Cisco 819 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

2012 年 11 月 2 日

Text Part Number: OL-23590-02-J

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

本書は、米国シスコ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 819 シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド

CONTENTS

CHAPTER 1

製品概要

この章では、Cisco 819 サービス統合型ルータ（ISR）で利用できる機能の概要について説明します。この章の内容は次のとおりです。

全般的な機能

Cisco 819 ISR では、20 ユーザ未満の規模の在宅勤務者、リモート オフィス、および小規模オフィスに対して、インターネット、VPN、データ、バックアップの各機能が提供されます。これらのルータは、LAN ポートと WAN ポートの間でのブリッジングおよびマルチプロトコル ルーティング機能を備えており、アンチウイルスなどの高度な機能も提供します。

Cisco 819 ISR は、4 つの 10/100 ファスト イーサネット（FE）、1 つのギガビット イーサネット（GE）、シリアルおよびセルラー（3G）インターフェイスを介する WAN 接続を提供する固定構成のデータ ルータです。

Cisco 819HGW および Cisco 819HWD ISR は、WiFi 無線（AP802H-AGN）をサポートします。ワイヤレス ローカルエリア ネットワーク（WLAN）は、ビルや敷地内の有線 LAN を交換するのではなく、頻繁に増強して、柔軟なデータ通信システムを実装します。WLAN では、無線周波数を使用して、データを無線で送受信し、有線接続の必要性を最小限にします。

Cisco 819HG-4G および Cisco 819G-4G は、マルチ モード 4G LTE をサポートし、Sierra Wireless 社製マルチモード モデムが組み込まれています。

（注） 特に別の方法で示さない限り、Cisco 819G、Cisco 819HG、Cisco 819H、Cisco 819HWD、Cisco 819HGW、シスコ 819HG-4G、および Cisco 819G-4G ISR を指すために Cisco 819 ISR を使用します。

図 1-1 に、Cisco 819HG ISR を示しています。

図 1-1　Cisco 819HG サービス統合型ルータ

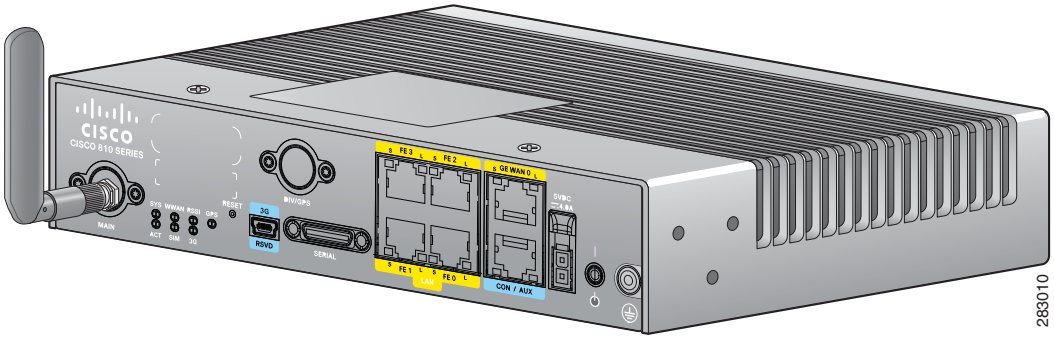
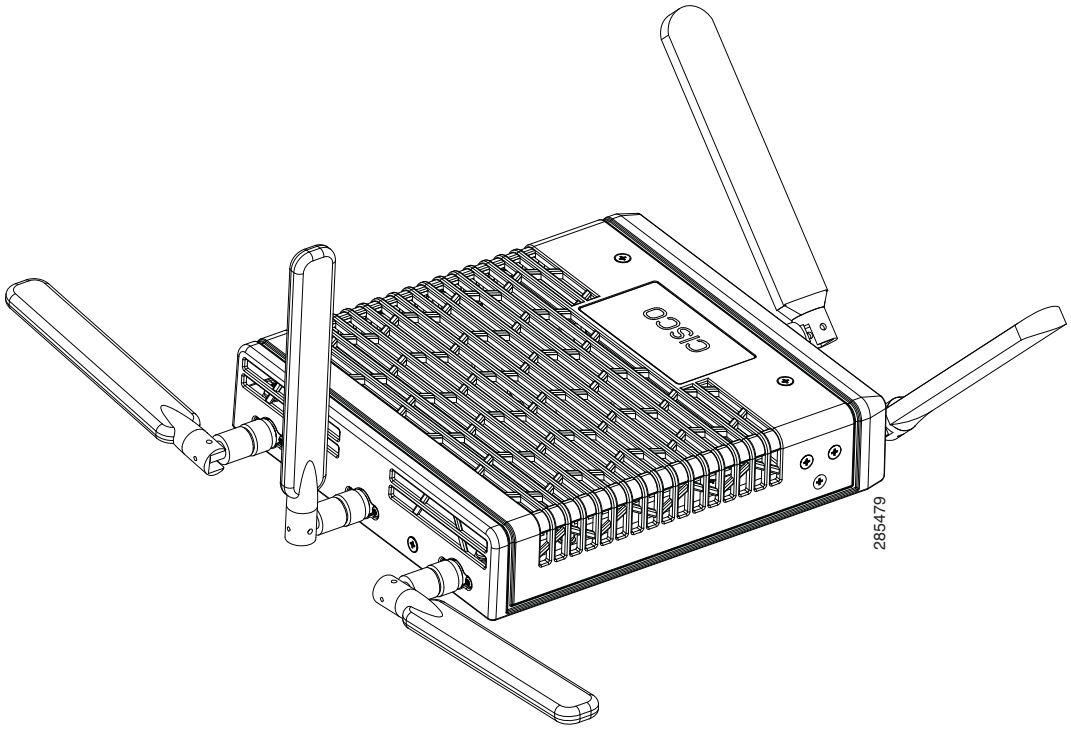


図 1-2 に、Cisco 819HGW ISR を示しています。

図 1-2　Cisco 819HGW サービス統合型ルータ



SKU 情報

Cisco 819 ISR で使用可能な SKU の完全なリストについては、「*SKU の情報*」を参照してください。

新機能

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

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

3G 機能

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

WLAN の機能

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

4G LTE 機能

- IPv4 ベアラー
- MIPv4、NEMOv4、RFC 3025
- LTE UE インターフェイス背後の IPv4 サブネット
- 4G LTE および 3G サービス間のシームレスなハンドオフを可能にする Evolved High-Rate Packet Data（EHRPD）（C819(H)G-4G-V-K9 のみ）
- LTE および EHRPD ネットワーク間のシームレスなハンドオフ（C819(H)G-4G-V-K9 のみ）
- LTE サービスからのフォールバック オプションとして UMTS サービスのサポート（C819(H)G-4G-A-K9 および C819(H)G-4G-G-K9 のみ）
- LTE と UMTS サービス間のシームレスなハンドオフ（C819(H)G-4G-A-K9 および C819(H)G-4G-G-K9 のみ）
- Qualcomm の診断モニタ ポートへのリモート アクセス
- ワイヤレス設定 FOTA を含む OTA-DM（C819(H)G-4G-V-K9 のみ）
- モデムのプロビジョニングのためのミニ USB タイプ 2 コネクタ

プラットフォーム機能

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

セキュリティ機能

Cisco 819 ISR は、次のセキュリティ機能を提供します。

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

CHAPTER 2

ワイヤレス デバイス概要

Cisco 819 ISR では、20 ユーザ未満の規模の在宅勤務者、リモート オフィス、および小規模オフィスに対して、インターネット、VPN、データ、バックアップの各機能が提供されます。これらの固定式ルータは、LAN ポートと WAN ポートの間でのブリッジングおよびマルチプロトコル ルーティング機能を備えており、アンチウイルスなどの高度な機能も提供します。

固定式 3G ルータは、プライマリ WAN 接続および重要なアプリケーションのバックアップとして使用でき、プライマリ WAN 接続としても使用できます。

（注） Cisco 819 ISR には 2 個の SIM カード スロットがあります。SIM カードの取り付け方法については、『*Cisco 819 Integrated Services Router Hardware Installation Guide*』を参照してください。

ScanSafe

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

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

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

イーサネット WAN インターフェイスを使用した TFTP のサポート

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

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

詳細については、「TFTP ダウンロード コマンドの使用」（P.C-5）を参照してください。

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

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

LED

LED は、ルータの前面パネルにあります。表 2-1 では、Cisco 819 ISR の 3G LED について説明します。

表 2-1　3G LED の説明

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

表 2-1　3G LED の説明 （続き）

LED	色	説明
GPS	緑色（点灯）	独立型 GPS。
	緑色（ゆっくり点滅）	GPS が取得中です。
	黄色（点灯）	アシスト型 GPS。
	黄色（ゆっくり点滅）	アシスト型 GPS が取得中です。
	Off	GPS は設定されていません。
RSSI	緑色（点灯）	信号 > – 60 非常に強い信号
	緑色（4 回点滅した後、長い一時停止）	信号 <= –60 ～ 74 強い信号
	緑色（2 回点滅した後、長い一時停止）	信号 <= –75 ～ -89 適正な信号
	緑色（1 回点滅した後、長い一時停止）	信号 <= –90 ～ -109 最低限の信号
	Off	信号 <= –110 使用不可能な信号
SIM[1,2]	緑色 / 黄色（1 回緑色点滅した後、2 回黄色点滅が続く）	スロット 0 の SIM はアクティブで、スロット 1 の SIM はアクティブではありません。
	黄色 / 緑色（1 回黄色点滅した後、2 回緑色点滅が続く）	スロット 1 の SIM はアクティブで、スロット 0 の SIM はアクティブではありません。
	Off/ 緑色（2 回緑色点滅した後、一時停止）	スロット 0 に SIM がなく、スロット 1 に SIM があります。
	緑色 /Off（ゆっくり 1 回緑色点滅した後、一時停止）	スロット 0 に SIM があり、スロット 1 に SIM がありません。
	Off / Off	いずれかのスロットに SIM がありません。
3G	1 回緑色点滅した後、一時停止	1xRTT、EGPRS、GPRS サービスの場合。
	2 回緑色点滅した後、一時停止	EVDO、EVDO/1xRTT、UMTS の場合。
	3 回緑色点滅した後、一時停止	EVDO/1xRTT RevA、HSPA、HSUPA/HSDPA の場合。
	緑色（点灯）	HSPA PLUS の場合。

1. Verizon および Sprint EVDO のモデムには適用されません。
2. 2 つの SIM のステータスを示す 1 つの LED があります。1 回の点滅パターンはスロット 0 の SIM のステータスを表し、その後に 2 回の点滅パターンが続いてスロット 1 の SIM のステータスを表します。

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

- **show platform led**（すべての LED の場合）
- **show controller cellular 0**（3G LED の場合）

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

```
router# show platform led

LED STATUS:
==========
LEDS  :  SYSTEM   WWAN           RSSI            GPS
STATUS:  GREEN    GREEN          GREEN(2 BLINK)  OFF

LEDS  :  ACTIVITY   SIM(slot0  / slot1)          3G
STATUS:  OFF            GREEN  / YELLOW          GREEN


LAN PORTS       :  FE0      FE1      FE2      FE3
LINK/ENABLE LED :  OFF      OFF      OFF      OFF
SPEED LED       :  Unknown  Unknown  Unknown  Unknown


PORT            :  GE-WAN0
LINK/ENABLE LED :  OFF
SPEED LED       :  Unknown
```

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

```
router# show controllers cellular 0

Interface Cellular0
3G Modem-QuadBand HSPA+R7/HSPA/UMTS QuadBand EDGE/GPRS Global and GPS,
Cellular modem configuration:
----------------------------
GSM-Carrier Type  : Cellular GSM Global.
SKU (PRI) Value: 9900198    .

Modem is recognized as valid
manufacture id:  0x00001199     product id: 0x000068A3
Sierra Wireless Mini Card MC8705 HSPA+R7 modem.

Cellular Dual SIM details:
--------------------------

SIM 0 is present
SIM 0 is active SIM

Modem Management Statistics
---------------------------
Modem resets = 2
Last known modem state = 'application' mode
Packets sent = 2508, Packets received = 44621, Packets pending = 0
DIP MDM link status retry count = 0 pdp context = 0
DIP MDM link up pending = 0 pdp context = 0
IDB Cellular0: DIP profile id = 255
RSSI LED    : 3-blink Green      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Service LED : 3-blink Green      <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
SIM LED     : Slot0 - Green;    Slot1 - Off    <<<<<<<<<<<<<<<<<<<<<<<<
GPS LED     : Off                <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
GPS NMEA port = Disabled   (Stream OFF)
DM port = Disabled
    :
    :
```

:

B

CHAPTER 3

ワイヤレス ローカルエリア ネットワーク

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

Cisco 819HGW と Cisco 819HWD ISR には､最初のコアで実行されるホスト ルータ ソフトウェアがあります。2 番目のコアは WLAN アクセス ポイント ソフトウェアを実行します。

WLAN が SKU でサポートされていない場合、すべての 1 GB の DRAM メモリは、最初のコアに割り当てられます。WLAN をサポートする SKU の場合は、メイン メモリ 1 GB のうち 128 MB が 2 番目のコアに割り当てられます。

WLAN が SKU でサポートされていない場合、すべての 1 GB のコンパクト フラッシュ メモリは、最初のコアに割り当てられます。WLAN をサポートする SKU の場合は、メイン メモリ 1 GB のうち 64 MB が 2 番目のコアに割り当てられます。

（注） WLAN は、IOS Release 15.2(4)M1 に導入された Cisco 819HGW および Cisco 819HWD ISR だけでサポートされます。

WLAN の機能

Cisco 819HGW および Cisco 819HWD ISR は次の機能をサポートします。

デュアル無線

このリリースは、Cisco 802 アクセス ポイント（AP802）をサポートします。AP802 は Cisco 819HGW Cisco 819HWD ISR の次世代の統合アクセス ポイントです。

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

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

デュアル無線/デュアルバンドの IEEE 802.11n アクセス ポイントを使用して、Cisco 819HGW および Cisco 819HWD ISR は、単一デバイスでセキュアな統合アクセス ポイントを提供します。ISR は、自律モードと統合モードの両方をサポートし、802.11a/b/g との下位互換性があります。

ルータは、IEEE 802.11n ドラフト 2.0 をサポートし、スループット、信頼性、および予測可能性を向上させる、複数入力、複数出力（MIMO）テクノロジーを使用します。

ワイヤレス デバイスと無線の設定方法の詳細については、「*Basic Wireless Device Configuration*」および「*Configuring Radio Settings*」を参照してください。

サポートされるイメージ

AP802 デュアル無線でサポートされるイメージについては、「*Minimum software version needed to support AP802*」を参照してください。

CleanAir テクノロジー

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

動的周波数選択

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

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

LED

WLAN LED は、ルータの前面パネルにあります。表 3-1 では、Cisco 819HGW および Cisco 819HWD ISR の WLAN LED について説明します。

表 3-1　WLAN LED の説明

WLAN LED	色	説明
ブートローダの状態シーケンス	緑色に点滅	ボードの初期化中。
		フラッシュ ファイル システムの初期化中。
		イーサネットの初期化中。
		イーサネットは正常です。
		Cisco IOS の起動中。
		初期化成功。
アソシエーションの状態	緑色	通常の動作状態（ワイヤレス クライアントのアソシエーションなし）。
	青色	通常の動作状態（少なくとも 1 つのワイヤレス クライアントのアソシエーションあり）。
動作状態	青色に点滅	ソフトウェアのアップグレード中。
	青色、緑色、赤色、白色の点灯が高速に切り替わる	アクセス ポイントの位置コマンドの呼び出し。
	赤色に点滅	イーサネット リンクが停止中。
ブートローダ エラー	赤色と青色の点滅	フラッシュ ファイル システムの障害。
	赤色の点滅とオフ	環境変数の障害。
		MAC アドレスが無効。
		イメージ復元中のイーサネットの障害。
		ブート環境の障害。
		Cisco イメージ ファイルなし。
		ブートの失敗。
Cisco IOS のエラー	赤色	ソフトウェア障害。装置の電源を切断し、再接続してみてください。

CHAPTER 4

4G LTE ワイヤレス WAN

Cisco IOS Release 15.2(4)M1 の場合、Cisco 819 ISR ではマルチモード 4G LTE 機能がサポートされます。Cisco 819HG-4G および Cisco 819G-4G LTE ISR は、4G LTE と 3G セルラー ネットワークをサポートします。4G LTE ISR には、次のモードをサポートする Sierra Wireless 社製マルチモード モデムが付いています。

- **3G Evolution-Data Optimized（EVDO または DOrA）**：EVDO は、無線信号を介したデータのワイヤレス伝送、特にブロードバンド インターネット アクセスの 3G 通信規格です。DOrA とは EVDO Rev-A を指します。EVDO は、個々のユーザのスループットおよびシステム全体のスループットの両方を最大化するために、符号分割多重接続（CDMA）や時分割多重アクセス（TDMA）などの多重化技術を使用します。
- **3G Evolution High-Speed Packet Access（HSPA/HSPA+）**：HSPA は UMTS ベースの 3G ネットワークです。これは、ダウンロードおよびアップロード速度の向上のため、High-Speed Downlink Packet Access（HSDPA）および High-Speed Uplink Packet Access（HSUPA）データをサポートします。Evolution High-Speed Packet Access（HSPA+）は、Multiple Input/Multiple Output（MIMO）アンテナ機能をサポートします。
- **4G LTE**：4G LTE モバイル仕様では、マルチメガビットの帯域幅、より効率的な無線ネットワーク、遅延の減少、改善されたモビリティが提供されます。LTE ソリューションは新しいセルラー ネットワークを対象とします。これらのネットワークは、最初にダウンリンクで最大 100 Mb/s のピーク レートを、アップリンクで最大 50 Mb/s のピーク レートをサポートします。これらのネットワークのスループットは既存の 3G ネットワークよりも大きくなります。

この章の内容は、次のとおりです。

Cisco 819HG-4G および Cisco 819G-4G LTE ISR の前提条件

- ルータが物理的に配置される 4G LTE のネットワーク カバレッジが必要です。サポートされている通信事業者の一覧については、次の製品のデータ シートを参照してください。
- ワイヤレス サービス プロバイダーのサービス プランに登録し、SIM カードを取得する必要があります。
- SIM カードを取り付けてから 4G LTE ルータを設定する必要があります。SIM カードの取り付けおよび交換の手順については、『*Cisco 819 Integrated Services Routers Hardware Installation Guide*』の「Installing the Router」の項を参照してください。

Cisco 819HG-4G および Cisco 819G-4G LTE ISR の制限事項

- 現在、セルラー ネットワークは発信コールだけをサポートします。
- スループット：ワイヤレス通信の共有特性により、発生するスループットは、使用しているネットワークでアクティブなユーザの数または輻輳状況によって、さまざまです。
- セルラー ネットワークは、有線ネットワークと比較して、より大きな遅延が発生します。遅延レートは、テクノロジーおよび通信事業者に左右されます。ネットワークで輻輳が発生している場合、遅延がより大きくなる場合があります。
- 使用する通信事業者からのサービス規約の一部である制約事項。
- 3G/4G 簡易ネットワーク管理プロトコル（SNMP）MIB はこのリリースでもサポートされていません。
- このリリースでは、パブリック ランド モバイル ネットワーク（PLMN）CLI がありますが、その機能はサポートされていません。
- デュアル SIM 機能は、このリリースではサポートされていません。
- GPS はこのリリースでもサポートされていません。

Cisco 819HG-4G および Cisco 819G-4G LTE ISR の設定方法

Cisco 819 ISR の 4G LTE 機能を設定する方法については、『*Configuring Cisco 4G LTE Wireless WAN EHWIC*』の「How to Configure Cisco 4G LTE Wireless WAN EHWICs」の項を参照してください。

（注）　Cisco 819HG-4G および Cisco 819G-4G LTE ISR の場合は、すべてのコマンドにスロット「0」を使用します。

Cisco 819HG-4G および Cisco 819G-4G LTE ISR の設定例

次に、Cisco 819HG-4G および Cisco 819G-4G LTE ISR のセルラー インターフェイスを設定する例を示します。

基本的なセルラー設定：例

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

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
!
!
controller Cellular 0
!
!
interface Cellular0
 ip address negotiated
 encapsulation slip
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer string lte
 dialer-group 1
 no peer default ip address
 async mode interactive
 routing dynamic
!
dialer-list 1 protocol ip permit
!
line 3
 script dialer lte
 modem InOut
 no exec
 transport input all
 transport output all
!
```

外部ダイヤラ インターフェイスを使用しないダイヤラウォッチの設定：例

次に、外部ダイヤラ インターフェイスを使用しないダイヤラウォッチを設定する例を示します。太字テキストはダイヤラウォッチに固有の重要なコマンドを示します。

```
chat-script lte "" "AT!CALL1" TIMEOUT 20 "OK"
interface Cellular0
ip address negotiated
encapsulation slip
dialer in-band
dialer string LTE
```

```
dialer watch-group 1
async mode interactive
!
dialer watch-list 1 ip 5.6.7.8 0.0.0.0
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
!
ip route 0.0.0.0 0.0.0.0 cellular 0
line 3
script dialer LTE
modem InOut
no exec
transport input all
transport output all
```

外部ダイヤラ インターフェイスを使用する dialer-persistent の設定：例

次に、外部ダイヤラ インターフェイスを使用する dialer-persistent を設定する例を示します。太字テキストは dialer-persistent に固有の重要なコマンドを示します。

```
interface Cellular0
ip address negotiated
encapsulation slip
dialer in-band
dialer pool-member 1
async mode interactive
routing dynamic
interface Dialer1
ip address negotiated
encapsulation slip
dialer pool 1
dialer idle-timeout 0
dialer string lte
dialer persistent
dialer-group 1
!
dialer-list 1 protocol ip permit
ip route 0.0.0.0 0.0.0.0 dialer 1
line 3
script dialer lte
modem InOut
no exec
transport input all
transport output all
```

セルラー インターフェイスを介する GRE トンネルの設定：例

次に、GRE トンネル インターフェイスが **ip address unnumbered** *cellular interface* で設定されている場合に、スタティック IP アドレスを設定する例を示します。

（注） GRE トンネルの設定は、サービス プロバイダーが LTE インターフェイスのパブリック IP アドレスを提供している場合にだけサポートされます。

（注）　プライベート IP アドレスを使用するサービス プロバイダーの場合、ポイントツーポイント スタティック GRE トンネルの一方のエンドをプライベート IP アドレスに、もう一方のエンドをパブリック IP アドレスに設定することはできません。

```
interface Tunnel2
ip unnumbered <internal LAN interface GE0/0 etc.>
tunnel source Cellular0
tunnel destination a.b.c.d
interface Cellular0
ip address negotiated
encapsulation slip
no ip mroute-cache
dialer in-band
dialer string lte
dialer-group 1
async mode interactive
! traffic of interest through the tunnel/cellular interface
ip route x.x.x.x 255.0.0.0 Tunnel2
! route for the tunnel destination via cellular
ip route a.b.c.d 255.255.255.255 cellular 0
```

LED

表 1 に、Cisco 819HG-4G および Cisco 819G-4G ISR の 3G/4G LED 動作の定義を示します。

表 1　4G LTE LED の説明

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

表 1　4G LTE LED の説明 （続き）

LED	色	説明
GPS	緑色（点灯）	独立型 GPS。
	緑色（ゆっくり点滅）	GPS が取得中です。
	黄色（点灯）	アシスト型 GPS。
	黄色（ゆっくり点滅）	アシスト型 GPS が取得中です。
	Off	GPS は設定されていません。
RSSI	緑色（点灯）	信号 > – 60 dBm 非常に強い信号
	緑色（3 回点滅した後、長い一時停止）	信号 <= –60 ～ 74 dBm 強い信号
	緑色（2 回点滅した後、長い一時停止）	信号 <= –75 ～ 89 dBm 適正な信号
	緑色（1 回点滅した後、長い一時停止）	信号 <= –90 ～ 109 dBm 最低限の信号
	Off	信号 <= –110 dBm 使用不可能な信号
SIM	緑色 / 黄色（1 回緑色点滅した後、2 回黄色点滅が続く）	スロット 0 の SIM はアクティブで、スロット 1 の SIM はアクティブではありません。
	黄色 / 緑色（1 回黄色点滅した後、2 回緑色点滅が続く）	スロット 1 の SIM はアクティブで、スロット 0 の SIM はアクティブではありません。
	Off/ 緑色（2 回緑色点滅した後、一時停止）	スロット 0 に SIM がなく、スロット 1 に SIM があります。
	緑色 /Off（ゆっくり 1 回緑色点滅した後、一時停止）	スロット 0 に SIM があり、スロット 1 に SIM がありません。
	Off / Off	いずれかのスロットに SIM がありません。
3G/4G	緑色（1 回点滅した後、一時停止）	1xRTT、EGPRS、または GPRS サービスの場合。
	緑色（2 回点滅した後、一時停止）	EVDO、EVDO/1xRTT、または UMTS サービスの場合。
	緑色（3 回点滅した後、一時停止）	EVDO/1xRTT RevA、HSPA、または HSUPA/HSDPA サービスの場合。
	緑色（4 回点滅した後、一時停止）	HSPA+ サービスの場合。
	緑色（点灯）	4G/LTE サービスの場合。
	Off	サービスがありません。

モデム ファームウェアのアップグレード

Cisco 819HG-4G および Cisco 819G-4G ISR のモデム ファームウェアをアップグレードする方法については、『*Configuring Cisco 4G LTE Wireless WAN EHWIC*』の「Modem Firmware Upgrade」の項を参照してください。

トラブルシューティング

Cisco 819HG-4G および Cisco 819G-4G ISR のトラブルシューティングの手順については、『*Configuring Cisco 4G LTE Wireless WAN EHWIC*』の「Troubleshooting」の項を参照してください。

（注）　Cisco 819HG-4G および Cisco 819G-4G ISR の場合は、すべてのコマンドにスロット「0」を使用します。

CHAPTER 5

ルータの基本設定

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

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

この章では、該当するものがある場合には設定例と確認手順が記載されています。

グローバル コンフィギュレーション モードにアクセスする方法の詳細については、「グローバル コンフィギュレーション モードの開始」（P.A-6）を参照してください。

インターフェイス ポート

表 5-1 は、各ルータでサポートされているインターフェイスと装置に表記されているポート ラベルを示しています。

表 5-1　Cisco ルータでサポートされているインターフェイスと対応するポート ラベル

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

（注） ラベルの付いた関連アンテナには、メインおよび DIV/GPS の 2 種類のラベルがあります。

デフォルト コンフィギュレーション

Cisco ルータを初めて起動すると、一部の基本的な設定はすでに行われています。LAN および WAN インターフェイスはすべて作成されており、コンソール ポートと VTY ポートの設定やネットワーク アドレス変換（NAT）用の内部インターフェイスの割り当てもすでに行われています。初期設定を表示するには、**show running-config** コマンドを使用します（次の Cisco 819 ISR ルータの例を参照してください）。

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

Current configuration : 977 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
no aaa new-model
ip source-route
ip cef

no ipv6 cef
license udi pid CISCO819G-G-K9 sn FHK1429768Q
controller Cellular 0
interface Cellular0
 no ip address
 encapsulation ppp
interface Ethernet-wan0
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
interface FastEthernet0
interface FastEthernet1
interface FastEthernet2
interface FastEthernet3
interface Serial0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server

logging esm config

control-plane
line con 0
 no modem enable
line aux 0
line 3
 no exec
line 7
 stopbits 1
 speed 115200
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
end
```

設定に必要な情報

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

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

  - ルータにアクセスするための PPP クライアント名
  - ルータにアクセスするための PPP パスワード
- IP ルーティングを設定する場合、次の準備が必要です。
  - IP ネットワークのアドレス指定方式を作成します。
- シリアル インターフェイスを設定している場合：
  - 動作のモード（sync、async、bisync）
  - モードによるクロック レート
  - モードによる IP アドレス
- 3G を設定している場合：
  - Cisco 819 ISR で通信事業者からのサービスを使用可能でなければなりません。また、ルータが物理的に置かれているネットワーク カバレッジも必要です。サポートされている通信事業者の一覧については、「*Cisco 3G Wireless Connectivity Solutions*」のデータ シートを参照してください。
  - ワイヤレス サービス プロバイダーのサービス プランに登録し、SIM カードを取得する必要があります。
  - SIM カードを取り付けてから 3G Cisco 819 ISR を設定する必要があります。SIM カードの取り付け方法については、「*Cisco 800 Series RoutersConfiguring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)*」を参照してください。
- Cisco 819 ISR の 3G を設定する前に必要なアンテナを取り付ける必要があります。アンテナの取り付け方法の説明については、次の URL を参照してください。
  - 3G-ANTM1919D：「*Cisco Multiband Swivel-Mount Dipole Antenna (3G-ANTM1919D)*」を参照。
  - 3G-ANTM1916-CM：「*Cisco Multiband Omnidirectional Ceiling Mount Antenna (3G-ANTM1916-CM)*」を参照。
  - 3G-AE015-R（アンテナの拡張）：「*Cisco Single-Port Antenna Stand for Multiband TNC Male-Terminated Portable Antenna (Cisco 3G-AE015-R)*」を参照。
  - 3G-AE010-R（アンテナの拡張）：「*Cisco Single-Port Antenna Stand for Multiband TNC Male-Terminated Portable Antenna (Cisco 3G-AE015-R)* 」を参照。このマニュアルは、3G-AE015-R と 3G-AE010-R に該当します。製品の違いはケーブルの長さのみです。
  - 3G-ANTM-OUT-OM：「*Cisco 3G Omnidirectional Outdoor Antenna (3G-ANTM-OUT-OM)*」を参照。
  - 3G-ANTM-OUT-LP：「*Cisco Multiband Omnidirectional Panel-Mount Antenna (3G-ANTM-OUT-LP)*」を参照。
  - 3G-ACC-OUT-LA：「*Cisco 3G Lightning Arrestor (3G-ACC-OUT-LA)*」を参照。
  - 4G-ANTM-OM-CM：「*Cisco 4G Indoor Ceiling-Mount Omnidirectional Antenna (4G-ANTM-OM-CM)*」を参照。
- 表 2-1 に説明したように、信号の受信状況について LED を確認する必要があります。
- Cisco IOS ソフトウェアに精通している必要があります。Cisco 3G のサポートについては、リリース 12.4(15)T またはそれ以降の *Cisco IOS マニュアル*を参照してください。
- 3G データ プロファイルを設定するには、サービス プロバイダーからユーザ名、パスワード、およびアクセス ポイント名（APN）を取得する必要があります。

該当する情報の収集が済んだら、ルータの設定を行うことができます。「コマンドライン アクセスの設定」（P.5-5）から設定を始めてください。

ソフトウェア ライセンスを取得または変更する場合：

- 『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

コマンドライン アクセスの設定

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

手順の概要

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

手順の詳細

	コマンド	目的

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

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

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

ステップ 4	**exec-timeout** *minutes* [*seconds*]
	
	例：
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		ユーザ入力が検出されるまで EXEC コマンド インタープリタが待機する間隔を設定します。デフォルトは 10 分です。任意で、間隔値に秒数を追加します。
		この例では、5 分 30 秒のタイムアウトを表示します。「0 0」のタイムアウトを入力すると、タイムアウトが発生しません。

ステップ 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	例：
	`Router(config-line)# line vty 0 4`
	`Router(config-line)#`
		リモート コンソール アクセス用の仮想端末を指定します。

ステップ 6	**password** *password*
	
	例：
	`Router(config-line)# password aldf2ad1`
	`Router(config-line)#`
		仮想端末回線に固有のパスワードを指定します。

	コマンド	目的

ステップ 7	**login**
	
	例：
	`Router(config-line)# login`
	`Router(config-line)#`
		仮想端末セッション ログイン時のパスワード チェックをイネーブルにします。

ステップ 8	**end**
	
	例：
	`Router(config-line)# end`
	`Router#`
		回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

例

次の設定は、コマンドライン アクセス コマンドを示します。

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

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

グローバル パラメータの設定

ルータに選択したグローバル パラメータを設定するには、次の作業を行います。

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

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

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

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

WAN インターフェイスの設定

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

ギガビット イーサネット WAN インターフェイスの設定

Cisco 819 ISR でイーサネット インターフェイスを設定するには、グローバル コンフィギュレーション モードから次の手順を実行します。

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface gigabitethernet 0`
	`Router(config-if)#`
		ルータのギガビット イーサネット WAN インターフェイスのコンフィギュレーション モードを開始します。

ステップ 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-if)#`
		指定したギガビット イーサネット インターフェイスの IP アドレスとサブネット マスクを設定します。

ステップ 3	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		イーサネット インターフェイスをイネーブルにして、インターフェイスの状態を管理上のダウンからアップに変更します。

ステップ 4	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		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。

セル ワイヤレス WAN インターフェイスの設定

Cisco 819 ISR は、Global System for Mobile Communications（GSM）および符号分割多重接続（CDMA）ネットワークを介して使用する、第 3 世代（3G）ワイヤレス インターフェイスを提供します。インターフェイスは 34 mm の埋め込みミニ エクスプレス カードです。

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

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

3G ワイヤレス インターフェイスの設定に関する要件

次に、3G ワイヤレス インターフェイスの設定に関する要件を示します。

- 通信事業者のワイヤレス サービスが必要です。また、ルータが物理的に配置されるネットワーク カバレッジも必要です。サポートされている通信事業者の一覧については、次の URL のデータ シートを参照してください。

  www.cisco.com/go/m2m

- ワイヤレス サービス プロバイダーとのサービス プランに契約し、そのサービス プロバイダーから SIM カード（GSM モデムだけ）を取得する必要があります。
- 表 2-1 の説明に従い、信号強度について LED をチェックする必要があります。
- Cisco IOS ソフトウェアに精通している必要があります。Cisco 3G ワイヤレス サポートについては、Cisco IOS Release 12.4(15)XZ またはそれ以降の *Cisco IOS マニュアル*を参照してください。
- GSM データ プロファイルを設定するには、サービス プロバイダーから次の情報を取得する必要があります。
  - ユーザ名
  - パスワード
  - アクセス ポイント名（APN）
- 手動でアクティブにするために CDMA（CDMA のみ）データ プロファイルを設定するには、サービス プロバイダーから次の情報を取得する必要があります。
  - Master Subsidy Lock（MSL）番号
  - Mobile Directory Number（MDN）
  - Mobile Station Identifier（MSID）
  - Electronic Serial Number (ESN)
- ルータの前面パネルにある LED で信号強度などの表示を確認します。表 2-1 では、Cisco 819 ISR の 3G LED について説明します。

セル ワイヤレス インターフェイスの設定に関する制約事項

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

- データ接続は、3G ワイヤレス インターフェイスだけから行うことができます。リモート ダイヤルインはサポートされていません。
- ワイヤレス通信共通の性質により、スループットは、ネットワークでのアクティブ ユーザの数や輻輳の量により異なります。
- セル ネットワークの遅延は、優先ネットワークの場合よりも大きくなります。遅延レートは、テクノロジーおよび通信事業者に左右されます。ネットワーク輻輳が発生している場合、遅延が大きくなることがあります。
- VoIP は現在サポートされていません。
- 通信事業者のサービス条件に含まれるいずれの制約事項も Cisco 3G ワイヤレス インターフェイスに適用されます。
- 取り外されたモデムとは別のタイプのモデムを取り付けた場合は、設定を変更して、システムをリロードしなければなりません。

データ アカウントのプロビジョニング

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

データ アカウントをプロビジョニングするには、次の手順を実行します。

- 「信号の強さとサービスの可用性」（P.5-12）
- 「GSM モデム データ プロファイルの設定」（P.5-13）
- 「CDMA モデム アクティベーションおよびプロビジョニング」（P.5-14）

信号の強さとサービスの可用性

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**show cellular 0 gps** **例：** `Router# show cellular 0 gps`	セルラー gps 情報を表示します。
ステップ 5	**show cellular 0 radio** **例：** `Router# show cellular 0 radio`	無線信号の強さを示します。 **（注）** 安定した信頼性の高い接続には、RSSI が -90 dBm を超える必要があります。
ステップ 6	**show cellular 0 profile** **例：** `Router# show cellular 0 profile`	作成されたモデム データ プロファイルに関する情報を示します。
ステップ 7	**show cellular 0 security** **例：** `Router# show cellular 0 security`	SIM およびモデムのロック ステータスに関するセキュリティ情報を示します。
ステップ 8	**show cellular 0 sms** **例：** `Router# show cellular 0 sms`	セルラー sms 情報を表示します。
ステップ 9	**show cellular 0 all** **例：** `Router# show cellular 0 all`	モデムに関する統合的な情報、たとえば、作成されたプロファイル、無線信号強度、ネットワーク セキュリティなどの情報を表示します。

GSM モデル データ プロファイルの設定

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

手順の概要

1. **cellular 0 gsm profile create <profile number> <apn> <authentication> <username> <password> ipv4**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cellular 0 gsm profile create <profile number> <apn> <authentication> <username> <password> ipv4** **例：** `Router# gsm profile create 2 <apn-name> chap username password ipv4`	新しいモデム データ プロファイルを作成します。コマンド パラメータの詳細については、表 5-2 を参照してください。

表 5-2 は、モデム データ プロファイルのパラメータのリストです。

表 5-2　モデム データ プロファイル パラメータ

profile number	作成するプロファイルの番号。最大 16 個のプロファイルを作成できます。
apn	アクセス ポイント名。この情報はサービス プロバイダーから取得する必要があります。
authentication	CHAP、PAP などの認証タイプ。
Username	サービス プロバイダーから提供されるユーザ名。
Password	サービス プロバイダーから提供されるパスワード。

CDMA モデム アクティベーションおよびプロビジョニング

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

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

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

表 5-3

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

1. OTASP = Over the Air Service Provisioning（電波によるサービス提供）
2. IOTA = Internet Over the Air（インターネット地上波）

手動によるアクティベーション

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

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

cellular *unit* **cdma activate manual** *mdn msid msl*

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

次に、このコマンドの出力例を示します。

```
router# cellular 0 cdma activate manual 1234567890 1234567890 12345
NAM 0 will be configured and will become Active
Modem will be activated with following Parameters
MDN :1234567890; MSID :1234567890; SID :1234; NID 12:
Checking Current Activation Status
```

```
Modem activation status: Not Activated
Begin Activation
Account activation - Step 1 of 5
Account activation - Step 2 of 5
Account activation - Step 3 of 5
Account activation - Step 4 of 5
Account activation - Step 5 of 5
Secure Commit Result: Succeed
Done Configuring - Resetting the modem
The activation of the account is Complete
Waiting for modem to be ready to start IOTA
Beginning IOTA
router#
*Feb  6 23:29:08.459: IOTA Status Message Received. Event: IOTA Start, Result: SUCCESS
*Feb  6 23:29:08.459: Please wait till IOTA END message is received
*Feb  6 23:29:08.459: It can take up to 5 minutes
*Feb  6 23:29:27.951: OTA State = SPL unlock, Result = Success
*Feb  6 23:29:32.319: OTA State = Parameters committed to NVRAM, Result = Success
*Feb  6 23:29:40.999: Over the air provisioning complete; Result:Success
*Feb  6 23:29:41.679: IOTA Status Message Received. Event: IOTA End, Result: SUCCESS
```

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

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

cellular cdma activate iota

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

電波によるサービス提供（OTASP）のプロビジョニングおよびアクティベーションを行うには、EXEC モードから次のコマンドを使用します。

router # **cellular 0 cdma activate otasp** *phone_number*

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

次に、このコマンドの出力例を示します。

```
router# cellular 0 cdma activate otasp  *22899
Beginning OTASP activation
OTASP number is *22899
819H#
OTA State = SPL unlock, Result = Success
router#
OTA State = PRL downloaded, Result = Success
OTA State = Profile downloaded, Result = Success
OTA State = MDN downloaded, Result = Success
OTA State = Parameters committed to NVRAM, Result = Success
Over the air provisioning complete; Result:Success
```

セルラー インターフェイスの設定

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

手順の概要

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

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	端末からグローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface cellular 0** **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。
ステップ 3	**encapsulation ppp** **例：** `Router (config-if)# encapsulation ppp`	専用非同期モード用またはダイヤルオンデマンド ルーティング（DDR）用のインターフェイスの PPP カプセル化を指定します。
ステップ 4	**ppp chap hostname** *hostname* **例：** `Router (config-if)# ppp chap hostname cisco@wwan.ccs`	インターフェイス固有のチャレンジ ハンドシェイク認証プロトコル（CHAP）ホスト名を定義します。これは、通信事業者から提供されたユーザ名に一致する必要があります。GSM だけに適用されます。
ステップ 5	**ppp chap password 0** *password* **例：** `Router (config-if)# ppp chap password 0 cisco`	インターフェイス固有の CHAP パスワードを指定します。これは、通信事業者から提供されたパスワードに一致する必要があります。

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

（注）　セル インターフェイスでスタティック IP アドレスが必要な場合、アドレスは、**ip address negotiated** として設定できます。インターネット プロトコル制御プロトコル（IPCP）を介して、ネットワークにより、正しいスタティック IP アドレスがデバイスに割り当てられるようになります。トンネル インターフェイスが **ip address unnumbered** <*cellular interface*> コマンドで設定されている場合、実際のスタティック IP アドレスは **ip address negotiated** でなく、セルラー インターフェイス下で設定されなければなりません。セルラー インターフェイスの例については、「基本セルラー インターフェイスの設定」（P.5-20）を参照してください。

DDR の設定

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

手順の概要

1. **configure terminal**
2. **interface cellular 0**
3. **dialer in-band**
4. **dialer idle-timeout** *seconds*
5. **dialer string** *string*
6. **dialer group** *number*
7. **exit**
8. **dialer-list** *dialer-group* **protocol** *protocol-name* **{permit** | **deny** | **list** *access-list-number* | **access-group}**
9. **ip access-list** <*access list number*> **permit** <*ip source address*>
10. **line 3**
11. **script dialer** <regexp>
12. **exit**
13. **chat-script <script name> "" "ATDT*99*<profile number>#" TIMEOUT <timeout value> CONNECT**
    または
    chat-script <script name> "" "ATDT*777*<profile number>#" TIMEOUT <timeout value> CONNECT

14. **interface cellular 0**
15. **dialer string** <*string*>

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface cellular 0** **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。
ステップ 3	**dialer in-band** **例：** `Router (config-if)# dialer in-band`	DDR をイネーブルにし、インバンド ダイヤリングに指定されたシリアル インターフェイスを設定します。
ステップ 4	**dialer idle-timeout** *seconds* **例：** `Router (config-if)# dialer idle-timeout 30`	回線切断後のアイドル時間を秒単位で指定します。
ステップ 5	**dialer string** *string* **例：** `Router (config-if)# dialer string gsm`	ダイヤルする番号または文字列を指定します。チャット スクリプトの名前をここで使用します。
ステップ 6	**dialer-group** *number* **例：** `Router (config-if)# dialer-group 1`	特定のインターフェイスが属するダイヤラ アクセス グループの番号を指定します。
ステップ 7	**exit** **例：** `Router (config-if)# exit`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number* | **access-group**} **例：** `Router (config)# dialer-list 1 protocol ip list 1`	関係するトラフィックのダイヤラ リストを作成し、プロトコル全体に対してアクセスを許可します。
ステップ 9	**ip access-list** <*access list number*> **permit** <*ip source address*> **例：** `Router (config)# ip access list 1 permit any`	関係するトラフィックを定義します。

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

セル ワイヤレス インターフェイスの設定例

ここでは、次の設定例について説明します。

基本セルラー インターフェイスの設定

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

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

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

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

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

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

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

ip route 0.0.0.0 0.0.0.0 Cellular0
!
!
access-list 1 permit any
dialer-list 1 protocol ip list 1
!
```

```
line 3
 exec-timeout 0 0
 script dialer cdma
 login
 modem InOut
```

セルラー インターフェイスを介するトンネルの設定

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

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

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

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

8705 モデムの設定

次に、HSPA+ のモデムを設定する例を示します。

```
chat-script hspa "" "AT!SCACT=1,1" TIMEOUT 60 "OK"

interface Cellular0
 ip address negotiated
 encapsulation slip
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async mode interactive

interface Dialer1
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
 encapsulation slip
 dialer pool 1
 dialer string hspa
 dialer-group 1

ip nat inside source list 1 interface Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
access-list 1 permit any
dialer-list 1 protocol ip permit
```

```
line 3
 script dialer hspa+
 modem InOut
 no exec
 transport input all
```

デュアル SIM の設定

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

次のコマンドを使用して、デュアル SIM 機能を設定できます。

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

次の点に注意してください。

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

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

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

次に、暗号化されていないピンを使用して認証する例を示します。

```
router(config-controller)# gsm sim authenticate 0 1234 slot 0
```

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

```
router(config-controller)# gsm sim max-retry 20
```

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

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

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

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

手動で SIM を切り替えるには、次のコマンドを実行します。

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

次のコマンドは、強制的にモデムを SIM1 に接続します。

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

GPS の設定

次のコマンドを使用して、GPS 機能を設定できます。

コマンド	構文	説明
gsm gps mode	**gsm gps mode standalone**	GPS スタンドアロン モードをイネーブルにします。
gsm gps nmea	**gsm gps nmea** [**ip** | **serial**]	NMEA モードをイネーブルにします。 • **ip**：IP インターフェイスを介する NMEA。 • **serial**：シリアル インターフェイスを介する NMEA。
show cellular gps	**show cellular** *unit* **gps**	GPS データの要約を表示します。
	show cellular *unit* **gps detail**	GPS データの詳細なリストを表示します。

次に、Cisco 819 ISR の概要と詳細な GPS データを表示する例を示します。出力には次の情報が含まれています。

- GPS の状態とモード情報
- GPS のトラッキング状態
- NMEA のストリーム状態
- GPS の位置およびタイムスタンプ情報
- GPS 衛星情報

```
router# show cellular 0 gps
GPS Info
-------------
GPS State: GPS enabled
GPS Mode Configured: standalone
Latitude: 37 Deg 24 Min 59 Sec North
Longitude: 121 Deg 55 Min 8 Sec West
Timestamp (GMT): Thu Jul 29 11:08:39 2010
Fix type: 3D, Height: -6 m
Heading: 408, Velocity Horiz: 3, Velocity Vert: 0
Satellite Info
----------------
Satellite #13, elevation 75, azimuth 46, SNR 21
...

router# show cellular 0 gps detail
GPS Info
-------------
GPS State: GPS enabled
GPS Mode Configured: standalone
Latitude: 37 Deg 24 Min 59 Sec North
Longitude: 121 Deg 55 Min 7 Sec West
Timestamp (GMT): Thu Jul 29 22:17:57 2010
Fix type: 3D, Height: 12 m
Heading: 0, Velocity Horiz: 0, Velocity Vert: 0
HEPE: 2680 cm
Uncertainty Info:
  Angle: 0 deg, A: 24 m, Position: 12 m, Vertical: 12 m
Satellite Info
----------------
Satellite #7, elevation 16, azimuth 123, SNR 14 *
...
```

GPS NMEA の設定

外部 NMEA 2.0 準拠 GPS プロッター アプリケーションへの GPS NMEA ストリーミングは、Cisco 819 ISR でサポートされています。

NMEA データ ストリーミングをイネーブルにするには、次のコマンドを実行します。

手順の概要

1. **conf t**
2. **controller cellular 0**
3. **gsm gps mode standalone**
4. **gsm gps nmea** [**ip** | **serial**]
5. **end**
6. **show running**
7. **show line**
8. **telnet** *ip address port*

手順の詳細

	コマンド	説明
ステップ 1	**conf t** **例：** `Router# conf t`	コンフィギュレーション モードに入ります。
ステップ 2	**controller cellular 0** **例：** `router(config)# controller cellular  0`	コントローラ セルラー コンフィギュレーション モードを開始します。
ステップ 3	**gsm gps mode standalone** **例：** `Router(config-controller)# gsm gps mode standalone`	独立型 GPS をイネーブルにします。
ステップ 4	**gsm gps nmea** [**ip** | **serial**] **例：** `Router(config-controller)# gsm gps nmea ip`	IP インターフェイスを介する NMEA をイネーブルにします。 • **ip**：IP インターフェイスを介する NMEA。 • **serial**：シリアル インターフェイスを介する NMEA。
ステップ 5	**end** **例：** `Router(config-controller)# end`	コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ステップ 6	**show running**
	
	例：
	`Router# show running`
	`<snip>`
	`controller Cellular 0`
	`gsm gps mode standalone`
	`gsm gps nmea ip`
		設定の出力を表示します。

	コマンド	説明

ステップ 7	**show line**
	
	例：
	`Router# show line`
	`Tty Typc Tx/Rx A Modem Roty AccO AccI Uses`
	`Noise  Overruns  Int`
	`*0 CTY - - - - -  1  56  0/207449798  -`
	`1 AUX 0/0 - - - -  -  0  0  0/0  -`
	`3 TTY - inout - - -  0  0  0/0  Ce0`
	`6 TTY - inout - - -  1 1233437  0/0  NMEA5`
	`7 TTY 9600/9600 - - - 0  0  0/0  Se0`
	`10 VTY - - - - -  0  0  0/0  -`
	`11 VTY - - - - -  0  0  0/0  -`
	`12 VTY - - - - -  0  0  0/0  -`
	`13 VTY - - - - -  0  0  0/0  -`
	`14 VTY - - - - - 0 0 0/0 -
		非同期ポート番号を表示します。
		
		NMEA が設定されている場合、IOS は NMEA 非同期ポートを作成します。ポート番号はプラットフォームに依存します。この例では、非同期ポート番号はライン 6 です。
		
		（注） ライン 2、4、5、8、9 は非同期モードではないか、ハードウェアが対応していません。

ステップ 8	**telnet** *ip address port*
	
	例：
	`Router# telnet 1.1.1.1 2006`
	`Trying 1.1.1.1, 2006 ... Open`
	`$GPGSV,4,1,16,27,,,,09,,,,15,,,,26,,,*77`
	`$GPGSV,4,2,16,17,,,,32,,,,28,,,,19,,,*7D`
	`$GPGSV,4,3,16,11,,,,08,,,,03,,,,01,,,*73`
	`$GPGSV,4,4,16,07,,,,06,,,,22,,,,16,,,*78`
	`$GPGGA,230924.6,,,,,0,,,,,,,,*70`
	`$GPVTG,,T,,M,,N,,K,N*2C`
	`$GPRMC,,V,,,,,,,,,,N*53`
	`$GPGSA,A,1,,,,,,,,,,,,,,,*1E`
	`$GPGSV,4,1,16,27,,,,09,,,,15,,,,26,,,*77`
	`$GPGSV,4,2,16,17,,,,32,,,,28,,,,19,,,*7D`
	`$GPGSV,4,3,16,11,,,,08,,,,03,,,,01,,,*73`
	`$GPGSV,4,4,16,07,,,,06,,,,22,,,,16,,,*78`
	`$GPGGA,230925.6,,,,,0,,,,,,,,*71`
	`$GPVTG,,T,,M,,N,,K,N*2C`
	`$GPRMC,,V,,,,,,,,,,N*53`
	`$GPGSA,A,1,,,,,,,,,,,,,,,*1E`
		NMEA ストリーミングがイネーブルの場合、モデムは、GPS の変更が取得されるかにかかわらず、NMEA ポート上の NMEA データのストリームを開始します。NMEA ポートにリバース Telnet を実行して、NMEA データをチェックできます。

Cisco 819 ISR の 3G 機能の設定については、次のマニュアルを参照してください。

- *「Configuring EHWIC-3G-EVDO-x Cards and C881G-x-K9 ISRs」*
- *「Configuring Cisco EHWIC-3G-HSPA-U and C881G-U-K9」*

Microsoft Streets を実行する PC への Cisco 819 ISR の接続

GPS アプリケーションをホストするリモート サーバに NMEA データをフィードできます。サーバは、イーサネット ケーブルを使用して、または LAN あるいは WAN ネットワーク経由でルータに直接接続できます。アプリケーションでシリアル ポートをサポートしている場合、シリアル ポート エミュレーション プログラムを実行して、LAN または WAN 接続で仮想シリアル ポートを作成する必要があります。

（注） Microsoft Streets は、Microsoft の Web サイトからダウンロード可能なライセンス ソフトウェアです。

Microsoft Streets を実行する PC に Cisco 819 ISR を接続するには、次の手順を実行します。

ステップ 1　イーサネット ケーブルで PC とルータをつなげます。

ステップ 2　PC とルータで ping を実行できることを確認します。

ステップ 3　PC のシリアル ポート リダイレクタを起動します。

ステップ 4　ルータの NMEA ポートに接続する仮想シリアル ポートを作成します。

ステップ 5　PC で Microsoft Streets を起動します。

ステップ 6　[GPS Menu] を選択します。

ステップ 7　[Start Tracking] をクリックします。

ステップ 8　ルータで **show cellular gps** コマンドの出力から位置の変更が得られれば、グラフに示された現在位置と、マップ上のその地点を中心とする円で赤茶色のドット カーソルが表示されます。

（注）　位置の変更が得られない場合、Microsoft アプリケーションはタイム アウトし、切断されます。

（注）　GPS 固定位置を取得するには、サポートされている GPS アンテナを DIV/GPS ポートに接続する必要があります。スタンドアロン モードを使用して GPS 固定位置を取得するには、最大 12 分かかることがあります。これは、位置と使用されるアンテナの種類に依存します。

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

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

この機能を使用するには、次の手順を実行します。

ステップ 1　電源プラグを外します。

ステップ 2　ルータの前面パネルのリセット ボタンを押します。

ステップ 3　リセット ボタンを押しながら、システムの電源を投入します。

システム LED が 4 回点滅し、ルータがボタンの押下を受け入れていることを示します。

このボタンの使用は、ROMMON の初期化中にのみ有効です。ウォーム リブート中にこのボタンを押しても、パフォーマンスには影響しません。表 5-4 に、ROMMON の初期化中にボタンが押された場合の高レベルの機能を示します。

表 5-4　ROMMON の初期化中のプッシュ ボタンの機能

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

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

ボタンが押されていないときの出力：例

```
router# show platform boot-record

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

ボタンが押されたときの出力：例

```
router# show platform boot-record

Platform Config Boot Record :
============================
Configuration Register at boot time : 0x0
Reset Button Status at Boot Time    : Pressed
Startup-config Backup Status at Boot: Ok
Startup-config(backup file)location : flash:/startup.backup.19000716-225840-UTC
Golden config file at location      : flash:/golden.cfg
Config Recovery Status              : Ok
```

WLAN AP のプッシュ ボタン

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

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

設定の復元を実行する場合、WLAN AP は、フラッシュ ドライブで **flash:/cpconfig-ap802.cfg** ファイルを使用できる場合、その内容で **flash:/config.txt** の内容を上書きします。それ以外の場合は、**flash:/config.txt** が削除されます。

ファスト イーサネット LAN インターフェイスの設定

ルータのファスト イーサネット LAN インターフェイスは、デフォルト VLAN の一部として自動的に設定され、個別のアドレスによる設定は行われません。アクセスは VLAN を通じて提供されます。必要に応じて、このインターフェイスを別の VLAN に割り当てることが可能です。VLAN の作成方法の詳細については、「イーサネット スイッチの設定」（P.10-1）を参照してください。

ループバック インターフェイスの設定

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

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

手順の概要

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

手順の詳細

	コマンド	目的

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

ステップ 2	**ip address** *ip-address mask*
	
	例：
	`Router(config-if)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-if)#`
		ループバック インターフェイスの IP アドレスとサブネット マスクを設定します。

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ループバック インターフェイスのコンフィギュレーション モードを終了します。続いて、グローバル コンフィギュレーション モードに戻ります。

例

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

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

設定の確認

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

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
```

```
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

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

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

スタティック ルートの設定

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

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

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
	`Router(config)#`
		IP パケットのスタティック ルートを指定します。
		このコマンドと設定可能な追加パラメータについては、『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』を参照してください。

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

スタティック ルーティングの一般的な説明については、「フローティング スタティック ルート」（P.B-5）を参照してください。

例

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

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

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

設定の確認

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

次のような確認用の出力が表示されます。

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

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
```

```
C       10.108.1.0 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, FastEthernet0
```

ダイナミック ルートの設定

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

Cisco ルータは、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。

- 「ルーティング情報プロトコルの設定」（P.5-33）
- 「拡張インテリア ゲートウェイ ルーティング プロトコルの設定」（P.5-35）

ルーティング情報プロトコルの設定

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

手順の概要

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

手順の詳細

	コマンド	作業

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

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

ステップ 3	**network** *ip-address*
	
	例：
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
	`Router(config-router)#`
		直接接続しているネットワークの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 4	**no auto-summary**
	
	例：
	`Router(config-router)# no auto-summary`
	`Router(config-router)#`
		ネットワークレベル ルートへのサブネット ルートの自動サマライズをディセーブルにします。これにより、サブプレフィックス 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 5	**end**
	
	例：
	`Router(config-router)# end`
	`Router#`
		ルータ コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

RIP に関する一般情報については、「RIP」（P.B-2）を参照してください。

例

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

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

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

設定の確認

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

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

Gateway of last resort is not set

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

拡張インテリア ゲートウェイ ルーティング プロトコルの設定

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

手順の概要

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

手順の詳細

	コマンド	目的

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

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

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

EIGRP の概念について一般的な説明は、「EIGRP」（P.B-3）を参照してください。

例

次の設定例は、IP ネットワーク 192.145.1.0 および 10.10.12.115 でイネーブルにされる EIGRP ルーティング プロトコルを示します。EIGRP の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 モードで開始し、**show running-config** コマンドを使用します。

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

設定の確認

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

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

Gateway of last resort is not set
     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CHAPTER 6

バックアップ データ回線およびリモート管理の設定

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

Cisco 819 サービス統合型ルータ（ISR）は、WAN のダウンタイムの削減を可能にするバックアップ データ ラインとのバックアップ データ接続をサポートします。

Cisco 819 ISR は、任意の Cisco 819 シリーズ ISR の補助ポートを介してリモート管理機能もサポートします。

（注） Cisco 819 シリーズ ISR では、コンソール ポートおよび補助ポートは、同じ物理 RJ-45 ポートにあります。そのため、これら 2 つのポートを同時にアクティブにできません。コマンドライン インターフェイス（CLI）を使用して、目的の機能をイネーブルにする必要があります。

バックアップ インターフェイスの設定

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

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

表 6-1 に、各 Cisco 819 ISR で使用できるバックアップ インターフェイス、およびポート指定を示します。これらのインターフェイスの基本設定を「WAN インターフェイスの設定」（P.5-9）に示します。

表 6-1　モデル番号およびデータ ライン バックアップ機能

ルータ モデル番号		3G
819		Yes

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

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface xxx 0`
	`Router(config-if)#`
		バックアップ用に設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
		
		ここで指定できるのは、シリアル インターフェイス、ISDN インターフェイス、または非同期インターフェイスです。

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

ステップ 3	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

セルラー ダイヤルオンデマンド ルーティング バックアップの設定

必要な場合にプライマリ接続を監視し、セルラー インターフェイスでバックアップ接続を開始する場合、ルータは次のいずれかの方法を使用できます。

- バックアップ インターフェイス：スタンバイの状態のまま待機し、プライマリ インターフェイス回線プロトコルがダウンと認識されると、アップ状態になります。「バックアップ インターフェイスの設定」（P.6-1）を参照してください。
- ダイヤラ ウォッチ：ダイヤラ ウォッチは、ダイヤル バックアップをルーティング機能と統合するバックアップ機能です。「ダイヤラ ウォッチを使用した DDR バックアップの設定」（P.6-3）を参照してください。
- 浮動スタティック ルート：バックアップ インターフェイスを介する経路に、プライマリ接続のアドミニストレーティブ ディスタンスよりも大きいアドミニストレーティブ ディスタンスがあり、プライマリ インターフェイスがダウンするまで、ルーティング テーブルには存在しません。プライマリ インターフェイスがダウンすると、フローティング スタティック ルートが使用されます。「浮動スタティック ルートを使用した DDR バックアップの設定」（P.6-5）を参照してください。

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

ダイヤラ ウォッチを使用した DDR バックアップの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *type number* **例：** `Router (config)# interface 0`	インターフェイスを指定します。
ステップ 3	**dialer watch-group** *group-number* **例：** `Router(config-if)# dialer watch-group 2`	バックアップ インターフェイスでダイヤラ ウォッチをイネーブルにします。
ステップ 4	**dialer watch-list** *group-number* **ip** *ip-address address-mask* **例：** `Router(config-if)# dialer watch-list 2 ip 10.4.0.254 255.255.0.0`	監視されるすべての IP アドレスのリストを定義します。
ステップ 5	**dialer-list** *<dialer-group>* **protocol** *<protocol-name>* {**permit** | **deny** | **list** <access-list-number> | **access-group**} **例：** `Router(config)# dialer-list 2 protocol ip permit`	関係するトラフィックのダイヤラ リストを作成し、プロトコル全体に対してアクセスを許可します。
ステップ 6	**ip access-list** *<access list number>* **permit** *<ip source address>* **例：** `Router(config)# access list 2 permit 10.4.0.0`	関係するトラフィックを定義します。 IP ネットワークへのトラフィック送信を回避するには、**access list permit all** コマンドは使用しないでください。これによって、コールが強制的に終了される場合があります。

	コマンドまたはアクション	目的
ステップ 7	**interface cellular** *0* **例：** `Router (config)# interface cellular 0`	セルラー インターフェイスを指定します。

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

浮動スタティック ルートを使用した DDR バックアップの設定

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

（注）　ルータで ip classless がイネーブルにされていることを確認してください。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	端末からグローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route** *network-number network-mask* {ip-address | interface} [administrative distance] [**name** name] **例：** `Router (config)# ip route 0.0.0.0 Dialer 2 track 234`	指定されたインターフェイスを介して、設定されているアドミニストレーティブ ディスタンスを使用して、浮動スタティック ルートを確立します。 プライマリ インターフェイスがダウンしたときだけバックアップ インターフェイスを使用するよう、バックアップ インターフェイスを通したルートのアドミニストレーティブ ディスタンスをより高く設定する必要があります。

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

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

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

```
Current configuration : 3433 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key gsm address 128.107.241.234
!
!
crypto ipsec transform-set gsm ah-sha-hmac esp-3des
!
crypto map gsm1 10 ipsec-isakmp
 set peer 128.107.241.234
 set transform-set gsm
 match address 103
!
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!
archive
 log config
```

```
  hidekeys
!
!
interface 0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no ilmi-keepalive
!
interface 0.1 point-to-point
 backup interface Cellular0
 ip nat outside
 ip virtual-reassembly
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Cellular0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string gsm
 dialer-group 1
 async mode interactive
 no ppp lcp fast-start
 ppp chap hostname chunahayev@wwan.ccs
 ppp chap password 0 B7uhestacr
 ppp ipcp dns request
 crypto map gsm1
!
interface Vlan1
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
interface Dialer2
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto map gsm1
!
ip local policy route-map track-primary-if
ip forward-protocol nd
```

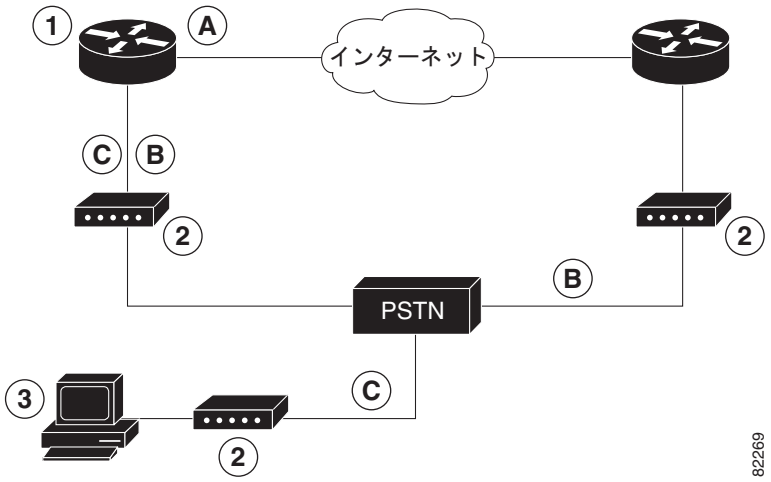
```
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0 254
no ip http server
no ip http secure-server
!
!
ip nat inside source route-map nat2cell interface Cellular0 overload
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 2 permit 10.4.0.0 0.0.255.255
access-list 3 permit any
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 209.131.36.158
access-list 103 permit ip host 166.136.225.89 128.107.0.0 0.0.255.255
access-list 103 permit ip host 75.40.113.246 128.107.0.0 0.0.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line 3
 exec-timeout 0 0
 script dialer gsm
 login
 modem InOut
 no exec
line vty 0 4
 login
!
scheduler max-task-time 5000

!
webvpn cef
end
```

コンソール ポートを使用したダイヤル バックアップおよびリモート管理の設定

Cisco 819 ISR などの加入者宅内機器とインターネット サービス プロバイダー（ISP）が接続されている場合、IP アドレスは動的にルータに割り当てられます。また、中央管理機能を使用して、ルータのピアによって割り当てられることもあります。プライマリ回線に障害が発生した場合にフェールオーバー ルートを提供するため、ダイヤル バックアップ機能を追加できます。Cisco 819 ISR はダイヤル バックアップおよびリモート管理に補助ポートを使用できます。

図 6-1 は、リモート管理アクセスおよびプライマリ WAN 回線にバックアップを提供する場合に使用するネットワーク コンフィギュレーションを示しています。

図 6-1　補助ポートによるダイヤル バックアップおよびリモート管理



1	Cisco 819 ルータ	**A**	メイン WAN リンク。インターネット サービス プロバイダーへのプライマリ接続です。
2	モデム	**B**	ダイヤル バックアップ。プライマリ回線がダウンした場合に Cisco 819 ルータのフェールオーバー リンクとして機能します。
3	PC	**C**	リモート管理。Cisco IOS コンフィギュレーションへの変更または更新を可能にするダイヤルイン アクセスとして機能します。

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

手順の概要

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

手順の詳細

	コマンド	目的

ステップ 1	**ip name-server** *server-address*
	
	例：
	`Router(config)#ip name-server 192.168.28.12`
	`Router(config)#`
		ISP DNS IP アドレスを入力します。
		
		ヒント 可能な場合は、複数のサーバ アドレスを追加できます。

ステップ 2	**ip dhcp pool** *name*
	
	例：
	`Router(config)#ip dhcp pool 1`
	`Router(config-dhcp)#`
		ルータ上に DHCP アドレス プールを作成します。続いて、DHCP プール コンフィギュレーション モードを開始します。*name* 引数は、ストリングまたは整数にすることができます。
		
		• DHCP アドレス プールを設定します。DHCP プール コンフィギュレーション モードで使用できるサンプル コマンドについては、「例」（P.6-13）を参照してください。

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

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

ステップ 5	**interface** *type number*
	
	例：
	`Router(config)# interface Async 1`
	`Router(config-if)#`
		非同期インターフェイスのコンフィギュレーション モードを作成および開始します。
		
		非同期インターフェイスを設定します。非同期インターフェイス コンフィギュレーション モードで使用できるサンプル コマンドについては、「例」（P.6-13）を参照してください。

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

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

	コマンド	目的

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

ステップ 9	`exit`
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

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

ステップ 11	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	例：
	`Router(config)# ip route 0.0.0.0 0.0.0.0 22.0.0.2`
	`Router(config)#`
		ダイヤラ インターフェイスにポイントする IP ルートをデフォルト ゲートウェイとして設定します。

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

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

ステップ 14	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
	
	例：
	`Router(config)# line console 0`
	`Router(config-line)#`
		ライン インターフェイスのコンフィギュレーション モードを開始します。

	コマンド	目的

ステップ 15	**modem enable**
	
	例：
	`Router(config-line)# modem enable`
	`Router(config-line)#`
		ポートをコンソールから AUX ポート機能に変更します。

ステップ 16	exit
	
	例：
	`Router(config-line)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 17	**line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
	
	例：
	`Router(config)# line aux 0`
	`Router(config)#`
		補助インターフェイスのコンフィギュレーション モードを開始します。

ステップ 18	**flowcontrol** {**none** | **software** [**lock**] [**in** | **out**] | **hardware** [**in** | **out**]}
	
	例：
	`Router(config)# flowcontrol hardware`
	`Router(config)#`
		ハードウェア信号フロー制御をイネーブルにします。

例

次の設定例では、インターフェイスの IP アドレスを、PPP および IPCP アドレス ネゴシエーションおよびコンソール ポートを介したダイヤル バックアップによって指定します。

```
!
ip name-server 192.168.28.12
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool 1
 import all
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
! Need to use your own correct ISP phone number.
modemcap entry MY-USER_MODEM:MSC=&F1S0=1
chat-script Dialout ABORT ERROR ABORT BUSY "" "AT" OK "ATDT 5555102\T"
TIMEOUT 45 CONNECT \c
!
!
!
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip tcp adjust-mss 1452
 hold-queue 100 out
!
```

```
! Dial backup and remote management physical interface.
interface Async1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 3
 async default routing
 async dynamic routing
 async mode dedicated
 ppp authentication pap callin
!
interface ATM0
 mtu 1492
 no ip address
 no atm ilmi-keepalive
 pvc 0/35
 pppoe-client dial-pool-number 1
!
! Primary WAN link.
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 ppp authentication pap callin
 ppp pap sent-username account password 7 pass
 ppp ipcp dns request
 ppp ipcp wins request
 ppp ipcp mask request
!
! Dialer backup logical interface.
interface Dialer3
 ip address negotiated
 ip nat outside
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 dialer pool 3
 dialer idle-timeout 60
 dialer string 5555102 modem-script Dialout
 dialer watch-group 1
!
! Remote management PC IP address.
peer default ip address 192.168.2.2
no cdp enable
!
! Need to use your own ISP account and password.
ppp pap sent-username account password 7 pass
ppp ipcp dns request
ppp ipcp wins request
ppp ipcp mask request
!
! IP NAT over Dialer interface using route-map.
ip nat inside source route-map main interface Dialer1 overload
ip nat inside source route-map secondary interface Dialer3 overload
ip classless
!
! When primary link is up again, distance 50 will override 80 if dial backup
! has not timed out. Use multiple routes because peer IP addresses are alternated
! among them when the CPE is connected.
ip route 0.0.0.0 0.0.0.0 64.161.31.254 50
ip route 0.0.0.0 0.0.0.0 66.125.91.254 50
ip route 0.0.0.0 0.0.0.0 64.174.91.254 50
ip route 0.0.0.0 0.0.0.0 63.203.35.136 80
```

```
ip route 0.0.0.0 0.0.0.0 63.203.35.137 80
ip route 0.0.0.0 0.0.0.0 63.203.35.138 80
ip route 0.0.0.0 0.0.0.0 63.203.35.139 80
ip route 0.0.0.0 0.0.0.0 63.203.35.140 80
ip route 0.0.0.0 0.0.0.0 63.203.35.141 80
ip route 0.0.0.0 0.0.0.0 Dialer1 150
no ip http server
ip pim bidir-enable
!
! PC IP address behind CPE.
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
access-list 103 permit ip 192.168.0.0 0.0.255.255 any
!
! Watch multiple IP addresses because peers are alternated
! among them when the CPE is connected.
dialer watch-list 1 ip 64.161.31.254 255.255.255.255
dialer watch-list 1 ip 64.174.91.254 255.255.255.255
dialer watch-list 1 ip 64.125.91.254 255.255.255.255
!
! Dial backup will kick in if primary link is not available
! 5 minutes after CPE starts up.
dialer watch-list 1 delay route-check initial 300
dialer-list 1 protocol ip permit
!
! Direct traffic to an interface only if the dialer is assigned an IP address.
route-map main permit 10
 match ip address 101
 match interface Dialer1
!
route-map secondary permit 10
 match ip address 103
 match interface Dialer3
!
! Change console to aux function.
line con 0
 exec-timedout 0 0
 modem enable
 stopbits 1
line aux 0
 exec-timeout 0 0
 ! To enable and communicate with the external modem properly.
 script dialer Dialout
 modem InOut
 modem autoconfigure discovery
 transport input all
 stopbits 1
 speed 115200
 flowcontrol hardware
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
scheduler max-task-time 5000
end
```

CHAPTER 7

環境および電源管理

Cisco 819 サービス統合型ルータは、環境温度のモニタリングおよび温度のロギングのため、30 秒ごとにルータ本体にセンサーが装備されています。ルータ シャーシの四隅に 4 つのセンサーがあります。さらにシステム アンビエント センサーおよび 3G センサーがあります。

コーナー センサーは次のメッセージを表示します。

- コンソールへのエラー メッセージ：温度範囲が設定されている温度しきい値を外れると、モニタにエラー メッセージを表示します。ルータの異なる SKU ごとに違う温度範囲が設定されています。
  - Cisco 819G（非強化）：0 ～ 60 °C
  - Cisco 819HG（強化）：–25 ～ 75 °C
- SNMP トラップ：syslog メッセージは、温度が指定範囲外の場合に作成されます。
- サーバの「Call Home」機能：サーバの CallHome 機能は、非常に高温または低温になった場合に、Cisco TAC にすでに問い合わせできるようになっています。

コーナー センサーに加えて、システム周囲センサーと 3G センサーでも 30 秒おきに温度をブートフラッシュ メモリに記録されます。

温度が上限しきい値を超えたり、下限しきい値を下回ったりすると、温度情報が不揮発性メモリ領域に保存され、この出力の一部として表示されます。

ルータの動作温度を確認するには、**show environment** コマンドを使用します。または最後に装置の電力使用量および電力消費量を表示するには、このコマンドを使用できます。

次に、**show environment** コマンドの出力例を示します。

```
router# show environment

SYSTEM WATTAGE
===============
 Board Power consumption is: 4.851 W
 Power Supply Loss:  1.149 W
 Total System Power consumption is: 6.000 W


REAL TIME CLOCK BATTERY STATUS
==============================
 Battery OK (checked at power up)

TEMPERATURE STATUS
==================
 Sensor                Current                       High/Low
 Name                  Temperature    Status         Threshold
 --------------------- -------------- -------------- ---------
 Sensor 1              36             Normal         60/0
```

```
Sensor 2              34             Normal         60/0
Sensor 3              40             Normal         60/0
Sensor 4              38             Normal         60/0
System Ambient Sensor 35             Normal         60/0
3G Modem Sensor       33             Normal         85/0

Environmental information last updated 00:00:26 ago
```

（注）　モデムの温度が、非強化バージョンの場合は 85 度まで、強化バージョンでは 90 度まで上がると、警告メッセージが表示されます。温度が 108 度を超えた場合、ルータは自動的にシャットダウンします。

Cisco EnergyWise サポート

Cisco 819 ISR には、電力消費を減らすためのハードウェアおよびソフトウェア機能があります。ハードウェア機能としては、高性能 AC 電源および RAM 選択やクロック ゲーティングなど、省電力機能を内蔵した電気部品があります。詳細については、『*Cisco 819 Integrated Services Router Hardware Installation Guide*』を参照してください。

ソフトウェア機能には、未使用のモジュールの電源を切り、ルータのモジュールおよび周辺機器への未使用のクロックをディセーブルにする電力効率管理機能である Cisco EnergyWise があります。

Cisco 819 ISR で EnergyWise をサポートするには、Cisco IOS Release 15.0(1)M 以降を実行している必要があります。

詳細な設定手順については、『*Cisco EnergyWise Configuration Guide, EnergyWise Phase 1*』および『*Cisco EnergyWise Configuration Guide, EnergyWise Phase 2*』を参照してください。

CHAPTER 8

シリアル インターフェイスの設定

この章では、次の項でシリアル インターフェイス管理の設定について説明します。

Cisco 819 サービス統合型ルータ（ISR）では、同期（デフォルト）および非同期のシリアル インターフェイス プロトコルがサポートされます。

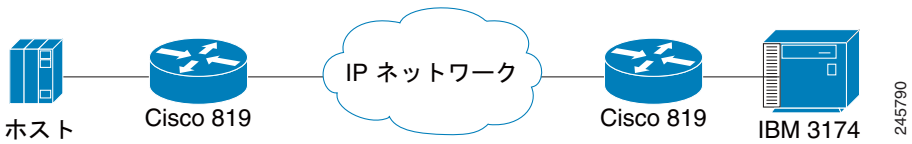
Cisco 819 ISR のシリアル インターフェイスを設定すると、WAN アクセス、レガシー プロトコル転送、コンソール サーバおよびダイヤル アクセス サーバなどのアプリケーションをイネーブルにすることができます。また、リモート ネットワーク管理、外部ダイヤル モデム アクセス、低密度 WAN アグリゲーション、レガシー プロトコル転送および高ポート密度のサポートをイネーブルにします。

シリアル インターフェイスにより、次の機能が実現されます。

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

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

図 8-1　　WAN コンセントレーション

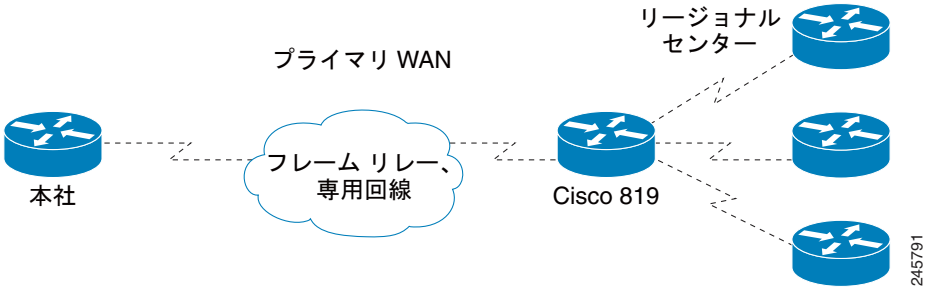


レガシー プロトコル転送

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

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

図 8-2　　ネットワーク コンバージェンス



Cisco 819 ISR では Cisco Smart Serial コネクタを使用します。サポートされているケーブルを表 8-1 に示します。

表 8-1　　Cisco 819 ISR のスマート シリアル ケーブル接続

製品番号	ケーブル タイプ	長さ	コネクタ タイプ
CAB-SS-V35MT	V.35 DTE	10 フィート（3m）	オス型
CAB-SS-V35FC 10 フィート（3m）メス型	V.35 DCE	10 フィート（3m）	メス型
CAB-SS-232MT	EIA/TIA-232 DTE	10 フィート（3m）	オス型
CAB-SS-232FC	EIA/TIA-232 DTE	10 フィート（3m）	メス型
CAB-SS-449MT	EIA/TIA-449 DTE	10 フィート（3m）	オス型
CAB-SS-449FC	EIA/TIA-449 DTE	10 フィート（3m）	メス型
CAB-SS-X21MT	X.21 DTE	10 フィート（3m）	オス型
CAB-SS-X21FC	X.21 DTE	10 フィート（3m）	メス型
CAB-SS-530MT	EIA/TIA-530 DTE	10 フィート（3m）	オス型
CAB-SS-530AMT	EIA/TIA-232 DTE	10 フィート（3m）	オス型

シリアル インターフェイスの設定

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

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

シリアル インターフェイスの設定に関する情報

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

- 「Cisco HDLC カプセル化」（P.8-3）
- 「PPP カプセル化」（P.8-3）
- 「キープアライブ タイマー」（P.8-5）
- 「フレーム リレー カプセル化」（P.8-5）

Cisco HDLC カプセル化

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

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

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

Cisco HDLC は、キープアライブを使用してリンク ステートをモニタリングします（「キープアライブ タイマー」（P.8-5）を参照）。

PPP カプセル化

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

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

PPP は、リンク上で動作するデータ プロトコルのプロパティをネゴシエートする、次のネットワーク制御プロトコル（NCP）を提供します。

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

PPP は、キープアライブを使用してリンク ステートをモニタリングします（「キープアライブ タイマー」（P.8-5）を参照）。

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

- チャレンジ ハンドシェイク認証プロトコル（CHAP）：CHAP は、リモート デバイスにチャレンジ メッセージを送信します。リモート デバイスは、共有秘密を使用してチャレンジの値を暗号化し、暗号化された値とその名前を応答メッセージでローカル ルータに戻します。ローカル ルータは、リモート デバイスの名前をローカル ユーザ名またはリモート セキュリティ サーバ データベース内に保存された関連秘密に一致させようとします。保存された秘密を使用して、元のチャレンジを暗号化し、暗号化された値が一致していることを確認します。
- マイクロソフト チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）：MS-CHAP は CHAP の Microsoft バージョンです。CHAP の標準バージョンと同様に、MS-CHAP は PPP 認証に使用されます。この場合、認証は、Microsoft Windows NT または Microsoft Windows 95 を使用するパーソナル コンピュータとネットワーク アクセス サーバとして機能する Cisco ルータまたはアクセス サーバの間で行われます。
- パスワード認証プロトコル（PAP）：PAP 認証では、ローカル ユーザ名データベース内またはリモート セキュリティ サーバ データベース内の一致するエントリに照らし合わせてチェックする名前とパスワードを送信するために、リモート デバイスが必要です。

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

（注）　PPP 認証をイネーブル化またはディセーブル化しても、ローカル ルータがリモート デバイスに対して自身を認証しようとすることには変わりありません。

マルチリンク PPP

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

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

- 128 バイト、256 バイト、および 512 バイトのフラグメント サイズ
- 長いシーケンス番号（24 ビット）

- 失われたフラグメントの検出タイムアウト期間（80 ms）
- 最小アクティブ リンクの設定オプション
- マルチリンク インターフェイスでの LCP エコー要求および応答のサポート
- フル T1 および E1 フレームおよび非フレーム リンク

キープアライブ タイマー

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

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

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

LCP が ECHOREQ パケットをピアに送信する頻度を設定するには、インターフェイス コンフィギュレーション モードで **keepalive** コマンドを使用します。システムを 10 秒のデフォルト キープアライブ インターバルに戻すには、**keepalive** コマンドを **no** キーワードとともに使用します。キープアライブをディセーブルにするには、**keepalive disable** コマンドを使用します。PPP と Cisco HDLC では、0 のキープアライブはキープアライブをディセーブルにし、**show running-config** コマンド出力では、**keepalive disable** として報告されます。

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

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

フレーム リレー カプセル化

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

- シリアル メイン インターフェイスは、物理インターフェイスおよびポートで構成されます。Cisco HDLC および PPP カプセル化接続をサポートするシリアル インターフェイスを使用していない場合、シリアル メイン インターフェイスの下に相手先固定接続（PVC）があるサブインターフェイスを設定する必要があります。フレーム リレー接続は、PVC でのみサポートされます。
- シリアル サブインターフェイスは、シリアル メイン インターフェイスの下に設定されます。シリアル サブインターフェイスは、シリアル サブインターフェイスの下に PVC を設定するまで、トラフィックをアクティブに伝送しません。レイヤ 3 の設定は、一般的にサブインターフェイス上で行われます。

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

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

シリアル インターフェイスにフレーム リレー カプセル化を設定するには、**encapsulation (Frame Relay VC-bundle)** コマンドを使用します。

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

- Cisco（デフォルト）
- IETF

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

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

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

フレーム リレー インターフェイスでの LMI

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

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

```
(MTU - 13)/8 = PVC の最大数
```

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

シリアル インターフェイスの設定方法

ここでは、次のタスクについて説明します。

同期シリアル インターフェイスの設定

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

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

- 「同期シリアル インターフェイスの指定」（P.8-7）（必須）
- 「同期シリアル カプセル化の指定」（P.8-7）（任意）
- 「PPP の設定」（P.8-9）（任意）
- 「Cisco 819 ISR での同期シリアル ポート アダプタの半二重と Bisync の設定」（P.8-9）（任意）
- 「HDLC データの圧縮の設定」（P.8-9）（任意）
- 「NRZI ライン コーディング フォーマットの使用」（P.8-10）（任意）
- 「内部クロックのイネーブル化」（P.8-10）（任意）
- 「送信クロック信号の反転」（P.8-11）（任意）
- 「送信遅延の設定」（P.8-11）（任意）
- 「DTR 信号パルシングの設定」（P.8-12）（任意）
- 「回線アップ/ダウン インジケータとしての DCD の無視と DSR のモニタリング」（P.8-12）（任意）
- 「シリアル ネットワーク インターフェイス モジュールのタイミングの指定」（P.8-12）（任意）

この章で説明する設定作業の例については、「設定例」（P.8-19）を参照してください。

同期シリアル インターフェイスの指定

同期シリアル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで次のいずれかのコマンドを使用します。

コマンド	目的
`Router(config)# interface serial 0`	インターフェイス コンフィギュレーション モードを開始します。

同期シリアル カプセル化の指定

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

- HDLC

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

カプセル化方式を定義するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

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

デフォルトでは、同期インターフェイスは全二重方式で動作します。半二重モードの SDLC インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

全二重方式のシリアル インターフェイスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

PPP の設定

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

Cisco 819 ISR での同期シリアル ポート アダプタの半二重と Bisync の設定

Cisco 819 ISR の同期シリアル ポート アダプタは、半二重と Bisync をサポートします。Bisync は、半二重アプリケーションのための文字指向のデータリンク層プロトコルです。半二重モードでは、データは一度に 1 つの方向に送信されます。方向は送信要求（RST）およびクリア ツー センド（CTS）制御回線のハンドシェイクによって制御されます。これらについては、「Bisync の設定」（P.8-9）で説明しています。

Bisync の設定

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

HDLC データの圧縮の設定

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

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

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

HDLC で圧縮を設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **encapsulation hdlc**
2. **compress stac**

手順の詳細

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

NRZI ライン コーディング フォーマットの使用

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

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

すべてのシリアル インターフェイスのデフォルト設定は、NRZ フォーマットです。デフォルトは **no nrzi-encoding** です。

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

手順の概要

1. **nrzi-encoding**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**nrzi-encoding**
	
	例：
	`Router(config-if)# nrzi-encoding`
	または
	`Router(config-if)# nrzi-encoding [mark]`
		NRZI 符号化フォーマットをイネーブルにします。
		
		ルータの NRZI 符号化フォーマットをイネーブルにします。

内部クロックのイネーブル化

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

手順の概要

1. **transmit-clock-internal**

手順の詳細

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

送信クロック信号の反転

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

手順の概要

1. **invert txclock**
2. **invert rxclock**

手順の詳細

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

送信遅延の設定

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

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

DTR 信号パルシングの設定

すべてのシリアル インターフェイスにパルシング専用トークン リング（DTR）信号を設定できます。シリアル回線プロトコルがダウンした場合（同期ずれなどの原因による）、インターフェイス ハードウェアはリセットされ、DTR 信号は少なくとも指定された間隔で非アクティブになります。この機能は、DTR 信号のトグリングによって同期をリセットする暗号化デバイスまたは他の同様のデバイスの処理に役立ちます。DTR 信号パルシングを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

一部の構成（SDLC マルチドロップ環境など）では、DCE デバイスは、インターフェイスの活動を妨げる DCD 信号ではなく、データ セット レディ（DSR）信号を送信します。インターフェイスが回線アップ/ダウン インジケータとして DCD 信号ではなく DSR 信号をモニタリングするように設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **ignore-dcd**

手順の詳細

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

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

シリアル ネットワーク インターフェイス モジュールのタイミングの指定

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

DCE が DTE から SCTE を使用するように設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **dce-terminal-timing enable**

手順の詳細

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

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

ルータが TXC クロック信号を反転させるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **dte-invert-txc**

手順の詳細

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

低速シリアル インターフェイスの設定

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

- 「半二重 DTE および DCE ステート マシンの概要」（P.8-14）
- 「同期モードと非同期モードとの間の変更」（P.8-18）

設定例については、「低速シリアル インターフェイスの設定例」（P.8-20）を参照してください。

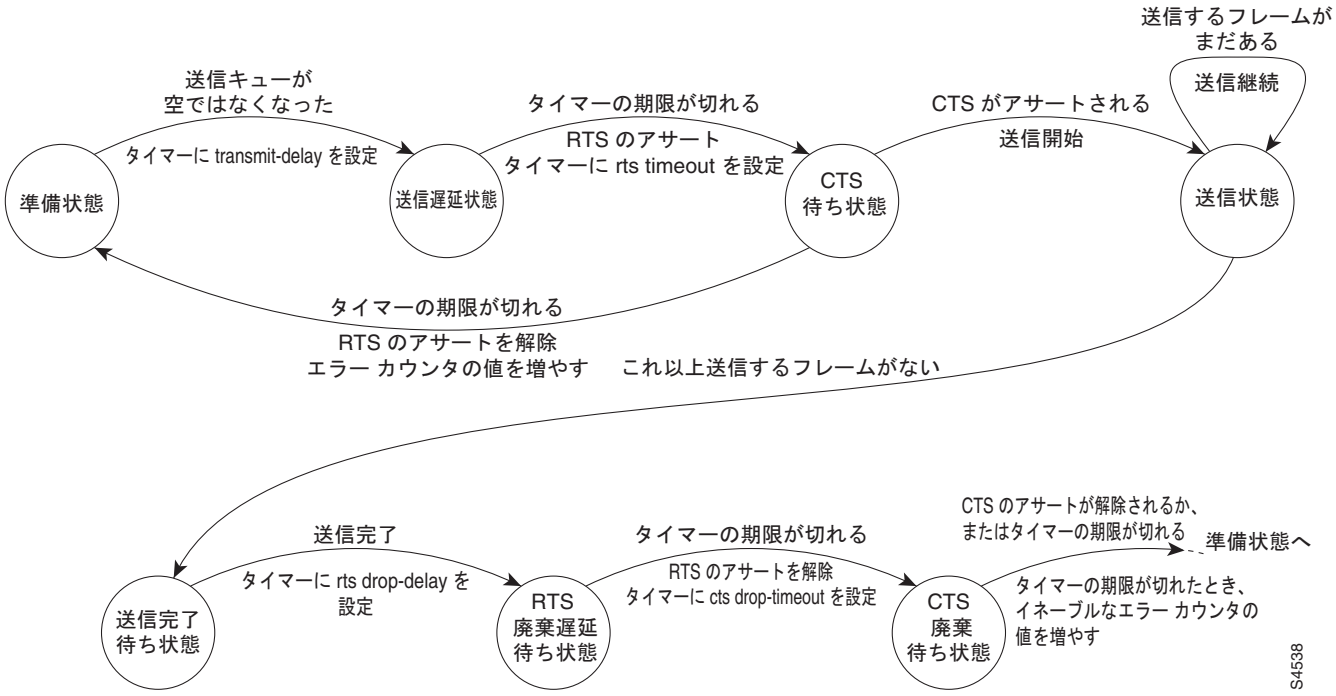
半二重 DTE および DCE ステート マシンの概要

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

半二重 DTE ステート マシン

図 8-3 で説明されているように、低速インターフェイス用の半二重 DTE 送信ステート マシンは、休止されているときには、準備状態のままです。送信のためにフレームが使用可能な場合、ステート マシンは送信遅延状態になり、**half-duplex timer transmit-delay** コマンドで定義された時間の間、待ち状態になります。デフォルトは 0 ミリ秒です。送信遅延は、半二重リンクをデバッグし、バックツーバック フレームを処理できない低速レシーバを補助するために使用されます。

図 8-3　　半二重 DTE 送信ステート マシン



定義されたミリ秒（ms）の間、アイドル状態になった後で、ステート マシンにより、送信要求（RTS）信号がアサートされ、DCE がクリア ツー センド（CTS）待ち状態に変わって CTS がアサートされます。**half-duplex timer rts-timeout** コマンドで設定された値でタイムアウト タイマーが開始されます。

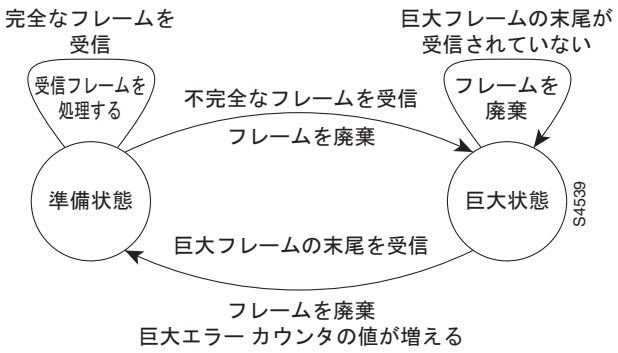
デフォルトは 3 ms です。CTS がアサートされる前にタイムアウト タイマーの期限が切れた場合、ステート マシンは準備状態に戻り、RTS のアサートが解除されます。タイマーが切れる前に CTS がアサートされると、ステート マシンは送信のステートになり、フレームを送信します。

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

RTS ドロップ待ち遅延状態のタイマーの期限が切れると、ステート マシンでは、RTS のアサートが解除され、CTS ドロップ待ち状態に変わります。**half-duplex timer cts-drop-timeout** インターフェイス コマンドで設定された値でタイムアウト タイマーが開始され、ステート マシンでは、CTS のアサート解除を待ちます。デフォルト値は 250 ms です。CTS 信号のアサートが解除されるか、または、タイムアウト タイマーの期限が切れると、ステート マシンは準備状態に戻ります。CTS のアサートが解除される前にタイマーの期限が切れると、エラー カウンタの値が増加します。この値は、該当のシリアル インターフェイスで **show controllers** コマンドを実行すると表示できます。

図 8-4 で説明されているように、低速インターフェイス用の半二重 DTE 受信ステート マシンは、アイドル状態にあり、準備状態でフレームを受信します。巨大フレームは、サイズが最大伝送単位（MTU）を超えるすべてのフレームです。巨大フレームの先頭を受信すると、ステート マシンは巨大状態に代わり、巨大フレームの末尾を受信するまで、フレーム フラグメントは廃棄されます。この時点で、ステート マシンは準備状態に戻り、次のフレームの到達を待ちます。

図 8-4　　半二重 DTE 受信ステート マシン

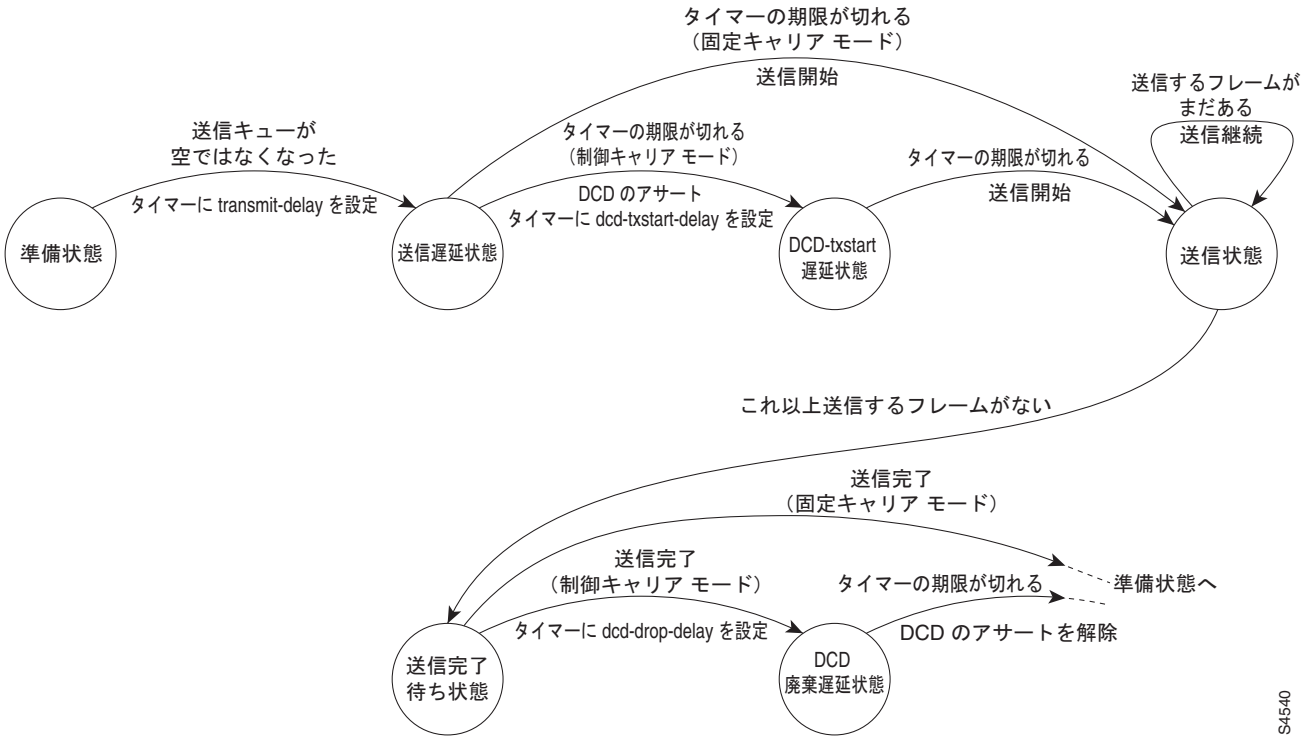


巨大フレームを受信すると、エラー カウンタの値が増やされます。エラー カウンタを表示するには、問題のシリアル インターフェイスで **show interfaces** コマンドを使用します。

半二重 DCE ステート マシン

図 8-5 で説明されているように、DCE モードの低速シリアル インターフェイスでは、半二重 DCE 送信ステート マシンは、休止されているときには、準備状態でアイドルになっています。出力キューが空ではなくなったときなど、シリアル インターフェイスで送信にフレームを使用できる場合、ステート マシンでは（**half-duplex timer transmit-delay** コマンドのミリ秒単位の値に基づいて）タイマーが開始され、送信遅延状態に変わります。DTE 送信状態のマシンと同様、送信遅延状態により、フレームの送信間の遅延を設定するオプションが与えられます。たとえば、この機能を使用すると、高速に継続されて複数フレームが受信されるときに、データを損失した低速レシーバを補うことができます。デフォルトの **transmit-delay** の値は 0 ms です。0 ではない遅延値を指定する場合は、**half-duplex timer transmit-delay** インターフェイス コンフィギュレーション コマンドを使用します。

図 8-5　半二重 DCE 送信ステート マシン



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

インターフェイスが固定キャリア モードの場合、次の状態を経過します。

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

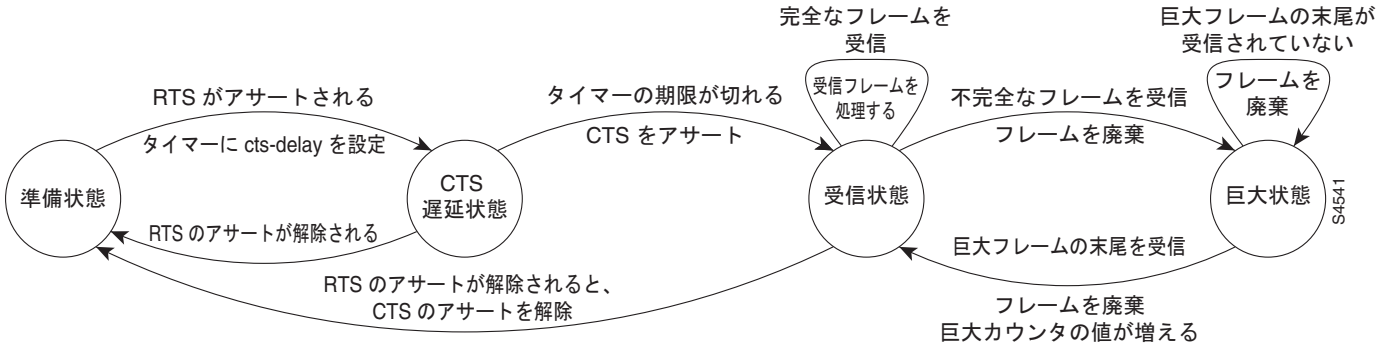
インターフェイスが制御キャリア モードの場合、インターフェイスでは、データ キャリア検出（DCD）信号を使用してハンドシェイクが実行されます。このモードでは、インターフェイスがアイドル状態で、送信するものがない場合に、DCD のアサートが解除されます。送信ステート マシンは、次の状態を経過します。

1. **transmit-delay** タイマーの期限が切れると、DCE によって DCD がアサートされ、DCD-txstart 遅延状態に変わって、DCD のアサーションと送信の開始との間の時間に遅延が生じるようになります。タイマーは、**dcd-txstart-delay** コマンドを使用して指定された値に基づいて、開始されます（このタイマーのデフォルト値は 100 ms です。遅延値を指定するには、**half-duplex timer dcd-txstart-delay** インターフェイス コンフィギュレーション コマンドを使用します）。
2. この遅延タイマーの期限が切れると、ステート マシンが送信状態になり、送信するフレームがなくなるまでフレームが送信されます。

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

図 8-6 で説明されているように、半二重 DCE 受信ステート マシンは、休止されているとき、準備状態でアイドルになっています。DTE によって RTS がアサートされると、この状態から変化します。応答で、**cts-delay** コマンドを使用して指定された値に基づいて、DCE によってタイマーが開始されます。一部の DTE インターフェイスでは、この遅延が想定されているため、このタイマーによって、CTS のアサーションが遅延されます （このタイマーのデフォルト値は 0 ms です。遅延値を指定するには、**half-duplex timer cts-delay** インターフェイス コンフィギュレーション コマンドを使用します）。

図 8-6　　半二重 DCE 受信ステート マシン



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

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

低速シリアル インターフェイスを固定キャリア モードに設定

低速シリアル インターフェイスを制御キャリア モードから固定キャリア モードに戻すには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **no half-duplex controlled-carrier**

手順の詳細

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

半二重タイマーの調整

半二重タイマーのパフォーマンスを最適化するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

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

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

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

- **sdlc cts-delay**
- **sdlc rts-timeout**

同期モードと非同期モードとの間の変更

低速シリアル インターフェイスのモードを同期または非同期のいずれかに指定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

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

手順の詳細

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

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

（注）　シリアル インターフェイス上で非同期モードから同期モードに変更するときには、インターフェイスの状態は、デフォルトで、ダウン状態になります。次にインターフェイスをアップ状態にするには、**no shutdown** オプションを使用する必要があります。

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

- **sdlc cts-delay**
- **sdlc rts-timeout**

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

（注）　このコマンドは物理層コマンドであるため、このコマンドを使用する場合、**show running-config** コマンドと **show startup-config** コマンドの出力には表示されません。

Cisco 2520 ルータから Cisco 2523 ルータで低速シリアル インターフェイスのデフォルト モード（同期）に戻るには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. **no physical-layer**

手順の詳細

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

設定例

インターフェイスイネーブル化の設定例

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

```
interface serial 0
 encapsulation ppp
```

スロット 1 のポート 0 に PPP カプセル化を割り当てている、ルータの同じ例では次のコマンドも必要です。

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

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

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

低速シリアル インターフェイスの設定例

ここでは、低速シリアル インターフェイスの次の設定例について説明します。

- 「同期モードまたは非同期モードの設定例」（P.8-20）
- 「半二重タイマーの設定例」（P.8-20）

同期モードまたは非同期モードの設定例

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

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

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

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

または

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

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

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

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

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

半二重タイマーの設定例

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

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

CHAPTER 9

セキュリティ機能の設定

この章では、Cisco 819 サービス統合型ルータ（ISR）で設定可能な特定のセキュリティ機能を実装するための、シスコの主要なフレームワークである認証、許可、アカウンティング（AAA）の概要について説明します。

この章の内容は、次のとおりです。

認証、許可、アカウンティング

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

AAA は RADIUS、TACACS+、または Kerberos などのプロトコルを使用してセキュリティ機能を管理します。ルータがネットワーク アクセス サーバとして機能している場合、AAA は、ネットワーク アクセス サーバと RADIUS、TACACS+、または Kerberos セキュリティ サーバ間の通信を確立するための手段となります。

AAA サービス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、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』を参照してください。

AutoSecure の設定

AutoSecure 機能は、ネットワーク攻撃に悪用される可能性のある一般的な IP サービスをディセーブルにし、攻撃を受けたときはネットワークの防御に役立つ IP サービスおよび機能をイネーブルにできます。この IP サービスは、1 つのコマンドですべてを同時にディセーブル/イネーブルにすることにより、ルータ上のセキュリティ設定を大幅に簡易化しています。AutoSecure 機能の詳細については、「*AutoSecure*」機能のマニュアルを参照してください。

アクセス リストの設定

アクセス リスト ACL は、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上でネットワーク トラフィックの許可または拒否を行います。アクセス リストは、標準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 リスト作成の詳細については、『*Security Configuration Guide: Access Control Lists, Cisco IOS Release 12.4T*』を参照してください。

アクセス リストは、一般的なタグによってコマンドがバインドされる一連のコマンドです。タグは、番号または名前のどちらかです。表 9-1 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 9-1　アクセス リストのコンフィギュレーション コマンド

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

アクセス リストの作成、調整、および管理については、『*Security Configuration Guide: Access Control Lists, Cisco IOS Release 12.4T*』を参照してください。

アクセス グループ

アクセス グループとは、一般的な名前または番号にバインドされている一連のアクセス リストの定義のことです。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際には、次の点に注意します。

- アクセス リストの定義の順序は重要です。パケットは、最初のアクセス リストから順に照合されます。一致するものがない場合（つまり、許可または拒否が発生しない場合）は、パケットが次のアクセス リストに照合され、さらに次のアクセス リストへと順に進められます。
- パケットが許可または拒否される前に、すべてのパラメータがアクセス リストに一致する必要があります。
- すべてのシーケンスの末尾には、暗黙の「deny all」が付きます。

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

Cisco IOS ファイアウォールの設定

Cisco IOS ファイアウォールでは、ステートフルなファイアウォールを設定できます。ステートフルなファイアウォールでは、パケットが内部的に検査され、ネットワーク接続の状態が監視されます。ステートフル ファイアウォールは、アクセス リストがパケットのストリームに基づくのではなく、個別のパケットに基づいてトラフィックを許可または拒否するだけなので、スタティックなアクセス リストよりも優れています。また、Cisco IOS ファイアウォールはパケットの検査を行うため、アプリケーション層のデータを調べてトラフィックの許可または拒否を判断できます。スタティックなアクセス リストでは、このような検査を行うことはできません。

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

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

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

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

Cisco IOS ファイアウォールの設定に関する追加情報については、『*Securing the Data Plane Configuration Guide Library, Cisco IOS Release 12.4*』を参照してください。

また、Cisco IOS ファイアウォールは、セッション開始プロトコル（SIP）アプリケーションでの音声セキュリティを提供するようにも設定できます。SIP インスペクションは、プロトコルの適合性およびアプリケーションの保護に加え、基本的な検査機能（SIP パケット インスペクションおよびピンホール開口の検出）が提供されます。詳細については、『*Cisco IOS Firewall: SIP Enhancements: ALG and AIC*』を参照してください。

Cisco IOS IPS の設定

Cisco 819 ISR で利用可能な Cisco IOS Cisco IOS 侵入防御システム（IPS）テクノロジーは、セキュリティ ポリシーに違反したり、不正なネットワーク動作を示したりするパケットおよびフローに適切に対処することによって、境界部分のファイアウォール保護を強化します。

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

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

Cisco IOS IPS の設定に関する追加情報については、『*Securing the Data Plane Configuration Guide Library, Cisco IOS Release 12.4*』を参照してください。

URL フィルタリング

Cisco 819 ISR は URL フィルタリングに基づいたカテゴリが提供されます。ユーザは、許可または拒否する Web サイトのカテゴリを選択し、ISR 上で URL フィルタリングを準備します。サード パーティで管理されている外部サーバを使用して、それぞれのカテゴリの URL を調べます。ポリシーの許可および拒否は、ISR 上で保守されています。サービスは加入ベースで提供され、各カテゴリの URL はサードパーティ ベンダーによってメンテナンスされています。

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

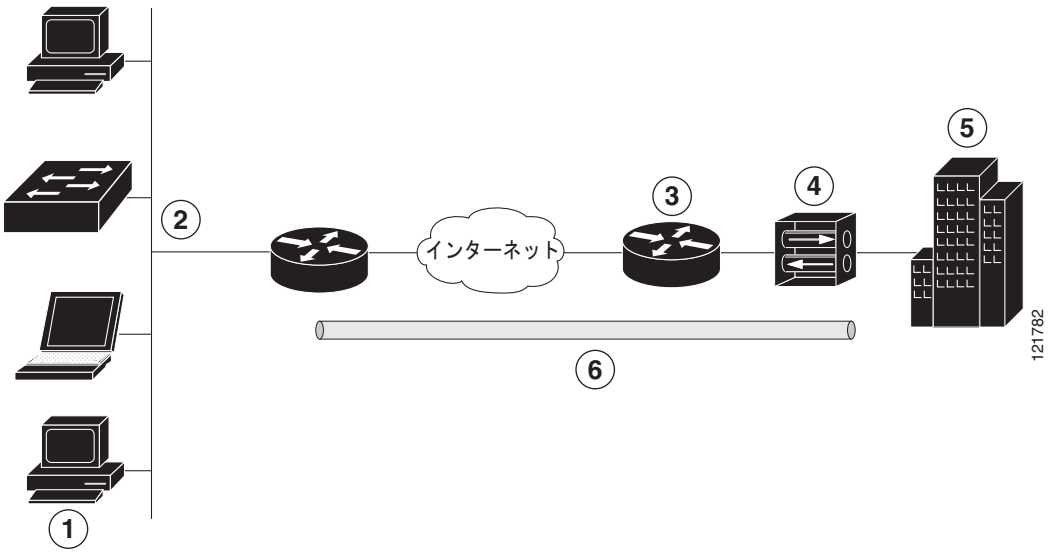
VPN の設定

バーチャル プライベート ネットワーク（VPN）接続を使用すると、インターネットなどのパブリック ネットワーク上で 2 つのネットワーク間のセキュアな接続を実現できます。Cisco 819 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。サイト間 VPN は、ブランチ オフィスとコーポレート オフィスを接続する場合などに使用します。リモート アクセス VPN は、企業ネットワークにログインする際にリモート クライアントによって使用されます。リモート アクセス VPN およびサイト間 VPN の両方についてこのセクションで 2 つの例を挙げて説明します。

リモート アクセス VPN

リモート アクセス VPN コンフィギュレーションでは、Cisco Easy VPN および IP Security（IPSec）トンネルを使用して、リモート クライアントとコーポレート ネットワーク間の接続を設定および保護します。図 9-1 は、一般的な構成例を示します。

図 9-1　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 819 アクセス ルータ
3	ルータ：本社オフィスへのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ（外部インターフェイス アドレスが 210.110.101.1 の Cisco VPN 3000 コンセントレータなど）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

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

Cisco Easy VPN サーバ対応のデバイスでは、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を使用すると、（VPN 3000 シリーズ コンセントレータが配置された）中央サイトのユーザがクライアント サイトのネットワーク リソースにアクセスできます。

IPSec サーバを設定したら、サポート対象の Cisco 819 ISR などの IPSec クライアント上で最小限の設定を行うことにより、VPN 接続を作成できます。IPSec クライアントが VPN トンネル接続を開始すると、IPSec サーバは IPSec ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

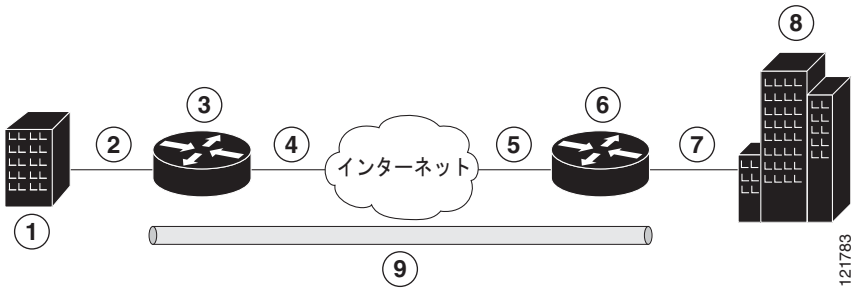
（注）　Cisco Easy VPN クライアント機能に設定できるのは、1 つの宛先ピアだけです。アプリケーションで複数の VPN トンネルを作成する必要がある場合、手動でクライアントおよびサーバ側の両方に IPSec VPN およびネットワーク アドレス変換 / ピア アドレス変換（NAT/PAT）パラメータを設定する必要があります。

Cisco 819 ISR は、Cisco Easy VPN サーバとして動作するように設定することもでき、この機能を使用すると、許可された Cisco Easy VPN クライアントは接続されたネットワークに対してダイナミックな VPN トンネルを確立できます。Cisco Easy VPN サーバの設定については、『*Easy VPN Server*』機能マニュアルを参照してください。

サイト間 VPN

サイト間 VPN の設定では、IPSec 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 9-2 は、一般的な構成例を示します。

図 9-2　IPSec トンネルおよび GRE を使用したサイト間の VPN



1	複数の LAN および VLAN を使用しているブランチ オフィス
2	ファスト イーサネット LAN インターフェイス（NAT 用の内部インターフェイス、アドレスは 192.165.0.0/16）
3	VPN クライアント：Cisco 819 ISR
4	ファスト イーサネット：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：企業ネットワークと接続（内部インターフェイス アドレス 10.1.1.1）
8	コーポレート オフィス ネットワーク
9	GRE を使用した IPSec トンネル

IPSec および GRE の設定の詳細については、『*Secure Connectivity Configuration Guide Library, Cisco IOS Release 12.4T*』を参照してください。

設定例

各例では、「IPSec トンネル上での VPN の設定」（P.9-7）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 819 ISR のエンドポイント設定にだけ適用されます。いずれの VPN 接続も、両端のエンドポイントが適切に機能するように設定されている必要があります。他のルータ モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

VPN コンフィギュレーション情報は、両方のエンドポイントに設定する必要があります。設定する必要のあるパラメータは、内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、およびネットワーク アドレス変換（NAT）などです。

IPSec トンネル上での VPN の設定

IPSec トンネル上に VPN を設定するには、次の作業を行います。

- 「IKE ポリシーの設定」（P.9-7）
- 「グループ ポリシー情報の設定」（P.9-9）
- 「クリプト マップへのモード設定の適用」（P.9-10）
- 「ポリシー ルックアップのイネーブル化」（P.9-11）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.9-12）
- 「IPSec 暗号方式およびパラメータの設定」（P.9-12）
- 「物理インターフェイスへのクリプト マップの適用」（P.9-14）
- 「次の作業」（P.9-14）

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

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

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

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

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

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

ステップ 7	**exit**
	
	例：
	`Router(config-isakmp)# exit`
	`Router(config)#`
		IKE ポリシー 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。

グループ ポリシー情報の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

	コマンドまたはアクション	目的

ステップ 5	**exit**
	
	例：
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		IKE グループ ポリシー 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** | *pool name*} [*low-ip-address* {*high-ip-address*]]
	
	例：
	`Router(config)# ip local pool dynpool 30.30.30.20 30.30.30.30`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

クリプト マップへのモード設定の適用

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

ポリシー ルックアップのイネーブル化

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

手順の概要

1. **aaa new-model**
2. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
3. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
4. **username** *name* {**no password** | **password** *password* | **password** *encryption-type encrypted-password*}

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authentication login** {**default** | *list-name*} *method 1* [*method2...*]
	
	例：
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。
		
		この例では、ローカル認証データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method 1* [*method2...*]
	
	例：
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに許可方式を指定します。
		
		この例では、ローカル許可データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 4	**username** *name* {**no password** | **password** *password* | **password** *encryption-type encrypted-password*}
	
	例：
	`Router(config)# username Cisco password 0 Cisco`
	`Router(config)#`
		ユーザ名をベースとした認証システムを構築します。
		
		この例では、ユーザ名 *Cisco* と暗号化パスワード *Cisco* を指定しています。

IPSec トランスフォームおよびプロトコルの設定

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

IKE ネゴシエーションの実行時に、両ピアは、複数のトランスフォーム セットから両ピアに共通するトランスフォームを検索します。このようなトランスフォームが含まれているトランスフォーム セットが検出された場合は、両方のピアの設定の一部として選択され、保護対象トラフィックに適用されます。

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
	
	例：
	`Router(config)# crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac`
	`Router(config)#`
		トランスフォーム セット（IPSec セキュリティ プロトコル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については、『*Secure Connectivity Configuration Guide Library, Cisco IOS Release 12.4T*』を参照してください。

ステップ 3	**crypto ipsec security-association lifetime {seconds** *seconds* **| kilobytes** *kilobytes***}**
	
	例：
	`Router(config)# crypto ipsec security-association lifetime seconds 86400`
	`Router(config)#`
		IPSec SA ネゴシエーション時のグローバル ライフタイム値を指定します。

IPSec 暗号方式およびパラメータの設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

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

物理インターフェイスへのクリプト マップの適用

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		クリプト マップを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

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

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

次の作業

Cisco Easy VPN リモート コンフィギュレーションを作成する場合は、「Cisco Easy VPN リモート コンフィギュレーションの作成」（P.9-15）を参照してください。

IPSec トンネルおよび GRE を使用してサイト間 VPN を作成する場合は、「サイト間 GRE トンネルの設定」（P.9-18）を参照してください。

Cisco Easy VPN リモート コンフィギュレーションの作成

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

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

手順の概要

1. **crypto ipsec client ezvpn** *name*
2. **group** *group-name* **key** *group-key*
3. **peer** {*ip address* | *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`
	`Router(config-crypto-ezvpn)#`
		Cisco Easy VPN Remote コンフィギュレーションを作成し、Cisco Easy VPN Remote コンフィギュレーション モードを開始します。

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

	コマンドまたはアクション	目的

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

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

ステップ 6	**crypto isakmp keepalive** *seconds*
	
	例：
	`Router(config-crypto-ezvpn)# crypto isakmp keepalive 10`
	`Router(config)#`
		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 fastethernet 4`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定を適用するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
		（注） ATM WAN インターフェイスを使用しているルータの場合、このコマンドは **interface atm 0** になります。

	コマンドまたはアクション	目的

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

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

設定例

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

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

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

```
!

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

サイト間 GRE トンネルの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

	コマンドまたはアクション	目的

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

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

ステップ 5	**crypto map** *map-name*
	
	例：
	`Router(config-if)# crypto map static-map`
	`Router(config-if)#`
		トンネルにクリプト マップを割り当てます。
		（注） トンネル インターフェイスへのダイナミック ルーティングまたはスタティック ルートは、サイト間の接続を確立するために設定しておく必要があります。

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

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

ステップ 8	**permit** *protocol source source-wildcard destination destination-wildcard*
	
	例：
	`Router(config-acl)# permit gre host 192.168.100.1 host 192.168.101.1`
	`Router(config-acl)#`
		発信インターフェイスでは GRE トラフィックだけが許可されるように指定します。

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

設定例

次の設定例は、前述の各項で説明した GRE トンネルのシナリオを使用した VPN のコンフィギュレーション ファイルの一部です。

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

tunnel source fastethernet 0

tunnel destination interface 192.168.101.1

ip route 20.20.20.0 255.255.255.0 tunnel 1

crypto isakmp policy 1
    encryption 3des
    authentication pre-share
    group 2
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond
!
! Defines the key association and authentication for IPsec tunnel.
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 200.1.1.1
!
!
! Defines encryption and transform set for the IPsec tunnel.
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
! Associates all crypto values and peering address for the IPsec tunnel.
crypto map to_corporate 1 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set set1
 match address 105
!
!
```

```
! VLAN 1 is the internal home network.
interface vlan 1
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip inspect firewall in ! Inspection examines outbound traffic.
 crypto map static-map
 no cdp enable
!
! FE4 is the outside or Internet-exposed interface
interface fastethernet 4
 ip address 210.110.101.21 255.255.255.0
 ! acl 103 permits IPsec traffic from the corp. router as well as
 ! denies Internet-initiated traffic inbound.
 ip access-group 103 in
 ip nat outside
 no cdp enable
 crypto map to_corporate ! Applies the IPsec tunnel to the outside interface.
!
! Utilize NAT overload in order to make best use of the
! single address provided by the ISP.
ip nat inside source list 102 interface Ethernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.110.101.1
no ip http server
!
!
! acl 102 associated addresses used for NAT.
access-list 102 permit ip 10.1.1.0 0.0.0.255 any
! acl 103 defines traffic allowed from the peer for the IPsec tunnel.
access-list 103 permit udp host 200.1.1.1 any eq isakmp
access-list 103 permit udp host 200.1.1.1 eq isakmp any
access-list 103 permit esp host 200.1.1.1 any
! Allow ICMP for debugging but should be disabled because of security implications.
access-list 103 permit icmp any any
access-list 103 deny ip any any ! Prevents Internet-initiated traffic inbound.
! acl 105 matches addresses for the IPsec tunnel to or from the corporate network.
access-list 105 permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
no cdp run
```

CHAPTER 10

イーサネット スイッチの設定

この章では、Cisco 819 サービス統合型ルータ（ISR）上に組み込まれているワイヤレス アクセス ポイントに対してサービスを提供する、4 ポート ファスト イーサネット（FE）スイッチと、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。

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

GE スイッチは、ルータと組み込みワイヤレス アクセス ポイントの間の内部インターフェイスを備えた 1000Base T レイヤ 2 ギガビット イーサネット スイッチです。

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

この章の内容は、次のとおりです。

スイッチ ポートの番号付けと命名

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

FE スイッチの制限事項

FE スイッチには次の制限事項があります。

- FE スイッチのポートを、ルータのファスト イーサネット オンボード ポートに接続してはなりません。
- Cisco 819 ISR では、インライン パワーはサポートされていません。
- VTP プルーニングはサポートされません。
- FE スイッチは、最大 200 個の安全な MAC アドレスをサポートできます。

イーサネット スイッチについて

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

VLAN および VLAN トランク プロトコル

VLAN および VLAN トランク プロトコル（VTP）の概念については、「*VLANs*」を参照してください。

レイヤ 2 イーサネット スイッチング

レイヤ 2 イーサネット スイッチングの概念については、「*Layer 2 Ethernet Switching*」を参照してください。

802.1X 認証

802.1x 認証の概念については、「*802.1x Authentication*」を参照してください。

スパニングツリー プロトコル

スパニングツリー プロトコルの概念については、「*Using the Spanning Tree Protocol with the Cisco EtherSwitch Network Module*」を参照してください。

Cisco Discovery Protocol

Cisco Discovery Protocol（CDP）は、シスコ製のすべてのルータ、ブリッジ、アクセス サーバ、スイッチで、レイヤ 2（データリンク層）上で動作します。CDP を使用することにより、ネットワーク管理アプリケーションで、既知装置のネイバーであるシスコ製の装置、特に下位レイヤのトランスペアレント プロトコルを実行しているネイバーを検索することができます。ネットワーク管理アプリケーションは CDP によって、近接装置の装置タイプおよび SNMP エージェント アドレスを学習できます。この機能によって、アプリケーションからネイバー デバイスに SNMP クエリーを送信できます。

CDP は、サブネットワーク アクセス プロトコル（SNAP）をサポートしているすべての LAN および WAN メディア上で動作します。CDP を設定した各デバイスは、マルチキャスト アドレスに対して定期的にメッセージを送信します。各デバイスは、SNMP メッセージを受信できるアドレスを少なくとも 1 つアドバタイズします。アドバタイズには、存続可能時間（ホールドタイム情報）も含まれています。これは、受信側の装置が CDP 情報を破棄せずに保持する時間の長さを示します。

スイッチド ポート アナライザ

スイッチド ポート アナライザの概念については、「*Switched Port Analyzer*」を参照してください。

IGMP スヌーピング

IGMP スヌーピングの概念については、「*IGMP Snooping*」を参照してください。

IGMP バージョン 3

Cisco 819 ISR は、IGMP スヌーピングのバージョン 3 をサポートしています。

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

ストーム制御

ストーム制御の概念については、「*Storm Control*」を参照してください。

フォールバック ブリッジング

フォールバック ブリッジングの概念については、「*Fallback Bridging*」を参照してください。

SNMP MIB の概要

簡易ネットワーク管理プロトコル（SNMP）の開発と使用は、管理情報ベース（MIB）周辺で一元化されます。SNMP MIB は抽象的なデータベースで、管理アプリケーションが特定の形式で読み取りおよび変更できる、情報の概念的な仕様です。これは、情報が同じ形式で管理対象システムに保持されているという意味は含まれません。SNMP エージェントでは、管理対象システムの内部データ構造と形式、および MIB 用に定義された外部データ構造と形式の間で変換が行われます。

SNMP MIB は、概念的には、概念上のテーブルを使用するツリー構造です。シスコのレイヤ 2 スイッチング インターフェイス MIB については、次の項で詳しく説明します。このツリー構造に対して、MIB という用語は 2 つの意味で使用されます。1 つ目の意味では、実際に MIB ブランチであり、通常、伝送メディアまたはルーティング プロトコルなどのテクノロジーの 1 つの側面に関する情報を含みます。この意味で使用される MIB は、正確には MIB モジュールと呼ばれ、通常は 1 つのドキュメントで

定義されます。もう 1 つの意味では、MIB はこのようなブランチの集合です。このような集合体は、たとえば、該当のエージェントによって実装されたすべての MIB モジュール、または、SNMP で定義された MIB モジュールの全体の集まりで構成されます。

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

Cisco 819 4 G LTE ルータでサポートされる MIB の一覧については、『*Configuring Cisco 4G LTE Wireless WAN EHWIC*』の「SNMP MIBs」の項を参照してください。

MIB は、IOS Release 15.2(4)M1 で Cisco 819HGW および Cisco 819HWD SKU をサポートするように変更されました。表 10-1 に、Cisco 819 ISR の MIB を示します。

表 10-1　Cisco 819 ISR の MIB

MIB	MIB のリンク
CISCO-PRODUCTS-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index
CISCO-ENTITY-VENDORTYPE-OID-MIB	
OLD-CISCO-CHASSIS-MIB	
CISCO-WAN-3G-MIB	

レイヤ 2 イーサネット スイッチングの BRIDGE-MIB

レイヤ 2 イーサネット スイッチング インターフェイス BRIDGE-MIB は Cisco 819 プラットフォームでサポートされます。BRIDGE-MIB により、ユーザはイーサネット スイッチ モジュールのメディア アクセス コントロール（MAC）アドレスとスパニングツリー情報を把握することができます。ユーザは、SNMP プロトコルを使用して MIB エージェントを照会し、MAC アドレスなどのイーサネット スイッチ モジュールの詳細や、各インターフェイスおよびスパニング プロトコル情報に関する詳細を取得できます。

ブリッジ MIB は L2 レイヤ BRIDGE-MIB 情報を取得するために次のアプローチを使用します。

- コミュニティ ストリングに基づくアプローチ
- コンテキストに基づくアプローチ

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

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

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

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

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

（注）　VLAN「x」を作成すると、論理エンティティ public@x が追加されます。パブリック コミュニティについてクエリを実行すると、L3 MIB が表示されます。public@x についてクエリを実行すると、VLAN「x」の L2 MIB が表示されます。

コンテキストに基づくアプローチでは、L2 インターフェイスの値を表示するために、SNMP コンテキスト マッピング コマンド使用されます。各 VLAN はコンテキストにマッピングされます。ユーザがコンテキストを使用してクエリを実行すると、MIB は、コンテキストにマッピングされた特定の VLAN のデータを表示します。このアプローチでは、各 VLAN はコンテキストに手動でマッピングされます。

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

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

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

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

（注）　パブリック コミュニティについてクエリを実行すると、L2 MIB が表示されます。L3 MIB のプライベート グループを使用します。

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

MAC アドレス通知

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

MAC アドレス通知の設定については、「*Configuring MAC Address Notification Traps*」を参照してください。

イーサネット スイッチの設定方法

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

VLAN の設定

ここでは、VLAN の設定方法について説明します。Cisco 819 ISR は 2 個の VLAN をサポートし、Cisco 819 ISR は 8 個の VLAN をサポートします。

FE ポート上の VLAN

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

	コマンド	目的
ステップ 1	**interface fe** *port*	設定対象のファスト イーサネット ポートを選択します。
ステップ 2	**shutdown**	（任意）設定が完了するまでトラフィック フローを防止するために、インターフェイスをシャットダウンします。

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

追加情報については、「*Layer 2 LAN Ports*」を参照してください。

GE ポート上の VLAN

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

	コマンド	目的
ステップ 1	**interface** *Wlan-GigabitEthernet0*	設定対象のギガビット イーサネット ポートを選択します。
ステップ 2	**switchport mode trunk**	ポートをトランク モードにします。
ステップ 3	**switchport access vlan** *vlan_id*	（任意）ポートがトランク モードになったら、1 以外の VLAN 番号を割り当てることができます。

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスの設定方法については、「*Configuring Layer 2 Interfaces*」を参照してください。

ここでは、次のトピックについて説明します。

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

802.1x 認証の設定

802.1x ポートベース認証の設定方法については、「*Configuring IEEE 802.1x Port-Based Authentication*」を参照してください。

ここでは、次のトピックについて説明します。

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

スパニングツリー プロトコルの設定

スパニングツリー プロトコルの設定方法については、「*Configuring Spanning Tree*」を参照してください。

ここでは、次のトピックについて説明します。

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

MAC テーブルの操作の設定

MAC テーブルの操作の設定方法については、「*Configuring MAC Table Manipulation*」を参照してください。

ポート セキュリティ

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

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

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

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

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

Cisco Discovery Protocol の設定

Cisco Discovery Protocol（CDP）を設定する方法については、「*Configuring Cisco Discovery Protocol*」を参照してください。

ここでは、次のトピックについて説明します。

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

スイッチド ポート アナライザ（SPAN）の設定

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

ここでは、次のトピックについて説明します。

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

IP マルチキャスト レイヤ 3 スイッチングの設定

IP マルチキャスト レイヤ 3 スイッチングの設定方法については、「*Configuring IP Multicast Layer 3 Switching*」を参照してください。

ここでは、次のトピックについて説明します。

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

IGMP スヌーピングの設定

IGMP スヌーピングの設定方法については、「*Configuring IGMP Snooping*」を参照してください。

ここでは、次のトピックについて説明します。

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

IGMP バージョン 3

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

ポート単位のストーム制御の設定

ポート単位のストーム制御の設定方法については、「*Configuring Per-Port Storm-Control*」を参照してください。

ここでは、次のトピックについて説明します。

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

フォールバック ブリッジングの設定

フォールバック ブリッジングの設定方法については、「*Configuring Fallback Bridging*」を参照してください。

ここでは、次のトピックについて説明します。

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

スイッチの管理

スイッチの管理については、「*Managing the EtherSwitch HWIC*」を参照してください。

ここでは、次のトピックについて説明します。

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

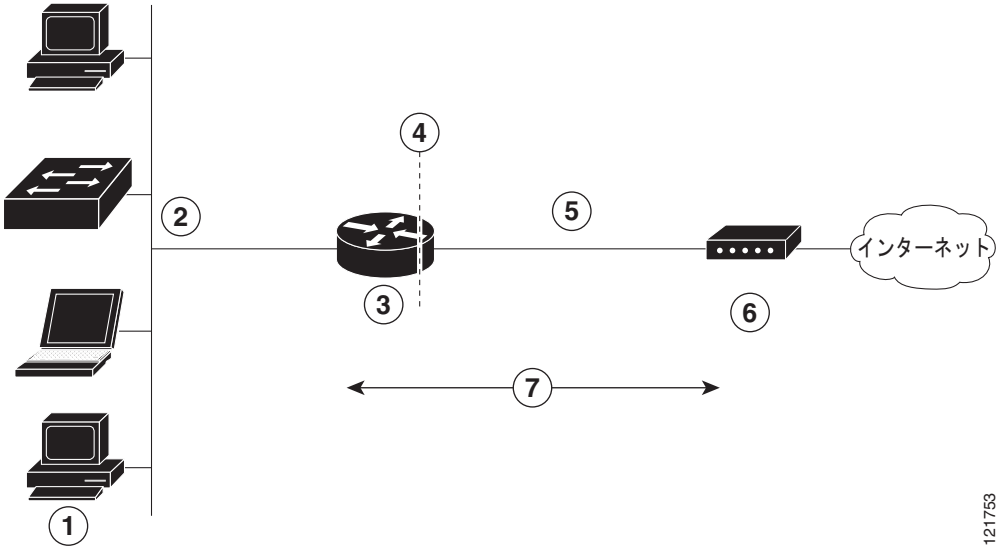
CHAPTER 11

PPP over Ethernet と NAT の設定

この章では、Cisco 819 サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet (PPPoE) クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。

ルータの背後の LAN には、複数の PC を接続できます。これらの PC からのトラフィックは PPPoE セッションに送信する前に暗号化やフィルタリングなどを行うことができます。図 11-1 に、Cisco ルータに PPPoE クライアントと NAT が設定された一般的な配置シナリオを示します。

図 11-1　PPP over Ethernet と NAT



1	複数のネットワーク デバイス：デスクトップ、ラップトップ PC、スイッチ
2	ファスト イーサネット LAN インターフェイス（NAT の内部インターフェイス）
3	PPPoE クライアント：Cisco 819 ISR
4	NAT が実行されるポイント
5	ファスト イーサネット WAN インターフェイス（NAT 用の外部インターフェイス）
6	ケーブル モデムまたはインターネットに接続している他のサーバ
7	クライアントと PPPoE サーバ間の PPPoE セッション

PPPoE

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

PPPoE セッションが Cisco 819 ISR によってクライアント側で開始されます。確立された PPPoE クライアント セッションは、次のいずれかの方法で終了できます。

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

NAT

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

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定」（P.11-2）
- 「ファスト イーサネット WAN インターフェイスの設定」（P.11-3）
- 「ダイヤラ インターフェイスの設定」（P.11-4）
- 「ネットワーク アドレス変換の設定」（P.11-6）

この設定タスクの結果を示す例は「設定例」（P.11-10）に示されています。

バーチャル プライベート ダイヤルアップ ネットワーク グループ番号の設定

バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）を設定すると、複数のクライアントが 1 つの IP アドレスを使用してルータを介して通信できるようになります。

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

手順の概要

1. **vpdn enable**
2. **vpdn-group** *name*
3. **request-dialin**
4. **protocol** {**l2tp** | **pppoe**}

5. **exit**
6. **exit**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**vpdn enable**
	
	例：
	`Router(config)# vpdn enable`
	`Router(config)#`
		ルータで VPDN をイネーブルにします。

ステップ 2	**vpdn-group** *name*
	
	例：
	`Router(config)# vpdn-group 1`
	`Router(config-vpdn)#`
		VPDN グループを作成し、カスタマーまたは VPDN プロファイルに関連付けます。

ステップ 3	**request-dialin**
	
	例：
	`Router(config-vpdn)# request-dialin`
	`Router(config-vpdn-req-in)#`
		ダイヤリング方向を示す request-dialin VPDN サブグループを作成し、トンネルを開始します。

ステップ 4	**protocol** {**l2tp** | **pppoe**}
	
	例：
	`Router(config-vpdn-req-in)# protocol pppoe`
	`Router(config-vpdn-req-in)#`
		VPDN サブグループが確立できるセッションのタイプを指定します。

ステップ 5	**exit**
	
	例：
	`Router(config-vpdn-req-in)# exit`
	`Router(config-vpdn)#`
		request-dialin VPDN グループのコンフィギュレーションを終了します。

ステップ 6	**exit**
	
	例：
	`Router(config-vpdn)# exit`
	`Router(config)#`
		VPDN の設定を終了し、グローバル コンフィギュレーション モードに戻ります。

ファスト イーサネット WAN インターフェイスの設定

このシナリオでは、PPPoE クライアント（Cisco ルータ）が、内部および外部の 10/100 Mbps イーサネット インターフェイスを介して通信します。

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

手順の概要

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

	コマンド	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		ファスト イーサネット WAN インターフェイスに対するインターフェイス コンフィギュレーション モードを開始します。

ステップ 2	**pppoe-client dial-pool-number** *number*
	
	例：
	`Router(config-if)# pppoe-client`
	`dial-pool-number 1`
	`Router(config-if)#`
		PPPoE クライアントを設定し、クローニングに使用するダイヤラ インターフェイスを指定します。

ステップ 3	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		ファスト イーサネット インターフェイスとそれに対して行った設定変更をイネーブルにします。

ステップ 4	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ファスト イーサネット インターフェイスのコンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

ダイヤラ インターフェイスの設定

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

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

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	目的

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

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

ステップ 3	**ip mtu** *bytes*
	
	例：
	`Router(config-if)# ip mtu 1492`
	`Router(config-if)#`
		IP 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`
	`Router(config-if)#`
		送受信中のデータ パケットに対するカプセル化タイプを PPP に設定します。

ステップ 5	**ppp authentication** {*protocol1* [*protocol2...*]}
	
	例：
	`Router(config-if)# ppp authentication chap`
	`Router(config-if)#`
		PPP 認証方式をチャレンジ ハンドシェイク認証プロトコル（CHAP）に設定します。
		
		このコマンドと設定可能な追加パラメータについては、『*Cisco IOS Security Command Reference*』を参照してください。

	コマンド	目的

ステップ 6	**dialer pool** *number*
	
	例：
	`Router(config-if)# dialer pool 1`
	`Router(config-if)#`
		特定の宛先サブネットワークへの接続に使用するダイヤラ プールを指定します。

ステップ 7	**dialer-group** *group-number*
	
	例：
	`Router(config-if)# dialer-group 1`
	`Router(config-if)#`
		ダイヤラ グループ（1 ～ 10）にダイヤラ インターフェイスを割り当てます。
		
		ヒント ダイヤラ グループを使用して、ルータへのアクセスを制御します。

ステップ 8	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ダイヤラ 0 インターフェイスの設定を終了します。

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

ステップ 10	**ip route** *prefix mask* {*interface-type interface-number*}
	
	例：
	`Router(config)# ip route 10.10.25.2 255.255.255.255 dialer 0`
	`Router(config)#`
		ダイヤラ 0 インターフェイスのデフォルト ゲートウェイに IP ルートを設定します。
		
		このコマンドと設定可能な追加パラメータについては、『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.2* 』および『*Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols, Release 12.3*』を参照してください。

ネットワーク アドレス変換の設定

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

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

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	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`
	`Router(config)#`
		NAT 用のグローバル IP アドレスのプールを作成します。

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

ステップ 3	**interface** *type number*
	
	例：
	`Router(config)# interface vlan 1`
	`Router(config-if)#`
		NAT の内部インターフェイスにする VLAN（ファスト イーサネット LAN インターフェイス（FE0–FE3）が存在する）に対して、コンフィギュレーション モードを開始します。

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

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

	コマンド	目的

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

ステップ 7	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		NAT の外部インターフェイスとするファスト イーサネット WAN インターフェイス（FE4 または NAT）に対して、コンフィギュレーション モードを開始します。

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

ステップ 9	**no shutdown**
	
	例：
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		イーサネット インターフェイスに対する設定変更をイネーブルにします。

ステップ 10	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		ファスト イーサネット インターフェイスに対するコンフィギュレーション モードを終了します。

ステップ 11	**access-list** *access-list-number* {**deny** | **permit**} **source** [*source-wildcard*] **例：** `Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0`	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） NAT を仮想テンプレート インターフェイスで使用する場合は、ループバック インターフェイスを設定する必要があります。ループバック インターフェイスの設定の詳細については、「ルータの基本設定」（P.5-1）を参照してください。

NAT コマンドの詳細については、Cisco IOS Release 12.3 のマニュアル セットを参照してください。NAT の概念についての一般的な説明は、「Cisco IOS ソフトウェアの基礎知識」（P.A-1）を参照してください。

設定例

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

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

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

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
interface FastEthernet 4
no ip address
no ip directed-broadcast (default)
ip nat outside
pppoe enable group global
pppoe-client dial-pool-number 1
no sh
!
interface dialer 0
ip address negotiated
ip mtu 1492
encapsulation ppp
ppp authentication chap
dialer pool 1
dialer-group 1
!
dialer-list 1 protocol ip permit
ip nat inside source list 1 interface dialer 0 overload
ip classless (default)
ip route 10.10.25.2 255.255.255.255 dialer 0
ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0
ip nat inside source list acl1 pool pool1
!
```

設定の確認

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

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

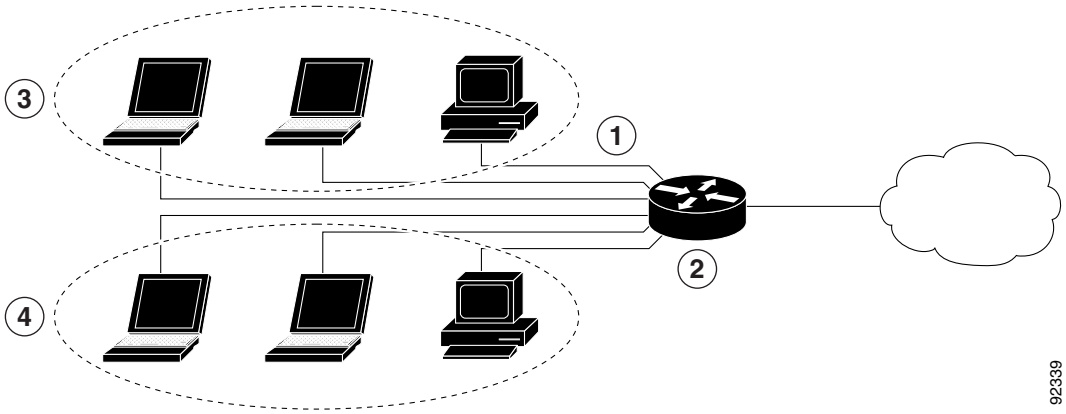
CHAPTER 12

DHCP および VLAN による LAN の設定

Cisco 819 サービス統合型ルータ（ISR）は、物理 LAN および仮想 LAN（VLAN）の両方でクライアントをサポートしています。各ルータはダイナミック ホスト コンフィギュレーション プロトコル（DHCP）を使用して、このようなネットワーク上にある各ノードに対して、IP 設定の自動割り当てをイネーブルにできます。

図 12-1 に、ルータおよび 2 つの VLAN を介して接続された 2 つの物理 LAN の一般的な構成例を示します。

図 12-1　Cisco ルータで DHCP が設定された物理および仮想 LAN



1	ファスト イーサネット LAN（複数のネットワーク デバイス）
2	インターネットに接続されたルータおよび DHCP サーバ（Cisco 819 ISR）
3	VLAN 1
4	VLAN 2

DHCP

DHCP は、RFC 2131 に説明されているように、アドレス割り当てにクライアント/サーバ モデルを採用しています。管理者は、Cisco 800 シリーズ ルータを DHCP サーバとして動作するように設定できます。この場合、IP アドレスの割り当てと他の TCP/IP 関連の設定情報をワーク ステーションに提供します。DHCP を使用すると、IP アドレスを各クライアントに手動で割り当てるという作業を省くことができます。

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

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

VLAN

Cisco 819 ルータは VLAN を設定できる 4 つのファスト イーサネット ポートをサポートします。

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

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- 「DHCP の設定」（P.12-2）
- 「VLAN の設定」（P.12-5）

（注）　この章の各手順では、ルータの基本機能、NAT による PPPoE または PPPoA をすでに設定していることを前提とします。これらの設定作業を実行していない場合は、使用しているルータに応じて、「ルータの基本設定」（P.5-1）、および「Easy VPN および IPSec トンネルを使用した VPN の設定」（P.13-1）を参照してください。

DHCP の設定

DHCP 動作用にルータを設定するには、グローバル コンフィギュレーション モードから始め、次の手順を実行します。

手順の概要

1. **ip domain name** *name*
2. **ip name-server** *server-address1* [*server-address2...server-address6*]
3. **ip dhcp excluded-address** *low-address* [*high-address*]
4. **ip dhcp pool** *name*
5. **network** *network-number* [*mask* | *prefix-length*]
6. **import all**
7. **default-router** *address* [*address2...address8*]
8. **dns-server** *address* [*address2...address8*]
9. **domain-name** *domain*
10. **exit**

手順の詳細

	コマンド	目的

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

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

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

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

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

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

ステップ 7	**default-router** *address* [*address2...address8*]
	
	例：
	`Router(config-dhcp)# default-router 10.10.10.10`
	`Router(config-dhcp)#`
		DHCP クライアントのデフォルト ルータを最大 8 つまで指定します。

	コマンド	目的

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

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

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

設定例

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

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

DHCP 設定の確認

DHCP 設定を表示するには、次のコマンドを使用します。

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

```
Router# show ip dhcp import
Address Pool Name: dpool1

Router# show ip dhcp pool
Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
```

```
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0

Router# show ip dhcp server statistics
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

VLAN の設定

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

手順の概要

1. **vlan ?**
2. **ISL VLAN** *ID*
3. **exit**

手順の詳細

	コマンド	目的

ステップ 1	**vlan ?**
	例：
	`Router# config t`
	`Router(config)# vlan database?`
	
	`WORD  ISL VLAN IDs 1-4094`
	`accounting  VLAN accounting configuration`
	`ifdescr  VLAN subinterface ifDescr`
	
	`Router(config)# vlan 2`
		VLAN コンフィギュレーション モードを開始します。

ステップ 2	**ISL VLAN** *ID*
	
	例：
	`Router(config)#vlan 2`
	`Router(config-vlan)#`
		VLAN を追加します（識別番号の範囲は 1 ～ 4094）。
		このコマンドと設定可能な追加パラメータについては、『*Cisco IOS Switching Services Command Reference*』を参照してください。

ステップ 3	**exit**
	
	例：
	`Router(config-vlan)# exit`
	`Router(config)#`
		VLAN データベースを更新し、それを管理ドメイン全体に伝播して、グローバル コンフィギュレーション モードに戻ります。

VLAN へのスイッチ ポートの割り当て

VLAN にスイッチ ポートを割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

手順の概要

1. **interface** *switch port id*
2. **switchport access vlan** *vlan-id*
3. **end**

手順の詳細

	コマンド	目的

ステップ 1	**interface** *switch port id*
	
	例：
	`Router(config)# interface FastEthernet 2`
	`Router(config-if)#`
		VLAN に割り当てるスイッチ ポートを指定します。

ステップ 2	**switchport access vlan** *vlan-id*
	
	例：
	`Router(config-if)# switchport access vlan 2`
	`Router(config-if)#`
		VLAN にポートを割り当てます。

ステップ 3	**end**
	
	例：
	`Router(config-if)# end`
	`Router#`
		インターフェイス モードを終了し、特権 EXEC モードに戻ります。

VLAN コンフィギュレーションの確認

VLAN コンフィギュレーションを表示するには、次のコマンドを使用します。

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

```
Router# vlan database
Router(vlan)# show

  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Translational Bridged VLAN: 1002
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 2
    Name: VLAN0002
    Media Type: Ethernet
    VLAN 802.10 Id: 100002
    State: Operational
    MTU: 1500

  VLAN ISL Id: 3
    Name: red-vlan
    Media Type: Ethernet
    VLAN 802.10 Id: 100003
    State: Operational
    MTU: 1500

  VLAN ISL Id: 1002
    Name: fddi-default
    Media Type: FDDI
    VLAN 802.10 Id: 101002
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1003

  VLAN ISL Id: 1003
    Name: token-ring-default
    Media Type: Token Ring
    VLAN 802.10 Id: 101003
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Ring Number: 0
    Bridge Number: 1
    Parent VLAN: 1005
    Maximum ARE Hop Count: 7
    Maximum STE Hop Count: 7
    Backup CRF Mode: Disabled
    Translational Bridged VLAN: 1
    Translational Bridged VLAN: 1002

  VLAN ISL Id: 1004
    Name: fddinet-default
    Media Type: FDDI Net
    VLAN 802.10 Id: 101004
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

  VLAN ISL Id: 1005
    Name: trnet-default
```

```
    Media Type: Token Ring Net
    VLAN 802.10 Id: 101005
    State: Operational
    MTU: 1500
    Bridge Type: SRB
    Bridge Number: 1
    STP Type: IBM

Router# show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0, Fa1, Fa3
2    VLAN0002                         active    Fa2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
```

CHAPTER 13

Easy VPN および IPSec トンネルを使用した VPN の設定

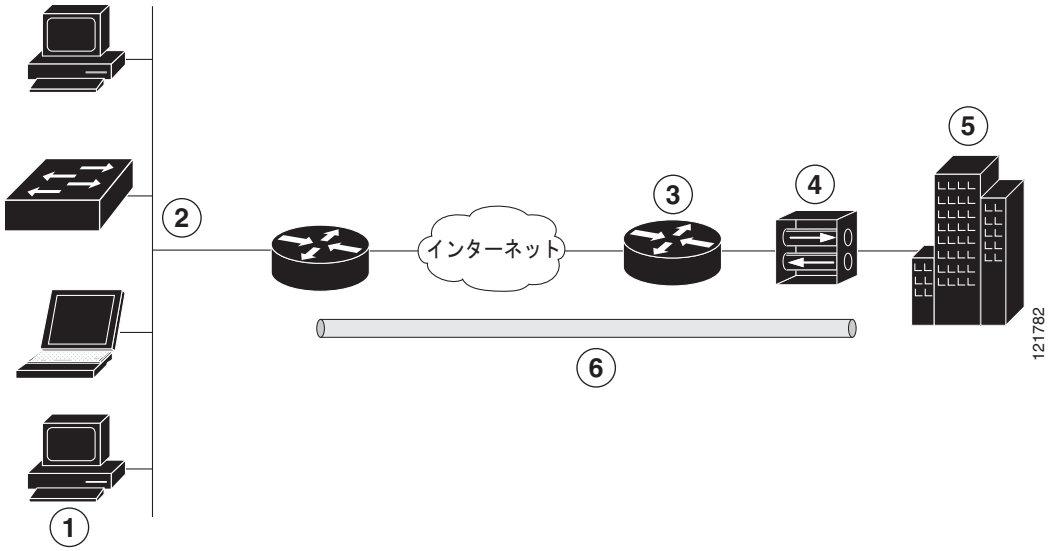
この章では、Cisco 819 サービス統合型ルータ（ISR）で設定できるバーチャル プライベート ネットワーク（VPN）の作成の概要について説明します。

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

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

この章の例は、Cisco Easy VPN と IPSec トンネルを使用してリモート クライアントと企業ネットワーク間の接続を設定し、セキュアにするリモート アクセス VPN の構成を示しています。図 13-1 は、一般的な構成例を示します。

図 13-1　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 819 ISR
3	ルータ：本社オフィスへのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

Cisco Easy VPN

Cisco Easy VPN クライアント機能を使用し、Cisco Unity Client プロトコルを実装することにより、面倒な設定作業が大幅に削減されます。このプロトコルでは、内部 IP アドレス、内部サブネット マスク、DHCP サーバ アドレス、WINS サーバ アドレス、およびスプリットトンネリング フラグなど、ほとんどの VPN パラメータを IPSec サーバとして機能している VPN サーバで定義できます。

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

Cisco Easy VPN クライアント機能は、クライアント モードとネットワーク拡張モードの 2 つのモードのいずれかに設定できます。デフォルト設定はクライアント モードで、クライアント サイトの装置だけが中央サイトのリソースにアクセスできます。クライアント サイトのリソースは、中央サイトでは利用できません。ネットワーク拡張モードでは、中央サイトのユーザはクライアント サイトのネットワーク リソースにアクセスできます。

IPSec サーバを設定したら、サポート対象の Cisco 819 ISR などの IPSec クライアント上で最小限の設定を行うことにより、VPN 接続を作成できます。IPSec クライアントが VPN トンネル接続を開始すると、IPSec サーバは IPSec ポリシーを IPSec クライアントに転送し、対応する VPN トンネル接続を作成します。

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

設定作業

このネットワーク シナリオのルータを設定するには、次の作業を実行します。

- 「IKE ポリシーの設定」（P.13-3）
- 「グループ ポリシー情報の設定」（P.13-5）
- 「クリプト マップへのモード設定の適用」（P.13-6）
- 「ポリシー ルックアップのイネーブル化」（P.13-7）
- 「IPSec トランスフォームおよびプロトコルの設定」（P.13-8）
- 「IPSec 暗号方式およびパラメータの設定」（P.13-9）
- 「物理インターフェイスへのクリプト マップの適用」（P.13-11）
- 「Easy VPN リモート コンフィギュレーションの作成」（P.13-11）

この設定タスクの結果を示す例は「設定例」（P.13-13）で提供されます。

（注）　この章の手順では、基本的なルータ機能と、NAT、DCHP、および VLAN を使用した PPPoE または PPPoA がすでに設定されていることを前提とします。これらの設定作業を実行していない場合、「ルータの基本設定」（P.5-1）を参照してください。

（注）　この章の例は、Cisco 819 ルータのエンドポイント設定だけを示しています。いずれの VPN 接続も、両端のエンドポイントが適切に機能するように設定されている必要があります。他のルータ モデルでの VPN 設定については、必要に応じてソフトウェア コンフィギュレーション マニュアルを参照してください。

IKE ポリシーの設定

インターネット キー交換（IKE）を設定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

手順の概要

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

6. **lifetime** *seconds*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

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

	コマンドまたはアクション	目的

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

ステップ 7	**exit**
	
	例：
	`Router(config-isakmp)# exit`
	`Router(config)#`
		IKE ポリシー 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。

グループ ポリシー情報の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

	コマンドまたはアクション	目的

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

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

ステップ 5	**exit**
	
	例：
	`Router(config-isakmp-group)# exit`
	`Router(config)#`
		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`
	`Router(config)#`
		グループのローカル アドレス プールを指定します。
		このコマンドの詳しい説明およびその他の設定可能なパラメータについては、『*Cisco IOS Dial Technologies Command Reference*』を参照してください。

クリプト マップへのモード設定の適用

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

ポリシー ルックアップのイネーブル化

AAA を使用してポリシー ルックアップをイネーブルにするには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

ステップ 2	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
	
	例：
	`Router(config)# aaa authentication login rtr-remote local`
	`Router(config)#`
		選択したユーザのログイン時の AAA 認証を指定し、使用する方式を指定します。
		
		この例では、ローカル認証データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

ステップ 3	**aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access** | **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
	
	例：
	`Router(config)# aaa authorization network rtr-remote local`
	`Router(config)#`
		PPP を含むすべてのネットワーク関連サービス要求の AAA 許可を指定してから、さらに許可方式を指定します。
		
		この例では、ローカル許可データベースを使用します。RADIUS サーバを使用することもできます。詳細については、『*Securing User Services Configuration Guide Library, Cisco IOS Release 12.4T*』および『*Cisco IOS Security Command Reference*』を参照してください。

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

IPSec トランスフォームおよびプロトコルの設定

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

IKE ネゴシエーションの実行時に、両ピアは、複数のトランスフォーム セットから両ピアに共通するトランスフォームを検索します。このようなトランスフォーム セットが検出された場合は、それが選択され、両方のピアの設定の一部として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 セットとプロトコルを指定するには、グローバル コンフィギュレーション モードを開始し、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

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

IPSec 暗号方式およびパラメータの設定

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

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

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

物理インターフェイスへのクリプト マップの適用

クリプト マップは、IP セキュリティ（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 モードを開始し、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		クリプト マップを適用するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

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

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

Easy VPN リモート コンフィギュレーションの作成

IPSec リモート ルータとして機能するルータは、Easy VPN リモート コンフィギュレーションを作成し、発信インターフェイスに割り当てる必要があります。

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

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. **interface** *type number*
7. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
8. **exit**

手順の詳細

	コマンドまたはアクション	目的

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

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

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

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

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

	コマンドまたはアクション	目的

ステップ 6	**interface** *type number*
	
	例：
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定を適用するインターフェイスで、インターフェイス コンフィギュレーション モードを開始します。
		（注） ATM WAN インターフェイスを使用しているルータの場合、このコマンドは **interface atm 0** になります。

ステップ 7	**crypto ipsec client ezvpn** *name* [**outside** | **inside**]
	
	例：
	`Router(config-if)# crypto ipsec client ezvpn ezvpnclient outside`
	`Router(config-if)#`
		Cisco Easy VPN リモートの設定を WAN インターフェイスに関連付けます。これにより、ルータは VPN 接続に必要な NAT またはポート アドレス変換（PAT）、およびアクセス リストの設定を自動的に作成します。

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

Easy VPN の設定の検証

次の例では、Easy VPN の接続を確認します。

```
Router# show crypto ipsec client ezvpn

Tunnel name :ezvpnclient
Inside interface list:vlan 1
Outside interface:fastethernet 4
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

設定例

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

```
!
aaa new-model
!
aaa authentication login rtr-remote local
aaa authorization network rtr-remote local
aaa session-id common
!
username Cisco password 0 Cisco
!
crypto isakmp policy 1
    encryption 3des
    authentication pre-share
```

```
    group 2
    lifetime 480
!
crypto isakmp client configuration group rtr-remote
    key secret-password
    dns 10.50.10.1 10.60.10.1
    domain company.com
    pool dynpool
!
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
!
crypto ipsec security-association lifetime seconds 86400
!
crypto dynamic-map dynmap 1
    set transform-set vpn1
    reverse-route
!
crypto map static-map 1 ipsec-isakmp dynamic dynmap
crypto map dynmap isakmp authorization list rtr-remote
crypto map dynmap client configuration address respond

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

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

APPENDIX A

Cisco IOS ソフトウェアの基礎知識

Cisco IOS ソフトウェアの使用方法について理解しておくと、ルータの設定を効率的に行うことができます。この付録では、次の内容で基礎知識について説明します。

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

- 「ルータの基本設定」（P.5-1）

PC からのルータの設定

コンソール ポート経由で接続された PC からルータを設定するには、端末エミュレーション ソフトウェアを使用します。PC はこのソフトウェアを使用して、ルータにコマンドを送信します。表 A-1 に、実行しているオペレーティング システムに応じて使用できる一般的な種類の端末エミュレーション ソフトウェアをいくつか示します。

表 A-1　端末エミュレーション ソフトウェアの種類

PC オペレーティング システム	端末エミュレーション ソフトウェア
Windows 95、Windows 98、Windows 2000、Windows NT、Windows XP	HyperTerm（Windows ソフトウェアに組み込まれています）、ProComm Plus
Windows 3.1	Terminal（Windows ソフトウェアに組み込まれています）
Macintosh	ProComm、VersaTerm

端末エミュレーション ソフトウェアを使用して、PC に接続されているルータの設定を変更できます。PC がルータと対話できるようにするため、ソフトウェアを次の標準 VT-100 エミュレーション設定に合わせて設定してください。

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

この設定は、ご使用のルータのデフォルト設定に一致する必要があります。ルータのボー、データ ビット、パリティ、またはストップ ビットの設定を変更するには、ROM モニタのパラメータを再設定する必要があります。詳細については、「ROM モニタ」（P.C-1）を参照してください。ルータ フロー制御設定を変更するには、グローバル コンフィギュレーション モードで **flowcontrol** コマンドを使用します。

ルータを設定するためにグローバル コンフィギュレーション モードを開始する手順については、「グローバル コンフィギュレーション モードの開始」（P.A-6）を参照してください。

コマンド モードの概要

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

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

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

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

表 A-2　コマンド モードの概要

モード	アクセス方法	プロンプト	モードの終了および開始	モードの用途
ユーザ EXEC	ルータ セッションを開始します。	`Router>`	ルータ セッションを終了するには、**logout** コマンドを入力します。	このモードは次の場合に使用します。 • 端末の設定変更 • 基本テストの実行 • システム情報の表示
特権 EXEC	ユーザ EXEC モードから **enable** コマンドを入力します。	`Router#`	• ユーザ EXEC モードに戻る場合は、**disable** コマンドを入力します。 • グローバル コンフィギュレーション モードを開始するには、**configure** コマンドを入力します。	このモードは次の場合に使用します。 • ルータの動作パラメータを設定する。 • このマニュアルで説明されている確認手順を実行する。 ルータ コンフィギュレーションに対する不正な変更を防ぐため、「イネーブル シークレット パスワードおよびイネーブル パスワード」（P.A-6）の手順に説明されているようにパスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードから **configure** コマンドを入力します。	`Router (config)#`	• 特権 EXEC モードに戻る場合は、**exit** または **end** コマンドを入力するか、Ctrl+Z を押します。 • インターフェイス コンフィギュレーション モードを開始するには、**interface** コマンドを入力します。	このモードは、ルータにグローバルに適用するパラメータを設定する目的で使用します。 このモードからは次のモードにアクセスできます。 • インターフェイス コンフィギュレーション • ルータ コンフィギュレーション • ライン コンフィギュレーション

表 A-2　コマンド モードの概要 （続き）

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

ヘルプの表示

コマンド入力の補助手段として、疑問符（?）および矢印キーを使用できます。

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

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

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

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

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

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

↑キーを押すと、直前に入力したコマンドが再表示されます。↑キーを押し続けると、さらに前に入力したコマンドにさかのぼって、順に表示されます。

イネーブル シークレット パスワードおよびイネーブル パスワード

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

パスワードの設定には、次の 2 つのコマンドを使用します。

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

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

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

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

グローバル コンフィギュレーション モードの開始

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

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

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

```
Router> enable
```

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

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

```
Password: enable_password
Router#
```

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

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

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

この時点でルータ コンフィギュレーションの変更を行うことができます。

コマンドの使用方法

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

コマンドの短縮形

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

```
Router # sh v
```

コマンドの取り消し

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

コマンドライン エラー メッセージ

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

表 A-3　CLI の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
`% Ambiguous command: "show con"`	ルータがコマンドとして認識できる十分な文字数を入力していません。	コマンドを再入力し、最後に疑問符（**?**）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに入力できる利用可能なキーワードが表示されます。

表 A-3　CLI の代表的なエラー メッセージ （続き）

エラー メッセージ	意味	ヘルプの表示方法
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドを再入力し、最後に疑問符（**?**）を入力します。コマンドと疑問符の間にはスペースを入れません。 コマンドとともに入力できる利用可能なキーワードが表示されます。
% Invalid input detected at '^' marker.	コマンドの入力ミスです。エラーのある位置に、カレット記号（^）が表示されます。	疑問符（**?**）を入力して、このコマンド モードで使用できるコマンドをすべて表示します。

変更した設定の保存

コンフィギュレーションの変更内容を NVRAM に保存して、システムのリロード時または停電時に消失しないようにするには、**copy running-config startup-config** コマンドを入力する必要があります。次に、このコマンドを使用して変更を保存する例を示します。

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

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

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

```
Building configuration...
Router#
```

サマリー

以上、Cisco IOS ソフトウェアの基本事項について学習したため、ルータの設定作業を開始することができます。以下に留意してください。

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

次の作業

ルータを設定する場合は、「ルータの基本設定」（P.5-1）に進みます。

次の作業

APPENDIX B

概要

この付録では、インターネット サービス プロバイダーまたはネットワーク管理者が Cisco ルータを設定する際に役立つ機能の概要について説明します。

この付録に記載されている内容は、次のとおりです。

ネットワーク プロトコル

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

IP

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

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

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

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

ルーティング プロトコルのオプション

ルーティング プロトコルには次のものがあります。

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

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

表 B-1　RIP と EIGRP の比較

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

RIP

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

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

EIGRP

EIGRP は、シスコ独自仕様による高度なディスタンス ベクタおよびリンク ステート ルーティング プロトコルであり、距離（ホップ カウント）よりも洗練されたメトリックに基づいてルートを選択します。EIGRP は、後継ルータ（ルーティング ループを形成しないことが保証され、宛先までのコスト パスが最小になる近接ルータ）を基準とするメトリックを使用します。特定の宛先への後継ルータが存在しないにもかかわらず、近接ルータが宛先をアドバタイズしている場合、ルータはルートを再計算しなければなりません。

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

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

PPP 認証プロトコル

ポイントツーポイント プロトコル（PPP）は、ポイントツーポイント リンクを介して送信されるネットワーク層プロトコル情報をカプセル化します。

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

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

- パスワード認証プロトコル（PAP）
- チャレンジ ハンドシェイク認証プロトコル（CHAP）

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

PAP

PAP は双方向のハンドシェイクを使用して、ルータ間のパスワードを検証します。PAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。PPP リンクが確立された後、リモート オフィス ルータは、本社オフィス ルータが認証を受け付けるまで、設定されているユーザ名およびパスワードの送信を繰り返します。

PAP の特徴は、次のとおりです。

- 認証のパスワード部分は、リンク上をクリア テキストで送信されます（スクランブル処理または暗号化は行われません）。
- PAP では、プレイバック攻撃または反復的な総当り攻撃からの保護機能が提供されません。

- 認証試行の頻度およびタイミングは、リモート オフィス ルータが制御します。

CHAP

CHAP は 3 ウェイ ハンドシェイクを使用して、パスワードを検証します。CHAP の仕組みを理解するために、リモート オフィスのシスコ ルータが本社オフィスのシスコ ルータに接続されているネットワーク トポロジを例にとります。

PPP リンクが確立された後、本社オフィス ルータはリモート オフィス ルータに対し、チャレンジ メッセージを送信します。リモート オフィス ルータは可変の値で応答します。本社オフィス ルータは、独自に計算した値と照らし合わせて、この応答をチェックします。両方の値が一致していれば、本社オフィス ルータは認証を受け付けます。リンクを確立した後は、いつでも認証プロセスを繰り返すことができます。

CHAP の特徴は、次のとおりです。

- 認証プロセスでは、パスワードではなく、可変のチャレンジ値を使用します。
- CHAP は、一意の予測不可能な可変のチャレンジ値の使用により、プレイバック攻撃から保護します。チャレンジの反復により、1 回の攻撃にさらされる時間を限定します。
- 認証試行の頻度およびタイミングは、本社オフィス ルータが制御します。

（注）　2 つのプロトコルのうち、より安全性の高い CHAP の使用を推奨します。

TACACS+

Cisco 819 ルータは、Telnet を介して Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。TACACS+ は、リモート アクセス認証およびイベント ロギングなどの関連ネットワーク セキュリティ サービスを提供するシスコ独自の認証プロトコルです。ユーザ パスワードは、個々のルータではなく中央のデータベースで管理されます。TACACS+ は、ルータごとに設定された、別個のモジュールである認証、許可、アカウンティング（AAA）ファシリティもサポートします。

イーサネット

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

イーサネット CSMA/CD メディアアクセス プロセスでは、CSMA/CD LAN 上のすべてのホストはいつでもネットワークにアクセスできます。データを送信する前に、CSMA/CD ホストはネットワークを通過するトラフィックを待ち受けます。データを送信するホストは、トラフィックが検出されなくなるまで待機してから、データを送信します。イーサネットでは、ネットワーク上をデータが流れていない場合、ネットワーク上のすべてのホストがデータを送信できます。トラフィックを待ち受けていた 2 台のホストがトラフィックを検出せず、同時にデータを送信すると、衝突が発生します。衝突が発生すると両方の送信内容が破壊されるため、ホストは後で再送信する必要があります。衝突したホストがいつ再送信を行うかは、アルゴリズムによって決まります。

ダイヤル バックアップ

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

- 「バックアップ インターフェイス」（P.B-5）
- 「フローティング スタティック ルート」（P.B-5）
- 「ダイヤラ ウォッチ」（P.B-5）

バックアップ インターフェイス

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

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

フローティング スタティック ルート

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

ダイヤラ ウォッチ

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

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

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

NAT

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

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

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

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

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

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

Easy IP（フェーズ 1）

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

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

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

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

Easy IP（フェーズ 2）

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

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

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

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

QoS

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

- 「IP Precedence」（P.B-8）
- 「PPP フラグメンテーションおよびインターリーブ」（P.B-8）
- 「CBWFQ」（P.B-8）
- 「RSVP」（P.B-9）
- 「低遅延キューイング」（P.B-9）

QoS は、ATM、イーサネットおよび IEEE 802.1 ネットワーク、これらの基本テクノロジーの一部またはすべてを使用した IP ルーテッド ネットワークなど、さまざまなテクノロジーを介して、選択されたネットワーク トラフィックに対し、より優れたサービスを提供するためのネットワーク機能です。QoS の主な目的は、専用帯域幅の確保、ジッタおよび遅延の制御（一部のリアルタイム トラフィックおよび対話型トラフィックで必要）、および損失特性の改善です。QoS テクノロジーは、キャンパス、WAN、およびサービス プロバイダー ネットワークの今後のビジネス用途に対応するための基本的な構成単位を提供します。

音声ネットワークのパフォーマンスを高めるには、VoIP が稼働しているルータだけでなく、ネットワーク全体に QoS を設定する必要があります。すべての QoS テクニックがすべてのネットワーク ルータに適しているわけではありません。ネットワーク内のエッジ ルータとバックボーン ルータは、必ず

しも同じ動作をするわけではありません。同様に、実行する QoS の作業もそれぞれ異なる場合があります。リアルタイム音声トラフィックに対応するように IP ネットワークを設定するには、ネットワーク内のエッジ ルータとバックボーン ルータの両方の機能を検討する必要があります。

QoS ソフトウェアを使用すると、複雑なネットワークにおいて、さまざまなネットワーク アプリケーションおよびトラフィック タイプを制御し、予測どおりに処理することができます。ほとんどすべてのネットワークは、小規模企業ネットワーク、インターネット サービス プロバイダー、エンタープライズ ネットワークのいずれであるかに関係なく、QoS を利用して効率を最適化できます。

IP Precedence

IP precedence を使用すると、最大 6 つのサービス クラスにトラフィックを分類できます（他の 2 つのクラスは、内部ネットワーク用に予約されています）。ネットワークに適用されたキューイング テクノロジーは、この信号を使用して処理を促進することができます。

ポリシーベース ルーティングや 専用アクセス レート（CAR）などの機能を使用すると、拡張アクセス リスト分類に基づいて優先順位を設定できます。これにより、アプリケーションまたはユーザ別、宛先および送信元サブネット別など、優先順位をきわめて柔軟に割り当てることができます。通常、この機能は可能な限りネットワーク（または管理ドメイン）のエッジ付近に配備されるため、これ以降のネットワーク要素は決定されたポリシーに基づいてサービスを提供できます。

オプションの信号方式を使用している場合は、ホストまたはネットワーク クライアントに IP Precedence を設定することもできます。IP precedence を使用すると、既存ネットワーク キューイング メカニズム（クラスベース均等化キューイング（CBWFQ）など）を使用して、サービス クラスを確立できます。既存アプリケーションの変更の必要性や複雑なネットワーク要件はありません。

PPP フラグメンテーションおよびインターリーブ

マルチクラス マルチリンク PPP インターリーブにより、大きいパケットをマルチリンクでカプセル化し、リアルタイム音声トラフィックの遅延条件を満たす小さいパケットに分割することができます。もともと小さいリアルタイム パケットは、マルチリンクでカプセル化されず、大きいパケットのフラグメントの合間に伝送されます。インターリーブ機能はさらに、小型で遅延に敏感なパケット用に特殊な送信キューを提供するので、そのようなパケットを他のフローより先に送信できます。インターリーブ機能は、他のベスト エフォート型トラフィックに使用される低速リンク上で、遅延に敏感な音声パケットに遅延限度を設定します。

マルチリンク PPP インターリーブは、通常、CBWFQ および RSVP または IP Precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、マルチリンク PPP インターリーブおよび CBWFQ を使用します。音声パケットにプライオリティを設定する場合は、リソース予約プロトコル（RSVP）または IP precedence を使用します。

CBWFQ

通常、CBWFQ はマルチリンク PPP インターリーブおよび RSVP または IP Precedence と組み合わせて使用し、音声パケットの配信を保証します。データの管理方法を定義する場合は、CBWFQ とマルチリンク PPP を組み合わせて使用します。音声パケットにプライオリティを設定する場合は、RSVP または IP Precedence を使用します。

ATM キューと Cisco IOS キューの 2 つのキューイング レベルがあります。CBWFQ は Cisco IOS キューに適用されます。PVC が作成されると、ファーストイン ファーストアウト（FIFO）Cisco IOS キューが自動的に作成されます。CBWFQ を使用してクラスを作成し、それらを PVC に関連付けると、クラスごとにキューが作成されます。

CBWFQ により、キューに十分な帯域幅が確保され、トラフィックは予測どおりのサービスを受けます。小容量トラフィック ストリームが優先されます。大容量トラフィック ストリームに残りの容量が分配され、同等または比例配分された帯域幅が与えられます。

RSVP

RSVP を使用すると、ルータはインターフェイス上に十分な帯域幅を確保して、信頼性および品質性能を高めることができます。RSVP により、エンド システムはネットワークに特定の QoS を要求できます。リアルタイム音声トラフィックには、ネットワークの一貫性が不可欠です。一貫した QoS が得られなかった場合、リアルタイム トラフィックにジッター、帯域幅不足、遅延変動、または情報損失が生じる可能性があります。RSVP は、最新のキューイング メカニズムと連動します。予約がどのように実行されるかは、インターフェイス キューイング メカニズム（CBWFQ など）に依存します。

RSVP は、PPP、HDLC、および同様なシリアル回線インターフェイス上で適切に動作します。マルチアクセス LAN 上では、適切に動作しません。RSVP は、パケット フローに関するダイナミック アクセス リストと同様のものと考えることができます。

ネットワークに次の条件が存在する場合は、RSVP を設定して QoS を保証する必要があります。

- 小規模な音声ネットワークの実装
- 2 Mbps 未満のリンク
- 使用率の高いリンク
- 可能なかぎり最良の音質を必要とする場合

低遅延キューイング

低遅延キューイング（LLQ）は、リアルタイム トラフィック用の低遅延完全優先送信キューを提供します。完全プライオリティ キューを使用すると、（他のキュー内のパケットがキューから取り出される前に）最初に遅延に敏感なデータをキューから取り出して送信することにより、遅延に敏感なデータを他のトラフィックよりも優先的に処理することができます。

アクセス リスト

基本的な標準アクセス リストおよびスタティック拡張アクセス リストを使用すると、**permit** コマンドにキーワードを指定して、セッション フィルタリングと同様の処理を行うことができます。指定されたキーワードは、ACK または RST ビットが設定されているかどうかに基づいて、TCP パケットをフィルタリングします （ACK または RST ビットが設定されているパケットはセッション内の最初のパケットではないため、このパケットは確立されたセッションに属します）。このフィルタ基準は、インターフェイスに永久的に適用されるアクセス リストの一部になります。

APPENDIX C

ROM モニタ

ROM モニタ ファームウェアは、ルータの電源投入時またはリセット時に起動します。このファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムのブートを助けます。ROM モニタを使用して、忘れてしまったパスワードの回復やコンソール ポートでのソフトウェアのダウンロードなど、特定の設定作業を実行できます。ルータに Cisco IOS ソフトウェア イメージがロードされていない場合、ROM モニタがルータを実行します。

この付録の構成は、次のとおりです。

ROM モニタの設置

ROM モニタを使用するには、端末または PC をコンソール ポート経由でルータに接続している必要があります。

次に再起動するときは ROM モニタ モードで起動するようにルータを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	**enable**	特権 EXEC モードを開始します。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**config-reg 0x0**	コンフィギュレーション レジスタをリセットします。

	コマンド	目的
ステップ 4	**exit**	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**reload**	新しいコンフィギュレーション レジスタ値でルータを再起動します。ルータは ROM モニタ モードのままで、Cisco IOS ソフトウェアを起動しません。 設定値が 0x0 である限り、コンソールから手動でオペレーティング システムを起動する必要があります。「コマンドの説明」（P.C-3）の **boot** コマンドを参照してください。 再起動したルータは ROM モニタ モードになります。新しく行が増えるごとにプロンプトの数字が増加します。

ワンポイント アドバイス　ルータを再起動してから 60 秒間は、コンフィギュレーション レジスタで Break（システム割り込み）がオフに設定されていても、Break が常に有効となります。再起動から 60 秒間のあいだに Break キーを押すと、ROM モニタのプロンプトに割り込むことができます。

ROM モニタ コマンド

次にコマンドラインに入力する必要があるコマンドを表示するには、**?** ROM モニタ プロンプトに ? または **help** を入力すると、次のように、使用できるコマンドおよびオプションの一覧が表示されます。

```
rommon 1 > ?
alias             set and display aliases command
boot              boot up an external process
break             set/show/clear the breakpoint
confreg           configuration register utility
cont              continue executing a downloaded image
context           display the context of a loaded image
cookie            display contents of cookie PROM in hex
copy              Copy a file-copy [-b <buffer_size>] <src_file> <dst_file>
delete            Delete file(s)-delete <filenames ...>
dir               List files in directories-dir <directory>
dis               display instruction stream
dnld              serial download a program module
format            Format a filesystem-format <filessystem>
frame             print out a selected stack frame
fsck              Check filesystem consistency-fsck <filesystem>
help              monitor builtin command help
history           monitor command history
meminfo           main memory information
mkdir             Create dir(s)-mkdir <dirnames ...>
more              Concatenate (type) file(s)-cat <filenames ...>
rename            Rename a file-rename <old_name> <new_name>
repeat            repeat a monitor command
reset             system reset
rmdir             Remove a directory
set               display the monitor variables
stack             produce a stack trace
sync              write monitor environment to NVRAM
sysret            print out info from last system return
tftpdnld          tftp image download
unalias           unset an alias
unset             unset a monitor variable
xmodem            x/ymodem image download
```

コマンドの大文字と小文字は区別されます。端末上で Break キーを押すとコマンドを停止できます。PC を使用している場合、Ctrl キーと Break キーを同時に押すと、ほとんどの端末エミュレーション プログラムはコマンドを停止します。別のタイプの端末エミュレータまたは端末エミュレーション ソフトウェアを使用している場合は、該当製品のマニュアルに記載された **Break** コマンドの送信方法を参照してください。

コマンドの説明

表 C-1 に、一般的に使用される ROM モニタ コマンドを示します。

表 C-1　一般的な ROM モニタ コマンド

コマンド	説明
help または **?**	使用できるすべての ROM モニタ コマンドを表示します。

-?	次のような、コマンド構文に関する情報を表示します。
	`rommon 16 > dis -?`
	`usage : dis [addr] [length]`
	
	このコマンドの出力は、**xmodem** ダウンロード コマンドの出力とわずかに異なります。
	`rommon 11 > xmodem -?`
	`xmodem: illegal option -- ?`
	`usage: xmodem [-cyrxu] <destination filename>`
	`-c  CRC-16`
	`-y  ymodem-batch protocol`
	`-r  copy image to dram for launch`
	`-x  do not launch on download completion`
	`-u  upgrade ROMMON, System will reboot after upgrade`

reset または **i**	ルータをリセットまたは初期化します。電源投入に似ています。

dir *device***:**	指定したデバイス（フラッシュ メモリ ファイルなど）上のファイルがリストされます。
	`rommon 4 > dir flash:`
	`Directory of flash:/`
	`2 -rwx 10283208 <date> c880-advsecurityk9-mz`
	`9064448 bytes available (10289152 bytes used)`

ブート コマンド	ROM モニタの boot コマンドを詳細については、『*Cisco IOS Configuration Fundamentals and Network Management Guide*』を参照してください。
b	フラッシュ メモリ内の最初のイメージをブートします。
b flash: [*filename*]	フラッシュ メモリの最初のパーティションからイメージを直接ブートします。ファイル名を入力しないと、フラッシュ メモリ内の最初のイメージがブートされます。

TFTP ダウンロードによるディザスタ リカバリ

ルータに新しいソフトウェアをロードするには、通常、Cisco IOS ソフトウェアのコマンドライン インターフェイス（CLI）から **copy tftp flash** 特権 EXEC コマンドを実行します。ただし、ルータが Cisco IOS ソフトウェアをブートできない場合は、ROM モニタ モード中に新しいソフトウェアをロードすることができます。

ここでは、リモート TFTP サーバからルータのフラッシュ メモリに Cisco IOS ソフトウェア イメージをロードする方法について説明します。**tftpdnld** コマンドを実行すると、ルータに新しいソフトウェア イメージをダウンロードする前にフラッシュ メモリ内のすべての既存データが消去されるため、このコマンドはディザスタ リカバリの場合にだけ使用してください。

TFTP ダウンロードのコマンド変数

ここでは、ROM モニタ モードで設定し、TFTP ダウンロード プロセスで使用するシステム変数について説明します。必須変数とオプション変数があります。

（注） ここに記載されたコマンドは大文字と小文字の区別があり、表記どおり正確に入力する必要があります。

必須の変数

tftpdnld コマンドを使用する前に、次のコマンドを使用して、次に示す変数を設定する必要があります。

変数	コマンド
GE WAN の設定	**FE_PORT**=4
スイッチ ポートの設定	**FE_PORT=**{0-3}
ルータの IP アドレス	**IP_ADDRESS**=*ip_address*
ルータのサブネット マスク	**IP_SUBNET_MASK**=*ip_address*
ルータのデフォルト ゲートウェイの IP アドレス	**DEFAULT_GATEWAY=*ip_address***
ソフトウェアのダウンロード元となる TFTP サーバの IP アドレス	**TFTP_SERVER**=*ip_address*
ルータにダウンロードするファイルの名前	**TFTP_FILE**=*filename*

オプションの変数

次の変数は、**tftpdnld** コマンドを使用する前に各コマンドで設定できます。

変数	コマンド
ファイル ダウンロードの進行状況をどのように表示するかを設定します。 0：進行状況は表示されません。 1：感嘆符（!!!）でファイル ダウンロードの進行状況を表示します。これがデフォルト設定です。 2：ファイル ダウンロードの処理中に詳細な進行状況を表示します。例を示します。 • Initializing interface. • Interface link state up. • ARPing for 1.4.0.1 • ARP reply for 1.4.0.1 received.MAC address 00:00:0c:07:ac:01	**TFTP_VERBOSE**=*setting*
ルータが ARP および TFTP ダウンロードを試行する回数。デフォルト値は 7 です。	**TFTP_RETRY_COUNT=***retry_times*
ダウンロード プロセスがタイムアウトするまでの時間（秒）です。デフォルトは 2400 秒（40 分）です。	**TFTP_TIMEOUT**=*time*
ダウンロードされたイメージに対してルータがチェックサム テストを実行するかどうか。 1：チェックサム テストを実行します。 0：チェックサム テストを実行しません。	**TFTP_CHECKSUM**=*setting*

TFTP ダウンロード コマンドの使用

TFTP を使用してファイルをダウンロードするには、ROM モニタ モードで次の手順を実行します。

ステップ 1　適切なコマンドを使用して、上記のすべての必須変数およびオプション変数を入力します。

ステップ 2　次のように、**tftpdnld** コマンドを入力します。

```
rommon 1 > tftpdnld -r
```

（注）　**-r** 変数は任意です。この変数を入力すると、新しいソフトウェアがダウンロードされ、ブートされますが、ソフトウェアはフラッシュ メモリに保存されません。次回に **reload** を入力した場合は、フラッシュ メモリ内のイメージを使用することができます。

次のような出力が表示されます。

```
IP_ADDRESS: 10.3.6.7
IP_SUBNET_MASK: 255.255.0.0
DEFAULT_GATEWAY: 10.3.0.1
TFTP_SERVER: 192.168.254.254
TFTP_FILE: c880-advsecurityk9-mz
Do you wish to continue? y/n:  [n]:
```

ステップ 3　継続する場合は、出力内の質問に対して **y** を入力します。

```
Do you wish to continue? y/n:  [n]:y
```

ルータが新しいファイルのダウンロードを開始します。

誤って y を入力した場合、**Ctrl+C** または **Break** を入力するとフラッシュ メモリを消去する前に転送を止めることができます。

例

次に、WAN インターフェイスを使用した TFTP のサポートの設定例を示します。

```
rommon 1 >
rommon 1 >
rommon 1 > set
PS1=rommon ! >
RTC_STAT=0
GE_SPEED_MODE=4
LICENSE_BOOT_LEVEL=advipservices,all:c800;
WARM_REBOOT=FALSE
TFTP_SERVER=209.165.200.225
IP_SUBNET_MASK=255.255.255.224
DEFAULT_GATEWAY=209.165.200.225
IP_ADDRESS=209.165.200.226
TFTP_FILE=c800-universalk9-mz.SPA.152-3.16.M0.1
FE_PORT=4
?=0
RELOAD_TYPE=1
CRASHINFO=flash:crashinfo_20120406-133436-UTC
BSI=0
RANDOM_NUM=683383170
RET_2_RTS=22:51:49 UTC Fri Jul 13 2012
RET_2_RCALTS=1342219899
rommon 2 >
rommon 2 >
rommon 2 > tftpdnld -r

          IP_ADDRESS: 209.165.200.225
      IP_SUBNET_MASK: 255.255.255.224
     DEFAULT_GATEWAY: 209.165.200.225
         TFTP_SERVER: 209.165.200.225
           TFTP_FILE: c800-universalk9-mz.SPA.152-3.16.M0.1
        TFTP_MACADDR: 00:22:bd:ec:23:f4
    TFTP_DESTINATION: flash:
        TFTP_VERBOSE: Progress
    TFTP_RETRY_COUNT: 18
        TFTP_TIMEOUT: 7200
       TFTP_CHECKSUM: Yes
             FE_PORT: 4
.......
```

```
Receiving c800-universalk9-mz.SPA.152-3.16.M0.1 from 209.165.200.225
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
File reception completed.
IOS Image Load Test
___________________
Digitally Signed Production Software

Validating checksum.

loading image c800-universalk9-mz.SPA.152-3.16.M0.1
program load complete, entry point: 0x4000000, size: 0x307eeb0
Self decompressing the image :
##########################################################################################
##########################################################################################
##########################################################################################
##########################################################################################
################################################################### [OK]
*** No sreloc section
Smart Init is enabled
smart init is sizing iomem
                 TYPE      MEMORY_REQ
    Onboard devices &
         buffer pools      0x020ECEC0
-----------------------------------------------
               TOTAL:      0x020ECEC0

Rounded IOMEM up to: 32Mb.
Using 3 percent iomem. [32Mb/896Mb]

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706

Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.2(3.16)M0.1,
MAINTENANCE INTERIM SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 07-Jun-12 04:44 by prod_rel_team

WDC is not configured
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
```

```
export@cisco.com.

Installed image archive
Cisco C819HGW+7-A-A-K9 (revision 4.0) with 883788K/33715K bytes of memory.
Processor board ID FAC15455YYZ
4 FastEthernet interfaces
2 Gigabit Ethernet interfaces
1 Serial(sync/async) interface
2 terminal lines
1 Virtual Private Network (VPN) Module
1 Cellular interface
1 cisco Embedded AP (s)
DRAM configuration is 32 bits wide
255K bytes of non-volatile configuration memory.
961128K bytes of ATA System CompactFlash (Read/Write)

Press RETURN to get started!

*Jan  2 00:00:02.391: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c800
Next reboot level = advipservices and License = advipservices
*Jul 13 23:00:20.435: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State changed to:
Initialized
*Jul 13 23:00:20.515: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State changed to:
Enabled
*Jul 13 23:00:24.431: c3600_scp_set_dstaddr2_idb(184)add = 0 name is Wlan-GigabitEthernet0
*Jul 13 23:00:41.395: %LINEPROTO-5-UPDOWN: Line protocol on Interface wlan-ap0, changed
state to up
*Jul 13 23:00:41.395: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up
*Jul 13 23:00:41.399: %LINK-3-UPDOWN: Interface Serial0, changed state to down
*Jul 13 23:00:42.187: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to down
*Jul 13 23:00:42.395: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to up
*Jul 13 23:00:42.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed
state to down
*Jul 13 23:00:55.915: %SYS-5-CONFIG_I: Configured from memory by console
*Jul 13 23:00:56.159: %FW-6-INIT: Firewall inspection startup completed; beginning
operation.
*Jul 13 23:00:56.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan114, changed
state to down
*Jul 13 23:00:56.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan192, changed
state to down
*Jul 13 23:00:56.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan193, changed
state to down
*Jul 13 23:00:56.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan194, changed
state to down
*Jul 13 23:00:56.255: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan195, changed
state to down
*Jul 13 23:00:57.011: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.2(3.16)M0.1,
MAINTENANCE INTERIM SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 07-Jun-12 04:44 by prod_rel_team
*Jul 13 23:00:57.095: %SNMP-5-COLDSTART: SNMP agent on host router is undergoing a cold
start
*Jul 13 23:00:57.103: %SYS-6-BOOTTIME: Time taken to reboot after reload =  558 seconds
*Jul 13 23:00:57.167: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 13 23:00:57.175: %LINK-5-CHANGED: Interface Serial0, changed state to
administratively down
*Jul 13 23:00:57.203: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jul 13 23:00:57.203: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
Jul 13 23:00:57.303: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 195.168.100.234 port
514 started - CLI initiated
```

```
Jul 13 23:00:57.303: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 100.100.100.100 port
520 started - CLI initiated
Jul 13 23:00:58.059: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
Jul 13 23:00:58.079: %LINK-3-UPDOWN: Interface FastEthernet1, changed state to up
Jul 13 23:00:58.099: %LINK-3-UPDOWN: Interface FastEthernet2, changed state to up
Jul 13 23:00:58.111: %LINK-3-UPDOWN: Interface FastEthernet3, changed state to up
Jul 13 23:00:58.123: %LINK-3-UPDOWN: Interface Wlan-GigabitEthernet0, changed state to up
Jul 13 23:00:59.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0,
changed state to down
Jul 13 23:00:59.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1,
changed state to down
Jul 13 23:00:59.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2,
changed state to down
Jul 13 23:00:59.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3,
changed state to down
Jul 13 23:00:59.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Wlan-GigabitEthernet0, changed state to up
Jul 13 23:00:59.883: %DTP-5-TRUNKPORTON: Port Fa3 has become dot1q trunk
Jul 13 23:01:01.091: %LINK-3-UPDOWN: Interface FastEthernet0, changed state to up
Jul 13 23:01:01.231: %LINK-3-UPDOWN: Interface FastEthernet1, changed state to up
Jul 13 23:01:01.259: %LINK-3-UPDOWN: Interface FastEthernet2, changed state to up
Jul 13 23:01:01.375: %LINK-3-UPDOWN: Interface FastEthernet3, changed state to up
Jul 13 23:01:02.091: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0,
changed state to up
Jul 13 23:01:02.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1,
changed state to up
Jul 13 23:01:02.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2,
changed state to up
Jul 13 23:01:02.527: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3,
changed state to up
Jul 13 23:01:07.811: %SECONDCORE-5-BOOTSTAGE: ROMMON on 2nd core UP
Jul 13 23:01:07.915: %SECONDCORE-5-BOOTSTAGE: AP-BOOTLOADER on 2nd core UP
Jul 13 23:01:09.687: %CISCO800-6-SIM_STATUS: SIM in slot 1 is not present
router>
router>
router>
router>en
router#
router#
router#
router#
Jul 13 23:01:17.063: %CISCO800-2-MODEM_DOWN: Cellular0 modem is now DOWN.sh
router#sh pla
router#sh platform ver
router#sh platform versions

Platform Revisions/Versions :
============================
FPGA       : 1.02   [Val = 0x12]]
Env Rev    : 4.5    [Val = 0x405]
Rework Rev : 00 00 00 00 00 00
CPU Name   : P1021SEC
CPU Ver    : 1.1    [Val = SVR:0x80EC0311]
Core Rev   : 5.1    [Val = PVR:0x80212051]
CCB CLOCK  : 269 MHz

IOS        :
Cisco IOS Software, C800 Software (C800-UNIVERSALK9-M), Version 15.2(3.16)M0.1,
MAINTENANCE INTERIM SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 07-Jun-12 04:44 by prod_rel_team

ROMMON (Readonly) :
```

```
System Bootstrap, Version 15.2(2r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012 by cisco Systems, Inc.

WLAN AP Boot loader (bundled):
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team

router#
Jul 13 23:01:25.291: %CELLWAN-2-SIM_FAILURE: [Cellular0]: SIM read failed for slot 0
Jul 13 23:01:25.391: %CISCO800-2-MODEM_UP: Cellular0 modem is now UP.
Jul 13 23:01:25.391: %CISCO800-6-SIM_STATUS: SIM in slot 0 is not present
router#
router#
router#
router#
Jul 13 23:01:27.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up
router#
router#
router#
Jul 13 23:01:30.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan114, changed
state to up
Jul 13 23:01:30.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan193, changed
state to up
Jul 13 23:01:30.295: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan194, changed
state to up
Jul 13 23:01:30.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan195, changed
state to up
router#
router#
router#
router#
router#sh inv
NAME: "C819HGW+7-A-A-K9", DESCR: "C819HGW+7-A-A-K9 chassis, Hw Serial#: FAC15455YYZ, Hw
Revision: 4.0"
PID: C819HGW+7-A-A-K9  , VID: V01, SN: FAC15455YYZ

NAME: "C819HGW Mother board on Slot 0", DESCR: "C819HGW Mother board"
PID: C819HGW+7-A-A-K9  , VID: V01, SN: FOC15455YYZ

NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless Mini Card MC8705 HSPA+R7 modem"
PID: MC8705            , VID: 1.0, SN: 357115040057411

router#
router#
router#
router#
```

コンフィギュレーション レジスタ

仮想コンフィギュレーション レジスタは不揮発性 NVRAM 内に存在し、他の Cisco ルータと同じ機能を持っています。ROM モニタからでも、オペレーティング システム ソフトウェアからでも、仮想コンフィギュレーション レジスタの表示および変更ができます。ROM モニタ内でコンフィギュレーション レジスタを変更するには、レジスタ値を 16 進形式で入力するか、ROM モニタ プロンプトを使用して各ビットを設定します。

コンフィギュレーション レジスタの手動での変更

ROM モニタから仮想コンフィギュレーション レジスタを手動で変更するには、**confreg** コマンドを入力し、続けて新しいレジスタ値を 16 進数で入力します（次の例を参照）。

```
rommon 1 > confreg 0x2101


You must reset or power cycle for new config to take effect
rommon 2 >
```

値は常に 16 進数と見なされます。新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットまたは再起動するまでは有効になりません。

コンフィギュレーション レジスタのプロンプトでの変更

confreg コマンドを引数なしで入力すると、仮想コンフィギュレーション レジスタの内容と、各ビットの意味を指定することによって内容を変更するためのプロンプトが表示されます。

いずれの場合も、新しい仮想コンフィギュレーション レジスタ値は NVRAM に書き込まれますが、ルータをリセットまたは再起動するまでは有効になりません。

次に、**confreg** コマンドの入力例を示します。

```
rommon 7> confreg

     Configuration Summary
enabled are:
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
enable  "diagnostic mode"? y/n  [n]:  y
enable  "use net in IP bcast address"? y/n  [n]:
enable  "load rom after netboot fails"? y/n  [n]:
enable  "use all zero broadcast"? y/n  [n]:
enable  "break/abort has effect"? y/n  [n]:
enable  "ignore system config info"? y/n  [n]:
change console baud rate? y/n  [n]:  y
enter rate: 0 = 9600, 1 = 4800, 2 = 1200, 3 = 2400  [0]:  0
change the boot characteristics? y/n  [n]:  y
enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
    [0]:  0

Configuration Summary
enabled are:
diagnostic mode
console baud: 9600
boot: the ROM Monitor

do you wish to change the configuration? y/n  [n]:


You must reset or power cycle for new config to take effect
```

コンソール ダウンロード

ROM モニタ機能の 1 つであるコンソール ダウンロードを使用すると、ルータ コンソール ポートを介して、ソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードすることができます。ダウンロードされたファイルは、ミニフラッシュ メモリ モジュールまたはメイン メモリに保存されて実行されます（イメージ ファイルの場合だけ）。

TFTP サーバにアクセスできない場合は、コンソール ダウンロードを使用してください。

（注）　コンソール ポートを介してソフトウェア イメージまたはコンフィギュレーション ファイルをルータにダウンロードする場合は、ROM モニタの **dnld** コマンドを使用する必要があります。

（注）　PC を使用し Cisco IOS イメージをルータ コンソール ポート経由で 115,200 bps でダウンロードする場合は、PC シリアル ポートで 16550 汎用非同期送受信器（UART）が使用されていることを確認します。PC のシリアル ポートに 16550 UART が使用されていない場合は、コンソール ポートを介して Cisco IOS イメージをダウンロードするときに、38,400 bps 以下の速度を使用することを推奨します。

コマンドについて

xmodem コンソール ダウンロード コマンドの構文および説明を、次に示します。

xmodem [-cyrx] *destination_file_name*

c	オプション。パケット検証に CRC-16 エラー チェックを使用して、ダウンロードを実行します。デフォルトは 8 ビットの CRC です。
y	オプション。Ymodem プロトコルを使用してダウンロードを実行するように、ルータに指示します。デフォルトは Xmodem プロトコルです。各プロトコルの相違は次のとおりです。 • Xmodem は 128 ブロックの転送サイズをサポートします。Ymodem は 1024 ブロックの転送サイズをサポートします。 • Ymodem は、各パケットの検証に CRC-16 エラー チェックを使用します。ソフトウェアのダウンロード元となるデバイスによっては、この機能が Xmodem でサポートされないことがあります。
r	オプション。イメージは DRAM にロードされ、実行されます。デフォルトでは、フラッシュ メモリにイメージをロードします。
x	オプション。イメージは DRAM にロードされますが、実行されません。
destination_file_name	システム イメージ ファイルまたはシステム コンフィギュレーション ファイルの名前です。ルータが認識できるようにするには、コンフィギュレーション ファイル名を *router_confg* にする必要があります。

次の手順に従って、Xmodem を実行します。

ステップ 1　Xmodem を実行するローカル ドライブに、イメージ ファイルを移動します。

ステップ 2　**xmodem** コマンドを入力します。

エラー レポート

ROM モニタのコンソール ダウンロードは、コンソールを使用してデータ転送を行うため、データ転送中にエラーが発生した場合、エラー メッセージがコンソール上に表示されるのはデータ転送が終了してからです。

デフォルトのボー レートを変更した場合は、端末のボー レートをコンフィギュレーション レジスタに指定されたボー レートに戻すことを指示するメッセージがエラー メッセージに続いて表示されます。

デバッグ コマンド

ROM モニタのほとんどのデバッグ コマンドは、Cisco IOS ソフトウェアがクラッシュまたは停止した場合にだけ機能します。デバッグ コマンドの入力時に Cisco IOS クラッシュ情報が得られない場合は、次のエラーメッセージが表示されます。

```
"xxx: kernel context state is invalid, can not proceed."
```

次に、ROM モニタのデバッグ コマンドを示します。

- **stack** または **k**：スタック トレースが生成されます。次に例を示します。

```
rommon 6> stack
Stack trace:
PC = 0x801111b0
Frame 00: FP = 0x80005ea8    PC = 0x801111b0
Frame 01: FP = 0x80005eb4    PC = 0x80113694
Frame 02: FP = 0x80005f74    PC = 0x8010eb44
Frame 03: FP = 0x80005f9c    PC = 0x80008118
Frame 04: FP = 0x80005fac    PC = 0x80008064
Frame 05: FP = 0x80005fc4    PC = 0xfff03d70
```

- **context**：プロセッサのコンテキストが表示されます。次に例を示します。

```
rommon 7> context
CPU context of the most recent exception:
PC  = 0x801111b0  MSR = 0x00009032  CR  = 0x53000035  LR    = 0x80113694
CTR = 0x801065e4  XER = 0xa0006d36  DAR = 0xffffffff  DSISR = 0xffffffff
DEC = 0xffffffff  TBU = 0xffffffff  TBL = 0xffffffff  IMMR  = 0xffffffff
R0  = 0x00000000  R1  = 0x80005ea8  R2  = 0xffffffff  R3    = 0x00000000
R4  = 0x8fab0d76  R5  = 0x80657d00  R6  = 0x80570000  R7    = 0x80570000
R8  = 0x00000000  R9  = 0x80570000  R10 = 0x0000954c  R11   = 0x00000000
R12 = 0x00000080  R13 = 0xffffffff  R14 = 0xffffffff  R15   = 0xffffffff
R16 = 0xffffffff  R17 = 0xffffffff  R18 = 0xffffffff  R19   = 0xffffffff
R20 = 0xffffffff  R21 = 0xffffffff  R22 = 0xffffffff  R23   = 0xffffffff
R24 = 0xffffffff  R25 = 0xffffffff  R26 = 0xffffffff  R27   = 0xffffffff
R28 = 0xffffffff  R29 = 0xffffffff  R30 = 0xffffffff  R31   = 0xffffffff
```

- **frame**：個々のスタック フレームが表示されます。
- **sysret**：最後に起動したシステム イメージからの戻り情報が表示されます。この情報には、イメージを中止した理由、最大 8 フレームのスタック ダンプ、および例外が発生したアドレス（例外がある場合）などが含まれます。

```
rommon 8> sysret
System Return Info:
```

```
count: 19,  reason: user break
pc:0x801111b0,  error address: 0x801111b0
Stack Trace:
FP: 0x80005ea8, PC: 0x801111b0
FP: 0x80005eb4, PC: 0x80113694
FP: 0x80005f74, PC: 0x8010eb44
FP: 0x80005f9c, PC: 0x80008118
FP: 0x80005fac, PC: 0x80008064
FP: 0x80005fc4, PC: 0xfff03d70
FP: 0x80005ffc, PC: 0x00000000
FP: 0x00000000, PC: 0x00000000
```

- **meminfo**：メイン メモリのサイズ（バイト）、開始アドレス、および使用可能範囲、パケット メモリの開始ポイントとサイズ、NVRAM のサイズが表示されます。次に例を示します

```
rommon 9> meminfo
Main memory size: 40 MB.
Available main memory starts at 0x10000, size 40896KB
IO (packet) memory size: 5 percent of main memory.
NVRAM size: 32KB
```

ROM モニタの終了

ルータの起動時または再ロード時に Cisco IOS イメージをフラッシュ メモリから起動させるには、コンフィギュレーション レジスタ値を 0x2 ～ 0xF に設定する必要があります。

次に、コンフィギュレーション レジスタをリセットして、ルータがフラッシュ メモリに格納された Cisco IOS イメージを起動するように設定する例を示します。

```
rommon 1 > confreg 0x2101
```

新しいコンフィギュレーションを有効にするには、リセットまたは電源の再投入を行う必要があります。

```
rommon 2 > boot
```

ルータは、フラッシュ メモリ内の Cisco IOS イメージを起動します。ルータの次のリセット時または電源の再投入時に、コンフィギュレーション レジスタの値は 0x2101 になります。

APPENDIX D

共通ポート割り当て

表 D-1 に、現在割り当てられている伝送制御プロトコル（TCP）ポート番号を示します。ユーザ データグラム プロトコル（UDP）でも、可能な限り同じ番号が使用されています。

表 D-1　　現在割り当てられている TCP および UDP ポート番号

ポート	キーワード	説明
0	—	予約済み
1 ～ 4	—	未割り当て
5	RJE	リモート ジョブ入力
7	echo	エコー
9	DISCARD	廃棄
11	USERS	アクティブ ユーザ
13	DAYTIME	日時
15	NETSTAT	Who is up または NETSTAT
17	QUOTE	Quote of the day
19	CHARGEN	キャラクタ ジェネレータ
20	FTP-DATA	ファイル転送プロトコル（データ）
21	FTP	ファイル転送プロトコル
23	TELNET	端末接続
25	SMTP	シンプル メール転送プロトコル
37	TIME	時間
39	RLP	リソース ロケーション プロトコル
42	NAMESERVER	ホストネーム サーバ
43	NICNAME	名前
49	LOGIN	ログイン ホスト プロトコル
53	DOMAIN	ドメイン ネーム サーバ
67	BOOTPS	ブートストラップ プロトコル サーバ
68	BOOTPC	ブートストラップ プロトコル クライアント
69	TFTP	トリビアル ファイル転送プロトコル

表 D-1　現在割り当てられている TCP および UDP ポート番号 （続き）

ポート	キーワード	説明
75	—	任意のプライベート ダイヤルアウト サービス
77	—	任意のプライベート RJE サービス
79	FINGER	Finger
95	SUPDUP	SUPDUP プロトコル
101	HOST NAME	ネットワーク インターフェイス カード（NIC）ホスト ネーム サーバ
102	ISO-TSAP	ISO-Transport Service Access Point（TSAP）
103	X400	X400
104	X400-SND	X400-SND
111	SUNRPC	Sun Microsystems のリモート プロシージャ コール
113	AUTH	認証サービス
117	UUCP-PATH	UNIX 間コピー プログラム（UUCP）パス サービス
119	NNTP	Usenet Network News Transfer Protocol
123	NTP	ネットワーク タイム プロトコル
126	SNMP	簡易ネットワーク管理プロトコル
137	NETBIOS-NS	NetBIOS ネーム サービス
138	NETBIOS-DGM	NetBIOS データグラム サービス
139	NETBIOS-SSN	NetBIOS セッション サービス
161	SNMP	簡易ネットワーク管理プロトコル
162	SNMP-TRAP	簡易ネットワーク管理プロトコル トラップ
512	rexec	UNIX のリモート実行（制御）
513	TCP：rlogin UDP：rwho	TCP：UNIX リモート ログイン UDP：UNIX ブロードキャスト ネーム サービス
514	TCP：rsh UDP：syslog	TCP：UNIX リモート シェル UDP：システム ログ
515	Printer	UNIX ライン プリンタ リモート スプーリング
520	RIP	ルーティング情報プロトコル
525	Timed	タイム サーバ

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