MultiModem®

Wireless EDGE, GPRS, CDMA Modems with Ethernet Interface

User Guide

MultiTech® Systems

User Guide
MultiModem® Wireless EDGE, GPRS, and CDMA Modems with an Ethernet Interface
MTCBA-E-EN, MTCBA-G-EN-Fx, MTCBA-C-EN-Nx
S000375F, Revision F

Record of Revisions

Revision	Date	Description
B	08/10/06	Software version 1.14. Added a *Wake-Up-on-Call* setup example. Added a *Connecting to the Internet* section. Added a *Setting Up DNAT* example. Added more information about activating and setting up a wireless modem account. Added a table of commonly supported subnets.
C	04/23/07	Updated the Technical Support contact list. Removed the Multi-Tech Certified National Activation Agent statement. Updated the Multi-Tech Warranty statement.
D	11/15/07	Updated Hazardous Warnings statements. Updated the operating temperature for EDGE models. Changed GPRS from multi-band to quad-band. The Wireless Activation section now sends the user to the Wireless Activation Notices for directions on activating a wireless account. Added PTCRB and FCC regulatory statements to Appendix B. Improved the quality of some screen shots. Add AT Command for changing quad-band frequency.
E	03/24/08	Updated for software version 1.19
F	08/07/08	Add wall mount dimensional drawing.

Trademarks
Trademarks and registered trademarks of Multi-Tech Systems, Inc. include MultiModem, the Multi-Tech logo, and Multi-Tech. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. All other products or technologies referenced in this manual are the trademarks or registered trademarks of their respective holders.

World Headquarters
Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
Phone: 763-785-3500 or 800-328-9717
Fax: 763-785-9874
Internet Address: http://www.multitech.com

Technical Support

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	800-972-2439 or 763-717-5863

Table of Contents

Chapter 1 – Introduction and Product Description

This User Guide describes the MultiModem Wireless EDGE, GPRS, and CDMA modems with an Ethernet Interface.

Product and Interface Descriptions

Ethernet Interface

The MultiModem wireless modems with an Ethernet interface provide shared Internet access with one IP address. The built-in routing capabilities provide DHCP services and firewall security using Network Address Translation. Due to the routing capabilities, these modems are sometimes called routers.

These modems support "always-on" network connection as well as "dial-on-demand" for Internet services. The "always-on" network connection automatically establishes a wireless data connection and allows for around the clock surveillance, monitoring or real-time data acquisition of any remote Ethernet device such as a Web camera. If the data link is dropped in the event of poor reception or a complete loss of service, it will automatically re-establish the data link. When configured for "dial-on-demand" the wireless modem only accesses the Internet when data is present. This configuration is ideal for sharing Internet access among networked PCs.

Software features include remote configuration, firmware upgrade, load configuration screen, and a save configuration screen.

MultiModem EDGE

The MultiModem® EDGE wireless modem delivers some of the fastest cellular wireless data speeds utilizing EDGE technology. It allows users to connect to the Internet and send and receive data up to three times faster than possible with an ordinary GSM/GPRS network making it ideal for highly data-intensive multimedia applications. The MultiModem EDGE wireless modem is equipped with quad-band GSM, which means it can be used worldwide on all existing GSM networks.

> **AT Commands:** The MultiModem EDGE wireless modem is configured using the EDGE AT Commands. These commands are documented in the Reference Guide for the MultiModem Wireless EDGE Modems, document number S000371*x*.

MultiModem GPRS

The MultiModem® GPRS wireless modem offers standards-based quad-band GSM/GPRS Class 10 performance. The ready-to-deploy, standalone data/fax/voice modem allows developers to add wireless communication to products with a miniumum of development time and expense. The MultiModem® GPRS wireless modem is base on industry-standard open interfaces and can be desktop or panel mounted.

> **AT Commands:** The MultiModem GPRS wireless modem is configured using the GPRS AT Commands. These commands are documented in the Reference Guide for the MultiModem Wireless GPRS Modems, document number S000293*x* and also the Reference Guide for the GSM IP Commands, document number S000333*x*.

MultiModem CDMA

The MultiModem® CDMA wireless modem offers standards-based multi-band CDMA200 1xRTT performance. The ready-to-deploy, standalone data/fax/voice modem allows developers to add wireless communication to products with a miniumum of development time and expense. The MultiModem® CDMA wireless modem is base on industry-standard open interfaces and can be desktop or panel mounted.

> **AT Commands:**The MultiModem CDMA wireless modem is configured using the CDMA AT Commands. These commands are documented in the Reference Guide for the MultiModem Wireless CDMA Modems, document number S000294*x*.

Application Example
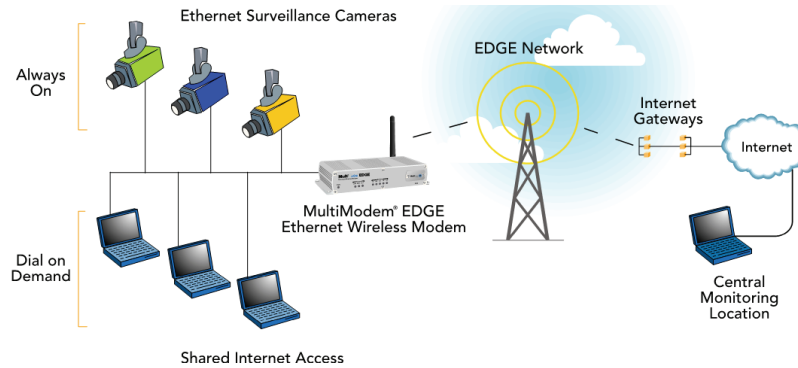
Ship Kit Contents

The wireless modem is shipped with the following:

Unbundled Package (Modem without Accessories)	Bundled Package (Modem with Accessories)
1 modem 1 fused DC power cable 4 rubber feet for flat surface mounting 1 Quick Start Guide 1 MultiModem CD **Note:** You must supply an antenna.	1 modem 1 power supply cable (type varies) 4 rubber feet for flat surface mounting 1 antenna 1 Quick Start Guide 1 MultiModem CD

Note: Some ship kits may contain printed Customer Activation Notices (directions for activating your modem through your wireless service provider).

Safety Warnings

Ethernet Ports Caution

The Ethernet ports are **not** designed to be connected to a Public Telecommunication Network.

Handling Precautions

All devices must be handled with certain precautions to avoid damage due to the accumulation of static charge. Although input protection circuitry has been incorporated into the devices to minimize the effect of this static build up, proper precautions should be taken to avoid exposure to electrostatic discharge during handling and mounting.

> **Caution:** Maintain a separation distance of at least 20 cm (8 inches) between the transmitter's antenna and the body of the user or nearby persons. The modem is not designed for, nor intended to be, used in applications within 20 cm (8 inches) of the body of the user.

Safety Instructions for Hazardous Locations

Installation Instructions

Installation instructions are provided which state:

1. The modems are open devices intended for installation in an ultimate enclosure suitable for the intended application.
2. THIS EQUIPMENT IS SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C, AND D OR NON-HAZARDOUS LOCATIONS ONLY.
3. "WARNING – Explosion Hazard – Substitution of Components may Impair Suitability for Class I, Division 2".
4. "WARNING – Explosion Hazard – Do not Disconnect Equipment Unless Power has been switched off or the area is known to be Non-hazardous".
5. "WARNING – Explosion Hazard – Do not replace fuse unless power has been switched off or the area is known to be non-hazardous"
6. "WARNING – Do not install or remove SIM card unless power has been switched off or the area is known to be non-hazardous".

Vehicle Safety

- Do not use your Wireless MultiModem while driving, unless equipped with a correctly installed vehicle kit allowing 'Hands-Free' Operation.
- Respect national regulations on the use of cellular telephones in vehicles. Road safety always comes first.
- If incorrectly installed in a vehicle, the operation of Wireless MultiModem telephone could interfere with the correct functioning of vehicle electronics. To avoid such problems, be sure that qualified personnel have performed the installation. Verification of the protection of vehicle electronics should be part of the installation.
- The use of an alert device to operate a vehicle's lights or horn on public roads is not permitted.

Specifications

Features	EDGE Modems	GPRS Modems	CDMA Modems
Performance	**EDGE:** E-GPRS Class 10, **GPRS:** Class 12	GPRS Class 10	CDMA2000 1xRTT
Band, Frequency	Quad-band GSM 850/900/1800/1900 MHz	Quad-band GSM 850/900/1800/1900 MHz	Dual-band 800/1900 MHz CDMA; 800 MHz and 800/1900 MHz with R-UIM support
Packet Data	**EDGE:** E-GPRS Up to 240K bps, coding scheme MCS-9, mobile station Class B, LLC layer, 4 time slots **GPRS:** Full PBCCH support, coding scheme 1-4, mobile station Class B	Up to 85.6K bps, coding schemes CS1 to CS4	Up to 153.6K bps forward and reverse
Circuit-Switched Data	Up to 14.4K bps, non-transparent	Up to 14.4K bps transparent and non-transparent	IS-95A, IS 95B up to 14.4K bps forward and reverse
Short Message Services-SMS	Text & PDU, Point-to-Point (MO/MT), cell broadcast	Text & PDU, Point-to-Point, cell broadcast	Text & UCS-2, Point-to-Point, cell broadcast
Fax	Class 1 Group 3	GSM Class 1 and Class 2 Group 3	Class 2.0 Group 3
Voice Features	Half rate (HR), Full rate (FR), Enhanced full rate (EHR), Adaptive multi rate (AMR), hands free echo cancellation, noise reduction	Half rate (HR), Full rate (FR), Enhanced full rate (EHR), echo cancellation, noise reduction (option), telephony and Dual Tone Multi Frequency (DTMF) transmission, emergency calls	Telephony and Dual Tone Multi Frequency (DTMF) functionality, AMPS Voice, QCELP (13K), echo cancellation
Antenna Connectors	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)
SIM Connector	Standard 3V SIM receptacle	Standard 3V SIM receptacle	
Interface Connectors	**Ethernet Model:** RJ-45, 10BaseT/100BaseTX, 802.3	**Ethernet Model:** RJ-45, 10BaseT/100BaseTX, 802.3	**Ethernet Model:** RJ-45, 10BaseT/100BaseTX, 802.3
Power Connectors	**Ethernet Model:** 2.5mm miniature screw	**Ethernet Model:** 2.5mm miniature screw	**Ethernet Model:** 2.5mm miniature screw
Voice Connectors	**Ethernet Model:** RJ-9 4-pos modjack	NA	NA
Voltage	5V to 32 VDC	5V to 32 VDC	5V to 32 VDC
Power (Max. Current Draw)	950mA at 5V	800mA at 5V	840mA at 5V
Physical Description	**Ethernet Model:** 2.8" L x 6.4" W x 1.2" H; 11.5 oz. (7.1 cm x 16.3 cm x 3.0 cm; 326G)	**Ethernet Model:** 2.8" L x 6.4" W x 1.2" H; 11.5 oz. (7.1 cm x 16.3 cm x 3.0 cm; 326G)	**Ethernet Model:** 2.8" L x 6.4" W x 1.2" H; 11.5 oz. (7.1 cm x 16.3 cm x 3.0 cm; 326G)
Operating Temperature	-30° to +60° C	-20° to +55° C	-20° to +55° C
Storage Temperature	-40° to +85° C	-40° to +85° C	-40° to +85° C
Humidity	Relative humidity 20% to 90% condensing	Relative humidity 20% to 90% condensing	Relative humidity 20% to 90% condensing
Certifications	**CE Mark, R&TTE** **EMC:** FCC Part 2, 15, 22, 24; EN 55022, EN 55024 **Safety:** cUL, UL 60950; EN 60950 **Network:** PTCRB	**CE Mark, R&TTE** **EMC:** FCC Part 2, 15, 22, 24; EN 55022, EN 55024 **Safety:** cUL, UL 60950; EN 60950 **Network:** PTCRB	**EMC:** FCC Part 2, 15, 22, 24; EN 55022, EN 55024 **Safety:** cUL, UL 60950; EN 60950 **Network:** CDG 1 & 2
Miscellaneous	AT Command Compatible Desktop or panel mounting Carrier approved Numerous LEDs provide status Embedded TCP/IP stack Two year warranty	AT Command Compatible Desktop or panel mounting Carrier approved Numerous LEDs provide status Embedded TCP/IP stack Two year warranty	AT Command Compatible Desktop or panel mounting Carrier approved Numerous LEDs provide status Over-the-air activation Embedded TCP/IP stack Two year warranty

AT Command Information

AT Commands: AT commands for the GPRS, GPRS-F4-IP, CDMA, and EDGE wireless modem are published in separate Reference Guides included on the MultiModem CD and posted on the Multi-Tech web site.

Chapter 2 – Getting Started

Setup a Wireless Account

Please see the wireless account **Activation Notices** located on the MultiModem CD. Choose the one for your wireless network provider and follow the directions to activate your account. These directions may also be included in your ship kit.

Phone Numbers for the Wireless Modem
Every wireless modem will have its own unique phone number. The phone number may simply be given to you by your wireless service provider. For GPRS and EDGE, it may also be on the SIM card. Wireless provider implementations may vary.

Connect Antenna, Ethernet, & Power

Antenna
Connect a suitable antenna to SMA connector. An antenna is supplied with the bundled package ship kit. If you purchase a single unit, you must supply your own antenna.

Ethernet
Using an RJ-45 Ethernet cable, connect the 10/100 jack to an internal network switch or hub.
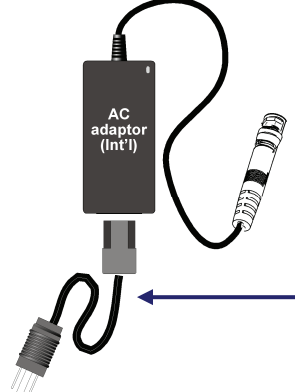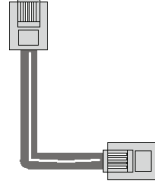
Power
Plug one end of the power cord into the device and the other end onto a live power outlet.

Notes
- **The PWR LED.** The **PWR** LED lights after power-up.
- **The Reset Button.** Pressing and holding the **Reset button** for 5 seconds will restore all factory default settings.

Back Panel
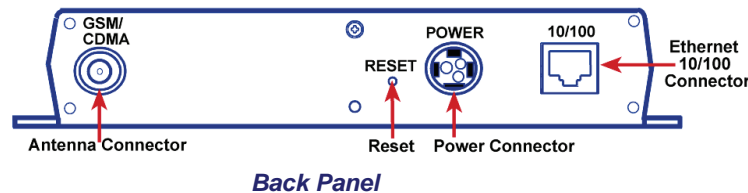
Antenna	Power Supply Cable	Ethernet Cable
	This part of the power supply cable varies by the region of the world to which the product is shipped: NAM / EU / GB / IE	

Note: Units shipped with the universal AC power supply are not suited for installation in hazardous locations.

Optional Fused DC Power Connection

**Fused DC
Power Cable**

Fuse

6.35 (.25")

31.75
(1.25")

Recommended Replacement
Fuses:
1. Manufacture: Littelfuse
   Part Number: 313 02.5
2. Manufacture: Sun Fuse
   Part Number: 6S

**In-Line
Fuse**

**red wire
is positive
(+)**

Fused DC Power Connection
- Connect the direct-DC power supply cable into the DC power source on the vehicle or machine in which you are mounting the modem. Be sure the GND connection is correct.
- Connect red wire to + (positive) and black wire to – (negative).

Note: For automotive application: according to the type of application, you can use permanent "+" or key-switched "+". Connect the power supply to its source (for example, in a mobile situation, to the vehicle's DC fuse/terminal block).

Warning: Over-voltage protection is provided on the device. To ensure complete protection, you may want to add additional filtering to the DC input.

Optional – Attach the Modem to a Flat Surface

Before you mount your modem to a permanent surface, verify signal strength, refer to Getting Started, AT Command for Verifying Signal Strength in Chapter 3.

The modem can be panel mounted with screws spaced according to the measurement shown.

Old Chassis

New Chassis
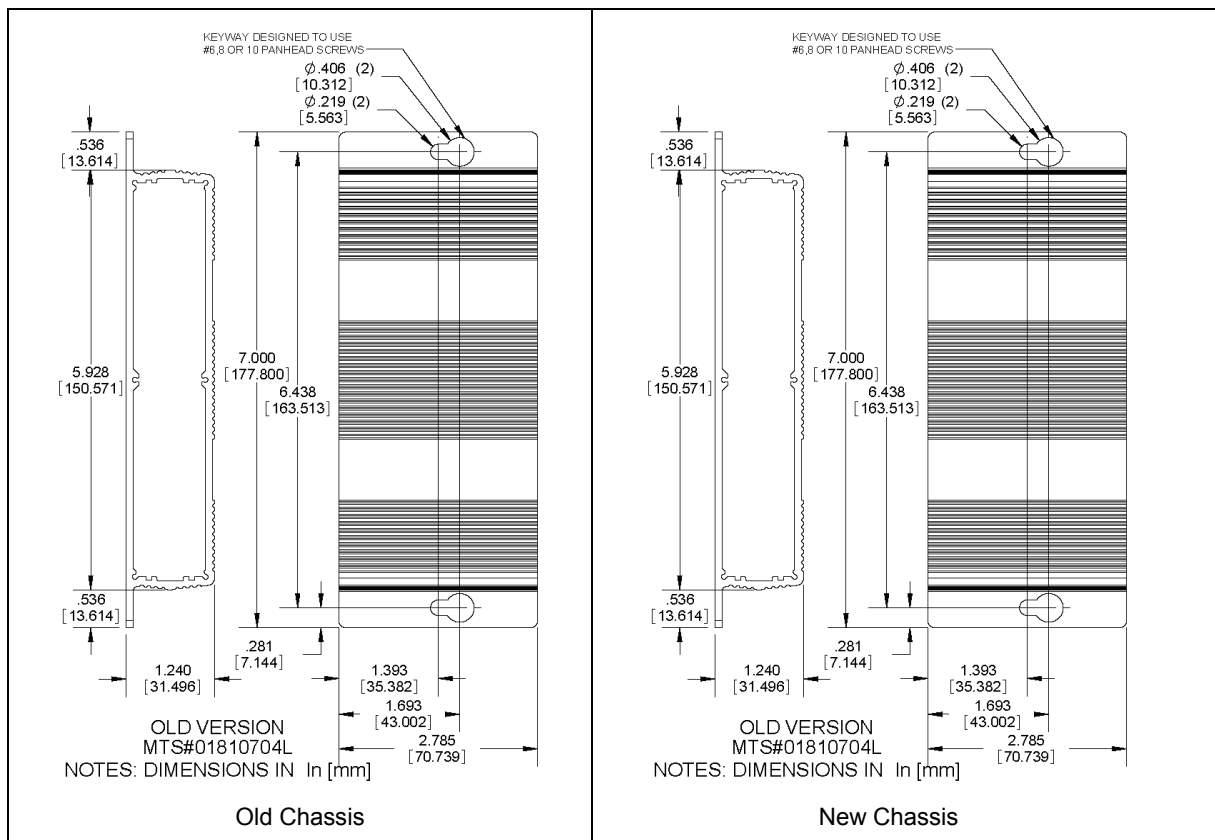
Front Panel LEDs

Once the power is connected, the LEDs on the front panel will provide information about the Ethernet functions and the wireless modem functions.

The front panel of the Ethernet EDGE has a power LED, 3 Ethernet LEDs, 5 modem LEDs, and a SIM card slot.

MultiModem® EDGE
Ethernet Wireless Modem

	Ethernet	Modem	
PWR	IP SPD L/A	TD RD CD TR LS	SIM

The front panel of the Ethernet GPRS is the same as the Ethernet EDGE.

MultiModem® GPRS
Ethernet Wireless Modem

	Ethernet	Modem	
PWR	IP SPD L/A	TD RD CD TR LS	SIM

The front panel of the Ethernet CDMA has the same LEDs as the EDGE modem. However, it does not have a SIM card slot.

MultiModem® CDMA
Ethernet Wireless Modem

MultiTech® Systems

	Ethernet	Modem
PWR	IP SPD L/A	TD RD CD TR LS
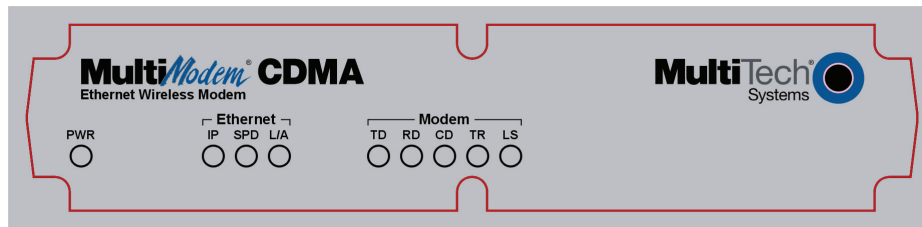
Ethernet LEDs

IP **IP FUNCTION.** This LED blinks when the IP function of the modem/router is operating normally. It shows a steady light when powering-up, initializing, or flashing the firmware.

SPD **SPEED.** This LED lights when the Ethernet is linked at 100 Mbps. If it is not lit, the Ethernet is linked at 10 Mbps.
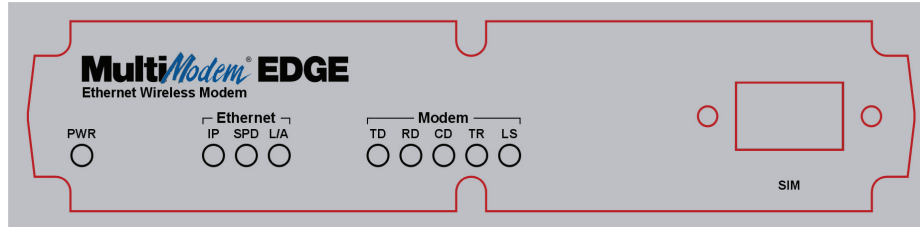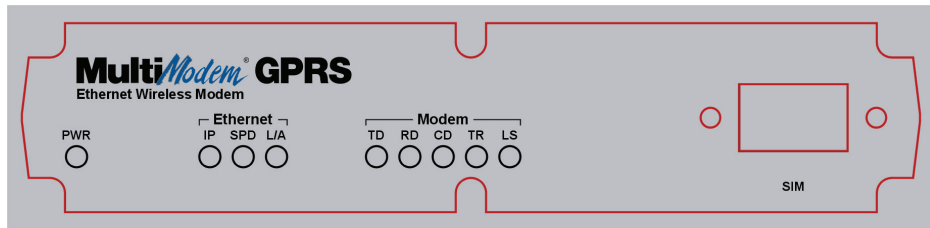
L/A **LINK ACTIVITY.** This LED blinks when there is transmit and receive activity on the Ethernet. It shows a steady light when there is a valid Ethernet connection.

Modem LEDs

TD **TRANSMIT DATA.** This LED blinks when the modem is transmitting data to your wireless carrier.

RD **RECEIVE DATA.** This LED blinks when the modem is receiving data from your wireless carrier.

CD **CARRIER DETECT.** This LED lights when the modem detects a valid carrier signal from a wireless carrier.

TR **(DATA) TERMINAL READY.** This LED lights when the modem is trying to establish a wireless connection.

LS **LINK STATUS.**

EDGE: This LED blinks when there is network activity between the carrier and the cellular module. At all other times, the light will be off.

GPRS & CDMA:
Continuous "on" state indicates that the wireless modem is not registered on the network.
Flashing state indicates registration on network.
Off state. Modem is off (not ready) or in download mode.

Set Your PC's TCP/IP Address for Ethernet Functionality

After the wireless account is established and the modem is properly connected, it is now time to set up the PC for the Ethernet functionality. First, you will have to set the TCP/IP address on your PC, if not previously set.

1. Open the PC's **Control Panel**.

2. Select **Networks** or **Network Connections**.

3. Under **Protocols**, select **TCP/IP**.

4. Under **Properties**, choose one of the following:

    - Check *Obtain IP Address Automatically* and *Obtain DNS Server Address Automatically*. If you check these, then the DHCP function obtains the IP Address automatically from the Ethernet wireless modem, or

    - Check *Use the Following IP Address* and *Use the Following DNS Server Address.* If you check these, then enter the following addresses:
      IP Address: 192.168.2.2
      Subnet Mask: 255.255.255.0
      Gateway: 192.168.2.1
      Specify a DNS Server. For example, 205.171.3.65

Using AT Commands

Prerequisite Steps

In order to communicate directly with the internal cellular module with AT commands, you first must disable **PPP** by logging into the Web Management software:

1. **Open Web Browser**

   From the workstation, open a Web browser.

   Type the default Gateway Address: http://192.168.2.1

2. **Login**

   After entering the Address, the **Login** screen displays.

   - Type the default User name: **admin** (all lower-case).
   - Type the default password: **admin** (all lower-case).
     Note: The **User name** and **Password** are case-sensitive (both must be typed in lower-case). If Windows displays the **AutoComplete** screen, you may want to click **No** to tell the Windows OS not to remember the password; this helps maintain PC security.
   - Click the **Login** button. The Web Management Home screen displays.

3. **Go to the Wizard Setup Screen**

   - On the **Wizard Setup** screen under **PPP Configuration**, disable **PPP**.
   - Click the **Submit** button.
   - Click **Save & Restart**.

4. **Open the Command Window and Access Modem Mode**

   From modem mode you can enter AT Commands.

   - From the workstation, open the command window by clicking the **Start** button and selecting **Run.**
   - Type **CMD** to open the command window. Click **OK**.
   - When the command window opens, type: **Telnet 192.168.2.1 5000**
     Note: 5000 is the port number.
   - At **Login**, enter the user name **admin**.
   - At **Password**, enter the password **admin**. Once logged in, you can use AT commands to communicate with the cellular module.

   For CDMA, you will have to enter some AT Commands to complete your activation steps. See the Customer Activation Notices included in your ship kit.

   For GPRS, you will have to use AT Commands to change the quad-band frequency.

   For CDMA, EDGE, and GPRS, you can use AT commands to verify signal strength, check network registration and roaming status, etc. See the AT Command guides available on the CD in your ship kit for other functionality you can view and set.

AT Command for Changing the GPRS-F4 Model's Quad-Band Frequency

AT Command for Changing the GPRS-F4 Quad-Band Frequency

For the GPRS-F4 Quad-Band modem, the default setting may be either 850/1900MHz dual-band mode or 900/1800MHz depending upon the model you ordered. If for any reason you want to change the band, you can accomplish this by using the **+WMBS** command.

Steps for Changing the GPRS Band for Ethernet Models

Using the command window (see steps above), you can enter the AT Command for changing the GPRS Band.

Type **AT+WMBS=<Band>,<Param>**. Press Enter.

For **<Band>**, enter the option you desire:

      4 = Dual-band mode 850/1900MHz

      5 = Dual-band mode 900/1800MHz

For **<Param>**, enter the option you desire:

      0 = The modem will have to be reset to start on the specified band(s). This is the default.

      1 = The modem restarts immediately on the specified band(s).

Example: AT+WMBS=4,0. Press Enter.

AT Command for Verifying Signal Strength

1. In the command window, type **AT+CSQ**
2. The modem responds with the received signal strength (rssi) and the channel bit error rate (ber). RSSI ranges from 0 to 31. BER ranges from 0 to 7   (7 is the highest error rate).

Signal Strength – RSSI	
10 - 31	Sufficient
0 - 9	Weak or Insufficient
99	Insufficient

Note: Sprint models will respond differently. Please refer to the *CDMA AT Command Reference Guide*.

AT Command for Checking Network Registration and Roaming Status

Use this command to verify that the wireless MultiModem has been registered on a wireless network.

1. In the command window, type **AT+CREG?**
2. The modem will respond in one of the following ways:

Network Registration Verification	
Value	**Network Registration Status**
+CREG: 0,0	The modem is not registered on any network
+CREG: 0,1	The modem is registered on the home network
+CREG: 0,5	The modem is registered on a network and it is roaming

Note: If the modem indicates that it is not registered, verify the signal strength to determine if the problem is the strength of the received signal.

Exiting Modem Mode

1. After the last AT Command is entered, press:

   CTRL +] (the right bracket).
2. The following prompt displays:

   telnet>

   Type **quit** and press **Enter**.
3. Then the following prompt displays:

   c:>

   Type **exit** and press **Enter**.

Configure the Ethernet Interface Using the Web Management Software

You are now ready to configure the Ethernet interface. This is accomplished by using the modem's factory-installed Web Management software. The software is accessed through a Web browser.

1. **Open a Web browser**

   From the workstation, open a Web browser.

2. **Type the default Gateway Address: http://192.168.2.1**

3. **Login**

   After entering the Address, the **Login** screen displays.

   - Type the default User name: **admin** (all lower-case).
   - Type the default password: **admin** (all lower-case).

     Note: The **User name** and **Password** are case-sensitive (both must be typed in lower-case).

     A password can be up to 12 characters. If Windows displays the **AutoComplete** screen, you may want to click **No** to tell the Windows OS not to remember the password; this helps maintain PC security.

     Password Caution: It is recommended that you change the default password to better protect the security of your modem. Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

   - Click the **Login** button. The Web Management Home screen displays.

4. **Use the Wizard Setup for Quick Configuration**

   A quick way to configure the modem is to use the *Wizard Setup*. The *Wizard Setup* can be opened by clicking the words *Wizard Setup* located under the Web Management software's menu bar. The information entered here will default to other screens that require this information.

   Benefits of Using the Wizard Setup

   - Saves time so that you are not entering the same information several times.
   - Allows you to start using your device with a minimum configuration.

     Note: Additional features and functions can be set up using the complete Web Management software program, described in Chapter 3.

   - Provides a short way to enter and save information needed to create a connection to the Internet.

   Select **Wizard Setup**
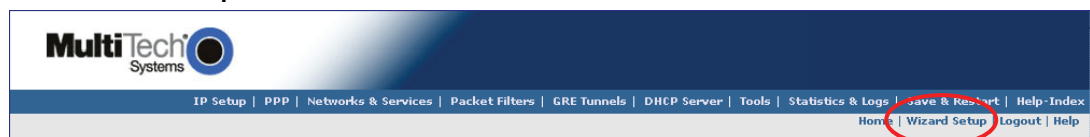
After clicking the **Wizard Setup** selection, the *Wizards Setup* screen displays.

Wizard Setup

IP Configuration	
IP Address	The default is 192.168.2.1. To change it, simply enter your own IP address.
Mask	The default is 255.255.255.0
DNS	Enter the primary DNS IP address for the system. The default is 0.0.0.0

PPP Configuration	
PPP	The default is *Enable*. This allows the PPP dialer to operate.
Dial-on-Demand	The default is *Enable*. This allows the dial-on-demand feature to operate. When *Disabled*, the modem always stays connected.
Idle Time Out	Sets the amount of time the PPP link stays active before disconnecting. Setting the value to zero causes the link to stay active continuously.
Dial Number	Enter the dial number. This number connects you to the Internet. **For GPRS and EDGE**, the number is ***99***1#**. **For CDMA**, the number is **#777**
APN	For GPRS and EDGE, enter the APN (Access Point Name). The APN is assigned by your wireless service provider.
Init String	You can set up to 4 modem initialization strings.

PPP Authentication	
Authentication Type	Click the button corresponding to the authentication protocol you want to use to negotiate with the remote peer. PAP, CHAP, or PAP-CHAP. Default = PAP-CHAP
User Name	Enter the PPP User Name. This name authenticates the remote peer. The default is **ipmodule**.
Password	Enter the PPP Password. This password authenticates the remote peer. The default is **ipmodule**.

A Note About the Access Point Name
The APN (Access Point Name) is assigned by your GPRS or EDGE wireless service provider, but you may have to ask for it. An access point is an IP network to which a wireless modem connects. The Web Management software asks for the APN on the *Wizard Setup* screen and the *PPP* screen.

5. Click the **Submit** button.
6. Click the **Save & Restart** button.

IMPORTANT NOTE ABOUT *SUBMIT* AND *SAVE & RESTART*

Click the **Submit** button located at the bottom of most screens in order to save any changes you make. Then you must click the **Save & Restart** button, located on the Menu bar, in order for your settings to take effect. **Save & Restart** does not have to be executed after each screen; you can change and **Submit** several screens, and then click **Save & Restart**.

Set Time and Date

The date and time must be set using the Web Management software.
The time and date set in *IP Setup* will not be correct unless SNTP client is enabled and you have a live Internet connection. See SNTP client.

Shutdown Caution

Never unplug the power until you have first performed the **Save & Reset** process. If the setup changes are not properly saved before unplugging the power, data could be lost.

Connecting to the Internet

Connecting to the Internet Through Your Cellular Provider's Service

This section provides step-by-step instructions for connecting to the Internet, which must be accessed through your cellular provider.

Important Note About Provider Fees:
Your provider will charge you for your data usage. Please check with your provider to make sure you are aware of the charges.
If you plan to use the router for large amounts of data transfers, Multi-Tech recommends an unlimited data plan with your account. Multi-Tech will not be responsible for any charges relating to your cellular bill.

Connecting to the Internet Steps

1. Turn on your PC and login. Make sure your LAN connection is set to **Obtain an IP Address Automatically**.

2. Connect the Multi-Tech router at the 10/100 port and the PC to a hub or switch using the Ethernet RJ-45 cable. Turn on the MTCBA-x-EN by plugging in the power cable. Make sure your antenna is connected.
   For GPRS and EDGE models, make sure your SIM card is inserted correctly.

3. From the workstation, open the command window by clicking the **Start** button and selecting **Run**.

4. Type **CMD** to open the command window. Click **OK**.

5. When the command window opens, type **IPCONFIG**.

6. Check to make sure your LAN connection has received an IP address in the 192.168.2.x subnet from the router. If not, type **IPCONFIG /RELEASE**, and then type **IPCONFIG /RENEW** to see if you receive an IP address. Close the command window.

7. Open a Web browser and complete the following:
   - In the **Address bar** type **http://192.168.2.1**
     This opens the Web Management software included with your wireless product.
   - Click **Go**. A *Login* screen displays.
   - Type the following:
     For **Username:** *admin*
     For **Password:** *admin*

8. Once you are logged in, select **PPP** from the Menu bar. The *PPP* screen displays. Setup the following to configure the PPP dialer:

PPP:	Enable (the default).
Dial-on-Demand:	Select Disable (select *disable* to stay connected at all times).
Idle time out:	0 (zero indicates that the connection will not disconnect)
Username:	You can keep the default (*ipmodule*) unless your wireless account requires your own user name.
Password:	You can keep the default (*ipmodule*) unless your wireless account requires your own individual password.
Baud Rate:	For CDMA and GPRS models, select **115200**. For EDGE models, select **230400**.
Dial Number:	**For CDMA models**, type **#777** **For GPRS and EDGE** models, type ***99***1#**.
APN:	**For GPRS and EDGE,** enter the APN (Access Point Name). The APN is assigned by your wireless service provider.
Init String 1:	You can set any initialization string you desire.
Submit:	Click the **SUBMIT** button.

9. Click **Save & Restart** (located on the Menu bar). The router will shut down and reboot.

10. After your router has restarted and the **IP** LED is flashing, wait for about 1 minute to be sure that the **TR** and **CD** LEDs are lit and showing a solid light (not blinking).

11. From the workstation, open the command window by clicking the **Start** button and selecting **Run**.

12. Type **CMD** to open the command window. Click **OK.**

13. When the command window opens, type **IPCONFIG /RELEASE** to release your current IP received from the router.

14. Then type **IPCONFIG /RENEW** to renew your IP address from the router. You should also receive a DNS addresses from the router.

15. Close the command window.

16. Open a Web browser. You are now connected to the Internet.

Chapter 3 – Using the Web Management Software

The Web Management software configures the Ethernet functionality of your MultiModem.

Navigating the Web Management Software

This section explains the menu structure and the navigation buttons of the router's Web Management software.

Menu Bar
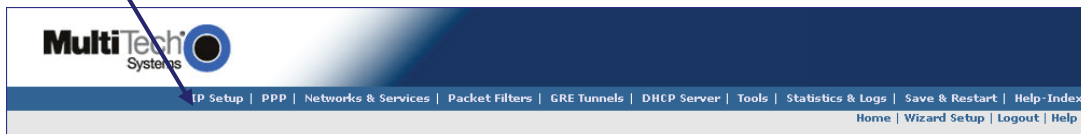
IP Setup: Sets up a General Configuration, HTTP, DDNS, SNTP, Static Routes, and Remote Configuration.

PPP: Sets up the PPP authentication, dial-on-demand, modem authentication, and Wakeup on Call.

Networks & Services: Defines networks and services to make them available to other functions such as allowed packet filters, DHCP Server, and Statistics & Logs.

Packet Filters: Defines filter rules, DNAT configuration, and ICMP rules.

GRE Tunnels: Generic Routing Encapsulation (GRE). Defines the remote network and the tunnel through which traffic is to be routed.

DHCP Server: Configures the DHCP server settings.

Tools: Sets DDNS Force Update and Reset Modem, displays Service Status, and provides screens for Firmware Upgrade, Load Configuration, and Save Configuration.

**Statistics & Logs:** Shows statistics and logs maintained by the modem.

Save & Restart: Saves your settings and reboots your PC.

Help Index: Accesses the online Help text.

IMPORTANT NOTE ABOUT _SUBMIT_ AND _SAVE & RESTART_

Click the **Submit** button located at the bottom of most screens in order to save any changes you make.
Then you must click the **Save & Restart** button, located on the Menu bar, in order for your settings to take effect.
Save & Restart does not have to be executed after each screen; you can change and **Submit** several screens, and then click **Save & Restart**.

Screen Parts

Menu Bar   **Submenu Title**   **Submenu List**
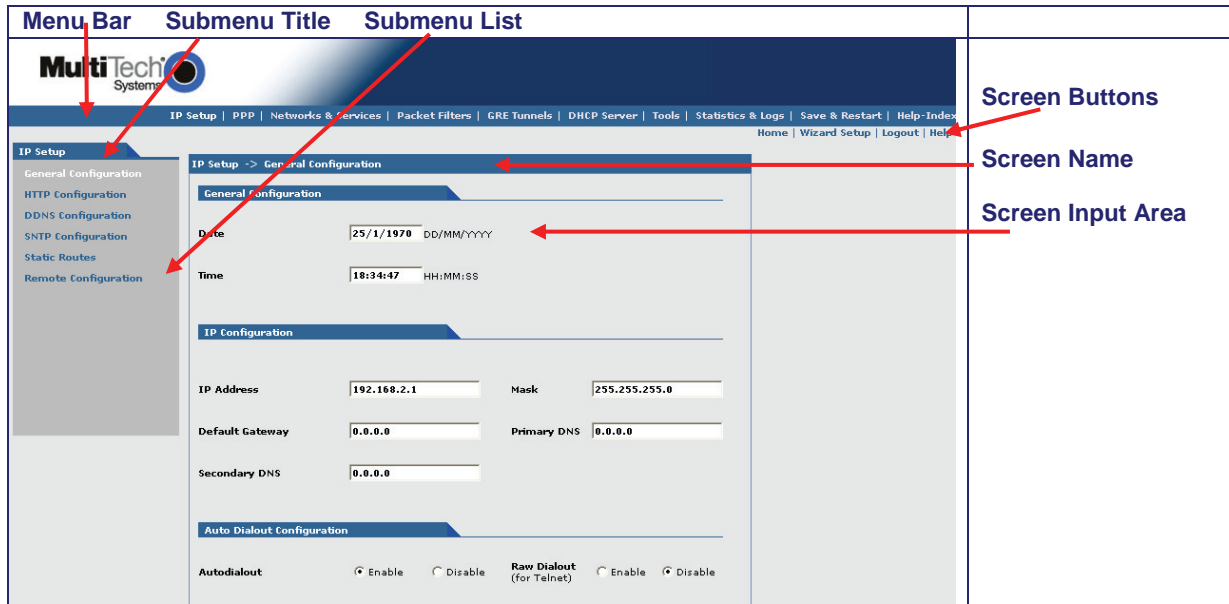
Screen Buttons

Home: Click this button to return to the Home screen.

Wizard Setup: Click this button to display the Wizard Setup screen on which you can quickly set up your wireless modem with basic configuration settings.

Logout: Click this button to Logout and return to the login screen.

Help: Click this button to display the Help text.

Submenus

The submenus display on the left side of the screen.

The following table shows the sub-menu selections under each main menu category.

IP Setup	PPP	Networks & Services	Packet Filters	GRE Tunnels	DHCP Server	Tools	Statistics & Logs
General Config. HTTP Config. DDNS Config. SNTP Config. Static Routes Remote Config.	PPP Config. Wakeup on Call Power On Config. Modem Commands	Network Configuration Service Configuration	Packet Filters DNAT Config. Advanced	GRE Tunnels GRE Routes	Subnet Settings Fixed Addresses	Tools Service Status Firmware Upgrade Load Config. Save Config.	Ethernet Serial PPP PPP Trace SysInfo DHCP Stat GRE Stat Modem Info

Web Management Software Screens

The rest of this chapter describes each of the Web Management software screens.

IP Setup
IP Setup > General Configuration
In the General Configuration, you will set the general system-based parameters.

General Configuration
Date and Time: The system date and time display in these formats: **DD/MM/YYYY / HH:MM:SS**. SNTP Client must be enabled and you must have a live Internet connection for the date and time to display correctly.

IP Configuration
Enter the following addresses for the Ethernet interface.
IP Address (Default = 192.168.2.1), Mask (Default 255.255.255.0), Default Gateway (Default 0.0.0.0), Primary DNS (Default 0.0.0.0), Secondary DNS (Default 0.0.0.0).
Note: See *Appendix A – Table of Commonly Supported Subnets.*

Auto Dialout Configuration
Auto Dialout: Check the box to enable/disable Auto Dialout. Default = Enable.
Raw Dialout: Check the box to enable/disable raw mode for an Auto Dialout session. Default = Disable.
Auto Dialout Login: Check the box to enable or disable Auto Dialout Login feature. Default = Enable.
Auto Dialout Port: Enter the serial Auto Dialout Port number. Default = 5000.
Handle EIA Signal: Check the box to enable/disable the EIA standard signal characteristics (time and duration) used between different electronic devices.
Inactivity: Enter the time in seconds that the auto dialout session will stay active before going inactive.

Syslog Configuration
Syslog: Check the box to enable or disable Syslog. Default = Disable.
Syslog Server IP Address: If a Remote Syslog Server IP Address is specified, the syslog feature acts as a remote Syslog.

Auto Discovery
Auto Discovery: Check the box to enable or disable Auto Discovery to broadcast (MAC level), the MAC Address, IP Address, and DHCP information to the configured server port. Default = Enable.
Server Port: Enter the Server Port Number. Default port is 1020.
Broadcast Timer: Enter the amount of time in seconds for the auto-discovery packet granularity of periodic broadcasting. Default is 10 seconds.

Auto Reboot Timer Configuration
Auto Reboot Timer: Enter the number of hours to lapse between each automatic reboot. The default of zero deactivates the timer. Range is 0 to 999.

Telnet Configuration
Enables/Disables the Telnet port. The default is **Enable**.

Submit Button
Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup > HTTP Configuration

HTTP Configuration
HTTP Port: Enter the port number on which the HTTP server will listen for requests. Default is 80.

Authentication
User Name: Enter the User Name that can access to the Web Management software. Default is **admin**.
Password: Enter the Password for access to the Web Management software. Default is **admin**.
Note: You should change the password to one of your choosing. It can be up to 12 characters. Use a safe password. Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

Submit Button
Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup > DDNS Configuration

DDNS (Dynamic Domain Naming System) updates the IP address of the modem/router in a DDNS server for the configured domain name whenever the IP Address changes; thus, it leaves the domain name pointing to the current IP Address of the modem/router at all times.

General
DDNS: Check the Enable or Disable box. This enables/disables DDNS. Default = Disable.

Use Check IP: Check the Enable or Disable box. If enabled, the program will query the server to determine the IP address before it performs the DDNS update (the IP address is still assigned by the wireless provider and the DDNS will be updated based on the address returned by Check IP Server). If disabled, the program will perform the DDNS update using the IP address that it obtains from the PPP link. Default = Enable.

Check IP Server: Enter the Server name from which the currently assigned IP address is obtained.
Check IP Port: Enter the port number of the *Check IP Server.* Default is 80.
Server: Enter the Server name to which the IP Address change is registered. Example: *members.dyndns.org*
Port: Enter the Server port number. Default is 80.
Max Retries: Enter the maximum number of tries that will be allowed if the update fails. Default = 5. Range is 0 – 100.
Update Interval: Enter the intervals in days that will be allowed to pass when there is no IP Address change. At the end of this interval, the existing IP Address will be updated in the server so that it will not expire. Default = 28 days. Range is 1 – 99 days.
System: Sets the system registration type as either Dynamic or Custom. Default = Dynamic.
Domain: Enter the registered Domain name.

Authentication
User Name: Enter the User Name that can access the DDNS Server. Default = NULL.
Password: Enter the Password that can access the DDNS Server. Default = NULL.

Submit
Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup > SNTP Configuration

General Configuration

SNTP Client: Enable or disable the SNTP Client to contact the configured server on the UDP port 123 and set the local time. The default is *Disable*.

Server: Enter the SNTP server name or IP address to which the SNTP Client must contact in order to update the time. No default.

Polling Time: Enter the polling time at which the SNTP client requests the server to update the time. Default is 300 minutes. Time must be entered in minutes.

Time Zone Configuration

Time Zone: Enter your time zone. Default = UTC (Universal Coordination).
See the following Web site for Time Zone information:
http://wwp.greenwichmeantime.com/info/timezone.htm

Time Zone Offset: Enter +/- hh:mm. Default = +00:00. Offset is the amount of time varying from the standard time of a Time Zone.

Daylight Configuration

Daylight Saving: Enables/disables Daylight Saving mode. The default is *Enable*.

Daylight Saving Offset: Set the offset to use during Daylight Saving mode. Default is +60 minutes. Enter the time in + / - minutes.

Daylight Saving Start Time

Start Ordinal: Set the start ordinal to use during Daylight Saving mode. Options are first/second/third/fourth/last. Default is first.

Daylight Saving time usually starts at the same time on the same day of the week in the same month every year. Each day of the week occurs four or five times a month. Therefore, you will be selecting the week in which daylight saving time starts: the first, second, third, fourth or the last of the month. In the U.S.A., daylight saving time starts at 2:00 a.m. on the first Sunday in April.

Start Month: Set the start month to use during Daylight Saving mode. Default is April.

Start Day: Set the start weekday to use during Daylight Saving mode. Default is Sunday.

Start Time: Set the start time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Daylight Saving End Time

End Ordinal: Set the end ordinal to use during Daylight Saving mode. Select the week in which daylight saving time ends. Options are first/second/third/fourth/last. Default is last.

End Month: Set the end month to use during Daylight Saving mode. Default is October.

End Day: Set the end weekday to use during Daylight Saving mode. Default is Sunday.

End Time: Set the end time to use during Daylight Saving mode. Default is 02:00 (hh:mm).

Submit Button

Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

IP Setup > Static Routes

Routing information is used by every computer connected to a network to identify whether it is sending a data packet directly to the firewall or passing it on to another network. The options to Delete or Edit a route after it has been defined and added are available by using the table at the bottom of the screen.

Add Static Routes

Static Route: Select a static route from the drop down list box, and then click the **Add** button.

Add Button: After clicking the **Add** button, the new route is added and will display at the bottom of the screen.

Important Note:

The Static Route screen will not display until the network is defined under **Networks & Services.**

IP Setup > Remote Configuration

Remote Configuration

Add Network/Host for Remote Configuration:
Select a network or host from the drop down box. The choices are Any, LAN, and WAN Interface. Choose all that apply. Click the **Add** button after each selection.

Add Button: After clicking the **Add** button, the network or host is added and displays at the bottom of the screen.

Delete: You will have the option to delete **Any** and **WAN Interface**.

PPP
PPP > PPP Configuration

NAT Configuration

NAT Enable/disable NAT (Network Address Translation). The default is *Enable*.

If NAT is enabled:
- Your LAN can use one set of IP addresses for internal traffic and a second set of addresses for external traffic. In other words, the router with NAT does the simple IP routing between the LAN interface and the WAN interface.
- Your internal addresses are shielded from the public Internet.

If NAT is disabled:
- The router functions without performing any address translation on the packets passing through it.
- Masquerading of packets originating from the LAN is disabled.
- Address translation of packets arriving from the WAN is also disabled.
- Any DNAT Configuration previously setup in the DNAT Configuration screen is disabled. This prevents the user from adding any DNAT rules, which if allowed would defeat the purpose of enabling Routing.

Note: For routing to take effect, the configuration must be saved after enabling it. It won't be effective on the fly at runtime.

PPP General

PPP	Enable/disable PPP. The default is *Enable*.
Dial-on-Demand:	Enable/disable Dial-on-Demand. The default is *Enable.* If you disable it, the modem will always stay connected.
Idle Time Out:	Set the amount of idle time that will pass before the modem will timeout. The default is 180 seconds.
Connect Time Out:	Set the number of seconds to wait for a connection while in receive mode before timing out.
Dialing Max Retries:	Enter the number of dialing retries allowed. The default is zero, which means an infinite number is allowed. Range 0 to 100.

Authentication

Authentication Type:	Set the authentication protocol type that will negotiate with the remote peer: pap/chap/pap-chap. Default is pap-chap.
User Name:	Enter the User Name with which the remote peer will authenticate. Default is ipmodule. You can leave this field blank, if desired.
Password:	Enter the Password with which the remote peer will authenticate. Default is ipmodule. You can leave this field blank, if desired.

ICMP Keep Alive Check

Keep Alive Check:	Enable/disable Keep Alive Check. The default is *Disable*.
Keep Alive Type:	Select ICMP or TCP (the protocol type for Keep Alive).
Host Name:	Enter the Host Name or IP Address for Keep Alive Check. No default.
TCP Port:	Enter the TCP Port number to connect with the TCP server.
Interval:	Set the number of seconds for Keep Alive Check. Default is 30 seconds.
ICMP Count:	Set the number of ICMP Keep Alive Checks to be sent to the specified host. Default is 10.

Modem Configuration

(Refer to the Customer Activation Notices included with the product for proper information to enter).

Baud Rate:	Set the serial baud rate. Default is 115200.
Dial Number:	Set the dial number to be dialed. Default is NULL. For **EDGE** or **GPRS** the number is ***99***1#**. For **CDMA** the number is **#777**.
Dial Prefix:	Set the modem dial prefix. The default is ATDT.
Connect String:	Set the modem Connect String. The default is CONNECT.
APN:	**For GPRS and EDGE,** enter the APN (Access Point Name). The APN is assigned by your wireless service provider.
Init String:	Configure the modem init strings. You can set up to 4 modem initialization strings.

Submit Button

Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

PPP > Wakeup-on-Call

The Wakeup-on-Call feature allows the modem to wake up and initiate a connection when there is an incoming call. If you desired some security with this feature, you can set up the modem to wake up based on Caller ID or SMS instead of allowing all incoming calls to wakeup the modem. The Wakeup-on-Call feature will reduce the cost incurred when a modem is online and available 24 / 7.

Wakeup-on-Call Configuration

Wakeup on Call: Enable/disable the Wakeup-on-Call feature. The default is *Disable*.

Time Delay: Enter the amount of time that you want to pass between the reception of a call and the initiation of the Wakeup-on-Call connection. A time delay is needed to make sure that the incoming call has ended before the connection is initiated. The default is 10 seconds.

Dial-on-Demand from LAN: The default is *Enable*. If this feature is disabled, Dial-on-Demand initiates PPP only from the WAN, not from the LAN.

Init Strings: Configure the modem initialization strings. Init-num can range from 1-5. The default is NULL.

Submit: Click the **SUBMIT** button to save these settings.

Caller ID Configuration

Add "Wakeup on Call" Caller ID: To add *Caller ID* to the *Wakeup-on-Call* function, enter the *Caller ID* to be allowed to wakeup the modem.

After entering the *Caller ID*, click the **Add** button. The *Caller ID* displays at the bottom of screen. You can enter any number of IDs you desire.

A Caller ID can be edited or deleted using *Options*, which will be available once a Caller ID is displayed.

Caller Acknowledgement Configuration

Acknowledgement String to Caller: The configured string of (0 to 40 characters) will be sent on modem upon receiving a valid caller ID from the WAN. The default is NULL string.

Note: If the string is not configured, acknowledgement to the caller will not be sent upon successful caller ID reception.

Submit

Click the **SUBMIT** button to save these settings.

Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

PPP > Wakeup-On-Call Examples

Example 1 – Set Up the Ethernet Router to Activate on Incoming SMS Message

Note: You must have firmware version 1.14 or above in order for **Wakeup-on-Call** to work.

1. On the *PPP > PPP Configuration* screen, set up the following parameters:

   PPP General
   - Make sure that **PPP** is *Enabled* (the default).
   - Make sure **Dial-on-Demand** is *Enabled* (the default).
   - Set the **Idle Time Out** to the number of seconds you desire.

   Authentication
   - Your wireless service provider may require you to have a separate PPP *User name* and *Password*. If so, enter them here. **Note:** If a user name and password are required, your wireless provider would have given them to you when you activated your account.

   Modem Configuration
   - Make sure your **Dial Number** is entered correctly:
       For CDMA, it is **#777**
       For GPRS and EDGE, it is ***99***1#**
   - Make sure your **Init String 1** is set up correctly.
       For GPRS and EDGE, **Init string 1** should be the **APN**.
       Example: **AT+CGDCONT=1,"IP","internet"**

   Submit
   - Click the **Submit** button to save the changes made on this screen.

2. On the *PPP > Wakeup-on-Call* screen, set up the following parameters:

   Wakeup-on-Call Configuration
   - Select *Enable* for **Wakeup-on-Call**.
   - Set the **Time Delay**. You can use the 10 second default.
   - Enter the **Init Strings:**

       For the EDGE modem:
       Enter Wakeup **Init String 1** as **at+cmgf=1**
       Enter Wakeup **Init String 2** as **at+csms=1**
       Enter Wakeup **Init String 3** as **at+cnmi=2,2,0,0,1**

       For the GPRS modem:
       Enter Wakeup **Init String 1** as **at+cmgf=1**
       Enter Wakeup **Init String 2** as **at+csms=1**
       Enter Wakeup **Init String 3** as **at+cnmi=2,2,0,0,0**

       For the CDMA modem:
       Enter Wakeup **Init String 1** as **at+cnmi=2,2,0,0,0**
   - Click the **Submit** button to save these settings.

   Caller ID Configuration
   - Enter a caller's ID that you want added to the Caller ID list.
     Note: Add the SMS message string into the Caller ID list. When the string configured matches the SMS message string, it will activate the Wakeup-on-Call feature.
   - **Add** Button
     Click the **Add** button to save each Caller ID as it is entered to the Caller ID list.

   Caller Acknowledgement Configuration
   - Enter a configured string that will be sent to the modem upon receiving a valid Caller ID from the WAN.
       For the CDMA, GPRS, and EDGE modems:
       Set the Wakeup Acknowledgement string configuration with the command **at+cnma**
   - Click the **Submit** button to save the Acknowledgement Configuration.

3. **Save and Restart**

   You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Example 2 – Determine if the Wireless Modem Is Supporting Incoming Calls and Caller ID

1. On the *PPP > PPP Configuration* screen, make sure that **PPP** is *Disabled*.

2. On the **PPP > Wakeup-on-Call** screen, make sure that **Wakeup-on-Call** is *Disabled*.

3. Open a command prompt by clicking the **Start** button and selecting **Run**.

4. Type **CMD** to open the command window. Click **OK**.

5. When the command window opens, type **Telnet 192.168.2.1 5000**
   Note: 5000 is the port number.

   5.1. Enter your user name and password to login.

   5.2. Enter an AT command to make sure you receive a response; i.e., *OK*.

   5.3. Enter the Command **AT+CNUM** to determine the dial number of your wireless modem.
   Note: For a CDMA modem, you might have to enter the command **AT+CICB=0**

6. From another phone, call your modem using the number identified in Step 5.3. This will let you know if the RING message shows.

7. To enable Caller ID, enter the **AT+CLIP=1** command on the command screen and make the call again to see if it shows Caller ID information.

Notes:
- Step 5.3 must show the RING or CALLER ID information in order for the Wakeup-on-Call function to work.
- Some wireless providers might not provide caller ID information if you have only a data plan.

Example 3 – Set Up the Ethernet Router to Activate on ALL Incoming Calls

1. On the *PPP >PPP Configuration* screen, set up the following parameters:

   PPP General
   - Make sure that **PPP** is *Enabled* (the default).
   - Make sure **Dial-on-Demand** is *Enabled* (the default).
   - Set the **Idle Time Out** to the number of seconds you desire.

   Authentication
   - Your wireless service provider may require you to have a separate PPP *User name* and *Password*. If so, enter them here. Note: If a user name and password are required, your wireless provider would have given them to you when you activated your account.

   Modem Configuration
   - Make sure your **Dial Number** is entered correctly:
     For CDMA, it is **#777**
     For GPRS and EDGE, it is ***99***1#**
   - Make sure your **Init String 1** is setup correctly.
     For GPRS and EDGE, **Init string 1** should be the **APN**.
     Example: **AT+CGDCONT=1,"IP","internet"**

   Submit
   - Click the **Submit** button to save the changes made on this screen.

2. On the *PPP > Wakeup-on-Call* screen, set up the following parameters:

   Wakeup-on-Call Configuration
   - Select *Enable* for **Wakeup-on-Call**.
   - Set the **Time Delay** to *3* seconds. You can use the 10 second default.
   - All **Init Strings** should be empty.
   - **Submit** Button
     Click the **Submit** button to save these settings.

   Caller ID Configuration
   - Enter the string **RING** to the Caller ID list.
   - Click the **Add** Button to save the string to the Caller ID list.

3. **Save and Restart**
   Click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Example 4 – Set Up the Ethernet Router to Activate on Matching Caller IDs Only:

1. On the *PPP > PPP Configuration* screen, set up the following parameters:

   ### PPP General
   - Make sure that **PPP** is *Enabled* (the default).
   - Make sure **Dial-on-Demand** is *Enabled* (the default).
   - Set the **Idle Time Out** to the number of seconds you desire.

   ### Authentication
   - Your wireless service provider may require you to have a separate PPP *username* and *password*. If so, enter them here. Note: If a username and password are required, your wireless provider would have given them to you when you activated your account.

   ### Modem Configuration
   - Make sure your **Dial Number** is entered correctly:
     For **CDMA**, it is **#777**
     For **GPRS and EDGE**, it is ***99***1#**
   - Make sure your **Init String 1** is setup correctly.
     For **GPRS and EDGE**, **Init string 1** should be the APN
     (i.e., **AT+CGDCONT=1,"IP","internet"**)

   ### Submit
   - Click the **Submit** button to save the changes made on this screen.

2. On the *PPP > Wakeup-on-Call* screen, set up the following parameters:

   ### Wakeup-on-Call Configuration
   - Select *Enable* for **Wakeup-on-Call**.
   - Set the **Time Delay**. Use can use the 10 second default.
   - Enter the **Init Strings:**
     Set Wakeup **Init String 1** by entering **AT+CLIP=1**
     Set Wakeup **Init String 2** by entering **AT+CICB=0** (CDMA only)
   - **Submit** Button
     Click the **Submit** button to save these settings.

   ### Caller ID Configuration
   - Enter a caller's ID that you want added to the Caller ID list.
   - **Add** Button
     Click the **Add** button to save each Caller ID as it is entered to the Caller ID list.

3. ### Save and Restart
   Click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

PPP > Power-On Configuration

The Power-On Configuration feature allows you to set an initialization string that will be sent to the modem upon boot up.

PPP -> PowerOn Configuration

'PowerOn Init String' Configuration

PowerOn Init String [   ]

SUBMIT

Power-On Init String Configuration

Power-On Init String: You can enter a string of 0 to 40 characters that will be sent to the modem upon boot up. All commands will initialize before you proceed with regular PPP related activity.
Note: When no initialization string is configured, regular functionality of the modem is retained.

Submit: Click the **SUBMIT** button to save this setting.
Note: You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

PPP > Modem Commands

Setting up certain modem commands will allow an external application to query modem information (based on the commands entered). The application can use the URL HTTP://192.168.2.1/modeminfo.html to get the IP address that is currently assigned to the wireless modem after the PPP connection is established. It also will show the results of up to ten AT commands entered here.

PPP -> Modem Commands

Modem AT Commands Configuration

AT 1: [   ]   AT 2: [   ]

AT 3: [   ]   AT 4: [   ]

AT 5: [   ]   AT 6: [   ]

AT 7: [   ]   AT 8: [   ]

AT 9: [   ]   AT 10: [   ]

SUBMIT

These commands will be sent every time a PPP connection to the network is initiated.

Example of Useful GPRS AT Commands:

AT+CGSN	Product Serial Number
AT+CGMR	Software Version
AT+CNUM	Wireless Subscriber Number
AT+COPS?	Network Information (Operator)
AT+CREG?	Network Registration
AT+CSQ	Signal Quality

Notes:
- You can also retrieve the modem information without using a browser:
  Make a TCP connection to port 80 (same as the Web Admin port) and send data as:
  GET /atinfor.html HTTP/1.1
  Then press **Enter** twice.
- See the GPRS AT Command Reference Guide (Number S000293x) for other commands.

Networks & Services
Networks & Services > Network Configuration

Networks or Hosts can be added here. The options to Delete or Edit a network after it has been defined and added are available by using the table at the bottom of the screen.

Network Configuration

Enter the Name, IP Address, and Mask for a new Network or Host.

Notes:
- A Network/Host Name cannot be edited.
- A Network/Host cannot be deleted if it is used in another configuration.
- Network/Host changes are reflected in all the configurations in the Web Management software where they are used.
- A Network/Host added here will be displayed in the following sections: Static Routes, DNAT, and Packet Filters.

Name:	Enter the name of the Network/Host. The same address-mask pair should not already be present in the displayed list.
IP Address:	Enter the IP Address of the Network/Host. The same address-mask pair should not already be present in the displayed list.
Subnet Mask:	Enter the Network Mask of the Network/Host. For Host addresses, the mask is entered as 32. *Note:* See *Appendix A -- Table of Commonly Supported Subnets.*
Add Button:	Click the **Add** button. The defined network is added and will display at the bottom of the screen.

Networks & Services > Service Configuration

On this screen you can specify the standard set of well known services available on the system. These services enable the configuration of the user-defined services. The options to Delete or Edit a service after it has been defined and added are available by using the table at the bottom of the screen.

Networks & Services -> Service Configuration

Service Configuration

Name	Protocol	S-Port/Client	D-Port/Server
	tcp		

ADD

Name	Protocol	S-Port	D-Port	Options
Any	any	1:65535	1:65535	Static
DNS-tcp	tcp	1:65535	53	Static
DNS-udp	udp	1:65535	53	Static
FTP	tcp	1024:65535	20:21	Static
FTP-CONTROL	tcp	1024:65535	21	Static
H323	tcp	1024:65535	1720	Static
HTTP	tcp	1024:65535	80	Static
HTTPS	tcp	1024:65535	443	Static
IDENT	tcp	1024:65535	113	Static
IMAP	tcp	1024:65535	143	Static
netbios-dgm-tcp	tcp	138	138	Static
netbios-dgm-udp	tcp	138	138	Static
netbios-ns-tcp	tcp	137	137	Static
netbios-ns-udp	udp	137	137	Static
netbios-ssn-tcp	tcp	1024:65535	139	Static
netbios-ssn-udp	udp	1024:65535	139	Static
NEWS	tcp	1024:65535	119	Static
POP3	tcp	1024:65535	110	Static
PPTP	tcp	1024:65535	1723	Static
SMTP	tcp	1024:65535	25	Static
SNMP	udp	1024:65535	161	Static
SNTP	tcp	1024:65535	123	Static
SOCKS	tcp	1024:65535	1080	Static
SQUID	tcp	1024:65535	3128	Static
SSH	tcp	1:65535	22	Static
TFTP	udp	1:65535	69	Static
TELNET	tcp	1024:65535	23	Static
TRACEROUTE	udp	1024:65535	33000:34000	Static

Service Configuration

Enter the Name, Protocol, Source Port/Client, and Destination Port/Server for the new Service.

- A Service Name cannot be edited.
- A Service cannot be deleted if it is used in another configuration.
- Service changes are reflected in all the configurations in the Web Management software where they are used.
- Services added here will be displayed in the following sections: DNAT, Packet Filters.

Name: Enter the name of the Service. It has to be unique.
Protocol: Enter the type of protocol (ITCP, UDP).
Source Port: Enter the Source Port for this service.
Destination Port: Enter the name of the Destination Port for the service.
Add Button: Click the **Add** button. The new service is added and will display on the screen.

Packet Filters
Packet Filters > Packet Filters.
You can Delete or Edit a packet filter rule after it has been defined and added by using the table at the bottom of the screen.

Packet Filter
From (Host/Networks): Enter the network/host from which the packet must originate for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned addresses or private addresses, may also be entered. The network/host must be pre-defined in the Networks section.

Service: Enter the service that is to be matched with the filter rule. These services must be pre-defined in the Services section. These services precisely define the traffic to be filtered.

To (Host/Networks): Enter the network/host to which the packet must send for the filter rule to match. The *Any* option, which matches all IP addresses regardless of whether they are officially assigned addresses or private addresses, may also be entered. The network/host must be pre-defined in the Networks section.

Action: Enter the action that the packet filter executes if the rule matches any traffic traversing the firewall. Types of actions defined are:

Accept: Allows/accepts all packets that match this rule.

Reject: Blocks all packets that match this rule. The host sending the packet will be informed that the packet has been rejected.

Drop: Blocks all packets that match this rule, but the host is not informed; i.e., this is a silent drop.

Log: Packets matching the rule; i.e., the corresponding source address, destination address, and service will be logged.

Add Button: Click the **Add** button. The defined packet filter rule is added and will display at the bottom of the screen.

Packet Filters > DNAT Configuration

Destination Network Address Translation (DNAT) is a process that allows the placing of servers within the protected network and making them available for a certain service to the outside world. The DNAT process running of the wireless modem/router translates the destination address of incoming packets to the address of the real network server on the LAN. The packets are then forwarded.

You can Delete or Edit a DNAT rule after it has been defined and added by using the table at the bottom of the screen.

Important Note: When adding rules, at least one host must be defined in the Network Configuration section.

DNAT Configuration

Allow Access:	Select a network or host to which IP packets will be allowed and re-routed. The network/host must be pre-defined in the Network Configuration section.
External Service:	Select the External Service that you want allowed. The service must be defined in the Service Configuration section.
LAN IP:	Select the LAN IP to which the packets are to be diverted. Only one host can be defined as the destination.
Internal Service:	Select the Internal Service to be the destination.
Internal Source:	Select the source address for packets that going to be sent. If you do not want to change the address, select **NOCHANGE**.
Save Button:	Click the **Save** button. The defined DNAT configuration is added and will display at the bottom of the screen. Entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Packet Filters > DNAT Example
Set Up DNAT and Port Forwarding to an Internal Device

Note: The internal device can be camera, meter, security device, etc.

Situation: Assume the device is on a LAN with an IP address of 192.168.2.100 and the port to access the device is port 7700.

1. On the **Network & Services > Network Configuration** screen, set up the following parameters:

   Name – Enter a name for the LAN device.

   IP Address and Subnet Address – Enter the IP address and subnet address of the device.
   > **Example:** Name = MeterIP
   > IP Address = 192.168.2.100
   > Subnet Address = 255.255.255.255

   Add – Click the **Add** button to save this configuration.

2. On the **Network & Services > Service Configuration** screen, define a service name. For this example, the service will be a meter.

   Name – Enter a name for the service (use a name that will identify the service for you).
   > **Example:** MeterPort

   Protocol – Select a protocol.
   > **Example:** tcp/udp

   S-Port / Client – Enter the source port for this service.
   > **Example:** 1:65535

   D-Port / Server – Enter the destination port for this service.
   > **Example:** 7700

   Add – Click the **Add** button to save this configuration.

3. On the **Packet Filters > DNAT Configuration** screen, define the DNAT rule.

> **Source –**   Select the original target network/host of the IP packets that you now want rerouted. The original target network/host is the one previously defined in the Network Configuration section.
>
> > **Example:** Any
>
> **Pre DNAT Service –**   Select the service for the Pre-DNAT destination. This service was just defined in the Service Configuration section.
>
> > **Example:** MeterPort
>
> **Post DNAT IP –** Select the destination to which the IP packets are to be diverted. Only one host can be defined as the Post DNAT destination.
>
> > **Example:** MeterIP
>
> **Post DNAT Service –** Select the service for the Post DNAT configuration.
>
> > **Example:** MeterPort
>
> **Internal Source –** Select the source address for packets that going to be sent. If you do not want to change the address, select **NOCHANGE**.
> > **Example:** NOCHANGE

4. **Save –**   Click the **Save** button to save this configuration. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device will save all the settings and reboot the PC.

Packet Filters > Advanced

Connection Tracking
H323: Enable/disable the forwarding of H323 packets across the firewall.
PPTP: Enable/disable PPTP Packet Pass-through (PPTP NAT support).

ICMP Configuration
The Internet Control Message Protocol (ICMP) is used to test the network connections and the functionality of the firewall and is also used for diagnostic purposes. *ICMP on Firewall* and *ICMP Forwarding* always apply to all IP addresses; i.e., *Any*. When these are enabled, all IP hosts can Ping the firewall (*ICMP on Firewall*) or the network behind it (*ICMP Forwarding*).
ICMP on LAN: Enable/disable the transfer of ICMP packets on the LAN interface.
ICMP on WAN: Enable/disable the transfer of ICMP packets on the WAN interface.
ICMP Forward: Enable/disable the forwarding of ICMP packets through the firewall into the local network.

Submit
Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

GRE Tunnels

GRE tunneling and GRE routing together are referred to Generic Routing Encapsulation (GRE). GRE Routing is an integral part of GRE tunneling. First, the GRE Tunnels are created using the GRE Tunnel Configuration. Then the routes for the remote networks that are to be routed through a tunnel need to be specified in the GRE Routes Configuration. Thus, all the traffic destined to remote networks associated to a tunnel will get routed through that tunnel.

GRE Tunnels > GRE Tunnels

Tunneling allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols. If you want to read more about how this works, see the online Help.

GRE Tunnel Configuration

Tunnel Name: Enter a name for the new tunnel.

Local IP: Select the local interface on which the tunnel is being created. Eventually, the packets destined for this tunnel will be routed through it.

Note: When adding a tunnel, use only one of the following: **Remote IP** or **FQDN**.

Remote IP: Select the Remote IP address that marks the other end point of the tunnel (this is the one to which the routed packets will be received).

OR

FQDN: Enter the FQDN (Fully Qualified Domain Name) for the Remote IP, which can be either the IP Address of an FQDN.

Add Button: Click the **Add** button. The defined GRE tunnel configuration is added and will display at the bottom of the screen.

GRE Tunnels > GRE Routes Configuration

GRE Routes Configuration

Remote Network:	Select the remote network for which the traffic destined to it must be routed through the given tunnel.
Tunnel Name:	Select the name of the tunnel through which the traffic will be routed.
Note:	To add a tunneled route, the remote network and the tunnel must have been defined in Network Configuration. The tunnel configuration must be completed before setting the GRE route configuration.
Add Button:	Click the **Add** button. The defined GRE route configuration is added and will display at the bottom of the screen.

DHCP Server
DHCP Server > Subnet Settings

General Configuration

DHCP (Dynamic Host Configuration Protocol) is a protocol that allows individual devices on an IP network to get their own network configuration information (IP address, subnet mask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network.

DHCP:	Enable/disable the DHCP server.
Subnet:	Enter the subnet address. For the subnet change, all the ranges have to be deleted; otherwise, you would not be able to edit the subnet.
Mask:	Enter the subnet mask address.
Gateway:	Enter the gateway address.
DNS:	Enter the DNS address.
Lease Time:	Select the DHCP Lease Time from the selection box. Lease time is set in days, hours, and minutes. A Lease Time of 00-00-00 is an Infinite Lease Time.
Submit	Click the **Submit** button to save these settings. **Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes.

Subnet Settings

From-To Range:	Enter the range of IP address for the subnet. For every range, the *From* and the *To* addresses have to be entered in these fields.
Add:	Click the **Add** button. The address range is added and will display in the table at the bottom of the screen. Once the range displays, you can delete if necessary.
Note:	See *Appendix A – A Table of Commonly Supported Subnets.*

DHCP Server > Fixed Addresses

DHCP Server -> Fixed Addresses

DHCP Subnet Settings

Mac-Address [   ]   IP Address [   ]

ADD

Mac-Address	IP Address	Options

DHCP Fixed Configuration
The DHCP server can be made to assign a fixed IP address for a particular user by identifying the MAC address. This binding can be made permanent by configuring it here. The same IP address will not be used for any DHCP client with a different MAC address, even if there is no active DHCP connection with that IP address.

MAC Address: Enter the MAC address to which the specified IP address binds.
IP Address: Enter the fixed IP address to be assigned.
Add: Click the **Add** button. The addresses are added and will display in the table at the bottom of the screen from where they can be deleted or changed.

Tools
Tools > Tools

Tools
Tools
Service Status
Firmware Upgrade
Load Configuration
Save Configuration

Tools -> Tools

DDNS

DDNS Force Update   Update

DDNS Status: DDNS is disabled   Refresh

Modem

Reset Modem   Reset

DDNS
DDNS Force Update: Click the **Update** button to give the DDNS force update condition.
DDNS Status: Click the **Refresh** button to display the DDNS Status after a forced update.

Modem
Reset Modem: Click the **Reset** button to reset the wireless modem.

Tools > Service Status

This screen displays the status of each service that is available at run time. The first column lists the services available at run time; the second column identifies the configuration (enabled/disabled); the third column reports the current status of each service.

Tools

Tools
Tools
Service Status
Firmware Upgrade
Load Configuration
Save Configuration

Tools -> Service Status

Service Name	Configuration	Status
DDNS		DDNS is disabled
SNTP	disable	SNTP is disabled
Ping Keep Alive		PING Keep alive is disabled
Dial-on-Demand	enable	PPP Link is up

Tools > Firmware Upgrade

Tools

Tools
Tools
Service Status
Firmware Upgrade
Load Configuration
Save Configuration

Tools -> Firmware Upgrade

Firmware Upgrade

Browse file for upgrade [ ] Browse...

Upgrade

Firmware Upgrade

Browse File for Upgrade: Click the **Browse** button and select the firmware bin file. When found, highlight the file name and press **Enter** so that the file name displays in the text box. Make sure you select the correct BIN file; otherwise, your MTCBA-x-EN can become inoperable. Then click the **Upgrade** button.

When upgrade is completed, the program will return to the main login screen.

Important Notes:

- **Firmware Upgrade** is available only when **Firmware Upgrade Configuration** is enabled on the IP Setup screen.
- The new firmware is written into the flash.
- A **Firmware Upgrade** will take at least 3 minutes while the firmware is downloaded. Do not cycle power during this time.
- **DO NOT** perform firmware upgrade remotely via the Cellular wireless connection.

Tools > Load Configuration
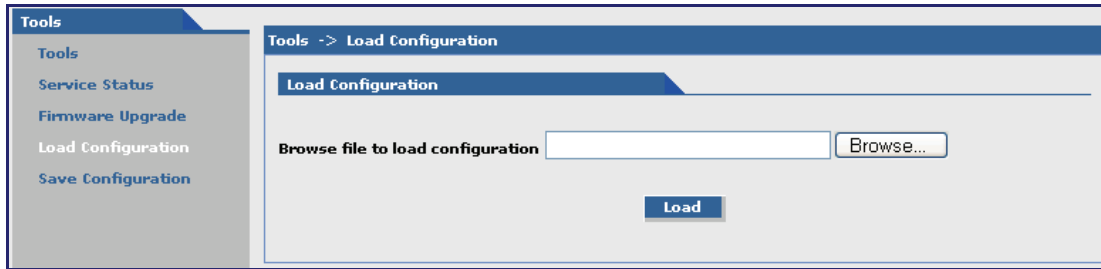
Load Configuration

Browse File for Load Configuration: Click the **Browse** button to open the file that allows you to locate the configuration file. When found, highlight the file name and press Enter so that the file name displays in the text box. Then click the **Load** button.

Important Notes:
* The new configuration is written into the flash.
* A **Configuration Upgrade** will take at least 3 seconds to download and 60 seconds to install the settings and reboot. Reboot happens automatically.

When you click the **Load** button, the following screen displays. It shows the name of the file you selected.
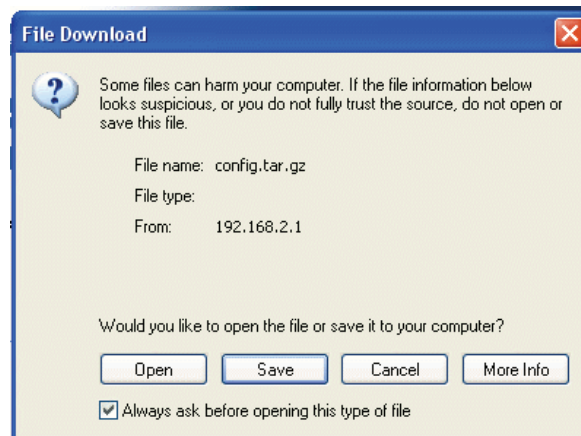
Click the **Open**, **Save**, **Cancel**, or **More Info** buttons as desired. The **More Info** button displays Microsoft's Internet Explorer Help on downloading files.

Tools > Save Configuration

Click this option to save the configuration.

Statistics & Logs
Statistics & Logs > Ethernet

This is an example of the Ethernet Statistics & Logs screen. It shows Ethernet statistics.

Statistics & Logs > Serial

This is an example of the Serial Statistics & Logs screen. It shows serial statistics.

Statistics & Logs > PPP

Statistics & Logs -> PPP	
	pppO statistics		
PPP Link	UP (dialed)
PPP Local ip	208.54.128.253
PPP Remote ip	192.168.111.111
MTU	1500 bytes
Rx Bytes	260535 bytes
Rx Packets	313
Rx Errors	0
Rx dropped	0
Rx Overruns	0
Rx Frame	0
Rx Compressed	0
Tx Bytes	37738 bytes
Tx Packets	344
Tx Errors	0
Tx dropped	6
Tx Overruns	0
Tx Carrier	0
Tx Collisions	0
Tx Compressed	0
Tx Queue Length	3

This is an example of the PPP Statistics & Logs screen. It shows PPP statistics when PPP is enabled.

Statistics & Logs > PPP Trace

This is an example of the PPP Trace Statistics & Logs screen. It shows the PPP Trace messages.

Statistics & Logs > SysInfo

This is an example of the System Information Statistics & Logs screen. It shows the information of the module: processor details, uptime memory, utilization, version, date, binary details.

Statistics & Logs > DHCP Stat

This is an example of the DHCP Statistics & Logs screen. It shows the statistics of DHCP leases.

Statistics & Logs > GRE Statistics

This screen displays the statistics of active tunnels.

Statistics & Logs > Modem Information

This screen displays the modem commands set on the **PPP > Modem Commands** screen and also displays the results of the commands.

Appendix A – A Reference Table of Commonly Supported Subnets

This table lists commonly supported Subnets organized by Address.

	Network Number	Hosts Available	Broadcast Address
255.255.255.128 /25	N.N.N.0	N.N.N.1-126	N.N.N.127
	N.N.N.128	N.N.N.129-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.192 /26	N.N.N.0	N.N.N.1-62	N.N.N.63
	N.N.N.64	N.N.N.65-126	N.N.N.127
	N.N.N.128	N.N.N.129-190	N.N.N.191
	N.N.N.192	N.N.N.193-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.224 /27	N.N.N.0	N.N.N.1-30	N.N.N.31
	N.N.N.32	N.N.N.33-62	N.N.N.63
	N.N.N.64	N.N.N.65-94	N.N.N.95
	N.N.N.96	N.N.N.97-126	N.N.N.127
	N.N.N.128	N.N.N.129-158	N.N.N.159
	N.N.N.160	N.N.N.161-190	N.N.N.191
	N.N.N.192	N.N.N.193-222	N.N.N.223
	N.N.N.224	N.N.N.225-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.240 /28	N.N.N.0	N.N.N.1-14	N.N.N.15
	N.N.N.16	N.N.N.17-30	N.N.N.31
	N.N.N.32	N.N.N.33-46	N.N.N.47
	N.N.N.48	N.N.N.49-62	N.N.N.63
	N.N.N.64	N.N.N.65-78	N.N.N.79
	N.N.N.80	N.N.N.81-94	N.N.N.95
	N.N.N.96	N.N.N.97-110	N.N.N.111
	N.N.N.112	N.N.N.113-126	N.N.N.127
	N.N.N.128	N.N.N.129-142	N.N.N.143
	N.N.N.144	N.N.N.145-158	N.N.N.159
	N.N.N.160	N.N.N.161-174	N.N.N.175
	N.N.N.176	N.N.N.177-190	N.N.N.191
	N.N.N.192	N.N.N.193-206	N.N.N.207
	N.N.N.208	N.N.N.209-222	N.N.N.223
	N.N.N.224	N.N.N.225-238	N.N.N.239
	N.N.N.240	N.N.N.241-254	N.N.N.255

	Network Number	Hosts Available	Broadcast Address
255.255.255.248 /29	N.N.N.0	N.N.N.1-6	N.N.N.7
	N.N.N.8	N.N.N.9-14	N.N.N.15
	N.N.N.16	N.N.N.17-22	N.N.N.23
	N.N.N.24	N.N.N.25-30	N.N.N.31
	N.N.N.32	N.N.N.33-38	N.N.N.39
	N.N.N.40	N.N.N.41-46	N.N.N.47
	N.N.N.48	N.N.N.49-54	N.N.N.55
	N.N.N.56	N.N.N.57-62	N.N.N.63
	N.N.N.64	N.N.N.65-70	N.N.N.71
	N.N.N.72	N.N.N.73-78	N.N.N.79
	N.N.N.80	N.N.N.81-86	N.N.N.87
	N.N.N.88	N.N.N.89-94	N.N.N.95
	N.N.N.96	N.N.N.97-102	N.N.N.103
	N.N.N.104	N.N.N.105-110	N.N.N.111
	N.N.N.112	N.N.N.113-118	N.N.N.119
	N.N.N.120	N.N.N.121-126	N.N.N.127
	N.N.N.128	N.N.N.129-134	N.N.N.135
	N.N.N.136	N.N.N.137-142	N.N.N.143
	N.N.N.144	N.N.N.145-150	N.N.N.151
	N.N.N.152	N.N.N.153-158	N.N.N.159
	N.N.N.160	N.N.N.161-166	N.N.N.167
	N.N.N.168	N.N.N.169-174	N.N.N.175
	N.N.N.176	N.N.N.177-182	N.N.N.183
	N.N.N.184	N.N.N.185-190	N.N.N.191
	N.N.N.192	N.N.N.193-198	N.N.N.199
	N.N.N.200	N.N.N.201-206	N.N.N.207

	N.N.N.208	N.N.N.209-214	N.N.N.215
	N.N.N.216	N.N.N.217-222	N.N.N.223
	N.N.N.224	N.N.N.225-230	N.N.N.231
	N.N.N.232	N.N.N.233-238	N.N.N.239
	N.N.N.240	N.N.N.241-246	N.N.N.247
	N.N.N.248	N.N.N.249-254	N.N.N.255
	Network Number	**Hosts Available**	**Broadcast Address**
255.255.255.252	N.N.N.0	N.N.N.1-2	N.N.N.3
/30	N.N.N.4	N.N.N.5-6	N.N.N.7
	N.N.N.8	N.N.N.9-10	N.N.N.11
	N.N.N.12	N.N.N.13-14	N.N.N.15
	N.N.N.16	N.N.N.17-18	N.N.N.19
	N.N.N.20	N.N.N.21-22	N.N.N.23
	N.N.N.24	N.N.N.25-26	N.N.N.27
	N.N.N.28	N.N.N.29-30	N.N.N.31
	N.N.N.32	N.N.N.33-34	N.N.N.35
	N.N.N.36	N.N.N.37-38	N.N.N.39
	N.N.N.40	N.N.N.41-42	N.N.N.43
	N.N.N.44	N.N.N.45-46	N.N.N.47
	N.N.N.48	N.N.N.49-50	N.N.N.51
	N.N.N.52	N.N.N.53-54	N.N.N.55
	N.N.N.56	N.N.N.57-58	N.N.N.59
	N.N.N.60	N.N.N.61-62	N.N.N.63
	N.N.N.64	N.N.N.65-66	N.N.N.67
	N.N.N.68	N.N.N.69-70	N.N.N.71
	N.N.N.72	N.N.N.73-74	N.N.N.75
	N.N.N.76	N.N.N.77-78	N.N.N.79
	N.N.N.80	N.N.N.81-82	N.N.N.83
	N.N.N.84	N.N.N.85-86	N.N.N.87
	N.N.N.88	N.N.N.89-90	N.N.N.91
	N.N.N.92	N.N.N.93-94	N.N.N.95
	N.N.N.96	N.N.N.97-98	N.N.N.99
	N.N.N.100	N.N.N.101-102	N.N.N.103
	N.N.N.104	N.N.N.105-106	N.N.N.107
	N.N.N.108	N.N.N.109-110	N.N.N.111
	N.N.N.112	N.N.N.113-114	N.N.N.115
	N.N.N.116	N.N.N.117-118	N.N.N.119
	N.N.N.120	N.N.N.121-122	N.N.N.123
	N.N.N.124	N.N.N.125-126	N.N.N.127
	N.N.N.128	N.N.N.129-130	N.N.N.131
	N.N.N.132	N.N.N.133-134	N.N.N.135
	N.N.N.136	N.N.N.137-138	N.N.N.139
	N.N.N.140	N.N.N.141-142	N.N.N.143
	N.N.N.144	N.N.N.145-146	N.N.N.147
	N.N.N.148	N.N.N.149-150	N.N.N.151
	N.N.N.152	N.N.N.153-154	N.N.N.155
	N.N.N.156	N.N.N.157-158	N.N.N.159
	N.N.N.160	N.N.N.161-162	N.N.N.163
	N.N.N.164	N.N.N.165-166	N.N.N.167
	N.N.N.168	N.N.N.169-170	N.N.N.171
	N.N.N.172	N.N.N.173-174	N.N.N.175
	N.N.N.176	N.N.N.177-178	N.N.N.179
	N.N.N.180	N.N.N.181-182	N.N.N.183
	N.N.N.184	N.N.N.185-186	N.N.N.187
	N.N.N.188	N.N.N.189-190	N.N.N.191
	N.N.N.192	N.N.N.193-194	N.N.N.195
	N.N.N.196	N.N.N.197-198	N.N.N.199
	N.N.N.200	N.N.N.201-202	N.N.N.203
	N.N.N.204	N.N.N.205-206	N.N.N.207
	N.N.N.208	N.N.N.209-210	N.N.N.211
	N.N.N.212	N.N.N.213-214	N.N.N.215
	N.N.N.216	N.N.N.217-218	N.N.N.219
	N.N.N.220	N.N.N.221-222	N.N.N.223
	N.N.N.224	N.N.N.225-226	N.N.N.227
	N.N.N.228	N.N.N.229-230	N.N.N.231
	N.N.N.232	N.N.N.233-234	N.N.N.235
	N.N.N.236	N.N.N.237-238	N.N.N.239
	N.N.N.240	N.N.N.241-242	N.N.N.243
	N.N.N.244	N.N.N.245-246	N.N.N.247
	N.N.N.248	N.N.N.249-250	N.N.N.251
	N.N.N.252	N.N.N.253-254	N.N.N.255

Appendix B – Wireless Antenna

The Antenna

The antenna sub-system and integration in the application is a major issue: Choice of antenna (type, length, performances, thermal resistance, etc.) These elements could affect GSM performances such as sensitivity and emitted power.

PTCRB Requirements Note:

There cannot be any alteration to the authorized antenna system. The antenna system must be the same type with similar in-band and out-of-band radiation patterns and maintain the same specifications.

FCC Requirements Note:

The antenna gain, including cable loss, must not exceed 3.0 dBi at 1900 MHz / 1.6 dBi at 850 MHz for mobile operating configurations and 7.0 dBi at 1900 MHz / 2.3 dBi at 850 MHz for fixed mounted operations, as defined in 2.1091 and 1.1307 of the rules for satisfying RF exposure compliance.

GSM, EDGE, and CDMA Antenna

The integrated modem antenna connector is a SMA connector. The SMA connector incorporates a 'Screw-on' action in order to make the connection easier while providing an excellent RF performance. An additional advantage is its small physical size, which is 50% of the standard MCX connector.

This type of connector is suitable for the standard ranges of flexible and semi-rigid cables. The characteristic impedance of the MMCX coaxial connector is 50 ohm. The antenna manufacturer must guarantee that the antenna will be working according to the radio characteristics presented in the table below.

GSM and E-GSM Radio Characteristics

	GSM 850	E-GSM 900	GSM 1800	GSM 1900
Frequency RX	869 to 894 MHz	925 to 960 MHz	1805 to 1880 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz
RF Power Stand	2W at 12.5% duty cycle	2W at 12.5% duty cycle	1W at 12.5% duty cycle	1W at 12.5% duty cycle
Impedance	50 ohms			
VSWR	<2			
Typical Radiated Gain	0 dBi on azimuth plane			

CDMA Radio Characteristics

	CDMA 800	CDMA 1900
Frequency RX	869 to 894 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	1850 to 1910 MHz
Impedance	50 ohms	
VSWR	<2	
Typical Radiated Gain	0 dBi in at least one direction	

Fused DC Power Cable Dimensions
How to Change the Fuse

The Fused DC power cable is provided when a single unit is purchased.
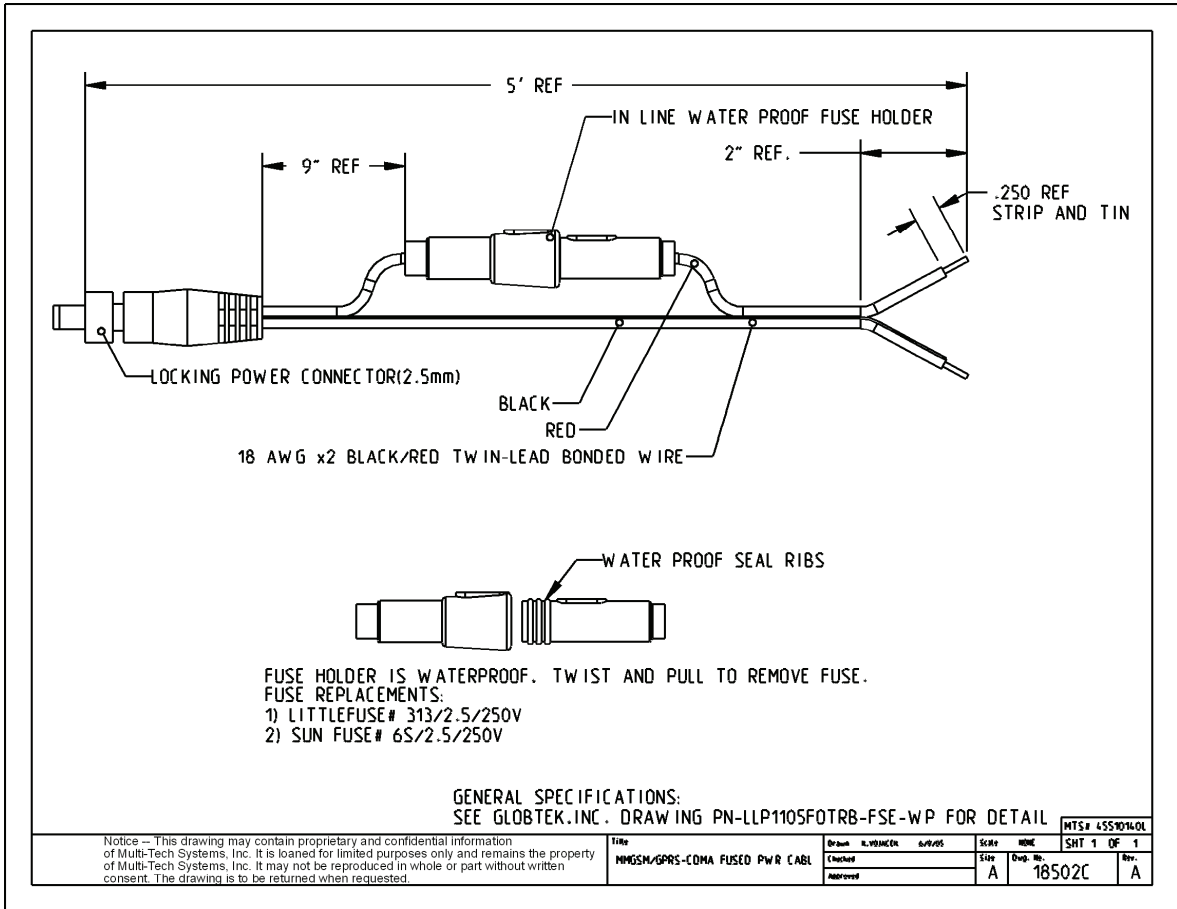
Appendix C – Firmware Upgrade Using External TFTP Client

Follow the steps below to install new firmware from the Multi-Tech Systems, Inc. Web site:

Obtaining the Latest Firmware Version
To obtain the latest version of the firmware, contact you Multi-Tech Sales Representative or contact Multi-Tech directly by phone or email:

        Phone: 763-785-3500 or 800-328-9717
        See the Multi-Tech Web site: www.multitech.com

1. Open the modem/router's Web Management software using a Web Browser. Enter the Gateway Address http://192.168.2.1 (default) and complete the login.

2. Go to the **IP Setup > General Configuration** screen and check the **Enable** button for **Firmware Upgrade** under the **TFTP Configuration** at the button of the screen.

3. Click **Save & Restart** located on the Menu bar.

4. Then open the DOS screen by clicking the PC's **Start** button and selecting **Programs > Accessories > Command Prompt**.

5. At the **C:** prompt, enter the upload request by typing the following:

    tftp -i <ip-address> put <firmware-filename>-tftp.bin AMD-tftp.bin

    Then press **Enter.**

    Example: tftp -i 192.168.254.253 put c:\example.bin   (Press Enter)

        Definitions of the Upload Request Parameters:

- **<ip-address>**
Address of the Serial-to-Ethernet Adapter to which you are uploading the firmware image.
- **<firmware filename>**
Filename under which the firmware file was saved on your PC or local network.
- **AMD-tftp.bin <>**
. This is a case-sensitive file name; type it as shown here.

6. After the upgrade is completed, open the Web Management software to see if the new version shows.

Appendix D – Multi-Tech Systems, Inc. Warranty and Repair Policies

Multi-Tech Warranty Statement

Multi-Tech Warranty Statement

Multi-Tech Systems, Inc., (hereafter "MTS") warrants that its products will be free from defects in material or workmanship for a period of two, five, or ten years (depending on model) from date of purchase, or if proof of purchase is not provided, two, five, or ten years (depending on model) from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by Customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory — transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES, AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PRICE FOR DEFECTIVE PRODUCTS.

Repair Procedures for U.S. and Canadian Customers

In the event that service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota factory:

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112 U.S.A.
Attn: Repairs, Serial # _____

A Returned Materials Authorization (RMA) is not required. Return shipping charges (surface) will be paid by MTS to destinations in U.S. and Canada.

Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), and your telephone number. If the product is out of warranty, a payment in advance is required. Acceptable means of payment include credit card, wire transfer or a check in U.S. dollars drawn on a U.S. Bank.

For out of warranty repair charges, go to COMPANY/Policies/warranty/

Extended two-year overnight replacement service agreements are available for selected products. Please call MTS customer service at (888) 288-5470 or visit our web site at /PARTNERS/Programs/overnight_replacement/ for details on rates and coverages.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department at (800) 972-2439 or email support@multitech.com. Please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at (800) 328-9717 or (763) 717-5631, or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Customers

(Outside U.S.A. and Canada)

Your original point-of-purchase Reseller may offer the quickest and most economical repair option for your Multi-Tech product. You may also contact any Multi-Tech sales office for information about the nearest distributor or other repair service for your Multi-Tech product. The Multi-Tech sales office directory is available at www.multitech.com/PARTNERS/Channels/offices/

In the event that factory service is required, products may be shipped, freight prepaid to our Mounds View, Minnesota factory. Recommended international shipment methods are via Federal Express, UPS or DHL courier services, or by airmail parcel post; shipments made by any other method will be refused. Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), and your telephone number. If the product is out of warranty, a payment in advance is required. Acceptable means of payment include credit card, wire transfer or a check in U.S. dollars drawn on a U.S. Bank. Repaired units shall be shipped freight collect, unless other arrangements are made in advance.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department nearest you or email support@multitech.com. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A., or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Distributors

International distributors should contact their MTS International sales representative for information about the repair of Multi-Tech product(s).

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our International Technical Support department at +(763)717-5863. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A. or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

April 2007

Replacement Parts

SupplyNet, Inc. can supply you with replacement power supplies, cables, and connectors for selected Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax, or the Internet at the following addresses:

Mail:	SupplyNet, Inc.
	614 Corporate Way
	Valley Cottage, NY 10989
Phone:	800 826-0279
Fax:	914 267-2420
Email:	*info@thesupplynet.com*
Internet:	http://www.thesupplynet.com

Appendix E – Waste Electrical and Electronic Equipment

July, 2005

Waste Electrical and Electronic Equipment (WEEE)

The WEEE directive places an obligation on EU-based manufacturers, distributors, retailers and importers to take-back electronics products at the end of their useful life. A sister Directive, ROHS (Restriction of Hazardous Substances) complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all Multi-Tech products imported into the EU as of August 13, 2005. EU-based manufacturers, distributors, retailers and importers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging, which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of their waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or where you purchased the product.

Index