Cisco 900 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

2019 年 1 月 11 日

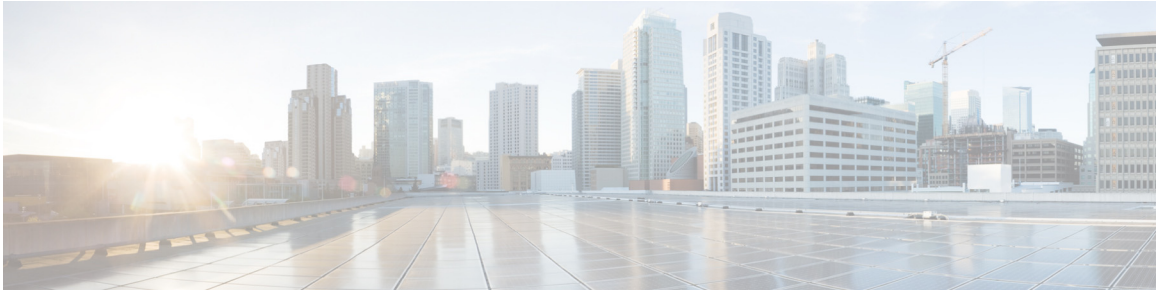
シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

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

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

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

Cisco 900 シリーズ サービス統合型ルータ ソフトウェア コンフィギュレーション ガイド



はじめに

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

目的

このマニュアルでは、Cisco 900 シリーズ サービス統合型ルータ（ISR）の各種機能の設定方法を説明します。

対象読者

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

マニュアルの構成

このマニュアルは、次の章で構成されています。

章	説明
製品概要	Cisco 900 シリーズ ISR のハードウェアおよびソフトウェア機能の概要について説明します。
ソフトウェアのインストール	Cisco IOS イメージ、現場交換可能ユニット、およびシスコ ライセンスをアップグレードする方法について説明します。
ルータの基本設定	ルータ、インターフェイスおよびルーティングの基本設定方法について説明します。

章	説明
イーサネット スイッチの設定	ギガビット イーサネット（GE）スイッチを設定する手順について説明します。
PPP over Ethernet と NAT の設定	Point-to-point Protocol on Ethernet（PPPoE）クライアントおよびネットワークアドレス変換（NAT）を設定する手順について説明します。
DHCP および VLAN による LAN の設定	DHCP および VLAN を使用して LAN を設定する手順について説明します。
レイヤ 3 インターフェイスでの ID 機能の設定	レイヤ 3 インターフェイスでの ID 機能の設定について説明します。
セキュリティ機能の設定	セキュリティ機能の設定方法について説明します。
VDSL2 と ADSL2/2+ の設定	Cisco 900 シリーズ ISR でマルチモード VDSL2 および ADSl2+ WAN 接続を設定する方法について説明します。
4G 無線 WAN の設定	4G ワイヤレス WAN インターフェイスを設定する方法について説明します。
セキュア ストレージの設定	セキュア ストレージを有効または無効にする方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

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

(注) 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

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

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

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

関連資料

『Cisco 900 シリーズ ISR ソフトウェア コンフィギュレーション ガイド』(本マニュアル)に加え、以下のリファレンス ガイドが含まれます。

マニュアルの種類	リンク
『Cisco 900 Series ISR Hardware Installation Guide』	*https://www.cisco.com/c/en/us/td/docs/routers/access/900/hardware/installation/guide/b-cisco-ISR900-series-hig.html*
『Regulatory Compliance and Safety Information for Cisco 900 Series Routers』	*https://www.cisco.com/c/en/us/td/docs/routers/access/900/regulatory/compliance/900rcsi.html*

マニュアルの入手方法およびテクニカル サポート

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

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

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

Cisco 900 シリーズ サービス統合型ルータの概要

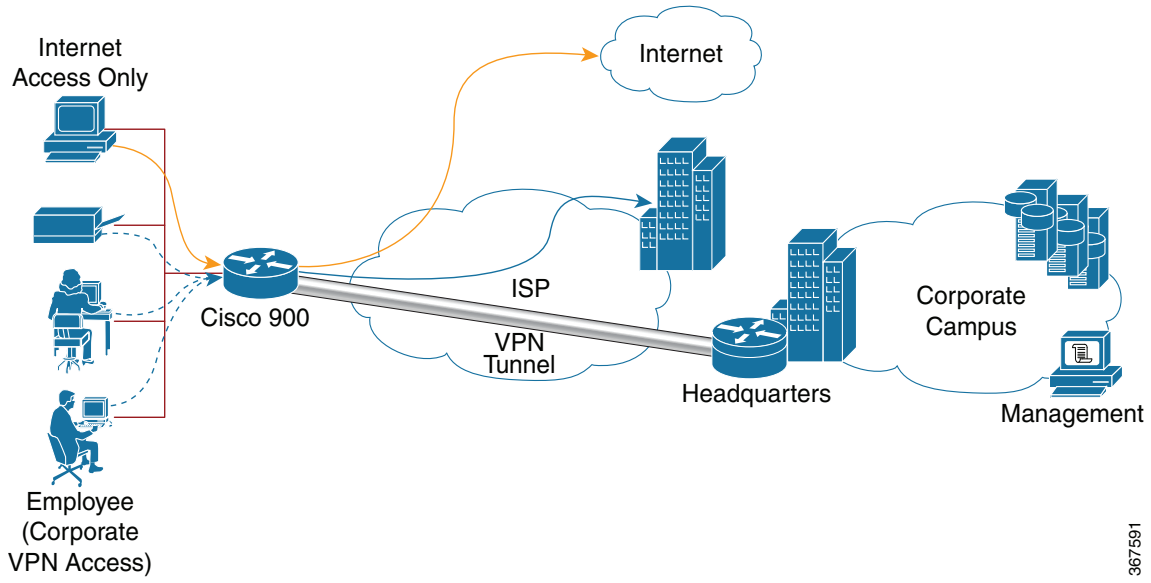
この章では、Cisco 900 シリーズ サービス統合型ルータ（ISR）の概要について説明します。この章の構成は、次のとおりです。

Cisco 900 シリーズ ISR の概要

Cisco 900 シリーズ ISR は、小規模オフィスや、センター拠点に安全なネットワーク接続を提供する、エントリ レベルのブランチ ルータです。この高性能で固定構成のルータは、ブロードバンドおよびメトロ イーサネットによる安全な接続を提供します。イーサネット WAN マネージド サービスを提供するサービス プロバイダーは、このルータを CPE として顧客の事業所に導入できます。

図 1-1 Cisco 900 シリーズ ISR を展開し、小規模オフィスからセキュア VPN トンネル経由で本社にリモート接続できるようにするシナリオを示します。このシナリオでの企業ユーザは、インターネット ユーザとは別の VLAN を使用します。

図 1-1　　Cisco 900 シリーズの展開例



Cisco 900 シリーズ ISR モデル

Cisco 900 シリーズ ISR は、次のモデルで使用できます。

- Cisco C921-4P
- Cisco C921J-4P
- Cisco C931-4P

表 1-1 Cisco 900 シリーズ ISR モデルで使用可能な LAN および WAN インターフェイス オプションの概要を示します。

表 1-1　　Cisco 900 シリーズ ISR の LAN および WAN インターフェイス

900 シリーズ モデル	LAN インターフェイス	GE WAN インターフェイス
Cisco C921-4P	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート
Cisco C921J-4P	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート
C921-4PLTEGB	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート

900 シリーズ モデル	LAN インターフェイス	GE WAN インターフェイス
C921-4PLTEAU	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート
C921-4PLTENA	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート
C926-4P	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C926-4PLTEGB	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C927-4P	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C927-4PM	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C927-4PLTEGB	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C927-4PMLTEGB	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
C927-4PLTEAU	4 ポート 10/100/1000 Mbps マネージド スイッチ	1 ギガビット イーサネット ポート
Cisco C931-4P	4 ポート 10/100/1000 Mbps マネージド スイッチ	2 ギガビット イーサネット ポート

Cisco 900 シリーズ ISR の機能

Cisco 900 シリーズ ISR でサポートされている主要な機能には次のものがあります。

- フェールオーバーによる保護とロード バランシングのための冗長 WAN 接続
- 仮想ルータ冗長プロトコル（VRRP、RFC 2338）、Hot Standby Router Protocol（HSRP）などのダイナミック フェールオーバー プロトコル
- 統合型アプリケーション インスペクション ファイアウォールによるネットワーク周辺セキュリティ
- 高速 IP Security（IPsec）Triple Data Encryption Standard（3DES）および Advanced Encryption Standard（AES）の暗号化によるデータ プライバシー
- 侵入防御を備えたセキュリティ ポリシーの適用
- セキュリティ ハードウェアの高速化
- 今後 10 年間にわたって信頼性が高く安全なネットワーク通信システムを提供するための次世代暗号化
- LAN 接続をサポート
- ワイヤレス/有線デバイスの設定と管理を簡略化および一元化ワイヤレス LAN コントローラを必要とせずに WLAN サービスをサポート
- コンソール ポートおよび USB ポートを個別にサポート

Cisco 900 シリーズ ISR の LED

表 1-2 Cisco 900 シリーズ ISR の LED について説明します。

表 1-2 Cisco 900 シリーズ ISR の LED

LED	色	説明
SYS	消灯	システムの電源がオフです。
	点滅	起動フェーズまたは ROM モニタ mode。
	点灯	通常動作中です。
	オレンジ（点灯）	サーマル トリップ。
	オレンジ（点滅）	ROMMON コード署名の検証に失敗しました。
VPN OK	グリーン	少なくとも 1 つの VPN 接続が確立しています。
	消灯	VPN 接続は確立していません。
LAN	グリーン（点灯）	LAN 接続が確立されています。
	グリーン（点滅）	WAN ポートでデータ伝送中です。
	消灯	LAN に接続していません。
WAN	グリーン（点灯）	WAN リンクが確立されています。
	グリーン（点滅）	WAN ポートでデータ伝送中です。
	消灯	WAN リンクに接続していません。
DSL CD	消灯	無効。
	グリーン（点滅）	トレーニング中、または有効ですがケーブルが切断されています。
	グリーン（点灯）	トレーニング済み。
DSL データ	消灯	無効。
	グリーン（点滅）	TX/RX データ。
RSSI	グリーン（点灯）	信号 > – 60 dBm 非常に強い信号
	黄色	60 dBm > 信号 > -75 dBm 強い信号
	黄色（点滅）	75 dBm > 信号 > -90 dBm 適正な信号
	消灯	信号 < –90 dBm 使用不可能な信号
SIM	消灯	SIM 未挿入。
	点灯	SIM がスロットに挿入されています。
	点滅	TXD/RXD データ。

ソフトウェアのインストール

この章では、Cisco IOS イメージのアップグレード方法、ROM モニタの使用方法、Field Programmable ユニットのアップグレード方法、および Cisco ISR 900 シリーズルータでサポートされているライセンス パッケージについて説明します。この章は、次の項で構成されています。

ROM モニタ

ROM モニタ ファームウェアは、ルータの電源投入時またはリセット時に実行され、このファームウェアは、プロセッサ ハードウェアの初期化とオペレーティング システムのブートを助けます。ROM モニタを使用して、忘れてしまったパスワードの回復や Cisco IOS 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。

ROM モニタを使用するには、次の概念を理解しておく必要があります。

ROM モニタ モードのコマンド プロンプト

ROM モニタでは、`rommon x >` コマンド プロンプトが使用されます。*x* 変数は 1 から始まり、ROM モニタ モードで **[Return]** または **[Enter]** を押すたびに増えます。

ルータが ROM モニタ モードである理由

次のいずれかが当てはまる場合、ルータは ROM モニタ モードで起動します。

- 電源投入またはリロード中に、ルータで有効なシステム イメージが検出されない。
- コンフィギュレーション レジスタのブート フィールドの最終桁が 0 になっている（0x100、0x0 など）
- ルータのリロード後 60 秒以内に **Ctrl+C** が入力された。

ROM モニタ モードを終了する方法については、「ROM モニタ モードの終了」セクション（2-10 ページ）を参照してください。

ROM モニタの使用タイミング

ROM モニタは、次の場合に使用します。

- システム イメージを手動でロードしている場合：今後システムをリロードしたり電源を再投入する時に、ルータを設定せず、システム イメージをロードできます。これは、新しいシステム イメージをテストする場合やトラブルシューティングを行う場合に便利です。「コンフィギュレーション レジスタ（confreg）の変更」セクション（2-9 ページ）を参照してください。
- TFTP サーバまたはネットワーク接続がない場合にシステム イメージをアップグレードし、ルータ コンソールに直接 PC を接続するのが唯一可能なオプションである場合：ルータのコンフィギュレーション マニュアルのシステム イメージのアップグレードに関する情報を参照してください。
- ルータがクラッシュまたは停止した場合のトラブルシューティング。「ROM モニタ モードの終了」セクション（2-10 ページ）を参照してください。
- ディザスタ リカバリ：次の方法で、システム イメージまたはコンフィギュレーション ファイルを回復します。
  - TFTP ダウンロード（**tftpdnld**）：ルータの固定 WAN ポートに TFTP サーバを直接接続できる場合。「ROM モニタ モードの終了」セクション（2-10 ページ）を参照してください。

（注） システム イメージの回復とシステム イメージのアップグレードは異なります。システム イメージの回復が必要になるのは、システム イメージが壊れた場合、または障害がメモリ デバイスに与えた影響が大きくて、メモリ デバイス上のすべてのデータを削除してシステム イメージをロードしなければならなくなったために、システム イメージが削除された場合です。

ROM モニタ コマンドを使用する場合のヒント

- ROM モニタ コマンドでは大文字と小文字が区別されます。
- ROM モニタ コマンドを停止するには、PC または端末で **Ctrl+C** を入力します。
- ルータ上で使用できるコマンドを調べ、コマンド構文のオプションを表示する方法については、「コンフィギュレーション レジスタ（confreg）の変更」セクション（2-9 ページ）を参照してください。

ROM モニタの使用方法:一般的な作業

この項では、次の手順について説明します。

- ROM モニタ モードの開始(7 ページ)
- コンフィギュレーション レジスタ(confreg)の変更(9 ページ)
- USB フラッシュ装置の情報の入手(9 ページ)
- ROM モニタ モードの終了(10 ページ)

(注) ここでは、ROM モニタで行うことのできる作業をすべて取り上げるわけではありません。この資料で扱っていない作業については、コマンド ヘルプを利用してください。「コンフィギュレーション レジスタ(confreg)の変更」セクション(2-9 ページ)を参照してください。

ROM モニタ モードの開始

ここでは、2 種類の ROM モニタ モードの開始方法について説明します。

- Break キー シーケンスでシステム リロードを中断して ROM モニタ モードを開始する場合(7 ページ)
- ROM モニタ モードで起動するようにコンフィギュレーション レジスタを設定する場合(8 ページ)

前提条件

ルータのコンソール ポートに端末または PC を接続します。ヘルプについては、ルータの『Hardware Installation Guide』を参照してください。

Break キー シーケンスでシステム リロードを中断して ROM モニタ モードを開始する場合

ルータをリロードし、Break キー シーケンスを入力して、ROM モニタ モードを開始するには、次の手順を実行します。

```
Router> enable
Router# reload
Press Ctrl+ C
```

reload コマンドを入力してから 60 秒以内に **Ctrl+C** を押す必要があります。次の例に示すとおり、**Ctrl+C** を押す前に、5 つのドットが表示されるまで待機します。

```
Router#reload
Proceed with reload? [confirm]

*Sep 14 08:52:19.147: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
System Bootstrap, Version 15.8(3r)M0b, RELEASE SOFTWARE (fc1)
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Mon 03-Sep-2018  9:01:14.57

C931-4P platform with 1048576 Kbytes of main memory

System Integrity Status: 0x00000000
Current image running: Upgrade
Last reset cause: Software initiated

Rom image verified correctly
```

```
..... <<<<<<<<<<-----------Pressed Ctrl+C to break autoboot and enter ROMMON shell

rommon 1 >
```

次の作業

- 「コンフィギュレーション レジスタ（confreg）の変更」セクション（2-9 ページ）に進みます。
- 通常であればルータがシステム イメージを起動している状況で、Break キー シーケンスを入力して ROM モニタ モードを開始した場合、**i** または **reset** コマンドを入力し、もう一度ブートプロセスを開始してシステム イメージをロードすることにより、ROM モニタ モードを終了できます。

ROM モニタ モードで起動するようにコンフィギュレーション レジスタを設定する場合

ここでは、次回のシステム リロード時またはオフ/オン時に ROM モニタ モードで起動するように、コンフィギュレーション レジスタを設定することによって、ROM モニタ モードを開始する方法について説明します。

注意 ボー レートを設定した後に、**config-register 0x0** コマンドを使用してコンフィギュレーション レジスタを設定しないでください。ボー レートに影響を与えずにコンフィギュレーション レジスタを設定するには、**show ver | inc configuration** コマンドを入力して現在のコンフィギュレーション レジスタ設定を使用し、コンフィギュレーション レジスタ コマンドで最後の（右端の）数字を 0 に置き換えます。

次の例で、ROM モニタ モードで起動するようにコンフィギュレーション レジスタを設定する方法を示します。

```
Router>
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# config-register 0x0
Router(config)# exit
Router#
*Sep 14 08:56:31.265: %SYS-5-CONFIG_I: Configured from console by console
Router#write memory
Building configuration...
[OK][OK]
Router#
*Sep 14 08:56:41.715: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
Router#reload
Proceed with reload? [confirm]

*Sep 14 08:56:47.531: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
System Bootstrap, Version 15.8(3r)M0b, RELEASE SOFTWARE (fc1)
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Mon 03-Sep-2018  9:01:14.57

C931-4P platform with 1048576 Kbytes of main memory

System Integrity Status: 0x00000000
Current image running: Upgrade
Last reset cause: Software initiated

Rom image verified correctly
```

次の作業

「コンフィギュレーション レジスタ（confreg）の変更」セクション（2-9 ページ）に進みます。

コンフィギュレーション レジスタ（confreg）の変更

このセクションでは、**confreg** ROM モニタ コマンドを使用して、コンフィギュレーション レジスタを変更する方法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 モードで **config-register** コマンドを使用して、Cisco IOS コマンドライン インターフェイス（CLI）からコンフィギュレーション レジスタの設定を変更することもできます。

注意　ボー レートの設定後に、**config-register 0x0** コマンドを使用してコンフィギュレーション レジスタを設定しないでください。ボー レートに影響を与えずにコンフィギュレーション レジスタを設定するには、**show ver | inc configuration** コマンドを入力して現在のコンフィギュレーション レジスタ設定を使用し、コンフィギュレーション レジスタ コマンドで最後の（右端の）数字を 0 に置き換えます。

（注）　変更したコンフィギュレーション レジスタ値は、NVRAM に自動的に書き込まれますが、新しい値が有効になるのは、ルータをリセットまたはオフ/オンしてからです。

次の例では、フラッシュ メモリのシステム イメージが起動されるようにコンフィギュレーション レジスタを設定します。

```
rommon 3 > confreg 0x2102
```

次の例では、値を入力しないので、レジスタの各ビットへの入力が求められます。

```
rommon 3> confreg

Configuration Summary
   (Virtual Configuration Register: 0x100)
enabled are:
[ 0 ] console baud: 9600
boot:...... the ROM Monitor
do you wish to change the configuration? y/n [n]: y
enable "diagnostic mode"? y/n [n]: n
enable "break/abort has effect"? y/n [n]: n
enable "ignore system config info"? y/n [n]: n
change console baud rate? y/n [n]: n
change the boot characteristics? y/n [n]: y
0 = the ROM Monitor
1-15 = boot system
enter boot option [0]: 3
```

USB フラッシュ装置の情報の入手

次の例で、ディレクトリ、ファイル、アクセス権、サイズなど、USB フラッシュ装置の内容を表示する方法を示します。

```
rommon 3 > dir usbflash0:


Size       Attributes Name
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

```
8192          drw-     System Volume Information
60865852      -rw-     c900-åuniversalk9_npe-mz.SPA.158-3.M0b
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

次の例で、ルータに挿入されているターゲットの USB フラッシュ装置と、現在挿入されているかどうかを問わず有効な装置名を示します。

```
rommon 2 > dev
Devices in device table:
id name
tftp: network via tftp
flash: Internal flash drive
usbflash0: External USB drive 0
```

ROM モニタ モードの終了

ここでは、ROM モニタ モードを終了して、Cisco IOS コマンドライン インターフェイス（CLI）を開始する方法について説明します。ROM モニタ モードの終了方法は、ROM モニタ モードの開始方法によって決まります。

- 通常であればルータがシステム イメージを起動している状況で、ルータをリロードし、Break キー シーケンスを入力して ROM モニタ モードを開始した場合、**i** コマンドまたは **reset** コマンドを入力し、もう一度ブートプロセスを開始してシステム イメージをロードすることにより、ROM モニタ モードを終了できます。
- システム イメージの場所を見つけてロードすることができなかったために ROM モニタ モードが開始された場合は、次の手順が必要です。

	コマンドまたはアクション	目的
ステップ 1	**dir flash:**[*directory*] 例: `rommon > dir flash:`	フラッシュ メモリに含まれているファイルおよびディレクトリの一覧を表示します。 • ルータにロードさせるシステム イメージを見つけます。 • システム イメージがフラッシュ メモリにない場合は、ステップ 2 の 2 つめまたは 3 つめのオプションを使用します。

	コマンドまたはアクション	目的

ステップ 2	**boot flash:**[*directory*] [*filename*]
	または
	boot *filename tftpserver*
	または
	boot [*filename*]
	
	例:
	`ROMMON > boot flash:myimage`
	
	例:
	`ROMMON > boot someimage 172.16.30.40`
	
	例:
	`ROMMON > boot`
		上から順に、次のようにルータに指示します。
		• フラッシュ メモリ内の最初のイメージまたは指定されたイメージを起動します。
		• 指定された TFTP サーバ(ホスト名または IP アドレス)からネットワーク経由で指定されたイメージを起動します。
		• 装置 ID を認識しないので、ブートヘルパー イメージから起動します。このコマンド形式は、指定されたイメージをネットブートする場合に使用します。
		別のイメージを示すように BOOTLDR モニタ環境変数を設定することによって、ブートヘルパー イメージのデフォルト値を変更できます。この目的には、任意のシステム イメージを使用できます。
		(注) boot コマンドのオプションは **-x**(イメージをロードするが実行しない)および **-v**(詳細)です。

カプセル アップグレードを使用した ROMMON のアップグレード

カプセルアップグレードを使用して ROMMON をアップグレードできます。次の例で、カプセルアップグレードを使用して ROMMON をアップグレードする方法を示します。

```
router# > upgrade rom-monitor file flash:c900-CapsuleUpdateFile.15.8-3rM0b
```

(注) アップグレードする前に、ルータ フラッシュにカプセル イメージ **'c900-CapsuleUpdateFile.15.8-3rM0b'** があることを確認してください。

ROMMON バージョンを確認するには、**showmon -v** コマンドを使用します。次の例はコマンドの出力を示しています。

```
rommon 1 > showmon -v

System Bootstrap, Version 15.8(3r)M0b, RELEASE SOFTWARE (fc1)
Copyright (c) 2018 by cisco Systems, Inc.
Compiled Mon 03-Sep-2018  9:01:14.57
```

Cisco IOS ソフトウェアのアップグレード

ルータには Cisco IOS イメージがプリインストールされています。ただし、ルータ機能を最新の状態に保つために新しいバージョンをインストールすることができます。このセクションでは、Cisco 900 シリーズ ISR での Cisco Internet Operating System(IOS)ソフトウェア イメージのアップグレード方法を説明します。

- システム イメージのアップグレードに関する情報(12 ページ)
- Cisco IOS イメージのアップグレード方法(13 ページ)

システム イメージのアップグレードに関する情報

ルータのシステム イメージをアップグレードする方法については、次のセクションを参照してください。

- システム イメージをアップグレードする理由（12 ページ）
- ルータ上で稼働している Cisco IOS Release を調べる方法（12 ページ）
- 新しい Cisco IOS Release およびフィーチャ セットの選択方法（12 ページ）
- システム イメージのダウンロード元（12 ページ）

システム イメージをアップグレードする理由

システム イメージには Cisco IOS ソフトウェアが収められています。出荷時、ルータにはイメージがインストール済みです。ある段階で、ルータまたはアクセス ポイントのいずれかに異なるイメージをロードしなければならない場合があります。たとえば、自身が使用している IOS ソフトウェアを最新バージョンにアップグレードする場合や、ネットワーク内のすべてのルータで同一の Cisco IOS Release を使用する場合などが考えられます。各システム イメージには Cisco IOS 機能の異なるセットが含まれます。そのため、ネットワーク要件に応じて適切なシステム イメージを選択する必要があります。

ルータ上で稼働している Cisco IOS Release を調べる方法

使用しているルータで実行中の Cisco IOS Release とシステム イメージのファイル名を確認するには、ユーザ EXEC モードまたは特権 EXEC モードで **show version** コマンドを実行します。

新しい Cisco IOS Release およびフィーチャ セットの選択方法

使用しているプラットフォームでサポートされている Cisco IOS リリースと機能を確認するには、http://www.cisco.com/go/cfn から Cisco Feature Navigator にアクセスしてください。アクセスするには、Cisco.com のアカウントが必要です。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

システム イメージのダウンロード元

システム イメージをダウンロードするには、Cisco.com のアカウントを取得し、次の Web サイトにアクセスする必要があります。アカウントをお持ちでない場合や、ユーザ名やパスワードを忘れた場合は、ログイン ダイアログボックスで [Cancel] をクリックし、表示される説明に従ってください。

ダウンロードする Cisco IOS Release とフィーチャ セットがわかっている場合は、次のページに直接アクセスしてください。

https://software.cisco.com/download/home

システム イメージのロードと管理の詳細については、次を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book/cf-config-overview.html

Cisco IOS イメージのアップグレード方法

ここでは、ルータでの Cisco IOS イメージのアップグレードについて説明します。

- 旧システム イメージおよびコンフィギュレーションのバックアップ コピーの保存（13 ページ）
- フラッシュ メモリへのシステム イメージのコピー（14 ページ）
- 新しいシステム イメージのロード（17 ページ）
- 新しいシステム イメージおよびコンフィギュレーションのバックアップ コピーの保存（21 ページ）

旧システム イメージおよびコンフィギュレーションのバックアップ コピーの保存

新しいシステム イメージやスタートアップ コンフィギュレーションを使用することで重大な問題が発生した場合に、予期しないダウンタイムが発生するのを防ぐため、現在のスタートアップ コンフィギュレーション ファイルと Cisco IOS ソフトウェア システムのイメージ ファイルのバックアップ コピーをサーバに保存することをお勧めします。

次の例では、TFTP サーバにスタートアップ コンフィギュレーションをコピーします。また、フラッシュ メモリから FTP サーバにコピーします。

スタートアップ コンフィギュレーションの TFTP サーバへのコピー：例

次に、スタートアップ コンフィギュレーションを TFTP サーバにコピーする例を示します。

```
Router# copy nvram:startup-config tftp:

Remote host[]? 192.0.0.1

Name of configuration file to write [rtr2-confg]? rtr2-config-b4upgrade
Write file rtr2-confg-b4upgrade on host 192.0.0.1?[confirm] <cr>
![OK]
```

フラッシュ メモリから TFTP サーバへのコピー：例

次に、特権 EXEC モードで **dir flash:** コマンドを使用して、システム イメージ ファイルの名前を学習し、特権 EXEC モードで **copy flash: tftp:** コマンドを使用してシステム イメージを TFTP サーバにコピーする場合の例を示します。このルータはデフォルトのユーザ名とパスワードを使用しています。

```
Router# copy flash: tftp:
Source filename [running-config]?
Address or name of remote host []? 192.0.0.1
Destination filename [router-confg]? running-config
983 bytes copied in 0.048 secs (20479 bytes/sec)

Router#
Router# dir flash:
Directory of flash:/

    1  -rw-    64383100  Sep 17 2018 05:58:14 +00:00  c900-universalk9-mz.SSA_09-10
    2  -rw-        1524  Sep 17 2018 05:55:30 +00:00  c900_startupconfig-backup
    3  -rw-         919  Sep 17 2018 05:58:44 +00:00  PSZ22241BW6_20180906052515287.zip

1936031744 bytes total (1871634432 bytes free)
Router#
```

フラッシュ メモリへのシステム イメージのコピー

このセクションでは、ルータのフラッシュ メモリ カードにシステム イメージをコピーする方法について説明します。

（注） ルータには、Cisco IOS を保存するのに十分なディスクまたはフラッシュ メモリが必要です。さらに、ルータには Cisco IOS を実行するための十分なメモリ（DRAM）も必要です。ルータに十分なメモリ（DRAM）が搭載されていない場合、ルータが新しい Cisco IOS を使用して起動するときに起動に関する問題が発生します。

システム イメージをルータのフラッシュ メモリ カードにコピーするには、次のいずれかの方法を選択します。

- ROM モニタ モードの開始（7 ページ）
- ROM モニタを使用してネットワーク経由でシステム イメージをコピーする方法（15 ページ）
- 新しいシステム イメージのロード（17 ページ）

TFTP または RCP を使用してフラッシュ メモリにシステム イメージをコピーする方法

ここでは、TFTP または Remote Copy Protocol（RCP）を使用してシステム イメージをアップグレードする方法について説明します。システム イメージをアップグレードする場合は、この方法を推奨します。また、この方法が最も一般的です。

前提条件

次に、システム イメージのアップグレード ロジスティックスの詳細を示します。

- TCP/IP 対応のワークステーションまたは PC に、TFTP サーバまたは RCP サーバ アプリケーションをインストールします。さまざまなベンダーが無料の TFTP サーバ ソフトウェアを提供しています。Web の検索エンジンで「TFTP サーバ」を検索して見つけることができます。

  TFTP を使用する場合

  - TFTP *クライアント*としてではなく、TFTP *サーバ*として動作するように、TFTP アプリケーションを設定します。
  - システム イメージをダウンロードして保管する、アウトバウンド ファイルのディレクトリを指定します。
- ワークステーションまたは PC に新しい Cisco IOS ソフトウェア イメージをダウンロードします。「システム イメージのダウンロード元」セクション（2-12 ページ）を参照してください。
- ルータとのコンソール セッションを確立します。ルータのコンソール ポートに PC を直接接続することを推奨します。ご使用のルータのハードウェア インストレーション ガイドを参照してください。
- TFTP サーバまたは RCP サーバとルータ間の IP 接続を確認します。TFTP サーバまたは RCP サーバとルータ間で ping が失敗する場合は、次のいずれか 1 つを行います。
  - ルータ上でデフォルト ゲートウェイを設定します。
  - サーバとルータのそれぞれに、同じネットワークまたは同じサブネット内の IP アドレスを与えます。.

ヒント 前提となる作業手順の詳細については、テクニカル ノート『*Software Installation and Upgrade Procedure*』を参照してください。

ルータのフラッシュ メモリ カードにシステム イメージをコピーするには、次の手順を実行します。

ステップ 1 **enable**

このコマンドを使用して特権 EXEC モードを開始します。プロンプトにパスワードを入力します。

```
Router> enable
Password: <password>
Router#
```

ステップ 2 **copy tftp: flash:**

または

copy rcp flash

上記コマンドのいずれか 1 つを使用して、サーバからフラッシュ メモリにファイルをコピーします。

```
Router# copy tftp: flash:
```

ステップ 3 プロンプトに、TFTP サーバまたは RCP サーバの IP アドレスを入力します。

```
Address or name of remote host []? 10.10.10.2
```

ステップ 4 プロンプトに、インストールする Cisco IOS ソフトウェア イメージのファイル名を入力します。

```
Source filename []? c900-universalk9-mz.bin
```

(注) ファイル名では、大文字と小文字が区別されます。

ステップ 5 プロンプトに、ルータ上で使用する予定のファイル名を入力します。通常は、ステップ 4 で使用したのと同じファイル名を入力します。

```
Destination filename []? c900-universalk9-mz.bin
```

ステップ 6 「Not enough space on device（デバイスに十分なスペースがありません）」というエラーメッセージが表示された場合には、フラッシュからファイルを削除して、もう一度やり直してください。フラッシュからファイルを削除するには、**delete flash**: *filename* コマンドを使用します。

ステップ 7 エラー メッセージが表示されない場合には、プロンプトに **no** を入力し、コピーする前にフラッシュ メモリを消去します。

```
Accessing tftp://10.10.10.2/c900-universalk9-mz.bin...
     Erase flash: before copying? [confirm] no
```

次の作業

「新しいシステム イメージのロード」セクション（2-17 ページ）に進みます。

ROM モニタを使用してネットワーク経由でシステム イメージをコピーする方法

このセクションでは、**tftpdnld** ROM モニタ コマンドを使用して、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 イメージをダウンロードする方法について説明します。

tftpdnld ROM モニタ コマンドを入力するには、先に ROM モニタ環境変数を設定しておく必要があります。

前提条件

ルータ上の固定ネットワーク ポートに TFTP サーバを接続します。

（注） **tftpdnld** コマンドを使用できるのは、ルータにファイルをダウンロードする場合のみです。ルータからファイルを取得する目的で **tftpdnld** コマンドを使用することはできません。

tftpdnld ROM モニタ コマンドを使用して、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 イメージをダウンロードするには、次の手順に従います。

ステップ 1 ROM モニタ モードを開始します。

ステップ 2 ルータの IP アドレスを設定します。次に例を示します。

```
rommon > IP_ADDRESS=172.16.23.32
```

ステップ 3 IP サブネット マスクを設定します。次に例を示します。

```
rommon > IP_SUBNET_MASK=255.255.255.224
```

ステップ 4 デフォルト ゲートウェイ アドレスを設定します。次に例を示します。

```
rommon > DEFAULT_GATEWAY=172.16.23.40
```

ステップ 5 TFTP サーバのどこからソフトウェアをダウンロードするのか、保管場所の IP アドレスを設定します。

```
rommon > TFTP_SERVER=172.16.23.33
```

ステップ 6 ルータのどこにイメージ ファイルをダウンロードするのか、保管場所の名前とディレクトリを設定します。次に例を示します。

```
rommon > TFTP_FILE=archive/rel22/<image name>
```

ステップ 7 （任意）入力ポートとしてギガビット イーサネット ポートを使用するように設定します。設定方法は、GE_PORT=[0 | 1 | 2] です。次に例を示します。

```
rommon > GE_PORT=0
```

ステップ 8 **set** コマンドを使用して ROM モニタ環境変数を表示し、各変数が正しく設定されているかどうかを確認します。次に例を示します。

```
rommon > set
```

ステップ 9 **tftpdnld [-r]** コマンドを使用して、ROM モニタ環境変数で指定したとおりにシステム イメージをダウンロードします。**-r** オプションを指定しなかった場合、指定したイメージがダウンロードされてフラッシュ メモリに保存されます。**-r** オプションを指定すると、新しいソフトウェアがダウンロードされて起動されますが、フラッシュ メモリには保存されません。

```
rommon 5 > tftpdnld -r
Attempting to boot from [tftp:]
```

次の作業

「新しいシステム イメージのロード」セクション（2-17 ページ）に進みます。

新しいシステム イメージのロード

ここでは、フラッシュ メモリにコピーした新しいシステム イメージをロードする方法について説明します。最初に、ROM モニタ モードになっているのか、Cisco IOS CLI なのかを判別し、さらに、次の方法のどちらか 1 つで、新しいシステム イメージをロードします。

- Cisco IOS ソフトウェアから新しいシステム イメージをロードする方法（17 ページ）
- ROM モニタ モードから新しいシステム イメージをロードする方法（19 ページ）

Cisco IOS ソフトウェアから新しいシステム イメージをロードする方法

Cisco IOS ソフトウェアから新しいシステム イメージをロードするには、次の手順を実行します。

ステップ 1 **dir flash:**

フラッシュ メモリ内のすべてのファイルおよびディレクトリを表示します。

```
Router# dir flash:

Directory of flash:/

    1  -rw-    64383100  Sep 17 2018 05:58:14 +00:00  c900-universalk9-mz.SSA_09-10
    2  -rw-        1524  Sep 17 2018 05:55:30 +00:00  c900_startupconfig-backup
    3  -rw-         919  Sep 17 2018 05:58:44 +00:00  PSZ22241BW6_20180906052515287.zip

1936031744 bytes total (1871634432 bytes free)
Router#
```

（注） 新しいシステム イメージが **dir flash:** コマンドの出力で先頭のファイルまたは唯一のファイルかどうかを判別します（最初に表示されたファイルまたは唯一のファイルの場合、は不要です）。

ステップ 2 **configure terminal**

グローバル コンフィギュレーション モードを開始します。

```
Router# configure terminal

Router(config)#
```

ステップ 3 **no boot system**

ブート可能なイメージ リストの全エントリを削除します。このイメージ リストを使用して、次回のシステム リロード時またはオフ/オン時に、ルータにシステム イメージのロードを試行させる順序を指定します。

```
Router(config)# no boot system
```

ステップ 4 新しいシステム イメージが **dir flash:** コマンドの出力で先頭のファイルまたは唯一のファイルだった場合、次の手順は不要です。

boot system flash:*system-image-filename*

次回システム リロード後またはオフ/オン後に新しいシステム イメージをロードします。次に例を示します。

```
Router(config)# boot system flash:c900-universalk9-mz.bin
```

ステップ 5 （任意）を繰り返して、ルータにバックアップ システム イメージのロードを試行させる順序を指定します。

ステップ 6 **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。

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

ステップ 7 **show version**

コンフィギュレーション レジスタの設定値を表示します。

```
Router# show version

Cisco Internetwork Operating System Software
.
.
.
Configuration register is 0x0

Router#
```

ステップ 8 コンフィギュレーション レジスタの最終桁が 0 または 1 の場合は、ステップ 9 に進みます。コンフィギュレーション レジスタの最終桁が 2 ～ F の場合は、ステップ 12 に進みます。

ステップ 9 **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。

```
Router# configure terminal

Router(config)#
```

ステップ 10 **config-register 0x2102**

次回のシステム リロード後またはオフ/オン後に、ルータがスタートアップ コンフィギュレーション ファイルの **boot system** コマンドに基づいてシステム イメージをロードするように、コンフィギュレーション レジスタ値を設定します。

```
Router(config)# config-register 0x2102
```

ステップ 11 **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。

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

ステップ 12 **copy run start**

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
Router# copy run start
```

ステップ 13 **reload**

このコマンドを使用してオペレーティング システムをリロードします。

```
Router# reload
```

ステップ 14 システム コンフィギュレーションの保存に関するプロンプトに、**no** を入力します。

```
System configuration has been modified. Save? [yes/no]: no
```

ステップ 15 リロードを確認するプロンプトに、**y** を入力します。

```
Proceed with reload? [confirm] y
```

ステップ 16 **show version**

正しいシステム イメージがロードされたことを確認します。

```
Router# show version

00:22:25: %SYS-5-CONFIG_I: Configured from console by console
Cisco Internetwork Operating System Software
.
.
.
System returned to ROM by reload
System image file is "flash:c900-universalk9-mz.bin"
```

次の作業

「新しいシステム イメージおよびコンフィギュレーションのバックアップ コピーの保存」セクション（2-21 ページ）に進みます。

ROM モニタ モードから新しいシステム イメージをロードする方法

ROM モニタ モードから新しいシステム イメージをロードするには、次の手順を実行します。

ステップ 1 **dir flash:**[*partition-number:*]

フラッシュ メモリ内のファイルを表示します。

```
rommon > dir flash:

program load complete, entry point: 0x4000000, size: 0x18fa0
Directory of flash:

2       48296872  -rw-     c900-universalk9-mz.SPA
```

新しいシステム イメージが **dir flash:** コマンドの出力で先頭のファイルまたは唯一のファイルかどうかに注意します。

ステップ 2 **confreg 0x2102**

次回のシステム リロード後またはオフ/オン後に、ルータがスタートアップ コンフィギュレーション ファイルの **boot system** コマンドに基づいてシステム イメージをロードするように、コンフィギュレーション レジスタ値を設定します。

```
rommon > confreg 0x2102
```

ステップ 3 **boot flash:**[*partition-number*:]*filename*

新しいシステム イメージのロードをルータに強制します。

```
rommon > boot flash:c900-universalk9-mz.binT
```

ステップ 4 新しいシステム イメージがロードされた後、[Return] を数回押して、Cisco IOS CLI プロンプトを表示します。

ステップ 5 **enable**

特権 EXEC モードを開始して、プロンプトにパスワードを入力します。

```
Router> enable
Password: <password>
Router#
```

ステップ 6 **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。

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

ステップ 7 **no boot system**

ブート可能イメージ リストの全エントリを削除します。このイメージ リストには、起動時にルータがロードするシステム イメージが指定されています。

```
Router(config)# no boot system
```

ステップ 8 新しいシステム イメージが **dir flash:** コマンドの出力で先頭のファイルまたは唯一のファイルだった場合、この手順は不要です。

boot system flash:*new-system-image-filename*

次回システム リロード後またはオフ/オン後に新しいシステム イメージをロードします。

```
Router(config)# boot system flash:c900-universalk9-mz.bin
```

ステップ 9 （任意）を繰り返して、ルータにバックアップ システム イメージのロードを試行させる順序を指定します。

ステップ 10 **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。

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

ステップ 11 **copy run start**

実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

```
Router# copy run start
```

次の作業

「新しいシステム イメージおよびコンフィギュレーションのバックアップ コピーの保存」セクション（2-21 ページ）に進みます。

新しいシステム イメージおよびコンフィギュレーションのバックアップ コピーの保存

ファイルが壊れた場合でもファイルを回復できるように、また、ダウンタイムが最小限ですむように、スタートアップ コンフィギュレーション ファイルと Cisco IOS ソフトウェア システム イメージ ファイルのバックアップ コピーをサーバに保存しておくことを推奨します。

ヒント　システムイメージをアップグレードする前に保存したコンフィギュレーションおよびシステムイメージのバックアップ コピーがある場合は、それらを削除しないでください。新しいシステムイメージまたはスタートアップ コンフィギュレーションを使用したときに、重大な問題が発生した場合、以前の実行コンフィギュレーションおよびシステム イメージに即座に戻すことができます。

詳細については、次の URL で『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Managing Configuration Files」の章と「Loading and Maintaining System Images」の章を参照してください。
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book.html

スタートアップ コンフィギュレーション ファイルおよびシステム イメージ ファイルのバックアップ コピーを保存する手順は、次のとおりです。

	コマンドまたはアクション	目的
ステップ 1	**enable** 例: `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します(要求された場合)。
ステップ 2	**copy nvram:startup-config {ftp: | rcp: | tftp:}** 例: `Router# copy nvram:startup-config ftp:`	スタートアップ コンフィギュレーション ファイルをサーバにコピーします。 • コンフィギュレーション ファイルのコピーは、バックアップ コピーとして使用できます。 • プロンプトが表示されたら、コピー先の URL を入力します。
ステップ 3	**dir flash:** 例: `Router# dir flash:`	フラッシュ メモリ ファイル システムのレイアウトとコンテンツを表示します。 • システム イメージ ファイルの名前を書き留めます。
ステップ 4	**copy flash: {ftp: | rcp: | tftp:}** 例: `Router# copy flash: ftp:`	フラッシュ メモリのファイルをサーバにコピーします。 • システム イメージ ファイルをサーバにコピーし、バックアップ コピーとして使用します。 • プロンプトにフラッシュ メモリのパーティション番号を入力します。 • プロンプトが表示されたら、ファイル名とコピー先の URL を入力します。

例

スタートアップ コンフィギュレーションの TFTP サーバへのコピー:例

次に、スタートアップ コンフィギュレーションを TFTP サーバにコピーする例を示します。

```
Router# copy nvram:startup-config tftp:

Remote host[]? 172.16.101.101

Name of configuration file to write [rtr2-confg]? <cr>
Write file rtr2-confg on host 172.16.101.101?[confirm] <cr>
![OK]
```

フラッシュ メモリから TFTP サーバへのコピー:例

次に、**dir flash:** 特権 EXEC コマンドを使用してシステム イメージ ファイルの名前を学習し、**copy flash: tftp:** 特権 EXEC コマンドを使用してシステム イメージを TFTP サーバにコピーする場合の例を示します。このルータはデフォルトのユーザ名とパスワードを使用しています。

```
Router# dir flash:

System flash directory:
File Length Name/status
1 4137888 c920-mz
[4137952 bytes used, 12639264 available, 16777216 total]
16384K bytes of processor board System flash (Read/Write)\

Router# copy flash: tftp:
IP address of remote host [255.255.255.255]? 192.0.0.1
filename to write on tftp host? c920-universalk9-mz
writing c920-mz !!!!...
successful ftp write.
```

移行が可能

新しいルータを注文すると、指定したパッケージおよび機能のソフトウェア イメージとそれに対応するライセンスがプリインストールされた状態で出荷されます。使用前にソフトウェアをアクティブにしたり、登録したりする必要はありません。新しい Cisco IOS 機能をアップグレードまたはインストールするには、ライセンスが必要です。ライセンス タイプ、テクノロジー パッケージおよびインストールの詳細については、『*Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*』を参照してください。

ルータの基本設定

この章では、Cisco 900 シリーズ サービス統合型ルータ（ISR）の設定手順を説明します。また、設定例および検証ステップについても記載されている場合があります。この章は、次の内容で構成されています。

デフォルト設定

Cisco ルータを初めて起動した場合でも、基本的な設定の一部はすでに実行されています。初期設定を表示するには、次の例に示すように、**show running-config** コマンドを使用します。

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

Current configuration : 1087 bytes
!
! No configuration change since last restart
! NVRAM config last updated at 06:11:03 UTC Mon Sep 17 2018
!
version 15.8
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 cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid C921J-4P sn PSZ22241C1T
!
!
!
redundancy
!
!
!
!
!
!
interface GigabitEthernet0
no ip address
!
interface GigabitEthernet1
no ip address
!
interface GigabitEthernet2
no ip address
!
interface GigabitEthernet3
no ip address
!
interface GigabitEthernet4
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet5
ip address 9.6.12.137 255.255.0.0
duplex auto
speed auto
!
interface Vlan1
no ip address
!
ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
!
!
ip route 202.153.144.25 255.255.255.255 9.6.0.1
!
!
!
!
control-plane
!
!
vstack
!
line con 0
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end

Router#
```

グローバル パラメータの設定

次の例で、グローバル パラメータを設定する方法を示します。グローバル パラメータを設定することで、ルータの名前を指定し、ルータへの不正アクセスを防止するための暗号化されたパスワードを指定し、ルータが未知の単語(誤入力)を IP アドレスに変換できないようにします。

```
Router> enable
Router# configure terminal
Router(config)# hostname Router
Router(config)# enable secret pass123
Router(config)# no ip domain-lookup
Router(config)#
```

グローバル パラメータ コマンドの詳細については、Cisco IOS リリース コンフィギュレーション ガイド のマニュアル セットを参照してください。

I/O メモリ割り当ての設定

Cisco 900 シリーズ ISR ルータの I/O メモリおよびプロセッサ メモリで使用中の DRAM の割合を変更するには、グローバル コンフィギュレーション モードで **memory-size iomem** *i/o-memory-percentage* コマンドを使用します。デフォルト メモリの割り当てに戻すには、このコマンドの **no** 形式を使用します。この手順では **smartinit** が有効になります。

構文	説明
i/o-memory-percentage	I/O メモリに割り当てられる DRAM の割合。指定できる値は、5、10、15、20、および 25 です。I/O メモリには、少なくとも 50 MB のメモリが必要です。

コマンドラインで I/O メモリの割合を指定すると、プロセッサ メモリが自動的に DRAM メモリの残りの割合を取得します。

次の例で、DRAM メモリの 25% を I/O メモリに、残りの 75% をプロセッサ メモリに割り当てる方法を示します。

```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# memory-size iomem 5
IO memory size too small:  minimum IO memory size is 201M
Router(config)#
Router(config)# memory-size iomem ?
<5-25>  percentage of DRAM to use for I/O memory: 5, 10, 15, 20, 25

Router(config)# memory-size iomem 25
Smart-init will be disabled and new I/O memory size will take effect upon reload.
Router(config)# end
```

IOMEM の設定の確認

```
Router# show run
Building configuration...

Current configuration : 1087 bytes
!
! No configuration change since last restart
! NVRAM config last updated at 06:11:03 UTC Mon Sep 17 2018
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 25
!
```

インターフェイス ポート

表 3-1 は、Cisco 900 シリーズ サービス統合型ルータでサポートされているインターフェイスのリストです。

表 3-1　Cisco ルータによるインターフェイス

スロット、ポート、論理インターフェイス、インターフェイス	C921	C931	C941
オンボード GE スイッチ ポート	Gi0、Gi1、Gi2、Gi3	Gi0、Gi1、Gi2、Gi3	Gi0、Gi1、Gi2、Gi3
オンボード GE WAN ポート	Gi4、Gi5	Gi4、Gi5	Gi4、Gi5
USB[1]	usbflash0	usbflash0	usbflash0

1. **usbflash0** は、すべての Cisco 900 シリーズ ルータ用の USB インターフェイスです。

ギガビット イーサネット インターフェイスの設定

次の例で、オンボード ギガビット イーサネット(GE)インターフェイスの設定方法を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 4
Router(config-if)# ip address 192.168.12.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

(注) スイッチ ポートは、自動、全二重、および半二重をサポートします。WAN ポートは、全二重のみをサポートします。

インターフェイスの設定を確認するには、**show interface** コマンドを使用します。次に、スイッチ ポートの出力例を示します。

```
Router#show interfaces gig0
GigabitEthernet0 is up, line protocol is up
  Hardware is Gigabit Ethernet, address is 7872.5dab.fe73 (bia 7872.5dab.fe73)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     86738 packets output, 9316451 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

次に、WAN ポートの出力例を示します。

```
Router#show interfaces gig5
GigabitEthernet5 is administratively down, line protocol is down
  Hardware is iGbE, address is 7872.5dab.fe75 (bia 7872.5dab.fe75)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto Duplex, Auto Speed, media type is RJ45
  output flow-control is XON, input flow-control is XON
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     1 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
Router#
```

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。

次の例で、仮想テンプレート インターフェイス上のネットワーク アドレス変換（NAT）をサポートするためにループバック インターフェイスを使用する方法を示します。この設定例は、スタティック IP アドレスとして機能する IP アドレス 200.200.100.1/24 のギガビット イーサネット インターフェイス上に設定されるループバック インターフェイスを示します。ループバック インターフェイスは、ネゴシエートされた IP アドレスを持つ virtual-template1 に紐付けられます。

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

ループバック インターフェイス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
```

コマンドライン アクセスの設定

TTY 回線は、インバウンドまたはアウトバウンド モデムおよび端末接続に使用される非同期回線であり、ルータまたはアクセス サーバの設定で回線 *x* として確認できます。特定の回線番号は、ルータまたはアクセス サーバに組み込まれているか取り付けられているハードウェアの機能です。Cisco 900 シリーズ ルータでは、TTY 回線が 1 つ増えて、回線番号 3 から始まります。

次に、コマンドライン アクセス コマンドの例を示します。"default" とマークされているコマンドを入力する必要はありません。これらのコマンドは、**show running-config** コマンドの使用時に生成されるコンフィギュレーション ファイルに自動的に表示されます。

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

スタティック ルートの設定

スタティック ルートは、ネットワークを介した固定ルーティング パスを提供します。これらは、ルータ上で手動で設定されます。ネットワーク トポロジ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。

次の設定例では、宛先 IP アドレスが 192.168.1.0、サブネット マスクが 255.255.255.0 のすべての IP パケットを、IP アドレス 10.10.10.2 の他の装置に対して、ギガビット インターフェイス上からスタティック ルートで送信します。具体的には、パケットが設定済みの PVC に送信されます。

「(**default**)」と示されているコマンドは、入力する必要はありません。このコマンドは、**show running-config** コマンドの使用時に、生成されたコンフィギュレーション ファイルに自動的に示されます。

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

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, gigabitethernet0
```

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（30 ページ）
- 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（31 ページ）

ルーティング情報プロトコルの設定

次の設定例は、IP ネットワーク 10.0.0.0 および 192.168.1.0 で有効にされる RIP version 2 を示しています。

```
Router> configure terminal
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.1
Router(config-router)# network 10.10.7.1
Router(config-router)# no auto-summary
Router(config-router)# end
```

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。次に示す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

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

```
Router> configure terminal
Router(config)# router eigrp 109
Router(config)# network 192.145.1.0
Router(config)# network 10.10.12.115
Router(config-router)# end
```

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" で示される 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
```

イーサネット スイッチの設定

この章では、Cisco 900 シリーズ ISR のギガビット イーサネット（GE）スイッチの設定作業の概要について説明します。

この章の内容は、次のとおりです。

VLAN の設定

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

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

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

VLAN の設定例については、「例：VLAN の設定」を参照してください。

例：VLAN の設定

次の例で、VLAN 間ルーティングの設定方法を示します。

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

VTP の設定

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

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

VTP の設定に関する次の概念を理解する必要があります。

- VTP ドメイン：VTP ドメイン（別名 VLAN 管理ドメイン）は、1 つのスイッチ、または同じ VTP ドメイン名を共有して同一管理下にある相互接続された複数のスイッチまたはスイッチ スタックで構成されます。スイッチは、1 つの VTP ドメインにだけ所属できます。そのドメインに対してグローバル VLAN の設定を変更します。
- VTP サーバ：VTP サーバ モードでは、VLAN の作成、変更、削除ができます。また、VTP ドメイン全体に対して他のコンフィギュレーション パラメータ（VTP バージョンなど）を指定できます。VTP サーバは、同一 VTP ドメイン内の他のスイッチに自分の VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズメントに基づいて、自分の VLAN 設定を他のスイッチと同期させます。VTP サーバはデフォルト モードです。
- VTP クライアント：VTP クライアントは VTP サーバと同様に動作し、対応するトランクで VTP アップデートを送受信しますが、VTP クライアント上で VLAN の作成、変更、削除を行うことはできません。VLAN は、ドメインに含まれる、他のサーバ モードのスイッチで設定します。

- VTP トランスペアレント:VTP トランスペアレント スイッチは、VTP に参加しません。VTP トランスペアレント スイッチは自身の VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて自身の VLAN 設定を同期させることもありません。ただし、VTP バージョン 2 またはバージョン 3 では、トランスペアレント スイッチは、トランク インターフェイスを介して他のスイッチから受信した VTP アドバタイズを転送します。VTP トランスペアレント モードでは、スイッチ上の VLAN を作成、変更、削除できます。

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

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

VTP の設定例については、「例:VTP の設定」を参照してください。

例:VTP の設定

次に、スイッチを VTP サーバとして設定する例を示します。

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

次に、スイッチを VTP クライアントとして設定する例を示します。

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

次に、スイッチを VTP トランスペアレントとして設定する例を示します。

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

802.1x 認証の設定

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

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

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

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

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

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

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

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

次の例で、Cisco 900 シリーズ ISR を 802.1x オーセンティケータとして設定する方法を示します。

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

スパニングツリー プロトコルの設定

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

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

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

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

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

STP の設定に関する詳細については、次のリンクを参照してください。

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

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

例:スパニングツリー プロトコルの設定

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MAC アドレス テーブル操作の設定

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

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

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

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

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

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

例:MAC アドレス テーブル操作

次に、ポートのセキュア MAC アドレス オプションを有効にする設定の例を示します。

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

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

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

次に、セキュア MAC アドレスの最大数を 10 に設定する例を示します。

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

次に、エージング タイマーを設定する例を示します。

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

MAC アドレス通知トラップの設定

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

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

例:MAC アドレス通知トラップの設定

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

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

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

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

スイッチド ポート アナライザ(SPAN)の設定

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

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

SPAN 設定の例については、例:SPAN の設定(40 ページ)を参照してください。

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

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

例:SPAN の設定

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

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

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

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

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

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

IGMP スヌーピングの設定

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

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

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

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

例：IGMP スヌーピングの設定

次の例で、IGMP スヌーピングを VLAN インターフェイスで有効にする方法を示します。

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

次の例で、マルチキャスト ルータへの静的な接続を有効にする方法を示します。

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

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

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

ポート単位のストーム コントロールの設定

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

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

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

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

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

（注） C900 プラットフォームでは、**storm-control action shutdown** コマンドを設定すると、ポートの状態が管理上ダウンに変化します。ポートの状態を手動で元に戻すには、**no shutdown** コマンドを使用します。

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

例：ポート単位のストーム コントロールの設定

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

```
Router# configure terminal
Router(config)# interface gigabitethernet 2
Router(config-if)# storm-control multicast level 70.0 30.0
Router(config-if)# end
Router# show storm-control multicast
Interface  Filter State   Upper    Lower    Current
---------  -------------  -------  -------  -------
Gi0        inactive       100.00%  100.00%    N/A
Gi1        inactive       100.00%  100.00%    N/A
Gi2        Forwarding      70.00%   30.00%   0.00%
```

HSRP の設定

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

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

HSRP の設定に関する詳細については、次のリンクを参照してください。

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

HSRP の設定例については、「例：HSRP の設定」を参照してください。

例：HSRP の設定

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

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

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

```
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

VRRP の設定

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

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

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

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

VRRP に関する詳細については、次のリンクを参照してください。

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

VRRP の設定例については、「例：VRRP の設定」を参照してください。

例：VRRP の設定

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

グループ 1：

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

グループ 5:

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

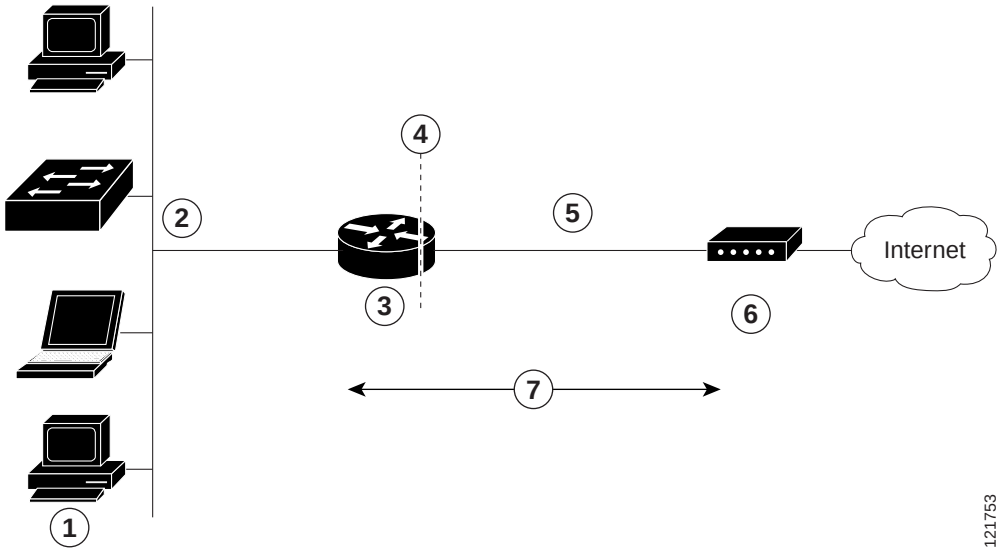
```
RouterA(config)# interface GigabitEthernet 1
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip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

RouterA(config-if)# end

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

PPP over Ethernet と NAT の設定

この章では、Cisco 900 シリーズ サービス統合型ルータ（ISR）で設定できる Point-to-Point Protocol over Ethernet（PPPoE）クライアントおよびネットワーク アドレス変換（NAT）の概要について説明します。

ルータの背後の LAN には、複数の PC を接続できます。これらの PC からのトラフィックは PPPoE セッションに送信する前に暗号化やフィルタリングなどを行うことができます。図 5-1 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 5-1　　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 900 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 860 または Cisco 880 ISR によってクライアント側で開始されます。確立された PPPoE クライアント セッションは、次のいずれかの方法で終了できます。

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

NAT

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

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

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

この設定タスクの結果を示す例は「設定例」セクション（50 ページ）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。

次の例で、VPDN を設定する方法を示します。

```
Router(config)# vpdn enable
Router(config)# vpdn-group 1
Router(config-vpdn)# request-dialin
Router(config-vpdn-req-in)# protocol pppoe
Router(config-vpdn-req-in)# exit
Router(config-vpdn)# exit
```

イーサネット WAN インターフェイスの設定

このシナリオでは、PPPoE クライアント（Cisco ルータ）が、内部および外部インターフェイスの 10/100/1000 Mbps イーサネット インターフェイスと通信します。

次の例で、ファスト イーサネット WAN インターフェイスの設定方法を示します。

```
Router(config)# interface gigabitethernet 4
Router(config-if)# pppoe-client dial-pool-number 1
Router(config-if)# no shutdown
Router(config-if)# exit
```

イーサネット運用管理およびメンテナンス

イーサネット運用管理およびメンテナンス（OAM）は、イーサネット メトロポリタン エリア ネットワーク（MAN）およびイーサネット WAN の設置、モニタリング、トラブルシューティングのためのプロトコルで、開放型システム間相互接続（OSI）モデルのデータ リンク層の新しいオプション サブレイヤを使用します。このプロトコルによって提供される OAM の機能には、ディスカバリ、リンク モニタリング、リモート障害検知、リモート ループバック、および Cisco Proprietary Extension（シスコ独自の拡張機能）があります。

イーサネット OAM の設定および構成情報については、次の URL で『*Using Ethernet Operations, Administration, and Maintenance*』を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/configuration/15-mt/ce-15-mt-book/ce-oam.html

ダイヤラ インターフェイスの設定

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

次の例で、ルート上のギガビット イーサネット LAN インターフェイスの 1 つにダイヤラ インターフェイスを設定する方法を示します。

```
Router(config)# interface dialer 0
Router(config-if)# ip address negotiated
Router(config-if)# ip mtu 1492
Router(config-if)# encapsulation ppp
Router(config-if)# ppp authentication chap
Router(config-if)# dialer pool 1
Router(config-if)# dialer-group 1
Router(config-if)# exit
Router(config)# dialer-list 1 protocol ip permit
Router(config)# ip route 10.10.25.2 255.255.255.255 dialer 0
```

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。

次の例で、ダイナミック NAT を使用して外部ギガビット イーサネット WAN インターフェイスを設定する方法を示します。

```
Router(config)# ip nat pool pool1 192.168.1.0 192.168.2.0 netmask 255.255.252.0
Router(config)# ip nat inside source list 1 interface dialer 0 overload
Router(config)# interface vlan 1
Router(config-if)# ip nat inside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gigabitethernet1 Router(config-if)# ip nat outside
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# access-list 1 permit 192.168.1.0 255.255.255.0
```

(注) 仮想テンプレート インターフェイスとともに NAT を使用するには、ループ バック インターフェイスを設定する必要があります。ループバック インターフェイスの設定の詳細については、第 3 章「ルータの基本設定」を参照してください。

設定例

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

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

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

```
vpdn enable
vpdn-group 1
request-dialin
protocol pppoe
!
interface vlan 1
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast (default)
ip nat inside
interface gigabitethernet 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。

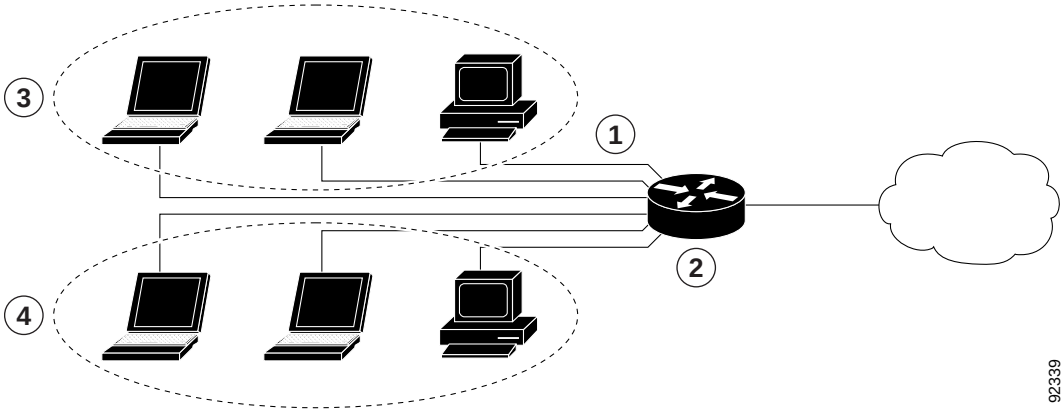
```
Router# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  gigabitethernet4
Inside interfaces:
  Vlan1
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 interface Dialer0 refcount 0
Queued Packets: 0
```

DHCP および VLAN による LAN の設定

Cisco 900 シリーズ サービス統合型ルータ（ISR）は、物理 LAN と VLAN の両方でクライアントをサポートします。各ルータは Dynamic Host Configuration Protocol（DHCP）を使用して、このようなネットワーク上にある各ノードに対して、IP 設定の自動割り当てをイネーブルにできます。

図 6-1 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 6-1　　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 900 シリーズ アクセス ルータ）
3	VLAN 1
4	VLAN 2

DHCP

DHCP は、RFC 2131 に説明されているように、アドレス割り当てにクライアント/サーバ モデルを採用しています。管理者は、Cisco 900 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。

VLANs

Cisco 900 シリーズ アクセス ルータは、VLAN を設定できる 4 つのギガビット イーサネット ポートをサポートします。

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

設定作業

次の作業を実行して、このネットワーク シナリオを設定します。

- DHCP の設定
- VLAN の設定

(注) この章の各手順では、ルータの基本機能、NAT による PPPoE または PPPoA をすでに設定していることを前提とします。これらの設定作業を実行していない場合には、使用しているルータに応じて第 3 章「ルータの基本設定」と第 5 章「PPP over Ethernet と NAT の設定」を参照してください。

DHCP の設定

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

```
Router(config)# ip domain name smallbiz.com
Router(config)# ip name-server 192.168.11.12
Router(config)# ip dhcp excluded-address 192.168.9.0
Router(config)# ip dhcp pool dpool1
Router(config-dhcp)# import all
Router(config-dhcp)# network 10.10.0.0 255.255.255.0
Router(config-dhcp)# default-router 10.10.10.10
Router(config-dhcp)# dns-server 192.168.35.2
Router(config-dhcp)# domain-name cisco.com
Router(config-dhcp)# exit
```

DHCP 設定を表示するには、次のコマンドを使用します。

- **show ip dhcp import**：DHCP サーバ データベースにインポートされたオプションのパラメータを表示します。
- **show ip dhcp pool**：DHCP アドレス プールに関する情報を表示します。
- **show ip dhcp server statistics**：アドレス プールおよびバインディングの数などの DHCP サーバ統計情報を表示します。

```
Router# show ip dhcp import
Address Pool Name: dpool1

Router# show ip dhcp pool
```

```
Pool dpool1 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 10.10.0.1            10.10.0.1        - 10.10.0.254       0

Router# show ip dhcp server statistics
Memory usage         15419
Address pools        1
Database agents      0
Automatic bindings   0
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
Router#
```

VLAN の設定

次の例で、ルータで VLAN を設定する方法を示します。

```
Router(config)# vlan 2
Router(config)# exit
```

VLAN へのスイッチ ポートの割り当て

次の例で、VLAN にスイッチ ポートを割り当てる方法を示します。

```
Router(config)# interface gigabitethernet 2
Router(config-if)# switchport access vlan 2
Router(config-if)# end
Router(config-if)#
```

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
```

レイヤ 3 インターフェイスでの ID 機能の設定

この章では、Cisco 900 サービス統合型ルータ（ISR）のオンボード ギガビット イーサネット レイヤ 3 ポートでサポートされている ID 機能について説明します。

この章の内容は、次のとおりです。

（注） クリティカル認証（アクセス不能認証バイパスまたは AAA 失敗ポリシーとも呼ばれる）は、オンボード ギガビット イーサネット レイヤ 3 ポートの ID 機能をサポートしていません。

認証方法

ID 機能は、さまざまな種類のエンド ホストおよびユーザに適したさまざまなタイプの認証方法をサポートしています。主に次の 2 つの方法が使用されます。

- IEEE 802.1X
- MAC 認証バイパス（MAB）

IEEE 802.1X の設定

次の例で、Cisco 900 ISR で IEEE 802.1X を設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control auto
Router(config-if)#dot1x pae authenticator
Router(config-if)# end
Router#
```

設定を確認するには、**show authentication sessions** コマンドを使用します。

```
Router#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi1          000d.e105.c771  dot1x    DATA     Authz Success  0303030300000000000BA04

Router#show authentication sessions interface Gi1
            Interface:  GigabitEthernet1
          MAC Address:  0201.0201.0201
           IP Address:  Unknown
            User-Name:  testUser1
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
         AAA Policies:
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0303030300000000000BA04
      Acct Session ID:  0x00000001
               Handle:  0x6D000001

Runnable methods list:
       Method   State
       dot1x    Authc Success

Router#
```

MAC 認証バイパス（MAB）の設定

次の例で、MAB を設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control auto
Router(config-if)# mab
Router(config-if)# end
Router#
```

設定を確認するには、**show authentication sessions** コマンドを使用します。

```
Router#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi1          0201.0201.0201  mab      DATA     Authz Success  0303030300000004002500A8
```

```
Router#show authentication sessions interface Gi1
            Interface:  GigabitEthernet1
          MAC Address:  0201.0201.0201
           IP Address:  Unknown
            User-Name:  02-01-02-01-02-01
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
         AAA Policies:
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  03030303000000004002500A8
      Acct Session ID:  0x00000007
               Handle:  0x3D000005

Runnable methods list:
       Method   State
       mab      Authc Success

Router#
```

ポートの認証状態の制御

ポート認証を制御するには、次の方法を使用します。

- force-authorized：IEEE 802.1X を無効にして、認証交換を要求せずにポートを認証済み状態に移行させます。ポートは、クライアントの IEEE 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
- force-unauthorized：クライアントによる認証の試みをすべて無視し、ポートを未認証状態のままにします。ルータは、インターフェイス経由でクライアントに認証サービスを提供できません。
- auto：IEEE 802.1X 認証を有効にして、ポートを未認証状態で開始します。ポート経由で送受信できるのは、Extensible Authentication Protocol over LAN（EAPoL）フレームのみです。ポートのリンク状態がダウンからアップに移行するか、EAPoL-Start フレームを受信すると、認証プロセスが開始されます。ルータは、クライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。ルータは、クライアントの MAC アドレスを使用して、ネットワーク アクセスを試みる各クライアントを一意に識別します。クライアントが正常に認証されると、ポートが認証済みの状態に変わり、認証されたクライアントからの全フレームはポート経由で許可されるようになります。認証が失敗した場合、ポートは無許可ステートのままですが、認証を再試行できます。

ポート認証状態の制御の設定

次の例で、ポート認証状態の制御を設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication port-control {auto | force-authorized |
force-unauthorized}
Router(config-if)# mab
Router(config-if)# end
Router#
```

ポート認証状態の制御を確認するには、**show authentication sessions** コマンドと **show dot1x** コマンドを使用します。

```
Router#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi1          (unknown)       dot1x    DATA     Authz Success  030303030000000A002CFCBC

Router#show authentication sessions interface gi1
            Interface:  GigabitEthernet1
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  030303030000000A002CFCBC
      Acct Session ID:  0x0000000D
               Handle:  0x7C00000B

Runnable methods list:
       Method   State
       dot1x    Authc Success

Router#show dot1x interface g0
Dot1x Info for GigabitEthernet0
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = FORCE_AUTHORIZED
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Router#show authentication sessions

Interface      MAC Address     Method   Domain   Status         Session ID
Gi1          (unknown)       dot1x    DATA     Authz Failed   030303030000009002AB7FC

Router#show authentication sessions interface gi0
            Interface:  GigabitEthernet0
```

```
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Failed
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0303030300000009002AB7FC
      Acct Session ID:  0x0000000C
               Handle:  0x8B00000A

Runnable methods list:
       Method   State
       dot1x    Authc Failed

Router#show dot1x interface g0
Dot1x Info for GigabitEthernet0
-----------------------------------
PAE                         = AUTHENTICATOR
PortControl                 = FORCE_UNAUTHORIZED
ControlDirection            = Both
HostMode                    = SINGLE_HOST
QuietPeriod                 = 60
ServerTimeout               = 0
SuppTimeout                 = 30
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30
```

フレキシブル認証

フレキシブル認証シーケンシングを使用すると、ユーザは、ルータ ポートで認証方法のすべてまたは一部を有効にして、認証方法を実行する順序を指定できます。

フレキシブル認証の設定

フレキシブル認証の設定の詳細については、次を参照してください。

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-service/application_note_c27-573287.html

ホスト モード

オンボード ギガビット イーサネット レイヤ 3 ポートの ID 機能では、シングルホスト モードのみがサポートされています。シングルホスト モードの場合、IEEE 802.1X 対応のルータ ポートに接続できるのは 1 つのクライアントのみです。ルータは、ポートのリンク状態がアップに変化したときに、EAPoL フレームを送信することによってクライアントを検出します。クライアントがログオフした場合、または別のクライアントに替わった場合、ルータは、ポートのリンク状態をダウンに変更し、ポートは未認証状態に戻ります。

オープン アクセス

オープン アクセス機能を使用すると、クライアントまたはデバイスは、認証が実行される前にネットワーク アクセスを取得できます。この機能は、主にブート前実行環境（PXE）シナリオで必要です。このシナリオでは、デバイスが、PXE がタイムアウトする前にネットワークにアクセスし、サプリカントが含まれるブート可能イメージをダウンロードする必要があります。

オープン アクセスの設定

次の例で、オープン アクセスを設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication open
Router(config-if)# end
Router#
```

Control-Direction（Wake-on-LAN）

ルータが Wake-on-LAN（WoL）による IEEE 802.1X 認証を使用している場合、ルータは、マジックパケットを含むトラフィックを未認証の IEEE 802.1X ポートに転送します。ポートが未認証の間、スイッチは、EAPoL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内の他のデバイスに送信することはできません。

Control-Direction（Wake-on-LAN）の設定

次の例で、Control-Direction（Wake-on-LAN）を設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 0
Router(config-if)# authentication control-direction both
Router(config-if)# end
Router#
```

デフォルトの control-direction setting-both を確認するには、**show authentication sessions** コマンドと **show dot1x** コマンドを使用します。

```
Router#show authentication sessions interface Gi0
            Interface:  GigabitEthernet0
          MAC Address:  0201.0201.0201
           IP Address:  Unknown
            User-Name:  testUser1
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
         AAA Policies:
      Session timeout:  N/A
```

```
         Idle timeout:  N/A
    Common Session ID:  0303030300000000000BA04
      Acct Session ID:  0x00000001
               Handle:  0x6D000001

Runnable methods list:
       Method   State
       dot1x    Authc Success

Router#

Router#show dot1x int g0
Dot1x Info for GigabitEthernet0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

authentication control-direction setting-in を確認するには、show authentication sessions コマンドと show dot1x コマンドを使用します。

```
Router#show authentication sessions interface gi0
            Interface:  GigabitEthernet0
          MAC Address:  0201.0201.0201
           IP Address:  Unknown
            User-Name:  testUser1
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  in
        Authorized By:  Authentication Server
           Vlan Group:  N/A
         AAA Policies:
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  030303030000000C00310024
      Acct Session ID:  0x0000000F
               Handle:  0x8C00000D

Runnable methods list:
       Method   State
       dot1x    Authc Success

Router#show dot1x interface g0
Dot1x Info for GigabitEthernet0
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = In
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

事前認証アクセス制御リスト

Open-Access がインストールされている場合、デフォルトのポートアクセス制御リスト（ACL）をオーセンティケータで設定することを推奨します。ACL を使用すると、エンドポイントは、IP アドレスの取得と実行に必要な最小限のネットワーク アクセスを取得できます。

事前認証アクセス制御リストの設定

ACL の事前設定の詳細については、次を参照してください。

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/port_acls.html#wp1039754

ダウンロード可能アクセス コントロール リスト

ダウンロード可能な ACL は dACL とも呼ばれます。dACL をポートで動作させるには、IP デバイストラッキング機能を有効にし、ポートに接続されているエンドポイントに IP アドレスを割り当てる必要があります。ポートでの認証後、**show ip access-list privileged EXEC** コマンドを使用して、ポートにダウンロードした ACL を表示します。

フィルタ ID または名前付きアクセス制御リスト

フィルタ ID も dACL として機能しますが、オーセンティケータに ACL コマンドが設定されています。認証、認可、およびアカウンティング（AAA）は、オーセンティケータに ACL の名前を提示します。

IP デバイス トラッキング

dACL およびフィルタ ID 機能を有効にするには、IP デバイス トラッキング機能が必要です。デバイスで dACL またはフィルタ ID をプログラムするには、IP アドレスが必要です。IP デバイストラッキングは、対応するデバイスの IP アドレスを Enterprise Policy Manager（EPM）モジュールに提示します。その IP アドレスを dACL に追加することにより、各ユーザ向けに dACL が変換されます。

セキュリティ機能の設定

この章では、Cisco 900 シリーズ サービス統合型ルータ（ISR）でのセキュリティ機能の設定方法について説明します。この章の内容は、次のとおりです。

SSL VPN の設定

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

SSL VPN 設定の詳細については、次の URL で『*SSL VPN Configuration Guide, Cisco IOS Release 15M&T*』を参照してください。

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

認証、許可、アカウンティング

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

AAA では、Remote Authentication Dial-In User Service（RADIUS; リモート認証ダイヤルイン ユーザ サービス）、Terminal Access Controller Access Control System Plus（TACACS+; ターミナル アクセス コントローラ アクセス コントロール システム プラス）、または Kerberos などのプロトコルを使用してセキュリティ機能を管理します。ルータがネットワーク アクセス サーバとして機能している場合、AAA は、ネットワーク アクセス サーバと RADIUS、TACACS+、または Kerberos セキュリティ サーバ間の通信を確立するための手段となります。

AAA サービスおよびサポートされているセキュリティ プロトコル、認証、許可、アカウンティング、RADIUS、TACACS+、または Kerberos の設定については、次の URL で『*Cisco IOS Security Configuration Guide: Securing User Services*』を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-mt/secuser-15-mt-library.html

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

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、https://www.cisco.com/c/en/us/td/docs/ios/sec_user_services/configuration/guide/convert/user_security/sec_autosecure.html にある機能ガイドを参照してください。

アクセス リストの設定

アクセス リストは、送信元 IP アドレス、宛先 IP アドレス、またはプロトコルに基づいてインターフェイス上のネットワーク トラフィックを許可または拒否します。アクセス リストは、標準版または拡張版のどちらかに設定されます。標準アクセス リストは、指定された送信元からのパケットの通過を許可または拒否します。拡張アクセス リストでは、宛先および送信元の両方を指定できます。また、各プロトコルを指定して、通過を許可または拒否することができます。

アクセス リスト作成の詳細については、次の URL で『*Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T*』を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book.html

アクセス 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 8-1 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 8-1　アクセス リスト コンフィギュレーション コマンド

アクセス コントロール リスト（ACL）タイプ	コンフィギュレーション コマンド
番号形式	
規格	**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	
規格	**ip access-list standard** *name* **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 グループ

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

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

アクセス グループの設定および管理の詳細については、次の URL で『*Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T*』の「Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values」セクションを参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book.html

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 ファイアウォールでは、パケットを検査するため、アプリケーション層のデータを検証してトラフィックの許可または拒否を決定できます。静的アクセス リストでは、これは検証不可能です。

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 パラメータは、リターン トラフィックがルータを通過せずに、ダイナミック アクセス リストがアクティブの状態を保つ時間を指定します。タイムアウト値が指定値に達すると、ダイナミック アクセス リストが削除され、後続のパケット（有効なパケットの場合もある）が許可されなくなります。

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

Cisco IOS ファイアウォールの設定の詳細については、『*Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T*』（https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html）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 インスペクションでは、基本的な検査機能（ピンホール開口部の SIP パケット インスペクションおよび検出）に加え、プロトコルの適合性やアプリケーション セキュリティを提供します。詳細については、『*Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T*』（https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/fw-sip-alg-aic.html）を参照してください。

ゾーンベース ポリシー ファイアウォール

Cisco IOS ゾーンベース ポリシー ファイアウォールを使用すると、インターフェイスを異なるゾーンに割り当て、ポリシーを設定することでセキュリティ ポリシーを展開し、これらのゾーン間を行き来するトラフィックを検査できるようになります。ポリシーでは、定義したトラフィック クラスに適用する一連のアクションを指定します。

ゾーンベース ポリシー ファイアウォール設定の詳細については、『*Security Configuration Guide: Zone-Based Policy Firewall, Cisco IOS Release 15M&T*』（https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html）を参照してください。

Cisco IOS IPS の設定

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

Cisco IOS IPS では、「シグネチャ」を使用して攻撃を特定し、ネットワーク トラフィック内における悪用パターンを検出します。Cisco IOS IPS は、インライン侵入検出センサーとして機能し、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、現在アクティブな（ロードされている）アタック シグネチャのいずれかと一致するかどうかについてそれぞれをスキャンします。Cisco IOS IPS により不審なアクティビティが検出されると、ネットワーク セキュリティが損なわれる前に対応し、イベントを記録します。また、検出されたシグニチャに対して設定されたアクションに基づいて、次の操作を実行します。

- syslog フォーマットでアラームを送信する、または Secure Device Event Exchange（SDEE; セキュア デバイス イベント交換）フォーマットでアラームのログを取る
- 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 設定の詳細については、次のマニュアルの「Cisco IOS IPS 5.x Signature Format Support and Usability Enhancements」セクションを参照してください。

次の URL の『*Cisco IOS Intrusion Prevention System Configuration Guide, Cisco IOS Release 15MT*』:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_ios_ips/configuration/15-mt/sec-data-ios-ips-15-mt-book/sec-ips5-sig-fs-ue.html

コンテンツのフィルタリング

Cisco 900 シリーズ ISR には、カテゴリに基づく URL フィルタリング機能があります。ユーザは、許可または拒否する Web サイトのカテゴリを選択し、ISR 上で URL フィルタリングを準備します。各カテゴリの URL のチェックには、サードパーティが保守する外部サーバが使用されています。ポリシーの許可および拒否は、ISR 上で保守されています。サービスは、加入ベースで提供され、各カテゴリの URL はサードパーティ ベンダーによってメンテナンスされています。

URL フィルタリングの設定に関する詳細情報については、『Subscription-based Cisco IOS Content Filtering』（https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/subscrip-cont-filter.html）を参照してください。

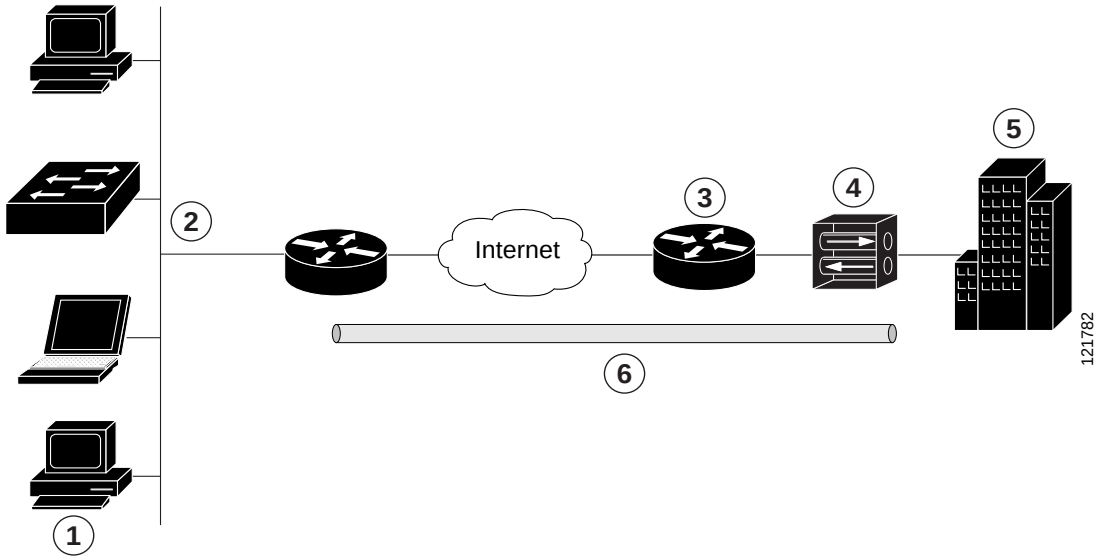
VPN の設定

バーチャル プライベート ネットワーク（VPN）接続は、インターネットなどのパブリック ネットワークを介して、2 つのネットワーク間に安全な接続を提供します。Cisco 900 シリーズ ISR は、VPN のサイト間アクセスとリモート アクセスの 2 種類をサポートします。リモート アクセス VPN は、企業ネットワークにログインする際にリモート クライアントによって使用されます。サイト間 VPN は、たとえば、ブランチ オフィスと企業オフィスを接続する際に使用されます。この項では、それぞれの例を示します。

リモート アクセス VPN の例

リモート アクセス VPN コンフィギュレーションでは、Cisco Easy VPN および IP Security（IPSec）トンネルを使用して、リモート クライアントとコーポレート ネットワーク間の接続を設定および保護します。図 8-1 は、一般的な構成例を示します。

図 8-1　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 900 シリーズ ISR
3	ルータ：コーポレート オフィスのネットワーク アクセスを提供
4	VPN サーバ：Easy VPN サーバ（外部インターフェイス アドレスが 210.110.101.1 の VPN 終端装置など）
5	ネットワーク アドレスが 10.1.1.1 のコーポレート オフィス
6	IPSec トンネル

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

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

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

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

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

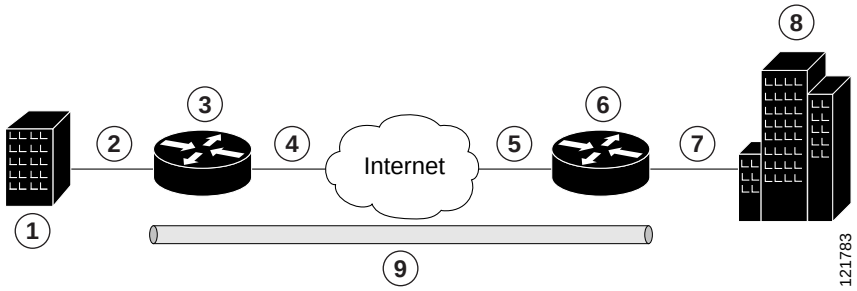
Cisco 900 シリーズ ISR は、Cisco Easy VPN サーバとして動作するように設定することもでき、この機能を使用すると、許可された Cisco Easy VPN クライアントは、接続されたネットワークへのダイナミック VPN トンネルを確立できます。Cisco Easy VPN サーバの設定手順については、次の URL で *Easy VPN サーバ* 機能を参照してください。

https://www.cisco.com/c/en/us/td/docs/ios/sec_secure_connectivity/configuration/guide/convert/sec_easy_vpn_15_1_book.html

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 8-2 は、一般的な構成例を示します。

図 8-2　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 900 シリーズ ISR
4	ファスト イーサネットまたは ATM インターフェイス（NAT 用の外部インターフェイス、アドレスは 200.1.1.1）
5	LAN インターフェイス（外部インターフェイス アドレスは 210.110.101.1）：インターフェイスに接続
6	VPN クライアント：企業ネットワークへのアクセスを制御する別のルータ
7	LAN インターフェイス（内部インターフェイス アドレスは 10.1.1.1）：企業ネットワークに接続
8	コーポレート オフィス ネットワーク
9	GRE を使用した IPSec トンネル

IPSec および GRE の設定の詳細については、次の URL で『*Security for VPNs with IPsec Configuration Guide, Cisco IOS Release 15M&T*』の「Configuring Security for VPNs with IPSec」の章を参照してください。
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book.html

ダイナミック マルチポイント VPN の設定

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）機能を使用すると、ユーザは、GRE トンネル、IPsec 暗号化、および Next Hop Resolution Protocol（NHRP; ネクスト ホップ レゾリューション プロトコル）を組み合わせて大規模および小規模な IP セキュリティ（IPsec）VPN を設定できるようになります。

DMVPN 設定の詳細については、次の URL で『*Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T*』を参照してください。

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

Group Encrypted Transport VPN の設定

Group Encrypted Transport（GET; グループ暗号化トランスポート）VPN は、Cisco IOS デバイス上で発生する、または Cisco IOS デバイス を経由するプライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能です。GET VPN では、キー プロトコル Group Domain of Interpretation（GDOI; グループ ドメイン オブ インタープリテーション）と IPsec 暗号化を組み合わせ、IP マルチキャスト トラフィックまたはユニキャスト トラフィックを保護するための効率的な方法をユーザに提供します。GET VPN では、ルータによって、トンネル化されていない（つまり「ネイティブな」）IP マルチキャストおよびユニキャスト パケットに対して暗号化を適用できるので、マルチキャストおよびユニキャスト トラフィックを保護するためにトンネルを設定する必要がありません。

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

GET VPN 設定の詳細については、
https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-2mt/sec-get-vpn.html
を参照してください。

イーサネット タギングにおける SGT

Cisco TrustSec（CTS）は、エンドツーエンドのネットワーク インフラストラクチャであり、ロールベースのアクセス制御、ID 認識型ネットワーキングを適用するための拡張性に優れたアーキテクチャを提供するとともに、ネットワークとそのリソースの保護に役立つデータ機密性を実現します。CTS は、各ネットワーク ユーザおよびリソースの特定と認証、およびセキュリティ グループ タグ（SGT）と呼ばれる 16 ビットの番号の割り当てによって機能します。その後、SGT がネットワーク ホップ間で順番に伝搬されます。結果として、中間デバイス（スイッチとルータ）はアイデンティティ タグに基づいたポリシーを適用できるようになります。

CTS 対応デバイスには、MAC（L2）レイヤ内に組み込まれた SGT を持つパケットを送受信できる、ハードウェア機能が組み込まれています。この機能は、L2-SGT インポジションと呼ばれます。この機能により、デバイスのイーサネット インターフェイスで L2-SGT インポジションを有効にできるため、そのデバイスはネクスト ホップ イーサネット ネイバーに伝送されるパケットに SGT を挿入できるようになります。イーサネット タギングにおける SGT は、クリアテキスト（非暗号化）イーサネット パケットに組み込まれた SGT のホップバイホップ伝搬の一種です。

Cisco TrustSec の詳細については、
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/config.html
を参照してください。

暗号化エンジン スループット ポリシング

暗号化スループット ポリシングには、パケット レート ポリシングとビット レート ポリシングの 2 つのタイプがあります。

パケット レート ポリシング

Cisco 921J ルータは、パケット レート（パケット/秒）ポリシングをサポートしています。実際のビット レート スループット（ビット/秒）は、パケット サイズによって異なります。

SKU	パケット レート制限（pps）
C921J	85616

ビット レート ポリシング

Cisco 931 および C921 ルータは、ビット レート（ビット/秒）ポリシングをサポートしています。

SKU	ビット レート制限（Mbps）
C931	250
C921	150

ポリシングによるパケット ドロップを表示するには、**show crypto engine accelerator statistic** コマンドを使用します。次に、Cisco 921J ルータに対するコマンドの出力例を示します。

```
router#show crypto engine accelerator statistic

Device:   Onboard VPN
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 1440809 seconds ago
            95487781408 packets in                95486424592 packets out
         33644619163784 bytes in               33644414868202 bytes out
                  66273 paks/sec in                     66272 paks/sec out
                 186809 Kbits/sec in                   186808 Kbits/sec out
              497655085 packets decrypted           499488995 packets encrypted
         18274163849048 bytes before decrypt    15370455314736 bytes encrypted
         15369938845298 bytes decrypted         18274476022904 bytes after encrypt
                Last 5 minutes:
               26066232 packets in                    26066232 packets out
                  86887 paks/sec in                      86887 paks/sec out
              250994648 bits/sec in                  250995151 bits/sec out
```

```
             4247760866 bytes decrypted            4248382774 bytes encrypted
              114804347 Kbits/sec decrypted         114821156 Kbits/sec encrypted

Onboard VPN:
        ds: 0x10E31D10        idb:0x0EA74988

        Statistics for Virtual Private Network (VPN) Module:

        RAW API handler invoked:       997144123
        Available IPSEC static pak:          957
        Packets returned from drops:     1356816
        Pkts returned from raw rtrn:   997144110
        Available Pre-batch entries:         959

        Particle copy:                     0
        Particle swap:                     0
        Particle reparent:        998500926
        Packet overruns:                   0
        Output packets dropped:            0

        1440809 seconds since last clear of counters

CE Status Related Packet Stats
===============================
           Crypto Internal Error : 1
                 Resource Errors : 1356815

SKU information:
================
Max Bandwidth:250 Mbps  IMIX-size:365 Packets-per-second (PPS):85616
Statistics information:
  Packets handled 95486424673
  Packets dropped 1356815
```

次に、Cisco 931 ルータに対するコマンドの出力例を示します。

```
Router#show crypto engine accelerator statistic
Device:   Onboard VPN
Location: Onboard: 0
                :Statistics for encryption device since the last clear
                 of counters 2569 seconds ago
                     151982466 packets in                  142427991 packets out
                   54548953852 bytes in                  51715073454 bytes out
                         59160 paks/sec in                     55441 paks/sec out
                        169858 Kbits/sec in                   161033 Kbits/sec out
                      67912187 packets decrypted            74515857 packets encrypted
                   27818735160 bytes before decrypt       26730230184 bytes encrypted
                   22213021398 bytes decrypted            29502075720 bytes after encrypt
                                Last 5 minutes:
                      22436614 packets in                   22436387 packets out
                         74788 paks/sec in                     74787 paks/sec out
                     219207775 bits/sec in                  219204787 bits/sec out
                    3667993316 bytes decrypted             3670433984 bytes encrypted
                      99134954 Kbits/sec decrypted           99200918 Kbits/sec encrypted

Onboard VPN:
                ds: 0x12EA45B8        idb:0x123EF0D0

                Statistics for Virtual Private Network (VPN) Module:

                RAW API handler invoked:       142428045
                Available IPSEC static pak:          957
                Packets returned from drops:     9554448
```

```
                Pkts returned from raw rtrn:   142428044
                Available Pre-batch entries:         959

                Particle copy:                     0
                Particle swap:             70265739
                Particle reparent:         81716753
                Packet overruns:                   0
                Output packets dropped:            0

                2569 seconds since last clear of counters

CE Status Related Packet Stats
===============================
           Crypto Internal Error : 1
                 Resource Errors : 9554447

SKU information:
=================
Max Bandwidth:250 Mbps
Statistics information:
  Packets handled 142428045
  Packets dropped 9554447
```

次に、Cisco 921 ルータに対するコマンドの出力例を示します。

```
Router#show crypto engine accelerator statistic
Device:   Onboard VPN
Location: Onboard: 0
                :Statistics for encryption device since the last clear
                 of counters 3014 seconds ago
                      36412147 packets in                   33336964 packets out
                   13812996658 bytes in                  11412671776 bytes out
                         12081 paks/sec in                    11060 paks/sec out
                         36661 Kbits/sec in                   30290 Kbits/sec out
                      26024533 packets decrypted             7312452 packets encrypted
                   10920338080 bytes before decrypt        2892660426 bytes encrypted
                    8516694798 bytes decrypted             2895986384 bytes after encrypt
                                Last 5 minutes:
                      14963577 packets in                   12694499 packets out
                         49878 paks/sec in                    42314 paks/sec out
                     146860315 bits/sec in                  123543958 bits/sec out
                    2179066680 bytes decrypted             2349328596 bytes encrypted
                      58893694 Kbits/sec decrypted           63495367 Kbits/sec encrypted

Onboard VPN:
                ds: 0x135C41CC        idb:0x132B2FE0

                Statistics for Virtual Private Network (VPN) Module:

                RAW API handler invoked:        33336985
                Available IPSEC static pak:          957
                Packets returned from drops:     3075165
                Pkts returned from raw rtrn:    33336985
                Available Pre-batch entries:         959

                Particle copy:                     0
                Particle swap:             36412150
                Particle reparent:                 0
                Packet overruns:                   0
                Output packets dropped:            0
```

```
                 3014 seconds since last clear of counters

CE Status Related Packet Stats
================================
                  Resource Errors : 3075165

SKU information:
=================
Max Bandwidth:150 Mbps
Statistics information:
  Packets handled 33336985
  Packets dropped 3075165
```

VDSL2 と ADSL2/2+ の設定

この章では、Cisco 900 シリーズ ISR でマルチモード VDSL2 および ADSl2+ WAN 接続を設定する方法について説明します。VDSL2 および ADSl2+ WAN 接続により、顧客宅内機器（CPE）とセントラル オフィス間の高速デジタル データ伝送が実現します。この章の内容は、次のとおりです。

概要

組織は、データ機器とセントラルオフィス間での高速デジタル データ伝送の運用を必要とします。セントラルオフィスは、通常、電気通信サービスプロバイダー施設内に配置されます。シスコのマルチモード VDSL2 および ADSL2/2+ は、1 ポート（2 ペア）マルチモード VDSL2 および ADSL2/2+ WAN 接続を提供します。この接続と Cisco 900 シリーズ サービス統合型ルータを組み合わせることにより、顧客宅内機器（CPE）とセントラルオフィス間の高速デジタル データ伝送が実現します。

次の表で、VDSL2 および ADSL2/2+ のバリエーションについて説明します。

未完成ドキュメント(レビュー要) - シスコ社外秘

製品番号	説明
C926-4P Annex B	1 ポート(1 ペア)VDSL2/ADSL2 + over ISDN • ADSL1/2/2+ Annex B、最適化されていない ADSL2/2+ Annex J • ベクタリングを使用した VDSL2 over ISDN バンド プラン(8b ～ 17a)
C927-4P Annex A	1 ポート(2 ペア)VDSL2/ADSL2+ over POTS • VDSL2 over POTS バンド プラン – VDSL2 プロファイル:8a、8b、8c、8d、12a、12b、17a – ベクタリング • ADSL1/2/2+ Annex A、ADSL2 Annex L、最適化されていない ADSL2/2+ Annex M
C927-4PM Annex M	1 ポート(2 ペア)VDSL2/ADSL2+ over POTS with Annex M • VDSL2 over POTS バンド プラン – VDSL2 プロファイル:8a、8b、8c、8d、12a、12b、17a – ベクタリング • 最適化された ADSL2/2+ Annex M • ADSL/ADSL2/2+ Annex A/M

DSL の設定

Cisco 900 シリーズ サービス統合型ルータ(ISR)は、非対称デジタル加入者線(ADSL)2/2+ と超高速デジタル加入者線 2(VDSL2)の伝送モード(マルチモードとも呼ばれる)をサポートします。

DSL 設定の制限事項

- Cisco 900 シリーズ ルータは、ペア 0 のみをサポートします。
- VDSL モード ボンディングはサポートされていません。30a プロファイルはサポートされていません。

ADSL モードの設定

ADSL モードを設定するには、次の作業を行います。

- ADSL auto モードの設定(81 ページ)
- ADSL モードの CPE およびピアの設定(81 ページ)
- ADSL 設定の確認(83 ページ)
- ADSL の CPE からピアへの接続の確認(85 ページ)

ADSL auto モードの設定

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

次の例で、ADSL コントローラを auto モードに設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# controller vdsl 0
Router(config-controller)# operating mode auto
Router(config-controller)# end
Router#
```

ADSL モードの CPE およびピアの設定

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

ATM CPE 側の設定

次の例で、ATM CPE 側の設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface atm0
Router(config-if)# no shutdown
Router(config-if)# interface ATM0.1 point-to-point
Router(config-subif)# ip address 30.0.0.1 255.255.255.0
Router(config-subif)# pvc 13/32
Router(config-if-atm-vc)# protocol ip 30.0.0.2 broadcast
Router(config-if-atm-vc)# end
```

ATM ピア側の設定

次の例で、ATM ピア側の設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface atm0
Router(config-if)# no shutdown
Router(config-if)# interface ATM0.1 point-to-point
Router(config-subif)# ip address 30.0.0.2 255.255.255.0
Router(config-subif)# pvc 13/32
Router(config-if-atm-vc)# protocol ip 30.0.0.1 broadcast
Router(config-if-atm-vc)# end
Router#
```

ADSL の設定例

次の例で、auto モードに設定された一般的な ADSL2+ 設定を示します。

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

未完成ドキュメント(レビュー要) - シスコ社外秘

```
Current configuration : 1519 bytes
!
! Last configuration change at 08:46:20 UTC Fri Jan 11 2019
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:c900-universalk9-mz.SPA.158-3.M1
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid C927-4P sn FGL22511283
!
!
!
redundancy
!
!
controller VDSL 0
!
!
!
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 13/32
  protocol ip 30.0.0.2 broadcast
 !
!
interface Ethernet0
 no ip address
```

```
!
interface GigabitEthernet0
 no ip address
!
interface GigabitEthernet1
 no ip address
!
interface GigabitEthernet2
 no ip address
!
interface GigabitEthernet3
 no ip address
!
interface GigabitEthernet4
 ip address 9.6.9.29 255.255.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip tftp source-interface GigabitEthernet4
ip tftp blocksize 8192
ip route 0.0.0.0 0.0.0.0 9.6.0.1
ip route 202.153.144.25 255.255.255.255 9.6.0.1
!
!
!
tftp-server flash:/firmware/vadsl_module_img.bin
!
control-plane
!
!
line con 0
exec-timeout 0 0
line 4
no activation-character
transport preferred none
transport input all
transport output all
stopbits 1
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end
```

ADSL 設定の確認

特権 EXEC モードで **show controller vdsl 0** コマンドを使用して、正しく設定されていることを確認します。

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

未完成ドキュメント(レビュー要) - シスコ社外秘

```
Daemon Status:           Up

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xB11F
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    FCH2234TH6R C927-4P 15.8(3)M1
Serial Number Far:     eq_nr multiline_cpe software_rev
Modem Version Near:    15.8(3)M1
Modem Version Far:     0xb11f

Modem Status:          TC Sync (Showtime!)

DSL Config Mode:         AUTO
Trained Mode:   G.992.5 (ADSL2+) Annex A

TC Mode:                 ATM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Link Status:             UP

Full inits:             26
Failed full inits:      15
Short inits:            8
Failed short inits:     3

Firmware        Source          File Name
--------        ------          ----------
VDSL            embedded        VDSL_LINUX_DEV_01212008

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039x8.d26d

Line:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                       ON
SRA:                     disabled                 disabled
 SRA count:              0                        0
Bit swap:                enabled                  enabled
 Bit swap count:         0                        1
Line Attenuation:         1.0 dB                   2.4 dB
Signal Attenuation:       1.9 dB                   2.1 dB
Noise Margin:            10.8 dB                   7.3 dB
Attainable Rate:        27564 kbits/s            1283 kbits/s
Actual Power:            - 0.4 dBm               12.0 dBm
Total FECC:             0                        0
Total ES:               284                      77
Total SES:              150                      1
Total LOSS:             13                       0
Total UAS:              86969                    86840
Total LPRS:             0                        0
Total LOFS:             71                       0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):           0            27547            0               1279
SRA Previous Speed:     0                0            0                  0
```

```
Previous Speed:          0           27547            0             1279
Total Cells:             0        11338923            0           520053
User Cells:              0               0            0                0
Reed-Solomon EC:         0               0            0                0
CRC Errors:              0            5166            0              717
Header Errors:           0               0            0                0
Interleave (ms):      0.00            0.07         0.00             0.49
Actual INP:           0.00            0.00         0.00             0.00

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

ADSL の CPE からピアへの接続の確認

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

```
Router# ping 30.0.0.2 rep 20

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

VDSL モードの設定

VDSL モードを設定するには、次の作業を行います。

- VDSL auto モードの設定（85 ページ）
- VDSL モードの CPE およびピアの設定（85 ページ）
- VDSL 設定の確認（88 ページ）
- VDSL の CPE からピアへの接続の確認（89 ページ）

VDSL auto モードの設定

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

次の例で、VDSL コントローラを auto モードに設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# controller vdsl 0
Router(config-controller)# operating mode auto
Router(config-controller)# end
Router#
```

VDSL モードの CPE およびピアの設定

VDSL を設定する場合には、ethernet 0 インターフェイスを設定し、必要に応じて **no shutdown** コマンドを実行します。

未完成ドキュメント（レビュー要）- シスコ社外秘

VDSL CPE 側の設定

次の例で、VDSL CPE 側の設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet0
Router(config-if)# ip address 90.0.0.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
```

VDSL ピア側の設定

次の例で、VDSL ピア側の設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet0
Router(config-if)# ip address 90.0.0.2 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
```

VDSL の設定例

次の例で、VDSL 設定の一般的な出力を示します。

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

Current configuration : 1456 bytes
!
! Last configuration change at 08:51:44 UTC Fri Jan 11 2019
!
version 15.8
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot system flash:c900-universalk9-mz.SPA.158-3.M1
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid C927-4P sn FGL22511283
!
!
!
redundancy
!
!
controller VDSL 0
!
!
!
!
!
interface ATM0
 no ip address
 shutdown
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
!
interface Ethernet0
 ip address 90.0.0.1 255.255.255.0
!
interface GigabitEthernet0
 no ip address
!
interface GigabitEthernet1
 no ip address
!
interface GigabitEthernet2
 no ip address
!
interface GigabitEthernet3
 no ip address
!
interface GigabitEthernet4
 ip address 9.6.9.29 255.255.0.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip tftp source-interface GigabitEthernet4
ip tftp blocksize 8192
ip route 0.0.0.0 0.0.0.0 9.6.0.1
ip route 202.153.144.25 255.255.255.255 9.6.0.1
!
!
!
tftp-server flash:/firmware/vadsl_module_img.bin
!
```

未完成ドキュメント（レビュー要）- シスコ社外秘

```
control-plane
!
!
line con 0
exec-timeout 0 0
line 4
no activation-character
transport preferred none
transport input all
transport output all
stopbits 1
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end
```

VDSL 設定の確認

特権 EXEC モードで **show controller vdsl 0** コマンドを使用して、正しく設定されていることを確認します。

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

Daemon Status:           Up

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xB11F
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:    FCH2234TH6R C927-4P 15.8(3)M1
Serial Number Far:     eq_nr multiline_cpe software_rev
Modem Version Near:    15.8(3)M1
Modem Version Far:     0xb11f

Modem Status:          TC Sync (Showtime!)

DSL Config Mode:         AUTO
Trained Mode:   G.993.2 (VDSL2) Profile 17a

TC Mode:                 PTM
Selftest Result:         0x00
DELT configuration:      disabled
DELT state:              not running
Link Status:             UP

Full inits:             28
Failed full inits:      15
Short inits:            8
Failed short inits:     7

Firmware        Source          File Name
--------        ------          ----------
VDSL            embedded        VDSL_LINUX_DEV_01212008

Modem FW  Version:      4.14L.04
```

```
Modem PHY Version:      A2pv6F039x8.d26d

Line:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                       ON
SRA:                     disabled                disabled
 SRA count:              0                       0
Bit swap:                enabled                 enabled
 Bit swap count:         0                       0
Line Attenuation:         0.9 dB                  0.0 dB
Signal Attenuation:       1.8 dB                  0.0 dB
Noise Margin:            18.6 dB                 17.6 dB
Attainable Rate:        138139 kbits/s           87957 kbits/s
Actual Power:            14.1 dBm                 3.8 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   0.2     0.9     1.7     N/A     0.0     0.0     0.0
Signal Attenuation(dB): 0.2     0.9     1.7     N/A     0.0     0.0     0.0
Noise Margin(dB):       27.7    16.9    10.9    N/A     15.5    16.3    21.3
Total FECC:             302690                   3
Total ES:               295                      77
Total SES:              161                      1
Total LOSS:             14                       0
Total UAS:              87189                    87049
Total LPRS:             0                        0
Total LOFS:             80                       0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):            0           128857            0             60013
SRA Previous Speed:      0                0            0                 0
Previous Speed:          0            27451            0              1288
Reed-Solomon EC:         0                0            0                 0
CRC Errors:              0            24722            0                 1
Header Errors:           0                8            0                 0
Interleave (ms):       0.00             7.00         0.00              1.00
Actual INP:      0.00      1.00      0.00      0.10

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

VDSL の CPE からピアへの接続の確認

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

```
Router# ping 90.0.0.2 rep 20

Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 90.0.0.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 20/22/28 ms
Router#
```

未完成ドキュメント（レビュー要）- シスコ社外秘

VLAN 0 優先順位タギングの設定

VLAN 0 優先順位タギング機能を使用すると、VLAN ID をゼロに設定した 802.1Q イーサネットフレームを送信できます。これらのフレームは優先順位がタグ付けされたフレームと呼ばれます。VLAN ID のタグをゼロに設定すると、VLAN ID タグを無視して、802.1Q イーサネット フレーム ヘッダーの 802.1P ビットで設定されている優先順位に従って処理することができます。

次の例で、CPE 側での VLAN 優先順位タギングの設定方法を示します。

```
Router# configure terminal
Router(config)# interface GigabitEthernet0
Router(config-if)# encapsulation priority-tagged
Router(config-if)# ip address 2.2.2.1 255.255.255.0
Router(config-if)# end
```

次の例で、ピア側での VLAN 優先順位タギングの設定方法を示します。

```
Router# configure terminal
Router(config)# interface GigabitEthernet0
Router(config-if)# encapsulation priority-tagged
Router(config-if)# ip address 2.2.2.2 255.255.255.0
Router(config-if)# end
```

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

```
Router#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
isr4221#sh run int gi0/0/0.1
Building configuration...

Current configuration : 105 bytes
!
interface GigabitEthernet0/0/0.1
 encapsulation priority-tagged
 ip address 2.2.2.2 255.255.255.0
end
```

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

次の例で、Over POTS VDSL2/ADSL マルチモード Annex A SKU で ADSL2/2+ Annex M モードを有効にする方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# controller vdsl 0
Router(config-controller)# operating mode adsl2+ annex m
Router(config-controller)# end
Router#
```

シームレス レート適応のイネーブル化

次の例で、SRA モードを有効にする方法を示します。

```
router# configure terminal
router(config)# controller vdsl 0
router(config-controller)# sra
router(config-controller)# end
router#
```

(注) SRA を無効にするには、コマンドの **no** 形式を使用します。SRA モードはデフォルトでディセーブルです。

UBR+ の設定

次の例で、DSL 回線で UBR + PVC を設定する方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# interface ATM 0/0
Router(config-if)# pvc 4/100
Router(config-if-atm-vc)# ubr+ 2304 2304
```

次の例では、ATM PVC の output-pcr 引数に 100000 kbps を、output-mcr 引数に 3000 kbps を指定しています。

```
Router> enable
Router# configure terminal
Router(config)# interface ATM 0/0
Router(config-if)# pvc 1/32
Router(config-if-atm-vc)# ubr+ 100000 3000
```

次の例では、ATM SVC の output-pcr、output-mcr、input-pcr、および input-mcr 引数に、それぞれ 10000 kbps、3000 kbps、9000 kbps、および 1000 kbps を指定しています。

```
Router> enable
Router# configure terminal
Router(config)# interface ATM 0/0
Router(config-if)# svc lion nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
Router(config-if-atm-vc)# ubr+ 10000 3000 9000 1000
```

トラブルシューティング

DSL のトラブルシューティングには、次の show コマンドを使用します。

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

未完成ドキュメント（レビュー要）- シスコ社外秘

DSL トレーニング ログの収集

トレーニング ログには、ADSL トレーニング中に発生したさまざまなイベントに関する情報が記載されています。

次の例は DSL トレーニング ログの収集を開始する方法を示します。

```
Router#debug vdsl 0 training log
Training log generation started for VDSL 0.
```

次の例は DSL トレーニング ログの収集を中止する方法を示します。

```
Router#no debug vdsl 0 training log
Training Log file for VDSL 0 written to flash:vdsllog.bin.
```

トレーニング ログでは、自動停止オプションもサポートされています。自動停止には次のコマンドを使用します。

no debug vdsl 0 training log autostop linkdown: リンクがダウンした場合、収集を中止します。
no debug vdsl 0 training log autostop linkup: リンクが showtime に達した場合、収集を中止します。

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

トレーニング ログが保存されているファイル名を変更してから、トレーニング ログの収集を開始します。次の例は、ファイル名を変更する方法を示します。

```
Router#conf t
Router(config)#controller vdsl 0
Router(config-controller)#training log filename flash:mytraininglog.bin
Router(config-controller)#end
Router#sh controller vdsl 0 | sec Training Log
Training Log :Stopped
Training Log Filename :flash:mytraininglog.bin
Router#
```

DSL ファームウェアのアップグレード

DSL インターフェイスのファームウェアをアップグレードするには、次の手順を実行します。

ステップ 1 https://software.cisco.com/download/home のシスコ ソフトウェア ダウンロード センターから VDSL2 ファームウェアをダウンロードします。

ステップ 2 ファームウェアをルータにコピーします。

ステップ 3 指定された場所から新しいファームウェアをロードするようにルータを設定します。

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#controller vdsl 0
Router(config-controller)#firmware filename ?
  archive:   Download fw file name
  cns:       Download fw file name
  flash:     Download fw file name
  ftp:       Download fw file name
  http:      Download fw file name
```

```
  https:     Download fw file name
  null:      Download fw file name
  nvram:     Download fw file name
  pram:      Download fw file name
  rcp:       Download fw file name
  scp:       Download fw file name
  security:  Download fw file name
  system:    Download fw file name
  tar:       Download fw file name
  tftp:      Download fw file name
  tmpsys:    Download fw file name

Router(config-controller)#firmware filename flash:vdsl_fw.bin_39p1
```

ステップ 4 新しいファームウェアを有効にするには、コントローラ インターフェイスを再起動します。

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#controller vdsl 0
Router(config-controller)#shut
Router(config-controller)#no shut
Router(config-controller)#end
```

未完成ドキュメント（レビュー要）- シスコ社外秘

4G 無線 WAN の設定

この章では、Cisco 900 シリーズ ISR での 4G 無線 WAN インターフェイスの設定について説明します。具体的な内容は次のとおりです。

4G LTE の概要

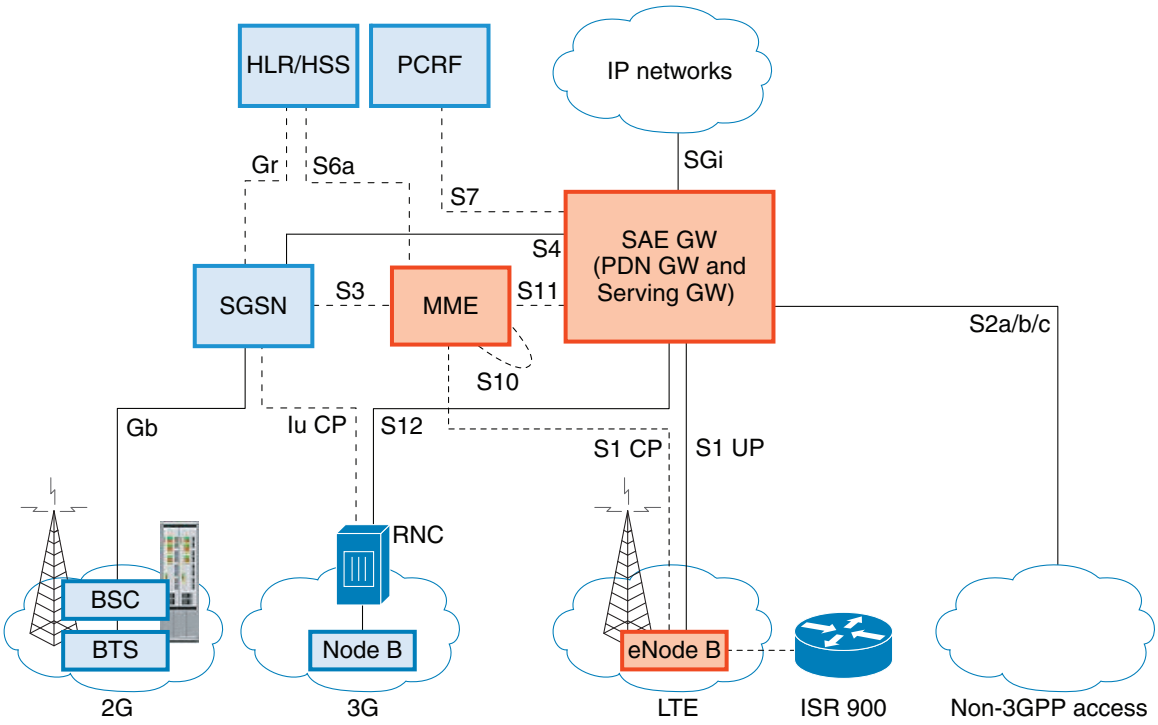
Cisco 900 シリーズ ルータは、無線 WAN（WWAN）をサポートしています。WWAN SKU は、第 4 世代 Long-Term Evolution（4G LTE）の携帯電話ネットワークや第 3 世代（3G）携帯電話ネットワークで動作します。Cisco 900 シリーズ ルータは、DSL やフレーム リレーに代わる、安全性が高くシンプルでコスト効率の高い WAN を提供します。地上ブロードバンド サービス（ケーブル、DSL、T1）が利用できない地域や、設備投資が高額となる地域では、4G LTE WWAN 接続が現実的な選択肢です。

Cisco 900 シリーズ ルータは、次の 4G/3G モードをサポートしています。

- **4G LTE**：4G LTE モバイル仕様では、マルチメガビットの帯域幅、より効率的な無線ネットワーク、遅延の減少、改善されたモビリティが提供されます。LTE ソリューションは新しい携帯電話ネットワークを対象とします。これらのネットワークは、当初、ダウンリンクで最大 97 Mb/s のピーク レートを、アップリンクで最大 50 Mb/s のピーク レートをサポートします。これらのネットワークのスループットは既存の 3G ネットワークよりも大きくなります。
- **3G Evolution High-Speed Packet Access（HSPA/HSPA+）**：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。

図 1 で、4G LTE パケット コア ネットワーク アーキテクチャを説明します。

図 1　　4G LTE のパケット コア ネットワーク アーキテクチャ



ゲートウェイ	Serving Gateway（SGW）は、ユーザ プレーンのモビリティ アンカーとしても機能する一方で、ユーザ データ パケットをルーティングおよび転送します。また、LTE および他の 3 GPP 技術間のモビリティ アンカーでもあります。Packet Data Network（PDN）ゲートウェイ（PGW）は、ユーザ機器（UE）のトラフィックが出入りするポイントになることによって、UE から外部パケット データ ネットワークへの接続を提供します。 UE は複数の PDN にアクセスするために複数の PGW との同時接続を持つ場合があります。PGW は、ポリシー施行、各ユーザへのパケット フィルタリング、課金サポート、合法的傍受、およびパケット スクリーニングを実行します。PGW のもう一つの主な役割は、3GPP と非 3GPP 技術との間のモビリティ アンカーとして機能することです。後者には、WiMAX や 3GPP2（CDMA 1X、EvDO）などがあります。 System Architecture Evolution GW（SAE GW）は、Evolved Packet Core（EPC）内の PGW および SGW 機能を扱うエンティティです。
RNC	Radio Network Controller（RNC）は、接続先の Radio Access Network（RAN）の制御に責任を持ちます。RNC は、無線リソース管理および一部のモビリティ管理機能を実行し、ユーザ データがモバイルへまたはモバイルから送信される前に暗号化が実行されるポイントです。RNC はメディア ゲートウェイ（MGW）を介して回線交換のコア ネットワークに接続します。
MME	モビリティ マネージメント エンティティ。
SGW	サービング ゲートウェイ。
PCRF	ポリシー/課金ルール機能
SAE	サービス アーキテクチャの進化。

SGSN	サービング GPRS サポート ノード
HSS	ホーム サブスクライバ サーバ
HLR	ホーム ロケーション レジスタ
BTS	ベース トランシーバ ステーション
BSC	ベース ステーション コントローラ
SGSN	サービス GPRS サポート ノード

Cisco 4G-LTE の機能

Cisco 4G LTE WWAN は、次の主な機能をサポートしています。

- 3G/4G Simple Network Management Protocol（SNMP）MIB
- プライマリおよびバックアップのリンク間の自動切り替えフェールオーバー
- SIM のロックおよびロック解除機能
- PLMN 検索
- ショート メッセージ サービス（SMS）
- 3G 後方互換性
- IPv4 および IPv6 のアドレッシング
- 自動 SIM ファームウェア スイッチング
- コール履歴
- セルラー バックオフ
- モデムのリセット、モデムの電源再投入、無線のオン/オフ
- モデムの crashdump の収集
- ダイヤラ
- DM ロギング
- 外部マイクロ USB
- Firmware アップグレード
- リンク リカバリ
- モデム LED
- 複数のプロファイル
- PnP LTE WebUI の統合
- SIM OIR
- DMVPN
- CAT

次の機能はサポートされていません。

- Dying Gasp
- MEP
- マルチ PDN コンテキスト

- LTE モジュール OIR
- GPS と NMEA
- デュアル SIM
- QoS
- NAS メッセージ（SVB）
- デュアル モデム
- 2K MTU
- キャリア アグリゲーション
- FOTA（ファームウェア Over-The-Air）
- CAT6

Cisco 4G LTE 設定の前提条件

- 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、加入者認証モジュール（SIM）カードを取得する必要があります。
- 4G LTE ワイヤレス WAN モジュールを設定する前に、SIM カードを取り付ける必要があります。SIM カードの取り付け手順について詳しくは、データ コール用の SIM 設定（101 ページ）を参照してください。

Cisco 4G LTE 設定の制約事項

Cisco 4G LTE を設定する際は、次の制約事項および使用上のガイドラインにしたがってください。

- 現在、携帯電話ネットワークは、ユーザによるベアラーの確立だけをサポートします。
- 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。
- 携帯電話ネットワークは、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。遅延は信号条件に依存し、ネットワークで輻輳が発生している場合、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。
- SNMP エージェントが実行されるルータでは、NMS およびエージェントが適切に動作するよう、Cisco IOS CLI を使用して、適切なアクセス コントロール（たとえば、SNMP サーバ コミュニティなど）を設定する必要があります。
- SNMP SET 動作を実装する場合、認証/プライバシーを使用した SNMP V3 を設定することを、強く推奨します。

Cisco 4G LTE の設定方法

このセクションでは、Cisco 900 シリーズ ルータで 4G LTE を設定する方法について説明します。

モデム信号強度およびサービス可用性の確認

モデム信号強度とサービス可用性を確認するには、次の show コマンドを使用します。

- **show cellular** *unit* **network**
- **show cellular** *unit* **radio**
- **show cellular** *unit* **profile**
- **show cellular** *unit* **security**
- **show cellular** *unit* **all**

	コマンドまたはアクション	目的
ステップ 1	**show cellular** *unit* **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** *unit* **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 3	**show cellular** *unit* **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 4	**show cellular** *unit* **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 5	**show cellular** *unit* **all** 例: `Router# show cellular 0 all`	モデム、作成されたプロファイル、無線信号の強さ、ネットワーク セキュリティなどに関する統合的な情報を示します。

モデム データ プロファイルの作成、変更、削除

4G LTE SKU で複数のプロファイルを作成できます。一部のモデムのデフォルトのインターネット プロファイル番号は次のとおりです。

- WP7607:プロファイル 1
- WP7608:プロファイル 1
- WP7609:接続用のプロファイル 1 とデータ プロファイル用のプロファイル 3

データ プロファイルの作成、変更、削除に関する使用上のガイドライン

データ プロファイルの設定では、次のガイドラインにしたがってください。

- モデムにデータ プロファイルが付属している場合、通常はプロファイル関連の変更は不要です。
- 接続タイプ用にプロファイル パラメータの変更が必要な場合は、原則として、デフォルト プロファイル内で変更を実施します。
- プロファイル タイプを別々に設定し、それぞれ異なる接続で使用したい場合は、APN 名などのパラメータを変えることで、別々のプロファイルを作成することが可能です。なお、一度にアクティブにできるプロファイルは 1 つだけであることに注意してください。
- プロファイルを作成または変更するには、**cellular 0 lte profile create 1** ***APN-name*** **none ipv4v6** を使用します。
- プロファイルを削除するには、**cellular 0 lte profile delete 1** ***APN-name*** **none ipv4v6** または **cellular 0 lte profile delete 1** を使用します。
- データ プロファイルを表示するには、**show cellular <> profile** コマンドを使用します。データ プロファイルには、アスタリスク(*)が表示されます。
- データ プロファイルはデータ コールの設定に使用されます。別のプロファイルを使用したい場合、そのプロファイルをデフォルトにする必要があります。デフォルト プロファイルを変更するには、**lte sim data-profile** *number attach-profile number* コマンドを使用します。

設定例

次の例で、デフォルト プロファイルを変更する方法を示します。

```
router(config-controller)# lte sim data-profile 2 attach-profile 1
router(config-controller)# end
router#
router# sh run
Building configuration...
controller Cellular 0
 lte sim profile 2

router# ping 8.8.4.4 rep 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.192.187.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/69/106 ms
Viper-19#
```

次に、**show cellular** コマンドの出力例を示します。

```
router# show cellular 0 profile
Profile 1 = ACTIVE* **
```

```
--------
PDP Type = IPv4v6
PDP address = 29.29.29.73
PDP IPV6 address = 2001:2678:2680:6E88:4DCC:F4F5:B936:C7EF/64 Scope: Global
Access Point Name (APN) = broadband
Authentication = None
Username:
Password:
Primary DNS address = 8.0.0.8
Secondary DNS address = 8.8.4.4
Primary DNS IPV6 address = 2006:4888:4888:0:0:0:0:8899
Secondary DNS IPV6 address = 2002:8888:9999:0:0:0:0:7722

* - Default profile
** - LTE attach profile
```

データ コール用の SIM 設定

PIN コードを使用した SIM カードのロックおよびアンロック

サービス プロバイダーによって指定された SIM カードをロックまたはロック解除するには、**cellular** *unit* **lte sim** {**lock** | **unlock**} *pin* コマンドを使用します。

注意 誤った PIN が連続して 3 回入力されると SIM カードはブロックされます。SIM に設定されている正しい PIN を必ず入力してください。SIM カードがブロックされた場合、PUK コードのサービス プロバイダーにお問い合わせください。PUK コードを使用することで、SIM カードのブロックが解除できます。

次の例で、PIN コードを使用して SIM をロックする方法を示します。

```
Router# cellular 0 lte sim lock 1111
```

PIN コードの変更

SIM の PIN コードを変更するには、**cellular** *unit* **lte sim change-pin** *pin new-pin* コマンドを使用します。次の例で、PIN コードを変更する方法を示します。

```
Router# cellular 0 lte sim change-pin 1111 1234
```

モデムのセキュリティ情報の確認

モデムのセキュリティ情報を確認するには、**show cellular** *unit* **security** コマンドを使用します。次の例で、セキュリティ情報を確認する方法を示します。

```
Router# show cellular 0 security
```

ロックされた SIM の自動認証の設定

暗号化されていない PIN を設定して、モデムを認証する Card Holder Verification（CHV1）コードをアクティベートすることができます。

注意 誤った PIN が連続して 3 回入力されると SIM カードはブロックされます。SIM に設定されている正しい PIN を必ず入力してください。SIM カードがブロックされた場合、PUK コードのサービス プロバイダーにお問い合わせください。

（注） CHV1 を設定するために暗号化されないレベル 0 の PIN を使用する場合は次の手順にしたがってください。暗号化されたレベル 7 の PIN を使用して CHV1 を設定する方法については、SIM の暗号化ピンの設定（102 ページ）を参照してください。

（注） SIM 認証が機能するには、SIM がロックされている必要があります。SIM ステータスを確認するには、**show cellular** *unit* **security** コマンドを使用します。

次の例で、ロックされた SIM の自動認証を設定する方法を示します。

```
Router# configure terminal
Router(config)# controller cellular 0
Router(config-controller)# lte sim authenticate 0 1111
```

SIM の暗号化ピンの設定

暗号化された PIN を設定するには、PIN のスクランブル値を取得する必要があります。次の例で、スクランブル レベル 7 の PIN を取得し、この暗号化 PIN を使用して検証用の SIM CHV1 コードを設定する方法を示します。

```
Router# configure terminal
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do show run | i SIM
Router(config)# controller cellular 0
Router(config-controller)# lte sim authenticate 7 055A575E70
Router(config-controller)# exit
```

（注） SIM の暗号化ピンを取得すると、パスワード暗号化を設定し、ユーザ名と関連パスワードを決定し、スクランブルがかかったパスワードをコピーし、スクランブルがかかったパスワードを SIM 認証コマンドで使用することによって、ユーザ名とパスワードが作成されます。スクランブル PIN が取得され、SIM 認証で使用されると、作成されたユーザ名を Cisco IOS コンフィギュレーションから削除することができます。

(注) SIM 認証が機能するには、SIM がロックされている必要があります。SIM ステータスを確認するには、**show cellular** *unit* **security** コマンドを使用します。

SIM コンフィギュレーションのモデム プロファイルの適用

次の例で、モデム プロファイルの適用方法を示します。

```
Router# configure terminal
Router(config)# controller cellular 0
Router(config-controller)# lte sim data-profile 2 attach-profile 2
```

詳細については、SIM の設定：例（113 ページ）を参照してください。

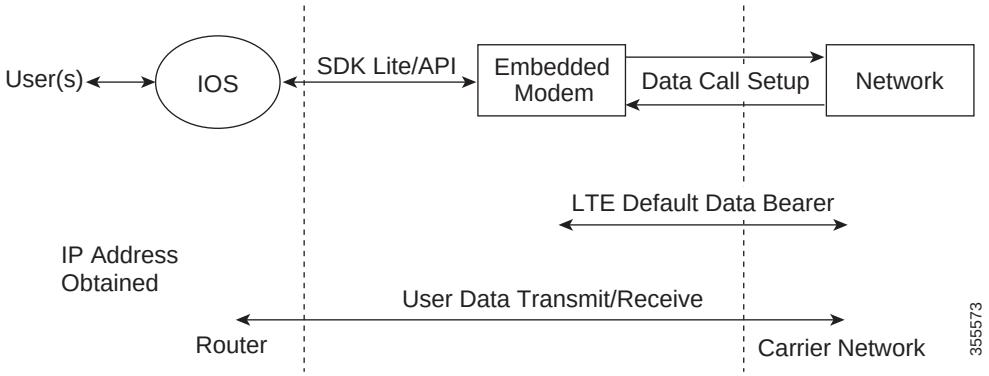
データ コール セットアップ

データ コールを設定するには、次の手順を実行します。

- セルラー インターフェイスの設定（103 ページ）
- DDR の設定（104 ページ）
- DDR バックアップの設定（104 ページ）

図 2 は一般的なデータ コール設定を示しています。

図 2　WIM-LTE でのデータ コールの設定



セルラー インターフェイスの設定

次の例で、セルラー インターフェイスを設定する方法を示します。

```
Router# configure terminal
Router(config)# interface cellular 0
Router(config-if)# ip address negotiated
Router(config-if)# encapsulation slip
Router(config-if)# dialer in-band
Router(config-if)# dialer string lte
Router(config-if)# dialer-group 1
Router(config-if)# exit
Router(config)# chat-script lte"" "AT!CALL" TIMEOUT 60 "OK"
```

```
Router(config)# ip route 209.165.200.225 255.255.255.224 cellular 0
Router(config)# dialer-list 1 protocol ip list 1
Router(config)# line 3
Router(config-line)# script dialer lte
```

DDR の設定

次の例で、DDR を設定する方法を示します。

```
Router# configure terminal
Router(config)# interface cellular 0
Router(config-if)# ip address negotiated
Router(config-if)# encapsulation slip
Router(config-if)# dialer in-band
Router(config-if)# dialer pool-member 1
Router(config-if)# interface dialer 1
Router(config-if)# ip address negotiated
Router(config-if)# encapsulation slip
Router(config-if)# dialer pool 1
Router(config-if)# dialer idle-timeout 30
Router(config-if)# dialer string lte
Router(config-if)# dialer-group 1
Router(config-if)# exit
Router(config)# dialer-list 1 protocol ip list 1
Router(config)# access-list 1 permit any
Router(config)# line 3
Router(config-line)# script dialer lte
Router(config-line)# exit
Router(config)# chat-script lte"" "AT!CALL" TIMEOUT 60 "OK"
```

DDR バックアップの設定

プライマリ接続をモニタし、必要なときにバックアップ接続を開始するには、ルータで次の方式の 1 つを使用できます。

- 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。
- 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。
- 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。

バックアップ インターフェイスを使用するインターフェイスの設定

(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。

次の例で、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設定する方法を示します。

```
Router# configure terminal
Router(config)# interface atm 0
Router(config-if)# backup interface cellular 0
Router(config-if)# backup delay 0 10
```

AutoSIM とファームウェア ベースのスイッチング

AutoSIM 機能の利点は次のとおりです。

- キャリア固有の SKU のため発注が容易
- デュアル SIM の使用によるフェールオーバー時間の短縮
- 他のサービス プロバイダーから Telstra ネットワークへのスイッチオーバーが容易

AutoSIM モードのモデムは、SIM スロットスイッチと自動モデムのリセット後に、適切なキャリア ファームウェアを選択します。AutoSIM は、WP7607、WP7608、および WP7609 モデムでサポートされています。ブートアップの際、モデムの AutoSIM 設定が IOS 設定と一致しない場合には、対応する AutoSIM または手動モードがモデムにプッシュされます。

AutoSIM 設定が変更されると、モデムは自動的にリセットされます。デフォルトでは 'auto-sim' が有効になっています。

次の例で、AutoSIM を有効にする方法を示します。

```
router(config)#controller cellular <slot>
router(config-controller)#lte firmware auto-sim
```

(注) auto-sim を有効にした後、無線が起動するまで 5 分間待機します。無線が起動したら、モデムの電源を再投入し、無線が再び起動するまで 3 分間待機します。auto-sim 設定を有効にするには、モデムの電源の再投入が必要です。

次の例で、AutoSIM を無効にする方法を示します。

```
router(config)#controller cellular <slot>
router(config-controller)# no lte firmware auto-sim
```

4G SMS メッセージングの設定

次の例で、すべての入出力 SMS メッセージを送信する FTP サーバのフォルダ パスを指定する方法を示します。フォルダ パスが認識されると、SMS メッセージが送受信されるフォルダの末尾に outbox および inbox が自動的に付加されます。

```
Router# configure terminal
Router(config)# controller cellular 0
Router(config-controller)# lte sms archive path
ftp://username:password@172.25.211.175/SMS-LTE
Router# end
```

次の例で、モデムに受信された受信テキストの内容を表示する方法を示します。

```
Router# cellular 0 lte sms view summary

ID FROM YY/MM/DD HR:MN:SC SIZE CONTENT
0 4442235525 12/05/29 10:50:13 137 Your entry last month has...
2 5553337777 13/08/01 10:24:56 5 First
3 5553337777 13/08/01 10:25:02 6 Second
```

次の例で、送受信されたテキスト メッセージのすべての情報を表示する方法を示します。メッセージ情報には、送信済み、受信、アーカイブ、送信保留テキスト メッセージが含まれます。試行が FAILED となった場合、LTE 固有のエラー情報が表示される場合もあります。

```
Router# show cellular 0 sms
Incoming Message Information
----------------------------
SMS stored in modem = 20
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 20
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0

Outgoing Message Information
----------------------------
Total SMS sent successfully = 0
Total SMS send failure = 0
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status = 0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
Reference Number = 0
Result Code = 0x0
Diag Code = 0x0 0x0 0x0 0x0 0x0

SMS Archive URL = ftp://lab:lab@1.3.150.1/outbox
```

次の例で、ユーザにテキスト メッセージ プランがある場合、他の有効な受信者への 4G LTE バンド SMS メッセージ送信を有効にする方法を示します。

```
Router# cellular 0 lte sms send 15554443333 <sms text>
```

モデムのファームウェアのアップグレード

モデムのファームウェアをアップグレードするには、次の手順を実行します。

ステップ 1 シスコのソフトウェア ダウンロード Web サイト（https://software.cisco.com/download/home）に移動します。

ステップ 2 ダウンロード ページで、**[900 series integrated services router]** を検索し、フィルタ処理されたリストから **[900 integrated services router]** を選択します。

ステップ 3 **[Routers] > [900 Series Integrated Routers] > [900 Integrated Services Router]** を選択します。

ステップ 4 左側のペインからリリースを選択します。使用可能なファームウェアが右側のペインに表示されます。

ステップ 5 適切なファームウェアを選択してダウンロードします。

ステップ 6 モデム ファームウェアを保存するためのディレクトリをルータ フラッシュに作成します。

ステップ 7 ファームウェアをフラッシュ ディレクトリにコピーします。

ステップ 8 次のコマンドを使用して、アップグレード プロセスを開始します。

```
Router# microcode reload cellular 0 lte modem-provision flash:firmware directory
```

ステップ 9 アップグレードを検証します。

```
Router# show cellular 0 hardware

Modem Firmware Version = SWI9X07Y_02.18.05.00 000
Modem Firmware built = 2018/07/19 17:40:21
Device Model ID: WP7608
International Mobile Subscriber Identity (IMSI) = 123456000009205
International Mobile Equipment Identity (IMEI) = 354365090106005
Integrated Circuit Card ID (ICCID) = 8952530076180099205
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Factory Serial Number (FSN) = XG814285250410
Modem Status = Online
Current Modem Temperature = 42 deg C
PRI SKU ID = 1103787, PRI version = 002.041_002, Carrier = Generic
OEM PRI version = 001.004
```

モデム DM ログ収集の設定

Diagnostic Monitor（DM）は、Qualcomm の独自プロトコルです。Sierra Wireless SwiLog や Qualcomm QXDM などの診断ソフトウェア ツールは、DM プロトコルに基づいています。これらのツールは、RF インターフェイスによるモデムとネットワーク間のデータ トランザクションのキャプチャに使用できるため、3G および 4G データ接続やパフォーマンスに関する問題のトラブルシューティングに役立ちます。

次の例で、DM ログ収集を有効にする方法を示します。

```
Router(config-controller)# lte modem dm-log enable
```

次の例で、ログ ファイルの最大サイズを指定する方法を示します。

```
Router(config-controller)# lte modem dm-log filesize 8
```

次の例で、フィルタ ファイルを指定する方法を示します。

```
Router(config-controller)# lte modem dm-log filter flash:SwiLogPlus_generic_filter_6.3.sqf
```

次の例で、DM ログ出力ファイルが保存されるパスを指定する方法を示します。

```
Router(config-controller)# lte modem dm-log output path ftp://@172.25.211.175/
```

次の例で、DM ログ ローテーションを有効にする方法を示します。

```
Router(config-controller)# lte modem dm-log rotation
```

次の例で、ログの最大サイズを指定する方法を示します。

```
Router(config-controller)# lte modem dm-log size 128
```

出力例については、次を参照してください。例：cellular logs modem-crashdump コマンドの出力例（117 ページ）

モデムの crashdump 収集の有効化

モデムの crashdump の収集は、ファームウェア クラッシュのデバッグに役立ちます。クラッシュ データを収集するには、クラッシュ後に memdump モードのままになるようにモデムを事前設定する必要があります。memdump モードは、クラッシュ データを収集する memdump ユーティリティの特殊なブート アンド ホールド モードです。

モデムの crashdump の収集を有効にするには、次の手順を実行します。

前提条件

crashdump ロギングの有効化を試みる前に、次の前提条件が満たされていることを確認してください。

- モデムは、モデムの crashdump の収集用にプロビジョニングする必要があります。テスト モードで動作するように設定する必要があります。デバッグ ブートローダもインストールする必要があります。詳細については、Cisco TAC にお問い合わせください。
- モデムはクラッシュ状態である必要があります。モデムのファームウェア クラッシュを発生させるテストを実行します。ルータのコンソールまたは syslog の "MODEM_DOWN" メッセージは、モデムのファームウェア クラッシュを示しています。

（注） モデムのファームウェアがクラッシュした後、そのモデムは crashdump ログの収集のみに使用できます。データ コールは実行できません。

次の例で、クラッシュ後に memdump モードを維持するようにモデムを事前設定する方法を示します。

```
Router# configure terminal
Router(config)# controller cellular 0
Router(config-controller)#lte modem crash-action boot-and-hold
Router(config-controller)#end
```

次の例で、crashdump ログの収集を有効にする方法を示します。

```
Router# configure terminal
Router(config)# service internal
Router(config)# end
Router(config)# test cell-host 0 modem-crashdump off
```

次の例で、FTP サーバに保存されているログを使用した crashdump ログの収集を有効にする方法を示します。

```
Router# configure terminal
Router(config)# service internal
Router(config)# end
Router(config)# test cell-host 0 modem-crashdump on ftp://@172.25.211.175/
```

モデム ログ エラーとダンプ情報の表示

ログ エラーとダンプ情報を取得するには、次のコマンドを使用します。

- **show cellular** *unit* **log error**

	コマンドまたはアクション	目的
ステップ 1	**show cellular** *unit* **log error** 例: Router# show cellular 0 log error	モデムのログ エラーとダンプ情報を表示します。 出力例については、次を参照してください。 例:show cellular log error コマンドの出力例(118 ページ)

4G LTE の設定例

例:基本セルラー インターフェイスの設定

次の例で、プライマリとして使用されるようにセルラー インターフェイスを設定し、デフォルト ルートとして設定する方法を示します。

```
Router# show running-config
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"

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

ip route 172.22.1.10 255.255.255.255 cellular 0

dialer-list 1 protocol ip permit

line 3
script dialer lte
modem InOut
```

常時接続のセルラー インターフェイスの設定

ここでは、次の設定例について説明します。

- 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（110 ページ）
- 外部ダイヤラ インターフェイスを使用する dialer-persistent の設定（110 ページ）

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

次の例で、外部ダイヤラ インターフェイスを使用せずに dialer-watch を設定する方法を示します。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!CALL" 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

次の例で、外部ダイヤラ インターフェイスを使用して dialer-persistent を設定する方法を示します。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。

```
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"

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
```

NAT および IPsec を使用したバックアップとしての 4G LTE ワイヤレス WAN

次の例で、NAT および IPSec を使用して、ルータで 4G-LTE ワイヤレス WAN をバックアップとして設定する方法を示します。

(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。

```
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lan-pool
   network 10.4.0.0 255.255.0.0
   dns-server 10.4.0.254
   default-router 10.4.0.254
!
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"

crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key  address a.b.c.d
!
!
crypto ipsec transform-set  ah-sha-hmac esp-3des
!
crypto map gsm1 10 ipsec-isakmp
 set peer a.b.c.d
 set transform-set
 match address 103
!
!
interface ATM0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0.1 point-to-point
 backup interface Cellular0
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
```

```
!
interface Cellular0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
 encapsulation slip
 no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
 dialer string lte
 dialer-group 1
 async mode interactive
 crypto map gsm1
!

interface Vlan104
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
interface Dialer2
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@dsl.com
 ppp chap password 0 cisco
 ppp ipcp dns request
 crypto map gsm1
!
ip local policy route-map track-primary-if
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
ip sla 1
 icmp-echo 2.2.2.2 source-interface Dialer2
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 101 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 2.2.2.2
access-list 103 permit ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2
!
route-map nat2dsl permit 10
 match ip address 101
```

```
 match interface Dialer2
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
line 3
 exec-timeout 0 0
 script dialer lte
 login
 modem InOut
```

(注) プライベート IP アドレスを使用するサービス プロバイダーに対して、**crypto ipsec transform-set esp** コマンド(つまり、esp-aes esp-sha256-hmac…)を使用します。

SIM の設定:例

SIM カードのロック:例

次の例で、SIM をロックする方法を示します。この設定例内で斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。

```
Router# show cellular 0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in unlocked state.
!
Router# cellular 0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in locked state.
!
```

SIM カードのロック解除:例

次の例で、SIM のロックを解除する方法を示します。この設定例内で斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。

```
Router# show cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in locked state.
!

Router# cellular 0 lte sim unlock 1111
!!!WARNING: SIM will be unlocked with pin=1111(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in unlocked state.
!
```

自動 SIM 認証:例

次の例で、自動 SIM 認証を設定する方法を示します。この設定例内で斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。

```
Router# show cellular 0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in unlocked state.
!
Router# cellular 0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:22:34.555: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:23:06.495: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#
!
```

```
!   SIM is in locked state. SIM needs to be in locked state for SIM authentication to
!   work.
!
Router#
Router# conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller cellular 0
Router(config-controller)# lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
Router(config-controller)# end
Router#
Apr 26 21:23:50.571: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is now in locked state but it can be used for connectivity since authentication is
!   good. Authentication can be saved in the router configuration so that when you boot up
!   the router with the same locked SIM, connection can be established with the correct
!   Cisco IOS configuration.
!
```

PIN コードの変更:例

次の例で、割り当てられた PIN コードを変更する方法を示します。この設定例内で斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。

```
Router# show cellular 0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in unlocked state.
!
Router#
Router# cellular 0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:58:11.903: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:58:43.775: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM is in locked state. SIM needs to be in locked state to change its PIN.
!
Router#
Router# cellular 0 lte sim change-pin 1111 0000
!!!WARNING: SIM PIN will be changed from:1111(4) to:0000(4)
```

```
Call will be disconnected. If old PIN is entered incorrectly in 3 attempt(s), SIM will be
blocked!!!
Are you sure you want to proceed?[confirm]
Resetting modem, please wait...

CHV1 code change has been completed. Please enter the new PIN in controller configuration
for verfication
Router#
Apr 26 21:59:16.735: %CELLWAN-2-MODEM_DOWN: Modem in HWIC slot 0/0 is DOWN
Apr 26 21:59:48.387: %CELLWAN-2-MODEM_UP: Modem in HWIC slot 0/0 is now UP
Router#
Router#
Router# sh cellular 0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#
!
!   SIM stays in locked state, as expected, but with new PIN.
!
Router# cellular 0 lte sim unlock 0000
!!!WARNING: SIM will be unlocked with pin=0000(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# show cellular 0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#
!
!   Unlock with new PIN is successful. Hence, changing PIN was successful.
!
```

暗号化された PIN の設定:例

次の例で、暗号化された PIN を使用して自動 SIM 認証を設定する方法を示します。この設定例内で斜体で記載されたテキストはコメントを示すために使用されており、通常のコンソール出力を表示した場合には表示されません。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do sh run | i SIM
username SIM privilege 0 password 7 055A575E70.
!
!   Copy the encrypted level 7 PIN. Use this scrambled PIN in the SIM authentication
!   command.
!
Router(config)#
Router(config)# controller cellular 0
Router(config-controller)# lte sim authenticate 7 055A575E70
CHV1 configured and sent to modem for verification
Router(config-controller)# exit
Router(config)# no username SIM
Router(config)# end
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console
```

4G 有用性強化の設定例

ここでは、次の内容について説明します。

例：show cellular logs dm-log コマンドの出力例

次に、**show cellular logs dm-log** コマンドの出力例を示します。

```
Router# show cellular 0 logs dm-log
Integrated DM logging is on
output path = flash:
filter = MC74xx generic - GSM_GPRS_EDGE_WCDMA_LTE_EVDO.sqf
maximum log size = 67108864
maximum file size = 20971520
log rotation = disabled

33 packets sent to the modem, 4663 bytes, 0 errors
262 packets received from the modem, 374428 bytes, 0 input drops
262 packets stored in file system, 374428 bytes, 0 errors, 0 aborts
1 max rcv queue size

current file size = 374428
current log size = 374428
total log size = 374428
DM log files: (1 files)
flash:dmlog19560707-032507.bin size 374428
```

例：cellular logs modem-crashdump コマンドの出力例

次に、**show cellular logs modem-crashdump** コマンドの出力例を示します。

```
Router# show cellular 0 logs modem-crashdump
Modem crashdump logging: off
Progress = 100%
Last known State = Getting memory chunks
Total consecutive NAKs = 0
Number of retries = 0
Memory Region Info:
1: Full SDRAM [Base:0x0, Length:0x2000000]
2: MDSP RAM A region [Base:0x91000000, Length:0x8000]
3: MDSP RAM B region [Base:0x91200000, Length:0x8000]
4: MDSP RAM C region [Base:0x91400000, Length:0xC000]
5: MDSP Register region [Base:0x91C00000, Length:0x28]
6: ADSP RAM A region [Base:0x70000000, Length:0x10000]
7: ADSP RAM B region [Base:0x70200000, Length:0x10000]
8: ADSP RAM C region [Base:0x70400000, Length:0xC000]
9: ADSP RAM I region [Base:0x70800000, Length:0x18000]
10: CMM Script [Base:0x6A350, Length:0x310]
Router#
```

例：show cellular log error コマンドの出力例

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

```
Router# show cellular 0 log error
 Cached info is displayed

at!err

00   4E hsu_conf_sel_nv  00536
01   9B uim              08280
02   FF rrcllcpcie       15762
03   FF rrccspfscan      02169
04   4E dsatact          00696
05   4E dsatcmdp         01841
06   4D gsdi_convert     01526
07   04 rrccsputil       18579
08   02 cmss             03459
09   2D tmc              03825


OK

at!gcdump

No crash data available

OK
```

例：test cellular modem-error-clear コマンドの出力例

次に、**test cellular modem-error-clear** コマンドの出力例を示します。

```
Router# test cellular 0 modem-error-clear
Cellular0/1/0 Dump/Error info before clear command

at!err

00   4E hsu_conf_sel_nv  00536
01   9C uim              08280
02   FF rrcllcpcie       15762
03   FF rrccspfscan      02169
04   4E dsatact          00696
05   4E dsatcmdp         01841
06   4E gsdi_convert     01526
07   04 rrccsputil       18579
08   02 cmss             03459
09   2D tmc              03825

OK

at!gcdump

No crash data available

OK

Cellular0/1/0 Dump/Error registers cleared

Router#
```

PLMN の検索および選択

この機能を使用すると、利用可能なパブリック ランド モバイル ネットワーク（PLAMN）を検索し、その PLMN の 1 つに接続できます。

制約事項

次の制約事項が、PLMN の検索と選択に適用されます。

- LTE 2.0 および MC76XX モデム シリーズ以上でサポートされます。
- お使いのセルラー サービスが、ローミングをサポートしているかどうかを確認する必要があります。
- ローミングをサポートする SIM カードを使用している必要があります。
- この機能は 4G+WiFi プラットフォームではサポートされません。
- サポート対象のファームウェア バージョンは 02.18.05.00 以降です。

コマンド

PLMN 機能には、次のコマンドを使用します。

- **cellular <*unit*> lte plmn search**
- **cellular <*unit*> lte plmn select <*mode*> <*mcc*> <*mnc*> <*rat*> <*duration*>**
- **show cellular <*unit*> network**

ネットワークの検索

cellular 0 lte plmn search コマンドを使用して、使用可能な PLMN を検索できます。次の例で、ネットワークを検索する方法を示します。

```
router#cellular 0 lte plmn search
Searching for available PLMNs.This may take up to 3 minutes.
Please wait.........................
PLMN search done. Please use "show cellular 0 network" to see available PLMNS
```

検索後、**show cellular 0 network** コマンドを使用して使用可能なネットワークを参照します。

```
router#show cellular 0 network
Current System Time = Fri Sep 18 18:49:24 2015
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Manual
Network = O2 - UK
Mobile Country Code (MCC) = 234
Mobile Network Code (MNC) = 10
Packet switch domain(PS) state = Attached
Location Area Code (LAC) = 4931
Cell ID = 34319
Available PLMNs:
Idx MCC MNC RAT     Desc
1   234 10  umts    O2 - UK
2   234 10  gsm     O2 - UK
3   234 20  umts    3 UK
4   234 30  umts    EE
5   234 15  gsm     voda UK
```

```
6   234 33  gsm     EE
7   234 20  lte     3 UK
8   234 30  gsm     EE
9   234 15  umts    voda UK
10  234 30  lte     EE
11  234 10  lte     O2 - UK
12  234 15  lte     voda UK
```

ネットワークの選択

使用可能なネットワークの選択方法には、自動モード、強制モード、手動モードの 3 つのタイプがあります。自動モードでは、ルータは SIM の選択するネットワークに自動的に接続します。強制モードでは、ネットワークの検索をせずに、使用可能なネットワークか既知のネットワークを、ルータに強制的に選択させます。ネットワークが使用できないか、ルータがネットワークに接続できない場合は、ルータは「未接続」状態のままとなります。**cellular x lte plmn select auto** コマンドを使用して、SIM の選択するネットワークに接続できます。手動モードでは、検索結果から使用可能なネットワークを選択できます。

次の例で、手動でネットワークを検索する方法を示します。

```
router#cellular 0 lte plmn select manual ?
  <0-999>  Mobile Country Code (MCC)

router#cellular 0 lte plmn select manual 234 ?
  <0-999>  Mobile Network Code (MNC)

router#cellular 0 lte plmn select manual 234 10 ?
  gsm   GSM
  lte   LTE
  umts  UMTS

router#cellular 0 lte plmn select manual 234 10 gsm ?
  permanent    PERMANENT
  power-cycle  POWER_CYCLE

router#cellular 0 lte plmn select manual 234 10 gsm power-cycle ?

  <cr>

router#cellular 0 lte plmn select manual 234 10 gsm power-cycle
```

次の例で、ネットワーク選択を強制する方法を示します。

```
router#cellular 0 lte plmn select force ?
  <0-999>  Mobile Country Code (MCC)

router#cellular 0 lte plmn select force 310 ?
  <0-999>  Mobile Network Code (MNC)

router#cellular 0 lte plmn select force 310 410 ?
  <2-3>  MNC Digits Ex 23 means 2 Digits, 023 Means 3 Digits

router#cellular 0 lte plmn select force 310 410 2 ?
  gsm   GSM
  lte   LTE
  umts  UMTS

router#cellular 0 lte plmn select force 310 410 2 lte ?
  permanent    PERMANENT
  power-cycle  POWER_CYCLE
```

```
Router#cellular 0 lte plmn select force 310 410 2 lte power-cycle ?
  <cr>

Router#cellular 0 lte plmn select force 310 410 2 lte power-cycle
```

PLMN の選択の確認

show cellular 0 network コマンドを使用して、PLMN の選択を確認できます。

```
router#show cellular 0 network
Current System Time = Fri Sep 18 18:53:25 2015
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Manual
Network = O2 - UK
Mobile Country Code (MCC) = 234
Mobile Network Code (MNC) = 10
Packet switch domain(PS) state = Attached
Location Area Code (LAC) = 4931
Cell ID = 34319
Available PLMNs:
Idx MCC MNC RAT     Desc
1   234 10  umts    O2 - UK
2   234 10  gsm     O2 - UK
3   234 20  umts    3 UK
4   234 30  umts    EE
5   234 15  gsm     voda UK
6   234 33  gsm     EE
7   234 20  lte     3 UK
8   234 30  gsm     EE
9   234 15  umts    voda UK
10  234 30  lte     EE
11  234 10  lte     O2 - UK
12  234 15  lte     voda UK

router#show cellular 0 radio
Radio power mode = ON
Channel Number = 122
Current Band = GSM 900 Extended
Current RSSI = -48 dBm
Current ECIO = -127 dBm
Radio Access Technology(RAT) Preference = GSM
Radio Access Technology(RAT) Selected = EDGE
```

(注) ネットワークによっては、ルータの接続が許可されない場合があります。このような場合は、別のネットワークを選択する必要があります。

(注) ルータがネットワークに接続できない場合は、モデムを再起動します。

SNMP MIB

Cisco 4G LTE モジュールでは、次の簡易ネットワーク管理プロトコル（SNMP）MIB がサポートされています。

- IF-MIB
- ENTITY-MIB
- CISCO-WAN-3G-MIB

CISCO-WAN-3G-MIB では、次のテーブルとサブ テーブルが 3G および LTE テクノロジー向けにサポートされています。

- ciscoWan3gMIB(661)
- ciscoWan3gMIBNotifs(0)
- ciscoWan3gMIBObjects(1)
- c3gWanCommonTable(1)
- c3gWanGsm(3)
- c3gGsmIdentityTable(1)
- c3gGsmNetworkTable(2)
- c3gGsmPdpProfile(3)
- c3gGsmPdpProfileTable(1)
- c3gGsmPacketSessionTable(2)
- c3gGsmRadio(4)
- c3gGsmRadioTable(1)
- c3gGsmSecurity(5)
- c3gGsmSecurityTable(1)

http://www.cisco.com/go/mibs の Cisco MIB Locator から MIB をダウンロードできます。

SNMP 4G LTE の設定：例

次の例で、SNMP 機能をルータに設定する方法を示します。

```
snmp-server group neomobilityTeam v3 auth notify 3gView
snmp-server view 3gView ciscoWan3gMIB included
snmp-server community neomobility-test RW
snmp-server community public RW
snmp-server enable traps c3g
snmp-server host 172.19.153.53 neomobility  c3g
snmp-server host 172.19.152.77 public  c3g
snmp-server host 172.19.152.77 public udp-port 6059
```

次の例で、SNMP 経由でルータと通信するように外部ホスト デバイスを設定する方法を示します。

```
setenv SR_MGR_CONF_DIR /users/<userid>/mibtest
setenv SR_UTIL_COMMUNITY neomobility-test
setenv SR_UTIL_SNMP_VERSION -v2c
setenv SR_TRAP_TEST_PORT 6059
```

トラブルシューティング

このセクションでは、Cisco 4G-LTE ワイヤレス モジュールのトラブルシューティングに必要なバックグラウンド情報および使用可能なリソースについて説明します。

データ コール設定の確認

データ コール設定を確認するには、次の手順に従います。

ステップ 1 **cellular profile create** コマンドを使用してモデム データ プロファイルを作成し、セルラー インターフェイスで DDR を設定した後、ルータからワイヤレス ネットワーク経由でホストに ping を送信します。

ステップ 2 ping に失敗した場合、次の **debug** および **show** コマンドを使用してこの失敗をデバッグします。

- **debug chat**
- **debug modem**
- **debug dialer**
- **show cellular all**
- **show interface cellular**
- **show running-config**
- **show ip route**

ステップ 3 これらのコマンドの出力を保存し、システム管理者に問い合わせます。

信号強度の確認

Received Signal Strength Indication（RSSI）レベルが非常に低い場合（たとえば、-110 dBm 未満の場合）、次の手順に従います。

ステップ 1 アンテナ接続を確認します。SMA コネクタが適切に取り付けられ、しっかり締め付けられていることを確認します。

ステップ 2 リモート アンテナを使用している場合、アンテナ クレードルを移動して RSSI が改善されたかどうかを確認します。

ステップ 3 ワイヤレス サービス プロバイダーに問い合わせて、ユーザのいるエリアにサービス アベイラビリティがあるかどうかを確認します。

サービス アベイラビリティの確認

次に、アンテナが取り外され、モデム データ プロファイルが作成されていないシナリオでの **show cellular all** コマンド出力例を示します。ここでのエラーは、>>>>>>>> で強調表示されています。

```
Router# show cellular 0 all

Hardware Information
====================
Modem Firmware Version = SWI9600M_01.00.09.03
Modem Firmware built = 2011/07/01 19:31:09
Hardware Version = 20460000
International Mobile Subscriber Identity (IMSI) = <specific sim number>
International Mobile Equipment Identity (IMEI) = <specific modem number>
Electronic Serial Number (ESN) = <specific ESN in Hex> [specific ESN in Dec]
Integrated Circuit Card ID (ICCID) = <specific ICCID number>
Mobile Subscriber International Subscriber
IDentity Number (MSISDN) = <specific phone number>


Profile Information
====================
 * - Default profile >>>>>>>> no profile here.

Data Connection Information
===========================

Profile 1, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 2, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 3, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 4, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 5, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 6, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 7, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 8, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 9, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 10, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 11, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 12, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 13, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 14, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 15, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
Profile 16, Packet Session Status = INACTIVE
        Inactivity Reason = Normal inactivate state
```

```
Network Information
===================
Current Service Status = No service, Service Error = None    >>>>>>> no service means not
connected to the network.
Current Service = Packet Switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Country = , Network =
Mobile Country Code (MCC) = 0
Mobile Network Code (MNC) = 0


Radio Information
=================
Radio power mode = Online
Current RSSI = -125 dBm        >>>>>>> either no antenna, or bad antenna or out of
network.
Radio power mode = Online
LTE Technology Selected = LTE

Modem Security Information
==========================
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
```

正しいコール設定

次に、CHAT スクリプトを使用してコールが設定されている場合の出力例を示します。ネットワークから受信した IP アドレスが表示されます。コール設定が正常に行われ、データ パスが開いています。

```
debug modem
debug chat

Router#
Aug 25 18:46:59.604: CHAT0: Attempting async line dialer script
Aug 25 18:46:59.604: CHAT0: Dialing using Modem script: lte & System script: none
Aug 25 18:46:59.604: CHAT0: process started
Aug 25 18:46:59.604: CHAT0: Asserting DTR
Aug 25 18:46:59.604: CHAT0: Chat script lte started
Aug 25 18:46:59.604: CHAT0: Sending string: AT!CALL
Aug 25 18:46:59.604: CHAT0: Expecting string: OK
Aug 25 18:47:00.641: CHAT0: Completed match for expect: OK
Aug 25 18:47:00.641: CHAT0: Chat script lte finished, status = Success
Aug 25 18:47:00.641: TTY0: no timer type 1 to destroy
Aug 25 18:47:00.641: TTY0: no timer type 0 to destroy
Aug 25 18:47:00.641: TTY0: no timer type 2 to destroy
Aug 25 18:47:02.642: %LINK-3-UPDOWN: Interface Cellular0, changed state to up
Aug 25 18:47:02.642: %DIALER-6-BIND: Interface Ce0 bound to profile Di1
Aug 25 18:47:03.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed
state to up (69.78.96.14) [OK]
```

セキュア ストレージの設定

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

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

セキュア ストレージの有効化

次に、セキュア ストレージをイネーブルにする例を示します。

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

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

セキュア ストレージの無効化

次に、セキュア ストレージをディセーブルにする例を示します。

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

暗号化のステータスの確認

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

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

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

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

プラットフォーム ID の確認

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

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

```
router#show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
```

BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 MIIDhzCCAm+gAwIBAgIEAJT3DDANBgkqhkiG9w0BAQsFADAnMQ4wDAYDVQQKEwVD
aXNjbzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMB4XDTE1MTExNDA5MzMzN1oXDTI1
MTExNDA5MzMzN1owczEsMCoGA1UEBRMjUElEOldTLUMzNjUwLTEyWDQ4VVEgU046
RkRPMTk0NkJHMDUxDjAMBgNVBAoTBUNpc2NvMRgwFgYDVQQLEw9BQ1QtMiBMaXRl
IFNVREkxGTAXBgNVBAMTEFdTLUMzNjUwLTEyWDQ4VVEwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC6SARWyImWrRV/x7XQogAE+02WmzKki+4arMVBvl9o
GgvJfkoJDdaHOROSUkEE3qXtd8N3lfKy3TZ+jtHD85m2aGz6+IRx/e/lLsQzi6dl
WIB+N94pgecFBONPR9wJriox1IGD3B43b0hMLkmro4R5Zrs8XFkDo9k1tBU7F2O7
GEzb/WkO5NLexznef2Niglx9fCDL0HC27BbsR5+03p8jhG0+mvrp8M9du1HKiGin
ZIV4XgTMp1/k/TVaIepEGZuWM3hxdUZjkNGG1c1m+oB8vLX3UlSL76sDBBoiaprD
rjXBgBIozyFW8tTjh50jMDG84hKD5s31ifOe4KpqEcnVAgMBAAGjbzBtMA4GA1Ud
DwEB/wQEAwIF4DAMBgNVHRMBAf8EAjAAME0GA1UdEQRGMESgQgYJKwYBBAEJFQID
oDUTM0NoaXBJRD1VWUpOTlZJMENBUkhVM1Z1SUVSbFl5QXlPQ0F4TXpvek5Ub3lN
U0EwS0NnPTANBgkqhkiG9w0BAQsFAAOCAQEADjtM8vdlf+p1WKSKX1C1qQ4aEnD5
p8T5e4iTer7Y1fbCrHIEEm3mnip+568j299z0H8V7PDp1ljuLHyMFTC+945F9RfA
eAuVWVb5A9dnGL8MssBJe2lVSnZwrWkT1EIdxLYrTiPAQHtll6CN77S4u/f71oYE
tzPE5AGfyGw7ro1MEPVGffaQmYUDAwKFNBH1uI7c2S1qlwk4WWZ6xxci+lhaQnIG
pWzapaiAYL1XrcBz4KwFc1ZZpQT6hHw24jzYaYimvCo+/kSKuA9xNdtSu18ycox0
zKnXQ17s6aChMMt7Y8Nh4iz9BDejoOF6/b3sM0wRi+2/4j+6/GhcMRs0Og==
-----END CERTIFICTAE
Signature version: 1
Signature:
405C70D802B73947EDBF8D0D2C8180F10D4B3EF9694514219C579D2ED52F7D583E0F40813FC4E9F549B2EB1C21
725F7C
B1C79F98271E47E780E703E67472380FB52D4963E1D1FB9787B38E28B8E696570A180B7A2F131B1F174EA79F5D
B4765DF67386126D8
9E07EDF6C26E0A81272EA1437D03F2692937082756AE1F1BFAFBFACD6BE9CF9C84C961FACE9FA0FE64D85AE4FA
086969D0702C536ABD
B8FBFDC47C14C17D02FEBF4F7F5B24D2932FA876F56B4C07816270A0B4195C53D975C85AEAE3A74F2DBF293F52
423ECB7B853967080A
9C57DA3E4B08B2B2CA623B2CBAF7080A0AEB09B2E5B756970A3A27E0F1D17C8A243

プラットフォーム イメージの旧バージョンへのダウングレード

セキュア ストレージがサポートされていない旧バージョンにプラットフォーム イメージをダウングレードする場合は、サポートされているバージョンでこの機能を事前に無効にする必要があります。セキュア ストレージを無効にするには、次を参照してください。セキュア ストレージの無効化（127 ページ）

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

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

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