



MultiConnect® rCell 100

MTR-H5 User Guide

MultiConnect® rCell 100 Series Router User Guide

Model: MTR-H5

Part Number: S000566 Version: 1.14

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 MULTI-TECH 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

Chapter 1 Product Overview	7
About MultiConnect rCell 100 Series Router	7
Documentation	8
Product Build Options	8
Descriptions of LEDs.....	9
Side Panel Connectors	10
Ethernet LED Descriptions	11
Specifications	11
Dimensions.....	13
Label locations	13
Power Draw.....	15
RF Specifications	15
Chapter 2 Safety Warnings	16
Lithium Battery	16
ITE Equipment Ordinary Locations (US, Canada, and Europe)	16
Class I, Division 2, Groups A, B, C, and D Hazardous Locations (US and Canada)	16
ATEX (Europe only)	17
Hazardous Location Special Considerations	17
Ethernet Ports	17
Radio Frequency (RF) Safety	17
Interference with Pacemakers and Other Medical Devices	18
Potential interference	18
Precautions for pacemaker wearers	18
Notice regarding Compliance with FCC and Industry Canada Requirements for RF Exposure	18
Chapter 3 Cellular Information	20
Antenna System Cellular Devices.....	20
HEPTA Antenna Information.....	20
Authorized Antenna/Antenna Specifications for Cellular Bands	20
3G Antenna Requirements/Specifications	20
GPS Antennas Specifications.....	21
Bluetooth and Wi-Fi Antennas	21
Multi-Tech Ordering Information	21
Antenna Specifications.....	21
Chapter 4 Installing the Router	22
Installing the Router.....	22
Using Diversity	22
Mounting the Device.....	23

Activating the Account for Wireless Devices	23
Installing the SIM Card	23
Setting up Wi-Fi.....	24
Resetting the Device	25
Restoring User Defined Settings to the Device	25
Notice for Devices that Use Aeris Radios.....	25
Chapter 5 Using the Wizard to Configure Your Device.....	26
Setting Up Your Device	26
Chapter 6 Configuring Your Device.....	28
Home Page (Dashboard)	28
Configuring IP Address and DNS Information for LAN	29
Configuring WAN Failover Priority	29
Editing Failover Configuration.....	30
Failover Configuration Fields	30
Configuring Dynamic Domain Naming System (DDNS)	31
Entering authentication information	31
Forcing a DDNS server update	31
Configuring Dynamic Host Configuration Protocol (DHCP) Server	31
Assigning fixed addresses	32
Configuring the Global Positioning System (GPS).....	32
Dumping NMEA sentence information to the router's TCP server port	32
Sending GPS information to a remote server	33
Configuring NMEA Sentences	33
Configuring the serial port	33
Configuring Device to Act as Client	34
Configuring Device to Act as Server.....	34
Setting the device's date and time	35
Setting the date and time	35
Configuring SNTP to update date and time	35
Adding Networks Overview	35
Adding Networks.....	35
Editing or Deleting an Existing Network	36
Setting Up Your Device	36
Chapter 7 Setting Up Wireless Features	38
Setting Up Wi-Fi Access Point.....	38
Setting security options	38
Viewing information about Wi-Fi clients using your wireless network.....	39
Setting Up Wi-Fi as WAN	39
Setting up Bluetooth	39
IP Pipe in TCP/UDP Server mode	40

Chapter 8 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 9 Setting Up Cellular Features	43
Configuring Cellular	43
Cellular Configuration Fields	43
Configuring Wake Up On Call.....	45
Wake Up On Call Settings	45
Wake Up On Call General Configurations	45
Using Telnet to communicate with the cellular radio	46
Radio Status	46
Chapter 10 Configuring SMS	48
Configuring SMS.....	48
SMS Field Descriptions.....	48
Sending an SMS Message.....	48
Viewing Received SMS Messages	48
Viewing Sent SMS Messages.....	48
Chapter 11 Defining Tunnels	50
Setting up Generic Routing Encapsulation (GRE) tunnels	50
Configuring Network-to-Network Virtual Private Networks (VPNs)	50
IPsec Tunnel Configuration Field Descriptions	51
Chapter 12 Device Administration	53
Resetting the Device	53
Restoring User Defined Settings to the Device	53
Configuring Device Access	53
Web Server.....	53
IP Defense	54
Configuring IP defense	55
Denial of service (DOS) attack	55
Ping limit	56
Brute force	56
Generating a New Certificate.....	56
Uploading a New Certificate	56
Setting up the Remote Server.....	57
Managing Your Device Remotely with Multi-Tech Device Manager	57
Customizing the user interface	57
Customizing support information	58
Specifying Device Settings	58

Upgrading firmware	58
Saving and restoring settings	59
Using the router's debugging options	60
Automatically rebooting the device.....	60
Configuring Syslog.....	60
SMTP Settings	60
Chapter 13 Device Status	62
Viewing device statistics	62
Mail Log.....	62
Mail Queue.....	63
RF Survey.....	63
Service Statistics.....	63
Statistics Configuration Fields.....	63
Appendix: Regulatory Information	65
47 CFR Part 15 Regulation Class B Devices	65
Industry Canada Class B Notice.....	65
FCC Interference Notice	65
FCC and IC Antenna Requirements Toward License Exempt Radio Transmitters (Bluetooth/WLAN)	66
Requirements for Cellular Antennas with regard to FCC/IC Compliance	66
EMC, Safety, and R&TTE Directive Compliance	66
Restriction of the Use of Hazardous Substances (RoHS)	67
REACH Statement	68
Registration of Substances.....	68
Substances of Very High Concern (SVHC)	68
Waste Electrical and Electronic Equipment Statement	68
WEEE Directive.....	68
Instructions for Disposal of WEEE by Users in the European Union	68
Information on HS/TS Substances According to Chinese Standards	69
Information on HS/TS Substances According to Chinese Standards (in Chinese)	70

Chapter 1 Product Overview

About MultiConnect rCell 100 Series Router

This guide describes the MultiConnect rCell 100 Series router. The rCell family of routers is carrier approved and ready-to-deploy. You can use your device to provide secure data communication between many types of devices that use legacy as well as the latest communication technologies. Some device models support:

- Bluetooth communication to devices with this technology
- Wi-Fi communication to devices with this technology
- 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:





Items bundled with the MTR-H5-B10 device: 1 Taoglas GW.11.A153 Wi-Fi antenna, 2 Laird Hepta-SM MAF94300 antennas, 1 Trimble GPS antenna 66800-52 and 1 Globtek GT-41052-1509 9V 1.7A power supply.

Documentation

The following table describes additional documentation for your device. The documentation is available on the Multi-Tech Installation Resources website at www.multitech.com/setup/product.go.

Document	Description
User Guide	This document. Provides an overview, safety and regulatory information, schematics and general device information.
API Developer Guide	You can use the rCell API to manage configurations, poll statistics, and issue commands. The design, patterns, and methods are documented in the rCell API Developer Guide part number S000576.
AT Commands	This document describes AT commands that are available for your device. These commands are documented in the Reference Guide part number S000574.

Product Build Options

Product	Description
MTR-H5-B07	Supports HSPA+
MTR-H5-B08	Supports HSPA+ and GPS
MTR-H5-B09	Supports HSPA+, Wi-Fi, and Bluetooth
MTR-H5-B10	Supports HSPA+, Wi-Fi, Bluetooth, and GPS.

Descriptions of LEDs

The top panel contains the following LEDs:

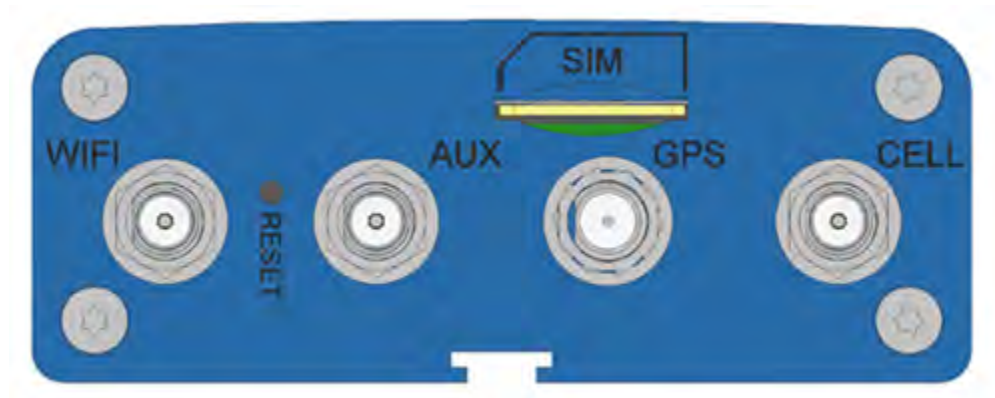
- **Power and Status LEDs**—The Power LED indicates that DC power is present and the Status LED blinks when the unit is functioning normally.
- **Wi-Fi**—Indicates if the device is serving as a Wi-Fi access point or acting as a Wi-Fi client. Not all models support Wi-Fi.
- **Modem LEDs**—Two modem LEDs 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.
WiFi	<p>Infrastructure mode</p> <ul style="list-style-type: none"> ■ The WiFi LED is lit when WiFi AP mode is enabled, unlit when disabled. ■ The LED flashes rapidly to indicate traffic. <p>Client mode:</p> <ul style="list-style-type: none"> ■ The WiFi LED is lit when WiFi client mode is enabled. ■ The WiFi LED blinks slowly when associated with an Access Point. ■ The WiFi LED flashes rapidly to indicate traffic.
CD	Carrier Detect. When lit, indicates data connection has been established.
LS	<p>Link Status</p> <p>OFF — No power to the cellular radio</p> <p>Continuously Lit — Not registered</p> <p>Slow Blink (-0.2Hz) — Registered or connected</p>
SIGNAL	<p>Signal strength for cellular.</p> <p>ALL OFF—Unit is off, not registered on network, or extremely weak signal ($0 \leq \text{RSSI} < 6$).</p> <p>1 Bar “ON” —Very weak signal ($7 \leq \text{RSSI} < 14$).</p> <p>1 Bar and 2 Bar “ON” —Weak signal ($15 \leq \text{RSSI} < 23$).</p> <p>1 Bar, 2 Bar, and 3 Bar “ON” — Good signal ($24 \leq \text{RSSI} \leq 31$).</p>

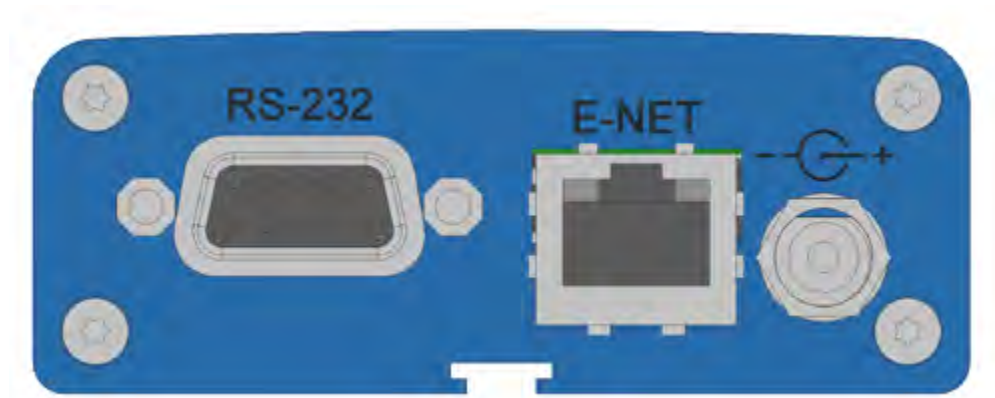
Side Panel Connectors

The device has connectors on both sides of the housing. The right side of the device has a SIM card holder, as well as Wi-Fi, auxiliary, GPS, and cellular antenna connectors. It also has a reset button. Depending on the model of your device, the GPS antenna connector may or may not appear.

The following shows the right side panel of the device:




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



The following table describes the connectors and other items on the two side panels:

Label	Description
WIFI	Connector for the Taoglas GW.11.A153 Wi-Fi antenna.
CELL, AUX	Cellular antenna inputs. Use with the 2 Laird Hepta-SM MAF94300 antennas that are supplied with the device. ■ CELL - Primary. AUX - Diversity.
GPS	GPS antenna input. Use with the Trimble GPS antenna 66800-52 supplied with the device. Used only on the MTR-LTE B08 models.
RS-232	DCE 9-pin, female-D Sub through-hole connector
SIM	Receptacle for a SIM card (Subscriber Identity Module). Use when operating on GSM/HSPA network.

Label	Description
RESET	Resets the device. Refer to Resetting the Device or Resetting the Device to Factory Defaults.
E-NET	RJ-45 receptacle for standard Ethernet 10/100 Base-T. Caution: Ethernet ports and command ports are not designed to be connected to a public telecommunication network or used outside the building or campus.
USB HOST	High-speed, standard USB 2.0 Type A connector. 500mA maximum current draw.
Power 	9-32 Vdc power receptacle for provided power cord. The device uses a Globtek GT-41052-1509 9V 1.7A power supply.


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.

Specifications

Category	Description
General	
Performance	HSPA+
	GPRS/EDGE
Frequency Bands	Tri-Band 850/900/2100 MHz
	Quad Band 850/900/1800/1900 MHz
Radio	
Cellular	Telit HE910-D
Wi-Fi, Bluetooth	Murata LBEE5ZSTNC-523
Speed	
Packet Data	Up to 7.2 Mbps downlink/5.76 Mbps uplink
SMS	
SMS	Point-to-Point Messaging
	Mobile-Terminated SMS
	Mobile-Originated SMS
Connectors	
Cellular	Female SMA connectors for cellular

Category	Description
WiFi	Reverse polarity male SMA connector for Wi-Fi
SIM Holder	Mini-SIM, standard 1.8 V and 3 V SIM receptacle 
GPS	Female SMA connector
Power Requirements¹	
Voltage	7 V to 32 V DC
Physical Description	
Dimensions	Refer to the <i>Dimensions</i> topic that follows.
Weight	8.2 ounces or 230 grams
Environment	
Operating Temperature ²	-40° C to +85° C
Humidity	Relative humidity 15% to 93% non-condensing
Certifications, Compliance, Warranty	
EMC Compliance	EN55022 Class B
	EN55024
Safety Compliance	UL 60950-1
	UL 201
	IEC 60950-1
	ANSI/ISA 12.12.01 2013 and CSA C22.2 No. 213
	EN 60079-0:2012+A11:2013
	EN 60079-15:2010
Network Compliance	GCF
Warranty	Two years

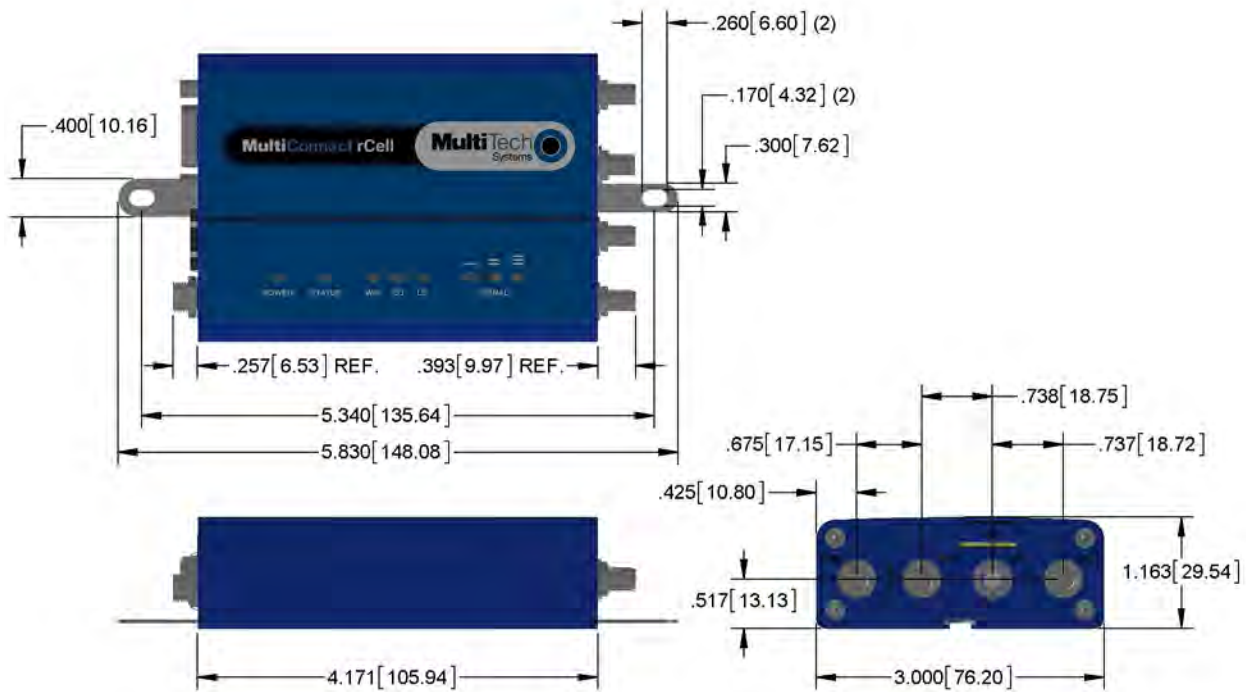
¹Optional power supply must be a Listed ITE power supply marked LPS or Class 2 rated 7-32Vdc, 1A minimum. Certification does not apply or extend to Voltages outside certified range, and has not been evaluated by UL for operating voltages beyond tested range.

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 use 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.

Dimensions



Label locations

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





Power Draw

Radio Protocol	Cellular Cell Box Connection No Data (Amps)	(AVG) Measured Current (Amps) at Max Power	TX Pulse (AVG) Amplitude Current (Amps) for GSM850 or Peak Current for HSDPA)	Total Inrush Charge Measured in Millicoulomb (mC)
7.0 Volts				
GSM 850MHz	0.239	0.589	1.67	2.09
HSDPA 1800MHz	N/A	0.797	0.808	N/A
9.0 Volts				
GSM 850MHz	0.206	0.315	1.06	1.86
HSDPA 1800MHz	N/A	0.606	0.624	N/A
32.0 Volts				
GSM 850MHz	0.067	0.151	0.356	0.720
HSDPA 1800MHz	N/A	0.185	0.188	N/A

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

RF Specifications

	GSM 850	EGSM	GSM 1800	GSM 1900
Frequency RX	869 to 894 MHz	900 925 to 960 MHz	1805 to 1800 MHz	1930 to 1990 MHz
Frequency TX	824 to 849 MHz	880 to 915 MHz	1710 to 1785 MHz	1850 to 1910 MHz

Chapter 2 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 Multi-Tech Systems for battery replacement.
- Lithium cells and batteries are subject to the Provisions for International Transportation. Multi-Tech Systems, Inc. confirms that the Lithium batteries used in the Multi-Tech product(s) referenced in this manual comply with Special Provision 188 of the UN Model Regulations, Special Provision A45 of the ICAO-TI/IATA-DGR (Air), Special Provision 310 of the IMDG Code, and Special Provision 188 of the ADR and RID (Road and Rail Europe).

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.

Class I, Division 2, Groups A, B, C, and D Hazardous Locations (US and Canada)

ANSI_ISA_12.12.01_2013 and CSA C22.2 No. 213

MTR -HZ models only

1. The modems are open devices intended for installation in an enclosure suitable for the intended application.
 2. THIS EQUIPMENT IS SUITABLE FOR USE IN CLASS I, DIVISION 2, GROUPS A, B, C, AND D OR NON-HAZARDOUS LOCATIONS ONLY.
 3. WARNING – Explosion Hazard – Substituting components may impair suitability for Class I Division 2.
 4. WARNING – Explosion Hazard – Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.
 5. WARNING – Explosion Hazard - Do not replace the fuse or battery unless power has been switched off or the area is known to be non-hazardous.
 6. WARNING – Do not install or remove SIM card unless power has been switched off or the area is known to be non-hazardous.
 7. “CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.”
1. Les modems sont des appareils ouverts conçus pour être installés dans une enceinte adaptée à l'application prévue.
 2. CET ÉQUIPEMENT EST ADAPTÉ EXCLUSIVEMENT POUR UNE UTILISATION EN ZONE DE CLASSE I, DIVISION 2, GROUPES A, B, C, ET D OU EN ZONE NON DANGEREUSE.

3. AVERTISSEMENT – Risque d'explosion – Le remplacement des composants peut annuler la compatibilité du produit avec les zones de Classe I Division 2.
4. AVERTISSEMENT – Risque d'explosion – Ne débranchez pas l'équipement sauf s'il est hors tension ou si la zone est considérée comme non dangereuse.
5. AVERTISSEMENT - Risque d'explosion - Ne remplacer le fusible ou la batterie que si l'alimentation électrique est coupée ou que la zone est connue pour être non dangereuse.
6. AVERTISSEMENT – N'installez ou ne retirez pas de carte SIM sauf si l'alimentation a été coupée ou si la zone est considérée comme non dangereuse.
7. ATTENTION : Risque d'explosion si vous remplacez la batterie par un modèle incompatible. Jetez les piles usagées selon les instructions.

ATEX (Europe only)

EN 60079-0:2012+A11:2013 & EN60079-15:2010

MTR -HZ models only

- Battery is not user replaceable. If the battery fails, the device must be sent back to Multi-Tech Systems for battery replacement.
- **EXPLOSION HAZARD**— Battery must only be changed by manufacturer in an area known to be non-hazardous.

Manufacturer approved lithium batteries:

Manufacturer	Part Number	Safety File No.
Renata	CR1632	MH14002
Hitachi	CR1632	MH12568
Panasonic	CR1632	MH12210

Hazardous Location Special Considerations

Special conditions for safe use:

- MTR Series Router wireless modem is intended for installation into an ATEX certified IP54 enclosure and accessible only by the use of a tool.
- The equipment shall only be used in an area of not more than pollution degree 2, as defined in IEC 60664-1.
- Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 140%.
- The device is intended to be powered by a Certified SELV non-energy hazardous power supply.

Ethernet Ports

CAUTION: Ethernet ports and command ports are not designed to be connected to a public telecommunication network.

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 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 3 Cellular 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.

HEPTA Antenna Information

Authorized Antenna/Antenna Specifications for Cellular Bands

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:	HEPTA-SM
Model Number:	MAF94300
Multi-Tech Part Number:	45009735L

Multi-Tech ordering information:

Model	Quantity
ANHB-1HRA	1
ANHB-10HRA	10
ANHB-50HRA	50

3G Antenna Requirements/Specifications

Category	Description	
Frequency Range	824 – 960 MHz / 1710 – 1990 MHz / 1920 – 2170 MHz	
Impedance	50 Ohms	
VSWR	VSWR should not exceed 2.0:1 at any point across the bands of operation	
Typical Radiated Gain	850 MHz	3.17 dBi
	950 MHz	3.51 dBi
	1800 MHz	3.55 dBi
	1900 MHz	3.0 dBi
	2100 MHz	3.93 dBi
Radiation	Omni-directional	
Polarization	Linear Vertical	

GPS Antennas Specifications

Category	Description
Frequency Range	1575.24 MHz
Impedance	50 Ohms
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

Bluetooth and Wi-Fi Antennas

Manufacturer: Taoglas Antenna Solutions
 Manufacturer's Model Number: GW.11.A153
 Multi-Tech Systems: 45009740L

Multi-Tech Ordering Information

Model Number	Quantity
ANWF-1HRA	1
ANWF-10HRA	10
ANWF-50HRA	50

Antenna Specifications

Category	Description
Frequency Range	2.4000 to 2.4835 GHz
Impedance	50 Ohms
VSWR	VSWR should not exceed 2.0:1 at any point across the bands of operation
Peak Radiated Gain	2.3 dBi on azimuth plane
Radiation	Omni-directional
Polarization	Linear Vertical
Connector	RP-SMA(M)

Chapter 4 Installing the Router

Installing the Router

1. To use the router's cellular features, connect a suitable antenna to the antenna connector.
2. If your device is capable of supporting antenna diversity, see the section about diversity.
3. Some routers support Wi-Fi. To use the router's Wi-Fi access point features, install a suitable antenna to the Wi-Fi antenna connector on the router.

The Wi-Fi antenna connection is reverse polarity. If you use a standard antenna on the Wi-Fi connector, you can damage the antenna and the connector.

Five Wi-Fi devices can concurrently use your Wi-Fi access point.

4. Using an Ethernet cable, connect one end of the cable to the ETHERNET connector on the back of the router and the other end to your computer, either directly or through a switch or hub.
5. If you are connecting to a serial interface, connect the DE9 connector (9-pin) of the RS232 cable to the RS232 connector on the router, then connect the other end to the serial port on the desired device.
6. 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.
7. Attach a power cable to your power supply module.
8. Screw-on the power lead from the power supply module into the power connection on the router.
9. 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.

10. 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 an Internet 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

Using Diversity

Some devices support antenna diversity. Antenna diversity uses two receive antennas to improve the downlink connection (cell tower to mobile). It has no effect on the uplink (mobile to cell tower). Antenna diversity is useful in environments where the signal arrives at the device after bouncing off or around buildings or other objects.

When antenna diversity is on and a like or similar antenna is installed on both radio connectors, the radio automatically chooses the antenna with the best reception. To use this feature:

1. Connect both antennas to your device, using both antenna connectors.
2. Use the device's web interface to enable the diversity feature. See the help file for details.

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.

Activating the Account for Wireless Devices

For information on activating your cellular modem:

1. Go to <http://www.multitech.com/support>.
2. Select your device.
3. Scroll to **Activation** and click **Download**.

Note: If you need remote access to your MultiConnect device over the Internet for remote configuration, ensure that your wireless network provider has provisioned mobile terminated data and fixed or dynamic public IP address in which they can configure the network to redirect any incoming connection to that predefined IP.

Installing the SIM Card

If you want to operate the router on a GSM/HSPA 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.

Setting up Wi-Fi

Some models have Wi-Fi capability. If your device supports this feature, you need to use the device's web management interface to enable Wi-Fi. Then, see the online help file for information on working with Wi-Fi.

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 Conduit. 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.

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.

The Conduit mLinux Model is shown. The RESET button is in the same location on both Conduit models.

Notice for Devices that Use Aeris Radios

One component of your device is a radio. A radio algorithm prevents your device from repeatedly attempting to connect to the network when the radio:

- Cannot establish a packet data connection or
- Fails to access the application server.

When writing applications for your devices, ensure that your applications do not interfere with the radio's connection retry algorithm. If you fail to do so, Aeris might block network access for your devices.

After your devices reach the end of their commercial lifespan, you must remove them from the Aeris network. To do so, remove power from the devices and remove their antennas. If your devices continue to attempt to register with the network after you cancel device subscriptions, Aeris can bill you for any traffic generated by those devices.

Chapter 5 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 panel, 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 passes the IP address it receives from the cellular provider during a PPP connection to another device.

Note: In this mode, the rCell only allows one DHCP lease. Many of the services the rCell provides as a router are disabled in this mode due to the passing of its WAN IP address to another device.

- c. Click **Next**.
3. In the Choose Password panel, 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 panel, set the date time and time zone.
 - a. In the **Time** field, type the desired time.
 - b. In the **Date** field, type the desired date.
 - c. From the **Time Zone** drop-down, 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 panel, 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 panel, 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.

- c. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the router that it should only bring up the PPP connection when there is outgoing IP traffic, and that it would bring the PPP connection down after a given idle timeout.
- d. In the **Idle Timeout** field, type the amount of idle time that passes before the router times out. If the time expires, the PPP connection to the Internet is disconnected. The default is 180 seconds.

Note: The Idle Timeout configuration only applies to Dial-on-Demand.

- e. In the **APN** field, type the APN (Access Point Name). The APN is assigned by your wireless service provider.

Note: This configuration does not apply for rCell units with embedded CDMA/EVDO radios. For these devices, you will not be able to modify this field.

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

7. In the PPP Authentication panel:

- a. From **Type**, select the authentication protocol type used to negotiate with the remote peer: pap, chap, or pap-chap. The default is pap-chap.
- 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 will authenticate. You can leave this field blank, if desired. Password is limited to 60 characters.

8. Click **Finish**.

Chapter 6 Configuring Your Device

Home Page (Dashboard)

This page provides a high-level view of the MultiConnect rCell device.

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.

Note: Not applicable for the MTR-C2 or MTR-EV3 models.

- **MEID:** Mobile Equipment Identifier.

Note: Only for the MTR-C2 or MTR-EV3 models.

- **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. If two WAN interfaces are configured for use (Wi-Fi and cellular), the current WAN will be set based on the WAN configurations at *Setup > WAN Configuration*.

■ LAN:

- **MAC Address:** Media Access Control Address used to uniquely identify the device's 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:

- **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).
- **Tower:** Tower ID of the cellular tower currently providing cellular service to this device.

- **Wi-Fi:**
 - **Mode:** Indicates the current Wi-Fi mode. Options include None, Wi-Fi as WAN, or Wi-Fi Access Point. For configuration go to *Wireless > Wi-Fi*.
 - **MAC Address:** Media Access Control Address used to uniquely identify the Wi-Fi interface. This MAC will be the same as the Ethernet MAC when in Access Point mode.
 - **State:** Current state of the Wi-Fi.
 - **SSID:** In Access Point mode, this is the Service Set Identifier (SSID) for this device's Wi-Fi Access Point. In Wi-Fi As WAN mode, this is the SSID of the Wi-Fi Access Point this device is currently connected to or trying to connect to. For configuration go to *Wireless > Wi-Fi*.
 - **Security:** In Access Point mode, this is the current security protocol of this device's Wi-Fi Access Point. To configure go to *Wireless > Wi-Fi*.
- **Bluetooth:**
 - **State:** Current state of the Bluetooth link. To configure go to *Wireless > Bluetooth*.
 - **MAC Address:** Media Access Control Address used to uniquely identify the Bluetooth interface.
 - **Device Name:** Name of Bluetooth device configured to link to. For configuration go to *Wireless > Bluetooth*.
 - **Device MAC:** Media Access Control Address of the Bluetooth device configured to link to. To configure go to *Wireless > Bluetooth*.

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:

1. From **Setup**, select **IP Configuration**.
2. 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.
3. 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.
4. Click **Submit**.
5. When you are finished making changes, click **Save and Restart**.

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

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:

1. From **Setup**, select **DDNS Configuration**.
2. In the **Configuration** group, check **Enabled**.
3. In the **Server** field, type the name of the server from which the currently assigned IP address is obtained.
4. In the **Port** field, type the server's port number. Default is 80.
5. 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.
6. 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. If you want to query the server to determine the IP address before the DDNS update, check **Use Check IP**. 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. From the **System** drop-down list, select the desired system registration type, either Dynamic or Custom. The default is Dynamic.
11. In the **Domain** field, type the registered Domain name.
12. Click **Submit**. If you are finished making 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

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**. The addresses are added.

Configuring the Global Positioning System (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. To configure GPS on your router:

1. From **Setup**, select **GPS Configuration**.
2. To configure the TCP server port and enable a serial port dump of NMEA sentences, see [Dumping NMEA sentence information to the router's TCP server port](#).
3. To allow your router to connect and send GPS data to a remote server, see [Sending GPS information to a remote server](#).
4. To set the time interval after which GPS data is sent, and to configure further details about the GPS information that is sent, see [Configuring NMEA Sentences](#).

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. From the **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** field.

4. To use the serial port for GPS, disable the serial port client/server. The serial port configuration settings are used to configure the port. The serial port client/server must be disabled to use the serial port for GPS.

Sending GPS information to a remote server

The Remote 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, check **TCP/UDP**.
2. From the **Protocol** drop-down list, select the protocol of the client.
3. In the **Remote Host** field, type the IP address of the remote host.
4. In the **Port** field type the port number of the remote host.
5. If your remote host requests a password, type that password in the **Password** field. The password is sent to the server in response.

Configuring NMEA Sentences

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

1. 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. To do so, check the desired options: GGA, GSA, GSV, GLL, RMC, and VTG.

Configuring the serial port

To configure the serial terminal connected to the RS-232 connector DE9 on the router:

1. From **Setup**, select **Serial IP Configuration**.
2. In the pane that appears, check **Enabled**.
3. From the **Baud Rate** drop-down list, select the baud-rate at which the serial terminal communicates. The default is 115200.
4. From the **Flow Control** drop-down list, select the flow control for the serial port. The selections are None or RTS-CTS. The default is None.
5. From the **Parity** drop-down list, select the parity for the serial port. The selections are None, Even, or Odd. The default is None.
6. To use the Modbus protocol as the protocol the serial devices use to communicate, check **Modbus**.
7. From the **Data Bits** drop-down list, select the data bits for the serial port. Data bit selection is 7 or 8. The default is 8.
8. From the **Stop Bits** drop-down list, select the stop bits for the serial port. The selections are 1 or 2. The default is 1.

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 DE9, 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 configure the IP Pipe in TCP, UDP, or SSL/TLS client mode:

1. Go to **Setup > Serial-IP Configuration** to display the **Serial Port Settings** window.
2. In the **IP Pipe** group, 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 and in the Secondary Port field, type the IP address and port number, respectively, of the alternate TCP, UDP, or SSL/TLS server.
7. 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.
8. 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.
9. Click **Submit**. If you are finished making 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 DE9, 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 configure the IP Pipe in TCP, UDP, SSL/TLS server mode:

1. Go to **Setup > Serial-IP Configuration** to display the **Serial Port Settings** window.
2. In the **IP Pipe** group, from 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**. If you are finished making changes, click **Save and Restart**.

Setting the device's date and time

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://wwp.greenwichmeantime.com/info/current-time.htm>

5. Click **Submit**. If you are finished making 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**. If you are finished making changes click **Save and Restart**.

Adding Networks Overview

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 un-do 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.

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 panel, 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 passes the IP address it receives from the cellular provider during a PPP connection to another device.

Note: In this mode, the rCell only allows one DHCP lease. Many of the services the rCell provides as a router are disabled in this mode due to the passing of its WAN IP address to another device.

- c. Click **Next**.
3. In the Choose Password panel, 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 panel, set the date, time and time zone.
 - a. In the **Time** field, type the desired time.
 - b. In the **Date** field, type the desired date.
 - c. From the **Time Zone** drop-down, 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 panel, 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 panel, 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.

c. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the router that it should only bring up the PPP connection when there is outgoing IP traffic, and that it would bring the PPP connection down after a given idle timeout.

d. In the **Idle Timeout** field, type the amount of idle time that passes before the router times out. If the time expires, the PPP connection to the Internet is disconnected. The default is 180 seconds.

Note: The Idle Timeout configuration only applies to Dial-on-Demand.

e. In the **APN** field, type the APN (Access Point Name). The APN is assigned by your wireless service provider.

Note: This configuration does not apply for rCell units with embedded CDMA/EVDO radios. For these devices, you will not be able to modify this field.

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

7. In the PPP Authentication panel:

a. From **Type**, select the authentication protocol type used to negotiate with the remote peer: pap, chap, or pap-chap. The default is pap-chap.

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 will authenticate. You can leave this field blank, if desired. Password is limited to 60 characters.

8. Click **Finish**.

Chapter 7 Setting Up Wireless Features

Setting Up Wi-Fi Access Point

Your router can be configured as a wireless access point (AP) to allow Wi-Fi enabled devices to connect to the router using Wi-Fi. The Wi-Fi access point can have up to 8 clients at a time. To set up your router as an access point:

1. Go to **Wireless > Wi-Fi** to display the **Wi-Fi** window.
2. From the **Wi-Fi Mode** dropdown list, select **Access Point**.
3. To set the SSID (service set identifier) for the access point supported by your router, in the **SSID** field, type the name. The Wi-Fi devices look for this ID in order to join the wireless network. All wireless devices on a WLAN must use the same SSID in order to communicate with the access point.
4. To specify the data rates supported, in the **Network Mode** drop-down list, select the desired option. Possible values are B/G/N-Mixed, B/G-Mixed, B-Only, and N-Only.
5. From the **Channel** drop-down list, select the channel on which the router operates. Channels 1-11 are available.
6. In the **Beacon Interval** field, enter the period of time, in milliseconds, when the access point sends a beacon packet. Beacons help synchronize a wireless network. For most applications, the default value of 100 provides good performance.
7. In the **DTIM Interval** field, enter how often a beacon frame includes a Delivery Traffic Indication Message, and this number is included in each beacon frame. It is generated within the periodic beacon at a frequency specified by the DTIM Interval. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients about the presence of buffered multicast/broadcast data on the access point. The default value of 1 provides good performance for most applications. You might want to increase this value when using battery powered Wi-Fi devices, which can sleep (at reduced power consumption) during the longer DTIM interval period. You must balance the power savings from increasing the DTIM interval against possible reduced communication throughput.
8. In the **RTS Threshold** field, type the frame size at which the AP transmissions must use the RTS/CTS protocol. This is often used to solve hidden node problems. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions.

For related information, see [Setting security options](#) and [Viewing information about Wi-Fi clients using your wireless network](#).

Setting security options

You can specify the security protocol that the router uses to secure the communications from the router to the connected devices.

1. From the **Mode** drop-down list, select the security protocol you want to use. Options include:
 - None
 - WEP**: Use Wired Equivalent Privacy protocol to allow a group of devices on the network to exchange coded messages.
 - WPA-PSK**: Use Wi-Fi protected access to secure data exchanged on your network.
 - WPA2-PSK**: Use Wi-Fi protected access version 2 to secure data exchanged on your network.
2. To configure **WEP**:

- a. From the **Encryption** drop-down list, select the encryption to be used.
 - b. To generate a key from a phrase, in the **Passphrase** field, type a phrase. Click **Generate**.
 - c. To manually enter keys, type the keys in the Key 1, Key 2, Key 3 or Key 4 fields.
3. To configure WPA-PSK and WPA2-PSK:
 - a. Select the WPA Algorithm from the drop-down list.
 - b. In the **Shared Key** field, type the key that is used for encrypting and decrypting the data.
 - c. To remove the mask characters, thereby making the Shared Key visible, check **Unmask**.
 4. When done, click **Submit**, then **Save and Restart**.

Viewing information about Wi-Fi clients using your wireless network

To view information about clients (such as computers, tablets, and smart phones) that are connected to your router's Wi-Fi access point:

1. The Clients group displays a list of clients using your router's WiFi.
2. To update the list, click **Refresh**.

Setting Up Wi-Fi as WAN

To setup the router's WiFi as WAN:

1. Go to **Wireless > Wi-Fi** to display the **Wi-Fi** window.
2. From the **Wi-Fi Mode** drop down list, select **Wi-Fi as WAN**.
3. Searching for available Wi-Fi networks starts automatically. After 30 to 60 seconds, a list of detected Wi-Fi Access Points appears in the **Available Networks** group.
4. In the **Available Wi-Fi Networks** group, click the SSID for the Wi-Fi access point you want to use. The **Add Saved Network** window opens.
5. Review the information, enter any required security info, then click **Finish**. The Wi-Fi access point you just added appears in the **Saved Wi-Fi Networks** group.
6. If desired, add additional access points to the list of Saved Networks. The router tries to connect to Saved Networks in the order they are listed. You can change the order by clicking the up or down arrows shown under **Options**.
7. When finished, click **Save and Restart**. The Status field displays "Connected" if you have successfully connected to the Wi-Fi access point.

Setting up Bluetooth

The Bluetooth-IP feature allows a data connection between a remote TCP/UDP client or server and a local Bluetooth device. To set up the Bluetooth connection:

1. Go to **Wireless > Bluetooth**
2. To enable the feature, check **Enabled**. Click **Submit**.
3. Confirm that the far-end Bluetooth device is powered on and waiting for a connection.
4. In the **Available Devices** group, click **Refresh**. A list of detected Bluetooth devices appears.
5. Click the name of the Bluetooth device that you want to use. The name and MAC address appear under the selected device.

IP Pipe in TCP/UDP Server mode

1. In the **IP Pipe** group, from the Mode drop-down list, select **SERVER**.
2. From the **Protocol** drop-down list, select the desired protocol, either TCP or UDP.
3. In the **Server Port** field, type the desired port value in the range 1 to 65535.
4. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:
 - Always Connected
 - Sequence A sequence of characters received from the Bluetooth side used to disconnect the IP pipe.
 - Timeout The IP pipe connection disconnects if the configured timer expires with no data sent or received.

To configure the IP Pipe in TCP/UDP Client mode:

1. In the **IP Pipe** group, from the Mode drop-down list, select **CLIENT**.
2. From the **Protocol** drop-down list, select the desired protocol, either TCP or UDP.
3. In the **Server IP Address** field, type the address of the far-end TCP-UDP server.
4. In the **Server Port** field, type the port value used by the far-end TCP/UDP Server.
5. In case the primary server is unavailable, in the **Secondary IP Address** field and in the **Secondary Port** field, type the IP address and port number, respectively, of the alternate TCP/UDP server.
6. From the **Connection Activation** drop-down list, select a connection method. Options are:
 - Always On
 - CR Three carriage returns must be received from the Bluetooth side before TCP/UDP connection is established to the remote server.
7. From the **Connection Termination** drop-down list select a disconnect method for the IP pipe. Options are:
 - Always Connected
 - Sequence A sequence of characters received from the Bluetooth side used to disconnect the IP pipe
 - Timeout The IP pipe connection disconnects if the configured timer expires with no data sent or received
8. Click **Submit**.

After you are finished with configuring the Bluetooth feature, Save and Restart.

The router immediately connects to the local bluetooth device. If successful the Status field displays Connected. If IP Pipe is configured for SERVER, the IP connection is initiated by the far-end TCP/UDP client.

If Mode is set to Client, the router initiates connections for the far-end TCP/UDP server based on the configured Connection Activation conditions are met.

Chapter 8 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. In the Port Forwarding group, click **Add Rule**.
2. Enter a name and description. Click **Next**.
3. In the IP Forwarding DNAT pane, enter the following:

In the **External WAN Ports** 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.

In the **Destination LAN IP** field, type the IP address of the device packets will be forwarded to. The attached drop-down list contains DHCP leased and Saved Network addresses.

In the **Destination LAN Ports** 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.

From the **Protocol** drop-down list, select the protocol of the messages that can be forwarded.

A default filter allowing forwarded packets through the firewall is automatically created. If desired you can use the Advanced Setting mode of the Port Forwarding wizard to further restrict packets based on source address and source ports. In most cases this is not necessary.

4. Click **Finish**.

Adding Outbound Traffic Rules

To prevent a device within the LAN from communicating with a device in an external network, a rule has to be established in the firewall to drop packets destined to the external device.

1. Click **Add Rule** in the Outbound Traffic section.
2. Enter a name and description. Click **Next**.
3. In the **Destination IP** field, type the IP address of the device or network packets are being 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 packets are destined for. 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 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.

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. From **Firewall**, select **Static Routes**.
2. In the pane that appears, click **Add Route**.
3. In the **Name** field, 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**.

Chapter 9 Setting Up Cellular Features

Configuring Cellular

To configure how cellular is used on your router:

1. Go to **Cellular > Cellular Configuration** to display the **Cellular Configuration** window.
2. Check the **Enabled** box.
3. For GSM radios, enter the APN in the field located in the **Modem Configuration** section of the window.
4. Click **Submit**.

For field descriptions see Cellular Configuration Fields.

Cellular Configuration Fields

Field	Description
General Configuration	
Enabled	Allows the router to establish a cellular PPP connection (Cellular WAN).
Dial-on-Demand	Enables or disables 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
Idle Timeout	When Dial-On-Demand is enabled and no network traffic occurs for the given amount of time, the cellular link disconnects. (Only applies to Dial-On-Demand.)
Diversity	Allows the use of two antennas to increase receive signal quality Not all models support diversity. If diversity is enabled, connect a second cellular antenna to the AUX port on the device. Otherwise, the cellular performance of the device may degrade.
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; 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 and #777 for CDMA.
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.

Field	Description
Sim Pin	The pin used to unlock SIM for use (only required if SIM is locked). This does not apply to CDMA radios.
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: 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	Enable or disable active keep alive check.
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 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.
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, so there may be situations where due to no network traffic, the monitor will 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

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.

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.
4. Click **Submit**.

Note: This feature only defines when the device should bring up its cellular link, not when the device should bring 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 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:
 - 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.
Dial On Demand LAN	When checked, the router will allow 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 SMS.
Time Delay	Time that passes between receiving call and initiation the Wake Up On Call connection.

Field	Description
Acknowledgment String to Caller	String used to acknowledge (to the delivering SMSC) 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 redirector 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 **Cellular**, select **Telnet Radio Access**.
2. In the pane that appears, 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 redirector software on your computer to communicate to the cellular modem integrated on the router.
5. In the **Port** field, type the serial Auto Dialout Port number. The default is 5000.
6. In the **Inactivity** field, type 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**.

Radio Status

Field	Description
Module Information	
IMEI	International Mobile Station Equipment Identifier (not available for C2 or EV3 models)
MEID	Mobile Equipment Identifier (C2 or EV3 models only)
IMSI	International Mobile Subscriber Identifier
Manufacturer	Company that developed the cellular module
Model Number	Manufacturer model ID
Hardware Revision	Module's hardware revision
MDN (Phone Number)	Mobile Directory Number
MSID	Mobile Station ID
Firmware Version	Module's firmware version
Service Information	

Field	Description
Home Network	Cellular service provider associated with the module's data account
Current Network	Current cellular service operator (Not available for C2 or EV3 models)
RSSI	Received Signal Strength Indication
Service	Cellular service connection type
Roaming	Indicates whether or not current service is provided by Home Network carrier
Provisioned	Indicates whether or not the device has been activated (C2 and EV3 models only)
	Note: Some radios and cellular services provide additional details, which may be found under an Engineering Details section.
Update Options	
This section provides the ability to update certain radio specific configurations. Note: Sprint models have additional OMA DM and Mobile IP update options	
MDN (Phone Number)	Update the cellular module's phone number(this is only updated on the device, it does not change the MDN the carrier has associated with this device)

Chapter 10 Configuring SMS

Configuring SMS

To enable SMS messaging via the web UI or API:

1. Go to **SMS > SMS Configuration**.
2. Check **Enabled**
3. Set messages to keep and resend options.
4. Click **Submit**.

For field descriptions see SMS Field Descriptions.

SMS Field Descriptions

Field	Description
Enabled	Enables the SMS utilities required to send SMS via API and web UI.
Sent SMS to Keep	The total number of sent SMS messages to keep in the device's history.
Received SMS to Keep	The total number of received SMS messages to keep in the device's history.
Resend Failed SMS	The total number of resend attempts for SMS messages that failed to send.

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 cross icon) 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 the **Delete All** button. 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 "cross" icon 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 the **Delete All** button. A dialog box asks you to confirm that you want to delete all the SMS messages. Click **OK**.

Chapter 11 Defining Tunnels

Setting up Generic Routing Encapsulation (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 **Tunnels**, select **GRE Tunnels**. The Tunnels: GRE Tunnels pane opens.
2. From the Tunnels:GRE Tunnels pane, click **Add Tunnel**. A series of wizard panels helps you configure the connection.
3. In the **Tunnel Name** field, enter a name for the new tunnel.
4. In the description area, type 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 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 **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**.

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. There is a two stage negotiation process to setting up an IPsec tunnel. 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 there are additional options that 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 are: SHA-1, SHA-2, and MD5.

The default set of DH Group Algorithms are: 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 setup a Network-to-Network VPN tunnel on your router:

1. Go to **Tunnels > IPsec Tunnels**.
2. Click **Add Tunnel** in upper right.
3. Enter a name for the tunnel.
4. Click **Next**.
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.
10. Click **Next**.
11. If the remote endpoint is setup with unique IDs, check the **Enable UID** box, and enter the Local and Remote IDs.
12. Click **Finish**.

For field descriptions see IPsec Tunnel Configuration Field Descriptions

IPsec Tunnel Configuration Field Descriptions

Field	Description
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.
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. 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, and describes the remote endpoint's subnet. This is used to identify 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.
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 phase 1 and 2 are specified by the user.
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.
LocalID	String identifier for the local security gateway.
RemotelD	String identifier for the remote security gateway.
Compression	Enable IPComp. This protocol will increase the overall communication performance by compressing the datagrams through. This 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. This mode is faster to negotiate phase 1. The downside is that the authentication hash is transmitted unencrypted. It's possible to capture the hash and start a dictionary or brute force attacks to recover the PSK.

Chapter 12 Device Administration

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 Conduit. 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.

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.

The Conduit mLinux Model is shown. The RESET button is in the same location on both Conduit models.

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.

Web Server

HTTP Redirect to HTTPS:

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

Note: The router can be configured to allow HTTP access to its RESTFUL JSON API. This is intended to allow embedded devices that do not have SSL/TLS or HTTPS capabilities to configure, monitor, and control the router. Please see the MTR API Developer Guide for more information.

Field	Description
Enabled	Enables HTTP to HTTPS redirect. This will automatically redirect users trying to access the device via HTTP to HTTPS.

Field	Description
Port	The port the router will listen for HTTP requests on.
Via LAN	If checked, the router will listen and respond to HTTP requests from the LAN.
Via WAN	If checked, the router will listen and respond to HTTP requests from the WAN.

HTTPS:

The router provides secure Web UI 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 ICMP responses.
Via LAN	If checked, the router will respond to ICMP traffic from the LAN, such as ping requests.
Via WAN	If checked, the router will respond to ICMP traffic from the WAN, such as ping requests. This increases susceptibility to malicious activity.

IP Defense

A set of rules that decrease susceptibility to malicious activity. If these settings are configured too strictly, they may interfere with non-malicious activity.

DoS Prevention:

This engages a set of rules at the firewall that prevents Denial-of-Service attacks by limiting the amount of new connection requests to the router.

Field	Description
Enabled	Enables the DoS prevention.

Field	Description
Per Minute	Allowed 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, drop the packet.
Burst	Number of burst points. 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.

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.

Field	Description
Enabled	Enables the Ping Limit feature.
Per Minute	Allowed number of pings per second before burst points are consumed. Once burst points run out, ICMP packets will be dropped.
Burst	Number of burst points. On a period where the "Per Second" limit is not reached, one burst point is regained, up to this maximum.

Brute Force Protection:

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.

Field	Description
Enabled	Enables the Brute Force Prevention feature.
Attempts	The number of failed attempts allowed before the user's account is locked out.
Lockout Minutes	The number of minutes an account is locked out before a new login attempt will be accepted.

Configuring IP defense

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

Denial of service (DOS) attack

To mitigate the effects of a denial of service attack:

1. Check **Enabled**.
2. In the **Per Minute** field, type the average number of pings per minute.
3. In the **Burst** field, type the allowed burst for traffic spikes.

Ping limit

To mitigate the effects of a ping DoS on your router:

1. Check **Enable**.
2. In the **Per Second** field, type the average number of ICMP pings to the router.
3. To limit the burst of traffic from any source, in the **Burst** field, type the allowed burst for traffic spikes.

Brute force

To foil brute force, password-guessing attacks:

1. Check **Enabled**.
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.
3. In the **Lockout Minutes** field, type the number of minutes that an account is locked out after login attempts fail.

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 **Country** field, enter the 2-letter code for the country name.
5. In the **State/Province** field, enter the state or province for which the certificate is valid.
6. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
7. In the **Organization** field, enter the organization name for which the certificate is valid.
8. 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.
9. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.
10. If you are finished making 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. Choose a valid certificate file.
4. Click **Save**. Wait until the file is uploaded.
5. If you are finished making changes, click **Save and Restart**.

Setting up the Remote Server

1. 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 ID** field type the account key received from the Multi Tech Remote Management Administrator. The device is not allowed to connect to the Remote Management Server without a valid account key .

Managing Your Device Remotely with Multi-Tech Device Manager

Multi-Tech Device Manager can monitor devices, perform remote software and configuration updates, and reboot devices.

To configure your device to use Multi-Tech Device Manager:

1. From **Administration**, select **Remote Management**.
2. On the page the opens, check **Enabled**.
3. To use a secure connection, check **SSL Enabled**.
4. In the Account ID field, type the account key that you receive. You might find it easier to copy and paste this key into the field.
5. If you want the device to connect to Multi-Tech Device Manager 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 Multi-Tech Device Manager, and the device only connects to Multi-Tech Device Manager when other traffic brings up the link.

6. To define how often the device connects to Multi-Tech Device Manager 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 Multi-Tech Device Manager every 4 hours, at a minimum. If you set the check-in interval to less than 4 hours, your change is ignored.

7. To define how often the device connects to Multi-Tech Device Manager to send GPS data, set the GPS Data Interval field to the desired number of minutes, between 1-10080 (1 minute to 1 week).

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 that displays information that can be used to support users:

1. To enable display of the custom support information, check **Show Custom Info**.
2. Type the desired information into the fields. For example, type the desired zip code in the **Zip Code** field, a city name in the **City** field, and so on.
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**.

To delete an existing image, click **Remove Image**.

Specifying Device Settings

To define other custom settings for devices:

1. In the **Device Name** field, type a name to identify the device.
2. In the **Custom ID** field, type an identifier for the device.
3. You can change the color of the interface's buttons, button fonts, highlights and highlight font by specifying red, green, and blue settings in their respective fields. Use the format #rrggbb to define the desired color in the respective field.
4. To add a favorite icon, also known as a shortcut icon or bookmark icon, in the **Custom Fav Icon** field, click **Browse**, navigate to the area where the file for the Fav icon resides, and select the desired file.
5. To add a custom logo, next to the Custom Logo field, click **Browse**. Navigate to the area where the logo resides, select the desired file.
6. Click **Submit**.

Upgrading firmware

Use this feature to upgrade the router's firmware to the latest version. You can download firmware upgrades from the Multi-Tech website.

Before you begin

Before you upgrade your firmware, save your present configuration as a backup.

To upgrade the firmware on your device:

1. Go to the Multi-Tech website, locate the firmware upgrade file you want for your router, and download this file to a known location.
2. From **Administration**, select **Firmware Upgrade**. The Administration: Firmware Upgrade pane opens.
3. 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 **Browse**. Navigate to the location of the file that is the firmware version you want to apply to your router.
 - b. In this location select the file name and click **Open**. The file name appears in the Firmware Upgrade File field. Make sure you select the correct BIN file; otherwise, your router can become inoperable.
4. Click **Start Upgrade**.
5. 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.

Note:

- The new firmware is written into flash memory.
- It may take up to five minutes to upgrade the router's firmware. Do not interfere with the router's power or press the router's reset button during this time.
- The Multi-Tech Device Manager 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.
- After the firmware upgrade is complete, verify your configuration to make sure it is what you expected.

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. From the navigation bar, select **Administration**, then **Save/Restore**.
2. To restore a previous configuration:
 - a. Next to the Restore Configuration field, click **Browse**.
 - b. Navigate to the location where the configuration file is stored and select the desired file.
 - c. Click **Restore**. The device reboots.
3. To restore the router's configuration to the factory default settings:
 - a. Next to the Restore Factory Defaults field, click **Restore**.
 - b. A dialog box appears, asking you to confirm that you want to restore factory default settings.
 - c. Click **OK**.
4. 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. In the dialog box that appears, 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 at a particular hour 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**.

See also: Statistics Configuration Fields

Automatically rebooting the device

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

1. In the **Auto Reboot Timer** field, type the number of hours that lapse before the device automatically reboots itself. The range you can enter is 0 to 999.
2. If you do NOT want the device to automatically reboot, set the time to 0. The default setting is 0.

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.

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	

Field	Description
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 .

Chapter 13 Device Status

Viewing device statistics

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

1. From **Status**, select **Statistics**.
2. The application categorizes statistics about your device. To see statistics that appear in a particular category, click the appropriate tab.
 - System
 - Ethernet
 - Wireless
 - PPP
 - Serial
 - Bluetooth
 - GRE .
 - IPSec
3. A data usage bar chart and a cumulative usage line chart are available for Ethernet, Wi-Fi, and Cellular. The Data Usage bar chart also shows statistics for data sent and data received.
 - Total:** displays the total number of sent/received bytes for a 365-day period.
 - Today:** displays the total number of sent/received bytes for today.
 - Sessions:**
 - Packets:** Number of successfully transmitted (TX) and received (RX) packets.
 - Errors:** Number of errors that occurred. Possibly due to connection issues or network congestion.
 - 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.
4. Click **Show Cumulative Usage** or **Show Daily Usage** to display the desired view. Default chart view is Daily Usage for 30-day period.
5. 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**.
6. **Show Log:** The associated runtime logs for this section.

Mail Log

Go to **Status & Logs > Mail Log** to display the **Mail Log** window. This window shows the recent email delivery attempts and the mail log details. Mail log entries are sorted by date with the most recent on top.

You can select the number of emails to display in the queue. Possible values are 5, 10, 25, 50, or all the emails.

To see the delivery details, click the "eye" icon under **Options** for the desired email entry.

To delete all mail log entries, click **Purge Log**.

Note: Logs do not persist through power cycles.

Mail Queue

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

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 the emails.

To view the delivery details for an individual email, click the "eye" icon under **Options** for the desired email entry.

To delete all mail log entries, click **Purge Log**.

Note: Logs do not persist through power cycles.

RF Survey

The RF Survey tool allows you to view the list of the cell towers that belong to the carrier and their signal quality details such as Signal Level and Signal Noise Ratio. You need a SIM card to acquire the list of available cell towers.

Note: Selecting this tool terminates any existing PPP connection

Click **Status & Logs > RF Survey** to open the **RF Survey** page. The search for the cell towers can take up to 2 minutes. While the search is in progress, the wait icon is displayed.

The cell tower to which the router is currently connected displays at the top of the list.

To view the Signal Strength chart of a carrier, under **Options**, click the "eye" icon for the carrier. The **Carrier Details** window appears. This feature can help you decide which area has better signal strength and thus a better location for the router.

Service Statistics

Click **Status & Logs > Services** to display the **Service Statistics** window. 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
- Failover

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 condition 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 Wi-Fi History	Deletes all Wi-Fi history on the router.
Delete Cellular History	Deletes all Cellular history on the router.
Delete Ethernet History	Deletes all Ethernet history on the router.

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

FCC and IC Antenna Requirements Toward License Exempt Radio Transmitters (Bluetooth/WLAN)

The license-exempt Bluetooth/WLAN radio transmitter contained in this equipment may only be operated with an antenna of a type, a maximum gain and the required antenna impedance as approved and specified below. To reduce potential radio interference to other users, choose the antenna type and its gain so that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

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 image shows the CE mark, which consists of the letters 'C' and 'E' in a stylized font, followed by the number '0682'. The 'C' and 'E' are larger and more prominent than the number.

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。