



## **3G 高速 WAN インターフェイス カード ソリューション 導入ガイド**

バージョン 1  
2010 年 5 月 6 日

**【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/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

3G 高速 WAN インターフェイス カード ソリューション 導入ガイド  
© 2010 Cisco Systems, Inc. All rights reserved.

## CONTENTS

### 概要 1-1

内容 1-1

概要 1-1

背景説明 1-2

Cisco 3G ワイヤレス WAN サービス 1-2

3G ワイヤレス ブロードバンド ネットワークのタイプ 1-2

パフォーマンス特性 1-3

スループット 1-4

遅延 1-4

共有アクセス 1-4

RSSI および搬送波対干渉波比 1-5

Quality of Service 1-5

### Cisco 3G GSM ベースの高速 WAN インターフェイス カード 2-1

内容 2-1

2.5/3G GSM ベースのブロードバンド データ ネットワーク アーキテクチャの概要 2-1

2.5/3G GSM データ コールの確立 2-2

ネットワーク接続のための GSM モデム プロファイルの作成と準備 2-4

サービス プラン 2-4

最良の無線ネットワークの選択 2-4

モデム プロファイルの作成 2-4

ネットワーク接続の準備 2-6

### Cisco 3G CDMA ベースの高速 WAN インターフェイス カード 3-1

内容 3-1

3G CDMA ブロードバンド データ ネットワーク アーキテクチャの概要 3-1

3G CDMA データ コールの確立 3-2

ネットワーク接続のための CDMA モデムのアクティブ化と準備 3-4

サービス プラン 3-5

最良の無線ネットワークの選択 3-5

モデムのアクティブ化 3-5

IOTA を使用したアクティブ化 3-6

OTASP を使用したアクティブ化 3-7

ネットワーク接続の準備 3-8

### 基本設定 4-1

内容 4-1

GSM ベースのワイヤレス ネットワーク 4-1

ネットワーク / ポート アドレス変換 (PAT) を使用した導入	4-1
デバッグおよびトラブルシューティング	4-5
CDMA ベースのワイヤレス ネットワーク	4-15
ネットワーク / ポート アドレス変換 (PAT) を使用した導入	4-15
デバッグおよびトラブルシューティング	4-19

## 高度なネットワーク導入シナリオ 5-1

内容	5-1
NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入	5-2
ブランチ オフィス ルータの設定	5-2
本社サイトのルータの設定	5-8
GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入	5-11
ブランチ オフィス ルータの設定	5-12
本社サイトのルータの設定	5-18
GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入	5-21
ブランチ オフィス ルータの設定	5-22
本社サイトのルータの設定	5-28
IPSec および OSPF を使用した DMVPN の導入	5-32
ブランチ 1 のオフィス ルータの設定	5-33
ブランチ 2 のオフィス ルータの設定	5-35
本社サイトのルータの設定	5-38
プライマリ リンクおよびバックアップ リンクを使用した EzVPN 導入	5-41
EzVPN クライアント (ブランチ ルータ) の設定	5-42
EzVPN サーバルータの設定	5-45
CCOA-Only モードでの NEMO Over 3G	5-47
ブランチ オフィスのモバイル ルータ (MR) の設定	5-47
本社のホーム エージェント (HA) のルータの設定	5-51

## 用語集 6-1



## はじめに

---

このマニュアルでは、3G ワイヤレス ネットワーク テクノロジーと Cisco 3G 高速 WAN インターフェイス カード (HWIC) オファリングについて簡単に説明します。特に、プロトコルおよびネットワーク接続の側面から、このテクノロジーと 3G ワイヤレス ネットワーク アーキテクチャに関する情報を提供します。この情報は、お客様の導入を成功させたり、導入期間または導入後に生じる可能性のある問題のトラブルシューティングを行ったりする際に、3G ワイヤレス特有の設定を理解するのに役立ちます。

また、セルラー インターフェイスがワイヤレス サービス プロバイダーのネットワークへの接続を正常に取得するために必要な、モデムのアクティブ化、プロファイルの作成、および他のセルラー固有の要件についての情報も含まれています。

さまざまについてタイプの一般的なネットワーク導入例を理解します。このテクノロジーに固有のさまざまな設定の詳細およびガイドラインについて説明します。

一般的に生じる問題の解決に役立つ、トラブルシューティングやデバッグの詳細情報についても説明されています。

## 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は、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

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





# CHAPTER 1

## 概要

---

この章では、Cisco 3G ワイヤレス WAN サービス、3G ワイヤレス ブロードバンド ネットワークのタイプ、および 3G 高速 WAN インターフェイス カードの他の特徴について説明します。

## 内容

「概要」(P.1-1)

「背景説明」(P.1-2)

## 概要

このマニュアルでは、3G 高速 WAN インターフェイス カード (HWIC) の導入、デバッグ、およびトラブルシューティングについて説明します。このカードは **Second Generation Integrated Services Routers (ISR G2)** で 3G ワイヤレス ネットワーキング機能を提供します。

このマニュアルは、システム インテグレータ、セールス エンジニア、カスタマー サポート エンジニア、およびネットワーク環境で 3G ワイヤレス サービスの設計および実装を担当するユーザによって使用されることが想定されています。このマニュアルは、3G 環境における経験が豊富なユーザと、データおよび音声ネットワーキングにおける経験が豊富なユーザのギャップを埋めるように作成されています。

HWIC ハードウェアに関する特定の情報については、<http://www.cisco.com/go/3g> を参照してください。

3G サービスの各要素を理解するには、ある程度の基本的な知識が必要です。実装するサービスの内容によっては、さらに高度な知識が必要になる場合があります。適切に実装するには、次の分野の知識が必要です。

- 有線インターフェイスの特性など、ネットワークに接続される 3G サービスの動作についての知識
- Cisco IOS ソフトウェア ベースのルータでのデータのプロビジョニング サービス

インストールでは、シスコのダイヤラ インターフェイスとトンネル インターフェイスの設定に関する技術が必要になる場合もあります。

## 背景説明

ここでは、3G ワイヤレス ブロードバンド ネットワークに対応した Cisco 3G ワイヤレス WAN サービスとさまざまな特性について説明します。

## Cisco 3G ワイヤレス WAN サービス

3G 高速 WAN インターフェイス カード、または HWIC-3G-CDMA および HWIC-3G-GSM を使用すると、高速モバイル ブロードバンドを基盤とした、新しい企業サービスや、小規模から中規模の企業 (SMB) サービスを行えるようになります。具体的には、次のようなサービスがあります。

- リモート ブランチのプライマリ/バックアップ WAN 接続：多くの企業および SMB は ISDN を代替テクノロジーに変えることを希望するため、ターゲット サービスはリモート ブランチのバックアップになります。ワイヤレス WAN は、銀行の現金自動支払機 (ATM) などの非リアルタイムで低速度から中速度のアプリケーション、または 9600 ビット/秒で動作するシリアル カプセル化されたテクノロジーに対応したプライマリ アクセスとしても機能できます。
- 高速で固定されていない導入：3G HWIC によって実現可能なワイヤレス WAN サービスは、ワークグループなどの固定されていない接続や、見本市および建築現場からの一時的な接続に対応する際に便利です。
- モバイル ディザスタ リカバリ ソリューション：このサービスは、稼働中のファシリティに大規模な停止が発生したときに重要になります。セルラー サービスは、異なるセントラル オフィス経由で代替パスを取得できるため、機能し続けることができます。

## 3G ワイヤレス ブロードバンド ネットワークのタイプ

3G ワイヤレス データのネットワークは、少なくとも 2 Mb/秒のアクセス速度 (必ずしも平均して持続されるスループットではありません) をサポートするブロードバンド ワイヤレス パブリック ネットワークとして定義されています。これらのネットワークは、符号分割多重接続 (CDMA) 無線アクセス テクノロジーに基づいており、これによって複数の同時アクセスが提供されます。これらのネットワークで使用可能なアクセス帯域幅は、同時アクティブユーザの間で共有されるため、使用可能なすべての帯域幅がこれらのユーザ間で共有されます。

これらのワイヤレス ブロードバンド ネットワークは、元来、主に回線交換音声用に設計された既存のセルラー ネットワークから発展してきました。IP ベースのネットワークと IP データ接続が発展していく中で、ブロードバンド サービスがこれらのネットワークに導入されました。元のネットワークは主に回線交換音声用に設計されているため、このネットワーク パスはブロードバンド IP データのサポートには適していません。オーバーレイ ネットワークは、この機能をサポートするために作成されました。

現在、セルラー ワイヤレス データ ネットワークには、次の 2 種類があります。

- GSM/UMTS：GSM/UMTS のアーキテクチャは、3GPP 標準組織によって定義されています。この標準セットには、GPRS、EDGE、HSPA および HSPA+ エア インターフェイスが含まれています。
- CDMA2000 テクノロジー：CDMA2000 テクノロジーのアーキテクチャは、3GPP2 標準組織によって定義されています。この標準セットには、1xRTT、EvDO-Rev0、および EvDO-RevA エア インターフェイスが含まれています。

このマニュアルでは、*GSM* という言葉は、3GPP 標準でカバーされている無線送信テクノロジーを示すために使用されます。*CDMA* という言葉は、3GPP2 標準でカバーされている無線送信テクノロジーを示すために使用されます。UMTS と CDMA2000 は両方とも CDMA 変調テクノロジーを使用しますが、CDMA より UMTS のほうがより広い帯域幅を使用するため、W-CDMA と呼ばれています。CDMA2000 は UMTS で使用される 5.0 MHz の帯域幅ではなく、1.25 MHz の帯域幅で動作します。

CDMA のブロードバンドワイヤレス ネットワークは Qualcomm CDMA-2000 テクノロジーに基づいています。このネットワーク アーキテクチャは既存の IETF プロトコルを最大限に活用するため、IETF 中心型です。GSM のブロードバンド アーキテクチャは既存のいずれかのプロトコルを使用するのではなく、独自のプロトコルの一部を使用するため、IETF 中心型ではありません。

## パフォーマンス特性

3G HWIC は HSDPA および EV-DO Rev A をサポートします。図 1-1 には、CDMA2000 テクノロジーと GSM/UMTS テクノロジーが示されています。

図 1-1 CMDA2000、GSM、および CDMA テクノロジーのパフォーマンス特性

<p><b>GSM</b> TDMA ベースの携帯電話 世界標準 速度：28 Kbps</p> <p><b>GPRS、EDGE (2.5G)</b> 複数のタイム スロットを使用した GSM 経路の пакет データ サービス ダウンリンク：384 Kbps アップリンク：180 Kbps</p> <p><b>UMTS/HSDPA (3G)</b> WCDMA ベースのデータ サービス。 ダウンリンク：3.6 Mbps アップリンク：384 Kbps</p> <p><b>HS PA (3G)</b> WCDMA ベースのデータ サービス。 ダウンリンク：3.6 Mbps アップリンク：2.1 Mbps</p> <p><b>HS PA + (3G)</b> WCDMA ベースのデータ サービス。 ダウンリンク：7.2 Mbps アップリンク：5.1 Mbps</p>	<p><b>CDMA</b> 北アメリカで導入されている cdmaOne が使用する IS-95 であり、 S America &amp; Asia の一部 速度：28 Kbps</p> <p><b>1 x RTT (2.5G)</b> シングル 1.25MHz チャンネルを 使用する пакет データ サービス。 ダウンリンク：307 Kbps アップリンク：153 Kbps</p> <p><b>EVDO Rev0 (3G)</b> データ専用無線チャンネル。 ダウンリンク：2.4 Mbps アップリンク：160 Kbps</p> <p><b>EVDO RevA (3G)</b> 改善されたアップリンクおよび QoS ダウンリンク：3.18 Mbps アップリンク：1.8 Mbps</p>
--	---

278748

## スループット

スループットはセル セクターごとと、搬送波周波数ごとに共有されます。表 1-1 には、EVDO Rev A、HSDPA、および HSPA のセクター ダウンリンクおよびアップリンクごとの合計論理スループットの値が示されています。

表 1-1 3G HWIC チップセットのセクターごとの合計論理スループット

テクノロジー/サービス	アップリンク (Mbps)	ダウンリンク (Mbps)
EVDO Rev A	1.8	3.1
HSDPA	3.84 (Kbps)	3.6
HSPA	5.1	7.2

実際のスループットは、当該時点でのネットワークの状態、Received Signal Strength Indicator (RSSI)、および ISP ネットワークのセルラー バックホール ファシリティによって異なります。

## 遅延

3G セルラー ネットワークの遅延は、有線ネットワークの場合より長くなります。これは、ネットワークの状態によって変化し、エアー リンクおよび Radio Access Network (RAN) では最大で 100 ミリ秒になることがあります。下の表には、テスト段階で確認されたエンドツーエンドのスループットと遅延が示されています。

表 1-2 テスト段階で確認されたエンドツーエンドの遅延とスループット

テクノロジー/サービス	アップリンク (Kbps)	ダウンリンク (Kbps)	1 方向遅延 (ms)
EDGE	80	140	250-300
UMTS	250	400	150-200
HSDPA	300	700	100-125
1xRTT	80	150	250
EVDO Rel 0	140	500	125
EVDO Rev A	500	800	75-100

## 共有アクセス

WiFi、イーサネット、DSL および 3G のセルラーは、すべて共有アクセス テクノロジーで表示されます。同じセルおよびセクターで無線リソースを使用している PC カード ユーザや他の 3G HWIC など、他のデータ サブスクリバによって、3G HWIC のパフォーマンスに影響が及ぼされる可能性があります。

## RSSI および搬送波対干渉波比

RSSI は、入力信号の強度を測定する回路です。この基本回路は、RF 信号を選択し、信号の強度に応じて出力を生成するように設計されています。レシーバが最も弱い信号を選択する機能を、レシーバ感度と呼びます。レシーバ感度が高くなるほど、パフォーマンスは高くなります。出力電圧に基づいて信号強度を測定する回線があります。信号強度が強い場合は出力電圧が高くなり、信号強度が弱い場合は出力電圧が低くなります。

セル内を移動しているモバイル ハンドセットは、変化し続ける信号強度を記録します。信号強度は、低速フェージング、高速フェージング、および搬送波対干渉波比 (C/I 比) の低下によって生じる他の信号からの干渉によって影響を受けます。C/I 比が高ければ、高品質の通信を行うことができます。大部分のリンクで電力制御を介した最適な電力レベルを使用することで、セルラー システムで高い C/I 比が実現されます。搬送波電力が高すぎると、過度の干渉波が作成され、他のトラフィックの C/I 比が低下し、無線サブシステムのトラフィック容量が下がります。搬送波電力が低すぎると、C/I は低くなり過ぎ、Quality of Service (QoS) の目標が満たされなくなります。理想的には、C/I 比は可能な限り高くする必要があり、受信するパイロット エネルギー (Ec) と合計受信エネルギーまたは合計パワースペクトル密度 (Io) 値の比率 (Ec/Io) は、可能な限り低くする必要があります。シスコでは許容値は決定していません。これらの値は、セルラーのキャリアによって決められています。Ec/Io 値が高く、Received Signal Strength Indicator (RSSI) 値が低い状況では、より最適な信号特性を得る方法を決定するためのサイト調査が必要です。

これらのパフォーマンス特性により、3G HWIC のスイートスポットは非リアルタイムで、サブ 512Kbps アプリケーションです。ネットワークが拡大して、遅延が減少し、QoS を使用できるようになると、VoIP などのリアルタイム アプリケーションを実行できるようになります。

## Quality of Service

現在、エアー リンクおよび Radio Access Network (RAN) QoS は実稼働セルラー ネットワークでは使用できません。このため、従来の IP QoS は ISR および 3G HWIC インターフェイス上で使用できませんが、エアー リンクへのマッピングは行われません。Cisco IOS QoS 機能を活用して、アプリケーション エクスペリエンスを向上させることができます。輻輳管理、輻輳回避、ポリシングおよびシェーピング、Modular QoS CLI (MQC) などは、すべて有用な技術です。詳細については、以下を参照してください。

[http://www.cisco.com/en/US/partner/docs/ios/isg/configuration/guide/isg\\_mqc\\_ipsession\\_ps6922\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/partner/docs/ios/isg/configuration/guide/isg_mqc_ipsession_ps6922_TSD_Products_Configuration_Guide_Chapter.html)

3G は共有アクセスを使用するため、**show interface** を発行して表示される帯域幅 (BW) の出力フィールドには、使用可能な論理帯域幅 (EV-DO Rev A の 1.8Mbps など) が反映され、実際の帯域幅は反映されません。瞬間的なダウンリンクのネットワーク速度は 2 Mbps、または 300Kbps になる可能性があります。





## CHAPTER 2

# Cisco 3G GSM ベースの高速 WAN インターフェイス カード

この章では 2.5/3G GSM ベースのブロードバンド データ ネットワークのアーキテクチャとデータ コールの確立について説明します。また、GSM モデム プロファイルの作成方法と、ネットワーク接続の準備方法についても説明します。

## 内容

[「2.5/3G GSM ベースのブロードバンド データ ネットワーク アーキテクチャの概要」\(P.2-1\)](#)

[「2.5/3G GSM データ コールの確立」\(P.2-2\)](#)

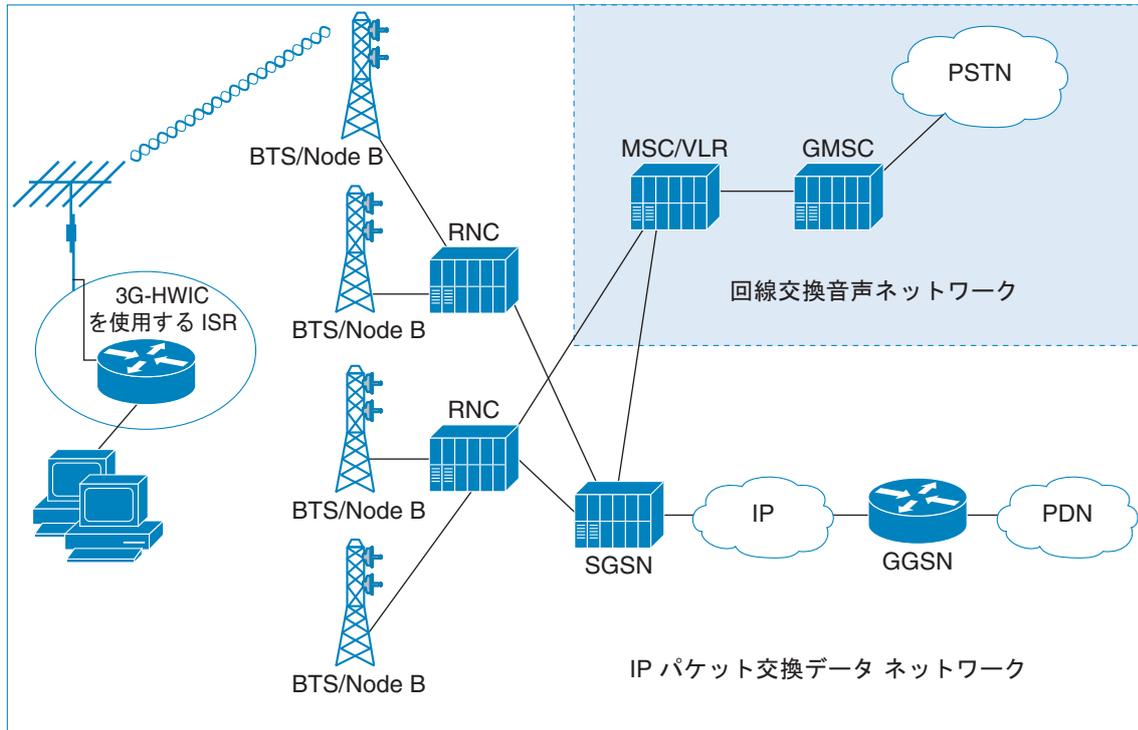
[「ネットワーク接続のための GSM モデム プロファイルの作成と準備」\(P.2-4\)](#)

## 2.5/3G GSM ベースのブロードバンド データ ネットワーク アーキテクチャの概要

[図 2-1](#) に示されている GSM ベースのネットワークは、セル タワーでベース ステーション トランシーバ システム (BTS) を使用します。これは UMTS では Node-B として知られています。3G-HWIC ベースの ISR は Node-B と無線で通信し、ネットワークを使用してデータ セッション (PDP コンテキストと呼ばれる) をセットアップする前に、自身をネットワークに接続します。Node-B は無線ネットワーク アクセス テクノロジーを終了します。Radio Network Controller (RNC) は、接続されている Node-B によってサービスが提供されているモバイル機器にモビリティ サービスを提供します。

ブロードバンド IP データ ネットワーク機能をサポートするために、SGSN および GGSN という 2 種類のネットワーク ノード タイプが導入されています。SGSN は、ビジター ロケーション レジスタ (VLR) 機能の代わりに、モビリティ機能を実行します。GGSN は、インターネットに対する IP パケットのゲートウェイとして機能します。ブロードバンド IP データ パケットのパスは、モバイル ノード (携帯電話) から、Node-B、RNC、GGSN、SGSN、およびインターネットに実行されます。従来の回線交換パスは MSC、GMSC、および PSTN を介して続行されます。ブロードバンド IP データ ネットワークは既存のセルラー ネットワーク経由でオーバーレイ ネットワークとして機能します。2.5G ネットワークは最初の GPRS ネットワークであり、[図 2-1](#) に示されているものと同じ物理トポロジを使用します。

図 2-1 GSM 3G IP ワイヤレス データ ネットワーク



278749

## 2.5/3G GSM データ コールの確立

図 2-2 には、GSM ネットワークでの 3G データ コールが示されています。PPP は 3G-HWIC で IOS とモデムの間で終了します。無線通信を経由した PPP は使用されません。代わりに、3GPP で定義されたプロトコルが、コールのセットアップに使用されます。3GPP で定義されたプロトコルは、一端のモデムと、もう一端の SGSN/GGSN で終了します。

最初のコールを設定する前に、サービス プロバイダーからデータ サービス アカウントを取得する必要があります。このサービスの一環として、プロバイダーから SIM カードが提供されます。SIM カードを 3G-HWIC に取り付ける必要があります。

- PPP CHAP ユーザ名 (ホスト名)
- PPP CHAP パスワード
- APN (アクセス ポイント ネーム)

例 2-1 に示されているように、モデムでプロファイルを作成できます。このプロファイルによって、モデムの NVRAM にこれらのパラメータが保存されます。これにより、モデムは PPP CHAP フェーズで IOS を認証できるようになるため、IOS は無線を介したワイヤレス ネットワークを使用して実際に行われる実際の認証を待たずに、次のフェーズ PPP IPCP を続けることができます。

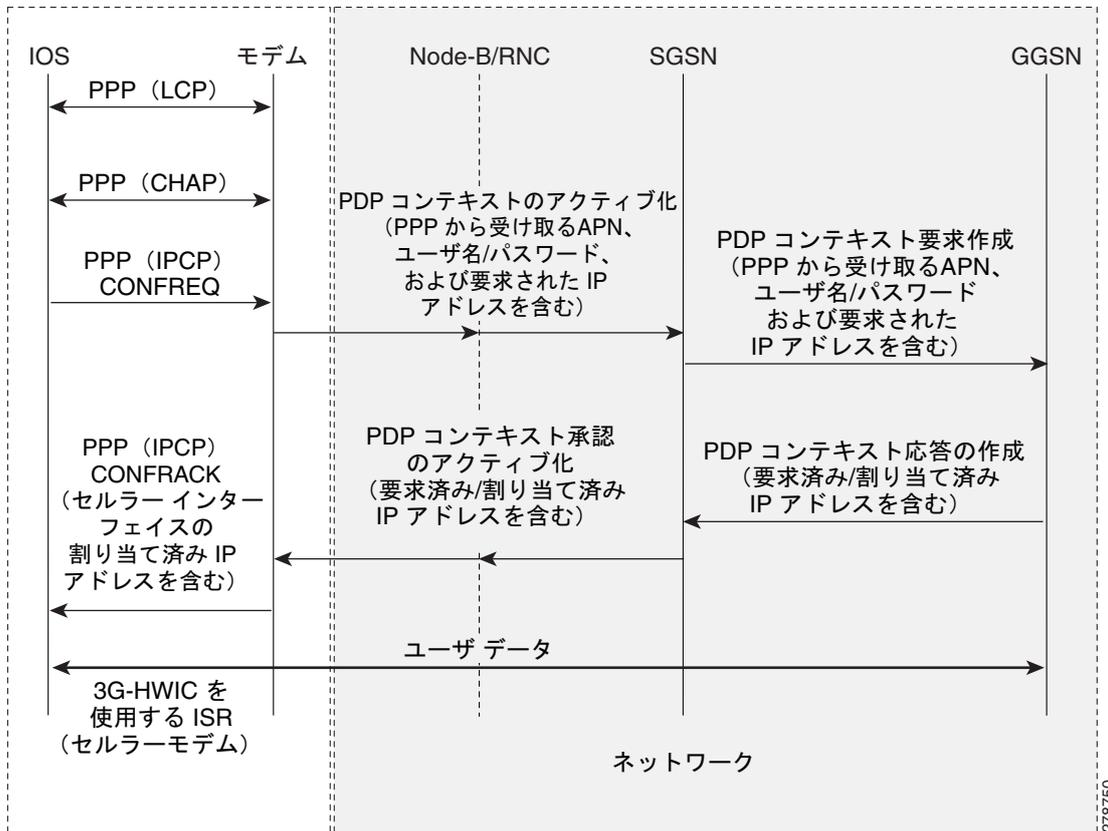
関連する ACL によって定義されているように、*interesting traffic* 基準を満たす最初の packets によってセルラー インターフェイスを介したダイヤル アウトが生じます。これにより、PPP LCP および PPP CHAP は IOS とモデムの間で完了します。モデムは PPP ユーザ名 (ホスト名) とパスワードを保存するため、CHAP はローカルで続行できるようになり、IPCP フェーズをすぐに開始できます。

PPP IPCP フェーズの一環として、IOS は CONFREQ メッセージを送信し、セルラー インターフェイスの IP アドレスを要求します（また、これらのアドレスに設定されている場合は、DNS アドレスが要求される場合もあります）。モデムが CONFREQ を受信すると、無線で「Activate PDP Context Request」メッセージが送信されます。このメッセージには、プロファイルの一部として作成され、NVRAM に保存されているユーザ名、パスワード、および APN が含まれています。このメッセージはセルラー メッセージの IP アドレスと DNS IP アドレス（該当する場合）を要求します。

SGSN は「Activate PDP Context Request」メッセージを受け取ると、「Create PDP Context Request」メッセージを送信し、これらのパラメータを適切な GGSN にリレーします。GGSN はユーザを検証し、セルラー インターフェイスに IP アドレスを割り当ててから、SGSN への「Create PDP Context Response」メッセージでこれを返します。この情報は、「Activate PDP Context Accept」メッセージとして、SGSN によってモデムにリレーされます。

最後に、モデムは保留中の IPCP 応答を IOS に返し（CONFACK）、IP アドレスや要求された他の情報（DNS アドレスなど）を返します。IP アドレスは、セルラー インターフェイスにバインドされ、ルーティング テーブルに取り込まれます。これで、ユーザデータの転送を開始できます。

図 2-2 GSM 3G データ コールの確立コールフロー



# ネットワーク接続のための GSM モデム プロファイルの作成と準備

新しくインストールされた 3G GSM ワイヤレス HWIC がワイヤレス ネットワークに接続するには、一連のステップを完了する必要があります。これらの手順について、以降のセクションで説明します。

## サービス プラン

3G HWIC をキャリア ネットワークでアクティブ化するには、それをサービス プランに関連付ける必要があります。モバイル オペレータに応じて、無制限、従量制、またはプール式など、複数のモバイルブロードバンド データ プランを使用できます。3G HWIC サービスを既存の企業ワイヤレス契約と組み合わせて、月ごとの継続費用 (MRC) を抑えることができます。

以下のリンクには、3G HWIC を保証しているモバイル オペレータがリストされており、記載されているこれらのキャリアの Web サイトへのリンクを使用して、サービスに関する追加情報を入手できます。

[http://www.cisco.com/en/US/products/hw/routers/networking\\_solutions\\_products\\_generic\\_content0900aecd80601f7e.html](http://www.cisco.com/en/US/products/hw/routers/networking_solutions_products_generic_content0900aecd80601f7e.html)

## 最良の無線ネットワークの選択

HSDPA を使用する場合、3G HWIC は使用可能な最良の無線ネットワークにダウンシフトし、2.5G テクノロジーにダウンします。これは、3G HWIC がオペレータ ネットワークで利用可能な最良のネットワークに接続しようとしていることを意味します。HSDPA を使用できない場合、3G HWIC は UMTS に対応するようにネゴシエーションし、それを使用できない場合は 2.5G テクノロジー EDGE、GPRS の順番でネゴシエーションします。

## モデム プロファイルの作成

セルラー ネットワークを使用してデータ接続を設定する前に、セルラー モデムで GSM データ接続プロファイルを作成します。このプロファイルによって、モデムを持つユーザとその認証パラメータのセット、およびセルラー ネットワークが定義されます。

GSM プロファイルを作成するには、`cellular <x/x> gsm profile create` コマンドを使用します。これは、PPP を使用するダイヤルアウトに使用され、3G セルラー モデムとセルラー データ ネットワークとのデータ接続 (PPP 接続/PDP コンテキスト) が確立されます。

## 例 2-1 モデム プロファイルの作成

```
ROUTER#cellular <x/x/x> gsm profile create <profile number> <APN - Access Point Name>
<chap | pap> <chap-or-pap-user-name> <chap-or-pap-password>
```

引数	説明
<profile number>	1 から 16 までの数字。最大 16 個のプロファイルを作成できますが、通常では 1 個のプロファイルで十分です。
<APN -Access Point Name>	ワイヤレス サービス プロバイダーによって提供される値  <chap   pap> : 使用するワイヤレス サービス プロバイダーによって PPP にサポートされている認証プロトコルに応じて、chap または pap キーワードを選択します。
<chap-or-pap-user-name>	ワイヤレス サービス プロバイダーによって提供される値
<chap-or-pap-password>	ワイヤレス サービス プロバイダーによって提供される値

cellular <x/x/x> gsm profile create コマンドの出力を次に示します。

```
ROUTER#cellular 0/0/0 gsm profile create 12 xyz.com chap userXyz passwordForXyz
Profile 12 will be created with the following values:
APN = xyz.com
Authenticaton = CHAP
Username = userXyz
Password = passwordForXyz
Are you sure? [confirm]
Profile 12 written to modem
ROUTER#

ROUTER#sh cellular 0/0/0 profile 12
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *18:09:14.944 UTC Tue Jun 26 2007

Profile 12 = INACTIVE
-----
PDP Type = IPv4
Access Point Name (APN) = xyz.com
Authentication = CHAP
Username: userXyz, Password: passwordForXyz

ROUTER#
```

## ネットワーク接続の準備

3G HWIC がアクティブ化された後、モバイル ネットワークに最初にダイヤルするときに、エンドツーエンドの無線および IP 接続の確立に 2 秒から 5 秒かかる場合があります。モデムがリダイヤルする必要がある場合は、5 秒より長くかかる場合があります。また、ネットワーク上でモデムが最初にアクティブ化されたときに、いくつかのプロビジョニングプロセスがバックグラウンドで開始され、これによって最初のエンドツーエンドの接続により長い時間を要する場合があります。

ネットワーク接続を準備するには、次の手順を実行します。

- ステップ 1** サービス プロバイダーから入手した SIM カードが 3G HWIC に正しく取り付けられていることを確認します。
- ステップ 2** HWIC にアンテナを接続します。
- ステップ 3** RSSI 信号レベルが、マイナス 90 dBm より高いことを確認します。
- ステップ 4** `show cellular x/x/x all` コマンドを実行して、ネットワークへの接続を確認します。  
`show cellular x/x/x all` コマンドからの出力を次に示します。

### 例 2-2 ネットワーク接続の確認

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

```
ROUTER#sh cell 0/0/0 all
!  
関連情報のみを表示し、その他は見やすくするため省略しています。  
!  
  
Profile Information  
=====
Profile 1 = INACTIVE*
-----
PDP Type = IPv4
Access Point Name (APN) = xyz.com
Authentication = CHAP
Username: userXyz, Password: passwordForXyz

* - Default profile
!  
作成したプロファイルに入力ミスや不注意によるスペースがなく、想定どおりであることを確認します。  
!  
  
Data Connection Information  
=====
Profile 12, Packet Session Status = INACTIVE
      Inactivity Reason = Unknown

Network Information  
=====
Current Service Status = Normal, Service Error = None
Current Service = Combined
Packet Service = UMTS/WCDMA (Attached)
Packet Session Status = Inactive
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Country = USA, Network = GSM
```

```
Mobile Country Code (MCC) = 310
Mobile Network Code (MNC) = 380
Location Area Code (LAC) = 56997
Routing Area Code (RAC) = 253
Cell ID = 5931
Primary Scrambling Code = 184
PLMN Selection = Automatic
Registered PLMN = GSM, Abbreviated =
Service Provider =
```

!

この例は、ネットワーク パケット サービス 'UMTS/WCDMA' が 'Attached' である様子を示しています。実際のサービスは、サービス プロバイダによって提供されるサービスによって多少異なる場合があります。

現在のサービス ステータスは、このように 'Normal' を示している必要があります

!

```
Radio Information
```

```
=====
```

```
Current Band = WCDMA 1900, Channel Number = 9721
```

```
Current RSSI (RSCP) = -87 dBm
```

!

データ サービスはより低いレベルで動作する場合がありますが、RSSI シグナル レベルは -90 dBm よりも高くする必要があります。

!

```
Modem Security Information
```

```
=====
```

```
Card Holder Verification (CHV1) = Disabled
```

```
SIM Status = OK
```

```
SIM User Operation Required = None
```

```
Number of Retries remaining = 3
```

!

SIM カードが正しく認識されています。

!

**ステップ 5** 第 5 章「高度なネットワーク導入シナリオ」で説明されているように、ルータを設定します。

**ステップ 6** 導入要件に応じて、適切なプロトコルを使用してネットワークに接続し、データ転送を確認してください。

詳細については、以下を参照してください。

<http://www.cisco.com/en/US/docs/routers/access/1800/1861/software/feature/guide/3ghwic.html>

■ ネットワーク接続のための GSM モデム プロファイルの作成と準備



## CHAPTER 3

# Cisco 3G CDMA ベースの高速 WAN インターフェイス カード

この章では、3G CDMA ブロードバンド データ ネットワーク アーキテクチャ、CDMA データ コールの確立方法、および CDMA モデムのアクティブ化とネットワーク接続について説明します。

## 内容

「3G CDMA ブロードバンド データ ネットワーク アーキテクチャの概要」(P.3-1)

「3G CDMA データ コールの確立」(P.3-2)

「ネットワーク接続のための CDMA モデムのアクティブ化と準備」(P.3-4)

「ネットワーク接続の準備」(P.3-8)

## 3G CDMA ブロードバンド データ ネットワーク アーキテクチャの概要

CDMA ベースのワイヤレス ブロードバンド データ ネットワークは IETF 中心型です。これは、IP データ接続/モビリティに使用されるプロトコルが、これらの標準、あるいは標準をわずかに変更したものに基いていることを意味します。

図 3-1 は、CDMA ネットワークのアーキテクチャを示しています。3G HWIC は BTS と無線で通信します。ネットワーク側の CDMA は BTS で終了します。

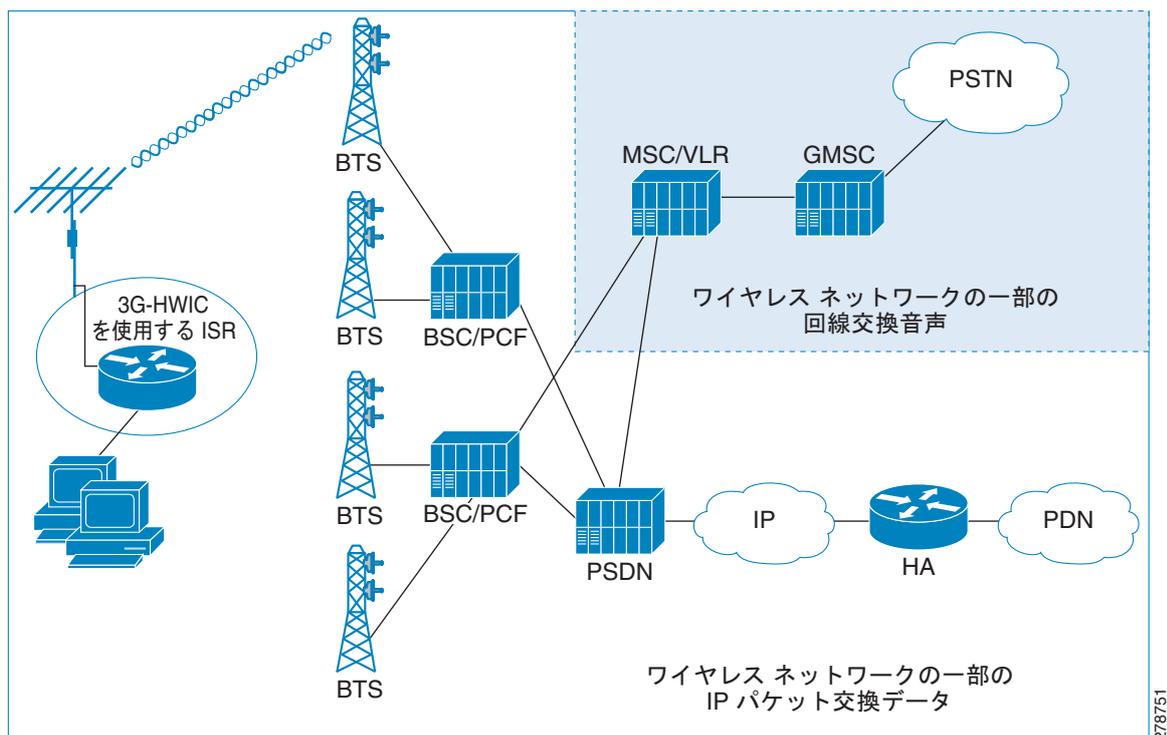
Base Station Controller/Packet Control Function (BSC/PCF) はビジター ロケーション レジスタ (VLR) およびホーム ロケーション レジスタ (HLR) と組み合わされており、モバイル機能を実行します。従来の BSC に追加された PCF の機能によって、3G 高速データをサポートするために必要な IP 機能が提供されます。レガシー BSC は高速データ サービスをサポートできません。これは、MSC を介した回線交換、非 IP の音声サービスのサポートを提供します。

PCF、パケット データ サービング ノード (PDSN)、および HA (ホーム エージェント) は、特に高速データ アクセス用のオーバーレイ ネットワークを提供します。

ISR ベースの 3G HWIC は PPP を一端では IOS/モデム内で終了し、ネットワーク側では PDSN で終了します。PDSN によって PPP が固定されるため、Simple IP (SIP) モードのアクセスを使用するときに、PPP を再確立しなくても、関連する BSC/PCF と、それに関連する BTS にわたって、モバイル ノードのモビリティが提供されます。

通常、Simple IP は使用されず、Mobile IP (MIP) が PDSN とともに使用されて Foreign Agent (FA) として機能します。ホーム エージェント (HA) は、サービス プロバイダー ネットワーク内に配置されます。この場合、HA はモバイル ノード (3G HWIC ベースの ISR) に IP アドレスを提供するアンカー ポイントとして機能します。HA によって提供されるアンカー ポイントを使用すると、モバイル端末の IP 接続を失うことなく、複数の PDSN にわたって (理論上は、ネットワーク全体にわたって) モビリティを拡張しながら、移動中に別の PDSN に接続することができます。

図 3-1 CDMA 3G IP ワイヤレス データ ネットワーク



## 3G CDMA データ コールの確立

図 3-2 は、CDMA ネットワークでのデータ コール フローを示しています。関連する ACL によって定義されているように、*interesting traffic* 基準を満たす最初のパケットによってセルラー インターフェイスを介したダイヤル アウトが生じます。これにより、PPP が IOS とモデムの間で開始します。Cisco IOS とモデムの間で LCP フェーズが完了した後、CHAP/PAP をバイパスして、IOS は PPP IPCP (CONFREQ) フェーズを開始します。CHAP/PAP は IOS に必要ないためバイパスされます。このため、セルラー インターフェイスでは設定されません。

LCP/IPCP メッセージが Cisco IOS から受信されると、モデムが開始し、ネットワークとの PPP 接続 (PDSN) が完了します。モデムは、モデムの NVRAM に保存されたパラメータを使用して PPP フェーズ中にネットワークによって認証されます。これらの認証パラメータは、モデムがアクティブ化/プロビジョニングされると、モデムの NVRAM にロードされます。モデムのアクティブ化/プロビジョニングは 1 回のみプロセスです。ネットワークを使用した IPCP フェーズの間に、モデムによって IP アドレスが要求されることはありません。PPP は、IP アドレスなしで確立され、モデム /IOS に割り当てられます。



(注) この時点で、PPP (IPCP) は IOS とモデム間でまだ保留中です。

PPP がモデムとネットワークの間で確立された後、モデムはモバイル IP フェーズを開始します。これにより、ネットワーク アドレス識別子 (NAI)、MN-AAA、MN-HA 共有秘密、HA IP アドレスを含む「Mobile IP Registration Request」メッセージが送信され、モデム/IOS (ホーム IP アドレス) の IP アドレスが要求されます。NAI、MN-AAA、MN-HA 共有秘密、および HA IP アドレスは、すべてモデムのアクティブ化またはプロビジョニングの一環としてモデムの NVRAM にロードされます。

「Mobile IP Registration Request」メッセージは PDSN によってインターセプトされ、HA IP アドレスによって示されているとおりに、該当する HA に転送されます。受信 HA は AAA を使用してユーザ NAI を検証し、「Registration Reply」メッセージを返します。これにより、ホーム IP アドレスである IP アドレスがユーザ モデムに割り当てられます。図 3-2 に示されているように、PDSN はこのメッセージを受け取ると、モデムに転送します。

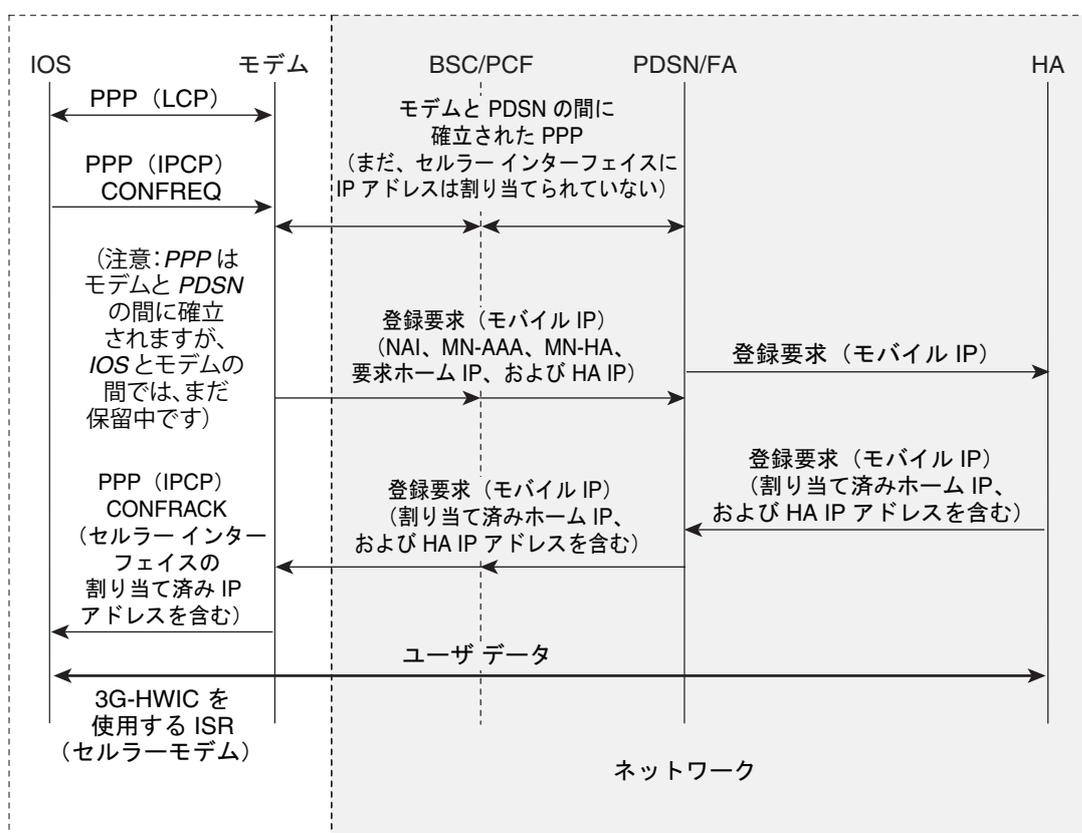
最後に、モデムは PPP IPCP (CONFACK) メッセージを IOS に送信し、IOS とモデム間の保留中の PPP 接続を完了します。モデムは HA からセルラー インターフェイスの IP アドレスを受け取るとその ID アドレスを返し、DNS などの他の IP アドレスが要求されている場合は、その IP アドレスを受け取るとそれを返します。

アドレスはセルラー インターフェイスに割り当てられ、ルーティング テーブルにルートが組み込まれます。



(注) IOS は、モデムおよび HA を経由するモバイル IP プロトコルを認識しません。

図 3-2 CDMA データ コールの確立コール フロー



278762

## ネットワーク接続のための CDMA モデムのアクティブ化と準備

新しくインストールされた 3G CDMA ワイヤレス HWIC がワイヤレス ネットワークに接続するには、一連の特定のステップを実行する必要があります。これらの手順を次に示します。詳細については、後続のセクションで説明します。

- ステップ 1** サービス プロバイダーからセルラー モデムのワイヤレス データ サービスおよび Equipment Serial Number (ESN) を取得します。
- ステップ 2** HWIC のセルラー モデムがワイヤレス サービス プロバイダーのネットワークに登録されていることを確認します。
- ステップ 3** サービス プロバイダーのサポート内容に応じて、インターネット地上波 (IOTA) または地上波サービスプロビジョニング (OTASP) を介して、サービス プロバイダーのネットワークでモデムをアクティブ化します。

3G HWIC は、サービス プロバイダーのネットワークで使用できる最適なネットワークに接続します。

## サービス プラン

3G HWIC をサービス プロバイダーのネットワークでアクティブ化するには、それをサービス プランに関連付ける必要があります。以下の URL には、3G HWIC を保証しているモバイル オペレータがリストされており、記載されているこれらのキャリアの Web サイトへのリンクを使用して、サービスに関する追加情報を入手できます。モバイル オペレータに応じて、無制限、従量制、またはプール式など、複数のモバイル ブロードバンド データ プランを使用できます。3G HWIC サービスを既存の企業ワイヤレス契約と組み合わせ、月ごとの継続費用 (MRC) を抑えることができます。

[http://www.cisco.com/en/US/products/hw/routers/networking\\_solutions\\_products\\_generic\\_content0900aecd80601f7e.html](http://www.cisco.com/en/US/products/hw/routers/networking_solutions_products_generic_content0900aecd80601f7e.html)

## 最良の無線ネットワークの選択

3G HWIC は、サービス プロバイダーのネットワークで使用できる最適なネットワークに接続しようとします。EVDO Rev A を使用できない場合、3G HWIC は次に使用可能な最良の無線ネットワークにダウンシフトし、2.5G テクノロジーにダウンします。たとえば、EVDO Rev A を使用できない場合、3G HWIC は EVDO Rev 0 に対応するようにネゴシエーションし、これを使用できない場合は、1xRTT を介して接続します。

## モデムのアクティブ化

3G CDMA HWIC のアクティブ化は、サービス プロバイダーによってサポートされているアクティブ化方法によって異なります。アクティベーション方法には次のタイプがあります。

- インターネット地上波 (IOTA)
- 地上波サービス プロビジョニング (OTASP)

サポートされているアクティベーション方法をサービス プロバイダーに確認してください。米国では、Sprint は IOTA をサポートし、Verizon Wireless は OTASP をサポートしています。

アクティブ化を行う前に、HWIC が無線接続レベルでネットワークと通信できることを確認します。モデムが通信できることを確認するには、**show cellular x/x/x** コマンドを発行します。

### 例 3-1 モデムのアクティベーションのサンプル出力

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
ROUTER#sh cellular 0/1/0 all
!  
! 見やすくするため、情報の一部を省略しています。
!  
Hardware Information
=====
Modem Firmware Version = p2005800
Modem Firmware built = 02-09-07
Hardware Version = 1.0
```

```

Electronic Serial Number (ESN) = 0x6032691E
Preferred Roaming List (PRL) Version = 60607
Current Modem Temperature = 35 degrees Celsius
!
!   PRL および ESN の情報が想定どおりであることを確認します。
!
Profile Information
=====
Electronic Serial Number (ESN) = 0x6032691E
Modem activated = NO

Network Information
=====
Current Service = 1xRTT only
Current Roaming Status(1xRTT) = HOME, (HDR) = HOME
Current Idle Digital Mode = CDMA
Current System Identifier (SID) = 4183
Current Network Identifier (NID) = 87
Current Call Setup Mode = Mobile IP only
Serving Base Station Longitude = -121 deg -55 min -8 sec
Serving Base Station Latitude = 37 deg 25 min 22 sec
Current System Time = Thu Jun 28 7:29:20 2007
!
!   サービスをアクティブにするには、HWIC が 1xRTT ネットワーク サービスを
!   取得する必要があります。この場合、1xRTT ネットワークのみを使用できます。
!
Radio Information
=====
1xRTT related info
-----
Current RSSI = -82 dBm, ECIO = -1 dBm
Current Channel Number = 50
Current Channel State = Acquired
Current Band Class = Band Class 1
!
!   1xRTT サービスは比較的正常的な RSSI (Received Signal Strength Indication)
!   レベルであるため、サービス アクティベーションを行えます。
!
HDR (1xEVDO) related info
-----
Current RSSI = -125 dBm, ECIO = -2 dBm
Current Channel Number = 25
Current Band Class = Band Class 1
Sector ID (Hex) = 0084:0AC0:0000:0000:000A:05DC:A801:1202
Subnet Mask = 104, Color Code = 32, PN Offset = 240
Rx gain control(Main) = Unavailable, Diversity = Unavailable
Tx total power = -5 dBm, Tx gain adjust = -256 dBm
Carrier-to-interference (C/I) ratio = 12
!
!   1xEvDO サービスは、この特定の事例では検知されません (この領域では使用不可)。
!   このサービスを使用できることが、HWIC のアクティベーション要件というわけではありません。
!

```

## IOTA を使用したアクティブ化

IOTA の手順を使用して HWIC をアクティブにするには、次のコマンドを使用します。

```
ROUTER# cellular <x/x/x> cdma activate manual <MDN> <MSIN> <SID> <NID> <MSL>
```



(注)

次にリストされている変数の値を取得するには、**sh cellular x/x/x all** コマンドを使用します。

- Mobile Directory Number (MDN) : 10 桁の数
- Mobile Subscriber Identification Number (MSIN) : 10 桁の数
- System ID (SID)
- Network ID (NID)
- Mobile Subsidy Lock (MSL)

### 例 3-2 IOTA の出力を使用したアクティブ化

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
ROUTER#cellular 0/1/0 cdma activate manual 9134397785 9132262534 4183 87 596027
```

```
Modem will be activated with following Parameters
MDN :9134397785; MSIN :9132262534; SID :4183; NID 87:
Aug 18 19:05:50.295: Checking Current Activation Status
Aug 18 19:05:50.347: Modem activation status: Activated
Aug 18 19:05:50.351: Mobile Parameters Unchanged
Aug 18 19:05:50.351: Skip Activation
2851-bl-cdma1#
Aug 18 19:06:00.403: Begin IOTA
Aug 18 19:06:00.403: Please wait till 'IOTA End' event notification is received
Aug 18 19:06:01.247: IOTA Status Message Received. Event = IOTA Start, Result = SUCCESS
Aug 18 19:06:31.567: OTASP State = SPL unlock, Result = Success
Aug 18 19:06:39.847: OTASP State = Parameters committed to NVRAM, Result = Success
Aug 18 19:06:52.015: IOTA Status Message Received. Event = IOTA End, Result = SUCCESS
!
!   モデムは IOTA サーバと通信し、
!   必要な情報をモデムにダウンロードします。
!
```

## OTASP を使用したアクティブ化

OTASP の手順を使用して HWIC をアクティブにするには、次のコマンドを使用します。

```
ROUTER#cellular <x/x/x> cdma activate otasp <phone number>
```



(注) **phone number** 変数には、サービス プロバイダーによって提供された電話番号を使用します。

### 例 3-3 OTASP の出力を使用したアクティブ化

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

ROUTER#cell 0/3/0 cdma activate otasp *22899
Beginning OTASP activation
OTASP number is *22899
ROUTER#Call Connecting - Call State - CnS Async Data Voice Call Packet 1xRtt Call , Number *22899
Jul 25 18:48:47.563: Begin IOTA
Jul 25 18:48:49.819: Call Connected. Call State - Voice Call OTA Call , Service Option - Loopback Enhanced Variable Rate Voice (8Kbps) SMS Rate 1 packet Data Service SMS Rate 2 Packet Data Service (14.4Kbps) Over The Air Parameter Administration - Rate 1 Over The Air Parameter Administration - Rate 2
Jul 25 18:48:58.091: OTASP State = SPL unlock, Result = Success
Jul 25 18:49:15.483: OTASP State = PRL downloaded, Result = Success
Jul 25 18:49:16.335: OTASP State = Profile downloaded, Result = Success
Jul 25 18:49:16.335: OTASP State = MDN downloaded, Result = Success
Jul 25 18:49:20.279: OTASP State = Parameters committed to NVRAM, Result = Success

```

## ネットワーク接続の準備

3G HWIC がアクティブ化された後、モバイル ネットワークに最初にダイヤルするときに、エンドツーエンドの無線および IP 接続の確立に 2 秒から 5 秒かかる場合があります。モデムがリダイヤルする必要がある場合は、5 秒より長くかかる場合があります。また、前のセクションで説明したように、ネットワーク上でモデムが最初にアクティブ化されたときに、いくつかのプロビジョニングプロセスがバックグラウンドで開始され、これによって最初のエンドツーエンドの接続により長い時間を要する場合があります。

HWIC がネットワーク導入要件に従ってアクティブ化されて設定された後、3G ワイヤレス ネットワーク経由の接続に ISR を使用できるようになります。アンテナを HWIC に接続し、RSSI 信号レベルがマイナス 90 dBm より良いことを確認します。show cellular x/x/x all コマンドの出力によって示されるネットワークへの接続が、「[Configuring the 3G Wireless High-Speed WAN Interface Card for Cisco 1841, and 2800 and 3800 Series Routers \(HWIC-3G-CDMA-x\)](#)」に表示されているものと同じであることを確認します。



# CHAPTER 4

## 基本設定

---

この章では、GSM と CDMA ベースのワイヤレス ネットワークの基本設定について説明します。

### 内容

「GSM ベースのワイヤレス ネットワーク」(P.4-1)

「CDMA ベースのワイヤレス ネットワーク」(P.4-15)

## GSM ベースのワイヤレス ネットワーク

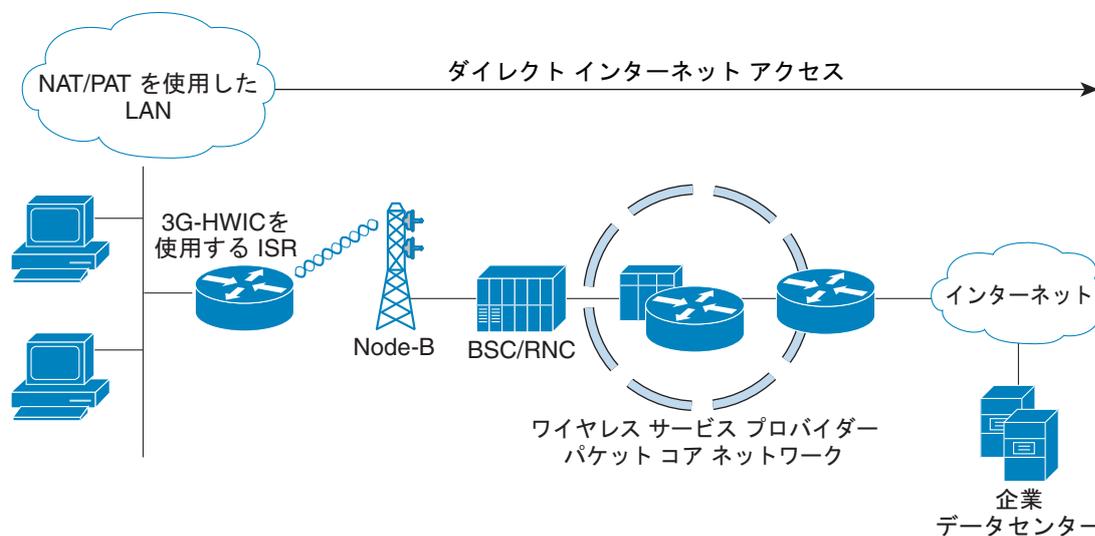
この章では、詳細な設定を使用して、非常に一般的な導入シナリオを説明し、各項目について説明します。

### ネットワーク/ポート アドレス変換 (PAT) を使用した導入

この単純な導入例では、[図 4-1](#) に示されている、ワイヤレス特有の設定に焦点を当てた NAT/PAT を使用します。NAT の詳細については、次を参照してください。

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product\\_data\\_sheet0900aec8064c999.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aec8064c999.html)。

図 4-1 GSM ワイヤレス ネットワーク用の NAT/PAT を使用した単純な導入



278753

## 例 4-1 NAT/PAT を使用した導入用の IOS 設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
hostname ROUTER
!
ip cef
!
ip dhcp excluded-address 10.1.0.254
!
ip dhcp pool gsm105
  network 10.1.0.0 255.255.0.0
  default-router 10.1.0.254
  dns-server 66.102.163.231 66.102.163.232
!
! ネットワーク 10.1.0.0/16、VLAN 101 で接続されているホスト、および
! ファスト イーサネット ポート 0/1/0 から 0/1/3 の DHCP プールを定義します。
!
ip domain name yourdomain.com
!
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
! ダイアログ 'gsm' を定義します。'atdt*98*1#' コマンドを使用すると、セルラー モデムは
! プロファイル 1 を使用してダイヤル アウトようになります (プロファイルは、'cellular x/x/x gsm
! profile create ...' コマンドを使用して作成されます)。応答で、IOS はダイヤル アウトの成功時にモデム
! から 'Connect' スtringを得ることを想定しています。この場合、IOS は応答がないか想定外の応答の
! 場合に、タイムアウトとして 30 秒待機します。モデムからの想定される 'Connect' 応答は
! 大文字と小文字が区別されます。
!
interface Loopback0
```

```

ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  switchport access vlan 101
!
interface FastEthernet0/1/1
  switchport access vlan 101
!
interface FastEthernet0/1/2
  switchport access vlan 101
!
interface FastEthernet0/1/3
  switchport access vlan 101
!
! 上記のファスト イーサネット ポートに接続されている DHCP クライアント ホスト。
!
interface Cellular0/0/0
  ip address negotiated
  ip nat outside
  no ip virtual-reassembly
  encapsulation ppp
  dialer in-band
  dialer idle-timeout 0
  dialer string cingular
  dialer-group 1
  async mode interactive
  ppp chap hostname SP-provided-user-name@sp-domain
  ppp chap password 0 SP-provided-password
  ppp ipcp dns request
!
! IP アドレスは、固定 (永続的) IP アドレスが必要な場合でも、ネゴシエートされた IP アドレス
! として常に設定することを強くお勧めします。セルラー インターフェイスは、
! PPP が確立されているかどうかに関係なく、'up'/'up' (ステータス / プロトコル ステート)
! としてスプーフィングされます。このインターフェイスが特定の IP アドレスによって設定されている場合に
! ('ip address negotiated' ではない)、PPP がまだ確立されていないと、
! ルーティング テーブルは、セルラー インターフェイスで使用できる有効なルートとしてそれを解釈します。
! ネゴシエートされた IP アドレスを割り当てることにより、この問題は回避されます。これは特に、
! セルラーをバックアップ インターフェイスとして使用する場合は重要です。

! ip nat outside は、セルラー インターフェイスを通過する IP パケットのソース IP アドレスとして
! セルラー インターフェイスに割り当てられ、VLAN 101 上のホストから取得された
! IP アドレスを使用します。

! dialer in-band は、ダイヤル オンデマンド ルーティングをサポートするようにインターフェイスを設定し、
! チャット スクリプトがダイヤル アウトされるように追加指定します。この場合、
! 前に定義されたように、チャット スクリプト 'gsm' を使用します。

! dialer idle-timeout を「0」に設定し、このコマンドで定義された特定の時間内にトラフィックがないことで
! PPP の切断が行われないようにしてください。'dialer
! idle-timeout 0' に設定すると、このタイマーのタイムアウト期間は無制限になります。

! dialer group と dialer-list は関連付けられたコマンドであり、
! PPP 接続がまだ確立されていない場合にそれをセットアップするためにセルラー モデム ダイアル アウトを
! トリガーする 'interesting' トラフィックを指定できます。

! ユーザ名 (ホスト名)、および PPP のパスワードは、

```

```

! サービス プロバイダ (SP) によって提供されます。ユーザ名とパスワードは、PPP に関する限り、
! IOS とセルラー モデム (3G HWIC に常駐) との間で、ローカルで
! 認証されます。PPP は IOS とモデムの間で終了します。これらの同じパラメータ
! (ユーザ名とパスワード) がセルラー モデムでも設定されている必要があります。
! このモデムは、セルラー ネットワークとの接続 (PDP コンテキストと呼ばれます) をセットアップするために、
! PDP コンテキストのアクティベーション メッセージを使用して、ネットワークを使用するユーザを認証
! するためにこれらのパラメータを無線で使用します。

! ppp ipcp dns-request オプション コマンドを使用すると、必要な場合は PPP の手順を使用して、
! セルラー ネットワークから DNS IP アドレスを取得できるようになります。
!
interface Vlan1
no ip address
!
interface Vlan101
ip address 10.1.0.254 255.255.0.0
ip nat inside
!
! インターフェイス VLAN 101 を定義します。この VLAN は、関連するホストで使用されます (ファスト
! イーサネット ポート)。これは、ip nat inside コマンドを使用して、NAT/PAT 機能を提供します。
!
ip virtual-reassembly
!
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0
!
! デフォルト ルートがセルラー インターフェイスを介するように定義します。この場合、すべての IP
! パケットは、セルラー インターフェイス経由でルーティングされます。
!
!
ip nat inside source list 2 interface Cellular0/0/0 overload
!
! NAT/PATed である必要があるトラフィックのソースがセルラー インターフェイスを介するように
! 指定します。この場合、'overload' パラメータを使用して PAT を実行しています。
! source list 2 は access-list 2 (以下で定義) に関連付けられています。
! これにより、(この場合は 10.1.0.0/16 ネットワークから) 対象のトラフィックの送信元が指定されます。
!
!
access-list 1 permit any
!
access-list 2 permit 10.1.0.0 0.0.0.255
!
dialer-list 1 protocol ip list 1
!
! dialer-list 1 コマンドは、セルラー インターフェイスの下に指定されている dialer-group 1
! コマンドに関連付けられています。
!
! access-list 1 コマンドは dialer-list 1 protocol ip list 1 コマンドに関連付けられています。
!
! これらのコマンドは、セルラー モデムを介したダイヤル アウトをトリガーする対象の
! トラフィックを指定し、確立されていない場合は PPP を確立します。
!
no cdp run
!
!
control-plane
!
line con 0
exec-timeout 0 0
exec prompt timestamp
stopbits 1
line aux 0
stopbits 1
line 0/0/0
exec-timeout 0 0

```

```
script dialer gsm
login
modem InOut
no exec
transport input all
transport output all
rxspeed 236800
txspeed 118000
!
!   セルラー インターフェイスの対応する行の下に、script dialer コマンドを指定する
!   必要があります。この場合セルラー インターフェイスは 0/0/0 であるため、
!   回線も基本的に 0/0/0 です。
!
!   rxspeed と txspeed を設定することはできません。
!
!   modem InOut を使用すると、ネットワークによって着信コールが現在サポートされていない場合でも、
!   着信および発信コールを実行できるようになります。
!
!   transport input all と transport output all は、セルラー モデムへの
!   リバース telnet 用に使用できます。
!
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet
!
scheduler allocate 20000 1000
!
end
```

## デバッグおよびトラブルシューティング

次のデバッグ方式は、一般的な問題をデバッグする場合に役立ちます。

- PPP
  - PPP 詳細イベント
  - PPP プロトコル ネゴシエーション
- チャット スクリプト
  - チャット スクリプトのアクティビティのデバッグ

応答が期待され、*interesting traffic* の一部である宛先 IP アドレスを Ping して、接続があるかどうかを確認できます。

## 例 4-2 通常の動作のデバッグ出力

この設定内で青色の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。太字のテキストは、エラーが発生した場合に参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次のデバッグ出力は、コール確立が成功した場合の典型的な例です。

```
ROUTER#ping ip 209.131.36.158 source 10.1.0.254
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.131.36.158, timeout is 2 seconds:
```

```
Packet sent with a source address of 10.1.0.254
```

```
*Jun 21 00:45:43.679: CHAT0/0/0: Attempting async line dialer script
*Jun 21 00:45:43.679: CHAT0/0/0: Dialing using Modem script: gsm & System script: none
*Jun 21 00:45:43.679: CHAT0/0/0: process started
*Jun 21 00:45:43.683: CHAT0/0/0: Asserting DTR
*Jun 21 00:45:43.683: CHAT0/0/0: Chat script gsm started
*Jun 21 00:45:43.683: CHAT0/0/0: Sending string: atdt*98*1#
*Jun 21 00:45:43.683: CHAT0/0/0: Expecting string: CONNECT
*Jun 21 00:45:43.727: CHAT0/0/0: Completed match for expect: CONNECT
*Jun 21 00:45:43.727: CHAT0/0/0: Chat script gsm finished, status = Success.
```

```
*Jun 21 00:45:45.931: %LINK-3-UPDOWN: Interface Cellular0/0/0, changed state to up
```

```
!
```

```
! 'interesting' トラフィックが検出されると、IOS は正常に
! セルラー モデムと通信し、ダイヤル アウトするようにコマンドを発行します。
!
```

```
*Jun 21 00:45:45.931: Ce0/0/0 PPP: Using dialer call direction
*Jun 21 00:45:45.931: Ce0/0/0 PPP: Treating connection as a callout
*Jun 21 00:45:45.931: Ce0/0/0 PPP: Session handle[3C00021F] Session id[180]
*Jun 21 00:45:45.931: Ce0/0/0 PPP: Phase is ESTABLISHING, Active Open
*Jun 21 00:45:45.931: Ce0/0/0 PPP: No remote authentication for call-out
```

```
!
```

```
! PPP の開始を準備する LCP (Link Control Protocol) フェーズ
!
```

```
*Jun 21 00:45:45.931: Ce0/0/0 LCP: O CONFREQ [Closed] id 189 len 20
*Jun 21 00:45:45.931: Ce0/0/0 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Jun 21 00:45:45.931: Ce0/0/0 LCP: MagicNumber 0x3F7E2331 (0x05063F7E2331)
*Jun 21 00:45:45.931: Ce0/0/0 LCP: PFC (0x0702)
*Jun 21 00:45:45.931: Ce0/0/0 LCP: ACFC (0x0802)
```

```
!
```

```
! Cisco IOS からセルラー モデムに送信される発信 CONFREQ.
!
```

```
*Jun 21 00:45:45.935: Ce0/0/0 LCP: I CONFREQ [REQsent] id 63 len 25
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACCM 0x00000000 (0x020600000000)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: AuthProto CHAP (0x0305C22305)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: MagicNumber 0xB9F4D928 (0x0506B9F4D928)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: PFC (0x0702)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACFC (0x0802)
```

```
!
```

```
! セルラー モデムから IOS によって受信される着信 CONFREQ.
!
```

```
*Jun 21 00:45:45.935: Ce0/0/0 LCP: O CONFACK [REQsent] id 63 len 25
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACCM 0x00000000 (0x020600000000)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: AuthProto CHAP (0x0305C22305)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: MagicNumber 0xB9F4D928 (0x0506B9F4D928)
```

```
*Jun 21 00:45:45.935: Ce0/0/0 LCP: PFC (0x0702)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACFC (0x0802)
!
! IOS からセルラー モデムに送信される発信 CONFACK。
!
*Jun 21 00:45:45.935: Ce0/0/0 LCP: I CONFACK [ACKsent] id 189 len 20
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: MagicNumber 0x3F7E2331 (0x05063F7E2331)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: PFC (0x0702)
*Jun 21 00:45:45.935: Ce0/0/0 LCP: ACFC (0x0802)
!
! セルラー モデムから IOS によって受信される着信 CONACK。
!
*Jun 21 00:45:45.935: Ce0/0/0 LCP: State is Open
!
! LCP フェーズが正常に完了し、現在開いています。
!
*Jun 21 00:45:45.939: Ce0/0/0 PPP: Phase is AUTHENTICATING, by the peer.
!
! 認証フェーズ開始されます。
!
*Jun 21 00:45:45.939: Ce0/0/0 CHAP: I CHALLENGE id 1 len 35 from "UMTS_CHAP_SRVR"
*Jun 21 00:45:45.943: Ce0/0/0 CHAP: Using hostname from interface CHAP
*Jun 21 00:45:45.943: Ce0/0/0 CHAP: Using password from interface CHAP

*Jun 21 00:45:45.943: Ce0/0/0 CHAP: O RESPONSE id 1 len 40 from
SP-provided-user-name@wwan.ccs

*Jun 21 00:45:45.943: Ce0/0/0 CHAP: I SUCCESS id 1 len 4
!
! CHAP (チャレンジ ハンドシェーク認証プロトコル) フェーズは、正常に完了し、
! 現在開いています。

! この CHAP 認証は、3G-HWIC 上の IOS とセルラー モデムの間でのみ行われ、
! ネットワークとはまだ行われていません。PPP は、ネットワークで終了せず、
! モデムのローカル側で終了することに留意してください。
!
! セルラー ネットワーク (GGSN) は、まだユーザを認証していません。次に、
! セルラー モデムは無線を介して 'Activate PDP context' メッセージを使用し、
! ネットワークから IP アドレスを取得して、ネットワークに対してそれ自体を認証します。
! ネットワークはユーザを認証して IP アドレスを返すことで、
! 'Activate PDP context Accept' メッセージに応答します。'Activate PDP context' メッセージには、
! セルラー インターフェイスの下で設定された CHAP のクレデンシャルが含まれています。
!
*Jun 21 00:45:45.943: Ce0/0/0 PPP: Phase is FORWARDING, Attempting Forward
*Jun 21 00:45:45.947: Ce0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
*Jun 21 00:45:45.947: Ce0/0/0 PPP: Phase is UP
!
! NCP [Network Control Protocol]/ IPCP [IP Control Protocol] フェーズの開始
!
*Jun 21 00:45:45.947: Ce0/0/0 IPCP: O CONFREQ [Closed] id 1 len 22
*Jun 21 00:45:45.947: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 00:45:45.947: Ce0/0/0 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Jun 21 00:45:45.947: Ce0/0/0 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
!
! ホスト IP アドレス、および DNS アドレスを要求する、Cisco IOS によってモデムに送信される
! IPCP CONFREQ (Configure-Request)。
!
*Jun 21 00:45:45.947: Ce0/0/0 PPP: Process pending ncp packets

*Jun 21 00:45:46.955: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 1 len 16
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
```

```

! 上記の CONFREQ の代わりに、モデムによって Cisco IOS に送信された
! IPCP CONFNAK (受信される設定オプションは認識および許容可能ですが、
! 一部の値は許容されません)。
!
! モデムはセルラー ネットワークによってまだ認証されていません。モデムはセルラー ネットワークからの
! 'Activate PDP context Accept' メッセージを待機しています。モデムは、
! IOS のみに応答を送ります。これには、プライマリとセカンダリの DNS アドレスが含まれます
! (実際のアドレスはネットワークによって提供されるため、これらのアドレスは任意です)。
! 理由は明白ですが、これはホスト IP アドレスを IOS に返しません。
!
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 2 len 22
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:46.955: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! モデムから CONFNAK に欠落しているホストの IP アドレスを要求する、
! IOS によってモデムに送信された新しい IPCP CONFREQ。
!
*Jun 21 00:45:47.959: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 2 len 16
*Jun 21 00:45:47.959: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:47.959: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! モデムは、要求されたホストの IP アドレスを除外したまま、IPCP CONFNAK と応答します。
!
! このように除外するのは、モデムがまだ、これらの要求されたパラメータを含む、
! ネットワークからの 'Activate context Accept' メッセージを
! 待っているためです。
!
*Jun 21 00:45:47.959: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 3 len 22
*Jun 21 00:45:47.959: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 00:45:47.963: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:47.963: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! IOS はモデムに IPCP CONREQ を送信し続けます。
!
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 3 len 16
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! モデムは、ここでも要求されたホストの IP アドレスを除外したまま、
! IPCP CONFNAK に応答します。
!
! モデムは、ネットワークからまだ 'Activate PDP context Accept' メッセージを
! 待っています。
!
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 4 len 22
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 00:45:48.967: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! IOS はモデムに IPCP CONREQ を送信し続けます。
!
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: I CONFREQ [REQsent] id 108 len 4
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: O CONFACK [REQsent] id 108 len 4
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: I CONFNAK [ACKsent] id 4 len 22
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: Address 166.138.186.120 (0x0306A68ABA78)
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: PrimaryDNS 66.102.163.231 (0x81064266A3E7)
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: SecondaryDNS 66.102.163.232 (0x83064266A3E8)
!
! 最後に、モデムはセルラー ネットワークから 'Activate PDP context Accept' メッセージを受信します。
! これはモデム/IOS を正常に認証します。また、ネットワークから受信する
! ホスト IP アドレスと DNS アドレスも提供します。

```

```

!
!   ネットワークから受信したこれらの有効なアドレスを含む、
!   モデムによって IOS に送信された IPCP CONFNAK。
!
*Jun 21 00:45:49.263: Ce0/0/0 IPCP: O CONFREQ [ACKsent] id 5 len 22
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   Address 166.138.186.120 (0x0306A68ABA78)
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   PrimaryDNS 66.102.163.231 (0x81064266A3E7)
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   SecondaryDNS 66.102.163.232 (0x83064266A3E8)
!
!   示唆されているホスト IP アドレスと DNS アドレスを要求する、
!   IOS によってモデムに送信された IPCP CONFREQ。
!

*Jun 21 00:45:49.267: Ce0/0/0 IPCP: I CONFACK [ACKsent] id 5 len 22
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   Address 166.138.186.120 (0x0306A68ABA78)
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   PrimaryDNS 66.102.163.231 (0x81064266A3E7)
*Jun 21 00:45:49.267: Ce0/0/0 IPCP:   SecondaryDNS 66.102.163.232 (0x83064266A3E8)
!
!   要求された IP アドレスと DNS アドレスを受け入れ、モデムによって Cisco IOS に送信された
!   IPCP CONFACK (CONFREQ メッセージ内のすべてのオプションが認識可能であり、
!   すべての値が受け入れ可能な場合、ルータは CONFACK メッセージを送信します)。
!

*Jun 21 00:45:49.267: Ce0/0/0 IPCP: State is Open
!
!   IPCP フェーズは現在正常で、開いています。
!

*Jun 21 00:45:49.291: Ce0/0/0 IPCP: Install negotiated IP interface address
166.138.186.120
!
!   セルラー インターフェイスに割り当てられ、ルーティング テーブルにインストールされる IP アドレス。
!

```

#### 例 4-3 通常の動作のセルラー インターフェイス情報

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の出力は、コールのセットアップに成功した後の、**show cellular 0/0/0 all** コマンドの典型的な状態を示しています。

```

ROUTER#sh cellular 0/0/0 all
!
!   見やすくするため通常表示される情報の一部を省略し、
!   重要な情報を強調しています。
!

Profile Information
=====
Profile 1 = ACTIVE
-----
PDP Type = IPv4
PDP address = 166.138.186.120
Access Point Name (APN) = wwan.ccs
Authentication = CHAP
Username: SP-provided-user-name@wwan.ccs, Password: SP-provided-password

Data Connection Information

```

```

=====
Data Transmitted = 276 bytes, Received = 200 bytes
Profile 1, Packet Session Status = ACTIVE
    IP address = 166.138.186.120
!
!   セルラー インターフェイスは、PPP が確立され、IP アドレスが割り当てられたセルラー ネットワークに、
!   プロファイル 1 を使用してアクティブに接続されます。
!
Network Information
=====
Current Service Status = Normal, Service Error = None
Current Service = Combined
Packet Service = UMTS/WCDMA (Attached)
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Country = USA, Network = gsm
Mobile Country Code (MCC) = 310
Mobile Network Code (MNC) = 380
Location Area Code (LAC) = 56997
Routing Area Code (RAC) = 253
Cell ID = 5933
Primary Scrambling Code = 196
PLMN Selection = Automatic
Registered PLMN = gsm , Abbreviated =
Service Provider =
!
!   サービスのタイプ (無線アクセス テクノロジー) に関する情報と、
!   他のセルラー情報を示します。
!
Radio Information
=====
Current Band = WCDMA 1900, Channel Number = 9721
Current RSSI (RSCP) = -77 dBm
!
!   Received Signal Strength Indication (無線の受信レベルを決定する重要な要素) と、
!   使用されるサービスのタイプおよび無線帯域を示します。
!
Modem Security Information
=====
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of Retries remaining = 3
!
!   SIM カードの正常なステータスを表示します
!

```

#### 例 4-4 セルラー インターフェイスについて接続と IP アドレスの入手を行えなかった場合のデバッグ出力 および考えられる原因

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次のデバッグ出力は、IPCP フェーズでの失敗、または IP アドレスを取得できなかった場合の典型的な例です。

```
ROUTER#ping 209.131.36.158 source 10.1.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.131.36.158, timeout is 2 seconds:
Packet sent with a source address of 10.1.0.254

*Jun 21 22:47:51.467: CHAT0/0/0: Attempting async line dialer script
*Jun 21 22:47:51.471: CHAT0/0/0: Dialing using Modem script: gsm & System script: none
*Jun 21 22:47:51.471: CHAT0/0/0: process started
*Jun 21 22:47:51.471: CHAT0/0/0: Asserting DTR
*Jun 21 22:47:51.471: CHAT0/0/0: Chat script gsm started
*Jun 21 22:47:51.471: CHAT0/0/0: Sending string: atdt*98*1#
*Jun 21 22:47:51.471: CHAT0/0/0: Expecting string: CONNECT
*Jun 21 22:47:51.515: CHAT0/0/0: Completed match for expect: CONNECT
*Jun 21 22:47:51.515: CHAT0/0/0: Chat script gsm finished, status = Success.
*Jun 21 22:47:53.719: %LINK-3-UPDOWN: Interface Cellular0/0/0, changed state to up
!
*Jun 21 22:47:53.727: Ce0/0/0 LCP: State is Open
!
*Jun 21 22:47:53.735: Ce0/0/0 CHAP: I SUCCESS id 1 len 4
!
! CHAT、LCP、および CHAP が成功した後に開始される IPCP
!
*Jun 21 22:47:53.735: Ce0/0/0 IPCP: O CONFREQ [Closed] id 1 len 22
*Jun 21 22:47:53.735: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:53.735: Ce0/0/0 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Jun 21 22:47:53.735: Ce0/0/0 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Jun 21 22:47:53.735: Ce0/0/0 PPP: Process pending ncp packets

*Jun 21 22:47:54.739: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 1 len 16
*Jun 21 22:47:54.739: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:54.739: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:54.739: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 2 len 22
*Jun 21 22:47:54.739: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:54.739: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:54.739: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:55.743: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 2 len 16
*Jun 21 22:47:55.747: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:55.747: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:55.747: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 3 len 22
*Jun 21 22:47:55.747: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:55.747: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:55.747: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:56.751: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 3 len 16
*Jun 21 22:47:56.751: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:56.751: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:56.751: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 4 len 22
*Jun 21 22:47:56.751: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:56.751: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:56.751: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:57.755: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 4 len 16
*Jun 21 22:47:57.755: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:57.755: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:57.755: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 5 len 22
*Jun 21 22:47:57.755: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
```

```

*Jun 21 22:47:57.755: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:57.755: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:58.759: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 5 len 16
*Jun 21 22:47:58.759: Ce0/0/0 IPCP: .PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:58.759: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:58.759: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 6 len 22
*Jun 21 22:47:58.759: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:58.759: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:58.759: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:59.799: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 6 len 16
*Jun 21 22:47:59.803: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:59.803: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:47:59.803: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 7 len 22
*Jun 21 22:47:59.803: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:47:59.803: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:47:59.803: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:00.807: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 7 len 16
*Jun 21 22:48:00.811: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:00.811: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:00.811: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 8 len 22
*Jun 21 22:48:00.811: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:48:00.811: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:00.811: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:01.815: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 8 len 16
*Jun 21 22:48:01.815: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:01.815: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:01.815: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 9 len 22
*Jun 21 22:48:01.815: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:48:01.815: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:01.815: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:02.819: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 9 len 16
*Jun 21 22:48:02.819: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:02.819: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:02.819: Ce0/0/0 IPCP: O CONFREQ [REQsent] id 10 len 22
*Jun 21 22:48:02.819: Ce0/0/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 21 22:48:02.819: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:02.819: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)

*Jun 21 22:48:03.823: Ce0/0/0 IPCP: I CONFNAK [REQsent] id 10 len 16
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: PrimaryDNS 10.11.12.13 (0x81060A0B0C0D)
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: SecondaryDNS 10.11.12.14 (0x83060A0B0C0E)
!
! モデムは、セルラー ネットワークで PDP コンテキストを正常に確立できないため、
! PPP によって要求されるホストの IP アドレスおよび他の要求されたパラメータを
! 取得できません。
!
! この理由は、次のいずれかである可能性があります。
! - 無線の受信状態が悪い
! - アンテナが切断されている可能性がある
! - ユーザ名/パスワードおよび APN (アクセス ポイント ネーム) が間違っているか無効である、
!   あるいは設定が間違っている
!
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: Failed to negotiate with peer
!

```

```
! おそらく上記のいずれかの理由で IPCP が失敗しました
!
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: State is Closed
```

#### 例 4-5 IP アドレスを取得できなかった場合のセルラー インターフェイスの詳細

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
ROUTER#sh cellular 0/0/0 all
!
! 見やすくするため通常表示される情報の一部を省略し、
! 重要な情報を強調しています。
!

Profile Information
=====
Profile 1 = INACTIVE
-----
PDP Type = IPv4
Access Point Name (APN) = wwan.ccs
Authentication = CHAP
Username: SP-provided-user-name@wwan.ccs, Password: SP-provided-password
!
! ユーザ名、パスワード、および APN がサービス プロバイダによって提供されているとおりであることを確認して
! ください。それらが、セルラー インターフェイスとモデムの両方に適切に設定されていることも
! 確認してください ('cellular 0/0/0 gsm profile create ...' コマンドを使用)
!

Data Connection Information
=====
Data Transmitted = 14428 bytes, Received = 13852 bytes
Profile 1, Packet Session Status = INACTIVE
Inactivity Reason = Unknown

Network Information
=====
Current Service Status = No service, Service Error = None
Current Service = Combined
Packet Service = None
Packet Session Status = Inactive
Current Roaming Status = Home
Network Selection Mode = Automatic
Country = USA, Network = Cinglr
Mobile Country Code (MCC) = 310
Mobile Network Code (MNC) = 380
Location Area Code (LAC) = 56997
Routing Area Code (RAC) = 255
Cell ID = 0
Primary Scrambling Code = 0
PLMN Selection = Automatic
!
! これは、無線レベルの接続に潜在的な問題があることを示しています。おそらく信号レベルが
! 非常に低いことが原因で、モデムはセルラー ネットワークと通信できません。
!

Radio Information
=====
```

```

Current Band = None, Channel Number = 0
Current RSSI = -110 dBm
!
!   これは、Received Signal Strength Indication (RSSI) が非常に低いことを示しています
!   (-110 dBm)。これは、おそらくアンテナが切断されているか、無線受信レベルが低いために
!   生じています
!

```

```

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

```

#### 例 4-6 ダイアルアウトできない場合のデバッグ出力および考えられる原因

この設定内で青色の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。太字のテキストは、エラーが発生した場合に参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

ROUTER#ping ip 209.131.36.158 source 10.1.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.131.36.158, timeout is 2 seconds:
Packet sent with a source address of 10.5.0.254

*Jun 22 21:50:30.187: CHAT0/0/0: Attempting async line dialer script
*Jun 22 21:50:30.187: CHAT0/0/0: Dialing using Modem script: gsm & System script: none
*Jun 22 21:50:30.187: CHAT0/0/0: process started
*Jun 22 21:50:30.187: CHAT0/0/0: Asserting DTR
*Jun 22 21:50:30.187: CHAT0/0/0: Chat script gsm started
*Jun 22 21:50:30.187: CHAT0/0/0: Sending string: atdt*69*1# 20
*Jun 22 21:50:30.187: CHAT0/0/0: Expecting string: CONNECT"...
*Jun 22 21:50:35.187: CHAT0/0/0: Timeout expecting: CONNECT"
*Jun 22 21:50:35.187: CHAT0/0/0: Chat script gsm finished, status = Connection timed out;
remote host not responding
Success rate is 0 percent (0/5)
!
!   モデムがダイアルアウト コマンドに応答していません。
!
!   おそらくダイヤラ スtringの指定が間違っているために、'chat-script ...' コマンドに
!   問題があることを示しています
!
!   次のような場合に、同様の問題が発生する可能性があります。
!   - 期待されるString ('CONNECT') にタイプミスがあるか、
!   大文字で指定されていない。
!   - 構成内で chat-script コマンドが欠落している
!   - 'script dialer ...' コマンドが対応する行 x/x/x で欠落している
!

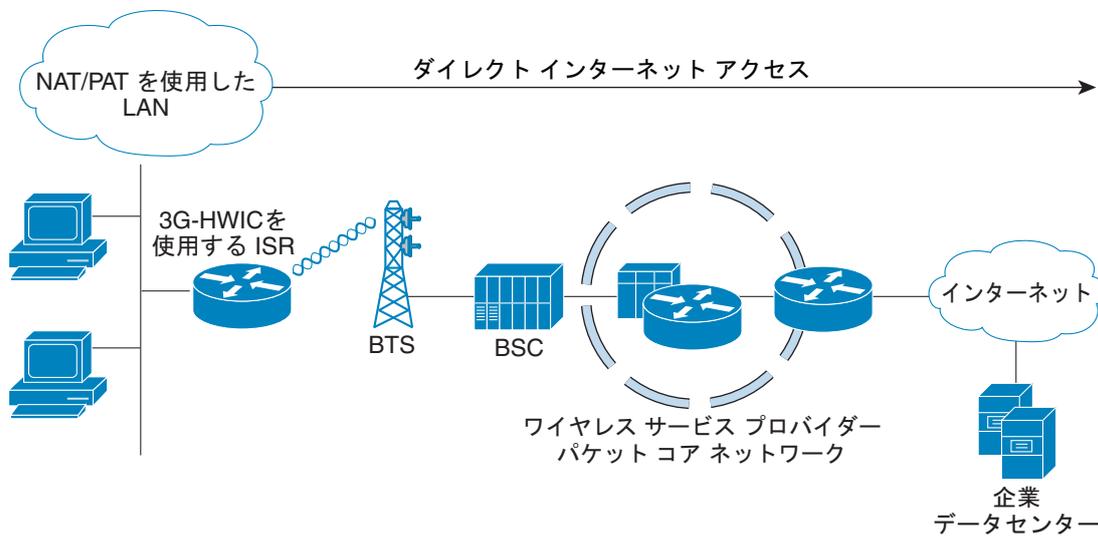
```

# CDMA ベースのワイヤレス ネットワーク

## ネットワーク/ポート アドレス変換 (PAT) を使用した導入

図 4-2 には、NAT/PAT を使用した導入が示されています。これは、ワイヤレス特有の設定に焦点を当てています。より理解を深めるために、この例を確認する前に 3G ワイヤレス特有の設定をよく理解しておく必要があります。NAT の詳細については、[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product\\_data\\_sheet0900aec8064c999.html](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aec8064c999.html) を参照してください。

図 4-2 CDMA ワイヤレス ネットワーク用の NAT/PAT を使用した単純な導入



278754

## 例 4-7 NAT/PAT を使用した導入用の IOS 設定

```

hostname ROUTER
!
ip cef
!
ip dhcp excluded-address 10.3.0.254
!
ip dhcp pool cdmapool
  network 10.3.0.0 255.255.0.0
  dns-server 68.28.58.11
  default-router 10.3.0.254
!
! ネットワーク 10.3.0.0/16、VLAN 103 で接続されているホスト、ファスト イーサネット ポート
! 0/2/0 から 0/2/3 の DHCP プールを定義します
!
chat-script cdma2 "" "atdt#777" TIMEOUT 30 "CONNECT"
chat-script cdma1 "" "atdt#777" TIMEOUT 30 "CONNECT"
!
! cdma2 ワイヤレス ネットワークと cdma1' のネットワークに、ダイヤラ スtring 'cdma2'
! および 'cdma1' をそれぞれ定義します。次の 2 つのどちらのサービス プロバイダを使用しているかに応じて、
! これらの chat-script コマンドを選択する必要があります。'atdt#777' または 'atdt#777'
! コマンドにより、セルラー モデムがダイヤル アウトします。応答で、IOS は正常なダイヤル アウトが行われる
! とモデムから 'CONNECT' スtringを受け取ることを期待します。応答がないか、予期しない応答の場合、
! タイムアウトとして IOS は 30 秒間待機します。モデムからの期待される 'CONNECT' 応答は
! 大文字と小文字が区別されることに注意してください。
!
!
username cisco privilege 15 secret 5 $1$c/50$W4sr3BFW3AhIB9BRXjy84/
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.0
!
interface GigabitEthernet0/0
  no ip address
  ip virtual-reassembly
  shutdown
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/2/0
  switchport access vlan 103
!
interface FastEthernet0/2/1
  switchport access vlan 103
!
interface FastEthernet0/2/2
  switchport access vlan 103
!
interface FastEthernet0/2/3
  switchport access vlan 103
!
! 上記のファスト イーサネット ポートに接続されている DHCP クライアント ホスト。
!
!
interface Cellular0/1/0
  ip address negotiated
  ip nat outside
  no ip virtual-reassembly
  encapsulation ppp
  dialer in-band
  dialer idle-timeout 0

```

```

dialer string cdma1
async mode interactive
dialer-group 1
ppp ipcp dns request
!
!   IP アドレスは、固定 (永続的) IP アドレスが必要な場合でも、ネゴシエートされた IP アドレス
!   として常に設定することを強くお勧めします。セルラー インターフェイスは、
!   PPP が確立されているかどうかに関係なく、'up'/'up' (ステータス/プロトコル ステート)
!   としてスプーフィングされます。このインターフェイスが特定の IP アドレスによって設定されている場合に
!   ('ip address negotiated' ではない)、PPP がまだ確立されていないと、
!   ルーティング テーブルは、セルラー インターフェイスで使用できる有効なルートとして それを解釈します。
!   ネゴシエートされた IP アドレスを割り当てることで、この問題は回避されます。これは特に、
!   セルラーをバックアップ インターフェイスとして使用する場合は重要です。
!
!   ip nat outside は、セルラー インターフェイスを通過する IP パケットのソース IP アドレスとして
!   セルラー インターフェイスに割り当てられ、VLAN 103 上のホストから取得された
!   IP アドレスを使用します。
!
!   dialer in-band は、ダイヤル オンデマンド ルーティングをサポートするようにインターフェイスを設定し、
!   チャット スクリプトがダイヤル アウトされるようにさらに指定します。この場合、
!   前に定義されたように、チャット スクリプト 'cdma1' を使用します。
!
!   dialer idle-timeout を「0」に設定し、このコマンドで定義された特定の時間内にトラフィックがないことで
!   PPP の切断が行われないようにすることをお勧めします。'dialer
!   idle-timeout 0' に設定すると、このタイマーのタイムアウト期間は無制限になります。
!
!   dialer group と dialer-list は関連付けられたコマンドであり、PPP 接続がまだ確立されていない場合に
!   それをセットアップするためにセルラー モデム ダイヤル アウトをトリガーする
!   'interesting' トラフィックを指定できます。
!
!   ppp ipcp dns-request オプション コマンドを使用すると、必要な場合は PPP の手順を使用して、
!   セルラー ネットワークから DNS IP アドレスを取得できるようになります。
!
interface Vlan1
  no ip address
!
interface Vlan103
  ip address 10.3.0.254 255.255.0.0
  ip nat inside
  ip virtual-reassembly
!
!   インターフェイス VLAN 103 を定義します。この VLAN は、関連するホストで使用されます (ファスト
!   イーサネット ポート)。これは、ip nat inside コマンドを使用して、NAT/PAT 機能を提供します。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
!
!   デフォルト ルートがセルラー インターフェイスを介するように定義します。この場合、すべての IP パケットは
!   セルラー インターフェイス経由でルーティングされます。
!
ip nat inside source list 2 interface Cellular0/1/0 overload
!
!   NAT/PATed である必要があるトラフィックのソースがセルラー インターフェイスを介するように指定します。
!   この場合、'overload' パラメータを使用して PAT を実行しています。source
!   list 2 は access-list 2 (以下で定義) に関連付けられています。これにより、
!   対象のトラフィックの送信元が指定されます (この場合は 10.3.0.0/16 ネットワークから)。
!
access-list 1 permit any
access-list 2 permit 10.3.0.0 0.0.255.255
dialer-list 1 protocol ip list 1
no cdp run
!
!   dialer-list 1 コマンドは、セルラー インターフェイスの下に指定されている dialer-group 1 コマンドに
!   関連付けられています。

```

```

!
!   access-list 1 コマンドは dialer-list 1 protocol ip list 1 コマンドに関連付けられています。
!
!   これらのコマンドは、セルラー モデムを介したダイヤル アウトをトリガーする
!   対象のトラフィックを指定し、確立されていない場合は PPP を確立します。
!
control-plane
!
!
line con 0
  exec-timeout 0 0
line aux 0
line 0/1/0
  exec-timeout 0 0
  script dialer cdma1
  login
  modem InOut
  no exec
  transport input all
  transport output all
  speed 144000
!
!   セルラー インターフェイスの対応する行の下に、script dialer コマンドを
!   指定する必要があります。この場合、セルラー インターフェイスは 0/1/0 であるため、
!   回線も基本的に 0/1/0 です。
!
!   speed は設定できません。
!
!   modem InOut を使用すると、ネットワークによって着信コールが現在サポートされていない場合でも、
!   着信および発信コールを実行できるようになります。
!
!   transport input all と transport output all は、セルラー モデムへの
!   リバース telnet 用に使用できます。
!

line vty 0 4
  privilege level 15
  no login
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet
!
scheduler allocate 20000 1000
!
webvpn cef
!
end

```

## デバッグおよびトラブルシューティング

次のデバッグ方式は、一般的な問題をデバッグする場合に役立ちます。

- PPP
  - PPP 詳細イベント
  - PPP プロトコル エラー
  - PPP プロトコル ネゴシエーション
- チャット スクリプト
  - チャット スクリプトのアクティビティのデバッグ

応答が期待され、*interesting traffic* の一部である宛先 IP アドレスを Ping して、接続があるかどうかを確認します。

### 例 4-8 通常の動作のデバッグ出力

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次のデバッグ出力は、コール確立が成功した場合の典型的な例です。

```
ROUTER# ping ip 209.131.36.158 source 10.3.0.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.131.36.158, timeout is 2 seconds:
Packet sent with a source address of 10.3.0.254

*Jun 29 15:40:51.248: CHAT0/1/0: Attempting async line dialer script
*Jun 29 15:40:51.248: CHAT0/1/0: Dialing using Modem script: cdmal & System script: none
*Jun 29 15:40:51.248: CHAT0/1/0: process started
*Jun 29 15:40:51.248: CHAT0/1/0: Asserting DTR
*Jun 29 15:40:51.248: CHAT0/1/0: Chat script cdmal started
*Jun 29 15:40:51.248: CHAT0/1/0: Sending string: atdt#777
*Jun 29 15:40:51.252: CHAT0/1/0: Expecting string: CONNECT..
*Jun 29 15:40:55.728: CHAT0/1/0: Completed match for expect: CONNECT
*Jun 29 15:40:55.728: CHAT0/1/0: Chat script cdmal finished, status = Success
*Jun 29 15:40:55.896: TTY0/1/0: no timer type 1 to destroy
*Jun 29 15:40:55.896: TTY0/1/0: no timer type 0 to destroy
*Jun 29 15:40:55.896: TTY0/1/0: no timer type 2 to destroy.

*Jun 29 15:40:57.896: %LINK-3-UPDOWN: Interface Cellular0/1/0, changed state to up
!
! 'interesting' トラフィックが検出されると、IOS は正常にセルラー モデムと通信し、
! ダイヤル アウトするようにコマンドを発行します。
!
*Jun 29 15:40:57.896: Ce0/1/0 PPP: Using dialer call direction
*Jun 29 15:40:57.896: Ce0/1/0 PPP: Treating connection as a callout
*Jun 29 15:40:57.896: Ce0/1/0 PPP: Session handle[57000CC5] Session id[89]
*Jun 29 15:40:57.896: Ce0/1/0 PPP: Phase is ESTABLISHING, Active Open
*Jun 29 15:40:57.896: Ce0/1/0 PPP: No remote authentication for call-out
!
! PPP の開始を準備する LCP フェーズ。
!
```

```

*Jun 29 15:40:57.896: Ce0/1/0 LCP: O CONFREQ [Closed] id 125 len 20
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: MagicNumber 0x89803B5B (0x050689803B5B)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: PFC (0x0702)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACFC (0x0802)
!
! IOS からモデムへの発信 LCP CONFREQ。
!
*Jun 29 15:40:57.896: Ce0/1/0 LCP: I CONFREQ [REQsent] id 136 len 20
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACCM 0x00000000 (0x020600000000)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: MagicNumber 0xE7985207 (0x0506E7985207)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: PFC (0x0702)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACFC (0x0802)
!
! モデムから Cisco IOS への着信 LCP CONFREQ
!
*Jun 29 15:40:57.896: Ce0/1/0 LCP: O CONFACK [REQsent] id 136 len 20
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACCM 0x00000000 (0x020600000000)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: MagicNumber 0xE7985207 (0x0506E7985207)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: PFC (0x0702)
*Jun 29 15:40:57.896: Ce0/1/0 LCP: ACFC (0x0802)
!
! IOS からモデムへの、CONFREQ をモデムから確認する発信 LCP CONFACK。
!
*Jun 29 15:40:57.900: Ce0/1/0 LCP: I CONFACK [ACKsent] id 125 len 20
*Jun 29 15:40:57.900: Ce0/1/0 LCP: ACCM 0x000A0000 (0x0206000A0000)
*Jun 29 15:40:57.900: Ce0/1/0 LCP: MagicNumber 0x89803B5B (0x050689803B5B)
*Jun 29 15:40:57.900: Ce0/1/0 LCP: PFC (0x0702)
*Jun 29 15:40:57.900: Ce0/1/0 LCP: ACFC (0x0802)
!
! モデムから IOS への、CONFREQ をモデムから確認する着信 LCP CONFACK。
!
*Jun 29 15:40:57.900: Ce0/1/0 LCP: State is Open

*Jun 29 15:40:57.900: Ce0/1/0 PPP: Phase is FORWARDING, Attempting Forward
*Jun 29 15:40:57.900: Success rate is 20 percent (1/5), round-trip min/avg/max = 612/612/612 ms

2851-b1-cdma1#:40:57.900: Ce0/1/0 PPP: Phase is ESTABLISHING, Finish LCP

*Jun 29 15:40:57.900: Ce0/1/0 PPP: Phase is UP
!
! この時点で、LCP が確立されました。次のフェーズは IPCP であり、
! Cisco IOS に関する限り、NOT CHAP または PAP です。
!
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: O CONFREQ [Closed] id 1 len 22
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: Address 0.0.0.0 (0x030600000000)
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Jun 29 15:40:57.900: Ce0/1/0 PPP: Process pending ncp packets
!
! ホスト (セルラー インターフェイス) の IP アドレス、および DNS IP アドレスを提供する、
! IOS からモデム / ネットワークへの発信 IPCP CONFREQ。ホストの IP アドレスは、
! ネットワークから永続的 IP アドレスが要求される場合でも、
! 0.0.0.0 (動的に割り当てられた IP アドレス) に設定されます。
!
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: I CONFREQ [REQsent] id 65 len 10
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: Address 68.28.57.69 (0x0306441C3945)
!
! ネットワークから受信したものとしてそれ自体のアドレスを提供する、
! モデム / ネットワークからの着信 IPCP CONFREQ。
!
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: O CONFACK [REQsent] id 65 len 10
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: Address 68.28.57.69 (0x0306441C3945)

```

```
!  
! ネットワーク アドレスを受け入れる、IOS からモデム / ネットワークへの発信 IPCP CONFACK。  
!  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: I CONFNAK [ACKsent] id 1 len 22  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: Address 70.12.221.250 (0x0306460CDDFA)  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: PrimaryDNS 68.28.58.11 (0x8106441C3A0B)  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: SecondaryDNS 68.28.50.11 (0x8306441C320B)  
!  
! Cisco IOS からの 以前の CONFREQ への応答での、  
! モデム / ネットワークからの着信 IPCP CONFNAK。  
!  
! CONFNAK は、モデムとネットワークの間に発生したモバイル IP 手順の一部として  
! ネットワークから受信した DNS アドレスと、  
! ホスト (セルラー インターフェイス) の IP アドレスを提供します。  
!  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: O CONFREQ [ACKsent] id 2 len 22  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: Address 70.12.221.250 (0x0306460CDDFA)  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: PrimaryDNS 68.28.58.11 (0x8106441C3A0B)  
*Jun 29 15:40:57.900: Ce0/1/0 IPCP: SecondaryDNS 68.28.50.11 (0x8306441C320B)  
!  
! モデム / ネットワークからの上記の CONFNAK への応答での、  
! IOS からの発信 IPCP CONFREQ。  
!  
! CONFNAK は、以前に受信した CONFNAK に含まれるものと同じアドレスと、  
! ホスト (セルラー インターフェイス) の IP アドレスを提供します。  
!  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: I CONFACK [ACKsent] id 2 len 22  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: Address 70.12.221.250 (0x0306460CDDFA)  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: PrimaryDNS 68.28.58.11 (0x8106441C3A0B)  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: SecondaryDNS 68.28.50.11 (0x8306441C320B)  
!  
! これらのアドレスがモデム / ネットワークに受け入れ可能であることを認識している  
! モデム / ネットワークからの着信 IPCP CONFACK。  
!  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: State is Open  
!  
! IPCP フェーズはアップしています  
!  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: Install negotiated IP interface address 70.12.221.250  
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: Install route to 68.28.57.69  
*Jun 29 15:40:57.908: Ce0/1/0 IPCP: Add link info for cef entry 68.28.57.69  
!  
! セルラー インターフェイスに割り当てられ、ルーティング テーブルにインストールされる IP アドレス。  
!  
  
*Jun 29 15:40:58.896: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0/1/0,  
changed state to up
```

## 例 4-9 通常の動作のセルラー インターフェイス情報

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の出力は、コールのセットアップに成功した後の、**show cellular 0/0/0 all** コマンドの典型的な状態を示しています。

```
ROUTER#sh cellular 0/1/0 all
!
!   見やすくするため通常表示される情報の一部を省略し、
!   重要な情報を強調しています。
!
2851-b1-cdma1#sh cellular 0/1/0 all
Hardware Information
=====
Modem Firmware Version = p2005800
Modem Firmware built = 02-09-07
Hardware Version = 1.0
Electronic Serial Number (ESN) = 0x6032691E
Preferred Roaming List (PRL) Version = 60607
Current Modem Temperature = 35 degrees Celsius

Profile Information
=====
Electronic Serial Number (ESN) = 0x6032691E
Modem activated = YES
!
!   HWIC のモデムがアクティブになりました。
!
Account Information:
=====
Activation Date: Not available
Phone Number (MDN) : 9134390870
Mobile Station Identifier (MSID) : 9132214671

Data Profile Info:
=====
Number of data profiles configured : 2
Current active data profile : 1

Data Profile 0 Information
=====
NAI (Network Access Identifier) = 6032691E@hcm.cdma1pcs.com
MN-HA SS = Set
MN-HA SPI = 1234
MN-AAA SS = Set
MN-AAA SPI = 1234
Reverse Tunneling Preference = Set
Home Address = 0.0.0.0
Primary Home Agent Address = 68.28.15.12
Secondary Home Agent Address = 68.28.31.12
!
!   データ プロファイル 0 に関して、モデムの NVRAM でネットワークからロードされる情報を表示します。
!   これはユーザによって使用されるのではなく、管理用にモデムによって使用されます。
!   - NAI を表示
!   - MN-HA および MN-AAA の共有秘密の値は非表示
```

! - 管理用に使用されるプライマリおよびセカンダリの HA のアドレスを  
! 表示。  
!

#### Data Profile 1 Information (Active)

=====  
NAI (Network Access Identifier) = productmarketing393@cdmalpcs.com  
MN-HA SS = Set  
MN-HA SPI = 1234  
MN-AAA SS = Set  
MN-AAA SPI = 1234  
Reverse Tunneling Preference = Set  
Home Address = 0.0.0.0  
Primary Home Agent Address = 68.28.81.76  
Secondary Home Agent Address = 68.28.89.76

!  
! データ プロファイル 1 に関して、モデムの NVRAM でネットワークからロードされる情報を表示します。  
! これはユーザによって使用されます。  
! - NAI を表示  
! - MN-HA および MN-AAA の共有秘密の値は非表示  
! - モバイル IP 用に使用されるプライマリおよびセカンダリの HA のアドレスを  
! 表示。  
!

#### Data Connection Information

=====  
Phone number of outgoing call = #777  
HDR AT State = Inactive, HDR Session State = Open  
HDR Session Info:  
    UATI (Hex) = 0084:0AC0:0000:0000:000A:05DC:A812:00A9  
    Color Code = 32, RATI = 0x266DF468  
    Session duration = 480 msecs, Session start = 4365427257 msecs  
    Session end = 4365428118 msecs, Authentication Status = Authenticated  
HDR DRC Value = 14, DRC Cover = 1, RRI = 9.6 kbps  
Current Transmitted = 8777 bytes, Received = 8036 bytes  
Total Transmitted = 31520 KB, Received = 312411 KB  
Current Call Status = CONNECTED Privacy Mode = OFF, Service Option = 33  
Current Call Duration = 261 secs  
Total Call Duration = 7938948 seconds  
Current Call State = AT Packet Call  
Last Call Disconnect Reason = Client ended call  
Last Connection Error = None  
HDR DDTM (Data Dedicated Transmission Mode) Preference = Off  
Mobile IP Error Code (RFC-2002) = 0 (Registration accepted)

!  
! データ接続に関する情報が表示されます。  
!

#### Network Information

=====  
Current Service = 1xRTT only  
Current Roaming Status(1xRTT) = HOME, (HDR) = HOME  
Current Idle Digital Mode = CDMA  
Current System Identifier (SID) = 4183  
Current Network Identifier (NID) = 87  
Current Call Setup Mode = Mobile IP only  
Serving Base Station Longitude = -121 deg -55 min -8 sec  
Serving Base Station Latitude = 37 deg 25 min 22 sec  
Current System Time = Fri Jun 29 12:10:54 2007

#### Radio Information

=====  
1xRTT related info  
-----  
Current RSSI = -93 dBm, ECIO = -9 dBm

```
Current Channel Number = 50
Current Channel State = Acquired
Current Band Class = Band Class 1
```

#### HDR (1xEVDO) related info

```
-----
Current RSSI = -125 dBm, ECIO = -2 dBm
Current Channel Number = 25
Current Band Class = Band Class 1
Sector ID (Hex) = 0084:0AC0:0000:0000:000A:05DC:A801:1202
Subnet Mask = 104, Color Code = 32, PN Offset = 240
Rx gain control(Main) = Unavailable, Diversity = Unavailable
Tx total power = -5 dBm, Tx gain adjust = -256 dBm
Carrier-to-interference (C/I) ratio = 12
```

#### Modem Security Information

```
=====
Modem PIN Security UNLOCKED
Power-up lock DISABLED
ROUTER#
```

### 例 4-10 セルラー インターフェイスについて接続と IP アドレスの入手を行えなかった場合のデバッグおよび考えられる原因

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
ROUTER#ping ip 209.131.36.158 source ip 10.3.0.254
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.131.36.158, timeout is 2 seconds:
Packet sent with a source address of 10.3.0.254
```

```
*Jun 29 20:37:19.043: CHAT0/1/0: Attempting async line dialer script
*Jun 29 20:37:19.043: CHAT0/1/0: Dialing using Modem script: cdma1 & System script: none
*Jun 29 20:37:19.043: CHAT0/1/0: process started
*Jun 29 20:37:19.043: CHAT0/1/0: Asserting DTR
*Jun 29 20:37:19.043: CHAT0/1/0: Chat script cdma1 started
*Jun 29 20:37:19.043: CHAT0/1/0: Sending string: atdt#777
*Jun 29 20:37:19.043: CHAT0/1/0: Expecting string: CONNECT.....
Success rate is 0 percent (0/5)
*Jun 29 20:40:19.043: CHAT0/1/0: Timeout expecting: CONNECT
*Jun 29 20:40:19.043: CHAT0/1/0: Chat script cdma1 finished, status = Connection timed out; remote host not responding
*Jun 29 20:40:19.043: TTY0/1/0: Line reset by "Async dialer"
*Jun 29 20:40:19.043: TTY0/1/0: Modem: (unknown)->HANGUP
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 0 to destroy
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 1 to destroy
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 3 to destroy
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 4 to destroy
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 10 to destroy
*Jun 29 20:40:19.043: TTY0/1/0: no timer type 2 to destroy
2851-b1-cdma1#
!
!   - モデムがダイヤル アウト コマンドに応答していない。
!   - アンテナの切断、または信号受信状態が非常に悪いことが原因である
!   可能性がある。
```

- ! - 考えられる他の原因として、'chat-script …' コマンドに関する問題が挙げられる。
- ! おそらく、ダイヤラ スtringの指定が間違っています
- ! 次のような場合に、同様の問題が発生する可能性があります。
- ! - 期待されるString ('CONNECT') にタイプミスがあるか、
- ! 大文字で指定されていない。
- ! - 構成内で chat-script コマンドが欠落している
- ! - 'script dialer …' コマンドが対応する行 x/x/x で欠落している
- !

## 例 4-11 接続できず、IP アドレスを取得できなかった場合のセルラー インターフェイスの詳細

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
ROUTER#sh cellular 0/1/0 all
!
! 見やすくするため通常表示される情報の一部を省略し、
! 重要な情報を強調しています。
!

Network Information
=====
Current Service = No Service
Current Roaming Status(1xRTT) = HOME, (HDR) = HOME
Current Idle Digital Mode = CDMA
Current System Identifier (SID) = 4183
Current Network Identifier (NID) = 87
Current Call Setup Mode = Mobile IP only
Serving Base Station Longitude = -121 deg -55 min -8 sec
Serving Base Station Latitude = 37 deg 25 min 22 sec
Current System Time = Fri Jun 29 13:26:48 2007

Radio Information
=====
1xRTT related info
-----
Current RSSI = -125 dBm, ECIO = -2 dBm
Current Channel Number = 950
Current Channel State = Scanning
Current Band Class = Band Class 0

HDR (1xEVDO) related info
-----
Current RSSI = -125 dBm, ECIO = -2 dBm
Current Channel Number = 25
Current Band Class = Band Class 1
Sector ID (Hex) = 0084:0AC0:0000:0000:000A:05DC:A801:1202
Subnet Mask = 104, Color Code = 32, PN Offset = 240
Rx gain control(Main) = Unavailable, Diversity = Unavailable
Tx total power = -5 dBm, Tx gain adjust = -256 dBm
Carrier-to-interference (C/I) ratio = 12

Modem Security Information
=====
Modem PIN Security UNLOCKED
Power-up lock DISABLED
!
! 見やすくするため通常表示される情報の一部を省略し、
! 重要な情報を強調しています。
!
```



## CHAPTER 5

# 高度なネットワーク導入シナリオ

---

この章では、高度な導入シナリオについて説明します。この章全体で導入シナリオに使用されている設定は、GSM 用です。同じ設定にわずかな変更を加えることで、CDMA 導入シナリオに使用できます。

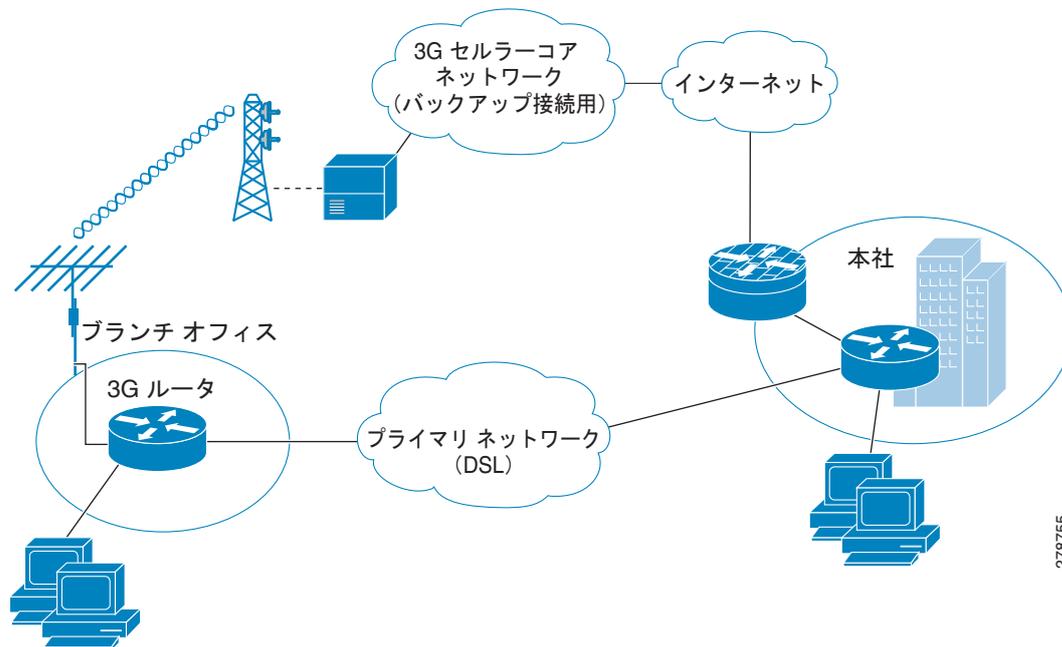
## 内容

- 「NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入」(P.5-2)
- 「GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入」(P.5-11)
- 「本社サイトのルータの設定」(P.5-18)
- 「GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入」(P.5-21)
- 「本社サイトのルータの設定」(P.5-28)
- 「IPSec および OSPF を使用した DMVPN の導入」(P.5-32)
- 「本社サイトのルータの設定」(P.5-38)
- 「プライマリ リンクおよびバックアップ リンクを使用した EzVPN 導入」(P.5-41)
- 「CCOA-Only モードでの NEMO Over 3G」(P.5-47)

# NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入

図 5-1 には、プライマリ リンクとして DSL インターフェイスを使用し、バックアップリンクとしてセルラー インターフェイスを使用する導入が示されています。この導入では、ブランチ オフィス ルータのホストとパブリック ネットワーク経由の本社サイトのホスト間のセキュア通信に、ブランチ オフィスで NAT/PAT および IPSec を使用します。この導入により、インターネット上のホストとのノンセキュア (非 IPSec) 通信も行えるようになります。

図 5-1 NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入



## ブランチ オフィス ルータの設定

例 5-1 ブランチ オフィス ルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPsec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
! この設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は
! 任意です。これを使用して、このプライマリ インターフェイスを介した外部ネットワークで、
! ICMP の ping を使用して、ある既知の IP 宛先アドレスへのプライマリ (DSL) インターフェイスを介した
! 接続性のトラッキングを行えます。ping への応答の受信に失敗すると、プライマリ インターフェイスを介した

```

```

! デフォルト ルートがルーティング テーブルから削除され、セルラー インターフェイスを介した
! (より高い管理距離で設定されている) デフォルト ルートが有効なパスになり、
! バックアップ パスを介して接続できるようになります。
!
! これが設定されていなくても、PPP/ 物理層でネットワーク接続障害を検出し、
! バックアップ (セルラー) インターフェイスへのスイッチオーバーを行う
! 'backup interface …' コマンドを使用して、
! プライマリ/バックアップ接続を実行できます。
!
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
! 基本的に、このコマンドはどのホストに対しても IP アドレス 10.4.0.254 の割り当てを行いません。
! これは、このアドレスが VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 で
! 接続されているホストのデフォルト ゲートウェイ アドレスとして使用されているからです。
!
!
ip dhcp pool gsmppool
network 10.4.0.0 255.255.0.0
dns-server 66.209.10.201 66.102.163.231
default-router 10.4.0.254
!
! VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に接続されている
! ホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
! セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト。
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
! operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
! を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。
!
! これは、(プライマリ リンクとして使用される) ATM DSL インターフェイスを介して ping パケットを送信し、
! 応答を監視するために使用されます。また、応答がない場合に (セルラーへの) スwitchオーバーが
! 必要かどうかを判別するために使用されます。
!
!
crypto isakmp policy 1
encr 3des
authentication pre-share
!
! (priority 1 を設定して) IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
! 事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値 (1 日に 86,400 秒に設定)、
! グループ (768 ビットディフィー・ヘルマン鍵共有に設定)、
! およびハッシュ (SHA-1 に設定) は、デフォルト値に設定されます。
!
!
crypto isakmp key mykey address 20.20.241.234
!
! セキュリティ アソシエーションの設定に使用されるキー (mykey)
! およびゲートウェイの IP アドレス (IPsec peer) を定義します。
!
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
! セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
! トランスフォーム セット (mytransformset) を定義して、IPsec で保護されている

```

```

!   トラフィックを適用します。
!
crypto map gsm1 10 ipsec-isakmp
  set peer 20.20.241.234
  set transform-set mytransformset
  match address 103
!
!   クリプト マップ gsm1 を定義します
!
!   クリプト マップは (match address <access-list> コマンドを使用して) 保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット
!   (以前に定義した mytransformset) を指定します。
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  switchport access vlan 104
!
interface FastEthernet0/1/1
  switchport access vlan 104
!
interface FastEthernet0/1/2
  switchport access vlan 104
!
interface FastEthernet0/1/3
  switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート。
!
interface ATM0/0/0
  no ip address
  ip virtual-reassembly
  load-interval 30
  no atm ilmi-keepalive
  dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM (DSL) 物理インターフェイス。
!
interface ATM0/0/0.1 point-to-point
  ip nat outside
  ip virtual-reassembly
  no snmp trap link-status
  pvc 0/35
  pppoe-client dial-pool-number 2
!
!
!   プライマリ接続として PVC に使用する ATM サブインターフェイス。このインターフェイスでは
!   NAT (外部) が使用されます。
!
!   pppoe-client dial-pool-number 2 は PPP over Ethernet (PPOE) クライアントを設定し、
!   使用するダイヤラ プール 2 を指定します。このインターフェイスは、以下で定義されている 'interface
!   Dialer 2' に関連付けられます。
!
interface Cellular0/3/0
  ip address negotiated

```

```

ip nat outside
ip virtual-reassembly
encapsulation ppp
dialer in-band
dialer idle-timeout 0
dialer string gsmscript
dialer-group 1
ppp chap hostname isp-provided-hostname
ppp chap password 0 isp-provided-password
ppp ipcp dns request
crypto map gsm1
!
!   上記で定義したクリプト マップ gsm1 を、このバックアップ インターフェイスに適用します。
!
!   dialer-group 1 は group number 1 を定義します。この設定では、これは以下で指定される
!   dialer-list 1... コマンドに関連付けられます。これは、ダイヤル アウトをトリガーし、
!   PPP を確立した後にインターフェイスをオンラインにする「対象のトラフィック」を
!   定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意してください。このため、
!   対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに
!   プライマリ (ATM DSL) インターフェイスを介してフローしています。
!
!   NAT のインターフェイスを外部で定義します。
!
interface Vlan104
description ip address used as default gateway address for DHCP    clients
ip address 10.4.0.254 255.255.0.0
ip nat inside
ip virtual-reassembly
!
!   NAT (内部インターフェイス) を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3
!   に接続されたホストに VLAN 104 を定義します
!
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 isp-provided-hostname
ppp chap password 0 isp-provided-password
ppp pap sent-username isp-provided-hostname password 0 isp-provided-password
ppp ipcp dns request
crypto map gsm1
!
!   dialer pool 2 コマンドはこのダイヤラ インターフェイスを ATM サブインターフェイス
!   atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
!   これは以下で指定されている dialer-list 2... コマンドに関連付けられます。これは、PPP を確立した後に、
!   ダイヤル アウトをトリガーし、インターフェイスをオンラインにする「対象のトラフィック」
!   を定義します。
!
!   NAT のインターフェイスを外部で定義します。
!
!   上記で定義したクリプト マップ gsm1 をこのプライマリ インターフェイスに適用します。
!
ip local policy route-map track-primary-if
!
!   ルート マップの track-primary-if で定義されているように、
!   IP ルート ポリシーを指定します。
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234

```

## ■ NAT/PAT および IPSec を使用したプライマリおよびバックアップの導入

```

!
!   上記で定義したトラッキング オブジェクト (234) を指定し、ダイヤラ 2 (ATM DSL)
!   を介してデフォルト ルートを定義します。
!
!   ルートはトラッキング対象オブジェクト (234) が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   管理距離を 254 (ダイヤラ 2 のインターフェイスより高い) に設定して、
!   セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは
!   バックアップ インターフェイスとして想定されているからです。
!
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を
!   定義します (以下で指定)。'overload' オプションを使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   上記と同様に、ダイヤラ 2 インターフェイス (ATM DSL) を使用して、外部 NAT トラフィックに対して
!   ルート マップ nat2cell を (以下で定義されているように) 定義します。'overload' オプションを
!   使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip sla 1
  icmp-echo 209.131.36.158 source-interface Dialer2
  timeout 1000
  frequency 2
ip sla schedule 1 life forever start-time now
!
!   2 秒間隔 (frequency 2) で、ping への応答に 1000 ミリ秒の待機 (タイムアウト 1000) を設定し、
!   ソース インターフェイスとしてダイヤラ 2 (ATM DSL) を使用して、
!   IP アドレス 209.131.36.158 に ping を送信するためのサービス レベル契約 (SLA) を
!   定義します。
!
!   定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
!   以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   ルート マップ nat2dsl と nat2cell の下に定義されているように、
!   適切な発信インターフェイスを決定するために、トラフィックが一致するように指定します
!   (ネットワーク 10.4.0.0 のソース アドレスと一致)。
!
access-list 102 permit icmp any host 209.131.36.158
!
!   このインターフェイスがアクティブな場合にのみ、ATM DSL インターフェイスを介して送信されるように、
!   ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
!   この特定のアドレスは、ATM DSL インターフェイス (プライマリ リンク) を介して定期的に ping される
!   アドレスであるため、リンク / PPP レベル以外のネットワーク障害も検出される場合があり、
!   セルラー (セカンダリ) インターフェイスへのスイッチオーバーが

```

```

!   まだ実行される可能性があります。
!
!   ping されるアドレスが信頼でき、ping に応答することを確認します。
!
access-list 103 permit ip host 166.138.186.119 20.20.0.0 0.0.255.255
access-list 103 permit ip host 75.40.113.246 20.20.0.0 0.0.255.255
!
!   クリプト マップ gsm1 の下に定義されたとおりの、
!   IPsec に対して保護されたトラフィックの指定。
!
!   ソース アドレス (166.138.186.119 および 75.40.113.246) は、セルラー インターフェイス (セカンダリ)
!   と ATM DSL インターフェイス (プライマリ) の IP アドレスです。
!
!   20.20.0.0 は宛先ネットワークであり、対応するゲートウェイが接続されています
!
dialer-list 1 protocol ip list 1
!
!   セルラー インターフェイスがダイヤル アウトする原因となる 'interesting traffic' を指定します。
!   それによって、access-list 1 が (上記で定義されたこのコマンドの一部として) さらに指定されます。
!
dialer-list 2 protocol ip permit
!
!   ATM DSL インターフェイスが (ダイヤラ 2 インターフェイスの一部として) ダイヤル アウトするようにする
!   'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10
  match ip address 102
  set interface Dialer2 null0
!
!   ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
!   (上記の関連するコマンド 'ip local policy route-map track-primary-if'
!   を参照してください)。
!
!   これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイアラ 2
!   (ATM DSL) が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
!   ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
!   これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
!   接続 (到達可能性) を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
  match ip address 101
  match interface Dialer2
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイアラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイスのダイアラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
!   このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
  match ip address 101
  match interface Cellular0/3/0
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイアラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
!   が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!

```

```

! スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
  event track 234 state any
  action 2.0 cli command "clear ip nat trans forced"

control-plane
!
line con 0
  exec-timeout 0 0
  exec prompt timestamp
  stopbits 1
line aux 0
  stopbits 1
line 0/3/0
  exec-timeout 0 0
  script dialer gsmscript
  login
  modem InOut
  no exec
  transport input all
  transport output all
  rxspeed 236800
  txspeed 118000
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet
!
scheduler allocate 20000 1000
!
end

```

## 本社サイトのルータの設定

### 例 5-2 本社サイトのルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 20.20.248.253
ip dhcp excluded-address 20.20.248.225
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!

```

```
! DHCP の除外アドレス
!
ip dhcp pool 20
  network 20.20.248.224 255.255.255.224
  dns-server 20.20.248.254
  default-router 20.20.248.254
!
! 20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
  network 10.10.0.0 255.255.0.0
  default-router 10.10.0.254
!
! 10.10.0.0 ネットワーク上の VPN のホストの DHCP プール
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e519DCU1
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share

crypto isakmp key mykey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set mytset ah-sha-hmac esp-3des
!
crypto dynamic-map gw_map 10
  description IPsec tunnel to DSL/Cellular at remote branch-router
  set transform-set mytset
  match address 101
!
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gw_map
!
! リモート ブランチ ルータで、IPsec トンネルの mytunnelcrypto マップを
! ATM DSL/ およびセルラー インターフェイスに定義します。
!
!
interface GigabitEthernet0/0
  description connected to cisco network, next hop:20.20.241.233
  ip address 20.20.241.234 255.255.255.252
  load-interval 30
  duplex auto
  speed auto
  media-type rj45
  negotiation auto
  crypto map mytunnelcrypto
!
! クリプト マップを適用する物理インターフェイス。上記の IPsec トンネルが
! 確立されるインターフェイス。
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  switchport access vlan 10
  spanning-tree portfast
!
!
! VPN のホストが (10.10.0.0 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
  switchport stacking-partner interface FastEthernet0/3/8
```

```

!
interface FastEthernet0/3/0
  switchport access vlan 20
  spanning-tree portfast
!
!
!   他のホストが (20.20 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
  switchport mode trunk
  switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
description private networking vlan
ip address 10.10.0.254 255.255.0.0
no ip route-cache cef
vlan-range dot1q 1 4095
exit-vlan-config
!
!
!   VPN のホストの VLAN (10.10.0.0 ネットワーク内)
!
interface Vlan20
  description network:20.20.248.224/27
  ip address 20.20.248.254 255.255.255.224
  vlan-range dot1q 1 4095
  exit-vlan-config
!
!
!   他のホストの VLAN (20.20 ネットワーク内)
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   GigabitEthernet0/0 インターフェイスのネクスト ホップを介するデフォルト ルート。
!
ip dns server
!
access-list 101 permit ip host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドで DSL インターフェイスに送信されるトラフィックです。
!
access-list 101 permit ip host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
!
control-plane
!
line con 0
  exec-timeout 0 0
  login local
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet

```

```

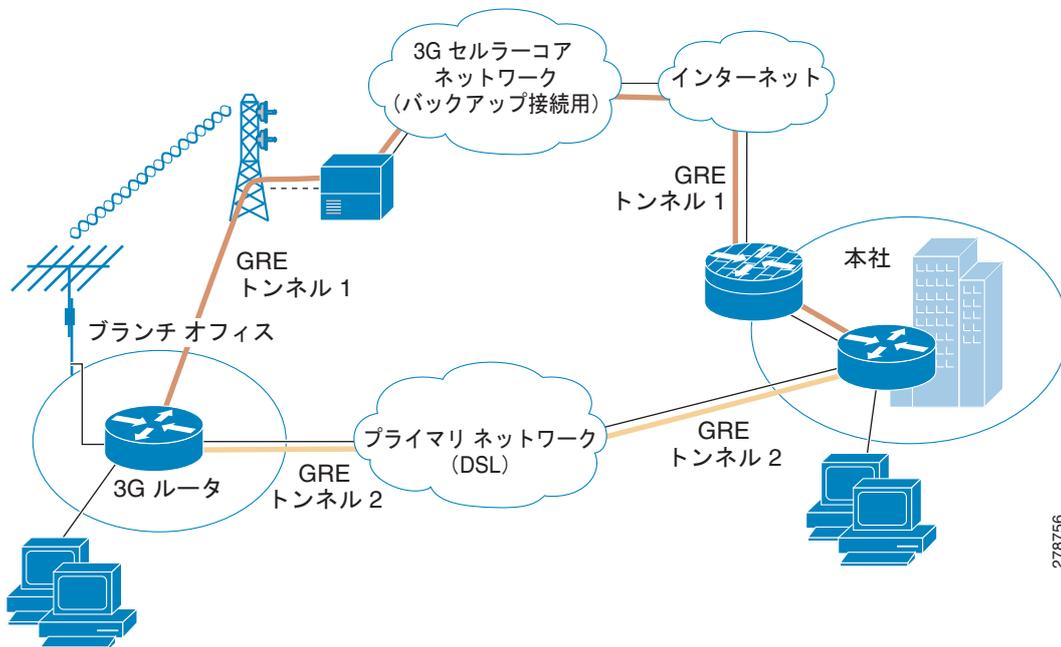
!
scheduler allocate 20000 1000
!
webvpn context Default_context
  ssl authenticate verify all
!
no inservice
!
!
end

```

## GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入

この導入では、パブリック ネットワークを介したブランチ オフィスのルータのホストと本社サイトのホストの間でセキュアな通信を行うために、GRE トンネルと IPSec をブランチ オフィスで使用して、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー インターフェイスを使用します。この導入により、インターネット上のホストとのノンセキュア（非 IPSec）通信も行えるようになります。ダイナミック ルーティングを使用した GRE トンネル経由の IPSec 構成の詳細については、「[Configuring a GRE Tunnel over IPsec with OSPF](#)」を参照してください。

図 5-2 GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入



## ブランチ オフィス ルータの設定

### 例 5-3 ブランチ オフィス ルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

特に明記されていない限り、太字のテキストは基本セルラー コマンドに関連付けられているコマンドを示します。太字のテキストは暗号化 IPSec 設定、バックアップ設定、IP SLA 設定、およびモバイル IP の設定など、他の設定にも使用されます。これらの各設定に関連付けられているコマンドはサンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は任意です。

```

!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
!   このアドレスは、VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 上で
!   接続されているホストのデフォルト ゲートウェイ アドレスとして使用されます。
!
ip dhcp pool gsmppool
  network 10.4.0.0 255.255.0.0
  dns-server 66.209.10.201 66.102.163.231
  default-router 10.4.0.254
!
!   VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に
!   接続されているホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト。
!
!
username cisco privilege 15 secret 5 $l$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
!   を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。
!
!   これは、(プライマリ リンクとして使用される) ATM DSL インターフェイスを介して ping パケットを送信し、
!   応答を監視するために使用されます。また、応答がない場合に (セルラーへの) スイッチオーバーが
!   必要かどうかを判別するために使用されます。
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
!
!   (priority 1 を設定して) IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
!   事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値 (1 日に 86,400 秒に設定)、
!   グループ (768 ビットディフィー・ヘルマン鍵共有に設定)、
!   およびハッシュ (SHA-1 に設定) は、デフォルト値に設定されます。
!
crypto isakmp key mykey address 20.20.241.234

```

```

!
!   セキュリティ アソシエーションの設定に使用されるキー (mykey)
!   およびゲートウェイの IP アドレス (IPsec peer) を定義します。
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
!   トランスフォーム セット (mytransformset) を定義して、IPsec で保護されている
!   トラフィックを適用します。
!
crypto map mytunnelcrypto 10 ipsec-isakmp
  set peer 20.20.241.234
  set transform-set mytransformset
  match address gre-traffic
!
!   クリプト マップの mytunnelcrypto を定義します
!
!   クリプト マップは (match address <access-list> コマンドを使用して) 保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット
!   (以前に定義した mytransformset) を指定します。
!
!
interface Tunnel1
  ip unnumbered Dialer2
  ip mtu 1400
  tunnel source Dialer2
  tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL (プライマリ) インター
!   フェイスに関連付けられたトンネル。このトンネルは、通常 'UP' の状態です。リモート トンネルのエンド
!   ポイント (20.20.241.234) は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンドポイント
!   は、ATM DSL リンクによって取得されるアドレスです。
!
interface Tunnel2
  ip unnumbered Cellular0/3/0
  ip mtu 1400
  tunnel source Cellular0/3/0
  tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL (プライマリ) インターフェイ
!   スに関連付けられたトンネル。セルラー (セカンダリ) インターフェイス。このトンネルは、通常 'Down' の
!   状態です。リモート トンネルのエンドポイント (20.20.241.234) は、リモート VPN ゲートウェイにありま
!   す。ローカル トンネルのエンドポイントは、セルラー リンクによって取得されるアドレスです。このトンネルは、
!   セルラー インターフェイスでスイッチオーバーが行われると 'UP' になります。
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  switchport access vlan 104
!
interface FastEthernet0/1/1
  switchport access vlan 104
!
interface FastEthernet0/1/2
  switchport access vlan 104

```

## GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入

```

!
interface FastEthernet0/1/3
  switchport access vlan 104
!
! DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
  no ip address
  ip virtual-reassembly
  load-interval 30
  no atm ilmi-keepalive
  dsl operating-mode auto
!
! プライマリ インターフェイスとして使用される ATM (DSL) 物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
  ip nat outside
  ip virtual-reassembly
  no snmp trap link-status
  pvc 0/35
  pppoe-client dial-pool-number 2
!
!
! プライマリ接続として PVC に使用する ATM サブインターフェイス。このインターフェイスでは
! NAT (外部) が使用されます。
!
! pppoe-client dial-pool-number 2 は PPP over Ethernet (PPOE) クライアントを設定し、
! 使用するダイヤラ プール 2 を指定します。このインターフェイスは、
! 'interface Dialer 2' に関連付けられています。
!
interface Cellular0/3/0
  ip address negotiated
  ip nat outside
  encapsulation ppp
  dialer in-band
  dialer idle-timeout 0
  dialer string gsmscript
  dialer-group 1
  async mode interactive
  ppp chap hostname crlaswlech@wwan.ccs
  ppp chap password 0 frludi3gIa
  ppp ipcp dns request
  crypto map mytunnelcrypto
!
! 上記で定義したクリプト マップ mytunnelcrypto を、このバックアップ インターフェイスに適用します。
!
! dialer-group 1 は group number 1 を定義します。
! この設定では、これは以下に定義されている 'dialer-list 1 ...' コマンドに関連付けられます。これは、
! ダイヤル アウトをトリガーし、PPP を確立した後にインターフェイス をオンラインにする「対象のトラフィッ
! ク」を定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意してください。
! このため、対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに
! プライマリ (ATM DSL) インターフェイスを介してフローしています。
!
! NAT のインターフェイスを外部で定義します。
!
!
interface Vlan104
  description used as default gateway address for DHCP clients
  ip address 10.4.0.254 255.255.0.0
  ip nat inside
!
! NAT (内部インターフェイス) を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3 に
! 接続されたホストに VLAN 104 を定義します。
! NAT/PAT は、トンネルを介してピア ゲートウェイの 20.20.0.0 ネットワークに送信されるように

```

```

! 意図されていないトラフィックに使用されます。
!
interface Dialer2
 ip address negotiated
 ip nat outside
 encapsulation ppp
 load-interval 30
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname cisco@cisco.com
 ppp chap password 0 cisco123
 ppp pap sent-username cisco@cisco.com password 0 cisco123
 ppp ipcp dns request
 crypto map mytunnelcrypto
!
! "dialer pool 2" コマンドは、このダイヤラ インターフェイスを ATM サブ インターフェイス
! atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
! これは以下で指定されている 'dialer-list 2 ...' コマンドに関連付けられます。これは、PPP を確立した
! 後に、ダイヤラ アウトをトリガーし、インターフェイスをオンラインにする
! 「対象のトラフィック」を定義します。
!
! NAT のインターフェイスを外部で定義します。
!
! 上記で定義したクリプト マップ mytunnelcrypto をこのプライマリ インターフェイスに適用します。
!
ip local policy route-map track-primary-if
!
! ルート マップの track-primary-if で定義されているように、
! IP ルート ポリシーを指定します。
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
! 上記で定義したトラッキング オブジェクト (234) を指定し、ダイヤラ 2 (ATM DSL)
! を介してデフォルト ルートを定義します。
!
! ルートはトラッキング対象オブジェクト (234) が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
! 管理距離を 254 (ダイヤラ 2 のインターフェイスより高い) に設定して、
! セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは
! バックアップ インターフェイスとして想定されているからです。
!
ip route 10.10.0.0 255.255.0.0 Tunnel1
!
! リモート 10.10.0.0 VPN ネットワークへのルートは、ATM DSL (プライマリ) インターフェイスに
! 関連付けられた GRE トンネルを経由します。
!
ip route 10.10.0.0 255.255.0.0 Tunnel2 254
!
! リモート 10.10.0.0 VPN ネットワークへのルートは、セルラー (セカンダリ) インターフェイスに
! 関連付けられた GRE トンネルを経由します。管理距離は 254 (Tunnel1 のものよりも高い) に
! 設定されています。
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
! セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を定義し
! ます (以下で指定)。'overload' オプションを使用すると、PAT が使用されるようになります。
!
! ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!

```

## GRE トンネルおよび IPSec を使用したプライマリおよびバックアップの導入

```

! 上記と同様に、ダイヤラ 2 インターフェイス (ATM DSL) を使用して、外部 NAT トラフィックに対して
route-map nat2cell を (以下で定義されているように) 定義します。'overload' オプションを使用すると、
PAT が使用されるようになります。
!
! ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip access-list extended gre-traffic
 permit gre host 75.40.113.246 host 20.20.241.234
 permit gre host 166.138.186.119 host 20.20.241.234
!
! GRE トンネルを経由して IPSec トラフィックを保護するための gre-traffic アクセス リスト。
!
! これは DSL/ セルラー インターフェイス (どちらかアクティブな方) と、
! リモート ゲートウェイ上の IPsec ピア (20.20.241.234) を介した GRE トンネリング
! されたトラフィックのみを保護します。
!
ip sla 1
 icmp-echo 209.131.36.158 source-interface Dialer2
 timeout 1000
 frequency 2
!
ip sla schedule 1 life forever start-time now
!
! 2 秒間隔 (frequency 2) で、ping への応答に 1000 ミリ秒の待機 (タイムアウト 1000) を設定し、
! ソース インターフェイスとしてダイヤラ 2 (ATM DSL) を使用して、
! IP アドレス 209.131.36.158 に ping を送信するための
! サービス レベル契約 (SLA) を定義します。
!
! 定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
! 以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
! ルート マップ nat2dsl と nat2cell の下に定義されているように、
! 適切な発信インターフェイスを決定するために、トラフィックが一致するように
! 指定します (ネットワーク 10.4.0.0 のソース アドレスと一致)。
!
access-list 102 permit icmp any host 209.131.36.158
!
! このインターフェイスがアクティブな場合にのみ、ATM DSL インターフェイスを介して
! 送信されるように、ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
! この特定のアドレスは、ATM DSL インターフェイス (プライマリ リンク) を介して定期的に ping される
! アドレスであるため、リンク / PPP レベル以外のネットワーク障害も検出される場合があり、
! セルラー (セカンダリ) インターフェイスへのスイッチオーバーがまだ実行される
! 可能性があります。
!
! ping されるアドレスが信頼でき、ping に応答することを確認します。
!
dialer-list 1 protocol ip list 1
!
! セルラー インターフェイスがダイヤラ アウトする原因となる 'interesting traffic' を指定します。
! それによって、access-list 1 が (上記で定義されたこのコマンドの一部として) さらに指定されます。
!
dialer-list 2 protocol ip permit
!
! ATM DSL インターフェイスが (ダイヤラ 2 インターフェイスの一部として) ダイヤラ アウトするようにする
! 'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10

```

```

match ip address 102
set interface Dialer2 null10
!
! ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
! (上記の関連するコマンド 'ip local policy route-map track-primary-if'
! を参照してください)。
!
! これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイアラ
! 2 (ATM DSL) が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
! ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
! これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
! 接続 (到達可能性) を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
match ip address 101
match interface Dialer2
!
! 上記のアクセス リスト 101 によって定義されている一致条件を満たし、
! ダイアラ 2 インターフェイスが 'UP' の状態で接続されている場合、
! このルート マップが使用されるように指定します。
!
! トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
! インターフェイスのダイアラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
! このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
match ip address 101
match interface Cellular0/3/0
!
! 上記のアクセス リスト 101 によって定義されている一致条件を満たし、
! ダイアラ 2 インターフェイスが 'UP' の状態で接続されている場合、
! このルート マップが使用されるように指定します。
!
! トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
! インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
! が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!
! スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
  event track 234 state any
  action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line con 0
  exec-timeout 0 0
  exec prompt timestamp
  stopbits 1
line aux 0
  stopbits 1
line 0/3/0
  exec-timeout 0 0
  script dialer gsmscript
  login
  modem InOut
  no exec
  transport input all
  transport output all
  rxspeed 236800
  txspeed 118000
line vty 0 4
  privilege level 15
  login local
  transport input telnet

```

```

line vty 5 15
  privilege level 15
  login local

transport input telnet
!
scheduler allocate 20000 1000
!
End

```

## 本社サイトのルータの設定

### 例 5-4 本社サイトのルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 20.20.248.253
ip dhcp excluded-address 20.20.248.225
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
!   DHCP の除外アドレス
!
ip dhcp pool 20
  network 20.20.248.224 255.255.255.224
  dns-server 20.20.248.254
  default-router 20.20.248.254
!
!   20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
  network 10.10.0.0 255.255.0.0
  default-router 10.10.0.254
!
!   10.10.0.0 ネットワーク上の VPN のホストの DHCP プール
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share

crypto isakmp key mykey address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set mytset ah-sha-hmac esp-3des
!
crypto dynamic-map gre_tunnel2 10

```

```

description IPsec tunnel to DSL at remote
set transform-set mytset
match address gre-tunnel2
!
crypto dynamic-map gre_tunnel21 10
description IPsec tunnel to Cellular at remote
set transform-set mytset
match address gre-tunnel21
!
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gre_tunnel2

crypto map mytunnelcrypto 20 ipsec-isakmp dynamic gre_tunnel21
!
!
!   リモート ブランチ ルータで、トンネルの mytunnelcrypto マップを ATM DSL インターフェイス
!   (Tunnel2) およびセルラー インターフェイス (Tunnel21) に定義します。
!
!
interface Tunnel2
description tunnel to remote DSL link 75.40.113.246
ip unnumbered Vlan20
tunnel source GigabitEthernet0/0
tunnel destination 75.40.113.246
!
!   リモート ブランチ ルータの ATM DSL インターフェイスへのトンネル。通常、これは
!   「アクティブなトンネル」です。
!
!
interface Tunnel21
description tunnel to remote Cellular link 166.138.186.119
ip unnumbered Vlan20
tunnel source GigabitEthernet0/0
tunnel destination 166.138.186.119
!
!   リモート ブランチ ルータのセルラー インターフェイスへのトンネル。リモート エンドでの DSL インター
!   フェイスを介した接続がダウンしない限り、通常、このトンネルはアクティブではありません。
!
!
interface GigabitEthernet0/0
description connected to cisco network, next hop:20.20.241.233
ip address 20.20.241.234 255.255.255.252
load-interval 30
duplex auto
speed auto
media-type rj45
negotiation auto
crypto map mytunnelcrypto
!
!   クリプト マップを適用する物理インターフェイス。上記のトンネルが
!   確立されるインターフェイス
!
interface GigabitEthernet0/1
no ip address
shutdown
!
interface FastEthernet0/1/0
switchport access vlan 10
spanning-tree portfast
!
!
!   VPN のホストが (10.10.0.0 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
switchport stacking-partner interface FastEthernet0/3/8
!
interface FastEthernet0/3/0

```

```

switchport access vlan 20
spanning-tree portfast
!
!
!   他のホストが (20.20 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
switchport mode trunk
switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
description private networking vlan
ip address 10.10.0.254 255.255.0.0
vlan-range dot1q 1 4095
exit-vlan-config
!
!
!   VPN のホストの VLAN (10.10.0.0 ネットワーク内)
!
interface Vlan20
description network:20.20.248.224/27
ip address 20.20.248.254 255.255.255.224
no ip route-cache cef
vlan-range dot1q 1 4095
exit-vlan-config
!
!
!   他のホストの VLAN (20.20 ネットワーク内)
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   デフォルト ルート
!
ip route 10.4.0.0 255.255.0.0 Tunnel2
!
!   DSL インターフェイスにリモート エンドポイントを持つトンネルを経由する、
!   ブランチ ルータ上のリモート VPN (10.4.0.0 ネットワーク) へのルート
!
ip route 10.4.0.0 255.255.0.0 Tunnel21 254
!
!   セルラー インターフェイスにリモート エンドポイントを持つトンネルを経由する、
!   ブランチ ルータ上のリモート VPN (10.4.0.0 ネットワーク) へのルート。このルートの管理距離は
!   高く設定されています。
!
ip access-list extended gre-tunnel2
permit gre host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
ip access-list extended gre-tunnel21
permit gre host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。
!
control-plane
!
line con 0
exec-timeout 0 0
login local
stopbits 1
line aux 0
stopbits 1

```

```

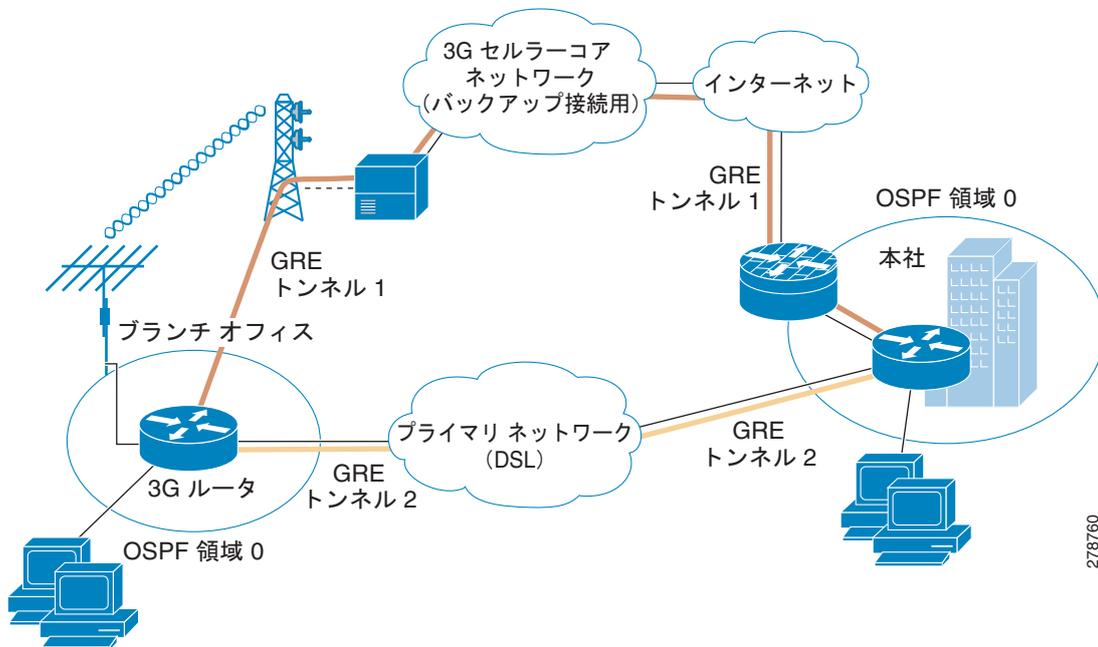
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet
!
scheduler allocate 20000 1000
!
end

```

## GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入

この導入では、パブリック ネットワークを介したブランチ オフィスのルータのホストと本社サイトのホストの間でセキュアな通信を行うために、GRE トンネルと IPSec をブランチ オフィスで使用して、プライマリ リンクとして DSL インターフェイスを使用し、バックアップ リンクとしてセルラー インターフェイスを使用します。また、VPN ネットワーク (10.4.0.0 および 10.10.0.0 ネットワーク) で OSPF を使用し、OSPF でサポートされたルーティングを行えるようにもします。この導入により、インターネット上のホストとのノンセキュア (非 IPSec) 通信を行えるようになります。詳細については、「[Configuring a GRE Tunnel over IPsec with OSPF](#)」を参照してください。

図 5-3 GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入



278760

## ブランチ オフィス ルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPSec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

次の設定では、信頼できるオブジェクト トラッキングを使用した IP SLA が使用されます。この設定は任意です。

### 例 5-5 ブランチ オフィス ルータの設定

```

!
hostname branch-router
!
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
!   このアドレスは、VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 上の
!   接続済みホスト用デフォルト ゲートウェイ アドレスとして使用されます。
!
ip dhcp pool gsmppool
  network 10.4.0.0 255.255.0.0
  dns-server 66.209.10.201 66.102.163.231
  default-router 10.4.0.254
!
!   VLAN 104 のファスト イーサネット ポート 0/1/0 から 0/3/0 に接続されている
!   ホストの DHCP プール
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   operation 1 を使用して、到達可能性のトラッキングに使用されるトラッキング対象のオブジェクト番号 234
!   を設定します。オブジェクトは、到達可能性条件が満たされる場合は 'UP' です。
!
!   これは、(プライマリ リンクとして使用される) ATM DSL インターフェイスを介して ping パケットを送信し、
!   応答を監視するために使用されます。また、応答がない場合に (セルラーへの) スイッチオーバーが
!   必要かどうかを判別するために使用されます。
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
!
!   (priority 1 を設定して) IKE ポリシーを定義し、IKE ネゴシエーション中に 3DES を指定します。また、
!   事前定義されたキーを使用して事前共有認証を指定します。ライフタイムの値 (1 日に 86,400 秒に設定)、
!   グループ (768 ビット ディフィー・ヘルマン鍵共有に設定)、
!   およびハッシュ (SHA-1 に設定) は、デフォルト値に設定されます。
!

```

```

crypto isakmp key mykey address 20.20.241.234
!
!   セキュリティ アソシエーションの設定に使用されるキー (mykey) およびゲートウェイの
!   IP アドレス (IPsec peer) を定義します。
!
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   セキュリティ プロトコル、アルゴリズム、および他の設定の許容可能な組み合わせである
!   トランスフォーム セット (mytransformset) を定義して、IPsec で保護されている
!   トラフィックを適用します。
!
crypto map mytunnelcrypto 10 ipsec-isakmp
set peer 20.20.241.234
set transform-set mytransformset
match address gre-traffic
!
!   クリプト マップの mytunnelcrypto を定義します
!
!   クリプト マップは (match address <access-list> コマンドを使用して) 保護対象のトラフィック、
!   使用するピア エンド ポイント、および使用するトランスフォーム セット (以前に定義した
!   mytransformset) を指定します。
!
!
interface Tunnel1
ip unnumbered Vlan104
ip mtu 1400
tunnel source Dialer2
tunnel destination 20.20.241.234
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。ATM DSL (プライマリ)
!   インターフェイスに関連付けられたトンネル。このトンネルは、通常 'UP' の状態です。リモート トンネルの
!   エンドポイント (20.20.241.234) は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンド
!   ポイントは、ATM DSL リンクによって取得されるアドレスです。
!
interface Tunnel2
ip ospf demand-circuit
ip unnumbered Vlan104
ip mtu 1400
tunnel source Cellular0/3/0
tunnel destination 20.20.241.234
!
!   'ip ospf demand-circuit' オプション コマンドは、OSPF Hello パケットを抑制します。これは、
!   定期的に、セルラー無線レベルの接続が不必要に ('休止' 状態から) 「アクティブ」 状態
!   にならないように保つのに役立ちます。
!
!   宛先 10.10.0.0 のネットワークへのトラフィックの GRE トンネル。セルラー (セカンダリ) インターフェイス
!   に関連付けられたトンネル。このトンネルは、通常 'Down' の状態です。リモート トンネルの
!   エンドポイント (20.20.241.234) は、リモート VPN ゲートウェイにあります。ローカル トンネルのエンド
!   ポイントは、セルラー リンクによって取得されるアドレスです。このトンネルは、
!   セルラー インターフェイスでスイッチオーバーが行われると 'UP' になります。
!
interface Loopback1
ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
no ip address
shutdown
!
interface GigabitEthernet0/1
no ip address
shutdown
!
interface FastEthernet0/1/0

```

## GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入

```

switchport access vlan 104
!
interface FastEthernet0/1/1
switchport access vlan 104
!
interface FastEthernet0/1/2
switchport access vlan 104
!
interface FastEthernet0/1/3
switchport access vlan 104
!
! DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
no ip address
ip virtual-reassembly
load-interval 30
no atm ilmi-keepalive
dsl operating-mode auto
!
! プライマリ インターフェイスとして使用される ATM (DSL) 物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
ip nat outside
ip virtual-reassembly
no snmp trap link-status
pvc 0/35
pppoe-client dial-pool-number 2
!
!
! プライマリ接続として PVC に使用する ATM サブ インターフェイス。このインターフェイスでは
! NAT (外部) が使用されます。
!
! 'pppoe-client dial-pool-number 2' は PPP over Ethernet (PPOE) クライアントを設定し、
! 使用するダイヤラ プール 2 を指定します。このインターフェイスは、以下で定義されている 'interface
! Dialer 2' に関連付けられます。
!
interface Cellular0/3/0
ip address negotiated
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip ospf demand-circuit
dialer in-band
dialer idle-timeout 0
dialer string gsmscript
dialer-group 1
async mode interactive
ppp chap hostname crlaswlech@wwan.ccs
ppp chap password 0 frludi3gIa
ppp ipcp dns request
crypto map mytunnelcrypto
!
!
! 'ip ospf demand-circuit' オプション コマンドは、OSPF Hello パケットを抑制します。これは、定期的
! に、セルラー無線レベルの接続が不必要に (「休止」状態から)「アクティブ」状態に
! ならないように保つのに役立ちます。
!
! 上記で定義したクリプト マップ mytunnelcrypto を、このバックアップ インターフェイスに適用します。
!
! 'dialer-group 1' は group number 1 を定義します。
! この設定では、これは以下に定義されている 'dialer-list 1 ...' コマンドに関連付けられます。これは、
! ダイヤル アウトをトリガーし、PPP を確立した後にインターフェイス をオンラインにする
! 「対象のトラフィック」を定義します。通常、このインターフェイスはスタンバイ状態のままになることに注意して
! ください。このため、対象のトラフィックではダイヤル アウトはトリガーされません。トラフィックはすでに

```

```

!   プライマリ (ATM DSL) インターフェイスを介してフローしています。
!
!   NAT のインターフェイスを外部で定義します。
!
!
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
!
!   NAT (内部インターフェイス) を使用して、ファスト イーサネット ポート 0/1/0 から 0/1/3 に
!   接続されたホストに VLAN 104 を定義します。
!
!   NAT/PAT は、トンネルを介してピア ゲートウェイの 20.20.0.0 ネットワークに送信されるように
!   意図されていないトラフィックに使用されます。
!
interface Dialer2
  ip address negotiated
  ip nat outside
  encapsulation ppp
  load-interval 30
  dialer pool 2
  dialer-group 2
  ppp authentication chap callin
  ppp chap hostname cisco@cisco.com
  ppp chap password 0 cisco123
  ppp pap sent-username cisco@cisco.com password 0 cisco123
  ppp ipcp dns request
  crypto map mytunnelcrypto
!
!   'dialer pool 2' コマンドはこのダイヤラ インターフェイスを ATM サブインターフェイス
!   atm0/0/0.1 に関連付けます。'dialer-group 2' は group number 2 を定義します。この設定では、
!   これは以下で指定されている 'dialer-list 2 ...' コマンドに関連付けられます。これは、
!   PPP を確立した後に、ダイヤラ アウトをトリガーし、インターフェイスをオンラインにする
!   「対象のトラフィック」を定義します。
!
!   NAT のインターフェイスを外部で定義します。
!
!   上記で定義したクリプト マップ mytunnelcrypto をこのプライマリ インターフェイスに適用します。
!
router ospf 11
  log-adjacency-changes
  network 10.4.0.0 0.0.0.255 area 0
!
!   VPN ネットワーク 10.4.0.0 (Tunnel1/Tunnel2 が含まれます) は、OSPF エリア 0 に含まれています
!
!   OSP Hello は、これらのトンネルを介してブランチ ルータに送信されます
!
ip local policy route-map track-primary-if
!
!   ルート マップの 'track-primary-if' で定義されているように、IP ルート ポリシーを指定します
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   上記で定義したトラッキング オブジェクト (234) を指定し、ダイヤラ 2 (ATM DSL)
!   を介してデフォルト ルートを定義します。
!
!   ルートはトラッキング対象オブジェクト (234) が 'UP' である場合のみインストールされます。
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   管理距離を 254 (ダイヤラ 2 のインターフェイスより高い) に設定して、
!   セルラー インターフェイスを介してデフォルト ルートを定義します。通常このインターフェイスは

```

## GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入

```

!   バックアップ インターフェイスとして想定されているからです。
!
ip http server
ip http authentication local
no ip http secure-server
ip http timeout-policy idle 5 life 86400 requests 10000

ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   セルラー インターフェイスを介して、外部 NAT トラフィックの条件としてルート マップ nat2cell を定義し
!   ます (以下で指定)。'overload' オプションを使用すると、PAT が使用されるようになります。
!
!   ルート マップ nat2cell で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   上記と同様に、ダイヤラ 2 インターフェイス (ATM DSL) を使用して、
!   ルート マップ nat2cell を定義します (以下で指定)。'overload' オプションを使用すると、
!   PAT が使用されるようになります。
!
!   ルート マップ nat2dsl で定義されている条件が満たされる場合に、このコマンドが使用されます。
!
ip access-list extended gre-traffic
  permit gre host 75.40.113.246 host 20.20.241.234
  permit gre host 166.138.186.119 host 20.20.241.234
!
!   GRE トンネルを経由して IPSec トラフィックを保護するための 'gre-traffic' アクセス リスト
!
!   これは DSL/セルラー インターフェイス (どちらかアクティブな方) と、リモート ゲートウェイ上の
!   IPsec ピア (20.20.241.234) を介した GRE トンネリングされた
!   トラフィックのみを保護します。
!
ip sla 1
  icmp-echo 209.131.36.158 source-interface Dialer2
  timeout 1000
  frequency 2

ip sla schedule 1 life forever start-time now
!
!   2 秒間隔 (frequency 2) で、ping への応答に 1000 ミリ秒の待機 (タイムアウト 1000) を設定し、
!   ソース インターフェイスとしてダイヤラ 2 (ATM DSL) を使用して、
!   IP アドレス 209.131.36.158 に ping を送信するための
!   サービス レベル契約 (SLA) を定義します。
!
!   定義された SLA を開始し、これを継続的に実行します。
!
access-list 1 permit any
!
!   以下の 'dialer-list 1 protocol ip list 1' コマンドに関連付けられています
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   ルート マップ nat2dsl と nat2cell の下に定義されているように、適切な発信インターフェイスを
!   決定するために、トラフィックが一致するように指定します
!   (ネットワーク 10.4.0.0 のソース アドレスと一致)。
!
access-list 102 permit icmp any host 209.131.36.158
!
!   このインターフェイスがアクティブな場合にのみ、ICMP の ping が ATM DSL インターフェイスを介して
!   送信されるように、ルート マップ 'track-primary-interface' のトラフィックを指定します。
!
!   この特定のアドレスは、ATM DSL インターフェイス (プライマリ リンク) を介して定期的に ping される
!   アドレスであるため、リンク /PPP レベル以外のネットワーク障害も検出される場合があり、
!   セルラー (セカンダリ) インターフェイスへのスイッチオーバーが

```

```

!   まだ実行される可能性があります。
!
!   ping されるアドレスが信頼でき、ping に応答することを確認します。
!
dialer-list 1 protocol ip list 1
!
!   セルラー インターフェイスがダイヤル アウトする原因となる 'interesting traffic' を指定します。
!   それによって、access-list 1 が (上記で定義されたこのコマンドの一部として) さらに指定されます。
!
dialer-list 2 protocol ip permit
!
!   ATM DSL インターフェイスが (ダイヤラ 2 インターフェイスの一部として)
!   ダイヤル アウトするようにする 'interesting traffic' を指定します。
!
!
route-map track-primary-if permit 10
  match ip address 102
  set interface Dialer2 null0
!
!   ローカル ルーティング用にポリシー条件として使用されるルート マップを指定します
!   (上記の関連するコマンド 'ip local policy route-map track-primary-if'
!   を参照してください)。
!
!   これが宛先 209.131.36.158 の ping パケットで、インターフェイス ダイヤラ
!   2 (ATM DSL) が 'UP' の状態で接続されている場合、ping パケットを送信します。この ping パケットは、
!   ATM DSL インターフェイスを介してのみ送信され、セルラー インターフェイスを介しては送信されません。
!   これは、接続が失敗したときにスイッチオーバーを実行するために、ATM DSL インターフェイスを介して
!   接続 (到達可能性) を定期的にモニタリングするためです。
!
route-map nat2dsl permit 10
  match ip address 101
  match interface Dialer2
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイスのダイヤラ 2 が 'UP' の状態で DSL ネットワークに接続されている場合、
!   このルート マップが 'ip nat inside source nat2dsl ...' コマンドによって使用されます。
!
route-map nat2cell permit 10
  match ip address 101
  match interface Cellular0/3/0
!
!   上記のアクセス リスト 101 によって定義されている一致条件を満たし、
!   ダイヤラ 2 インターフェイスが 'UP' の状態で接続されている場合、
!   このルート マップが使用されるように指定します。
!
!   トラフィックのソースが 10.4.0.0 ネットワークからのものであり、
!   インターフェイス セルラーが 'UP' の状態でセルラー ネットワークに接続されている場合、このルート マップ
!   が 'ip nat inside source nat2cell ...' コマンドによって使用されます。
!
!   スイッチオーバーで、プライマリおよびバックアップ インターフェイスから NAT エントリを削除します。
event manager applet pri_back
  event track 234 state any
  action 2.0 cli command "clear ip nat trans forced"
!
control-plane
!
line con 0
  exec-timeout 0 0
  exec prompt timestamp
  stopbits 1

```

```

line aux 0
  stopbits 1
line 0/3/0
  exec-timeout 0 0
  script dialer gsmscript
  login
  modem InOut
  no exec
  transport input all
  transport output all
  rxspeed 236800
  txspeed 118000
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet
!
scheduler allocate 20000 1000
!
End

```

## 本社サイトのルータの設定

### 例 5-6 本社サイトのルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
hostname gateway-router
!
ip cef
!
ip dhcp excluded-address 20.20.248.254
ip dhcp excluded-address 10.10.0.254
ip dhcp excluded-address 10.10.0.1
!
!   DHCP の除外アドレス
!
ip dhcp pool 20
  network 20.20.248.224 255.255.255.224
  dns-server 20.20.248.254
  default-router 20.20.248.254
!
!   20.20 ネットワーク上のホストの DHCP プール
!
ip dhcp pool 10
  network 10.10.0.0 255.255.0.0
  default-router 10.10.0.254
!
!   10.10.0.0 ネットワーク上の VPN のホストの DHCP プール

```

```
!  
!  
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1  
!  
crypto isakmp policy 1  
  encr 3des  
  authentication pre-share  
  
crypto isakmp key mykey address 0.0.0.0 0.0.0.0  
!  
!  
crypto ipsec transform-set mytset ah-sha-hmac esp-3des  
!  
crypto dynamic-map gre_tunnel2 10  
  description IPsec tunnel to DSL at remote  
  set transform-set mytset  
  match address gre-tunnel2  
!  
crypto dynamic-map gre_tunnel21 10  
  description IPsec tunnel to Cellular at remote  
  set transform-set mytset  
  match address gre-tunnel21  
!  
crypto map mytunnelcrypto 10 ipsec-isakmp dynamic gre_tunnel2  
  
crypto map mytunnelcrypto 20 ipsec-isakmp dynamic gre_tunnel21  
!  
! リモート ブランチ ルータで、トンネルの mytunnelcrypto マップを ATM DSL インターフェイス  
! (Tunnel2) およびセルラー インターフェイス (Tunnel21) に定義します。  
!  
!  
interface Tunnel2  
  description tunnel to remote DSL link 75.40.113.246  
  ip unnumbered Vlan10  
  ip mtu 1400  
  tunnel source GigabitEthernet0/0  
  tunnel destination 75.40.113.246  
!  
! リモート ブランチ ルータの ATM DSL インターフェイスへのトンネル。通常、これは  
! 「アクティブなトンネル」です。  
!  
interface Tunnel21  
  description tunnel to remote Cellular link 166.138.186.119  
  ip unnumbered Vlan10  
  ip mtu 1400  
  tunnel source GigabitEthernet0/0  
  tunnel destination 166.138.186.119  
!  
! リモート ブランチ ルータのセルラー インターフェイスへのトンネル。リモート エンドでの DSL インター  
! フェイスを介した接続がダウンしない限り、通常、このトンネルはアクティブではありません。  
!  
interface GigabitEthernet0/0  
  description connected to cisco network, next hop:20.20.241.233  
  ip address 20.20.241.234 255.255.255.252  
  load-interval 30  
  crypto map mytunnelcrypto  
!  
! クリプト マップを適用する物理インターフェイス。上記のトンネルが  
! 確立されるインターフェイス。  
!  
interface GigabitEthernet0/1  
  no ip address  
  shutdown  
!
```

## GRE トンネル、IPSec、および OSPF ルーティングを使用したプライマリおよびバックアップの導入

```

interface FastEthernet0/1/0
  switchport access vlan 10
  spanning-tree portfast
!
!   VPN のホストが (10.10.0.0 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/1/8
  switchport stacking-partner interface FastEthernet0/3/8
!
interface FastEthernet0/3/0
  switchport access vlan 20
  spanning-tree portfast
!
!   他のホストが (20.20 ネットワークで) 接続されるファスト イーサネット ポート。
!
interface FastEthernet0/3/8
  switchport mode trunk
  switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
  description private networking vlan
  ip address 10.10.0.254 255.255.0.0
  no ip route-cache cef
  vlan-range dot1q 1 4095
  exit-vlan-config
!
!   VPN のホストの VLAN (10.10.0.0 ネットワーク内)。
!
interface Vlan20
  description network:20.20.248.224/27
  ip address 20.20.248.254 255.255.255.224
  no ip route-cache cef
  vlan-range dot1q 1 4095
  exit-vlan-config
!
!   他のホストの VLAN (20.20 ネットワーク内)
!
router ospf 10
  log-adjacency-changes
  network 10.10.0.0 0.0.0.255 area 0
!
!   VPN ネットワーク 10.10.0.0 (Tunnel2/Tunnel21 が含まれています) は、OSPF エリア 0 に含まれています
!
!   OSP Hello は、これらのトンネルを介してブランチ ルータに送信されます
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   GigabitEthernet0/0 インターフェイスのネクスト ホップを介するデフォルト ルート。
!
ip dns server
!
ip access-list extended gre-tunnel2
  permit gre host 20.20.241.234 host 75.40.113.246
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドで DSL インターフェイスに送信されるトラフィックです。
!
ip access-list extended gre-tunnel21
  permit gre host 20.20.241.234 host 166.138.186.119
!
!   IPsec で保護されるトラフィックを定義するアクセス リスト。これは、
!   リモート エンドでセルラー インターフェイスに送信されるトラフィックです。

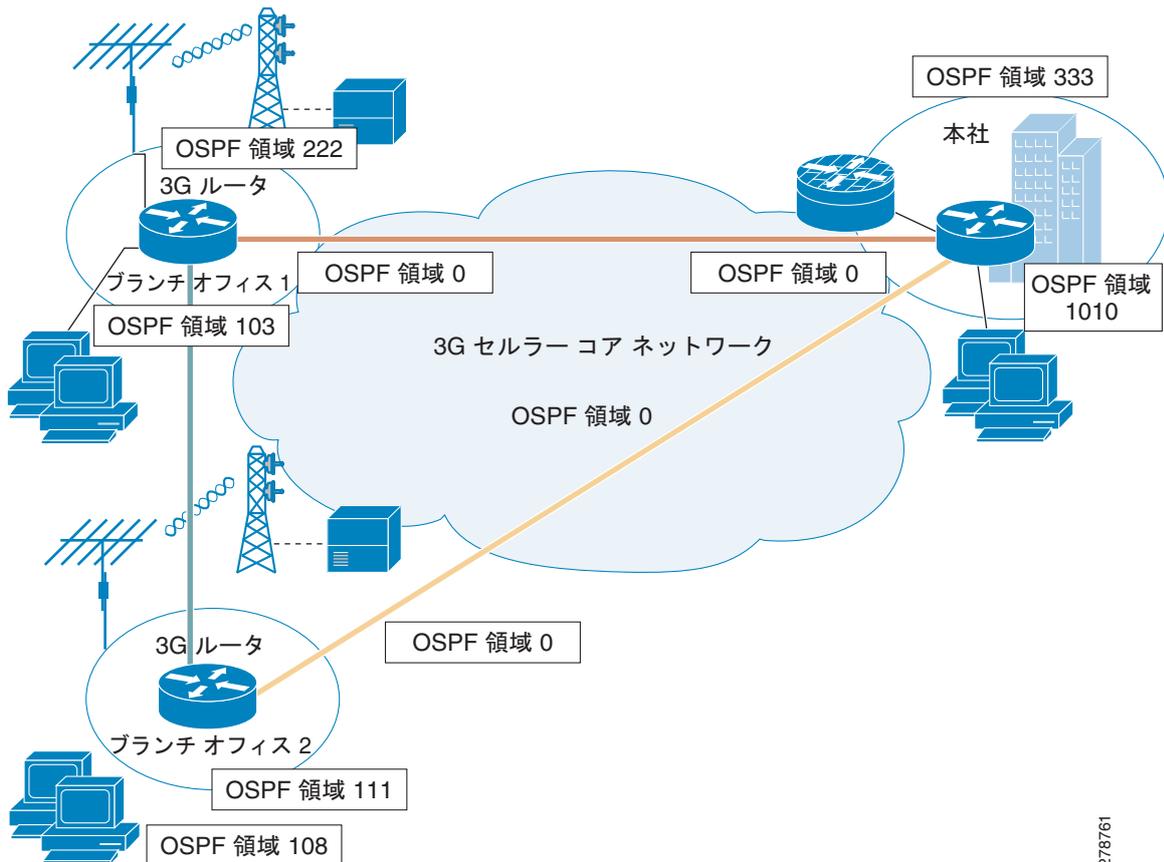
```

```
!  
control-plane  
!  
line con 0  
  exec-timeout 0 0  
  login local  
  stopbits 1  
line aux 0  
  stopbits 1  
line vty 0 4  
  privilege level 15  
  login local  
  transport input telnet  
line vty 5 15  
  privilege level 15  
  login local  
  transport input telnet  
!  
scheduler allocate 20000 1000  
!  
End
```

## IPsec および OSPF を使用した DMVPN の導入

この導入では、ルーティングプロトコルの OSPF とパブリック ネットワークを使用して、ブランチ オフィスのルータのホストと、本社サイトのホストの間でセキュアな通信を行うために、DMVPN (GRE トンネル) と IPsec を使用し、プライマリ リンクとしてセルラー インターフェイスを使用します。DMVPN の詳細については、「[Dynamic Multipoint VPN \(DMVPN\)](#)」を参照してください。

図 5-4 IPsec および OSPF 使用する DMVPN を使用した初期導入



278761

## ブランチ 1 のオフィス ルータの設定

### 例 5-7 ブランチ 1 のオフィス ルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPSec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!  
hostname DMVPN_Spoke_1  
!  
Ip cef  
!  
crypto isakmp policy 10  
  hash md5  
  authentication pre-share  
!  
!  
フェーズ 1 ネゴネーションの ISAKMP ポリシー  
!  
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0  
!  
!  
ハブの事前共有キー、およびリモート DMVPN スポーク  
!  
!  
crypto ipsec transform-set strong esp-3des esp-md5-hmac  
!  
!  
実際のデータ暗号化 / 整合性のための IPsec (フェーズ 2) ポリシー  
!  
!  
crypto ipsec profile cisco  
  set security-association lifetime seconds 86400  
  set transform-set strong  
!  
!  
IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル  
!  
!  
ip dhcp excluded-address 10.3.0.254  
!  
ip dhcp pool cdmapi  
  network 10.3.0.0 255.255.0.0  
  dns-server 68.28.58.11  
  default-router 10.3.0.254  
!  
chat-script cdmal "" "atdt#777" TIMEOUT 180 "CONNECT"  
!  
username cisco privilege 15 secret 5 $1$c/50$W4sr3BFW3AhIB9BRXjy84/  
!  
interface Loopback0  
  ip address 2.2.2.1 255.255.255.0  
!  
interface Tunnel0  
  ip address 192.168.10.3 255.255.255.0  
  no ip redirects  
  ip mtu 1440  
  ip nhrp map multicast dynamic  
  ip nhrp map multicast 20.20.241.234
```

```

ip nhrp map 192.168.10.1 20.20.241.234
ip nhrp network-id 1
ip nhrp nhs 192.168.10.1
ip nhrp registration no-unique
ip nhrp cache non-authoritative
ip ospf network broadcast
tunnel source dialer 1
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile Cisco
!
! 動的に作成されたすべての GRE トンネルに割り当てられた GRE トンネル テンプレート。
!
!
interface GigabitEthernet0/0
no ip address
shut down
!
interface GigabitEthernet0/1
no ip address
shutdown
!
interface FastEthernet0/2/0
switchport access vlan 103
!
interface FastEthernet0/2/1
switchport access vlan 103
!
interface FastEthernet0/2/2
switchport access vlan 103
!
interface FastEthernet0/2/3
switchport access vlan 103
!
!
! 次のセルラー設定は永続的ダイヤラ用です。これは、常にセルラー インターフェイスを
! 起動状態に保ち、IP アドレスを取得します。ダイヤラ プールおよび dialer pool-member コマンドは、
! ダイヤラ インターフェイスとセルラー インターフェイスを関連付けます。
!
!
interface Cellular0/1/0
no ip address
encapsulation ppp
dialer in-band
dialer pool-member 1
!
interface Dialer1
ip address negotiated
ip nat outside
encapsulation ppp
dialer pool 1
dialer string cdma1
dialer persistent
ppp chap hostname isp-provided-hostname
ppp chap password 0 isp-provided-password
ppp ipcp dns request
!
interface Vlan1
no ip address
!
interface Vlan103
ip address 10.3.0.254 255.255.0.0
ip nat inside

```

```
ip virtual-reassembly
!
router ospf 90
log-adjacency-changes
network 2.2.2.0 0.0.0.255 area 222
network 10.3.0.0 0.0.255.255 area 103
network 192.168.10.0 0.0.0.255 area 0
!
ip route 20.20.241.234 255.255.255.255 dialer 1
!
!
control-plane
!
line con 0
exec-timeout 0 0
line aux 0
line 0/1/0
exec-timeout 0 0
script dialer cdma1
login
modem InOut
no exec
transport input all
transport output all
rxspeed 3100000
txspeed 1800000
line vty 0 4
privilege level 15
no login
transport input telnet
line vty 5 15
privilege level 15
login local
transport input telnet
!
scheduler allocate 20000 1000

!
webvpn cef
!
end
```

## ブランチ 2 のオフィス ルータの設定

### 例 5-8 ブランチ 2 のオフィス ルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPSec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
!
hostname DMVPN_Spoke_2
!
!
crypto isakmp policy 10
```

```

hash md5
authentication pre-share
!
! フェーズ 1 ネゴシエーションの ISAKMP ポリシー
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
! すべてのリモート DMVPN スポークの事前共有キー
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
! 実際のデータ暗号化 / 整合性のための IPsec (フェーズ 2) ポリシー
!
crypto ipsec profile cisco
  set security-association lifetime seconds 86400
  set transform-set strong
!
! IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル
!
ip cef
!
ip dhcp excluded-address 10.8.0.1
ip dhcp excluded-address 10.8.0.254
!
ip dhcp pool cdmapi
  network 10.8.0.0 255.255.0.0
  default-router 10.8.0.254
!
!
chat-script cdma2 "" "atdt#777" TIMEOUT 180 "CONNECT"
!
username cisco privilege 15 secret 5 $1$YNWp$10LVYb0qkTnZFmkgcCK1L0
!
interface Loopback1
  ip address 1.1.1.1 255.255.255.0
!
interface Tunnel0
  ip address 192.168.10.2 255.255.255.0
  no ip redirects
  ip mtu 1440
  ip nhrp map multicast dynamic
  ip nhrp map multicast 20.20.241.234
  ip nhrp map 192.168.10.1 20.20.241.234
  ip nhrp network-id 1
  ip nhrp nhs 192.168.10.1
  ip nhrp registration no-unique
  ip nhrp cache non-authoritative
  ip ospf network broadcast
  tunnel source dialer 1
  tunnel mode gre multipoint
  tunnel key 0
  tunnel protection ipsec profile Cisco
!
! 動的に作成されたすべての GRE トンネルに割り当てられた GRE トンネル テンプレート。
!
interface FastEthernet0/0
  no ip address
  shutdown
!

```

```
interface FastEthernet0/1
 ip address dhcp
 shutdown
!
interface FastEthernet0/3/0
 switchport access vlan 108
!
interface FastEthernet0/3/1
!
interface FastEthernet0/3/2
 switchport access vlan 108
!
interface FastEthernet0/3/3
 switchport access vlan 108
!
!  
! 次のセルラー設定は永続的ダイヤラ用です。これは、常にセルラー インターフェイスを起動状態に保ち、
! IP アドレスを取得します。ダイヤラ プールおよび dialer pool-member コマンドは、
! ダイヤラ インターフェイスとセルラー インターフェイスを関連付けます。
!  
!  
interface Cellular0/1/0
 no ip address
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
!
interface Dialer1
 ip address negotiated
 ip nat outside
 encapsulation ppp
 dialer pool 1
 dialer string cdma2
 dialer persistent
 ppp chap hostname isp-provided-hostname
 ppp chap password 0 isp-provided-password
 ppp ipcp dns request
!
interface Vlan108
 description used as default gateway address for DHCP clients
 ip address 10.8.0.254 255.255.0.0
 ip virtual-reassembly
!
router ospf 90
 log-adjacency-changes
 network 1.1.1.0 0.0.0.255 area 111
 network 10.8.0.0 0.0.0.255 area 108
 network 192.168.10.0 0.0.0.255 area 0
!
ip route 20.20.241.234 255.255.255.255 dialer 1
!
control-plane
!
line con 0
 exec-timeout 0 0
line aux 0
line 0/1/0
 exec-timeout 0 0
 script dialer cdma2
 login
 modem InOut
 no exec
 transport input all
```

```

transport output all
autoselect during-login
autoselect ppp
rxspeed 3100000
txspeed 1800000
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end

```

## 本社サイトのルータの設定

### 例 5-9 本社サイトのルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
hostname DMVPN_Hub
!
ip cef
!
ip dhcp pool 20
network 20.20.248.224 255.255.255.224
dns-server 20.20.248.254
default-router 20.20.248.254
!
ip dhcp pool 10
network 10.10.0.0 255.255.0.0
default-router 10.10.0.254
!
ip dhcp pool 192
network 192.168.1.0 255.255.255.0
dns-server 192.168.1.254
default-router 192.168.1.254
!
!
crypto isakmp policy 10
hash md5
authentication pre-share
!
! フェーズ 1 ネゴシエーションの ISAKMP ポリシー
!
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

```

```
!  
!   すべてのリモート DMVPN スポークの事前共有キー  
!  
!  
crypto ipsec transform-set strong esp-3des esp-md5-hmac  
!  
!   実際のデータ暗号化 / 整合性のための IPsec (フェーズ 2) ポリシー  
!  
!  
crypto ipsec profile cisco  
  set security-association lifetime seconds 86400  
  set transform-set strong  
!  
!   IPsec を介した GRE トンネルに動的に適用される IPsec プロファイル  
!  
!  
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e519DCU1  
!  
interface Loopback33  
  ip address 3.3.3.3 255.255.255.0  
!  
interface Tunnel0  
  ip address 192.168.10.1 255.255.255.0  
  no ip redirects  
  ip mtu 1440  
  ip nhrp map multicast dynamic  
  ip nhrp network-id 1  
  ip nhrp cache non-authoritative  
  ip ospf network broadcast  
  tunnel source GigabitEthernet0/0  
  tunnel mode gre multipoint  
  tunnel key 0  
  tunnel protection ipsec profile cisco  
!  
!  
!   動的に作成されたすべての GRE トンネルに割り当てられた  
!   GRE トンネル テンプレート  
!  
interface GigabitEthernet0/0  
  description connected to cisco network, next hop:20.20.241.233  
  ip address 20.20.241.234 255.255.255.252  
!  
interface GigabitEthernet0/1  
  no ip address  
  shutdown  
!  
interface FastEthernet0/1/0  
  switchport access vlan 10  
  no cdp enable  
  spanning-tree portfast  
!  
!  
interface FastEthernet0/1/8  
  switchport stacking-partner interface FastEthernet0/3/8  
  no cdp enable  
!  
interface FastEthernet0/3/0  
  switchport access vlan 20  
  no cdp enable  
  spanning-tree portfast  
!  
interface FastEthernet0/3/8  
  switchport mode trunk  
  switchport stacking-partner interface FastEthernet0/1/8
```

## ■ IPsec および OSPF を使用した DMVPN の導入

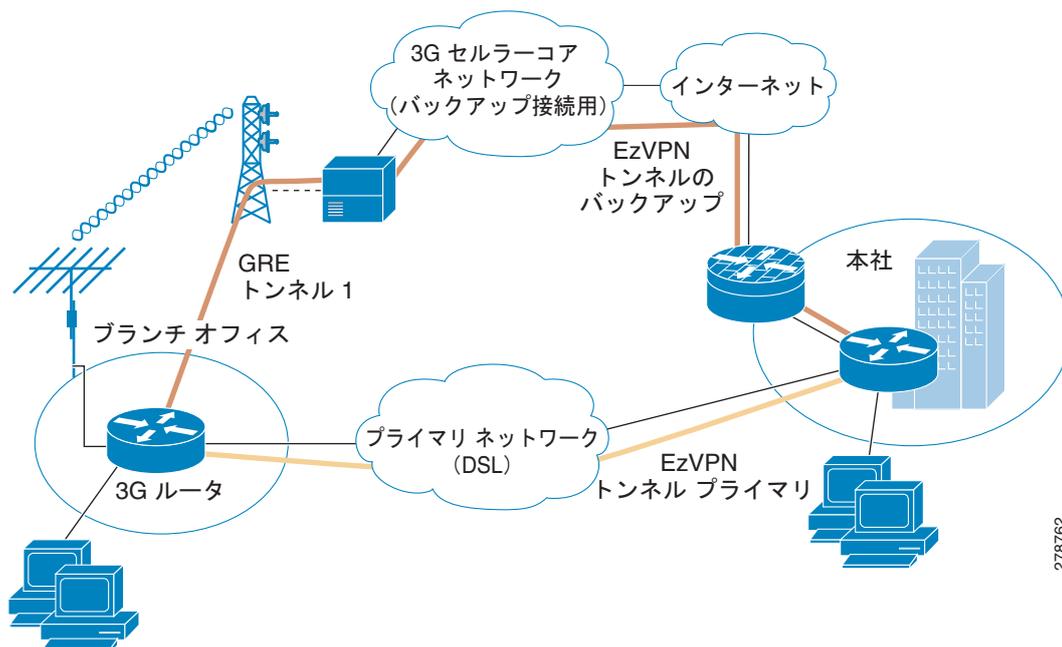
```
no cdp enable
!
interface Vlan10
description private networking vlan
ip address 10.10.0.254 255.255.0.0
no ip route-cache cef
!
interface Vlan20
description network:20.20.248.224,mask:/27,last host:20.20.248.254
ip address 20.20.248.254 255.255.255.224
no ip route-cache cef
!
router ospf 90
log-adjacency-changes
network 3.3.3.0 0.0.0.255 area 333
network 10.10.0.0 0.0.255.255 area 1010
network 192.168.10.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
control-plane
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
privilege level 15
transport input telnet
line vty 5 15
privilege level 15
transport input telnet
!
scheduler allocate 20000 1000

!
webvpn cef
!
end
```

## プライマリ リンクおよびバックアップリンクを使用した EzVPN 導入

EzVPN は、特に、多数のブランチを持つ本社ブランチでの導入に対して導入と拡張を簡単に行えるように設計されています。この導入では、プライマリ リンクとして DSL インターフェイスを使用し、バックアップリンクとしてセルラーリンクを使用します。EzVPN の詳細については、「[Cisco Easy VPN](#)」を参照してください。

図 5-5 プライマリおよびバックアップを使用した EzVPN の導入



## EzVPN クライアント（ブランチ ルータ）の設定

### 例 5-10 EzVPN クライアント（ブランチ ルータ）の設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```

!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsm pool
  network 10.4.0.0 255.255.0.0
  dns-server 66.209.10.201 66.102.163.231
  default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
username cisco123@cisco.com password 0 lab
username cisco password 0 lab
username sachin@cisco.com password 0 lab
!
!   EzVPN クライアント認証用のローカル ユーザ名およびパスワード。
!
!
track 234 rtr 1 reachability
!
crypto ipsec client ezvpn hw-client-pri
  connect auto
  group hw-client-group key cisco123
  backup hw-client track 234
  mode network-extension
  peer 128.107.248.243
  username cisco123@cisco.com password lab
  xauth userid mode local
!
!   プライマリ WAN インターフェイスの EzVPN クライアントの設定。バックアップ WAN の使用中に、
!   ファイルオーバーにトラック 234 を使用してバックアップします。
!
!
crypto ipsec client ezvpn hw-client
  connect auto
  group hw-client-group key cisco123
  mode network-extension
  peer 128.107.248.243
  username sachin@cisco.com password lab
  xauth userid mode local
!
!   バックアップ WAN インターフェイスの EzVPN クライアントの設定
!
!

```

```
interface Loopback1
 ip address 1.1.1.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 104
!
interface FastEthernet0/1/1
 switchport access vlan 104
!
interface FastEthernet0/1/2
 switchport access vlan 104
!
interface FastEthernet0/1/3
 switchport access vlan 104
!
! DHCP クライアント ホストによって使用されるファスト イーサネット ポート。
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
! プライマリ インターフェイスとして使用される ATM (DSL) 物理インターフェイス
!
interface ATM0/0/0.1 point-to-point
 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
!
interface Cellular0/1/0
 no ip address
 ip nat outside
 encapsulation ppp
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async mode interactive
 ppp ipcp dns request
!
interface Vlan104
 description ip address used as default gateway address for DHCP clients
 ip address 10.13.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
 crypto ipsec client ezvpn hw-client-pri inside
 crypto ipsec client ezvpn hw-client inside
!
! EzVPN 暗号化のための内部インターフェイスの一部となるように、ファスト イーサネット ポート
! 0/1/0 から 0/1/3 に接続されたホストに VLAN 104 を定義します。
!
interface Dialer1
 ip address negotiated
```

## ■ プライマリ リンクおよびバックアップリンクを使用した EzVPN 導入

```

ip nat outside
encapsulation ppp
dialer pool 1
dialer string gsmscript
dialer persistent
dialer-group 1
ppp chap hostname cisco@cisco.com
ppp chap password 0 cisco123
ppp ipcp dns request
crypto ipsec client ezvpn hw-client
!
!   セルラー インターフェイスと関連付ける外部ダイヤラ インターフェイス
!
!   このバックアップ インターフェイスにおいて、上記で定義した暗号化 IPsec クライアント ezvpn hw-client。
!   これにより、これが EzVPN 暗号化の外部インターフェイスであることが確認されます
!
interface Dialer2
ip address negotiated
ip nat outside
encapsulation ppp
dialer pool 2
dialer-group 2
ppp chap hostname Cisco@cisco.com
ppp chap password 0 cisco
ppp ipcp dns request
crypto ipsec client ezvpn hw-client-pri inside
!
!
!   プライマリ WAN の外部 EzVPN インターフェイスを定義します。
!
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 Dialer 1 253
!
access-list 1 permit any
!
access-list 102 permit icmp any host 209.131.36.158
!
dialer-list 1 protocol ip list 1
!
dialer-list 2 protocol ip permit
no cdp run
!
!
!
route-map track-primary-if permit 10
match ip address 102
set interface Dialer2 null0
!
control-plane
!
line con 0
exec-timeout 0 0
exec prompt timestamp
stopbits 1
line aux 0
stopbits 1
line 0/1/0
exec-timeout 0 0
script dialer gsmscript
login
modem InOut
no exec

```

```
transport input all
transport output all
rxspeed 236800
txspeed 118000
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet
!
scheduler allocate 20000 1000
!
end
```

## EzVPN サーバルータの設定

### 例 5-11 EzVPN サーバルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に戻って参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
hostname ezvpn_gw
!
ip cef
!
username cisco123@cisco.com password 0 lab
username sachin@cisco.com password 0 lab
!
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 1800
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group hw-client-group
  key cisco123
  dns 10.11.0.1
  domain cisco.com
  pool dynpool
  acl 111
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
crypto dynamic-map dynmap 1
  set transform-set set1
!
!
crypto map dynmap isakmp authorization list hw-client-groupname
```

## ■ プライマリ リンクおよびバックアップリンクを使用した EzVPN 導入

```

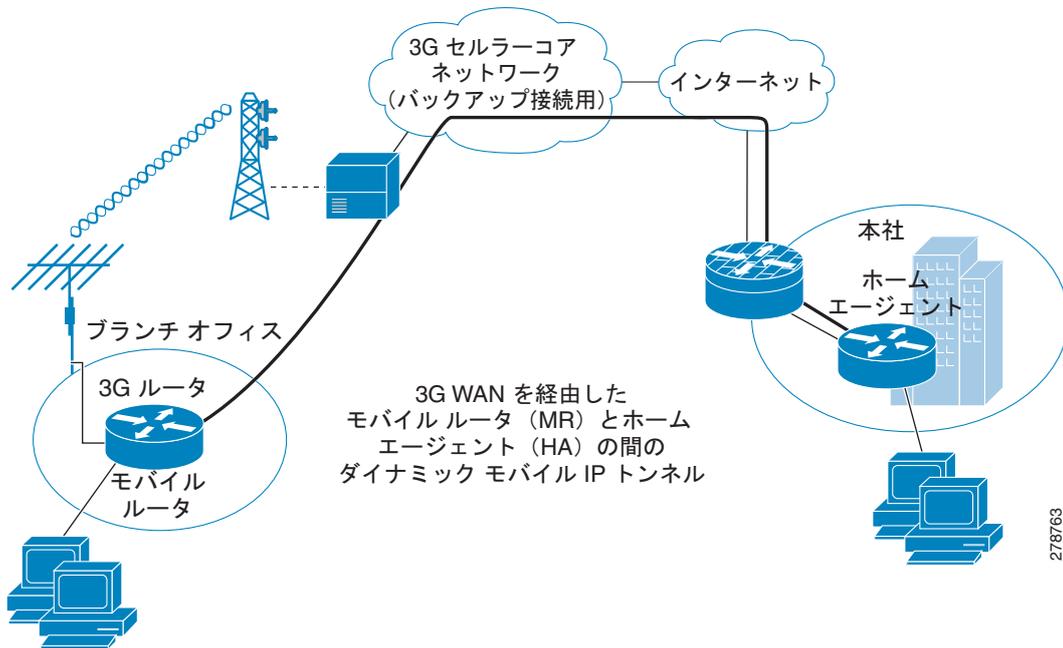
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!   EzVPN サーバ側設定。ACL 111 は、EzVPN クライアントから暗号化される許可されたトラフィックを定義し、
!   IPsec トンネルのセットアップ中にネゴシエーションされます
!
!
interface GigabitEthernet0/0
ip address 128.107.248.243 255.255.255.224
ip nat outside
duplex auto
speed auto
crypto map dynmap
!
!
!   クリプト マップはサーバの WAN インターフェイスに適用されます。
!
!
interface GigabitEthernet0/1
ip address 10.11.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
media-type rj45
no cdp enable
!
ip local pool dynpool 10.11.0.50 10.11.0.100
!
!   ローカル プールを定義して、IP アドレスをリモート EzVPN クライアントに指定します。
!
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 128.107.248.254
!
access-list 111 permit ip 10.11.0.0 0.0.0.255 10.13.0.0 0.0.0.255
!
!   EzVPN リモート クライアント用の暗号化が許可される必要のある対象トラフィックを
!   定義します。このような ACL 版は、暗号化および NAT 用に EzVPN の
!   リモート クライアントに伝達されます。
!
!
control-plane
!
!
!
line con 0
exec-timeout 0 0
exec prompt timestamp
line aux 0
line vty 0 4
login
!
end

```

## CCOA-Only モードでの NEMO Over 3G

Network Mobility (NEMO) は、広範囲にわたる地理的領域にわたって、スタブ ネットワークとして複数のブランチを導入するために使用できる、スケーラブルなオプションです。すべてのブランチはブランチ ルータの背後に接続されたモバイル ネットワークとして機能し、WAN リンクを介したダイナミック モバイル IP トンネルによって、すべての接続を確立します。次の設定例は、Foreign Agent (FA) が存在しない、コロケーション気付アドレスのみ (CCOA-only) のモードでのモバイル IP を示しています。ブランチでの NEMO 導入の詳細については、「[Introduction to Mobile IP](#)」を参照してください。

図 5-6 3G WAN 経由での NEMO の配置



278763

## ブランチ オフィスのモバイル ルータ (MR) の設定

例 5-12 ブランチ オフィスのモバイル ルータ (MR) の設定

```
!
hostname mobile-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsmppool
  network 10.4.0.0 255.255.0.0
  dns-server 66.209.10.201 66.102.163.231
  default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   セルラー インターフェイスを介したダイヤル アウトへのチャット スクリプト
!
```

```

track 234 rtr 1 reachability
!
!   バックアップ方法のオブジェクト トラッキング。
!
interface Loopback100
  ip address 10.100.0.3 255.255.255.0
!
!   モバイル ルータに割り当てられた静的 IP アドレス。このアドレスは
!   HA-MR サブネットの一部です
!
interface GigabitEthernet0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/1
  no ip address
  shutdown
!
interface FastEthernet0/1/0
  switchport access vlan 104
!
interface FastEthernet0/1/1
  switchport access vlan 104
!
interface FastEthernet0/1/2
  switchport access vlan 104
!
interface FastEthernet0/1/3
  switchport access vlan 104
!
!   DHCP クライアント ホストによって使用されるファスト イーサネット ポート
!
interface ATM0/0/0
  no ip address
  ip virtual-reassembly
  load-interval 30
  no atm ilmi-keepalive
  dsl operating-mode auto
!
!   プライマリ インターフェイスとして使用される ATM (DSL) 物理インターフェイス。
!
interface ATM0/0/0.1 point-to-point
  ip nat outside
  ip virtual-reassembly
  no snmp trap link-status
  pvc 0/35
  pppoe-client dial-pool-number 2
!
interface Cellular0/1/0
  no ip address
  ip nat outside
  encapsulation ppp
  dialer in-band
  dialer pool-member 1
  dialer-group 1
  async mode interactive
  ppp ipcp dns request
!
!   モバイル IP の導入に外部ダイヤラ (ダイヤラ 1) を使用し、ダイヤラ pool-member 1 は、
!   ダイヤラ プール 1 が設定されているダイヤラ 1 にセルラー インターフェイスを関連付けます
!
interface Vlan104
  description ip address used as default gateway address for DHCP   clients

```

```
ip address 10.13.0.254 255.255.0.0
ip nat inside
ip virtual-reassembly
!
!   ファスト イーサネット ポート 0/1/0 から 0/1/3 に接続されたホストに VLAN 104 を定義します。
!   このサブネットは、モバイル ルータの背後にあるモバイル ネットワークになります。
!
interface Dialer1
ip address negotiated
ip nat outside
ip mobile router-service roam
ip mobile router-service collocated ccoa-only
encapsulation ppp
dialer pool 1
dialer string gsmscript
dialer persistent
dialer-group 1
ppp chap hostname cisco@cisco.com
ppp chap password 0 cisco123
ppp ipcp dns request
!
!   ccoa-only モバイル IP モードのモバイル IP 設定のセルラーと関連付けられた
!   外部のダイヤラ インターフェイス。
!

interface Dialer2
ip address negotiated
ip nat outside
encapsulation ppp
dialer pool 2
dialer-group 2
ppp chap hostname Cisco@cisco.com
ppp chap password 0 cisco
ppp ipcp dns request
!
router mobile
!
!   このコマンドはルータでモバイル IP 機能をオンにします
!

!
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 dialer 0/0/0 253
!
ip mobile secure home-agent 128.107.248.243 spi decimal 1003 key ascii 1234567891234563
algorithm md5 mode prefix-suffix
!
!   このステートメントは ASCII 値を使用して暗号化の詳細と認証を定義します。
!   ASCII 値は HQ 側のルータの HA 設定の値と一致している必要があります
!
ip mobile registration-lifetime 1800
ip mobile router
address 10.100.0.3 255.255.255.0
collocated single-tunnel
home-agent 128.107.248.243
mobile-network GigabitEthernet0/1
register retransmit initial 5000 maximum 10000 retry 5
reverse-tunnel
!
!   アドレスは、ループバック 100 に定義されたモバイル ルータの静的 IP アドレスを定義します
!
!   モバイル IP リクエストを開始するユーザをルータが認識できるように、
```

```
! ホーム エージェント アドレスが定義されます。
!  
ip sla 1  
 icmp-echo 209.131.36.158 source-interface Dialer2  
 timeout 1000  
 frequency 2  
  
ip sla schedule 1 life forever start-time now  
  
access-list 1 permit any  
!  
access-list 102 permit icmp any host 209.131.36.158  
!  
dialer-list 1 protocol ip list 1  
!  
dialer-list 2 protocol ip permit  
no cdp run  
!  
!  
!  
route-map track-primary-if permit 10  
 match ip address 102  
 set interface Dialer2 null0  
!  
control-plane  
!  
bridge 1 protocol ieee  
!  
line con 0  
 exec-timeout 0 0  
 exec prompt timestamp  
 stopbits 1  
line aux 0  
 stopbits 1  
line 0/1/0  
 exec-timeout 0 0  
 script dialer gsmscript  
 login  
 modem InOut  
 no exec  
 transport input all  
 transport output all  
 rxspeed 236800  
 txspeed 118000  
line vty 0 4  
 privilege level 15  
 login local  
 transport input telnet  
!  
scheduler allocate 20000 1000  
!  
end
```

## 本社のホーム エージェント (HA) のルータの設定

### 例 5-13 本社のホーム エージェント (HA) のルータの設定

この設定内で青色の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。太字のテキストは、エラーが発生した場合に参照するための重要なコマンドを示すために使用されています。デバッグする場合は、太字で示されているすべてのコマンドがコンソール出力でも同じであることを確認します。

太字のテキストは基本セルラー設定、暗号化 IPsec 設定、IP SLA バックアップ設定、およびモバイル IP 設定の呼び出しに使用されます。これらの各設定に関連付けられている次の各コマンドは、サンプル全体にわたって呼び出されるため、デバッグ時に簡単に参照できます。

```
hostname HQ-HomeAgent
!
ip cef
!
interface Loopback100
  ip address 10.100.0.1 255.255.255.0
  !
  !   ホーム エージェント (HA) とモバイル ルータ (MR) 間のモバイル IP サブネット
  !
interface GigabitEthernet0/0
  ip address 128.107.248.243 255.255.255.224
  ip nat outside
  duplex auto
  speed auto
  !
  !   これは、インターネットを介してモバイル ルータに接続する WAN インターフェイスです
  !
interface GigabitEthernet0/1
  ip address 10.11.0.1 255.255.255.0
  ip nat inside
  ip virtual-reassembly
  duplex auto
  speed auto
  media-type rj45
  no cdp enable
  !
router mobile
  !
  !   HA のルータ上のモバイル IP を有効にします
  !
  !
  ip nat inside source list 101 interface GigabitEthernet0/0 overload
  !
  ip route 0.0.0.0 0.0.0.0 128.107.248.254
  !
  ip mobile home-agent reverse-tunnel private-address
  ip mobile home-agent QoS policer
  ip mobile home-agent address 128.107.248.243 lifetime 1800 replay 255 unknown-ha accept
  reply
  !
  !   ホーム エージェントの設定
  !
  ip mobile host 10.100.0.3 virtual-network 10.100.0.0 255.255.255.0
  ip mobile mobile-networks 10.100.0.3
  register
  !
  !   登録用のモバイル ルータ エントリ
  !
```

```
ip mobile secure host 10.100.0.3 spi decimal 1003 key ascii 1234567891234563 algorithm md5
mode prefix-suffix
ip mobile registration-lifetime 1800
!
!   セキュアな通信のためのモバイル ルータ認証 (MR に設定されているものと同じ ASCII)
!   および暗号化詳細
!
access-list 101 permit ip 13.1.1.0 0.0.0.255 any
!
control-plane
!
line con 0
  exec-timeout 0 0
  exec prompt timestamp
line aux 0
line vty 0 4
  login
!
end
```



# CHAPTER 6

## 用語集

---

**3G** : 携帯電話テクノロジーに関連する第 3 世代テクノロジー。3G に関連付けられたサービスには、モバイル環境内の広域ワイヤレス音声通話とブロードバンドワイヤレス データがあります。

**3GPP** : 第 3 世代パートナーシップ プロジェクト。

**3GPP2** : 第 3 世代パートナーシップ プロジェクト 2。

**ACL** : アクセス コントロール リスト。

**BTS** : ベース ステーション トランシーバ システム。

**CDMA** : 符号分割多重接続。

**CDMA2000** : 携帯電話とセル サイト間で音声、データ、およびシグナリング データ (ダイヤルされた電話番号など) を送信するために、CDMA、デジタル無線用の複数のアクセス方法を使用するモバイル電気通信規格のハイブリッド 2.5G/3G プロトコル。CDMA2000 は、1xRTT では 2.5G プロトコルとみなされ、EVDO では 3G プロトコルとみなされます。

**CHAP** : チャレンジ ハンドシェイク 認証プロトコル。

**EDGE** : GSM Evolution (EDGE) または Enhanced GPRS (EGPRS) の拡張データ レート。

**EVDO** : Evolution-Data Optimized または Evolution-Data Only。

**GGSN** : GPRS サポート ノード。

**GPRS** : General Packet Radio Service。

**GSM** : モバイル通信用グローバル システム。

**HA** : ホーム エージェント。

**HSDPA** : High-Speed Downlink Packet Access または High-Speed Downlink Protocol Access。

**HWIC** : 高速 WAN WAN インターフェイス カード。

**IPCP** : IP 制御プロトコル。

**MIP** : モバイル インターネット プロトコル。

**NAI** : ネットワーク アドレス識別子。

**PCF** : パケット制御機能。

**PDP** : パケット データ プロトコル。

**PDSN** : パケット データ サービング ノード。

**PPP** : ポイントツーポイント プロトコル。

**PSTN** : 公衆電話交換網。

**QoS** : Quality of Service。

**RAN** : 無線アクセス ネットワーク。

**SGSN** : サービング GPRS サポート ノード。

**SIM** : 加入者識別モジュール。

**SIP** : Simple Internet Protocol。

**SMB** : 小規模から中規模の企業。

**UMTS** : Universal Mobile Telecommunications System は、3G 携帯電話テクノロジーの 1 つです。

**WCDMA** : ワイドバンド符号分割多重接続。

**Wi-Fi** : ワイヤレス フィデリティ。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先: シスコ コンタクトセンター

0120-092-255(フリーコール、携帯・PHS含む)

電話受付時間: 平日 10:00~12:00、13:00~17:00

<http://www.cisco.com/jp/go/contactcenter/>