

---

# MultiModem® rCell

## Intelligent Wireless Router

### User Guide



### MultiModem® rCell User Guide

Intelligent Wireless Router  
MTCBA-Xx-EN2 , MTCBA-Xx-EN2-GP  
S000485D, Revision D

### Copyright

This publication may not be reproduced, in whole or in part, without prior expressed written permission from Multi-Tech Systems, Inc. All rights reserved.

Copyright © 2011 by Multi-Tech Systems, Inc.

Multi-Tech Systems, Inc. makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc., to notify any person or organization of such revisions or changes. Check Multi-Tech's Website for current versions of our product documentation.

### Revisions

Revision	Date	Description
A	08/31/10	Initial release of MultiModem rCell with GPS and without GPS for C1,E1,G2,H4, and EV2 models.
B	10/25/10	Added Sprint and Verizon Activation into a new Carrier Activation chapter (Chapter 3) and restructured installation.
C	12/27/10	Changed Carrier Activation chapter to incorporate new website activation.
D	10/19/11	Applied template. Removed references to product CD and to printed quick start guide.

### 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.

### Contacting Multi-Tech Support

**Online Support Portal:** <https://support.multitech.com>

To better serve our customers, manage support requests and shorten resolution times, we have created the online web portal allowing you to submit questions regarding Multi-Tech products directly to our technical support team. Get answers to your most complex questions, ranging from implementation, troubleshooting, product configuration, firmware upgrades and much more.

To create an account and submit a Support Case on the Portal, visit <https://support.multitech.com>.

**Knowledge Base and Support Services:** [www.multitech.com/support.go](http://www.multitech.com/support.go)

The Knowledge Base provides immediate answers to your questions and gives you access to support resolutions for all Multi-Tech products. Visit our support area on the website for other support services.

### World Headquarters

Multi-Tech Systems, Inc.  
2205 Woodale Drive, Mounds View, Minnesota 55112 U.S.A.  
Phone: 763-785-3500 or 800-328-9717 Fax: 763-785-9874  
Internet Address: [www.multitech.com](http://www.multitech.com)

### Technical Support

Business Hours: M-F, 9am to 5pm CST

#### Country

Europe, Middle East, Africa:  
U.S., Canada, all others:

#### By Email

support@multitech.co.uk  
support@multitech.com

#### By Phone

(44) 118 959 7774  
(800) 972-2439 or (763) 717-5863

### Warranty

Warranty information can be found at: <http://www.multitech.com/warranty.go>

---

# Contents

<b>Chapter 1 – Product Overview .....</b>	<b>7</b>
<b>Related Documentation .....</b>	<b>8</b>
<b>Safety Warnings .....</b>	<b>9</b>
Ethernet Ports Caution .....	9
Handling Precautions .....	9
RF Interference Issues .....	9
Vehicle Safety .....	9
Internal Lithium Battery .....	10
<b>Front Panel.....</b>	<b>10</b>
<b>Package Contents .....</b>	<b>12</b>
Unbundled Package with No Accessories .....	12
Bundled Package with Accessories .....	12
<b>Specifications .....</b>	<b>13</b>
RF Specifications .....	15
<b>Cellular Information .....</b>	<b>16</b>
Antenna System for Cellular Devices .....	16
PTCRB Requirements for the Antenna.....	16
FCC Requirements for the Antenna .....	16
Antenna Specifications .....	16
<b>Global Positioning System (GPS) .....</b>	<b>17</b>
Technical Specifications .....	17
Global Positioning System (GPS) – Underwriters Laboratories, Inc. Statement .....	18
<b>RS232 9-Pin Functions of the Female End Connector .....</b>	<b>18</b>
<b>Chapter 2 – Installing the Router .....</b>	<b>19</b>
<b>Inserting the SIM Card into Holder, for GSM Network Access .....</b>	<b>19</b>
<b>Making the Connection .....</b>	<b>19</b>
Using Optional Direct DC Power .....	20
Powering Down and Resetting Hardware for MTCBA-C1 Router .....	20
<b>Optional – Attaching the Router to a Flat Surface .....</b>	<b>21</b>
<b>Setting TCP/IP Address .....</b>	<b>21</b>
Setting a Static IP Address .....	22
<b>Configuring Ethernet Interface.....</b>	<b>23</b>
Quickly Configuring the Router by Using Wizard Setup.....	23
<b>Verifying Signal Strength .....</b>	<b>25</b>
Before You Begin.....	25
<b>Verifying Provider Fees.....</b>	<b>25</b>
<b>Activating an Account for Wireless Devices.....</b>	<b>25</b>
Setting Up the Account to Enable Remote Configuration .....	25
<b>Chapter 3 - Using the WEB Management Software .....</b>	<b>26</b>
<b>Software Interface Overview .....</b>	<b>26</b>
Menu Bar Overview .....	26
<b>Submitting, Saving and Restarting Overview .....</b>	<b>26</b>
<b>Overview of the Web Management Software’s Interface .....</b>	<b>27</b>
Navigation bar.....	27

---

Submenus .....	28
<b>IP Setup, General Configuration Parameters .....</b>	<b>29</b>
General Configuration Group .....	30
IP Configuration Group .....	30
Auto Dial out Configuration Group .....	30
Syslog Configuration Group .....	30
Auto Discovery Group .....	30
Auto Reboot Timer Configuration Group .....	31
Telnet Configuration Group .....	31
Submitting and Saving Your Changes .....	31
<b>IP Setup, HTTP Configuration Parameters .....</b>	<b>32</b>
HTTP Configuration Group .....	32
Authentication Group .....	32
Submitting and Saving Your Changes .....	32
<b>IP Setup, DDNS Configuration Parameters .....</b>	<b>33</b>
General Group .....	33
Authentication Group .....	34
Submitting and Saving Your Changes .....	34
<b>IP Setup, SNTP Configuration Parameters .....</b>	<b>35</b>
General Configuration Group .....	35
Time Zone Configuration Group .....	35
Daylight Configuration Group .....	36
Daylight Saving Start Time Group .....	36
Daylight Saving End Time Group .....	36
Submitting and Saving Your Changes .....	36
<b>IP Setup, Static Routes Parameters .....</b>	<b>36</b>
Add Static Routes Group .....	37
<b>IP Setup, Remote Configuration Parameters .....</b>	<b>37</b>
Remote Configuration Group .....	37
<b>IP Setup, GPS Configuration Parameters .....</b>	<b>38</b>
Local Configuration Group .....	38
Remote Configuration Group .....	39
NMEA Configuration Group .....	39
Communication Examples .....	39
<b>PPP, PPP Configuration Parameters .....</b>	<b>41</b>
NAT Configuration Group .....	41
PPP General Group .....	42
Authentication Group .....	42
ICMP Keep Alive Check .....	42
Modem Configuration Group .....	42
Submitting and Saving Your Changes .....	43
<b>PPP, Wakeup-on-Call Parameters .....</b>	<b>44</b>
Wakeup-on-Call Configuration Group .....	44
Caller ID Configuration Group .....	46
Submitting and Saving Your Changes .....	46
Wakeup-On-Call Examples .....	46
<b>PPP, Power-On Configuration Parameters .....</b>	<b>50</b>
<b>PPP, Modem Commands Parameters .....</b>	<b>51</b>
Modem AT Commands Configuration Group .....	51
<b>Networks &amp; Services, Network Configuration Parameters .....</b>	<b>52</b>
Network Configuration Group .....	52
Configuring the Network .....	52
<b>Networks &amp; Services, Service Configuration Parameters .....</b>	<b>53</b>

Service Configuration Group.....	53
<b>Packet Filters, Packet Filters Parameters.....</b>	<b>54</b>
Packet Filter Group .....	54
<b>Packet Filters, DNAT Configuration Parameters .....</b>	<b>56</b>
DNAT Configuration Group .....	56
Example: Setting Up DNAT and Port Forwarding to an Internal Device .....	56
<b>Packet Filters, Advanced Parameters .....</b>	<b>58</b>
Connection Tracking Group .....	58
ICMP Configuration Group.....	58
Submitting and Saving Your Changes.....	58
<b>GRE Tunnels .....</b>	<b>58</b>
GRE Tunnels > GRE Tunnels .....	59
GRE Tunnel Configuration Group.....	59
GRE Tunnels > GRE Routes Configuration.....	60
<b>DHCP Server, Subnet Settings .....</b>	<b>61</b>
General Configuration.....	61
DHCP Server > Fixed Addresses .....	62
<b>IPSec .....</b>	<b>63</b>
Authentication and Encryption Overview.....	63
IPSec > IPSec .....	63
Add an IKE Connection.....	65
Add Manual Connection .....	67
<b>Serial-Port, Serial Port Settings Parameters .....</b>	<b>69</b>
Serial-Port Configuration Group .....	69
<b>Serial Port, Client Settings Parameters.....</b>	<b>70</b>
TCP/UDP – Client Configuration Group .....	70
<b>Serial Port, Server Settings Parameters.....</b>	<b>71</b>
TCP/UDP – Server Configuration Group .....	71
<b>Tools, Tools Parameters .....</b>	<b>73</b>
DDNS Group .....	73
Modem Group .....	73
<b>Tools, Firmware Upgrade Parameters .....</b>	<b>73</b>
Firmware Upgrade Group .....	73
<b>Tools, Load Configuration Parameters .....</b>	<b>75</b>
Load Configuration Group .....	75
<b>Tools, Save Configuration .....</b>	<b>75</b>
<b>Statistics &amp; Logs .....</b>	<b>76</b>
Statistics & Logs > System Information.....	76
Statistics & Logs > Ethernet .....	77
Statistics & Logs > PPP .....	78
Statistics & Logs > PPP Trace.....	79
Statistics & Logs > DHCP Statistics .....	79
Statistics & Logs > GRE Statistics.....	79
Statistics & Logs > Modem Information.....	80
Statistics & Logs > Service Status .....	80
Statistics & Logs > TCP/UDP Client Live Log.....	80
Statistics & Logs > TCP/UDP Server Live Log.....	80
Statistics & Logs > IPSec Live Log .....	81
Statistics & Logs > IPSec Log Traces .....	81
<b>Appendix A – Commonly Supported Subnets.....</b>	<b>82</b>
<b>Appendix B – Regulatory Compliance .....</b>	<b>86</b>
<b>EMC, Safety, and R&amp;TTE Directive Compliance.....</b>	<b>86</b>

FCC Part 15 Class A Statement .....	86
Industry Canada .....	86
<b>Appendix C – Environmental Information .....</b>	<b>87</b>
REACH Statement .....	87
Restriction of the Use of Hazardous Substances (RoHS) .....	88
China ROHS .....	89

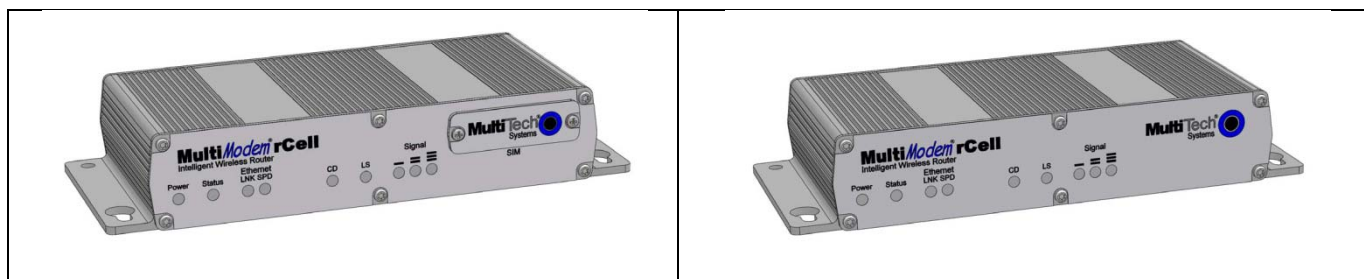
# Chapter 1 – Product Overview

This User Guide describes the MultiModem® rCell intelligent wireless routers with an Ethernet II interface. You can configure the MultiModem rCell Router for one of three connectivity modes: always-on, wake-up on ring, or dial-on demand.

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 due to poor reception or a complete loss of service, this feature automatically re-establishes the data link.

The wake-up on ring configuration allows the router to “wake up” and initiate a connection when it detects an incoming ring. For security reasons, you can setup the router to wake up based on a particular caller ID number. This configuration is ideal for reducing the costs associated with the modem being online and available 24/7.

When configured for dial-on demand, the router only accesses the Internet when data is present. This configuration is ideal for sharing Internet access among networked computers.



Model	Description
MTCBA-E1-EN2	Quad-band E-GPRS Class 12 performance without GPS option
MTCBA-E1-EN2-GP	Quad-band E-GPRS Class 12 performance with GPS option
MTCBA-G2-EN2	Quad-band GPRS Class 10 performance without GPS option
MTCBA-G2-EN2-GP	Quad-band GPRS Class 10 performance with GPS option
MTCBA-C1-EN2	Multi-band CDMA2000 1xRTT performance without GPS option
MTCBA-C1-EN2-GP	Multi-band CDMA2000 1xRTT performance with GPS option
MTCBA-H4-EN2	Tri-band UMTS/HSPA 7.2 performance without GPS option
MTCBA-H4-EN2-GP	Tri-band UMTS/HSPA 7.2 performance with GPS option
MTCBA-EV2-EN2	Dual-band 800/1900 MHz EV-DO Rev A performance without GPS option
MTCBA-EV2-EN2-GP	Dual-band 800/1900 MHz EV-DO Rev A performance with GPS option

## Related Documentation

The following table describes additional documentation for each model.

Model	Additional Documentation
MultiModem MTCBA-E1-EN2 (EDGE)	You can configure the MultiModem MTCBA-E1-EN2 wireless router using the EDGE AT Commands. For more information refer to the Reference Guide for the MultiModem Wireless EDGE Modems, part number S000474x.
MultiModem MTCBA-G2-EN2 (GPRS)	You can configure the MultiModem MTCBA-G2-EN2 wireless modem using the GPRS AT Commands. For more information, refer to the Reference Guide for the MultiModem Wireless GPRS Modems, part number S000463x
MultiModem MTCBA-C1-EN2 (CDMA)	You can configure the MultiModem MTCBA-C1-EN2 wireless router using the CDMA-C1 AT Commands. For more information, refer to the Reference Guide for the MultiModem Wireless CDMA-C1 Modems, part number S000478x.
MultiModem MTCBA-H4-EN2 (HSPA)	You can configure the MultiModem MTCBA-H4-EN2 wireless router using the HSPA AT Commands. These commands are documented in the Reference Guide part number S000483x.
MultiModem MTCBA-EV2-EN2 (EV-DO)	You can configure the MultiModem MTCBA-EV2-EN2 wireless router using the EV-DO AT Commands. These commands are documented in the Reference Guide part number S000482x.



# Safety Warnings

## Ethernet Ports Caution

The Ethernet ports are **not** designed to be connected to a Public Telecommunication Network or used outside the building.

## 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 router is not designed for, nor intended to be, used in applications within 20 cm (8 inches) of the body of the user.

## RF Interference Issues

It is important to follow any special regulations regarding the use of radio equipment due in particular to the possibility of radio frequency, RF, interference. Please follow this safety advice:

- Switch OFF your Wireless MultiModem when in an aircraft. The use of cellular telephones in an aircraft may endanger the operation of the aircraft, disrupt the cellular network and is illegal. Failure to observe this instruction may lead to suspension or denial of cellular telephone services to the offender, or legal action or both.
- Switch OFF your Wireless MultiModem when around gasoline or diesel-fuel pumps and before filling your vehicle with fuel.
- Switch OFF your Wireless MultiModem in hospitals and any other place where medical equipment may be in use.
- Respect restrictions on the use of radio equipment in fuel depots, chemical plants or where blasting operations are in progress.
- There may be a hazard associated with the operation of your Wireless MultiModem close to inadequately protected personal medical devices such as hearing aids and pacemakers. Consult the manufacturers of the medical device to determine if it is adequately protected.
- Operation of your Wireless MultiModem close to other electronic equipment may also cause interference if the equipment is inadequately protected. Observe any warning signs and manufacturers' recommendations.

## Vehicle Safety

- Do not use your Router 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 router 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.

## Internal Lithium Battery

- A lithium battery located within product provides backup power for the timekeeping capability. The battery has an estimated life expectancy of ten years.
- When the battery starts to weaken, the date and time may be incorrect. If the battery fails, the board must be sent back to Multi-Tech Systems for battery replacement.
- Lithium cells and batteries are subject to the Provisions for International Transportation. Multi-Tech Systems Inc. confirms that the Lithium batteries used in the Multi-Tech product(s) referenced in this manual comply with **Special Provision 188 of the UN Model Regulations, Special Provision A45 of the ICAO-TI/IATA-DGR (Air), Special Provision 310 of the IMDG Code, and Special Provision 188 of the ADR and RID (Road and Rail Europe).**

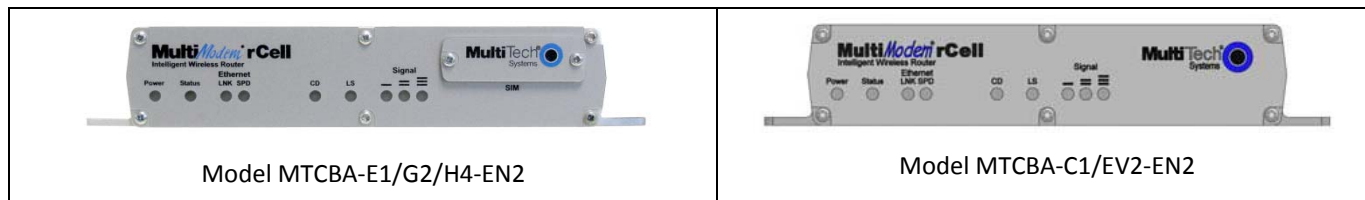
**Warning!** There is danger of explosion if the battery is incorrectly replaced!

## Front Panel

The front panel contains the following LEDs:

- Power and Status LEDs—The Power LED indicates that DC power is present. The Status LED blinks when the unit is functioning normally
- Two Ethernet LEDs—The two Ethernet LEDs indicate transmit and receive activity and connection speed of 10 or 100Mbps on the Ethernet link.
- Two modem LEDs—The two modem LEDs indicate carrier detection and link status.
- Three signal LEDs—The three signal LEDs display the signal strength level of the wireless connection.

The SIM door on the right side of the router provides access to the SIM card holder on the E1, G2, and H4 versions.



LED Indicators				
<b>Power</b>	Indicates presence of DC power when lit.			
<b>Status</b>	The LED is a solid light when the rCell is booting up, saving the configuration, restarting, or updating the firmware. When the Status LED begins to blink, the router is ready.			
<b>LNK</b>	<b>Link.</b> Blinks when there is transmit and receive activity on the Ethernet link. It shows a steady light when there is a valid Ethernet connection.			
<b>SPD</b>	<b>Speed.</b> Lit when the Ethernet is linked at 100 Mbps. If it is not lit, the Ethernet is linked at 10 Mbps.			
<b>CD</b>	<b>Carrier Detect.</b> Lit when data connection has been established.			
<b>LS</b>	Link Status Dependent on Model			
	-E1 version* (AT^SSYNC=1)	G2 version	C1version	-H4 and EV2 versions
	<p><b>Permanently off.</b> ME is in one of the following modes: Power Down mode, Airplane mode Non-Cyclic Sleep mode with no temporary wake-up event in progress.</p> <p><b>600 ms on/600 ms off</b></p> <p>Limited Network Service: No SIM card inserted or no PIN entered, or network search in progress or ongoing user authentication, or network login in progress.</p> <p><b>75 ms on/3 sec off</b></p> <p>Idle mode: The mobile is registered to the GSM network (monitoring control channels and user interactions). No call is in progress.</p> <p><b>75 ms on/ 75 ms off/75 ms on/3 sec off</b></p> <p>One or more GPRS contexts activated.</p> <p><b>500 ms on/ 25 ms off</b></p> <p>Packet switched data transfer in progress.</p> <p><b>Permanently on</b></p> <p><u>CSD call</u> – Connected to remote party.</p>	<p><b>Permanently On:</b> Not registered on network.</p> <p><b>Flashing states:</b></p> <p><b>200 ms on/2 sec off</b></p> <p>Registered on network.</p> <p><b>200 ms on/600 ms off</b></p> <p>Registered on the network and communications in progress</p> <p><b>100 ms on/200 ms off</b></p> <p>Software downloaded is either corrupted or non-compatible (“bad software”)</p>	<p><b>Permanently On:</b> Not registered on network.</p> <p><b>Flashing states:</b></p> <p><b>200 ms on/2 sec off</b></p> <p>Registered on network.</p> <p><b>200 ms on/600 ms off</b></p> <p>Registered on the network and communications in progress</p> <p><b>100 ms on/200 ms off</b></p> <p>Software downloaded is either corrupted or non-compatible (“bad software”)</p>	<p><b>Permanently On:</b> Powered on and connected, but not transmitting or receiving.</p> <p><b>Slow flashing state (5 Seconds)</b></p> <p>Powered on searching for a connection.</p> <p><b>Fast flashing state (0.3 seconds)</b> Transmitting and receiving.</p>
<b>Signal</b>	<p><b>ALL OFF</b> - Unit is off, not registered on network, or extremely weak signal (<math>0 \leq \text{RSSI} &lt; 6</math>).</p> <p><b>1 Bar “ON”</b> – Very weak signal (<math>7 \leq \text{RSSI} &lt; 14</math>)</p> <p><b>1 Bar and 2 Bar “ON”</b> – Weak signal (<math>15 \leq \text{RSSI} &lt; 23</math>)</p> <p><b>1 Bar, 2 Bar, and 3 Bar “ON”</b> – Good signal (<math>24 \leq \text{RSSI} \leq 31</math>)</p>			

\* To be accurate, the AT^SSYNC command must be set to 1 so that the factory default LED timings are used.

## Package Contents

This section describes items in the MultiModem rCell package.

Your wireless provider supplies the SIM card.

### Unbundled Package with No Accessories

1 router

**Note:** You supply mounting screws, AC or DC power supply, and an antenna.

### Bundled Package with Accessories

1 router

1 antenna

1 Ethernet cable

1 RS-232 cable

1 power supply

**Note:** You supply mounting screws.

# Specifications

Features	MTCBA-E1-EN2	MTCBA-C1-EN2	MTCBA-G2-EN2	MTCBA-H4-EN2	MTCBA-EV2-EN2
<b>Performance</b>	<b>EDGE:</b> E-GPRS Class 12, <b>GPRS:</b> Class 10	CDMA2000 1xRTT	GPRS Class 10	HSPA	CDMA2000 1xRTT EV-DO Rev. A
<b>Band, Frequency</b>	Quad-band GSM/GPRS/EDGE 850/900/1800/1900 MHz	Dual-band 800/1900 MHz CDMA; 800 MHz and 800/1900 MHz with R-UIM support	Quad-band GSM 850/900/1800/1900 MHz	HSUPA / HSDPA / UMTS Triple-band: 2100/1900/850 MHz with Rx diversity	Dual-band 800/1900 MHz CDMA; 800 MHz and 800/1900 MHz with R-UIM support
<b>Packet Data</b>	<b>EDGE:</b> E-GPRS Up to 240K bps, coding scheme MCS1-9, mobile station Class B, LLC layer, 4 time slots <b>GPRS:</b> Full PBCCH support, coding scheme 1-4, mobile station Class B	Up to 153.6K bps forward and reverse	Up to 85.6K bps, coding schemes CS1 to CS4	HSDPA data service of up to 7.2 Mbps HSUPA data service of up to 5.76 Mbps	Peak download 3.1 Mbps, peak upload 1.8 Mbps
<b>Circuit-Switched Data</b>	Up to 14.4K bps, non-transparent	IS-95A, IS-95B up to 14.4K bps forward and reverse	Up to 14.4K bps transparent and non-transparent	Up to 14.4K bps transparent and non- transparent	IS-95A, IS-95B up to 14.4K bps forward and reverse
<b>Short Message Services-SMS</b>	Text & PDU, Point-to-Point (MO/MT), cell broadcast	Text & PDU, Point-to-Point (MO/MT), cell broadcast	Text & PDU, Point-to-Point, cell broadcast	Text & PDU, Point-to-Point (MO/MT), cell broadcast	Text & PDU, Point-to-Point (MO/MT), cell broadcast
<b>Antenna Connector</b>	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)	RF Antenna: 50 ohm SMA (female connector)
<b>SIM Connector</b>	Standard 1.8 and 3V SIM receptacle	-	Standard 1.8 and 3V SIM receptacle	Standard 1.8 and 3V SIM receptacle	-
<b>RS232 Connector</b>	DE9				
<b>Power Connector</b>	2.5mm miniature (screw-on)				
<b>Voltage</b>	9V to 32 VDC				
<b>Physical Description</b>	7"W x 1.24"H x 2.93"D 0.75lbs 17.78cmW x3.15cmH x7.44cmD 0.340Kg				
<b>Operating Temperature *</b>	-35° to +75° C*	-40° to +85° C*	-40° to +85° C*	-30° to +60° C*	-40° to +75° C*
<b>Storage Temp</b>	-40° to +85° C				
<b>Humidity</b>	Relative humidity 20% to 90% noncondensing				
<b>Certifications</b>	<b>EMC Compliance</b>  FCC Part 15  EN55022  EN55024  <b>Radio Compliance</b>	<b>EMC Compliance</b>  FCC Part 15  <b>Radio Compliance</b>  FCC Part 22, 24  RSS132,133	<b>EMC Compliance</b>  FCC Part 15  EN55022  EN55024  <b>Radio Compliance</b>	<b>EMC Compliance</b>  FCC Part 15  EN55022  EN55024  <b>Radio Compliance</b>	<b>EMC Compliance</b>  FCC Part 15  <b>Radio Compliance</b>  FCC Part 22, 24  RSS132,133

Features	MTCBA-E1-EN2	MTCBA-C1-EN2	MTCBA-G2-EN2	MTCBA-H4-EN2	MTCBA-EV2-EN2
	FCC Part 22, 24 RSS132,133 EN301 489-1 EN489-3 (-GP only) EN301 489-7 EN301 511 AS/ACIF S042.1, S042.3 <b>Safety:</b> UL60950-1 cUL60950-1 IEC60950-1 <b>Network:</b> PTCRB	<b>Safety:</b> UL60950-1 cUL60950-1 IEC60950-1 <b>Network:</b> CDG 1&2	FCC Part 22, 24 RSS132,133 EN301 489-1 EN489-3 (-GP only) EN301 489-7 EN301 511 AS/ACIF S042.1, S042.3 <b>Safety:</b> UL60950-1 cUL60950-1 IEC60950-1 AS/NZS60950-1 <b>Network:</b> PTCRB	FCC Part 22, 24 RSS132,133 EN301 489-1 EN489-3 (-GP only) EN301 489-7 EN301 511 AS/ACIF S042.1, S042.3 <b>Safety:</b> UL60950-1 cUL60950-1 IEC60950-1 <b>Network:</b> PTCRB	<b>Safety:</b> UL60950-1 cUL60950-1 IEC60950-1 <b>Network:</b> CDG 1&2

\* UL Listed @ 40° C, limited by power supply. UL Certification does not apply or extend to an ambient above 40° C and has not been evaluated by UL for ambient greater than 40° C.

“ UL has evaluated this device for use in ordinary locations only. Installation in a vehicle or other outdoor locations has not been evaluated by UL. UL Certification does not apply or extend to use in vehicles or outdoor applications or in ambient above 40° C.”

## Power Specifications

MTCBA-E1-EN2	MTCBA-C1-EN2	MTCBA-G2-EN2	MTCBA-H4-EN2	MTCBA-EV2-EN2
<b>Sleep:</b> 0.175A, 1.6W @ 9V, 0.090A, 1.8W @ 20V, 0.060A, 1.9W @ 32V <b>Typical:</b> 0.277A, 2.5W @ 9V, 0.133A, 2.7W @ 20V, 0.089A, 2.8W @ 32V <b>Max:</b> 0.506A, 4.5W @ 9V, 0.240A, 4.8W @ 20V, 0.150A, 4.8W @ 32V <b>Peak:</b> 2.50A @ 9V, 1.00A @ 20V, 0.60A @ 32V	<b>Sleep:</b> 0.186A, 1.7W @ 9V, 0.091A, 1.8W @ 20V, 0.061A, 2.0W @ 32V <b>Typical:</b> 0.283A, 2.6W @ 9V, 0.137A, 2.7W @ 20V, 0.088A, 2.8W @ 32V <b>Max:</b> 0.457A, 4.1W @ 9V, 0.214A, 4.3W @ 20V, 0.138A, 4.4W @ 32V	<b>Sleep:</b> 0.163A, 1.5W @ 9V, 0.082A, 1.6W @ 20V, 0.055A, 1.8W @ 32V <b>Typical:</b> 0.240A, 2.2W @ 9V, 0.114A, 2.3W @ 20V, 0.077A, 2.5W @ 32V <b>Max:</b> 0.340A, 3.0W @ 9V, 0.153A, 3.1W @ 20V, 0.100A, 3.2W @ 32V <b>Peak:</b> 1.300A @ 9V, 0.518A @ 20V, 0.343A @ 32V	<b>GSM 850</b> <b>Sleep</b> 0.205A, 1.89W @ 9v, 0.110A, 2.20W @ 20v, 0.068A, 2.18W @ 32v <b>Typical</b> 0.240A, 2.21W @ 9v, 0.114A, 2.28W @ 20v, 0.077A, 2.46W @ 32v <b>Max</b> 0.429A, 3.91W @ 9v, 0.153A, 3.06W @ 20v, 0.100A, 3.20W @ 32v <b>Peak</b> 2.50A @ 9v, 0.812A @ 20v, 0.500A @ 32v <b>HSPA</b> <b>Sleep</b> 0.205A, 1.89W @ 9v, 0.110A, 2.20W @ 20v, 0.068A, 2.18W @ 32v <b>Typical</b> 0.480A, 4.38W @ 9v, 0.230A, 4.60W @ 20v, 0.148A, 4.74W @ 32v <b>Max</b> 0.640A, 5.79W @ 9v, 0.290A,	<b>CDMA2000</b> <b>Sleep</b> 0.125A, 1.15W @ 9v, 0.060A, 1.20W @ 20v, 0.044A, 1.41W @ 32v <b>Typical</b> 0.215A, 1.98W @ 9v, 0.130A, 2.60W @ 20v, 0.085A, 2.72W @ 32v <b>Max</b> 0.600A, 5.45W @ 9v, 0.297A, 5.94W @ 20v, 0.195A, 6.05W @ 32v <b>EV-DO</b> <b>Sleep</b> 0.125A, 1.15W @ 9v, 0.060A, 1.20W @ 20v, 0.044A, 1.41W @ 32v <b>Typical</b> 0.335A, 3.08W @ 9v, 0.190A, 3.30W @ 20v, 0.125A, 4.00W @ 32v <b>Max</b> 0.672A, 6.10W @ 9v, 0.320A, 6.40W @ 20v, 0.204A, 6.53W @ 32v

			5.80W @20v, 0.190A, 6.08W @32v	
<a href="#"><u>MTCBA-E1-EN2-GP</u></a>	<a href="#"><u>MTCBA-C1-EN2-GP</u></a>	<a href="#"><u>MTCBA-G2-EN2-GP</u></a>	<b>1. <a href="#"><u>MTCBA-H4-EN2-GP</u></a></b>	<b>2. <a href="#"><u>MTCBA-EV2-EN2-GP</u></a></b>
<b>Sleep:</b> 0.188A, 1.7W @ 9V, 0.095A, 1.9W @ 20V, 0.061A, 1.9W @ 32V <b>Typical:</b> 0.297A, 2.7W @ 9V, 0.138A, 2.8W @ 20V, 0.092A, 2.9W @ 32V <b>Max:</b> 0.513A, 4.5W @ 9V, 0.240A, 4.8W @ 20V, 0.152A, 4.8W @ 32V <b>Peak:</b> 2.50A @ 9V, 1.000A @ 20V, 0.625A @ 32V	<b>Sleep:</b> 0.186A, 1.7W @ 9V, 0.091A, 1.8W @ 20V, 0.061A, 2.0W @ 32V <b>Typical:</b> 0.384A, 3.5W @ 9V, 0.193A, 3.9W @ 20V, 0.122A, 3.9W @ 32V <b>Max:</b> 0.541A, 4.8W @ 9V, 0.256A, 5.1W @ 20V, 0.162A, 5.2W @ 32V	<b>Sleep:</b> 0.195A, 1.8W @ 9V, 0.099A, 2.0W @ 20V, 0.066A, 2.1W @ 32V <b>Typical:</b> 0.285A, 2.6W @ 9V, 0.136A, 2.7W @ 20V, 0.093A, 3.0W @ 32V <b>Max:</b> 0.408A, 3.7W @ 9V, 0.183A, 3.7W @ 20V, 0.120A, 3.8W @ 32V <b>Peak:</b> 2.25A @ 9V, 0.960A @ 20V, 0.650A @ 32V	<b>GSM 850</b> <b>Sleep</b> 0.270A, 2.48W @9v, 0.130A, 2.60W @20v, 0.087A, 2.78W @32v <b>Typical</b> 0.320A, 2.94W @9v, 0.160A, 3.20W @20v, 0.104A, 3.33W @32v <b>Max</b> 0.590A, 5.37W @9v, 0.280A, 5.60W @20v, 0.180A, 5.76W @32v <b>Peak</b> 2.50A @9v, 0.812A @20v, 0.500A @32v <b>HSPA</b> <b>Sleep</b> 0.270A, 2.48W @9v, 0.130A, 2.60W @20v, 0.087A, 2.78W @32v <b>Typical</b> 0.540A, 4.93W @9v, 0.265A, 5.30W @20v, 0.172A, 5.50W @32v <b>Max</b> 0.780A, 7.06W @9v, 0.370A, 7.40W @20v, 0.240A, 7.68W @32v	<b>CDMA2000</b> <b>Sleep</b> 0.245A, 2.26W @9v, 0.125A, 2.50W @20v, 0.083A, 2.66W @32v <b>Typical</b> 0.340A, 3.12W @9v, 0.166A, 3.32W @20v, 0.110A, 3.52W @32v <b>Max</b> 0.690A, 6.27W @9v, 0.330A, 6.60W @20v, 0.210A, 6.72W @32v <b>EV-DO</b> <b>Sleep</b> 0.0465A, 2.27W @9v, 0.125A, 2.50W @20v, 0.238A, 7.62W @32v <b>Typical</b> 0.370A, 3.40W @9v, 0.220A, 4.40W @20v, 0.145A, 4.64W @32v <b>Max</b> 0.780A, 7.13W @9v, 0.374A, 7.48W @20v, 0.385A, 7.62W @32v

**Note:** Multi-Tech Systems, Inc. recommends that the customer incorporate a 10% buffer into their power source when determining product load.

## RF Specifications

	GSM 850	EGSM 900	GSM 1800	GSM 1900	CDMA 800	CDMA 1900
<b>Frequency RX</b>	869 to 894 MHz	925 to 960 MHz	1805 to 1800 MHz	1930 to 1990 MHz	869 to 894 MHz	1930 to 1990 MHz
<b>Frequency TX</b>	824 to 849 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz	824 to 849 MHz	1850 to 1910 MHz
<b>RF Power Stand</b>	2W at 12.5% duty cycle	2W at 12.5% duty cycle	1W at 12.5% duty cycle	1W at 12.5% duty cycle	-	-

## Cellular Information

### Antenna System for Cellular Devices

The cellular/wireless performance depends on the implementation and antenna design. The integration of the antenna system into the product is a critical part of the design process; therefore, it is essential to consider it early so the performance is not compromised. If changes are made to the certified antenna system of the MultiModem, then recertification is required by specific network carriers such as Sprint. The Antenna System is defined as the UFL connection point from the MultiModem to the specified cable specifications and specified antenna specifications.

### PTCRB Requirements for the Antenna

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

### FCC Requirements for the Antenna

The antenna gain, including cable loss, for the radio you are incorporating into your product design must not exceed the requirements at 850 MHz and 1900 MHz as specified by the FCC grant for mobile operations and fixed mounted operations as defined in 2.1091 and 1.1307 of the FCC rules for satisfying RF exposure compliance. The antenna used for transmitting must be installed to provide a separation distance of at least 20cm from all persons and must not transmit simultaneously with any other antenna transmitters. User and installers must be provided with antenna installation instructions and transmitter operating conditions to satisfying RF exposure compliance.

## Antenna Specifications

### CDMA RF Specifications

	CDMA 800	CDMA 1900
Frequency RX	869 to 894 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	1850 to 1910 MHz

### CDMA Antenna Requirements/Specifications

Frequency Range	824 – 894 MHz / 1850 – 1990 MHz
Impedance	50 Ohms
VSWR	VSWR shall not exceed 2.0:1 at any point across the bands of operation
Typical Radiated Gain	3 dBi on azimuth plane
Radiation	Omni-directional
Polarization	Vertical
Antenna Loss	Free space not to exceed -3dB
TRP/TIS	The total radiated power (TRP) at the antenna shall be no less than +21/20 dBm for PCS/CELL channels respectively, and the total isotropic sensitivity (TIS) at the antenna shall be no less than -104/104 dBm for PCS/CELL channels respectively.

### GSM/EGSM RF Specifications

	GSM 850	EGSM 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



## GSM Antenna Requirements/Specifications

<b>Frequency Range</b>	824 – 960 MHz / 1710 – 1990 MHz
<b>Impedance</b>	50 Ohms
<b>VSWR</b>	VSWR shall not exceed 2.0:1 at any point across the bands of operation
<b>Typical Radiated Gain</b>	3 dBi on azimuth plane
<b>Radiation</b>	Omni-directional
<b>Polarization</b>	Vertical
<b>Antenna Loss</b>	Free space not to exceed -3db
<b>TRP/TIS</b>	Including cable loss the total radiated power (TRP) at the antenna shall be no less than +22/24.5 dBm for 850/1900 MHz respectively, and the total isotropic sensitivity (TIS) at the antenna shall be no less than -99/101.5 dBm for 850/1900 MHz respectively.

## GPS (Global Positioning) RF Specifications

	<b>GPS L1</b>
<b>Frequency RX</b>	1575.42
<b>LNA Bias Voltage</b>	5V
<b>LNA Current Consumption</b>	40mA Max

## GPS Antenna Requirements/Specifications

<b>Frequency</b>	1575MHz
<b>Impedance</b>	50 Ohms
<b>VSWR</b>	1.5db
<b>Input voltage</b>	3.0V +/- 0.3V
<b>GPS TIS</b>	The total isotropic sensitivity (TIS) at the antenna shall be no less than 47 dBm

# Global Positioning System (GPS)

Point the GPS toward the sky, as the GPS antenna needs to find the satellites that provide location information.

## Technical Specifications

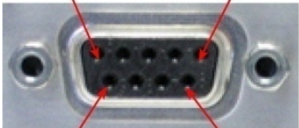
<b>Receiver Type</b>	L1 Frequency, GPS C/A code, SBAS Capable, 51 Channel Acquisitions, 14 Channel Tracking
<b>Accuracy</b>	Position 2.5m CEP, Velocity 0.1m/sec
<b>Open Sky TTFF</b>	Hot start 1 second, Cold start 29 seconds average, Reacquisition <1s
<b>Sensitivity Tracking</b>	-161dBm
<b>Update Rate</b>	1 Hz standard
<b>Dynamics</b>	4G
<b>Operational Limits</b>	Altitude <18,000m or Velocity < 515m/s
<b>Datum</b>	Default WGS-84
<b>Interface</b>	UART
<b>Protocol</b>	NMEA-0183, V3.01, GGA, GLL, GSA, GSV, RMC, VTG

## Global Positioning System (GPS) – Underwriters Laboratories, Inc. Statement

Underwriters Laboratories Inc. (“UL”) has not tested the performance or reliability of the Global Positioning System (“GPS”) hardware, operating software or other aspects of this product. UL has only tested for fire, shock or casualties as outlined in UL’s Standard(s) for Safety. UL60950-1 Certification does not cover the performance or reliability of the GPS hardware and GPS operating software. UL MAKES NO REPRESENTATIONS, WARRANTIES OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY GPS RELATED FUNCTIONS OF THIS PRODUCT.

## RS232 9-Pin Functions of the Female End Connector

The following table explains the pin functions.

External Power		Serial Cable Female Connector
Signal	IN/OUT	
Pin 1 CD	O	
Pin 2 RX	O	
Pin 3 TX	I	
Pin 4 DTR	I	
Pin 5 GND	--	
Pin 6 DSR*	O	
Pin 7 RTS	I	
Pin 8 CTS	O	
Pin 9 RI	O	

**Note:** The DSR signal on pin 6 is always asserted by the router.

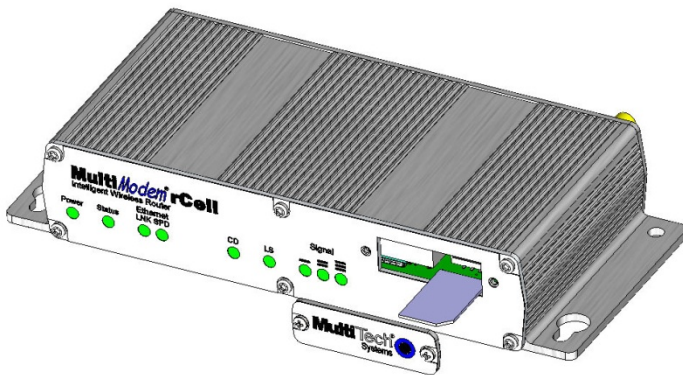
## Chapter 2 – Installing the Router

### Inserting the SIM Card into Holder, for GSM Network Access

The router requires the power supply connection to begin operation. It also requires a SIM card (Subscriber Identity Module) to operate on a GSM network. To install the SIM, do the following:

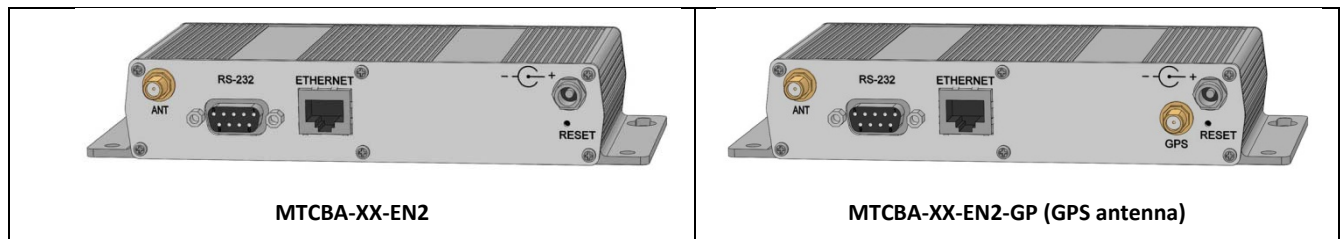
1. Using a small Phillips screwdriver, remove the two SIM door screws and remove the SIM door.

**Note:** When changing a SIM, ensure that power is removed from the unit.

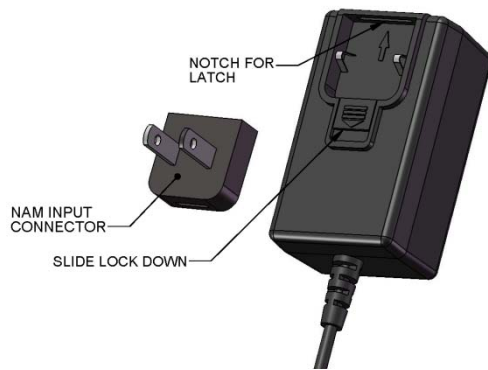


2. Insert the SIM card into the card holder. The above graphic illustrates the correct SIM card orientation.
3. Verify that the SIM card fits into the holder properly and then replace the cover.

### Making the Connection



1. Connect a suitable antenna to the SMA connector (see antenna specifications in Chapter 1)
2. Optional: If you have the GPS version, connect a suitable GPS antenna to the GPS connector. Ensure that when you position the GPS antenna, the antenna can see the sky to locate the satellites for accurate values.
3. Using an Ethernet cable, connect one end of the cable to the ETHERNET connector on the back of the router and the other end to your computer either directly or through a switch or hub.
4. If you are connecting a customer's serial legacy device to the router, connect the serial, RS-232 cable from the customer's device to the RS232 connector on the back of the router.
5. Depending on the power source, connect either the power supply module with the appropriate blade or the optional DC power cable. If you are using the power supply module, remove the protective shipping cover. Attach the appropriate interchangeable blade piece to the power supply module.



6. Screw on the power lead from the power supply module into the power connection on the router. Plug the power supply into your power source.

## Using Optional Direct DC Power

1. Screw-on the DC power cable to the power connector on the router.
2. Then attach the two wires at the other end of the DC power cable to a DC fuse/terminal block in which you are mounting the router.
3. Connect the red wire to the "+" (positive) terminal and the black wire to the "-" (negative) terminal. Be sure the GND connection is correct.

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

### Notes:

- For an application involving a battery: you can use permanent "+" or key-switched "+" source. Connect the power supply to its source (for example, in a mobile situation, to the DC fuse/terminal block).
- The **POWER** LED. The **POWER** LED lights after power-up.
- The **Status** LED is a solid ON when the router is booting up, saving a configuration, or updating firmware. When the **Status** LED begins to blink, the router is ready.

## Using the Reset Button

Press and hold in the **Reset** button until the Status Light goes out. Then release the button. This sets the username and password back to admin and admin, as well as sets the IP address to the default of 192.168.2.1.

## Powering Down and Resetting Hardware for MTCBA-C1 Router

Before you turn off power to the router, and before you reset the hardware, it is recommended you complete the following sequence.

The shutdown sequence informs the network that the mobile station is going offline, and saves critical data to the module's non-volatile memory (flash).

1. Issue the following command:  
`AT+CFUN=0` (issue this command)
2. Wait for this response from the modem  
`+WIND:10 ()`

You can now power off the router or reset it.

If you do not see the +WIND:10 response, you may need to activate the unsolicited message by using the command `AT+WUSLSK=00020000,0`

## Optional – Attaching the Router to a Flat Surface

Before you mount your router to a permanent surface, verify signal strength. For more information, refer to Verify Signal Strength in this chapter.

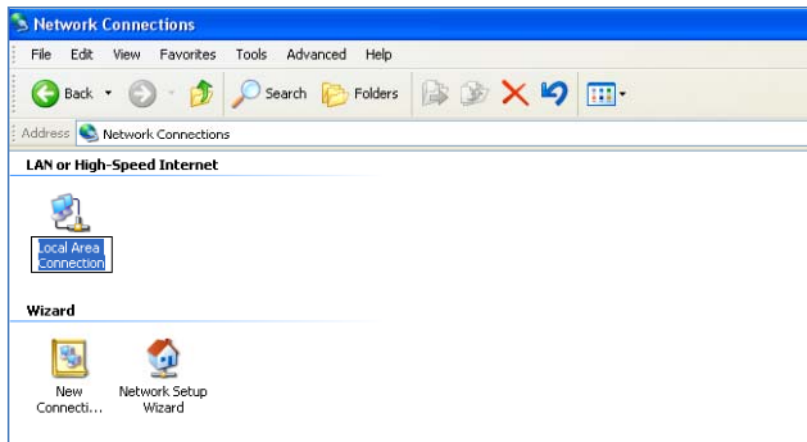
The router can be panel mounted with screws spaced according to the measurement shown.

**Note:** Use either #6 or #8 pan head screws for all four mount locations.

## Setting TCP/IP Address

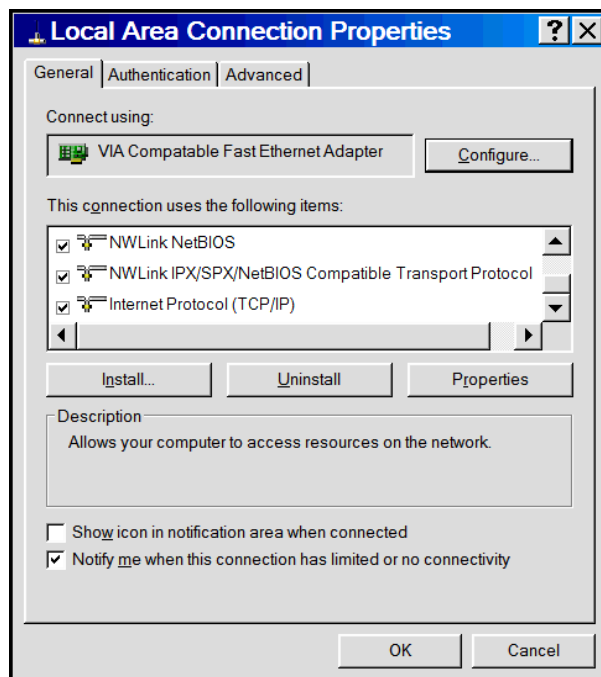
This section describes how to configure a TCP/IP address so the computer can communicate with the router.

1. From the **Start** menu, select **Control Panel**. In the window that opens, double-click **Network Connections**. The **Network Connections** window opens.

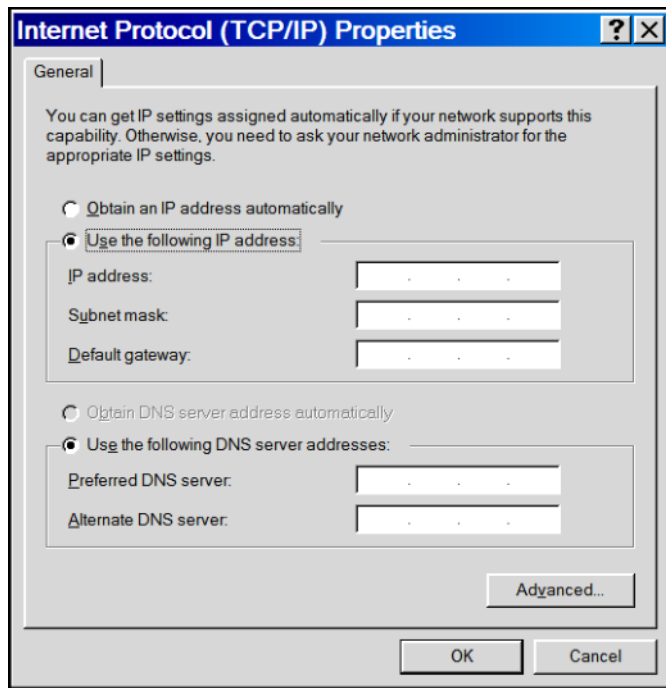


2. Right-click **Local Area Connection**. From the menu that appears, select **Properties**.

The Local Area Connection Properties window opens.



3. Select **Internet Protocol [TCP/IP]**.
4. Click **Properties**. The Internet Protocol (TCP/IP) Properties window opens.



**Note:** If this window displays your current IP configuration, it is recommended that you record this information for future reference. This information is handy, for example, if you want to return the computer to its original settings.

## Setting a Static IP Address

To set a static IP address:

1. Select **Use the following IP address**.
2. In the IP address field type the IP address of the computer, for example 192.168.2.x.
3. In the **Subnet mask** field, type the number of the subnet mask, for example: 255.255.255.0
4. In the **Default Gateway** field, type the default gateway, for example, 192.168.2.1

**Note:** The computer settings must be in the same subnet range as the router.

The factory default settings for the router are:

**IP Address:** 192.168.2.1

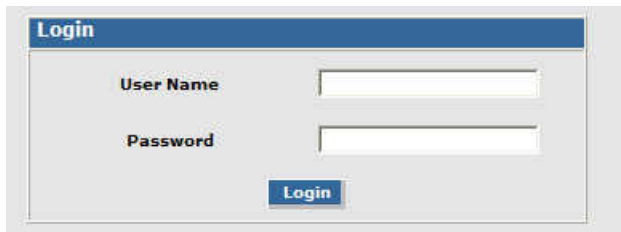
**Subnet Mask:** 255.255.255.0

5. Select **Use the following DNS server addresses**.
  - a. Enter the IP Address for the Preferred DNS Server. Example: 205.171.3.65
  - b. Click **OK**.
6. To close the Local Area Properties window, click **OK**.
7. Close the Control Panel.
8. Repeat these steps for each computer on your network.

## Configuring Ethernet Interface

You use the router's factory-installed Web Management software to configure the Ethernet interface. Access this software using a Web browser.

1. Ensure that the Status LED is blinking, indicating that the router is ready.
2. On the computer, open a Web browser
3. In the browser's address field, type the default Gateway Address: `http://192.168.2.1`
4. After entering the Address, the **Login** page opens.



- a. In the **User Name** field, type the default user name: **admin** (all lower-case).
- b. In the **Password** field, type the default password: **admin** (all lower-case).
- c. Click **Login**. The Web Management Home page opens.

The user name and password are case-sensitive. You must use lower-case for both.

A password can be up to 12 characters. If Windows displays the **AutoComplete** message, click **No** so that the operating system does not remember the password. This helps maintain computer security.

It is recommended that you change the default password to better protect the security of your router. Use a safe password.

## Quickly Configuring the Router by Using Wizard Setup

The Wizard Setup tool helps you quickly configure the router. Benefits of using this tool include:

- Saves time by allowing you to configure the basic setup in one place.
- The information entered defaults to other windows that require this information.
- Lets you enter and save information needed to create a connection to the Internet.

This section describes how to configure the basic parameters to start using your router. You can configure more than the basics by using other features of the Web Management software. For more information, see Chapter 3.

To use Wizard Setup to setup basic router features:

1. From the Web Management software's menu bar, select **Wizard Setup**.

- The Wizard Setup page opens, where a minimum router configuration is provided.

The table that follows describes the basic parameters you need to set before you can connect to the Internet.

IP Configuration	
IP Address	The default is 192.168.2.1. To change it, type a new 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 <b>disable</b> . To connect to the Internet, you need to enable PPP. Depending on the model, commands may need to be issued to the integrated cellular modem before connecting to the wireless service. To issue commands to the integrated cellular modem, PPP must be disabled and telnet port 5000 used.
Dial-on-Demand	The default is <b>disable</b> .
Idle Time Out	Sets the 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 GSM, the number is *99***1#. For CDMA, the Dial Number is #777.
APN	For GSM models, enter the APN (Access Point Name). Your wireless service provider assigns the APN. If you don't know the name, ask your provider for it. An access point is an IP network to which a MultiModem rCell Router connects. The Web Management software asks for the APN on the Wizard Setup and the PPP screen. For CDMA models, the APN does not apply.
Init String	You can set up to 4 router initialization strings.
PPP Authentication	
Authentication Type	Select the radio button of the authentication protocol used to negotiate with the remote peer: PAP, CHAP, or PAP-CHAP. The default is PAP-CHAP
Username	Enter the PPP Username. This name authenticates the remote peer.
Password	Enter the PPP Password. This password authenticates the remote peer.

- To save changes, click **Submit**.
- To cause your changes to go into effect, from the Menu bar, click **Save & Restart**. The router reboots.  
You don't need to click **Save & Restart** after every change you make. You can submit several changes on various pages, and then click **Save & Restart**.



## Verifying Signal Strength

This section describes how to verify signal strength by using telnet to communicate directly with the modem.

### Before You Begin

- Ensure that the Status LED is blinking, indicating that the router is ready.
- Ensure that PPP is disabled.

To verify signal strength:

1. Use one of the following methods to open a command prompt:
  - From the Start menu, select Run. In the Open window, enter cmd and then press ENTER.
  - From the **Start** menu, select **All Programs, Accessories, Command Prompt**
2. In the command window, type **telnet 192.168.2.1 5000**
3. At the Login prompt, type the default user name: **admin** (all lower-case). Press **ENTER**
4. At the Password prompt, type the default password: **admin** (all lower-case). Press **ENTER**
5. In the command window, type **AT+CSQ** . The router responds with the received signal strength (rssi).

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

6. To find the best location in which to run the router, check the signal from a few different locations.

## Verifying Provider Fees

Your provider charges you for data usage so be aware of your payment obligations. If you use the router for large data transfers, Multi-Tech recommends an unlimited data plan with your account. Multi-Tech is not responsible for any charges relating to your cellular bill.

## Activating an Account for Wireless Devices

See Multi-Tech’s Cellular Activation Website at <http://www.multitech.com/activation.go> for information on activating your cellular modem.

### Setting Up the Account to Enable Remote Configuration

You can remotely configure the MultiModem over the Internet if your wireless provider has provisioned some features for you.

- Make sure your wireless network provider has provisioned for mobile terminated data.
- The provider also needs to setup a fixed or dynamic public IP address to which the network can redirect any incoming connection.

# Chapter 3 - Using the WEB Management Software

This chapter describes how to configure the router by using the Web Management software.

## Software Interface Overview

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

### Menu Bar Overview



You can select the following items from the menu bar:

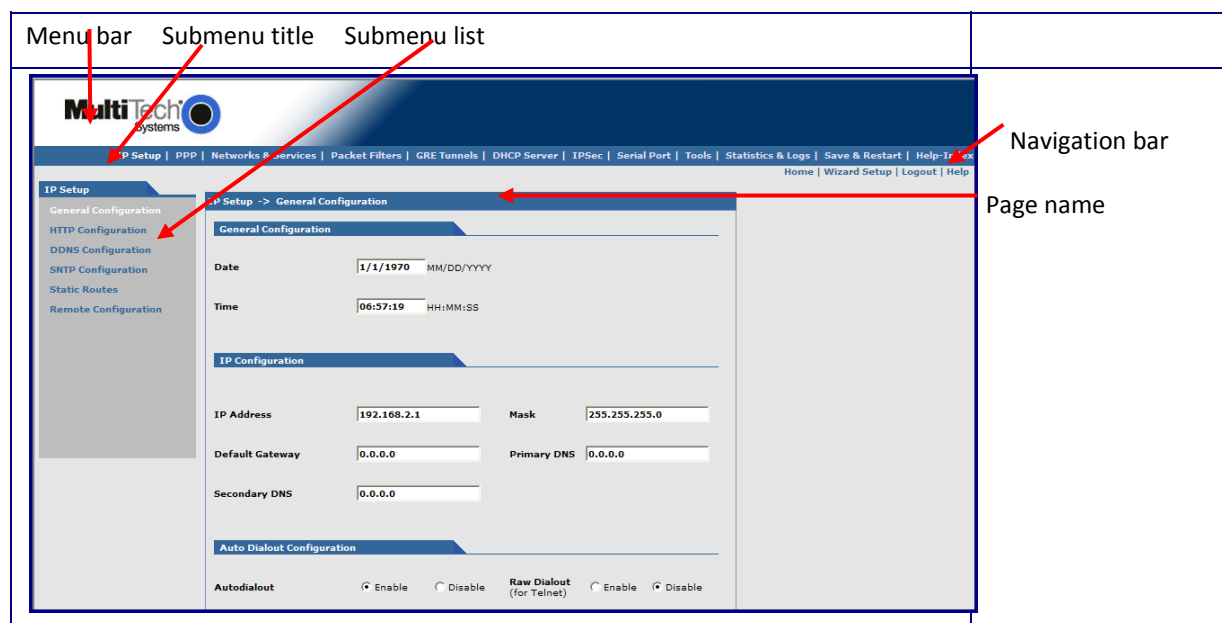
<b>IP Setup</b>	Sets up a General Configuration, HTTP, DDNS, SNTP, Static Routes, and Remote Configuration.
<b>PPP</b>	Used to configure the PPP authentication, dial-on-demand, router authentication, and Wakeup on Call.
<b>Networks &amp; Services</b>	Used to configure networks and services to make them available to other functions such as allowed packet filters, static routes, remote configuration, DNAT, and GRE tunnels and routes.
<b>Packet Filters</b>	Defines filter rules, DNAT configuration, and ICMP rules.
<b>GRE Tunnels</b>	Used to define Generic Routing Encapsulation (GRE). Defines the remote network and the tunnel through which traffic is routed.
<b>DHCP Server</b>	Used to configure the DHCP server settings.
<b>IPSec</b>	Allows the device to support LAN-to-LAN VPN tunneling with 3DES and AES 128-192-256 encryption support
<b>Serial Port</b>	Adds support for RS-232 serial port so that Ethernet and legacy serial devices can share the same cellular connection.
<b>Tools</b>	Sets DDNS Force Update, displays DDNS Status, resets the modem, and provides interfaces for Firmware Upgrade, Load Configuration, and Save Configuration.
<b>Statistics &amp; Logs</b>	Shows statistics and logs maintained by the router.
<b>Save &amp; Restart</b>	Saves your settings and reboots your router.
<b>Help Index</b>	Opens the online Help file.

## Submitting, Saving and Restarting Overview

Nearly every page of the software's interface includes a Submit button. This button allows you to save changes you make to the software pages and their parameters.

To ensure your changes go into effect, you must eventually use **Save & Restart**, located on the Menu bar. You do not need to click Save& Restart after each change you make. You can change several areas, and then click Save & Restart.

## Overview of the Web Management Software's Interface



### Navigation bar

<b>Home</b>	To return to the home page, click <b>Home</b> .
<b>Wizard Setup</b>	To use the Wizard Setup tool for quick set up of your MultiModem, click Wizard Setup. This tool helps you configure basic settings needed to run the rCell Router.
<b>Logout</b>	To log out of the software, click <b>Logout</b> . You return to the login screen.
<b>Help</b>	To open an online help file, click <b>Help</b> .

## Submenus

The submenus display on the left side of the page. The following table lists the submenu selections under each main menu category.

<b>IP Setup</b>	<b>PPP</b>	<b>Networks &amp; Services</b>	<b>Packet Filters</b>	<b>GRE Tunnels</b>
General Configuration HTTP Configuration DDNS Configuration SNTP Configuration Static Routes Remote Configuration GPS Configuration	PPP Configuration Wakeup on Call Power On Config Modem Commands	Network Configuration Service Configuration	Packet Filters DNAT Configuration Advanced	GRE Tunnels GRE Routes
<b>DHCP Server</b>	<b>IPSec</b>	<b>Serial Port</b>	<b>Tools</b>	<b>Statistics &amp; Logs</b>
Subnet Settings Fixed Addresses	IP Sec	Serial Port Settings Client Settings Server Settings	Tools Firmware Upgrade Load Configuration Save Configuration	SysInfo Ethernet PPP PPP Trace DHCP Statistics GRE Statistics Modem Info Service Status TCP/UDP Client Live Log TCP/UDP Server Live Log IPSec Live Log IPSec Log Traces

# IP Setup, General Configuration Parameters

**IP Setup**  
 General Configuration  
 HTTP Configuration  
 DDNS Configuration  
 SNTP Configuration  
 Static Routes  
 Remote Configuration  
 GPS Configuration

IP Setup -> General Configuration  
**General Configuration**  
 Date  MM/DD/YYYY  
 Time  HH:MM:SS  
**IP Configuration**  
 IP Address  Mask   
 Default Gateway  Primary DNS   
 Secondary DNS   
**Auto Dialout Configuration**  
 Autodialout ☒ Enable ☐ Disable Raw Dialout (for Telnet) ☐ Enable ☒ Disable  
 Autodialout login ☒ Enable ☐ Disable Autodialout Port   
 Handle EIA Signal ☐ Enable ☒ Disable Inactivity (Secs)   
**Syslog Configuration**  
 Syslog ☒ Enable ☐ Disable  
 Syslog Server IP Address   
**Auto Discovery**  
 Autodiscovery ☒ Enable ☐ Disable Server Port   
 Broadcast Timer  seconds  
**Auto Reboot Timer Configuration**  
 Auto Reboot Timer  ( in hrs )  
 ( 0: Deactivate )  
**Telnet Configuration**  
 Telnet ☒ Enable ☐ Disable  
 SUBMIT

## General Configuration Group

In the General Configuration group , set the general system-based parameters.

<b>Date</b>	The system date: <b>MM/DD/YYYY</b>
<b>Time</b>	<b>HH:MM:SS</b> . A real time clock is part of SNTP to display proper time.

## IP Configuration Group

Use the IP Configuration group to configure the Ethernet interface. If desired see Appendix A for a table of commonly supported subnets.

<b>IP Address</b>	(Default is 192.168.2.1),
<b>Mask</b>	(Default 255.255.255.0),
<b>Default Gateway</b>	(Default 0.0.0.0),
<b>Primary DNS</b>	(Default 0.0.0.0),
<b>Secondary DNS</b>	(Default 0.0.0.0).

## Auto Dial out Configuration Group

<b>Auto Dialout</b>	Check the box to enable or disable Auto Dialout. Default is Enable. The Auto Dialout settings allow you to use the integrated cellular modem directly with no router functions. This is accomplished using redirector software on your computer. This software creates a virtual serial port allowing your computer to communicate with the integrated cellular modem over IP using telnet.
<b>Raw Dialout</b>	Check the box to enable or disable raw mode for an Auto Dialout session. Default is Disable.
<b>Auto Dialout Login</b>	Check the box to enable or disable Auto Dialout Login feature. Default is Enable. The Auto Dialout port is the telnet port used by the redirector software on your computer to communicate to the integrated cellular modem.
<b>Auto Dialout Port</b>	Enter the serial Auto Dialout Port number. Default is 5000.
<b>Handle EIA Signal</b>	Check the box to enable or disable the EIA standard signal characteristics (time and duration) used between different electronic devices.
<b>Inactivity</b>	Enter the seconds that the auto dialout session stays active before going inactive.

## Syslog Configuration Group

<b>Syslog</b>	Check the box to enable or disable Syslog. Default is Disable.
<b>Syslog Server IP Address</b>	If a Remote Syslog Server IP Address is specified, the syslog feature acts as a remote Syslog.

## Auto Discovery Group

<b>Auto Discovery</b>	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 is Enable. The router sends a broadcast packet on the specified server port every 10 seconds or whatever interval the broadcast timer is set to.
<b>Server Port</b>	Enter the Server Port Number. Default port is 1020.
<b>Broadcast Timer</b>	Enter the amount of time in seconds for the auto-discovery packet granularity of periodic broadcasting. Default is 10 seconds.

## Auto Reboot Timer Configuration Group

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

## Telnet Configuration Group

Enables or disables the Telnet port. The default is Enable. This is specifically for telnet port 23 for technical support debug. You can still access the integrated cellular modem using port 5000 when this is disabled. Ensure that PPP is also disabled before telnetting to the port.

## Submitting and Saving Your Changes

Click **Submit** to save these settings.

Click **Save and Restart** after you complete and submit all the pages where you changed parameters.

## IP Setup, HTTP Configuration Parameters

### HTTP Configuration Group

**HTTP Port** Enter the port number on which the HTTP server listens for requests. The default is 80.

**HTTP Time-Out** Set the HTTP session in seconds. The default is 120 seconds.

### Authentication Group

Use the Authentication group to change the user name and password. The Username and password combination provide access the Web Management software, as well as telnet access to the router and integrated cellular modem.

**Username** Enter the name of a user who is allowed access to the Web Management software. Default is **admin**.

**Password** Enter the Password associated with the user who is allowed access to the Web Management software. Default is **admin**. It can be up to 100 characters. Use a safe password. Your first name spelled backwards is not a sufficiently safe password; a password similar to xft35\$4 is better.

### Submitting and Saving Your Changes

To save these settings, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.



## IP Setup, DDNS Configuration Parameters

DDNS (Dynamic Domain Naming System) allows you to have a static domain name with a dynamic IP address.

When the dynamic IP address changes, it is submitted to the DDNS server. Here, the domain name is updated to point to the new IP address.

You must register with a DDNS server to use this feature.

### General Group

This section describes the parameters that you can configure in the General group.

- |                        |   |
|------------------------|---|
| <b>DDNS</b>            | Check the Enable or Disable box. This enables/disables DDNS. Default is Disable.  |
| <b>Use Check IP</b>    | Check the Enable or Disable box. If enabled, the program queries 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 is updated based on the address returned by Check IP Server). If disabled, the program performs the DDNS update using the IP address that it obtains from the PPP link. Default is Enable. |
| <b>Check IP Server</b> | Enter the Server name from which the currently assigned IP address is obtained. This server is a server the router accesses to check its current IP address.  |
| <b>Check IP Port</b>   | Enter the port number of the Check IP Server. Default is 80.  |
| <b>Server</b>          | Enter the Server name to which the IP Address change is registered; for example, members.dyndns.org   |
| <b>Port</b>            | Enter the Server port number. Default is 80.  |
| <b>Max Retries</b>     | Enter the maximum number of tries that are allowed if the update fails. Default is 5. Range is 0 – 100.   |
| <b>Update Interval</b> | Enter the interval, in days, that lapse before the IP Address can change. At the end of this interval, the existing IP Address is updated in the server so that it does not expire. Default is 28 days. Range is 1 – 99 days.   |
| <b>System</b>          | Sets the system registration type as either Dynamic or Custom. Default is Dynamic.  |
| <b>Domain</b>          | Enter the registered Domain name.   |

## Authentication Group

This section describes the parameters that you can configure in the Authentication group.

- |                 |   |
|-----------------|---|
| <b>Username</b> | Enter the Username of the person who can access the DDNS Server. Default is NULL. You received your username when you registered with the DDNS service. |
| <b>Password</b> | Enter the Password of the user who can access the DDNS Server. Default is NULL. You received your password when you registered with the DDNS service.   |

## Submitting and Saving Your Changes

To save the changes you made to these parameters, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.

## IP Setup, SNTP Configuration Parameters

### General Configuration Group

- 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 that the SNTP Client contacts to update the time. No default.
- Polling Time** Enter the time, in minutes, after which the SNTP client requests the server to update the time. Default is 300 minutes.

### Time Zone Configuration Group

**Time Zone:** Enter the time zone. Default is UTC (Universal Coordinated Time, Universal Time). See the following website for Time Zone information:

<http://www.greenwichmeantime.com/info/current-time.htm>

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

## Daylight Configuration Group

- Daylight Saving** Enable or disable 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 Group

- Start Ordinal** Set the start ordinal to use during Daylight Saving mode. Options are first, second, third, fourth and last. Default is second. 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, select the week in which daylight saving time starts, either the first, second, third, fourth or the last of the month.
- Start Month** Set the start month to use during Daylight Saving mode. Default is March.
- 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 Group

- 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 and last. Default is first.
- End Month** Set the end month to use during Daylight Saving mode. Default is November.
- 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).

## Submitting and Saving Your Changes

To save your changes, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.

## IP Setup, Static Routes Parameters

Networked computers use routing information to identify whether they are sending data packets directly to the firewall or to another network.

After you define and add a route, you can use the table at the bottom of the group to delete or edit the route.

The screenshot displays the 'IP Setup -> Static Routes' configuration interface. On the left, a sidebar lists various configuration options, with 'Static Routes' currently selected. The main panel features a header 'IP Setup -> Static Routes' and a sub-header 'Add Static Routes'. Below the sub-header, there is a 'Static Route' configuration area. This area includes a dropdown menu labeled 'LANInterface', a right-pointing arrow '-->', and an adjacent empty text input field. A blue 'ADD' button is positioned below these elements. At the bottom of the configuration area, a table is visible with three columns: 'Name', 'IP Address', and 'Options'.

## Add Static Routes Group

IP packets destined for the network indicated in the drop down list are routed to the IP address in field pointed to by the arrow. You can define the networks in the drop down list under the 'Networks & Services' tab. The Static Route page does not display until the network is defined under **Networks & Services**.

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

**Add Button:** After you click **Add**, the new route appears in the table.

## IP Setup, Remote Configuration Parameters

Network/Host	Options
LAN	Static

## Remote Configuration Group

To add a network or host for remote configuration:

1. From the drop down list, select a network or host. Options are Any, LAN, and WAN Interface.  
To define more networks or hosts use the **Network & Services** tab.
2. Click **Add**. The network or host is added and appears in the table.
3. Repeat these steps for all that apply.
4. To delete **Any** and **WAN Interface** in the **Options** columns after either is added, click **Delete**.

## IP Setup, GPS Configuration Parameters

An rCell unit with a –GP build option enables the GPS Configuration. The –GP option allows you to configure forwarding of NMEA (National Marine Electronics Association) sentences from the built in GPS receiver to a device connected to the serial port or over the network to a remote host.

The TCP Server, TCP/UDP Client and Serial Port Dump can be enabled simultaneously.

All enabled sentences are forwarded periodically using the interval specified in the NMEA Configuration group. Before forwarding, the rCell inserts an ID Prefix and ID to each enabled NMEA sentence.

Available NMEA sentences are: GPGLA, GPGSA, GPGSV, GPGLL, GPRMC, GPVTG.

For detailed descriptions of the supported NMEA sentences, see the Universal IP AT Commands Reference Guide. You can download this guide from the Multi-Tech website.

The screenshot shows the 'IP Setup -> GPS Configuration' web page. On the left is a sidebar with navigation links: General Configuration, HTTP Configuration, DDNS Configuration, SMTP Configuration, Static Routes, Remote Configuration, and GPS Configuration. The main content area has three tabs: Local Configuration, Remote Configuration, and NMEA Configuration. The Local Configuration tab is active, showing 'TCP Server' set to 'Disable' with a 'Port' of '5445', a 'Password' field, and 'Serial Port Dump' set to 'Disable'. The Remote Configuration tab shows 'TCP/UDP Client' set to 'Disable', 'Protocol' set to 'TCP', 'Remote Host' as '192.168.2.3', 'Port' as '5445', and a 'Password' field. The NMEA Configuration tab shows an 'Interval' of '10', 'Add ID Prefix' and 'Add ID' fields, and checkboxes for 'GGA', 'GSA', 'GSV', 'GLL', 'RMC', and 'VTG', all of which are currently 'On'. A 'SUBMIT' button is located at the bottom of the NMEA Configuration section.

### Local Configuration Group

The Local Configuration group allows you to configure the TCP server port and allows for a serial port dump.

**TCP Server** Enable or disable TCP Server. The default is Disable.

**Port** Sets the port on which the server is listening. The default is 5445. The port range is from 1 to 5 digits, each digit between 0 and 9 inclusive. Note that numbers above 65,535 are illegal as the port identification fields are 16 bits long in the TCP header.

**Password** If a password is supplied, the TCP server requests that the remote client supply a password before sending the NMEA sentences.

**Serial Port Dump** Enable or disable the Serial Port. The default is Disable. The serial port configuration settings are used to configure the port. The serial port client/server must be disabled in order to use the serial port for GPS.

## Remote Configuration Group

The Remote Configuration group allows the device to connect to a remote server using the IP and port information for uploading GPS data.

<b>TCP/UDP Client</b>	Enable or disable the TCP/UDP Client and defines the protocol of the client. The defaults are Disable and TCP.
<b>Remote Host</b>	Displays the IP address and port number of the Remote Host.
<b>Password</b>	If the Remote Host requests a password, the password entered here is sent to the server in response.

## NMEA Configuration Group

The NMEA Configuration allows you to configure the time interval, any additional prefix or ID information and forward NMEA sentences.

<b>Interval</b>	The Interval is defined in seconds. The default is 10 seconds. The range is 1 to 255 seconds.
<b>Add ID Prefix</b>	The ID Prefix is 0 to 10 character prefix added to the ID.
<b>Add ID</b>	The ID is a unique remote asset identification string. You can specify up to 20 characters for the ID string. The & and \$ are invalid characters. The ID must follow the standard NMEA sentence structure. The Universal IP AT Commands Reference Guide, which you can download from the Multi-Tech website, describes sentence structure.
<b>NMEA Sentences</b>	GGA, GSA, GSV, GLL, RMC, and VTG are the NMEA sentences. You can turn each sentence On or Off. The default is On.

## Communication Examples

Communication is shown from the remote side.

### TCP Server example

```
read: "PASSWORD\r\n"
write: "serverpasswd\r\n"
read: "OK\r\n"
read: "&&rcell$GPGGA,192913.002,4505.9845,N,09311.7705,W,1,10,1.0,249.0,M,-29.0,M,,0000*6F\r\n"
read: "&&rcell$GPGSA,A,3,13,07,03,05,19,06,23,08,16,10,,,1.8,1.0,1.6*3F\r\n"
read: "&&rcell$GPGSV,3,1,12,07,59,308,33,13,59,202,32,03,55,083,33,19,50,136,33*76\r\n"
read: "&&rcell$GPGSV,3,2,12,06,43,065,26,23,35,177,26,08,24,296,27,16,19,059,21*79\r\n"
read: "&&rcell$GPGSV,3,3,12,10,14,286,29,05,07,321,28,24,06,087,23,21,01,029,*76\r\n"
read: "&&rcell$GPGLL,4505.9845,N,09311.7705,W,192913.002,A,A*43\r\n"
read: "&&rcell$GPRMC,192913.002,A,4505.9845,N,09311.7705,W,000.0,117.3,220710,,,A*76\r\n"
read: "&&rcell$GPVTG,117.3,T,,M,000.0,N,000.0,K,A*09\r\n"
read: "&&rcell$GPGGA,192915.002,4505.9842,N,09311.7699,W,1,10,1.0,248.9,M,-29.0,M,,0000*62\r\n"
read: "&&rcell$GPGSA,A,3,13,07,03,05,19,06,23,08,16,10,,,1.8,1.0,1.6*3F\r\n"
read: "&&rcell$GPGSV,3,1,12,07,59,308,33,13,59,202,33,03,55,083,33,19,51,136,33*76\r\n"
read: "&&rcell$GPGSV,3,2,12,06,43,065,25,23,35,177,26,08,24,296,27,16,19,059,21*7A\r\n"
read: "&&rcell$GPGSV,3,3,12,10,14,286,28,05,07,321,28,24,06,087,23,21,01,029,*77\r\n"
read: "&&rcell$GPGLL,4505.9842,N,09311.7699,W,192915.002,A,A*46\r\n"
read: "&&rcell$GPRMC,192915.002,A,4505.9842,N,09311.7699,W,000.0,117.3,220710,,,A*73\r\n"
read: "&&rcell$GPVTG,117.3,T,,M,000.0,N,000.0,K,A*09\r\n"
```

**TCP Client Example with password**

```
write: "PASSWORD\r\n"
read: "clientpasswd\r\n"
write: "OK\r\n"
read: "&&rcell$GPGGA,193038.002,4505.9798,N,09311.7646,W,1,10,1.0,230.2,M,-29.0,M,,0000*6B\r\n"
read: "&&rcell$GPGSA,A,3,13,07,03,05,19,06,23,08,16,10,,,1.8,1.0,1.5*3C\r\n"
read: "&&rcell$GPGSV,3,1,12,07,60,309,31,13,59,201,30,03,54,082,30,19,51,135,28*75\r\n"
read: "&&rcell$GPGSV,3,2,12,06,42,064,21,23,34,177,25,08,24,297,20,16,18,060,20*70\r\n"
read: "&&rcell$GPGSV,3,3,12,10,13,285,31,05,07,320,28,24,07,086,26,21,01,028,*7E\r\n"
read: "&&rcell$GPGLL,4505.9798,N,09311.7646,W,193038.002,A,A*4B\r\n"
read: "&&rcell$GPRMC,193038.002,A,4505.9798,N,09311.7646,W,000.0,117.3,220710,,,A*7E\r\n"
read: "&&rcell$GPVTG,117.3,T,,M,000.0,N,000.0,K,A*09\r\n"
read: "&&rcell$GPGGA,193040.002,4505.9796,N,09311.7646,W,1,10,1.0,230.1,M,-29.0,M,,0000*69\r\n"
read: "&&rcell$GPGSA,A,3,13,07,03,05,19,06,23,08,16,10,,,1.8,1.0,1.5*3C\r\n"
read: "&&rcell$GPGSV,3,1,12,07,60,309,32,13,59,201,29,03,54,082,31,19,51,135,28*7F\r\n"
read: "&&rcell$GPGSV,3,2,12,06,42,064,22,23,34,177,26,08,24,297,19,16,18,060,21*7B\r\n"
read: "&&rcell$GPGSV,3,3,12,10,13,285,32,05,07,320,28,24,07,086,25,21,01,028,*7E\r\n"
read: "&&rcell$GPGLL,4505.9796,N,09311.7646,W,193040.002,A,A*4A\r\n"
read: "&&rcell$GPRMC,193040.002,A,4505.9796,N,09311.7646,W,000.0,117.3,220710,,,A*7F\r\n"
read: "&&rcell$GPVTG,117.3,T,,M,000.0,N,000.0,K,A*09\r\n"
```



## PPP, PPP Configuration Parameters

The screenshot displays the 'PPP -> PPP Configuration' web page. On the left is a sidebar with links: 'PPP Configuration', 'Wakeup on call', 'PowerOn Configuration', and 'Modem Commands'. The main content area is divided into several sections:

- NAT Configuration:** Includes a 'NAT' toggle with 'enable' (selected) and 'disable' options.
- PPP General:** Contains 'PPP' (enable/disable), 'Dial-on-Demand' (enable/disable), 'Idle time out (in Sec)' (150), 'Connect time out (in Sec)' (90), and 'Dialing Max retries' (0).
- Authentication:** Features 'Authentication Type' (ppp, chap, ppp-chap), 'Username', and 'Password' fields.
- ICMP/TCP Keep Alive check:** Includes 'Keep Alive check' (enable/disable), 'Keep Alive Type' (ICMP, TCP), 'HostName', 'TCP Port', 'Interval (in Secs)' (60), and 'ICMP Count' (10).
- Modem Configuration:** Contains 'Dial number' (\*pp\*\*\*1#), 'Dial Prefix' (ATDT), 'Connect String' (CONNECT), 'APN', 'Init String1' (AT+CSQ), 'Init String2', 'Init String3', 'Init String4', and 'Baud Rate' (230400 bps).

A 'SUBMIT' button is located at the bottom right of the configuration area.

### NAT Configuration Group

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

**Note:** For routing to take effect, enable then save the configuration.

### Enabling NAT

Your LAN can use one set of IP addresses for internal traffic and a second set of addresses for external traffic. The router with NAT does the simple IP routing between the LAN interface and the WAN interface. NAT hides the LAN address behind a single IP address on the wireless side.

Your internal addresses are shielded from the public Internet.

## Disabling NAT

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 defeat the purpose of enabling Routing.

## PPP General Group

**PPP:** Enable or disable PPP. The default is Disable. When enabled, the unit functions as a router. PPP must be disabled to access the integrated cellular modem directly using telnet port 5000. If PPP is enabled, you cannot access the integrated cellular modem.

**Dial-on-Demand:** Enable or disable Dial-on-Demand. The default is Disable. If you disable it, the router always stays connected unless the Idle Time Out expires. When Dial-on-Demand is enabled, use the 'Wakeup on Call' settings under the PPP menu to configure the settings for re-establishment of the connection.

**Idle Time Out:** Set the amount of idle time that passes before the router timeouts. The default is 180 seconds. If the time expires, the PPP connection to the Internet disconnects. Any IP packets from the LAN side or IP traffic from the wireless side resets this timer and prevents the connection from dropping.

**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 Group

**Authentication Type:** Set the authentication protocol type that negotiates with the remote peer: pap/chap/pap-chap. Default is pap-chap.

**Username:** Enter the Username with which the remote peer authenticates. You can leave this field blank, if desired. Username is limited to 60 characters.

**Password:** Enter the Password with which the remote peer authenticates. You can leave this field blank, if desired. Password is limited to 60 characters.

## ICMP Keep Alive Check

**Keep Alive Check:** Enable or disable Keep Alive Check. The default is Disable. This is used to periodically check that the Internet connection is up. If it is not, the router tries to reconnect.

**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 60 seconds.

**ICMP Count:** Set the number of ICMP Keep Alive Checks to be sent to the specified host. Default is 10.

## Modem Configuration Group

To know the proper information to enter into this group, refer to the Customer Activation Notices included with the product.

**Dial Number:** Set the dial number to be dialed. Default is NULL.

For GSM models, the Dial Number is **\*99\*\*\*1#**

For CDMA models, the Dial 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:** Enter the APN (Access Point Name). The APN is assigned by your wireless service provider.

**Init String 1-4:** Configure the modem init strings. You can set up to 4 modem initialization strings.

**Baud Rate:** The Baud Rate option is only displayed on certain models and is set at 230.4K, by default. The default setting is set for maximum performance. Setting the baud rate higher, particularly on the G2 models, is not recommended as it may adversely affect the performance.

## Submitting and Saving Your Changes

To save these settings, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.

# PPP, Wakeup-on-Call Parameters

The Wakeup-on-Call feature allows the router to wake up and initiate a connection when there is an incoming call or LAN activity. . The Wakeup-on-Call feature reduces the cost incurred when a router is online and available 24/7.

If you desire some security with this feature, you can set up the router to wake up based on Caller ID or SMS instead of allowing all incoming calls to wake up the router. Dial-on-Demand in the IP Setup menu must be enabled for wakeup-on-call features to go into effect.

**Note:** When provisioning this feature, you must allow incoming calls, SMS capability, and caller-id.

PPP

PPP Configuration

Wakeup on call

PowerOn Configuration

Modem Commands

PPP -> Wakeup on call

Wakeup on call Configuration

Wakeup on Call

Enable

Disable

Time Delay (sec)

10

Dial On Demand from LAN

Enable

Disable

Init String 1

Init String 2

Init String 3

Init String 4

Init String 5

Caller ID Configuration

Add 'Wakeup on call' Caller ID

ADD

Sl No	Caller ID	Options
-------	-----------	---------

Caller Acknowledgement Configuration

Acknowledgement String to Caller

SUBMIT

## Wakeup-on-Call Configuration Group

**Wakeup on Call:** Enable or disable the Wakeup-on-Call feature. The default is Disable. Wakeup on Call occurs when a ring or caller ID is detected. This triggers the router to reconnect after the 'Time Delay' expires.

**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 disable. When enabled, the router reconnects when it sees IP traffic on the LAN is needed to route. If this feature is disabled, Dial-on-Demand initiates a PPP connection to the Internet only from the WAN, not from the LAN.

44

Multi-Tech Systems, Inc. MultiModem rCell User Guide

**Init Strings:** Configure the router initialization strings. These init strings need to be specific to the integrated cellular modem. Some initialization may be required for the integrated cellular modem to accept SMS for 'Wakeup on Call'. Init-num can range from 1-5. The default is NULL. Refer to the following table for examples of Init Strings depending on model.

Model	Init 1	Init 2	Init 3	Init 4	Ack	Comment
C1-EN2-GP			AT+CNMI=2,2,0,0,1	AT+CLIP=1	AT+CNMA	Ring with CLI, SMS with ACK
E1-EN2-GP	AT+CMGF=1	AT+CSMS=1	AT+CNMI=2,2,0,0,1	AT+CLIP=1	AT+CNMA	Ring with CLI, SMS with ACK
G2-EN2-GP	AT+CMGF=1	AT+CSMS=1	AT+CNMI=2,2,0,0,1	AT+CLIP=1	AT+CNMA	Ring with CLI, SMS with ACK
H4-EN2*			AT+CLIP=1			Ring with CLI
H4-EN2- GP*			AT+CLIP=1			Ring with CLI
EV2-EN2*			AT+CLIP=1			Ring with CLI
EV2-EN2- GP*			AT+CLIP=1			Ring with CLI

**\*Does NOT support Wakeup On Call using SMS.**

**Submit:** Click **Submit** to save these settings.

## Caller ID Configuration Group

**Add “Wakeup on Call” Caller ID:** To add Caller ID to the Wakeup-on-Call function, enter the Caller ID that can wake up the router. Enter ‘RING’ (all Caps) to wake up on any call. Enter a CID phone number or an SMS message. Ensure the SMS message string does not contain any spaces between words.

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

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

Caller Acknowledgement Configuration

**Acknowledgement String to Caller:** The configured string of (0 to 40 characters) that is sent to the integrated cellular 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 is not sent upon successful caller ID reception.

## Submitting and Saving Your Changes

To save these settings, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.

## Wakeup-On-Call Examples

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

1. On the **PPP > PPP Configuration** page, configure 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 likely gave these items to you when you activated your account.

- Modem Configuration

Make sure your Dial Number is entered correctly.

For GSM models, the Dial Number is **\*99\*\*\*1#**

For CDMA models, the Dial Number is **#777**

Enter your APN. Your wireless service provider assigns the APN.

Example: AT+CGDCONT=1,"IP","Internet" The Example: AT+CGDCONT=1,"IP","Internet" needs to be removed. Just the APN name needs to be entered in the APN field.

2. To save the changes made on this page, click **Submit**.

3. On the **PPP > Wakeup-on-Call** screen, configure 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 from the model dependent table described in the Wakeup-on-Call Configuration.
4. To save the changes made on this page, click **Submit**.
  - Caller ID Configuration  
Enter an SMS to add to the Caller ID list.  
**Note:** Add the SMS message string into the Caller ID list. The SMS message string must not contain any spaces between words. When the configured string matches the SMS message string, it activates the Wakeup-on-Call feature.  
To save each message as it is entered into the Caller ID list click **Add**.
  - Caller Acknowledgement Configuration  
Enter a configured string (0 to 40 characters) that is sent to the integrated cellular modem upon receiving a valid Caller ID from the WAN.  
Set the Wakeup Acknowledgement string configuration with the command **at+cnma**  
To save the Acknowledgement Configuration, click the Submit.
5. To ensure your changes go into effect, click **Save and Restart**. The device saves all the settings and reboots the computer.

### Example 2 – Determine if the router Is Supporting Incoming Calls and Caller ID

1. On the **PPP > PPP Configuration** page, make sure that **PPP** is **Disabled**.
2. On the PPP > Wakeup-on-Call screen, make sure that Wakeup-on-Call is Disabled.
3. To open a command prompt, from the **Start** button and select **Run**.
4. Type **CMD** to open the command window. Click **OK**.
5. When the command window opens, telnet to the router.  
**Note:** 5000 is the router port number.
  - d. Enter your username and password to login.
  - e. Enter an AT command to make sure you receive a response; i.e., OK.
  - f. To determine the dial number of your router, enter the command AT+CNUM.  
For the Wakeup-on-Call function to work the RING or CALLER ID information must appear.
6. To determine if the RING message shows, from another phone, call your router using the dial number of your router.
7. To enable Caller ID, enter the **AT+CLIP=1** command. Make the call again to verify Caller ID information.  
Some wireless providers do 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** page, set up the following parameters:

#### PPP General

- Make sure that PPP is Enabled.
- Make sure Dial-on-Demand is Enabled.
- 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 username and password are required, your wireless provider likely gave you these items when you activated your account.

#### Modem Configuration

- Make sure your Dial Number is entered correctly:
- For GSM models, the Dial Number is \*99\*\*\*1#
  - For CDMA models, the Dial Number is #777

#### 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.
- Ensure all Init Strings are 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. To ensure your changes go into effect, click **Save and Restart**. The device saves all the settings and reboots the computer.

### 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.
- Make sure Dial-on-Demand is Enabled.
- 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 likely gave you these items when you activated your account.

#### Modem Configuration

- Make sure your Dial Number is entered correctly:

For GSM models, the Dial Number is **\*99\*\*\*1#**

For CDMA models, the Dial Number is **#777**

2. To save the changes, click **Submit**.
3. On the **PPP > Wakeup-on-Call** screen, set up the following parameters:

#### Wakeup-on-Call Configuration

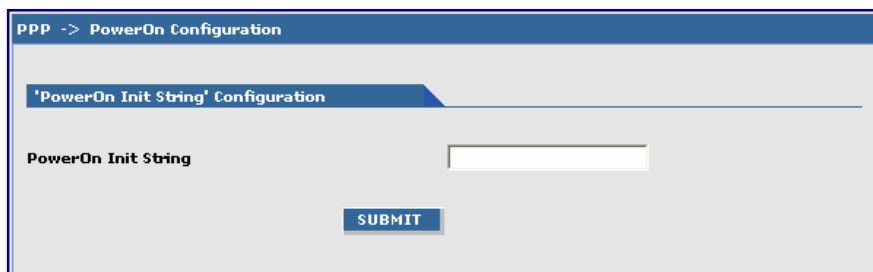
- Select **Enable** for Wakeup-on-Call.
- Set the Time Delay. You can use the 10 second default.
- Enter the Init Strings:
- To set Wakeup Init String 1 type **AT+CLIP=1**.
- To save settings, click Submit.

#### Caller ID Configuration

- To add a caller's ID, to the Caller ID list, type that id.
- Click **Add**.
- To save each Caller ID as it is entered to the Caller ID list, click **Add**.
- To ensure your changes go into effect, click **Save and Restart**. The device saves all the settings and reboots the computer.

## PPP, Power-On Configuration Parameters

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



**Power-On Init String:** You can enter a string of 0 to 40 characters that is sent to the router upon boot up. All commands initializes before you proceed with regular PPP related activity.

**Note:** When no initialization string is configured, regular functions of the router is retained.

To save this setting click **SUBMIT**.

To ensure your changes go into effect, click **Save and Restart**.

## PPP, Modem Commands Parameters

You can configure modem commands to allow an external application to query modem information.

- The application can use the URL [HTTP://xxx.xxx.xxx.xxx/modeminfor.html](http://xxx.xxx.xxx.xxx/modeminfor.html) to determine the IP address that is currently assigned to the integrated cellular modem after the PPP connection is established.
- You can also display the results of up to ten AT commands.

### Modem AT Commands Configuration Group

These commands are sent when a PPP connection to the network is initiated.

Useful HSDPA AT commands include:

Command	Description
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

#### Retrieving Modem Information without using a browser:

To obtain the integrated cellular modem information without using a browser:

1. Make a TCP connection to port 80 (same as the Web Admin port) and send data as:  
GET /atinfor.html HTTP/1.1
2. Press Enter twice.

Refer to the AT Command Reference Guides for other commands.

## Networks & Services, Network Configuration Parameters

### Network Configuration Group

Use this group to add networks or hosts. After you define and add a network, you can delete or edit it by using the table.

The screenshot shows the MultiTech Systems Web Management Software interface. The top navigation bar includes links for IP Setup, PPP, Networks & Services, Packet Filters, GRE Tunnels, DHCP Server, Tools, Statistics & Logs, Save & Restart, and Help-Index. The sidebar on the left has 'Networks & Services' selected, with sub-links for 'Network Configuration' and 'Service Configuration'. The main content area is titled 'Networks & Services -> Network Configuration' and contains a 'Network Configuration' section. This section has three input fields: 'Name', 'IP Address', and 'Subnet Mask'. Below these fields is an 'ADD' button. At the bottom of the section is a table with the following data:

Name	IP Address	Mask	Options
Any	0.0.0.0	0	Static
LAN	192.168.2.0	24	Static
WANInterface	NotAcquired	32	Static
LANInterface	192.168.2.1	32	Static

### Configuring the Network

Before you configure the network, note the following:

- You cannot edit a Network/Host Name.
- You cannot delete a Network/Host another configuration is using it.
- Network/Host changes are reflected in all the configurations in the Web Management software where they are used.
- Network/Hosts that you add here are displayed in the following sections: Static Routes, DNAT, and Packet Filters.

To configure:

1. In the **Name** field, type the name of the Network/Host. Make sure the same address-mask pair does not already appear in the list. The Name is limited to 15 characters maximum.
2. In the **IP Address** field, type the IP Address of the Network/Host. Make sure the same address-mask pair does not already appear in the list.
3. In the **Subnet Mask** field, type 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.

4. To add the network, click **Add**. The defined network appears in the table.

# Networks & Services, Service Configuration Parameters

## Service Configuration Group

These parameters let you specify the standard set of well known services available on the system. These services enable the configuration of the user-defined services. You can delete or edit services after defining and adding them. Use 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

## Configuring New Services

Before you configure the network, note the following:

- 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 are displayed in the following sections: DNAT, Packet Filters.

To configure:

1. For the new service, configure the following parameters:

**Name:** Enter the name of the Service which is limited to 16 characters. It has to be unique.

**Protocol:** Enter the type of protocol (TCP, UDP).

**Source Port:** Enter the Destination Port for this service. The source and destination ports can be entered either as a single port or a range using a colon as the separator.

**Destination Port:** Enter the name of the Destination Port for the service.

2. Click **Add**. The new service is added and appears on the page.

## Packet Filters, Packet Filters Parameters

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.

The screenshot shows the MultiTech Systems web management interface. The top navigation bar includes links for IP Setup, PPP, Networks & Services, Packet Filters, GRE Tunnels, DHCP Server, Tools, and Statistics. The left sidebar has links for Packet Filters, DNAT Configuration, and Advanced. The main content area is titled 'Packet Filters -> Packet Filters' and contains a 'Packet filter' form. The form has four fields: 'From (Hosts/Networks)' with a dropdown menu showing 'Any', 'Service' with a dropdown menu showing 'Any', 'To (Hosts/Networks)' with a dropdown menu showing 'Any', and 'Action' with a dropdown menu showing 'ACCEPT'. Below the form is an 'ADD' button. At the bottom, there is a table with the following data:

From (Host/Network)	Service	To (Host/Network)	Action	Options
LAN	Any	Any	ACCEPT	Edit Delete

## Packet Filter Group

**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 is informed that the packet has been rejected.
- **Drop:** Blocks all packets that match this rule, but the host is not informed; that is, this is a silent drop.
- **Log:** Packets matching the rule; that is, the corresponding source address, destination address, and service are logged.

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

## Packet Filters, DNAT Configuration Parameters

### DNAT Configuration Group

Destination Network Address Translation (DNAT) allows you to place servers within the protected network and make them available for a certain service to the outside world. The DNAT process running on the 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.

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

Allow Access	External Service	LAN IP	Internal Service	Internal Source	Options
Any	Any	WANInterface	Any	NOCHANGE	Edit Delete

**Allow Access:** Select a network or host to which IP packets are 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 are going to be sent. If you do not want to change the address, select **NOCHANGE**.

**Save Button:** Click **Save**. The defined DNAT configuration is added and appears at the bottom of the page. Entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

### Example: Setting Up DNAT and Port Forwarding to an Internal Device

**Note:** The internal device can be camera, meter, security device, and so on.

**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. In the **Network & Services > Network Configuration** group, define 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. The subnet mask in the network configuration is not defined using x.x.x.x notation. It uses 'bit' notation. So 255.255.255.255 = 32.



2. To save this configuration, click **Add**.
3. In the **Network & Services > Service Configuration** group, define a service name. For this example, the service is a meter.

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

**Protocol** – Select a protocol. **Example:** tcp or 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.
4. In the **Packet Filters > DNAT Configuration** group, define the DNAT rule.

**Allow Access** – 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

**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.

**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 are going to be sent. If you do not want to change the address, select **NOCHANGE**. **Example:** NOCHANGE
5. To save this configuration, click **Save**.

**Note:** You must click **Save and Restart** once you have completed and submitted all the screens on which you have made changes. The device saves all the settings and reboot the computer.

## Packet Filters, Advanced Parameters

Packet Filters -> Advanced

**Connection Tracking**

**H323** ☐ enable ☒ disable

**PPTP** ☐ enable ☒ disable

**ICMP Configuration**

**ICMP on LAN** ☒ enable ☐ disable

**ICMP on WAN** ☒ enable ☐ disable

**ICMP Forward** ☒ enable ☐ disable

**SUBMIT**

### Connection Tracking Group

**H323:** Enable or disable the forwarding of H323 packets across the firewall.

**PPTP:** Enable or disable PPTP Packet Pass-through (PPTP NAT support).

**Note:** H323 and PPTP are disabled by default.

### ICMP Configuration Group

Use the Internet Control Message Protocol (ICMP) to test the network connections and the firewall. You can also use ICMP 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 or disable the transfer of ICMP packets on the LAN interface.

**ICMP on WAN:** Enable or disable the transfer of ICMP packets on the WAN interface.

**ICMP Forward:** Enable or disable the forwarding of ICMP packets through the firewall into the local network.

**Note:** ICMP on the LAN, WAN, and Forward are enabled by default.

### Submitting and Saving Your Changes

To save these settings, click **Submit**.

To ensure your changes go into effect, click **Save and Restart**.

## GRE Tunnels

Generic Routing Encapsulation (GRE) includes GRE tunneling and GRE routing

First, you create the GRE Tunnels by using the GRE Tunnel Configuration group.

Then, you configure the routes for the remote networks that are routed through a tunnel, by using the GRE Routes Configuration group. All the traffic destined to remote networks associated to a tunnel are 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.

The screenshot shows the MultiTech Systems web management interface. The top navigation bar includes links for IP Setup, PPP, Networks & Services, Packet Filters, GRE Tunnels, DHCP Server, Tools, and Statistics. The left sidebar has a 'GRE Tunnels' tab selected, with sub-links for 'GRE Tunnels' and 'GRE Routes'. The main content area is titled 'GRE Tunnel Configuration' and contains the following fields:

- Tunnel Name:** A text input field.
- Local IP:** A dropdown menu currently showing 'WANInterface'.
- Remote IP:** A dropdown menu currently showing 'FQDN', with an 'OF' radio button next to it.

Below these fields is an 'ADD' button. At the bottom of the configuration area, there is a table with the following headers:

Tunnel Name	Local IP	Remote IP	Options
-------------	----------	-----------	---------

### GRE Tunnel Configuration Group

**Tunnel Name:** Enter a name for the new tunnel.

**Local IP:** Select the local interface on which the tunnel is created. Eventually, the packets destined for this tunnel are 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 where the routed packets are received).

OR

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

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

## GRE Tunnels > GRE Routes Configuration

The screenshot shows a web interface for configuring GRE routes. At the top, there is a breadcrumb trail: "GRE Tunnels -> GRE Routes". Below this is a tabbed interface with the "GRE Routes Configuration" tab selected. The configuration area contains two dropdown menus: "Remote Network" with "Any" selected, and "Tunnel Name" with an empty selection. Below these is a blue "ADD" button. At the bottom, there is a table with three columns: "Remote Network", "Tunnel Name", and "Options".

Remote Network	Tunnel Name	Options
----------------	-------------	---------

**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 is 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 **Add**. The defined GRE route configuration is added and appears at the bottom of the page.

## DHCP Server, Subnet Settings

**MultiTech Systems**

IP Setup | PPP | Networks & Services | Packet Filters | GRE Tunnels | **DHCP Server** | IPSec | Serial Port | Tools | Statistics & Logs

**DHCP Server**

Subnet Settings  
Fixed Addresses

**DHCP Server -> Subnet Settings**

**General Configuration**

DHCP ☒ Enable ☐ Disable

Subnet  Mask

Default Gateway  DNS

Lease Time(dd-hh-mm)  (00-00-00 : infinite lease time)

**SUBMIT**

**Subnet Settings**

From  To

**ADD**

From	To	Options
192.168.2.100	192.168.2.200	<a href="#">Delete</a>

### 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 or disable the DHCP server.

**Subnet:** Enter the subnet address. If you want to change the DHCP subnet address, you first have to delete all the subnet settings below.

**Mask:** Enter the subnet mask.

**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.

To save your changes, click **SUBMIT**.

To ensure your changes go into effect, click **Save and Restart**.

### Subnet Settings

**From-To Range:** Enter the range of IP addresses to be assigned by DHCP.

**Add:** Click the **Add** button. The address range is added and appears in the table at the bottom of the screen. Once the range displays, you can delete if necessary.

**Note:** See Appendix A Commonly Supported Subnets.

## DHCP Server > Fixed Addresses

The screenshot shows a web interface for configuring DHCP fixed addresses. At the top, there is a breadcrumb trail 'DHCP Server -> Fixed Addresses'. Below this is a tabbed interface with 'DHCP Subnet Settings' selected. The main area contains two input fields: 'Mac-Address' and 'IP Address'. Below these fields is an 'ADD' button. At the bottom, there is a table with three columns: 'Mac-Address', 'IP Address', and 'Options'.

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 is 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 appear in the table at the bottom of the page from where they can be deleted or changed.

## IPSec

The IPSec (IP Security) protocol suite, based on modern cryptographic technologies, provides security services like encryption and authentication at the IP network layer. It secures the whole network traffic providing guaranteed security for any application using the network.

You can use IPSec to create private secured tunnels between two hosts, two security gateways, or a host and a security gateway. Up to three tunnels can be active at any given time. You can save more than three active tunnels, but they are not active.

IPSec provides encryption and authentication services at the IP level of the protocol stack. IPSec can protect any traffic carried over IP.

## Authentication and Encryption Overview

IPSec provides the following services:

- Authentication only
- Encryption only

To transmit and receive data securely over an unprotected network:

1. Select the type of IPSec service—authentication or encryption—required for the connection.
2. Establish a secure connection by a key exchange process, using one of the following:
  - Manual Keying where the authentication and encryption keys are provided manually on both sides of the connection.
  - Auto Keying using IKEv2 Protocol where the authentication and encryption keys are generated on either side of the connection and exchanged by different methods.
3. Transfer data using the connection.

## IPSec > IPSec

The screenshot displays the MultiTech Systems web management interface. The top navigation bar includes links for IP Setup, PPP, Networks & Services, Packet Filters, GRE Tunnels, DHCP Server, IPSec, Serial Port, and Tools. The left sidebar shows 'IPSec' as the selected menu item. The main content area is titled 'IPSec -> IPSec' and contains the following elements:

- VPN Status:** A checkbox that is currently unchecked, followed by a 'Save' button.
- Add New Connection:** A section with two options:
  - IKE Connection:** With an 'Add' button.
  - Manual Connection:** With an 'Add' button.
- Table:** A table with the following columns: Status, Connection Name, Local WAN IP, Local LAN, Remote Gateway IP, Remote LAN, and Command.

## IPSec

**VPN Status:** Check the VPN Status checkbox to enable IPSec. Click **Save**.

### Add a New Connection

**Add IKE Connection:** Click **Add IKE Connection**. A page opens where you can configure an IKE connection.

**Add Manual Connection:** Click **Add Manual Connection**. A page opens where you can configure a manual connection.



## Add IKE Connection

The screenshot shows a web management interface for adding an IKE connection. The form is titled 'ADD IKE Connection' and contains the following fields and options:

- Connection Name:** A text input field.
- Compression:** A checkbox, currently unchecked.
- Perfect Forward Secrecy:** A checkbox, currently checked.
- Authentication Method:** A dropdown menu set to 'Secret'.
- Pre-Shared Key:** A text input field.
- Select Encryption:** A dropdown menu set to '3DES'.
- IKE Life Time:** A text input field with '1' and a unit of 'hours'.
- Key Life:** A text input field with '1' and a unit of 'hours'.
- Number of retries (zero for unlimited):** A text input field with '0'.
- Local WAN IP:** A dropdown menu set to 'WANInterface'.
- Local LAN:** A dropdown menu set to 'LAN'.
- Remote Gateway IP:** A text input field.
- OR**
- FQDN:** A text input field.
- Remote LAN:** A dropdown menu set to 'None'.
- UID:** A checkbox, currently unchecked.
- Local ID:** A text input field.
- Remote ID:** A text input field.
- NetBIOS Broadcast:** A checkbox, currently unchecked.
- Save:** A button at the bottom right.

## Add an IKE Connection

**Connection Name:** Type a name for the connection.

**Compression:** Check the compression checkbox to enable IPCOMP, the compression algorithm.

**Perfect Forward Secrecy (PFS):** Check the PFS checkbox to enable PFS, a concept in which the newly generated keys are unrelated to the older keys). This is enabled by default.

**Authentication Method:** Authentication can be done using Pre-Shared Secrets.

**Pre-Shared Key:** The Pre-Shared Key must be agreed upon and shared by the VPN endpoints. Configured it at both endpoints of the tunnel.

**Select Encryption:** Select the encryption method. 3DES is recommended. Options include 3DES, AES-128, AES-192, AES-256

**IKE Life Time:** The duration for which the ISAKMP SA lasts, from successful negotiation to expiration. The default value is one hour and the maximum is 8 hours.

**Key Life:** The duration for which the IPsec SA lasts, from successful negotiation to expiration. The default value is one hour and the maximum is 24 hours.

**Number of Retries:** Specify the number of retries for the IPsec tunnel. Enter zero for unlimited retries.

**Local WAN IP:** This is the interface initiating the IPsec tunnel.

**Local LAN:** Internal subnet of the local security gateway for which the security services are provided. If the router acts as a host, configured as None.

**Remote Gateway IP:** Interface where the IPSec tunnel ends. In the case of a Road Warrior with a Dynamic IP address, configure to **ANY**.

**FQDN:** FQDN is a Fully Qualified Domain Name that resolves to the Local Wan IP of the router or in the case of GRE/IPSEC, it is used to identify the Wan IP of the remote location. This is provided by your ISP or created by you if you are using a Dynamic DNS service. When FQDN is selected, leave the Remote Gateway IP blank.

**Remote LAN:** Internal subnet of the remote security gateway for which the security services are provided. If the remote end is the host, set this to None.

**UID (Unique Identifier String):** Check the UID box to enable the Local ID and Remote ID. Local ID and Remote ID are active only when UID is enabled.

Local ID

Enter a string identifier for the local security gateway.

Remote ID

Enter a string identifier for the remote security gateway.

**NetBIOS Broadcast:** Check this option to enable broadcasts over the connection. It allows computers on the network to share Microsoft file and printer sharing information.

**Save Button:** Click the Save button to save these settings.

## Add Manual Connection

The screenshot shows the 'ADD Manual Connection' form within the IPsec management interface. The form contains the following fields and options:

- Connection Name:** A text input field.
- Compression:** A checkbox.
- Authentication Method:** A dropdown menu with 'SHA1-96' selected.
- Authentication Key:** A text input field.
- Encryption Method:** A dropdown menu with '3DES' selected.
- Encryption Key:** A text input field.
- SPI Base:** A text input field.
- Local WAN IP:** A dropdown menu with 'WANInterface' selected.
- Local LAN:** A dropdown menu with 'LAN' selected.
- Remote Gateway IP:** A text input field.
- OR:** A text label between the Remote Gateway IP and FQDN fields.
- FQDN:** A text input field.
- Remote LAN:** A dropdown menu with 'None' selected.
- NetBIOS Broadcast:** A checkbox.
- Save:** A button at the bottom right.

**Connection Name:** Type name to identify the connection.

**Compression:** Check the compression checkbox to enable IPCOMP, the compression algorithm.

**Authentication Method:** Select the authentication algorithms used for the respective security services. Options are MD5-96 and SHA1-96.

**Authentication Key:** The VPN firewall can use either MD5-96 or SHA1-96 for authentication. For example, MD5-96 with a key of abcdefgh12345678.

Authentication Protocol	Key Length	Accepted Characters
SHA1-96	Must be 20 characters	Alphanumeric characters
MD5-96	Must be 16 characters	Alphanumeric characters

**Encryption Method:** Select the encryption method. Options include 3DES, AES-128, AES-192, AES-256, and NULL (no encryption).

**Encryption Key:** The router can use any one of the methods specified in its encryption algorithm. For example 3DES uses 24 alphanumeric characters (192 bits) as its encryption key. Example: 1234567890abcdefabcdab

Encryption Protocol	Key Length	Accepted Characters
Null	Must be 24 characters	Alphanumeric Characters
3DES	Must be 24 characters	Alphanumeric Characters
AES-128	Must be 16 characters	Alphanumeric Characters
AES-192	Must be 24 characters	Alphanumeric Characters
AES-256	Must be 32 characters	Alphanumeric Characters

**SPI Base:** The Security Parameter Index identifies a manual connection. The SPI is a unique identifier in the SA (Secure Association – a type of secure connection) that allows the receiving computer to select the SA under which a packet is processed. The SPI Base is a number needed by the manual keying code. Enter any 3-digit hexadecimal number, which is unique for a security association. Enter in the format of 0xhex (0x100 through 0xfff is recommended). If you have more than one manual connection, then the SPI Base must be different for each one.

**Left Next Hop:** Next Hop is the address of the next device in a routing table's path that moves a packet to its destination. You can configure this setting or leave it as a static value: 0.0.0.0. When not configured, the value is set to the Gateway of the Box/Gateway configured on the Interface/Right IP. The selection is based on the Left and Right IP.

**Local WAN IP:** Select the Interface to initiate the IPSec tunnel (Left Security Gateway).

**Local LAN:** Select the internal subnet of the local security gateway for which the security services are to be provided. If the router acts as a host, configure as **None**. Other options are Any, LAN, LAN Interface, WAN 1, WAN 1 Interface.

**Remote Gateway IP:** Select the interface in which the IPSec tunnel ends. In the case of Road Warriors with a Dynamic IP addresses, set to **ANY**. Other options include: LAN, LAN Interface, WAN 1, WAN 1 Interface, and None.

**FQDN:** FQDN is a Fully Qualified Domain Name that resolves to the Local Wan IP of the router or in the case of GRE/IPSEC, it is used to identify the Wan IP of the remote location. This is provided by your ISP or created by you if you are using a Dynamic DNS service. When FQDN is selected, leave the Remote Gateway IP blank.

**Remote LAN:** This is the internal subnet of the remote security gateway for which the security services are to be provided. If the remote end is a host, set to **None**.

**NetBIOS Broadcast:** Check this option to enable broadcasts over the connection. This allows computers on the network to share Microsoft file and printer sharing information.

**Save Button:** Click **Save** to save these settings.

## Serial-Port, Serial Port Settings Parameters

The screenshot displays the MultiTech Systems web management interface. At the top, a navigation bar includes links for IP Setup, PPP, Networks & Services, Packet Filters, GRE Tunnels, DHCP Server, IPSec, Serial Port, and Tools. A left sidebar highlights the 'Serial Port' section, with sub-links for 'Serial Port Settings', 'Client Settings', and 'Server Settings'. The main content area, titled 'Serial Port -> Serial Port Settings', features a 'Serial-Port Configuration' section. This section contains several configuration parameters: Baud Rate (set to 115200 bps), Data Bits (set to 8), Parity (set to None), Buffer Length (set to 32), Timeout (set to 1 Sec), Flow Control (set to None), and Stop Bits (set to 1). A 'SUBMIT' button is located at the bottom right of the configuration area.

### Serial-Port Configuration Group

Serial-Port Configuration lets you configure the serial terminal connected to the RS-232 connector DE9 on the back of the unit.

**Baud Rate:** Sets the baud-rate at which the serial terminal is communicating. The default is 115200.

**Flow Control:** Sets the flow control for the serial port. Options are None or RTS-CTS. The default is None.

**Data Bits:** Sets the data bits for the serial port. Data bit selection is 7 or 8. The default is 8.

**Stop Bits:** Sets the stop bits for the serial port. Options are 1 or 2. The default is 1.

**Parity:** Sets the parity for the serial port. Options are None, Even, or Odd. The default is None.

**Buffer Length:** Sets the length up to which the data from the serial device is buffered before IP transmission. The default length is 32-characters.

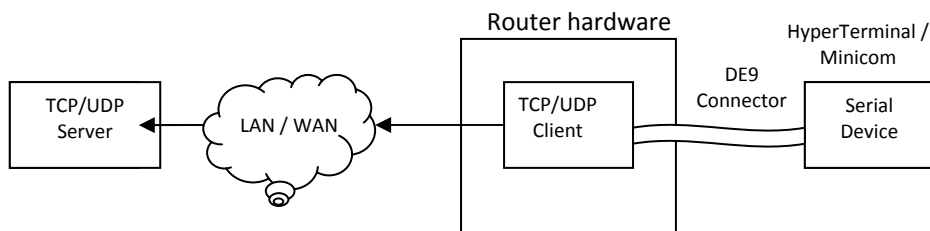
**Timeout:** Sets the timeout value for the serial terminal of how long it waits before IP transmission. The default is 1-second.

**Submit Button:** Click **Submit** to save these settings.

## Serial Port, Client Settings Parameters

The TCP/UDP client feature enables the router to act as a proxy TCP/UDP client to the serial terminal connected to the DE9, RS232 port on the router thus facilitating the serial terminal to access any TCP/UDP server on the LAN/WAN. Once the session, serial terminal to TCP/UDP server, is opened successfully, it allows two-way traffic between the serial device and the remote server.

Initial connection setup for the TCP/UDP client is as follows:



**Serial Port -> Client Settings**

**TCP/UDP - Client Configuration**

Status: ☐ Enable ☒ Disable

Client Type:

Primary Server:  Port:

Secondary Server:  Port:

Connection start By:

Connection Terminate By:

☐ Escape Sequence:

☐ Inactivity timeout:  (Secs)

☒ Others:

**SUBMIT**

### TCP/UDP – Client Configuration Group

Configures TCP/UDP Client through which the serial terminal connected to the RS-232 connector, DE9 on the back of the unit communicates with the remote TCP/UDP server on the LAN/WAN.

**Status:** Sets the client status to either Enable or Disable. The default is Disable.

**Client Type:** Sets the client to either TCP or UDP. The default is TCP.

**Primary Server:** Enter the Primary Server IP address or Hostname. The default is blank.

**Port:** If a Primary Server IP address or hostname is enabled, enter the port number of the server.

**Secondary Server:** Enter the Secondary Server IP address or Hostname. The default is blank.

**Port:** If a Secondary Server IP address or hostname is enabled, enter the port number of the server.

**Connection start By:** Sets the trigger (Carriage Return (CR), DTR Assert, or Always on) in the serial port by which the connection starts. The default is Carriage Return (CR).

**Connection Terminate By:** Sets the connection terminate sequence as follows:

**Escape Sequence:** Set the escape sequence characters at which the connection terminates.

**Inactivity timeout:** Set the inactivity timeout at which the connection terminates.

**Others:** Use to set the other terminating sequences: DTR-toggle or Always-On.

**DTR-toggle:** If DTR status goes low, the connection terminates.

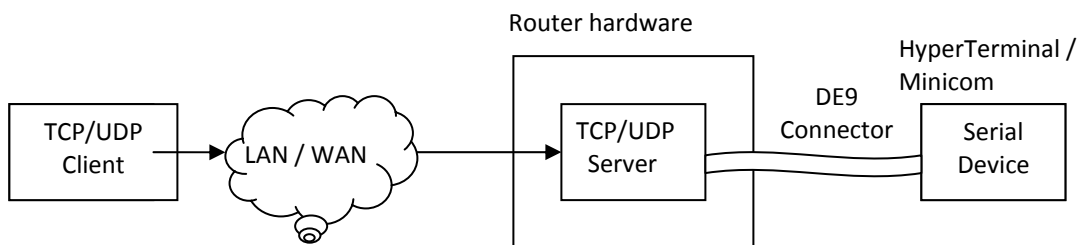
**Always-On:** Sets the terminate sequence as Always-on.

**Submit Button:** Click Submit to save these settings.

## Serial Port, Server Settings Parameters

This feature enables a TCP/UDP client on the Ethernet network to connect to the remote serial terminal connected to the DE9, RS232 port on the router. The router acts as a TCP/UDP server which allows two way traffic between the TCP/UDP client and the remote terminal on the serial port.

The initial connection setup for the TCP/UDP server is shown in the figure that follows.



**Serial Port**

- Serial Port Settings
- Client Settings
- Server Settings

**Serial Port -> Server Settings**

**TCP/UDP - Server Configuration**

**Status** ☐ Enable ☒ Disable

**Server Type** TCP

**Port**

**Connection Terminate By**

☐ Escape Sequence

☒ Inactivity timeout 0 (Secs)

☐ Others DTR-toggle

**SUBMIT**

### TCP/UDP – Server Configuration Group

Configures TCP/UDP Server through which the serial terminal connected to the RS-232 connector, DE9 on the back of the unit listens for the remote TCP/UDP client to communicate on the LAN/WAN.

**Status:** Sets the client status to either Enable or Disable. The default is Disable

**Server Type:** Sets the client to either TCP or UDP. The default is TCP.

**Port:** Sets the server port. The default is None

**Connection Terminate By:** Sets the connection's terminate sequence as follows:

**Escape Sequence:** Set the escape sequence characters at which the connection terminates.

**Inactivity timeout:** Set the inactivity timeout at which the connection terminates.

**Others:** The other terminating sequences are: DTR-toggle or Always-On.

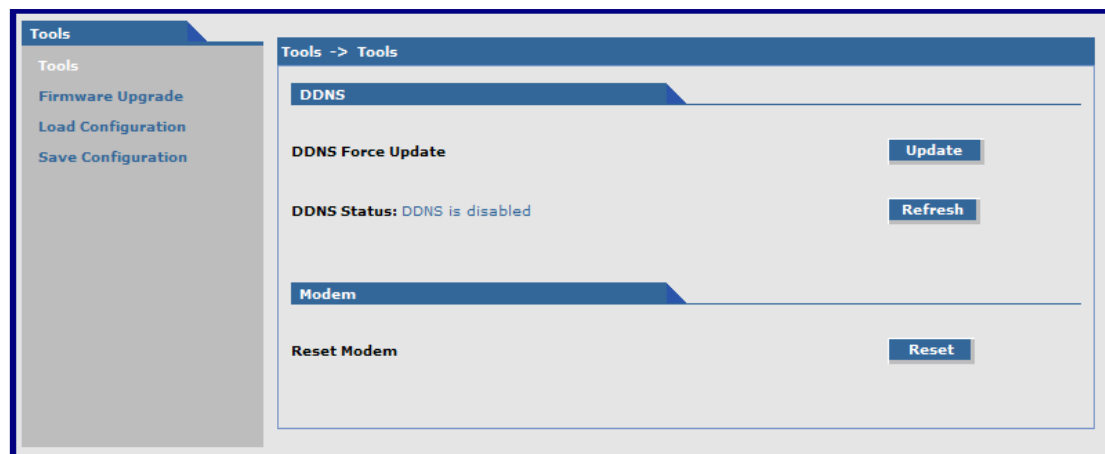
**DTR-toggle:** If DTR status goes low, the connection terminates.

**Always-On:** Sets the terminate sequence as Always-on.

**Submit Button:** Click Submit to save these settings.



## Tools, Tools Parameters



### DDNS Group

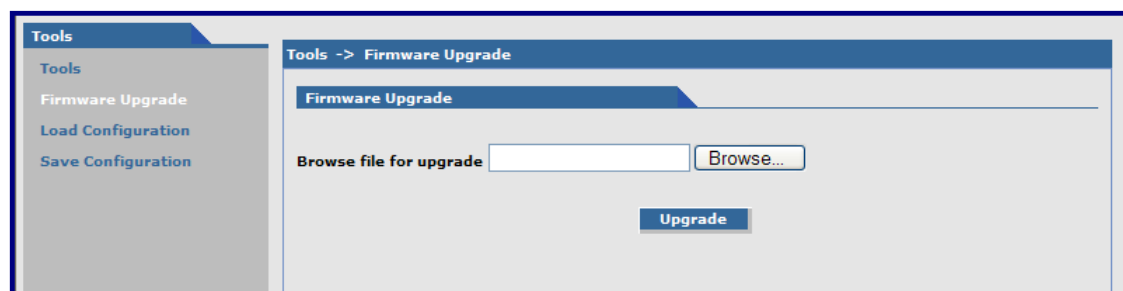
**DDNS Force Update:** Click **Update** to update the DDNS server with your current dynamically assigned IP address.

**DDNS Status:** Click **Refresh** to display the DDNS Status after a forced update.

### Modem Group

**Reset Modem:** Click **Reset** to reset the integrated cellular modem.

## Tools, Firmware Upgrade Parameters



### Firmware Upgrade Group

Use the Firmware Upgrade group to upgrade the firmware for the router. You can find and download all Multi-Tech firmware upgrades from the Multi-Tech Website.

Before you upgrade your firmware, note the following:

- Save your present configuration in case you want to use it again.
- The new firmware is written into flash memory.
- A firmware upgrade takes at least 4 minutes. Do not turn off power during this time because the firmware is being downloaded.
- Do not upgrade the firmware remotely through the Cellular wireless connection.

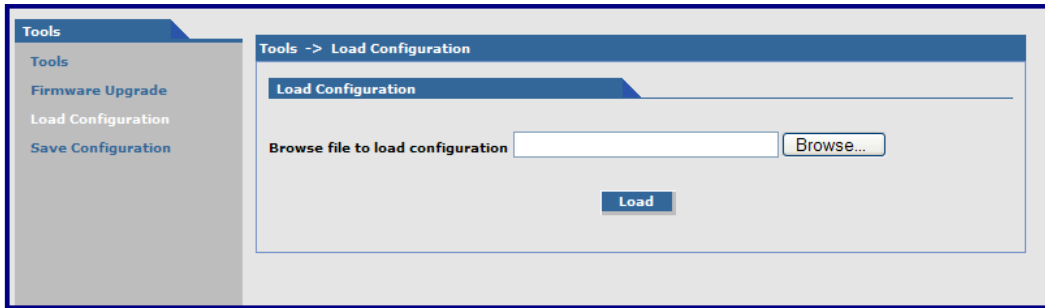
To upgrade firmware:

1. Navigate to the area where you stored the firmware upgrade. To do so, click **Browse**.
2. Select the mtcba-en2-u-xxx.bin file and press **Enter**. The file name displays in the **Browse file for upgrade** field. Make sure you select the correct BIN file; otherwise, your router can become inoperable.
3. Click **Upgrade**.

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

4. After the firmware upgrade is complete, verify the configuration is as expected.
  - In particular, check that the DHCP scope settings are set properly.
  - Also, up to four IPSEC tunnels can be active at any given time. You can save more than four active tunnels, but they are not active.

## Tools, Load Configuration Parameters



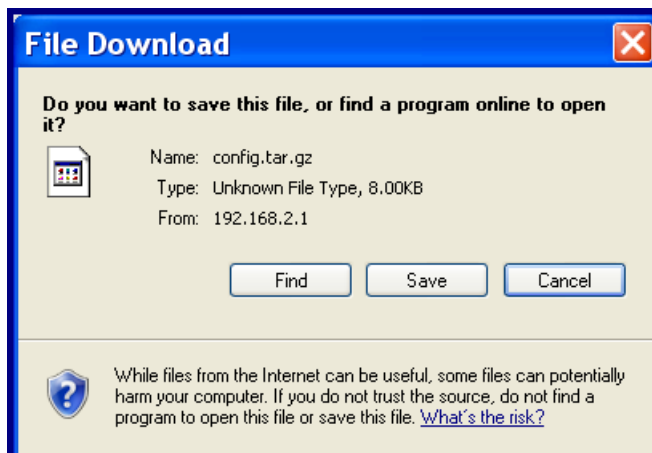
### Load Configuration Group

**Browse File for Load Configuration:** Click **Browse** 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 field. Then click **Load**.

#### Notes:

- The new configuration is written into the flash.
- A Configuration Upgrade takes at least 3 seconds to download and 60 seconds to install the settings and reboot. Reboot happens automatically.

When you click **Load**, the following dialog box opens. It shows the name of the file you selected.



Click the **Find**, **Save**, or **Cancel** buttons as desired.

## Tools, Save Configuration

Click this option to save the configuration.

# Statistics & Logs

## Statistics & Logs > System Information

This is an example of the Statistics & Logs System Information.

Statistics & Logs

System Information

Ethernet

PPP

PPP Trace

DHCP Statistics

GRE Statistics

Modem Information

Service Status

TCP/UDP Client Live Log

TCP/UDP Server Live Log

IPSec Live Log

IPSec Log Traces

Statistics & Logs -> System Information

Firmware Information:

Release : v2.00 - Beta 1 Release

Date : 17-Jul-2009

System Uptime:

00:40:37 up 40 min, load average: 0.09, 0.17, 0.16

Memory Utilization:

	total	used	free	shared	buffers
Mem:	61900	13600	48300	0	0
Swap:	0	0	0		
Total:	61900	13600	48300		

Model Number:

MTCBA-H-EN2

Mac-Address:

00:D0:A0:01:0D:E3

## Statistics & Logs > Ethernet

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

Statistics & Logs -> Ethernet	
Ethernet Statistics	
MTU	1500 bytes
Rx Bytes	138343 bytes
Rx Packets	1429
Rx Errors	0
Rx dropped	0
Rx Overruns	0
Rx Frame	0
Rx Compressed	0
Tx Bytes	696194 bytes
Tx Packets	3005
Tx Errors	0
Tx dropped	0
Tx Overruns	0
Tx Carrier	0
Tx Collisions	0
Tx Compressed	0
Tx Queue Length	1000

## Statistics & Logs > PPP

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

Statistics & Logs -> PPP	
ppp0 statistics	
PPP Link	UP (dialed)
PPP Local ip	200.54.120.253
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

## Statistics & Logs > PPP Trace

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

Statistics & Logs -> PPP Trace

PPP Trace

```
Physical Link Establishment
Sent: AT^M
Rcvd: AT^M^M
Rcvd: OK
Sent: at+cgdcont=1,"IP","internet3.voicestream.com"^M
Rcvd: ^M
Rcvd: at+cgdcont=1,"IP","internet3.voicestream.com"^M^M
Rcvd: OK
Sent: ATDT*99***1#^M
Rcvd: ^M
Rcvd: ATDT*99***1#^M^M
Rcvd: CONNECT
Sent: ^M
Physical link established
LCP: Sent Configure Ack
LCP: Rcvd Configure Reject
LCP: Rcvd Configure Ack
LCP: LAYER IS UP
PAP: Authentication Success
IPCP: Sent Configure ACK
IPCP: Rcvd Configure Nak
IPCP: Rcvd Configure Ack
IPCP: LAYER IS UP
PPP Established
```

## Statistics & Logs > DHCP Statistics

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

Statistics & Logs -> DHCP Statistics

DHCP Statistics

Mac Address	IP Address
00:e0:4c:b6:59:14	192.168.2.100

## Statistics & Logs > GRE Statistics

This page displays the statistics of active tunnels.

Statistics & Logs -> GRE Statistics

Tunnel	Local	Remote	Tx	Rx
--------	-------	--------	----	----

## Statistics & Logs > Modem Information

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

Statistics & Logs -> Modem Information

Modem AT Commands Trace

```

ATE0
ATE0^M
OK

```

## Statistics & Logs > Service Status

This page displays the summary of the service status.

Statistics & Logs -> Service Status

Service Name	Configuration	Status
DDNS	disable	DDNS is disabled
SNTP	disable	SNTP is disabled
TCP/ICMP Keep Alive	disable	PING Keep alive is disabled
Dial-on-Demand	disable	PPP is not running

## Statistics & Logs > TCP/UDP Client Live Log

This page displays the TCP/UDP Client Live Log.

Statistics & Logs -> TCP/UDP Client Live Log

Client Trace

```

13:36:4: Start trigger is Carriage return. Waiting for 3 CRs
13:36:16: Got 3 CR's
13:36:16: connected to primary server address
13:36:17: DCD turned ON

```

## Statistics & Logs > TCP/UDP Server Live Log

This page displays the TCP/UDP Server Live Log.

Statistics & Logs -> TCP/UDP Server Live Log

Server Trace

```

10:31:8: Server is listening
13:16:19: Server is connected to client
13:16:19: DCD turned ON

```



## Statistics & Logs > IPsec Live Log

This page displays the IPsec Live Log.

Statistics & Logs -> IPsec Live Log				
IPsec Live Connections				
Connection Name	Start Time	Local Gateway	Remote Gateway	Remote Subnet
RF830APVPN	17-Aug-2009 13hr-38min-38sec	166.213.212.34	65.126.90.108	192.168.22.0
RF850VPN	17-Aug-2009 13hr-38min-24sec	166.213.212.34	65.126.90.107	192.168.131.0
IPsec Statistics				
Connection Name	Received Packets	Transmitted Packets	Received Bytes	Transmitted Bytes
RF830APVPN	4	4	240	480
RF850VPN	4	4	240	480

## Statistics & Logs > IPsec Log Traces

This page displays the IPsec Log Traces.

Statistics & Logs -> IPsec Log Traces	
Ipsec Log Trace	
Aug 17 13:37:44	WirelessRTR user.info hstr-ipsec: pluto was unable to start
Aug 17 13:37:44	WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --down RF850VPN
Aug 17 13:37:44	WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --delete RF850VPN
Aug 17 13:37:44	WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --down RF830APVPN
Aug 17 13:37:45	WirelessRTR user.info ipsec_stop: /sbin/ipsec auto --delete RF830APVPN

# Appendix A – Commonly Supported Subnets

This table lists commonly supported subnets organized by address.

	Network Number	Hosts Available	Broadcast Address
255.255.255.128	N.N.N.0	N.N.N.1-126	N.N.N.127
/25	N.N.N.128	N.N.N.129-254	N.N.N.255
	Network Number	Hosts Available	Broadcast Address
255.255.255.192	N.N.N.0	N.N.N.1-62	N.N.N.63
/26	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	N.N.N.0	N.N.N.1-30	N.N.N.31
/27	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	N.N.N.0	N.N.N.1-14	N.N.N.15
/28	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

	<b>Network Number</b>	<b>Hosts Available</b>	<b>Broadcast Address</b>
255.255.255.248	N.N.N.0	N.N.N.1-6	N.N.N.7
/29	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
	<b>Network Number</b>	<b>Hosts Available</b>	<b>Broadcast Address</b>
	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 – Regulatory Compliance



### EMC, Safety, and R&TTE Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

Council Directive 2004/108/EC of 15 December 2004 on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 2006/95/EC of 12 December 2006 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

and

Council Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

### FCC Part 15 Class A Statement

This equipment has been tested and found to comply with the limits for a **Class A** digital device, pursuant to 47 CFR Part 15 regulations. The stated limits in this regulation are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Plug the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the CFR 47 rules. Operation of this device is subject to the following conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference that may cause undesired operation.

**Warning:** Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement Canadien sur le matériel brouilleur.

# Appendix C – Environmental Information

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.



## REACH Statement

### Registration of Substances:

After careful review of the legislation and specifically the definition of an "article" as defined in EC Regulation 1907/2006, Title II, Chapter 1, Article 7.1(a)(b), it is our current view Multi-Tech Systems, Inc. products would be considered as "articles". In light of the definition in § 7.1(b) which requires registration of an article only if it contains a regulated substance that "is intended to be released under normal or reasonable foreseeable conditions of use," our analysis is that Multi-Tech Systems, Inc. products constitute nonregisterable articles for their intended and anticipated use.

### Substances of Very High Concern (SVHC):

Per the candidate list of Substances of Very high Concern (SVHC) published October 28, 2008 we have reviewed these substances and certify the Multi-Tech Systems, Inc. products are compliant per the EU "REACH" requirements of less than 0.1% (w/w) for each substance.

If new SVHC candidates are published by the European Chemicals Agency, and relevant substances have been confirmed, that exceeds greater than 0.1% (w/w), Multi-Tech Systems, Inc. will provide updated compliance status.

Multi-Tech Systems, Inc. also declares it has been duly diligent in ensuring that the products supplied are compliant through a formalized process which includes collection and validation of materials declarations and selective materials analysis where appropriate. This data is controlled as a part of a formal quality system and will be made available upon request.

## Restriction of the Use of Hazardous Substances (RoHS)



**Multi-Tech Systems, Inc.**

### **Certificate of Compliance**

#### **2002/95/EC**

Multi-Tech Systems, Inc. confirms that this product now complies with the chemical concentration limitations set forth in the directive **2002/95/EC** of the European Parliament (Restriction Of the use of certain Hazardous Substances in electrical and electronic equipment - **RoHS**)

These Multi-Tech Systems, Inc. products do not contain the following banned chemicals:

Lead, [Pb] < 1000 PPM

Mercury, [Hg] < 1000 PPM

Hexavalent Chromium, [Cr+6] < 1000 PPM

Cadmium, [Cd] < 100 PPM

Polybrominated Biphenyl, [PBB] < 1000 PPM

Polybrominated Diphenyl Ether, [PBDE] < 1000 PPM

#### **Notes:**

1. Lead usage in some components is exempted by the following RoHS annex; therefore, higher lead concentration could be found.
  - a. Lead in high melting temperature type solders (i.e., tin-lead solder alloys containing more than 85% lead).
  - b. Lead in electronic ceramic parts (e.g., piezoelectronic devices).



## China ROHS

### 依照中国标准的有毒有害物质信息

根据中华人民共和国信息产业部 (MII) 制定的电子信息产品 (EIP) 标准 - 中华人民共和国《电子信息产品污染控制管理办法》(第 39 号), 也称作中国

RoHS, 下表列出了 Multi-Tech Systems Inc. 产品中可能含有的有毒物质 (TS) 或有害物质 (HS) 的名称及含量水平方面的信息。

成分名称	有害/有毒物质/元素					
	铅 (PB)	汞 (Hg)	镉 (CD)	六价铬 (CR6+)	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
印刷电路板	O	O	O	O	O	O
电阻器	X	O	O	O	O	O
电容器	X	O	O	O	O	O
铁氧体磁环	O	O	O	O	O	O
继电器/光学部件	O	O	O	O	O	O
IC	O	O	O	O	O	O
二极管/晶体管	O	O	O	O	O	O
振荡器和晶振	X	O	O	O	O	O
调节器	O	O	O	O	O	O
电压传感器	O	O	O	O	O	O
变压器	O	O	O	O	O	O
扬声器	O	O	O	O	O	O
连接器	O	O	O	O	O	O
LED	O	O	O	O	O	O
螺丝、螺母以及其它五金件	X	O	O	O	O	O
交流-直流电源	O	O	O	O	O	O
软件/文档 CD	O	O	O	O	O	O
手册和纸页	O	O	O	O	O	O
底盘	O	O	O	O	O	O

**X** 表示所有使用类似材料的设备中有害/有毒物质的含量水平高于 SJ/Txxx-2006 限量要求。

**O** 表示不含该物质或者该物质的含量水平在上述限量要求

# Index

## A

Access Point Name .....	24
AH Key .....	67
Authentication Algorithms .....	67
Auto Dialout configuration .....	30
Autodiscovery configuration.....	30

## B

Broadcast timer .....	30
Browse File for Upgrade in Tools.....	74
Browse File to Load Configuration.....	75

## C

Caller ID for Wakeup on Call .....	46
Canadian Regulations.....	86
CDMA Antenna Specifications.....	16
CDMA RF Specifications .....	16
Circuit Switched Data .....	14
Configure Ethernet interface .....	23

## D

Daylight Savings Time configuration .....	36
DDNS Client.....	33
DDNS configuration .....	33
DDNS Status in Tools.....	73
DHCP configuration.....	61
DHCP fixed addresses.....	62
DHCP Lease Time .....	61
DHCP server .....	61
Dial-on-Demand.....	42
DNAT configuration .....	56
DNAT example .....	56
Dynamic DNS configuration.....	33

## E

EMC, Safety, and R&TTE Directive Compliance .....	86
Ethernet ports caution .....	9

## F

Firmware Upgrade .....	74
------------------------	----

## G

General Configuration – IP Setup .....	30
GPS Antenna Specifications .....	17
GPS RF Specifications .....	17
GRE route configuration .....	60

GRE routing.....	58
GRE tunnel configuration.....	59
GRE tunneling .....	58
GSM RF Specifications .....	16

## H

H323 packets connection tracking .....	58
Handling Precautions.....	9
HTTP authentication.....	32
HTTP configuration .....	32

## I

ICMP configuration.....	58
ICMP Keep Alive Check .....	42
IP Configuration .....	30
IP Server .....	33
ITCP .....	54

## L

Load Configuration.....	75
-------------------------	----

## M

Menu structure.....	26
Modem Information.....	82

## N

NAT configuration .....	41
Navigating .....	26
Network configuration.....	52
Network/Host for Remote Configuration .....	37

## P

Packet Filter.....	54
Packet filter rules .....	54
Perfect Forward Secrecy.....	65
Pin Functions .....	18
Polling time .....	35
Power Requirements.....	15
Power-On Configuration .....	50
PPP authentication.....	42
PPP configuration .....	42
PPTP connection tracking.....	58
protocol.....	54

## R

Raw Dialout configuration .....	30
Remote Configuration .....	37

---

Reset Modem in Tools .....	73
Route configuration.....	36

**S**

Safe password .....	32
Save configuration in Tools .....	75
Select encryption method.....	67
Server Port.....	30
Service Configuration .....	53
SNTP configuration .....	35
Static Routes configuration .....	36
Statistics & Logs > DHCP Statistics .....	79
Statistics & Logs > Ethernet.....	77
Statistics & Logs > Modem Information.....	80
Statistics & Logs > PPP .....	78
Submenus .....	28
Subnets .....	82
Syslog configuration .....	30
System domain name .....	33

**T**

Technical Specifications.....	14
Temperatures .....	14
Time zone configuration.....	35
Tools .....	73

**U**

UDP .....	54
-----------	----

**V**

Vehicle Safety .....	9
----------------------	---

**W**

Wakeup on Call .....	44
Wakeup on Call Examples.....	46, 48, 49
Wizard Setup .....	23, 24