Cisco 800M J シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

2015 年 8 月 28 日

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

【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。

Cisco 800M J シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

はじめに ix

目的 ix

対象読者 ix

マニュアルの構成 ix

表記法 x

関連資料 xi

マニュアルの入手方法およびテクニカル サポート xi

Cisco 800M J シリーズ サービス統合型ルータの概要 1-1

Cisco 800M J シリーズ ISR の概要 1-1

Cisco 800M J シリーズ ISR モデル 1-2

Cisco 800M J シリーズ ISR の機能 1-3

Cisco 800M J シリーズ ISR の LED 1-3

ルータの基本設定 2-5

グローバル パラメータの設定 2-5

ギガビット イーサネット WAN インターフェイスの設定 2-6

ループバック インターフェイスの設定 2-7

例：ループバック インターフェイスの設定 2-8

ループバック インターフェイス設定の確認 2-9

コマンドライン アクセスの設定 2-9

ギガビット イーサネット LAN インターフェイスの設定 2-11

スタティック ルートの設定 2-12

例：スタティック ルートの設定 2-12

設定の確認 2-13

ダイナミック ルートの設定 2-13

Routing Information Protocol の設定 2-13

例：RIP の設定 2-14

RIP の設定確認 2-15

Enhanced Interior Gateway Routing Protocol の設定 2-15

例：EIGRP の設定 2-16

EIGRP 設定の確認 2-16

プッシュ ボタンを使用したイメージとコンフィギュレーション リカバリの設定 2-16
ROMMON 初期化中のプッシュ ボタンの動作 2-17
IOS 稼働中のプッシュ ボタンの動作 2-17
プッシュ ボタンを使用した Cisco 800M J シリーズ ISR のゼロ タッチ導入 2-17

イーサネット スイッチ ポートの設定 3-19
VLAN の設定 3-19
例：VLAN の設定 3-20
VTP の設定 3-20
例：VTP の設定 3-21
802.1x 認証の設定 3-21
例：スイッチポートでの IEEE 802.1x および AAA のイネーブル化 3-22
スパニングツリー プロトコルの設定 3-22
例：スパニングツリー プロトコルの設定 3-23
MAC アドレス テーブル操作の設定 3-24
例：MAC アドレス テーブル操作 3-25
MAC アドレス通知トラップの設定 3-25
例：MAC アドレス通知トラップの設定 3-25
スイッチド ポート アナライザ（SPAN）の設定 3-26
例：SPAN の設定 3-26
IGMP スヌーピングの設定 3-27
例：IGMP スヌーピングの設定 3-27
ポート単位のストーム コントロールの設定 3-28
例：ポート単位のストーム コントロールの設定 3-28
HSRP の設定 3-29
例：HSRP の設定 3-29
VRRP の設定 3-30
例：VRRP の設定 3-30

PPP over Ethernet と NAT の設定 4-33
ギガビット イーサネット WAN インターフェイスの設定 4-34
ダイヤラ インターフェイスの設定 4-35
ネットワーク アドレス変換の設定 4-37
設定例 4-39
設定の確認 4-40

セキュリティ機能の設定 5-41
認証、許可、アカウンティングの設定 5-41
アクセス リストの設定 5-42
アクセス グループ 5-43
VPN の設定 5-43
IPSec トンネル上での VPN の設定 5-46
IKE ポリシーの設定 5-47
グループ ポリシー情報の設定 5-48
クリプト マップへのモード設定の適用 5-50
ポリシー ルックアップのイネーブル化 5-51
IPSec トランスフォームおよびプロトコルの設定 5-52
IPSec 暗号方式およびパラメータの設定 5-53
物理インターフェイスへのクリプト マップの適用 5-54
次の作業 5-55
Cisco Easy VPN リモート コンフィギュレーションの作成 5-55
設定例 5-57
サイト間 GRE トンネルの設定 5-57
設定例 5-59
ダイナミック マルチポイント VPN の設定 5-61
例：DMVPN の設定 5-61
Group Encrypted Transport VPN の設定 5-67
例：GETVPN の設定 5-67
SSL VPN の設定 5-71
例：SSL VPN の設定 5-72
FlexVPN の設定 5-74
例：FlexVPN の設定 5-75
ゾーンベース ポリシー ファイアウォールの設定 5-80
VRF-Aware Cisco ファイアウォールの設定 5-80
サブスクリプションベースの Cisco IOS コンテンツ フィルタリングの設定 5-80
On-Device Management for Security Features の設定 5-81
関連資料 5-81

QoS の設定 6-83
クラスベース重み付け均等化キューイングの設定 6-83
例：クラスベース重み付け均等化キューイング 6-84
低遅延キューイングの設定 6-84
例：低遅延キューイング 6-84

クラスベース トラフィック シェーピングの設定 6-85
例：クラスベース トラフィック シェーピング 6-85
クラスベース トラフィック ポリシングの設定 6-85
例：クラスベース トラフィック ポリシング 6-86
クラスベース重み付けランダム早期検出の設定 6-86
例：クラスベース重み付けランダム早期検出 6-86
QoS 階層型キューイング フレームワークの設定 6-87
Network-Based Application Recognition の設定 6-87
例：Network Based Application Recognition 6-87
Resource Reservation Protocol の設定 6-87
VPN 用 Quality of Service の設定 6-88
DMVPN の Per-Tunnel QoS の設定 6-88
レイヤ 2 自動 QoS の設定 6-89

ネットワーク管理機能の設定 7-91
Cisco Configuration Professional 7-91
Cisco Configuration Professional Express 7-92
Cisco Prime Infrastructure 7-92
Embedded Event Manager 7-92
IP SLA の設定 7-93
RADIUS の設定 7-93
TACACS+ の設定 7-93
SSH の設定 7-94
SNMP の設定 7-94
NetFlow の設定 7-94
Flexible NetFlow の設定 7-95
MIB のサポート 7-95

IP アドレッシングおよび IP サービス機能の設定 8-97
DHCP の設定 8-97
DNS の設定 8-98
NAT の設定 8-98
NHRP の設定 8-98
RIP の設定 8-99
EIGRP の設定 8-99
OSPF の設定 8-99
BGP の設定 8-100

パフォーマンス ルーティング v3 の設定 8-100
IP マルチキャストの設定 8-100
BFD の設定 8-101
Multi-VRF の設定 8-101
IPv6 機能の設定 8-101

はじめに

ここでは、本ガイドの目的、対象読者、構成、および表記法について説明し、本マニュアルセットに付属の参考資料について紹介します。内容は次のとおりです。

- 目的、ix ページ
- 対象読者、ix ページ
- マニュアルの構成、ix ページ
- 表記法、x ページ
- 関連資料、xi ページ
- マニュアルの入手方法およびテクニカル サポート、xi ページ

目的

このマニュアルでは、Cisco 800M J シリーズ サービス統合型ルータ（ISR）の各種機能の設定方法を説明します。

対象読者

本マニュアルの対象読者は、サービス契約に基づきルータをインストール、監視およびトラブルシューティングする熟練した技術者、ならびに Information Technology（IT; 情報技術）部のもとで働く技術者です。

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
概要	Cisco 800M J シリーズ ISR のハードウェアおよびソフトウェア機能の概要について説明します。
ルータの基本設定	ルータ、インターフェイスおよびルーティングの基本設定方法について説明します。
イーサネット スイッチ ポートの設定	Cisco 800M J シリーズ ISR のギガビット イーサネット スイッチの設定作業の概要について説明します。

章	説明
PPP over Ethernet と NAT の設定	Point-to-Point Protocol over Ethernet （PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。
セキュリティ機能の設定	Cisco 800M J シリーズ ISR のセキュリティ機能の設定方法について説明します。
QoS の設定	Cisco 800M J シリーズ ISR でサポートされている Quality of Service（QoS）機能の設定について説明します。
ネットワーク管理機能の設定	Cisco 800M J シリーズ ISR のネットワーク管理機能の設定について説明します。
IP アドレッシングおよび IP サービス機能の設定	Cisco 800M J シリーズ ISR の IP アドレッシングおよび IP サービス機能の設定について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードなどの出力されない文字は、山カッコで（< >）囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

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

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

警告 **「*警告*」の意味です。人身事故を予防するための注意事項が記述されています。**

関連資料

『Cisco 800M J シリーズ ISR ソフトウェア コンフィギュレーション ガイド』（本マニュアル）に加え、以下のリファレンス ガイドが含まれます。

マニュアルの種類	リンク
ハードウェア	*『Cisco 800M J シリーズ ハードウェア インストレーション ガイド』*
適合規格	*『Regulatory Compliance and Safety Information for Cisco 800 Series Routers』*

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/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

Cisco 800M J シリーズ サービス統合型ルータの概要

この章では、Cisco 800M J シリーズ サービス統合型ルータ（ISR）の概要と、機能の設定方法を説明します。この章の内容は次のとおりです。

- 「Cisco 800M J シリーズ ISR の概要」1 ページ
- 「Cisco 800M J シリーズ ISR モデル」2 ページ
- 「Cisco 800M J シリーズ ISR の機能」3 ページ

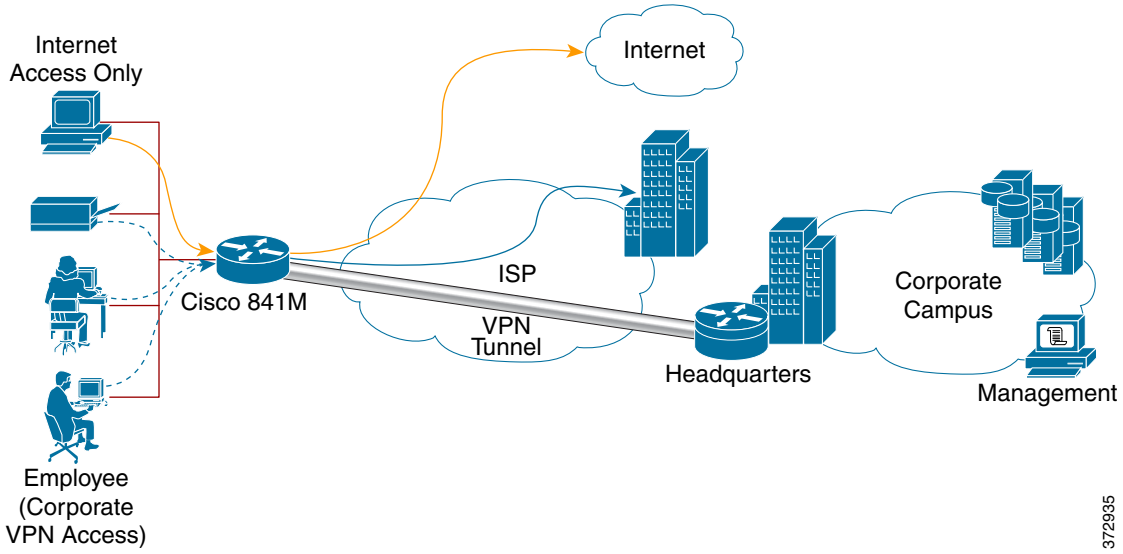
Cisco 800M J シリーズ ISR の概要

Cisco 800M J シリーズ ISR は、中央拠点への安全なネットワーク接続を提供する、小規模オフィスのためのエントリレベルのブランチ ルータです。Cisco 800M J シリーズ ISR は、2 ポートのギガビット イーサネット WAN ポートを備え、ギガビット イーサネット WAN 接続オプションを提供します。Cisco 800M J シリーズ ISR には、LAN 接続用に 4 ポートまたは 8 ポートのギガビット イーサネット LAN ポートが搭載されています。

Cisco 800M J シリーズ ISR は Cisco IOS ソフトウェアを実行することによって組み込みのセキュリティ機能を提供します。セキュリティのための追加のソフトウェア ライセンスは不要です。Cisco 800M J シリーズ ISR は、ネットワーク エッジでのアプリケーションの開発と実行を行うのためのオープンな拡張可能環境を提供します。

図 1-1 に、Cisco 800M J シリーズ ISR を導入し、小規模オフィスからセキュア VPN トンネル経由で本社にリモート接続できるようにするシナリオを示します。このシナリオでの企業ユーザは、インターネット ユーザとは別の VLAN を使用します。

図 1-1　Cisco 800M シリーズの導入例



Cisco 800M J シリーズ ISR モデル

表 1-1 に、Cisco 800M J シリーズ ISR の各種 SKU を示します。

表 1-1　Cisco 800M J シリーズ ISR の SKU

SKU ID	説明
C841M-4X-JAIS/K9	Cisco C841M-4X/K9 ISR（GE LAN ポート X 4 および GE WAN ポート X 2）および Cisco Advanced IP Services IOS イメージ。
C841M-4X-JSEC/K9	Cisco C841M-4X/K9 ISR（GE LAN ポート X 4 および GE WAN ポート X 2）および Cisco Advanced Security IOS イメージ。
C841M-8X-JAIS/K9	Cisco C841M-4X/K9 ISR（GE LAN ポート X 8 および GE WAN ポート X 2）および Cisco Advanced IP Services IOS イメージ。

Cisco 800M J シリーズ ISR の機能

Cisco 800M J シリーズ ISR でサポートされている主要な機能には次のものがあります。

- Advanced Security 機能（IP Security（IPSec）VPN、トンネルレス Group Encrypted Transport（GETVPN）など）
- レイヤ 2 機能（VLAN/802.1q トランキングなど）
- Cisco Configuration Professional Express を使用した統合デバイス管理
- SNMP、Telnet、HTTP を使用した、リモート管理とネットワーク モニタリング。ローカルのコンソール ポートからも実行可能。

Cisco 800M J シリーズ ISR の LED

表 1-2 に、Cisco 800M J シリーズ ISR の LED の説明を示します。

表 1-2　Cisco 800M J シリーズ ISR の LED

LED	色	説明
SYS	グリーン（点滅）	システムは ROMMON モードで稼働しているか、または IOS を起動中です。
	消灯	システムの電源がオフです。
	グリーンで点灯	IOS は正常に機能しています。
VPN OK	グリーン	少なくとも 1 つの VPN 接続が確立しています。
	消灯	VPN 接続は確立していません。
PPP OK	グリーン	少なくとも 1 つの PPP 接続が確立しています。
	消灯	PPP 接続は確立していません。
LAN	グリーンで点灯	LAN 接続が確立されています。
	グリーン（点滅）	LAN ポートでデータ伝送中です。
	消灯	LAN に接続していません。
WAN	グリーンで点灯	WAN リンクが確立されています。
	グリーン（点滅）	WAN ポートでデータ伝送中です。
	消灯	WAN リンクに接続していません。

ルータの基本設定

このモジュールでは、Cisco 800M J シリーズ ISR の基本的な設定手順について説明します。具体的な内容は、次のとおりです。

- 「グローバル パラメータの設定」5 ページ
- 「ギガビット イーサネット WAN インターフェイスの設定」6 ページ
- 「ループバック インターフェイスの設定」7 ページ
- 「コマンドライン アクセスの設定」9 ページ
- 「ギガビット イーサネット LAN インターフェイスの設定」11 ページ
- 「スタティック ルートの設定」12 ページ
- 「ダイナミック ルートの設定」13 ページ
- 「プッシュ ボタンを使用したイメージとコンフィギュレーション リカバリの設定」16 ページ
- 「プッシュ ボタンを使用した Cisco 800M J シリーズ ISR のゼロ タッチ導入」17 ページ

グローバル パラメータの設定

ルータのグローバル パラメータを設定するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**configure terminal**
	
	例：
	`Router> enable`
	`Router# configure terminal`
		グローバル コンフィギュレーション モードを開始します（コンソール ポート使用時）。

ステップ 2	**hostname** *name* **例：** `Router(config)# hostname Router`	ルータ名を指定します。
ステップ 3	**enable secret** *password* **例：** `Router(config)# enable secret cr1ny5ho`	ルータへの不正なアクセスを防止するには、暗号化パスワードを指定します。
ステップ 4	**no ip domain-lookup** **例：** `Router(config)# no ip domain-lookup`	ルータが未知の単語（入力ミス）を IP アドレスに変換しないようにします。

ギガビット イーサネット WAN インターフェイスの設定

ギガビット イーサネット（GE）WAN インターフェイスを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface gigabitethernet** *slot*/*port*
3. **ip address** *ip-address mask*
4. **no shutdown**
5. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet** *slot*/*port* **例：** `Router(config)# interface gigabitethernet 0/8`	ルータ上で ギガビット イーサネット インターフェイスのコンフィギュレーション モードを開始します。 **（注）** ギガビット イーサネット WAN インターフェイスは、8 ポートの LAN ポートを備えた Cisco 800M J シリーズ ISR モデルでは 0/8 および 0/9、4 ポートの LAN ポートを備えた Cisco 800M J シリーズ ISR では 0/4 から 0/5 です。
ステップ 3	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	指定した GE 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-if)# no shutdown`	GE インターフェイスを有効化（閉塞解除）し、管理上の状態をダウンからアップに変更します。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	GE 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。

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 アドレスを設定するために用いられ、デフォルトのルーティング情報を提供します。

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **例：** `Router(config)# interface Loopback 0`	ループバック インターフェイスのコンフィギュレーション モードを開始します。
ステップ 3	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.108.1.1 255.255.255.0`	ループバック インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 4	**exit** **例：** `Router(config-if)# exit`	ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例：ループバック インターフェイスの設定

このコンフィギュレーション例のループバック インターフェイスは、仮想テンプレート インターフェイス上の NAT をサポートするために使用されています。この設定例は、スタティック IP アドレスとして機能する IP アドレス 200.200.100.1/24 のギガビット イーサネット インターフェイス上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 に紐付けられます。

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

ループバック インターフェイス設定の確認

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、次の例に示すように **show interface loopback** コマンドを入力します。

```
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
```

次の例に示すように、**ping** コマンドを使用してループバック インターフェイスを確認することもできます。

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

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、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **例：** `Router(config)# line console 0`	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。
ステップ 3	**password** *password* **例：** `Router(config)# password 5dr4Hepw3`	コンソール端末回線に固有のパスワードを指定します。
ステップ 4	**login** **例：** `Router(config-line)# login`	端末ログイン セッションでのパスワード検証をイネーブルにします。
ステップ 5	**exec-timeout** *minutes* [*seconds*] **例：** `Router(config-line)# exec-timeout 5 30`	ユーザ入力が検出されるまで EXEC コマンド インタープリタが待機する間隔を設定します。デフォルトは 10 分です。任意で、間隔値に秒数を追加することもできます。
ステップ 6	**line** [**aux** | **console** | **tty** | **vty**] *line-number* **例：** `Router(config-line)# line vty 0 4`	リモート コンソール アクセス用の仮想端末を指定します。
ステップ 7	**password** *password* **例：** `Router(config-line)# password aldf2ad1`	仮想端末回線に固有のパスワードを指定します。
ステップ 8	**login** **例：** `Router(config-line)# login`	仮想端末ログイン セッションでのパスワード検証をイネーブルにします。
ステップ 9	**end** **例：** `Router(config-line)# endRouter#`	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。

ギガビット イーサネット LAN インターフェイスの設定

ギガビット イーサネット（GE）LAN インターフェイスを手動で設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface gigabitethernet** *slot*/*port*
3. **ip address** *ip-address mask*
4. **no shutdown**
5. **exit**

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface gigabitethernet** *slot*/*port* **例：** `Router(config)# interface gigabitethernet 0/1`	ルータ上で ギガビット イーサネット インターフェイスのコンフィギュレーション モードを開始します。 **（注）** ギガビット イーサネット LAN インターフェイスは、8 ポートの LAN ポートを備えた Cisco 800M J シリーズ ISR では 0/0 から 0/7、4 ポートの LAN ポートを備えた Cisco 800M J シリーズ ISR では 0/0 から 0/3 です。
ステップ 3	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 192.168.12.2 255.255.255.0`	指定した GE 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-if)# no shutdown`	GE インターフェイスを有効化（閉塞解除）し、管理上の状態をダウンからアップに変更します。
ステップ 5	**exit** **例：** `Router(config-if)# exit`	GE 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。

スタティック ルートの設定

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

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

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} **例：** `Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`	IP パケットのスタティック ルートを指定します。
ステップ 3	**end** **例：** `Router(config)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例：スタティック ルートの設定

次の設定例は、宛先 IP アドレスが 192.168.1.0、サブネット マスクが 255.255.255.0 のすべての IP パケットを、IP アドレス 10.10.10.2 の他の装置に対して、ギガビット インターフェイス上からスタティック ルートで送信します。

「**(default)**」と示されているコマンドは、入力する必要はありません。このコマンドは、**show running-config** コマンドの使用時に、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示されます。

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

設定の確認

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

次のような確認用の出力が表示されます。

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

Gateway of last resort is not set

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

ダイナミック ルートの設定

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

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

- 「Routing Information Protocol の設定」セクション（13 ページ）
- 「Enhanced Interior Gateway Routing Protocol の設定」セクション（15 ページ）

Routing Information Protocol の設定

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

手順の概要

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

手順の詳細

	コマンド	タスク
ステップ 1	**configure terminal** **例：** `Router> configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router rip** **例：** `Router(config)# router rip`	ルータ コンフィギュレーション モードを開始します。続いて、ルータの RIP をイネーブルにします。
ステップ 3	**version** {**1** | **2**} **例：** `Router(config-router)# version 2`	RIP version 1 または 2 の使用を指定します。
ステップ 4	**network** *ip-address* **例：** `Router(config-router)# network 192.168.1.1`	直接接続しているネットワークの各アドレスを使用して、RIP を適用するネットワーク リストを指定します。
ステップ 5	**no auto-summary** **例：** `Router(config-router)# no auto-summary`	ネットワークレベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。これにより、サブプレフィックス ルーティング情報がクラスフル ネットワーク境界を越えて送信されます。
ステップ 6	**end** **例：** `Router(config-router)# end`	ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例：RIP の設定

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

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

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

RIP の設定確認

RIP が正しく設定されたかどうかを確認するには、**show ip route** コマンドを入力し、次の例に示すように「R」で表される RIP ルートを探します。

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

Gateway of last resort is not set

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

Enhanced Interior Gateway Routing Protocol の設定

Enhanced Interior Gateway Routing Protocol（EIGRP）を設定するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンド	目的
ステップ 1	**configure terminal** **例：** `Router> configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router eigrp** *as-number* **例：** `Router(config)# router eigrp 109`	ルータ コンフィギュレーション モードを開始して、ルータ上で EIGRP をイネーブルにします。自律システム（AS）番号は、他の EIGRP ルータへのルートを識別します。また、EIGRP 情報のタグ付けに使用されます。
ステップ 3	**network** *ip-address* **例：** `Router(config)# network 192.145.1.0`	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）。

	コマンド	目的

ステップ 4	**end**
	
	例：
	`Router(config-router)# end`
	`Router#`
		ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

例：EIGRP の設定

次に、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 プロトコルの設定例を示します。EIGRP の自律システム番号として、109 が割り当てられています。

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

```
Router# show running-config...
!
router eigrp 109
    network 192.145.1.0
        network 10.10.12.115
!
...
```

EIGRP 設定の確認

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、次の例に示すように「D」で表される EIGRP ルートを探します。

```
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
```

プッシュ ボタンを使用したイメージとコンフィギュレーション リカバリの設定

Cisco 800M J シリーズ ISR の背面にプッシュ ボタン、つまりリセット ボタンがあります。このボタンは、ルータでディザスタ リカバリを実行できるようにすることを目的としています。

プッシュ ボタンは、次の 2 つのシナリオでのリカバリに便利です。

- ROMMON の初期化中
- IOS が起動し、稼働状態になった後で、ルータ IOS プロンプトにアクセスせずに特定のコンフィギュレーション ファイルをロードする場合

ROMMON 初期化中のプッシュ ボタンの動作

表 2-1 に、ROMMON の初期化中にプッシュ ボタンが押された場合の機能の概要を示します。

表 2-1　ROMMON の初期化中のプッシュ ボタンの機能

ROMMON の動作	IOS の動作
• デフォルトのボー レートを使用してブートします。 • 自動ブートを実行します。 • コンパクト フラッシュで *.default イメージを使用可能な場合はロードします。	*.cfg という名前の設定が NVRAM ストレージまたはフラッシュ ストレージで使用できる場合、IOS は元の設定のバックアップを実行し、その設定を使用して起動されます。

IOS 稼働中のプッシュ ボタンの動作

IOS が稼働状態になった後でプッシュ ボタンを 3 秒以上押してから放すと、IOS がこのイベントを検出し、優先順位に従ってコンフィギュレーション ファイルを検索します。IOS がコンフィギュレーション ファイルを検出すると、そのファイルがスタートアップ コンフィギュレーション ファイルにコピーされます。その後、ルータ自体がリロードし、新しい設定が有効になります。コンフィギュレーション ファイルが見つからない場合、リセット ボタンを押しても何も起こりません。

ルータがコンフィギュレーション ファイルを検索する優先順位は次のとおりです。

1. usbflash0:customer-config.*SN*
2. usbflash0:customer-config
3. flash:customer-config.*SN*
4. flash:customer-config

（注）　*SN* はハードウェア シリアル番号です。

プッシュ ボタンを使用した Cisco 800M J シリーズ ISR のゼロ タッチ導入

Cisco 800M J シリーズ ISR の USB 機能によるゼロタッチ導入（ZTD）は、USB フラッシュ ドライブからカスタマイズされた設定をロードする使いやすい機能です。この機能を使用するには、ルータの不揮発性 RAM（NVRAM）にスタートアップ コンフィギュレーションが存在しない状態である必要があります。また、有効なコンフィギュレーション ファイル（ファイル拡張子が**.cfg**）が USB フラッシュ ドライブに保存されている必要があります。有効なコンフィギュレーション ファイルは、ルータの実行コンフィギュレーションをフラッシュ、USB フラッシュ、または TFTP サーバに保存することにより作成できます。

スタートアップ コンフィギュレーションがないルータでは、起動時にプッシュ ボタンが押されると、システムが USB フラッシュ ドライブ内に有効なコンフィギュレーション ファイルがあるかどうかをチェックします。USB 機能によるゼロ タッチ導入を使用した導入の前提条件を次に示します。

- スタートアップ コンフィギュレーションが存在しない状態でルータを起動すること。
- Cisco USB フラッシュ ドライブが使用可能な最初の USB スロットに挿入されていること。
- ファイル名拡張子が **.cfg** の ASCII テキスト形式の有効なコンフィギュレーション ファイル。

USB フラッシュ ドライブに複数の .cfg ファイルがある場合、ルータは USB フラッシュ ドライブ内でインデックス番号が最も大きいファイルを選択します。誤った .cfg ファイルがロードされないようにするため、USB フラッシュドライブには 1 つの .cfg ファイルだけを保存してください。

イーサネット スイッチ ポートの設定

この章では、Cisco 800M J シリーズ ISR のギガビット イーサネット（GE）スイッチの設定作業の概要について説明します。

この章の内容は、次のとおりです。

- 「VLAN の設定」19 ページ
- 「VTP の設定」20 ページ
- 「802.1x 認証の設定」21 ページ
- 「スパニングツリー プロトコルの設定」22 ページ
- 「MAC アドレス テーブル操作の設定」24 ページ
- 「MAC アドレス通知トラップの設定」25 ページ
- 「スイッチド ポート アナライザ（SPAN）の設定」26 ページ
- 「IGMP スヌーピングの設定」27 ページ
- 「ポート単位のストーム コントロールの設定」28 ページ
- 「HSRP の設定」29 ページ
- 「VRRP の設定」30 ページ

VLAN の設定

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラッディングが行われます。各 VLAN は論理ネットワークと見なされ、VLAN に属さないステーション宛てのパケットはルータで転送する必要があります。

VLAN の設定に関する詳細については、次の Web リンクを参照してください。

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

VLAN の設定例については、「例：VLAN の設定」を参照してください。

例：VLAN の設定

VLAN 間ルーティングの設定方法の例を示します。

```
Router# configure terminal
Router(config)# vlan 1
Router(config)# vlan 2
Router(config)# interface vlan 1
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 2
Roouter(config-if)# ip address 2.2.2.2 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface gigabitethernet 0/1
Router(config-if)# switchport access vlan 1
Router(config-if)# interface gigabitethernet 0/2
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

VTP の設定

VTP は、レイヤ 2 のメッセージ プロトコルであり、ネットワーク全体にわたって VLAN の追加、削除、名前の変更を管理することにより、VLAN 設定の整合性を維持します。VTP により、VLAN 名の重複、誤った VLAN タイプの指定、セキュリティ違反など、さまざまな問題を引き起こしかねない設定の誤りや矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のスイッチ上で集中的に設定変更を行い、その変更を自動的にネットワーク上の他のスイッチに伝達できます。VTP を使用しない場合、VLAN に関する情報を他のスイッチに送信できません。VTP は、1 台のスイッチで行われた更新が VTP を介してドメイン内の他のスイッチに送信される環境で動作するように設計されています。VLAN データベースに対する複数の更新が同一ドメイン内のスイッチ上で同時に発生する環境の場合、VTP は適していません。VLAN データベースの不整合が生じます。

VTP の設定に関する次の概念を理解する必要があります。

- VTP ドメイン：VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチまたはスイッチ スタックで構成されます。スイッチは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。
- VTP サーバ：VTP サーバ モードでは、VLAN の作成、変更、削除ができます。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 サーバは、同一 VTP ドメイン内の他のスイッチに自分の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズメントに基づいて、自分の VLAN 設定を他のスイッチと同期させます。VTP サーバはデフォルト モードです。
- VTP クライアント：VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。
- VTP トランスペアレント：VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できます。

VTP の設定に関する詳細については、次の Web リンクを参照してください。

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

VTP の設定例については、「例：VTP の設定」を参照してください。

例：VTP の設定

スイッチを VTP サーバとして設定する方法の例を示します。

```
Router# configure terminal
Router(config)# vtp mode server
Router(config)# vtp domain Lab_Network
Router(config)# vtp password WATER
Router(config)# exit
```

スイッチを VTP クライアントとして設定する方法の例を示します。

```
Router# configure terminal
Router(config)# vtp mode client
Router(config)# exit
```

スイッチを VTP トランスペアレントとして設定する方法の例を示します。

```
Router# configure terminal
Router(config)# vtp mode transparent
Router# exit
```

802.1x 認証の設定

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

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

- サプリカント：LAN およびスイッチ サービスへのアクセスを要求し、ルータからの要求に応答するデバイス（ワークステーション）。ワークステーションでは、Microsoft Windows XP オペレーティング システムで提供されるクライアントなど、IEEE 802.1x 準拠のクライアント ソフトウェアが稼働している必要があります （サプリカントはクライアントと呼ばれることもあります）。
- 認証サーバ：サプリカントの実際の認証を実行する装置。認証サーバはサプリカントの識別情報を確認し、そのサプリカントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをルータに通知します。ネットワーク アクセス デバイス（この例では Cisco ISR ルータ）は、サプリカントと認証サーバ間で認証メッセージを透過的に渡し、サプリカントと認証サーバ間で認証プロセスが実行されます。サプリカントと認証サーバ（RADIUS サーバ）間で使用される EAP 方式が決定されます。EAP 拡張機能を搭載した RADIUS セキュリティ システムは、Cisco Secure Access Control Server バージョン 3.0 以降で使用できます。RADIUS はクライアントおよびサーバ モデルで動作し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

- オーセンティケータ：サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御するルータ。ルータは、サプリカントと認証サーバ間で仲介装置として動作し、サプリカントからの ID 情報を要求し、その情報を認証サーバで確認し、応答をサプリカントにリレーします。ルータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

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

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

802.1x 認証の設定例については、「例：スイッチポートでの IEEE 802.1x および AAA のイネーブル化」を参照してください。

例：スイッチポートでの IEEE 802.1x および AAA のイネーブル化

次に、Cisco 800M J シリーズ ISR を 802.1x オーセンティケータとして設定する例を示します。

```
Router> enable
Router# configure terminal
Router(config)# dot1x system-auth-control
Router(config)# aaa new-model
Router(config)# aaa authentication dot1x default group radius
Router(config)# interface gigabitethernet 0/1
Router(config-if)# switchport mode access
Router(config-if)# authentication port-control auto
Router(config-if)# dot1x pae authenticator
Router(config-if)# end
```

スパニングツリー プロトコルの設定

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

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

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

すべてのポートに役割が指定されているスイッチ、またはバックアップの役割が指定されているスイッチはルート スイッチです。少なくとも 1 つのポートに役割が指定されているスイッチは、指定スイッチを意味します。スパニング ツリーは、冗長データ パスを強制的にスタンバイ（ブロック）ステートにします。スパニングツリーのネットワーク セグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリー アルゴリズムがスパニングツリー トポロジを再計算し、スタンバイ パスをアクティブにします。スイッチは、定期的にブリッジ プロトコル データ ユニット（BPDU）と呼ばれるスパニングツリー フレームを送受信します。スイッチはこのフレームを転送しませんが、このフレームを使用してループフリー パスを構築します。BPDU には、送信側スイッチおよびそのポートについて、スイッチおよび MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなどの情報が含まれます。スパニングツリーはこの情報を使用して、スイッチド ネットワーク用のルート スイッチおよびルート ポートを選定し、さらに、各スイッチド セグメントのルート ポートおよび指定ポートを選定します。

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

STP の設定に関する詳細については、次のリンクを参照してください。

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

設定例については、「例：スパニングツリー プロトコルの設定」を参照してください。

例：スパニングツリー プロトコルの設定

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MAC アドレス テーブル操作の設定

MAC アドレス テーブルには、スイッチがポート間のトラフィック転送に使用するアドレス情報が含まれています。このアドレス テーブルに登録されたすべての MAC アドレスは、1 つまたは複数のポートに対応しています。アドレス テーブルに含まれるアドレス タイプには、次のものがあります。

- ダイナミック アドレス：スイッチが学習し、使用されなくなった時点でドロップされる送信元 MAC アドレス。エージング タイム設定を使用して、テーブル内で使用されていないアドレスをスイッチが保持する期間を定義します。
- スタティック アドレス：手動で入力され、期限切れにならず、スイッチのリセット時にも消去されないユニキャスト アドレス。

アドレス テーブルは、宛先 MAC アドレス、対応する VLAN（仮想 LAN）ID、アドレスに対応付けられたポート番号、およびタイプ（スタティックまたはダイナミック）のリストです。

セキュア MAC アドレスのイネーブル化、スタティック エントリの作成、セキュア MAC アドレス最大数の設定、エージング タイムの設定の例については、「例：MAC アドレス テーブル操作」を参照してください。

MAC アドレス テーブルの操作の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1048223

例：MAC アドレス テーブル操作

次に、ポートのセキュア MAC アドレス オプションをイネーブルにする設定の例を示します。

```
Router# configure terminal
Router(config)# mac-address-table secure 0004.0005.0006 GigabitEthernet 0/1 vlan 5
Router(config)# end
```

次に、MAC アドレス テーブルにスタティック エントリを作成する例を示します。

```
Router# configure terminal
Router(config)# mac-address-table static 0002.0003.0004 interface GigabitEthernet 0/2 vlan
3
Router(config)# end
```

次に、セキュア MAC アドレスの最大数を 10 に設定する例を示します。

```
Router# configure terminal
Router(config)# mac-address-table secure maximum 10 GigabitEthernet 0/1
Router(config)# end
```

次に、エージング タイマーを設定する例を示します。

```
Router# configure terminal
Router(config)# mac-address-table aging-time 300
Router(config)# end
```

MAC アドレス通知トラップの設定

MAC アドレス通知は、スイッチに MAC アドレス アクティビティを保存することでネットワーク上のユーザを追跡できます。スイッチが MAC アドレスを学習または削除するたびに、SNMP 通知を生成してネットワーク管理システム（NMS）に送信させることができます。ネットワークに多数のユーザの出入りがある場合は、トラップ インターバル タイムを設定して通知トラップを組み込み、ネットワーク トラフィックを削減できます。MAC 通知履歴テーブルは、トラップがイネーブルに設定されたハードウェアのポートごとの MAC アドレス アクティビティを保存します。MAC アドレス通知は、動的でセキュアな MAC アドレスについて生成されます。自己アドレス、マルチキャスト アドレス、またはその他のスタティック アドレスについては、イベントは生成されません。

設定例については、「例：MAC アドレス通知トラップの設定」を参照してください。

例：MAC アドレス通知トラップの設定

次に、MAC アドレスがインターフェイスに追加されたときに MAC 通知トラップをイネーブルにする方法の例を示します。

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# snmp trap mac-notification added
Router(config-if)# end
```

次に、MAC アドレスがインターフェイスから削除されたときに MAC 通知トラップをイネーブルにする方法の例を示します。

```
Router(config)# interface gigabitethernet 0/1
Router(config-if)# snmp trap mac-notification removed
Router(config-if)# end
```

スイッチド ポート アナライザ（SPAN）の設定

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、そのスイッチ上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングには影響しません。宛先ポートは SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に出入りするトラフィックだけです。送信元 VLAN にルーティングされたトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

SPAN 設定の例については、「例：SPAN の設定」26 ページを参照してください。

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

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

例：SPAN の設定

ギガビット イーサネット送信元インターフェイスからの双方向トラフィックをモニタするように SPAN セッションを設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 source gigabitethernet 0/1
Router(config)# end
```

ギガビット イーサネット インターフェイスを SPAN セッションの宛先として設定する方法の例を示します。

```
Router# configure terminal
Router(config)# monitor session 1 destination gigabitethernet 0/2
Router(config)# end
```

SPAN セッション 1 の SPAN 送信元としてのギガビット イーサネットを削除する方法の例を示します。

```
Router# configure terminal
Router(config)# no monitor session 1 source gigabitethernet 0/1
Router(config)# end
```

IGMP スヌーピングの設定

IGMP スヌーピングは、レイヤ 2 インターフェイスを動的に設定し、マルチキャスト トラフィックが IP マルチキャスト デバイスと対応付けられたインターフェイスにだけ転送されるようにすることによって、マルチキャスト トラフィックのフラッディングを制限します。名称が示すとおり、IGMP スヌーピングの場合は、LAN スイッチでホストとルータ間の IGMP 伝送をスヌーピングし、マルチキャスト グループとメンバ ポートを追跡する必要があります。特定のマルチキャスト グループについて、ホストから IGMP レポートを受信したスイッチは、ホストのポート番号を転送テーブル エントリに追加します。ホストから IGMP Leave Group メッセージを受信した場合は、テーブル エントリからホスト ポートを削除します。マルチキャスト クライアントから IGMP メンバーシップ レポートを受信しなかった場合にも、スイッチはエントリを定期的に削除します。

マルチキャスト ルータは、すべての VLAN に定期的にジェネラル クエリーを送出します。このマルチキャスト トラフィックに関心のあるホストはすべて Join 要求を送信し、転送テーブルのエントリに追加されます。スイッチは、IGMP Join 要求の送信元となる各グループの IGMP スヌーピング IP マルチキャスト転送テーブルで、VLAN ごとに 1 つずつエントリを作成します。

デフォルトでは、IGMP スヌーピングはグローバルに（システム全体で）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、既存のすべての 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。デフォルトでは、IGMP スヌーピングはすべての VLAN で有効ですが、VLAN 単位で有効または有効にすることができます。グローバルな IGMP スヌーピングは VLAN 単位の IGMP スヌーピング機能よりも優先されます。グローバル スヌーピングがディセーブルの場合、VLAN スヌーピングをイネーブルに設定することはできません。グローバルなスヌーピングが有効な場合、VLAN 単位でスヌーピングを有効または無効にすることができます。

IGMP スヌーピングの設定例については、「例：IGMP スヌーピングの設定」を参照してください。

例：IGMP スヌーピングの設定

IGMP スヌーピングを VLAN インターフェイスでイネーブルにする方法の例を示します。

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1
Router# end
```

マルチキャスト ルータへのスタティックな接続をイネーブルにする方法の例を示します。

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/1
Router# end
```

ポートをマルチキャスト グループのメンバーとして追加する方法の例を示します。ポートは通常、IGMP レポート メッセージを通じてマルチキャスト グループに加入しますが、ポートをマルチキャスト グループのメンバーとしてスタティックに設定することもできます。

```
Router# configure terminal
Router(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface gigabitethernet
0/1
Router# end
```

ポート単位のストーム コントロールの設定

ストーム コントロールは、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャスト ストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワーク パフォーマンスが低下します。ストームは、プロトコル スタック実装でのエラー、ネットワーク設定の誤り、またはサービス妨害攻撃を行うユーザにより引き起こされる可能性があります。

ストーム コントロール（またはトラフィック抑制）は、インターフェイスからスイッチング バスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

ストーム コントロールは、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャスト トラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、しきい値のレベルが高いほど、ブロードキャスト ストームに対する保護効果は薄くなります。

ポート単位のストーム コントロールの設定例については、「例：ポート単位のストーム コントロールの設定」を参照してください。

例：ポート単位のストーム コントロールの設定

ギガビット イーサネット インターフェイスで帯域幅に基づくマルチキャスト ストーム コントロールを 70 パーセントで有効にする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/2
Router(config-if)# storm-control multicast level 70.0 30.0
Router(config-if)# end
Router# show storm-control multicast
Interface  Filter State   Upper    Lower    Current
---------  -------------  -------  -------  -------
Gi0/0      inactive       100.00%  100.00%      N/A
Gi0/1      inactive       100.00%  100.00%      N/A
Gi0/2      Forwarding      70.00%   30.00%    0.00%
```

HSRP の設定

Hot Standby Router Protocol（HSRP）は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークの可用性を高めるシスコの標準方式です。HSRP を使用すると、特定のルータのアベイラビリティに依存せず IP トラフィックをルーティングできます。また、一連のルータ インターフェイスを組み合わせることで、1 台の仮想ルータ、または LAN 上のホストへのデフォルト ゲートウェイのように機能させることができます。ネットワークまたはセグメント上に HSRP を設定すると、仮想 MAC（メディア アクセス コントロール）アドレス、および設定されたルータ グループ間で共有される IP アドレスを使用できるようになり HSRP が設定された複数のルータは、仮想ルータの MAC アドレスおよび IP ネットワーク アドレスを使用できるようになります。仮想ルータは、実際には存在しません。仮想ルータは、相互にバックアップ機能を提供するように設定されている複数のルータの共通のターゲットを表します。1 台のルータがアクティブなルータとして、もう 1 台のルータがスタンバイ ルータとして選択されます。スタンバイ ルータは、指定されたアクティブ ルータが故障した場合に、グループの MAC アドレスおよび IP アドレスを制御するルータです。

HSRP では、プライオリティ メカニズムを使用して、デフォルトのアクティブ デバイスにする HSRP 設定済みデバイスを決定します。デバイスをアクティブ デバイスとして設定するには、他のすべての HSRP 設定済みデバイスのプライオリティよりも高いプライオリティをそのデバイスに割り当てます。デフォルトのプライオリティは 100 です。したがって、100 よりも高いプライオリティを持つデバイスを 1 つだけ設定した場合、そのデバイスがデフォルトのアクティブ デバイスになります。プライオリティが等しい場合、プライマリ IP アドレスが比較され、大きい IP アドレスが優先されます。ルータの設定で standby preempt インターフェイス コンフィギュレーション コマンドを使用しない場合、そのルータのプライオリティが他のルータよりも高い場合でもそのルータはアクティブス ルータになりません。

HSRP の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp.html

HSRP の設定例については、「例：HSRP の設定」を参照してください。

例：HSRP の設定

この例では、ルータ A は、グループ 1 のアクティブ デバイスおよびグループ 2 のスタンバイ デバイスになるように設定されています。ルータ B は、グループ 2 のアクティブ デバイスおよびグループ 1 のスタンバイ デバイスになるように設定されています。

```
RouterA# configure terminal
RouterA(config)# interface GigabitEthernet 0/1
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.3
RouterA(config-if)# standby 2 priority 95
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.1.0.4
RouterA(config-if)# end

RouterB# configure terminal
RouterB(config)# interface GigabitEthernet 0/1
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.3
RouterB(config-if)# standby 2 priority 110
```

```
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

VRRP の設定

仮想ルータ冗長プロトコル（VRRP）は、LAN 上の VRRP ルータに対し、1 台または複数台の仮想ルータの役割をダイナミックに割り当てる選択プロトコルです。この場合、マルチアクセス リンク上にある何台かのルータが同じ仮想 IP アドレスを使用できるようにします。VRRP ルータは、LAN に接続された 1 つ以上の他のルータと連係して VRRP プロトコルを実行するように設定されます。VRRP 設定では、1 台のルータが仮想マスター ルータとして選定され、他のルータは仮想マスター ルータが機能を停止した場合のバックアップとして動作します。

VRRP の重要な設定項目に、VRRP ルータ プライオリティがあります。プライオリティにより、各 VRRP ルータが実行する役割と、仮想マスタールータが機能を停止したときにどのようなことが起こるかが決定されます。VRRP ルータが仮想ルータの IP アドレスと物理インターフェイスの IP アドレスのオーナーである場合には、このルータが仮想マスタールータとして機能します。VRRP ルータが仮想バックアップ ルータとして機能するかどうかや、仮想マスタールータが機能を停止した場合に仮想マスタールータを引き継ぐ順序も、プライオリティによって決定されます。**vrrp priority** コマンドを使用して、各仮想バックアップ ルータのプライオリティを設定できます。

デフォルトでは、プリエンプティブ設定はイネーブルになっています。この場合、仮想マスタールータになるように選択されている仮想バックアップ ルータの中で、より高いプライオリティが設定されている仮想バックアップルータが仮想マスタールータになります。このプリエンプティブ設定をディセーブルにするには、**no vrrp preempt** コマンドを使用します。プリエンプションがディセーブルになっている場合は、元の仮想マスタールータが回復して再びマスターになるまで、仮想マスタールータになるように選択されている仮想バックアップルータがマスターの役割を実行します。

仮想マスタールータは、同じグループ内の他の VRRP ルータに VRRP アドバタイズメントを送信します。アドバタイズメントでは、仮想マスタールータのプライオリティとステートを伝えます。VRRP アドバタイズメントは IP パケットにカプセル化され、VRRP グループに割り当てられた IP バージョン 4 マルチキャスト アドレスに送信されます。アドバタイズメントは、デフォルトで 1 秒に 1 回送信されますが、この間隔は設定可能です。

VRRP に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html

VRRP の設定例については、「例：VRRP の設定」を参照してください。

例：VRRP の設定

次の例では、ルータ A とルータ B はそれぞれ 2 つの VRRP グループ（グループ 1 とグループ 5）に属しています。この設定では、各グループに次の特性があります。

グループ 1：

- 仮想 IP アドレスは 10.1.0.10 です。
- ルータ A はプライオリティ 120 で、このグループのマスターになります。
- アドバタイズ インターバルは 3 秒です。
- プリエンプションはイネーブルです。

グループ 5：

- ルータ B はプライオリティ 200 で、このグループのマスターになります。
- アドバタイズ インターバルは 30 秒です。
- プリエンプションはイネーブルです。

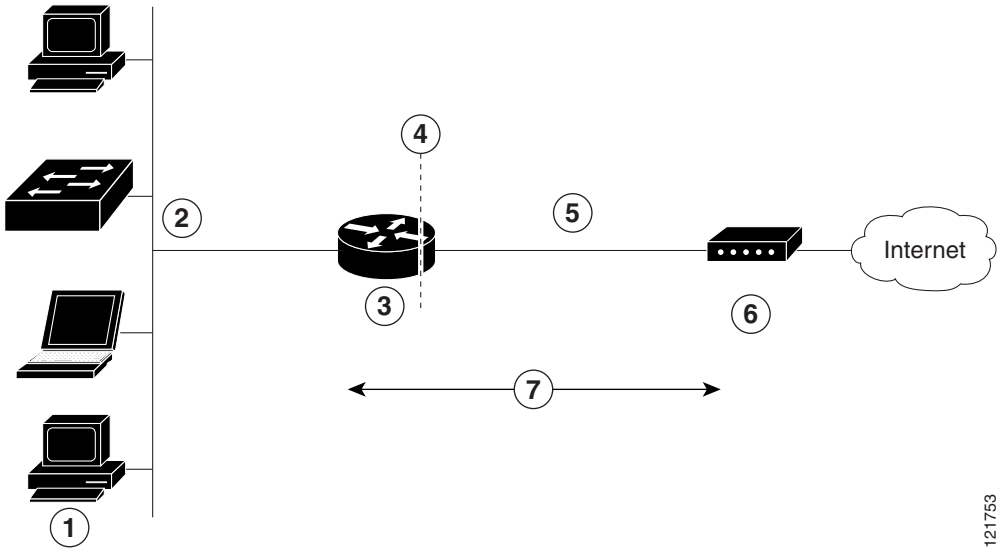
```
RouterA(config)# interface GigabitEthernet 0/1
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# no shutdown

RouterA(config-if)# end

RouterB(config)# interface GigabitEthernet 0/1
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# no shutdown
RouterB(config-if)# end
```

PPP over Ethernet と NAT の設定

この章では、Cisco 800M J シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。

ルータの背後の LAN には、複数の PC を接続できます。これらの PC からのトラフィックは PPPoE セッションに送信する前に暗号化やフィルタリングなどを行うことができます。図 4-1 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 4-1　PPP over Ethernet と NAT



1	複数のネットワーク デバイス：デスクトップ、ラップトップ PC、スイッチ
2	ギガビット 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 800M J シリーズ ISR
4	NAT が実行されるポイント
5	ギガビット イーサネット WAN インターフェイス（NAT 用の外部インターフェイス）
6	ケーブル モデムまたはインターネットに接続している他のサーバ
7	クライアントと PPPoE サーバ間の PPPoE セッション

PPPoE

ルータ上の PPPoE クライアント機能により、イーサネット インターフェイスでの PPPoE クライアント サポートが可能になります。仮想アクセスのクローニングには、ダイヤラ インターフェイスを使用する必要があります。イーサネット インターフェイスには、複数の PPPoE クライアント セッションを設定できますが、セッションごとに別個のダイヤラ インターフェイスと別個のダイヤラ プールを使用する必要があります。

PPPoE セッションが Cisco 800M J シリーズ ISR によってクライアント側で開始されます。確立された PPPoE クライアント セッションは、次のいずれかの方法で終了できます。

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

NAT

NAT（ルータの端に破線で表示）は、2 つのアドレッシング ドメインと内部発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。

- ギガビット 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

この設定タスクの結果を示す例は「設定例」に示されています。

ギガビット イーサネット WAN インターフェイスの設定

このシナリオでは、PPPoE クライアント（Cisco ルータ）が、内部および外部のギガビット イーサネット インターフェイスを介して通信します。

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

手順の概要

1. **interface** *type number*
2. **pppoe-client dial-pool-number** *number*
3. **no shutdown**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface gigabitethernet 0/8`	WAN インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**pppoe-client dial-pool-number** *number* **例：** `Router(config-if)# pppoe-client dial-pool-number 1`	PPPoE クライアントを設定し、クローニングに使用するダイヤラ インターフェイスを指定します。
ステップ 3	**no shutdown** **例：** `Router(config-if)# no shutdown`	ギガビット 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`	ギガビット イーサネット インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

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。ギガビット 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。

ルータのギガビット イーサネット LAN インターフェイスの 1 つにダイヤラ インターフェイスを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface dialer** dialer-rotary-group-number
2. **ip address negotiated**
3. **ip mtu** *bytes*
4. **encapsulation** *encapsulation-type*
5. **ppp authentication** {*protocol1* [*protocol2*...]}
6. **dialer pool** *number*
7. **dialer-group** *group-number*

8. **exit**
9. **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**}
10. **ip route** *prefix mask* {*interface-type interface-number*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface dialer** *dialer-rotary-group-number* **例：** `Router(config)# interface dialer 0`	ダイヤラ インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。 • 範囲は 0 ～ 255 です。
ステップ 2	**ip address negotiated** **例：** `Router(config-if)# ip address negotiated`	インターフェイスの IP アドレスを PPP/IPCP（IP Control Protocol）アドレス ネゴシエーションで取得することを指定します。
ステップ 3	**ip mtu** *bytes* **例：** `Router(config-if)# ip mtu 1492`	IP 最大伝送単位（MTU）のサイズを設定します。 • デフォルトの最小値は 128 バイトです。イーサネットの最大値は 1492 バイトです。
ステップ 4	**encapsulation** *encapsulation-type* **例：** `Router(config-if)# encapsulation ppp`	送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。
ステップ 5	**ppp authentication** {*protocol1* [*protocol2*...]} **例：** `Router(config-if)# ppp authentication chap`	PPP 認証方式を Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）に設定します。
ステップ 6	**dialer pool** *number* **例：** `Router(config-if)# dialer pool 1`	特定の宛先サブ ネットワークへの接続に使用するダイヤラ プールを指定します。
ステップ 7	**dialer-group** *group-number* **例：** `Router(config-if)# dialer-group 1`	ダイヤラ グループにダイヤラ インターフェイスを割り当てます。 • 指定できる範囲は 1 ～ 10 です。 **ヒント** ダイヤラ グループを使用して、ルータへのアクセスを制御します。
ステップ 8	**exit** **例：** `Router(config-if)# exit`	ダイヤラ 0 のインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**} **例：** `Router(config)# dialer-list 1 protocol ip permit`	ダイヤラ リストを作成し、ダイヤル グループを関連付けます。パケットは、指定されたインターフェイス ダイヤラ グループを通じて転送されます。
ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*} **例：** `Router(config)# ip route 10.10.25.2 255.255.255.255 dialer 0`	ダイヤラ 0 インターフェイスのデフォルト ゲートウェイに IP ルートを設定します。

ネットワーク アドレス変換の設定

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

外部ギガビット イーサネット WAN インターフェイスをダイナミック NAT で設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **ip nat pool** *name start-ip end-ip* {**netmask** *netmask* \| **prefix-length** *prefix-length*}
2. **ip nat inside source** {**list** *access-list-number*} {**interface** *type number* \| **pool** *name*} [**overload**]
3. **interface** *type number*
4. **ip nat** {**inside** \| **outside**}
5. **no shutdown**
6. **exit**
7. **interface** *type number*
8. **ip nat** {**inside** \| **outside**}
9. **no shutdown**
10. **exit**
11. **access-list** *access-list-number* {**deny** \| **permit**} *source* [*source-wildcard*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*} **例：** `Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0`	NAT 用のグローバル IP アドレスのプールを作成します。

ステップ 2	**ip nat inside source** {**list** *access-list-number*} {**interface** *type number* | **pool** *name*} [**overload**]
	
	例：
	`Router(config)# ip nat inside source list 1 interface dialer 0 overload`
	
	または
	`Router(config)# ip nat inside source list acl1 pool pool1`
		内部インターフェイス上のダイナミック アドレス変換をイネーブルにします。
		最初の例は、アクセス リスト *1* で許可されたアドレスが、ダイヤラ インターフェイス *0* に指定されているいずれかのアドレスに変換されることを示しています。
		次の例は、アクセス リスト *acl1* で許可されたアドレスが、NAT プール *pool1* に指定されたいずれかのアドレスに変換されることを示しています。

ステップ 3	**interface** *type number* **例：** `Router(config)# interface vlan 1`	NAT の内部インターフェイスにする VLAN（ギガビット 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`	指定の VLAN インターフェイスを NAT の内部インターフェイスとして識別します。
ステップ 5	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。
ステップ 6	**exit** **例：** `Router(config-if)# exit`	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。
ステップ 7	**interface** *type number* **例：** `Router(config)# gigabitethernet 0/8`	NAT の外部インターフェイスとするギガビット イーサネット WAN 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 8	**ip nat** {**inside** | **outside**} **例：** `Router(config-if)# ip nat outside`	指定の WAN インターフェイスを NAT の外部インターフェイスとして識別します。

	コマンドまたはアクション	目的
ステップ 9	**no shutdown** **例：** `Router(config-if)# no shutdown`	イーサネット インターフェイスに対する設定変更をイネーブルにします。
ステップ 10	**exit** **例：** `Router(config-if)# exit`	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。
ステップ 11	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] **例：** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	変換が必要なアドレスを示す標準アクセス リストを定義します。 **（注）** その他のアドレスはすべて、暗黙的に拒否されます。

（注） 仮想テンプレート インターフェイスとともに NAT を使用するには、ループ バック インターフェイスを設定する必要があります。ループバック インターフェイスの設定の詳細については、第 2 章「ルータの基本設定」を参照してください。

設定例

次の設定例は、この章で説明した PPPoE シナリオのコンフィギュレーション ファイルの一部を示しています。

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

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

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
interface GigabitEthernet 0/8
no ip address
no ip directed-broadcast (default)
ip nat outside
pppoe enable group global
pppoe-client dial-pool-number 1
no sh
```

```
!
interface dialer 0
ip address negotiated
ip mtu 1492
encapsulation ppp
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
ip classless (default)
ip route 10.10.25.2 255.255.255.255 dialer 0
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0
ip nat inside source list acl1 pool pool1
!
```

設定の確認

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

```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
GigabitEthernet 0/8
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
```

セキュリティ機能の設定

Cisco 800M J シリーズ ISR は、次のセキュリティ機能を提供します。

- 「認証、許可、アカウンティングの設定」41 ページ
- 「アクセス リストの設定」42 ページ
- 「VPN の設定」43 ページ
- 「ダイナミック マルチポイント VPN の設定」61 ページ
- 「Group Encrypted Transport VPN の設定」67 ページ
- 「SSL VPN の設定」71 ページ
- 「FlexVPN の設定」74 ページ
- 「ゾーンベース ポリシー ファイアウォールの設定」80 ページ
- 「VRF-Aware Cisco ファイアウォールの設定」80 ページ
- 「サブスクリプションベースの Cisco IOS コンテンツ フィルタリングの設定」80 ページ
- 「On-Device Management for Security Features の設定」81 ページ
- 「関連資料」81 ページ

認証、許可、アカウンティングの設定

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

AAA では、Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）、Terminal Access Controller Access Control System Plus（TACACS+; ターミナル アクセス コントローラ アクセス コントロール システム プラス）、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、次のガイドを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-mt/sec-usr-aaa-15-mt-book.html

アクセス リストの設定

アクセス リストは、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のネットワーク トラフィックを許可または拒否します。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、共通のタグによってまとめられた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 5-1 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 5-1　アクセス リスト コンフィギュレーション コマンド

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

アクセス リストの作成の詳細については、次の Web リンクを参照してください：
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book.html

アクセス グループ

アクセス グループとは、共通の名前または番号によってまとめられた一連のアクセス リストの定義のことです。アクセス グループは、インターフェイスを設定するときに、インターフェイスに対してイネーブルにされます。アクセス グループを作成する場合は、次の注意事項に従ってください。

- 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。
- すべてのパラメータがアクセス リストに一致した場合に、パケットが許可または拒否されます。
- すべてのシーケンスの末尾には、暗黙の「deny all」が付きます。

アクセス グループの設定と管理の詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book/sec-create-ip-al-filter.html

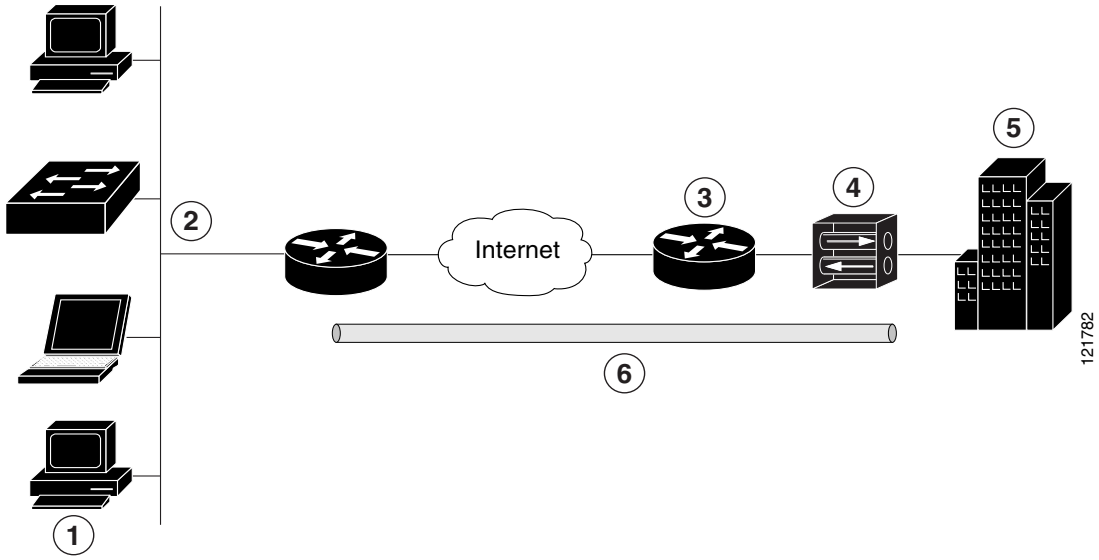
VPN の設定

バーチャル プライベート ネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介して、2 つのネットワーク間に安全な接続を提供します。Cisco 800M J シリーズ ISR は、VPN のサイト間アクセスとリモート アクセスの 2 種類をサポートします。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。サイト間 VPN は、たとえば、ブランチ オフィスと企業オフィスを接続する際に使用されます。ここでは、サイト間 VPN およびリモート アクセス VPN の例を示します。

リモート アクセス VPN の例

リモート アクセス VPN コンフィギュレーションでは、Cisco Easy VPN および IP Security（IPSec）トンネルを使用して、リモート クライアントとコーポレート ネットワーク間の接続を設定および保護します。図 5-1 は、一般的な構成例を示します。

図 5-1　IPSec トンネルを使用したリモート アクセス VPN



1	リモート ネットワークで接続されたユーザ
2	VPN クライアント：Cisco 800M J シリーズ ISR
3	ルータ：コーポレート オフィスのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ（外部インターフェイス アドレスが 210.110.101.1 の VPN 終端装置など）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN クライアント機能は、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業の大部分を排除します。このプロトコルでは、ほとんどの VPN パラメータ（内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、Windows インターネット ネーム サービス（WINS）サーバ アドレス、スプリットトンネリング フラグなど）を、VPN サーバに定義することできます。

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

Cisco Easy VPN クライアント機能は、2 つのモード（クライアント モードまたはネットワーク拡張モード）のいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、中央サイトでは利用できません。ネットワーク拡張モードでは、VPN 終端装置が配置されている中央サイトのユーザは、クライアント サイトのネットワーク リソースにアクセスできます。

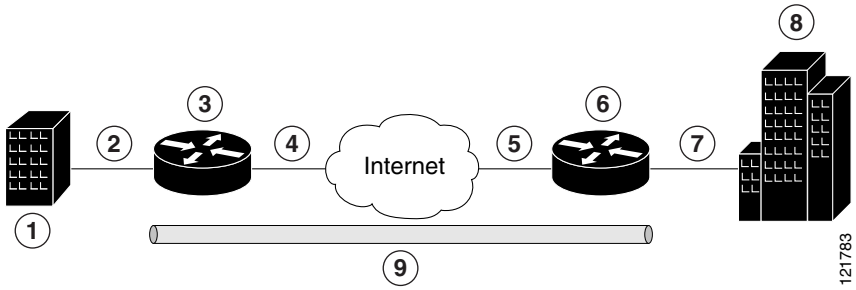
IPSec サーバの設定を完了すると、IPSec クライアント上で最小限の設定を行って VPN 接続を作成できます。IPSec クライアントが VPN トンネル接続を開始すると、IPSec サーバは IPSec ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

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

サイト間 VPN

サイト間 VPN の設定では、IPSec および汎用ルーティング カプセル化（GRE）プロトコルを使用して、ブランチ オフィスとコーポレート ネットワーク間の接続を保護します。図 5-2 は、一般的な構成例を示します。

図 5-2　IPSec トンネルおよび GRE を使用したサイト間の VPN



1	複数の LAN および VLAN を使用しているブランチ オフィス
2	ギガビット 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 800M J シリーズ ISR
4	ギガビット イーサネット インターフェイス：アドレスは 200.1.1.1（NAT 用の外部インターフェイス）
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（内部インターフェイス アドレスは 10.1.1.1）：企業ネットワークに接続
8	コーポレート オフィス ネットワーク
9	GRE を使用した IPSec トンネル

IPSec および GRE の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book/sec-cfg-vpn-ipsec.html

設定例

各例では、「IPSec トンネル上での VPN の設定」セクション（46 ページ）の手順を使用して IPSec トンネル上に VPN を設定します。次に、リモート アクセス設定およびサイト間設定の具体的な手順を順番に説明します。

この章の設定例は、Cisco 800M J シリーズ ISR のエンドポイント設定にだけ適用されます。VPN 接続では、機能するためには両方のエンドポイントが正しく設定されていることが必要です。他のルータ モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

VPN コンフィギュレーション情報は、両方のエンドポイントに設定する必要があります。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、ネットワーク アドレス変換（NAT）などのパラメータを指定する必要があります。

- 「IPSec トンネル上での VPN の設定」セクション（46 ページ）
- 「Cisco Easy VPN リモート コンフィギュレーションの作成」セクション（55 ページ）
- 「サイト間 GRE トンネルの設定」セクション（57 ページ）

IPSec トンネル上での VPN の設定

IPSec トンネル上に VPN を設定するには、次の作業を行います。

- 「IKE ポリシーの設定」47 ページ
- 「グループ ポリシー情報の設定」48 ページ
- 「クリプト マップへのモード設定の適用」50 ページ
- 「ポリシー ルックアップのイネーブル化」51 ページ
- 「IPSec トランスフォームおよびプロトコルの設定」52 ページ
- 「IPSec 暗号方式およびパラメータの設定」53 ページ
- 「物理インターフェイスへのクリプト マップの適用」54 ページ
- 「次の作業」55 ページ

IKE ポリシーの設定

インターネット キー交換（IKE）ポリシーを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto isakmp policy** *priority* **例：** `Router(config)# crypto isakmp policy 1`	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、ISAKMP[1] 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 128**	**aes 192**	**aes 256**} **例：** `Router(config-isakmp)# encryption 3des`	IKE ポリシーに使用される暗号化アルゴリズムを指定します。 この例では、168 ビット DES[2] を指定します。
ステップ 3	**hash** {**md5**	**sha**	**sha256**	**sha384**	**sha512**} **例：** `Router(config-isakmp)# hash md5`	IKE ポリシーに使用されるハッシュ アルゴリズムを指定します。 この例では、MD5[3] アルゴリズムを指定します。デフォルト値は SHA-1 です[4]。
ステップ 4	**authentication** {**rsa-sig**	**rsa-encr**	**pre-share**} **例：** `Router(config-isakmp)# authentication pre-share`	IKE ポリシーに使用される認証方式を指定します。 この例では、事前共有キーを指定します。
ステップ 5	**group** {**1**	**2**	**5**} **例：** `Router(config-isakmp)# group 2`	IKE ポリシーに使用される Diffie-Hellman グループを指定します。

	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`	IKE SA[5] のライフタイムを 60～86400 秒に指定します。
ステップ 7	**exit** **例：** `Router(config-isakmp)# exit`	IKE ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードを開始します。

1. ISAKMP = インターネット セキュリティ アソシエーション キーおよび管理プロトコル
2. DES = データ暗号規格
3. MD5 = メッセージ ダイジェスト 5
4. SHA-1 = Secure Hash 標準
5. SA = セキュリティ アソシエーション

グループ ポリシー情報の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto isakmp client configuration group** {*group-name*	*default*} **例：** `Router(config)# crypto isakmp client configuration group rtr-remote`	リモート クライアントにダウンロードされる属性を含む IKE ポリシー グループを作成します。 また、ISAKMP グループ ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**key** *name* **例：** `Router(config-isakmp-group)# key secret-password`	グループ ポリシーの IKE 事前共有キーを指定します。
ステップ 3	**dns** *primary-server* **例：** `Router(config-isakmp-group)# dns 10.50.10.1`	グループのプライマリ DNS[1] サーバを指定します。 **wins** コマンドを使用して、グループ用の WINS[2] 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`	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`	IKE グループ ポリシー コンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**ip local pool** {**default** | *poolname*} [*low-ip-address* [*high-ip-address*]] **例：** `Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`	グループのローカル アドレス プールを指定します。 このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

1. DNS = ドメイン ネーム システム
2. WINS = Windows インターネット ネーム サービス

クリプト マップへのモード設定の適用

クリプト マップにモード設定を適用するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto map** *map-name* **isakmp authorization list** *list-name* **例：** `Router(config)# crypto map dynmap isakmp authorization list rtr-remote`	クリプト マップにモード設定を適用し、AAA サーバからのグループ ポリシーのキー ルックアップ（IKE クエリ）をイネーブルにします。

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

ポリシー ルックアップのイネーブル化

AAA 経由でポリシー ルックアップをイネーブルにするには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** **例：** `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 2	**aaa authentication login** {**default**	*list-name*} *method1* [*method2*...] **例：** `Router(config)# aaa authentication login rtr-remote local`	選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。 この例では、ローカル認証データベースを使用します。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: Securing User Services, Release 15M&T*』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`	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。
ステップ 4	**username** *name* {**nopassword**	**password** *password*	**password** *encryption-type encrypted-password*} **例：** `Router(config)# username username1 password 0 password1`	ユーザ名をベースとした認証システムを構築します。

IPSec トランスフォームおよびプロトコルの設定

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

IKE のネゴシエーション中に、ピアは、複数のトランスフォーム セットの中から両方のピアで同一のトランスフォーム セットを検索します。このようなトランスフォームが含まれているトランスフォーム セットが検出された場合は、両方のピアの設定の一部として選択され、保護対象トラフィックに適用されます。

IPSec トランスフォーム セットおよびプロトコルを指定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **crypto ipsec profile** *profile-name*
2. **crypto ipsec transform-set** *transform-set-name*
3. **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**crypto ipsec profile** *profile-name*
	
	例：
	`Router(config)# crypto ipsec profile pro1`
	`Router(config)#`
		IPSec プロファイルを設定し、暗号化用にトンネル上で保護を適用します。

ステップ 2	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **例：** `Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`	トランスフォーム セット（IPSec セキュリティ プロトコルとアルゴリズムの有効な組み合わせ）を定義します。 有効なトランスフォームおよび組み合わせの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 3	**crypto ipsec security-association lifetime** {**seconds** *seconds*	**kilobytes** *kilobytes*} **例：** `Router(config)# crypto ipsec security-association lifetime seconds 86400`	IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。

IPSec 暗号方式およびパラメータの設定

ダイナミック クリプト マップ ポリシーでは、ルータがすべてのクリプト マップ パラメータ（IP アドレスなど）を認識していない場合でも、リモート IPSec ピアからの新規の SA のネゴシエーション要求を処理します。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **例：** `Router(config)# crypto dynamic-map dynmap 1`	ダイナミック クリプト マップ エントリを作成し、クリプト マップ コンフィギュレーション モードを開始します。 このコマンドの詳細については、『*Cisco IOS Security Command Reference*』を参照してください。
ステップ 2	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **例：** `Router(config-crypto-map)# set transform-set vpn1`	クリプト マップ エントリで使用可能なトランスフォーム セットを指定します。
ステップ 3	**reverse-route** **例：** `Router(config-crypto-map)# reverse-route`	クリプト マップ エントリの送信元プロキシ情報を作成します。
ステップ 4	**exit** **例：** `Router(config-crypto-map)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**crypto map** *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*] **例：** `Router(config)# crypto map static-map 1 ipsec-isakmp dynamic dynmap`	クリプト マップ プロファイルを作成します。

物理インターフェイスへのクリプト マップの適用

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

インターフェイスにクリプト マップを適用するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface gigabitethernet 0/0`	クリプト マップを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**crypto map** *map-name* **例：** `Router(config-if)# crypto map static-map`	クリプト マップをインターフェイスに適用します。
ステップ 3	**exit** **例：** `Router(config-crypto-map)# exit`	グローバル コンフィギュレーション モードに戻ります。

次の作業

Cisco Easy VPN リモート コンフィギュレーションを作成する場合は、「Cisco Easy VPN リモート コンフィギュレーションの作成」セクション（55 ページ）を参照してください。

IPSec トンネルおよび GRE を使用してサイト間 VPN を作成する場合は、「サイト間 GRE トンネルの設定」セクション（57 ページ）を参照してください。

Cisco Easy VPN リモート コンフィギュレーションの作成

Cisco Easy VPN クライアントとして動作しているルータでは、Cisco Easy VPN リモート コンフィギュレーションを作成し、それを発信インターフェイスに割り当てる必要があります。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ipsec client ezvpn** *name* **例：** `Router(config)# crypto ipsec client ezvpn ezvpnclient`	Cisco Easy VPN リモート コンフィギュレーションを作成します。続いて、Cisco Easy VPN リモート コンフィギュレーション モードを開始します。
ステップ 2	**group** *group-name* **key** *group-key* **例：** `Router(config-crypto-ezvpn)# group ezvpnclient key secret-password`	VPN 接続の IPSec グループおよび IPSec キー値を指定します。

	コマンドまたはアクション	目的
ステップ 3	**peer** {*ipaddress* | *hostname*} **例：** `Router(config-crypto-ezvpn)# peer 192.168.100.1`	VPN 接続のピア IP アドレスまたはホスト名を指定します。 **（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。 **（注）** このコマンドを使用して、バックアップとして使用する複数のピアを設定します。1 つのピアがダウンすると、次に使用可能なピアを用いて Easy VPN トンネルが確立されます。プライマリ ピアが再起動すると、プライマリ ピアを用いてトンネルが再確立されます。
ステップ 4	**mode** {**client** | **network-extension** | **network extension plus**} **例：** `Router(config-crypto-ezvpn)# mode client`	VPN 動作モードを指定します。
ステップ 5	**exit** **例：** `Router(config-crypto-ezvpn)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**crypto isakmp keepalive** *seconds* **例：** `Router(config-crypto-ezvpn)# crypto isakmp keepalive 10`	デッド ピア検出メッセージがイネーブルになります。メッセージ間の時間は、秒単位で 10 ～ 3600 の範囲で指定します。
ステップ 7	**interface** *type number* **例：** `Router(config)# interface Gigabitethernet 0/2`	Cisco Easy VPN リモート コンフィギュレーションを適用するインターフェイスでインターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **例：** `Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`	WAN インターフェイスに Cisco Easy VPN リモート コンフィギュレーションを割り当てることにより、ルータが VPN 接続に必要な NAT または PAT[1]、およびアクセス リスト コンフィギュレーションを自動作成します。
ステップ 9	**exit** **例：** `Router(config-crypto-ezvpn)# exit`	グローバル コンフィギュレーション モードに戻ります。

1. PAT = ポート アドレス変換

設定例

次に、EasyVPN クライアントの設定例を示します。

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username username1 password 0 password1
!
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 gigabitethernet 0/4
    crypto ipsec client ezvpn ezvpnclient outside
    crypto map static-map

interface vlan 1
    crypto ipsec client ezvpn ezvpnclient inside
!
```

サイト間 GRE トンネルの設定

サイト間 GRE トンネルを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**interface** *type number* **例：** `Router(config)# interface tunnel 1`	トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 2	**ip address** *ip-address mask* **例：** `Router(config-if)# ip address 10.62.1.193 255.255.255.252`	トンネルにアドレスを割り当てます。
ステップ 3	**tunnel source** *interface-type number* **例：** `Router(config-if)# tunnel source gigabitethernet 0/0`	GRE トンネルにルータの送信元エンドポイントを指定します。
ステップ 4	**tunnel destination** *default-gateway-ip-address* **例：** `Router(config-if)# tunnel destination 192.168.101.1`	GRE トンネルにルータの宛先エンドポイントを指定します。
ステップ 5	**crypto map** *map-name* **例：** `Router(config-if)# crypto map static-map`	トンネルにクリプト マップを割り当てます。 **（注）** トンネル インターフェイスへのダイナミック ルーティングまたはスタティック ルートは、サイト間の接続を確立するために設定しておく必要があります。

	コマンドまたはアクション	目的
ステップ 6	**exit** **例：** `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**ip access-list** {**standard** | **extended**} *access-list-name* **例：** `Router(config)# ip access-list extended vpnstatic1`	クリプト マップに使用されている名前付き ACL[1] の ACL コンフィギュレーション モードを開始します。
ステップ 8	**permit** *protocol source source-wildcard destination destination-wildcard* **例：** `Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`	発信インターフェイスでは GRE トラフィックだけが許可されるように指定します。
ステップ 9	**exit** **例：** `Router(config-acl)# exit`	グローバル コンフィギュレーション モードに戻ります。

1. ACL = アクセス コントロール リスト

設定例

次の設定例は、これまでの項で説明してきた GRE トンネルを使用した、サイト間 VPN 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 username1 password 0 password1
!
interface tunnel 1
    ip address 10.62.1.193 255.255.255.252

tunnel source GigabitEthernet 0/3

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

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

```
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPsec tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Defines encryption and transform set for the IPsec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPsec tunnel.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
! VLAN 1 is the internal home network.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Inspection examines outbound traffic.
    crypto map static-map
    no cdp enable
!
! GE4 is the outside or Internet-exposed interface
interface Gigabitethernet 0/4
 ip address 210.110.101.21 255.255.255.0
 ! acl 103 permits IPsec traffic from the corp. router as well as
 ! denies Internet-initiated traffic inbound.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Applies the IPsec tunnel to the outside interface.
!
! Utilize NAT overload in order to make best use of the
! single address provided by the ISP.
ip nat inside source list 102 interface Gigabitethernet 0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
!
! acl 102 associated addresses used for NAT.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
```

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

ダイナミック マルチポイント VPN の設定

ダイナミック マルチポイント VPN（DMVPN）機能は、GRE トンネル、IPsec 暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせて大規模および小規模な IP Security（IPsec）VPN を導入できるようにするシンプルなソリューションです。DMVPN は、大規模な VPN 導入の設定作業を簡素化し、管理面での負担を軽減します。

DMVPN は、本社に設置されている 1 つの中央ルータがハブとして機能し、その他のブランチ ルータがスポークとして機能し、社内のリソースにアクセスするためにハブ ルータに接続しているシナリオで便利です。DMVPN はスポーク間導入にも有用であり、ブランチ間相互接続に使用できます。

ハブ アンド スポーク導入の標準的な DMVPN 設定については、「例：DMVPN の設定」61 ページを参照してください。DMVPN の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html

例：DMVPN の設定

次に、DMVPN ハブ アンド スポーク導入モデルの設定例を示します。この例では、Cisco 800M J シリーズ ISR がスポークとして設定され、Cisco 2900 シリーズ ISR がハブとして設定されます。読みやすくするため、設定の一部が省略されています。

次の設定セクションは、800M J シリーズ ISR をスポークとして設定する部分を示します。

800M_spoke# **show running-config**

```
Building configuration...
Current configuration : 2546 bytes
!
! Last configuration change at 09:09:39 UTC Tue Jun 24 2014
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 800M_spoke
!
boot-start-marker
boot-end-marker
!
!
logging buffered 10000000
!
no aaa new-model
```

```
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 2
crypto isakmp key ISA_KEY address 0.0.0.0
crypto isakmp keepalive 10 periodic
!

crypto ipsec transform-set DMVPN-TRANS-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile DMVPN-PROFILE
 set security-association lifetime seconds 120
 set transform-set DMVPN-TRANS-SET
!

interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface Tunnel0
 ip address 24.1.1.2 255.255.255.0
 no ip redirects
 ip mtu 1440
 ip nhrp authentication ISA_KEY
 ip nhrp map multicast 172.16.0.1
 ip nhrp map 24.1.1.1 172.16.0.1
 ip nhrp network-id 1
 ip nhrp holdtime 120
 ip nhrp nhs 24.1.1.1
 ip nhrp registration timeout 30
 ip nhrp shortcut
 tunnel source GigabitEthernet0/9
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN-PROFILE
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface GigabitEthernet0/3
 no ip address
!
interface GigabitEthernet0/4
 no ip address
!
interface GigabitEthernet0/5
 no ip address
!
interface GigabitEthernet0/6
 no ip address
!
```

```
interface GigabitEthernet0/7
 no ip address
!
interface GigabitEthernet0/8
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/9
 ip address 172.15.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 ip address 190.160.10.111 255.255.255.0
!
!
router eigrp 20
 network 2.2.2.0 0.0.0.255
 network 24.1.1.0 0.0.0.255
!
!
router eigrp 10
 network 172.15.0.0 0.0.0.255
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.4.0 255.255.255.0 100.100.100.2
ip route 192.168.5.0 255.255.255.0 100.100.100.2
!
access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 102 permit ip 100.100.100.0 0.0.0.255 200.200.200.0 0.0.0.255
!
control-plane
!
!
line con 0
 no modem enable
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

次の設定セクションは、2900 シリーズ ISR をハブとして設定する部分を示します。

2901_hub# **show running-config**

```
Building configuration...

Current configuration : 3210 bytes
!
! Last configuration change at 7:34:35 UTC Tue Jun 24 2014
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2901_hub
!
boot-start-marker
boot-end-marker
!
!
logging buffered 10000000
!
no aaa new-model
!
ip cef
!
!
no ipv6 cef
!
multilink bundle-name authenticated
!
license udi pid CISCO2901/K9 sn FGL180322RF
license boot module c2900 technology-package securityk9
!
!
!
redundancy
!

lldp run
!
!
crypto isakmp policy 1
 encr aes
 hash sha256
 authentication pre-share
 group 2
crypto isakmp key ISA_KEY address 0.0.0.0
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec transform-set DMVPN-TRANS-SET esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile DMVPN-PROFILE
 set security-association lifetime seconds 120
 set transform-set DMVPN-TRANS-SET
!
!

interface Loopback0
 ip address 1.1.1.1 255.255.255.255
 ip ospf message-digest-key 1 md5 cisco
!
```

```
interface Loopback1
 ip address 12.12.12.2 255.255.255.255
!
interface Loopback2
 ip address 12.12.12.3 255.255.255.255
!
interface Loopback3
 ip address 12.12.12.4 255.255.255.255
!
interface Loopback4
 ip address 12.12.12.5 255.255.255.255
!
interface Tunnel0
 ip address 24.1.1.1 255.255.255.0
 no ip redirects
 ip mtu 1440
 no ip split-horizon eigrp 10
 ip nhrp authentication ISA_KEY
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp shortcut
 ip nhrp redirect
 ip summary-address eigrp 20 192.168.0.0 255.255.0.0
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN-PROFILE
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.5.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 ip ospf message-digest-key 1 md5 cisco
 ip ospf priority 10
 duplex auto
 speed auto
!
interface GigabitEthernet0/1/0
 switchport access vlan 2
 no ip address
 shutdown
!
interface GigabitEthernet0/1/1
 switchport access vlan 10
 no ip address
!
interface GigabitEthernet0/1/2
 switchport access vlan 10
 no ip address
!
interface GigabitEthernet0/1/3
 switchport access vlan 20
 no ip address
!
interface GigabitEthernet0/1/4
 no ip address
!
```

```
interface GigabitEthernet0/1/5
 switchport access vlan 10
 no ip address
!
interface GigabitEthernet0/1/6
 no ip address
!
interface GigabitEthernet0/1/7
 no ip address
!
interface Vlan1
 no ip address
!
!
router eigrp 10
 network 172.16.0.0 0.0.0.255
!
!
router eigrp 20
 network 1.1.1.0 0.0.0.255
 network 24.1.1.0 0.0.0.255
 network 192.168.5.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 100.100.100.0 255.255.255.0 150.150.150.2
ip route 192.168.3.0 255.255.255.0 150.150.150.2
ip route 192.168.4.0 255.255.255.0 150.150.150.2
ip route 200.200.200.0 255.255.255.0 150.150.150.2
!
!

control-plane
!

line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Group Encrypted Transport VPN の設定

Group Encrypted Transport VPN（GETVPN）は、ネイティブ モードでネットワーク トラフィックにエンドツーエンド セキュリティを提供し、メッシュ トポロジを維持するトンネルレス VPN テクノロジーです。GET VPN では、キー プロトコル Group Domain of Interpretation（GDOI; グループ ドメイン オブ インタープリテーション）と IPsec 暗号化を組み合わせ、IP マルチキャスト トラフィックまたはユニキャスト トラフィックを保護するための効率的な方法をユーザに提供します。GET VPN では、ルータによって、トンネルレス（ネイティブ）IP マルチキャストおよびユニキャスト パケットに対して暗号化を適用できるので、マルチキャストおよびユニキャスト トラフィックを保護するためにトンネルを設定する必要がありません。

ポイントツーポイント トンネルが不要になるため、QoS、ルーティング、およびマルチキャストなどの音声およびビデオ品質にとって重要なネットワーク インテリジェンス機能を維持しながら、メッシュ ネットワークをより大規模に設定できます。GET VPN では、「信頼できる」グループ メンバーというコンセプトを基にした、新しい標準ベースの IP Security（IPsec）モデルが用意されています。信頼できるメンバーのルータでは、ポイントツーポイント IPsec トンネル関係とは独立した共通のセキュリティ方式が使用されます。

GETVPN 導入には、キー サーバ（KS）、グループ メンバ（GM）、およびグループドメイン オブ インタープリテーション（GDOI）プロトコルという、3 つの主要コンポーネントがあります。GM はトラフィックを暗号化または復号化し、KS はすべてのグループ メンバに暗号キーを配布します。KS は、ある一定期間において 1 つだけのデータ暗号化キーを決定します。すべての GM が同じキーを使用するため、どの GM も他のすべての GM によって暗号化されたトラフィックを復号化することができます。GDOI プロトコルは、GM と KS の間でグループ キーおよびグループの SA 管理に使用されます。GETVPN を展開するには、最小 1 つの KS が必要です。

従来の IPSec 暗号化ソリューションとは異なり、GET VPN ではグループ SA の概念が使用されます。GETVPN グループ内のすべてのメンバは、共通の暗号化ポリシーと共有 SA を使用して互いに通信することができます。したがって、GM 間でピアツーピア ベースの IPSec のネゴシエーションを行う必要はなく、これによって GM ルータにかかるリソースの負荷が軽減されます。

GETVPN 導入設定の例については、「例：GETVPN の設定」67 ページを参照してください。

GET VPN の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn-15-mt-book/sec-get-vpn.html

例：GETVPN の設定

次に、GETVPN 導入の設定例を示します。この例では、Cisco 800M J シリーズ ISR が GM として設定され、Cisco 1900 シリーズ ISR が KS として設定されます。

次の設定セクションは、800M J シリーズ ISR を GM として設定する部分を示します。

800M_GM# **show running-config**

```
Building configuration...

Current configuration : 1752 bytes
!
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 800M_GM
```

```
!
boot-start-marker
boot-end-marker
!

no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
cts logging verbose
license udi pid C841M-8X/K9 sn FOC18170PNJ
license accept end user agreement
license boot module c800m level advipservices
!
redundancy
!
crypto isakmp policy 100
 encr aes
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 192.168.1.2
!
crypto gdoi group gdoi
 identity number 1234
 server address ipv4 192.168.1.2

!
crypto map crypto 10 gdoi
 set group gdoi
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface GigabitEthernet0/3
 no ip address
!
interface GigabitEthernet0/4
 no ip address
!
interface GigabitEthernet0/5
 no ip address
!
interface GigabitEthernet0/6
 no ip address
!
interface GigabitEthernet0/7
 no ip address
!
interface GigabitEthernet0/8
 ip address 10.1.3.1 255.255.255.0
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/9
 ip address 192.168.3.2 255.255.255.0
 duplex auto
 speed auto
 crypto map crypto
!
interface Vlan1
 no ip address
!
!
router eigrp 1
 network 10.1.3.0 0.0.0.255
 network 192.168.3.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
control-plane
!
line con 0
 no modem enable
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```

次の設定セクションは、Cisco 1900 シリーズ ISR を KS として設定する部分を示します。

1921_KS# **show running-config**

```
Building configuration...
Current configuration : 2019 bytes
!
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 1921_KS
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!

!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!

license udi pid CISCO1921/K9 sn FGL155022DY
license boot module c1900 technology-package securityk9
```

```
license boot module c1900 technology-package datak9
!
!
!
redundancy
!
crypto isakmp policy 100
 encr aes
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key cisco address 0.0.0.0
!

crypto ipsec transform-set trans esp-aes esp-sha-hmac
 mode tunnel
!
!
crypto ipsec profile ipsec
 set transform-set trans
!
crypto gdoi group gdoi
 identity number 1234
 server local
  rekey algorithm aes 256
  rekey lifetime seconds 3600
  rekey authentication mypubkey rsa vpnkeys
  rekey transport unicast
  sa ipsec 10
   profile ipsec
   match address ipv4 getvpn
   replay counter window-size 64
   no tag
  address ipv4 192.168.1.2
!
!
crypto map crypto 10 gdoi
 set group gdoi
!

interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map crypto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
```

```
!

router eigrp 1
 network 192.168.1.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

ip access-list extended getvpn
 permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
!

control-plane
!

line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

SSL VPN の設定

セキュア ソケット レイヤ バーチャル プライベート ネットワーク（SSL VPN）機能を使用すると、リモート ユーザは、どのような場所にいても、インターネット上からエンタープライズ ネットワークにアクセスできるようになります。リモート アクセスは、SSL 対応の SSL VPN ゲートウェイを介して提供されています。SSL VPN ゲートウェイによりリモート ユーザは、Web ブラウザを使用してセキュアな VPN トンネルを確立できます。この機能は、ネイティブ HTTP over SSL（HTTPS）ブラウザ サポートを使用して、幅広い Web リソースおよび Web 対応アプリケーションに簡単にアクセスできる包括的なソリューションを実現します。SSL VPN は、クライアントレス、シンクライアント、フル トンネル クライアント サポートの 3 種類の SSL VPN アクセス モードを提供します。

SSL VPN ゲートウェイの設定例については、「例：SSL VPN の設定」の項を参照してください。

SSL VPN の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-mt/sec-conn-sslvpn-15-mt-book/sec-conn-sslvpn-ssl-vpn.html

例：SSL VPN の設定

次に、Cisco 800M J シリーズ ISR を使用した SSL VPN ゲートウェイの設定の例を示します。

800M# **show running-config**

```
Building configuration...

Current configuration : 4053 bytes
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 800M
!
boot-start-marker
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login ciscocp_vpn_xauth_ml_1 local
!
!

aaa session-id commont
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
!
crypto pki trustpoint TP-self-signed-2716339910
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2716339910
 revocation-check none
 rsakeypair TP-self-signed-2716339910
!
!
crypto pki certificate chain TP-self-signed-2716339910
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32373136 33333939 3130301E 170D3134 31313132 31313430
  35355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 37313633
  33393931 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100A775 D34D41D6 281317C5 427BBC6D 3D97F5B4 F91E924B AB23F5CC F92336E6
  29EBDC57 45A455B7 D7300C0C 07C5DDF8 62E2BDFB CDEB57CC EFAE7006 A72D4C20
  2D9995E7 472D2C4E 079828B3 B63DDB66 A9D3D77F BC844CBD 255D81F0 84564748
  4FAD69E1 94F5AFC9 0450EFDC 9096BD38 3F4FA022 0680E969 174197EA 3F85DD4C
  B1490203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 145602C5 80924574 A895C527 F177A81B 4EA03C94 EA301D06
  03551D0E 04160414 5602C580 924574A8 95C527F1 77A81B4E A03C94EA 300D0609
  2A864886 F70D0101 05050003 81810090 823846F0 FAA084FB F5C17F04 00E11E54
  D9D9B32A 4EBB96D4 8414C5DD 0DB8728B 84518031 0B22A20A 989C341C 4AB15B7B
  B192E99B E29138E9 56263016 5565DEAA 9CE9E40B D945EF2C 1BFE110C 4622F707
  39E7FA48 DA3B15DD CA66AA8F 61783562 7C09932F BD4E5AB4 A1242A71 90E27B22
  71CD3A0D A0004521 D1DB1E2C D95BEF
        quit
!

ip cef
```

```
no ipv6 cef
!
!
multilink bundle-name authenticated
!
cts logging verbose
license udi pid C841M-8X/K9 sn FCW1842005Y
!
!
username cisco privilege 15 password 0 cisco
!
redundancy
!
crypto vpn anyconnect sdflash:/webvpn/anyconnect-win-3.1.03103-k9.pkg sequence 1


!
interface Loopback10
 ip address 100.100.100.100 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface GigabitEthernet0/3
 no ip address
!
interface GigabitEthernet0/4
 no ip address
!
interface GigabitEthernet0/5
 no ip address
!
interface GigabitEthernet0/6
 no ip address
!
interface GigabitEthernet0/7
 no ip address
!
interface GigabitEthernet0/8
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/9
 ip address 9.43.17.81 255.255.0.0
 duplex auto
 speed auto
!
interface Virtual-Template1
 ip unnumbered GigabitEthernet0/8
 ip virtual-reassembly in
!
interface Vlan1
 no ip address
!
ip local pool IP_Pool 10.10.10.1 10.10.10.10
ip forward-protocol nd
no ip http server
```

```
no ip http secure-server
!
!
ip route 202.153.144.0 255.255.255.0 9.43.0.1
!

control-plane
!

line con 0
 no modem enable
line vty 0 4
 transport input none
!
scheduler allocate 20000 1000
!

webvpn gateway gateway_1
 ip address 192.168.10.1 port 443
 ssl trustpoint TP-self-signed-2716339910
 inservice
 !
webvpn context Test
 secondary-color white
 title-color #FF9900
 text-color black
 virtual-template 1
 aaa authentication list ciscocp_vpn_xauth_ml_1
 gateway gateway_1
 !
 ssl authenticate verify all
 inservice
 !
 policy group policy_1
   functions svc-enabled
   svc address-pool "IP_Pool" netmask 255.255.255.255
   svc default-domain "cisco.com"
   svc keep-client-installed
   svc rekey time 240
   svc dns-server primary 10.105.130.1
   svc wins-server primary 10.105.130.1
 default-group-policy policy_1
!
end
```

FlexVPN の設定

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイト間アクセス、リモート アクセス、ハブ アンド スポーク トポロジ、および部分メッシュ（スポーク間ダイレクト）を組み合わせたユニファイド パラダイムと CLI を備えています。FlexVPN は、トンネル インターフェイス パラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

FlexVPN ハブ アンド スポーク設定の例については、「例：FlexVPN の設定」の項を参照してください。

FlexVPN の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-flex-vpn-15-mt-book/sec-intro-ikev2-flex.html

例：FlexVPN の設定

次に、FlexVPN ハブ アンド スポーク導入モデルの設定例を示します。この例では、Cisco 800M J シリーズ ISR がスポークとして設定され、Cisco 3900 シリーズ ISR がハブとして設定されます。

次の設定セクションは、800M J シリーズ ISR をスポークとして設定する部分を示します。

800M# **show running-config**

```
Building configuration...

Current configuration : 2461 bytes
!
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 800M
!
boot-start-marker
boot-end-marker
!

aaa new-model
!
!
aaa authorization network FLEX local
!

aaa session-id common
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2

!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
chat-script multimode "" "AT!CALL" TIMEOUT 20 "OK"
cts logging verbose
license udi pid C841M-4X/K9 sn FCW1839001E
!

redundancy
!
crypto ikev2 authorization policy FLEX
 route set interface
!
!
!
crypto ikev2 keyring KEYRING
 peer R1
  address 172.16.0.1
  pre-shared-key CISCO
 !
!
!
crypto ikev2 profile default
 match identity remote address 172.16.0.1 255.255.255.255
 identity local key-id FLEX
```

```
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list FLEX FLEX
!
!
!

!
interface Loopback0
 ip address 2.2.2.2 255.255.255.0
!
interface Tunnel0
 ip address negotiated
 tunnel source GigabitEthernet0/5
 tunnel mode ipsec ipv4
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/1
 no ip address
!
interface GigabitEthernet0/2
 no ip address
!
interface GigabitEthernet0/3
 no ip address
!
interface GigabitEthernet0/4
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/5
 ip address 172.16.0.2 255.255.255.0
 duplex auto
 speed auto
!


interface Vlan1
 no ip address
!
!
router eigrp 1
 network 0.0.0.0
 passive-interface default
 no passive-interface Tunnel0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!

control-plane
!

line con 0
 no modem enable
line 2
```

```
 no activation-character
 no exec
 transport preferred none
 transport input all
 stopbits 1
line 3
 script dialer multimode
 no exec
line vty 0 4
 transport input none
!
scheduler allocate 20000 1000
!
end
```

次の設定セクションは、800M J シリーズ ISR をスポークとして設定する部分を示します。

C3900# **show running-config**

```
Building configuration...

Current configuration : 2690 bytes
!
! Last configuration change at 13:10:19 UTC Fri Oct 31 2014
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3900
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
!
aaa new-model
!
!
aaa authorization network LOCALIKEv2 local

!
!
aaa session-id common

!
!
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!

!
voice-card 0
!

!
license udi pid C3900-SPE200/K9 sn FOC16075NAN
license accept end user agreement
license boot module c3900e technology-package securityk9
```

```
license boot module c3900e technology-package datak9
!
!
!
redundancy
!
crypto ikev2 authorization policy AUTHOR-POLICY
 pool POOL
!
!
!
crypto ikev2 keyring KEYRING
 peer R2
  address 172.16.0.2
  pre-shared-key CISCO
 !
!
!
crypto ikev2 profile default
 match identity remote key-id FLEX
 authentication remote pre-share
 authentication local pre-share
 keyring local KEYRING
 aaa authorization group psk list LOCALIKEv2 AUTHOR-POLICY
 virtual-template 1

!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/3
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
 no ip address
!
interface FastEthernet0/1/1
 no ip address
!
interface FastEthernet0/1/2
 no ip address
!
interface FastEthernet0/1/3
 no ip address
```

```
!
interface FastEthernet0/1/4
 no ip address
!
interface FastEthernet0/1/5
 no ip address
!
interface FastEthernet0/1/6
 no ip address
!
interface FastEthernet0/1/7
 no ip address
!
interface FastEthernet0/1/8
 no ip address
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel source GigabitEthernet0/1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
!
interface Vlan1
 no ip address
!
!
!
router eigrp 1
 network 1.1.1.1 0.0.0.0
 passive-interface default
 no passive-interface Virtual-Template1
!
ip local pool POOL 192.168.0.1 192.168.0.10
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
nls resp-timeout 1
cpd cr-id 1
!
!
!
!
control-plane
!
 !

mgcp behavior rsip-range tgcp-only
mgcp behavior comedia-role none
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!

gatekeeper
 shutdown
!
!
!
line con 0
```

```
line aux 0
line vty 0 4
 transport input all
!
scheduler allocate 20000 1000
!
end
```

ゾーンベース ポリシー ファイアウォールの設定

ゾーンベース ポリシー ファイアウォール（別名ゾーンポリシー ファイアウォールまたは ZFW）は、インターフェイス ベース モデルのファイアウォール設定を、柔軟性が高く容易に理解できるゾーンベース モデルに変更します。インターフェイスがゾーンに割り当てられ、ゾーン間を移動するトラフィックに検査ポリシーが適用されます。ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。

ゾーンベース ポリシー ファイアウォールの設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html

VRF-Aware Cisco ファイアウォールの設定

サービス プロバイダー（SP）または大企業のエッジ デバイスで VRF-Aware Cisco ファイアウォールが設定されている場合、Cisco ファイアウォール機能が Virtual Routing and Forwarding（VRF）インターフェイスに適用されます。SP は中小企業の市場向けにマネージド サービスを提供することができます。

VRF-Aware Cisco ファイアウォールの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-cbac-vrf-fw.html

サブスクリプションベースの Cisco IOS コンテンツ フィルタリングの設定

サブスクリプションベースの Cisco IOS コンテンツ フィルタリング機能は、Trend Micro の URL フィルタリング サービスと共に動作します。これにより、コンテンツ フィルタリング ポリシーに基づいて HTTP 要求を許可またはブロックし、ログに記録することができます。コンテンツ フィルタリング ポリシーは、Web カテゴリ、レピュテーション（またはセキュリティ レーティング）、信頼ドメイン、信頼できないドメイン、キーワードなどの項目を処理する方法を指定します。URL がルータでキャッシュされるため、同じ URL に対する後続の要求では、ルックアップ要求を必要とせず、パフォーマンスが向上します。

サブスクリプションベースの Cisco IOS コンテンツ フィルタリングの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/subscrip-cont-filter.html

On-Device Management for Security Features の設定

On-Device Management for Security Features は、さまざまなセキュリティ機能を導入するための直感的でシンプルな管理インターフェイスである Cisco Configuration Professional Express を提供します。Cisco Configuration Professional Express を使用して、ゾーンベースのファイアウォール、VPN、侵入検知システム（IDS）、URL フィルタリングといったセキュリティ機能を導入できます。

Cisco Configuration Professional Express では、既存のゾーンベース ファイアウォール CLI と Network-Based Application Recognition 2（NBAR2）CLI を組み合わせて使用して、アプリケーション カテゴリを判別し、ファイアウォールによってサポートされている NBAR2 プロトコルを該当するアプリケーション カテゴリに位置付けます。

ゾーンベースのファイアウォールでの NBAR2 のイネーブルに関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/on-device-mgmt.html

関連資料

トピック	マニュアル タイトル
DMVPN	Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T
GETVPN	Cisco Group Encrypted Transport VPN Configuration Guide, Cisco IOS Release 15M&T
SSL VPN	SSL VPN Configuration Guide, Cisco IOS Release 15M&T
FlexVPN	FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T
IPSec VPN 向け IKE	Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS Release 15M&T

QoS の設定

この章では、Cisco 800M J シリーズ ISR での Quality of Service（QoS）の設定について説明します。具体的な内容は、次のとおりです。

- 「クラスベース重み付け均等化キューイングの設定」83 ページ
- 「低遅延キューイングの設定」84 ページ
- 「クラスベース トラフィック シェーピングの設定」85 ページ
- 「クラスベース トラフィック ポリシングの設定」85 ページ
- 「クラスベース重み付けランダム早期検出の設定」86 ページ
- 「QoS 階層型キューイング フレームワークの設定」87 ページ
- 「Network-Based Application Recognition の設定」87 ページ
- 「Resource Reservation Protocol の設定」87 ページ
- 「VPN 用 Quality of Service の設定」88 ページ
- 「DMVPN の Per-Tunnel QoS の設定」88 ページ
- 「レイヤ 2 自動 QoS の設定」89 ページ

クラスベース重み付け均等化キューイングの設定

クラスベース重み付け均等化キューイング（CBWFQ）は、ユーザ定義のトラフィック クラスの輻輳管理サポートを提供します。CBWFQ では、プロトコル、アクセス コントロール リスト（ACL）、および入力インターフェイスなどの一致基準を基にトラフィック クラスを定義します。クラスの一致基準を満たすパケットは、そのクラスのトラフィックの一部となります。FIFO キューはそれぞれのクラスで予約され、クラスに属するトラフィックはそのクラスのキューに誘導されます。

クラスが一致基準によって定義されると、それに特性を割り当てることができます。クラスに特性を持たせるには、帯域幅、重み、最大パケット制限を割り当てます。クラスに割り当てられた帯域幅は、輻輳中のクラスに適用する保証帯域幅です。

CBWFQ の設定の詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-mt/qos-conmgt-15-mt-book/qos-conmgt-cfg-wfq.html

例：クラスベース重み付け均等化キューイング

次の例では、2 つのクラス マップが作成され、その一致基準が定義されます。1 つめの class1 という名前のクラス マップでは、一致基準として番号付きの ACL 101 が使用されます。2 つめの class2 という名前のマップクラスでは、一致基準として番号付きの ACL 102 が使用されます。パケットはこれらの ACL の内容と照合され、そのクラスに属するかどうかが判断されます。

```
Router# configure terminal
Router(config)# access-list 101 permit udp host 10.10.10.10 host 10.10.10.20 range 16384
20000
Router(config# access-list 102 permit udp host 10.10.10.10 host 10.10.10.20 range 53000
56000
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config-cmap)# class-map class2
Router(config-cmap)# match access-group 102
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# queue-limit 30
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 2000
Router(config)# interface gigabitethernet 0/4
Router(config-if)# service output policy1
Router(config-if)# exit
```

低遅延キューイングの設定

完全プライオリティ キューイングでは、音声などの遅延に影響されやすいデータを、他のキューのパケットをキューから取り出す前にキューから取り出して送信できます。低遅延キューイング（LLQ）は、CBWFQ で完全プライオリティ キューイングを実現し、音声通話パケットでのジッタを減らします。LLQ は CBWFQ 内の単一の、完全プライオリティ キューをクラス レベルでイネーブルにし、クラスに属するトラフィックを CBWFQ 完全プライオリティ キューに誘導できます。クラス トラフィックを完全プライオリティ キューに入力するには、ポリシー マップの名前が付いたクラスを指定し、priority コマンドをクラスに設定します ポリシー マップ内で、1 つ以上のクラスにプライオリティ ステータスを設定できます。1 つのポリシー マップに複数のクラスがプライオリティ クラスとして設定されている場合、これらのクラスからのトラフィックはすべて、同じ単一の完全プライオリティ キューに入力されます。

低遅延キューイングの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-mt/qos-conmgt-15-mt-book/qos-conmgt-cfg-wfq.html

例：低遅延キューイング

```
Router# configure terminal
Router(config)# class-map voice
Router(config-cmap)# match access-group 102
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

```
Router(config-pmap)# class bar
Router(config-pmap-c)# bandwidth 20
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config)# interface gigabitethernet 0/0
Router(config-if)# service-policy output policy1
Router(config-if)# exit
```

クラスベース トラフィック シェーピングの設定

トラフィック シェーピングでは、インターフェイスから出力されるトラフィックを制御して、リモート ターゲット インターフェイスの速度にフローを合わせ、指定されているポリシーにトラフィックを準拠させることができます。このように、ダウンストリーム要件を満たすように、特定のプロファイルに適合するトラフィックをシェーピングできるため、データレートが一致しないトポロジで発生するボトルネックが排除されます。

クラスベース トラフィック シェーピングに関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfcbshp.html

例：クラスベース トラフィック シェーピング

次に、通常バースト サイズ 15440 ビットでトラフィックを 384 kbps にシェーピングするように設定されたクラス c1 の定義例を示します。

```
Router# configure terminal

Router(config)# policy-map shape
Router(config-pmap)# class c1
Router(config-pmap-c)# shape average 384000 15440
Router(config-pmap-c)# end
Router(config)# interface gigabitethernet 0/0
Router(config-if)# service out shape
```

クラスベース トラフィック ポリシングの設定

クラスベース トラフィック ポリシングを使用すると、インターフェイスでのトラフィックの最大送受信レートを制御できます。クラスベース トラフィック ポリシングは、多くの場合、ネットワークのエッジにあるインターフェイスで設定され、ネットワークを出入りするトラフィックを制限します。ほとんどのクラスベース ポリシング設定では、レート パラメータ内に収まるトラフィックは送信されますが、パラメータを超えるトラフィックはドロップされるか、異なる優先度で送信されます。

クラスベース トラフィック ポリシングの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-class-plc.html

例：クラスベース トラフィック ポリシング

次の例では、クラスベース トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ギガビット イーサネット インターフェイス 0/4 から発信される全パケットに対して通常バースト サイズが 1000 バイトとなります。

```
Router# configure terminal
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# violate-action drop
Router(config)# interface gigabitethernet 0/4
Router(config-if)# service-policy output policy-setting
Router(config-if)# exit
```

クラスベース重み付けランダム早期検出の設定

重み付けランダム早期検出（WRED）は、ランダム早期検出（RED）アルゴリズムの機能を IP プレシデンス機能と統合して、優先順位の高いパケットの優先的なトラフィック処理を実現します。WRED では、インターフェイスで輻輳が発生し始めると、優先順位が低いトラフィックを選択的に廃棄し、異なるサービス クラスに対して差別化したパフォーマンス特性を提供できます。

重み付けされていない RED の動作が行われるように、ドロップの決定を行う際に IP プレシデンスを無視するよう WRED を設定できます。WRED により輻輳の早期検出が可能になります。WRED は複数のトラフィック クラスを対象としています。また、グローバル同期に対して保護されます。そのため、WRED は輻輳が発生すると予測されるいずれの出力インターフェイスでも有用です。

WRED の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conavd/configuration/15-mt/qos-conavd-15-mt-book/qos-conavd-cfg-wred.html

例：クラスベース重み付けランダム早期検出

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-if)# service-policy output p1
```

QoS 階層型キューイング フレームワークの設定

QoS 階層型キューイング フレームワーク（HQF）機能を使用すると、Quality of Service（QoS）を 3 つのレベル（QoS キューイングおよびシェーピング メカニズムの物理インターフェイス レベル、論理インターフェイス レベル、クラス レベル）で管理できます。これは、モジュラ QoS コマンドライン インターフェイス（MQC）を使用して、よりきめ細かく柔軟な包括的 QoS アーキテクチャを得ることにより行われます。

階層型キューイング フレームワークの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_hrhqf/configuration/15-mt/qos-hrhqf-15-mt-book/qos-hrhqf.html

Network-Based Application Recognition の設定

Network-Based Application Recognition（NBAR）は、多様なプロトコルとアプリケーションを認識および分類する分類エンジンです。プロトコルまたはアプリケーションが NBAR に認識および分類されると、そのアプリケーションまたはそのプロトコルによるトラフィックに適した Quality of Service（QoS）を適用するようにネットワークを設定できるようになります。

NBAR の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/15-mt/qos-nbar-15-mt-book.html

例：Network Based Application Recognition

```
Router# configure terminal
Router(config)# class-map cmap1
Router(config-cmap)# match protocol citrix
Router(config-cmap)# end
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 50
Device(config-pmap-c)# end
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/4
Device(config-if)# service-policy input policy1
Device(config-if)# end
```

Resource Reservation Protocol の設定

Resource Reservation Protocol（RSVP）は、異種ネットワーク上でエンドツーエンド QoS を動的にセットアップする業界標準プロトコルです。IP 上で動作する RSVP を使用すれば、アプリケーションでネットワーク帯域を動的に予約できます。また、RSVP を使用すれば、アプリケーションで、ネットワーク上のデータ フローに対して一定レベルの QoS を要求できます。

Cisco IOS QoS 実装を使用すれば、設定されたプロキシ RSVP を使用して RSVP をネットワーク内で開始できます。この機能を使用すれば、RSVP に対応していないアプリケーションとホストからなるネットワークでも RSVP の利点を享受できます。RSVP は、IP ネットワークでエンドツーエンドでネットワーク帯域幅を保証するように設計されています。

RSVP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_rsvp/configuration/15-mt/qos-rsvp-15-mt-book/config-rsvp.html

VPN 用 Quality of Service の設定

VPN 用 QoS 機能には、インターフェイス上で Cisco IOS QoS サービスがトンネリングおよび暗号化と連携して動作するためのソリューションが用意されています。Cisco IOS ソフトウェアでパケットを分類し、適切な QoS サービスを適用してから、データを暗号化およびトンネリングできます。VPN 用 QoS 機能を使用すると、元のポート番号とソースおよび宛先 IP アドレスに基づいてパケットの分類を実行できるように、パケット内を確認できます。サービス プロバイダーはこの機能を使用して、ネットワーク内の重要なサービスまたはマルチサービスのトラフィックを高い優先度で処理できます。

VPN 用 QoS の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_classn/configuration/15-mt/qos-classn-15-mt-book/qos-classn-vpn.html

DMVPN の Per-Tunnel QoS の設定

Dynamic Multipoint VPN（DMVPN）の Per-Tunnel QoS 機能を使用すると、トンネル別インスタンス（スポーク別ベース）で DMVPN ハブからスポークへのトンネルの出力方向で、DMVPN ハブに Quality of Service（QoS）ポリシーを適用できます。トンネル別インスタンスの DMVPN ハブに対する QoS ポリシーにより、各スポークにトンネル トラフィックをシェーピングし（親ポリシー）、ポリシングのためにトンネルを通る個別のデータ フローを区別（子ポリシー）できます。特定のスポークにハブが使用する QoS ポリシーは、そのスポークが設定されている特定の NHRP（Next Hop Resolution Protocol）グループに基づいて選択されます。同じ NHRP グループに複数のスポークを設定できますが、各スポークのトンネル トラフィックは個別に測定されてシェーピングおよびポリシングされます。Internet Protocol Security（IPSec）の有無に関係なく、DMVPN にこの機能を使用できます。

DMVPN の Per-Tunnel QoS の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-per-tunnel-qos.html

レイヤ 2 自動 QoS の設定

自動 QoS 機能を使用して、QoS 機能の配置を容易にできます。自動 QoS は、ネットワーク設計を確認し、ルータがさまざまなトラフィック フローに優先度を指定できるように QoS 設定をイネーブルにします。自動 QoS は、デフォルト（ディセーブル）の QoS 動作を使用せずに、入力および出力キューを使用します。スイッチはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供し、単一キューからパケットを送信します。

自動 QoS をイネーブルにすると、トラフィック タイプおよび入力パケット ラベルに基づいてトラフィックを自動的に分類します。スイッチは分類した結果を使用して適切な出力キューを選択します。

自動 QoS の設定に関する詳細については、次のリンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swqos.html#wp1231112

ネットワーク管理機能の設定

この章では、Cisco 800M J シリーズ ISR のネットワーク管理機能の設定について説明します。具体的な内容は、次のとおりです。

- 「Cisco Configuration Professional」91 ページ
- 「Cisco Configuration Professional Express」92 ページ
- 「Cisco Prime Infrastructure」92 ページ
- 「Embedded Event Manager」92 ページ
- 「IP SLA の設定」93 ページ
- 「RADIUS の設定」93 ページ
- 「TACACS+ の設定」93 ページ
- 「SSH の設定」94 ページ
- 「SNMP の設定」94 ページ
- 「NetFlow の設定」94 ページ
- 「Flexible NetFlow の設定」95 ページ
- 「MIB のサポート」95 ページ

Cisco Configuration Professional

Cisco Configuration Professional は、シスコ アクセス ルータを対象とした GUI ベースのデバイス管理ツールです。このツールでは、ルーティング、ファイアウォール、IPS、VPN、ユニファイド コミュニケーション、および WAN/LAN を GUI ベースのウィザードで簡単に設定できます。Cisco CP は、ネットワーク管理者とチャネル パートナーが確実に、かつより簡単にルータを展開できる、生産性向上のために有益なツールです。ワンクリックでルータをロックすることができ、音声およびセキュリティ監査機能ではルータの設定の確認と推奨される変更を提示します。また、ルータの状態の監視と、WAN および VPN の接続のトラブルシューティングも行われます。

Cisco Configuration Professional を使用した Cisco 800M J シリーズ ISR の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/cisco_configuration_professional/v2_5/olh/ccp.pdf

Cisco Configuration Professional Express

Cisco Configuration Professional Express（Cisco CP Express）は、Cisco Configuration Professional の簡易バージョンであり、ブートストラップと、Cisco サービス統合型ルータ（ISR）をプロビジョニングすることができる組み込みのデバイス管理ツールです。Cisco CP Express を使用して、完全な WAN および LAN コンフィギュレーションとセキュリティ機能を備えたネットワークをセットアップできます。

Cisco CP Express を使用した Cisco 800M J シリーズ ISR の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_configuration_professional_express/v3_1/guides/featureguide/ccp_express_Feature_Guide.html

Cisco Prime Infrastructure

Cisco Prime Infrastructure は、1 つのグラフィカル インターフェイスからネットワーク インフラストラクチャ全体のライフサイクルを管理できる、ネットワーク管理ツールです。Prime Infrastructure は、ネットワーク管理者に、有線デバイスとワイヤレス デバイス両方のプロビジョニング、モニタリング、最適化、トラブルシューティングを行うための単一ソリューションを提供します。堅牢なグラフィカル インターフェイスを使用することで、デバイスの導入と操作を簡略化し、コスト効率を上げることができます。

Cisco Prime Infrastructure を使用した Cisco 800M J シリーズ ISR の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-1/user/guide/pi_ug.html

Embedded Event Manager

Embedded Event Manager（EEM）は、イベント検出と回復を Cisco IOS 内部で直接行うための分散型でカスタマイズされた手法です。EEM はイベントをモニタし、モニタ対象イベントが発生したり、しきい値に達したりすると、情報取得や対処などの必要な EEM 処理を実行します。EEM ポリシーは、イベントおよびイベントが発生した場合に行う処理を定義するエンティティです。

Embedded Event Manager の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/15-mt/eem-15-mt-book.html

IP SLA の設定

IP Service Level Agreements（IP SLA）により、シスコのお客様は IP アプリケーションとサービスの IP サービス レベルを分析するとともに、生産性の向上、運用コストの削減、ネットワーク停止頻度の低減を実現できます。IP SLA は、アクティブ トラフィック モニタリングを使用します。これにより、継続的で信頼性のある予測可能な方法でトラフィックが生成され、ネットワーク パフォーマンスを測定できます。IP SLA を使用すると、サービス プロバイダーのお客様は測定したうえでサービス レベル契約を提供することができ、企業のお客様はサービス レベルや外部委託しているサービス レベル契約を検証したり、ネットワーク パフォーマンスを把握したりできます。IP SLA は、ネットワーク アセスメントを実行し、Quality of Service（QoS）を検証したり新規サービスの展開を簡易化するとともに、管理者によるネットワークのトラブルシューティングをサポートします。IP SLA によって取得されたデータは、コマンドラインまたは Simple Network Management Protocol（SNMP）による Cisco Round-Trip Time Monitor（RTTMON）や syslog Management Information Base（MIB）のポーリングを通じてアクセスできます。

IP SLA の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-class-plc.html

RADIUS の設定

RADIUS セキュリティ システムは、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバ システムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。

RADIUS の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/15-mt/sec-usr-rad-15-mt-book/sec-cfg-radius.html

TACACS+ の設定

TACACS+ は、ユーザによるデバイスまたはネットワーク アクセス サーバへのアクセス試行を中央から確認できるセキュリティ アプリケーションです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）を個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを提供できます。TACACS+ の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。

TACACS+ の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-mt/sec-usr-tacacs-15-mt-book/sec-cfg-tacacs.html

SSH の設定

セキュア シェル（SSH）は信頼性の高いトランスポート層で実行され、強力な認証および暗号機能を提供します。SSH により、ネットワーク上の他のコンピュータへのアクセスとコマンドの実行を安全に行うことができます。

SSH の設定の詳細については、次の Web リンクを参照してください:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book/sec-usr-ssh-sec-shell.html

SNMP の設定

簡易ネットワーク管理プロトコル（SNMP）は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。SNMP はネットワーク デバイスのモニタリングや管理に使用される標準化されたフレームワークと共通言語を提供します。

SNMP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-mt/snmp-15-mt-book/nm-snmp-cfg-snmp-support.html

NetFlow の設定

NetFlow は、ネットワーク内のルーティング装置を経由するパケットの統計情報を示す Cisco IOS アプリケーションであり、ネットワーク アカウンティングおよびセキュリティの新たな主要テクノロジーになりつつあります。

NetFlow では、入力と出力の両方の IP パケットに対してパケット フローが識別されます。ルータ間でも、他のネットワーキング デバイスまたは端末に対しても、接続確立のプロトコルは含まれません。NetFlow はいかなる外部（パケット自体やネットワーキング デバイス）の変更も必要としません。NetFlow は、既存のネットワーク（端末、アプリケーション ソフトウェア、LAN スイッチなどのネットワーク デバイスを含む）に対して完全に透過的です。また、NetFlow のキャプチャおよびエクスポートは、各インターネットワーキング デバイス上で独立して実行されます。したがって、NetFlow は、ネットワーク内の各ルータ上で動作可能である必要はありません。

NetFlow の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book.html

Flexible NetFlow の設定

Flexible NetFlow は、ルータを通過するパケットの統計情報が得られる Cisco IOS テクノロジーです。NetFlow は、IP ネットワークから実際の IP データを取得するための標準規格です。NetFlow は、ネットワークとセキュリティの監視、ネットワーク計画、トラフィック分析、および IP アカウンティングをイネーブルにするためのデータを提供します。

Flexible NetFlow は、実際の要件に合わせてトラフィック分析パラメータをカスタマイズする機能を追加することで、以前の NetFlow よりも改善されています。Flexible NetFlow では、トラフィック分析のための非常に複雑な構成を作成したり、再利用可能な構成コンポーネントを使用してデータをエクスポートすることが容易になります。

NetFlow の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/15-mt/nf-15-mt-book.html

MIB のサポート

Cisco 800M J シリーズ ISR は以下のMIBをサポートします。

- CISCO-PRODUCTS-MIB
- OLD-CISCO-CHASSIS-MIB
- ENTITY-MIB
- IF-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-LICENSE-MGMT-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB

IP アドレッシングおよび IP サービス機能の設定

この章では、Cisco 800M J シリーズ ISR での IP アドレッシングおよび IP サービス機能の設定について説明します。具体的な内容は、次のとおりです。

- 「DHCP の設定」97 ページ
- 「DNS の設定」98 ページ
- 「NAT の設定」98 ページ
- 「NHRP の設定」98 ページ
- 「BFD の設定」101 ページ
- 「RIP の設定」99 ページ
- 「BGP の設定」100 ページ
- 「OSPF の設定」99 ページ
- 「BGP の設定」100 ページ
- 「パフォーマンス ルーティング v3 の設定」100 ページ
- 「Multi-VRF の設定」101 ページ
- 「IPv6 機能の設定」101 ページ

DHCP の設定

Dynamic Host Configuration Protocol（DHCP）は、ブートストラップ プロトコル（BOOTP）に基づいています。DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。DHCP により、再利用可能なネットワーク アドレスおよび設定オプションをインターネット ホストに自動的に割り当てられるようになります。DHCP は 2 つのコンポーネントで構成されます。1 つはホスト固有の設定パラメータを DHCP サーバからホストに配信するためのプロトコルで、もう 1 つはホストにネットワーク アドレスを割り当てるためのメカニズムです。DHCP はクライアント/サーバ モデルに基づいています。指定された DHCP サーバ ホストが、ダイナミックに設定されるホストに対して、ネットワーク アドレスを割り当て、設定パラメータを提供します。DHCP は、TCP/IP ネットワーク上のホストに設定情報をダイナミックに渡すフレームワークを提供します。DHCP クライアントは、DHCP を使用して IP アドレスなどの設定パラメータを取得するインターネット ホストです。DHCP リレー エージェントは、クライアントとサーバ間で DHCP パケットを転送する任意のホストです。リレー エージェントは、同一の物理サブネット上にないクライアントとサーバ間で要求および応答を転送するために使用されます。

DHCP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-mt/dhcp-15-mt-book.html

DNS の設定

ドメイン ネーム システム（DNS）は、DNS サーバから DNS プロトコルを使用してホスト名を IP アドレスにマッピングできる分散データベースです。一意の各 IP アドレスにホスト名を関連付けることができます。Cisco IOS ソフトウェアは、connect、telnet、ping EXEC コマンド、および関連する Telnet サポート操作で使用するための hostname-to-address マッピングのキャッシュを保持します。このキャッシュにより、名前とアドレスの変換プロセスが高速化されます。

DNS の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/dns-15-mt-book/dns-config-dns.html

NAT の設定

ネットワーク アドレス変換（NAT）は、登録されていない IP アドレスを使用してインターネットへ接続するプライベート IP インターネットワークを可能にします。NAT はデバイス（通常、2 つのネットワークを接続するもの）で動作し、パケットを別のネットワークに転送する前に、社内ネットワークの（グローバルに一意のアドレスではなく）プライベート アドレスを正規のアドレスに変換します。NAT は、ネットワーク全体で 1 つだけのアドレスを外部にアドバタイズするように設定できます。この機能により内部ネットワーク全体はこの 1 つのアドレスの背後に効果的に隠されるので、セキュリティが強化されます。NAT はエンタープライズ エッジでも使用され、内部ユーザのインターネットへのアクセスを許可し、メール サーバなど内部デバイスへのインターネット アクセスを許可します。

NAT の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-addr-consv.html

NHRP の設定

Next Hop Resolution Protocol（NHRP）は、ノンブロードキャスト マルチアクセス（NBMA）ネットワークをダイナミックにマッピングする Address Resolution Protocol（ARP）と同様のプロトコルです。NHRP を使用すると、NBMA ネットワークに接続されたシステムは、そのネットワークに参加している他のシステムの NBMA（物理）アドレスをダイナミックに学習でき、これらのシステムが直接通信できるようになります。

NHRP は、ハブがネクスト ホップ サーバ（NHS）であり、スポークがネクスト ホップ クライアント（NHC）である、クライアントおよびサーバのプロトコルです。ハブには、各スポークのパブリック インターフェイス アドレスが格納された NHRP データベースが保持されます。各スポークでは、起動時にそれぞれの実際のアドレスが登録され、ダイレクト トンネルを確立する場合には、NHRP サーバに対し、宛先スポークの実際のアドレスに関する照会が行われます。

NHRP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-class-plc.html

RIP の設定

Routing Information Protocol（RIP）は小規模から中規模の TCP/IP ネットワークで一般的に使用されるルーティング プロトコルです。また、ディスタンスベクタ アルゴリズムを使用してルートを計算する安定したプロトコルです。

RIP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/15-mt/qos-plcshp-15-mt-book/qos-plcshp-class-plc.html

EIGRP の設定

Enhanced Interior Gateway Routing Protocol（EIGRP）は、シスコによって開発された Interior Gateway Routing Protocol（IGRP）の拡張バージョンです。EIGRP のコンバージェンス テクノロジーは、Diffusing Update Algorithm（DUAL）と呼ばれるアルゴリズムに基づいています。このアルゴリズムは、ルート計算中のどの時点でもループが発生しないようにし、トポロジ変更に関与するすべてのデバイスを同期できるようにします。トポロジ変更の影響を受けないデバイスは、再計算に含まれません。

EIGRP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/ire-15-mt-book/ire-enhanced-igrp.html

OSPF の設定

Open Shortest Path First（OSPF）は、Internet Engineering Task Force（IETF）の OSPF ワーキング グループによって開発された内部ゲートウェイ プロトコル（IGP）です。OSPF は特に IP ネットワーク向けに設計されており、IP サブネット化、および外部から取得したルーティング情報のタギングをサポートしています。OSPF はパケット認証も利用可能であり、パケットを送受信するときに IP マルチキャストが使用されます。

OSPF の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_tacacs/configuration/15-mt/sec-usr-tacacs-15-mt-book/sec-cfg-tacacs.html

BGP の設定

ボーダー ゲートウェイ プロトコル（BGP）は、独立したルーティング ポリシーを持つルーティング ドメイン（自律システム）の間に、ループのないルーティングを提供するように設計されたドメイン間ルーティング プロトコルです。シスコの BGP バージョン 4 のソフトウェア実装では、4 バイト自律システム番号およびマルチプロトコル拡張がサポートされており、IP バージョン 4（IPv4）、IP バージョン 6（IPv6）、バーチャル プライベート ネットワーク バージョン 4（VPNv4）、コネクションレス型ネットワークサービス（CLNS）、レイヤ 2 VPN（L2VPN）を含むインターネット プロトコル（IP）マルチキャスト ルートおよび複数のレイヤ 3 プロトコル アドレス ファミリのルーティング情報が BGP により伝送されるようになっています。

BGP の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/15-mt/sec-usr-ssh-15-mt-book/sec-usr-ssh-sec-shell.html

パフォーマンス ルーティング v3 の設定

パフォーマンス ルーティング v3（PfRv3）は、インテリジェント フレームワークを介した自動プレフィックスおよびサービス レベル契約（SLA）検出のための一連のソリューションを提供します。パス最適化、P2P ネットワークでのオーバーサブスクリプションのインテリジェント管理、マルチサイト導入、ネットワーク インフラストラクチャ使用率の最適化、ポリシー配布および適用、ネットワーク ベースの帯域幅管理など、容易なアプリケーション パフォーマンス管理制御機能を提供します。

PfRv3 は、アプリケーション配信と WAN の効率性を改善するインテリジェント パス制御機能です。PfRv3 は重要なアプリケーションを保護し、帯域幅の利用率を向上させ、シスコ インテリジェント WAN（IWAN）ソリューション全体の不可欠な部分として機能します。

IPマルチキャストの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/15-mt/pfrv3-15-mt-book/pfrv3.html

IP マルチキャストの設定

IP マルチキャストは、単一の情報ストリームを何千もの潜在的な企業および家庭に同時に配信することによってトラフィックを削減する帯域幅節約テクノロジーです。マルチキャストの応用例としては、ビデオ会議、企業間通信、遠隔学習、そして、ソフトウェア、株価、ニュースの配信などがあります。IP マルチキャスト ルーティングを使用すると、ホスト（送信元）は IP マルチキャスト グループ アドレスと呼ばれる特殊な形式の IP アドレスを使用し、IP ネットワーク内の任意の場所にあるホスト（レシーバ）のグループにパケットを送信できます。ソースのホストは、マルチキャスト グループ アドレスをパケットの宛先 IP アドレス フィールドに挿入します。IP マルチキャスト ルータおよびマルチレイヤ スイッチは、受信した IP マルチキャスト パケットを、マルチキャスト グループのメンバにつながるすべてのインターフェイスから転送します。どのホストも、グループのメンバであるかどうかにかかわらず、グループに送信できます。ただし、グループのメンバだけがメッセージを受信します。

IPマルチキャストの設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipmulti_pim/configuration/imc-pim-15-mt-book.html

BFD の設定

Bidirectional Forwarding Detection（BFD）は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用して、さまざまなルーティング プロトコルのインターバルの異なる hello メカニズムではなく単一レートで転送パスの障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再コンバージェンス時間の整合性が保たれ、予測可能になります。

BFD の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-mt/irb-15-mt-book/irb-bi-fwd-det.html

Multi-VRF の設定

Multi-VRF 機能を使用すると、サービス プロバイダーは複数のバーチャル プライベート ネットワーク（VPN）をサポートすることができ、複数の VPN で IP アドレスが重複することが可能になります。Multi-VRF サポート機能は、入力インターフェイスを使用して複数の異なる VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスを各仮想ルーティングおよび転送（VRF）インスタンスに関連付けることによって仮想パケット転送テーブルを作成します。VRF のインターフェイスは、FastEthernet ポートなどの物理インターフェイス、または VLAN スイッチ仮想インターフェイス（SVI）などの論理インターフェイスにすることができますが、レイヤ 3 インターフェイスは、一度に複数の VRF に属することはできません。Multi-VRF サポート機能により、オペレータはカスタマー エッジ（CE）デバイス上で複数のルーティング ドメインをサポートできます。各ルーティング ドメインでは、独自のセットのインターフェイスと独自のセットのルーティングおよび転送テーブルが使用されます。Multi-VRF サポート機能は、CE がサポートする各ルーティング ドメインに CE のラベル スイッチド パス（LSP）を拡張することができます。

Multi-VRF の設定に関する詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-mt/iri-15-mt-book/mp-multi-vrf-vrf-lite.html

IPv6 機能の設定

インターネット プロトコル バージョン 6（IPv6）は、ネットワーク アドレス ビット数を（IPv4 での）32 ビットから 128 ビットに拡張しているため、地球上のすべてのネットワーク デバイスにグローバルに一意な IP アドレスを十分に提供できます。IPv6 により実現する無制限のアドレス空間により、シスコは信頼性があり、ユーザ エクスペリエンスとセキュリティが強化された新しいアプリケーションとサービスをより多く提供できます。

IPv6 アドレッシングと基本接続の設定の詳細については、次の Web リンクを参照してください。

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-mt/ip6b-15-mt-book.html