microhard SYSTEMS INC.

Operating Manual

IPn3G / IPn3Gb

3G/HSPA/HSPA+ Cellular Ethernet/Serial/USB Gateway

Revision 3.1 - March 2014
Firmware: v2.2.0-r2102

microhard SYSTEMS INC.

150 Country Hills Landing N.W.
Calgary, AB, 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.

ℹ **Information**
Information regarding a particular technology or concept.

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 :

IPn3G Version 2

FCCID: RI7T56KL1
IC: 5131A-KL1

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.

IPn3G Version 1

FCCID: IHDT56KL1
IC: 1090-KL1

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.

IPn3Gb

FCCID: XPYLISAU230
IC: 8595A-LISAU230

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.

Revision History

Revision	Description	Initials	Date
1.0	Initial Release	PEH	July 2010
1.1	Updated drawings (SMA), screen shots, pictures	PEH	Sept 2010
1.2	Updated drawings (Diversity, GPS)	PEH	Sept 2010
1.3	Updated graphics, drawings to reflect new enclosure design	PEH	Oct 2010
1.4	Update to Quick Start & WebUI menu changes	PEH	Jan 2011
1.5	Updates to screen shots as required	PEH	Feb 2011
1.6	Added GPS specs and antenna info	PEH	Feb 2011
1.7	NTP moved to system configuration, timezone added, phone number added to stats page, ICMP description updated (v1.1.6-r026)	PEH	Apr 2011
1.8	Updated VPN IPSec, GPS, Firewall, Misc Updates (v1.1.8-r1032h	PEH	June 2011
2.0	New menu format, Added AT Commands, UDP Reporting (v1.1.10-r1036)	PEH	Sept 2011
2.1	Added AT Command Syntax for each command, Added SMS At Commands	PEH	Feb 2012
2.2	Updated to reflect changes in v1.2.2-r1045. SMS, SMS Alerts, GRE, Added info on SNMP MIB, Backup/Restore, System conf etc	PEH	Feb 2012
2.3	Updated FCC & IC ID's, Misc Screen Shots, Formatting	PEH	Feb 2012
2.4	Updated SNMP MIB	PEH	Feb 2012
2.41	Removed references to Appendix D in Regulatory Info.	PEH	Mar 2012
2.5	Added Digital I/O, COM Logging, Event NMS Support, Management, Scheduled Reboots, SMS, PPP, Email Updates, Screen Shots etc. v1.2.4-r1058	PEH	June 2012
2.6	Added System > History (RSSI, EC/NO, Temp, VDC logs), System Reboot History, Network > Ethernet Port Status. V2.0.0-r2002b	PEH	June 2012
2.61	Fixed links in TOC	PEH	July 2012
2.7	Updated NMS Configuration and related info, Syslog, Static Routing, updated screen shots, etc. V2.0.18-r2040, added Appendix on IP-Passthrough, Port Forwarding, added GPS to Serial.	PEH	Nov 2012
2.8	Updated to reflect changes up to v2.0.28-r2070. Added History > Frequency ,Updated Network DHCP Lease time, MAC binding, Updated Carrier > Frequency, Added Security > Certificate Management, Updated VPN, Updated GRE, Added Modbus, Added Power Saving. Misc formatting, updated screen shots throughout.	PEH	Mar 2013
2.81	Added PoE, for units shipped after March 1, 2013	PEH	Jul 2013
2.9	Added Data Usage, Local Monitor, VPN Appendix, Firewall Appendix, Troubleshooting Appendix, updated screen shots, added Modbus options to serial port, added SMS Control Commands, AT Commands, misc corrections & formatting. Changes current up to firmware v2.0.44-r2090.	PEH	Oct 2013
3.0	Added FCC ID for IPn3Gb, Added additional spec data for IPn3Gb	PEH	Jan 2014
3.1	Additional updates for IPn3Gb, Updated to reflect firmware v2.2.0-r2102. Updated Carrier Config, Added Wireless Bus to COM1.	PEH	Mar 2014

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.

Table of Contents

Table of Contents (continued)

Appendices

1.0 Overview

The IPn3G is a high-performance 3G Cellular Ethernet/Serial/USB Gateway. Equipped with 2 serial data ports, 1 USB, and 1 Ethernet Port, the IPn3G provides complete access to remote devices. Using the vast established infrastructure of cellular networks, the IPn3G can provide data services anywhere coverage is provided.

While private wireless networks can provide wireless data services, using FHSS ISM bands, or secure dedicated licensed radio's, coverage is only available where radio's, repeaters, and other equipment is deployed. Achieving a wide coverage area generally involves many radio units, antennas, possibly private or shared towers and large amounts of planning.

The IPn3G/IPn3Gb operates on HSPA & Quad Band GSM cellular networks, using 3G/HSPA// HSPA+/EDGE/GPRS technology to provide fast and reliable data transfer.

The small size and superior performance of the IPn3G makes it ideal for many applications. Some typical uses for this modem:

- SCADA
- remote telemetry
- traffic control
- industrial controls
- remote monitoring
- LAN extension
- GPS
- wireless video
- robotics
- display signs
- fleet management

A SERIAL GATEWAY allows asynchronous serial data to enter (as through a gate) the realm of IP communications.

The serial data is encapsulated within UDP or TCP packets.

1.1 Performance Features

Key performance features of the IPn3G/IPn3Gb include:

- communicates with virtually all PLCs, RTUs, and serial devices through either one of two available RS232 interface, RS422, or RS485
- fastest serial rates: 300 baud to 921kbps
- advanced serial port supports legacy serial devices, including RTS, CTS, DSR, DTR, and DCD.
- Easy to manage through web- or text-based user interface, or SNMP
- wireless firmware upgrades
- system wide remote diagnostics
- advanced security features
- industrial temperature specifications
- DIN rail mountable
- Optional Class 1 Div 2
- Available as OEM solution

Supporting co-located independent networks and with the ability to carry both serial and IP traffic, the IPn3G supports not only network growth, but also provides the opportunity to migrate from asynchronous serial devices connected today to IP-based devices in the future.

1.0 Overview

1.2 IPn3G / IPn3Gb Specifications

Electrical/General

IPn3G Supported Bands:	HSPA & Quad Band GSM 850/1900/1700-2100 (HSPA) 850/900/1800/1900 MHz (GSM)
IPn3Gb Supported Bands:	UMTS/HSPA FDD Bands [MHz] - Six band Band I (2100MHz), Band II (1900MHz), Band IV (1700MHz), Band V (850MHz), Band VI (800MHz), Band VIII (900Hz) 3GPP Release 7 5.76 Mb/s uplink, 21.1 Mb/s downlink or 5.76 Mb/s uplink, 7.2 Mb/s downlink
IPn3G Data Features:	HSPA Up to 7.2 Mbps downlink Up to 5.76 Mbps uplink EDGE/GPRS Multi-Slot Class 12
IPn3Gb Data Features:	HSDPA cat 14, up to 21.1 Mb/s DL for LISA-U230 GPRS multi-slot class 125, coding scheme CS1-CS4, up to 85.6 kb/s DL/UL EDGE multi-slot class 125, coding scheme MCS1-MCS9, up to 236.8 kb/s DL/UL CSD GSM max 9.6 kb/s UMTS max 64 kb/s
IPn3G TX Power:	HSPA - Class 3 (0.25W) GSM 850/900 MHz - Class 4 (2W) GSM 1800/1900 MHz - Class 1 (1W) EDGE 850/900 MHz - Class E2 (0.5W) EDGE 1800/1900 MHz - Class E2 (0.4W)
IPn3Gb TX Power:	WCDMA/HSDPA/HSUPA Power Class · Power Class 3 (24 dBm) for WCDMA/HSDPA/HSUPA mode GSM/GPRS Power Class · Power Class 4 (33 dBm) for GSM/E-GSM bands · Power Class 1 (30 dBm) for DCS/PCS bands EDGE Power Class · Power Class E2 (27 dBm) for GSM/E-GSM bands · Power Class E2 (26 dBm) for DCS/PCS bands
IPn3Gb Current Consumption:	UMTS Active Connection Current: Avg Serial Data: 75mA Avg Ethernet: 94mA Peak Tx: 275mA
Serial Interface:	RS232, RS485, RS422
Serial Baud Rate:	300bps to 921kbps
USB:	USB 2.0 USB Console Port USB to Serial Data Routing USB to Ethernet Data Routing

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

1.0 Overview

1.2 IPn3G / IPn3Gb Specifications (Continued)

Ethernet:	10/100 BaseT, Auto - MDI/X, IEEE 802.3
SIM Card:	1.8 / 3.0V
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 (Units shipped after March 1, 2013)
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^{o}F(-40^{o}C) to 185^{o}F(85^{o}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):**	Main TX/RX:	SMA Female
		Diversity:	SMA Female
		GPS:	SMA Female
	Data, etc:	Data:	DE-9 Female
		Ethernet :	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

1.0 Overview

1.3 IPn3Gb RF Performance

Frequency Range		Min. (MHz)	Max. (MHz)	Remarks
GSM 850	Uplink	824	849	Module transmit
	Downlink	869	894	Module receive
E-GSM 900	Uplink	880	915	Module transmit
	Downlink	925	960	Module receive
DCS 1800	Uplink	1710	1785	Module transmit
	Downlink	1805	1880	Module receive
PCS1900	Uplink	1850	1910	Module transmit
	Downlink	1930	1990	Module receive
UMTS 800 (band VI)	Uplink	830	840	Module transmit
	Downlink	875	885	Module receive
UMTS 850 (band V)	Uplink	824	849	Module transmit
	Downlink	869	894	Module receive
UMTS 900 (band VIII)	Uplink	880	915	Module transmit
	Downlink	925	960	Module receive
UMTS 1700 (band VIII)	Uplink	1710	1755	Module transmit
	Downlink	2110	2155	Module receive
UMTS 1900 (band II)	Uplink	1850	1910	Module transmit
	Downlink	1930	1990	Module receive
UMTS 2100 (band 1)	Uplink	1920	1980	Module transmit
	Downlink	2110	2170	Module receive

Table 1-1: IPn3Gb Operating RF Frequency Bands

Receiver Input Sensitivity	Min. (dBm)	Typ. (dBm)	Max. (dBm)	Remarks
GSM 850 / E-GSM 900	-102.0	-110.0		Downlink RF level @ BER Class II < 2.4%
DCS 1800 / PCS 1900	-102.0	-109.0		Downlink RF level @ BER Class II < 2.4%
UMTS 800 (band VI)	-106.7	-111.0		Downlink RF level for RMC @ BER < 0.1%
UMTS 850 (band V)	-104.7	-112.0		Downlink RF level for RMC @ BER < 0.1%
UMTS 900 (band VIII)	-103.7	-111.0		Downlink RF level for RMC @ BER < 0.1%
UMTS 1700 (band VIII)	-106.7	-111.0		Downlink RF level for RMC @ BER < 0.1%
UMTS 1900 (band II)	-104.7	-111.0		Downlink RF level for RMC @ BER < 0.1%
UMTS 2100 (band 1)	-106.7	-111.0		Downlink RF level for RMC @ BER < 0.1%
Condition: 50 Ω source				

Table 1-2: IPn3Gb Receiver sensitivity performance

1.3 IPn3Gb RF Performance (continued…)

Maximum Output Power	Min.	Typ. (dBm)	Max.	Remarks
GSM 850 / E-GSM 900		32.5		Uplink burst RF power for GSM or GPRS 1-slot TCH at PCL 5 or Gamma 3
		32.5		Uplink burst RF power for GPRS 2-slot TCH at Gamma 3
		31.7		Uplink burst RF power for GPRS 3-slot TCH at Gamma 3
		30.5		Uplink burst RF power for GPRS 4-slot TCH at Gamma 3
		27.0		Uplink burst RF power for EDGE 8PSK 1-slot TCH at PCL 8 or Gamma 6
		27.0		Uplink burst RF power for EDGE 8PSK 2-slot TCH at Gamma 6
		26.2		Uplink burst RF power for EDGE 8PSK 3-slot TCH at Gamma 6
		25.0		Uplink burst RF power for EDGE 8PSK 4-slot TCH at Gamma 6
DCS 1800 / PCS 1900		29.5		Uplink burst RF power for GSM or GPRS 1-slot TCH at PCL 0 or Gamma 3
		29.5		Uplink burst RF power for GPRS 2-slot TCH at Gamma 3
		28.7		Uplink burst RF power for GPRS 3-slot TCH at Gamma 3
		27.5		Uplink burst RF power for GPRS 4-slot TCH at Gamma 3
		26.0		Uplink burst RF power for EDGE 8PSK 1-slot TCH at PCL 2 or Gamma 5
		26.0		Uplink burst RF power for EDGE 8PSK 2-slot TCH at Gamma 5
		25.2		Uplink burst RF power for EDGE 8PSK 3-slot TCH at Gamma 5
		24.0		Uplink burst RF power for EDGE 8PSK 4-slot TCH at Gamma 5
UMTS 800 (band VI)		23.0		Uplink continuous RF power for RMS at maximum power
UMTS 850 (band V)		23.0		Uplink continuous RF power for RMS at maximum power
UMTS 900 (band VIII)		23.0		Uplink continuous RF power for RMS at maximum power
UMTS 1700 (band VIII)		23.0		Uplink continuous RF power for RMS at maximum power
UMTS 1900 (band II)		23.0		Uplink continuous RF power for RMS at maximum power
UMTS 2100 (band 1)		23.0		Uplink continuous RF power for RMS at maximum power
Condition for all parameters: 50 Ω output load Condition for GPRS/EDGE multi-slot output power: Multi-Slot Power Reduction profile 2				

Table 1-3: IPn3Gb Transmitter maximum output power

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.

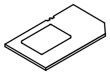
Note that the units arrive from the factory with the Local Network setting configured as ‘Static’ (IP Address 192.168.0.1, Subnet Mask 255.255.255.0, and Gateway 192.168.0.1), in DHCP server mode. (This is for the Ethernet Adapter on the back of the IPn3G unit.

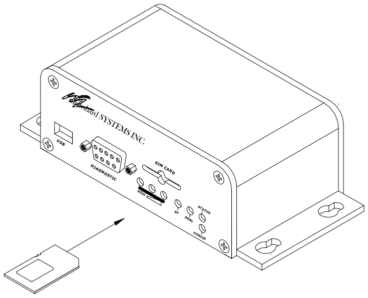
2.1 Installing the SIM Card

To reset to factory defaults, press and hold the CFG button for 8 seconds with the IPn3G powered up. The LED’s will flash quickly and the IPn3G will reboot with factory defaults.

✓ Before the IPn3G 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 below.

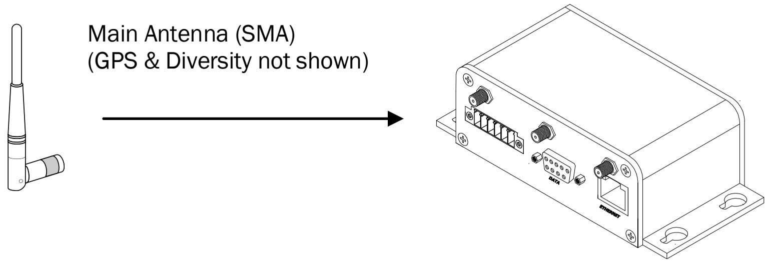
SIM Card Slot





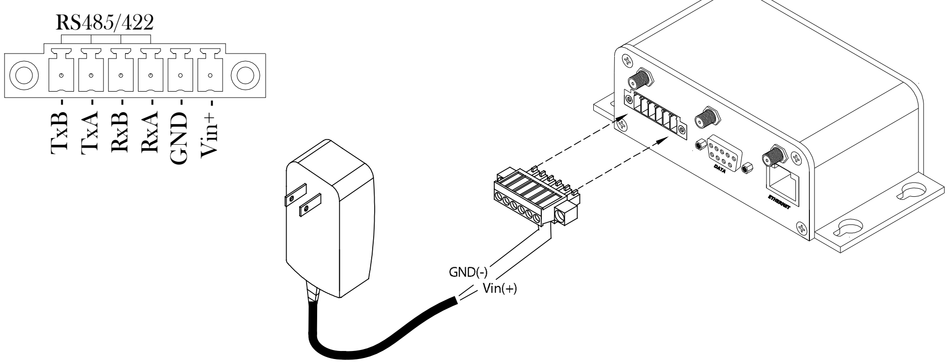
2.2 Getting Started

✓ Connect the Antenna’s to the applicable ***ANTENNA*** jack’s of the IPn3G.



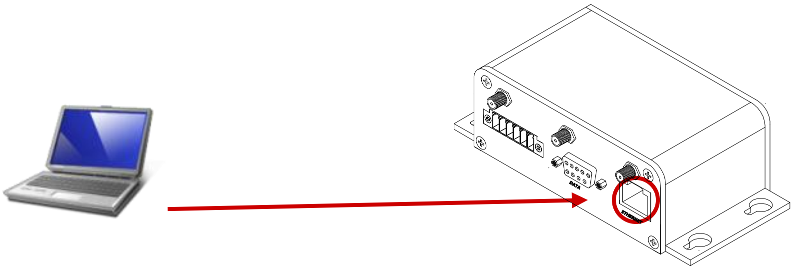
Use the MHS-supplied power adapter or an equivalent power source.

✓ Connect the Phoenix-Type Connector to the power adapter as shown below and apply power to the unit.



2.0 Quick Start

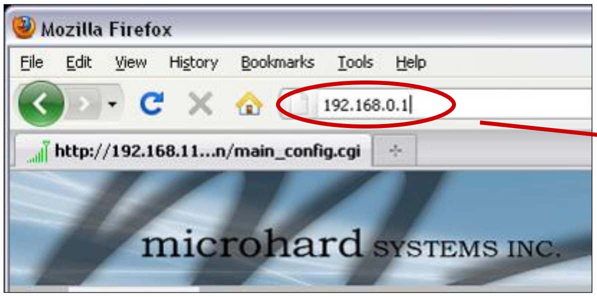
- ✓ Connect A PC configured for DHCP directly to the ***ETHERNET*** port of the IPn3G, using an Ethernet Cable. If the PC is configured for DHCP it will acquire a IP Address from the IPn3G.



- ✓ Open a Browser Window and enter the IP address 192.168.0.1 into the address bar.

The factory default network settings:

IP: 192.168.0.1
Subnet: 255.255.255.0
Gateway: 192.168.0.1


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.11...n/main_config.cgi
microhard SYSTEMS INC.

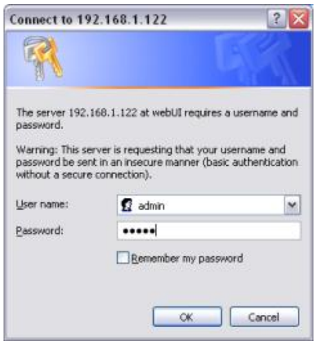
192.168.0.1

- ✓ The IPn3G will then ask for a Username and Password. Enter the factory defaults listed below.

The factory default login:

User name: admin
Subnet: admin

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



Connect to 192.168.1.122

The server 192.168.1.122 at webUI requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: •••••

□ Remember my password

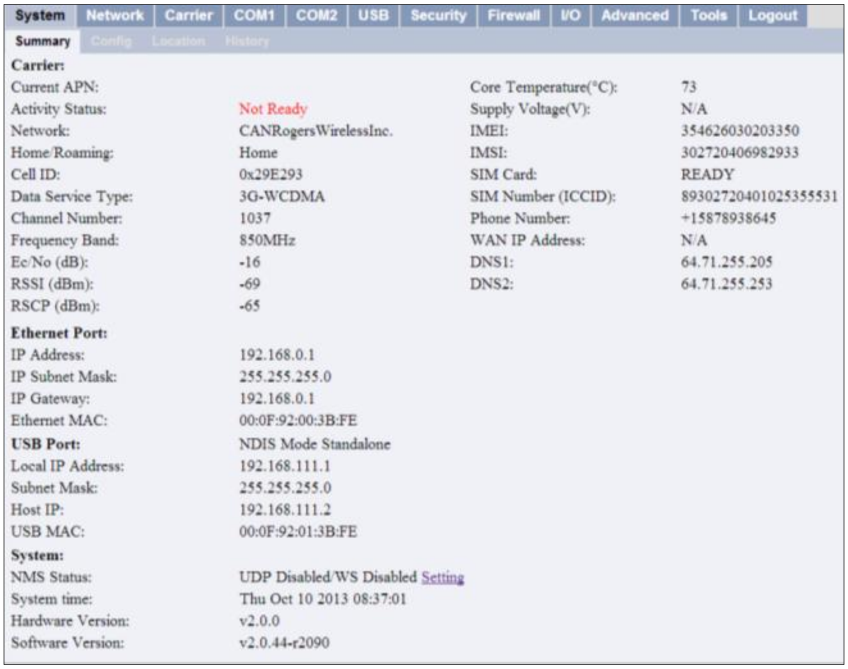
OK Cancel

The Factory default login:

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

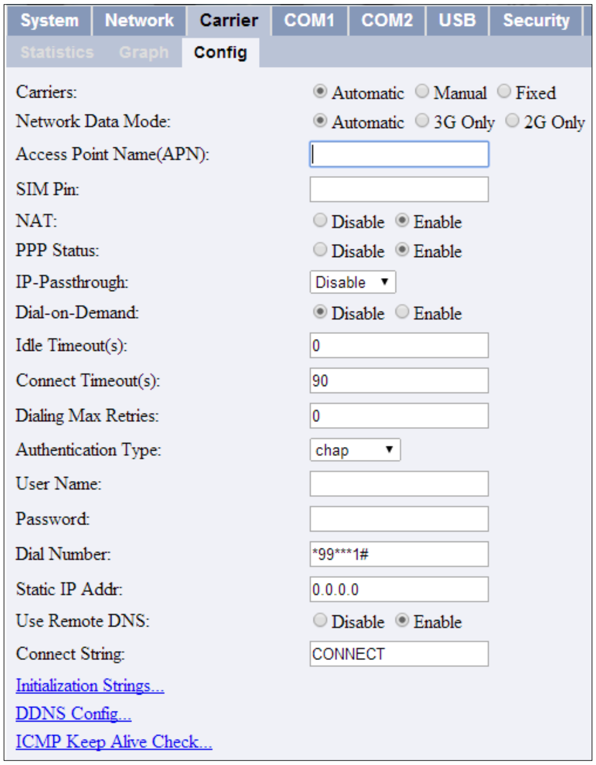
2.0 Quick Start

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



Carrier:			
Current APN:		Core Temperature(°C):	73
Activity Status:	Not Ready	Supply Voltage(V):	N/A
Network:	CANRogersWirelessInc.	IMEI:	354626030203350
Home/Roaming:	Home	IMSI:	302720406982933
Cell ID:	0x29E293	SIM Card:	READY
Data Service Type:	3G-WCDMA	SIM Number (ICCID):	89302720401025355531
Channel Number:	1037	Phone Number:	+15878938645
Frequency Band:	850MHz	WAN IP Address:	N/A
Ec/No (dB):	-16	DNS1:	64.71.255.205
RSSI (dBm):	-69	DNS2:	64.71.255.253
RSCP (dBm):	-65		
Ethernet Port:			
IP Address:	192.168.0.1		
IP Subnet Mask:	255.255.255.0		
IP Gateway:	192.168.0.1		
Ethernet MAC:	00:0F:92:00:3B:FE		
USB Port:	NDIS Mode Standalone		
Local IP Address:	192.168.111.1		
Subnet Mask:	255.255.255.0		
Host IP:	192.168.111.2		
USB MAC:	00:0F:92:01:3B:FE		
System:			
NMS Status:	UDP Disabled/WS Disabled Setting		
System time:	Thu Oct 10 2013 08:37:01		
Hardware Version:	v2.0.0		
Software Version:	v2.0.44-r2090		

✓ To establish basic wireless connectivity with your carrier, the information in the **Carrier > Config** menu must be completed as provided by your carrier.



Carriers:	● Automatic ○ Manual ○ Fixed
Network Data Mode:	● Automatic ○ 3G Only ○ 2G Only
Access Point Name(APN):	
SIM Pin:	
NAT:	○ Disable ● Enable
PPP Status:	○ Disable ● Enable
IP-Passthrough:	Disable ▾
Dial-on-Demand:	● Disable ○ Enable
Idle Timeout(s):	0
Connect Timeout(s):	90
Dialing Max Retries:	0
Authentication Type:	chap ▾
User Name:	
Password:	
Dial Number:	*99***1#
Static IP Addr:	0.0.0.0
Use Remote DNS:	○ Disable ● Enable
Connect String:	CONNECT

Initialization Strings...
DDNS Config...
ICMP Keep Alive Check...

Carriers may require different information to be filled out. Contact them for specific connection information.

For SIM Cards issued with Dynamic IP addresses most carriers simply require the correct APN. SIM Cards assigned Static public IP address often require additional login details.

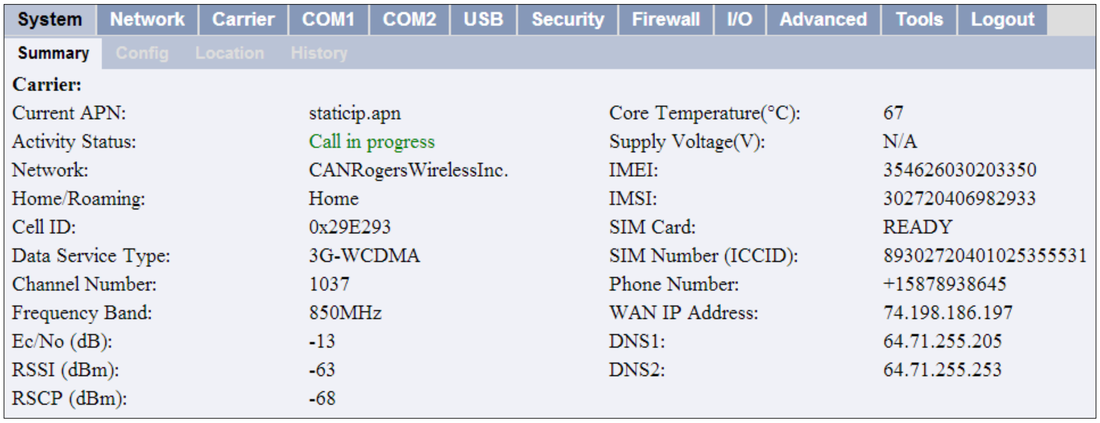
Wireless Carriers require the following information:

Always Required:
Access Point Name (APN)

Some Carriers Require:
Authentication Type
User Name
Password

2.0 Quick Start

✓ Verify connectivity with your Wireless Carrier by selecting **Carrier > Statistics** or **System > Summary**. Your carriers name should appear next to the Network entry and the Activity Status should read as: ***Call in progress***



Carrier:

Current APN:	staticip.apn	Core Temperature(°C):	67
Activity Status:	Call in progress	Supply Voltage(V):	N/A
Network:	CANRogersWirelessInc.	IMEI:	354626030203350
Home/Roaming:	Home	IMSI:	302720406982933
Cell ID:	0x29E293	SIM Card:	READY
Data Service Type:	3G-WCDMA	SIM Number (ICCID):	89302720401025355531
Channel Number:	1037	Phone Number:	+15878938645
Frequency Band:	850MHz	WAN IP Address:	74.198.186.197
Ec/No (dB):	-13	DNS1:	64.71.255.205
RSSI (dBm):	-63	DNS2:	64.71.255.253
RSCP (dBm):	-68		

✓ If you do not see "Call in Progress" you are not connected to or communicating with your wireless carrier.

- Check that the SIM card is installed correctly.
- Verify that the proper antennas are installed correctly
- Verify the APN assigned by the carrier.
- Re-Enter the login details, if required by the carrier, to ensure any typing errors.

✓ You see "Call in Progress", but no Internet Access. Check the WAN IP Address in the **Carrier > Statistics** or **System > Summary** screens. If an IP Address is not shown, check the APN and login details for errors.

Ensure the default passwords are changed.

✓ Refer to Section 4.0 WebUI Configuration to configure serial ports, USB, or any security or firewall features required on the IPn3G.

✓ 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.)

✓ To access devices attached to the IPn3G remotely, see Appendix C: IP-Passthrough, and/or Appendix D: Port Forwarding for working examples of how to configure your devices and the IPn3G to provide remote connectivity.

3.0 Hardware Description

3.1 IPn3G Hardware

The IPn3G provides a fully enclosed, stand alone modem, requiring only cabled connections. The IPn3G can be used on a table top like surface, or using the mounting holes provided can be mounted anywhere for a permanent solution.

- Power
- Data (Serial) Interface
- Ethernet Interface
- USB Interface
- LED Indicators
- Antenna’s (Main, GPS, Diversity)

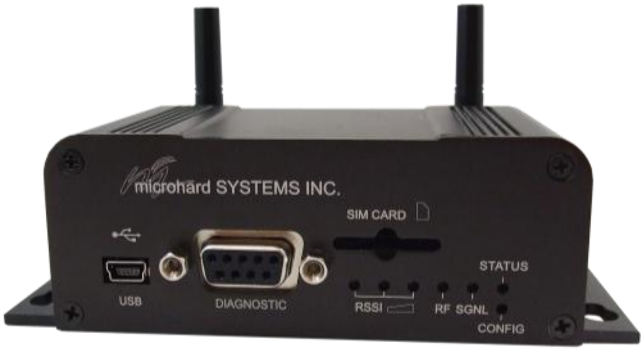


Image 3-1: IPn3G Front View

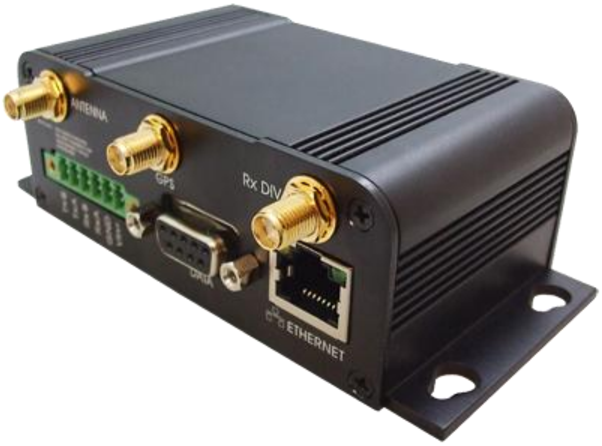
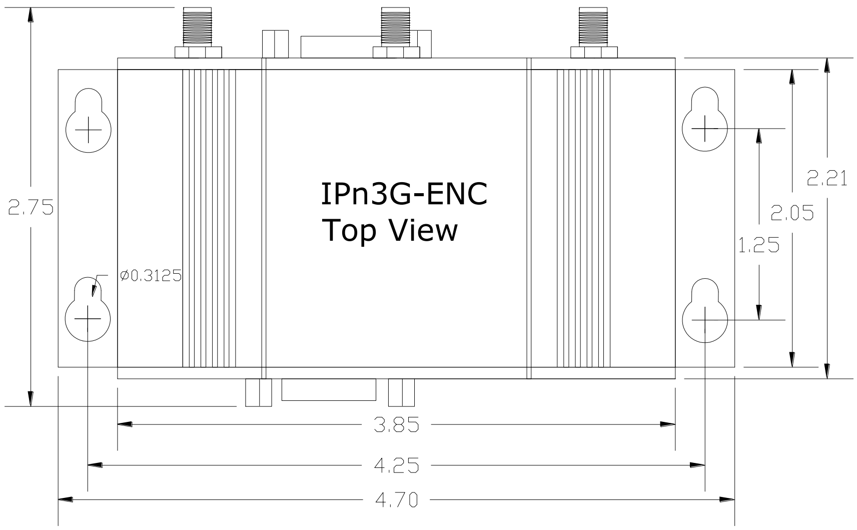


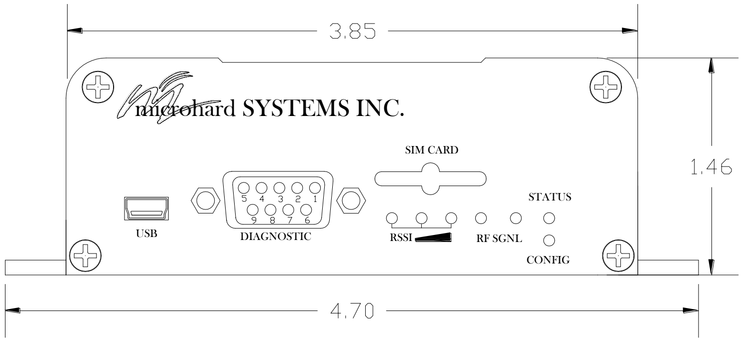
Image 3-2: IPn3G Back View

3.0 Hardware Description

3.1.1 IPn3G Mechanical Drawings



Drawing 3-1: IPn3G Top View



Drawing 3-2: IPn3G Front View

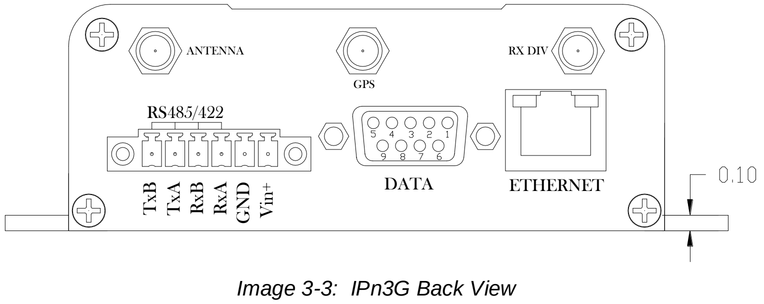


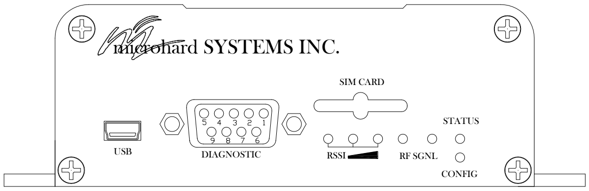
Image 3-3: IPn3G Back View

Notes: The dimension unit is inches.

3.1.2 Connectors and Indicators

3.1.2.1 Front

On the front of the IPn3G is the USB port, DIAGNOSTIC port, CONFIG Button, RSSI, STATUS, RF and SGNL LED's as described below:



Drawing 3-4: IPn3G Front View

Windows USB driver downloads are available to registered users from: **microhardcorp.com/support**

The **USB** port can be used for: (See **Section 4.1.7** USB Configuration)

- Console Port
- Data Mode
- NDIS Mode

The **Diagnostic** port (RS232) is used for:

- AT Command Interface at 115.2kbps and HyperTerminal (or equivalent).
- User data (RS232 - RxD, TxD, and SG)
- Digital I/O—Input Pin 7, Output Pin 8

Signal Name	PIN #	Input or Output
RXD	2	O
TXD	3	I
SG	5	
Digital In	7	I
Digital Out	8	O

Table 3-1: Diagnostic Port RS232 Pin Assignment

Digital I/O is only available and has been implemented on units shipped after June 1, 2012

CONFIG (Button) - Holding this button depressed while powering-up the IPn3G 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.

If the unit has been powered-up for some time (>1 minute), depressing the CFG Button for 8 seconds will result in FACTORY DEFAULTS being restored, including a static IP address of 192.168.0.1. This IP address is useable in a Web Browser for accessing the Web User Interface.

RF LED (Red) - When connected to a 2G/EDGE or 3G-WCDMA Network, the RF LED indicates a transmission burst. When connected to a 3G/HSPA Network the LED has no function.

SGNL LED (Green) - When illuminated, the SGNL LED indicates that the modem is connected and synchronized with a wireless carrier.

Receive Signal Strength Indicator (RSSI) (3x Green) - As the received signal strength increases, starting with the furthest left, the number of active RSSI LEDs increases. If the measured signal strength is less than –110dBm no LED's will be illuminated. If the signal is greater than –105dBm, 1 LED will be on, -100dBm equals 2 LED's, and any signal greater than –95dBm will show all 3 RSSI LED's to be ON.

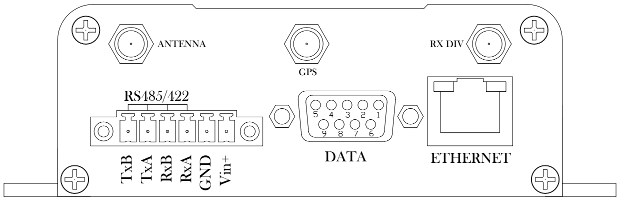
STATUS LED (Red) - Upon initial application of power the STATUS LED will be illuminated for approximately 20 seconds, after which time it will being to blink slowly (loading) for an additional 25 seconds, then stay ON ‗solid‘ (indicating it has achieved its specific operational status).

3.0 Hardware Description

3.1.2 Connectors and Indicators

3.1.2.2 Rear

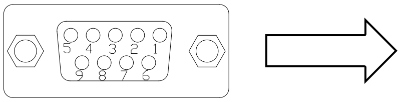
On the back of the IPn3G is the Data port, RS485/422 interface, as well as the power connections. The unit also has the SMA(F) connectors for the Main (TX/RX), GPS and the Diversity (RX) antenna's.



Drawing 3-5: IPn3G Rear View

The **DATA (RS232 Port (DCE))** on the rear of the circuit board is used for:

- RS232 serial data (300-921kbps).

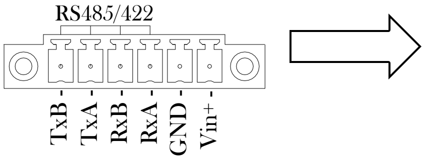


Name	Data Port	Input or Output
DCD	1	O
RXD	2	O
TXD	3	I
DTR	4	I
SG	5	
DSR	6	O
RTS	7	I
CTS	8	O
RING	9	O

Table 3-2: Data RS232 Pin Assignment

The **RS422/485 Port** is used to interface the Nano Development Board to a DTE with the same interface type. Either the RS232 **or** RS422/485 interface is used for data traffic.

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



Green Conn. Pin No.	Name	Input or Output
6	TxB (D+)	O
5	TxA (D-)	O
4	RxB (R+)	I
3	RxA (R-)	I
2	Vin -	
1	Vin +	I

Table 3-3: Data RS422/485 / Vin Pin Assignment

PoE*– The IPn3G can also be powered using Passive PoE on the Ethernet Port, via a PoE injector.

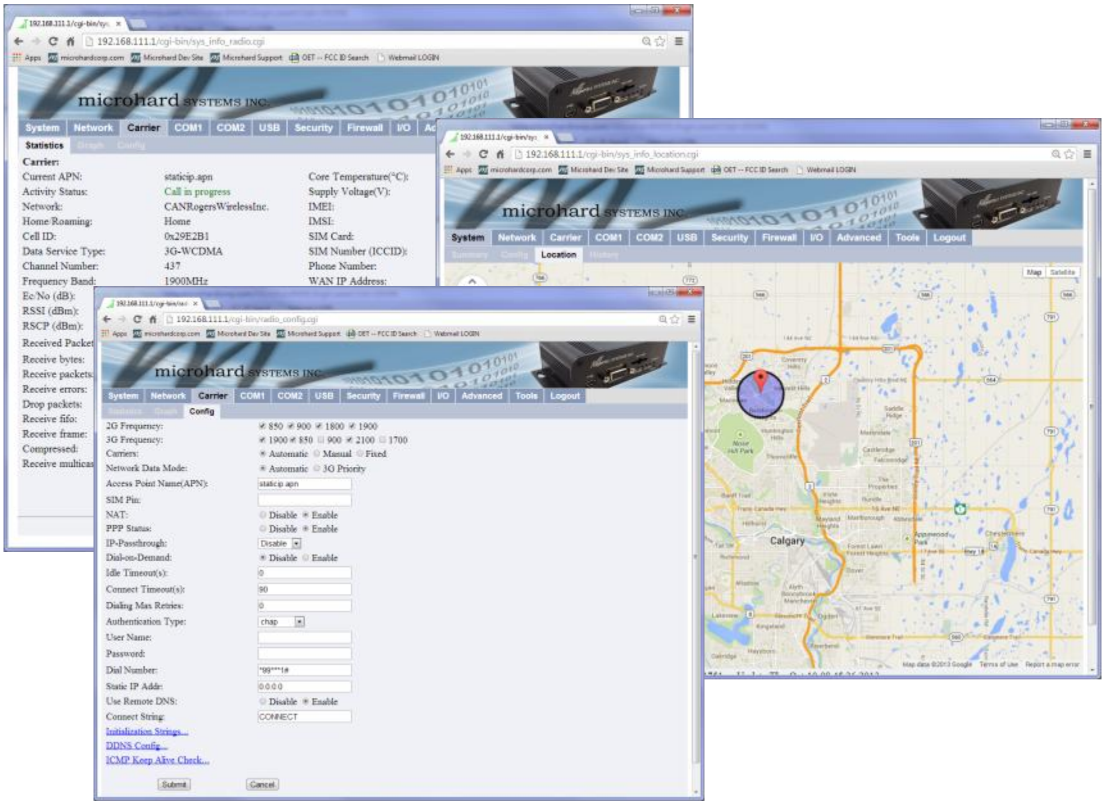
Caution: Using a power supply that does not provide proper voltage may damage the modem.

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 3-4: Ethernet PoE Connections

PoE only available on models shipped after March 1, 2013

4.0 WebUI Configuration



Carrier:

Current APN: staticip.apn
Activity Status: Call in progress
Network: CANRogersWirelessInc.
Home/Roaming: Home
Cell ID: 0x29E2B1
Data Service Type: 3G-WCDMA
Channel Number: 437
Frequency Band: 1900MHz
Ec/No (dB):
RSSI (dBm):
RSCP (dBm):
Received Packet
Receive bytes:
Receive packets:
Receive errors:
Drop packets:
Receive fifo:
Receive frame:
Compressed:
Receive multicas

Core Temperature(°C):
Supply Voltage(V):
IMEI:
IMSI:
SIM Card:
SIM Number (ICCID):
Phone Number:
WAN IP Address:

2G Frequency: ☑ 850 ☑ 900 ☑ 1800 ☑ 1900
3G Frequency: ☑ 1900 ☑ 850 □ 900 ☑ 2100 □ 1700
Carriers: ● Automatic ○ Manual ○ Fixed
Network Data Mode: ● Automatic ○ 3G Priority
Access Point Name(APN): staticip.apn
SIM Pin:
NAT: ○ Disable ● Enable
PPP Status: ○ Disable ● Enable
IP-Passthrough: Disable
Dial-on-Demand: ● Disable ○ Enable
Idle Timeout(s): 0
Connect Timeout(s): 90
Dialing Max Retries: 0
Authentication Type: chap
User Name:
Password:
Dial Number: *99***1#
Static IP Addr: 0.0.0.0
Use Remote DNS: ○ Disable ● Enable
Connect String: CONNECT
Initialization Strings...
DDNS Config...
ICMP Keep Alive Check...

The Web User Interface (WebUI) is a browser based configuration method that allows a user to use a graphical interface to configure, test and troubleshoot a IPn3G unit. Any standard web browser can be used and no additional software is required. Using the Web User Interface a user can:

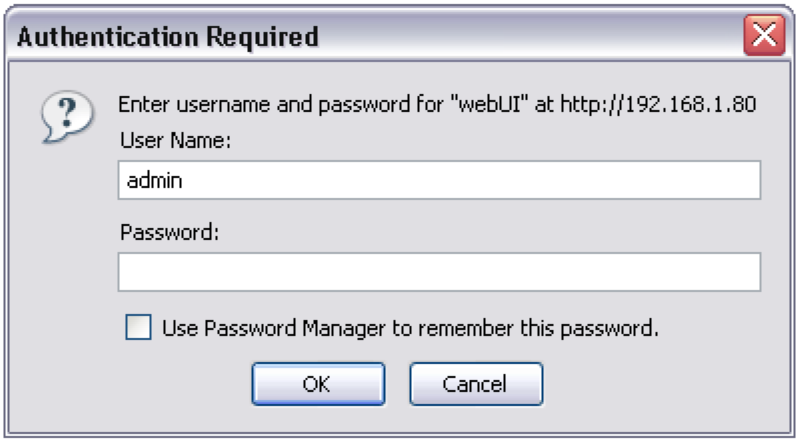
- Remotely or locally configure a IPn3G unit, including:
    - Network settings
    - Radio configuration
    - Serial Port configuration
    - Security
    - USB
    - Firewall
    - I/O
    - VPN
    - Retrieve unit revisions
    - Update system firmware
    - Much more...

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

4.0 WebUI Configuration

4.1 Logon Window

Upon successfully accessing the IPn3G using a Web Browser, the Logon window will appear.



Authentication Required

Enter username and password for "webUI" at http://192.168.1.80

User Name: admin

Password:

□ Use Password Manager to remember this password.

Image 4-1: Logon Window

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

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

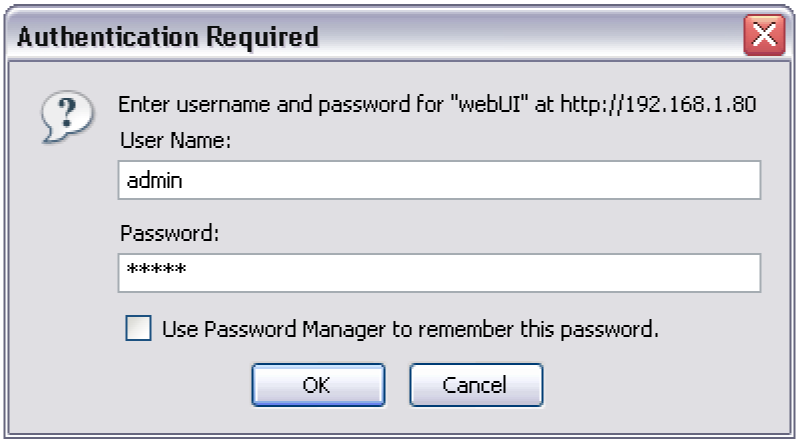
The default password is: **admin**

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.

It is advisable to change the login Password (see Section 4.1.8.1). Do not FORGET the new password as it cannot be recovered.



Authentication Required

Enter username and password for "webUI" at http://192.168.1.80

User Name: admin

Password: *****

□ Use Password Manager to remember this password.

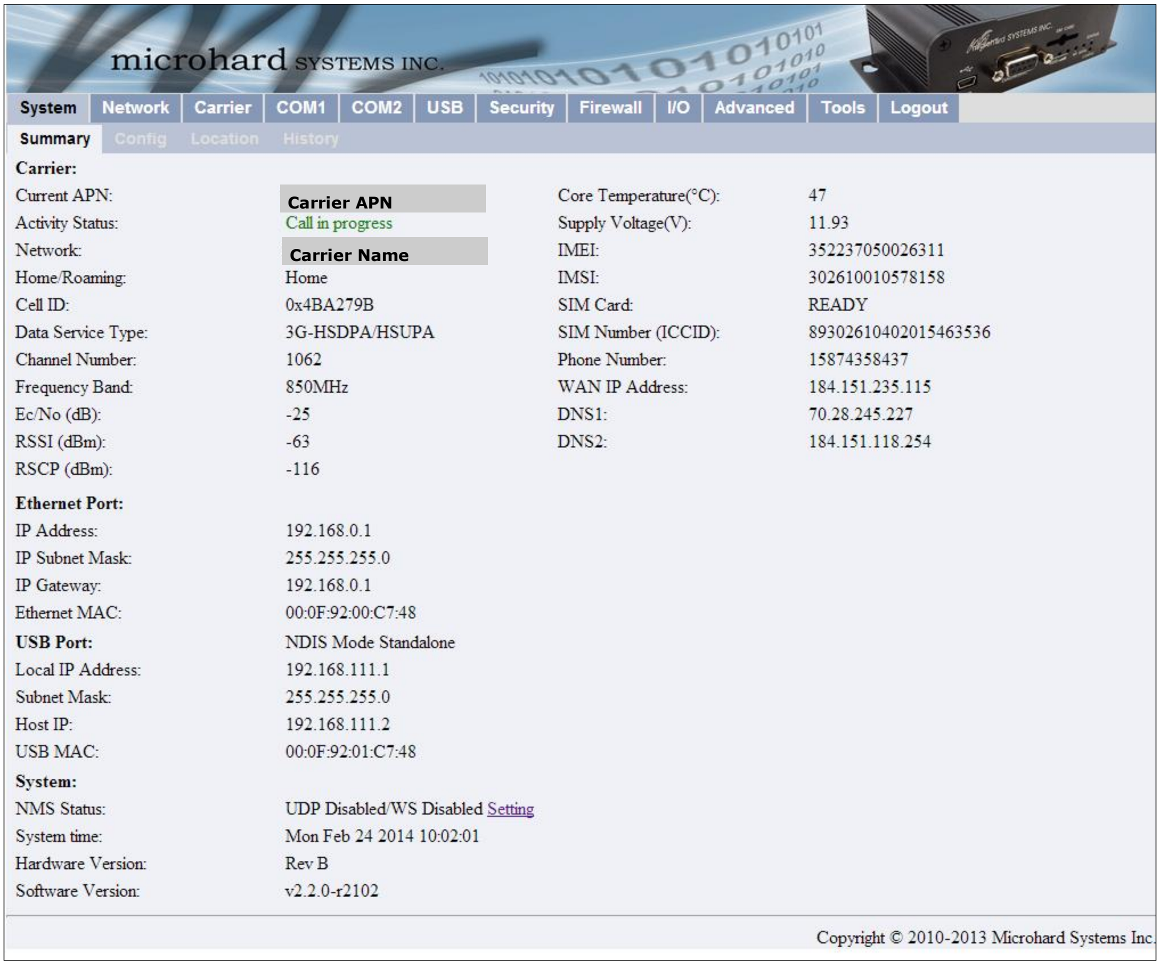
Image 4-2: Logon Window With Password Input

4.0 WebUI Configuration

4.2 System

4.2.1 System > Summary

The System Summary window displays an overview of the current IPn3G configuration. When initially logging into the unit, this will be the first window displayed, allowing a user to quickly identify configuration information.



Carrier:			
Current APN:	Carrier APN	Core Temperature(°C):	47
Activity Status:	Call in progress	Supply Voltage(V):	11.93
Network:	Carrier Name	IMEI:	352237050026311
Home/Roaming:	Home	IMSI:	302610010578158
Cell ID:	0x4BA279B	SIM Card:	READY
Data Service Type:	3G-HSDPA/HSUPA	SIM Number (ICCID):	89302610402015463536
Channel Number:	1062	Phone Number:	15874358437
Frequency Band:	850MHz	WAN IP Address:	184.151.235.115
Ec/No (dB):	-25	DNS1:	70.28.245.227
RSSI (dBm):	-63	DNS2:	184.151.118.254
RSCP (dBm):	-116		
Ethernet Port:			
IP Address:	192.168.0.1		
IP Subnet Mask:	255.255.255.0		
IP Gateway:	192.168.0.1		
Ethernet MAC:	00:0F:92:00:C7:48		
USB Port:	NDIS Mode Standalone		
Local IP Address:	192.168.111.1		
Subnet Mask:	255.255.255.0		
Host IP:	192.168.111.2		
USB MAC:	00:0F:92:01:C7:48		
System:			
NMS Status:	UDP Disabled/WS Disabled Setting		
System time:	Mon Feb 24 2014 10:02:01		
Hardware Version:	Rev B		
Software Version:	v2.2.0-r2102		

Copyright © 2010-2013 Microhard Systems Inc.

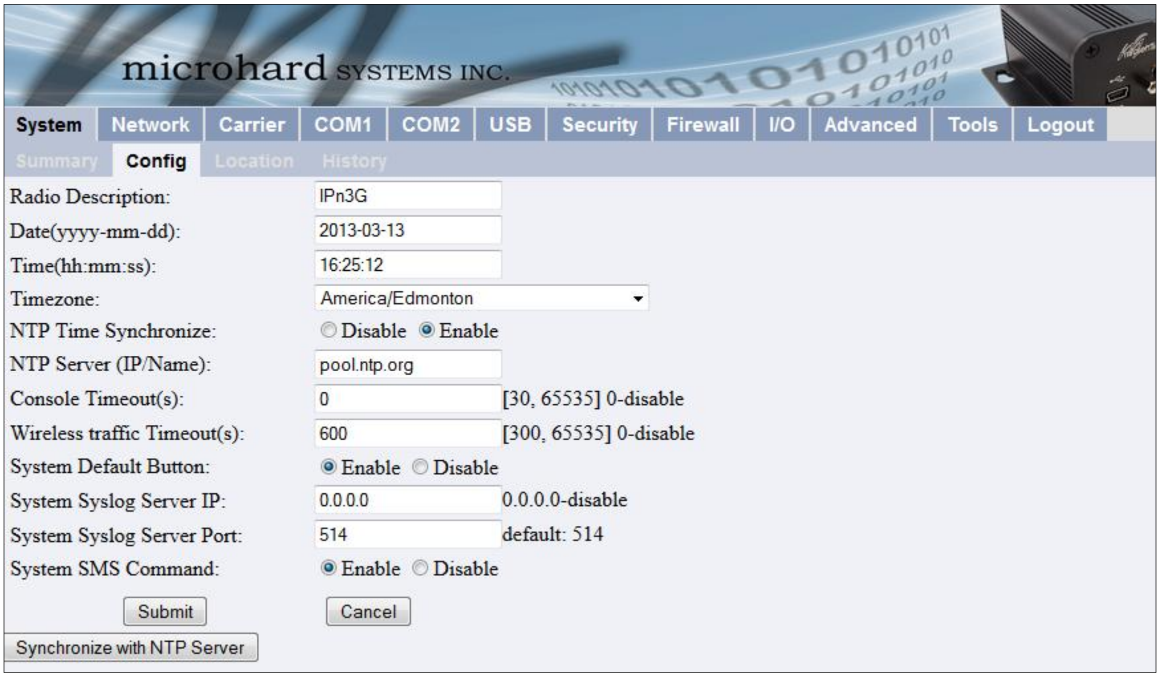
Image 4-3: System Summary Window

The System Summary window displays information about the wireless carrier as well as local network, USB and System information:

- **Carrier:** Activity Status, Network, WAN IP, Phone Number, SIM Card info etc
- **Ethernet Port:** Local Ethernet Port information of rear RJ45 Connector.
- **USB Port:** USB Port information, NDIS IP Address etc.
- **System:** Hardware and Software versions and System time.

4.2.2 System > Config

The System Config submenu allows the configuration of the Radio Description, the Time and Date, including NTP time server parameters. As well as the Console and Wireless Traffic timeouts.



Radio Description:	IPn3G	
Date(yyyy-mm-dd):	2013-03-13	
Time(hh:mm:ss):	16:25:12	
Timezone:	America/Edmonton	
NTP Time Synchronize:	○ Disable ● Enable	
NTP Server (IP/Name):	pool.ntp.org	
Console Timeout(s):	0	[30, 65535] 0-disable
Wireless traffic Timeout(s):	600	[300, 65535] 0-disable
System Default Button:	● Enable ○ Disable	
System Syslog Server IP:	0.0.0.0	0.0.0.0-disable
System Syslog Server Port:	514	default: 514
System SMS Command:	● Enable ○ Disable	

Image 4-4: System Config Window

Radio Description

The Radio Description is simply a convenient identifier for a specific IPn3G, e.g. Pump Station 5, 123 Main Street, etc. This feature is most welcome when accessing units remotely: a convenient cross-reference for the unit's IP address. This 'name' appears in all menu windows. It has no bearing on the unit's operation.

Values (Characters)

Default is model-dependent

up to 30 characters

Date (yyyy-mm-dd)

The calendar date may be entered in this field. Note that the entered value is lost should the IPn3G lose power for some reason.

Values (2010-08-05)

valid date values, where

yyyy	= 4-digit year
mm	= 2-digit month
dd	= 2-digit day

4.0 WebUI Configuration

Time (hh:mm:ss)

The calendar date may be entered in this field. Note that the entered value is lost should the IPn3G lose power for some reason.

Values (11:27:28)

hh	= 2-digit hours
mm	= 2-digit minutes
ss	= 2-digit seconds

Timezone

The Timezone field allows you to set the time zone in the IPn3G. Select the time zone from the dropdown list that matches your location. Time zones are sorted by UTC (+/-) offset.

Values (List)

Select the applicable time zone from the dropdown list.

NTP may be used to synchronize the time in the IPn3G within a network to a reference time source.

NTP Time Synchronize

Note that if NTP Server Status is ENABLED, the 'Synchronize with NTP Server' soft button on the System Configuration menu will be available for use.
Leave as DISABLED (default) if a server is not available.

Values (Selection)

Disable
Enable

NTP Server (IP/Name)

IP address or domain name for NTP server (on local LAN or website (provided that Internet access is available)) is to be entered in this field if the NTP Server Status is configured as ENABLED.

Values (0.0.0.0)

valid NTP server IP address or 'name'

Console Timeout (s)

This value determines when the console connection (made via COM2) will timeout after becoming inactive.

Values (seconds)

60
0-65535

Wireless Traffic Timeout (s)

The Wireless Traffic Timeout will reset the unit if there has been no RF activity in the configured time. 0 = Disabled (default)

Values (seconds)

600
300-65535

System Default Button

Enabled by default, when the CONFIG button on the front of the IPn3G 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

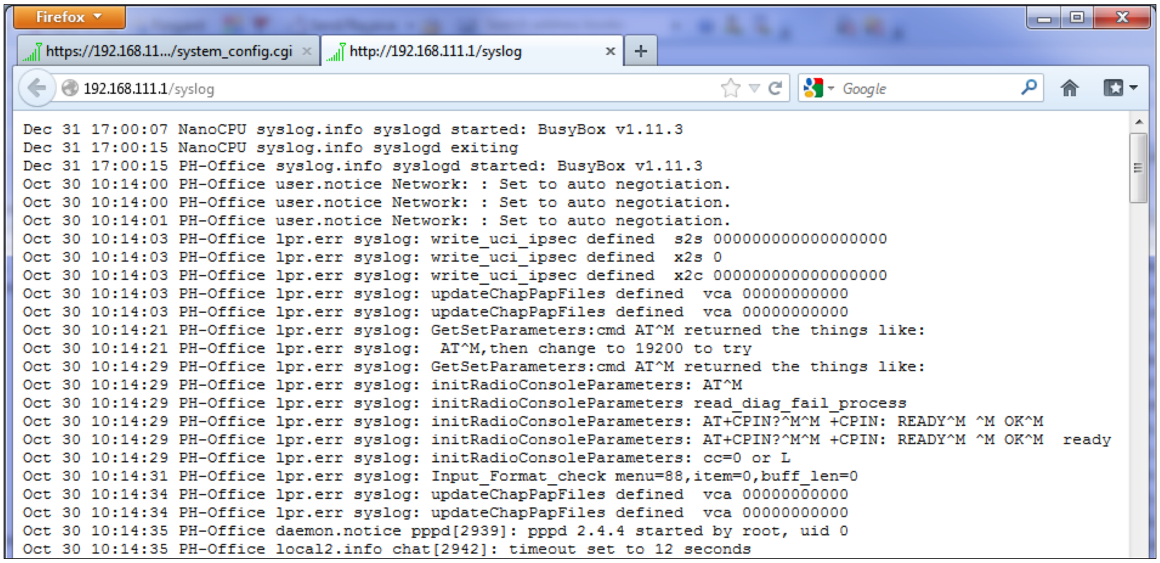
4.0 WebUI Configuration

System Syslog Server IP

The IPn3G can report system level events to a third party Syslog server, which can be used to monitor events reported by the IPn3G. The raw event syslog can be view by entering the following URL into the web browser http://X.X.X.X/syslog, Where X.X.X.X is the IP address of the IPn3G.

IP Address

0.0.0.0


Firefox
https://192.168.11.../system_config.cgi
http://192.168.111.1/syslog
192.168.111.1/syslog
Google

```
Dec 31 17:00:07 NanoCPU syslog.info syslogd started: BusyBox v1.11.3
Dec 31 17:00:15 NanoCPU syslog.info syslogd exiting
Dec 31 17:00:15 PH-Office syslog.info syslogd started: BusyBox v1.11.3
Oct 30 10:14:00 PH-Office user.notice Network: : Set to auto negotiation.
Oct 30 10:14:00 PH-Office user.notice Network: : Set to auto negotiation.
Oct 30 10:14:01 PH-Office user.notice Network: : Set to auto negotiation.
Oct 30 10:14:03 PH-Office lpr.err syslog: write_uci_ipsec defined  s2s 000000000000000000
Oct 30 10:14:03 PH-Office lpr.err syslog: write_uci_ipsec defined  x2s 0
Oct 30 10:14:03 PH-Office lpr.err syslog: write_uci_ipsec defined  x2c 000000000000000000
Oct 30 10:14:03 PH-Office lpr.err syslog: updateChapPapFiles defined  vca 00000000000
Oct 30 10:14:03 PH-Office lpr.err syslog: updateChapPapFiles defined  vca 00000000000
Oct 30 10:14:21 PH-Office lpr.err syslog: GetSetParameters:cmd AT^M returned the things like:
Oct 30 10:14:21 PH-Office lpr.err syslog:  AT^M,then change to 19200 to try
Oct 30 10:14:29 PH-Office lpr.err syslog: GetSetParameters:cmd AT^M returned the things like:
Oct 30 10:14:29 PH-Office lpr.err syslog: initRadioConsoleParameters: AT^M
Oct 30 10:14:29 PH-Office lpr.err syslog: initRadioConsoleParameters read_diag_fail_process
Oct 30 10:14:29 PH-Office lpr.err syslog: initRadioConsoleParameters: AT+CPIN?^M^M +CPIN: READY^M ^M OK^M
Oct 30 10:14:29 PH-Office lpr.err syslog: initRadioConsoleParameters: AT+CPIN?^M^M +CPIN: READY^M ^M OK^M  ready
Oct 30 10:14:29 PH-Office lpr.err syslog: initRadioConsoleParameters: cc=0 or L
Oct 30 10:14:31 PH-Office lpr.err syslog: Input_Format_check menu=88,item=0,buff_len=0
Oct 30 10:14:34 PH-Office lpr.err syslog: updateChapPapFiles defined  vca 00000000000
Oct 30 10:14:34 PH-Office lpr.err syslog: updateChapPapFiles defined  vca 00000000000
Oct 30 10:14:35 PH-Office daemon.notice pppd[2939]: pppd 2.4.4 started by root, uid 0
Oct 30 10:14:35 PH-Office local2.info chat[2942]: timeout set to 12 seconds
```

Image 4-5: Syslog

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

System SMS Command

This option allows a user to enable or disable to use of the following SMS commands to reboot or trigger events in the IPn3G:

Values (Selection)

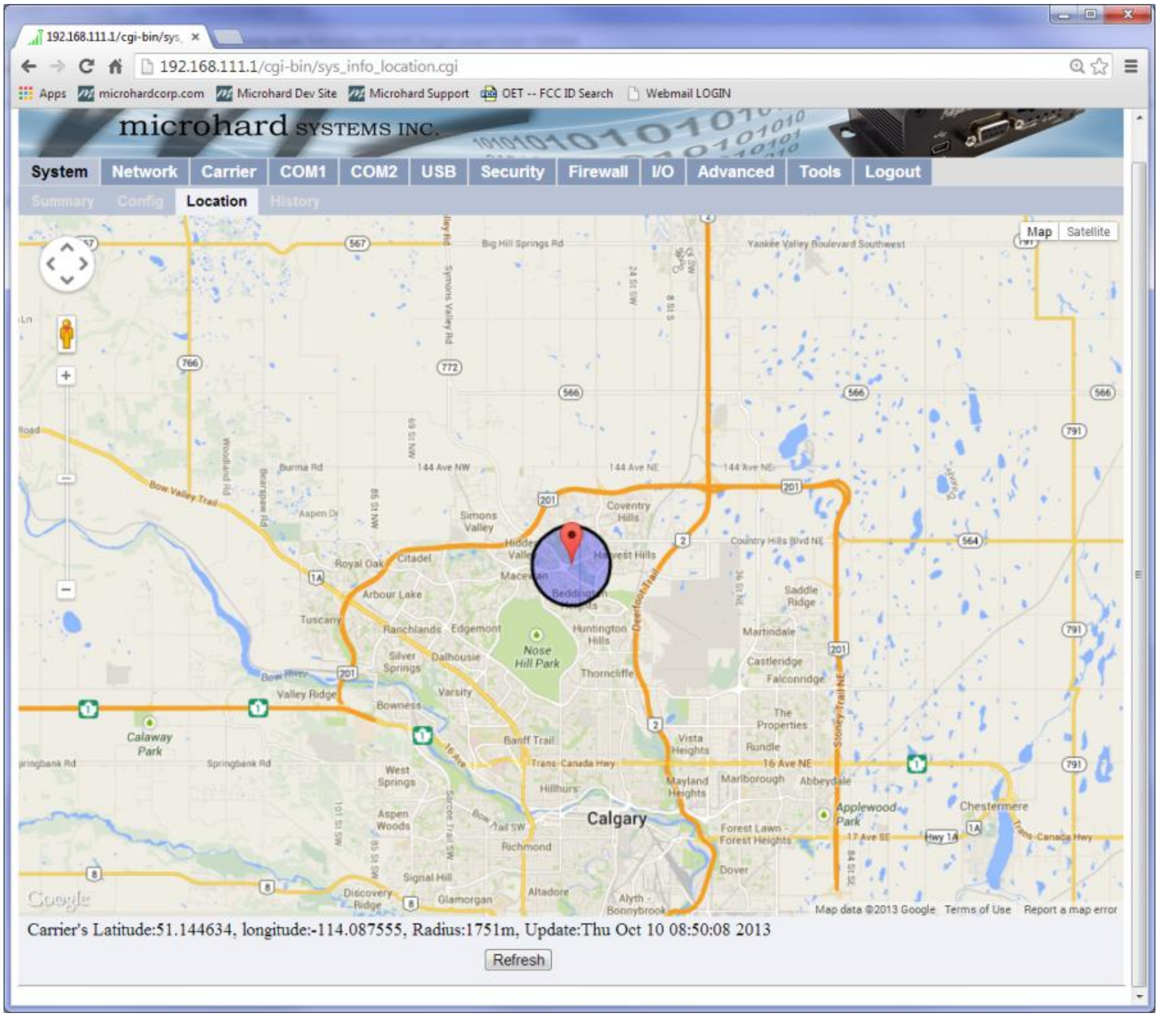
Enable / Disable

MSC#REBOOT	Reboot system
MSC#MIOP1	open I/O ouput1
MSC#MIOC1	close I/O ouput1
MSC#EURD0	trigger event report0
MSC#EURD1	trigger event report1
MSC#EURD2	trigger event report2
MSC#NMS	trigger NMS UDP report
MSC#WEB	trigger NMS webclient service immediately
MSC#PSCLOSE	close power saving mode
MSC#PSVOL	enable/switch to supply voltage power mode
MSC#PSTIMER	enable/switch to timer power mode
MSC#PSSNIFF	enable/switch to sniff power mode
MSC#APN	set APN and reconnect. MSC=apn[,usr][,pwd]

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

4.2.3 System > Location

The Location menu shows current modem location with online map and exact GPS Coordinate. If the GPS is not valid, it uses the Cell Tower ID that the unit is currently connect to, to approximate the general location of the IPn3G.

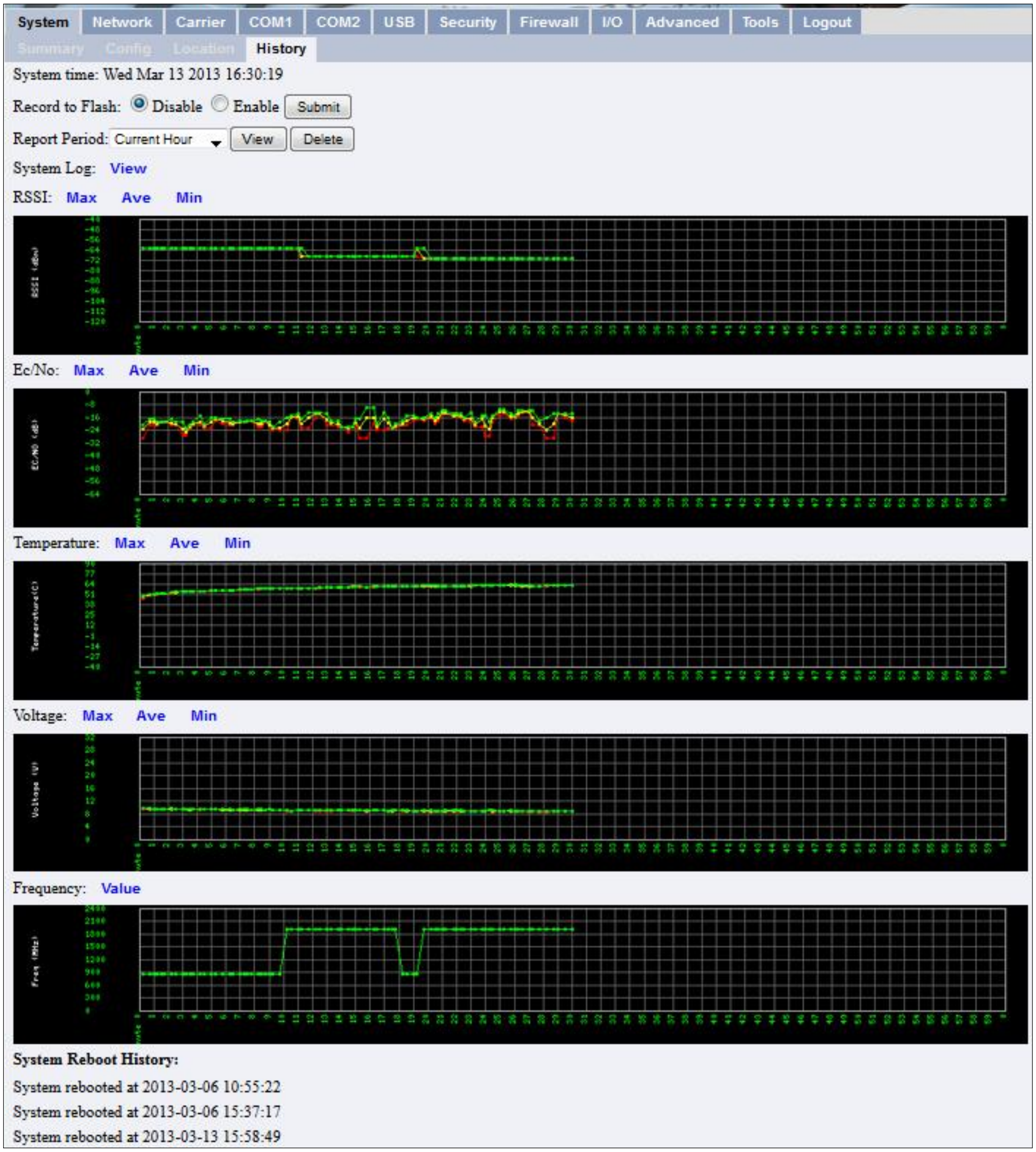


Carrier's Latitude:51.144634, longitude:-114.087555, Radius:1751m, Update:Thu Oct 10 08:50:08 2013

Image 4-6: System > Location

4.2.4 System > History

The History menu shows a graphical history of RSSI, Ec/No, Temperature, Voltage and Frequency of the Cellular module. Data for the current hour, as well as a specific 24 hour period of a calendar date. Clicking the Max, Ave and Min links will show the raw data used to plots the points on the graphs. The data points are optionally stored in non-volatile (flash) memory, so data is saved even when the IPn3G is restarted or power is lost.



System time: Wed Mar 13 2013 16:30:19

Record to Flash: ● Disable ○ Enable

Report Period: Current Hour

System Log: View

RSSI: Max Ave Min

Ec/No: Max Ave Min

Temperature: Max Ave Min

Voltage: Max Ave Min

Frequency: Value

System Reboot History:

System rebooted at 2013-03-06 10:55:22

System rebooted at 2013-03-06 15:37:17

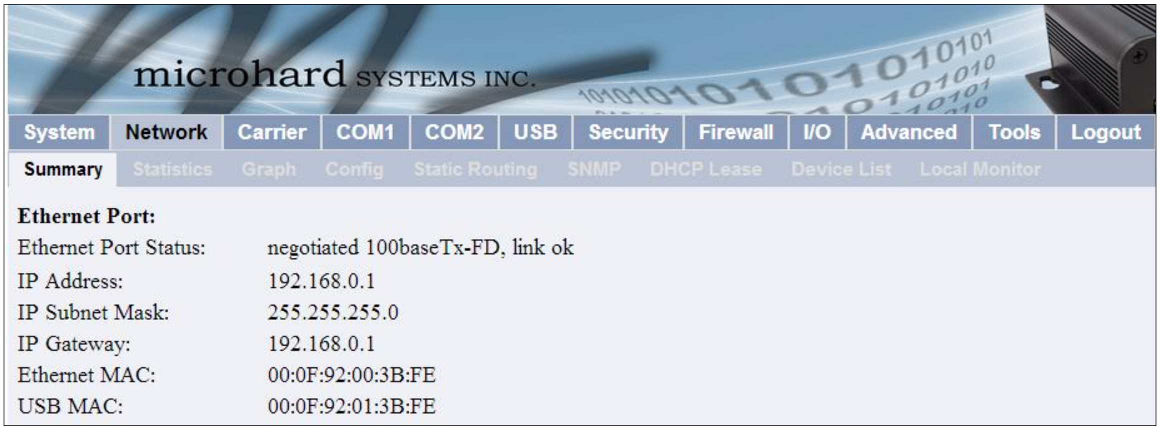
System rebooted at 2013-03-13 15:58:49

Image 4-7: System > Location

4.3 Network

4.3.1 Network > Summary

The Network > Summary tab gives an overview of the configuration of the Ethernet port on the IPn3G. This port is the RJ45 port located on the back of the IPn3G.



Ethernet Port:

Ethernet Port Status:	negotiated 100baseTx-FD, link ok
IP Address:	192.168.0.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.0.1
Ethernet MAC:	00:0F:92:00:3B:FE
USB MAC:	00:0F:92:01:3B:FE

Image 4-8: Network Configuration , Local IP Configuration Submenu

Ethernet Port Status: The Ethernet port status shows the type and status of the local Ethernet Link.

IP Address: This is the currently configured logical IP address of the IPn3G. This IP address must be set statically in the Network > Config tab. This is generally set to a Private IP address for a local network.

IP Subnet Mask: The IP Subnet Mask is the current Subnet Mask being used by the unit to define the subnet and host address of the IPn3G.

IP Gateway: The IP Gateway sets the default gateway for traffic leaving the IPn3G.

Ethenet MAC: This is the physical MAC address of the RJ45 Ethernet Port of the back of the IPn3G

USB MAC: For quick reference, this is the physical MAC address of the USB port on the front of the IPn3G, when it is configured as a NDIS Ethernet Interface. See the USB section for more information.

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

4.3.2 Network > Statistics

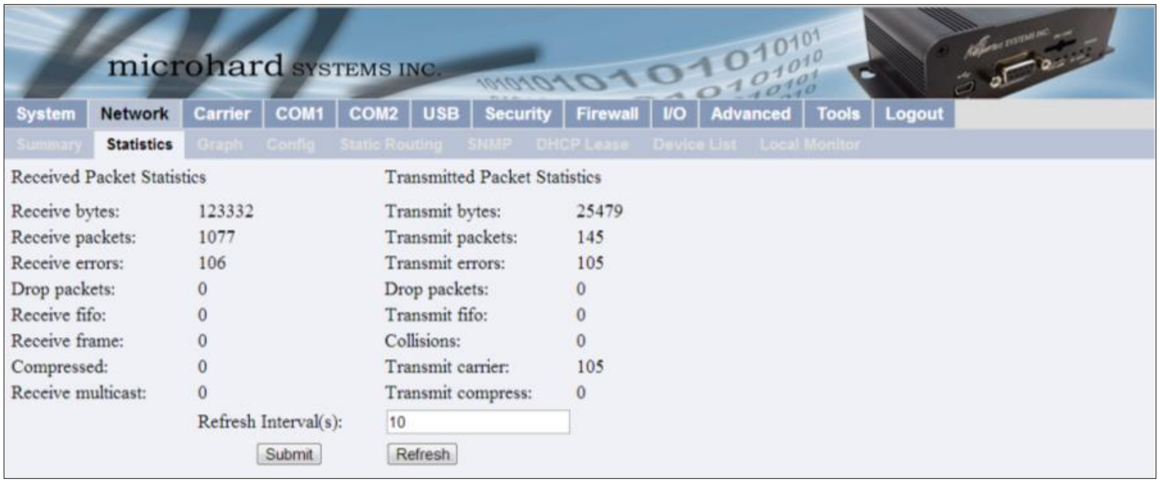
The Network > Statistics tab displays a variety of parameters which apply to the traffic through, and status of, the physical Ethernet port (hardware interface) on the rear of the IPn3G.

Received and Transmitted information are applicable to the local data traffic into and out of the IPn3G, respectively. Errors which are counted include alignment, frame check sequence (FCS), frame too long, and internal MAC. The dropped packet count could increment if, for example, the network layer was too busy to accept the data.

The FIFO errors are related to interface-specific hardware.

Collisions occur on all Ethernet networks being that Ethernet operates as a logical bus. The amount of collisions is typically related to the number of devices on the attached network and the amount of data being moved.

The Transmit Carrier count relates to carrier sense errors.



Received Packet Statistics		Transmitted Packet Statistics	
Receive bytes:	123332	Transmit bytes:	25479
Receive packets:	1077	Transmit packets:	145
Receive errors:	106	Transmit errors:	105
Drop packets:	0	Drop packets:	0
Receive fifo:	0	Transmit fifo:	0
Receive frame:	0	Collisions:	0
Compressed:	0	Transmit carrier:	105
Receive multicast:	0	Transmit compress:	0
	Refresh Interval(s):	10	

Image 4-9: Network Statistics

4.0 WebUI Configuration

4.3.3 Network > Graph

The Network > Graph tab displays a graphical display of the Ethernet Traffic on the Ethernet interface of the IPn3G.

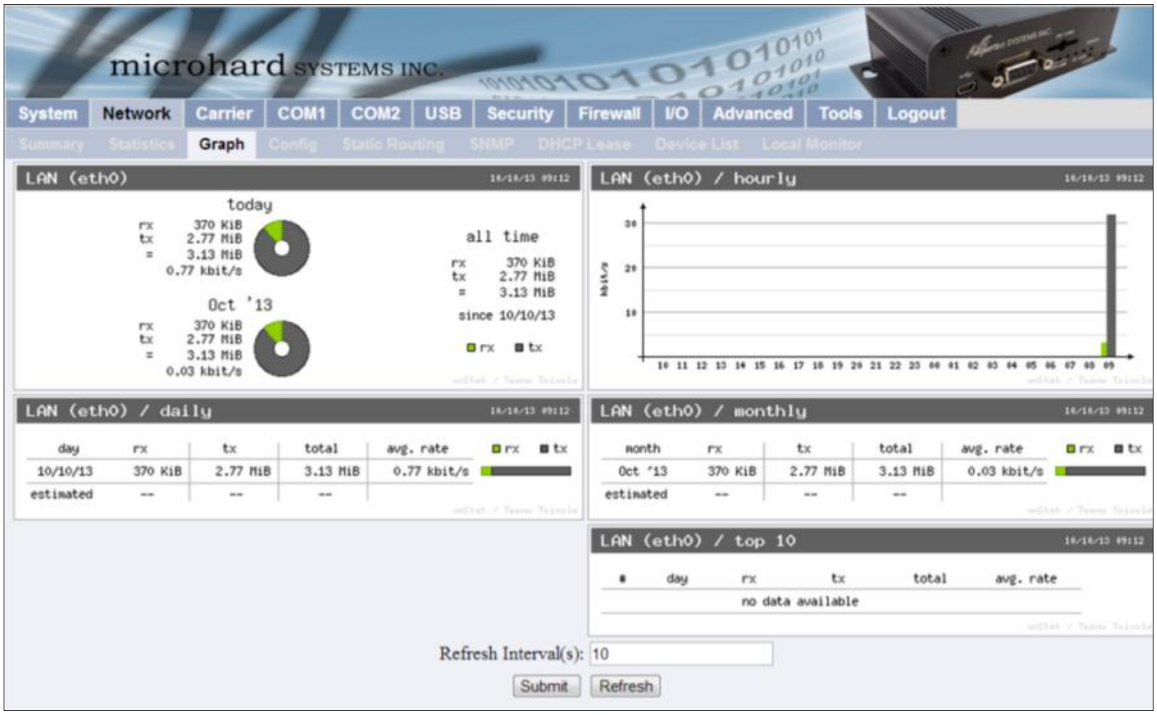
LAN (eth0) Shows an overview of all data sent or received by the IPn3G at the physical Ethernet port on the rear of the unit. A summary of the data of the current day and the current month is shown.

LAN (eth0) / hourly Shows the traffic volumes (TX = green, RX = grey) at hourly intervals during the current 24 hour period. This could be useful to see when the most or least amount of traffic is present.

LAN (eth0) / daily Shows the total data received and transmitted for the day, as well as the average rate of data.

LAN (eth0) / monthly Shows the total data received and transmitted for the current month, as well as the average rate of data.

LAN (eth0) / Top 10 Show the top 10 days with the most data sent or received.



LAN (eth0) 10/10/13 09:12

today
rx 370 KiB
tx 2.77 MiB
= 3.13 MiB
0.77 kbit/s

Oct '13
rx 370 KiB
tx 2.77 MiB
= 3.13 MiB
0.03 kbit/s

all time
rx 370 KiB
tx 2.77 MiB
= 3.13 MiB
since 10/10/13

LAN (eth0) / hourly 10/10/13 09:12

LAN (eth0) / daily 10/10/13 09:12

day	rx	tx	total	avg. rate
10/10/13	370 KiB	2.77 MiB	3.13 MiB	0.77 kbit/s
estimated	--	--	--	

LAN (eth0) / monthly 10/10/13 09:12

month	rx	tx	total	avg. rate
Oct '13	370 KiB	2.77 MiB	3.13 MiB	0.03 kbit/s
estimated	--	--	--	

LAN (eth0) / top 10 10/10/13 09:12

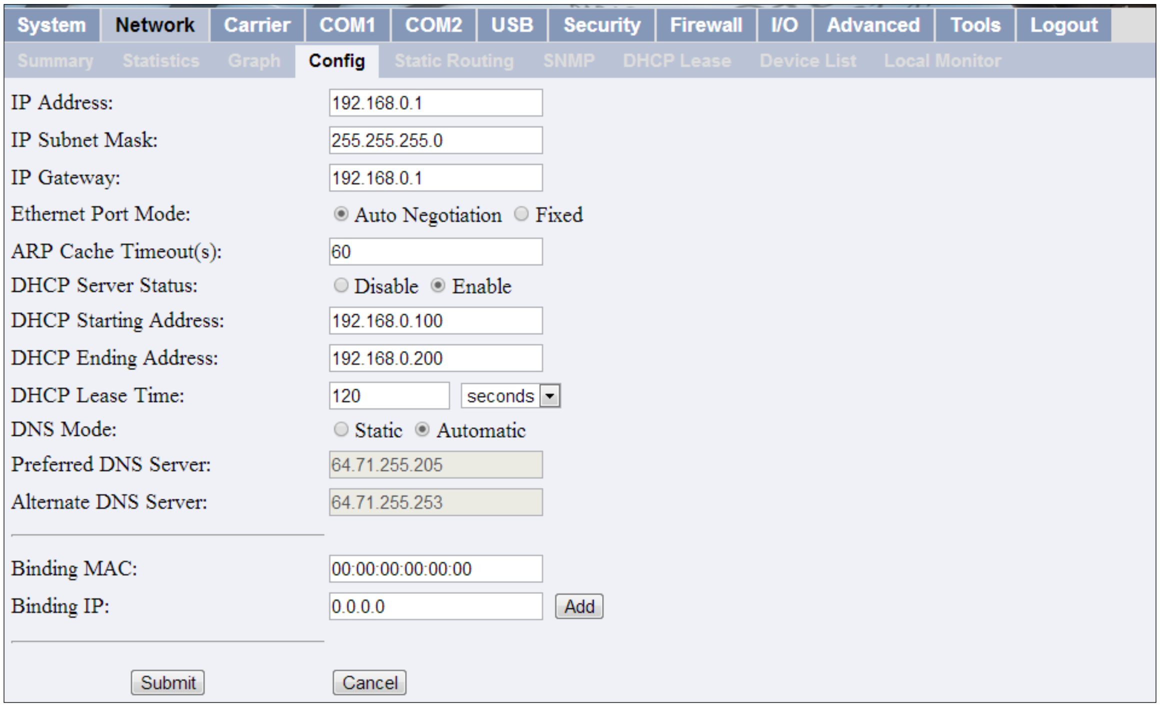
#	day	rx	tx	total	avg. rate
		no data available			

Refresh Interval(s): 10

Image 4-10: Network Graph

4.3.4 Network > Config

The Network > Config tab allows the configuration of the Ethernet port on the IPn3G (Rear RJ45). This port is configured as static port and must be configured by the user if the default values are not to be used. By default this port acts as a simple DHCP server, allowing the IPn3G to assign IP addresses and enable communication to attached devices. Caution must be taken not to connect the IPn3G to an existing network where a DHCP server may already be running.



IP Address:	192.168.0.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.0.1
Ethernet Port Mode:	● Auto Negotiation ○ Fixed
ARP Cache Timeout(s):	60
DHCP Server Status:	○ Disable ● Enable
DHCP Starting Address:	192.168.0.100
DHCP Ending Address:	192.168.0.200
DHCP Lease Time:	120 seconds
DNS Mode:	○ Static ● Automatic
Preferred DNS Server:	64.71.255.205
Alternate DNS Server:	64.71.255.253
Binding MAC:	00:00:00:00:00:00
Binding IP:	0.0.0.0 Add

Image 4-11: Network Configuration , Local IP Configuration Submenu

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

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.

IP Address

Enter a valid IP Address. The default IP address for the Ethernet Port on the IPn3G is **192.168.0.1**.

Values

192.168.0.1

IP Subnet Mask

For a small private network with IP addresses appearing similar to 192.168.1.xx (Class C address), the standard 255.255.255.0 subnet mask may be applicable.

Values

255.255.255.0

IP Gateway

If the IPn3G units are 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.

Values

192.168.0.1

4.0 WebUI Configuration

Ethernet Port Mode

This option allows a user to select between Auto Negotiation (10/100), or Fixed. If fixed is selected, additional options appear below.

Values (selection)

Auto Negotiation
Fixed

Ethernet Port Speed

This option allows a user to select between Auto Negotiation (10/100), or Fixed. If fixed is selected, additional options appear below.

Values (selection)

100MBit/s / 10MBit/s

Ethernet Port Duplex

Choose between full and half duplex.

Values (selection)

Full / Half

ARP Cache Timeout(s)

The ARP Cache timeout allows the configuration of how long a ARP entry stays in the ARP table.

Values (seconds)

60

DHCP Server Status

Choose to enable or disabled the DHCP Server service. Devices on the network, which are intended to receive IP address information from this DHCP Server, must have their local IP settings set for 'DHCP' (as opposed to 'static'). The default is **Enabled**.

Values

Disable
Enable

⚠

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

DHCP Starting/Ending Address

Use the Starting and Ending Address fields to define the range that the DHCP server will assign IP Addresses. (also known as the address pool).

Values

192.168.0.100 to 192.168.0.200

DHCP Lease Time

This is the amount of time a device can lease an IP Address from the IPn3G before it must renew or obtain a new IP address. This option allows the user to specify if the lease time specified in in seconds, minutes, hours etc.

Values (selection)

Seconds
Minutes
Hours
Days
Weeks

DNS Mode

Select between Static (user must specify DNS server addresses), or Automatic (the DNS servers are assigned by the Carrier).

Values (selection)

Static
Automatic

Preferred DNS Server

If set for Static, a user would enter the IP Address of the desired primary DNS server in this field. If set for automatic, this field will be populated by the currently assigned DNS address.

Values (IP Address)

(current DNS Server)

Alternate DNS Server

If set for Static, a user would enter the IP Address of the desired alternate DNS server in this field. If set for automatic, this field will be populated by the currently assigned DNS address.

Values (IP Address)

(current DNS Server)

Binding MAC

It may be desirable to ensure specific devices always obtain the same IP address from the DHCP service. Enter the MAC address of that device in this field.

Values (MAC)

00:00:00:00:00:00

Binding IP

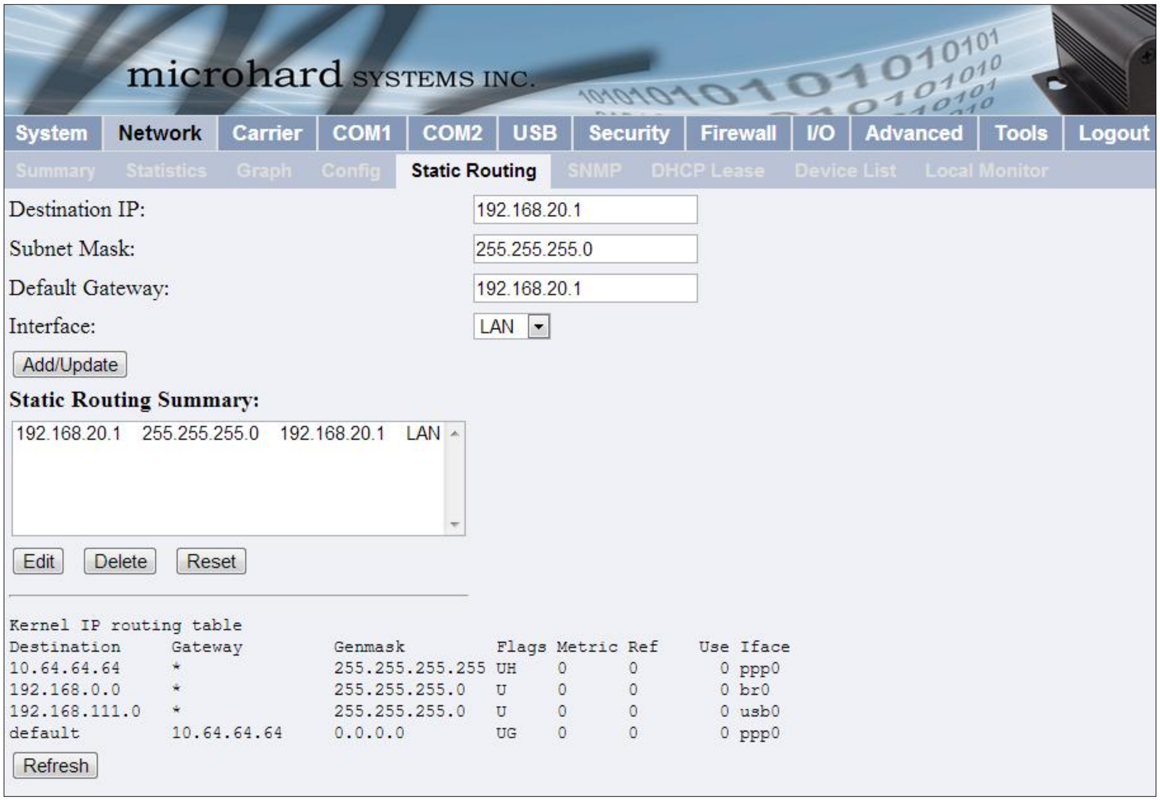
It may be desirable to ensure specific devices always obtain the same IP address from the DHCP service. Enter the IP Address to be assigned to that device here.

Values (IP Address)

0.0.0.0

4.3.5 Network > Static Routing

The Network > Static Routing Menu, allows for the user to add static routes to the IPn3G. Static routes can be used to inform IPn3G of networks that are not directly attached.



Destination IP:	192.168.20.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.20.1
Interface:	LAN

Static Routing Summary:

192.168.20.1 255.255.255.0 192.168.20.1 LAN

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.64.64.64     *               255.255.255.255 UH    0      0        0 ppp0
192.168.0.0     *               255.255.255.0   U     0      0        0 br0
192.168.111.0   *               255.255.255.0   U     0      0        0 usb0
default         10.64.64.64     0.0.0.0         UG    0      0        0 ppp0
```

Image 4-12: Network Configuration , Local IP Configuration Submenu

Destination IP / Subnet Mask

Enter the destination IP Address and subnet mask of the remote network for which the data is intended.

Values (IP Address)

0.0.0.0 / 255.255.255.0

Default Gateway

Enter the IP Address of the next hop to the destination network.

Values

0.0.0.0

Interface

Select the interface from which the destination network is available. LAN refers to the network attached locally through the RJ45, and the WAN is the Cellular network.

Values (selection)

WAN / LAN

4.3.6 Network > SNMP

The IPn3G may be configured to operate as a Simple Network Management Protocol (SNMP) agent.

Network management is most important in larger networks, so as to be able to manage resources and measure performance.

SNMP may be used in several ways:

- configure remote devices
- monitor network performance
- detect faults
- audit network usage
- detect authentication failures

A SNMP management system (a PC running SNMP management software) is required for this service to operate. An SNMP MIB Browser can be also be used to provision the IPn3G, these utilities are not supplied by Microhard Systems, but many free and premium types of browsers are available on the market. This system must have full access to the IPn3G network. 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 IPn3G 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. Contact Microhard Systems Inc, for the most recent MIB file.

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).

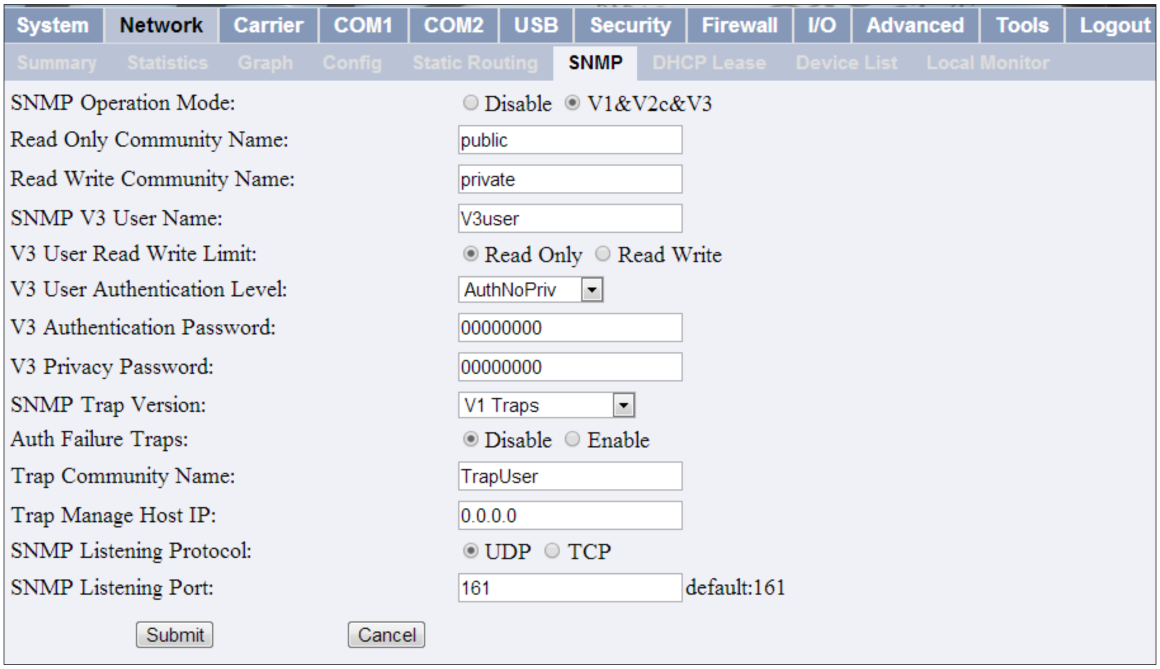
SNMPv2c adds to the above the ability to retrieve a large number of objects in response to a single request.

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.

Custom MIBs can be obtained by contacting Microhard Systems Inc. ***Appendix F: SNMP MIB Sample*** contains the first few pages of the IPn3G MIB to be used as a reference The MIB file can change when new features are added, so it is best to contact us for the complete and latest MIB file for the IPn3G.

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.



SNMP Operation Mode:	○ Disable ● V1&V2c&V3
Read Only Community Name:	public
Read Write Community Name:	private
SNMP V3 User Name:	V3user
V3 User Read Write Limit:	● Read Only ○ Read Write
V3 User Authentication Level:	AuthNoPriv
V3 Authentication Password:	00000000
V3 Privacy Password:	00000000
SNMP Trap Version:	V1 Traps
Auth Failure Traps:	● Disable ○ Enable
Trap Community Name:	TrapUser
Trap Manage Host IP:	0.0.0.0
SNMP Listening Protocol:	● UDP ○ TCP
SNMP Listening Port:	161 default:161

Image 4-13: Network > SNMP

SNMP Operation Mode

If disabled, no SNMP service is provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2, & v3.

Values

Disable / V1&V2&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 (char string)

public

Read Write 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/WRITE priority.

Values (char string)

private

SNMP V3 User Name

Defines the user name for SNMPv3.

Values (char string)

V3user

V3 User Read Write Limit

Defines accessibility of SNMPv3; select either Read Only or Read/Write priority. 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

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, encrpytion.

Values

NoAuthNoPriv
AuthNoPriv
AuthPriv

V3 Authentication Password

SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv (see above).

Values (char string)

00000000

V3 Authentication Password

SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).

Values (char string)

00000000

SNMP Trap Version

Select which version of trap will be sent should a failure or alarm condition occur.

Values

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

Disable / Enable

Trap Community Name

The community name which may receive traps.

Values (char string)

TrapUser

Trap Manage Host IP

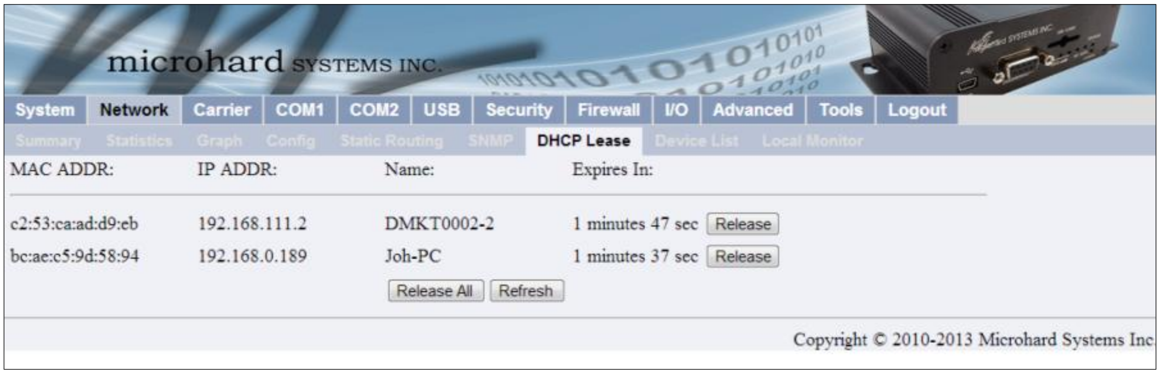
Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address).

Values

0.0.0.0

4.3.7 Network > DHCP Lease

The Network > DHCP Lease tab shows a summary of IP Addresses assigned by the IPn3G's DHCP server. As seen below the MAC address, IP Address, Name and the amount of time remaining on the DHCP lease is shown.



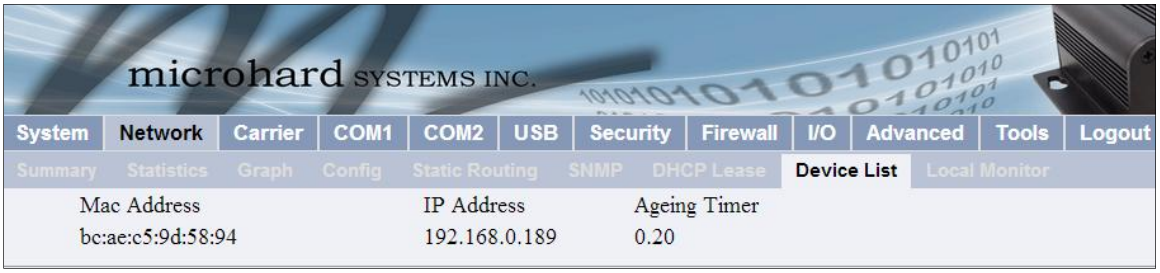
MAC ADDR:	IP ADDR:	Name:	Expires In:
c2:53:ca:ad:d9:eb	192.168.111.2	DMKT0002-2	1 minutes 47 sec Release
bc:ae:c5:9d:58:94	192.168.0.189	Joh-PC	1 minutes 37 sec Release

Copyright © 2010-2013 Microhard Systems Inc.

Image 4-14: Network Configuration , Local IP Configuration Submenu

4.3.8 Network > Device List

The Network > Device List shows the current ARP table for the local network adapter. Similar to the DHCP list 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.

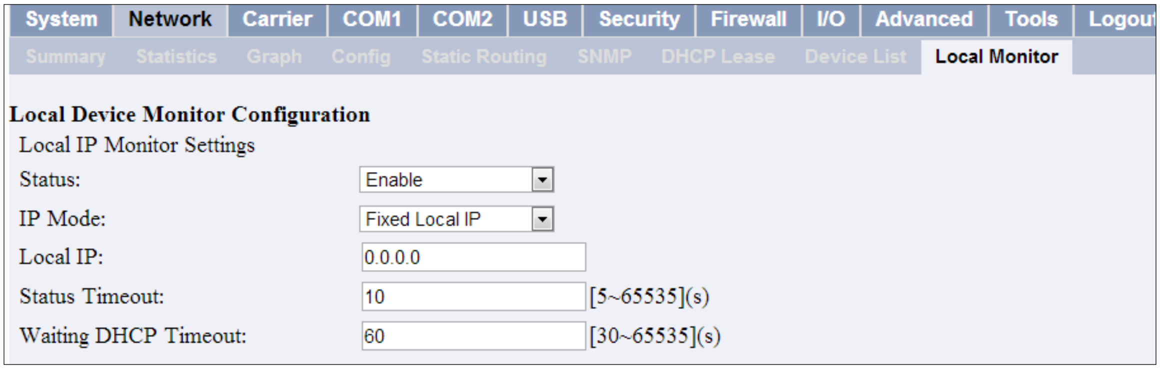


Mac Address	IP Address	Ageing Timer
bc:ae:c5:9d:58:94	192.168.0.189	0.20

Image 4-15: Network Configuration , Device List

4.3.9 Network > Local Monitor

The Local Device Monitor allows a user to monitor a local device connected locally to the Ethernet port or to the locally attached network. If the IPn3G 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.



Local Device Monitor Configuration

Local IP Monitor Settings

Status:	Enable	
IP Mode:	Fixed Local IP	
Local IP:	0.0.0.0	
Status Timeout:	10	[5~65535](s)
Waiting DHCP Timeout:	60	[30~65535](s)

Image 4-16: Network Configuration , 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 IPn3G will detect and monitor DHCP assigned IP address.

Values (selection)

Fixed local IP
Auto Detected IP

Local IP

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 IPn3G will wait to detect the monitored device. At this time the IPn3G will restart the DHCP service.

Values (seconds)

10

Waiting DHCP Timeout

This field defines the amount of time the IPn3G will wait to detect the monitored device before it will reboot the modem.

Values (seconds)

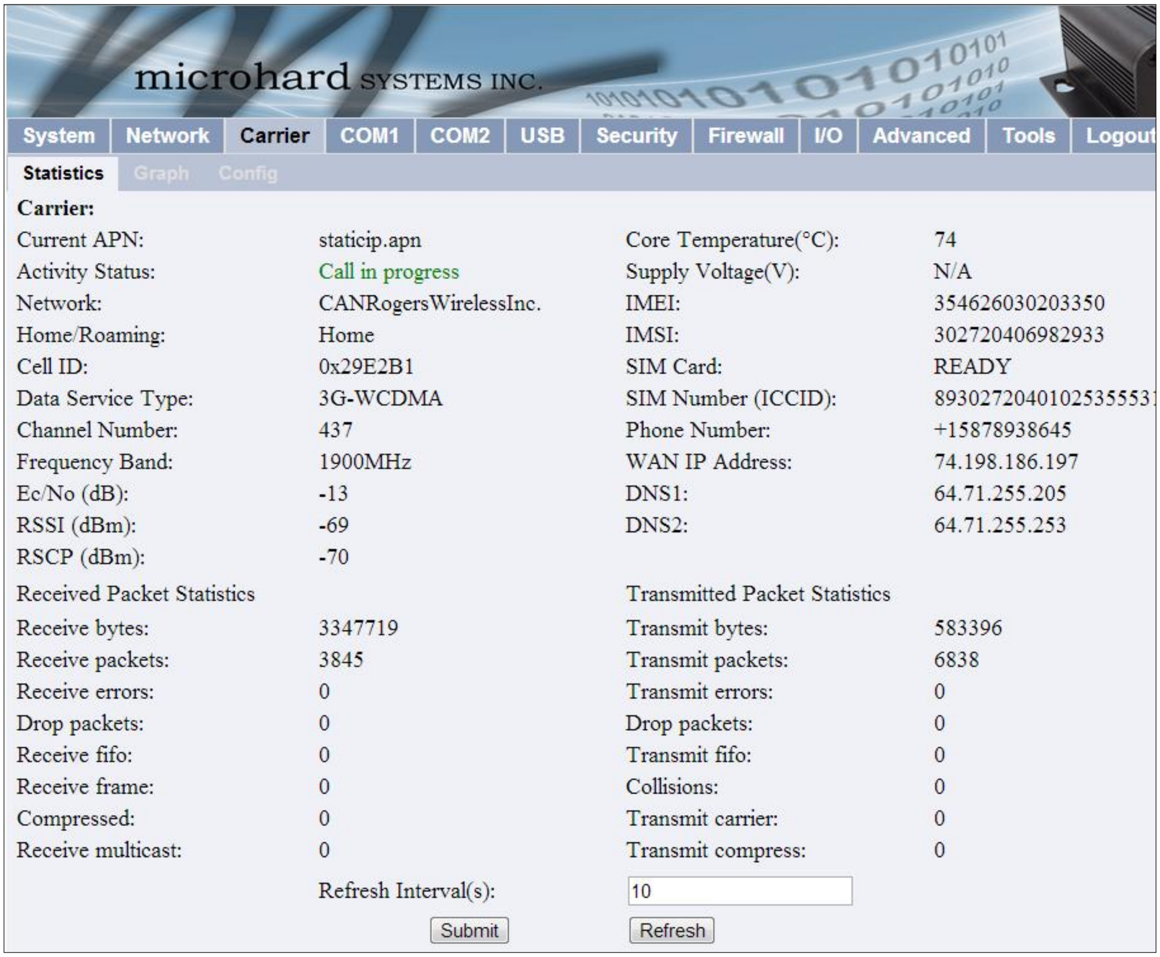
60

4.0 WebUI Configuration

4.4 Carrier

4.4.1 Carrier > Statistics

The Carrier Statistics window provides information related to the Wireless Carrier portion of the IPn3G. A variety of information can be found here, such as Activity Status, Network (Name of Wireless Carrier connected) , Data Service Type(2G/3G/HSPA etc), Frequency band, Phone Number etc.



Carrier:

Current APN:	staticip.apn	Core Temperature(°C):	74
Activity Status:	Call in progress	Supply Voltage(V):	N/A
Network:	CANRogersWirelessInc.	IMEI:	354626030203350
Home/Roaming:	Home	IMSI:	302720406982933
Cell ID:	0x29E2B1	SIM Card:	READY
Data Service Type:	3G-WCDMA	SIM Number (ICCID):	89302720401025355553
Channel Number:	437	Phone Number:	+15878938645
Frequency Band:	1900MHz	WAN IP Address:	74.198.186.197
Ec/No (dB):	-13	DNS1:	64.71.255.205
RSSI (dBm):	-69	DNS2:	64.71.255.253
RSCP (dBm):	-70		
Received Packet Statistics		Transmitted Packet Statistics	
Receive bytes:	3347719	Transmit bytes:	583396
Receive packets:	3845	Transmit packets:	6838
Receive errors:	0	Transmit errors:	0
Drop packets:	0	Drop packets:	0
Receive fifo:	0	Transmit fifo:	0
Receive frame:	0	Collisions:	0
Compressed:	0	Transmit carrier:	0
Receive multicast:	0	Transmit compress:	0

Refresh Interval(s): 10

Submit Refresh

Image 4-17: Carrier Configuration Menu

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.

4.4.2 Carrier > Graph

The Carrier > Graph tab displays a graphical display of the Carrier Traffic on the Wireless interface of the IPn3G.

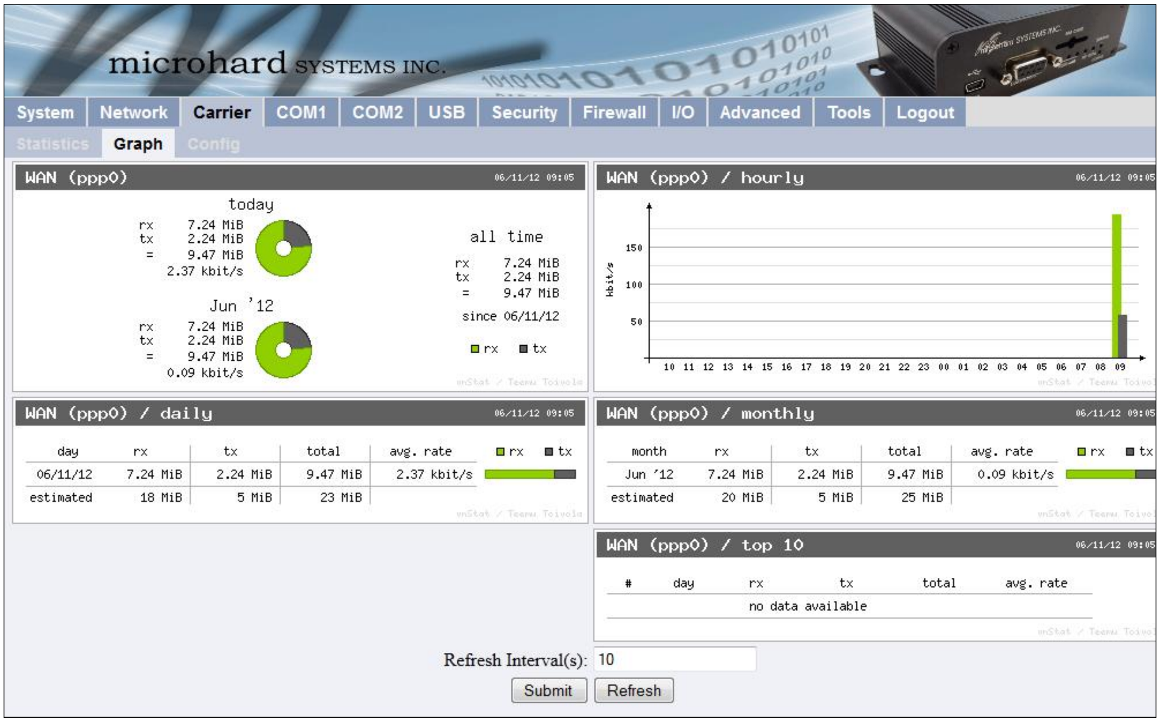
WAN (ppp0) Shows an overview of all data sent or received by the IPn3G on the Wireless portion of the unit. A summary of the data of the current day and the current month is shown.

WAN (ppp0) / hourly Shows the traffic volumes (TX = green, RX = grey) at hourly intervals during the current 24 hour period. This could be useful to see when the most or least amount of traffic is present.

WAN (ppp0) / daily Shows the total data received and transmitted for the day, as well as the average rate of data.

WAN (ppp0) / monthly Shows the total data received and transmitted for the current month, as well as the average rate of data.

WAN (ppp0) / Top 10 Show the top 10 days with the most data sent or received.



WAN (ppp0) 06/11/12 09:05

today

rx	7.24 MiB
tx	2.24 MiB
=	9.47 MiB
	2.37 kbit/s

Jun '12

rx	7.24 MiB
tx	2.24 MiB
=	9.47 MiB
	0.09 kbit/s

all time

rx	7.24 MiB
tx	2.24 MiB
=	9.47 MiB

since 06/11/12

🟩 rx ■ tx

WAN (ppp0) / hourly 06/11/12 09:05

WAN (ppp0) / daily 06/11/12 09:05

day	rx	tx	total	avg. rate	🟩 rx ■ tx
06/11/12	7.24 MiB	2.24 MiB	9.47 MiB	2.37 kbit/s	
estimated	18 MiB	5 MiB	23 MiB		

WAN (ppp0) / monthly 06/11/12 09:05

month	rx	tx	total	avg. rate	🟩 rx ■ tx
Jun '12	7.24 MiB	2.24 MiB	9.47 MiB	0.09 kbit/s	
estimated	20 MiB	5 MiB	25 MiB		

WAN (ppp0) / top 10 06/11/12 09:05

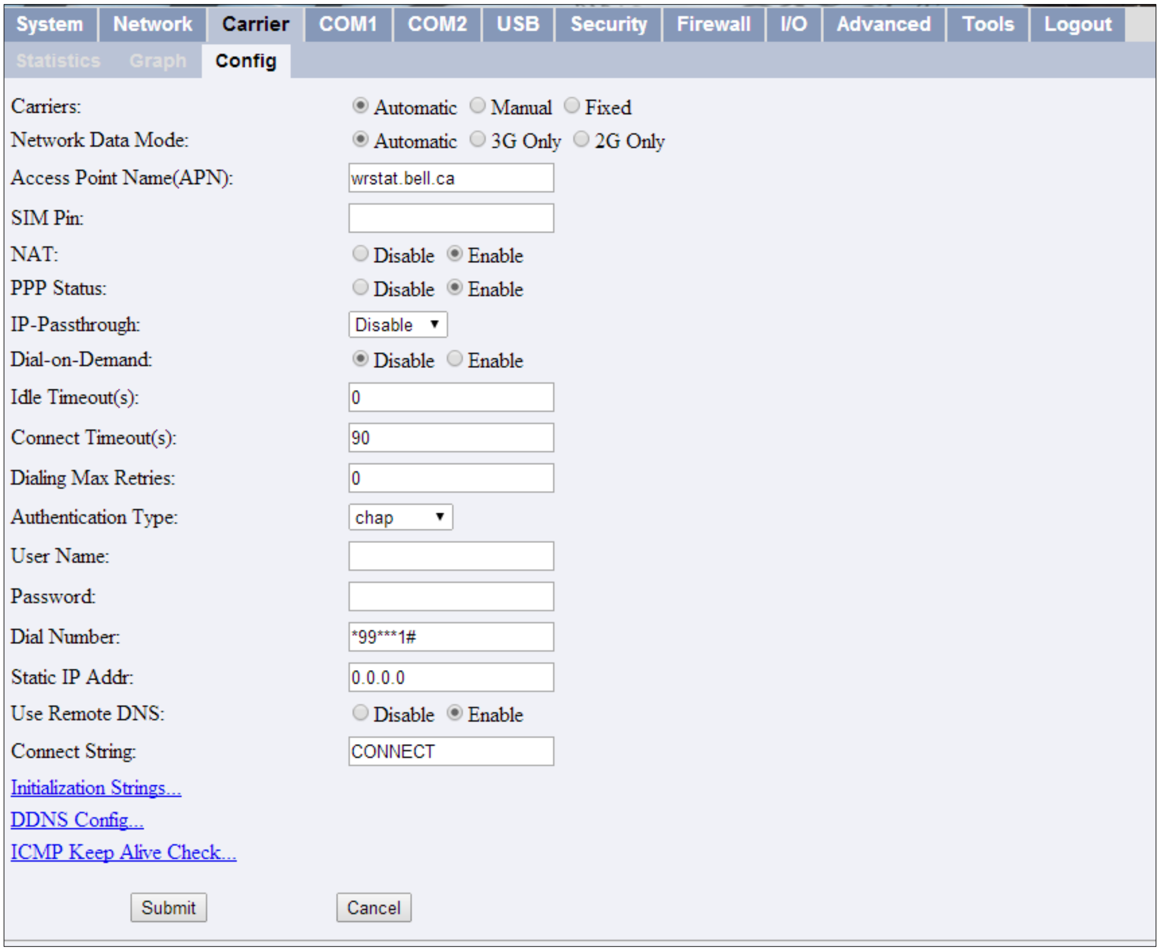
#	day	rx	tx	total	avg. rate
		no data available			

Refresh Interval(s): 10

Image 4-18: Carrier Graph

4.4.3 Carrier Configuration

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.



Carriers:	● Automatic ○ Manual ○ Fixed
Network Data Mode:	● Automatic ○ 3G Only ○ 2G Only
Access Point Name(APN):	wrstat.bell.ca
SIM Pin:	
NAT:	○ Disable ● Enable
PPP Status:	○ Disable ● Enable
IP-Passthrough:	Disable ▾
Dial-on-Demand:	● Disable ○ Enable
Idle Timeout(s):	0
Connect Timeout(s):	90
Dialing Max Retries:	0
Authentication Type:	chap ▾
User Name:	
Password:	
Dial Number:	*99***1#
Static IP Addr:	0.0.0.0
Use Remote DNS:	○ Disable ● Enable
Connect String:	CONNECT

Initialization Strings...
DDNS Config...
ICMP Keep Alive Check...

Image 4-19: Carrier Config

Carriers

This option allows for the automatic detection of available carriers, the manual selection of detected carriers, or the fixed selection of entering a carriers ID. Manual and Fixed are commonly used when the IPn3G is Roaming and it is desirable to control which carrier the unit connects to.

Values (selection)

Automatic
Manual
Fixed

4.0 WebUI Configuration

Carrier ID

In Manual Carrier mode, select the desired carrier from the list of available carriers. In fixed mode, enter the Carrier ID.

Values

Varies

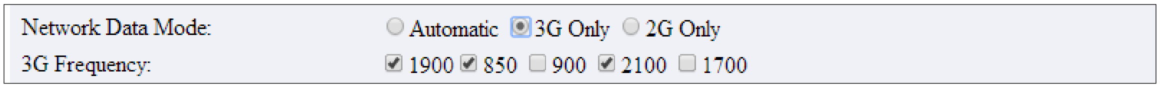
Network Data Mode

When set to Automatic the modem will automatically decide on the best signal to connect to, in some cases this may be 2G. When set to **3G Only,** the modem will continually try to connect to 3G, the same for 2G only.

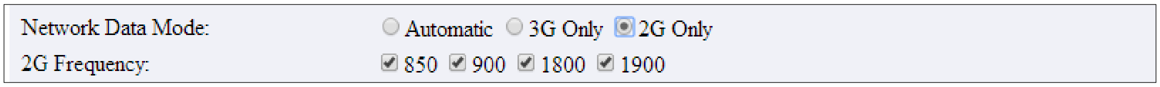
Once set to operate in a specific technology, a user can then select which frequencies within that technology to use. It is recommended to be careful, as if no useable frequency/technology (3G/2G) is available, the modem will not connect.

Values (selection)

Automatic
3G Only
(1900/850/900/2100/1700)
2G Only
(850/900/1800/1900 MHz)



Network Data Mode: ○ Automatic ● 3G Only ○ 2G Only
3G Frequency: ☑ 1900 ☑ 850 □ 900 ☑ 2100 □ 1700



Network Data Mode: ○ Automatic ○ 3G Only ● 2G Only
2G Frequency: ☑ 850 ☑ 900 ☑ 1800 ☑ 1900

Access Point Name (APN)

The (Access Point Name) APN is required and assigned by the wireless carrier. A Carrier will have different APNs for different service types (Static vs Dynamic etc).

Values (String)

Carrier dependant

SIM Pin

It is possible to have a Pin number associated with a SIM card that is required to use the SIM card on a device. If the installed SIM card has been set up with a SIM Pin, enter the number here.

Values (String)

Carrier dependant

NAT (Network Address Translation)

When NAT is enabled internal addresses are not visible to external networks. When disabled the router does not perform any address translation on the packets passing through it.

Values (selection)

Disable / **Enable**

PPP Status

This option allows the operation of PPP.

Values (selection)

Disable / **Enable**

IP-Passthrough

IP pass-through allows the WAN IP address to be assigned to the device connected to the rear Ethernet port on the IPn3G. In this mode the IPn3G is transparent and forwards all traffic to the device connected to the Ethernet port. The WebUI port (Default HTTP Port:**80**), this port is retained for remote management of the IPn3G. This port can be changed to a different port under the **Security > Access** Menu. It is recommended to reboot the IPn3G after changing these settings.

Values (selection)

Disable / Ethernet

Dial-on-Demand

If disabled, the modem will always remain connected. The default is **Disabled**.

Values (selection)

Disable / Enable

Idle Time Out

The maximum amount of time to pass before modem will timeout. The default is **0 seconds.**

Values (seconds)

0-65535

Connect Time Out

The maximum amount of time to wait for a connection The default is **90 seconds.**

Values (seconds)

0-65535

Dialing Max Retries

The maximum amount of attempts to dial and establish a connection. The default is 0, which means that there is no maximum and the modem will keep trying indefinitely.

Values

0-100

Authentication Type

Sets the authentication type required to negotiate with peer.

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

Values (selection)

NoAuth
pap
chap
pap-chap

User Name

User Name as required for authentication to remote peer. May not be required for dynamically assigned IP addresses from the wireless carrier. Usually required for static IP addresses.

Values (char string)

Carrier/peer dependant

Password

Password as required for authentication to remote peer. May not be required for dynamically assigned IP addresses from the wireless carrier. Usually required for static IP addresses.

Values (char string)

Carrier/peer dependant

Dial Number

Sets the number to be dialed. Carrier dependant, the default number is ***99***1#**

Values (String)

*99***1#

Static 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

0.0.0.0

Use Remote DNS

Enabled by default, the IPn3G, will use the DNS server as specified automatically by the service provider.

Values (Selection)

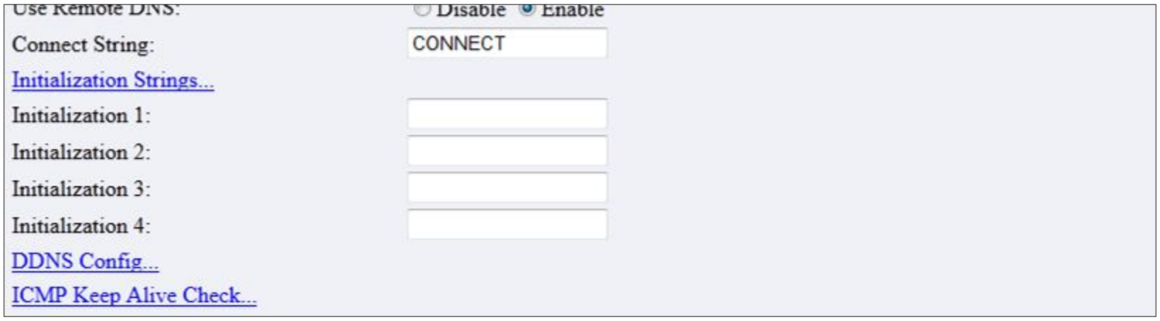
Disable / **Enable**

Connect String

Sets the modems connect string if required by the carrier.

Values (String)

CONNECT



Use Remote DNS: ○ Disable ● Enable

Connect String: CONNECT

Initialization Strings...

Initialization 1:

Initialization 2:

Initialization 3:

Initialization 4:

DDNS Config...

ICMP Keep Alive Check...

Image 4-20: Carrier Configuration Menu, DDNS Config...

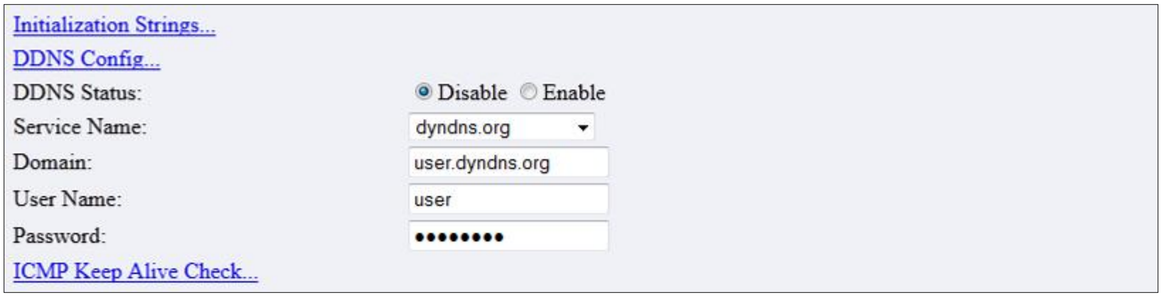
Initialization 1 - 4

The modem can have up to 4 initialization strings.

Values (String)

Init-string

4.0 WebUI Configuration



Initialization Strings...

DDNS Config...

DDNS Status:	● Disable ○ Enable
Service Name:	dyndns.org
Domain:	user.dyndns.org
User Name:	user
Password:	••••••••

ICMP Keep Alive Check...

Image 4-21: Carrier Configuration Menu, DDNS Config...

DDNS Status

This selection allows the use of a Dynamic Domain Name Server (DDNS), for the IPn3G.

Values (Selection)

Disable / Enable

Service Name

Unless a carrier issues a Static IP address, it may be desirable to use a dynamic DNS service to track dynamic IP changes and automatically update DNS services. This allows the use of a constant resolvable host name for the IPn3G.

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)

dyndns.org
changeip.com
zoneedit.com
no-ip.com
noip.com
freedns.afraid.org
dnsmax.com
thatip.com

Domain

This is the host or domain name for the IPn3G as assigned by the DDNS provider.

Values

user.dyndns.org

User Name

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

Values

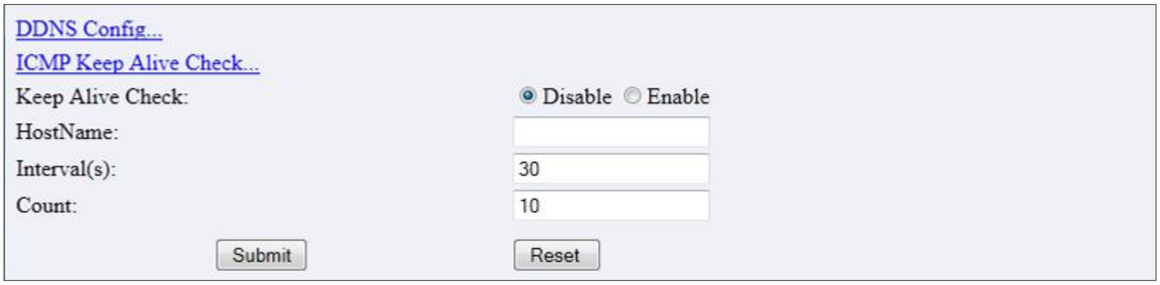
username

Password

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

Values

username



DDNS Config...

ICMP Keep Alive Check...

Keep Alive Check:	● Disable ○ Enable
HostName:	
Interval(s):	30
Count:	10

Image 4-22: Carrier Configuration Menu, ICMP Keep Alive Check...

ICMP Keep Alive Check

This selection allows the use of a ICMP Keep Alive Check for the IPn3G. The default is disabled.

Values (selection)

Disable / Enable

HostName

A user can set up a reachable host (IP or domain) for the unit to ping periodically to keep the WAN connection alive (Wireless Carrier) in case the carrier shuts it down due to lack of activity. PING frequency is defined by the ***Interval***.

Values (IP Address)

IP Address or Name of host for ICMP PING.

Interval

The Interval value determines the frequency, or how often, the IPn3G will send out PING messages to the Host.

Values (seconds)

30

Count

The ***Count*** field is the maximum number of PING errors such as “Host unreachable” the IPn3G will attempt before the unit will reboot itself to attempt to correct connection issues. If set to zero (0), the unit will never reboot itself.

Values

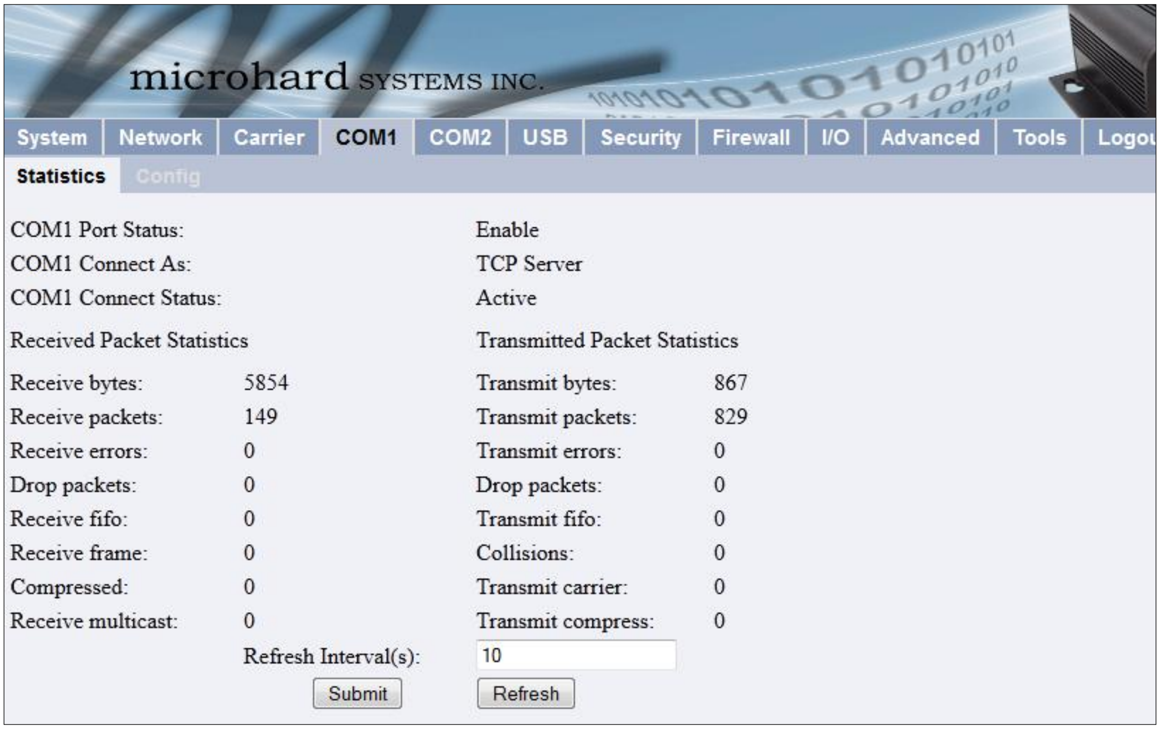
10

4.5 COM1/COM2

4.5.1 COM1/2 > Statistics

This window displays information related to the serial interfaces of the IPn3G.

- COM1/2 Port Status
  Enabled by default. (IF COM2 is disabled it is available as a 'Console' port.)
- COM1/2 Connect As
  Display of chosen protocol with respect to serial gateway function.
- COM1/2 Connect Status
  If port is enabled and there is data traffic, this will display 'Active'.



COM1 Port Status: Enable
COM1 Connect As: TCP Server
COM1 Connect Status: Active

Received Packet Statistics		Transmitted Packet Statistics	
Receive bytes:	5854	Transmit bytes:	867
Receive packets:	149	Transmit packets:	829
Receive errors:	0	Transmit errors:	0
Drop packets:	0	Drop packets:	0
Receive fifo:	0	Transmit fifo:	0
Receive frame:	0	Collisions:	0
Compressed:	0	Transmit carrier:	0
Receive multicast:	0	Transmit compress:	0

Refresh Interval(s): 10

Image 4-23: COM1 Configuration Menu

The other displayed parameters are not all applicable. Of most use are the transmitted and received bytes/packets: these will indicate if data is coming into and out of the COM ports.

4.5.2 COM1 and COM2 Configuration

The menus **’COM1 > Config**’ and **’COM2 > Config**’ are used to configure the serial device server for the serial communications ports:

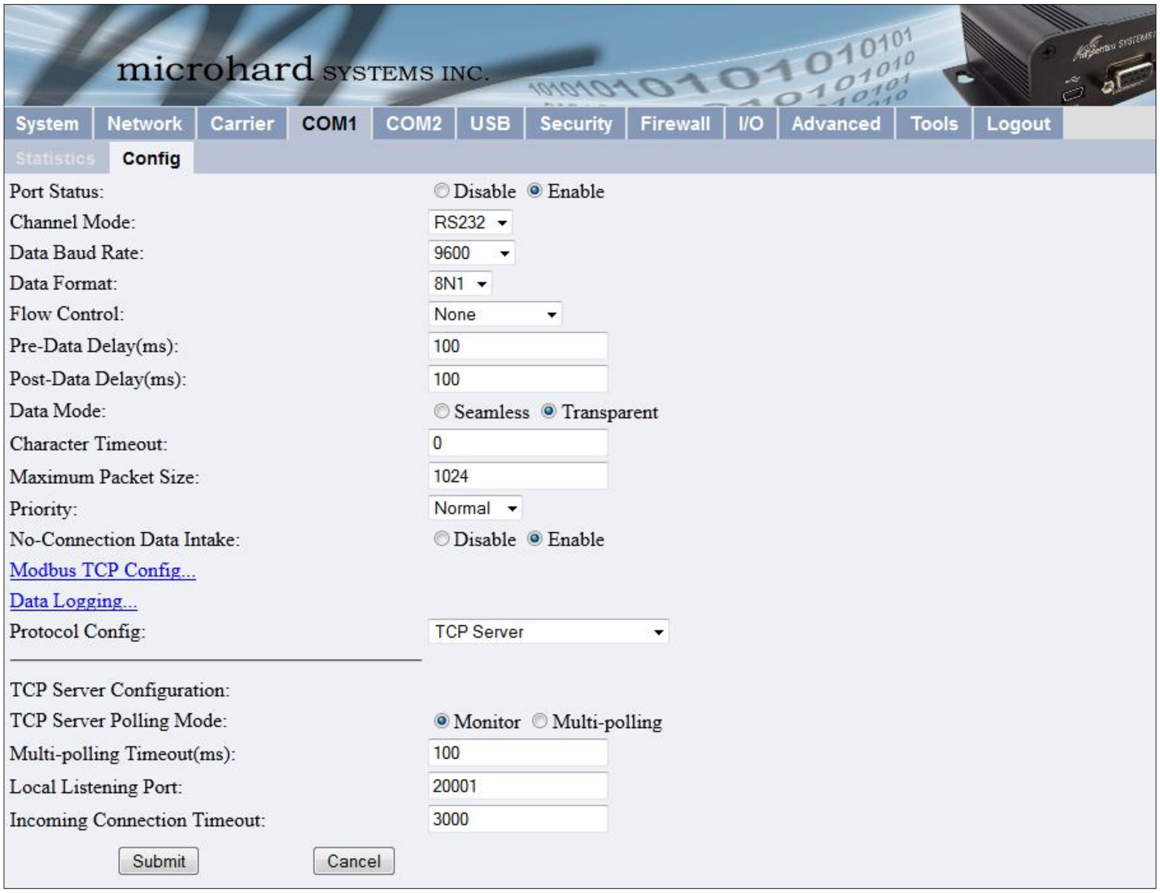
- COM1 (DATA), the rear DE9 connector on the IPn3G, and
- COM2 (DIAGNOSTIC), the front DE9 connector.

Serial device data may be brought into a LAN network through TCP, UDP, or multicast; it may also exit the IPn3G network on another IPn3G ’s serial port. Ensure that the firewall allows access to the assigned ports by either creating rules to allow it, or by setting the WAN Request to allow.

COM1 is a full-featured RS232 interface dedicated to serial data traffic. It supports hardware handshaking. By default, this port is enabled.

COM2 is, by default, disabled. In this state, it may be used as the console port for the text user interface. Enabled, it becomes another serial port for data traffic. It is a 3-wire (TxD, RxD, and SG) interface and does not support hardware handshaking.

For brevity, only COM1 is fully detailed in this section; the relative limitations of COM2 are noted where applicable.



Port Status:	○ Disable ● Enable
Channel Mode:	RS232
Data Baud Rate:	9600
Data Format:	8N1
Flow Control:	None
Pre-Data Delay(ms):	100
Post-Data Delay(ms):	100
Data Mode:	○ Seamless ● Transparent
Character Timeout:	0
Maximum Packet Size:	1024
Priority:	Normal
No-Connection Data Intake:	○ Disable ● Enable
Modbus TCP Config...	
Data Logging...	
Protocol Config:	TCP Server
TCP Server Configuration:	
TCP Server Polling Mode:	● Monitor ○ Multi-polling
Multi-polling Timeout(ms):	100
Local Listening Port:	20001
Incoming Connection Timeout:	3000

Image 4-24: COM1 Configuration Menu

Port Status

Select operational status of port. Enabled by default.

*COM2 is Disabled by default. If COM2 is Enabled and there is a desire to switch it back to Disabled (console mode) via the serial connection to it, the escape sequence of '**+++**' may be entered at the Data Baud Rate for which the port is configured.

Values

Enable
Disable

Channel Mode

Determines which (rear of unit) serial interface shall be used to connect to external devices: RS232, RS485, or RS422. This option applies only to COM1 / DATA. When an interface other than RS232 is selected, the DE9 port will be inactive.

Values

RS232 / RS485 / RS422

Data Baud Rate

The serial baud rate is the rate at which the modem is to communicate with the attached local asynchronous device.
*COM2 data baud rate maximum is 115200bps.

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

Values (bits per second (bps))

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

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

8N1
8N2
8E1
8O1
7N1
7N2
7E1
7O1
7E2
7O2

Flow Control

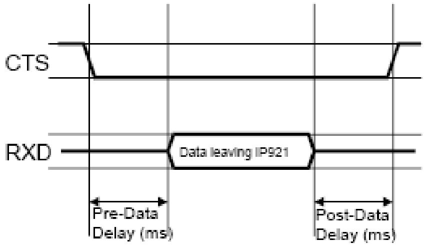
Flow control may be used to enhance the reliability of serial data communications, particularly at higher baud rates. If the attached device does not support hardware handshaking, leave this setting at the default value of 'None'.

When CTS Framing is selected, the IPn3G uses the CTS signal to gate the output data on the serial port. Figure 3A below illustrates the timing of framed output data.
*COM2 does not support Flow Control.

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

Values

None / Hardware / CTS Framing



Drawing 4A: CTS Output Data Framing

Pre-Data Delay (ms)

Refer to ***Drawing 3A.***
*COM2 does not support this function.

Values (ms)

100

Post-Data Delay (ms)

Refer to ***Drawing 3A.***
*COM2 does not support this function.

Values (ms)

100

Data Mode

This setting defines the serial output data framing. In **Transparent** mode (default), the received data will be output promptly from the IPn3G. When set to **Seamless**, the serial port server will add a gap between data frames to comply with the MODBUS protocol for example.

Values

Seamless
Transparent

Character Timeout

In Seamless mode (see Data Mode), 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

4

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)

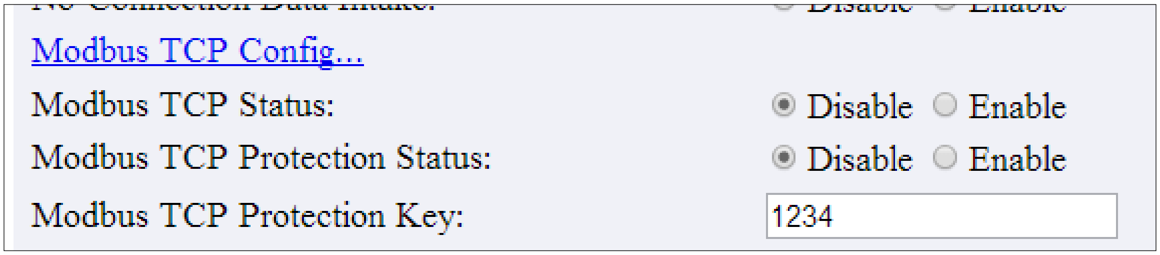
1024

Priority

This setting effects the Quality of Service (QoS) associated with the data traffic on the specific COM port.

Values

Normal
Medium
High



No-Connection Data Intake: ○ Disable ○ Enable

Modbus TCP Config...

Modbus TCP Status: ● Disable ○ Enable

Modbus TCP Protection Status: ● Disable ○ Enable

Modbus TCP Protection Key: 1234

Image 4-25: COM1 Modbus Config

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 IPn4G 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

The field allows the Modbus TCP Protection Status flag to be enabled or disabled. If enabled the Modbus data will be encrypted with the Modbus Protection Key.

Values (IP Address)

Disable
Enable

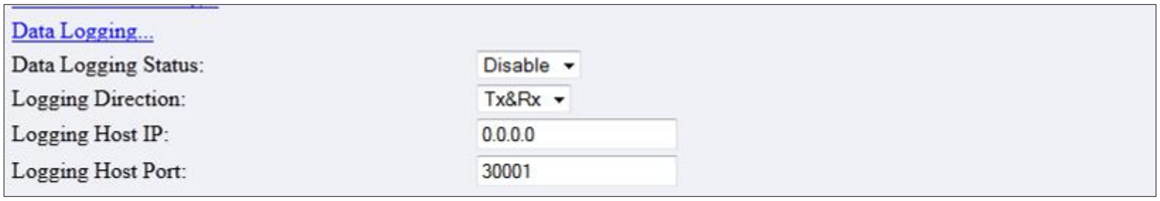
Modbus TCP Protection Key

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

Values (UDP Port)

1234

4.0 WebUI Configuration



Data Logging...

Data Logging Status: Disable

Logging Direction: Tx&Rx

Logging Host IP: 0.0.0.0

Logging Host Port: 30001

Image 4-26: COM1 Data Logging

Data Logging Status

Data Logging on the COM ports allows for the actual serial port data to be sent to a remote host. This data can be in the Raw form or converted to Hex before it is sent.

Values (selection)

Disable
Raw
Hex

Logging Direction

Select Tx&Rx to log data to/from the serial port. Select Tx to log data that is being transmitted from the serial port, and Rx to log data being received at the serial port.

Values (selection)

Tx&Rx
Tx
Rx

Logging Host IP

Enter the IP Address of the where the logging data is to be sent. Generally this is a PC listening on the specified UDP port.

Values (IP Address)

0.0.0.0

Logging Host Port

Enter the UDP port of the IP Address where the data is to be sent.

Values (UDP Port)

30001

The protocol selected in the Protocol Config field will determine which configuration options appear in the remainder of the COM*n* Configuration Menu.

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.

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.

Protocol Config

This setting determines which protocol the serial server will use to transmit serial port data over the IP Series network. Ensure that the firewall allows access to the assigned ports by either creating rules to allow it, or by setting the WAN Request to allow.

TCP Client: When TCP Client is selected and data is received on its serial port, the IPn3G takes the initiative to find and connect to a remote TCP server. The TCP session is terminated by this same unit when the data exchange session is completed and the connection timeout has expired. If a TCP connection cannot be established, the serial port data is discarded.

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

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

- Outgoing Connection Timeout
  This parameter determines when the IPn3G 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 IPn3G will not INITIATE a session, rather, it will wait for a Client to request a session of it (it's being the Server—it 'serves' a Client). The unit will 'listen' on a specific TCP port. If a session is established, data will flow from the Client to the Server, and, if present, from the Server to the Client. If a session is not established, both Client-side serial data, and Server-side serial data , if present, will be discarded.

- Local Listening Port
  The TCP port which the Server listens to. It allows a TCP connection to be created by a TCP Client to carry serial port data.
  Default: **20001**
- Incoming Connection Timeout
  Established when the TCP Server will terminate the TCP connection is the connection is in an idle state.
  Default: **300** (seconds)

TCP Client/Server: In this mode, the IPn3G 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.

Protocol Config (continued)

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.

UDP Point-to-Point: In this configuration the IPn3G will send serial data to a specifically-defined point, using UDP packets. This same IPn3G will accept UDP packets from that same point.

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

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

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

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.

UDP Point-to-Multipoint (P): This mode is configured on an IPn3G which is to send multicast UDP packets; typically, the MASTER in the IPn3G network.

- Multicast IP Address
  A valid multicast address this unit uses to send multicast UDP packets upon receiving data from the serial port. The default value is a good example of a valid multicast address.
  Default: **224.1.1.1**

- Multicast Port
  A UDP port that this IPn3G will send UDP packets to. The Multipoint (MP - see the UDP Point-to-Multipoint (MP) description) stations should be configured to listen to this point in order to receive multicast packets from this IPn3G.
  Default: **20001**

- Listening Port
  The UDP port that this unit receives incoming data on from multiple remote units.
  Default: **20011**

- Time to Live
  Time to live for the multicast packets.
  Default: **1** (hop)

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.

UDP Point-to-Multipoint (MP): This protocol is selected on the units which are to receive multicast UDP packets, typically the Remote units. See the previous description of UDP Point-to-Multipoint (P).

- Remote IP Address
  The IP address of a distant device (IP Series or, for example, a PC) to which the unit sends UDP packets of data received on the serial port. Most often this is the IP address of the Master IP Series.
  Default: **0.0.0.0**

- Remote Port
  The UDP port associated with the Remote IP Address (above). In the case of this 'Remote' being the Master IPn3G, the value in this field should match the Listening Port of the Master (see UDP Point-to-Multipoint (P)).
  Default: **20011**

Protocol Config (continued)

In a Point-to-Multipoint (PMP) network topology which is to utilize UDP multicast, typically the MASTER would be configured as '(P)' (the POINT) and the REMOTES would be configured as '(MP)' (the MULTIPOINTS).

- Multicast IP Address

  A valid MULTICAST address that this unit will use to receive multicast UDP packets sent by a UDP Point-to-Multipoint (P) unit. Note that the default value for this field matches the default Multicast IP Address of the UDP Point-to-Multipoint (P) configuration described on the previous page.
  Default: **224.1.1.1**

- Multicast Port

  The UDP port that this unit will use, along with the Multicast IP Address detailed above, to receive the multicast UDP packets sent by the UDP Point-to-Multipoint (P) unit.
  Default: **20001**

UDP Multipoint-to-Multipoint

- Multicast IP Address

  A valid multicast address the unit will use to send multicast UDP packets upon receiving them at its serial port.
  Default: **224.1.1.1**

- Multicast Port

  UDP port that the packets are sent to. Multipoint stations should be configured to listen to this port in order to receive multicast packets.
  Default: **20011**

- Time to Live

  Time to live for the multicast packets.
  Default: **1** (hop)

- Listening Multicast IP Address

  A valid multicast address the unit is to listen to receive multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.
  Default: **224.1.1.1**

- Listening Multicast Port

  UDP port that the unit will listen to for multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.
  Default: **20011**

Protocol Config (continued)

SMTP Client: If the IPn3G network 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. Note: COM2 does not support this mode.

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

- 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**
- Username / Password
  The username/password of the email account being used, if authentication is required for outgoing email.
  Default: ***varies/varies***
- Mail Recipient
  A valid e-mail address for the intended addressee, entered in the proper format.
  Default: **host@**
- Message Max Size
  Maximum size for the e-mail message.
  Default: **1024**
- Timeout (s)
  How long the unit will wait to gather data from the serial port before sending an e-mail message; data will be sent immediately upon reaching Message Max Size.
  Default: **10**
- Transfer Mode
  Select how the data received on COM1 is to be sent to the email addressee. Options are: Text, Attached File, Hex Code.
  Default: **Text**

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 IPn3G. Note: COM2 does not support this mode.

- PPP Local IP
  Enter the local PPP IP Address, the IP Address of the IPn3G COM1 Port.
  Default: **192.168.0.1**

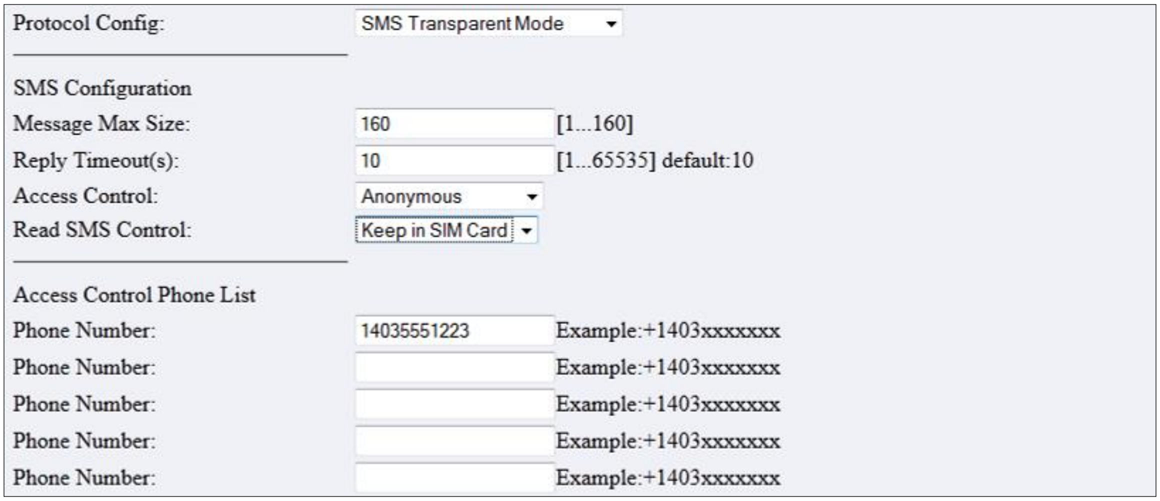
- PPP Host IP
  Enter the PPP Host IP here. This is the IP of the PC or attached device.
  Default: **192.168.0.99**

- PPP Idle Timeout(s)
  Enter the desired PPP Idle Timeout in seconds.
  Default: **30**

4.0 WebUI Configuration

Protocol Config (continued)

SMS Transparent Mode: Serial data from the COM1 port can be send to one or multiple destinations via SMS text messaging. SMS messages received by the IPn3G can also be sent to the COM1 port.



Protocol Config:	SMS Transparent Mode	
SMS Configuration		
Message Max Size:	160	[1...160]
Reply Timeout(s):	10	[1...65535] default:10
Access Control:	Anonymous	
Read SMS Control:	Keep in SIM Card	
Access Control Phone List		
Phone Number:	14035551223	Example:+1403xxxxxxx
Phone Number:		Example:+1403xxxxxxx
Phone Number:		Example:+1403xxxxxxx
Phone Number:		Example:+1403xxxxxxx
Phone Number:		Example:+1403xxxxxxx

Image 4-27: COM > SMS Transparent Mode

- Message Max Size
  Enter the maximum message size. Once the number of characters has been reached the IPn3G will package the data up and send it as a SMS message to the number(s) specified. [1….160]. The character timeout can be used to send messages more frequently by detecting a pause in the incoming data.
  Default: **160**

- Reply Timeout(s)
  Enter a value for the Reply Timeout.
  Default: **10**

- Access Control
  By selecting **Anonymous,** the IPn3G will accept a SMS message from any number. If **Control Phone List** is selected, only messages from the numbers in the Access Control List will be accepted.
  Default: **Anonymous**

- Read SMS Control
  Select **Keep in SIM Card** to save incoming SMS messages in the SIM card, select **Delete** to delete messages once they have been output to serial port.
  Default: **Keep in SIM Card**

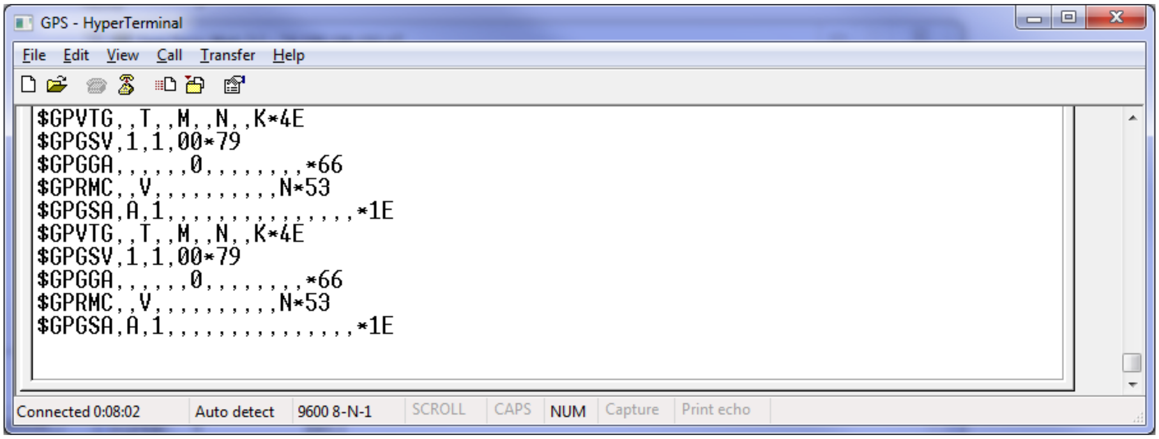
- Access Control Phone List
  Messages can be sent to up to five (5) numbers, also, this list can be used to filter incoming

Protocol Config (continued)

SMS AT Mode: When set to SMS AT Mode, the serial port accepts the SMS AT subset of the AT Command Set. Only SMS AT Commands are available. For more detailed information about specific commands, refer to the **Section 5: AT Commands**. The following commands are available on the COM1 serial port:

- AT+CMGR - Read Message
- AT+CMGL - List Message
- AT+CMGD - Delete Message
- AT+CMGS - Send SM to Network
- AT+CGMI - Request Manufacturer ID
- AT+CGMM - Request Model ID
- AT+CGMR - Request Revision
- AT+CSQ - Signal Strength
- AT+MMGR - Read Message (Does not change Status)
- AT+MMGL - List Message (Does not change Status)
- AT+CMFG - Message Format
- AT+CCLK - Read System Date and Time
- AT+CSCA - Service Center Address
- AT+CREG - Network Registration Status
- AT+CNMI - New Message Indications to Terminal
- AT+CMTI - Stored SMS-DELIVER Indication Unsolicited Response

GPS Transparent Mode: When in GPS Transparent Mode, GPS data is reported out of the serial port. Sample output is shown below:



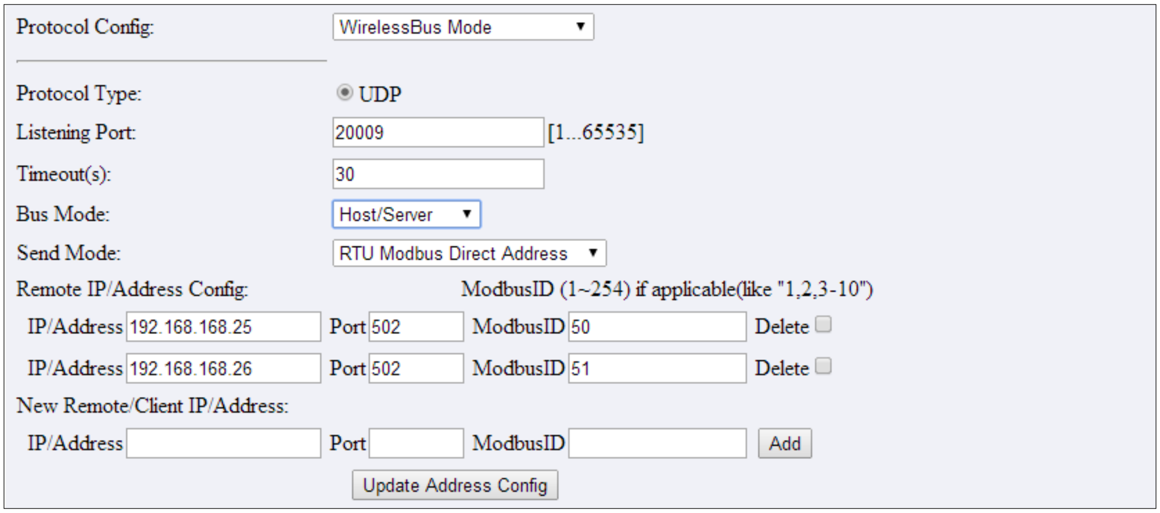
```
$GPVTG,,T,,M,,N,,K*4E
$GPGSV,1,1,00*79
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,,N*53
$GPGSA,A,1,,,,,,,,,,,,,,,*1E
$GPVTG,,T,,M,,N,,K*4E
$GPGSV,1,1,00*79
$GPGGA,,,,,,0,,,,,,,,*66
$GPRMC,,V,,,,,,,,,,N*53
$GPGSA,A,1,,,,,,,,,,,,,,,*1E
```

Connected 0:08:02 | Auto detect | 9600 8-N-1 | SCROLL | CAPS | NUM | Capture | Print echo

Image 4-28: COM > GPS Transparent Mode

Protocol Config (continued)

WirelessBus Mode: WirelessBus Mode can be used in systems where serial based polled SCADA systems such as Modbus have one master/host and multiple remote/slave RTU/PLC's located at several different locations. The IPn3G that is connected to the Master is provided a list of IP Addresses/ports of IPn3G's that are connected to each of the remotes. Several Modbus (or other serial based protocols), can be connected to each of the remote IPn3G's (Using RS485 for multi-drop etc). WirelessBus Mode supports Modbus RTU, and Modbus ASCII modes, as well as other protocols using broadcast mode.



Protocol Config: WirelessBus Mode ▼

Protocol Type: ● UDP

Listening Port: 20009 [1...65535]

Timeout(s): 30

Bus Mode: Host/Server ▼

Send Mode: RTU Modbus Direct Address ▼

Remote IP/Address Config: ModbusID (1~254) if applicable(like "1,2,3-10")

IP/Address 192.168.168.25 Port 502 ModbusID 50 Delete □

IP/Address 192.168.168.26 Port 502 ModbusID 51 Delete □

New Remote/Client IP/Address:

IP/Address Port ModbusID

Image 4-29: COM1 > Wireless Bus Mode (Host/Server)

WirelessBus Mode uses UDP packets to communicate between the Host and the Remotes. When a IPn3G is configured as a Host/Server it retains a list of ModbusID's and the respective IP/Port information required to communicate with any remotes. When a Modbus poll is received by the IPn3G it looks at the Modbus ID, then assembles a UDP packet to be sent to the corresponding IP/Port listed in the table. At the remote side, the packet is disassembled and sent out the remote serial port as original serial data.

Listening Port

This is the UDP port used by the IPn3G configured as a Host/Server to listen for incoming traffic from remote devices using the WirelessBus mode and set as Remote/Clients.

Values (UDP)

20009

Timeout

The IPn3G features a configurable timeout. This timeout checks to ensure the specified port is open and ready.

Values (seconds)

30

Bus Mode

When set to Remote/Client, and data received on the serial port will automatically be encapsulated into an UDP packet and sent to the configured host IP. When set to Host/Server the IPn3G will encapsulate data received on the serial port into a UDP packet and send to the applicable IP addresses/Ports listed.

Values (selection)

Remote/Client
Host/Server

4.0 WebUI Configuration

Protocol Config (continued)

Send Mode

When configured as Host/Server Bus Mode, this option will allow a user to select between Modbus RTU, Modbus ASCII, or as Broadcast (for other protocols. When set to broadcast the IPn3G will send any incoming serial data to all the IP/Port numbers listed. When in either Modbus mode the IPn3G will only send to the IP/Port that matches the Modbus ID.

Values (selection)

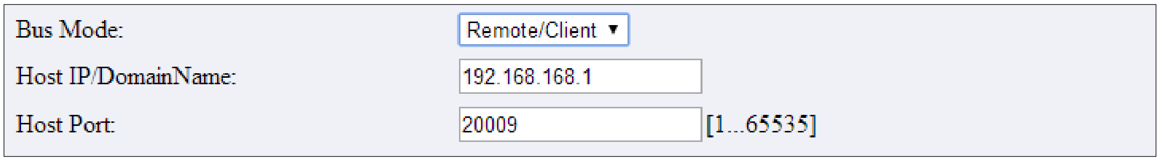
RTU Modbus Direct Access
ASCII Modbus Direct Access
Broadcast For Any Protocol

Remote IP/ Adress Config

For each remote IPn3G enter the reachable IP address and configured UDP port configured for serial data. The ModbusID is not required when in broadcast mode for polled protocols other than Modbus.

Values (UDP)

IP Address (required)
Port (UDP Port #)
ModbusID (if applicable)



Bus Mode:	Remote/Client ▼
Host IP/DomainName:	192.168.168.1
Host Port:	20009 [1...65535]

Image 4-30: COM1 > Wireless Bus Mode (Remote/Client)

Host IP/Domain Name

When the Bus Mode is configured for Remote/Client, enter the IP address or domain address where the Host/Server is located.

Values (IP/Domain)

192.168.168.1

Host Port

Enter the UDP port number configured on the Host/Server where the WirelessBus service is listening. By default this is configured as 20009 on the Host/Server.

Values (UDP Port)

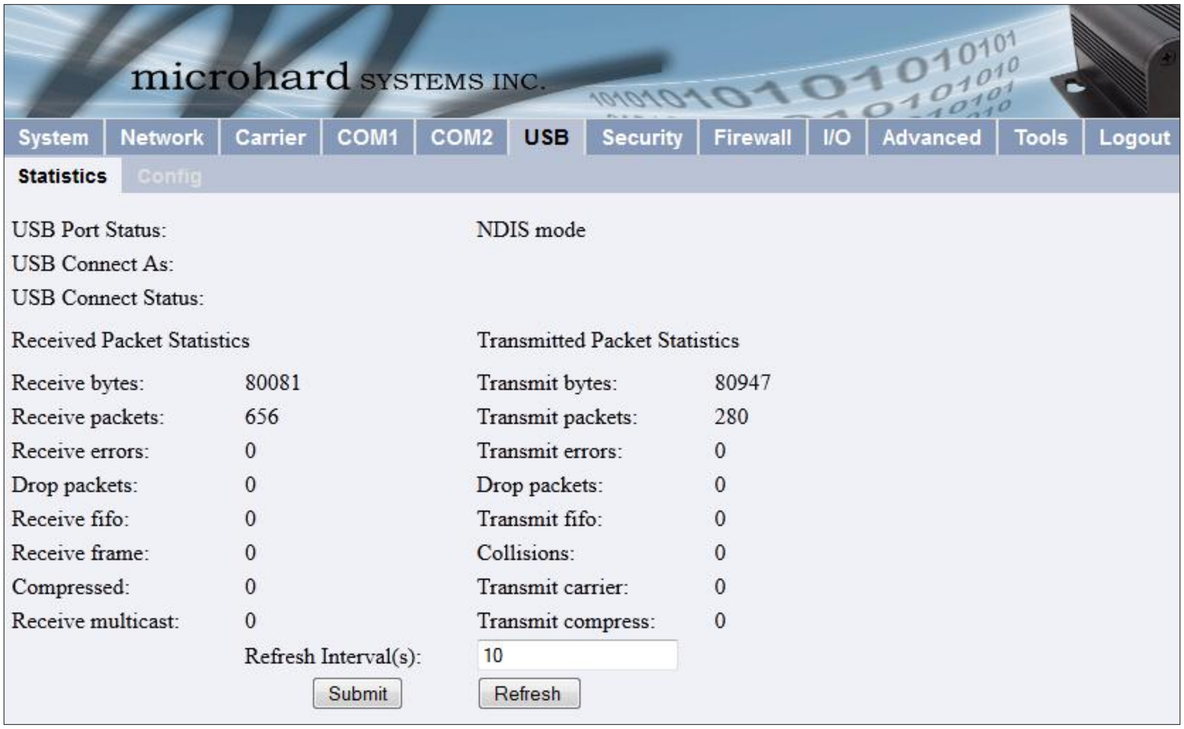
20009

4.6 USB

4.6.1 USB > Statistics

This window displays information related to the USB port located on the front of the IPn3G.

- USB Port Status
  Displays the status of the USB Port.
  Configure via USB Configuration menu.
- USB Connect As
  Display of chosen protocol with respect to serial gateway function.
  Configure via USB Configuration menu.
- USB Connect Status
  If port is enabled and there is data traffic, this will display 'Active'.



USB Port Status:		NDIS mode	
USB Connect As:			
USB Connect Status:			
Received Packet Statistics		Transmitted Packet Statistics	
Receive bytes:	80081	Transmit bytes:	80947
Receive packets:	656	Transmit packets:	280
Receive errors:	0	Transmit errors:	0
Drop packets:	0	Drop packets:	0
Receive fifo:	0	Transmit fifo:	0
Receive frame:	0	Collisions:	0
Compressed:	0	Transmit carrier:	0
Receive multicast:	0	Transmit compress:	0
	Refresh Interval(s):	10	

Image 4-29: USB > Statistics

The other displayed parameters are not all applicable. Of most use are the transmitted and received bytes/ packets: these will indicate if data is coming into and out of the USB port.

4.6.2 USB > Config

The USB Device Port Mode allows a user to define the operation of the IPn3G 's USB Port. The port can be configured to be used as any one of the following:

Console Mode Provides support for the USB-to-Serial console port. In this case, Mini USB port can be used as a USB-to-Serial console port for the text user interface.

Data Mode Provides support for the USB-to-Serial port. Mini USB port can be used as a RS232 interface dedicated to serial data traffic.

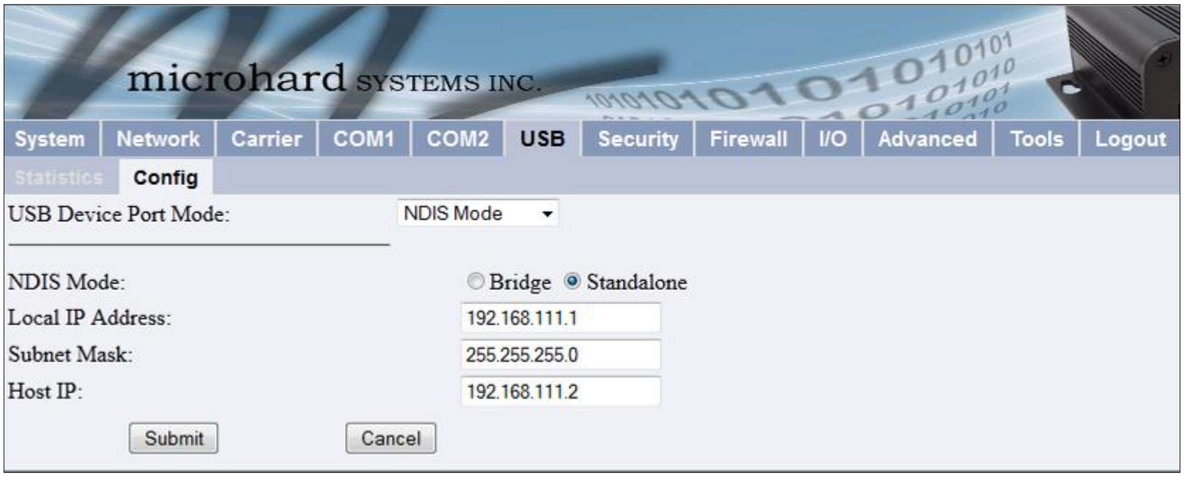
NDIS Mode The USB port can be used as a network interface card. The IPn3G USB port is configured by default in NDIS Standalone Ethernet Mode with a DHCP server running in the background.

This means that a user can use the USB port communicate with the IPn3G via Ethernet on the USB port of their PC's.

Windows Drivers are available from the Support Desk on the Microhard Systems Inc website.

Please register and login into:

http://www.microhardcorp.com/support



USB Device Port Mode: NDIS Mode

NDIS Mode: ○ Bridge ● Standalone

Local IP Address: 192.168.111.1

Subnet Mask: 255.255.255.0

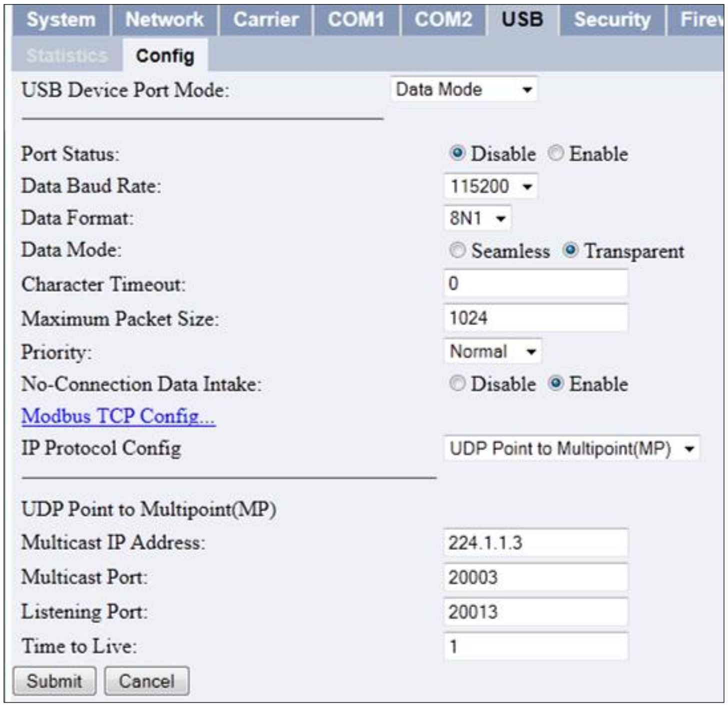
Host IP: 192.168.111.2

Image 4-30: USB Configuration Menu

USB Device Port Mode

Console Mode:
When the USB port in configured as Console Mode, the port acts as a console port.

Data Mode:
USB Data Mode is Disabled by default. If USB Data Mode is selected and there is a desire to switch it back to Disabled (console mode) via the USB-to-Serial connection to it, the escape sequence of '+++' may be entered at the Data Baud Rate for which the port is configured.



USB Device Port Mode: Data Mode

Port Status: ● Disable ○ Enable
Data Baud Rate: 115200
Data Format: 8N1
Data Mode: ○ Seamless ● Transparent
Character Timeout: 0
Maximum Packet Size: 1024
Priority: Normal
No-Connection Data Intake: ○ Disable ● Enable
Modbus TCP Config...
IP Protocol Config: UDP Point to Multipoint(MP)

UDP Point to Multipoint(MP)
Multicast IP Address: 224.1.1.3
Multicast Port: 20003
Listening Port: 20013
Time to Live: 1

Image 4-31: USB Configuration Data Port

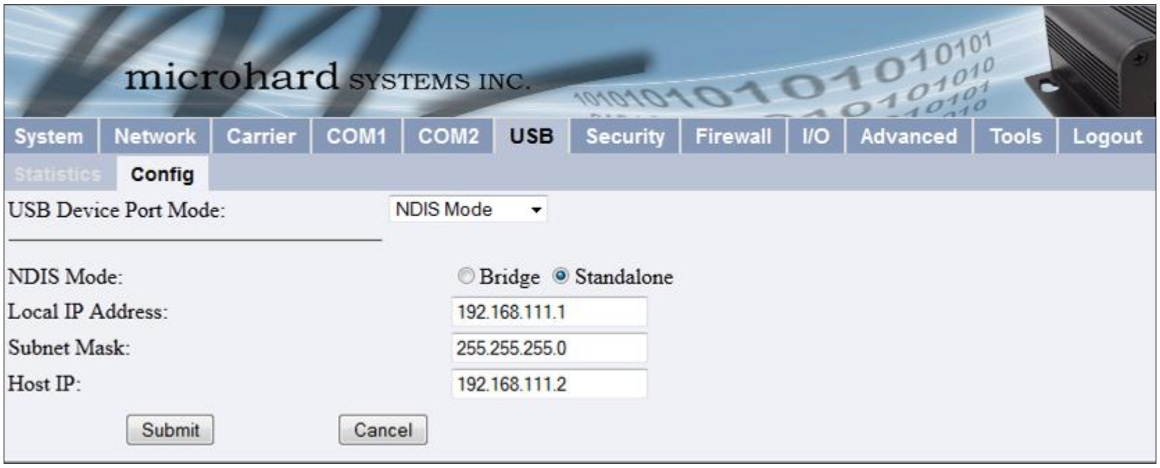
For more information about any of the Data Port field parameters refer to **COM1/COM2 Configuration.**

Values

Console Mode
Data Mode
NDIS Mode

USB Device Port Mode (Continued)

NDIS Mode:
NDIS Standalone Mode is **enabled** by default. This setting will allow the USB port to act as a network interface card.



USB Device Port Mode: NDIS Mode

NDIS Mode: ○ Bridge ● Standalone
Local IP Address: 192.168.111.1
Subnet Mask: 255.255.255.0
Host IP: 192.168.111.2

Image 4-32: USB NDIS Network Configuration

NDIS Mode

In standalone Mode the USB port will act as a separate NIC for the IPn3G. In Bridge Mode the USB port wil use the same settings as the rear ethernet port.

Values (selection)

Bridge / **Standalone**

Local IP Address

This is the IP Address of the USB NDIS adapter on the IPn3G. The IPn3G acts as a DHCP server on this port and assigns an IP address to connecting devices, i.e your PC.

Values

192.168.111.1

Subnet Mask

Enter a valid subnet for the USB NIC.

Values

255.255.255.0

Host IP

Enter a valid host IP for the USB NIC.

Values

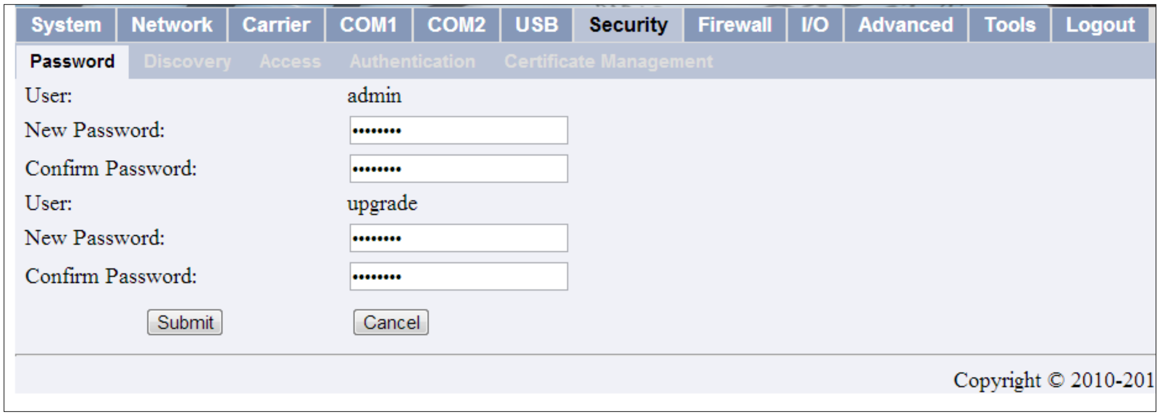
192.168.111.2

4.0 WebUI Configuration

4.7 Security

For best practices and to control unwanted access it is critical that any passwords not be left at the default values.

4.7.1 Security > Password



User: admin
New Password: ••••••••
Confirm Password: ••••••••
User: upgrade
New Password: ••••••••
Confirm Password: ••••••••

Copyright © 2010-201

Image 4-33: Security > Password Configuration Menu

To keep a system secure, the Administrator Password (which is prompted-for at the LogOn window, Console, and Telnet sessions) should be modified rather than retaining the factory default value of 'admin'.

The Upgrade Password protects the IPn3G from having firmware upgrade performed via FTP by an unauthorized person. It is recommended that the default password be changed when the system is deployed.

New Password/Repeat Password (admin)

Enter a new password for the Admin user. Repeat to ensure the intended password was entered and that it was entered correctly. Do not forget the admin password as, if lost, it cannot be recovered.

Values (char string)

admin

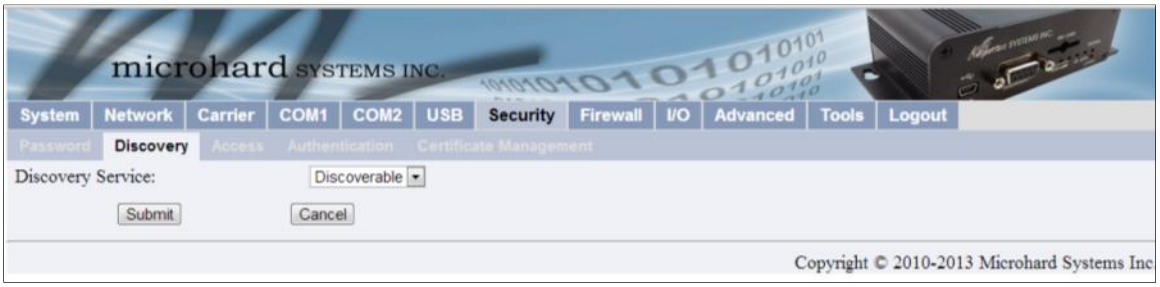
New Password/Repeat Password (upgrade)

Enter a new password for the Upgrade user. Repeat to ensure the intended password was entered and that it was entered correctly.

Values (char string)

admin

4.7.2 Security > Discovery



Discovery Service: Discoverable

Copyright © 2010-2013 Microhard Systems Inc

Image 4-34: Security Config. Menu, Discovery Service Config. Submenu

Discovery Service

Allows, or disables use of the DiscoverIP utility. The discover IP utility allows a user to scan a network for all available IPn3G units, and displays the MAC and IP addresses as well as the unit description. The port used for Discovery is 20077.

Values (selection)

Disable
Discoverable
Changeable

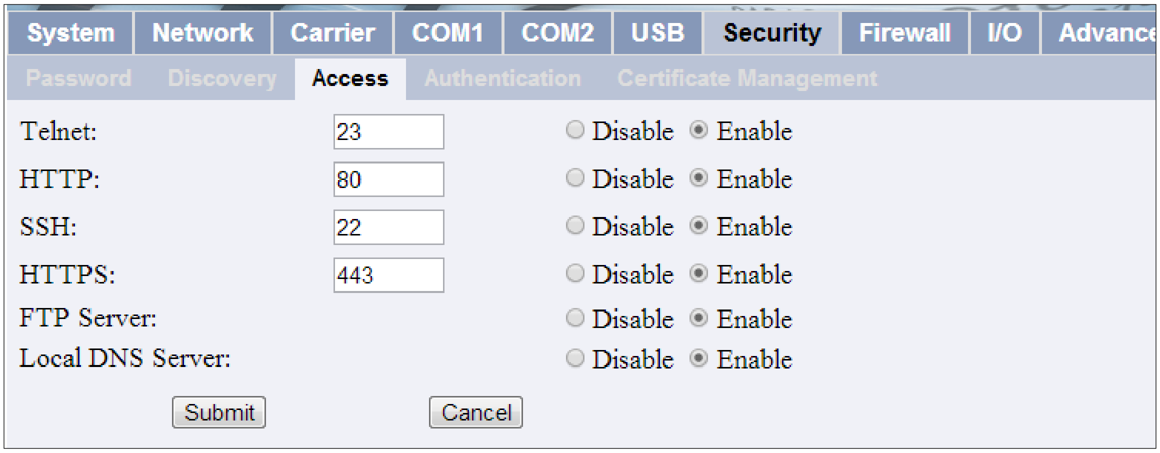
Telnet: A user command which uses the TCP/IP protocol to access a remote device.

Format, from DOS prompt:
>telnet 192.168.1.50
where the IP address is that of the target device.

If the above IP address is that of an IPn3G accessible via the network, the user will arrive at the unit's LogOn window.

HTTP: HyperText Transfer Protocol. The standard protocol for transferring data between a Web server and a Web browser.

4.7.3 Security > Access



Telnet:	23	○ Disable ● Enable
HTTP:	80	○ Disable ● Enable
SSH:	22	○ Disable ● Enable
HTTPS:	443	○ Disable ● Enable
FTP Server:		○ Disable ● Enable
Local DNS Server:		○ Disable ● Enable

Image 4-35: Security Config. Menu, UI Access Config. Submenu

Access

User Interface (UI) Access Configuration allows the port configuration of access services in the IPn3G, the default ports are shown below.

- Telnet (23)
- HTTP (80)
- SSH (22)
- HTTPS (443)

It is also possible to disable the **FTP Server**, and the **Local DNS Server**.

Values (selection)

Disable / **Enable**

SSH & HTTPS: Must be specified at the time of order and enabled via the factory. Once enabled, the options can be set.

4.7.4 Security > Authentication

There are two methods whereby a user may be authenticated for access to the IPn3G:

- Local

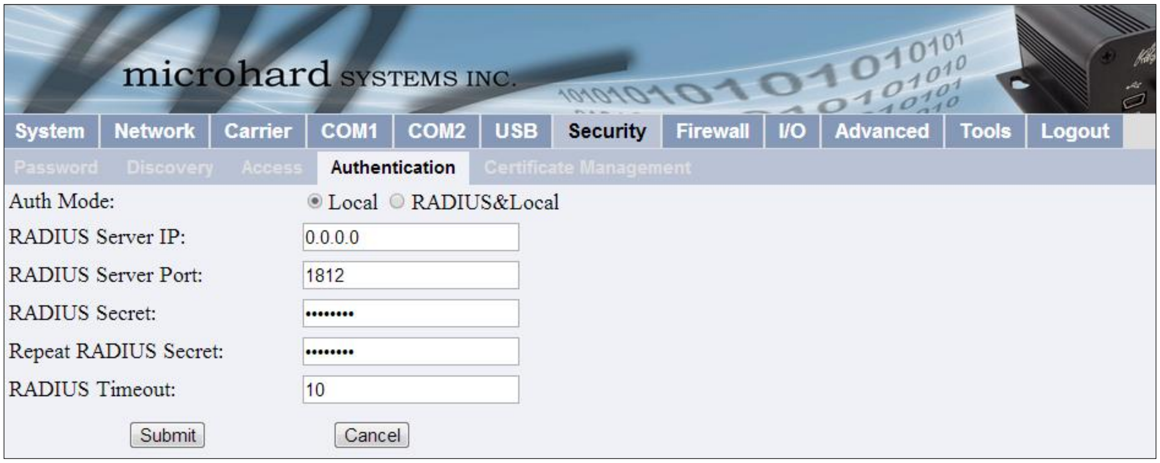
  Using the Admin or Upgrade access and associated passwords - the authentication is done ‘locally’ within the IPn3G, and

- 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.



Auth Mode: ● Local ○ RADIUS&Local

RADIUS Server IP: 0.0.0.0

RADIUS Server Port: 1812

RADIUS Secret: ••••••••

Repeat RADIUS Secret: ••••••••

RADIUS Timeout: 10

Image 4-36: Security Config. Menu, Authentication Config. Submenu

Auth Mode

Select the Authentication Mode: Local (default) or RADIUS&Local. For the latter selection, RADIUS authentication must be attempted FIRST; if unsuccessful, THEN Local authentication may be attempted.

Values

Local
RADIUS&Local

RADIUS Server IP

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 Server Port

In this field, the applicable Port number for the RADIUS Server is to be entered if RADIUS&Local has been selected as the Authorization Mode.

Normally, a RADIUS Server uses Port 1812 for the authentication function.

Values

Applicable RADIUS Server Port number

1812

RADIUS Secret

If the IP Series’ 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, and the following field. (You will also want to obtain the applicable RADIUS User Name from your RADIUS Server Administrator.)

Values

Specific RADIUS Server secret

nosecret

Repeat RADIUS Secret

See above. Re-enter RADIUS Secret in this field.

Values

Specific RADIUS Server secret

nosecret

RADIUS Timeout

Amount of time to wait for RADIUS authentication.

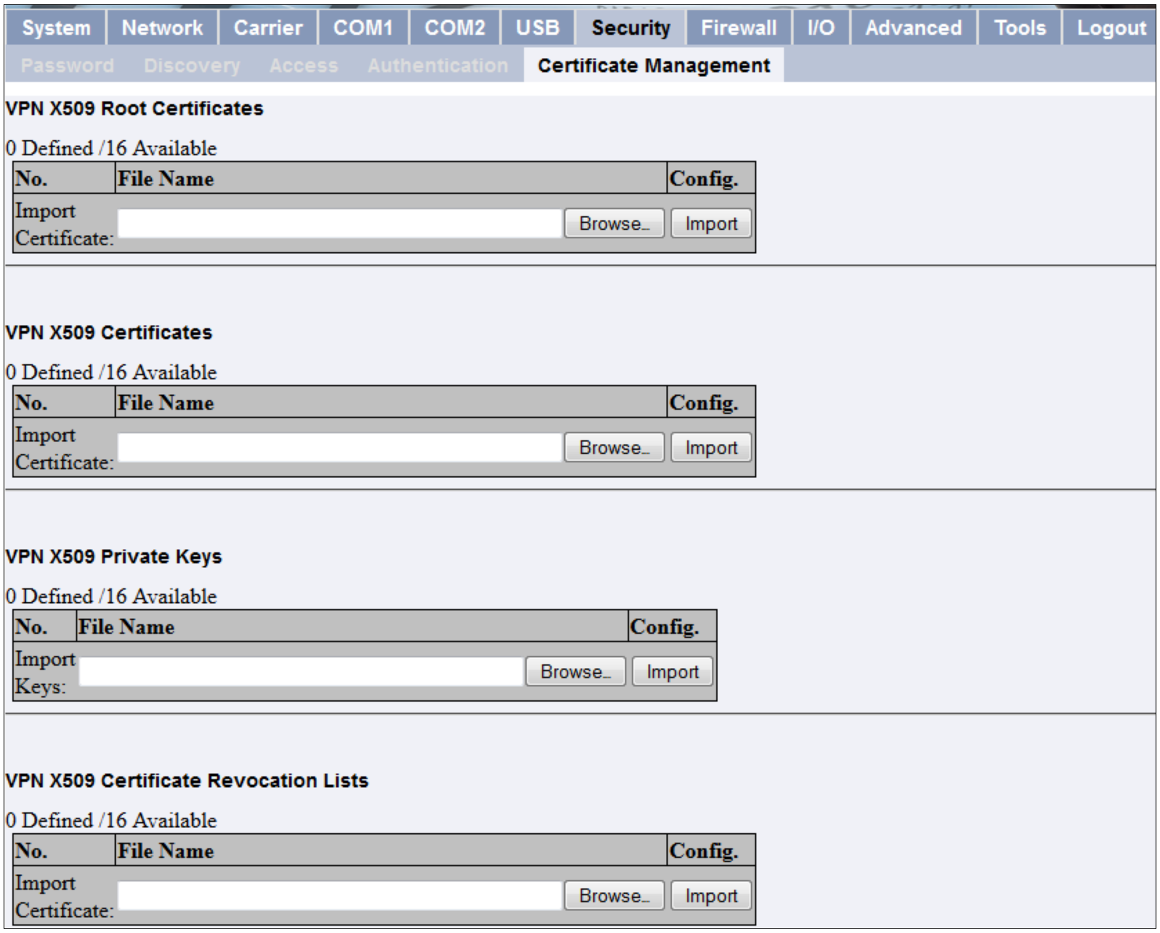
Values

10
1-65535
seconds

4.0 WebUI Configuration

4.7.5 Security > Certificate Management

When using the VPN features of the IPn3G, it is possible to select X.509 for the Authentication Type. If that is the case, the IPn3G 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.



VPN X509 Root Certificates

0 Defined /16 Available

No.	File Name	Config.
Import Certificate:		Browse... Import

VPN X509 Certificates

0 Defined /16 Available

No.	File Name	Config.
Import Certificate:		Browse... Import

VPN X509 Private Keys

0 Defined /16 Available

No.	File Name	Config.
Import Keys:		Browse... Import

VPN X509 Certificate Revocation Lists

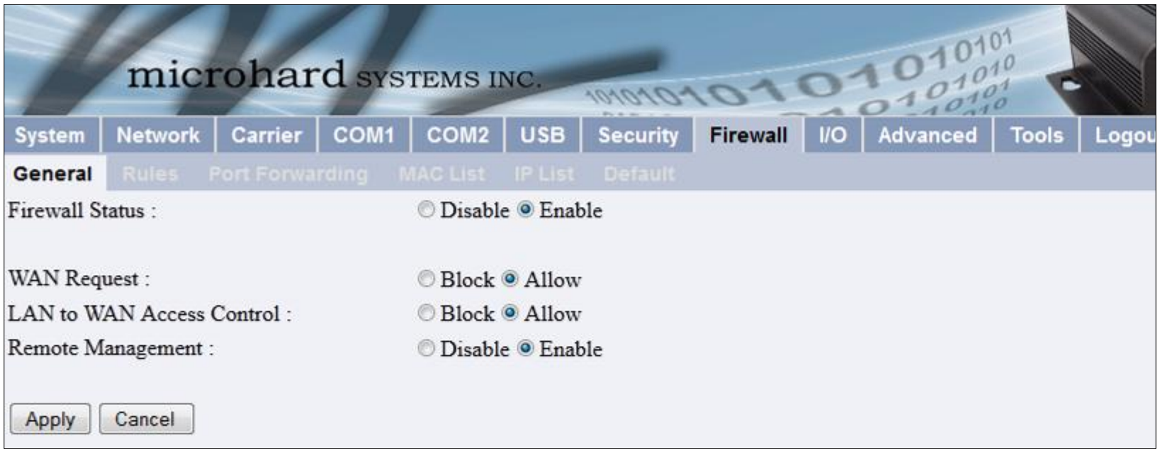
0 Defined /16 Available

No.	File Name	Config.
Import Certificate:		Browse... Import

Image 4-37: Security Config. Menu, Authentication Config. Submenu

4.8 Firewall

The Firewall Configuration is used to allow or disallow particular types of traffic access to and from the network.



Firewall Status : ○ Disable ● Enable

WAN Request : ○ Block ● Allow

LAN to WAN Access Control : ○ Block ● Allow

Remote Management : ○ Disable ● Enable

Image 4-38: Security Config. Menu, Firewall Configuration Submenu

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

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

Firewall Status

When enabled, the firewall settings are in effect. When disabled, none of the settings configured in the menu's below have an effect, the modem is "open".

Values

Disable / Enable

WAN Request

When Blocked the IPn3G will block at traffic on the WAN (Wireless Carrier) 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 **Remote Management** option.

Values

Block / **Allow**

LAN to WAN Access Control

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

Values

Block / **Allow**

Remote Management

Allow remote management of the IPn3G 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.

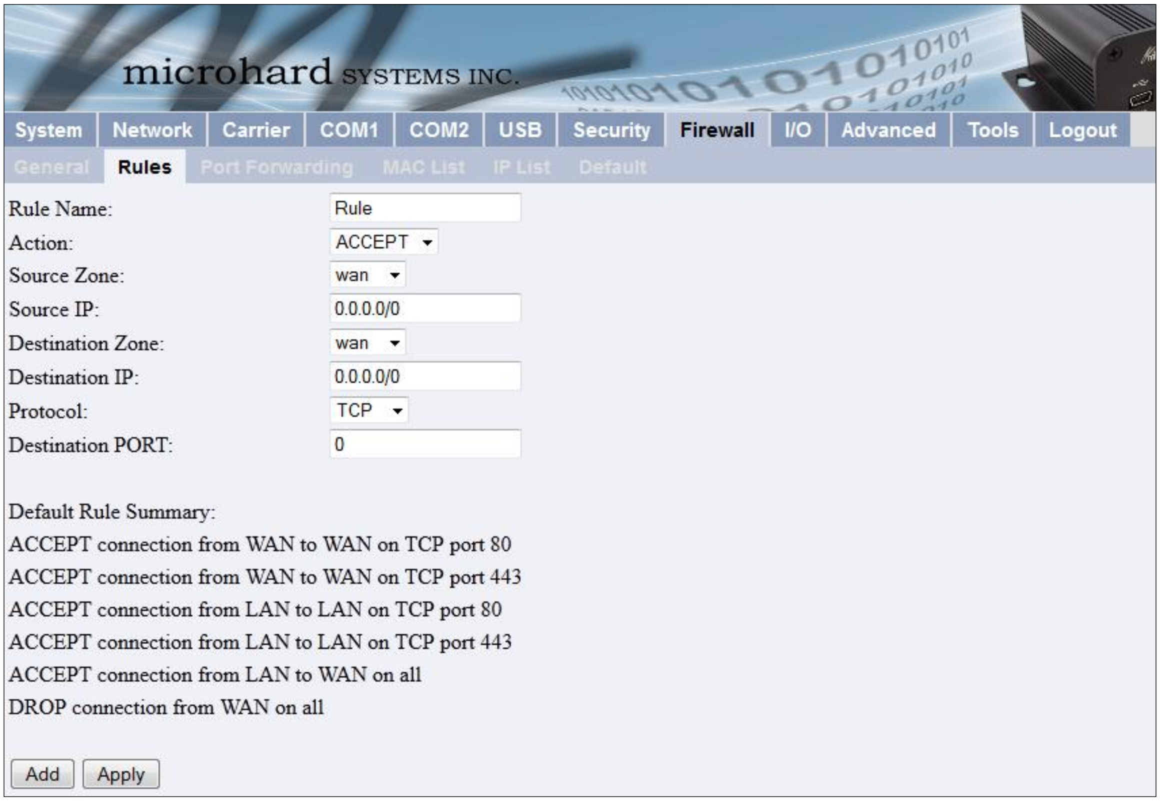
Values

Disable / **Enable**

4.0 WebUI Configuration

4.8.1 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.



Rule Name:	Rule
Action:	ACCEPT
Source Zone:	wan
Source IP:	0.0.0.0/0
Destination Zone:	wan
Destination IP:	0.0.0.0/0
Protocol:	TCP
Destination PORT:	0

Default Rule Summary:
ACCEPT connection from WAN to WAN on TCP port 80
ACCEPT connection from WAN to WAN on TCP port 443
ACCEPT connection from LAN to LAN on TCP port 80
ACCEPT connection from LAN to LAN on TCP port 443
ACCEPT connection from LAN to WAN on all
DROP connection from WAN on all

Image 4-39: Firewall Configuration, Rules Config. Submenu

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 Request** and **LAN to WAN Access Control** are configured in the previous menus.

Values (selection)

ACCEPT
REJECT
DROP

Source Zone

Select the zone which is to be the source of the data traffic. WAN applies to the wireless connection to the cellular carrier and the LAN refers to local connections on the IPn3G (Ethernet, USB NDIS etc)

Values

WAN
LAN
none

Source IP

If a valid IP/Network address is specified, the action will apply against that address; otherwise, leaving the default value of 0.0.0.0/0 in this field results in the action applying to all source IP addresses.

Values (IP Address)

0.0.0.0/0

Destination Zone

Select the zone which is the intended destination of the data traffic. WAN applies to the wireless connection to the cellular carrier and the LAN refers to local connections on the IPn3G (Ethernet, USB NDIS etc)

Values (selection)

WAN
LAN
none

Destination IP

If a valid IP/Network address is specified, the action will apply against that address; otherwise, leaving the default value of 0.0.0.0/0 in this field results in the action applying to all source IP addresses.

Values (IP Address)

0.0.0.0/0

Protocol

The protocol field defines the transport protocol type controlled by the rule.

Values

TCP
UDP
ICMP
all

Destination Port

This field is used to define a port or service used in the rule (i.e. Port 80 = HTTP which is generally a web server)

Values (port)

0

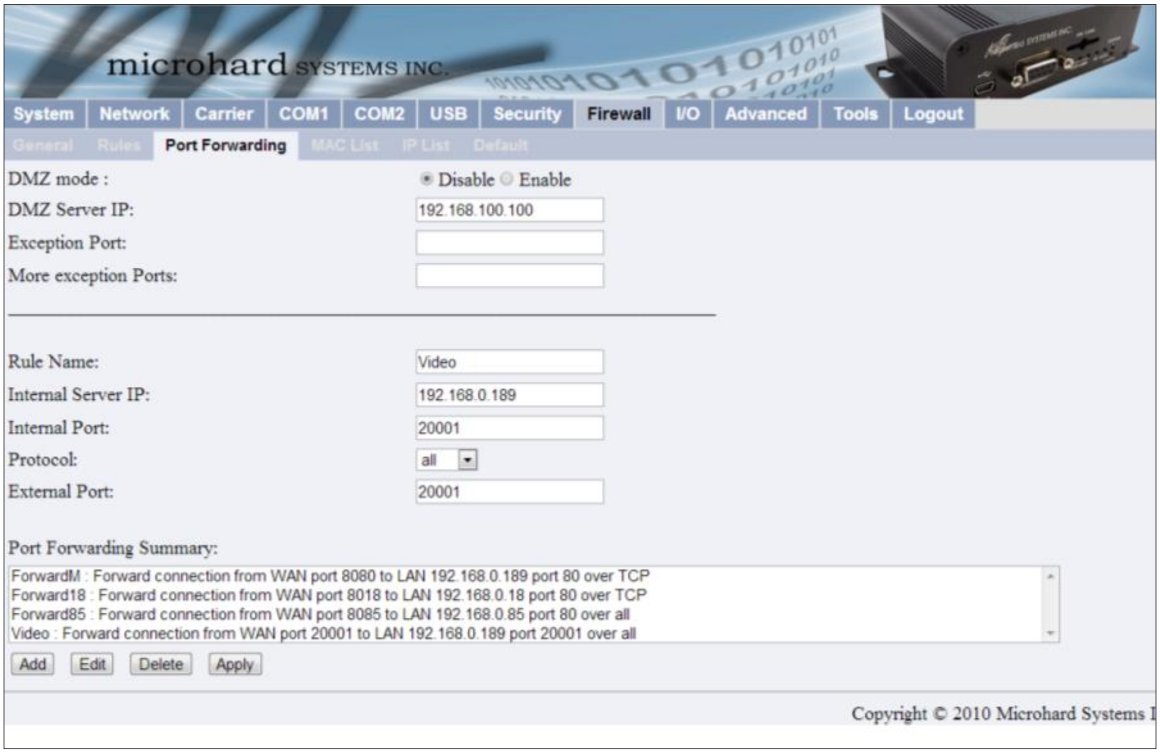
4.0 WebUI Configuration

4.8.2 Firewall > Port Forwarding

The IPn3G 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 IPn3G. 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 > Config) is another option for passing traffic through the IPn3G, in this case all traffic is passed to the device connected to the RJ45 port of the IPn3G, The device must be set for DHCP, as the IPn3G 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 IPn3G, as well as all other features of the IPn3G such as COM, VPN, GPS etc.



DMZ mode : ● Disable ○ Enable

DMZ Server IP: 192.168.100.100

Exception Port:

More exception Ports:

Rule Name: Video

Internal Server IP: 192.168.0.189

Internal Port: 20001

Protocol: all

External Port: 20001

Port Forwarding Summary:

```
ForwardM : Forward connection from WAN port 8080 to LAN 192.168.0.189 port 80 over TCP
Forward18 : Forward connection from WAN port 8018 to LAN 192.168.0.18 port 80 over TCP
Forward85 : Forward connection from WAN port 8085 to LAN 192.168.0.85 port 80 over all
Video : Forward connection from WAN port 20001 to LAN 192.168.0.189 port 20001 over all
```

Copyright © 2010 Microhard Systems I

Image 4-40: Firewall Configuration, Port Forwarding Config. Submenu

DMZ Mode

Enable or disable DMZ Mode. DMZ can be used to forward all traffic to a specific PC/Device on the LAN (DMZ Server IP listed below).

Values (selection)

Disable / Enable

DMZ Server IP

Enter the IP address of the destination device on the LAN side of the IPn3G.

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 IPn3G.

Values (Port #)

none

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.

More Exception Ports

Enter any additional ports that are not to be forwarded, each separated by a comma.

Values (Port #)

none

Rule 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

Internal Server IP

Enter the IP address of the intended internal (i.e. on LAN side of IPn3G) server.

Values (IP Address)

192.168.2.1

Internal Port

Target port number of 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

TCP
UDP
all

External Port

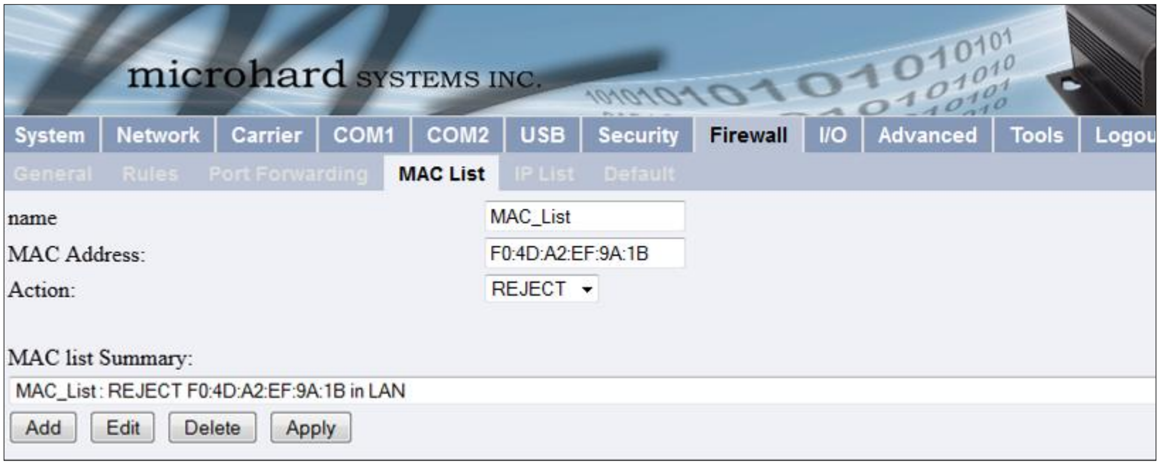
Port number of incoming request (from WAN-side).

Values (Port #)

2000

4.8.3 Firewall > MAC List

MAC List configuration can be used to control which physical LAN devices can access the ports on the IPn3G, by restricting or allowing connections based on the MAC address. MAC List can be used alone or in combination with LAN to WAN Access Control to provide secure access to the physical ports of the IPn3G.



name: MAC_List

MAC Address: F0:4D:A2:EF:9A:1B

Action: REJECT

MAC list Summary:

MAC_List : REJECT F0:4D:A2:EF:9A:1B in LAN

Image 4-41: Firewall Configuration, MAC List Config. Submenu

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)

MAC_List

MAC Address

Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above.

Values (MAC Address)

00:00:00:00:00:00

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.

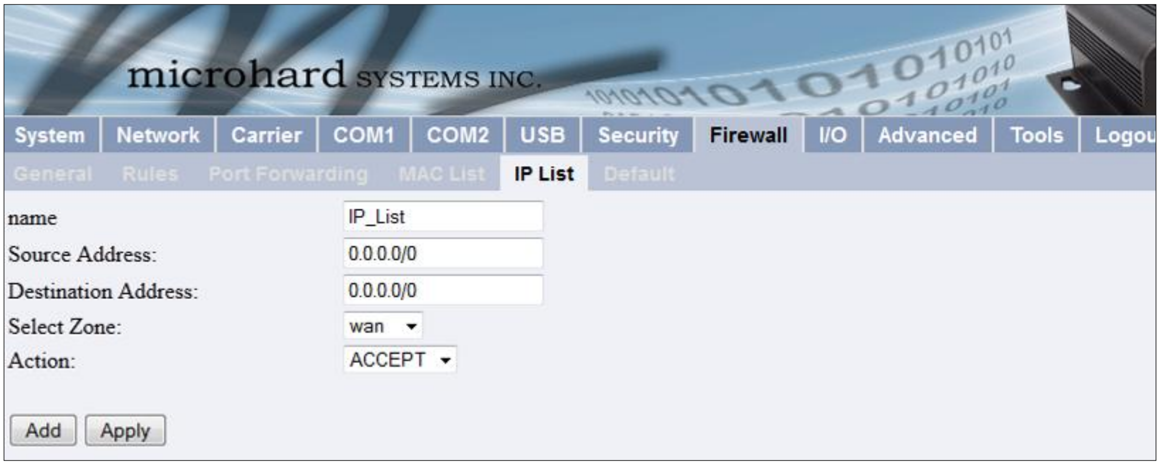
Values (selection)

ACCEPT
DROP
REJECT

4.0 WebUI Configuration

4.8.4 Firewall > IP List

IP List configuration can be used to define who or what can access the IPn3G, by restricting or allowing connections based on the IP Address/Subnet. Can be used alone or in combination with WAN Request and LAN to Wan Access Control.



name: IP_List
Source Address: 0.0.0.0/0
Destination Address: 0.0.0.0/0
Select Zone: wan
Action: ACCEPT

Image 4-42: Firewall Configuration, Blacklist Configuration Submenu

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

Source Address

Specify the specific IP or Network address (With /subnet, for example 192.168.0.0/24 will apply to all IP addresses in the 192.168.0.1 - 192.168.0.254 range (subnet /24 = 255.255.255.0).

Values (IP Address)

0.0.0.0/0

Destination Address

Optional, enter a destination IP address to make the IP list more specific. Leave as 0.0.0.0/0 to not use.

Values (IP Address)

0.0.0.0/0

Select Zone

Enter the specific zone that the IP List will apply to, WAN (Wireless), LAN (Ethernet, USB NDIS) or None (both).

Values (Selection)

WAN / LAN / NONE

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

4.0 WebUI Configuration

4.8.5 Firewall > Default

This menu provides a soft button which, when selected, will reset the firewall settings to factory defaults. Once the button is pressed all configured firewall settings will immediately be reset to factory defaults.

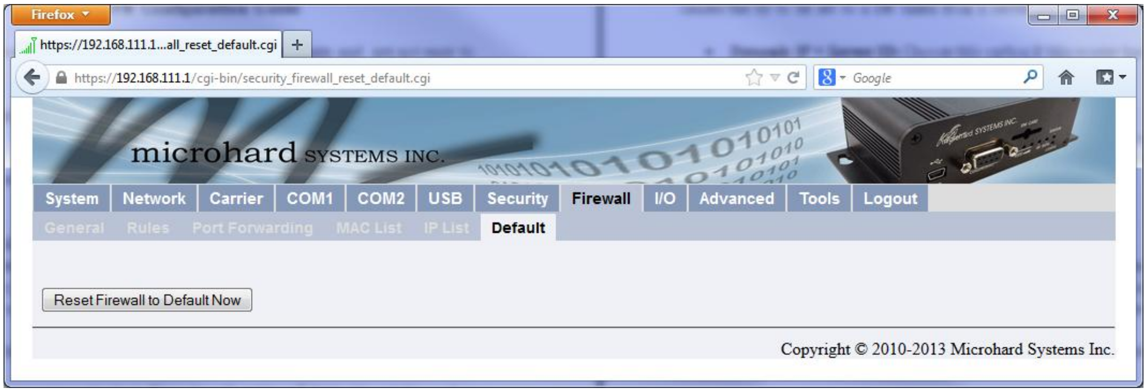

Firefox
https://192.168.111.1...all_reset_default.cgi
https://192.168.111.1/cgi-bin/security_firewall_reset_default.cgi
Google
microhard SYSTEMS INC.
System
Network
Carrier
COM1
COM2
USB
Security
Firewall
I/O
Advanced
Tools
Logout
General
Rules
Port Forwarding
MAC List
IP List
Default
Reset Firewall to Default Now
Copyright © 2010-2013 Microhard Systems Inc.

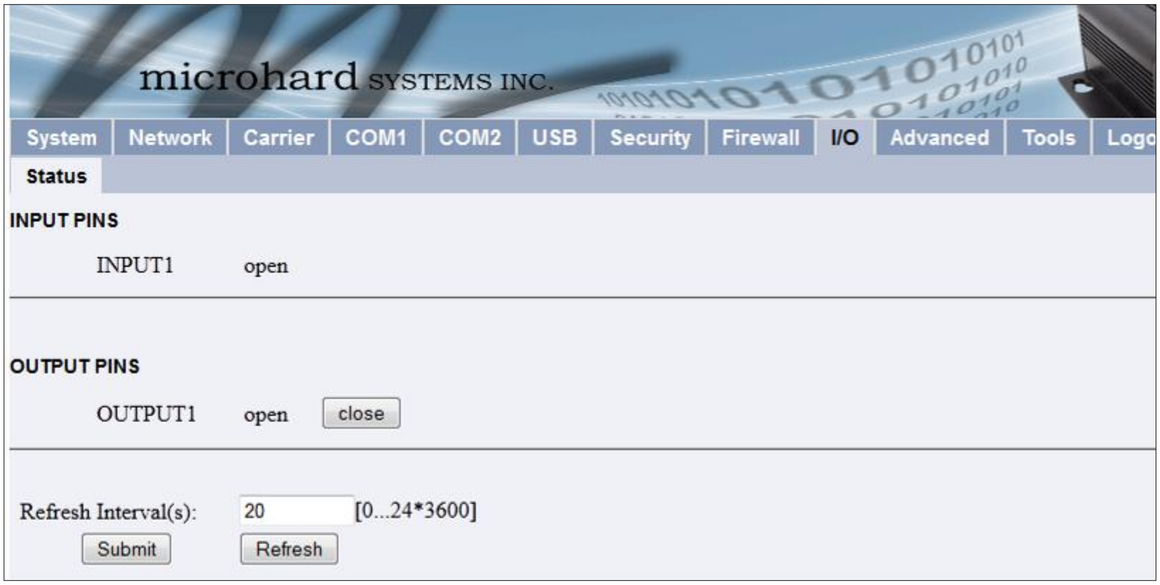
Image 4-43: Reset Firewall to Default

4.0 WebUI Configuration

4.9 I/O

4.9.1 Status

On the front diagnostics (COM2) port of the IPn3G (***Units shipped after June 1, 2012***), 2 pins have been set aside to be used for Digital I/O. Pin **7** is used as an **INPUT**, and Pin **8**, is used for an **OUTPUT**. The status window shows the current status of these pins.



INPUT PINS

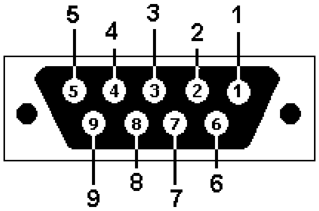
INPUT1 open

OUTPUT PINS

OUTPUT1 open close

Refresh Interval(s): 20 [0...24*3600]

Image 4-44: I/O > Status



Diagnostics Port (DB9 - Female)

Pin 7 - INPUT
Pin 8 - OUTPUT

Image 4-45: I/O > Pin Location

INPUT PINS

Pin 7 on the Diagnostics port of the IPn3G can be used to detect an input. Pin 7 has a small wetting current (Vin) used to detect a contact closure, and prevent false readings by any noise or intermittent signals, it has a threshold sensitivity of 1.8V.

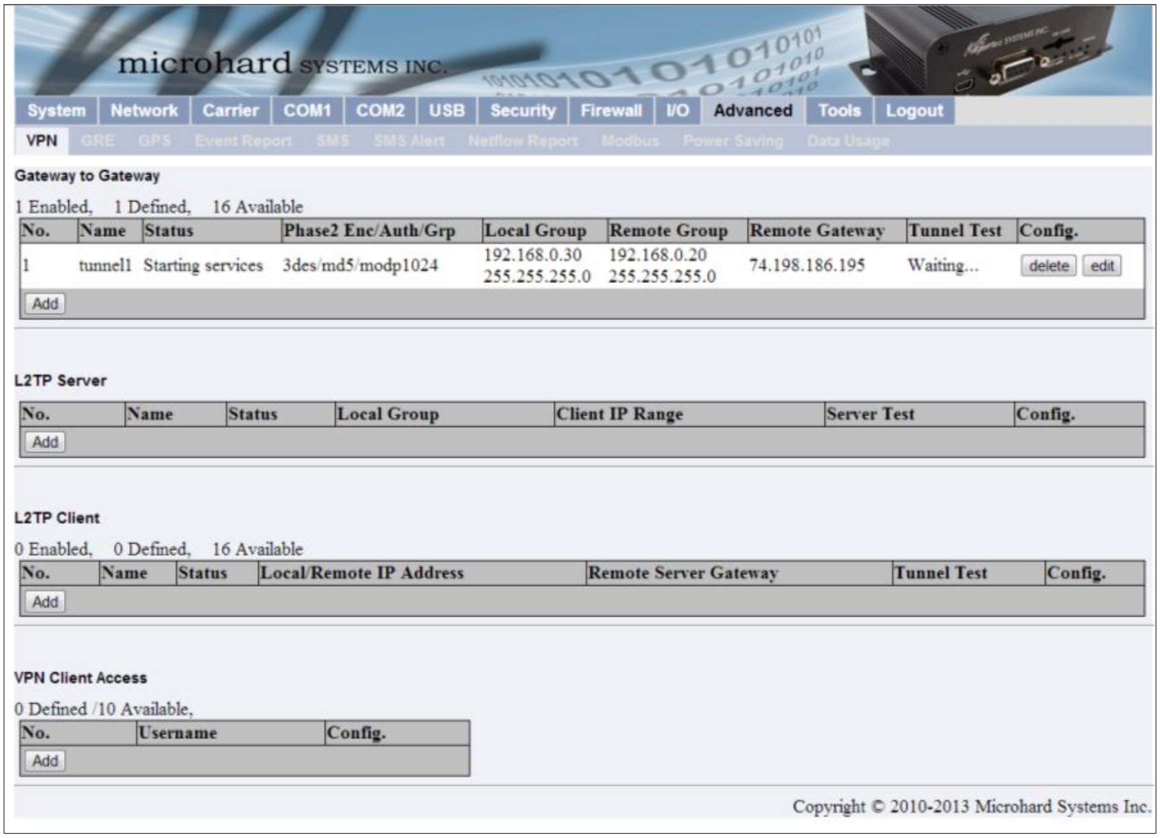
OUTPUT PINS

Pin 8 on the diagnostics port of the IPn3G can be used to provide an output signal, which can be used, for example, to drive an external relay to control an external device. **Appendix G: Digital I/O: Driving an External Relay**, provides a example schematic of how this would work. Maximum recommended load for the Output Pin is 150mA @ 32 VDC (Vin)

4.10 Advanced

4.10.1 VPN

A Virtual Private Network (VPN) may be configured to enable a tunnel between the IPn3G and a remote network.. The IPn3G supports VPN IPsec Gateway to Gateway (site-to-site) tunneling, meaning you are using the IPn3G to create a tunnel between two VPN devices. The IPn3G can also operate as a L2TP Server, allowing users to VPN into the unit from a remote PC, and a L2TP Client.



Gateway to Gateway

1 Enabled, 1 Defined, 16 Available

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	tunnel1	Starting services	3des/md5/modp1024	192.168.0.30 255.255.255.0	192.168.0.20 255.255.255.0	74.198.186.195	Waiting...	delete edit
Add								

L2TP Server

No.	Name	Status	Local Group	Client IP Range	Server Test	Config.
Add						

L2TP Client

0 Enabled, 0 Defined, 16 Available

No.	Name	Status	Local/Remote IP Address	Remote Server Gateway	Tunnel Test	Config.
Add						

VPN Client Access

0 Defined /10 Available,

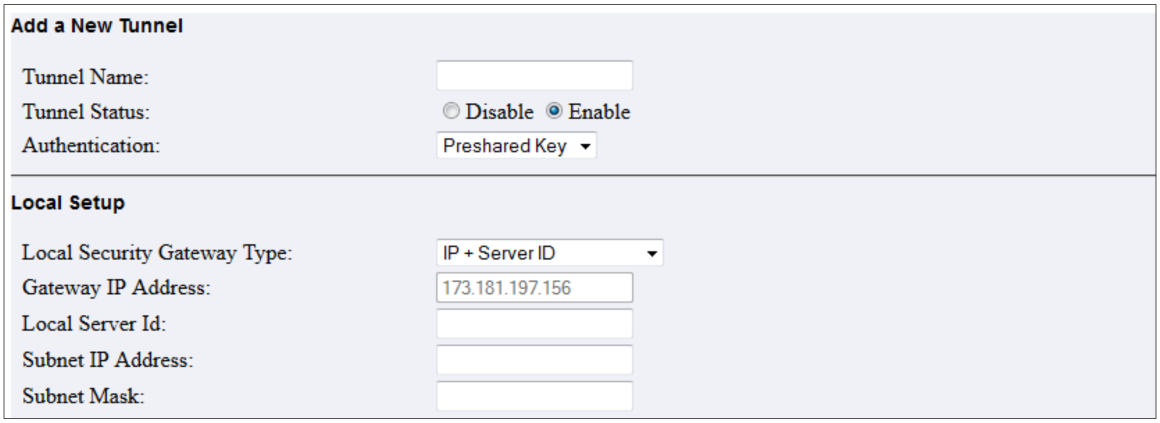
No.	Username	Config.
Add		

Copyright © 2010-2013 Microhard Systems Inc.

Image 4-46: VPN IPsec Configuration Submenu

4.10.1.1 VPN > Gateway-to-Gateway

The Site to Site configuration allows the connection of two VPN devices to create a tunnel, such as a IPn3G router at the office and a VPN capable router at a teleworker's home. To establish a tunnel, settings must be mirrored on the two routers. A successful connection requires that at least one router is identifiable by a static IP address or a Server ID. If one end of the tunnel uses a dynamic IP address, the server ID can be used to establish a connection. The two ends of the tunnel cannot be on the same subnet.



Add a New Tunnel

Tunnel Name:	
Tunnel Status:	○ Disable ● Enable
Authentication:	Preshared Key

Local Setup

Local Security Gateway Type:	IP + Server ID
Gateway IP Address:	173.181.197.156
Local Server Id:	
Subnet IP Address:	
Subnet Mask:	

Image 4-47: VPN IPsec, Site-to-Site Submenu

Add/Edit Tunnel > Tunnel Name

Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name. The VPN tunnel name can be comprised of 1-0, A-Z, a-z or '_'. The space and dash '-', are not valid characters.

Values (chars)

tunnel1

Add/Edit Tunnel > Tunnel Status

Tunnel Status is used to Enable or Disable the current tunnel.

Values (selection)

Disable / **Enable**

Add/Edit Tunnel > Authentication

Select the type of Authentication. If Preshared Key is used, the same key must be entered under IPsec Setup > Preshared Key. If X.509 is selected, Certificate Management (Security) must be used to load the required certificates and private keys related to X.509

Values (selection)

Preshared Key
X.509 CA

Local 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

(Continued…)

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.

Local Setup > Gateway IP Address

Displays the current WAN IP address of the IPn3G.

Values (IP Address)

Current WAN IP Address

Local Setup > Local 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)

Local Setup > Subnet IP Address

Define the local network by specifying the local subnet. Each end of the tunnel must be on different subnets. To setup/change the local subnet on the IPn3G, visit the Network Configuration Tab prior to setting up a VPN tunnel.

Values (IP Address)

(no default)

Local Setup > Subnet Mask

Specify the subnet mask of the local network address.

Values (IP Address)

(no default)

Local Setup > Certificate

If X.509 CA Authentication is selected, this field will appear. Enter the certificate to be used by the current tunnel.

Values (IP Address)

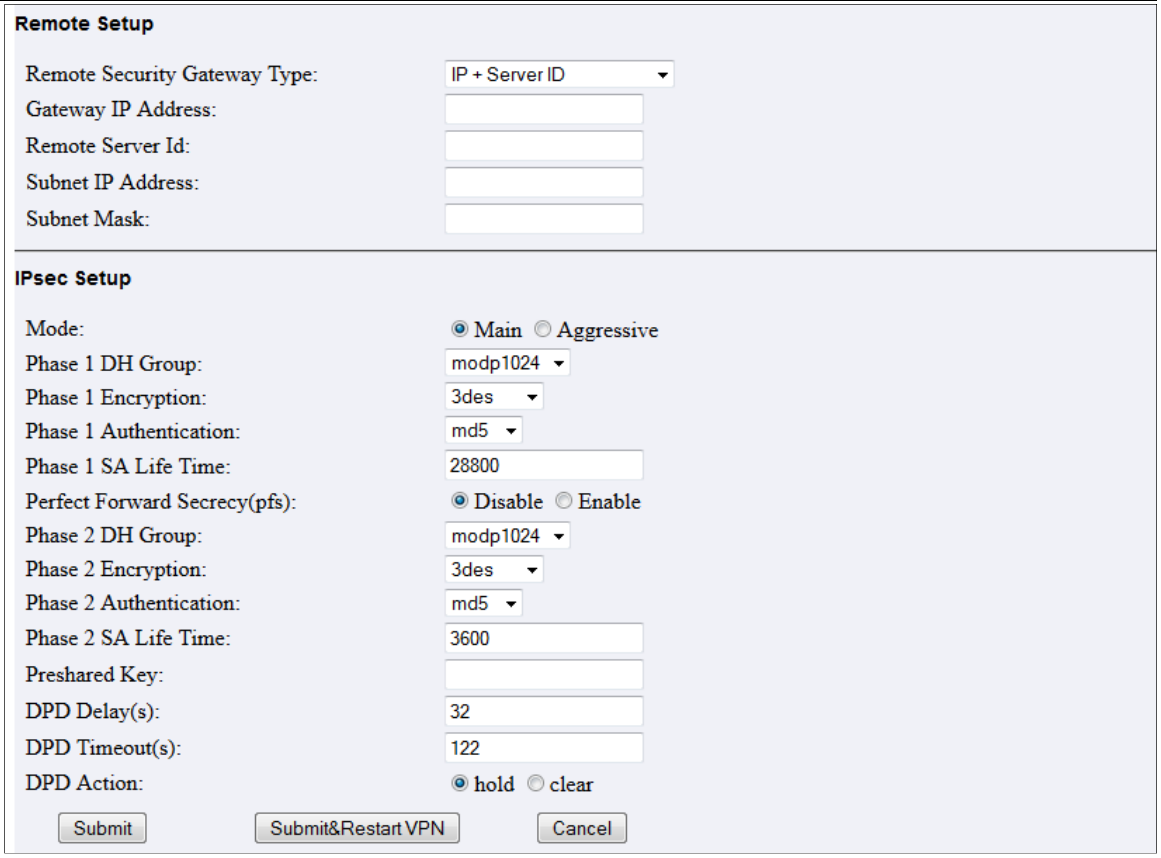
(no default)

Local Setup > Private Key

If X.509 CA Authentication is selected, this field will appear. Enter the Private Key required by the X.509 protocol.

Values (IP Address)

(no default)



Remote Setup

Remote Security Gateway Type:	IP + Server ID
Gateway IP Address:	
Remote Server Id:	
Subnet IP Address:	
Subnet Mask:	

IPsec Setup

Mode:	● Main ○ Aggressive
Phase 1 DH Group:	modp1024
Phase 1 Encryption:	3des
Phase 1 Authentication:	md5
Phase 1 SA Life Time:	28800
Perfect Forward Secrecy(pfs):	● Disable ○ Enable
Phase 2 DH Group:	modp1024
Phase 2 Encryption:	3des
Phase 2 Authentication:	md5
Phase 2 SA Life Time:	3600
Preshared Key:	
DPD Delay(s):	32
DPD Timeout(s):	122
DPD Action:	● hold ○ clear

Image 4-48: VPN IPsec, Site-to-Site Submenu

Remote 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

Remote Setup > 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)

Remote Setup > Remote 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 (characters)

(no default)

Remote Setup > Subnet IP Address

Define the remote network by specifying the subnet local to that router.

Values (IP Address)

(no default)

Remote Setup > Subnet Mask

Specify the subnet mask of the remote network address.

Values (IP Address)

(no default)

Remote Setup > Certificate

If X.509 CA Authentication is selected, this field will appear. Enter the certificate to be used by the current tunnel.

Values (characters)

(no default)

IPsec Setup > Mode

Select the IPsec IKE (Internet Key Exchange) mode used for authentication. Main mode is the standard mode, but aggressive mode can be used to provide faster negotiation.

Values (selection)

Main / Aggressive

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

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

Set the DPD Delay required to authenticate with the remote VPN router.

Values (seconds)

32

DPD Timeout

Set the DPD Timeout required to authenticate with the remote VPN router.

Values (seconds)

122

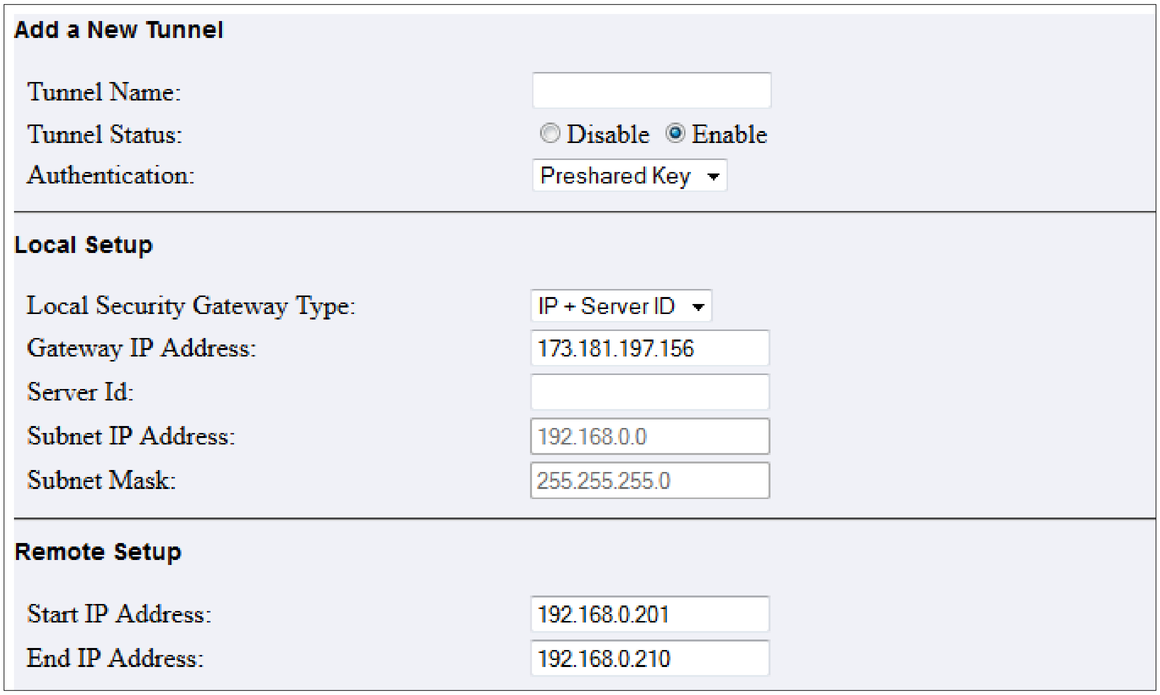
DPD Action

Set the DPD action required to authenticate with the remote VPN router.

Values (selection)

Hold / Clear

4.10.1.2 VPN > L2TP Server



Add a New Tunnel

Tunnel Name:	
Tunnel Status:	○ Disable ● Enable
Authentication:	Preshared Key

Local Setup

Local Security Gateway Type:	IP + Server ID
Gateway IP Address:	173.181.197.156
Server Id:	
Subnet IP Address:	192.168.0.0
Subnet Mask:	255.255.255.0

Remote Setup

Start IP Address:	192.168.0.201
End IP Address:	192.168.0.210

Image 4-49: VPN, L2TP Submenu

Add/Edit Tunnel > Tunnel Name

Enter a name for the L2TP VPN Tunnel. The L2TP VPN tunnel name can be comprised of 1-0, A-Z, a-z or '_'. The space and dash '-', are not valid characters.

Values (chars)

(no default)

Add/Edit Tunnel > Tunnel Status

Tunnel Status is used to Enable or Disable the current tunnel.

Values (selection)

Disable / **Enable**

Add/Edit Tunnel > Authentication

Select the type of Authentication. If Preshared Key is used, the same key must be entered under IPsec Setup > Preshared Key. If X.509 is selected, Certificate Management (Security) must be used to load the required certificates and private keys related to X.509

Values (selection)

Preshared Key
X.509 CA

4.0 WebUI Configuration

Local Setup > Local Security Gateway Type

Specify the method for identifying incoming L2TP connections. Remote systems can simply specify the IP address, or it can be configured that the Server ID must also be known.

Values (selection)

IP Only
IP + Server ID

Local Setup > Gateway IP Address

Displays the current WAN IP address of the IPn3G, which is the local VPN Gateway.

Values (IP Address)

Current IP Address

Server ID

Specify the Server ID if required by the Local Security Gateway Type above. Usually this is in the format of @name.

Values (characters)

(no default)

Subnet IP Address

Displays the local subnet used by the IPn3G for local devices, those connected to the Ethernet Port. To modify the subnet used, visit the Network Configuration menus.

Values (IP Address)

192.168.0.0

Subnet Mask

Displays the local subnet mask used by the IPn3G for local devices.

Values (IP Address)

255.255.255.0

Certificate / Private Key

If X.509 CA is chosen as the authentication method for the L2TP server, then the certificates must be loaded using the Certificate Management menu located under security. Specify which certificate / private key is being used with this tunnel here.

Values (characters)

(no default)

Remote Setup > Start IP Address

Enter the starting range of IP Addresses that will be assigned to a remote VPN adapter (such as a remote PC) when a VPN tunnel is created.

Values (IP Address)

192.168.0.201

End IP Address

Enter the end of the range of IP Addresses that will be assigned to a remote VPN adapter (such as a remote PC) when a VPN tunnel is created.

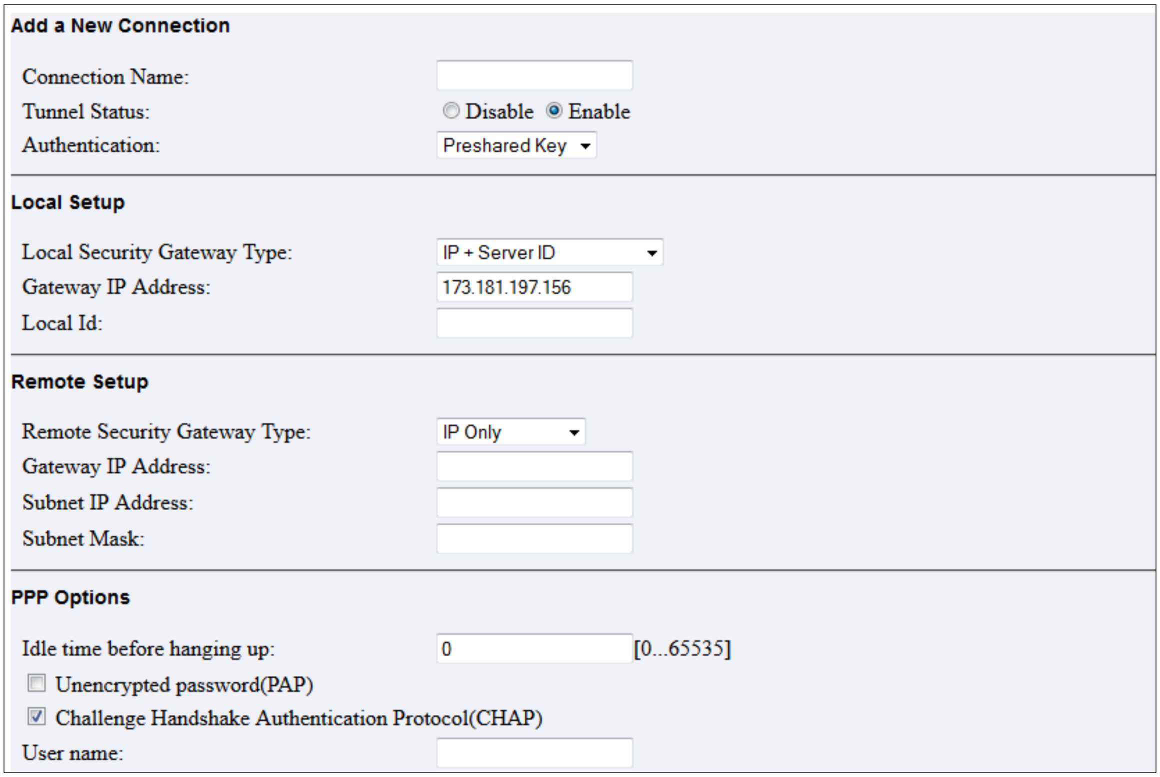
Values (IP Address)

192.168.0.210

IPsec Setup - Refer back to the previous section for information about IPsec parameters.

4.10.1.3 VPN > L2TP Client

The IPn3G can also operate as a L2TP Client, allowing a VPN connection to be made with a L2TP Server.



Add a New Connection

Connection Name:
Tunnel Status: ○ Disable ● Enable
Authentication: Preshared Key

Local Setup

Local Security Gateway Type: IP + Server ID
Gateway IP Address: 173.181.197.156
Local Id:

Remote Setup

Remote Security Gateway Type: IP Only
Gateway IP Address:
Subnet IP Address:
Subnet Mask:

PPP Options

Idle time before hanging up: 0 [0...65535]
□ Unencrypted password(PAP)
☑ Challenge Handshake Authentication Protocol(CHAP)
User name:

Image 4-50: VPN IPsec, VPN Client Submenu

Add New Connection > Connection Name

The Connection Name is used as a reference name for easy identification of the connection.

Values (characters)

none

Add New Connection > Tunnel Status

Enable or disable the connection to the specified L2TP server here.

Values (selection)

Disable / **Enable**

Add New Connection > Authentication

Select the type of Authentication. If Preshared Key is used, the same key must be entered under IPsec Setup > Preshared Key. If X.509 is selected, Certificate Management (Security) must be used to load the required certificates and private keys related to X.509

Values (selection)

Preshared Key
X.509 CA

Local Setup > Local Security Gateway Type

The L2TP requires that incoming connections know their IP Address and/or the Server ID. Select which parameters are used by the L2TP server.

Values (selection)

IP Only
IP + Server ID
Dynamic IP + Server ID

Local Setup > Gateway IP Address

The current WAN IP address is shown here.

Values (IP Address)

Current IP Address

Local Setup > Local ID

If the server ID is required, enter the ID here.

Values (characters)

(no default)

Remote Setup > Remote Security Gateway Type

The L2TP requires that incoming connections know their IP Address and/or the Server ID. Select which parameters are used by the L2TP server. The L2TP server must have a static, known IP address to create a tunnel.

Values (selection)

IP Only
IP + Server ID

Remote Setup > Gateway IP Address

Enter the IP address of the L2TP server that is to be connected to.

Values (IP Address)

(no default)

Remote Setup > Server ID

If the server ID is required, enter the ID here.

Values (characters)

(no default)

Remote Setup > Subnet IP Address

Enter the IP Address of the remote network.

Values (IP Address)

(no default)

Remote Setup > Subnet Mask

Enter the subnet mask of the remote network.

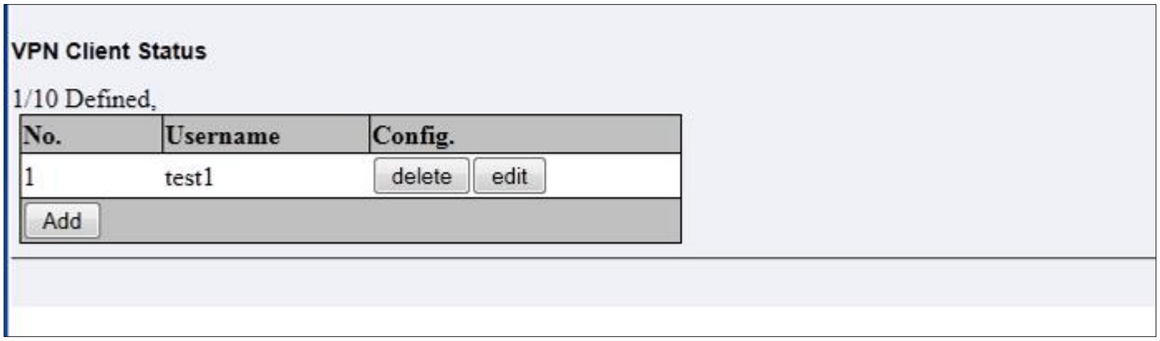
Values (IP Address)

(no default)

IPsec Setup - Refer back to the previous sections for information about IPsec parameters.

4.10.1.4 VPN > VPN Client Status

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

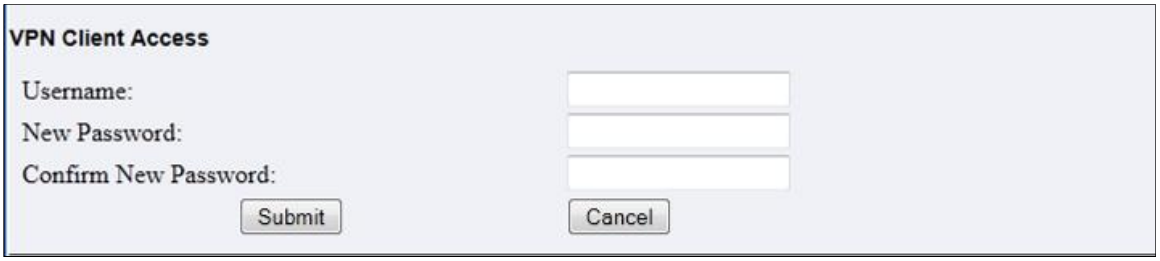


VPN Client Status

1/10 Defined,

No.	Username	Config.
1	test1	delete edit

Image 4-51: VPN IPsec, VPN Client Submenu



VPN Client Access

Username:

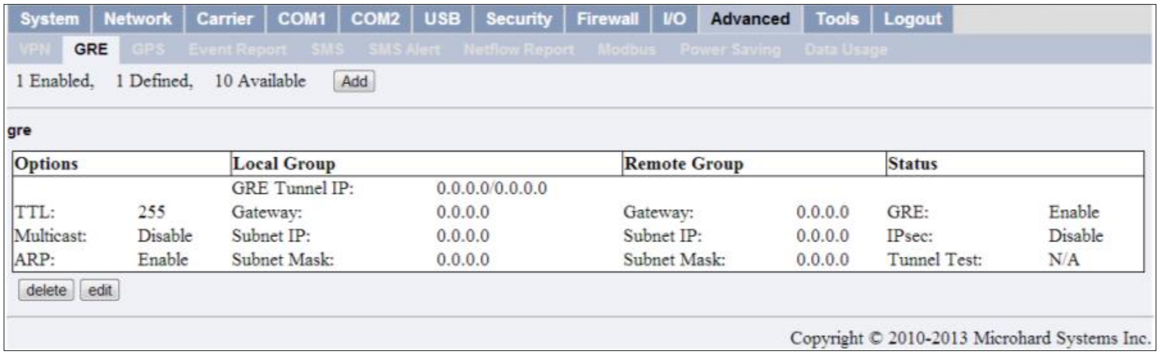
New Password:

Confirm New Password:

Image 4-52: VPN IPsec, VPN Client Submenu

4.10.2 GRE

The IPn3G also supports GRE (Generic Routing Encapsulation), 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.



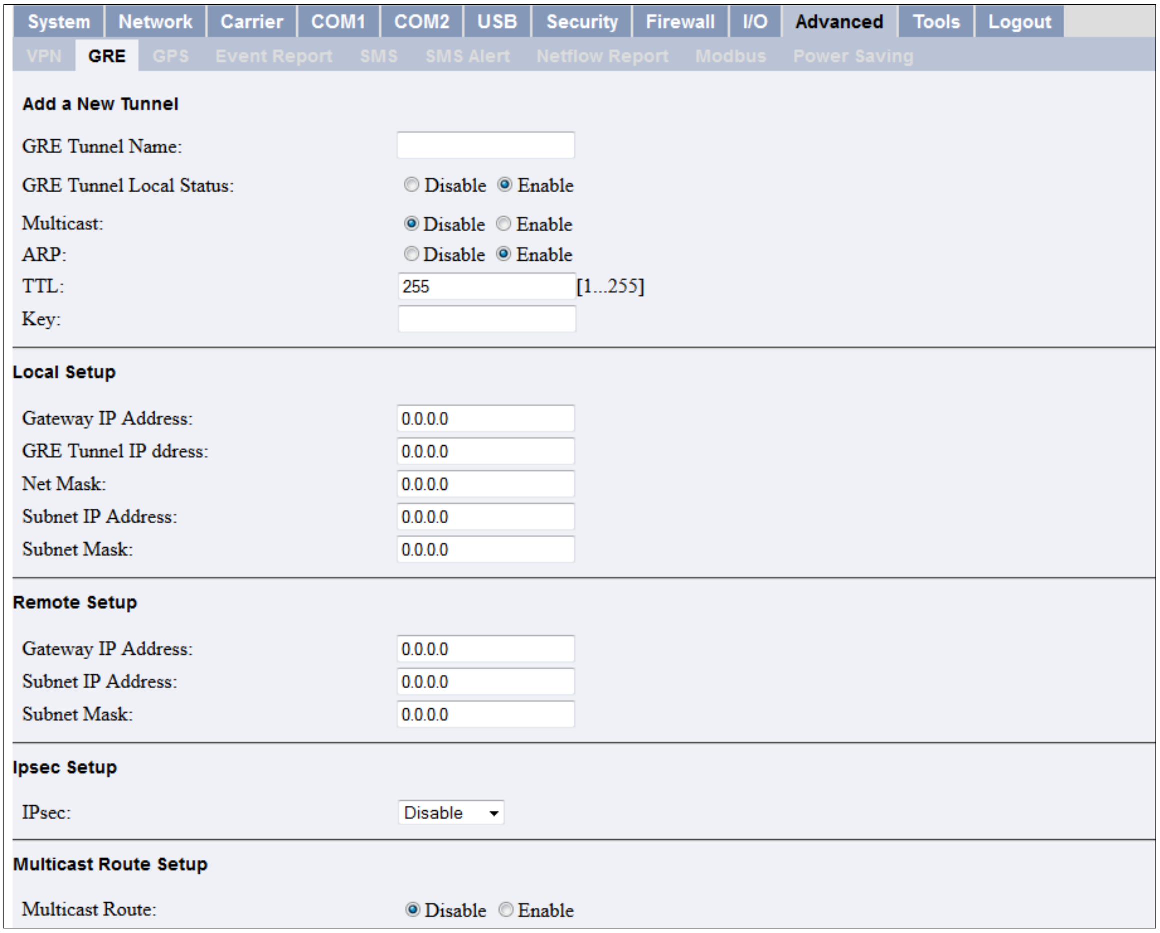
1 Enabled, 1 Defined, 10 Available

gre

Options		Local Group		Remote Group		Status	
		GRE Tunnel IP:	0.0.0.0/0.0.0.0				
TTL:	255	Gateway:	0.0.0.0	Gateway:	0.0.0.0	GRE:	Enable
Multicast:	Disable	Subnet IP:	0.0.0.0	Subnet IP:	0.0.0.0	IPsec:	Disable
ARP:	Enable	Subnet Mask:	0.0.0.0	Subnet Mask:	0.0.0.0	Tunnel Test:	N/A

Copyright © 2010-2013 Microhard Systems Inc.

Image 4-53: Advanced > GRE



Add a New Tunnel

GRE Tunnel Name:
GRE Tunnel Local Status: ○ Disable ● Enable
Multicast: ● Disable ○ Enable
ARP: ○ Disable ● Enable
TTL: 255 [1...255]
Key:

Local Setup

Gateway IP Address: 0.0.0.0
GRE Tunnel IP ddress: 0.0.0.0
Net Mask: 0.0.0.0
Subnet IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0

Remote Setup

Gateway IP Address: 0.0.0.0
Subnet IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0

Ipsec Setup

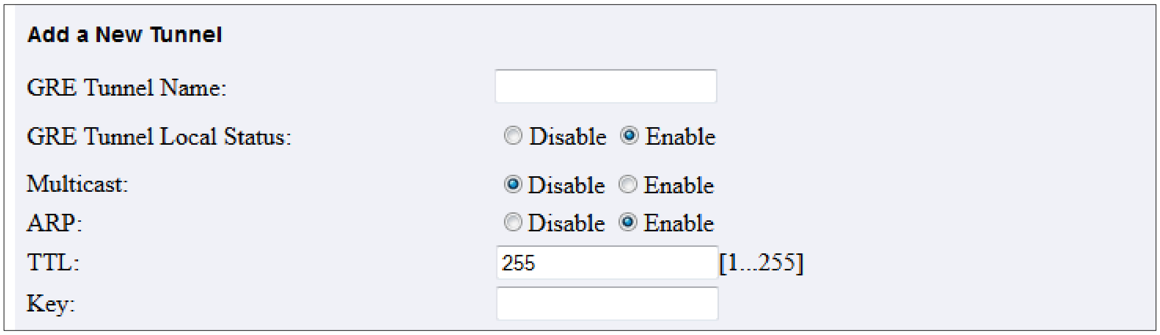
IPsec: Disable

Multicast Route Setup

Multicast Route: ● Disable ○ Enable

Image 4-54: GRE Configuration

4.0 WebUI Configuration



Add a New Tunnel

GRE Tunnel Name:	
GRE Tunnel Local Status:	○ Disable ● Enable
Multicast:	● Disable ○ Enable
ARP:	○ Disable ● Enable
TTL:	255 [1...255]
Key:	

Image 4-55: GRE > Adding a New Tunnel

GRE Tunnel Name

Each GRE tunnel must have a unique name. Up to 10 GRE tunnels are supported by the IPn3G. Valid characters include A-Z, a –z, 1 - 0, '_'. Spaces and dashes are not allowed.

Values (chars(32))

gre

GRE Tunnel Local Status

Enable / Disable the GRE Tunnel.

Values (selection)

Disable / **Enable**

Multicast

Enable / Disable Multicast support over the GRE tunnel.

Values (selection)

Disable / **Enable**

ARP

Enable / Disable ARP (Address Resolution Protocol) 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**

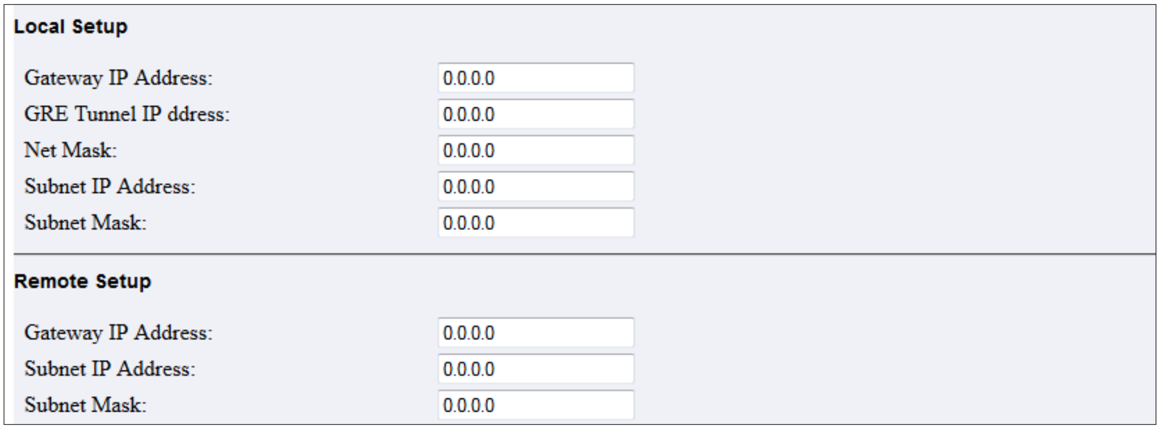
Key

Enter the key for the GRE tunnel.

Values (characters)

(no default)

4.0 WebUI Configuration



Local Setup

Gateway IP Address:	0.0.0.0
GRE Tunnel IP ddress:	0.0.0.0
Net Mask:	0.0.0.0
Subnet IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0

Remote Setup

Gateway IP Address:	0.0.0.0
Subnet IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0

Image 4-56: GRE > Local / Remote Setup

Local Setup > Gateway IP Address

Enter the current WAN IP address of the IPn3G.

Values (IP Address)

0.0.0.0

Local Setup > GRE Tunnel IP Address

This is the IP Address of the local GRE Tunnel, this must be in the same subnet as the remote GRE tunnel. This is not the local subnet.

Values (IP Address)

0.0.0.0

Local Setup > Net Mask

Set the subnet mask of the Local GRE Tunnel IP Address.

Values (IP Address)

0.0.0.0

Local Setup > Subnet IP Address

Enter the IP Address of the local subnet. Each end of the GRE tunnel must be on different subnets.

Values (IP Address)

0.0.0.0

Local Setup > Subnet Mask

Enter the Subnet Mask of the local subnet.

Values (IP Address)

0.0.0.0

Remote Setup > Gateway IP Address

Enter the WAN IP address of the remote router. This is the address to which the tunnel will be created between.

Values (IP Address)

0.0.0.0

Remote Setup > Subnet IP Address

Specify the LAN subnet being used on the remote network. This must be a different subnet than on the local router.

Values (IP Address)

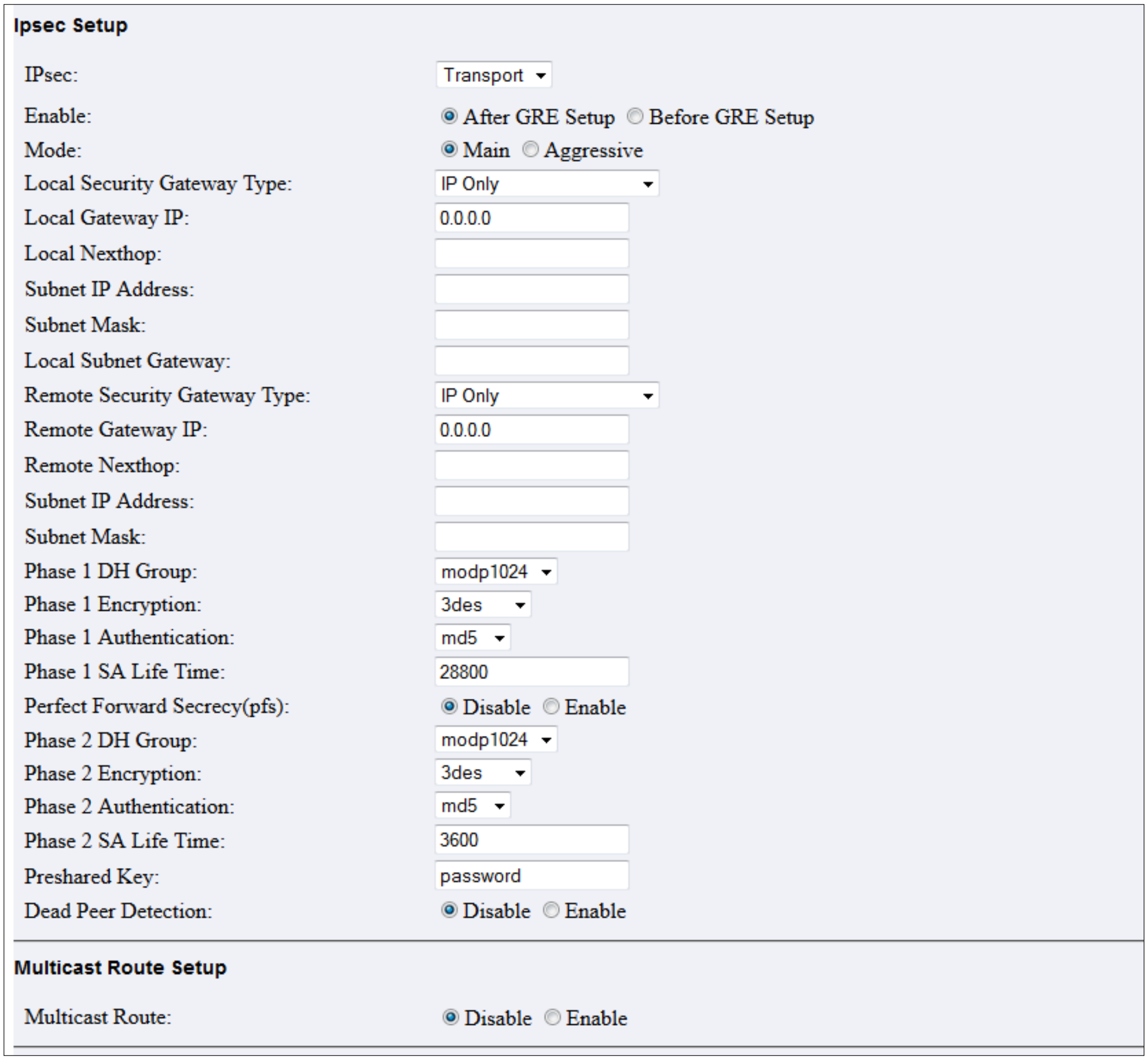
0.0.0.0

Remote Setup > Subnet Mask

Specify the LAN subnet mask being used on the remote network.

Values (IP Address)

0.0.0.0



Ipsec Setup

IPsec:	Transport
Enable:	● After GRE Setup ○ Before GRE Setup
Mode:	● Main ○ Aggressive
Local Security Gateway Type:	IP Only
Local Gateway IP:	0.0.0.0
Local Nexthop:	
Subnet IP Address:	
Subnet Mask:	
Local Subnet Gateway:	
Remote Security Gateway Type:	IP Only
Remote Gateway IP:	0.0.0.0
Remote Nexthop:	
Subnet IP Address:	
Subnet Mask:	
Phase 1 DH Group:	modp1024
Phase 1 Encryption:	3des
Phase 1 Authentication:	md5
Phase 1 SA Life Time:	28800
Perfect Forward Secrecy(pfs):	● Disable ○ Enable
Phase 2 DH Group:	modp1024
Phase 2 Encryption:	3des
Phase 2 Authentication:	md5
Phase 2 SA Life Time:	3600
Preshared Key:	password
Dead Peer Detection:	● Disable ○ Enable

Multicast Route Setup

Multicast Route:	● Disable ○ Enable

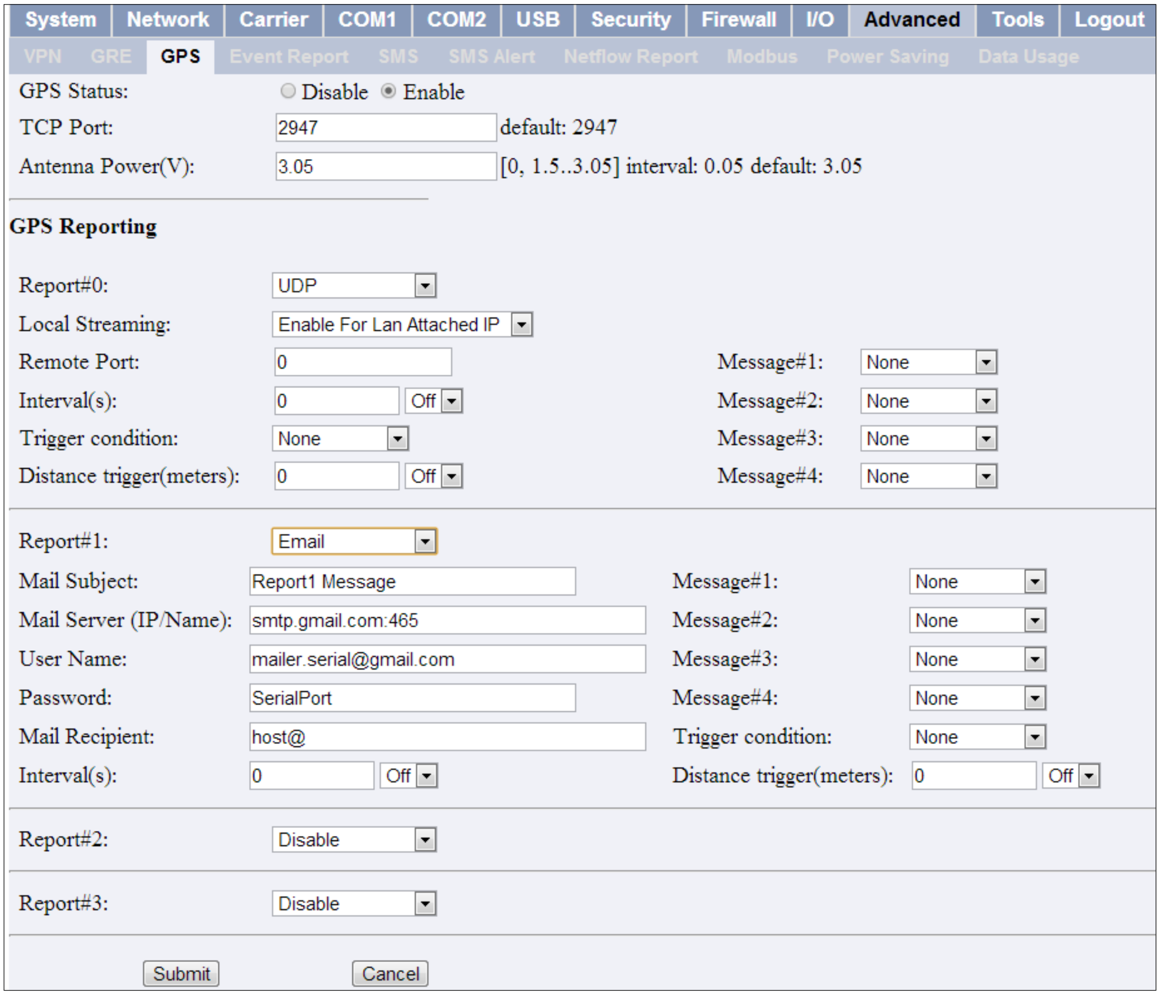
Image 4-57: GRE > IPsec Setup

The setup for GRE IPsec is identical to the setup of VPN IPsec, refer to the previous section for more information.

4.10.3 Advanced > GPS

Some models of the IPn3G support GPS and can provide GPS data to a client. The IPn3G can be polled for GPS data via GPSD standards and/or provide customizable reporting to up to 4 different destination IP addresses via UDP packets, or by Email.

GPS data can also be reported out the COM1 RS232/485 Serial Port. For more information, refer to the ***COM1 > IP Protocol Config > GPS Transparent Mode*** section.



GPS Status: ○ Disable ● Enable
TCP Port: 2947 default: 2947
Antenna Power(V): 3.05 [0, 1.5..3.05] interval: 0.05 default: 3.05

GPS Reporting

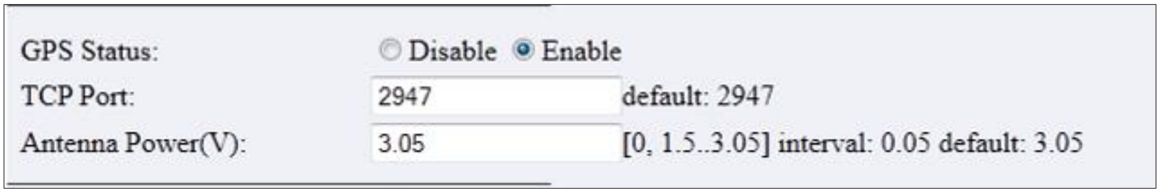
Report#0: UDP
Local Streaming: Enable For Lan Attached IP
Remote Port: 0
Interval(s): 0 Off
Trigger condition: None
Distance trigger(meters): 0 Off
Message#1: None
Message#2: None
Message#3: None
Message#4: None

Report#1: Email
Mail Subject: Report1 Message
Mail Server (IP/Name): smtp.gmail.com:465
User Name: mailer.serial@gmail.com
Password: SerialPort
Mail Recipient: host@
Interval(s): 0 Off
Message#1: None
Message#2: None
Message#3: None
Message#4: None
Trigger condition: None
Distance trigger(meters): 0 Off

Report#2: Disable

Report#3: Disable

Image 4-58: Advanced > GPS submenu



GPS Status: ○ Disable ● Enable

TCP Port: 2947 default: 2947

Antenna Power(V): 3.05 [0, 1.5..3.05] interval: 0.05 default: 3.05

Image 4-59: GPS Polling submenu

GPS Status

Enable or disable the GPS polling function of the IPn3G. The default is **disabled**.

Values (selection)

Disable / Enable

TCP Port

Specify the TCP port on the IPn3G running that a remote GPS system can connect and poll for GPSD information.

Values (1-65535)

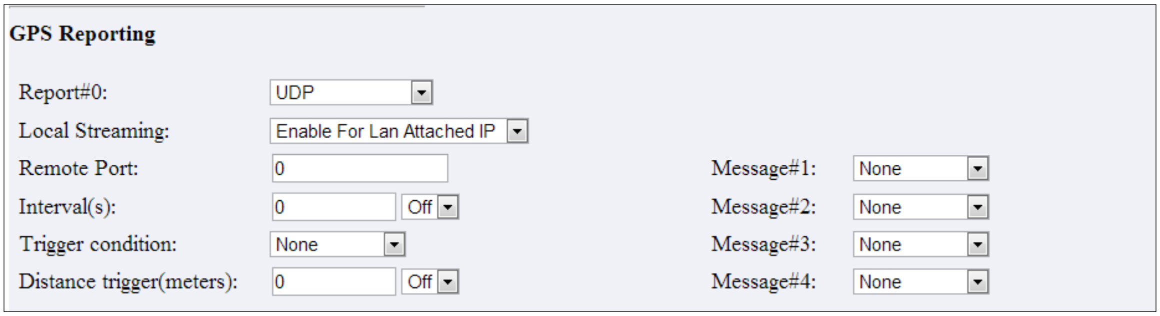
2947

Antenna Power (V)

Specifies the output power supplied to the GPS antenna as required for the specific antenna being used. Refer to your antennas manufacturer for more information. In 0.05V intervals.

Values (1.5 - 3.05)

3.05



GPS Reporting

Report#0: UDP

Local Streaming: Enable For Lan Attached IP

Remote Port: 0

Interval(s): 0 Off

Trigger condition: None

Distance trigger(meters): 0 Off

Message#1: None

Message#2: None

Message#3: None

Message#4: None

Image 4-60: GPS Reporting submenu - UDP

GPS Reporting Report

Enable UDP and/or Email or disable GPS Reporting. Up to 4 reports can be set up and configured independently.

Values (selection)

Disable
UDP
Email

Local Streaming

If enabled local streaming will stream the GPS data selected to a device connected to the LAN.

Values (selection)

Disable
Enable for LAN Attached IP

GPS Reporting - UDP

Remote IP

Specify the IP Address of the destination of the GPS data UDP packets.

Values (IP Address)

0.0.0.0

Remote Port

Specify the port number running the GPS services at the IP Address specified in the IP Address field.

Values (Port #)

0

Interval(s)

The repeat timer specifies the frequency at which the GPS data is reported in seconds.

Values (seconds)

0

Trigger condition

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)

OR
AND

Distance trigger (meters)

The distance trigger allows a specified distance to be traveled before the GPS data is reported.

Values (meters)

0

Message#

The Message field allows customization of up to 4 different GPS messages to be sent to the specified host.

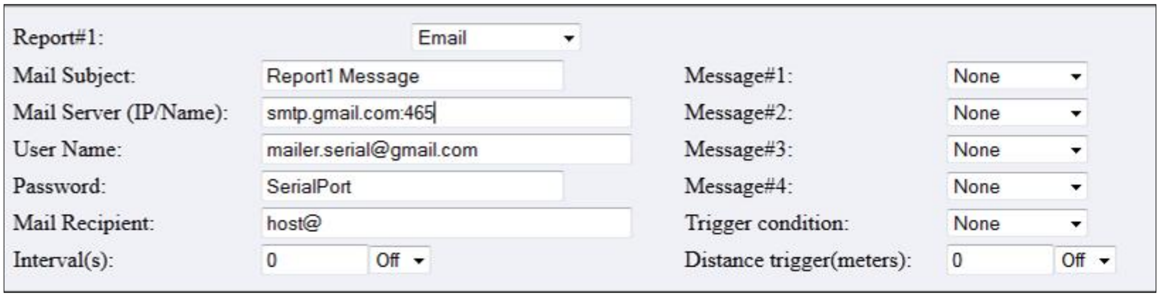
None	-	Message is not used, no data will be sent
ALL	-	Sends all of the below
GGA	-	GPS Fix Data
GSA	-	Overall Satellite Data
GSV	-	Detailed Satellite Data
RMC	-	Recommended Min Data for GPS
VTG	-	Vector Track & Ground Speed

Values (selection)

None
ALL
GGA
GSA
GSV
RMC
VTG

4.0 WebUI Configuration

GPS Reporting - Email



Report#1:	Email		
Mail Subject:	Report1 Message	Message#1:	None
Mail Server (IP/Name):	smtp.gmail.com:465	Message#2:	None
User Name:	mailer.serial@gmail.com	Message#3:	None
Password:	SerialPort	Message#4:	None
Mail Recipient:	host@	Trigger condition:	None
Interval(s):	0 Off	Distance trigger(meters):	0 Off

Image 4-61: GPS Reporting submenu - Email

Mail Subject

The Mail Subject field allows a user to enter a subject for the email sent by the IPn3G.

Values (Chars)

Report1 Message

Mail Server (IP/Name)

Enter the IP Address or Domain name of the account of the outgoing mail server used to send the message.

Values (IP/Name)

varies

User Name

Enter the User Name of the email account used to send email from the IPn3G.

Values (Chars)

varies

Password

Enter the Password for the email account used to send Email, only required if the email server required outgoing authentication.

Values (Chars)

varies

Mail Recipient

Enter the Email address of where the message is to be sent to.

Values (Chars)

varies

Interval(s)

The repeat timer specifies the frequency at which the GPS data is reported in seconds.

Values (seconds)

0

Trigger condition

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)

OR
AND

Distance trigger (meters)

The distance trigger allows a specified distance to be traveled before the GPS data is reported.

Values (meters)

0

Message#

The Message field allows customization of up to 4 different GPS messages to be sent to the specified host.

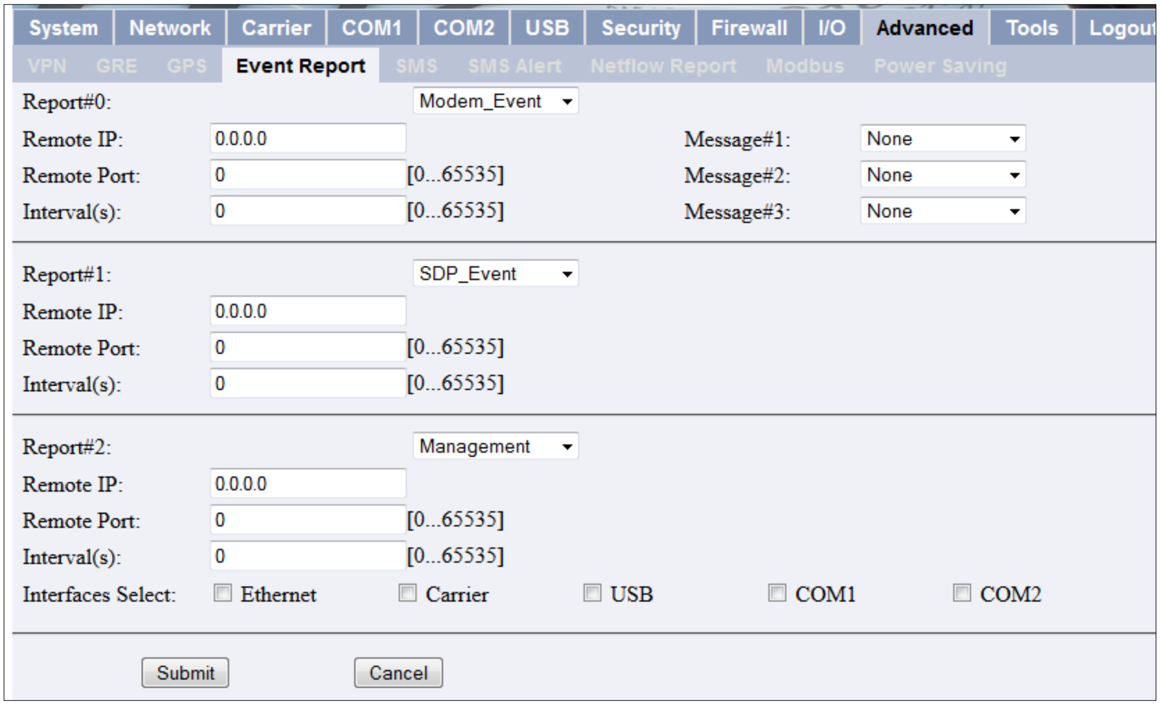
None	-	Message is not used, no data will be sent
ALL	-	Sends all of the below
GGA	-	GPS Fix Data
GSA	-	Overall Satellite Data
GSV	-	Detailed Satellite Data
RMC	-	Recommended Min Data for GPS
VTG	-	Vector Track & Ground Speed

Values (selection)

None
ALL
GGA
GSA
GSV
RMC
VTG

4.10.4 Advanced > Event Reporting

Event Reporting allows the IPn3G to send periodic updates on the modem status via UDP packets. These packets are customizable and can be sent to up to 4 different IP Addresses, at a programmable interval. The event packet can report information about the modem such as the hardware and software versions, core temperature, supply voltage, etc ; about the carrier 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.



Report#0: Modem_Event
Remote IP: 0.0.0.0
Remote Port: 0 [0...65535]
Interval(s): 0 [0...65535]
Message#1: None
Message#2: None
Message#3: None

Report#1: SDP_Event
Remote IP: 0.0.0.0
Remote Port: 0 [0...65535]
Interval(s): 0 [0...65535]

Report#2: Management
Remote IP: 0.0.0.0
Remote Port: 0 [0...65535]
Interval(s): 0 [0...65535]
Interfaces Select: □ Ethernet □ Carrier □ USB □ COM1 □ COM2

Image 4-62: Advanced > Event Reporting submenu

4.10.4.1 Event Reporting > Configuration

Report#

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)

Disable
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

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 (value)

0

Interval (s)

This is the interval time in seconds, that the IPn3G will send the configured UDP message to the Remote IP and Port specified.

Values (seconds)

0

Message#

Up to 3 Messages can be used to construct the reported UDP packets. Only available when reporting is set to Modem_event.

Values (selection)

None
Modem Info
Carrier Info
WAN Info

4.10.4.2 Event Reporting > 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

4.10.4.3 Event Reporting > 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)

Carrier info:

Content length	-	2 BYTES (UINT16_T)
RSSI	-	1 BYTE (UINT8_T)
RF Band	-	2 BYTES (UINT16_T)
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,

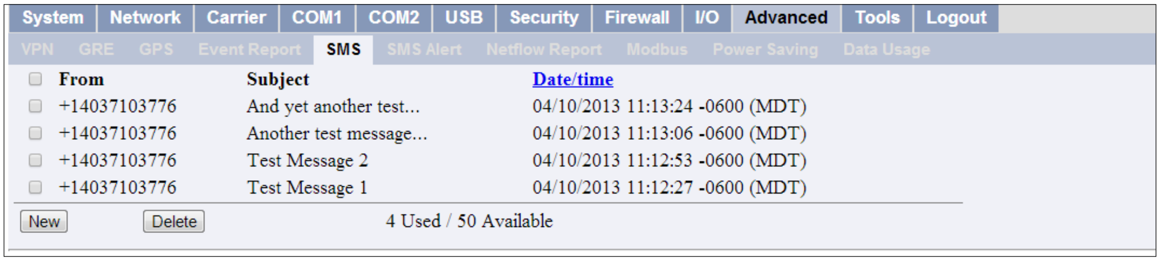
If message type mask = 0x15, the eurd package will be equipped by header+modem information+carrier information+wanip information.

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.

4.10.5 Advanced > SMS

The IPn3G supports SMS messaging through the serial port (See IP Protocol Config under COM1), Through AT Command via Serial and Telnet (See AT Commands), as well as SMS Alerts based on different conditions (See SMS Alerts). The Advanced > SMS menu allows a user to view the messages stored on the SIM card, and if desired to respond to messages from within the WebUI.

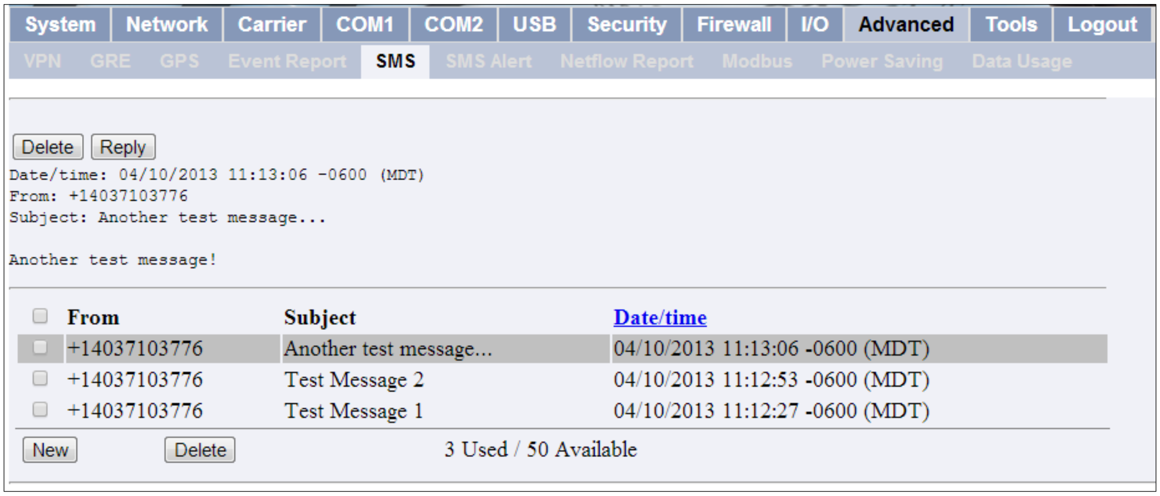


	From	Subject	Date/time
□	+14037103776	And yet another test...	04/10/2013 11:13:24 -0600 (MDT)
□	+14037103776	Another test message...	04/10/2013 11:13:06 -0600 (MDT)
□	+14037103776	Test Message 2	04/10/2013 11:12:53 -0600 (MDT)
□	+14037103776	Test Message 1	04/10/2013 11:12:27 -0600 (MDT)

4 Used / 50 Available

Image 4-63: Advanced > SMS Message List

Selecting the message will show greater message detail, as well as giving the option to delete, or reply to the message.

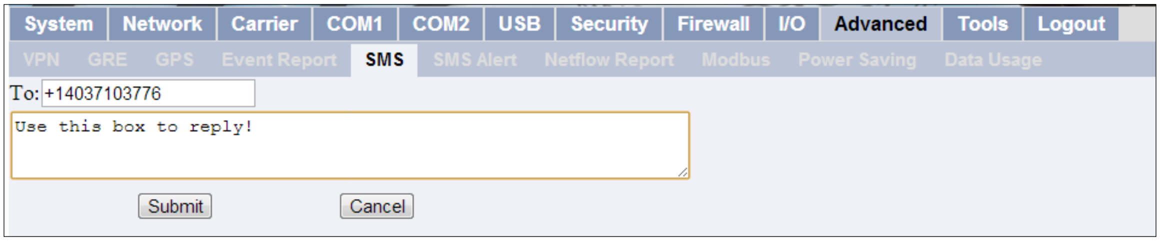


```
Date/time: 04/10/2013 11:13:06 -0600 (MDT)
From: +14037103776
Subject: Another test message...

Another test message!
```

□	From	Subject	Date/time
□	+14037103776	Another test message...	04/10/2013 11:13:06 -0600 (MDT)
□	+14037103776	Test Message 2	04/10/2013 11:12:53 -0600 (MDT)
□	+14037103776	Test Message 1	04/10/2013 11:12:27 -0600 (MDT)

3 Used / 50 Available

Image 4-64: Advanced > SMS Message Detail



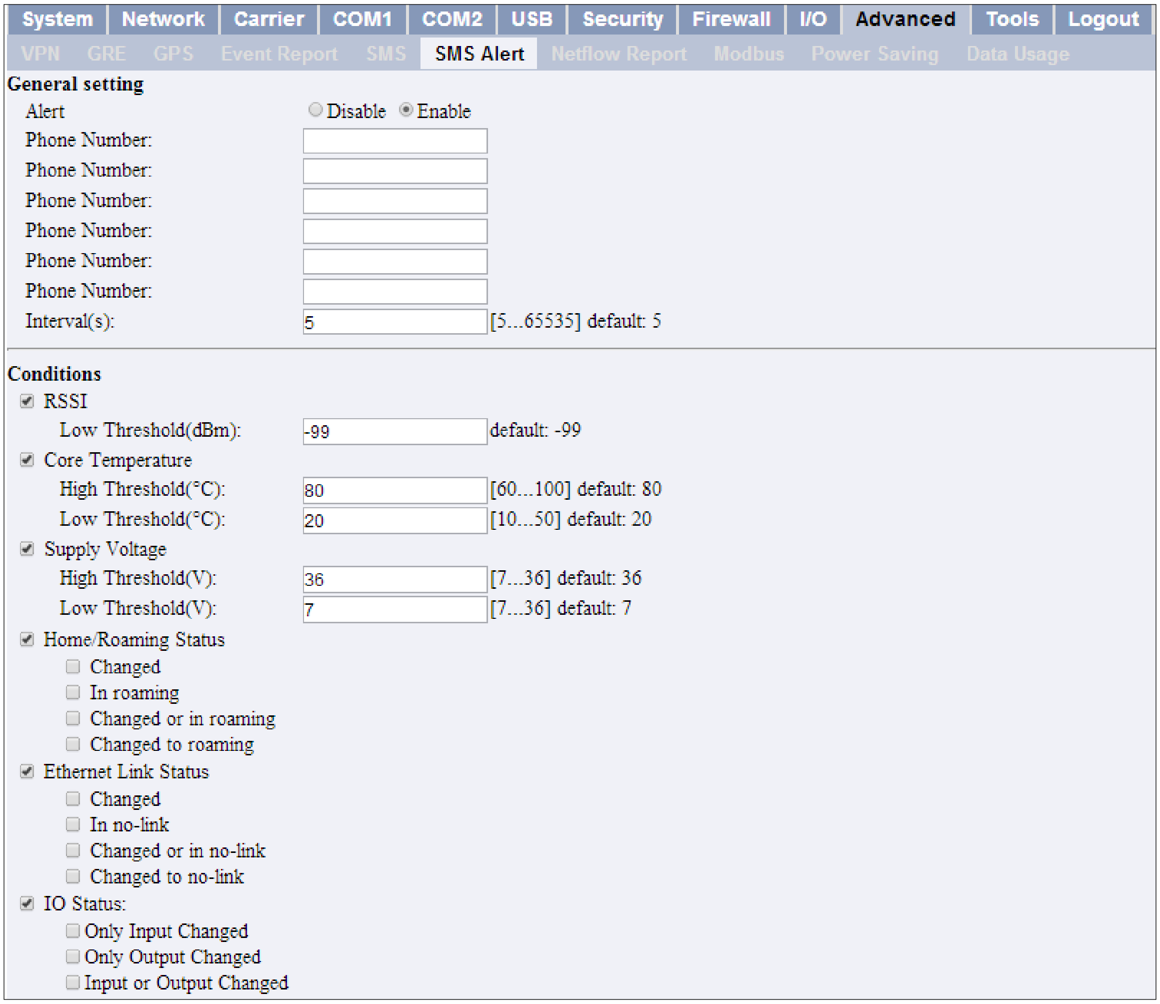
To: +14037103776

```
Use this box to reply!
```

Image 4-65: Advanced > SMS Message Reply

4.10.6 Advanced > SMS Alerts

SMS Alerts can be setup in the IPn3G to report conditions that may affect the integrity of the communications to the modem. This can be used to get alerts before problems become critical and actions can be taken to correct any issues before a complete failure occurs.



General setting

Alert ○ Disable ● Enable

Phone Number:

Phone Number:

Phone Number:

Phone Number:

Phone Number:

Phone Number:

Interval(s): 5 [5...65535] default: 5

Conditions

☑ RSSI

Low Threshold(dBm): -99 default: -99

☑ Core Temperature

High Threshold(°C): 80 [60...100] default: 80

Low Threshold(°C): 20 [10...50] default: 20

☑ Supply Voltage

High Threshold(V): 36 [7...36] default: 36

Low Threshold(V): 7 [7...36] default: 7

☑ Home/Roaming Status

□ Changed

□ In roaming

□ Changed or in roaming

□ Changed to roaming

☑ Ethernet Link Status

□ Changed

□ In no-link

□ Changed or in no-link

□ Changed to no-link

☑ IO Status:

□ Only Input Changed

□ Only Output Changed

□ Input or Output Changed

Image 4-66: Advanced > SMS Message List

Alert

Enable / Disable SMS Alerts.

Values (selection)

Disable / Enable

Phone Number

Set up to six (6) different phone numbers to send SMS Alerts.

Values (phone #)

4035550123

Interval (s)

Define how often, in seconds, SMS are sent.

Values (seconds)

5 - 65535

RSSI - Low Threshold

Set the low RSSI threshold. Once the RSSI level drops below this threshold, the IPn3G will begin to send SMS Alerts.

Values (dBm)

-99

Core Temperature (High / Low)

Set the High and Low Core Temperature thresholds, This is the temperature of the actual module, not the air temperature around the modem. Default values are in brackets.

Values (C)

High: 60 - 100 (80)
Low: 10 - 50 (20)

Supply Voltage

Power supply issues may be able to be detected and alerts sent. Default values are in brackets.

Values (V)

High: 7 - 36 (36)
Low: 7 - 36 (7)

Home / Roaming Status

The IPn3G can be configured to send a warning when the unit changes roaming status. This can be critical as often roaming data rates are obscenely expensive.

Values (selection)

Changed / In Roaming
Changed or in roaming
Changed to roaming

Ethernet Link Status

Problems with end devices can be detected by sensing the Ethernet Link Status.

Values (selection)

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

I/O Status

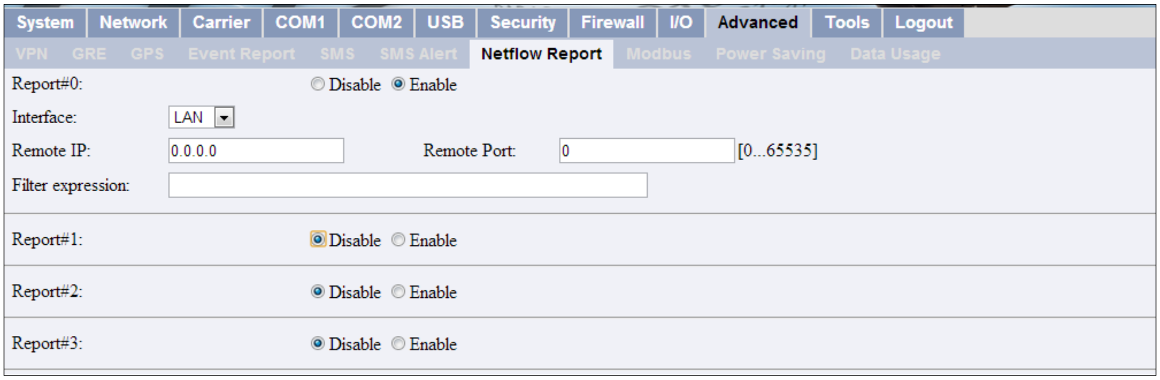
SMS alerts can be triggered by the change in status of the I/O.

Values (selection)

Only Input Changed
Only Output changed
Input or Output Changed

4.10.7 Advanced > Netflow Report

The IPn3G can be configured to send Netflow reports to up to 4 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.



Report#0: ○ Disable ● Enable

Interface: LAN

Remote IP: 0.0.0.0 Remote Port: 0 [0...65535]

Filter expression:

Report#1: ● Disable ○ Enable

Report#2: ● Disable ○ Enable

Report#3: ● Disable ○ Enable

Image 4-67: Advanced > Netflow Reports

Report#

Enable / Disable Netflow Reporting.

Values (selection)

Disable / Enable

Interface

Select between WAN (3G) and LAN interfaces, or capture data from all interfaces.

Values (selection)

LAN / WAN / ALL

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**

Values (chars)

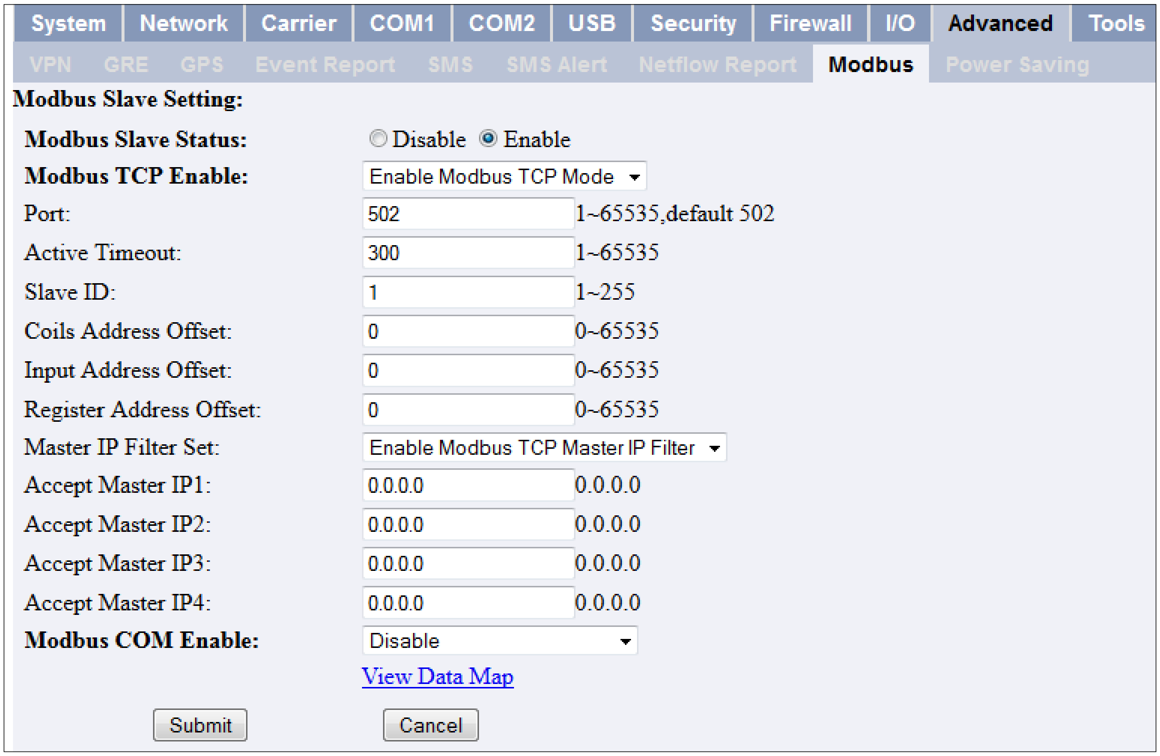
(no default)

The "tcpdump" manual, available on the internet provides detailed expression syntax.

4.10.8 Advanced > Modbus

4.10.8.1 Modbus > TCP Modbus

The IPn3G 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.



Modbus Slave Setting:

Modbus Slave Status:	○ Disable ● Enable	
Modbus TCP Enable:	Enable Modbus TCP Mode	
Port:	502	1~65535,default 502
Active Timeout:	300	1~65535
Slave ID:	1	1~255
Coils Address Offset:	0	0~65535
Input Address Offset:	0	0~65535
Register Address Offset:	0	0~65535
Master IP Filter Set:	Enable Modbus TCP Master IP Filter	
Accept Master IP1:	0.0.0.0	0.0.0.0
Accept Master IP2:	0.0.0.0	0.0.0.0
Accept Master IP3:	0.0.0.0	0.0.0.0
Accept Master IP4:	0.0.0.0	0.0.0.0
Modbus COM Enable:	Disable	

Image 4-68: Advanced > Modbus TCP Setup

Modbus Slave Status

Disable or enable TCP and Serial Modbus services on the IPn3G.

Values (selection)

Disable
Enable

Modbus TCP Enable

Enable or disable TCP Modbus on the IPn3G.

Values (selection)

Disable
Enable Modbus TCP Mode

Port

Enter the port number on the IPn3G in which to listen for incoming Modbus messages.

Values (Port #)

502

Active Timeout

Define the active timeout in seconds.

Values (seconds)

300

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

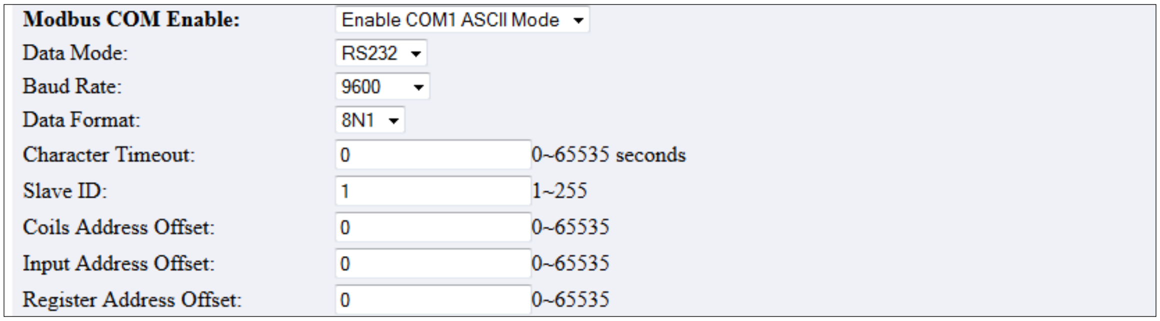
It is possible to only accept connections from specific Modbus Master IP's, to use this feature enable the Master IP Filter and specify the IP Addresses in the fields provided.

Values (selection)

Disable / Enable

4.10.8.2 Modbus > COM (Serial) Modbus

The IPn3G can also participate in serial based Modbus, to configure and view the serial Modbus settings, the COM1 port must first be disabled in the ***COM1 > Settings*** menu. Only the settings that are different from TCP Modbus will be discussed.



Modbus COM Enable:	Enable COM1 ASCII Mode	
Data Mode:	RS232	
Baud Rate:	9600	
Data Format:	8N1	
Character Timeout:	0	0~65535 seconds
Slave ID:	1	1~255
Coils Address Offset:	0	0~65535
Input Address Offset:	0	0~65535
Register Address Offset:	0	0~65535

Image 69: Advanced > 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

Data Mode

Determines which (rear of unit) serial interface shall be used to connect to external devices: RS232, RS485, or RS422. This option applies only to COM1. When an interface other than RS232 is selected, the DE9 port will be inactive.

Values (selection)

RS232
RS485
RS422

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

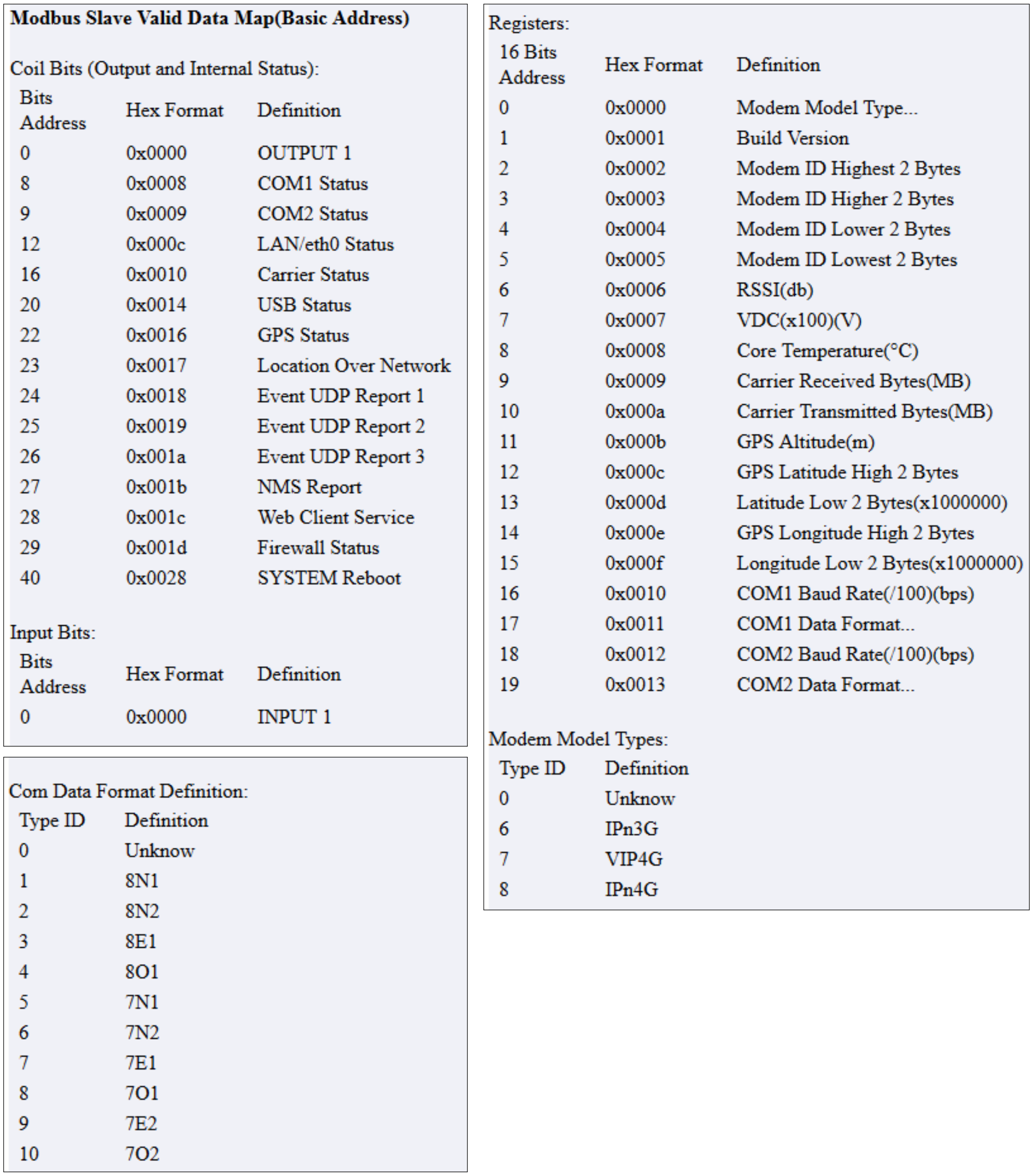
Data Format

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
8N2
8E1
8O1
7N1
7N2
7E1
7O1
7E2
7O2

4.10.8.3 Modbus > Modbus Data Map



Modbus Slave Valid Data Map(Basic Address)

Coil Bits (Output and Internal Status):

Bits Address	Hex Format	Definition
0	0x0000	OUTPUT 1
8	0x0008	COM1 Status
9	0x0009	COM2 Status
12	0x000c	LAN/eth0 Status
16	0x0010	Carrier Status
20	0x0014	USB 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
29	0x001d	Firewall Status
40	0x0028	SYSTEM Reboot

Input Bits:

Bits Address	Hex Format	Definition
0	0x0000	INPUT 1

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

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(db)
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)
16	0x0010	COM1 Baud Rate(/100)(bps)
17	0x0011	COM1 Data Format...
18	0x0012	COM2 Baud Rate(/100)(bps)
19	0x0013	COM2 Data Format...

Modem Model Types:

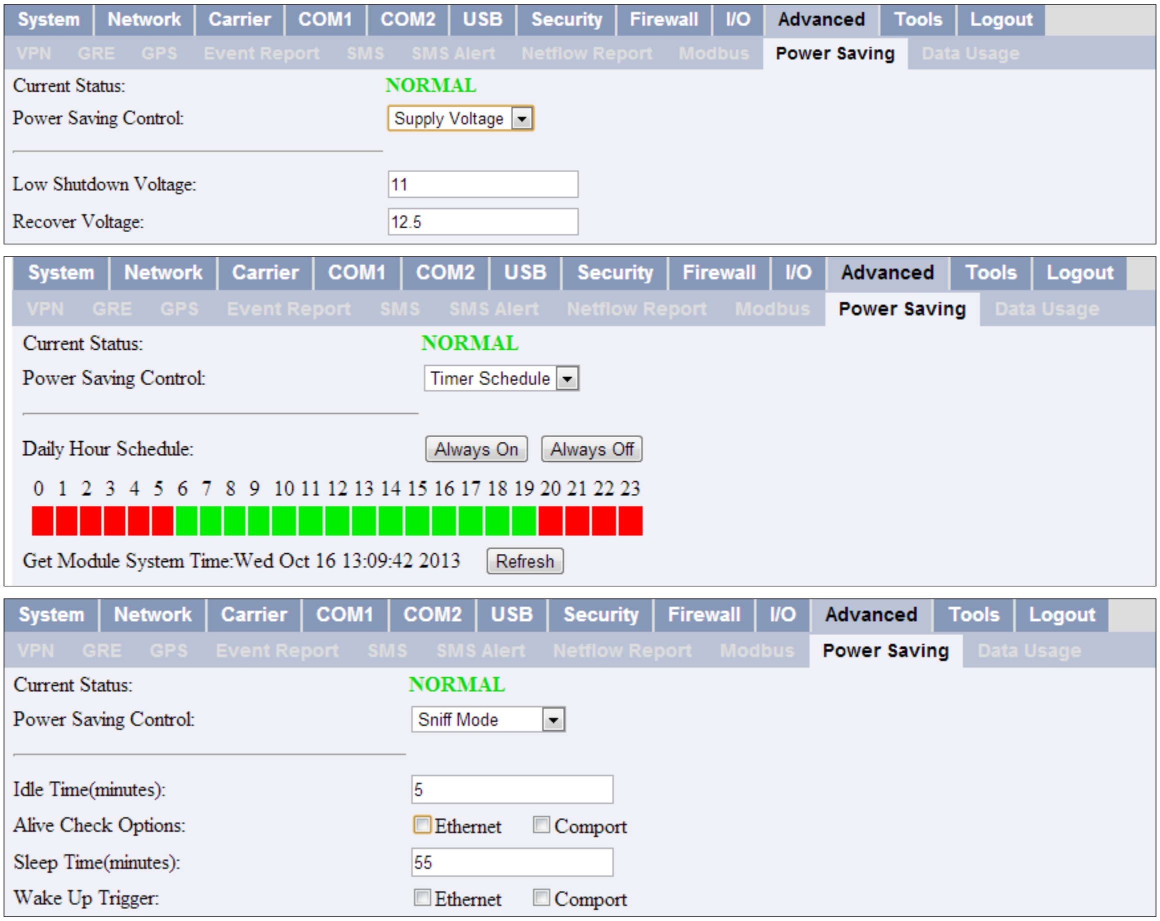
Type ID	Definition
0	Unknow
6	IPn3G
7	VIP4G
8	IPn4G

Image 70: Advanced > Modbus Data Map

4.10.9 Advanced > Power Saving

Various power saving options are available in the IPn3G. The IPn3G can be put into power saving mode by either using the input voltage, a simple timer, or by sensing incoming local data.

The power saving mode can be enabled/switched using System SMS Commands.



Current Status: NORMAL
Power Saving Control: Supply Voltage
Low Shutdown Voltage: 11
Recover Voltage: 12.5

Current Status: NORMAL
Power Saving Control: Timer Schedule
Daily Hour Schedule: Always On Always Off

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥

Get Module System Time:Wed Oct 16 13:09:42 2013 Refresh

Current Status: NORMAL
Power Saving Control: Sniff Mode
Idle Time(minutes): 5
Alive Check Options: □ Ethernet □ Comport
Sleep Time(minutes): 55
Wake Up Trigger: □ Ethernet □ Comport

Image 4-71: Advanced > Power Saving Options

Power Saving Control

Select the desired power saving mode for the IPn3G. Note that while in power saving mode (asleep), the unit cannot be reached remotely using the WAN IP address.

Supply Voltage Mode - The IPn3G will go into power saving mode when the voltage supplied to the IPn3G drops below a specified value. The unit will return to normal operation once the recovery threshold is crossed.

Timer Schedule - The IPn3G can go into power saving modes at specific time intervals on hourly intervals.

Sniff Mode - The IPn3G will enter power saving mode after the Idle time has expired until the sleep timer expires, unless woken up by data being detected on the Ethernet and/or Serial com port.

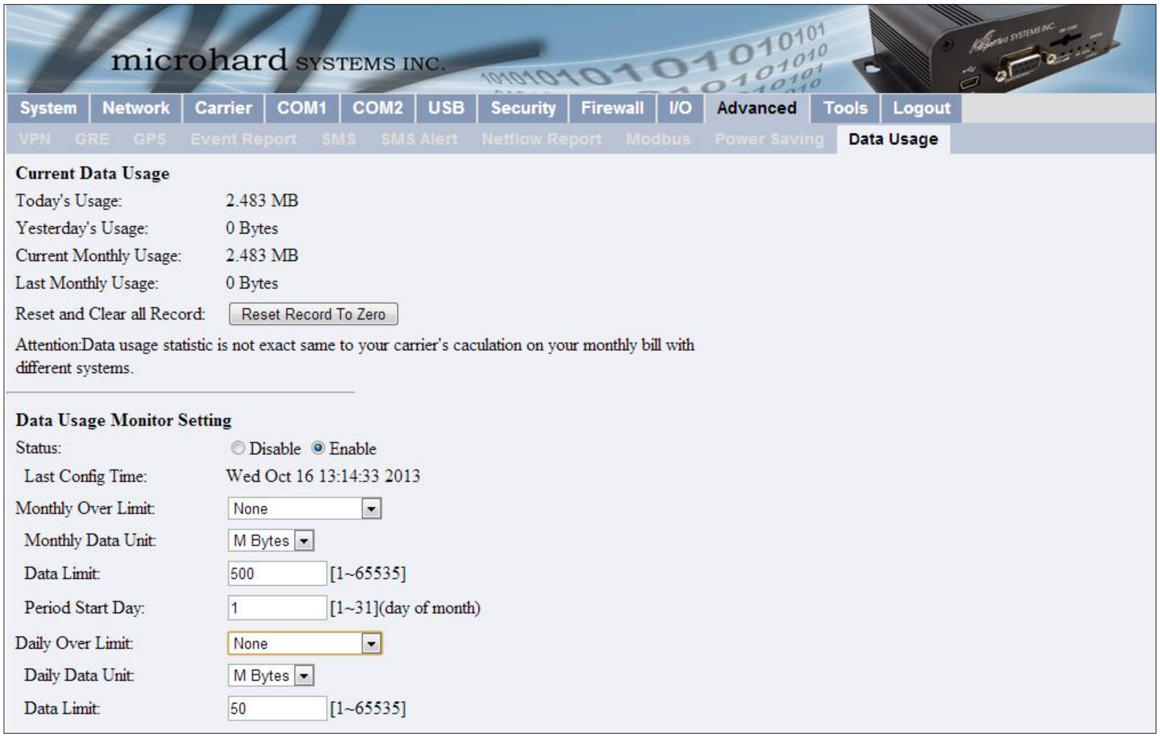
Values (selection)

Disable
Supply Voltage
Timer Schedule
Sniff Mode

4.0 WebUI Configuration

4.10.10 Advanced > Data Usage

The Data Usage tool on the IPn3G 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 IPn3G.



Current Data Usage

Today's Usage: 2.483 MB
Yesterday's Usage: 0 Bytes
Current Monthly Usage: 2.483 MB
Last Monthly Usage: 0 Bytes
Reset and Clear all Record:

Attention:Data usage statistic is not exact same to your carrier's caculation on your monthly bill with different systems.

Data Usage Monitor Setting

Status: ○ Disable ● Enable
Last Config Time: Wed Oct 16 13:14:33 2013
Monthly Over Limit: None
Monthly Data Unit: M Bytes
Data Limit: 500 [1~65535]
Period Start Day: 1 [1~31](day of month)
Daily Over Limit: None
Daily Data Unit: M Bytes
Data Limit: 50 [1~65535]

Image 4-72: Advanced > Data Usage

Status

If enabled the IPn3G will track the amount of cellular data consumed. If disabled, data is not recorded, even in the Current Data Usage display.

Values (selection)

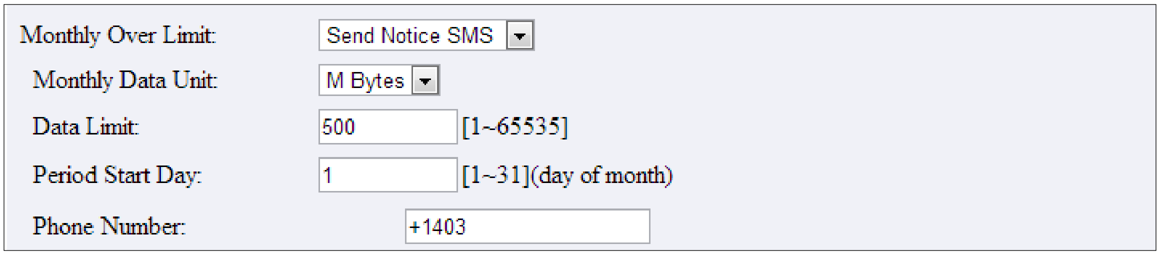
Disable
Enable

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



Monthly Over Limit:	Send Notice SMS
Monthly Data Unit:	M Bytes
Data Limit:	500 [1~65535]
Period Start Day:	1 [1~31](day of month)
Phone Number:	+1403

Image 4-73: Advanced > 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 IPn3G will reset the data usage monitor numbers.

Values (1-31)

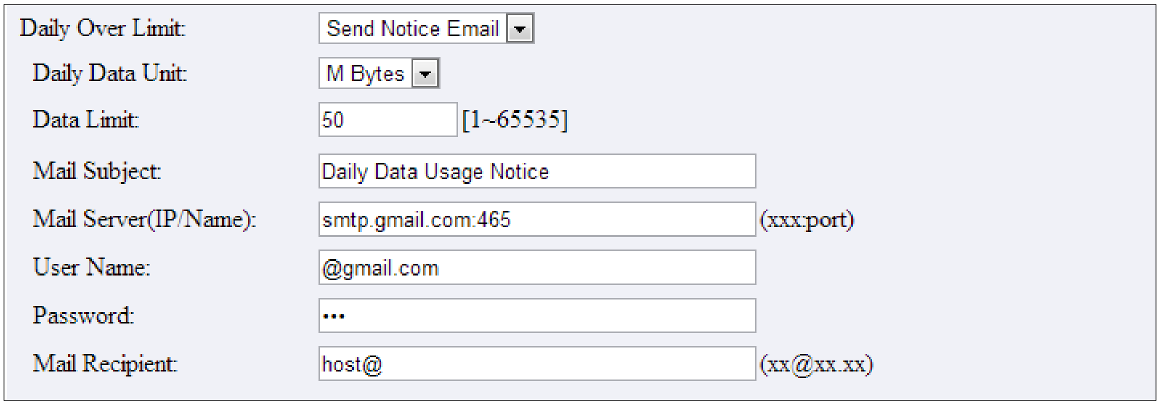
1 (Day of Month)

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



Daily Over Limit:	Send Notice Email
Daily Data Unit:	M Bytes
Data Limit:	50 [1~65535]
Mail Subject:	Daily Data Usage Notice
Mail Server(IP/Name):	smtp.gmail.com:465 (xxx:port)
User Name:	@gmail.com
Password:	•••
Mail Recipient:	host@ (xx@xx.xx)

Image 4-74: Advanced > 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)

****

Mail Recipient

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

Values (xx@xx.xx)

host@

4.11 Tools

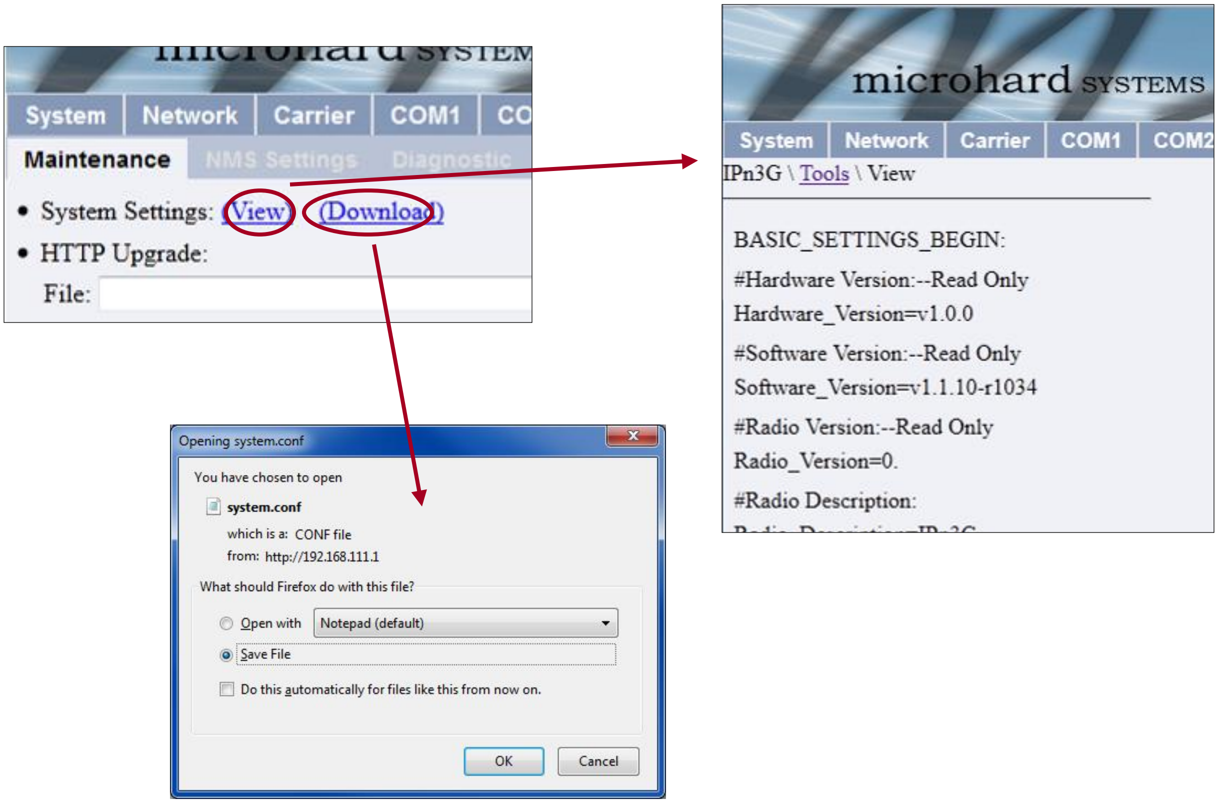
4.11.1 Tools > Maintenance > System Settings

The System Settings menu allows a user to view all system settings using the ***System Settings 'View'*** option. Selecting '*Download'* affords the opportunity to download the various values to a "system.conf" text file. This file may be useful for reference or requested by Microhard Support to aid in any required troubleshooting or application analysis. The file can also be modified and uploaded back to the IPn3G, or used as a template.

4.11.1.1 Backup Configuration Settings (WebUI)

Under ***System Settings*** selecting View will dump the configuration file to the screen, and selecting Download will allow a text file to be downloaded to a PC for use as a backup or template. The name of the file is the "system.conf" file.

A sample "system.conf" file can be found under ***Appendix E: "system.conf" File Structure***.



- System Settings: (View) (Download)
- HTTP Upgrade:

File:

IPn3G \ Tools \ View

```
BASIC_SETTINGS_BEGIN:
#Hardware Version:--Read Only
Hardware_Version=v1.0.0
#Software Version:--Read Only
Software_Version=v1.1.10-r1034
#Radio Version:--Read Only
Radio_Version=0.
#Radio Description:
```

Opening system.conf

You have chosen to open

system.conf

which is a: CONF file

from: http://192.168.111.1

What should Firefox do with this file?

○ Open with Notepad (default)

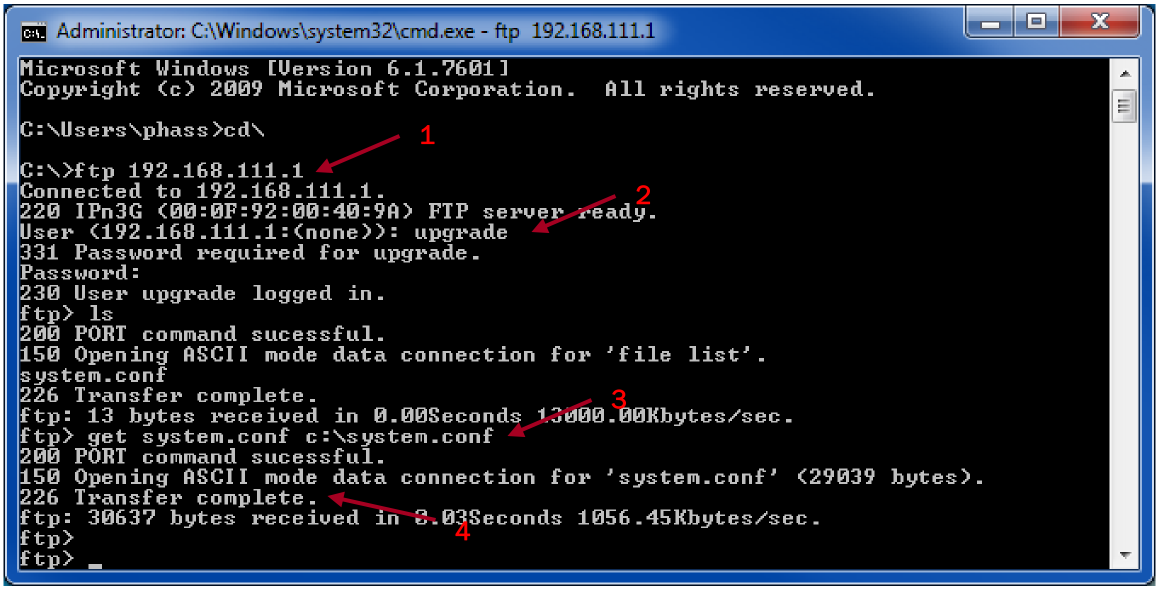
● Save File

□ Do this automatically for files like this from now on.

Image 4-75: Tools > Maintenance > Configuration Backup (WebUI)

4.11.1.2 Backup Configuration Settings (FTP)

An FTP session can also be used to get the configuration file from the IPn3G. The following procedure can be used:



Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.111.1

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\phass>cd\

C:\>ftp 192.168.111.1
Connected to 192.168.111.1.
220 IPn3G (00:0F:92:00:40:9A) FTP server ready.
User (192.168.111.1:(none)): upgrade
331 Password required for upgrade.
Password:
230 User upgrade logged in.
ftp> ls
200 PORT command sucessful.
150 Opening ASCII mode data connection for 'file list'.
system.conf
226 Transfer complete.
ftp: 13 bytes received in 0.00Seconds 13000.00Kbytes/sec.
ftp> get system.conf c:\system.conf
200 PORT command sucessful.
150 Opening ASCII mode data connection for 'system.conf' (29039 bytes).
226 Transfer complete.
ftp: 30637 bytes received in 0.03Seconds 1056.45Kbytes/sec.
ftp>
ftp> _
```

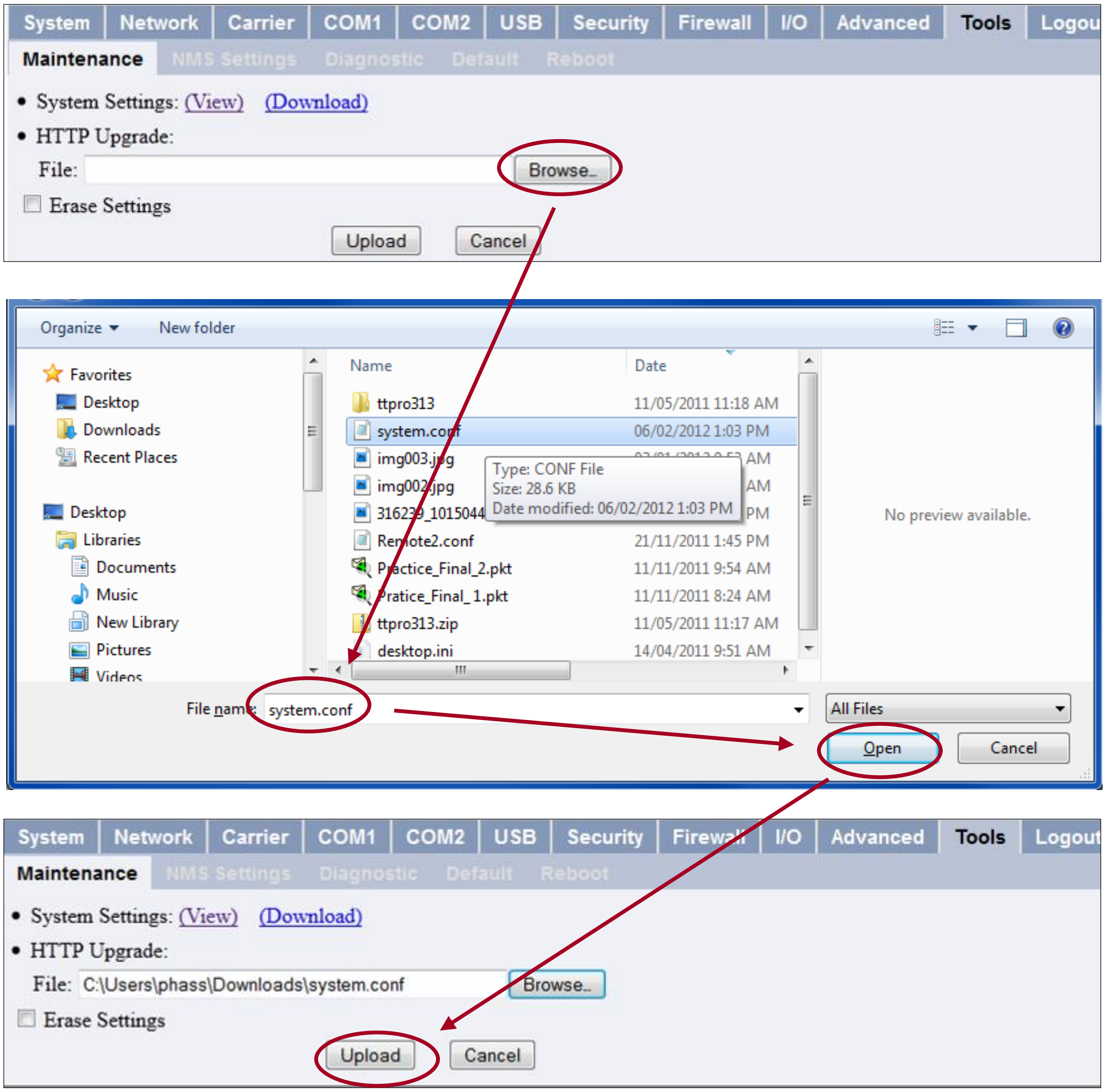
Image 4-76: Tools > Maintenance > Configuration Backup (FTP)

1. From a DOS command prompt, start a FTP session with the IPn3G, you can FTP to the USB NDIS IP Address, the LAN IP Address, and if the firewall settings allow, the WAN IP Address. The example uses the USB NDIS Interface address:
2. Login using the username: ***upgrade*** and the password: ***admin***
3. “Get” the file by specifiying the filename “system.conf” and the destination and destination filename (use system.conf). In the example just the root directory of the PC is being used, so the destination is c:\system.conf,
4. The Transfer should show as complete.
5. Navigate to the destination indicated on the PC and move/copy/edit as required.

4.11.1.3 Restoring Configuration Settings

A system.conf file can be uploaded to the IPn3G to restore previous settings or as a template to aid in configuration of multiple units that have similar settings. ***The filename must be "system.conf" or an error message will be reported by the IPn3G.***

To upload a "system.conf" file, click the browse button on the File: path selection bar under HTTP Upgrade. Select the "system.conf" file that is to be uploaded to the IPn3G, and then click the upload button. The setting will be loaded on the IPn3G and the unit will immediately reboot.



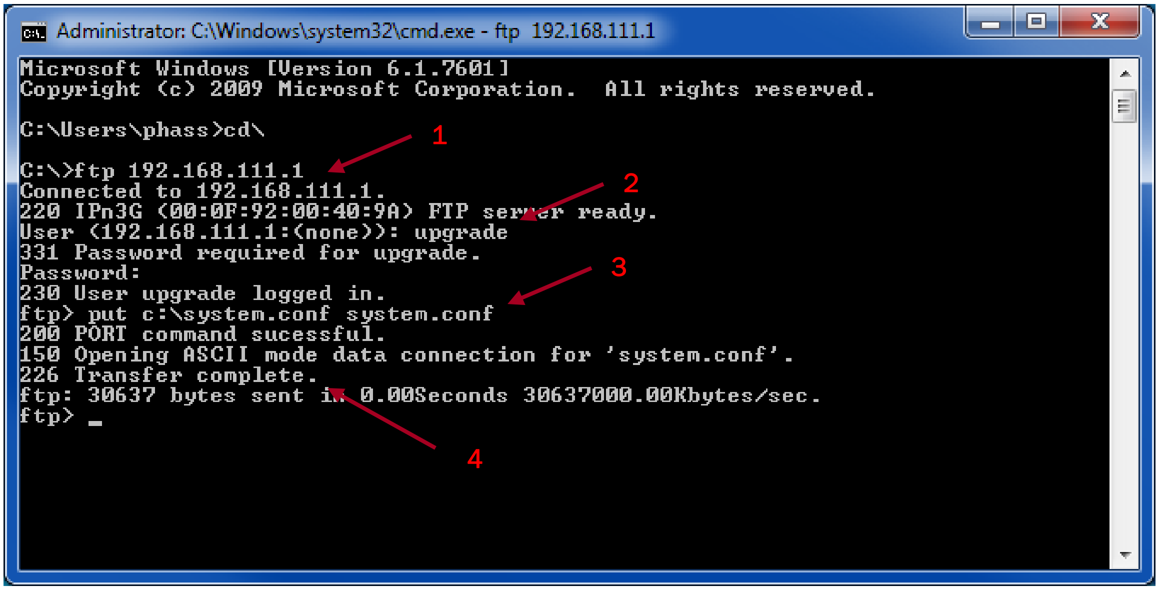
File name: system.conf

File: C:\Users\phass\Downloads\system.conf

Image 4-77: Tools > Maintenance > Configuration Restore (WebUI)

4.11.1.4 Restoring Configuration Settings (FTP)

A system.conf file can be also be uploaded to the IPn3G using FTP as seen below:



Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.111.1
1
2
3
4

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\phass>cd\

C:\>ftp 192.168.111.1
Connected to 192.168.111.1.
220 IPn3G (00:0F:92:00:40:9A) FTP server ready.
User (192.168.111.1:(none)): upgrade
331 Password required for upgrade.
Password:
230 User upgrade logged in.
ftp> put c:\system.conf system.conf
200 PORT command sucessful.
150 Opening ASCII mode data connection for 'system.conf'.
226 Transfer complete.
ftp: 30637 bytes sent in 0.00Seconds 30637000.00Kbytes/sec.
ftp> _
```

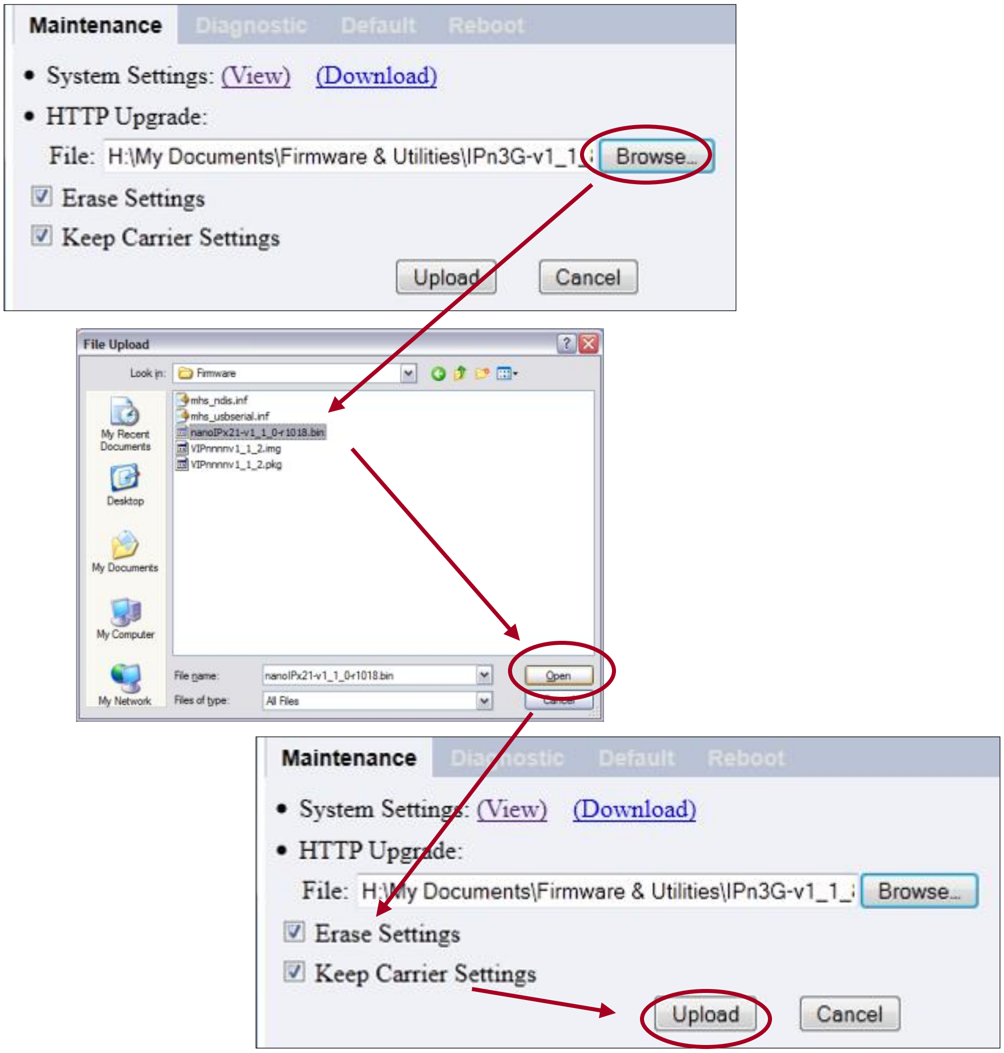
Image 4-78: Tools > Maintenance > Configuration Backup (FTP)

1. From a DOS command prompt, start a FTP session with the IPn3G, you can FTP to the USB NDIS IP Address (192.168.111.1), the LAN IP Address (192.168.0.1), and if the firewall settings allow, the WAN IP Address. The example uses the USB NDIS Interface address. It is recommended to navigate to the folder (in DOS) in which the system.conf is located and launch the FTP session from there.
2. Login using the username: ***upgrade*** and the password: ***admin***
3. "put" the file by specifying the location of the source file "c:\system.conf" and the destination filename (it has to be "system.conf"). In the example just the root directory of the PC is being used, so the source is c:\system.conf,
4. The Transfer should show as complete.
5. The unit will reboot with the settings specified in the system.conf file.

4.0 WebUI Configuration

4.11.1.5 Firmware Upgrades

HTTP Upgrade is used to upgrade the IPn3G 's system software (firmware). Select the Browse button to locate the upgrade file provided my Microhard Systems.



- System Settings: (View) (Download)
- HTTP Upgrade:

File: H:\My Documents\Firmware & Utilities\IPn3G-v1_1_

☑ Erase Settings

☑ Keep Carrier Settings

File Upload

Look in: Firmware

mhs_ndis.inf
mhs_usbserial.inf
nanoIPx21-v1_1_0-r1018.bin
VIPnnnnv1_1_2.img
VIPnnnnv1_1_2.pkg

File name: nanoIPx21-v1_1_0-r1018.bin

Files of type: All Files

Image 4-79: Tools > Maintenance > WebUI Firmware Upload

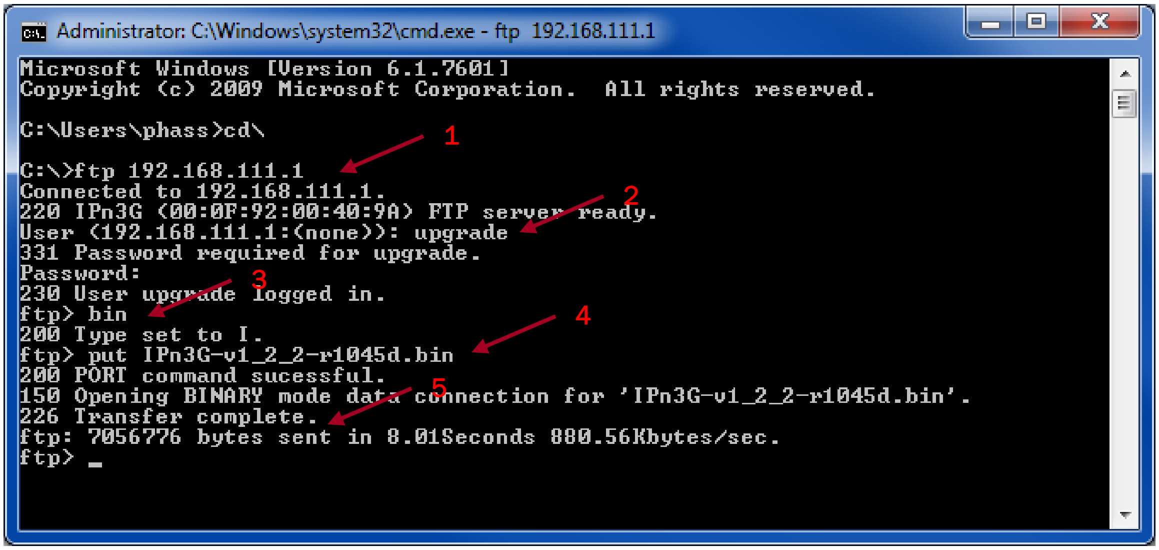
Using the ***Erase Settings*** checkbox tells the IPn3G not to store the current configuration settings, therefore once the upgrade process is complete the unit will have factory default settings (Including the default Carrier Settings).

Use the ***Keep Carrier Settings*** checkbox to retain the carrier settings. This is recommended if the unit is remote as all access will be lost if the carrier settings are erased.

The Upload button will begin the process. It can take several minutes to complete. The unit will reboot once the upgrade process is complete.

4.11.1.6 Firmware Upgrades (FTP)

FTP can also be used to upgrade the system firmware as seen below:


Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.111.1
1
2
3
4
5

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\phass>cd\

C:\>ftp 192.168.111.1
Connected to 192.168.111.1.
220 IPn3G (00:0F:92:00:40:9A) FTP server ready.
User (192.168.111.1:(none)): upgrade
331 Password required for upgrade.
Password:
230 User upgrade logged in.
ftp> bin
200 Type set to I.
ftp> put IPn3G-v1_2_2-r1045d.bin
200 PORT command sucessful.
150 Opening BINARY mode data connection for 'IPn3G-v1_2_2-r1045d.bin'.
226 Transfer complete.
ftp: 7056776 bytes sent in 8.01Seconds 880.56Kbytes/sec.
ftp> _
```

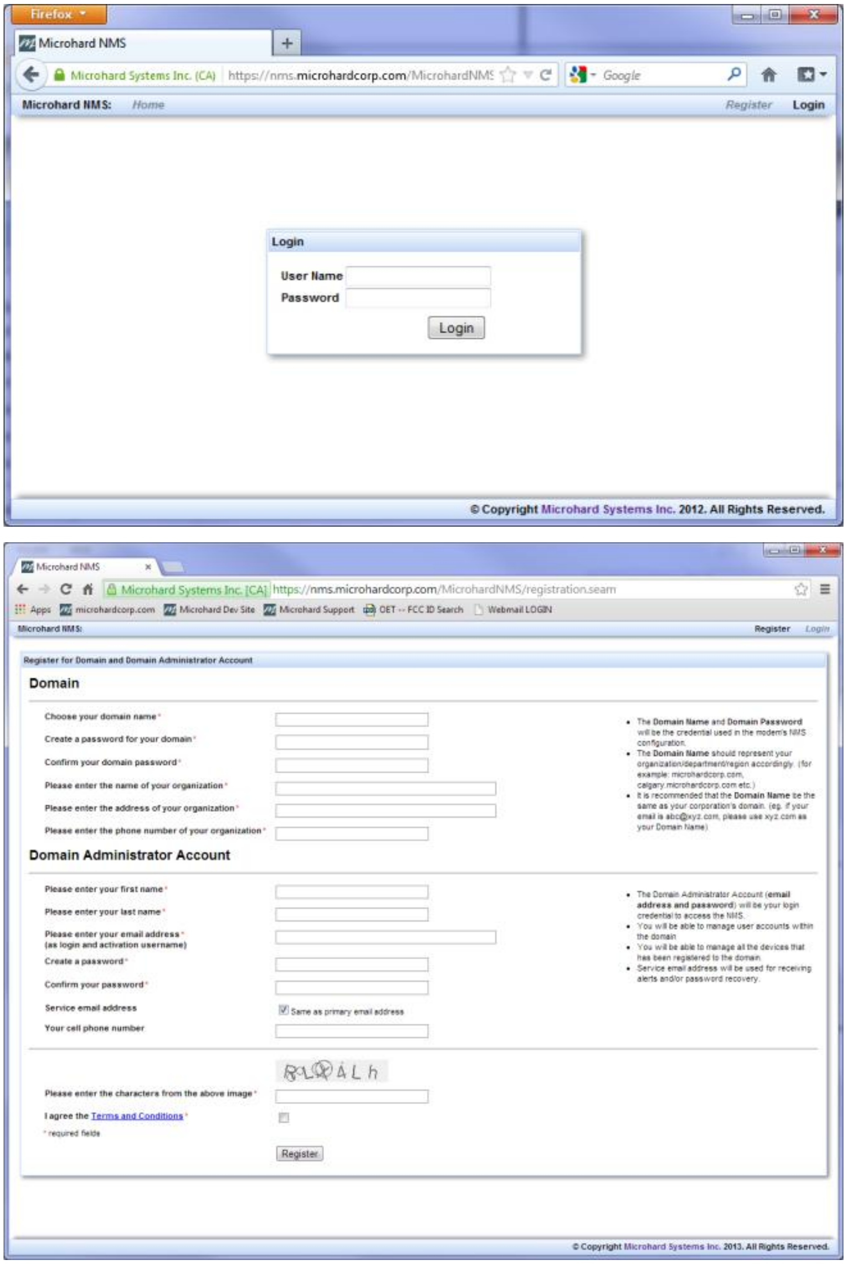
Image 4-80: Tools > Maintenance > Firmware Upgrade (FTP)

1. From a DOS command prompt, start a FTP session with the IPn3G, you can FTP to the USB NDIS IP Address (192.168.111.1), the LAN IP Address (192.168.0.1), and if the firewall settings allow, the WAN IP Address. The example uses the USB NDIS Interface address. It is recommended to navigate to the folder (in DOS) in which the firmware file is located and launch the FTP session from there.
2. Login using the username: ***upgrade*** and the password: ***admin***
3. Since the firmware files are in binary format, the bin command must be issued to the IPn3G to but it into binary transfer mode.
4. "put" the file by specifying the complete filename of the firmware file.
5. The Transfer should show as complete.
6. The unit will reboot with the new firmware.

4.11.2 Tools > 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 IPn3G 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.


Firefox
Microhard NMS
Microhard Systems Inc. (CA) https://nms.microhardcorp.com/MicrohardNMS
Google
Microhard NMS: Home
Register Login

Login

User Name

Password

Login

© Copyright Microhard Systems Inc. 2012. All Rights Reserved.

Microhard NMS
Microhard Systems Inc. [CA] https://nms.microhardcorp.com/MicrohardNMS/registration.seam
Apps microhardcorp.com Microhard Dev Site Microhard Support OET -- FCC ID Search Webmail LOGIN
Microhard NMS:
Register Login

Register for Domain and Domain Administrator Account

Domain

Choose your domain name *

Create a password for your domain *

Confirm your domain password *

Please enter the name of your organization *

Please enter the address of your organization *

Please enter the phone number of your organization *

- The **Domain Name** and **Domain Password** will be the credential used in the modem's NMS configuration.
- The **Domain Name** should represent your organization/department/region accordingly. (for example: microhardcorp.com, calgary.microhardcorp.com etc.)
- It is recommended that the **Domain Name** be the same as your corporation's domain. (eg. if your email is abc@xyz.com, please use xyz.com as your Domain Name)

Domain Administrator Account

Please enter your first name *

Please enter your last name *

Please enter your email address *
(as login and activation username)

Create a password *

Confirm your password *

Service email address ☑ Same as primary email address

Your cell phone number

- The Domain Administrator Account (**email address and password**) will be your login credential to access the NMS.
- You will be able to manage user accounts within the domain
- You will be able to manage all the devices that has been registered to the domain
- Service email address will be used for receiving alerts and/or password recovery.

Please enter the characters from the above image *

I agree the Terms and Conditions * □

* required fields

Register

© Copyright Microhard Systems Inc. 2013. All Rights Reserved.

Image 4-81: NMS

4.0 WebUI Configuration

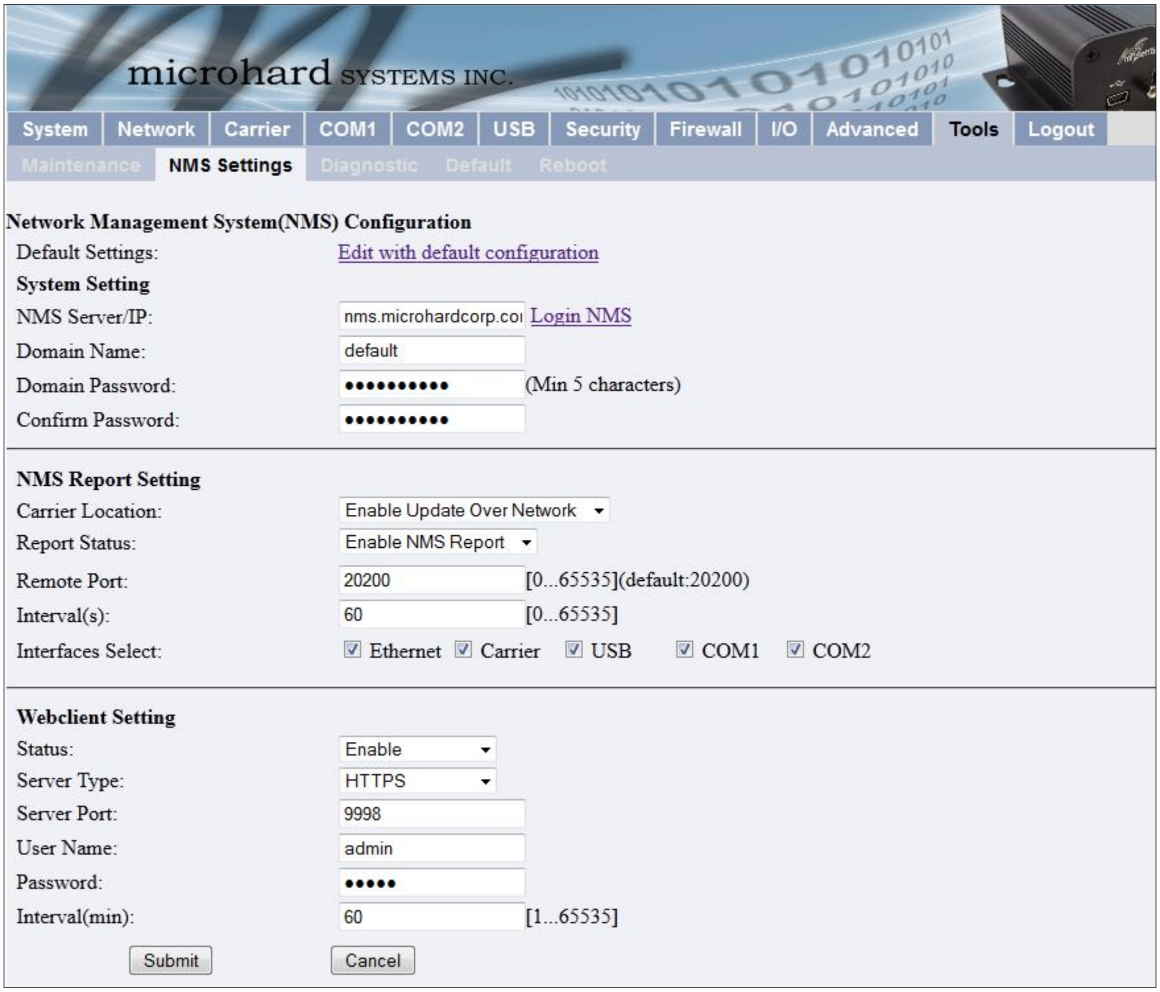
Domain Name: A logical management zone for 3G or 4G devices will report to on NMS, the logged data is separated from any other users that are using NMS. The Domain Name is required in every 3G or 4G device for it to report to right zone. Under this user domain, one can create and manage sub-domain. The 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 IPn3G must be configured to report into NMS.



Network Management System(NMS) Configuration

Default Settings:	Edit with default configuration
System Setting	
NMS Server/IP:	nms.microhardcorp.coı Login NMS
Domain Name:	default
Domain Password:	●●●●●●●●●●● (Min 5 characters)
Confirm Password:	●●●●●●●●●●●
NMS Report Setting	
Carrier Location:	Enable Update Over Network
Report Status:	Enable NMS Report
Remote Port:	20200 [0...65535](default:20200)
Interval(s):	60 [0...65535]
Interfaces Select:	☑ Ethernet ☑ Carrier ☑ USB ☑ COM1 ☑ COM2
Webclient Setting	
Status:	Enable
Server Type:	HTTPS
Server Port:	9998
User Name:	admin
Password:	●●●●●
Interval(min):	60 [1...65535]

Image 4-82: Tools > NMS Settings

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 IPn3G will consume some data to retrieve location information from the internet if GPS data is not valid or available.

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

Interfaces Select

The IPn3G can report information about the different interfaces it has. By default the IPn3G is set to send information about the Carrier, such as usage and RSSI. Statistical and usage data on USB, 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
USB
COM1
COM2

Webclient Setting

Status

The Web Service can be enabled or disabled. This service is used to remotely control the IPn3G. 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 IPn3G 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.

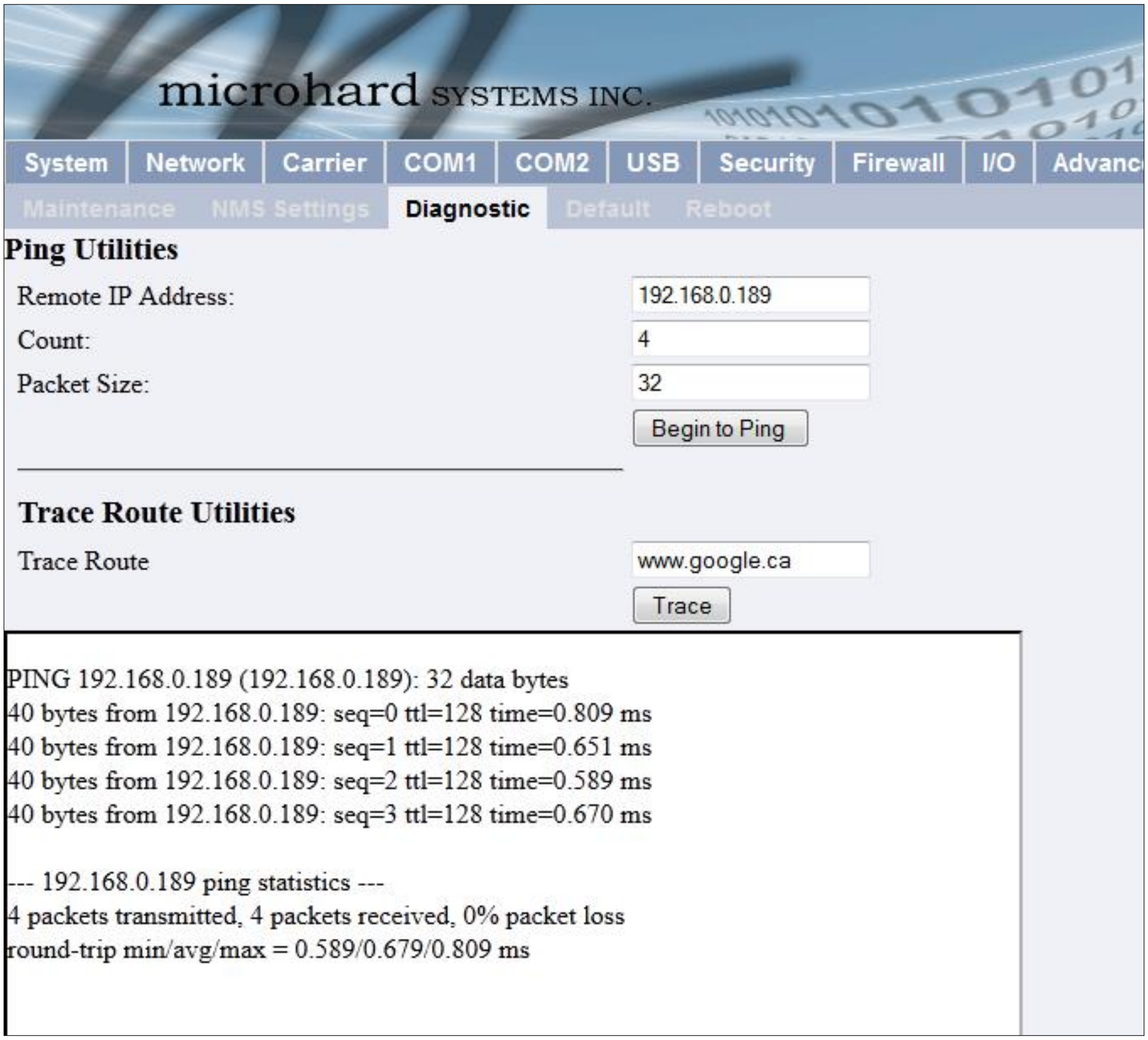
Values (min)

60

4.0 WebUI Configuration

4.11.3 Tools > Diagnostic

The Diagnostic menu provides **Ping** and **Trace Route** tools to use to test connectivity of the IPn3G.



Ping Utilities

Remote IP Address: 192.168.0.189

Count: 4

Packet Size: 32

Trace Route Utilities

Trace Route www.google.ca

```
PING 192.168.0.189 (192.168.0.189): 32 data bytes
40 bytes from 192.168.0.189: seq=0 ttl=128 time=0.809 ms
40 bytes from 192.168.0.189: seq=1 ttl=128 time=0.651 ms
40 bytes from 192.168.0.189: seq=2 ttl=128 time=0.589 ms
40 bytes from 192.168.0.189: seq=3 ttl=128 time=0.670 ms

--- 192.168.0.189 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.589/0.679/0.809 ms
```

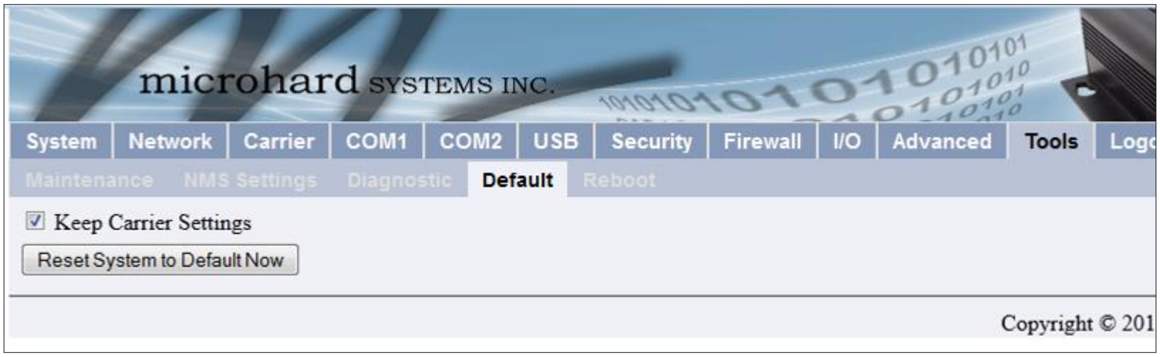
Image 4-83: Diagnostic Utilities

A user can use the Ping command by entering the IP address of destination device in the **Remote IP Address**, use **Count** for the number of ping messages to send, and the **Packet Size** to modify the size of the packets sent.

The **Trace Route** command can also be used to provide connectivity data by providing information about the number of hops, routers and the path taken to reach a particular destination.

4.11.4 Tools > Default

There are many configuration options for the IPn3G units. Should a unit reach a state where it is not performing as desired and it is possible that one or many configuration options may be improperly set, resetting the system to default - essentially back to factory settings - will enable one to take a fresh start in reprogramming the unit.



☑ Keep Carrier Settings

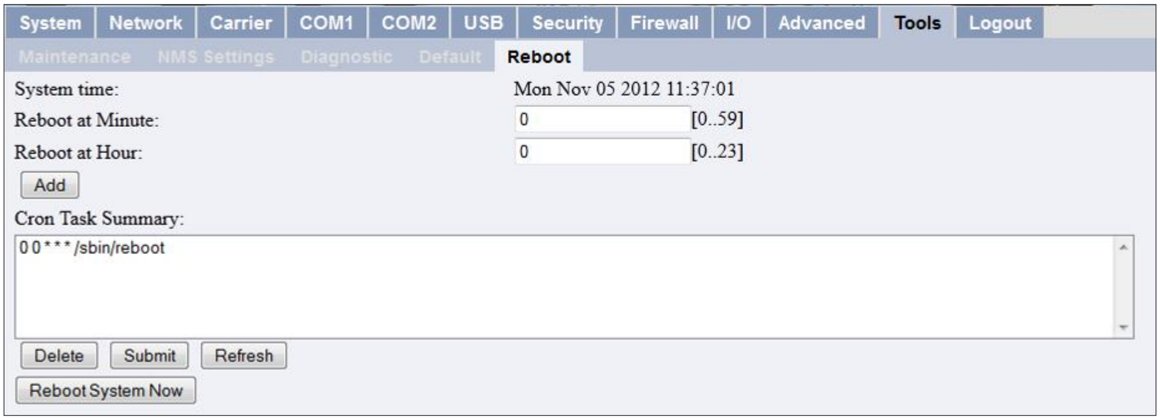
Copyright © 201

Image 4-84: Tools Menu, Reset System to Default

Selecting the 'Keep Carrier Settings' option before resetting the unit to defaults will allow the unit to retain all settings required to establish and maintain a connection with the Cellular Carrier. This is important when resetting a unit to defaults remotely, otherwise the unit will not be reachable and will have to be accessed via a local port for configuration.

4.11.5 Tools > Reboot System

This feature is particularly useful for rebooting remote units and has the same effect as power cycling the unit. Using the supplied interface, It is also possible to reboot the IPn3G on a schedule. Up to 10 tasks can be added to reboot the IPn3G at specific intervals if required. Both the Hour and Minute parameters are required to ensure the feature works as intended.



System time: Mon Nov 05 2012 11:37:01

Reboot at Minute: 0 [0..59]

Reboot at Hour: 0 [0..23]

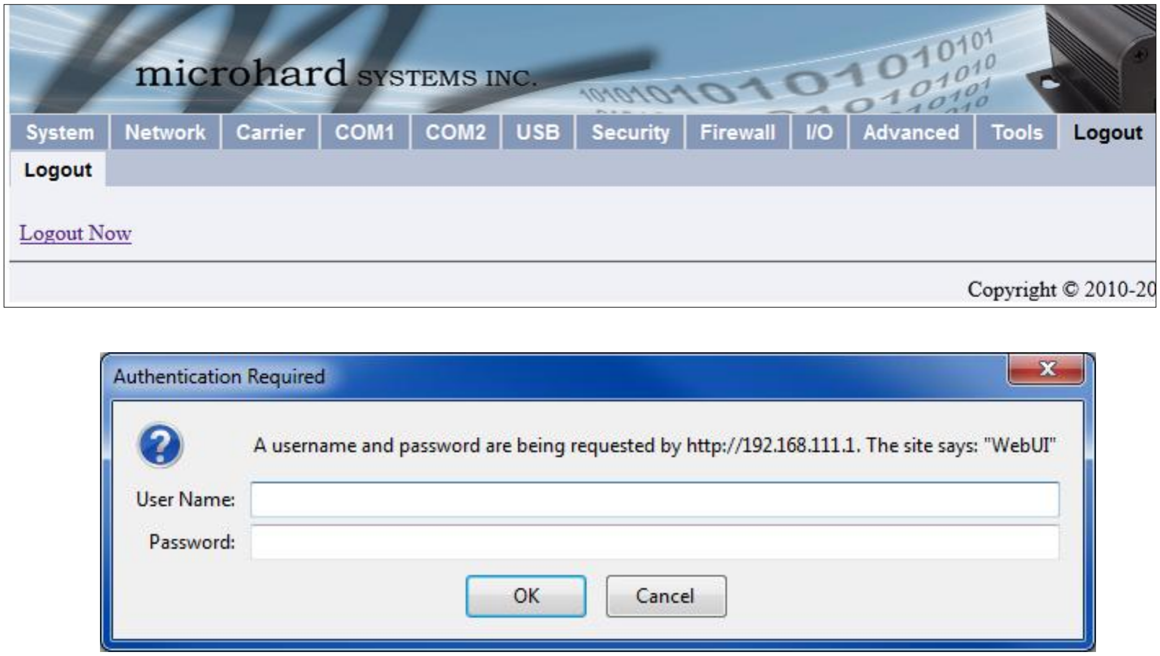
Cron Task Summary:

```
0 0 * * * /sbin/reboot
```

Image 4-85: Tools Menu, Reboot System

4.12 Logout

The Logout menu allows a user to logout of the current session and brings up the logion prompt.



Copyright © 2010-20

Authentication Required

A username and password are being requested by http://192.168.111.1. The site says: "WebUI"

User Name:

Password:

Image 4-86: Logout Window

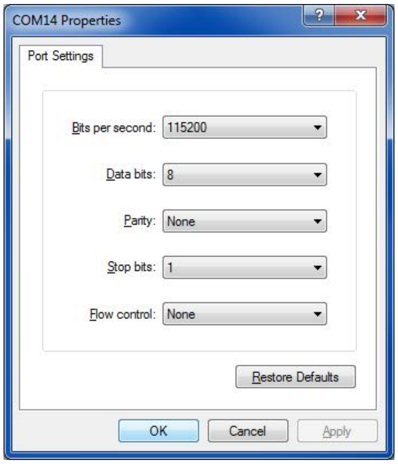
5.0 AT Command Line Interface

5.1 AT Command Overview

AT Commands can be issued to configure and manage the IPn3G, via the front diagnostics port (COM2), or by TCP/IP (telnet). This is only available in software version v1.1.10-r1034c or later. (version info can be found on the bottom of the System > Summary screen in the WebUI.).

5.1.1 Serial Port

To connect and access the AT Command interface on the IPn3G, a physical connection must be made on the RS232 DB9 serial port on the front of the IPn3G labeled ‘Diagnostic’. A terminal emulation program (Hyperterminal, Tera Term, ProComm, Putty etc) can then be used to communicate with the IPn3G. The port settings of this port can be modified by changing the settings of COM2, in the configuration menus.



Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Default Settings:

Baud rate: **115200**

Data bits: **8**

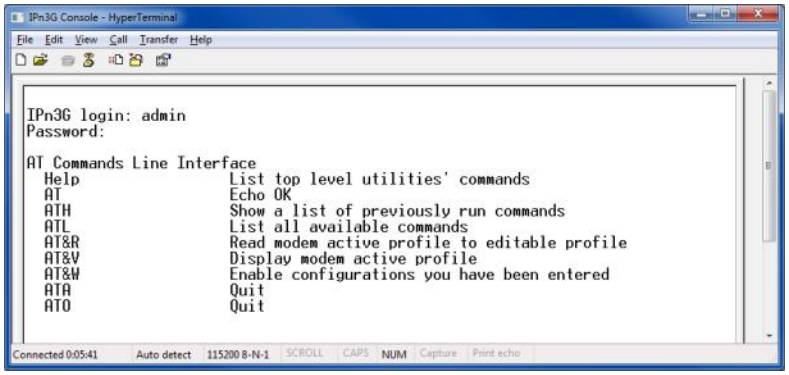
Parity: **None**

Stop Bits: **1**

Flow Control: **None**

Image 5-1: Diagnostic 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.



```
IPn3G login: admin
Password:

AT Commands Line Interface
  Help                  List top level utilities' commands
  AT                    Echo OK
  ATH                   Show a list of previously run commands
  ATL                   List all available commands
  AT&R                  Read modem active profile to editable profile
  AT&V                  Display modem active profile
  AT&W                  Enable configurations you have been entered
  ATA                   Quit
  ATO                   Quit
```

Default Settings:

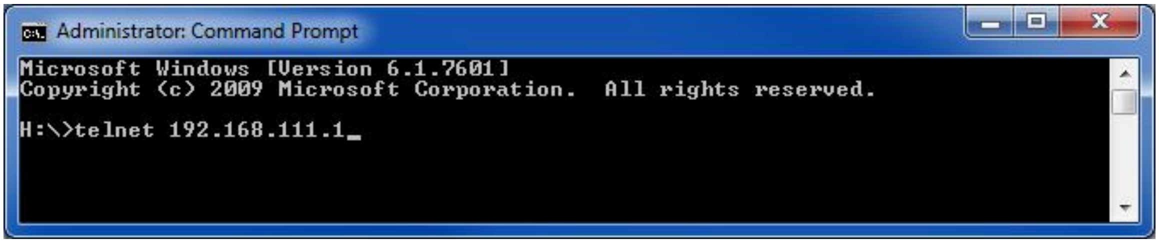
IPn3G login: **admin**

Password: **admin**

Image 5-2: AT Command Window

5.1.2 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the IPn3G. 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.

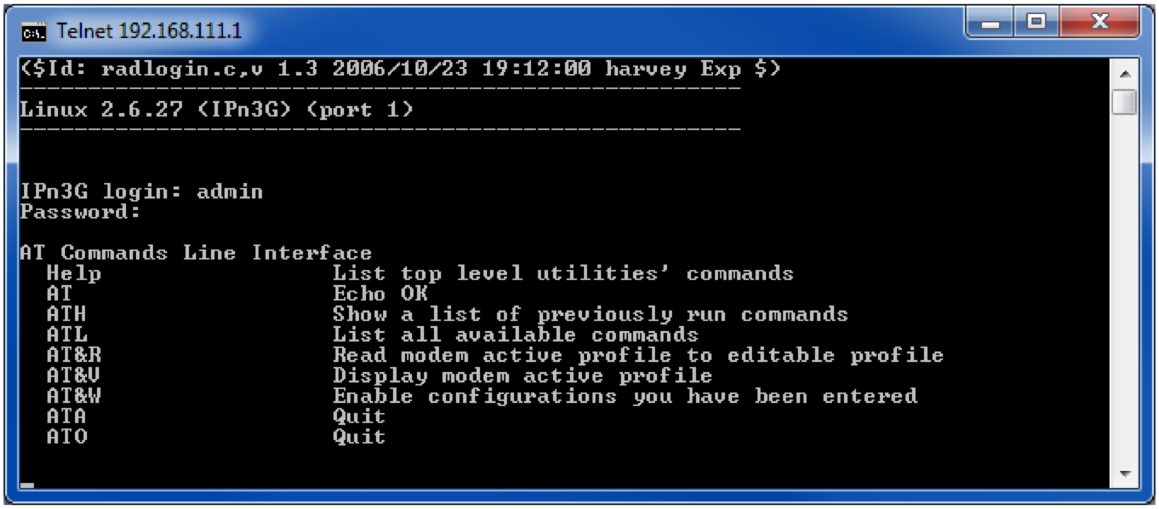


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

H:\>telnet 192.168.111.1_
```

Image 5-3: Establishing a Telnet Session

The screen capture above shows a telnet request being made to the local NDIS port (USB). 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 (default IP: 192.168.0.1).

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.



```
($Id: radlogin.c,v 1.3 2006/10/23 19:12:00 harvey Exp $)
------------------------------------------------------
Linux 2.6.27 (IPn3G) (port 1)
------------------------------------------------------


IPn3G login: admin
Password:

AT Commands Line Interface
  Help                   List top level utilities' commands
  AT                     Echo OK
  ATH                    Show a list of previously run commands
  ATL                    List all available commands
  AT&R                   Read modem active profile to editable profile
  AT&V                   Display modem active profile
  AT&W                   Enable configurations you have been entered
  ATA                    Quit
  ATO                    Quit

_
```

Image 5-4: Telnet AT Command Session

5.2 AT Command Syntax

The follow syntax is used when issuing AT Commands on the IPn3G

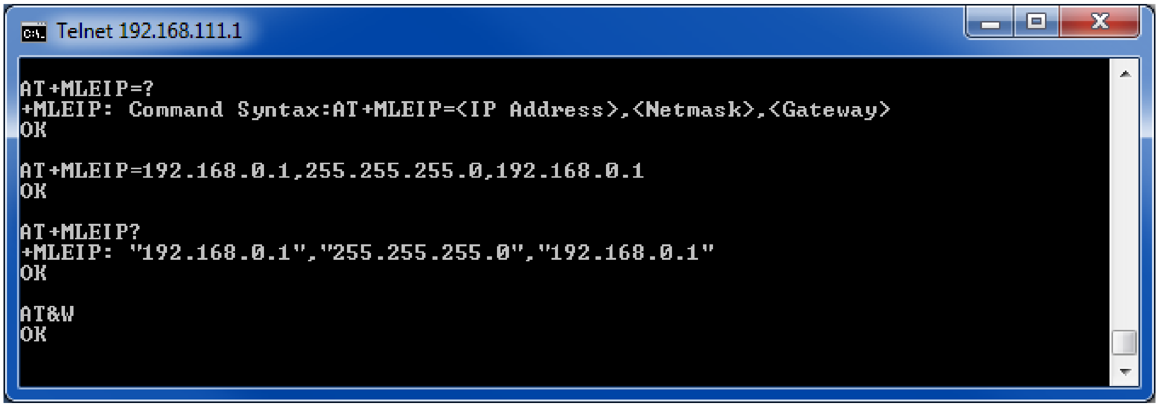
- All commands start with the AT characters and end with the <Enter> key
- Microhard Specific Commands start with +M
- Help will list top level commands (ATL will list ALL available AT Commands)
- To query syntax of a command: AT+<command_name>=?
- Syntax for commands that are used only to query a setting:
  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+MLEIP=? <Enter>
+MLEIP: Command Syntax:AT+MLEIP=<IP Address>,<Netmask>,<Gateway>
OK

Setting a value:
AT+MLEIP=192.168.0.1,255.255.255.0,192.168.0.1 <Enter>
OK

Query a setting:
AT+MLEIP? <Enter>
+MLEIP: “192.168.0.1”, “255.255.255.0”, “192.168.0.1”
OK

A screen capture of the above commands entered into a unit is shown below:



```
AT+MLEIP=?
+MLEIP: Command Syntax:AT+MLEIP=<IP Address>,<Netmask>,<Gateway>
OK

AT+MLEIP=192.168.0.1,255.255.255.0,192.168.0.1
OK

AT+MLEIP?
+MLEIP: "192.168.0.1","255.255.255.0","192.168.0.1"
OK

AT&W
OK
```

Image 5-5: Telnet AT Command Syntax

Once AT commands are entered, they must be saved into the filesystem 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.

5.3 Supported AT Commands

AT

Description

Echo OK.

Command Syntax

AT <enter>

Example

Input:

```
AT <enter>
```

Response:

```
OK
```

ATH

Description

Show a list of previously run commands.

Command Syntax

ATH <enter>

Example

Input:

```
ATH <enter>
```

Response:

```
Command history:
  0. ATL
  1. AT?
  2. AT=?
  3. at
  4. help
  5. AT
  6. □ATL
  7. ATL
  8. ATH
OK
```

AT&R

Description

Read modem profile to editable profile.

Command Syntax

AT&R <enter>

Example

Input:

```
AT&R <enter>
```

Response:

```
OK
```

AT&V

Description	Command Syntax
Read modem active profile.	**AT&V <enter>**

Example

Input:

```
AT&V <enter>
```

Response:

```
BASIC_SETTINGS_BEGIN:


#Hardware Version:–Read Only

Hardware_Version=v2.0.0


#Software Version:–Read Only

Software_Version=v1.2.2-r1045c


#Radio Version:–Read Only

Radio_Version=0.


#Radio Description:

Radio_Description=IPn3G


#Date(yyyy-mm-dd):

System_Date=2012-02-01


#Time(hh:mm:ss):

System_Time=10:41:25
```

<Additional Output Omitted>

5.0 AT Commands

AT&W

Description	Command Syntax
Writes configuration to memory.	**AT&W <enter>**

Example

Input:
AT&W <enter>
Response:
OK

ATA

Description	Command Syntax
Quit. Exits AT Command session and returns you to login prompt.	**ATA <enter>**

The AT&W command must be issued to save changes!

Example

Input:
ATA <enter>
Response:
OK
IPn3G Login:

ATO

Description	Command Syntax
Quit. Exits AT Command session and returns you to login prompt.	**ATO <enter>**

Example

Input:
ATA <enter>
Response:
OK
IPn3G Login:

5.0 AT Commands

AT+MSYSI

Description	Command Syntax
System Summary Information	**AT+MSYSI <enter>**

Example

Input:

```
AT+MSYSI <enter>
```

Response:

```
Carrier:
Current APN:staticip.apn
Activity Status:Call in progress
Network:CANRogersWirelessInc.
Home/Roaming:Home
Cell ID:0x29E2B1
Data Service Type:3G-WCDMA
Channel Number:437
Frequency Band:1900MHz
Ec/No (dB):14
RSSI (dBm):-67
Core Temperature(&deg;C):73
Supply Voltage(V):12.20
IMEI:354626030256080
IMSI:302720406979607
SIM Card:READY
SIM Number (ICCID):89302720401025322275
Phone Number:+15878938645
WAN IP Address:74.198.186.197

DNS1:64.71.255.198

DNS2:64.71.255.253


Ethernet Port:
IP Address:192.168.0.1
IP Subnet Mask:255.255.255.0
IP Gateway:192.168.0.1
Ethernet MAC:00:0F:92:00:40:9A

USB Port:NDIS Mode Standalone
Local IP Address:192.168.111.1
Subnet Mask:255.255.255.0
Host IP:192.168.111.2
USB MAC:00:0F:92:01:40:9A
System:

System time:Wed Feb 01 2012 16:42:03
Hardware Version:v2.0.0
Software Version:v1.2.2-r1045c
OK
```

The AT&W command must be issued to save changes!

5.0 AT Commands

AT+GMR

Description	Command Syntax
Modem Record Information	**AT+GMR <enter>**

Example

Input:
```
AT+GMR <enter>
```
Response:
```
+GMR: Hardware Version:v2.0.0,Software Version:v1.2.2-r1045c,System time:Wed Feb
 01 2012 16:44:17
OK
```

AT+MMNAME

Description	Command Syntax
Modem Name / Radio Description. 30 chars.	**AT+MMNAME=<modem_name>**

The AT&W command must be issued to save changes!

Example

Input: (To set value)
```
AT+MMNAME=IPn3G_CLGY<enter>
```
Response:
```
OK
```

Input: (To retrieve value)
```
AT+MMNAME=?<enter>
```
Response:
```
+MMNAME: IPn3G_CLGY
OK
```

AT+GMI

Description	Command Syntax
Get Manufacturer Identification	**AT+GMI=<enter>**

Example

Input:
```
AT+GMI<enter>
```

Response:
```
+GMI: 2010-2011 Microhard Systems Inc.
OK
```

5.0 AT Commands

AT+CNUM

Description	Command Syntax
Check modem’s phone number.	**AT+CNUM <enter>**

Example

Input:

```
AT+CNUM <enter>
```

Response:

```
+CNUM: "+15875558645"
OK
```

AT+CIMI

Description	Command Syntax
Check modem’s IMEI and IMSI numbers.	**AT+CIMI <enter>**

Example

Input:

```
AT+CIMI <enter>
```

Response:

```
+CIMI: IMEI:354626030256080,IMSI:302720406979607
OK
```

The AT&W command must be issued to save changes!

AT+CCID

Description	Command Syntax
Check modem’s SIM card number.	**AT+CCID=<enter>**

Example

Input:

```
AT+CCID<enter>
```

Response:

```
+CCID: 89302720401025322275
OK
```

AT+MRTF

Description

Reset the modem to the factory default settings stored in non-volatile (NV) memory. Unit will reboot with default settings. Set flag to 1, to save carrier settings, 0 will erase all settings.

Command Syntax

AT+CNUM <action>
Action:
0 no-action (all settings will be erased)
1 save carrier settings

Example

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

AT+MREB

Description

Reboots the modem.

Command Syntax

AT+MREB <enter>

Example

Input:
AT+MREB <enter>
Response:
OK

The AT&W command must be issued to save changes!

AT+MNTP

Description

Enable and define a NTP server.

Command Syntax

AT+MNTP=<status>,<NTP server>
Status:
0 Disable
1 Enable

Example

Input:
AT+MNTP=1,pool.ntp.org<enter>
Response:
OK

AT+MTWT

Description

Enable/Disable the Wireless Traffic Timeout. Unit will reset if it does not see any traffic from the carrier for the amount of time defined.

Command Syntax

AT+MTWT=<value>
Value:
0 Disable
300 - 65535 (seconds)

Example

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

AT+MCNTO

Description

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

Command Syntax

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

The AT&W command must be issued to save changes!

Example

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

AT+MSDBE

Description

Enables/Disables the system default button located on the front of the IPn3G (CONFIG)

Command Syntax

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

Example

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

5.0 AT Commands

AT+MLEIP

Description

Set the IP Address, Netmask, and Gateway for the local Ethernet interface.

Command Syntax

AT+MLEIP=<IPAddress>, <Netmask>, <Gateway>

Example

Input:
```
AT+MLEIP=192.168.0.1,255.255.255.0,192.168.0.1 <enter>
```
Response:
```
OK
```

AT+MDHCP

Description

Enable/Disable the DHCP server running of the local Ethernet interface.

Command Syntax

AT+MDHCP=<action>
0 Disable
1 Enable

The AT&W command must be issued to save changes!

Example

Input:
```
AT+MDHCP=1 <enter>
```
Response:
```
OK
```

AT+MDHCPA

Description

Define the Starting and Ending IP Address (range) assignable by DHCP on the local Ethernet interface.

Command Syntax

AT+MDHCPA=<Start IP>, <End IP>

Example

Input:
```
AT+MDHCPA=192.168.0.100,192.168.0.200 <enter>
```
Response:
```
OK
```

AT+MEMAC

Description	Command Syntax
Retrieve the MAC Address of the local Ethernet interface.	**AT+MEMAC <enter>**

Example

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

AT+MUMAC

Description	Command Syntax
Query the MAC Address of the local USB Ethernet interface.	**AT+MUMAC <enter>**

The AT&W command must be issued to save changes!

Example

```
Input:
AT+MUMAC<enter>
Response:
+MUMAC: "00:0F:92:01:40:9A"
OK
```

AT+MUDPM

Description	Command Syntax
Set the operating mode of the USB port.	**AT+MUDPM=<mode>** 0 - Console Mode 1 - Data Mode 2 - NDIS Mode

Example

```
Input:
AT+MUDPM=2 <enter>
Response:
OK
```

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MUNDIS

Description

Configuration of the USB that is set to NDIS mode.

Command Syntax

AT+MUNDIS=<mode>, <IP Address>, <Netmask>, <Host IP>
Mode:
0 - Bridge
1 - Standalone

Example

Input:
AT+MUNDIS=1,192.168.111.1,255.255.255.0,192.168.111.2 <enter>
Response:
OK

AT+MUDPS

Description

Enable/Disable USB Data port.

Command Syntax

AT+MUDPS=<mode>
0 - Disable
1 - Enable

Example

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

AT+MUDBR

Description

Set USB data port baud rate.

Command Syntax

AT+MUDBR=<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

Example

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

5.0 AT Commands

AT+MUDDF

Description

Set the USB data port data format.

Command Syntax

AT+MUDDF=<data format>

0 - 8N1
1 - 8N2
2 - 8E1
3 - 8O1
4 - 7N1
5 - 7N2
6 - 7E1
7 - 7O1
8 - 7E2
9 - 7O2

Example

Input:
```
AT+MUDDF=0 <enter>
```
Response:
```
OK
```

AT+MUDDM

The AT&W command must be issued to save changes!

Description

Set the USB data port data mode.

Command Syntax

AT+MUDDM=<data mode>

0 - Seamless
1 - Transparent

Example

Input:
```
AT+MUDDM=1<enter>
```
Response:
```
OK
```

AT+MUDCT

Description

Set USB data port character timeout

Command Syntax

AT+MUDCT=<Timeout_s>

0 - 65535 (seconds)

Example

Input:
```
AT+MUDCT=0 <enter>
```
Response:
```
OK
```

5.0 AT Commands

AT+MUDMPS

Description	Command Syntax
Set the USB data port maximum packet size (bytes).	**AT+MUDMPS=<size>**

Example

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

AT+MUDPL

Description	Command Syntax
Set the USB data port priority.	**AT+MUDPL=<mode>** 0 - Normal 1 - Medium 2 - High

The AT&W command must be issued to save changes!

Example

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

AT+MUDNCDI

Description	Command Syntax
Enable/Disable USB data port no-connection data intake.	**AT+MUDNCDI=<mode>** 0 - Disable 1 - Enable

Example

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

AT+MUDMTC

Description

Set USB data port modbus tcp configuration

Command Syntax

AT+MUDMTC=<Status>, <Protection Status>, <Protection Key>
Status and Protection Status:
0 - Disable
1 - Enable

Example

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

AT+MUDIPM

Description

Set the USB data port IP protocol mode.

Command Syntax

AT+MUDIPM=<mode>
0 - TCP Client
1 - TCP Server
2 - TCP Client/Server
3 - UDP Point to Point
4 - UDP Point to Multipoint (P)
5 - UDP Point to Multipoint (MP)
6 - UDP Multipoint to Multipoint

Example

Input:
AT+MUDIPM=5<enter>
Response:
OK

The AT&W command must be issued to save changes!

AT+MUDTC

Description

Set USB data port TCP Client configuration, when set to TCP Client mode.

Command Syntax

AT+MUDTC=<Remote Server IP>, <Remote Server Port>, <Outgoing Connection Timeout>

Example

Input:
AT+MUDTC=192.168.0.189,20001,60 <enter>
Response:
OK

5.0 AT Commands

AT+MUDTS

Description

Set USB data port TCP Server configuration when set to TCP Server mode.

Command Syntax

AT+MUDTS=<Polling Mode>, <Polling Timeout_ms>, <Local Listening Port>, <Connection Timeout_ms>
Polling Mode:
0 - Monitor
1 - Multi-polling

Example

Input: (Entering Values)

```
AT+MUDTS=0,100,20003,300<enter>
```

Response:

```
OK
```

Input: (Retrieving Values)

```
AT+MUDTS?<enter>
```

Response:

```
+MUDTS: TCP Server Polling Mode:Monitor,Multi-polling Timeout(ms):100,Local List
ening Port:20003,Incoming Connection Timeout:300
OK
```

The AT&W command must be issued to save changes!

AT+MUDTCS

Description

Set the USB data port TCP Client/Server configuration when in TCP Client/Server mode.

Command Syntax

AT+MUDMTCS=<Remote Server IP>, <Remote Server Port>, <Outgoing Connection Timeout_s>, <Polling Mode>, <Polling Timeout_ms>, <Local Listening Port>, <Connection Timeout_ms>
Polling Mode:
0 - Monitor
1 - Multi-polling

Example

Input: (Entering Values)

```
AT+MUDTCS=0.0.0.0,20003,60,0,100,20003,300 <enter>
```

Response:

```
OK
```

Input: (Retriieving Values)

```
AT+MUDTCS?<enter>
```

Response:

```
+MUDTCS: Remote Server IP Address:0.0.0.0,Remote Server Port:20003,Outgoing Conn
ection Timeout:60,TCP Server Polling Mode:Monitor,Multi-polling Timeout(ms):100,
Local Listening Port:20003,Incoming Connection Timeout:300
OK
```

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MUDUPP

Description

Set USB data port UDP point to point configuration when configured in UDP point to point mode.

Command Syntax

AT+MUDUPP=<Remote Server IP>, <Remote Server Port>, <Local Listening Port>, <UDP timeout_s>

Example

Input: (Entering Values)

```
AT+MUDUPP=0.0.0.0,20003,20003,10<enter>
```

Response:

```
OK
```

Input: (Retrieving Values)

```
AT+MUDUPP?<enter>
```

Response:

```
+MUDUPP: Remote IP Address:0.0.0.0,Remote Port:20003,Listening Port:20003,UDP Ti
meout(s):10
OK
```

AT+MUDUPMP

Description

Set the USB data port UDP point to multipoint as point configuration when IP protocol is set to UDP point to multipoint (P)

Command Syntax

AT+MUDUPMP=<Multicast IP>, <Multicast Port>, <Listener Port>, <Time to live>

Example

Input: (Entering Values)

```
AT+MUDUPMP=224.1.1.3,20003,20013,1 <enter>
```

Response:

```
OK
```

Input: (Retriieving Values)

```
AT+MUDUPMP?<enter>
```

Response:

```
+MUDUPMP: Multicast IP Address:224.1.1.3,Multicast Port:20003,Listening Port:200
13,Time to Live:1
OK
```

AT+MUDUPMM

Description

Set the USB data port UDP point to multipoint as MP configuration when IP protocol is set to UDP point to multipoint (MP)

Command Syntax

AT+MUDUPMM=<Remote IP>, <Remote Port>, <Multicast IP>, <Multicast Port>

Example

```
Input: (Entering Values)
AT+MUDUPMM=0.0.0.0,20003,224.1.1.3,20003<enter>
Response:
OK

Input: (Retrieving Values)
AT+MUDUPMM?<enter>
Response:
+MUDUPMM: Remote IP Address:0.0.0.0,Remote Port:20013,Multicast IP Address:224.1
.1.3,Multicast Port:20003
OK
```

The AT&W command must be issued to save changes!

AT+MUDUMPMP

Description

Set the USB data port UDP multipoint to multipoint configuration when IP protocol is set to UDP multipoint to multipoint.

Command Syntax

AT+MUDUMPMP=<Multicast IP>, <Multicast Port>, <Time to live>, <Listen Multicast IP>, <Listen Multicast Port>

Example

```
Input:  (Entering Values)
AT+MUDUMPMP=224.1.1.3,20013,1,224.1.1.3,20013 <enter>
Response:
OK

Input:  (Retriieving Values)
AT+MUDUMPMP?<enter>
Response:
+MUDUMPMP: Multicast IP Address:224.1.1.3,Multicast Port:20013,Time to Live:1,Li
sten Multicast IP Address:224.1.1.3,Listen Multicast Port:20013
OK
```

AT+MPWD

Description	Command Syntax
Used to set or change the ADMIN password for the IPn3G.	**AT+MPWD=<New password>, <confirm password>**

Example

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

AT+MAUTH

Description	Command Syntax
Configure RADIUS authentication on the IPn3G.	**AT+MAUTH=<Mode>, <Radius Server IP>, <Port>, <Secret>, <Timeout_s>** Mode: 0 Local 1 Radius&Local

The AT&W command must be issued to save changes!

Example

Input: (Entering Values)
```
AT+MAUTH=0,0.0.0.0,1812,nosecret,10 <enter>
```
Response:
```
OK
```

Input: (Retriieving Values)
```
AT+MAUTH?<enter>
```
Response:
```
+MAUTH: Local,"0.0.0.0","1812","nosecret",10
OK
```

AT+MDISS

Description	Command Syntax
Configure discovery mode service used by IPn3G and utilities such as “IP Discovery”.	**AT+MDISS=<Mode>** Mode: 0 Disable 1 Discoverable 2 Changeable

Example

Input:
```
AT+MDISS=1 <enter>
```
Response:
```
OK
```

5.0 AT Commands

AT+MNAT

Description

Enable/Disable NAT

Command Syntax

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

Example

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

AT+MPPPS

The AT&W command must be issued to save changes!

Description

Enable/Disable PPP

Command Syntax

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

Example

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

AT+MPIPP

Description

Enable/Disable IP-Passthrough

Command Syntax

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

Example

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

AT+MDOD

Description

Enable/Disable Dial-on-Demand. If disabled, the modem will always remain connected. The default is **Disabled**.

Command Syntax

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

Example

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

AT+MPITO

Description

The maximum amount of time to pass before modem will timeout. The default is **0 seconds.**

Command Syntax

AT+MPITO=<Value>
0 - 65535 seconds

The AT&W command must be issued to save changes!

Example

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

AT+MPCTO

Description

The maximum amount of time to wait for a connection The default is **90 seconds.**

Command Syntax

AT+MPCTO=<Value>
0 - 65535 seconds

Example

Input:
AT+MPCTO=90<enter>
Response:
OK

5.0 AT Commands

AT+MPDMR

Description

The maximum amount of attempts to dial and establish a connection with the carrier. The default is 0, which means the modem will keep trying indefinitely.

Command Syntax

AT+MPDMR=<Value>

Example

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

AT+MPAT

The AT&W command must be issued to save changes!

Description

Sets the authentication type required to negotiate with carrier.

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

Command Syntax

AT+MPAT=<Value>

Value

0	No-auth
1	chap
2	pap
3	pap-chap

Example

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

AT+MPUP

Description

Enter login credentials for connection to the wireless carrier.

Command Syntax

AT+MPUP=<user name>, <password>

Example

Input:
AT+MPUP=4035558709@carrier.isp, 35&HJ345<enter>
Response:
OK

5.0 AT Commands

AT+MPDN

Description

Sets the PPP dial number. Carrier dependant, the default number is ***99***1#**

Command Syntax

AT+MPDN=<Value>

Example

Input:
```
AT+MPDN=*99***1#<enter>
```
Response:
```
OK
```

AT+MPCS

Description

Sets the modems connect string if required by the carrier.

Command Syntax

AT+MPCS=<connect string>

The AT&W command must be issued to save changes!

Example

Input:
```
AT+MPCS=CONNECT <enter>
```
Response:
```
OK
```

AT+MAPN

Description

Sets the Access Point Name (APN). Required and assigned by the wireless carrier.

Command Syntax

AT+MAPN=<access point name>

Example

Input: (Enter value)
```
AT+MAPN=myapn.isp.com <enter>
```
Response:
```
OK
```

Input: (Retrieve value)
```
AT+MAPN?<enter>
```
Response:
```
+MAPN: myapn.isp.com
OK
```

The AT&W command must be issued to save changes!

AT+MPINS1
AT+MPINS2
AT+MPINS3
AT+MPINS4

Description	Command Syntax
Sets initialization Strings. Carrier dependant.	**AT+MPINS1=<initialization string>** **AT+MPINS2=<initialization string>** **AT+MPINS3=<initialization string>** **AT+MPINS4=<initialization string>**

Example

Input:
AT+MPINS1=init-string <enter>
Response:
OK

AT+MWSIP

Description	Command Syntax
Sets WAN Static IP. Do not set unless specifically advised to do so by the carrier.	**AT+MWSIP=<static IP address>**

Example

Input:
AT+MWSIP=0.0.0.0 <enter>
Response:
OK

AT+MURD

Description	Command Syntax
Enable/Disable remote DNS. Enabled by default, the IPn3G, will use the DNS server as specified automatically by the service provider.	**AT+MURD=<Mode>** Mode: 0 Disable 1 Enable

Example

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

AT+MDDNSE

Description

Enable/Disable DDNS.

Command Syntax

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

Example

Input:

```
AT+MDDNSE=0<enter>
```

Response:

```
OK
```

AT+MDDNS

The AT&W command must be issued to save changes!

Description

Select DDNS service provider, and login credentials as required for DDNS services.

Command Syntax

AT+MDDNS=<service name>, <domain>, <user name>, <password>
Service name:
0 - dyndns.org
1 - changeip.com
2 - zoneedit.com
3 - no-ip.com
4 - noip.com
5 - freedns.afraid.org
6 - dnsmax.com
7 - thatip.com

Example

Input:

```
AT+MDDNS=0,user.dydns.org,user,password <enter>
```

Response:

```
OK
```

AT+MIKACE

Description

Enable or Disable IMCP ICMP keep-alive check.

Command Syntax

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

Example

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

AT+MIKAC

The AT&W command must be issued to save changes!

Description

Set ICMP Keep-alive check parameters.

Command Syntax

AT+MIKAC=<host name>, <interval in seconds>, <count>

Example

Input:
AT+MIKAC=www.google.com,600,10<enter>
Response:
OK

5.0 AT Commands

AT+MCOPS

Description

Enable or Disable COM1 serial port.

Command Syntax

AT+MCOPS=<Mode>
Mode:

0	Disable
1	Enable

Example

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

AT+MCOCM

The AT&W command must be issued to save changes!

Description

Sets COM1 serial port channel mode.

Command Syntax

AT+MCOCM=<Mode>
Mode:

0	RS232
1	RS485
2	RS422

Example

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

AT+MCOBR

Description

Set COM1 port baud rate.

Example

Input:
AT+MCOBR=7<enter>
Response:
OK

Command Syntax

AT+MCOBR=<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+MCODF

Description

Set COM1 data format.

Example

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

Command Syntax

AT+MCODF=<data format>
Data Format:

0	8N1	5	7N2
1	8N2	6	7E1
2	8E1	7	7O1
3	8O1	8	7E2
4	7N1	9	7O2

AT+MCOFC

Description

Set COM1 flow control.

Command Syntax

AT+MCOFC=<Value>

0	None
1	Hardware
2	CTS Framing

The AT&W command must be issued to save changes!

Example

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

AT+MCOPRDD

Description

Set COM1 port pre-data delay (ms)

Command Syntax

AT+MCOPRDD=<delay_ms>

Example

Input:
AT+MCOPRDD=100<enter>

AT+MCOPODD

Description

Set COM1 port post-data delay (ms)

Command Syntax

AT+MCOPODD=<delay_ms>

Example

Input:
AT+MCOPODD=100<enter>

AT+MCODM

Description

Set COM1 data mode.

Command Syntax

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

Example

Input:
```
AT+MCODM=1<enter>
```
Response:
```
OK
```

AT+MCOCT

Description

Set COM1 port character timeout.

Command Syntax

AT+MCOCT=<timeout_s>

The AT&W command must be issued to save changes!

Example

Input:
```
AT+MCOCT=0 <enter>
```
Response:
```
OK
```

AT+MCOMPS

Description

Set COM1 maximum packet size.

Command Syntax

AT+MCOMPS=<size>

Example

Input:
```
AT+MCOMPS=1024<enter>
```
Response:
```
OK
```

AT+MCOP

Description

Set COM1 port priority.

Command Syntax

AT+MCOP=<Mode>

Mode:

0	Normal
1	Medium
2	High

Example

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

AT+MCONCDI

The AT&W command must be issued to save changes!

Description

Enable/Disable no-connection data intake.

Command Syntax

AT+MCONCDI=<Mode>

Mode:

0	Disable
1	Enable

Example

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

AT+MCOMTC

Description

Set COM1 modbus TCP configuration

Command Syntax

AT+MCOMTC=<Status>, <Protection status>, <Protection Key>

Status and Protection Status:

0	Disable
1	Enable

Example

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

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MCOIPM

Description

Set COM1 serial port IP Protocol Mode. This setting determines which protocol the serial server will use to transmit serial port data over the IPn3G.

Command Syntax

AT+MCOIPM=<Mode>

Mode:

0	TCP Client
1	TCP Server
2	TCP Client/Server
3	UDP Point to Point
4	UDP Point to Multipoint(P)
5	UDP Point to Multipoint(MP)
6	UDP Multipoint to Multipoint
7	SMTP Client
8	PPP

Example

Input:

```
AT+MCOIPM=0<enter>
```

Response:

```
OK
```

AT+MCOTC

Description

Set COM1 TCP Client parameters when configured as TCP Client mode.

Command Syntax

AT+MCOTC=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>

Example

Input:

```
AT+MCOTC=0.0.0.0,20001,60 <enter>
```

Response:

```
OK
```

AT+MCOTS

Description

Set COM1 TCP Server parameters when configured as TCP Server mode.

Example

Input:

```
AT+MCOTS=0,100,20001,300 <enter>
```

Response:

```
OK
```

Command Syntax

AT+MCOTS=<Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:

0	Monitor
1	Multi-polling

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MCOTCS

Description

Set COM1 TCP Client/Server parameters when configured as TCP Client/Server mode.

Command Syntax

AT+MCOTCS=<Remote Server IP>, <Remote Server Port>, <Outgoning timeout_s>, <Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:

0	Monitor
1	Multi-polling

Example

Input:
```
AT+MCOTCS=0.0.0.0,20001,60,0,100,20001,300<enter>
```
Response:
```
OK
```

AT+MCOUPP

Description

Set COM1 UDP Point-to-Point configuration when set to UDP Point-to-Point mode.

Command Syntax

AT+MCOUPP=<Remote Server IP>, <Remote Server Port>, <Listener Port>, <UDP timeout_s>

Example

Input:
```
AT+MCOUPP=0.0.0.0,20001,20001,10<enter>
```
Response:
```
OK
```

AT+MCOUPMP

Description

Set COM1 UDP Point-to-Multipoint as point parameters when configured in UDP Point-to-Multipoint (P) mode.

Command Syntax

AT+MCOUPMP=<Multicast IP>, <Multicast Port>, <Listener Port>, <Time to live>

Example

Input:
```
AT+MCOUPMP=224.1.1.1, 20001, 20001, 1 <enter>
```
Response:
```
OK
```

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MCOUPMM

Description	Command Syntax
Set COM1 UDP Point-to-Multipoint as MP parameters when configured in UDP Point-to-Multipoint (MP) mode.	**AT+MCOUPMM=<Remote IP>, <Remote Port>, <Multicast IP>, <Multicast Port>**

Example

Input:

```
AT+MCOUPMM=0.0.0.0,20001,224.1.1.1,20001<enter>
```

Response:

```
OK
```

AT+MCOUMPMP

Description	Command Syntax
Set COM1 UDP Multipoint-to-Multipoint parameters when set to UDP Multipoint-to-Multipoint mode.	**AT+MCOUMPMP=<Multicast IP>, <Multicast Port>, <Time to live>, <Listen Multicast IP>, <Listen Multicast Port>**

Example

Input:

```
AT+MCOUMPMP=224.1.1.1,20011,1,224.1.1.1,20011<enter>
```

Response:

```
OK
```

AT+MCOSMTP

Description	Command Syntax
Set COM1 SMTP Client Configuration when set to SMTP Client mode.	**AT+MCOSMTP=<Mail Subject>, <Mail Server>, <Mail Recipient>, <Message Max Size>, <Timeout_s>, <Transfer Mode>** Transfer Mode: 0 Text 1 Attached File 2 Hex Code

Example

Input:

```
AT+MCOSMTP=COM1 Message, mail.mymail.com, host@email.com, 1024, 10, 0<enter>
```

Response:

```
OK
```

5.0 AT Commands

AT+MCOPPP

Description

Set COM1 PPP parameters when COM1 is configured in PPP Mode.

Command Syntax

AT+MCOPPP=<PPP Local IP>, <PPP Host IP>, <PPP idle timeout_s>

Example

Input:

```
AT+MCOPPP=192.168.0.1,192.168.0.99,30<enter>
```

Response:

```
OK
```

AT+MCTPS

Description

Enable/Disable the COM2 serial port. This port is located on the front of the IPn3G and is labelled as the DIAGNOSTIC port.

The AT&W command must be issued to save changes!

Command Syntax

AT+MCTPS=<Mode>

Mode:

0	Disable
1	Enable

Example

Input:

```
AT+MCTPS=0<enter>
```

Response:

```
OK
```

AT+MCTBR

Description

Set COM2 baud rate.

Command Syntax

AT+MCTBR=<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

Example

Input:

```
AT+MCTBR=13<enter>
```

Response:

```
OK
```

5.0 AT Commands

The AT&W command must be issued to save changes!

AT+MCTDF

Description

Set COM2 data format

Command Syntax

AT+MCTDF=<data format>

Data Format:

0	8N1
1	8N2
2	8E1
3	8O1
4	7N1
5	7N2
6	7E1
7	7O1
8	7E2
9	7O2

Example

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

AT+MCTDM

Description

Set COM2 data mode.

Command Syntax

AT+MCTDM=<Data Mode>

Data Mode:

0	Seamless
1	Transparent

Example

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

AT+MCTCT

Description

Set COM2 character timeout.

Command Syntax

AT+MCTCT=<timeout_s>

Example

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

The AT&W command must be issued to save changes!

AT+MCTMPS

Description

Set COM2 data format

Command Syntax

AT+MCTMPS=<size>

Example

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

AT+MCTP

Description

Set COM2 port priority.

Command Syntax

AT+MCTP=<Mode>
Mode:
0 Normal
1 Medium
2 High

Example

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

AT+MCTNCDI

Description

Enable/Disable COM2 port no-connection data intake.

Command Syntax

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

Example

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

The AT&W command must be issued to save changes!

AT+MCTMTC

Description

Set COM2 modbus TCP configuration.

Command Syntax

AT+MCTMTC=<Status>, <Protection status>, <Protection Key>

Status and Protection Status:

0 Disable
1 Enable

Example

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

AT+MCTIPM

Description

Set the COM2 serial port IP Protocol Mode.

Example

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

Command Syntax

AT+MCTIPM=<Mode>

Mode:

0 TCP Client
1 TCP Server
2 TCP Client/Server
3 UDP Point to Point
4 UDP Point to Multipoint(P)
5 UDP Point to Multipoint(MP)
6 UDP Multipoint to Multipoint

AT+MCTTC

Description

Set COM2 TCP Client parameters when IP Protocol Mode is set to TCP Client.

Command Syntax

AT+MCTTC=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>

Example

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

AT+MCTTS

Description

Set COM2 TCP Server parameters when IP Protocol Mode is set to TCP Server.

Example

Input:
AT+MCTTS=0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTS=<Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:

0	Monitor
1	Multi-polling

AT+MCTTCS

The AT&W command must be issued to save changes!

Description

Set COM2 TCP Client/Server parameters when IP Protocol is set to TCP Client/Server mode.

Example

Input:
AT+MCTCS=0.0.0.0,20002,60,0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTCS=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>, <Polling Mode>, <Polling timeout_s>,<Local Listener Port>, <Connection timeout_s>

Polling Mode:

0	Monitor
1	Multi-polling

AT+MCTUPP

Description

Set COM2 UDP Point-to-Point parameters when IP Protocol is set to UDP Point-to-Point mode.

Command Syntax

AT+MCTUPP=<Remote Server IP>, <Remote Server Port>, <Liste ner Port>, <UDP timeout_s>

Example

Input:
AT+MCTUPP=0.0.0.0,20002,20002,10<enter>
Response:
OK

AT+MCTUPMP

Description

Set COM2 UDP Point-to-Multipoint as point parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (P)

Command Syntax

AT+MCTUPMP=<Multicast IP>, <Multicast Port>, <Listener Port>, <Time to live>

Example

Input:
AT+MCTUPMP=224.1.1.2,20002,20012,1<enter>
Response:
OK

AT+MCTUPMM

Description

Set COM2 UDP Point-to-Multipoint as MP parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (MP)

Command Syntax

AT+MCTUPMM=<Remote IP>, <Remote Port>, <Multicast IP>, <Multicast Port>

Example

Input:
AT+MCTUPMM=0.0.0.0,20012,224.1.1.2,20002<enter>
Response:
OK

The AT&W command must be issued to save changes!

AT+MCTUMPMP

Description

Set COM2 UDP Multipoint-to-Multipoint parameters when IP Protocol is set to UDP Multipoint-to-Multipoint mode.

Command Syntax

AT+MCTUMPMP=<Multicast IP>, <Multicast Port>, <Time to live>, <Listen Multicast IP>, <Listen Multicast Port>

Example

Input:
AT+MCTUMPMP=224.1.1.2,20012,1,224.1.1.2,20012<enter>
Response:
OK

AT+CMGS

Description

Send SMS message. To send message CTRL+Z must be entered, to exit, ESC.

Command Syntax

AT+CMGS=<“Phone Number”><CR>
text is entered <CTRL+Z/ESC>

Example

Input:
AT+CMGS=“4035551714” <enter>

This is message <CTRL+Z> // <CTRL+Z> ends the text mode and returns to regular AT command mode.

Response:
OK

The AT&W command must be issued to save changes!

AT+CMGR

Description

This command allows the application to read stored messages. The messages are read from the SIM card memory.

Command Syntax

AT+CMGR=<index>

Example

Input:
AT+CMGR=<index><enter>

Response:
+CMGR: <stat>,<oa>,,<dt>
<data>
OK

Parameters:
<index> Index in SIM card storage of the message
<stat> Status of Message in Memory (Text Mode)
"REC UNREAD" Received unread messages
"REC READ" Received read messages
<oa> Originator Address
String type
<dt> Discharge Time
String format: "yy/MM/dd,hh:mm:ss±zz" (year [00-99]/ month [01-12]/Day [01-31], Hour:Min:Second and TimeZone [quarters of an hour])
<data> SMS User Data in Text Mode
String type

AT+MMGR

Description

This command allows the application to read stored messages. The messages are read from the SIM card memory. It is same as +CMGR, but the +MMGR command does not change the message status.

Command Syntax

AT+MMGR=<index><CR>

Example

Input:

```
AT+MMGR=<index><enter>
```

Response:

```
+MMGR: <stat>,<oa>,,<dt>
<data>
OK
```

Parameters:

<index> Index in SIM card storage of the message
<stat> Status of Message in Memory (Text Mode)
“REC UNREAD” Received unread messages
“REC READ” Received read messages
<oa> Originator Address
String type
<dt> Discharge Time
String format: "yy/MM/dd,hh:mm:ss±zz" (year [00-99]/ month [01-12]/Day [01-31], Hour:Min:Second and TimeZone [quarters of an hour])
<data> SMS User Data in Text Mode
String type

The AT&W command must be issued to save changes!

AT+CMGL

Description

This command allows the application to read stored messages by indicating the type of the message to read. The messages are read from the SIM card memory.

Command Syntax

AT+CMGL=<status>
Status:
0 - Lists all unread messages
1 - Lists all read messages
4 - Lists all messages

Example

Input:

```
AT+CMGL=0 <enter>
```

Response:

```
+CMGR: "REC READ","+14035555776",,"2012/02/06,10:39:43-07"
This is the SMS message.

OK
```

AT+MMGL

Description

This command allows the application to read stored messages by indicating the type of the message to read. The messages are read from the SIM card memory. It is same as +CMGL, but the +MMGL command does not change the message status.

Command Syntax

AT+MMGL=<status>
Status:
0 - Lists all unread messages
1 - Lists all read messages
4 - Lists all messages

Example

Input:

```
AT+MMGL=4 <enter>
```

Response:

```
+MMGL: 1,"REC UNREAD","+14035553776",,"2012/02/06,10:57:38-07"
This is another message

+MMGL: 0,"REC READ","+14035553776",,"2012/02/06,10:39:43-07"
This is the reply

OK
```

The AT&W command must be issued to save changes!

AT+CMGD

Description

This command handles deletion of a single message from memory location <index>, or multiple messages according to <delflag>.

Command Syntax

AT+CMGD=<index>,<delflag>
delflag:
0 - Deletes the message specified in <index>
1 - Deletes all read messages
4 - Deletes all messages

Example

Input:

```
AT+CMGD=0,4 <enter>
```

Response:

```
index=0 dflag=4

OK
```

AT+MIS

Description

This command allows the application to read the current status of the Digital Input.

Command Syntax

AT+MIS

Example

Input:

```
AT+MIS <enter>
```

Response:

```
+MIS: available input status
INPUT 1: 0   open
OK
```

AT+MOS

Description

This command allows setting of digital output, and to check the current status.

Command Syntax

AT+MOS=<Mode[,<Setting No.>,<Status>]

Mode:
0 - All Output Status
1 - Output Setting
Setting No.: 1 (if output available)
Status: 0 open; 1 close

Example

Input:

```
AT+MOS=0 <enter>
```

Response:

```
+MOS: available output status
OUTPUT 1: 0    open
OK
```

Input:

```
AT+MOS=1,1,1 <enter>
```

Response:

```
+MOS: Set OUTPUT 1 : 1    close
OK
```

Input:

```
AT+MOS=1,1,0 <enter>
```

Response:

```
+MOS: Set OUTPUT 1: 0    open
OK
```

5.0 AT Commands

ATL

Description

Lists all available AT Commands.

Command Syntax

ATL <enter>

Example

```
ATL <enter>

Help            List top level utilities' commands
AT              Echo OK
ATH             Show a list of previously run commands
ATL             List all available commands
AT&R            Read modem active profile to editable profile
AT&V            Display modem active profile
AT&W            Enable configurations you have been entered
ATA             Quit
ATO             Quit
AT+MSYSI        System summary information
AT+GMR          Modem Record Information
AT+MMNAME       Modem Name
AT+GMI          Get Manufacturer Identification
AT+CNUM         Check Modem's Phone Number
AT+CIMI         Check Modem's IMEI and IMSI
AT+CCID         Check Modem's SIM Card Number
AT+MRTF         Reset the modem to the factory default settings of  from non-volatile (NV) memory
AT+MREB         Reboot the modem
AT+MNTP         Define NTP server
AT+MTWT         Enable or disable traffic watchdog timer used to reset the modem
AT+MCNTO        Set console timeout
AT+MSDBE        Enable or disable system default button
AT+MLEIP        Set the IP address of the modem Local Ethernet interface
AT+MDHCP        Enable or disable DHCP server running on the Ethernet interface
AT+MDHCPA       Set the range of IP addresses to be assigned by the DHCP server
AT+MEMAC        Query the MAC address of local Ethernet interface
AT+MUMAC        Query the MAC address of local USB Ethernet interface
AT+MUDPM        Set the USB device mode
AT+MUNDIS       Configuration of USB device that be set to NDIS mode
AT+MUDPS        Enable or disable usb data port
AT+MUDBR        Set usb data port baud rate
AT+MUDDF        Set usb data port data format
AT+MUDDM        Set usb data port data mode
AT+MUDCT        Set usb data port character timeout
AT+MUDMPS       Set usb data port maximum packet size
AT+MUDPL        Set usb data port priority
AT+MUDNCDI      Enable or disable usb data port no-connection data intake
AT+MUDMTC       Set usb data port modbus tcp configuration
AT+MUDIPM       Set usb data port IP protocol mode
AT+MUDTC        Set usb data port tcp client configuration when IP protocol mode be set to TCP Client
AT+MUDTS        Set usb data port tcp server configuration when IP protocol mode be set to TCP Server
AT+MUDTCS       Set usb data port tcp client/server configuration when IP protocol mode be set to TCP
                Client/Server
AT+MUDUPP       Set usb data port UDP point to point configuration when IP protocol mode be set to UDP
                point to point
AT+MUDUPMP      Set usb data port UDP point to multipoint as point configuration when IP protocol mode
                be set to UDP point to multipoint(P)
AT+MUDUPMM      Set usb data port UDP point to multipoint as MP configuration when IP protocol mode be
                set to UDP point to multipoint(MP)
AT+MUDUMPMP     Set usb data port UDP multipoint to multipoint configuration when IP protocol mode be
                set to UDP multipoint to multipoint
AT+MPWD         Set password
AT+MAUTH        Set authentication used by the modem
```

5.0 AT Commands

AT+MDISS	Set discovery service used by the modem
AT+MNAT	Enable or disable NAT
AT+MPPPS	Enable or disable PPP
AT+MPIPP	Enable or disable IP-Passthrough
AT+MDOD	Enable or disable Dial-on-Demand
AT+MPITO	Set idle Timeout
AT+MPCTO	Set Connect Timeout
AT+MPDMR	Set dialing max retries
AT+MPAT	Set authentication type used by PPP
AT+MPUP	Set authentication type used by PPP
AT+MPDN	Set PPP dial number
AT+MPCS	Set PPP connect string
AT+MAPN	Set access point name
AT+MPINS1	Set initialization string #1
AT+MPINS2	Set initialization string #2
AT+MPINS3	Set initialization string #3
AT+MPINS4	Set initialization string #4
AT+MWSIP	Set WAN static IP
AT+MURD	Enable or disable use remote DNS
AT+MDDNSE	Enable or disable DDNS
AT+MDDNS	Set DDNS
AT+MIKACE	Enable or disable ICMP keep-alive check
AT+MIKAC	Set ICMP keep-alive check
AT+MCOPS	Enable or disable com1 port
AT+MCOCM	Set com1 port channel mode
AT+MCOBR	Set com1 port baud rate
AT+MCODF	Set com1 port data format
AT+MCOFC	Set com1 port flow control
AT+MCOPRDD	Set com1 port pre-data delay(ms)
AT+MCOPODD	Set com1 port post-data delay(ms)
AT+MCODM	Set com1 port data mode
AT+MCOCT	Set com1 port character timeout
AT+MCOMPS	Set com1 port maximum packet size
AT+MCOP	Set com1 port priority
AT+MCONCDI	Enable or disable no-connection data intake
AT+MCOMTC	Set com1 port modbus tcp configuration
AT+MCOIPM	Set com1 port IP protocol mode
AT+MCOTC	Set com1 port tcp client configuration when IP protocol mode be set to TCP Client
AT+MCOTS	Set com1 port tcp server configuration when IP protocol mode be set to TCP Server
AT+MCOTCS	Set com1 port tcp client/server configuration when IP protocol mode be set to TCP Client/Server
AT+MCOUPP	Set com1 port UDP point to point configuration when IP protocol mode be set to UDP point to point
AT+MCOUPMP	Set com1 port UDP point to multipoint as point configuration when IP protocol mode be set to UDP point to multipoint(P)
AT+MCOUPMM	Set com1 port UDP point to multipoint as MP configuration when IP protocol mode be set to UDP point to multipoint(MP)
AT+MCOUMPMP	Set com1 port UDP multipoint to multipoint configuration when IP protocol mode be set to UDP multipoint to multipoint
AT+MCOSMTP	Set com1 port SMTP client configuration when IP protocol mode be set to SMTP Client
AT+MCOPPP	Set com1 port PPP configuration when IP protocol mode be set to PPP
AT+MCOPPP	Set com1 port PPP configuration when IP protocol mode be set to PPP
AT+MCTPS	Enable or disable com2 port
AT+MCTBR	Set com2 port baud rate
AT+MCTDF	Set com2 port data format
AT+MCTDM	Set com2 port data mode
AT+MCTCT	Set com2 port character timeout
AT+MCTMPS	Set com2 port maximum packet size
AT+MCTP	Set com2 port priority
AT+MCTNCDI	Enable or disable com2 port no-connection data intake
AT+MCTMTC	Set com2 port modbus tcp configuration
AT+MCTIPM	Set com2 port IP protocol mode
AT+MCTTC	Set com2 port tcp client configuration when IP protocol mode be set to TCP Client
AT+MCTTS	Set com2 port tcp server configuration when IP protocol mode be set to TCP Server

AT+MCTTCS	Set com2 port tcp client/server configuration when IP protocol mode be set to TCP Client/Server
AT+MCTUPP	Set com2 port UDP point to point configuration when IP protocol mode be set to UDP point to point
AT+MCTUPMP	Set com2 port UDP point to multipoint as point configuration when IP protocol mode be set to UDP point to multipoint(P)
AT+MCTUPMM	Set com2 port UDP point to multipoint as MP configuration when IP protocol mode be set to UDP point to multipoint(MP)
AT+MCTUMPMP	Set com2 port UDP multipoint to multipoint configuration when IP protocol mode be set to UDP multipoint to multipoint
AT+CMGS	Send SMS
AT+CMGR	Read SMS with changing status
AT+MMGR	Read SMS without changing status
AT+CMGL	List SMSs with changing status
AT+MMGL	List SMSs without changing status
AT+CMGD	Delete SMS
AT+MIS	Module Digital Input status
AT+MOS	Module Digital Output status and setting

Appendix A: RS485 Wiring

The IPn3G can be connected into a 2– or 4-wire RS485 network. A transmission line termination should be placed only on the extreme ends of the data line if the RS485 network runs at high speed and the cable run is very long.

2-Wire

Figure C1 illustrates a typical 2-wire RS485 wiring configuration. The cable pair is shared for both transmit and receive data: it is very important that the IPn3G seize control of the line at the proper time when it is to transmit data.

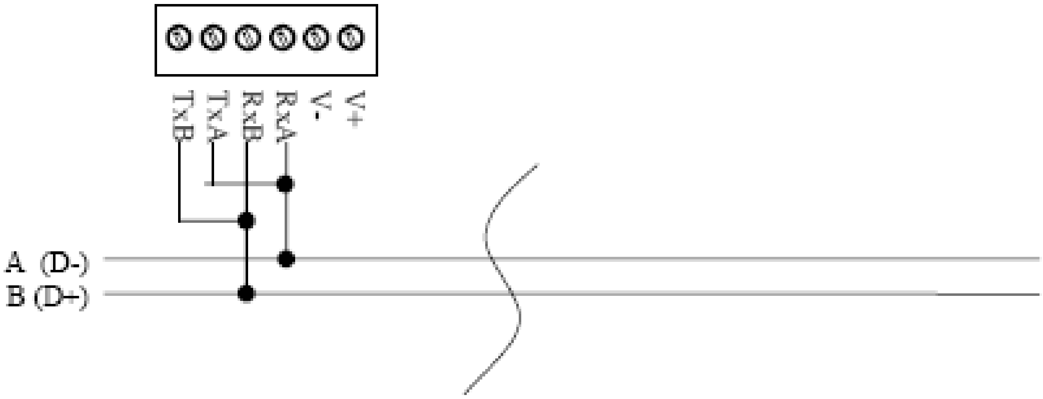


Figure A1: 2-Wire RS485 Wiring

4-Wire

In a 4-wire network, one node will be the master and all other nodes will be remotes. The master node may talk to all remote nodes, yet each remote may only communicate with the one master. Since the remote nodes never ’hear’ each other, a remote node could not conceivably reply incorrectly to another remote’s communication.

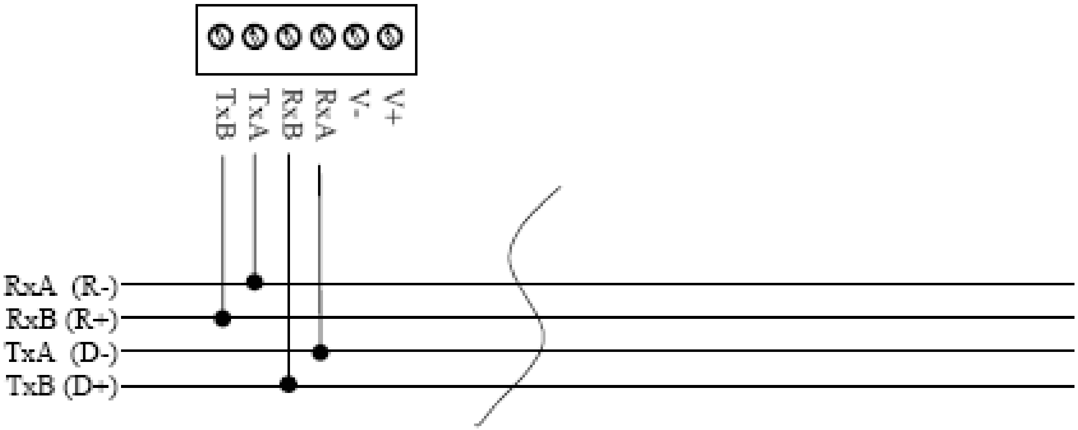


Figure A2: 4-Wire RS485 Wiring

Appendix B: Serial Interface

Module (DCE)		Signal		Host Microprocessor (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 without level shifting, so direct connection to a host microprocessor is possible.

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 MHX 920A.

RX *Receive Data* - Output from Module - Signals transferred from the MHX 920A are received by the DTE via RX.

TX *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the MHX 920A.

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 microprocessor.

Appendix C: IP-Passthrough

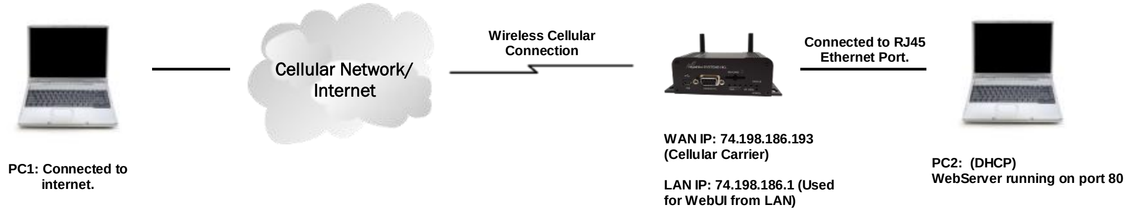
By completing the Quick Start process, a user should have been able to log in and set up the IPn3G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the IPn3G is to access connected devices remotely. In order to do this, the IPn3G 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 IPn3G and the connected device/PC to work with IP-Passthrough. IP-Passthrough means that the IPn3G is transparent, and all outside (WAN) traffic is simply sent directly to the device connected to the physical RJ-45 port on the back of the IPn3G (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 IPn3G.

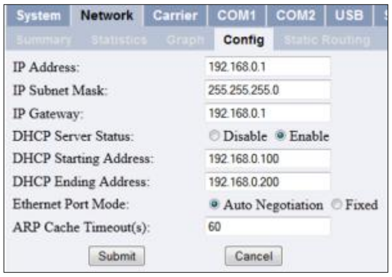
IP-Passthrough is ideal for applications where only a single device is connected to the IPn3G, and other features of the IPn3G are not required. When in passthrough mode, most features of the IPn3G are bypassed, this includes the serial ports, the GPS features, VPN, the Firewall, and much more. The advantage of IP-Passthrough is that the configuration is very simple.

In the example below we have a IPn3G 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 IPn3G, the IPn3G would then automatically assign, via DHCP, the WAN IP to the attached PC2, creating a transparent connection.



Step 1

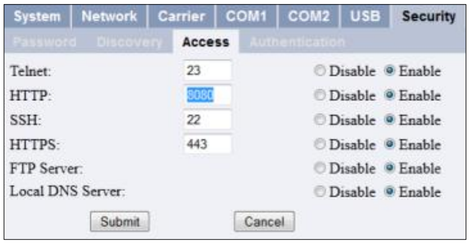
Log into the IPn3G (Refer to Quick Start), and ensure that DHCP is enabled on the **Network > Config** page.



IP Address:	192.168.0.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.0.1
DHCP Server Status:	○ Disable ● Enable
DHCP Starting Address:	192.168.0.100
DHCP Ending Address:	192.168.0.200
Ethernet Port Mode:	● Auto Negotiation ○ Fixed
ARP Cache Timeout(s):	60

Step 2

Since PC2 requires port 80 to be used as its Web server port, port 80 cannot be used on the IPn3G, by default it retains this port for remote configuration. To change the port used by the IPn3G, navigate to the **Security > Access** page as seen below. For this example we are going to change it to port 8080. When changing port numbers on the IPn3G, it is recommended to reboot the unit before continuing, remember the new WebUI port is now 8080 when you log back into the IPn3G. (e.g. 192.168.0.1:8080).



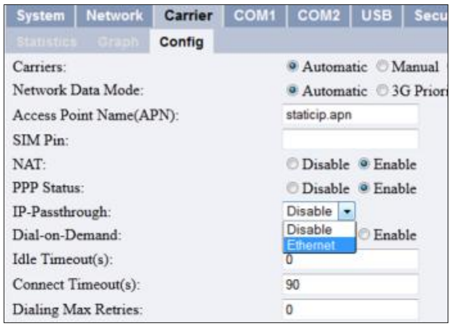
Telnet:	23	○ Disable ● Enable
HTTP:	8080	○ Disable ● Enable
SSH:	22	○ Disable ● Enable
HTTPS:	443	○ Disable ● Enable
FTP Server:		○ Disable ● Enable
Local DNS Server:		○ Disable ● Enable

Appendix C: IP-Passthrough

Step 3

Now IP-Passthrough can be enabled on the IPn3G. Under the ***Carrier > Config*** 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 RJ45 port, will dynamically be assigned the WAN IP Address. In this example, this would be 74.198.186.193.

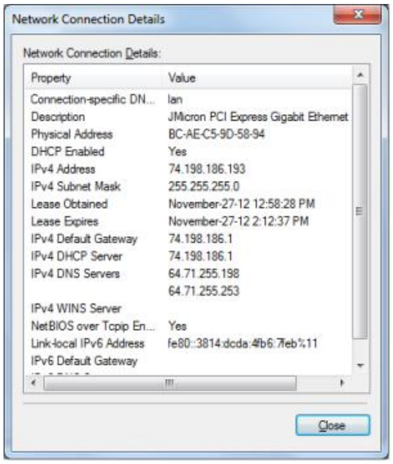
The default IP address of 192.168.0.1 on the LAN is no longer available, but it is still possible to access and configure the IPn3G on the LAN side, by using the X.X.X.1 IP Address, where the first 3 octets of the WAN IP are used in place of the X’s. (e.g. 74.198.186.1, and remember the HTTP port in this example was changed to 8080).



Carriers:	● Automatic ○ Manual
Network Data Mode:	● Automatic ○ 3G Priori
Access Point Name(APN):	staticip.apn
SIM Pin:	
NAT:	○ Disable ● Enable
PPP Status:	○ Disable ● Enable
IP-Passthrough:	Disable ▾ Disable Ethernet
Dial-on-Demand:	○ Enable
Idle Timeout(s):	0
Connect Timeout(s):	90
Dialing Max Retries:	0

Step 4

Attach the remote device or PC to the RJ45 port of the IPn3G. The end device has to be set up for DHCP to get an IP address from the IPn3G. 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 IPn3G has a IP Address of 74.198.186.193, which is the IP address assign by the cellular carrier for the modem.



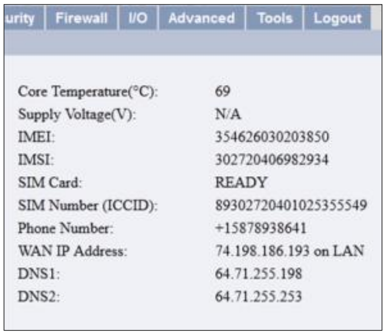
Property	Value
Connection-specific DN...	lan
Description	JMicron PCI Express Gigabit Ethernet
Physical Address	BC-AE-C5-9D-58-94
DHCP Enabled	Yes
IPv4 Address	74.198.186.193
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	November-27-12 12:58:28 PM
Lease Expires	November-27-12 2:12:37 PM
IPv4 Default Gateway	74.198.186.1
IPv4 DHCP Server	74.198.186.1
IPv4 DNS Servers	64.71.255.198 64.71.255.253
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::3814:dcda:4fb6:7feb%11
IPv6 Default Gateway	

Step 5 (Optional)

IP-Passthrough operation can also be verified in the IPn3G. Once IP-Passthrough is enabled you can access the IPn3G 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.
- By using the NDIS/USB interface, by entering in 192.168.111.1:8080

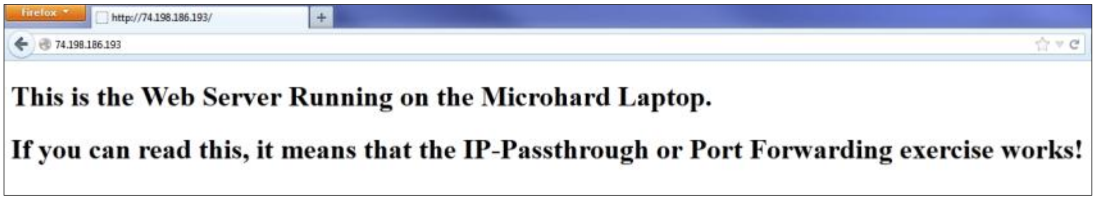
Once logged in, navigate to the ***System > Summary*** page. Under WAN IP Address it should look something like shown in the image to the right, 74.198.186.193 on LAN.



Core Temperature(°C):	69
Supply Voltage(V):	N/A
IMEI:	354626030203850
IMSI:	302720406982934
SIM Card:	READY
SIM Number (ICCID):	89302720401025355549
Phone Number:	+15878938641
WAN IP Address:	74.198.186.193 on LAN
DNS1:	64.71.255.198
DNS2:	64.71.255.253

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 IPn3G. 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 IPn3G into a web browser. As seen below, when the IP Address of the IPn3G is entered, the data is passed through to the attached PC. The screen shot below shows that our test setup was successful.



This is the Web Server Running on the Microhard Laptop.

If you can read this, it means that the IP-Passthrough or Port Forwarding exercise works!

Appendix D: Port Forwarding

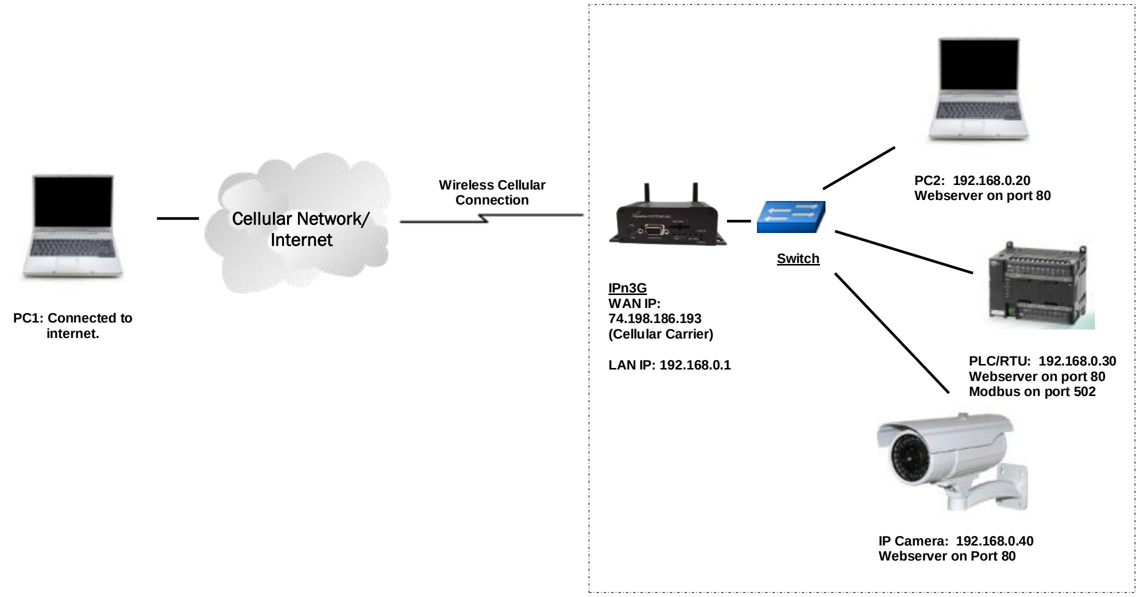
By completing the Quick Start process, a user should have been able to log in and set up the IPn3G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the IPn3G is to access connected devices remotely. In order to do this, the IPn3G 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 IPn3G through a switch, or if other features of the IPn3G are required (Serial Ports, Firewall, GPS, etc). In port forwarding, the IPn3G 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 IPn3G 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 IPn3G, 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 IPn3G are required, since in pass-through 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 IPn3G directly using the public static IP assigned by the wireless carrier, but not the devices behind it. In this case the IPn3G 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 IPn3G.



Step 1

Log into the IPn3G (Refer to Quick Start), and ensure that the ***Firewall*** is enabled. This can be found under ***Firewall > General.*** Also ensure that either ***WAN Request*** is set to Allow, which allows traffic to come in from the WAN, or that sufficient ***Rules*** or ***IP lists*** have been setup to allow specific traffic to pass through the IPn3G. Once that is complete, remember to “Apply” the changes.

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
IPn3G WebUI	74.198.186.193	80	N/A	N/A
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

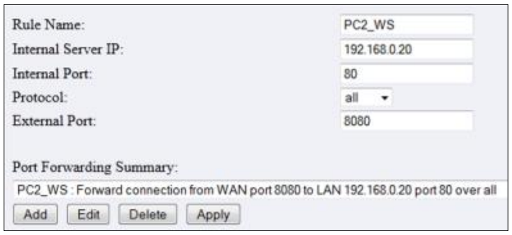
Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this is fine because they are located on different IP addresses, and the different external ports mapped by the IPn3G (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 IPn3G 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"** button to add each rule to the IPn3G.

Once all rules have been added, the IPn3G configuration should look something like what is illustrated in the screen shot to the right. Be sure to **"Apply"** the Port Forwarding list to the IPn3G.

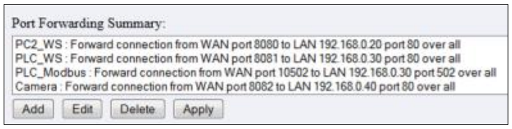
For best results, reboot the IPn3G.



Rule Name:	PC2_WS
Internal Server IP:	192.168.0.20
Internal Port:	80
Protocol:	all
External Port:	8080

Port Forwarding Summary:

PC2_WS : Forward connection from WAN port 8080 to LAN 192.168.0.20 port 80 over all



Port Forwarding Summary:

PC2_WS : Forward connection from WAN port 8080 to LAN 192.168.0.20 port 80 over all
PLC_WS : Forward connection from WAN port 8081 to LAN 192.168.0.30 port 80 over all
PLC_Modbus : Forward connection from WAN port 10502 to LAN 192.168.0.30 port 502 over all
Camera : Forward connection from WAN port 8082 to LAN 192.168.0.40 port 80 over all

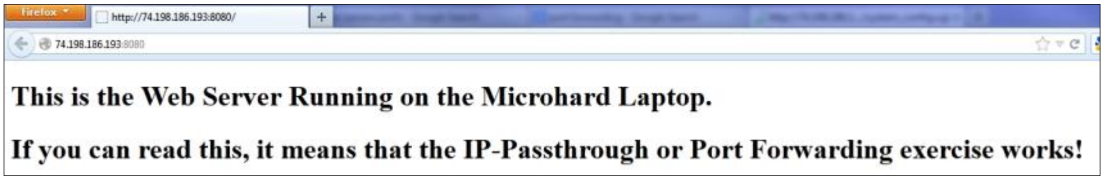
Step 4

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 IPn3G 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:



This is the Web Server Running on the Microhard Laptop.

If you can read this, it means that the IP-Passthrough or Port Forwarding exercise works!

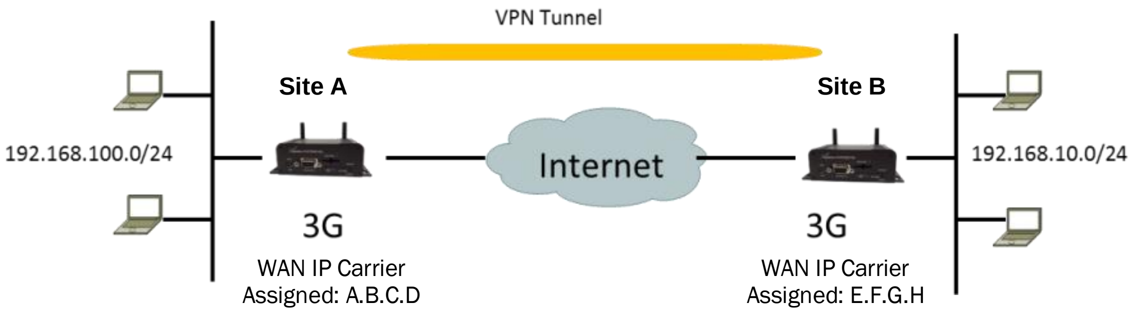
To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.

Appendix E: VPN Example

By completing the Quick Start process, a user should have been able to log in and set up the IPn3G 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 IPn3G is to access connected devices remotely. In addition to Port Forwarding and IP-Passthrough, the IPn3G 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 IPn3G 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 IPn3G devices (Example 1), 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 IPn3G to existing VPN capable devices, such as Cisco (Example 2) or Firebox.

Example 1: IPn3G to IPn3G (Site-to-Site)



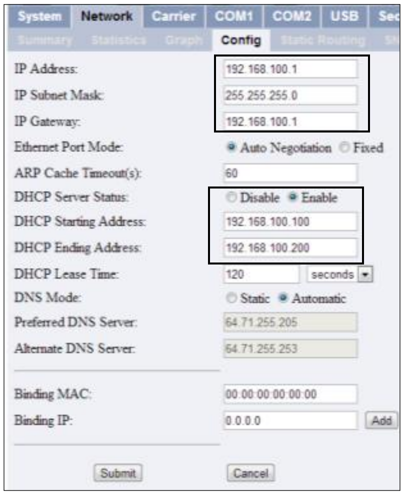
Step 1

Log into each of the IPn3Gs (Refer to Quick Start), and ensure that the ***Firewall*** is enabled. This can be found under ***Firewall > General.*** Also ensure that either ***WAN Request*** is set to Allow, which allows traffic to come in from the WAN, or that sufficient ***Rules*** or ***IP lists*** have been setup to allow specific traffic to pass through the IPn3G. Once that is complete, remember to "Apply" the changes.

Step 2

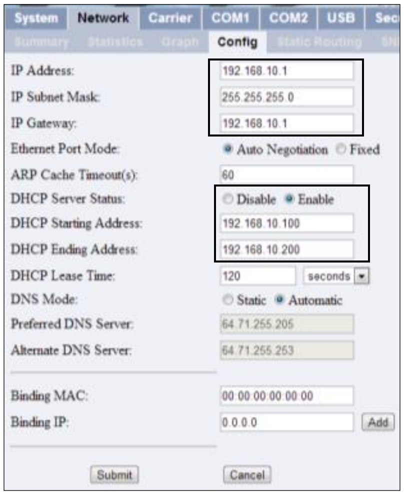
Configure the LAN IP and subnet for each IPn3G. The subnets must be different and cannot overlap.

Site A



IP Address:	192.168.100.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.100.1
Ethernet Port Mode:	● Auto Negotiation ○ Fixed
ARP Cache Timeout(s):	60
DHCP Server Status:	○ Disable ● Enable
DHCP Starting Address:	192.168.100.100
DHCP Ending Address:	192.168.100.200
DHCP Lease Time:	120 seconds
DNS Mode:	○ Static ● Automatic
Preferred DNS Server:	64.71.255.205
Alternate DNS Server:	64.71.255.253
Binding MAC:	00:00:00:00:00:00
Binding IP:	0.0.0.0

Site B

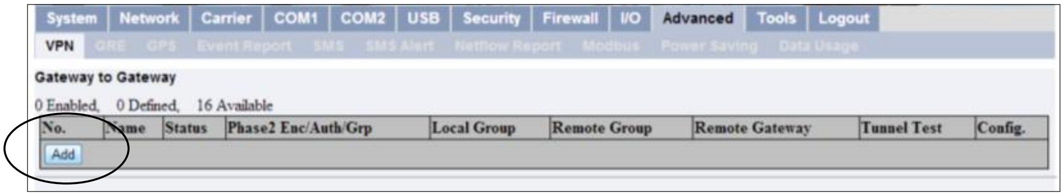


IP Address:	192.168.10.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.10.1
Ethernet Port Mode:	● Auto Negotiation ○ Fixed
ARP Cache Timeout(s):	60
DHCP Server Status:	○ Disable ● Enable
DHCP Starting Address:	192.168.10.100
DHCP Ending Address:	192.168.10.200
DHCP Lease Time:	120 seconds
DNS Mode:	○ Static ● Automatic
Preferred DNS Server:	64.71.255.205
Alternate DNS Server:	64.71.255.253
Binding MAC:	00:00:00:00:00:00
Binding IP:	0.0.0.0

Appendix E: VPN Example

Step 3

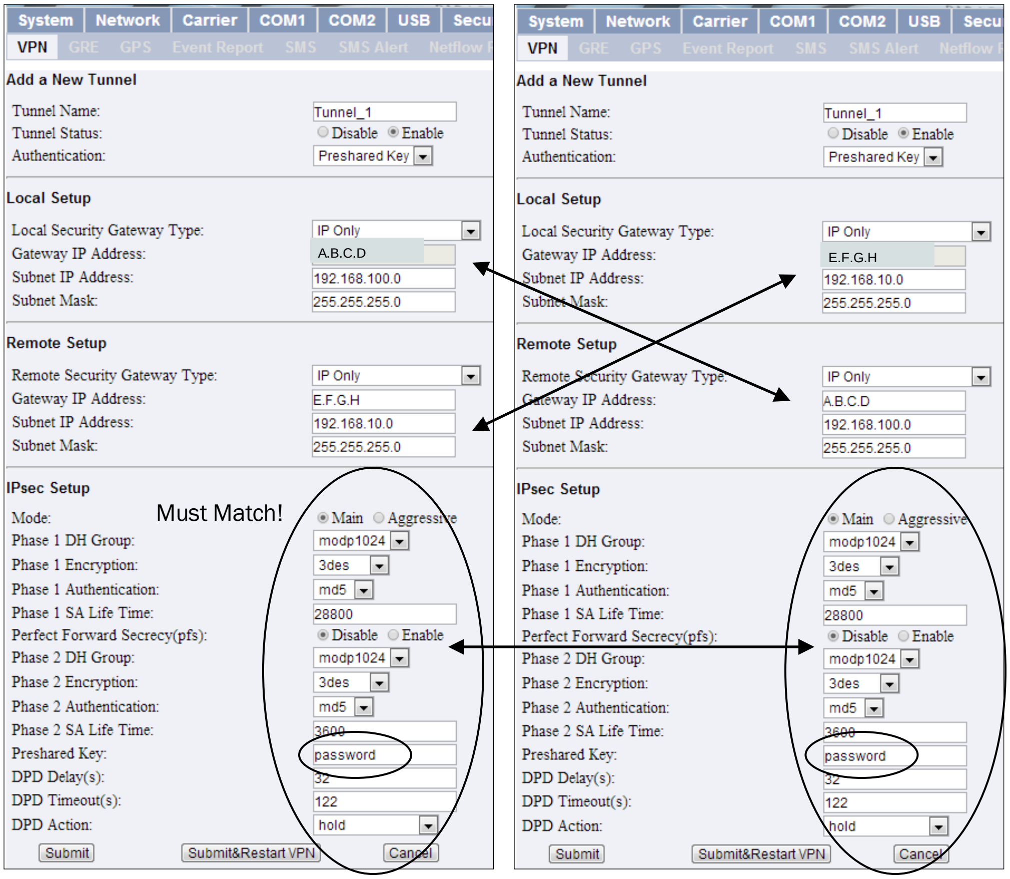
Add a VPN Gateway to Gateway tunnel on each IPn3G.



Gateway to Gateway

0 Enabled, 0 Defined, 16 Available

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.



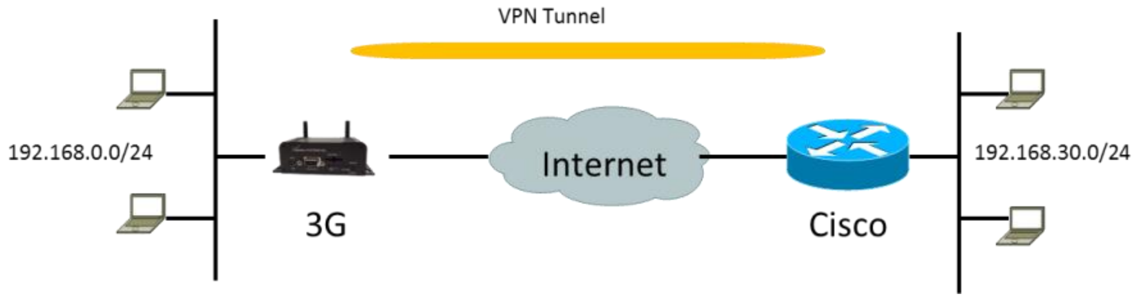
	Site A	Site B
Add a New Tunnel		
Tunnel Name:	Tunnel_1	Tunnel_1
Tunnel Status:	○ Disable ● Enable	○ Disable ● Enable
Authentication:	Preshared Key	Preshared Key
Local Setup		
Local Security Gateway Type:	IP Only	IP Only
Gateway IP Address:	A.B.C.D	E.F.G.H
Subnet IP Address:	192.168.100.0	192.168.10.0
Subnet Mask:	255.255.255.0	255.255.255.0
Remote Setup		
Remote Security Gateway Type:	IP Only	IP Only
Gateway IP Address:	E.F.G.H	A.B.C.D
Subnet IP Address:	192.168.10.0	192.168.100.0
Subnet Mask:	255.255.255.0	255.255.255.0
IPsec Setup		
Mode:	● Main ○ Aggressive	● Main ○ Aggressive
Phase 1 DH Group:	modp1024	modp1024
Phase 1 Encryption:	3des	3des
Phase 1 Authentication:	md5	md5
Phase 1 SA Life Time:	28800	28800
Perfect Forward Secrecy(pfs):	● Disable ○ Enable	● Disable ○ Enable
Phase 2 DH Group:	modp1024	modp1024
Phase 2 Encryption:	3des	3des
Phase 2 Authentication:	md5	md5
Phase 2 SA Life Time:	3600	3600
Preshared Key:	password	password
DPD Delay(s):	32	32
DPD Timeout(s):	122	122
DPD Action:	hold	hold

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: VPN Example

Example 2: IPn3G to Cisco ASA 5505

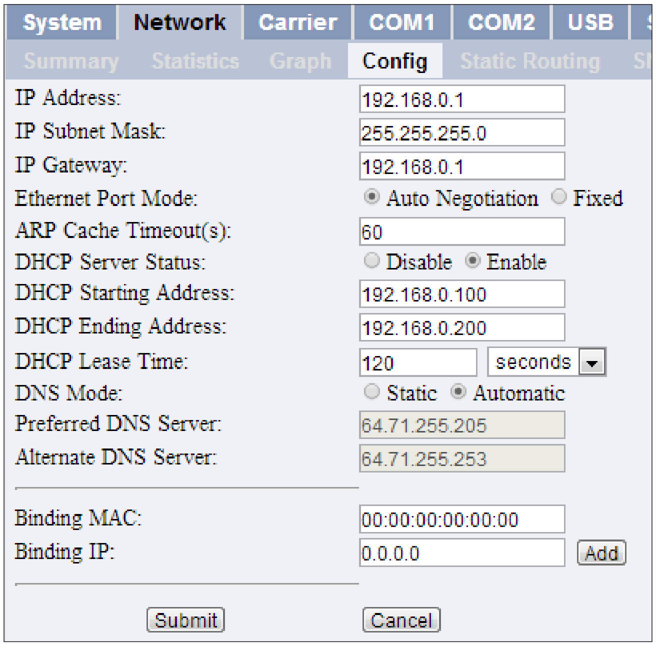


Step 1

Log into the IPn3G (Refer to Quick Start), and ensure that the ***Firewall*** is enabled. This can be found under ***Firewall > General.*** Also ensure that either ***WAN Request*** is set to Allow, which allows traffic to come in from the WAN, or that sufficient ***Rules*** or ***IP lists*** have been setup to allow specific traffic to pass through the IPn3G. Once that is complete, remember to "Apply" the changes.

Step 2

Configure the LAN IP and subnet for the IPn3G.

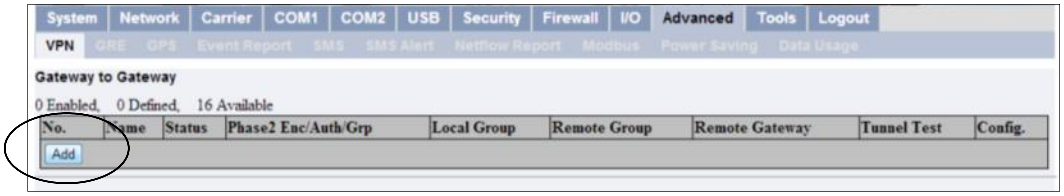


IP Address:	192.168.0.1
IP Subnet Mask:	255.255.255.0
IP Gateway:	192.168.0.1
Ethernet Port Mode:	● Auto Negotiation ○ Fixed
ARP Cache Timeout(s):	60
DHCP Server Status:	○ Disable ● Enable
DHCP Starting Address:	192.168.0.100
DHCP Ending Address:	192.168.0.200
DHCP Lease Time:	120 seconds
DNS Mode:	○ Static ● Automatic
Preferred DNS Server:	64.71.255.205
Alternate DNS Server:	64.71.255.253
Binding MAC:	00:00:00:00:00:00
Binding IP:	0.0.0.0 Add

Appendix E: VPN Example

Step 3

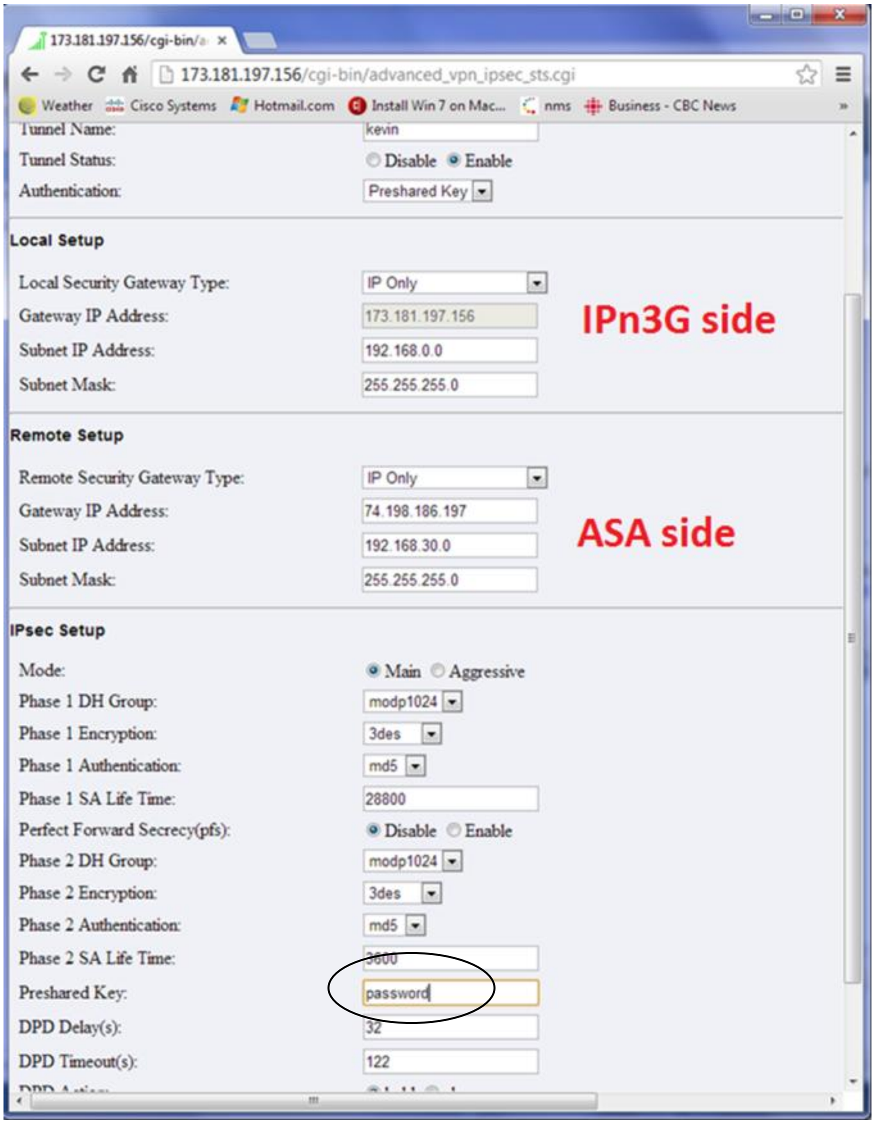
Add and configure a Gateway to Gateway VPN tunnel for the IPn3G.



Gateway to Gateway

0 Enabled, 0 Defined, 16 Available

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
Add								



Tunnel Name: kevin

Tunnel Status: ○ Disable ● Enable

Authentication: Preshared Key

Local Setup

Local Security Gateway Type: IP Only

Gateway IP Address: 173.181.197.156

Subnet IP Address: 192.168.0.0

Subnet Mask: 255.255.255.0

Remote Setup

Remote Security Gateway Type: IP Only

Gateway IP Address: 74.198.186.197

Subnet IP Address: 192.168.30.0

Subnet Mask: 255.255.255.0

IPsec Setup

Mode: ● Main ○ Aggressive

Phase 1 DH Group: modp1024

Phase 1 Encryption: 3des

Phase 1 Authentication: md5

Phase 1 SA Life Time: 28800

Perfect Forward Secrecy(pfs): ● Disable ○ Enable

Phase 2 DH Group: modp1024

Phase 2 Encryption: 3des

Phase 2 Authentication: md5

Phase 2 SA Life Time: 3600

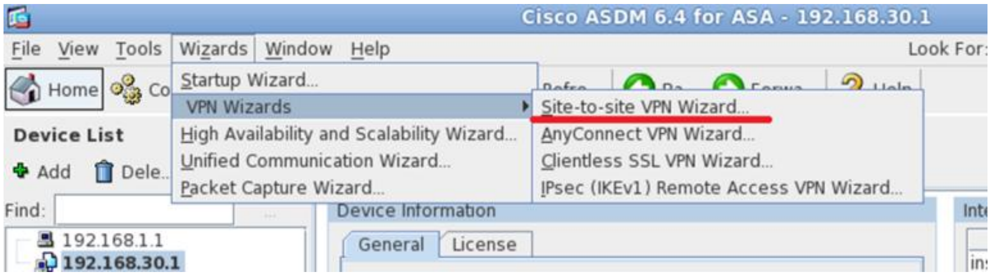
Preshared Key: password

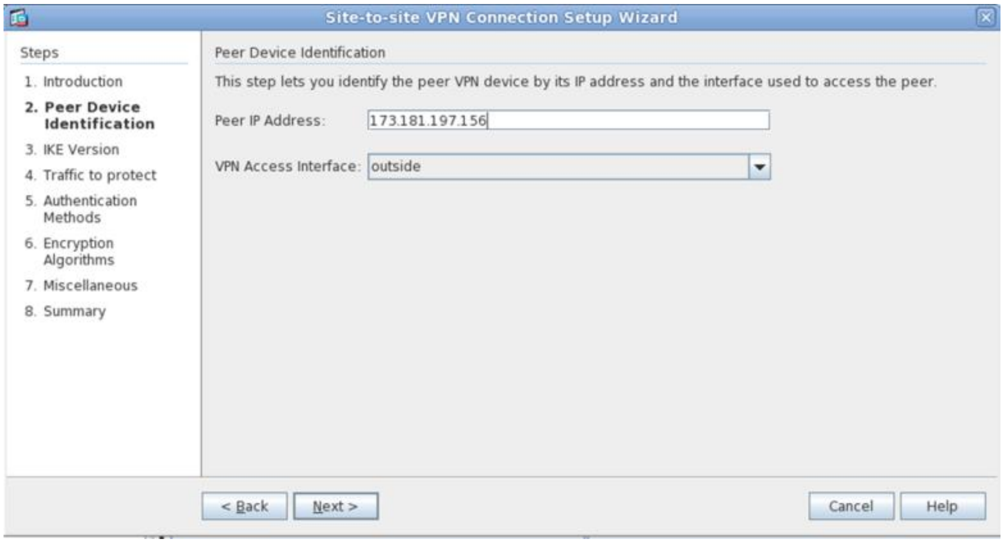
DPD Delay(s): 32

DPD Timeout(s): 122

Step 4

Using Cisco ASDM configure the ASA 5505:


Cisco ASDM 6.4 for ASA - 192.168.30.1
File View Tools Wizards Window Help
Look For:
Home
Co
Startup Wizard...
VPN Wizards
High Availability and Scalability Wizard...
Unified Communication Wizard...
Packet Capture Wizard...
Site-to-site VPN Wizard...
AnyConnect VPN Wizard...
Clientless SSL VPN Wizard...
IPsec (IKEv1) Remote Access VPN Wizard...
Device List
Add
Dele...
Find:
192.168.1.1
192.168.30.1
Device Information
General
License
Inte

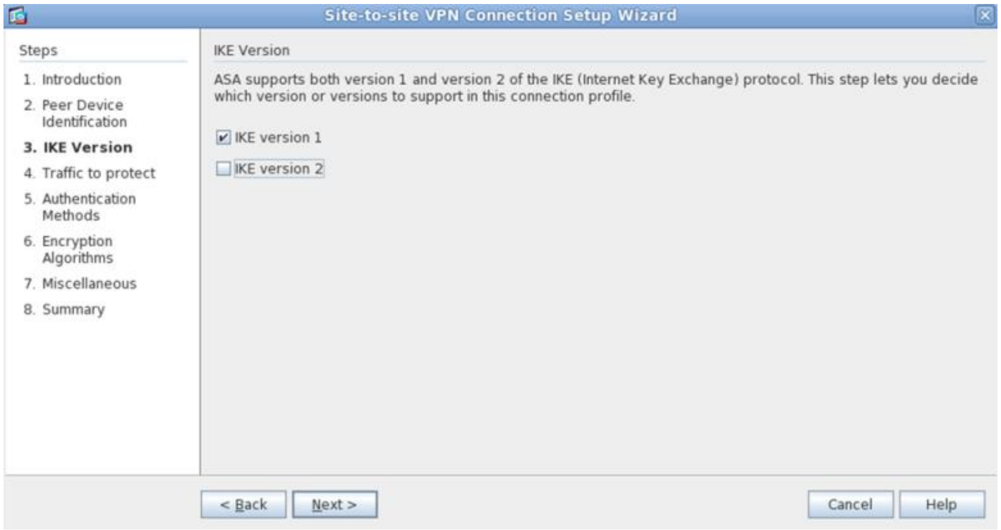


Peer Device Identification

This step lets you identify the peer VPN device by its IP address and the interface used to access the peer.

Peer IP Address: 173.181.197.156

VPN Access Interface: outside



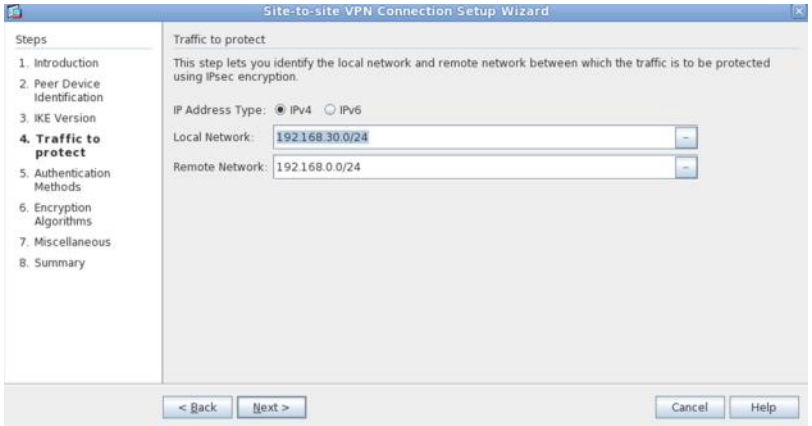
IKE Version

ASA supports both version 1 and version 2 of the IKE (Internet Key Exchange) protocol. This step lets you decide which version or versions to support in this connection profile.

☑ IKE version 1

☐ IKE version 2

Step 4 (continued…)



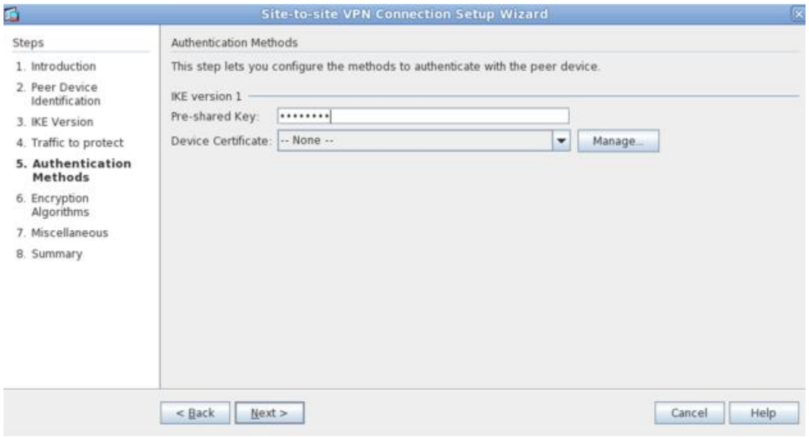
Traffic to protect

This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption.

IP Address Type: ● IPv4 ○ IPv6

Local Network: 192.168.30.0/24

Remote Network: 192.168.0.0/24



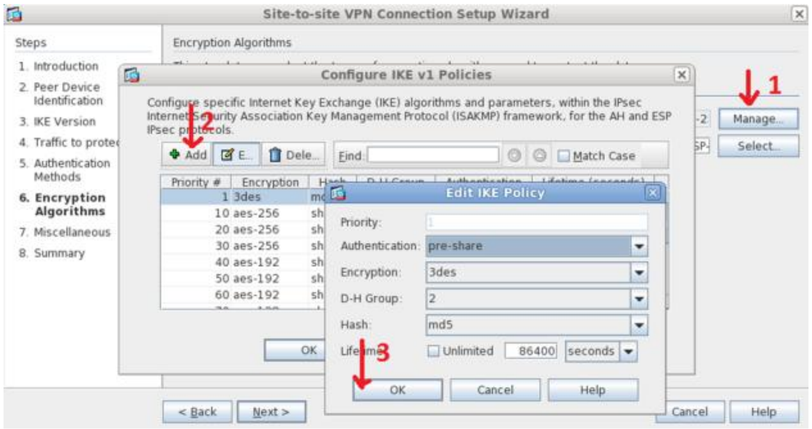
Authentication Methods

This step lets you configure the methods to authenticate with the peer device.

IKE version 1

Pre-shared Key: ••••••••

Device Certificate: -- None --



Configure IKE v1 Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Hash
1	3des	md
10	aes-256	sh
20	aes-256	sh
30	aes-256	sh
40	aes-192	sh
50	aes-192	sh
60	aes-192	sh

Edit IKE Policy

Priority: 1

Authentication: pre-share

Encryption: 3des

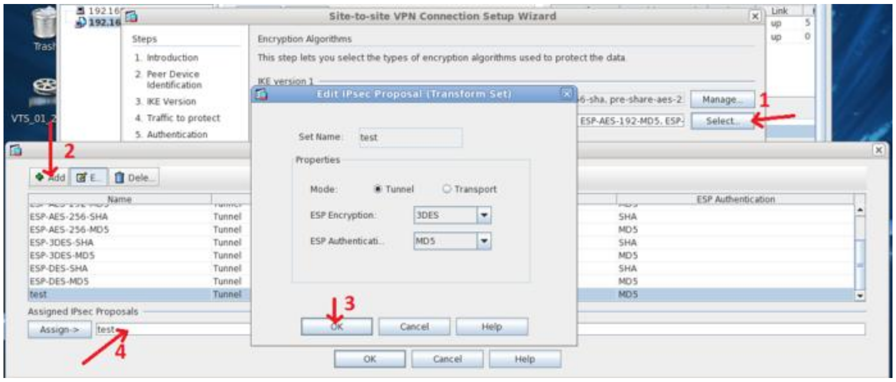
D-H Group: 2

Hash: md5

Lifetime: □ Unlimited 86400 seconds

Appendix E: VPN Example

Step 4 (continued…)



Site-to-site VPN Connection Setup Wizard

Steps
1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication

Encryption Algorithms

This step lets you select the types of encryption algorithms used to protect the data

IKE version 1

Edit IPsec Proposal (Transform Set)

Set Name: test

Properties

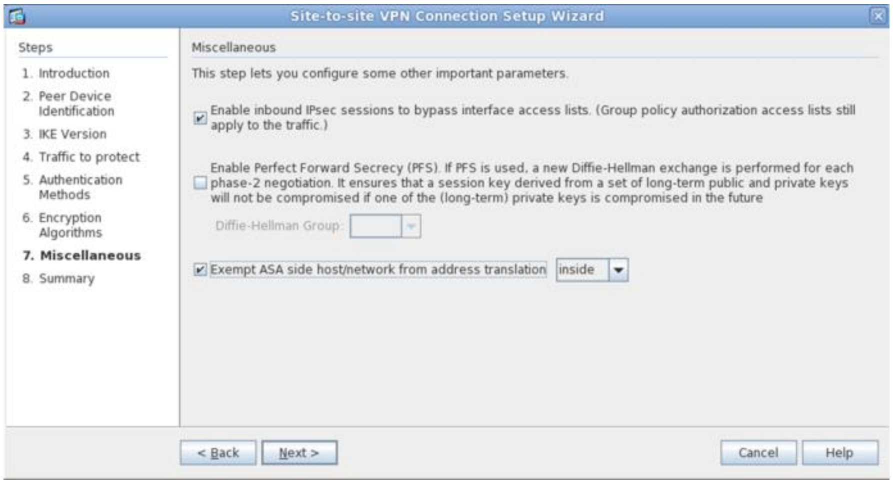
Mode: ● Tunnel ○ Transport

ESP Encryption: 3DES

ESP Authenticati..: MD5

Name	Mode	ESP Authentication
ESP-AES-256-SHA	Tunnel	SHA
ESP-AES-256-MD5	Tunnel	MD5
ESP-3DES-SHA	Tunnel	SHA
ESP-3DES-MD5	Tunnel	MD5
ESP-DES-SHA	Tunnel	SHA
ESP-DES-MD5	Tunnel	MD5
test	Tunnel	MD5

Assigned IPsec Proposals: test



Site-to-site VPN Connection Setup Wizard

Steps
1. Introduction
2. Peer Device Identification
3. IKE Version
4. Traffic to protect
5. Authentication Methods
6. Encryption Algorithms
7. **Miscellaneous**
8. Summary

Miscellaneous

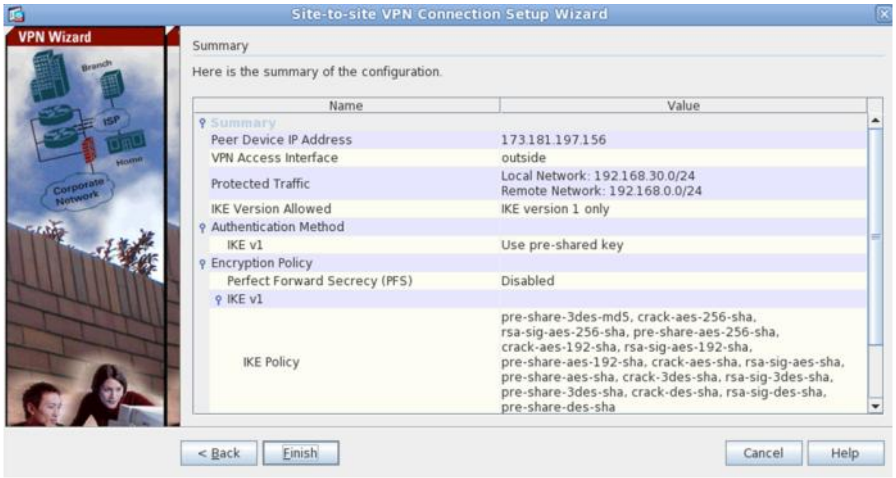
This step lets you configure some other important parameters.

☑ Enable inbound IPsec sessions to bypass interface access lists. (Group policy authorization access lists still apply to the traffic.)

□ Enable Perfect Forward Secrecy (PFS). If PFS is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation. It ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the (long-term) private keys is compromised in the future.

Diffie-Hellman Group:

☑ Exempt ASA side host/network from address translation: inside



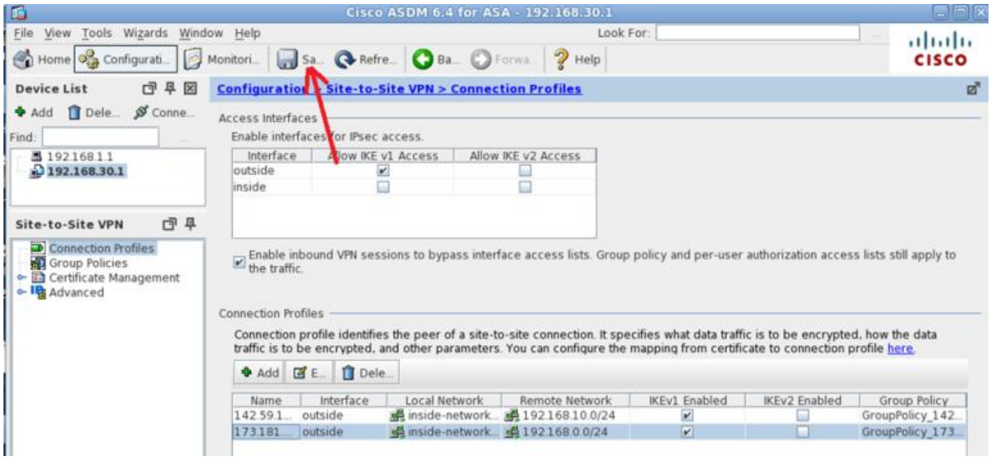
Site-to-site VPN Connection Setup Wizard

Summary

Here is the summary of the configuration.

Name	Value
Summary	
Peer Device IP Address	173.181.197.156
VPN Access Interface	outside
Protected Traffic	Local Network: 192.168.30.0/24 Remote Network: 192.168.0.0/24
IKE Version Allowed	IKE version 1 only
Authentication Method	
IKE v1	Use pre-shared key
Encryption Policy	
Perfect Forward Secrecy (PFS)	Disabled
IKE v1	
IKE Policy	pre-share-3des-md5, crack-aes-256-sha, rsa-sig-aes-256-sha, pre-share-aes-256-sha, crack-aes-192-sha, rsa-sig-aes-192-sha, pre-share-aes-192-sha, crack-aes-sha, rsa-sig-aes-sha, pre-share-aes-sha, crack-3des-sha, rsa-sig-3des-sha, pre-share-3des-sha, crack-des-sha, rsa-sig-des-sha, pre-share-des-sha

Step 4 (continued…)



Enable interfaces for IPsec access.

Interface	Allow IKE v1 Access	Allow IKE v2 Access
outside	☑	□
inside	□	□

☑ Enable inbound VPN sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Connection profile identifies the peer of a site-to-site connection. It specifies what data traffic is to be encrypted, how the data traffic is to be encrypted, and other parameters. You can configure the mapping from certificate to connection profile here.

Name	Interface	Local Network	Remote Network	IKEv1 Enabled	IKEv2 Enabled	Group Policy
142.59.1...	outside	inside-network...	192.168.10.0/24	☑	□	GroupPolicy_142...
173.181...	outside	inside-network...	192.168.0.0/24	☑	□	GroupPolicy_173...

Step 5

ASA 5505 configuration using command line interface.

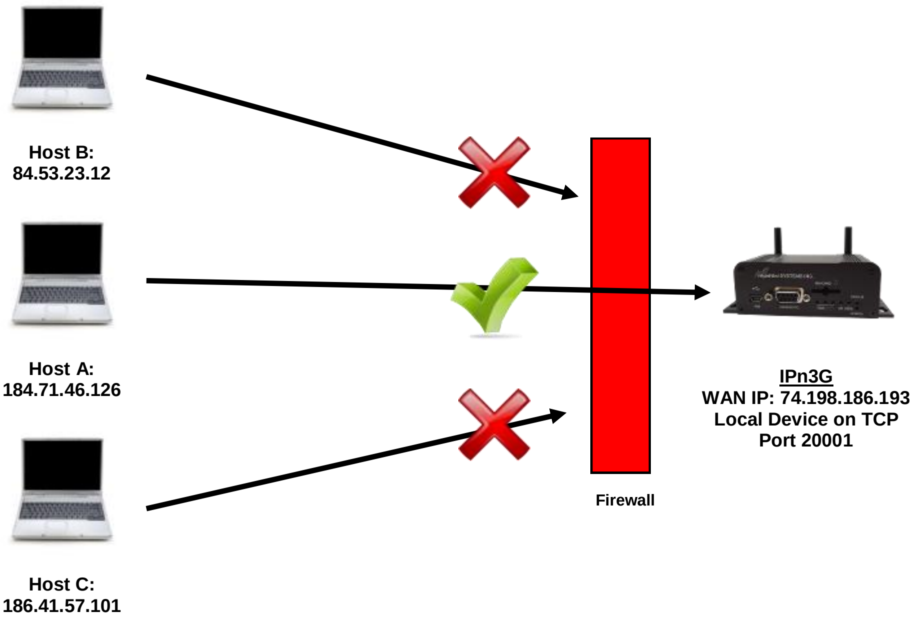
```
object network NETWORK_OBJ_192.168.0.0_24
  subnet 192.168.0.0 255.255.255.0

access-list outside_cryptomap_1 line 1 extended permit ip 192.168.30.0 255.255.255.0
192.168.0.0 255.255.255.0

group-policy GroupPolicy_173.181.197.156 internal
group-policy GroupPolicy_173.181.197.156 attributes
  vpn-tunnel-protocol ikev1
exit

tunnel-group 173.181.197.156 type ipsec-l2l
tunnel-group 173.181.197.156 general-attributes
  default-group-policy GroupPolicy_173.181.197.156
tunnel-group 173.181.197.156 ipsec-attributes

  ikev1 pre-shared-key **********
  isakmp keepalive threshold 10 retry 2

crypto map outside_map 2 match address outside_cryptomap_1
crypto map outside_map 2 set  peer  173.181.197.156
crypto map outside_map 2 set  ikev1 transform-set  test

nat (inside,outside) 2 source static NETWORK_OBJ_192.168.30.0_24

NETWORK_OBJ_192.168.30.0_24 destination static NETWORK_OBJ_192.168.0.0_24
NETWORK_OBJ_192.168.0.0_24 no-proxy-arp route-lookup
```

Appendix F: Firewall Example

By completing the Quick Start process, a user should have been able to log in and set up the IPn3G 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 IPn3G 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 IPn3G is paramount for a secure deployment. The firewall features of the IPn3G allow a user to limit access to the IPn3G and the devices connected to it by the following means

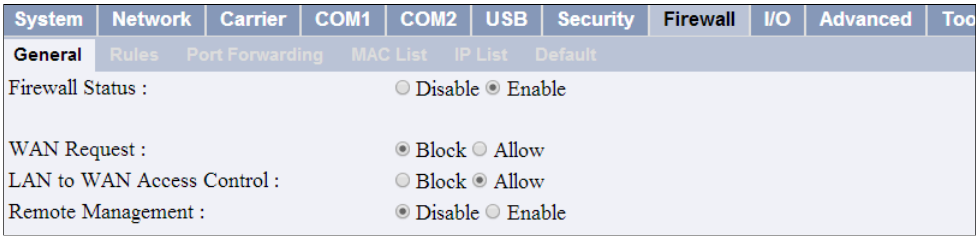
- Customizable Rules
- MAC and/or IP List
- ACL (Access Control List) or Blacklist using the above tools.

Consider the following example. An IPn3G 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 IPn3G and attached device, including the remote management features.



Step 1

Log into the IPn3G (Refer to Quick Start). Navigate to the Firewall tab as shown below and ensure that the Firewall is turned on by enabling the ***Firewall Status***. Next block all WAN traffic by setting the ***WAN Request*** to Block, and disable ***Remote Management***. Be sure to Apply the settings. At this point it should be impossible to access the IPn3G from the WAN.



Firewall Status : ○ Disable ● Enable

WAN Request : ● Block ○ Allow

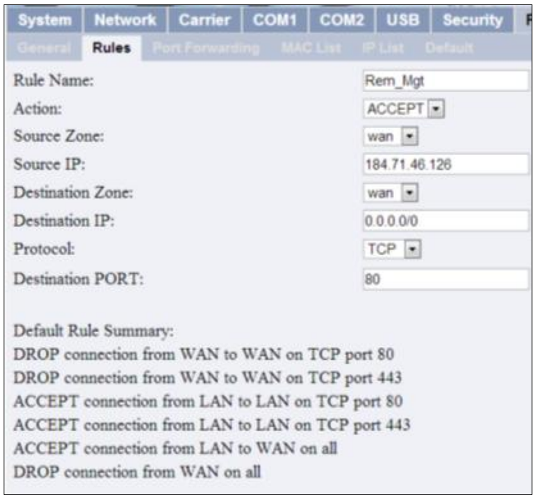
LAN to WAN Access Control : ○ Block ● Allow

Remote Management : ● Disable ○ Enable

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).

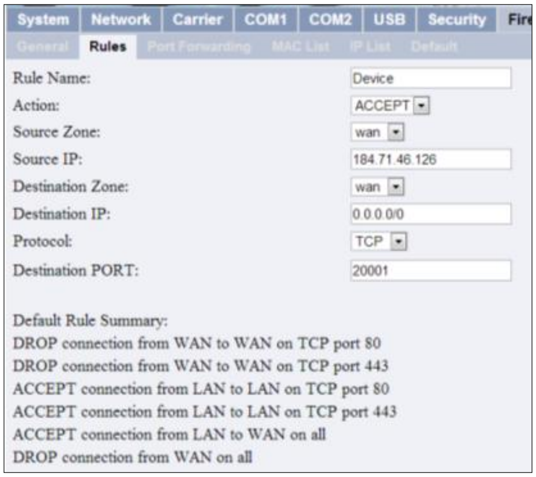
Rule 1



Rule Name:	Rem_Mgt
Action:	ACCEPT
Source Zone:	wan
Source IP:	184.71.46.126
Destination Zone:	wan
Destination IP:	0.0.0.0/0
Protocol:	TCP
Destination PORT:	80

Default Rule Summary:
DROP connection from WAN to WAN on TCP port 80
DROP connection from WAN to WAN on TCP port 443
ACCEPT connection from LAN to LAN on TCP port 80
ACCEPT connection from LAN to LAN on TCP port 443
ACCEPT connection from LAN to WAN on all
DROP connection from WAN on all

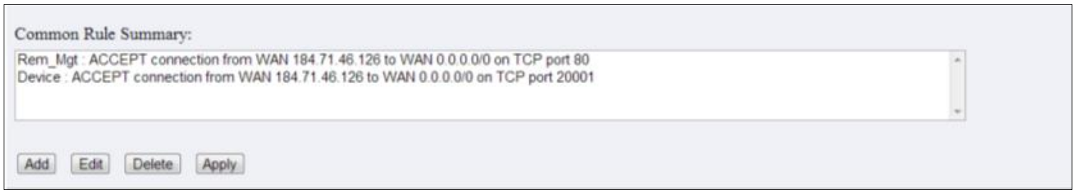
Rule 2



Rule Name:	Device
Action:	ACCEPT
Source Zone:	wan
Source IP:	184.71.46.126
Destination Zone:	wan
Destination IP:	0.0.0.0/0
Protocol:	TCP
Destination PORT:	20001

Default Rule Summary:
DROP connection from WAN to WAN on TCP port 80
DROP connection from WAN to WAN on TCP port 443
ACCEPT connection from LAN to LAN on TCP port 80
ACCEPT connection from LAN to LAN on TCP port 443
ACCEPT connection from LAN to WAN on all
DROP connection from WAN on all

After each rule is created be sure to click the ***ADD*** button, once both rules are created select the ***APPLY*** button to write the rules to the IPn3G. The common rule summary should look like what is shown below.



Common Rule Summary:
Rem_Mgt : ACCEPT connection from WAN 184.71.46.126 to WAN 0.0.0.0/0 on TCP port 80
Device : ACCEPT connection from WAN 184.71.46.126 to WAN 0.0.0.0/0 on TCP port 20001

Step 3

Test the connections. The IPn3G should only allow connections to the port specified from the Host A. An alternate means to limit connections to the IPn3G to a specific IP would have been to use the 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 G: Troubleshooting

Below is a number of the common support questions that are asked about the IPn3G. The purpose of the section is to provide answers and/or direction on how to solve common problems with the IPn3G.

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 IPn3G. For instructions of how to log into the IPn3G refer to the Quick Start.

Question: *What is the default IP Address of the IPn3G?*

Answer: The IPn3G has two interfaces that are available for local configuration. The default IP address for the LAN (the RJ45 connector on the back of the unit) is 192.168.0.1. The default IP address for the USB (requires drivers to be installed), is 192.168.111.1.

Question: *What is the default login for the IPn3G?*

Answer: The default username is ***admin***, *the default password is* ***admin***.

Question: *Where do I get the USB drivers?*

Answer: The drivers can be downloaded from the Microhard Support Site. Which is located at:

www.microhardcorp.com/support

To download items from the support site, you must first login. An account can be created, or you can use the default account ***cellular@microhardcorp.com***, password ***mhscell***.

Question: *How do I install the USB drivers?*

Answer: Watch our video at: *http://www.microhardcorp.com/IPn3G-Video.php*, for step by step instructions.

Question: *What information do I need to get from my wireless carrier to set up the IPn3G?*

Answer: The APN is required to configure the IPn3G 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.

Question: *How do I reset my modem to factory default settings?*

Answer: If you are logged into the IPn3G navigate to the Tools > Default Tab. If you cannot log in, power on the IPn3G and wait until the status LED in on solid (not flashing). Press and hold the CONFIG button until the unit reboots (about 8 seconds).

Appendix G: Troubleshooting

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 IPn3G and nothing happens?*

Answer: In addition to the basic serial port settings, the IP Protocol Config has to be configured. Refer to the COM1/2 Configuration pages for a description of the different options.

Question: *How do I access the devices behind the modem remotely?*

Answer: To access devices behind the IPn3G remotely, several methods can be used:

A. IP Passthrough - The IPn3G 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 set up firewall rules and/or port forwarding rules but they do not work?*

Answer: Ensure that the Firewall is turned ***ON***. Even port forwarding requires that the firewall feature is enabled. Also, ensure the WAN request is enabled. If blocked, additional rules will need to be created for any external request.

Question: *I have Internet/WAN access but I cannot ping the device remotely?*

Answer: Ensure that the WAN request is enabled in the Firewall settings.

Question: *I have Internet/WAN access but I cannot ping the device remotely?*

Answer: Ensure that the WAN request is enabled in the Firewall settings.

Question: *I’m using IP-Passthrough but the serial ports won’t work?*

Answer: When using IP-Passthrough, the WAN 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.

Appendix G: Troubleshooting

Question: *I'm using IP-Passthrough but the modem won't take my Firewall settings?*

Answer: When using IP-Passthrough, the WAN 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: *I cannot get IP-Passthrough to work?*

Answer: When using IP-Passthrough, the WAN IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. In order for IP-Passthrough to work, the connected local device ***must*** have DHCP enabled.

Question: *Why does my modem reset every 10 minutes (or other time)?*

Answer: There are a number of processes in the IPn3G 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. Wireless Traffic Timeout - Detects if there is any Wireless Traffic between the IPn3G and the Cellular Carrier. Will reboot modem when timer expires unless there is traffic. System > Settings.
2. ICMP Keep Alive - Attempts to contact a configured host on a defined basis. Will reboot modem if host is unreachable. Enabled by default to attempt to ping www.google.com. May need to disable of private networks. Carrier > Config.
3. Reboot Scheduler - The IPn3G can be set to reboot on a regular basis. Tools > Reboot.
4. Local Device Monitor - The IPn3G will monitor a local device, if that device is not present the IPn3G may reboot. Network > Device Monitor.

Question: *How do I set up VPN?*

Answer: Refer to the VPN Appendix for an example.

Appendix H: “system.conf” File Structure (1 of 25)

The following pages show an example “system.conf” file exported from a IPn3G running Software Version v1.2.2-r1045d, file may change as features are added or modified.

```
BASIC_SETTINGS_BEGIN:

#Hardware Version:--Read Only
Hardware_Version=v2.0.0

#Software Version:--Read Only
Software_Version=v1.2.2-r1045c

#Radio Version:--Read Only
Radio_Version=0.

#Radio Description:
Radio_Description=IPn3G

#Date(yyyy-mm-dd):
System_Date=2012-02-01

#Time(hh:mm:ss):
System_Time=10:41:25

#UTC Time Offset(+/-hh:mm):
System_UTC_Time_Offset=America/Edmonton

#Console Timeout(s):
System_Console_Timeout=0

#Wireless traffic Timeout(s):
System_Traffic_Watchdog_Timer=600

#System Default Button: A - Enable B - Disable
System_Default_Button=A

#System Syslog Server IP:
System_Syslog_Server_IP=0.0.0.0

#System Syslog Server Address:
System_Syslog_Server_Port=514

#NAT: A - Disable B - Enable
PPP_NAT=B

#PPP Status: A - Disable B - Enable
PPP_STATUS=B

#IP-Passthrough: A - Disable B - Ethernet
PPP_IP_Passthrough=A

#Dial-on-Demand: A - Disable B - Enable
PPP_DIAL_ONDEMAND=A

#Idle Timeout(s):
PPP_IDLE_TIME_OUT=0

#Connect Timeout(s):
PPP_CONNECT_TIMEOUT=90
```

Appendix H: “system.conf” File Structure (2 of 25)

```
#Dialing Max Retries:
PPP_DIALING_MAX_RETRY=0

#Authentication Type: A - NoAuth B - chap C - pap D - pap-chap
PPP_AUTH_TYPE=B

#User Name:
PPP_USERNAME=

#Password:
PPP_PASSWORD=

#SIM Pin:
PPP_SIM_PIN=

#Dial Number:
PPP_DIAL_NUM=*99***1#

#Connect String:
PPP_CONN_STR=CONNECT

#Access Point Name(APN):
PPP_Acess_Point_Name=staticip.apn

#Carriers: A - Automatic B - Manual
PPP_Carriers=A

#Carrier ID:
PPP_Carrier_Manal_ID=0

#Initialization 1:
PPP_INIT_STR1=

#Initialization 2:
PPP_INIT_STR2=

#Initialization 3:
PPP_INIT_STR3=

#Initialization 4:
PPP_INIT_STR4=

#Static IP Addr:
PPP_Static_IP=0.0.0.0

#Use Remote DNS: A - Disable B - Enable
PPP_Use_Remote_IP=B

#Port Status: A - Disable B - Enable
COM1_Port_Status=B

#Channel Mode: A - RS232 B - RS485 C - RS422
COM1_Chanel_Mode=A

#Data Baud Rate: A - 300  B - 600  C - 1200 D - 2400
#   E - 3600 F - 4800 G - 7200 H - 9600 I - 14400 J - 19200
#   K - 28800 L - 38400 M - 57600 N - 115200 O - 230400
#   P - 460800 Q - 921600
COM1_Data_Baud_Rate=H

#Data Format: A - 8N1 B - 8N2 C - 8E1 D - 8O1 E - 7N1
#   F - 7N2 G - 7E1 H - 7O1 I - 7E2 J - 7O2
COM1_Data_Format=A
```

Appendix H: “system.conf” File Structure (3 of 25)

```
#Flow Control: A - None B - Hardware C - CTS Framing
COM1_Flow_Control=A

#Pre-Data Delay(ms):
COM1_Pre_Data_Delay=100

#Post-Data Delay(ms):
COM1_Post_Data_Delay=100

#Data Mode: A - Seamless B - Transparent
COM1_Data_Mode=B

#Character Timeout:
COM1_Character_Timeout=0

#Maximum Packet Size:
COM1_Max_Packet_Len=1024

#Priority: A - Normal B - Medium C - High
COM1_QoS=A

#No-Connection Data Intake: A - Disable B - Enable
COM1_NoConnect_Data_Intake=B

#Protocol Config A - TCP Client B - TCP Server C - TCP Client/Server
#   D - UDP Point to Point E - UDP Point to Multipoint(P)
#   F - UDP Point to Multipoint(MP) G - UDP Multipoint to Multipoint
#   H - SMTP Client I - PPP J - SMS Transparent Mode
#   K - SMS AT Mode
COM1_IP_Protocol=F

#Port Status: A - Disable B - Enable
COM2_Port_Status=A

#Data Baud Rate: A - 300 B - 600 C - 1200 D - 2400
#   E - 3600 F - 4800 G - 7200 H - 9600 I - 14400 J - 19200
#   K - 28800 L - 38400 M - 57600 N - 115200
COM2_Data_Baud_Rate=N

#Data Format: A - 8N1 B - 8N2 C - 8E1 D - 8O1 E - 7N1
#   F - 7N2 G - 7E1 H - 7O1 I - 7E2 J - 7O2
COM2_Data_Format=A

#Data Mode: A - Seamless B - Transparent
COM2_Data_Mode=B

#Character Timeout:
COM2_Character_Timeout=0

#Maximum Packet Size:
COM2_Max_Packet_Len=1024

#Priority: A - Normal B - Medium C - High
COM2_QoS=A

#No-Connection Data Intake: A - Disable B - Enable
COM2_NoConnect_Data_Intake=B

#Protocol Config A - TCP Client B - TCP Server C - TCP Client/Server
#   D - UDP Point to Point E - UDP Point to Multipoint(P)
#   F - UDP Point to Multipoint(MP) G - UDP Multipoint to Multipoint
COM2_IP_Protocol=F

#USB Device Port Mode: A - Console Mode B - Data Mode
#   C - NDIS Mode
USB_Device_Mode=C
```

Appendix H: “system.conf” File Structure (4 of 25)

```
#IP Address:
NetWork_IP_Address=192.168.0.1

#IP Subnet Mask:
NetWork_IP_Subnet_Mask=255.255.255.0

#IP Gateway:
NetWork_IP_Gateway=192.168.0.1

#Preferred DNS Server:
NetWork_IP_Primary_DNS_Server=8.8.8.8

#Alternate DNS Server:
NetWork_IP_Alternate_DNS_Server=8.8.4.4

#IP Address:
NetWork_IP_WL_Address=192.168.2.1

#IP Subnet Mask:
NetWork_IP_WL_Subnet_Mask=255.255.255.0

#Preferred DNS Server:
NetWork_IP_WL_Prim_DNS_Server=0.0.0.0

#Alternate DNS Server:
NetWork_IP_WL_Alter_DNS_Server=0.0.0.0

#VPN Status: A - Disable B - Enable
NetWork_IP_VPN_Status=B

#VPN Admin Password:
NetWork_IP_VPN_Passwd=admin

#NTP Time Synchronize: A - Disable B - Enable
NetWork_NTP_Server_Status=B

#NTP Server (IP/Name):
NetWork_NTP_Server_Address=pool.ntp.org

#DHCP Server Status: A - Disable B - Enable
NetWork_DHCP_Server_Status=B

#DHCP Server Subnet:
NetWork_DHCP_Server_Subnet=192.168.0.0

#DHCP Server Netmask:
NetWork_DHCP_Server_Netmask=255.255.255.0

#DHCP Starting Address:
NetWork_DHCP_Start_Address=192.168.0.100

#DHCP Ending Address:
NetWork_DHCP_End_Address=192.168.0.200

#Gateway Address:
NetWork_DHCP_Gateway_Address=192.168.0.1
NetWork_DHCP_DNS_Address=0.0.0.0

#WINS Address:
NetWork_DHCP_Wins_Address=0.0.0.0

#New Binding MAC:
NetWork_DHCP_Binding_MAC=00:00:00:00:00:00

#New Binding IP:
NetWork_DHCP_Binding_IP=0.0.0.0
```

Appendix H: “system.conf” File Structure (5 of 25)

```
#Delete Binding: A - No
NetWork_DHCP_Binding_Delete=A

# Already bound MAC and IP
NetWork_DHCP_BIND_MAC1=
NetWork_DHCP_BIND_IP1=
NetWork_DHCP_BIND_MAC2=
NetWork_DHCP_BIND_IP2=
NetWork_DHCP_BIND_MAC3=
NetWork_DHCP_BIND_IP3=
NetWork_DHCP_BIND_MAC4=
NetWork_DHCP_BIND_IP4=
NetWork_DHCP_BIND_MAC5=
NetWork_DHCP_BIND_IP5=

#SNMP Operation Mode: A - Disable B - V1&V2c&V3
NetWork_SNMP_MODE=B

#Read Only Community Name:
NetWork_SNMP_Read_Community_Name=public

#Read Write Community Name:
NetWork_SNMP_Write_Community_Name=private

#SNMP V3 User Name:
NetWork_SNMP_V3_User_Name=V3user

#V3 User Read Write Limit: A - Read Only B - Read Write
NetWork_SNMP_V3_User_ReadWrite_Limit=A

#V3 User Authentication Level: A - NoAuthNopriv B - AuthNoPriv
#   C - AuthPriv
NetWork_SNMP_V3_User_Auth_Level=B

#V3 Authentication Password:
NetWork_SNMP_V3_Auth_Password=00000000

#V3 Privacy Password:
NetWork_SNMP_V3_Privacy_Password=00000000

#SNMP Trap Version: A - V1 Traps B - V2 Traps C - V3 Traps
#   D - V1&V2 Traps E - V1&V2&V3 Traps
NetWork_SNMP_Trap_Version=A

#Auth Failure Traps: A - Disable B - Enable
NetWork_SNMP_Auth_Traps_Status=A

#Trap Community Name:
NetWork_SNMP_Trap_Community_Name=TrapUser

#Trap Manage Host IP:
NetWork_SNMP_Trap_Manage_Host=0.0.0.0

#SNMP Listening Protocol: A - UDP B - TCP
NetWork_SNMP_Listening_Protocol=A

#SNMP Listening Port:
NetWork_SNMP_Listening_Port=161

#Spanning-Tree Protocol Status: A - On B - Off
NetWork_Bridge_STP_Status=A

#Quality of Service Status: A - Disable B - Enable
NetWork_QoS_Status=A
```

Appendix H: “system.conf” File Structure (6 of 25)

```
#VLAN Status: A - Disable B - Enable
VLAN_Status=A

#Management VLAN (VLAN ID):
Management_VLAN_ID=1

#Mesh Status: A - Disable B - Enable
Mesh_L2_Status=A

#Keep Alive Check: A - Disable B - Enable
Radio_KeepAlive_Status=B

#HostName:
Radio_KeepAlive_HostName=www.google.com

#Interval(s):
Radio_KeepAlive_Interval=600

#Count:
Radio_KeepAlive_Count=10

#Wakeup On Call: A - Disable B - Enable
Radio_WakeOnCall_Status=A

#Time Delay(s):
Radio_WakeOnCall_TimeDelay=10

#Dial On Demand From LAN: A - Disable B - Enable
Radio_WakeOnCall_From_LAN=B

#Initialization 1:
Radio_WakeOnCall_InitStr1=

#Initialization 2:
Radio_WakeOnCall_InitStr2=

#Initialization 3:
Radio_WakeOnCall_InitStr3=

#Initialization 4:
Radio_WakeOnCall_InitStr4=

#Caller IDs:
Radio_Static_IP_Addr=

#Caller Acknowledgement:
Radio_WakeOnCall_CallerID=
Radio_WakeOnCall_CallerAck=

#PowerOn Init String:
Radio_PowerOn_InitStr=

#Remote Server IP Address:
COM1_T_Client_Server_Addr=0.0.0.0

#Remote Server Port:
COM1_T_Client_Server_Port=20001

#Outgoing Connection Timeout:
COM1_T_Client_Timeout=60

#TCP Server Polling Mode: A - Monitor B - Multi-polling
COM1_T_Server_Polling_Mode=A

#Multi-polling Timeout(ms):
COM1_T_Server_Polling_Timeout=100
```

Appendix H: “system.conf” File Structure (7 of 25)

```
#Local Listening Port:
COM1_T_Server_Listen_Port=20001

#Incoming Connection Timeout:
COM1_T_Server_Timeout=300

#Remote IP Address:
COM1_U_PtoP_Remote_Addr=0.0.0.0

#Remote Port:
COM1_U_PtoP_Remote_Port=20001

#Listening Port:
COM1_U_PtoP_Listen_Port=20001

#UDP Timeout(s):
COM1_U_PtoP_Timeout=10

#Multicast IP Address:
COM1_UM_P_Multicast_Addr=224.1.1.1

#Multicast Port:
COM1_UM_P_Multicast_Port=20001

#Listening Port:
COM1_UM_P_Listen_Port=20011

#Time to Live:
COM1_UM_P_TTL=1

#Remote IP Address:
COM1_UM_M_Remote_Addr=0.0.0.0

#Remote Port:
COM1_UM_M_Remote_Port=20011

#Multicast IP Address:
COM1_UM_M_Multicast_Addr=224.1.1.1

#Multicast Port:
COM1_UM_M_Multicast_Port=20001

#Multicast IP Address:
COM1_UMTOM_Multicast_Addr=224.1.1.1

#Multicast Port:
COM1_UMTOM_Multicast_Port=20011

#Time to Live:
COM1_UMTOM_Multicast_TTL=1

#Listen Multicast IP Address:
COM1_UMTOM_Listen_Multicast_Addr=224.1.1.1

#Listen Multicast Port:
COM1_UMTOM_Listen_Multicast_Port=20011

#Mail Subject:
COM1_SMTP_Mail_Subject=COM1 Message

#Mail Server (IP/Name):
COM1_SMTP_Server=0.0.0.0

#Mail Recipient:
COM1_SMTP_Recipient=host@
```

Appendix H: “system.conf” File Structure (8 of 25)

```
#Message Max Size:
COM1_SMTP_Buffer=1024

#Timeout(s):
COM1_SMTP_Timeout=10

#Transfer Mode: A - Text B - Attached File C - Hex Code
COM1_SMTP_Transfer_Mode=A

#PPP Local IP:
COM1_PPP_LocalIP=192.168.0.1

#PPP Host IP:
COM1_PPP_RemoteIP=192.168.0.99

#PPP Idle Timeout(s):
COM1_PPP_Idle_Timeout=30

#Remote Server IP Address:
COM2_T_Client_S_Addr=0.0.0.0

#Remote Server Port:
COM2_T_Client_S_Port=20002

#Outgoing Connection Timeout:
COM2_T_Client_Timeout=60

#TCP Server Polling Mode: A - Monitor B - Multi-polling
COM2_T_Server_Polling_Mode=A

#Multi-polling Timeout(ms):
COM2_T_Server_Polling_Timeout=100

#Local Listening Port:
COM2_T_S_Listen_Port=20002

#Incoming Connection Timeout:
COM2_T_S_Timeout=300

#Remote IP Address:
COM2_U_PtoP_R_Addr=0.0.0.0

#Remote Port:
COM2_U_PtoP_R_Port=20002

#Listening Port:
COM2_U_PtoP_L_Port=20002

#UDP Timeout(s):
COM2_U_PtoP_Timeout=10

#Multicast IP Address:
COM2_UM_P_Multicast_Addr=224.1.1.2

#Multicast Port:
COM2_UM_P_Multicast_Port=20002

#Listening Port:
COM2_UM_P_Listen_Port=20012

#Time to Live:
COM2_UM_P_TTL=1

#Remote IP Address:
COM2_UM_M_Remote_Addr=0.0.0.0
```

Appendix H: “system.conf” File Structure (9 of 25)

```
#Remote Port:
COM2_UM_M_Remote_Port=20012

#Multicast IP Address:
COM2_UM_M_Multicast_Addr=224.1.1.2

#Multicast Port:
COM2_UM_M_Multicast_Port=20002

#Multicast IP Address:
COM2_UMTOM_Multicast_Addr=224.1.1.2

#Multicast Port:
COM2_UMTOM_Multicast_Port=20012

#Time to Live:
COM2_UMTOM_Multicast_TTL=1

#Listen Multicast IP Address:
COM2_UMTOM_Listen_Multicast_Addr=224.1.1.2

#Listen Multicast Port:
COM2_UMTOM_Listen_Multicast_Port=20012

#Discovery Service: A - Disable B - Discoverable C - Changeable
Discovery_Service_Status=B

#Telnet: A - Disable B - Enable
UI_Access_Telnet=B

#HTTP: A - Disable B - Enable
UI_Access_HTTP=B

#SSH: A - Disable B - Enable
UI_Access_SSH=B

#HTTPS: A - Disable B - Enable
UI_Access_HTTPS=B

#HTTP Port:
UI_Access_HTTP_Port=80

#HTTPS Port:
UI_Access_HTTPS_Port=443

#Telnet Port:
UI_Access_Telnet_Port=23

#SSH Port:
UI_Access_SSH_Port=22

#Auth Mode: A - Local B - RADIUS&Local
AUTH_Mode=A

#RADIUS Server IP:
AUTH_Server_IP=0.0.0.0

#RADIUS Server Port:
AUTH_Server_Port=1812

#RADIUS Secret:
AUTH_Seceret=nosecret

#Repeat RADIUS Secret:
AUTH_Repeat_Seceret=nosecret
```

Appendix H: “system.conf” File Structure (10 of 25)

```
#RADIUS Timeout:
AUTH_Server_Reply_Timeout=10

#Firewall Status: A - Disable B - Enable
Firewall_Status=A

#Source Zone: A - WAN B - LAN C - FW D - VPN E - all
FW_Policy_Source_Zone=A

#Destination Zone: A - WAN B - LAN C - FW D - VPN E - all
FW_Policy_Destination_Zone=A

#Policy: A - ACCEPT B - DROP C - REJECT D - QUEUE E - CONTINUE
#   F - NONE
FW_Policy_Policy=A

#Log: A - No B - Emergancy C - Alert D - Critical E - Error
#   F - Warning G - Notice H - Information I - Debug
FW_Policy_Log=A

#Select Policy Number:
FW_Policy_Number=0

#Action: A - ACCEPT B - ACCEPT+ C - NONAT D - DROP
#   E - REJECT F - DNAT G - SAME H - REDIRECT I - CONTINUE
#   J - LOG K - QUEUE
FW_Rule_Action=A

#Source Zone: A - WAN B - LAN C - FW D - VPN E - all
FW_Rule_Source_Zone=A

#Source IP:
FW_Rule_Source_IP=0.0.0.0

#Destination Zone: A - WAN B - LAN C - FW D - VPN E - all
FW_Rule_Destination_Zone=A

#Select Service: A - Custom Service

FW_Rule_Select_Service=0

#Destination IP:
FW_Rule_Destination_IP=0.0.0.0

#Destination Port
FW_Rule_Destination_Port=0

#Protocol: A - TCP B - TCP:SYN C - UDP D - ICMP E - IPP2P
#   F - IPP2P:UDP G - IPP2P:all H - All
FW_Rule_Protocol=A

#Comment:
FW_Rule_Name=Rule 1

#Select Rule Number:
FW_Rule_Number=0

#Internal Server IP:
FW_Portfw_Server_IP=192.168.2.5

#Internal Port:
FW_Portfw_Internal_Port=0

#Protocol: A - TCP B - TCP:SYN C - UDP D - ICMP E - IPP2P
#   F - IPP2P:UDP G - IPP2P:all H - All
FW_Portfw_Protocol=A
```

Appendix H: “system.conf” File Structure (11 of 25)

```
#External Port:
FW_Portfw_External_Port=0

#Comment:
FW_Portfw_Comment=Forward 1

#Select Rule Number:
FW_Portfw_Number=0

#WAN MAC List Status: A - Disable B - Enable
FW_MAClist_WAN_Status=A

#LAN MAC List Status: A - Disable B - Enable
FW_MAClist_LAN_Status=A

#MAC Address:
FW_MAClist_MAC_Address=00:00:00:00:00:00

#Disposition: A - ACCEPT B - DROP C - REJECT
FW_MAClist_Disposition=A

#Interface: A - WAN B - LAN
FW_MAClist_Interface=A

#WAN Blacklist Status: A - Disable B - Enable
FW_Blacklist_WAN_Status=A

#LAN Blacklist Status: A - Disable B - Enable
FW_Blacklist_LAN_Status=A

#IP/Subnet or MAC Address:
FW_Blacklist_IP_MAC_Address=192.168.1.5

#Select Number:
FW_Blacklist_Number=0

#Remote IP Address:
Tool_Ping_Remote_IP_Addr=0.0.0.0

#Count:
Tool_Ping_Count=4

#Packet Size:
Tool_Ping_Packet_Size=32

#Trace Route
Tool_TraceRoute=www.google.ca

#VLAN ID (2-4094):
VLAN_ID=2

#Description:
VLAN_Description=

#Port: A - Wired Port (eth0) B - Wireless Port (ppp0)
VLAN_Seting_Port=A

#VLAN (VLAN ID):
VLAN_Setting_VLAN_ID=1

#Port Status: A - Disable B - Enable
USB_Port_Status=A
```

Appendix H: “system.conf” File Structure (12 of 25)

```
#Data Baud Rate: A - 300 B - 600 C - 1200 D - 2400
#   E - 3600 F - 4800 G - 7200 H - 9600 I - 14400 J - 19200
#   K - 28800 L - 38400 M - 57600 N - 115200 O - 230400
#   P - 460800 Q - 921600
USB_Data_Baud_Rate=N

#Data Format: A - 8N1 B - 8N2 C - 8E1 D - 8O1 E - 7N1
#   F - 7N2 G - 7E1 H - 7O1 I - 7E2 J - 7O2
USB_Data_Format=A

#Data Mode: A - Seamless B - Transparent
USB_Data_Mode=B

#Character Timeout:
USB_Character_Timeout=0

#Maximum Packet Size:
USB_Max_Packet_Len=1024

#Priority: A - Normal B - Medium C - High
USB_QoS=A

#No-Connection Data Intake: A - Disable B - Enable
USB_NoConnect_Data_Intake=B

#Modbus TCP Config...
USB_MODBUS_Mode=A

#IP Protocol Config A - TCP Client B - TCP Server C - TCP Client/Server
#   D - UDP Point to Point E - UDP Point to Multipoint(P)
#   F - UDP Point to Multipoint(MP) G - UDP Multipoint to Multipoint
USB_IP_Protocol=F

#Remote Server IP Address:
USB_T_Client_S_Addr=0.0.0.0

#Remote Server Port:
USB_T_Client_S_Port=20003

#Outgoing Connection Timeout:
USB_T_Client_Timeout=60

#TCP Server Polling Mode: A - Monitor B - Multi-polling
USB_T_Server_Polling_Mode=A

#Multi-polling Timeout(ms):
USB_T_Server_Polling_Timeout=100

#Local Listening Port:
USB_T_S_Listen_Port=20003

#Incoming Connection Timeout:
USB_T_S_Timeout=300

#Remote IP Address:
USB_U_PtoP_R_Addr=0.0.0.0

#Remote Port:
USB_U_PtoP_R_Port=20003

#Listening Port:
USB_U_PtoP_L_Port=20003

#UDP Timeout(s):
USB_U_PtoP_Timeout=10
```

Appendix H: “system.conf” File Structure (13 of 25)

```
#Multicast IP Address:
USB_UM_P_Multicast_Addr=224.1.1.3

#Multicast Port:
USB_UM_P_Multicast_Port=20003

#Listening Port:
USB_UM_P_Listen_Port=20013

#Time to Live:
USB_UM_P_TTL=1

#Remote IP Address:
USB_UM_M_Remote_Addr=0.0.0.0

#Remote Port:
USB_UM_M_Remote_Port=20013

#Multicast IP Address:
USB_UM_M_Multicast_Addr=224.1.1.3

#Multicast Port:
USB_UM_M_Multicast_Port=20003

#Multicast IP Address:
USB_UMTOM_Multicast_Addr=224.1.1.3

#Multicast Port:
USB_UMTOM_Multicast_Port=20013

#Time to Live:
USB_UMTOM_Multicast_TTL=1

#Listen Multicast IP Address:
USB_UMTOM_Listen_Multicast_Addr=224.1.1.3

#Listen Multicast Port:
USB_UMTOM_Listen_Multicast_Port=20013

#Modbus TCP Status: A - Disable B - Enable
COM1_MODBUS_Mode=A

#Modbus TCP Protection Status: A - Disable B - Enable
COM1_Modbus_Protect_Status=A

#Modbus TCP Protection Key:
COM1_Modbus_Protect_Key=1234

#Modbus TCP Status: A - Disable B - Enable
COM2_MODBUS_Mode=A

#Modbus TCP Protection Status: A - Disable B - Enable
COM2_Modbus_Protect_Status=A

#Modbus TCP Protection Key:
COM2_Modbus_Protect_Key=1234

#Modbus TCP Protection Status: A - Disable B - Enable
USB_Modbus_Protect_Status=A

#Modbus TCP Protection Key:
USB_Modbus_Protect_Key=1234

#DDNS Status: A - Disable B - Enable
DDNS_Status=A
```

Appendix H: “system.conf” File Structure (14 of 25)

```
#Service Name: A - dyndns.org B - changeip.com C - zoneedit.com
#   D - no-ip.com E - noip.com F - freedns.afraid.org
#   G - dnsmax.com H - thatip.com
DDNS_Service_Name=A

#Domain:
DDNS_Domain=user.dyndns.org

#User Name:
DDNS_UserName=user

#Password:
DDNS_Password=12345678

#GPS Status: A - Disable B - Enable
Advanced_GPS_Status=B

#TCP Port:
Advanced_GPS_TCP_Port=2947

#Antenna Power(V):
Advanced_GPS_Antenna_Power=3.05

#NDIS Mode: A - Bridge B - Standalone
USB_NDIS_Bridge_Mode=B

#Local IP Address:
USB_NDIS_IP_Addr=192.168.111.1

#Subnet Mask:
USB_NDIS_Netmask=255.255.255.0

#Host IP:
USB_NDIS_Host_IP=192.168.111.2

#Tunnel Name:
VPN_Tunnel_Name=tunnel

#Tunnel Type:
VPN_Tunnel_Type=0

#Tunnel Status: A - Disable B - Enable
VPN_Tunnel(s)_Status=B

#Tunnel No.:
VPN_Tunnel_S2S_No=0

#Tunnel(s) Used:
VPN_S2S_Tunnel(s)_Used=0

#Tunnel(s) Enabled:
VPN_S2S_Tunnel(s)_Enabled=0

#Tunnel(s) Defined:
VPN_S2S_Tunnel(s)_Defined=0000000000000000000

#Edit Tunnel No.:
VPN_S2S_Tunnel_EDITING=100

#Tunnel No.:
VPN_Tunnel_C2S_No=0

#Tunnel(s) Used:
VPN_C2S_Tunnel(s)_Used=0
```

Appendix H: “system.conf” File Structure (15 of 25)

```
#Tunnel(s) Enabled:
VPN_C2S_Tunnel(s)_Enabled=0

#Tunnel(s) Defined:
VPN_C2S_Tunnel(s)_Defined=0000000000000

#Edit No.:
VPN_C2S_Tunnel_EDITING=100
VPN_VCA_No=0
VPN_VCA_Used=0

#Enabled:
VPN_VCA_Enabled=0

#Defined:
VPN_VCA_Defined=0000000000000000

#Edit No.:
VPN_VCA_EDITING=100

# A - Disable B - Waiting for connection C - Connected
VPN_S2S_Tunnel_Status=B

# A - N/A B - Connect C - Waiting... D - Disconnect
#   E - Waiting...
VPN_S2S_Tunnel_Connection=B

#Gateway IP Address:
VPN_Local_Grp_IP_Address=0.0.0.0

#Subnet IP Address:
VPN_Local_Grp_Subnet_IP=192.168.30.0

#Subnet Mask:
VPN_Local_Grp_Subnet_Mask=255.255.255.0

#Gateway IP Address:
VPN_Remote_Grp_IP_Address=0.0.0.0

#Subnet IP Address:
VPN_Remote_Grp_Subnet_IP=192.168.0.0

#Subnet Mask:
VPN_Remote_Grp_Subnet_Mask=255.255.255.0

#Start IP Address:
VPN_Remote_Client_Start_IP=192.168.0.201

#End IP Address:
VPN_Remote_Client_End_IP=192.168.0.210

#Keying Mode: A - Manual B - IKE with Preshared Key
VPN_Keying_Mode=A

#Phase 1 DH Group: A - modp1024 B - modp1536 C - modp2048
VPN_Phase1_DH_Group=A

#Phase 1 Encryption: A - 3des B - aes C - aes128 D - aes256
VPN_Phase1_Encryption=A

#Phase 1 Authentication: A - md5 B - sha1
VPN_Phase1_Authentication=A

#Phase 1 SA Life Time:
VPN_Phase1_SA_Life_Time=28800
```

Appendix H: “system.conf” File Structure (16 of 25)

```
#Perfect Forward Secrecy(pfs): A - Disable B - Enable
VPN_Perfect_Forward_Secrecy=A

#Phase 2 DH Group: A - modp1024 B - modp1536 C - modp2048
VPN_Phase2_DH_Group=A

#Phase 2 Encryption: A - 3des B - aes C - aes128 D - aes256
VPN_Phase2_Encryption=A

#Phase 2 Authentication: A - md5 B - sha1
VPN_Phase2_Authentication=A

#Phase 2 SA Life Time:
VPN_Phase2_SA_Life_Time=3600

#Preshared Key:
VPN_Preshared_Key=password

#DPD Delay(s):
VPN_DPD_Delay=32

#DPD Timeout(s):
VPN_DPD_Timeout=122

#DPD Action: A - hold B - clear
VPN_DPD_Action=A

# A - Disconnected B - Connected
VPN_TUNNEL_STATUS=A

#Username:
VPN_VCA_User_Name=

#New Password:
VPN_VCA_User_Password=

#Confirm New Password:
VPN_VCA_User_RepeatPasswd=

#Report# A - Disable B - Enable
AGCR_Remote_Reporting_Status=AAAA

#Remote IP:
AGCR_Remote_IP_address0=0.0.0.0

#Remote IP:
AGCR_Remote_IP_address1=0.0.0.0

#Remote IP:
AGCR_Remote_IP_address2=0.0.0.0

#Remote IP:
AGCR_Remote_IP_address3=0.0.0.0

#Remote Port:
AGCR_Remote_PORT0=0

#Remote Port:
AGCR_Remote_PORT1=0

#Remote Port:
AGCR_Remote_PORT2=0

#Remote Port:
AGCR_Remote_PORT3=0
```

Appendix H: “system.conf” File Structure (17 of 25)

```
#Interval(s): A - Off B - On
AGCR_Timer_trigger=AAAA

#Interval(s):
AGCR_Timer0=0

#Interval(s):
AGCR_Timer1=0

#Interval(s):
AGCR_Timer2=0

#Interval(s):
AGCR_Timer3=0

#Distance trigger(meters): A - Off B - On
AGCR_Distance_trigger=AAAA
AGCR_Distance0=0
AGCR_Distance1=0
AGCR_Distance2=0
AGCR_Distance3=0

#Trigger condition: A - None B - AND C - OR
AGCR_Trigger_condition=AAAA

#Message#1: A - None B - ALL C - GGA D - GSA E - GSV
#   F - RMC G - VTG
AGCR_Message_type0=AAAA

#Message#2:
AGCR_Message_type1=AAAA

#Message#3:
AGCR_Message_type2=AAAA

#Message#4:
AGCR_Message_type3=AAAA

#Report# A - Disable B - Modem_Event C - SDP_Event
Event_Remote_Reporting_Status=AAAA

#Remote IP:
Event_Remote_IP_address0=0.0.0.0

#Remote IP:
Event_Remote_IP_address1=0.0.0.0

#Remote IP:
Event_Remote_IP_address2=0.0.0.0

#Remote IP:
Event_Remote_IP_address3=0.0.0.0

#Remote Port:
Event_Remote_PORT0=0

#Remote Port:
Event_Remote_PORT1=0

#Remote Port:
Event_Remote_PORT2=0

#Remote Port:
Event_Remote_PORT3=0
```

Appendix H: “system.conf” File Structure (18 of 25)

```
#Interval(s):
Event_Timer0=0

#Interval(s):
Event_Timer1=0

#Interval(s):
Event_Timer2=0

#Interval(s):
Event_Timer3=0

#Message#1: A - None B - Modem Info C - Carrier Info
#   D - WAN Info
Event_Message_type0=AAAA

#Message#2:
Event_Message_type1=AAAA

#Message#3:
Event_Message_type2=AAAA

#GRE Tunnel Name:
GRE_Tunnel_Name=gre

#GRE Tunnel Local Status: A - Disable B - Enable
GRE_Tunnel_Local_Status=B

#GRE Tunnel Remote Status: A - None B - Dead C - Alive
GRE_Tunnel_Remote_Status=A

#Multicast: A - Disable B - Enable
GRE_Tunnel_Multicase=B

#ARP: A - Disable B - Enable
GRE_Tunnel_ARP=B
GRE_Tunnel_TTL=255

#Keep Alive Check: A - Disable B - Enable
GRE_Tunnel_DPD=A

#Peer IP Address:
GRE_Tunnel_DPD_IP=0.0.0.0

#Delay(s):
GRE_Tunnel_DPD_Delay=30

#Timeout(s):
GRE_Tunnel_DPD_Timeout=120

#Action: A - Hold_Tunnel B - Disable_Tunnel C - Delete_Tunnel
GRE_Tunnel_DPD_Action=A

#Local GRE Tunnel IP ddress:
GRE_Tunnel_Local_IP=0.0.0.0

#Net Mask:
GRE_Tunnel_Local_Netmask=0.0.0.0

#Local WAN IP Address:
GRE_Tunnel_Local_WAN_IP=0.0.0.0

#Subnet IP Address:
GRE_Tunnel_Remote_SubIP=0.0.0.0
```

Appendix H: “system.conf” File Structure (19 of 25)

```
#Subnet Mask:
GRE_Tunnel_Remote_Submask=0.0.0.0

#WAN IP Address:
GRE_Tunnel_Remote_WAN_IP=0.0.0.0

#Ipsec: A - Disable B - Enable
GRE_Tunnel_Ipsec=A

#Ipsec Connection: A - N/A B - Connect C - Waiting...
#   D - Disconnect
GRE_Ipsec_Connection=A

#Tunnel(s) Defined:
GRE_Tunnel_Defined=0000000000

#Tunnel Edit No.:
GRE_Tunnel_Edit_No=100

#Tunnel No.:
GRE_Tunnel_No=0

#Phase 1 DH Group: A - modp1024 B - modp1536 C - modp2048
GRE_Phase1_DH_Group=A

#Phase 1 Encryption: A - 3des B - aes C - aes128 D - aes256
GRE_Phase1_Encryption=A

#Phase 1 Authentication: A - md5 B - sha1
GRE_Phase1_Authentication=A

#Phase 1 SA Life Time:
GRE_Phase1_SA_Life_Time=28800

#Perfect Forward Secrecy(pfs): A - Disable B - Enable
GRE_Perfect_Forward_Secrecy=A

#Phase 2 DH Group: A - modp1024 B - modp1536 C - modp2048
GRE_Phase2_DH_Group=A

#Phase 2 Encryption: A - 3des B - aes C - aes128 D - aes256
GRE_Phase2_Encryption=A

#Phase 2 Authentication: A - md5 B - sha1
GRE_Phase2_Authentication=A

#Phase 2 SA Life Time:
GRE_Phase2_SA_Life_Time=3600

#Preshared Key:
GRE_Preshared_Key=password

#DPD Delay(s):
GRE_DPD_Delay=32

#DPD Timeout(s):
GRE_DPD_Timeout=122

#DPD Action: A - hold B - clear
GRE_DPD_Action=A

#GRE Ipsec Status: A - Disconnected B - Connected
GRE_IPSEC_STATUS=A

#Dead Peer Detection: A - Disable B - Enable
GRE_DPD_Status=A
```

Appendix H: “system.conf” File Structure (20 of 25)

```
#Phone Number:
COM1_SMS_PHONE1=

#Phone Number:
COM1_SMS_PHONE2=

#Phone Number:
COM1_SMS_PHONE3=

#Phone Number:
COM1_SMS_PHONE4=

#Phone Number:
COM1_SMS_PHONE5=

#Message Max Size:
COM1_SMS_MMS=160

#Reply Timeout(s):
COM1_SMS_TIMEOUT=10

#Access Control: A - Anonymous B - Control Phone List
COM1_SMS_ANON=A

#Read SMS Control: A - Keep in SIM Card B - Delete
COM1_SMS_GETSMS_MODE=A

#SMS Sender:
From:

#SMS Subject:
Subject:

#SMS Data/time:
Date/time:

#SMS Location:
COM1_SMS_LOCATION=

#SMS SM Total:
SMS_SM_TOTAL=

#SMS SM Used:
SMS_SM_USED=

#SMS ME Total:
SMS_ME_TOTAL=

#SMS ME Used:
SMS_ME_USED=

#Alert A - Disable B - Enable
SAL_Enable=A
RSSI_CHECK=A

#Low Threshold(dBm):
RSSI_LOW=-99

#Core Temperature
CORE_TEMPERATURE_CHECK=A

#High Threshold(°C):
CTEMP_HIGH=80

#Low Threshold(°C):
CTEMP_LOW=20
```

Appendix H: “system.conf” File Structure (21 of 25)

```
#Supply Voltage
VOLTAGE_CHECK=A

#High Threshold(V):
VOLTAGE_HIGH=36

#Low Threshold(V):
VOLTAGE_LOW=7

#Home/Roaming Status
ROAMING_CHECK=A
ROAMING_STATUS=Roaming

#Ethernet Link Status
ETH_CHECK=A
ETH_LINK_STATUS=0

#Phone Number:
SAL_Phone1=

#Phone Number:
SAL_Phone2=

#Phone Number:
SAL_Phone3=

#Phone Number:
SAL_Phone4=

#Phone Number:
SAL_Phone5=

#Phone Number:
SAL_Phone6=

#Interval(s):
SAL_Interval=5

#Report# A - Disable B - Enable
Netflow_Reporting_Status=AAAA

#Interface: A - LAN B - WAN C - ALL
Netflow_Remote_IF0=A

#Interface: A - LAN B - WAN C - ALL
Netflow_Remote_IF1=A

#Interface: A - LAN B - WAN C - ALL
Netflow_Remote_IF2=A

#Interface: A - LAN B - WAN C - ALL
Netflow_Remote_IF3=A

#Remote IP:
Netflow_Remote_IP0=0.0.0.0

#Remote IP:
Netflow_Remote_IP1=0.0.0.0

#Remote IP:
Netflow_Remote_IP2=0.0.0.0

#Remote IP:
Netflow_Remote_IP3=0.0.0.0
```

```
#Remote Port:
Netflow_Remote_PORT0=0

#Remote Port:
Netflow_Remote_PORT1=0

#Remote Port:
Netflow_Remote_PORT2=0

#Remote Port:
Netflow_Remote_PORT3=0

# User Expand Keywords
QueryListenPort=20077
User_Parameter_0=
User_Parameter_1=
User_Parameter_2=
User_Parameter_3=
User_Parameter_4=
User_Parameter_5=
User_Parameter_6=
User_Parameter_7=
User_Parameter_8=
User_Parameter_9=

BASIC_SETTINGS_END

QOS_BEGIN:
#Enbale or Disable
QOS=Disable

#19k,115k,172k,230k,345k,1100k
LINKRATE=345

#Custom ports
QOS_HIGH=
QOS_MEDIUM=

#COM1 priority
COM1_HIGH=
COM1_MEDIUM=

#COM2 priority
COM2_HIGH=
COM2_MEDIUM=


QOS_END

IPSEC_Site2Site_Tunnel1_BEGIN:

IPSEC_Site2Site_Tunnel1_END

IPSEC_Site2Site_Tunnel2_BEGIN:

IPSEC_Site2Site_Tunnel2_END

IPSEC_Site2Site_Tunnel3_BEGIN:

IPSEC_Site2Site_Tunnel3_END

IPSEC_Site2Site_Tunnel4_BEGIN:

IPSEC_Site2Site_Tunnel4_END

IPSEC_Site2Site_Tunnel5_BEGIN:
```

Appendix H: “system.conf” File Structure (23 of 25)

```
IPSEC_Site2Site_Tunnel5_END
IPSEC_Site2Site_Tunnel6_BEGIN:
IPSEC_Site2Site_Tunnel6_END
IPSEC_Site2Site_Tunnel7_BEGIN:
IPSEC_Site2Site_Tunnel7_END
IPSEC_Site2Site_Tunnel8_BEGIN:
IPSEC_Site2Site_Tunnel8_END
IPSEC_Site2Site_Tunnel9_BEGIN:
IPSEC_Site2Site_Tunnel9_END
IPSEC_Site2Site_Tunnel10_BEGIN:
IPSEC_Site2Site_Tunnel10_END
IPSEC_Site2Site_Tunnel11_BEGIN:
IPSEC_Site2Site_Tunnel11_END
IPSEC_Site2Site_Tunnel12_BEGIN:
IPSEC_Site2Site_Tunnel12_END
IPSEC_Site2Site_Tunnel13_BEGIN:
IPSEC_Site2Site_Tunnel13_END
IPSEC_Site2Site_Tunnel14_BEGIN:
IPSEC_Site2Site_Tunnel14_END
IPSEC_Site2Site_Tunnel15_BEGIN:
IPSEC_Site2Site_Tunnel15_END
IPSEC_Site2Site_Tunnel16_BEGIN:
IPSEC_Site2Site_Tunnel16_END
IPSEC_L2TPD_Tunnel1_BEGIN:
IPSEC_L2TPD_Tunnel1_END
IPSEC_Client1_BEGIN:
IPSEC_Client1_END
IPSEC_Client2_BEGIN:
IPSEC_Client2_END
IPSEC_Client3_BEGIN:
IPSEC_Client3_END
IPSEC_Client4_BEGIN:
IPSEC_Client4_END
```

Appendix H: “system.conf” File Structure (24 of 25)

```
IPSEC_Client5_BEGIN:

IPSEC_Client5_END

IPSEC_Client6_BEGIN:

IPSEC_Client6_END

IPSEC_Client7_BEGIN:

IPSEC_Client7_END

IPSEC_Client8_BEGIN:

IPSEC_Client8_END

IPSEC_Client9_BEGIN:

IPSEC_Client9_END

IPSEC_Client10_BEGIN:

IPSEC_Client10_END

Firewall_Config_BEGIN:
firewall.Dplc_0=defaults
firewall.Dplc_0.syn_flood=1
firewall.Dplc_0.input=ACCEPT
firewall.Dplc_0.output=ACCEPT
firewall.Dplc_0.forward=REJECT
firewall.Zplc_0=zone
firewall.Zplc_0.name=lan
firewall.Zplc_0.input=ACCEPT
firewall.Zplc_0.output=ACCEPT
firewall.Zplc_0.forward=REJECT
firewall.Zplc_1=zone
firewall.Zplc_1.name=wan
firewall.Zplc_1.input=ACCEPT
firewall.Zplc_1.output=ACCEPT
firewall.Zplc_1.forward=REJECT
firewall.Zplc_1.masq=1
firewall.Fplc_0=forwarding
firewall.Fplc_0.src=lan
firewall.Fplc_0.dest=wan
firewall.Rule_4=rule
firewall.Rule_4.proto=all
firewall.Rule_4.src=lan
firewall.Rule_4.dest=wan
firewall.Rule_4.src_ip=0.0.0.0/0
firewall.Rule_4.dest_ip=0.0.0.0/0
firewall.Rule_4.target=ACCEPT
firewall.Rule_5=rule
firewall.Rule_5.proto=all
firewall.Rule_5.src=wan
firewall.Rule_5.src_ip=0.0.0.0/0
firewall.Rule_5.dest_ip=0.0.0.0/0
firewall.Rule_5.target=ACCEPT
firewall.Rule_0=rule
firewall.Rule_0.proto=TCP
firewall.Rule_0.src=wan
firewall.Rule_0.dest=wan
firewall.Rule_0.src_ip=0.0.0.0/0
firewall.Rule_0.dest_ip=0.0.0.0/0
firewall.Rule_0.dest_port=80
firewall.Rule_0.target=ACCEPT
firewall.Rule_1=rule
```

Appendix H: “system.conf” File Structure (25 of 25)

```
firewall.Rule_1.proto=TCP
firewall.Rule_1.src=wan
firewall.Rule_1.dest=wan
firewall.Rule_1.src_ip=0.0.0.0/0
firewall.Rule_1.dest_ip=0.0.0.0/0
firewall.Rule_1.dest_port=443
firewall.Rule_1.target=ACCEPT
firewall.Forward1=redirect
firewall.Forward1.src=wan
firewall.Forward1.proto=TCP
firewall.Forward1.src_dport=2000
firewall.Forward1.dest_ip=192.168.2.1
firewall.Forward1.dest_port=3000
firewall.HMI=redirect
firewall.HMI.src=wan
firewall.HMI.proto=TCP
firewall.HMI.src_dport=8080
firewall.HMI.dest_ip=192.168.0.189
firewall.HMI.dest_port=80
firewall.Rule_2=rule
firewall.Rule_2.proto=TCP
firewall.Rule_2.src=lan
firewall.Rule_2.dest=lan
firewall.Rule_2.src_ip=0.0.0.0/0
firewall.Rule_2.dest_ip=0.0.0.0/0
firewall.Rule_2.dest_port=80
firewall.Rule_2.target=ACCEPT
firewall.Rule_3=rule
firewall.Rule_3.proto=TCP
firewall.Rule_3.src=lan
firewall.Rule_3.dest=lan
firewall.Rule_3.src_ip=0.0.0.0/0
firewall.Rule_3.dest_ip=0.0.0.0/0
firewall.Rule_3.dest_port=443
firewall.Rule_3.target=ACCEPT

Firewall_Config_END
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 1 of 15)

The following pages show an example MIB file for the IPn3G. This is not the complete MIB file, only the first 15 pages of the MIB are shown for reference. Contact Microhard Systems for the complete and most current release, as the MIB will change as features are added.

```
MICROHARD-IP3G

-- Title:     MICROHARD MIB
-- Date:      Feb 15, 2012
-- Version              1.28
-- Disription: Not all parameters are supported in a paticular device,Support of parameters varies
-- from version to version

            DEFINITIONS ::= BEGIN

            IMPORTS
                        enterprises, OBJECT-TYPE, NetworkAddress, IpAddress,
                        Counter, Gauge, TimeTicks
                        FROM RFC1065-SMI;
--          DisplayString
--                      FROM RFC1158-MIB;

            MicrohardOBJECT IDENTIFIER ::=      { enterprises 21703 }

--IP3G
            IP3G                                OBJECT IDENTIFIER ::=       { Microhard 5000 }
            SystemConfig                        OBJECT IDENTIFIER ::=       { IP3G 1 }
            NetworkConfig                       OBJECT IDENTIFIER ::=       { IP3G 2 }
            CarrierConfig                       OBJECT IDENTIFIER ::=       { IP3G 3 }
            COM1Config                          OBJECT IDENTIFIER ::=       { IP3G 4 }
            COM2Config                          OBJECT IDENTIFIER ::=       { IP3G 5 }
            SecurityConfig                      OBJECT IDENTIFIER ::=       { IP3G 6 }
            SystemInformation                   OBJECT IDENTIFIER ::=       { IP3G 7 }
            SystemTools                         OBJECT IDENTIFIER ::=       { IP3G 8 }
            USBConfig                           OBJECT IDENTIFIER ::=       { IP3G 9 }

-- SystemConfig parameter group

            System_Unit_Description     OBJECT-TYPE
                        SYNTAX  DisplayString (SIZE (0..32))
                        ACCESS  read-write
                        STATUS  mandatory
                        DESCRIPTION "Radio Discription."
                        ::= { SystemConfig 1 }

            System_Date         OBJECT-TYPE
                        SYNTAX  DisplayString (SIZE (0..32))
                        ACCESS  read-write
                        STATUS  mandatory
                        DESCRIPTION "System Date."
                        ::= { SystemConfig 2 }

            System_Time         OBJECT-TYPE
                        SYNTAX  DisplayString (SIZE (0..32))
                        ACCESS  read-write
                        STATUS  mandatory
                        DESCRIPTION "System Time."
                        ::= { SystemConfig 3 }

            System_Timezone     OBJECT-TYPE
                        SYNTAX  DisplayString (SIZE (0..32))
                        ACCESS  read-write
                        STATUS  mandatory
                        DESCRIPTION "System Timezone."
                        ::= { SystemConfig 4 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 2 of 15)

```
System_NTP_Server_Status   OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "NTP Server Status:  0 - Disable 1 - Enable."
                ::= { SystemConfig 5 }

        System_NTP_Server_Name    OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "NTP Server Address."
                ::= { SystemConfig 6 }

        System_ConsoleTimeout        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "System Console Timeout(s). 0 means never timeout "
                ::= { SystemConfig 7}

        System_Wireless_Traffic_Timeout          OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "System Wireless Traffic Timeout(s). 0 means never timeout,[300..65535]"
                ::= { SystemConfig 8 }

        System_Default_Button           OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "System default Button"
                ::= { SystemConfig 9 }

        System_Syslog_Server_IP      OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "System Syslog Server IP Address"
                ::= { SystemConfig 11 }

        System_Syslog_Server_Port   OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "System Syslog Server IP Port"
                ::= { SystemConfig 12 }

        System_Config_ACTION        OBJECT-TYPE
                SYNTAX  INTEGER {192.168.0
                SubmitOrReset(0),
                Submit(1),
                Reset(2),
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "0-Default no selection.1-Submit,this will update setting immidiately.
                2-Reset,this will cacel all related settings in the sub tree"
                ::= { SystemConfig 10 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 3 of 15)

```
-- Network parameter group

        IPConfig  OBJECT IDENTIFIER ::=       { NetworkConfig 2 }
                  -- IPConfig parameter group


        NetWork_IP_Address            OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "IP Address."
                  ::= { IPConfig 1 }

        NetWork_IP_Subnet_Mask     OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "IP SubNet Mask."
                  ::= { IPConfig 2 }

        NetWork_IP_Gateway            OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                   DESCRIPTION "IP Gate Way."
                  ::= { IPConfig 3 }

        NetWork_DHCP_Server_Status            OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "NetWork DHCP Server Status."
                  ::= { IPConfig 4 }

        NetWork_DHCP_Start_Address            OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "IP Preferred DNS Server."
                  ::= { IPConfig 5 }

        NetWork_DHCP_End_Address              OBJECT-TYPE
                  SYNTAX  DisplayString (SIZE (0..32))
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "IP Alternate DNS Server."
                  ::= { IPConfig 6 }


        NetWork_IP_Config_ACTION OBJECT-TYPE
                  SYNTAX  INTEGER {
                  SubmitOrReset(0),
                  Submit(1),
                  Reset(2),
                  }
                  ACCESS  read-write
                  STATUS  mandatory
                  DESCRIPTION "0-Default no selection.1-Submit,this will update setting immidiately.
                  2-Reset,this will cacel all related settings in the sub tree"
                  ::= { IPConfig 7 }


        SNMPConfig           OBJECT IDENTIFIER ::=       { NetworkConfig 5 }
                  -- SNMPConfig parameter group
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 4 of 15)

```
NetWork_SNMP_Mode          OBJECT-TYPE
        SYNTAX  INTEGER {
        Disable(0),
        Enable(1)
        }
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP Mode: 0 - Disable  1- Enable v1 v2c v3."
        ::= { SNMPConfig 1 }

NetWork_SNMP_Read_Community_Name          OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP Read CommunityName."
        ::= { SNMPConfig 2 }

NetWork_SNMP_Write_Community_Name          OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP Write Community Name."
        ::= { SNMPConfig 3 }

NetWork_SNMP_V3_User_Name          OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP Version 3 User Name."
        ::= { SNMPConfig 4 }

NetWork_SNMP_V3_User_ReadWrite_Limit          OBJECT-TYPE
        SYNTAX  INTEGER {
        ReadOnly(0),
        ReadWrite(1)
        }
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP V3 User Read Write Limit: 0 - Read Only  1 - Read Write."
        ::= { SNMPConfig 5 }

NetWork_SNMP_V3_User_Auth_Level  OBJECT-TYPE
        SYNTAX  INTEGER {
        NoAuthNopriv(0),
        AuthNoPriv(1),
        AuthPriv(2)
        }
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP V3 User Authentication Level: 0 - NoAuthNopriv  1 - AuthNoPriv
        2 - AuthPriv."
        ::= { SNMPConfig 6 }

NetWork_SNMP_V3_Auth_Password     OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "SNMP V3 Authentication Password."
        ::= { SNMPConfig 7 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 5 of 15)

```
NetWork_SNMP_V3_Privacy_Password OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "SNMP V3 Privacy Passord."
                ::= { SNMPConfig 8 }

        NetWork_SNMP_Trap_Version               OBJECT-TYPE
                SYNTAX  INTEGER {V1Traps(0),V2Traps(1),V3Traps(2),V1&V2Traps(3),V1&V2&V3Traps(4)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "SNMP Trap Version: 0 - V1 Traps  1 - V2 Traps  2 - V3 Traps
                3 - V1&V2 Traps  4 - V1&V2&V3 Traps."
                ::= { SNMPConfig 9 }

        NetWork_SNMP_Auth_Traps_Status          OBJECT-TYPE
                SYNTAX  INTEGER {Disable(0),Enable(1)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "SNMP Authentication Traps Status: 0 - Disable  1 - Enable."
                ::= { SNMPConfig 10 }

        NetWork_SNMP_Trap_Community_Name                OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "SNMP Trap Community Name."
                ::= { SNMPConfig 11 }

        NetWork_SNMP_Trap_Manage_Host           OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "SNMP Manage Host."
                ::= { SNMPConfig 12 }

        NetWork_SNMP_Config_ACTION              OBJECT-TYPE
                SYNTAX  INTEGER {
                SubmitOrReset(0),
                Submit(1),
                Reset(2),
                }
                ACCESS  read-write
            STATUS          mandatory
                DESCRIPTION "0-Default no selection.1-Submit,this will update setting immidiately.
                2-Reset,this will cacel all related settings in the sub tree"
                ::= { SNMPConfig 13 }



-- Carrier  parameter group
        Carrier_NAT_Status              OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "NAT Mode: 0 - Disable  1- Enable."
                ::= { CarrierConfig 1 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 6 of 15)

```
Carrier_PPP_Status      OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Status: 0 - Disable  1- Enable."
                ::= { CarrierConfig 2 }

        Carrier_IP_Passthrough  OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Ethernet(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier IP Passthrough"
                ::= { CarrierConfig 3 }

        Carrier_Dial_On_Command_Status  OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Dial On Command Status: 0 - Disable  1- Enable."
                ::= { CarrierConfig 4 }

        Carrier_Idle_Timeout    OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Idle Timeout"
                ::= { CarrierConfig 5 }

        Carrier_Connect_Timeout OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Connect Timeout"
                ::= { CarrierConfig 6 }

        Carrier_DIAL_MAX_RETRY  OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier DIAL MAX RETRY"
                ::= { CarrierConfig 7 }

        Carrier_AUTH_TYPE       OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier AUTH TYPE: 0 - NoAuth  1- pap 2-chap 3 pap-chap"
                ::= { CarrierConfig 8 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 7 of 15)

```
Carrier_USER_NAME             OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier USER NAME"
                    ::= { CarrierConfig 9 }

          Carrier_Password    OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Password"
                    ::= { CarrierConfig 10 }


          Carrier_SIM_PIN     OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier SIM Card Pin"
                    ::= { CarrierConfig 51 }

          Carrier_Dial_Num    OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Dial Num"
                    ::= { CarrierConfig 12 }

          Carrier_Conn_Str    OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Conn Str"
                    ::= { CarrierConfig 13 }

          Carrier_APN         OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier APN"
                    ::= { CarrierConfig 14 }

          Carrier_Init_Str1   OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Init Str1"
                    ::= { CarrierConfig 15 }

          Carrier_Init_Str2   OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Init Str2"
                    ::= { CarrierConfig 16 }

          Carrier_Init_Str3   OBJECT-TYPE
                    SYNTAX  DisplayString (SIZE (0..32))
                    ACCESS  read-write
                    STATUS  mandatory
                    DESCRIPTION "Carrier Init Str3"
                    ::= { CarrierConfig 17 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 8 of 15)

```
Carrier_Init_Str4     OBJECT-TYPE
                      SYNTAX  DisplayString (SIZE (0..32))
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Init Str4"
                      ::= { CarrierConfig 18 }

            Carrier_Static_IP     OBJECT-TYPE
                      SYNTAX  DisplayString (SIZE (0..32))
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Static IP"
                      ::= { CarrierConfig 19 }

            Carrier_DDNS_Config           OBJECT IDENTIFIER ::=        { CarrierConfig 20 }
                      -- Carrier_DDNS_Config parameter group

            Carrier_DDNS_Status           OBJECT-TYPE
                      SYNTAX  INTEGER {
                      Disable(0),
                      Enable(1)
                      }
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier DDNS Status: 0 - Disable  1- Enable."
                      ::= { Carrier_DDNS_Config 1 }

            Carrier_DDNS_Service_Name             OBJECT-TYPE
                      SYNTAX  INTEGER {
                      dyndns(0),
                      changeip(1),
                      zoneedit.com(2),
                      no-ip(3),
                      noip(4),
                      freedns.afraid.org(5),
                      dnsmax.com(6),
                      thatip(7),
                      }
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Service Name."
                      ::= { Carrier_DDNS_Config 2 }

            Carrier_DDNS_Domain           OBJECT-TYPE
                      SYNTAX  DisplayString (SIZE (0..32))
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Service Name"
                      ::= { Carrier_DDNS_Config 3 }

            Carrier_DDNS_UserName       OBJECT-TYPE
                      SYNTAX  DisplayString (SIZE (0..32))
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Service Name"
                      ::= { Carrier_DDNS_Config 4 }

            Carrier_DDNS_Password       OBJECT-TYPE
                      SYNTAX  DisplayString (SIZE (0..32))
                      ACCESS  read-write
                      STATUS  mandatory
                      DESCRIPTION "Carrier Service Name"
                      ::= { Carrier_DDNS_Config 5 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 9 of 15)

```
Carrier_Keep_Alive_Config     OBJECT IDENTIFIER ::=        { CarrierConfig 22 }
                -- Carrier_Keep_Alive_Config parameter group

        Carrier_Keep_Alive_Status     OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Keep Alive Status: 0 - Disable  1- Enable."
                ::= { Carrier_Keep_Alive_Config 1 }

        Carrier_Keep_Alive_HostName             OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Keep Alive HostName"
                ::= { Carrier_Keep_Alive_Config 2 }


        Carrier_Keep_Alive_Interval    OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Keep Alive Interval"
                ::= { Carrier_Keep_Alive_Config 3 }


        Carrier_Keep_Alive_Count      OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Keep Alive Count"
                ::= { Carrier_Keep_Alive_Config 4 }

        Carrier_Wakeup_Oncall_Config            OBJECT IDENTIFIER ::=        { CarrierConfig 25 }
                -- Carrier_Wakeup_Oncall_Config parameter group

        Carrier_Wakeup_Oncall_Status            OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall Status: 0 - Disable  1- Enable."
                ::= { Carrier_Wakeup_Oncall_Config 1 }

        Carrier_Wakeup_Oncall_TIME_DELAY  OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Keep Alive HostName"
                ::= { Carrier_Wakeup_Oncall_Config 2 }

        Carrier_Wakeup_Oncall_FROM_LAN     OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1)
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall FROM LAN: 0 - Disable  1- Enable."
                ::= { Carrier_Wakeup_Oncall_Config 3 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 10 of 15)

```
Carrier_Wakeup_Oncall_INITSTR1        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR1"
                ::= { Carrier_Wakeup_Oncall_Config 4 }


    Carrier_Wakeup_Oncall_INITSTR2        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR2"
                ::= { Carrier_Wakeup_Oncall_Config 5 }

    Carrier_Wakeup_Oncall_INITSTR3        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR3"
                ::= { Carrier_Wakeup_Oncall_Config 6 }

    Carrier_Wakeup_Oncall_INITSTR4        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR4"
                ::= { Carrier_Wakeup_Oncall_Config 7 }


    Carrier_Wakeup_Oncall_CALLER_ID     OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR4"
                ::= { Carrier_Wakeup_Oncall_Config 8 }

    Carrier_Wakeup_Oncall_CALLER_ACK OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier Wakeup Oncall INITSTR4"
                ::= { Carrier_Wakeup_Oncall_Config 9 }

    Carrier_PowerOn__Config      OBJECT IDENTIFIER ::=        { CarrierConfig 28 }
                -- Carrier_PowerOn__Config parameter group

    Carrier_PowerOn_InitStr        OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "Carrier PowerOn InitStr"
                ::= { Carrier_PowerOn__Config 1 }

    Carrier_Config_ACTION          OBJECT-TYPE
                SYNTAX  INTEGER {
                SubmitOrReset(0),
                Submit(1),
                Reset(2),
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "0-Default no selection.1-Submit,this will update setting immidiately.
                2-Reset,this will cacel all related settings in the sub tree"
                ::= { CarrierConfig 30 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 11 of 15)

```
-- COM1 parameter group

        COM1_Port_Status  OBJECT-TYPE
                SYNTAX  INTEGER {          Disable(0),            Enable(1)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Port Status: 0 - Disable  1 - Enable"
                ::= { COM1Config 1 }

        COM1_Chanel_Mode            OBJECT-TYPE
                SYNTAX  INTEGER {RS232(0),RS485(1),RS422(2)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Channel Mode: A - RS232  B - RS485  C - RS422"
                ::= { COM1Config 2 }

        COM1_Data_Baud_Rate         OBJECT-TYPE
                SYNTAX  INTEGER {B300(0),B600(1),B1200(2),B2400(3), B3600(4),B4800(5),
                B7200(6),B9600(7),B14400(8),B19200(9),B28800(10),B38400(11),B57600(12),
                B115200(13),B230400(14),B460800(15),B921600(16)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Data 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 15-460800,16-961600"
                ::= { COM1Config 3 }

        COM1_Data_Format            OBJECT-TYPE
                SYNTAX  INTEGER {_8N1(0),_8N2(1),_8E1(2),_8O1(3), _7N1(4),
                _7N2(5),_7E1(6),_7O1(7),_7E2(8), _7O2(9)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Data Format: 0 - 8N1  1 - 8N2  2 - 8E1  3 - 8O1
                4 - 7N1  5 - 7N2  6 - 7E1  7 - 7O1  8 - 7E2  9 - 7O2 "
                ::= { COM1Config 4 }

        COM1_Flow_Control           OBJECT-TYPE
                SYNTAX  INTEGER { None(0),Hardware(1),CTSFraming(2)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Flow Control: 0 - None  1 - Hardware 2- CTS Framing"
                ::= { COM1Config 5 }

        COM1_PreData_Delay          OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Pre-frame Delay."
                ::= { COM1Config 6 }

        COM1_PostData_Delay         OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Post-frame Delay."
                ::= { COM1Config 7 }

        COM1_Data_Mode  OBJECT-TYPE
                SYNTAX  INTEGER {Modbus(0),Transparent(1)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Data Mode: 0 - Modbus  1 - Transparent."
                ::= { COM1Config 8 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 12 of 15)

```
COM1_Character_Timeout     OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Character Timeout."
                ::= { COM1Config 9 }

        COM1_Maximum_Packet_Size              OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Maxmum Packet Size."
                ::= { COM1Config 10 }

        COM1_Priority        OBJECT-TYPE
                SYNTAX  INTEGER {
                Normal(0),
                Medium(1),
                High(2),
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 Data Format: 0 - Normal  1 - Medium  2 - High "
                ::= { COM1Config 11 }

        COM1_No_Connection_Data_Intake      OBJECT-TYPE
                SYNTAX  INTEGER {
                Disable(0),
                Enable(1),
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 No Connection Data Intake: 0 - Disable  1 - Enable "
                ::= { COM1Config 12 }

        COM1_IP_Protocol OBJECT-TYPE
                SYNTAX  INTEGER {TCPClient(0),        TCPServer(1),        TCPClient/Server(2),UDPPointtoPoint
(3),
                UDPPointtoMultiPoint_as_point(4),UDPPointtoMultiPoint_as_Multipoint(5),
                UDPMultiPoint_to_Multipoint(6),smtp(7)}
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 IP Protocol: 0 - TCP Client  1 - TCP Server  2 - TCP Client/Server
                3 - UDP Point to Point  4 - UDP Point to MultiPoint(as point)
                5 - UDP Point to MultiPoint(as Multipoint).6-UDP MultiPoint to Multipoint
                7 - smtp"
                ::= { COM1Config 13 }

        COM1AsTCPClientConfig       OBJECT IDENTIFIER ::=        { COM1Config 14}

                -- COM1TCPClientConfig Command group

        COM1_TCP_Client_Server_Addr            OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Client Remote Server Ip Addresss."
                ::= { COM1AsTCPClientConfig 1 }
```

Appendix I: SNMP MIB IPn3G "Sample" (Page 13 of 15)

```
COM1_TCP_Client_Server_Port             OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Client Remote Server Listen Port."
                ::= { COM1AsTCPClientConfig 2 }

        COM1_TCP_Client_Timeout OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Client Connection Timeout."
                ::= { COM1AsTCPClientConfig 3 }

        COM1AsTCPServerConfig   OBJECT IDENTIFIER ::=       { COM1Config 15 }

                -- COM1TCPServerConfig Command group

        COM1_TCP_Server_Mode    OBJECT-TYPE
                SYNTAX  INTEGER {
                Monitor(0),
                Multi-polling(1),
                }
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Server, polling mode, Monitor or Multi-polling "
                ::= { COM1AsTCPServerConfig 1 }

        COM1_TCP_Server_Polling_Timeout OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Server,Multi-polling Timeout(ms)."
                ::= { COM1AsTCPServerConfig 2 }

        COM1_TCP_Server_Listen_Port             OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Local as Server Listen Port."
                ::= { COM1AsTCPServerConfig 3 }

        COM1_TCP_Server_Timeout OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Server  Remote Client Connection Timeout."
                ::= { COM1AsTCPServerConfig 4 }

        COM1AsTCPClientOrServerConfig           OBJECT IDENTIFIER ::=       { COM1Config 16}
                -- COM1TCPClientOrServerConfig Command group

        COM1_TCP_COrS_Remote_Server_Addr                OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Client Remote Server Ip Addresss."
                ::= { COM1AsTCPClientOrServerConfig 1 }

        COM1_TCP_COrS_Remote_Server_Port                OBJECT-TYPE
                SYNTAX  DisplayString (SIZE (0..32))
                ACCESS  read-write
                STATUS  mandatory
                DESCRIPTION "COM1 as TCP Client Remote Server Listen Port."
                ::= { COM1AsTCPClientOrServerConfig 2 }
```

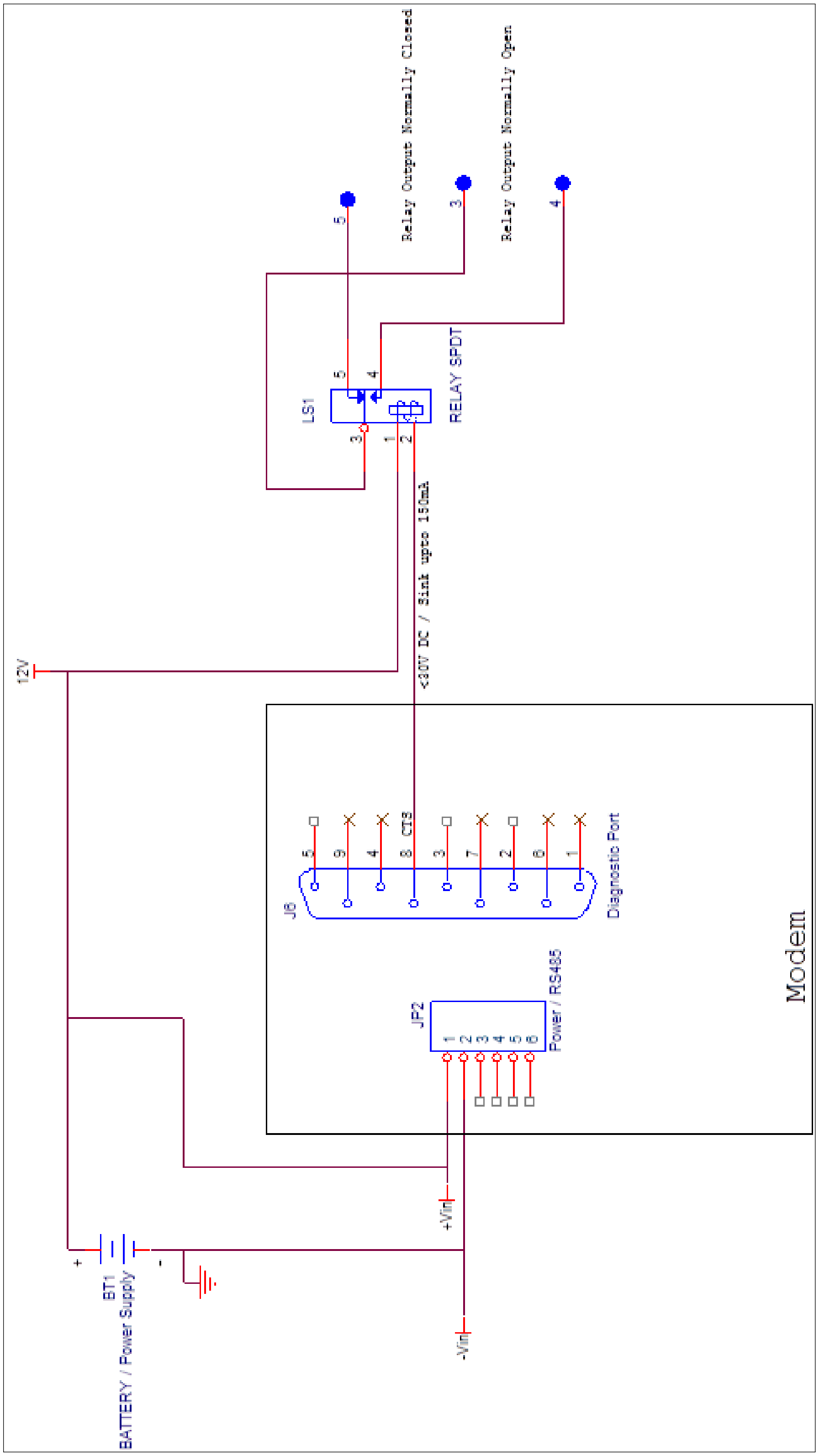
Appendix I: SNMP MIB IPn3G “Sample” (Page 14 of 15)

```
COM1_TCP_COrS_Timeout   OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as TCP Client Connection Timeout."
        ::= { COM1AsTCPClientOrServerConfig 3 }

COM1_TCP_COrS_Server_Mode         OBJECT-TYPE
        SYNTAX  INTEGER {
        Monitor(0),
        Multi-polling(1),
        }
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as TCP Server, polling mode, Monitor or Multi-polling "
        ::= { COM1AsTCPClientOrServerConfig 4 }

COM1_TCP_COrS_Server_Polling_Timeout        OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as TCP Server,Multi-polling Timeout(ms)."
        ::= { COM1AsTCPClientOrServerConfig 5 }

COM1_TCP_COrS_Local_Listen_Port   OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as TCP Local as Server Listen Port."
        ::= { COM1AsTCPClientOrServerConfig 6 }

COM1_TCP_COrS_Local_Server_Timeout          OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as TCP Server  Remote Client Connection Timeout."
        ::= { COM1AsTCPClientOrServerConfig 7 }

 COM1AsUDPPointToPointConfig                OBJECT IDENTIFIER ::=       { COM1Config 17 }

        -- COM1UDPPointToPointConfig Command group

COM1_UDP_PtoP_Remote_Addr         OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as UDP Point to Point Remote Ip Addresss."
        ::= { COM1AsUDPPointToPointConfig 1 }

COM1_UDP_PtoP_Remote_Port         OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as UDP Point to Point Remote Server Listen Port."
        ::= { COM1AsUDPPointToPointConfig 2 }

COM1_UDP_PtoP_Listen_Port         OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as UDP Point to Point Connection Local Listen Port."
        ::= { COM1AsUDPPointToPointConfig 3 }
```

Appendix I: SNMP MIB IPn3G “Sample” (Page 15 of 15)

```
COM1_UDP_PtoP_Timeout   OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "COM1 as UDP Point to Point Connection Timeout."
        ::= { COM1AsUDPPointToPointConfig 4 }


    COM1AsUDPPointToMultiPointasPointConfig     OBJECT IDENTIFIER ::=     { COM1Config 18 }

        -- COM1UDPPointToMultiPointasPointConfig Command group

    COM1_UM_P_Multicast_Addr OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Multicast Addresss."
        ::= { COM1AsUDPPointToMultiPointasPointConfig 1 }

    COM1_UM_P_Multicast_Port  OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Multicast Port."
        ::= { COM1AsUDPPointToMultiPointasPointConfig 2 }

    COM1_UM_P_Listen_Port     OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Local Listen Port."
        ::= { COM1AsUDPPointToMultiPointasPointConfig 3 }

    COM1_UM_P_TTL  OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Multicast TTL Value."
        ::= { COM1AsUDPPointToMultiPointasPointConfig 4 }

    COM1AsUDPPointToMultiPointasMultiPointConfig OBJECT IDENTIFIER ::=    { COM1Config 19 }
        -- COM1UDPPointToMultiPointasMultiPointConfig Command group

    COM1_UM_M_Remote_Addr  OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Remote IP Addresss."
        ::= { COM1AsUDPPointToMultiPointasMultiPointConfig 1 }

    COM1_UM_M_Remote_Port  OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Remote Port."
        ::= { COM1AsUDPPointToMultiPointasMultiPointConfig 2 }

    COM1_UM_M_Multicast_Addr            OBJECT-TYPE
        SYNTAX  DisplayString (SIZE (0..32))
        ACCESS  read-write
        STATUS  mandatory
        DESCRIPTION "Multicast Address."
        ::= { COM1AsUDPPointToMultiPointasMultiPointConfig 3 }
```

Appendix J: Digital I/O - Example Output driving external relay



microhard SYSTEMS INC.

microhard SYSTEMS INC.

150 Country Hills Landing N.W.
Calgary, AB, Canada T3K 5P3

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