



MultiConnect® rCell 100

MTR-LTE User Guide

MultiConnect[®] rCell 100 Series Router User Guide

Product: MTR-LTE Models: MTR-LAT1-B07, MTR-LAT1-B08, MTR-LVW2-B07, MTR-LVW2-B08, MTR-LEU1-B07, MTR-LEU1-B08

Part Number: S000626 Version: 1.0

Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2015 by Multi-Tech Systems, Inc.**

Multi-Tech Systems, Inc. makes no representations or warranties, whether express, implied or by estoppels, with respect to the content, information, material and recommendations herein and specifically disclaims any implied warranties of merchantability, fitness for any particular purpose and non-infringement.

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.

Legal Notices

The MultiTech products are not designed, manufactured or intended for use, and should not be used, or sold or re-sold for use, in connection with applications requiring fail-safe performance or in applications where the failure of the products would reasonably be expected to result in personal injury or death, significant property damage, or serious physical or environmental damage. Examples of such use include life support machines or other life preserving medical devices or systems, air traffic control or aircraft navigation or communications systems, control equipment for nuclear facilities, or missile, nuclear, biological or chemical weapons or other military applications ("Restricted Applications"). Use of the products in such Restricted Applications is at the user's sole risk and liability.

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A CELLULAR COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY CELLULAR COMMUNICATIONS NETWORK. MULTITECH WILL HAVE NO LIABILITY FOR ANY LOSSES, DAMAGES, OBLIGATIONS, PENALTIES, DEFICIENCIES, LIABILITIES, COSTS OR EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES) RELATED TO TEMPORARY INABILITY TO ACCESS A CELLULAR COMMUNICATIONS NETWORK USING THE PRODUCTS.

Contacting MultiTech

Knowledge Base

The Knowledge Base provides immediate access to support information and resolutions for all MultiTech products. Visit <http://www.multitech.com/kb.go>.

Support Portal

To create an account and submit a support case directly to our technical support team, visit: <https://support.multitech.com>.

Support

Business Hours: M-F, 8am to 5pm CT

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

Warranty

To read the warranty statement for your product, visit www.multitech.com/warranty.go. For other warranty options, visit www.multitech.com/es.go.

World Headquarters

Multi-Tech Systems, Inc.
 2205 Woodale Drive, Mounds View, MN 55112
 Phone: (800) 328-9717 or (763) 785-3500
 Fax (763) 785-9874

Contents

MultiConnect® rCell 100 Series Router User Guide	2
Chapter 1 Product Overview	7
About MultiConnect rCell 100 Series Router	7
Documentation	7
Product Build Options	8
Package Contents	9
Descriptions of LEDs.....	10
Ethernet LED Descriptions	10
Side Panel Connectors	11
Chapter 2 LTE Specifications	12
Dimensions.....	12
Specifications	12
Power Draw.....	14
Regulatory Information Labels.....	15
RF Specifications LTE.....	16
Chapter 3 Safety Warnings.....	17
Lithium Battery	17
ITE Equipment Ordinary Locations (US, Canada, and Europe)	17
Radio Frequency (RF) Safety	17
Interference with Pacemakers and Other Medical Devices	17
Potential interference	17
Precautions for pacemaker wearers	18
Notice regarding Compliance with FCC and Industry Canada Requirements for RF Exposure	18
Chapter 4 Antenna Information	19
Antenna System Cellular Devices.....	19
LTE Antenna Used With MTR-LAT1 and MTR-LVW2 Models	19
LTE Antenna Specifications	19
LTE Antenna Used With MTR-LEU1 Models	20
LTE Antenna Specifications	20
GPS Antenna Specifications	20
Chapter 5 Installing the Router	22
Installing the Router.....	22
Mounting the Device.....	22
Installing the SIM Card	22
Resetting the Device	23
Restoring User Defined Settings to the Device	23

Chapter 6 Using the Wizard to Configure Your Device.....	25
Setting Up Your Device	25
Chapter 7 Configuring Your Device.....	27
Home Page (Dashboard)	27
WAN Setup.....	28
Editing Failover Configuration.....	28
Failover Configuration Fields	28
Unavailable Services in PPP-IP Passthrough Mode.....	29
Configuring IP Address and DNS Information for LAN	29
Configuring Dynamic Domain Naming System (DDNS)	29
Entering authentication information	30
Forcing a DDNS server update	30
Configuring Dynamic Host Configuration Protocol (DHCP) Server	30
Assigning Fixed Addresses	30
Configuring the Global Positioning System (GPS).....	31
Dumping NMEA Sentence Information to the Router's TCP Server Port	31
Sending GPS information to a remote server	31
Configuring NMEA Sentences	32
SMTP Settings	32
Configuring the serial port	32
Configuring Device to Act as Client	33
Configuring Device to Act as Server.....	34
Time Configuration	34
Setting the Date and Time	34
Configuring SNTP to Update Date and Time	35
Adding Saved Networks	35
Adding Networks.....	35
Editing or Deleting an Existing Network	35
Unavailable Services in PPP-IP Passthrough Mode.....	35
Chapter 8 Setting Up Cellular Features.....	36
Configuring Cellular.....	36
Cellular Configuration Fields	36
Unavailable Services in PPP-IP Passthrough Mode.....	38
Configuring Wake Up On Call.....	38
Wake Up On Call Settings	38
Wake Up On Call General Configurations.....	38
Using Telnet to Communicate with the Cellular Radio.....	39
Radio Status	40
Chapter 9 Setting Up the Firewall	41
Defining firewall rules	41
Adding Forwarding Rules	41

Adding Outbound Traffic Rules	41
Advanced Settings.....	42
Setting up Static Routes	42
Chapter 10 Configuring SMS	43
Configuring SMS.....	43
Sending an SMS Message.....	43
Viewing Received SMS Messages	43
Viewing Sent SMS Messages.....	43
Chapter 11 Defining Tunnels	45
Setting Up GRE Tunnels	45
Configuring Network-to-Network Virtual Private Networks (VPNs)	45
IPsec Tunnel Configuration Field Descriptions	46
Unavailable Services in PPP-IP Passthrough Mode.....	47
Chapter 12 Device Administration	48
Configuring Device Access	48
HTTP Redirect to HTTPS	48
HTTPS	48
SSH	48
ICMP	49
Configuring IP Defense	49
Denial of Service (DOS) Prevention.....	49
Ping limit	49
Brute force	50
Unavailable Services in PPP-IP Passthrough Mode.....	50
Generating a New Certificate.....	50
Uploading a New Certificate	51
Setting up the Remote Management	51
Managing Your Device Remotely	51
Unavailable Services in PPP-IP Passthrough Mode.....	52
Customizing the User Interface	52
Customizing Support Information	52
Specifying Device Settings	53
Upgrading Firmware	53
Saving and Restoring Settings	54
Using the Router's Debugging Options.....	55
Automatically rebooting the device.....	55
Setting up Telnet.....	55
Configuring Syslog.....	56
Statistics Settings	56
Ping and Reset Options.....	56

Chapter 13 Status and Logs	57
Viewing Device Statistics	57
Service Statistics.....	58
Statistics Configuration Fields	58
Mail Log.....	58
Mail Queue.....	58
Appendix: Regulatory Information	60
47 CFR Part 15 Regulation Class B Devices	60
Industry Canada Class B Notice.....	60
FCC Interference Notice	60
Requirements for Cellular Antennas with regard to FCC/IC Compliance	61
EMC, Safety, and R&TTE Directive Compliance	61
Restriction of the Use of Hazardous Substances (RoHS)	62
REACH Statement	63
Registration of Substances.....	63
Substances of Very High Concern (SVHC)	63
Waste Electrical and Electronic Equipment Statement	63
WEEE Directive.....	63
Instructions for Disposal of WEEE by Users in the European Union	63
Information on HS/TS Substances According to Chinese Standards	64
Information on HS/TS Substances According to Chinese Standards (in Chinese)	65

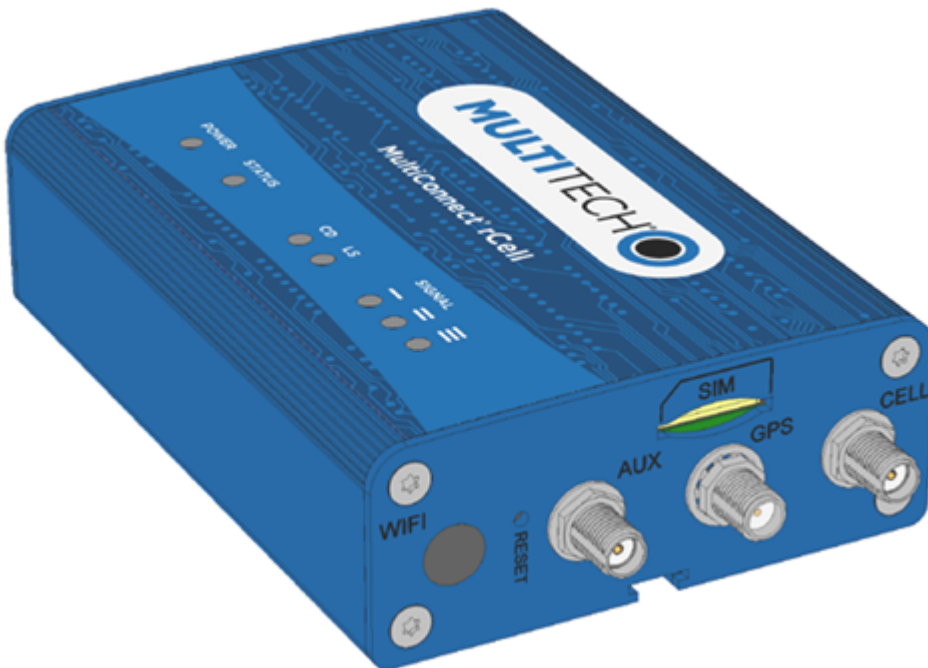
Chapter 1 Product Overview

About MultiConnect rCell 100 Series Router

This guide describes the MultiConnect rCell 100 Series Router. Use the rCell family of routers to provide secure data communication between many types of devices that use legacy and the latest communication technologies. Some device models support:

- GPS capability

The router has an integrated cellular modem and includes 10/100 BaseT Ethernet and RS-232 serial connectivity. An image of the device follows:



Documentation

The following documentation is available at <http://www.multitech.com/brands/multiconnect-rcell-100-series>.

Document	Description	Part Number
MultiConnect rCell100 Series Router (MTR-LTE) User Guide	This document provides overview, safety and regulatory information, design considerations, schematics, and device information.	S000626
Getting Started with AT Commands for LEU1 Devices	AT Command release notes and basic operations for LEU1 and LEU1-U Devices.	S000615
Getting Started with AT Commands for LAT1 Devices	AT Command release notes and basic operations for LAT1 and LAT1-U Devices.	S000617
Getting Started with AT Commands for LVW2 Devices	AT Command release notes and basic operations for LVW2 and LVW2-U Devices.	S000618


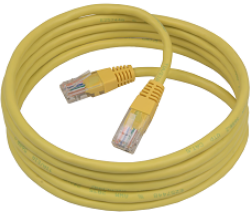




Document	Description	Part Number
Telit LE910 AT Commands Reference Guide	Lists AT Commands and parameters used to configure your device. (Applies to LAT1 and LEU1 devices, not LVW2)	80421ST10585A Rev 3

Product Build Options

Product	Description	Carrier/Region
MTR-LAT1-B07	LTE router - cellular data only	AT&T/North America
MTR-LAT1-B08	LTE router - cellular data and GPS	AT&T/North America
MTR-LVW2-B07	LTE router - cellular data only	Verizon/North America
MTR-LVW2-B08	LTE router - cellular data and GPS	Verizon/North America
MTR-LEU1-B07	LTE router - cellular data only	Europe/Australia
MTR-LEU1-B08	LTE router - cellular data and GPS	Europe/Australia

Package Contents

Your MTR-LTE package includes the following:

Contents	Description
	1 - Power Supply with Removable Blades
	1 - Ethernet Cable RJ45 6-ft.
	2 - Cellular Antennas
	1 - GPS Antenna (B08 models only)
Customer Notices	Legal and Support Information
	Extended Services
	1 - Mounting Tab and Bracket
	4 - Rubber Feet

Note: The above information does not apply to the Router Only option.

Descriptions of LEDs

The top panel contains the following LEDs:

- **Power and Status LEDs**—The Power LED indicates that DC power is present and the Status LED blinks when the unit is functioning normally.
- **Modem LEDs**—Two modem LEDs indicate carrier detection and link status.
- **Signal LEDs**—Three signal LEDs display the signal strength level of the wireless connection.
- **Ethernet LEDs**—These LEDs are not on the top panel. See the section Ethernet LED Descriptions for descriptions of these LEDs.

LED Indicators	
POWER	Indicates presence of DC power when lit.
STATUS	The LED is a solid light when the device is booting up, saving the configuration, restarting, or updating the firmware. When the Status LED begins to blink, the router is ready for use.
CD	Carrier Detect. When lit, indicates data connection has been established.
LS	Link Status (for LVW2 only, not LAT1 and LEU1) OFF — No power to the cellular radio Continuously Lit — Not registered Slow Blink (-0.2Hz) — Registered or connected
SIGNAL	Signal strength for cellular (RSSI range: 0 - 31) ALL OFF — Unit is off, not registered on network, or extremely weak signal ($0 \leq \text{RSSI} < 6$). 1 Bar "ON" — Very weak signal ($7 \leq \text{RSSI} < 14$). 1 Bar and 2 Bar "ON" — Weak signal ($15 \leq \text{RSSI} < 23$). 1 Bar, 2 Bar, and 3 Bar "ON" — Good signal ($24 \leq \text{RSSI} \leq 31$).

Ethernet LED Descriptions

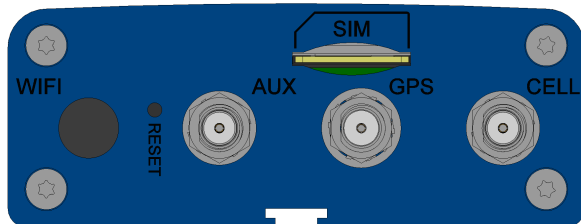
Two Ethernet LEDs are physically on the RJ-45 connector(s). The table that follows describes these LEDs.

Ethernet Link	Right LED on Ethernet connector. Blinks when there is transmit and receive activity on the Ethernet link. It shows a steady light when there is a valid Ethernet connection.
Ethernet Speed	Left LED on Ethernet connector. Lit when the Ethernet is linked at 100 Mbps. If it is not lit, the Ethernet is linked at 10 Mbps.

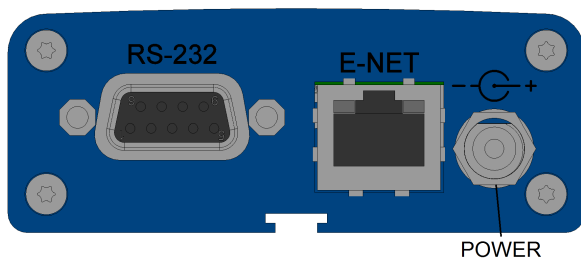
Side Panel Connectors

The device has connectors on both sides of the housing. The right side of the device contains a SIM card holder, a reset button, a GPS antenna connector, and a cellular-auxiliary antenna connector pair. Depending on the model of your device, the GPS antenna connector may or may not be present.


The following shows the right side panel of the device:



The following shows the left side panel of the device. It includes an RS-232 connector, an Ethernet connector, and the power receptacle.

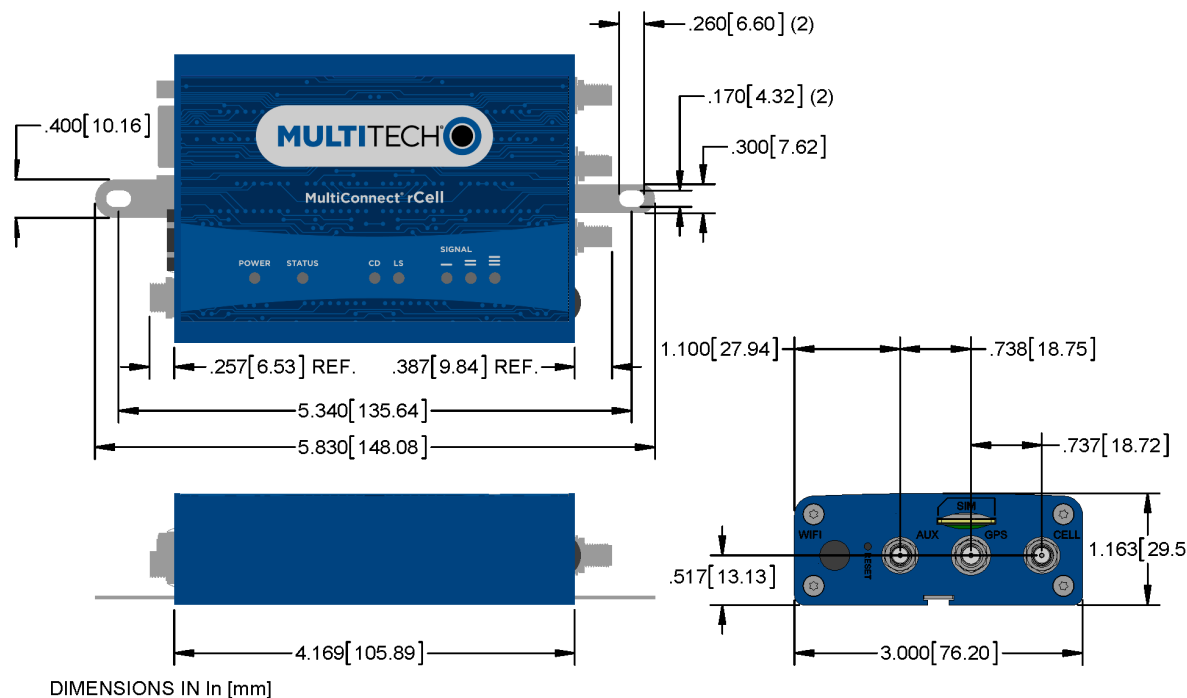


The following table describes the items on the two side panels:

Label	Description
CELL, AUX	Cellular antenna inputs. Use with the 2 Laird LTE DBA6927C1-FSMAM antennas or (for the LEU1 only) with the 2 Wison Technologies LTE GY115HT467-017 supplied with the device if ordered as a bundle. ■ CELL - Primary. AUX - Diversity.
GPS	GPS antenna input. Use with the Trimble GPS antenna 66800-52 supplied with the device when ordered as a bundle. Used only on the B08 models.
SIM	Receptacle for a SIM card (Subscriber Identity Module).
RESET	Resets the device. Refer to Resetting the Device or Resetting User Defined Settings to the Device.
RS-232	DCE 9-pin, female-D Sub through-hole connector.
E-NET	RJ-45 receptacle for standard Ethernet 10/100 Base-T (RJ-45 connector has two Ethernet LEDs).
Power 	7-32 VDC power receptacle for provided power cord. The device uses a minimum 7V 1.0A power supply.

Chapter 2 LTE Specifications

Dimensions



Specifications

Category	MTR-LAT1 (North America AT&T, T-Mobile)	MTR-LVW2 (North America Verizon)	MTR-LEU1 (EU Carriers)
General			
Performance	LTE Cat. 3GPP Release 9		
Frequency Bands (MHz)	4G LTE: 700 (B17) / 850 (B5) / AWS1700 (B4) /1900 (B2)	4G LTE: Single-mode: 700 (B13) / AWS1700 (B4)	4G: LTE: 800 (B20) / 1800 (B3) /2600 (B7)
	3G UMTS HSPA+:850 (B5) / 1900(B2)		3G UMTS HSPA+:850 (B5) / 900 (B8) / 2100 (B1)
	2G: GSM GPRS EDGE: 850/1900		2G GSM GPRS EDGE: 900/1800
Cellular radio module	Telit LE910-NAG	Telit LE910-SVG	Telit LE910-EUG
GPS radio module	SKYTRAQ Venus638LP (for B08 models only)		

Category	MTR-LAT1 (North America AT&T, T-Mobile)	MTR-LVW2 (North America Verizon)	MTR-LEU1 (EU Carriers)
Cellular packet data	Up to 100 Mbps downlink (Theoretical maximum - actual performance may be affected by multiple environmental factors.)		
	Up to 50 Mbps uplink (See above note.)		
Diversity/MIMO	Rx Diversity and MIMO DL 2x2		
SMS	Point-to-Point messaging, Mobile terminated SMS, Mobile originated SMS		
Connectors			
Cellular	Female SMA connector		
GPS	Female SMA connector		
SIM Holder	Mini-SIM standard 1.8 V and 3 V	N/A	Mini-SIM standard 1.8 V and 3 V
eNet (LAN)	RJ-45, 10/100 Base T		
GPS	Female SMA connector		
RS-232	DCE 9-pin, female connector		
Power	25 mm miniature locking power jack (screw on)		
Power Requirements¹			
Voltage	7 V to 32 V DC		
Physical Description			
Dimensions	4.17" x 3.0" x 1.15" (10.6cm x 7.6cm x 2.9cm)		
Weight	0.51 lbs (0.231 Kg)		
Chassis type	Aluminum		
Environment			
Operating Temperature ²	-40° C to +80° C		
Storage Temperature ²	-40° C to +85° C		
Humidity	Relative humidity 15% to 93% non-condensing		
Certifications, Compliance, Warranty			
Regulatory	FCC Class B (U.S.), IC (Canada)	FCC Class B (U.S.)	CE Mark, R&TTE (EU)
Safety	UL60950-1, UL 201, cUL60950-1	UL60950-1, UL 201	IEC60950-1(EU)
Network	PTCRB, AT&T, T-Mobile	Verizon (pending)	Telstra, EU carriers
Quality	Designed and built-in ISO 9001/13485 facilities		
	MIL-STD-810: High Temp, Low Temp, Cold Dwell, Random, and Sine vibration		
	SAE J1455: Random and Sine vibration		

¹Optional power supply must be a Listed ITE power supply marked LPS or Class 2 rated 1.0 A minimum. Certification does not apply or extend to voltages outside certified range, and has not been evaluated by UL for operating voltages beyond tested range.

²UL Recognized @ 40° C, Limited by AC power supply. UL Recognized @ 60° C when used with the fused DC power cable, part number FPC-532-DC.

Installation in outdoor locations has not been evaluated by UL. UL Certification does not apply or extend to outdoor applications.

Note: Radio performance may be affected at the temperature extremes. This is considered normal. There is no single cause for this function. Rather, it is the result of an interaction of several factors, such as the ambient temperature, the operating mode, and the transmit power.

Power Draw

MTR-LAT1-B08 Power Draw

Radio Protocol	Sleep Mode Current (If Applicable) (Amps)	Cellular Call Box Connection No Data (Amps)	Average Measured Current (Amps) at Maximum Power	TX Pulse (Avg) Amplitude Current (Amps)) for GSM850 or Peak Current for HSDPA/LTE	Total Inrush Charge Measured in Millicoulombs (mC)
9.0 Volts					
GSM 850Mhz	NA	0.185	0.329	0.900	1.53
LTE	NA	0.193	0.488	NA	1.53
20.0 Volts					
GSM 850Mhz	NA	0.094	0.160	0.455	.721
LTE	NA	0.100	0.232	NA	.721
32.0 Volts					
GSM 850Mhz	NA	0.062	0.103	0.370	1.91
LTE	NA	0.065	0.154	NA	1.91

MTR-LEU1-B08 Power Draw

Radio Protocol	Sleep Mode Current (If Applicable) (Amps)	Cellular Call Box Connection No Data (Amps)	Average Measured Current (Amps) at Maximum Power	TX Pulse (Avg) Amplitude Current (Amps)) for GSM850 or Peak Current for HSDPA/LTE	Total Inrush Charge Measured in Millicoulombs (mC)
9.0 Volts					
EGSM 900Mhz	NA	0.185	0.305	1.05	0.118
LTE	NA	0.181	0.487	0.580	0.118

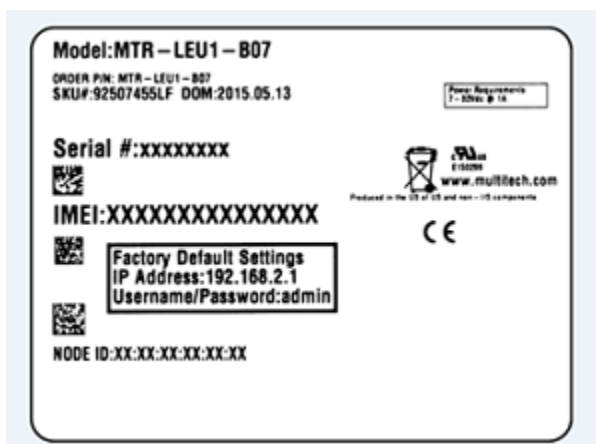
Radio Protocol	Sleep Mode Current (If Applicable) (Amps)	Cellular Call Box Connection No Data (Amps)	Average Measured Current (Amps) at Maximum Power	TX Pulse (Avg) Amplitude Current (Amps)) for GSM850 or Peak Current for HSDPA/LTE	Total Inrush Charge Measured in Millicoulombs (mC)
20.0 Volts					
EGSM 900Mhz	NA	0.095	0.149	0.505	0.106
LTE	NA	0.101	0.236	0.316	0.106
32.0 Volts					
EGSM 900Mhz	NA	0.063	0.097	0.300	0.281
LTE	NA	0.069	0.153	0.228	0.281

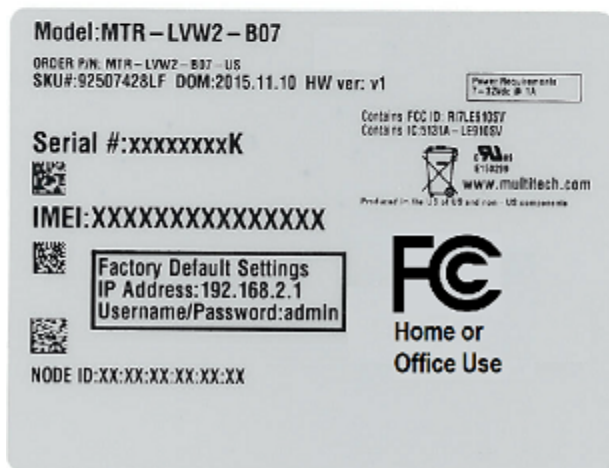
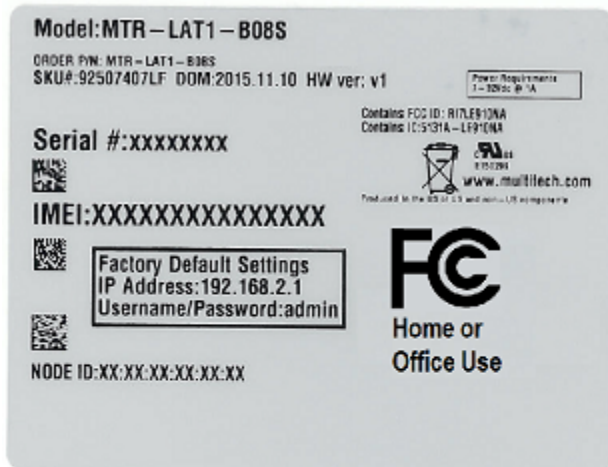
MTR-LVW2-B08 Power Draw

Radio Protocol	Sleep Mode Current (If Applicable) (Amps)	Cellular Call Box Connection No Data (Amps)	Average Measured Current (Amps) at Maximum Power	TX Pulse (Avg) Amplitude Current (Amps)) for GSM850 or Peak Current for HSDPA/LTE	Total Inrush Charge Measured in Millicoulombs (mC)
9.0 Volts					
LTE	NA	0.174	0.442	0.528	0.856
20.0 Volts					
LTE	NA	0.094	0.214	0.288	0.860
32.0 Volts					
LTE	NA	0.062	0.138	0.204	2.74

Regulatory Information Labels

The images that follow show where you can find regulatory information for your device.





RF Specifications LTE

Device	Supported RF Technologies
MTR-LAT1	GSM/GPRS/Edge 850, GSM/GPRS/Edge 1900, UMTS/HSPA+ 850, UMTS/HSPA+ 1900, LTE 850, LTE 1700, LTE 1900
MTR-LEU1	GSM/GPRS/Edge 900, GSM/GPRS/Edge 1800, UMTS/HSPA+ 850, UMTS/HSPA+ 900, UMTS/HSPA+ 2100, LTE 800, LTE 1800, LTE 2600
MTR-LVW2	LTE 700, LTE 1700

Chapter 3 Safety Warnings

Lithium Battery

- A lithium battery located within the product provides backup power for the timekeeping. This battery has an estimated life expectancy of ten years.
- When this battery starts to weaken, the date and time may be incorrect.
- Battery is not user replaceable. If the battery fails, the device must be sent back to MultiTech 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 MultiTech 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).

ITE Equipment Ordinary Locations (US, Canada, and Europe)

UL60950-1 and IEC 60950-1

CAUTION: Risk of explosion if this battery is replaced by an incorrect type. Dispose of batteries according to instructions.

Attention: Risque d'explosion si vous remplacez la batterie par un modèle incompatible. Jetez les piles usagées selon les instructions.

Radio Frequency (RF) Safety

Due to the possibility of radio frequency (RF) interference, it is important that you follow any special regulations regarding the use of radio equipment. Follow the safety advice given below.

- Operating your device close to other electronic equipment may cause interference if the equipment is inadequately protected. Observe any warning signs and manufacturers' recommendations.
- Different industries and businesses restrict the use of cellular devices. Respect restrictions on the use of radio equipment in fuel depots, chemical plants, or where blasting operations are in process. Follow restrictions for any environment where you operate the device.
- Do not place the antenna outdoors.
- Switch OFF your wireless device when in an aircraft. Using portable electronic devices in an aircraft may endanger aircraft operation, disrupt the cellular network, and is illegal. Failing to observe this restriction may lead to suspension or denial of cellular services to the offender, legal action, or both.
- Switch OFF your wireless device when around gasoline or diesel-fuel pumps and before filling your vehicle with fuel.
- Switch OFF your wireless device in hospitals and any other place where medical equipment may be in use.

Interference with Pacemakers and Other Medical Devices

Potential interference

Radiofrequency energy (RF) from cellular devices can interact with RF some electronic devices. This is electromagnetic interference (EMI). The FDA helped develop a detailed test method to measure EMI of implanted cardiac

pacemakers and defibrillators from cellular devices. This test method is part of the Association for the Advancement of Medical Instrumentation (AAMI) standard. This standard allows manufacturers to ensure that cardiac pacemakers and defibrillators are safe from cellular device EMI.

The FDA continues to monitor cellular devices for interactions with other medical devices. If harmful interference occurs, the FDA will assess the interference and work to resolve the problem.

Precautions for pacemaker wearers

If EMI occurs, it could affect a pacemaker in one of three ways:

- Stop the pacemaker from delivering the stimulating pulses that regulate the heart's rhythm.
- Cause the pacemaker to deliver the pulses irregularly.
- Cause the pacemaker to ignore the heart's own rhythm and deliver pulses at a fixed rate.

Based on current research, cellular devices do not pose a significant health problem for most pacemaker wearers. However, people with pacemakers may want to take simple precautions to be sure that their device doesn't cause a problem.

- Keep the device on the opposite side of the body from the pacemaker to add extra distance between the pacemaker and the device.
- Avoid placing a turned-on device next to the pacemaker (for example, don't carry the device in a shirt or jacket pocket directly over the pacemaker).

Notice regarding Compliance with FCC and Industry Canada Requirements for RF Exposure

The antenna intended for use with this unit meets the requirements for mobile operating configurations and for fixed mounted operations, as defined in 2.1091 of the FCC rules for satisfying RF exposure compliance. If an alternate antenna is used, consult user documentation for required antenna specifications.

Compliance of the device with the FCC and IC rules regarding RF Exposure was established and is given with the maximum antenna gain as specified above for a minimum distance of 20 cm between the devices radiating structures (the antenna) and the body of users. Qualification for distances closer than 20 cm (portable operation) would require re-certification.

Chapter 4 Antenna Information

Antenna System 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 device's certified antenna system, then recertification will be required by specific network carriers.

The antenna system is defined as the UFL connection point from the gateway to the specified cable specifications and specified antenna specifications.

LTE Antenna Used With MTR-LAT1 and MTR-LVW2 Models

The cellular radio portion of the device is approved with the following antenna or for alternate antennas meeting the given specifications.

Manufacturer:	Laird Technologies
Description:	Dipole Blade Antenna for LTE
Model Number:	DBA6927C1-FSMAM
MultiTech Part Number:	95218149LF

MultiTech ordering information:

Model	Quantity
ANLTE1-2HRA	2
ANLTE1-10HRA	10
ANLTE1-50HRA	50

LTE Antenna Specifications

Category	Description
Frequency Range	698-806 MHz
	824-894 MHz
	880-960 MHz
	1710-1880 MHz
	1850-1990 MHz
	1920-2170 MHz
	2100-2500 MHz
	2500-2690 MHz
Impedance	50 Ohms
VSWR	< 2.5:1

Category	Description	
Typical Radiated Gain	Low band	0.5 dBi (698-960 MHz)
	High band	2.2 dBi (1710-2700 MHz)
Radiation	Omni-directional	
Polarization	Linear	

LTE Antenna Used With MTR-LEU1 Models

The cellular radio portion of the device is approved with the following antenna or for alternate antennas meeting the given specifications.

Manufacturer:	Wieson Technologies
Description:	LTE Antenna
Model Number:	GY115HT467-017
MultiTech Part Number:	95218146LF

MultiTech ordering information:

Model	Quantity
ANLTE2-2HRA	2
ANLTE2-10HRA	10
ANLTE2-50HRA	50

LTE Antenna Specifications

Category	Description
Frequency Range	690-960 MHz
	1710-2170 MHz
	2300-2690 MHz
Impedance	50 Ohms
VSWR	3:1
Peak Radiated Gain	3.5 dBi
Radiation	Omni-directional
Polarization	Linear

GPS Antenna Specifications

Category	Description
Frequency Range	1575.24 MHz
Impedance	50 Ohms

Category	Description
VSWR	2.0:1 max
Gain	10-30 dBi
LNA Current Consumption	40 mA max
Noise Figure	< 2dB
Polarization	RHCP
Input voltage	3.0V \pm 0.2V

Chapter 5 Installing the Router

Installing the Router

1. To use the router's cellular features, connect two suitable antennas to both the CELL and AUX connectors.
2. Using an Ethernet cable, connect one end of the cable to the E-NET connector on the back of the router and the other end to your computer, either directly or through a switch or hub.
3. If you are connecting to a serial interface, connect the DE-9 connector (9-pin) of the RS-232 cable to the RS-232 connector on the router. Then connect the other end to the serial port on the desired device.
4. Some routers support the use of a GPS receiver. If you are using a GPS receiver with the router, attach the GPS cable to the GPS connector on the router.
5. Attach a power cable to your power supply module.
6. Screw-on the power lead from the power supply module into the power connection on the router.
7. Plug the power supply into your power source.
The POWER LED lights after the device powers up.
When the Status LED begins to blink, the device is ready for use.
8. You can configure your router by using your router's web management interface. You might need to change the IP address of your computer to be in the same IP and subnet mask range as the device.
 - a. Open a web browser. In the browser's address field, type the default address for the router:
`http://192.168.2.1`
 - b. A login page opens. In the **username** field, type the default user name: admin (all lower-case).
 - c. In the **password** field, type the default password: admin (all lower-case).
 - d. Click **Login**. The Web Management Home page opens. Online documentation included with the web management interface describes how to configure your router.

Mounting the Device

1. Locate the groove on the bottom of the modem.
2. Slide the mounting rod through the groove.
3. To secure the rod to the desired surface, place and tighten two screws in the holes on either end of the mounting rod. The dimensions illustration in this guide shows the mounting rod, as well as the dimensions for placement of the screws.

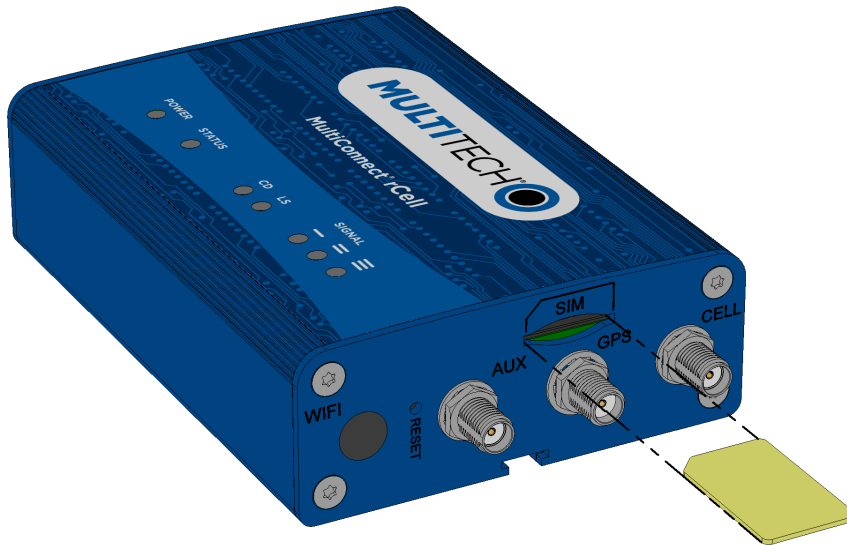
Installing the SIM Card

If you want to operate the router on a GSM/HSPA/LTE network, install a SIM card (Subscriber Identity Module).

To install the SIM:

1. Locate the SIM card slot on the side of the router. The slot is labeled SIM.

2. Push the SIM card into the slot until it snaps into place.



3. To remove the SIM, push the edge of the card in. When released, the card pops out of the device.

Resetting the Device

You need:

- A pin, paperclip, or similar thin object that can fit into the reset hole

The following is the default condition for the RESET button on the device. You can program a change to the behavior of the button if needed.

To reset the device:

1. Find the hole in the front panel labeled RESET. The reset button is recessed into the case.
2. Use the pin to quickly press and release the RESET button.

The device reboots.

Here are the different options using the RESET button:

- To reboot, press RESET for less than 3 seconds.
- To set factory settings or user-defined defaults (if previously set), press RESET for 3 to 29 seconds.
- To set factory settings and erase user-defined defaults, press RESET for 30 seconds or longer.

Restoring User Defined Settings to the Device

You can restore user defined settings to your device.

You need:

- A pin, paperclip, or similar thin object that can fit into the reset hole
1. Locate the hole in the panel labeled RESET. The reset button is recessed into the housing.
 2. Use the pin to press in the button for about 3 seconds and then release the reset button.
 - a. If you do not press in the button long enough, the device will reset, but the user defined settings will not be restored.

- b. If you hold it too long, factory default settings will be restored.

Chapter 6 Using the Wizard to Configure Your Device

Setting Up Your Device

The initial setup wizard can help you quickly set up the main features of your rCell. To use the wizard:

1. From **Administration**, select **Initial Setup**, and follow the on-screen instructions.

Note: The wizard also launches the first time you log into the device's webpage.

2. On the first page, the mode option lets you set up the rCell as a **Network Router** or a **PPP-IP Passthrough** device.

- a. The **Network Router** mode is the default and establishes the device as a cellular network router.
- b. In the **PPP-IP Passthrough** mode, the rCell assigns the IP address it receives from the cellular provider to the Ethernet-attached device. In this mode, the rCell only allows one DHCP lease.

Note: In this mode, many of the rCell services described in this document are non-configurable and do not appear in the device configuration menu. All IP traffic is passed between the Ethernet-attached device and the cellular provider with no firewall functionality.

- c. Click **Next**.

3. In the **Choose Password** page, enter the following:

- a. In the **Current Password** field, type the current password. The default password is **admin**.
- b. In the **New Password** field, type the password you want to use to replace the current one.
- c. To confirm the accuracy of the password, re-type it in the **Confirm Password** field.
- d. Click **Next**. Or if you are done making changes, click **Finish**.

Note: If you do not want to change your password, click **Skip**.

4. In the **Time Configuration** page, set the date, time, and time zone.

- a. In the **Date** field, type the desired date.
- b. In the **Time** field, type the desired time.
- c. From the **Time Zone** drop-down list, select the time zone in which the router operates.
- d. Click **Next**. Or if you are done making changes, click **Finish**.

5. In the **IP Setup** page, give the router its address and network information:

- a. In the **IP Address** field, type the router's IP address.
- b. In the **Mask** field, type the mask for the network. The default is 255.255.255.0.
- c. In the **Primary DNS** field, type the address of the primary DNS.

Note: This is an optional value that can be used if you use a DNS server other than the servers received from your carrier.

- d. Click **Next**. Or if you are done making changes, click **Finish**.

6. In the **PPP Configuration** page, configure PPP for your router.

- a. To use PPP, check **Enable**. When enabled, your device functions as a router.

- b. Check **Diversity** to enable the use of two cellular antennas for better performance. (For devices that use two antennas, Diversity is enabled by default. See Installing the Router for more details).
 - c. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the router to bring up the PPP connection when there is outgoing IP traffic, and take down the PPP connection after a given idle timeout.
 - d. In the **APN** field, type the APN (Access Point Name). The APN is assigned by your wireless service provider.
 - e. Click **Next**. Or if you are done making changes, click **Finish**.
7. In the PPP Authentication page:
- a. From **Type**, select the authentication protocol type used to negotiate with the remote peer: **PAP, CHAP, or PAP-CHAP**. The default value is **NONE**.
 - b. In the **Username** field, type user name with which the remote peer authenticates. You can leave this field blank, if desired. Username is limited to 60 characters.
 - c. In the **Password** field, type the password with which the remote peer authenticates. You can leave this field blank, if desired. Password is limited to 60 characters.
8. Click **Finish**.

Chapter 7 Configuring Your Device

Home Page (Dashboard)

The Home page (dashboard) displays a summary of the configuration settings for the MultiConnect rCell device. The following settings, where applicable, include the area of the Web Management interface where they can be accessed and changed.

Click **Home** to display the following information:

- **Router:**
 - **Model Number:** The MultiConnect rCell model ID.
 - **Serial Number:** The MultiTech device ID.
 - **IMEI:** International Mobile Station Equipment Identity.
 - **Firmware:** MultiConnect rCell MTR firmware version.
 - **Current Time:** Current date and time of the router. For information on setting the date and time, go to **Setup > Time Configuration**.
 - **Up Time:** Amount of time the device has been continuously operating.
 - **WAN Transport:** Current transport for IP traffic leaving the LAN.
- **LAN:**
 - **MAC Address:** Media Access Control Address used to uniquely identify the devices LAN Ethernet interface.
 - **IP Address:** LAN IP address of this device. To configure the IP address, go to **Setup > IP Configuration**.
 - **Netmask:** Network mask of the LAN. To configure the network mask, go to **Setup > IP Configuration**.
 - **Gateway:** Default gateway IP address of the LAN. To configure the default gateway, go to **Setup > IP Configuration**.
 - **DNS:** Current Domain Name System IP addresses known by this device. To configure the DNS, go to **Setup > IP Configuration**.
 - **DHCP State:** Current state of this device's DHCP server. To configure, go to **Setup > DHCP Configuration**.
 - **Lease Range:** Current DHCP lease range of this device's DHCP server. To configure, go to **Setup > DHCP Configuration**.
- **Cellular:**
 - **Protocol Support** (only available when you choose **PPP-IP Passthrough**): Choose from **IPv4** or **IPv6**. If you choose **IPv6**, also enter the **Connect Timeout**.
 - **State:** Current state of the cellular PPP link. For more information, go to **Cellular > Cellular Configuration**.
 - **Signal:** Current signal strength of the cellular link. Mouse hover provides dBm value.
 - **Connected:** Total time connected for the current PPP session.
 - **IP Address:** Current cellular WAN IP address issued to this device by the cellular carrier.
 - **Roaming:** Indicates whether or not this device's cellular link is currently connected to its home network.
 - **Phone number:** Device's cellular phone number also known as Mobile Directory Number (MDN). This field is blank if the MDN is not stored in the SIM card.
 - **Tower:** Tower ID of the cellular tower currently providing cellular service to this device.

WAN Setup

Configuring WAN Failover Priority

Failover mode regulates which WAN is used for the Internet connection and switches the WAN if a connectivity failure is detected.

Failover mode enables the WAN with the highest priority as displayed on the **WAN Configuration** page. If the WAN with priority 1 is disabled or a connection failure is detected, the WAN with priority 2 is automatically selected for establishing connection to the Internet. Wi-Fi as WAN is priority 1 by default.

1. Click **Setup > WAN Configuration**.
2. Under **Options**, click the up and down arrows to change the priority of the appropriate WAN.
3. Click **Save and Restart** to save the change.

For field descriptions see Failover Configuration Fields

For information on editing WAN Failover see Editing Failover Configuration

Editing Failover Configuration

The router can use the active or passive mode to monitor the Internet availability in WAN. The default condition is active mode.

Active mode can be type ICMP (ping) or TCP. ICMP periodically pings the designated host at the specified interval. TCP tries to make a connection to the designated host at the interval specified.

For both ICMP and TCP, if a response is not received, the router switches to the WAN with lower priority. The router continues to ping the designated host at the interval specified for WAN with the higher priority and switches back when the ping is successful. When passive mode is enabled, the router switches the WANs when the network interface is down. The currently active WAN is displayed on the home page under the label WAN Transport.

To edit failover configuration:

1. Click **Setup > WAN Configuration**.
2. Under the **Options** column at the right, click the pencil icon (edit) for the selected WAN. The **Failover Configuration** page is displayed.
3. Make the desired changes. Refer to Failover Configuration Fields for details.
4. Click **Finish**. If you are finished making changes, click **Save and Restart**.

Failover Configuration Fields

Field	Description
Monitoring Mode	Use the drop-down list to select the mode to connect to the host: PASSIVE or ACTIVE.
Interval	Enter the number of seconds between each check. Default is 60 seconds.
Host Name	Enter the host name or IP address to use for the check. Default is www.google.com.
Mode Type	Use the drop-down list to select the mode type: ICMP or TCP. Default is ICMP. (Active Monitoring Mode)
TCP Port	Enter the TCP Port number to connect to the host. (Mode TCP)

Field	Description
ICMP Port	Enter the number of ICMP pings to be sent to the specified host. Default is 10. (Mode ICMP)

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the next note on this subject are not available.

Configuring IP Address and DNS Information for LAN

Your router manages traffic for your local area network (LAN). To change the IP address and DNS configuration:

- From **Setup**, select **IP Configuration**.
- To configure the address information:
 - In the **IP Address** field, type the router's IP address. The default is 192.168.2.1.
 - In the **Mask** field, type the mask for the network. The default is 255.255.255.0.
 - In the **Gateway** field, type the IP address of the network's gateway (router). If this device is the gateway, leave this field blank.
- To resolve domain names, configure domain name server information (DNS).
 - To allow the router to behave as a local DNS forwarder, check **Enable Forwarding Server**.
 - Note:** When a DNS request is received, the router forwards the request to a remote DNS server if there is no record in the router's cache. New requests are cached in the router for future requests.
 - In the **Primary Server** field, type the address of the primary DNS.
 - In the **Secondary Server** field, type the address of the secondary DNS.
 - The **WAN DNS Servers** field displays information about DNS servers, if any, that have been detected on the WAN link of the router.
- Click **Submit**.
- To save your changes, click **Save and Restart**.

Configuring Dynamic Domain Naming System (DDNS)

This feature allows your router to use a DDNS service to associate a hosted server's domain name with a dynamically changing internet address. To configure your router to use DDNS:

- From **Setup**, select **DDNS Configuration**.
- In the **Configuration** group, check **Enabled**.
- In the **Service** field, use the drop-down list to select the desired DDNS service provider.
- In the **Domain** field, type the registered Domain name.
- In the **Max Retries** field, type the maximum number of tries that are allowed if the update fails. The default is 5. The range is 0 to 100.
- In the **Update Interval** field, type the days that can pass with no IP Address change. At the end of this interval, the existing IP Address is updated on the server so that the address does not expire. The range of the interval you can enter is between 1 and 99 days. The default is 28 days.

7. Check **Use Check IP**, if you want to query the server to determine the IP address before 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 DDNS update uses the IP address from the PPP link. The default is **Use Check IP**.
8. In the **Check IP Server** field, type the name to which the IP Address change is registered. Example: members.dyndns.org
9. In the **Check IP Port** field, type the port number of the Check IP Server. The default is 80.
10. Click **Submit**.
11. To save your changes, click **Save and Restart**.

Entering authentication information

Your DDNS server requires you to identify yourself before you can make changes.

1. In the **Username** field, type the name that can access the DDNS Server. The default is NULL. You receive your name when you register with the DDNS service.
2. In the **Password** field, type the password that can access the DDNS Server. The default is NULL. You receive your password when you register with the DDNS service.
3. Click **Submit**. If you are finished making changes click **Save and Restart**.

Forcing a DDNS server update

To update the DDNS server with your IP address, click **Update**.

Configuring Dynamic Host Configuration Protocol (DHCP) Server

You can configure your router to function as a DHCP server that supplies network configuration information, such as IP address, subnet mask, and broadcast address, to devices on the network. To configure the DHCP server:

1. From **Setup**, select **DHCP Configuration**.
2. To use the DHCP feature, check **Enabled**.
3. The Subnet field displays the subnet address.
4. The Mask field displays the network's subnet mask.
5. In the **Gateway** field, type the gateway address. The default Gateway address is the LAN IP address of the router.
6. In the **Domain** field, type your network domain, if any.
7. In the **Lease Time** field, type the DHCP lease time. Lease time is set in days, hours, and minutes. A Lease Time of 00-00-00 is an infinite lease time.
8. In the **Lease Range Start** field and in the **Lease Range End** field, type the range of IP addresses to be assigned by DHCP.
9. Click **Submit**. If you are finished making changes, click **Save and Restart**.

Assigning Fixed Addresses

To add fixed addresses for the DCHP server:

1. In the **Fixed Address** group, click **Add**. A dialog box opens, where you define the address.
2. In the **MAC Address** field, type the MAC address to which the specified IP address binds.
3. In the **IP Address** field, type the fixed IP address to be assigned.
4. Click **Finish**.

5. To save your changes, click **Save and Restart**.

Configuring the Global Positioning System (GPS)

This GPS information applies only to the MTR models (MTR-xxxx-B08) that support GPS.

Some routers have a built-in GPS receiver. If your router has a GPS receiver, the router can forward NMEA (National Marine Electronics Association) sentences from the GPS receiver to a device connected to the router's serial port. You can also send the GPS data over the network to a remote computer.

There are four areas of GPS configuration including: **Server Configuration**, **Local Configuration**, **Client Configuration** and **NMEA Configuration** along with **Current Position** information.

Notes:

- All enabled sentences are forwarded periodically using the interval specified in the **NMEA Configuration** section. Before forwarding, the router adds an ID prefix and ID to each enabled NMEA sentence. If set, the NMEA sentences available are those provided by the built-in receiver which are: GPGGA, GPGSA, GPGSV, GPGLL, GPRMC, GPVTG.
- You can simultaneously enable the TCP Server, TCP/UDP client, and serial port dump.

Dumping NMEA Sentence Information to the Router's TCP Server Port

To configure the TCP server port where you can send the NMEA sentences:

1. Go to **Setup > GPS Configuration > Local Configuration** group, check **TCP Server**.
2. In the **Port** field, type the port number on which the TCP server is listening for connections. The default is **5445**. You can use up to five digits. Each digit itself must be between **0** and **9**. Numbers above **65,535** are illegal as the port identification fields are 16 bits long in the TCP header.
3. If you want the server to request that the remote client supply a password before the NMEA sentences are sent, type that password in the **Password** and **Confirm Password** fields.
4. To use the serial port for GPS, you must disable the serial port client/server. Go to **Setup > Serial IP Configuration > Serial Port Settings** and uncheck **Enabled**.
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

Sending GPS information to a remote server

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

1. To allow the device to connect, go to **Setup > GPS Configuration > Client Configuration**.
2. Check **TCP/UDP Client**.
3. From the **Protocol** drop-down list, select the protocol of the client.
4. In the **Remote Host** field, type the IP address of the remote host.
5. In the **Port**, field type the port number of the remote host.
6. If your remote host requests a password, type that password in the **Password** field. The password is sent to the server in response.
7. Click **Submit**.
8. To save your changes, click **Save and Restart**.

Configuring NMEA Sentences

To configure the time interval, additional prefix or ID information, and which NMEA sentences that can be sent:

1. Go to **Setup > GPS Configuration > NEMA Configuration** and in the **Interval** field, type the amount of time, in seconds, that passes before the NMEA information is sent. The default is **10** seconds. The range is **1 to 255** seconds.
2. You can further identify the router, also called a remote asset, that is collecting and sending the GPS information. To do so:
Add ID: The ID is an unique remote asset identification string. The ID string can be any length up to 20 characters. The **&** and **\$** are invalid characters. The ID must follow the standard NMEA sentence structure. Refer to the Universal IP AT Commands Reference Guide for sentence structure.
 To add more information to the beginning of the ID, in the Add ID Prefix field, type the information.
3. You can select which NMEA sentence types you want to send. Check the desired options: **GGA, GSA, GSV, GLL, RMC,** and **VTG**.

SMTP Settings

The following table lists the configuration fields in the SMTP window.

Field	Description
SMTP Configuration	
Enabled	Click to use the SMTP feature.
Server	Enter the SMTP server address.
Port	Enter the port number that the SMTP server uses.
Email	Enter the sender email address. This address will be added as the sender email address to the sent emails.
Username	Enter the name that can access the SMTP server.
Password	Enter the password that can access the SMTP server.
Mail Log Settings	
Entries to Keep	Enter the desired number of mail log entries that are to be stored in the router. The range of values is 10 to 1000 . If you click Submit , this setting is not applied to the emails that are in progress or deferred. Note that logs are not saved on the device. Also, logs do not persist through power cycles.
Send a Test Email	
Address	To make sure that the SMTP is configured properly, enter a destination email address, then click Send Test Email .

Configuring the serial port

To configure the serial terminal connected to the RS-232 connector on the router:

1. Go to **Setup > Serial IP Configuration > Serial Port Settings**, check **Enabled**.

2. From the **Baud Rate** drop-down list, select the baud-rate at which the serial terminal communicates. The default is **115200**.
3. From the **Flow Control** drop-down list, select the flow control for the serial port. The options are **NONE** or **RTS-CTS**. The default is **NONE**.
4. From the **Parity** drop-down list, select the parity for the serial port. The options are **NONE**, **EVEN**, or **ODD**. The default is **NONE**.
5. To use the Modbus protocol as the protocol the serial devices use to communicate, check **Modbus**.
6. From the **Data Bits** drop-down list, select the data bits for the serial port. Data bit options are **7** or **8**. The default is **8**.
7. From the **Stop Bits** drop-down list, select the stop bits for the serial port. The options are **1** or **2**. The default is **1**.
8. Click **Submit**.
9. To save your changes, click **Save and Restart**.

Configuring Device to Act as Client

You can set up the router to act as a client.

The TCP, UDP, SSL/TLS client feature enables the router to act as a proxy TCP, UDP, or SSL/TLS client to the serial terminal connected to the RS-232 port on the router. This helps the serial terminal access any TCP, UDP, or SSL/TLS server on the LAN/WAN allowing two-way traffic between the serial device and the remote server.

To use this function, you must first check **Enabled** under **Serial Port Settings**. To configure the IP Pipe in TCP, UDP, or SSL/TLS client mode:

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. From the **Mode** drop-down list, select **CLIENT**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP**, **UDP**, or **SSL/TLS**.
4. In the **Server IP Address** field, enter the address of the far-end TCP, UDP, or SSL/TLS server.
5. In the **Server Port** field, enter the port value used by the far-end TCP, UDP, or SSL/TLS server.
6. If the primary server is unavailable, in the **Secondary IP Address** field, enter the address of the alternate TCP, UDP, or SSL/TLS server.
7. If the primary server is unavailable, in the **Secondary Port** field, enter port number value of the alternate TCP, UDP, or SSL/TLS server.
8. From the **Connection Activation** drop-down list, select a connection method. Options are:
 - ALWAYS-ON**. If you select this option, you cannot change the **Connection Termination** option.
 - DTR-ASSERT**. When the DTR signal is asserted, the connection is established.
 - CR**. Three carriage returns must be received before the TCP, UDP, or SSL/TLS connection is established to the remote server.
9. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:
 - ALWAYS-ON**.
 - TIMEOUT**. The IP pipe connection disconnects if the configured timer expires with no data sent or received. In the **Timeout** field, enter the desired number of seconds for this timeout.
 - SEQUENCE**. A sequence of received characters disconnects the IP pipe.
 - DTR-TOGGLE**. When the DTR control signal is toggled, the IP pipe disconnects.
10. Click **Submit**.

11. To save your changes, click **Save and Restart**.

Configuring Device to Act as Server

You can set up the router to act as a server.

The TCP, UDP, SSL/TLS server feature enables a TCP, UDP, SSL/TLS client on the Ethernet network to connect to the remote serial terminal that is connected to the RS-232 port on the router. The router acts as a TCP, UDP, SSL/TLS server which allows two-way traffic between the TCP, UDP, SSL/TLS client and the remote terminal on the serial port.

To use this function, you must first check **Enabled** under **Serial Port Settings**. To configure the IP Pipe in TCP, UDP, SSL/TLS server mode:

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. In the **Mode** drop-down list, select **SERVER**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP, UDP, or SSL/TLS**.
4. In the **Server Port** field, type the desired port value in the range **1 to 65535**.
5. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:
 - ALWAYS-ON.**
 - TIMEOUT.** The IP pipe connection disconnects if the configured timer expires with no data sent or received. In the **Timeout** field, enter the desired number of seconds for this timeout.
 - SEQUENCE.** A sequence of received characters disconnects the IP pipe.
 - DTR-TOGGLE.** When the DTR control signal is toggled, the IP pipe disconnects.
6. Click **Submit**.
7. To save your changes, click **Save and Restart**.

Time Configuration

You can configure how your router manages the setting of time on its domain of systems. The system date and time display in these formats: **MM/DD/YYYY / HH:MM:SS** You can set the date and time manually, or you can configure the router to get this information from an SNTP server.

Setting the Date and Time

To set the router's date and time:

1. From **Setup**, select **Time Configuration**.
2. In the **Date** field, type in the date you desire, or select the date from the pop-up calendar that opens.
3. In the **Time** field, type the time.
4. From the **Time Zone** drop-down list, select your time zone. The default selection is UTC (Universal Coordinated Time, Universal Time).

Note: To learn more about time zones, visit the following website :
<http://www.greenwichmeantime.com/info/current-time.htm>
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

Configuring SNTP to Update Date and Time

To configure the server from which the SNTP date and time information is taken, and how often:

1. To enable SNTP to update the date and time, check **Enabled**.
2. In the **Server** field, type the SNTP server name or IP address that is contacted to update the time.
3. In the **Polling Time** field, type the time that passes, after which the SNTP client requests the server to update the time. Default is 120 minutes. You must enter time in minutes.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

Adding Saved Networks

You can define, edit, and delete networks that your router supports. These networks can appear in your list of choices when configuring other items, such as tunnels. To setup networks:

1. From the **Setup** group, select **Saved Networks**. A list of networks already saved appears.
2. Add, edit, or delete networks, as described in Adding Networks and Editing or Deleting an Existing Network.

Adding Networks

To add a network:

1. Click **Add Network**.
2. In the **Name** field, type the name of the network.
3. In the **IP Address** field, type the IP address of the network.
4. In the **Subnet Mask** field, type the network mask.

Editing or Deleting an Existing Network

1. To delete a network, click **Delete**.
2. At the top of the pane, a message tells you the network is deleted. To undo the delete, click the **Undo** link found in the message.
3. To edit a network, click **Edit**. Change the IP address or subnet mask as desired. Click **Finish**.

Note: You cannot edit the network name and you cannot delete a network if it is used in another configuration.

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the previous note on this subject are not available.

Chapter 8 Setting Up Cellular Features

Configuring Cellular

To configure how cellular is used on your router:

1. On the Web Management interface, go to **Cellular > Cellular Configuration** to display the **Cellular Configuration** window. If you choose IPv6 Passthrough mode, you must select **Setup > PPP-IP Passthrough > Cellular Configuration**.
2. Check **Enabled**.
3. Check and change the Cellular Configuration fields as desired. For field descriptions see Cellular Configuration Fields.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

Cellular Configuration Fields

Field	Description
General Configuration	
Enabled	Allows the router to establish a cellular PPP connection (Cellular WAN).
Dial-on-Demand*	Enables the Dial-on-Demand feature. If enabled, the router brings up and maintains a cellular connection while network activity on the LAN requires WAN access. The router brings down the cellular connection when outgoing network traffic ceases for the given Idle Timeout duration. Enable this feature when Wakeup-on-Call is enabled to allow the device to "sleep" after it has been "woken up". See Configuring Wakeup-on-Call for more information.
Diversity	Allows the use of two antennas to increase receive signal quality. Because diversity is required on MTR-LTE model routers, this field must be enabled.
Connect Timeout	The time (in seconds) that the device waits before it deems that the connection attempt has failed. The value used is the amount of time that elapses between each dialing retry.
Dialing Max Retries	Number of dialing retries allowed; the default is zero, which means an infinite number is allowed.
Modem Configuration	
Dial Number	The modem dial string that initiates a PPP connection, usually *99***1# for GSM. The Verizon dial command should be *99***3# if the device is using a modem for PPP versus module NDIS.
Connect String	The modem response to initiate a PPP connection, usually CONNECT .
Dial Prefix	The modem AT command that initiates a PPP connection, usually ATDT or ATD .
SIM Pin	The pin used to unlock the SIM for use (only required if the SIM is locked).

Field	Description
APN	The Access Point Name assigned by the wireless service provider (carrier specific).
Init String#	Optional fields to apply additional AT commands that execute just before every PPP connection attempt. Use these fields to expand functionality and to troubleshoot.
Authentication	
Authentication Type	The type of authentication to use when establishing a PPP connection: NONE, PAP, CHAP, or PAP-CHAP (either). Authentication may not be required by the cellular service provider.
Username	Name of the user that the remote PPP peer uses to authenticate.
Password	Password that the remote PPP peer uses to authenticate.
Keep Alive*	
Used to periodically check if the cellular link is up; if not, the router tries to establish the link.	
ICMP/TCP Check*	
An active check that provides the most reliable and reactive diagnosis of the cellular link, but requires sending data through the cellular link.	
Enabled*	Enables the Active Keep Alive check. Depending on the plan type and data usage, this may result in additional data charges.
Keep Alive Type*	Protocol type for active keep alive, either TCP or ICMP . ICMP periodically pings the designated host at the specified interval. TCP tries to make a connection to the designated host at the interval specified.
Interval*	Time in seconds between active checking of the cellular link.
Hostname*	Host name or IP address for the keep alive check.
TCP Port*	TCP port number to connect with the TCP server (only visible when Keep Alive Type TCP is selected).
ICMP Count*	Number of sequential, unsuccessful ping attempts to the specified host to declare that the link needs to be re-established (only visible when Keep Alive Type ICMP is selected).
Data Receive Monitor	
A passive check that observes the absence of packets received over a given amount of time. This check cannot reliably determine if the link is down; no network traffic may cause the monitor to signal to shutdown and re-establish the cellular link even though the link was in a good state.	
Enabled	Enable or disable the passive monitoring of the cellular link.
Window	The amount of time that can pass without receiving network traffic before the cellular link is torn down and re-established.

***Note:** If you choose **PPP-IP Passthrough** mode, this field is not available.

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the next note on this subject are not available.

Configuring Wake Up On Call

This feature allows the router to wake up and initiate a cellular connection when there is an incoming call, SMS, or LAN activity.

The Wake Up on Call function is not available for the LVW2 (even though you can access those settings in the device software.)

1. Go to **Cellular > Wake Up On Call** to display the configurations.
2. Check the **Wake Up On Call** box.
3. Select a Wake Up method. For wakeup methods, see Wake Up On Call Settings.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

Note: This feature only defines when the device brings up its cellular link, not when the device takes it down. See the **Dial on Demand** option on the **Cellular Configuration** page at **Cellular > Cellular Configuration** to configure the criteria for bringing the cellular link down.

Wake Up On Call Settings

The triggers that wake up the router to re-establish the cellular link are:

- On Ring:
 - Any incoming call will bring up the cellular link.
 - **Enabled:** Check to allow any incoming call to wake up the router.
 - **Message:** The expected response from the integrated cellular modem to an incoming call.
- On Caller ID:
 - Only incoming calls in the caller ID list will bring up the cellular link.
 - **Enabled:** Check to allow a specific caller to wake up the router.
 - **Caller ID:** Field to specify a caller ID. Click **Add** to add the caller to the approved caller ID trigger list.
- On SMS (not available if you enabled SMS through **SMS > General Configuration**):
 - Only specific SMS messages will bring up the cellular link.
 - **Enabled:** Check to allow specific SMS messages to wake up the router.
 - **Message:** Field to specify the SMS message contents. Click **Add** to add the SMS message to the approved SMS trigger list.

For Wake-Up-On-Call field descriptions, see Wake Up On Call General Configurations.

Wake Up On Call General Configurations

Field	Description
Wake Up on Call check box	Enables the Wake Up On Call feature.

Field	Description
Dial On Demand LAN	When checked, the router allows network activity on the LAN that needs WAN access to trigger the Wake Up and establish the cellular link. If this configuration is not checked, the router will only establish a cellular connection when the selected Wake Up method is triggered via incoming call, caller ID, and/or short message service (SMS).
Time Delay	Time that passes between a receiving call and initiating the Wake Up On Call connection.
Acknowledgment String to Caller	String used to acknowledge to the delivering SMSC (short message service center) the receipt of an SMS.
Init String Number	Router initialization strings specific to the integrated cellular modem required for the Wake Up On Call feature.

Using Telnet to Communicate with the Cellular Radio

Your router comes with an integrated cellular radio. You can use this cellular radio directly without using any router functions. To do so, you must use re-director software on your computer. This software creates a virtual serial port that allows your computer to communicate with the integrated cellular radio over IP using telnet. To communicate directly with the cellular modem:

1. From the Web Management interface, go to **Cellular > Telnet Radio Access**.
2. Check **Enabled**.
3. To enable raw mode, check **Raw**. The program transfers data between the computer and cellular modem without any processing.
4. To enable the Auto Dialout Login feature, check **Login**. The Auto Dialout port is the Telnet port used by the re-director software on your computer to communicate to the cellular modem integrated on the router.
5. In the **Port** field, enter the serial **Auto Dialout Port** number. The default is **5000**.
6. In the **Inactivity** field, enter the time in seconds that the auto dialout session remains active before becoming inactive.
7. To enable the EIA standard signal characteristics (time and duration) used between different electronic devices, check **Handle EIA Signal**.
8. In the **Telnet Keep Alive** section of the window, in the **Time** field, enter the time in seconds that the device waits before it probes the Telnet connection for the first time. The default is **7200** (seconds).
9. In the **Interval** field, enter the time interval in seconds that the device waits between probes. The default is **75** (seconds).
10. In the **Probes** field, enter the number of probes that the device makes. The default is **9**.
11. Click **Submit**.
12. To save your changes, click **Save and Restart**.

Radio Status

Field	Description
Module Information	
IMEI	International Mobile Station Equipment Identifier
Manufacturer	Company that developed the cellular module
Model	Cellular module model number
Hardware Revision	Module's hardware revision
MDN (Phone Number)	Mobile Directory Number. In some SIM/carriers, the value may not be present and therefore not displayed.
MSID	Mobile Station ID. Some SIM/carriers do not contain this value and therefore the value is not displayed.
Firmware Version	Module's firmware version
Service Information	
Home Network	Cellular service provider associated with the module's data account
Current Network	Current cellular service operator
RSSI	Received Signal Strength Indication
Service	Cellular service connection type
Roaming	Indicates whether or not the current service is provided by the Home Network carrier
Update Options	
MDN (Phone Number)	Update the cellular module's phone number. This number is updated only on the device. The MDN that the carrier has associated with this device does not change.

Chapter 9 Setting Up the Firewall

Defining firewall rules

The router's firewall enforces a set of rules that determine how incoming and outgoing packets are handled. By default, all outbound traffic originating from the LAN is allowed to pass through the firewall, and all inbound traffic originating from external networks is dropped. This effectively creates a protective barrier between the LAN and all other networks. For additional information, see:

- Adding Forwarding Rules
- Adding Devices
- Advanced Settings

Adding Forwarding Rules

For a device within the LAN to be visible from the internet or from an outside network, create a forwarding rule to allow incoming packets to reach the device.

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Port Forwarding** group, click **Add Rule**.
3. In the **Inbound Forwarding Rule** dialog box, enter a name for the rule and optionally, a description. Click **Next**.
4. In a second **Inbound Forwarding Rule** dialog box, in the **External WAN Port(s)** field, type the port(s) to be forwarded. Common ports are listed in the field's attached drop-down list and are exposed once you enter a character. Type **ANY** to forward all ports.
5. In the **Destination LAN IP** field, type the IP address of the device that packets will be forwarded to. The attached drop-down list contains DHCP leased and Saved Network addresses.
6. In the **Destination LAN Port(s)** field, type the port to which packets are translated. If there is a range of ports, the ending port is automatically set. The Destination LAN ending port is based on the Destination LAN starting port and the range provided in the **External WAN Port(s)** field.
7. From the **Protocol** drop-down list, select the protocol of the messages that can be forwarded.
8. A default filter allowing forwarded packets through the firewall is automatically created. If desired, you can use the **Advanced Settings** mode of the Port Forwarding wizard to further restrict packets based on source address and source ports. In most cases, this is not necessary.
9. Click **Finish**.
10. To save your changes, click **Save and Restart**.

Adding Outbound Traffic Rules

To prevent a device within the LAN from communicating with a device in an external network, you must establish a firewall rule to drop packets destined to the external device.

1. Click **Add Rule** in the **Outbound Traffic** section.
2. Enter a name for the rule and optionally, a description. Click **Next**.
3. In the **Filter Rule** dialog box, in the **Destination IP** field, type the IP address of the device or network that packets are to be sent to. Type **ANY** if the destination address does not matter.
4. In the **Destination Mask** field, type the network mask of the destination network.

5. In the **Destination Port** field, type the port for which that the packets are destined. Common destination ports are listed in the Destination Port field's attached drop down list. Type **ANY** if the destination port does not matter.
6. In the **Source IP** field, type the IP address of the device or network that the traffic originates from. Type **ANY** if the source address does not matter.
7. In the **Source Mask** field, type a network mask for the origin of the traffic.
8. In the **Source Port** field, type the port that is the origin of the traffic. Type **ANY** if the source port does not matter.
9. From the **Action** drop-down list, select the action to perform on the traffic. You can allow the traffic to be **accepted, rejected, logged** or **dropped**. Accepted packets are allowed to continue through the firewall. Dropped packets are removed and no further processing is performed on them. Rejected packets are dropped, and an error message is sent to the source of the packet. Logged packets are logged to the system's main log file with the rule's name prepended as an identifier (viewable from the Statistics page). Log rules do not affect the packet's fate.
10. The **Direction** field is locked to **OUTGOING** while using the Outbound Traffic wizard.
11. From the **Protocol** drop-down list, select the protocol of the traffic that is being filtered.
12. Click **Finish**.
13. To save your changes, click **Save and Restart**.

Advanced Settings

The **Firewall's Advanced Settings** mode lets you manipulate **DNAT, SNAT**, and **Filter** rules directly. **DNAT** rules can manipulate the destination address and port of a packet; similarly **SNAT** rules can manipulate the source address and port of a packet.

Filter rules apply an **ACCEPT, REJECT, DROP**, or **LOG** action to a packet. **DNAT, SNAT**, and **Filter** rules can be associated if they are named the same. This association is recognized within the **Port Forwarding** and **Outbound Traffic** wizards accessed from the **Normal Settings** mode, and allows the associated rules to be viewed and edited as a series.

Setting up Static Routes

To set up a manually configured mapping of an IP address to a next-hop destination for data packets:

1. Go to **Firewall > Static Routes**.
2. In the **Static Routes** window, click **Add Route**.
3. In the **Name** field of the **Add Route** dialog box, type the name of the route.
4. In the **Address** field, type the remote network IP address of the remote location.
5. In the **Mask** field, type the network mask that is assigned on the remote location.
6. In the **Gateway** field, type the IP address of the routing device that supports the remote IP Network.
7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

Chapter 10 Configuring SMS

Configuring SMS

This function is not available if you enable SMS through **Cellular > Wake Up On Call**. To enable short message service (SMS) via the Web Management interface or API:

1. From the Web Management interface, go to **SMS > SMS Configuration**.
2. Check **Enabled**.
3. In the **Sent SMS to Keep** field, enter the total number of sent SMS messages to keep in the device's history.
4. In the **Received SMS to Keep** field, enter the total number of received SMS messages to keep in the device's history.
5. In the **Resend Failed SMS** field, enter the total number of resend attempts for SMS messages that failed to send.
6. Set messages to keep and resend options.
7. Click **Submit**.
8. To save your changes, click **Save and Restart**.

Sending an SMS Message

To send an SMS message from the router:

1. Go to **SMS > Send SMS** to display the **Send SMS** window.
2. In the **Recipient** field, enter a phone number and click **Add**. You can add up to 100 phone numbers.
3. In the **Message** field, enter a text message up to 160 characters long.
4. Click **Send**.

Viewing Received SMS Messages

To view received SMS messages from the router:

1. Go to **SMS > Received** to display the **Received SMS** window. The messages are sorted by date with the most recent messages on top. The table shows up to 30 characters for each message.
2. To view the full message, click the eye icon to the right of the message entry.
3. To delete an SMS message, click the **X** under **Options** to the right of the message. A dialog box asks you to confirm that you want to delete the SMS message. Click **OK**.
4. To delete all the received SMS messages, click **Delete All**. A dialog box asks you to confirm that you want to delete all SMS messages. Click **OK**.

Viewing Sent SMS Messages

To view sent SMS messages from the router:

1. Go to **SMS > Sent** to display the **Sent SMS** window. The messages are sorted by date with the most recent messages on top. The table shows up to 30 characters for each message.
2. To view a full message, click the eye icon to the right of the message entry.

3. To delete a sent SMS message, click the **X** to the right of the message entry. A dialog box asks you to confirm that you want to delete the SMS message. Click **OK**.
4. To delete all the sent SMS messages, click **Delete All**. A dialog box asks you to confirm that you want to delete all the SMS messages. Click **OK**.

Chapter 11 Defining Tunnels

Setting Up 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. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can be used for carrying many different passenger protocols.

The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. Configuring a GRE tunnel involves creating a tunnel interface, which is a logical interface, then configuring the tunnel endpoints for the tunnel interface. To set up GRE tunnels:

1. From the Web Management interface, go to **Tunnels > GRE Tunnels > GRE Tunnels Configuration**.
2. Click **Add Tunnel**. A series of wizard pages helps you configure the connection.
3. In the **Tunnel Name** field, enter a name for the new tunnel.
4. (Optional) In the **Description** field, you can enter a description that helps you further identify the tunnel. Click **Next**.
5. In the next wizard pane:
 - a. In the **Remote WAN IP** field, type the IP address of the gateway to which you want to connect.
 - b. (Optional) From the **Saved Network** drop-down list, select the network that is to be routed through the tunnel. To select a local interface: Select the local interface on which the tunnel is being created. Eventually, the packets destined for this tunnel will be routed through it.
 - c. If you are not using a saved network, in the **Remote Network Route** field, type the IP address of the network that is routed through the tunnel.
 - d. If you are not using a saved network, in the **Remote Network Mask** field, type the mask of the network.
 - e. Click **Add Route**. The defined GRE tunnel configuration is added and appears in the **Network Routes** list.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

Configuring Network-to-Network Virtual Private Networks (VPNs)

The device supports site-to-site VPNs via IPsec tunnels for secure network-to-network communication. Both tunnel endpoints should have static public IP addresses and must be able to agree on the encryption and authentication methods to use. Setting up an IPsec tunnel is a two-stage negotiation process. The first stage negotiates how the key exchange is protected. The second stage negotiates how the data passing through the tunnel is protected. For endpoints that do not have public static IP addresses, additional options may help such as **NAT Traversal** and **Aggressive Mode**.

By default, based on the encryption method chosen, the device negotiates ISAKMP hash and group policies from a default set of secure algorithms with no known vulnerabilities. This allows flexibility in establishing connections with remote endpoints. There is an **ADVANCED** mode that provides a way to specify a strict set of algorithms to use per phase, limiting the remote endpoint's negotiation options.

The default set of Hash Algorithms is: **SHA-1**, **SHA-2**, and **MD5**.

The default set of DH Group Algorithms is: **DH2(1024-bit)**, **DH5(1536-bit)**, **DH14(2048-bit)**, **DH15(3072-bit)**, **DH16(4096-bit)**, **DH17(6144-bit)**, **DH18(8192-bit)**, **DH22(1024-bit)**, **DH23(2048-bit)**, and **DH24(2048-bit)**.

To set up a Network-to-Network VPN tunnel on your router:

1. From the Web Management interface, go to **Tunnels > IPsec Tunnels**.
2. Click **Add Tunnel** in upper right.
3. Enter a name for the tunnel and an optional description.
4. Click **Next**. The **IPsec Remote Tunnel Endpoint** pane opens.
5. In the **Remote WAN IP** field, enter the external IP address of the remote endpoint.
6. In the **Remote Network Route** and **Mask** fields, enter the remote subnet.
7. Click **Next**. The public IP address and LAN of this device do not need to be configured because they are already known by this device.
8. Enter the **Pre-Shared Key**. This key needs to be the same on both endpoints.
9. Select the **Encryption Method**. **AES** is the successor of **3DES** and is recommended, but **3DES** may be required to operate with legacy endpoints. The encryption method needs to be the same on both endpoints.
10. Click **Next**.
11. If the remote endpoint is set up with unique IDs, check the **Enable UID** box, and enter the **Local and Remote IDs**.
12. Click **Finish**.
13. To save your changes, click **Save and Restart**.

For field descriptions, see IPsec Tunnel Configuration Field Descriptions.

IPsec Tunnel Configuration Field Descriptions

Field	Description
IPSec Tunnel	
Name	Name used to identify the IPsec tunnel in configurations and logs.
Description	Optional text to describe the IPsec tunnel. This description shows up in the UI while hovering over the summary of an IPsec tunnel.
IPSec Remote Tunnel Endpoint	
Remote WAN IP	External IP address of the remote tunnel endpoint. The remote device is typically another router.
Saved Network	Select a saved network from the pre-defined list of user-defined networks on the Setup > Saved Networks page. This network describes the remote endpoint's subnet, and is used to identify packets that are routed over the tunnel to the remote network.
Remote Network Route	This field is used in conjunction with the Remote Network Mask field and describes the remote endpoint's subnet. This is used to identify packets that are routed over the tunnel to the remote network.
Remote Network Mask	This field is used in conjunction with the Remote Network Route field, to describe the remote endpoint's subnet. It identifies packets that are routed over the tunnel to the remote network.

Field	Description
Tunnel Type	Internet Key Exchange (IKE) for host-to-host, host-to-subnet, or subnet-to-subnet tunnels. This field cannot be modified.
IPsec Tunnel: IKE	
Authentication Method	Authentication is performed using secret pre-shared keys and hashing algorithms (SHA1 MD5). This field cannot be modified.
Pre-Shared Key	Secret key that is known by both endpoints.
Encryption Method	IKE encryption algorithm used for the connection (phase 1 - ISAKMP SA). Based off of phase 1, a secure set of defaults are used for phase 2, unless the Advanced option is used, in which case, all components of both phases 1 and 2 are specified by the user.
IPSec Tunnel: Advanced	
IKE Lifetime	Duration for which the ISAKMP SA exists from successful negotiation to expiration.
Key Life	Duration for which the IPsec SA exists from successful negotiation to expiration.
Max Retries	Number of retry attempts for establishing the IPsec tunnel. Enter zero for unlimited retries.
Enable UID	Enable Unique Identifier String (UID) to enable the Local ID and Remote ID fields.
Local ID	String identifier for the local security gateway.
Remote ID	String identifier for the remote security gateway.
Compression	Enable IPComp. This protocol increases the overall communication performance by compressing the datagrams. Compression requires greater CPU processing.
Perfect Forward Secrecy	Newly generated keys are unrelated to older keys.
NAT Traversal	A technique that establishes and maintains the tunnel while traversing network address translation gateways. This may be necessary if this device or the remote endpoint is behind a NAT firewall.
Aggressive Mode	Whether to allow a less secure mode that exchanges identification in plain text. This may be used for establishing tunnels where one or more endpoints have a dynamic public IP address. Although this mode is faster to negotiate phase 1, the authentication hash is transmitted unencrypted. You can capture the hash and start a dictionary or use brute force attacks to recover the PSK.

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the previous note on this subject are not available.

Chapter 12 Device Administration

Configuring Device Access

This section contains configurations that determine how the device can be accessed as well as security features that decrease susceptibility to malicious activity.

To display the **Access Configuration** window containing the fields described below, go to **Administration > Access Configuration**.

HTTP Redirect to HTTPS

The router allows only secure access to its Web UI. This set of rules provides the optional convenience of automatically redirecting HTTP requests to the device's secure HTTPS port.

The router can be configured to allow HTTP access to its RESTFUL JSON API. Embedded devices that do not have SSL/TLS or HTTPS capabilities can then configure, monitor, and control the router.

See the [MTR API Developer Guide](#) for more information.

Field	Description
Enabled	Enables HTTP to HTTPS redirect which automatically redirects users trying to access the device via HTTP to HTTPS.
Port	The port the router listens for HTTP requests on.
Via LAN	If checked, the router listens and responds to HTTP requests from the LAN.
Via WAN	If checked, the router listens and respond to HTTP requests from the WAN.

HTTPS

The router provides secure Web UT access to modify its configurations and execute actions.

Field	Description
Port	The port the router will listen for HTTPS requests on.
Via WAN	If checked, the router will listen and respond to HTTPS requests from the WAN. This increases susceptibility to malicious activity.
Timeout Minutes	Amount of time a user's session can remain dormant before automatically being logged out.
Change Password	Utility to change the user's password.

SSH

The router's internal system can be accessed securely via SSH. This is intended for advanced troubleshooting and/or custom deployment solutions.

Field	Description
Enabled	Enables SSH redirect which automatically redirects users trying to access the device via SSH.
Port	The port the router listens for SSH requests on.
Via LAN	If checked, the router listens and responds to SSH requests from the LAN.
Via WAN	If checked, the router listens and respond to SSH requests from the WAN.

ICMP

Internet Control Message Protocol (ICMP) is used by routers, to send error messages such as that a requested service is not available or a host or router could not be reached. ICMP can also relay query messages.

Field	Description
Enabled	Enables ICMP responses.
Respond to LAN	If checked, the router will respond to ICMP traffic from the LAN, such as ping requests.
Respond to WAN	If checked, the router will respond to ICMP traffic from the WAN, such as ping requests. This increases susceptibility to malicious activity.

Configuring IP Defense

You can configure your router to slow malicious actions against it.

Denial of Service (DOS) Prevention

To mitigate the effects of a denial of service attack:

1. Check **Enabled** to enable the DoS prevention.
2. In the **Per Minute** field, type the average number of pings per minute. This is the number of new connections per minute until burst points are consumed. For example, if 60 new connections are received in a minute, decrement one burst point. If no more burst points occur, drop the packet.
3. In the **Burst** field, type the allowed burst for traffic spikes. A "burst" occurs when the "Per Minute" limit is reached. On a period where the "Per Minute" limit is not reached, one burst point is regained, up to the maximum.
4. Select **Submit** to save changes.
5. To save your changes, click **Save & Restart**.

Ping limit

This engages a set of rules at the firewall that aims to prevent Ping Flood attacks by limiting the number of ICMP requests to the router. This does not apply if ICMP is disabled. To mitigate the effects of a ping DoS on your router:

1. Check **Enabled** to enable the Ping Limit feature.

2. In the **Per Second** field, type the average number of ICMP pings to the router, and the allowed number of pings per second before burst points are consumed. Once burst points run out, ICMP packets will be dropped.
3. To limit the burst of traffic from any source, in the **Burst** field, type the allowed burst for traffic spikes. On a period where the **Per Second** limit is not reached, one burst point is regained, up to this maximum.
4. Select **Submit**.
5. To save your changes, click **Save & Restart**.

Brute force

This feature tracks login attempts at the RESTFUL API level. Its purpose is to prevent Dictionary attacks that attempt to brute force the user's password. To foil brute force, password-guessing attacks:

1. Check **Enabled** to enable the Brute Force Prevention feature.
2. To define how many times someone can try to log in and fail, in the **Attempts** field, type the number of attempts made before the account is locked out. This is the number of failed attempts allowed before the user's account is locked out.
3. In the **Lockout Minutes** field, type the number of minutes that an account is locked out after login attempts fail. This is the number of minutes an account is locked out before a new login attempt will be accepted.

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the next note on this subject are not available.

Generating a New Certificate

Because the router uses a self-signed website certificate, your browser shows a certificate error or warning. Ignore the warning and add an exception or add your rCell IP address to the trusted sites.

To generate a new certificate:

1. Go to **Administration > Certificate Management**. The **Certificate** window displays the details of the certificate that is currently used.
2. Click **Create** to open the **Generate Certificate** window.
3. In the **Common Name** field, enter the name, hostname, or IP address, depending on what you use to connect to the router. The web browser uses this field to check for a valid certificate.
4. In the **Days** field, enter the amount of days before the certificate will expire.
5. In the **Country** field, enter the 2-letter code for the country name.
6. In the **State/Province** field, enter the state or province for which the certificate is valid.
7. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
8. In the **Organization** field, enter the organization name for which the certificate is valid.
9. In the **Email Address** field, enter the email address of the person responsible for the router. Typically this is the administrator. This field may be left blank.
10. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.
11. Click **Submit**.

12. To save your changes, click **Save and Restart**.

Uploading a New Certificate

To upload a new certificate:

1. Go to **Administration > Certificate Management**. The Certificate window displays the details of the certificate that is currently used.
2. Click **Upload** to open **Upload Certificate** window.
3. In the **Days** field, enter the amount of days before the certificate will expire.
4. Click **Choose File** to select a valid certificate to be uploaded.
5. Click **Save**. Wait until the file is uploaded.
6. Click **Submit**.
7. To save your changes, click **Save and Restart**.

Setting up the Remote Management

To modify DeviceHQ™ automatic update settings, go to options under **Auto-Update Settings** and refer to Managing Your Device Remotely.

1. Go to **Administration > Remote Management > Remote Server**. To allow the device to connect to the Remote Management Server, check **Enabled**.
2. If you want the device to use a secure connection, check **SSL Enabled**. This feature might be supported in a future release.
3. The **Server Name** field is pre-populated with the address of the Remote Management Server.
4. The **Server Port** field is pre-populated with the port the Remote Management Server listens on. You likely do not need to change this.
5. In the **Account Key** field, type the account key received from the Remote Management administrator. The device is not allowed to connect to the Remote Management Server without a valid account key.
6. Click **Submit**.
7. To save your changes, click **Save and Restart**.

Managing Your Device Remotely

DeviceHQ™ can monitor devices, reboot devices, and perform remote software and configuration updates.

To configure your device to use DeviceHQ™:

1. Go to **Administration > Remote Management** and check **Enabled**. See other options under Setting up the Remote Server.
2. Go to options under **Auto-Update Settings**.
3. To define how often the device connects to DeviceHQ™ to check in and request any pending updates, set the **Check-In Interval** field to the desired number of minutes between 1-10080 (1 minute to 1 week).

Note:

Your device must connect to DeviceHQ™ every 4 hours at a minimum. If you set the check-in interval to less than 4 hours, your change is ignored.

4. To define how often the device connects to DeviceHQ™ to send GPS data, set the **GPS Data Interval** field to the desired number of minutes, between 1-10080 (1 minute to 1 week).
5. If you want the device to connect to DeviceHQ™ only when the device's cellular link is up, check **Sync with Dial-On-Demand**.

If **Sync with Dial-On-Demand** is checked and cellular dial-on-demand is enabled, the connection is not dialed solely for the purpose of connecting to DeviceHQ™. The device will connect to the system only when other traffic brings up the link.

6. Check **Allow Firmware Upgrade** if you want DeviceHQ™ to make automatic updates of your firmware.
7. Check **Allow Configuration Upgrade** if you want DeviceHQ™ to make automatic updates of your configuration software.
8. Click **Submit**.
9. Click **Save and Restart** to save your changes.

Unavailable Services in PPP-IP Passthrough Mode

In **PPP-IP Passthrough** mode, many rCell services described in this document are non-configurable and therefore do not appear in the device configuration menu. If you choose this mode, all sections between this and the previous note on this subject are not available.

Customizing the User Interface

You can change how the user interface on your device appears. To change the interface:

1. From the Navigation pane, select **Administration > Web UI Customization**.
2. To define what information appears on the **Administration: Support** page, use the Support group. See Customizing Support Information.
3. To define other settings, use the **Device Settings** group. See Specifying Device Settings.

Customizing Support Information

To customize the interface displaying information that can be used to support users:

1. To enable display of the custom support information, go to **Administration > Web UI Customization > Support Information** and check **Show Custom Info**.
2. Type the desired information into the optional fields including:
 - **Company Name**
 - **Country**
 - **Fax**
 - **Address 1**
 - **Address 2**
 - **City**
 - **State/ Prv**
 - **Zip Code**
 - **City**
3. To add a phone number:

- a. Click **Add Phone**.
 - b. A label can appear next to the phone number, for example "Fax" or "Phone" or "International". In the **Label** field, enter text that describes the phone number.
 - c. In the **Number** field, type the phone number.
4. To add a link to a website, click **Add Link**.
 - a. To label the website, type label text in **Label** field.
 - b. In the **URL** field, type the website's link.
 - c. To add further descriptive text about the site, type the information in the **Text** field.
5. To add an image, click **Upload Image**:
 - a. Click **Browse**, go to the location of the image, and select the image.
 - b. Click **OK**.
 6. To delete an existing image, click **Remove Image**.
 7. Click **Submit**.
 8. To save your changes, click **Save and Restart**.

Specifying Device Settings

To define other custom settings for devices:

1. Go to **Administration > Web UI Customization > Device Settings**.
2. Enter desired information in the optional fields including:
 - **Device Name**
 - **Custom ID**
 - **Button Color**
 - **Button Font Color**
 - **Highlight Color**
 - **Highlight Font Color**

Note: To define color fields, use **#rrggbb** format.

3. To add a favorite icon, also known as a shortcut icon or bookmark icon, in the **Custom Favicon** field, click **Choose File**, browse to where the Favicon file resides, select the desired file, and click **Upload Icon**.
4. To remove an existing favorite icon, click **Remove Icon**.
5. To add a custom logo, next to the **Custom Logo** field, click **Choose File** browse to where the logo file resides, select the desired file, and click **Upload Logo**.
6. To remove an existing logo, click **Remove Logo**.
7. Click **Submit**.
8. To save your changes, click **Save and Restart**.

Upgrading Firmware

Upgrade the router's firmware to the latest version.

You can download firmware upgrades from the MultiTech website or update your firmware automatically through MultiTech's Device HQ™ system.

First, check your firmware version. Refer to the upper right corner of your configuration software window. To upgrade the firmware on your device:

1. Before you upgrade your firmware, save your present configuration as a backup. See Device HQ™.
2. Go to the MultiTech website, locate the firmware upgrade file you want for your router, and download this file to a known location.
3. From **Administration**, select **Firmware Upgrade**. The Administration: Firmware Upgrade pane opens.
4. In the **Firmware Upgrade File** field, point to the area where the upgrade file resides, and select the firmware file. To do so:
 - a. Click **Choose File**. Browse to where the firmware file resides that you want to apply.
 - b. Select the file and click **Open**. The file appears in the **Firmware Upgrade File** field. Make sure you select the correct BIN file; otherwise, your router can become inoperable.
5. Click **Start Upgrade**.
6. A message about time needed to upgrade appears. Click **OK**. A progress bar appears indicating the status of the upgrade. When upgrade is completed, your device reboots.
7. After the firmware upgrade is complete, verify your configuration to make sure it is what you expected.

Note:

- The new firmware is written into flash memory.
- It may take up to five minutes to upgrade the firmware. Do not interfere with the router's power or press the router's reset button during this time.
- The Device HQ™ is a cloud platform that provides the ability to remotely manage and upgrade rCell devices. Please see the **Remote Management** section or visit mdm.multitech.com for more information.

Saving and Restoring Settings

To restore previous configuration settings to your router, to restore settings to their factory defaults, or to save the current configuration:

1. Go to **Administration > Save/Restore > Upload Configuration**.
2. To restore a configuration from a previously saved file, go to **Restore Configuration From File**:
 - a. Next to the **Restore Configuration** field, click **Choose File**.
 - b. Navigate to the location where the configuration file is stored and select the desired file.
 - c. Click **Restore**. The device reboots.
3. To save your current configuration to a file, go to **Save Configuration To File**:
 - a. Click **Save**.
 - b. Navigate to the location where you wish to save the file and select location.
4. This option is only available if you had reset to user-defined configuration. (Also, holding the reset button on the device for 30 seconds overrides user-defined settings and resets to factory default.) To reset the router's configuration to the factory settings, go to **Reset to Factory Default Configuration**:
 - a. Click **Reset**.
 - b. A dialog box appears prompting you to confirm that you want to restore to factory default settings.
 - c. Click **OK**.

5. This option is only available if you set user-defined settings first. (Also, holding the reset button on the device for 5 seconds sets user-defined defaults) To restore the router's configuration to the user-defined configuration settings, go to **Reset to User-Defined Configuration**:
 - a. Click **Restore**.
 - b. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
 - c. Click **OK**.
6. To set deployment-specific default settings, click **Set Current Configuration As User-Defined Default**.
 - a. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
 - b. Click **OK**.
7. To save a current configuration:
 - a. Click **Save**.
 - b. A dialog box appears asking you if you want to open or save the configuration file. Click **Save**.
 - c. Navigate to the location where you want to store the configuration. Click **Save**.
 - d. A progress dialog box appears to indicate that the configuration is being saved. Click **Close**.

Using the Router's Debugging Options

The router has utilities to help troubleshoot and solve technical problems. You can set up your device:

- To automatically reboot itself at a particular time of day or use a particular offset in hours from boot.
- To record and report Syslog messages that can help you resolve issues you might experience with your device.

You can also communicate directly with the device's cellular radio. To do this:

1. From **Administration**, select **Debug Options**.
2. Click the down arrow to the far right of the Radio Terminal screen to view the terminal window.
3. Enter AT commands to the radio.

See also: Statistics Configuration Fields

Automatically rebooting the device

To specify the amount of time that passes before the device automatically reboots itself:

1. Go **Administration > Debug Options > Auto Reboot Timer**, select **ENABLED** from the drop-down list under **Auto Reboot**.
2. In the **Auto Reboot Timer** field, select the **Hour of the Day (0-23)** and then enter **Hour of the Day to Restart (0-23)**.
3. If you do NOT want the device to automatically reboot, set the time to **0**. The default setting is **0**.

Setting up Telnet

To enable and configure Telnet on your device:

1. Go to **Administration > Debug Options > Telnet**, check **Enabled**.

2. Enter the **Port** number for Telnet.
3. Enter the **Username**.
4. Enter the **Password**. Enter it again under **Confirm Password**.
5. Click **Submit**.
6. To save your settings, click **Save and Restart**.

Configuring Syslog

To enable and configure Syslog to capture and send messages from your device:

1. To activate Syslog, check **Enabled**.
2. To enable a remote server to receive and store the router's log data, in the **IP Address** field, type the IP address of the desired server.
3. To determine the amount of log information that is collected, in the **Debug Log Level**, type the value that represents the type of information you want to log. All messages with a priority level up to the given value are logged. For example, if you set the log level to 6 all messages with a priority from 0 through 6 are logged, and messages with a priority level of 7 are ignored.
4. To download Syslog information directly from the device, click **Download**.

Statistics Settings

To configure **Statistics**:

1. Go to **Administration > Debug Options > Statistics**.
2. Enter the **Save Timeout** in seconds.
3. Enter the **Save Data Limit** in megabytes.
4. To delete cell activity history, click **Delete Cellular History**.
5. To delete ethernet history, click **Delete Ethernet History**.
6. Click **Submit**.
7. To save your settings, click **Save and Restart**.

Ping and Reset Options

Perform a Ping Test

Ping allows you to test the IP address or URL to ensure it is operational.

To perform a ping test:

1. Go to **Administration > Debug Options > Ping**.
2. Enter the **IP address or URL** of the site you wish to ping.
3. Under **Network Interface**, choose from the available drop-down list options including: **ANY**, **LAN**, **CELLULAR**, and **ETHERNET**. The device does not have a **WiFi** capability.
4. Click **Ping**.

Reset Options

To reset the modem, go to **Administration > Debug Options > Reset Options**, click **Reset Modem**. Click **OK** to confirm.

Chapter 13 Status and Logs

Viewing Device Statistics

The router collects sent/received traffic data for WAN, Cellular, and Ethernet networks. The daily statistical data is stored on the device for a 365-day period. All data that is older than 365 days is automatically deleted.

1. From **Status & Logs** on the left side of the Web Management interface, select **Statistics**. (If you select **PPP-IP Passthrough** mode, go to **Status** menu and then **Statistics**.)
2. The application categorizes statistics about your device. To see statistics that appear in a particular category, click the appropriate tab.

System

Ethernet

Cellular

Serial

GRE

IPSec

Definitions

A data usage bar chart and a cumulative usage line chart are available for Ethernet and Cellular. The Data Usage bar chart also shows statistics for data sent and data received. The following list includes some definitions to help you understand some of the data. Not all of the available statistics are listed here or shown in every tab.

- **Total:** Total number of sent/received bytes for a 365-day period.
- **Today:** Total number of sent/received bytes for today.
- **Sessions:** Bytes
- **Packets:** Number of successfully transmitted (TX) and received (RX) packets.
- **Errors:** Number of errors that occurred. Possibly due to connection issues or network congestion.: Bytes
- **Dropped:** Number of dropped packets. Possibly due to memory constraints.
- **Overruns:** Number of overruns that occurred. Possibly due to processing constraints.
- **Frame:** Number of invalid packets.
- **Carrier:** Number of signal modulation errors that occurred (possibly due to physical connection).
- **Collisions:** Number of packet collisions that occurred due to network congestion.
- **Queue Length:** Length of the transmit queue.

Cumulative and Daily Usage

Click **Show Cumulative Usage** or **Show Daily Usage** to display the desired view. Default chart view is Daily Usage for 30-day period.

Timeframe of Chart

Change the time frame for the chart by clicking **Configure**. In the dialog that appears, set the **Start Date** and **End Date**, then click **Finish**.

Show Log

The associated run-time logs for this section.

Service Statistics

On the Web Management interface side menu, click **Status & Logs > Services** to display the **Service Statistics** window. (If you use **PPP-IP Passthrough** mode, go to **Status** menu and follow the remaining instructions.) This window shows the configuration (enabled or disabled) and the status of the following services:

- **DDNS**
- **SNTP**
- **TCP/ICMP Keep Alive**
- **Dial-on-Demand**
- **SMTP**
- **SMS**

Statistics Configuration Fields

The router saves the statistics periodically depending on the configured timeout and data limit. By default, the Save Timeout is set to 300 seconds and the Data Limit is set to 5 MBytes. For the default scenario, the router saves the data if more than 5 minutes has elapsed, or if more than 5 MBytes has been sent or received from the last check. The router checks these conditions every minute, but the data is saved only if one of the conditions is met.

Field	Description
Save Timeout	The router saves the statistical data when the desired timeout period has elapsed. Default is 300 seconds (5 minutes).
Save Data Limit	The router saves the statistical data if the data limit is reached. Default is 5 MBytes.
Delete Cellular History	Deletes all Cellular history on the router.
Delete Ethernet History	Deletes all Ethernet history on the router.

Mail Log

Mail Log shows the recent email delivery attempts and the mail log details. Mail log entries are sorted by date with the most recent on top. (This function is not available if you use **PPP-IP Passthrough** mode). You can select the number of emails to display in the queue. Possible values are **5, 10, 25, 50**, or **All emails**.

1. Go to **Status & Logs > Mail Log** to display the **Mail Log** window.
2. To see the delivery details, click the eye icon under **Options** for the desired email entry.
3. To delete all mail log entries, click **Purge Log**.
Note: Logs do not persist through power cycles.

Mail Queue

Mail Queue shows the emails that are waiting to be sent. The most recent email delivery attempts are on top. You can select the number of emails to display in the queue. Possible values are **5, 10, 25, 50**, and **All emails**. (This function is not available if you use **PPP-IP Passthrough** mode).

1. Go to **Status & Logs > Mail Queue** to display the **Mail Queue** window.

2. To view the delivery details for an individual email, click the eye icon under **Options** for the desired email entry.
3. To delete all mail log entries, click **Purge Log**.
Note: Logs do not persist through power cycles.

Appendix: Regulatory Information

47 CFR Part 15 Regulation Class B Devices

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential 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.
- Connect 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.

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 Class B Notice

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

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

This device complies with Industry Canada RSS Appliance radio exempt from licensing. The operation is permitted for the following two conditions:

1. the device may not cause harmful interference, and
2. the user of the device must accept any interference suffered, even if the interference is likely to jeopardize the operation.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

FCC Interference Notice

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

Requirements for Cellular Antennas with regard to FCC/IC Compliance

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. This device has been designed to operate with the antennas listed below and having a maximum gain for 850 Mhz of ≤ 6.4 dBi , for 1700 Mhz of ≤ 6.5 dBi, and for 1900 Mhz of ≤ 3 dBi. Antennas not included in this list or that have a gain greater than specified are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

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 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment;

and

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

Restriction of the Use of Hazardous Substances (RoHS)



Multi-Tech Systems, Inc.

Certificate of Compliance

2011/65/EU

Multi-Tech Systems, Inc. confirms that its embedded products comply with the chemical concentration limitations set forth in the directive 2011/65/EU of the European Parliament (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment - RoHS).

These MultiTech products do not contain the following banned chemicals¹:

- 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

Environmental considerations:

- Moisture Sensitivity Level (MSL) =1
- Maximum Soldering temperature = 260C (in SMT reflow oven)

¹Lead usage in some components is exempted by the following RoHS annex, therefore higher lead concentration would be found in some modules (>1000 PPM);

- Resistors containing lead in a glass or ceramic matrix compound.

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 reasonably 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 part of a formal quality system and will be made available upon request.

Waste Electrical and Electronic Equipment Statement

WEEE Directive

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 MultiTech 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.

July, 2005



Information on HS/TS Substances According to Chinese Standards

In accordance with China's Administrative Measures on the Control of Pollution Caused by Electronic Information Products (EIP) # 39, also known as China RoHS, the following information is provided regarding the names and concentration levels of Toxic Substances (TS) or Hazardous Substances (HS) which may be contained in Multi-Tech Systems Inc. products relative to the EIP standards set by China's Ministry of Information Industry (MII).

Hazardous/Toxic Substance/Elements

Name of the Component	Lead (PB)	Mercury (Hg)	Cadmium (CD)	Hexavalent Chromium (CR6+)	Polybrominated Biphenyl (PBB)	Polybrominated Diphenyl Ether (PBDE)
Printed Circuit Boards	O	O	O	O	O	O
Resistors	X	O	O	O	O	O
Capacitors	X	O	O	O	O	O
Ferrite Beads	O	O	O	O	O	O
Relays/Opticals	O	O	O	O	O	O
ICs	O	O	O	O	O	O
Diodes/ Transistors	O	O	O	O	O	O
Oscillators and Crystals	X	O	O	O	O	O
Regulator	O	O	O	O	O	O
Voltage Sensor	O	O	O	O	O	O
Transformer	O	O	O	O	O	O
Speaker	O	O	O	O	O	O
Connectors	O	O	O	O	O	O
LEDs	O	O	O	O	O	O
Screws, Nuts, and other Hardware	X	O	O	O	O	O
AC-DC Power Supplies	O	O	O	O	O	O
Software /Documentation CDs	O	O	O	O	O	O
Booklets and Paperwork	O	O	O	O	O	O
Chassis	O	O	O	O	O	O

X Represents that the concentration of such hazardous/toxic substance in all the units of homogeneous material of such component is higher than the SJ/Txxx-2006 Requirements for Concentration Limits.

O Represents that no such substances are used or that the concentration is within the aforementioned limits.

Information on HS/TS Substances According to Chinese Standards (in Chinese)

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。

有害/有毒物质/元素

成分名称	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
ICs	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
LEDs	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之内。