方法を示しています。

```
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関する ATM に固有の情報を表示するには、**showatminterfaceatm0commandfrom** 特権 EXEC モードを使用します。

次の例は、ATM インターフェイスに関する情報を表示する方法を示しています。

```
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
```

以下の表に、コマンド出力で表示されるフィールドの一部について説明します。

表 *48*：*show atm interface* コマンド出力の説明

フィールド	説明
ATM interface	インターフェイス番号。Cisco 860 および Cisco 880 シリーズ アクセス ルータの場合は常に 0 です。
AAL enabled	イネーブルの AAL のタイプ。Cisco 860 および Cisco 880 シリーズ アクセス ルータは AAL5 をサポートしています。
Maximum VCs	インターフェイスがサポートする仮想接続の最大数。
Current VCCs	アクティブな仮想チャネル接続（VCC）の数。
Maximum TransmitChannels	伝送チャネルの最大数。

フィールド	説明
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	物理層インターフェイス モジュール（PLIM）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** コマンドは、問題の解決に役立つさまざまな情報を表示します。

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、**loggingconsoledebug** 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。
- デバッグを無効にするには、**undebugall** コマンドを使用します。
- ルータで Telnet セッション時に **debug** コマンドを使用するには、**terminalmonitor** コマンドを入力します。

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 コマンドのその他の情報およびドキュメンテーションは、『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、**debugatm 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。

次の例は、ATM エラーを表示する方法を示しています。

```
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、ATM ネットワークの問題点を診断するには、**debugatm 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。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。

次の例は、ATM インターフェイス プロセッサ イベントの成功を表示する方法を示しています。

```
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]
```

次の例は、ATM インターフェイス プロセッサ イベントの失敗を表示する方法を示しています。

```
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

debugatm 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 レベルの 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 **debugatmpacket** 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** [**interfaceatm** *number* [**vcd** *vcd-number*][**vc** *vpi/vci number*]]

no debug atm **packet** [**interfaceatm** *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。

interfaceatm*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）仮想回線識別子（VCD）の番号。

vc *vpi/vci number* ：ATM PVC の VPI/VCI 値。

以下に、**debugatmpacket** コマンドの出力例を示します。

```
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 ABCD
01:23:48:ABCD 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 ABCD
01:23:48:ABCD 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:
```

以下の表に、**debug atm packet** コマンド出力で表示されるフィールドの一部について説明します。

表 *49* : ***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。

フィールド	説明
（O）	出力パケット。（I）は、受信パケットを意味します。
VCD: 0x*n*	このパケットに関連付けられる仮想回線。*n* はある特定の値です。
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，（488 ページ）
2 ルータのリセット，（489 ページ）
3 パスワードのリセットと変更の保存，（491 ページ）（イネーブル シークレット パスワードを忘れた場合のみ）
4 コンフィギュレーション レジスタ値のリセット，（492 ページ）

（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。

手順の概要

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 プログラムが稼働している PC を接続します。
2. 端末を 9600 ボー、8 データ ビット、パリティなし、および 1 ストップ ビットで動作するように設定します。
3. 特権 EXEC プロンプト（*router_name* #）で **showversion** コマンドを入力すると、既存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）。
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。
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 モードから **config-register0x01** コマンドを入力します。

手順の詳細

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 プログラムが稼働している 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、および 1 ストップ ビットで動作するように設定します。

ステップ 3 特権 EXEC プロンプト（*router_name* #）で **showversion** コマンドを入力すると、既存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）。

例：

```
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 モードから **config-register0x01** コマンドを入力します。

- 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。

手順の概要

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, （490ページ）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, （490 ページ）に進みます。
2. break を押します。端末に次のプロンプトが表示されます。
3. **confreg0x142** 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。
4. **reset** コマンドを入力して、ルータを初期化します。
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。
6. **Return** を押します。次のプロンプトが表示されます。
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。
8. **showstartup-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。

手順の詳細

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, （490ページ） 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, （490ページ） 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。

例：

```
rommon 2>
```

ステップ 3 **confreg0x142** 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。

例：

```
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。

例：

```
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。

例：

```
--- 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。

例：

```
Press RETURN to get started!
```

ステップ 6 **Return** を押します。次のプロンプトが表示されます。

例：

```
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。

例：

```
Router> enable
```

プロンプトが特権 EXEC プロンプトに変わります。

例：

```
Router#
```

ステップ 8 **showstartup-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。

例：

```
Router# show startup-config
```

次の作業

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, （491 ページ）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, （492 ページ）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 パスワードを回復する場合、**showstartup-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, （491 ページ）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。

手順の概要

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、**configureterminal** コマンドを実行します。
2. **enablesecret** 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。
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。
4. 設定変更を保存します。

手順の詳細

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、**configureterminal** コマンドを実行します。

例：

```
Router# configure terminal
```

ステップ 2 **enablesecret** 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。

例：

```
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。

例：

```
Router(config)# exit
```

ステップ 4 設定変更を保存します。

例：

```
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、次の手順を実行します。

手順の概要

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、**configureterminal** コマンドを実行します。
2. **configureregister** 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。
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。
4. ルータを再起動し、回復したパスワードを入力します。

手順の詳細

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、**configureterminal** コマンドを実行します。

例：

```
Router# configure terminal
```

ステップ 2 **configureregister** 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。

例：

```
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。

例：

```
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。

付 録 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。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。

- ルータの基本設定
- 展開シナリオ

この付録では、次の内容で基礎知識について説明します。

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。以下の表に、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 *50* : 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、「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, （501 ページ）の項を参照してください。

コマンド モードについて

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

以下の表には、このマニュアルで使用されているコマンド モードを一覧し、各モードへのアクセス方法、各モードのプロンプト、モードを終了する方法および別のモードを開始する方法について説明します。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 *51*：コマンド モードの概要

モード	Access Method	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 モードに戻るには、**disable** コマンドを入力します。 • グローバル コンフィギュレーション モードを開始するには、**configure** コマンドを入力します。	このモード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,（500 ページ）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。

モード	Access Method	プロンプト	モードの終了および開始	モードの用途
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 モードに戻るには、**exit**または**end**コマンドを入力するか、**Ctrl-Z**を押します。 • 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、**interface**コマンドを入力します。	このモードは、ルータにグローバルに適用するパラメータを設定する目的で使用します。 このモードからは次のモードにアクセスできます。 • インターフェイス コンフィギュレーション • ルータ コンフィギュレーション • ライン コンフィギュレーション
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**コマンド（**interfaceatm0**などの特定のインターフェイスで）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。 • 特権 EXEC モードに戻るには、**end**コマンドを入力するか、**Ctrl-Z**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。

モード	Access Method	プロンプト	モードの終了および開始	モードの用途
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** コマンドのいずれかに、適切なキーワードとして、たとえば、**routerrip** を指定して入力します。	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。 • 特権 EXEC モードに戻るには、**end** コマンドを入力するか、**Ctrl-Z** を押します。	このモードは、IP ルーティングプロトコルを設定する目的で使用します。
ライン コンフィギュレーション	グローバル コンフィギュレーションモードから、**line** コマンドに、目的の回線番号およびオプションの回線タイプとして、たとえば、**line0** を指定して入力します。	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。 • 特権 EXEC モードに戻るには、**end** コマンドを入力するか、**Ctrl-Z** 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

疑問符（?）と矢印キーを使用すると、コマンドの入力に役立ちます。

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
.
.
.
```

コマンドを完成させるには、わかっている文字を数文字入力し、続けて疑問符を入力します（スペースなし）。

```
Router> sh?
* s=show set show slip systat
```

コマンド変数のリストを表示するには、コマンドに続けてスペースと疑問符を入力します。

```
Router> show ?
.
.
.
clock   Display the system clock
dialer   Dialer parameters and statistics
exception   exception information
.
.
.
```

UpArrow 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。**UpArrow** 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。

- **enablesecret** *password*：非常にセキュア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 および **enablesecret** のパスワードはどちらも、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。**enablesecret** パスワードは、ネットワークで使用する、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。特権 EXEC モード コマンドにアクセスするには、権限レベル 1 の **enablesecret** または **enable** パスワードを入力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。

enablesecret パスワードには、大文字小文字の英数字 1 ～ 25 文字を含めることができます。**enable** パスワードには、任意の数の大文字と小文字の英数字を使用できます。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。

手順の概要

1. ルータの起動後、**enable** または **enablesecret** コマンドを入力します。
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。
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、**configureterminal** コマンドを実行します。

手順の詳細

ステップ 1 ルータの起動後、**enable** または **enablesecret** コマンドを入力します。

例：

```
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。

例：

```
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、**configureterminal** コマンドを実行します。

例：

```
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、コマンドライン インターフェイス（CLI）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、**showversion** 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

機能を無効にする、または入力したコマンドを元に戻すには、ほとんどのコマンドで前に **no** キーワードを付けます。たとえば、**noiprouting** のようにします。

コマンドライン エラー メッセージ

次の表に、CLI を使用してルータを設定するときに表示される可能性のあるエラー メッセージの一部を紹介します。

表 *52* : *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

設定の変更は、システムのリロードや停電が発生した際に失われないように、**copy running-configstartup-config** コマンドを使用して NVRAM に保存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]?
```

Enter を押して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か、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#
```

まとめ

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。

- 疑問符（?）と矢印キーを使用すると、コマンドの入力に役立ちます。
- 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。
- 機能をディセーブルにするには、コマンドの前に **no** キーワードを挿入します。たとえば、**noiprouting** のように入力します。
- 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。

次の手順：

ルータを設定するには、「ルータの基本設定」および「展開シナリオ」に進みます。展開シナリオ，（471 ページ）

付 録 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。

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。

Network Protocols

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。アドレス解決プロトコル（ARP）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 プロトコルであるルーティング情報プロトコル（RIP）を使用して、ルーティング情報を交換します。RIP については、この後で詳細に説明します。

ルーティング プロトコルのオプション

ルーティング プロトコルには次のものがあります。

- ルーティング情報プロトコル（RIP）
- 拡張 IGRP

以下の表に、RIP と 拡張 IGRP の相違点を示します。

表 *53*：*RIP* と 拡張 *IGRP* 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 のトリガー拡張機能を使用することもできます。
拡張 IGRP	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 ベクター 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 のトリガー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 のトリガー拡張機能については、Cisco IOS Release 12.3 のマニュアルを参照してください。

拡張 IGRP

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 が稼働する各ルータは、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

ポイントツーポイント プロトコル（PPP）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。これらの機能をサポートするために、オプションの設定パラメータや機能をネゴシエートするための、拡張可能なリンク コントロール プロトコル（LCP）とネットワーク コントロール プロトコル（NCP）が提供されています。

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）
- チャレンジ ハンドシェイク認証プロトコル（CHAP）

通常、PPP と PAP または CHAP 認証の組み合わせは、接続されているリモート サイトを中央サイトに通知する場合に使用されます。

PAP

PAP は双方向のハンドシェイクを使用して、ルータ間のパスワードを検証します。PAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。PPP リンクが確立された後、リモート オフィス ルータは、本社オフィス ルータが認証を受け付けるまで、設定されているユーザ名およびパスワードの送信を繰り返します。

PAP の特徴は、次のとおりです。

- 認証のパスワード部分は、リンク上をクリアテキストで送信されます（スクランブル処理または暗号化は行われません）。
- PAP では、プレイバック攻撃または反復的な総当り攻撃からの保護機能が提供されません。
- 認証試行の頻度およびタイミングは、リモート オフィス ルータが制御します。

CHAP

CHAP は 3 ウェイ ハンドシェイクを使用して、パスワードを検証します。CHAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。

PPP リンクが確立された後、本社オフィス ルータはリモート オフィス ルータに対し、チャレンジ メッセージを送信します。リモート オフィス ルータは可変の値で応答します。本社オフィス ルータは、独自に計算した値と照らし合わせて、この応答をチェックします。両方の値が一致していれば、本社オフィス ルータは認証を受け付けます。リンクを確立した後は、いつでも認証プロセスを繰り返すことができます。

CHAP の特徴は、次のとおりです。

- 認証プロセスでは、パスワードではなく、可変のチャレンジ値を使用します。
- CHAP は、一意の予測不可能な可変のチャレンジ値の使用により、プレイバック攻撃から保護します。チャレンジの反復により、1 回の攻撃にさらされる時間を限定します。
- 認証試行の頻度およびタイミングは、本社オフィス ルータが制御します。

（注） 2 つのプロトコルのうち、より安全性の高い CHAP の使用を推奨します。

TACACS+

Cisco 860 および Cisco 880 シリーズ ルータは、Telnet を介して Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。TACACS+ は、リモート アクセス認証およびイベント ロギングなどの関連ネットワーク セキュリティ サービスを提供するシスコ独自の認証プロトコルです。ユーザ パスワードは、個々のルータではなく中央のデータベースで管理されます。TACACS+ は、ルータごとに設定された別個のモジュールである認証、許可、アカウンティング（AAA）ファシリティもサポートします。

ネットワーク アドレス変換

ネットワーク アドレス変換（NAT）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（NAT）と PPP/インターネット プロトコル コントロール プロトコル（IPCP）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を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、インターネット サービス プロバイダー（ISP）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、ダイナミック ホスト コンフィギュレーション プロトコル（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

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、キャリア検知多重アクセス/衝突検知（CSMA/CD）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 アダプテーション層（AAL）

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、可変ビット レート（VBR）トラフィックおよび未指定ビット レート（UBR）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

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、基本速度インターフェイス（BRI）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がわかっ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、および専用回線のバックアップに使用されます。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。この代替ルートにダイヤルオンデマンド ルーティング（DDR）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ーするトラフィックを定義しなくても、信頼できる接続を確立できます。したがって、ダイヤラ ウォッチは対象トラフィックに関する条件がない正規の DDR と見なすことができます。プライマリ インターフェイスを定義するウォッチ対象ルートを設定することにより、ウォッチ対象ルートの追加および削除にともない、プライマリ インターフェイスのステータスを監視し追跡することができます。

ウォッチ対象ルートを削除すると、ダイヤラ ウォッチはウォッチ中のいずれかのIPアドレスまたはネットワークに対して、有効なルートが少なくとも 1 つ存在するかどうかを確認します。有効なルートが存在しない場合、プライマリ回線はダウンしており、使用不可能であると見なされます。定義済みのウォッチ対象 IP ネットワークの少なくとも 1 つに有効なルートが存在し、このルートがダイヤラ ウォッチに設定されたバックアップインターフェイス以外のインターフェイスを示している場合、プライマリ リンクは起動していると見なされ、ダイヤラ ウォッチはバックアップ リンクを起動しません。

QoS

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 が稼働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（クラス ベース WFQ（CBWFQ）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 プレシデンス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 プレシデンスを使用します。

CBWFQ

通常、CBWFQ（クラスベース均等化キューイング）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、先入れ先出し（FIFO）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

低遅延キューイング（LLQ）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場合、そのパケットはセッションの最初ではなく、既存のセッションに属していることを示します）。このフィルタ基準は、インターフェイスに永続的に適用されるアクセス リストの一部になります。

付 録 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、このファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムのブートを助けます。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は、ROM モニタがルータを実行します。

この付録の内容は、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。

手順の概要

1. **enable**
2. **configureterminal**
3. **config-reg0x0**
4. **exit**
5. **reload**

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**	特権 EXEC モードを開始します。 パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal**	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-reg0x0**	コンフィギュレーション レジスタをリセットします。
ステップ 4	**exit**	グローバル コンフィギュレーション モードを終了します。
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 ソフトウェアを起動しません。 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。付録の「ROM モニタ コマンドの説明,（522 ページ）」セクションで、**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。

次の作業

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。

ROM モニタ コマンドの説明

以下の表に、一般的に使用される ROM モニタ コマンドを示します。

表 *54*：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`

reset または**i**	ルータをリセットまたは初期化します。電源投入に似ています。

dir デバイス**:**	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)`

コマンド	説明
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 **copytftpflash** 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：ファイル ダウンロードが進行中であることを示す感嘆符（!!!）が表示されます。これがデフォルト設定です。 2：ファイルダウンロードプロセス中に、次のような詳細な進行状況が表示されます。 • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received.MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** 設定
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。デフォルト値は2,400秒（40分）です。	**TFTP_TIMEOUT=** *time*

変数	コマンド
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 テストを実行しません。	**TFTP_CHECKSUM=**設定

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。

手順の概要

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。
2. 次のように **tftpdnld** コマンドを入力します。
3. 処理を続ける場合は、出力に示された問い合わせに **y** で応答します。

手順の詳細

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。

例：

```
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** コマンドを入力したときは、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。

例：

```
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 処理を続ける場合は、出力に示された問い合わせに **y** で応答します。

例：

```
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 レジスタは不揮発性 RAM（NVRAM）にあり、他の Cisco ルータと同じ機能を持っています。仮想コンフィギュレーション レジスタは、ROMモニタまたはオペレーティング システムで表示または変更できます。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 ポートを通じてルータにソフトウェア 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場合は、ROM monitor **dnld** コマンドを使用します。

（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 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。

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。

手順 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。

手順 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。

ROM モニタ debug 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 フレームを表示します。
- **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**：サイズ（バイト）、開始アドレス、使用可能なメインメモリの範囲、パケットメモリの開始点およびサイズ、NVRAM のサイズなどを表示します。

```
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フラッシュ メモリにある Cisco IOS イメージを起動するには、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。

次の例は、コンフィギュレーション レジスタをリセットし、フラッシュ メモリに格納された Cisco IOS イメージをルータが起動するように設定する方法を示しています。

```
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。

索 引

数字

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

V

W

あ

い

お

か

き

く

け

こ

さ

し

す

せ

そ

た

て

と

な

に

は

ひ

ふ

ほ

み

む

め

も

ゆ

よ

ら

り

る

ろ

わ