Operating Manual

BulletPlus
4G/LTE Dual SIM Ethernet/Serial/USB Gateway w/WIFI

FW: v1.3.0 Build 1014

June 2016
Important User Information

Warranty

Microhard Systems Inc. warrants that each product will be free of defects in material and workmanship for a period of one (1) year for its products. The warranty commences on the date the product is shipped by Microhard Systems Inc. Microhard Systems Inc.’s sole liability and responsibility under this warranty is to repair or replace any product which is returned to it by the Buyer and which Microhard Systems Inc. determines does not conform to the warranty. Product returned to Microhard Systems Inc. for warranty service will be shipped to Microhard Systems Inc. at Buyer’s expense and will be returned to Buyer at Microhard Systems Inc.’s expense. In no event shall Microhard Systems Inc. be responsible under this warranty for any defect which is caused by negligence, misuse or mistreatment of a product or for any unit which has been altered or modified in any way. The warranty of replacement shall terminate with the warranty of the product.

Warranty Disclaims

Microhard Systems Inc. makes no warranties of any nature of kind, expressed or implied, with respect to the hardware, software, and/or products and hereby disclaims any and all such warranties, including but not limited to warranty of non-infringement, implied warranties of merchantability for a particular purpose, any interruption or loss of the hardware, software, and/or product, any delay in providing the hardware, software, and/or product or correcting any defect in the hardware, software, and/or product, or any other warranty. The Purchaser represents and warrants that Microhard Systems Inc. has not made any such warranties to the Purchaser or its agents. EXPRESS WARRANTY TO BUYER CONSTITUTES MICROHARD SYSTEMS INC. SOLE LIABILITY AND THE BUYER’S SOLE REMEDIES. EXCEPT AS PROVIDED, MICROHARD SYSTEMS INC. DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

MICROHARD SYSTEMS INC. PRODUCTS ARE NOT DESIGNED OR INTENDED TO BE USED IN ANY LIFE SUPPORT RELATED DEVICE OR SYSTEM RELATED FUNCTIONS NOR AS PART OF ANY OTHER CRITICAL SYSTEM AND ARE GRANTED NO FUNCTIONAL WARRANTY.

Indemnification

The Purchaser shall indemnify Microhard Systems Inc. and its respective directors, officers, employees, successors and assigns including any subsidiaries, related corporations, or affiliates, shall be released and discharged from any and all manner of action, causes of action, liability, losses, damages, suits, dues, sums of money, expenses (including legal fees), general damages, special damages, including without limitation, claims for personal injuries, death or property damage related to the products sold hereunder, costs and demands of every and any kind and nature whatsoever at law.

IN NO EVENT WILL MICROHARD SYSTEMS INC. BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, BUSINESS INTERRUPTION, CATASTROPHIC, PUNITIVE OR OTHER DAMAGES WHICH MAY BE CLAIMED TO ARISE IN CONNECTION WITH THE HARDWARE, REGARDLESS OF THE LEGAL THEORY BEHIND SUCH CLAIMS, WHETHER IN TORT, CONTRACT OR UNDER ANY APPLICABLE STATUTORY OR REGULATORY LAWS, RULES, REGULATIONS, EXECUTIVE OR ADMINISTRATIVE ORDERS OR DECLARATIONS OR OTHERWISE, EVEN IF MICROHARD SYSTEMS INC. HAS BEEN ADVISED OR OTHERWISE HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND TAKES NO ACTION TO PREVENT OR MINIMIZE SUCH DAMAGES. IN THE EVENT THAT REGARDLESS OF THE WARRANTY DISCLAIMERS AND HOLD HARMLESS PROVISIONS INCLUDED ABOVE MICROHARD SYSTEMS INC. IS SOMEHOW HELD LIABLE OR RESPONSIBLE FOR ANY DAMAGE OR INJURY, MICROHARD SYSTEMS INC’S LIABILITY FOR ANY DAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY MICROHARD SYSTEMS INC. ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.

Proprietary Rights

The Buyer hereby acknowledges that Microhard Systems Inc. has a proprietary interest and intellectual property rights in the Hardware, Software and/or Products. The Purchaser shall not (i) remove any copyright, trade secret, trademark or other evidence of Microhard Systems Inc.’s ownership or proprietary interest or confidentiality other proprietary notices contained on, in or to the Hardware, Software or Products, (ii) reproduce or modify any Hardware, Software or Products or make any copies thereof, (iii) reverse assemble, reverse engineer or decompile any Software or copy thereof in whole or in part, (iv) sell, transfer or otherwise make available to others the Hardware, Software, or Products or documentation thereof or any copy thereof, except in accordance with this Agreement.
Important User Information (continued)

About This Manual

It is assumed that users of the products described herein have either system integration or design experience, as well as an understanding of the fundamentals of radio communications.

Throughout this manual you will encounter not only illustrations (that further elaborate on the accompanying text), but also several symbols which you should be attentive to:

- **Caution** or **Warning**
  Usually advises against some action which could result in undesired or detrimental consequences.

- **Point to Remember**
  Highlights a key feature, point, or step which is noteworthy. Keeping these in mind will simplify or enhance device usage.

- **Tip**
  An idea or suggestion to improve efficiency or enhance usefulness.

- **Information**
  Information regarding a particular technology or concept.
Important User Information (continued)

Regulatory Requirements / Exigences Réglementaires

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna being used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

WARNING

Pour satisfaire aux exigences de la FCC d'exposition RF pour les appareils mobiles de transmission, une distance de séparation de 23cm ou plus doit être maintenue entre l'antenne de cet appareil et les personnes au cours de fonctionnement du dispositif. Pour assurer le respect, les opérations de plus près que cette distance n'est pas recommandée. L'antenne utilisée pour ce transmetteur ne doit pas être co-localisées en conjonction avec toute autre antenne ou transmetteur.

MAXIMUM EIRP

FCC Regulations allow up to 36dBm Effective Isotropic Radiated Power (EIRP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed 36dBm.

WARNING

Réglementation de la FCC permettra à 36dBm Puissance isotope rayonnée équivalente (EIRP). Par conséquent, la somme de la puissance transmise (en dBm), la perte de câblage et le gain d'antenne ne peut pas dépasser 36dBm.

EQUIPMENT LABELING / ÉTIQUETAGE DE L'ÉQUIPEMENT

This device has been modularly approved. The manufacturer, product name, and FCC and Industry Canada identifiers of this product must appear on the outside label of the end-user equipment.

WARNING

Ce dispositif a été approuvé de façon modulaire. Le fabricant, le nom du produit, et la FCC et de l'Industrie du Canada identifiants de ce produit doit figurer sur l'étiquette à l'extérieur de l'équipement de l'utilisateur final.

SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE :

BulletPlus (Contains):

FCCID: NS915PX2
IC: 3142A-15PX2

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.

Please Note: These are only sample labels; different products contain different identifiers. The actual identifiers should be seen on your devices if applicable. S'il vous plaît noter: Ce sont des exemples d'étiquettes seulement; différents produits contiennent des identifiants différents. Les identifiants réels devrait être vu sur vos périphériques le cas échéant.
CSA Class 1 Division 2 Option

CSA Class 1 Division 2 is Available Only on Specifically Marked Units

If marked this for Class 1 Division 2 – then this product is available for use in Class 1 Division 2, in the indicated Groups on the product.

In such a case the following must be met:

The transceiver is not acceptable as a stand-alone unit for use in hazardous locations. The transceiver must be mounted within a separate enclosure, which is suitable for the intended application. Mounting the units within an approved enclosure that is certified for hazardous locations, or is installed within guidelines in accordance with CSA rules and local electrical and fire code, will ensure a safe and compliant installation.

The antenna feed line; DC power cable and interface cable must be routed through conduit in accordance with the National Electrical Code.

Do not connect or disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver’s installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

The wall adapters supplied with your transceivers are NOT Class 1 Division 2 approved, and therefore, power must be supplied to the units using the screw-type or locking type connectors supplied from Microhard Systems Inc. and a Class 1 Division 2 power source within your panel.

If you are unsure as to the specific wiring and installation guidelines for Class 1 Division 2 codes, contact CSA International.

CSA Classe 1 Division 2 est disponible uniquement sur les unités particulièrement marquées

Si marqué cette Classe 1 Division 2 - alors ce produit est disponible pour une utilisation en Classe 1 Division 2 , dans les groupes indiqués sur le produit .

Dans un tel cas, la suivante doit être remplie :

L'émetteur-récepteur n'est pas acceptable comme une unité autonome pour une utilisation dans des endroits dangereux . L'émetteur-récepteur doit être monté dans un boîtier séparé , qui est approprié pour l'application envisagée. Montage des unités dans une enceinte approuvée qui est certifié pour les emplacements dangereux , ou est installé à l'intérieur des lignes directrices , conformément aux règles de la CSA et le code électrique local et le feu , assurera une installation sûre et conforme .

La ligne d'alimentation d'antenne , câble d'alimentation CC et le câble d'interface doivent être acheminés à travers le conduit en conformité avec le National Electrical Code .

Ne pas connecter ou déconnecter l'équipement que l'alimentation est coupée ou que la zone est connue pour être non dangereux .

Installation, l'exploitation et la maintenance de l'émetteur-récepteur doivent être en conformité avec le manuel d'installation de l'émetteur-récepteur , et le National Electrical Code .

Falsification ou le remplacement des composants non - usine peut nuire à l'utilisation sécuritaire de l'émetteur-récepteur dans des endroits dangereux , et peut annuler l'approbation .

Les adaptateurs muraux fournis avec les émetteurs-récepteurs sont PAS classe 1, division 2 ont approuvé , et par conséquent, doit être alimenté pour les unités à l'aide des connecteurs de type vis ou verrouillage fournis par Microhard Systems Inc. et une Division 2 source d'alimentation de classe 1 au sein de votre panneau .

Si vous n'êtes pas sûr de l'établissement et de câblage des lignes directrices spécifiques pour la classe 1 Division 2 codes , communiquer avec la CSA International.
# Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
<th>Initials</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Preliminary. (Firmware v1.3.0-r1009-28)</td>
<td>PEH</td>
<td>Nov 2015</td>
</tr>
<tr>
<td>1.1</td>
<td>Updated to firmware v1.3.0-r1010. Added Bandwidth, Cloud Filter, Webfilter, MultiWAN, GRE. Misc updates to screenshots &amp; formatting.</td>
<td>PEH</td>
<td>Dec 2015</td>
</tr>
<tr>
<td>1.2</td>
<td>Updated to firmware v1.3.0-r1012. Misc corrections, added VRRP, updated Data Usage, Carrier Settings.</td>
<td>PEH</td>
<td>Apr 2016</td>
</tr>
<tr>
<td>1.3</td>
<td>Updated to firmware v1.3.0-r1014.</td>
<td>PEH</td>
<td>May 2016</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Misc. corrections.</td>
<td>PEH</td>
<td>June 2016</td>
</tr>
</tbody>
</table>
Table of Contents

1.0 Overview .................................................................................................................. 10
  1.1 Performance Features .......................................................................................... 10
  1.2 Specifications ....................................................................................................... 11

2.0 QUICK START ......................................................................................................... 13
  2.1 Installing the SIM Card ....................................................................................... 13
  2.2 Getting Started with Cellular ............................................................................. 13

3.0 Hardware Features ................................................................................................. 17
  3.1 BulletPlus ............................................................................................................. 17
    3.1.1 BulletPlus Mechanical Drawings .................................................................. 18
    3.1.2 BulletPlus Mounting Bracket (Optional) ..................................................... 19
    3.1.2.1 BulletPlus Connectors & Indicators ....................................................... 20
    3.1.2.2 Front & Top ............................................................................................. 20
    3.1.2.3 Rear & Side ......................................................................................... 21

4.0 Configuration .......................................................................................................... 22
  4.0 Web User Interface ............................................................................................... 22
    4.0.1 Logon Window ............................................................................................. 23
  4.1 System .................................................................................................................. 24
    4.1.1 Summary ...................................................................................................... 24
    4.1.2 Settings ........................................................................................................ 25
        Host Name ..................................................................................................... 25
        Console Timeout ............................................................................................ 25
        Date/Time ...................................................................................................... 26
        NTP Server Settings .................................................................................... 27
    4.1.3 Services ........................................................................................................ 28
        FTP ................................................................................................................ 28
        Telnet ............................................................................................................. 28
        HTTP/HTTPS ............................................................................................... 28
    4.1.4 Keepalive ...................................................................................................... 29
    4.1.5 Maintenance ................................................................................................. 31
        Firmware Upgrade .......................................................................................... 31
        Reset to Default ............................................................................................ 31
        Backup & Restore Configurations .................................................................. 32
    4.1.6 Reboot .......................................................................................................... 33
  4.2 Network ................................................................................................................. 34
    4.2.1 Summary ...................................................................................................... 34
    4.2.2 LAN .............................................................................................................. 35
        LAN DHCP .................................................................................................... 37
        VLAN Configuration ...................................................................................... 39
    4.2.3 WAN .............................................................................................................. 40
    4.2.4 DHCP (MAC Binding) ................................................................................... 42
    4.2.5 DDNS ........................................................................................................... 43
    4.2.6 Routes .......................................................................................................... 44
    4.2.7 VRRP (Virtual Router Redundancy Protocol) ............................................. 46
    4.2.8 Ports (Switch) .............................................................................................. 47
    4.2.9 Bandwidth (Throttling Control) .................................................................... 48
    4.2.10 Device List .................................................................................................. 49
    4.2.11 Cloud Filter (Content/Security Filter) ....................................................... 50
    4.2.12 WebFilter (MAC/Network Content Filter) .............................................. 51
    4.2.13 MultiWAN ................................................................................................. 53
# Table of Contents

4.3 Carrier .................................................................................................................. 56
  4.3.1 Status .................................................................................................................. 56
  4.3.2 Settings .............................................................................................................. 57
    Dual Cards Management .......................................................................................... 58
    APN ......................................................................................................................... 59
  4.3.3 SMS .................................................................................................................... 61
  4.3.4 SMS Config ....................................................................................................... 61
    SMS Commands ........................................................................................................ 61
    SMS Alerts .............................................................................................................. 63
  4.3.5 Data Usage ....................................................................................................... 65
    Data Usage History .................................................................................................. 68
4.4 Wireless .................................................................................................................. 69
  4.4.1 Status ................................................................................................................ 69
  4.4.2 Radio1 ................................................................................................................ 70
    Radio1 Phy Configuration ....................................................................................... 70
    Radio Virtual Interface ............................................................................................ 73
  4.4.3 Hotspot ............................................................................................................. 76
4.5 Firewall ................................................................................................................... 80
  4.5.1 Summary .......................................................................................................... 80
  4.5.2 General ............................................................................................................. 81
  4.5.3 Port Forwarding ................................................................................................. 83
  4.5.4 MAC-IP List ..................................................................................................... 85
  4.5.5 Rules ................................................................................................................ 87
  4.5.6 Firewall Default ............................................................................................... 89
4.6 VPN ......................................................................................................................... 90
  4.6.1 Summary .......................................................................................................... 90
  4.6.2 Gateway to Gateway ...................................................................................... 91
  4.6.3 Client to Gateway (L2TP Client) ..................................................................... 96
  4.6.4 OpenVPN ......................................................................................................... 98
    OpenVPN Server .................................................................................................... 98
    OpenVPN Client ................................................................................................... 101
  4.6.4 GRE ................................................................................................................ 103
  4.6.5 VPN Users ...................................................................................................... 106
  4.6.6 Certificate Management .................................................................................. 107
4.7 Router ..................................................................................................................... 108
  4.7.1 RIPV2 ............................................................................................................. 108
  4.7.2 OSPF .............................................................................................................. 109
4.8 Serial ....................................................................................................................... 110
  4.8.1 Summary ......................................................................................................... 110
  4.8.2 Settings .......................................................................................................... 111
    USB ......................................................................................................................... 111
    Data Baud Rate ..................................................................................................... 112
    IP Protocol Config ............................................................................................... 114
      TCP Client ........................................................................................................ 114
      TCP Server ....................................................................................................... 114
      TCP Client/Server ............................................................................................. 115
    UDP Point-to-Point ............................................................................................. 115
    SMTP Client ........................................................................................................ 115
    PPP ......................................................................................................................... 116
    GPS Transparent Mode ...................................................................................... 117
4.9 I/O .......................................................................................................................... 118
  4.9.1 Settings .......................................................................................................... 118
# Table of Contents

## 4.10 GPS
- 4.10.1 Location ........................................................................................................... 120
- 4.10.2 Settings ........................................................................................................... 121
- 4.10.3 Report .............................................................................................................. 122
- 4.10.4 GPSGate .......................................................................................................... 124
- 4.10.5 Recorder .......................................................................................................... 127
- 4.10.6 Load Record .................................................................................................... 129
- 4.10.7 TAIP ................................................................................................................ 131

## 4.11 Apps .................................................................................................................... 133
- 4.11.1 Modbus ........................................................................................................... 133
  - 4.11.1.1 TCP Modbus ............................................................................................. 133
  - 4.11.1.2 Serial (COM) Modbus ............................................................................. 135
  - 4.11.1.3 Modbus Data Map .................................................................................... 136
- 4.11.2 Netflow Report ............................................................................................... 137
- 4.11.3 Local Monitor ................................................................................................ 138
- 4.11.4 Event Report ................................................................................................... 140
  - 4.11.4.1 Configuration ........................................................................................... 140
  - 4.11.4.2 Message Structure .................................................................................... 141
  - 4.11.4.2 Message Payload ...................................................................................... 142
- 4.11.5 Websocket ...................................................................................................... 143

## 4.12 Diag ....................................................................................................................... 145
- 4.12.1 Ping ................................................................................................................ 145
- 4.12.2 Traceroute ...................................................................................................... 145
- 4.12.3 Iperf ............................................................................................................... 146

## 4.13 Admin .................................................................................................................. 148
- 4.13.1 Users ............................................................................................................. 148
- 4.13.2 Authentication (RADIUS) .......................................................................... 150
- 4.13.3 NMS .............................................................................................................. 151
- 4.13.4 SNMP ........................................................................................................... 155
- 4.13.5 Discovery ....................................................................................................... 158
- 4.13.6 Logout ............................................................................................................ 159

## 5.0 AT Command Line Interface ................................................................................. 160

### 5.1 AT Command Overview ...................................................................................... 160
- 5.1.1 Serial Port ...................................................................................................... 160
- 5.1.2 Telnet .............................................................................................................. 161

### 5.2 AT Command Syntax ............................................................................................ 162

### 5.3 Supported AT Commands ..................................................................................... 163

## Appendices ................................................................................................................. 212
- Appendix A: Serial Interface ................................................................................... 212
- Appendix B: IP-Passthrough Example ..................................................................... 213
- Appendix C: Port Forwarding Example ..................................................................... 215
- Appendix D: VPN (Site to Site) Example ................................................................. 217
- Appendix E: Firewall Rules Example ...................................................................... 219
- Appendix F: Port Forwarding w/IP-Passthrough (Iperf) ......................................... 221
- Appendix G: Troubleshooting .................................................................................. 223

© Microhard Systems Inc.
1.0 Overview

The BulletPlus is a high-performance Cellular Dual Ethernet/Serial/USB Gateways w/WiFi, equipped with 3x RJ45 Ethernet Ports, dual SIM capability, 2x Programmable Analog I/O, Standalone GPS, 802.11b/g/n WiFi, and an RS232 serial communication port.

The BulletPlus utilizes the cellular infrastructure to provide network access to wired or wireless devices anywhere cellular coverage is supported by a cellular carrier. The BulletPlus supports 4G/LTE connections with blazing fast speeds.

Providing reliable Cellular Ethernet bridge functionality as well gateway service for most equipment types which employ an RS232, RJ45 or WiFi interface, the BulletPlus can be used in a limitless types of applications such as:

- High-speed backbone
- IP video surveillance
- Voice over IP (VoIP)
- Facilitating internetwork wireless communications
- Legacy network/device migration
- SCADA (PLC’s, Modbus, Hart)

1.1 Performance Features

Key performance features of the BulletPlus include:

- Fast, reliable connection speeds to 4G, 3G, LTE, and HSPA Networks (varies by model)
- 2x Programmable Analog/Digital Inputs OR up to 8 Digital Outputs
- DMZ and Port Forwarding
- 3x 10/100 Ethernet Ports (WAN/2LAN)
- Standalone GPS (TCP Server/UDP/SMTP Reporting)
- User interface via local console, telnet, web browser
- Compatibility with virtually all PLCs, RTUs, and other RS232 serial devices.
- Local & remote wireless firmware upgradable
- User configurable Firewall with IP/MAC ACL
- IP/Sec secure VPN and GRE Tunneling
- Industrial Temperature Rating (-40°C to +85°C)
1.0 Overview

1.2 Specifications

**BulletPlus**

**BulletPlus Supported Bands:**

(North America)
- LTE FDD (Bands 1, 3, 8, all bands with diversity)
- LTE TDD: Band 39, 40, 41(38), all bands with diversity
- DC-HSPA+/HSPA+/HSPA/UMTS: Band 1, 5, 8, 9, all bands with diversity
- TD-SCDMA: Band 34, 39, all bands with diversity
- GSM/GPRS/EDGE: 1800 MHz/900 MHz

**BulletPlus Supported Bands:**

(China)
- LTE FDD: Band 1, 3, 8, all bands with diversity
- LTE TDD: Band 39, 40, 41(38), all bands with diversity
- DC-HSPA+/HSPA+/HSPA/UMTS: Band 1, 5, 8, 9, all bands with diversity
- TD-SCDMA: Band 34, 39, all bands with diversity
- GSM/GPRS/EDGE: 1800 MHz/900 MHz

**BulletPlus Data Features:**

(North America)
- LTE: DL 100 Mbps, UL 50 Mbps
- HSPA+: DL 42 Mbps, UL 5.7 Mbps
- HSPA+: DL 21 Mbps, UL 5.7 Mbps
- WCDMA: DL/UL 384 kbps
- EDGE Class 33: DL/UL 236.8 kbps
- GPRS Class 33: DL/UL 85.6 kbps

**BulletPlus Data Features:**

(China)
- LTE FDD: UL 50Mbit/s, DL 150Mbit/s @20M BW cat4
- LTE TDD: UL 10Mbit/s; DL 112Mbit/s @20M BW cat4
- TD-SCDMA PS: UL 384 kbit/s; DL 384 kbit/s
- TD-HSPA+: UL 2.2 Mbit/s; DL 4.2 Mbit/s
- DC-HSPA+: UL 5.76 Mbit/s; DL 42 Mbit/s
- HSPA+: UL 5.76 Mbit/s; DL 21.6 Mbit/s
- WCDMA PS: UL 384 kbit/s; DL 384 kbit/s
- WCDMA CS: UL 64 kbit/s; DL 64 kbit/s
- EDGE: UL 236.8 kbit/s; DL 236.8 kbit/s
- GPRS: UL 85.6 kbit/s; DL 85.6 kbit/s

**General**

**Serial Interface:**
- RS232, RS485, RS422

**Serial Baud Rate:**
- 300bps to 921kbps

**USB:**
- USB 2.0
- USB Console Port
- USB to Serial Data Routing
- USB to Ethernet Data Routing (NDIS)

**Current Consumption:**
- (@12VDC)
- | Model            | AVG (mA) | w/WiFi (AP) |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BulletPlus</td>
<td>120</td>
<td>170</td>
</tr>
<tr>
<td>BulletPlus + Serial Data</td>
<td>142</td>
<td>180</td>
</tr>
<tr>
<td>BulletPlus + Ethernet</td>
<td>155</td>
<td>195</td>
</tr>
<tr>
<td>BulletPlus Peak</td>
<td>230</td>
<td>305</td>
</tr>
</tbody>
</table>
1.0 Overview

General Specifications (Continued)

Ethernet: 2 x LAN 10/100 BaseT, Auto - MDI/X, IEEE 802.3
1 x WAN 10/100 BaseT, Auto - MDI/X, IEEE 802.3

I/O: 2x Programmable Analog/Digital Inputs or up to 2x Digital Outputs
60mA current sink on open drain

SIM Card: Dual: 1.8 / 3.0V Standard/2FF size

PPP Characteristics: Dial on Demand/Idle Time

Network Protocols: TCP, UDP, TCP/IP, TFTP, ARP, ICMP, HTTP, HTTPS*, SSH*, SNMP,
FTP, DNS, Serial over IP, QoS

Management: Local Serial Console, Telnet, WebUI, SNMP, FTP &
Wireless Upgrade, RADIUS authentication, IPsec VLAN

Diagnostics: Temperature, RSSI, remote diagnostics

Input Voltage: 7-30 VDC

Power over Ethernet: Passive PoE on Ethernet Port (WAN)

GPS:
- Sensitivity: - Autonomous acquisition: -145 dBm
- Tracking Sensitivity: -158 dBm (50% valid fixes)
- Position Accuracy: - Tracking L1, CA code
- 12 Channels
- Max. update rate 1 Hz
- Error calculated location less than 11.6 meters 67% of the time, and
  less than 24.2 meters 95% of the time.

Environmental

Operation Temperature: -40°F(-40°C) to 185°F(85°C)

Humidity: 5% to 95% non-condensing

Mechanical

Dimensions: 2.21” (56mm) X 3.85” (97mm) X 1.46” (37mm)

Weight: Approx. 245 grams

Connectors: Antenna(s): CELL, DIV, GPS: SMA Female
ANT3: RP-SMA Female
Data, etc: Data: DE-9 Female (Front RS232)
Ethernet: 2x RJ-45

GPS Antenna Requirements:
- Frequency Range: 1575.42 MHz (GPS L1 Band)
- Bandwidth: +/- 2 MHz
- Total NF < 2.5dB
- Impedance 50ohm
- Amplification (Gain applied to RF connector): 19dB to 23dB
- Supply voltage 1.5V to 3.05V
- Current consumption - Typical 20mA (100mA max)
- Cellular Power Antenna Rejection + Isolation:
  - 824 - 915 MHz > 10dB
  - 1710 - 1785 MHz > 19dB
  - 1850 - 1980 MHz > 23dB
2.0 Quick Start

This QUICK START guide will walk you through the setup and process required to access the WebUI configuration window and to establish a basic wireless connection to your carrier.

Note that the units arrive from the factory with the Local Network setting configured as ‘Static’ (IP Address 192.168.168.1, Subnet Mask 255.255.255.0, and Gateway 192.168.168.1), in DHCP server mode. (This is for the LAN Ethernet Adapter on the back of the BulletPlus unit.)

2.1 Installing the SIM Card

Before the BulletPlus can be used on a cellular network a valid SIM Card for your Wireless Carrier must be installed. Insert the SIM Card into the slot as shown, the bottom SIM slot is for SIM1: (The contacts should face down, and the notch to the right)

SIM Card Slot (s)

To reset to factory defaults, press and hold the CFG button for 8 seconds with the BulletPlus powered up. The LED’s will flash quickly and the modem will reboot with factory defaults.

2.2 Getting Started with Cellular

Connect the Antenna’s to the applicable ANTENNA jack’s of the BulletPlus.

Use the MHS-supplied power adapter or an equivalent power source.

The unit can also be powered via PoE using a MHS PoE injector.

Connect the power connector to the power adapter and apply power to the unit, the CPU LED will flash during boot-up, once on solid, proceed to the next step.
2.0 Quick Start

- Connect A PC configured for DHCP directly to a LAN port of the BulletPlus, using an Ethernet Cable. If the PC is configured for DHCP it will automatically acquire a IP Address from the BulletPlus.

![Diagram of PC and BulletPlus connection]

- Open a Browser Window and enter the IP address **192.168.168.1** into the address bar.

![Screenshot of web browser with IP address]

- The BulletPlus will then ask for a Username and Password. Enter the factory defaults listed below.

![Authentication Required dialog box]

**The factory default network settings:**
- IP: 192.168.168.1
- Subnet: 255.255.255.0
- Gateway: 192.168.168.1

**The Factory default login:**
- User name: **admin**
- Password: **admin**

As of Firmware version v1.3.0-r1014 you will be required to change the default password when you login for the first time.

It is always a good idea to change the default admin login for future security.
2.0 Quick Start

✓ Once successfully logged in, the System Summary page will be displayed.

As seen above under Carrier Status, the SIM card is installed, but an APN has not been specified. Setting the APN to auto (default) may provide quick network connectivity, but may not work with some carriers, or with private APN’s. To set or change the APN, click on the Carrier > Settings tab and enter the APN supplied by your carrier in the APN field. Some carriers may also require a Username and Password.

Auto APN: The BulletPlus will attempt to detect the carrier based on the SIM card installed and cycle through a list of commonly used APN’s to provide quick network connectivity.

✓ Once the APN and any other required information is entered to connect to your carrier, click on “Submit”.

© Microhard Systems Inc.
2.0 Quick Start

✓ On the Carrier > Status Tab, verify that a WAN IP Address has been assigned by your carrier. It may take a few minutes, so try refreshing the page if the WAN IP Address doesn’t show up right away. The Activity Status should also show “Connected”.

✓ If you have set a static IP on your PC, you may need to add the DNS Servers shown in the Carrier Status Menu to your PC to enable internet access.

✓ Congratulations! Your BulletPlus is successfully connected to your Cellular Carrier.

✓ To access devices connected to BulletPlus remotely, one or more of the following must be configured: IP-Passthrough, Port Forwarding, DMZ. Another option would be to set up a VPN.

✓ Ensure that all default passwords are changed to limit access to the modem. (Firmware version v1.3.0-r1014 requires the defaults passwords are changed upon initial login).

✓ For best practices and to limit data charges it is critical to properly set up the firewall. (Especially important for Public Static IP addresses.)

Ensure the default passwords are changed.

Set up appropriate firewall rules to block unwanted incoming data.
3.0 Hardware Features

3.1 BulletPlus

The BulletPlus is a fully-enclosed unit ready to be interfaced to external devices with standard connectors as discussed below. An optional mounting bracket can be ordered to allow the BulletPlus to be mounted for a fixed installation.

The BulletPlus Hardware Features Include:

- Standard Connectors for:
  - 3x 10/100 Ethernet Ports (RJ45 - 1xWAN / 2xLAN)
  - Data Port (RS232/DB9)
  - 4-Pin: MATE-N-LOK Type Connector for Power / I/O 1/2
  - Cellular Antenna (SMA Female Antenna Connection x2)
  - GPS Antenna (SMA Female Antenna Connection)
  - WiFi Antenna (RP-SMA Female Antenna Connection)
  - Status/Diagnostic LED’s for RSSI(x3), Tx, Rx, GPS, CPU
  - Dual SIM (Mini-SIM (2FF)) Card Slots
  - CFG Button for factory default / firmware recovery operations
  - USB 2.0 Connector
3.0 Hardware Features

3.1.1 Mechanical Drawings

*Note: All dimension units: Millimeter*
3.0 Hardware Features

3.1.2 BulletPlus Mounting Bracket (Order Option)

Drawing 3-4: BulletPlus Top View Dimensions (Shown with removable TS35 DIN Rail Mount)

Drawing 3-5: BulletPlus Mounting Bracket Dimensions

Note: All dimension units: Millimeter
3.0 Hardware Features

3.1.3 Connectors and Indicators

3.1.3.1 Front & Top

On the front of the Bullet is the CFG Button, USB Port, Main, GPS & Diversity, GPS & WIFI Antenna Connectors and SIM Card Slot. The top of the Bullet are the status indicators, RSSI, Tx, RX, GPS and PWR.

The **USB** port is a future development to be available in later releases of firmware.

**CFG (Button)** - Holding this button while powering-up the Bullet will boot the unit into FLASH FILE SYSTEM RECOVERY mode. The default IP address for system recovery (only - not for normal access to the unit) is static: 192.168.1.39. Hold for 1 second for httpd recovery mode, 5 seconds for tftp recovery mode, or 10 seconds for master reset. If button is held for longer than 15 seconds the button will be ignored.

If the unit has been powered-up for some time (>1 minute), depressing the CFG Button for ~10 seconds (unit will reboot) will result in FACTORY DEFAULTS being restored, including the static factory IP address. This IP address is useable in a Web Browser for accessing the Web User Interface.

**Receive Signal Strength Indicator (RSSI)** - As the received signal strength increases, starting with the furthest left, the number of active RSSI LEDs increases.

**Tx(Red)/Rx(Green) LED's** - The Tx/Rx LED's indicate carrier (cellular) traffic.

**GPS** - Indicates that the optional standalone GPS module has synchronized and is ready for use.

**PWR LED** - The Power LED indicates that power has been applied to the module. Flashing indicates a bootup process.

**SIM Card** - This slot is used to install SIM card(s) provided by the cellular carrier. Ensure that the SIM card is installed properly by paying attention to the diagram printed next the SIM card slot. The Bottom slot is SIM1, the contact should face down, and the notch should be to the right.

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

<table>
<thead>
<tr>
<th>Signal (dBm)</th>
<th>RSSI1</th>
<th>RSSI2</th>
<th>RSSI3</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-85, 0]</td>
<td>ON</td>
<td>ON</td>
<td>ON</td>
</tr>
<tr>
<td>(-90, -85]</td>
<td>ON</td>
<td>ON</td>
<td>FLASH</td>
</tr>
<tr>
<td>(-95, -90]</td>
<td>ON</td>
<td>ON</td>
<td>OFF</td>
</tr>
<tr>
<td>(-100, -95]</td>
<td>ON</td>
<td>FLASH</td>
<td>OFF</td>
</tr>
<tr>
<td>(-105, -100]</td>
<td>ON</td>
<td>OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>(-109, -105]</td>
<td>FLASH</td>
<td>OFF</td>
<td>OFF</td>
</tr>
<tr>
<td>Other</td>
<td>SCANNING</td>
<td>SCANNING</td>
<td>SCANNING</td>
</tr>
</tbody>
</table>

Table 3-1: RSSI LED's
3.0 Hardware Features

3.1.3.2 Rear & Side View

On the side of the Bullet is the Data Port (RS232) and on the back are the Power and Ethernet(PoE) interfaces and the 2x Programmable I/O.

The Data Port (RS232 DCE) on the side of the unit is used for RS232 Serial Data based field devices at 300 bps to 921kbps.

The Ethernet Ports (2LAN/WAN) are 10/100 Mbps RJ-45 interfaces used to connect devices Ethernet based field devices.

Programmable I/O— The Bullet has 2 programmable Analog/Digital Inputs or 2 Digital Outputs. Maximum recommended load for the output pin is 150mA @ 30 Vdc (Vin).

Vin+/Vin− is used to power the unit. The input Voltage range is 7-30 Vdc.

PoE— The Bullet can also be powered using Passive PoE on the Ethernet Port (WAN), via a PoE injector.

Caution: Using a power supply that does not provide proper voltage may damage the modem.
4.0 Configuration

4.0 Web User Interface

Initial configuration of an BulletPlus using the Web User (Browser) Interface (Web UI) method involves the following steps:

- configure a static IP Address on your PC to match the default subnet or if your PC is configured for DHCP, simply connect a PC to a LAN port of the BulletPlus and it will be assigned a IP address automatically.

- connect the BulletPlus ETHERNET(LAN) port to PC NIC card using an Ethernet cable

- apply power to the BulletPlus and wait approximately 60 seconds for the system to load

- open a web browser and enter the factory default IP address (192.168.168.1) of the unit:

- logon window appears; log on using default Username: admin Password: admin

- use the web browser based user interface to configure the BulletPlus as required.

- refer to Section 2.0: Quick Start for step by step instructions.

In this section, all aspects of the Web Browser Interface, presented menus, and available configuration options will be discussed.
4.0 Configuration

4.0.1 Logon Window

Upon successfully accessing the BulletPlus using a Web Browser, the Logon window will appear.

The factory default User Name is: **admin**

The default password is: **admin**

Note that the password is case sensitive. It should be changed (discussed further along in this section), but once changed, if forgotten, may not be recovered.

When entered, the password appears as ‘dots’ as shown in the image below. This display format prohibits others from viewing the password.

The ‘Remember my password’ checkbox may be selected for purposes of convenience, however it is recommended to ensure it is deselected - particularly once the unit is deployed in the field - for one primary reason: security.

If the BulletPlus is restored to factory defaults the password is also restored to the original default password.

*As of firmware version v1.3.0-r1014 it is required to change the password upon initial login, once the password is changed, it will be required to login to the unit once again with the updated password.*
4.0 Configuration

4.1 System

The main category tabs located at the top of the navigation bar separate the configuration of the BulletPlus into different groups based on function. The System Tab contains the following sub menu’s:

- **Summary** - Status summary of entire radio including network settings, version information, and radio connection status
- **Settings** - Host Name, System Log Settings, System Time/Date
- **Services** - Enable/Disable and configure port numbers for SSH, Telnet, HTTP and HTTPS services
- **Keepalive** - Configure System keep alive to ensure network/internet access.
- **Maintenance** - Remote firmware Upgrades, reset to defaults, configuration backup and restore.
- **Reboot** - Schedule reboots and/or immediately reboot the system.

4.1.1 System > Summary

The System Summary screen is displayed immediately after initial login, showing a summary and status of all the functions of the BulletPlus in a single display. This information includes System Status, Carrier Status, Cellular & LAN/WAN network information, version info, etc.

<table>
<thead>
<tr>
<th>System Information</th>
<th>Description</th>
<th>System Info Window</th>
<th>Image 4-1-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>BulletPlus-GPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product Name</td>
<td>BulletPlus-GPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Version</td>
<td>v1.3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Build</td>
<td>1014</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temperature (°C)</td>
<td>47.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrier Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module Status</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current APN</td>
<td>westatbell.ca</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection Status</td>
<td>Connected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home/Roaming</td>
<td>Home</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Current Technology</td>
<td>WCDMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Mode</td>
<td>WCDMA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>184.151.220.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>70.28.245.227</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:0F:92:02:95:38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.168.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Network Interface Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:0F:92:03:95:38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Address</td>
<td>00:0F:92:03:95:38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WX</td>
<td>Status Point</td>
<td>TESTSSID</td>
<td></td>
</tr>
<tr>
<td>Frequency Band</td>
<td>2.4Ghz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radio Frequency</td>
<td>2.462 GHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Mode</td>
<td>WPA2 (PSK)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Receive Bytes</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmit Bytes</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The System Summary page will Auto Refresh, each time this happens a small amount of data is used. If viewing over the Cellular Network this data could add up to a significant amount over a long period of time.
4.0 Configuration

4.1.2 System > Settings

System Settings

Options available in the System Settings menu allow for the configuration of the Host Name, Description, Console Timeout and System Log server settings.

<table>
<thead>
<tr>
<th>System Settings</th>
<th>Values (characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>BulletPlus.MKT</td>
</tr>
<tr>
<td>Description</td>
<td>myBulletPlus.GPS</td>
</tr>
<tr>
<td>Console Timeout (s)</td>
<td>120 [30 ~ 65535] 0-Disable</td>
</tr>
<tr>
<td>CFG Reset to Default Button</td>
<td>Enable ✗ Disable</td>
</tr>
<tr>
<td>System Log Server IP/Name</td>
<td>0.0.0.0 0.0.0-Disable</td>
</tr>
<tr>
<td>System Log Server Port</td>
<td>514 [Default: 514]</td>
</tr>
</tbody>
</table>

Time Settings

<table>
<thead>
<tr>
<th>Time Settings</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Date/yyyy-mm-dd</td>
<td>2016-04-26</td>
</tr>
<tr>
<td>Current Time.hh:mm:ss</td>
<td>11:40:08</td>
</tr>
<tr>
<td>Date and Time Setting Mode</td>
<td>Local Time ✗ NTP</td>
</tr>
<tr>
<td>Timezone</td>
<td>Mountain Time ⬤</td>
</tr>
<tr>
<td>PDSX TZ String</td>
<td>MST/MDT/MST 2.0.11.0</td>
</tr>
<tr>
<td>NTP Server IP/Name</td>
<td>pool.ntp.org</td>
</tr>
<tr>
<td>NTP Server Port</td>
<td>123</td>
</tr>
<tr>
<td>NTP Client Interval (seconds)</td>
<td>0 [0 ~ 65535] 0-Disable</td>
</tr>
</tbody>
</table>

The Host Name is a convenient identifier for a specific BulletPlus unit. This feature is most used when accessing units remotely: a convenient cross-reference for the unit’s WAN/Carrier IP address. This name appears when logged into a telnet session, or when the unit is reporting into Microhard NMS System.

The description provides an additional field for text characters, but is not displayed anywhere but in this field.

<table>
<thead>
<tr>
<th>Host Name/Description</th>
<th>Values (characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BulletPlus (varies)</td>
</tr>
<tr>
<td></td>
<td>up to 30 characters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Console Timeout (s)</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>0-65535</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CFG Reset to Default Button</th>
<th>Values (Selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable</td>
</tr>
<tr>
<td></td>
<td>Disable</td>
</tr>
</tbody>
</table>
4.0 Configuration

System Syslog Server IP

The BulletPlus can report system level events to a third party Syslog server, which can be used to monitor events reported by the BulletPlus.

IP Address
0.0.0.0

System Syslog Server Port

Enter the UDP listening port of the Syslog Server. The default port number is generally 514, but could vary from Server to Server.

UDP Port
514

Time Settings

The BulletPlus can be set to use a local time source, thus keeping time on its own, or it can be configured to synchronize the date and time via a NTP Server. The options and menus available will change depending on the current setting of the Date and Time Setting Mode, as seen below.

Network Time Protocol (NTP) can be used to synchronize the time and date of computer systems with a centralized, referenced server. This can help ensure all systems on a network have the same time and date.

Date and Time Setting Mode

Select the Date and Time Setting Mode required. If set for ‘Use Local Time’ the unit will keep its own time and not attempt to synchronize with a network server. If ‘Synchronize Date And Time Over Network’ is selected, a NTP server can be defined.

Date

The calendar date may be entered in this field. Note that the entered value is lost should the BulletPlus lose power for some reason.

Values (yyyy-mm-dd)
2015.04.01 (varies)
4.0 Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>Values (hh:mm:ss)</td>
</tr>
<tr>
<td></td>
<td>11:27:28 (varies)</td>
</tr>
<tr>
<td><strong>Timezone</strong></td>
<td>Values (selection)</td>
</tr>
<tr>
<td></td>
<td>User Defined (or out of date)</td>
</tr>
<tr>
<td><strong>POSIX TZ String</strong></td>
<td>Values (read only)</td>
</tr>
<tr>
<td></td>
<td>(varies)</td>
</tr>
<tr>
<td><strong>NTP Server</strong></td>
<td>Values (address)</td>
</tr>
<tr>
<td></td>
<td>pool.ntp.org</td>
</tr>
<tr>
<td><strong>NTP Port</strong></td>
<td>Values (port#)</td>
</tr>
<tr>
<td></td>
<td>123</td>
</tr>
<tr>
<td><strong>NTP Client Interval</strong></td>
<td>Values (seconds)</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>
## 4.1.3 System > Services

Certain services in the BulletPlus can be disabled or enabled for either security considerations or resource/power considerations. The Enable/Disable options are applied after a reboot and will take affect after each start up. The Start/Restart/Stop functions only apply to the current session and will not be retained after a power cycle.

![Image 4-1-5: System > Services](image)

<table>
<thead>
<tr>
<th>Service</th>
<th>Enable/Disable</th>
<th>Port</th>
<th>Values (port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>Enable/Disable</td>
<td>Port 22</td>
<td>Update</td>
</tr>
<tr>
<td>Telnet</td>
<td>Enable/Disable</td>
<td>Port 23</td>
<td>Update</td>
</tr>
<tr>
<td>SSH</td>
<td>Enable/Disable</td>
<td>Port 22</td>
<td>Update</td>
</tr>
<tr>
<td>Web UI</td>
<td>HTTP/HTTPS</td>
<td>Port 80</td>
<td>Update</td>
</tr>
<tr>
<td>Microhard Sh</td>
<td>Enable/Disable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### FTP

The FTP service can be enabled/disabled using the Services Status Menu. The FTP service is used for firmware recovery operations.

Enable / Disable

### Telnet

Using the Telnet Service Enable/Disable function, you can disable the Telnet service from running on the modem. The port used by the Telnet service can also be modified. The default is 23.

**Values (port)**

| Port | 23 |

### SSH

Using the SSH Service Enable/Disable function, you can disable the SSH service (Port 22) from running on the modem. The port used by the SSH service can also be modified. The default is 22.

**Values (port)**

| Port | 22 |

### Web UI

The default web server port for the web based configuration tools used in the modem is port 80 (http) and port 443 (HTTPS).

Change as required, but keep in mind that if a non standard port is used, it must be specified in a internet browser to access the unit. (example: http://192.168.168.1:8080).

**Values (selection)**

<table>
<thead>
<tr>
<th>HTTP/HTTPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
</tr>
<tr>
<td>HTTPS</td>
</tr>
</tbody>
</table>

### Microhard Sh

Reserved for internal use.
4.0 Configuration

4.1.4 System > Keepalive

The Keep alive tab allows for the configuration of the keep alive features of the BulletPlus. The BulletPlus can check for activity on the Wireless Interface, The CLI (Command Line Interface), The WEBUI, and ensure that they are working as expected. In the event that the BulletPlus does not detect activity on a interface it will reboot to attempt to resolve any issues that may have occurred.

Enable or Disable the keep alive functions of the modem. If it is disabled, the user can configure the Traffic Check separately. The unit will monitor traffic on the Cell interface.

Monitors traffic on the Cell interface as well as the WAN interface if the WAN port is configured as independent in the Network Settings. If the Bullet detects that there is no activity on the above interfaces it will attempt a ICMP, HTTP or DNS Lookup as configured below to determine if service has been lost.

Monitors the activity of CLI. If the console isn't accessed within the certain period which is specified by Console Timeout in System-Settings web page, the modem will send out the connection request.

Monitors the activity of Web UI. If the Web UI isn't accessed or refreshed within the certain period which is specified by Console Timeout in System-Settings web page, the modem will send out the connection request.

Image 4-1-6: Carrier > Keepalive
4.0 Configuration

<table>
<thead>
<tr>
<th>Type</th>
<th>Values (Selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ICMP</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td>DNS Lookup</td>
</tr>
</tbody>
</table>

Keepalive Interval

<table>
<thead>
<tr>
<th>Host Name</th>
<th>Values (IP or Domain)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8.8.8.8</td>
</tr>
</tbody>
</table>

Keepalive Retry

<table>
<thead>
<tr>
<th>Type</th>
<th>Values (Selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ICMP</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td>DNS Lookup</td>
</tr>
</tbody>
</table>

Once the connection is lost, the modem will send one of the requests to the remote host to determine the connection status. If the modem fails to get the response, it will re-send the request within the seconds specified by Keepalive Interval below:

- **ICMP**: Send a "ping" request
- **HTTP**: Send a "wget" request to a HTTP server
- **DNS Lookup**: Send a "dslookup" request to a DNS server

The Interval value determines the frequency, or how often, the unit will send out PING messages to the Host. The BulletPlus will first attempt to re-initialize the cellular model before performing a full system reboot, thus the interval may be delayed by up to 120 seconds:

Keepalive Retry

The Keepalive Retry is the maximum number of connection failures such as "Host unreachable" the unit will attempt before the unit will reboot itself to attempt to correct connection issues. The default number is 20, and valid value is from 10 to 200.

Specify a IP Address or Domain that is used to test the modem's connection. The modem will send out the connection requests to the specified Host.
4.0 Configuration

4.1.5 System > Maintenance

Firmware Upgrade

Occasional firmware updates may be released by Microhard Systems which may include fixes and/or new features. The firmware can be updated wirelessly using the WebUI.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
<th>Reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Summary</td>
<td>Settings</td>
<td>Services</td>
<td>Keepalive</td>
<td>Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Version Information**

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Hardware Type</th>
<th>Build Version</th>
<th>Build Date</th>
<th>Build Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>BulletPlus-GPS</td>
<td>1.0</td>
<td>v1.3.0 build 1014</td>
<td>2016-03-09</td>
<td>10:49:31</td>
</tr>
</tbody>
</table>

**Firmware Upgrade**

- **Erase Current Configuration**
  - Keep All Configurations
  - Upgrade Firmware

- **Firmware Image**
  - Choose file: No file chosen

- **Upgrade**

**Backup Configurations**

- **Configuration File Name**: MicrohardBulletPlus-GPS.c
- **Backup**: Backup Configurations

**Restore Configurations**

- **Select Configuration File**: Choose file: No file chosen
- **Check Configuration File**: Check Configuration File

*Image 4-1-7: Maintenance > Firmware Upgrade*

**Erase Current Configuration**

Check this box to erase the configuration of the BulletPlus unit during the upgrade process. This will upgrade, and return the unit to factory defaults, including the default IP Addresses and passwords. Not checking the box will retain all settings during a firmware upgrade procedure.

Values (check box)

unchecked

**Firmware Image**

Use the Browse button to find the firmware file supplied by Microhard Systems. Select “Upgrade Firmware” to start the upgrade process. This can take several minutes.

Values (file)

(no default)

**Reset to Default**

The BulletPlus may be set back to factory defaults by using the Reset to Default option under System > Maintenance > Reset to Default. *Caution* - All settings will be lost!!!
4.0 Configuration

Backup & Restore Configuration

The configuration of the BulletPlus can be backed up to a file at any time using the Backup Configuration feature. The file can then be restored using the Restore Configuration feature. It is always a good idea to backup any configurations in case of unit replacement. The configuration files cannot be edited offline, they are used strictly to backup and restore units.

Use this field to name the configuration file. The .config extension will automatically be added to the configuration file.

Use the ‘Browse’ button to find the backup file that needs to be restored to the unit. Use the ‘Check Restore File’ button to verify that the file is valid, and then the option to restore the configuration is displayed, as seen above.

The Keep Carrier Settings box can be selected before the restore process is started, if it is selected the BulletPlus will retain the current carrier settings and not overwrite them with the settings contained in the backup file.
4.0 Configuration

4.1.6 System > Reboot

The BulletPlus can be remotely rebooted using the System > Reboot menu. As seen below a button ‘Reboot now’ is provided. Once pressed, the unit immediately reboots and starts its boot up procedure. The BulletPlus can also be restarted on a regular basis by setting up a daily/weekly/monthly schedules.

![Image 4-1-9: System > Reboot](Image 4-1-9: System > Reboot)

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Settings</td>
<td>Services</td>
<td>Keepalive</td>
<td>Maintenance</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
<td>Reboot</td>
</tr>
</tbody>
</table>

**Config Scheduled Reboot**

**Schedule No. 1**

<table>
<thead>
<tr>
<th>Status</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Reboot Daily</td>
</tr>
<tr>
<td>Time</td>
<td>01:00</td>
</tr>
</tbody>
</table>

**Schedule No. 2**

<table>
<thead>
<tr>
<th>Status</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Reboot Weekly</td>
</tr>
<tr>
<td>Days</td>
<td>1, 2, 3</td>
</tr>
<tr>
<td>Time</td>
<td>01:00</td>
</tr>
</tbody>
</table>

**Schedule No. 5**

<table>
<thead>
<tr>
<th>Status</th>
<th>Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Reboot Monthly</td>
</tr>
<tr>
<td>Days</td>
<td>1, 2, 3</td>
</tr>
<tr>
<td>Time</td>
<td>01:00</td>
</tr>
</tbody>
</table>

**Values (selection)**

**Status**

- Disable / Enable

**Type**

- Reboot Daily
- Reboot Weekly
- Reboot Monthly

**Days / Time**

- 1, 2, 3...

Use this option to enable or disabled schooled reboots. If enabled the BulletPlus is reboot at the interval defined below.

Schedule daily, weekly or monthly reboots. Setting up a reboot schedule can help keep the modem connected to the cellular carrier and prevent physically rebooting the modem if located at a remote destination.

If set for weekly, days are counted from Sunday to Saturday (0 to 6), and if set to monthly the days are counted 1 to 31. Multiple days can be specified by separating with a comma ','. Set the time of day (24hr clock) for which to reboot the device.
4.0 Configuration

4.2 Network

4.2.1 Network > Summary

The Network Summary display gives an overview of the currently configured network interfaces including the Connection Type (Static/DHCP), IP Address, Net Mask, Default Gateway, DNS, and IPv4 Routing Table.

Image 4-2-1: Network > Network Status
4.0 Configuration

4.2.2 Network > LAN

LAN Port Configuration

The BulletPlus features 2x LAN ports that can be used for connection of devices on a local network. The WAN port can also be bridged with the LAN therefore providing up to 3 LAN ports. By default the has a static IP Address assigned, 192.168.168.1. Also, by default the LAN is running a DHCP server to provide IP Addresses to devices that are connected to the physical LAN port (s) (directly or via a switch).

DHCP: Dynamic Host Configuration Protocol may be used by networked devices (Clients) to obtain unique network addresses from a DHCP server.

Advantage:
Ensures unique IP addresses are assigned, from a central point (DHCP server) within a network.

Disadvantage:
The address of a particular device is not 'known' and is also subject to change.

STATIC addresses must be tracked (to avoid duplicate use), yet they may be permanently assigned to a device.

LAN Add/Edit Interface

The BulletPlus has the capability to have multiple SSID’s for the WiFi radio. New Interfaces can be added for additional SSID’s, providing, if required, separate subnets for each SSID. By default any additional interfaces added will automatically assign IP addresses to connecting devices via DHCP. Additional interfaces can only be used by additional WIFI SSID’s (virtual interfaces).

Spanning Tree (STP)

This option allows the BulletPlus to participate in the Spanning Tree protocol with other devices to prevent local loops. By default this is disabled.
4.0 Configuration

This selection determines if the BulletPlus will obtain an IP address from a DHCP server on the attached network, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

**Connection Type**

- Values (selection)
  - DHCP
  - Static

**IP Address**

- Values (IP Address)
  - 192.168.168.1

If ‘Static’ Connection Type is selected, a valid IPv4 Address for the network being used must be entered in the field. If ‘DHCP’ is chosen this field will not appear and it will be populated automatically from the DHCP server.

**Netmask**

- Values (IP Address)
  - 255.255.255.0

If ‘Static’ Connection Type is selected, the Network Mask must be entered for the Network. If ‘DHCP’ is chosen this field will not appear and it will be populated automatically from the DHCP server.

**DNS Mode**

- Values (selection)
  - Auto
  - Manual

If the Connection Type is set to DHCP, you can use Auto for the DNS Mode and a DNS server will automatically be defined. If the connection type is set as static, DNS servers can be manually specified.

**Primary DNS / Secondary DNS**

- Values (selection)
  - Auto
  - Manual

Within any IP network, each device must have its own unique IP address.
LAN DHCP

A BulletPlus may be configured to provide dynamic host control protocol (DHCP) service to all attached (either wired or wireless (WiFi)-connected) devices. By default the DHCP service is enabled, so devices that are connected to the physical Ethernet LAN ports, as well as any devices that are connected by WiFi will be assigned an IP by the BulletPlus. The LAN DHCP service is available for each interface, and is located in the add/edit interface menus.

Prior to enabling this service, verify that there are no other devices - either wired (e.g. LAN) or wireless with an active DHCP SERVER service. (The Server issues IP address information at the request of a DHCP Client, which receives the information.)

<table>
<thead>
<tr>
<th>DHCP Server</th>
<th>Enable / Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>192.168.168.100</td>
</tr>
<tr>
<td>Limit</td>
<td>150</td>
</tr>
<tr>
<td>Lease Time (in minutes)</td>
<td>720</td>
</tr>
<tr>
<td>Alternate Gateway</td>
<td></td>
</tr>
<tr>
<td>Preferred DNS server</td>
<td></td>
</tr>
<tr>
<td>Alternate DNS server</td>
<td></td>
</tr>
<tr>
<td>WINS/NBNS Servers</td>
<td></td>
</tr>
<tr>
<td>WINS/NBT Node Type</td>
<td>none</td>
</tr>
</tbody>
</table>

**DHCP Server**

The option is used to enable or disable the DHCP service for devices connected to the LAN Port(s).

**Start**

Select the starting address DHCP assignable IP Addresses. The first octets of the subnet will be pre-set based on the LAN IP configuration, and can not be changed.

```
Start Values (IP Address)
192.168.168.100
```

**Limit**

Set the maximum number of IP addresses that can be assigned by the BulletPlus.

```
Limit Values (integer)
150
```

**Lease Time**

The DHCP lease time is the amount of time before a new request for a network address must be made to the DHCP Server.

```
Lease Time Values (minutes)
720
```

**Alternate Gateway**

Specify an alternate gateway for DHCP assigned devices if the default gateway is not to be used.

```
Alternate Gateway Values (IP Address)
```
4.0 Configuration

DNS: Domain Name Service is an Internet service that translates easily-remembered domain names into their not-so-easily-remembered IP addresses.

Being that the Internet is based on IP addresses, without DNS, if one entered the domain name www.microhardcorp.com (for example) into the URL line of a web browser, the website ‘could not be found’.

Specify a preferred DNS server address to be assigned to DHCP devices.

**Preferred DNS Server**

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(IP Address)</td>
</tr>
</tbody>
</table>

Specify the alternate DNS server address to be assigned to DHCP devices.

**Alternate DNS Server**

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(IP Address)</td>
</tr>
</tbody>
</table>

Enter the address of the WINS/NBNS (NetBIOS) Server. The WINS server will translate computers names into their IP addresses, similar to how a DNS server translates domain names to IP addresses.

**WINS/NBNS Servers**

<table>
<thead>
<tr>
<th>Values (IP/Domain)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>

Select the method used to resolve computer names to IP addresses. Four name resolution methods are available:

- B-node: broadcast
- P-node: point-to-point
- M-node: mixed/modified
- H-node: hybrid

**WINS/NBT Node Type**

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
</tr>
<tr>
<td>b-node</td>
</tr>
<tr>
<td>p-node</td>
</tr>
<tr>
<td>m-node</td>
</tr>
<tr>
<td>h-node</td>
</tr>
</tbody>
</table>
## VLAN Configuration

The BulletPlus has the capability to add multiple network interfaces, as such it may be desirable to segment these different subnets. The BulletPlus features 802.1Q VLAN. 802.1Q VLAN uses tagging to allow separation of network segments. Ports can belong to multiple VLANs. A Trunk port can be configured to communicate with other VLAN switch by adding all configured VLANs to a single port. The native VLAN1 is used by default, it is important that any connected VLAN switch use the same Native VLAN.

![Image of VLAN Configuration](Image 4-2-5: Network > VLAN)

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
<td></td>
</tr>
</tbody>
</table>

### VLAN ID

When adding a VLAN you must select a VLAN ID. Select between 2 and 127 for valid VLAN IDs.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 (2-127)</td>
<td></td>
</tr>
</tbody>
</table>

### Port 1 - 2

Assign port to the current VLAN.

**Excluded**: Not part of the current VLAN

**Tagged**: In 802.1Q this assigns the current VLAN to the port,

**Untagged**: In port based VLAN this assigns a port to the current VLAN.

### Network

Allows the user the ability to assign specific configured network interfaces to a specific VLAN. (802.1Q)

<table>
<thead>
<tr>
<th>Network</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>(additional network interfaces)</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.2.3 Network > WAN

WAN Configuration

The WAN configuration refers to the wired WAN connection on the BulletPlus. The WAN port can be used to connect the BulletPlus to other networks, the internet and/or other network resources.

This selection determines if the BulletPlus will obtain a WAN IP address from a DHCP server, or if a static IP address will be entered. If 'Static' Connection Type is selected, a valid IPv4 Address for the network being used must be entered in the field. If 'DHCP' is chosen this field will not appear and it will be populated automatically from the DHCP server.

DHCP: Dynamic Host Configuration Protocol may be used by networked devices (Clients) to obtain unique network addresses from a DHCP server.

Advantage:
Ensures unique IP addresses are assigned, from a central point (DHCP server) within a network.

Disadvantage:
The address of a particular device is not known and is also subject to change.

STATIC addresses must be tracked (to avoid duplicate use), yet they may be permanently assigned to a device.
4.0 Configuration

**Default Gateway**
If the BulletPlus is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway’s IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>

**Default Route**
The Default Route parameter allows you to set this interface as the default route in the routing table. This is result in all data being sent to the WAN interface if there the destination network is not directly connected (LAN, WIFI etc), and no other route has been specified (4G). In cases where the WAN is the primary connection this would be set to Yes.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No / Yes</td>
</tr>
</tbody>
</table>

**DNS Mode**
Select between Manual or Auto for DNS server(s) for the WAN interface. If set to Auto the BulletPlus will try to automatically detect the DNS servers to use, which is normally the case when the WAN is DHCP. Manual required the DNS addresses to be known and entered below.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual / Auto</td>
</tr>
</tbody>
</table>

**Primary DNS**
DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If set to auto and the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page. To add additional static servers, enter them here.

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>

**Secondary DNS**
DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If set to auto and the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page. To add additional static servers, enter them here.

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.2.4 DHCP (MAC Binding)

In some applications it is important that specific devices always have a predetermined IP address. This menu allows for MAC Address binding to a IP Address, so that whenever the device that has the specified MAC address, will always get the selected IP address from the DHCP service. In this situation, all attached (wired or wireless) devices can all be configured for DHCP, but still get a known IP address.

Enter in the MAC address of the device to be bound to a set IP address. Set the IP Address in the next field. Must use the format: AB:CD:DF:12:34:D3. It is not case sensitive, but the colons must be present.

Enter the IP Address to be assign to the device specified by the MAC address above.

**Static Addresses**

This section displays the IP address and MAC address currently assigned through the DHCP service, that are bound by it’s MAC address. Also shown is the Name, and the ability to remove the binding by clicking “Remove _______”.

**Active DHCP Leases**

This section displays the IP Addresses currently assigned through the DCHP service. Also shown is the MAC Address, Name and Expiry time of the lease for reference. The ‘Release All’ button terminates all active leased and requires all connected devices to request new network information (IP/Subnet/etc)

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>LAN</td>
<td>WAN</td>
<td>DHCP</td>
<td>DDNS</td>
<td>Routes</td>
<td>VRRP</td>
<td>Ports</td>
<td>Bandwidth</td>
<td>Device List</td>
<td>Cloud Filter</td>
<td>Webfilter</td>
<td>MultiWAN</td>
</tr>
</tbody>
</table>

**DHCP Configuration**

**Static IP addresses (for DHCP Server)**

Name
MAC Address
IP Address
Add static

**Static Addresses**

MAC Address
IP Address
Name
NetStatus

**Active DHCP Leases**

MAC Address
IP Address
Name
Expires in

Image 4-2-7: Network > MAC Address Binding
4.0 Configuration

4.2.5 Network > DDNS

Unless a carrier issues a Static IP address, it may be desirable to use a Dynamic DNS (DDNS) service to track dynamic IP changes and automatically update DNS services. This allows the use of a constant resolvable host name for the BulletPlus.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>LAN</td>
<td>WAN</td>
<td>DHCP</td>
<td>DDNS</td>
<td>Routes</td>
<td>VRRP</td>
<td>Ports</td>
<td>Bandwidth</td>
<td>Device List</td>
<td>Cloud Filter</td>
<td>Webfilter</td>
<td>MultiWAN</td>
</tr>
</tbody>
</table>

**DDNS Configuration**

**DDNS Status**

This selection allows the use of a Dynamic Domain Name Server (DDNS), for the BulletPlus.

**Values (Selection)**

- Enable / Disable

**Network**

If the BulletPlus is using a wired WAN (ISP) as well as a Cellular carrier, specify which will use the DNS service.

**Values (Selection)**

- Auto / Carrier / WAN

**Service**

This is a list of supported Dynamic DNS service providers. Free and premium services are offered, contact the specific providers for more information.

<table>
<thead>
<tr>
<th>Service Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>changeip</td>
</tr>
<tr>
<td>dyndns</td>
</tr>
<tr>
<td>eurodyndns</td>
</tr>
<tr>
<td>hn</td>
</tr>
<tr>
<td>noip</td>
</tr>
</tbody>
</table>

**User Name / Password**

Enter a valid user name and password for the DDNS service selected above.

**Values (characters)**

- (none)

**Host**

This is the host or domain name for the BulletPlus as assigned by the DDNS provider. Use the provided button to query the server (if configured correctly).

**Values (domain name)**

- (none)
4.0 Configuration

4.2.6 Network > Routes

Static Routes Configuration

It may be desirable to have devices on different subnets to be able to talk to one another. This can be accomplished by specifying a static route, telling the BulletPlus where to send data.

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Values (characters)</th>
<th>(no default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Values (IP Address)</td>
<td>(192.168.168.0)</td>
</tr>
<tr>
<td>Gateway</td>
<td>Values (IP Address)</td>
<td>192.168.168.1</td>
</tr>
<tr>
<td>Netmask</td>
<td>Values (IP Address)</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
```

![Image 4-2-9: Network > Routes](image-url)
# 4.0 Configuration

## Metric

| Values (Integer) | 
|-----------------|---|
| 255.255.255.0   | 

In some cases there may be multiple routes to reach a destination. The Metric can be set to give certain routes priority, the lower the metric is, the better the route. The more hops it takes to get to a destination, the higher the metric.

## Interface

| Values (Selection) | 
|-------------------|---|
| LAN / LAN1 / WAN / Cell / USB | None |
4.0 Configuration

4.2.7 Network > VRRP

The BulletPlus when paired with other VRRP enabled devices (another BulletPlus or compatible devices) can provide redundant internet access for LAN devices by using VRRP (Virtual Router Redundancy Protocol) as illustrated below. If a connected device needs to access the internet it will use whichever virtual router has the highest priority, if that device is not available the next router with the higher priority will router the traffic.

Enable or disable the VRRP service on the BulletPlus. To change settings the VRRP service must be disabled (then submitted) and then re-enabled.

---

**Image 4-2-10: Network > VRRP**

**VRRP Status**

Enable or disable the VRRP service on the BulletPlus. To change settings the VRRP service must be disabled (then submitted) and then re-enabled.
4.0 Configuration

4.2.8 Network > Ports

The Network > Ports menu can be used to determine the characteristics of the physical Ethernet interfaces on the BulletPlus. As seen below the Mode (Auto/Manual), Auto-Negotiation, Speed (10/100Mbit/s) and the Duplex (Full/Half) can all be configured on the BulletPlus.

<table>
<thead>
<tr>
<th>Virtual Router IP</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.220.211</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Router ID</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Router Priority</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>150</td>
</tr>
</tbody>
</table>

4.2.8 Network > Ports

This is the IP Address of the virtual router, this must be the same on all devices participating in VRRP. This is the IP that any attached LAN PC/device would use as its default gateway.

This is the Router ID. Each router/ participating in VRRP should have a router ID to distinguish between them.

This is the Router priority. This number to assigned to each router to determine which router(s) will be used first or as the primary. The higher the ID, the higher the priority.

Image 4-2-11: Network > Ports
4.2.9 Network > Bandwidth

The BulletPlus features Bandwidth Throttling, which allows the upload/download of connected networks/users data speeds to be limited to a specified value. Network Bandwidth Throttling can be implemented by each physical Ethernet interface as seen in the image below.

The rule name is used as a reference to be able to help identify which interface or network is attached to the affected network interface.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>rule1</td>
</tr>
</tbody>
</table>

Network

Select the physical interface to be affected by the Bandwidth Throttling as defined below.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(varies)</td>
</tr>
</tbody>
</table>

Upload Bandwidth Enable

Enable or disable uploading on the specified interface. This prevent data from being uploaded to a server. (i.e uploading/sending videos or other files to a server).

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable / Disable</td>
</tr>
</tbody>
</table>

Upload Bandwidth

Set the data limit (speed) for file uploads if uploads have been allowed using the Upload Bandwidth Enable.

<table>
<thead>
<tr>
<th>Values (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10000</td>
</tr>
</tbody>
</table>
4.0 Configuration

**Download Bandwidth Enable**

Enable or disable downloading on the specified interface. This prevents data from being downloaded from a server. (i.e., downloading files, internet browsing, etc).

**Values (chars)**

<table>
<thead>
<tr>
<th>Enable</th>
<th>Disable</th>
</tr>
</thead>
</table>

**Download Bandwidth**

Set the data limit (speed) for file downloads if downloads have been allowed using the Download Bandwidth Enable.

**Values (kbps)**

| 30000 |

4.2.10 Network > Device List

The Network > Device List shows the current ARP table for the network adapters. The MAC address and IP address are shown, however not only DHCP assigned devices are listed in the device list, any devices, even those statically assigned, that are connected through the local network interface (RJ45) are displayed, including those connected through a hub or switch.

![Image 4-2-13: Network > Device List](image)
4.2.11 Network > Cloud Filter

The BulletPlus provides Cloud based content filtering and security using the third-party service by OpenDNS. OpenDNS is a service which offers free or premium DNS services with added security, phishing protection and optional, advanced content filtering. To get started with OpenDNS an account must first be created with OpenDNS by visiting their website.

Enable or Disable the OpenDNS cloud based filtering & security.

**OpenDNS Cloud Filter**

Enable / Disable

**Disable Bypassing OpenDNS**

If enabled all clients connected through the BulletPlus will be forced to use OpenDNS and is subject to any and all content filtering and security, to prevent circumvention.

**Status**

When Cloud Filter is enabled, this status will be refreshed every 30 seconds, showing the OpenDNS status. For OpenDNS to be active, the status must be green and show "Connected to OpenDNS".

**User Name / Password**

Enter the user name and password for the OpenDNS account that was specified during registration and setup of the service.

Enable / Disable
4.0 Configuration

4.2.12 Network > Webfilter

The BulletPlus can provide comprehensive content filtering, limiting access to specific websites and other content. By MAC Address, the BulletPlus allows content to be filtering regardless of the assigned IP address. Filtering can also be applied on a entire network, limiting access to any connected device.

Enable or Disable the Webfilter of the BulletPlus.

Webfilter Status
Values (selection)
Enable / Disable

Check Filter HTTPS will redirect all port 443 traffic into the webfilter. (Please make sure system DNS works.)

Filter HTTPS
Values (selection)
Enable / Disable
### 4.0 Configuration

#### MAC Address Webfilter Default Setting

Default setting can be used for MAC addresses where all addresses may be allowed (Allow) with a few exceptions, or where all addresses are block (Deny), with a few exceptions.

After a Default rule has been applied, exceptions can be added by adding MAC Webfilter Rules.

#### MAC Webfilter Rules

Add MAC Webfilter rules to apply filtering. If a default rule has been added these rules can be used to specify exceptions. MAC Webfilter Rules can also be applied to limit access to just one or a few websites by simply adding the to the MAC Webfilter list without using a default rule.

- **Name**: Add a name for the MAC Webfilter Rule.
- **MAC Address**: Enter the MAC Address to apply rule to.
- **Domain/URL/IP**: Enter the Domain Name or URL of the website control access for, i.e. www.company.com. To ensure the full domain is blocked, enter the most inclusive domain, i.e. .company.com will block www.company.com and images.company.com and videos.company.com. Alternatively you can use an IP address or address range written in CIDR notation, i.e. 8.8.8.0/24.
- **Action**: Specify if the rule Allows access or Denies access to the specified address.
- **Rule Priority**: The Rule Priority is used to determine the order rules are evaluated. Higher priority rules (bigger number) are evaluated first and the first one to match has its assigned action taken.
- **Enabled**: Enable or Disable the MAC Webfilter rule.

#### MAC Address Webfilter Default Setting

When a network is set to Allow (Blacklist) it will allow access to all sites not blocked in the Filter Rules. Selecting Deny (Whitelist) will only allow access to websites with an Allow action in the Filter rules, all other sites will be blocked.

#### MAC Webfilter Rules

Add Network Webfilter Rules to allow or deny access to specified content. The Network rules work with the Network Webfilter Default Settings.

- **Name**: Add a name for the MAC Webfilter Rule.
- **Network**: Select the local network for which the rule applies.
- **Domain/URL/IP**: See description in MAC Filtering Rules above.
- **Action**: See description in MAC Filtering Rules above.
- **Enabled**: Enable or Disable the Network Webfilter rule.
4.2.13 Network > MultiWAN

MultiWAN is used to manage the primary data connection used by the BulletPlus. In cases where a wired WAN (ISP) is available it is generally used for the primary connection as data is usually cheaper (unlimited) than a cellular connection. The BulletPlus can provide automatic failover services, switching the connection (or default route) used for outside data.

Enable or disable the MultiWAN service on the BulletPlus. To use MultiWAN, the WAN (wired) must be configured as independent in the Network > WAN settings and/or the Wireless must be set to Client & bound to the WIFI interface.
4.0 Configuration

**Primary WAN**

Define which connection is the primary network/internet connection for the BulletPlus. Normally this is the wired WAN connection to an ISP.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN / Carrier / WIFI Client</td>
</tr>
</tbody>
</table>

**Second WAN**

Select which WAN connection is the secondary connection. When a failure of the main WAN occurs this will be the first alternative. Generally this will be the cellular connection.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN / 4G / WIFI</td>
</tr>
</tbody>
</table>

**Third WAN**

The WiFi on the BulletPlus can be configured as a client and used as a data connection to access the internet.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN / 4G / WIFI / Disable</td>
</tr>
</tbody>
</table>

**Health Monitor Interval**

This is the frequency at which the BulletPlus will send ICMP packets to the defined host to determine if the interface has failed.

<table>
<thead>
<tr>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
</tr>
</tbody>
</table>

**Switch Notification**

It is possible for the BulletPlus to send out a notification when the MultiWAN has switched its available connection and is routing data through an alternate interface.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable / Email / SMS / Both</td>
</tr>
</tbody>
</table>

**Failover Settings (Same settings for WAN, WIFI Client and Carrier)**

**Type**

Select the type of failover detection to be used. By default ICMP is used to ping a specified address(s), a DNS Lookup can also be selected.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP / DNS Lookup</td>
</tr>
</tbody>
</table>

**Host Name**

Up to three(3) reachable addresses can be specified to test for link health at the frequency specified above for the Health Monitor Interval. A test button is provided to ensure that reachable address have been entered and that there are no errors.

<table>
<thead>
<tr>
<th>Values (Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8.8.8</td>
</tr>
<tr>
<td>4.2.2.1</td>
</tr>
<tr>
<td>208.67.222.222</td>
</tr>
</tbody>
</table>

**Advanced+ (Only shown if selected)**
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping Mode</td>
<td>3</td>
</tr>
<tr>
<td>ICMP Timeout</td>
<td>3</td>
</tr>
<tr>
<td>Attempts Before Failover</td>
<td>1, 3, 5, 10, 15, 20</td>
</tr>
<tr>
<td>Attempts Before Recovery</td>
<td>1, 2, 5, 10, 15, 20</td>
</tr>
<tr>
<td>Recovery Immediate Mode / Wait</td>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

- **Ping Mode**: The Ping mode allows for the selected hosts to be pinged either Sequentially or Simultaneously. This option is only displayed when the failover mode is set to ICMP.

- **ICMP Timeout**: This is the amount of time the Health Monitor will wait for a response from the ICMP Host (when type is configured as ICMP).

- **Attempts Before Failover**: This is the number of attempts the BulletPlus will attempt to reach the IMCP host before going into failover and switching WAN interfaces.

- **Attempts Before Recovery**: The BulletPlus will continue to monitor the failed interface, even after failover has occurred. This defines the number of successful attempts required before recovering the failed interface.

- **Recovery Immediate Mode / Wait**: Once the preferred connection is again deemed available, it can be specified to wait a configurable amount of time before restoring the connection.
4.0 Configuration

4.3 Carrier

4.3.1 Carrier > Status

The Carrier Status window provides complete overview information related to the Cellular Carrier portion of the BulletPlus. A variety of information can be found here, such as Activity Status, Network (Name of Wireless Carrier connected), Data Service Type (WCDMA/HSPA/HSPA+/LTE etc), Frequency band, Phone Number etc.

Not all statistics parameters displayed are applicable.

The Received and Transmitted bytes and packets indicate the respective amount of data which has been moved through the radio.

The Error counts reflect those having occurred on the wireless link.
4.0 Configuration

4.3.2 Carrier > Settings

The parameters within the Carrier Configuration menu must be input properly; they are the most basic requirement required by your cellular provider for network connectivity. The BulletPlus can support dual SIM cards, as described below either slot can be specified as the primary slot and if a connectivity issue occurs, the unit can be configured to automatically switch to the alternate SIM card.

Carrier Status is used to Enable or Disable the connection to the Cellular Carrier. By default this option is enabled.

MTU Size

Allows a user to specify the MTU size for custom applications. In most cases this will be left blank and the system will determine the best value.
4.0 Configuration

**IP-Passthrough**

IP pass-through allows the WAN IP address to be assigned to the device connected to the LAN or WAN ports. In this mode the Bullet is for the most part transparent and forwards all traffic to the device connected to the selected Ethernet port except that listed below:

- The WebUI port (Default Port: TCP 80), this port is retained for remote management of the Bullet. This port can be changed to a different port under the **System > Services** Menu.
- The SNMP Listening Port (Default Port: UDP 161).
- Port Forwarding Rules. The BulletPlus forward to other internal modem services (iperf etc) by using X.X.X.1 for an internal IP Address.

The virtual IP address is configurable to allow access to the unit on the LAN/WAN connector once IP-Passthrough has been enabled.

*The firewall/rules must be configured to allow traffic, all incoming carrier traffic is blocked by default.*

**SIM Selection**

The BulletPlus supports one or two SIM cards to be installed. By default the primary SIM is the top SIM, and the unit will try to connect using SIM1 first, and then if it fails to connect, or loses connection to a valid carrier, it will then attempt SIM2.

**Dual Cards Management**

By default the Primary SIM is the SIM installed into the SIM1 slot on the unit. The SIM card installed into the Primary slot will be the Cellular Carrier in which the BulletPlus will attempt to make a connection with. This can be modified here.

**SIM Card-1 Settings**

This feature allows the disabling or enable of data roaming. When data roaming is enabled the modem will be allowed to use data when in roaming status. It is not recommended to allow roaming unless the appropriate data plans are in place.
4.0 Configuration

Carrier Operator

In some cases, a user may want to lock onto a certain carrier. There are four options to choose from: Auto, SIM based, Manual and Fixed.

- Auto will allow the unit to pick the carrier automatically. Data roaming is permitted.
- SIM based will only allow the unit to connect to the network indicated by the SIM card used in the unit.
- Manual will scan for available carriers and allow a user to select from the available carriers. It takes 2 to 3 minutes to complete a scan.
- Fixed allows a user to enter the carrier code (numerical) directly and then the unit will only connect to that carrier.

Technologies Mode

Select the valid types of Carrier connections allowed. For example if set to auto the BulletPlus will connect to any data type. If set to WCDMA only, the BulletPlus will only allow connection to WCDMA related technologies, and not allow the device to connect to lesser (slower) technologies.

APN (Access Point Name)

The APN is required by every Carrier in order to connect to their networks. The APN defines the type of network the Bullet is connected to and the service type. Most Carriers have more than one APN, usually many, dependant on the types of service offered.

Auto APN (default) may allow the unit to quickly connect to a carrier, by cycling through a predetermined list of common APN's. Auto APN will not work for private APN’s or for all carriers.

Advanced+

SIM Pin

The SIM Pin is required for some international carriers. If supplied and required by the cellular carrier, enter the SIM Pin here.

Authentication

Sets the authentication type required to negotiate with peer.

PAP - Password Authentication Protocol.
CHAP - Challenge Handshake Authentication Protocol.

Only required if the carrier requires a User Name and Password.
4.0 Configuration

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Values (characters)</th>
<th>Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A User Name may be required for authentication to a remote peer. Although usually not required for dynamically assigned IP addresses from the wireless carrier. Varies by carrier.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enter the password for the user name above. May not be required by some carriers, or APN's</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network+</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Values (IP Address)</td>
<td>(none)</td>
</tr>
<tr>
<td>In some cases the Static IP address must be entered in this field if assigned by a wireless carrier. In most cases the IP will be read from the SIM card and this field should be left at the default value.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Use Remote DNS</strong></td>
<td>Values (selection)</td>
<td>Enable / Disable</td>
</tr>
<tr>
<td>If enabled the Bullet with use the DNS server as specified automatically by the service provider.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Default Route</strong></td>
<td>Values (Selection)</td>
<td>Yes / No</td>
</tr>
<tr>
<td>Use this interface as the default route for all outbound traffic unless specified in the Network &gt; Routes table.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DNS-Passthrough</strong></td>
<td>Values (Selection)</td>
<td>Enable / Disable</td>
</tr>
<tr>
<td>When enabled DNS-Passthrough will pass on the WAN assigned DNS information to the end device.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SIM Card-2 Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings for SIM Card-2 are identical to that of SIM Card-1, refer to the previous section for information on how to configure SIM Card-2.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.0 Configuration

4.3.3 Carrier > SMS

**SMS Command History**

The SMS menu allows a user to view the SMS Command History and view the SMS messages on the SIM Card.

![Image 4-3-3: SMS > SMS Command History]

**4.3.4 Carrier > SMS Config**

SMS messages can be used to remotely reboot or trigger events in the BulletPlus. SMS alerts can be set up to get SMS messages based on system events such as Roaming status, RSSI, Ethernet Link Status or IO Status.

**System SMS Command**

![Image 4-3-4: SMS > SMS Configuration]
4.0 Configuration

This option allows a user to enable or disable to use of the following SMS commands to reboot or trigger events in the BulletPlus:

<table>
<thead>
<tr>
<th>Status</th>
<th>Values (Selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enable / Disable</td>
</tr>
</tbody>
</table>

MSC#REBOOT  Reboot system
MSC#NMS Send NMS UDP Report
MSC#WEB Send web client inquiry
MSC#MIOP1  open I/O output1
MSC#MIOP2  open I/O output2
MSC#MIOC1  close I/O output1
MSC#MIOC2  close I/O output2

MSC#EURD0  trigger event report0
MSC#EURD1  trigger event report1
MSC#EURD2  trigger event report2
MSC#EURD3  trigger event report3

MSC#GPSR0  trigger gps report0
MSC#GPSR1  trigger gps report1
MSC#GPSR2  trigger gps report2
MSC#GPSR3  trigger gps report3

**Set Phone Filter**

If enabled, the BulletPlus will only accept and execute commands originating from the phone numbers in the Phone Filter List. Up to 6 numbers can be added.
### System SMS Alerts

<table>
<thead>
<tr>
<th>Status</th>
<th>Enable SMS Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Phone Numbers</td>
<td></td>
</tr>
<tr>
<td>Phone No.1</td>
<td></td>
</tr>
<tr>
<td>Phone No.2</td>
<td></td>
</tr>
<tr>
<td>Phone No.3</td>
<td></td>
</tr>
<tr>
<td>Phone No.4</td>
<td></td>
</tr>
<tr>
<td>Phone No.5</td>
<td></td>
</tr>
<tr>
<td>Phone No.6</td>
<td></td>
</tr>
<tr>
<td>Alert Condition Settings</td>
<td></td>
</tr>
<tr>
<td>Time Interval(s)</td>
<td>300 [5-65535]</td>
</tr>
<tr>
<td>Device Alias</td>
<td>UserDevice</td>
</tr>
<tr>
<td>RSSI Check</td>
<td>Enable RSSI Check</td>
</tr>
<tr>
<td>Low Threshold(dBm)</td>
<td>59 [Default -99]</td>
</tr>
<tr>
<td>Carrier Network</td>
<td>Enable Roaming Check</td>
</tr>
<tr>
<td>Home/Roaming Status</td>
<td>Changed</td>
</tr>
<tr>
<td>LAN Ethernet Port</td>
<td>Enable Ethernet Check</td>
</tr>
<tr>
<td>Link Status</td>
<td>Changed</td>
</tr>
<tr>
<td>IO Status</td>
<td>Disable IO Check</td>
</tr>
</tbody>
</table>

#### Status

Enable SMS Alerts. IF enabled SMS alerts will be send when conditions are met as configured to the phone numbers listed.

**Values (Selection)**

Enable / Disable

#### Received Phone Numbers

SMS Alerts can be sent to up to 6 different phone numbers that are listed here.

**Values (Selection)**

(no default)

#### Time Interval(s)

SMS alerts, when active, will be sent out at the frequency defined here.

**Values (Seconds)**

300

#### Device Alias

The device Alias is text that is sent with the SMS message to provide additional information or help identify the source of the SMS alert.

**Values (30 chars)**

UserDevice
## 4.0 Configuration

<table>
<thead>
<tr>
<th><strong>RSSI Check</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable the RSSI alerts.</td>
<td></td>
</tr>
<tr>
<td>Disable RSSI check</td>
<td></td>
</tr>
<tr>
<td>Enable RSSI check</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Low Threshold (dBm)</strong></th>
<th><strong>Values (dBm)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the threshold for RSSI alerts. When the signal strength drops below this threshold, an SMS alert will be sent to the number(s) specified.</td>
<td></td>
</tr>
<tr>
<td>-99</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Carrier Network</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable SMS Alerts for Roaming Status.</td>
<td></td>
</tr>
<tr>
<td>Disable Roaming Check</td>
<td></td>
</tr>
<tr>
<td>Enable Roaming Check</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Home / Roaming Status</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The BulletPlus can send alerts based on the roaming status. Data rates during roaming can be expensive and it is important to know when a device has started roaming.</td>
<td></td>
</tr>
<tr>
<td>In Roaming</td>
<td></td>
</tr>
<tr>
<td>Changed or In Roaming</td>
<td></td>
</tr>
<tr>
<td>Changed to Roaming</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Ethernet</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable SMS Alerts for the Ethernet Link status of the LAN RJ45 port.</td>
<td></td>
</tr>
<tr>
<td>Disable Ethernet check</td>
<td></td>
</tr>
<tr>
<td>Enable Ethernet check</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Ethernet Link Status</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The status of the Ethernet Link of the LAN (RJ45) can be used to send SMS Alerts. The link status may indicate an issue with the connected device.</td>
<td></td>
</tr>
<tr>
<td>Changed</td>
<td></td>
</tr>
<tr>
<td>In no-link</td>
<td></td>
</tr>
<tr>
<td>Changed or in no-link</td>
<td></td>
</tr>
<tr>
<td>Changed to no-link</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>I/O Status</strong></th>
<th><strong>Values (Selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Alerts can be sent based on the state changes of the Digital I/O lines.</td>
<td></td>
</tr>
<tr>
<td>Disable IO Check</td>
<td></td>
</tr>
<tr>
<td>Enable: INPUT Changed</td>
<td></td>
</tr>
<tr>
<td>Enable: Output Changed</td>
<td></td>
</tr>
<tr>
<td>Enable: INPUT or OUTPUT Changed</td>
<td></td>
</tr>
</tbody>
</table>
4.3.5 Carrier > Data Usage

The Data Usage tool on the BulletPlus allows users to monitor the amount of cellular data consumed. Since cellular devices are generally billed based on the amount of data used, alerts can be triggered by setting daily and/or monthly limits. Notifications can be sent using SMS or Email, allowing a early warning if configurable limits are about to be exceeded. The usage data reported by the Data Usage Monitor may not match the data reported by the carrier, but it gives the users an idea of the bandwidth consumed by the BulletPlus.

Status

If enabled the BulletPlus will track the amount of cellular data consumed. If disabled, data is not recorded, even in the Current Data Usage display.

<table>
<thead>
<tr>
<th>Status</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Image 4-3-7: Carrier > Data Usage
### 4.0 Configuration

#### Monthly/Daily Over Limit

Select the notification method used to send alerts when daily or monthly thresholds are exceeded. If none is selected, notifications will not be sent, but data usage will be recorded for reference purposes.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
<tr>
<td>Send Notice SMS</td>
</tr>
<tr>
<td>Send Notice Email</td>
</tr>
<tr>
<td>Both SMS &amp; Email</td>
</tr>
</tbody>
</table>

#### Monthly/Daily Data Unit

Select the data unit to be used for data usage monitoring.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes / K Bytes / M Bytes</td>
</tr>
<tr>
<td>G Bytes</td>
</tr>
</tbody>
</table>

#### Data Limit

Select the data limit for the day or month, used in connection with the data unit is the previous field. If you want to set the limit to 250 Mbytes, select M Bytes for the data unit, and 250 for the data limit.

<table>
<thead>
<tr>
<th>Values (1-65535)</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
</tr>
</tbody>
</table>

#### Period Start Day

For Monthly tracking, select the day the billing/data cycles begins. On this day each month the BulletPlus will reset the data usage monitor numbers.

<table>
<thead>
<tr>
<th>Values (1-31)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Day of Month)</td>
</tr>
</tbody>
</table>

#### Additional Notice 1/2

Up to two (2) additional notices can be sent based on a percentage (10-500%) of the threshold value.

<table>
<thead>
<tr>
<th>Values (10-500%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(none)</td>
</tr>
</tbody>
</table>

#### Phone Number

If SMS is selected as the notification method, enter the phone number to send any SMS messages generated when the data usage exceeds the configured limits.

<table>
<thead>
<tr>
<th>Values (phone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1403</td>
</tr>
</tbody>
</table>
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Daily Over Limit</th>
<th>Send Notice Email</th>
<th>Values (string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily Data Units</td>
<td>MBytes</td>
<td>Daily/Monthly Data Usage Notice</td>
</tr>
<tr>
<td>Data Limit</td>
<td>0-1000</td>
<td></td>
</tr>
<tr>
<td>Mail Subject</td>
<td>Daily Data Usage Notice</td>
<td></td>
</tr>
<tr>
<td>Mail Server(IP/Name)</td>
<td>smtp.gmail.com:465</td>
<td>Values (xxx:port)</td>
</tr>
<tr>
<td>User Name</td>
<td>@gmail.com</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>***</td>
<td></td>
</tr>
<tr>
<td>Authentication</td>
<td>None</td>
<td>Values (selection)</td>
</tr>
<tr>
<td>Mail Recipient</td>
<td>host@</td>
<td>Values (<a href="mailto:xx@xx.xx">xx@xx.xx</a>)</td>
</tr>
</tbody>
</table>

**Mail Subject**

If Email is selected as the notification method, enter the desired email subject line for the notification email sent when daily and/or monthly usage limits are exceeded.

**Mail Server(IP/Name)**

If Email is selected as the notification method, enter the SMTP server details for the account used to send the Email notifications. Domain or IP address with the associated port as shown.

**Username**

If Email is selected as the notification method, enter the username of the Email account used to send Emails.

**Password**

If Email is selected as the notification method, enter the password of the Email account used to send Emails. Most email servers require authentication on outgoing emails.

**Authentication**

If Email is selected as the notification method, enter the password of the Email account used to send Emails. Most email servers require authentication on outgoing emails.

**Mail Recipient**

Enter the email address of the individual or distribution list to send the email notification to.
4.0 Configuration

Data Usage History

The BulletPlus provides an Odometer that shows the total data used by the BulletPlus. You can also click on the More link to get a data usage history summary as seen below.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Settings</td>
<td>SMS</td>
<td>SMSConfig</td>
<td>DataUsage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data Usage Odometer

Total Odometer: 3.69 MB

Last 6 Months Records
- 2015-06: N/A
- 2015-07: N/A
- 2015-08: N/A
- 2015-09: N/A
- 2015-10: N/A
- 2015-11: 2.15 MB

Last 15 days Records
- 2015-10-26: N/A
- 2015-10-27: N/A
- 2015-10-28: N/A
- 2015-10-29: N/A
- 2015-10-30: N/A
- 2015-10-31: N/A

Attention: Measured by local monitor and time zone for reference. Your carrier's data usage accounting on your monthly bill may differ.

Image 4-3-11: Data Usage > Data Usage Odometer
4.0 Configuration

4.4 Wireless (WiFi)

4.4.1 Wireless > Status

The Status window gives a summary of all radio or wireless related settings and connections.

The General Status section shows the Wireless MAC address of the current radio, the Operating Mode (Access Point, Client), the SSID being used, frequency channel information and the type of security used.

Traffic Status shows statistics about the transmitted and received data.

The BulletPlus shows information about all Wireless connections in the Connection Info section. The Wireless MAC address, Noise Floor, Signal to Noise ratio (SNR), Signal Strength (RSSI), The transmit and receive Client Connection Quality (CCQ), TX and RX data rates, and a graphical representation of the signal level or quality.

Image 4-4-1: Wireless > Status
4.0 Configuration

4.4.2 Wireless > Radio1

Radio1 Phy Configuration

The top section of the Wireless Configuration allows for the configuration of the physical radio module. You can turn the radio on or off, and select the channel bandwidth and frequency as seen below.

- **Radio**
  - **Values (selection)**: On / Off
  - This option is used to turn the radio module on or off. If turned off, Wireless connections cannot be made. The default is On.

- **Mode**
  - **Values (selection)**: 802.11B ONLY, 802.11BG, 802.11NG
  - The Mode defines which wireless standard to use for the wireless network. The BulletPlus supports 802.11/b/g/n modes as seen here. Select the appropriate operating mode from the list.
  - The options below are dependant and vary on the operating mode chosen here.

- **Channel Bandwidth**
  - **Values (selection)**: 20MHz Normal Rate
  - Only appears when using 802.11b or b/g modes. Lower channel bandwidths may provide longer range and be less susceptible to noise but at the trade off of data rates. Higher channel bandwidth may provide greater data rates but will be more susceptible to noise and shorter distance potentials.
4.0 Configuration

High Throughput Mode

Select HT20 for a 20MHz channel, or HT40 for a 40 MHz Channel. The 40MHz channel is comprised of 2 adjacent 20MHz channels and the + and—designate to use the higher or lower of the adjacent channels.

HT20
HT40-
HT40+

Advanced Capabilities (Only shown if box is checked)

MPDU Aggregation (Enable/Disable) - Allows multiple data frames to be sent in a single transmission block, allowing for acknowledging or retransmitting if errors occur.

Short GI (Enable/Disable) - GI (guard interval) is the time the receiver waits for any RF reflections to settle before sampling data. Enabling a short GI (400ns) can increase throughput, but can also increase the error rate in some installations.

HT Capabilities Info - TX-STBC RX-STBC1 DSSS_CCK-40
Maximum AMSDU (byte) - 3839
Maximum AMPDU (byte) - 65535

Channel-Freq

The Channel-Freq setting allows configuration of which channel to operate on, auto can be chosen where the unit will automatically pick a channel to operate. If a link cannot be established it will try another channel.

Auto
Channel 01 : 2.412 GHz
Channel 02 : 2.417 GHz
Channel 03 : 2.422 GHz
Channel 04 : 2.427 GHz
Channel 05 : 2.432 GHz
Channel 06 : 2.437 GHz
Channel 07 : 2.442 GHz
Channel 08 : 2.447 GHz
Channel 09 : 2.452 GHz
Channel 10 : 2.457 GHz
Channel 11 : 2.462 GHz

TX Power

This setting establishes the transmit power level which will be presented to the antenna connectors at the rear of the BulletPlus. Unless required, the Tx Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

11 dBm 21 dBm
12 dBm 22 dBm
13 dBm 23 dBm
14 dBm 24 dBm
15 dBm 25 dBm
16 dBm 26 dBm
17 dBm 27 dBm
18 dBm 28 dBm
19 dBm 29 dBm
20 dBm 30 dBm

Refer to FCC (or as otherwise applicable) regulations to ascertain, and not operate beyond, the maximum allowable transmitter output power and effective isotropic radiated power (EIRP).
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values (meters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Distance</td>
<td>100 meters</td>
</tr>
</tbody>
</table>

The Wireless Distance parameter allows a user to set the expected distance the WiFi signal needs to travel. The default is 100m, so the BulletPlus will assume that the signal may need to travel up to 100m so it sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS Thr (256 ~ 2346)</td>
<td>On / OFF</td>
</tr>
</tbody>
</table>

Once the RTS Threshold defined packet size is reached, the system will invoke RTS/CTS flow control. A large RTS Threshold will improve bandwidth, while a smaller RTS Threshold will help the system recover from interference or collisions caused by obstructions.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment Thr (256 ~ 2346)</td>
<td>On / OFF</td>
</tr>
</tbody>
</table>

The Fragmentation Threshold allows the system to change the maximum RF packet size. Increasing the RF packet size reduces the need to break packets into smaller fragments. Increasing the fragmentation threshold slightly may improve performance if a high packet error rate is experienced.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCA Power Thr (4 ~ 127)</td>
<td>28</td>
</tr>
</tbody>
</table>

The Clear Channel Assessment uses carrier sense and energy detection to determine if a channel/medium is available for transmission. Changing the threshold will impact how the BulletPlus Wifi determines channel availability.
4.0 Configuration

Radio1 Virtual Interface

The bottom section of the Wireless Configuration provides for the configuration of the Operating Mode of the Wireless Interface, the TX power, Wireless Network information, and Wireless Encryption. The BulletPlus can support multiple virtual interfaces. These interfaces provide different SSID's for different users, and can also be assigned to separate subnets (Network Interfaces) to prevent groups from interacting.

![Radio Virtual Interface](Image 4-4-3: Wireless > Radio Configuration)

**Network**

Choose between LAN or WAN for the Virtual Interface. If additional Network Interfaces have been defined in the Network > LAN section, the Interface name will also appear here.

**Mode**

**Access Point** - An Access Point may provide a wireless data connection to many clients, such as stations, repeaters, or other supported wireless devices such as laptops etc.

If more than 1 Virtual Interface (more than 1 SSID) has been defined, the BulletPlus can ONLY operate as a Access Point, and will be locked into this mode.

**Station/Client** - A Station may sustain one wireless connection, i.e. to an Access Point.

**Repeater** - A Repeater can be connected to an Access Point to extend the range and provide a wireless data connection to many clients, such as stations.
4.0 Configuration

TX bitrate

This setting determines the rate at which the data is to be wirelessly transferred.

The default is ‘Auto’ and, in this configuration, the unit will transfer data at the highest possible rate in consideration of the receive signal strength (RSSI).

Setting a specific value of transmission rate has the benefit of ‘predictability’ of that rate, but if the RSSI drops below the required minimum level to support that rate, communications will fail.

<table>
<thead>
<tr>
<th>802.11 b/g</th>
<th>802.11n (HT20/HT40)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto</strong></td>
<td><strong>Auto</strong></td>
</tr>
<tr>
<td>1 Mbps (802.11b,g)</td>
<td>mcs-0 (7.2/15) Mbps</td>
</tr>
<tr>
<td>2 Mbps (802.11b,g)</td>
<td>mcs-1 (14.4/30.0) Mbps</td>
</tr>
<tr>
<td>5.5 Mbps (802.11b,g)</td>
<td>mcs-2 (21.7/45.0) Mbps</td>
</tr>
<tr>
<td>11 Mbps (802.11b,g)</td>
<td>mcs-3 (28.9/60.0) Mbps</td>
</tr>
<tr>
<td>6 Mbps (802.11g)</td>
<td>mcs-4 (43.3/90.0) Mbps</td>
</tr>
<tr>
<td>9 Mbps (802.11g)</td>
<td>mcs-5 (57.8/120.0) Mbps</td>
</tr>
<tr>
<td>12 Mbps (802.11g)</td>
<td>mcs-6 (65.0/135.0) Mbps</td>
</tr>
<tr>
<td>18 Mbps (802.11g)</td>
<td>mcs-7 (72.2/150.0) Mbps</td>
</tr>
<tr>
<td>24 Mbps (802.11g)</td>
<td></td>
</tr>
<tr>
<td>36 Mbps (802.11g)</td>
<td></td>
</tr>
<tr>
<td>48 Mbps (802.11g)</td>
<td></td>
</tr>
<tr>
<td>54 Mbps (802.11g)</td>
<td></td>
</tr>
</tbody>
</table>

ESSID Broadcast

Disabling the SSID broadcast helps secure the wireless network. Enabling the broadcast of the SSID (Network Name) will permit others to ‘see’ the wireless network and perhaps attempt to ‘join’ it.

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>On / Off</th>
</tr>
</thead>
</table>

AP Isolation

When AP Isolation is enabled wireless devices connected to this SSID will not be able to communicate with each other. In other words if the BulletPlus is being used as a Hot Spot for many wireless clients, AP Isolation would provide security for those clients by not allowing access to any other wireless device.

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>On / Off</th>
</tr>
</thead>
</table>

WMM

WiFi Multimedia (WMM) is a feature that enhances the quality of service on a network by prioritizing data packets according to data type. (Video, Voice, Best Effort, Background).

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>On / Off</th>
</tr>
</thead>
</table>

© Microhard Systems Inc.
4.0 Configuration

SSID: Service Set Identifier. The 'name' of a wireless network. In an open wireless network, the SSID is broadcast; in a closed system it is not. The SSID must be known by a potential client for it to be able to access the wireless network.

All devices connecting to the BulletPlus in a given network must use the SSID of the BulletPlus. This unique network address is not only a security feature for a particular network, but also allows other networks - with their own unique network address - to operate in the same area without the possibility of undesired data exchange between networks.

Encryption Types

The encryption types define the type of security used for the Wireless Interface, to join a network a device must know the correct password/passphrase/key.

Security options are dependent on the version type. This section describes all available options. Export versions may not have all optional available to meet regulatory requirements set government policies.

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>WPA (PSK)</td>
<td></td>
</tr>
<tr>
<td>WPA2 (PSK)</td>
<td></td>
</tr>
<tr>
<td>WPA+WPA2 (PSK)</td>
<td></td>
</tr>
<tr>
<td>WPA Enterprise (RADIUS)</td>
<td></td>
</tr>
<tr>
<td>WPA2 Enterprise (RADIUS)</td>
<td></td>
</tr>
<tr>
<td>WPA+WPA2 Enterprise(RADIUS)</td>
<td></td>
</tr>
</tbody>
</table>

WPA PSK

This is the password, or preshared key that is required by any device to connect to the wireless interface of the BulletPlus. It is strongly recommended to always have a password defined, and changed from the factory default.

<table>
<thead>
<tr>
<th>WPA PSK</th>
<th>Values (string)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0123456789</td>
</tr>
</tbody>
</table>

Show Password

Check this box to show the currently configured password for WPA/WPA2 encryption passphrase.

<table>
<thead>
<tr>
<th>Show Password</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>unchecked</td>
</tr>
</tbody>
</table>

RADIUS IP Address

If using Enterprise (RADIUS) encryption, enter the IP Address of the RADIUS authentication server here.

<table>
<thead>
<tr>
<th>RADIUS IP Address</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(no default)</td>
</tr>
</tbody>
</table>

RADIUS Port

If using Enterprise (RADIUS) encryption, enter the port number of the RADIUS authentication server here.

<table>
<thead>
<tr>
<th>RADIUS Port</th>
<th>Values (port)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(no default)</td>
</tr>
</tbody>
</table>

RADIUS Server Key

This is the password, or preshared key that is required by any device to connect to the wireless interface of the BulletPlus. It is strongly recommended to always have a password defined, and changed from the factory default.

<table>
<thead>
<tr>
<th>RADIUS Server Key</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0123456789</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.4.3 Wireless > HotSpot

The Wireless Hotspot configuration is used when providing public hotspot services and it is required to use a server or web based authentication service to verify users, provide terms of use or other information.

Use this option to enable or disable the hotspot authentication service. There are three different options for the Hotspot Mode:

- **Simple Internal** - Display a simple text based terms of use or statement to connected users.
- **Simple External** - Display an external webpage
- **RADIUS/UAM** - Use a 3rd Party Authentication service to authenticate and/or prompt users to agree to terms of service.

If the Hotspot Mode, RADIUS/UAM is chosen, this is a secret password between the Redirect URL and the Hotspot given by the hotspot provider.

**UAM Login URL**

- **Values**

**UAM Secret**

- **Values**
  - hotsys123
## 4.0 Configuration

### Hotspot Network Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspot Network</td>
<td>Varies</td>
</tr>
<tr>
<td>This field is used to specify which configured network is bonded to the hotspot. Sub networks can be created in the Network &gt; LAN menu, which are dedicated to the hotspot devices.</td>
<td></td>
</tr>
<tr>
<td>&quot;The DHCP service for the network used should be turned off as all IP address assignments will be made by the hotspot service provider.&quot;</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network IP Address</td>
<td>192.168.182.0</td>
</tr>
<tr>
<td>Specify the IP Address of the Hotspot application. All hotspot clients will get an IP address in the same network as the Hotspot.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Specify the Netmask of the Hotspot application. All hotspot clients will get an IP address in the same network as the Hotspot.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Domain</td>
<td>Key.chillispot.info</td>
</tr>
<tr>
<td>Provide your service providers 1st DNS Server domain.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary DNS</td>
<td>208.67.222.222</td>
</tr>
<tr>
<td>Specify the Primary DNS server to be used by devices connected to the Hotspot network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary DNS</td>
<td>208.67.222.220</td>
</tr>
<tr>
<td>Specify the Secondary DNS server to be used by devices connected to the Hotspot network.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Start</td>
<td>3</td>
</tr>
<tr>
<td>When devices connect to the BulletPlus Wifi and Hotspot is enabled, the Hotspot will assign the IP addresses to the connected devices, select the starting range here.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP End</td>
<td>250</td>
</tr>
<tr>
<td>When devices connect to the BulletPlus Wifi and Hotspot is enabled, the Hotspot will assign the IP addresses to the connected devices, select the ending range here.</td>
<td></td>
</tr>
</tbody>
</table>
4.0 Configuration

Hotspot Radius Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius NAS ID</td>
<td>Microhard_1</td>
</tr>
<tr>
<td>Radius Server 1</td>
<td>radius.hotspotsystem.com</td>
</tr>
<tr>
<td>Radius Server 2</td>
<td>radius2.hotspotsystem.com</td>
</tr>
<tr>
<td>Radius Auth Port</td>
<td>1812</td>
</tr>
<tr>
<td>Radius Acct Port</td>
<td>1813</td>
</tr>
<tr>
<td>Radius Secret</td>
<td>hotsys123</td>
</tr>
<tr>
<td>Radius CoA UDP Port</td>
<td>1799</td>
</tr>
<tr>
<td>Radius Session Timeout</td>
<td>8640 Secs (0-Disabled)</td>
</tr>
<tr>
<td>Radius Idle Timeout</td>
<td>900 Secs (0-Disabled)</td>
</tr>
</tbody>
</table>

This is the RADIUS name of your Hotspot as given by your Hotspot Service Provider.

As assigned by the Hotspot Service Provider, the name or IP address of the primary RADIUS Server.

As assigned by the Hotspot Service Provider, the name or IP address of the alternate RADIUS Server.

The Radius Authentication Port Number. The default is 1812. This is provided by your Hotspot service provider.

The Radius Account Port Number. The default is 1813. This is provided by your Hotspot service provider.

Also called a shared key, this is the RADIUS password assigned by you Hotspot provider.
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius CoA UDP Port</td>
<td>Specify the Radius CoA UDP Port here. This information is supplied by the hotspot service provider.</td>
<td>3799</td>
</tr>
<tr>
<td>Radius Session Timeout</td>
<td>Specify the Radius Session Timeout. In seconds, 0 = disabled.</td>
<td>3600</td>
</tr>
<tr>
<td>Radius Idle Timeout</td>
<td>Specify the Radius Idle Timeout. In seconds, 0 = disabled.</td>
<td>900</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.5 Firewall

4.5.1 Firewall > Summary

The Firewall Summary allows a user to see detailed information about how the firewall is operating. The All, Filter, Nat, Raw, and Mangle options can be used to view different aspects of the firewall.

![Image 4-5-1: Firewall > Status]
4.0 Configuration

4.5.2 Firewall > General

The General Firewall settings allow users to enable or disable the firewall, and to decide which areas of the modem to protect. The Firewall can also be reset to factory defaults from this area of the WebUI.

In a cellular device such as this, it is highly recommended to configure the firewall to protect any devices connected to the modem, and to control data usage. This is especially important with units set up with a public IP address as the modem is effectively on the public internet and is susceptible to a wide range of threats which may severely impact the data usage. This can be avoided by blocking all Cellular traffic and setting up specific rules to either open only used ports, or even restrict access to specific IP/networks.

- **WAN Remote Management**
  - **Values**: Enable / Disable
  - Allow remote management of the BulletPlus on the WAN side using the WebUI on port 80 (HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or Cellular if enabled).

- **Carrier Remote Management**
  - **Values**: Enable / Disable
  - Allow remote management of the BulletPlus from the Cellular side of using the WebUI on port 80 (HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or WAN if enabled).

- **WAN Request**
  - **Values**: Block / Allow
  - When Blocked the BulletPlus will block all requests from devices on the WAN unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **WAN Remote Management** option.

- **Carrier Request**
  - **Values**: Block / Allow
  - When Blocked all requests from devices on the Cellular (Wireless Carrier) side will be blocked, unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **4G Remote Management** option.
4.0 Configuration

### LAN to WAN Access Control

Allows or Blocks traffic from the LAN accessing the WAN unless specified otherwise using the Access Rules, MAC, and IP List configuration.

**Values**

| Block / Allow |

### LAN to Carrier Access Control

Allows or Blocks traffic from the LAN accessing the Cell connection unless specified otherwise using the Access Rules, MAC, and IP List configuration.

**Values**

| Block / Allow |

### Anti-Spoof

The Anti-Spoof protection is to create some firewall rules assigned to the external interface (WAN & Cellular) of the firewall that examines the source address of all packets crossing that interface coming from outside. If the address belongs to the internal network or the firewall itself, the packet is dropped.

**Values**

| Enable / Disable |

### Packet Normalization

Packet Normalization is the normalization of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembled fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations.

**Values**

| Enable / Disable |
4.0 Configuration

4.5.3 Firewall > Port Forwarding

The BulletPlus can be used to provide remote access to connected devices. To access these devices a user must define how incoming traffic is handled by the BulletPlus. If all incoming traffic is intended for a specific connected device, DMZ could be used to simplify the process, as all incoming traffic can be directed towards a specific IP address.

In the case where there is multiple devices, or only specific ports need to be passed, Port forwarding is used to forward traffic coming in from the WAN (Cellular) to specific IP Addresses and Ports on the LAN. Port forwarding can be used in combination with other firewall features, but the Firewall must be enabled for Port forwarding to be in effect. If the WAN Request is blocked on the General Tab, additional rules and/or IP Lists must be set up to allow the port forwarding traffic to pass through the firewall.

IP-Passthrough (Carrier > Settings) is another option for passing traffic through the BulletPlus, in this case all traffic is passed to a single device connected to the RJ45 port of the BulletPlus, The device must be set for DHCP, as the BulletPlus assigns the WAN IP to the device, and the modem enters into a transparent mode, routing all traffic to the RJ45 port. This option bypasses all firewall features of the BulletPlus, as well as all other features of the BulletPlus such as COM, VPN, GPS etc.

**Firewall Port Forwarding**

<table>
<thead>
<tr>
<th>System</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>General</td>
<td>Port Forwarding</td>
<td>MAC-IP List</td>
<td>Rules</td>
<td>Firewall Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notice**

Port Forwarding rules are taken into consideration after the General firewall settings are applied. If the WAN and/or cellular traffic is blocked, additional rules must be created:
1. Add rules in the Rules configuration to open ports or allow IP addresses.
2. Create a IP/Mac List to allow desired connections.

**Firewall DMZ Configuration**

<table>
<thead>
<tr>
<th>DMZ Source: Carrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ Mode</td>
</tr>
<tr>
<td>DMZ Server IP</td>
</tr>
<tr>
<td>Exception Port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DMZ Source: WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMZ Mode</td>
</tr>
<tr>
<td>DMZ Server IP</td>
</tr>
<tr>
<td>Exception Port</td>
</tr>
</tbody>
</table>

**Firewall Port Forwarding Configuration**

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Internal Server IP</th>
<th>Internal Port</th>
<th>Protocol</th>
<th>External Port</th>
<th>Add Port Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward1</td>
<td>Carrier</td>
<td>192.168.2.1</td>
<td>8000</td>
<td>TCP</td>
<td>2600</td>
<td></td>
</tr>
</tbody>
</table>

**Firewall Port Forwarding Summary**

If DMZ is enabled and an exception port for the WebUI is not specified, remote management will not be possible. The default port for remote management is TCP 80.
## 4.0 Configuration

<table>
<thead>
<tr>
<th><strong>DMZ Mode</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable DMZ Mode. DMZ can be used to forward all traffic to the DMZ Server IP listed below.</td>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>DMZ Server IP</strong></th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address of the device on the LAN side of the BulletPlus where all the traffic will be forwarded to.</td>
<td>192.168.100.100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Exception Port</strong></th>
<th>Values (Port #)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter an exception port number that will NOT be forwarded to the DMZ server IP. Usually a configuration or remote management port that is excluded to retain external control of the BulletPlus.</td>
<td>0</td>
</tr>
</tbody>
</table>

### Firewall Port Forwarding Configuration

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Values (10 chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to 10 characters.</td>
<td>Forward</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Source</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the source for the traffic, from either the 3G/Cellular or from the WAN.</td>
<td>Carrier / WAN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Internal Server IP</strong></th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP address of the intended internal (i.e. on LAN side of BulletPlus) server. This is the IP address of the device you are forwarding traffic to.</td>
<td>192.168.2.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Internal Port</strong></th>
<th>Values (Port #)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target port number of the internal server on the LAN IP entered above.</td>
<td>3000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Protocol</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the type of transport protocol used. For example Telnet uses TCP, SNMP uses UDP, etc.</td>
<td>TCP / UDP / Both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>External Port</strong></th>
<th>Values (Port #)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port number of the incoming request (from 4G/WAN-side).</td>
<td>2000</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.5.4 Firewall > MAC-IP List

MAC List configuration can be used to control which physical LAN devices can access the ports on the BulletPlus, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the BulletPlus, by restricting or allowing connections based on the IP Address/Subnet.

MAC-IP List can be used alone or in combination with LAN to WAN/4G Access Control to provide secure access to the physical ports of the BulletPlus.

Firewall MAC List Configuration

- **Rule Name**: The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.
- **MAC Address**: Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above. Not case sensitive.

```
| MAC List | 00:00:00:00:00:00 |
```

Image 4-5-5: Firewall > MAC-IP List

Firewall MAC List Configuration

- **Rule Name**: The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.
- **MAC Address**: Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above. Not case sensitive.

```
| MAC List | 00:00:00:00:00:00 |
```

Image 4-5-5: Firewall > MAC-IP List
## 4.0 Configuration

### Firewall MAC List Configuration (Continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACCEPT / DROP / REJECT</td>
</tr>
</tbody>
</table>

The Action is used to define how the rule handles the connection request. ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

### Firewall IP List Configuration

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Values (10 chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP_List</td>
</tr>
</tbody>
</table>

The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.

<table>
<thead>
<tr>
<th>Action</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ACCEPT / DROP / REJECT</td>
</tr>
</tbody>
</table>

The Action is used to define how the rule handles the connection request. ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

<table>
<thead>
<tr>
<th>Source</th>
<th>Values (Selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LAN/LAN1/WAN/Cell/USB NONE</td>
</tr>
</tbody>
</table>

Enter the specific zone that the IP List will apply to, Cellular, LAN, WAN or None (both).

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>192.168.0.0</td>
</tr>
</tbody>
</table>

Match incoming traffic from the specified source IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)
4.0 Configuration

4.5.5 Firewall > Rules

Once the firewall is turned on, rules configuration can be used to define specific rules on how local and remote devices access different ports and services. MAC List and IP List are used for general access, and are applied before rules are processed.

It is highly recommended to block as much traffic as possible from the modem, especially when using a public IP address. The best security would be to allow traffic only from trusted IP addresses, and only the specific ports being used, and block everything else. Not configuring the firewall and the firewall rules correctly could result in unpredictable data charges from the cellular carrier.

Refer to Appendix D for an example of how to set up a firewall to block all connections and then add access to only specific IP's and Ports.

Appendix D: Firewall Example

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Values (10 Chars)</th>
<th>characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTION</td>
<td>Accept, Reject, Drop</td>
<td>Values (selection)</td>
</tr>
<tr>
<td>Source</td>
<td>LAN/LAN1/WAN/Carrier Access Control</td>
<td>Values</td>
</tr>
<tr>
<td>Destination</td>
<td>None, IP range, Subnet</td>
<td>Values</td>
</tr>
<tr>
<td>Destination Port</td>
<td>0-65535</td>
<td>Values</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP, UDP</td>
<td>Values</td>
</tr>
</tbody>
</table>

Image 4-5-6: Firewall > Rules

The rule name is used to identify the created rule. Each rule must have a unique name and up to 10 characters can be used.

The Action is used to define how the rule handles the connection request. ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

This is configured based on how the WAN/Carrier Request and LAN to WAN/Carrier Access Control are configured in the previous menus.

Select the zone which is to be the source of the data traffic. The LAN/LAN1 refers to local connections on the BulletPlus.
## 4.0 Configuration

<table>
<thead>
<tr>
<th>Source IPs</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match incoming traffic from the specified source IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0 to 192.168.0.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the zone which is the intended destination of the data traffic. 3G/4G applies to the wireless connection to the cellular carrier and the LAN, LAN1, USB refers to local connections on the BulletPlus.</td>
<td></td>
</tr>
<tr>
<td>LAN/LAN1/Cell/WAN/USB None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination IPs</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match incoming traffic from the specified destination IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</td>
<td></td>
</tr>
<tr>
<td>192.168.0.0 to 192.168.0.0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination Port</th>
<th>Values (port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match incoming traffic directed at the given destination port or port range. (To specify a port range use a From:To (100:200) format)</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>The protocol field defines the transport protocol type controlled by the rule.</td>
<td></td>
</tr>
<tr>
<td>TCP UDP Both ICMP</td>
<td></td>
</tr>
</tbody>
</table>
4.0 Configuration

4.5.6 Firewall > Firewall Default

The Firewall Default option allows a user to return the modem's firewall setting back to the default values without having to reset the entire modem.

Image 4-4-7: Firewall > Firewall Default
4.0 Configuration

4.6 VPN

4.6.1 VPN > Summary

A Virtual Private Network (VPN) may be configured to enable a tunnel between the BulletPlus and a remote network. The BulletPlus supports VPN IPsec Gateway to Gateway (site-to-site) tunneling, meaning you are using the BulletPlus to create a tunnel to a network with VPN capabilities (Another BulletPlus or VPN capable device). The BulletPlus can also operate as a L2TP Server, allowing users to VPN into the unit from a remote PC, and a L2TP Client.
4.6.2 VPN > Gateway To Gateway (Site-to-Site)

A Gateway to Gateway connection is used to create a tunnel between two VPN devices such as an BulletPlus and another device (another BulletPlus or Cisco VPN Router or another vendor…). The local and remote group settings will need to be configured below to mirror those set on the other VPN device.

```
<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Enable</th>
<th>Authentication</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Prepared Key</td>
<td>40</td>
</tr>
</tbody>
</table>

Local Group Setup

<table>
<thead>
<tr>
<th>Local Security Gateway Type</th>
<th>Interface IP Address</th>
<th>Next-hop Gateway IP</th>
<th>Group Subnet Gateway</th>
<th>Group Subnet IP/Mask - 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Only</td>
<td>192.168.199.2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remote Group Setup

<table>
<thead>
<tr>
<th>Remote Security Gateway Type</th>
<th>Gateway IP Address</th>
<th>Next-hop Gateway IP</th>
<th>Group Subnet IP/Mask - 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPsec Setup

<table>
<thead>
<tr>
<th>Aggressive Mode</th>
<th>Phase1 Strict Mode</th>
<th>Phase 1 DH Group</th>
<th>Phase 1 Encryption</th>
<th>Phase 1 Authentication</th>
<th>Phase 1 SA Lifetimes</th>
<th>Perfect Forward Secrecy</th>
<th>Phase 2 SA Type</th>
<th>Phase2 Strict Mode</th>
<th>Phase 2 DH Group</th>
<th>Phase 2 Encryption</th>
<th>Phase 2 Authentication</th>
<th>Phase 2 SA Lifetimes</th>
<th>Preshared Key</th>
<th>DPD Delay(s)</th>
<th>DPD Disable timeout</th>
<th>DPD Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>modp1024</td>
<td>3des</td>
<td>0</td>
<td>0</td>
<td>ESP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>9000</td>
<td></td>
<td></td>
<td></td>
<td>90</td>
</tr>
</tbody>
</table>

```

Image 4-6-2: VPN > Gateway to Gateway

Tunnel Name

Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name.

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel1</td>
<td></td>
</tr>
</tbody>
</table>
# 4.0 Configuration

## Local Group Setup

<table>
<thead>
<tr>
<th>Enable</th>
<th>Used to enable (checked) is disable (unchecked) the VPN tunnel.</th>
</tr>
</thead>
</table>

### Interface IP Address

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the IP address of the BulletPlus, which is the local VPN Gateway.</td>
</tr>
</tbody>
</table>

### Current IP Address

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used to enable (checked) is disable (unchecked) the VPN tunnel.</td>
</tr>
</tbody>
</table>

### Server ID

<table>
<thead>
<tr>
<th>Values (characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This option appears when the Local Security Gateway Type specifies that the Server ID is required for the connection. The Server ID must be in the format @name, where name can be anything. Both routers must know each others names to establish a connection.</td>
</tr>
</tbody>
</table>

### Next-hop Gateway IP

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.</td>
</tr>
</tbody>
</table>

### Group Subnet IP

<table>
<thead>
<tr>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the local network by specifying the local subnet. The local and remote routers must use different subnets.</td>
</tr>
</tbody>
</table>
## 4.0 Configuration

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group Subnet Mask</strong></td>
<td>Specify the subnet mask of the local network address.</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td><strong>Group Subnet Gateway</strong></td>
<td>Enter the Gateway for the local group network.</td>
<td>(no default)</td>
</tr>
<tr>
<td><strong>Remote Group Setup</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Remote Security Gateway Type</strong></td>
<td>Specify the method for identifying the router to establish the VPN tunnel. The Local Security Gateway is on this router; the Remote Security Gateway is on the other router. At least one of the routers must have either a static IP address or a dynamic IP with server id to make a connection. (See Local Group Setup for details)</td>
<td>IP Only, IP + Server ID, Dynamic IP + Server ID</td>
</tr>
<tr>
<td><strong>Gateway IP Address</strong></td>
<td>If the remote VPN router has a static IP address, enter the IP address of the remote VPN Gateway here.</td>
<td>(no default)</td>
</tr>
<tr>
<td><strong>Server ID</strong></td>
<td>This option appears when the Remote Security Gateway Type specifies that the Server ID is required for the connection. The Server ID must be in the format @name, where name can be anything. Both routers must know each others names to establish a connection.</td>
<td>(no default)</td>
</tr>
<tr>
<td><strong>Next-hop Gateway IP</strong></td>
<td>Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.</td>
<td>(no default)</td>
</tr>
<tr>
<td><strong>Subnet IP Address</strong></td>
<td>Define the remote network by specifying the local subnet.</td>
<td>(no default)</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Specify the subnet mask of the remote network address.</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
## 4.0 Configuration

### IPsec Setup

<table>
<thead>
<tr>
<th>Phase 1 DH Group</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>modp1024</td>
</tr>
<tr>
<td></td>
<td>modp1536</td>
</tr>
<tr>
<td></td>
<td>modp2048</td>
</tr>
</tbody>
</table>

Select value to match the values required by the remote VPN router.

### Phase 1 Encryption

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
</tr>
<tr>
<td>aes</td>
</tr>
<tr>
<td>aes128</td>
</tr>
<tr>
<td>aes256</td>
</tr>
</tbody>
</table>

Select value to match the Phase 1 Encryption type used by the remote VPN router.

### Phase 1 Authentication

<table>
<thead>
<tr>
<th>md5</th>
<th>sha1</th>
</tr>
</thead>
</table>

Select value to match the Phase 1 Authentication used by the remote VPN router.

### Phase 1 SA Life Time

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>28800</td>
</tr>
</tbody>
</table>

Select value to match the values required by the remote VPN router.

### Perfect Forward Secrecy (pfs)

<table>
<thead>
<tr>
<th>Disable / Enable</th>
</tr>
</thead>
</table>

Select value to match the values required by the remote VPN router.

### Phase 2 DH Group

<table>
<thead>
<tr>
<th>modp1024</th>
</tr>
</thead>
<tbody>
<tr>
<td>modp1536</td>
</tr>
<tr>
<td>modp2048</td>
</tr>
</tbody>
</table>

Select value to match the values required by the remote VPN router.

### Phase 2 Encryption

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
</tr>
<tr>
<td>aes</td>
</tr>
<tr>
<td>aes128</td>
</tr>
<tr>
<td>aes256</td>
</tr>
</tbody>
</table>

Select value to match the Phase 1 Encryption type used by the remote VPN router.
## 4.0 Configuration

### Phase 2 Authentication
Select value to match the Phase 1 Authentication used by the remote VPN router.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>md5</td>
</tr>
<tr>
<td>sha1</td>
</tr>
</tbody>
</table>

### Phase 2 SA Life Time
Select value to match the values required by the remote VPN router.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>3600</td>
</tr>
</tbody>
</table>

### Preshared Key
Set the Preshared Key required to authenticate with the remote VPN router.

<table>
<thead>
<tr>
<th>Values (characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
</tr>
</tbody>
</table>

### DPD Delay(s)
Dead Peer Detection is used to detect if there is a dead peer. Set the DPD Delay (seconds), as required.

<table>
<thead>
<tr>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
</tr>
</tbody>
</table>

### DPD Timeout(s)
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.

<table>
<thead>
<tr>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>122</td>
</tr>
</tbody>
</table>

### DPD Action
Set the DPD action, hold or clear, as required.

<table>
<thead>
<tr>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold</td>
</tr>
<tr>
<td>Clear</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.6.3 VPN > L2TP Client

The BulletPlus can operate as a L2TP Client, allowing a VPN connection to be made with a L2TP Server.

<table>
<thead>
<tr>
<th>Tunnel Name</th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable</th>
<th>Values (checkbox)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable (Checked)</td>
<td></td>
</tr>
</tbody>
</table>
## 4.0 Configuration

<table>
<thead>
<tr>
<th><strong>Local Interface IP Address</strong></th>
<th>This will display the current BulletPlus WAN (Cellular) IP Address.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (IP Address)</strong></td>
<td><strong>Current IP</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Remote Gateway IP Address</strong></th>
<th>Enter the IP Address of the Remote Gateway that you wish to establish a connection with.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (IP Address)</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Remote Server ID</strong></th>
<th>Some servers require that you know the Server ID as well as the IP address. Enter the Server ID of the remote router here.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Remote Subnet IP</strong></th>
<th>In order to communicate with the devices on the other side of the tunnel, the BulletPlus must know which data to pass through the tunnel, to do this enter the Remote Subnet network IP address here.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (IP Address)</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Remote Subnet Mask</strong></th>
<th>Enter the Remote Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (IP Address)</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Idle time before hanging up</strong></th>
<th>Enter the Idle time (in seconds) to wait before giving up the PPP connection. The default is 0, which means the time is infinite. (0—65535)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (seconds)</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Username</strong></th>
<th>Enter the Username</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (chars)</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Preshared Key</strong></th>
<th>The preshared key is required to connect to the L2TP Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Values (chars)</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

**IPSec Setup - See previous sections for additional info.**
4.0 Configuration

4.6.4 Network > OpenVPN

OpenVPN Server

The BulletPlus supports OpenVPN and can be configured as a Server or a Client. This section outlines the configuration of a OpenVPN Server.

Enable/Disable the OpenVPN Mode by selecting the mode to operate in, Client or Server. When the Server is enabled it will be listening for incoming connection requests from OpenVPN Clients.

The TCP/UDP port which the server is listening on. Default is 1194
## 4.0 Configuration

<table>
<thead>
<tr>
<th><strong>Tunnel Protocol</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP / UDP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>MSSFIX/Fragment size</strong></th>
<th>Values (size)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1370</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Root Certificate</strong></th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ca.crt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Public Server Certificate</strong></th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server.crt</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Private Server Key</strong></th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server.key</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>TLS Auth Key</strong></th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(no default)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>User/Password Authentication</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(no default)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Diffie hellman parameter</strong></th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DH2048 / DH1024</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Server Virtual Subnet / Subnet Mask</strong></th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.8.0.0</td>
</tr>
</tbody>
</table>
4.0 Configuration

Push DNS to Client
If enabled (Auto) the server will push its DNS server information to the client. Manual allows the DNS information to be manually entered.

Values (selection)
NO / Auto / Manual

Client Isolation
When select yes, the clients will not see each other. Select no, it will allow different clients to be able to "see" each other. By default, clients will only see the server.

Values (selection)
No / Yes

Keep Alive Ping Interval
The keep alive directive causes ping-like messages to be sent back and forth over the link so that each side knows when the other side has gone down. Default 10 seconds.

Values (seconds)
10

Keep Alive Ping Period
Default 120 seconds. Ping every 10 seconds, assume that remote peer is down if no ping received during a 120 second time period. (must be at least twice the interval specified above)

Values (seconds)
120

Cipher
Select a cryptographic cipher. Must be the same on Server and Client.

Values (selection)
DES-CBC
RC2-CBC
DES-EDE-CBC
DES-EDE3-CBC
DESX-CBC
BF-CBC
RC2-40-CBC
CAST5-CBC
RC2-64-CBC
AES-128-CBC
AES-192-CBC
AES-256-CBC
SEED-CBC

Use LZO Compression
Enable/Disable LZO compression on the VPN link. Lempel–Ziv–Oberhumer (LZO) is a lossless data compression algorithm.

Values (selection)
Enable / Disable

OpenVPN Server Network Settings
OpenVPN support multiple subnet behind server/client. So that the vpn connection can reach the subnet behind. Each subnet must be specified to the data can be routed correctly.

Values (selection)
(no default)
4.0 Configuration

OpenVPN Client

The BulletPlus supports OpenVPN and can be configured as a Server or a Client. This section outlines the configuration of a OpenVPN Client.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Gateway To Gateway</td>
<td>L2TP Client</td>
<td>OpenVPN</td>
<td>GRE</td>
<td>VPN Users</td>
<td>Certificates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OpenVPN Setup**

- **OpenVPN Mode**: 
  - **Values (selection)**: Client / Server / Disable
  - **Client**

**OpenVPN Client Setup**

- **Client bridge Mode**: 
  - **Values (selection)**: (unchecked)

- **Tunnel Protocol**: 
  - **Values (selection)**: TCP / UDP

- **MSSFix/Fragment size**: 1370

- **Server IP: Port**: 
  - **Add Remove**

- **Root Certificate**: ca.crt
  - **Client Certificate**: client.crt
  - **Client Key**: client.key
  - **TLS Auth Key**: ca.key

- **User/Password Authentication**: (unchecked)

- **Keep Alive Ping Interval(seconds)**: 10
  - **Keep Alive Ping Period(seconds)**: (at least twice of interval)

- **Cipher**: BF-CBC
  - **Use LZO Compression**: Disable

**Image 4-6-4: VPN > OpenVPN Client**

OpenVPN Mode

Enable/Disable the OpenVPN Mode by selecting the mode to operate in, Client or Server. When the Server is enabled it will be listening for incoming connection requests from OpenVPN Clients.

Client Bridge Mode

Select the box to enable Client Bridge Mode.

Pseudowire Mode

When Client Bridge Mode is selected the option to enable Pseudowire Mode is made available.

Tunnel Protocol

Select the Tunnel Protocol to be used. The options are TCP and UDP, the default is UDP.
## 4.0 Configuration

### MSSFIX/Fragment size

The maximum resulting UDP send packet size after the OpenVPN has fully encapsulated data. Packets exceeding this max value will be fragmented.

<table>
<thead>
<tr>
<th>Values (size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1370</td>
</tr>
</tbody>
</table>

### Server IP/Port

The IP Address and TCP/UDP port which the server is located. This is generally the Public IP Address of the router/modem where the Server is running.

<table>
<thead>
<tr>
<th>Values (IP/Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>

### Root Certificate

The root certificate file (CA file) that all the server and clients must have in common.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca.crt</td>
</tr>
</tbody>
</table>

### Client Certificate

The Client Certificate which is the certificate file that resides on only the client.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>client.crt</td>
</tr>
</tbody>
</table>

### Client Key

The private Client Key, which should not be disclosed.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>client.key</td>
</tr>
</tbody>
</table>

### TLS Auth Key

The server and each client must have a copy of this key to do TLS authentication.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no default)</td>
</tr>
</tbody>
</table>

### Cipher

Select a cryptographic cipher. Must be the same on Server and Client.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES-CBC</td>
</tr>
<tr>
<td>RC2-CBC</td>
</tr>
<tr>
<td>DES-EDE-CBC</td>
</tr>
<tr>
<td>DES-EDE3-CBC</td>
</tr>
<tr>
<td>DESX-CBC</td>
</tr>
<tr>
<td>BF-CBC</td>
</tr>
<tr>
<td>RC2-40-CBC</td>
</tr>
<tr>
<td>CAST5-CBC</td>
</tr>
<tr>
<td>RC2-64-CBC</td>
</tr>
<tr>
<td>AES-128-CBC</td>
</tr>
<tr>
<td>AES-192-CBC</td>
</tr>
<tr>
<td>AES-256-CBC</td>
</tr>
<tr>
<td>SEED-CBC</td>
</tr>
</tbody>
</table>

### Use LZO Compression

Enable/Disable LZO compression on the VPN link. Lempel–Ziv–Oberhumer (LZO) is a lossless data compression algorithm.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable / Disable</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.6.4 Network > GRE

GRE Configuration

The BulletPlus supports GRE (Generic Routing Encapsulation) Tunneling which can encapsulate a wide variety of network layer protocols not supported by traditional VPN. This allows IP packets to travel from one side of a GRE tunnel to the other without being parsed or treated like IP packets.

Each GRE tunnel must have a unique name. Up to 10 GRE tunnels are supported by the BulletPlus.

Name
Values (Chars(32))
gre

Enable
Values (selection)
Disable / Enable
4.0 Configuration

<table>
<thead>
<tr>
<th>Multicast</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable / Disable Multicast support over the GRE tunnel.</td>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TTL</th>
<th>Values (value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the TTL (Time-to-live) value for packets traveling through the GRE tunnel.</td>
<td>1 - 255</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a key is required, key must be the same for each end of the GRE tunnel.</td>
<td>(none)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ARP</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable / Disable ARP (Address Resolution Protocol) support over the GRE tunnel.</td>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

**Local Setup**

The local setup refers to the local side of the GRE tunnel, as opposed to the remote end.

<table>
<thead>
<tr>
<th>Gateway IP Address</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the WAN IP Address of the BulletPlus, this field should be populated with the current WAN IP address.</td>
<td>(varies)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel IP Address</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the IP Address of the local tunnel.</td>
<td>(varies)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Netmask</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the subnet mask of the local tunnel IP address.</td>
<td>(varies)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subnet IP Address</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the subnet address for the local network.</td>
<td>(varies)</td>
</tr>
</tbody>
</table>
4.0 Configuration

<table>
<thead>
<tr>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>The subnet mask for the local network/subnet.</td>
</tr>
</tbody>
</table>

**Remote Setup**

The remote setup tells the BulletPlus about the remote end, the IP address to create the tunnel to, and the subnet that is accessible on the remote side of the tunnel.

<table>
<thead>
<tr>
<th>Gateway IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the WAN IP Address of the BulletPlus or other GRE supported device in which a tunnel is to be created with at the remote end.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subnet IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>The is the IP Address of the remote network, on the remote side of the GRE Tunnel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>The is the subnet mask for the remote network/subnet.</td>
</tr>
</tbody>
</table>

**IPsec Setup**

Refer to the IPsec setup in the VPN Site to Site section of the manual for more information.
4.0 Configuration

4.6.5 VPN > VPN Users

For VPN L2TP & OpenVPN operation, users will be required to provide a username and password. Use the VPN Users menu to set up the required users.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>Gateway To Gateway</td>
<td>L2TP Client</td>
<td>OpenVPN</td>
<td>GRE</td>
<td>VPN Users</td>
<td>Certificates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**VPN Users**

**New L2TP user name/password**

- L2TP Username
- L2TP New Password [5-64 characters, no space]
- L2TP Confirm New Password

**New OpenVPN user name/password**

- OpenVPN Username
- OpenVPN New Password [5-64 characters, no space]
- OpenVPN Confirm New Password

**Username**

Enter a username for the user being set up.

*Values (characters)*

(no default)

**New Password**

Enter a password for the use.

*Values (characters)*

(no default)

**Confirm New Password**

Enter the password again, the BulletPlus will ensure that the password match.

*Values (IP Address)*

(no default)
4.0 Configuration

4.6.6 VPN > Certificate Management

When using the VPN features of the BulletPlus, it is possible to select X.509 for the Authentication Type. If that is the case, the BulletPlus must use the required x.509 certificates in order to establish a secure tunnel between other devices. Certificate Management allows the user a place to manage these certificates.

![Certificate Management Interface](Image 4-6-7: VPN > Certificate Management)
4.0 Configuration

4.7 Router

4.7.1 Router > RIPv2

The BulletPlus is capable of providing and participating in RIPv2 (Routing Information Protocol v2), to exchange routing information from attached devices. Static routes can also be added in the Network > Routes menu.

![RIPv2 Configuration](image)

**RIPv2 Status**

Enable or disable RIPv2 routing on the BulletPlus. If enabled the BulletPlus will exchange routing information on the specified (interfaces) attached networks.

**Values (selection)**

- Enable
- Disable

**Authentication Type / Port / Password**

Enable MD5 authentication on for the RIPv2 protocol. Also select the port used for RIPv2, and the required password.

**Values (selection)**

- None
- MD5

**RIPv2 Network Announcement Configuration**

Each attached network that is to participate with the RIPv2 exchange must be specified here. Once added they participating networks are shown in the list.

**Values (Subnet/Length)**

(no default)
4.0 Configuration

4.7.2 Router > OSPF

The BulletPlus is also capable of providing and participating in OSPF (Open Shortest Path First), to exchange routing information from attached devices. Static routes can also be added in the Network > Routes menu.

**Router Configuration**

**OSPF Status**

Enable or disable OSPF routing on the BulletPlus. If enabled the BulletPlus will exchange routing information on the specified (interfaces) attached networks.

**OSPF Network Announcement Configuration**

Each attached network that is to participate with the OSPF exchange must be specified here. Once added they participating networks are shown in the list.
4.0 Configuration

4.8 Serial

4.8.1 Serial > Status

The Serial > Status menu presents a summary of the RS232 Serial Data Port located on the side of the BulletPlus, the port uses a standard DB-9 connector. If USB-to-Serial converters are connected they will also appear as new tabs listed as USB devices. At this time the BulletPlus only supports select devices using generic FTDI or Prolific USB-to-Serial drivers.

The Summary window shows a number of status items that aid in viewing the operation, statistics, and troubleshooting of the RS232 or USB Serial Port.

**General Status**
- Port - Lists available RS232 or USB (Serial) ports available.
- Port Status - Shows if the port has been enabled in the configuration.
- Baud Rate - The current baud rate used to interface with the connected device.
- Connect As - The type of IP Protocol Config is displayed here (TCP, UDP, SMTP, PPP, etc)
- Connect Status - Shows if there are any current connections / if the port is active.
- Receive Bytes - Displays the total bytes received by the modem in the current session.
- Receive Packets - Displays the total packets received in the current session.
- Transmit Bytes - Displays the total bytes transmitted by the modem in the current session.
- Transmit Packets - Displays the total packets transmitted in the current session.
4.0 Configuration

4.8.2 Serial > Settings

This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the BulletPlus network on another BulletPlus serial port. The fully-featured RS232 interface supports hardware handshaking.

The BulletPlus is equipped with 2 Serial Communication Modes as described below:

- **Data** - The primary RS232 data port for end devices. This port supports full handshaking.
- **Console** - The default mode for this port is to be configured as a console port and is used for diagnostics and configuration using an AT Command set. (115200/8/N/1)

**USB**

The BulletPlus supports the use of USB-to-Serial converters and new tabs for the USB configuration will appear once a converter has been connected to the USB port of the BulletPlus. At this time only specific generic FTDI and Prolific drivers are supported.

Although the BulletPlus can be connected to a USB hub and multiple USB ports can be utilized as additional serial ports, this is not practical as each time a device is connected (or the BulletPlus is restarted) it is assigned a port number and there is currently not a dependable way to ensure this port will be the same each time.

The USB ports support basic TCP/UDP serial port settings are discussed for the RS232 serial port.

![Image 4-8-2: Serial > Settings Configuration](image-url)
4.0 Configuration

Port Status
Select operational status of the Serial Port. The port is disabled by default.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled / Enable</td>
</tr>
</tbody>
</table>

Data Baud Rate
The serial baud rate is the rate at which the modem is to communicate with the attached local asynchronous device.

<table>
<thead>
<tr>
<th>Values (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>921600 9600</td>
</tr>
<tr>
<td>460800 7200</td>
</tr>
<tr>
<td>230400 4800</td>
</tr>
<tr>
<td>115200 3600</td>
</tr>
<tr>
<td>57600 2400</td>
</tr>
<tr>
<td>38400 1200</td>
</tr>
<tr>
<td>28800 600</td>
</tr>
<tr>
<td>19200 300</td>
</tr>
<tr>
<td>14400</td>
</tr>
</tbody>
</table>

Data Format
This setting determines the format of the data on the serial port. The default is 8 data bits, No parity, and 1 Stop bit.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8N1 / 8E1 / 8O1</td>
</tr>
</tbody>
</table>

Flow Control
Flow control may be used to enhance the reliability of serial data communications, particularly at higher baud rates. If the attached device does not support hardware handshaking, leave this setting at the default value of 'None'. When CTS Framing is selected, the BulletPlus uses the CTS signal to gate the output data on the serial port.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
</tr>
<tr>
<td>Hardware</td>
</tr>
<tr>
<td>CTS Framing</td>
</tr>
</tbody>
</table>

Software flow control (XON/XOFF) is not supported.

Pre-Data Delay
Refer to Drawing 4A above.

<table>
<thead>
<tr>
<th>Values (time (ms) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
</tr>
</tbody>
</table>

Post-Data Delay
Refer to Drawing 4A above.

<table>
<thead>
<tr>
<th>Values (time (ms) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
</tr>
</tbody>
</table>
4.0 Configuration

**Data Mode**

This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the BulletPlus.

When set to Seamless, the serial port server will add a gap between data frames to comply with the MODBUS protocol for example. See 'Character Timeout' below for related information.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seamless / Transparent</td>
</tr>
</tbody>
</table>

**Character Timeout**

In Seamless mode (see Data Mode described on the preceding page), this setting determines when the serial server will consider the recently received incoming data as being ready to transmit. As per the MODBUS standard, frames will be marked as 'bad' if the time gap between frames is greater than 1.5 characters, but less than the Character Timeout value.

The serial server also uses this parameter to determine the time gap inserted between frames. It is measured in 'characters' and related to baud rate.

Example: If the baud rate is 9600bps, it takes approximately 1ms to move one character. With the Character Timeout set to 4, the timeout period is 4ms. When the calculated time is less than 3.5ms, the serial server will set the character timeout to a minimum value of 3.5ms.

If the baud rate is greater than 19200bps, the minimum character timeout is internally set to 750us (microseconds).

<table>
<thead>
<tr>
<th>Values (characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
</tr>
</tbody>
</table>

**Maximum Packet Size**

Defines the buffer size that the serial server will use to receive data from the serial port. When the server detects that the Character Timeout criteria has been met, or the buffer is full, it packetizes the received frame and transmits it.

<table>
<thead>
<tr>
<th>Values (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
</tr>
</tbody>
</table>

**No-Connection Data**

When enabled the data will continue to buffer received on the serial data port when the radio loses synchronization. When disabled the BulletPlus will disregard any data received on the serial data port when radio synchronization is lost.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

**MODBUS TCP Status**

This option will enable or disable the MODBUS decoding and encoding features.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>

**MODBUS TCP Protection Key**

MODBUS encryption key used for the MODBUS TCP Protection Status feature.

<table>
<thead>
<tr>
<th>Values (string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1234</td>
</tr>
</tbody>
</table>
4.0 Configuration

This setting determines which protocol the serial server will use to transmit serial port data over the BulletPlus network.

The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the RS232 Configuration Menu.

<table>
<thead>
<tr>
<th>IP Protocol Config</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Client</td>
<td>TCP Client</td>
</tr>
<tr>
<td>TCP Server</td>
<td>TCP Server</td>
</tr>
<tr>
<td>TCP Client/Server</td>
<td>TCP Client/Server</td>
</tr>
<tr>
<td>UDP Point-to-Point</td>
<td>SMTP Client</td>
</tr>
<tr>
<td></td>
<td>PPP</td>
</tr>
<tr>
<td></td>
<td>GPS Transparent Mode</td>
</tr>
</tbody>
</table>

**TCP Client:** When TCP Client is selected and data is received on its serial port, the BulletPlus takes the initiative to find and connect to a remote TCP server. The TCP session is terminated by this same unit when the data exchange session is completed and the connection timeout has expired. If a TCP connection cannot be established, the serial port data is discarded.

- **Remote Server Address**
  - IP address of a TCP server which is ready to accept serial port data through a TCP connection. For example, this server may reside on a LAN network server.
  - Default: 0.0.0.0

- **Remote Server Port**
  - A TCP port which the remote server listens to, awaiting a session connection request from the TCP Client. Once the session is established, the serial port data is communicated from the Client to the Server.
  - Default: 20001

- **Outgoing Connection Timeout**
  - This parameter determines when the BulletPlus will terminate the TCP connection if the connection is in an idle state (i.e. no data traffic on the serial port).
  - Default: 60 (seconds)

**TCP Server:** In this mode, the BulletPlus Series will not INITIATE a session, rather, it will wait for a Client to request a session of it (it's being the Server—it 'serves' a Client). The unit will 'listen' on a specific TCP port. If a session is established, data will flow from the Client to the Server, and, if present, from the Server to the Client. If a session is not established, both Client-side serial data, and Server-side serial data, if present, will be discarded.

- **Local Listening Port**
  - The TCP port which the Server listens to. It allows a TCP connection to be created by a TCP Client to carry serial port data.
  - Default: 20001

- **Incoming Connection Timeout**
  - Established when the TCP Server will terminate the TCP connection is the connection is in an idle state.
  - Default: 300 (seconds)
4.0 Configuration

TCP Client/Server: In this mode, the BulletPlus will be a combined TCP Client and Server, meaning that it can both initiate and serve TCP connection (session) requests. Refer to the TCP Client and TCP Server descriptions and settings described previously as all information, combined, is applicable to this mode.

UDP Point-to-Point: In this configuration the BulletPlus will send serial data to a specifically-defined point, using UDP packets. This same BulletPlus will accept UDP packets from that same point.

- Remote IP Address
  IP address of distant device to which UDP packets are sent when data received at serial port.
  Default: 0.0.0.0

- Remote Port
  UDP port of distant device mentioned above.
  Default: 20001

- Listening Port
  UDP port which the IP Series listens to (monitors). UDP packets received on this port are forwarded to the unit’s serial port.
  Default: 20001

SMTP Client: If the BulletPlus has Internet access, this protocol may be used to send the data received on the serial port (COM1), in a selectable format (see Transfer Mode (below)), to an e-mail addressee. Both the SMTP Server and the e-mail addressee must be ‘reachable’ for his feature to function.

- Mail Subject
  Enter a suitable ‘e-mail subject’ (e-mail heading).
  Default: COM1 Message

- Mail Server (IP/Name)
  IP address or ‘Name’ of SMTP (Mail) Server.
  Default: 0.0.0.0

- Mail Recipient
  A valid e-mail address for the intended addressee, entered in the proper format.
  Default: host@

- Message Max Size
  Maximum size for the e-mail message.
  Default: 1024

- Timeout (s)
  How long the unit will wait to gather data from the serial port before sending an e-mail message; data will be sent immediately upon reaching Message Max Size.
  Default: 10

- Transfer Mode
  Select how the data received on COM1 is to be sent to the email addressee. Options are: Text, Attached File, Hex Code.
  Default: Text

A UDP or TCP port is an application end-point. The IP address identifies the device and, as an extension of the IP address, the port essentially ‘fine tunes’ where the data is to go ‘within the device’.

Be careful to select a port number that is not predetermined to be associated with another application type, e.g. HTTP uses port 80.

Multicast is a one-to-many transmission of data over an IP network. It is an efficient method of transmitting the same data to many recipients. The recipients must me members of the specific multicast group.

TTL: Time to Live is the number of hops a packet can travel before being discarded.

In the context of multicast, a TTL value of 1 restricts the range of the packet to the same subnet.
4.0 Configuration

PPP: COM1 can be configured as a PPP server for a serial connection with a PC or other device. The attached PC could then use a dedicated serial (WindowsXP - dialup/modem) type PPP connection to access the network resources of the BulletPlus. Note: Console (if configured as data port) does not support this mode.

- **PPP Mode**
  Can be set for Active or Passive. If set for Active, the PPP server will initiate the PPP connection with a PPP client. The server will periodically send out link requests following PPP protocol. If set to Passive, the PPP server will not initiate the PPP connection with the PPP client. The server will wait passively for the client to initiate connection.
  Default: Passive

- **Expected String**
  When a client (PC or device) initiates a PPP session with the modem, this is the handshaking string that is expected in order to allow a connection. Generally this does not need to be changed.
  Default: CLIENT

- **Response String**
  This is the handshaking string that will be sent by the modem once the expected string is received. Generally this does not need to be changed.
  Default: CLIENTSERVER

- **PPP LCP Echo Failure Number**
  The PPP server will presume the peer to be dead if the LCP echo-requests are sent without receiving a valid LCP echo-reply. If this happens, PPP server will terminate the connection. Use of this option requires a non-zero value for the LCP Echo Interval parameter. This option can be used to enable PPP server to terminate after the physical connection has been broken (e.g., the modem has hung up).
  Default: 0

- **PPP LCP Echo Interval**
  The PPP server will send an LCP echo-request frame to the peer every ‘n’ seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the LCP-echo-failure option to detect that the peer is no longer connected.
  Default: 0

- **PPP Local IP**
  Enter the local PPP IP Address, the IP Address of the IPn4G COM0 Port.
  Default: 192.168.0.1

- **PPP Host IP**
  Enter the PPP Host IP here. This is the IP of the PC or attached device.
  Default: 192.168.0.99

- **PPP Idle Timeout(s)**
  It is the timeout for tearing down the ppp connection when there is no data traffic within the time interval. When there is data coming, new ppp connection will be created.
  Default: 30

SMTP: Simple Mail Transport Protocol is a protocol used to transfer mail across an IP network.
**4.0 Configuration**

**IP Protocol Config (Continued...)**

**GPS Transparent Mode:** When in GPS Transparent Mode, GPS data is reported out the serial port at 1 second intervals. Sample output is shown below:

```plaintext
$GPGGA,000001,4116.053,N,08003.135,E,0000000000,0000000000,0000000000,0000000000
$GPRMC,000001,4116.053,N,08003.135,E,0000000000,0000000000,0000000000,0000000000
$GPGSV,1.1,000001,0000000000,0000000000
$GPGSV,1.1,000001,0000000000,0000000000
```

*Image 4-8-3: Serial > GPS Transparent Mode*
4.0 Configuration

4.9 I/O

4.9.1 I/O > Settings

The BulletPlus has 8 programmable I/O’s, which can be used with various alarms and sensors for monitoring, telling the modem when certain events have occurred, such as an intrusion alarm on a door, etc. Any of the I/O’s can also be programmed to operate as an output, that can be used to drive external relays to remotely control equipment and devices. The I/O pins are available on the back connector shared with the input power (1&2).

The Status of the I/O’s can be read, and in the case of outputs, can be operated in the WebUI. Alerts can be setup to send SMS Messages if I/O Status changes, as well, SMS control messages can be sent to the device to trigger events. SNMP and/or Modbus can be used to poll for the status, or set controls. See the appropriate sections of the manual for more information.

![Image 4-9-1: I/O Settings]

**Settings**

The Settings menu is used to configure a I/O as either a Input or an Output. If configured as an output, the user can also set the output as open or closed. The output pin on the BulletPlus can be used to provide output signals, which can be used to drive an external relay to control an external device. See Table 4-9-1 for I/O specifications.

**Status**

The Status section will display the current state and measured voltage (Meter) of any I/O’s configured as inputs. The WebUI will also display the current state of each control output.
4.0 Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Parameter</th>
<th>Min.</th>
<th>Typ.</th>
<th>Max</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O 1 - 2 (Input)</td>
<td>Input low state voltage range</td>
<td>VIL</td>
<td>-0.5</td>
<td>0</td>
<td>1.2</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Input high state voltage range</td>
<td>VIH</td>
<td>1.5</td>
<td>3.3</td>
<td>30</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Input leakage current (3.3 VDC IN)</td>
<td>IIN</td>
<td>—</td>
<td>58</td>
<td>—</td>
<td>µA</td>
</tr>
<tr>
<td></td>
<td>Typical application input source is a dry switch</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>contact to ground. Pin includes an internal 56KΩ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>resistor pull up to 3.3 VDC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O 1 - 2 (Output)</td>
<td>Open drain drive to ground</td>
<td>Idc</td>
<td>—</td>
<td>100</td>
<td>110</td>
<td>mA</td>
</tr>
<tr>
<td></td>
<td>Maximum open circuit voltage applied</td>
<td>Voc</td>
<td>—</td>
<td>3.3</td>
<td>30</td>
<td>V</td>
</tr>
<tr>
<td></td>
<td>Typical application is to drive a relay coil to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ground.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4-9-1: Digital I/O Specifications
4.0 Configuration

4.10 GPS

4.10.1 GPS > Location

Location Map

The location map shows the location on the BulletPlus. The unit will attempt to get the GPS coordinates from the built in GPS receiver, and if unsuccessful, will use the Cell ID location reported by the Cellular Carrier.

The maps can be viewed with either Bing or Google maps by using the option located at the bottom, right hand corner near the refresh option.

If the unit had a GPS signal (GPS Module enabled and antenna attached), it will report the specific GPS coordinates of the modem, otherwise only the estimated coordinates reported by the Carrier.
4.0 Configuration

4.10.2 GPS > Settings

The BulletPlus can be polled for GPS data via GPSD standards and/or provide customizable reporting to up to 4 different hosts using UDP or Email Reporting. GPS is an optional feature of the BulletPlus, and must be specified at the time of order and factory prepared. If the screen below are not available on your unit, you do not have a GPS enabled model.

Image 4-10-2: GPS > Settings

**GPS Status**
Enable or disable the GPS polling function of the BulletPlus.

Values
- Disable
- Enable

**GPS Source**
The BulletPlus contains an standalone GPS module built into the unit. To use the GPS features of the BulletPlus an antenna must be connected to the GPS Antenna Port.

Values
- Standalone GPS
- Cellular Module GPS

**TCP Port**
Specify the TCP port on the BulletPlus where the GPS service is running and remote systems can connect and poll for GPSD data.

Values
- 2947

**GPS Online Assistance**
When enabled the BulletPlus will use the internet to download a file at bootup with information about its location to assist in quickly connecting to GPS satellites. This service does consume a small amount of data.

Values
- Enable
4.0 Configuration

4.10.3 GPS > Report

The BulletPlus can provide customizable reporting to up to 4 hosts using UDP or Email Reporting.

<table>
<thead>
<tr>
<th>Report No.1</th>
<th>Report No.2</th>
<th>Report No.3</th>
<th>Report No.4</th>
</tr>
</thead>
</table>

**Report Define**

- Enable UDP and/or Email or disable GPS Reporting. Up to 4 reports can be set up and configured independently.

**Values (selection)**
- Disable
- UDP Report
- Email Report

**Time Interval**

- The interval timer specifies the frequency at which the GPS data is reported in seconds.

**Values (seconds)**

- 600
# 4.0 Configuration

## Message 1-4

The Message field allows customization of up to 4 different GPS messages to be sent to the specified host.

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>None</th>
<th>ALL NMEA</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Message is not used, no data will be sent</td>
<td>ALL NMEA</td>
</tr>
<tr>
<td>ALL</td>
<td>Sends all of the below</td>
<td>GGA</td>
</tr>
<tr>
<td>GGA</td>
<td>GPS Fix Data</td>
<td>GSA</td>
</tr>
<tr>
<td>GSA</td>
<td>Overall Satellite Data</td>
<td>GSV</td>
</tr>
<tr>
<td>GSV</td>
<td>Detailed Satellite Data</td>
<td>RMC</td>
</tr>
<tr>
<td>RMC</td>
<td>Recommended Min Data for GPS</td>
<td>VTG</td>
</tr>
<tr>
<td>VTG</td>
<td>Vector Track &amp; Ground Speed</td>
<td>Latitude/Longitude</td>
</tr>
<tr>
<td>GPSGate</td>
<td>For use with GPSGate Tracking Software</td>
<td>GPSGate UDP Protocol</td>
</tr>
</tbody>
</table>

## Trigger Set

The trigger condition defines the conditions that must be met before a GPS update is reported. If OR is chosen, the Repeater Timer OR the Distance trigger conditions must be met before an update is sent. The AND condition requires that both the Repeat timer AND the Distance trigger conditions be met before an update is sent.

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>Only Timer</th>
<th>Timer OR Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only Timer</td>
<td>Only Timer</td>
<td>Timer OR Distance</td>
</tr>
<tr>
<td>Timer AND Distance</td>
<td>Timer AND Distance</td>
<td>Timer OR Distance</td>
</tr>
<tr>
<td>Timer OR Distance</td>
<td>Timer AND Distance</td>
<td>Timer OR Distance</td>
</tr>
</tbody>
</table>

## Distance Set

The distance parameter allows the GPS data to only be sent when a specified distance has been traveled since the last report.

<table>
<thead>
<tr>
<th>Values (meters)</th>
<th>1000</th>
</tr>
</thead>
</table>

## UDP Remote IP / Port

This is the IP Address and port of the remote host in which the UDP packets are to be sent.

<table>
<thead>
<tr>
<th>Values (Address/Port)</th>
<th>0.0.0.0 / 20175</th>
</tr>
</thead>
</table>

## Mail Subject

If an Email report is chosen, the subject line of the Email can be defined here.

<table>
<thead>
<tr>
<th>Values (characters)</th>
<th>1000</th>
</tr>
</thead>
</table>

## Mail Server

If an Email report is to be sent, the outgoing mail server must be defined, and the port number.

<table>
<thead>
<tr>
<th>Values (Address:port)</th>
<th>smtp.gmail.com:465</th>
</tr>
</thead>
</table>

## Username / Password

Some outgoing mail servers required username and password to prevent an account being used for spam. Enter the login credentials here.

<table>
<thead>
<tr>
<th>Values (characters)</th>
<th>Username / password</th>
</tr>
</thead>
</table>

## Mail Recipient

Some outgoing mail servers require a username and password to prevent an account being used for spam. Enter the login credentials here.

<table>
<thead>
<tr>
<th>Values (characters)</th>
<th><a href="mailto:host@email.com">host@email.com</a></th>
</tr>
</thead>
</table>
4.0 Configuration

4.10.4 GPS > GpsGate

The BulletPlus is compatible with GpsGate - GPS Tracking Software, which is a 3rd party mapping solution used for various GPS services including vehicle and asset tracking. The BulletPlus can communicate with GpsGate via Tracker Mode and TCP/IP. (UDP reporting can also send information to GpsGate, see the GPS > Report - UDP Reports)

---

**GpsGate - Tracker Mode**

Enable GpsGate Tracker Mode or TCP modes. In tracker mode, the BulletPlus and GpsGate software will communicate via TCP/IP, however, if a connection is not available, it will attempt to use SMS messaging.

**Mode Set**

Enable Tracker Mode, TCP and SMS, or only TCP.

**Server Command Channel**

By default, BulletPlus and GpsGate will use TCP and SMS to ensure communication between each other. It is also possible to specify TCP or SMS communication only. Initial setup in Tracker mode must be via SMS.

**TCP Alive Mode / Alive Time Interval**

TCP alive mode will keep TCP connection alive if the tracker is not enabled or the tracker interval is too long. The default is 150 seconds.
4.0 Configuration

**Setup Phone Filter**
A phone number filter can be applied to prevent SMS commands not intended for the BulletPlus from being processed.

**Values (selection)**
- Disable: Accept All
- Enable Filter

**Motion Trigger**
Use this parameter to enable or disable the motion trigger in the BulletPlus.

**Values (selection)**
- Disable
- Enable Motion Trigger

**Send IO Status**
When enabled, the BulletPlus will send the current status of the Digital I/O inputs and/or outputs to the GpsGate Server.

**Values (selection)**
- Disable
- Send Input Status
- Send Output Status
- Send Input&Output Status

**When GPS Invalid, Sending Data**
Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.

**Values (selection)**
- Not Use Last Valid Position
- Use Last Valid Position

**GpsGate - TCP Mode**

![GpsGate TrackerOne Connection](Image 4-10-5: GPS > GpsGate TCP Mode)
4.0 Configuration

<table>
<thead>
<tr>
<th><strong>Mode Set</strong></th>
<th><strong>Values (selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable GpsGate Tracker Mode or TCP modes. In TCP Mode the BulletPlus will establish a connection with the GpsGate Server directly without the SMS setup process. If the TCP connection is not available, the BulletPlus will continue to try to connect every few seconds.</td>
<td>Disable, Enable Tracker Mode, Enable TCP Send Mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Server Address / IP</strong></th>
<th><strong>Values (IP Address)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the IP Address of the server running the GpsGate application.</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Server Port</strong></th>
<th><strong>Values (Port)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the TCP Port of the server running the GpsGate application.</td>
<td>30175</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Server Interval</strong></th>
<th><strong>Values (seconds)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the interval at which the BulletPlus will send data to the GpsGate Server.</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Motion Distance</strong></th>
<th><strong>Values (meters)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the motion threshold in which the BulletPlus will be triggered to send location data.</td>
<td>100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Send IO Status</strong></th>
<th><strong>Values (selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>When enabled, the BulletPlus will send the current status of the Digital I/O inputs and/or outputs to the GpsGate Server.</td>
<td>Disable, Send Input Status, Send Output Status, Send Input&amp;Output Status</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>When GPS Invalid, Sending Data</strong></th>
<th><strong>Values (selection)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.</td>
<td>Not Use Last Valid Position, Use Last Valid Position</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.10.5 GPS > Recorder

The BulletPlus can be configured to record events based on time intervals, and/or an event trigger and store them in non-volatile memory. These events can then be viewed within the WebUI, on a map, or sent to a remote server in a number of different formats.

| GPS Recorder Service
| Current GPS Information

- Satellites in View: 15
- Satellites tracked: 10
- Latitude: 51.142662, N
- Longitude: -114.075331, W
- Altitude: 1130.2
- Speed: 0 (km/h)
- Orientation: N (Degrees to North)
- NMEA UTC Time: 26/03/2014 21:26:59

| GPS Recorder Setting
| Status

- Record Feature Selections: [Enable GPS Recorder]
- Time Interval: 300 [30-65535]s
- DI/DO Changed: Record
- Over Speed: [120] [Min 30] (km/h)
- Orientation Changed: [5-180] (180 Disable)
- Carrier RSSI Level: Record
- Altitude: Record

Use the Status parameter to enable the GPS recording functionality of the BulletPlus. The total number of records that can be recorded varies between 16,000 and 36,000, depending on the number of GPS parameters that are recorded.

Values (selection)

- Disable
- Enable GPS Recorder

Time Interval

Values (seconds)

- 300

DI/DO Changed

Values (selection)

- Record
- Don't Record

The BulletPlus can detect and report the current GPS info when a digital input or output status changes, regardless of the time interval setting.
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Speed</strong></td>
<td>Select Record to include the current speed in the reported data.</td>
</tr>
<tr>
<td><strong>Values (selection)</strong></td>
<td>Record / Don't Record</td>
</tr>
<tr>
<td><strong>Over Speed</strong></td>
<td>Trigger a GPS record entry when the speed has exceeded the configured threshold. A minimum of 30 Km/hr is required.</td>
</tr>
<tr>
<td><strong>Values (Km/hr)</strong></td>
<td>120</td>
</tr>
<tr>
<td><strong>Orientation</strong></td>
<td>Select Record to record the current orientation when a GPS entry is recorded. (Degree to North).</td>
</tr>
<tr>
<td><strong>Values (selection)</strong></td>
<td>Record / Don't Record</td>
</tr>
<tr>
<td><strong>Orientation Changed</strong></td>
<td>Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)</td>
</tr>
<tr>
<td><strong>Values (5 ~ 180)</strong></td>
<td>60</td>
</tr>
<tr>
<td><strong>Carrier RSSI Level</strong></td>
<td>Select Record to record the current 3G/Cellular RSSI level when a GPS entry is recorded. (-dB).</td>
</tr>
<tr>
<td><strong>Values (selection)</strong></td>
<td>Record / Don't Record</td>
</tr>
<tr>
<td><strong>Altitude</strong></td>
<td>Select Record to record the current Altitude when a GPS entry is recorded (meters).</td>
</tr>
<tr>
<td><strong>Values (selection)</strong></td>
<td>Record / Don't Record</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.10.6 GPS > Load Record

Data that has been recorded and saved by the BulletPlus can then be viewed or sent to a remote server in various formats. The data recorded can also be viewed directly by selecting “View Data” and the data can be traced on a map (internet access required), by selecting “Trace Map”, or “Quick Trace”. The screenshots below show the raw data that can be viewed and the Trace Map/Quick Trace output.
4.0 Configuration

<table>
<thead>
<tr>
<th>Record Time Range</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the boxes next to the records listed above that are to be sent to the server.</td>
<td>(no default)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Send Mode / Protocol</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the data format / protocol type for the data to be sent.</td>
<td>NMEA via UDP, NMEA via TCP, GpsGate via UDP, GpsGate via TCP, Plain Text via UDP, Plain Text via TCP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Address/IP</th>
<th>Values (IP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the address or IP address of the remote server to which the data is to be sent.</td>
<td>nms.microhardcorp.com</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server Port</th>
<th>Values (Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the UDP/TCP port number of the remote server to which the data is to be sent.</td>
<td>30175</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.10.7 GPS > TAIP

The BulletPlus has the ability to send GPS data in TAIP (Trimble ASCII Interface Protocol) format to up to 4 different TAIP servers. The following section describes the configuration parameters required to initialize TAIP reporting.

<table>
<thead>
<tr>
<th>TAIP Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings No.1</td>
</tr>
<tr>
<td>TAIP service status</td>
</tr>
<tr>
<td>Remote TAIP Server</td>
</tr>
<tr>
<td>Socket Type</td>
</tr>
<tr>
<td>Remote TAIP Port</td>
</tr>
<tr>
<td>Message Type</td>
</tr>
<tr>
<td>Interval</td>
</tr>
<tr>
<td>Vehicle ID</td>
</tr>
<tr>
<td>Settings No.2</td>
</tr>
<tr>
<td>TAIP service status</td>
</tr>
<tr>
<td>Settings No.3</td>
</tr>
<tr>
<td>TAIP service status</td>
</tr>
<tr>
<td>Settings No.4</td>
</tr>
<tr>
<td>TAIP service status</td>
</tr>
</tbody>
</table>

TAIP service status
Enable or disable TAIP service on the modem. The unit can report TAIP to up to 4 different hosts.

Remote TAIP Server
Enter the IP Address of the Remote TAIP Server.

Socket Type
Select the socket type that is used by the Remote TAIP server. Select TCP or UDP, this will define how the connection (TCP) or data is sent (UDP) to the server.

Remote TAIP Port
Enter the TCP or UDP port number used on the Remote TAIP server.
## 4.0 Configuration

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select between RPV and RLN message types.</td>
<td>RPV / RLN</td>
</tr>
<tr>
<td>RPV - Position/Velocity</td>
<td></td>
</tr>
<tr>
<td>RLN - Long Navigation Message</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interval</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the frequency at which TAIP messages are reported to the remote server. The unit used is seconds, and the default value is 60 seconds.</td>
<td>60</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vehicle ID</th>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the Vehicle ID using 4 alpha-numeric characters.</td>
<td>0000</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.11 Apps

4.11.1 Apps > Modbus

4.11.1.1 Modbus > TCP Modbus

The BulletPlus can be configured to operate as a TCP/IP or Serial (COM) Modbus slave and respond to Modbus requests and report various information as shown in the Data Map.

Status

Disable or enable the Modbus service on the BulletPlus.

Values (selection)

<table>
<thead>
<tr>
<th>Disable Service</th>
<th>Enable Service</th>
</tr>
</thead>
</table>

TCP Mode Status

Disable or enable the Modbus TCP Connection Service on the BulletPlus.

Values (selection)

<table>
<thead>
<tr>
<th>Disable</th>
<th>Enable</th>
</tr>
</thead>
</table>
### 4.0 Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td><strong>Values (Port #)</strong></td>
</tr>
<tr>
<td>Specify the Port in which the Modbus TCP service is to listen and respond to polls.</td>
<td>502</td>
</tr>
<tr>
<td><strong>Active Timeout(s)</strong></td>
<td><strong>Values (seconds)</strong></td>
</tr>
<tr>
<td>Define the active timeout in seconds.</td>
<td>30</td>
</tr>
<tr>
<td><strong>Slave ID</strong></td>
<td><strong>Values (value)</strong></td>
</tr>
<tr>
<td>Each Modbus slave device must have a unique address, or Slave ID. Enter this value here as required by the Modbus Host System.</td>
<td>1</td>
</tr>
<tr>
<td><strong>Coils Address Offset</strong></td>
<td><strong>Values (value)</strong></td>
</tr>
<tr>
<td>Enter the Coils Address offset as required by the Master.</td>
<td>0</td>
</tr>
<tr>
<td><strong>Input Address Offset</strong></td>
<td><strong>Values (value)</strong></td>
</tr>
<tr>
<td>Enter the Input Address offset as required by the Master.</td>
<td>0</td>
</tr>
<tr>
<td><strong>Register Address Offset</strong></td>
<td><strong>Values (value)</strong></td>
</tr>
<tr>
<td>Enter the Register Address offset as required by the Master.</td>
<td>0</td>
</tr>
<tr>
<td><strong>Master IP Filter Set</strong></td>
<td><strong>Values (selection)</strong></td>
</tr>
<tr>
<td>It is possible to only accept connections from specific Modbus Master IP’s, to use this feature enable the Master IP Filter and specify the IP Addresses in the fields provided.</td>
<td>Disable / Enable</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.11.2 Modbus > COM (Serial) Modbus

The BulletPlus can also participate in serial based Modbus, to configure and view the serial Modbus settings, the COM1 port must first be disabled in the Comport > Settings menu. Only the settings that are different from TCP Modbus will be discussed.

![Image 4-11-2: Apps > Modbus Serial Configuration]

**COM Mode Status**

Disable to select the Serial (COM) mode for the Modbus service. In RTU mode, communication is in binary format and in ASCII mode, communication is in ASCII format.

<table>
<thead>
<tr>
<th>Values (selection)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable</td>
<td></td>
</tr>
<tr>
<td>Enable COM ASCII Mode</td>
<td></td>
</tr>
<tr>
<td>Enable COM RTU Mode</td>
<td></td>
</tr>
</tbody>
</table>

**Baud Rate**

The serial baud rate is the rate at which the modem is to communicate with the attached local serial device.

<table>
<thead>
<tr>
<th>Values (selection (bps))</th>
</tr>
</thead>
<tbody>
<tr>
<td>921600</td>
</tr>
<tr>
<td>57600</td>
</tr>
<tr>
<td>14400</td>
</tr>
<tr>
<td>3600</td>
</tr>
<tr>
<td>460800</td>
</tr>
<tr>
<td>38400</td>
</tr>
<tr>
<td><strong>9600</strong></td>
</tr>
<tr>
<td>2400</td>
</tr>
<tr>
<td>230400</td>
</tr>
<tr>
<td>28800</td>
</tr>
<tr>
<td>7200</td>
</tr>
<tr>
<td>1200</td>
</tr>
<tr>
<td>115200</td>
</tr>
<tr>
<td>19200</td>
</tr>
<tr>
<td>4800</td>
</tr>
<tr>
<td>600</td>
</tr>
</tbody>
</table>

**Data Format**

This setting determines the format of the data on the serial port. The default is 8 data bits, No parity, and 1 Stop bit.

<table>
<thead>
<tr>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8N1</td>
</tr>
<tr>
<td>8E1</td>
</tr>
<tr>
<td>8O1</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.10.1.3 Modbus > Modbus Data Map

**Modbus Data Map**

**Supported Function Codes:**
- 1: Read Coils
- 2: Read Inputs
- 3: Read Registers
- 5: Write Single Coil
- 6: Write Single Register

**Data Address = Offset + Basic Address**

**Coil Bits (Output if config) and Internal Status:**

<table>
<thead>
<tr>
<th>Bit Address</th>
<th>Hex Format</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x0000</td>
<td>OUTPUT 1</td>
</tr>
<tr>
<td>1</td>
<td>0x0001</td>
<td>OUTPUT 2</td>
</tr>
<tr>
<td>9</td>
<td>0x0009</td>
<td>Serial Status</td>
</tr>
<tr>
<td>12</td>
<td>0x000c</td>
<td>LAN/eth0 Status(Read)</td>
</tr>
<tr>
<td>13</td>
<td>0x000d</td>
<td>WAN/eth1 Status(Read)</td>
</tr>
<tr>
<td>16</td>
<td>0x0010</td>
<td>Carrier Status</td>
</tr>
<tr>
<td>18</td>
<td>0x0012</td>
<td>Wifi Status</td>
</tr>
<tr>
<td>22</td>
<td>0x0016</td>
<td>GPS Status</td>
</tr>
<tr>
<td>23</td>
<td>0x0017</td>
<td>Location Over Network</td>
</tr>
<tr>
<td>24</td>
<td>0x0018</td>
<td>Event UDP Report 1</td>
</tr>
<tr>
<td>25</td>
<td>0x0019</td>
<td>Event UDP Report 2</td>
</tr>
<tr>
<td>26</td>
<td>0x001a</td>
<td>Event UDP Report 3</td>
</tr>
<tr>
<td>27</td>
<td>0x001b</td>
<td>NMS Report</td>
</tr>
<tr>
<td>28</td>
<td>0x001c</td>
<td>Web Client Service</td>
</tr>
<tr>
<td>32</td>
<td>0x0020</td>
<td>Carrier Connection(Read)</td>
</tr>
<tr>
<td>40</td>
<td>0x0028</td>
<td>SYSTEM Reboot</td>
</tr>
</tbody>
</table>

**Input Bits (if config):**

<table>
<thead>
<tr>
<th>Bit Address</th>
<th>Hex Format</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x0000</td>
<td>INPUT 1</td>
</tr>
<tr>
<td>1</td>
<td>0x0001</td>
<td>INPUT 2</td>
</tr>
</tbody>
</table>

**Registers:**

<table>
<thead>
<tr>
<th>Address</th>
<th>Hex Format</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x0000</td>
<td>Modern Model Type...</td>
</tr>
<tr>
<td>1</td>
<td>0x0001</td>
<td>Build Version</td>
</tr>
<tr>
<td>2</td>
<td>0x0002</td>
<td>Modern ID Highest 2 Bytes</td>
</tr>
<tr>
<td>3</td>
<td>0x0003</td>
<td>Modern ID Higher 2 Bytes</td>
</tr>
<tr>
<td>4</td>
<td>0x0004</td>
<td>Modern ID Lower 2 Bytes</td>
</tr>
<tr>
<td>5</td>
<td>0x0005</td>
<td>Modern ID Lowest 2 Bytes</td>
</tr>
<tr>
<td>6</td>
<td>0x0006</td>
<td>RSSI(dbm)</td>
</tr>
<tr>
<td>7</td>
<td>0x0007</td>
<td>VDC(V100K)</td>
</tr>
<tr>
<td>8</td>
<td>0x0008</td>
<td>Core Temperature (C)</td>
</tr>
<tr>
<td>9</td>
<td>0x0009</td>
<td>Carrier Received Bytes(MB)</td>
</tr>
<tr>
<td>10</td>
<td>0x000a</td>
<td>Carrier Transmitted Bytes(MB)</td>
</tr>
<tr>
<td>11</td>
<td>0x000b</td>
<td>GPS Altitude (m)</td>
</tr>
<tr>
<td>12</td>
<td>0x000c</td>
<td>GPS Latitude High 2 Bytes</td>
</tr>
<tr>
<td>13</td>
<td>0x000d</td>
<td>Latitude Low 2 Bytes(x1000000)</td>
</tr>
<tr>
<td>14</td>
<td>0x000e</td>
<td>GPS Longitude High 2 Bytes</td>
</tr>
<tr>
<td>15</td>
<td>0x000f</td>
<td>Longitude Low 2 Bytes(x1000000)</td>
</tr>
<tr>
<td>16</td>
<td>0x0012</td>
<td>Serial Baud Rate(100)(bps)</td>
</tr>
<tr>
<td>19</td>
<td>0x0013</td>
<td>Serial Data Format...</td>
</tr>
</tbody>
</table>

**Calculation:**

Real Latitude = (signed integer)(High 2 Bytes + Low 2 Bytes) / 1

**Modern Model Types:**

<table>
<thead>
<tr>
<th>Type ID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>6</td>
<td>IPin3G</td>
</tr>
<tr>
<td>7</td>
<td>VIP4G</td>
</tr>
<tr>
<td>8</td>
<td>IPin4C</td>
</tr>
<tr>
<td>9</td>
<td>IPin3Gii</td>
</tr>
<tr>
<td>10</td>
<td>IPin4Gii</td>
</tr>
<tr>
<td>11</td>
<td>PWi/BulletPlus</td>
</tr>
</tbody>
</table>

**Com Data Format Definition:**

<table>
<thead>
<tr>
<th>Type ID</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown</td>
</tr>
<tr>
<td>1</td>
<td>8N1</td>
</tr>
<tr>
<td>2</td>
<td>8N2</td>
</tr>
<tr>
<td>3</td>
<td>8E1</td>
</tr>
<tr>
<td>4</td>
<td>8O1</td>
</tr>
<tr>
<td>5</td>
<td>7N1</td>
</tr>
<tr>
<td>6</td>
<td>7N2</td>
</tr>
<tr>
<td>7</td>
<td>7E1</td>
</tr>
<tr>
<td>8</td>
<td>7O1</td>
</tr>
<tr>
<td>9</td>
<td>7E2</td>
</tr>
<tr>
<td>10</td>
<td>7O2</td>
</tr>
</tbody>
</table>

Image 4-11-3: Applications > Modbus Data Map
4.11.2 Apps > Netflow Report

The BulletPlus can be configured to send Netflow reports to up to 3 remote systems. Netflow is a tool that collects and reports IP traffic information, allowing a user to analyze network traffic on a per interface basis to identify bandwidth issues and to understand data needs. Standard Netflow Filters can be applied to narrow down results and target specific data requirements.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>ModBus</td>
<td>Netflow Report</td>
<td>LocalMonitor</td>
<td>Event Report</td>
<td>Websocket</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Netflow Report**

- **Report Configuration No.1**
  - **Status**: Enable / Disable Netflow Reporting.
  - **Source Address**: 0.0.0.0 Default 0.0.0.0
  - **Interface**: ALL
  - **Remote IP**: 0.0.0.0
  - **Remote Port**: 2055 [0 ~ 65535]
  - **Filter expression**: V6

- **Report Configuration No.2**
  - **Status**: Disable

- **Report Configuration No.3**
  - **Status**: Disable

**Image 4-11-4: Apps > Netflow Report**

**Status**

Enable / Disable Netflow Reporting.

**Values (selection)**

- **Disable** / **Enable**

**Source Address**

The Source Address is the IP Address, of which data is to be collected and analyzed. The default of 0.0.0.0 will collect and report information about all addresses connected to the interface selected below.

**Values (IP Address)**

- 0.0.0.0

**Interface**

Select between LAN, WAN and Carrier interfaces, or capture data from all interfaces.

**Values (selection)**

- LAN / WAN / Carrier / ALL
4.0 Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Remote Port</td>
<td>0</td>
</tr>
<tr>
<td>Filter expression</td>
<td>(no default)</td>
</tr>
</tbody>
</table>

- Remote IP: The Remote IP is the IP Address of the NetFlow collector where the flow reports are be sent.
- Remote Port: Enter the Remote Port number.
- Filter expression: Filter expression selects which packets will be captured. If no expression is given, all packets will be captured. Otherwise, only packets for which expression is "true" will be captured. Example: tcp&&port 80

The "tcpdump" manual, available on the internet provides detailed expression syntax.
4.0 Configuration

4.11.3 Apps > Local Monitor

The Local Device Monitor allows the BulletPlus to monitor a local device connected locally to the Ethernet port or to the locally attached network. If the BulletPlus cannot detect the specified IP or a DHCP assigned IP, the unit will restart the DHCP service, and eventually restart the modem to attempt to recover the connection.

**Image 4-11-5: Apps > Local Monitor**

- **Status**
  
  Enable or disable the local device monitoring service.

- **IP Mode**
  
  Select the IP mode. By selecting a fixed IP address the service will monitor the connection to that specific IP. If auto detect is selected, the BulletPlus will detect and monitor DHCP assigned IP address.

- **Local IP Setting**
  
  This field is only shown if Fixed Local IP is selected for the IP Mode. Enter the static IP to be monitored in this field.

- **Status Timeout**
  
  The status timeout is the maximum time the BulletPlus will wait to detect the monitored device. At this time the BulletPlus will restart the DHCP service. (5-65535 seconds)

- **Waiting DHCP Timeout**
  
  This field defines the amount of time the BulletPlus will wait to detect the monitored device before it will reboot the modem. (30-65535 seconds)
4.0 Configuration

4.11.4 Applications > Event Report

4.11.4.1 Event Report > Configuration

Event Reporting allows the BulletPlus to send periodic updates via UDP packets. These packets are customizable and can be sent to up to 3 different hosts, and at a programmable interval. The event packet can report information about the modem such as the hardware/software versions, core temperature, supply voltage, etc; carrier info such as signal strength (RSSI), phone number, RF Band; or about the WAN such as if the assigned IP Address changes. All events are reported in binary.

This box allows the selection of the type of event to be reported. The default is disabled. If Modem_event is selected, additional options appear to the right and allow for customization of the event reported via Messages. If Management is selected, additional check boxes appear below to select the interfaces to report to the Microhard NMS system.

Enter the IP Address of a reachable host to send the UDP packets

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem_Event</td>
<td></td>
</tr>
<tr>
<td>SDP_Event</td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote IP Values (IP Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
</table>
4.0 Configuration

<table>
<thead>
<tr>
<th>Remote Port</th>
<th>Values (Port #)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the UDP port number of the Remote IP Address.</td>
<td>20200</td>
</tr>
</tbody>
</table>

*Default Port Numbers for Microhard NMS (20100 for modem events, 20200 for Management)*

<table>
<thead>
<tr>
<th>Interval Time(s)</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the interval time in seconds, that the BulletPlus will send the configured UDP message to the Remote IP and Port specified.</td>
<td>600</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Message Info Type</th>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>When Modem_Event is selected, up to three different payloads can be selected.</td>
<td>Modem, Carrier, WAN</td>
</tr>
</tbody>
</table>

4.11.4.2 Event Report > Message Structure

**Modem_event message structure**

- fixed header (fixed size 20 bytes)
- Modem ID (uint64_t (8 bytes))
- Message type mask (uint8_t(1 byte))
- reserved
- packet length (uint16_t(2 bytes))

Note: packet length = length of fixed header + length of message payload.

**Message type mask**

- **Modem info** - 2 bits
  00 no
  01 yes (0x1)
- **Carrier info** - 2 bits
  00 no
  01 yes (0x4)
- **WAN info** - 2 bits
  00 no
  01 yes (0x10)

**sdp_event message structure**

- spd_cmd (1 byte(0x01))
- content length (1 byte)
- spd_package - same as spd response inquiry package format
4.0  Configuration

4.11.4.3 Event Report > Message Payload

Modem info:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type/Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content length</td>
<td>2 BYTES (UINT16_T)</td>
</tr>
<tr>
<td>Modem name</td>
<td>STRING (1-30 bytes)</td>
</tr>
<tr>
<td>Hardware version</td>
<td>STRING (1-30 bytes)</td>
</tr>
<tr>
<td>Software version</td>
<td>STRING (1-30 bytes)</td>
</tr>
<tr>
<td>Core temperature</td>
<td>STRING (1-30 bytes)</td>
</tr>
<tr>
<td>Supply voltage</td>
<td>STRING (1-30 bytes)</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>4 BYTES (UINT32_T)</td>
</tr>
<tr>
<td>Local IP Mask</td>
<td>4 BYTES (UINT32_T)</td>
</tr>
</tbody>
</table>

Carrier info:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type/Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content length</td>
<td>2 BYTES (UINT16_T)</td>
</tr>
<tr>
<td>RSSI</td>
<td>1 BYTE (UINT8_T)</td>
</tr>
<tr>
<td>RF Band</td>
<td>2 BYTES (UINT16_T)</td>
</tr>
<tr>
<td>3G_Network</td>
<td>STRING (1-30 Bytes)</td>
</tr>
<tr>
<td>Service type</td>
<td>STRING (1-30 Bytes)</td>
</tr>
<tr>
<td>Channel number</td>
<td>STRING (1-30 Bytes)</td>
</tr>
<tr>
<td>SIM card number</td>
<td>STRING (1-30 Bytes)</td>
</tr>
<tr>
<td>Phone number</td>
<td>STRING (1-30 Bytes)</td>
</tr>
</tbody>
</table>

WAN Info:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type/Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content length</td>
<td>2 BYTES (UINT16_T)</td>
</tr>
<tr>
<td>IP address</td>
<td>4 BYTES (UINT32_T)</td>
</tr>
<tr>
<td>DNS1</td>
<td>4 BYTES (UINT32_T)</td>
</tr>
<tr>
<td>DNS2</td>
<td>4 BYTES (UINT32_T)</td>
</tr>
</tbody>
</table>

Message Order:

Messages will be ordered by message type number.

For example,

If message type mask = 0x15, the eurd package will be equipped by header+modem information+carrier information+wanip information.

If message type mask = 0x4, the eurd package will be equipped by header+carrier information.

If message type mask = 0x11, the eurd package will be equipped by header+modem information+wanip information.

A fixed message tail:

- content length --- 2 BYTES(UINT16_T)
- product name --- STRING(1—64 bytes)
- image name --- STRING(1—64 bytes)
- domain name --- STRING(1—64 bytes)
- domain password --- STRING(32 bytes) // MD5 encryption
- module list --- 5 BYTES // radio, ethernet, carrier, usb, com
4.0 Configuration

4.11.5 Applications > Websocket

The Websocket service is a feature of HTML5.0 or later. Web Socket is designed to be implemented in web browsers and web servers to allow XML scripts to access the HTML web service with a TCP socket connection.

It is mainly used for two purposes:
- refreshing page information without refreshing the entire page to reduce network stream.
- to integrate internet applications with xml to get required information in real time.

Currently we provide four types of information as configured:
- GPS Coordinate Information
- GPS NMEA Data
- Carrier Information
- Comport Data

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modbus</td>
<td>Netflow Report</td>
<td>LocalMonitor</td>
<td>Event Report</td>
<td>Websocket</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web Socket Service**

**Online Connected Data**
Browser Type: Chrome 46 Windows

**Setting**

<table>
<thead>
<tr>
<th>Status</th>
<th>Values (selection)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Socket Port (default: 7681)</td>
<td>7681 [100-65535]</td>
</tr>
<tr>
<td>Data Fresh Interval (seconds)</td>
<td>10 [2-65535]</td>
</tr>
<tr>
<td>Connect Password</td>
<td>Blank for Disable</td>
</tr>
<tr>
<td>Max Keep Time (minutes)</td>
<td>90 [0-keep alive]</td>
</tr>
<tr>
<td>GPS Coordinate</td>
<td>Disable/Enable</td>
</tr>
<tr>
<td>GPS NMEA Data</td>
<td>Disable/Enable</td>
</tr>
<tr>
<td>Carrier Information</td>
<td>Disable/Enable</td>
</tr>
<tr>
<td>Comport Data</td>
<td>Disabled (Please enable comport tcp server.)</td>
</tr>
</tbody>
</table>

*Image 4-11-7: Applications > Web Socket Service*

**Status**
Enable or disable the web socket service in the modem.

**Values (selection)**
Enable / Disable

**Web Socket Port**
Enter the desired web socket TCP port number. The default is 7681, and the valid range is 100 to 65535.

**Values (TCP port)**
7681
# 4.0 Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Fresh Intervals</strong></td>
<td>Enter in the time at which data is to be refreshed. The default is 10 seconds, the valid range is 2 to 65535 seconds.</td>
<td>Values (seconds)</td>
</tr>
<tr>
<td><strong>Connect Password</strong></td>
<td>For added security a password can be required to connect to the web socket service. To disable, leave this field blank. The default is disabled.</td>
<td>Values</td>
</tr>
<tr>
<td><strong>Max Keep Time</strong></td>
<td>This field determines how long the web socket is open once started/ enabled. The default is 60 mins, a value of zero means the service will continue to run indefinitely.</td>
<td>Values (minutes)</td>
</tr>
<tr>
<td><strong>GPS Coordinate</strong></td>
<td>If enabled the modem will report GPS coordinate data to the websocket.</td>
<td>Values (selection)</td>
</tr>
<tr>
<td><strong>GPS NMEA Data</strong></td>
<td>If enabled the modem will report GPS NMEA data to the websocket.</td>
<td>Values (selection)</td>
</tr>
<tr>
<td><strong>Carrier Information</strong></td>
<td>If enabled the modem will report carrier information to the websocket.</td>
<td>Values (selection)</td>
</tr>
<tr>
<td><strong>Comport Data</strong></td>
<td>If enabled, and the RS232 port is configured for TCP Server, the comport data will be reported to the web socket.</td>
<td>Values (selection)</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.12 Diag

4.12.1 Network Tools Ping

The Network Tools Ping feature provides a tool to test network connectivity from within the unit. A user can use the Ping command by entering the IP address or host name of a destination device in the Ping Host Name field, use Count for the number of ping messages to send, and the Packet Size to modify the size of the packets sent.

4.12.2 Network Tools Traceroute

The Traceroute feature can be used to provide connectivity data by providing information about the number of hops, routers and the path taken to reach a particular destination.
4.0 Configuration

4.12.3 Iperf

The BulletPlus features an integrated Iperf server/client to use to measure and analyze throughput of TCP/UDP packets to and/or from the BulletPlus. Iperf is a 3rd party utility that can be loaded on any PC to measure network performance. For additional information about Iperf, please visit the Iperf website.

The BulletPlus can be configured to operate as a Server, listening for an incoming connection from another device (with Iperf), or PC running an Iperf client. If set to Iperf client, the BulletPlus will connect to or send packets to a specified Iperf server.

<table>
<thead>
<tr>
<th>Throughput Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iperf Configuration</td>
</tr>
<tr>
<td>Iperf Mode</td>
</tr>
<tr>
<td>Server Status</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>TCP Window Size</td>
</tr>
<tr>
<td>TCP Maximum Segment Size</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Iperf Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iperf Mode</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Remote Server IP Address</td>
</tr>
<tr>
<td>Duration(seconds)</td>
</tr>
<tr>
<td>TCP Window Size</td>
</tr>
<tr>
<td>TCP Maximum Segment Size</td>
</tr>
<tr>
<td>Report Format</td>
</tr>
</tbody>
</table>

Iperf Mode

Select between an Iperf Server (listens for incoming connections) and client (initiates a connection with a server)

Server / Client

Server Status

If the Iperf mode to set to Server, this Server Status allows a user to Enable or Disable the server.

Enable / Disable

Protocol

Select the type of packets to be sent to test the throughput. TCP packets are connection oriented and require additional overhead for the handshaking that occurs, while UDP is a connectionless, best effort oriented protocol.

TCP / UDP
## 4.0 Configuration

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Window Size</td>
<td><strong>Set the TCP Window size for the Iperf Client/Server. The recommended default is 85.3K, which can be set by entering 0.</strong></td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>TCP Maximum Segment Size</td>
<td><strong>Set the TCP Max Segment Size for the Iperf Client/Server. Set to 0 for recommended settings.</strong></td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>Remote Server Address</td>
<td><strong>When in Client mode, select the Iperf Server by entering its IP Address here.</strong></td>
</tr>
<tr>
<td></td>
<td>192.168.168.100</td>
</tr>
<tr>
<td>Duration</td>
<td><strong>When in Client mode, select the duration of the test (in seconds). The default is 5.</strong></td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Report Format</td>
<td><strong>Select the format to display the bandwidth numbers in. Supported formats are:</strong></td>
</tr>
<tr>
<td></td>
<td>'Kbits' = Kbits/sec</td>
</tr>
<tr>
<td></td>
<td>'Kbytes' = KBytes/sec</td>
</tr>
<tr>
<td></td>
<td>'Mbits' = Mbits/sec</td>
</tr>
<tr>
<td></td>
<td>'Mbytes' = MBytes/sec</td>
</tr>
<tr>
<td></td>
<td>Kbits</td>
</tr>
<tr>
<td></td>
<td>Mbits</td>
</tr>
<tr>
<td></td>
<td>Kbytes</td>
</tr>
<tr>
<td></td>
<td>Mbytes</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.13 Admin

4.13.1 Admin > Users

Password Change

The Password Change menu allows the password of the user ‘admin’ to be changed. The ‘admin’ username cannot be deleted, but additional users can be defined and deleted as required as seen in the Users menu below.

Enter a new password for the ‘admin’ user. It must be at least 5 characters in length. The default password for ‘admin’ is ‘admin’.

The exact password must be entered to confirm the password change, if there is a mistake all changes will be discarded.
4.0 Configuration

Add Users

Different users can be set up with customized access to the WebUI. Each menu or tab of the WebUI can be disabled on a per user basis as seen below.

![Image 4-13-2: Access Control > Users]

**Username**

Enter the desired username. Minimum or 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted.

**Values (characters)**

(no default)

Min 5 characters

Max 32 characters

**Password / Confirm Password**

Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.

**Values (characters)**

(no default)

Min 5 characters

**User Type**

Users can be specified as a “End User”, in this case only limited access to the modem (summary and wifi SSID/password).

**Values (check box)**

unchecked
4.0 Configuration

4.13.2 Admin > Authentication

There are two methods whereby a user may be authenticated for access to the BulletPlus:

- **Local**

  Using the Admin or Upgrade access and associated passwords - the authentication is done 'locally' within the BulletPlus, and

- **RADIUS&Local**

  RADIUS authentication (using a specific user name and password supplied by your RADIUS Server Administrator) - this authentication would be done 'remotely' by a RADIUS Server; if this authentication fails, proceed with Local authentication as per above.

---

**RADIUS:** Remote Authentication Dial In User Service. An authentication, authorization, and accounting protocol which may be used in network access applications.

A RADIUS server is used to verifying that information is correct.

---

<table>
<thead>
<tr>
<th>Authentication Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Server</strong></td>
</tr>
<tr>
<td><strong>Remote Server IP Address</strong></td>
</tr>
<tr>
<td><strong>Remote Server IP Port</strong></td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
</tr>
</tbody>
</table>

**Image 4-13-3: Authentication Configuration**

---

**Authentication Server**

Select the Authentication Mode: Local (default) or Local&RADIUS. For the latter selection, RADIUS authentication must be attempted FIRST; if unsuccessful, THEN Local authentication may be attempted.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
</tr>
<tr>
<td>Local&amp;RADIUS</td>
</tr>
</tbody>
</table>

**Remote Server IP Address**

In this field, the IP address of the RADIUS server is to be entered if RADIUS&Local has been selected as the Authorization Mode.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid RADIUS server IP address</td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**RADIUS Secret**

If the Authorization Mode has been set to RADIUS&Local, obtain the RADIUS Secret for his particular client from your RADIUS Server Administrator and enter it into this field.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>nosecret</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.13.3 Admin > NMS Settings

The Microhard NMS is a no cost server based monitoring and management service offered by Microhard Systems Inc. Using NMS you can monitor online/offline units, retrieve usage data, perform backups and centralized upgrades, etc. The following section describes how to get started with NMS and how to configure the BulletPlus to report to NMS.

To get started with NMS, browse to the Microhard NMS website, nms.microhardcorp.com, click on the register button in the top right corner to register for a Domain (profile), and set up a Domain Administrator Account.

![Image 4-13-4: NMS]
4.0 Configuration

**Domain Name:** A logical management zone for 3G or 4G devices will report to on NMS, the logged data is separated from any other users that are using NMS. The Domain Name is required in every 3G or 4G device for it to report to right zone. Under this user domain, one can create and manage sub-domain. The sub-domain can only be created by the domain administrator, NOT by the NMS subscription page.

**Domain Password:** This password is used to prevent misuse of the domain. This needs to be entered into each 3G or 4G device for it to report to right zone.

**Email Address:** The email address entered here will be the login username. During the registration stage, a confirmation email will be sent by the NMS system for verification and confirmation to activate your account.

Once confirmed, this account will be the administrator of the domain. The administrator can manage sub-domain and user accounts that belong to this domain.

Once NMS has been configured, each BulletPlus must be configured to report into NMS.

![Image 4-13-5: NMS Settings](image-url)
# 4.0 Configuration

## Network Management System (NMS) Configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default Settings</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default Settings link will reset the configuration form to the default factory values. The form still needs to be submitted before any changes will occur.</td>
</tr>
<tr>
<td><strong>NMS Server/IP</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The default server address for NMS is nms.microhardcorp.com. The NMS can also be hosted privately, and if that is the case, enter the address here.</td>
</tr>
<tr>
<td><strong>Values (IP/Name)</strong></td>
<td>nms.microhardcorp.com</td>
</tr>
<tr>
<td><strong>Domain Name / Password</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is the domain name and password that was registered on the NMS website, it must be entered to enable reporting to the NMS system.</td>
</tr>
<tr>
<td><strong>Values (chars)</strong></td>
<td>default</td>
</tr>
<tr>
<td><strong>NMS Report Setting</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Carrier Location</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable or Disable location estimation via carrier connection. When enabled, the BulletPlus will consume some data to retrieve location information from the internet.</td>
</tr>
<tr>
<td><strong>Values (chars)</strong></td>
<td>Disable/Enable</td>
</tr>
<tr>
<td><strong>Report Status</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable or Disable UDP reporting of data to the NMS system.</td>
</tr>
<tr>
<td><strong>Values (chars)</strong></td>
<td>Enable NMS Report Disable NMS Report</td>
</tr>
<tr>
<td><strong>Remote Port</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is the port to which the UDP packets are sent, and the NMS system is listening on. Ensure this matches what is configured on NMS. The default is 20200.</td>
</tr>
<tr>
<td><strong>Values (UDP Port#)</strong></td>
<td>20200</td>
</tr>
<tr>
<td><strong>Interval(s)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Interval defines how often data is reported to NMS. The more often data is reported, the more data is used, so this should be set according to a user’s data plan. (0 to 65535 seconds)</td>
</tr>
<tr>
<td><strong>Values (seconds)</strong></td>
<td>300</td>
</tr>
</tbody>
</table>
### 4.0 Configuration

#### Information Selection

The BulletPlus can report information about the different interfaces it has. By default, the BulletPlus is set to send information about the Carrier, such as usage and RSSI. Statistical and usage data on the Radio (WiFi), Ethernet, and Serial interfaces can also be reported.

The more that is reported, the more data is sent to the NMS system, be aware of data plan constraints and related costs.

<table>
<thead>
<tr>
<th>Values (check boxes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
</tr>
<tr>
<td>Carrier</td>
</tr>
<tr>
<td>Radio</td>
</tr>
<tr>
<td>COM</td>
</tr>
<tr>
<td>DI / DO</td>
</tr>
</tbody>
</table>

#### Webclient Setting

The Web Service can be enabled or disabled. This service is used to remotely control the BulletPlus. It can be used to schedule reboots, firmware upgrade and backup tasks, etc.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable/Enable</td>
</tr>
</tbody>
</table>

#### Server Type

Select between HTTPS (secure), or HTTP server type.

<table>
<thead>
<tr>
<th>Values (chars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS/HTTP</td>
</tr>
</tbody>
</table>

#### Server Port

This is the port where the service is installed and listening. This port should be open on any installed firewalls.

<table>
<thead>
<tr>
<th>Values (Port#)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9998</td>
</tr>
</tbody>
</table>

#### Username / Password

This is the username and password used to authenticate the unit.

<table>
<thead>
<tr>
<th>Values (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/admin</td>
</tr>
</tbody>
</table>

#### Interval

The Interval defines how often the BulletPlus checks with the NMS System to determine if there are any tasks to be completed. Carrier data will be consumed every time the device probes the NMS system.

<table>
<thead>
<tr>
<th>Values (min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
</tr>
</tbody>
</table>
4.0 Configuration

4.13.4 Admin > SNMP

The BulletPlus may be configured to operate as a Simple Network Management Protocol (SNMP) agent. Network management is most important in larger networks, so as to be able to manage resources and measure performance. SNMP may be used in several ways:

- configure remote devices
- monitor network performance
- detect faults
- audit network usage
- detect authentication failures

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the BulletPlus. Communications is in the form of queries (information requested by the management system) or traps (information initiated at, and provided by, the SNMP agent in response to predefined events).

Objects specific to the BulletPlus are hosted under private enterprise number 21703.

An object is a variable in the device and is defined by a Management Information Database (MIB). Both the management system and the device have a copy of the MIB. The MIB in the management system provides for identification and processing of the information sent by a device (either responses to queries or device-sourced traps). The MIB in the device relates subroutine addresses to objects in order to read data from, or write data to, variables in the device.

An SNMPv1 agent accepts commands to retrieve an object, retrieve the next object, set an object to a specified value, send a value in response to a received command, and send a value in response to an event (trap).

SNMPv2c adds to the above the ability to retrieve a large number of objects in response to a single request.

SNMPv3 adds strong security features including encryption; a shared password key is utilized. Secure device monitoring over the Internet is possible. In addition to the commands noted as supported above, there is a command to synchronize with a remote management station.

The pages that follow describe the different fields required to set up SNMP on the BulletPlus. MIBS may be requested from Microhard Systems Inc.

The MIB file can be downloaded directly from the unit using the ‘Get MIB File’ button on the Network > SNMP menu.
4.0 Configuration

## SNMP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Agent Status</td>
<td>Enable ▼</td>
</tr>
<tr>
<td>Read Only Community Name</td>
<td>public</td>
</tr>
<tr>
<td>Read Write Community Name</td>
<td>private</td>
</tr>
<tr>
<td>Listening Port</td>
<td>161</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>Version 3 ▼</td>
</tr>
<tr>
<td>V3 User Name</td>
<td>UserV3</td>
</tr>
<tr>
<td>V3 User Read Write Limit</td>
<td>Read Only ▼</td>
</tr>
<tr>
<td>V3 User Authentication Level</td>
<td>NoAuthNoPriv ▼</td>
</tr>
<tr>
<td>SNMP Trap Settings</td>
<td></td>
</tr>
<tr>
<td>SNMP Trap Status</td>
<td>Enable ▼</td>
</tr>
<tr>
<td>Trap Community Name</td>
<td>TrapUser</td>
</tr>
<tr>
<td>Trap Manage Host IP</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Auth Failure Traps</td>
<td>Disable ▼</td>
</tr>
</tbody>
</table>

**Download MIB File**

### SNMP Operation Mode

- **Values (selection)**
  - Disable / V1&V2c&V3

### Read Only Community Name

- **Values (string)**
  - public

### Read Only Community Name

- **Values (string)**
  - private

### SNMP V3 User Name

- **Values (string)**
  - V3user

---

If disabled, an SNMP service is not provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2c, & v3.

Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ priority.

Also a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ/WRITE priority.
4.0 Configuration

### V3 User Read Write Limit

Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.

**Values (selection)**
- Read Only
- Read Write

### V3 User Authentication Level

Defines SNMPv3 user's authentication level:
- NoAuthNoPriv: No authentication, no encryption.
- AuthNoPriv: Authentication, no encryption.
- AuthPriv: Authentication, encryption.

**Values (selection)**
- NoAuthNoPriv
- AuthNoPriv
- AuthPriv

### V3 User Authentication Password

SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv.

**Values (string)**
- 00000000

### V3 User Privacy Password

SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).

**Values (string)**
- 00000000

### SNMP Trap Version

Select which version of trap will be sent should a failure or alarm condition occur.

**Values (string)**
- V1 Traps
- V2 Traps
- V3 Traps
- V1&V2 Traps
- V1&V2&V3 Traps

### Auth Failure Traps

If enabled, an authentication failure trap will be generated upon authentication failure.

**Values (selection)**
- Disable
- Enable

### Trap Community Name

The community name which may receive traps.

**Values (string)**
- TrapUser

### Trap Manage Host IP

Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address).

**Values (IP Address)**
- 0.0.0.0
4.0 Configuration

4.13.5 Admin > Discovery

Microhard Radio employ a discovery service that can be used to detect other Microhard Radio’s on a network. This can be done using a stand alone utility from Microhard System’s called ‘IP Discovery’ or from the Admin > Discovery menu. The discovery service will report the MAC Address, IP Address, Description, Product Name, Firmware Version, Operating Mode, and the SSID.

Use this option to disable or enable the discovery service.

Values (selection)

Disable / Discoverable / Changable

Specify the port running the discovery service on the BulletPlus unit.

Values (Port #)

20077
4.0 Configuration

4.13.6 System > Logout

The logout function allows a user to end the current configuration session and prompt for a login screen.

![Image 4-13-9: System > logout]
5.0 AT Command Line Interface

5.1 AT Command Overview

AT Commands can be issued to configure and manage the BulletPlus, via the back serial port (Console), or by TCP/IP (telnet).

5.1.1 Serial Port

To connect and access the AT Command interface on the BulletPlus, a physical connection must be made on the Console (TX/RX) serial port on the back of the BulletPlus. A terminal emulation program (Hyperterminal, Tera Term, ProComm, Putty etc) can then be used to communicate with the BulletPlus. The port settings of this port can be modified by changing the settings of the Console Port, in the Serial Port Settings window.

Image 5-1: Console Port Settings

Default Settings:
- Baud rate: 115200
- Data bits: 8
- Parity: None
- Stop Bits: 1
- Flow Control: None

Once communication is established, a login is required to access the AT Command interface, once logged in, the AT Command Line Interface menu is displayed. Type “?” or Help to list the menu commands.

Image 5-2: AT Command Window

Default Settings:
- BulletPlus login: admin
- Password: admin
5.0 AT Command Line Interface

5.1.2 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the BulletPlus. The default port is TCP Port 23. A telnet session can be made to the unit using any Telnet application (Windows Telnet, Tera Term, ProComm etc). Once communication is established, a login is required to continue.

A session can be made to the WAN IP Address (if allowed in the firewall settings) for remote configuration, or to the local RJ45 interface.

Once a session is established a login is required to continue. As seen in the Serial port setup, the default login is admin, and the password is admin. Once verified, the AT Command Line Interface menu is shown and AT Commands can now be issued. (Type “?” or Help to list the commands).

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1
5.0 AT Command Line Interface

5.2 AT Command Syntax

The following syntax is used when issuing AT Commands on the BulletPlus:

- All commands start with the AT characters and end with the <Enter> key.
- Microhard Specific Commands start with +M.
- Help will list top level commands (ATL will list ALL available AT Commands).
- To query syntax of a command: AT+<command_name>=?
- Syntax for commands that are used only to query a setting:
  AT<command_name>
- Syntax for commands that can be used to query and set values:
  AT<command_name>=parameter1,parameter2,… (Sets Values)
  AT<command_name>? (Queries the setting)

**Query Syntax:**
AT+MSMNAME=? <Enter>
+MSMNAME: Command Syntax:AT+MLEIP=<modern_name>
OK

**Setting a value:**
AT+MSMNAME=BulletPlus-Test <Enter>
OK

**Query a setting:**
AT+MSMNAME? <Enter>
Host name: BulletPlus-Test
OK

A screen capture of the above commands entered into a unit is shown below:

![Image 5-5: Telnet AT Command Syntax](image)

Once AT commands are entered, they must be saved into the file system to enable the changes.
- AT&W Saves changes.
- ATO or ATA Exits the AT Command Line Interface, if used before AT&W, changes are discarded.
## 5.0 AT Command Line Interface

### 5.3 Supported AT Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT</strong></td>
<td>Echo OK.</td>
<td>AT &lt;enter&gt;</td>
</tr>
<tr>
<td><strong>ATE0</strong></td>
<td>Disables Local Echo.</td>
<td>ATE0 &lt;enter&gt;</td>
</tr>
<tr>
<td><strong>ATE1</strong></td>
<td>Enables Local Echo.</td>
<td>ATE1 &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input:**
- AT <enter>
- ATE0 <enter>
- ATE1 <enter>

**Response:**
- OK
- OK
## 5.0 AT Command Line Interface

### ATH

**Description**
Show a list of previously run commands.

**Command Syntax (Effect: Immediate)**
ATH <enter>

**Example**

**Input:**
ATH <enter>

**Response:**
AT Command history: 1. ATH 2. ATL 3. ATH

### ATL

**Description**
Show a list of all available AT Commands.

**Command Syntax (Effect: Immediate)**
ATL <enter>

**Example**

**Input:**
ATL <enter>

**Response:**
AT Commands available:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT</td>
<td>AT Echo OK</td>
</tr>
<tr>
<td>ATE0</td>
<td>Disable Echo</td>
</tr>
<tr>
<td>ATE1</td>
<td>Enable Echo</td>
</tr>
<tr>
<td>ATH</td>
<td>Show a list of previously run AT commands</td>
</tr>
<tr>
<td>ATL</td>
<td>List all available AT commands</td>
</tr>
<tr>
<td>AT&amp;R</td>
<td>Reserved</td>
</tr>
<tr>
<td>AT&amp;V</td>
<td>Display modem active profile</td>
</tr>
<tr>
<td>AT&amp;W</td>
<td>Enable configurations you have been entered</td>
</tr>
<tr>
<td>ATA</td>
<td>Quit</td>
</tr>
<tr>
<td>ATO</td>
<td>Quit</td>
</tr>
</tbody>
</table>

### AT&R

**Description**
Read modem profile to editable profile. (Reserved)

**Command Syntax (Effect: Immediate)**
AT&R <enter>

**Example**

**Input:**
AT&R <enter>

**Response:**
OK
## 5.0 AT Command Line Interface

### AT&V

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read modem active profile.</td>
<td>AT&amp;V &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;V &lt;enter&gt;</td>
<td>&amp;V: hostname: BulletPlus-Test</td>
</tr>
<tr>
<td></td>
<td>timezone: MST7/MDT, M3.2.0, M11.1.0</td>
</tr>
<tr>
<td></td>
<td>systemmode: gateway</td>
</tr>
<tr>
<td></td>
<td>time mode: local</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
</tbody>
</table>

### AT&W

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable configurations changes that have been entered.</td>
<td>AT&amp;W &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT&amp;W &lt;enter&gt;</td>
<td>Restarting the services to enable the configurations changed recently.....</td>
</tr>
</tbody>
</table>

### ATA / ATO

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quit. Exits AT Command session and returns you to login prompt.</td>
<td>ATA &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA &lt;enter&gt;</td>
<td>OKConnection closed by foreign host</td>
</tr>
</tbody>
</table>
### 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT+MSCNTO</strong></td>
<td>Sets the timeout value for the serial and telnet consoles. Once expired, user will be return to login prompt.</td>
<td><strong>AT+MSCNTO=&lt;Timeout_s&gt;</strong>&lt;br&gt;0 - Disabled&lt;br&gt;0 - 65535 (seconds)</td>
</tr>
</tbody>
</table>

**Example**

Input:
AT+MSCNTO=300 <enter>

Response:
OK

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT+MSPWD</strong></td>
<td>Used to set or change the ADMIN password.</td>
<td><strong>AT+MSPWD=&lt;New password&gt;,&lt;confirm password&gt;</strong>&lt;br&gt;password: at least 5 characters</td>
</tr>
</tbody>
</table>

**Example**

Input:
AT+MSPWD=admin,admin<enter>

Response:
OK

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT+MSGMI</strong></td>
<td>Get Manufacturer Identification</td>
<td><strong>AT+MSGMI=&lt;enter&gt;</strong></td>
</tr>
</tbody>
</table>

**Example**

Input:
AT+MSGMI<enter>

Response:
+MSGMI: 2014-2015 Microhard Systems Inc.<br>OK
## 5.0 AT Command Line Interface

### AT+MSSYSI

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Summary Information</td>
<td>AT+MSSYSI &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input:**
AT+MSSYSI <enter>

**Response:**
Carrier:
- MMIMEI: 356406060882064
- SIMID: 89302610203010832398
- MMIMSI: 302610012606734
- Status: Connected
- Network: Bell
- RSSI: -64
- Temperature: 46

Ethernet Port:
- MAC: 00:0F:92:02:8A:05
- IP: 192.168.168.1
- MASK: 255.255.255.0
- Wan MAC: 00:0F:92:FE:00:01
- Wan IP: 184.151.220.2
- Wan MASK: 255.255.255.255

System:
- Device: BulletPlus-Test
- Product: Bulletplus
- Image: PWii
- Hardware: Rev A
- Software: v1.3.0 build 1009-28

Time: Thu Nov 19 10:17:43 2015

### AT+MSGMR

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Record Information</td>
<td>AT+MSGMR &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input:**
AT+MSGMR <enter>

**Response:**
Hardware Version: Rev A
Software Version: v1.3.0 build 1009-28
System Time: Thu Nov 19 10:19:42 2015
OK
## 5.0 AT Command Line Interface

### AT+MSMNAME

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Name / Radio Description. 30 chars.</td>
<td>AT+MSMNAME=&lt;modem_name&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input: (To set value)**

```
AT+MSMNAME=BulletPlus-Test<enter>
```

**Response:**

```
OK
```

**Input: (To retrieve value)**

```
AT+MSMNAME?<enter>
```

**Response:**

```
Host name:BulletPlus-Test
OK
```

### AT+MSRTF

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the modem to the factory default settings from non-volatile memory.</td>
<td>AT+MSRTF=&lt;Action&gt;</td>
</tr>
</tbody>
</table>

**Action:**

- 0 pre-set action
- 1 confirm action

#### Example

**Input: (To set value)**

```
AT+MSRTF=1<enter>
```

**Response:**

```
OK
```

### AT+MSREB

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot the modem.</td>
<td>AT+MSREB &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input:**

```
AT+MSREB <enter>
```

**Response:**

```
OK. Rebooting...
```
5.0 AT Command Line Interface

### AT+MSNTP

**Description**
Get/Set NTP Server.

**Command Syntax (Effect: AT&W)**

AT+MSNTP=<status>[,.<NTP server>[,.<Port>]]

- **Status:**
  - 0: Local Time
  - 1: NTP

**Example**

**Input:**
AT+MSNTP=1,pool.ntp.org<enter>

**Response:**
OK

### AT+MSSYSLOG

**Description**
Get/Set syslog server

**Command Syntax (Effect: AT&W)**

AT+MSSYSLOG=<Server>[,.<Port>]

- **Server:** Valid IP Address or Name. 0.0.0.0 - Disable. 1 to 256 characters
- **Port:** 1 to 65535. Default is 514

**Example**

**Input:**
AT+MSSYSLOG=192.168.168.35,514<enter>

**Response:**
OK

**Input:**
AT+MSSYSLOG?

**Response:**
Syslog Server : 192.168.168.35
Syslog Port   : 514
OK

### AT+MSSERVICE

**Description**
Get/Set service status and port.

**Command Syntax (Effect: AT&W)**

AT+MSSERVICE[=<Service>[,.<Mode>[,.<Port>]]]

- **Parameters:**
  - **Service:**
    - 0: FTP
    - 1: Telnet
    - 2: SSH
    - 3: Microhard Sh
  - **Mode:**
    - 0: Disable
    - 1: Enable
  - **Port:** 1 to 65535. For Telnet (23 by default) and SSH (22 by default) only

**Example**

**Input:**
AT+MSSERVICE=0,0<enter>

**Response:**
OK
## 5.0 AT Command Line Interface

### AT+MSWEBUI

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set WebUI protocol and port</td>
<td>AT+MSWEBUI[=&lt;Mode&gt;[,&lt;HTTP Port&gt;] [,&lt;HTTPS Port&gt;]]</td>
</tr>
</tbody>
</table>

- **Mode**: 0 - HTTP/HTTPS
- 1 - HTTP
- 2 - HTTPS

- **HTTP Port**: 1 to 65535. 80 by default
- **HTTPS Port**: 1 to 65535. 443 by default

### Example

**Input:**
AT+MSWEBUI=0,80,443<enter>

**Response:**
OK

### AT+MSKA

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set ICMP Keep-alive mode.</td>
<td>AT+MSKA=&lt;Mode&gt;</td>
</tr>
</tbody>
</table>

- **Mode**: 0 - Disable
- 1 - Enable

### Example

**Input:**
AT+MSKA=1<enter>

**Response:**
OK
5.0 AT Command Line Interface

### AT+MSKAS

**Description**

Get/Set IMCP Keep-alive settings.

**Command Syntax (Effect: AT&W)**

```
AT+MSKAS=<host name>,<interval in seconds>,<count>
```

**Example**

**Input:**

```
AT+MSKAS=8.8.8.8,300,20<enter>
```

**Response:**

```
OK
```

**Input:**

```
AT+MSKAS?
```

**Response:**

```
+MSKAS: ICMP status:0 hostname:8.8.8.8 interval:300 count:20 OK
```

### AT+MNLAN

**Description**

Show/Add/Edit/Delete the network interface.

**Command Syntax (Effect: AT&W)**

```
AT+MNLAN=[<LAN Name>[,[<Operation>[,[<Protocol>[,<IP Address>,<Netmask>]]]]]]
```

**LAN Name:** Name of Network LAN interface

**Operation:**

- SHOW - Show the details of an existing LAN interface
- ADD - Add a new LAN interface, followed by the other parameters
- EDIT - Edit an existing LAN interface, followed by the other parameters
- DEL - Delete an existing LAN interface

**Protocol:**

- 0 - DHCP
- 1 - Static IP

**STP:**

- 0 - Spanning Tree Off
- 1 - Spanning Tree On

**IP Address:** Valid IP address

**Netmask:** Valid netmask

**Example**

**Input:**

```
AT+MNLAN?
```

**Response:**

```
1: lan - 192.168.168.1, static (connection type), On (LAN DHCP), off (STP)
OK
```
5.0 AT Command Line Interface

AT+MNLANDHCP

Description
Get/Set LAN DHCP server running on the Ethernet interface.

Command Syntax (Effect: AT&W)

AT+MNLANDHCP=\<LAN Name\>[,\<Mode\>[,\<Start IP\>[,\<Limit\>[,\<Lease Time\>[,\<Alt. Gateway\>[,\<Pre. DNS\>[,\<Alt. DNS\>[,\<WINS/NBNS Servers\>[,\<WINS/NBT Node\>]]]])
LAN Name: Name of Network LAN interface
Mode:  
0 - Disable DHCP Server
1 - Enable DHCP Server
Start IP: The starting address DHCP assignable IP Addresses
Limit: The maximum number of IP addresses. min=0 max=16777214
Lease Time: The DHCP lease time in minutes. min=0 max=214748364
Alt. Gateway: Alternate Gateway for DHCP assigned devices if the default gateway is not to be used
Pre. DNS: Preferred DNS server address to be assigned to DHCP devices
Alt. DNS: Alternate DNS server address to be assigned to DHCP devices
WINS/NBNS Server : WINS/NBNS Servers
WINS/NBT Node : WINS/NBT Node Type
0 - none
1 - b-node
2 - p-node
3 - m-node
4 - h-node

Example
Input:
AT+MNLANDHCP=lan<enter>
Response:
LAN Name : lan
Mode : 1 - DHCP Server enabled
Start IP : 192.168.168.100
Limit : 150
Lease Time : 720m
Alt. Gateway :
Pre. DNS :
Alt. DNS :
WINS/NBNS Server :
WINS/NBT Node : 0 - none
OK
5.0 AT Command Line Interface

### AT+MNLANSTP

**Command Syntax (Effect: AT&W)**

```
AT+MNLANSTP=<LAN Name>[,<STP>]
```

Parameters:
- **LAN Name**: Name of Network LAN interface
- **Spanning Tree**: 0 - Off, 1 - On

**Description**

Get/Set the network LAN interface: Spanning Tree (STP)

**Example**

**Input:**

```
AT+MNLANSTP=lan,0<enter>
```

**Response:**

```
OK
```

### AT+MNLANDNS

**Command Syntax (Effect: AT&W)**

```
AT+MNLANDNS=<LAN Name>[,<Mode>[,<Primary DNS>,<Secondary DNS>]]
```

**Usage:**

```
AT+MNLANDNS=<LAN Name>
AT+MNLANDNS=<LAN Name>,<Mode>
Where <Mode>=0
AT+MNLANDNS=<LAN Name>,<Mode>[,<Primary DNS>,<Secondary DNS>] Where <Mode>=1
```

Parameters:
- **LAN Name**: Name of Network LAN interface
- **Mode**: 0 - Auto, 1 - Manual
- **Primary DNS**: Valid IP Address or 0 (Reset)
- **Secondary DNS**: Valid IP address or 0 (Reset)

**Description**

Get/Set the network LAN interface: DNS

**Example**

**Input:**

```
AT+MNLANDNS=lan,0<enter>
```

**Response:**

```
OK
```
# 5.0 AT Command Line Interface

## AT+MNWAN

### Description

Show/Add/Edit/Delete the network WAN interface.

### Command Syntax (Effect: AT&W)

```
AT+MNWAN[=<Mode>[,<Protocol>[,<IP>,<Netmask>[,<Gateway>]]]]
```

Usage:
- AT+MNWAN
- AT+MNWAN=<Mode>,<Protocol>,<IP>,<Netmask>[,<Gateway>] Where <Mode>=0/2 and <Protocol>=0
- AT+MNWAN=<Mode>,<Protocol> Where <Mode>=0/2 and <Protocol>=1
- AT+MNWAN=<Mode>,<Protocol> Where <Mode>=2 and <Protocol>=2
- AT+MNWAN=<Mode> Where <Mode>=1

Parameters:
- Mode: 0 - Independent WAN
  1 - Bridge with LAN Port
  2 - Independent LAN
- Protocol: 0 - Static IP
  1 - DHCP
  2 - None
- IP: Valid IP address
- Netmask: Valid netmask
- Gateway: Valid IP address. 0 - Reset

### Example

**Input:**
```
AT+MNWAN=0,1<enter>
```

**Response:**
```
OK
```

**Input:**
```
AT+MNWAN?
```

**Response:**
```
Working Mode: Independent WAN
WAN Configuration
Connection Type: DHCP
Default Route: Yes
DNS Server Mode: auto
OK
```
# 5.0 AT Command Line Interface

## AT+MNWANDR

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set the network WAN interface: Default Route</td>
<td>AT+MNWANDR[=&lt;Default Route&gt;]</td>
</tr>
<tr>
<td>Parameters:</td>
<td>Default Route : 0 - No</td>
</tr>
<tr>
<td></td>
<td>1 - Yes</td>
</tr>
</tbody>
</table>

### Example

**Input:**

AT+MNWANDR=1<enter>

**Response:**

OK

## AT+MNWANDNS

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set DNS Server when WAN port set as Independent WAN.</td>
<td>AT+MNWANDNS[=&lt;Mode&gt; [,&lt;Primary DNS&gt;,&lt;Secondary DNS&gt;] ]</td>
</tr>
<tr>
<td>Usage:</td>
<td></td>
</tr>
<tr>
<td>AT+MNWANDNS</td>
<td></td>
</tr>
<tr>
<td>AT+MNWANDNS=&lt;Mode&gt; Where &lt;Mode&gt;=0</td>
<td></td>
</tr>
<tr>
<td>AT+MNWANDNS=&lt;Mode&gt;[,&lt;Primary DNS&gt;,&lt;Secondary DNS&gt;] Where &lt;Mode&gt;=1</td>
<td></td>
</tr>
<tr>
<td>Parameters:</td>
<td>Mode: 0 - Auto</td>
</tr>
<tr>
<td></td>
<td>1 - Manual</td>
</tr>
<tr>
<td>Primary DNS: Valid IP Address or 0 (Reset)</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS: Valid IP Address or 0 (Reset)</td>
<td></td>
</tr>
</tbody>
</table>

### Example

**Input:**

AT+MNWANDR=0<enter>

**Response:**

OK
5.0 AT Command Line Interface

**AT+MNWANLANDHCP**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set the LAN DHCP Server when WASN port set as Independent LAN.</td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

\[
\text{AT+MNWANLANDHCP} = \langle\text{Mode}\rangle,\langle\text{Start IP}\rangle,\langle\text{Limit}\rangle,\langle\text{Lease Time}\rangle,\langle\text{Alt.Gateway}\rangle,\langle\text{Pre.DNS}\rangle,\langle\text{Alt.DNS}\rangle)]
\]

**Usage:**
- AT+MNWANLANDHCP
- AT+MNWANLANDHCP=\langle\text{Mode}\rangle Where \langle\text{Mode}\rangle=0
- AT+MNWANLANDHCP=\langle\text{Mode}\rangle,\langle\text{Start IP}\rangle,\langle\text{Limit}\rangle,\langle\text{Lease Time}\rangle,\langle\text{Alt.Gateway}\rangle,\langle\text{Pre.DNS}\rangle,\langle\text{Alt.DNS}\rangle Where \langle\text{Mode}\rangle=1

**Parameters:**
- Mode: 0 - Disable DHCP Server
- 1 - Enable DHCP Server
- Start IP: The starting address DHCP assignable IP Addresses
- Limit: The maximum number of IP addresses. min=0 max=16777214
- Lease Time: The DHCP lease time in minutes. 2~2147483647 minutes. 0 means 'infinity'
- Alt. Gateway: Alternate Gateway for DHCP assigned devices if the default gateway is not to be used
- Pre. DNS: Preferred DNS server address to be assigned to DHCP devices
- Alt. DNS: Alternate DNS server address to be assigned to DHCP devices

**Example**

**Input:**
AT+MNWANLANDHCP=0<enter>

**Response:**
OK
5.0 AT Command Line Interface

### AT+MNIPMAC

#### Description
Show/Add/Delete/Release/ReleaseAll the MAC-IP Address binding.

#### Command Syntax (Effect: AT&W)

**AT+MNIPMAC=\(<Operation>\>[\,<Name>\],[\,<IP Address>],[\,<MAC Address>]\)**

- **Operation:**
  - **SHOW** - Show the details of the MAC-IP address binding
  - **ADD** - Add a new MAC-IP address binding
  - **DEL** - Delete an existing MAC-IP address binding
  - **RELEASE** - Release the active DHCP lease
  - **RELEASEALL** - Release all active DHCP leases

- **Name:** Name of the MAC-IP binding
- **IP Address:** Valid IP address
- **MAC Address:** The physical MAC address of the device or interface

#### Usage:

- **AT+MNIPMAC**
- **AT+MNIPMAC=SHOW,\(<Name>\)**
- **AT+MNIPMAC=ADD,\(<Name>\),\,<IP Address>\>,\,<MAC Address>\)**
- **AT+MNIPMAC=DEL,\,<NAME>\)**
- **AT+MNIPMAC=RELEASE,\,<NAME>\)**
- **AT+MNIPMAC=RELEASEALL\)**

#### Example

**Input:**

AT+MNIPMAC=ADD,PC,192.168.168.150,0A0B0C0D0E0F<enter>

**Response:**

OK

**Input:**

AT+MNIPMAC?

**Response:**

1: PC, 192.168.168.150, 0A0B0C0D0E0F, Not active

OK

**Input:**

AT+MNIPMAC=RELEASEALL<enter>

**Response:**

Network DHCP server is restarted.

OK
## 5.0 AT Command Line Interface

### AT+MNEMAC

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve the MAC Address of the local Ethernet interface.</td>
<td>AT+MNEMAC &lt;enter&gt;</td>
</tr>
</tbody>
</table>

#### Example

**Input:**
AT+MNEMAC<enter>

**Response:**
+MNEMAC: "00:0F:92:00:40:9A"
OK

### AT+MNPORT

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/set the Ethernet port configuration.</td>
<td>AT+MNPORT[=&lt;Ethernet Port&gt;[,&lt;Mode&gt;[,&lt;Auto Negotiation&gt;,&lt;Speed&gt;,&lt;Duplex&gt;]]]</td>
</tr>
</tbody>
</table>

**Command Syntax**

- **Ethernet Port:**
  - 0 - WAN
  - 1 - LAN1
  - 2 - LAN2

- **Mode:**
  - 0 - Auto
  - 1 - Manual

- **Auto-Neg:**
  - 0 - Off
  - 1 - On

- **Speed:**
  - 0 - 10
  - 1 - 100

- **Duplex:**
  - 0 - Full
  - 1 - Half

#### Example

**Input:**
AT+MNPORT<enter>

**Response:**
0: WAN: Mode: auto
1: LAN1: Mode: auto
2: LAN2: Mode: auto
OK

**Input:**
AT+MNPORT=1,0<enter>

**Response:**
OK
5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>Command Syntax (Effect: Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MNSTATUS?</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MNSTATUS<enter>

**Response:**
LAN Port Status
General Status
IP Address : 192.168.168.1
Connection Type : static
Subnet Mask : 255.255.255.0
MAC Address : 00:0F:92:02:A8:E4
Traffic Status
Receive bytes : 1.884MB
Receive packets : 18542
Transmit bytes : 2.694MB
Transmit packets : 14377

WAN Port Status
General Status
IP Address : N/A
Connection Type : dhcp
Subnet Mask : N/A
MAC Address : 00:0F:92:03:A8:E4
Traffic Status
Receive bytes : 0B
Receive packets : 0
Transmit bytes : 684B
Transmit packets : 2

4G Port Status
General Status
IP Address : 184.151.220.2
Connection Type : static
Subnet Mask : 255.255.255.255
MAC Address : 00:0F:92:FE:00:01
Traffic Status
Receive bytes : 1.096MB
Receive packets : 8602
Transmit bytes : 10.021MB
Transmit packets : 9461
Default Gateway : 184.0.0.1
DNS Server(s) : 70.28.245.227 184.151.118.254

Kernel IP routing table
<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Subnet Mask</th>
<th>Flags</th>
<th>Metric</th>
<th>Ref</th>
<th>Use</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>184.0.0.1</td>
<td>0.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>br-wan2</td>
</tr>
<tr>
<td>169.254.0.0</td>
<td>0.0.0.0</td>
<td>255.255.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>br-lan</td>
</tr>
<tr>
<td>184.0.0.1</td>
<td></td>
<td>255.255.255.255</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>br-wan2</td>
</tr>
<tr>
<td>192.168.168.0</td>
<td></td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>br-lan</td>
</tr>
</tbody>
</table>
## 5.0 AT Command Line Interface

### AT+MNDDNSE

**Description**
Get/Set Dynamic DNS (DDNS) mode.

**Command Syntax (Effect: AT&W)**

```
AT+MNDDNSE=<Mode>
```

**Mode:**
- 0: Disable
- 1: Enable

**Example**

**Input:**

```
AT+MNDDNSE?
```

**Response:**

```
+MNDDNSE: Mode 0
OK
```

**Input:**

```
AT+MNDDNSE=1<enter>
```

**Response:**

```
OK
```

### AT+MNDDNS

**Description**
Get/Set Dynamic DNS (DDNS) settings.

**Command Syntax (Effect: AT&W)**

```
AT+MNDDNS=<service type>,<host>,<username>,<password>
```

**service type:**
- 0: changeip
- 1: dyndns
- 2: eurodyndns
- 3: hn
- 4: noip
- 5: ods
- 6: ovh
- 7: regfish
- 8: tzo
- 9: zoneedit

**Example**

**Input:**

```
AT+MNDDNSE?
```

**Response:**

```
+MNDDNSE: Mode 0
OK
```

**Input:**

```
AT+MNDDNSE=4,mydomain.com,user1,password21<enter>
```

**Response:**

```
OK
```
## 5.0 AT Command Line Interface

### AT+MFGEN

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set firewall general configuration</td>
<td>AT+MFGEN[=&lt;Config&gt;[,&lt;Mode&gt;]]</td>
</tr>
</tbody>
</table>

**Parameters**
- **Config:**
  - 0 - WAN Remote Management
  - 1 - LAN to WAN Access Control
  - 2 - Anti-Spoof
  - 3 - Packet Normalization
  - 4 - Carrier Remote Management
  - 5 - Carrier Request
- **Mode:**
  - 0 - Disable (Block)
  - 1 - Enable (Allow)

**Example**

<table>
<thead>
<tr>
<th>Input:</th>
<th>Response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MFGEN=6,0&lt;enter&gt;</td>
<td>OK</td>
</tr>
</tbody>
</table>

### AT+MFDMZ

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set firewall DMZ configuration</td>
<td>AT+MFDMZ[=&lt;DMZ Source&gt;[,&lt;DMZ Mode&gt;,&lt;DMZ Server IP&gt;,&lt;Exception Port&gt;]]</td>
</tr>
</tbody>
</table>

**Parameters:**
- **DMZ Source:**
  - 0 - WAN
  - 1 - Carrier
- **DMZ Mode:**
  - 0 - Disable
  - 1 - Enable
- **DMZ Server IP:** Valid IP address
- **Exception Port:** 0 - 65535

**Example**

<table>
<thead>
<tr>
<th>Input:</th>
<th>Response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MFDMZ=0,0&lt;enter&gt;</td>
<td>OK</td>
</tr>
</tbody>
</table>
5.0 AT Command Line Interface

**AT+MFDMZ**

**Description**

Get/Set firewall Port Forwarding rules

**Command Syntax**

AT+MFPORTFWD[=<Name>[,<Operation>[,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>]]]

Parameters:
- Name: Name of Port Forwarding rule, 1 - 64 characters
- Operation: ADD - Add a rule
  - EDIT - Edit a rule
  - DEL - Delete a rule
- Source: 0 - WAN
  - 1 - Carrier
  - 2 - WIFI
- Internal IP: Valid IP address
- Internal Port: Valid port number, 1 - 65535
- Protocol: 0 - TCP
  - 1 - UDP
  - 2 - TCPUDP
- External Port: Valid port number, 1 - 65535

**Usage:**
AT+MFPORTFWD
AT+MFPORTFWD=<Name>
AT+MFPORTFWD=<Name>,DEL
AT+MFPORTFWD=<Name>,ADD,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>
AT+MFPORTFWD=<Name>,EDIT,<Source>,<Internal IP>,<Internal Port>,<Protocol>,<External Port>

**Example**

**Input:**
AT+MFPORTFWD=rule1,add,0,192.168.168.203,20001,0,20001<enter>

**Response:**
OK

**Input:**
AT+MFPORTFWD?

**Response:**
Name : rule1
Source : WAN
Internal IP : 192.168.168.203
Internal Port : 20001
Protocol : TCP
External Port : 20001
OK
5.0 AT Command Line Interface

### AT+MFMAC

**Description**

Get/Set firewall MAC List

**Command Syntax**

```plaintext
AT+MFMAC[=<Name>[,[<Operation>[,[<Action>,<Mac Address>]]]]
```

**Parameters:**
- Name: Name of firewall MAC list name, 1 - 64 characters
- Operation: ADD - Add a firewall MAC list
  - EDIT - Edit a firewall MAC list
  - DEL - Delete a firewall MAC list
- Action: 0 - Accept
  - 1 - Drop
  - 2 - Reject
- MAC Address: Valid MAC address

**Usage:**
- AT+MFMAC
- AT+MFMAC=<Name>
- AT+MFMAC=<Name>,DEL
- AT+MFMAC=<Name>,ADD,<Action>,<Mac Address>
- AT+MFMAC=<Name>,EDIT,<Action>,<Mac Address>

**Example**

**Input:**

AT+MFMAC=mac1,add,1,00:0A:0A:0A:0B:FF<enter>

**Response:**

OK

**Input:**

AT+MFMAC?

**Response:**

Name: mac1
Action: DROP
MAC address: 00:0A:0A:0A:0B:FF
OK
5.0 AT Command Line Interface

**AT+MFIP**

### Description

Get/Set firewall IP List

### Command Syntax

\[
\text{AT+MFIP[=]<Name>[,<Operation>[,<Action>,<Source>,<IP Address>[,<Prefix>]]]]}
\]

**Parameters:**
- **Name:** Name of firewall IP list name, 1 - 64 characters
- **Operation:** ADD - Add a firewall IP list
  - EDIT - Edit a firewall IP list
  - DEL - Delete a firewall IP list
- **Action:**
  - 0 - Accept
  - 1 - Drop
  - 2 - Reject
- **Source:**
  - 0 - LAN
  - 1 - Independent LAN
  - 2 - WAN
  - 3 - Carrier
  - 4 - WIFI
- **Source IP:** Valid IP address
- **Prefix:** 0 ~ 32. 32 (default) - single IP address

**Usage:**
- AT+MFIP
- AT+MFIP=<Name>
- AT+MFIP=<Name>,DEL
- AT+MFIP=<Name>,ADD,<Action>,<Source>,<IP Address>[,<Prefix>]
- AT+MFIP=<Name>,EDIT,<Action>,<Source>,<IP Address>[,<Prefix>]

### Example

**Input:**

AT+MFIP=iplist1,add,0,2,184.71.46.138,32<enter>

**Response:**

OK

**Input:**

AT+MFIP?

**Response:**

Name: ip1
Action: ACCEPT
Source: WAN
Source IP: 184.71.46.126
Prefix: 32
Name: iplist1
Action: ACCEPT
Source: WAN
Source IP: 184.71.46.138
Prefix: 32
OK
5.0 AT Command Line Interface

**AT+MFRULE**

**Description**

Get/Set firewall rule.

**Command Syntax**

```
AT+MFRULE=<Name>[,<Operation>[,<Action>,<Source>,<Src IP Format>,<Src IP From/Subnet>,<Src IP To/Prefix>,
<Destination>,<Dest IP Format>,<Dest IP From/Subnet>,<Dest IP To/Prefix>,<Dest Port>,<Protocol>]]
```

**Parameters:**

- **Name:** Name of firewall rule name, 1 - 64 characters
- **Operation:** ADD - Add a firewall rule
  EDIT - Edit a firewall rule
  DEL - Delete a firewall rule
- **Action:**
  0 - Accept
  1 - Drop
  2 - Reject
- **Source:**
  0 - LAN
  1 - Independent LAN
  2 - WAN
  3 - Carrier
  4 - WiFi
  5 - None
- **IP Format:**
  0 - IP Range
  1 - Subnet / Prefix
- **IP From/Subnet:** Valid IP address. 0 - Set to blank
- **IP To/Prefix:** Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix
- **Destination:**
  0 - LAN
  1 - Independent LAN
  2 - WAN
  3 - Carrier
  4 - WiFi
  5 - None
- **IP Format:**
  0 - IP Range
  1 - Subnet / Prefix
- **IP From/Subnet:** Valid IP address. 0 - Set to blank
- **IP To/Prefix:** Valid IP address. 0 - Set to blank; or 0 ~ 32 for Prefix
- **Port/Range:** Port 0 ~ 65535 or Port range specified as 100:200 format
- **Protocol:**
  0 - TCP
  1 - UDP
  2 - TCPUDP
  3 - ICMP
  4 - GRE

**Example**

**Input:**

```
AT+MFRULE=rule1,ADD,0,3,0,0,0,5,0,0,0,34567,2<enter>
```

**Response:**

```
OK
```

**Input:**

```
AT+MFRULE?
```

**Response:**

```
Name        : rule1
Action      : ACCEPT
Source      :
Src IP From :
Src IP To   :
Destination :
Dest IP From :
Dest IP To  :
Dest Port   : 34567
Protocol    : tcpudp
OK
```
# 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT+MFRST</strong></td>
<td>Reset to default firewall</td>
<td>AT+MFRST &lt;enter&gt;</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MFRST<enter>

**Response:**
+MFRST: 0 OK

| **AT+MMIMEI** | Get modem’s IMEI. | AT+MMIMEI <enter> |

**Example**

**Input:**
AT+MMIMEI<enter>

**Response:**
+MMIMEI: 356406060882064 OK

| **AT+MMIMSI** | Get modem’s IMSI. | AT+MMIMSI <enter> |

**Example**

**Input:**
AT+MMIMSI<enter>

**Response:**
+MMIMSI: 302610012606734 OK

| **AT+MMNETRSSI** | Get modem’s RSSI. | AT+MMNETRSSI <enter> |

**Example**

**Input:**
AT+MMNETRSSI<enter>

**Response:**
+MMNETRSSI: -59 OK
## 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>AT+MMPOWERIN</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get modem’s input voltage.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MMPOWERIN &lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>AT+MMPOWERIN&lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>+MMPOWERIN: 12.27</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AT+MMBOARDTEMP</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get modem’s temperature.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MMBOARDTEMP &lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>AT+MMBOARDTEMP&lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>+MMBOARDTEMP: 46.65</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AT+MMWANIP</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get modem’s WAN IP Address (Carrier).</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MMWANIP &lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>AT+MMWANIP&lt;enter&gt;</td>
</tr>
<tr>
<td><strong>Response</strong></td>
<td>+MMWANIP: 184.151.220.2</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
</tbody>
</table>
### 5.0 AT Command Line Interface

#### AT+MMPIPP

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set IP-Passthrough.</td>
<td>AT+MMPIPP=&lt;Mode&gt;</td>
</tr>
</tbody>
</table>

**Mode:**

- 0 Disable
- 1 Ethernet

**Example**

**Input:**

AT+MMPIPP=1<enter>

**Response:**

OK

**Input:**

AT+MMPIPP?

**Response:**

+MMPIPP: 1 Ethernet

OK

#### AT+MMNUM

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get modem’s phone number.</td>
<td>AT+MMNUM &lt;enter&gt;</td>
</tr>
</tbody>
</table>

**Example**

**Input:**

AT+MMNUM <enter>

**Response:**

+MMNUM: 15874327939

OK

#### AT+MMIMI

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get modem’s IMEI and IMSI.</td>
<td>AT+MMIMI &lt;enter&gt;</td>
</tr>
</tbody>
</table>

**Example**

**Input:**

AT+MMIMI <enter>

**Response:**

+MMIMI: MMIMEI:356406060882064, MMIMSI:302610012606734

OK
5.0 AT Command Line Interface

### AT+MMCID

**Description**
Get modem’s SIM card number.

**Command Syntax**

AT+MMCID <enter>

**Example**

**Input:**
AT+MMCID <enter>

**Response:**
+MMCID: 89302610203010832398
OK

### AT+MMMGS

**Description**
Send SMS message.

**Command Syntax (Immediate)**

AT+MMMGS=<Phone Number><CR>

<Phone Number>: Valid phone number
Text is entered and ended by <ctrl-Z/ESC>

**Example**

**Input:**
AT+MMMGS=4035555151<enter>

Test Message <esc>

**Response:**
OK
+CMGS: 15
OK

### AT+MMMGR

**Description**
Read SMS messages.

**Command Syntax (Immediate)**

AT+MMMGR=<index>

**Example**

**Input:**
AT+MMMGR=1<enter>

**Response:**
+CMGL: 1,"REC READ","+19022110349","15/11/14,23:41:39-20"
Test Message

OK
# 5.0 AT Command Line Interface

## AT+MMMGGL

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>List all SMS messages.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Syntax (Immediate)</strong></td>
<td>AT+MMMGGL&lt;enter&gt;</td>
</tr>
</tbody>
</table>

### Example

**Input**:
AT+MMMGGL<enter>

**Response**:
+CMGL: 1,"REC READ","+19022060349","15/11/14,23:41:39-20"
Test Message

+CMGL: 6,"REC READ","+14036129217","15/09/23,15:07:04-16"
This is also a test.

OK

## AT+MMMGD

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>Delete SMS messages from system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Syntax (Immediate)</strong></td>
<td>AT+MMMGD=&lt;index&gt;</td>
</tr>
</tbody>
</table>

### Example

**Input**:
AT+MMMGD=12<enter>

**Response**:
OK

## AT+MMSCMD

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>GET/SET system SMS command service.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Syntax (Effect: AT&amp;W)</strong></td>
<td>AT+MMSCMD=&lt;Mode&gt;[,&lt;Filter Mode&gt;[,&lt;Phone No.1&gt;[],...,&lt;Phone No.6&gt;]]</td>
</tr>
</tbody>
</table>

### Example

**Input**:
AT+MMSCMD=1<enter>

**Response**:
OK
## 5.0 AT Command Line Interface

### AT+MIOMODE

**Description**
Get/Set IO input or output mode.

**Command Syntax (Effect: AT&W)**

\[
\text{AT+MIOMODE} = \langle \text{Index}, \langle \text{Mode} \rangle \rangle \\
\text{Index:} \\
\text{The index of IO port, 1 to 2} \\
\text{Mode:} \\
0 \quad \text{Input} \\
1 \quad \text{Output}
\]

**Example**

**Input:**
\[
\text{AT+MIOMODE} = 1, 0 <\text{enter}>
\]

**Response:**

```
OK
```

**Input:**
\[
\text{AT+MIOMODE}?
\]

**Response:**

```
+MIOMODE: IO port mode
Mode1: 0    Input
Mode2: 0    Input
OK
```

### AT+MIOOC

**Description**
Get/Set output control. (I/O point must be set as output)

**Command Syntax (Immediate)**

\[
\text{AT+MIOOC} = \langle \text{Index}, \langle \text{Output Control} \rangle \rangle \\
\text{Index:} \\
\text{The index of IO port, 1 to 2} \\
\text{Output Control:} \\
0 \quad \text{Open} \\
1 \quad \text{Close}
\]

**Example**

**Input:**
\[
\text{AT+MIOOC} = 1, 1 <\text{enter}>
\]

**Response:**

```
OK
```

**Input:**
\[
\text{AT+MIOOC}?
\]

**Response:**

```
+MIOOC: IO Output Control
OutputCtrl1: 1    Close
OutputCtrl2: 0    Open
OK
```
## 5.0 AT Command Line Interface

### AT+MIOSTATUS

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET IO status.</td>
<td>AT+MIOSTATUS &lt;enter&gt;</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MIOSTATUS <enter>

**Response:**
+MIOSTATUS: IO status
iodigiinval1=High
iodigiinval2=High
OK

### AT+MIOMETER

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET IO meter (V).</td>
<td>AT+MIOMETER &lt;enter&gt;</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MIOMETER <enter>

**Response:**
+MIOMETER: IO meter(V)
iovolts1=2.77
iovolts2=2.81
OK

### AT+MCPS2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Serial port as either a console port (AT Commands) or a Data Port.</td>
<td>AT+MCPS2=&lt;Mode&gt;</td>
</tr>
</tbody>
</table>

**Mode:**
- 0 Console
- 1 Data

**Example**

**Input:**
AT+MCPS2=0<enter>

**Response:**
OK
## 5.0 AT Command Line Interface

### AT+MCBR2

**Description**
Get/Set Serial port baud rate.

**Command Syntax (Effect: AT&W)**

```plaintext
AT+MCBR2=<Baud Rate>
```

**Baud Rate:**
- 0 300
- 1 600
- 2 1200
- 3 2400
- 4 3600
- 5 4800
- 6 7200
- 7 9600
- 8 14400
- 9 19200
- 10 28800
- 11 38400
- 12 57600
- 13 115200
- 14 230400
- 15 460800
- 16 921600

### Example

**Input:**

AT+MCBR2=13<enter>

**Response:**

OK

**Input:**

AT+MCBR2?

**Response:**

+MCBR2: 13 115200

OK

### AT+MCDF2

**Description**
Get/Set Serial port data format

**Command Syntax (Effect: AT&W)**

```plaintext
AT+MCDF2=<data format>
```

**Data Format:**
- 0 8N1
- 2 8E1
- 3 8O1

### Example

**Input:**

AT+MCDF2=0<enter>

**Response:**

OK

### AT+MCDM2

**Description**
Set Serial port data mode.

**Command Syntax (Effect: AT&W)**

```plaintext
AT+MCDM2=<Data Mode>
```

**Data Mode:**
- 0 Seamless
- 1 Transparent

### Example

**Input:**

AT+MCDM2=1<enter>

**Response:**

OK
## 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AT+MCCT2</strong></td>
<td>Set Comport character timeout.</td>
<td><strong>AT+MCCT2=&lt;/timeout_s&gt;</strong>&lt;br&gt;(0 to 65535 seconds)</td>
</tr>
<tr>
<td><strong>AT+MCMPS2</strong></td>
<td>Get/Set Serial port maximum packet size.</td>
<td><strong>AT+MCMPS2=&lt;/size&gt;</strong>&lt;br&gt;size: 0 to 65535</td>
</tr>
<tr>
<td><strong>AT+MCNCDI2</strong></td>
<td>Enable/Disable Serial port no-connection data intake.</td>
<td><strong>AT+MCNCDI2=&lt;/Mode&gt;</strong>&lt;br&gt;Mode:&lt;br&gt;0 Disable&lt;br&gt;1 Enable</td>
</tr>
</tbody>
</table>

### Example

**Input:**

AT+MCCT2=0<enter>  
AT+MCMPS2=1024<enter>  
AT+MCNCDI2=1<enter>

**Response:**

OK
## 5.0 AT Command Line Interface

### AT+MCMTC2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set Serial port modbus TCP configuration.</td>
<td>AT+MCMTC2=&lt;Status&gt;, &lt;Protection status&gt;, &lt;Protection Key&gt;</td>
</tr>
<tr>
<td>Status and Protection Status:</td>
<td>0 Disable</td>
</tr>
<tr>
<td>1 Enable</td>
<td></td>
</tr>
</tbody>
</table>

#### Example

**Input:**
```
AT+MCMTC2=0,0,1234<enter>
```

**Response:**
```
OK
```

### AT+MCIPM2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the Serial port IP Protocol Mode.</td>
<td>AT+MCIPM2=&lt;Mode&gt;</td>
</tr>
<tr>
<td>Mode:</td>
<td>0 TCP Client</td>
</tr>
<tr>
<td>1 TCP Server</td>
<td></td>
</tr>
<tr>
<td>2 TCP Client/Server</td>
<td></td>
</tr>
<tr>
<td>3 UDP Point to Point</td>
<td></td>
</tr>
<tr>
<td>7 SMTP Client</td>
<td></td>
</tr>
<tr>
<td>8 PPP</td>
<td></td>
</tr>
<tr>
<td>11 GPS Transparent Mode</td>
<td></td>
</tr>
</tbody>
</table>

#### Example

**Input:**
```
AT+MCIPM2=1<enter>
```

**Response:**
```
OK
```

### AT+MCTC2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Serial port TCP Client parameters when IP Protocol Mode is set to TCP Client.</td>
<td>AT+MCTC2=&lt;Remote Server IP&gt;, &lt;Remote Server Port&gt;, &lt;Outgoing timeout_s&gt;</td>
</tr>
<tr>
<td>Remote Server IP : valid IP address</td>
<td></td>
</tr>
<tr>
<td>Remote Server Port : 1 to 65535</td>
<td></td>
</tr>
<tr>
<td>Outgoing timeout_s: 0 to 65535</td>
<td></td>
</tr>
</tbody>
</table>

#### Example

**Input:**
```
AT+MCTC2=0.0.0.0,20002,60<enter>
```

**Response:**
```
OK
```
# 5.0 AT Command Line Interface

## AT+MCTS2

**Description**
Set TCP Server parameters when IP Protocol Mode is set to TCP Server.

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MCTS2=20002,300&lt;enter&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

> AT+MCTS2=<Local Listener Port>,<Connection timeout_s>

- Local Listener Port: 1 to 65535
- Connection timeout_s: 0 to 65535

## AT+MCTCS2

**Description**
Set TCP Client/Server parameters when IP Protocol is set to TCP Client/Server mode.

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MCCS2=0.0.0.0,20002,60,20002&lt;enter&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

> AT+MCTCS2=<Remote Server IP>,<Remote Server Port>,<Outgoing timeout_s>,<Local Listener Port>

- Remote Server IP: valid IP address
- Remote Server Port: 1 to 65535
- Outgoing timeout_s: 0 to 65535
- Local Listener Port: 1 to 65535

## AT+MCUPP2

**Description**
Set UDP Point-to-Point parameters when IP Protocol is set to UDP Point-to-Point mode.

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MCUPP2=0.0.0.0,20002,20002&lt;enter&gt;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

> AT+MCUPP2=<Remote IP>,<Remote Port>,<Listener Port>

- Remote IP: valid IP address
- Remote Port: 1 to 65535
- Listener Port: 1 to 65535
## 5.0 AT Command Line Interface

### AT+MCSMTP2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set Serial port SMTP client configuration when IP Protocol mode is set to SMTP client.</td>
<td>AT+MCSMTP2=&lt;Mail Subject&gt;,&lt;Mail Server&gt;,&lt;Username&gt;,&lt;Password&gt;,&lt;Mail Recipient&gt;,&lt;Message Max Size&gt;,&lt;TimeOut&gt;,&lt;Transfer Mode&gt;</td>
</tr>
<tr>
<td>Mail Subject</td>
<td>: 1 to 63 bytes</td>
</tr>
<tr>
<td>Mail Server</td>
<td>: Valid IP Address or Name</td>
</tr>
<tr>
<td>Username</td>
<td>: 1 to 63 bytes</td>
</tr>
<tr>
<td>Password</td>
<td>: 1 to 63 bytes</td>
</tr>
<tr>
<td>Mail Recipient</td>
<td>: 1 to 63 bytes</td>
</tr>
<tr>
<td>Message Max Size</td>
<td>: [1 .. 65535]</td>
</tr>
<tr>
<td>TimeOut</td>
<td>: [0 .. 65535] in seconds</td>
</tr>
<tr>
<td>Transfer Mode</td>
<td>: 0: Text; 1: Attached File; 2: Hex Code</td>
</tr>
</tbody>
</table>

### AT+MCPPP2

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set Serial port PPP configuration when IP protocol mode to set to PPP.</td>
<td>AT+MCPPP2=&lt;Mode&gt;,&lt;LCP Echo Failure Number&gt;,&lt;LCP Echo Interval&gt;,&lt;Local IP&gt;,&lt;Host IP&gt;,&lt;Idle Timeout&gt;[,&lt;Expected String&gt;,&lt;Response String&gt;]</td>
</tr>
<tr>
<td>COM2:</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>: 0 - Active; 1 - Passive</td>
</tr>
<tr>
<td>LCP Echo Failure Number</td>
<td>: [0 .. 65535]</td>
</tr>
<tr>
<td>LCP Echo Interval</td>
<td>: [0 .. 65535]</td>
</tr>
<tr>
<td>Local IP</td>
<td>: Valid IP address</td>
</tr>
<tr>
<td>Host IP</td>
<td>: Valid IP address</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>: [0 .. 65535] in seconds</td>
</tr>
<tr>
<td>Expected String</td>
<td>: (Optional) 0 - 63 characters</td>
</tr>
<tr>
<td>Response String</td>
<td>: (Optional) 0 - 63 characters</td>
</tr>
</tbody>
</table>

### Example

<table>
<thead>
<tr>
<th>Input:</th>
<th>Response:</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MCPPP2?</td>
<td>+MCPPP2:</td>
</tr>
<tr>
<td>Mode</td>
<td>: 1 - Passive</td>
</tr>
<tr>
<td>LCP Echo Failure Number</td>
<td>: 0</td>
</tr>
<tr>
<td>LCP Echo Interval</td>
<td>: 0</td>
</tr>
<tr>
<td>Local IP</td>
<td>: 192.168.12.1</td>
</tr>
<tr>
<td>Idle Timeout(s)</td>
<td>: 30</td>
</tr>
<tr>
<td>Expected String</td>
<td>: CLIENT</td>
</tr>
<tr>
<td>Response String</td>
<td>: CLIENTSERVER</td>
</tr>
<tr>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>
# 5.0 AT Command Line Interface

## AT+MAEURD1

**Command Syntax (Effect: AT&W)**

```
AT+MAEURD1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Time> [,Interfaces]]
```

- **Mode**: 0 Disable  
  1 Modem Event Report  
  2 SDP Event Report  
  3 Management Report

- **Remote IP**: valid IP address
- **Remote Port**: 0 to 65535
- **Interval Time**: 0 to 65535 seconds
- **Interfaces**: (optional) 0 Disable; 1 Enable Modem, Carrier and WAN for Modem Event Report. For instance, "1,1,1" to enable all interfaces Ethernet, Carrier, USB, COM and IO for Management Report. For instance, "0,0,0,0,0" to disable all interfaces

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
Response: OK |

## AT+MANMSR

**Command Syntax (Effect: AT&W)**

```
AT+MANMSR=<Mode>[,<Remote Port>,<Interval Time_s>]
```

- **Mode**: 0 Disable  
  1 Enable NMS Report

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Define NMS Report. | Input: AT+MANMSR=1,20200,300<enter>
Response: OK |

## AT+MANMSSRV

**Command Syntax (Effect: AT&W)**

```
AT+MANMSSRV=<<Server>,<Name>,<Password>,<Confirm Password>]
```

- **Server**: NMS Server/IP. 1 to 63 characters
- **Name**: Domain Name. 1 to 63 characters
- **Password**: Domain Password. 5 to 64 characters
- **Confirm Password**: Same as <Password>. 5 to 64 characters

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| Get/Set NMS Server. | Input: AT+MANMSSRV=nms.microhardcorp.com,mytech,mypass,mypass<enter>
Response: OK |
5.0 AT Command Line Interface

### AT+MADISS

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure discovery mode service used by pX2 and utilities such as “IP Discovery”.</td>
<td>AT+MADISS=&lt;Mode&gt;</td>
</tr>
<tr>
<td></td>
<td>Mode:</td>
</tr>
<tr>
<td></td>
<td>0 Disable</td>
</tr>
<tr>
<td></td>
<td>1 Discoverable</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MADISS=1 <enter>

**Response:**
OK

### AT+MAWSCLIENT

<table>
<thead>
<tr>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set Web Service Client.</td>
<td>AT+MAWSCLIENT[=&lt;Mode&gt;[,&lt;ServerType&gt;,&lt;Port&gt;,&lt;UserName&gt;,&lt;Password&gt;,&lt;Interval&gt;]]</td>
</tr>
<tr>
<td></td>
<td>Mode: 0 - Disable</td>
</tr>
<tr>
<td></td>
<td>1 - Enable</td>
</tr>
<tr>
<td></td>
<td>ServerType: 0 - https</td>
</tr>
<tr>
<td></td>
<td>1 - http</td>
</tr>
<tr>
<td></td>
<td>Port: 1 to 65535. Default is 9998</td>
</tr>
<tr>
<td></td>
<td>UserName: 1 to 63 characters</td>
</tr>
<tr>
<td></td>
<td>Password: 1 to 63 characters</td>
</tr>
<tr>
<td></td>
<td>Interval: In minute. 1 to 65535 minutes.</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MAWSCLIENT=1,1,9998,username,password,10<enter>

**Response:**
OK
5.0 AT Command Line Interface

**AT+MASNMP**

<table>
<thead>
<tr>
<th>Description</th>
<th>Get/Set SNMP service.</th>
</tr>
</thead>
</table>

**Command Syntax (Effect: AT&W)**

AT+MASNMP=[<Mode> [,<ROCommunity>,<RWCommunity>,<Port>,<Version>]]

- **Mode:**
  - 0 - Disable
  - 1 - Enable

- **ROCommunity:** Read Only Community Name 1 to 31 characters
- **RWCommunity:** Read Write Community Name 1 to 31 characters
- **Port:** Listening Port 0 to 65535. Default is 161
- **Version:** SNMP version
  - 1 - Version 1
  - 2 - Version 2
  - 3 - Version 3 (Use AT+MASNMPV3 to set Authentication and Privacy parameters)

**Example**

**Input:**
AT+MASNMP=1,public,private,161,2<enter>

**Response:**
OK
5.0 AT Command Line Interface

**AT+MASNMPV3**

**Description**
Get/Set SNMP version 3.

**Command Syntax (Effect: AT&W)**

\[
\text{AT+MASNMPV3=}<\text{UserName}>,<\text{RWLimit}>,<\text{AuthLevel}>,[<\text{Auth}>,<\text{AuthPassword}> [,<\text{Privacy}>,<\text{PrivacyPassword}>]]
\]

- **UserName**: V3 User Name 1 to 31 characters
- **RWLimit**: V3 User Read Write Limit
  - 0 - Read Only
  - 1 - Read Write
- **AuthLevel**: V3 User Authentication Level
  - 0 - NoAuthNoPriv
  - 1 - AuthNoPriv
  - 2 - AuthPriv
- **Auth**: V3 Authentication Protocol
  - 0 - MD5
  - 1 - SHA
- **AuthPassword**: V3 Authentication Password 1 to 255 characters
- **Privacy**: V3 Privacy Protocol
  - 0 - DES
  - 1 - AES
- **PrivacyPassword**: V3 Privacy Password 1 to 255 characters

**Usage**:

- \(\text{AT+MASNMPV3=}<\text{UserName}>,<\text{RWLimit}>,0\) If \(<\text{AuthLevel}>=0\) (NoAuthNoPriv)
- \(\text{AT+MASNMPV3=}<\text{UserName}>,<\text{RWLimit}>,1,<\text{Auth}>,<\text{AuthPassword}>\) If \(<\text{AuthLevel}>=1\) (AuthNoPriv)
- \(\text{AT+MASNMPV3=}<\text{UserName}>,<\text{RWLimit}>,2,<\text{Auth}>,<\text{AuthPassword}>,<\text{Privacy}>,<\text{PrivacyPassword}>\) If \(<\text{AuthLevel}>=2\) (AuthPriv)

**Example**

**Input**:  
AT+MASNMPV3 <enter>  

**Response**:  
+MASNMPV3:  
  UserName : userV3  
  RWLimit : Read Only  
  AuthLevel : NoAuthNoPriv  
  OK
5.0 AT Command Line Interface

### AT+MASNMMPTRAP

**Description**
Get/Set SNMP Trap.

**Command Syntax (Effect: AT&W)**

```
AT+MASNMMPTRAP[=<Mode>,<Name>,<IP>[,<AuthFailureTraps>]]
```

- **<Mode>**: 0 - Disable, 1 - Enable
- **<Name>**: Trap Community Name. 1 to 32 characters
- **<IP>**: Trap Manage Host IP. Default 0.0.0.0 (Disable)
- **<AuthFailureTraps>**: 0 - Disable, 1 - Enable

**Usage**:

```
AT+MASNMMPTRAP
AT+MASNMMPTRAP=0
AT+MASNMMPTRAP=1[,<Name>,<IP> [,<AuthFailureTraps>]]
```

**Example**

**Input**:

```
AT+MASNMMPTRAP=1 <enter>
```

**Response**:

```
OK
```

**Input**:

```
AT+MASNMMPTRAP?
```

**Response**:

```
+MASNMMPTRAP:
  Mode : 1 - Enable
  Name : TrapUser
  IP : 0.0.0.0
  AuthFailureTraps : 0 - Disable
OK
```

### AT+MAAUTH

**Description**
Get/Set authentication configuration.

**Command Syntax (Effect: AT&W)**

```
AT+MAAUTH[=<Mode>,<ServerIP>,<ServerPort>,<SharedSecret>]
```

- **<Mode>**: 0 - Local, 1 - Local&RADIUS
- **<ServerIP>**: Remote Server IP Address
- **<ServerPort>**: Remote Server IP Port. 0 to 65535. Default 1812
- **<SharedSecret>**: 5 to 64 characters

**Usage**:

```
AT+MAAUTH=
AT+MAAUTH=0
AT+MAAUTH=1 [, <ServerIP>, <ServerPort>, <SharedSecret>]
```

**Example**

**Input**:

```
AT+MAAUTH?
```

**Response**:

```
+MAAUTH:
  Mode         : 1 - Local&RADIUS
  ServerIP     : 0.0.0.0
  ServerPort   : 1812
  SharedSecret : nosecret
OK
```
### 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>AT+MWRADIO</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get/Set radio status, on or off.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MWRADIO=&lt;Radio&gt;</td>
</tr>
<tr>
<td><strong>Input:</strong></td>
<td>Radio:</td>
</tr>
<tr>
<td></td>
<td>0 - Off</td>
</tr>
<tr>
<td></td>
<td>1 - On</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AT+MWMODE</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get/Set radio mode.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MWMODE=&lt;Mode&gt;</td>
</tr>
<tr>
<td><strong>Input:</strong></td>
<td>Mode:</td>
</tr>
<tr>
<td></td>
<td>0 - 802.11B ONLY</td>
</tr>
<tr>
<td></td>
<td>1 - 802.11BG</td>
</tr>
<tr>
<td></td>
<td>2 - 802.11NG - High Throughput on 2.4GHz</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AT+MWTXPOWER</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get/Set radio TX Power.</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td>AT+MWTXPOWER=&lt;Tx Power&gt;</td>
</tr>
<tr>
<td><strong>Input:</strong></td>
<td>Tx Power:</td>
</tr>
<tr>
<td></td>
<td>0 - 20 dbm</td>
</tr>
<tr>
<td></td>
<td>1 - 21 dbm</td>
</tr>
<tr>
<td></td>
<td>2 - 22 dbm</td>
</tr>
<tr>
<td></td>
<td>3 - 23 dbm</td>
</tr>
<tr>
<td></td>
<td>4 - 24 dbm</td>
</tr>
<tr>
<td></td>
<td>5 - 25 dbm</td>
</tr>
<tr>
<td></td>
<td>6 - 26 dbm</td>
</tr>
<tr>
<td></td>
<td>7 - 27 dbm</td>
</tr>
<tr>
<td></td>
<td>8 - 28 dbm</td>
</tr>
<tr>
<td></td>
<td>9 - 29 dbm</td>
</tr>
<tr>
<td></td>
<td>10 - 30 dbm</td>
</tr>
</tbody>
</table>
### 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>AT+MWDISTANCE</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Get/Set radio Wireless Distance.</td>
<td>AT+MWDISTANCE=&lt;Distance&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distance (m): Minimum 1</td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MWDISTANCE=1000 <enter>

**Response:**
OK

<table>
<thead>
<tr>
<th>AT+MWCHAN</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Set radio channel</td>
<td>AT+MWCHAN=&lt;Channel&gt;</td>
</tr>
</tbody>
</table>

**Available radio channels for mode 11ng and high throughput mode HT20:**

- 0 - auto
- 1 - 1
- 2 - 2
- 3 - 3
- 4 - 4
- 5 - 5
- 6 - 6
- 7 - 7
- 8 - 8
- 9 - 9
- 10 - 10
- 11 - 11

**Example**

**Input:**
AT+MWCHAN=0 <enter>

**Response:**
OK

<table>
<thead>
<tr>
<th>AT+MWHTMODE</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Get/Set radio high throughput mode.</td>
<td>AT+MWHTMODE=&lt;High Throughput Mode&gt;</td>
</tr>
</tbody>
</table>

**High Throughput Mode:**

- 0 - HT20
- 1 - HT40-
- 2 - HT40+
- 3 - Force HT40-
- 4 - Force HT40+

**Example**

**Input:**
AT+MWHTMODE=2 <enter>

**Response:**
OK
## 5.0 AT Command Line Interface

### AT+MWMPDUAGG

**Description**
Get/Set radio MPDU Aggregation.

**Command Syntax (Effect: AT&W)**
AT+MWMPDUAGG=<MPDU Aggregation>
MPDU Aggregation:
0 - Disable
1 - Enable

**Example**

Input:
AT+MWMPDUAGG=1<enter>
Response:
OK

---

### AT+MWSHORTGI

**Description**
Get/Set radio short GI

**Command Syntax (Effect: AT&W)**
AT+MWSHORTGI=<Short GI>
Short GI:
0 - Disable
1 - Enable

**Example**

Input:
AT+MWSHORTGI=1<enter>
Response:
OK

---

### AT+MWHTCAPAB

**Description**
Get Radio HT Capabilities Info

**Command Syntax**
AT+MWHTCAPAB <enter>

**Example**

Input:
AT+MWHTCAPAB <enter>
Response:
+MWHTCAPAB: HT Capabilities Info -
OK
# 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>AT+MWAMSDU</th>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get radio maximum AMSDU (byte).</td>
<td>AT+MWAMSDU</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MWAMSDU <enter>

**Response:**
+MWAMSDU: Maximum AMSDU (byte) - 3839

OK

<table>
<thead>
<tr>
<th>AT+MWAMPDU</th>
<th>Description</th>
<th>Command Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get radio maximum AMPDU (byte).</td>
<td>AT+MWAMPDU</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MWAMPDU <enter>

**Response:**
+MWAMPDU: Maximum AMPDU (byte) - 65535

OK

<table>
<thead>
<tr>
<th>AT+MWRTSTHRESH</th>
<th>Description</th>
<th>Command Syntax (Effect: AT&amp;W)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get/Set radio RTS Threshold.</td>
<td>AT+MWRTSTHRESH=&lt;RTS Threshold&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

**Input:**
AT+MWRTSTHRESH=0 <enter>

**Response:**
OK
## 5.0 AT Command Line Interface

### AT+MWFRAGTHRESH

- **Description**: Get/Set radio Fragment Threshold.
- **Example**:
  
  **Input**:
  
  AT+MWFRAGTHRESH=0 <enter>
  
  **Response**:
  
  OK

- **Command Syntax (Effect: AT&W)**:
  
  AT+MWFRAGTHRESH=<Fragmentation Threshold>
  
  Fragmentation Threshold:
  
  0                Disabled
  
  256-2346   Enabled with the value

### AT+MWCCATHRESH

- **Description**: Get/Set radio CCA Threshold.
- **Example**:
  
  **Input**:
  
  AT+MWCCATHRESH=28 <enter>
  
  **Response**:
  
  OK

- **Command Syntax (Effect: AT&W)**:
  
  AT+MWCCATHRESH=<CCA Threshold>
  
  CCA Threshold:
  
  Range of values: 4-127

### AT+MWIFACE

- **Description**: List/Add/Delete radio virtual interface.
- **Example**:
  
  **Input**:
  
  AT+MWIFACE=0 <enter>
  
  **Response**:
  
  Radio Virtual Interface [0]:
  
  Network         : lan
  Mode            : ap
  TX bitrate      : auto
  ESSID Broadcast : Off
  AP Isolation    : Off
  SSID            : PWii
  Encryption Type : psk2
  WPA PSK         : 1234567890
  OK

- **Command Syntax (Effect: AT&W)**:
  
  AT+MWIFACE=0[,<Index>]
  
  AT+MWIFACE=1
  
  AT+MWIFACE=2,<Index>
  
  Index:
  
  Radio Virtual Interface Index: 0-3
## 5.0 AT Command Line Interface

### AT+MWNETWORK

**Description**
Get/Set radio virtual interface: Network

**Command Syntax (Effect: AT&W)**

```
AT+MWNETWORK=[<Index>[,.<Network>]]
```

**Index:**
- Radio Virtual Interface Index: 0-3

**Network:**
- Radio Virtual Interface Network:
  - 0 - LAN
  - 1 - lan1

**Example**

**Input:**
```
AT+MWNETWORK=0 <enter>
```

**Response:**
```
+MWNETWORK: Virtual Interface 0: 0 - LAN
OK
```

### AT+MWSSID

**Description**
Get/Set radio virtual interface: SSID

**Command Syntax (Effect: AT&W)**

```
AT+MWSSID=[<Index>[,.<SSID>]]
```

**Index:**
- Radio Virtual Interface Index: 0-3

**SSID:**
- Radio Virtual Interface SSID: 1 - 63 character

**Example**

**Input:**
```
AT+MWSSID=0,MySSID <enter>
```

**Response:**
```
OK
```

### AT+MWDEVICEMODE

**Description**
Get/Set radio virtual interface: Mode

**Command Syntax (Effect: AT&W)**

```
AT+MWDEVICEMODE=[<Index>[,.<Device Mode>]]
```

**Index:**
- Radio Virtual Interface Index: 0-3

**Device Mode:**
- Radio Virtual Interface Mode:
  - 0 - Access Point
  - 1 - Client
  - 2 - Repeater

**Example**

**Input:**
```
AT+MWDEVICEMODE=0,0 <enter>
```

**Response:**
```
OK
```
### 5.0 AT Command Line Interface

#### AT+MWRATE

**Description**
Get/Set radio virtual interface: TX bit rate

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MWTXRATE=0,0 &lt;enter&gt;</td>
<td>OK</td>
</tr>
</tbody>
</table>

#### Command Syntax (Effect: AT&W)

AT+MWRATE=[<Index>[,<TX bitrate>]]

- **Index:**
  - Radio Virtual Interface Index: 0-3
- **TX bitrate:**
  - Radio Virtual Interface TX bitrate:
    - 0 - auto
    - 1 - mcs-0
    - 2 - mcs-1
    - 3 - mcs-2
    - 4 - mcs-3
    - 5 - mcs-4
    - 6 - mcs-5
    - 7 - mcs-6
    - 8 - mcs-7
    - 9 - mcs-8
    - 10 - mcs-9
    - 11 - mcs-10
    - 12 - mcs-11
    - 13 - mcs-12
    - 14 - mcs-13
    - 15 - mcs-14
    - 16 - mcs-15

#### AT+MWWSDS

**Description**
Get/Set radio virtual interface: WDS

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MWWSDS=0,1 &lt;enter&gt;</td>
<td>OK</td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

AT+MWWSDS=[<Index>[,<WDS>]]

- **<Index>:**
  - Radio Virtual Interface Index: 0-3
- **<WDS>:**
  - 0 - Off
  - 1 - On

#### AT+MWSSIDBCAST

**Description**
Get/Set radio virtual interface: ESSID Broadcast.

**Example**

<table>
<thead>
<tr>
<th>Input</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+MWSSIDBCAST=0,1 &lt;enter&gt;</td>
<td>OK</td>
</tr>
</tbody>
</table>

**Command Syntax (Effect: AT&W)**

AT+MWSSIDBCAST=[<Index>[,<ESSID Broadcast>]]

- **Index:**
  - Radio Virtual Interface Index: 0-3
- **ESSID Broadcast:**
  - Radio Virtual Interface ESSID Broadcast:
    - 0 - Off
    - 1 - On
5.0 AT Command Line Interface

AT+MWENCRYPT

Command Syntax (Effect: AT&W)

Get/Set radio virtual interface: Encryption Type

For PSK,

AT+MWENCRYPT=[<Index>,[<Encryption Type>,<PSK Password>]]

For RADIUS,

AT+MWENCRYPT=[<Index>,[<Encryption Type>,<RADIUS Server Key>,<RADIUS IP Address>,<RADIUS Port>]]

<Index>
Radio Virtual Interface Index: 0-3
AP Isolation:
Radio Virtual Interface AP Isolation:
  0 - Off
  1 - On

<Encryption Type>
Radio Virtual Interface Encryption Type:
  0 - Disabled
  1 - WPA (PSK)
  2 - WPA2 (PSK)
  3 - WPA+WPA2 (PSK)
  4 - WPA Enterprise (RADIUS)
  5 - WPA2 Enterprise (RADIUS)
  6 - WPA+WPA2 Enterprise (RADIUS)

<PSK Password>: Min 8 characters, Max 63 characters
<RADIUS Server Key>: Min 4 characters, Max 63 characters
<RADIUS IP Address>: Valid IP address
<RADIUS Port>: Valid port 0 - 65535

Example

Input:
AT+MWENCRYPT=0,1,#microhard123 <enter>
Response:
OK

Input:
AT+MWENCRYPT> <enter>
Response:
+MWENCRYPT: Virtual Interface 0:
  Encryption Type: 1 - WPA (PSK)
  Password: #microhard123
  OK

AT+MWAPISOLATION

Command Syntax (Effect: AT&W)

Get/Set radio virtual interface: AP Isolation

AT+MWSSIDBCAST=[<Index>,[<AP Isolation>]]

Index:
Radio Virtual Interface Index: 0-3
AP Isolation:
Radio Virtual Interface AP Isolation:
  0 - Off
  1 - On

Example

Input:
AT+MWAPISOLATION=0,0 <enter>
Response:
OK
### 5.0 AT Command Line Interface

<table>
<thead>
<tr>
<th>AT+WSCAN</th>
<th>AT+MWRSSI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Get radio network scan information. (Must be in client mode, scans for available networks).</td>
</tr>
<tr>
<td><strong>Example</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Input:**
AT+WSCAN <enter>  
**Response:**
Varies

**Input:**
AT+MWRSSI <enter>  
**Response:**
+MWRSSI: -76 dBm  
OK
Appendix A: Serial Interface

<table>
<thead>
<tr>
<th>Module (DCE)</th>
<th>Host (e.g., PC) (DTE)</th>
<th>Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present).</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DCD → IN</td>
<td>The interface conforms to standard RS-232 signals, so direct connection to a host PC (for example) is accommodated.</td>
</tr>
<tr>
<td>2</td>
<td>RX → IN</td>
<td>The signals in the asynchronous serial interface are described below:</td>
</tr>
<tr>
<td>3</td>
<td>← TX OUT</td>
<td><strong>DCD</strong> <em>Data Carrier Detect</em> - Output from Module - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another device.</td>
</tr>
<tr>
<td>4</td>
<td>← DTR OUT</td>
<td><strong>RX</strong> <em>Receive Data</em> - Output from Module - Signals transferred from the BulletPlus are received by the DTE via RX.</td>
</tr>
<tr>
<td>5</td>
<td>SG</td>
<td><strong>TX</strong> <em>Transmit Data</em> - Input to Module - Signals are transmitted from the DTE via TX to the BulletPlus.</td>
</tr>
<tr>
<td>6</td>
<td>DSR → IN</td>
<td><strong>DTR</strong> <em>Data Terminal Ready</em> - Input to Module - Asserted (TTL low) by the DTE to inform the module that it is alive and ready for communications.</td>
</tr>
<tr>
<td>7</td>
<td>← RTS OUT</td>
<td><strong>SG</strong> <em>Signal Ground</em> - Provides a ground reference for all signals transmitted by both DTE and DCE.</td>
</tr>
<tr>
<td>8</td>
<td>CTS → IN</td>
<td><strong>DSR</strong> <em>Data Set Ready</em> - Output from Module - Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the module’s equivalent of the DTR signal.</td>
</tr>
</tbody>
</table>

**Notes:** It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

“DCE” and “module” are often synonymous since a module is typically a DCE device.

“DTE” is, in most applications, a device such as a host PC.
Appendix B: IP-Passthrough Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, a common application of the BulletPlus is to access connected devices remotely. In order to do this, the BulletPlus must be told how to deal with incoming traffic, where to send it to. To accomplish this there are three options:

- IP-Passthrough
- Port Forwarding
- DMZ (a type of Port Forwarding)

In this section we will talk about IP-Passthrough and how to configure the BulletPlus and the connected device/PC to work with IP-Passthrough. IP-Passthrough means that the BulletPlus is transparent, and all outside (WAN) traffic is simply sent directly to a single device connected to the physical LAN RJ45 port on the BulletPlus (With exception of port 80, which is retained for remote configuration (configurable). Also, any traffic that is sent to the RJ45 port is sent directly out the WAN port and is not processed by the BulletPlus.

IP-Passthrough is ideal for applications where only a single device is connected to the BulletPlus, and other features of the BulletPlus are not required. When in pass-through mode, most features of the BulletPlus are bypassed, this includes the serial ports, the GPS features, VPN, and much more. The advantage of IP-Passthrough is that the configuration is very simple.

In the example below we have a BulletPlus connected to a PC (PC2). The application requires that PC1 be able to access several services on PC2. Using Port Forwarding this would require a new rule created for each port, and some applications or services may require several ports so this would require several rules, and the rules may be different for each installation, making future maintenance difficult. For IP-passthrough, PC1 only needs to know the Public Static IP Address of the BulletPlus, the BulletPlus would then automatically assign, via DHCP, the WAN IP to the attached PC2, creating a transparent connection.

![Diagram showing BulletPlus connected to PC1 and PC2]

**Step 1**

Log into the BulletPlus (Refer to Quick Start), and ensure that DHCP is enabled on the Network > LAN (edit) page.

**Step 2**

Since PC2 requires port 80 to be used as its Web server port, port 80 cannot be used on the BulletPlus, by default it retains this port for remote configuration. To change the port used by the BulletPlus, navigate to the System > Services page. For this example we are going to change it to port 8080. When changing port numbers on the BulletPlus, it is recommended to reboot the unit before continuing, remember the new WebUI port is now 8080 when you log back into the BulletPlus. (e.g. 192.168.168.1:8080).

![Diagram showing BulletPlus services settings]

**Services Status**

- FTP: Enable/Disable
- Telnet: Enable/Disable
- SSH: Enable/Disable
- Web UI: HTTP/HTTPS/HTTP/HTTPS
- Port 23
- Port 22
- Port 8080
- HTTP/445

© Microhard Systems Inc.
Appendix B: IP-Passthrough Example (Page 2 of 2)

Step 3

Now IP-Passthrough can be enabled on the BulletPlus. Under the Carrier > Settings tab, IP-Passthrough can be found. To enable this feature, select "Ethernet" from the drop down box. Once the changes are applied, whichever device is physically connected to the LAN RJ45 port, will dynamically be assigned the WAN IP Address. In this example, this would be 74.198.186.193.

The default IP address of 192.168.168.1 on the LAN is no longer available, but it is still possible to access and configure the BulletPlus on the LAN side, by using the X.X.X.1 IP Address, where the first 3 octets of the WAN IP are used in place of the X's. (e.g. 74.198.186.1, and remember the HTTP port in this example was changed to 8080).

The firewall must be configured and/or rules must be created to allow Carrier traffic. See Firewall Example for more information.

Step 4

Attach the remote device or PC to the RJ45 port of the BulletPlus. The end device has to be set up for DHCP to get an IP address from the BulletPlus. In the test/example setup we can verify this by looking at the current IP address. In the screenshot to the right we can see that the Laptop connected to the BulletPlus has a IP Address of 74.198.186.193, which is the IP address assign by the cellular carrier for the modem.

Step 5 (Optional)

IP-Passthrough operation can also be verified in the BulletPlus. Once IP-Passthrough is enabled you can access the BulletPlus WebUI by one of the following methods:

- Remotely on the WAN side (usually the internet), using the WAN IP, and the port specified for HTTP operation (or, if enabled, by using the HTTPS (443) ports), in this example with would be 74.198.186.193:8080.
- On the LAN side, by entering in the first 3 octets of the WAN IP and .1 for the fourth, so in our example 74.198.186.1:8080.

Once logged in, navigate to the Carrier > Status page. Under WAN IP Address it should look something like shown in the image to the right, 74.198.186.193 on LAN.

Step 6

The last step is to verify the remote device can be accessed. In this example a PC is connected to the RJ45 port of the BulletPlus. On this PC a simple apache web server is running to illustrate a functioning system. On a remote PC, enter the WAN IP Address of the BulletPlus into a web browser. As seen below, when the IP Address of the BulletPlus is entered, the data is passed through to the attached PC. The screen shot below shows that our test setup was successful.

This is the Web Server Running on the Microhard Laptop.

If you can read this, it means that the IP-Passthrough or Port Forwarding exercise works!
Appendix C: Port Forwarding Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the BulletPlus is to access connected devices remotely. In order to do this, the BulletPlus must be told how to deal with incoming traffic, where to send it to. To accomplish this there are three options:

- IP-Passthrough
- Port Forwarding
- DMZ (a type of Port Forwarding)

In the previous section we illustrated how to use and setup IP-Passthrough. In this section we will talk about port forwarding. Port forwarding is ideal when there are multiple devices connected to the BulletPlus, or if other features of the BulletPlus are required (Serial Ports, Firewall, GPS, etc). In port forwarding, the BulletPlus looks at each incoming Ethernet packet on the WAN and by using the destination port number, determines where it will send the data on the private LAN. The BulletPlus does this with each and every incoming packet.

DMZ (a form of port forwarding) is useful for situations where there are multiple devices connected to the BulletPlus, but all incoming traffic is destined for a single device. It is also popular to use DMZ in cases where a single device is connected but several ports are forwarded and other features of the BulletPlus are required, since in passthrough mode all of these features are lost.

Consider the following example. A user has a remote location that has several devices that need to be accessed remotely. The User at PC1 can only see the BulletPlus directly using the public static IP assigned by the wireless carrier, but not the devices behind it. In this case the BulletPlus is acting a gateway between the Cellular Network and the Local Area Network of its connected devices. Using port forwarding we can map the way that data passes through the BulletPlus.

Step 1

Log into the BulletPlus (Refer to Quick Start), and ensure that the Firewall is enabled. This can be found under Firewall > General. Also ensure that sufficient Rules or IP lists have been setup to allow specific traffic to pass through the BulletPlus. See the Firewall Example in the next Appendix for information on how to allow connections from an IP or to open ports. Once that is complete, remember to “Submit” the changes.
Appendix C: Port Forwarding Example (Page 2 of 2)

Step 2

Determine which external ports (WAN) are mapped to which internal IP Addresses and Ports (LAN). It is important to understand which port, accessible on the outside, is connected or mapped to which devices on the inside. For this example we are going to use the following ports, in this case it is purely arbitrary which ports are assigned, some systems may be configurable, other systems may require specific ports to be used.

<table>
<thead>
<tr>
<th>Description</th>
<th>WAN IP</th>
<th>External Port</th>
<th>Internal IP</th>
<th>Internal Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>BulletPlus WebUI</td>
<td>74.198.186.193</td>
<td>80</td>
<td>192.168.0.1</td>
<td>80</td>
</tr>
<tr>
<td>PC2 Web Server</td>
<td>74.198.186.193</td>
<td>8080</td>
<td>192.168.0.20</td>
<td>80</td>
</tr>
<tr>
<td>PLC Web Server</td>
<td>74.198.186.193</td>
<td>8081</td>
<td>192.168.0.30</td>
<td>80</td>
</tr>
<tr>
<td>PLC Modbus</td>
<td>74.198.186.193</td>
<td>10502</td>
<td>192.168.0.30</td>
<td>502</td>
</tr>
<tr>
<td>Camera Web Server</td>
<td>74.198.186.193</td>
<td>8082</td>
<td>192.168.0.40</td>
<td>80</td>
</tr>
</tbody>
</table>

Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this is fine because they are located on different IP addresses, and the different external ports mapped by the BulletPlus (80, 8080, 8081, 8082), will send the data to the intended destination.

Step 3

Create a rule for each of the lines above. A rules does not need to be created for the first line, as that was listed simply to show that the external port 80 was already used, by default, by the BulletPlus itself. To create port forwarding rules, Navigate to the Firewall > Port Forwarding menu. When creating rules, each rules requires a unique name, this is only for reference and can be anything desired by the user. Click on the “Add Port Forwarding” button to add each rule to the BulletPlus.

Once all rules have been added, the BulletPlus configuration should look something like what is illustrated in the screen shot to the right. Be sure to “Submit” the Port Forwarding list to the BulletPlus.

For best results, reboot the BulletPlus.

Step 4

Configure the static addresses on all attached devices. Port forwarding required that all the attached devices have static IP addresses, this ensure that the port forwarding rules are always correct, as changing IP addresses on the attached devices would render the configured rules useless and the system will not work.

Step 5

Test the system. The devices connected to the BulletPlus should be accessible remotely. To access the devices:

For the Web Server on the PC, use a browser to connect to 74.198.186:193:8080, in this case the same webservice is running as in the IP-Passthrough example, so the result should be as follows:

If you can read this, it means that the IP-Passthrough or Port Forwarding exercise works!

To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.
Appendix D: VPN Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the BulletPlus is to access connected devices remotely. In addition to Port Forwarding and IP-Passthrough, the BulletPlus has several VPN capabilities, creating a tunnel between two sites, allowing remote devices to be accessed directly.

VPN allows multiple devices to be connected to the BulletPlus without the need to individually map ports to each device. Complete access to remote devices is available when using a VPN tunnel. A VPN tunnel can be created by using two BulletPlus devices, each with a public IP address. At least one of the modems require a static IP address. VPN tunnels can also be created using the BulletPlus to existing VPN capable devices, such as Cisco or Firebox.

Example: BulletPlus to BulletPlus (Site-to-Site)

Step 1
Log into each BulletPlus (Refer to Quick Start) and ensure that the Firewall is configured. This can be found under Firewall > General. Ensure that sufficient Rules or IP lists have been setup to allow specific traffic to pass through the BulletPlus. Once that is complete, remember to “Apply” the changes.

Step 2
Configure the LAN IP and subnet for each BulletPlus. The subnets must be different and cannot overlap.
Appendix D: VPN Example (Page 2 of 2)

Step 3

Add a VPN Gateway to Gateway tunnel on each BulletPlus.

<table>
<thead>
<tr>
<th>System</th>
<th>Network</th>
<th>Carrier</th>
<th>Wireless</th>
<th>Firewall</th>
<th>VPN</th>
<th>Router</th>
<th>Serial</th>
<th>I/O</th>
<th>GPS</th>
<th>Apps</th>
<th>Diag</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Gateway To Gateway</td>
<td>L2TP Client</td>
<td>OpenVPN Server</td>
<td>OpenVPN Client</td>
<td>L2TP Users</td>
<td>Certificates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gateway To Gateway</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Status</td>
<td>Phase2 Enc/Auth/Grp</td>
<td>Interface</td>
<td>Local Group</td>
<td>Remote Group</td>
<td>Remote Gateway</td>
<td>RX/TX Bytes</td>
<td>Tunnel Text</td>
<td>Config</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Site A

Site B

Step 4

Submit changes to both units. It should be possible to ping and reach devices on either end of the VPN tunnel if both devices have been configured correctly and have network connectivity.
Appendix E: Firewall Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the BulletPlus is to access connected devices remotely. Security plays an important role in M2M deployments as in most cases the modem is publically available on the internet. Limiting access to the BulletPlus is paramount for a secure deployment. The firewall features of the BulletPlus allow a user to limit access to the BulletPlus and the devices connected to it by the following means:

- Customizable Rules
- MAC and/or IP List
- ACL (Access Control List) or Blacklist using the above tools.

Consider the following example. An BulletPlus is deployed at a remote site to collect data from an end device such as a PLC or RTU connected to the serial DATA port (Port 20001). It is required that only a specific host (Host A) have access to the deployed BulletPlus and attached device, including the remote management features.

Step 1

Log into the BulletPlus (Refer to Quick Start). Navigate to the Firewall > General tab as shown below and block all Carrier traffic by setting the Carrier Request to Block, and disable Carrier Remote Management. Be sure to Apply the settings. At this point it should be impossible to access the BulletPlus from the Cellular Connection.
Step 2

Under the Rules tab we need to create two new rules. A rule to enable Host A access to the Remote Management Port (TCP Port 80), and another to access the device attached to the serial port (TCP Port 20001).

**Rule 1**

<table>
<thead>
<tr>
<th>Firewall Rules Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
</tr>
<tr>
<td>ACTION</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Source IPs</td>
</tr>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>Destination IPs</td>
</tr>
<tr>
<td>Destination Port</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

**Rule 2**

<table>
<thead>
<tr>
<th>Firewall Rules Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
</tr>
<tr>
<td>ACTION</td>
</tr>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Source IPs</td>
</tr>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>Destination IPs</td>
</tr>
<tr>
<td>Destination Port</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
</tbody>
</table>

After each rule is created be sure to click the *ADD Rule* button, once both rules are created select the *Submit* button to write the rules to the BulletPlus. The *Firewall Rules Summary* should look like what is shown below.

<table>
<thead>
<tr>
<th>Firewall Rules Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Rule_Name</td>
</tr>
<tr>
<td>Device</td>
</tr>
</tbody>
</table>

Step 3

Test the connections. The BulletPlus should only allow connections to the port specified from the Host A. An alternate means to limit connections to the BulletPlus to a specific IP would have been to use the MAC-IP List Tool. By using Rules, we can not only limit specific IP’s, but we can also specify ports that can be used by an allowed IP address.
Appendix F: Port Forwarding with IP-Passthrough (Page 1 of 2)

When the BulletPlus is set into IP-Passthrough mode the modem passes all traffic onto the connected device with the exception of WebUI, SNMP and internal port forwarding rules. The following example shows how to use Port Forwarding to utilize the internal Iperf capabilities of the modem while retaining the remaining features of IP-Passthrough.

Step 1: Enable IP-Passthrough

After IP pass-through mode is enabled the IP address of LAN network is changed to 184.151.218.1

Step 2. Add Port Forwarding

A) Specify the internal IP and port of port forwarding. We are demonstrating forward port 5001 which is Iperf's default port.

B) Allow incoming traffic. Method 1: Allow all incoming traffic on carrier. (Not recommended)
Method 2: Specify which source IP Address(s) are allowed.

The incoming request on port 5001 from the carrier will not forward to the device behind the modem, the Iperf server running on the modem will now get this incoming request.
Appendix G: Troubleshooting

Below is a number of the common support questions that are asked about the BulletPlus. The purpose of the section is to provide answers and/or direction on how to solve common problems with the BulletPlus.

Question: Why can’t I connect to the internet/network?
Answer: To connect to the internet a SIM card issued by the Wireless Carrier must be installed and the APN programmed into the Carrier Configuration of the BulletPlus. For instructions of how to log into the BulletPlus refer to the Quick Start.

Question: What is the default IP Address of the BulletPlus?
Answer: The default IP address for the LAN (RJ45 connector on the back of the unit) is 192.168.168.1.

Question: What is the default login for the BulletPlus?
Answer: The default username is admin, the default password is admin.

Question: What information do I need to get from my wireless carrier to set up the BulletPlus?
Answer: The APN is required to configure the BulletPlus to communicate with a wireless carrier. Some carriers also require a username and password. The APN, username and password are only available from your wireless carrier.

Newer units may support an AUTO APN feature, which will attempt to determine the APN from a preconfigured list of carriers and commonly used APN’s. This is designed to provide quick network connectivity, but will not work with private APN’s. Success with AUTO APN will vary by carrier.

Question: How do I reset my modem to factory default settings?
Answer: If you are logged into the BulletPlus navigate to the System > Maintenance Tab. If you cannot log in, power on the BulletPlus and wait until the status LED in on solid (not flashing). Press and hold the CONFIG button until the unit reboots (about 8-10 seconds).

Question: I can connect the Carrier, but I can’t access the Internet/WAN/network from a connected PC?
Answer: Ensure that you have DHCP enabled or manually set up a valid IP, Subnet, Gateway and DNS set on the local device.

Question: I connected a device to the serial port of the BulletPlus and nothing happens?
Answer: In addition to the basic serial port settings, the IP Protocol Config has to be configured. Refer to the Serial Configuration pages for a description of the different options.
Appendix G: Troubleshooting

Question: How do I access the devices behind the modem remotely?
Answer: To access devices behind the BulletPlus remotely, several methods can be used:

A. IP Passthrough - The BulletPlus is transparent and the connected device can be accessed directly. Refer to The IP-Passthrough Appendix for a detailed example of how this may be deployed.
B. Port Forwarding/DMZ - Individual external WAN ports are mapped to internal LAN IP’s and Ports. See the Port-Forwarding Appendix for a detailed example.
C. VPN - A tunnel can be created and full access to remote devices can be obtained. Required the use of multiple modems or VPN routers. See the VPN Appendix on an example of how to set up a VPN.

Question: I have Internet/Carrier access but I cannot ping the device remotely?
Answer: Ensure that appropriate Rules have been created in the Firewall to allow traffic.

Question: I'm using IP-Passthrough but the serial ports won't work?
Answer: When using IP-Passthrough, the Carrier IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result serials port will not work. The only port not being passed through is the remote management port (default port 80), which can be changed in the security settings.

Question: I'm using IP-Passthrough but the modem won't take my Firewall settings?
Answer: When using IP-Passthrough, the Carrier IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result the firewall settings have no effect on the unit, and is automatically disabled.

Question: Why does my modem reset every 10 minutes (or other time)?
Answer: There are a number of processes in the BulletPlus that ensure that the unit is communicating at all times, and if a problem is detected will reboot the modem to attempt to resolve any issues:

1. Keepalive - Attempts to contact a configured host on a defined basis. Will reboot modem if host is unreachable. Enabled by default to attempt to ping 8.8.8.8. May need to disable on private networks, or provide a reachable address to check. Access via System > Keepalive.
2. Local Device Monitor - The BulletPlus will monitor a local device, if that device is not present the BulletPlus may reboot. Apps > LocalMonitor.

Question: How do I set up VPN?
Answer: Refer to the VPN Appendix for an example.