Operating Manual

BulletPlus

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

Document: BulletPlus.Operating Manual.v1.2.pdf
FW: v1.3.0 Build 1012

April 2016

150 Country Hills Landing NW
Calgary, Alberta
Canada T3K 5P3

Phone: (403) 248-0028
Fax: (403) 248-2762
www.microhardcorp.com

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 MICROHARD SYSTEMS INC. EXPRESS WARRANTY TO BUYER CONSTITUTES MICROHARD SYSTEMS INC. SOLE LIABILITY AND THE BUYER'S SOLE REMEDIES. EXCEPT AS THUS PROVIDED, MICROHARD SYSTEMS INC. DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PROMISE.

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 ANYDAMAGES 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, or in, 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.

© Microhard Systems Inc.

Important User Information (continued)

Regulatory Requirements / Exigences Réglementaires

WARNING

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.

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-localisés en conjonction avec toute autre antenne ou transmetteur.

WARNING

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.

Réglementation de la FCC permettra à 36dBm Puissance isotrope 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.

WARNING

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.

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 fournies 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' installation et de câblage des lignes directrices spécifiques pour la classe 1 Division 2 codes , communiquer avec la CSA International.

Revision History

Revision	Description	Initials	Date
1.0	Preliminary. (Firmware v1.3.0-r1009-28)	PEH	Nov 2015
1.1	Updated to firmware v1.3.0-r1010. Added Bandwidth, Cloud Filter, Webfilter, MultiWAN, GRE. Misc updates to screenshots & formatting.	PEH	Dec 2015
1.2	Updated to firmware v1.3.0-r1012. Misc corrections, added VRRP, updated Data Usage, Carrier Settings.	PEH	Apr 2016

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 BulletPlus Connectors & Indicators 20
3.1.2.1 Front & Top 20
3.1.2.2 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
SSH 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
MAC Binding 39
4.2.3 WAN 40
4.2.4 DDNS 42
4.2.5 Routes 43
4.2.6 VRRP (Virtual Router Redundancy Protocol) 45
4.2.7 Ports (Switch) 46
4.2.8 Bandwidth (Throttling Control) 47
4.2.9 Device List 48
4.2.10 Cloud Filter (Content/Security Filter) 49
4.2.11 WebFilter (MAC/Network Content Filter) 50
4.2.12 MultiWAN 52

Table of Contents

4.3 Carrier 55
4.3.1 Status 55
4.3.2 Settings 56
Dual Cards Management 57
APN 58
4.3.3 SMS 60
4.3.4 SMS Config 60
SMS Commands 60
SMS Alerts 62
4.3.5 Data Usage 64
Data Usage History 67
4.4 Wireless 68
4.4.1 Status 68
4.4.2 Radio1 69
Radio1 Phy Configuration 69
Radio Virtual Interface 72
4.4.3 Hotspot 75
4.5 Firewall 79
4.5.1 Summary 79
4.5.2 General 80
4.5.3 Port Forwarding 82
4.5.4 MAC-IP List 84
4.5.5 Rules 86
4.5.6 Firewall Default 88
4.6 VPN 89
4.6.1 Summary 89
4.6.2 Gateway to Gateway 90
4.6.3 Client to Gateway (L2TP Client) 95
4.6.4 GRE 97
4.6.5 L2TP Users 100
4.6.6 Certificates 101
4.7 Router 102
4.7.1 RIPV2 102
4.7.2 OSPF 103
4.8 Serial 104
4.8.1 Summary 104
4.8.2 Settings 105
Data Baud Rate 106
IP Protocol Config 108
TCP Client 108
TCP Server 108
TCP Client/Server 109
UDP Point-to-Point 109
SMTP Client 109
PPP 110
GPS Transparent Mode 111
4.9 I/O 112
4.9.1 Settings 112

Table of Contents

4.10 GPS 114
4.10.1 Location 114
4.10.2 Settings 115
4.10.3 Report 116
4.10.4 GPSGate 118
4.10.5 Recorder 121
4.10.6 Load Record 123
4.10.7 TAIP 125
4.11 Apps 127
4.11.1 Modbus 127
4.11.1.1 TCP Modbus 127
4.11.1.2 Serial (COM) Modbus 129
4.11.1.3 Modbus Data Map 130
4.11.2 Netflow Report 131
4.11.3 Local Monitor 132
4.11.4 Event Report 134
4.11.4.1 Configuration 134
4.11.4.2 Message Structure 135
4.11.4.2 Message Payload 136
4.11.5 Websocket 137
4.12 Diag 139
4.12.1 Ping 139
4.12.2 Traceroute 139
4.12.3 Iperf 140
4.13 Admin 142
4.13.1 Users 142
4.13.2 Authentication (RADIUS) 144
4.13.3 NMS 145
4.13.4 SNMP 149
4.13.5 Discovery 152
4.13.6 Logout 153

5.0 AT Command Line Interface 154
5.1 AT Command Overview 154
5.1.1 Serial Port 154
5.1.2 Telnet 155
5.2 AT Command Syntax 156
5.3 Supported AT Commands 157

Appendices 195
Appendix A: Serial Interface 195
Appendix B: IP-Passthrough Example 196
Appendix C: Port Forwarding Example 198
Appendix D: VPN (Site to Site) Example 200
Appendix E: Firewall Rules Example 202
Appendix F: Troubleshooting 204

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^{o}C to +85^{o}C)

1.0 Overview

1.2 Specifications

BulletPlus

BulletPlus Supported Bands: (North America)
LTE FDD (Bands 1-5,7,8,13,17,18,19,20)
UMTS | DC-HSPA+ (Bands 1,2,4,5,8)
GSM | GPRS | EDGE (Bands 2,3,5,8)
3GPP Protocol Stack Release 9

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 85.6kbps

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*: (*Future) 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)
BulletPlus	120	170
BulletPlus + Serial Data	142	180
BulletPlus + Ethernet	155	195
BulletPlus Peak	230	305

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, DHCP, 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)

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.

SIM Card Slot (s)

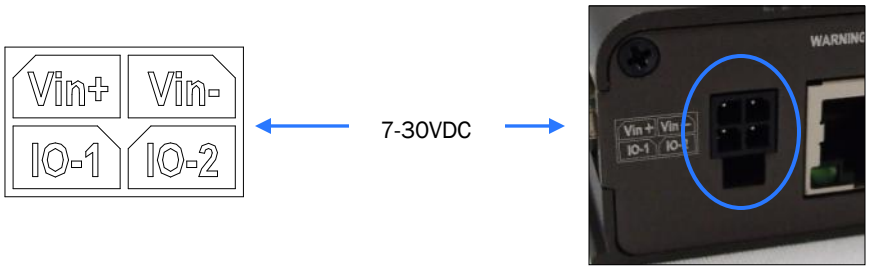
2.2 Getting Started with Cellular

✓ Connect the Antenna's to the applicable ***ANTENNA*** jack's of the BulletPlus.

✓ 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.

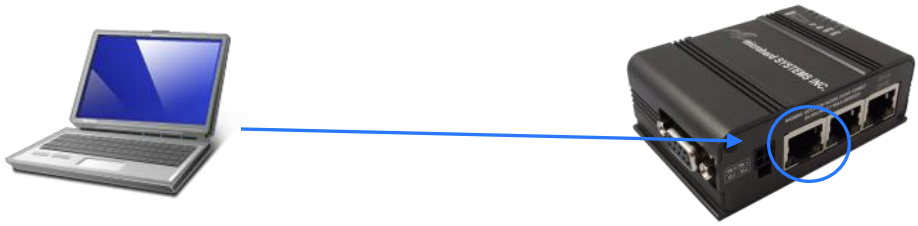
Use the MHS-supplied power adapter or an equivalent power source.

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

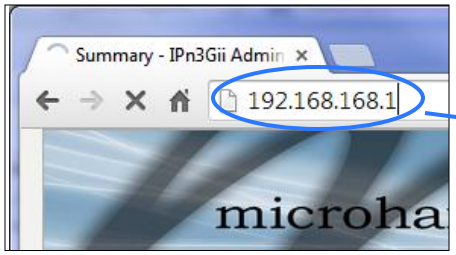


2.0 Quick Start

✓ 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.



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

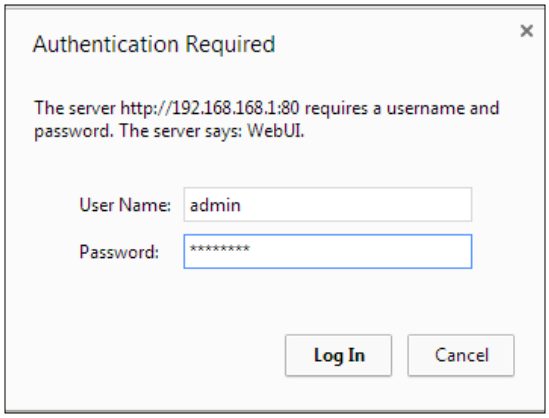


192.168.168.1

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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



The Factory default login:

User name: **admin**
Password: **admin**

The factory default login:

User name: admin
Subnet: admin

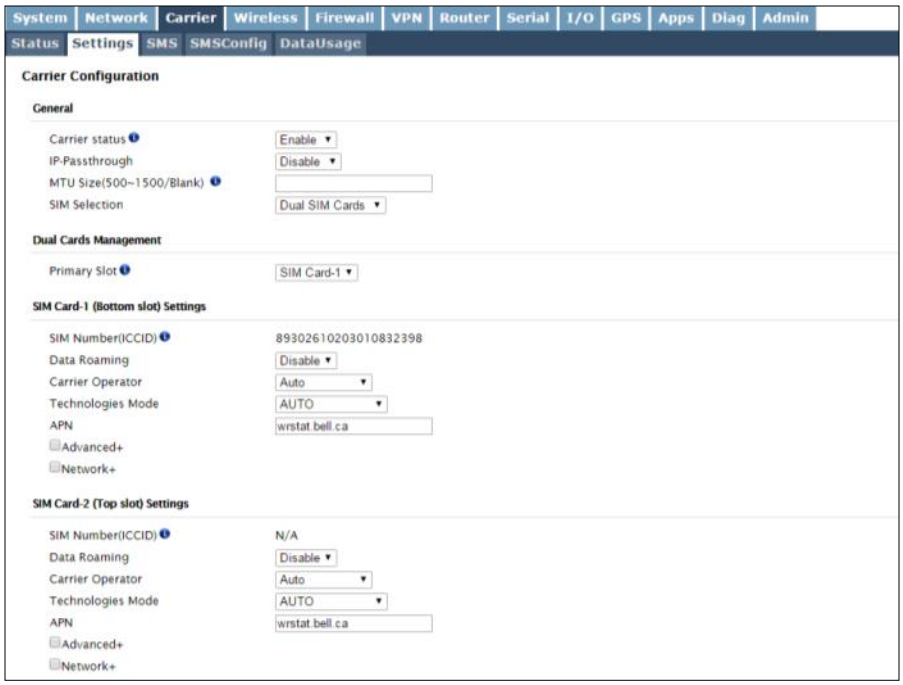
It is always a good idea to change the default admin login for future security.

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.

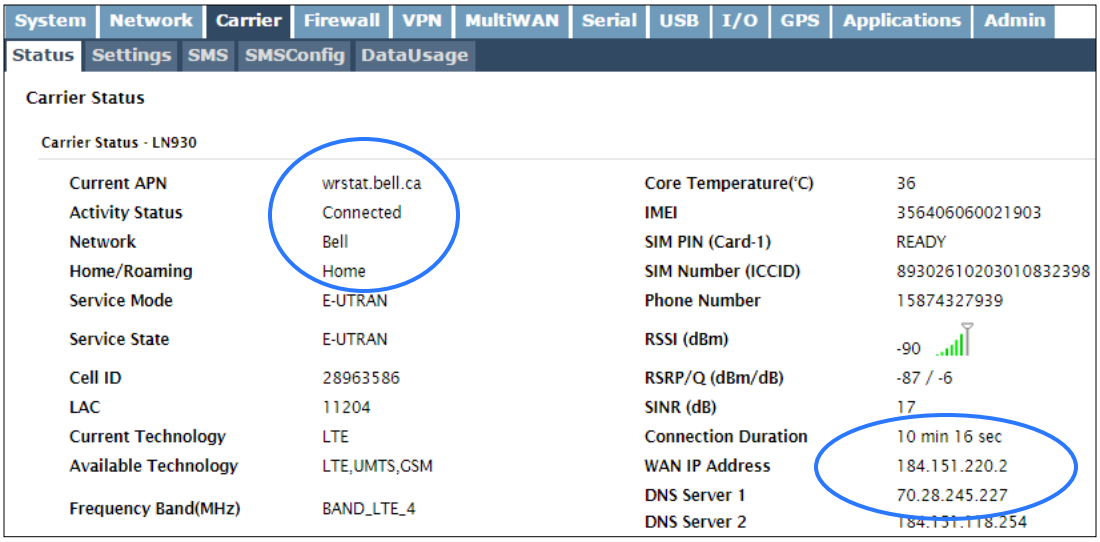


✓ Once the APN and any other required information is entered to connect to your carrier, click on "Submit".

✓ *Verizon Models may not require a APN and should Auto Connect if a valid SIM card is inserted.*

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 you 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 the default passwords are changed.

✓ **Ensure that all default passwords are changed to limit access to the modem.**

Set up appropriate firewall rules to block unwanted incoming data.

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

3.0 Hardware Features

3.1 BulletPlus

The BulletPlus is a fully-enclosed unit ready to be interfaced to external devices.

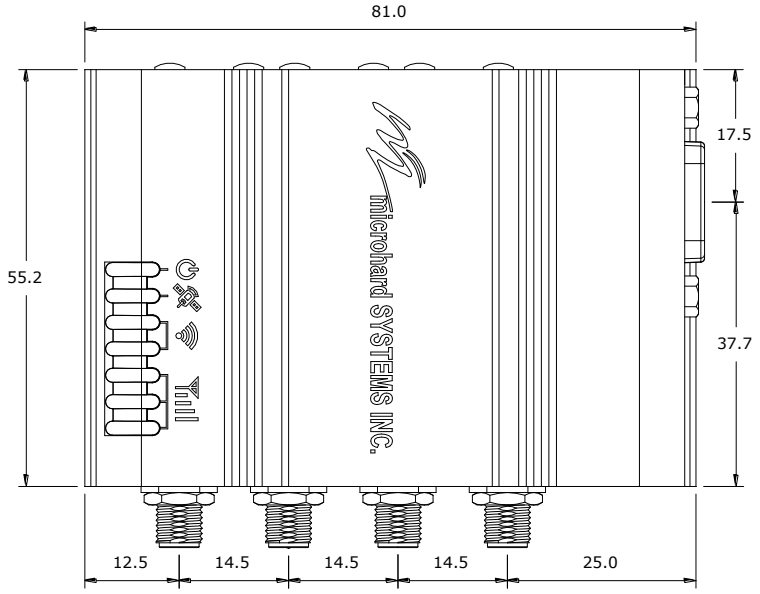
Image 3-1: BulletPlus

The BulletPlus Hardware Features Include:

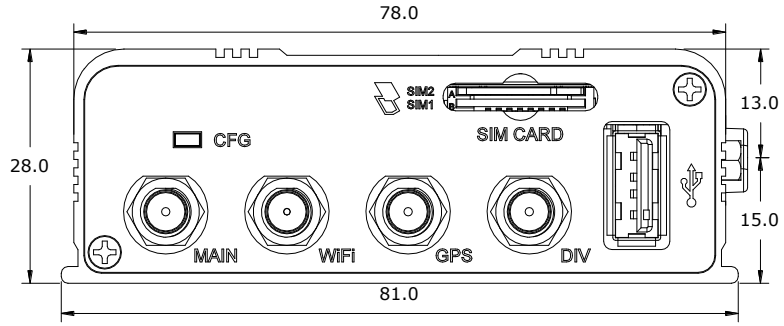
- Standard Connectors for:
  - 3x 10/100 Ethernet Ports (RJ45 - 1xWAN / 2xLAN)
  - Data Port (RS232/DB9)
  - 4-Pin: MATE-N-LOK Type Connector for Power / I/O 1/2
  - Cellular Antenna (SMA Female Antenna Connection x2)
  - GPS Antenna (SMA Female Antenna Connection)
  - WiFi Antenna (RP-SMA Female Antenna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

3.0 Hardware Features

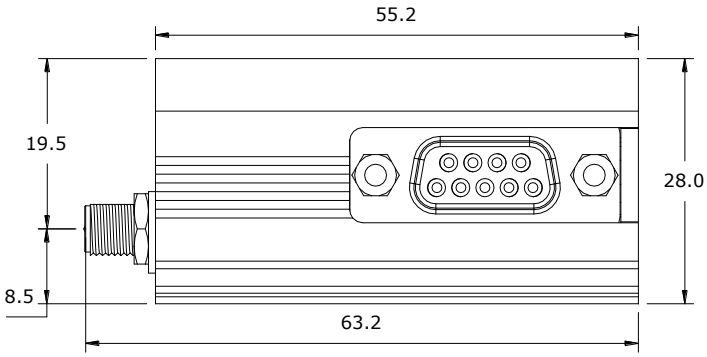
3.1.1 Mechanical Drawings



Drawing 3-1: BulletPlus Top View Dimensions



Drawing 3-2: BulletPlus Back View Dimensions

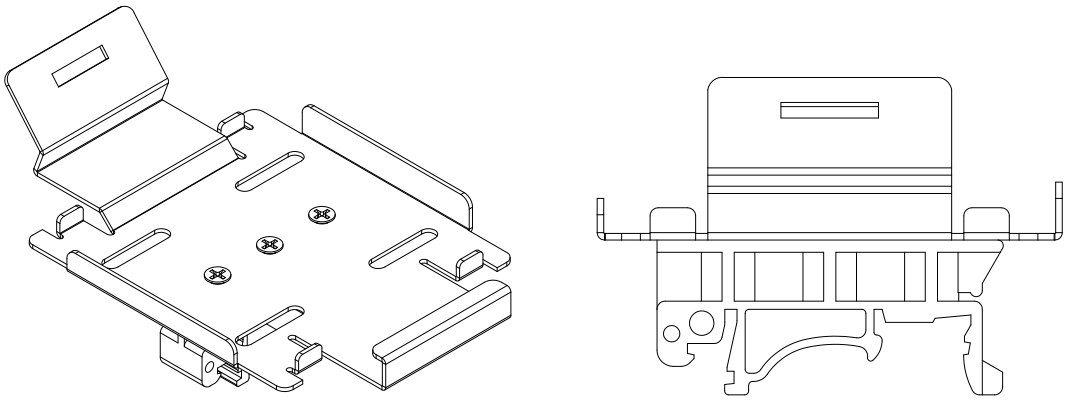


Drawing 3-3: BulletPlus Side View Dimensions

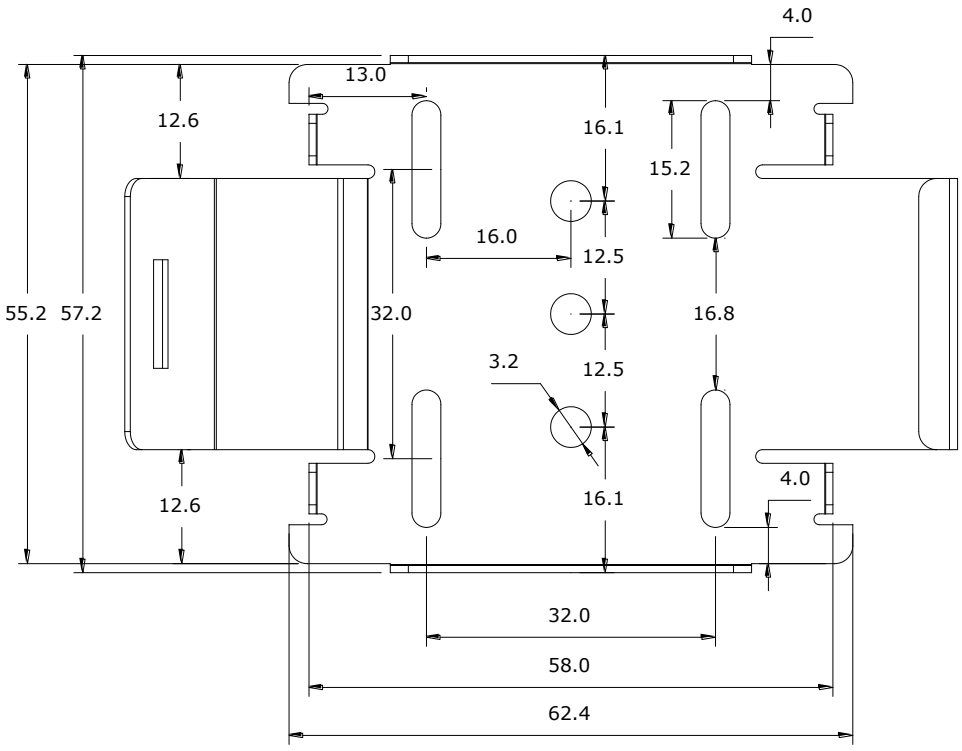
Note: All dimension units: Millimeter

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

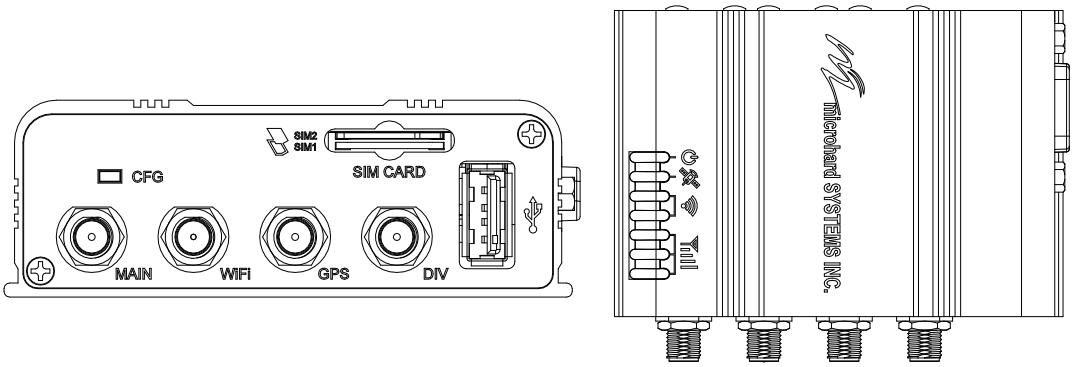
Note: All dimension units: Millimeter

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.



Drawing 3-6: Bullet Front & Top View

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 that 15 seconds the button will be ignored.

If the unit has been powered-up for some time (>1 minute), depressing the CFG Button for 8 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.

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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.

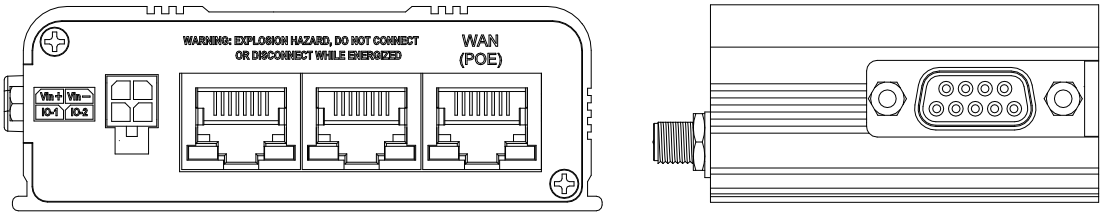
Signal (dBm)	RSSI1	RSSI2	RSSI3
(-85, 0]	ON	ON	ON
(-90, -85]	ON	ON	FLASH
(-95, -90]	ON	ON	OFF
(-100, -95]	ON	FLASH	OFF
(-105, -100]	ON	OFF	OFF
(-109, -105]	FLASH	OFF	OFF
Other	SCANNING	SCANNING	SCANNING

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.



Drawing 3-7: BulletPlus Rear & Side View

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.

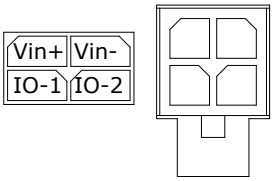
Name	Data Port	Input or Output
DCD	1	O
RXD	2	O
TXD	3	I
DTR	4	I
SG	5	
DSR	6	O
RTS	7	I
CTS	8	O
RING	9	O

Table 3-2: Data RS232 Pin Assignment

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

Ethernet RJ45 Connector Pin Number								
Source Voltage	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
9 - 30 Vdc	Data	Data	Data	DC+	DC+	Data	DC-	DC-

Table 3-3: Ethernet PoE Connections



4.0 Configuration

4.0 Web User Interface

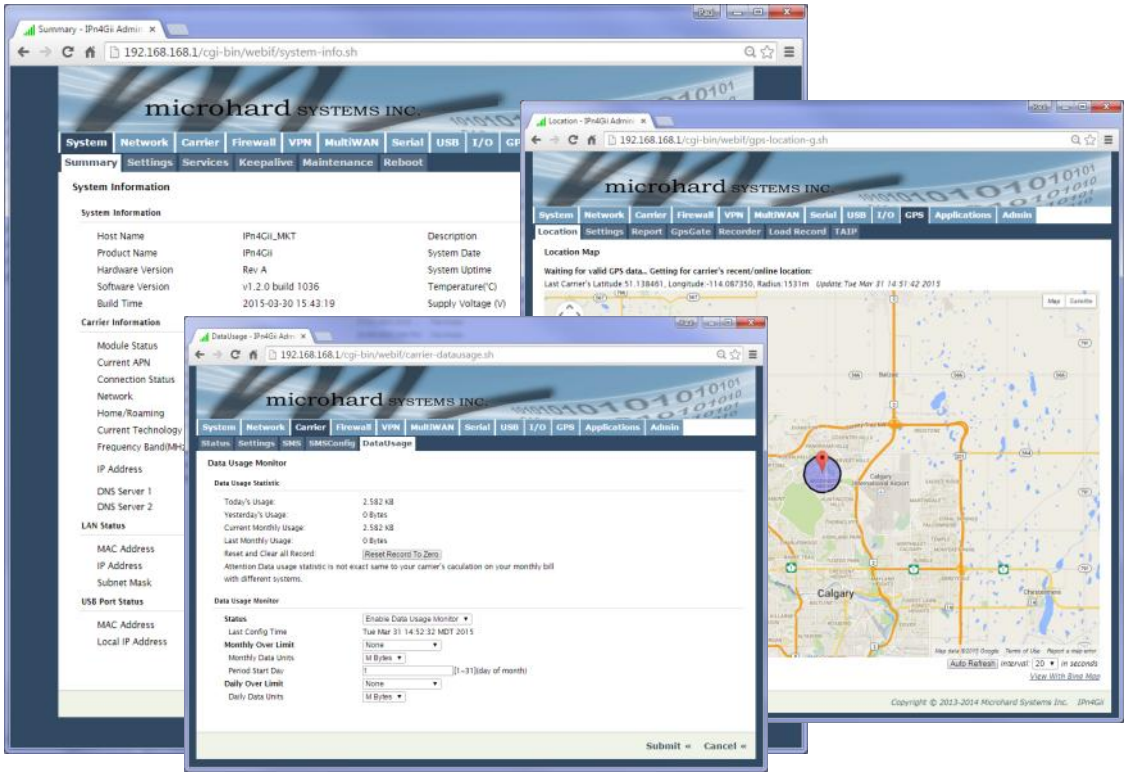


Image 4-0-1: WebUI

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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.

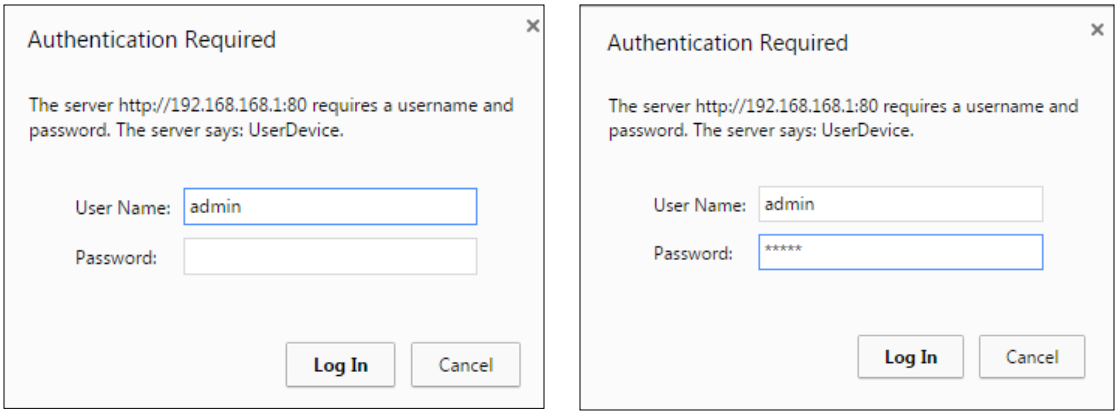


Image 4-0-2: Logon Window

For security, do not allow the web browser to remember the User Name or Password.

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

The default password is: **admin**

It is advisable to change the login Password. Do not FORGET the new password as it cannot be recovered.

Note that the password is case sensitive. It may 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.

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 - Remotely 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.

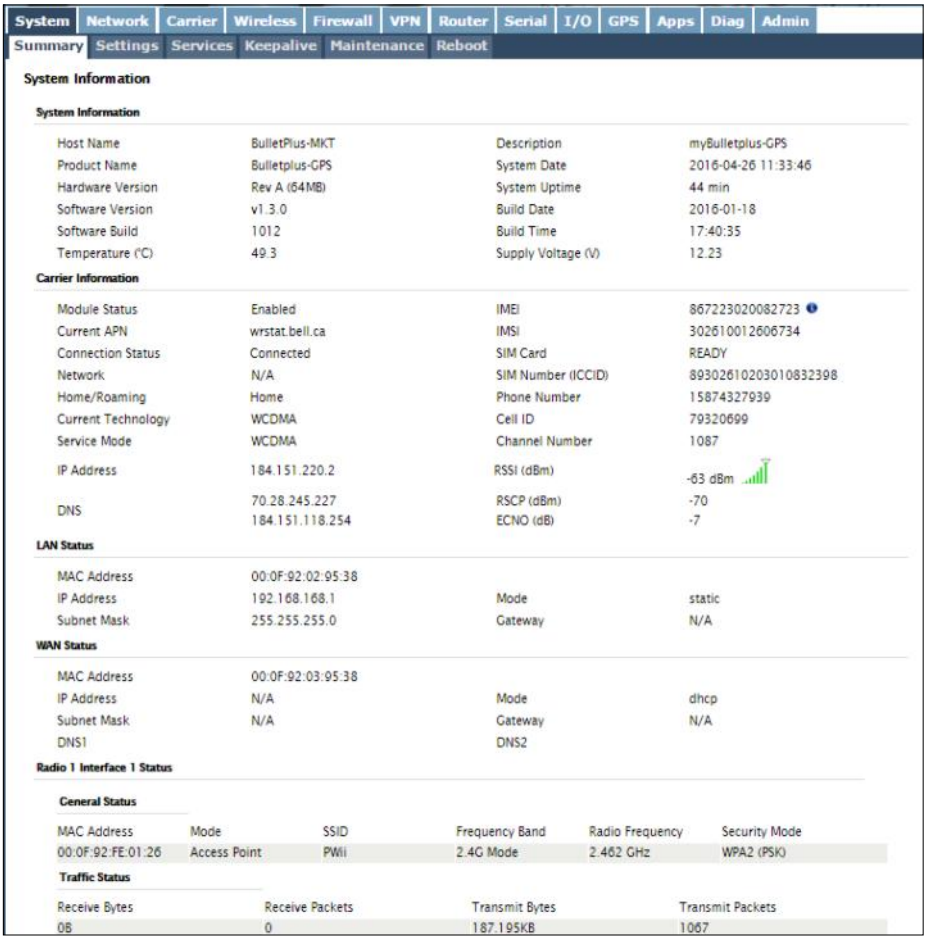


Image 4-1-1: System Info Window

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.

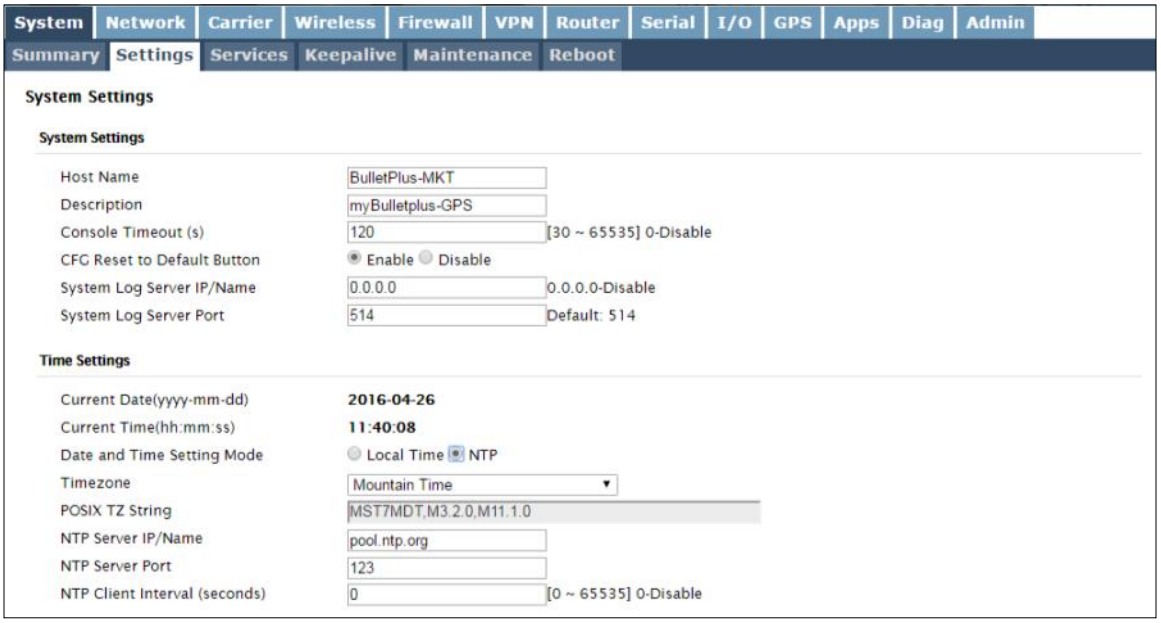


Image 4-1-2: System Settings > System Settings

Host Name/Description

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.

Values (characters)

BulletPlus **(varies)**

up to 30 characters

Console Timeout (s)

This value determines when a console connection (made via Console Port or Telnet) will timeout after becoming inactive.

Values (seconds)

60
0-65535

CFG Reset to Default Button

Enabled by default, when the CFG button on the front of the BulletPlus is held down for 10s while the unit is powered up, the unit will reset and all settings will be reset to factory defaults. When disabled the unit will reset, but the settings will not be overwritten.

Values (Selection)

Enable
Disable

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 or computer systems with a centralized, referenced server. This can help ensure all systems on a network have the same time and date.

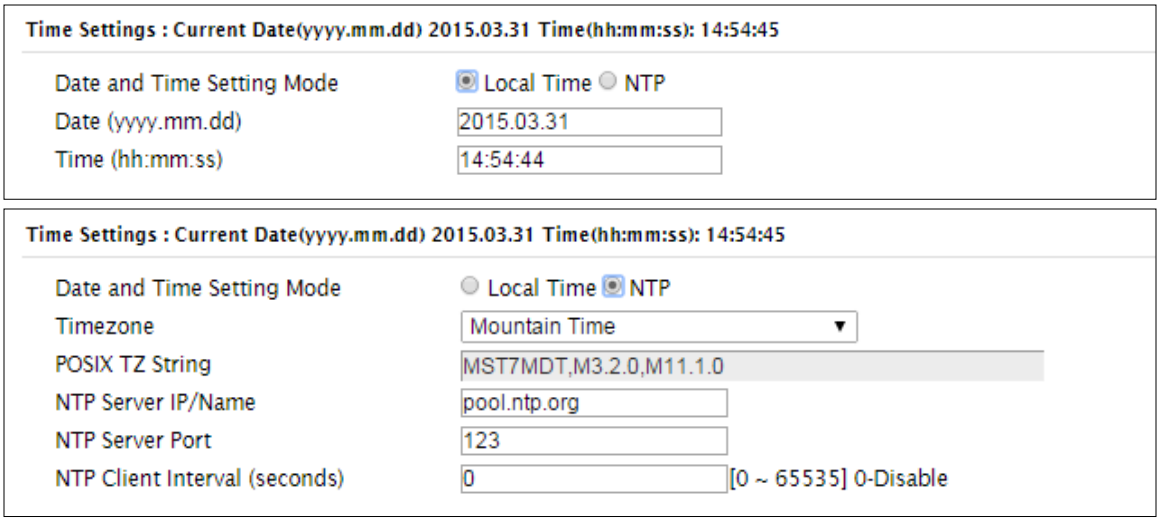


Image 4-1-3: System Settings > Time Settings

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.

Values (selection)

Use Local Time Source
Synchronize Date And Time Over Network

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

Time	
The time may be entered in this field. Note that the entered value is lost should the BulletPlus lose power for some reason.	**Values (hh:mm:ss)** **11:27:28** *(varies)*
Timezone	
If connecting to a NTP time server, specify the timezone from the dropdown list.	**Values (selection)** **User Defined** (or out of date)
POSIX TZ String	
This displays the POSIX TZ String used by the unit as determined by the timezone setting.	**Values (read only)** *(varies)*
NTP Server	
Enter the IP Address or domain name of the desired NTP time server.	**Values (address)** **pool.ntp.org**
NTP Port	
Enter the IP Address or domain name of the desired NTP time server.	**Values (port#)** **123**
NTP Client Interval	
By default the modem only synchronizes the time and date during system boot up (default: 0), but it can be modified to synchronize at a regular interval. *This process does consume data and should be set accordingly.*	**Values (seconds)** **0**

4.0 Configuration

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.

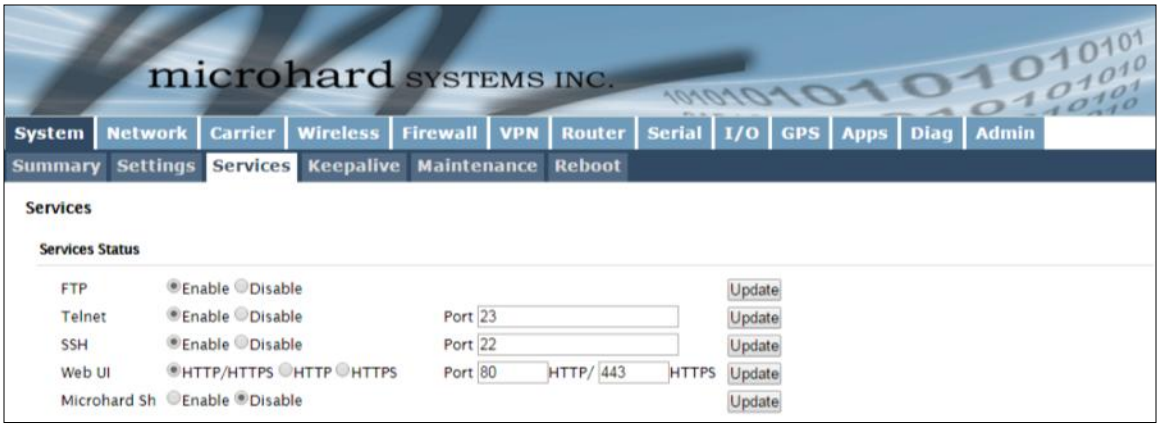


Image 4-1-5: System > Services

FTP

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

Values (port)

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)

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)

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)

HTTP/HTTPS
HTTP
HTTPS

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.

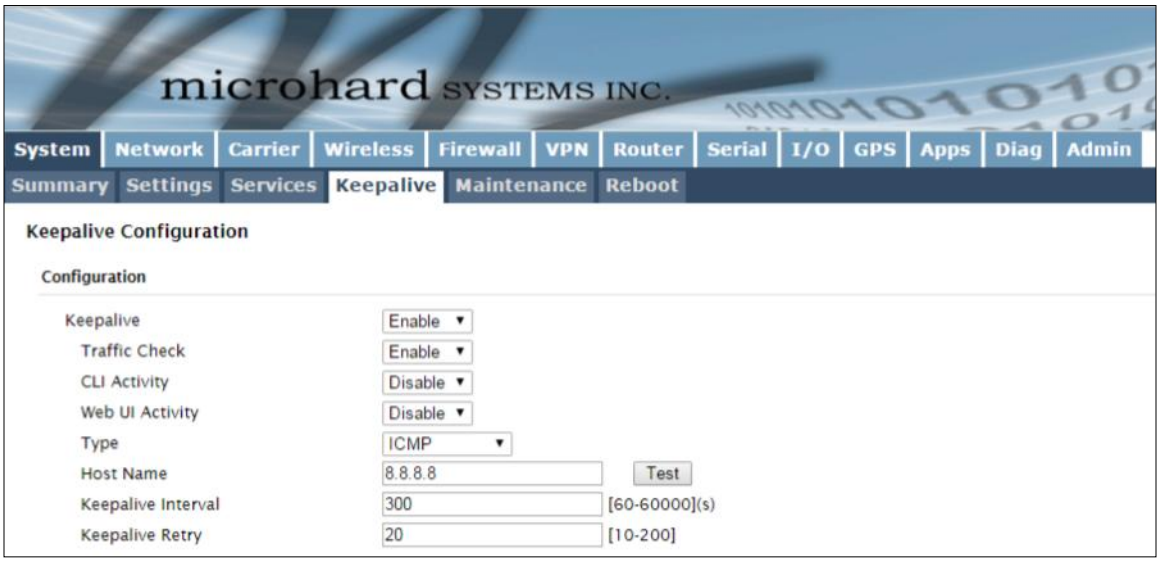


Image 4-1-6: Carrier > Keepalive

Keep Alive

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.

Values (Selection)

Enable / Disable

Traffic Check

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.

Values (Selection)

Enable / Disable

CLI Activity

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.

Values (Selection)

Enable / Disable

Web UI Activity

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.

Values (Selection)

Enable / Disable

4.0 Configuration

Type

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 "dsloopup" request to a DNS server

Values (Selection)

ICMP
HTTP
DNS Lookup

Host Name

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

Values (IP or Domain)

8.8.8.8

Keepalive Interval

The Interval value determines the frequency, or how often, the unit will send out PING messages to the Host.

Values (seconds)

60

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.

Values (number)

10

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.

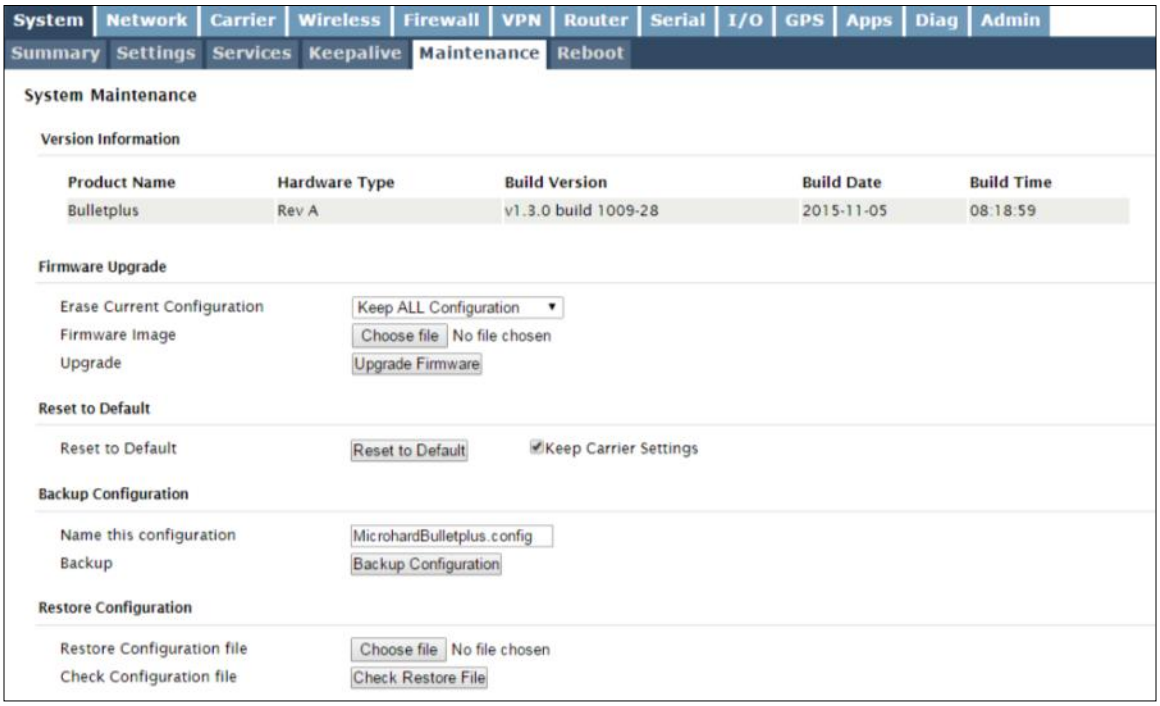


Image 4-1-7: Maintenance > Firmware Upgrade

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 the 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.

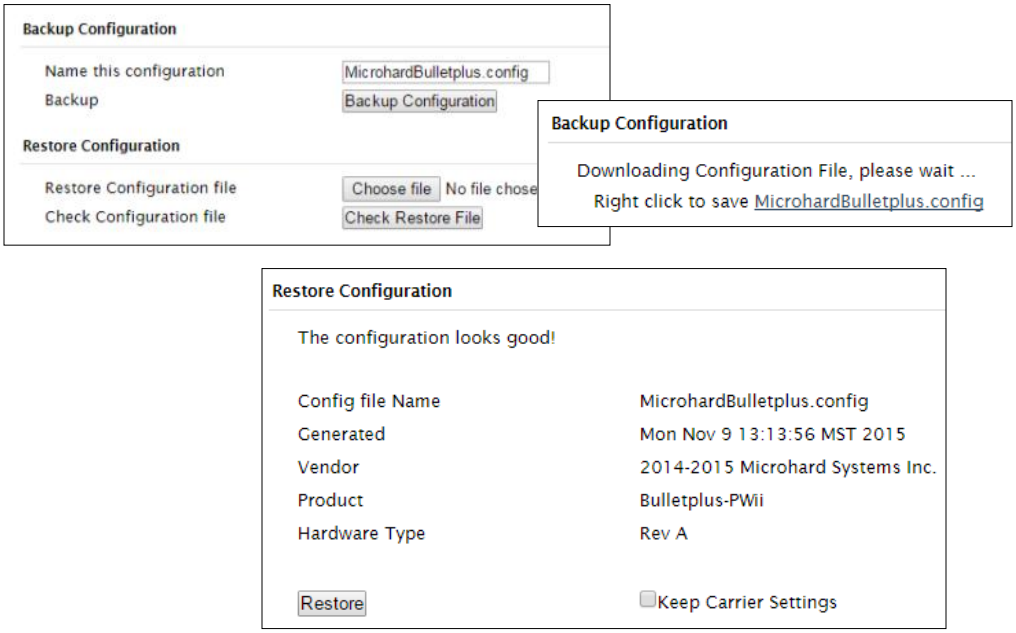


Image 4-1-8: Maintenance > Reset to Default / Backup & Restore Configuration

Name this Configuration / Backup Configuration

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

Restore Configuration file / Check Restore File / Restore

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 'OK, reboot now' is provided. Once pressed, the unit immediately reboots and starts its boot up procedure.

Image 4-1-9: System > Reboot

4.0 Configuration

4.2 Network

4.2.1 Network > Summary

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

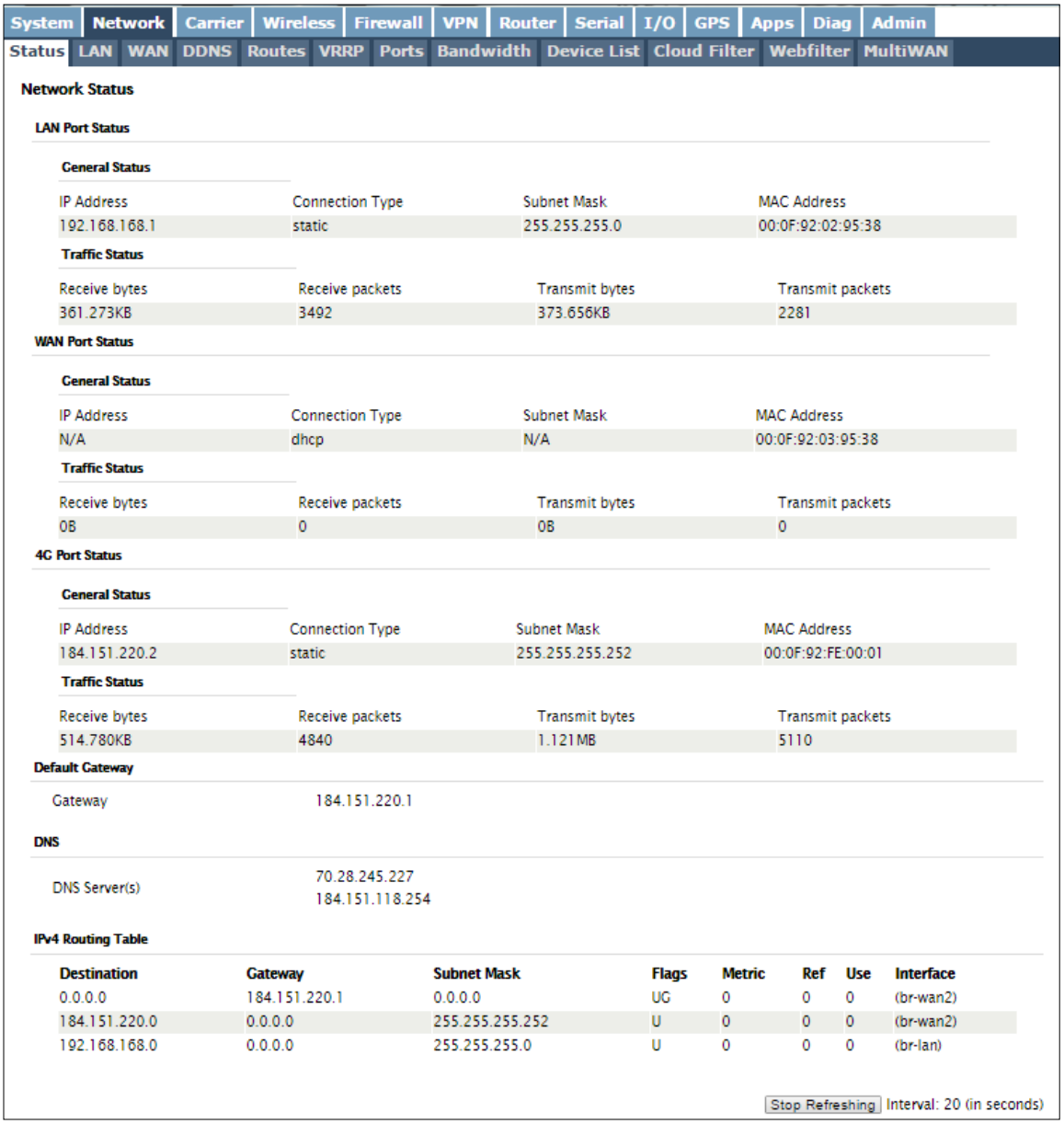


Image 4-2-1: Network > Network Status

4.0 Configuration

4.2.2 Network > LAN

LAN Port Configuration

The Ethernet port (RJ45) on the back of the BulletPlus is the LAN ports, used for connection of devices on a local network. By default, this port has a static IP Address. It also, by default is running a DHCP server to provide IP Addresses to devices that are connected to the physical LAN port (directly or via a switch).

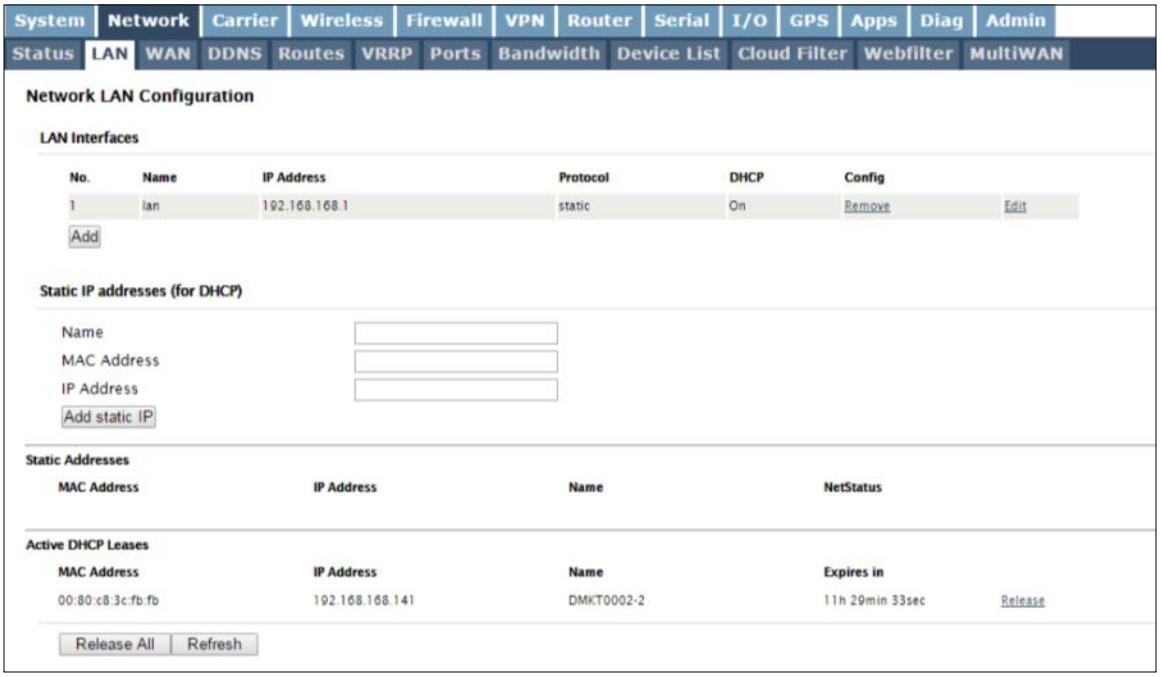


Image 4-2-2: Network > Network LAN Configuration

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).

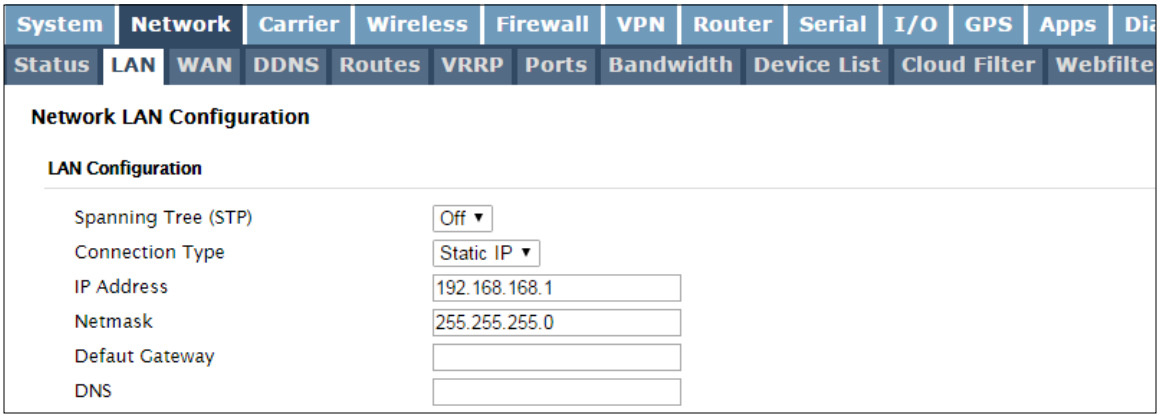


Image 4-2-3: Network > LAN Port Configuration

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

4.0 Configuration

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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.

Values (selection)

Off
On

Connection Type

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.

Values (selection)

DHCP
Static

IP Address

A SUBNET MASK is a bit mask that separates the network and host (device) portions of an IP address.

The 'unmasked' portion leaves available the information required to identify the various devices on the subnet.

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.

Values (IP Address)

192.168.168.1

Netmask

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.

Values (IP Address)

255.255.255.0

Default Gateway

A GATEWAY is a point within a network that acts as an entrance to another network.

In typical networks, a router acts as a 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.

Values (IP Address)

(no default)

A simple way of looking at what the gateway value should be is: If a device has a packet of data is does not know where to send, send it to the gateway. If necessary - and applicable - the gateway can forward the packet onwards to another network.

DNS

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

Set the DNS (Domain Name Server) for use by devices on the LAN port, if required.

Values (IP Address)

(no default)

4.0 Configuration

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.

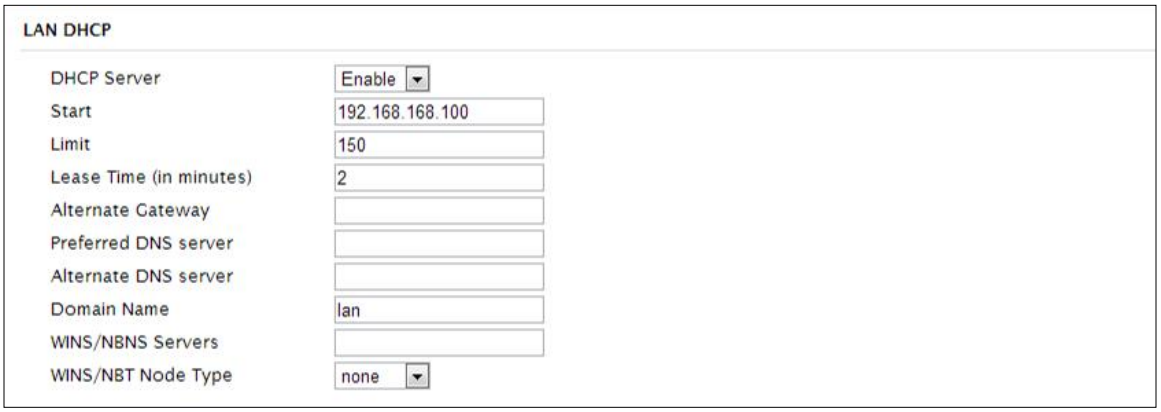


Image 4-2-4: Network > DHCP Server

DHCP Server

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

Values (selection)

Enable / Disable

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.

Values (IP Address)

192.168.168.100

Limit

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

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.

Values (minutes)

720

Alternate Gateway

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

Values (IP Address)

(IP Address)

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.)

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').

Preferred DNS Server

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

Values (IP Address)

(IP Address)

Alternate DNS Server

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

Values (IP Address)

(IP Address)

Domain Name

Enter the Domain Name for the DHCP devices.

Values (string)

(IP Address)

WINS/NBNS Servers

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.

Values (IP/Domain)

(no default)

WINS/NBT Node Type

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

Values (selection)

none
b-node
p-node
m-node
h-node

4.0 Configuration

Static IP Addresses (for DHCP)

In some applications it is important that specific devices always have a predetermined IP address. This section 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. In this situation, all attached (wired or wireless) devices can all be configured for DHCP, but still get a known IP address.

Image 4-2-5: Network > MAC Address Binding

Name

The name field is used to give the device a easily recognizable name.

Values (characters)

(no default)

MAC 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.

Values (MAC Address)

(no default)

IP Address

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

Values (IP Address)

(minutes)

Static Addresses

This section displays the IP address and MAC address currently assigned through the DCHP 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.

Network Interfaces

When additional Network Interfaces are added, they will show up here in a list. You can remove Network Interfaces by clicking "Remove _____".

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.

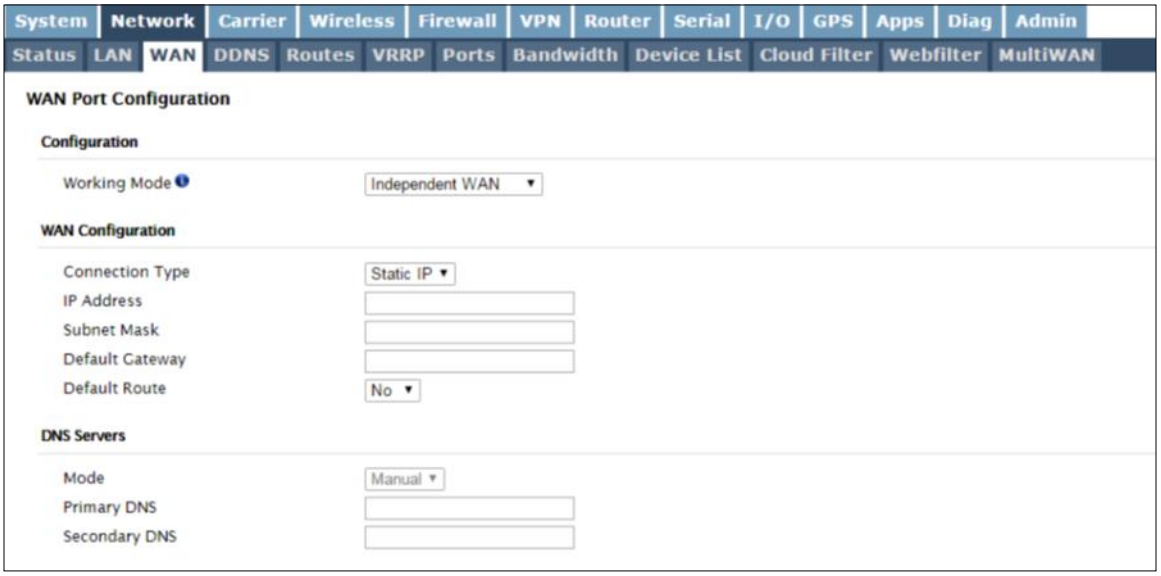


Image 4-2-6: Network > WAN Configuration

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.

Working Mode

Use this to set the function of the physical WAN RJ45 port. If set to independent WAN , the physical WAN port will operate as a standard WAN port. Alternatively it can be configured to be bridged to the LAN, and operate as a second LAN port, or even as an independent LAN.

Values (selection)

Independent WAN
Bridged with LAN Port
Independent LAN

Connection Type

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

Values (selection)

DHCP
Static

IP Address

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.

Values (IP Address)

(no default)

Netmask

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.

Values (IP Address)

(no default)

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.

Values (IP Address)

(no default)

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.**

Values (selection)

No / Yes

DNS Servers

The following section will allow a user to specify DNS Server(s) to be used by the WAN interface of the BulletPlus.

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.

Values (selection)

Manual / **Auto**

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.

Values (IP Address)

(no default)

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.

Values (IP Address)

(no default)

4.0 Configuration

4.2.4 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.

Image 4-2-7: Carrier > Traffic Watchdog

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, specific 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.

Values (selection)

changeip	ods
dyndns	ovh
eurodyndns	regfish
hn	tzo
noip	zoneedit

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

4.2.5 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.

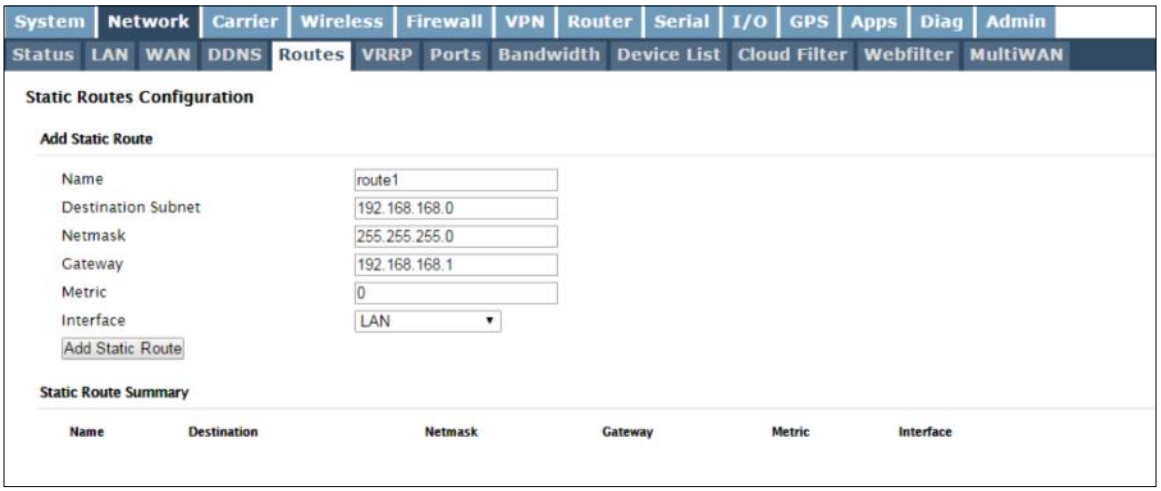


Image 4-2-8: Network > Routes

Name

Routes can be names for easy reference, or to describe the route being added.

Values (characters)

(no default)

Destination

Enter the network IP address for the destination.

Values (IP Address)

(192.168.168.0)

Gateway

Specify the Gateway used to reach the network specified above.

Values (IP Address)

192.168.168.1

Netmask

Enter the Netmask for the destination network.

Values (IP Address)

255.255.255.0

4.0 Configuration

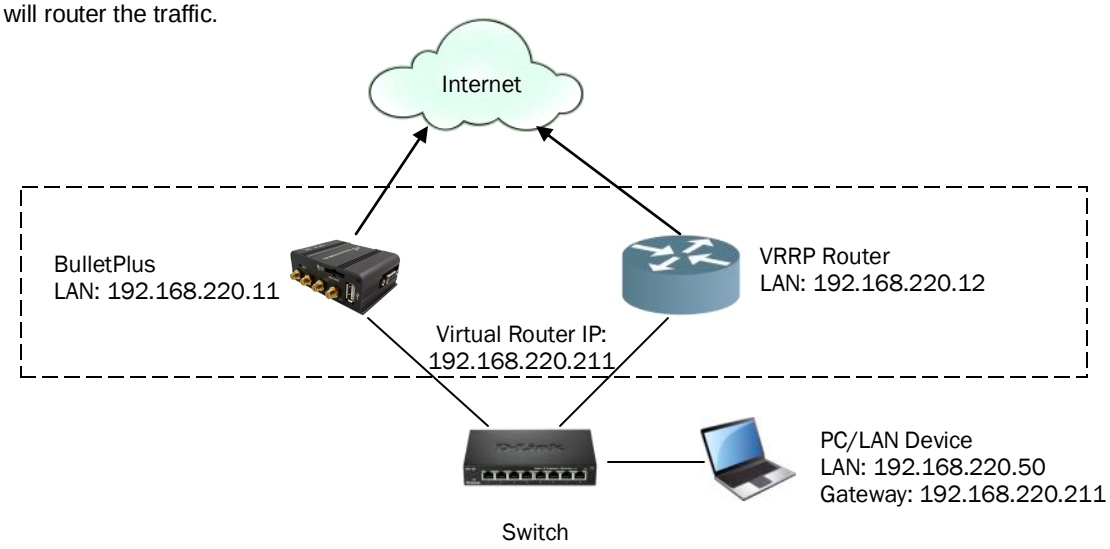
Metric	
In some cases there may be multiple routes to reach a destination. The Metric can be set to give certain routes priority, the lower the metric is, the better the route. The more hops it takes to get to a destination, the higher the metric.	**Values (Integer)** **255.255.255.0**

Interface	
Define the exit interface. Is the destination a device on the LAN, LAN1 (If physical WAN port is bridged as an independent LAN), 3G/4G (cellular), USB or the WAN?	**Values (Selection)** **LAN** / LAN1 / WAN / Cell / USB None

4.0 Configuration

4.2.6 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.



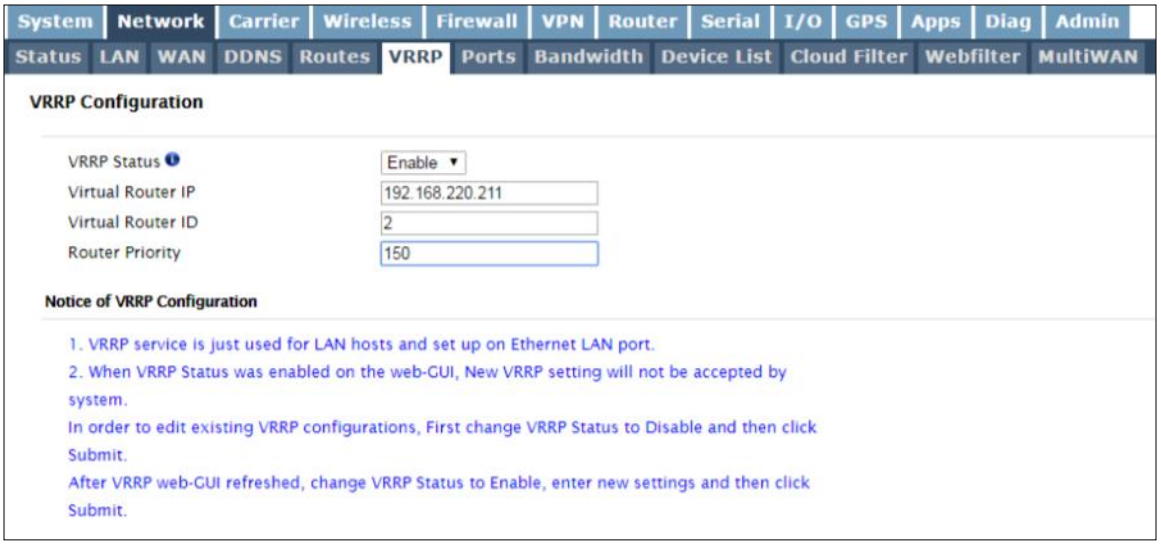


Image 4-2-9: Network > VRRP

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.	**Values (Selection)** **Enable /** Disable

4.0 Configuration

Virtual Router IP	
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.	**Values** **192.168.220.211**

Virtual Router ID	
This is the Router ID. Each router/ participating in VRRP should have a router ID to distinguish between them.	**Values** **2**

Router Priority	
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.	**Values** **150**

4.2.7 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.

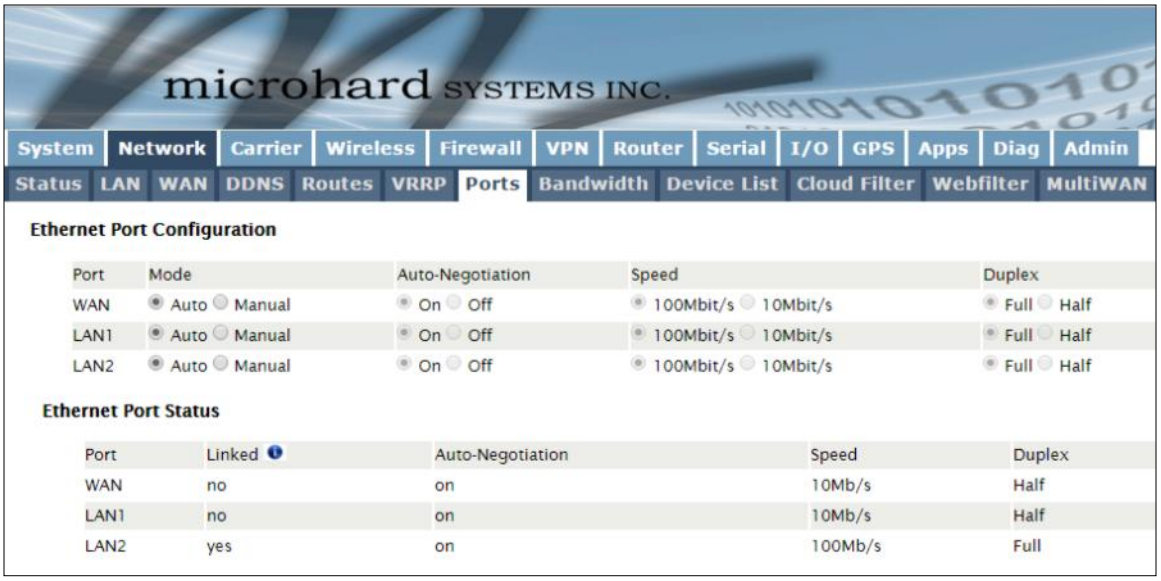


Image 4-2-10: Network > Ports

4.0 Configuration

4.2.8 Network > Bandwidth

The Bulletplus features Bandwidth Throttling, which allows the upload/downloads 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.

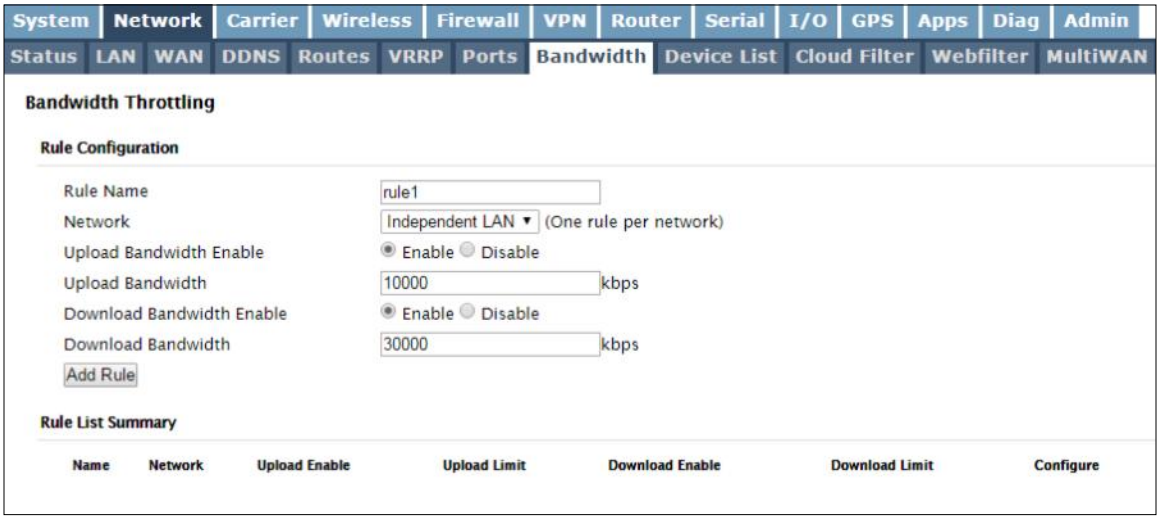


Image 4-2-11: Network > Bandwidth Throttling

Rule Name

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.

Values (chars)

rule1

Network

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

Values (selection)

(varies)

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).

Values (selection)

Enable / Disable

Upload Bandwidth

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

Values (kbps)

10000

4.0 Configuration

Download Bandwidth Enable	Values (chars)
Enable or disable downloading on the specified interface. This prevent data from being downloaded from a server. (i.e downloading files, internet browsing etc).	**Enable** / Disable

Download Bandwidth	Values (kbps)
Set the data limit (speed) for file downloads if downloads have been allowed using the Download Bandwidth Enable.	**30000**

4.2.9 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 4-2-12: Network > Device List

4.0 Configuration

4.2.10 Network > Cloud Filter

The BulletPlus provides Cloud based content filtering and security using the third-party service by Open DNS. 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.

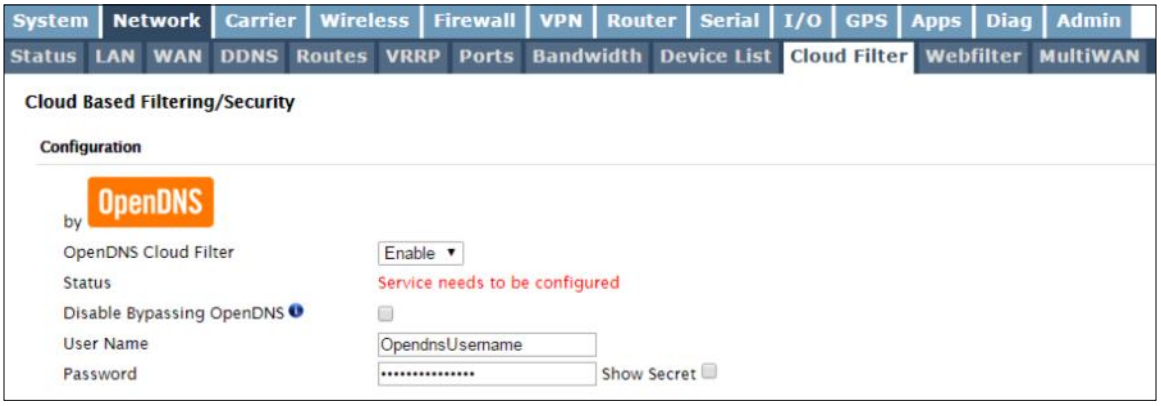


Image 4-2-13: Network > Cloud Filtering

OpenDNS Cloud Filter

Enable or Disable the OpenDNS cloud based filtering & security.

Values (selection)

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.

Values (selection)

Enable / **Disable**

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**".

Values (selection)

Enable / **Disable**

User Name / Password

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

Values (selection)

Enable / **Disable**

4.0 Configuration

4.2.11 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.

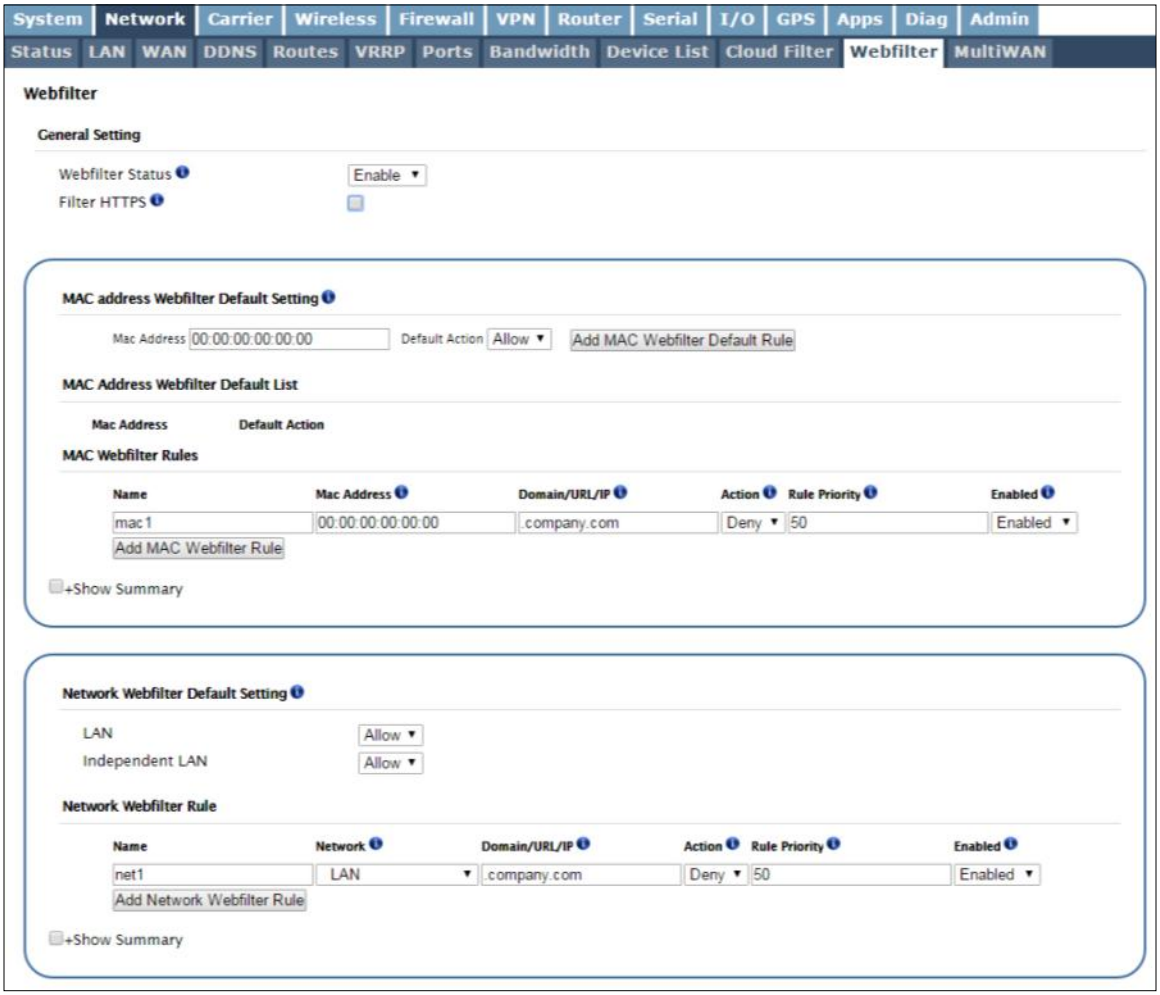


Image 4-2-14: Network > Web Filtering

Webfilter Status

Enable or Disable the Webfilter of the BulletPlus.

Values (selection)

Enable / **Disable**

Filter HTTPS

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

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.

Values

00:00:00:00:00:00 Allow

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.

Values

Mac1
00:00:00:00:00:00
Company.com
Deny
50
Enabled

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.

Values (selection)

Allow / Deny

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.

Rule Priority: See description in MAC Filtering Rules above.

Enabled: Enable or Disable the Network Webfilter rule.

Values

net1
LAN
Company.com
Deny
50
Enabled

4.0 Configuration

4.2.12 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.

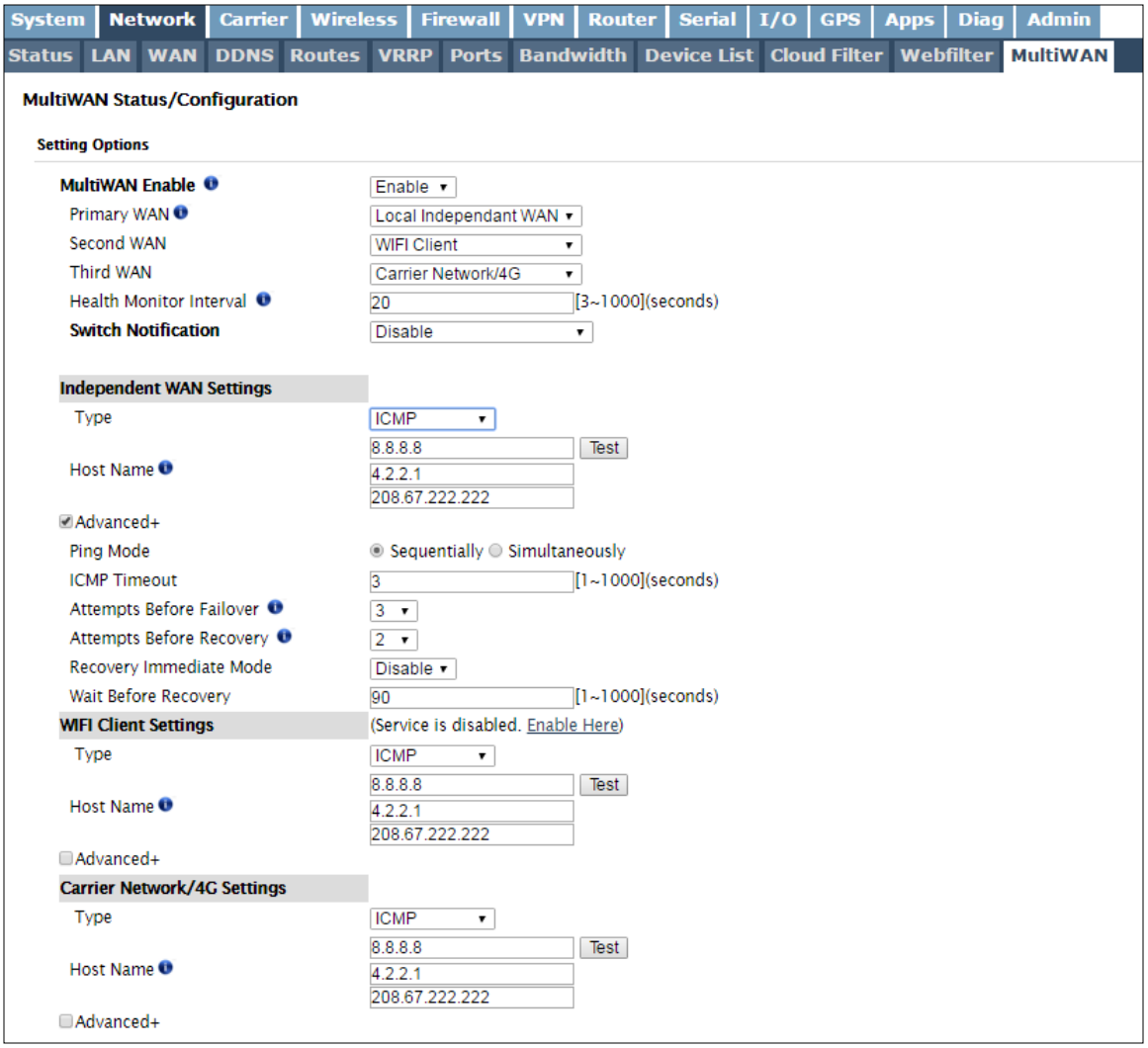


Image 4-2-15: Network > MultiWAN

MultiWAN Enable

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.

Values (selection)

Enable / **Disable**

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.

Values (selection)

WAN / Carrier / WIFI Client

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.

Values (selection)

WAN / **4G** / WIFI

Third WAN

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

Values (selection)

WAN / 4G / **WIFI** / Disable

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.

Values (seconds)

20

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.

Values (selection)

Disable / Email / SMS / Both

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 configure address(s), a DNS Lookup can also be selected.

Values (selection)

ICMP / DNS Lookup

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.

Values (Address)

8.8.8.8
4.2.2.1
208.67.222.222

Advanced+ (Only shown if selected)

4.0 Configuration

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.

Values (seconds)

3

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).

Values (seconds)

3

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.

Values (selection)

1, **3**, 5, 10, 15, 20

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.

Values (selection)

1, **2, 5**, 10, 15, 20

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.

Values (selection)

Disable / Enable

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.

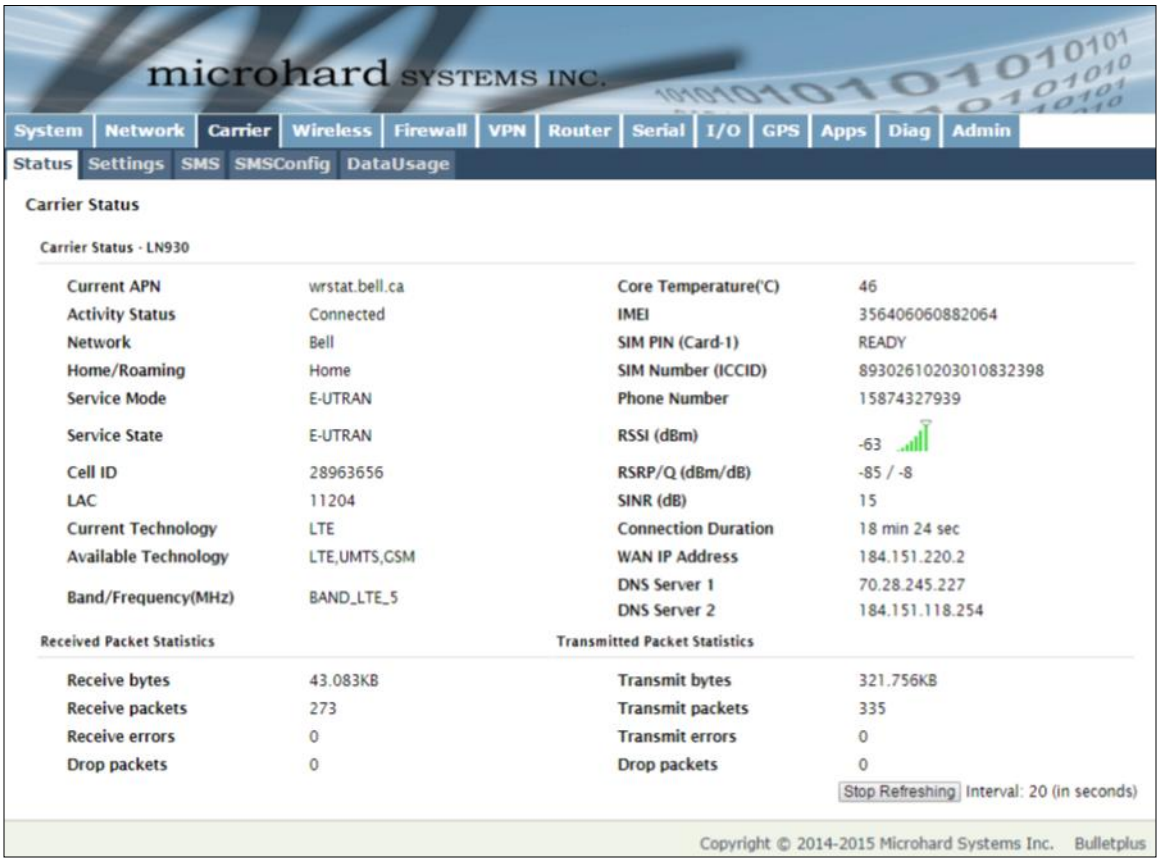


Image 4-3-1: Carrier > Status

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.

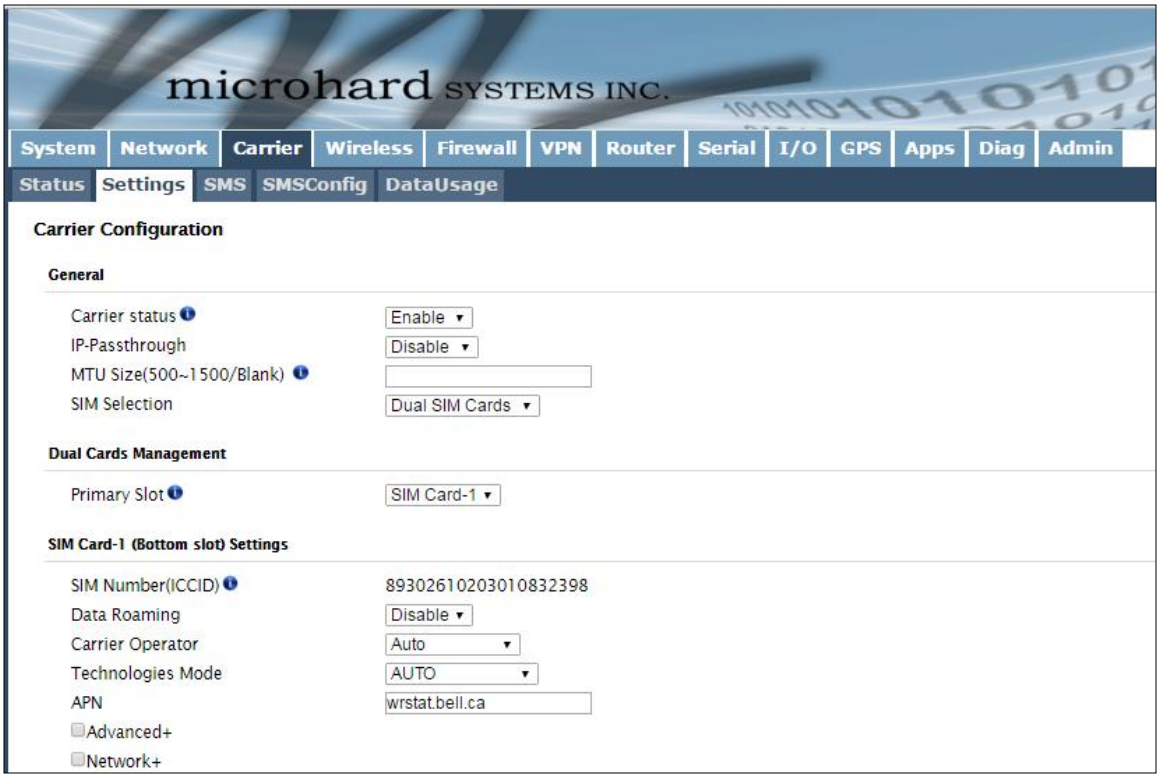


Image 4-3-2: Carrier > Settings

Carrier Status

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

Values (Selection)

Enable / Disable

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.

Values

(blank)

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*).

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.

Values (Selection)

Disable
Ethernet (LAN)
WAN

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.

Values (Selection)

Dual SIM Cards
SIM Card-1 Only
SIM Card-2 Only

Dual Cards Management

Primary Slot

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.

Values (Selection)

SIM Card-1
SIM Card-2

SIM Card-1 Settings

Data Roaming

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.

Values (Selection)

Enable / **Disable**

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.

Values (Selection)

Auto
Based on SIM
Manual
Fixed

4.0 Configuration

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.

Values (Selection)

AUTO
WCDMA, LTE, GSM
GSM Only
WCDMA Only
LTE Only
WCDMA, GSM
LTE,WCDMA
WCDMA, LTE
LTE, GSM

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.

Values (characters)

auto

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.

Values (characters)

(none)

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.

Values (Selection)

Device decide (AUTO)
PAP
CHAP
No Auth

User Name

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.

Values (characters)

Carrier/peer dependant

Password

Enter the password for the user name above. May not be required by some carriers, or APN's

Values (characters)

Carrier/peer dependant

4.0 Configuration

Network+

IP Address	
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.	**Values (IP Address)** *(none)*

Use Remote DNS	
If enabled the Bullet with use the DNS server as specified automatically by the service provider.	**Values (selection)** **Enable** / Disable

Default Route	
Use this interface as the default route for all outbound traffic unless specified in the Network > Routes table.	**Values (Selection)** **Yes** / No

DNS-Passthrough	
When enabled DNS-Passthrough will pass on the WAN assigned DNS information to the end device.	**Values (Selection)** Enable / **Disable**

SIM Card-2 Settings

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.

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.

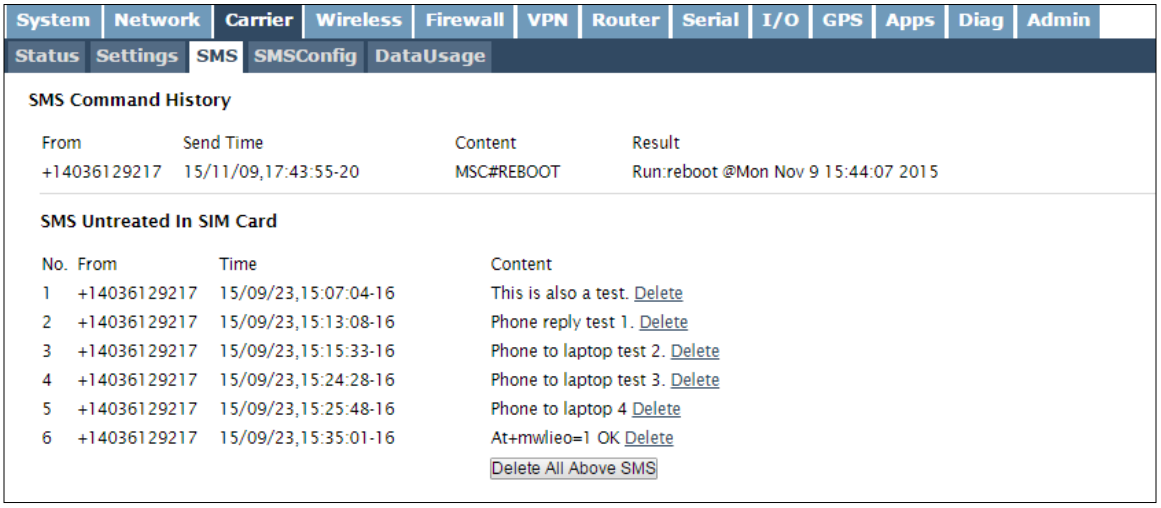


Image 4-3-3: SMS > SMS Command History

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

Status

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

Values (Selection)

Enable / Disable

MSC#REBOOT Reboot system
MSC#NMS Send NMS UDP Report
MSC#WEB Send web client inquiry
MSC#MIOP1 open I/O ouput1
MSC#MIOP2 open I/O ouput2
MSC#MIOC1 close I/O ouput1
MSC#MIOC2 close I/O ouput2

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.

Values (Selection)

Enable / **Disable**

4.0 Configuration

System SMS Alerts

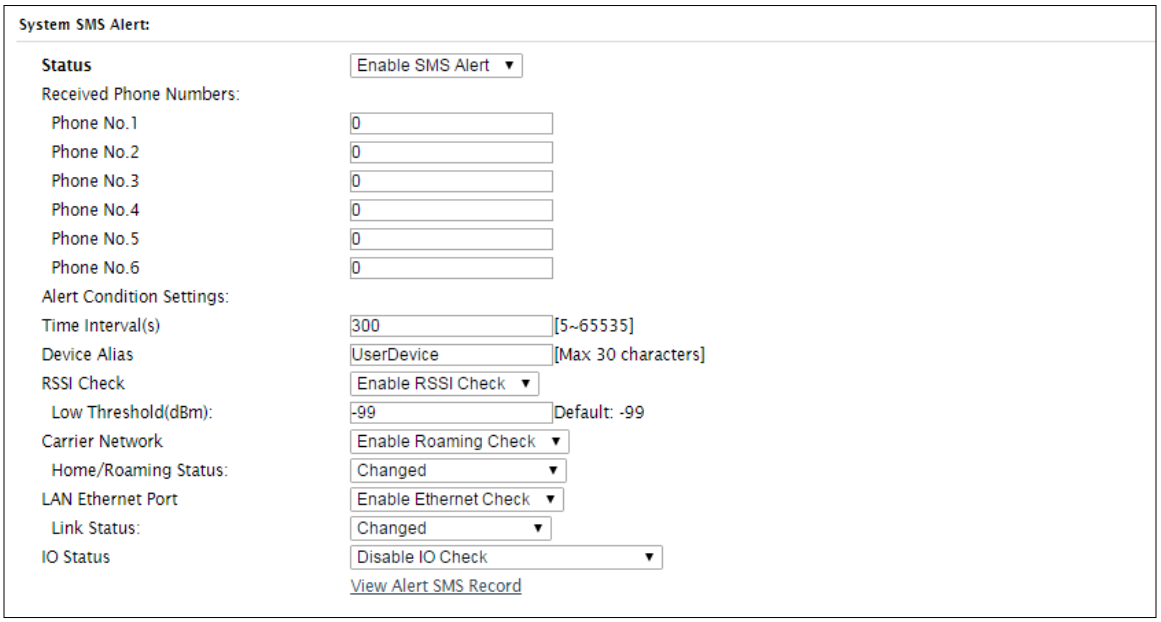


Image 4-3-6: SMS > SMS Alerts

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

RSSI Check

Enable or disable the RSSI alerts.

Values (Selection)

Disable RSSI check
Enable RSSI check

Low Threshold (dBm)

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.

Values (dBm)

-99

Carrier Network

Enable or disable SMS Alerts for Roaming Status.

Values (Selection)

Disable Roaming Check
Enable Roaming Check

Home / Roaming Status

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.

Values (Selection)

In Roaming
Changed or In Roaming
Changed to Roaming

Ethernet

Enable or disable SMS Alerts for the Ethernet Link status of the LAN RJ45 port.

Values (Selection)

Disable Ethernet check
Enable Ethernet check

Ethernet Link Status

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.

Values (Selection)

Changed
In no-link
Changed or in no-link
Changed to no-link

I/O Status

SMS Alerts can be sent based on the state changes of the Digital I/O lines.

Values (Selection)

Disable IO Check
Enable: INPUT Changed
Enable: Output Changed
Enable: INPUT or OUTPUT Changed.

4.0 Configuration

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.

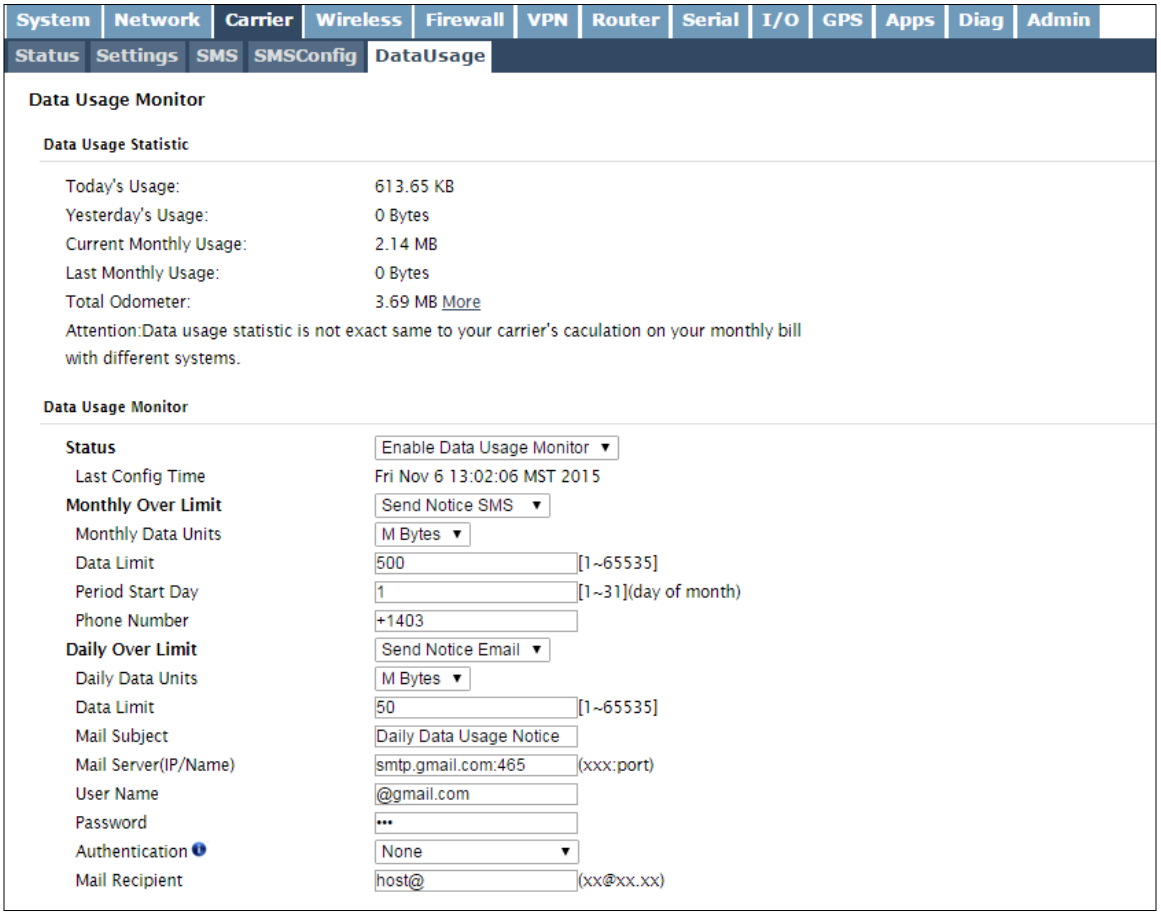


Image 4-3-7: Carrier > Data Usage

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.	**Values (selection)** **Disable** Enable

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.

Values (selection)

None
Send Notice SMS
Send Notice Email
Both SMS & Email

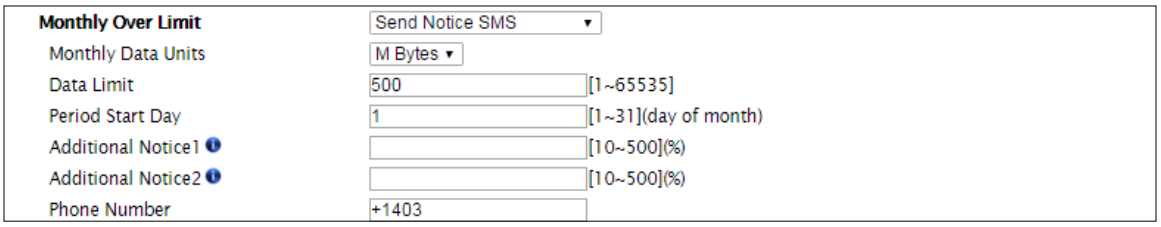


Image 4-3-9: Data Usage > SMS Config

Monthly/Daily Data Unit

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

Values (selection)

Bytes / K Bytes / **M Bytes**
G Bytes

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.

Values (1-65535)

500

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.

Values (1-31)

1 (Day of Month)

Additional Notice 1/2

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

Values (10-500%)

(none)

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.

Values (phone)

+1403

4.0 Configuration

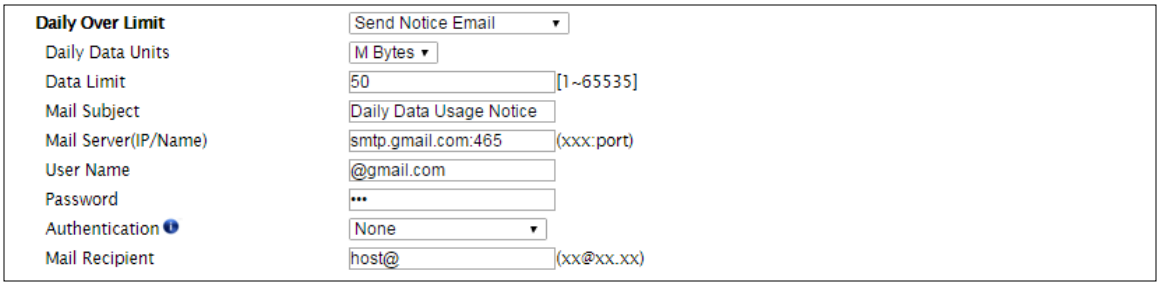


Image 4-3-10: Data Usage > Email Config

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.

Values (string)

Daily/Monthly Data Usage Notice

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.

Values (xxx:port)

smtp.gmail.com:465

Username

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

Values (username)

@gmail.com

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.

Values (string)

***

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.

Values (selection)

None
SSL/TLS
STARTTLS
SSL/TLS + STARTTLS

Mail Recipient

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

Values (xx@xx.xx)

host@

4.0 Configuration

Data Usage History

The BulletPlus provides a 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.

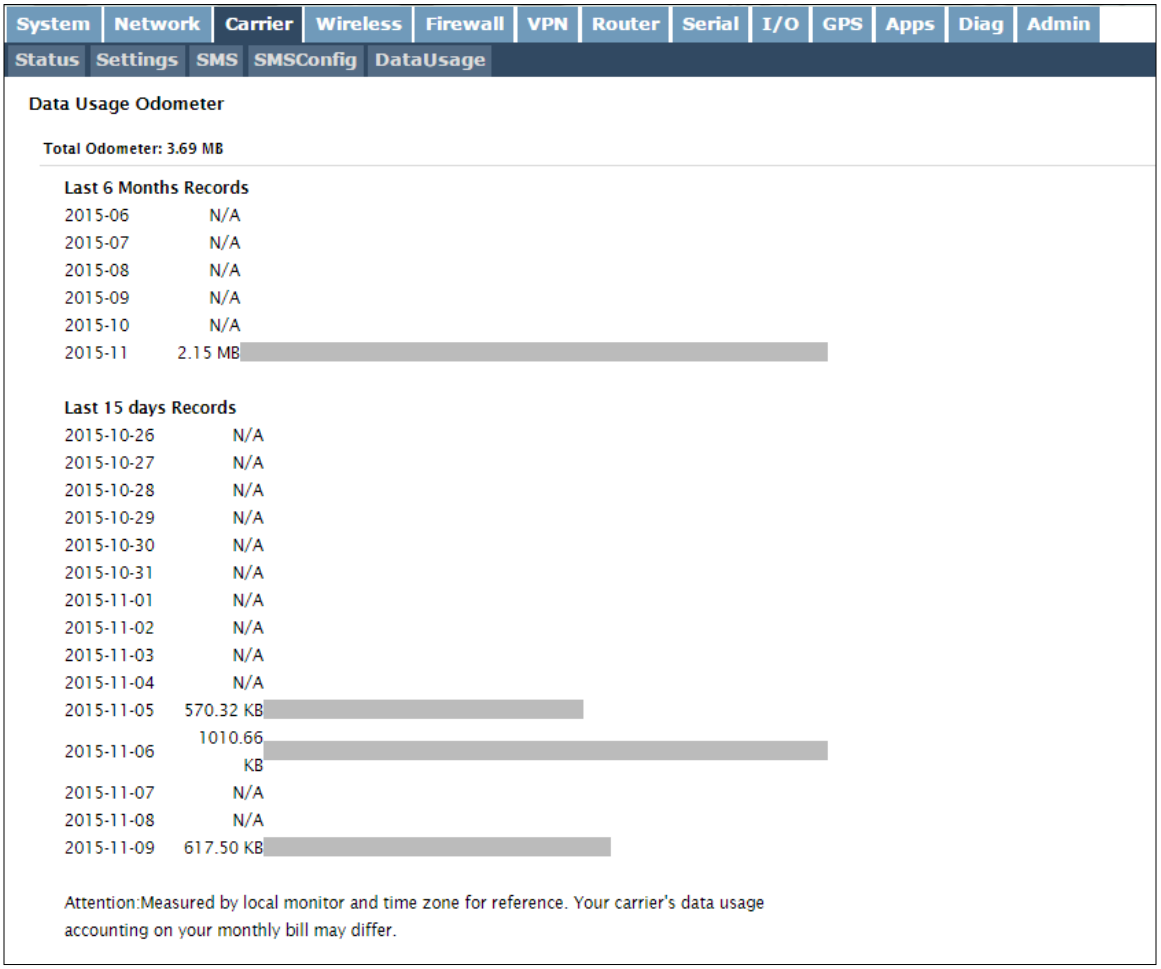


Image 4-3-11: Data Usage > Data Usage Odometer

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.

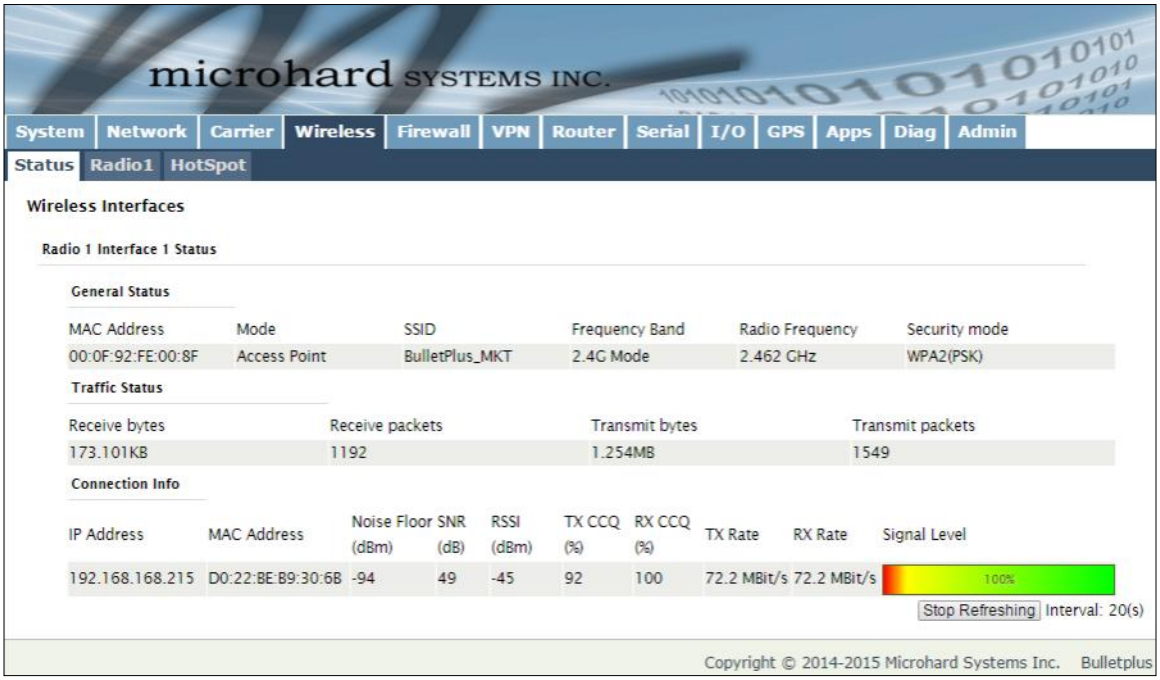


Image 4-4-1: Wireless > Status

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.

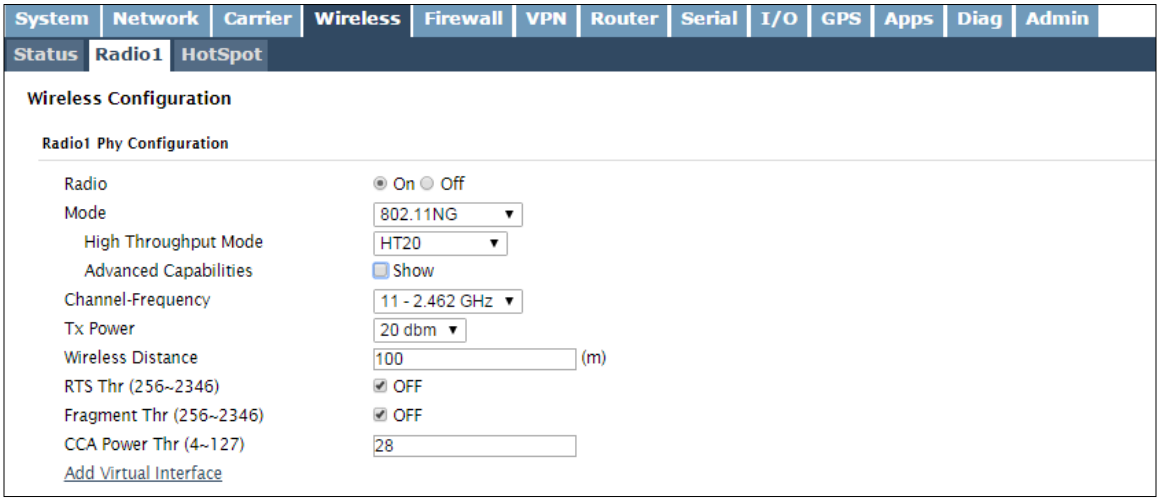


Image 4-4-2: Wireless > Radio Configuration

Radio

This option is used to turn the radio module on or off. If turned off Wireless connections can not be made. The default is On.

Values (selection)

On / Off

Mode

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.

Values (selection)

802.11B ONLY
802.11BG
802.11NG

Channel Bandwidth

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.

Values (selection)

20MHz Normal Rate

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.

Values (selection)

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.

Values (selection)

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.

Values (selection)

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

Wireless Distance

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.

Values (meters)

100

RTS Thr (256 ~ 2346)

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.

Values (selection)

On / **OFF**

Fragment Thr (256 ~ 2346)

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.

Values (selection)

On / **OFF**

CCA Power Thr (4 ~ 127)

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.

Values (selection)

28

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.

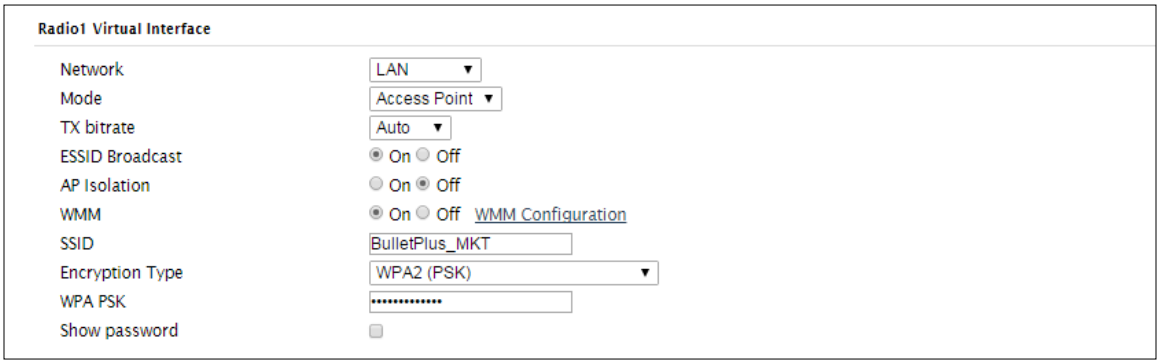


Image 4-4-3: Wireless > Radio Configuration

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.

Values (selection)

LAN
WAN
Etc..
(Additional Interfaces…)

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.

Values (selection)

Access Point
Client
Repeater

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.

802.11 b/g

Auto
1 Mbps (802.11b,g)
2 Mbps (802.11b,g)
5.5 Mbps (802.11b,g)
11 Mbps (802.11b,g)
6 Mbps (802.11g)
9 Mbps (802.11g)
12 Mbps (802.11g)
18 Mbps (802.11g)
24 Mbps (802.11g)
36 Mbps (802.11g)
48 Mbps (802.11g)
54 Mbps (802.11g)

802.11n (HT20/HT40)

Auto
mcs-0 (7.2/15) Mbps
mcs-1 (14.4/30.0) Mbps
mcs-2 (21.7/45.0) Mbps
mcs-3 (28.9/60.0) Mbps
mcs-4 (43.3/90.0) Mbps
mcs-5 (57.8/120.0) Mbps
mcs-6 (65.0/135.0) Mbps
mcs-7 (72.2/150.0) Mbps

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.

Values (selection)

On / Off

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.

Values (selection)

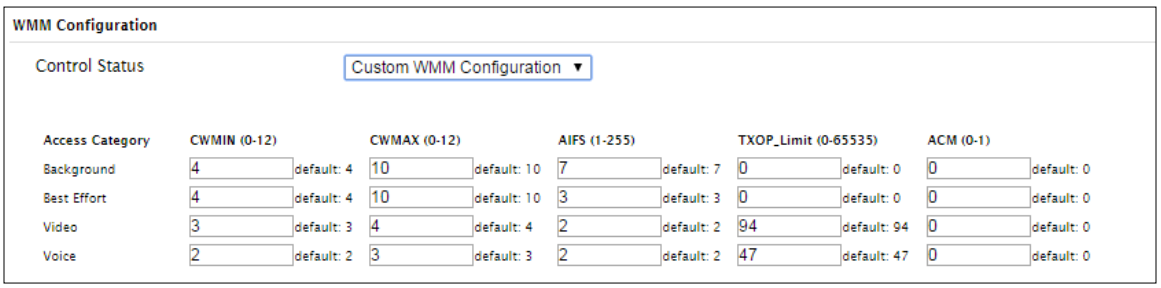
On / **Off**

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).

Values (selection)

On / **Off**



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.

Change the default value for the Network Name to something unique for your network. Do this for an added measure of security and to differentiate your network from others which may be operating nearby.

SSID

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.

Values (string)

BulletPlus

Encryption Type

The encryption types defines 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.

Values (selection)

Disabled
WPA (PSK)
WPA2 (PSK)
WPA+WPA2 (PSK)
WPA Enterprise (RADIUS)
WPA2 Enterprise (RADIUS)
WPA+WPA2 Enterprise(RADIUS)

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.

Values (string)

0123456789

Show Password

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

Values (selection)

unchecked

RADIUS IP Address

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

Values (IP Address)

(no default)

RADIUS Port

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

Values (port)

(no default)

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.

Values (selection)

0123456789

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.

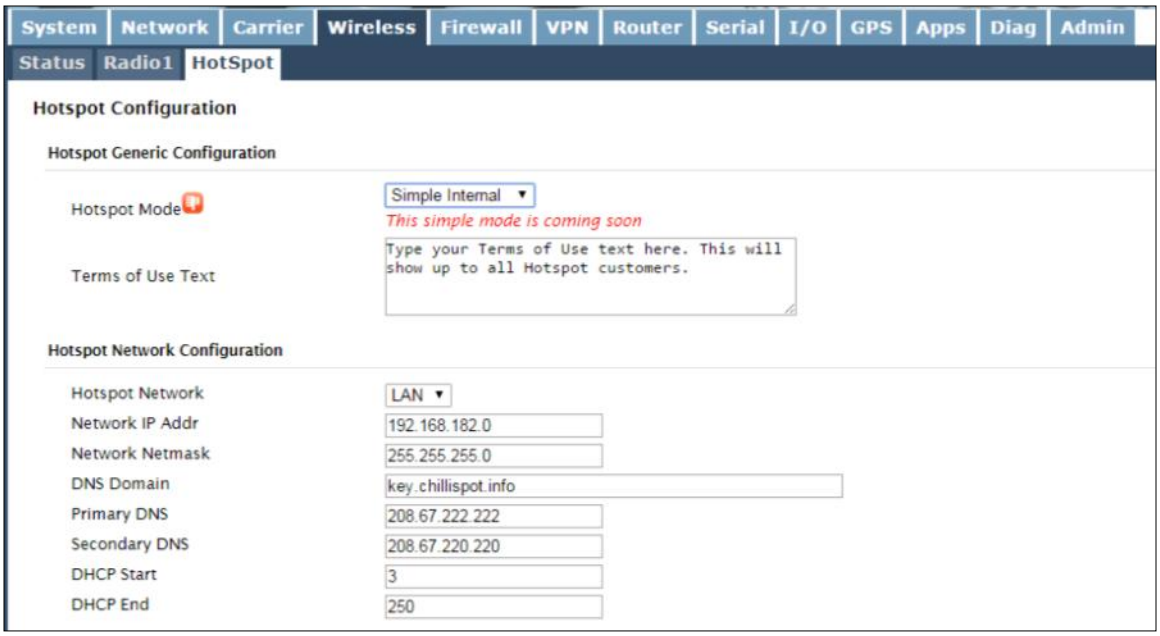


Image 4-4-4: Wireless > Hotspot Network Configuration

Hotspot Mode

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.

*** Coming Soon**

Values (selection)

Disable
Simple Internal*
Simple External*
RADIUS/UAM

UAM Login URL

If the Hotspot Mode, RADIUS/UAM is chosen, specify the hotspot URL as given by your service provider. The address of the UAM Server, the authentication portal.

Values

https://
customer.hotspotsystem.com/
customer/hotspotlogin.php

UAM Secret

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.

Values

hotsys123

4.0 Configuration

Hotspot Network Configuration

Hotspot Network	
This field is used to specify which configured network is bonded to the hotspot. Sub networks can be created in the Network > LAN menu, which are dedicated to the hotspot devices. *The DHCP service for the network used should be turned off as all IP address assignments will be made by the hotspot service provider.*	**Values** *Varies*

Network IP Address	
Specify the IP Address of the Hotspot application. All hotspot clients will get an IP address in the same network as the Hotspot.	**Values** 192.168.182.0

Network Netmask	
Specify the Netmask of the Hotspot application. All hotspot clients will get an IP address in the same network as the Hotspot.	**Values** 255.255.255.0

DNS Domain	
Provide your service providers 1st DNS Server domain.	**Values** Key.chillispot.info

Primary DNS	
Specify the Primary DNS server to be used by devices connected to the Hotspot network.	**Values** 208.67.222.222

Secondary DNS	
Specify the Secondary DNS server to be used by devices connected to the Hotspot network.	**Values** 208.67.222.220

DHCP Start	
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.	**Values** 3

DHCP End	
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.	**Values** 250

4.0 Configuration

Hotspot Radius Configuration

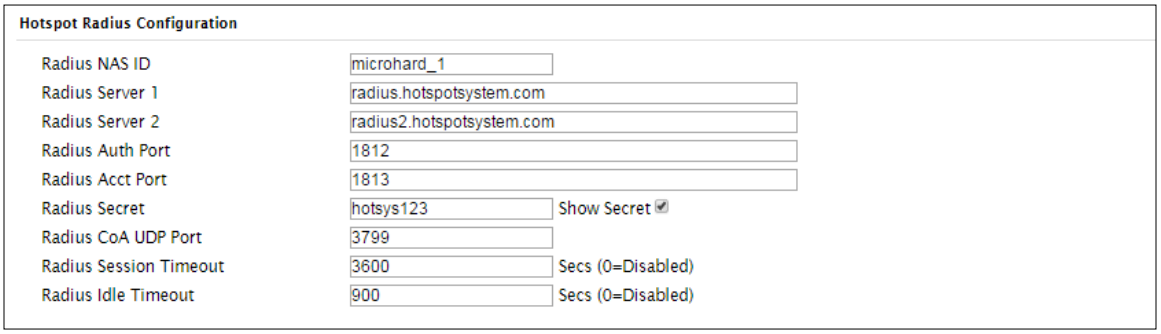


Image 4-4-5: Wireless > Hotspot Radius Configuration

Radius NAS ID

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

Values

Microhard_1

Radius Server 1

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

Values

radius.hotspotsystem.com

Radius Server 2

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

Values

radius2.hotspotsystem.com

Radius Auth Port

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

Values

1812

Radius Acct Port

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

Values

1813

Radius Secret

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

Values

hotsys123

4.0 Configuration

Radius CoA UDP Port	
Specify the Radius CoA UDP Port here. This information is supplied by the hotspot service provider.	**Values (port)** 3799

Radius Session Timeout	
Specify the Radius Session Timeout. In seconds, 0 = disabled.	**Values (seconds)** 3600

Radius Idle Timeout	
Specify the Radius Idle Timeout. In seconds, 0 = disabled.	**Values (seconds)** 900

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.

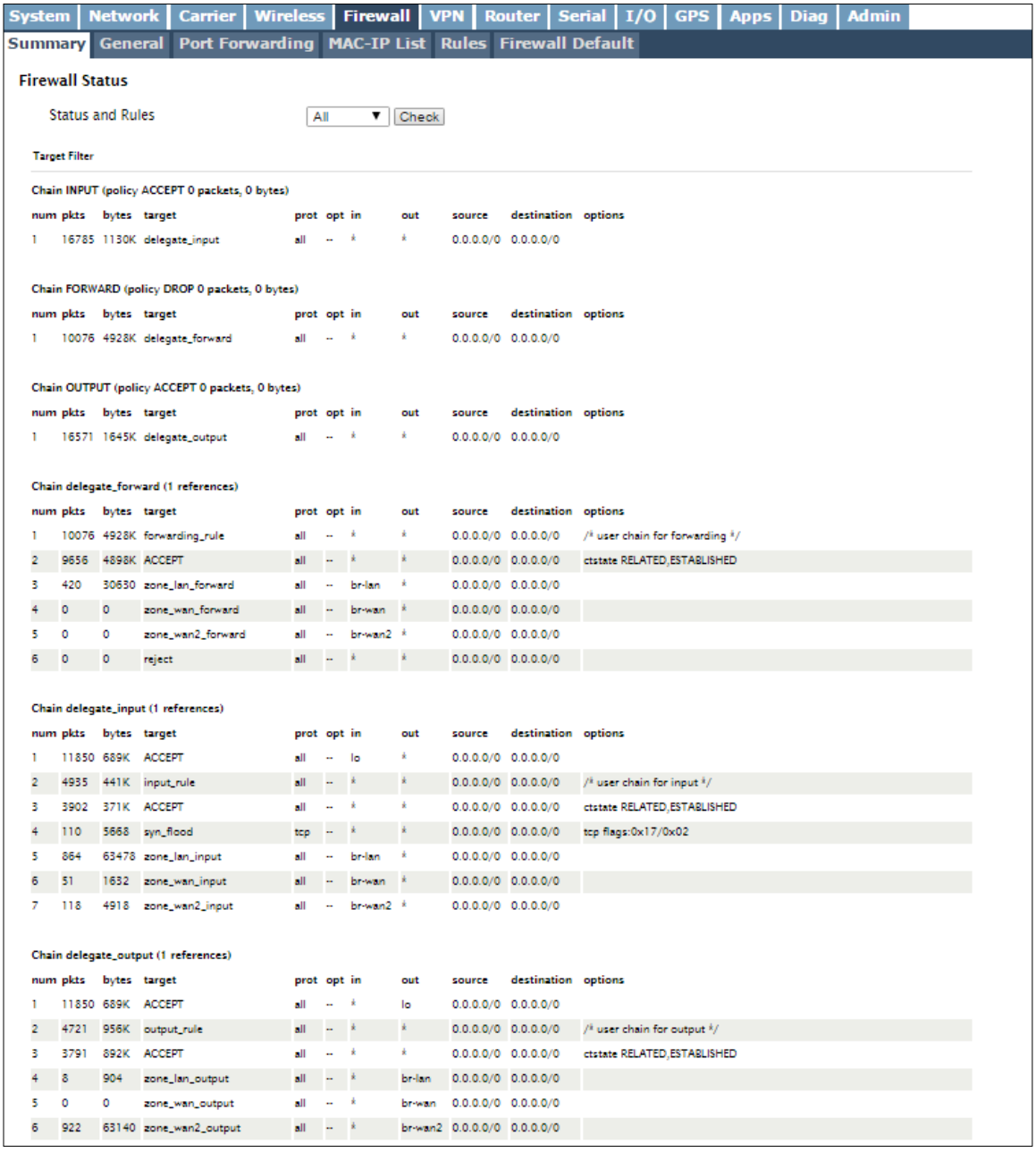


Image 4-5-1: Firewall > Status

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.

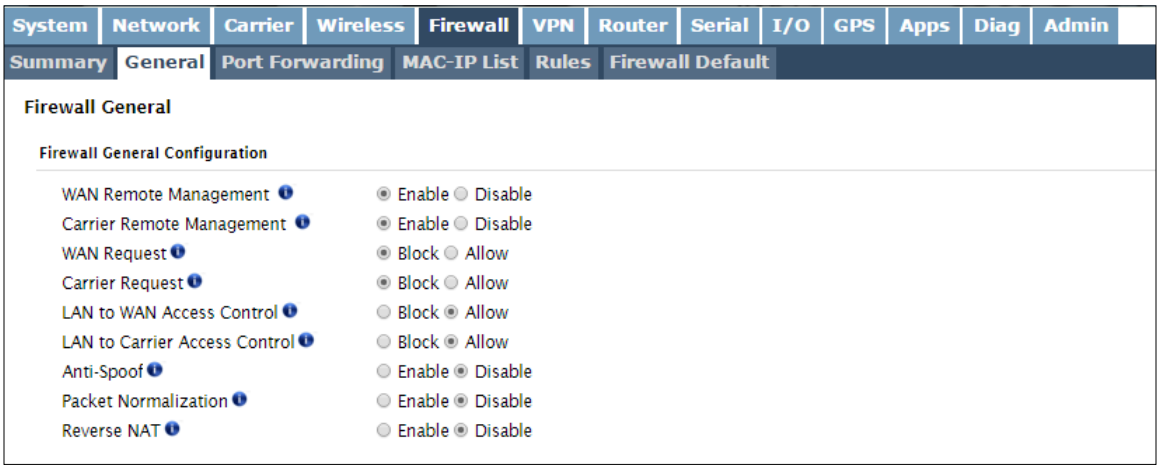


Image 4-5-2: Firewall > General

For best practices and to control data usage it is critical that the firewall be configured properly.

It is recommended to block all incoming Cellular traffic and create rules to open specific ports and/or use ACL lists to limit incoming connections.

WAN Remote Management

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)..

Values

Enable / Disable

Carrier Remote Management

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)..

Values

Enable / Disable

When Carrier Request is set to 'Allow' the modem is open to anyone, this is not recommended as it may impact data usage from unwanted sources.

WAN Request

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.

Values

Block / Allow

Carrier Request

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.

Values

Block / Allow

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**

Reverse NAT

The Reverse NAT allows access to the modem from the LAN port using the carrier's IP address.

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.

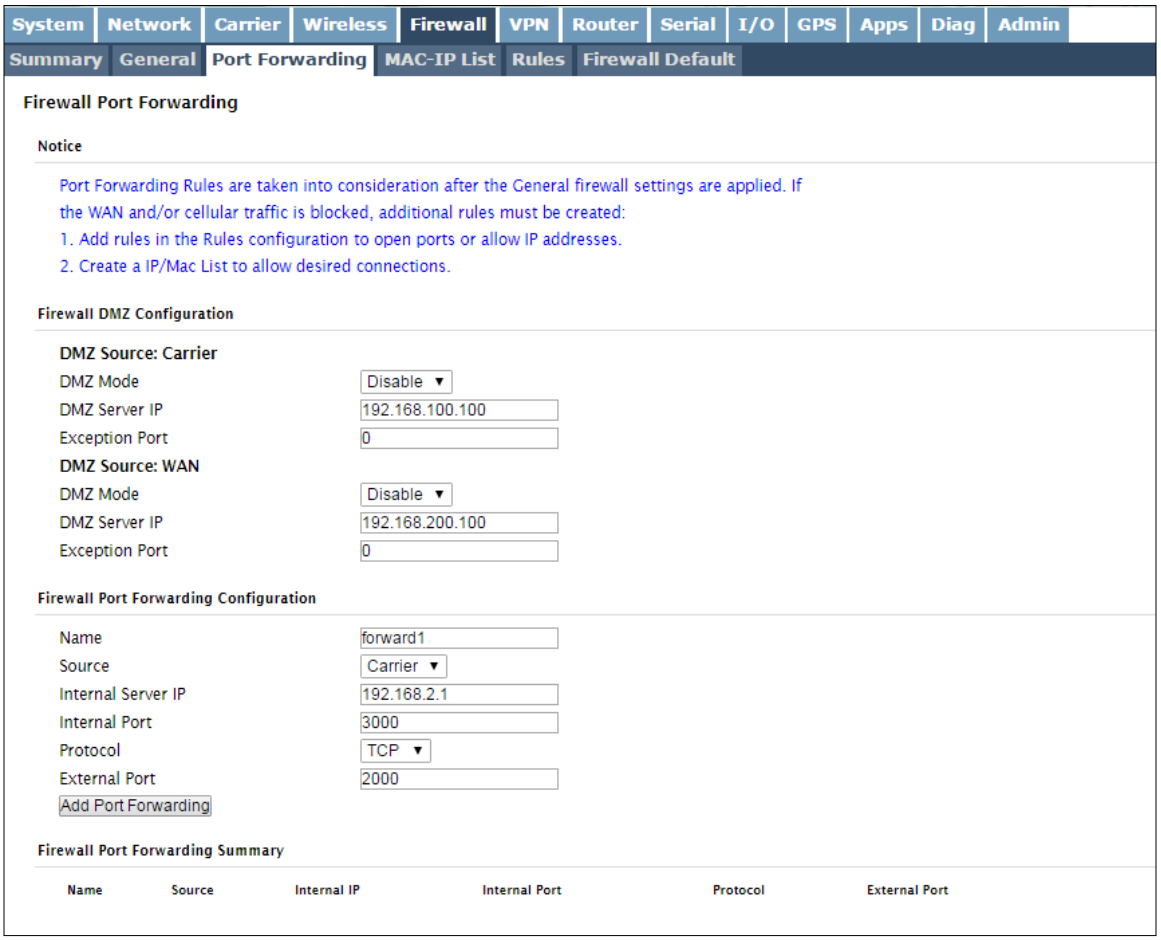


Image 4-5-3: Firewall > Port Forwarding

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

If the firewall is set to block incoming traffic on the WAN and/or Carrier interfaces, additional rules or IP/MAC lists must be configured to allow desired traffic access.

DMZ Mode	
Enable or disable DMZ Mode. DMZ can be used to forward all traffic to the DMZ Server IP listed below.	**Values (selection)** **Disable** / Enable

DMZ Server IP	
Enter the IP address of the device on the LAN side of the BulletPlus where all the traffic will be forwarded to.	**Values (IP Address)** **192.168.100.100**

Exception Port	
Enter a 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.	**Values (Port #)** **0**

Firewall Port Forwarding Configuration

Name	
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.	**Values (10 chars)** **Forward**

Source	
Select the source for the traffic, from either the 3G/Cellular or from the WAN.	**Values (selection)** **Carrier /** WAN

Internal Server IP	
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.	**Values (IP Address)** **192.168.2.1**

Internal Port	
Target port number of the internal server on the LAN IP entered above.	**Values (Port #)** **3000**

Protocol	
Select the type of transport protocol used. For example Telnet uses TCP, SNMP uses UDP, etc.	**Values (selection)** **TCP /** UDP / Both

External Port	
Port number of the incoming request (from 4G/WAN-side).	**Values (Port #)** **2000**

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.

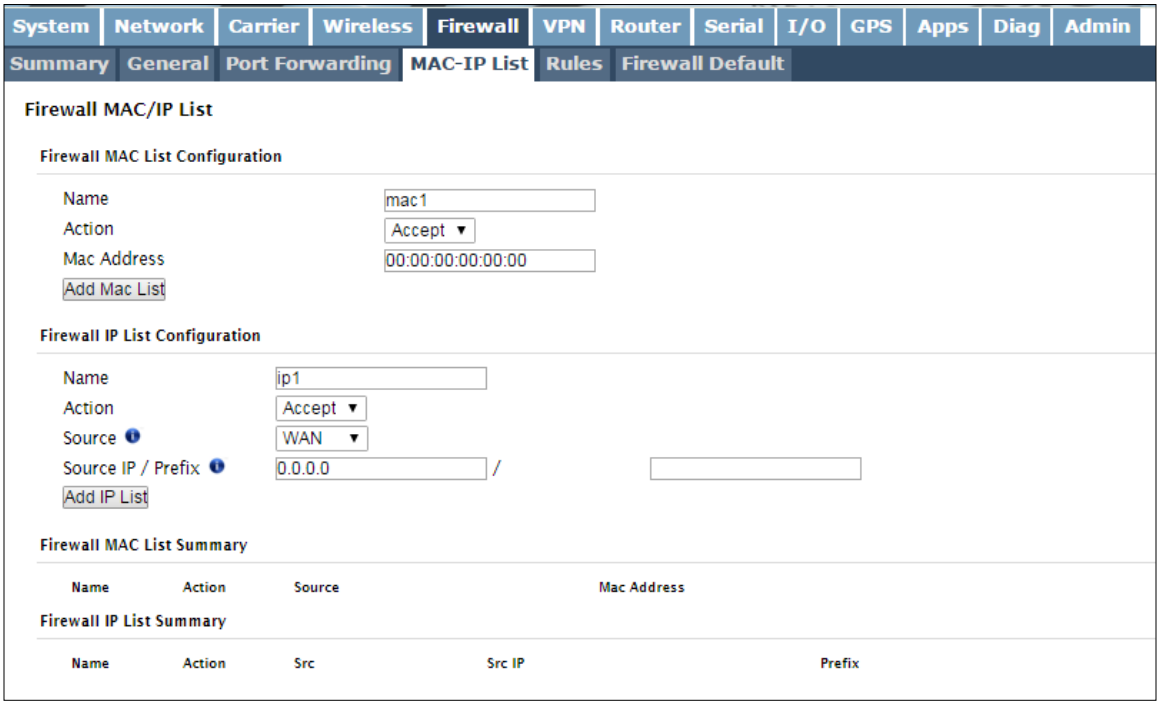


Image 4-5-5: Firewall > MAC-IP List

Firewall MAC List Configuration

Rule Name	Values (10 chars)
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_List**

MAC Address	Values (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.	**00:00:00:00:00:00**

4.0 Configuration

Firewall MAC List Configuration (Continued)

Action	
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.	**Values (selection)** **ACCEPT** DROP REJECT

Firewall IP 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.	**Values (10 chars)** **IP_List**

Action	
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.	**Values (selection)** **ACCEPT /** DROP / REJECT

Source	
Enter the specific zone that the IP List will apply to, Cellular, LAN, WAN or None (both).	**Values (Selection)** LAN/LAN1/WAN/Cell/USB **NONE**

Source IP Address	
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.)	**Values (IP Address)** **192.168.0.0**

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 to 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

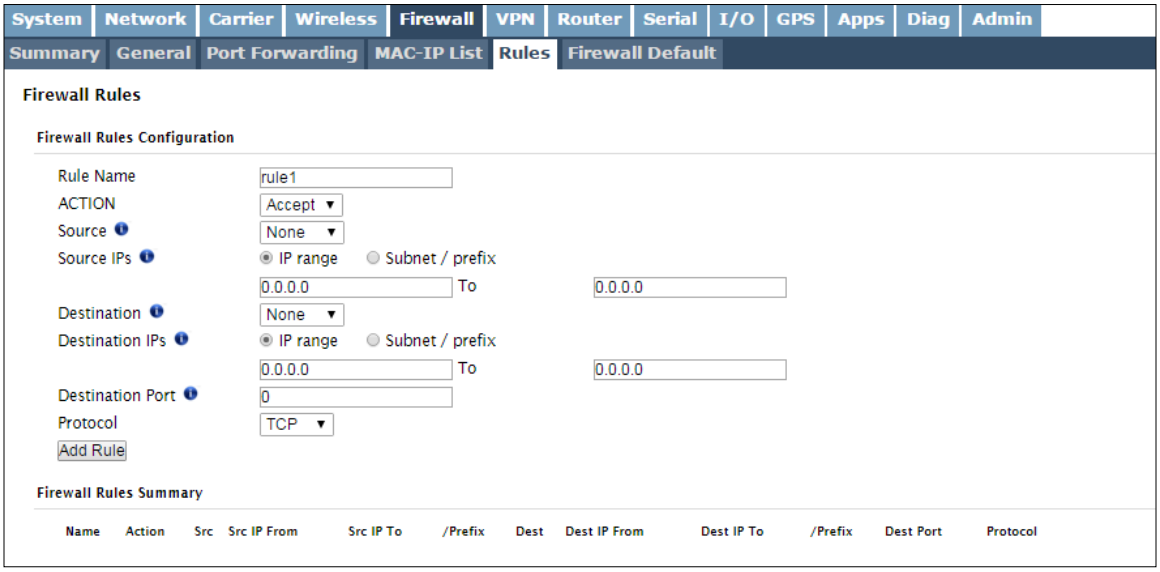


Image 4-5-6: Firewall > Rules

Rule Name

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.

Values (10 Chars)

characters

Action

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.

Values (selection)

ACCEPT
DROP
REJECT

Source

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

Values

LAN/LAN1/WAN/Carrier
None

4.0 Configuration

Source IPs	
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.)	**Values (IP Address)** **192.168.0.0 to 192.168.0.0**

Destination	
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.	**Values (selection)** LAN/LAN1/Cell/WAN/USB **None**

Destination IPs	
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.)	**Values (IP Address)** **192.168.0.0 to 192.168.0.0**

Destination Port	
Match incoming traffic directed at the given destination port or port range. (To specify a port range use a From:To (100:200) format)	**Values (port)** **0**

Protocol	
The protocol field defines the transport protocol type controlled by the rule.	**Values** **TCP** UDP Both ICMP

4.0 Configuration

4.5.6 Firewall > Firewall Default

The Firewall Default option allows a user to return the modems 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.

Image 4-6-1: VPN > Summary

4.0 Configuration

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.

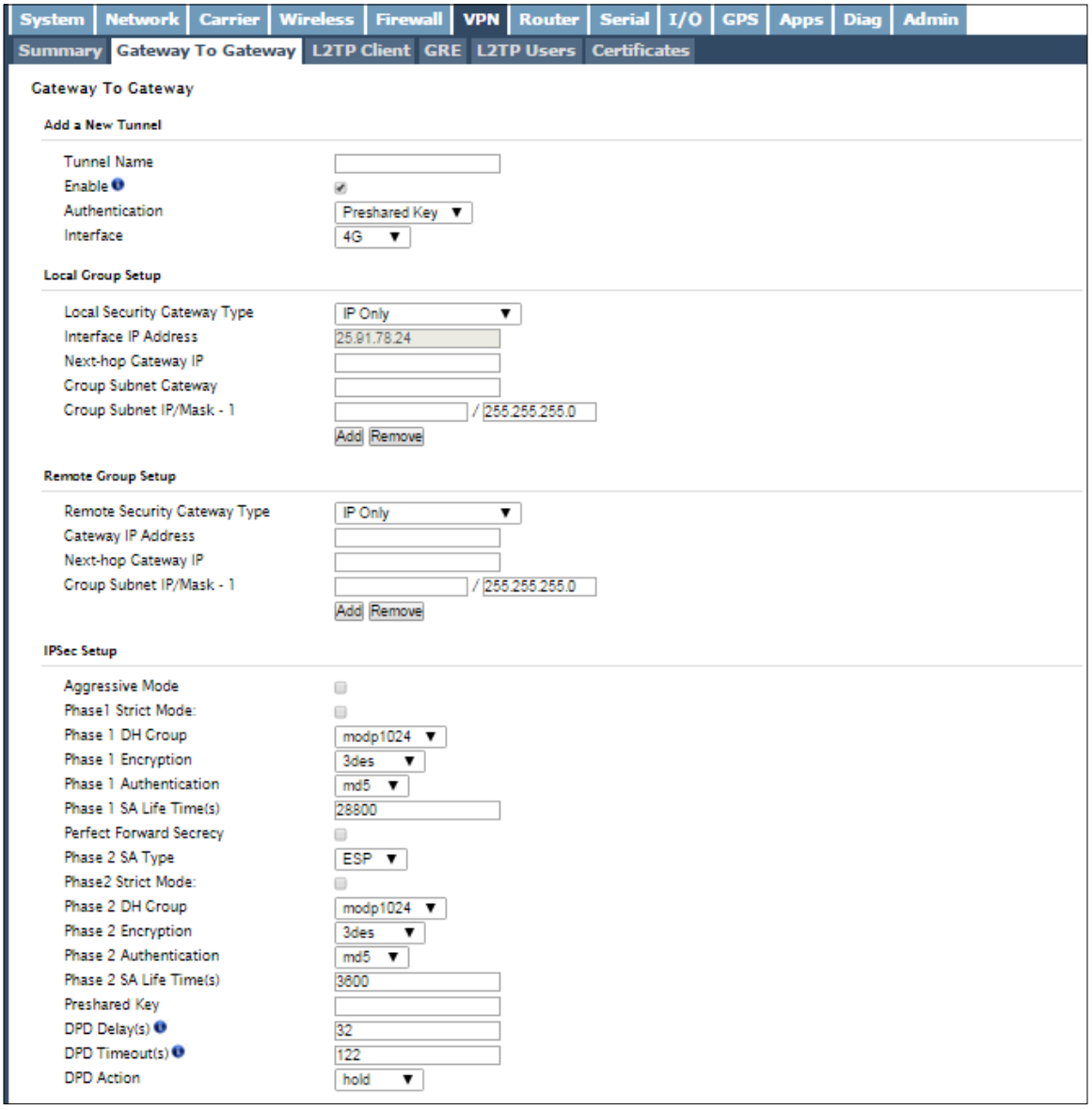


Image 4-6-2: VPN > Gateway to Gateway

Tunnel Name

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

Values (chars)

tunnel1

4.0 Configuration

Enable

Used to enable (checked) is disable (unchecked) the VPN tunnel.

Values (checkbox)

Enable (Checked)

Local Group Setup

Local Security Gateway Type

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.

Values (selection)

IP Only
IP + Server ID
Dynamic IP + Server ID

IP Only: Choose this option if this router has a static WAN IP address. The WAN IP address appears automatically. For the Remote Security Gateway Type, an extra field appears. If you know the IP address of the remote VPN router, choose IP Address, and then enter the address.

IP + Server ID: Choose this option if this router has a static WAN IP address and a server id. The WAN IP address appears automatically. For the Remote Security Gateway Type, an extra field appears. If you know the IP address of the remote VPN router, choose IP Address, and then enter the address.

Dynamic IP + Server ID: Choose this option if this router has a dynamic IP address and a server id (available such as @microhard.vpn). Enter the server id to use for authentication. The server id can be used only for one tunnel connection.

Interface IP Address

Displays the IP address of the BulletPlus, which is the local VPN Gateway.

Values (IP Address)

Current IP Address

Server ID

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.

Values (characters)

(no default)

Next-hop Gateway IP

Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.

Values (IP Address)

(no default)

Group Subnet IP

Define the local network by specifying the local subnet. The local and remote routers must use different subnets.

Values (IP Address)

(no default)

4.0 Configuration

Group Subnet Mask

Specify the subnet mask of the local network address.

Values (IP Address)

255.255.255.0

Group Subnet Gateway

Enter the Gateway for the local group network.

Values (IP Address)

(no default)

Remote Group Setup

Remote Security Gateway Type

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)

Values (selection)

IP Only
IP + Server ID
Dynamic IP + Server ID

Gateway IP Address

If the remote VPN router has a static IP address, enter the IP address of the remote VPN Gateway here.

Values (IP Address)

(no default)

Server ID

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.

Values (IP Address)

(no default)

Next-hop Gateway IP

Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.

Values (IP Address)

(no default)

Subnet IP Address

Define the remote network by specifying the local subnet.

Values (IP Address)

(no default)

Subnet Mask

Specify the subnet mask of the remote network address.

Values (IP Address)

255.255.255.0

4.0 Configuration

IPsec Setup

Phase 1 DH Group	
Select value to match the values required by the remote VPN router.	**Values (selection)** **modp1024** modp1536 modp2048

Phase 1 Encryption	
Select value to match the Phase 1 Encryption type used by the remote VPN router.	**Values (selection)** 3des aes aes128 aes256

Phase 1 Authentication	
Select value to match the Phase 1 Authentication used by the remote VPN router.	**Values (selection)** md5 sha1

Phase 1 SA Life Time	
Select value to match the values required by the remote VPN router.	**Values** **28800**

Perfect Forward Secrecy (pfs)	
Select value to match the values required by the remote VPN router.	**Values (selection)** **Disable** / Enable

Phase 2 DH Group	
Select value to match the values required by the remote VPN router.	**Values (selection)** **modp1024** modp1536 modp2048

Phase 2 Encryption	
Select value to match the Phase 1 Encryption type used by the remote VPN router.	**Values (selection)** 3des aes aes128 aes256

4.0 Configuration

Phase 2 Authentication	
Select value to match the Phase 1 Authentication used by the remote VPN router.	**Values (selection)** md5 sha1

Phase 2 SA Life Time	
Select value to match the values required by the remote VPN router.	**Values** **3600**

Preshared Key	
Set the Preshared Key required to authenticate with the remote VPN router.	**Values (characters)** **password**

DPD Delay(s)	
Dead Peer Detection is used to detect if there is a dead peer. Set the DPD Delay (seconds), as required.	**Values (seconds)** **32**

DPD Timeout(s)	
Set the DPD (Dead Peer Detection) Timeout (seconds), as required.	**Values (seconds)** **122**

DPD Action	
Set the DPD action, hold or clear, as required.	**Values (seconds)** **Hold** Clear

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.

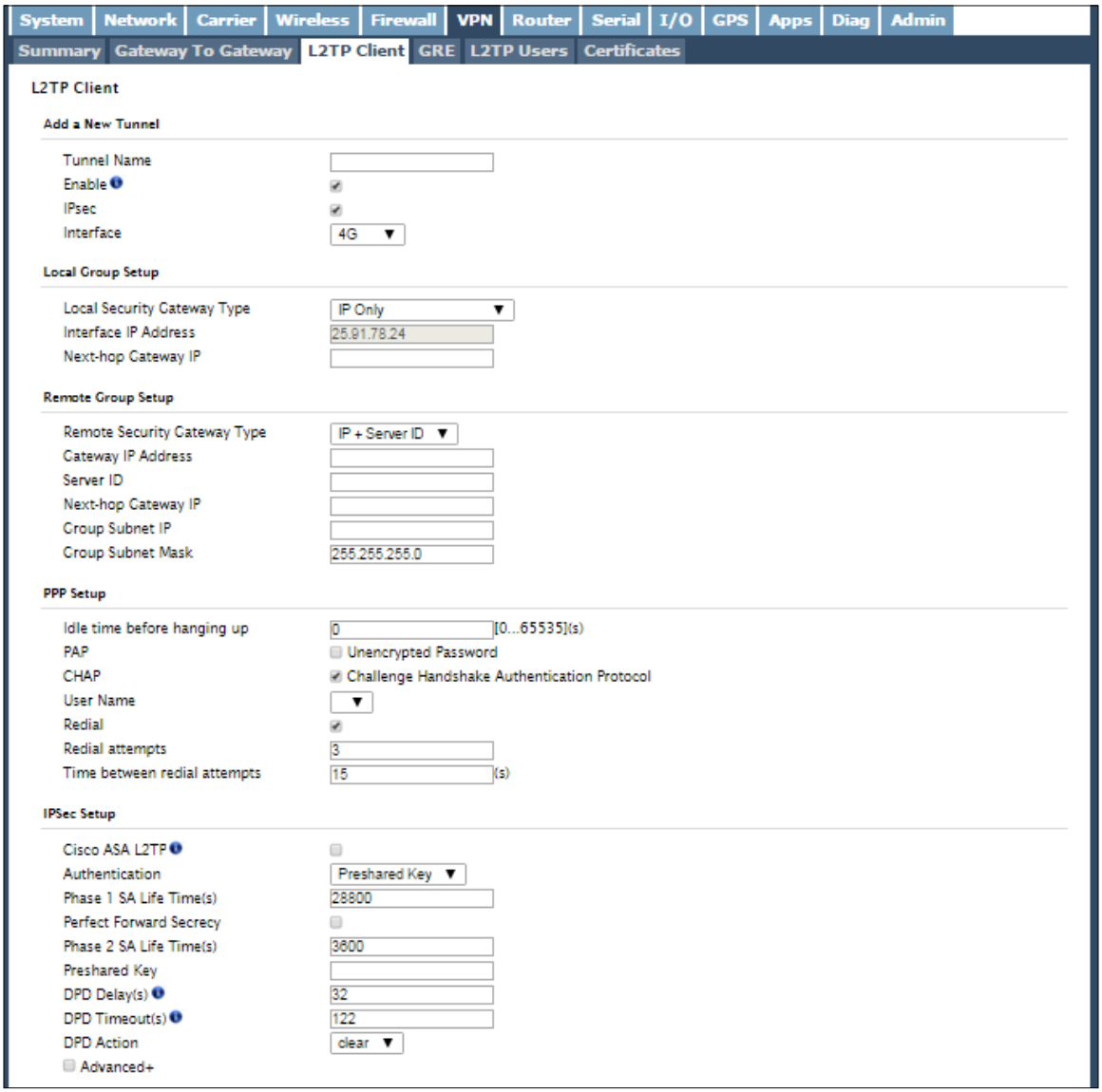


Image 4-6-3: VPN > Client to Gateway

Tunnel Name

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

Values (chars)

tunnel1

Enable

Used to enable (checked) is disable (unchecked) the VPN tunnel.

Values (checkbox)

Enable (Checked)

4.0 Configuration

Local Interface IP Address

This will display the current BulletPlus WAN (3G/Cellular) IP Address.

Values (IP Address)

Current IP

Remote Gateway IP Address

Enter the IP Address of the Remote Gateway that you wish to establish a connection with.

Values (IP Address)

none

Remote Server ID

Some servers require that you know the Server ID as well as the IP address. Enter the Server ID of the remote router here.

Values

none

Remote Subnet IP

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.

Values (IP Address)

none

Remote Subnet Mask

Enter the Remote Subnet Mask

Values (IP Address)

none

Idle time before hanging up

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)

Values (seconds)

0

Username

Enter the Username

Values (chars)

0

Preshared Key

The preshared key is required to connect to the L2TP Server.

Values (chars)

0

IPSec Setup - See previous sections for additional info.

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.

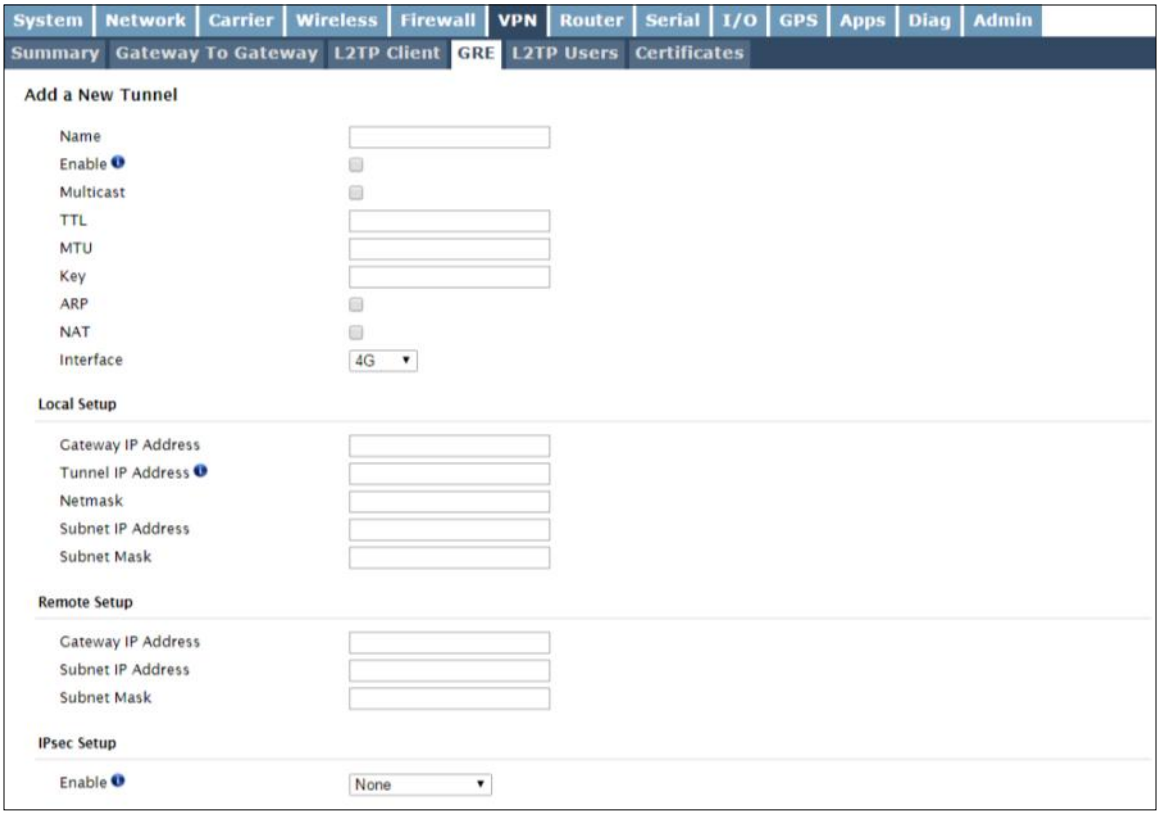


Image 4-6-4: Network > Edit/Add GRE Tunnel

Name

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

Values (Chars(32))

gre

Enable

Enable / Disable the GRE Tunnel.

Values (selection)

Disable / **Enable**

4.0 Configuration

Multicast	
Enable / Disable Multicast support over the GRE tunnel.	**Values (selection)** Disable / **Enable**

TTL	
Set the TTL (Time-to-live) value for packets traveling through the GRE tunnel.	**Values (value)** 1 - **255**

Key	
Enter a key is required, key must be the same for each end of the GRE tunnel.	**Values (chars)** *(none)*

ARP	
Enable / Disable ARP (Address Resolution Protocol) support over the GRE tunnel.	**Values (selection)** Disable / **Enable**

Local Setup

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

Gateway IP Address	
This is the WAN IP Address of the BulletPlus, this field should be populated with the current WAN IP address.	**Values (IP Address)** *(varies)*

Tunnel IP Address	
This is the IP Address of the local tunnel.	**Values (IP Address)** *(varies)*

Netmask	
Enter the subnet mask of the local tunnel IP address.	**Values (IP Address)** *(varies)*

Subnet IP Address	
Enter the subnet address for the local network.	**Values (IP Address)** *(varies)*

4.0 Configuration

Subnet Mask	
The subnet mask for the local network/subnet.	**Values (IP Address)** *(varies)*

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.

Gateway IP Address	
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.	**Values (IP Address)** *(varies)*

Subnet IP Address	
The is the IP Address of the remote network, on the remote side of the GRE Tunnel.	**Values (IP Address)** *(varies)*

Subnet Mask	
The is the subnet mask for the remote network/subnet.	**Values (IP Address)** *(varies)*

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 > L2TP Users

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

Image 4-6-5: VPN > VPN Client Access

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.

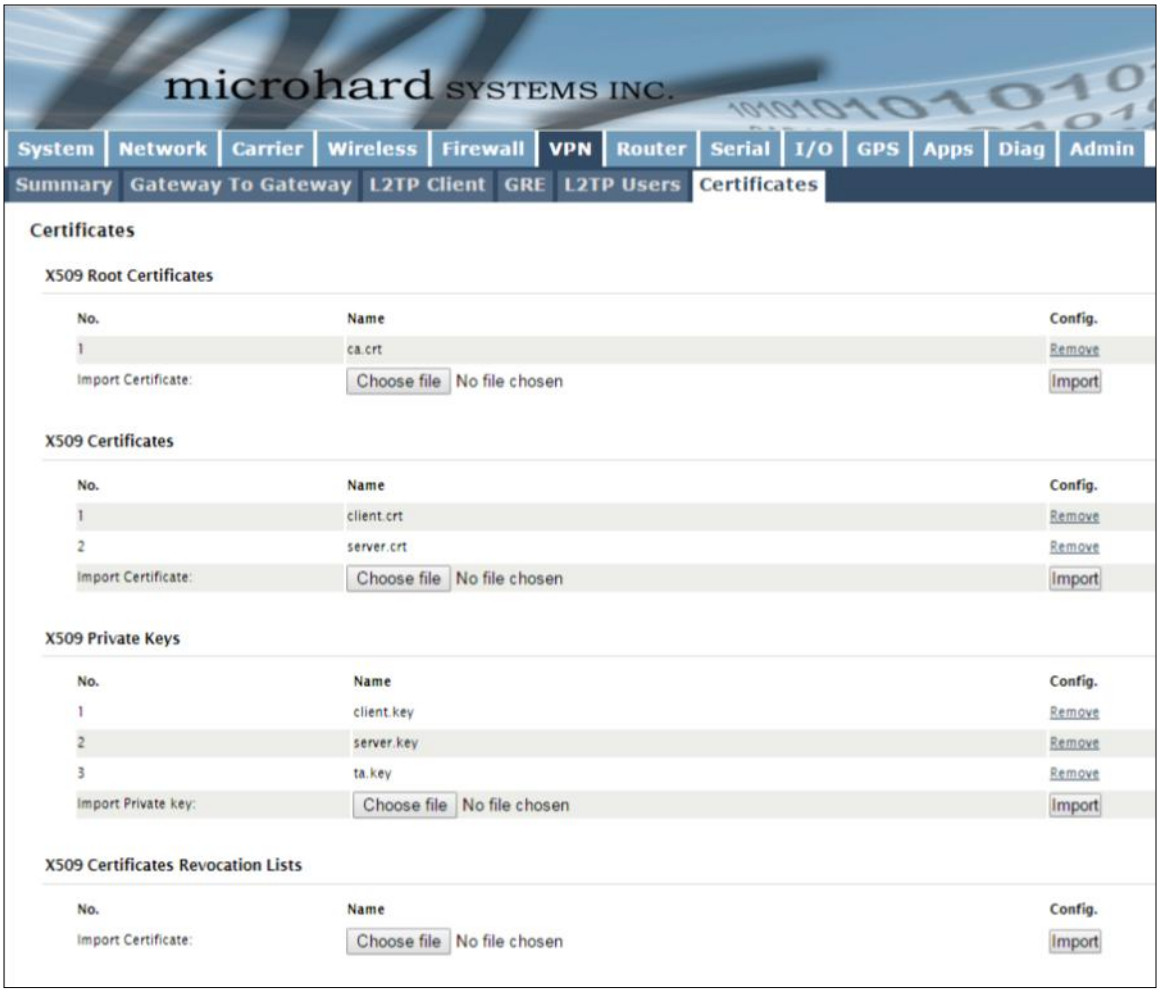


Image 4-6-6: VPN > Certificate Management

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.

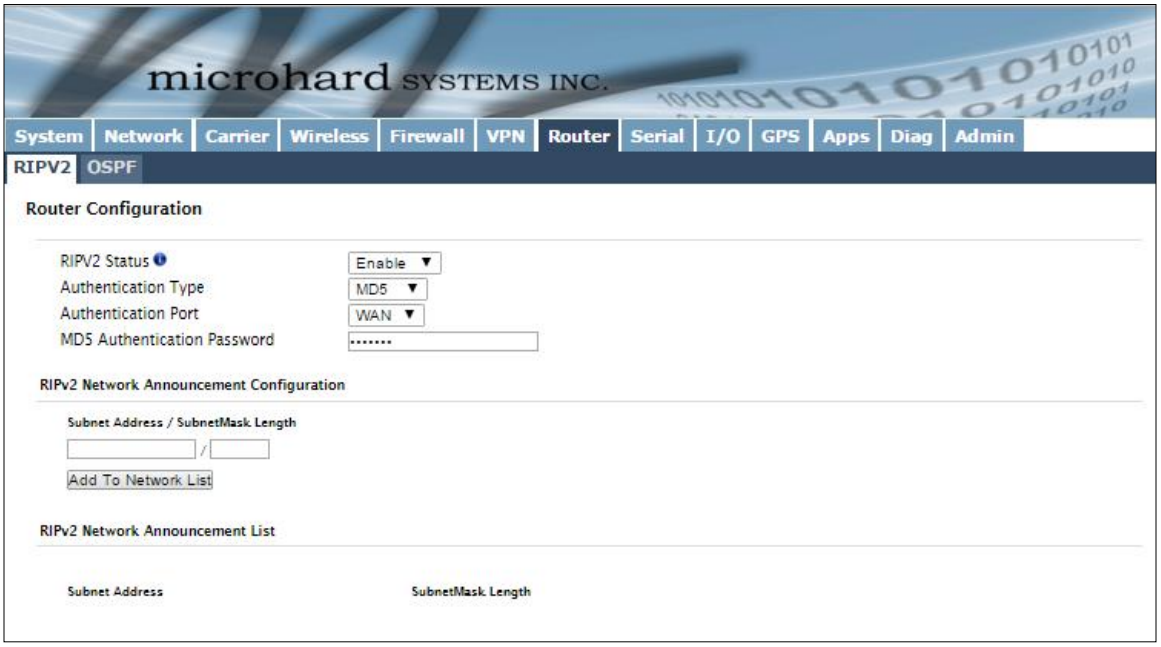


Image 4-7-1: Router > RIPv2

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.

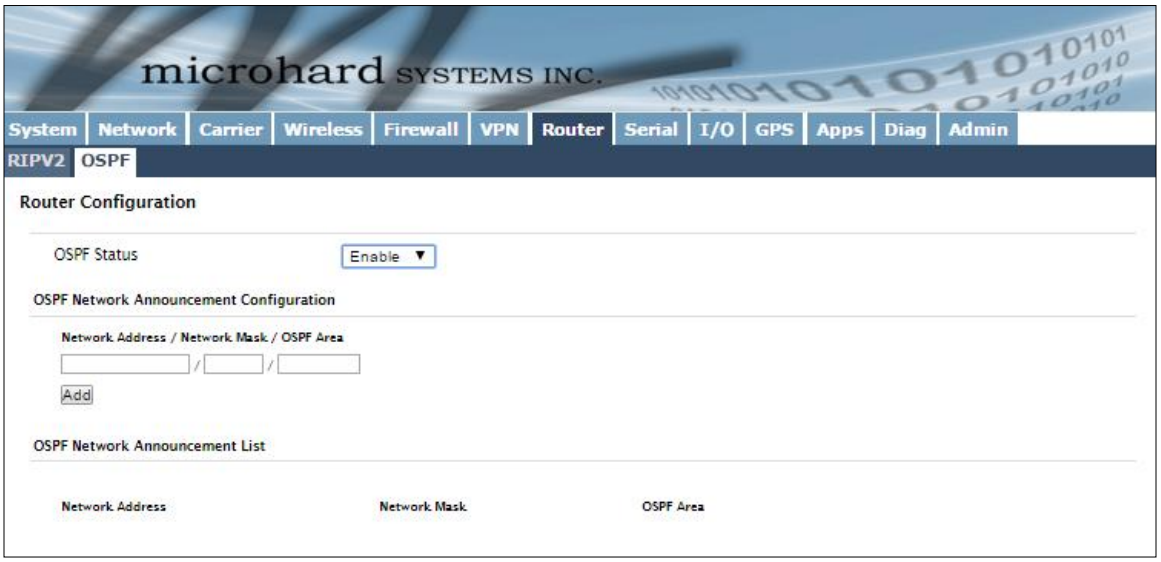


Image 4-7-2: Router > OSPF

OSPF Status

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

Values (selection)

Enable / **Disable**

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.

Values (Subnet/Length))

(no default)

4.0 Configuration

4.8 Serial

4.8.1 Serial > Summary

The Serial > Summary window gives a summary of the RS232 Serial Data Port located on the side of the Bullet, the port uses a standard DB-9 connector.

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

General Status

- Port Status - Shows if the RS232 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.

Image 4-8-1: Serial > Summary

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 a AT Command set. (115200/8/N/1)

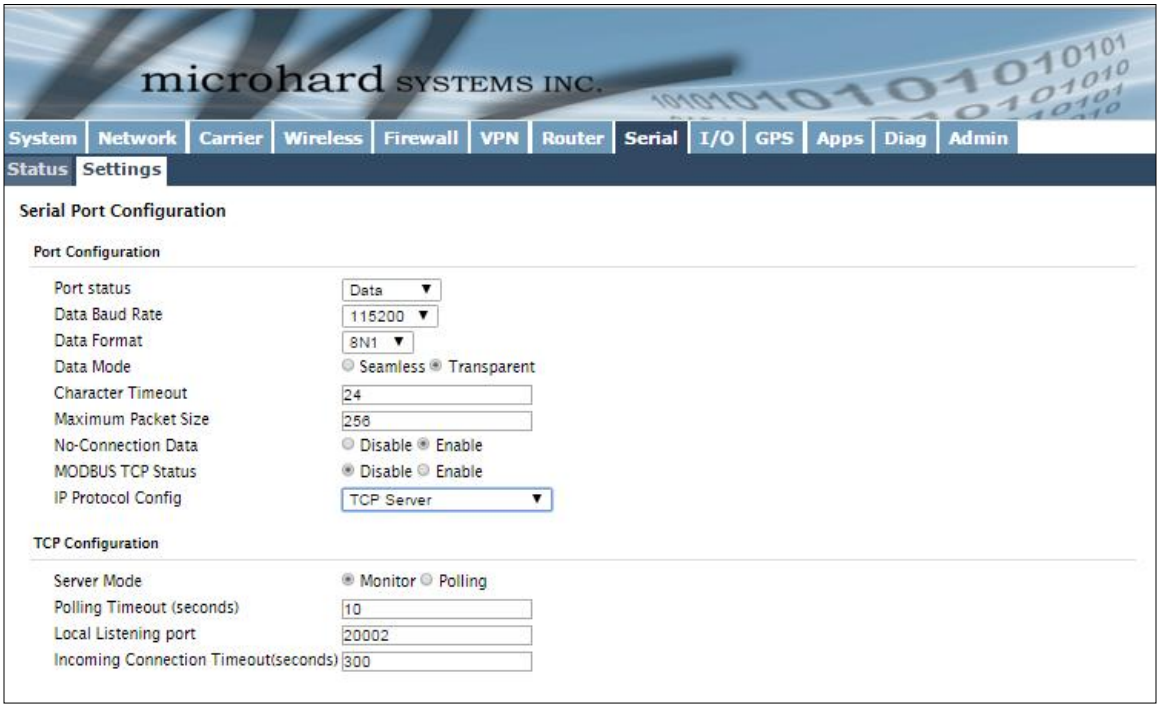


Image 4-8-2: Serial > Settings Configuration

4.0 Configuration

Port Status

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

Values (selection)

Disabled / Enable

Data Baud Rate

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

Values (bps)

921600	**9600**
460800	7200
230400	4800
115200	3600
57600	2400
38400	1200
28800	600
19200	300
14400	

Note: Most PCs do not readily support serial communications greater than 115200bps.

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.

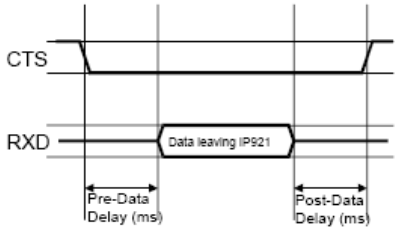
Values (selection)

8N1 / 8E1 / 8O1

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.

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



Drawing 4A: CTS Output Data Framing

Values (selection)

None
Hardware
CTS Framing

Pre-Data Delay

Refer to **Drawing 4A** above.

Values (time (ms))

100

Post-Data Delay

Refer to **Drawing 4A** above.

Values (time (ms))

100

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.

Values (selection)

Seamless / **Transparent**

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.

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.

Values (characters)

24

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).

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.

Values (bytes)

1024

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.

Values (selection)

Disable / Enable

MODBUS TCP Status

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

Values (selection)

Disable / Enable

MODBUS TCP Protection Key

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

Values (string)

1234

4.0 Configuration

IP Protocol Config

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.

Values (selection)

TCP Client
TCP Server
TCP Client/Server
UDP Point-to-Point
SMTP Client
PPP
GPS Transparent Mode

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.

UDP: User Datagram Protocol does not provide sequencing information for the packets sent nor does it establish a 'connection' ('handshaking') and is therefore most suited to communicating small packets of data.

- **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.

TCP: Transmission Control Protocol in contrast to UDP does provide sequencing information and is connection -oriented; a more reliable protocol, particularly when large amounts of data are being communicated.

Requires more bandwidth than UDP.

- **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

IP Protocol Config (Continued…)

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.

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.

- **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.

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.

- 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**

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.

- 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**

4.0 Configuration

IP Protocol Config (Continued…)

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.

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

- 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 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 doe 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**

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:

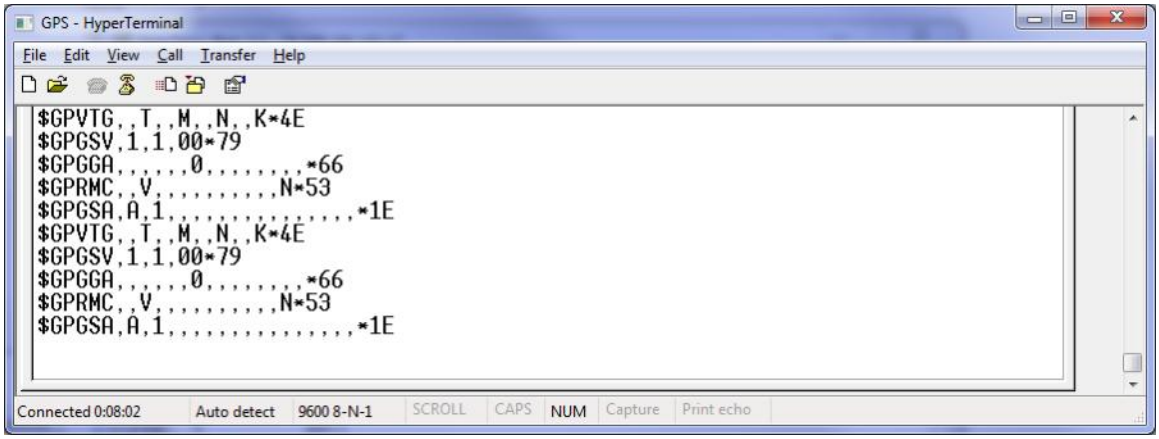


Image 4-8-3: Serial > GPS Transparent Mode

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 a 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

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

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.

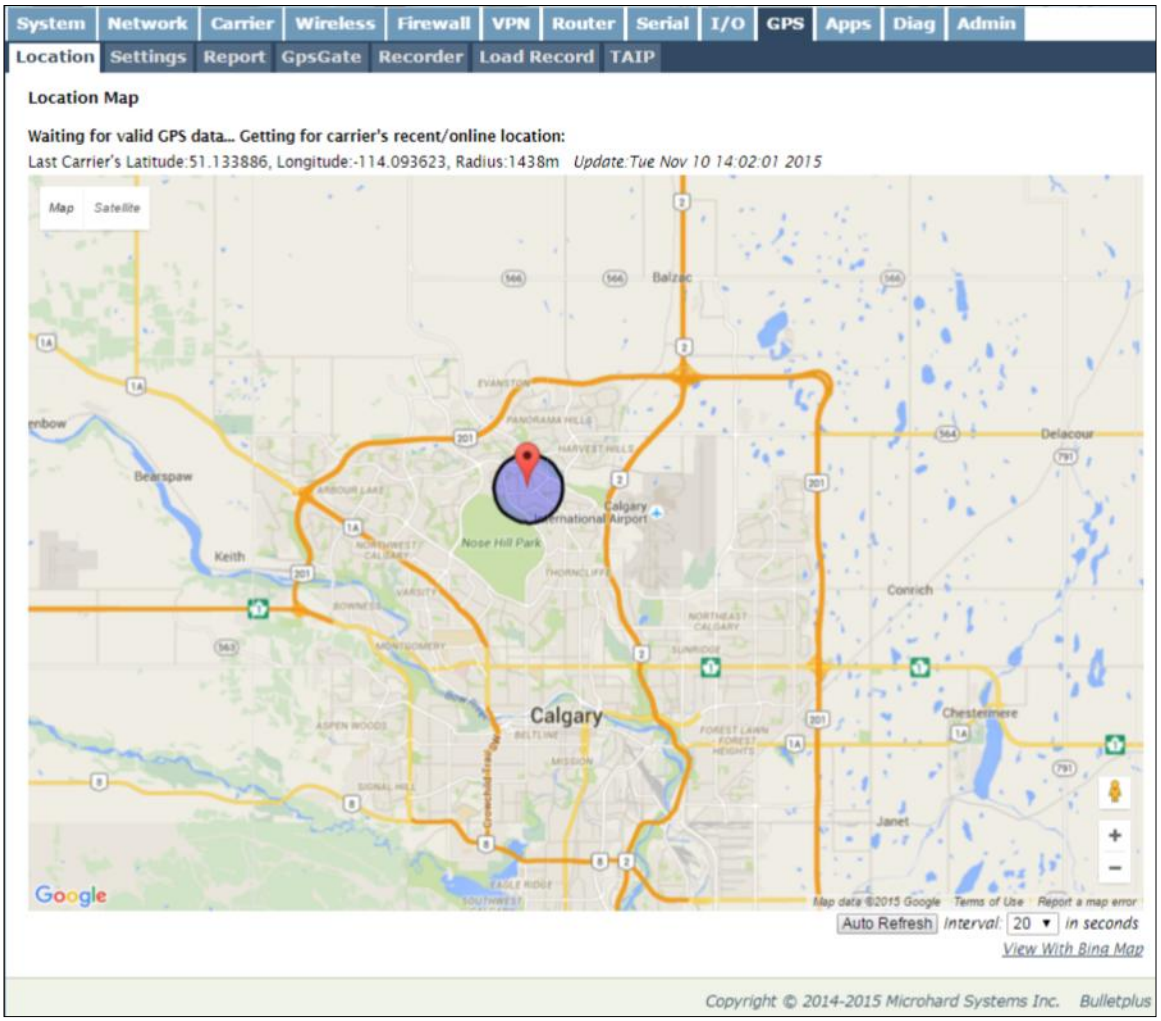


Image 4-10-1: GPS > Location Map

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

4.0 Configuration

4.10.3 GPS > Report

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

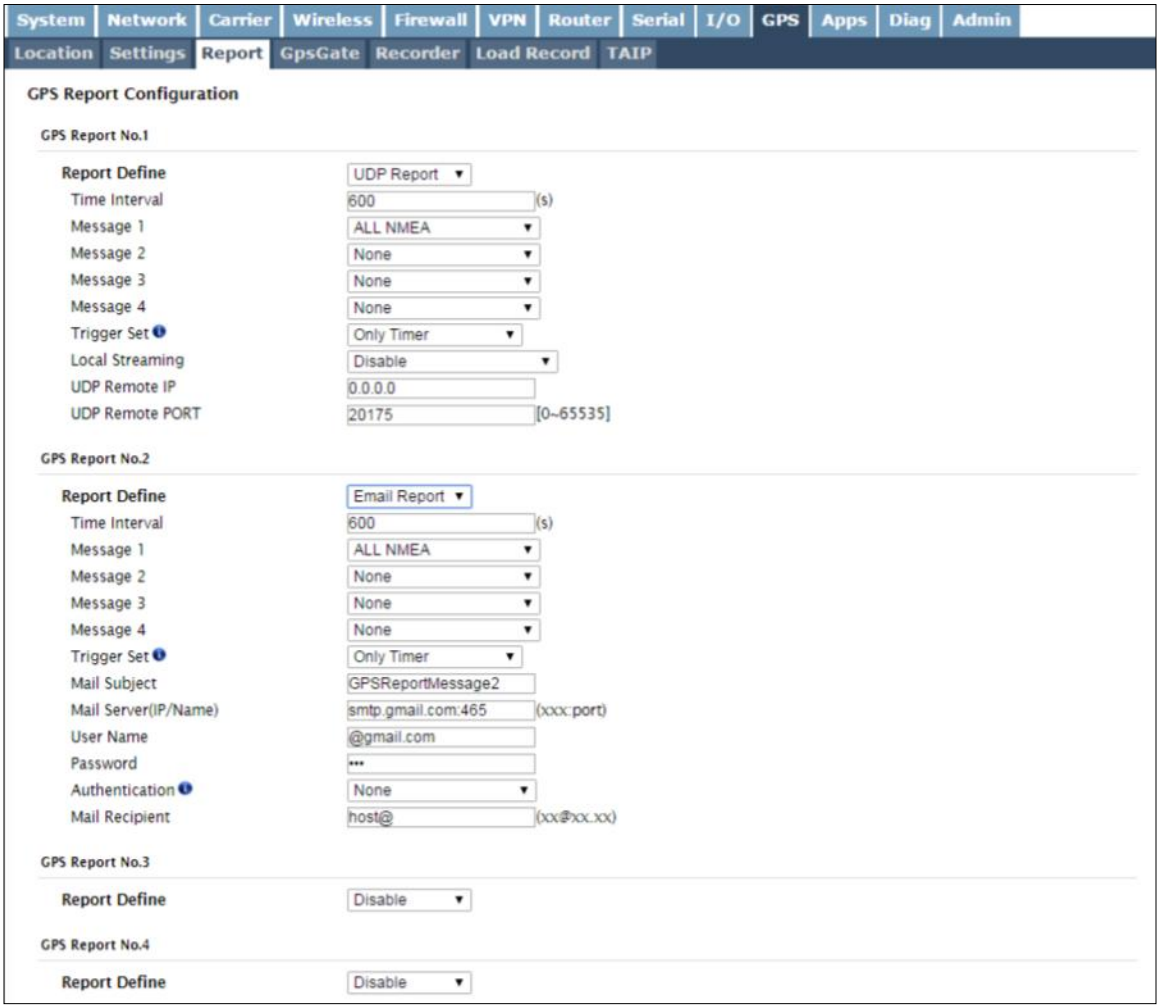


Image 4-10-3: GPS > GPS Report

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.

None	-	Message is not used, no data will be sent
ALL	-	Sends all of the below
GGA	-	GPS Fix Data
GSA	-	Overall Satellite Data
GSV	-	Detailed Satellite Data
RMC	-	Recommended Min Data for GPS
VTG	-	Vector Track & Ground Speed
GPSGate	-	For use with GPSGate Tracking Software

Values (selection)

None
ALL NMEA
GGA
GSA
GSV
RMC
VTG
Latitude/Longitude
GPSGate UDP Protocol

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.

Values (selection)

Only Timer
Timer AND Distance
Timer OR Distance

Distance Set

The distance parameter allows the GPS data to only be sent when a specified distance has been traveled since the last report.

Values (meters)

1000

UDP Remote IP / Port

This is the IP Address and port of the remote host in which the UDP packets are to be sent.

Values (Address/Port)

0.0.0.0 / 20175

Mail Subject

If an Email report is chosen, the subject line of the Email can be defined here.

Values (characters)

1000

Mail Server

If an Email report is to be sent, the outgoing mail server must be defined, and the port number.

Values (Address:port)

smtp.gmail.com:465

Username / Password

Some outgoing mail servers required username and password to prevent an account being used for spam. Enter the login credentials here.

Values (characters)

Username / password

Mail Recipient

Some outgoing mail servers require a username and password to prevent an account being used for spam. Enter the login credentials here.

Values (characters)

host@email.com

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)

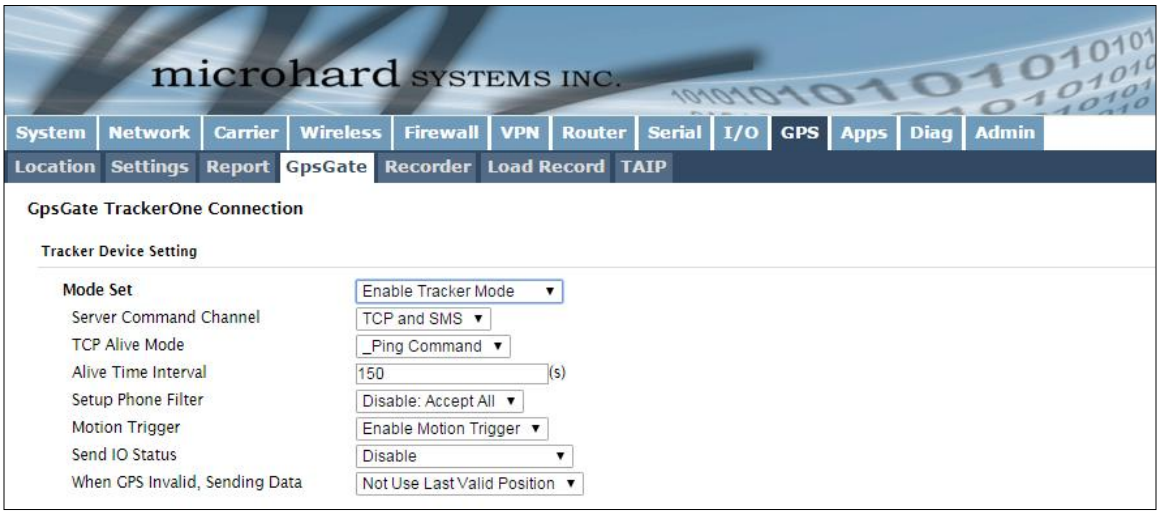


Image 4-10-4: GPS > GpsGate Tracker Mode

GpsGate - Tracker Mode

Mode Set

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.

Values (selection)

Disable
Enable Tracker Mode
Enable TCP Send Mode

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.

Values (seconds)

TCP and SMS
TCP Only
SMS Only

TCP Alive Mode / Alive Time Interval

TCP alive mode will keep TCP connection alive if tracker is not enabled or the tracker interval is too long. The default is 150 seconds.

Values (seconds)

150

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

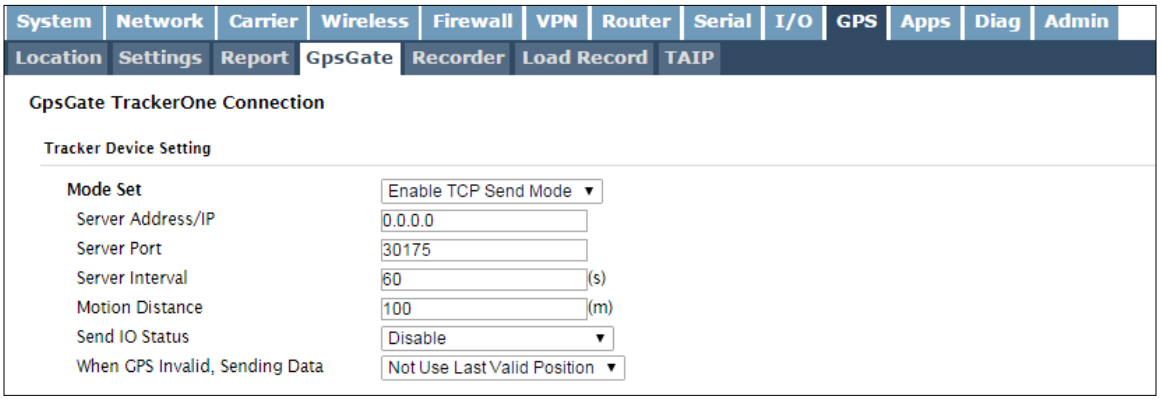


Image 4-10-5: GPS > GpsGate TCP Mode

4.0 Configuration

Mode Set

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.

Values (selection)

Disable
Enable Tracker Mode
Enable TCP Send Mode

Server Address / IP

Enter the IP Address of the server running the GpsGate application.

Values (IP Address)

0.0.0.0

Server Port

Enter the TCP Port of the server running the GpsGate application.

Values (Port)

30175

Server Interval

Define the interval at which the BulletPlus will send data to the GpsGate Server.

Values (seconds)

60

Motion Distance

Set the motion threshold in which the BulletPlus will be triggered to send location data.

Values (meters)

100

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

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.

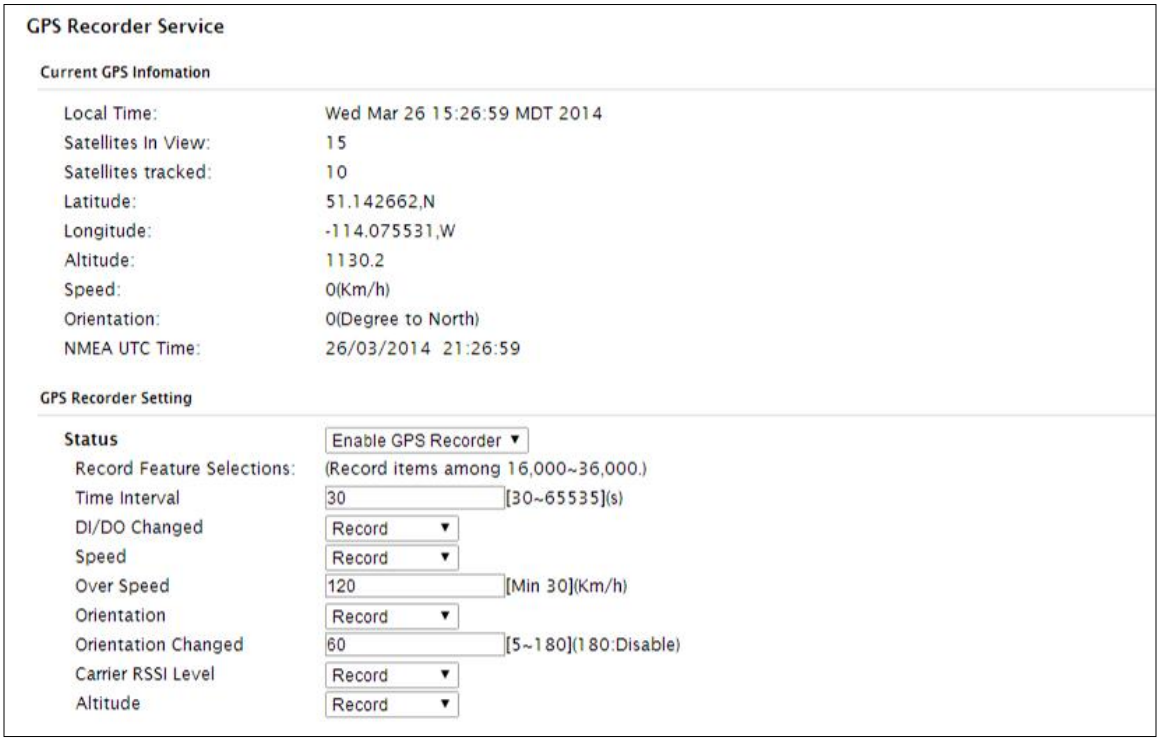


Image 4-10-6: GPS > GPS Recorder Service

Status

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

Define the interval at which the BulletPlus will record GPS data. If there is no valid data available at the specified time (i.e. no connected satellites), the unit will wait until the next time valid information is received.

Values (seconds)

300

DI/DO Changed

The BulletPlus can detect and report the current GPS info when a digital input or output status changes, regardless of the time interval setting.

Values (selection)

Record / **Don't Record**

4.0 Configuration

Speed	
Select Record to include the current speed in the reported data.	**Values (selection)** Record / **Don't Record**

Over Speed	
Trigger a GPS record entry when the speed has exceeded the configured threshold. A minimum of 30 Km/hr is required.	**Values (Km/hr)** **120**

Orientation	
Select Record to record the current orientation when a GPS entry is recorded. (Degree to North).	**Values (selection)** Record / **Don't Record**

Orientation Changed	
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)	**Values (5 ~ 180)** **60**

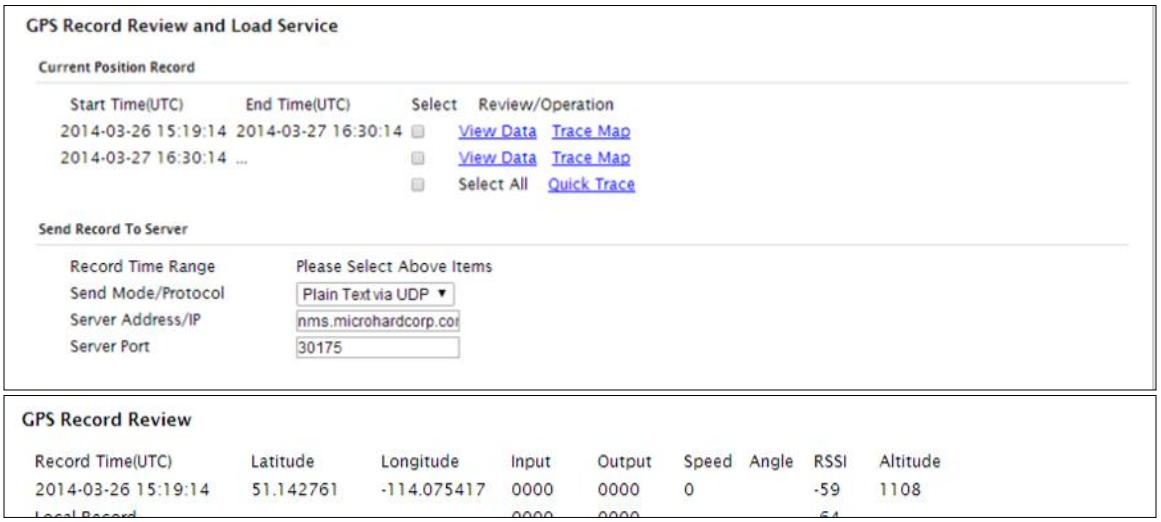
Carrier RSSI Level	
Select Record to record the current 3G/Cellular RSSI level when a GPS entry is recorded. (-dB).	**Values (selection)** Record / **Don't Record**

Altitude	
Select Record to record the current Altitude when a GPS entry is recorded (meters).	**Values (selection)** Record / **Don't Record**

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.



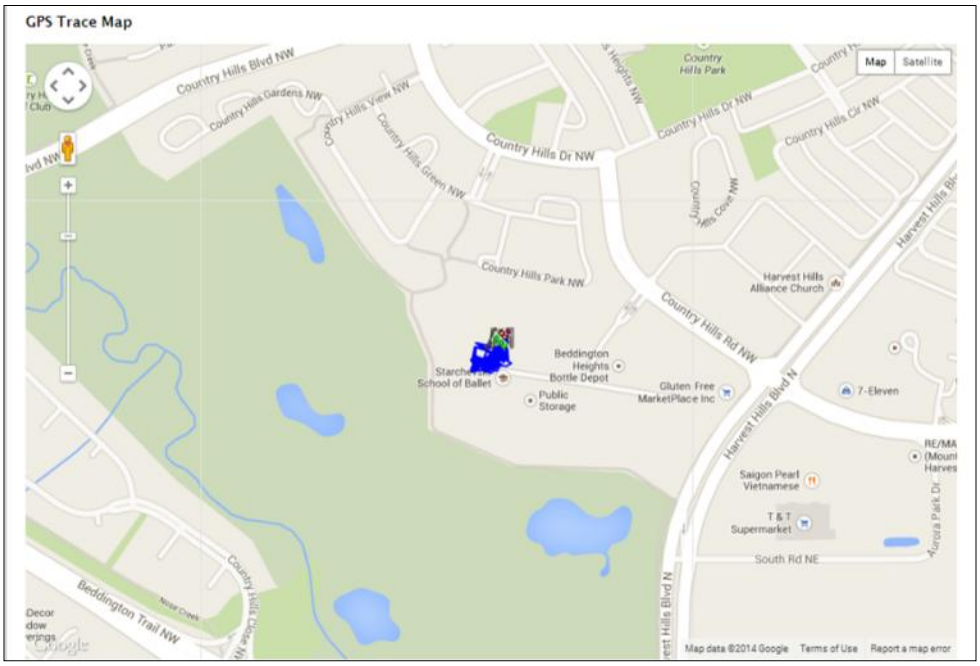


Image 4-10-7: GPS > GPS Load Record

4.0 Configuration

Record Time Range	
Check the boxes next to the records listed above that are to be sent to the server.	**Values (selection)** *(no default)*

Send Mode / Protocol	
Specify the data format / protocol type for the data to be sent.	**Values (selection)** NMEA via UDP NMEA via TCP GpsGate via UDP GpsGate via TCP **Plain Text via UDP** Plain Text via TCP

Server Address/IP	
Enter the address or IP address of the remote server to which the data is to be sent.	**Values (IP)** nms.microhardcorp.com

Server Port	
Enter the UDP/TCP port number of the remote server to which the data is to be sent.	**Values (Port)** 30175

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.

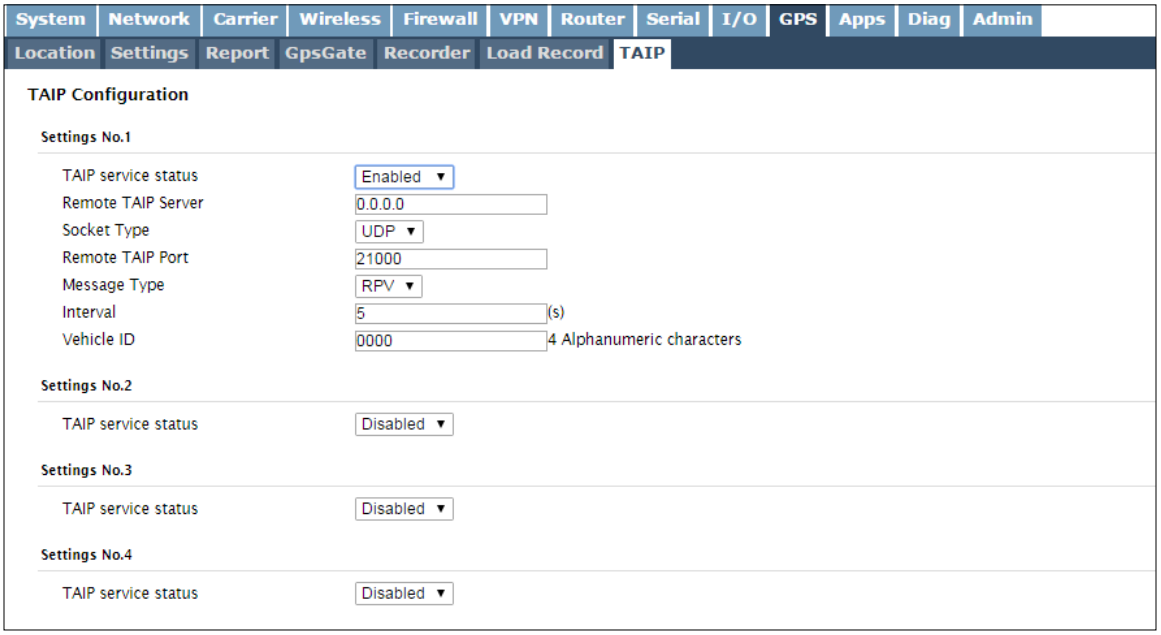


Image 4-10-8: GPS > TAIP

TAIP service status

Enable or disable TAIP service on the modem. The unit can report TAIP to up to 4 different hosts.

Values (selection)

Enable / **Disable**

Remote TAIP Server

Enter the IP Address of the Remote TAIP Server.

Values (IP Address)

0.0.0.0

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.

Values (selection)

UDP / TCP

Remote TAIP Port

Enter the TCP or UDP port number used on the Remote TAIP server.

Values (TCP/UDP)

UDP / TCP

4.0 Configuration

Message Type	
Select between RPV and RLN message types. RPV - Position/Velocity RLN - Long Navigation Message	**Values (selection)** **RPV** / RLN

Interval	
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.	**Values (seconds)** 60

Vehicle ID	
Set the Vehicle ID using 4 alpha-numeric characters.	**Values (chars)** **0000**

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.

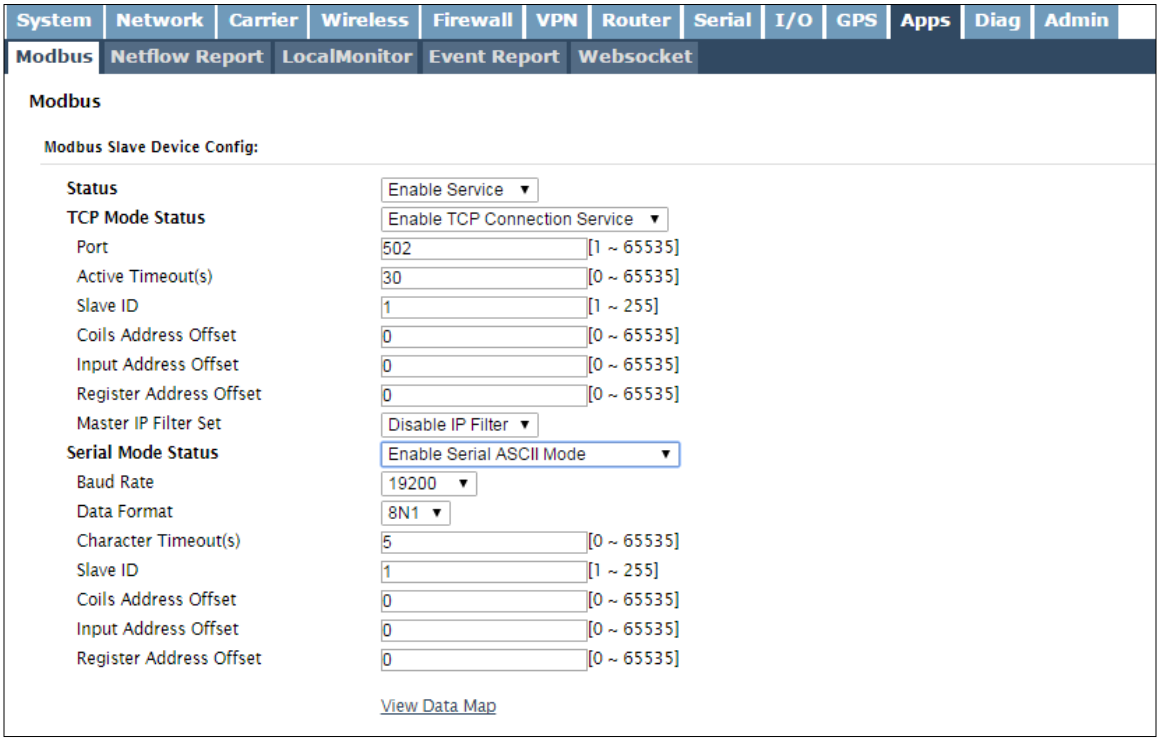


Image 4-11-1: Apps > Modbus

Status

Disable or enable the Modbus service on the BulletPlus.

Values (selection)

Disable Service
Enable Service

TCP Mode Status

Disable or enable the Modbus TCP Connection Service on the BulletPlus.

Values (selection)

Disable
Enable

4.0 Configuration

Port	
Specify the Port in which the Modbus TCP service is to listen and respond to polls.	**Values (Port #)** **502**

Active Timeout(s)	
Define the active timeout in seconds.	**Values (seconds)** **30**

Slave ID	
Each Modbus slave device must have a unique address, or Slave ID. Enter this value here as required by the Modbus Host System.	**Values (value)** **1**

Coils Address Offset	
Enter the Coils Address offset as required by the Master.	**Values (value)** **0**

Input Address Offset	
Enter the Input Address offset as required by the Master.	**Values (value)** **0**

Register Address Offset	
Enter the Register Address offset as required by the Master.	**Values (value)** **0**

Master IP Filter Set	
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.	**Values (selection)** **Disable /** Enable

4.0 Configuration

4.11.1.2 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.

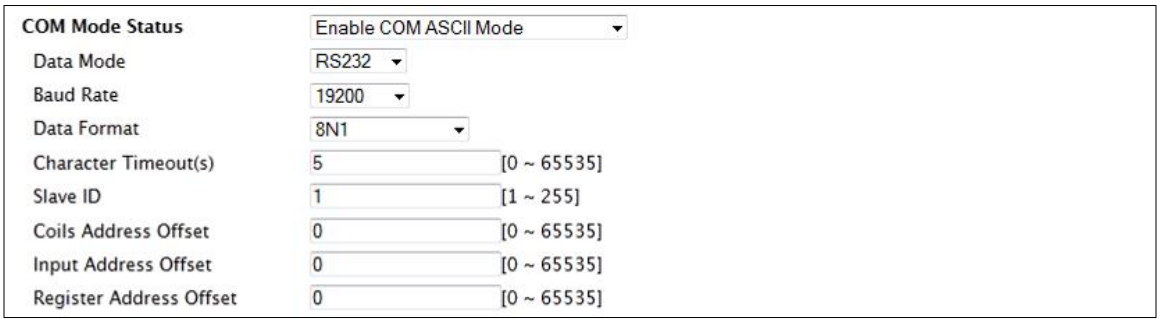


Image 4-11-2: Apps > Modbus Serial Configuration

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.

Values (selection)

Disable
Enable COM ASCII Mode
Enable COM RTU Mode

Baud Rate

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

Values (selection (bps))

921600	57600	14400	3600
460800	38400	**9600**	2400
230400	28800	7200	1200
115200	19200	4800	600

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.

Values (selection)

8N1 / 8E1 / 8O1

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):

Bit Address	Hex Format	Definition
0	0x0000	OUTPUT 1
1	0x0001	OUTPUT 2
9	0x0009	Serial Status
12	0x000c	LAN/eth0 Status(Read)
13	0x000d	WAN/eth1 Status(Read)
16	0x0010	Carrier Status
18	0x0012	Wifi Status
22	0x0016	GPS Status
23	0x0017	Location Over Network
24	0x0018	Event UDP Report 1
25	0x0019	Event UDP Report 2
26	0x001a	Event UDP Report 3
27	0x001b	NMS Report
28	0x001c	Web Client Service
32	0x0020	Carrier Connection(Read)
40	0x0028	SYSTEM Reboot

Input Bits:(if config)

Bit Address	Hex Format	Definition
0	0x0000	INPUT 1
1	0x0001	INPUT 2

Registers:

16 Bits Address	Hex Format	Definition
0	0x0000	Modem Model Type...
1	0x0001	Build Version
2	0x0002	Modem ID Highest 2 Bytes
3	0x0003	Modem ID Higher 2 Bytes
4	0x0004	Modem ID Lower 2 Bytes
5	0x0005	Modem ID Lowest 2 Bytes
6	0x0006	RSSI(dbm)
7	0x0007	VDC(x100)(V)
8	0x0008	Core Temperature(C)
9	0x0009	Carrier Received Bytes(MB)
10	0x000a	Carrier Transmitted Bytes(MB)
11	0x000b	GPS Altitude(m)
12	0x000c	GPS Latitude High 2 Bytes
13	0x000d	Latitude Low 2 Bytes(x1000000)
14	0x000e	GPS Longitude High 2 Bytes
15	0x000f	Longitude Low 2 Bytes(x1000000)
18	0x0012	Serial Baud Rate(/100)(bps)
19	0x0013	Serial Data Format...

Caculation: Real Latitude = (signed integer)[High 2 Bytes + Low 2 Bytes] / 1

Modem Model Types:

Type ID	Definition
0	Unknow
6	IPn3G
7	VIP4G
8	IPn4G
9	IPn3Gii
10	IPn4Gii
11	PWii/BulletPlus

Com Data Format Definition:

Type ID	Definition
0	Unknow
1	8N1
2	8N2
3	8E1
4	8O1
5	7N1
6	7N2
7	7E1
8	7O1
9	7E2
10	7O2

Image 4-11-3: Applications > Modbus Data Map

4.0 Configuration

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 identity bandwidth issues and to understand data needs. Standard Netflow Filters can be applied to narrow down results and target specific data requirements.

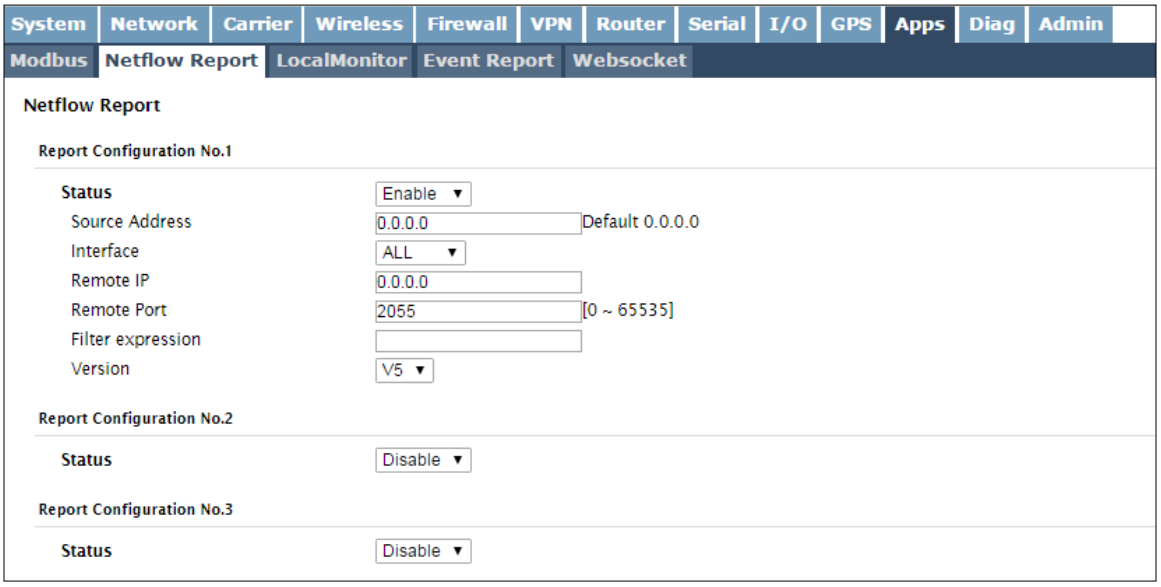


Image 4-11-4: Apps > Netflow Report

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

Remote IP	
The Remote IP is the IP Address of the NetFlow collector where the flow reports are be sent.	**Values (IP Address)** **0.0.0.0**

Remote Port	
Enter the Remote Port number.	**Values (IP Address)** **0**

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.*	**Values (chars)** *(no default)*

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.

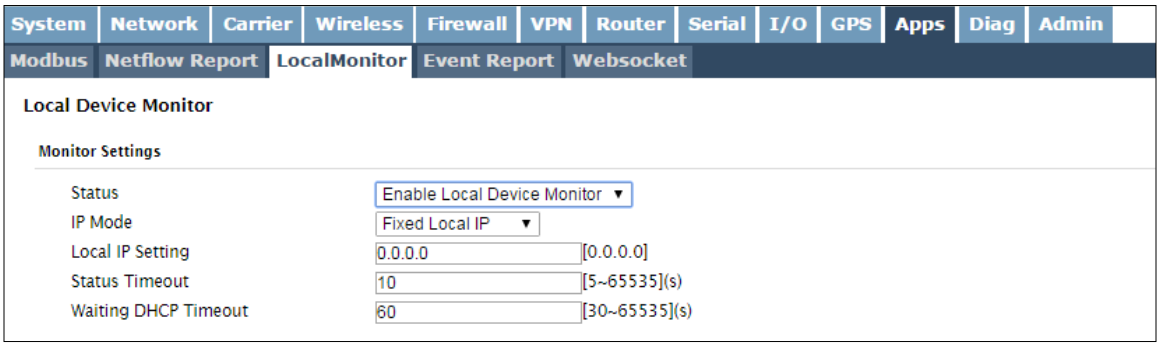


Image 4-11-5: Apps > Local Monitor

Status

Enable or disable the local device monitoring service.

Values (selection)

Disable / Enable

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.

Values (selection)

Fixed local IP
Auto Detected IP

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.

Values (IP)

0.0.0.0

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)

Values (seconds)

10

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)

Values (seconds)

60

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.

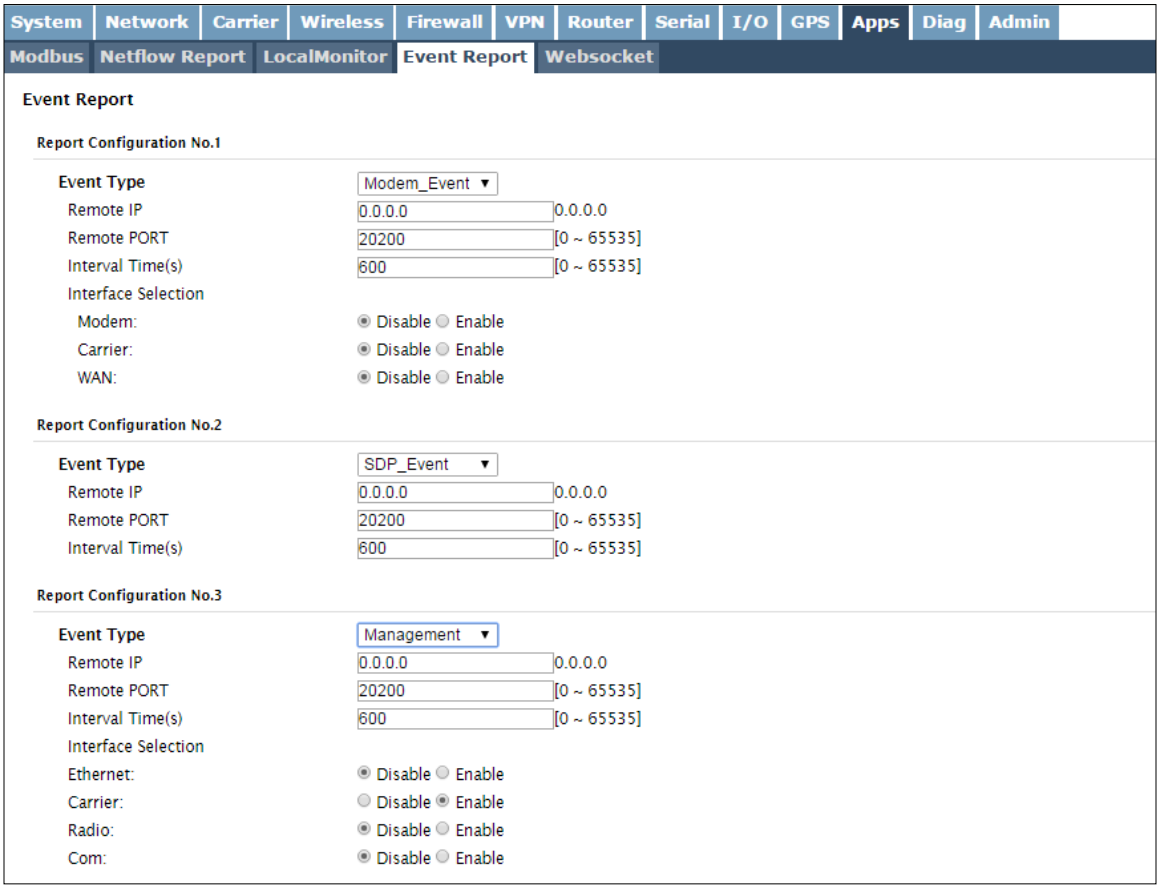


Image 4-11-6: Applications > Event Report

Event Type

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.

Values (selection)

Modem_Event
SDP_Event
Management

Remote IP

Enter the IP Address of a reachable host to send the UDP packets

Values (IP Address)

0.0.0.0

4.0 Configuration

Remote Port	
Specify the UDP port number of the Remote IP Address. *Default Port Numbers for Microhard NMS (20100 for modem events, 20200 for Management)	**Values (Port #)** **20200**

Interval Time(s)	
This is the interval time in seconds, that the BulletPlus will send the configured UDP message to the Remote IP and Port specified.	**Values (seconds)** **600**

Message Info Type	
When Modem_Event is selected, up to three different payloads can be selected.	**Values (seconds)** **Modem** **Carrier** **WAN**

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:

Content length	-	2 BYTES (UINT16_T)
Modem name	-	STRING (1-30 bytes)
Hardware version	-	STRING (1-30 bytes)
Software version	-	STRING (1-30 bytes)
Core temperature	-	STRING (1-30 bytes)
Supply voltage	-	STRING (1-30 bytes)
Local IP Address	-	4 BYTES (UINT32_T)
Local IP Mask	-	4 BYTES (UINT32_T)

Carrier info:

Content length	-	2 BYTES (UINT16_T)
RSSI	-	1 BYTE (UINT8_T)
RF Band	-	2 BYTES (UINT16_T)
3G_Network	-	STRING (1-30 Bytes)
Service type	-	STRING (1-30 Bytes)
Channel number	-	STRING (1-30 Bytes)
SIM card number	-	STRING (1-30 Bytes)
Phone number	-	STRING (1-30 Bytes)

WAN Info:

Content length	-	2 BYTES (UINT16_T)
IP address	-	4 BYTES (UINT32_T)
DNS1	-	4 BYTES (UINT32_T)
DNS2	-	4 BYTES (UINT32_T)

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 infomation+wanip infomation.

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

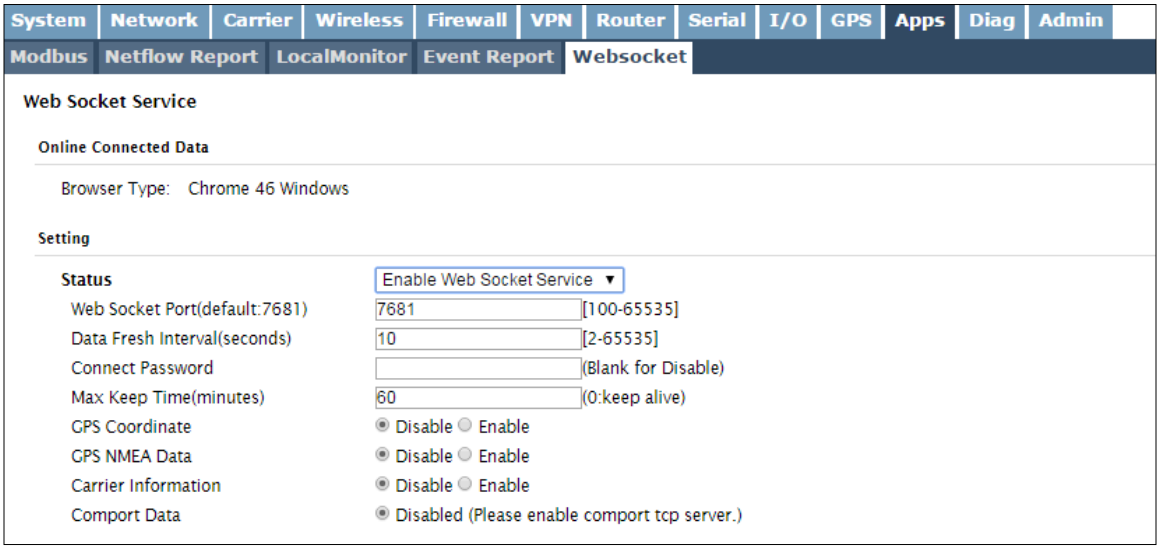


Image 4-11-7: Applications > Web Socket Service

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

Data Fresh Intervals	
Enter in the time at which data is to be refreshed. The default is 10 seconds, the valid range is 2 to 65535 seconds.	**Values (seconds)** 10

Connect Password	
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.	**Values** *(blank)*

Max Keep Time	
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 with continue to run indefinitely.	**Values (minutes)** **60**

GPS Coordinate	
If enabled the modem will report GPS coordinate data to the websocket.	**Values (selection)** **Disable** / Enable

GPS NMEA Data	
If enabled the modem will report GPS NMEA data to the websocket.	**Values (selection)** **Disable** / Enable

Carrier Information	
If enabled the modem will report carrier information to the websocket.	**Values (selection)** **Disable** / Enable

Comport Data	
If enabled, and the RS232 port is configured for TCP Server, the comport data will be reported to the web socket.	**Values (selection)** **Disable** / Enable

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.

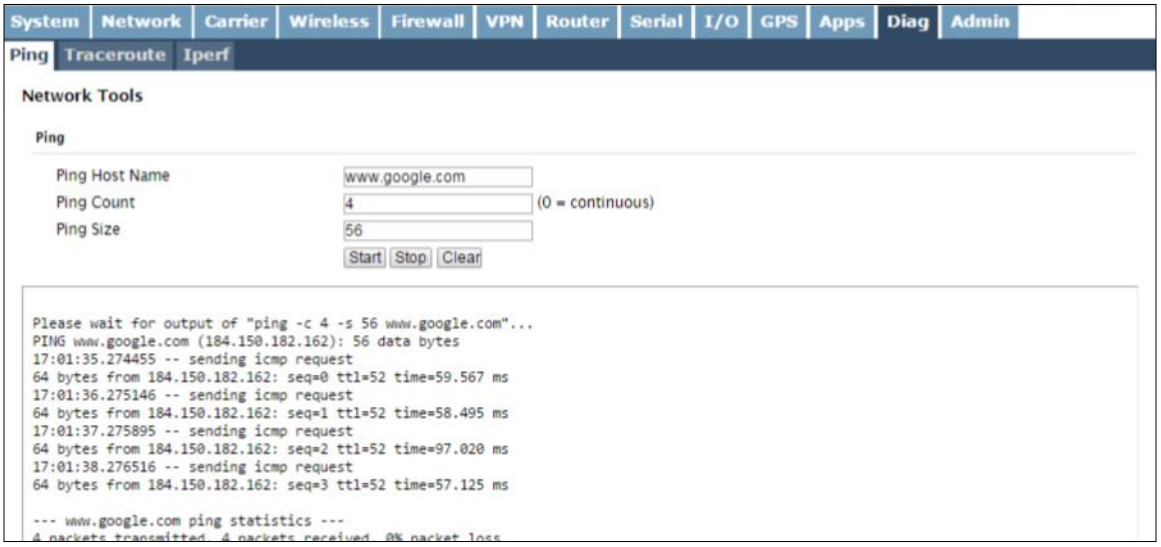


Image 4-12-1: Diag > Ping

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.

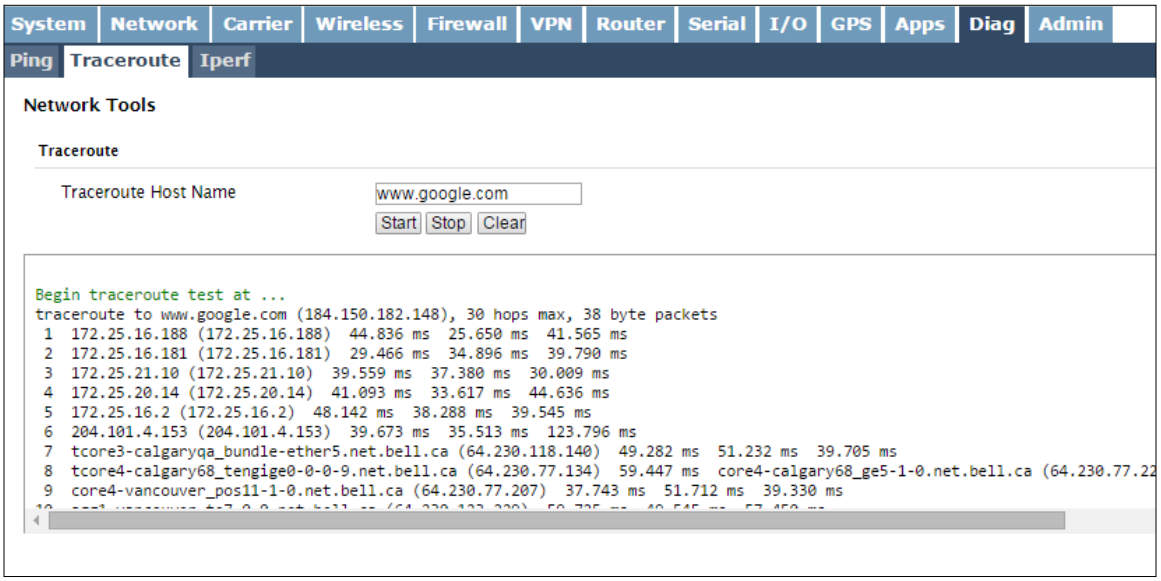


Image 4-12-2: Diag > Traceroute

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.

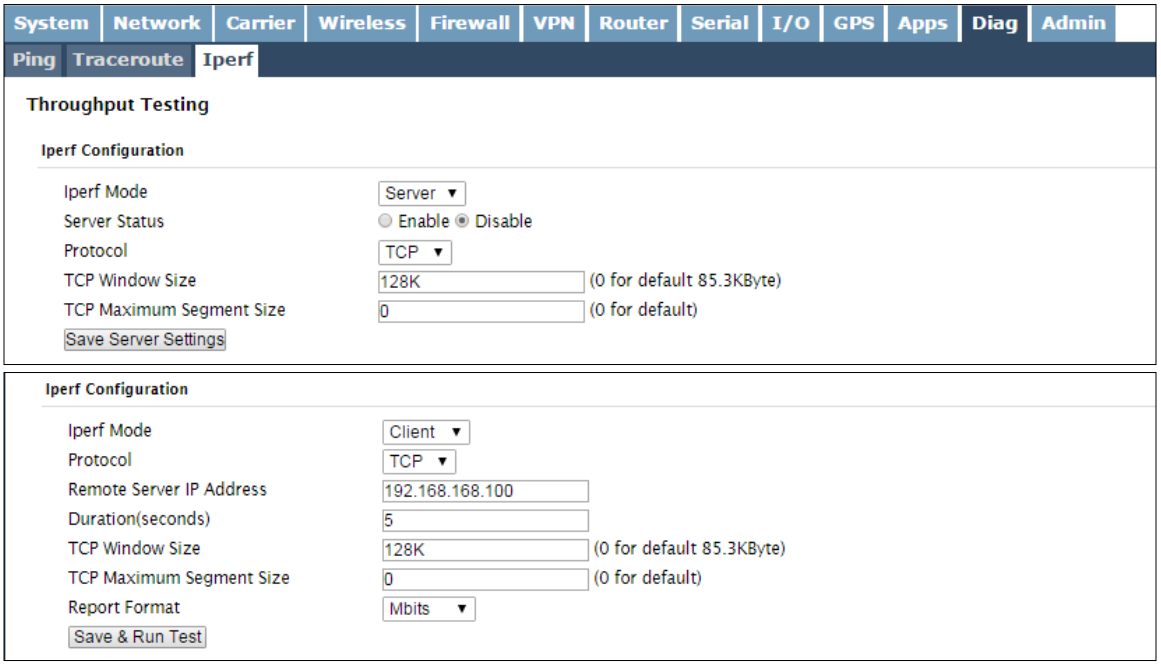


Image 4-12-3: Diag > Iperf

Iperf Mode

Select between an Iperf Server (listens for incoming connections) and client (initiates a connection with a server)

Values (selection)

Server / Client

Server Status

If the Iperf mode to set to Server, this Server Status allows a user to Enable or Disable the server.

Values (selection)

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.

Values (selection)

TCP / UDP

4.0 Configuration

TCP Window Size

Set the TCP Window size for the Iperf Cleint/Server. The recommended default is 85.3K, which can be set by entering 0.

Values (kbytes)

0

TCP Maximum Segment Size

Set the TCP Max Segment Size for the Iperf Cleint/Server. Set to 0 for recommended settings.

Values (string)

0

Remote Server Address

When in Client mode, select the Iperf Server by entering its IP Address here.

Values (IP Address)

192.168.168.100

Duration

When in Client mode, select the duration of the test (in seconds). The default is 5.

Values (seconds)

5

Report Format

Select the format to display the bandwidth numbers in. Supported formats are:

'Kbits' = Kbits/sec
'Mbits' = Mbits/sec
'Kbytes' = KBytes/sec
'M'bytes = MBytes/sec

Values (selection)

Kbits
Mbits
Kbytes
Mbytes

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.

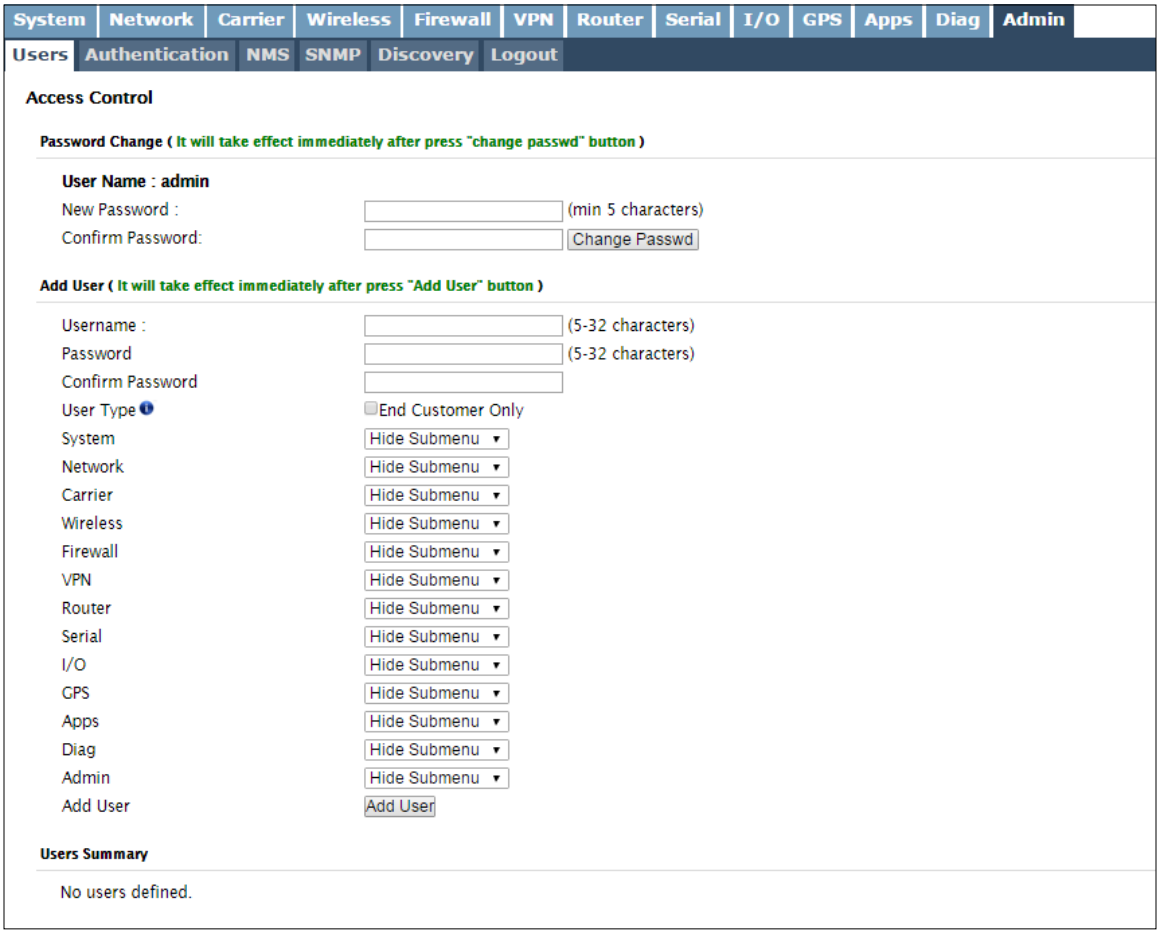


Image 4-13-1: Users > Password Change

New Password

Enter a new password for the 'admin' user. It must be at least 5 characters in length. The default password for 'admin' is 'admin'.

Values (characters)

admin

Confirm Password

The exact password must be entered to confirm the password change, if there is a mistake all changes will be discarded.

Values (characters)

admin

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.

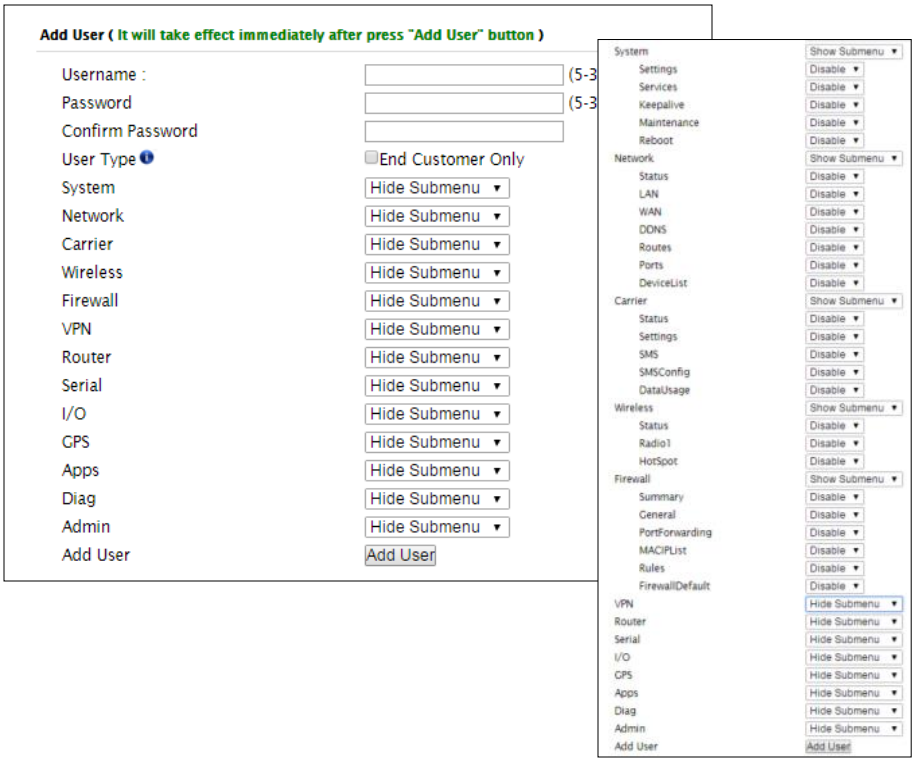


Image 4-13-2: Access Control > Users

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.

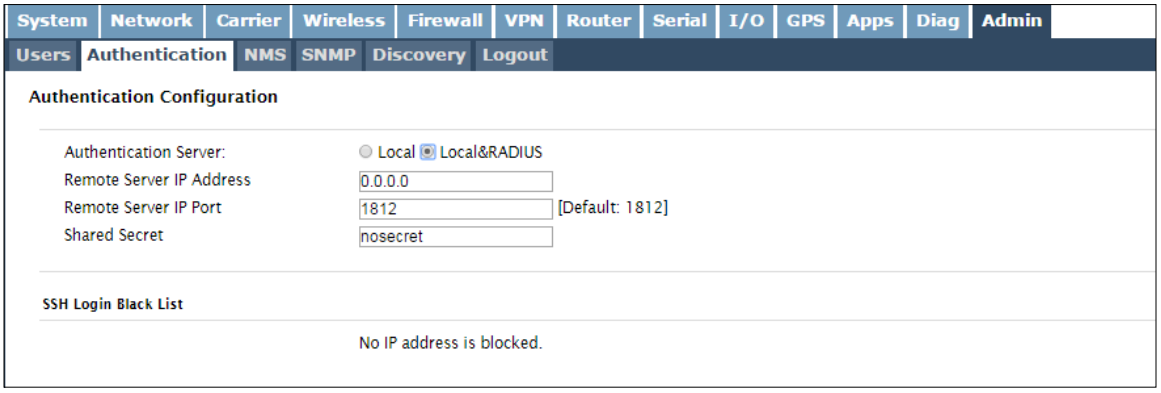


Image 4-13-3: Authentication Configuration

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.

Values

Local
Local&RADIUS

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.

Values

Valid RADIUS server IP address

0.0.0.0

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.

Values

nosecret

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.

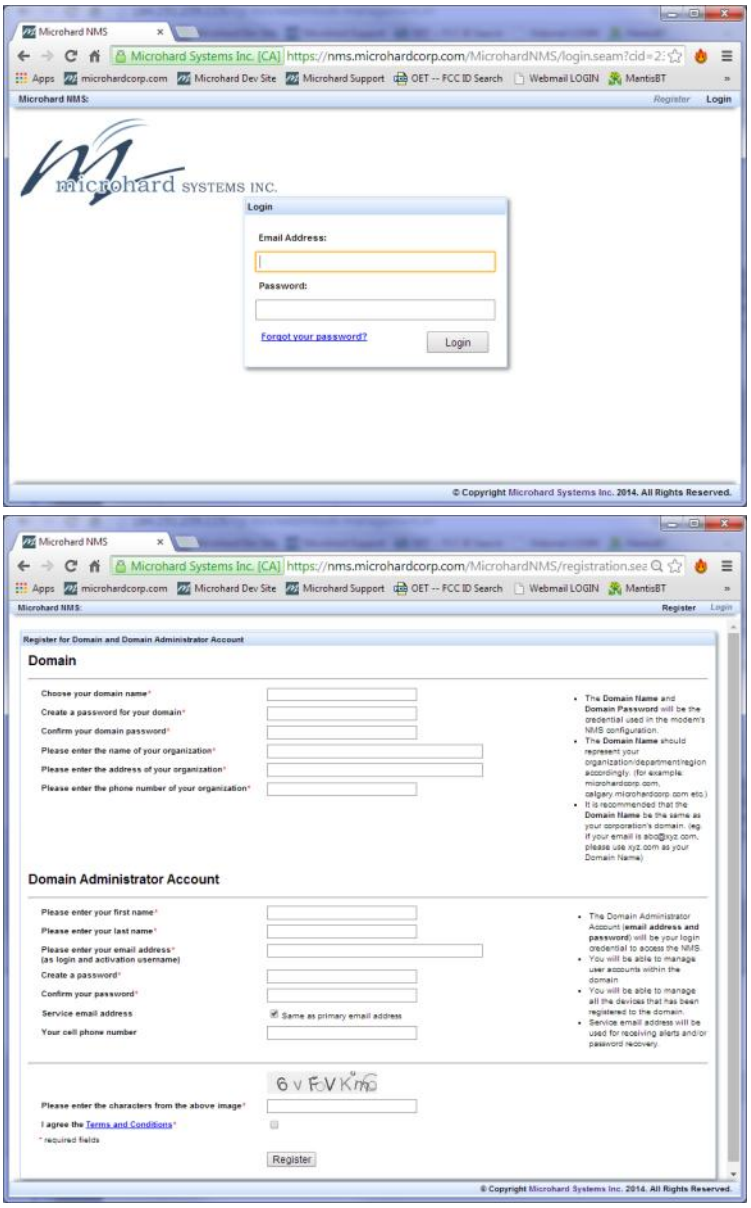


Image 4-13-4: NMS

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.

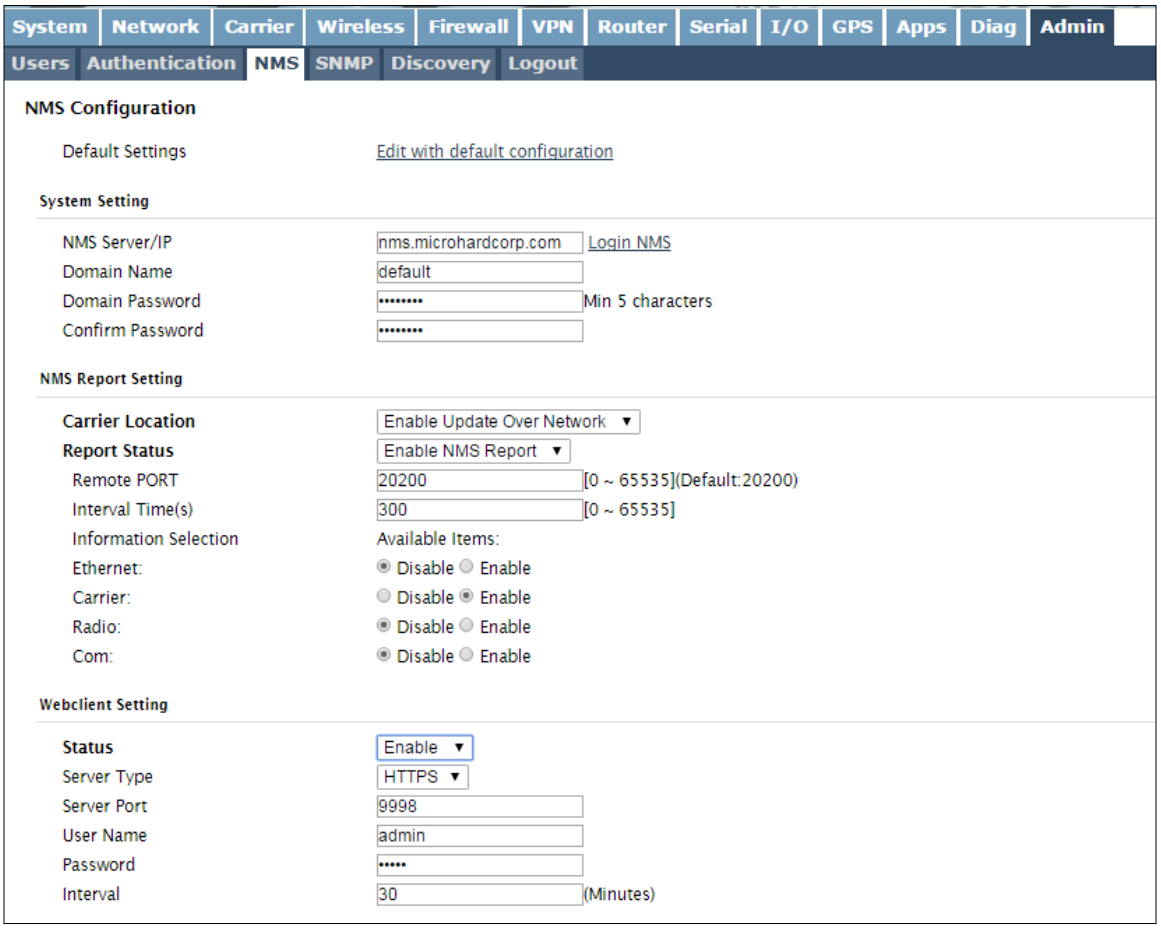


Image 4-13-5: NMS Settings

4.0 Configuration

Network Management System (NMS) Configuration

Default Settings

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.

NMS Server/IP

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.

Values (IP/Name)

nms.microhardcorp.com

Domain Name / Password

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.

Values (chars)

default

NMS Report Setting

Carrier Location

Enable or Disable location estimation via carrier connection. When enabled, the BulletPlus will consume some data to retrieve location information from the internet.

Values (chars)

Disable/Enable

Report Status

Enable or Disable UDP reporting of data to the NMS system.

Values (chars)

Enable NMS Report
Disable NMS Report

Remote Port

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.

Values (UDP Port#)

20200

Interval(s)

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)

Values (seconds)

300

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 that is sent to the NMS system, be aware of data plan constraints and related costs.

Values (check boxes)

Ethernet
Carrier
Radio
COM
DI / DO

Webclient Setting

Status

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.

Values (chars)

Disable/Enable

Server Type

Select between HTTPS (secure), or HTTP server type.

Values (chars)

HTTPS/ HTTP

Server Port

This is the port where the service is installed and listening. This port should be open on any installed firewalls.

Values (Port#)

9998

Username / Password

This is the username and password used to authenticate the unit.

Values (seconds)

admin/admin

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.

Values (min)

60

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

SNMP: Simple Network Management Protocol provides a method of managing network devices from a single PC running network management software.

Managed networked devices are referred to as SNMP agents.

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 and 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

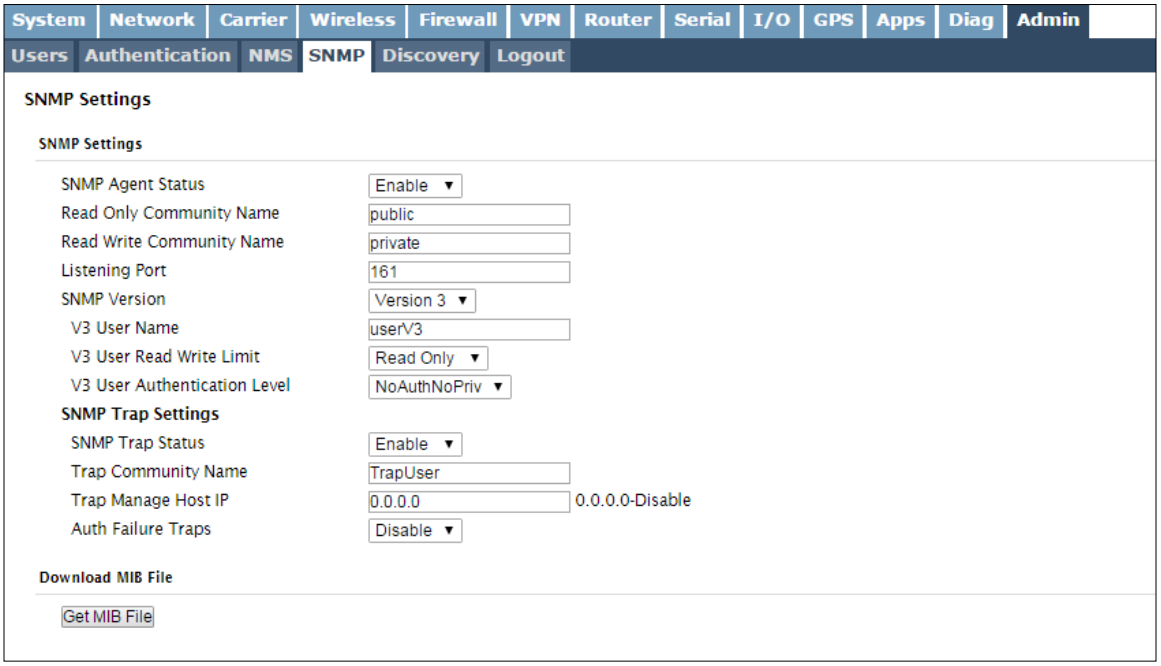


Image 4-13-6: Network > SNMP

SNMP Operation Mode

If disabled, an SNMP service is not provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2, & v3.

Values (selection)

Disable / V1&V2c&V3

Read Only Community Name

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.

Values (string)

public

Read Only Community Name

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.

Values (string)

private

SNMP V3 User Name

Defines the user name for SNMPv3.

Values (string)

V3user

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.

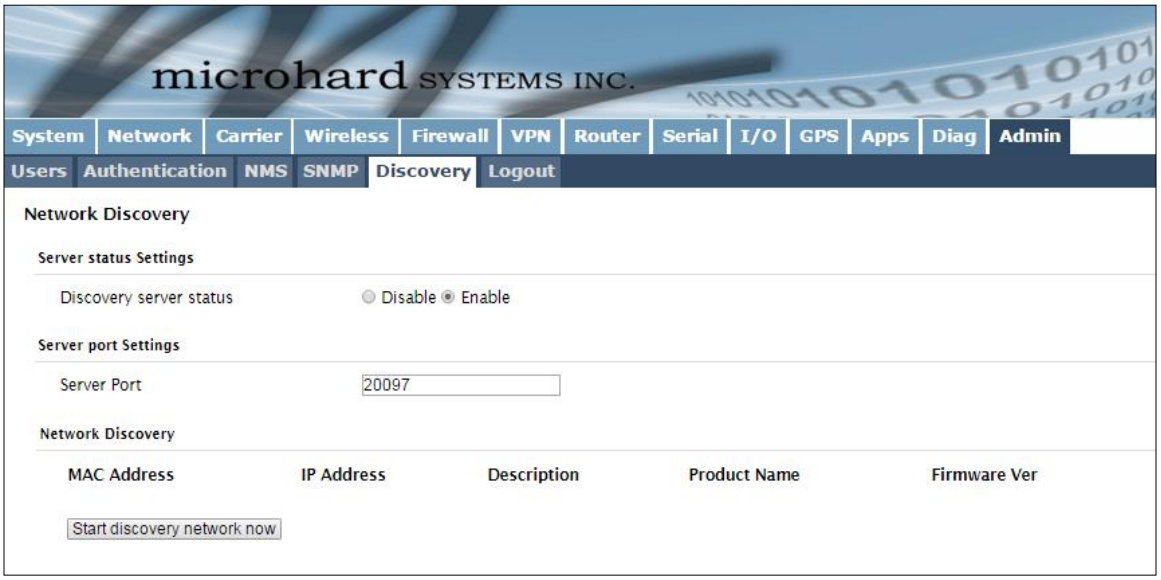


Image 4-13-7: Admin > Discovery Settings

Discovery Service Status

Use this option to disable or enable the discovery service.

Values (selection)

Disable / **Discoverable** / Changable

Server Port Settings

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.

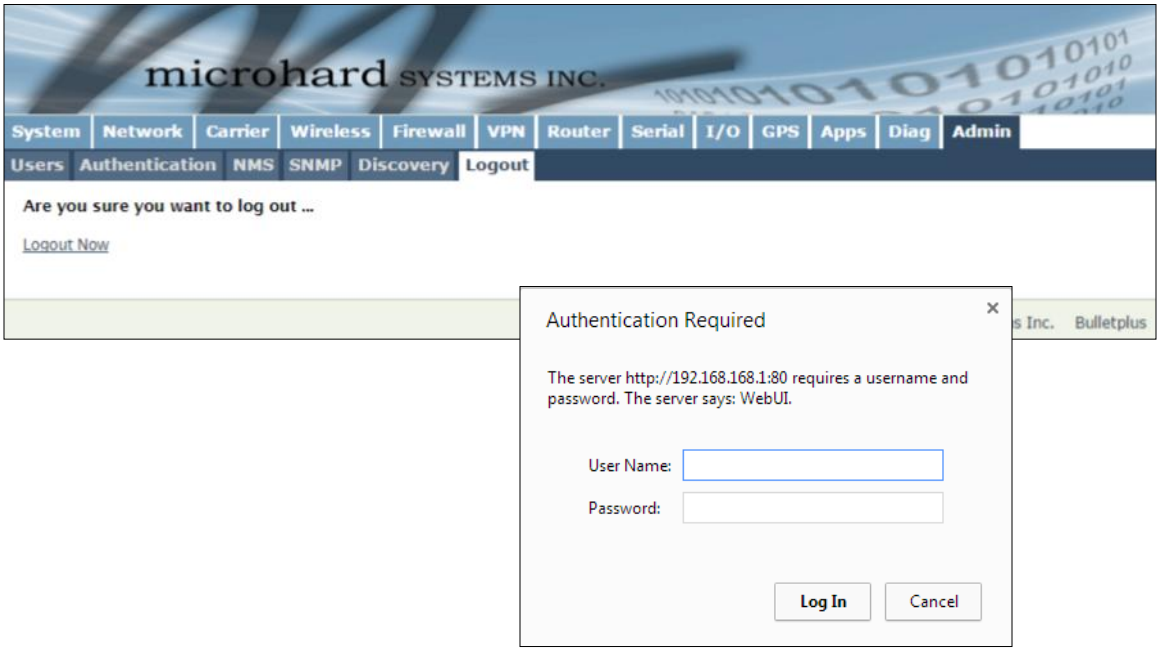


Image 4-13-9: System > logout

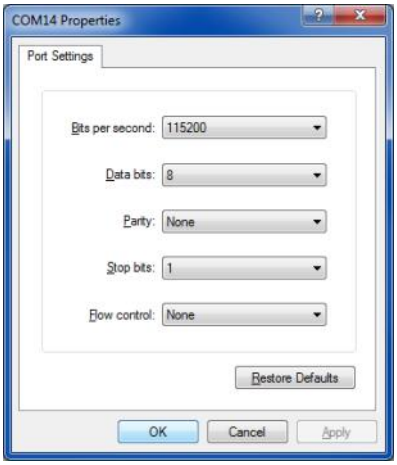
5.0 AT Command Line Interface

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



Default Settings:

Baud rate: **115200**

Data bits: **8**

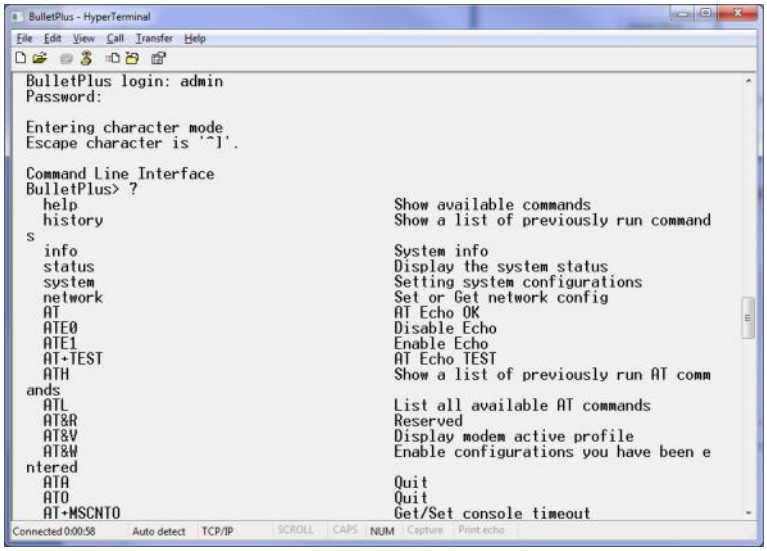
Parity: **None**

Stop Bits: **1**

Flow Control: **None**

Image 5-1: Console Port Settings

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.



Default Settings:

BulletPlus login: **admin**

Password: **admin**

Image 5-2: AT Command Window

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.

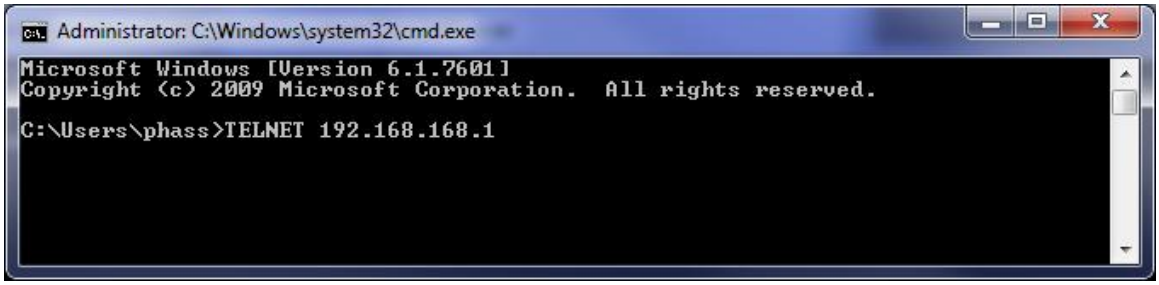


Image 5-3: Establishing a Telnet Session

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

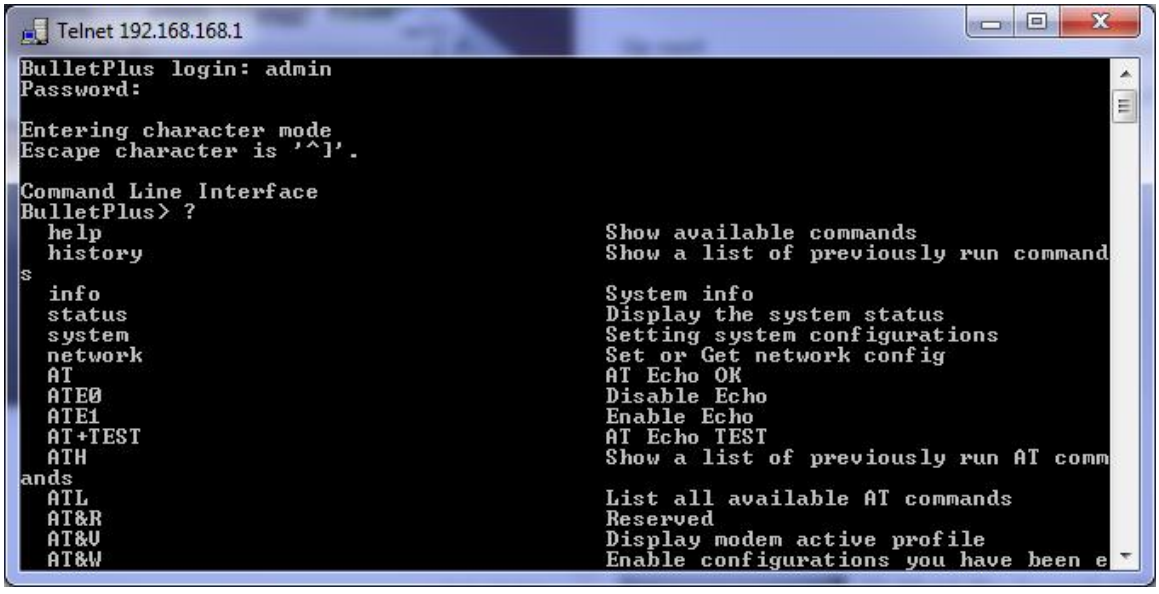


Image 5-4: Telnet AT Command Session

5.0 AT Command Line Interface

5.2 AT Command Syntax

The follow 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=<modem_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:

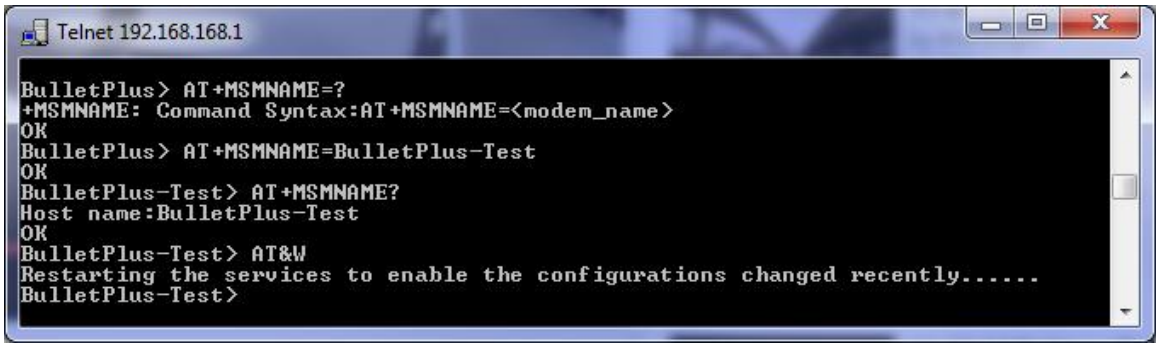


Image 5-5: Telnet AT Command Syntax

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

AT

Description	Command Syntax (Effect: Immediate)
Echo OK.	**AT <enter>**

Example

Input:
AT <enter>
Response:
OK

ATE0

Description	Command Syntax (Effect: Immediate)
Disables Local Echo.	**ATE0 <enter>**

Example

Input:
ATE0 <enter>
Response:
OK

ATE1

Description	Command Syntax (Effect: Immediate)
Enables Local Echo.	**ATE1 <enter>**

Example

Input:
ATE1 <enter>
Response:
OK

AT+TEST

Description	Command Syntax (Effect: Immediate)
Echo TEST	**AT+TEST <enter>**

Example

Input:
AT+TEST <enter>
Response:
AT ECHO TEST:
:0

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:

AT	AT Echo OK
ATE0	Disable Echo
ATE1	Enable Echo
AT+TEST	AT Echo TEST
ATH	Show a list of previously run AT commands
ATL	List all available AT commands
AT&R	Reserved
AT&V	Display modem active profile
AT&W	Enable configurations you have been entered
ATA	Quit
ATO	Quit

.
.
.
<Output Omitted>

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

Description	Command Syntax (Effect: Immediate)
Read modem active profile.	**AT&V <enter>**

Example

Input:
AT&V <enter>
Response:
&V:
hostname:BulletPlus-Test
timezone:MST7MDT,M3.2.0,M11.1.0
systemmode:gateway
time mode:local
OK

AT&W

Description	Command Syntax (Effect: Immediate)
Enable configurations changes that have been entered.	**AT&W <enter>**

Example

Input:
AT&W <enter>
Response:
Restarting the services to enable the configurations changed recently.....

ATA / ATO

Description	Command Syntax (Effect: Immediate)
Quit. Exits AT Command session and returns you to login prompt.	**ATA <enter>**

Example

Input:
ATA <enter>
Response:
OKConnection closed by foreign host

5.0 AT Command Line Interface

AT+MSCNTO

Description

Sets the timeout value for the serial and telnet consoles. Once expired, user will be return to login prompt.

Command Syntax (Effect: AT&W)

AT+MSCNTO=<Timeout_s>
0 - Disabled
0 - 65535 (seconds)

Example

Input:
AT+MSCNTO=300 <enter>
Response:
OK

AT+MSPWD

Description

Used to set or change the ADMIN password.

Command Syntax (Effect: Immediate)

AT+MSPWD=<New password>,<confirm password>
password: at least 5 characters

Example

Input:
AT+MSPWD=admin,admin<enter>
Response:
OK

AT+MSGMI

Description

Get Manufacturer Identification

Command Syntax

AT+MSGMI=<enter>

Example

Input:
AT+MSGMI<enter>

Response:
+MSGMI: 2014-2015 Microhard Systems Inc.
OK

5.0 AT Command Line Interface

AT+MSSYSI

Description

System Summary Information

Command Syntax

AT+MSSYSI <enter>

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

Copyright: 2014-2015 Microhard Systems Inc.
Time: Thu Nov 19 10:17:43 2015

AT+MSGMR

Description

Modem Record Information

Command Syntax

AT+MSGMR <enter>

Example

Input:
AT+MSGMR <enter>
Response:
+MSGMR:
 Hardware Version:Rev A Software Version:v1.3.0 build 1009-28
 Copyright: 2014-2015 Microhard Systems Inc.
 System Time: Thu Nov 19 10:19:42 2015
OK

5.0 AT Command Line Interface

AT+MSMNAME

Description

Modem Name / Radio Description. 30 chars.

Command Syntax (Effect: AT&W)

AT+MSMNAME=<modem_name>

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

Description

Reset the modem to the factory default settings from non-volatile memory.

Command Syntax (Effect: Immediate)

AT+MSRTF=<Action>
Action:
0 pre-set action
1 confirm action

Example

Input: (To set value)
AT+MSRTF=1<enter>
Response:
OK

AT+MSREB

Description

Reboot the modem.

Command Syntax (Effect: Immediate)

AT+MSREB <enter>

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+MSKA

Description

Get/Set ICMP Keep-alive mode.

Command Syntax (Effect: AT&W)

AT+MSKA=<Mode>
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>[,STP[,<IP Address>,<Netmask>]]]]]
LAN Name: Name of Network LAN interface
Operation:
SHOW - Show the details of an exsiting LAN interface
ADD - Add a new LAN interface, followed by the other parameters
EDIT - Edit an exsiting 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+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

Description

Retrieve the MAC Address of the local Ethernet interface.

Command Syntax

AT+MNEMAC <enter>

Example

Input:
AT+MNEMAC<enter>
Response:
+MNEMAC: "00:0F:92:00:40:9A"
OK

AT+MNPORT

Description

Get/set the Ethernet port configuration.

Command Syntax (Effect: AT&W)

AT+MNPORT[=<Ethernet Port>[,<Mode>[,<Auto Negotiation>,<Speed>,<Duplex>]]]

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:
OK

Input:
AT+MNPORT=1,0<enter>
Response:
OK

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>,<user name>,<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+MMIMEI

Description

Get modem's IMEI.

Command Syntax

AT+MMIMEI <enter>

Example

Input:
AT+MMIMEI<enter>
Response:
+MMIMEI: 356406060882064
OK

AT+MMIMSI

Description

Get modem's IMSI.

Command Syntax

AT+MMIMSI <enter>

Example

Input:
AT+MMIMSI<enter>
Response:
+MMIMSI: 302610012606734
OK

AT+MMNETRSSI

Description

Get modem's RSSI.

Command Syntax

AT+MMNETRSSI <enter>

Example

Input:
AT+MMNETRSSI<enter>
Response:
+MMNETRSSI:-59
OK

5.0 AT Command Line Interface

AT+MMPOWERIN

Description	Command Syntax
Get modem's input voltage.	**AT+MMPOWERIN <enter>**

Example

Input:
AT+MMPOWERIN<enter>
Response:
+MMPOWERIN: 12.27
OK

AT+MMBOARDTEMP

Description	Command Syntax
Get modem's temperature.	**AT+MMBOARDTEMP <enter>**

Example

Input:
AT+MMBOARDTEMP<enter>
Response:
+MMBOARDTEMP: 46.65
OK

AT+MMWANIP

Description	Command Syntax
Get modem's WAN IP Address (Carrier).	**AT+MMWANIP <enter>**

Example

Input:
AT+MMWANIP<enter>
Response:
+MMWANIP: 184.151.220.2
OK

5.0 AT Command Line Interface

AT+MMPIPP

Description

Get/Set IP-Passthrough.

Command Syntax (Effect: AT&W)

AT+MMPIPP=<Mode>
Mode:
0 Disable
1 Ethernet

Example

Input:
AT+MMPIPP=1<enter>
Response:
OK

Input:
AT+MMPIPP?
Response:
+MMPIPP: 1 Ethernet
OK

AT+MMNUM

Description

Get modem's phone number.

Command Syntax

AT+MMNUM <enter>

Example

Input:
AT+MMNUM <enter>
Response:
+MMNUM: 15874327939
OK

AT+MMIMI

Description

Get modem's IMEI and IMSI.

Command Syntax

AT+MMIMI <enter>

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+MMMGL

Description

List all SMS messages.

Command Syntax (Immediate)

AT+MMMGL<enter>

Example

Input:
AT+MMMGL<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

Description

Delete SMS messages from system.

Command Syntax (Immediate)

AT+MMMGD=<index>
<Index> : the index of the message to be deleted

Example

Input:
AT+MMMGD=12<enter>

Response:
OK

AT+MMSCMD

Description

GET/SET system SMS command service.

Command Syntax (Effect: AT&W)

AT+MMSCMD=<Mode>[,<Filter Mode>[,<Phone No.1>[,...,<Phone No.6>]]]
Mode:
0 Disable
1 Enable SMS Command
Filter Mode:
0 Disable
1 Enable Phone Filter

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)

AT+MIOMODE=<Index>,<Mode>
Index:
The index of IO port, 1 to 2
Mode:
0 Input
1 Output

Example

Input:
AT+MIOMODE=1,0 <enter>

Response:
OK

Input:
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)

AT+MIOOC=<Index>,<Output Control>
Index:
The index of IO port, 1 to 2
Output Control:
0 Open
1 Close

Example

Input:
AT+MIOOC=1,1 <enter>

Response:
OK

Input:
AT+MIOOC?

Response:
+MIOOC: IO Output Control
OutputCtrl1: 1 Close
OutputCtrl2: 0 Open
OK

5.0 AT Command Line Interface

AT+MIOSTATUS

Description

GET IO status.

Command Syntax

AT+MIOSTATUS <enter>

Example

Input:
AT+MIOSTATUS <enter>

Response:
+MIOSTATUS: IO status
iodigiinval1=High
iodigiinval2=High
OK

AT+MIOMETER

Description

GET IO meter (V).

Command Syntax

AT+MIOMETER <enter>

Example

Input:
AT+MIOMETER <enter>

Response:
+MIOMETER: IO meter(V)
iovolts1=2.77
iovolts2=2.81
OK

AT+MCPS2

Description

Configure the Serial port as either a console port (AT Commands) or a Data Port.

Command Syntax (Effect: AT&W)

AT+MCPS2=<Mode>
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.

Example

Input:
AT+MCBR2=13<enter>
Response:
OK

Input:
AT+MCBR2?
Response:
+MCBR2: 13 115200
OK

Command Syntax (Effect: AT&W)

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

AT+MCDF2

Description

Get/Set Serial port data format

Example

Input:
AT+MCDF2=0<enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MCDF2=<data format>
Data Format:
0 8N1
2 8E1
3 8O1

AT+MCDM2

Description

Set Serial port data mode.

Example

Input:
AT+MCDM2=1<enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MCDM2=<Data Mode>
Data Mode:
0 Seamless
1 Transparent

5.0 AT Command Line Interface

AT+MCCT2

Description

Set Comport character timeout.

Command Syntax (Effect: AT&W)

AT+MCCT2=<timeout_s>
(0 to 65535 seconds)

Example

Input:
AT+MCCT2=0<enter>
Response:
OK

AT+MCMPS2

Description

Get/Set Serial port maximum packet size.

Command Syntax (Effect: AT&W)

AT+MCMPS2=<size>
size: 0 to 65535

Example

Input:
AT+MCMPS2=1024<enter>
Response:
OK

AT+MCNCDI2

Description

Enable/Disable Serial port no-connection data intake.

Command Syntax (Effect: AT&W)

AT+MCNCDI2=<Mode>
Mode:
0 Disable
1 Enable

Example

Input:
AT+MCNCDI2=1<enter>
Response:
OK

5.0 AT Command Line Interface

AT+MCMTC2

Description

Get/Set Serial port modbus TCP configuration.

Command Syntax (Effect: AT&W)

AT+MCMTC2=<Status>, <Protection status>, <Protection Key>
Status and Protection Status:
0 Disable
1 Enable

Example

Input:
AT+MCMTC2=0,0,1234<enter>
Response:
OK

AT+MCIPM2

Description

Set the Serial port IP Protocol Mode.

Command Syntax (Effect: AT&W)

AT+MCIPM2=<Mode>
Mode:
0 TCP Client
1 TCP Server
2 TCP Client/Server
3 UDP Point to Point
7 SMTP Client
8 PPP
11 GPS Transparent Mode

Example

Input:
AT+MCIPM2=1<enter>
Response:
OK

AT+MCTC2

Description

Set Serial port TCP Client parameters when IP Protocol Mode is set to TCP Client.

Command Syntax (Effect: AT&W)

AT+MCTC2=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>
Remote Server IP : valid IP address
Remote Server Port : 1 to 65535
Outgoning timeout_s: 0 to 65535

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.

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

Example

Input:
AT+MCTS2=20002,300<enter>
Response:
OK

AT+MCTCS2

Description

Set TCP Client/Server parameters when IP Protocol is set to TCP Client/Server mode.

Command Syntax (Effect: AT&W)

AT+MCTCS2=<Remote Server IP>,<Remote Server Port>,<Outgoning timeout_s>,<Local Listener Port>
Remote Server IP : valid IP address
Remote Server Port : 1 to 65535
Outgoning timeout_s: 0 to 65535
Local Listener Port: 1 to 65535

Example

Input:
AT+MCCS2=0.0.0.0,20002,60,20002<enter>
Response:
OK

AT+MCUPP2

Description

Set UDP Point-to-Point parameters when IP Protocol is set to UDP Point-to-Point mode.

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

Example

Input:
AT+MCUPP2=0.0.0.0,20002,20002<enter>
Response:
OK

5.0 AT Command Line Interface

AT+MCSMTP2

Description

Get/Set Serial port SMTP client configuration when IP Protocol mode is set to SMTP client.

Command Syntax (Effect: AT&W)

AT+MCSMTP2=<Mail Subject>,<Mail Server>,<Username>,<Password>,<Mail Recipient>,<Message Max Size>,<TimeOut>,<Transfer Mode>
Mail Subject : 1 to 63 bytes
Mail Server : Valid IP Address or Name
Username : 1 to 63 bytes
Password : 1 to 63 bytes
Mail Recipient : 1 to 63 bytes
Message Max Size : [1 .. 65535]
TimeOut : [0 .. 65535] in seconds
Transfer Mode : 0: Text; 1: Attached File; 2: Hex Code

AT+MCPPP2

Description

Get/Set Serial port PPP configuration when IP protocol mode to set to PPP.

Command Syntax (Effect: AT&W)

AT+MCPPP2=<Mode>,<LCP Echo Failure Number>,<LCP Echo Interval>,<Local IP>,<Host IP>,<Idle Timeout>[,<Expected String>,<Response String>]

COM2:
Mode : 0 - Active; 1 - Passive
LCP Echo Failure Number : [0 .. 65535]
LCP Echo Interval : [0 .. 65535]
Local IP : Valid IP address
Host IP : Valid IP address
Idle Timeout : [0 .. 65535] in seconds
Expected String : (Optional) 0 - 63 characters
Response String : (Optional) 0 - 63 characters

Example

Input:
AT+MCPPP2?
Response:
+MCPPP2:
Mode : 1 - Passive
LCP Echo Failure Number : 0
LCP Echo Interval : 0
Local IP : 192.168.12.1
Host IP : 192.168.12.99
Idle Timeout(s) : 30
Expected String : CLIENT
Response String : CLIENTSERVER
OK

5.0 AT Command Line Interface

AT+MAEURD1
AT+MAEURD2
AT+MAEURD3

Description

Define Event Report UDP Report No.1/2/3.

Example

Input:
AT+MAEURD1=1,192.168.168.111,2010,10<enter>
Response:
OK

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 instant, "1,1,1" to enable all interfaces Ethernet, Carrier, USB, COM and IO for Management Report. For instant, "0,0,0,0,0" to disable all interfaces

AT+MANMSR

Description

Define NMS Report.

Example

Input:
AT+MANMSR=1,20200,300<enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MANMSR=<Mode>[,<Remote Port>,<Interval Time_s>]
Mode:
0 Disable
1 Enable NMS Report

AT+MADISS

Description

Configure discovery mode service used by pX2 and utilities such as “IP Discovery”.

Example

Input:
AT+MADISS=1 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MADISS=<Mode>
Mode:
0 Disable
1 Discoverable

5.0 AT Command Line Interface

AT+MAWSCLIENT

Description

Get/Set Web Service Client.

Command Syntax (Effect: AT&W)

AT+MAWSCLIENT[=<Mode>[,<ServerType>,<Port>,<UserName>,<Password>,<Interval>]]
Mode: 0 - Disable
1 - Enable
ServerType: 0 - https
1 - http
Port: 1 to 65535. Default is 9998
UserName: 1 to 63 characters
Password: 1 to 63 characters
Interval: In minute. 1 to 65535 minutes.

Example

Input:
AT+MAWSCLIENT=1,1,9998,username,password,10<enter>
Response:
OK

AT+MASNMP

Description

Get/Set SNMP service.

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)

AT+MASNMPV3=<UserName>,<RWLimit>,<AuthLevel>[,<Auth>,<AuthPassword> <Privacy> [,<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:
AT+MASNMPV3=<UserName>,<RWLimit>,0 If <AuthLevel>=0 (NoAuthNoPriv)
AT+MASNMPV3=<UserName>,<RWLimit>,1,<Auth>,<AuthPassword> If <AuthLevel>=1 (AuthNoPriv)
AT+MASNMPV3=<UserName>,<RWLimit>,2,<Auth>,<AuthPassword>,<Privacy>,<PrivacyPassword> If <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+MWRADIO

Description

Get/Set radio status, on or off.

Example

Input:
AT+MWRADIO=1 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWRADIO=<Radio>
Radio:
0 - Off
1 - On

AT+MWMODE

Description

Get/Set radio mode.

Example

Input:
AT+MWMODE=2 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWMODE=<Mode>
Mode:
0 - 802.11B ONLY
1 - 802.11BG
2 - 802.11NG - High Throughput on 2.4GHz

AT+MWTXPOWER

Description

Get/Set radio TX Power.

Example

Input:
AT+MWTXPOWER=10 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWTXPOWER=<Tx Power>
Tx Power:
0 - 20 dbm
1 - 21 dbm
2 - 22 dbm
3 - 23 dbm
4 - 24 dbm
5 - 25 dbm
6 - 26 dbm
7 - 27 dbm
8 - 28 dbm
9 - 29 dbm
10 - 30 dbm

5.0 AT Command Line Interface

AT+MWDISTANCE

Description

Get/Set radio Wireless Distance.

Example

Input:
AT+MWDISTANCE=1000 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWDISTANCE=<Distance>
Distance (m):
Minimum 1

AT+MWCHAN

Description

Set radio channel

Example

Input:
AT+MWCHAN=0 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWCHAN=<Channel>
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

AT+MWHTMODE

Description

Get/Set radio high throughput mode.

Example

Input:
AT+MWHTMODE=2 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWHTMODE=<High Throughput Mode>
High Throughput Mode:
0 - HT20
1 - HT40-
2 - HT40+
3 - Force HT40-
4 - Force HT40+

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

AT+MWAMSDU

Description

Get radio maximum AMSDU (byte).

Command Syntax

AT+MWAMSDU

Example

Input:
AT+MWAMSDU <enter>
Response:
+MWAMSDU: Maximum AMSDU (byte) - 3839

OK

AT+MWAMPDU

Description

Get radio maximum AMPDU (byte).

Command Syntax

AT+MWAMPDU

Example

Input:
AT+MWAMPDU <enter>
Response:
+MWAMPDU: Maximum AMPDU (byte) - 65535

OK

AT+MWRTSTHRESH

Description

Get/Set radio RTS Threshold.

Command Syntax (Effect: AT&W)

AT+MWRTSTHRESH=<RTS Threshold>
RTS Threshold:
0 Disabled
256-2346 Enabled with the value

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)

List one or all radio virtual interface(s) :
AT+MWIFACE=0[,<Index>]
Add one radio virtual interface :
AT+MWIFACE=1
Delete one radio virtual interface :
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

Example

Input:
AT+MWNETWORK=0 <enter>
Response:
+MWNETWORK: Virtual Interface 0: 0 - LAN
OK

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

AT+MWSSID

Description

Get/Set radio virtual interface: SSID

Example

Input:
AT+MWSSID=0,MySSID <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWSSID=[<Index>[,<SSID>]]
Index:
  Radio Virtual Interface Index: 0-3
SSID:
  Radio Virtual Interface SSID: 1 - 63 character

AT+MWDEVICEMODE

Description

Get/Set radio virtual interface: Mode

Example

Input:
AT+MWDEVICEMODE=0,0 <enter>
Response:
OK

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

5.0 AT Command Line Interface

AT+MWRATE

Description

Get/Set radio virtual interface: TX bit rate

Example

Input:
AT+MWTXRATE=0,0 <enter>
Response:
OK

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+MWSSIDBCAST

Description

Get/Set radio virtual interface: ESSID Broadcast.

Example

Input:
AT+MWSSIDBCAST=0,1 <enter>
Response:
OK

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

AT+MWAPISOLATION

Description

Get/Set radio virtual interface: AP Isolation

Example

Input:
AT+MWAPISOLATION=0,0 <enter>
Response:
OK

Command Syntax (Effect: AT&W)

AT+MWSSIDBCAST=[<Index>[,<AP Isolation>]]
Index:
  Radio Virtual Interface Index: 0-3
AP Isolation:
  Radio Virtual Interface AP Isolation:
    0 - Off
    1 - On

5.0 AT Command Line Interface

AT+MWENCRYPT

Description

Get/Set radio virtual interface: Encryption Type

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

Command Syntax (Effect: AT&W)

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
<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

AT+WSCAN

Description

Get radio network scan information. (Must be in client mode, scans for available networks).

Example

Input:
AT+WSCAN <enter>
Response:
Varies

Command Syntax

AT+WSCAN <enter>

5.0 AT Command Line Interface

AT+MWRSSI

Description

Get radio (WIFI) RSSI.

Command Syntax

AT+MWRSSI <enter>

Example

Input:
AT+MWRSSI <enter)
Response:
+MWRSSI: -76 dBm
OK

5.0 AT Command Line Interface

ATL

Description

Lists all available AT Commands.

Command Syntax

ATL <enter>

Example

ATL <enter>

AT Commands available:

AT	AT Echo OK
ATE0	Disable Echo
ATE1	Enable Echo
AT+TEST	AT Echo TEST
ATH	Show a list of previously run AT commands
ATL	List all available AT commands
AT&R	Reserved
AT&V	Display modem active profile
AT&W	Enable configurations you have been entered
ATA	Quit
ATO	Quit
AT+MSCNTO	Get/Set console timeout
AT+MSPWD	Set password
AT+MSGMI	Get manufacturer Identification
AT+MSSYSI	Get system summary information
AT+MSGMR	Get modem Record Information
AT+MSMNAME	Get/Set modem Name Setting
AT+MSRTF	Reset the modem to the factory default settings of from non-volatile (NV) memory
AT+MSREB	Reboot the modem
AT+MSNTP	Get/Set NTP server
AT+MSSYSLOG	Get/Set syslog server
AT+MSKA	Get/Set ICMP keep-alive mode
AT+MSKAS	Get/Set ICMP keep-alive settings
AT+MNLAN	Show/Add/Edit/Delete the network LAN interface
AT+MNLANDHCP	Get/Set LAN DHCP server running on the Ethernet interface
AT+MNIPMAC	Show/Add/Delete/Release/ReleaseAll the MAC-IP address binding
AT+MNEMAC	Get the MAC address of local Ethernet interface
AT+MNPORT	Get/set the Ethernet port configuration
AT+MNDDNSE	Get/Set DDNS mode
AT+MNDDNS	Set/Set DDNS settings
AT+MMIMEI	Get Modem's MMIMEI
AT+MMIMSI	Get Modem's MMIMSI
AT+MMNETRSSI	Get Modem's RSSI
AT+MMPOWERIN	Get Modem's Voltage
AT+MMBOARDTEMP	Get Modem's Temperature
AT+MMWANIP	Get Modem's WAN IP
AT+MMPIPP	Get/Set IP-Passthrough
AT+MMNUM	Get modem's Phone Number
AT+MMIMI	Get modem's MMIMEI and MMIMSI
AT+MMCID	Get modem's SIM Card Number
AT+MMMGS	Send SMS
AT+MMMGR	Read SMS
AT+MMMGL	List SMSs
AT+MMMGD	Delete SMSs
AT+MMSCMD	Get/Set system sms command service
AT+MIOMODE	Get/Set IO input or output mode
AT+MIOOC	Get/Set output control

(Continued….)

5.0 AT Command Line Interface

AT+MIOSTATUS	Get IO status
AT+MIOMETER	Get IO meter(V)
AT+MCPS2	Get/Set Serial port
AT+MCBR2	Get/Set Serial port baud rate
AT+MCDF2	Get/Set Serial port data format
AT+MCDM2	Get/Set Serial port data mode
AT+MCCT2	Get/Set Serial port character timeout
AT+MCMPS2	Get/Set Serial port maximum packet size
AT+MCNCDI2	Get/Set Serial port no-connection data intake
AT+MCMTC2	Get/Set Serial port modbus tcp configuration
AT+MCIPM2	Get/Set Serial port IP protocol mode
AT+MCTC2	Get/Set Serial port tcp client configuration when IP protocol mode is TCP Client
AT+MCTS2	Get/Set Serial port tcp server configuration when IP protocol mode is TCP Server
AT+MCTCS2	Get/Set Serial port tcp client/server configuration when IP protocol mode is TCP Client/Server
AT+MCUPP2	Get/Set Serial port UDP point to point configuration when IP protocol mode is UDP point to point
AT+MCSMTP2	Get/Set Serial port SMTP client configuration when IP protocol mode is SMTP client
AT+MCPPP2	Get/Set Serial port PPP configuration when IP protocol mode is PPP
AT+MAEURD1	Get/Set Event UDP Report No.1
AT+MAEURD2	Get/Set Event UDP Report No.2
AT+MAEURD3	Get/Set Event UDP Report No.3
AT+MANMSR	Get/Set NMS Report
AT+MADISS	Get/Set discovery service used by the modem
AT+MAWSCLIENT	Get/Set Web service client
AT+MASNMP	Get/Set SNMP service
AT+MASNMPV3	Get/Set SNMP Version 3
AT+MWRADIO	Get/Set radio status, On or Off
AT+MWMODE	Get/Set radio mode
AT+MWTXPOWER	Get/Set radio Tx power
AT+MWDISTANCE	Get/Set radio Wireless Distance
AT+MWCHAN	Get/Set radio channel
AT+MWHTMODE	Get/Set radio high throughput mode
AT+MWMPDUAGG	Get/Set radio MPDU Aggregation
AT+MWSHORTGI	Get/Set radio short GI
AT+MWHTCAPAB	Get radio HT Capabilities Info
AT+MWAMSDU	Get radio maximum AMSDU (byte)
AT+MWAMPDU	Get radio maximum AMPDU (byte)
AT+MWRTSTHRESH	Get/Set radio RTS Threshold
AT+MWFRAGTHRESH	Get/Set radio Fragment Threshold
AT+MWCCATHRESH	Get/Set radio CCA Power Threshold
AT+MWIFACE	List/Add/Delete radio virtual interface
AT+MWNETWORK	Get/Set radio virtual interface: Network
AT+MWSSID	Get/Set radio virtual interface: SSID
AT+MWDEVICEMODE	Get/Set radio virtual interface: Mode
AT+MWRATE	Get/Set radio virtual interface: TX bitrate
AT+MWSSIDBCAST	Get/Set radio virtual interface: ESSID Broadcast
AT+MWAPISOLATION	Get/Set radio virtual interface: AP Isolation
AT+MWENCRYPT	Get/Set radio virtual interface: Encryption Type
AT+MWSCAN	Get radio scanning information
AT+MWRSSI	Get radio RSSI

Appendix A: Serial Interface

Module (DCE)		Signal		Host (e.g. PC) (DTE)
1		DCD	→	IN
2		RX	→	IN
3	←	TX		OUT
4	←	DTR		OUT
5		SG		
6		DSR	→	IN
7	←	RTS		OUT
8		CTS	→	IN

Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present).

The interface conforms to standard RS-232 signals, so direct connection to a host PC (for example) is accommodated.

The signals in the asynchronous serial interface are described below:

DCD *Data Carrier Detect* - Output from Module - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another device.

RX *Receive Data* - Output from Module - Signals transferred from the BulletPlus are received by the DTE via RX.

TX *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the BulletPlus.

DTR *Data Terminal Ready* - Input to Module - Asserted (TTL low) by the DTE to inform the module that it is alive and ready for communications.

SG *Signal Ground* - Provides a ground reference for all signals transmitted by both DTE and DCE.

DSR *Data Set Ready* - 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.

RTS *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

CTS *Clear to Send* - Output from Module - A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.

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)

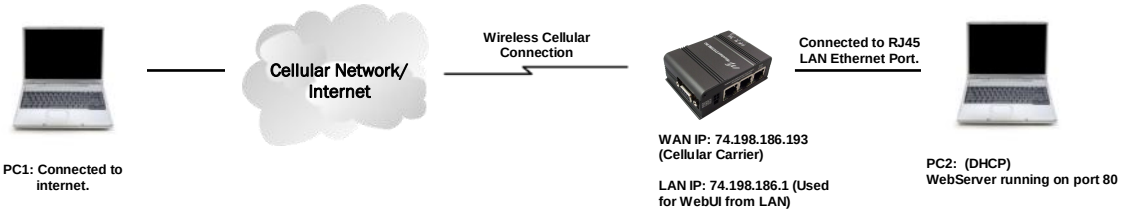
By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, a common application of the BulletPlus is to 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 RJ-45 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.

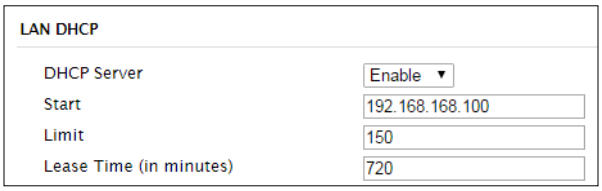
IP-Passthrough is ideal for applications where only a single device is connected to the BulletPlus, and other features of the BulletPlus are not required. When in pass-through mode, most features of the BulletPlus are bypassed, this includes the serial ports, the GPS features, VPN, and much more. The 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.



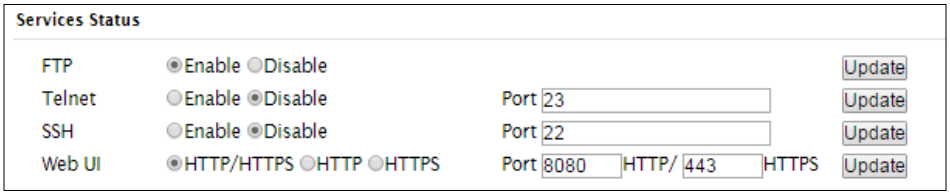
Step 1

Log into the BulletPlus (Refer to Quick Start), and ensure that DHCP is enabled on the **Network > LAN** (edit) page.



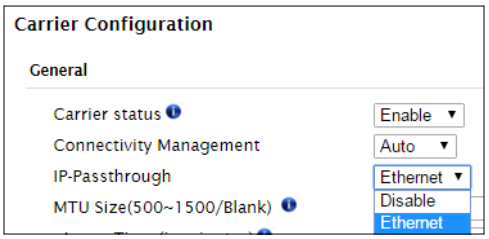
Step 2

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).



Appendix B: IP-Passthrough Example (Page 2 of 2)

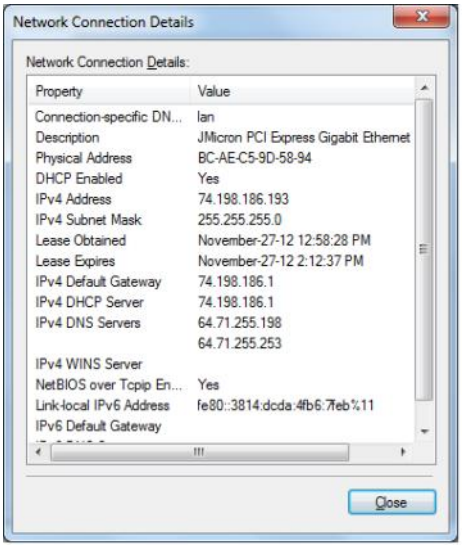
Step 3



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

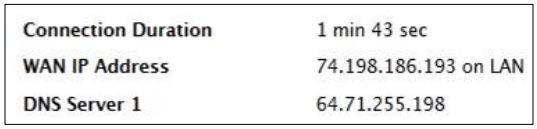
Attach the remote device or PC to the RJ45 port of the BulletPlus. The end device has to be set up for DHCP to get an IP address from the BulletPlus. In the test/example setup we can verify this by looking at the current IP address. In the screenshot to the right we can see that the Laptop connected 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:

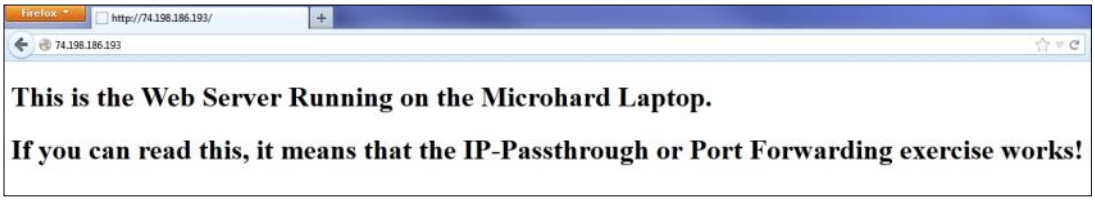
- Remotely on the WAN side (usually the internet), using the WAN IP, and the port specified for HTTP operation (or, if enabled, by using the HTTPS (443) ports), in this example with would be 74.198.186.193:8080.
- On the LAN side, by entering in the first 3 octets of the WAN IP and .1 for the fourth, 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.



Appendix C: Port Forwarding Example (Page 1 of 2)

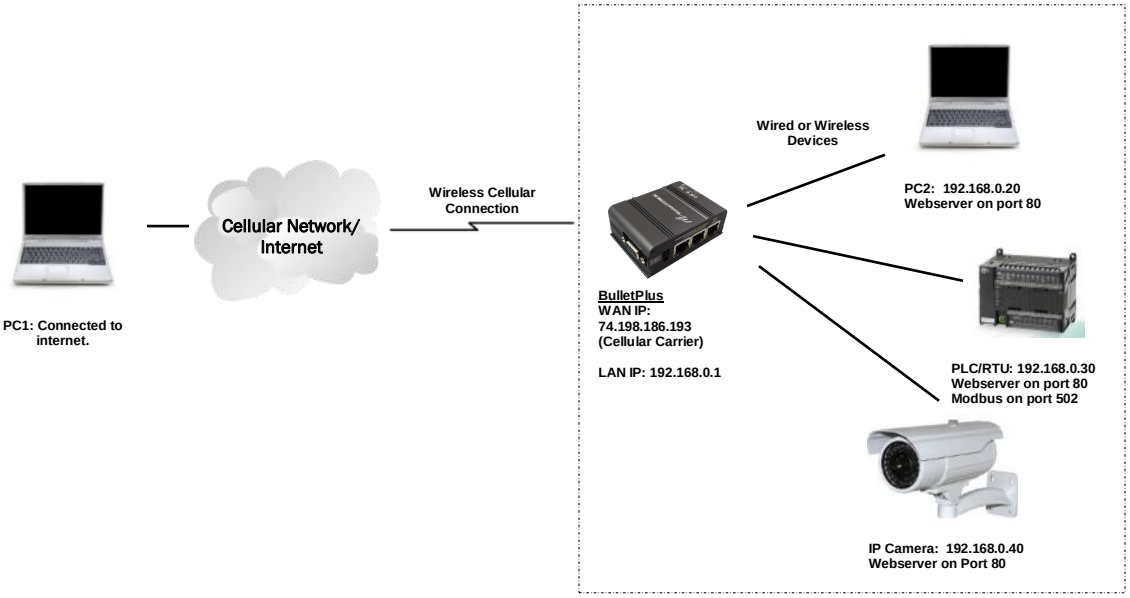
By completing the Quick Start process, a user should have been able to log in and set up the BulletPlus to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the BulletPlus 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.

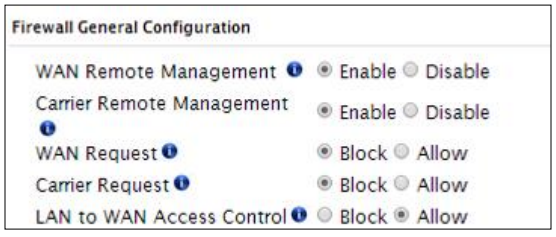
DMZ (a form of port forwarding) is useful for situations where there are multiple devices connected to the BulletPlus, but all incoming traffic is destined for a single device. It is also popular to use DMZ in cases where a single device is connected but several ports are forwarded and other features 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 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

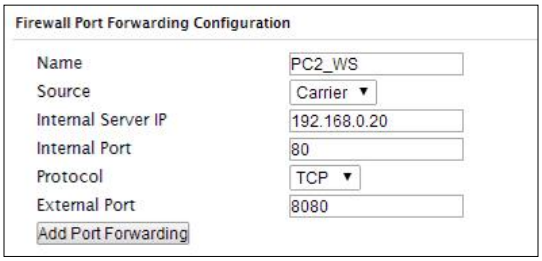
Determine which external ports (WAN) are mapped to which internal IP Addresses and Ports (LAN). It is important to understand which port, accessible on the outside, is connected or mapped to which devices on the inside. For this example we are going to use the following ports, in this case it is purely arbitrary which ports are assigned, some systems may be configurable, other systems may require specific ports to be used.

Description	WAN IP	External Port	Internal IP	Internal Port
BulletPlus WebUI	74.198.186.193	80	192.168.0.1	80
PC2 Web Server	74.198.186.193	8080	192.168.0.20	80
PLC Web Server	74.198.186.193	8081	192.168.0.30	80
PLC Modbus	74.198.186.193	10502	192.168.0.30	502
Camera Web Server	74.198.186.193	8082	192.168.0.40	80

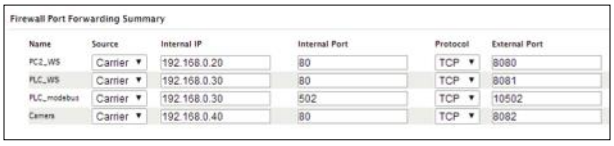
Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this 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.

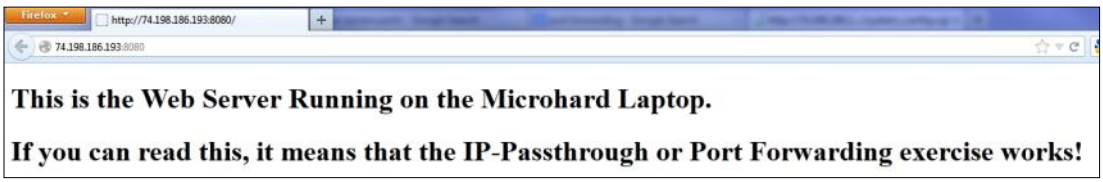
Step 4

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 webserver is



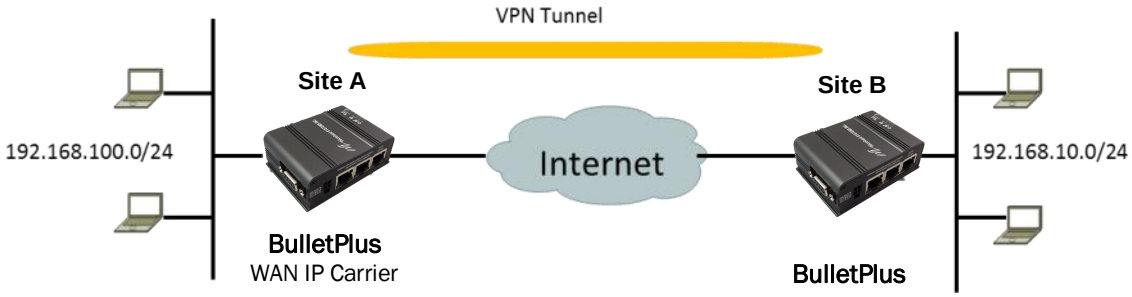
running as in the IP-Passthrough example, so the result should be as follows:
To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.

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)



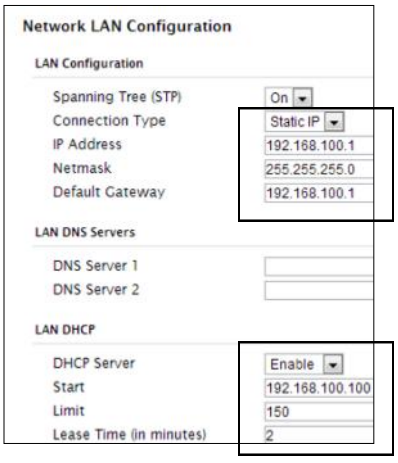
Step 1

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.

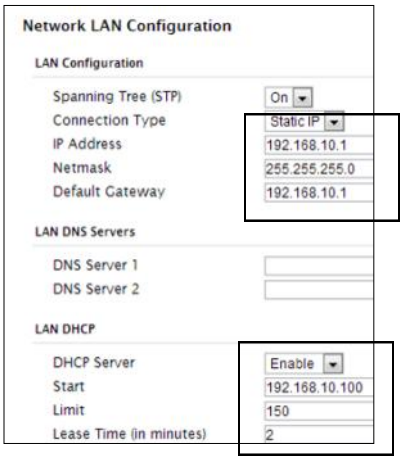
Step 2

Configure the LAN IP and subnet for each BulletPlus. The subnets must be different and cannot overlap.

Site A



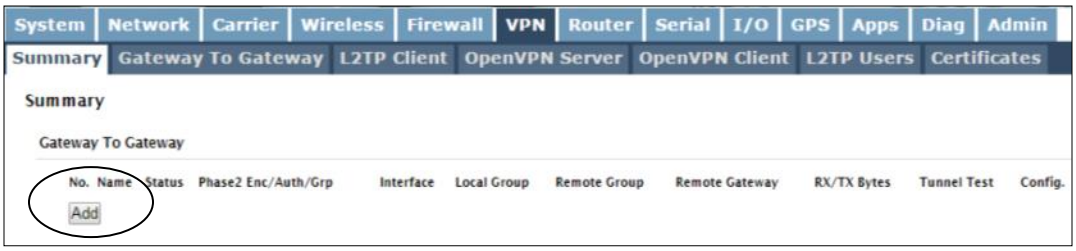
Site B



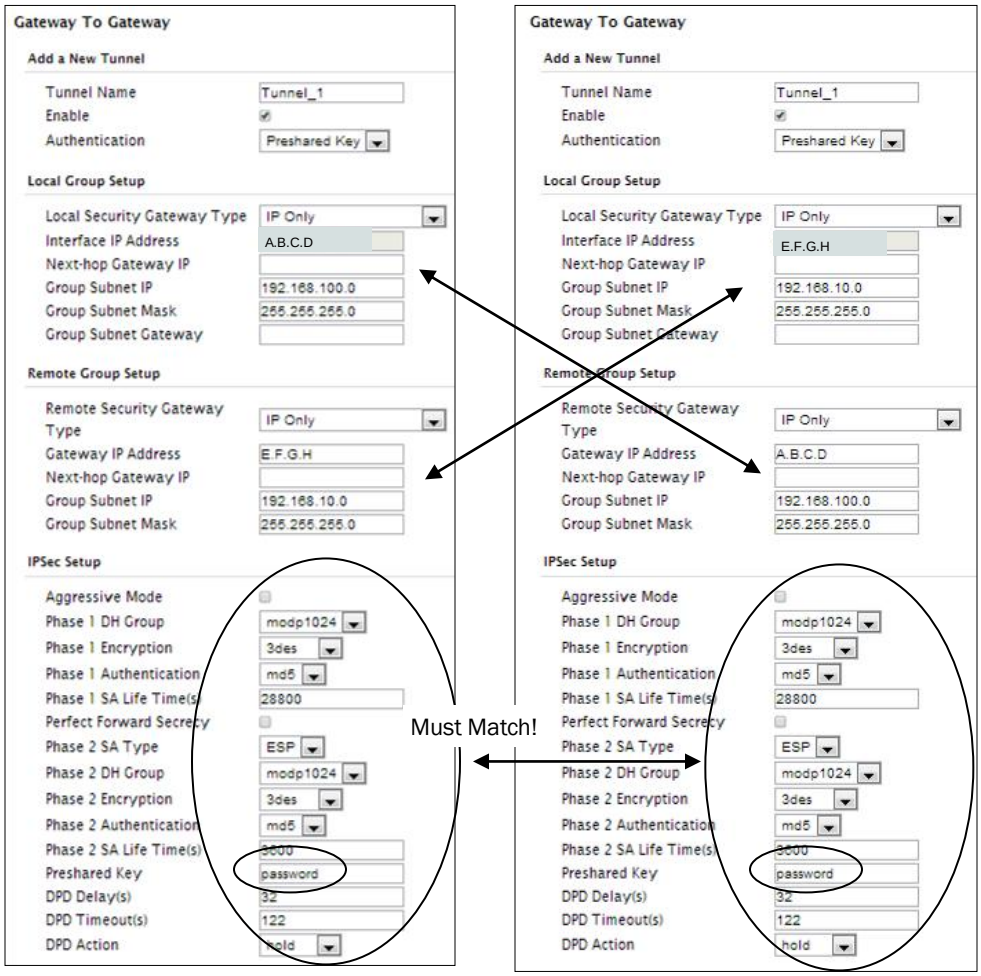
Appendix D: VPN Example (Page 2 of 2)

Step 3

Add a VPN Gateway to Gateway tunnel on each BulletPlus.



Site A



Site B

Step 4

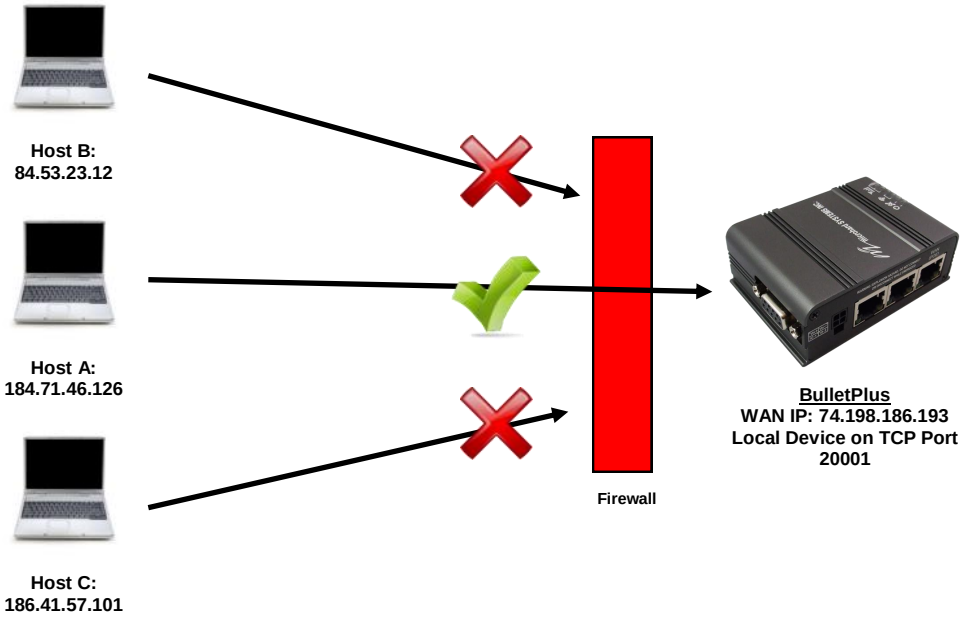
Submit changes to both units. It should be possible to ping and reach devices on either end of the VPN tunnel if both devices have been configured correctly and have network connectivity.

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

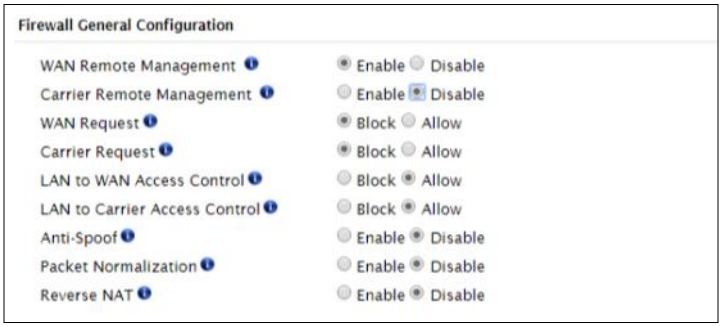
- Customizable Rules
- MAC and/or IP List
- ACL (Access Control List) or Blacklist using the above tools.

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 on the WAN. 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.

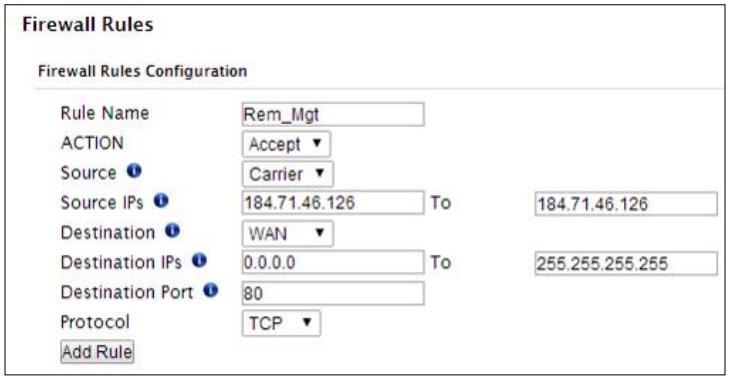


Appendix E: Firewall Example (Page 2 of 2)

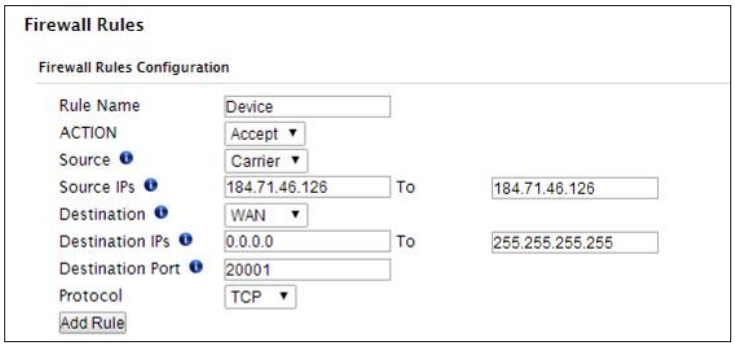
Step 2

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 the to serial port (WAN TCP Port 20001).

Rule 1



Rule 2



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.

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: 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 F: 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 access 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 appropriates 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.
3. 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.

microhard SYSTEMS INC.

150 Country Hills Landing NW
Calgary, Alberta
Canada T3K 5P3

Phone: (403) 248-0028
Fax: (403) 248-2762
www.microhardcorp.com