3G High-Speed WAN Interface Card Solution Deployment Guide

Version 1
May 6, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22739-01

3G High-Speed WAN Interface Card Solution Deployment Guide

CONTENTS

Preface

First Published: May 6, 2010, OL-22739-01

This guide provides a brief introduction to 3G wireless network technology and the Cisco 3G High-Speed WAN Interface Card (HWIC) offerings. It provides information about this technology and 3G wireless network architectures, particularly from protocols and network connectivity perspective. This information is helpful in understanding the 3G wireless specific configurations for successful customer deployments and for troubleshooting any problems that may arise during and after the deployment.

In addition, this guide provides information about modem activation, profile creation and other cellular specific requirements which are necessary before the cellular interface can successfully gain connectivity to the wireless service provider network.

You will learn about various types of typical network deployments. Detailed information on various configurations and guidelines specific to this technology are explained.

Troubleshooting and detailed debugging information is explained which should aid in resolving any commonly encountered problems.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

CHAPTER 1

Introduction

Revised: May 6, 2010, OL-22739-01

This chapter describes the Cisco 3G wireless WAN services, the types of 3G wireless broadband networks, and other characteristics for the 3G High-Speed WAN Interface Card.

Contents

Overview

This guide provides deployment, debugging, and troubleshooting information for the 3G High-Speed WAN Interface Card (HWIC). This card provides wireless 3G networking capability on the second generation Integrated Services Routers (ISR-G2).

This guide is intended for use by system integrators, sales engineers, customer support engineers, and those responsible for the design and implementation of 3G wireless services in a network environment. This guide bridges the gap for those who have a strong background in the 3G environment or in data and voice networking.

For specific information about the HWIC hardware, see http://www.cisco.com/go/3g.

Some basic knowledge is required to understand each element in the 3G services. Additional knowledge may be required depending on the specific service being implemented. A successful implementation will require knowledge in the following areas:

- Operational knowledge of the 3G services to be networked, including wired interface characteristics
- Provisioning data services on Cisco IOS software-based routers

Installations may also require skills in configuring the Cisco Dialer and Tunnel interfaces.

Background Information

This section describes the Cisco 3G wireless WAN services and various attributes for 3G wireless broadband networks.

Cisco 3G Wireless WAN Services

The 3G High-Speed WAN Interface Card, or the HWIC-3G-CDMA and HWIC-3G-GSM, enable new Enterprise and small to medium business (SMB) services based on high-speed mobile broadband. These services include:

- Remote Branch Primary/Backup WAN connection—Target service is remote branch backup because many Enterprises and SMBs choose to replace ISDN with alternative technologies. The Wireless WAN can also act as a primary access for non-real-time, low-to-medium speed applications such as bank automated teller machines (ATM), or any serial encapsulated technology running at 9600 Bps.
- Rapid, Nomadic Deployment—Wireless WAN service enabled by the 3G HWIC is beneficial for nomadic connectivity, such as workgroups and temporary connectivity from trade shows and construction sites.
- Mobile Disaster Recovery Solution—This service is important when there are major outages with whirling facilities. Cellular service can remain functional because it can take alternative paths through different central offices.

Types of 3G Wireless Broadband Networks

3G wireless data networks are defined as broadband wireless public networks, supporting at least 2 Mbit/sec access speeds (not necessarily average sustained throughput). These networks are based on Code Division Multiple Access (CDMA) radio access technology, which provides concurrent multiple accesses. The available access bandwidth on these networks is shared among concurrent *active* users; therefore, the total available bandwidth is shared amongst these users.

These wireless broadband networks have evolved from the existing cellular networks, which were primarily and originally designed for circuit switched voice. With the growth of IP-based networks and IP data connectivity, broadband service was introduced on these networks. Because the original network was primarily designed for circuit switched voice, this network path was not suitable for the support of broadband IP data. An overlay network was created to provide support for this capability.

There are two types of cellular wireless data networks deployed today:

- GSM/UMTS—The architecture for GSM/UMTS is defined by the 3GPP standards organization. This set of standards includes GPRS, EDGE, HSPA, and HSPA+ air interfaces.
- CDMA2000 technology—The architecture for CDMA2000 technology is defined by the 3GPP2 standards organization. This set of standards includes 1xRTT, EvDO-Rev0, and EvDO-RevA air interfaces.

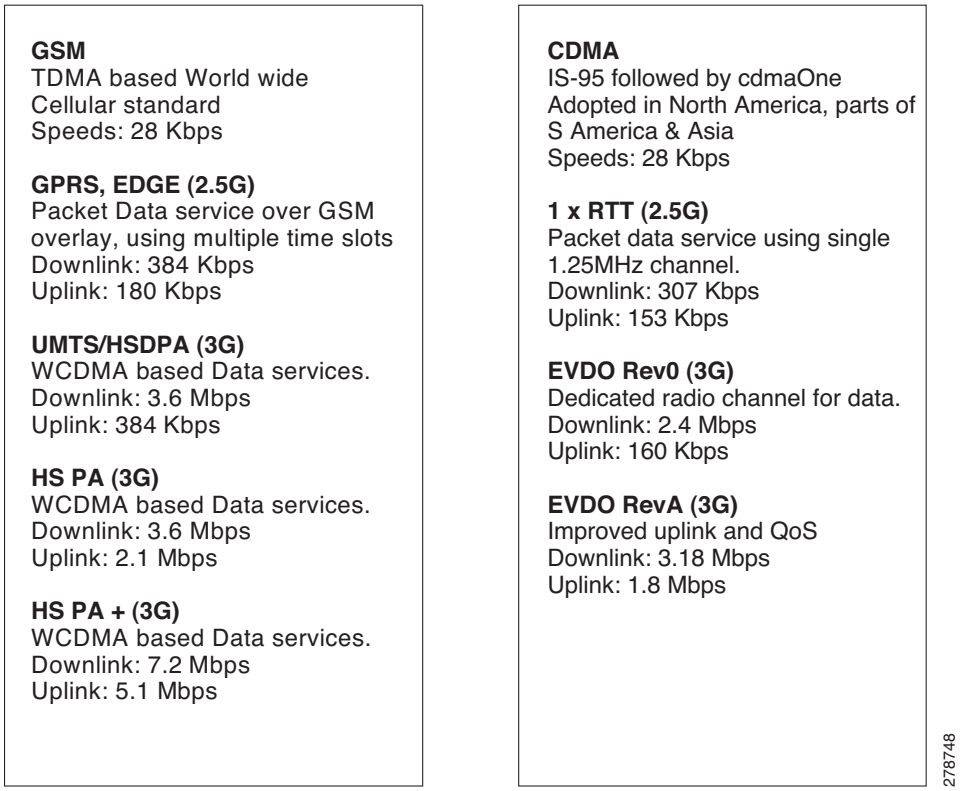
In this document, the term *GSM* is used to describe any of the radio transmission technologies covered by the 3GPP standards. The term *CDMA* is used to describe any of the radio transmission technologies covered by the 3GPP2 standards. Both the UMTS and CDMA2000 use CDMA modulation technology, but UMTS uses a wider bandwidth, compared to CDMA, thus known as W-CDMA. CDMA20000 operates at 1.25 MHz bandwidth, instead of the 5.0 MHz bandwidth used by UMTS.

The CDMA broadband wireless network is based on the Qualcomm CDMA-2000 technology. This network architecture is IETF centric because it makes use of the existing IETF protocols as much as possible. The GSM broadband architecture is not as IETF centric; it uses some of its own protocols instead of using any of the existing protocols.

Performance Characteristics

The 3G HWIC supports HSDPA and EV-DO Rev A. Figure 1-1 shows the CDMA2000 technologies and the GSM/UMTS technologies.

Figure 1-1 CMDA2000, GSM, and CDMA Technology Performance Characteristics



Throughput

Throughput is shared per cell sector and per carrier frequency. The values for total theoretical throughput per sector downlink and uplink for EVDO Rev A, HSDPA, and HSPA are shown in Table 1-1.

Table 1-1 Total Theoretical Throughput Per Sector for the 3G HWIC Chipset

Technology/Service	Uplink (Mbps)	Downlink (Mbps)
EVDO Rev A	1.8	3.1
HSDPA	384 (Kbps)	3.6
HSPA	5.1	7.2

Actual throughput depends on network conditions at the time, the Received Signal Strength Indicator (RSSI), and the cellular backhaul facilities on the ISP network.

Latency

Latency in the 3G cellular network is higher than that in wire-line networks. It is dependent on network conditions and may be up to 100 ms on the air-link and Radio Access Network (RAN). The below table depicts the observed end-to-end throughput and latency during beta.

Table 1-2 End-to-end Latency and Throughput Observed During Beta

Technology/Service	Uplink (Kbps)	Downlink (Kbps)	One way Latency (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

Shared Access

WiFi, Ethernet, DSL, and 3G cellular all display shared access technology. Other data subscribers, including PC card users and other 3G HWICs who are using radio resources in the same cell and sector, can impact the performance of the 3G HWIC.

RSSI and Carrier-to-Interference Ratio

RSSI is a circuit to measure the strength of an incoming signal. The basic circuit is designed to pick RF signals and generate an output equivalent to the signal strength. The ability of the receiver to pick the weakest signal is referred to as receiver sensitivity. The higher the receiver sensitivity, the better the performance. There are circuits that measure the signal strength based on the output voltage. If the signal strength is good, the output voltage is higher and the output voltage is poor if the signal strength is low.

A mobile handset which is moving in a cell will record a signal strength that varies. Signal strength is subject to slow fading, fast fading and interference from other signals, resulting in degradation of the carrier-to-interference (C/I) ratio. A high C/I ratio yields quality communication. A high C/I ratio is achieved in cellular systems by using optimum power levels through the power control of most links. When carrier power is too high, excessive interference is created, degrading the C/I ratio for other traffic and reducing the traffic capacity of the radio subsystem. When carrier power is too low, C/I is too low and quality of service (QoS) targets are not met. Ideally, the C/I ratio should be as high as possible, and the ratio of received pilot energy (Ec) to total received energy or total power spectral density (Io) value, (Ec/Io) value should be as low as possible. Cisco does not determine any acceptable values. These values are determined by the cellular carriers. In situations in which high Ec/Io values are observed and a low Received Signal Strength Indicator (RSSI) value, a site survey is necessary to determine how to achieve better characteristics of the signal.

Because of these performance characteristics, the sweet spot for the 3G HWIC is non-real time, sub-512Kbps applications. As networks evolve, latencies decrease, and QoS becomes available, real-time applications such as VoIP become viable.

Quality of Service

Currently, air-link and Radio Access Network (RAN) QoS are not available on production cellular networks. Therefore, while the traditional IP QoS are available on the ISRs and on the 3G HWIC interface, there is no mapping to the air-link. The Cisco IOS QoS capabilities may be leveraged to improve the application experience. Techniques such as congestion management, congestion avoidance, policing and shaping, and MQC (Modular QoS CLI) are all useful. For more information, see:

http://www.cisco.com/en/US/partner/docs/ios/isg/configuration/guide/isg_mqc_ipsession_ps6922_TSD_Products_Configuration_Guide_Chapter.html.

Since 3G uses shared access, the output field of BandWidth (BW) from **show interface** reflects the theoretical bandwidth available, (such as 1.8Mbps for EV-DO Rev A), and not actual bandwidth. Instantaneous downlink network speeds may be 2 Mbps, or 300Kbps.

CHAPTER 2

Cisco 3G GSM Based High-Speed WAN Interface Card

Revised: May 6, 2010, OL-22739-01

This chapter describes the 2.5/3G GSM based broadband data network architecture and data call establishment. It also explains how to create a GSM modem profile and prepare for network connectivity.

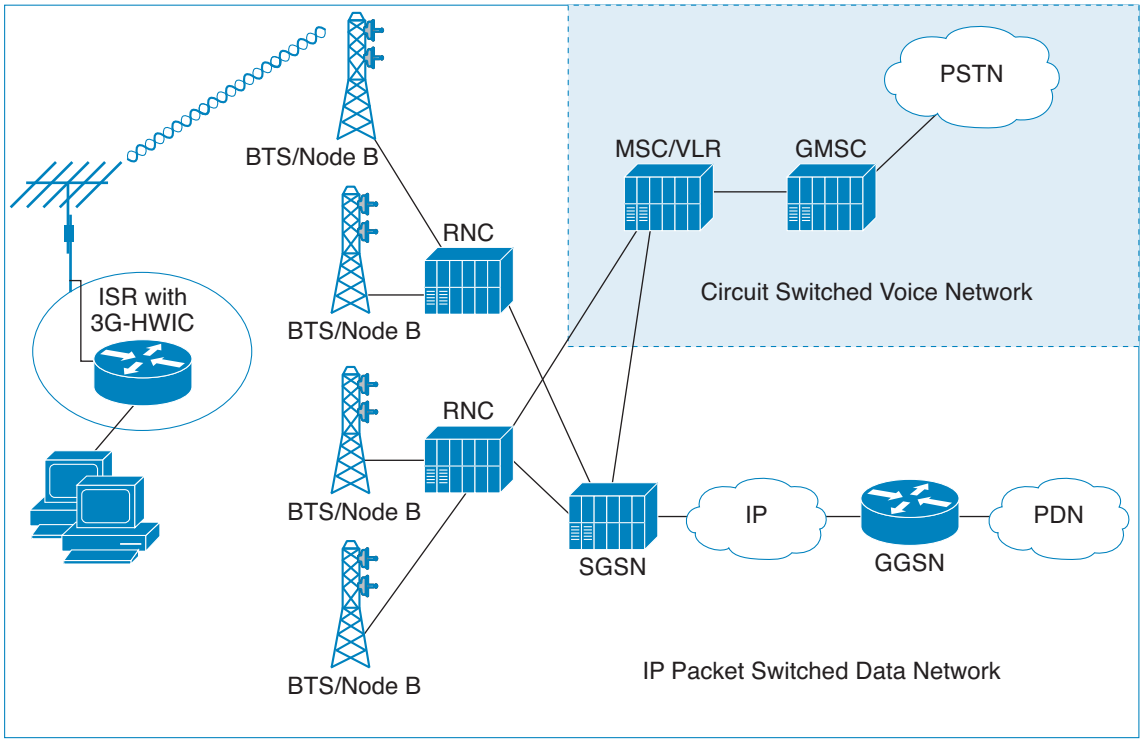
Contents

Overview of 2.5/3G GSM Based Broadband Data Network Architecture

The GSM based network, shown in Figure 2-1, uses the Base station Transceiver System (BTS) at the cell tower, known as the Node-B in UMTS. The 3G-HWIC-based ISR communicates with Node-B over the air, and attaches itself to the network before setting up a data session (known as PDP context) with the network. The Node-B terminates the radio network access technology. The Radio Network Controller (RNC) provides mobility service to mobiles served by the attached Node-Bs.

To support broadband IP data network capability, two network node types are introduced: SGSN and GGSN. SGSN performs mobility function to replace the Visitor Location Register (VLR) functionality. GGSN acts as an IP packet gateway to the Internet. The broadband IP data packet path takes place from the mobile node (hand set), to the Node-B, RNC, SGSN, GGSN, and to the Internet. The traditional circuit switched path continues via the MSC, GMSC, and PSTN. The broadband IP data network acts as an overlay network over the existing cellular network. The 2.5G network is the original GPRS network, with the same physical topology, as shown in Figure 2-1.

Figure 2-1 GSM 3G IP Wireless Data Network



2.5/3G GSM Data Call Establishment

Figure 2-2 shows 3G data calls in the GSM network. The PPP terminates between the IOS and the modem in the 3G-HWIC. Over the air PPP is not used; instead, 3GPP defined protocol is used to set up the call. The 3GPP defined protocol terminates on the modem on one end, and the SGSN/GGSN on the other end.

Before the very first call can be set up, you must get a data service account from your service provider. As a part of this service, a SIM card is provided by the service provider. The SIM card must be installed on the 3G-HWIC.

- PPP CHAP User-Name (hostname)
- PPP CHAP Password
- APN (Access Point Name)

You can create a profile in the modem, as shown in Example 2-1. The profile stores these parameters in the NVRAM of the modem. This allows the modem to authenticate the IOS at the PPP CHAP phase so that the IOS can continue on to the next phase PPP IPCP without having to wait for the real authentication that actually takes place with the wireless network over the air.

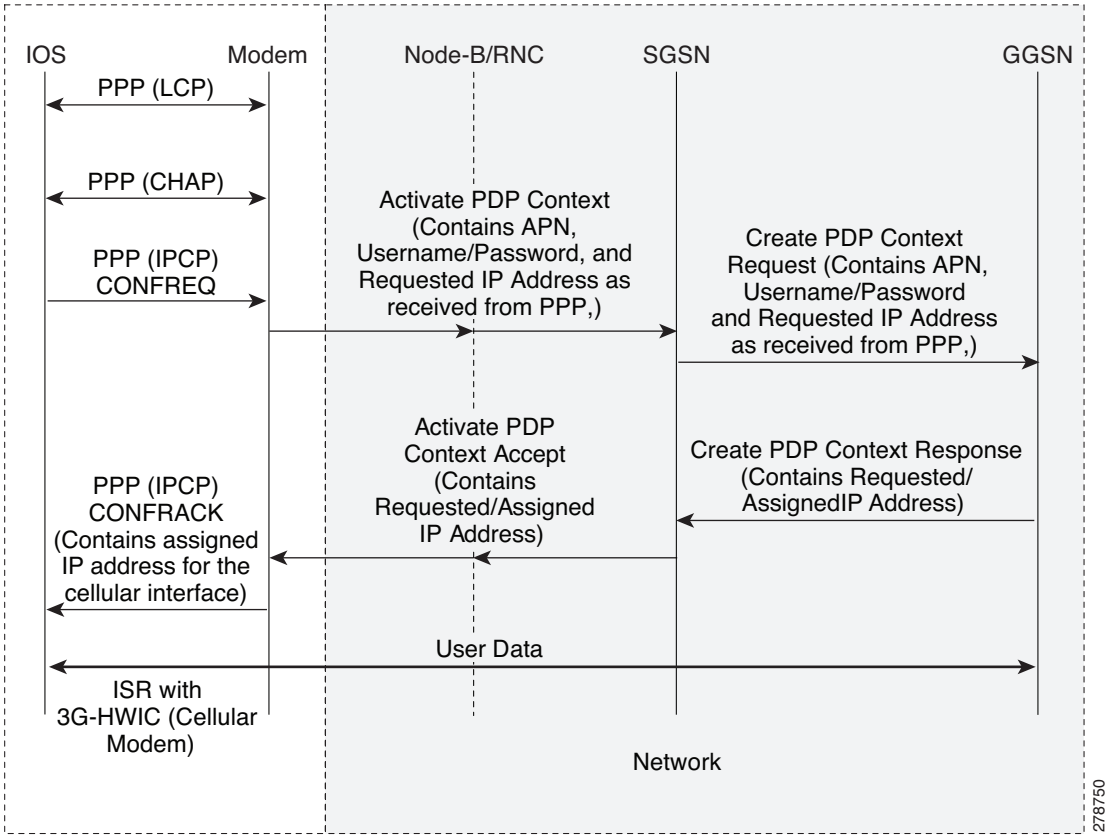
The very first packet that meets the *interesting traffic* criteria, as defined by the associated ACLs, causes the dial out to occur via the cellular interface. This causes PPP LCP, and PPP CHAP to complete between the IOS and the modem. The modem stores the PPP user-name (host name) and password, which allows the CHAP to succeed locally, and the IPCP phase can start immediately.

As part of the PPP IPCP phase, the IOS sends the CONFREQ message, requesting the IP address for the cellular interface (and possibly the DNS addresses, if configured for these addresses). After the modem receives the CONFREQ, it sends the Activate PDP Context Request message over the air. This message contains the Username, Password, and the APN stored in the NVRAM, which was created as part of the profile. The message requests the IP address for the cellular message and DNS IP addresses, if applicable.

The SGSN, upon receipt of Activate PDP Context Request message, sends the Create PDP Context Request message, relaying these parameters to the appropriate GGSN. The GGSN validates the user, assigns an IP address to the cellular interface, and returns this in the Create PDP Context Response message to the SGSN. This information is relayed to the modem, by the SGSN, as an Activate PDP Context Accept message.

Finally, the modem returns the pending IPCP response to the IOS (CONFACK), returning the IP address, and any other requested information, such as DNS addresses. The IP address is bound to the cellular interface, and installed in the routing table. Now the user data transfer can begin.

Figure 2-2 GSM 3G Data Call Establishment Call Flow



GSM Modem Profile Creation and Preparation for Network Connectivity

A newly installed 3G GSM wireless HWIC must complete a series of steps before it can connect to the wireless network. These steps are described in the following sections.

Service Plans

The 3G HWIC needs to be associated with a service plan before it can be activated on a carrier network. Depending on the mobile operator, there are multiple mobile broadband data plans available, unlimited, metered, or pooled. It may be possible to tie the 3G HWIC service to an existing enterprise wireless contract, which helps to keep down the monthly recurring cost (MRC).

The link below lists the mobile operators that have certified the 3G HWIC and provides links to these carrier websites for additional information on the service.

http://www.cisco.com/en/US/products/hw/routers/networking_solutions_products_generic_content0900aecd80601f7e.html

Selection of best radio network

If HSDPA, the 3G HWIC will downshift to the best radio network available, down to 2.5G technology. This means the 3G HWIC will attempt to connect to the best network available on the operator's network. If HSDPA is not available, the 3G HWIC will negotiate for UMTS, and if that is not available, it will negotiate for the 2.5G technology EDGE, and then GPRS.

Modem Profile Creation

Create a GSM data connectivity profile in the cellular modem before attempting to set up a data connection with the cellular network. This profile defines the user and its set of authentication parameters with the modem, and the cellular network.

The **cellular <x/x/x> gsm profile create** command is used for creating a GSM profile, which will be used for dialing out using PPP to establish a data connection (PPP connection/PDP context) with the 3G cellular modem, and the cellular data network.

Example 2-1 Creating a Modem Profile

```
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>
```

Argument	Description
<profile number>	number from 1 to 16 - up to 16 profiles may be created, although, normally, only one profile is sufficient.
<APN -Access Point Name>	As provided by your wireless service provider <chap | pap>: select chap, or pap keyword, depending upon what authentication protocol is supported for PPP by your wireless service provider.
<chap-or-pap-user-name>	As provided by your wireless service provider
<chap-or-pap-password>	As provided by your wireless service provider

The output from the `cellular <x/x/x> gsm profile create` command is shown below.

```
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#
```

Preparation for Network Connectivity

When the 3G HWIC first dials the mobile network after activation, it can take 2 to 5 seconds to establish end-to-end radio and IP connectivity. If the modem needs to redial, it can take longer than 5 seconds. In addition, the first time the modem is activated on the network, there are provisioning processes that kick off in the background that will cause the initial end-to-end connectivity to take longer.

Follow the steps below to prepare for network connectivity.

Step 1 Ensure that the SIM card obtained from your service provider is correctly in place on the 3G HWIC.

Step 2 Connect the antenna to the HWIC.

Step 3 Ensure that the RSSI signal level is better then negative 90 dBm.

Step 4 Run `show cellular x/x/x all` command to verify connectivity to the network.

The output from the `show cellular x/x/x all` command is shown below.

Example 2-2 Checking Network Connectivity

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

```
ROUTER#sh cell 0/0/0 all
!
only the relevant information is shown; rest is deleted, for readability purposes.
!

Profile Information
====================
Profile 1 = INACTIVE*
--------
PDP Type = IPv4
Access Point Name (APN) = xyz.com
Authentication = CHAP
Username: userXyz, Password: passwordForXyz

 * - Default profile
!
Ensure that your created profile is as expected, without any typographical errors, or any
inadvertent white space(s).
!

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 =
!
This particular example shows the network Packet Service is 'UMTS/WCDMA', and is
'Attached'. Your service may be somewhat different depending on service(s) provided by
your service provider.

Current Service Status should indicate 'Normal', as shown
!
Radio Information
=================
Current Band = WCDMA 1900, Channel Number = 9721
Current RSSI(RSCP) = -87 dBm
!
RSSI signal level should be better then -90 dBm, although data service may operate at
levels below these.
!
Modem Security Information
==========================
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of Retries remaining = 3
!
The SIM card is properly recognized.
!
```

Step 5 Configure the router as described in Chapter 5, “Advanced Network Deployment Scenarios”.

Step 6 Depending on your deployment requirement, connect to the network via the appropriate protocol and verify data transfer.

For more information, see:

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

CHAPTER 3

Cisco 3G CDMA Based High-Speed WAN Interface Card

Revised: May 6, 2010, OL-22739-01

This chapter describes the 3G CDMA broadband data network architecture, how CDMA data calls are established, and CDMA modem activation and network connectivity.

Contents

Overview of 3G CDMA Broadband Data Network Architecture

The CDMA-based wireless broadband data networks are IETF centric, which means that the protocols used for IP data connectivity/mobility are based on these standards, or are variants, derived from them.

Figure 3-1 shows the architecture for the CDMA networks. The 3G HWIC communicates with the BTS over the air. The CDMA on the network sides terminates on the BTS.

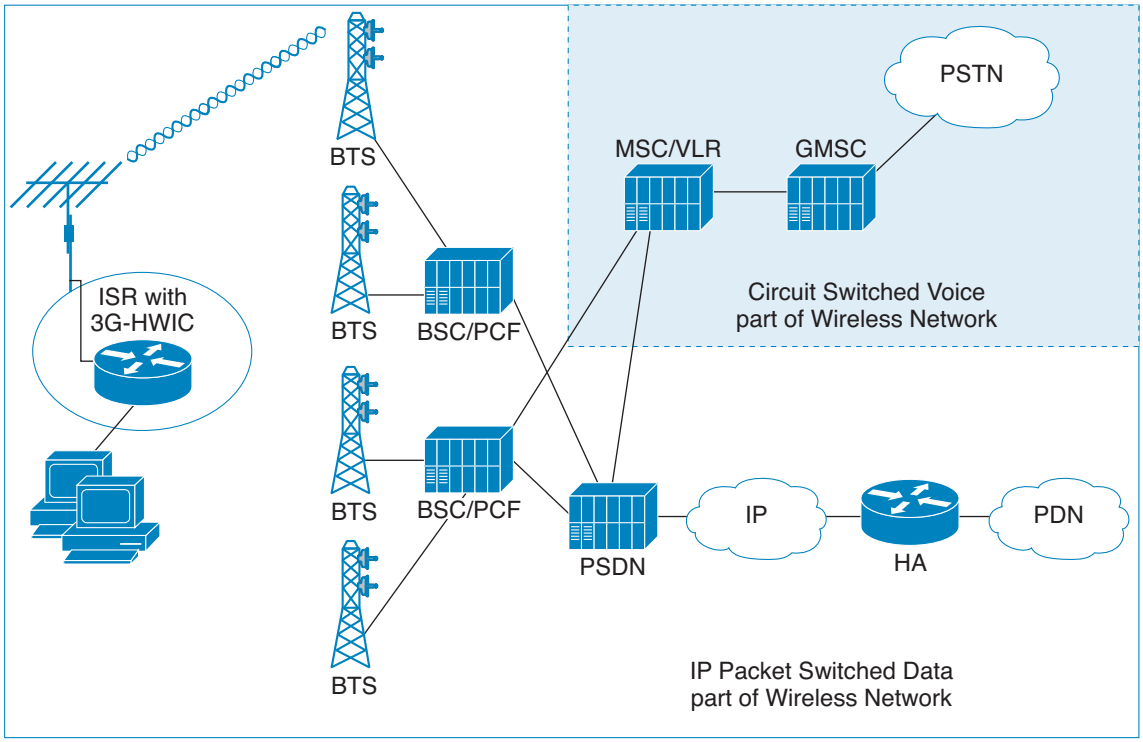
The Base Station Controller/Packet Control Function (BSC/PCF) combined with the Visitor Location Register (VLR), and the Home Location Register (HLR), perform mobility function. The PCF capability added on the traditional BSC provides the necessary IP capability for supporting 3G high speed data. The legacy BSC is not capable of supporting high speed data service; it provides support for circuit switched, non IP, voice service via the MSC.

The PCF, Packet Data Server Node (PDSN), and the HA (Home Agent) provide for an overlay network, specifically for high speed data access.

The ISR based 3G HWIC terminates PPP within the IOS/modem on one end, and on the PDSN on the network side. The PDSN anchors the PPP, and thus provides mobility for the mobile nodes across the associated BSC/PCFs and its associated BTSs, when using Simple IP (SIP) mode of access, without having to re-establish the PPP.

Normally, Simple IP is not used, and Mobile IP (MIP) is used with the PDSN acting as a Foreign Agent (FA). The Home Agent (HA) is located within the service provider network. In this case, the HA becomes the anchor point providing the IP address to the mobile node (3G HWIC based ISR). With the anchor point provided by the HA, mobility can be extended across multiple PDSNs (in theory across the entire network) without mobile terminals losing their IP connectivity while potentially attaching to different PDSNs during mobility.

Figure 3-1 CDMA 3G IP Wireless Data Network



3G CDMA Data Call Establishment

Figure 3-2 shows the data call flow in the CDMA network. The first packet that meets the *interesting traffic* criteria, as defined by the associated ACLs, causes the dial out to occur via the cellular interface. This causes the PPP to start between the IOS and the modem. After the LCP phase is completed between the Cisco IOS and modem, the IOS starts the PPP IPCP (CONFREQ) phase, bypassing the CHAP/PAP. The CHAP/PAP is bypassed because it is not required for IOS, and therefore not configured under the cellular interface.

After LCP/IPCP messages are received from the Cisco IOS, the modem starts, and completes the PPP connection with the network (PDSN). The modem is authenticated by the network during the PPP phase using parameters stored in the modem's NVRAM. These authentication parameters were loaded in the modem's NVRAM, after the modem was activated/provisioned. The activation/provisioning of the modem is a one time process. No IP address is requested by the modem during its IPCP phase with the network. The PPP is established with no IP address and assigned to the modem/IOS.

Note At this point, the PPP (IPCP) is still pending between the IOS and the modem.

After the PPP has been established between the modem and the network, the modem starts the Mobile IP phase. It sends the Mobile IP Registration Request message containing the Network Address Identifier (NAI), MN-AAA, MN-HA shared secrets, HA IP address, and requests an IP address for the modem/IOS (Home IP address). The NAI, MN-AAA, MN-HA shared secrets, and HA IP address are all loaded in the modem's NVRAM as part of modem activation/provisioning.

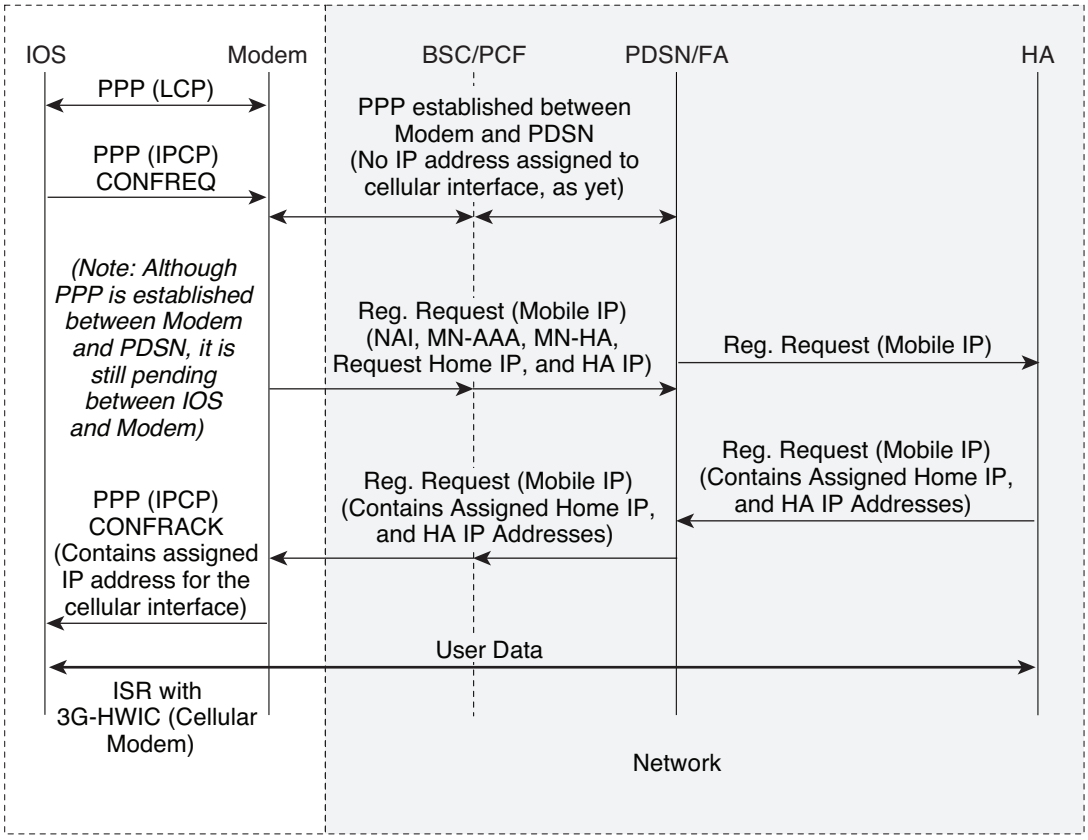
The Mobile IP Registration Request message is intercepted by the PDSN, which forwards this message to the appropriate HA, as indicated by the HA IP address. The receiving HA validates the user NAI, using the AAA, and returns the Registration Reply message. This assigns the IP address, which is the Home IP address, to the user modem. The PDSN, on receipt of this message, forwards it to the modem, as shown in Figure 3-2.

Finally, the modem sends the PPP IPCP (CONFACK) message to the IOS, completing the pending PPP connection between the IOS and the modem. The modem returns the IP address for the cellular interface, as received from the HA and any other IP addresses, such as DNS, if requested and received.

The address is assigned to the cellular interface, and route installed in the routing table.

Note The IOS is not aware of Mobile IP protocol running across the modem and the HA.

Figure 3-2 CDMA Data Call Establishment Call Flow



CDMA Modem Activation and Preparation for Network Connectivity

A newly installed 3G CDMA wireless HWIC requires going through a series of specific steps before connecting to the wireless network. These steps are listed below and described in detail in the following sections.

Step 1 Obtain wireless data service and the Equipment Serial Number (ESN) of the cellular modem from the service provider.

Step 2 Ensure that the cellular modem on the HWIC has been registered with the wireless service provider's network.

Step 3 Activate the modem on the service provider's network via Internet Over The Air (IOTA) or Over The Air Service Provisioning (OTASP) depending on what your service provider supports.

The 3G HWIC will connect to the best network available on the service provider's network.

Service Plans

The 3G HWIC must be associated with a service plan before it can be activated on a service provider's network. The URL below lists the mobile operators that have certified the 3G HWIC and provides links to these carriers' website for additional information on the service. Depending on the mobile operator, there are multiple mobile broadband data plans available: unlimited, metered, or pooled. It may be possible to tie the 3G HWIC service to an existing enterprise wireless contract, which can keep down the monthly recurring cost (MRC).

http://www.cisco.com/en/US/products/hw/routers/networking_solutions_products_generic_content0900aecd80601f7e.html

Selecting the Best Radio Network

The 3G HWIC will attempt to connect to the best network available on the service provider's network. If EVDO Rev A is not available, the 3G HWIC will downshift to the next best radio network available, down to 2.5G technology. For instance, if EVDO Rev A is not available, the 3G HWIC will negotiate for EVDO Rev 0, and if that is not available, it will connect via 1xRTT.

Activating the Modem

The 3G CDMA HWIC activation depends on what activation method is supported by your service provider. The types of activation methods are:

- Internet Over The Air (IOTA)
- Over The Air Service Provisioning (OTASP)

Check with your service provider to ensure the type of activation method supported. In the United States, Sprint supports IOTA, and Verizon Wireless supports OTASP.

Before attempting the activation, ensure that the HWIC is able to *communicate* with the network at *radio connectivity* level. To ensure that the modem is able to communicate, issue the **show cellular x/x/x** command.

Example 3-1 Sample Modem Activation Output

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

Unless otherwise noted, the bold text refers to commands associated with the basic cellular commands. The bold text is also used for other configurations such as the crypto IPsec configuration, the backup configuration, the IP SLA configuration, and the mobile IP configuration. Commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
ROUTER#sh cellular 0/1/0 all
!
!   Some of the information has been deleted for readability.
!
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
!
!   Ensure that the PRL, and the ESN information is as expected.
!
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
!
!   The HWIC must be able to get the 1xRTT network service before the service can be
!   activated.  In this case, only 1xRTT network is available.
!
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 service has relatively healthy RSSI (Received Signal Strength Indication)
!   levels, so service activation is possible.
!
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 service is not being sensed (not available in this area), for this particular
!   case.  Availability of this service is not a requirement for activating the HWIC.
!
```

Activating Using IOTA

To activate the HWIC using the IOTA procedure, use the following command.

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

Note Use the **sh cellular x/x/x all** command to obtain the values for the variables listed below.

- Mobile Directory Number (MDN)—10 digit number
- Mobile Subscriber Identification Number (MSIN)—10 digit number
- System ID (SID)
- Network ID (NID)
- Mobile Subsidy Lock (MSL)

Example 3-2 Activation Using IOTA Output

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

Unless otherwise noted, the bold text refers to commands associated with the basic cellular commands. The bold text is also used for other configurations such as the crypto IPsec configuration, the backup configuration, the IP SLA configuration, and the mobile IP configuration. Commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
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-b1-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 commited to NVRAM, Result = Success
Aug 18 19:06:52.015: IOTA Status Message Received. Event = IOTA End, Result = SUCCESS
```

```
!
!   The modem communicates with the IOTA server, and downloads the necessary information
!   to the modem.
!
```

Activation Using OTASP

To activate the HWIC using the OTASP procedure, use the following command.

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

Note Use the phone number provided by your service provider for the **phone number** variable.

Example 3-3 Activation Using OTASP Output

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

Unless otherwise noted, the bold text refers to commands associated with the basic cellular commands. The bold text is also used for other configurations such as the crypto IPsec configuration, the backup configuration, the IP SLA configuration, and the mobile IP configuration. Commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
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 Serice (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 commited to NVRAM, Result = Success
```

Preparation for Network Connectivity

When the 3G HWIC first dials the mobile network after activation, it can take 2 to 5 seconds to establish end-to-end radio and IP connectivity. If the modem needs to redial, then it can take longer than 5 seconds. In addition, the first time the modem is activated on the network, there are provisioning processes as explained in the previous sections which kick off in the background, which will cause the initial end-to-end connectivity to take longer.

After the HWIC has been activated and configured according to the network deployment requirements, the ISR is available for connectivity via the 3G wireless network. Connect the antenna to the HWIC, and ensure that RSSI signal level is better then negative 90 dBm. Ensure that the connectivity to the network indicated by the **show cellular x/x/x all** command output corresponds to what is shown in *Configuring the 3G Wireless High-Speed WAN Interface Card for Cisco 1841, and 2800 and 3800 Series Routers (HWIC-3G-CDMA-x)*.

CHAPTER 4

Basic Configurations

Revised: May 6, 2010, OL-22739-01

This chapter describes basic configurations for GSM and CDMA based wireless networks.

Contents

GSM Based Wireless Networks

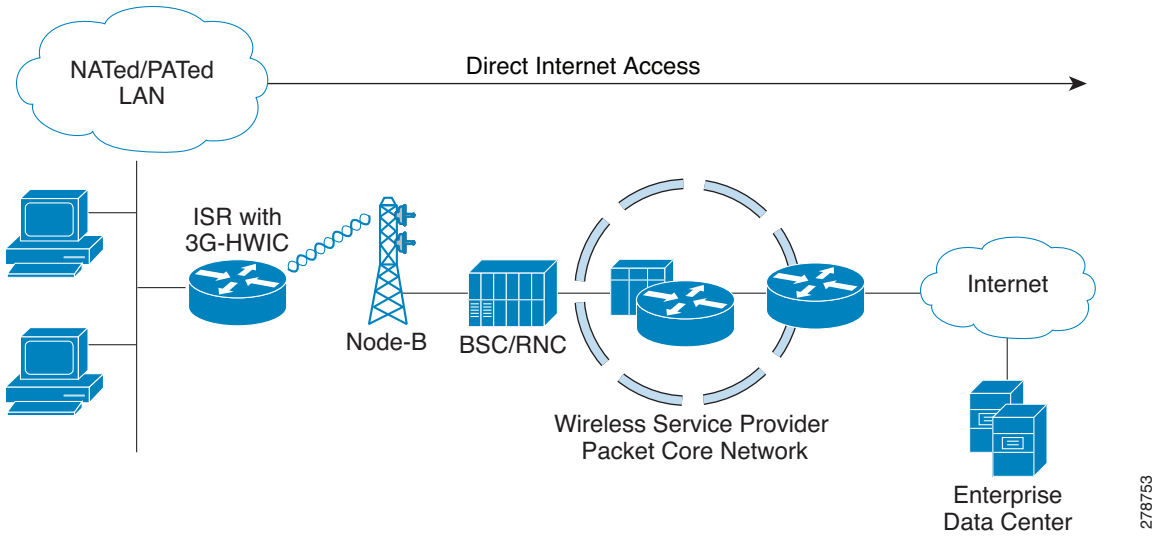
This chapter describes the most common deployment scenarios with detailed configurations and comments for each.

Deployment Using Network/Port Address Translation (NAT/PAT)

This simple deployment example uses NAT/PAT shown in Figure 4-1 that focuses on a wireless specific configuration. For more information on NAT, see:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aecd8064c999.html.

Figure 4-1 Simple Deployment Using NAT/PAT for GSM Wireless Networks



Example 4-1 IOS Configuration for Deployment Using NAT/PAT

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
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
!
!   Defines the DHCP pool for network 10.1.0.0/16, for hosts connected on VLAN 101, and
!   Fast Ethernet ports 0/1/0 thru 0/1/3.
!
ip domain name yourdomain.com
!
chat-script gsm "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   Defines dialer string 'gsm'. 'atdt*98*1#' command causes the cellular modem to
!   dial out using profile 1 (profiles are created using 'cellular x/x/x gsm profile
!   create …' command) . In response, the IOS expects the 'CONNECT' string from the modem
!   upon successful dial out. In this case, IOS waits 30 seconds as timeout, in case of
!   no/unexpected response. Note that the expected 'CONNECT' response from the modem is
!   case sensitive.
!
!
```

```
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
!
!   DHCP client hosts connected to the above Fast Ethernet ports.
!
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
!
!   It is highly recommended that the IP address is always configured as ip address
!   negotiated, even when a fixed (persistent) IP address is required. Cellular interface
!   is spoofed as 'up'/'up' (status/protocol states), regardless of whether the PPP is
!   established or not. If this interface is configured with a specific IP address
!   (instead of 'ip address negotiated'), and if the PPP is not yet established, the
!   routing table will interpret it as a valid route available via the cellular interface.
!   By assigning a negotiated IP address, this problem is avoided. This is particularly
!   important when using the cellular as a backup interface.

!   ip nat outside uses the IP address assigned to the cellular interface, as the
!   source IP address of IP packets going through the cellular interface, and sourced from
!   hosts on VLAN 101.

!   dialer in-band configures the interface to support dial on demand routing, and
!   additionally specifies that a chat script will be used for dialing out. In this case
!   it uses the chat script 'gsm', as defined earlier.

!   It is recommended that dialer idle-timeout is set to '0', to avoid disconnection of
!   PPP in the event of no traffic for a specified time, defined by this command. 'dialer
!   idle-timeout 0' sets this timer to indefinite timeout period.

!   dialer group and dialer-list are associated commands that allow the specification of
!   'interesting' traffic which will trigger the cellular modem dial out to occur, in
!   order to set up the PPP connection, if it is not yet established.
```

```
!   The user-name (hostname), and password for the PPP are provided by your service
!   provider (SP). Note that the user-name and password are locally authenticated between
!   the IOS and the cellular modem (which resides in the 3G HWIC), as far as the PPP is
!   concerned. The PPP terminates between the IOS and the modem. These same parameters
!   (i.e. the user-name and password) need to be also configured on the cellular modem).
!   The modem uses these parameters over the air, for the purposes of authenticating the
!   user with the network, using PDP context activation message, in order to set up a data
!   connection (known as PDP context) with the cellular network.

!   ppp ipcp dns-request is an optional command, which allows DNS IP address(es) to be
!   obtained from the cellular network, if required, via the PPP procedures.
!
interface Vlan1
 no ip address
!
interface Vlan101
 ip address 10.1.0.254 255.255.0.0
ip nat inside
!
!   Defines interface VLAN 101. This VLAN is used by the associated hosts (on the Fast
!   Ethernet ports). It provides NAT/PAT functionality using the ip nat inside command.
!
 ip virtual-reassembly
!
ip route 0.0.0.0 0.0.0.0 Cellular0/0/0
!
!   Defines the default route to be via the cellular interface - in this case all IP
!   packets are routed through the cellular interface.
!
!
ip nat inside source list 2 interface Cellular0/0/0 overload
!
!   Specifies the source of traffic that should be NAT/PATed is via the cellular
!   interface. In this case, it is performing PAT, by using the 'overload' parameter. The
!   source list 2 is associated with the access-list 2 (defined below), which
!   specifies the traffic source of interest (from 10.1.0.0/16 network, in this case).
!
!
access-list 1 permit any
!
access-list 2 permit 10.1.0.0 0.0.0.255
!
dialer-list 1 protocol ip list 1
!
!   The dialer-list 1 command is associated with dialer-group 1 command specified under
!   the cellular interface.
!
!   The access-list 1 command is associated with dialer-list 1 protocol ip list 1 command.
!
!   These commands specify the traffic of interest that will trigger the dial out to occur
!   through the cellular modem, and establish the PPP, if not already established.
!
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
!
!   It is necessary to specify the script dialer command under the corresponding line for
!   the cellular interface. In this case the cellular interface is 0/0/0, and hence the
!   line is also essentially 0/0/0.
!
!   rxspeed and txspeed cannot be configured.
!
!   modem InOut allows incoming and outgoing calls, although incoming call is not
!   currently supported by the network.
!
!   transport input all and transport output all may be used for the purposes of
!   reverse telneting to the cellular modem.
!
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
```

Debugging and Troubleshooting

The following debugging methods are useful for debugging common problems.

- PPP
  - PPP detailed event
  - PPP protocol negotiation
- Chat Script
  - Chat scripts activity debugging

You can ping a destination IP address that is expected to respond and is part of the *interesting traffic* to see if you have connectivity.

Example 4-2 Debug Output for Normal Operation

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The debug output below is typical for a successful call establishment.

```
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
!
!   Upon detecting 'interesting' traffic, the IOS has successfully communicated with the
!   cellular modem, and command it to dial out.
!
*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
!
!   Preparing to start the PPP - LCP (Link Control Protocol) phase
!
*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)
!
!   Outgoing CONFREQ sent out from Cisco IOS to the cellular modem.
!
*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)
!
!   Incoming CONFREQ received by IOS from the cellular modem.
!
*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)
!
!   Outgoing CONFACK sent out from the IOS to the cellular modem.
!
*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)
!
!   Incoming CONACK received by IOS from the cellular modem.
!
*Jun 21 00:45:45.935: Ce0/0/0 LCP: State is Open
!
!   LCP phase completed successfully, and is now OPEN.
!
*Jun 21 00:45:45.939: Ce0/0/0 PPP: Phase is AUTHENTICATING, by the peer.
!
!   Beginning the authentication phase.
!
*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 (Challenge Handshake Authentication Protocol) phase completed successfully, and
!   is now OPEN.

!   This CHAP authentication has only occurred between the IOS and the cellular
!   modem on the 3G-HWIC, and not yet with the network. It is important to remember that
!   the PPP does not terminate on the network; it terminates locally on the modem.
!
!   The cellular network (GGSN) has not yet authenticated the user. The cellular modem
!   then uses 'Activate PDP context' message, over the air, for the purposes of obtaining
!   a IP address from the network, and also for authenticating itself to the network.  The
!   network in turn, responds with 'Activate PDP context Accept' message, authenticating
!   the user, and returning the IP address. The 'Activate PDP context' message contain the
!   CHAP credentials configured under the cellular interface.
!
*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
!
!   Starting NCP [Network Control Protocol]/ IPCP [IP Control Protocol] phase
!
*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)
!
!   IPCP CONFREQ (Configure-Request) sent by Cisco IOS to the modem, requesting host IP
!   address, and the DNS addresses.
!
*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)
!
!   IPCP CONFNAK (Received configuration option is recognizable and acceptable, but some
!   values are not acceptable) sent by the modem to Cisco IOS, in return to the above
!   CONFREQ.
!
!   The modem has not yet been authenticated by the cellular network. The modem is waiting
!   for the 'Activate PDP context Accept' message from the cellular network. The modem is
!   merely returning a response to IOS, containing primary and secondary DNS addresses
!   (these addresses are arbitrary, since the real addresses are provided by the network).
!   For obvious reasons, it does not return any host IP Address to the IOS.
!
*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)
!
!   A new IPCP CONFREQ sent by the IOS to modem, requesting the missing host IP address in
!   the CONFNAK from the modem.
!
*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)
!
!   Modem responds with IPCP CONFNAK, still excluding the requested host IP address.
!
!   The reason for this exclusion is that the modem is still waiting for the 'Activate PDP
!   context Accept' message from the network which would contain these requested
!   parameters.
!
*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 continues sending IPCP CONREQ to the modem.
!
*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)
!
!   Modem responds with IPCP CONFNAK, still once again excluding the requested host
!   IP Address.
!
!   The modem is still waiting for the 'Activate PDP context Accept' message from the
!   network.
!
*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 continues sending IPCP CONREQ to the modem.
!
*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)
!
!   Finally, the modem receives the 'Activate PDP context Accept' message from the
```

```
!   cellular network, which successfully authenticates the modem/IOS, and also provides
!   the host IP address, and the DNS addresses, as received from the network.
!
!   IPCP CONFNAK sent by the modem to IOS, containing these valid addresses received from
!   the network.
!
*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)
!
!   IPCP CONFREQ sent by the IOS to the modem, requesting the suggested host IP address,
!   and the DNS addresses.
!

*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)
!
!   IPCP CONFACK (If all options in the CONFREQ message are recognizable and all values
!   are acceptable, then the router transmits a CONFACK message) sent by the modem to
!   Cisco IOS, accepting the requested host IP address, and the DNS addresses.
!
*Jun 21 00:45:49.267: Ce0/0/0 IPCP: State is Open
!
!   IPCP Phase is now successful, and is OPEN.
!
*Jun 21 00:45:49.291: Ce0/0/0 IPCP: Install negotiated IP interface address
166.138.186.120
!
!   IP address assigned to the cellular interface, and installed in the routing table.
!
```

Example 4-3 Cellular Interface Information for Normal Operation

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The output below shows the typical state of the **show cellular 0/0/0 all** command after a successful call set up.

```
ROUTER#sh cellular 0/0/0 all
!
!   Some of the normally displayed information is excluded, for readability purposes, so
!   as to highlight the important information.
!
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
!
!   Cellular interface is actively connected to the cellular network, with PPP
!   established and IP address assigned, using Profile 1
!
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 =
!
!   Shows information about the type of service (Radio Access Technology), and other
!   cellular information.
!
Radio Information
=================
Current Band = WCDMA 1900, Channel Number = 9721
Current RSSI(RSCP) = -77 dBm
!
!   Shows the Received Signal Strength Indication (an important parameter that determines
!   the radio reception level), and the type of service and radio band being used.
!
Modem Security Information
==========================
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of Retries remaining = 3
!
!   Shows the normal status of the SIM card
!
```

Example 4-4 Debug Output for Failure to Connect and Obtain IP Address for the Cellular Interface and Possible Reasons

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The following debug output is typical for a failure at the IPCP Phase or a failure to obtain the IP address.

```
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
!
!   IPCP started after CHAT, LCP and CHAP are successful
!
*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)
!
!   Modem is not able to successfully establish the PDP context with the cellular network,
!   and therefore unable to get the host IP address, and any other requested parameters,
!   as requested by the PPP.
!
!   The reason for this could be one of the several:
```

```
!       -Poor radio reception
!       -Antenna could be disconnected
!       -Authentication failure with the radio network, possibly due to incorrect/invalid
!       or mis-configured user-name/password, and APN (Access Point Name)
!
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: Failed to negotiate with peer
!
!   IPCP Failed, possibly due to one of the reasons above
!
*Jun 21 22:48:03.823: Ce0/0/0 IPCP: State is Closed
```

Example 4-5 Details of Cellular Interface When Failed to Obtain IP Address

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
ROUTER#sh cellular 0/0/0 all
!
!   Some of the normally displayed information is excluded for readability purposes, so as
!   to highlight the important information.
!

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
!
!   Ensure that the user-name, password, and APN are as provided by your service provider.
!   Also ensure that they are correctly configured, both under the cellular interface, as
!   well as on the modem (using the 'cellular 0/0/0 gsm profile create …' command)
!
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
!
!   This indicates a potential radio level connectivity problem. The modem is not able to
!   communicate with the cellular network - possibly due to very low signal level.
!

Radio Information
=================
Current Band = None, Channel Number = 0
Current RSSI = -110 dBm
!
!   This indicates that the Received Signal Strength Indication (RSSI) is very low
!   (-110 dBm). This is possibly due to antenna disconnection, or due to poor radio
!   reception levels
!

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

Example 4-6 Debug Output for Failure to Dial Out and Possible Reasons

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
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)
!
!   Modem is not responding to the dial out command.
!
!   Denotes a problem with the 'chat-script …' command - possibly incorrectly specified
!dialer string
!
!   A similar problem may be encountered:
!       -If the expected string ('CONNECT') has typo, or that it is not specified as upper
!       case.
```

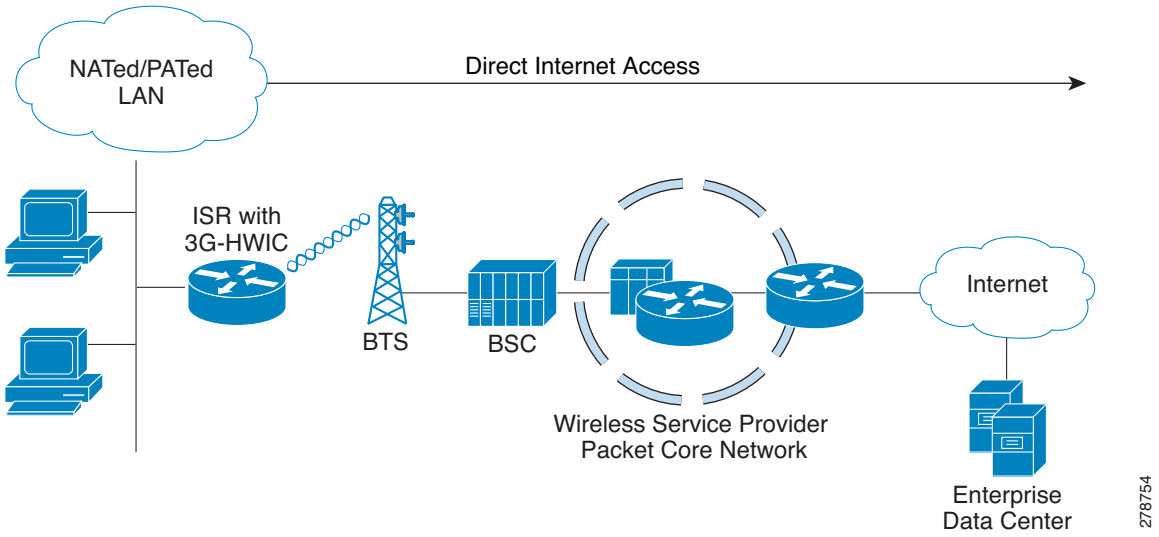
```
!       -If the chat-script command is missing in the configuration
!       -If the 'script dialer …' command is missing on the corresponding line x/x/x
!
```

CDMA Based Wireless Networks

Deployment Using Network/Port Address Translation (NAT/PAT)

Figure 4-2 shows deployment using NAT/PAT. It focuses on a wireless specific configuration. You should familiarize yourself with the 3G wireless specific configuration before reviewing this example for a better understanding. For more information on NAT, see http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6640/product_data_sheet0900aecd8064c999.html.

Figure 4-2 Simple Deployment Using NAT/PAT for CDMA Wireless Networks



Example 4-7 IOS Configuration for Deployment Using NAT/PAT

```
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
!
!   Defines DHCP pool for network 10.3.0.0/16, for hosts connected on VLAN 103, Fast
!   Ethernet ports 0/2/0 thru 0/2/3
!
chat-script cdma2 "" "atdt#777" TIMEOUT 30 "CONNECT"
chat-script cdma1 "" "atdt#777" TIMEOUT 30 "CONNECT"
!
!   Defines dialer strings 'cdma2', and 'cdma1', for a cdma2 wireless network, and cdma1's
!   network respectively. You need to choose one of these chat-script commands, depending
!   on which of these two is your service provider. 'atdt#777' or 'atdt#777' command
!   causes the cellular modem to dial out. In response, the IOS expects the 'CONNECT'
!   string from the modem, upon successful dial out. In this case, IOS waits 30 seconds as
!   timeout, in case of no/unexpected response. Note that the expected 'CONNECT' response
!   from the modem is case sensitive.
!
!
username cisco privilege 15 secret 5 $1$c/5O$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
!
!   DHCP client hosts connected to the above Fast Ethernet ports.
!
!
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
!
!   It is highly recommended that the IP address is always configured as ip address
!   negotiated, even when a fixed (persistent) IP address is required. Cellular interface
!   is spoofed as 'up'/'up' (status/protocol states), regardless of whether the PPP is
!   established or not. If this interface is configured with a specific IP address
!   (instead of 'ip address negotiated'), and if the PPP is not yet established, the
!   routing table will interpret a valid route available via the cellular interface. By
!   assigning a negotiated IP address, this problem is avoided. This is particularly
!   important when using the cellular as a backup interface.
!
!   ip nat outside uses the IP address assigned to the cellular interface, as the source
!   IP address of IP packets going through the cellular interface, and sourced from hosts
!   on VLAN 103.
!
!   dialer in-band configures the interface to support dial on demand routing, and
!   additionally specifies that a chat script will be used for dialing out. In this case
!   it uses the chat script 'cdma1', as defined earlier.
!
!   It is recommended that dialer idle-timeout is set to '0', to avoid disconnection of
!   PPP in the event of no traffic for a specified time, defined by this command. 'dialer
!   idle-timeout 0' sets this timer to indefinite timeout period.
!
!   dialer group and dialer-list are associated commands that allow the specification of
!   'interesting' traffic which will trigger the cellular modem dial out to occur, in
!   order to set up the PPP connection, if it is not yet established.
!
!   ppp ipcp dns-request is an optional command, which allows DNS IP address(es) to be
!   obtained from the cellular network, if required, via the PPP procedures.
!

interface Vlan1
 no ip address
!
interface Vlan103
 ip address 10.3.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
!   Defines interface VLAN 103. This VLAN is used by the associated hosts (on the Fast
!   Ethernet ports). It provides NAT/PAT functionality using the ip nat inside command.
!
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
!
!   Defines the default route via the cellular interface - in this case all IP packets are
!   routed through the cellular interface.
!
ip nat inside source list 2 interface Cellular0/1/0 overload
!
!   Specifies the source of traffic that should be NAT/PATed, via the cellular interface.
!   In this case, it is performing PAT, by using the 'overload' parameter. The source
!   list 2 is associated with the access-list 2 (defined below), which specifies the
!   traffic source of interest (from 10.3.0.0/16 network, in this case).
!
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 command is associated with dialer-group 1 command specified under the
!   cellular interface.
```

```
!
!   access-list 1 command is associated with dialer-list 1 protocol ip list 1 command.
!
!   These commands specify the traffic of interest that will trigger the dial out to occur
!   through the cellular modem, and establish the PPP, if not already established.
!
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
!
!   It is necessary to specify the script dialer command under the corresponding line
!   for the cellular interface. In this case the cellular interface is 0/1/0, and hence
!   the line is also essentially 0/1/0.
!
!   speed can not be configured.
!
!   modem InOut allows incoming/outgoing calls, although incoming call is not currently
!   supported by the network.
!
!   transport input all and transport output all may be used for the purposes of
!   reverse telneting to the cellular modem.
!

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
```

Debugging and Troubleshooting

The following debugging methods are useful for debugging common problems.

- PPP
  - PPP detailed event
  - PPP protocol errors
  - PPP protocol negotiation
- Chat Script
  - Chat scripts activity debugging

Ping a destination IP address that is expected to respond and is part of the *interesting traffic* to see if you have connectivity.

Example 4-8 Debug Output for Normal Operation

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The following debug information is typical for a successful call establishment.

```
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: cdma1 & 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 cdma1 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 cdma1 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
!
!   Upon detecting 'interesting' traffic, the IOS has successfully communicated with the
!   cellular modem, and command it to dial out.
!
*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
!
!   Preparing to start the PPP - LCP phase.
```

```
!
*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)
!
!   Outgoing LCP CONFREQ from IOS to the modem.
!
*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)
!
!   Incoming LCP CONFREQ from modem to Cisco IOS
!
*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)
!
!   Outgoing LCP CONFACK from IOS to modem, acknowledging the CONFREQ from the modem.
!
*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)
!
!   Incoming LCP CONFACK from modem to IOS, acknowledging the CONFREQ from the modem.
!
*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.!
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
!
!   At this point the LCP established. Note the next phase is IPCP, and as far as
!   Cisco IOS is concerned, and NOT CHAP or PAP.
!
*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
!
!   Outgoing IPCP CONFREQ from IOS to modem/network, proposing the IP address for the host
!   (cellular interface), and the DNS IP addresses. Note that the IP address for the host
!   is set to 0.0.0.0 (dynamically assigned IP address), even if a persistent IP address
!   is required from the network.
!
*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)
!
!   Incoming IPCP CONFREQ from modem/network, proposing its own address as received from
!   the network.
!
*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)
!
!   Outgoing IPCP CONFACK from IOS to modem/network accepting the network's address.
!
*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)
!
!   Incoming IPCP CONFNAK from modem/network, in response to the earlier CONFREQ from
!   Cisco IOS.
!
!   CONFNAK proposes the IP address for the host (cellular interface) and the DNS
!   addresses as received from the network as part of the Mobile IP procedure, which
!   occurred between the modem and the network.
!
*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)
!
!   Outgoing IPCP CONFREQ from IOS, in response to the above CONFNAK from the
!   modem/network.
!
!   CONFREQ proposes the same IP address for the host (cellular interface), and the DNS
!   addresses, as contained in the CONFNAK received earlier.
!
*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)
!
!   Incoming IPCP CONFACK from modem/network acknowledging these addresses as acceptable
!   to the modem/network.
!
*Jun 29 15:40:57.904: Ce0/1/0 IPCP: State is Open
!
!   IPCP phase is UP
!
*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
!
!   IP address assigned to the cellular interface, and installed in the routing table.
!

*Jun 29 15:40:58.896: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0/1/0,
changed state to up
```

Example 4-9 Cellular Interface Information for Normal Operation

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The output below shows the typical state of the **show cellular 0/0/0 all** command after a successful call set up.

```
ROUTER#sh cellular 0/1/0 all
!
!   Some of the normally displayed information is excluded, for readability purposes, so
!   as to highlight the important information,.
!
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
!
!   Modem on the HWIC has been activated.
!
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
!
!   -Displays information loaded from the network in modem's NVRAM, for data profile 0,
!   which is not used by the user, but by modem for management purposes.
!   -It displays the NAI
```

```
!   -MN-HA and MN-AAA shared secret values are not displayed
!   -Primary and Secondary Home Agent addresses, used for management purposes, are
!   displayed.
!

Data Profile 1 Information (Active)
==================================
NAI (Network Access Identifier) = productmarketing393@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 = 68.28.81.76
Secondary Home Agent Address = 68.28.89.76
!
!   -Displays information loaded from the network in modem's NVRAM, for data profile 1,
!   which is used by the user.
!   -It displays the NAI
!   -MN-HA, and MN-AAA shared secret values are not displayed
!   -Primary and Secondary Home Agent addresses, used for Mobile IP purposes, are
!   displayed
!
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)
!
!   Displays data connection related information.
!

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#
```

Example 4-10 Debug for Failure to Connect and Obtain IP Address for the Cellular Interface and Possible Reasons

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
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 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#
!
```

```
!   -modem is not responding to the dial out command.
!   -one of the reason could be due to antenna disconnection, or very poor signal
!   reception.
!   -The other possible reason could be due to a problem with the 'chat-script …'
!   command - possibly incorrectly specified dialer string
!   A similar problem may be encountered:
!       -If the expected string ('CONNECT') has typo, or that it is not specified as upper
!       case.
!       -If the chat-script command is missing in the configuration
!       -If the 'script dialer …' command is missing on the corresponding line x/x/x
!
```

Example 4-11 Details of Cellular Interface When Failed to Connect and Obtain IP Address

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
ROUTER#sh cellular  0/1/0 all
!
!   Some of the normally displayed information is excluded, for readability purposes, so
!   as to highlight the important information,.
!

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
!
!   Some of the normally displayed information is excluded, for readability purposes, so
!   as to highlight the important information.
!
```

CHAPTER 5

Advanced Network Deployment Scenarios

Revised: May 6, 2010, OL-22739-01

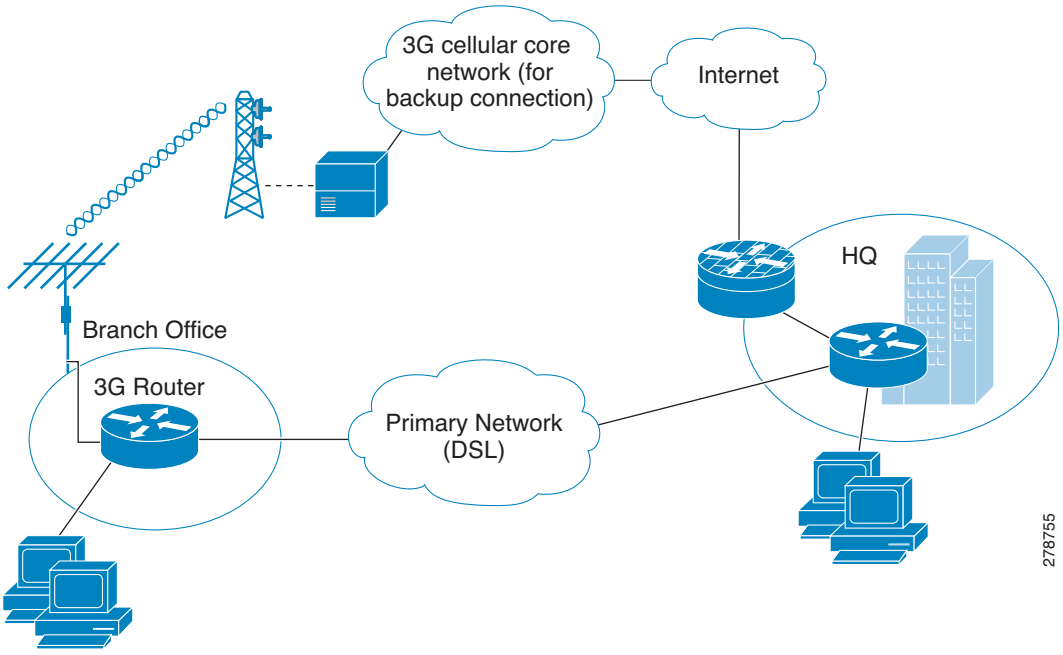
This chapter describes the advanced deployment scenarios. The configurations used for the deployment scenarios throughout this chapter are for GSM. The same configurations can be used for CDMA deployment scenarios, with slight modifications.

Contents

Primary/Backup Deployment Using NAT/PAT and IPSec

Figure 5-1 shows a deployment that uses the DSL interface as a primary link, and the Cellular interface as a backup link. It uses NAT/PAT and IPsec at a branch office for secure communication between the hosts on the branch office router and the hosts at the HQ site via a public network. This deployment also allows non-secure (non IPsec) communication with the hosts on the Internet.

Figure 5-1 Primary/Backup Deployment Using NAT/PAT and IPSec



Configuration for the Branch Office Router

Example 5-1 Configuration for the Branch Office Router

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

Unless otherwise noted, the bold text refers to commands associated with the basic cellular commands. The bold text is also used for other configurations such as the crypto IPsec configuration, the backup configuration, the IP SLA configuration, and the mobile IP configuration. Commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
!   This configuration uses IP SLA, using reliable object tracking. This configuration is
!   optional. It allows tracking the connectivity via the primary (DSL) interface using
!   ICMP pings to some known IP destination address in the outside network via this
!   primary interface. Failure to receive response to pings will cause the default route
!   via the primary interface to be removed from the routing table and the default route
!   (configured with a higher administrative distance) via the Cellular interface will
```

```
!   become the effective path providing the connectivity via the backup path.
!
!   Without this configuration it is still possible to achieve the primary/backup
!   connectivity, using the 'backup interface …' command which detects network
!   connectivity failure at PPP/physical layer and causes switchover to occur to the
!   backup (cellular) interface.
!
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
!   This command basically excludes the assignment of ip address 10.4.0.254 to any hosts
!   since this is used as a default gateway address for connected host on VLAN 104 - Fast
!   Ethernet ports 0/1/0 thru 0/3/0
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   DHCP pool for the hosts connected to the VLAN 104 - Fast Ethernet ports 0/1/0
!   thru 0/3/0
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   Chat script to dial out via cellular interface.
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   Configures tracked object number 234, to track for reachability, using operation 1.
!   The object is 'UP' if reachability condition is met.

!   This is used for the purposes of sending ping packets via the ATM DSL interface (used
!   as a primary link), and monitoring the response, to help determine if switchover (to
!   cellular) is necessary, in the event of no response.
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   Defines the IKE policy (with priority 1), specifies 3DES during IKE negotiation, and
!   authentication as pre-shared, using pre-defined keys. The values for lifetime (set to
!   86,400 sec - one day), group (set to 768 bit Diffie-Hellman), and Hash (set to SHA-1)
!   are set to their default values.
!
!
crypto isakmp key mykey address 20.20.241.234
!
!   Defines the key (mykey) and the IP address of the gateway
!   (IPsec peer) with which the Security Association will be set
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   Defines the transform set (mytransformset), which is an acceptable combination of
!   security protocols, algorithms, and other settings to apply to IPsec-protected
!   traffic.
!
```

```
crypto map gsm1 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address 103
!
!   Defines the crypto map gsm1
!
!   crypto map specifies the traffic to be protected (using match address <access-list>
!   command); the peer end-point to be used, and the transform set to use (mytransformset,
!   defined earlier).
!
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
!
!   Fast Ethernet ports used by DHCP Client hosts.
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   ATM (DSL) physical interface used as primary interface.
!
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
!
!
!   ATM sub-interface to be used for the PVC, as a Primary connection. NAT (outside) will
!   be used on this interface.
!
!   pppoe-client dial-pool-number 2 configures PPP over Ethernet (PPOE) client,
!   specifying the dialer pool 2 to be used. This interface is associated with 'interface
!   Dialer 2', defined below.
!
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
!
!   Applies crypto map gsm1, defined above, on this backup interface.
!
!   dialer-group 1, defines group number 1, which is associated with dialer-list 1...
!   command, specified below, in this configuration. It defines the 'interesting traffic'
!   that triggers the dial out, and places the interface online after establishing the
!   PPP. Note this interface normally remains in a standby state, hence the interesting
!   traffic does not trigger a dial out; rather the traffic already flows through the
!   primary (ATM DSL) interface.
!
!   Defines the interface for NAT, outside.
!
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
!
!   Defines VLAN 104 for the hosts connected on the Fast Ethernet ports 0/1/0 thru 0/1/3,
!   using NAT (inside interface).
!
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 command associates this dialer interface with the ATM sub interface
!   atm0/0/0.1. 'dialer-group 2' defines group number 2, which is associated with
!   dialer-list 2... command, specified below, in this configuration. It defines the
!   'interesting traffic' that triggers the dial out, and places the interface online
!   after establishing the PPP.
!
!   Defines the interface as for NAT, outside.
!
!   Applies crypto map gsm1, defined above, on this primary interface.
!
ip local policy route-map track-primary-if
!
!   Specifies the ip route policy as defined by the route map
!   track-primary-if
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   Defines the default route via Dialer 2 (ATM DSL), specifying the tracking object
```

```
!   (234), defined above.
!
!   The route will only be installed if the tracked object (234) is 'UP'.
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   Defines the default route via the cellular interface, with an administrative distance
!   of 254 (higher then the Dialer 2 interface). This is because this interface is
!   normally supposed to be a backup interface.
!
!
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
!
!   Defines route-map nat2cell (as defined below), as a criteria for the outside NAT
!   traffic, via the cellular interface. 'overload' option causes PAT to be used.
!
!   This command is used, if the criteria as defined by route-map nat2cell is satisfied.
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   Similarly, as above, defines route-map nat2cell (as defined below), for the outside
!   NAT traffic via the Dialer 2 interface (ATM DSL). 'overload' option causes PAT to be
!   used.
!
!   This command is used, if the criteria as defined by route-map nat2dsl is satisfied.
!
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
!
!   Defines the SLA (service level agreement) for sending pings to IP address
!   209.131.36.158, using the Dialer 2 (ATM DSL) as the source interface, at every 2
!   second interval (frequency 2), and wait for 1000 mSec (timeout 1000) for a response to
!   the ping.
!
!   Start the defined SLA, now, and run this for ever
!
access-list 1 permit any
!
!   Associated with 'dialer-list 1 protocol ip list 1' command below
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   Specifies the traffic to match (matches source address for network 10.4.0.0), in order
!   to determine the appropriate outgoing interface, as defined under route maps nat2dsl,
!   and nat2cell.
!
access-list 102 permit icmp any host 209.131.36.158
!
!   Specifies the traffic for route map 'track-primary-interface', so that the ICMP pings
!   are only sent through the ATM DSL interface when this interface is active.
!
!   This specific address is the one that is pinged through the ATM DSL interface (primary
!   link), on a periodic basis, so that network failures, other then at link/PPP level,
!   can also be detected and a switchover may still take place to the cellular (secondary)
!   interface.
!
```

```
!   Ensure that the address that is pinged is reliable and will respond to the ping.
!
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
!
!   Specification of the traffic to be protected for IPsec, as defined under crypto map
!   gsm1.
!
!   The source addresses (166.138.186.119, and 75.40.113.246) are the IP addresses of the
!   cellular interface (secondary), and ATM DSL interface (primary).
!
!   "20.20.0.0 is the destination network) where the corresponding gateway is connected
!
dialer-list 1 protocol ip list 1
!
!   Specifies 'interesting traffic' that will cause the cellular interface to dial out. It
!   further specifies access-list 1 (as part of this command, which is defined above)
!
dialer-list 2 protocol ip permit
!
!   Specifies 'interesting traffic' that will cause the ATM DSL interface (as part of
!   Dialer 2 interface) to dial out.
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
!   Specifies the route-map to be used as a policy criteria,
!   for local routing purpose (see the associated command
!   'ip local policy route-map track-primary-if', above).
!
!   If this is a ping packet for destination 209.131.36.158, and if the interface Dialer 2
!   (ATM DSL) is 'UP' and connected, send the ping packet. This ping packet is only sent
!   via the ATM DSL interface, and not via the cellular interface. The rationale is to
!   periodically monitor connectivity (reach ability) via the ATM DSL interface, so as to
!   perform the switchover when connectivity fails.
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Dialer 2 interface is 'UP' and connected.

!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface Dialer 2 is 'UP' and connected to DSL network,
!   this route map is used by 'ip nat inside source nat2dsl ...' command.
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Cellular interface is 'UP' and connected.
!
!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface cellular is 'UP' and connected to the cellular network, this route map
!   is used by 'ip nat inside source nat2cell ...'
!
!   Clears the NAT entries from the primary/backup interface upon switchover.
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
```

Configuration for the HQ Site Router

Example 5-2 Configuration for the HQ Site Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
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 excluded addresses
!
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
!
!   DHCP pool for hosts on the 20.20 network
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
!   DHCP pool for VPN hosts on the 10.10.0.0 network
!
!
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 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
!
!   Defines the mytunnelcrypto map for IPsec tunnels to the ATM DSL/ and Cellular
!   interface at the remote branch-router.
!
!
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
!
!   Physical interface on which the crypto map is applied. The interface through which the
!   above IPsec tunnels are established.
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!
!   Fast Ethernet ports on which the VPN hosts (on the 10.10.0.0 network) are connected.
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
```

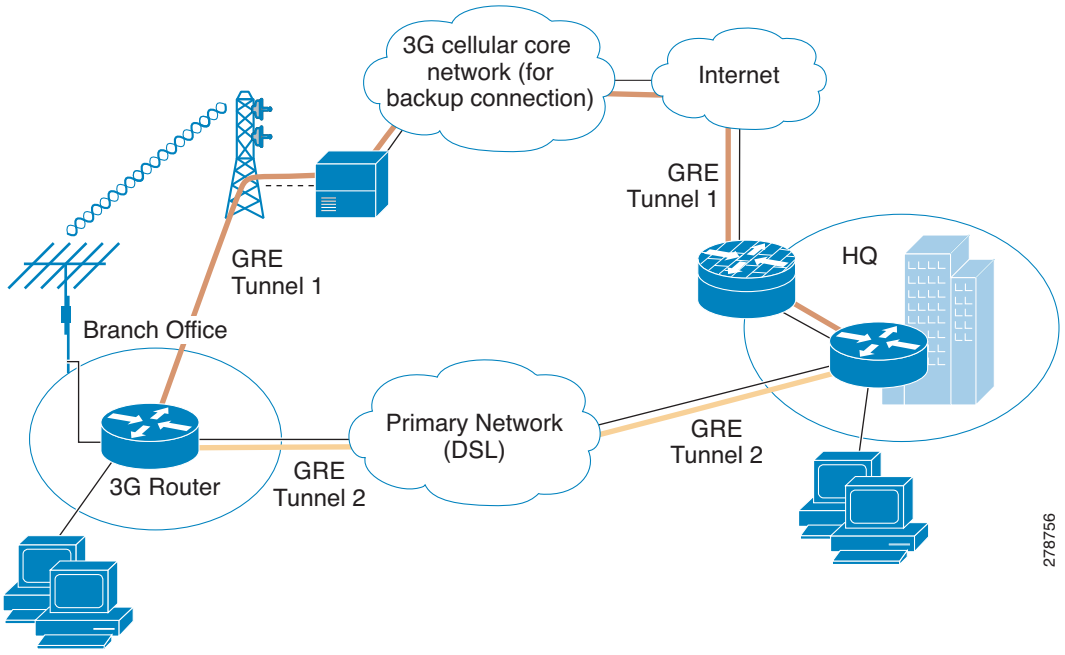
```
!
interface FastEthernet0/3/0
 switchport access vlan 20
 spanning-tree portfast
!
!
!   Fast Ethernet ports on which other hosts (on the 20.20 network) are connected.
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
 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
!
!
!   VLAN for the VPN hosts (on the 10.10.0.0 network)
!
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
!
!
!   VLAN for the other hosts (on the 20.20 network)
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   Default route via the next hop for GigabitEthernet0/0 interface.
!
ip dns server
!
access-list 101 permit ip host 20.20.241.234 host 75.40.113.246
!
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the DSL interface at the remote end.
!
access-list 101 permit ip host 20.20.241.234 host 166.138.186.119
!
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the Cellular interface at the remote end.
!
!
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
```

Primary/Backup Deployment using GRE Tunnels and IPSec

This deployment uses the DSL interface as a primary link, and the Cellular interface as a backup link, using GRE tunnels and IPsec at a branch office, for secure communication between the hosts on the branch office router, and the hosts at the HQ site via public networks. This deployment also allows non-secure (non IPsec) communication with the hosts on the Internet. For more information on the IPSec configuration over GRE tunnel with dynamic routing, see *Configuring a GRE Tunnel over IPsec with OSPF*.

Figure 5-2 Primary/Backup Deployment Using GRE Tunnels and IPsec



Configuration for the Branch Office Router

Example 5-3 Configuration for the Branch Office Router

The blue italicized text throughout this configuration is used to indicate *comments* and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

Unless otherwise noted, the bold text refers to commands associated with the basic cellular commands. The bold text is also used for other configurations such as the crypto IPsec configuration, the backup configuration, the IP SLA configuration, and the mobile IP configuration. Commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The following configuration uses IP SLA, with reliable object tracking. This configuration is optional.

```
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.4.0.254
!
!   This address is used as a default gateway address for connected host
!   on VLAN 104 - Fast Ethernet ports 0/1/0 thru 0/3/0
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   DHCP pool for the hosts connected to the VLAN 104 - Fast Ethernet ports 0/1/0
!   thru 0/3/0
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   chat script to dial out via cellular interface
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   Configures tracked object number 234, to track for reachability, using operation 1.
!   The object is 'UP' if reachability condition is met.
!
!   This is used for the purposes of sending ping packets via the ATM DSL interface (used
!   as a primary link), and monitoring the response, to help determine if switchover (to
!   cellular) is necessary, in the event of no response.
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   Defines the IKE policy (with priority 1), specifies 3DES during IKE negotiation, and
!   authentication as pre-shared, using pre-defined keys. The values for lifetime (set to
!   86,400 sec - one day), group (set to 768 bit Diffie-Hellman), and Hash (set to SHA-1)
!   are set to their default values.
!
crypto isakmp key mykey address 20.20.241.234
```

```
!
!   Defines the key (mykey) and the IP address of the gateway
!   (IPsec peer) with which the Security Association will be set
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   Defines the transform set (mytransformset), which is an acceptable combination of
!   security protocols, algorithms, and other settings to apply to IPsec-protected
!   traffic.
!
crypto map mytunnelcrypto 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address gre-traffic
!
!   Defines the crypto map mytunnelcrypto
!
!   Crypto map specifies the traffic to be protected (using match address <access-list>
!   command); the peer end-point to be used, and the transform set to use (mytransformset,
!   defined earlier).
!
!
interface Tunnel1
 ip unnumbered Dialer2
 ip mtu 1400
 tunnel source Dialer2
 tunnel destination 20.20.241.234
!
!   GRE tunnel for traffic to destination 10.10.0.0 network. Tunnel associated with the
!   ATM DSL (primary) interface. This tunnel is normally 'UP'. The remote tunnel end-point
!   (20.20.241.234) is on the remote VPN Gateway. The local tunnel end-point is the
!   address obtained by the ATM DSL link.
!
interface Tunnel2
 ip unnumbered Cellular0/3/0
 ip mtu 1400
 tunnel source Cellular0/3/0
 tunnel destination 20.20.241.234
!
!   GRE tunnel for traffic to destination 10.10.0.0 network. Tunnel associated with the
!   Cellular (secondary) interface. This tunnel is normally 'Down'. The remote tunnel
!   end-point (20.20.241.234) is on the remote VPN Gateway. The local tunnel end-point is
!   the address obtained by the Cellular link. This tunnel comes 'UP' when a switchover
!   occurs to the Cellular interface.
!
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
!
!   Fast Ethernet ports used by DHCP Client hosts
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   ATM (DSL) physical interface used as primary interface
!
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
!
!
!   ATM sub-interface to be used for the PVC, as a Primary connection. NAT (outside) will
!   be used on this interface.
!
!   pppoe-client dial-pool-number 2 configures PPP over Ethernet (PPOE) client, specifying
!   the dialer pool 2 to be used. This interface is associated with 'interface Dialer 2',
!   defined below.
!
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
!
!   Applies crypto map mytunnelcrypto, defined above, on this backup interface.
!
!   dialer-group 1, defines group number 1, which is associated with 'dialer-list 1 ...'
!   command, specified below, in this configuration. It defines the 'interesting traffic'
!   that triggers the dial out, and places the interface online after establishing the
!   PPP. Note this interface normally remains in a standby state, hence the interesting
!   traffic does not trigger a dial out; rather the traffic already flows through the
!   primary (ATM DSL) interface.
!
!   Defines the interface for NAT, outside.
!
!
interface Vlan104
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
!
!   Defines VLAN 104 for the hosts connected on the Fast Ethernet ports 0/1/0 thru 0/1/3,
!   using NAT (inside interface).
!   NAT/PAT will be used for traffic that is not intended to go via the tunnel(s), to the
```

```
!   20.20.0.0 network on the peer gateway.
!
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 command associates this dialer interface with the ATM sub interface
!   atm0/0/0.1. 'dialer-group 2' defines group number 2, which is associated with
!   'dialer-list 2 ...' command, specified below, in this configuration. It defines the
!   'interesting traffic' that triggers the dial out, and places the interface online
!   after establishing the PPP.
!
!   Defines the interface as for NAT, outside.
!
!   Applies crypto map mytunnelcrypto, defined above, on this primary interface
!
ip local policy route-map track-primary-if
!
!   Specifies the ip route policy as defined by the route map
!   'track-primary-if'
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   Defines the default route via Dialer 2 (ATM DSL), specifying the tracking object
!   (234), defined above.
!
!   The route will only be installed if the tracked object (234) is 'UP'.
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   Defines the default route via the cellular interface, with an administrative distance
!   of 254 (higher then the Dialer 2 interface). This is because this interface is
!   normally supposed to be a backup interface.
!
ip route 10.10.0.0 255.255.0.0 Tunnel1
!
!   Route to the remote 10.10.0.0 VPN network is via the GRE tunnel associated with ATM
!   DSL (primary) interface.
!
ip route 10.10.0.0 255.255.0.0 Tunnel2 254
!
!   Route to the remote 10.10.0.0 VPN network is via the GRE tunnel associated with
!   Cellular (secondary) interface. The administrative distance set to 254 (higher then
!   for the Tunnel1).
!
ip nat inside source route-map nat2cell interface Cellular0/3/0 overload
!
!   Defines route-map nat2cell (as defined below), as a criteria for the outside NAT
!   traffic, via the cellular interface. 'overload' option causes PAT to be used.
!
!   This command is used, if the criteria as defined by route-map nat2cell is satisfied.
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
```

```
!   Similarly, as above, defines route-map nat2cell (as defined below), for the outside
!   NAT traffic via the Dialer 2 interface (ATM DSL). 'overload' option causes PAT to be
!   used.
!
!   This command is used, if the criteria as defined by route-map nat2dsl is satisfied.
!
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-traffic access-list for the protection of IPSec traffic through the GRE tunnels.
!
!   It only protects the GRE tunneled traffic through the DSL/Cellular interface
!   (whichever is the active interface) and the IPsec peer (20.20.241.234) on the remote
!   gateway.
!
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
!
!   Defines the SLA (service level agreement) for sending pings to IP address
!   209.131.36.158, using the Dialer 2 (ATM DSL) as the source interface, at every 2
!   second interval (frequency 2), and wait for 1000 mSec (timeout 1000) for a response to
!   the ping.
!
!   Start the defined SLA, now, and run this for ever
!
access-list 1 permit any
!
!   Associated with 'dialer-list 1 protocol ip list 1' command below
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   Specifies the traffic to match (matches source address for network 10.4.0.0), in order
!   to determine the appropriate outgoing interface, for non-tunneled traffic, as defined
!   under route maps nat2dsl, and nat2cell.
!
access-list 102 permit icmp any host 209.131.36.158
!
!   Specifies the traffic for route map 'track-primary-interface', so that the ICMP pings
!   are only sent through the ATM DSL interface when this interface is active.
!
!   This specific address is the one that is pinged through the ATM DSL interface (primary
!   link), on a periodic basis, so that network failures, other then at link/PPP level,
!   can also be detected and a switchover may still take place to the cellular (secondary)
!   interface.
!
!   Ensure that the address that is pinged is reliable and will respond to the ping.
!
dialer-list 1 protocol ip list 1
!
!   Specifies 'interesting traffic' that will cause the cellular interface to dial out. It
!   further specifies access-list 1 (as part of this command, which is defined above)
!
dialer-list 2 protocol ip permit
!
!   Specifies 'interesting traffic' that will cause the ATM DSL interface (as part of
!   Dialer 2 interface) to dial out.
!
!
route-map track-primary-if permit 10
```

```
 match ip address 102
 set interface Dialer2 null0
!
!   Specifies the route-map to be used as a policy criteria,
!   for local routing purpose (see the associated command
!   'ip local policy route-map track-primary-if', above).
!
!   If this is a ping packet for destination 209.131.36.158, and if the interface Dialer
!   2 (ATM DSL) is 'UP' and connected, send the ping packet. This ping packet is only sent
!   via the ATM DSL interface, and not via the cellular interface. The rationale is to
!   periodically monitor connectivity (reach ability) via the ATM DSL interface, so as to
!   perform the switchover when connectivity fails.
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Dialer 2 interface is 'UP' and connected.
!
!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface Dialer 2 is 'UP' and connected to DSL network,
!   this route map is used by 'ip nat inside source nat2dsl ...' command.
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Cellular interface is 'UP' and connected.
!
!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface cellular is 'UP' and connected to the cellular network, this route map
!   is used by 'ip nat inside source nat2cell ...'
!
!   Clears the NAT entries from the primary/backup interface upon switchover.
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
```

Configuration for the HQ Site Router

Example 5-4 Configuration for the HQ Site Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
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 excluded addresses
!
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
!
!   DHCP pool for hosts on the 20.20 network
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
!
!   DHCP pool for VPN hosts on the 10.10.0.0 network
!
!
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
!
!
!   Defines the mytunnelcrypto map for tunnels to the ATM DSL interface (Tunnel2) and
!   Cellular interface (Tunnel21) at the remote branch-router.
!
!
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
!
!   Tunnel to the ATM DSL interface on the remote branch-router. Normally this is the
!   'active tunnel'.
!
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
!
!   Tunnel to the Cellular interface on the remote branch-router. Normally this tunnel is
!   not active unless connectivity via the DSL interface at the remote end goes down.
!
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
!
!   Physical interface on which the crypto map is applied. The interface through which
!   the above tunnels are established
!
interface GigabitEthernet0/1
 no ip address
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!
!   Fast Ethernet ports on which the VPN hosts (on the 10.10.0.0 network) are connected.
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
```

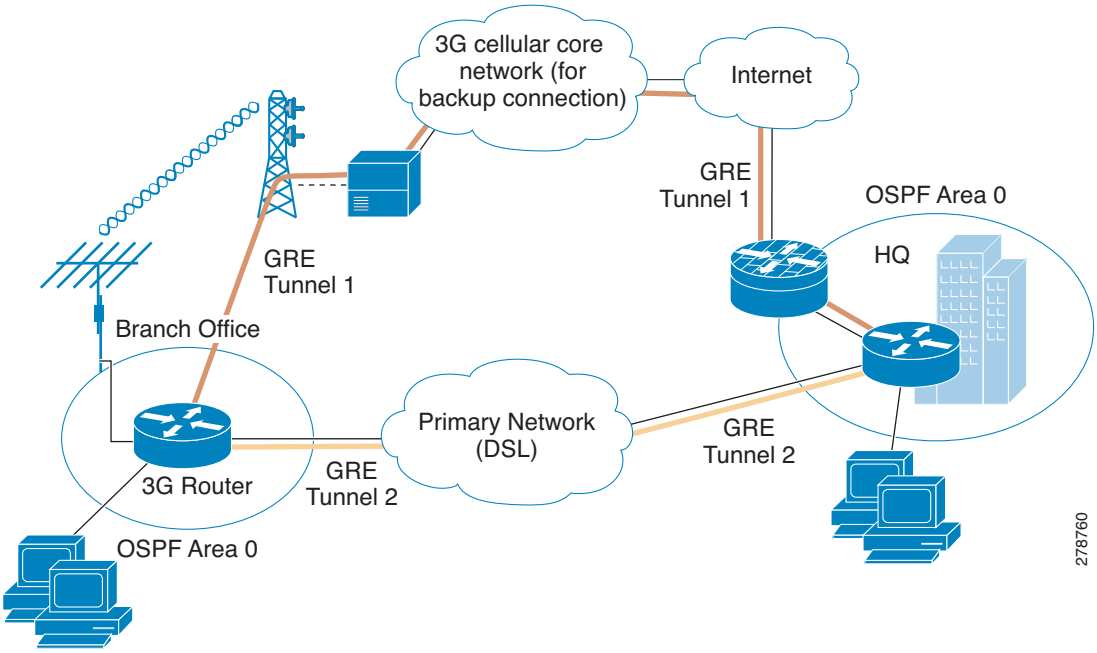
```
!
interface FastEthernet0/3/0
 switchport access vlan 20
 spanning-tree portfast
!
!
!   Fast Ethernet ports on which other hosts (on the 20.20 network) are connected.
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 vlan-range dot1q 1 4095
 exit-vlan-config
 !
!
!   VLAN for the VPN hosts (on the 10.10.0.0 network)
!
interface Vlan20
 description network:20.20.248.224/27
 ip address 20.20.248.254 255.255.255.224
 no ip route-cahe cef
 vlan-range dot1q 1 4095
  exit-vlan-config
 !
!
!   "VLAN for the other hosts (on the 20.20 network)
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   Default route
!
ip route 10.4.0.0 255.255.0.0 Tunnel2
!
!   The route to the remote VPN (10.4.0.0 network) on the branch-router, via the tunnel
!that has the remote end-point on the DSL interface
!
ip route 10.4.0.0 255.255.0.0 Tunnel21 254
!
!   The route to the remote VPN (10.4.0.0 network) on the branch-router, via the tunnel
!   that has the remote end-point on the Cellular interface. This route has a higher
!   administrative distance.
!
ip access-list extended gre-tunnel2
 permit gre host 20.20.241.234 host 75.40.113.246
!
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the DSL interface at the remote end.
!
ip access-list extended gre-tunnel21
 permit gre host 20.20.241.234 host 166.138.186.119
!
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the Cellular interface at the remote end.
!
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
```

Primary/Backup Deployment using GRE Tunnels, IPSec, and OSPF Routing

This deployment uses the DSL interface as a primary link, and the Cellular interface as a backup link, using GRE tunnels, and IPsec at a branch office, for secure communication between the hosts on the branch office router, and the hosts at the HQ site via public networks. It also uses OSPF on the VPN networks (10.4.0.0 and 10.10.0.0 networks) to enable OSPF assisted routing. This deployment allows non-secure (non IPsec) communication with the hosts on the Internet. For more information, see *Configuring a GRE Tunnel over IPsec with OSPF*.

Figure 5-3 Primary/Backup Deployment Using GRE Tunnels, IPsec, and OSPF Routing



Configuration for the Branch Office Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

The configuration below uses IP SLA, using reliable object tracking. This configuration is optional.

Example 5-5 Configuration for the Branch Office Router

```
!
hostname branch-router
!
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 10.4.0.254
!
!   This address is used as a default gateway address for connected host
!   on VLAN 104 - Fast Ethernet ports 0/1/0 thru 0/3/0
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.4.0.254
!
!   DHCP pool for the hosts connected to the VLAN 104 - Fast Ethernet ports 0/1/0
!   thru 0/3/0
!
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 30 "CONNECT"
!
!   Chat script to dial out via cellular interface
!
!
username cisco privilege 15 secret 5 $1$ccw8$TFmKUmI4QVZhOMuxzq/SH/
!
track 234 rtr 1 reachability
!
!   Configures tracked object number 234, to track for reachability, using operation 1.
!   The object is 'UP' if reachability condition is met.
!
!   This is used for the purposes of sending ping packets via the ATM DSL interface (used
!   as a primary link), and monitoring the response, to help determine if switchover (to
!   cellular) is necessary, in the event of no response.
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
!
!   Defines the IKE policy (with priority 1), specifies 3DES during IKE negotiation, and
!   authentication as pre-shared, using pre-defined keys. The values for lifetime (set to
!   86,400 sec - one day), group (set to 768 bit Diffie-Hellman), and Hash (set to SHA-1)
!   are set to their default values.
!
```

```
crypto isakmp key mykey address 20.20.241.234
!
!   Defines the key (mykey) and the IP address of the gateway
!   (IPsec peer) with which the Security Association will be set
!
!
crypto ipsec transform-set mytransformset ah-sha-hmac esp-3des
!
!   Defines the transform set (mytransformset), which is an acceptable combination of
!   security protocols, algorithms, and other settings to apply to IPsec-protected
!   traffic.
!
crypto map mytunnelcrypto 10 ipsec-isakmp
 set peer 20.20.241.234
 set transform-set mytransformset
 match address gre-traffic
!
!   Defines the crypto map mytunnelcrypto
!
!   crypto map specifies the traffic to be protected (using match address <access-list>
!   command); the peer end-point to be used, and the transform set to use (mytransformset,
!   defined earlier).
!
!
interface Tunnel1
 ip unnumbered Vlan104
 ip mtu 1400
 tunnel source Dialer2
 tunnel destination 20.20.241.234
!
!   GRE tunnel for traffic to destination 10.10.0.0 network. Tunnel associated with the
!   ATM DSL (primary) interface. This tunnel is normally 'UP'. The remote tunnel end-point
!   (20.20.241.234) is on the remote VPN Gateway. The local tunnel end-point is the
!   address obtained by the ATM DSL link.
!
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', optional command, suppresses OSPF Hello packets. It helps
!   keep the cellular radio level connectivity from unnecessarily going to 'active' state
!   (from a 'dormant' state), periodically.
!
!   GRE tunnel for traffic to destination 10.10.0.0 network. Tunnel associated with the
!   Cellular (secondary) interface. This tunnel is normally 'Down'. The remote tunnel
!   end-point (20.20.241.234) is on the remote VPN Gateway. The local tunnel end-point is
!   the address obtained by the Cellular link. This tunnel comes 'UP' when a switchover
!   occurs to the Cellular interface.
!
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
!
!   Fast Ethernet ports used by DHCP Client hosts
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   ATM (DSL) physical interface used as primary interface
!
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
!
!
!   ATM sub-interface to be used for the PVC, as a Primary connection. NAT (outside) will
!   be used on this interface.
!
!   'pppoe-client dial-pool-number 2' configures PPP over Ethernet (PPOE) client,
!   specifying the dialer pool 2 to be used. This interface is associated with 'interface
!   Dialer 2', defined below.
!
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' optional command suppresses OSPF Hello packets. It helps keep
!   the cellular radio level connectivity from unnecessarily going to 'active' state (from
!   a 'dormant' state), periodically.
!
!   Applies crypto map mytunnelcrypto, defined above, on this backup interface.
!
!   'dialer-group 1', defines group number 1, which is associated with 'dialer-list 1 ...'
!   command, specified below, in this configuration. It defines the 'interesting traffic'
!   that triggers the dial out, and places the interface online after establishing the
!   PPP. Note this interface normally remains in a standby state, hence the interesting
!   traffic does not trigger a dial out; rather the traffic already flows through the
```

```
!   primary (ATM DSL) interface.
!
!   Defines the interface for NAT, outside.
!
!
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
!
!   Defines VLAN 104 for the hosts connected on the Fast Ethernet ports 0/1/0 thru 0/1/3,
!   using NAT (inside interface).
!
!   NAT/PAT will be used for traffic that is not intended to go via the tunnel(s), to the
!   20.20.0.0 network on the peer gateway.
!
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' command associates this dialer interface with the ATM sub interface
!   atm0/0/0.1. 'dialer-group 2' defines group number 2, which is associated with
!   'dialer-list 2 ...' command, specified below, in this configuration. It defines the
!   'interesting traffic' that triggers the dial out, and places the interface online
!   after establishing the PPP.
!
!   Defines the interface as for NAT, outside.
!
!   Applies crypto map mytunnelcrypto, defined above, on this primary interface
!
router ospf 11
 log-adjacency-changes
 network 10.4.0.0 0.0.0.255 area 0
!
!   VPN network 10.4.0.0 (of which Tunnel1/Tunnel2 are part) is part of OSPF area 0
!
!   OSP Hello will be sent across to branch-router via these tunnels
!
ip local policy route-map track-primary-if
!
!   Specifies the ip route policy as defined by the route map 'track-primary-if'
!
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
!
!   Defines the default route via Dialer 2 (ATM DSL), specifying the tracking object
!   (234), defined above.
!
!   The route will only be installed if the tracked object (234) is 'UP'.
!
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!   Defines the default route via the cellular interface, with an administrative distance
!   of 254 (higher then the Dialer 2 interface). This is because this interface is
```

```
!   normally supposed to be a backup interface.
!
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
!
!   Defines route-map nat2cell (as defined below), as a criteria for the outside NAT
!   traffic, via the cellular interface. 'overload' option causes PAT to be used.
!
!   This command is used, if the criteria as defined by route-map nat2cell is satisfied.
!
ip nat inside source route-map nat2dsl interface Dialer2 overload
!
!   Similarly, as above, defines route-map nat2cell (as defined below), for the outside
!   NAT traffic via the Dialer 2 interface (ATM DSL). 'overload' option causes PAT to be
!   used.
!
!   This command is used, if the criteria as defined by route-map nat2dsl is satisfied.
!
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-traffic' access-list for the protection of IPSec traffic through the GRE tunnels
!
!   It only protects the GRE tunneled traffic through the DSL/Cellular interface
!   (whichever is the active interface) and the IPsec peer (20.20.241.234) on the remote
!   gateway.
!
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
!
!   Defines the SLA (service level agreement) for sending pings to IP address
!   209.131.36.158, using the Dialer 2 (ATM DSL) as the source interface, at every 2
!   second interval (frequency 2), and wait for 1000 mSec (timeout 1000) for a response to
!   the ping.
!
!   Start the defined SLA, now, and run this for ever.
!
access-list 1 permit any
!
!   Associated with 'dialer-list 1 protocol ip list 1' command below
!
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
!
!   Specifies the traffic to match (matches source address for network 10.4.0.0), in order
!   to determine the appropriate outgoing interface, for non-tunneled traffic, as defined
!   under route maps nat2dsl, and nat2cell.
!
access-list 102 permit icmp any host 209.131.36.158
!
!   Specifies the traffic for route map 'track-primary-interface', so that the ICMP pings
!   are only sent through the ATM DSL interface when this interface is active.
!
!   This specific address is the one that is pinged through the ATM DSL interface (primary
!   link), on a periodic basis, so that network failures, other then at link/PPP level,
!   can also be detected and a switchover may still take place to the cellular (secondary)
```

```
!   interface.
!
!   Ensure that the address that is pinged is reliable and will respond to the ping.
!
dialer-list 1 protocol ip list 1
!
!   Specifies 'interesting traffic' that will cause the cellular interface to dial out. It
!   further specifies access-list 1 (as part of this command, which is defined above)
!
dialer-list 2 protocol ip permit
!
!   Specifies 'interesting traffic' that will cause the ATM DSL interface (as part of
!   Dialer 2 interface) to dial out.
!
!
route-map track-primary-if permit 10
 match ip address 102
 set interface Dialer2 null0
!
!   Specifies the route-map to be used as a policy criteria,
!   for local routing purpose (see the associated command
!   'ip local policy route-map track-primary-if', above).
!
!   If this is a ping packet for destination 209.131.36.158, and if the interface Dialer
!   2 (ATM DSL) is 'UP' and connected, send the ping packet. This ping packet is only sent
!   via the ATM DSL interface, and not via the cellular interface. The rationale is to
!   periodically monitor connectivity (reach ability) via the ATM DSL interface, so as to
!   perform the switchover when connectivity fails.
!
route-map nat2dsl permit 10
 match ip address 101
 match interface Dialer2
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Dialer 2 interface is 'UP' and connected.
!
!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface Dialer 2 is 'UP' and connected to DSL network,
!   this route map is used by 'ip nat inside source nat2dsl ...' command.
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/3/0
!
!   Specifies this route map to be used, if it meets the match
!   criteria as defined by access-list 101, above, and, if the
!   Cellular interface is 'UP' and connected.
!
!   If the source of traffic is from 10.4.0.0 network, and if
!   the interface cellular is 'UP' and connected to the cellular network, this route map
!   is used by 'ip nat inside source nat2cell ...'
!
!   Clears the NAT entries from the primary/backup interface upon switchover.
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
```

Configuration for the HQ Site Router

Example 5-6 Configuration for the HQ Site Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
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 excluded addresses
!
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
!
!   DHCP pool for hosts on the 20.20 network
!
ip dhcp pool 10
   network 10.10.0.0 255.255.0.0
   default-router 10.10.0.254
```

```
!
!   DHCP pool for VPN hosts on the 10.10.0.0 network
!
!
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
!
!   Defines the mytunnelcrypto map for tunnels to the ATM DSL interface (Tunnel2) and
!   Cellular interface (Tunnel21) at the remote branch-router.
!
!
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
!
!   Tunnel to the ATM DSL interface on the remote branch-router. Normally this is the
!   'active tunnel'.
!
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
!
!   Tunnel to the Cellular interface on the remote branch-router. Normally this tunnel is
!   not active unless connectivity via the DSL interface at the remote end goes down.
!
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
!
!   Physical interface on which the crypto map is applied. The interface through which the
!   above tunnels are established
!
interface GigabitEthernet0/1
 no ip address
```

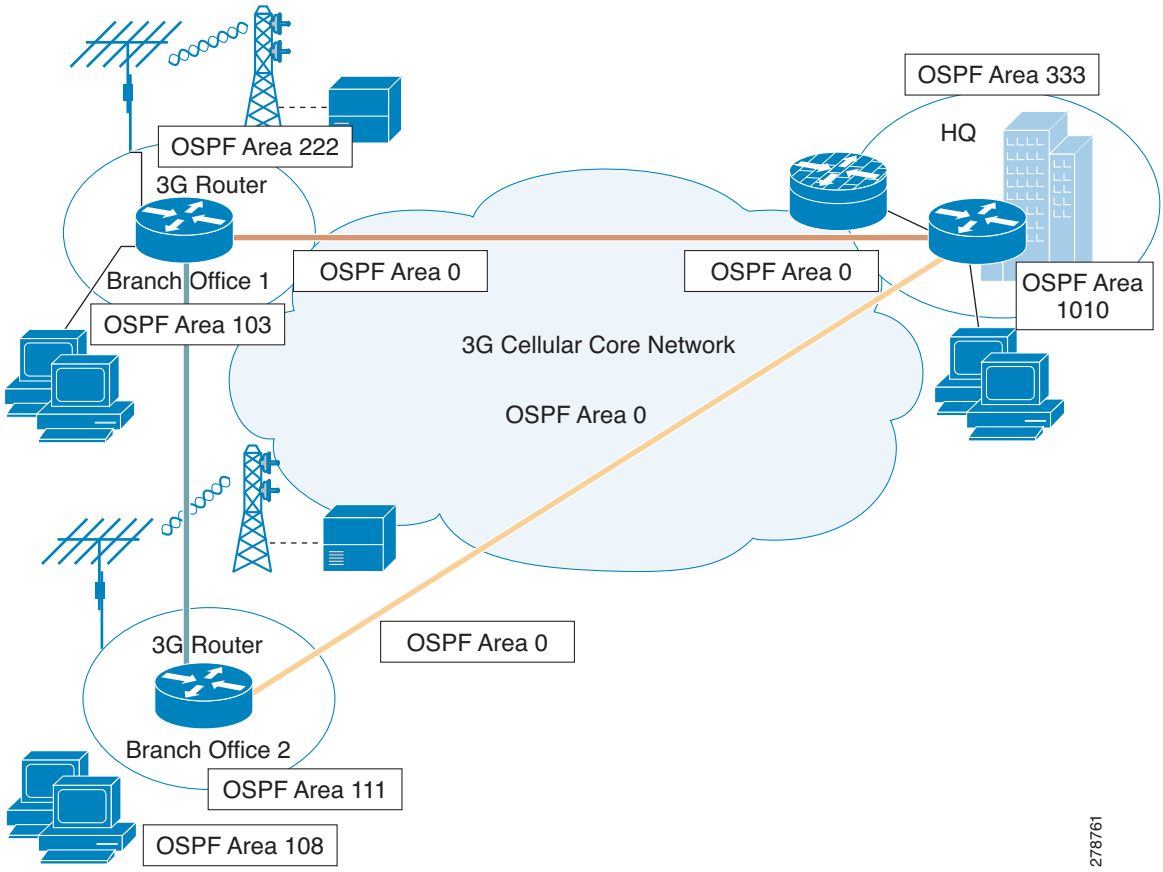
```
 shutdown
!
interface FastEthernet0/1/0
 switchport access vlan 10
 spanning-tree portfast
!
!   Fast Ethernet ports on which the VPN hosts (on the 10.10.0.0 network) are connected.
!
interface FastEthernet0/1/8
 switchport stacking-partner interface FastEthernet0/3/8
!
interface FastEthernet0/3/0
 switchport access vlan 20
 spanning-tree portfast
!
!   Fast Ethernet ports on which other hosts (on the 20.20 network) are connected.
!
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
 !
!
!   VLAN for the VPN hosts (on the 10.10.0.0 network).
!
interface Vlan20
 description network:20.20.248.224/27
 ip address 20.20.248.254 255.255.255.224
 no ip route-cahe cef
 vlan-range dot1q 1 4095
 exit-vlan-config
 !
!
!   VLAN for the other hosts (on the 20.20 network)
!
router ospf 10
 log-adjacency-changes
 network 10.10.0.0 0.0.0.255 area 0
!
!   VPN network 10.10.0.0 (of which Tunnel2/Tunnel21 are part) is part of OSPF area 0
!
!   OSP Hello will be sent across to branch-router via these tunnels
!
ip route 0.0.0.0 0.0.0.0 20.20.241.233
!
!   default route - the next hop for GigabitEthernet0/0 interface.
!
ip dns server
!
ip access-list extended gre-tunnel2
 permit gre host 20.20.241.234 host 75.40.113.246
!
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the DSL interface at the remote end.
!
ip access-list extended gre-tunnel21
 permit gre host 20.20.241.234 host 166.138.186.119
!
```

```
!   Access list defining the traffic that will be protected via IPsec. This is the traffic
!   sent to the Cellular interface at the remote end.
!
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
```

DMVPN Deployment with IPSec and OSPF

This deployment uses Cellular interface as a primary link, using DMVPN (GRE Tunnels) and IPsec for secure communication between the hosts on the branch office router, and the hosts at the HQ site via public networks and OSPF as the routing protocol. For more information on DMVPN, see *Dynamic Multipoint VPN (DMVPN)*.

Figure 5-4 Primary Deployment Using DMVPN with IPSec and OSPF



Configuration for the Branch-1 Office Router

Example 5-7 Configuration for the Branch-1 Office Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
hostname DMVPN_Spoke_1
!
Ip cef
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!
!   ISAKMP policy for phase 1 negotiation
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!   Preshared key for Hub, and remote DMVPN spokes
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   IPsec (Phase 2) policy for actual data encryption/integrity
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
!
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
!
chat-script cdma1 "" "atdt#777" TIMEOUT 180 "CONNECT"
!
username cisco privilege 15 secret 5 $1$c/5O$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
!
!   GRE tunnel template which will be applied to all dynamically created GRE tunnels.
!
!
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
!
!
!   Following cellular config is for dialer persistent. This will always keep the cellular
!   interface up and get an ip address. Dialer pool and dialer pool-member command
!   associate the dialer interface and the cellular interface.
!

!
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
```

Configuration for the Branch-2 Office Router

Example 5-8 Configuration for the Branch-2 Office Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
hostname DMVPN_Spoke_2
```

```
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
!   ISAKMP policy for phase 1 negotiation
!
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!   Preshared key for all the remote DMVPN spokes
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   IPsec (Phase 2) policy for actual data encryption/integrity
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
!
ip cef
!
ip dhcp excluded-address 10.8.0.1
ip dhcp excluded-address 10.8.0.254
!
ip dhcp pool cdmapool
   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$1OLVYb0qkTnZFmkgcCK1L0
!
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
!
!   GRE tunnel template which will be applied to all dynamically created GRE tunnels.
!
!
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
!
!
!   Following cellular config is for dialer persistent. This will always keep the cellular
!   interface up and get an ip address. Dialer pool and dialer pool-member command
!   associate the dialer interface and the cellular interface.
!

!
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
```

Configuration for the HQ Site Router

Example 5-9 Configuration for the HQ Site Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
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
```

```
!
!   ISAKMP policy for phase 1 negotiation
!
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
!   Preshared key for all the remote DMVPN spokes
!
!
crypto ipsec transform-set strong esp-3des esp-md5-hmac
!
!   IPsec (Phase 2) policy for actual data encryption/integrity
!
!
crypto ipsec profile cisco
 set security-association lifetime seconds 86400
 set transform-set strong
!
!   IPsec Profile to be applied dynamically to the GRE over IPsec tunnels
!
!
username cisco privilege 15 secret 5 $1$QF4K$Z1rE.mwS69FVx1e5l9DCU1
!
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
!
!
!   GRE tunnel template which will be applied to all dynamically created GRE
!   tunnels
!
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
```

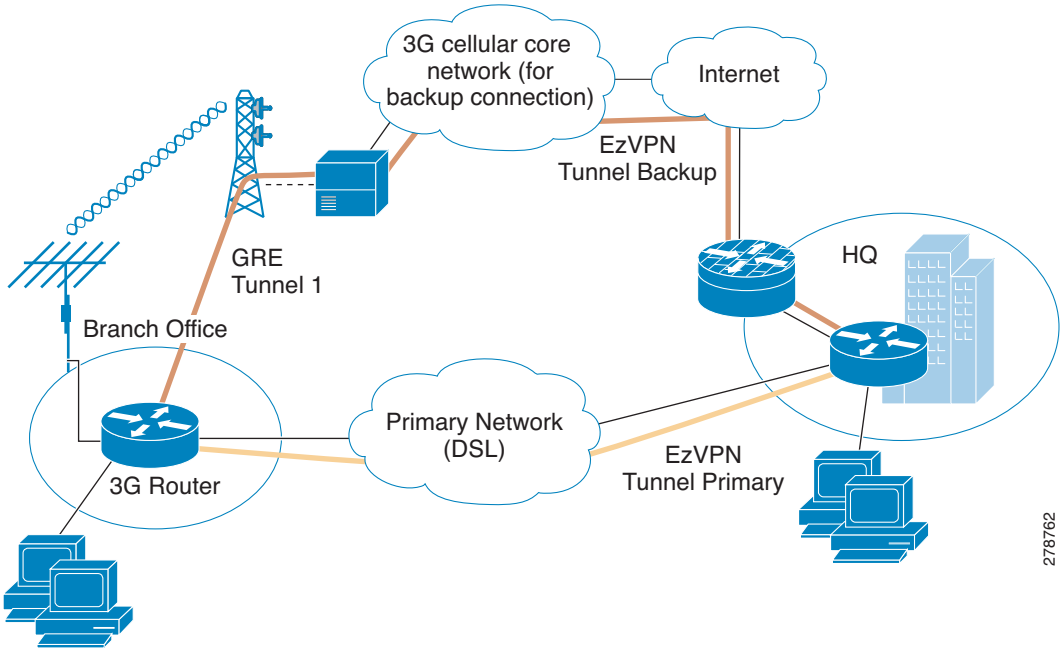
```
 spanning-tree portfast
!
interface FastEthernet0/3/8
 switchport mode trunk
 switchport stacking-partner interface FastEthernet0/1/8
 no cdp enable
!
interface Vlan10
 description private networking vlan
 ip address 10.10.0.254 255.255.0.0
 no ip route-cache cef
!
interface Vlan20
 description network:20.20.248.224,mask:/27,last 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
```

EzVPN Deployment with Primary and Backup Links

EzVPN is specifically designed for ease of deployment and scalability for the HQ-Branch deployment with a large number of branches. This deployment uses the DSL interface as a primary link and the cellular link as the backup link. For more information on EzVPN, see *Cisco Easy VPN*.

Figure 5-5 EzVPN Deployment Using Primary/Backup



Configuration for the EzVPN client (Branch Router)

Example 5-10 Configuration for the EzVPN client (Branch Router)

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
!
hostname branch-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   Chat script to dial out via cellular interface
!
username cisco123@cisco.com password 0 lab
username cisco password 0 lab
username sachin@cisco.com password 0 lab
!
!   Local username and password for authentication for EzVPN client.
!
!
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
!
!   Ezvpn client configuration for Primary WAN interface. Uses track 234 to failover to
!   backup when backup wan is being used
!
!
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
!
!   Ezvpn client configuration for Backup WAN interface
!
```

```
!
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
!
!   Fast Ethernet ports used by DHCP Client hosts.
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   ATM (DSL) physical interface used as primary interface
!
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
!
!   Defines VLAN 104 for the hosts connected on the Fast Ethernet ports 0/1/0 thru 0/1/3,
!   to be part of the internal interface for EZVPN encryption.
!
interface Dialer1
```

```
 ip address negotiated
 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
!
!   External dialer interface to associate with the cellular interface
!
!   crypto ipsec client ezvpn hw-client defined above, on this backup interface. This
!   ensures that this is external interface for ezvpn for encryption
!
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
!
!
!   Defines the outside EzVPN interface for primary WAN.
!
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
```

Configuration for the EzVPN Server Router

Example 5-11 Configuration for the EzVPN Server Router

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

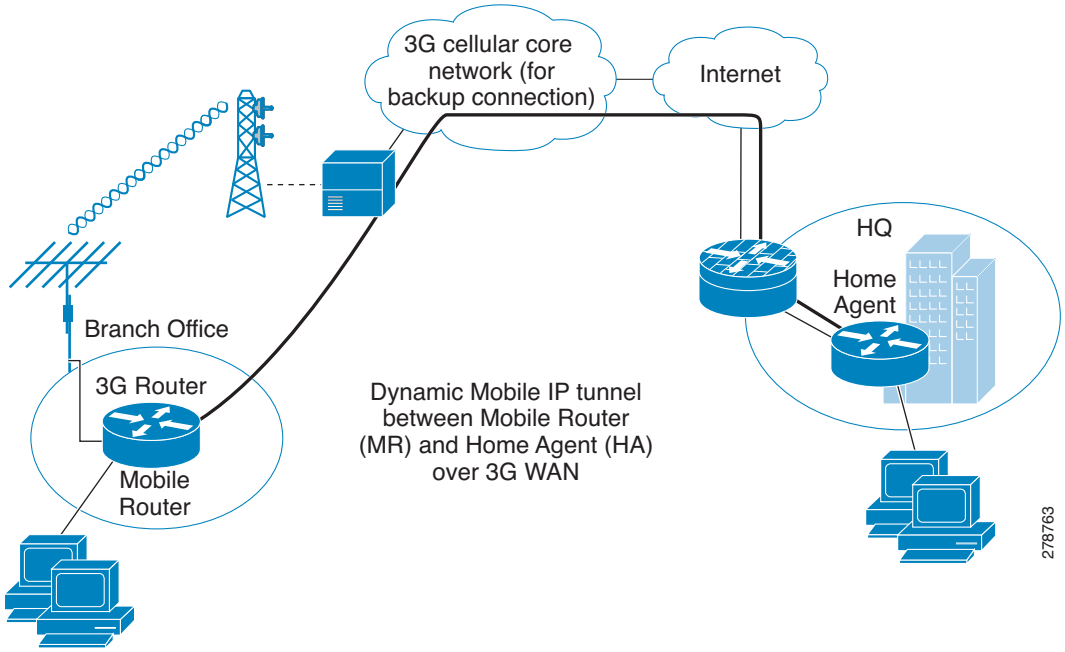
```
hostname ezvpn_gw
!
ip cef
!
username cisco123@cisco.com password 0 lab
username sachin@cisco.com password 0 lab
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 1800
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration 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
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!   EZVPN server side configuration. ACL 111 defines the allowed traffic to be encrypted
!   from the ezvpn client and is negotiated during IPSec tunnel setup
!
!
interface GigabitEthernet0/0
 ip address 128.107.248.243 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
 crypto map dynmap
!
!
!   Crypto map is applied on the WAN interface of the server.
!
!
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
!
!   Define the local pool to give IP address to the remote ezvpn clients.
!
!
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
!
!   Defines interesting traffic that should be allowed to be encrypted for the ezvpn
!   remote clients. The counterpart of such acl is communicated to the ezvpn remote client
!   for encryption and NAT.
!
!
control-plane
!
!
!
line con 0
 exec-timeout 0 0
 exec prompt timestamp
line aux 0
line vty 0 4
 login
!
end
```

NEMO Over 3G with CCOA-Only Mode

Network Mobility (NEMO) is a scalable option that can be used to deploy multiple branches as stub networks across wide geographic areas. All the branches act as mobile networks connected behind the branch router and establish all the connectivity by dynamic mobile IP tunnels over the WAN link. The example configuration below shows the mobile IP in collocated care of address only (CCOA-only) mode, where the Foreign Agent (FA) is absent. For more information on NEMO deployment in the branch, see *Introduction to Mobile IP*.

Figure 5-6 NEMO Deployment Over 3G WAN



Configuration for the Mobile Router (MR) at the Branch Office

Example 5-12 Configuration for the Mobile Router (MR) at the Branch Office

```
!
hostname mobile-router
!
ip cef
!
ip dhcp excluded-address 10.13.0.254
!
ip dhcp pool gsmpool
   network 10.4.0.0 255.255.0.0
   dns-server 66.209.10.201 66.102.163.231
   default-router 10.13.0.254
!
chat-script gsmscript "" "atdt*98*1#" TIMEOUT 20 "CONNECT"
!
!   Chat script to dial out via cellular interface
!
track 234 rtr 1 reachability
```

```
!
!   Object tracking for backup method.
!
interface Loopback100
 ip address 10.100.0.3 255.255.255.0
!
!   Static ip address assigned to the mobile router. This address is part of the HA-MR
!   subnet
!
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
!
!   Fast Ethernet ports used by DHCP Client hosts
!
interface ATM0/0/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
!   ATM (DSL) physical interface used as primary interface.
!
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
!
!   Using external dialer (dialer 1) for mobile ip deployment, dialer pool-member 1
!   associates cellular interface to the dialer 1 where dialar pool 1 is configured
!
!
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
!
!   Defines VLAN 104 for the hosts connected on the Fast Ethernet ports 0/1/0 thru 0/1/3,
!   this subnet will be the mobile network behind mobile router.
!
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
!
!   External dialer interface associated with the cellular with the mobile
!   ip ipconfiguration for ccoa-only mobile ip mode.
!

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
!
!   This commands turns on the mobile ip functionality on the router
!

!
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
!
!   This statement defines the encryption details and authentication using ascii value.
!   The ascii value must match to that of the HA configuration on the HQ side router
!
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
!
!   Address defines the Mobile router static ip address defined on the loopback 100
!
!   Home agent address is defined so the router knows who to initiate the mobile ip
!   request to.
```

```
!

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
```

Configuration for the Home Agent (HA) Router at HQ

Example 5-13 Configuration for the Home Agent (HA) Router at HQ

The blue italicized text throughout this configuration is used to indicate comments and will not be seen when a normal console output is viewed. The bold text is used to indicate important commands to refer back to in case of an error. When debugging, ensure that all the commands in bold are the same in your console output.

The bold text is used to call out the basic cellular configuration, the crypto IPsec configuration, the IP SLA backup configuration, and the mobile IP configuration. The comments below each of the commands associated with each of these configurations will be called out throughout the example for ease of reference when debugging.

```
hostname HQ-HomeAgent
!
ip cef
!
interface Loopback100
 ip address 10.100.0.1 255.255.255.0
!
!   Mobile IP Subnet between the Home-agent (HA) and Mobile router (MR)
!
interface GigabitEthernet0/0
 ip address 128.107.248.243 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
!
!   This is the WAN interface connecting to Mobile routers over internet
!
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
!
!   Enable mobile ip on HA router
!
!
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
!
!   Home agent configuration
!
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
!
!   Mobile router entry for registration
!
```

```
ip mobile secure host 10.100.0.3 spi decimal 1003 key ascii 1234567891234563 algorithm md5
mode prefix-suffix
ip mobile registration-lifetime 1800
!
!   Mobile router authentication (same ascii configured as that on the MR) and encryption
!   details for secure communication
!
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

Glossary

Revised: May 6, 2010, OL-22739-01

3G—Third generation technology in the context of mobile phone.technology. The services associated with 3G include wide-area wireless voice telephony and broadband wireless data within a mobile environment.

3GPP—3rd Generation Partnership Project.

3GPP2—3rd Generation Partnership Project 2.

ACL—Access Control Lists.

BTS—Base Station Transceiver System.

CDMA—Code Division Multiple Access.

CDMA2000—Hybrid 2.5G/3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio, to send voice, data, and signaling data (such as a dialed telephone number) between mobile phones and cell sites. CDMA2000 is considered a 2.5G protocol in 1xRTT and a 3G protocol in EVDO.

CHAP— Challenge Handshake Authentication Protocol.

EDGE—Enhanced Data rates for GSM Evolution (EDGE) or Enhanced GPRS (EGPRS).

EVDO—Evolution-Data Optimized or Evolution-Data only.

GGSN—GPRS support node.

GPRS— General Packet Radio Service.

GSM—Global System for Mobile Communications.

HA—Home Agent.

HSDPA—High-Speed Downlink Packet Access or High-Speed Downlink Protocol Access.

HWIC—High-speed WAN Interface Card.

IPCP— IP Control Protocol.

MIP—Mobile Internet Protocol.

NAI—Network Address Identifier.

PCF—Packet Control Function.

PDP—Packet Data Protocol.

PDSN— Packet Data Serving Node.

PPP—Point to Point Protocol.

PSTN—Public Switched Telephone Network.

QoS—Quality of Service.

RAN—Radio Access Network.

SGSN—Serving GPRS Support Node.

SIM—Subscriber Identity Module.

SIP—Simple Internet Protocol.

SMB—Small to Medium Business.

UMTS—Universal Mobile Telecommunications System is one of the 3G mobile phone technologies.

WCDMA—Wideband Code Division Multiple Access.

Wi-Fi—Wireless Fidelity.