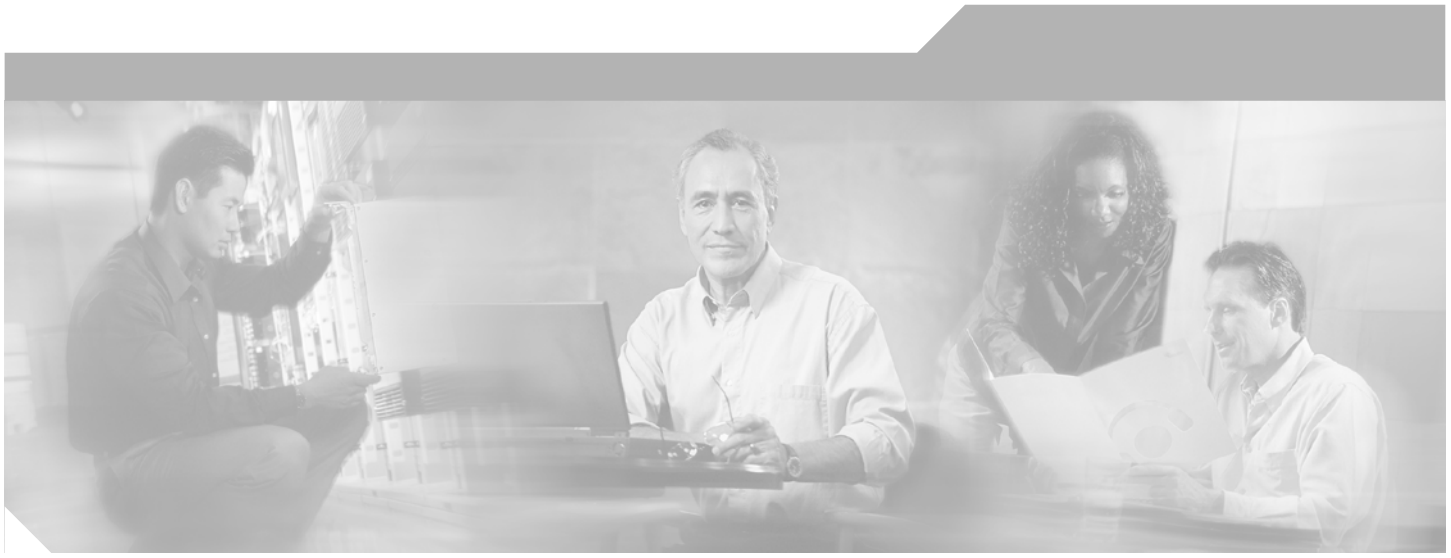


Cisco 1812J ソフトウェア コンフィギュレーション ガイド（最新版）

Cisco 1800 Series Integrated Services Routers (Fixed) Software Configuration Guide

Text Part Number: OL-6426-02-J

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

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

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Cisco 1812J ソフトウェア コンフィギュレーション ガイド（最新版）
Copyright © 2005, Cisco Systems, Inc.
All rights reserved.

Copyright © 2005–2011, シスコシステムズ合同会社 .
All rights reserved.

はじめに xi

PART 1 はじめに

CHAPTER 1 ルータの基本設定 1-1
インターフェイス ポート ラベル 1-2
デフォルト設定の表示 1-3
設定に必要な情報 1-4
基本パラメータの設定 1-5
グローバル パラメータの設定 1-6
ファスト イーサネット LAN インターフェイスの設定 1-6
WAN インターフェイスの設定 1-7
ファスト イーサネット WAN インターフェイスの設定 1-7
ATM WAN インターフェイスの設定 1-8
ワイヤレス インターフェイスの設定 1-9
ループバック インターフェイスの設定 1-9
設定例 1-9
設定の確認 1-10
ルータへのコマンドライン アクセスの設定 1-10
設定例 1-12
スタティック ルートの設定 1-12
設定例 1-13
設定の確認 1-13
ダイナミック ルートの設定 1-13
RIP の設定 1-14
設定例 1-15
設定の確認 1-15
拡張 IGRP の設定 1-15
設定例 1-16
設定の確認 1-16

PART 1 イーサネットおよび DSL アクセス用のルータの設定

CHAPTER 2 ネットワークの導入例 2-1

CHAPTER 3 PPP over Ethernet と NAT の設定 3-1
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 3-3
ファスト イーサネット WAN インターフェイスの設定 3-4
ダイヤラ インターフェイスの設定 3-5
ネットワーク アドレス変換の設定 3-7
設定例 3-9
設定の確認 3-10

CHAPTER 4 PPP over ATM と NAT の設定 4-1
ダイヤラ インターフェイスの設定 4-3
ATM WAN インターフェイスの設定 4-5
DSL シグナリング プロトコルの設定 4-6
ADSL の設定 4-6
設定の確認 4-7
SHDSL の設定 4-7
設定の確認 4-8
ネットワーク アドレス変換の設定 4-9
設定例 4-12
設定の確認 4-12

CHAPTER 5 DHCP および VLAN による LAN の設定 5-1
DHCP の設定 5-2
設定例 5-3
DHCP 設定の確認 5-4
VLAN の設定 5-5
VLAN コンフィギュレーションの確認 5-5
スイッチ ポートの設定 5-7
VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル） 5-8
802.1x 認証 5-8
レイヤ 2 インターフェイス 5-9
MAC テーブル操作 5-9
最大スイッチ仮想インターフェイス（SVI） 5-9
Switched Port Analyzer（SPAN） 5-9
IP マルチキャスト スイッチング 5-10
ポート単位のストーム制御 5-10
フォールバック ブリッジング 5-10

音声とデータ用の個別のサブネット 5-10
IGMP スヌーピング 5-10

CHAPTER 6 **Easy VPN および IPSec トンネルを使用した VPN の設定** 6-1
IKE ポリシーの設定 6-3
グループ ポリシー情報の設定 6-4
暗号マップへのモード設定の適用 6-5
ポリシー ルックアップのイネーブル化 6-6
IPSec トランスフォームおよびプロトコルの設定 6-6
IPSec 暗号方式およびパラメータの設定 6-7
物理インターフェイスへの暗号マップの適用 6-9
Easy VPN リモート コンフィギュレーションの作成 6-9
Easy VPN の設定の検証 6-11
設定例 6-11

CHAPTER 7 **IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定** 7-1
VPN の設定 7-3
IKE ポリシーの設定 7-3
グループ ポリシー情報の設定 7-4
ポリシー ルックアップのイネーブル化 7-5
IPSec トランスフォームおよびプロトコルの設定 7-6
IPSec 暗号方式およびパラメータの設定 7-7
物理インターフェイスへの暗号マップの適用 7-9
GRE トンネルの設定 7-10
設定例 7-11

CHAPTER 8 **簡易ファイアウォール** 8-1
アクセス リストの設定 8-3
インスペクション ルールの設定 8-4
インターフェイスへのアクセス リストおよびインスペクション ルールの適用 8-4
設定例 8-5

CHAPTER 9 **ワイヤレス LAN 接続** 9-1
ルート無線ステーションの設定 9-3
VLAN でのブリッジングの設定 9-5
無線ステーションのサブインターフェイスの設定 9-6
設定例 9-7

CHAPTER 10 設定例 10-1

PART 1 追加機能の設定とトラブルシューティング

CHAPTER 11 追加の設定オプション 11-1

CHAPTER 12 セキュリティ機能の設定 12-1
認証、許可、アカウンティング 12-1
AutoSecure の設定 12-2
アクセス リストの設定 12-2
アクセス グループ 12-3
アクセス グループの作成に関する注意事項 12-3
CBAC ファイアウォールの設定 12-3
Cisco IOS Firewall IDS の設定 12-4
VPN の設定 12-4

CHAPTER 13 ダイヤル バックアップとリモート管理の設定 13-1
ダイヤル バックアップ機能をアクティブにする方法 13-1
バックアップ インターフェイス 13-1
バックアップ インターフェイスの設定 13-2
フローティング スタティック ルート 13-2
フローティング スタティック ルートの設定 13-3
ダイヤラ ウォッチ 13-4
ダイヤラ ウォッチの設定 13-4
ダイヤル バックアップ機能の制限事項 13-5
設定例 13-6
ISDN S/T ポート経由でのダイヤル バックアップおよびリモート管理の設定 13-9
ISDN の設定 13-10
アグリゲータおよび ISDN ピア ルータの設定 13-12
V.92 モデム経由でのダイヤル バックアップおよびリモート管理の設定 13-13
非同期インターフェイスの設定 13-14
回線の設定 13-15

CHAPTER 14 トラブルシューティング 14-1
はじめに 14-1
代理店に連絡する前に 14-1
ADSL のトラブルシューティング 14-2

SHDSL のトラブルシューティング 14-2
PortFast のトラブルシューティング 14-2
ATM トラブルシューティング コマンド 14-3
ping atm interface コマンド 14-3
show interface コマンド 14-4
show atm interface コマンド 14-6
debug atm コマンド 14-6
debug コマンドを使用する場合の注意事項 14-6
debug atm errors コマンド 14-7
debug atm events コマンド 14-7
debug atm packet コマンド 14-8
ソフトウェア アップグレード方法 14-9
パスワードを忘れた場合の回復方法 14-9
コンフィギュレーション レジスタの変更 14-11
ルータのリセット 14-12
パスワードのリセットと変更の保存 14-13
コンフィギュレーション レジスタ値のリセット 14-13
SDM を使用したルータの管理 14-14

PART 1 参考資料

APPENDIX A Cisco IOS ソフトウェアの基礎知識 A-1
PC からのルータの設定 A-1
コマンド モードの概要 A-2
ヘルプの利用方法 A-4
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 A-6
グローバル コンフィギュレーション モードの開始 A-6
コマンドの使用方法 A-7
コマンドの短縮形 A-7
コマンドの取り消し A-7
コマンドライン エラー メッセージ A-7
変更した設定の保存 A-8
まとめ A-8
関連情報 A-9

APPENDIX B 概要 B-1
ADSL B-1
SHDSL B-2

ネットワーク プロトコル B-2
IP B-2
ルーティング プロトコルのオプション B-3
RIP B-3
EIGRP B-3
PPP 認証プロトコル B-4
PAP B-4
CHAP B-4
TACACS+ B-5
ネットワーク インターフェイス B-5
Ethernet B-5
ATM B-6
PVC B-6
ダイヤラ インターフェイス B-6
ダイヤル バックアップ B-7
バックアップ インターフェイス B-7
フローティング スタティック ルート B-7
ダイヤラ ウォッチ B-7
NAT B-8
Easy IP（フェーズ 1） B-8
Easy IP（フェーズ 2） B-9
QoS B-9
IP Precedence B-10
PPP フラグメンテーションおよびインターリーブ B-10
CBWFQ B-10
RSVP B-11
低遅延キューイング（LLQ） B-11
アクセス リスト B-11

APPENDIX C
ROM モニタ C-1
ROM モニタの設置 C-1
ROM モニタ コマンド C-2
コマンドの説明 C-3
TFTP ダウンロードによる障害時の回復 C-3
TFTP ダウンロードのコマンド変数 C-4
必須の変数 C-4
オプションの変数 C-5
TFTP ダウンロード コマンドの使用 C-5

コンフィギュレーション レジスタ C-6
コンフィギュレーション レジスタの手動での変更 C-6
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 C-6
コンソール ダウンロード C-7
コマンドの説明 C-8
エラー レポート C-8
デバッグ コマンド C-8
ROM モニタの終了 C-10

APPENDIX D 共通ポート割り当て D-1

INDEX

はじめに

このソフトウェア コンフィギュレーション ガイドでは、シスコの Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して次の Cisco 1800 シリーズ サービス統合型固定構成ルータの機能を設定する手順を説明します。

- Cisco 1801、Cisco 1802、および Cisco 1803 DSL アクセス ルータ
- Cisco 1811 および Cisco 1812J イーサネット アクセス ルータ

ここでは、対象読者、このマニュアルの構成、およびマニュアルに使用されているテキストとコマンドの表記法について説明します。この章は、次の項で構成されています。

- 「対象読者」
- 「マニュアルの構成」
- 「表記法」
- 「関連資料」
- 「マニュアルの入手方法およびテクニカル サポート」
- 「シスコのテクニカル サポート」
- 「その他の情報の入手方法」

対象読者

このマニュアルは、ルータの設定に関する経験がまったくない、あるいはほとんどないネットワーク管理者から、高レベルの経験を持つネットワーク管理者まで、さまざまなバックグラウンドを持つネットワーク管理者を対象としています。このマニュアルは、次の場合に使用できます。

- Cisco Router Web Setup ツールを使用してソフトウェアを設定しており、Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して高度なソフトウェア機能を追加設定する場合。
- CLI のみを使用してソフトウェアを設定する場合。

（注） Cisco ルータにあまり慣れていないネットワーク管理者には、Cisco Router and Security Device Manager（SDM）を使用することを強くお勧めします。この Web ベースのコンフィギュレーション ツールを使用すると、LAN および WAN インターフェイス、ルーティング、Network Address Translation（NAT; ネットワーク アドレス変換）、ファイアウォール、VPN、およびその他の機能を

ルータに設定できます。SDM リリース ノートおよびその他の SDM マニュアルを入手するには、http://www.cisco.com/go/sdm にアクセスして、[Technical Documentation] リンクをクリックしてください。

ルータの設定に必要な情報がどの章に記載されているかを判断するには、「はじめに」の「マニュアルの構成」を参照してください。

マニュアルの構成

このマニュアルの具体的な内容は、表 1 のとおりです。

表 1　マニュアルの構成

章	タイトル	説明
第 1 章	「ルータの基本設定」	基本的なルータ機能およびインターフェイスの設定方法を説明します。
第 2 章	「ネットワークの導入例」	考えられるネットワーク配置のロード マップを示します。
第 3 章	「PPP over Ethernet と NAT の設定」	Cisco ルータに PPPoE と Network Address Translation（NAT; ネットワーク アドレス変換）を設定する手順を示します。
第 4 章	「PPP over ATM と NAT の設定」	Cisco ルータに PPPoA と Network Address Translation（NAT; ネットワーク アドレス変換）を設定する手順を示します。
第 5 章	「DHCP および VLAN による LAN の設定」	Cisco ルータに複数の VLAN を設定し、ルータが DHCP サーバとして機能するように設定する手順を示します。
第 6 章	「Easy VPN および IPSec トンネルを使用した VPN の設定」	Virtual Private Network（VPN; バーチャル プライベート ネットワーク）に Cisco Easy VPN を使用するセキュアな IP トンネルを設定する手順を示します。
第 7 章	「IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定」	VPN にセキュアな IP トンネルと Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を設定する手順を示します。
第 8 章	「簡易ファイアウォール」	Cisco ルータに基本的なファイアウォールを設定する手順を示します。
第 9 章	「ワイヤレス LAN 接続」	ワイヤレス LAN を設定する手順を示します。
第 10 章	「設定例」	これより前の章で設定した機能を示す設定例の要約を示します。
第 11 章	「追加の設定オプション」	第 3 部のロード マップを示します。
第 12 章	「セキュリティ機能の設定」	ファイアウォールや VPN の設定など、Cisco IOS セキュリティ機能の基本設定について説明します。
第 13 章	「ダイヤル バックアップとリモート管理の設定」	Cisco ルータにダイヤル バックアップおよびリモート管理を設定する手順を示します。
第 14 章	「トラブルシューティング」	忘れてしまったソフトウェア パスワードの回復方法など、問題の識別と解決に関する情報を示します。
付録 A	「Cisco IOS ソフトウェアの基礎知識」	設定を開始する前に、Cisco IOS ソフトウェアについて知っておく必要のあることを説明します。
付録 B	「概要」	機能の概要を説明します。

表 1　マニュアルの構成（続き）

章	タイトル	説明
付録 C	「ROM モニタ」	ROM Monitor（ROMMON）ユーティリティの使い方を説明します。
付録 D	「共通ポート割り当て」	現在割り当てられている Transmission Control Protocol（TCP; 伝送制御プロトコル）および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号について説明します。
索引		

表記法

このマニュアルに記載されている手順や情報には、次の項に示す表記法が使用されています。

（注）、注意、ワンポイント アドバイス

（注）、注意、およびワンポイント アドバイスには、次の表記法と記号が使用されています。

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

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

ワンポイント アドバイス　この記号は、「*時間の節約に役立つ操作*」を意味します。

コマンドの表記法

表 2に、このマニュアルに使用されているコマンド構文を示します。

表 2　コマンド構文の表記法

表記法	説明
boldface	コマンドおよびキーワード
italic	ユーザによるコマンド入力
[　]	任意のキーワードと、システム プロンプトに対するデフォルトの応答は、角カッコに囲まれています。
{**x** | **x** | **x**}	選択すべきキーワード（**x** の部分）は、波カッコで囲み、縦棒で区切って表します。いずれか 1 つを選択しなければなりません。

表 2　　コマンド構文の表記法（続き）

表記法	説明
^ または Ctrl	*Control* というラベルの付いたキーを表します。たとえば、*^D* または *Ctrl-D* と表記されている場合、Ctrl キーを押さえながら D キーを押します。
`screen` フォント	画面に表示される情報の例を表します。
太字の **`screen`** フォント	入力が必要な情報の例

関連資料

表 3 に、これらのルータの関連情報が記載されたマニュアルを示します。

表 3　　関連資料および参照資料

シスコ製品	マニュアル名
Cisco 1800 シリーズ 固定構成ルータ	『*Cisco 1811 and Cisco 1812 Integrated Services Router Cabling and Installation*』
	『*Cisco 1801, Cisco 1802, and Cisco 1803 Integrated Services Router Cabling and Installation*』
	『*Cisco 1800 Series Integrated Services Router (Fixed) Hardware Installation Guide*』
	『*Regulatory Compliance and Safety Information for Cisco 1800 Integrated Services Routers (Fixed)*』
	『*Cisco Modular Access Router Cable Specifications*』
Cisco アクセス ルータ ワイヤレス LAN マニュアル	『*Cisco Access Router Wireless Configuration Guide*』
	Cisco アクセス ルータ アンテナ マニュアル
	『*Declarations of Conformity and Regulatory Information for Cisco Access Products with 802.11a/b/g and 802.11b/g Radios*』
ネットワーク管理システム	*Cisco Router and Security Device Manager (SDM) Quick Start Guide*
	ネットワーク管理ソフトウェア マニュアル
Cisco IOS ソフトウェア	Cisco IOS ソフトウェア マニュアル（全リリース）。ルータにインストールされている Cisco IOS ソフトウェア リリースに対応するマニュアルを参照してください。

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

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。
・テクニカル サポートを受ける
・ソフトウェアをダウンロードする
・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
・ツールおよびリソースへアクセスする
 - Product Alert の受信登録
 - Field Notice の受信登録
 - Bug Toolkit を使用した既知の問題の検索
・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
・トレーニング リソースへアクセスする
・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

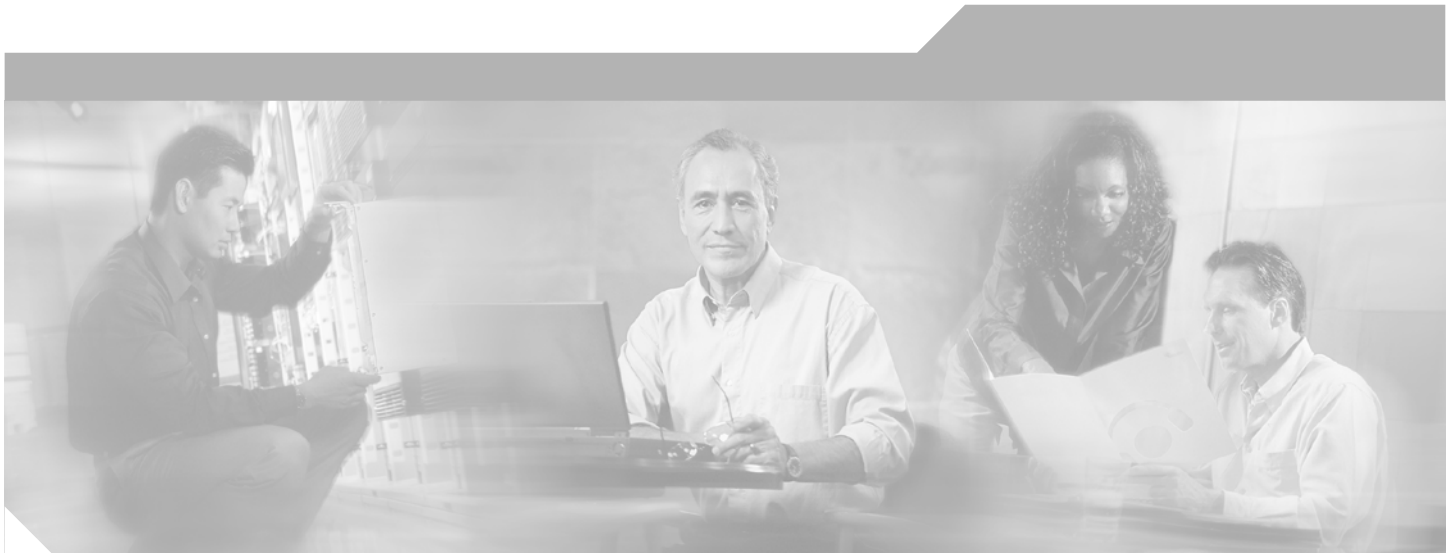
シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。
  http://www.cisco.com/offer/subscribe
- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。
  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/
- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。
  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en
- 『Cisco Product Quick Reference Guide』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『Cisco Product Quick Reference Guide』を発注するには、次の URL にアクセスしてください。
  http://www.cisco.com/go/guide
- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。
  http://www.cisco.com/go/services
- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/
- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。
  http://www.cisco.com/go/marketplace/docstore
- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。
  http://www.ciscopress.com
- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp
- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスできます。
  http://www.cisco.com/ipj
- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。
  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html
- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml



PART 1

はじめに

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。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。

この章で説明する内容は、次のとおりです。

- 「インターフェイス ポート ラベル」
- 「デフォルト設定の表示」
- 「設定に必要な情報」
- 「基本パラメータの設定」
- 「スタティック ルートの設定」
- 「ダイナミック ルートの設定」
- 「拡張 IGRP の設定」

該当する場合、各項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 モードへのアクセス方法の詳細については、付録 A「Cisco IOS ソフトウェアの基礎知識」の「グローバル コンフィギュレーション モードの開始」を参照してください。次の表に示すコマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。

インターフェイス ポート ラベル

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

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

ルータ	Interface	ポート ラベル
Cisco 1801	ファスト イーサネット LAN	SWITCH および FE8–FE5（上部）、FE x および FE4–FE1（下部）
	ファスト イーサネット WAN	FE0
	ATM WAN	ADSLoPOTS
	ワイヤレス LAN	LEFT、RIGHT/PRIMARY
	BRI	ISDN S/T
Cisco 1802	ファスト イーサネット LAN	SWITCH および FE8–FE5（上部）、FE x および FE4–FE1（下部）
	ファスト イーサネット WAN	FE0
	ATM WAN	ADSLoISDN
	ワイヤレス LAN	LEFT、RIGHT/PRIMARY
	BRI	ISDN S/T
Cisco 1803	ファスト イーサネット LAN	SWITCH および FE8–FE5（上部）、FE x および FE4–FE1（下部）
	ファスト イーサネット WAN	FE0
	ATM WAN	G.SHDSL
	ワイヤレス LAN	LEFT、RIGHT/PRIMARY
	BRI	ISDN S/T
Cisco 1811	ファスト イーサネット LAN	SWITCH および FE9–FE6（上部）、FE x および FE5–FE2（下部）
	ファスト イーサネット WAN	FE0–FE1
	ワイヤレス LAN	LEFT、RIGHT/PRIMARY
	USB	1–0
	V.92	MODEM
Cisco 1812J	ファスト イーサネット LAN	SWITCH および FE9–FE6（上部）、FE x および FE5–FE2（下部）
	ファスト イーサネット WAN	FE0–FE1
	ワイヤレス LAN	LEFT、RIGHT/PRIMARY
	BRI	ISDN S/T
	USB	1–0

デフォルト設定の表示

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、例 1 に示すように、**show running-config** コマンドを使用します。

（注）　初期設定を表示できず、「No Password Set」エラー メッセージを受信した場合は、初期パスワードをリセットする必要があります。詳細は、第 14 章「トラブルシューティング」の「パスワードを忘れた場合の回復方法」を参照してください。

例 1　　Cisco 1812J の起動時のデフォルト設定

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
ip cef
!
ip ips po max-events 100
no ftp-server write-enable
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 shutdown
!
interface FastEthernet3
 no ip address
 shutdown
!
```

```
interface FastEthernet4
 no ip address
 shutdown
!
interface FastEthernet5
 no ip address
 shutdown
!
interface FastEthernet6
 no ip address
 shutdown
!
interface FastEthernet7
 no ip address
 shutdown
!
interface FastEthernet8
 no ip address
 shutdown
!
interface FastEthernet9
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
ip classless
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
```

設定に必要な情報

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

- インターネット接続を設定する場合、次の情報を収集してください。
  - ログイン名として割り当てられている Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）クライアント名
  - PPP 認証のタイプ : Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）または Password Authentication Protocol（PAP）
  - Internet Service Provider（ISP; インターネット サービス プロバイダー）アカウントにアクセスするための PPP パスワード
  - DNS サーバの IP アドレスおよびデフォルト ゲートウェイ
- 企業ネットワークへの接続を設定する場合は、ユーザとネットワーク管理者の間で、ルータの WAN インターフェイスに関する次の情報について打ち合わせておく必要があります。

  - PPP 認証のタイプ：CHAP または PAP
  - ルータにアクセスするための PPP クライアント名
  - ルータにアクセスするための PPP パスワード
- IP ルーティングを設定する場合、次の準備が必要です。
  - IP ネットワークのアドレス指定方式を作成します。
  - IP アドレスなどの IP ルーティング パラメータ情報と ATM Permanent Virtual Circuit（PVC; 相手先固定接続）を特定します。通常、これらの PVC パラメータは、Virtual Path Identifier（VPI; 仮想パス識別子）、Virtual Circuit Identifier（VCI; 仮想回線識別子）、およびトラフィック シェーピング パラメータです。
  - サービス プロバイダーから付与された PVC 番号、VPI、および VCI を特定します。
  - PVC ごとに、サポートされている AAL5 カプセル化のタイプを判別します。次のいずれかになります。

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

    AAL5MUX PPP：このタイプでのカプセル化では、PPP 関連設定項目を判別する必要があります。
- ADSL または G.SHDSL 回線を使用して接続する場合、次の準備が必要です。
  - 電話会社と回線契約を結びます。

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

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

    該当する情報の収集が済んだら、ルータの設定を行うことができます。「基本パラメータの設定」の作業から設定を始めてください。

基本パラメータの設定

ルータを設定するには、次のいずれか、または複数の作業を実行します。

- 「グローバル パラメータの設定」
- 「ファスト イーサネット LAN インターフェイスの設定」
- 「WAN インターフェイスの設定」
- 「ループバック インターフェイスの設定」
- 「ルータへのコマンドライン アクセスの設定」

作業完了後のネットワーク設定を示すため、作業ごとに設定例が示されています。

グローバル パラメータの設定

ルータに対して選択したグローバル パラメータを設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します（コンソール ポート使用時）。
		リモート端末を使用してルータに接続している場合は、次のコマンドを使用します。
		`telnet router name or address`
		`Login: login id`
		`Password: *********`
		`Router> enable`

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

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

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

グローバル パラメータ コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。

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るので、個別のアドレスによる設定は行われません。アクセスは VLAN を通じて提供されます。必要に応じて、このインターフェイスを別の VLAN に割り当てることが可能です。VLAN 作成の詳細については、第 5 章「DHCP および VLAN による LAN の設定」を参照してください。

WAN インターフェイスの設定

Cisco 1811 ルータおよび Cisco 1812J ルータにはそれぞれ、WAN 接続用に 2 つのファスト イーサネット インターフェイスが搭載されています。Cisco 1801 ルータ、Cisco 1802 ルータ、および Cisco 1803 ルータにはそれぞれ、WAN 接続用に 1 つの ATM インターフェイスが搭載されています。

使用しているルータ モデルに基づいて、次のいずれかの手順で 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」
- 「ATM WAN インターフェイスの設定」

ファスト イーサネット WAN インターフェイスの設定

この手順は、Cisco 1811 ルータ モデルおよび Cisco 1812J ルータ モデルにのみ適用します。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 モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)#interface fastethernet 0`
	`Router(config-int)#`
		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。
		
		（注）　Cisco 1800 シリーズ ルータのファスト イーサネット WAN ポートには、0 ～ 1 の番号が割り当てられています。

ステップ 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-int)# ip address 192.1.12.2 255.255.255.0`
	`Router(config-int)#`
		指定されたファスト イーサネット インターフェイスの IP アドレスおよびサブネット マスクを設定します。

ステップ 3	**no shutdown**
	
	例：
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		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-int)# 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。

必要に応じて、その他のファスト イーサネット WAN インターフェイスに対してこの手順を繰り返します。

ATM WAN インターフェイスの設定

この手順は、Cisco 1801、Cisco 1802、および Cisco 1803 モデルにのみ適用します。

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

	コマンド	目的

ステップ 1	***Cisco 1803 の場合のみ：***
	controller dsl 0
	mode atm
	exit
	
	例：
	`Router(config)# controller dsl 0`
	`Router(config-controller)# mode atm`
	`Router(config-controller)# exit`
	`Router(config)#`
		G.SHDSL シグナリングを使用するルータに対して、これらのコマンドを実行します。
		ADSL シグナリングを使用するルータの場合は、このステップを無視します。

ステップ 2	**interface** *type number*
	
	例：
	`Router(config)# interface atm0`
	`Router(config-int)#`
		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	**ip address** *ip-address mask*
	
	例：
	`Router(config-int)# ip address 200.200.100.1 255.255.255.0`
	`Router(config-int)#`
		ATM 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 4	**no shutdown**
	
	例：
	`Router(config-int)# no shutdown`
	`Router(config-int)#`
		ATM 0 インターフェイスをイネーブルにします。

ステップ 5	**exit**
	
	例：
	`Router(config-int)# 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。

ワイヤレス インターフェイスの設定

ワイヤレス インターフェイスは、ワイヤレス LAN 接続を介してルータに接続できるようにします。ワイヤレス接続の設定の詳細については、第 9 章「ワイヤレス LAN 接続」および『*Cisco Access Router Wireless Configuration Guide*』を参照してください。

ループバック インターフェイスの設定

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

ループバック コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。

ループバック インターフェイスを設定するには、次の手順を実行します。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface Loopback 0`
	`Router(config-int)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-int)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-int)#`
		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-int)# exit`
	`Router(config)#`
		ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

設定例

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

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

```
ip nat outside
```

設定の確認

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

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

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

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

ルータへのコマンドライン 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。

	コマンド	目的

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

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

	コマンド	目的

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

ステップ 4	**exec-timeout** *minutes* [*seconds*]
	
	例：
	`Router(config)# exec-timeout 5 30`
	`Router(config)#`
		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。デフォルト値は 10 分です。任意で、間隔値に秒数を追加します。
		
		この例では、5 分 30 秒のタイムアウトを表示します。「0 0」のタイムアウトを入力すると、タイムアウトが発生しません。

ステップ 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	例：
	`Router(config)# line vty 0 4`
	`Router(config)#`
		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)# password aldf2ad1`
	`Router(config)#`
		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)# login`
	`Router(config)#`
		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)# end`
	`Router#`
		回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

コマンド ライン コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。

設定例

次の設定は、コマンドライン アクセス コマンドを示します。

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

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

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 トポロジー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。Cisco 1800 シリーズ ルータへのスタティック ルートの設定は任意です。

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。

	コマンド	目的

ステップ 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
	`Router(config)#`
		IP パケットのスタティック ルートを指定します。
		
		このコマンドの詳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 2 of 4: Routing Protocols*』を参照してください。

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

スタティック ルーティング コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。スタティック ルーティングの概要については、付録 B「概要」を参照してください。

設定例

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

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

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

設定の確認

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

次の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
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ーに基づいて、ネットワーク プロトコルがパスを自動調整します。ダイナミック ルーティングの変更は、ネットワーク上の他のルータにも反映されます。

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

RIP 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。

	コマンド	作業

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

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

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

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

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

ダイナミック ルーティング コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。RIP の概要については、付録 B「概要」を参照してください。

設定例

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

この設定を表示するには、特権 EXEC モードから **show running-config** コマンドを実行します。

```
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
```

設定の確認

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

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

Gateway of last resort is not set

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

拡張 IGRP の設定

Enhanced IGRP（EIGRP; 拡張 IGRP）を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

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

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

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

IP EIGRP コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。EIGRP の概要については、付録 B「概要」を参照してください。

設定例

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

この設定を表示するには、特権 EXEC モードから **show running-config** コマンドを実行します。

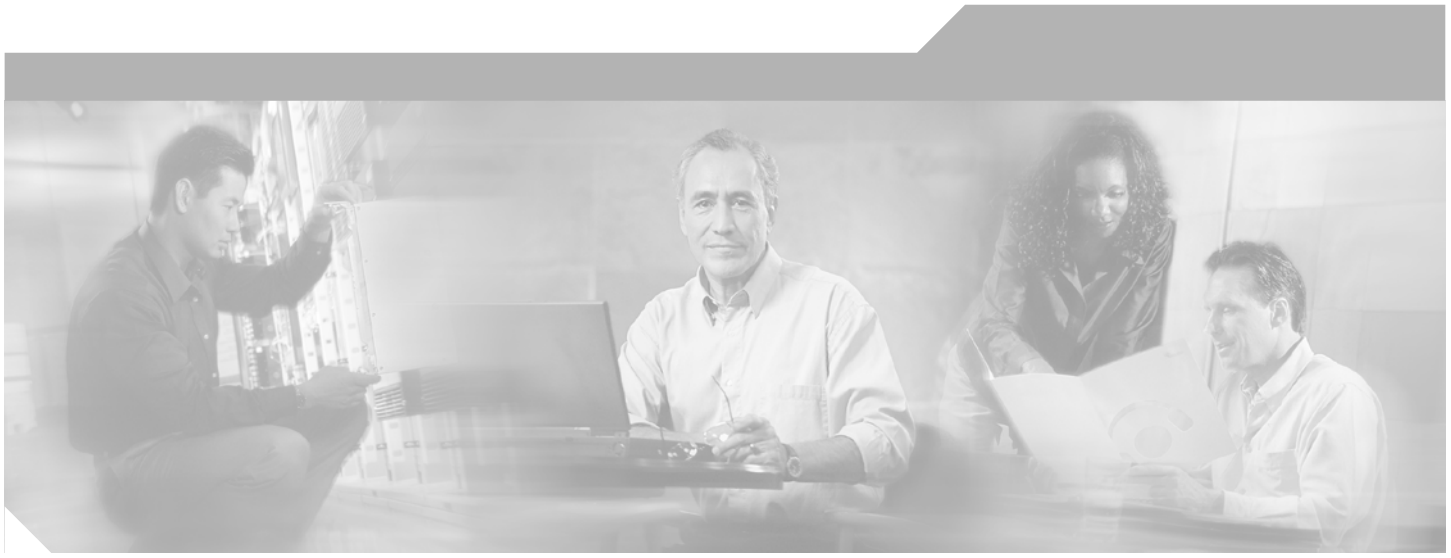
```
!
router eigrp 109
    network 192.145.1.0
        network 10.10.12.115
!
```

設定の確認

IP EIGRP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、「D」で表される EIGRP ルートを探します。次の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
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```



PART 2

イーサネットおよび DSL アクセス用のルータの設定

ネットワークの導入例

ここでは、Cisco ISR 1800 シリーズ ルータを使用したさまざまなイーサネットおよび Digital Subscriber Line（DSL; デジタル加入者線）ベースのネットワーク設定について紹介します。各シナリオの説明には、ネットワーク トポロジー、ネットワーク設定を実装するためステップ別手順、および設定の結果を示す設定例が使用されます。イーサネットベースのシナリオには、Cisco 1811 および Cisco 1812J ルータ モデル、DSL ベースのシナリオには、Cisco 1801、Cisco 1802 および Cisco 1803 ルータ モデルを使用できます。

最初のネットワーク シナリオでは、Network Address Translation（NAT; ネットワーク アドレス変換）による WAN インターフェイスを介した Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）による、簡易ネットワーク設定を提供します。主要な機能をさらに設定することにより、前のシナリオに基づいて次のシナリオが構成されています。

各シナリオは、ネットワークで考えられるすべてのニーズに対応するものではありません。ネットワークを構築するときのモデルとして使用してください。例で示されている機能を使用せずに、実際のニーズに合うように機能を追加したり置き換えたりすることもできます。

特定の機能が、使用しているルータと互換性があることを確認する場合は、Software Advisor ツールを使用します。このツールにアクセスするには www.cisco.com で [Technical Support & Documentation] > [Tools & Resources] と選択し、シスコのユーザ名とパスワードを入力します。

イーサネットベースのネットワーク導入の場合

イーサネットベースのネットワーク用にルータを設定する場合は、次の設定例を参考にしてください。

- 第 3 章「PPP over Ethernet と NAT の設定」
- 第 5 章「DHCP および VLAN による LAN の設定」
- 第 6 章「Easy VPN および IPSec トンネルを使用した VPN の設定」
- 第 7 章「IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定」
- 第 8 章「簡易ファイアウォール」

DSL ベースのネットワーク導入の場合

DSL ベースのネットワーク用にルータを設定する場合は、次の設定例を参考にしてください。

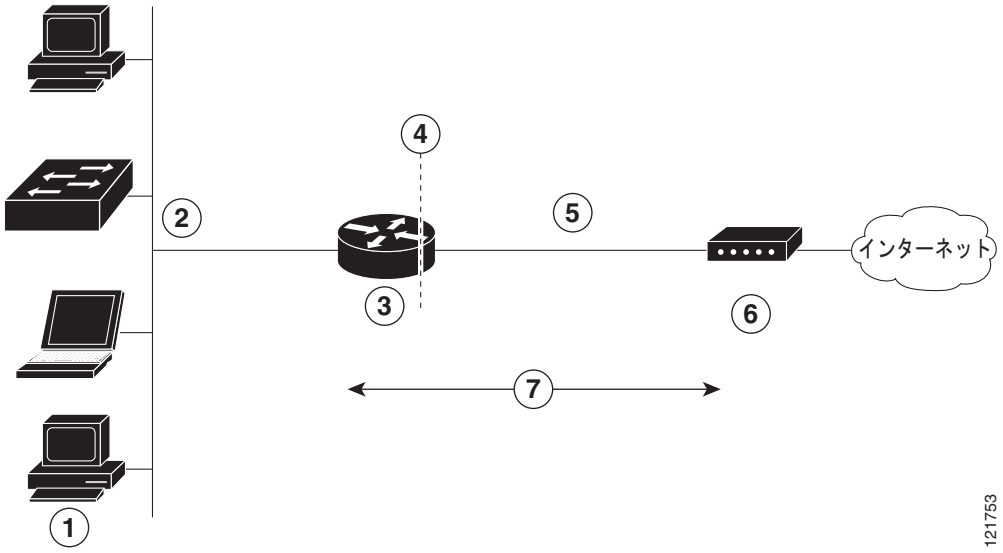
- 第 4 章「PPP over ATM と NAT の設定」
- 第 5 章「DHCP および VLAN による LAN の設定」
- 第 6 章「Easy VPN および IPSec トンネルを使用した VPN の設定」
- 第 7 章「IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定」
- 第 8 章「簡易ファイアウォール」

PPP over Ethernet と NAT の設定

Cisco 1811 および Cisco 1812J サービス統合型固定構成ルータは、Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよび Network Address Translation（NAT; ネットワーク アドレス変換）をサポートします。

ルータの背後の LAN には、複数の PC を接続できます。これらの PC からのトラフィックに対しては、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 3-1 に、Cisco ルータに PPPoE クライアントと NAT が設定された一般的な配置シナリオを示します。

図 3-1　　PPP over Ethernet 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
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 1811 または Cisco 1812J サービス統合型ルータ
4	NAT が実行されるポイント
5	ファスト イーサネット WAN インターフェイス（NAT の外部インターフェイス）
6	インターネットに接続しているケーブル モデムまたはその他のサーバ（Cisco 6400 サーバなど）
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 セッションは、Cisco 1800 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。確立された PPPoE クライアント セッションは、次のいずれかの方法で終了できます。

- **clear vpdn tunnel pppoe** コマンドを入力する。PPPoE クライアント セッションが終了し、PPPoE クライアントはただちにセッションの再確立を試みます。セッションがタイムアウトした場合にも、この動作が発生します。
- **no pppoe-client dial-pool** *number* コマンドを入力して、セッションをクリアする。PPPoE クライアントは、セッションの再確立を試みません。

NAT

NAT（Cisco ルータの端に点線で表示）は、2 つのアドレス指定ドメインと内部送信元アドレスを示します。送信元リストには、パケットがネットワークをどのように通過するかが定義されます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定」
- 「ファスト イーサネット WAN インターフェイスの設定」
- 「ダイヤラ インターフェイスの設定」
- 「ネットワーク アドレス変換の設定」

「設定例」には、これらの設定作業の結果を示した例が示されています。

バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定

Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）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。このモードの開始に関する詳細については、「グローバル パラメータの設定」（P.1-6）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 1	**vpdn enable**
	
	例：
	`Router(config)# vpdn enable`
	`Router(config-vpdn)#`
		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)# vpdn group 1`
	`Router(config-vpdn-grp)#`
		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-grp)# request-dialin`
	`Router(config-vpdn-grp)#`
		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	**initiate to ip** *ip-address*
	
	例：
	`Router(config-vpdn-grp)# initiate to 192.168.1.1`
	`Router(config-vpdn-grp)#`
		要求のトンネリング先にするアドレスを指定します。
		
		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。

ステップ 5	**protocol {l2f | l2tp | pppoe | any}**
	
	例：
	`Router(config-vpdn-grp)# protocol pppoe`
	`Router(config-vpdn-grp)#`
		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。

	コマンドまたはアクション	目的

ステップ 6	**exit**
	
	例：
	`Router(config-vpdn-grp)# exit`
	`Router(config-vpdn)#`
		VPDN グループの設定を終了します。

ステップ 7	**exit**
	
	例：
	`Router(config-vpdn)# exit`
	`Router(config)#`
		VPDN の設定を終了し、グローバル コンフィギュレーション モードに戻ります。

ファスト 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（お使いの Cisco ルータ）は内部と外部の両方で 10/100-Mbps イーサネット インターフェイスを介して通信します。

（注）Cisco 1800 シリーズのサービス統合型固定構成ルータには、ファスト イーサネット ポート FE0 および FE1 に関するハードウェア制限があります。半二重モードでトラフィックが許容量の 100 % 以上（各方向に 5 Mbps 以上発生することと同等）になると、インターフェイスでは過度の衝突が発生し、1 秒ごとにリセットされます。この問題を回避するため、トラフィックの許容量を 100 % 未満に制限する必要があります。

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。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)#interface fastethernet 0`
	`Router(config-if)#`
		ファスト イーサネット WAN インターフェイス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。
		
		Cisco 1800 サービス統合型ルータには、2 つのファスト イーサネット WAN インターフェイスが搭載されています。次の手順を使用して、これらのインターフェイスのいずれか、または両方を設定できます。

ステップ 2	**pppoe-client dial-pool-number** *number*
	
	例：
	`Router(config-if)# pppoe-client dial-pool-number 1`
	`Router(config-if)#`
		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。

	コマンド	目的

ステップ 3	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		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`
	`Router(config)#`
		ファスト イーサネット インターフェイスのコンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

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。

ルータの一方のファスト イーサネット LAN インターフェイスに対してダイヤラ インターフェイスを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**interface dialer** *dialer-rotary-group-number*
	
	例：
	`Router(config)# interface dialer 0`
	`Router(config-if)#`
		ダイヤラ インターフェイス（番号 0 ～ 255）を作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address negotiated**
	
	例：
	`Router(config-if)# ip address negotiated`
	`Router(config-if)#`
		インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。

ステップ 3	**ip mtu** *bytes*
	
	例：
	`Router(config-if)# ip mtu 1492`
	`Router(config-if)#`
		IP Maximum Transmission Unit（MTU; 最大伝送ユニット）のサイズを設定します。デフォルトの最小値は 128 バイトです。イーサネットの最大値は 1492 バイトです。

ステップ 4	**encapsulation** *encapsulation-type*
	
	例：
	`Router(config-if)# encapsulation ppp`
	`Router(config-if)#`
		送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。

	コマンド	目的

ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]}
	
	例：
	`Router(config-if)# ppp authentication chap`
	`Router(config-if)#`
		PPP 認証方式を Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）に設定します。
		
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 6	**dialer pool** *number*
	
	例：
	`Router(config-if)# dialer pool 1`
	`Router(config-if)#`
		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`
	`Router(config-if)#`
		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`
	`Router(config)#`
		ダイヤラ 0 インターフェイスの設定を終了します。

ステップ 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	
	例：
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		ダイヤラ リストを作成し、ダイヤル グループを関連付けます。パケットは、指定されたインターフェイス ダイヤラ グループを通じて転送されます。
		
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*}
	
	例：
	`Router(config)# ip route 10.10.25.2 0.255.255.255 dialer 0`
	`Router(config)#`
		ダイヤラ 0 インターフェイスのデフォルト ゲートウェイに IP ルートを設定します。
		
		このコマンドの詳細および設定可能なその他のパラメータについては、『*Cisco IOS IP Command Reference, Volume 2; Routing Protocols*』を参照してください。

ネットワーク アドレス変換の設定

Network Address Translation（NAT; ネットワーク アドレス変換）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。

外部のファスト イーサネット WAN インターフェイスにダイナミック NAT を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
	
	例：
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255`
	`Router(config)#`
		NAT 用のグローバル IP アドレスのプールを作成します。

ステップ 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	
	例 1：
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	
	または
	
	例 2：
	`Router(config)# ip nat inside source list acl1 pool pool1`
		内部インターフェイス上のダイナミック アドレス変換をイネーブルにします。
		
		最初の例は、アクセス リスト *1* で許可されたアドレスが、ダイヤラ インターフェイス *0* に指定されているいずれかのアドレスに変換されることを示しています。
		
		次の例は、アクセス リスト *acl1* で許可されたアドレスが、NAT プール *pool1* に指定されたいずれかのアドレスに変換されることを示しています。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)# interface vlan 1`
	`Router(config-if)#`
		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 インターフェイスが存在する）に対して、コンフィギュレーション モードを開始します。

ステップ 4	**ip nat** {**inside** | **outside**}
	
	例：
	`Router(config-if)# ip nat inside`
	`Router(config-if)#`
		指定の VLAN インターフェイスを NAT の内部インターフェイスとして識別します。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

	コマンド	目的

ステップ 5	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		イーサネット インターフェイス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`
	`Router(config)#`
		ファスト イーサネット インターフェイスに対するコンフィギュレーション モードを終了します。

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)#interface fastethernet 0`
	`Router(config-if)#`
		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（FE0 または FE1）に対して、コンフィギュレーション モードを開始します。

ステップ 8	**ip nat** {**inside** | **outside**}
	
	例：
	`Router(config-if)# ip nat outside`
	`Router(config-if)#`
		指定の WAN インターフェイスを NAT の外部インターフェイスとして識別します。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 9	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		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`
	`Router(config)#`
		ファスト イーサネット インターフェイスに対するコンフィギュレーション モードを終了します。

ステップ 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] 例： `Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255`	変換が必要なアドレスを示す標準アクセス リストを定義します。 （注）　その他のアドレスはすべて、暗黙的に拒否されます。

（注）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の詳細については、第 1 章「ルータの基本設定」を参照してください。

NAT コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。NAT の概要については、付録 B「概要」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）VLAN インターフェイスは LAN 上にあるので、ここではプライベート IP アドレスを使用しています。

（注）「**(default)**」のマークが付いているコマンドは、**show running-config** コマンドを実行すると自動的に生成されます。

```
!
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
!
interface FastEthernet 0
ip address 192.1.12.2 255.255.255.0
no ip directed-broadcast (default)
ip nat outside
!
interface dialer 1
ip address negotiated
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 1 overload
ip classless (default)
ip route 10.10.25.2 0.255.255.255 dialer 1
!
```

設定の確認

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。

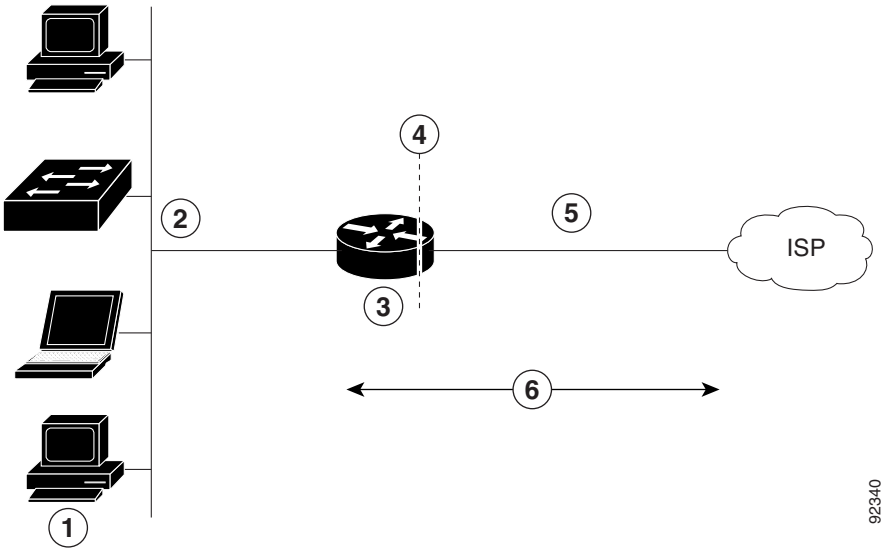
```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  FastEthernet4
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

PPP over ATM と NAT の設定

Cisco 1801、Cisco 1802、および Cisco 1803 アクセス ルータは、Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）クライアントと Network Address Translation（NAT; ネットワーク アドレス変換）をサポートします。

ルータの背後の LAN には、複数の PC を接続できます。PC からのトラフィックに対しては、PPPoA セッションに送信する前に暗号化やフィルタリングなどを行うことができます。PPP over ATM により、ダイヤル ネットワークのような簡素化されたアドレス処理と単純なユーザ検証がネットワーク ソリューションで実現します。図 4-1 に、Cisco ルータに PPPoA クライアントと NAT を設定する一般的な配置シナリオを示します。このシナリオでは、ATM 接続に単一のスタティック IP アドレスを使用しています。

図 4-1　　PPP over ATM と NAT



1	複数のネットワーク接続デバイス（デスクトップ、ラップトップ PC、スイッチ）を使用するスモール ビジネス
2	ファスト イーサネット LAN インターフェイス（NAT の内部インターフェイス、192.168.1.1/24）
3	PPPoA クライアント（Cisco 1801、Cisco 1802、または Cisco 1803 ルータ）
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	クライアントと ISP の 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 上のスモール ビジネスまたはリモート ユーザは、WAN 接続で次のプロトコルを使用して、Internet Service Provider（ISP; インターネット サービス プロバイダー）に接続できます。

- Cisco 1801 ルータを使用する Plain Old Telephone Service（POTS; 一般電話サービス）経由の Asymmetric Digital Subscriber Line（ADSL; 非対称デジタル加入者線）
- Cisco 1802 ルータを使用する ADSL over Integrated Services Digital Network（ISDN; サービス統合デジタル ネットワーク）
- Cisco 1803 ルータを使用する Single-pair High-speed Digital Subscriber Line（G.SHDSL; シングル ペア高ビットレート デジタル加入者線）

ファスト イーサネット インターフェイスは、LAN を通じてデータ 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、ADSL、ISDN、または G.SHDSL 回線で送信されます。ISP との接続には、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。ATM 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 1800 シリーズ ルータによってクライアント側で開始されます。

NAT

NAT（Cisco ルータの端に点線で表示）は、2 つのアドレス指定ドメインと内部送信元アドレスを示します。送信元リストには、パケットがネットワークをどのように通過するかが定義されます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「ダイヤラ インターフェイスの設定」
- 「ATM WAN インターフェイスの設定」
- 「DSL シグナリング プロトコルの設定」
- 「ネットワーク アドレス変換の設定」

「設定例」には、これらの設定作業の結果を示した例が示されています。

ダイヤラ インターフェイスの設定

ダイヤラ インターフェイスは、デフォルトのルーティング情報、カプセル化プロトコル、および使用するダイヤラ プールなど、クライアントからのトラフィックを処理する方法を示します。また、仮想アクセスのクローニングにも使用されます。ATM インターフェイスには、複数の PPPoA クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

ルータ上の ATM インターフェイスに対してダイヤラ インターフェイスを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**interface dialer** *dialer-rotary-group-number*
	
	例：
	`Router(config)# interface dialer 0`
	`Router(config-if)#`
		ダイヤラ インターフェイス（番号 0 ～ 255）を作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address negotiated**
	
	例：
	`Router(config-if)# ip address negotiated`
	`Router(config-if)#`
		ダイヤラ インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。

ステップ 3	**ip mtu** *bytes*
	
	例：
	`Router(config-if)# ip mtu 4470`
	`Router(config-if)#`
		IP Maximum Transmission Unit（MTU; 最大伝送ユニット）のサイズを設定します。デフォルトの最小値は 128 バイトです。ATM の最大値は、4470 バイトです。

ステップ 4	**encapsulation** *encapsulation-type*
	
	例：
	`Router(config-if)# encapsulation ppp`
	`Router(config-if)#`
		送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。

ステップ 5	**ppp authentication** {*protocol1* [*protocol2*...]}
	
	例：
	`Router(config-if)# ppp authentication chap`
	`Router(config-if)#`
		PPP 認証方式を設定します。
		
		この例では、Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）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。

	コマンド	目的

ステップ 6	**dialer pool** *number*
	
	例：
	`Router(config-if)# dialer pool 1`
	`Router(config-if)#`
		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`
	`Router(config-if)#`
		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`
	`Router(config)#`
		ダイヤラ 0 インターフェイスの設定を終了します。

ステップ 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	
	例：
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		ダイヤラ リストを作成し、ダイヤル グループを関連付けます。パケットは、指定されたインターフェイス ダイヤラ グループを通じて転送されます。
		
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*}
	
	例：
	`Router(config)# ip route 10.10.25.0 255.255.255.0 dialer 0`
	`Router(config)#`
		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設定可能なその他のパラメータについては、『*Cisco IOS IP Command Reference, Volume 1 of 4: Routing Protocols*』を参照してください。

ダイヤラ インターフェイスまたはダイヤラ プールを追加する必要がある場合は、この手順を繰り返します。

ATM WAN インターフェイスの設定

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

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface atm 0`
	`Router(config-if)#`
		ATM インターフェイス（ルータの背面に ADSLoPOTS または G.SHDSL というラベルがあります）に対するインターフェイス コンフィギュレーション モードを開始します。
		（注） このインターフェイスは、ルータの基本設定時に初期設定されています。「WAN インターフェイスの設定」（P.1-7）を参照してください。

ステップ 2	**pvc** *vpi/vci*
	
	例：
	`Router(config-if)# pvc 8/35`
	`Router(config-if-atm-vc)#`
		ルータが通信する各エンド ノード（最大 10 台）用に ATM PVC を作成します。ATM 仮想回線コンフィギュレーション モードを開始します。
		PVC が定義されると、AAL5SNAP カプセル化がデフォルトで定義されます。この設定を変更するには、ステップ 3 に示すように **encapsulation** コマンドを使用します。VPI および VCI 引数は同時に 0 に設定できません。一方が 0 の場合、もう一方は 0 にできません。
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。

ステップ 3	**encapsulation** {**aal5auto** | **aal5autoppp virtual-template** *number* [**group** *group-name*] | **aal5ciscoppp virtual-template** *number* | **aal5mux** *protocol* | **aal5nlpid** | **aal5snap**}
	
	例：
	`Router(config-if-atm-vc)# encapsulation aal5mux ppp dialer`
	`Router(config-if-atm-vc)#`
		PVC のカプセル化タイプを指定し、ダイヤラ インターフェイスに戻ります。
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。

ステップ 4	**dialer pool-member** *number*
	
	例：
	`Router(config-if-atm-vc)# dialer pool-member 1`
	`Router(config-if-atm-vc)#`
		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。

	コマンド	目的

ステップ 5	**no shutdown**
	
	例：
	`Router(config-if-atm-vc)# no shutdown`
	`Router(config-if)#`
		ATM インターフェイスに対するインターフェイスおよび設定の変更をイネーブルにします。

ステップ 6	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ATM インターフェイスに対するコンフィギュレーション モードを終了します。

DSL シグナリング プロトコルの設定

DSL シグナリングは、ISP への接続用に ATM インターフェイスに設定する必要があります。Cisco 1801 は POTS を介した ADSL シグナリングを、Cisco 1802 は ISDN を介した ADSL シグナリングを、Cisco 1803 は SHDSL シグナリングをそれぞれサポートします。

適切な DSL シグナリング プロトコルを設定するには、設定しているルータに基づいて次のいずれかの項を参照してください。

- 「ADSL の設定」
- 「SHDSL の設定」

ADSL の設定

表 4-1 には、ADSL シグナリングのデフォルト設定を示します。

表 4-1　ADSL のデフォルト設定

アトリビュート	説明	デフォルト値
動作モード	ATM インターフェイスの Digital Subscriber Line（DSL; デジタル加入者線）の動作モードを指定します。 • ADSL over POTS：ANSI または ITU フル レート、または自動選択。 • ADSL over ISDN：ITU フル レート、ETSI、または自動選択。	Auto
マージン損失	マージン損失の発生可能回数を指定します。	
トレーニング ログ	トレーニング ログの有効化と無効化を切り替えます。	ディセーブル

これらの設定を変更する場合は、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

- **dsl operating-mode**（ATM インターフェイス コンフィギュレーション モードから）
- **dsl lom** *integer*
- **dsl enable-training-log**

これらのコマンドの詳細については、『*Cisco IOS Wide-Area Networking Command Reference*』を参照してください。

設定の確認

設定に誤りがないことを確認するには、特権 EXEC モードで **show dsl interface atm 0** コマンドを使用します。

SHDSL の設定

SHDSL シグナリングを使用するように、ルータの DSL コントローラを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**controller dsl** *port*
	
	例：
	`Router(config)# controller dsl 0`
	`Router(config-controller)#`
		DSL コントローラに対するコンフィギュレーション モードを開始します。

ステップ 2	**line-term** {**co** | **cpe**}
	
	例：
	`Router(config-controller)# line-term co`
	`Router(config-controller)#`
		DSL 回線の終端が Central Office（CO; セントラル オフィス）であるか、Customer Premises Equipment（CPE; 顧客宅内機器）であるかを指定します。

ステップ 3	**exit**
	
	例：
	`Router(config-controller)# exit`
	`Router(config)#`
		コントローラ 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 4	**mode** *protocol*
	
	例：
	`Router(config)# mode atm`
	`Router(config-controller)#`
		DSL コントローラのモードを指定し、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。

	コマンド	目的

ステップ 5	**line-mode** {**4-wire enhanced** | **4-wire standard** | **2-wire**}
	
	例：
	`Router(config-controller)# line-mode 4-wire standard`
	`Router(config-controller)#`
		この DSL 接続の動作が 2 線モードであるか、4 線標準モードであるか、または 4 線拡張モードであるかどうかを指定します。
		
		（注）　**line mode 4-wire** は、デフォルトで 4 線拡張モードに設定されます。

ステップ 6	**ignore-error-duration** *number*
	
	例：
	`Router(config-controller)# ignore-error-duration 15`
	`Router(config-controller)#`
		エラーを無視する時間（15 ～ 30 秒）を指定します。

ステップ 7	**exit**
	
	例：
	`Router(config-controller)# exit`
	`Router(config)#`
		コントローラ 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。

（注）　Cisco ルータを欧州ネットワークに組み込む場合は、次のいずれかのコマンドを使用してください。

CO モードの場合は、**dsl dsl-mode shdsl symmetric annex** {**A** | **B** | **B-ANFP**} コマンドを使用して annex B または B-ANFP を選択します。

CPE モードの場合は、**dsl dsl-mode shdsl symmetric annex** {**A** | **A-B** | **A-B-ANFP** | **B** | **B-ANFP**} を使用してオプション A を除く任意のオプションを選択します。

ルータでは、デフォルトで annex A が使用されます（米国）。

設定の確認

設定に誤りがないことを確認するには、特権 EXEC モードで **show controllers dsl** コマンドを使用します。

```
Router# show controllers dsl 0
DSL 0 controller UP
SLOT 0: Globespan xDSL controller chipset
Line Mode: Four Wire Standard Mode
DSL mode: SHDSL Annex A
Frame mode: Utopia
Configured Line rate: Auto
Line Re-activated 6 times after system bootup
LOSW Defect alarm: ACTIVE
CRC per second alarm: ACTIVE
Line termination: CPE

    Current 15 min CRC: 0
    Current 15 min LOSW Defect: 0
    Current 15 min ES Defect: 0
```

```
    Current 15 min SES Defect: 0
    Current 15 min UAS Defect: 33287

    Previous 15 min CRC Defect: 0
    Previous 15 min LOSW Defect: 0
    Previous 15 min ES Defect: 0
    Previous 15 min SES Defect: 0
    Previous 15 min UAS Defect: 0

Line-0 status
Chipset Version: 0
Firmware Version: A388
Modem Status: Data, Status 1
Last Fail Mode: No Failure status:0x0
Line rate: 2312 Kbps
Framer Sync Status: In Sync
Rcv Clock Status: In the Range
Loop Attenuation: 341.1450 dB
Transmit Power: 7.5 dB
Receiver Gain: 22.5420 dB
SNR Sampling: 36.8590 dB
Dying Gasp: Present
```

ネットワーク アドレス変換の設定

Network Address Translation（NAT; ネットワーク アドレス変換）は、ダイヤラ インターフェイスによって割り当てられたグローバル アドレスを使用して、標準のアクセス リストに一致するアドレスからのパケットを変換します。内部インターフェイスを介してルータに到達したパケット、ルータから発信されたパケット、またはその両方のパケットについて、可能なアドレス変換がアクセス リストで確認されます。NAT には、スタティック アドレス変換もダイナミック アドレス変換も設定できます。

外部 ATM WAN インターフェイスにダイナミック NAT を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}
	
	例：
	`Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255`
	`Router(config)#`
		NAT 用のグローバル IP アドレスのプールを作成します。

ステップ 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	
	例 1：
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	
	または
	
	例 2：
	`Router(config)# ip nat inside source list acl1 pool pool1`
		内部インターフェイス上のダイナミック アドレス変換をイネーブルにします。
		
		最初の例は、アクセス リスト *1* で許可されたアドレスが、ダイヤラ インターフェイス *0* に指定されているいずれかのアドレスに変換されることを示しています。
		
		次の例は、アクセス リスト *acl1* で許可されたアドレスが、NAT プール *pool1* に指定されたいずれかのアドレスに変換されることを示しています。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)# interface vlan 1`
	`Router(config-if)#`
		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（FE2 -FE9）が存在する）に対して、コンフィギュレーション モードを開始します。

ステップ 4	**ip nat** {**inside** | **outside**}
	
	例：
	`Router(config-if)# ip nat inside`
	`Router(config-if)#`
		ファスト イーサネット LAN インターフェイスを内部インターフェイスとして、NAT を適用します。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 5	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		イーサネット インターフェイスに対する設定変更をイネーブルにします。

	コマンド	目的

ステップ 6	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ファスト イーサネット インターフェイスに対するコンフィギュレーション モードを終了します。

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)#interface fastethernet 0`
	`Router(config-if)#`
		NAT の外部インターフェイスとする ATM WAN インターフェイス（FE0 または FE1）に対して、コンフィギュレーション モードを開始します。

ステップ 8	**ip nat** {**inside** | **outside**}
	
	例：
	`Router(config-if)# ip nat outside`
	`Router(config-if)#`
		指定の WAN インターフェイスを NAT の外部インターフェイスとして識別します。
		
		このコマンドの詳しい説明とその他の設定可能なパラメータ、およびスタティック変換をイネーブルにする方法については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 9	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		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`
	`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。

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 0.0.0.255`	変換が必要なアドレスを許可する標準アクセス リストを定義します。 **（注）**　その他のアドレスはすべて、暗黙的に拒否されます。

（注） NAT を仮想テンプレート インターフェイスで使用する場合は、ループバック インターフェイスを設定する必要があります。ループバック インターフェイスの設定については、第 1 章「ルータの基本設定」を参照してください。

NAT コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。NAT の概要については、付録 B「概要」を参照してください。

設定例

次の設定例は、この章で説明した PPPoA シナリオにおけるクライアントのコンフィギュレーションファイルの一部を示します。

VLAN インターフェイスの IP アドレスは 192.168.1.1、サブネット マスクは 255.255.255.0 です。NAT は内部と外部に設定されています。

（注）「**(default)**」のマークが付いているコマンドは、**show running-config** コマンドを実行すると自動的に生成されます。

```
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly (default)
!
interface ATM0
 no ip address
 ip nat outside
 ip virtual-reassembly
 no atm ilmi-keepalive
 pvc 8/35
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
 dsl operating-mode auto
!
interface Dialer0
 ip address negotiated
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
ip classless (default)
!
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 0.0.0.255
ip nat inside source list 1 interface Dialer0 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
dialer-list 1 protocol ip permit

ip route 10.10.25.2 0.255.255.255 dialer 0
!
```

設定の確認

PPPoA クライアントと NAT の設定を確認するには、特権 EXEC モードで **show ip nat statistics** コマンドを使用します。次の例のような確認用の出力が表示されます。

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  ATM0
Inside interfaces:
  Vlan1
```

```
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

CHAPTER 5

DHCP および VLAN による LAN の設定

Cisco 1800 シリーズ サービス統合型固定構成ルータは、物理 LAN および Virtual LAN（VLAN; 仮想 LAN）の両方でクライアントをサポートしています。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。VLAN の他のインターフェイスおよび設定については、「スイッチ ポートの設定」（P.5-7）に示します。

1	ファスト イーサネット LAN（複数のネットワーク デバイス）
2	インターネットに接続されたルータおよび DHCP サーバ（Cisco 1800 シリーズ サービス統合型ルータ）
3	VLAN 1
4	VLAN 2

DHCP

DHCP は、RFC 2131 に説明されているように、アドレス割り当てにクライアント / サーバ モデルを採用しています。管理者は、DHCP サーバとして機能する Cisco 1800 サービス統合型固定構成ルータを設定して、IP アドレスの割り当ておよびその他の TCP/IP 関連の設定情報をワークステーションに提供できます。DHCP を使用すると、IP アドレスを各クライアントに手動で割り当てるという作業を省くことができます。

DHCP サーバの設定では、サーバのプロパティ、ポリシーおよび DHCP オプションを設定する必要があります。

（注） サーバのプロパティを変更する場合には、Network Registrar データベースからのコンフィギュレーション データでサーバを毎回リロードする必要があります。

VLAN

Cisco 1800 シリーズ サービス統合型ルータ（固定構成）は、VLAN を設定できるファスト イーサネット ポートを 8 つサポートしています。スイッチ ポートで設定できるインターフェイスや機能、および設定手順を示すマニュアルへのリンクについては、「スイッチ ポートの設定」（P.5-7）を参照してください。

VLAN によって、ユーザの物理的な配置または LAN 接続に関係なく、ネットワークをユーザの論理グループに分割して、まとめることができます。

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「DHCP の設定」
- 「VLAN の設定」

（注）　この章の各手順では、ルータの基本機能、NAT による PPPoE または PPPoA をすでに設定していることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、および第 4 章「PPP over ATM と NAT の設定」を参照してください。IP アドレスをポートに割り当てるには、『*Cisco IOS IP Configuration Guide*』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。

	コマンド	目的

ステップ 1	**ip domain name** *name*
	
	例：
	`Router(config)# ip domain name smallbiz.com`
	`Router(config)#`
		未修飾のホスト名（ドット付き 10 進表記ドメイン名のない名前）を完成させるためにルータが使用する、デフォルトのドメインを特定します。

ステップ 2	**ip name-server** *server-address1 [server-address2...server-address6]*
	
	例：
	`Router(config)# ip name-server 192.168.11.12`
	`Router(config)#`
		名前およびアドレス解決に使用する 1 つ以上の Domain Name System（DNS; ドメイン ネーム システム）サーバのアドレスを指定します。

ステップ 3	**ip dhcp excluded-address** *low-address [high-address]* 例： `Router(config)# ip dhcp excluded-address 192.168.9.0`	DHCP サーバが DHCP クライアントに割り当ててはいけない IP アドレスを指定します。この例では、ルータのアドレスを除外します。

ステップ 4	**ip dhcp pool** *name*
	
	例：
	`Router(config)# ip dhcp pool dpool1`
	`Router(config-dhcp)#`
		ルータ上に DHCP アドレス プールを作成します。続いて、DHCP プール コンフィギュレーション モードを開始します。*name* 引数は、ストリングまたは整数にすることができます。

ステップ 5	**network** *network-number* [*mask* | *prefix-length*]
	
	例：
	`Router(config-dhcp)# network 10.10.0.0 255.255.255.0`
	`Router(config-dhcp)#`
		DHCP アドレス プールのサブネット番号（IP）アドレスを定義します（任意でマスクを入力します）。

	コマンド	目的

ステップ 6	**import all**
	
	例：
	`Router(config-dhcp)# import all`
	`Router(config-dhcp)#`
		ルータ データベースの DHCP 部分に DHCP オプション パラメータをインポートします。

ステップ 7	**default-router** *address* [*address2...address8*]
	
	例：
	`Router(config-dhcp)# default-router 10.1.1.1`
	`Router(config-dhcp)#`
		DHCP クライアントのデフォルト ルータを最大 8 つまで指定します。

ステップ 8	**dns-server** *address* [*address2...address8*]
	
	例：
	`Router(config-dhcp)# dns-server 192.168.35.2`
	`Router(config-dhcp)#`
		DHCP クライアントが使用できる DNS サーバを最大 8 つまで指定します。

ステップ 9	**domain-name** *domain*
	
	例：
	`Router(config-dhcp)# domain-name cisco.com`
	`Router(config-dhcp)#`
		DHCP クライアントのドメイン名を指定します。

ステップ 10	**exit**
	
	例：
	`Router(config-dhcp)# exit`
	`Router(config)#`
		DHCP コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。

設定例

次の設定例は、この章で説明してきた DHCP 設定のコンフィギュレーション ファイルの一部を示します。

```
ip dhcp excluded-address 192.168.9.0
!
ip dhcp pool dpool1
   import all
   network 10.10.0.0 255.255.255.0
   default-router 10.10.10.10
   dns-server 192.168.35.2
   domain-name cisco.com
!
ip domain name smallbiz.com
ip name-server 192.168.11.12
```

DHCP 設定の確認

DHCP 設定を表示するには、次のコマンドを使用します。

- **show ip dhcp import** : DHCP サーバ データベースにインポートされたオプションのパラメータを表示します。
- **show ip dhcp pool** : DHCP アドレス プールに関する情報を表示します。
- **show ip dhcp server statistics** : アドレス プール数、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。

	コマンド	目的

ステップ 1	**vlan ?**
	例：
	`Router# config t`
	`Router(config)#vlan ?`
	
	`WORD  ISL VLAN IDs 1-4094`
	`accounting  VLAN accounting configuration`
	`ifdescr  VLAN subinterface ifDescr`
	
	`Router(config)#vlan`
		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	*ISL VLAN ID*
	例：
	`Router(config)#vlan 2`
	`Router(config-vlan)#`
		VLAN を追加します（識別番号の範囲は 1 ～ 4094）。
		このコマンドとその他の設定可能なパラメータに関する詳細については、『*Cisco IOS Switching Services Command Reference*』を参照してください。

ステップ 3	**exit**
	例：
	`Router(config-vlan)#exit`
	`Router(config)#`
		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 コンフィギュレーションの確認

VLAN コンフィギュレーションを表示するには、次のコマンドを使用します。

- **show**：VLAN データベース モードから入力します。設定されたすべての VLAN の設定情報の概要を表示します。
- **show vlan-switch**：特権 EXEC モードから入力します。設定されたすべての VLAN の詳細情報を表示します。

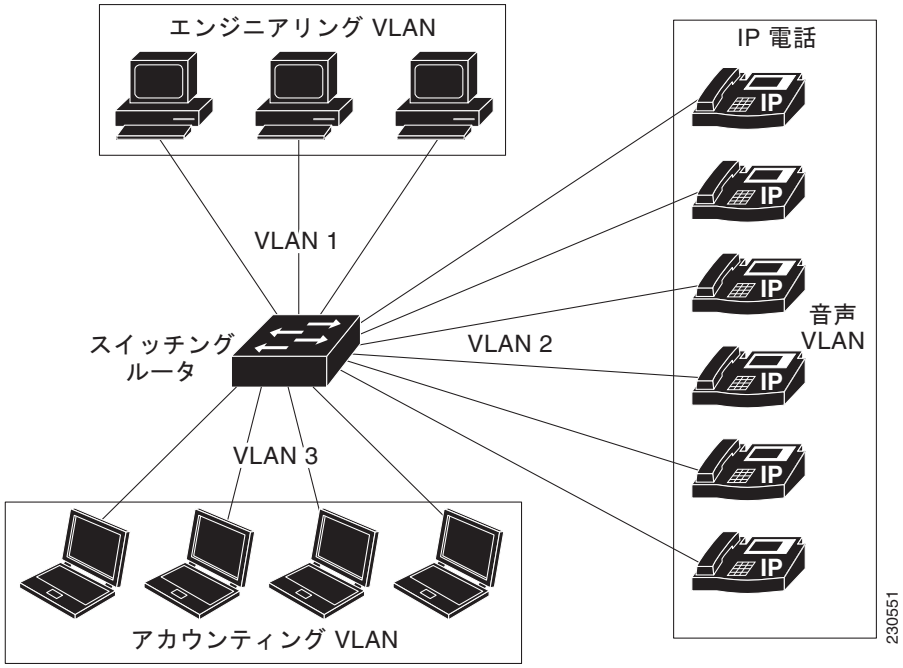
```
Router# vlan database
Router(vlan)# show
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 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, Fa2, Fa3
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
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
Router#
```

スイッチ ポートの設定

Cisco 1800（固定構成）統合型ルータの 8 つの高速イーサネット ポートは、ポートあたり 8 つの VLAN をサポートします。スイッチ ポートの VLAN を設定および確認するには、「VLAN の設定」（P.5-5）および「VLAN コンフィギュレーションの確認」（P.5-5）を参照してください。

図 5-1　VLAN セグメントが 3 つある Cisco 1800（固定構成）ルータの VLAN コンフィギュレーション



その他のスイッチ ポート設定手順（設定例を含む）や、機能およびインターフェイスについては、『*Cisco HWIC-4ESW and HWIC-9ESW EtherSwitch Interface Cards*』（Cisco.com）を参照してください。スイッチ ポートを設定するには、このマニュアルを参照してください。このマニュアルで説明されている設定手順を次に示します。

- VLAN の設定（必須）
- VLAN トランキング プロトコルの設定（任意）
- 802.1x 認証の設定（必須）
- VLAN でのスパニング ツリーの設定（必須）
- レイヤ 2 インターフェイスの設定（必須）
- MAC テーブル操作の設定（必須）
- スイッチド ポート アナライザの設定（必須）
- インターフェイスでの電源管理の設定（任意）
- IP マルチキャスト レイヤ 3 スイッチング（必須）
- ポート単位のストーム制御の設定（任意）
- フォールバック ブリッジング（任意）
- 音声とデータ用の個別のサブネットの設定（任意）
- IGMP スヌーピングの設定（任意）

ここでは、スイッチ ポートに割り当てられている VLAN で設定できる機能およびインターフェイスについて、また HWIC-4ESW および HWIC-9ESW の設定とスイッチ ポートの設定の違いについて簡単に説明します。

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）

VLAN Trunking Protocol（VTP; VLAN トランキング プロトコル）は、サーバ、クライアントおよびトランスペアレント モードの 3 種類の VTP モードをサポートします。VTP サーバ モードでは、VLAN の作成、変更、削除を実行できます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント上で VLAN の作成、変更または削除を行うことはできません。VTP トランスペアレント スイッチは、その VLAN コンフィギュレーションをアドバタイズせず、受信したアドバタイズに基づいて同期させることもありません。

802.1x 認証

スイッチ ポートは、クライアントがネットワーク アクセスを許可されているかどうかを判別します。デフォルト設定では、ポートは、無許可ステートで開始します。ポートはこのステートにある間、802.1x パケットを除いてすべての入力トラフィックおよび出力トラフィックを許容しません。クライアントの認証が成功すると、ポートは許可ステートに変更し、クライアントのすべてのトラフィック送受信を通常どおりに許可します。

802.1x 認証をサポートしていないクライアントが無許可ステートの 802.1x ポートに接続した場合、スイッチはクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

802.1x プロトコルは、ポート VLAN ID（PVID）や音声 VLAN ID（VVID）、および Cisco 1800（固定構成）シリーズでゲスト VLAN シングルおよびマルチホストをサポートする VLAN 割り当てで、認証および完全な Authentication, Authorization and Accounting（AAA; 認証、認可、アカウンティング）モードと RADIUS モードをサポートします。

（注）　スイッチ ポートでは、セキュリティ アクセス コントロール リスト、レイヤ 2 ポートの IP Access Control Lists（IP- ACL; IP アクセス コントロール リスト）および VLAN ACL 仮想 ACL はサポートされません。

レイヤ 2 インターフェイス

統合型スイッチ ポートは、Cisco IOS Catalyst ソフトウェアに基づいたイーサネット ポートでのレイヤ 2 スイッチングをサポートします。これらのポートは、レイヤ 2 イーサネット セグメント間での同時パラレル接続をサポートします。イーサネット セグメント間のスイッチド コネクションが維持されるのは、パケットの伝送時間の長さだけです。次のパケットの異なるセグメントに、別の接続を確立できます。レイヤ 2 インターフェイスの範囲を設定、範囲マクロを定義、インターフェイス速度を設定、デュプレックス モードを設定、インターフェイスの説明を追加できます。

MAC テーブル操作

MAC テーブルは、ポート セキュリティを提供するように設定されます。スイッチ ポートは、MAC アドレス テーブルを使用して、ポート間でトラフィックを転送します。このアドレス テーブルのすべての MAC アドレスは、1 つ以上のポートに対応付けられています。MAC テーブルには、次のタイプのアドレスがあります。

- ダイナミック アドレス：スイッチが学習する送信元 MAC アドレスで、使用されない場合はドロップされます。
- セキュア アドレス：手動で入力されたユニキャスト アドレスで、通常はセキュア ポートに関連付けされています。セキュア アドレスには有効期限がありません。
- スタティック アドレス：手動で入力されたユニキャストまたはマルチキャスト アドレスで、有効期限はなく、スイッチのリセット時にも消去されません。

Cisco 1800（固定構成）シリーズは、100 のセキュアおよびスタティック MAC アドレスをサポートします。通常の MAC アドレスは、50 のユーザでサポートされます。

最大スイッチ仮想インターフェイス（SVI）

Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）は、スイッチ ポートの VLAN をルータのルーティング機能またはブリッジング機能に対する 1 つのインターフェイスとして表します。1 つの VLAN に関連付けることができる SVI は 1 つだけです。VLAN に SVI を設定する必要があるのは、VLAN 間でルーティングする場合、ルーティング不能プロトコルを VLAN 間でフォールバック ブリッジングする場合、または IP ホスト接続を行う場合だけです。固定ルータの各ポートでは、8 つの SVI インターフェイスがサポートされます。

Switched Port Analyzer（SPAN）

モニタするネットワーク トラフィックのタイプを指定するパラメータを使用して、SPAN セッションを設定します。SPAN セッションを設定することで、1 つ以上のインターフェイスでトラフィックをモニタし、入力トラフィックまたは出力トラフィック、あるいはこれら両方を 1 つの宛先インターフェイスに送信できます。

スパニング ツリーを VLAN 単位でイネーブルにし、さまざまなスパニング ツリー機能を設定できます。すべてのフレームは 802.1q タグを持ちます。

IP マルチキャスト スイッチング

マルチキャスト スイッチングは、レイヤ 3 スイッチングです。マルチキャスト スイッチングを設定するには、設定される VLAN の最大数が 242 以下である必要があります。マルチキャスト グループの最大数は、VLAN の最大数と同じです。

マルチキャスト スイッチングをグローバルにイネーブルにし、レイヤ 3 インターフェイスで IP Protocol Independent Multicast（PIM）をイネーブルにして、マルチキャスト レイヤ 3 スイッチング情報を確認するように、ルータを設定できます。

（注）　Cisco 1800（固定構成）ルータでは、不明なマルチキャストまたはユニキャストのパケットをポート単位でイネーブルおよびディセーブルにすることはサポートされていません。

ポート単位のストーム制御

これらのポート単位のストーム制御手法を使用すると、フラッディングされた必要のないトラフィックの転送をブロックできます。

フォールバック ブリッジング

フォールバック ブリッジングを使用すると、スイッチは複数の VLAN またはルーテッド ポート（特に 1 つのブリッジ ドメイン内で複数の VLAN に接続されている VLAN またはルーテッド ポート）をまとめてブリッジングできます。

複数の SVI のフォールバック ブリッジングを設定するには、SVI をブリッジ グループに割り当てる必要があります。同じグループ内のすべてのブリッジは、同じブリッジ ドメインに属します。各 SVI を割り当てることができるブリッジ グループは 1 つだけです。

音声とデータ用の個別のサブネット

ネットワーク管理の簡易化とスケーラビリティの向上のために、ネットワーク管理者は Cisco IP Phone をサポートするようスイッチ ポートを設定して、音声トラフィックとデータ トラフィックが別々のサブネットに属するようにできます。

IGMP スヌーピング

デフォルトでは、IGMP スヌーピングはスイッチ ポート上でグローバルにイネーブルです。グローバルにイネーブルまたはディセーブルに設定されている場合、すべての VLAN インターフェイスでもイネーブルまたはディセーブルです。これは、VLAN 単位でイネーブルおよびディセーブルにできます。

（注）　すべてのスイッチ ポート設定手順（設定例を含む）や、機能およびインターフェイスについては、『*Cisco HWIC-4ESW and HWIC-9ESW EtherSwitch Interface Cards*』（Cisco.com）を参照してください。スイッチ ポートを設定するには、このマニュアルを参照してください。

Easy VPN および IPSec トンネルを使用した VPN の設定

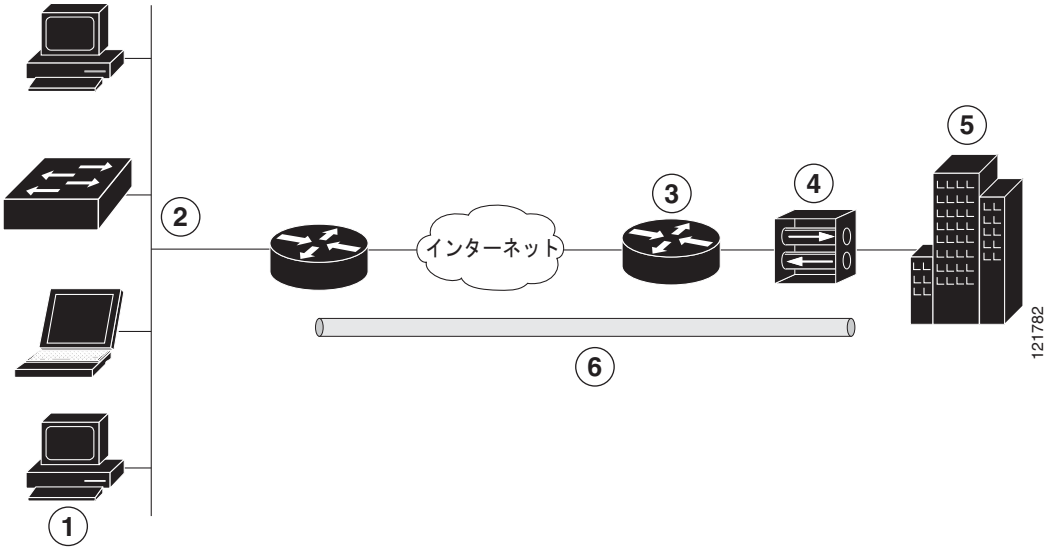
Cisco 1800 シリーズ サービス統合型固定構成ルータは Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の作成をサポートします。

Cisco ルータと他のブロードバンド デバイスは、インターネットへの高パフォーマンスな接続を提供しますが、多くのアプリケーションでは、高レベルの認証を実行し、2 つの特定のエンドポイント間でデータを暗号化する VPN 接続のセキュリティも必要です。

サイト間とリモート アクセスの 2 種類の VPN がサポートされます。サイト間 VPN は、ブランチ オフィスとコーポレート オフィスを接続する場合などに使用します。リモート アクセス VPN は、企業ネットワークにログインする際にリモート クライアントによって使用されます。

この章の例は、Cisco Easy VPN と IPSec トンネルを使用してリモート クライアントと企業ネットワーク間の接続を設定し、セキュアにするリモート アクセス VPN の構成を示しています。図 6-1 は、一般的な構成例を示します。

図 6-1　　IPSec トンネルを使用したリモート アクセス VPN



1	リモート、ネットワークで接続されたユーザ
2	VPN クライアント：Cisco 1800 シリーズ サービス統合型ルータ
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 192.168.101.1 の Cisco VPN 3000 コンセントレータなど）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN

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、WINS サーバ アドレス、スプリットトンネリング フラグなど）を、VPN サーバ（IPSec サーバとして機能している Cisco VPN 3000 シリーズ コンセントレータなど）で定義することができます。

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

Cisco Easy VPN クライアント機能は、クライアント モードとネットワーク拡張モードの 2 つのモードのいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、中央サイトでは利用できません。ネットワーク拡張モードを使用すると、（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 1800 サービス統合型ルータなどの 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 Network Address Translation/Peer Address Translation（NAT/PAT; ネットワーク アドレス変換 / ピア アドレス変換）パラメータを設定する必要があります。

設定作業

このネットワーク シナリオのルータを設定するには、次の作業を実行します。

- 「IKE ポリシーの設定」
- 「グループ ポリシー情報の設定」
- 「暗号マップへのモード設定の適用」
- 「ポリシー ルックアップのイネーブル化」
- 「IPSec トランスフォームおよびプロトコルの設定」
- 「IPSec 暗号方式およびパラメータの設定」
- 「物理インターフェイスへの暗号マップの適用」
- 「Easy VPN リモート コンフィギュレーションの作成」

これらの設定作業の結果を示す例は、「設定例」の項に示されています。

（注）この章の手順では、基本的なルータ機能と、NAT、DCHP、および VLAN を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、第 4 章「PPP over ATM と NAT の設定」および第 5 章「DHCP および VLAN による LAN の設定」を参照してください。

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp policy** *priority*
	
	例：
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		IKE ネゴシエーション時に使用される IKE ポリシーを作成します。プライオリティ番号の範囲は 1 ～ 10000 で、プライオリティが最も高いのは 1 です。
		また、Internet Security Association Key and Management Protocol（ISAKMP; インターネット セキュリティ アソシエーション キー および管理）ポリシー コンフィギュレーション モードを開始します。

ステップ 2	**encryption {des | 3des | aes | aes 192 | aes 256}**
	
	例：
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		IKE ポリシーに使用される暗号化アルゴリズムを指定します。
		この例では、168 ビット Data Encryption Standard（DES; データ暗号化規格）を指定します。

ステップ 3	**hash {md5 | sha}**
	
	例：
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。
		この例では、Message Digest 5（MD5）アルゴリズムを指定します。デフォルトは、Secure Hash 標準（SHA-1）です。

ステップ 4	**authentication {rsa-sig | rsa-encr | pre-share}**
	
	例：
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		IKE ポリシーに使用される認証方式を指定します。
		この例では、事前共有キーを指定します。

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

	コマンドまたはアクション	目的

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

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

グループ ポリシー情報の設定

グループ ポリシーを設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	
	例：
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		リモート クライアントにダウンロードされるアトリビュートを含む IKE ポリシー グループを作成します。
		また、ISAKMP グループ ポリシー コンフィギュレーション モードを開始します。

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

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

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

	コマンドまたはアクション	目的

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

ステップ 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]
	
	例：
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		
		このコマンドの詳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。

暗号マップへのモード設定の適用

暗号マップにモード設定を適用するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto map** *map-name* **isakmp authorization list** *list-name*
	
	例：
	`Router(config)# crypto map dynmap isakmp authorization list rtr-remote`
	`Router(config)#`
		暗号マップにモード設定を適用し、Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）サーバからのグループ ポリシーのキー ルックアップ（IKE クエリ）をイネーブルにします。

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

ポリシー ルックアップのイネーブル化

AAA を使用してポリシー 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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
	
	例：
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。
		
		この例では、ローカル認証データベースを使用します。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	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
	
	例：
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに許可方式を指定します。
		
		この例では、ローカル許可データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 4	**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}
	
	例：
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		ユーザ名をベースとした認証システムを構築します。
		
		この例では、ユーザ名 *Cisco* と暗号化パスワード *Cisco* を指定しています。

IPSec トランスフォームおよびプロトコルの設定

トランスフォーム セットは、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 セットと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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	
	例：
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		トランスフォーム セット（IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ）を定義します。
		
		有効なトランスフォームおよび組み合わせの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 2	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
	
	例：
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。
		
		詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

（注）　手動で確立したセキュリティ アソシエーションの場合は、ピアとのネゴシエーションが存在しないため、両方に同じトランスフォーム セットを指定する必要があります。

IPSec 暗号方式およびパラメータの設定

ダイナミック暗号マップ ポリシーでは、ルータがすべての暗号マップ パラメータ（IP アドレスなど）を認識していない場合でも、リモート IPSec ピアからの新規の 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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

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

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

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

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

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

物理インターフェイスへの暗号マップの適用

暗号マップは、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暗号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暗号マップを適用するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 0`
	`Router(config-if)#`
		暗号マップを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

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

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

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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec client ezvpn** *name*
	
	例：
	`Router(config)# crypto ipsec client ezvpn ezvpnclient`
	`Router(config-crypto-ezvpn)#`
		Cisco Easy VPN リモート コンフィギュレーションを作成します。続いて、Cisco Easy VPN リモート コンフィギュレーション モードを開始します。

ステップ 2	**group** *group-name* **key** *group-key*
	
	例：
	`Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`
	`Router(config-crypto-ezvpn)#`
		VPN 接続の IPSec グループおよび IPSec キー値を指定します。

ステップ 3	**peer** {*ipaddress* | *hostname*}
	
	例：
	`Router(config-crypto-ezvpn)# peer 192.168.100.1`
	`Router(config-crypto-ezvpn)#`
		VPN 接続のピア IP アドレスまたはホスト名を指定します。
		（注） ホスト名を指定できるのは、ルータから DNS サーバを介してホスト名解決を行える場合だけです。

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

ステップ 5	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		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 0`
	`Router(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。
		（注） ATM WAN インターフェイスを使用しているルータの場合、このコマンドは **interface atm 0** になります。

	コマンドまたはアクション	目的

ステップ 7	**crypto ipsec client ezvpn** *name* [***outside*** | ***inside***]
	
	例：
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		Cisco Easy VPN リモート コンフィギュレーションを WAN インターフェイスに割り当てます。これにより、ルータは VPN 接続に必要な NAT または PAT、およびアクセス リストの設定を自動的に作成します。

ステップ 8	**exit**
	
	例：
	`Router(config-crypto-ezvpn)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードに戻ります。

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 0
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

設定例

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

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

```
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

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

interface fastethernet 0
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
!
interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定

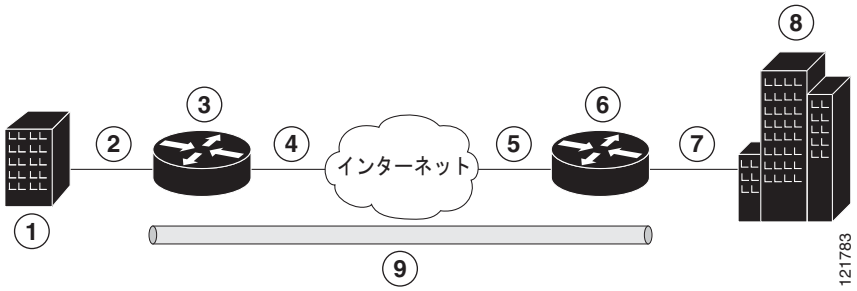
Cisco 1800 シリーズ サービス統合型固定構成ルータは Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の作成をサポートします。

Cisco ルータと他のブロードバンド デバイスは、インターネットへの高パフォーマンスな接続を提供しますが、多くのアプリケーションでは、高レベルの認証を実行し、2 つの特定のエンドポイント間でデータを暗号化する VPN 接続のセキュリティも必要です。

サイト間とリモート アクセスの 2 種類の VPN がサポートされます。サイト間 VPN は、ブランチ オフィスとコーポレート オフィスを接続する場合などに使用します。リモート アクセス VPN は、企業ネットワークにログインする際にリモート クライアントによって使用されます。

この章の例は、IPSec と Generic Routing Encapsulation（GRE; 汎用ルーティング カプセル化）プロトコルを使用して、支店オフィスと企業ネットワーク間の接続をセキュアにするサイト間 VPN の設定を示します。図 7-1 は、一般的な構成例を示します。

図 7-1　　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 1800 シリーズ サービス統合型ルータ
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

GRE トンネル

GRE トンネルは通常、Cisco ルータと、企業ネットワークなどのプライベート ネットワークへのアクセスを制御するリモート デバイス間で VPN を確立するために使用されます。GRE トンネルから転送されたトラフィックはカプセル化され、ルータの物理インターフェイスにルーティングされます。GRE インターフェイスが使用されている場合、Cisco ルータと、企業ネットワークへのアクセスを制御するルータは、トンネルを介してルーティング更新情報を交換し、IP マルチキャスト トラフィックをイネーブルにするダイナミック IP ルーティング プロトコルをサポートできます。サポートされる IP ルーティング プロトコルには、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP; ルーティング情報プロトコル）、Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、および Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）が含まれます。

（注）IP Security（IPSec; IP セキュリティ）が GRE とともに使用される場合は、トラフィックを暗号化するためのアクセス リストに、必要なエンド ネットワークとアプリケーションが示されず、代わりに送信方向の GRE トンネルの許可された送信元と送信先が示されます。追加の Access Control Llist（ACL; アクセス コントロール リスト）がトンネル インターフェイスに適用されない場合は、GRE トンネルに転送されたすべてのパケットが暗号化されます。

VPN

VPN 設定情報は、両方のエンドポイント（Cisco ルータ側とリモート ユーザ側、Cisco ルータ側と別のルータ側など）で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 Network Address Translation（NAT; ネットワーク アドレス変換）などです。

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。

- 「VPN の設定」
- 「GRE トンネルの設定」

これらの設定作業の結果を示す例は、「設定例」の項に示されています。

（注）この章の手順では、基本的なルータ機能と、NAT、DCHP、および VLAN を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、第 4 章「PPP over ATM と NAT の設定」、および第 5 章「DHCP および VLAN による LAN の設定」を参照してください。

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」
- 「グループ ポリシー情報の設定」
- 「ポリシー ルックアップのイネーブル化」
- 「IPSec トランスフォームおよびプロトコルの設定」
- 「IPSec 暗号方式およびパラメータの設定」
- 「物理インターフェイスへの暗号マップの適用」

IKE ポリシーの設定

Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp policy** *priority*
	
	例：
	`Router(config)# crypto isakmp policy 1`
	`Router(config-isakmp)#`
		IKE ネゴシエーション時に使用される 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が 1 です。
		
		また、Internet Security Association Key and Management Protocol（ISAKMP; インターネット セキュリティ アソシエーション キーおよび管理）ポリシー コンフィギュレーション モードを開始します。

ステップ 2	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	
	例：
	`Router(config-isakmp)# encryption 3des`
	`Router(config-isakmp)#`
		IKE ポリシーに使用される暗号化アルゴリズムを指定します。
		
		この例では、168 ビット Data Encryption Standard（DES; データ暗号化規格）を使用します。

ステップ 3	**hash** {**md5** | **sha**}
	
	例：
	`Router(config-isakmp)# hash md5`
	`Router(config-isakmp)#`
		IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。
		
		この例では、Message Digest 5（MD5）アルゴリズムを指定します。デフォルトは、Secure Hash 標準（SHA-1）です。

ステップ 4	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	
	例：
	`Router(config-isakmp)# authentication pre-share`
	`Router(config-isakmp)#`
		IKE ポリシーに使用される認証方式を指定します。
		
		この例では、事前共有キーを使用します。

	コマンドまたはアクション	目的

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

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

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

グループ ポリシー情報の設定

グループ ポリシーを設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto isakmp client configuration group** {**group-name** | **default**}
	
	例：
	`Router(config)# crypto isakmp client configuration group rtr-remote`
	`Router(config-isakmp-group)#`
		リモート クライアントにダウンロードされる属性を含む IKE ポリシー グループを作成します。
		
		また、Internet Security Association Key and Management Protocol（ISAKMP; インターネット セキュリティ アソシエーション キーおよび管理）ポリシー コンフィギュレーション モードを開始します。

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

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

	コマンドまたはアクション	目的

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

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

ステップ 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]]
	
	例：
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		
		このコマンドの詳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。

ポリシー ルックアップのイネーブル化

AAA を使用してポリシー 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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
	
	例：
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。
		
		この例では、ローカル認証データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的

ステップ 3	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
	
	例：
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		PPP を含むすべてのネットワーク関連サービス要求の AAA 許可と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。RADIUS サーバを使用することもできます。詳細については、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 4	**username** *name* {**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}
	
	例：
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		ユーザ名をベースとした認証システムを構築します。
		
		この例では、ユーザ名 *Cisco* と暗号化パスワード *Cisco* を指定しています。

IPSec トランスフォームおよびプロトコルの設定

トランスフォーム セットは、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 セットと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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	
	例：
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		トランスフォーム セット（IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ）を定義します。
		
		有効なトランスフォームおよび組み合わせの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 2	**crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}
	
	例：
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		IPsec セキュリティ アソシエーションのネゴシエーション時に使用されるグローバル ライフタイム値を設定します。
		
		詳細については、『*Cisco IOS Security Command Reference*』を参照してください。

（注）　手動で確立したセキュリティ アソシエーションの場合は、ピアとのネゴシエーションが存在しないため、両方に同じトランスフォーム セットを指定する必要があります。

IPSec 暗号方式およびパラメータの設定

ダイナミック暗号マップ ポリシーでは、ルータがすべての暗号マップ パラメータ（IP アドレスなど）を認識していない場合でも、リモート IPSec ピアからの新規の 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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

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

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

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

ステップ 4	**exit**
	
	例：
	`Router(config-crypto-map)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

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

物理インターフェイスへの暗号マップの適用

暗号マップは、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暗号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暗号マップを適用するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 0`
	`Router(config-if)#`
		暗号マップを適用するインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

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

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

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 モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface tunnel 1`
	`Router(config-if)#`
		トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**ip address** ***ip-address mask***
	
	例：
	`Router(config-if)# 10.62.1.193 255.255.255.252`
	`Router(config-if)#`
		トンネルにアドレスを割り当てます。

ステップ 3	**tunnel source** *interface-type number*
	
	例：
	`Router(config-if)# tunnel source fastethernet 2`
	`Router(config-if)#`
		GRE トンネルにルータの送信元エンドポイントを指定します。

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

ステップ 5	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		トンネルに暗号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。詳細については、『*Cisco IOS Security Configuration Guide*』を参照してください。

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

	コマンドまたはアクション	目的

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

ステップ 8	**permit** *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`
	`Router(config-acl)#`
		発信インターフェイスでは 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)#`
		グローバル コンフィギュレーション モードに戻ります。

設定例

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

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

tunnel source fastethernet 2

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
!
crypto isakmp policy 1 ! defines the key association and authentication for ipsec tunnel.
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac ! defines encryption and transform
set for the ipsec tunnel.
!
crypto map to_corporate 1 ipsec-isakmp ! associates all crypto values and peering address
for the ipsec tunnel.
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!!
interface vlan 1 ! VLAN 1 is the internal home network
 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
!
interface fastethernet 0! FE0 is the outside or internet exposed interface
 ip address 210.110.101.21 255.255.255.0
 ip access-group 103 in ! acl 103 permits ipsec traffic from the corp. router as well as
denies internet initiated traffic inbound.
 ip nat outside
 no cdp enable
 crypto map to_corporate ! applies the ipsec tunnel to the outside interface.
!
ip nat inside source list 102 interface Ethernet1 overload ! utilize nat overload in order
to make best use of the single address provided by the isp.
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
access-list 103 permit icmp any any ! allow icmp for debugging but should be disabled due
to security implications.
access-list 103 deny ip any any ! prevents internet initiated traffic inbound.
! acl 105 matches addresses for the ipsec tunnel to/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
```

簡易ファイアウォール

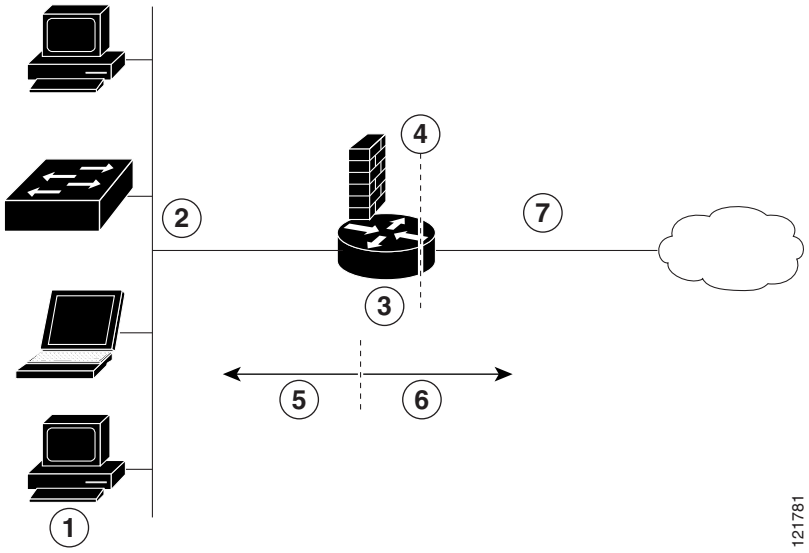
Cisco 1800 サービス統合型ルータは、アクセス リストによるネットワーク トラフィックのフィルタリングをサポートしています。また、Context-Based Access Control（CBAC; コンテキストベースのアクセス制御）によるパケット インスペクションおよび一時的なダイナミック アクセス リストについてもサポートしています。

基本的なトラフィック フィルタリングは、設定されたアクセス リストの実装に制限されます。つまり、パケットは、ネットワーク層、または最大でもトランスポート層で検証されて、ファイアウォールの通過が許可または拒否されます。ただし、CBAC でインスペクション ルールを使用することによって、一時的なダイナミック アクセス リストの作成および使用が可能になります。このダイナミック リストは、設定されたアクセス リストの一時的な開口部をファイアウォール インターフェイスで許可します。これらの開口部は、指定したユーザ セッションのトラフィックがファイアウォールを介して内部ネットワークから出るときに作成されます。開口部によって、指定したセッション（通常、ブロックされるセッション）に対するトラフィックをファイアウォールを介して戻すことが可能になります。

トラフィック フィルタリングおよびファイアウォールの詳細については『*Cisco IOS Security Configuration Guide, Release 12.3*』を参照してください。

図 8-1 は、NAT による PPPoE または PPPoA およびファイアウォールを使用したネットワーク導入を示します。

図 8-1　　ファイアウォールが設定されたルータ



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 用の内部インターフェイス）
3	PPPoE または PPPoA クライアントおよびファイアウォール実装：それぞれ Cisco 1811/1812J または Cisco 1801/1802/1803 シリーズサービス統合型ルータ
4	NAT が実行されるポイント
5	保護されたネットワーク
6	保護されていないネットワーク
7	ファスト イーサネットまたは ATM WAN インターフェイス（NAT 用の外部インターフェイス）

この後の設定例では、Cisco 1811 または Cisco 1812J 上の外部 WAN インターフェイス（FE0）にファイアウォールを適用し、ファスト イーサネット WAN インターフェイス FE1 でルータに入るすべてのトラフィックにフィルタリングとインスペクションを行って、FE2 のファスト イーサネット LAN を保護します。この例では、企業ネットワークから発信されるネットワーク トラフィック（ネットワーク アドレスは 10.1.1.0）は、安全なトラフィックと見なされ、フィルタリングされません。

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。

- 「アクセス リストの設定」
- 「インスペクション ルールの設定」
- 「インターフェイスへのアクセス リストおよびインスペクション ルールの適用」

各設定作業の結果を示す例は、「設定例」に示されています。

（注）この章の手順では、基本的なルータ機能と、NAT 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行っていない場合は、ご使用のルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、および第 4 章「PPP over ATM と NAT の設定」を参照してください。DHCP、VLAN、およびセキュアなトンネルが設定されていることもあります。

アクセス リストの設定

ファイアウォールで使用するアクセス リストを作成するには、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。

	コマンド	目的

ステップ 1	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard* [**operator** [*port*]] *destination*
	
	例：
	`Router(config)# access-list 103 permit host 200.1.1.1 eq isakmp any`
	`Router(config)#`
		インターネットから発信されたトラフィックがルータのローカル（内部）ネットワークに到達しないように、送信元および宛先ポートを比較するアクセス リストを作成します。
		
		このコマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services*』を参照してください。

ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Router(config)# access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255`
	`Router(config)#`
		設定された VPN トンネルを介してネットワーク トラフィックが企業ネットワークとローカル ネットワーク間を自由に行き来できるようにアクセス リストを作成します。

インスペクション ルールの設定

TCP および UDP のすべてのトラフィックにファイアウォール インスペクション ルールを設定し、セキュリティ ポリシーによって定義されている特定のアプリケーション プロトコルを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**ip inspect name** *inspection-name protocol*
	
	例：
	`Router(config)# ip inspect name firewall tcp`
	`Router(config)#`
		特定のプロトコルのインスペクション ルールを定義します。

ステップ 2	**ip inspect name** *inspection-name protocol*
	
	例：
	`Router(config)# ip inspect name firewall rtsp`
	`Router(config)# ip inspect name firewall h323`
	`Router(config)# ip inspect name firewall netshow`
	`Router(config)# ip inspect name firewall ftp`
	`Router(config)# ip inspect name firewall sqlnet`
	`Router(config)#`
		使用する各インスペクション ルールに対して、このコマンドを繰り返します。

インターフェイスへのアクセス リストおよびインスペクション ルールの適用

ネットワーク インターフェイスに ACL およびインスペクション ルールを適用するには、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。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface vlan 1`
	`Router(config-if)#`
		ルータの内部ネットワーク 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	**ip inspect** *inspection-name* {***in*** | ***out***}
	
	例：
	`Router(config-if)# ip inspect firewall in`
	`Router(config-if)#`
		ルータの内部インターフェイスにファイアウォール インスペクション ルールのセットを割り当てます。

	コマンド	目的

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

ステップ 4	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 0`
	`Router(config-if)#`
		ルータの外部ネットワーク 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 5	**ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
	
	例：
	`Router(config-if)# ip access-group 103 in`
	`Router(config-if)#`
		定義した ACL をルータの外部インターフェイスに割り当てます。

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

設定例

在宅勤務者は、IPSec トンネリングを使用して、企業ネットワークに安全にアクセスできます。ネットワークへのセキュリティは、ファイアウォール インスペクションによって実現されます。許可されているプロトコルは、TCP、UDP、RTSP、H.323、NetShow、FTP および SQLNet のすべてです。ホーム ネットワークにはサーバがないため、外部から発信されるトラフィックは許可されません。IPSec トンネリングは、ホーム LAN から企業ネットワークへの接続を保護します。

Java ブロッキングが必要ないため、インターネット ファイアウォール ポリシーと同様に、HTTP を指定する必要がありません。Telnet や HTTP などのシングルチャネル プロトコルに、TCP インスペクションを指定できます。UDP は、DNS に対して指定されます。

次の設定例は、これまでの項で説明してきた簡易ファイアウォール 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ます。

```
! Firewall inspection is setup for all tcp and udp traffic as well as specific application
protocols as defined by the security policy.
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
interface vlan 1! This is the internal home network
ip inspect firewall in ! inspection examines outbound traffic
```

```
    no cdp enable
!
interface fastethernet 0! FE0 is the outside or internet exposed interface.
ip access-group 103 in ! acl 103 permits ipsec traffic from the corp. router as well as
denies internet initiated traffic inbound.
    ip nat outside
    no cdp enable
!
! 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
access-list 103 permit icmp any any ! allow icmp for debugging but should be disabled due
to security implications.
access-list 103 deny ip any any ! prevents internet initiated traffic inbound.
no cdp run
!
```

ワイヤレス LAN 接続

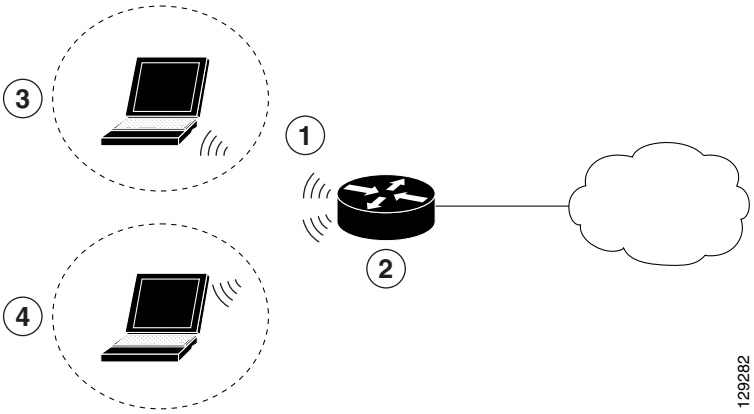
Cisco 1800 シリーズ サービス統合型固定構成ルータは、モビリティと柔軟性をネットワーク技術者が必要とするエンタープライズクラスの機能と組み合わせた、セキュアかつ安価で使いやすいワイヤレス LAN ソリューションをサポートします。Cisco IOS ソフトウェアをベースとした管理システムにより、Cisco ルータはアクセス ポイントとして機能し、Wi-Fi 認定を受けた、IEEE 802.11a/b/g 準拠のワイヤレス LAN トランシーバとなります。

これらのルータは、Command-Line Interface（CLI; コマンドライン インターフェイス）、ブラウザベースの管理システム、または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して設定およびモニタできます。この章では、CLI を使用してルータを設定する方法について説明します。**interface dot11radio** グローバル コンフィギュレーション CLI コマンドを使用して、デバイスを無線コンフィギュレーション モードにします。

ワイヤレス LAN アプリケーションでのこれらの Cisco ルータの設定に関する詳細については、『*Cisco Access Router Wireless Configuration Guide*』を参照してください。

図 9-1 に、ワイヤレス ネットワークの構成を示します。

図 9-1　　ワイヤレス LAN の例



1	ワイヤレス LAN（ネットワークで接続された複数のデバイスを使用）
2	インターネットに接続された Cisco 1800 シリーズ サービス統合型ルータ
3	VLAN 1
4	VLAN 2

以下の設定例では、リモート ユーザがワイヤレス接続を使用して Cisco 1800 シリーズ サービス統合型ルータにアクセスします。各リモート ユーザは独自の VLAN を持ちます。

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。

- 「ルート無線ステーションの設定」
- 「VLAN でのブリッジングの設定」
- 「無線ステーションのサブインターフェイスの設定」

これらの設定タスクの結果を示す例を、「設定例」の項に示します。

（注）この章の手順では、基本的なルータ機能と、NAT を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて第 1 章「ルータの基本設定」、第 3 章「PPP over Ethernet と NAT の設定」、および第 4 章「PPP over ATM と NAT の設定」を参照してください。DHCP、VLAN、およびセキュアなトンネルが設定されていることもあります。

ルート無線ステーションの設定

ワイヤレス LAN のルート無線ステーションを作成および設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンド	目的

ステップ 1	**interface** *name number*
	
	例：
	`Router(config)# interface dot11radio 0`
	`Router(config-if)#`
		指定したワイヤレス インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**broadcast-key** [[**vlan** *vlan-id*] **change** *secs*] [**membership-termination**] [**capability-change**]
	
	例：
	`Router(config-if)# broadcast-key vlan 1 change 45`
	`Router(config-if)#`
		クライアントに使用されるブロードキャスト暗号キーのローテーション間隔（秒単位）を指定します。
		
		（注） ブロードキャスト キー ローテーションをイネーブルにする場合は、スタティックな Wired Equivalent Privacy（WEP; 有線と同等のプライバシー）を使用しているクライアント デバイスはアクセス ポイントを使用できません。802.1x 認証（Light Extensible Authentication Protocol（LEAP）、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）、Protected Extensible Authentication Protocol（PEAP）など）を使用するワイヤレス クライアント デバイスのみがアクセス ポイントを使用できます。
		
		（注） このコマンドはブリッジでサポートされません。
		
		詳細については、『*Cisco IOS Commands for Access Points and Bridges*』を参照してください。

ステップ 3	**encryption** *method algorithm key*
	
	例：
	`Router(config-if)# encryption vlan 1 mode ciphers tkip`
	`Router(config-if)#`
		ワイヤレス インターフェイスにアクセスするために使用される暗号化方式、アルゴリズム、およびキーを指定します。
		
		例では、オプションのデータ暗号化方式で VLAN を使用します。

	コマンド	目的

ステップ 4	**ssid** *name*
	
	例：
	`Router(config-if)# ssid cisco`
	`Router(config-if-ssid)#`
		ワイヤレス ネットワークの公開名である Service Set ID（SSID）を作成します。
		（注）　WLAN 上のすべてのワイヤレス デバイスは、相互に通信するために同じ SSID を使用する必要があります。

ステップ 5	**vlan** *number*
	
	例：
	`Router(config-if-ssid)# vlan 1`
	`Router(config-if-ssid)#`
		SSID を VLAN にバインドします。

ステップ 6	**authentication** *type*
	
	例：
	`Router(config-if-ssid)# authentication open`
	`Router(config-if-ssid)# authentication network-eap eap_methods`
	`Router(config-if-ssid)# authentication key-management wpa`
		ワイヤレス LAN にアクセスするユーザに許可された認証方法を設定します。
		例で示されたように、複数の方法を指定できます。

ステップ 7	**exit**
	
	例：
	`Router(config-if-ssid)# exit`
	`Router(config-if)#`
		SSID コンフィギュレーション モードを終了し、ワイヤレス 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 8	**speed** *rate*
	
	例：
	`Router(config-if)# 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`
	`Router(config-if)#`
		（任意）ワイヤレス接続を介したトラフィックに対して必要かつ許可されたレート（Mbps 単位）を指定します。

ステップ 9	**rts** [**retries** | **threshold**]
	
	例：
	`Router(config-if)# rts threshold 2312`
	`Router(config-if)#`
		（任意）ワイヤレス LAN が到達可能であることを調べる前に Request to Send（RTS; 送信要求）しきい値または要求の送信回数を指定します。

ステップ 10	**power** [**client** | **local**] [**cck** [*number* | **maximum**] | **ofdm** [*number* | **maximum**]]
	
	例：
	`Router(config-if)# power local cck 50`
	`Router(config-if)# power local ofdm 30`
	`Router(config-if)#`
		（任意）無線トランスミッタの電力レベルを指定します。
		利用可能な電力レベルの値については、『*Cisco Access Router Wireless Configuration Guide*』を参照してください。

	コマンド	目的

ステップ 11	**channel** [*number* | **least-congested**]
	
	例：
	`Router(config-if)# channel 2462`
	`Router(config-if)#`
		（任意）通信が行われるチャンネルを指定します。
		利用可能なチャンネル数については、『*Cisco Access Router Wireless Configuration Guide*』を参照してください。

ステップ 12	**station-role** [**repeater** | **root**]
	
	例：
	`Router(config-if)# station-role root`
	`Router(config-if)#`
		（任意）このワイヤレス インターフェイスの役割を指定します。
		少なくとも 1 つのルート インターフェイスを指定する必要があります。

ステップ 13	**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 モードを開始します。

VLAN でのブリッジングの設定

VLAN で統合されたルーティングおよびブリッジングを設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

	コマンドまたはアクション	目的

ステップ 1	**bridge** [*number* | **crb** | **irb** |**mac-address-table**]
	
	例：
	`Router(config)# bridge irb`
	`Router(config)#`
		ブリッジングのタイプを指定します。
		この例では、統合されたルーティングおよびブリッジングを指定します。

ステップ 2	**interface** *name number*
	
	例：
	`Router(config)# interface vlan 1`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを開始します。
		VLAN でブリッジングを設定するため、この例では VLAN 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	**bridge-group** *number*
	
	例：
	`Router(config)# bridge-group 1`
	`Router(config)#`
		ブリッジ グループをインターフェイスに割り当てます。

	コマンドまたはアクション	目的

ステップ 4	**bridge-group** *parameter*
	
	例：
	`Router(config)# bridge-group spanning-disabled`
	`Router(config)#`
		ブリッジング インターフェイスに他のブリッジ パラメータを設定します。

ステップ 5	**interface** *name number*
	
	例：
	`Router(config)# interface bvi 1`
	`Router(config)#`
		仮想ブリッジ インターフェイス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 6	**ip address** *address mask*
	
	例：
	`Router(config)# ip address 10.0.1.1 255.255.255.0`
	`Router(config)#`
		仮想ブリッジ インターフェイスにアドレスを指定します。

ワイヤレス インターフェイスが必要な各 VLAN に対して上記のステップ 2 ～ステップ 6 を繰り返します。

無線ステーションのサブインターフェイスの設定

各ルート ステーションのサブ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 モードを開始し、次の手順を実行します。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface dot11radio 0.1`
	`Router(config-subif)#`
		ルート ステーションのインターフェイスに対して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 2	**description** *string*
	
	例：
	`Router(config-subif)# description Cisco open`
	`Router(config-subif)#`
		管理ユーザのためにサブインターフェイスの説明を提供します。

	コマンド	目的

ステップ 3	**encapsulation dot1q** *vlanID* [**native** | **second-dot1q**]
	
	例：
	`Router(config-subif)# encapsulation dot1q 1 native`
	`Router(config-subif)#`
		指定されたサブインターフェイスで IEEE 802.1q カプセル化をイネーブルにします。

ステップ 4	**no cdp enable**
	
	例：
	`Router(config-subif)# no cdp enable`
	`Router(config-subif)#`
		ワイヤレス インターフェイスで Cisco Discovery Protocol（CDP; シスコ検出プロトコル）をディセーブルにします。

ステップ 5	**bridge-group** *number*
	
	例：
	`Router(config-subif)# bridge-group 1`
	`Router(config-subif)#`
		ブリッジ グループをサブインターフェイスに割り当てます。

ステップ 6	**exit**
	
	例：
	`Router(config-subif)# exit`
	`Router(config)#`
		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、グローバル コンフィギュレーション モードを開始します。

必要に応じてこれらの手順を繰り返し、さらに多くのサブインターフェイスを設定します。

設定例

次の設定例は、これまでの項で説明されたワイヤレス LAN 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。

```
!
bridge irb
!
interface Dot11Radio0
 no ip address
 !
 broadcast-key vlan 1 change 45
 !
 !
 encryption vlan 1 mode ciphers tkip
 !
 ssid cisco
    vlan 1
    authentication open
    authentication network-eap eap_methods
    authentication key-management wpa
 !
 ssid ciscowep
    vlan 2
```

```
    authentication open
 !
 ssid ciscowpa
    vlan 3
    authentication open
 !
 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
 rts threshold 2312
 power local cck 50
 power local ofdm 30
 channel 2462
 station-role root
!
interface Dot11Radio0.1
 description Cisco Open
 encapsulation dot1Q 1 native
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 spanning-disabled
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 spanning-disabled
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface Vlan1
 no ip address
 bridge-group 1
 bridge-group 1 spanning-disabled
!
interface Vlan2
 no ip address
 bridge-group 2
 bridge-group 2 spanning-disabled
!
interface Vlan3
 no ip address
 bridge-group 3
 bridge-group 3 spanning-disabled
!
interface BVI1
 ip address 10.0.1.1 255.255.255.0
!
interface BVI2
 ip address 10.0.2.1 255.255.255.0
```

```
!
interface BVI3
 ip address 10.0.3.1 255.255.255.0
!
```

設定例

この章には、前の章で行ったイーサネット WAN インターフェイス、DHCP、VLAN、Easy VPN、およびワイヤレス インターフェイスの設定の結果がまとめられています。ここでは、例 10-1 を 1 つのサンプルとして、このマニュアルに記載されている基本設定を確認できます。

（注） 「**(default)**」のマークが付いているコマンドは、**show running-config** コマンドを実行すると自動的に生成されます。

例 10-1　　設定例

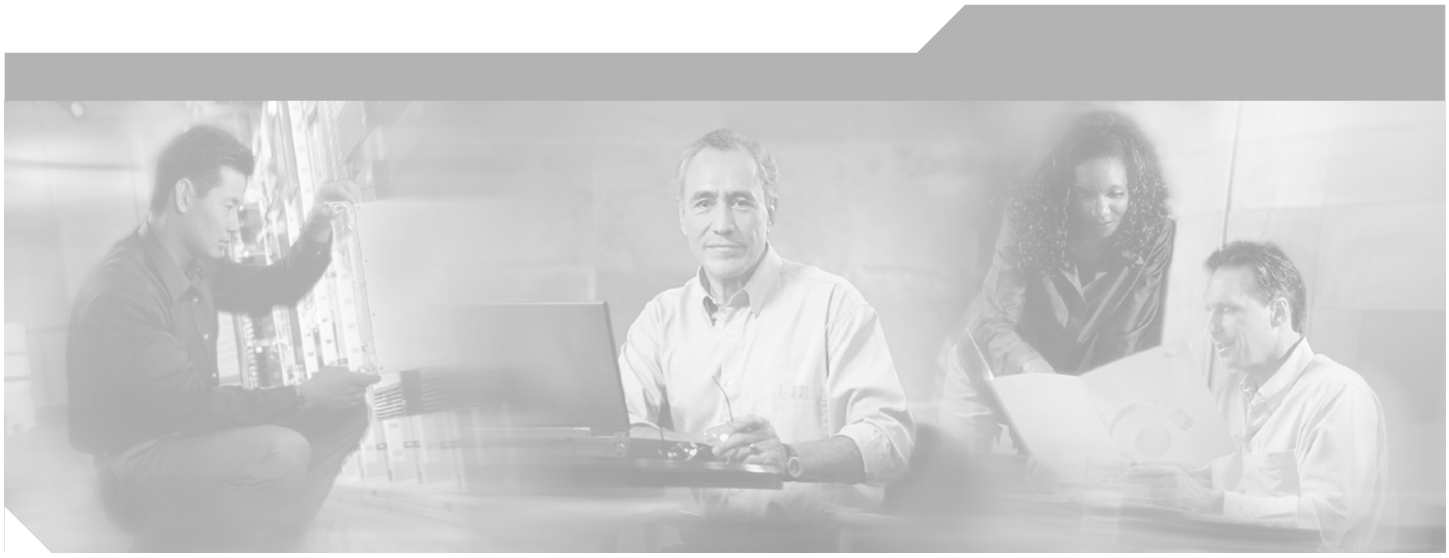
```
Router# show running-config
Building configuration...

Current configuration : 3781 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname retail
!
boot-start-marker
boot-end-marker
!
enable password cisco123
!
username jsomeone password 0 cg6#107X
aaa new-model
!
aaa group server radius rad_eap
    server 10.0.1.1 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa session-id common
ip subnet-zero
ip cef
!
vpdn enable
    vpdn-group 1
    request-dialin
    protocol pppoe
!
interface dialer 1
```

```
    ip address negotiated
    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 0.255.255.255 dialer 0
!
ip dhcp excluded-address 10.0.1.1 10.0.1.10
ip dhcp excluded-address 10.0.2.1 10.0.2.10
ip dhcp excluded-address 10.0.3.1 10.0.3.10
!
ip dhcp pool vlan1
   network 10.0.1.0 255.255.255.0
   default-router 10.0.1.1
!
ip dhcp pool vlan2
   network 10.0.2.0 255.255.255.0
   default-router 10.0.2.1
!
ip dhcp pool vlan3
   network 10.0.3.0 255.255.255.0
   default-router 10.0.3.1
!
ip ips po max-events 100
no ftp-server write-enable
!
bridge irb
!
interface FastEthernet2
    no ip address
!
interface FastEthernet3
    no ip address
!
interface FastEthernet4
    no ip address
!
interface FastEthernet5
    no ip address
!
interface FastEthernet6
    no ip address
!
interface FastEthernet7
    no ip address
!
interface FastEthernet8
    no ip address
!
interface FastEthernet9
    switchport mode trunk
    no ip address
!
interface FastEthernet0
    ip address 192.1.12.2 255.255.255.0
    no ip directed-broadcast (default)
    ip nat outside
    ip access-group 103 in
    no cdp enable
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map
```

```
    duplex auto
    speed auto
!
interface FastEthernet1
    no ip address
    duplex auto
    speed auto
!
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 Dot11Radio0
    no ip address
    !
    broadcast-key vlan 1 change 45
    !
    encryption vlan 1 mode ciphers tkip
    !
    ssid cisco
        vlan 1
        authentication open
        authentication network-eap eap_methods
        authentication key-management wpa optional
    !
    ssid ciscowep
        vlan 2
        authentication open
        !
    ssid ciscowpa
        vlan 3
        authentication open
    !
    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
    rts threshold 2312
    power local cck 50
    power local ofdm 30
    channel 2462
```

```
    station-role root
!
interface Dot11Radio0.1
    description Cisco Open
    encapsulation dot1Q 1 native
    no cdp enable
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 spanning-disabled
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
    encapsulation dot1Q 2
    bridge-group 2
    bridge-group 2 subscriber-loop-control
    bridge-group 2 spanning-disabled
    bridge-group 2 block-unknown-source
    no bridge-group 2 source-learning
    no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
    encapsulation dot1Q 3
    bridge-group 3
    bridge-group 3 subscriber-loop-control
    bridge-group 3 spanning-disabled
    bridge-group 3 block-unknown-source
    no bridge-group 3 source-learning
    no bridge-group 3 unicast-flooding
!
interface Vlan1
    ip address 192.168.1.1 255.255.255.0
    no ip directed-broadcast (default)
    crypto ipsec client ezvpn ezvpnclient inside
    ip inspect firewall in
    no cdp enable
    bridge-group 1
    bridge-group 1 spanning-disabled
!
interface Vlan2
    no ip address
    bridge-group 2
    bridge-group 2 spanning-disabled
!
interface Vlan3
    no ip address
    bridge-group 3
    bridge-group 3 spanning-disabled
!
interface BVI1
    ip address 10.0.1.1 255.255.255.0
    ip nat inside

!
interface BVI2
    ip address 10.0.2.1 255.255.255.0
!
interface BVI3
    ip address 10.0.3.1 255.255.255.0
!
ip classless
!
ip http server
```

```
no ip http secure-server
!
radius-server local
    nas 10.0.1.1 key 0 cisco123
    group rad_eap
!
user jsomeone nthash 7 0529575803696F2C492143375828267C7A760E1113734624452725707C010B065B
user AMER\jsomeone nthash 7
0224550C29232E041C6A5D3C5633305D5D560C09027966167137233026580E0B0D
!
radius-server host 10.0.1.1 auth-port 1812 acct-port 1813 key cisco123
!
control-plane
!
bridge 1 route ip
bridge 2 route ip
bridge 3 route ip
!
ip inspect name firewall tcp
ip inspect name firewall udp
ip inspect name firewall rtsp
ip inspect name firewall h323
ip inspect name firewall netshow
ip inspect name firewall ftp
ip inspect name firewall sqlnet
!
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
access-list 103 permit icmp any any
access-list 103 deny ip any any
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
!
line con 0
    password cisco123
    no modem enable
    transport preferred all
    transport output all
line aux 0
    transport preferred all
    transport output all
line vty 0 4
    password cisco123
    transport preferred all
    transport input all
    transport output all
!
```



PART 3

追加機能の設定とトラブルシューティング

追加の設定オプション

ここでは、Cisco 1800 シリーズ サービス統合型固定構成ルータ（Cisco 1801、Cisco 1802、Cisco 1803、Cisco 1811、および Cisco 1812J）に関する追加設定オプションとトラブルシューティングのヒントについて説明します。

設定オプションは次の章で説明されています。

- 第 12 章「セキュリティ機能の設定」
- 第 13 章「ダイヤル バックアップとリモート管理の設定」
- 第 14 章「トラブルシューティング」

これらの章の内容は、設定またはトラブルシューティングに関するユーザのすべてのニーズを満たすわけではありません。詳細については、適切な Cisco IOS 設定ガイドおよびコマンド リファレンスを参照してください。

（注） 特定の機能が、使用しているルータと互換性があることを確認する場合は、Software Advisor ツールを使用します。このツールにアクセスするには www.cisco.com で [Technical Support & Documentation] > [Tools & Resources] を選択し、シスコのユーザ名とパスワードを入力します。

セキュリティ機能の設定

この章では、Cisco 1800 サービス統合型固定構成ルータで設定可能な特定のセキュリティ機能を実装するシスコの主要なフレームワークである、Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）の概要について説明します。

（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。

この章で説明する内容は、次のとおりです。

- 「認証、許可、アカウンティング」
- 「AutoSecure の設定」
- 「アクセス リストの設定」
- 「CBAC ファイアウォールの設定」
- 「Cisco IOS Firewall IDS の設定」
- 「VPN の設定」

該当する場合、各項には設定例と確認手順が記載されています。

認証、許可、アカウンティング

AAA のネットワーク セキュリティ サービスは、ルータ上でアクセス制御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、Internetwork Packet Exchange（IPX; インターネットワーク パケット交換）、AppleTalk Remote Access（ARA; AppleTalk リモート アクセス）、および Telnet のサポートなど、リモート アクセスを制御するための方法を提供します。アカウンティングは、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、バイト数など、課金、監査、およびレポートに使用するセキュリティ サーバ情報を収集し、送信するための方法を提供します。

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 サービスおよびサポートされているセキュリティ プロトコルの設定については、『*Cisco IOS Security Configuration Guide*』の次の項を参照してください。

- 認証の設定
- 「Configuring Authorization」
- 「Configuring Accounting」
- 「Configuring RADIUS」
- 「Configuring TACACS+」
- 「Configuring Kerberos」

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃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』機能マニュアルを参照してください。

アクセス リストの設定

アクセス リスト（ACL）は、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上でネットワーク トラフィックの許可または拒否を行います。アクセス リストは、標準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 リストは、一般的なタグによってコマンドがバインドされる一連のコマンドです。タグは、番号または名前のどちらかです。表 12-1 は、アクセス リストの設定に使用するコマンドのリストです。

表 12-1　アクセス リストのコンフィギュレーション コマンド

ACL タイプ	コンフィギュレーション コマンド
番号形式	
標準	**access-list** {**1-99**}{**permit** | **deny**} *source-addr* [*source-mask*]
拡張	**access-list** {**100-199**}{**permit** | **deny**} *protocol source-addr* [*source-mask*] *destination-addr* [*destination-mask*]
名前形式	
標準	**ip access-list standard** *name* followed by **deny** {*source* | *source-wildcard* | **any**}
拡張	**ip access-list extended** *name* followed by {**permit** | **deny**} *protocol* {*source-addr* [*source-mask*] | **any**}{*destination-addr* [*destination-mask*] | **any**}

アクセス グループ

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 リストの定義をアクセス グループと呼びます。アクセス グループは、インターフェイスの設定時に次のコマンドを使用すると、インターフェイスに対してイネーブルになります。

ip access-group *number* | *name* [**in** | **out**]

ここで、**in** | **out** は、フィルタリングされるパケットの伝送方向を指します。

アクセス グループの作成に関する注意事項

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 リストの作成の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Access Control Lists: Overview and Guidelines」を参照してください。

CBAC ファイアウォールの設定

Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）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。これは、スタティックなアクセス リストよりも優れています。なぜならアクセス リストは、パケットのストリームではなく、個別のパケットに基づいてトラフィックの許可または拒否のみを実行するためです。また、CBAC はパケットの検査を行うため、アプリケーション レイヤのデータを調べてトラフィックの許可または拒否を判断できます。スタティックなアクセス リストでは、このような検査を行うことはできません。

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

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

指定したプロトコルがファイアウォールを通過していることがインスペクションで検出された場合、ダイナミック アクセス リストが作成され、リターン トラフィックの通過を許可します。**timeout** パラメータでは、ルータを通過する戻りトラフィックが存在しない場合にダイナミック アクセス リストをアクティブにしておく時間を指定します。タイムアウト値が指定値に達すると、ダイナミック アクセス リストが削除され、後続のパケット（有効なパケットの場合もある）が許可されなくなります。

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

サンプル設定については、第 8 章「簡易ファイアウォール」を参照してください。CBAC ファイアウォールの設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring Context-Based Access Control」を参照してください。

Cisco IOS Firewall IDS の設定

Cisco IOS Firewall Intrusion Detection System（IDS; 侵入防御システム）テクノロジーは、セキュリティ ポリシーに違反したり悪意のあるネットワーク アクティビティを表したりするパケットおよびフローを適切に処理することで、境界ファイアウォール保護を強化します。

Cisco IOS Firewall IDS は、「シグニチャ」を使用してネットワーク トラフィックから悪用のパターンを検出することで、最も一般的な 59 種類の攻撃を識別します。また、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モニタして、いずれかの IDS シグニチャとの比較を行います。疑わしいアクティビティを検出すると、ネットワーク セキュリティが損害を受ける前に対応し、イベントを記録し、設定に応じてアラームを送信するか、疑いのあるパケットをドロップするか、または TCP 接続をリセットします。

Cisco IOS Firewall IDS の設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring Cisco IOS Firewall Intrusion Detection System」を参照してください。

VPN の設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）接続を使用すると、インターネットなどのパブリック ネットワーク上で 2 つのネットワーク間のセキュアな接続を実現できます。Cisco 1800 シリーズの固定構成アクセス ルータは、IP Security（IPSec; IP セキュリティ）トンネルおよび Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用してサイト間 VPN をサポートします。2 つのピア間の永続的な VPN 接続、または、必要に応じて VPN 接続を作成および切断する EZVPN または DMVPN を使用した動的な VPN を設定できます。第 6 章「Easy VPN および IPSec トンネルを使用した VPN の設定」と第 7 章「IPSec トンネルと汎用ルーティング カプセル化を使用した VPN の設定」に、これらの機能を使用したルータの設定例を示しています。IPSec および GRE の設定の詳細については、『*Cisco IOS Release 12.3 Security Configuration Guide*』の「Configuring IPSec Network Security」を参照してください。

Cisco 1800 シリーズの固定構成アクセス ルータがサポートするその他の VPN 設定については、次の機能マニュアルを参照してください。

- 『VPN Access Control Using 802.1X Authentication』: 802.1x 認証の使用により、社員が企業ネットワークに自宅からアクセスでき、一方でリモート テレワーカー本人以外の家族はインターネットのみにアクセスできるようになります。
- 『EZVPN Server』: Cisco 1800 シリーズ固定構成ルータは、EZVPN サーバとして機能するように設定できます。これによって、許可された EZVPN クライアントは、接続しているネットワークへの動的な VPN トンネルを確立できるようになります。
- 『Dynamic Multipoint VPN (DMVPN)』: DMVPN 機能により、必要に応じてマルチポイント構成の複数のルータ間に VPN トンネルを作成でき、設定が簡素化され、永続的なポイントツーポイント VPN トンネルの必要がなくなります。

ダイヤル バックアップとリモート管理の設定

Cisco 1800 サービス統合型固定構成ルータは、ダイヤルイン機能（リモート管理用）およびダイヤルアウト機能（ダイヤル バックアップ用）をサポートしています。Cisco 1800 サービス統合型固定構成ルータは、バックアップ用のモデム回線接続を設定することで、WAN ダウンタイムを防止できます。デフォルトでは、ダイヤル バックアップは非アクティブなので、設定によってアクティブにする必要があります。

ダイヤル バックアップ機能およびリモート管理機能は、Cisco 1812J、Cisco 1801、Cisco 1802 および Cisco 1803 ルータの場合は ISDN S/T ポート経由で設定されます。これらの機能は、Cisco 1811 ルータでは、V.92 モデム ポート経由で設定されます。

この章の内容は、次のとおりです。

- 「ダイヤル バックアップ機能をアクティブにする方法」
- 「ダイヤル バックアップ機能の制限事項」
- 「ISDN S/T ポート経由でのダイヤル バックアップおよびリモート管理の設定」
- 「V.92 モデム経由でのダイヤル バックアップおよびリモート管理の設定」

ダイヤル バックアップ機能をアクティブにする方法

次の 3 つの方法で、ダイヤル バックアップ機能をアクティブに設定できます。

- 「バックアップ インターフェイス」
- 「フローティング スタティック ルート」
- 「ダイヤラ ウォッチ」

バックアップ インターフェイス

プライマリ回線がダウンしたことをルータが認識すると、バックアップ インターフェイスがアップになります。プライマリ接続が指定の時間で回復した場合に、バックアップ インターフェイスをダウンにするように設定できます。

この設定には、Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）を使用します。DDR を設定すると、指定のトラフィックによってバックアップ コールがトリガーされます。

（注）　バックアップ インターフェイスがスタンバイ モードを解除された（アップになった）場合にも、そのバックアップ インターフェイスで指定のトラフィックを受信しないかぎり、バックアップ コールはトリガーされません。

バックアップ インターフェイスの設定

ルータにバックアップ 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 モードから始め、次の手順を実行します。

	コマンド	目的

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

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

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

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、トラフィックの代替ルートを提供します。バックアップ インターフェイスに指定のトラフィックによって DDR バックアップ コールがトリガーされないかぎり、フローティング スタティック ルートはアクティブになりません。

フローティング スタティック ルートは、回線プロトコルのステータスとは無関係です。フレーム リレー回線の場合、これは重要な問題です。Data-Link Connection Identifier（DLCI; データ リンク接続識別子）が非アクティブの場合には回線プロトコルをダウンにできないからです。フローティング スタティック ルートは、カプセル化方式にも無関係です。

（注）　スタティック ルートを設定した場合、フローティング スタティック ルートをアクティブにするには、プライマリ インターフェイスのプロトコルをダウンにする必要があります。

フローティング スタティック ルートの設定

フローティング スタティック ルートのコンポーネントは、スタティック ルートおよびダイナミック ルートの 2 つです。ルータにスタティック ルートとダイナミック ルートを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

	コマンド	目的

ステップ 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		プライマリ スタティック ルートを割り当てます。

ステップ 2	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*]
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		バックアップ インターフェイス ルートの下位のルーティング管理ディスタンス値を割り当てます。192.168.2.2 は、バックアップ インターフェイスのピア IP アドレスです。

ステップ 3	**router rip**
	
	例：
	`Router(config)# router rip`
	`Router(config)#`
		RIP ルーティングをイネーブルにします。

ステップ 4	**network** *ip-address*
	
	例：
	`Router(config)# network 22.0.0.0`
	`Router(config)#`
		プライマリ インターフェイスのネットワークを定義します。22.0.0.0 は、プライマリ インターフェイスのネットワーク値です。

ステップ 5	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*]
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		バックアップ インターフェイス ルートの下位のルーティング管理ディスタンス値を割り当てます。192.168.2.2 は、バックアップ インターフェイスのピア IP アドレスです。

（注）　ダイナミック ルーティングをアクティブに設定した場合、フローティング スタティック ルートはルーティング プロトコルのコンバージェンス時間に依存します。

ダイヤラ ウォッチ

ダイヤラ ウォッチ方式は、Extended Interior Gateway Routing Protocol（EIGRP）リンクステート ダイナミック ルーティング プロトコルだけサポートします。

ダイヤラ ウォッチの設定

ルータにダイヤラ ウォッチを設定するには、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。

	コマンド	目的

ステップ 1	**interface** ***type number***
	
	例：
	`Router(config)# interface dialer 2`
	`Router(config-if)#`
		ダイヤル バックアップ 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	**dialerwatch-group** ***group-number***
	
	例：
	`Router(config-if)# dialer watch-group 2`
	`Router(config-if)#`
		ウォッチ リストのグループ番号を指定します。

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 4	**ip route** *prefix mask* {***ip-address*** | ***interface-type interface-number*** [***ip-address***]} [***distance***]
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		プライマリ ルートを割り当てます。22.0.0.2 は、プライマリ インターフェイスのピア IP アドレスです。

	コマンド	目的

ステップ 5	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*]
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.2 150`
	`Router(config)#`
		バックアップ インターフェイス ルートの下位のルーティング管理ディスタンス値を割り当てます。192.168.2.2 は、バックアップ インターフェイスのピア IP アドレスです。

ステップ 6	**dialerwatch-list** ***group-number*** {**ip** *ip-address address-mask* | **delay route-check initial** *seconds*}
	
	例：
	`Router(config)# dialer watch-list 2 ip 22.0.0.2 255.255.255.255`
	`Router(config)#`
		ウォッチ リストに IP アドレスを割り当てます。
		
		ルータ上でプライマリ インターフェイスの接続が切断され IP アドレスが使用不能になると、バックアップ インターフェイスのダイヤルアウト機能がトリガーされます。22.0.0.2 は、プライマリ インターフェイスのピア IP アドレスです。

ダイヤル バックアップ機能の制限事項

ダイヤル バックアップ機能には、次の制限事項があります。コンソール ポートまたは補助ポートのバックアップ インターフェイス上ではブリッジングはサポートされません。

表 13-1 に、Cisco 1800 シリーズ サービス統合型固定構成ルータでのダイヤル バックアップのサポートおよび制限事項を要約します。

表 13-1　ダイヤル バックアップ機能のサポートおよび制限事項

WAN カプセル化タイプ	ダイヤル バックアップの可否	ダイヤル バックアップ方式	制限事項
Cisco 1811 または Cisco 1812			
PPPoE	Yes	ダイヤラ ウォッチ	補助ポートなどの低速インターフェイスでは、ブリッジングはサポートされません。**dialerwatch** コマンドおよび IP スタティック ルートを設定するには、ISP のピア IP アドレスが必要です。
ケーブル モデム シナリオでの通常の IP	No	ダイヤラ ウォッチ	ダイヤラ ウォッチを正常に稼動させるには、ピアの IP アドレスが必要です。DHCP によって取得するリース時間が十分に短く設定されていない（1 ～ 2 分でない）場合、ダイヤル バックアップはサポートされません。

表 13-1　ダイヤル バックアップ機能のサポートおよび制限事項（続き）

WAN カプセル化タイプ	ダイヤル バックアップの可否	ダイヤル バックアップ方式	制限事項
Cisco 1801、Cisco 1802 または Cisco 1803			
ATM 上の PPP イーサネット上の PPP	Yes	バックアップ インターフェイス フローティング スタティック ルート ダイヤラ ウォッチ	フローティング スタティック ルートおよびダイヤラ ウォッチをルータで稼動させるには、ルーティング プロトコルが必要です。ダイヤラ ウォッチ方式により、プライマリ リンクがダウンした時点でただちにバックアップ インターフェイスがアップになります。ダイヤラ タイムアウトが経過し、プライマリ インターフェイスがアップになると、バックアップ インターフェイスはただちにダウンになります。ルータがプライマリ インターフェイスをチェックするのは、ダイヤラ タイムアウトが経過したときだけです。バックアップ インターフェイスは、プライマリ インターフェイスがアップになっていても、ダイヤラ タイムアウトが経過するまでアップのままです。 ダイヤラ ウォッチ方式を使用する場合、ピアの IP アドレスが既知であれば、ルータ上でルーティング プロトコルが稼動している必要はありません。
RFC 1483（AAL5、SNAP および MUX）	Yes	バックアップ インターフェイス フローティング スタティック ルート ダイヤラ ウォッチ	WAN インターフェイス経由でブリッジングを実行している場合、補助ポートではブリッジングはサポートされません。

設定例

次に、3 つのダイヤル バックアップ方式の設定例を示します。

例 13-1　バックアップ インターフェイスによるダイヤル バックアップの設定

```
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-net3
```

```
!
interface ATM0
backup interface BRI0
no ip address
no atm ilmi-keepalive
pvc 1/40
encapsulation aal5snap
pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface. Dialer pool 1 associates
it with BRI0’s dialer pool member 1
interface Dialer0
ip address negotiated
encapsulation ppp
dialer pool 1
dialer idle-timeout 30
dialer string 384040
dialer-group 1
!
! Primary interface associated with physical ATM0’s interface, dialer pool 2 associates it
with ATM0’s dial-pool-number2
interface Dialer2
ip address negotiated
ip mtu 1492
encapsulation ppp
dialer pool 2
dialer-group 2
no cdp enable
!
ip classless
!Primary and backup interface given route metric
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
```

例 13-2　　フローティング スタティック ルートによるダイヤル バックアップの設定

```
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-net3
```

```
!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 1/40
encapsulation aal5snap
pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface. Dialer pool 1 associates
it with BRI0's dialer pool member 1
interface Dialer0
ip address negotiated
encapsulation ppp
dialer pool 1
dialer idle-timeout 30
dialer string 384040
dialer-group 1
!
! Primary interface associated with physical ATM0's interface, dialer pool 2 associates it
with ATM0's dial-pool-number2
interface Dialer2
ip address negotiated
ip mtu 1492
encapsulation ppp
dialer pool 2
dialer-group 2
!
ip classless
no cdp enable
!Primary and backup interface given route metric (This example using static routes, thus
atm0 line protocol must be brought down for backup interface to function.)
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 150
ip http server
!
!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
```

例 13-3　　ダイヤラ ウォッチによるダイヤル バックアップの設定

```
!
vpdn enable
!
vpdn-group 1
accept-dialin
protocol pppoe
!
!Specifies the ISDN switch type
isdn switch-type basic-net3
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
hold-queue 100 out
!
!ISDN interface to be used as a backup interface
interface BRI0
no ip address
encapsulation ppp
dialer pool-member 1
isdn switch-type basic-net3
```

```
!
interface ATM0
no ip address
no atm ilmi-keepalive
pvc 1/40
encapsulation aal5snap
pppoe-client dial-pool-number 2
!
dsl operating-mode auto
!
! Dial backup interface, associated with physical BRI0 interface. Dialer pool 1 associates
it with BRI0's dialer pool member 1. Note "dialer watch-group 1" associates a watch list
with corresponding "dialer watch-list" command
interface Dialer0
ip address negotiated
encapsulation ppp
dialer pool 1
dialer idle-timeout 30
dialer string 384040
dialer watch-group 1
dialer-group 1
!
! Primary interface associated with physical ATM0 interface, dialer pool 2 associates it
with ATM0's dial-pool-number2
interface Dialer2
ip address negotiated
ip mtu 1492
encapsulation ppp
dialer pool 2
dialer-group 2
no cdp enable
!
ip classless

!Primary and backup interface given route metric
ip route 0.0.0.0 0.0.0.0 22.0.0.2
ip route 0.0.0.0 0.0.0.0 192.168.2.2 80
ip http server
!
!Watch for interesting traffic
dialer watch-list 1 ip 22.0.0.2 255.255.255.255

!Specifies interesting traffic to trigger backup ISDN traffic
dialer-list 1 protocol ip permit
!
```

ISDN S/T ポート経由でのダイヤル バックアップおよびリモート管理の設定

Cisco 1812J、Cisco 1801、Cisco 1802 および Cisco 1803 ルータでは、ISDN S/T ポートをダイヤル バックアップおよびリモート管理に使用します。ここでは、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手順を説明します。

- 「ISDN の設定」
- 「アグリゲータおよび ISDN ピア ルータの設定」

ISDN の設定

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

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、次の手順を実行します。

	コマンド	目的

ステップ 1	**isdn switch-type** ***switch-type***
	
	例：
	`Router(config)# isdn switch-type basic-net3`
	`Router(config)#`
		ISDN スイッチ タイプを指定します。
		この例では、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 タイプについての詳細は、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

ステップ 2	**interface** ***type number***
	
	例：
	`Router(config)# interface bri 0`
	`Router(config-if)#`
		ISDN 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`
	`Router(config-if)#`
		BRI0 インターフェイスのカプセル化タイプを設定します。

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

ステップ 5	**isdn switch-type** ***switch-type***
	
	例：
	`Router(config-if)# isdn switch-type basic-net3`
	`Router(config-if)#`
		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`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンド	目的

ステップ 7	**interface dialer** *dialer-rotary-group-number*
	
	例：
	`Router(config)# interface dialer 0`
	`Router(config-if)#`
		ダイヤラ インターフェイス（番号 0 ～ 255）を作成し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 8	**ip address negotiated**
	
	例：
	`Router(config-if)# ip address negotiated`
	`Router(config-if)#`
		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`
	`Router(config-if)#`
		インターフェイスのカプセル化タイプを PPP に設定します。

ステップ 10	**dialer pool** *number*
	
	例：
	`Router(config-if)# dialer pool 1`
	`Router(config-if)#`
		使用するダイヤラ プールを指定します。
		この例では、BRI0 の dialer pool-member 値は 1 なので、dialer pool 1 という設定により dialer 0 インターフェイスが BRI0 インターフェイスに対応付けられます。

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

ステップ 12	**dialer-group** *group-number*
	
	例：
	`Router(config-if)# dialer group 1`
	`Router(config-if)#`
		ダイヤラ 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	目的

ステップ 13	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		dialer 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 モードを開始します。

ステップ 14	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
	
	例：
	`Router(config)# dialer-list 1 protocol ip permit`
	`Router(config)#`
		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

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、この章に記載されている Cisco 876 ルータの設定例に対応する PPPoE サーバとしてアグリゲータを設定しています。

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。

```
!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
!
```

V.92 モデム経由でのダイヤル バックアップおよびリモート管理の設定

Cisco 1811 ルータの V.92 モデム経由でダイヤル バックアップおよびリモート管理を設定するには、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。

- 「非同期インターフェイスの設定」
- 「回線の設定」

非同期インターフェイスの設定

バックアップ インターフェイスとして使用する V.92 モデムを設定するには、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。

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface async 1`
	`Router(config-if)#`
		非同期シリアル 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。設定するインターフェイスの番号を入力します。

ステップ 2	**ip unnumbered** *type number*
	
	例：
	`Router(config-if)# ip unnumbered FastEthernet 2`
	`Router(config-if)#`
		非同期インターフェイスを unnumbered に設定して IP アドレスを節約し、利用するインターフェイス タイプの IP アドレスを割り当てます。

ステップ 3	**encapsulation** *encapsulation-type*
	
	例：
	`Router(config-if)# encapsulation ppp`
	`Router(config-if)#`
		インターフェイスのカプセル化タイプを PPP に設定します。

ステップ 4	**dialer in-band**
	
	例：
	`Router(config-if)# dialer in-band`
	`Router(config-if)#`
		この非同期インターフェイス上での Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）およびチャット スクリプトのサポートを指定します。

ステップ 5	**dialer string** *dial-string*
	
	例：
	`Router(config-if)# dialer string T14085551234`
	`Router(config-if)#`
		ダイヤルする電話番号を指定します。

ステップ 6	**dialer-group** *group-number*
	
	例：
	`Router(config-if)# dialer group 1`
	`Router(config-if)#`
		アクセスを制御するダイヤラ 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。ダイヤラ アクセス グループが所属する番号は、**dialer-list** コマンドで定義します。

ステップ 7	**async mode interactive**
	
	例：
	`Router(config-if)# async mode interactive`
	`Router(config-if)#`
		専用非同期ネットワーク モードの回線をインタラクティブ モードに戻し、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）および PPP EXEC コマンドを有効にします。

	コマンド	目的

ステップ 8	**peer default ip address** {*ip-address* | **pool** [*pool-name*]}
	
	例：
	`Router(config-if)# peer default ip address pool pool123`
	`Router(config-if)#`
		アドレス プールを使用してリモート クライアントに IP アドレスを割り当てます。IP アドレス プールを作成するには、**ip local pool** 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。

ステップ 9	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		非同期インターフェイスの設定を終了し、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。

回線の設定

V.92 モデムの回線を設定するには、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。

	コマンド	目的

ステップ 1	**line** *line-number*
	
	例：
	`Router(config)# line 1`
	`Router(config-line)`
		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） ここで入力する番号は、非同期シリアル インターフェイスで入力した番号と同じでなければなりません。

ステップ 2	**modem inout**
	
	例：
	`Router(config-line)# modem inout`
	`Router(config-line)#`
		着信コールと発信コールの両方に対応するように回線を設定します。

ステップ 3	**autoselect** {**arap** | **ppp** | **slip** | **during-login** | **timeout** *seconds*}
	
	例：
	`Router(config-line)# autoselect ppp`
	`Router(config-line)#`
		自動的に Appletalk Remote Access（ARA）、PPP または SLIP セッションを開始するように回線を設定します。
		（注） ダイヤル バックアップ機能には *ppp* を使用することをお勧めします。

	コマンド	目的

ステップ 4	**transport input {all | lat | mop | nasi | none | pad | rlogin | telnet | v120}**
	
	例：
	`Router(config-line)# transport input all`
	`Router(config-line)#`
		回線への接続に使用できるプロトコルを定義します。
		
		（注） ダイヤル バックアップ機能には *all* を使用することをお勧めします。

ステップ 5	**exit**
	
	例：
	`Router(config-line)# exit`
	`Router(config)#`
		ライン 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。

トラブルシューティング

この章では、問題を切り分けたり、問題の原因がそのルータにないことを判断する方法について説明します。この章で説明する内容は、次のとおりです。

- 「はじめに」
- 「代理店に連絡する前に」
- 「ADSL のトラブルシューティング」
- 「SHDSL のトラブルシューティング」
- 「PortFast のトラブルシューティング」
- 「ATM トラブルシューティング コマンド」
- 「ソフトウェア アップグレード方法」
- 「パスワードを忘れた場合の回復方法」
- 「SDM を使用したルータの管理」

はじめに

ソフトウェアに関する不具合のトラブルシューティングを行う前に、ライトブルーのコンソール ポートを使用して端末または PC をルータに接続してください（接続方法については、「関連資料」（P.xiv）にあるマニュアルを参照してください）。接続した端末または PC を使用して、ルータからのステータス メッセージの確認やコマンドの入力といったトラブルシューティング作業を行います。

また、Telnet を使用してリモートから各インターフェイス（イーサネット、ADSL、または電話）にアクセスすることもできます。Telnet オプションを使用する方法では、インターフェイスが稼動していることが前提になります。

代理店に連絡する前に

問題の原因が見つからない場合は、製品を購入した代理店に連絡し、指示を求めてください。代理店に連絡する前に、次の情報を用意してください。

- シャーシのタイプとシリアル番号
- 保守契約または保証情報
- 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

- 問題の概要
- 問題箇所を特定するために行った手順の概要

ADSL のトラブルシューティング

ADSL 接続に問題が起こった場合は、次のことを確認してください。

- ADSL 回線が接続されており、ピン 3 とピン 4 を使用している。ADSL 接続の詳細については、ご使用のルータのハードウェア ガイドを参照してください。
- ADSL CD LED がオンになっている。点灯していない場合は、ルータが DSL Access Multiplexer（DSLAM; DSL アクセス マルチプレクサ）に接続されていない可能性があります。ADSL LED の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- Asynchronous Transfer Mode（ATM; 非同期転送モード）の適切な Virtual Path Identifier（VPI; 仮想パス識別子）/Virtual Circuit Identifier（VCI; 仮想回線識別子）が使用されている。
- DSLAM は Discrete Multi-Tone（DMT; ディスクリート マルチトーン）Issue 2 をサポートしている。
- Cisco ルータに接続している ADSL ケーブルは、10 BASE-T カテゴリ 5、Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを使用する必要がある。通常の電話用のケーブルを使用すると、回線エラーが起こる場合があります。

SHDSL のトラブルシューティング

Cisco 1803 ルータ モデルでは、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 Access Multiplexer（DSLAM; DSL アクセス マルチプレクサ）に接続されていない可能性があります。G.SHDSL LED の詳細については、ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- Asynchronous Transfer Mode（ATM; 非同期転送モード）の適切な Virtual Path Identifier（VPI; 仮想パス識別子）/Virtual Circuit Identifier（VCI; 仮想回線識別子）が使用されている。
- DSLAM が G.SHDSL シグナリング プロトコルをサポートしている。

SHDSL の設定を確認するには、特権 EXEC モードで **show controllers dsl 0** コマンドを使用します。

PortFast のトラブルシューティング

PortFast は通常、ホストに接続するポートまたはインターフェイスに対してイネーブルにする機能です。このポートでリンクが確立されると、ブリッジは STA の最初の段階を省略し、直接転送モードに移行します。

他のスイッチ、ハブ、またはルータに接続するスイッチ ポートまたはインターフェイスで PortFast 機能を使用する場合は、ネットワーク ループが作成されることがあります。ループされたトラフィックが大きい場合は、ブリッジで障害が発生することがあります（ループを停止する BPDU は正常に伝送されます）。この障害によりコンバージェンスの遅延が発生することがあり、極端な場合は、ネットワークが停止します。

注意　PortFast 機能を、他のスイッチ、ハブ、またはルータに接続するスイッチ ポートまたはインターフェイスで使用しないでください。使用すると、ネットワーク ループが発生することがあります。

詳細については、『*Spanning Tree Protocol Problems and Related Design Considerations*』の「PortFast Configuration Error」の項を参照してください。

ATM トラブルシューティング コマンド

ATM インターフェイスのトラブルシューティングを行うには、次のコマンドを使用します。

- 「ping atm interface コマンド」
- 「show interface コマンド」
- 「show atm interface コマンド」
- 「debug atm コマンド」

ping atm interface コマンド

特定の PVC が使用中であるかどうかを判別するには、**ping atm interface** コマンドを使用します。このコマンドを使用する際にルータで PVC を設定する必要はありません。例 14-1 は、PVC 8/35 が使用中であるかどうかを判別するためにこのコマンドを使用する例を示しています。

例 14-1　　PVC が使用中かどうかの特定

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms


!----This command sends five OAM F5 loopback packets to the DSLAM (segment OAM packets).
If the PVC is configured at the DSLAM, the ping is successful.

!----To test whether the PVC is being used at the aggregator, enter the following command:

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

!----This command sends end-to-end OAM F5 packets, which are echoed back by the
aggregator.
```

show interface コマンド

すべての物理ポート（イーサネットおよび ATM）とルータ上の論理インターフェイスの状態を表示するには、**show interface** コマンドを使用します。例 14-2 に、コマンド出力例を示します。

例 14-2　　選択されたインターフェイスの状態の表示

```
Router# show interface 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

Router# show interface fastethernet 0
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.Oc13.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)

Router# show interface dialer 1
Dialer 1 is up, line protocol is up
    Hardware is Dialer interface
    Internet address is 1.1.1.1/24
    MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
        255/255. txload 1/255, rxload 1/255
    Encapsulation PPP, loopback not set
    Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

表 14-1 に、**show interface** コマンドの出力例を示します。

表 14-1　show interface 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。
ファスト イーサネット インターフェイスの場合	
Fast Ethernet *n* is up, line protocol is up	指定されたファスト 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。
Fast Ethernet *n* is up, line protocol is down	指定されたファスト 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 ケーブルが LAN から切断されている可能性があります。
Fast Ethernet *n* is administratively down, line protocol is down	指定されたファスト 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、コンフィギュレーション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。

show atm interface コマンド

ATM インターフェイスについての ATM 固有の情報を表示するには、特権 EXEC モードで **show atm interface atm 0** コマンドを使用します（例 14-3 を参照）。

例 14-3　ATM インターフェイスに関する情報の確認

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled:  AAL5   AAL2, Maximum VCs: 23, Current VCCs: 0

VCIs per VPI: 1024,
Max. Datagram Size: 4528
PLIM Type: ADSL - 4608Kbps Upstream, DMT, TX clocking: LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
 Avail bw = 4608
Config. is ACTIVE
```

表 14-2 は、コマンド出力で表示されるフィールドの一部です。

表 14-2　show atm interface コマンド出力の説明

フィールド	説明
ATM interface	インターフェイス番号。Cisco 1800 固定構成ルータの場合は常に 0 になります。
AAL enabled	イネーブルの AAL のタイプ。Cisco 1800 固定構成ルータは AAL5 をサポートします。
Maximum VCs	インターフェイスがサポートする仮想接続の最大数。
Current VCCs	アクティブな Virtual Channel Connection（VCC; 仮想チャネル接続）の数。
Maximum Transit Channels	伝送チャネルの最大数。
Max Datagram Size	最大データグラム内で設定されたバイトの最大数。
PLIM Type	Physical Layer Interface Module（PLIM; 物理レイヤ インターフェイス モジュール）タイプ。

debug atm コマンド

ネットワークのコンフィギュレーションに関する問題のトラブルシューティングを行うには、**debug** コマンドを使用します。**debug** コマンドでは、問題の解決に役立つさまざまな情報が表示されます。

debug コマンドを使用する場合の注意事項

正しい結果を得るために、debug コマンドを使用する前に次の注意事項をよく確認してください。

- debug コマンドはすべて特権 EXEC モードで実行します。
- デバッグ メッセージをコンソールに表示するには、**logging console debug** コマンドを入力します。
- ほとんどの **debug** コマンドは引数を使用しません。
- デバッグ機能をディセーブにするには、**undebug all** コマンドを使用します。
- ルータで Telnet セッション中に **debug** コマンドを使用する場合は、**terminal monitor** コマンドを使用します。

注意　デバッグにはルータ CPU プロセスの中で高いプライオリティを与えられているため、デバッグを実行するとルータが使用不能になる場合があります。そのため、特定の問題のトラブルシューティングを行う場合にだけ **debug** コマンドを使用してください。ネットワーク上の他のアクティビティが影響を受けないよう、ネットワーク トラフィックが少ないときに debug コマンドを使用することを推奨します。

debug コマンドに関する追加情報とドキュメントについては、『*Cisco IOS Debug Command Reference*』を参照してください。

debug atm errors コマンド

ATM エラーを表示するには、**debug atm errors** コマンドを使用します。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。例 14-4 に出力例を示します。

例 14-4　ATM エラーの確認

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

debug atm events コマンド

ATM インターフェイス プロセッサで発生したイベントを表示して、ATM ネットワークの問題点を診断するには、**debug atm events** コマンドを使用します。このコマンドは、ネットワークの安定性についての全体像を表示します。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

インターフェイスが電話会社の Digital Subscriber Line Access Multiplexer（DSLAM）とうまく通信できた場合、モデム状態は 0x10 です。インターフェイスが DSLAM と通信していない場合、モデム状態は 0x8 です。例 14-5 に、稼動中で正常に通信している ADSL 回線を示します。例 14-6 に、正常に通信していない ADSL 回線を示します。モデムの状態が 0x10 になっていないことに注意してください。

例 14-5　ATM インターフェイス プロセッサ イベントの表示：正常

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
```

```
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
00:03:09: DSL: Read firmware revision 0x1A04
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

例 14-6　ATM インターフェイス プロセッサ イベントの表示：不良

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

debug atm packet コマンド

debug atm packet コマンドは、着信および送信パケットのすべてのプロセス レベル ATM パケットを表示する場合に使用します。パケットが受信された場合、または送信が試行された場合、出力報告情報はオンラインです。デバッギング出力をディセーブルにするには、このコマンドの **no** 形式を使用します。

注意　**debug atm packet** コマンドは、処理するすべてのパケットについて、かなりの量の出力を生成します。他のシステム アクティビティが影響を受けないよう、ネットワーク トラフィックが少ない場合にだけ使用してください。

コマンド構文は次のとおりです。

debug atm packet [**interface atm** *number* [**vcd** *vcd-number*] [**vc** *vpi/vci number*]]

no debug atm packet [**interface atm** *number* [**vcd** *vcd-number*] [**vc** *vpi/vci number*]]

これらのキーワードの定義は、次のとおりです。

interface atm *number*	（任意）ATM インターフェイスまたはサブインターフェイス番号
vcd *vcd-number*	（任意）Virtual Circuit Designator（VCD; 仮想回線識別子）の番号
vc *vpi/vci number*	ATM PVC の VPI/VCI の値

例 14-7 に出力例を示します。

例 14-7　ATM パケット処理の確認

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD 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:
```

表 14-3 に、**debug atm packet** コマンド出力で表示されるフィールドの一部を示します。

表 14-3　debug atm packet コマンド出力の説明

フィールド	説明
ATM0	パケットを生成しているインターフェイス。
(O)	出力パケット。(I) は、受信パケットを意味します。
VCD: 0x*n*	このパケットに対応付けられる仮想回線。*n* は値です。
VPI: 0x*n*	このパケットの仮想パス識別子。*n* は値です。
DM: 0x*n*	記述子モード ビット。*n* は値です。
Length: *n*	ATM ヘッダーを含むパケットの全長（バイト単位）。

ソフトウェア アップグレード方法

Cisco 1800 シリーズ サービス統合型固定構成ルータでソフトウェアをアップグレードするには、次の方法を含む複数の方法が存在します。

- 既存の Cisco IOS ソフトウェア イメージの実行中に、LAN または WAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ブート イメージ（ROM モニタ）の実行中に、LAN 経由で新しいソフトウェア イメージをフラッシュ メモリにコピーします。
- ROM モニタ モードで新しいソフトウェア イメージをコンソール ポート経由でコピーします。
- ROM モニタ モードで、TFTP サーバにロードされたソフトウェア イメージからルータを起動します。この方法を使用するには、TFTP サーバがルータと同じ LAN 上にある必要があります。

パスワードを忘れた場合の回復方法

イネーブル パスワードまたはイネーブル シークレット パスワードを回復するには、次の作業を行います。

1. 「コンフィギュレーション レジスタの変更」
2. 「ルータのリセット」

3. 「パスワードのリセットと変更の保存」（イネーブル シークレット パスワードを忘れた場合だけ）
4. 「コンフィギュレーション レジスタ値のリセット」

（注）パスワードを回復できるのは、コンソール ポートを使用してルータに接続している場合だけです。Telnet セッション経由では実行できません。

ヒント　イネーブル シークレット パスワードの変更方法のさらに詳しい情報については、Cisco.com の「Hot Tips」を参照してください。

コンフィギュレーション レジスタの変更

コンフィギュレーション レジスタを変更する手順は、次のとおりです。

ステップ 1　ルータの背面パネルにある CONSOLE ポートに、ASCII 端末または端末エミュレーション プログラムが稼動している PC を接続します。

ステップ 2　端末を 9600 ボー、8 データ ビット、パリティなし、1 ストップ ビットに設定します。

ステップ 3　特権 EXEC プロンプト（*router_name* #）に、**show version** コマンドを入力すると、現在のコンフィギュレーション レジスタ値が表示されます（次の出力例の末尾の太字部分を参照）。

```
Router# show version
Cisco IOS Software, C180X Software (C180X-ADVENTERPRISEK9-M), Version 12.4(1.8)PI2c
ENGINEERING WEEKLY BUILD, synced to haw_t BASE_LABEL_OF_V124_2_T_THROTTLE
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 27-May-05 16:14 by ccai

ROM: System Bootstrap, Version 12.3(8r)YH4, RELEASE SOFTWARE (fc1)

ng-esw1-uut1 uptime is 1 hour, 21 minutes
System returned to ROM by power-on
System image file is "flash:bootimage.ng-esw1-uut1"


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
third-party authority to import, export, distribute or use encryption.
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 1801 (MPC8500) processor (revision 0x200) with 118784K/12288K bytes of memory.
Processor board ID FHK091412QA, with hardware revision 0000

9 FastEthernet interfaces
1 ISDN Basic Rate interface
1 ATM interface
31360K bytes of ATA CompactFlash (Read/Write)

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　**config-register** *value* コマンドを入力して新しいコンフィギュレーション レジスタの値を設定します。たとえば、ブレークの設定（コンフィギュレーション レジスタのビット 8 の値で示されます）をイネーブルにするには、特権 EXEC モードで **config-register 0x01** コマンドを入力します。

- 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。

ステップ 1　ブレークがイネーブルになっている場合は、ステップ 2 に進みます。ブレークがディセーブルになっている場合は、ルータの電源をオフ（O）にしてから 5 秒後に、再びオン（|）にします。その後 60 秒以内に、**Break** キーを押します。端末に ROM モニタ プロンプトが表示されます。ステップ 3 に進んでください。

（注）　一部の端末では、キーボードに *Break* というラベルの付いたキーがあります。使用するキーボードに Break キーがない場合は、端末に付属のマニュアルを参照して、ブレーク信号の送信方法を確認してください。

ステップ 2　**break** を押します。端末に次のプロンプトが表示されます。

```
rommon 2>
```

ステップ 3　**confreg 0x142** を入力して、コンフィギュレーション レジスタをリセットします。

```
rommon 2> confreg 0x142
```

ステップ 4　**reset** コマンドを入力して、ルータを初期化します。

```
rommon 2> reset
```

ルータの電源が一度オフになってからオンになり、コンフィギュレーション レジスタが 0x142 に設定されます。ルータはブート ROM システム イメージを使用します。その状況はシステム コンフィギュレーション ダイアログで示されます。

```
--- System Configuration Dialog ---
```

ステップ 5　次のメッセージが表示されるまで、プロンプトに **no** で応答します。

```
Press RETURN to get started!
```

ステップ 6　Return キーを押します。次のプロンプトが表示されます。

```
Router>
```

ステップ 7　**enable** コマンドを入力して、イネーブル モードを開始します。コンフィギュレーション変更は、イネーブル モードでだけ行うことができます。

```
Router> enable
```

プロンプトが特権 EXEC プロンプトに変わります。

```
Router#
```

ステップ 8　**show startup-config** コマンドを入力すると、コンフィギュレーション ファイルに保存されているイネーブル パスワードが表示されます。

```
Router# show startup-config
```

イネーブル パスワードを回復する場合は、次の「パスワードのリセットと変更の保存」の項を省略し、「コンフィギュレーション レジスタ値のリセット」の項の手順に従ってパスワード回復プロセスを完了します。

イネーブル シークレット パスワードを回復しているときには、**show startup-config** コマンド出力には表示されません。次の「パスワードのリセットと変更の保存」に記載されている手順を実行して、パスワード回復作業を完了させてください。

パスワードのリセットと変更の保存

パスワードをリセットして、変更を保存するには、次の作業を実行します。

ステップ 1　グローバル コンフィギュレーション モードを開始するには、**configure terminal** コマンドを実行します。

```
Router# configure terminal
```

ステップ 2　**enable secret** コマンドを入力して、ルータのイネーブル シークレット パスワードをリセットします。

```
Router(config)# enable secret password
```

ステップ 3　**exit** を入力して、グローバル コンフィギュレーション モードを終了します。

```
Router(config)# exit
```

ステップ 4　設定変更を保存します。

```
Router# copy running-config startup-config
```

コンフィギュレーション レジスタ値のリセット

パスワードの回復または再設定を行った後にコンフィギュレーション レジスタをリセットするには、次の作業を行います。

ステップ 1　グローバル コンフィギュレーション モードを開始するには、**configure terminal** コマンドを実行します。

```
Router# configure terminal
```

ステップ 2　**configure register** コマンドと、記録しておいた元のコンフィギュレーション レジスタ値を入力します。

```
Router(config)# config-reg value
```

ステップ 3　**exit** を入力して、コンフィギュレーション モードを終了します。

```
Router(config)# exit
```

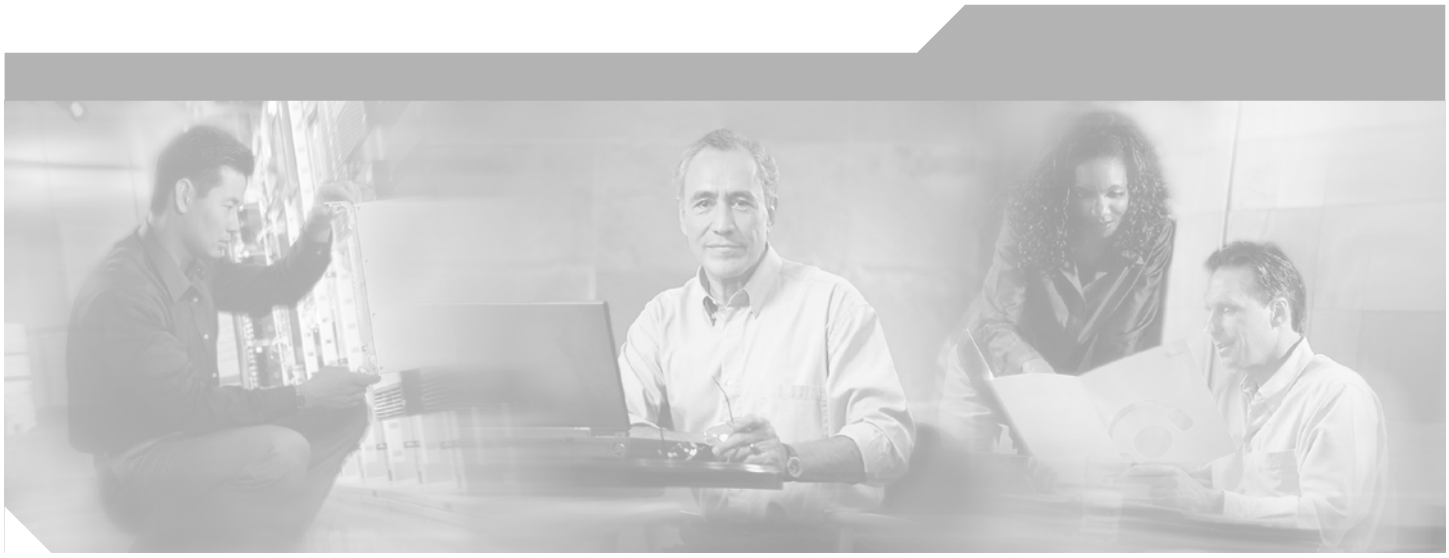
（注）　忘れたイネーブル パスワードを回復する前に使用していたコンフィギュレーションに戻るには、コンフィギュレーションの変更を保存せずに、ルータを再起動してください。

ステップ 4　ルータを再起動し、回復したパスワードを入力します。

SDM を使用したルータの管理

Cisco SDM ツールは無料のソフトウェア コンフィギュレーション ユーティリティであり、Cisco 1800 シリーズ サービス統合型固定構成ルータをサポートします。Cisco SDM は Web ベースの GUI を備えており、次の機能を利用することができます。

- 簡単なセットアップ
- 高度な設定
- ルータ セキュリティ
- ルータ モニタ



PART 4

参考資料

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。復習が必要な場合は、少し時間を取ってこの付録をお読みください。

この付録の内容は、次のとおりです。

- 「PC からのルータの設定」
- 「コマンド モードの概要」
- 「ヘルプの利用方法」
- 「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」
- 「グローバル コンフィギュレーション モードの開始」
- 「コマンドの使用方法」
- 「変更した設定の保存」
- 「まとめ」
- 「関連情報」

すでに Cisco IOS ソフトウェアを理解している場合は、次の章に進んでください。

- 第 1 章「ルータの基本設定」
- 第 2 章「ネットワークの導入例」
- このマニュアルの設定に関する章のいずれか

PC からのルータの設定

コンソール ポート経由で接続された PC からルータを設定するには、*端末エミュレーション* ソフトウェアを使用します。PC はこのソフトウェアを使用して、ルータにコマンドを送信します。表 A-1 に、使用している PC のタイプに基づいて、一般に使用されるこのソフトウェアのタイプを示します。

表 A-1　　端末エミュレーション ソフトウェア

PC オペレーティング システム	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（別途提供されます）

PC に接続しているデバイスのタイプ（この場合はルータ）の設定を変更するには、端末エミュレーション ソフトウェアを使用します。PC がルータと対話できるようにするため、ソフトウェアを次の標準 VT-100 エミュレーション設定に合わせて設定してください。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット
- フロー制御なし

この設定は、ご使用のルータのデフォルト設定に一致する必要があります。ルータのボー、データ ビット、パリティ、またはストップ ビットの設定を変更するには、ROM モニタのパラメータを再設定する必要があります。詳細については、付録 C「ROM モニタ」を参照してください。ルータ フロー制御設定を変更するには、**flowcontrol** ライン コンフィギュレーション コマンドを使用します。

ルータを設定するためにグローバル コンフィギュレーション モードを開始する手順については、この章で後述する「グローバル コンフィギュレーション モードの開始」を参照してください。

コマンド モードの概要

ここでは、Cisco IOS コマンド モードの構造について説明します。コマンド モードは、それぞれ固有の Cisco IOS コマンド群をサポートしています。たとえば、**interface** *type number* コマンドを使用できるのは、グローバル コンフィギュレーション モードだけです。

次に示す Cisco IOS コマンド モードは、階層構造になっています。ルータ セッションを開始した時点では、ユーザ EXEC モードが有効です。

- ユーザ EXEC
- 特権 EXEC
- グローバル コンフィギュレーション

表 A-2 では、このマニュアルで使用されるコマンド モード、各モードへのアクセス方法、各モードで表示されるプロンプト、およびモードを終了したり、別のモードを開始したりする方法を説明します。各モードでは、設定するルータの要素がそれぞれ異なるため、モードの切り替えを頻繁に行わなければならない場合があります。特定のモードで使用できるコマンドの一覧を表示するには、プロンプトで疑問符（?）を入力します。各コマンドの詳細（構文も含む）については、Cisco IOS 12.3 のマニュアル セットを参照してください。

表 A-2　コマンド モードの概要

モード	アクセス方法	プロンプト	終了および開始方法	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。	次の作業には、このモードを使用します。 • 端末設定の変更。 • 基本的なテストの実行。 • 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#`	• 終了してユーザ EXEC モードに戻るには、**disable** コマンドを入力します。 • グローバル コンフィギュレーション モードを開始するには、**configure** コマンドを入力します。	次の作業には、このモードを使用します。 • 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。 この章の「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」に記載されているとおり、ルータ設定の不正な変更を防止するため、このモードへのアクセスはパスワードで保護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	特権 EXEC モードから **configure** コマンドを入力します。	`Router (config)#`	• 終了して特権 EXEC モードに戻るには、**exit** コマンドまたは **end** コマンドを入力するか、**Ctrl+Z** を押します。 • インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを入力します。	このモードは、ルータ全体に適用するパラメータを設定する目的で使用します。 または、この表で後述する次のモードにアクセスすることもできます。 • インターフェイス コンフィギュレーション • ルータ コンフィギュレーション • ライン コンフィギュレーション

表 A-2　コマンド モードの概要（続き）

モード	アクセス方法	プロンプト	終了および開始方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードから（**interface atm 0** など特定のインターフェイスを指定して）**interface** コマンドを入力します。	`Router (config-if)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** キーを押します。 • サブインターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを入力し、サブインターフェイスを指定します。	このモードは、ルータのイーサネット インターフェイスおよびシリアル インターフェイスまたはサブインターフェイスのパラメータを設定する目的で使用します。
ルータ コンフィギュレーション	グローバル コンフィギュレーション モードから、**router** コマンドを入力し、続けて **router rip** などの適切なキーワードを入力します。	`Router (config-router)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** キーを押します。	このモードは、IP ルーティング プロトコルを設定する目的で使用します。
ライン コンフィギュレーション	グローバル コンフィギュレーション モードから、**line 0** などの目的のライン番号を指定して **line** コマンドを入力します。	`Router (config-line)#`	• 終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。 • 終了して特権 EXEC モードに戻るには、**end** コマンドを入力するか、または **Ctrl+Z** 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。

ヘルプの利用方法

コマンド入力の補助手段として、疑問符（?）および矢印キーを使用できます。

疑問符を入力すると、そのコマンド モードで使用できるコマンドの一覧が表示されます。

```
Router> ?
access-enable  Create a temporary access-list entry
access-profile Apply user-profile to interface
clear          Reset functions
...
```

コマンドの先頭の数文字を入力し、続けて（スペースを入れずに）疑問符を入力すると、完全なコマンドが表示されます。

```
Router> s?
* s=show set show slip systat
```

コマンドを入力し、続けてスペース 1 つと疑問符を入力すると、コマンド変数の一覧が表示されます。

```
Router> show ?
...
clock      Display the system clock
dialer     Dialer parameters and statistics
exception  exception information
...
```

以前に入力したコマンドを再表示するには、↑キーを押します。↑キーを押し続けると、さらに前に入力したコマンドにさかのぼって、順に表示されます。

イネーブル シークレット パスワードおよびイネーブル パスワード

デフォルトでは、ルータはパスワード保護なしで出荷されます。特権 EXEC コマンドの多くは動作パラメータの設定に使用されるため、これらのコマンドをパスワードで保護して、不正使用を防止する必要があります。

パスワードの設定には、次の 2 つのコマンドを使用します。

- **enable secret** *password*：非常に安全な、暗号化パスワード
- **enable** *password*：やや安全性の低い、暗号化されていないローカル パスワード

enable パスワードおよび **enable secret** パスワードは、各種権限レベル（0 ～ 15）へのアクセスを制御します。**enable** パスワードはローカルで使用することを前提としているため、暗号化されません。**enable secret** パスワードは、ネットワークで使用すること、つまり、ネットワークを超えてパスワードを使用したり、TFTP サーバにパスワードを保管したりする環境での使用を前提としています。**enable secret** パスワードまたは **enable** パスワードは、特権 EXEC モード コマンドが利用できる権限レベル 1 で使用する必要があります。

最大限のセキュリティを確保するには、これらのパスワードを別々のものにする必要があります。セットアップ時に両方のパスワードに同じ文字列を入力すると、ルータはそのパスワードを受け付けますが、異なったパスワードにするように指示する警告メッセージが表示されます。

enable secret パスワードには、1 ～ 25 文字の英数字（大文字および小文字）を指定できます。**enable** パスワードには、任意の文字数で英数字（大文字および小文字）を指定できます。どちらのパスワードでも、先頭文字に数字は使用できません。パスワードにはスペースも使用できます。たとえば、*two words* は有効なパスワードです。先行スペースは無視されますが、後続スペースは認識されます。

グローバル コンフィギュレーション モードの開始

ルータのコンフィギュレーションを変更するには、グローバル コンフィギュレーション モードを使用する必要があります。ここでは、ルータのコンソール ポートに接続された端末または PC を使用して、グローバル コンフィギュレーション モードを開始する手順について説明します。

グローバル コンフィギュレーション モードを開始する手順は、次のとおりです。

ステップ 1　ルータの起動後に、**enable** コマンドまたは **enable secret** コマンドを入力します。

```
Router> enable
```

ステップ 2　ルータにイネーブル パスワードを設定している場合は、プロンプトに対してそのパスワードを入力します。

イネーブル パスワードは、入力しても画面に表示されません。次に、特権 EXEC モードを開始する例を示します。

```
Password: enable_password
Router#
```

プロンプトに # が表示されることにより、特権 EXEC モードが開始されたことがわかります。この時点でルータ コンフィギュレーションの変更を行うことができます。

ステップ 3　グローバル コンフィギュレーション モードを開始するには、**configure terminal** コマンドを実行します。

```
Router# configure terminal
Router(config)#
```

この時点でルータ コンフィギュレーションの変更を行うことができます。

コマンドの使用方法

ここでは、Command-Line Interface（CLI: コマンドライン インターフェイス）で Cisco IOS コマンドを入力するときに役立つヒントをいくつか紹介します。

コマンドの短縮形

コマンドを入力する際、ルータが一意のコマンドとして認識できる文字数だけを入力すれば十分です。次に、**show version** コマンドを入力する例を示します。

```
Router # sh v
```

コマンドの取り消し

特定の機能を無効にするか、入力したコマンドを取り消すには、ほとんどの場合、該当するコマンドの前にキーワード **no** を入力します（例：**no ip routing**）。

コマンドライン エラー メッセージ

CLI を使用してルータを設定する際に、表示される可能性のあるエラー メッセージを表 A-3 に示します。

表 A-3　一般的な CLI エラー メッセージ

エラー メッセージ	意味	ヘルプの利用方法
`% 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。

表 A-3　一般的な CLI エラー メッセージ（続き）

エラー メッセージ	意味	ヘルプの利用方法
`% 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.`	コマンドを誤って入力しています。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（**?**）を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。

変更した設定の保存

システムのリロードや停電の発生時に変更内容が失われないように、設定の変更を Non-Volatile RAM（NVRAM; 不揮発性 RAM）に保存するには、**copy running-config startup-config** コマンドを入力する必要があります。次に、このコマンドを使用して変更を保存する例を示します。

```
router# copy running-config startup-config
Destination filename [startup-config]?
```

デフォルトの保存先ファイル名である *startup-config* をそのまま使用する場合は、Enter を押すか、または対象の保存先ファイル名を入力して Enter を押します。

コンフィギュレーションが NVRAM に保存されるまでに、1 ～ 2 分を要する場合があります。設定が保存されると、次のメッセージが表示されます。

```
Building configuration...
router#
```

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。

- コマンドの入力支援として、疑問符（**?**）と矢印キーを使用できます。
- 各コマンド モードは、一定のコマンド セットに制限されています。コマンドの入力に問題が生じたときは、プロンプトを確認したあと、疑問符（**?**）を入力して、使用できるコマンドの一覧を表示してください。間違ったコマンド モードを使用しているか、構文が不正である可能性があります。
- 機能を無効にするには、コマンドの前に **no** キーワードを入力します（例：**no ip routing**）。
- コンフィギュレーションの変更内容は NVRAM に保存して、システムの再ロード時または停電時に消失しないようにします。

関連情報

ルータを設定するには、第 1 章「ルータの基本設定」および第 2 章「ネットワークの導入例」を参照してください。

■ 関連情報

概要

この付録では、インターネット サービス プロバイダーまたはネットワーク管理者が Cisco ルータを設定する際に役立つ機能の概要について説明します。一般的なネットワーク シナリオを再検討するには、第 2 章「ネットワークの導入例」を参照してください。詳細または設定については、第 11 章「追加の設定オプション」を参照してください。

この付録に記載されている内容は、次のとおりです。

- 「ADSL」
- 「SHDSL」
- 「ネットワーク プロトコル」
- 「ルーティング プロトコルのオプション」
- 「PPP 認証プロトコル」
- 「TACACS+」
- 「ネットワーク インターフェイス」
- 「ダイヤル バックアップ」
- 「NAT」
- 「Easy IP（フェーズ 1）」
- 「Easy IP（フェーズ 2）」
- 「QoS」
- 「アクセス リスト」

ADSL

ADSL は、データと音声の両方を同一回線を介して伝送するためのテクノロジーです。ADSL のパケットベース ネットワーク テクノロジーを使用すると、Network Service Provider（NSP; ネットワーク サービス プロバイダー）のセントラル オフィスとカスタマー サイト間のローカル ループ（「ラストマイル」）、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

シリアル回線またはダイヤルアップ回線と比較した ADSL の利点は、常時接続状態になり、ダイヤルアップ回線または専用線に比べて帯域幅が増え、コストが低下することです。ADSL テクノロジーは非対称的であり、カスタマー サイトから NSP のセントラル オフィス方向での帯域幅よりも、セントラル オフィスからカスタマー サイト方向での帯域幅を大きくすることができます。この非対称性と常時

アクセス（コール セットアップが不要）を組み合わせることにより、ADSL はインターネットとイントラネットへのアクセス、ビデオ オン デマンド、およびリモート LAN アクセスに最適な手段になります。

SHDSL

SHDSL は、データと音声の両方を同一回線を介して伝送するための、G.SHDSL（G.991.2）標準に基づくテクノロジーです。SHDSL のパケットベース ネットワーク テクノロジーを使用すると、ネットワーク サービス プロバイダー（NSP）のセントラル オフィスとカスタマー サイト間で、または建物やキャンパス内で形成されるローカル ループ上で、ツイストペア銅線による高速伝送を実現できます。

G.SHDSL 装置は、セントラル オフィスおよびリモート端末からの到達距離を約 26,000 フィート（7925 m）に拡張することができます（72 kbps ～ 2.3 Mbps の対称的なデータ速度の場合）。また、より低速でリピートすることができるため、到達距離は事実上、無制限になります。

SHDSL テクノロジーは対称的であり、NSP のセントラル オフィスとカスタマー サイト間の両方向の帯域幅を同じにすることができます。この対称性と常時アクセス（コール セットアップが不要）を組み合わせることにより、SHDSL は LAN アクセスに最適な手段になります。

ネットワーク プロトコル

ネットワーク プロトコルを使用すると、送信元から特定の宛先に、LAN または WAN リンクを介してデータを渡すことができます。ネットワーク プロトコルには、ネットワークを介してデータを送信するための最適パスが格納されたルーティング アドレス テーブルが組み込まれています。

IP

インターネットワーク レイヤで最も一般的な Transmission Control Protocol/Internet Protocol（TCP; 伝送制御プロトコル /IP; インターネット プロトコル）は IP です。IP は、すべての TCP/IP ネットワークに基本的なパケット配信サービスを提供します。IP プロトコルは、物理ノード アドレスの他に、IP アドレスと呼ばれる論理ホスト アドレス システムを実装します。IP アドレスは、インターネットワーク以上のレイヤで、装置を特定したり、インターネットワーク ルーティングを実行するために使用されます。Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用すると、IP は指定の IP アドレスと一致する物理アドレスを識別できるようになります。

IP 以外のレイヤ内のすべてのプロトコルでは、データを配信するために IP を使用しています。つまり、最終宛先に関係なく、送受信される TCP/IP データはすべて IP を通過します。

IP はコネクションレス プロトコルであるため、データを伝送する前に、制御情報（*ハンドシェイク*）を交換してエンドツーエンド接続を確立することはありません。対照的に、コネクション型プロトコルはリモート コンピュータと制御情報を交換して、データ受信準備が完了したことを確認してから、データを送信します。ハンドシェイクに成功した場合は、コンピュータによって接続が確立されています。コネクション型サービスが必要な場合、IP は他のレイヤ内のプロトコルによって接続を確立します。

Internetwork Packet Exchange（IPX）は、動的なディスタンス ベクタ ルーティング プロトコルである Routing Information Protocol（RIP; ルーティング情報プロトコル）を使用して、ルーティング情報を交換します。RIP については、この後で詳細に説明します。

ルーティング プロトコルのオプション

ルーティング プロトコルには次のものがあります。

- Routing Information Protocol（RIP; ルーティング情報プロトコル）
- Enhanced Interior Gateway Routing Protocol（Enhanced IGRP; 拡張 IGRP）

RIP と拡張 IGRP には、いくつか異なる点があります（表 B-1 を参照）。

表 B-1　RIP と EIGRP の比較

Protocol	最適なトポロジ	メトリック	ルーティング アップデート
RIP	15 ホップ以内のトポロジに適しています。	ホップ カウント。最大ホップ カウントは 15 です。最良ルートは、ホップ カウントが最小のルートです。	デフォルトで 30 秒間隔。この間隔を変更することもできますし、RIP のトリガ拡張機能を使用することもできます。
EIGRP	宛先までのホップ数が 16 以上の、大規模なトポロジに適しています。	距離情報。後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準にします。	hello パケットが 5 秒間隔で送信されます。さらに、宛先のステートが変化した時点で差分更新が送信されます。

RIP

RIP は IP に関連するプロトコルで、インターネット上のルーティング プロトコル トラフィックとして幅広く使用されます。RIP は、ディスタンス ベクタ ルーティング プロトコルです。つまり、ルート選択のためのメトリックとして距離（ホップ カウント）を使用します。*ホップ カウント*は、パケットが宛先に到達するために経由しなければならないルータ数です。たとえば、あるルートのホップ カウントが 2 である場合、パケットを宛先に送るには 2 台のルータを経由しなければなりません。

デフォルトでは、RIP のルーティング アップデートは 30 秒おきにブロードキャストされます。ルーティング アップデートをブロードキャストする間隔は、ユーザ側で再設定することができます。さらに、RIP のトリガ拡張機能を使用して、ルーティング データベースが更新されたときにだけルーティング アップデートを送信するように設定することもできます。RIP のトリガ拡張機能については、Cisco IOS 12.3 のマニュアルを参照してください。

EIGRP

拡張 IGRP 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。

拡張 IGRP が稼動する各ルータは、5 秒おきに hello パケットを送信して、近接ルータに自らが動作していることを知らせます。所定時間内に hello パケットを送信しないルータがあれば、EIGRP は宛先のステートに変化があったと見なし、差分更新を送信します。

EIGRP は IP をサポートするため、マルチプロトコル ネットワーク環境で 1 つのルーティング プロトコルを使用して、ルーティング テーブルのサイズおよびルーティング情報の量を最小限に抑えることができます。

PPP 認証プロトコル

Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）は、ポイントツーポイント リンクを介して送信されるネットワーク レイヤ プロトコル情報をカプセル化します。PPP は最初、ポイントツーポイント リンク上で IP トラフィックを伝送するためのカプセル化プロトコルとして登場しました。また、IP アドレスの割り当てと管理、非同期（スタート/ストップ）カプセル化とビット型同期カプセル化、ネットワーク プロトコルの多重化、リンク コンフィギュレーション、リンク品質テスト、エラー検出、およびネットワーク レイヤ アドレス ネゴシエーションやデータ圧縮ネゴシエーションなどのオプションのネゴシエーション機能に関する標準も、PPP によって確立されました。上記機能をサポートするために、PPP には拡張可能な Link Control Protocol（LCP）および Network Control Protocol（NCP）ファミリが備わっており、これらによってオプションの設定パラメータおよびファシリティをネゴシエートします。

PPP の最新の実装では、PPP セッションを認証するためのセキュリティ認証プロトコルが 2 つサポートされています。

- Password Authentication Protocol（PAP）
- Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）

通常、PPP と PAP または CHAP 認証の組み合わせは、接続されているリモート サイトを中央サイトに通知する場合に使用されます。

PAP

PAP は双方向のハンドシェイクを使用して、ルータ間のパスワードを検証します。PAP の仕組みを示すために、リモート オフィスの Cisco ルータが本社オフィスの Cisco 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 の仕組みを示すために、リモート オフィスの Cisco ルータが本社オフィスの Cisco 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 1800 固定構成ルータは、Telnet を介して Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。TACACS+ は、リモート アクセス認証およびイベント ロギングなどの関連ネットワーク セキュリティ サービスを提供するシスコ独自の認証プロトコルです。ユーザ パスワードは、個々のルータではなく中央のデータベースで管理されます。TACACS+ は、ルータごとに設定された、別個のモジュールである Authentication, Authorization, Accounting（AAA; 認証、許可、アカウンティング）ファシリティもサポートします。

ネットワーク インターフェイス

ここでは、Cisco 1800 固定構成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。

- 「Ethernet」
- 「ATM」

Ethernet

イーサネットは、Carrier Sense Multiple Access Collision Detect（CSMA/CD; キャリア検知多重アクセス/衝突検知）を使用してデータおよび音声パケットを WAN インターフェイスに送信するベースバンド LAN プロトコルです。この用語は、通常、すべての CSMA/CD LAN を表します。イーサネットは、散発的な、場合によっては大量のトラフィックが発生するネットワーク内で機能するように設計されました。IEEE 802.3 仕様は、本来のイーサネット テクノロジーに基づいて、1980 年に開発されました。

イーサネット CSMA/CD メディアアクセス プロセスでは、CSMA/CD LAN 上のすべてのホストはいつでもネットワークにアクセスできます。データを送信する前に、CSMA/CD ホストはネットワークを通過するトラフィックを待ち受けます。データを送信するホストは、トラフィックが検出されなくなるまで待機してから、データを送信します。イーサネットでは、ネットワーク上をデータが流れていない場合、ネットワーク上のすべてのホストがデータを送信できます。トラフィックを待ち受けていた 2

台のホストがトラフィックを検出せず、同時にデータを送信すると、衝突が発生します。衝突が発生すると両方の送信内容が破壊されるため、ホストは後で再送信する必要があります。衝突したホストがいつ再送信を行うかは、アルゴリズムによって決まります。

ATM

Asynchronous Transfer Mode（ATM; 非同期転送モード）は、音声、データ、ビデオ、画像など複数のトラフィック タイプをサポートする、高速な多重化およびスイッチング プロトコルです。

ATM は、ネットワークのすべての情報をスイッチングおよび多重化する固定長セルで構成されます。ATM 接続は、単に宛先ルータまたはホストに情報を転送するために使用されます。ATM ネットワークは、帯域幅を幅広く利用できる LAN と考えられます。コネクションレス型である LAN と異なり、ATM を使用してユーザに LAN 環境を提供するには、特定の機能が必要となります。

各 ATM ノードは、ATM ネットワーク内の通信する必要があるすべてのノードに対して、接続を個別に確立する必要があります。このような接続はすべて、Permanent Virtual Circuit（PVC; 相手先固定接続）によって確立されます。

PVC

PVC はリモート ホストとルータ間の接続です。PVC は、ルータが通信する ATM エンド ノードごとに確立されます。PVC の作成時に確立される PVC の特性は、ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化タイプによって設定されます。AAL は、ユーザ情報をセルに変換する方法を定義します。AAL は、送信時に上位レイヤ情報をセルに分割し、受信時にセルを再び組み立てます。

Cisco ルータは AAL5 形式をサポートしています。AAL5 は、AAL3/4 よりもオーバーヘッドが少なく、エラー検出および訂正機能が優れている最新のデータ トランスポート サービスを提供します。AAL5 は通常、Variable Bit Rate（VBR; 可変ビット レート）トラフィックおよび Unspecified Bit Rate（UBR; 未指定ビット レート）トラフィックを対象とします。Cisco 1800 シリーズ ルータは、AAL1 および 2 形式もサポートしています。

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って、ATM PVC カプセル化のタイプが決定します。

ルータがサポートする ATM PVC カプセル化タイプは、次のとおりです。

- LLC/SNAP（RFC 1483）
- VC-MUX（RFC 1483）
- PPP（RFC 2364）

各 PVC は、宛先ノードへの完全な、独立したリンクと見なされます。ユーザは必要に応じて、接続間でデータをカプセル化できます。ATM ネットワークは、データの内容を無視します。必要となるのは、特定の AAL 形式に従って、ルータの ATM サブシステムにデータを送信することだけです。

ダイヤラ インターフェイス

ダイヤラ インターフェイスは、PVC に PPP 機能（認証方法や IP アドレス割り当て方法など）を割り当てます。PPP over ATM を設定する場合に使用します。

ダイヤラ インターフェイスは、すべての物理インターフェイスから独立して設定し、必要に応じて動的に適用することができます。

ダイヤル バックアップ

ダイヤル バックアップを使用すると、ユーザはバックアップ モデム回線接続を設定できるようになるため、WAN のダウンタイムが短縮されます。Cisco IOS ソフトウェアのダイヤル バックアップ機能を起動するために、以下を使用できます。

- 「バックアップ インターフェイス」
- 「フローティング スタティック ルート」
- 「ダイヤラ ウォッチ」

バックアップ インターフェイス

バックアップ インターフェイスは、WAN ダウンタイムなど、自らが起動する特定の環境が発生するまで、アイドル状態にとどまるインターフェイスです。バックアップ インターフェイスとして設定できるのは、Basic Rate Interface（BRI; 基本速度インターフェイス）などの物理インターフェイス、またはダイヤラ プールで使用されるように割り当てられたバックアップ ダイヤラ インターフェイスです。プライマリ回線が起動している場合、バックアップ インターフェイスはスタンバイ モードです。スタンバイ モードのバックアップ インターフェイスは、イネーブルになるまで、事実上のシャットダウン状態です。バックアップ インターフェイスに関連付けられたルートは、ルーティング テーブルに格納されません。

バックアップ インターフェイス コマンドは、インターフェイスが物理的にダウンしていることを識別したルータによって異なるため、通常は、ISDN BRI 接続、非同期回線、および専用線をバックアップするために使用されます。プライマリ回線に障害が発生すると、上記接続に対するインターフェイスがダウンして、バックアップ インターフェイスがこれらの障害をただちに識別します。

フローティング スタティック ルート

フローティング スタティック ルートは、管理距離がダイナミック ルートよりも長いスタティック ルートです。スタティック ルートに管理距離を設定すると、スタティック ルートの優先度をダイナミック ルートよりも小さくすることができます。この方法では、ダイナミック ルートが使用可能な場合、スタティック ルートは使用されません。ただし、ダイナミック ルートが失われると、スタティック ルートが引き継ぎ、この代替ルートを通してトラフィックを送信できます。この代替ルートに Dial-on-Demand Routing（DDR; ダイヤルオンデマンド ルーティング）インターフェイスが使用されている場合は、DDR インターフェイスをバックアップ インターフェイスとして使用できます。

ダイヤラ ウォッチ

ダイヤラ ウォッチは、ダイヤル バックアップとルーティング機能を統合するバックアップ機能です。ダイヤラ ウォッチを使用すると、中央ルータにおいて発信コールをトリガするトラフィックを定義しなくても、信頼できる接続を確立できます。したがって、ダイヤラ ウォッチは対象トラフィックに関する条件がない正規の DDR と見なすことができます。プライマリ インターフェイスを定義するウォッチ対象ルートを設定することにより、ウォッチ対象ルートの追加および削除にともない、プライマリ インターフェイスのステータスをモニタし追跡することができます。

ウォッチ対象ルートを削除すると、ダイヤラ ウォッチはウォッチ中のいずれかの IP アドレスまたはネットワークに対して、有効なルートが少なくとも 1 つ存在するかどうかを確認します。有効なルートが存在しない場合、プライマリ回線はダウンしており、使用不可能であると見なされます。定義済みのウォッチ対象 IP ネットワークの少なくとも 1 つに有効なルートが存在し、このルートがダイヤラ

ウォッチに設定されたバックアップ インターフェイス以外のインターフェイスを示している場合、プライマリ リンクは起動していると見なされ、ダイヤラ ウォッチはバックアップ リンクを起動しません。

NAT

Network Address Translation（NAT; ネットワーク アドレス変換）はプライベートにアドレス指定されたネットワークから、インターネットなどの登録済みネットワークにアクセスするためのメカニズムを提供します。サブネット アドレスが登録されている必要はありません。このメカニズムにより、ホスト番号の再設定は不要になり、複数のイントラネットで同じ IP アドレス範囲を使用できます。

NAT は、*内部ネットワーク*（登録されていない IP アドレスを使用するネットワーク）と*外部ネットワーク*（グローバルに一意な IP アドレスを使用するネットワーク（この場合はインターネット））の境界に配置されたルータに設定されます。NAT は内部ローカル アドレス（内部ネットワークのホストに割り当てられた登録されていない IP アドレス）をグローバルに一意な IP アドレスに変換してから、パケットを外部ネットワークに送信します。

NAT が設定されている場合、内部ネットワークは既存のプライベート アドレスまたは古い形式のアドレスを引き続き使用します。これらのアドレスが有効なアドレスに変換された後、パケットは外部ネットワークに転送されます。変換機能は標準ルーティングと互換性があります。この機能が必要となるのは、内部ネットワークと外部ドメインを接続しているルータだけです。

変換はスタティックにもダイナミックにも行えます。スタティック アドレス変換は、内部ネットワークと外部ドメインの 1 対 1 のマッピングを確立します。ダイナミック アドレス変換は、変換されるローカル アドレスと、外部アドレスの割り当て元となるアドレス プールとを指定することによって、定義されます。割り当ては番号順に行われ、連続するアドレス ブロックからなる複数のプールを定義できます。

NAT を使用すると、外部へのアクセスが必要なすべてのホストにアドレスを再指定する必要がなくなるため、時間が短縮され、コストが削減されます。また、アプリケーション ポートレベルの多重化によって、アドレスも節約されます。NAT が設定されていると、内部ホストはすべての外部通信に対して、1 つの登録済み IP アドレスを共有できます。このタイプの設定では、多数の内部ホストをサポートするために必要な外部アドレスが比較的少なくてすむため、IP アドレスが節約されます。

内部ネットワークのアドレス指定方式は、インターネット内で割り当てられた登録済みアドレスと競合することがあります。したがって、NAT は重複ネットワークごとに個別のアドレス プールを使用して、適切に変換することができます。

Easy IP（フェーズ 1）

Easy IP（フェーズ 1）機能は、ネットワーク アドレス変換と PPP/Internet Protocol Control Protocol（IPCP; インターネット プロトコル コントロール プロトコル）を組み合わせた機能です。この機能を使用すると、Cisco ルータは、独自の登録済み WAN インターフェイス IP アドレスを中央サーバから自動的にネゴシエートし、すべてのリモート ホストがこの単一の登録済みアドレスを使用してインターネットにアクセスできるようにします。Easy IP（フェーズ 1）では、Cisco IOS ソフトウェアに組み込まれた既存のポートレベル多重化 NAT 機能が使用されるため、リモート LAN 上の IP アドレスはインターネットから参照できません。

Easy IP（フェーズ 1）機能は、NAT と PPP/IPCP を組み合わせた機能です。NAT が設定されているルータは、LAN 装置で使用される登録されていない IP アドレスを、ダイヤラ インターフェイスで使用されるグローバルに一意な IP アドレスに変換します。複数の LAN 装置でグローバルに一意な同一 IP アドレスを使用する機能は、*オーバーローディング*といいます。NAT は、内部ネットワーク（登録

されていない IP アドレスを使用するネットワーク）と外部ネットワーク（グローバルに一意な IP アドレスを使用するネットワーク（この場合はインターネット））の境界に配置されたルータに設定されます。

PPP/IPCP が設定されている場合、Cisco ルータは、Internet Service Provider（ISP; インターネット サービス プロバイダー）ルータからダイヤラ インターフェイス用のグローバルに一意な（登録済み）IP アドレスを自動的にネゴシエートします。

Easy IP（フェーズ 2）

Easy IP（フェーズ 2）機能は、Dynamic Host Configuration Protocol（DHCP）サーバとリレーを組み合わせた機能です。DHCP は、IP ネットワーク上の装置（DHCP クライアント）が DHCP サーバ内の設定情報を要求できるようにするためのクライアント / サーバ プロトコルです。DHCP は必要に応じて、中央プールのネットワーク アドレスを割り当てます。DHCP は、一時的にネットワークに接続されるホストに IP アドレスを割り当てる場合や、永久的な IP アドレスが不要なホスト グループ間で、限られた IP アドレス プールを共有する場合に便利です。

DHCP を使用すると、ユーザはクライアントごとに IP アドレスを手動で設定する必要がなくなります。

DHCP では、ルータが DHCP クライアントからの UDP ブロードキャスト（IP アドレス要求を含む）を転送するように設定します。DHCP には、自動化を促進しネットワーク管理の問題を減少させるために、次の機能が備わっています。

- 各コンピュータ、プリンタ、および共有ファイル システムの手動設定が不要
- 2 つのクライアントで同じ IP アドレスが同時に使用される状況を防止
- 中央サイトからの設定が可能

QoS

ここでは、Quality of Service（QoS; サービス品質）パラメータについて説明します。具体的な内容は、次のとおりです。

- 「IP Precedence」
- 「PPP フラグメンテーションおよびインターリーブ」
- 「CBWFQ」
- 「RSVP」
- 「低遅延キューイング（LLQ）」

QoS は、ATM、イーサネットおよび IEEE 802.1 ネットワーク、これらの基本テクノロジーの一部またはすべてを使用した IP ルーテッド ネットワークなど、さまざまなテクノロジーを介して、選択されたネットワーク トラフィックに対し、より優れたサービスを提供するためのネットワーク機能です。QoS の主な目的は、専用帯域幅の確保、ジッタおよび遅延の制御（一部のリアルタイム トラフィックおよび対話型トラフィックで必要）、および損失特性の改善です。QoS テクノロジーは、キャンパス、WAN、およびサービス プロバイダー ネットワークの今後のビジネス用途に対応するための基本的な構成単位を提供します。

音声ネットワークのパフォーマンスを高めるには、VoIP が稼動しているルータだけでなく、ネットワーク全体に QoS を設定する必要があります。すべての QoS 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 Committed Access Rate（CAR; 専用アクセス レート）などの機能を使用すると、拡張アクセスリスト分類に基づいて優先順位を設定できます。これにより、アプリケーションまたはユーザ別、宛先および送信元サブネット別など、優先順位をきわめて柔軟に割り当てることができます。通常、この機能は可能な限りネットワーク（または管理ドメイン）のエッジ付近に配備されるため、これ以降のネットワーク要素は決定されたポリシーに基づいてサービスを提供できます。

オプションの信号方式を使用している場合は、ホストまたはネットワーク クライアントに IP Precedence を設定することもできます。IP Precedence を使用すると、既存ネットワーク キューイング メカニズム（Class-Based Weighted Fair Queuing（CBWFQ; クラス ベース均等化キューイング）など）を使用して、サービス クラスを確立できます。既存アプリケーションの変更の必要性や複雑なネットワーク要件はありません。

PPP フラグメンテーションおよびインターリーブ

マルチクラス マルチリンク PPP インターリーブにより、大きいパケットをマルチリンクでカプセル化し、リアルタイム音声トラフィックの遅延条件を満たす小さいパケットに分割することができます。もともと小さいリアルタイム パケットは、マルチリンクでカプセル化されず、大きいパケットのフラグメントの合間に伝送されます。インターリーブ機能はさらに、小型で遅延に敏感なパケット用に特殊な送信キューを提供するので、そのようなパケットを他のフローより先に送信できます。インターリーブ機能は、他のベスト エフォート型トラフィックに使用される低速リンク上で、遅延に敏感な音声パケットに遅延限度を設定します。

マルチリンク PPP インターリーブは、通常、CBWFQ および RSVP または IP Precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、マルチリンク PPP インターリーブおよび CBWFQ を使用します。音声パケットにプライオリティを設定する場合は、Resource Reservation Protocol（RSVP; リソース予約プロトコル）または IP Precedence を使用します。

CBWFQ

通常、CBWFQ はマルチリンク PPP インターリーブおよび RSVP または IP Precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、CBWFQ とマルチリンク PPP を組み合わせて使用します。音声パケットにプライオリティを設定する場合は、RSVP または IP Precedence を使用します。

ATM キューと Cisco IOS キューの 2 つのキューイング レベルがあります。CBWFQ は Cisco IOS キューに適用されます。PVC が作成されると、First-in First-out（FIFO; 先入れ先出し）Cisco IOS キューが自動的に作成されます。CBWFQ を使用してクラスを作成し、それらを PVC に関連付けると、クラスごとにキューが作成されます。

CBWFQ により、キューに十分な帯域幅が確保され、トラフィックは予測どおりのサービスを受けます。小容量トラフィック ストリームが優先されます。大容量トラフィック ストリームに残りの容量が分配され、同等または比例配分された帯域幅が与えられます。

RSVP

RSVP を使用すると、ルータはインターフェイス上に十分な帯域幅を確保して、信頼性および品質性能を高めることができます。RSVP により、エンド システムはネットワークに特定の QoS を要求できます。リアルタイム音声トラフィックには、ネットワークの一貫性が不可欠です。一貫した QoS が得られなかった場合、リアルタイム トラフィックにジッタ、帯域幅不足、遅延変動、または情報損失が生じる可能性があります。RSVP は、最新のキューイング メカニズムと連動します。予約がどのように実行されるかは、インターフェイス キューイング メカニズム（CBWFQ など）に依存します。

RSVP は、PPP、HDLC、および同様なシリアル回線インターフェイス上で適切に動作します。マルチアクセス LAN 上では、適切に動作しません。RSVP は、パケット フローに関するダイナミック アクセス リストと同様のものと考えることができます。

ネットワークに次の条件が存在する場合は、RSVP を設定して QoS を保証する必要があります。

- 小規模な音声ネットワークの実装
- 2 Mbps 未満のリンク
- 使用率の高いリンク
- 可能なかぎり最良の音質を必要とする場合

低遅延キューイング（LLQ）

Low Latency Queuing（LLQ; 低遅延キューイング）は、リアルタイム トラフィック用の低遅延完全優先送信キューを提供します。完全優先キューを使用すると、（他のキュー内のパケットがキューから取り出される前に）最初に遅延に敏感なデータをキューから取り出して送信することにより、遅延に敏感なデータを他のトラフィックよりも優先的に処理することができます。

アクセス リスト

基本的な標準アクセス リストおよびスタティック拡張アクセス リストを使用すると、**permit** コマンドにキーワードを指定して、セッション フィルタリングと同様の処理を行うことができます。指定されたキーワードは、ACK または RST ビットが設定されているかどうかに基づいて、TCP パケットをフィルタリングします（ACK または RST ビットが設定されているパケットはセッション内の最初のパケットではないため、このパケットは確立されたセッションに属します）。このフィルタ基準は、インターフェイスに永久的に適用されるアクセス リストの一部になります。

ROM モニタ

ROM モニタ ファームウェアは、ルータの電源投入時またはリセット時に実行され、ファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムの起動を助けます。ROM モニタを使用して、忘れてしまったパスワードの回復やコンソール ポートでのソフトウェアのダウンロードなど、特定の設定作業を実行できます。ルータに Cisco IOS ソフトウェア イメージがロードされていない場合、ROM モニタがルータを実行します。

この付録の内容は、次のとおりです。

- 「ROM モニタの設置」
- 「ROM モニタ コマンド」
- 「コマンドの説明」
- 「TFTP ダウンロードによる障害時の回復」
- 「コンフィギュレーション レジスタ」
- 「コンソール ダウンロード」
- 「デバッグ コマンド」
- 「ROM モニタの終了」

ROM モニタの設置

ROM モニタを使用するには、端末または PC をコンソール ポート経由でルータに接続している必要があります。

次に再起動するときは ROM モニタ モードで起動するようにルータを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードを開始します。イネーブル パスワードが設定されている場合、イネーブル コマンドとイネーブル パスワードを入力して特権 EXEC モードを開始する必要があります。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**config-reg 0x0**	コンフィギュレーション レジスタをリセットします。

	コマンド	目的
ステップ 4	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**reload**	新しいコンフィギュレーション レジスタ値でルータを再起動します。ルータは ROM モニタ モードのままで、Cisco IOS ソフトウェアを起動しません。 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。この付録の「コマンドの説明」の **boot** コマンドを参照してください。 再起動したルータは ROM モニタ モードになります。新しく行が増えるごとにプロンプトの数字が増加します。

ワンポイント アドバイス　ブレーク（システム割り込み）は、コンフィギュレーション レジスタでのオン / オフ設定に関係なく、ルータの再起動後、60 秒間は必ずイネーブルです。60 秒の間であれば、Break キーを押すことによって、ROM モニタ プロンプトを表示できます。

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
dir             List files in directories-dir <directory>
dis             display instruction stream
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
more            Concatenate (type) file(s)-cat <filenames ...>
repeat          repeat a monitor command
reset           system reset
set             display the monitor variables
stack           produce a stack trace
sync            write monitor environment to NVRAM
sysret          print out info from last system return
tftpdnld        tftp image download
unalias         unset an alias
unset           unset a monitor variable
xmodem          x/ymodem image download
```

コマンドの大文字と小文字は区別されます。端末上で Break キーを押すとコマンドを停止できます。PC を使用している場合、Ctrl キーと Break キーを同時に押すと、ほとんどの端末エミュレーション プログラムはコマンドを停止します。別のタイプの端末エミュレータまたは端末エミュレーション ソフトウェアを使用している場合は、製品のマニュアルに記載された Break コマンドの送信方法を参照してください。

コマンドの説明

表 C-1 に、一般的に使用される ROM モニタ コマンドを示します。

表 C-1　一般的な ROM モニタ コマンド

コマンド	説明
help または **?**	使用できるすべての ROM モニタ コマンドを表示します。

-?	次のような、コマンド構文に関する情報を表示します。
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	
	このコマンドの出力は、**xmodem** ダウンロード コマンドの出力とわずかに異なります。
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

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 *device*:	指定したデバイス（フラッシュ メモリ ファイルなど）上のファイルがリストされます。
	`rommon 4 > dir flash:`
	`Directory of flash:/`
	`2 -rwx 10283208 <date> c1800-advsecurityk9-mz`
	`9064448 bytes available (10289152 bytes used)`

boot コマンド	ROM モニタの boot コマンドを詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Guide*』を参照してください。
b	フラッシュ メモリ内の最初のイメージをブートします。
b flash: [*filename*]	フラッシュ メモリの最初のパーティションからイメージを直接ブートします。ファイル名を入力しないと、フラッシュ メモリ内の最初のイメージがブートされます。

TFTP ダウンロードによる障害時の回復

ルータに新しいソフトウェアをロードするには、通常、Cisco IOS ソフトウェアの Command-Line Interface（CLI; コマンドライン インターフェイス）から **copy tftp flash** 特権 EXEC コマンドを実行します。ただし、ルータが Cisco IOS ソフトウェアをブートできない場合は、ROM モニタ モード中に新しいソフトウェアをロードすることができます。

ここでは、リモート TFTP サーバからルータのフラッシュ メモリに Cisco IOS ソフトウェア イメージをロードする方法について説明します。**tftpdnld** コマンドを実行すると、ルータに新しいソフトウェア イメージをダウンロードする前にフラッシュ メモリ内のすべての既存データが消去されるため、このコマンドは障害回復の場合にだけ使用してください。

TFTP ダウンロードのコマンド変数

ここでは、ROM モニタ モードで設定し、TFTP ダウンロード プロセスで使用するシステム変数について説明します。必須変数とオプション変数があります。

（注）ここに記載されたコマンドは大文字と小文字の区別があり、表記どおり正確に入力する必要があります。

必須の変数

tftpdnld コマンドを使用する前に、次のコマンドを使用して、次に示す変数を設定する必要があります。

変数	コマンド
ルータの IP アドレス	**IP_ADDRESS=** ***ip_address***
ルータのサブネット マスク	**IP_SUBNET_MASK=** *ip_address*
ルータのデフォルト ゲートウェイの IP アドレス	**DEFAULT_GATEWAY=** *ip_address*
ネットワークの接続に使用するファスト イーサネット ポートのポート番号	**FE_PORT=***fe_port_number*
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

tftpdnld コマンドを使用する前に、次のコマンドを使用して、次に示す変数を設定できます。

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：進行状況を表示しません。 1：感嘆符（!!!）でファイル ダウンロードの進行状況を表示します。これがデフォルト設定です。 2：ファイル ダウンロードの処理中に詳細な進行状況を表示します。例を示します。 • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received.MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE=** *setting*
ルータが ARP および TFTP ダウンロードを試行する回数。デフォルト値は 7 です。	**TFTP_RETRY_COUNT=** *retry_times*
ダウンロード プロセスがタイムアウトするまでの時間（秒）です。デフォルト値は 2,400 秒（40 分）です。	**TFTP_TIMEOUT=** *time*
ダウンロードされたイメージに対してルータがチェックサム テストを実行するかどうか。 1：チェックサム テストを実行します。 0：チェックサム テストを実行しない	**TFTP_CHECKSUM=***setting*

TFTP ダウンロード コマンドの使用

TFTP を介してファイルをダウンロードするには、ROM モニタ モードで次の手順を実行します。

ステップ 1　適切なコマンドを使用して、上記のすべての必須変数およびオプション変数を入力します。

ステップ 2　**tftpdnld** コマンドを次のように入力します。

```
rommon 1 > tftpdnld -r
```

（注）　**-r** 変数は任意です。この変数を入力すると、新しいソフトウェアがダウンロードされ、ブートされますが、ソフトウェアはフラッシュ メモリに保存されません。次回に **reload** を入力した場合は、フラッシュ メモリ内のイメージを使用することができます。

次のような出力が表示されます。

```
IP_ADDRESS: 10.3.6.7
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 10.3.0.1
TFTP_SERVER: 223.255.254.254
TFTP_FILE: c1800-advsecurityk9-mz
Do you wish to continue? y/n:  [n]:
```

ステップ 3　継続する場合は、出力内の質問に対して **y** を入力します。

```
Do you wish to continue? y/n:  [n]:y
```

ルータが新しいファイルのダウンロードを開始します。

誤って y を入力した場合、**Ctrl+C** または **Break** を入力するとフラッシュ メモリを消去する前に転送を止めることができます。

コンフィギュレーション レジスタ

仮想コンフィギュレーション レジスタは Non-Volatile RAM（NVRAM; 不揮発性 RAM）にあり、他の Cisco ルータと同じ機能を持っています。ROM モニタからでも、オペレーティング システム ソフトウェアからでも、仮想コンフィギュレーション レジスタの表示および変更ができます。ROM モニタ内でコンフィギュレーション レジスタを変更するには、レジスタ値を 16 進形式で入力するか、ROM モニタ プロンプトを使用して各ビットを設定します。

コンフィギュレーション レジスタの手動での変更

ROM モニタから仮想コンフィギュレーション レジスタを手動で変更するには、**confreg** コマンドを入力し、続けて新しいレジスタ値を 16 進数で入力します（次の例を参照）。

```
rommon 1 > confreg 0x2101


You must reset or power cycle for new config to take effect
rommon 2 >
```

値は常に 16 進数と見なされます。新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットまたは再起動するまでは有効になりません。

コンフィギュレーション レジスタのプロンプトでの変更

引数を指定しないで **confreg** コマンドを入力すると、仮想コンフィギュレーション レジスタの内容が表示され、各ビットの意味と、設定を変更するかどうかを問い合せるプロンプトが表示されます。

いずれの場合も、新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセット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、CompactFlash 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）　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 Universal Asynchronous Receiver/Transmitter（UART; 汎用非同期送受信器）が使用されていることを確認します。PC のシリアル ポートに 16550 UART が使用されていない場合は、コンソール ポートを介して Cisco IOS イメージをダウンロードするときに、38,400 bps 以下の速度を使用することを推奨します。

コマンドの説明

xmodem コンソール ダウンロード コマンドの構文および説明を、次に示します。

xmodem [-cyrx] *destination_file_name*

c	(任意)。パケット検証に CRC-16 エラー チェックを使用して、ダウンロードを実行します。デフォルトは 8 ビットの CRC です。
y	(任意)。Ymodem プロトコルを使用してダウンロードを実行するようにルータを設定します。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	(任意)。イメージは DRAM にロードされ、実行されます。デフォルトでは、フラッシュ メモリにイメージをロードします。
x	(任意)。イメージは DRAM にロードされますが、実行されません。
destination_file_name	システム イメージ ファイルまたはシステム コンフィギュレーション ファイルの名前です。ルータに認識させるために、コンフィギュレーション ファイル名は *router_confg* にする必要があります。

次の手順に従って、Xmodem を実行します。

ステップ 1　Xmodem を実行するローカル ドライブに、イメージ ファイルを移動します。

ステップ 2　**xmodem** コマンドを入力します。

エラー レポート

ROM モニタのコンソール ダウンロードは、コンソールを使用してデータ転送を行うため、データ転送中にエラーが発生した場合、エラー メッセージがコンソール上に表示されるのはデータ転送が終了してからです。

デフォルトのボー レートを変更した場合は、端末のボー レートをコンフィギュレーション レジスタに指定されたボー レートに戻すことを指示するメッセージがエラー メッセージに続いて表示されます。

デバッグ コマンド

ROM モニタのほとんどのデバッグ コマンドは、Cisco IOS ソフトウェアがクラッシュまたは停止した場合にだけ機能します。デバッグ コマンドの入力時に Cisco IOS クラッシュ情報が得られない場合は、次のエラーメッセージが表示されます。

```
"xxx: kernel context state is invalid, can not proceed."
```

次に、ROM モニタのデバッグ コマンドを示します。

- **stack** または **k**：スタック トレースが生成されます。次に例を示します。

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**：プロセッサのコンテキストが表示されます。次に例を示します。

```
> context
xt of the most recent exception
000000 R1 = 0x832552c4 R2 = 0xffffffffR3 = 0x00000000
000021 R5 = 0x839960a8 R6 = 0x00029220R7 = 0xffffffff
9c0000 R9 = 0xffffffff R22 = 0xffffffff R23 = 0xffffffff
000e881 R13 = 0xffffffff R14 = 0xffffffff R15 = 0xffffffff
fffffff R25 = 0xffffffff R30 = 0xffffffff IVPR = 0xffffffff
fffffff R25 = 0xffffffff R26 = 0xffffffff R27 = 0xffffffff
fffffff R29 = 0xffffffff R30 = 0xffffffff R31 = 0xffffffff
888002 LR = 0x800e3638 CTR = 0x8003af88 XER = 0xffffffff
fffffff TBL = 0xffffffff DEAR = 0xffffffff DBCR2 = Oxffffffff
fffffff DBCR0 = 0xffffffff DBCR1 = 0xffffffff DBCR2 = 0xffffffff
ffffffff IAC2 = 0xffffffff DAC1 = 0xffffffff MCSRR1 = 0xffffffff
03af88 MSR = 0x00029220
```

- **frame**：個々のスタック フレームが表示されます。
- **sysret**：最後に起動したシステム イメージからの戻り情報が表示されます。この情報には、イメージを中止した理由、最大 8 フレームのスタック ダンプ、および例外が発生したアドレス（例外がある場合）などが含まれます。

```
rommon 8> sysret
System Return Info:
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**：メイン メモリのサイズ（バイト）、開始アドレス、および使用可能範囲、パケット メモリの開始ポイントとサイズ、NVRAM のサイズが表示されます。次に例を示します

```
rommon 9> meminfo
Main memory size: 256 MB.
Available main memory starts at 0x80012000, size 0x3ffb8 KB IO (packet) memory size:
10 percent of main memory.
NVRAM size: 192 KB
```

ROM モニタの終了

ルータの起動時または再ロード時に Cisco IOS イメージをフラッシュ メモリから起動させるには、コンフィギュレーション レジスタ値を 0x2 ～ 0xF に設定する必要があります。

次に、コンフィギュレーション レジスタをリセットして、ルータがフラッシュ メモリに格納された Cisco IOS イメージを起動するように設定する例を示します。

```
rommon 1 > confreg 0x2101
```

新しいコンフィギュレーション レジスタを有効にするには、リセットまたは電源の再投入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。

共通ポート割り当て

表 D-1 に、現在割り当てられている Transmission Control Protocol（TCP; 伝送制御プロトコル）ポート番号を示します。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）でも、可能な限り同じ番号が使用されています。

表 D-1　　現在割り当てられている TCP および UDP ポート番号

ポート	キーワード	説明
0	—	予約済み
1 ～ 4	—	未割り当て
5	RJE	リモート ジョブ入力
7	ECHO	エコー
9	DISCARD	廃棄
11	USERS	アクティブ ユーザ
13	DAYTIME	Daytime
15	NETSTAT	netstat
17	QUOTE	Quote of the day
19	CHARGEN	Character generator
20	FTP-DATA	ファイル転送プロトコル（データ）
21	FTP	File Transfer Protocol（ファイル転送プロトコル）
23	TELNET	端末接続
25	SMTP	Simple Mail Transport Protocol（シンプル メール転送プロトコル）
37	TIME	時間
39	RLP	リソース ロケーション プロトコル
42	NAMESERVER	ホストネーム サーバ
43	NICNAME	名前
49	LOGIN	ログイン ホスト プロトコル
53	DOMAIN	ドメイン ネーム サーバ
67	BOOTPS	Bootstrap Protocol Server（ブートストラップ プロトコル サーバ）

表 D-1　現在割り当てられている TCP および UDP ポート番号（続き）

ポート	キーワード	説明
68	BOOTPC	Bootstrap Protocol Client（ブートストラップ プロトコル クライアント）
69	TFTP	Trivial File Transfer Protocol（簡易ファイル転送プロトコル）
75	–	任意のプライベート ダイアルアウト サービス
77	–	任意のプライベート RJE サービス
79	FINGER	Finger
95	SUPDUP	SUPDUP プロトコル
101	HOST NAME	Network Interface Card（NIC; ネットワーク インターフェイス カード）ホスト ネーム サーバ
102	ISO-TSAP	ISO-Transport Service Access Point（TSAP）
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	Sun Microsystems のリモート プロシージャ コール
113	AUTH	認証サービス
117	UUCP-PATH	UNIX-to-UNIX Copy Protocol（UUCP; UNIX 間コピー プログラム）パス サービス
119	NNTP	Usenet Network News Transfer Protocol
123	NTP	Network Time Protocol（ネットワーク タイム プロトコル）
126	SNMP	簡易ネットワーク管理プロトコル
137	NETBIOS-NS	NetBIOS ネーム サービス
138	NETBIOS-DGM	NetBIOS データグラム サービス
139	NETBIOS-SSN	NetBIOS セッション サービス
161	SNMP	簡易ネットワーク管理プロトコル
162	SNMP-TRAP	簡易ネットワーク管理プロトコル トラップ
512	rexec	UNIX のリモート実行（制御）
513	TCP：rlogin UDP：rwho	TCP：UNIX リモート ログイン UDP：UNIX ブロードキャスト ネーム サービス
514	TCP：rsh UDP：syslog	TCP：UNIX リモート シェル UDP：システム ログ

表 D-1　現在割り当てられている TCP および UDP ポート番号（続き）

ポート	キーワード	説明
515	Printer	UNIX ライン プリンタ リモート スプーリング
520	RIP	Routing Information Protocol（ルーティング情報プロトコル）
525	Timed	タイム サーバ

記号

-? コマンド　C-3
? コマンド　A-4, C-3

数字

802.1x 認証　5-8

A

AAL　B-6
AAL3/4　B-6
AAL5　B-6
ACK ビット　B-11
Address Resolution Protocol（アドレス解決プロトコル）
　「ARP」を参照
ADSL　B-1
　概要　B-1
　順序　1-5
　設定　4-6
　トラブルシューティング　14-2
ARP　B-2
Asymmetric Digital Line Subscriber Line
　「ADSL」を参照
ATM
　ATM インターフェイスの設定　1-8
　PVC カプセル化タイプ　B-6
　WAN インターフェイス　4-5
　イベント、表示　14-7
　インターフェイス
　　設定シナリオ　4-5
　エラー、表示　14-7
　概要　B-6
　キュー　B-11
　トラブルシューティング コマンド　14-3 ～ 14-9
　パケット、表示　14-8
ATM Adaptation Layer（ATM アダプテーション レイヤ）
　「AAL」を参照
ATM インターフェイス
　「ATM」を参照
AutoSecure
　設定　12-2

B

b flash コマンド　C-3
b コマンド　C-3

C

CAR　B-10
CBAC ファイアウォール
　設定　12-3
CBWFQ　B-10
Challenge Handshake Authentication Protocol（チャレンジ ハンドシェイク認証プロトコル）
　「CHAP」を参照
CHAP　B-4, B-4 ～ B-5
Cisco IOS キュー　B-11
Cisco IOS ファイアウォール IDS　12-4
Committed Access Rate（専用アクセス レート）
　「CAR」を参照
confreg　C-6
confreg コマンド　C-6
context　C-9

context コマンド C-9
copy C-3
copy running-config startup-config コマンド A-8
copy tftp flash コマンド C-3

D

debug 14-6
debug atm errors コマンド 14-7
debug atm events コマンド 14-7, 14-8
debug atm packet コマンド 14-8, 14-9
debug atm コマンド 14-6
debug コマンド、ROM モニタ C-8, C-9
DHCP
　DHCP サーバの設定 5-2
　IP アドレス割り当て 5-1
DHCP および VLAN による LAN
　設定 5-1
DHCP サーバ
　設定の確認 5-4
　設定例 5-3
　として設定 5-1
DHCP と Easy IP（フェーズ 2） B-9
dir device コマンド C-3
DSL シグナリング プロトコル 4-6
Dynamic Host Configuration Protocol
　「DHCP」を参照

E

Easy IP（フェーズ 1）
　概要 B-8
Easy IP（フェーズ 2）
　概要 B-9
Easy VPN
　設定 6-1
　設定作業 6-2
　設定の確認 6-11
　リモート設定 6-9
EIGRP B-3
　IP 用の設定 1-15 ～ 1-17
　概要 B-3
　設定 1-15
　設定例 1-16
Enhanced Interior Gateway Routing Protocol
　「EIGRP」を参照
Ethernet B-5

F

flowcontrol コマンド A-2
frame C-9
frame コマンド C-9

G

GRE
　設定 7-1
GRE トンネル
　設定作業 7-10
　設定例 7-11
G.SHDSL
　概要 B-2
　順序 1-5
　設定 4-7
　トラブルシューティング 14-2

H

help C-3
help コマンド C-3

I

IGMP スヌーピング 5-10
IKE ポリシー

設定 6-3, 7-3
IP
概要 B-2
ルーティング、設定 1-5
IPCP B-8
IP precedence
CBWFQ B-10
概要 B-10
IPSec トンネル
暗号方式 6-7, 7-7
設定 6-1, 7-1
設定作業 6-2
設定例 6-11, 7-11
トランスフォームおよびプロトコル 6-6, 7-6
IP マルチキャスト スイッチング 5-10
ISDN S/T ポート
ダイヤル バックアップ用 13-9
ISDN インターフェイス
設定 13-10
ISDN ピア ルータ
設定 13-12
i コマンド C-3

K

k コマンド C-9

L

LCP B-4
LFQ B-11
Link Control Protocol
「LCP」を参照
LLC B-6
Low Latency Queuing（低遅延キューイング）
「LFQ」を参照

M

MAC テーブル操作 5-9
meminfo C-9
meminfo コマンド C-9

N

NAT
「Easy IP（フェーズ 1）」も参照
PPPoA を使用した設定 4-9
PPPoE による設定 3-1, 3-7
概要 B-8
設定例 3-9, 4-12
NCP B-4
Network Address Translation（ネットワーク アドレス変換）
「NAT」を参照
Network Control Protocols
「NCP」を参照
Non-Volatile RAM
「NVRAM」を参照
NVRAM、変更の保存 A-8

P

PAP B-4
Password Authentication Protocol
「PAP」を参照
Permanent Virtual Circuit（相手先固定接続）
「PVC」を参照
permit コマンド B-11
ping atm interface コマンド 14-3
PPP B-10
インターリーブ B-10
概要 B-4
認証プロトコル B-4 ～ B-5
フラグメンテーション B-10

PPP/Internet Protocol Control Protocol
「IPCP」を参照 B-8
PPPoA、設定例 4-12
PPPoE
設定 3-1
設定の確認 3-10
設定例 3-9
PPPoE クライアント 3-1, 4-1
PVC
概要 B-6
カプセル化タイプ B-6

Q

QoS
パラメータ B-9 ～ B-11

R

reset コマンド C-3
RIP B-3
概要 B-3
設定 1-14
ROM C-2
ROM モニタ
debug コマンド C-8, C-9
開始 C-1
コマンド C-2
終了 C-10
Routing Information Protocol（ルーティング情報プロトコル）
「RIP」を参照
RST ビット B-11
RSVP B-11

S

SHDSL B-2
「G.SHDSL」を参照
show atm interface コマンド 14-6
show controllers dsl コマンド 4-8
show dsl interface atm コマンド 4-7
show interface コマンド 14-4
stack C-9
stack コマンド C-9
Switched Port Analyzer（SPAN） 5-9
Switched Virtual Interface（SVI） 5-9
Symmetrical High-Data-Rate Digital Subscriber Line
「G.SHDSL」を参照
sysret C-9
sysret コマンド C-9

T

TACACS+ B-5
TCP/IP 関連の設定 5-1
TCP ポート番号、現在割り当てられている D-1 ～ D-3
TFTP C-4
tftpdnld C-4
tftpdnld コマンド C-4, C-5
TFTP ダウンロード C-3 ～ C-6
「コンソール ダウンロード」も参照

U

UDP
ポート番号、現在割り当てられている D-1 ～ D-3
User Datagram Protocol（ユーザ データグラム プロトコル）
「UDP」を参照

V

V.92 モデム
ダイヤル バックアップ用 13-13
VC B-6
VLAN
設定 5-1

設定の確認 5-5
VLAN Trunking Protocol（VTP） 5-8
VPDN 3-3
VPN
設定 6-1, 7-1, 12-4
設定例 6-11
VPN 設定作業 6-2, 7-3

W

WAN インターフェイス
設定 1-7, 3-4, 4-5

X

xmodem C-8
xmodem コマンド C-8

あ

アクセス グループ 12-3
アクセス リスト
インターフェイスへの適用 8-4
コンフィギュレーション コマンド 12-2
説明 B-11
ファイアウォールの設定 8-3
アグリゲータ
設定 13-12
暗号マップ
インターフェイスへの適用 6-7, 6-9, 7-9

い

イネーブル シークレット パスワード
回復 14-13
設定 A-6
イネーブル パスワード
回復 14-13
設定 A-6
イベント、ATM、表示 14-7, 14-8
インスペクション ルール
インターフェイスへの適用 8-4
設定 8-4
インターネット接続、設定 1-4
インターフェイス
ATM
ステータスの表示 14-6
ダイヤラ B-6
インターフェイス コンフィギュレーション モード A-4
インターフェイスのポート ラベル（表） 1-2
インターリーブ
PPP B-10

え

エラー、ATM、表示 14-7
エラー メッセージ、設定 A-7
エラー レポート、ROM モニタ C-8

お

オーバーローディング、定義 B-8

か

回線の設定
V.92 モデム用 13-15
拡張アクセス リスト
概要 B-11
確認
DHCP サーバの設定 5-4
Easy VPN 設定 6-11
NAT 設定による PPPoE 3-10
VLAN 設定 5-5
仮想コンフィギュレーション レジスタ C-6
カプセル化 B-6

「例」も参照

き

企業ネットワーク、接続 1-4
キュー、ATM B-11

く

クラス ベース WFQ
「CBWFQ」を参照
グループ ポリシー
設定 6-4, 7-4
グローバル コンフィギュレーション モード
概要 A-2, A-3
入力 A-6 ～ A-7
グローバル パラメータ、設定 1-6

け

現在割り当てられているポート番号 D-1 ～ D-3

こ

コマンド
ATM トラブルシューティング 14-3 ～ 14-9
debug atm events 14-7, 14-8
debug atm packet 14-9
ROM モニタ デバッグ C-9
アクセス リスト 12-2
完了 A-5
再表示 A-5
使用できる A-4
省略 A-7
特権 EXEC、アクセス A-6
取消 A-7
ヘルプ A-4
コマンドの短縮形 A-7
コマンドの取り消し A-7
コマンドのヘルプ A-4
コマンドの変数
TFTP ダウンロード C-4
一覧 A-5
コマンド モード A-2 ～ A-4
コマンドライン アクセスの設定例 1-12
コンソール ダウンロード C-7 ～ C-8
コンフィギュレーション変更
作成 A-6 ～ A-7
保存 14-13, A-8
コンフィギュレーション レジスタ
ROM モニタからの変更 C-6
値、リセット 14-13
変更 14-11

さ

サイト間 VPN
GRE および IPSec トンネルを使用した 7-1

し

障害の回復 C-3 ～ C-6

す

スイッチ 5-7
スイッチ ポートの設定 5-7
スイッチ ポートの設定、Cisco 1800 5-7
スタティック 1-13
スタティック ルート
設定 1-12
設定例 1-13

せ

セキュリティ機能

設定 12-1 ～ 12-4
セキュリティ認証プロトコル B-4
接続
設定 1-4
設定
ATM インターフェイス 1-8
DHCP サーバ 5-1
Easy VPN 6-1
EIGRP 1-15
EIGRP、IP 1-15 ～ 1-17
GRE トンネル 7-10
IKE ポリシー 7-3
IP EIGRP 1-15 ～ 1-17
IPSec トンネル 6-1
NAT 4-9
NAT による PPPoE 3-1, 3-2
PC からのルータ A-1
RIP 1-14
VLAN 5-1
VPN 6-1, 7-3
WAN インターフェイス 1-7
基本的なルータのパラメータ 1-1
グループ ポリシー 7-4
グローバル パラメータ 1-6
コマンドライン アクセス 1-10
スタティック ルート 1-12
ダイナミック ルート 1-13, 1-15
ダイヤラ インターフェイス 3-5
ダイヤル バックアップ 13-1
ネットワーク、準備 1-4
標準 VT-100 エミュレーション A-2
ファイアウォール 8-1
ファイアウォールのインスペクション ルール 8-4
ファスト イーサネット インターフェイス 1-6, 1-9
ブリッジング 1-10
ルータのデフォルト A-2
ループバック インターフェイス 1-9 ～ 1-10
設定の要件 1-4
設定例
DHCP サーバ 5-3
EIGRP 1-16
IPSec および GRE を使用した VPN 7-11
IPSec トンネルを使用した VPN 6-11
NAT による PPPoA 4-12
NAT による PPPoE 3-9
簡易ファイアウォール 8-5
コマンドライン アクセス 1-12
スタティック ルート 1-13
ダイナミック ルート 1-15
ワイヤレス LAN 9-7

そ

ソフトウェア、アップグレード方法 14-9
ソフトウェアのアップグレード、方法 14-9

た

ターミナル エミュレーション ソフトウェア A-1
ダイナミック ルート
設定 1-13, 1-15
設定例 1-15
ダイヤラ インターフェイス
設定 3-5, 4-3
説明 B-6
ダイヤラ ウォッチ 13-4, B-7
ダイヤル バックアップ
機能の制限事項および設定 13-1
設定 13-1, 13-9, 13-13
ダイヤラ ウォッチ 13-4
フローティング スタティック ルート 13-2

て

デフォルト設定、表示 1-3

と

特権 EXEC コマンド、アクセス　A-6
特権 EXEC モード　A-2, A-3
トラブルシューティング コマンド、ATM　14-3 ～ 14-9
トランスフォーム セット
　設定　6-6
トリガ拡張機能、RIP　B-3

に

認証プロトコル
　「PPP 認証プロトコル」を参照

ね

ネットワーク設定、準備　1-4
ネットワーク プロトコル　B-2

は

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
　設定　3-3
パケット、ATM、表示　14-8
パスワード
　回復　14-9 ～ 14-13
　設定　A-6
　リセット　14-13
パスワード保護　A-6
バックアップ インターフェイス
　ダイヤル バックアップのアクティブ化用　13-1
パラメータ
　グローバル、設定　1-6
ハンドシェイク
　3 方向　B-4
　双方向　B-4
　定義　B-2

ひ

非同期インターフェイス
　設定　13-14
表示、デフォルト設定を　1-3

ふ

ファイアウォール
　アクセス リストのインターフェイスへの適用　8-4
　アクセス リストの設定　8-3
　インスペクション ルールのインターフェイスへの適用　8-4
　インスペクション ルールの設定　8-4
　設定　8-1
　設定作業　8-2
　設定例　8-5
ファスト イーサネット WAN インターフェイス
　設定　1-7, 3-4
ファスト イーサネット インターフェイス
　設定　1-6, 1-9
フィルタリング
　「アクセス リスト」を参照
ブート コマンド　C-3
フォールバック ブリッジング　5-10
フラグメンテーション、PPP　B-10
ブリッジング
　設定　1-10, 9-5
フローティング スタティック ルート
　設定　13-3
　説明　B-7
ブロードキャスト インターバル、RIP　B-3
プロトコル
　ATM　B-6
　PPP 認証　B-4 ～ B-5
　イーサネット　B-5
　ネットワーク　B-2
　ネットワーク インターフェイス　B-5 ～ B-6
　ルーティングの概要　B-3 ～ B-4

へ

変換
　「NAT」を参照
変数、コマンド一覧　A-5

ほ

ポイントツーポイント プロトコル
　「PPP」を参照
ポート単位のストーム制御　5-10
ポート ラベル、インターフェイス用　1-2
ポート割り当て、共通　D-1 ～ D-3
保存、変更した設定の　14-13, A-8
ホップ カウント、定義　B-3
ポリシーベース ルーティング　B-10
ポリシー ルックアップ、イネーブル化　6-6, 7-4, 7-5

む

無線ステーションのサブインターフェイス
　設定　9-6

め

メトリック
　EIGRP　B-3
　RIP　B-3
メトリックとして　B-3

も

モード
　「コマンド モード」を参照
モード設定、暗号マップへの適用　6-5

ゆ

ユーザ EXEC モード　A-2, A-3

よ

要件、設定　1-4

ら

ライン コンフィギュレーション モード　A-4

り

リセット
　コンフィギュレーション レジスタ値　14-13
　パスワード　14-13
　ルータ　14-12 ～ 14-13
リモート アクセス VPN
　Easy VPN および IPSec トンネルを使用した　6-1
リモート管理
　設定　13-9, 13-13

る

ルータ コンフィギュレーション モード　A-4
ルータへのコマンドライン アクセス、設定　1-10
ルーティング プロトコルの概要　B-3 ～ B-4
ルート無線ステーション
　設定　9-3
ループバック インターフェイス
　設定　1-9 ～ 1-10

れ

レイヤ 2 インターフェイス　5-9

わ

ワイヤレス LAN
　設定作業　9-2
　設定例　9-7