

Mobile IP Simulator for the Agilent E5515C

Software Concepts, Inc

Mobile IP Simulator for the Agilent E5515C

by Software Concepts, Inc

Third Edition

Published 2006-1-24

Copyright © 2006 Software Concepts, Inc.

This is the user manual for the MIP-5800 and MIP-5850 Mobile IP Simulator. The document is specific to the Agilent E5515C RF test set and explains the installation and operation of the Mobile IP Simulator in that environment. The user is expected to have a familiarity with the Agilent E5515C and Mobile IP technology in general.

Copyright and License

All Rights Reserved

This product includes open source software developed by the Apache Software Foundation, the NetBSD Foundation, Inc., the OpenSSL Project, the University of California, Berkeley, and other contributors. Complete copyright information and acknowledgments are embedded in the product at <http://IP address of MOB-IP-SIM/copyright>.

Many product designations are claimed as trademarks or service marks. Where such designations appear in this manual, they are represented by capitals or initial capitals.

All copyrights are held by their respective owners unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark nor should the naming of particular products or brands be seen as endorsements.

Software Concepts, Inc. assumes no responsibility for errors or omissions in this publication, or for any damage resulting from any information contained herein.

Software Concepts, Inc. guarantees the Mobile IP Simulator to be free from defects in material and workmanship for one year from purchase.

Tampering, misuse, or modification shall void this agreement, as does damage caused by external overloads such as lightning or power source surges, or any acts of nature. In the event of failure we will at our discretion repair or replace the failed material upon prepaid return to the factory.

Table of Contents

Preface	7
1. Introduction	9
2. Installation	15
3. Configuration	17
Simulator Configuration.....	17
Configuration Menu.....	17
Network Configuration	19
PPP Configuration	22
MIP-5850 PPP Configuration.....	25
MIP-5800 Mobile IP Configuration	27
MIP-5850 Mobile IP Configuration	30
NAT Configuration	35
HTTP Proxy Configuration	37
E5515C Configuration	40
Mobile Device Configuration.....	41
Testing the Configuration.....	41
4. Logging	43
Logs Pages	43
tcpdump (show packet contents)	43
tcpdump (don't show packet contents).....	44
Agent-Advertiser Log.....	45
Foreign Agent Log	46
Access Log	47
Error Log	48
HTTP Proxy Log	49
System Log.....	50
5. Online Information	53
A. Uploading Procedures	55
B. AT Commands	57
Command Descriptions.....	59

C. CD Contents73
D. E5515C Interconnection.....75
E. Simulator Configuration Worksheet77
F. Manual MOB-IP-SIM Configuration.....79
Colophon.....81
Index.....83

List of Figures

1-1. MOB-IP-SIM Overview	9
1-2. MOB-IP-SIM Component Diagram.....	10
3-1. Mobile IP network simulator page	18
3-2. Configuration menu page	18
3-3. Network configuration page	20
3-4. MIP-5800 PPP configuration page.....	23
3-5. MIP-5850 PPP configuration page.....	26
3-6. MIP-5800 Mobile IP configuration page.....	28
3-7. MIP-5850 Mobile IP configuration page (advertiser)	31
3-8. MIP-5850 Mobile IP configuration page (home agent)	34
3-9. NAT Configuration menu page.....	36
3-10. HTTP Proxy Configuration menu page.....	38
4-1. Logs page	43
4-2. tcpdump (show packet contents) page.....	44
4-3. tcpdump (don't show packet contents) page	45
4-4. Agent-Advertiser log page	46
4-5. Foreign agent log page	47
4-6. Access log page.....	48
4-7. Error log page.....	49
4-8. HTTP proxy log page	50
4-9. System log page.....	51
5-1. Mobile IP network simulator page	53
D-1. MOB-IP-SIM / E5515C Interconnection diagram	75
D-2. MOB-IP-SIM / E5515C Interconnection diagram for hybrid mode	75

Preface

This manual is meant to provide the information required to fully utilize the Mobile IP Simulators from Software Concepts. It does not discuss the theory or standards upon which mobile IP depends, but succinctly presents the procedures required to accomplish your job. In short, resort to the manual when you need to perform a specific task. The tasks discussed include:

- Unpacking the required equipment
- Setting up the test system hardware
- Configuring the simulator, RF test set, and Mobile IP device
- Understanding the logs written by the MOB-IP-SIM
- Modifying the MOB-IP-SIM content and operating system

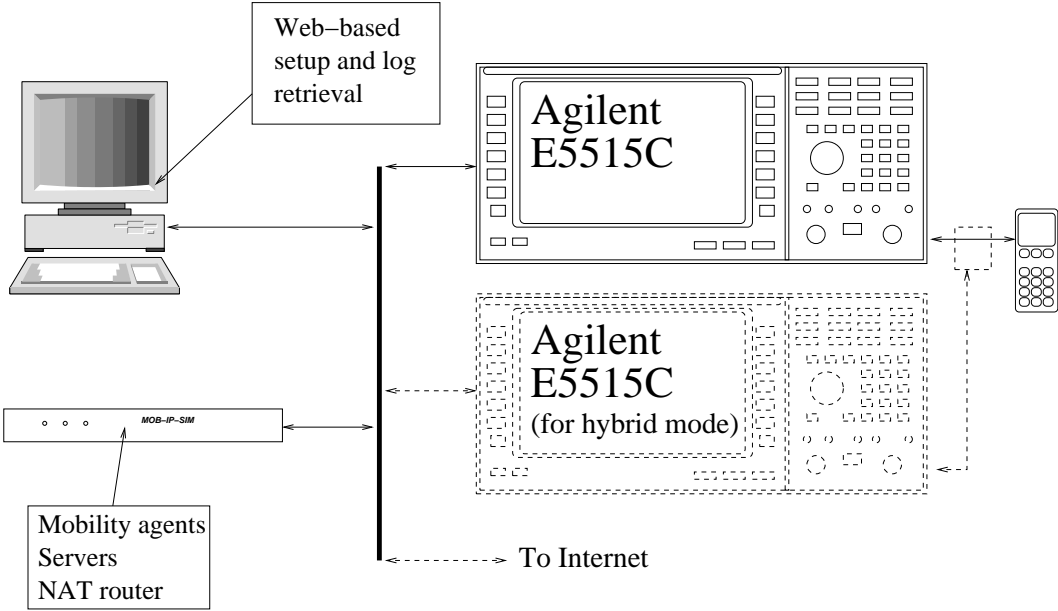
Chapter 1. Introduction

This chapter will:

- Describe what the MOB-IP-SIM can do
- Describe how the MOB-IP-SIM does its job

By simulating the Foreign Agent and Home Agent required for a Mobile IP connection, the Mobile IP Simulator (MOB-IP-SIM) provides the tools needed for complete developmental testing of wireless devices using Mobile IP as the high-speed data interconnectivity protocol. The wireless device can access web content supplied by the MOB-IP-SIM for testing specific features or can access the Internet by means of the simulator. Two models are available: The MIP-5800 provides the minimum set of configuration parameters needed to support Mobile IP connectivity under standard network conditions, while the MIP-5850 provides additional configuration parameters to allow network error simulation and system configuration control. The MIP-5850 is designed for Mobile IP protocol development and supports test features required to verify compliance with the IS-835 standard. Refer to Figure 1-1 for a conceptual overview of the system.

Figure 1-1. MOB-IP-SIM Overview



The previous figure shows the complete Mobile IP network test system. The Agilent E5515C communications test set provides the required cdma2000 or 1xEV-DO radio network emulation and control, containing the radio link, call setup, and Inter-Working Function (IWF) needed for packet data communications. A second E5515C may be connected for hybrid cdma2000/1xEV-DO testing of a single mobile station. The MOB-IP-SIM supports only a single mobile station; therefore, this configuration is useful only for hybrid-mode testing. The MOB-IP-SIM provides the additional IP network elements needed to complete the Mobile IP network simulation environment, namely the simulated PDSN, Foreign Agent (FA), and Home Agent (HA).

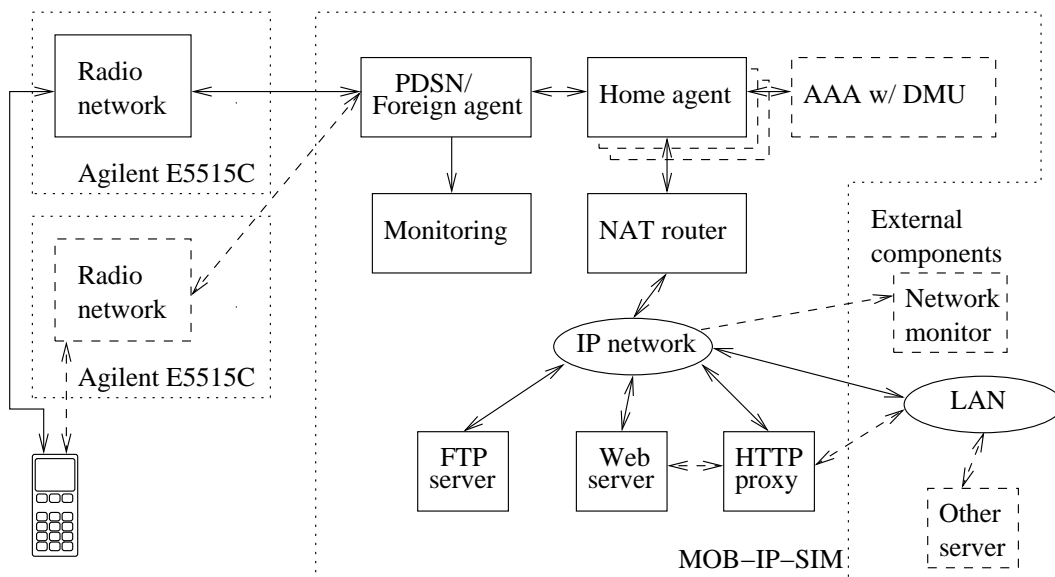
The combination of the E5515C and the MOB-IP-SIM therefore provides a complete solution for Mobile IP connectivity and testing, allowing you to choose levels of features that range from basic connectivity to semi-automated conformance testing.

The simulator is contained in a small enclosure with serial port and LAN connectors. PPP data running over the LAN interfaces the Mobile IP simulator to a cdma2000 or 1xEV-DO communication test set and supports Mobile IP for a single device. The LAN connection provides a web-based user interface to configure the simulator as well as a text-based command port. Configuration requires setting the MOB-IP-SIM to match your specific LAN connection, setting the PPP links for Simple IP and Mobile IP provisioning and operation, and setting up the NAT router. The user interface also provides access to system and data logs and online documentation.

The relationship of the various components required to set up an end-to-end data call is indicated in

Figure 1-2.

Figure 1-2. MOB-IP-SIM Component Diagram



The mobile station makes a data call or session to the Agilent E5515C, which forwards the data to the MOB-IP-SIM's internal PDSN. If the mobile supports hybrid mode, it can maintain a registration on a cdma2000 network and a data session on a 1xEV-DO network simultaneously; to test this behavior, two E5515C sets are required. The PDSN handles the PPP frames and forwards registration and user data messages between the home agent and the radio network. In hybrid mode, this includes keeping track of which radio network the mobile is using.

The home agent processes registration requests, consulting the AAA to decide how to handle them. It also forwards the user data to the IP network. The MIP-5850 supports simulation of three home agents; the MIP-5800 supports only one.

The AAA examines each incoming registration request and decides, based on the authenticator and timestamp, whether to accept or reject it. In addition, the AAA can perform dynamic mobile-IP key update (DMU), which uses public-key cryptography to set up the shared MN-HA, MN-AAA, and CHAP keys securely.

The MOB-IP-SIM includes a router with optional network address translation (NAT). NAT mapping allows the mobile station to share the MOB-IP-SIM's address when contacting external servers, so the MOB-IP-SIM and mobile need only one IP address on your LAN. The drawback to this mode is that servers on the LAN cannot initiate connections to the mobile, as the MOB-IP-SIM would receive the

connection attempts. NAT redirection allows you to redirect the mobile's connection requests to the server of your choice. This can be useful when testing mobiles or applications with hard-coded IP addresses.

The MOB-IP-SIM includes an FTP server and an HTTP server, into which you can upload your own content for testing. See Appendix A for details. In addition, the HTTP server is used to configure everything. See Chapter 3.

The HTTP proxy allows mobiles with HTTP mini-browsers (also known as WAP 2) to communicate with HTTP origin servers. It translates GIF images to PNG as required. The proxy can modify the requested URL before sending the request. This allows testing mobiles or applications with hard-coded URLs. The URL rewriting mechanism is described in detail in the Section called *HTTP Proxy Configuration* in Chapter 3. The proxy can communicate directly with an origin server, or it can use another proxy if required by local network policy.

If you need functionality beyond basic HTTP and FTP service, you can connect the MOB-IP-SIM to external servers, either on your local network or elsewhere on the Internet.

The MOB-IP-SIM provides three types of access to network packets. PPP frames in transit between the mobile station and the PDSN are captured in a file for inspection with any network analyzer that supports tcpdump format. All Ethernet frames between the MOB-IP-SIM and the Ethernet are repeated out a second network port for capture and analysis (see Appendix D. In addition, the MIP-5850 has AT commands to capture and analyze PPP frames.

The MOB-IP-SIM must be configured to work within the bounds of your local area network. This configuration, covered in Chapter 3, sets up access to the external Internet and provides routing connections to other entities that you may plan to use as part of your wireless IP test environment. Setup is accessed through any standard Internet browser connected to the LAN where the simulator is installed. The MIP-Manager, a simulator setup utility, is included on the accompanying CD to assist with the initial installation.

The MIP-5800 simulator provides web-based user access to the basic parameters needed to provision the mobile device for Simple IP and Mobile IP operation.

The MIP-5850 simulator provides dynamic control of many additional test parameters that can be modified prior to a data connection attempt or during the data connection in some cases. The most common setup parameters can be set using the web-based interface, while more complex controls must be changed using "AT" commands sent from a terminal or conformance test script.

The following table indicates the features supported by the two models of the Mobile IP Simulator.

Table 1-1. Features Matrix

Feature	MIP-5800	MIP-5850
Built-in NAT Routing	Yes	Yes
Built-in HTTP Proxy Server	Yes	Yes
Built-in Web Server	Yes	Yes
Built-in FTP Server	Yes	Yes
Status & Activity Logging	Yes	Yes
PPP Logging: (Includes PPP, IP, UDP, Mobile IP layers)	Yes	Yes
Registration Request: Automatic MD5 or HMAC-MD5 with or without SPI authentication	Yes	Yes
Primary HA Simulation	Yes	Yes
Secondary HA Simulation	No	Yes
Agent Advertisement: Configurable delay, # of repeats and delay between repeats	No	Yes
Agent Advertisement: Configurable Lifetime, Pref. Reg. Lifetime, care-of address, & bit options	No	Yes
Registration Response: Configurable Lifetime & Code	No	Yes
"AT" command set to support hand-off control, remote test configuration, and log search	No	Yes
PPP: Configurable CHAP or PAP authentication for Simple IP	No	Yes
DMU	No	Option

Chapter 2. Installation

This chapter will tell you:

- How to confirm you that have all the components of the MOB-IP-SIM
- What additional components you are required to supply
- How to connect the MOB-IP-SIM to your RF test set
- How to install the MOB-IP-SIM Manager configuration utility

Carefully unpack your MOB-IP-SIM and inspect for any damage. You should have one each of the following:

- Main MOB-IP-SIM unit (Either MIP-5800 or MIP-5850)
- DE-9 to DE-9 null-modem serial cable
- Category 5 10BaseT cable for connecting the MOB-IP-SIM to the LAN
- External 12VDC power supply
- MOB-IP-SIM CD-ROM
- This manual

You are expected to provide the following items:

- Agilent E5515C RF Test Set(s) with the E6702B cdma2000 lab application software and/or the E6706A 1xEV-DO lab application software
- A Windows PC with free serial and Ethernet ports

There is no need to open the MOB-IP-SIM enclosure since all configuration is done using software interfaces.

Since the MOB-IP-SIM is a feature extension product designed to be used with the Agilent E5515C, installation and operation will require reference to the Agilent documentation for those procedures outside the scope of this document.

After reviewing the connection diagram in Appendix D, install the MOB-IP-SIM Manager setup utility found on the accompanying CD-ROM by running `setup.exe` located in the `MobIpSimManager` folder.

Open the MOB-IP-SIM Manager from your PC by using the Windows Start menu. When the Options screen appears, click on the LAN Setup button and follow the instructions to configure the LAN

parameters. The manager will instruct you to power-on the unit, connect cables, etc. at the appropriate time. When the setup is complete, the MOB-IP-SIM will have been assigned a specific IP address. Record the MOB-IP-SIM IP address in section [B] of Appendix E.

The IP address may be set without the MOB-IP-SIM Manager by following the procedure in Appendix F.

Note: Do not connect anything until so instructed by the MOB-IP-SIM Manager software.

Chapter 3. Configuration

This chapter will teach you:

- How to configure the MOB-IP-SIM for use
- How to set up your wireless device for testing
- How to initiate a Mobile IP connection

Simulator Configuration

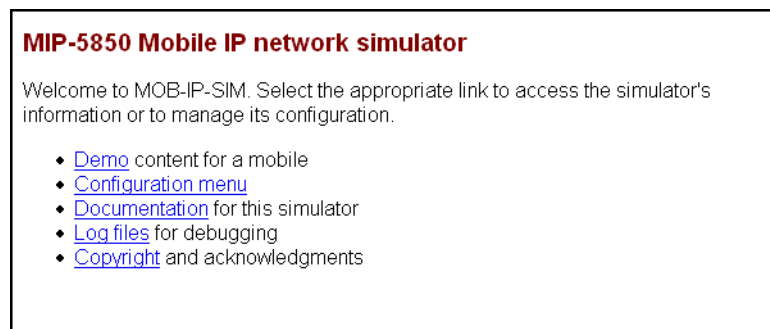
This section outlines the setup of the the MIP-5800 and MIP-5850 simulators. As the MIP-5800 has a reduced functionality when compared to the MIP-5850, some pages are available only to users of the MIP-5850, and will be so specified as appropriate. Access to all operational configuration is accomplished by these pages. Some information retrieval will be accomplished by accessing the Log Pages as described in Chapter 4

Configuration Menu

Once the initial IP address is set, record the provisioning information in sections [A] and [C] of Appendix E) for the Mobile IP enabled wireless device that you plan to test. A manufacturer's programming tool is typically required to access this information.

After pointing your web browser to `http://mobipsimaddress`, where `mobipsimaddress` is the address recorded in section [B] of the worksheet, you should see the page indicated in Figure 3-1. Access to the simulator documentation, debugging and operation logs, copyright information, and demonstration web content are also available on this page.

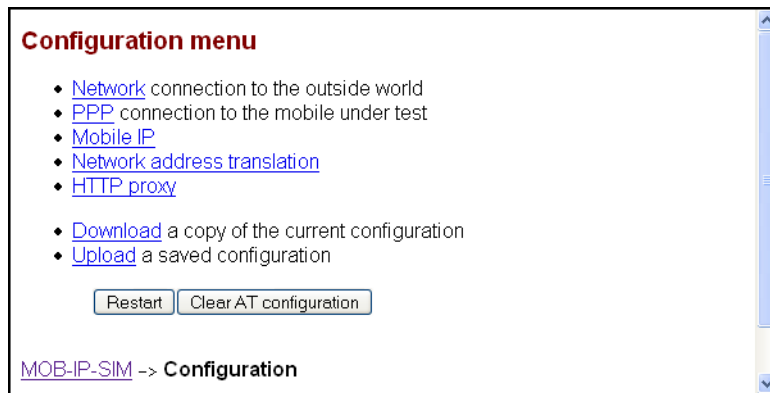
Figure 3-1. Mobile IP network simulator page



Click on the **Configuration** menu link to reach the main configuration menu page shown in Figure 3-2. From here the specific forms used for Network, PPP, Mobile IP, and NAT configuration may be reached. Additionally, the present configuration may be downloaded to the controlling PC, or a previously saved configuration file uploaded to the MOB-IP-SIM. Two commands are also accessed here, namely **Restart** and **Reset AT** configuration.

Clicking on the **Restart** button reboots the MOB-IP-SIM. This action, which is equivalent to a simulator power cycle, will restart the simulator following a operating system upgrade and reset the machine to the web-based configuration state. Clicking on the **Reset AT configuration** button will return all configuration parameters altered by manual or scripted AT commands to the web-based configuration state. Remember that the web-based configuration sets all parameters aside from realdate, PPP link, and script tcpdump commands and that the web-based configuration values will be reloaded following a MOB-IP-SIM power-cycle, **Restart**, or **Reset AT** configuration commands.

Figure 3-2. Configuration menu page



The next steps walk through each configuration form. You should carefully review each form during the initial setup so that you will know where the parameters are stored if you need to modify something later. The other network settings can be configured or reconfigured once the MOB-IP-SIM has a valid IP network address.

Network Configuration

Click on the **Network** link to display the first configuration page, which is the same in the MIP-5800 and the MIP-5850 .

Figure 3-3. Network configuration page

Network configuration

This form contains information needed to get to the outside network. See also the [PPP configuration](#) page.

DHCP [?]

Hostname [?]

IP address

Netmask

Broadcast address

Gateway address

DNS servers

Static [?]

IP address [?]

Netmask [?]

Gateway address [?]

Primary DNS server [?]

Secondary DNS server [?]

Tertiary DNS server [?]

Configure each network parameter as indicated in the following text. Consult with your I.T. department if you are not familiar with IP address management or if you don't know how your local network is configured.

IP configuration

Select static or dynamic (DHCP assigned) IP addressing for the MOB-IP-SIM unit. This should already be configured correctly if the MOB-IP-SIM Manager has been used for the initial LAN setup. Static mode is recommended for most test environments.

DHCP Operation: If the MOB-IP-SIM has been set to DHCP mode, the IP address, netmask, broadcast address, gateway address, and DNS server parameters will automatically be assigned and displayed in this form.

Hostname

Default = mip. Enter an alphanumeric name for the MOB-IP-SIM. This name is used by some DHCP servers to allow network addressing by name rather than direct IP addressing. This setting is not critical.

IP address

If a static IP configuration is used, then this is the static IP address of the MOB-IP-SIM.

Netmask

If a static IP configuration is used, then this is the subnet mask for the local network. Hosts with IP addresses matching the MOB-IP-SIM's address in these bits are contacted directly; others are contacted through the gateway.

Gateway address

This is the address of a local network router used to reach the Internet. This value only applies to the static IP mode since DHCP mode automatically sets this address. The address must be on the local network and the net mask must be compatible with the simulator net mask and IP address. If you have an isolated network, leave this field blank.

Primary DNS server

This is the IP address of a Domain Name Server that provides name lookups for your network. This value only applies in the static IP mode since DHCP mode automatically obtains this address. Type `ipconfig /all | more` at the Windows command prompt to determine this address on your network.

Secondary DNS server

See: Primary DNS server

Tertiary DNS server

See: Primary DNS server

Click the **Save** button to save the current information and then click **PPP** to go to the next configuration page, which varies depending upon the model.

PPP Configuration

The PPP configuration form shown in the following figure configures the test Simple IP data connections. Mobile IP connections also depend on the PPP connection; however, the PPP server address and TCP packet logging are the only parameters that are involved in a Mobile IP connection.

Figure 3-4. MIP-5800 PPP configuration page

PPP configuration

This form contains information on the PPP connection to the mobile under test. See also the [network configuration](#) page.

Propose IP addresses during IPCP [?](#) no yes

IP address of PPP server [?](#)

IP address to assign mobile [?](#)

Propose PPP authentication [?](#)

--Permit unauthenticated PPP [?](#)

PPP user name [?](#)

PPP password/shared-secret [?](#)

Log all TCP packets (off for normal operation) [?](#)

Propose IP address during IPCP

When enabled, the MOB-IP-SIM sends an IP-Address option in its initial IPCP Configuration-Request message. Turn this on for Simple IP, off for Mobile IP.

IP address of PPP server

Default is 192.168.14.1. This is an arbitrary address assigned to the simulated PDSN. The default value should work as long as it does not conflict with other existing network addresses. The address is used by Simple IP as the PDSN address.

The mobile may use this address to contact the built-in content servers, even on a Mobile IP call. This feature is useful if the mobile is attached to an Ethernet-connected PC, as the PC can contact this address only through the mobile station so a successful transfer means the airlink is working.

The MOB-IP-SIM uses this address internally to refer to the PPP interface, so it must not conflict with any other address the MOB-IP-SIM will need to use.

IP address to assign mobile

Default is 192.168.14.3. This address will be assigned to the mobile station for a Simple IP connection and is unlimited as long as it does not conflict with other existing network addresses. Applies only to Simple IP.

The MOB-IP-SIM uses this address internally to route packets to the mobile, so it must not conflict with any other address the MOB-IP-SIM will need to use.

Propose PPP authentication

Default is ON. Check this option to cause the simulator to propose PPP authentication during LCP.

Permit unauthenticated PPP

Default is ON. Check this option to allow the MOB-IP-SIM to continue a PPP connection even if the mobile rejects the proposed PPP authentication (but not if the mobile agrees to authenticate and then fails authentication).

PPP user name

This is the Authentication name that will be used for dial-up networking on a PC. Generally used only with Simple IP.

PPP password

This is the Authentication password (or secret) that will be used for dial-up networking on a PC. Generally used only with Simple IP. If the secret begins with 0x (first character is a zero), it is interpreted as a hexadecimal string (0x616263 is exactly equivalent to abc). It follows that if your secret starts with 0x, you will need to type something that starts with 0x3078.

Log all TCP packets

When enabled, the MOB-IP-SIM logs all TCP packets instead of only those that have TCP flags set. This can help with debugging but slows down data transfer.

MIP-5850 PPP Configuration

The MIP-5850 provides two additional parameters on its PPP configuration form as indicated by the following figure:

Figure 3-5. MIP-5850 PPP configuration page

PPP configuration

This form contains information on the PPP connection to the mobile under test. See also the [network configuration](#) page.

Propose IP addresses during IPCP [?]	<input checked="" type="radio"/> no <input type="radio"/> yes
IP address of PPP server [?]	<input type="text" value="192.168.14.1"/>
IP address to assign mobile [?]	<input type="text" value="192.168.14.3"/>
Primary DNS server to advertise to phone [?]	<input type="text"/>
Secondary DNS server [?]	<input type="text"/>
Propose PPP authentication [?]	<input checked="" type="checkbox"/>
--Permit unauthenticated PPP [?]	<input checked="" type="checkbox"/>
Require PAP authentication [?]	<input type="checkbox"/>
Require CHAP authentication [?]	<input type="checkbox"/>
PPP user name [?]	<input type="text" value="user"/>
PPP password/shared-secret [?]	<input type="text" value="password"/>
Log all TCP packets (off for normal operation) [?]	<input type="checkbox"/>

Primary DNS server to advertise to phone

This is the IP address of a DNS server for the mobile or the attached PC to use. It applies to both Simple IP and Mobile IP. Leave it blank to omit the DNS-Server option from IPCP. This option is available only in the MIP-5850.

Secondary DNS server to advertise to phone

See: Primary DNS server to advertise to phone

Require PAP authentication

Default is OFF. Check this option to require the Password Authentication Protocol, in which case a username and password will be used to authenticate. Applies only to Simple IP. This option is

available only in the MIP-5850 .

Require CHAP authentication

Default is OFF. Check this option to require the Challenge Handshake Authentication Protocol. The username and password will be used to authenticate in this case. Applies only to Simple IP. This option is available only in the MIP-5850.

When completed, click **Save** to store the parameters. Then click the **Mobile IP** link to go to the next configuration page, which varies depending upon the model.

MIP-5800 Mobile IP Configuration

The Mobile IP form sets values related to processing Mobile IP messages. The simulator only answers messages originating from the mobile's home address and only routes packets destined for the home address to the PPP link.

Transfer the recorded Mobile IP provisioning information from section [A] of Appendix E to the appropriate parameters on the Mobile IP configuration page. Explanations of each field are provided here. The following parameters are available for both the MIP-5800 and MIP-5850 Mobile IP simulators.

Figure 3-6. MIP-5800 Mobile IP configuration page

Mobile IP configuration

This form contains information related to the Mobile IP simulation.

Mobile Node home address [?](#)

Home agent configuration

IP address ?	Netmask ?	Request verification		Response	
		Secret ?	SPI ?	Secret ?	SPI ?
68.28.15.2	255.255.255.0	secret	1234	secret	1234

Mobile Node home address

Obtain this field from the worksheet, unless the recorded Home Address from the mobile is 0.0.0.0, in which case the mobile station is expecting a dynamic IP address assignment and a valid non-zero Home address should be entered. If the recorded Home Address is non-zero, then the recorded value should be entered into the Mobile Node home address field of the form. The address entered into the configuration form will be assigned to the mobile station in either case.

The Home agent configuration table represents independent Home Agents that are normally configured to act as the mobile stations Primary Home Agent (#1 entry) and Secondary Home Agent (#2 entry). The recorded data from section [A] of the Configuration Worksheet should be used to set the parameters in this table. When the simulator receives a registration request (RRQ) message, it searches the table in ascending order looking for a matching Home Agent IP address. When a match is found, a registration response (RRP) message is generated based on the parameters contained in that table entry. Table entries

affect the response in various ways as indicated in the following. The MIP-5800 supports only one Home Agent.

IP Address

Enter the IP address of the mobile's primary Home Agent. If the mobile is configured for dynamic home-agent addressing (0.0.0.0 or 255.255.255.255), enter any valid IP address here and the mobile will use it.

Netmask

Default = 255.255.0.0. This netmask supports dynamic home agent address resolution according to RFC-3344 which states ". . . the mobile node MAY use dynamic agent address resolution to learn the address of its home agent. In this case, the mobile node MUST set the Home Agent field to the subnet-directed broadcast address of the mobile node's home network. Each home agent receiving such a Registration Request with a broadcast destination address MUST reject the mobile node's registration and SHOULD return a rejection Registration Reply indicating its unicast IP address for use by the mobile node in a future registration attempt."

Request verification-Secret

This is the shared secret used for mobile to Home Agent authorization of the RRQ message. A mismatched secret will result in a response code = 131 (authentication failure) in the RRP. This field supports hexadecimal strings the same as the PPP password field.

Request verification-SPI

Range [0 to 65535]. This is the numeric index related to the shared secret used for mobile to Home Agent authentication of the RRQ message. A mismatched SPI will result in a response code = 131 (authentication failure) in the RRP.

Response-Secret

Normally set to match the Request verification-Secret, it can be mismatched to test mobile behavior due to invalid authenticator data in the RRP. A mismatch has no effect on the RRP response code, but the mobile should reject the reply. This field supports hexadecimal strings the same as the PPP password field.

Response-SPI

Range [0 to 65535]. Normally set to match the Request verification-SPI previously documented.
Can be mismatched to test the mobile stations behavior due to invalid authenticator data in the RRP.
A mismatch has no effect on the RRP response code, but the mobile should reject the reply.

MIP-5850 Mobile IP Configuration

The following parameters are available only on the Mobile IP Configuration page of the MIP-5850 simulator as shown in the following figure.

Figure 3-7. MIP-5850 Mobile IP configuration page (advertiser)

Mobile IP configuration

This form contains information related to the Mobile IP simulation.

Mobile Node home address [?](#)

Advertisement parameters

Number of spontaneous Agent Advertisements to send when PPP link comes up [?](#)

Number of seconds between spontaneous Agent Advertisements [?](#)

Number of seconds to delay Agent Advertisements [?](#)

Care-of address (if different from MOB-IP-SIM address) [?](#)

ICMP Router Advert lifetime [?](#)

ICMP Router Advert preference [?](#)

Registration lifetime [?](#)

Registration required [?](#)

Busy (should be off) [?](#)

Home agent (should be off) [?](#)

Foreign agent (should be on) [?](#)

Minimal encapsulation [?](#)

GRE encapsulation [?](#)

Reserved (was Van Jacobson, should be off) [?](#)

Reverse tunneling supported [?](#)

Number of spontaneous Agent Advertisements to send when the PPP link comes up

Default is 1. This is a protocol behavior test parameter designed to disable (value = 0) spontaneous advertisements or to send multiple advertisements to the mobile station when the PPP link is established.

Number of seconds between spontaneous Agent Advertisements

Default is 0.01. This is a protocol behavior test parameter designed to control the rate at which

advertisements are sent. This parameter applies only if the number of Agent Advertisements is set to a value greater than 1.

Number of seconds to delay Agent Advertisements

Default is 0.01. This is a protocol behavior test parameter designed to delay the first advertisement after the PPP link comes up. This parameter applies only if the number of Agent Advertisements is set to a value greater than 0.

Care-of address

Default is blank or 0.0.0.0 (not set). The default value allows the Foreign Agent Care-of address in the Agent Advertisement to automatically contain the Ethernet IP address of the MOB-IP-SIM that normally acts as the FA. This default address comes from the **Network Configuration** page.

Entering a specific non-zero address will override the normal address that is advertised in the FA care-of address field.

ICMP Router Advertisement lifetime

Default is 9000 seconds per IS-835B. This field defines the maximum period that the Advertisement is considered valid in the absence of further Advertisements. This value is included to test the mobile's action when the timeout expires.

ICMP Router Advertisement preference

Default is 0. This is a 32-bit number representing the preference level of the Router Address included in the Advertisement. A blank entry is treated as a 0.

Registration lifetime

Default is 600 sec. This is the longest lifetime that this agent claims to be willing to accept in a Registration Request. A value of 0xffff indicates infinity. The mobile station is required to re-register when this time expires. This field has no relation to the Lifetime field within the ICMP Router Advertisement portion of the Agent Advertisement.

Registration required

Default is OFF. ON indicates registration with this foreign agent (or another foreign agent on this link) is required even when using a co-located care-of address.

Busy

Default is OFF. ON indicates the foreign agent will not accept registrations from additional mobile nodes.

Home agent

Default is OFF. ON indicates this agent offers service as a home agent on the link on which this Agent Advertisement message is sent.

Foreign agent

Default is ON. ON indicates this agent offers service as a foreign agent on the link on which this Agent Advertisement message is sent.

Minimal encapsulation

Default is OFF. ON indicates this agent implements receiving tunneled datagrams that use minimal encapsulation.

GRE encapsulation

Default is OFF. ON indicates this agent implements receiving tunneled datagrams that use GRE encapsulation.

Reserved

Default is OFF. The previous revision of the Mobile IP specification (RFC 2002) defined this bit to indicate support for Van Jacobson TCP header compression. ON may be used to check that the mobile station ignores this bit.

Reverse tunneling supported

Default is OFF. ON indicates this Foreign Agent supports reverse tunneling.

Figure 3-8. MIP-5850 Mobile IP configuration page (home agent)

Reverse tunneling supported

Home agent configuration

Accept dynamic HA request

#	IP address	Netmask	Request verification		Response			Registration lifetime
			Secret	SPI	Secret	SPI	Code	
1	68.28.15.2	255.255.255.0	secret	1234	secret	1234	0	65535
2							0	65535
3							0	65535
0							-1	65535

AAA configuration

DMU PKOID

Accept dynamic HA request

If this option is enabled, the MOB-IP-SIM will respond to an otherwise valid Registration-Request to a directed broadcast address by sending a Registration-Accept message. If disabled, the MOB-IP-SIM will respond with a Registration-Reject with code 136 (unknown home agent address).

Response-Code

Range [0 to 255]. Default is 0. This is used to control the code field in the RRP message sent by the Home Agent to the mobile station. An entry of 0 allows the simulator to function normally with automatic handling of authentication and time sync operations. Code 131 will be returned if authentication fails and code 133 will be returned if a time sync error is detected. Otherwise, code 0 will be returned indicating a successful registration. Non-zero positive values will override normal

processing to force a specific code in the RRP message regardless of other conditions. The special case value of -1 is used to disable this Home Agent and the Registration Response message.

Registration lifetime

Range [0 to 65535 sec]. Default is 65535. The default value allows the simulator to automatically reply with the same value requested in the RRQ message for normal operation. All other values limit the registration lifetime contained in the RRP message response and are used to test the mobile station's compliance with the network-assigned lifetime. Note (ref: RFC-3344 3.4): A value of zero indicates that the mobile node has been deregistered.

DMU PKOID

Range [0 to 255]. Default is 129. This number indicates to the mobile which public key it should use for DMU. The default value corresponds to the DMU keypair supplied with the MOB-IP-SIM. This option is available only on the MIP-5850 with DMU.

Click **Save** and then click the **NAT** link to go to the next configuration page.

NAT Configuration

On the NAT configuration form, you may set up network address translations as required to conform to your network's or the mobile station's requirements. A common example is shown where the mobile accesses the internet using an HTTP proxy server at address 68.28.31.1 port 80. This server is not locally accessible, so the NAT is configured to direct these requests to the simulator's local proxy server at 127.0.0.1 port 8080.

Use the Proxy Server information from section [C] of Appendix E to set the NAT configuration if needed.

Figure 3-9. NAT Configuration menu page

NAT configuration

Translation and filtering

We can either allow the external network to see the mobile's home IP address ('route') or we can hide the mobile and make all its traffic appear to come from the MIP box's IP address ('nat').

Mobile traffic handling [\[?\]](#) route
 nat

Redirection

When the mobile asks to connect to some server, we can redirect it to another one. This is useful for testing phones that are hard to reconfigure.

The following services are available on this machine (which you can refer to as 127.0.0.1):

Port	Service
80	HTTP content server
8080	HTTP proxy server (also translates GIF to PNG images)

When the mobile requests		Connect it to	
IP address	Port	IP address	Port
68.28.31.1	80	127.0.0.1	8080

Mobile Traffic Handling

The MOB-IP-SIM can handle mobile traffic in two ways: translate all outgoing traffic so it appears to come from the MOB-IP-SIM (NAT mode) or make the mobile's address appear to be on the LAN (route mode). Select which you want here.

In NAT mode, the mobile's address appears only on the PPP link between the mobile and the MOB-IP-SIM, so nothing on the LAN or elsewhere needs to be able to reach this address. The address simply needs to be different from any address that the MOB-IP-SIM or mobile might need to reach for any other purpose. The safest choice for the mobile's address in this mode is some random address from the private address ranges of 10.x.x.x or 192.168.x.x.

In route mode, the MOB-IP-SIM forwards packets intact between the mobile and the LAN. Use this mode if you need to initiate connections from the LAN or internet to the mobile. In this mode, the mobile must have an address from the range used on the LAN. The MOB-IP-SIM will provide proxy ARP for the mobile's address on the LAN.

When the mobile requests

Enter an IP address and TCP or UDP port number that the mobile may attempt to connect to. Both TCP and UDP connections with the specified port number will be redirected.

Connect it to

Enter an IP address and port number of the server that you would like the mobile to be connected to instead of the one it requested. The server will see the mobile's address as the source of the request messages, and the mobile will see the address it originally tried to contact as the source of the response messages.

When completed, click **Save** and then click the **HTTP** link to go to the next configuration page.

HTTP Proxy Configuration

The built-in HTTP proxy server can use an external proxy server, and it can modify the request URL before passing the request along to the content server. Use the HTTP proxy configuration to configure these features.

Figure 3-10. HTTP Proxy Configuration menu page

HTTP proxy configuration

External HTTP proxy

External HTTP proxy URL [?]

URL redirection

Change (regexp) [?]	To [?]
vision\sprintpcs\.com	wap.yahoo.com

External HTTP proxy URL

Some network configurations do not allow the MOB-IP-SIM to connect directly to HTTP servers on the Internet but do provide an HTTP proxy server to allow indirect connections. If you have such a network, obtain the details and put the URL for your proxy server here. For example, if your proxy server is at `web-proxy.example.com` on port 8888, use `http://web-proxy.example.com:8888/` as the URL.

If the MOB-IP-SIM can contact HTTP servers directly, leave this entry blank.

Change

When the mobile requests a URL that matches the regular expression in this column, the proxy server changes the part of the URL that matches the regular expression before requesting the page from the origin server.

To

The part of the request URL that matches the regular expression is changed to this entry. This entry is not a regular expression, but the `$` and `\` characters are special, as described below.

Some mobiles have hard-coded home-page URLs or expect the network to transform the request URL in some way. The HTTP proxy can handle either of these cases by transforming the URL. The left column contains a list of regular expressions that the proxy matches against the requested URL. If one of these regular expressions matches the URL, the proxy replaces the matched text with the corresponding text from the right column.

In a regular expression, letters and digits stand for themselves, but many punctuation marks have special meanings:

Table 3-1. Regular Expression Operators

Operator	Description	Example	Matches	Does not match
.	Any one character	a.b	axb	axxb
()	Grouping: everything in parentheses is treated as a unit	a(bc)+d	abcabcd	abcabd
+	At least one of the previous thing	a.+c	abdefc	ac
*	Zero or more of the previous thing	a.*c	ac	ad
?	Optionally one of the previous thing	ab?c	ac	abbc
[]	Any one character from the set	[a-dx]+	acbdxaa	afd
[^]	Any one character not in the set	[^a-dx]+	efgtuv	efgatuv
\	Use the next character as a normal character	\.	.	x

To be safe, put a \ before each punctuation mark unless you want to use its special meaning.

In the right column of the form, all characters stand for themselves except \ and \$. You can use \1

through \9 to refer to the text matching first nine parenthesized groups from the original URL.

Table 3-2. URL Rewriting Examples

Change	To
www\example.com	www.example.net
abc	ghi
^http:\\\/search\example.com\/(.+)	http://www.google.com/search?q=\1
Original	Result
http://www.example.com/abc/def	http://www.example.net/ghi/def
http://search.example.com/testing	http://www.google.com/search?q=testing

When completed, click **Save** and then click the **Menu** link to return to the Configuration Menu.

E5515C Configuration

Mobile IP typically uses cdma2000 Service Option 33 or the 1xEV-DO Default Packet Application for data calls. All the normal data call setup parameters on the E5515C apply to mobile IP and are not covered in this manual. The E5515C configuration and connection required to link it to the MOB-IP-SIM are explained here, but the Mobile IP wireless device setup and MOB-IP-SIM configuration are assumed to be completed as described in Chapter 3. The E5515C is also assumed to be set up and ready to handle standard data calls.

1. Connect the required communications test set, PCs, hubs, phone, and MOB-IP-SIM as diagrammed in Appendix D.
2. Make sure power is applied to all devices and that the required power-up operations are complete.
3. Use the E5515C soft menu to navigate to the Data Channel Parameters menu and set the external PDSN address to the MOB-IP-SIM local address previously recorded in section [B] of Appendix E and set the External PDSN State to ON.
4. The E5515C should indicate that the link to the MOB-IP-SIM is active. You must perform this step each time you reset or turn on the E5515C, either manually or by recalling a register with the External PDSN State set ON.
5. For hybrid mode (two E5515C sets), synchronize the system time between the sets. On the E5515C with its TRIG IN port connected, navigate to the Cell Info or Access Network Info menu, then to

CDMA System Time/Sync Info. Verify that Ext 8960 IP Addr contains the IP address of the other E5515C, then press the Sync To External Server button.

6. Exit back to the E5515C call processing menu.

This completes the E5515C setup.

Mobile Device Configuration

If you plan to use a mobile phone's built-in browser, you will need to set the browser's home page to something that can be accessed when the browser is launched. The suggested home page setting is `http://mobipsimaddress/mobipdemo.htm` where *mobipsimaddress* is the MOB-IP-SIM address recorded in section [B] of Appendix E. You may also use URL rewriting to have the MOB-IP-SIM supply a home page. This will allow you to access the built-in web server. Any valid local or public web server is also acceptable as the home page, so long as it is designed for small mobile screen displays.

If you plan to use the mobile as a wireless modem from a PC, follow the phone manufacturer's instructions for configuring this connection.

Check to make sure you have completed the following steps before attempting a Mobile IP Call:

- The MOB-IP-SIM was set up on the network and its IP address was recorded on the worksheet.
- The mobile station provisioning parameters related to Mobile IP were recorded on the Configuration Worksheet.
- The MOB-IP-SIM was configured using the data from the Configuration Worksheet.
- The E5515C was successfully configured to use the External PDSN mode to establish a LAN connection to the MOB-IP-SIM .
- The test phone was configured to use either its built-in browser with a valid home page or to act as a wireless modem for a PC-based web browser.

Testing the Configuration

You are now ready to set up a Mobile IP data call.

1. Set up the E5515C for SO33 (for cdma2000) or Default Packet Application (for 1xEV-DO) data operation. Always start with the standard SO33 mode rather than the SO33+F-SCH mode to simplify the RF channel setup requirements (F-SCH channel power level adjustments are needed if you plan to use the SO33+F-SCH mode).

2. Initiate a data call using the PC browser or the phone's built-in browser.
3. Once the call connects, web access should be possible.
4. End the call by closing the PC browser connection or exiting the phone's browser.

Things to consider when testing Mobile IP operation:

Mobile IP establishes an IP connection on the first call attempt. The traffic channel may be released by the phone's dormant mode inactivity timer, by closing the dial up connection, by exiting the built-in browser, or by manually releasing the call from the E5515C. In most cases, the IP connection remains active even though the call is released. Phones typically have an icon to show this state where the connection is dormant. You will need to become familiar with the characteristics of the mobile device you are using to verify this state.

Note: The phone may unexpectedly start and end Mobile IP call sessions due to dormant timer expirations and registration lifetime expirations. This behavior is often confusing to first time Mobile IP users.

Chapter 4. Logging

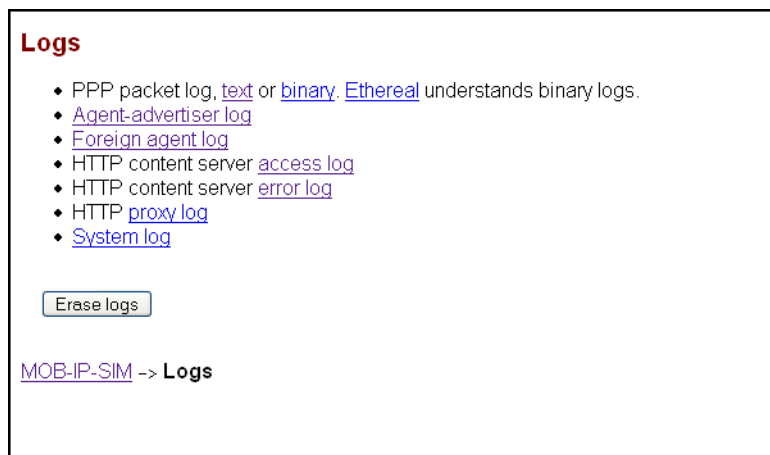
This chapter will teach you

- How to access message logs.
- How to access error logs.
- How to access operational logs.

Logs Pages

The Logs menu shown in the following figure provides access to a number of logs detailing the operational history of the MOB-IP-SIM . This page may be accessed from the Mobile IP Test Menu found at the root of the MOB-IP-SIM web server. Click on the Log files link to reach the following menu and then click on the appropriate link to reach the log of interest.

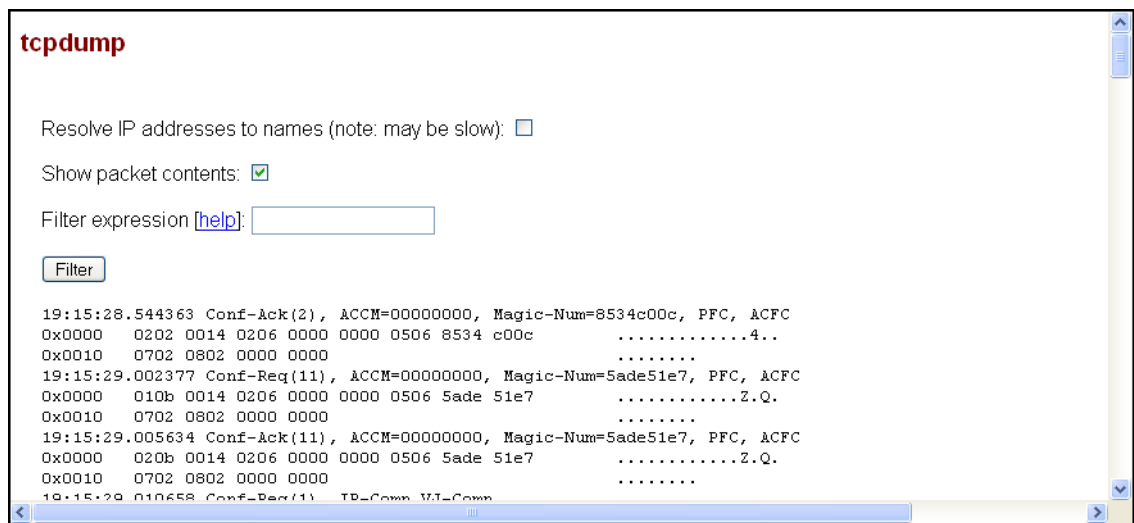
Figure 4-1. Logs page



tcpdump (show packet contents)

The PPP packet log may be accessed in either text or binary form. Check here to determine whether PPP negotiation succeeded and an IP connection was opened. Click on the [text](#) link to call up the embedded tcpdump utility, which will display the network traffic in text format as shown in the following figure. The user may filter the content of the tcpdump window by entering a suitable expression in the Filter expression field and clicking on the Filter button.

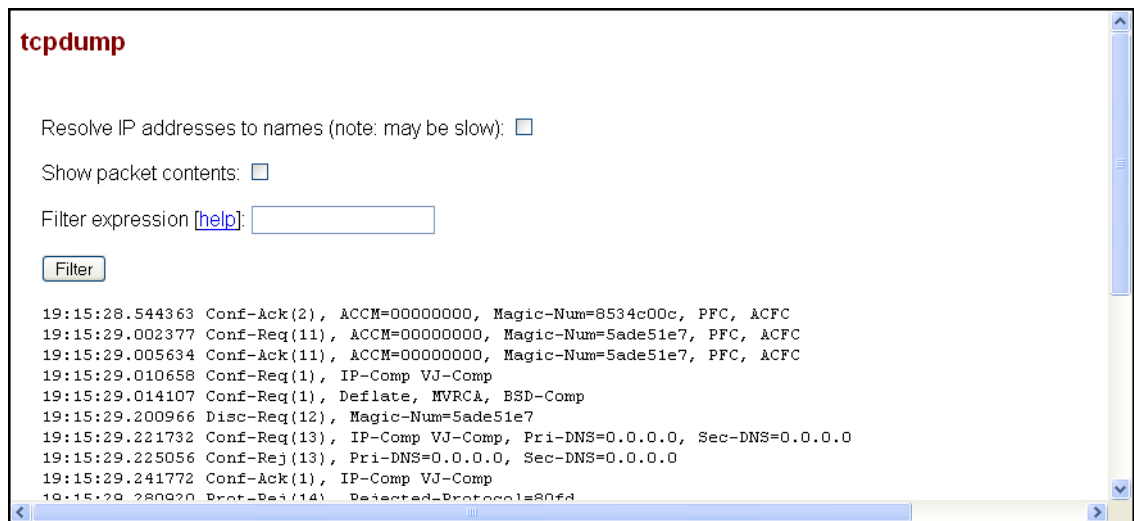
Figure 4-2. tcpdump (show packet contents) page



tcpdump (don't show packet contents)

To download the log in binary form, click on the binary link. The binary format may be read directly by the free Ethereal network software, which is included on the CD-ROM.

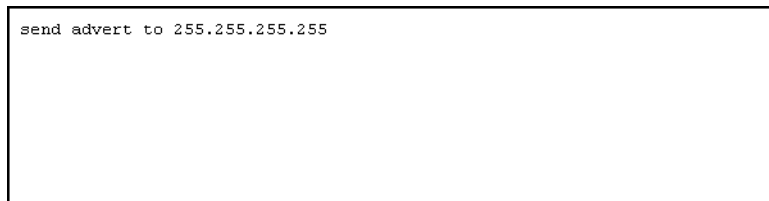
Figure 4-3. tcpdump (don't show packet contents) page



Agent-Advertiser Log

Click on the Agent-Advertiser log link on the Log menu to call up a log of all messages from the process that sends mobility agent advertisements as shown in the following figure.

Figure 4-4. Agent-Advertiser log page



Foreign Agent Log

Click on the Foreign agent log link on the Log menu to call up the log of messages from the foreign agent as shown in the following figure.

Figure 4-5. Foreign agent log page

```
msg rcvd on c0a801e5: 10 02 80 00 00 00 00 00 00 00 00 00 00 00 00: 0
find_ha(020f1c44)
  considering 1: 020f1c44/00ffffff
  --match: 1
Tentative reply code (before auth check): 0
auth checking key: 73 65 63 72 65 74
msg auth data verified, MD5 with SPI.
reply code (after auth check): 0
Recording data for request in table entry #3.
delta sec = 1
Sending registration response (0).
Appending NAI extension (8 0014)
Appending auth extension (8 0028)
reply generating key: 73 65 63 72 65 74
rsp check: msg auth data verified, MD5 with SPI.
reg reply to 10 02 80 00 ff ff ff ff 00 00 00 00 00 00 00: 03 00 02 5
```

Access Log

Click on the Access log link on the Log menu to call up the log of all accesses to the MOB-IP-SIM HTTP content server as shown in the following figure.

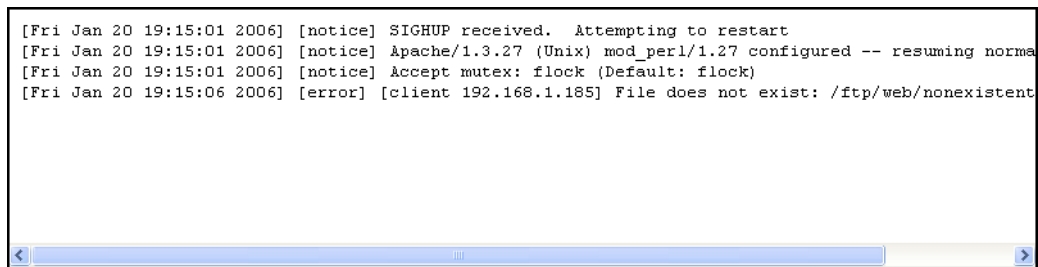
Figure 4-6. Access log page

```
192.168.1.185 - - [20/Jan/2006:19:15:00 +0000] "POST /logs/clear.cgi HTTP/1.1" 200 368
192.168.1.185 - - [20/Jan/2006:19:15:06 +0000] "GET /nonexistent.html HTTP/1.1" 404 292
192.168.1.202 - - [20/Jan/2006:19:16:24 +0000] "GET /config/ HTTP/1.1" 200 1085
192.168.1.202 - - [20/Jan/2006:19:16:29 +0000] "GET /config/mip.cgi HTTP/1.1" 200 7126
192.168.1.202 - - [20/Jan/2006:19:16:35 +0000] "GET /config/mip.cgi HTTP/1.1" 200 7126
192.168.1.202 - - [20/Jan/2006:19:16:40 +0000] "GET /config/nat.cgi HTTP/1.1" 200 7105
192.168.1.202 - - [20/Jan/2006:19:16:46 +0000] "GET /config/net.cgi HTTP/1.1" 200 2666
192.168.1.202 - - [20/Jan/2006:19:16:52 +0000] "GET /config/ppp.cgi HTTP/1.1" 200 3314
192.168.1.202 - - [20/Jan/2006:19:16:57 +0000] "GET /config/http.cgi HTTP/1.1" 200 4460
192.168.1.202 - - [20/Jan/2006:19:17:03 +0000] "GET /logs/tcpdump.cgi HTTP/1.1" 200 2450
192.168.1.202 - - [20/Jan/2006:19:17:09 +0000] "GET /logs/tcpdump.cgi?content=yes HTTP/1.1" 200 14655
```

Error Log

Click on the Error log link on the Log menu to call up the log of all errors reported by the MOB-IP-SIM content server as shown in the following figure.

Figure 4-7. Error log page

A screenshot of a web browser window displaying an error log. The log contains four lines of text: three notice messages and one error message. The error message indicates a file does not exist for a specific client IP address.

```
[Fri Jan 20 19:15:01 2006] [notice] SIGHUP received. Attempting to restart
[Fri Jan 20 19:15:01 2006] [notice] Apache/1.3.27 (Unix) mod_perl/1.27 configured -- resuming normal
[Fri Jan 20 19:15:01 2006] [notice] Accept mutex: flock (Default: flock)
[Fri Jan 20 19:15:06 2006] [error] [client 192.168.1.185] File does not exist: /ftp/web/nonexistent
```

HTTP Proxy Log

Click on the proxy log link on the Log menu to call up the log of the HTTP proxy server activity as shown in the following figure.

Figure 4-8. HTTP proxy log page



```
CONN new
REQ: GET http://vision.sprintpcs.com/ HTTP/1.1
Accept: application/xhtml+xml, application/vnd.wap.xhtml+xml, application/x-pmd, applicati
Accept-Charset: utf-8, UTF-8, us-ascii, iso-8859-1
Accept-Language: en, en, es
Host: vision.sprintpcs.com
Proxy-Authorization: Basic c2NpQG1vYi5pcC5sYWluY29tOnBjcw==
User-Agent: Mozilla/4.0 (MobilePhone SCP-4900/1.0) NetFront/3.0 MMP/2.0
Proxy-Connection: Keep-Alive
X-Wap-Profile: "http://device.sprintpcs.com/Sanyo/SCP4900/1021.rdf"

RESP sent
REQ: GET http://vision.sprintpcs.com/images/yahooicon.wbmp HTTP/1.1
Accept: application/xhtml+xml, application/vnd.wap.xhtml+xml, application/x-pmd, applicati
Accept-Charset: utf-8, UTF-8, us-ascii, iso-8859-1
```

System Log

Click on the System log link on the Log menu to call up the log of all system messages as shown in the following figure.

Figure 4-9. System log page

```

Jan 20 19:15:00 mip syslogd: restart
Jan 20 19:15:27 mip pppd[26096]: pppd 2.4.0 started by root, uid 0
Jan 20 19:15:27 mip pppd[26096]: Using interface ppp0
Jan 20 19:15:28 mip pppd[26096]: Connect: ppp0 <--> /dev/tty0
Jan 20 19:15:28 mip pppd[26096]: Warning - secret file /etc/ppp/pap-secrets has world and/or group access
Jan 20 19:15:28 mip pppd[26096]: sent [LCP ConfReq id=0x1 <asyncmap 0x0> <auth chap MD5> <magic 0x8534c00c> <
Jan 20 19:15:28 mip pppd[26096]: rcvd [LCP ConfRej id=0x1 <auth chap MD5>]
Jan 20 19:15:28 mip pppd[26096]: sent [LCP ConfReq id=0x2 <asyncmap 0x0> <magic 0x8534c00c> <pcomp> <accomp>]
Jan 20 19:15:28 mip pppd[26096]: rcvd [LCP ConfAck id=0x2 <asyncmap 0x0> <magic 0x8534c00c> <pcomp> <accomp>]
Jan 20 19:15:29 mip pppd[26096]: rcvd [LCP ConfReq id=0xb <asyncmap 0x0> <magic 0x5ade51e7> <pcomp> <accomp>]
Jan 20 19:15:29 mip pppd[26096]: sent [LCP ConfAck id=0xb <asyncmap 0x0> <magic 0x5ade51e7> <pcomp> <accomp>]
Jan 20 19:15:29 mip pppd[26096]: Warning - secret file /etc/ppp/pap-secrets has world and/or group access
Jan 20 19:15:29 mip pppd[26096]: sent [IPCP ConfReq id=0x1 <compress VJ Of 01>]
Jan 20 19:15:29 mip pppd[26096]: sent [CCP ConfReq id=0x1 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
Jan 20 19:15:29 mip pppd[26096]: rcvd [LCP DiscReq id=0xc magic=0x5ade51e7]
Jan 20 19:15:29 mip pppd[26096]: rcvd [IPCP ConfReq id=0xd <compress VJ Of 01> <ms-dns1 0.0.0.0> <ms-dns3 0.0
Jan 20 19:15:29 mip pppd[26096]: sent [IPCP ConfRej id=0xd <ms-dns1 0.0.0.0> <ms-dns3 0.0.0.0>]
Jan 20 19:15:29 mip pppd[26096]: rcvd [IPCP ConfAck id=0x1 <compress VJ Of 01>]
Jan 20 19:15:29 mip pppd[26096]: rcvd [LCP ProtRej id=0xe 80 fd 01 01 00 0f 1a 04 78 00 18 04 78 00 15 03 2f]
Jan 20 19:15:29 mip pppd[26096]: rcvd [IPCP ConfReq id=0xf <compress VJ Of 01>]
Jan 20 19:15:29 mip pppd[26096]: sent [IPCP ConfAck id=0xf <compress VJ Of 01>]
Jan 20 19:15:29 mip pppd[26096]: local IP address 192.168.14.1
Jan 20 19:15:29 mip pppd[26096]: remote IP address 192.168.14.3

```

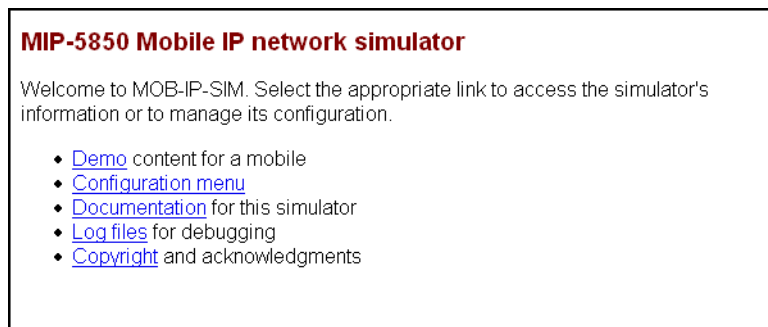

Chapter 5. Online Information

This chapter will teach you:

- How to access demonstration content
- How to access simulator configuration menus
- How to access a PDF of this manual
- How to access the simulator log files
- How to access copyright information and acknowledgments

Embedded documentation may be accessed via the Mobile IP network simulator page indicated below.

Figure 5-1. Mobile IP network simulator page



- The **Demo** link leads to files suitable for viewing on a mobile device.
- The **Configuration** link leads to the menu discussed in Chapter 3.
- The **Documentation** link leads to a PDF of the current operations manual.
- The **Logfiles** link leads to the log files discussed in Chapter 4.
- The **Copyright** link leads to the legal fine print.

Appendix A. Uploading Procedures

This appendix will teach you

- How to access embedded content for testing
- How to upload new content
- How to update the operating system

The MOB-IP-SIM includes FTP and HTTP content servers to which custom content may be uploaded. The operating system of the MOB-IP-SIM may also, if required, be updated by FTP.

The user has complete read/write access to the embedded FTP server. The user account is accessible with a user name of `test` and password of `ftp`. To view the files using a web browser, ftp to the simulator using the format `ftp://test:ftp@ipaddress/`. The server ships with the following five binary test files:

- `200k` 204800 bytes of random data
- `200k10` 200000 bytes of random data
- `50k` 51200 bytes of random data
- `50k10` 50000 bytes of random data
- `MD5.txt` MD5 checksums of the above four files

You can install more files with any standard FTP client. To update the operating system, FTP the binary file into the root directory of the MOB-IP-SIM, naming it `upgrade.bin`. After the transfer is complete, click on the Restart button at the bottom of the Configuration menu. The ERROR LED will blink once, then remain on during the the reset process, which will take five to ten minutes following the firmware upload. Normal operation will be possible when the ERROR light has gone off.

The embedded HTTP server reads the following files or directories from the `web` directory that is also accessible by FTP:

- `index.html`: The front page for the MOB-IP-SIM
- `mobipdemo.htm`: The menu page for the demo files

- `mobipdemo_files` : Directory for the demo files
- `config`: Directory for the built-in configuration forms
- `copyright`: Directory for the terms of use, copyright information, and acknowledgments
- `logs`: MOB-IP-SIM generated logs
- `docs`: Directory for the embedded documentation

Of the above HTML files, only the `index.html` file is modifiable by the user, though custom HTML pages may be installed to provide content for mobile access testing. To view the files using a web browser, ftp to the simulator using the format `ftp://test:ftp@ipaddress/web/`.

Appendix B. AT Commands

This appendix will teach you how to use AT commands to

- configure the simulator for your test requirements
- interrogate the simulator regarding its state
- command the simulator to perform an action
- query the simulator regarding AT command syntax

AT commands may be used to set the configuration of the MOB-IP-SIM, to query the simulator about its state, to command it to perform an action, or to test for the existence and syntax of a command. While the MIP-5850 is expected to be used by a mobile device software engineer who requires significant control of the PPP and Mobile-IP connection, the MIP-5800 user is expected to be the user applications programmer, who requires only those commands required to establish a normal Mobile IP connection for applications testing. The MIP-5800 command set is therefore smaller than that of the MIP-5850. With either model, the AT commands may be used over either the Ethernet or serial ports.

To configure the MOB-IP-SIM the appropriate command must be followed by one or more arguments. Some action commands may also require arguments. To query the simulator a command is followed by a question mark. To test a command requires following the command with =?. Some commands allow setting a value, or take an action that requires arguments. Use the command name followed by = and a value. Some of these commands return a value.

Action commands are used by themselves or sometimes with arguments:

Test commands are those followed by =?, which all commands support. The response is an indication of the syntax of the commands arguments. If no arguments are used, an empty template is returned.

Templates consist of the following pieces:

- Decimal numbers and ranges in parentheses
- (0-9) One of the integers 0 through 9 inclusive.
- (0, 1-9) One of the integers 0 through 9 inclusive, but number 0 is special.
- (0.0-9.9) Real numbers 0.0 through 9.9.
- Character strings specified in hexadecimal

- A string of printing ASCII characters and blanks
- A string of lower case as and blanks
- Hexadecimal numbers and ranges
- Punctuation

Some commands allow querying the current value of some parameter by adding a ? to the name of the command. The response returns the current value.

In the description following, each command description lists the methods supported (except for the =? test).

After the controller issues a command, the MOB-IP-SIM returns one or more lines of response. Each line is terminated with carriage return and line feed.

Every command returns a basic result code, currently either OK or ERROR, as its last line of response. Some commands return extended response lines, which start with a plus sign followed by the command name, a colon, a blank, and some additional information. This additional information is the return value.

Many of the AT commands affect and read configuration data visible from the web pages, one command per datum. While changes to some of these data, such as the fields in Mobile IP messages take effect immediately, changes to others such as the IP address and PPP settings, do not.

The commands are discussed using the following format:

+command [argument]

Query, Immediate, Disruptive, and/or Action

The command description

The template entry indicates what **at+foo=?** returns, if anything.

A command is labeled Query if it supports the =? command.

A command is labeled Immediate if it has an immediate effect but does not disrupt operation any more than one would expect from changing that parameter.

A command is labeled Disruptive if it forces changes to take effect other than what one may expect from the name or one-line summary of the command.

A command is labeled Action if it has a no-argument form.

The commands listed under “General Commands” are available on both the MIP-5800 and MIP-5850 simulators. The remaining commands are available only on the MIP-5850.

The serial port operates at 9600 bps, with 8-bit characters, no parity, one stop bit. It has the usual IBM AT-style pinout, so you need a null-modem cable to connect it to a PC. Commands are terminated by a CR character (decimal 13); each response line is terminated by CRLF (decimal 13, 10).

The MOB-IP-SIM also listens on TCP port 53614. On this port, both command lines and response lines end in CRLF, in accordance with the usual Internet conventions. A normal TELNET client starts in a mode compatible with the MOB-IP-SIM command processor.

General Commands

+datetime [(2000-2038),(1-12),(1-31),(0-23),(0-59),(0-59)]

Immediate Query:

Read or set the date and time for use in logs. Arguments are year, month, day, hour, minute, and second in numeric form separated by commas but without spaces.

+mipreset

Immediate Disruptive Action

Reset all the settings caused by other AT commands and make the reset take effect immediately. This command may disrupt PPP and network connectivity.

+version

Query

Return the version number tag (release-1_0 or similar)

+ipaddr [(0-255).(0-255).(0-255).(0-255)]

Query

Set the static IP address to use on the next **+ipdhcp=0** command.

+ipdhcp [(0,1)]

Immediate Disruptive Query

This command configures the Ethernet interface to use DHCP or static configuration of its IP address, router address, and net mask. As with all AT commands, the effect of this setting is temporary. For permanent changes, use a web browser once communication has been established.

Setting the value to **1** causes the MOB-IP-SIM to broadcast a DHCP request and obtain a dynamic IP configuration.

Setting the value to **0** causes the MOB-IP-SIM to use the static configuration.

+ipdhcpaddr []

Query

Return the DHCP-assigned IP address.

+ipgw [(0-255).(0-255).(0-255).(0-255)]

Query

Set the default gateway to use on the next **+ipdhcp=0** command.

+ipnetmask [(0-255).(0-255).(0-255).(0-255)]

Query

Set the net mask to use on the next **+ipdhcp=0** command.

PPP Commands (available only on the MIP-5850 simulator)

+pppauth [(0,1)]

Query

Set to **1** to propose PPP authentication for the next PPP session (either CHAP or PAP is acceptable). If **+pppauth** is disabled, the peer is allowed to pass IP without authenticating. The peer may reject the proposal if **+pppnonauth** is also enabled. See also **+pppchap**, **+ppppap**, **+pppauto**, **+pppkill**, **+pppterm**, **+pppactive**, **+ppppassive**.

+pppchap [(0,1)]

Query

Set to **1** to insist on the PPP Challenge Handshake Authentication Protocol (CHAP) for the next PPP session. See also **+pppchap**, **+ppppap**, **+pppauto**, **+pppkill**, **+pppterm**, **+pppactive**, **+ppppassive**.

+pppipmobile [(0-255).(0-255).(0-255).(0-255)]

Query

Set the address to use for the mobile-station end of the PPP link. The simulator uses this address internally even if **+pppippropose** is off, so it must be set to an address that does not conflict with the network to which the simulator is attached. See also **+pppipmobile**, **+ppprestart**, **+pppterm**

+pppipsim [(0-255).(0-255).(0-255).(0-255)]

Query

Set the address to use for the simulator end of the PPP link. This address is used internally by the simulator even if **+pppippropose** is off, so it must be set to an address that does not conflict with the network to which the simulator is attached. See also **+pppipmobile**, **+ppprestart**, **+pppterm**

+ppprestart []

Immediate Action

Kill the PPP link (without sending LCP Terminate-Request) and start a new one.

Agent Advertisement Commands (available only on the MIP-5850 simulator)

+advb [(0,1)]

Immediate Query

Set to **1** for the Busy bit in the Mobility Agent Advertisement. Must be set to **0** for normal operation.

+advdelay [(0.00-3600.00)]

Immediate Query

Simulated network delay in seconds for Mobility Agent Advertisement messages. The MOB-IP-SIM sends the advertisement this many seconds after receipt of a Router Solicitation or the establishment of a PPP link with the mobile station.

+advf [(0,1)]

Immediate Query

Foreign Agent bit in the Mobility Agent Advertisement. Must be set to **1** for normal operation.

+advg [(0,1)]

Immediate Query

GRE encapsulation supported bit in the Mobility Agent Advertisement.

+advh [(0,1)]

Immediate Query

Home Agent bit in the Mobility Agent Advertisement. Must be set to **0** for normal operation.

+advlife [(0-65535)]

Immediate Query

Set the number of seconds the Router Advertisement is valid. See also **+advreglife** .

+advm [(0,1)]

Immediate Query

Minimal encapsulation supported bit in the Mobility Agent Advertisement.

+advpref [(-32768-32767)]

Immediate Query

Set the preference level to advertise for this router (larger means more preferable).

+advr [(0,1)]

Immediate Query

Registration required bit in the Mobility Agent Advertisement. Set to 1 to require registration.

+advreglife [(0-65534, 65535)]

Immediate

Set the number of seconds to include in the Mobility Agent Advertisement as the maximum registration lifetime.

+advseq [(0-65535)]

Immediate Query

Set the sequence number to use the next Router Advertisement message.

+advr [(0,1)]

Immediate Query

Reverse tunneling supported bit in the Mobility Agent Advertisement.

+advv [(0,1)]

Immediate Query

Reserved (formerly Van Jacobson) bit in the Mobility Agent Advertisement.

+mipcoaddr [(0-255).(0-255).(0-255).(0-255)]

Immediate Query

Set a care-of address to include in the Mobility Agent Advertisement message. The special case 0.0.0.0 means the IP address of the of the MOB-IP-SIM .

+spadvcount [(0-100)]

Immediate Query

Set the number of spontaneous Mobility Agent Advertisements to send when the PPP link is established. The MOB-IP-SIM may send fewer than this many Advertisements if the mobile station sends a Registration Request.

+spadvinterval [(0.00-100)]

Immediate Query

Set the interval in seconds between Mobility Agent Advertisements.

Home Agent Commands (available only on the MIP-5850 simulator)

+miphaaddr [(0-255).(0-255).(0-255).(0-255)]

Immediate Query

Mobile Node home address to expect. Registration Replies will be sent only to mobile nodes requesting either this home address or the zero home address. See also **+miphnum**

+miphaaddr [(0-255).(0-255).(0-255).(0-255)]

Immediate Query

Mobile Node home address to expect. Registration Replies will be sent only to mobile nodes requesting either this home address or the zero home address. See also **+miphnum**

+miphamask [(0-255).(0-255).(0-255).(0-255)]

Immediate Query

Network mask of the Home Agent currently under configuration used to simulate directed-broadcast behavior. See **+mipphanum**.

+mipphanum [(0, 1-3)]

Immediate Query

Select which Home Agent to configure with the **+miphaaddr**, **+miphamask**, **+mipreplycode**, **+miphaspi**, **+miphasecret**, **+mipmnspi**, **+mipmnsecret**, and **+mipreglife** commands.

+miphasecret (20-7e)

Immediate Query

Set the secret (in ASCII) to use when verifying the Mobile-Home Authentication Extension in incoming Registration Requests.

+miphaspi [(0-4294967295)]

Immediate Query

Set the SPI to expect in the Mobile-Home Authentication Extension in incoming Registration Requests.

+mipmnaddr [(0-255).(0-255).(0-255).(0-255)]

Immediate Query

Set the Mobile Node home address to expect. Registration Replies will be sent only to mobile nodes requesting either this home address or the zero home address.

+mipmnsecret [(20-7e)]

Immediate Query

Set the secret (in ASCII) to use when generating the Mobile-Home Authentication Extension in outgoing Registration Replies. Must match **+miphasecret** .

+mipmnspi [(0-4294967295)]

Immediate Query

Set the SPI to include in the Mobile-Home Authentication Extension in outgoing Registration Replies. Must match **+miphasp**i for normal operation.

+mipreglife [(0-65534, 65535)]

Immediate Query

The upper bound on the number of seconds to include in the Registration Reply as the registration lifetime. It should be greater than zero; 65535 means unlimited lifetime.

+mipreplycode [(-1, 0, 1-255)]

Immediate Query

Set the registration result code to use when sending the next Registration Reply. -1 means no reply (simulate failure); 0 means success; codes from 64 to 192 indicate failures. See RFC 3344 for more details.

+miprrpdelay [(0.00-3600.00)]

Immediate Query

Set the delay in seconds between getting a Registration Request and sending a Reply.

DMU Commands(available only on the MIP-5850 simulator with DMU option)

+mipdmu [(0,1)]

Immediate Query

If the flag is set, the MOB-IP-SIM will respond to a registration-request message with a DMU key-request message. Upon receiving the DMU key-data message, the MOB-IP-SIM will clear **+mipdmu** and respond with either the AAA-authenticator or public-key-invalid message, depending on whether a private key is available to decrypt the key-data message.

+mipdmupkoid [(0-255)]

Immediate Query

The PKOID value to use in the DMU key-request message. For normal operation, the mobile must have a public key with this PKOID, and the MOB-IP-SIM must have the matching private key.

Packet Capture Commands (available only on the MIP-5850 simulator)

+capcount

Query

Return the number of packets captured so far. They are numbered 0 to N-1.

+capdump [(2e, 30-39, 5b-5d, 5f, 61-7a)]

List all fields in the specified packet or part thereof in alphabetical order. The argument is a field or PDU identifier. This command is not intended for use from scripts, as the format and sequence of data presented are subject to change.

+capfind [(0-9999), (2e, 30-39, 5b-5d, 5f, 61-7a)]

Locate the first packet with a number greater than or equal to START that contains a field named FIELD and return either the number of the found packet, or ERROR.

+capget [(2e, 30-39, 5b-5d, 5f, 61-7a)]

Return a field (not a PDU), generally in decimal. IP addresses are returned as dotted quads, sections and a few other binary fields are returned as hex strings. The data is a raw version of the

higher-layer-protocol data (everything but the preceding fixed-length fields; e.g. ip.icmp.data starts at the octet following ip.icmp.sum).

+capident [(2e, 30-39, 5b-5d, 5f, 61-7a)]

Identify the specified packet or part thereof. The argument is a field or PDU identifier. Returns the most specific protocol name for the packet or specified part. The command does not look in extensions by itself; you have to point it there.

+capstart [(20-7e)]

Clear the saved packet buffer and start capturing packets. The argument is a tcpdump filter expression and may be left blank to capture all packets.

+capident [(2e, 30-39, 5b-5d, 5f, 61-7a)]

Immediate

Identify the specified packet or part thereof. The argument is a field or PDU identifier. Returns the most specific protocol name for the packet or specified part. The command does not look in extensions by itself; you have to point it there.

+capstop

Immediate Action

Stop capturing packets. Any packets already captured are preserved.

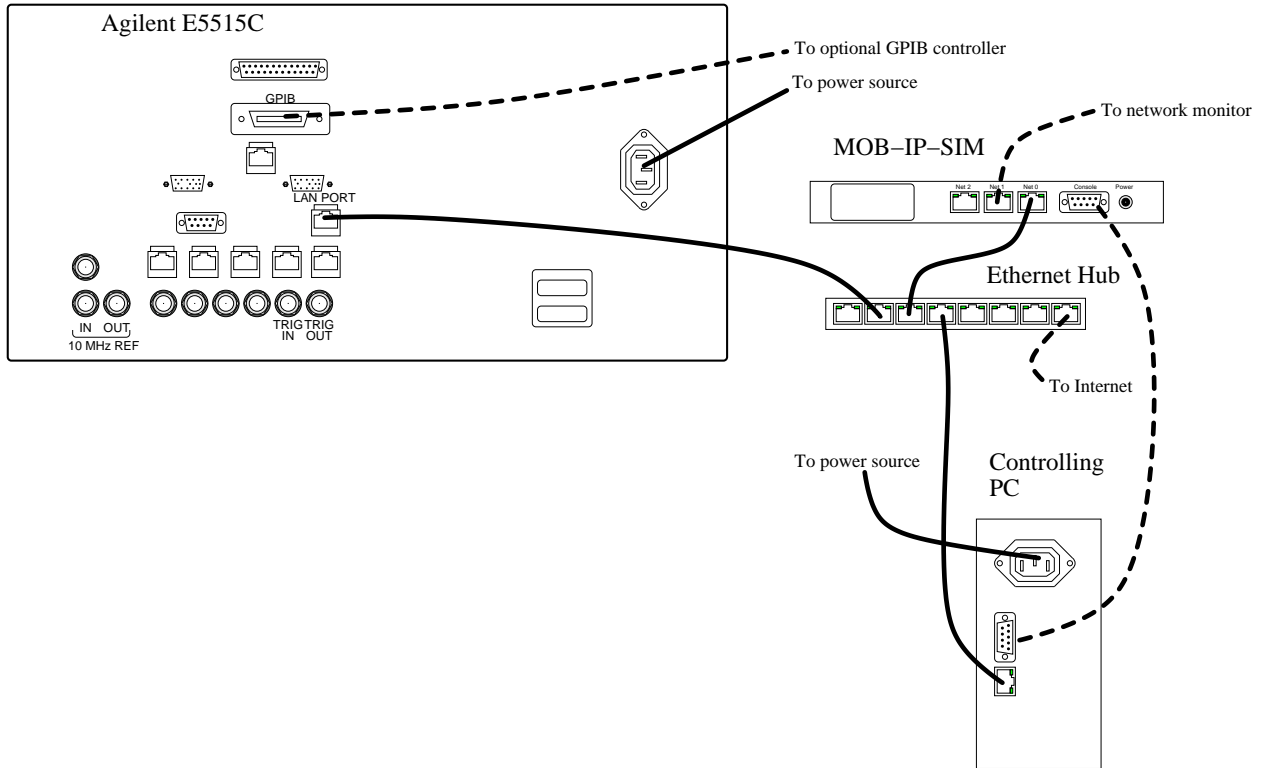
Appendix C. CD Contents

The Compact Disc that accompanies the MOB-IP-SIM contains a variety of files that may be helpful in the use of your simulator. These files include:

- MOB-IP-SIM Manager for Windows
- This manual in PDF and XHTML formats
- MOB-IP-SIM Tutorial
- Ethereal network analyzer software

Appendix D. E5515C Interconnection

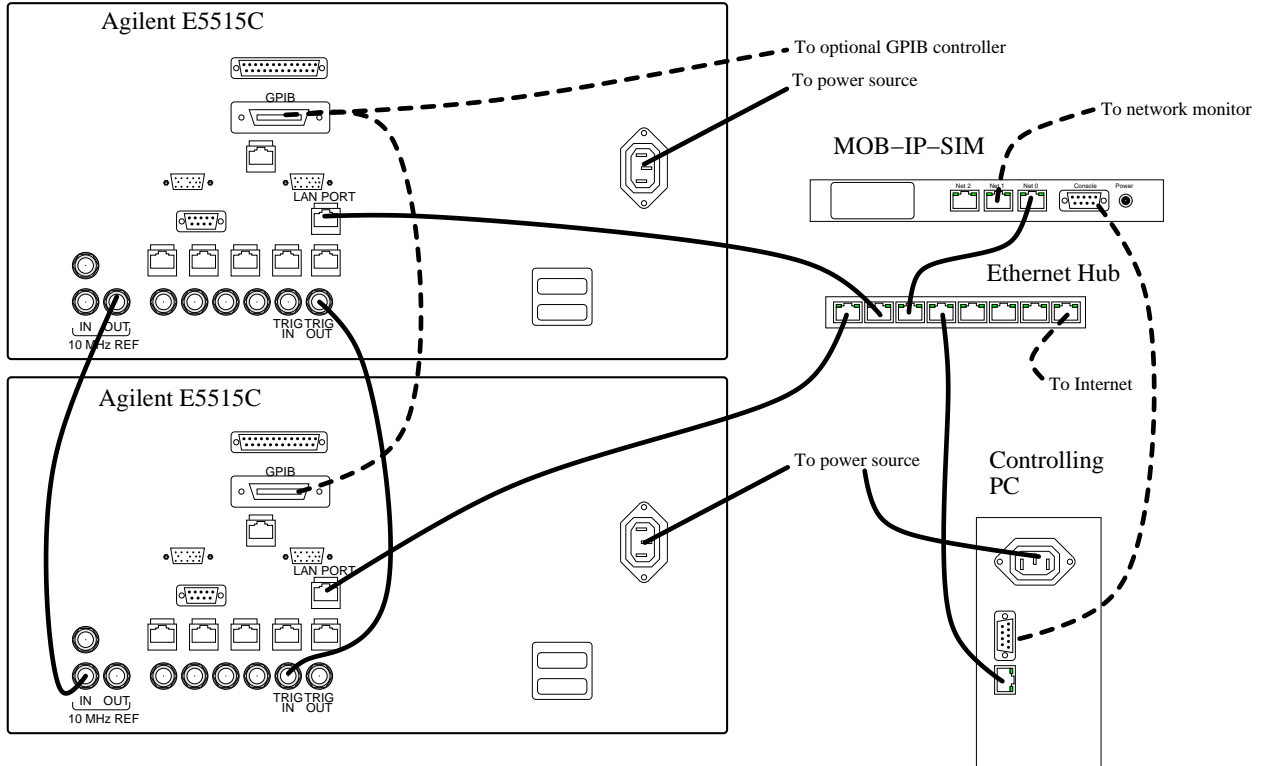
Figure D-1. MOB-IP-SIM / E5515C Interconnection diagram



The previous figure shows the typical interconnection required for the MOB-IP-SIM to be used with the E5515C. The MOB-IP-SIM, the E5515C, and a PC are all connected to an Ethernet for normal operation. The Ethernet may be connected to a larger LAN or the public Internet if desired.

During setup, the PC is connected to the serial port in order to configure the MOB-IP-SIM's network parameters; this link may be disconnected for normal operation.

Figure D-2. MOB-IP-SIM / E5515C Interconnection diagram for hybrid mode



The previous figure shows the typical interconnection for hybrid mode. Both E5515C sets are connected to the Ethernet, and one supplies a 10 MHz reference signal and a trigger signal to the other. The remaining connections are the same as for a non-hybrid system.

Appendix E. Simulator Configuration Worksheet

The Mobile IP device to be tested must be provisioned to match the MOB-IP-SIM configuration or vice versa. The following worksheet is included to record those test system parameters required for successful operation.

Table E-1. MOB-IP-SIM Configuration

Mobile Parameter Name	Common Name	Recorded Mobile Station Value	MOB-IP-SIM Parameter Name	Table Section
NAI	Mobile Identifier	____@____	Not Applicable	[A]
HomAdrs	Home Address	____.____.____.____	Mobile node home address	[A]
PrimHA	Primary Home Agent	____.____.____.____	Home agent IP address # 1	[A]
SecHA	Secondary Home Agent	____.____.____.____	Home agent IP address # 2	[A]
MNHA-SS	Home Agent Secret	_____	Home agent Request & Response Verification Secret	[A]
MNHA-SPI	Home Agent SPI	_____	Home agent Request & Response Verification SPI	[A]
MNAAA-SS	AAA secret	_____	Not Applicable	[A]
MNAAA-SPI	AAA-SPI	_____	Not Applicable	[A]
Rev Tun	Reverse Link Tunneling	0 or 1	Not Applicable	[A]
MOB-IP-SIM Network Address	Network address of the MOB-IP-SIM	____.____.____.____	Network configuration: Static or DHCP assigned address	[B]
ProxSvr	Proxy Server or Gateway address	____.____.____.____:____	NAT configuration: Redirection: ProxSvr :80 to 127.0.0.1:8080	[C]
Home Page	Home Page URL	_____	Not Applicable	[D]

Appendix F. Manual MOB-IP-SIM Configuration

The MOB-IP-SIM Manager Windows utility should be used to set up the MOB-IP-SIM on your network in most cases. However, if the software utility is not available, the simulator may be manually configured by using a terminal emulator software application such as HyperTerminal to send AT commands directly to the serial port located on the MOB-IP-SIM back panel. The COM port should be set to 9600 Baud, 8 bits, no parity, and 1 stop bit.

1. To determine the current DHCP configuration enter **at+ipdhcp?**

A response of

```
+IPDHCP: 1 OK
```

indicates that DHCP is in use. A zero indicates a static configuration.

2. Enter **at+ipdhcpaddr?** In this example, a response of

```
+IPDHCPADDR: 192.168.1.210 OK
```

indicates that the assigned address is 192.168.1.210.

3. If the configuration is indicated to be static then enter **at+ipgw?** A response of

```
+IPGW: 192.168.1.1 OK
```

indicates the gateway in this case is 192.168.1.1. To retrieve the netmask enter **at+ipnetmask?** A response of

```
+IPNETMASK: 255.255.255.0 OK
```

indicates that the netmask is set to 255.255.255.0 in this case.

4. To reconfigure a static IP address, set only the values that need changing, then enter **+ipdhcp=0** even if it was set to 0 already; this makes the new settings take effect.

5. For DHCP IP address assignment, set **+ipdhcp=1** and (optionally, but most likely useful) confirm the new address by entering **at+ipdhcpaddr?**

```
+IPDHCPADDR: 192.168.1.210 OK
```


Colophon

This manual was produced in the DocBookx version 4.2 format as a single-source document and converted to PDF and HTML formats using OpenJade and pdfjadetex. PDF documents were sent directly to the printer.

Index

- AAA
 - configuration, 28
 - defined, 11
- CD
 - contents, 73
- configuration, 17
 - AAA, 28
 - agent advertisements delay, 32
 - AT Commands, 57
 - busy, 33
 - care-of address, 32
 - Dynamic HA, 34
 - E5515C Interconnection, 75
 - foreign agent, 33
 - Gateway address, 21
 - GRE encapsulation, 33
 - home agent, 28, 33
 - Hostname, 21
 - HTTP proxy, 38
 - ICMP router advertisement lifetime, 32
 - ICMP router advertisement preference, 32
 - IP address, 21, 29
 - IP address of PPP server, 23
 - IP address to assign mobile, 24
 - manual, 79
 - minimal encapsulation, 33
 - MOB-IP-SIM Manager, 15
 - Netmask, 21, 29
 - Number of seconds between spontaneous Agent Advertisements, 31
 - Number of spontaneous Agent Advertisements, 31
 - permit unauthenticated PPP, 24
 - PPP password, 24
 - PPP user name, 24
 - Primary DNS server, 21
 - Primary DNS server to advertise to phone, 26
 - Propose IP address during IPCP, 23
 - propose PPP authentication, 24
 - registration lifetime, 32
 - registration required, 33
 - request verification-Secret, 29
 - request verification-SPI, 29
 - require CHAP authentication, 27
 - Require PAP authentication, 26
 - response-code, 34
 - response-secret, 29
 - response-SPI, 30
 - reverse tunneling, 34
 - Secondary DNS server, 22
 - Secondary DNS server to advertise to phone, 26
 - TCP logging, 24
 - Tertiary DNS server, 22
 - Uploading, 55
- DMU
 - Public Key Organization Identifier (PKOID), 35
- FTP server, 55
- home agent
 - configuration, 28
 - defined, 11
- HTTP proxy
 - configuration, 38
 - defined, 12
- HTTP server, 55
- Logs, 43
- NAT
 - defined, 11
- Online Information, 53
- PDSN
 - defined, 11
- regular expressions, 39
- web server, 55

