

MultiConnect® rCell 100

MTR-H5 User Guide



MultiConnect® rCell 100 Series Router User Guide

Model: MTR-H5

Part Number: S000566 Version: 4.0

Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2018 by Multi-Tech Systems, Inc.**

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

Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Legal Notices

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

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

Trademarks and Registered Trademarks

MultiTech, and the MultiTech logo, DeviceHQ, and MultiConnect are registered trademarks and Conduit is a trademark of Multi-Tech Systems, Inc. All other products and technologies are the trademarks or registered trademarks of their respective holders.

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 Wooddale Drive, Mounds View, MN 55112

Phone: (800) 328-9717 or (763) 785-3500

Fax (763) 785-9874

Contents

Chapter 1 – Product Overview	8
About MultiConnect rCell 100 Series Router	8
Documentation	9
Product Build Options	9
Descriptions of LEDs.....	10
Side Panel Connectors	11
Ethernet LED Descriptions	12
Specifications	12
Frequency Bands (H5).....	13
HE910 Telit Transmission Output Power	14
Dimensions.....	15
Label locations	15
Power Draw.....	18
RF Specifications	18
Additional RF Specifications.....	18
Bluetooth Specifications	19
WLAN Specifications (Wi-Fi).....	20
Chapter 2 – Safety Warnings	21
Lithium Battery	21
ITE Equipment Ordinary Locations (US, Canada, and Europe)	21
Class I, Division 2, Groups A, B, C, and D Hazardous Locations (US and Canada)	21
ATEX (Europe only)	22
Hazardous Location Special Considerations	22
Ethernet Ports	22
User Responsibility.....	22
Power Supply Caution.....	23
Device Maintenance	23
Vehicle Safety.....	23
Radio Frequency (RF) Safety	24
Interference with Pacemakers and Other Medical Devices	24
Potential interference	24
Precautions for pacemaker wearers	24
Notice regarding Compliance with FCC, EU, and Industry Canada Requirements for RF Exposure.....	25
Chapter 3 – Cellular Information	26
Antenna System Cellular Devices.....	26
HEPTA Antenna Information.....	26
Authorized Antenna/Antenna Specifications for Cellular Bands	26

3G Antenna Requirements/Specifications	26
GPS Antenna Specifications	27
MultiTech Ordering Information.....	27
Antenna Specifications.....	27
Bluetooth and Wi-Fi Antennas	27
Multi-Tech Ordering Information	27
Antenna Specifications.....	28
Chapter 4 – Installing the Router	29
Installing the Router.....	29
Using Diversity	29
Mounting the Device.....	30
Installing the SIM Card	30
Setting up Wi-Fi.....	30
Resetting the Device	30
Restoring User Defined Settings to the Device	31
Notice for Devices that Use Aeris Radios.....	31
Chapter 5 – Using the Wizard to Configure Your Device.....	32
First-Time Setup	32
Chapter 6 – Configuring Your Device.....	35
Home Page (Dashboard)	35
Time Configuration	36
Setting the Date and Time	36
Configuring SNTP to Update Date and Time	37
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	37
Configuring IP Address and DNS Information for LAN	37
WAN Setup.....	37
Editing Failover Configuration.....	38
Failover Configuration Fields	38
Configuring Dynamic Domain Naming System (DDNS)	39
Entering authentication information	39
Forcing a DDNS server update	39
Configuring Dynamic Host Configuration Protocol (DHCP) Server	40
Assigning Fixed Addresses	40
Configuring the Global Positioning System (GPS).....	40
GPS Server Configuration.....	40
Dumping NMEA Sentence Information to the Router's TCP Server Port	41
Sending GPS information to a remote server	41
Configuring NMEA Sentences	41
SMTP Settings	42
Configuring the Serial Port	42
Configuring Device to Act as Client	43

Configuring Device to Act as Server	44
Adding Saved Networks	45
Adding Networks.....	45
Editing or Deleting an Existing Network	45
Configuring SNMP	45
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	47
Chapter 7 – Setting Up Wireless Features	48
Setting Up Wi-Fi Access Point	48
Setting Security Options	48
Viewing Information About Wi-Fi Clients Using Your Wireless Network	49
Setting Up Wi-Fi as WAN	49
Setting up Bluetooth	50
IP Pipe in TCP/UDP Server mode	50
Chapter 8 – Setting Up the Firewall.....	52
Defining firewall rules	52
Inbound Forwarding Rule	52
Input Filter Rules	52
Output Filter Rules	53
Advanced Settings.....	54
Prerouting Rule	54
Postrouting Rule.....	55
Trusted IP	55
Setting up Static Routes	56
Chapter 9 – Setting Up Cellular Features	57
Configuring Cellular.....	57
Cellular Configuration Fields	57
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	59
Configuring Wake Up On Call.....	59
Wake Up On Call Method Settings	59
Wake Up On Call General Configurations	59
Using Telnet to Communicate with the Cellular Radio.....	60
Radio Status	61
Telit Radio Firmware Upgrade	61
Upgrading Cellular Firmware Using DeviceHQ (Remote Management).....	61
Upgrading Cellular Firmware using UI only	62
Chapter 10 – Configuring SMS.....	63
Configuring SMS.....	63
SMS Field Descriptions.....	63
SMS Commands	63
Sending an SMS Message.....	65
Viewing Received SMS Messages	65

Viewing Sent SMS Messages.....	65
Chapter 11 – Defining Tunnels	67
Setting Up GRE Tunnels	67
Configuring Network-to-Network Virtual Private Networks (VPNs)	67
IPsec Tunnel Configuration Field Descriptions	69
OpenVPN Tunnels	71
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	79
Chapter 12 – Device Administration.....	80
User Accounts	80
Self-Diagnostic.....	81
Configuring Device Access	82
HTTP Redirect to HTTPS	82
HTTPS	82
HTTPS Security	83
SSH	83
SSH Security	83
ICMP	84
SNMP.....	84
Modbus Slave.....	84
IP Defense	84
RADIUS Configuration	85
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	87
Generating a New Certificate.....	87
Importing a Certificate	87
Uploading CA Certificate	88
Setting up the Remote Management	88
Managing Your Device Remotely	88
Unavailable Services in PPP-IP Passthrough and Serial Modem Modes.....	89
Notifications.....	89
Customizing the User Interface	93
Customizing Support Information	93
Specifying Device Settings	94
Upgrading Firmware	94
Saving and Restoring Settings	95
Using the Debugging Options	96
Automatically rebooting the device.....	96
Setting up Telnet.....	97
Configuring Remote Syslog	97
Statistics Settings	97
Ping and Reset Options.....	98
Usage Policy	98

Chapter 13 – Device Status	99
Viewing Device Statistics	99
Mail Log.....	100
Mail Queue.....	100
RF Survey.....	100
Service Statistics.....	101
Statistics Configuration Fields.....	101
Notifications Sent.....	101
Chapter 14 – Regulatory Information	102
47 CFR Part 15 Regulation Class B Devices	102
Industry Canada Class B Notice.....	102
FCC Interference Notice	102
FCC and IC Antenna Requirements Toward License Exempt Radio Transmitters (Bluetooth/WLAN)	103
Requirements for Cellular Antennas with regard to FCC/IC Compliance	103
EMC, Safety, and Radio Equipment Directive (RED) Compliance	103
Restriction of the Use of Hazardous Substances (RoHS)	103
REACH Statement	104
Registration of Substances.....	104
Substances of Very High Concern (SVHC)	104
Waste Electrical and Electronic Equipment Statement	104
WEEE Directive.....	104
Instructions for Disposal of WEEE by Users in the European Union	105
Information on HS/TS Substances According to Chinese Standards	106
Information on HS/TS Substances According to Chinese Standards (in Chinese)	107

Chapter 1 – Product Overview

About MultiConnect rCell 100 Series Router

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

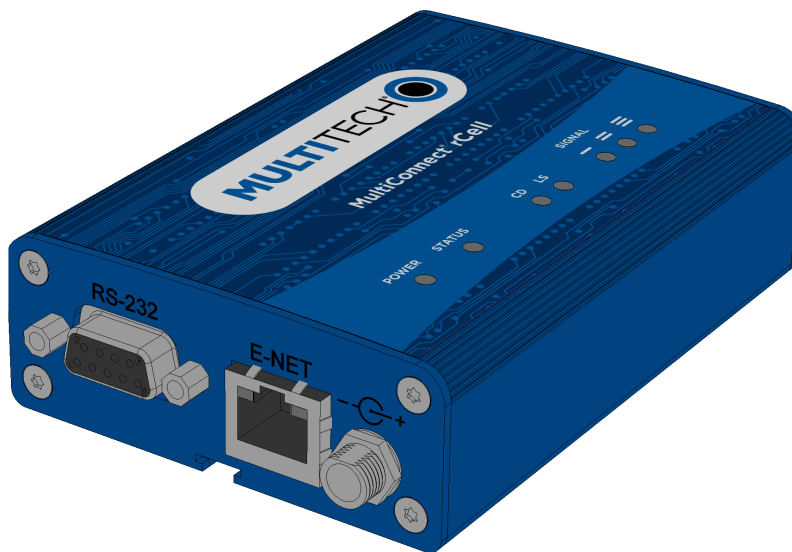
Some device models support:

- Bluetooth communication to devices with this technology
- Wi-Fi communication to devices with this technology
- GPS capability

What's New in This Release

Manual version	Update description
2.8	Modbus Slave, Cellular Radio Firmware Upgrade (H5 and H6 only)
3.0	Improvements to Firewall settings, User Accounts, Radius Configuration, and Commissioning Mode (First-Time Setup)
4.0	Trusted IP, Self-Diagnostic, Signed upgrade file (integrity check), improved security (authentication, encryption, and cipher suites), and more items for Notifications

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.

Intended use: office/home/light industrial

Documentation

The following table describes additional documentation for your device. The documentation is available on the Multi-Tech Installation Resources website at <http://www.multitech.com/brands/multiconnect-rcell-100-series>.

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. Documentation is available on the MultiTech Developer Resources website at http://www.multitech.net/developer/software/mtr-api-reference/ .
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:

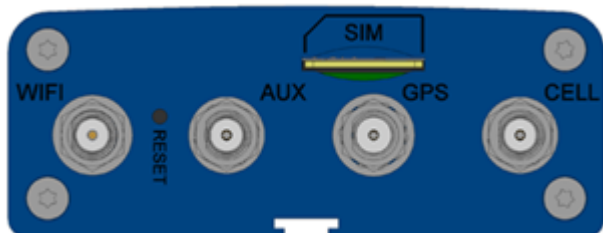
- Power and Status LEDs—The Power LED indicates that DC power is present and the Status LED blinks when the unit is functioning normally.
- Wi-Fi—Indicates if the device is serving as a Wi-Fi access point or acting as a Wi-Fi client. Not all models support Wi-Fi.
- Modem LEDs—Two modem LEDs indicate 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.
Wi-Fi	<p>Infrastructure mode:</p> <ul style="list-style-type: none"> ■ The Wi-Fi LED is lit when Wi-Fi 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 Wi-Fi LED is lit when Wi-Fi client mode is enabled. ■ The Wi-Fi LED blinks slowly when associated with an Access Point. ■ The Wi-Fi 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 (RSSI range: 0 - 31)</p> <p>ALL OFF — Unit is off, not registered on network, or extremely weak signal (0 <= RSSI < 6).</p> <p>1 Bar "ON" — Very weak signal (7 <= RSSI <14).</p> <p>1 Bar and 2 Bar "ON" — Weak signal (15 <= RSSI <23).</p> <p>1 Bar, 2 Bar, and 3 Bar "ON" — Good signal (24 <= RSSI >= 31).</p>

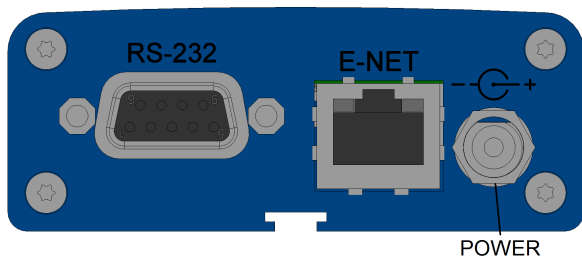
Side Panel Connectors

The device has connectors on both sides of the housing. The right side of the device contains a SIM card holder, a reset button, a GPS antenna connector, and a cellular-auxiliary antenna connector pair. Depending on the model of your device, the GPS and WiFi 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 the power receptacle.



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

Label	Description
CELL, AUX	Cellular antenna inputs. Use with the Laird HEPTA-SM MAF94300 antenna supplied with the device if ordered as a bundle. <ul style="list-style-type: none"> CELL - Primary. AUX - Diversity.
GPS	GPS antenna input. Use with the Trimble GPS antenna 66800-52 supplied with the device when ordered as a bundle. Used only on the B08 and B10 models.
WiFi	Wi-Fi antenna input. Use with the Taoglas Antenna Solutions GW.11.A153 antenna supplied with the device if ordered as a bundle.
SIM	Receptacle for a SIM card (Subscriber Identity Module).
RESET	Resets the device. Refer to Resetting the Device or Resetting User Defined Settings to the Device .
RS-232	DE 9-pin, female-D Sub through-hole connector.
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.


Label	Description
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	
Frequencies	Refer to the following Frequency Bands table for details.
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
Wi-Fi	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

Category	Description
Environment	
Operating Temperature ²	-40° C to +60° C
Humidity	Relative humidity 15% to 93% non-condensing
Certifications, Compliance, Warranty	
EMC/Radio Compliance	EN55032 Class B
	EN 301 511
	EN 301 489-1
	EN 301 489-52
	EN 301 908-1
	EN 301 908-2
	CE RED Radio/SAR
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
	EN 60950-1:2006+A11:2009+A1:2010+A12:2011/A2:2013
Network Compliance	GCF
Warranty	Two years

Note: * Not used in Brazil.

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

²For information regarding extended range, please contact MultiTech.

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

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

Frequency Bands (H5)

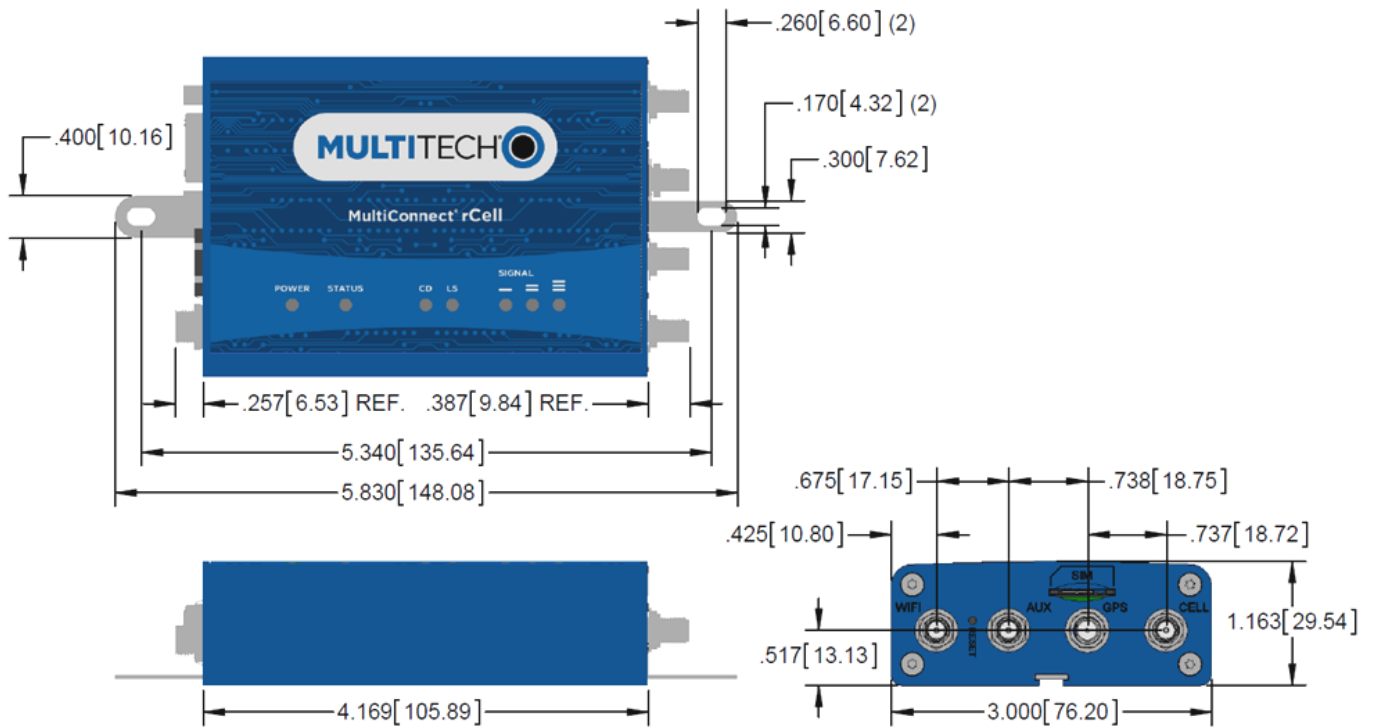
Mode	Freq. TX (MHz)	Freq. RX (MHz)	Channels	TX - RX offset
GSM850	824.2- 848.8	869.2 - 893.8	128 - 251	45 MHz

Mode	Freq. TX (MHz)	Freq. RX (MHz)	Channels	TX - RX offset
EGSM900	890.0 - 914.8	935.0 - 959.8	0 - 124	45 MHz
	880.2 - 889.8	925.2 - 934.8	975 - 1023	45 MHz
DCS1800	1710.2 - 1784.8	1805.2 - 1879.8	512 - 885	95MHz
PCS1900	1850.2 - 1909.8	1930.2 - 1989.8	512 - 810	80MHz
WCDMA850 (band V)	826.4 - 846.6	871.4 - 891.6	Tx: 4132 - 4233 Rx: 4357 - 4458	45MHz
WCDMA900 (band VIII)	882.4 - 912.6	927.4 - 957.6	Tx: 2712 - 2863 Rx: 2937 - 3088	45MHz
WCDMA1700 (band IV)	1710.4 - 1755.6	2112.4 - 2167.6	Tx: 1312 - 1513 Rx: 9662 - 9938	400MHz
WCDMA1900 (band II)	1852.4 - 1907.6	1932.4 - 1987.6	Tx: 9262 - 9538 Rx: 9662 - 9938	80MHz
WCDMA2100 (band I)	1922.4 - 1977.6	2112.4 - 2167.6	Tx: 9612 - 9888 Rx: 10562 - 10838	190MHz

HE910 Telit Transmission Output Power

Band	Power Class
GSM 850/900 MHz	4 (2W)
DCS 1800, PCS 1900 MHz	1 (1W)
EDGE, 850/900 MHz	E2 (0.557W)
EDGE, 1800/1900 MHz	Class E2 (0.4W)
WCDMA 850/900, AWS 1700, 1900/2100 MHz	Class 3 (0.25W)

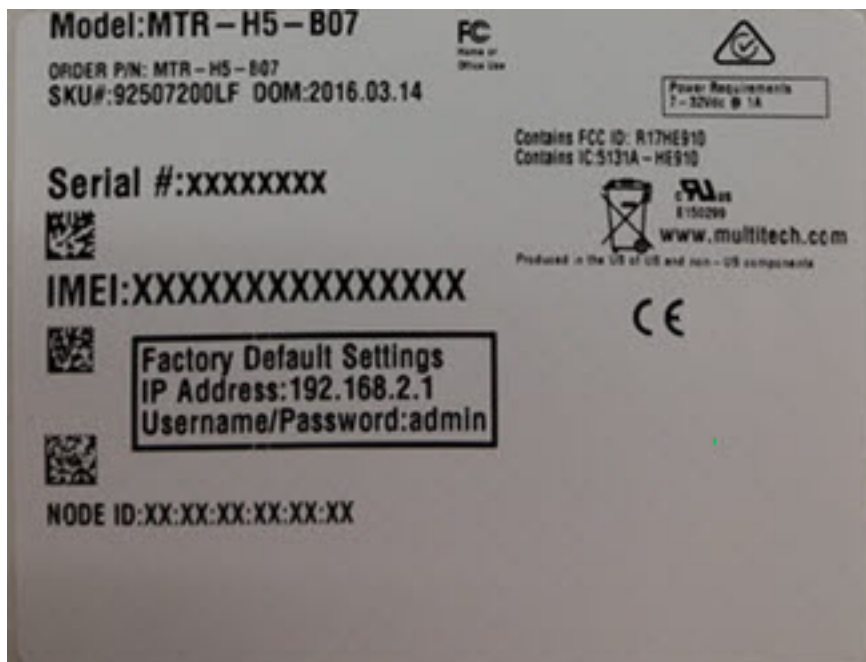
Dimensions

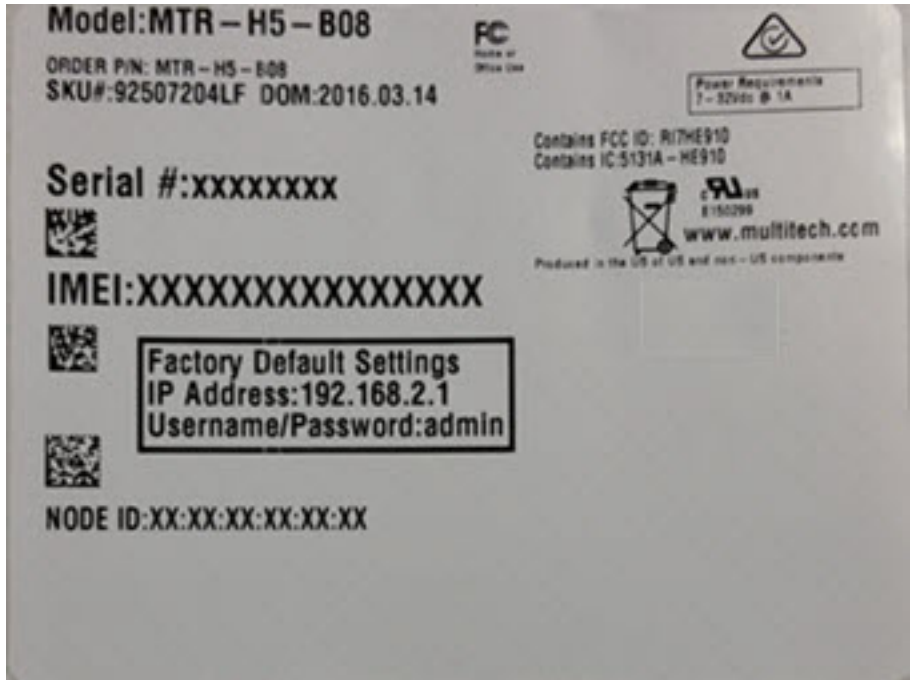


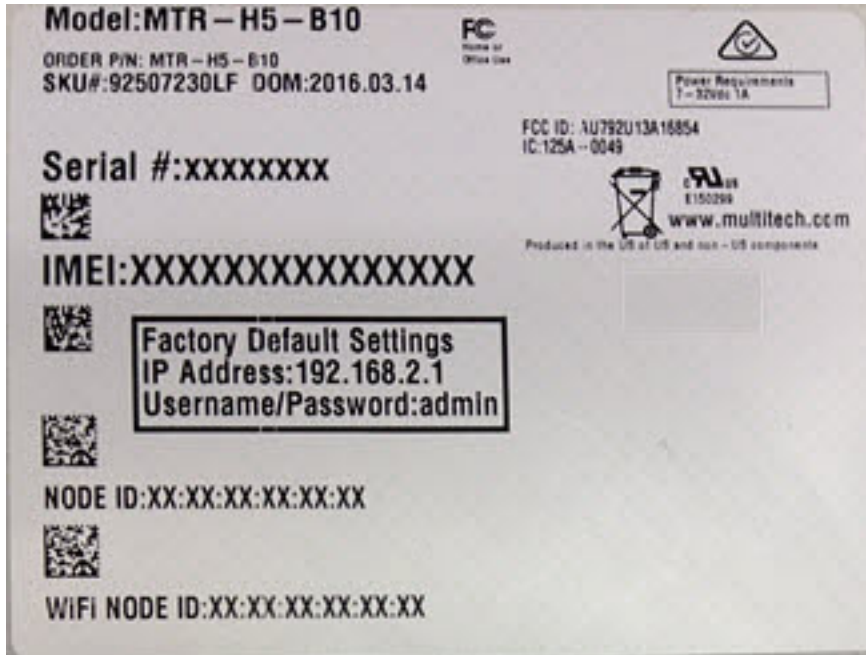
DIMENSIONS IN In [mm]

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 850 MHz	0.239	0.589	1.67	2.09
HSDPA	N/A	0.797	0.808	N/A
9.0 Volts				
GSM 850 MHz	0.206	0.315	1.06	1.86
HSDPA	N/A	0.606	0.624	N/A
32.0 Volts				
GSM 850 MHz	0.067	0.151	0.356	0.720
HSDPA	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. The above power draw numbers are measurements from an MTR-H5-B10.

RF Specifications

Mode	Frequency TX (MHz)	Frequency RX (MHz)	Channels	TX - RX Offset (MHz)
GSM850	824 to 849	869 to 894	128 to 251	45
EGSM900	890 to 915	935 to 960	0 to 124	45
	880 to 890	925 to 935	975 to 1023	45
DCS1800	1710 to 1785	1805 to 1880	512 to 885	95
PCS1900	1850 to 1910	1930 to 1990	512 to 810	80

Additional RF Specifications

Mode	Frequency TX (MHz)	Frequency RX (MHz)	Channels	TX - RX Offset
WCDMA800 * (Band VI)	830 to 840	875 to 885	TX: 4162 to 4188 Additional: 812, 837 RX: 4387 to 4413 Additional: 1037, 1062	45 MHz
WCDMA800 * (Band XIX)	830 to 845	875 to 890	TX: 312 to 363 Additional: 387, 412, 437 RX: 712 to 763 Additional: 787, 812, 837	45 MHz

Mode	Frequency TX (MHz)	Frequency RX (MHz)	Channels	TX - RX Offset
WCDMA850 (Band V)	824 to 849	869 to 894	TX: 4132 to 4233 Additional: 782, 787, 807, 812, 837, 862 RX: 4357 to 4458 Additional: 1007, 1012, 1032, 1037, 1062, 1087	45 MHz
WCDMA900 (Band VIII)	880 to 915	925 to 960	TX: 2712 to 2863 RX: 2937 to 3088	45 MHz
WCDMA1700 * (Band IV)	1710 to 1755	2110 to 2155	TX: 1312 to 1513 Additional: 1662, 1687, 1712, 1737, 1762, 1787, 1812, 1837, 1862 RX: 1537 to 1738 Additional: 1887, 1912, 1937, 1962, 1987, 2012, 2037, 2062, 2087	400 MHz
WCDMA1900 (Band II)	1850 to 1910	1930 to 1990	TX: 9262 to 9538 Additional: 12, 37, 62, 87, 112, 137, 162, 187, 212, 237, 262, 287 RX: 9662 to 9938 Additional: 412, 437, 462, 487, 512, 537, 562, 587, 612, 637, 662, 687	80 MHz
WCDMA2100 (Band I)	1920 to 1980	2110 to 2170	TX: 9612 to 9888 RX: 10562 to 10838	190 MHz

Note: * Not used in Brazil.

Bluetooth Specifications

Bluetooth Version	Max. Permitted Power (mW)	Max. Permitted Power (dBm)	Typical Range (m)	Data Rate (Mbit/s)	Max. Application Throughput (kbit/s)
2.1 +EDR	1 mw	+8 dBm	10m	3Mb/s	>80k

WLAN Specifications (Wi-Fi)

Standard	Mode	Frequency Range (MHz)	Data Rate (Mbps)	Typical Output Power (sBm)	Typical WLAN
IEEE 802.11b	DSSS / CCK	2400 to 2483.5	1, 2, 5.5, 11	+20.0 dBm at 11Mbps, CCK	-88.0dBm at 8% PER, 11Mbps
IEEE 802.11g	OFDM	2400 to 2483.5	6, 9, 12, 18, 24, 36, 48, 54	+15.0dBm at 54Mbps	-73.0dBm at 10% PER, 54Mbps
IEEE 802.11n (2.4GHz)	OFDM	2400 to 2483.5	6.5, 13, 19.5, 26, 39, 52, 58.5, 65	+14.5dBm at 65Mbps (*)	-70.0dBm at 10% PER, 65Mbps

Note: (*) Max up to +18dBm

Chapter 2 – Safety Warnings

Lithium Battery

- A lithium battery (3V, coin cell, CR1632) located within the product provides backup power for the timekeeping. This battery has an estimated life expectancy of ten years.
- When this battery starts to weaken, the date and time may be incorrect.
- Battery is not user replaceable. If the battery fails, the device must be sent back to MultiTech Systems for battery replacement.
- Lithium cells and batteries are subject to the Provisions for International Transportation. Multi-Tech Systems, Inc. confirms that the Lithium batteries used in the MultiTech product(s) referenced in this manual comply with Special Provision 188 of the UN Model Regulations, Special Provision A45 of the ICAO-TI/IATA-DGR (Air), Special Provision 310 of the IMDG Code, and Special Provision 188 of the ADR and RID (Road and Rail Europe).

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

UL60950-1

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.

User Responsibility

Respect all local regulations for operating your wireless device. Use the security features to block unauthorized use and theft.

Power Supply Caution

CAUTION: Do not replace the power supply with one designed for another product; doing so can damage the modem and void your warranty. Adapter shall be installed near the equipment and shall be easily accessible.

CAUTION: Pour garantir une protection continue contre les risques d'incendie, remplacez les fusibles uniquement par des fusibles du même type et du même calibre. L'adaptateur doit être installé à proximité de l'appareil et doit être facilement accessible.

Device Maintenance

Do not attempt to disassemble the device. There are no user serviceable parts inside.

When maintaining your device:

- Do not misuse the device. Follow instructions on proper operation and only use as intended. Misuse could make the device inoperable, damage the device and/or other equipment, or harm users.
- Do not apply excessive pressure or place unnecessary weight on the device. This could result in damage to the device or harm to users.
- Do not use this device in explosive or hazardous environments unless the model is specifically approved for such use. The device may cause sparks. Sparks in explosive areas could cause explosion or fire and may result in property damage, severe injury, and/or death.
- Do not expose your device to any extreme environment where the temperature or humidity is high. Such exposure could result in damage to the device or fire. Refer to the device specifications regarding recommended operating temperature and humidity.
- Do not expose the device to water, rain, or spilled beverages. Unless the device is IP67 rated, it is not waterproof. Exposure to liquids could result in damage to the device.
- Do not place the device alongside computer discs, credit or travel cards, or other magnetic media. The information contained on discs or cards may be affected by the device.
- Using accessories, such as antennas, that MultiTech has not authorized or that are not compliant with MultiTech's accessory specifications may invalidate the warranty.

If the device is not working properly, contact MultiTech Technical Support.

Vehicle Safety

When using your device in a vehicle:

- Do not use this device while driving.
- Respect national regulations on the use of cellular devices in vehicles.
- If incorrectly installed in a vehicle, operating the wireless device could interfere with the vehicle's electronics. To avoid such problems, use qualified personnel to install the device. The installer should verify the vehicle electronics are protected from interference.
- Using an alert device to operate a vehicle's lights or horn is not permitted on public roads.
- UL evaluated this device for use in ordinary locations only. UL did NOT evaluate this device for installation in a vehicle or other outdoor locations. UL Certification does not apply or extend to use in vehicles or outdoor applications.

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

Radio frequency 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, EU, 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. This device also meets the European RF exposure requirements of EN 62311. If an alternate antenna is used, consult user documentation for required antenna specifications.

Compliance of the device with the FCC, EU 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.

Wireless devices could generate radiation. Other nearby electronic devices, like microwave ovens, may also generate additional radiation to the user causing a higher level of RF exposure.

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

MultiTech 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 Antenna Specifications

Manufacturer:	Trimble
Description:	GPS Antenna with low noise amplifier
Model Number:	66800-52
Multi-Tech Part Number:	45009665L

MultiTech Ordering Information

Model	Quantity
ANGPS-1MM	1
ANGPS-10MM	10
ANGPS-50MM	50

Antenna 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 MM 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 E-NET 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 DE-9 connector (9-pin) of the RS-232 cable to the RS-232 connector on the router. Then connect the other end to the serial port on the desired device.
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 a web browser. In the browser's address field, type the default address for the router: `http://192.168.2.1`. (If the browser displays a message that there is a problem with the website's security certificate, ignore this and click **Continue to the webpage**).
 - b. On first-time power up of the device, its Web UI displays the initial setup in commissioning mode requiring a **username** and **password** for the first administrative user. Enter your desired username and password. Refer to **First-Time Setup** for more details.
 - c. If you are not powering up the device for the first time and simply upgrading the firmware of your device, your existing logins are still active.

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.

Installing the SIM Card

If you want to operate the router on a particular 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 device. You can program a change to the behavior of the button if needed.

To reset the device:

1. Find the hole labeled RESET. The reset button is recessed into the case.

2. Use the pin to press and release the RESET button as follows:

Reset options:

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

The device restarts in commissioning mode. The system automatically removes all user accounts.

Enter a new username and password to create your new administrative account. (Refer to **User Accounts** for more details on username and password requirements.)

Note: The device reboots when restoring settings.

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.

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

First-Time Setup

If you need to change the mode of your device, this is the only way to do so. This section is not available through the device management software.

Other than when you first power up the device, you must configure the device to factory default settings, reset it and then, access it through the default 192.168.2.1 IP address to see the first-time setup. This wizard helps you configure the main features of your device.

Depending on the mode you choose, your proceeding options and fields differ (see the description of each step for details below). Here are the steps for first-time setup:

1. Upon power up for the first time or after you reset the device and accept factory default settings, the device goes into commissioning mode. The system requires you to set up an admin user. Enter your desired username and click **OK**.
2. Enter a desired password for the admin user and click **OK**. This password must be of sufficient length and strength (with a mix of character classes such as letters, numbers, and symbols). Enter the password again to confirm. Click **OK**.
3. Next, the mode option lets you set up the product as a **Network Router**, **PPP-IP Passthrough**, or **Serial Modem** device. If you switch modes, we recommend that you reset the device and configure to factory default settings.
 - a. The **Network Router** mode is the default and establishes the device as a cellular network router.
 - b. In the **PPP-IP Passthrough** mode, the rCell assigns the IP address it receives from the cellular provider to the Ethernet-attached device. In this mode, the rCell only allows one DHCP lease.

Note: In this mode, many of the rCell services described in this document are non-configurable and do not appear in the device configuration menu. All IP traffic is passed between the Ethernet-attached device and the cellular provider with no firewall functionality.
 - c. The **Serial Modem** mode creates a serial connection to the device which can be configured for speed and flow control. The serial port talks to the cellular radio in order to send and receive messages via the cellular radio.
 - d. Click **Next**.
4. In the **Time Configuration** page, set the date, time, and time zone.
 - a. In the **Date** field, type in the date you desire, or select the date from the pop-up calendar that opens.
 - b. In the **Time** field, type the desired time.
 - c. From the **Time Zone** drop-down list, select the time zone in which the router operates.
 - d. Click **Next**. Or if you are done making changes, click **Finish**.
5. In the **IP Setup** page, give the router its address and network information (the fields shown vary based on the selected mode):

If you select **PPP-IP Passthrough** mode, the following options are displayed:

- a. In the **Protocol Support** field, choose the internet protocol from the drop down menu (select from **IPv4** and **IPv6**).
- b. In the **Protocol Support** field, choose **IPv4** only as the cell radios for C2 and EV3 do not support **IPv6**.
- c. In the **Mask** field, enter the IP mask (default: 255.255.255.255 for mask 32, 255.255.255.0 for mask 24).
- d. In the **IPv6/IPv4 Primary DNS** field, type the address of the primary DNS (optional).
Note: This is an optional value that can be used if you use a DNS server other than the servers received from your carrier.
- e. In the **Public IPv4 Mask** field, select the public mask from the drop down either **32** or **24**.
- f. Click **Next**. Or if you are done making changes, click **Finish**.

If you select **Network Router** or **Serial Modem** mode, the following options are displayed:

- 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. This field is only available in **Network Router** mode. If you select **Serial Modem** mode, skip this step. In the **IPv4 Primary DNS** field, type the address of the primary DNS (optional).
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. This section is only available if you select **Network Router** or **PPP-IP Passthrough** mode. If you select **Serial Modem** mode, skip this step. In the **PPP Configuration** page, configure PPP for your router.
 - a. To use PPP, check **Enabled**. When enabled, your device functions as a router.
 - b. For devices that use two antennas, **Diversity** is enabled by default. Diversity enables the use of two cellular antennas for better performance. (See **Installing the Router** for more details).
 - c. To enable the dial-on-demand feature, check **Dial-on-Demand**. This indicates to the router to bring up the PPP connection when there is outgoing IP traffic, and take down the PPP connection after a given idle timeout.
 - d. In the **APN** field, type the APN (Access Point Name). The APN is assigned by your wireless service provider (not applicable to LVW2 and certain Verizon devices).
 - e. Click **Next**. Or if you are done making changes, click **Finish**.
 7. This section is only available if you select **Network Router** or **PPP-IP Passthrough** mode. If you select **Serial Modem** mode, skip this step. In the PPP Authentication page:
 - a. From **Type**, select the authentication protocol type used to negotiate with the remote peer: **PAP**, **CHAP**, or **PAP-CHAP**. The default value is **NONE**.
 - b. In the **Username** field, type the username with which the remote peer authenticates. You can leave this field blank, if desired. Username is limited to 60 characters.
 - c. In the **Password** field, type the password with which the remote peer authenticates. You can leave this field blank, if desired. Password is limited to 60 characters.
 8. This section is only available if you select **Serial Modem** mode. For any other mode, skip this step. In the **Serial Port Configuration** page:

- a. From **Baud Rate**, select baud rate in BPS for the serial port from the drop down list. Default setting is **115200**.
 - b. In the **Flow Control** field, select the flow control option from the drop down list provided. Choose from **NONE** or **RTS-CTS**.
 - c. In the **Parity** field, select the parity option from the drop down list. Choose from **NONE**, **ODD**, or **EVEN**.
 - d. In the **Data Bits** field, select the data bits option from the drop down list. Choose from **7** or **8**.
 - e. In the **Stop Bits** field, select the stop bit option from the drop down list. Choose from **1** or **2**.
9. Click **Finish**.
 10. To save your settings, click **Save and Restart**.

Chapter 6 – Configuring Your Device

Home Page (Dashboard)

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

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

- **Router:**

Model Number: The MultiConnect rCell model ID.

Serial Number: The MultiTech device ID.

IMEI: International Mobile Station Equipment Identity.

Note: Not applicable 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 devices LAN Ethernet interface.

IP Address: LAN IP address of this device. To configure the IP address, go to **Setup > IP Configuration**.

Netmask: Network mask of the LAN. To configure the network mask, go to **Setup > IP Configuration**.

Gateway: Default gateway IP address of the LAN. To configure the default gateway, go to **Setup > IP Configuration**.

DNS: Current Domain Name System IP addresses known by this device. To configure the DNS, go to **Setup > IP Configuration**.

DHCP State: Current state of this device's DHCP server. To configure, go to **Setup > DHCP Configuration**.

Lease Range: Current DHCP lease range of this device's DHCP server. To configure, go to **Setup > DHCP Configuration**.

- **Cellular:**

Protocol Support (only available when you choose **PPP-IP Passthrough**): Choose from **IPv4** or **IPv6**. If you choose **IPv6**, also enter the **Connect Timeout**.

Protocol Support (only available when you choose **PPP-IP Passthrough**): Choose only **IPv4** for C2 and EV3 as their cell radios do not support **IPv6**.

State: Current state of the cellular PPP link. For more information, go to **Cellular > Cellular Configuration**.

Signal: Current signal strength of the cellular link. Mouse hover provides dBm value.

Connected: Total time connected for the current PPP session.

IP Address: Current cellular WAN IP address issued to this device by the cellular carrier.

Roaming: Indicates whether or not this device's cellular link is currently connected to its home network.

Phone number: Device's cellular phone number also known as Mobile Directory Number (MDN). This field is blank if the MDN is not stored in the SIM card.

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

- **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*.

Time Configuration

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

Setting the Date and Time

To set the device's date and time:

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

Note: To learn more about time zones, visit the following website :
<http://www.greenwichmeantime.com/info/current-time.htm>

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

Configuring SNTP to Update Date and Time

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

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

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Configuring IP Address and DNS Information for LAN

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

1. From **Setup**, select **IP Configuration**.
2. To configure the address LAN 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. To save your changes, click **Save and Restart**.

WAN Setup

Configuring WAN Failover Priority

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

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

Wi-Fi as WAN is priority 1 by default.

If Ethernet is used as WAN, the DHCP server must be disabled.

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 device 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 device switches to the WAN with lower priority. The device 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 device 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**.
5. If you are finished making changes, click **Save and Restart**.

Failover Configuration Fields

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

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

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 **Service** drop-down list, select a DDNS service. To define a service that isn't listed choose **Custom**.
 - a. For custom DDNS service, in the **Service** field, type the DDNS server's URL.
 - b. For custom DDNS service, in the **Port** field, type the DDNS server's port.
4. In the **Domain** field, type the registered Domain name.
5. 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.
6. Check **Use Check IP**, if you want to query the server to determine the IP address before the DDNS update. The IP address is still assigned by the wireless provider and the DDNS is updated based on the address returned by Check IP Server. If disabled, the DDNS update uses the IP address from the PPP link. The default is **Use Check IP**.
7. In the **Check IP Server** field, type the name to which the IP Address change is registered. Example: checkip.dyndns.org
8. In the **Check IP Port** field, type the port number of the Check IP Server. The default is 80.
9. From the **System** drop-down list, select the desired system registration type, either Dynamic or Custom. The default is Dynamic.
10. Enter **Username** of the server.
11. Enter **Password** of the server.
12. To force update of DDNS, click **Update**.
13. Click **Submit**.
14. To save your changes, click **Save and Restart**.

Entering authentication information

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

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

Forcing a DDNS server update

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

Configuring Dynamic Host Configuration Protocol (DHCP) Server

You can configure your device 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 device.
6. In the **Domain** field, type your network domain, if any.
7. In the **Lease Range Start** field and in the **Lease Range End** field, type the range of IP addresses to be assigned by DHCP.
8. In the **Lease Time** field, type the DHCP lease time. Lease time is set in days, hours, and minutes.
9. Click **Submit**. If you are finished making changes, click **Save and Restart**.

Assigning Fixed Addresses

To add fixed addresses for the DHCP server:

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

Configuring the Global Positioning System (GPS)

This GPS information applies only to the MTR models that support GPS including:

Models B08 and B10

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

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

Notes:

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

GPS Server Configuration

To setup the GPS Server Configuration:

1. Go to **Setup > GPS Configuration > Server Configuration**.
2. To enable server configuration, check **TCP Server**.
3. 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.
4. Enter **Password** and confirm **Password**.
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

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. Complete the steps under **GPS Server Configuration**.
2. To use the serial port for GPS, you must disable the serial port client/server. Go to **Setup > Serial IP Configuration > Serial Port Settings** and uncheck **Enabled**.
3. Then, under **Local Configuration**, check **Serial Port Dump**.
4. **Submit**.
5. To save your changes, click **Save and Restart**.

Sending GPS information to a remote server

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

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

Configuring NMEA Sentences

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

1. Go to **Setup > GPS Configuration > NMEA Configuration** and in the **Interval** field, type the amount of time, in seconds, that passes before the NMEA information is sent. The default is **10** seconds. The range is **1 to 255** seconds.
2. You can further identify the router, also called a remote asset, that is collecting and sending the GPS information. To do so:

Add ID: The ID is an unique remote asset identification string. The ID string can be any length up to 20 characters. The **&** and **\$** are invalid characters. The ID must follow the standard NMEA sentence structure. Refer to the Universal IP AT Commands Reference Guide for sentence structure.

To add more information to the beginning of the ID, in the Add ID Prefix field, type the information.

3. You can select which NMEA sentence types you want to send. Check any combination of the available options: **GGA**, **GSA**, **GSV**, **GLL**, **RMC**, and **VTG**.

SMTP Settings

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

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

Configuring the Serial Port

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

1. Go to **Setup > Serial IP Configuration > Serial Port Settings**, check **Enabled**.
2. From the **Baud Rate** drop-down list, select the baud-rate at which the serial terminal communicates. The default is **115200**.
3. From the **Flow Control** drop-down list, select the flow control for the serial port. The options are **NONE** or **RTS-CTS**. The default is **NONE**.
4. From the **Parity** drop-down list, select the parity for the serial port. The options are **NONE**, **EVEN**, or **ODD**. The default is **NONE**.
5. To use the Modbus protocol as the protocol the serial devices use to communicate, check **Modbus Gateway** to the right of **Enabled**. **NOTE:** You may have the TCP connection encrypted with TLS. Make sure to check **Protocol** under **IP Pipe** and select **SSL/TLS**.
6. From the **Data Bits** drop-down list, select the data bits for the serial port. Data bit options are **7** or **8**. The default is **8**.
7. From the **Stop Bits** drop-down list, select the stop bits for the serial port. The options are **1** or **2**. The default is **1**.

8. Click **Submit**.
9. To save your changes, click **Save and Restart**.

Configuring Device to Act as Client

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

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

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

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. From the **Mode** drop-down list, select **CLIENT**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP, UDP, or SSL/TLS**.
4. In the **Server IP Address** field, enter the address of the far-end TCP, UDP, or SSL/TLS server.
5. In the **Server Port** field, enter the port value used by the far-end TCP, UDP, or SSL/TLS server.
6. If the primary server is unavailable, in the **Secondary IP Address** field, enter the address of the alternate TCP, UDP, or SSL/TLS server.
7. If the primary server is unavailable, in the **Secondary Port** field, enter port number value of the alternate TCP, UDP, or SSL/TLS server.
8. From the **Connection Activation** drop-down list, select a connection method. Options are:
 - ALWAYS-ON**. If you select this option, you cannot change the **Connection Termination** option.
 - DTR-ASSERT**. When the DTR signal is asserted, the connection is established.
 - CR**. Three carriage returns must be received before the TCP, UDP, or SSL/TLS connection is established to the remote server.
 - ON-DEMAND**. Set the connection as available on-demand.
9. From the **Connection Termination** drop-down list, select a disconnect method for the IP pipe. Options are:
 - ALWAYS-ON**.
 - TIMEOUT**. The IP pipe connection disconnects if the configured timer expires with no data sent or received. In the **Timeout** field, enter the desired number of seconds for this timeout.
 - SEQUENCE**. A sequence of received characters disconnects the IP pipe.
 - DTR-TOGGLE**. When the DTR control signal is toggled, the IP pipe disconnects.
10. In the **Buffer Timeout** field, enter the timeout after which data is sent to the network if the buffer is not full (in milliseconds).
11. In the **Buffer Size** field, enter the size of the buffer for reading data from the serial port and sending to the network (in bytes). Data is sent when the buffer is full.
12. Click **Submit**.
13. To save your changes, click **Save and Restart**.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.

2. Under **Security Settings**, click the **Show** to the right.
3. By default, the **Use default cipher suite** is checked. If you accept this default, no other action is needed.
4. Uncheck this box, if you want to select specific TLS versions and Cipher Suites. These fields appear.
5. Select the **TLS version**. Check either **TLSv1.2** or **TLSv1.1**.
6. Check your preferred **Cipher Suite** from the following list: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA, and/or AES128-SHA
7. Click **Submit**.
8. To save your settings, click **Save and Restart**.

Configuring Device to Act as Server

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

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

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

1. Go to **Setup > Serial-IP Configuration > Serial Port Settings > IP Pipe** group.
2. In the **Mode** drop-down list, select **SERVER**.
3. From the **Protocol** drop-down list, select the desired protocol: **TCP**, **UDP**, or **SSL/TLS**.
4. In the **Buffer Timeout** field, enter the timeout after which data is sent to the network if the buffer is not full (in milliseconds).
5. In the **Server Port** field, type the desired port value in the range **1** to **65535**.
6. In the **Buffer Size** field, enter the size of the buffer for reading data from the serial port and sending to the network (in bytes). Data is sent when the buffer is full.
7. 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.
8. Click **Submit**.
9. To save your changes, click **Save and Restart**.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.
2. Under **Security Settings**, click the **Show** to the right.
3. By default, the **Use default cipher suite** is checked. If you accept this default, no other action is needed.

4. Uncheck this box, if you want to select specific TLS versions and Cipher Suites. These fields appear.
5. Select the **TLS version**. Check either **TLSv1.2** or **TLSv1.1**.
6. Check your preferred **Cipher Suite** from the following list: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA, and/or AES128-SHA
7. Click **Submit**.
8. To save your settings, click **Save and Restart**.

Adding Saved Networks

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

1. Go to **Setup > 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.
5. Click **Finish**.
6. To save your changes, click **Save and Restart**.

Editing or Deleting an Existing Network

1. To delete a network, click the **trash can**.
2. At the top of the pane, a message tells you the network is deleted. To undo the delete, click the **Undo** link found in the message.
3. To edit a network, click **pencil icon**. Change the IP address or subnet mask as desired.
4. Click **Finish**.
5. To save your changes, click **Save and Restart**.

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

Configuring SNMP

The device offers Simple Network Management Protocol (SNMP) which is used for collecting information from, and configuring network devices on an IP network.

You also have the option to configure SNMP traps which are alerts sent from SNMP-enabled devices to an SNMP agent or manager typically providing device status or condition information.

You can also access the **MIB** file which is a management information base. This file is a formal description of a set of network objects managed using the Simple Network Management Protocol (SNMP). The format of the **MIB** is defined as part of the SNMP. (All other **MIBs** are extensions of this basic management information base.)

Click **Download MIB**, to download the MIB file.

To configure SNMP:

1. Go to **Setup > SNMP Configuration**, check the **Enabled** box for each of the SNMP versions that apply (either **SNMP V1/V2C** and/or **SNMP V3**).
2. Under **SNMP Server Configuration**, check **Enabled** to activate the SNMP server. Click **Submit**.
3. If needed, click **Add** under **Allowed IP Addresses** for **SNMP v1/v2c**.
4. Click **Add Server Configuration**.
 - a. Make sure that **Enabled** is checked.
 - b. Under **Version**, select from the drop-down either **SNMP v1/v2c** or **SNMP v3**.
 - c. For **SNMP v1** and **SNMP v2c**:
 - i. Enter the **Configuration Name** for your SNMP configuration.
 - ii. Enter **Community String** which is a read-only string used to authenticate incoming SNMP requests.
 - d. For **SNMP v3**:
 - i. Enter the **Authentication Protocol** from the drop-down, including **NONE**, **MD5**, or **SHA1**. If you selected **MD5** or **SHA1** for Authentication Protocol:
 - Enter the **Security Name** which is a username used to authenticate incoming SNMP v3 requests.
 - Enter the **Authentication Password**, which is a password used to authenticate incoming SNMPv3 requests.
 - Confirm the password.
 - ii. Enter the **Encryption Protocol** for SNMPv3 messages from the drop-down, including **NONE**, **DES** or **AES-128**. If you selected **DES** or **AES-128** for **Encryption Protocol**:
 - Enter the **Encryption Password**.
 - Confirm the password.
5. Click **Submit**.
6. The **SNMP Configuration** list displays your recently added SNMP Server Configuration. To edit the configuration, click the pencil icon under **Options**.
7. To delete an existing configuration, click the trash can icon under **Options**.
8. If finished, click **Submit**. Or continue to **SNMP Trap Destinations** and **Add Trap Destinations**.
9. To save your changes, click **Save and Restart**.

To configure SNMP Traps:

1. Go to **Setup > SNMP Configuration > SNMP Trap Configuration**, check **Enabled** to enable sending SNMP traps on the device..
2. The engine ID displays to the right of **Enabled**. Modify the engine ID or use the default value.
3. Click **Submit**.
4. Click **Add Trap Destination**.
5. Make sure that **Enabled** box is checked.
6. Enter the **Destination Name**.

7. Select from the drop-down the **Version** of SNMP (**SNMP v1/v2c** or **SNMP v3**).
8. For **SNMP v1** or **SNMP v2c**:
 - a. Enter the **Destination IP Address**.
 - b. Enter the **Community String**.
 - c. Click **Submit**.
 - d. Click **Save and Restart**.
9. For **SNMPv3**:
 - a. Enter the **Destination IP Address**.
 - b. Enter **Security Name**.
 - c. Enter the **Authentication Protocol** from the drop-down, including **NONE**, **MD5**, or **SHA1**. If you selected **MD5** or **SHA1** for **Authentication Protocol**:
 - i. Enter the **Authentication Password**, which is a password used to authenticate incoming SNMPv3 requests.
 - ii. Confirm the password.
 - d. Enter the **Encryption Protocol** for SNMPv3 messages from the drop-down, including **NONE**, **DES**, or **AES-128**. If you selected **DES** or **AES-128** for Encryption Protocol:
 - i. Enter the **Encryption Password**.
 - ii. Confirm the password.
 - e. The **SNMP Trap Destination** list displays your recently added SNMP Trap Destination. To edit the destination, click the pencil icon under **Options**.
 - f. To delete an existing destination, click the **trash can** icon under **Options**.
 - g. To save your changes, click **Save and Restart**.

To download the MIB file:

1. Click **Download MIB** in the far right corner of the device display.
2. Download/save the file from your browser.

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Chapter 7 – Setting Up Wireless Features

Setting Up Wi-Fi Access Point

If you ordered a device with Wi-Fi capability, your router can be configured as a wireless access point (AP). This allows 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.
 - WPA/WPA2-PSK**: Use Wi-Fi protected access version 1 and 2 to secure data exchanged on your network.

2. To select **WEP** mode:
 - a. From the **Encryption** drop-down list, select the encryption to be used. Choose from **64 bit 10 hex digits** or **128 bit 26 hex digits**.
 - 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 select **WPA-PSK**, **WPA2-PSK** or **WPA-PSK/WPA2-PSK** modes:
 - a. Select the WPA Algorithm from the drop-down list. Choose from **TKIP**, **AES** or **TKIP+AES**.
 - 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**.
5. To save your changes, click **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 Wi-Fi.
2. To update the list, click **Refresh**.

Setting Up Wi-Fi as WAN

To setup the router's Wi-Fi 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. Here are the available fields to enter information:

Network Name

SSID

Security Mode: None, WEP, WPA, WPA-PSK, WPA-2, or WPA-2-PSK

Username

Password

Unmask (Check, Uncheck)

WPA Algorithm: TKIP, +AES, TKIP, or AES

Shared Key

Key Index: 0 - 3

Network Key

IEEE 802.1x

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.

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

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.
6. To add a device, click **Add Device** and enter the device name and the **MAC address**.
7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

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

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**

- **On-Demand**
- **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 On:**
 - **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**.
- 9. To save your changes, click **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.

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol**.
2. Under **Security Settings**, click the **Show** to the right.
3. By default, the **Use default cipher suite** is checked. If you accept this default, no other action is needed.
4. Uncheck this box, if you want to select specific TLS versions and Cipher Suites. These fields appear.
5. Select the **TLS version**. Check either **TLSv1.2** or **TLSv1.1**.
6. Check your preferred **Cipher Suite** from the following list: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA, and/or AES128-SHA
7. Click **Submit**.
8. To save your settings, click **Save and Restart**.

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 Port Forwarding Rules](#)
- [Adding Input Filter Rules](#)
- [Adding Output Filter Rules](#)
- [Advanced Settings](#)

Inbound Forwarding Rule

Adding Port Forwarding Rules

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

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Port Forwarding** group, click **Add Rule**.
3. In the **Inbound Forwarding Rule** dialog box, enter a name for the rule and optionally, a description.
4. In the second **Inbound Forwarding Rule** dialog box, in the **External WAN Port(s)** field, type the port(s) to be forwarded. Common ports are listed in the field's attached drop-down list and are exposed once you enter a character. Type **ANY** to forward all ports.
5. In the **Destination LAN IP** field, type the IP address of the device that packets will be forwarded to.
6. In the **Destination LAN Port(s)** field, type the port to which packets are translated. If there is a range of ports, the ending port is automatically set. The Destination LAN ending port is based on the Destination LAN starting port and the range provided in the **External WAN Port(s)** field.
7. From the **Protocol** drop-down list, select the protocol of the messages that can be forwarded. Select from **TCP/UDP**, **TCP**, **UDP**, or **ANY**.
8. In the **External Source IP** field, enter the IP address of the source of the messages.
9. In the **External Source Ports** field, enter the port range for the source of the messages.
10. In the **Mask** field, enter the external source subnet mask.
11. Check **Enable NAT Loopback** if you want to redirect LAN packets destined for the WAN's public IP address.
12. Click **Submit**.
13. To save your changes, click **Save and Restart**.

A default filter allowing forwarded packets through the firewall is automatically created.

Input Filter Rules

To add an input filter rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Input Filter Rules** group, click **Add Rule**.

3. In the **FilterRule** dialog box, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rules.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Ports** field, enter the source port range that applies to this rule.
10. In the **Source Mask** field, enter source subnet mask that applies to this rule.
11. In the **Source MAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **Source Interface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP, TCP, UDP, or ANY**.
14. In the **Chain** field, select the grouping based on the type of traffic affected by the rule from the drop-down menu. Select from **INPUT, FORWARD, or OUTPUT**.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **ACCEPT, REJECT, DROP, or LOG**.
16. Click **Submit**.
17. To save your changes, click **Save and Restart**.

Output Filter Rules

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

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. Click **Add Rule** in the **Output Filter Rules** section.
3. Enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, type the IP address of the device or network that packets are to be sent to. Type **ANY** if the destination address does not matter.
5. In the **Destination Port** field, type the port for which that the packets are destined. Common destination ports are listed in the Destination Port field's attached drop down list. Type **ANY** if the destination port does not matter.
6. In the **Destination Mask** field, type the network mask of the destination network.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
8. 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.
9. In the **Source Port** field, type the port that is the origin of the traffic. Type **ANY** if the source port does not matter.
10. In the **Source Mask** field, type a network mask for the origin of the traffic.
11. In the **SourceMAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **SourceInterface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.

13. From the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Choose from **TCP/UDP, TCP, UDP, or ANY**.
14. In the **Chain** field, select the grouping based on the type of traffic affected by the rule from the drop-down menu. Select from **INPUT, FORWARD, or OUTPUT**.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **ACCEPT, REJECT, DROP, or LOG**.
16. Click **Submit**.
17. To save your changes, click **Save and Restart**.

Advanced Settings

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

Filter rules apply an **ACCEPT, REJECT, DROP, or LOG** action to a packet. A **DNAT or SNAT** rule with the same name as a **Forwarding** rule will be associated under **Normal Settings** for **Port Forwarding/NAT** rules.

- [Adding Prerouting Rules](#)
- [Adding Postrouting Rules](#)

Prerouting Rule

Add a DNAT rule

To add prerouting or DNAT rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Prerouting Rules** group, click **Add DNAT Rule**.
3. In the **FilterRule** dialog box, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rules.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Port** field, enter the source port that applies to this rule.
10. In the **SourceMask** field, enter source subnet mask that applies to this rule.
11. In the **SourceMAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **SourceInterface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP, TCP, UDP, or ANY**.
14. In the **NAT IP** field, enter the public IP address for the Network Address Translation.
15. In the **NAT Port** field, enter the port used publicly for the Network Address Translation.
16. **Check Enable NAT Loopback if you want to redirect LAN packets destined for the WAN's public IP address.**

17. Click **Submit**.
18. To save your changes, click **Save and Restart**.

Postrouting Rule

Add a SNAT rule

To add postrouting or SNAT rule to your firewall:

1. Go to **Firewall > Settings** to display the **Firewall** window.
2. In the **Postrouting Rules** group, click **Add SNAT Rule**.
3. In the **Postrouting Rule** dialog box, enter a name for the rule and optionally, a description.
4. In the **Destination IP** field, enter the destination IP address that applies to this rule.
5. In the **Destination Port** field, enter the destination port that applies to this rule. If there is a range of ports, the ending port is automatically set.
6. In the **Destination Mask** field, enter the subnet mask of the destination that applies to this rules.
7. In the **Destination Interface** field, select the interface used by the destination that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
8. In the **Source IP** field, enter the source IP address that applies to this rule.
9. In the **Source Port** field, enter the source port that applies to this rule.
10. In the **SourceMask** field, enter source subnet mask that applies to this rule.
11. In the **SourceMAC** field, enter the source MAC address for the device that applies to this rule.
12. In the **SourceInterface** field, select the source interface that applies to this rule from the drop-down menu. Select from **ANY, LAN, WAN, CELLULAR, or WI-FI WAN**.
13. In the **Protocol** drop-down list, select the protocol of the messages that apply to this rule. Select from **TCP/UDP, TCP, UDP, or ANY**.
14. In the **NAT IP** field, enter the public IP address for the Network Address Translation.
15. In the **Target** field, select the desired action of the firewall based on this rule from the drop-down menu. Choose from **SNAT or MASQUERADE**.
16. In the **NAT Port** field, enter the port used publicly for the Network Address Translation.
17. Click **Submit**.
18. To save your changes, click **Save and Restart**.

Trusted IP

Trusted IP is a separate firewall configuration that allows users to create whitelists (which are allowed or trusted IPs) or black lists (which are blocked or unwanted IPs). You can add, edit, and delete IP addresses as needed.

If you select **White List** as **Trusted IP Mode** and you do not set any IP range, no traffic will be allowed. If you select **Black List** as **Trusted IP Mode** and you do not set any IP range, all traffic will be allowed.

To set up a Trusted IP range:

1. Go to **Firewall > Trusted IP**.
2. Check the **Enabled** box to turn on Trusted IP.
3. Select the **Trusted IP Mode** from the drop-down, either **White List** or **Black List**. (**NOTE:** Be aware of the behavior of each list and its consequences based on your specific configuration. For example, if you select **White List** as **Trusted IP Mode**, you should include the router **IP Address Range** or **IP Address** and **Subnet Mask** to maintain your local router LAN access.)

4. To add IP addresses, click **Add IP Range** in the upper right corner.
5. Under the **Add IP Range**, enter or select the following parameters:
 - a. **Name**
 - b. Mode from drop-down, either **Subnet** or **IP Range**.
 - c. For **Subnet**:
 - i. **IP Address**
 - ii. **Subnet Mask**
 - d. For **IP Range**:
 - i. **IP Address Start**
 - ii. **IP Address End**
 - e. **Destination Port** (default: **ANY**)
 - f. **Protocol** from drop-down including **ANY, TCP/UDP, TCP, or UDP**
 - g. Click **Finish**.
6. The system displays your recently added and existing IP ranges in a list. The list includes the relevant details. You may edit any IP ranges by clicking on the pencil icon under **Options**.
7. You may delete any IP ranges by clicking on the trash can icon under **Options**.
8. If you want to revert back to default settings (where **Trusted IP** is disabled and all IP ranges are removed), click the **Reset to Default** button in the lower right corner
9. Click **Submit**.
10. To save your changes, click **Save and Restart**.

Setting up Static Routes

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

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

Chapter 9 – Setting Up Cellular Features

Configuring Cellular

To configure how cellular is used on your device:

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

Cellular Configuration Fields

Field	Description
General Configuration	
Enabled	Allows the device to establish a cellular connection (Cellular WAN).
Dial-on-Demand ¹	Enables the Dial-on-Demand feature. If enabled, the device brings up and maintains a cellular connection while network activity on the LAN requires WAN access. The device brings down the cellular connection when outgoing network traffic ceases for the given Idle Timeout duration. Enable this feature when Wakeup-on-Call is enabled to allow the device to "sleep" after it has been "woken up." See Configuring Wakeup-on-Call for more information.
Diversity	Allows the use of two antennas to increase receive signal quality. 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; the default is zero, which means an infinite number is allowed.
Modem Configuration	
Dial Number	The modem dial string is: <ul style="list-style-type: none"> ■ *99***1# for GSM/GPRS/non-Verizon LTE devices
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 the SIM for use (only required if the 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: NONE, PAP, CHAP, or PAP-CHAP (either). Authentication may not be required by the cellular service provider.
Username	Name of the user that the remote PPP peer uses to authenticate.
Password	Password that the remote PPP peer uses to authenticate.
Keep Alive¹	
Used to periodically check if the cellular link is up; if not, the device tries to establish the link.	
ICMP/TCP Check¹	
An active check that provides the most reliable and reactive diagnosis of the cellular link, but requires sending data through the cellular link.	
Enabled ¹	Enables the Active Keep Alive check. Depending on the plan type and data usage, this may result in additional data charges.
Keep Alive Type ¹	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 ¹	Time in seconds between active checking of the cellular link.
Hostname ¹	Host name or IP address for the keep alive check.
TCP Port ¹	TCP port number to connect with the TCP server (only visible when Keep Alive Type TCP is selected).
ICMP Count ¹	Number of sequential, unsuccessful ping attempts to the specified host to declare that the link needs to be re-established (only visible when Keep Alive Type ICMP is selected).
Data Receive Monitor	
A passive check that observes the absence of packets received over a given amount of time. This check cannot reliably determine if the link is down; no network traffic may cause the monitor to signal to shutdown and re-establish the cellular link even though the link was in a good state.	
Enabled	Enable or disable the passive monitoring of the cellular link.
Window	The amount of time that can pass without receiving network traffic before the cellular link is torn down and re-established.

¹If you choose **PPP-IP Passthrough** and **Serial Modem** mode, this field is not available.

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Configuring Wake Up On Call

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

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 setting. For wakeup methods, see [Wake Up On Call Method Settings](#).
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

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

Wake Up On Call Method Settings

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

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

For Wake-Up-On-Call field descriptions, see [Wake Up On Call General Configurations](#).

Wake Up On Call General Configurations

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

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

Using Telnet to Communicate with the Cellular Radio

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

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

Radio Status

Field	Description
Module Information	
IMEI	International Mobile Station Equipment Identifier
IMSI	International Mobile Subscriber Identifier
Manufacturer	Company that developed the cellular module
Model	Cellular module model number
Hardware Revision	Module's hardware revision
MDN (Phone Number)	Mobile Directory Number. In some SIM/carriers, the value may not be present and therefore not displayed.
MSID	Mobile Station ID. Some SIM/carriers do not contain this value and therefore the value is not displayed.
Firmware Version	Module's firmware version
Service Information	
Home Network	Cellular service provider associated with the module's data account
Current Network	Current cellular service operator (Not available for C2 or EV3 models)
RSSI	Received Signal Strength Indication
Service	Cellular service connection type
Roaming	Indicates whether or not the current service is provided by the Home Network carrier
Update Options	
MDN (Phone Number)	Update the cellular module's phone number. This number is updated only on the device. The MDN that the carrier has associated with this device does not change.

Telit Radio Firmware Upgrade

H5 and H6 only

The update of Telit radio module firmware supports full firmware files and upgrade of H5 and H6 models. Refer to your product model number on the product label usually found on the bottom or back of your device or also at the top of the page of the device UI.

There are two methods for updating the cellular firmware offered: 1) Upgrading using DeviceHQ® and 2) Upgrading using the device UI only.

Upgrading Cellular Firmware Using DeviceHQ (Remote Management)

DeviceHQ can manage the Telit Firmware upgrade to your device when annex-client checks in. **NOTE:** You must first enable and properly configure Remote Management in the device UI (refer to [Managing Your Device Remotely](#)).

1. Open **DeviceHQ**.

2. Select **Device > Your Device Name > Schedule > Upgrade Radio Firmware**.
3. **DeviceHQ** provides a list of eligible Telit module firmware that a particular device can queue for download and install. Select the appropriate firmware.
4. The device checks in, downloads the firmware, automatically verifies the MD5 sum of the firmware to check the integrity of the upgrade file, and applies it to the modem module.
Note: Allow at least 10 minutes after the device has downloaded the firmware file before taking any action. The system should reboot on its own after a successful download. Otherwise, after 10 minutes, you may reboot the device manually.
5. Once you have refreshed or the device checks in again, verify that the cellular radio firmware has been updated in DeviceHQ.

In the device UI, you can also check that the cellular radio firmware has been updated. Refer to the **Current Radio Firmware** on the **Telit Radio Firmware Upgrade** page (see step 1 of **Upgrading Cellular Firmware Using UI only**) or also see the firmware version on the **Radio Status** page under **Cellular**.

Upgrading Cellular Firmware using UI only

You can also use the device UI to upgrade your Telit Firmware. You must first obtain the appropriate binary upgrade file for the cellular radio in your device.

NOTE: If you use the firmware upgrade via Cellular using the UI and you get a timeout failure, first try to boost the signal strength and attempt it again. Otherwise, update via an Ethernet connection or use **DeviceHQ**.

1. Open the **Telit Radio Firmware Upgrade** page on the device. The page is not available through the standard UI. Enter the IP address/URL manually: **https://<Device-IP>/upload_radio_firmware** (usually your device IP address is the default address unless you changed it).
2. Find the upgrade zip file in your product page under **Downloads** on www.multitech.com. (The file name starts with **stream**.) Download the zip file from the website and save it on your local computer. Extract the binary upgrade file and MD5 file.
3. Enter the MD5 Check Sum or hash under **File MD5**.
4. Browse for the file and select it.
5. Click **Start Upgrade**. The system should reboot automatically after a successful download. Otherwise, after 10 minutes, you may reboot the device manually.
6. Check that the cellular radio firmware has been updated. Refer to the **Current Radio Firmware** on the **Telit Radio Firmware Upgrade** page (see step 1 of **Upgrading Cellular Firmware Using UI only**) or also see the firmware version on the **Radio Status** page under **Cellular**.

Chapter 10 – Configuring SMS

Configuring SMS

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

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

For field descriptions see [SMS Field Descriptions](#).

SMS Field Descriptions

Field	Description
Enabled	Enables the SMS utilities required to send SMS via API and the Web Management interface.
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.

SMS Commands

SMS commands are disabled by default. To enable these available commands (for status and debugging purposes) and set security filters:

1. Go to **SMS > SMS Configuration > SMS Commands**, check the SMS commands you wish to enable. Refer to the table of [SMS Command Descriptions](#) for details on available commands.
2. Check the security filters, you wish to use (can be one or both):
 - **Password:** If enabled, SMS commands will require **p password** in the syntax. For example: **p 123456 #serial** where 123456 is your password.
 - Use the **default password** (last six digits of the radio's IMEI or last six digits of the MEID).
 - Or click on **Use custom password** and enter your own password.
 - You can also toggle the eye icon to make the password visible or hidden.
 - **Whitelist:** If enabled, SMS commands can only be received from a number in the whitelist (you must enter a phone number).

Enter the phone number and click **Add Number**.

Note: Due to differences between service providers, for every US number you add to the **Whitelist**, create two separate entries: 1) one using the **phone number** and 2) the other using **1 + phone number**.

3. Refer to the **Required SMS Command Format** field to see the format based on your chosen settings.
4. Click **Submit**.
5. To save your changes, click **Save and Restart**.

Here is an example SMS Command (#serial – Server mode):

```
Serial-IP Port Status:
Mode: Server
Protocol: SSL/TLS
Port: 3000
TX Bytes: 1234567
RX Bytes: 123456789
DCD Status: ON
2016-11-20 19:22
```

The response message to all SMS commands includes a time stamp. The time stamp format is **YYYY-MM-DD HH:MM**.

The system adds the time stamp to the existing commands at the end of the SMS message. In case the message exceeds the 160 character limit, the device information and the occurred event are not truncated. Only the time stamp is lost.

SMS Command Descriptions

The following table describes available SMS Commands under **SMS Configuration > SMS Commands > Enabled Commands**. All SMS Commands are disabled by default. Check to enable.

SMS Command	Description
#reboot	reboots the device
#checkin	checks in to DeviceHQ
#rm <enable disable> <AccountKey>	enable or disable remote management using DeviceHQ (You must specify AccountKey when enabling Remote Management if not previously configured.)
#setcellular <enable disable> [<APN>]	enable or disable Cellular and allows setting of the APN
#ping [<interface>] [<count>] <address>	ping IP address <count> times (range: 1-20, default = 4) through <interface> (choose from cellular, wifi, and ethernet or if not specified, the default gateway interface is used)
#apn	get APN string
#cellular	PPP status

SMS Command	Description
#radio	radio status
#ethernet	Ethernet LAN configuration details
#wan	WAN transport type and WAN priority configuration
#serial	get serial details: Mode (Server or Client), RX bytes, TX bytes, DCD Status, Protocol, Port (Server mode only), Server IP Address (Client mode only), and Server Port (Client Mode only)
#wifi	get Wi-Fi details: Date and time in format YYYY-MM-DD HH:MM, mode (WAN or Access Point), MAC address, status (for WAN mode only), SSID, Security settings (for Access Point only, None, WEP, WPA, WPA2-PSK, and WPA/WPA2-PSK)

Note: Arguments in square brackets [] are optional. Those in angle brackets < > are values.

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**. The system displays a confirmation indicating whether the message has been successfully sent or not.

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 **trash can** 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 **Delete All**. A dialog box asks you to confirm that you want to delete all SMS messages. Click **OK**.
5. To configure the receive list to automatically update, check the **Auto Refresh** box in the upper right corner.

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 **trash can** 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 **Delete All**. A dialog box asks you to confirm that you want to delete all the SMS messages. Click **OK**.
5. To configure, the receive list to automatically update, check the **Auto Refresh** box in the upper right corner.

Chapter 11 – Defining Tunnels

Setting Up GRE Tunnels

Tunneling allows the use of a public network to convey data on behalf of two remote private networks. It is also a way to transform data frames to allow them to pass networks with incompatible address spaces or even incompatible protocols. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can be used for carrying many different passenger protocols.

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

1. From the Web Management interface, go to **Tunnels > GRE Tunnels > GRE Tunnels Configuration**.
2. Click **Add Tunnel**. A series of wizard pages helps you configure the connection.
3. In the **Tunnel Name** field, enter a name for the new tunnel.
4. (Optional) In the **Description** field, you can enter a description that helps you further identify the tunnel.
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. Click **Add** under **Remote Network Routes**.
 1. (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.
 2. If you are not using a saved network, in the **Remote Network Route** field, type the IP address of the network that is routed through the tunnel.
 3. If you are not using a saved network, in the **Remote Network Mask** field, type the mask of the network.
 4. Click **Add**.
 - c. In the **Checking Period** field, enter the timeout interval in minutes. The default is 10 minutes.
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

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

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

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

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

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

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

1. From the Web Management interface, go to **Tunnels > IPsec Tunnels**.
2. Click **Add Tunnel** in upper right.
3. Enter a **Name** for the tunnel and an optional **Description**.
4. Click **Next**. The **IPsec Remote Tunnel Endpoint** pane opens.
5. Under the **Saved Network** drop-down, you can add a saved network **OR** enter a network manually by entering the **Remote Network Route** (LAN IP) and **Remote Network Mask** (Subnet).
6. Choose **Tunnel Type** from the drop-down. Values are **IKE** and **IKEv2**.
7. The public IP address and LAN of this device do not need to be configured because they are already known by this device.
8. Select the **Authentication Method** from the drop-down either **Pre-Shared Key** or **RSA Signatures**. Authentication is performed using secret pre-shared keys and hashing algorithms (like **SHA1 MD5**) or RSA signatures.
9. If you select **Pre-Shared Key**, then enter the **Secret**. This key needs to be the same on both endpoints.
10. If you select **RSA Signatures**, enter the following (in .pem format):
 - a. **CA Certificate**
 - b. **Local RSA Certificate**
 - c. **Local RSA Private Key**
11. Select the **Encryption Method** from the drop-down including **3DES**, **AES-128**, **AES-192**, **AES-256** , or **ADVANCED**. The encryption method needs to be the same on both endpoints. IKE encryption algorithm is used for the connection (**phase 1 - ISAKMP SA**). Based off of **phase 1**, a secure set of defaults are used for **phase 2**, unless you use the **Advanced** option, in which case, you must specify all components of both **phases 1 and 2** including **Encryption**, **Authentication**, and **Key Group**.
12. If the remote endpoint is set up with unique IDs, check the **Enable UID** box, and enter the **Local** and **Remote IDs**.
13. Click **Show** for **IPSec Tunnel: Advanced** features that limit the remote endpoint's negotiation options.
14. In the **IKE Lifetime** field, enter the duration in which ISAKMP SA lasts (in hours).
15. In the **Max Retries** field, enter the number of retries for the IPsec Tunnel. Enter zero for unlimited retries.
16. In the **Key Life** field, duration in which the IPsec SA lasts (in hours).
17. In the **Checking Period** field, enter the timeout interval (in minutes).
18. Check **Compression** to enable IPComp (compression algorithm).
19. Check **Aggressive Mode** to enable exchange identification in plain text (unencrypted for faster negotiation). NOTE: This mode is less secure and prone to dictionary and brute force attacks.
20. Click **Submit**.
21. To save your changes, click **Save and Restart**.

For field descriptions, see [IPsec Tunnel Configuration Field Descriptions](#).

IPsec Tunnel Configuration Field Descriptions

Field	Description
IPsec Tunnel	
Name	Name used to identify the IPsec tunnel in configurations and logs.
Description	Optional text to describe the IPsec tunnel. This description shows up in the UI while hovering over the summary of an IPsec tunnel.
IPsec Remote Tunnel Endpoint	
Remote WAN IP	External IP address of the remote tunnel endpoint. The remote device is typically another router.
Saved Network	Select a saved network from the pre-defined list of user-defined networks on the Setup > Saved Networks page. This network describes the remote endpoint's subnet, and is used to identify packets that are routed over the tunnel to the remote network.
Remote Network Route	This field is used in conjunction with the Remote Network Mask field and describes the remote endpoint's subnet. This is used to identify packets that are routed over the tunnel to the remote network.
Remote Network Mask	This field is used in conjunction with the Remote Network Route field, to describe the remote endpoint's subnet. It identifies packets that are routed over the tunnel to the remote network.
Tunnel Type	Internet Key Exchange (IKE) for host-to-host, host-to-subnet, or subnet-to-subnet tunnels. Choose from IKE or IKEv2 .
IPsec Tunnel: IKE	
Authentication Method	Choose between Pre-Shared Key or RSA Signatures . Authentication is performed using secret pre-shared keys and hashing algorithms (like SHA1 MD5) or RSA signatures (you provide the CA Certificate , Local RSA Certificate , and Local RSA Private Key in .pem format). If you check Enable UID , then Local ID and Remote ID become available as options.
Pre-Shared Key	Authentication is performed using a secret pre-shared key and hashing algorithms on both sides.
Secret	Secret key that is known by both endpoints.
Encryption Method	IKE encryption algorithm used for the connection (phase 1 - ISAKMP SA). Based off of phase 1, a secure set of defaults are used for phase 2, unless the Advanced option is used, in which case, all components of both phases 1 and 2 are specified by the user.
RSA Signatures	Authentication is performed using digital RSA signatures.
CA Certificate	Certificate Authority certificate used to verify the remote endpoint's certificate.
Local RSA Certificate	Certificate the local endpoint uses during Phase 1 Authentication .
Local RSA Private Key	The private key that the local endpoint uses during Phase 1 Authentication.

Field	Description
Encryption Method	Choose an Encryption Method from the following list: 3DES, AES-128, AES-192, AES-256, or ADVANCED . IKE encryption algorithm is used for the connection (phase 1 - ISAKMP SA). Based off of phase 1, a secure set of defaults are used for phase 2, unless the Advanced option is used, in which case, all components of both phases 1 and 2 are specified by the user.
Phase 1 Encryption	If Advanced is selected for Encryption Method , select Phase 1 Encryption from the drop-down: 3DES, AES-128, AES-192, AES-256, ANY AES, or ANY .
Phase 1 Authentication	If Advanced is selected for Encryption Method , select Phase 1 Authentication from the drop-down: MD5, SHA-1, SHA-2, SHA2-256, SHA2-384, SHA2-512, or ANY .
Phase 1 Key Group	If Advanced is selected for Encryption Method , select the Phase 1 Key Group from the drop-down: DH2 (1024-bit), DH5 (1536-bit), D14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit), and ANY .
Phase 2 Encryption	If Advanced is selected for Encryption Method , select Phase 2 Encryption from the drop-down: 3DES, AES-128, AES-192, AES-256, ANY AES, or ANY .
Phase 2 Authentication	If Advanced is selected for Encryption Method , select Phase 2 Authentication from the drop-down: MD5, SHA-1, SHA-2, SHA2-256, SHA2-384, SHA2-512, or ANY .
Phase 2 Key Group	If Advanced is selected for Encryption Method , select the Phase 2 Key Group from the drop-down: DH2 (1024-bit), DH5 (1536-bit), D14 (2048-bit), DH15 (3072-bit), DH16 (4096-bit), DH17 (6144-bit), DH18 (8192-bit), DH22 (1024-bit), DH23 (2048-bit), DH24 (2048-bit), and ANY .
Enable UID	Unique Identifier String to enable the Local ID and Remote ID fields.
Local ID	String Identifier for the local security gateway (optional)
Remote ID	String Identifier for the remote security gateway (optional)
IPSec Tunnel: Advanced	
IKE Lifetime	Duration for which the ISAKMP SA exists from successful negotiation to expiration.
Key Life	Duration for which the IPsec SA exists from successful negotiation to expiration.
Max Retries	Number of retry attempts for establishing the IPsec tunnel. Enter zero for unlimited retries.
Compression	Enable IPComp. This protocol increases the overall communication performance by compressing the datagrams. Compression requires greater CPU processing.

Field	Description
Aggressive Mode	Whether to allow a less secure mode that exchanges identification in plain text. This may be used for establishing tunnels where one or more endpoints have a dynamic public IP address. Although this mode is faster to negotiate phase 1, the authentication hash is transmitted unencrypted. You can capture the hash and start a dictionary or use brute force attacks to recover the PSK.

OpenVPN Tunnels

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can use and setup OpenVPN tunnels with this device.

To use OpenVPN, you must first install an OpenVPN application along with an easy-rsa tool and configure OpenVPN on your computer. Then you must also generate the certificates for the OpenVPN server and client before configuring the device.

To configure OpenVPN client and server on this device the following files are required:

- **The CA PEM file or CA certificate (.crt)**
- **The Diffie Hellman PEM file (.pem)**
- **The Server Certificate to be used by the device endpoint (.crt)**
- **The Server/Client Key to be used by the device endpoint (.key)**

Note: When you configure OpenVPN server and client make sure both sides use the same settings, and certificates.

Configuration 1: OpenVPN Tunnel with TLS Authorization Mode (Device only)

This first configuration establishes the OpenVPN Tunnel connection from a device client to a device server using TLS as Authorization Mode. This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

To add an **OpenVPN Server using TLS**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **TLS** from the drop-down.
 - c. **Protocol** as **UDP**.
 - d. **VPN Subnet**.
 - e. **Port** number.
 - f. **VPN Netmask**.
 - g. **LZO Compression** as **ADAPTIVE** from the drop-down.

- h. **Hash Algorithm** as **DEFAULT**.
 - i. **Encryption Cipher** as **DEFAULT**.
 - j. **Min. TLS Version** as **1.2**.
 - k. **TLS Cipher Suite** as **DEFAULT** as **1.2**.
 - l. Enter the contents of the following files generated from the easy-rsa tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad. (all required):
 - i. **CA PEM (.crt)**
 - ii. **Diffie Hellman PEM (.pem)**
 - iii. **Server Certificate PEM (.crt)**
 - iv. **Server Key PEM (.key)**
 - m. Select the **Encryption Cipher**
7. Click **Next**.
- Note: Use the same **CA PEM** certificate and parameters as the server for the OpenVPN clients .
8. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get an access to the client's network. In the **OpenVPN Tunnel** dialog box, under **Remote Network Routes**:
- a. Choose an available **Saved Network** as your remote network route from the drop-down if desired (optional).
 - b. Or enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
 - c. Enter the **Remote Network Mask** (usually 255.255.255.0).
 - d. You may enter **Gateway** (optional).
 - e. Click **Add Route**.
9. The system displays your recently-added **Push Route** with the client subnet (remote network route + mask).
10. **Push Routes** create a route from client's network to the server's network. This allows clients to get access to the server's network. Under **Push Routes**:
- a. Click **Client To Client** box if you want this optional feature (this establishes a connection between multiple clients that are connected to the server).
 - b. Choose an available **Saved Network** as your push route from the drop-down if desired (optional).
 - c. Or enter the **Remote Network Route** (same address as the server subnet above).
 - d. Or enter the **Remote Network Mask** (same as above).
 - e. You may enter **Gateway** (optional).
 - f. Click **Add Route**.
- Note: If you use **Static Key Authorization Mode**, the **Push Routes** do not work.
11. The system displays your recently-added **Push Route** with the client subnet (remote network route + mask).
12. Click **Next**.
13. The system displays the **Configuration Preview** window (read-only).
14. Click **Finish**.

15. Click **Save and Restart** to save your changes

To add an **OpenVPN Client using TLS**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name** of the tunnel.
4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Under OpenVPN Tunnel Configuration, enter the following fields (using **TLS** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **TLS** from the drop-down.
 - c. **Protocol** as **UDP**.
 - d. **Remote Host** (server public IP address).
 - e. **Remote Port** number.
 - f. **LZO Compression** as **ADAPTIVE** from the drop-down.
 - g. **Hash Algorithm** as **DEFAULT**.
 - h. **Encryption Cipher** as **DEFAULT**.
 - i. **Min. TLS Version** as **1.2**.
 - j. **TLS Cipher Suite** as **DEFAULT**.
 - k. Enter the contents of the following files generated from the easy-rsa tool. You can copy and paste this content from the certificate files after opening from a text editor like Notepad. (all required):
 - i. **CA PEM (.crt)**
 - ii. **Client Certificate PEM (.crt)**
 - iii. **Client Key PEM (.key)**
 - l. Click **Next**.
7. If you use **TLS** as **Authorization Mode**, you do not need configure or add **Remote Network Routes**. The server adds the routes if the server's **Push Routes** are already configured. If you use **Static Key** as **Authorization Mode**, you must add and configure **Remote Network Routes**.
8. Click **Next**.
9. The system displays the **Configuration Preview** window (read-only).
10. Click **Finish**.
11. Click **Save and Restart** to save your changes.

Now the device client can access the device server subnet. You can ping the IP address of the device server subnet from the client console to test this.

Note: The PC connected to the device does not have access to the device server subnet.

Configuration 2: OpenVPN Tunnel with TLS Authorization Mode (Device and Connected PC)

This second configuration provides access between a device server and its subnet and device client and its subnet. An additional configuration is needed on the device server side. This also allows your PC to connect with the device server and ultimately to the device client through that server.

1. Configure the device server as shown under how to add an **OpenVPN Server using TLS** (steps 1-14).
2. Open device console, go to `/var/config/ovpnccd/openVPNServerName`. Create the folder if not present in the device.
3. Create a file that has the client certificate name with the following information:
 - a. **iroute [Client_Subnet] [Mask]**
 - b. **example** -- echo "iroute 192.168.3.0 255.255.255.0" > mtrClient1
4. For each client, you must create a separate file in the folder `/var/config/ovpnccd/yourserverName`.
Note: Make the file name the same as the Common Name value used to create the certificate.
5. Configure device client as shown under how to **add an OpenVPN Client** (steps 1-12).

Once properly configured, you should have a connection between the device server and device client and their subnets. Your PC can also connect with the device server and thus the device client through that server.

Configuration 3: OpenVPN Tunnel with Static Key Authorization Mode (device server and client)

This third configuration establishes the OpenVPN Tunnel connection from a device client to a device server using Static Key as Authorization Mode. This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

When using Static Key, the OpenVPN tunnel is created between only two end-points, the client and server. You cannot connect more than one client to the server in this mode. Remote Network Route must be specified in both configurations, client and server, in order to establish the connection between subnets.

To add an **OpenVPN Server using Static Key**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Click **Next**.
7. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **STATIC KEY** from the drop-down.
 - c. **Protocol** as **UDP**.
 - d. **Local Address** as **DEFAULT**.
 - e. **Port** number.
 - f. **Remote Address** as **DEFAULT**.
 - g. **LZO Compression** as **ADAPTIVE** from the drop-down.
 - h. **Hash Algorithm** as **DEFAULT**.
 - i. **Encryption Cipher** as **DEFAULT**.
 - j. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

```
-----BEGIN OpenVPN Static key V1-----
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
```

```
d214482b8547ec9dca8910f514d9f4270ccaef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
c2e662128
```

-----END OpenVPN Static key V1-----

8. Click **Next**.
9. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel** dialog box, under **Remote Network Routes**:
 - a. Choose an available **Saved Network** as your remote network route from the drop-down if desired (optional).
 - b. Or enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
 - c. Enter the **Remote Network Mask** (usually 255.255.255.0).
 - d. Click **Add Route**.
10. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).
Note: **Push Routes are not required with Static Key as Authorization Mode.**
11. Click **Next**.
12. The system displays the **Configuration Preview** window (read-only).
13. Click **Finish**.
14. Click **Save and Restart** to save your changes.

To add an **OpenVPN Client using Static Key**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Click **Next**.
7. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **STATIC KEY** from the drop-down.
 - c. **Protocol** as **UDP**.
 - d. **Local Address** as **DEFAULT**.
 - e. **Remote Host**.
 - f. **Remote Address** as **DEFAULT**.
 - g. **Remote Port** number.
 - h. **LZO Compression** as **ADAPTIVE** from the drop-down.
 - i. Select the **Encryption Cipher** as **DEFAULT** from drop-down.
 - j. Select the **Hash Algorithm** as **DEFAULT** from drop-down.

- k. **Min. TLS Version** as **1.2**.
- l. **TLS Cipher Suite** as **DEFAULT**.
- m. Enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:


```
-----BEGIN OpenVPN Static key V1-----
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
d214482b8547ec9dca8910f514d9f4270ccaef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
c2e662128
-----END OpenVPN Static key V1-----.
```
- 8. Click **Next**.
- 9. **Remote Network Routes** create a route from the server network to the client network. This allows the client to get access to the server's network. In the **OpenVPN Tunnel** dialog box, under **Remote Network Routes**:
 - a. Choose an available **Saved Network** as your remote network route from the drop-down if desired (optional).
 - b. Or enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.2.1, enter 192.168.2.0.
 - c. Enter the **Remote Network Mask** (usually 255.255.255.0).
 - d. Click **Add Route**.
- 10. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).
Note: **Push Routes** are not required with **Static Key** as **Authorization Mode**.
- 11. Click **Next**.
- 12. The system displays the **Configuration Preview** window (read-only).
- 13. Click **Finish**.
- 14. Click **Save and Restart** to save your changes.

Configuration 4: OpenVPN Tunnel with Static Key Authorization Mode and TCP

This fourth configuration establishes the OpenVPN Tunnel connection from a device client to a device server using Static Key as Authorization Mode and TCP protocol (instead of UDP for the third configuration). This involves adding and configuring both OpenVPN Server and Client sides within the device UI.

To add an **OpenVPN Server** using **Static Key** and **TCP**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **SERVER** from the drop-down.
5. You can also enter an optional **Description**.
6. Click **Next**.

7. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **STATIC KEY** from the drop-down.
 - c. **Protocol** as **TCP**.
 - d. **Local Address** as **DEFAULT**.
 - e. **Port** number.
 - f. **Remote Address** as **DEFAULT**.
 - g. **Hash Algorithm** as **ECDSA-WITH-SHA1**.
 - h. **LZO Compression** as **ADAPTIVE** from the drop-down.
 - i. **Encryption Cipher** as **CAMELLIA-256-CBC**.
 - j. **Min. TLS Version** as **NONE**.
 - k. **TLS Cipher Suite** as **DEFAULT**.
 - l. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:


```
-----BEGIN OpenVPN Static key V1-----
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
d214482b8547ec9dca8910f514d9f4270ccaef1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
c2e662128
-----END OpenVPN Static key V1-----
```
8. Click **Next**.
9. **Remote Network Routes** create a route from the server network to the client network. This allows the server to get access to the client's network. In the **OpenVPN Tunnel** dialog box, under **Remote Network Routes**:
 - a. Choose an available **Saved Network** as your remote network route from the drop-down if desired (optional).
 - b. Or enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.3.1, enter 192.168.3.0.
 - c. Enter the **Remote Network Mask** (usually 255.255.255.0).
 - d. Or click **Add Route**.
10. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

Note: **Push Routes are not required with Static Key as Authorization Mode.**
11. Click **Next**.
12. The system displays the **Configuration Preview** window (read-only).
13. Click **Finish**.
14. Click **Save and Restart** to save your changes.

To add an **OpenVPN Client using Static Key and TCP**:

1. Go to **Tunnels > OpenVPN Tunnels > OpenVPN Tunnel Configuration**.
2. Click **Add Tunnel**.
3. Enter the **Name**.
4. Select the **Type** as **CLIENT** from the drop-down.
5. You can also enter an optional **Description**.
6. Click **Next**.
7. Enter the following fields (using **STATIC KEY** as **Authorization Mode**):
 - a. **Interface Type** as **TUN** from the drop-down.
 - b. **Authorization Mode** as **STATIC KEY** from the drop-down.
 - c. **Protocol** as **TCP**.
 - d. **Local Address** as **DEFAULT**.
 - e. **Remote Host**.
 - f. **Remote Address** as **DEFAULT**.
 - g. **Remote Port** number.
 - h. **Hash Algorithm** as **ECDSA-WITH-SHA1**.
 - i. **LZO Compression** as **ADAPTIVE** from the drop-down.
 - j. **Encryption Cipher** as **CAMELLIA-256-CBC**.
 - k. **Min. TLS Version** as **NONE**.
 - l. **TLS Cipher Suite** as **DEFAULT**.
 - m. Generate and enter the **Static Key PEM** (required). Both server and client must use the same static key. See example below:

```
-----BEGIN OpenVPN Static key V1-----
3f4c9113b2ec15a421cfe21a5af015bb967059021c1fd6f66ecfd00533d967237875215e20e80a2d59efd
79148d6acdea9358dcafe0efdbb54003ff376c71432dd9d16f55e7d8917a32bfe07d61591b7bbb43c7ba
d214482b8547ec9dca8910f514d9f4270ccaeff1a79852ae27c1c307c9dc3c836d1c380bece3c70fd2104
e1968ed29b6c3388719226f959f69f9be43688ed27bc3a4dbc83f640370524b47bb871816af79586d07
08781fad384480d0609b11c31d27baa6e902d29277a474e3e2785a8410d595c0f9c75312375b4bd098
76e1a47a598e114749a09c35f098e9123015c2795c702e4a346a8bccd00305c7cb30beef66ad33f43dac
c2e662128
-----END OpenVPN Static key V1-----
```
8. Click **Next**.
9. Remote Network Routes create a route from the server network to the client network. This allows the client to get access to the server's network. In the **OpenVPN Tunnel** dialog box, under **Remote Network Routes**:
 - a. Choose an available **Saved Network** as your remote network route from the drop-down if desired (optional).
 - b. Or enter the **Remote Network Route** (should be the client subnet). For example, if the client IP address is 192.168.2.1, enter 192.168.2.0.
 - c. Enter the **Remote Network Mask** (usually 255.255.255.0).
 - d. Click **Add Route**.
10. The system displays your recently-added **Remote Network Route** with the client subnet (remote network route + mask).

Note: **Push Routes are not required with Static Key as Authorization Mode.**

11. Click **Next**.
12. The system displays the **Configuration Preview** window (read-only).
13. Click **Finish**.
14. Click **Save and Restart** to save your changes.

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Chapter 12 – Device Administration

User Accounts

Use this feature to add user accounts or change the password.

The system offers three roles or user types: administrator, engineer, and monitor. Administrators have full rights and permissions including change settings on the device. Engineers have read/write privileges and some access to controls on the device. Monitors have read-only access. Note: the system automatically checks for a strong password and tells you how to improve it.

Username requirements include:

- Must be unique.
- Is case-sensitive (for example, admin and ADMIN are treated as two different usernames).
- Acceptable characters: uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric (symbols like #).
- A hyphen (-) should not be used as the first character.

Password requirements include:

- User account is disabled if password is not set up.
- Must be eight characters in length.
- Contains three or more different types of characters such as: uppercase alphabetic, lowercase alphabetic, numeric, and non-alphanumeric (symbols like #).

Administrator details:

- Able to delete any local users. (Engineer and Monitor cannot delete any users.)
- Able to modify any other user details, except username.
- Can not modify another administrator user account if it is the only enabled local administrator user on the device.
- Able to modify own account details except Role, Username, and Enabled values.
- Able to disable and enable any local users except their own account. Also, not able to disable local user account if this is only local administrator.
- Able to change own password and other user passwords.

Engineer and Monitor details:

- Able to view and modify own user account details except Role, Username, and Enabled values.
- Access to only their own user account.
- Not able to delete users.
- Able to change own password.

To add new users:

1. Go to **Administration > User Accounts**.
2. Click **Add New User**.
3. Under **User Details**, enter the following fields:

- a. Username (required)
 - b. Role (required). Select the user role from the drop-down menu including **administrator**, **engineer**, or **monitor**.
 - c. First Name
 - d. Last Name
 - e. Title
 - f. Division
 - g. Employee Identification
4. Under **Contact Information**, enter the following fields:
 - a. Email
 - b. Address
 - c. City
 - d. State
 - e. Country
 - f. Postal Code
 - g. Work Phone
 - h. Mobile Phone
 5. Click **Submit**.
 6. The **Change Password** page opens. Enter **New Password**. Click **Submit**.
 7. The **Change Password** page opens. Enter **New Password**. Click **Submit**.

If the password is not set up for the new user, the user is disabled until the password is set.

Self-Diagnostic

The device offers self-diagnostics or periodic monitoring of certain issues such as: flash memory checksums, memory errors or leaks, and security violations by applications.

This monitoring is intended to improve performance, detect corruption, or help prevent malicious activity. After an event is detected, the system disables the cellular radio module, sends an alarm or notification, logs the event, and sends a record of it to the SNMP server.

For the self-diagnostic features, go to **Administration > Self-Diagnostic** and refer to the following sections.

To turn on the **Resource Overuse** diagnostic that detects memory leaks or errors:

1. Check **Enabled** under **Resource Overuse**.
2. If you want the system to reboot the device after a **Resource Overuse** is detected, check **Reboot the device** under **Actions**.

To turn on the **Security Violation** diagnostic that detects security rule violations by applications:

1. Check **Enabled** under **Security Violation**.
2. If you want the system to disable WAN interfaces after a **Security Violation** is detected, check **Disable WAN Interfaces** under **Actions**.
3. If you want the system to disable user-defined firewall rules after a **Security Violation** is detected, check **Disable User-Defined Firewall Rules** under **Actions**.

To turn on the **Flash Memory Violation** diagnostic that performs a flash memory checksum check to protect the integrity of device firmware:

1. Check **Enabled** under **Flash Memory Violation**.
2. Enter the **Flash Memory Check Interval** (ranging between 4-24 hours). Default is 24.
3. If you want the system to disable WAN interfaces after a **Flash Memory Violation** is detected, check **Disable WAN Interfaces** under **Actions**.
4. If you want the system to disable user-defined firewall rules after a **Flash Memory Violation** is detected, check **Disable User-Defined Firewall Rules** under **Actions**.

After you completed your **Self-Diagnostic** configuration (selecting any or all of the above):

1. Click **Submit**.
2. To save changes, click **Save and Restart**.

If at any time you want to return the device to the default setting, click the **Reset to Default** button in the bottom right corner. (This disables or removes all enabled **Self-Diagnostic** features.)

Configuring Device Access

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

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

HTTP Redirect to HTTPS

The device allows only secure access to its Web UI. This set of rules automatically redirects HTTP requests to the device's secure HTTPS port.

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

HTTPS

The device provides secure Web UI access to modify its configurations and execute actions.

Field	Description
Port	The port on which the device will listen for HTTPS requests.

Field	Description
Via WAN/Cellular	If checked, the device 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.

HTTPS Security

Configure the HTTPS security settings (like version and cipher suite). Click the **Show** to the right under **Security Settings**. Must select **SSL/TLS** under **Protocol**.

Field	Description
Use default cipher suite	Enables use of the default cipher (check by default). No other user input is required.
TLS 1.2 or TLS 1.1	Check which version of the TLS protocol you want to use: TLS 1.2 or TLS 1.1. (Use default cipher suite must be unchecked.)
Cipher Suite Name	Check your preferred Cipher Suite from the following list: ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-GCM-SHA384, AES256-SHA, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-GCM-SHA256, DHE-RSA-AES128-SHA, and/or AES128-SHA

SSH

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

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

SSH Security

Configure the **SSH security settings** (like ciphers and HMAC). Click **Show** to the right under **Security Settings**. Must select **SSL/TLS** under **Protocol**.

Field	Description
Use default cipher suite	Enables use of the default cipher (check by default). No other user input is required.

Field	Description
Ciphers	Check which Cipher you want to use: AES128-CTR or AES256-CTR
HMAC	Check which hash-based message authentication code, you want to use: SHA1, SHA2-256,and/or SHA2-512

ICMP

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

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

SNMP

The device offers Simple Network Management Protocol (SNMP) which is used for collecting information from, and configuring network devices on an IP network. For more details, refer to **Configuring SNMP**.

Field	Description
Via LAN	Allows SNMP connections via LAN
Via WAN	Allows SNMP connections via WAN.

Modbus Slave

The Modbus feature allows the user to enable the Modbus query server. You can query this server over Modbus-TCP for status information.

Field	Description
Enabled (under Modbus Slave)	Enables the Modbus Query Server.
Via LAN	If checked, the device can query the Modbus server via LAN.
Port	Port number configured for Modbus.

For Modbus query information, refer to the MTR Modbus Information page on our Developer Resources website (on .net) for details: <http://www.multitech.net/developer/software/mtr-software/mtr-modbus-information/>

After making all your desired changes, click **Submit**, then click **Save and Restart**.

IP Defense

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

DoS Prevention

This area of the Access Configuration window engages a set of rules at the firewall that prevents Denial-of-Service attacks by limiting the amount of new connection requests to the device.

Field	Description
Enabled	Enables DoS prevention.
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 allowed burst for traffic spikes. A burst occurs when the Per Minute limit is reached. On a period where the Per Minute limit is not reached, one burst point is regained, up to the maximum.

Ping Limit

This area of the Access Configuration window engages a set of rules at the firewall that aims to prevent ping flood attacks by limiting the number of ICMP requests to the device. These rules that mitigate the effects of a ping DoS on your device do not apply if ICMP is disabled.

Field	Description
Enabled	Enables the Ping Limit feature.
Per Second	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.

RADIUS Configuration

The RADIUS protocol supports authentication, user session accounting, and authorization of users to the device. This authentication, accounting, and authorization is independent of the local users created on the device. The user can enable Authentication, Accounting, or both options.

RADIUS user details:

- Access to device if role is one of those in the provided list (Administrator, Engineer, or Monitor).
- All RADIUS users do not have SSH access to the device.
- RADIUS creates a temporary session instead of a local account like local users.
- RADIUS uses shared key encryption.
- Local users shall take priority over RADIUS user (if a RADIUS user has the same username as a local user, the RADIUS user cannot log in even if the local user is disabled).
- RADIUS user with Administrator role can view and modify all local users (but cannot delete a local Administrator if it is the only local admin user on the device).
- RADIUS users with Engineer and Monitor role cannot view or modify user details. They do not have access to the **User Accounts** page.
- RADIUS users cannot change their own password in the Web UI.

To set up the RADIUS server configuration:

1. Go to **Administration > RADIUS Configuration**.
2. To enable authentication, check **Enable Authentication**.
3. To enable accounting, check **Enable Accounting**.
4. Enter the following fields for **RADIUS configuration**:
 - a. Primary Server
 - b. Authentication Port (for Primary Server)
 - c. Accounting Port (for Primary Server)
 - d. Secondary Server
 - e. Authentication Port (for Secondary Server)
 - f. Accounting Port (for Secondary Server)
5. Under **Options**, enter the following fields:
 - a. **Shared Secret Key** value is used to: 1) encrypt packets between the RADIUS Server and device, 2) encrypt RADIUS attributes such as user password, and 3) verify that RADIUS messages have not been modified in transit. This value must be equal to the shared secret that is set up in RADIUS server. The Shared Secret Key can be up to 128 characters long. You can click the eye icon to hide the key.
 - b. Authentication Protocol: select from drop-down list including **PAP**, **EAP-PEAPv0/MSCHAPv2**, or **EAP-TTLS/PAPv0**
 - c. Timeout is the interval in seconds between tries to connect to RADIUS server in case of communication failure. Maximum is 10 seconds.
 - d. Retries is the number of tries to connect to RADIUS server in case of communication failure.
6. Advanced Options are used when Authentication Protocol is EAP-PEAPv0/MSCHAPv2 or EAP-TTLS/PAPv0. If Protocol is PAP, these settings are ignored:
 - a. Check **Use Anonymous ID** if you want to enable identity privacy. The device does not send its identity in plain text before the device has authenticated the RADIUS server.
 - b. Anonymous ID is a name or value that the device will use in the identity response when “Use Anonymous ID” is enabled.

- c. Check **Check Server Certificate Hostname** to allow the server certificate CN (common name) to be validated by the device.
7. Click **Submit**.
8. To save your changes, click **Save and Restart**

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Generating a New Certificate

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

To generate a new certificate:

1. Go to **Administration > X.509 Certificate**. The **X.509 Certificate** window displays the details of the certificate that is currently used.
2. Click **Generate** to open the **Generate Certificate** window.
3. In the **Common Name** field, enter the name, hostname, or IP address, depending on what you use to connect to the router. The web browser uses this field to check for a valid certificate.
4. In the **Days** field, enter the amount of days before the certificate will expire.
5. In the **Country** field, enter the 2-letter code for the country name.
6. In the **State/Province** field, enter the state or province for which the certificate is valid.
7. In the **Locality/City** field, enter the locality or the city for which the certificate is valid.
8. In the **Organization** field, enter the organization name for which the certificate is valid.
9. In the **Email Address** field, enter the email address of the person responsible for the router. Typically this is the administrator. This field may be left blank.
10. Click **Generate**. Wait until the certificate is generated. You may have to reboot to complete the operation.
11. If you are finished making changes, click **Save and Restart**.

Importing a Certificate

To import a certificate:

1. Go to **Administration > X.509 Certificate**. The Certificate window displays the details of the certificate that is currently used.
NOTE: A certificate with a key size greater than 2048 bits causes a delay accessing the Web UI after the device starts. A certificate with a key size less than 2048 bits is not recommended since it is less secure and may become breakable in the near future.
2. Click **Import** to open **Upload Certificate** window.
3. Click **Browse** to select a valid certificate to be uploaded.
4. Click **Upload**. Wait until the file is uploaded.

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

Uploading CA Certificate

This page allows a user to upload an X.509 CA (Certifying Authority) Certificate.

To upload a CA certificate:

1. Go to **Administration > X.509 CA Certificates**.
2. Click **Choose File** and browse for your CA certificate file.
3. Click **Open**.
4. Once your file is selected, click **Import**.
5. Your CA certificate file displays in the certificate list along with relevant details.
6. You may delete or remove a certificate by clicking the trash can icon to the right under **Options**.

Note: It can take up to two minutes to add or remove a certificate. The changes are applied immediately and there is no need to restart the device after CA certificate is added or removed.

Setting up the Remote Management

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

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

Managing Your Device Remotely

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

To configure your device to use DeviceHQ:

1. Go to **Administration > Remote Management** and check **Enabled**. See other options under *Setting up the Remote Server*.
2. Go to options under **Auto-Update Settings**.
3. To define how often the device connects to DeviceHQ to check in and request any pending updates, set the **Check-In Interval** field to the desired number of minutes between 240-10080 (240 minutes to 1 week).

Note:

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

4. To define how often the device connects to DeviceHQ to send GPS data, set the **GPS Data Interval** field to the desired number of minutes, between 240-10080 (240 minutes to 1 week). **Note:** Some MTR models do not have GPS. In this case, the system does not display this field.
5. If you want the device to connect to DeviceHQ only when the device's cellular link is up, check **Sync with Dial-On-Demand**.

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

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

Unavailable Services in PPP-IP Passthrough and Serial Modem Modes

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

Notifications

The device can send alerts via email, SMS, and/or SNMP. To use these options, enable SMTP (see [SMTP Settings](#) for details), SMS (see [Configuring SMS](#) for details), and SNMP Traps (see [Configuring SNMP](#) for details).

A time stamp is added to the actual notifications. The format is **YYYY-MM-DD HH:MM**.

To setup notifications:

1. Go to **Administration > Notifications > Configuration**.
2. Under **Recipient Group**, click **Add Group** (you must add a group before you can edit/save your alert).
3. In the **Create Recipient Group** window, enter your **Group Name**.
4. Click **Add Phone**. Enter the person's **Name** and **Phone Number**. Then click **Finish**.
5. Click **Add Email**. Enter the person's **Name** and **Email**. Then click **Finish**.
6. Add name, phone number and email for each person in your group. When done, click **Submit**.
7. See the list of available alerts:
 - **High Data Usage**
 - **Low Signal Strength**
 - **Device Reboots**
 - **Ethernet Interface Failure**
 - **Cellular Interface Failure**
 - **Ethernet Data Traffic**
 - **Cellular Data Traffic**
 - **WAN Interface Failover**

- Ping Failure
- Security Violation
- Flash Memory Violation
- Resource Overuse
- Wi-Fi Interface Failure*
- Wi-Fi Data Traffic*

*Only available on non-LTE devices

8. Click on the pencil icon under the **Edit** column for the alert you want to use and configure. The **Edit** dialog box appears for your chosen alert.

For **High Data Usage**:

1. Check **Enabled**.
2. Under **Data Plan Details**, select the **Plan Type** from the drop down menu which includes **Monthly** or **Custom Interval**.
3. If you choose **Custom Interval**, enter the **Interval** length in days.
4. Select the **Start Date** from the calendar picker.
5. Enter the **Limit** in **MB** for data usage.
6. In **Notify At**, enter the percentage of the limit that triggers notification to be sent.
7. Select alert recipients from **Recipient Group**.
8. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
9. Click **Finish**.
10. To save your changes, click **Save and Restart**.

For **Low Signal Strength**:

1. Check **Enabled**.
2. Enter the **Signal Threshold** in **dBm**.
3. Enter the **Duration** in seconds.
4. Under **Alerts**, select the recipients under **Recipient Group**.
5. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
6. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

For **Device Reboots**:

1. Check **Enabled**.
2. Under **Alerts**, select the recipients under **Recipient Group**.
3. In **Notify**, the field for frequency of notification is shown. The predefined value is **Always** and cannot be modified by the user.
4. Select how you want to send alerts by clicking **Email**, **SMS**, or **SNMP**.
5. Click **Finish**.
6. To save your changes, click **Save and Restart**.

For **Ethernet Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

For **Cellular Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

For **Ethernet Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **both**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

For **Cellular Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **both**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

For **WAN Interface Failover**:

1. Check **Enabled**.
2. Enter the **Timeout** in seconds.
3. Select what to **Notify On** from the drop-down.
4. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
5. In **Notify**, the constant value is **Always**.
6. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.

7. Click **Finish**.
8. To save your changes, click **Save and Restart**.

For **Ping Failure**:

1. Check **Enabled**.
2. Under **Ping Details**, select the **Network Interface** from the drop-down.
3. Enter the **IP Address** or **URL** that you want to ping.
4. Enter the **Count**.
5. Enter the **Failure Threshold**.
6. Enter the **Ping Interval**.
7. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
8. In **Notify**, the constant value is **Always**.
9. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
10. Click **Finish**.
11. To save your changes, click **Save and Restart**.

For **Security Violation**:

1. Check **Enabled**.
2. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
3. In **Notify**, the constant value is **Always**.
4. Select how you want to send alerts by clicking **Email**, **SMS** , or **SNMP**.
5. Click **OK**.

For **Flash Memory Violation**:

1. Check **Enabled**.
2. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
3. In **Notify**, the constant value is **Always**.
4. Select how you want to send alerts by clicking **Email**, **SMS** , or **SNMP**.
5. Click **OK**.

For **Resource Overuse**:

1. Check **Enabled**.
2. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
3. In **Notify**, the constant value is **Always**.
4. Select how you want to send alerts by clicking **Email**, **SMS** , or **SNMP**.
5. Click **OK**.

The following notifications are only available on non-LTE devices:

For **Wi-Fi Interface Failure**:

1. Check **Enabled**.
2. Enter the **Duration** in seconds.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.

4. In **Notify**, enter the frequency of notification (in hours). Default is **24**.
5. Select how you want to send alerts by clicking **Email**, **SMS** or **SNMP**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

For **Wi-Fi Data Traffic**:

1. Check **Enabled**.
2. Enter **Interval** in hours when alert is sent.
3. Under **Notification Options**, select the recipients from the drop-down in **Recipient Group**.
4. In **Notify**, the constant value is **Always**.
5. Select how you want to send alerts by clicking **Email** or **SMS**.
6. Click **Finish**.
7. To save your changes, click **Save and Restart**.

Customizing the User Interface

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

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

Customizing Support Information

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

1. To enable display of the custom support information, go to **Administration > Web UI Customization > Support Information** and check **Show Custom Info**.
2. Type the desired information into the optional fields including:
 - **Company Name**
 - **Country**
 - **Fax**
 - **Address 1**
 - **Address 2**
 - **City**
 - **State/ Prv**
 - **Zip Code**
 - **City**
3. To add a phone number:
 - a. Click **Add Phone**.
 - b. A label can appear next to the phone number, for example **Fax** or **Phone** or **International**. In the **Label** field, enter text that describes the phone number.
 - c. In the **Number** field, type the phone number.

4. To add a link to a website, click **Add Link**.
 - a. To label the website, type label text in **Label** field.
 - b. In the **URL** field, type the website's link.
 - c. To add further descriptive text about the site, type the information in the **Text** field.
5. To add an image, click **Upload Image**:
 - a. Click **Browse**, go to the location of the image, and select the image.
 - b. Click **OK**.
6. To delete an existing image, click **Remove Image**.
7. Click **Submit**.
8. To save your changes, click **Save and Restart**.

Specifying Device Settings

To define other custom settings for devices:

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

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

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

Upgrading Firmware

Before upgrading: reboot the device.

Upgrade the device's firmware to the latest version. You can download firmware upgrades from the MultiTech website or update your firmware automatically through MultiTech's DeviceHQ™ system.

For added security, you have the option to use **Signed Firmware Validation** when upgrading from version 4.1 and higher. This authentication method prevents attempts to load invalid or damaged firmware files in order to defeat possible tampering. If you check this option, the module does not load any firmware that Multitech did not digitally sign.

When downgrading to an older version of firmware or upgrading from versions lower than 4.1, you must uncheck this option.

If the **Signed Firmware Validation** is unchecked, the system runs an MD5 checksum automatically to check integrity of your target firmware file. If the MD5 checksum fails, the system generates an error saying the file integrity checks failed on the target file.

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

1. Before you upgrade your firmware, save your present configuration as a backup. Otherwise, see [DeviceHQ](#).
2. Go to the MultiTech website, locate the firmware upgrade file you want for your device, and download this file to a known location.
3. Select **Administration > Firmware Upgrade**. The Administration: Firmware Upgrade pane opens.
4. If you want further validation of your upgrade file, you can check **Signed Firmware Validation** option (checked by default). This works for upgrading from versions 4.1 or higher. (If unchecked, the system automatically runs an MD5 checksum.)
5. Click the **Choose Firmware Upgrade File** button:
 - a. Click **Browse** to find where the firmware file resides that you want to apply.
 - b. Select the file and click **Open**. The file name appears next to the **Choose Firmware Upgrade File** button. Make sure you select the correct BIN file; otherwise, your device can become inoperable.
6. Click **Start Upgrade**.
7. 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.
8. After the firmware upgrade is complete, verify your configuration to make sure it is what you expected.

Note:

- The new firmware is written into flash memory.
- It may take up to 10 minutes to upgrade the firmware. Do not interfere with the device's power or press the reset button during this time.
- The DeviceHQ is a cloud platform that provides the ability to remotely manage and upgrade devices. Please see the **Remote Management** section or visit www.devicehq.com for more information.

Saving and Restoring Settings

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

1. Go to **Administration > Save/Restore > Upload Configuration**.
2. To restore a configuration from a previously saved file, go to **Restore Configuration From File**:
 - a. Next to the **Restore Configuration** field, click **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 save your current configuration to a file, go to **Save Configuration To File**:
 - a. Click **Save**.

- b. Navigate to the location where you wish to save the file and select location.
- 4. This option is only available if you had reset to user-defined configuration. (Also, holding the reset button on the device for 30 seconds overrides user-defined settings and resets to factory default.) To reset the device's configuration to the factory settings, go to **Reset to Factory Default Configuration**:
 - a. Click **Reset**.
 - b. A dialog box appears prompting you to confirm that you want to restore to factory default settings.
 - c. Click **OK**.
- 5. This option is only available if you set user-defined settings first. (Also, holding the reset button on the device for 5 seconds sets user-defined defaults) To restore the device's configuration to the user-defined configuration settings, go to **Reset to User-Defined Configuration**:
 - a. Click **Restore**.
 - b. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
 - c. Click **OK**.
- 6. To set deployment-specific default settings, click **Set Current Configuration As User-Defined Default**.
 - a. A dialog box appears prompting you to confirm that you want to restore to a set of user-defined settings.
 - b. Click **OK**.
- 7. To save a current configuration:
 - a. Click **Save**.
 - b. A dialog box appears asking you if you want to open or save the configuration file. Click **Save**.
 - c. Navigate to the location where you want to store the configuration. Click **Save**.
 - d. A progress dialog box appears to indicate that the configuration is being saved. Click **Close**.

Using the Debugging Options

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

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

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

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

See also: [Statistics Configuration Fields](#)

Automatically rebooting the device

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

1. Go **Administration > Debug Options > Auto Reboot Timer**, select **DISABLED**, **HOUR OF DAY**, and **TIMER** from the drop-down list under **Auto Reboot**.

2. In the **Auto Reboot Timer** field, select the **Hour of the Day** (0-23) and then enter **Hour of the Day to Restart** (0-23).
3. If you do NOT want the device to automatically reboot, set the time to **0**. The default setting is **0**.

Setting up Telnet

To enable and configure Telnet on your device:

1. Go to **Administration > Debug Options > Telnet**, check **Enabled**.
2. Enter the **Port** number for Telnet.
3. Enter the **Username**.
4. Enter the **Password**. Enter it again under **Confirm Password**.
5. Click **Submit**.
6. To save your settings, click **Save and Restart**.

Configuring Remote Syslog

To enable and configure Remote Syslog to capture and send log data from your device, you must have local syslog software installed.

To set up a log request in DeviceHQ, under **Devices**, select your device. Then click on **Tasks** and select **Request Device Logs**. After the request has been completed, return to the device administration software.

1. To activate **Remote Syslog**, go to **Administration > Debug Options > Logging** under **Remote Syslog**, check **Enabled**.
2. To enable a remote server to receive and store the device'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**, select the type of information from the values in the dropdown menu which includes: **Minimum, Error, Warning, Info, Debug, and Maximum**. The system will collect the type of information you specify. For example, **Maximum** will collect all the log data available while **Warning** will collect anything that is a warning or above that level.
4. To download syslog information directly from the device, click **Download**.
5. Click **Submit**.
6. To save your changes, click **Save and Restart**.

Statistics Settings

To configure **Statistics**:

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

Ping and Reset Options

Perform a Ping Test

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

To perform a ping test:

1. Go to **Administration > Debug Options > Ping**.
2. Enter the **IP address or URL** of the site you wish to ping.
3. Under **Network Interface**, choose from the available drop-down list options including: **ANY, LAN, CELLULAR**, and **ETHERNET**.
4. Click **Ping**.

Reset Options

To reset the modem, go to **Administration > Debug Options > Reset Options**, click **Reset Modem**. If successful, the system displays a message confirming a successful reset.

Usage Policy

The device shall provide a Usage Policy for the system. The default usage policy reads as follows:

This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

This policy displays on the login page. You may modify or add language to the policy as needed.

To view or modify the **Usage Policy**:

1. Go to **Administration > Usage Policy**.
2. The default language appears. You may edit the language directly in the text box.
3. When completed, click **Submit**.
4. To save your changes, click **Save and Restart**.

If at any time you want to return the device to the default setting, click the **Reset to Default** button in the bottom right corner. (This reverts the **Usage Policy** back to the default language.)

Chapter 13 – Device Status

Viewing Device Statistics

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

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

System

Ethernet

Wi-Fi

Access Point

Cellular

Serial

Bluetooth

GRE

IPSec

OpenVPN

Definitions

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. The following list includes some definitions to help you understand some of the data. Not all of the available statistics are listed here or shown in every tab.

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

Cumulative and Daily Usage

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

Timeframe of Chart

Change the time frame for the chart by clicking **Start Date** or **End Date** using calendar to set a different date.

Show Log

The associated run-time logs for this section.

Mail Log

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

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

Mail Queue

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

1. Go to **Status & Logs > Mail Queue** to display the **Mail Queue** window.
2. To view the delivery details for an individual email, click the eye icon under **Options** for the desired email entry.

RF Survey

RF survey is not available for LTE models.

If you have a non-LTE device with a SIM card and want to perform an RF Survey, enter this address: 192.168.2.1/rf_survey and follow the instructions below. (The link uses the default IP address for the device upon log in. If you change the IP address of the device, make sure to use that new IP address in the link).

After the RF Survey, you must reset the device in order to restore cellular radio functionality.

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

1. Enter this address: 192.168.2.1/rf_survey to open the **RF Survey** page.
 - The search for the cell towers takes up to 2 minutes. The wait icon displays while the search is in progress.
 - The cell tower to which the router is currently connected displays at the top of the list.
2. 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 helps you decide which area has better signal strength and thus a better location for the router.

3. After the RF survey, reset your device. Go to **Commands > Restart Device**.

Service Statistics

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

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

Statistics Configuration Fields

The device 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 MB. For the default scenario, the device saves the data if more than 5 minutes has elapsed, or if more than 5 MB has been sent or received from the last check. The device checks these conditions every minute, but the data is saved only if one of the conditions is met.

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

Notifications Sent

This page displays attempts to send Notifications via email, SMS, or SNMP.

The list includes the following details of each attempted notification: **Date**, **Message**, **Recipient Group**, and the status of the notification under each communication method including **Email**, **SMS**, and **SNMP**. A check indicates success via that method. An **X** means failure. No symbol or a blank space indicates that method was not attempted.

To view **Notifications Sent**:

1. Go to **Status & Logs > Notifications Sent**.
2. In the upper right corner, click **Refresh** to update the list.
3. To the right of **Refresh**, click **Delete All Notifications** if you want to remove all items in the list.

Chapter 14 – 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 license-exempt RSS standard(s). The operation is permitted for the following two conditions:

1. the device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

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'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 Radio Equipment Directive (RED) Compliance



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

- Council Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment;
- and
- Council Directive 2014/53/EU on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

MultiTech declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The declaration of conformity may be requested at <https://support.multitech.com>.

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 that 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 to be 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。