microhard SYSTEMS INC.

Operating Manual

IPn4G

IPn4G LTE Ethernet Bridge/Serial Gateway
Document: IPn4G Operating Manual.v1.31.pdf
FW: v1.1.0-r1060

October 2014

microhard SYSTEMS INC.

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

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

Important User Information

Warranty

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

Warranty Disclaims

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

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

Indemnification

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

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

Proprietary Rights

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

Important User Information (continued)

About This Manual

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

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

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

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

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

Information
Information regarding a particular technology or concept.

Important User Information (continued)

Regulatory Requirements

WARNING

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23cm or greater for the IPn4G utilizing a 3dBi antenna, or 3.5m or greater for the IPn4G utilizing a 34dBi antenna, should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna being used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

WARNING

This device can only be used with Antennas approved for this device. Please contact Microhard Systems Inc. if you need more information or would like to order an antenna.

WARNING

MAXIMUM EIRP
FCC Regulations allow up to 36dBm Effective Isotropic Radiated Power (EIRP). Therefore, the sum of the transmitted power (in dBm and not to exceed +30dBm)), the cabling loss, and omnidirectional antenna gain cannot exceed 36dBm.

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.

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.

Revision History

Revision	Description	Initials	Date
1.0	Initial Release based on firmware v1_1_0-r1010.bin	PEH	Dec 2012
1.1	Updated Network > LAN (Add Interface), Updated SMS Commands, Added SMS Alerts, Updated Wireless Config (Virtual Interfaces), AP Isolation, Updated COM IP Protocol Config (C12.22, GPS), Updated GPS (UDP Report, GpsGate, Recorder, Load Recorder), Updated Firewall, Updated VPN (Gateway Type etc), Added Modbus, Updated misc screen shots, misc formatting. Etc. Based on Firmware v1.1.0-r1028.bin	PEH	Mar 2013
1.2	Misc formatting, updates. Updated WiFi antenna to RP-SMA Female.	PEH	Mar 2013
1.21	Corrected LTE Band Spec	PEH	Apr 2013
1.22	Added PoE information	PEH	Apr 2013
1.23	Added/Corrected Digital I/O pins location	PEH	Apr 2013
1.24	Corrected enclosure drawings	PEH	Nov 2013
1.3	Firmware v1.1.0-r1060	PEH	Dec 2013
1.31	Misc Corrections	PEH	Oct 2014

Table of Contents

Table of Contents

Table of Contents

1.0 Overview

The IPn4G is a high-performance 4G LTE Cellular Ethernet & Serial Gateway with 802.11 b/g WiFi capability, RJ45 Ethernet Port, Digital I/O, and two serial communication ports, one a fully complimented RS232/485/422 serial port.

The IPn4G utilizes the cellular infrastructure to provide network access to wired and wireless devices anywhere cellular coverage is supported by a cellular carrier. The IPn4G supports up to 100Mbps when connected to a LTE enabled carrier, or global fallback to 3G/Edge networks for areas without 4G LTE.

Providing reliable wireless Ethernet bridge functionality as well gateway service for most equipment types which employ an RS232, RS422, or RS485 interface, the IPn4G can be used in a limitless number and types of applications such as:

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

1.1 Performance Features

Key performance features of the IPn4G include:

- Fast 4G LTE Link to Wireless Carrier
- Up to 100Mbps Downlink / 50 Mbps Uplink
- Fast Data Rates to 802.11b/g WiFi Devices
- Digital I/O - 1 Input, 1 Output
- DMZ and Port Forwarding
- 10/100 Ethernet Port (WAN/LAN)
- Integrated GPS (TCP Server/UDP Reporting)
- User interface via local console, telnet, web browser
- communicates with virtually all PLCs, RTUs, and serial devices through either RS232, RS422, or RS485 interface
- Local & remote wireless firmware upgradable
- User configurable Firewall with IP/MAC ACL
- IP/Sec secure VPN and GRE Tunneling

1.0 Overview

1.2 Specifications

For detailed specifications, please see the specification sheets available on the Microhard web-site @ http:///www.microhardcorp.com for your specific model.

Electrical/General

Cellular:

Supported Bands: 4G LTE B4/B17 (1700/2100/700 MHz)
Global Fallback to:
HSPA+/UMTS 850/AWS/1900/2100 MHz
GPRS 850/900/1800/1900 MHz

Data Features: 4G LTE
Up to 100 Mbps downlink
Up to 50 Mbps uplink

SIM Card: 1.8 / 3.0 V

WiFi:

Frequency: 2.4 GHz

Spread Method: (CCK) QPSK/BPSK
(OFDM) BPSK, QPSK, QAM16, QAM32, QAM64

Data Rates: 802.11b/g

TX Power: Adjustable / Up to 30dBm

Data Encryption: WEP, WPA(PSK), WPA2(PSK), WPA+WPA2 (PSK)
(Subject to Export Restrictions)

General:

Input Voltage: 9 - 30 VDC

Power over Ethernet: Passive PoE on Ethernet Port

Current Consumption:
(@12VDC & 20dB WiFi)

Cellular	WiFi	Idle (mA)	Typical (mA)
On	On	350	390
On	Off	280	320
Off	On	270	320

Table 1-2-1: IPn4G Current Consumption

Serial Baud Rate: 300bps to 921kbps

Ethernet: 10/100 BaseT, Auto - MDI/X, IEEE 802.3

1.0 Overview

1.2 Specifications (Continued)

Network Protocols:	TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP
Operating Modes:	Access Point, Client/Station, Repeater, Mesh Point
Management:	Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade
Diagnostics:	Status LED's, RSSI, Ec/No, Temperature, Remote Diagnostics, Watchdog, UDP Reporting
Digital I/O:	1 Inputs / 1 Outputs

Environmental

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

Humidity: 5% to 95% non-condensing

Mechanical

Dimensions:

2.25" (57mm) X 3.85" (98mm) X 1.5" (45mm)

Weight:

Approx. 250 grams

Connectors:

Antenna: Wi-Fi: RP-SMA Female
Cellular: 2x SMA Female (Main, DIV)
GPS Uses Diversity Antenna

Data: RS232 COM1: DB-9 Female (Digital I/O)
RS232 Data: DB-9 Female
RS485: SMT: 6-Pin Micro MATE-N-LOK AMP 3-794618-6
Mating Connector: 6-Pin Micro MATE-N-LOK AMP 794617-6
Ethernet : RJ-45

PWR, Misc: Power: SMT: 4-Pin Micro MATE-N-LOK AMP 3-794618-4
Mating Connector: 4-Pin Micro MATE-N-LOK AMP 794617-4

2.0 Quick Start

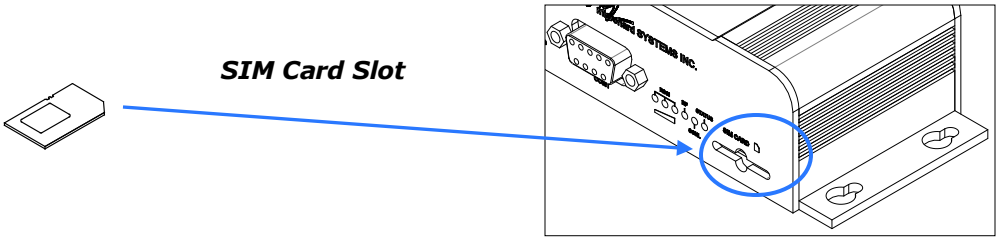
This QUICK START guide will walk you through the setup and process required to access the WebUI configuration window and to establish a basic wireless connection to your carrier.

Note that the units arrive from the factory with the Local Network setting configured as 'Static' (IP Address 192.168.168.1, Subnet Mask 255.255.255.0, and Gateway 192.168.168.1), in DHCP server mode. (This is for the LAN Ethernet Adapter on the back of the IPn4G unit.

2.1 Installing the SIM Card

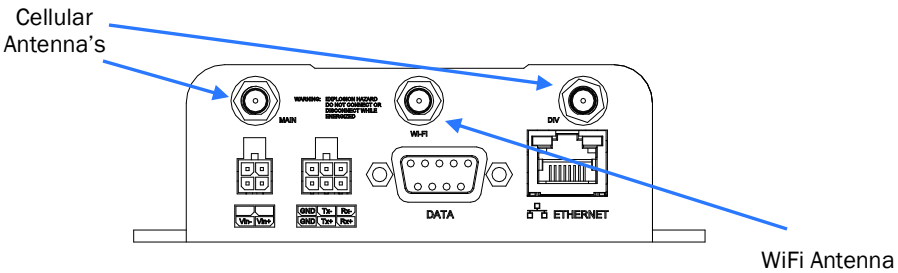
To reset to factory defaults, press and hold the CFG button for 8 seconds with the IPn4G powered up. The LED's will flash quickly and the IP4G will reboot with factory defaults.

✓ Before the IPn4G 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.



2.2 Getting Started with Cellular

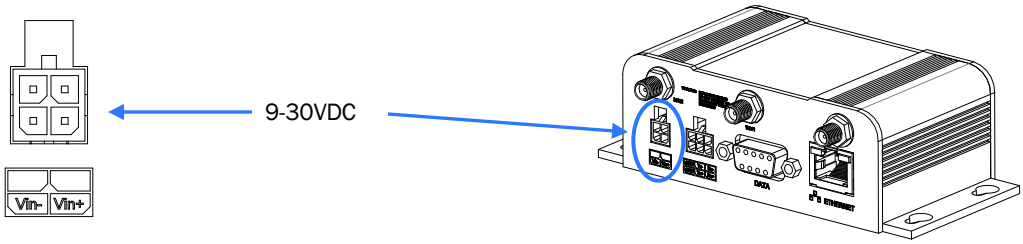
✓ Connect the Antenna's to the applicable ***ANTENNA*** jack's of the IPn4G.



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

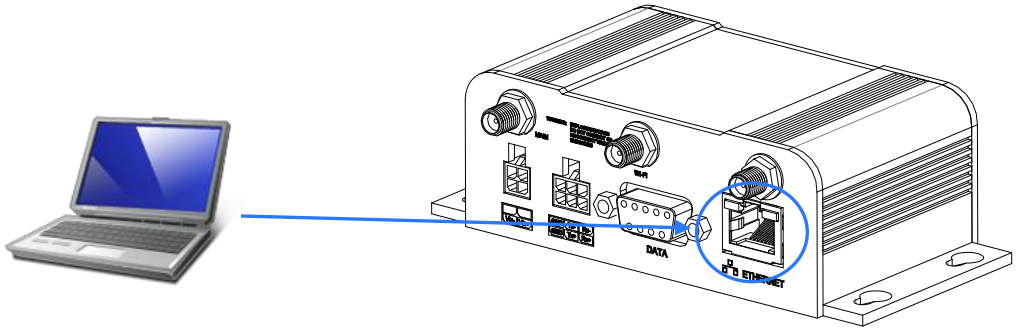
The unit can also be powered via PoE using a MHS PoE injector.

✓ Connect the power connector to the power adapter and apply power to the unit, the RF & SGNL LED's will flash during boot-up, once they stop, proceed to the next step.



2.0 Quick Start

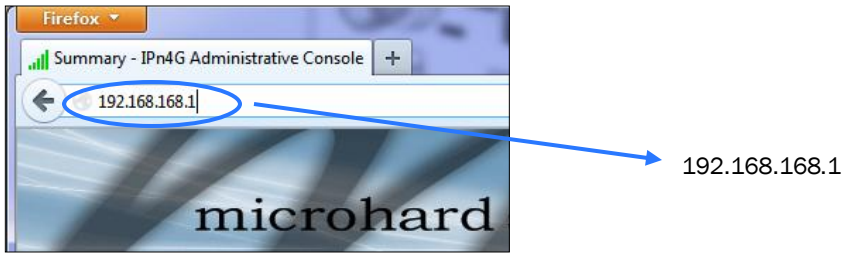
✓ Connect A PC configured for DHCP directly to the ***ETHERNET*** port of the IPn4G, using an Ethernet Cable. If the PC is configured for DHCP it will automatically acquire a IP Address from the IPn4G.



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

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

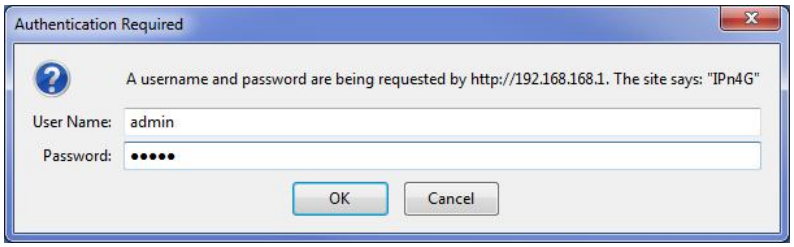


✓ The IPn4G will then ask for a Username and Password. Enter the factory defaults listed below.

The factory default login:

User name: admin
Subnet: admin

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

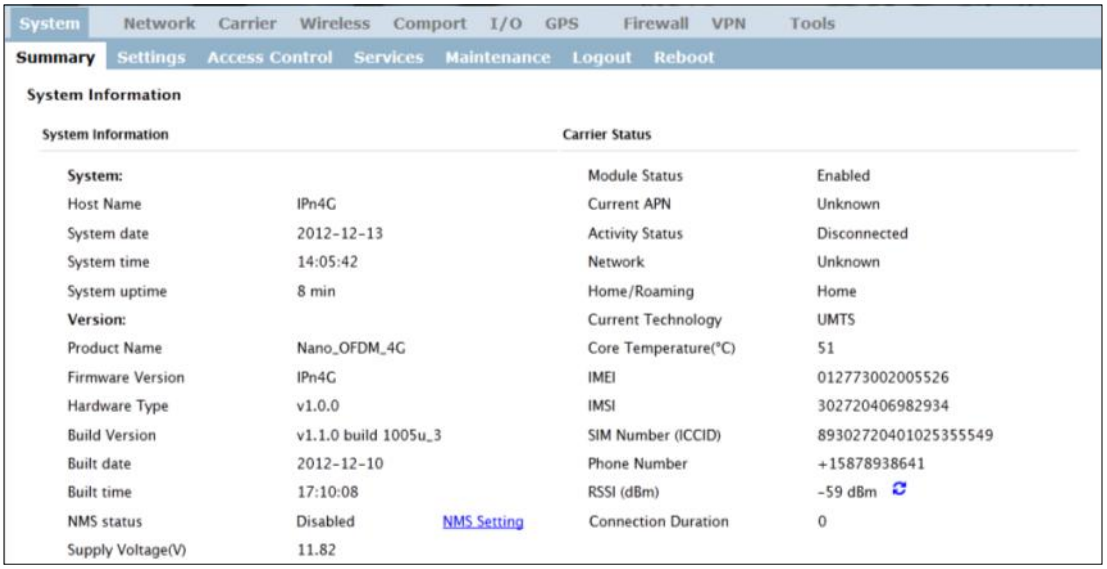


The Factory default login:

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

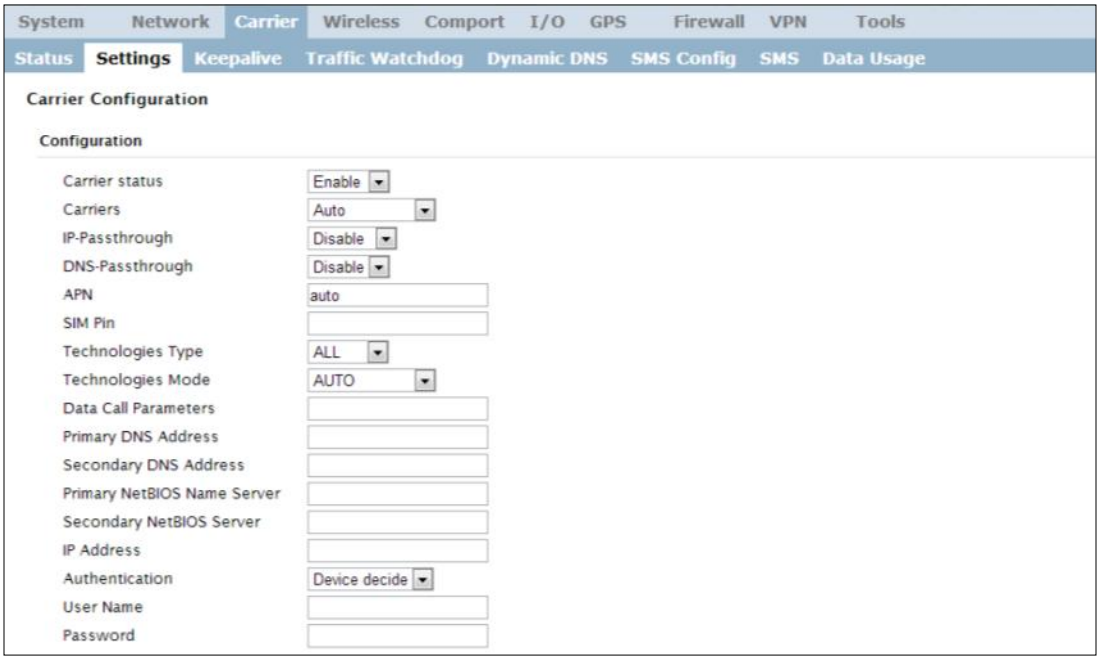
2.0 Quick Start

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



Auto APN: Introduced in firmware version v1.1.0-r1038, the IPn4G will attempt to detect the carrier based on the SIM card installed and cycle through a list of commonly used APN's to provide quick network connectivity.

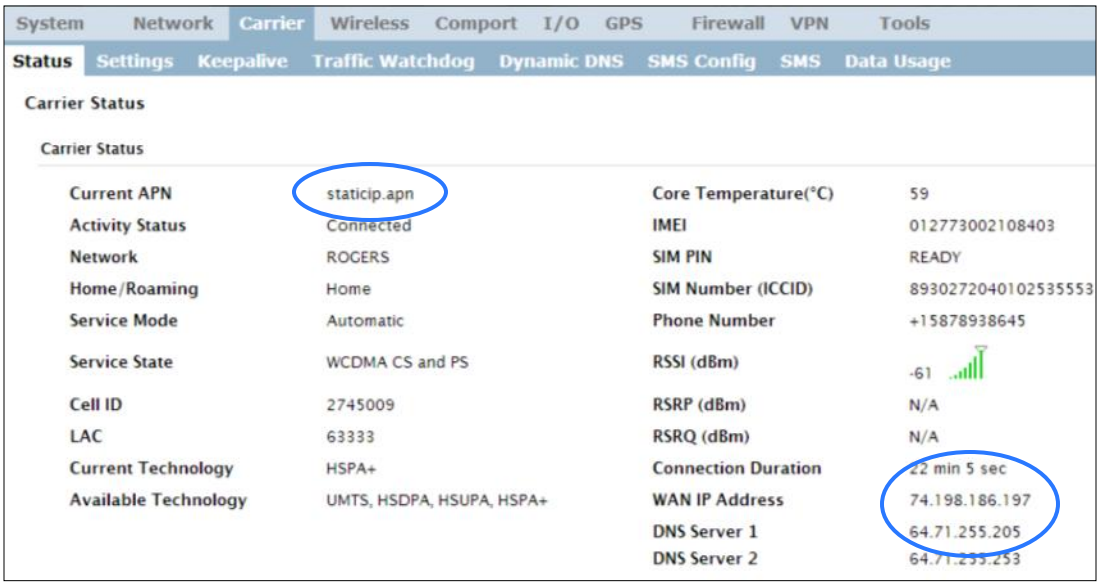
✓ As seen above under Carrier Status, the SIM card is installed, but an APN has not been specified. Setting the APN to auto (default) may provide quick network connectivity, but may not work with some carriers, or with private APN's. To set or change the APN, click on the Carrier > Settings tab and enter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



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

2.0 Quick Start

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



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

- ✓ Congratulations! Your IPn4G is successfully connected to your Cellular Carrier. The next section gives a overview on enabling and setting up the WiFi Wireless features of the modem giving 802.11 devices network access.

- ✓ To access devices connected to IPn4G remotely, one or more of the following must be configured: IP-Passthrough, Port Forwarding, DMZ. Another option would be to set up a VPN.

2.0 Quick Start

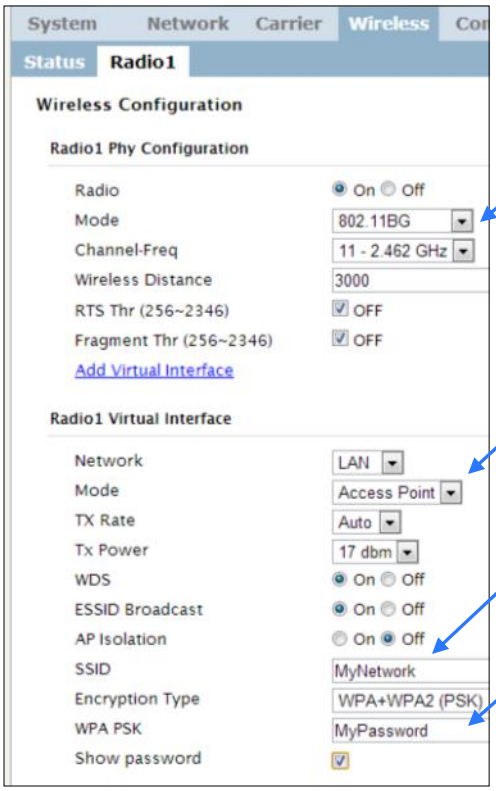
2.3 Getting Started with WiFi

This **Quick Start** section walks users through setting up a basic WiFi AP (Access Point). For additional settings and configuration considerations, refer to the appropriate sections in the manual. This walkthrough assumes all setting are in the factory default state.

2.3.1 Setting up WiFi

- ✓ Use ***Section 2.2*** *Getting Started with Cellular* to connect, power up and log in and configure the Carrier in a IPn4G.

- ✓ Click on the Wireless > Radio1 Tab to setup the WiFi portion of the IPn4G.



In **Radio1 Phy Configuration**, ensure the mode is set for 802.11BG.

In the **Radio1 Virtual Interface**, ensure that the Mode is set for Access Point.

Enter a name for the Wireless Network under **SSID**. This example uses MyNetwork

(Optional) Set a password for the WiFi, this example uses MyPassword

Click **Submit.**

2.0 Quick Start

2.3.2 Connecting to WiFi

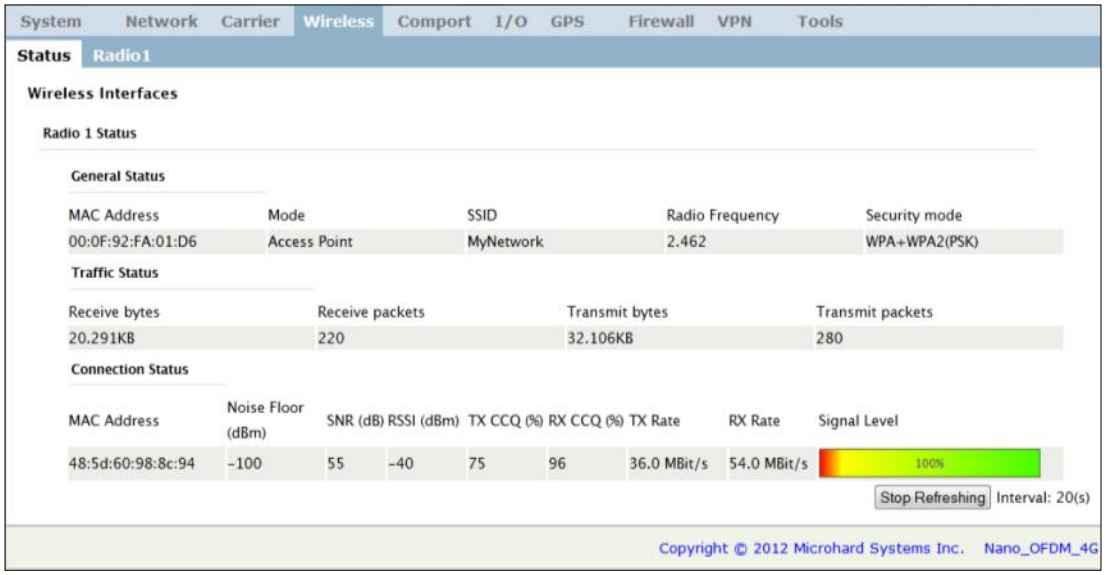
- ✓ Now that the IPn4G has connection to the Cellular Carrier (See Section 2.2) and the WiFI has been set up (See Section 2.3), WiFi devices should be able to detect and connect to the IPn4G.

- ✓ On a WiFi enabled PC/Device, the SSID of MyNetwork, that was created in the last example should be visible. Connect to that SSID and enter the password.

- ✓ Once connected the status should change to connected, and network access should be enabled.

2.0 Quick Start

✓ The status of the WiFi connection should also be visible in the Wireless > Status tab in the WebUI as seen below.



3.0 Hardware Features

3.1 IPn4G

The IPn4G is a fully-enclosed unit ready to be interfaced to external devices.

Image 3-1: Front View of IPn4G

Image 3-2: Rear View of IPn4G

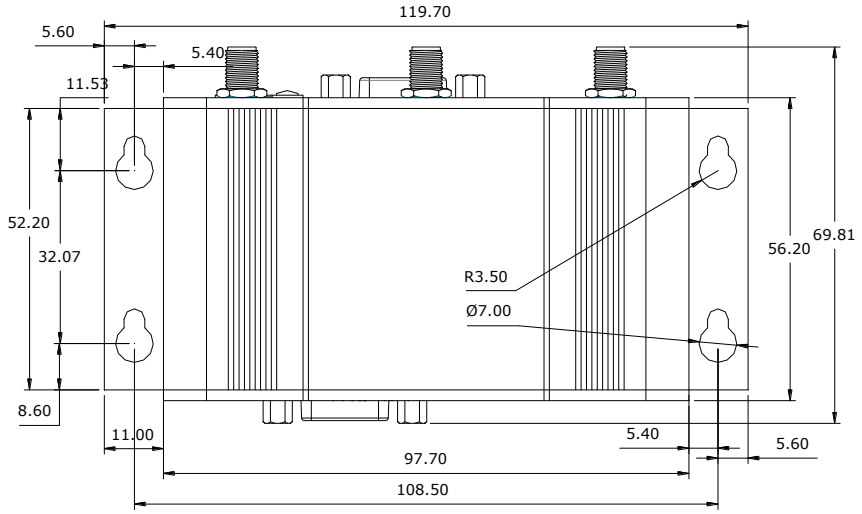
Any IPn4G may be configured as an Access Point, Station/Client, Repeater or Mesh Node. This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the device: if you are familiar with one unit, you will be familiar with all units.

The IPn4G features:

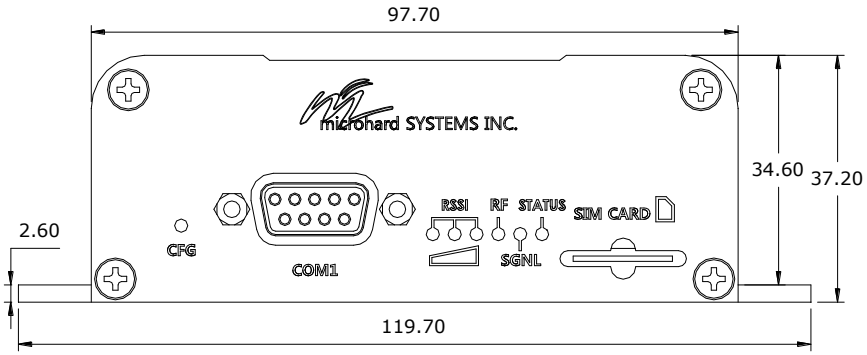
- Standard Connectors for:
  - 1 Ethernet Ports (RJ45)
  - Data Port (RS232/DB9)
  - COM2 Port (RS232)
  - 4-Pin: MATE-N-LOK Type Connector for Power
  - 6-Pin: MATE-N-LOK Type Connector for RS485 Data
  - Cellular Antenna (SMA Female Antenna Connection x2)
  - WiFi Antenna (RP-SMA Female Antenna Connection) (Optional)
- Status/Diagnostic LED's for STATUS, RF, SGNL, RSSI x 3
- CFG Button for factory default / firmware recovery operations
- Mounting Holes

3.0 Hardware Features

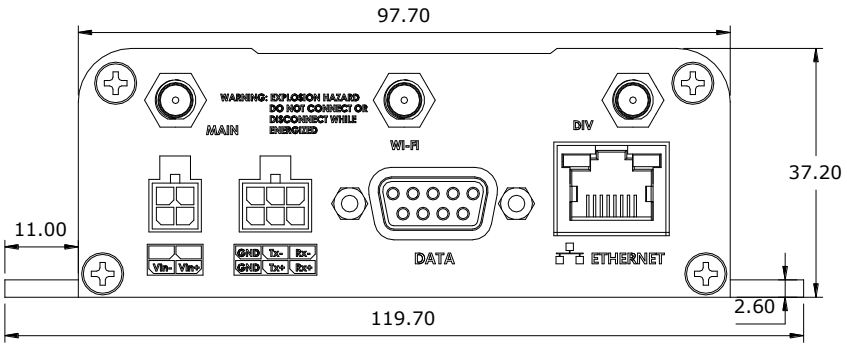
3.1.1 Mechanical Drawings



Drawing 3-1: IPn4G Top View Dimensions



Drawing 3-2: IPn4G Front View Dimensions



Drawing 3-3: IPn4G Rear View Dimensions

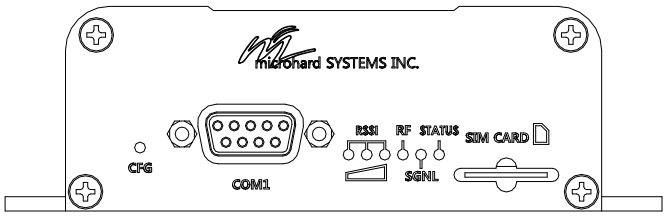
Note: All dimension units: Millimeter

3.0 Hardware Features

3.1.2 Connectors and Indicators

3.1.2.1 Front

On the front of the IPn4G is the COM1 port, CONFIG Button, RSSI, STATUS, RF and SGNL LED's as described below:



Drawing 3-4: IPn4G Front View

The **COM1** port (RS232) is used for:

- AT Command Interface at 115.2kbps and HyperTerminal (or equivalent).
- User data (RS232 - RxD, TxD, and SG)

Signal Name	PIN #	Input or Output
RXD	2	O
TXD	3	I
SG	5	

Table 3-1: COM1 Port RS232 Pin Assignment

Caution: Using a power supply that does not provide proper voltage may damage the IPn4G unit.

CONFIG (Button) - Holding this button depressed while powering-up the IPn4G 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 192.168.168.1. This IP address is useable in a Web Browser for accessing the Web User Interface.

RF(Red)/SGNL(Green) LED's - When the unit is equipped with WiFi, the RF/SGNL LED's indicate WiFi activity. In units not equipped with WiFi, the RF/SGNL LED's indicate carrier (cellular) traffic. Also, during system bootup, the RF & SGNL LED's will flash.

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.

STATUS LED (Red) - The Status LED indicates that power has been applied to the module.

SIM Card - This slot is used to install a SIM card provided by the cellular carrier to enable communication to their cellular network. Ensure the SIM card is installed properly by paying attention to the diagram printed above the SIM card slot.

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

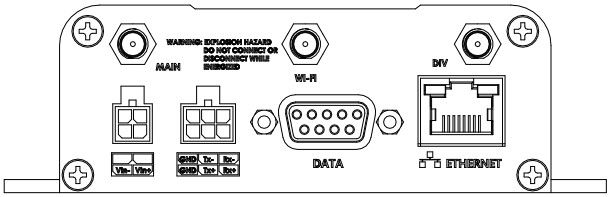
Table 3-2: RSSI LED's

3.0 Hardware Features

3.1.2 Connectors and Indicators

3.1.2.2 Rear

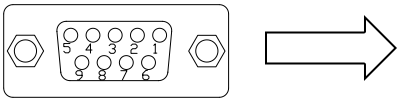
On the back of the IPn4G is the Data (COM0) port, RS485/422 interface, as well as the power connections. The unit also has the SMA(F) connectors for the Main (TX/RX), the Diversity (RX) antenna's, and a RP-SMA Female connector for the optional WiFi antenna.



Drawing 3-5: IPn4G Rear View

The **DATA (RS232 Port (COM0))** on the rear of the circuit board is used for:

- RS232 serial data (300-921kbps)

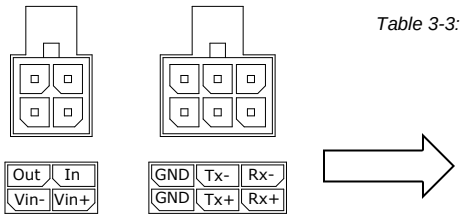


Name	Data Port	Input or Output
DCD	1	O
RXD	2	O
TXD	3	I
DTR	4	I
SG	5	
DSR	6	O
RTS	7	I
CTS	8	O
RING	9	O

Table 3-3: Data RS232 Pin Assignment

The **RS422/485 Port** is used to interface the IPn4G to a DTE with the same interface type. Either the RS232 or RS422/485 interface can be used for data traffic, not both.

Vin+/Vin– is used to power the unit. The input Voltage range is 9-30 Vdc.



Name	Input or Output
Tx+	O
Tx1	O
Rx+	I
Rx-	I
Vin -	
Vin +	I
Out	O
In	I

Table 3-4: Data RS422/485, Vin, Digital I/O Pin Assignment

Digital I/O– The IPn4G has 1 input / 1 output. Inputs have 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. Maximum recommended load for the output pin is 150mA @ 30 Vdc (Vin).

PoE– The IPn4G 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 3-5: Ethernet PoE Connections

4.0 Configuration

4.0 Web User Interface

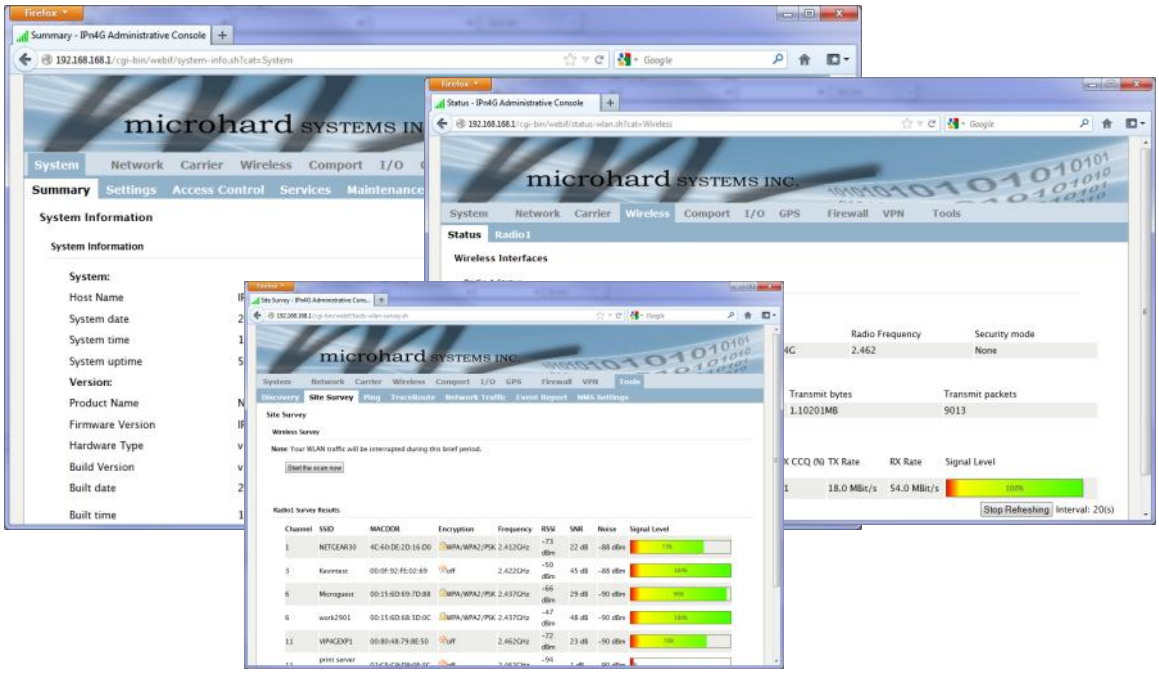


Image 4-0-1: WebUI

Initial configuration of an IPn4G using the Web User (Browser) Interface (Web UI) method involves the following steps:

- configure a static IP Address on your PC to 192.168.168.10 (or any address on the 192.168.168.X subnet other than the default IP of 192.168.168.1)
- connect the IPn4G ETHERNET port to PC NIC card using an Ethernet cable
- apply power to the IPn4G and wait approximately 60 seconds for the system to load
- open a web browser and enter the factory default IP address of the unit: 192.168.168.1
- logon window appears; log on using default Username: ***admin*** Password: ***admin***
- use the web browser based user interface to configure the IPn4G as required.
- refer to **Section 2.0: Quick Start** for step by step instructions.

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

4.0 Configuration

4.0.1 Logon Window

Upon successfully accessing the IPn4G using a Web Browser, the Logon window will appear.

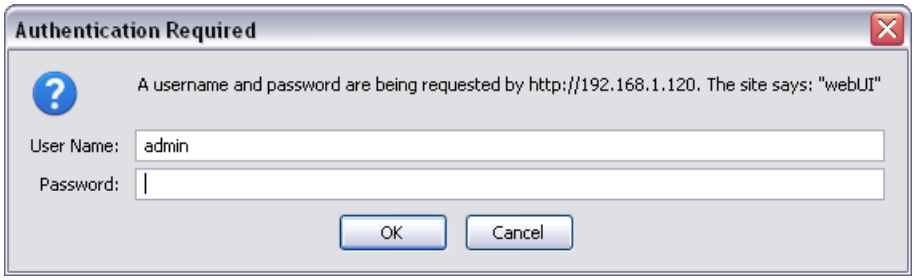


Image 4-0-2: Logon Window

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

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

The default password is: **admin**

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.

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

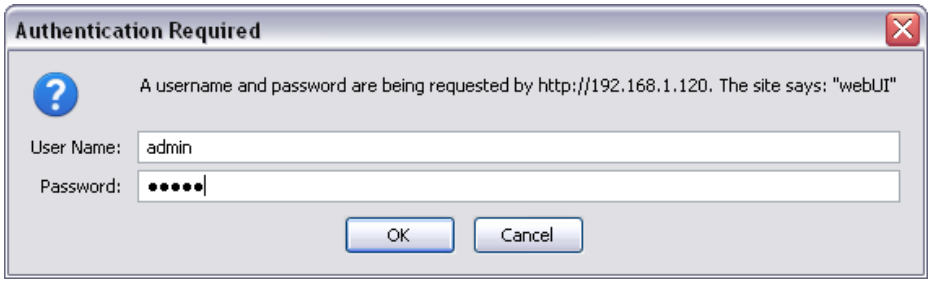


Image 4-0-3: Logon Window : Password Entry

4.0 Configuration

4.1 System

The main category tabs located at the top of the navigation bar separate the configuration of the IPn4G into different groups based on function. The System Tab contains the following sub menu's:

- Summary - Status summary of entire radio including network settings, version information, and radio connection status.
- Settings - Host Name, Default System Mode (Bridge or Router), System Time/Date, HTTP Port for the WebUI,
- Access Control - Change passwords, create new users
- Services - Enable/Disable RSSI LED's, SSH and Telnet services
- Maintenance - Version information, firmware Upgrades, reset to defaults, configuration backup and restore.
- Reboot - Remotely reboot the system.
- Logout - Logout of the current browser session.

4.1.1 System > Summary

The System Summary screen is displayed immediately after initial login, showing a summary and status of all the functions of the IPn4G in a single display. This information includes System Status, Carrier Status, 4G & LAN network information, version info and WiFi radio status as seen below.

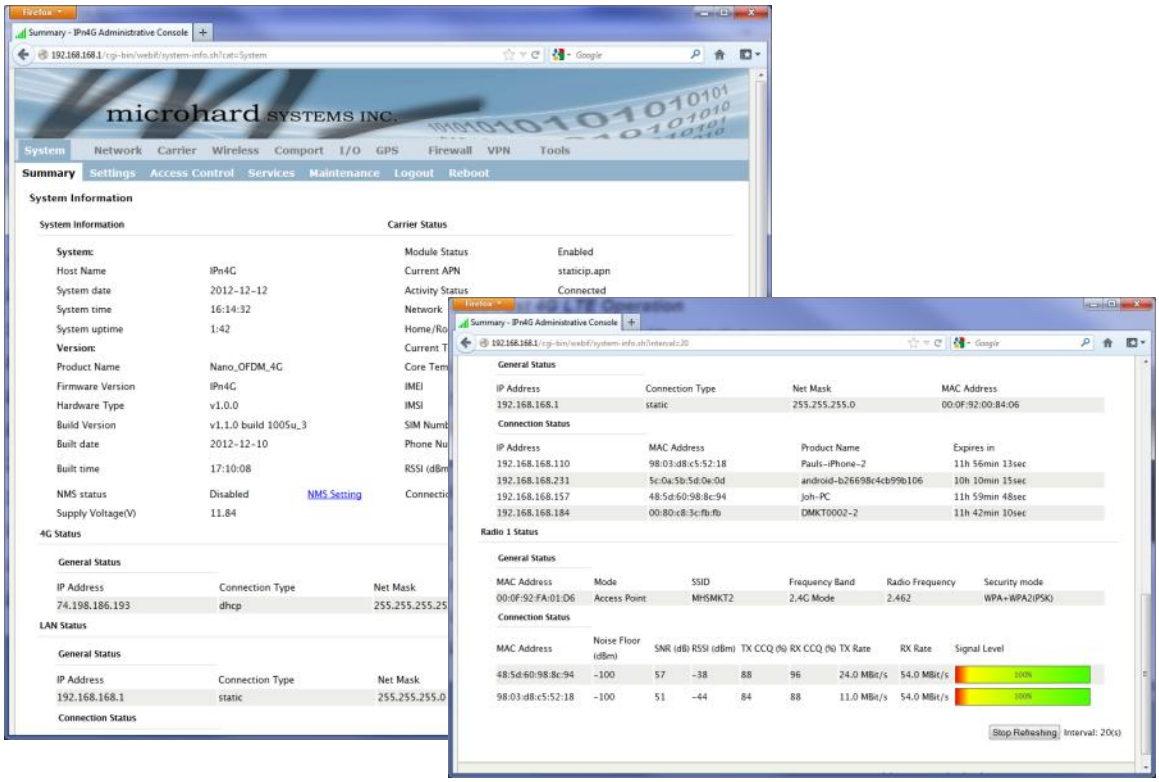


Image 4-1-1: System Info Window

4.0 Configuration

4.1.2 System > Settings

System Settings

Options available in the System Settings menu allow for the configuration of the Host Name.

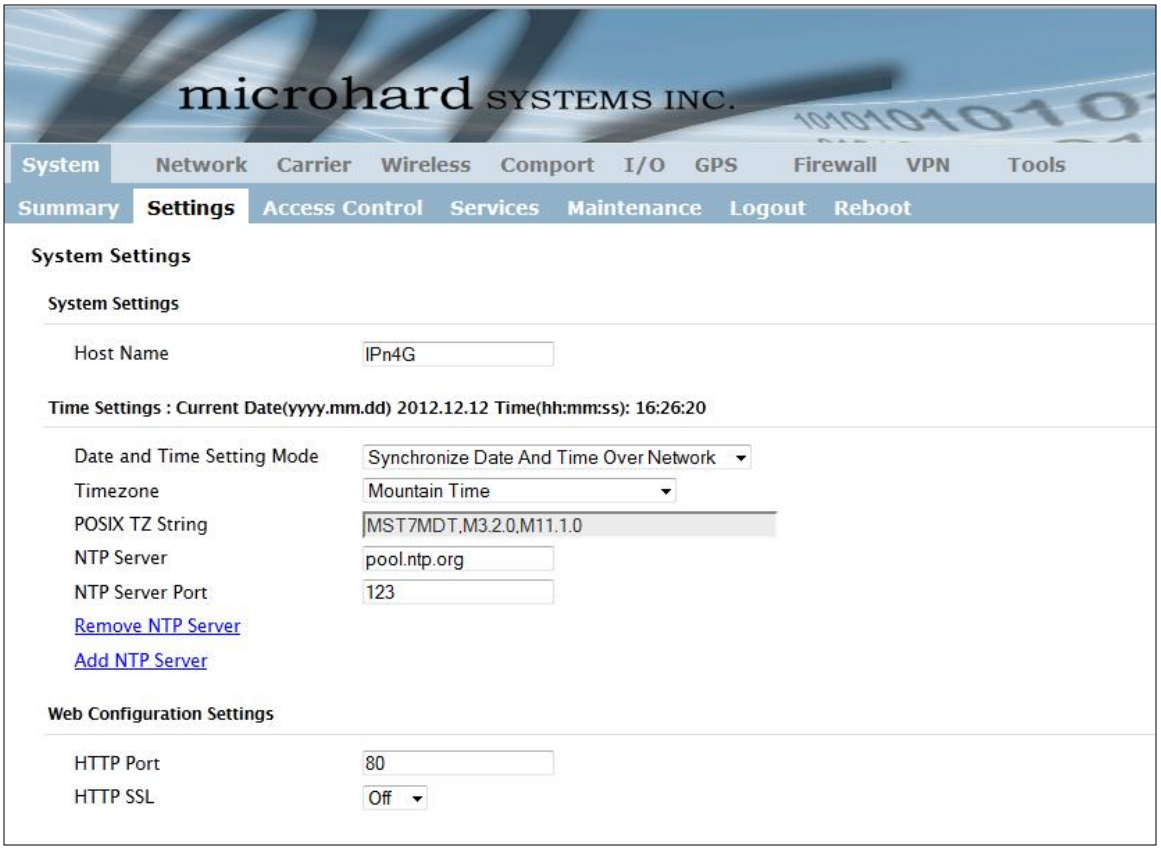


Image 4-1-2: System Settings > System Settings

The Host Name must not be confused with the **Network Name (SSID)** (Wireless Configuration menu). The Network Name MUST be exactly the same on each wireless device within a IPn4G network.

Host Name	Values (characters)
The Host Name is a convenient identifier for a specific IPn4G unit. This feature is most used when accessing units remotely: a convenient cross-reference for the unit's WAN IP address. This name appears when logged into a telnet session, or when the unit is reporting into Microhard NMS System.	IPn4G**+wifi (varies)** up to 30 characters

4.0 Configuration

Time Settings

The IPn4G can be set to use a local time source, thus keeping time on its own, or it can be configured to synchronize the date and time via a NTP Server. The options and menus available will change depending on the current setting of the Date and Time Setting Mode, as seen below.

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

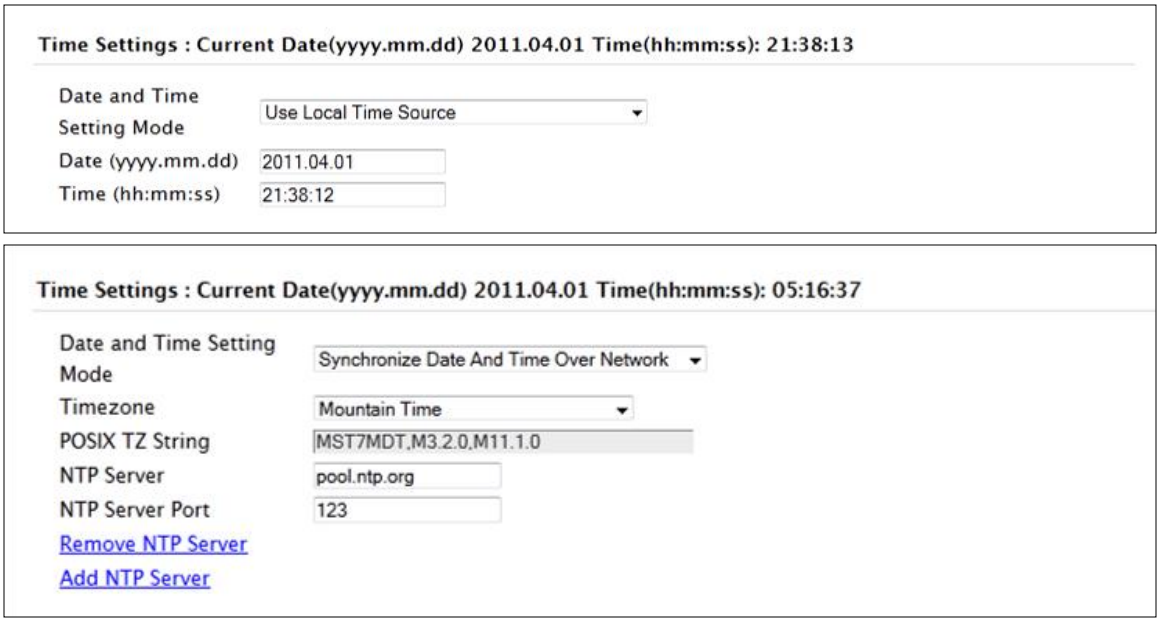


Image 4-1-3: System Settings > Time Settings

Date and Time Setting Mode

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

Values (selection)

Use Local Time Source
Synchronize Date And Time Over Network

Date

The calendar date may be entered in this field. Note that the entered value is lost should the IPn4G lose power for some reason.

Values (yyyy-mm-dd)

2011.04.01 *(varies)*

Time

The time may be entered in this field. Note that the entered value is lost should the VIP Series lose power for some reason.

Values (hh:mm:ss)

11:27:28 *(varies)*

4.0 Configuration

Timezone	
If connecting to a NTP time server, specify the timezone from the dropdown list.	**Values (selection)** **User Defined** (or out of date)

POSIX TZ String	
This displays the POSIX TZ String used by the unit as determined by the timezone setting.	**Values (read only)** *(varies)*

NTP Server	
Enter the IP Address or domain name of the desired NTP time server.	**Values (address)** **pool.ntp.org**

NTP Port	
Enter the IP Address or domain name of the desired NTP time server.	**Values (port#)** **123**

Web Configuration Settings

The last section of the System Setting menu allows the configuration of the HTTP and HTTPS Ports used for the web server of the WEBUI.

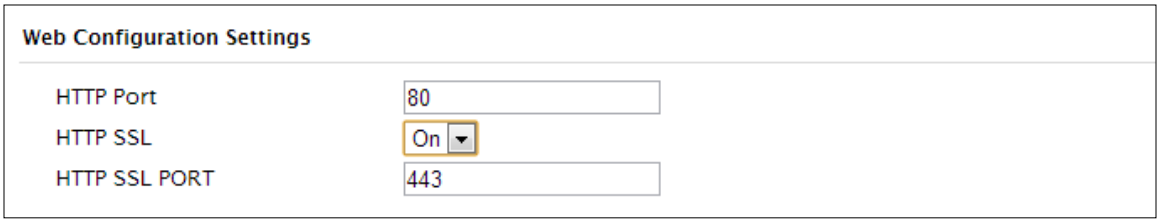


Image 4-1-4: System Settings > Web Configuration Settings

HTTP Port	
The default web server port for the web based configuration tools used in the VIP is port 80. Change as required, but keep in mind that if a non standard port is used, it must be specified in a internet browser to access the unit. (example: http://192.168.168.1:8080)	**Values (port#)** **80**

HTTP Port	
The secure web port (HTTPS) can be enabled or disabled using the **HTTP SSL** On/Off drop down menu. If enabled, the port used can be specified, the default is port 443.	**Values (port#)** **443**

4.0 Configuration

4.1.3 System > Access Control

Password Change

The Password Change menu allows the password of the user 'admin' to be changed. The 'admin' username cannot be deleted, but additional users can be defined and deleted as required as seen in the Users menu below.

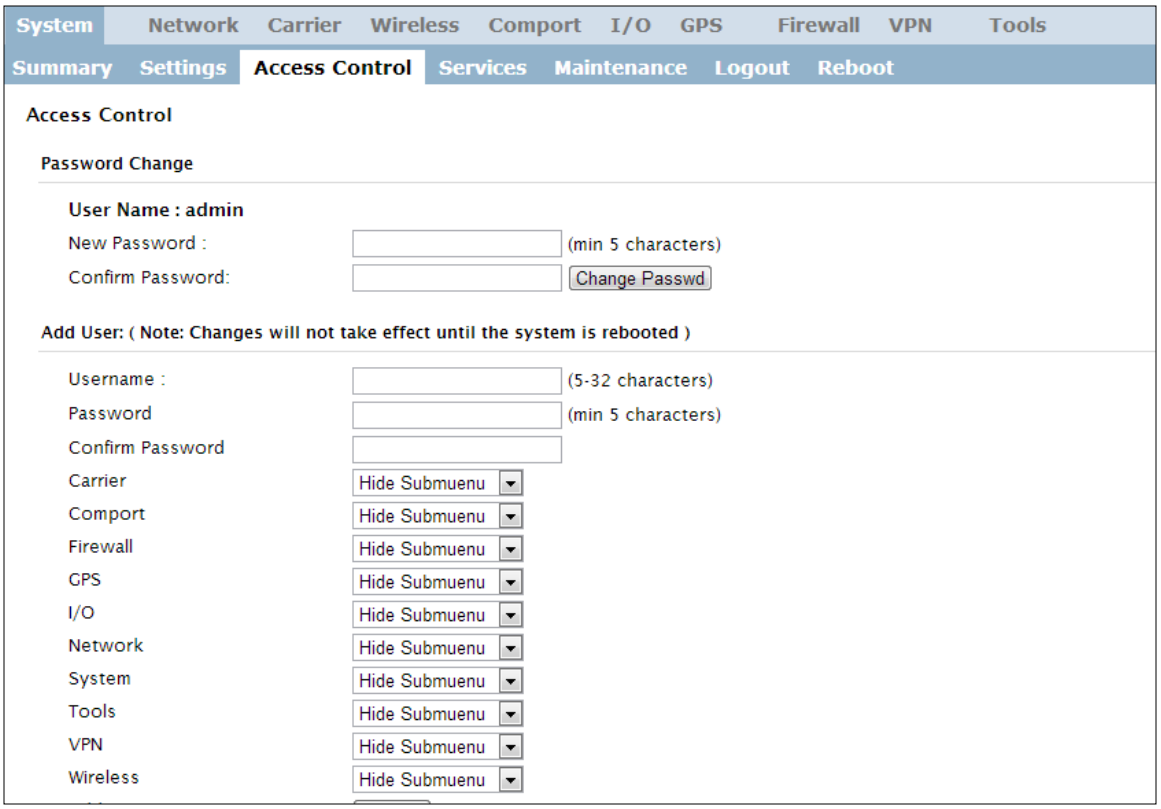


Image 4-1-5: Access Control > Password Change

New Password	Values (characters)
Enter a new password for the 'admin' user. It must be at least 5 characters in length. The default password for 'admin' is 'admin'.	**admin** min 5 characters

Confirm Password	Values (characters)
The exact password must be entered to confirm the password change, if there is a mistake all changes will be discarded.	**admin** min 5 characters

4.0 Configuration

4.1.3 System > Access Control

Users

Different users can be set up with customized access to the WebUI. Each menu or tab of the WebUI can be disabled on a per user basis as seen below.

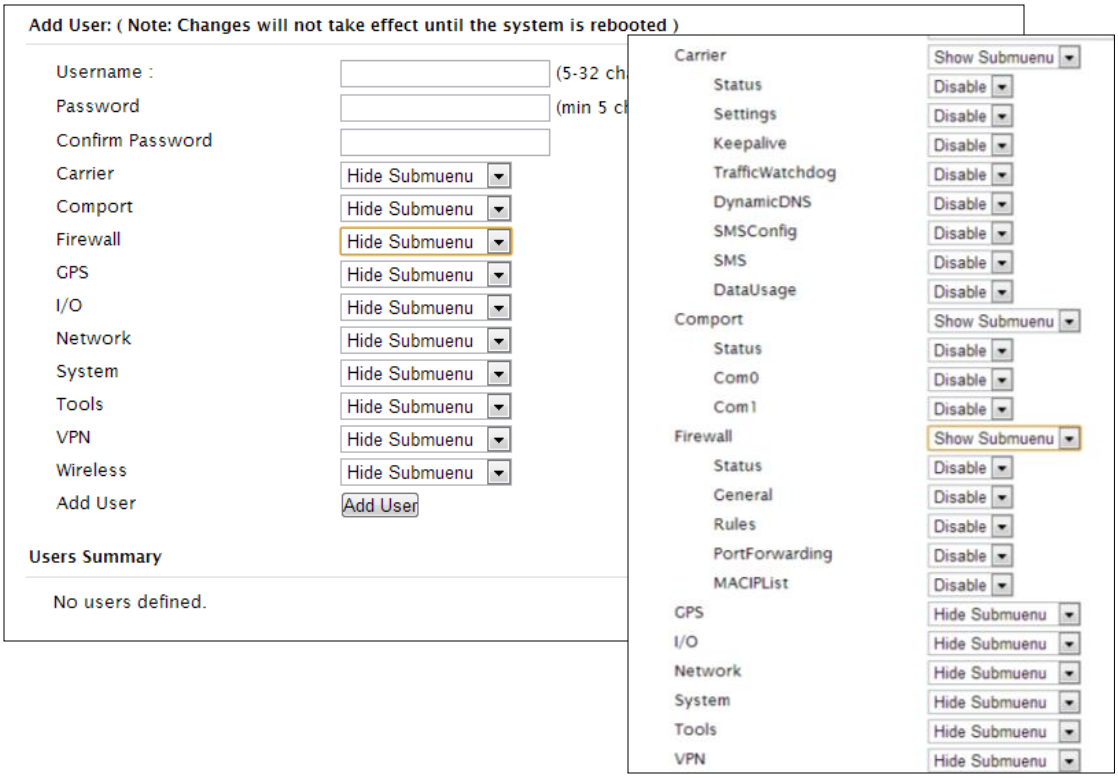


Image 4-1-6: Access Control > Users

Username	
Enter the desired username. Minimum or 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted.	**Values (characters)** *(no default)* *Min 5 characters* *Max 32 characters*

Password / Confirm Password	
Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.	**Values (characters)** *(no default)* min 5 characters

4.0 Configuration

4.1.4 System > Services

Available Services

Certain services in the IPn4G can be disabled or enabled for either security considerations or resource/power considerations. The Enable/Disable options are applied after a reboot and will take affect after each start up. The Start/Restart/Stop functions only apply to the current session and will not be retained after a power cycle.

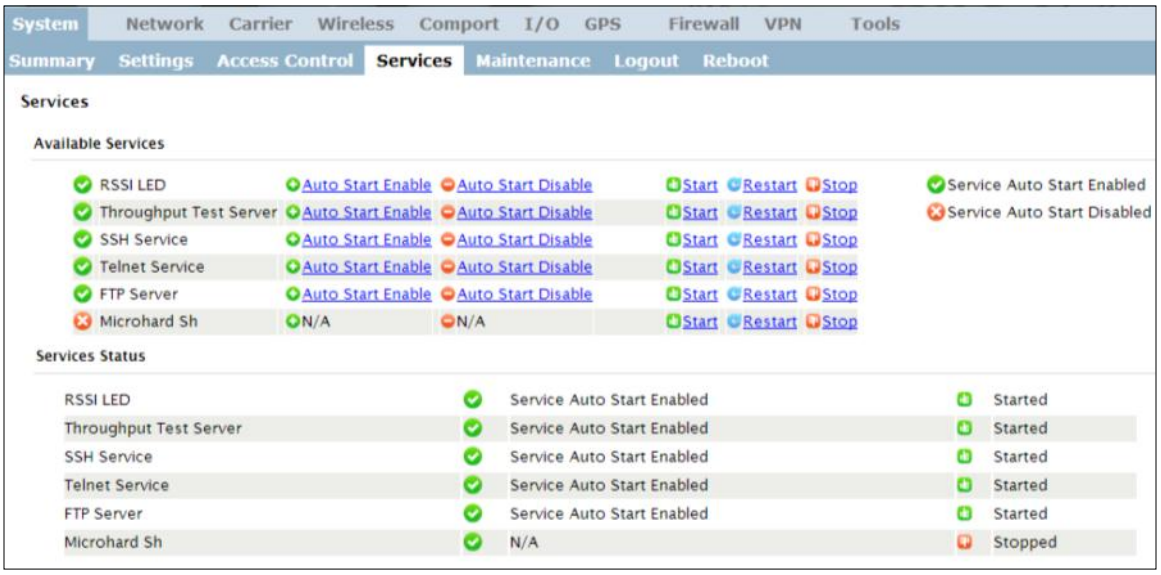


Image 4-1-7: System > Services

RSSI LED	
The IPn4G has the ability to turn off the RSSI LED's. The RSSI value can still be read from the unit, but the status will not be visible on the unit itself .	**Values (selection)** **Start** / Restart / Stop

Throughput Test Server	
For testing purposes the IPn4G has an internal iperf server that can be used to test unit performance. The user must install a iperf client to use this functionality.	**Values (selection)** **Start** / Restart / Stop

SSH Service	
Using the SSH Service Enable/Disable function, you can disable the SSH service (Port 22) from running on the IPn4G.	**Values (selection)** **Start** / Restart / Stop

4.0 Configuration

Telnet Service	
Using the Telnet Service Enable/Disable function, you can disable the Telnet service (Port 23) from running on the IPn4G.	**Values (characters)** **Start** / Restart / Stop

FTP Server	
Using the FTP Service Enable/Disable function, you can disable the FTP service (Port 21) from running on the IPn4G. This port is reserved for internal use / future use.	**Values (selection)** **Start** / Restart / Stop

Microhard Sh	
Custom SSH Port. Reserved for internal use.	**Values (selection)** Start / Restart / **Stop**

4.0 Configuration

4.1.5 System > Maintenance

Version Information

Detailed version information can be found on this display. The Product Name, Firmware Version, Hardware Type, Build Version, Build Date and Build Time can all be seen here, and may be requested from Microhard Systems to provide technical support.

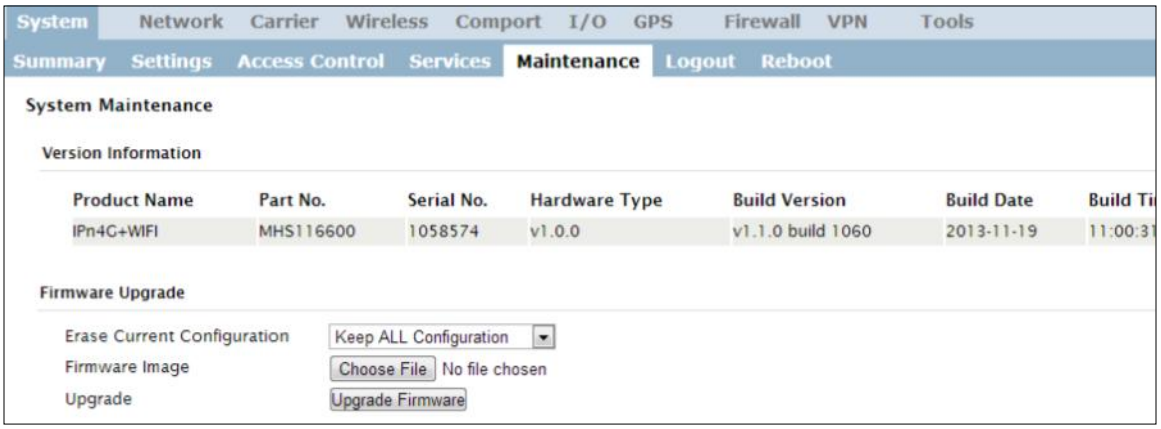


Image 4-1-8: Maintenance > Version Information / Firmware Upgrade

Firmware Upgrade

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

Erase Current Configuration	
Check this box to erase the configuration of the IPn4G unit during the upgrade process. This will upgrade, and return the unit to factory defaults, including the default IP Addresses and passwords. Not checking the box will retain all settings during a firmware upgrade procedure.	**Values (check box)** **unchecked**

Firmware Image	
Use the Browse button to find the firmware file supplied by Microhard Systems. Select “Upgrade Firmware” to start the upgrade process. This can take several minutes.	**Values (file)** *(no default)*

4.0 Configuration

4.1.5 System > Maintenance

Reset to Default

The IPn4G may be set back to factory defaults by using the Reset to Default option under System > Maintenance > Reset to Default. ***Caution* - All settings will be lost!!!**

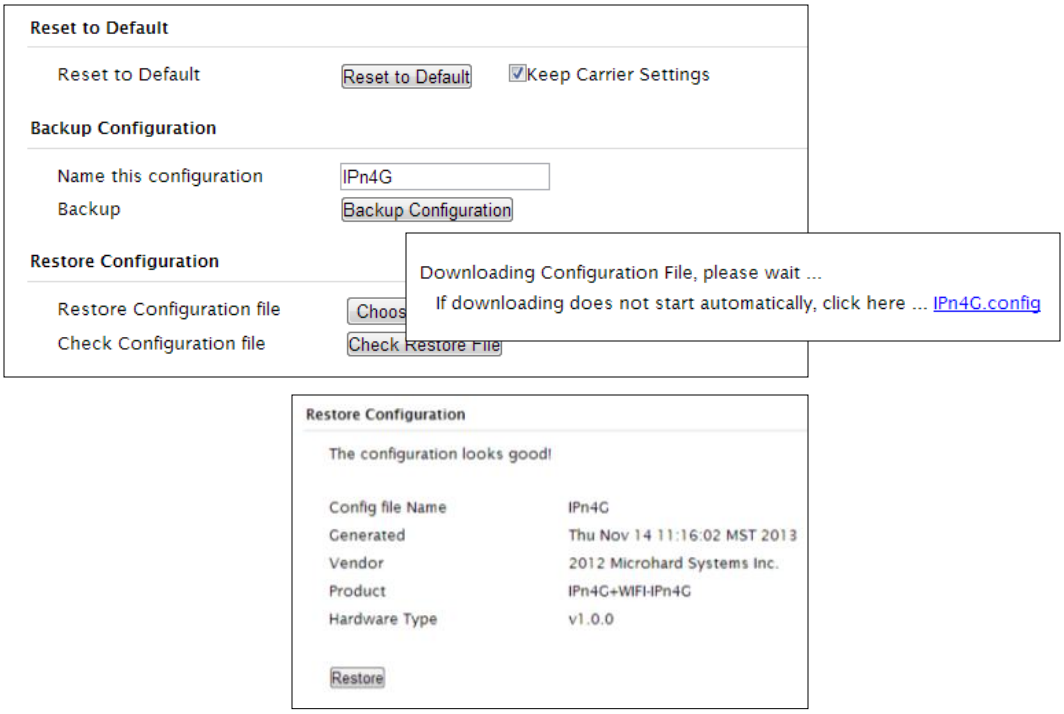


Image 4-1-9: Maintenance > Reset to Default / Backup & Restore Configuration

Backup & Restore Configuration

The configuration of the IPn4G can be backed up to a file at any time using the Backup Configuration feature. The file can the be restored using the Restore Configuration feature. It is always a good idea to backup any configurations in case of unit replacement. The configuration files cannot be edited offline, they are used strictly to backup and restore units.

Name this Configuration / Backup Configuration

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

Restore Configuration file / Check Restore File / Restore

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

4.0 Configuration

4.1.6 System > Logout

The logout function allows a user to end the current configuration session and prompt for a login screen.

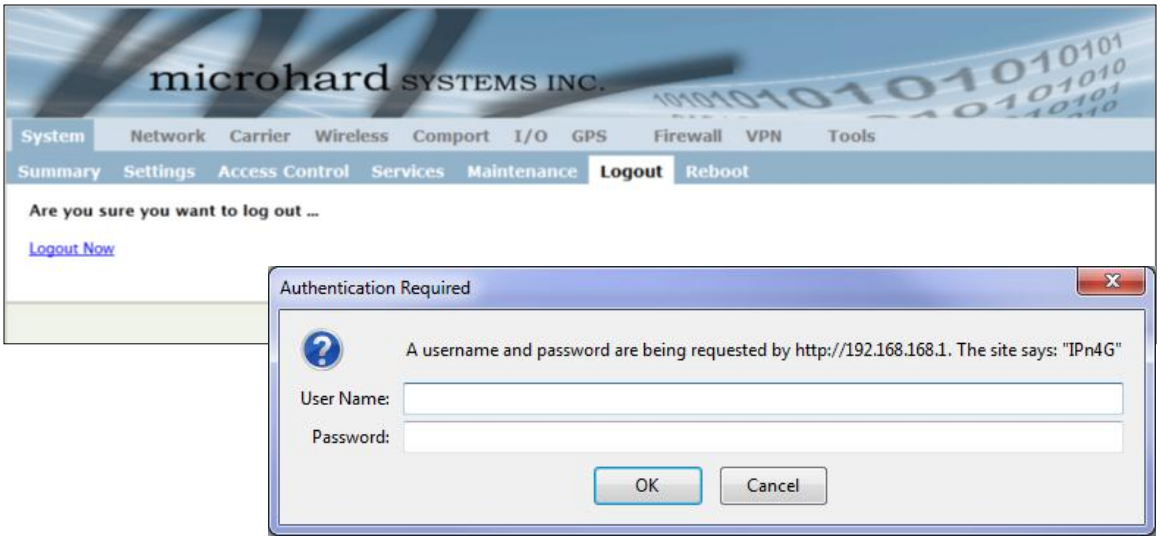


Image 4-1-10: System > logout

4.0 Configuration

4.1.7 System > Reboot

The IPn4G can be remotely rebooted using the System > Reboot menu. As seen below a button 'OK, reboot now' is provided. Once pressed, the unit immediately reboots and starts its boot up procedure.

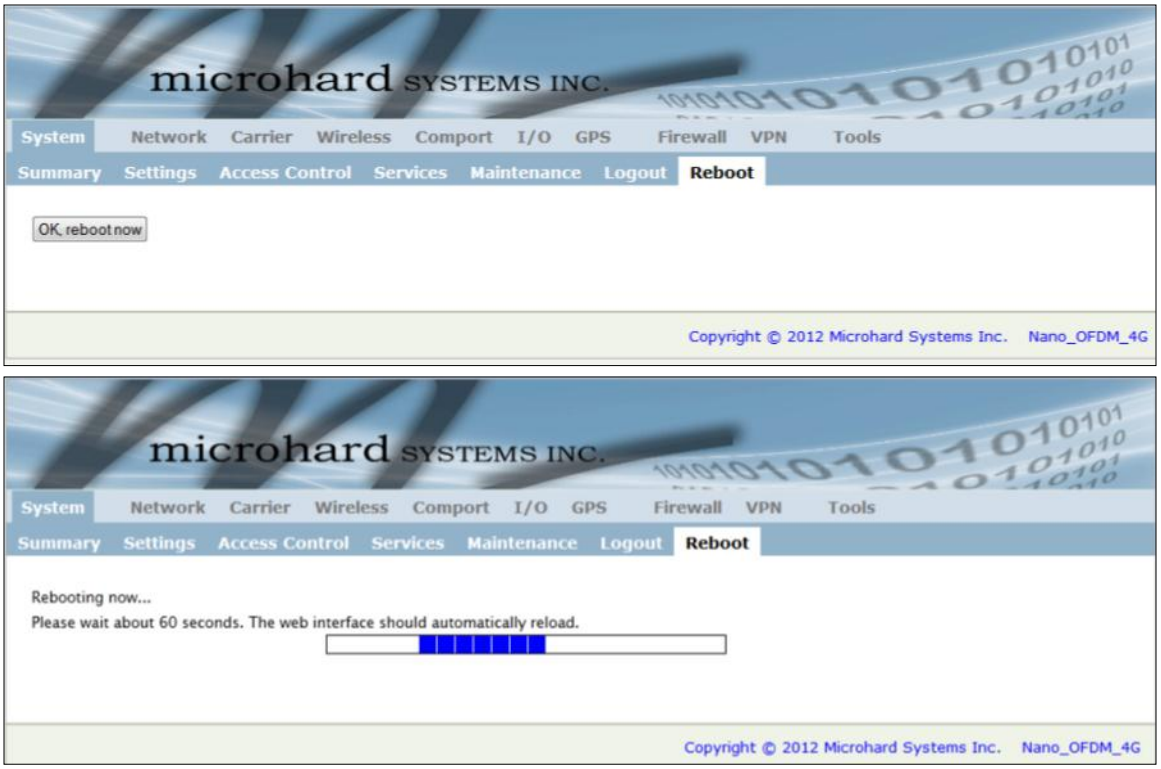


Image 4-1-11: System > Reboot

4.0 Configuration

4.2 Network

4.2.1 Network > Status

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

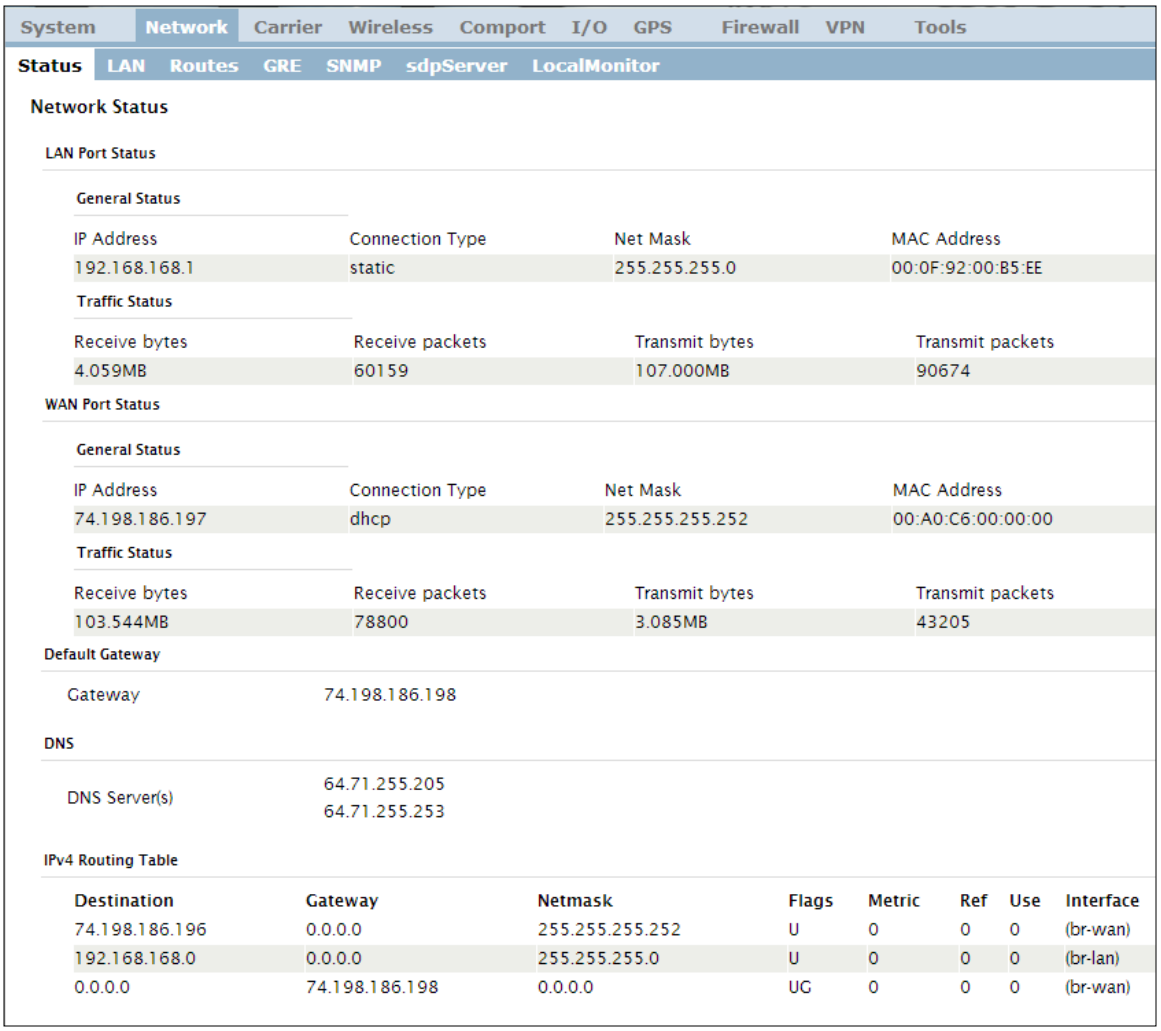


Image 4-2-1: Network > Network Status

4.0 Configuration

4.2.2 Network > LAN

Network LAN Configuration

The Ethernet port (RJ45) on the back of the IPn4G is the LAN port, used for connection of devices on a local network. By default, this port has a static IP Address of 192.168.168.1. It also, by default is running a DHCP server to provide IP Addresses to devices that are connected to the physical port, and devices connected by a WiFi connection (if equipped).

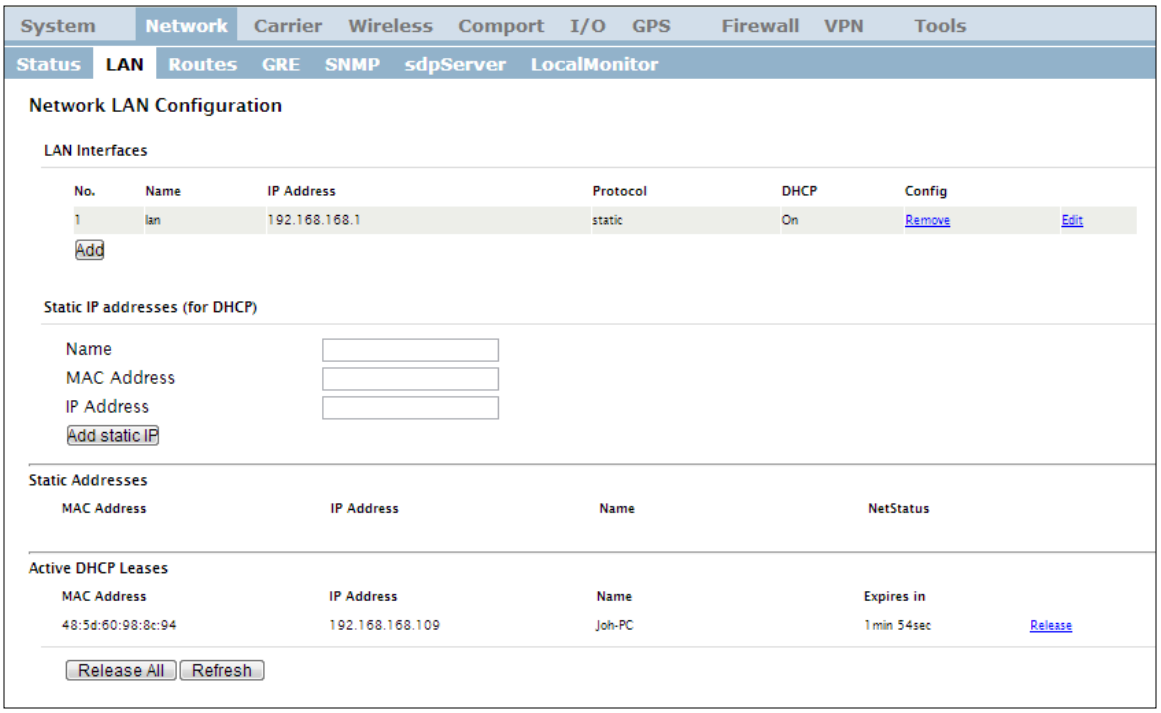


Image 4-2-2: Network > LAN

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

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

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

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

LAN Add/Edit Interface

The IPn4G has the capability to have multiple SSID's for the WiFi radio (optional). New Interfaces can be added for additional SSID's, providing, if required, separate subnets for each SSID. By default any additional interfaces added will automatically assign IP addresses to connecting devices via DHCP. Additional interfaces can only be used by additional WIFI SSID's (virtual interfaces).

Image 4-2-3: Network > Add/Edit LAN Interface

4.0 Configuration

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

Spanning Tree (STP)

Spanning Tree (STP) is used by default to detect and prevent any loops from occurring.

Values (selection)

On
Off

Connection Type

This selection determines if the IPn4G will obtain an IP address from a DHCP server on the attached network, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

Values (selection)

DHCP
Static

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.

IP Address

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

Values (IP Address)

192.168.168.1

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.

Netmask

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

Values (IP Address)

255.255.255.0

Default Gateway

If the IPn4G is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

Values (IP Address)

(no default)

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

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

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

LAN DNS Servers

DNS (Domain Name Service) Servers are used to resolve domain names into IP addresses. If the Connection Type is set for DHCP the DHCP server will populate this field and the value set can be viewed on the Network > Status page.

Values (IP Address)

(no default)

4.0 Configuration

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

LAN DHCP

A IPn4G may be configured to provide dynamic host control protocol (DHCP) service to all attached (either wired or wireless (WiFi)-connected) devices. By default the DHCP service is enabled, so devices that are connected to the physical Ethernet LAN ports, as well as any devices that are connected by WiFi will be assigned an IP by the IPn4G. The LAN DHCP service is available for each interface, and is located in the add/edit interface menus.

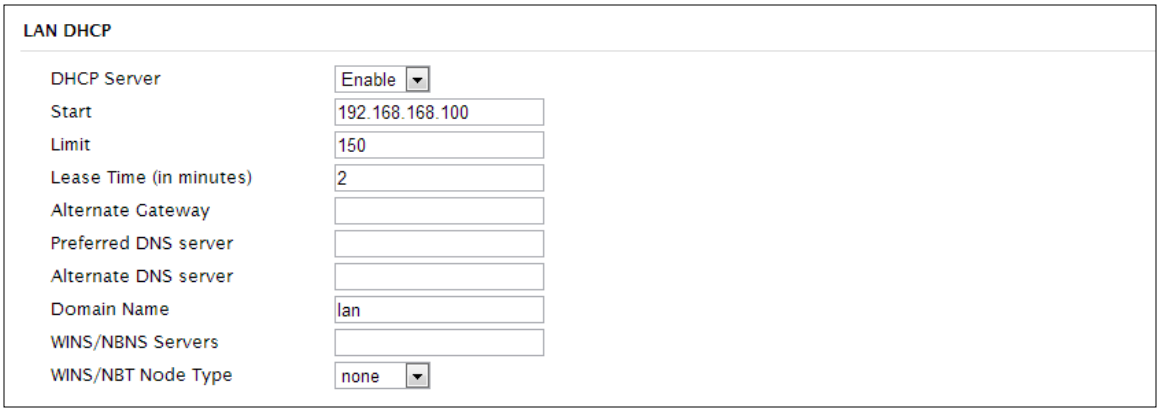


Image 4-2-4: Network > Add/Edit Interface DHCP

DHCP

The option is used to enable or disable the DHCP service for devices connected to the LAN Port and devices connected through a Wireless connection. This includes VIP connected as clients and other wireless devices such as 802.11 connections.

Values (selection)

On / Off

Start

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

Values (IP Address)

192.168.168.100

Limit

Set the maximum number of IP addresses that can be assigned by the IPn4G.

Values (integer)

150

Lease Time

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

Values (minutes)

(minutes)

4.0 Configuration

Alternate Gateway	
Specify an alternate gateway for DHCP assigned devices if the default gateway is not to be used.	**Values (IP Address)** *(IP Address)*

Preferred DNS Server	
Specify a preferred DNS server address to be assigned to DHCP devices.	**Values (IP Address)** *(IP Address)*

Alternate DNS Server	
Specify the alternate DNS server address to be assigned to DHCP devices.	**Values (IP Address)** *(IP Address)*

Domain Name	
Enter the Domain Name for the DHCP devices.	**Values (string)** *(IP Address)*

WINS/NBNS Servers	
Enter the address of the WINS/NBNS (NetBIOS) Server. The WINS server will translate computers names into their IP addresses, similar to how a DNS server translates domain names to IP addresses.	**Values (IP/Domain)** *(no default)*

WINS/NBT Node Type	
Select the method used to resolve computer names to IP addresses. Four name resolution methods are available: B-node: broadcast P-node: point-to-point M-node: mixed/modified H-node: hybrid	**Values (selection)** **none** b-node p-node m-node h-node

4.0 Configuration

Static IP Addresses (for DHCP)

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

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

Name	
The name field is used to give the device a easily recognizable name.	**Values (characters)** *(no default)*

MAC Address	
Enter in the MAC address of the device to be bound to a set IP address. Set the IP Address in the next field. Must use the format: AB:CD:DF:12:34:D3. It is not case sensitive, but the colons must be present.	**Values (MAC Address)** *(no default)*

IP Address	
Enter the IP Address to be assign to the device specified by the MAC address above.	**Values (IP Address)** *(minutes)*

Static Addresses

This section displays the IP address and MAC address currently assigned through the DCHP service, that are bound by it's MAC address. Also shown is the Name, and the ability to remove the binding by clicking "Remove _____".

Active DHCP Leases

This section displays the IP Addresses currently assigned through the DCHP service. Also shown is the MAC Address, Name and Expiry time of the lease for reference.

Using the "Release All" button, all DHCP leases are released and any connected devices must request new leases.

4.0 Configuration

4.2.3 Network > Routes

Static Routes Configuration

It may be desirable to have devices on different subnets to be able to talk to one another. This can be accomplished by specifying a static route, telling the IPn4G where to send data.

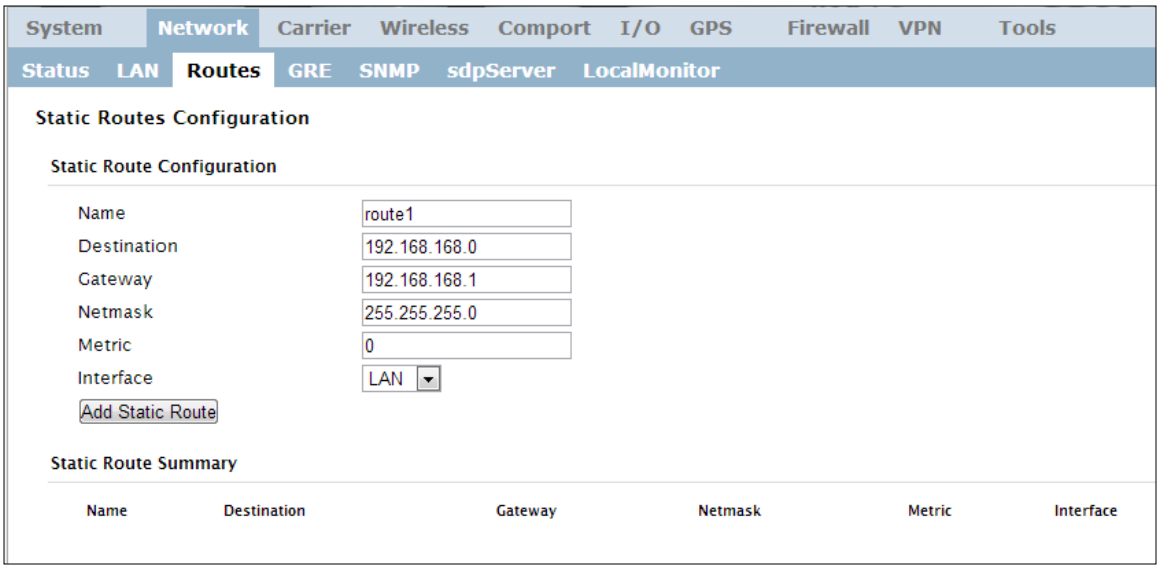


Image 4-2-6: Network > Routes

Name	
Routes can be names for easy reference, or to describe the route being added.	**Values (characters)** *(no default)*

Destination	
Enter the network IP address for the destination.	**Values (IP Address)** *(192.168.168.0)*

Gateway	
Specify the Gateway used to reach the network specified above.	**Values (IP Address)** **192.168.168.1**

Netmask	
Enter the Netmask for the destination network.	**Values (IP Address)** **255.255.255.0**

4.0 Configuration

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

Interface	
Define the exit interface. Is the destination a device on the LAN, or the WAN?	**Values (Selection)** **LAN** WAN None

4.0 Configuration

4.2.4 Network > GRE

GRE Configuration

The IPn4G supports GRE (Generic Routing Encapsulation) Tunneling which can encapsulate a wide variety of network layer protocols not supported by traditional VPN. This allows IP packets to travel from one side of a GRE tunnel to the other without being parsed or treated like IP packets.

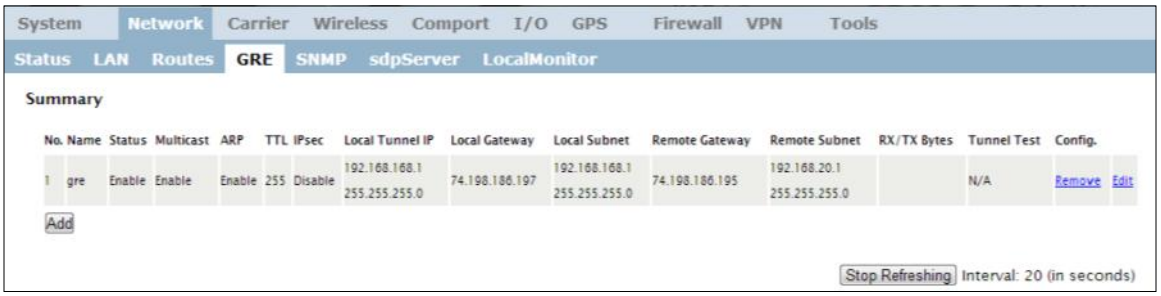


Image 4-2-7: Network > GRE Summary

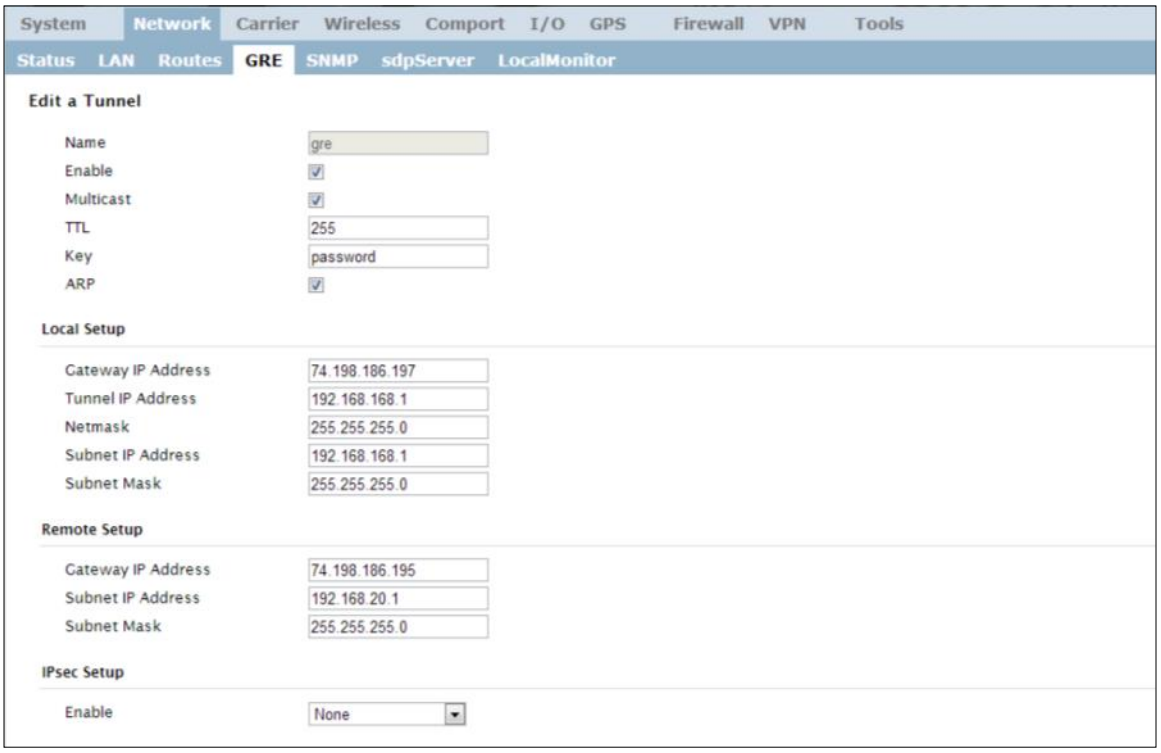


Image 4-2-8: Network > Edit/Add GRE Tunnel

	Name
Each GRE tunnel must have a unique name. Up to 10 GRE tunnels are supported by the IPn4G.	**Values (Chars(32))** *gre*

4.0 Configuration

Enable	
Enable / Disable the GRE Tunnel.	**Values (selection)** Disable / **Enable**

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

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

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

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

Local Setup

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

Gateway IP Address	
This is the WAN IP Address of the IPn4G, this field should be populated with the current WAN IP address.	**Values (IP Address)** *(varies)*

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

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

4.0 Configuration

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

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

Remote Setup

The remote setup tells the IPn4G about the remote end, the IP address to create the tunnel to, and the subnet that is accessible on the remote side of the tunnel.

Gateway IP Address	
Enter the WAN IP Address of the IPn4G or other GRE supported device in which a tunnel is to be created with at the remote end.	**Values (IP Address)** *(varies)*

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

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

IPsec Setup

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

4.0 Configuration

4.2.5 Network > SNMP

The IPn4G may be configured to operate as a Simple Network Management Protocol (SNMP) agent. Network management is most important in larger networks, so as to be able to manage resources and measure performance. SNMP may be used in several ways:

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

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

Managed networked devices are referred to as SNMP agents.

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the IPn4G. 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 IPn4G are hosted under private enterprise number **21703**.

An object is a variable in the device and is defined by a Management Information Database (MIB). Both the management system and the device have a copy of the MIB. The MIB in the management system provides for identification and processing of the information sent by a device (either responses to queries or device-sourced traps). The MIB in the device relates subroutine addresses to objects in order to read data from, or write data to, variables in the device.

An SNMPv1 agent accepts commands to retrieve an object, retrieve the next object, set and object to a specified value, send a value in response to a received command, and send a value in response to an event (trap).

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

SNMPv3 adds strong security features including encryption; a shared password key is utilized. Secure device monitoring over the Internet is possible. In addition to the commands noted as supported above, there is a command to synchronize with a remote management station.

The pages that follow describe the different fields required to set up SNMP on the IPn4G. MIBS may be requested from Microhard Systems Inc.

The MIB file can be downloaded directly from the unit using the ***'Get MIB File'*** button on the Network > SNMP menu.

4.0 Configuration

SNMP Settings

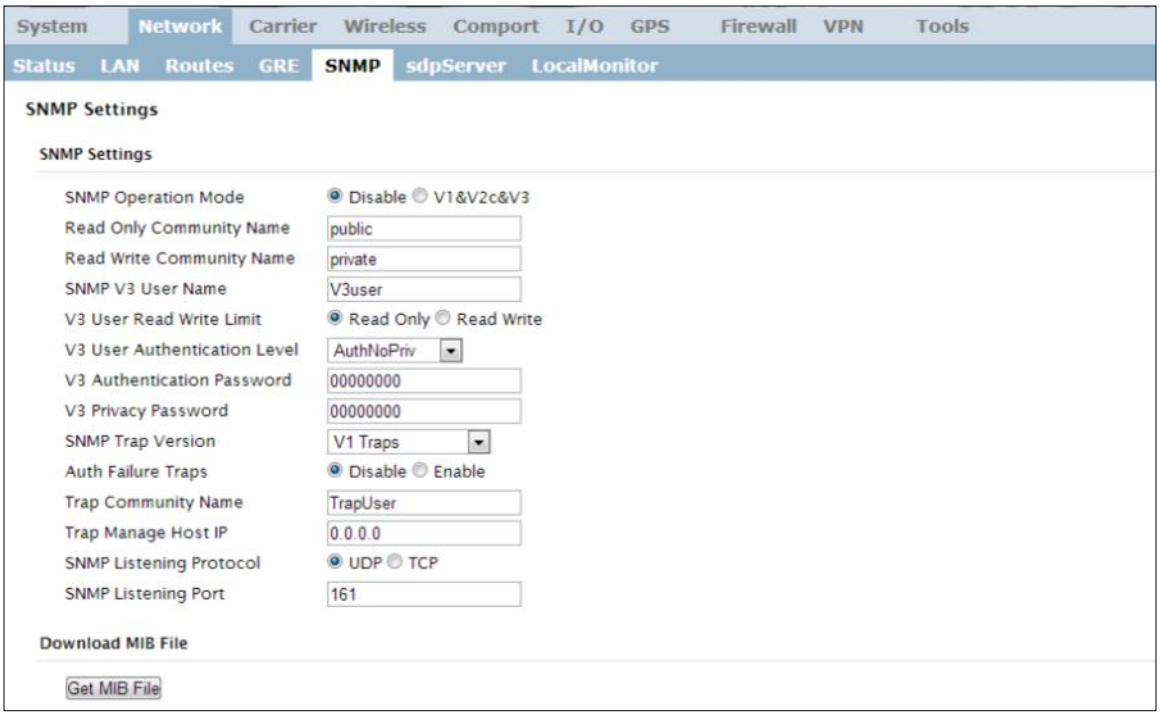


Image 4-2-9: Network > SNMP

SNMP Operation Mode	
If disabled, an SNMP service is not provided from the device. Enabled, the device - now an SNMP agent - can support SNMPv1, v2, & v3.	**Values (selection)** **Disable /** V1&V2c&V3

Read Only Community Name	
Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ priority.	**Values (string)** **public**

Read Only Community Name	
Also a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ/WRITE priority.	**Values (string)** **private**

SNMP V3 User Name	
Defines the user name for SNMPv3.	**Values (string)** **V3user**

4.0 Configuration

V3 User Read Write Limit	
Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.	**Values (selection)** **Read Only /** Read Write

V3 User Authentication Level	
Defines SNMPv3 user's authentication level: NoAuthNoPriv: No authentication, no encryption. AuthNoPriv: Authentication, no encryption. AuthPriv: Authentication, encryption.	**Values (selection)** **NoAuthNoPriv** AuthNoPriv AuthPriv

V3 User Authentication Password	
SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv.	**Values (string)** **00000000**

V3 User Privacy Password	
SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).	**Values (string)** **00000000**

SNMP Trap Version	
Select which version of trap will be sent should a failure or alarm condition occur.	**Values (string)** **V1 Traps** V2 Traps V3 Traps V1&V2 Traps V1&V2&V3 Traps

Auth Failure Traps	
If enabled, an authentication failure trap will be generated upon authentication failure.	**Values (selection)** **Disable** / Enable

Trap Community Name	
The community name which may receive traps.	**Values (string)** **TrapUser**

Trap Manage Host IP	
Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address).	**Values (IP Address)** **0.0.0.0**

4.0 Configuration

4.2.6 Network > sdpServer

sdpServer Settings

Microhard Radio employ a discovery service that can be used to detect other Microhard Radio's on a network. This can be done using a stand alone utility from Microhard System's called 'IP Discovery' or from the Tools > Discovery menu. The discovery service will report the MAC Address, IP Address, Description, Product Name, Firmware Version, Operating Mode, and the SSID.

Image 4-2-10: Network > sdpServer Settings

Discovery Service Status	
Use this option to disable or enable the discovery service.	**Values (selection)** Disable / **Discoverable** / Changable

Server Port Settings	
Specify the port running the discovery service on the IPn4G unit.	**Values (Port #)** 20097

4.0 Configuration

4.2.7 Network > Local Monitor

The Local Device Monitor allows the IPn4G to monitor a local device connected locally to the Ethernet port or to the locally attached network. If the IPn4G cannot detect the specified IP or a DHCP assigned IP, the unit will restart the DHCP service, and eventually restart the modem to attempt to recover the connection.

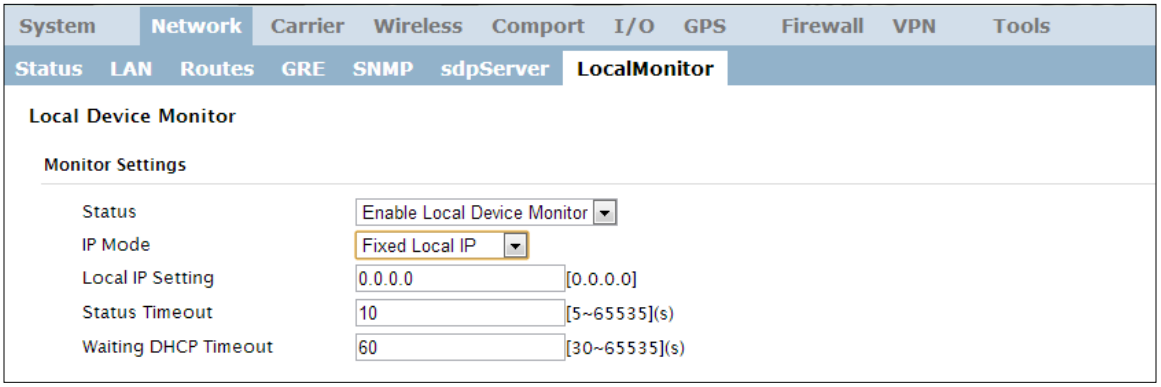


Image 4-2-11: Network Configuration , Local Monitor

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 IPn4G will detect and monitor DHCP assigned IP address.	**Values (selection)** **Fixed local IP** Auto Detected IP

Local IP Setting	
This field is only shown if Fixed Local IP is selected for the IP Mode. Enter the static IP to be monitored in this field.	**Values (IP)** **0.0.0.0**

Status Timeout	
The status timeout is the maximum time the IPn4G will wait to detect the monitored device. At this time the IPn4G will restart the DHCP service. (5-65535 seconds)	**Values (seconds)** **10**

Waiting DHCP Timeout	
This field defines the amount of time the IPn4G will wait to detect the monitored device before it will reboot the modem. (30-65535 seconds)	**Values (seconds)** **60**

4.0 Configuration

4.3 Carrier

4.3.1 Carrier > Status

The Carrier Status window provides complete overview information related to the Cellular Carrier portion of the IPn4G. A variety of information can be found here, such as Activity Status, Network (Name of Wireless Carrier connected) , Data Service Type(WCDMA/HSPA/HSPA+/LTE etc), Frequency band, Phone Number etc.

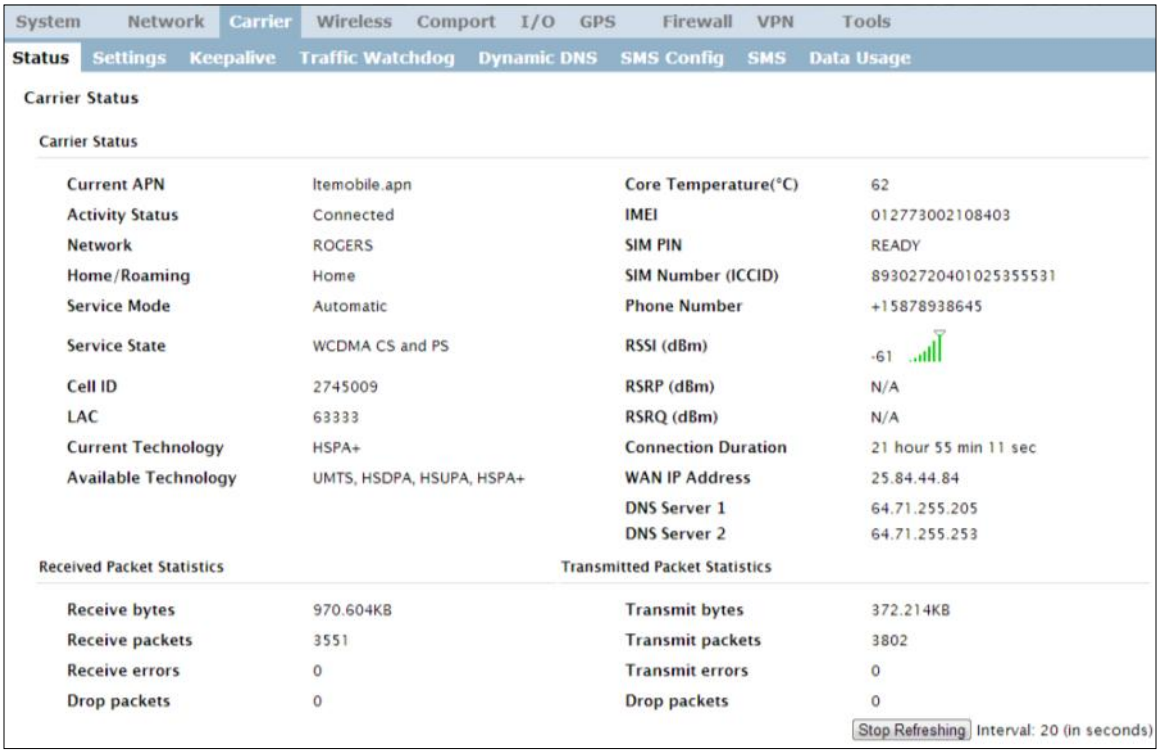


Image 4-3-1: Carrier > Status

Not all statistics parameters displayed are applicable.

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

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

4.0 Configuration

4.3 Carrier

4.3.2 Carrier > Settings

The parameters within the Carrier Configuration menu must be input properly; they are the most basic requirement required by your cellular provider for network connectivity.

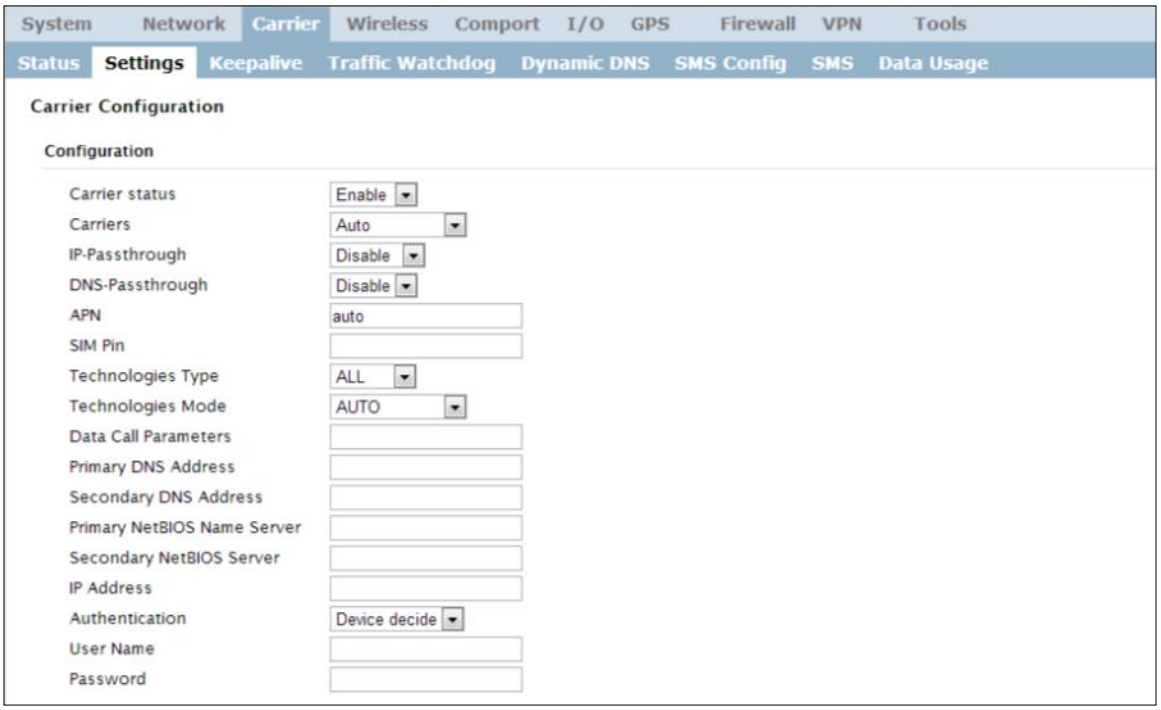


Image 4-3-2: Carrier > Settings

Carrier Status	
Carrier Status is used to Enable or Disable the connection to the Cellular Carrier. By default this option is enabled.	**Values (Selection)** **Enable** / Disable

Carriers	
In some cases, a user may want to lock onto certain carrier to avoid data roaming. There were four options presented to a user to choose from, Auto, SIM based, Scan & Select and Fixed. • Auto will allow the IPn4G to pick the carrier automatically. Data roaming is permitted. • SIM based will only allow the IPn4G to connect to the network indicated by the SIM card used in the unit. • Manual will scan for available carriers and allow a user to select from the available carriers. It takes 2 to 3 minutes to complete a scan. • Fixed allows a user to enter the carrier code (numerical) directly and then the IPn4G will only connect to that carrier.	**Values (Selection)** **Auto** Based on SIM Manual Fixed

4.0 Configuration

IP-Passthrough

IP pass-through allows the WAN IP address to be assigned to the device connected to the LAN. In this mode the IPn4G is for the most part transparent and forwards all traffic to the device connected to the Ethernet port except that listed below:

- The WebUI port (*Default Port:TCP 80*), this port is retained for remote management of the IPn4G. This port can be changed to a different port under the **System > Settings** Menu.
- The SNMP Listening Port (*Default Port: UDP 161*).

Values (Selection)

Disable / Ethernet

DNS-Passthrough

When enabled DNS-Passthrough will pass on the WAN assigned DNS information to the end device.

Values (Selection)

Enable / **Disable**

APN (Access Point Name)

The APN is required by every Carrier in order to connect to their networks. The APN defines the type of network the IPn4G is connected to and the service type. Most Carriers have more than one APN, usually many, dependant on the types of service offered.

Values (characters)

auto

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

SIM Pin

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

Values (characters)

(none)

Technologies Type

Set to ALL by default, the Technologies field allows the selection of 3GPP technologies (LTE), and or 3GPP2 technology (CDMA).

Values (Selection)

ALL / 3GPP / 3GPP2

Technologies Mode

The Technologies Mode option allows a user the ability to specify what type of Cellular networks to connect to.

Values (Selection)

AUTO / LTE Only / WCDMA Only / GSM Only

Data Call Parameters

Sets the modems connect string if required by the carrier. Not usually required in North America.

Values (string)

(none)

4.0 Configuration

Primary DNS Address	
If let blank the IPn4G with use the DNS server as specified automatically by the service provider.	**Values (IP Address)** *(none)*

Secondary DNS Address	
If let blank the IPn4G with use the DNS server as specified automatically by the service provider.	**Values (IP Address)** *(none)*

Primary NetBIOS Name Server	
Enter the Primary NetBIOS Name Server if required by the carrier.	**Values (IP Address)** *(none)*

Secondary NetBIOS Name Server	
Enter the Secondary NetBIOS Name Server if required by the carrier.	**Values (IP Address)** *(none)*

IP Address	
In some cases the Static IP address must be entered in this field if assigned by a wireless carrier. In most cases the IP will be read from the SIM card and this field should be left at the default value.	**Values (IP Address)** *(none)*

Authentication	
Sets the authentication type required to negotiate with peer. PAP - Password Authentication Protocol. CHAP - Challenge Handshake Authentication Protocol.	**Values (Selection)** **Device decide (AUTO)** PAP CHAP

User Name	
A User Name may be required for authentication to a remote peer. Although usually not required for dynamically assigned IP addresses from the wireless carrier, but required in most cases for static IP addresses. Varies by carrier.	**Values (characters)** Carrier/peer dependant

Password	
Enter the password for the user name above. May not be required by some carriers, or APN's	**Values (characters)** Carrier/peer dependant

4.0 Configuration

4.3 Carrier

4.3.3 Carrier > Keepalive

The Keep alive tab allows for the configuration of the keep alive features of the IPn4G. The IPn4G can either do a ICMP or HTTP keep alive by attempting to reach a specified address at a regular interval. If the IPn4G cannot reach the intended destination, it will reset the unit in an attempt to obtain a new connection to the carrier.

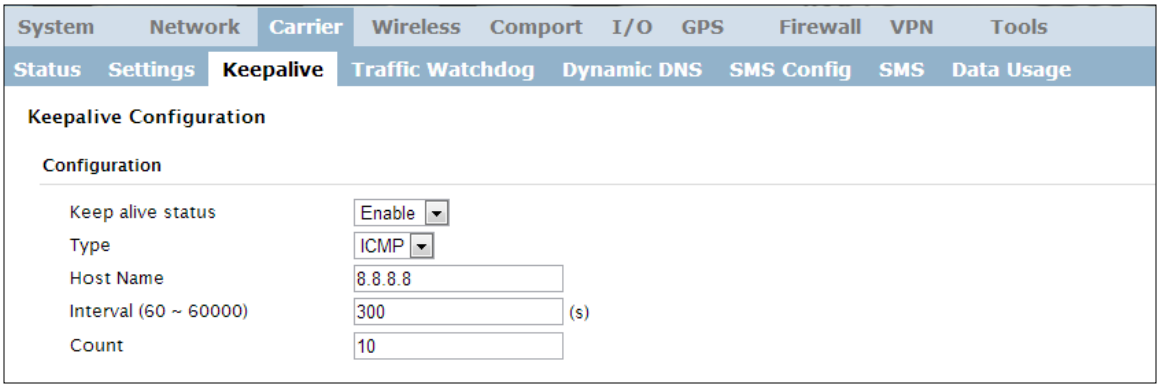


Image 4-3-3: Carrier > Keepalive

Keep Alive Status	
Enable or Disable the keep alive functions in the IPn4G.	**Values (Selection)** **Enable** / Disable

Type	
Select the type of keep alive used. ICMP uses a “ping” to reach a select destination.	**Values (Selection)** **ICMP** / HTTP

Host Name	
Specify a IP Address or Domain that is used to test the IPn4G connection.	**Values (IP or Domain)** **8.8.8.8**

Interval	
The Interval value determines the frequency, or how often, the IPn4G will send out PING messages to the Host.	**Values (seconds)** **300**

Count	
The ***Count*** field is the maximum number of PING errors such as “Host unreachable” the IPn4G 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 (number)** **10**

4.0 Configuration

4.3 Carrier

4.3.4 Carrier > Traffic Watchdog

The Wireless Traffic Watchdog will detect if there has been no wireless traffic, or communication with the Cellular carrier for a configurable amount of time. Once that time has elapsed, the unit will reset, and attempt to re-establish communication with the cellular carrier.

Image 4-3-4: Carrier > Traffic Watchdog

Traffic Watchdog	
Enable or Disable the Traffic Watchdog.	**Values (Selection)** **Enable** / Disable

Check Interval	
The Check Interval tells the IPn4G how often (in seconds) to check for wireless traffic to the cellular carrier. (1-60000 seconds)	**Values (seconds)** **1**

Reboot Time Limit	
The Reboot Timer will reset the unit if there has been no Cellular RF activity in the configured time. (300 –60000 seconds)	**Values (seconds)** **600**

4.0 Configuration

4.3 Carrier

4.3.5 Carrier > Dynamic DNS

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 IPn4G.

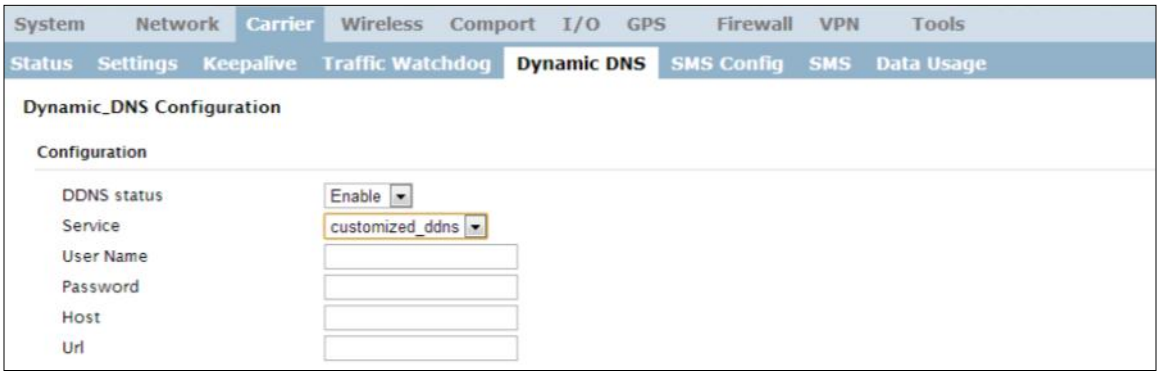


Image 4-3-5: Carrier > Traffic Watchdog

DDNS Status	
This selection allows the use of a Dynamic Domain Name Server (DDNS), for the IPn4G.	**Values (Selection)** **Enable** / Disable

Service	
This is a list of supported Dynamic DNS service providers. Free and premium services are offered, contact the specific providers for more information.	**Values (selection)** **changeip** ods dyndns ovh eurodyndns regfish hn tzo noip zoneedit

User Name	
Enter a valid user name for the DDNS service selected above.	**Values (characters)** *(none)*

Password	
Enter a valid password for the user name of the DDNS service selected above.	**Values (characters)** *(none)*

Host	
This is the host or domain name for the IPn4G as assigned by the DDNS provider.	**Values (domain name)** *(none)*

4.0 Configuration

4.3 Carrier

4.3.6 Carrier > SMS Config

SMS messages can be used to remotely reboot or trigger events in the IPn4G. SMS alerts can be set up to get SMS messages based on system events such as Roaming status, RSSI, Ethernet Link Status or IO Status.

System SMS Command

Image 4-3-6: SMS > SMS Configuration

Status

This option allows a user to enable or disable to use of the following SMS commands to reboot or trigger events in the IPn4G:

Values (Selection)

Enable / Disable

MSC#REBOOT Reboot system
MSC#NMS Send NMS UDP Report
MSC#WEB Send web client inquiry
MSC#MIOP1 open I/O ouput1
MSC#MIOP2 open I/O ouput2
MSC#MIOP3 open I/O ouput3
MSC#MIOP4 open I/O ouput4
MSC#MIOC1 close I/O ouput1
MSC#MIOC2 close I/O ouput2
MSC#MIOC3 close I/O ouput3
MSC#MIOC4 close I/O ouput4

MSC#EURD0 trigger event report0
MSC#EURD1 trigger event report1
MSC#EURD2 trigger event report2
MSC#EURD3 trigger event report3
MSC#GPSR0 trigger gps report0
MSC#GPSR1 trigger gps report1
MSC#GPSR2 trigger gps report2
MSC#GPSR3 trigger gps report3

SMS Commands are case sensitive.

Set Phone Filter

If enabled, the IPn4G will only accept and execute commands originating from the phone numbers in the Phone Filter List. Up to 6 numbers can be added.

Values (Selection)

Enable / **Disable**

4.0 Configuration

System SMS Alerts

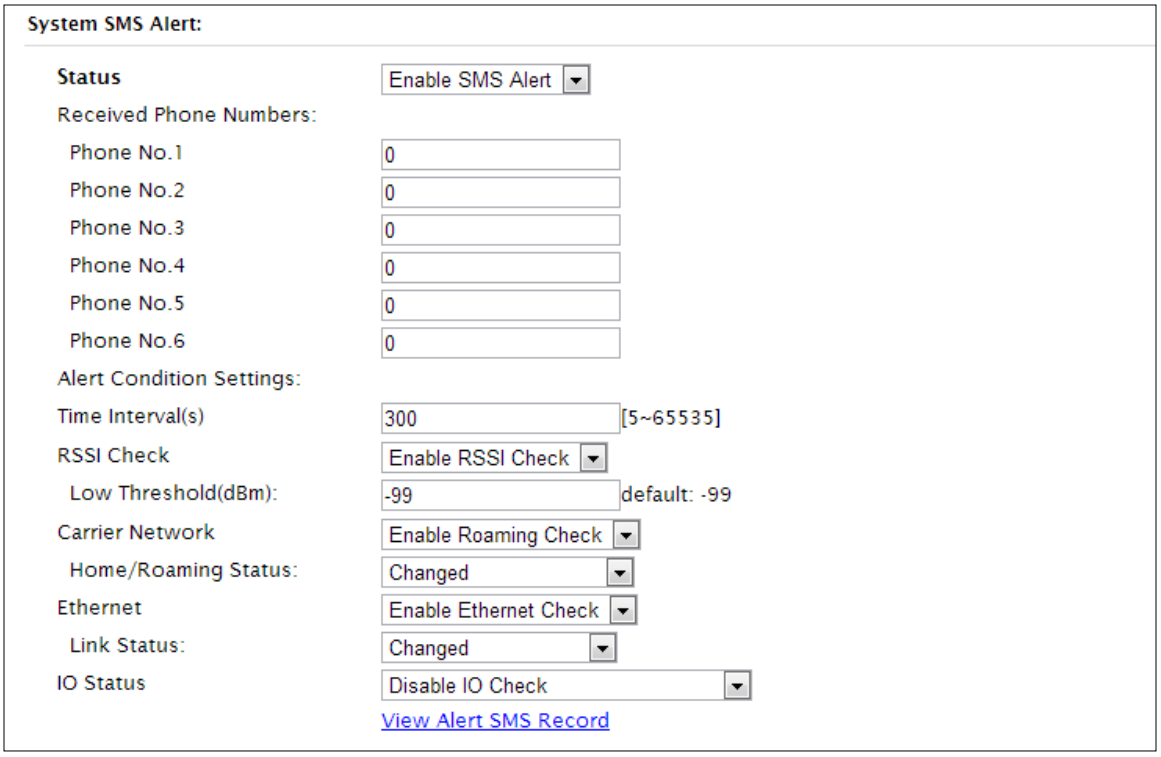


Image 4-3-7: SMS > SMS Alerts

Status

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

Values (Selection)

Enable / **Disable**

Received Phone Numbers

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

Values (Selection)

(no default)

Time Interval(s)

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

Values (Seconds)

300

RSSI Check

Enable or disable the RSSI alerts.

Values (Selection)

Disable RSSI check
Enable RSSI check

4.0 Configuration

RSSI Check	
Set the threshold for RSSI alerts.	**Values (dBm)** -99

Carrier Network	
Enable or disable SMS Alerts for Roaming Status.	**Values (Selection)** Disable Roaming Check Enable Roaming Check

Home / Roaming Status	
The IPn4G can send alerts based on the roaming status. Data rates during roaming can be expensive and it is important to know when a device has started roaming.	**Values (Selection)** In Roaming Changed or In Roaming Changed to Roaming

Ethernet	
Enable or disable SMS Alerts for the Ethernet Link status of the LAN RJ45 port.	**Values (Selection)** Disable Ethernet check Enable Ethernet check

Ethernet Link Status	
The status of the Ethernet Link of the LAN (RJ45) can be used to send SMS Alerts. The link status may indicate an issue with the connected device.	**Values (Selection)** Changed In no-link Changed or in no-link Changed to no-link

I/O Status	
SMS Alerts can be sent based on the state changes of the Digital I/O lines.	**Values (Selection)** Disable IO Check Enable: INPUT Changed Enable: Output Changed Enable: INPUT or OUTPUT Changed.

4.0 Configuration

4.3 Carrier

4.3.7 Carrier > SMS

SMS Command History

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

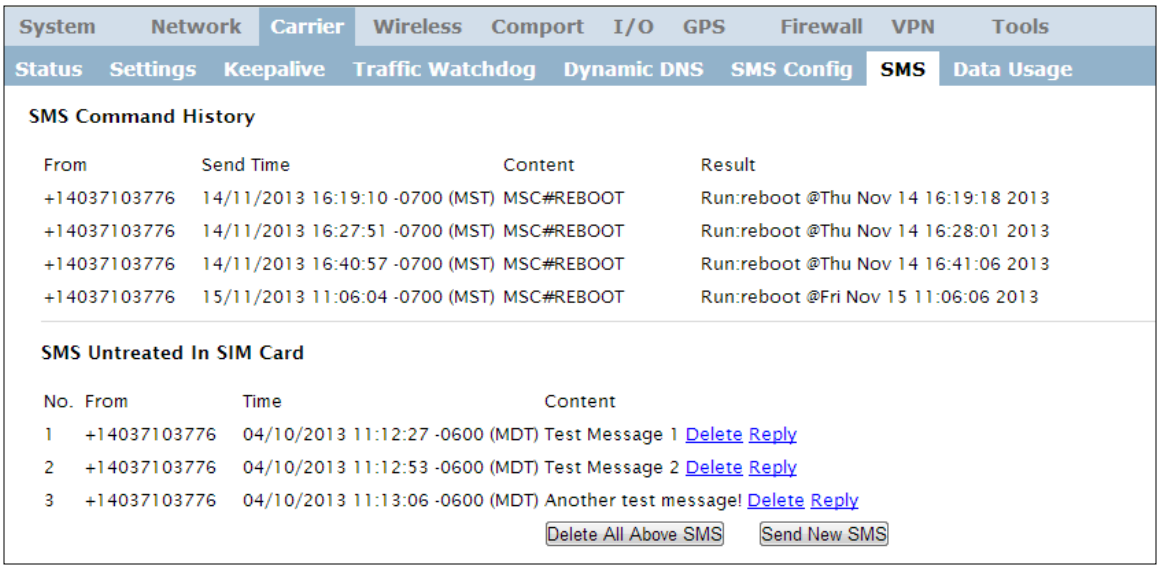


Image 4-3-8: SMS > SMS Command History

Send SMS Message

The SMS messages can be sent directly from the IPn4G WebUI interface. Also, the SMS message history can be viewed.

Image 4-3-9: SMS > SMS Send

4.0 Configuration

4.3.8 Carrier > Data Usage

The Data Usage tool on the IPn4G 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 IPn4G.

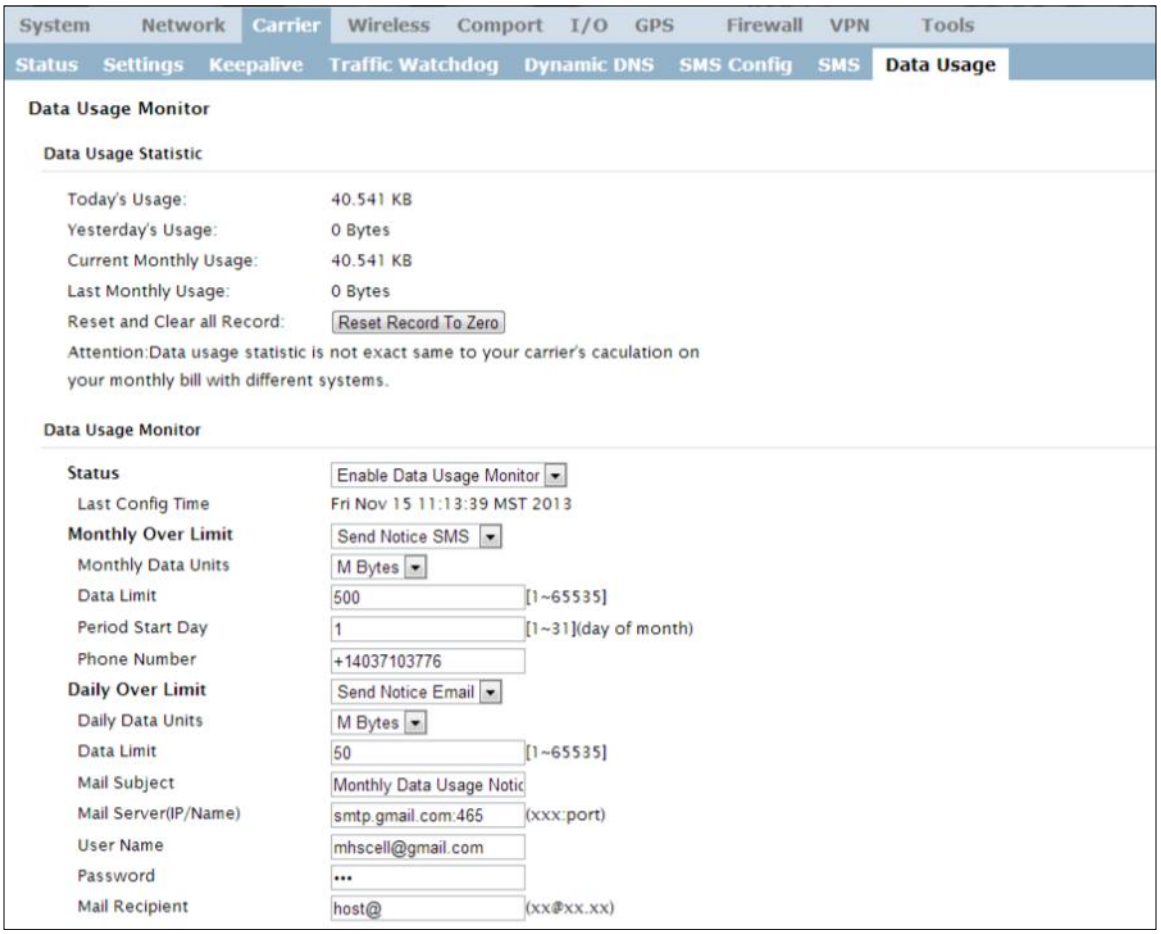


Image 4-3-10: Carrier > Data Usage

Status	Values (selection)
If enabled the IPn4G will track the amount of cellular data consumed. If disabled, data is not recorded, even in the Current Data Usage display.	**Disable** Enable

4.0 Configuration

Monthly/Daily Over Limit

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

Values (selection)

None
Send Notice SMS
Send Notice Email

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

Image 4-3-11: 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 IPn4G 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 Units	M Bytes	
Data Limit	50	[1~65535]
Mail Subject	Monthly Data Usage Notic	
Mail Server(IP/Name)	smtp.gmail.com:465	(xxx:port)
User Name	mhscell@gmail.com	
Password	•••	
Mail Recipient	host@	(xx@xx.xx)

Image 4-3-12: Data Usage > Email Config

4.0 Configuration

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@**

4.0 Configuration

4.4 Wireless (WiFi)

4.4.1 Wireless > Status

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

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

Traffic Status shows statistics about the transmitted and received data.

The IPn4G shows information about all Wireless connections in the **Connection Status** section. The Wireless MAC address, Noise Floor, Signal to Noise ratio (SNR), Signal Strength (RSSI), The transmit and receive Client Connection Quality (CCQ), TX and RX data rates, and a graphical representation of the signal level or quality.

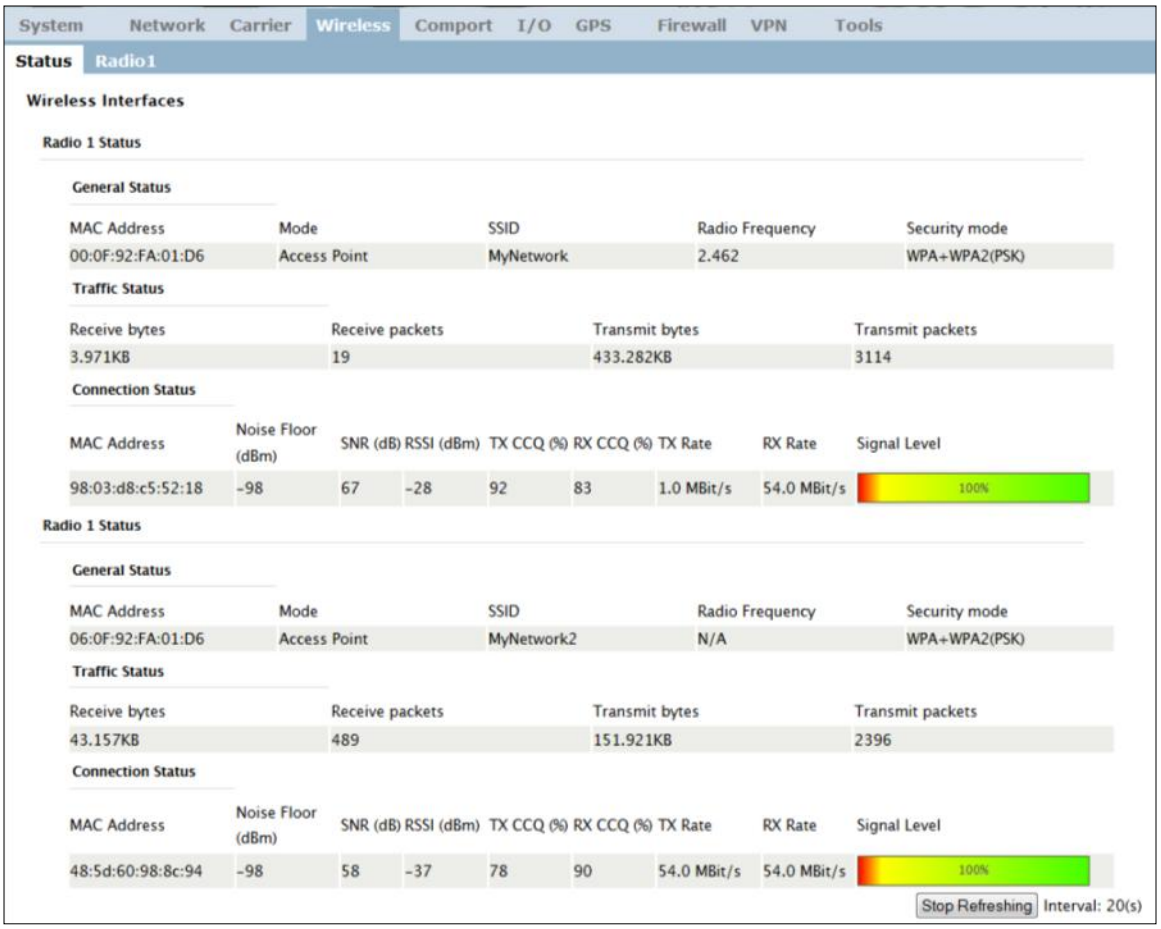


Image 4-4-1: Wireless > Status

4.0 Configuration

4.4.2 Wireless > Radio1

Radio1 Phy Configuration

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

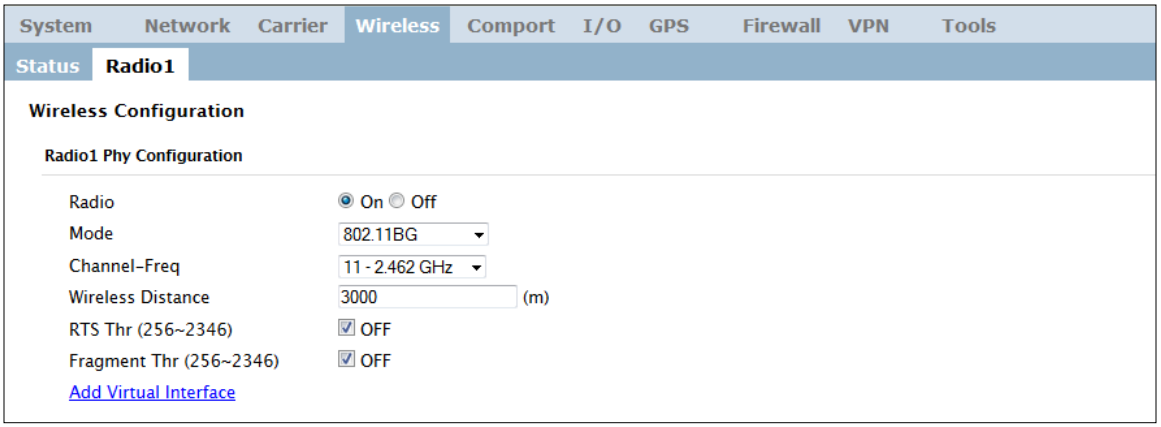


Image 4-4-2: Wireless > Radio Configuration

Radio

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

Values (selection)

On / Off

Mode

The Mode defines which wireless standard to use for the wireless network. The IPn4G supports 802.11b/g modes as seen here. Select the appropriate operating mode from the list.

Values (selection)

802.11B ONLY
802.11BG

Channel-Freq

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

2.4 GHz Channels

Auto
Channel 01 : 2.412 GHz
Channel 02 : 2.417 GHz
Channel 03 : 2.422 GHz
Channel 04 : 2.427 GHz
Channel 05 : 2.432 GHz
Channel 06 : 2.437 GHz
Channel 07 : 2.442 GHz
Channel 08 : 2.447 GHz
Channel 09 : 2.452 GHz
Channel 10 : 2.457 GHz
Channel 11 : 2.462 GHz
Channel 12 : 2.467 GHz

4.0 Configuration

Wireless Distance

The Wireless Distance parameter allows a user to set the expected distance the WiFi signal needs to travel. The default is 3km, so the IPn4G will assume that the signal may need to travel up to 3km so it sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced.

Values (meters)

3000

RTS Thr (256 ~ 2346)

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

Values (selection)

On / **OFF**

Fragment Thr (256 ~ 2346)

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

Values (selection)

On / **OFF**

Radio1 Virtual Interface

The bottom section of the Wireless Configuration provides for the configuration of the Operating Mode of the Wireless Interface, the TX power, Wireless Network information, and Wireless Encryption. The IPn4G can support multiple virtual interfaces. These interfaces provide different SSID's for different users, and can also be assigned to separate subnets (Network Interfaces) to prevent groups from interacting.

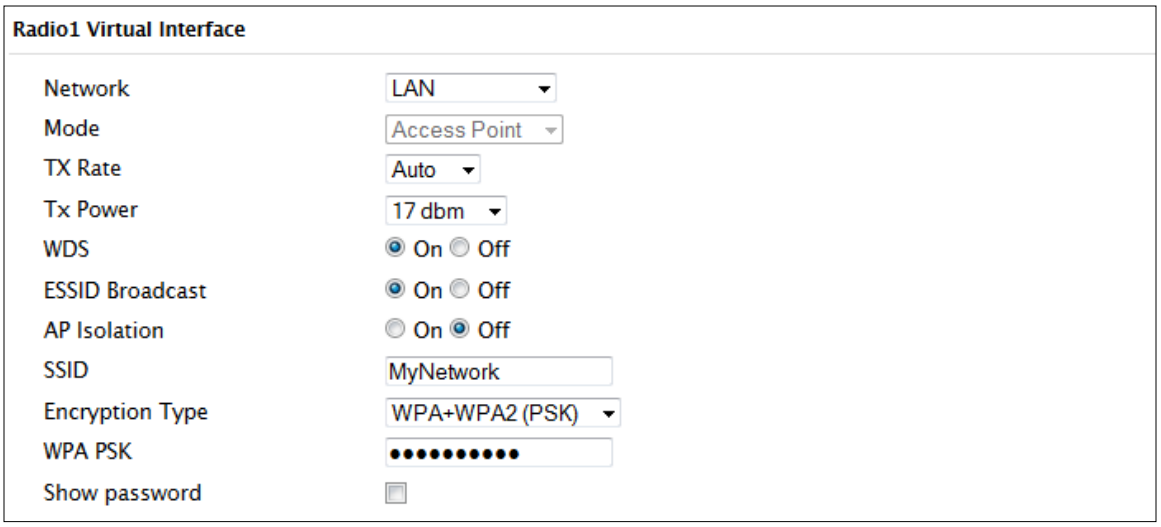


Image 4-4-3: Wireless > Radio1 Virtual Interface Configuration

4.0 Configuration

Network

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

Values (selection)

LAN
WAN
(Additional Interfaces…)

Mode

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

If more than 1 Virtual Interface (more than 1 SSID) has been defined, the IPn4G can **ONLY** operate as a Access Point, and will be locked into this mode.

Values (selection)

Access Point
Client
Repeater
Mesh Point

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

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

Mesh Point - Units can be configured as a Mesh "Node". When multiple units are configured as a Mesh node, they automatically establish a network between each other. SSID for each radio in a Mesh network must be the same.

TX Rate

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

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

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

802.11 b/g

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

4.0 Configuration

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

TX Power

This setting establishes the transmit power level which will be presented to the antenna connectors at the rear of the IPn4G. Unless required, the Tx Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

Values (selection)

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

WDS

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points. WDS preserves the MAC addresses of client frames across links between access points

Values (selection)

On / Off

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

ESSID Broadcast

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

Values (selection)

On / Off

AP Isolation

When AP Isolation is enabled wireless devices connected to this SSID will not be able to communicate with each other. In other words if the IPn4G is being used as a Hot Spot for many wireless clients, AP Isolation would provide security for those clients by not allowing access to any other wireless device.

Values (selection)

On / **Off**

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

SSID

All devices connecting to the IPn4G in a given network must use the SSID of the IPn4G. This unique network address is not only a security feature for a particular network, but also allows other networks - with their own unique network address - to operate in the same area without the possibility of undesired data exchange between networks.

Values (string)

wlan0

MESH ID

In Mesh Networks, this must be the same for all IPn4G, or VIP Series units participating, similar to the SSID for other wireless networks.

Values (string)

(no default)

4.0 Configuration

Encryption Type

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

Values (selection)

Disabled
WEP
WPA (PSK)
WPA2 (PSK)
WPA+WPA2 (PSK)

WEP: Wired Equivalency Privacy is a security protocol defined in 802.11b. It is commonly available for Wi-Fi networks and was intended to offer the equivalent security of a wired network, however, it has been found to be not as secure as desired.

Operating at the data link and physical layers, WEP does not provide complete end-to-end security.

WEP: Wired Equivalency Protocol (WEP) encryption adds some overhead to the data, thereby negatively effecting throughput to some degree.

The image below shows the associated configuration options:

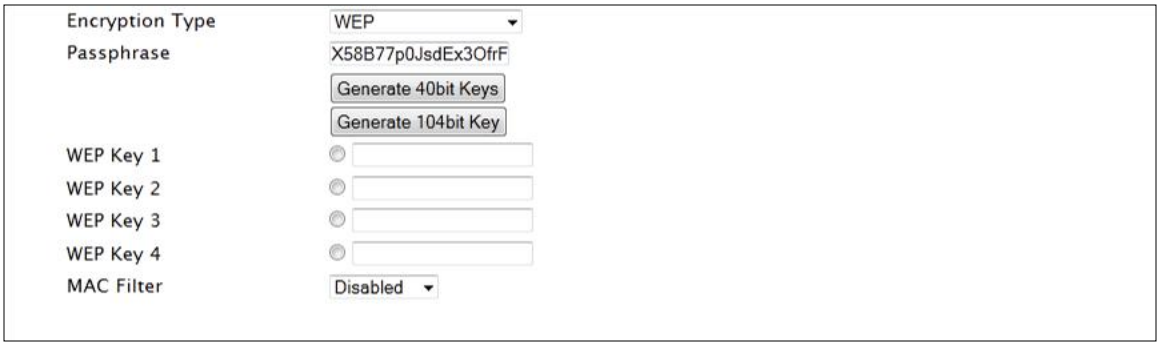


Image 4-4-4: Encryption Type > WEP

- Key Generation
  4 complex WEP keys may be generated based on the supplied Passphrase

  Procedure: Input a Key Phrase, select the type of Key to be generated using the Generate Key soft button.

  Using the same Passphrase on all IPn4G/VIP Series units within the network will generate the same Keys on all units. All units must operate with the same Key selected.

  Alternately, key phrases may be entered manually into each Key field.

WPA: Wi-Fi Protected Access (WPA/WPA2). It provides stronger security than WEP does. The configuration is essentially the same as for WEP (described above), without the option for automatic Key generation.

Show Password

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

Values (selection)

unchecked

4.0 Configuration

4.5 Comport

4.5.1 Comport > Status

The Status window gives a summary of the serial ports on the IPn4G. The Status window shows if the com port has been enabled, how it is configured (Connect As), and the connection status.

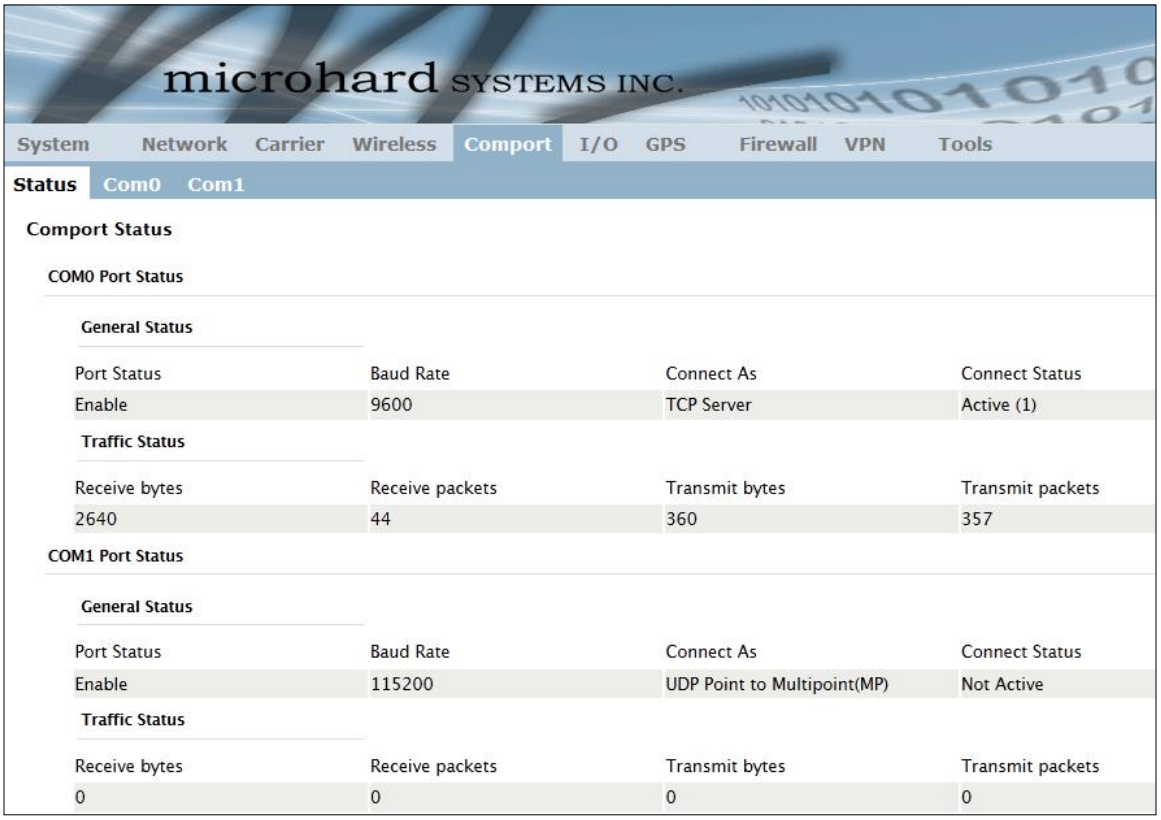


Image 4-5-1: Comport > Status

4.0 Configuration

4.5.2 Comport > COM0/1

This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the IPn4G network on another VIP Series' serial port. The fully-featured RS232 interface supports hardware handshaking.

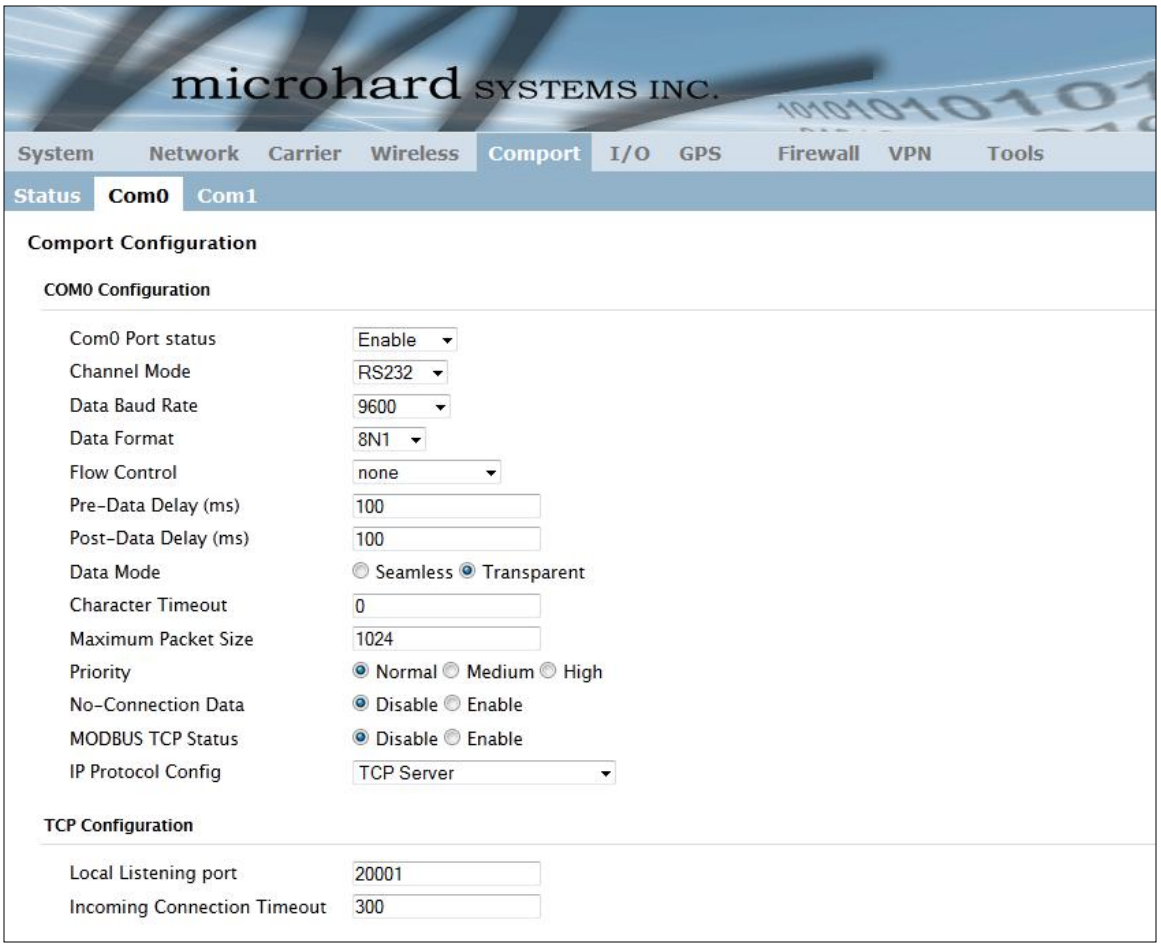


Image 4-5-2: Comport > Settings Configuration

4.0 Configuration

Com0/1 Port Status

Select operational status of the Com0/1 Serial Port. The port is disabled by default.

Values (selection)

Disabled / Enable

Channel Mode

Determines which serial interface shall be used to connect to external devices: RS232, RS485, or RS422. When an interface other than RS232 is selected, the DE9 port will be inactive.

Values (selection)

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.

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

Values (bps)

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

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.

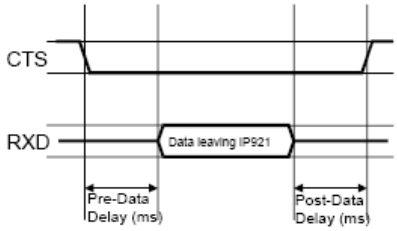
Software flow control (XON/XOFF) is not supported.

Values (selection)

8N1	7N2
8N2	7E1
8E1	7O1
8O1	7E2
7N1	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 IPn4G uses the CTS signal to gate the output data on the serial port.



Drawing 4A: CTS Output Data Framing

Values (selection)

None
Hardware
CTS Framing

4.0 Configuration

Pre-Data Delay

Refer to **Drawing 6A** on the preceding page.

Values (time (ms))

100

Post-Data Delay

Refer to **Drawing 6A** on the preceding page.

Values (time (ms))

100

Date Mode

This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the IPn4G.

Values (selection)

Seamless / **Transparent**

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

Character Timeout

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

Values (characters)

0

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 associated with the data traffic on the COM port.

Values (selection)

Normal / Medium / High

4.0 Configuration

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 (selection)** **Disable** / Enable

MODBUS TCP Protection Key	
MODBUS encryption key used for the MODBUS TCP Protection Status feature.	**Values (string)** **1234**

4.0 Configuration

IP Protocol Config

This setting determines which protocol the serial server will use to transmit serial port data over the IPn4G network.

The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the COM0/COM1 Configuration Menu.

Values (selection)

TCP Client
TCP Server
TCP Client/Server
UDP Point-to-Point
UDP Point-to-Multipoint (P)
UDP Point-to-Multipoint(MP)
UDP Multipoint-to-Multipoint
SMTP Client (COM0)
C12.22
GPS Transparent Mode

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

TCP Client: When TCP Client is selected and data is received on its serial port, the IPn4G 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 IPn4G 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: 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.

TCP Server: In this mode, the IPn4G Series will not INITIATE a session, rather, it will wait for a Client to request a session of it (it's being the Server—it 'serves' a Client). The unit will 'listen' on a specific TCP port. If a session is established, data will flow from the Client to the Server, and, if present, from the Server to the Client. If a session is not established, both Client-side serial data, and Server-side serial data , if present, will be discarded.

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

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

4.0 Configuration

IP Protocol Config (Continued…)

TCP Client/Server: In this mode, the IPn4G 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.

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 IPn4G will send serial data to a specifically-defined point, using UDP packets. This same IPn4G 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 IPn4G which is to send multicast UDP packets; typically, the Access Point in the IPn4G 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 IP Series 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 IPn4G unit.
  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.

4.0 Configuration

IP 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).

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 (IPn4G 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 Access Point.
  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 VIP Series Station, the value in this field should match the Listening Port of the Access Point (see UDP Point-to-Multipoint (P)).
  Default: **20011**
- **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**

4.0 Configuration

IP Protocol Config (Continued…)

SMTP Client: If the IPn4G 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.

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**

- 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**

4.0 Configuration

IP Protocol Config (Continued…)

C12.22: The C12.22 Protocol is used for electric utility networks & smartgrids. It is used to transport ANSI C12.19 tables used for specific metering data structures.

- **Register to Network - Disable** / Enable
- **Log Network Communication - Disable** / Enable
- **Using Different Sockets - Disable** / Enable
- **Reassembly Packet - Disable** / Enable

- **Host Server IP**
  Specify the Host Server IP. This is the IP Address of the where the C12.22 data should be sent.
  Default: **192.168.2.2**
- **Host Server Port**
  Specify the UDP port used on the Host for C12.22 communication.
  Default: **27016**
- **Local Server Port**
  Specify the Local Server Port for C12.22 communication.
  Default: **27015**

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

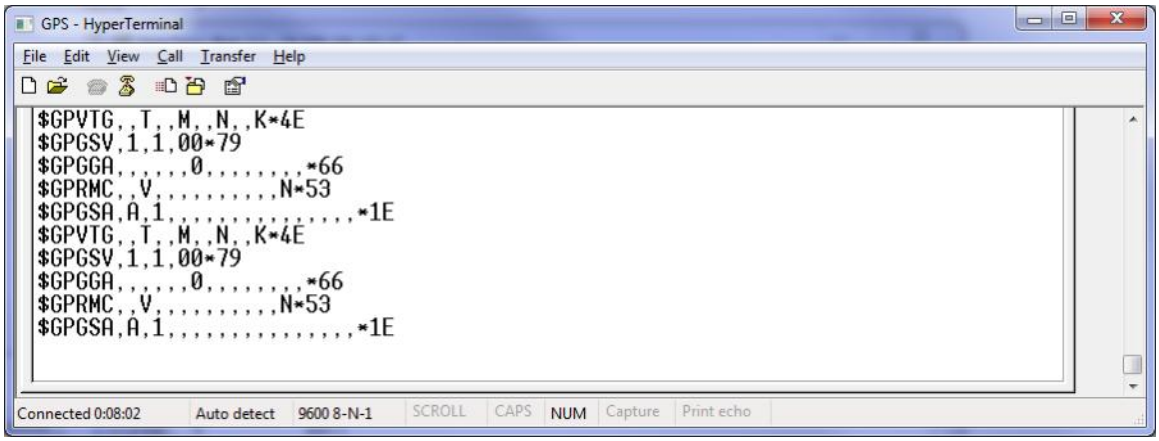


Image 4-5-3: Comport > GPS Transparent Mode

4.0 Configuration

4.6 I/O

4.6.1 I/O > Status

The IPn4G has 1 status input, which can be used with various alarms and sensors for monitoring, telling the modem when certain events have occurred, such as an intrusion alarm on a door, a temperature threshold has been exceed, or a generator has failed, out of fuel. Also included is 1 output, that can be used to drive external relays to remotely control equipment and devices. The Digital I/O pins are available on the back connector shared with the input power.

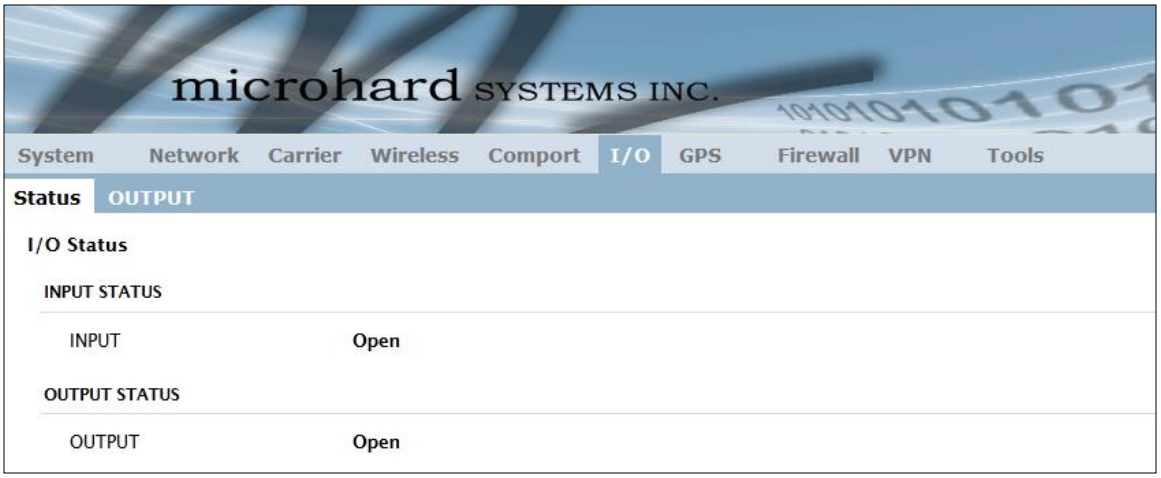


Image 4-6-1: I/O > Status

Input Status

The WebUI will display the current state the input. The I/O pins are all normally open so an open status indicates that there is nothing connected to the input pin, or that an event has not occurred to trigger the input. The inputs have 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 Status

The WebUI will display the current state of each control output. Using the Output menu discussed in the next section, a user can remotely control the status of the output pins.

4.0 Configuration

4.6.2 I/O > OUTPUT

The Output menu is used to open or close the output pin, allowing a user to remotely trigger an

Image 4-6-2: I/O > OUTPUT

The output pin on the IPn4G can be used to provide output signals, which can be used to drive an external relay to control an external device. Maximum recommended load for the Output Pin is 150mA @ 32 VDC (Vin)

4.0 Configuration

4.7 GPS

4.7.1 GPS > Location

Location Map

The location map shows the location on the IPn4G. The unit will attempt to get the GPS coordinates from the built in GPS receiver, and if unsuccessful, will use the Cell ID location reported by the Cellular Carrier.

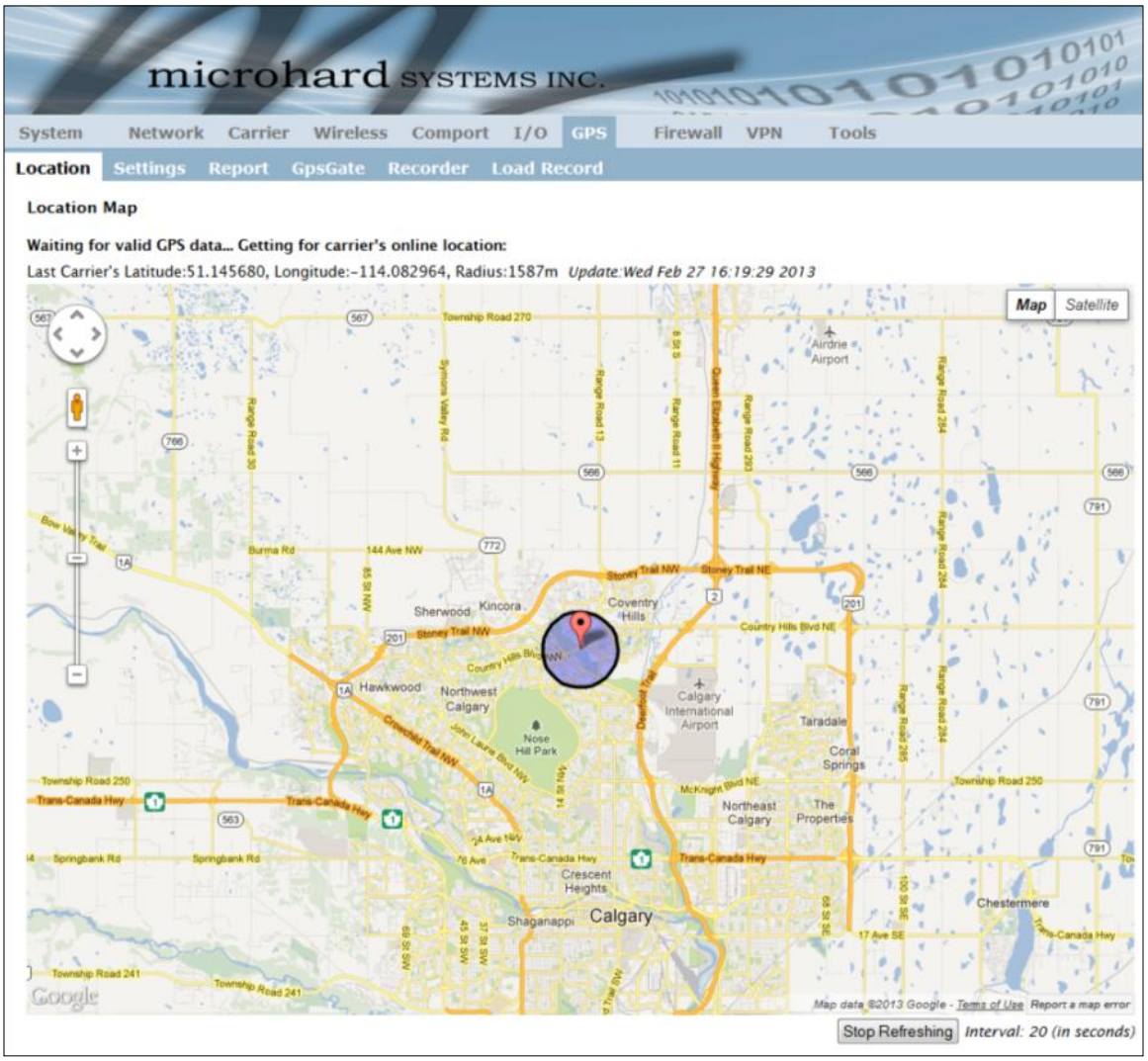


Image 4-7-1: GPS > Location Map

4.0 Configuration

4.7.2 GPS > Settings

The IPn4G can be polled for GPS data via GPSD standards and/or provide customizable reporting to up to 4 different hosts using UDP or Email Reporting.

Image 4-7-2: GPS > Settings

GPS Status	
Enable or disable the GPS polling function of the IPn4G.	**Values** Disable **/ Enable**

GPS Source	
The IPn4G contains an embedded GPS feature in the cellular module. To use the GPS features of the IPn4G a cellular antenna must be connected to the Diversity Antenna Port.	**Values** **Embedded Carrier GPS**

TCP Port	
Specify the TCP port on the IPn4G where the GPS service is running and remote systems can connect and poll for GPSD data.	**Values** **2947**

4.0 Configuration

4.7.3 GPS > Report

The IPn4G can provide customizable reporting to up to 4 hosts using UDP or Email Reporting.

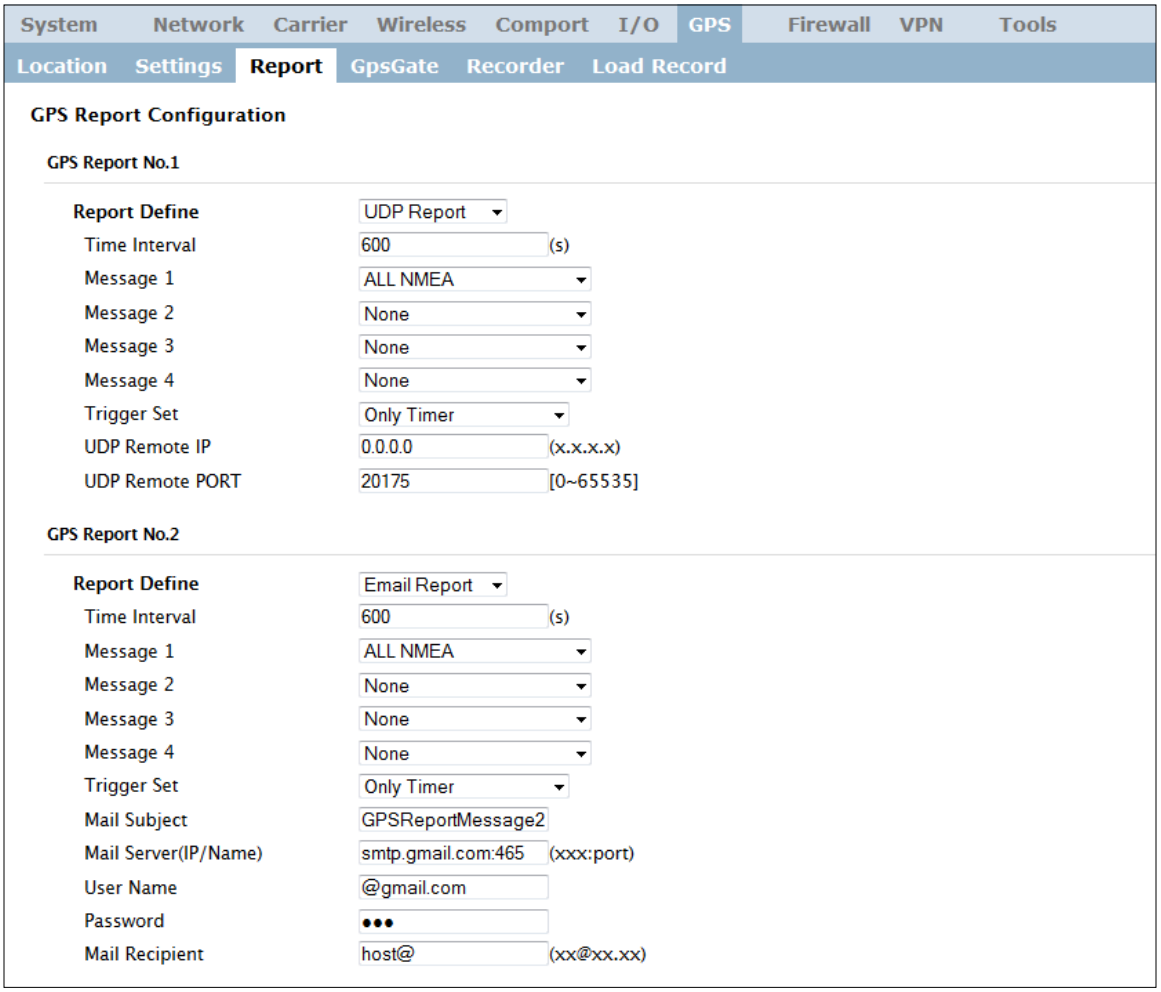


Image 4-7-3: GPS > GPS Report

Report Define	Values (selection)
Enable UDP and/or Email or disable GPS Reporting. Up to 4 reports can be set up and configured independently.	**Disable** UDP Report Email Report

Time Interval	Values (seconds)
The interval timer specifies the frequency at which the GPS data is reported in seconds.	**600**

4.0 Configuration

Message 1-4

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

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

Values (selection)

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

Trigger Set

The trigger condition defines the conditions that must be met before a GPS update is reported. If OR is chosen, the Repeater Timer OR the Distance trigger conditions must be met before an update is sent. The AND condition, requires that both the Repeat timer AND the Distance trigger conditions be met before an update is sent.

Values (selection)

Only Timer
Timer AND Distance
Timer OR Distance

Distance Set

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

Values (meters)

1000

UDP Remote IP / Port

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

Values (Address/Port)

0.0.0.0 / 20175

Mail Subject

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

Values (characters)

1000

Mail Server

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

Values (Address:port)

smtp.gmail.com:465

Username / Password

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

Values (characters)

Username / password

Mail Recipient

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

Values (characters)

host@email.com

4.0 Configuration

4.7.4 GPS > GpsGate

The IPn4G is compatible with *GpsGate - GPS Tracking Software*, which is a 3rd party mapping solution used for various GPS services including vehicle and asset tracking The IPn4G can communicate with GpsGate via Tracker Mode and TCP/IP. (UDP reporting can also send information to GpsGate, see the GPS > Report - UDP Reports)

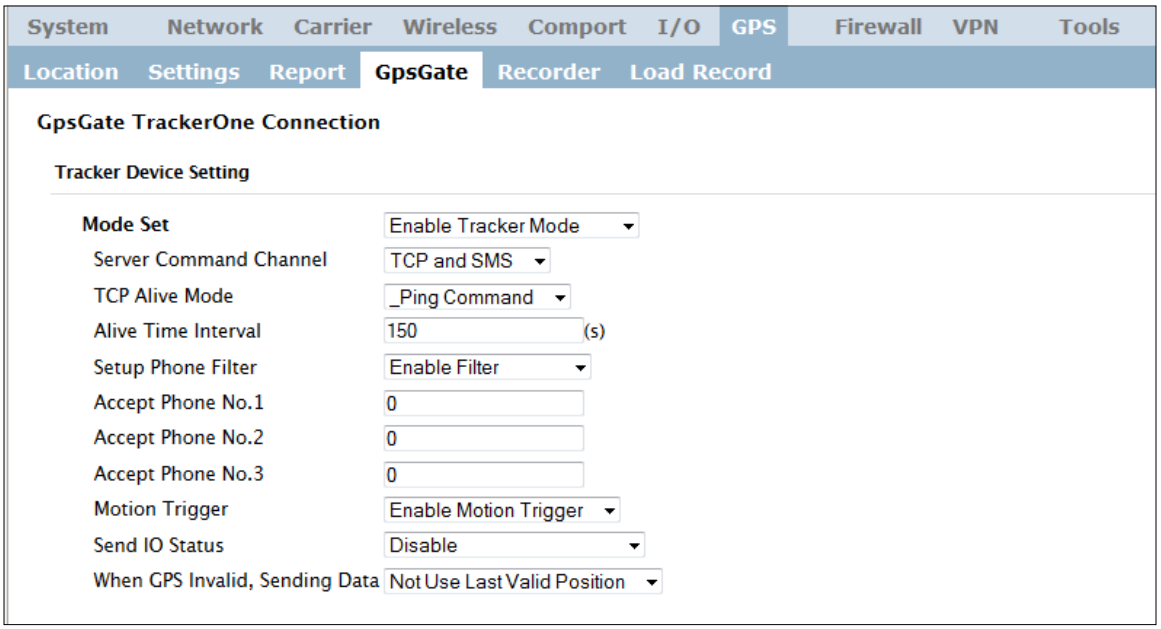


Image 4-7-4: GPS > GpsGate Tracker Mode

GpsGate - Tracker Mode

Mode Set	Values (selection)
Enable GpsGate Tracker Mode or TCP modes. In tracker mode The IPn4G and GpsGate software will communicate via TCP/IP, however if a connection is not available it will attempt to use SMS messaging.	**Disable** Enable Tracker Mode Enable TCP Send Mode

Server Command Channel	Values (seconds)
By default IPn4G and GpsGate will use TCP and SMS to ensure communication between each other. It is also possible to specify TCP or SMS communication only. Initial setup in Tracker mode must be via SMS.	**TCP and SMS** TCP Only SMS Only

TCP Alive Mode / Alive Time Interval	Values (seconds)
TCP alive mode will keep TCP connection alive if tracker is not enabled or the tracker interval is too long. The default is 150 seconds.	**150**

4.0 Configuration

Setup Phone Filter

A phone number filter can be applied to prevent SMS commands not intended for the IPn4G from being processed.

Values (selection)

Disable: Accept All
Enable Filter

Motion Trigger

Use this parameter to enable or disable the motion trigger in the IPn4G.

Values (selection)

Disable
Enable Motion Trigger

Send IO Status

When enabled, the IPn4G will send the current status of the Digital I/O inputs and/or outputs to the GpsGate Server.

Values (selection)

Disable
Send Input Status
Send Output Status
Send Input&Output Status

When GPS Invalid, Sending Data

Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.

Values (selection)

Not Use Last Valid Position
Use Last Valid Position

GpsGate - TCP Mode

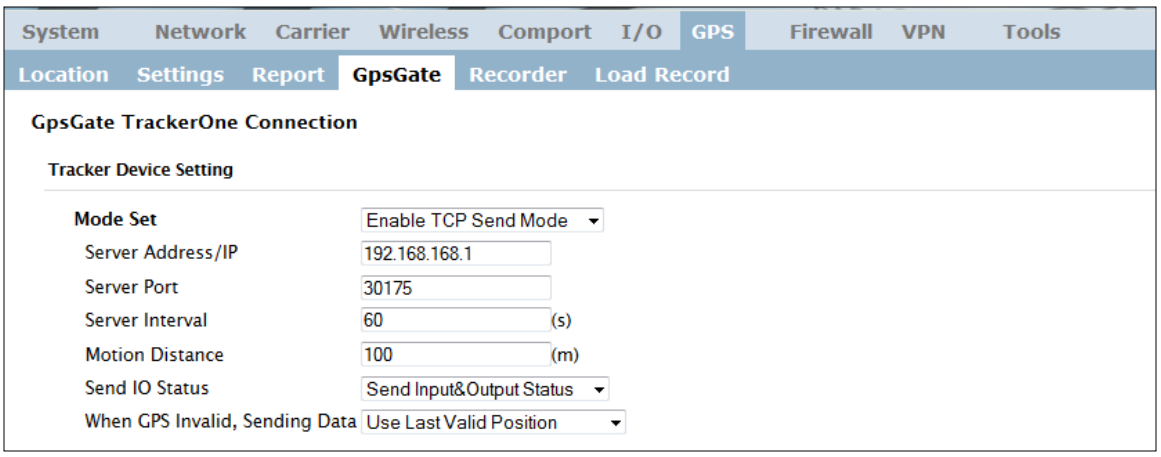


Image 4-7-5: GPS > GpsGate TCP Mode

4.0 Configuration

Mode Set

Enable GpsGate Tracker Mode or TCP modes. In TCP Mode the IPn4G will establish a connection with the GpsGate Server directly without the SMS setup process. If the TCP connection is not available, the IPn4G will continue to try to connect every few seconds.

Values (selection)

Disable
Enable Tracker Mode
Enable TCP Send Mode

Server Address / IP

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

Values (IP Address)

192.168.168.1

Server Port

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

Values (Port)

30175

Server Interval

Define the interval at which the IPn4G will send data to the GpsGate Server.

Values (seconds)

60

Motion Distance

Set the motion threshold in which the IPn4G will be triggered to send location data.

Values (meters)

100

Send IO Status

When enabled, the IPn4G will send the current status of the Digital I/O inputs and/or outputs to the GpsGate Server.

Values (selection)

Disable
Send Input Status
Send Output Status
Send Input&Output Status

When GPS Invalid, Sending Data

Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.

Values (selection)

Not Use Last Valid Position
Use Last Valid Position

4.0 Configuration

4.7.5 GPS > Recorder

The IPn4G can log the last 200 GPS events and store them in non-volatile memory. These events can then be viewed within the WebUI, on a map, or sent to a remote server.

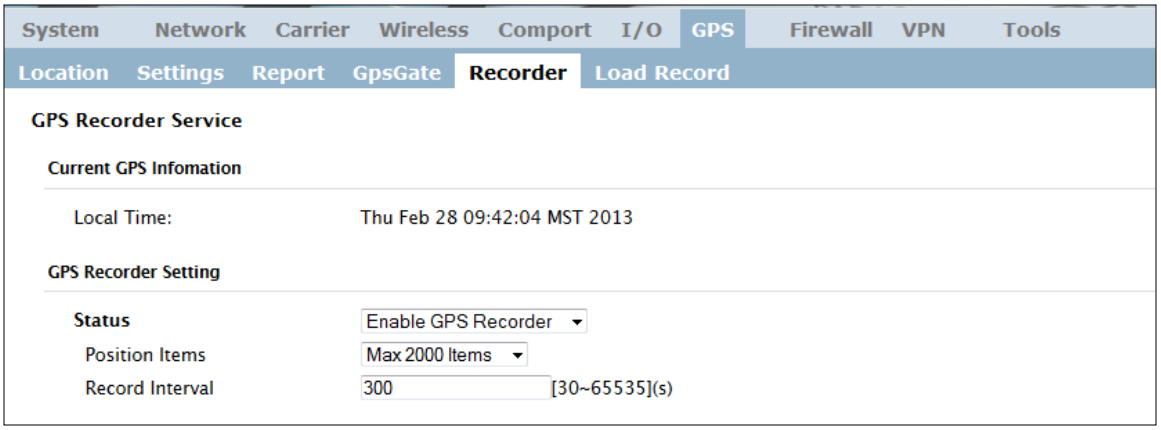


Image 4-7-6: GPS > GPS Recorder Service

Status	
Use the Status parameter to enable the GPS recording functionality of the IPn4G.	**Values (selection)** **Disable** Enable GPS Recorder

Position Items	
Specify the maximum number of events to be recorded by the IPn4G. Currently this is a fixed value at 2000 entries.	**Values (selection)** **Max 2000 Items**

Record Interval	
Define the interval at which the IPn4G will record GPS data. If there is no valid data available at the specified time, the unit will wait until the next time valid information is received.	**Values (seconds)** **300**

4.0 Configuration

4.7.6 GPS > Load Record

Data that has been recorded and saved by the IPn4G can then be viewed or sent to a remote server.

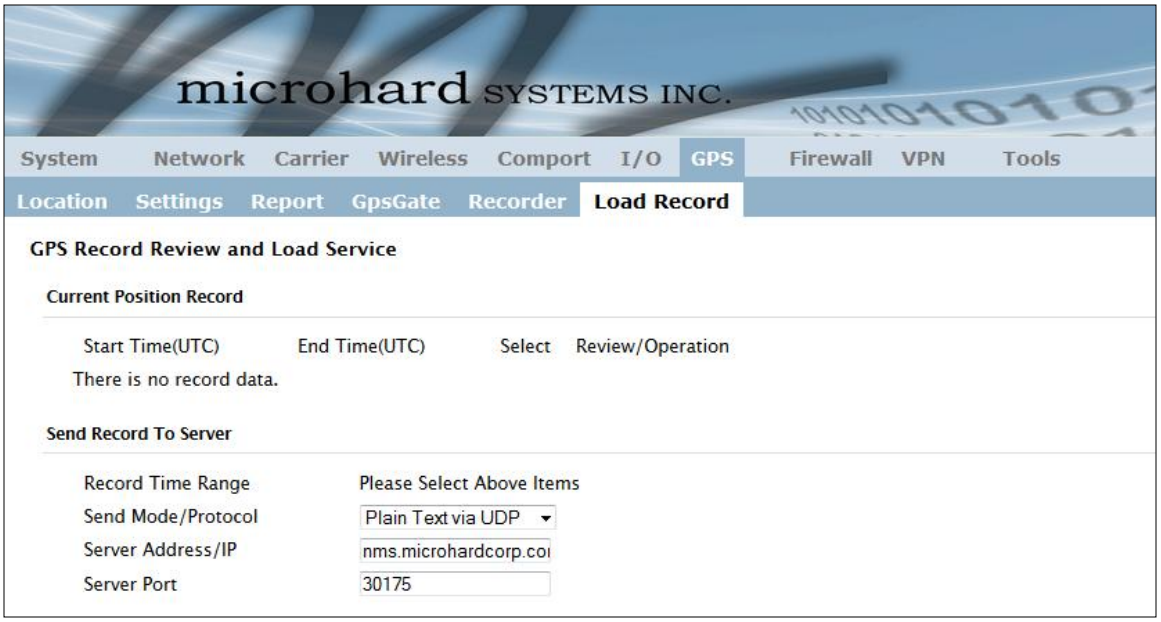


Image 4-7-7: GPS > GPS Load Record

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

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

Server Address/IP / Port	
Enter the address or IP address and port number of the remote server to which the data is to be sent.	**Values (IP/Port)** nms.microhardcorp.com 30175

4.0 Configuration

4.8 Firewall

4.8.1 Firewall > Status

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

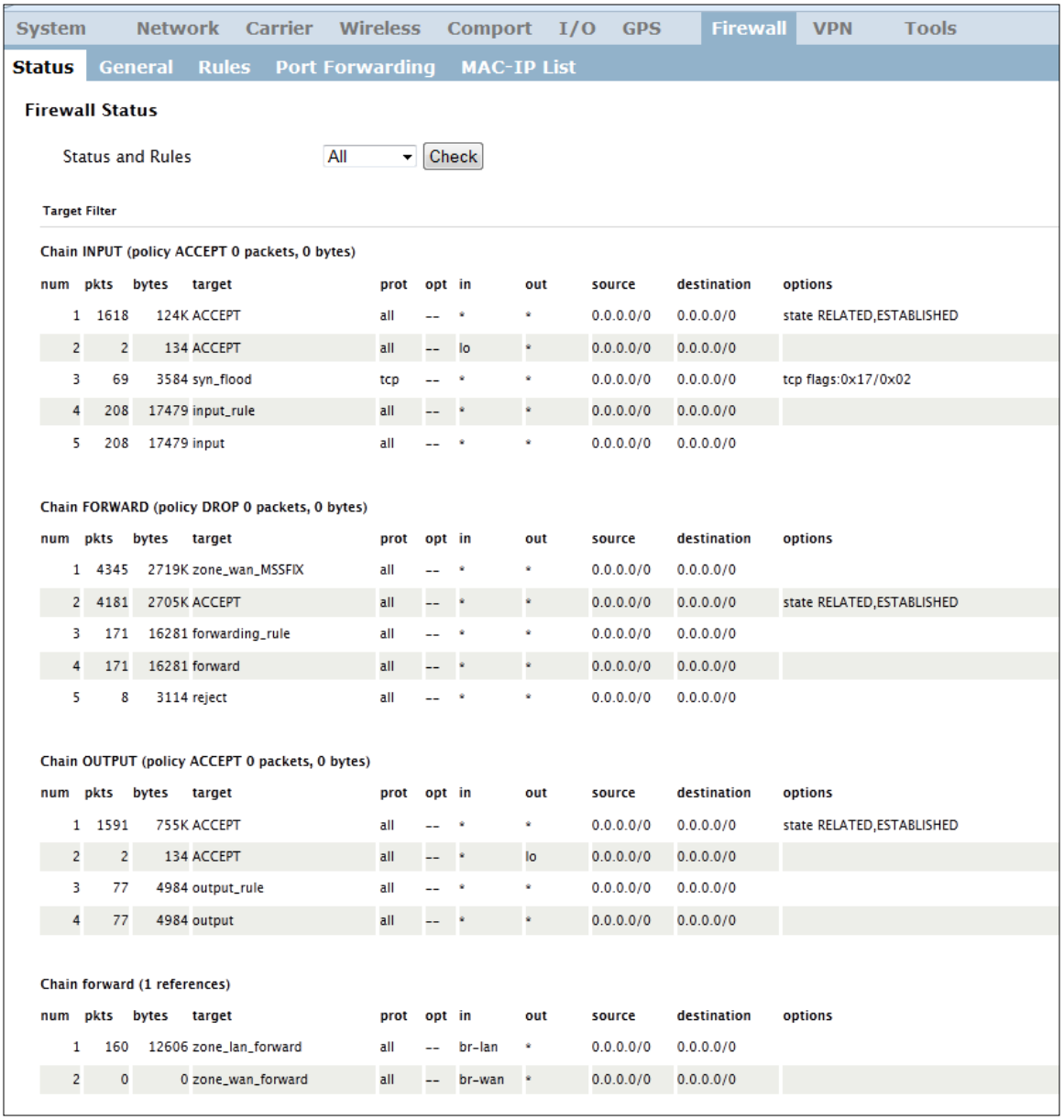


Image 4-8-1: Firewall > Status

4.0 Configuration

4.8.2 Firewall > General

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

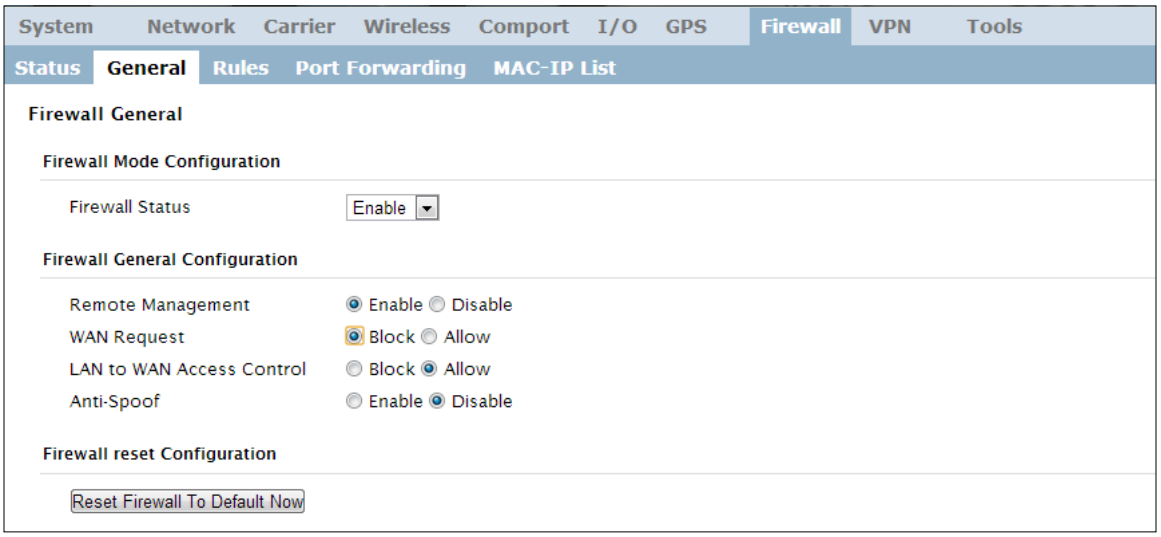


Image 4-8-2: Firewall > General

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

Remote Management	
Allow remote management of the IPn4G on the WAN/4G 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**

WAN Request	
When Blocked the IPn4G will block all requests from the WAN/4G unless specified otherwise in the Access Rules, MAC List, IP List configurations. Access to ports 80 (HTTP) and 443 (HTTPS-if enabled), is still available unless disabled in the **WAN Remote Management** option.	**Values** Block / **Allow**

LAN to WAN Access Control	
Allows or Blocks traffic from the LAN accessing the WAN unless specified otherwise using the Access Rules, MAC, and IP List configuration.	**Values** Block / **Allow**

4.0 Configuration

4.8.3 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.

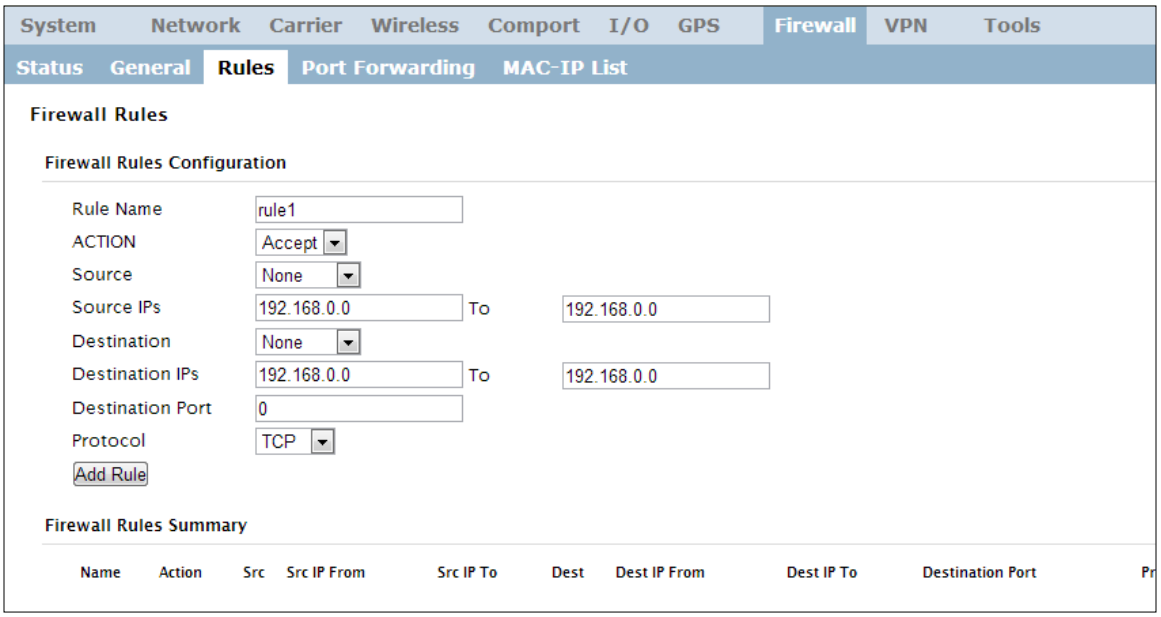


Image 4-8-3: Firewall > Rules

Rule Name

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

Values (10 Chars)

characters

Action

The Action is used to define how the rule handles the connection request.

ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.

This is configured based on how the **WAN/4G Request** and **LAN to WAN/4G Access Control** are configured in the previous menus.

Values (selection)

ACCEPT
DROP
REJECT

Source

Select the zone which is to be the source of the data traffic. WAN applies to the connection to the cellular carrier. The LAN refers to local connections on the IPn4G (Ethernet/WiFi).

Values

LAN
WAN
(Additional LAN Interfaces)
None

4.0 Configuration

Source IPs	
If a valid IP/Network address is specified, the action will apply against that address; otherwise, to allow access to any source IP, the value must be set to 0.0.0.0 to 255.255.255.255 in the Source to and from respectively.	**Values (IP Address)** **192.168.0.0**

Destination	
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 IPn4G (Ethernet/WiFi)	**Values (selection)** LAN WAN (Additional LAN Interfaces) None

Destination IPs	
If a valid IP/Network address is specified, the action will apply against that address; otherwise, setting the range to 0.0.0.0 - 255.255.255.255 in this field results in the action applying to all source IP addresses.	**Values (IP Address)** **192.168.0.0**

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**

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

4.0 Configuration

4.8.4 Firewall > Port Forwarding

The IPn4G 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 IPn4G. If all incoming traffic is intended for a specific connected device, DMZ could be used to simplify the process, as all incoming traffic can be directed towards a specific IP address.

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

IP-Passthrough (Carrier > Settings) is another option for passing traffic through the IPn4G, in this case all traffic is passed to a single device connected to the RJ45 port of the IPn4G, The device must be set for DHCP, as the IPn4G 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 IPn4G, as well as all other features of the IPn4G such as COM, VPN, GPS etc.

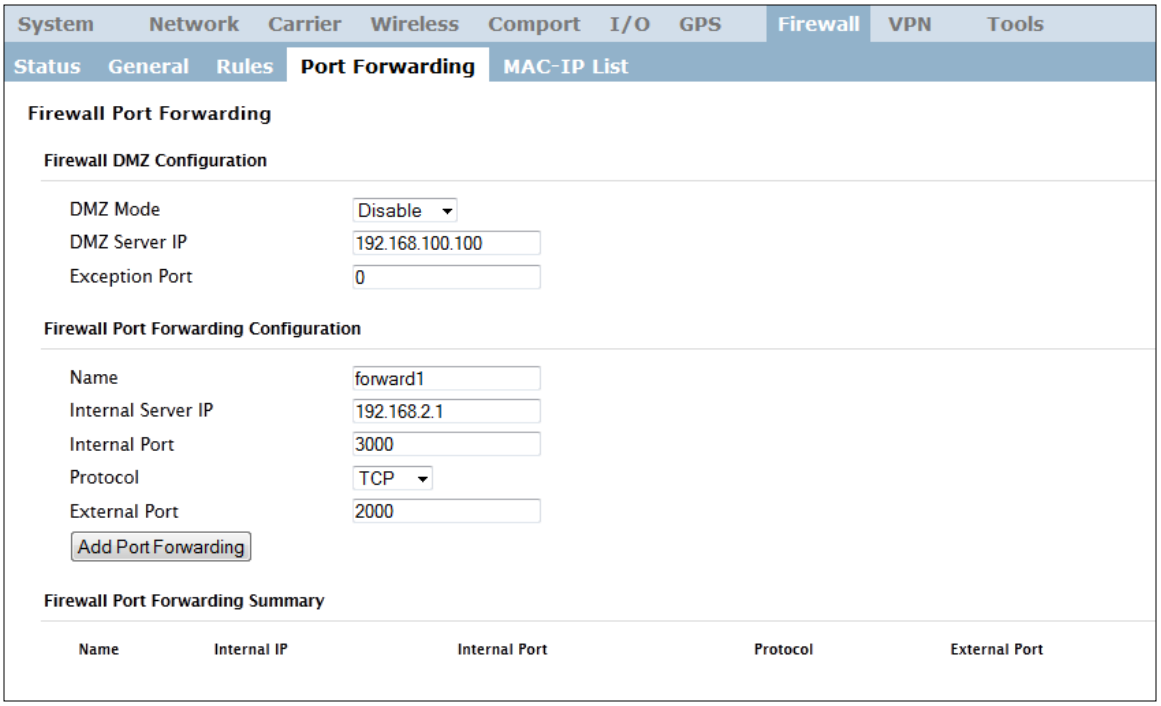


Image 4-8-4: Firewall > Port Forwarding

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

4.0 Configuration

DMZ Server IP	
Enter the IP address of the DMZ server on the LAN side of the IPn4G.	**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 IPn4G.	**Values (Port #)** **0**

Firewall Port Forwarding Configuration

Name	
This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to 10 characters.	**Values (10 chars)** **Forward**

Internal Server IP	
Enter the IP address of the intended internal (i.e. on LAN side of IPn4G) server. This is the IP address of the device you are forwarding traffic to.	**Values (IP Address)** **192.168.2.1**

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

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

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

4.0 Configuration

4.8.5 Firewall > MAC-IP List

MAC List configuration can be used to control which physical LAN devices can access the ports on the IPn4G, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the IPn4G, by restricting or allowing connections based on the IP Address/Subnet.

MAC-IP List can be used alone or in combination with LAN to WAN/4G Access Control to provide secure access to the physical ports of the IPn4G.

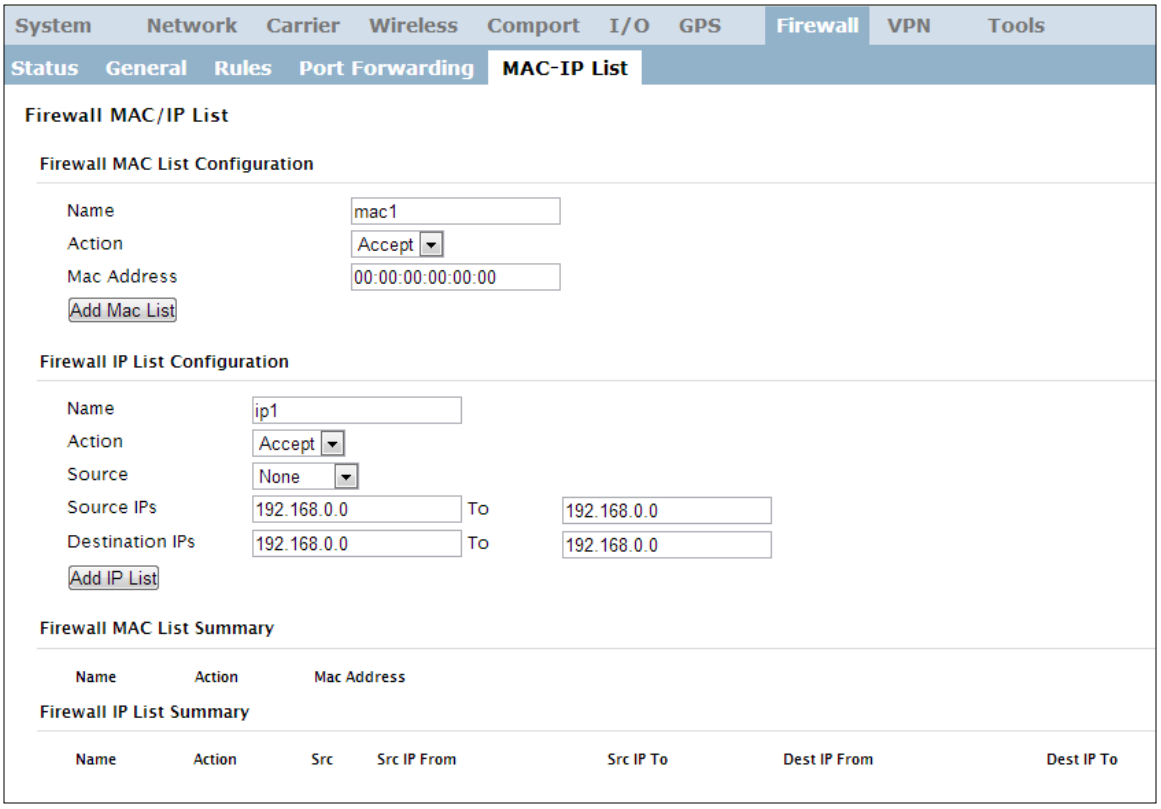


Image 4-8-5: Firewall > MAC-IP List

Firewall MAC List Configuration

Rule Name	
The Rule Name field is required to give the rule a convenient name for reference. Each rule must have a unique name, up to 10 characters in length.	**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. Not case sensitive.	**Values (MAC Address)** **00:00:00:00:00:00**

4.0 Configuration

Firewall MAC List Configuration (Continued)

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

Firewall IP List Configuration

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

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

	Source
Enter the specific zone that the IP List will apply to, 4G/WAN (Cellular), LAN (Ethernet, WiFi) or None (both).	**Values (Selection)** LAN / WAN/ **NONE**

	Source IP Address
Specify the specific IP or range. A range of 0.0.0.0 to 255.255.255.255 will allow/block all source IP's	**Values (IP Address)** **192.168.0.0**

	Destination Address
Optional, enter destination IP address(s) to make the IP list more specific. Set to 0.0.0.0 to 255.255.255.255 to cover the entire IP range if not being used.	**Values (IP Address)** **192.168.0.0**

4.0 Configuration

4.9 VPN

4.9.1 VPN > Summary

A Virtual Private Network (VPN) may be configured to enable a tunnel between the IPn4G and a remote network.. The IPn4G supports VPN IPsec Gateway to Gateway (site-to-site) tunneling, meaning you are using the IPn4G to create a tunnel to a network with VPN capabilities (Another IPn4G or VPN capable device). The IPn4G can also operate as a L2TP Server, allowing users to VPN into the unit from a remote PC, and a L2TP Client.

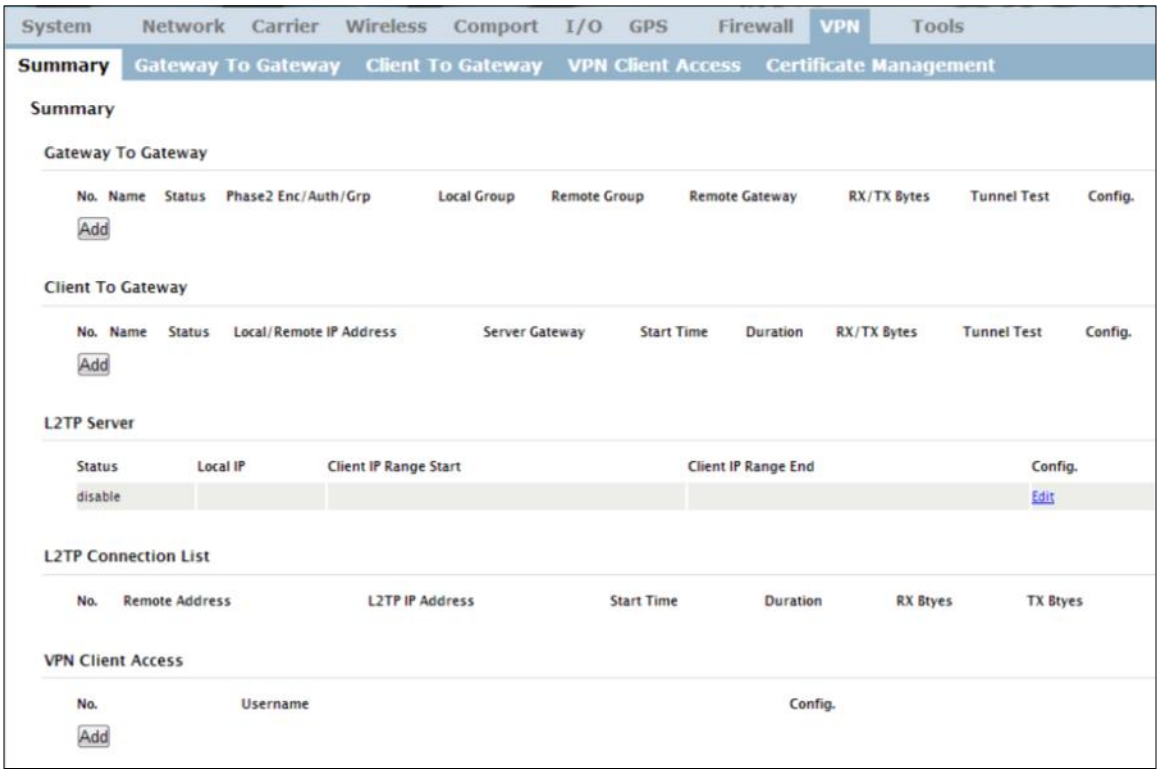


Image 4-9-1: VPN > Summary

4.0 Configuration

4.9.2 VPN > Gateway To Gateway (Site-to-Site)

A Gateway to Gateway connection is used to create a tunnel between two VPN devices such as an IPn4G and another device (another IPn4G or Cisco VPN Router or another vendor…). The local and remote group settings will need to be configured below to mirror those set on the other VPN device.

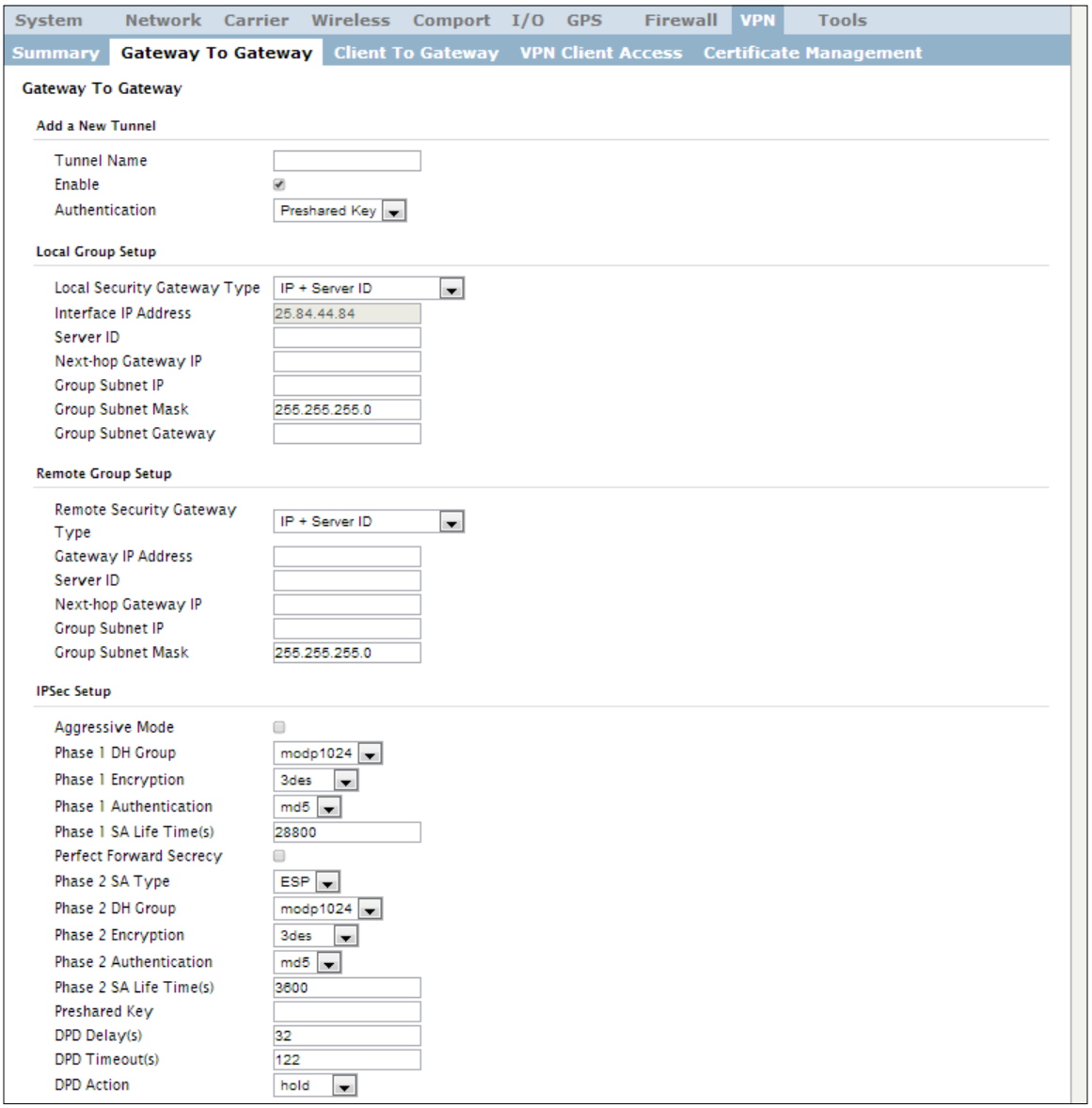


Image 4-9-2: VPN > Gateway to Gateway

Tunnel Name	
Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name.	**Values (chars)** **tunnel1**

4.0 Configuration

Enable

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

Values (checkbox)

Enable (Checked)

Local Group Setup

Local Security Gateway Type

Specify the method for identifying the router to establish the VPN tunnel. The Local Security Gateway is on this router; the Remote Security Gateway is on the other router. At least one of the routers must have either a static IP address or a dynamic IP with server id to make a connection.

Values (selection)

IP Only
IP + Server ID
Dynamic IP + Server ID

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

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

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

Interface IP Address

Displays the IP address of the IPn4G, which is the local VPN Gateway.

Values (IP Address)

Current IP Address

Server ID

This option appears when the Local Security Gateway Type specifies that the Server ID is required for the connection. The Server ID must be in the format @name, where name can be anything. Both routers must know each others names to establish a connection.

Values (characters)

(no default)

Next-hop Gateway IP

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

Values (IP Address)

(no default)

Group Subnet IP

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

Values (IP Address)

(no default)

4.0 Configuration

Group Subnet Mask	
Specify the subnet mask of the local network address.	**Values (IP Address)** **255.255.255.0**

Group Subnet Gateway	
Enter the Gateway for the local group network.	**Values (IP Address)** *(no default)*

Remote Group Setup

Remote Security Gateway Type	
Specify the method for identifying the router to establish the VPN tunnel. The Local Security Gateway is on this router; the Remote Security Gateway is on the other router. At least one of the routers must have either a static IP address or a dynamic IP with server id to make a connection. (See Local Group Setup for details)	**Values (selection)** IP Only **IP + Server ID** Dynamic IP + Server ID

Gateway IP Address	
If the remote VPN router has a static IP address, enter the IP address of the remote VPN Gateway here.	**Values (IP Address)** *(no default)*

Server ID	
This option appears when the Remote Security Gateway Type specifies that the Server ID is required for the connection. The Server ID must be in the format @name, where name can be anything. Both routers must know each others names to establish a connection.	**Values (IP Address)** *(no default)*

Next-hop Gateway IP	
Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.	**Values (IP Address)** *(no default)*

Subnet IP Address	
Define the remote network by specifying the local subnet.	**Values (IP Address)**

Subnet Mask	
Specify the subnet mask of the remote network address.	**Values (IP Address)** **255.255.255.0**

4.0 Configuration

IPsec Setup

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

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

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

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

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

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

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

4.0 Configuration

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

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

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

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

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

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

4.0 Configuration

4.9.3 VPN > Client To Gateway (L2TP Client)

The IPn4G can operate as a L2TP Client, allowing a VPN connection to be made with a L2TP Server.

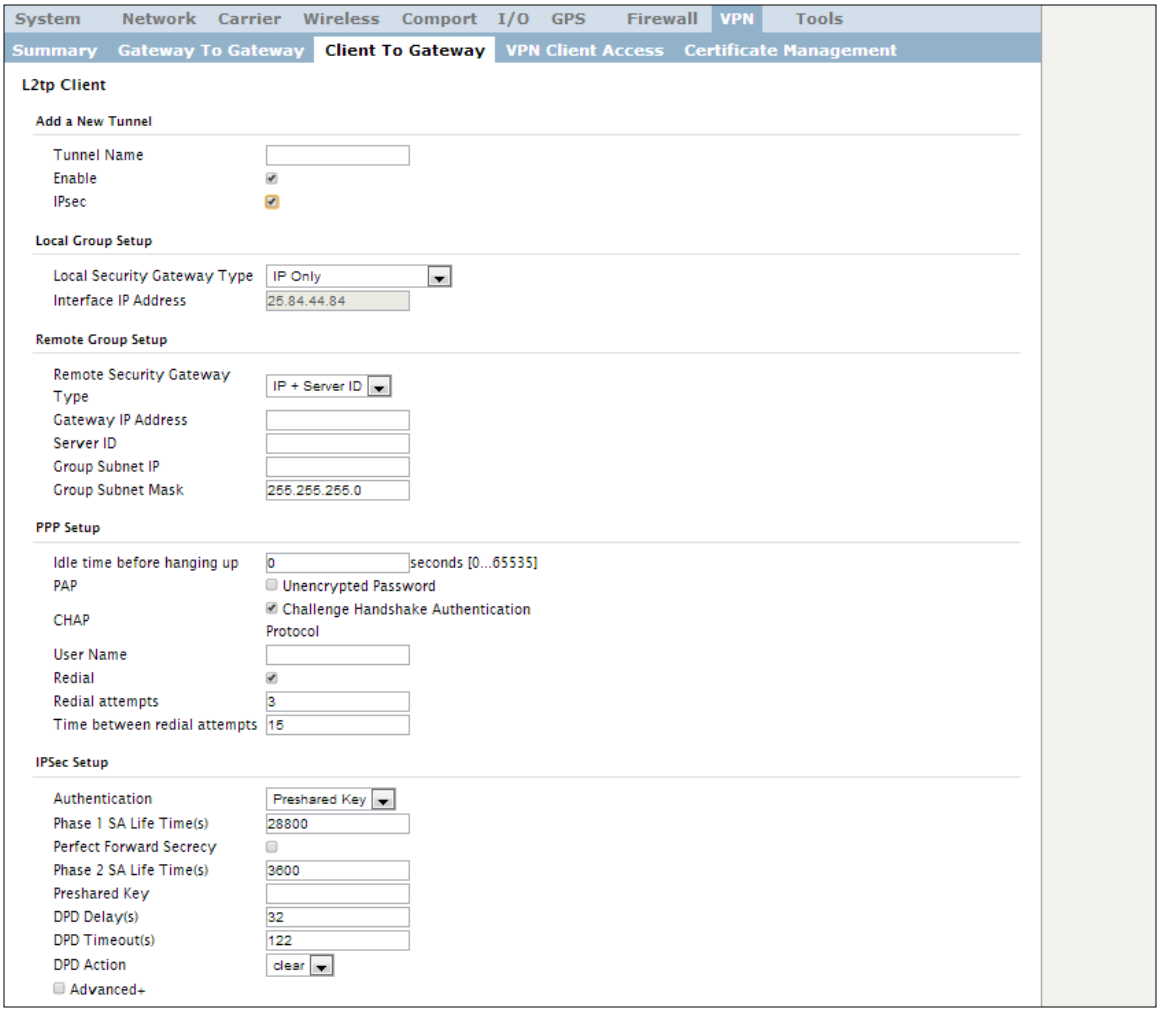


Image 4-9-3: VPN > Client to Gateway

Tunnel Name	
Enter a name for the VPN Tunnel. Up to 16 different tunnels can be created, each requiring a unique name.	**Values (chars)** **tunnel1**

Enable	
Used to enable (checked) is disable (unchecked) the VPN tunnel.	**Values (checkbox)** **Enable (Checked)**

4.0 Configuration

Local Interface IP Address	
This will display the current IPn4G WAN (4G/Cellular) IP Address.	**Values (IP Address)** ***Current IP***

Remote Gateway IP Address	
Enter the IP Address of the Remote Gateway that you wish to establish a connection with.	**Values (IP Address)** *none*

Remote Server ID	
Some servers require that you know the Server ID as well as the IP address. Enter the Server ID of the remote router here.	**Values** *none*

Remote Subnet IP	
In order to communicate with the devices on the other side of the tunnel, the IPn4G must know which data to pass through the tunnel, to do this enter the Remote Subnet network IP address here.	**Values (IP Address)** *none*

Remote Subnet Mask	
Enter the Remote Subnet Mask	**Values (IP Address)** *none*

Idle time before hanging up	
Enter the Idle time (in seconds) to wait before giving up the PPP connection. The default is 0, which means the time is infinite. (0—65535)	**Values (seconds)** *0*

Username	
Enter the Username	**Values (chars)** *0*

Preshared Key	
The preshared key is required to connect to the L2TP Server.	**Values (chars)** *0*

IPSec Setup - See previous sections for additional info.

4.0 Configuration

4.9.4 VPN > VPN Client Access

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

Image 4-9-4: VPN > VPN Client Access

Username	
Enter a username for the user being set up.	**Values (characters)**

New Password	
Enter a password for the use.	**Values (characters)**

Confirm New Password	
Enter the password again, the IPn4G will ensure that the password match.	**Values (IP Address)**

4.0 Configuration

4.9.5 VPN > Certificate Management

When using the VPN features of the IPn4G, it is possible to select X.509 for the Authentication Type. If that is the case, the IPn4G must use the required x.509 certificates in order to establish a secure tunnel between other devices. Certificate Management allows the user a place to manage these certificates.

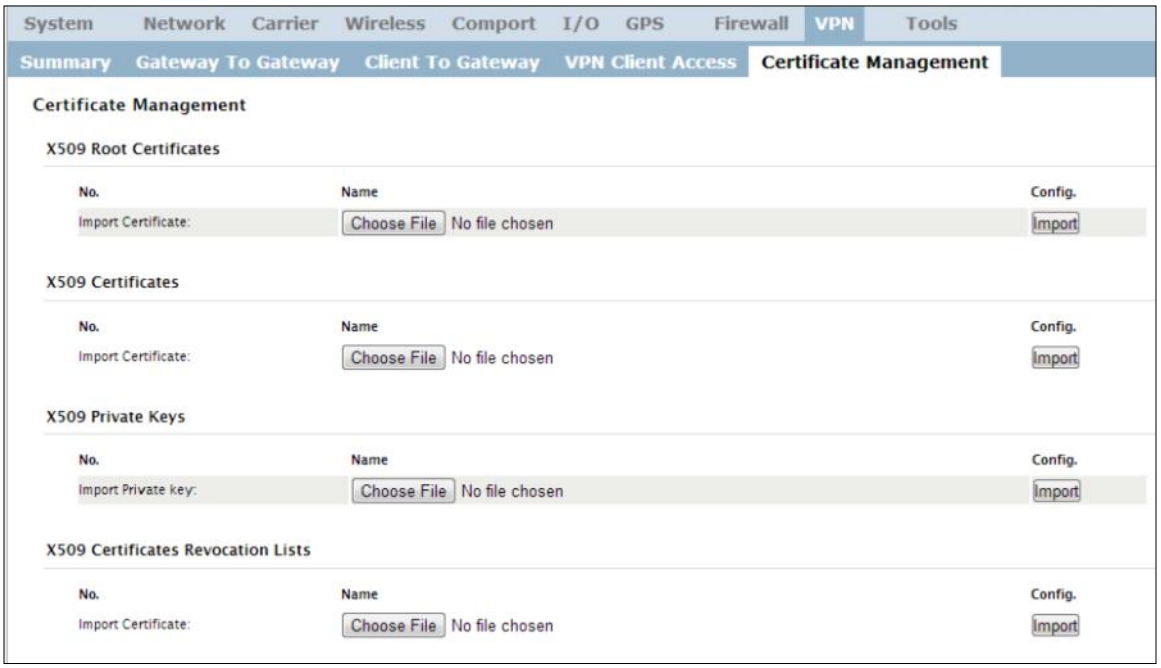


Image 4-9-5: VPN > Certificate Management

4.0 Configuration

4.10 Tools

4.10.1 Tools > Discovery

Network Discovery

The Network discovery tool allows the IPn4G to send a broadcast to all IPn4G/VIP Series units on the same network. Other units on the network will respond to the broadcast and report their MAC address, IP address (With a hyperlink to that units WebUI page), description, firmware version, operating mode, and the SSID (regardless of whether it was set to broadcast or not).

The discovery service can be a useful troubleshooting tool and can be used to quickly find and indentify other units on the network. It can be disabled from the Network > sdpServer menu.

Image 4-10-1: Tools > Discovery

4.0 Configuration

4.10.2 Tools > Netflow Report

The IPn4G can be configured to send Netflow reports to up to 3 remote systems. Netflow is a tool that collects and reports IP traffic information, allowing a user to analyze network traffic on a per interface basis to identity bandwidth issues and to understand data needs. Standard Netflow Filters can be applied to narrow down results and target specific data requirements.

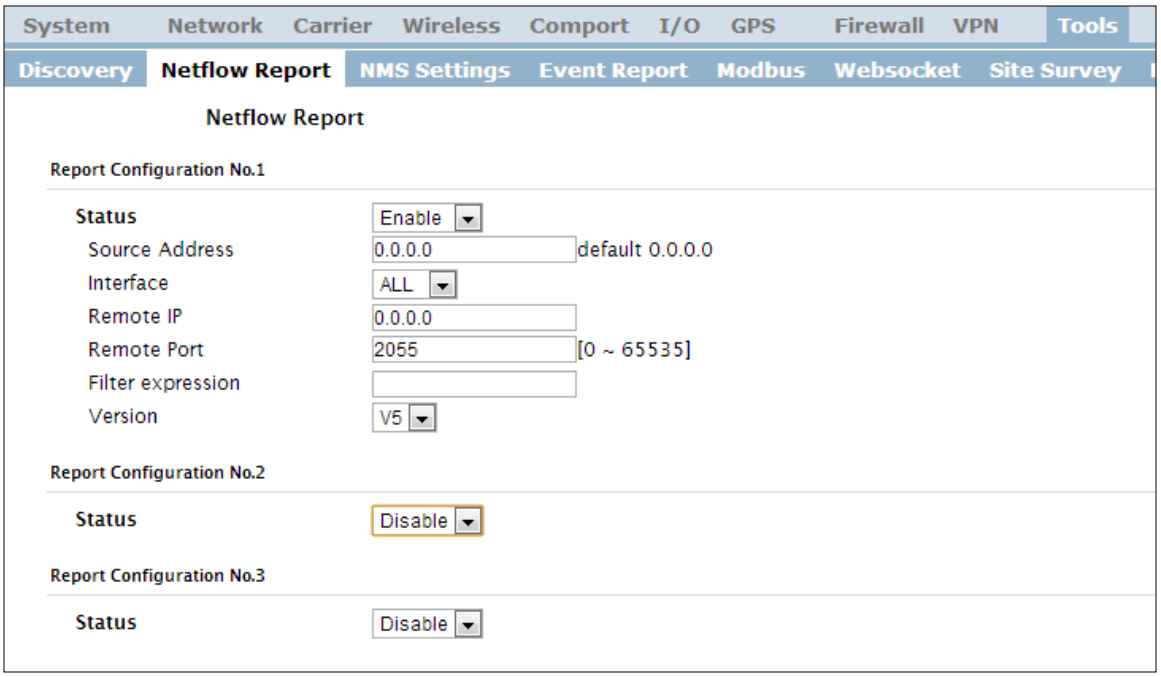


Image 4-10-2: Tools > Netflow Report

Status	
Enable / Disable Netflow Reporting.	**Values (selection)** **Disable /** Enable

Source Address	
The Source Address is the IP Address, of which data is to be collected and analyzed. The default of 0.0.0.0 will collect and report information about all addresses connected to the interface selected below.	**Values (IP Address)** **0.0.0.0**

Interface	
Select between WAN (4G) and LAN interfaces, or capture data from all interfaces.	**Values (selection)** **LAN /** WAN / ALL

4.0 Configuration

	Remote IP
The Remote IP is the IP Address of the NetFlow collector where the flow reports are be sent.	**Values (IP Address)** **0.0.0.0**
	Remote Port
Enter the Remote Port number.	**Values (IP Address)** **0**
	Filter expression
Filter expression selects which packets will be captured. If no expression is given, all packets will be captured. Otherwise, only packets for which expression is `true' will be captured. Example: **tcp&&port 80** *The "tcpdump" manual, available on the internet provides detailed expression syntax.*	**Values (chars)** *(no default)*
	Version
Select the Netflow version format to use. V1, 5 and 7 are supported.	**Values (selection)** **V1** / V5 / V7

4.0 Configuration

4.10.3 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 IPn4G to report to NMS.

To get started with NMS, browse to the Microhard NMS website, **nms.microhardcorp.com**, click on the register button in the top right corner to register for a Domain (profile), and set up a Domain Administrator Account.

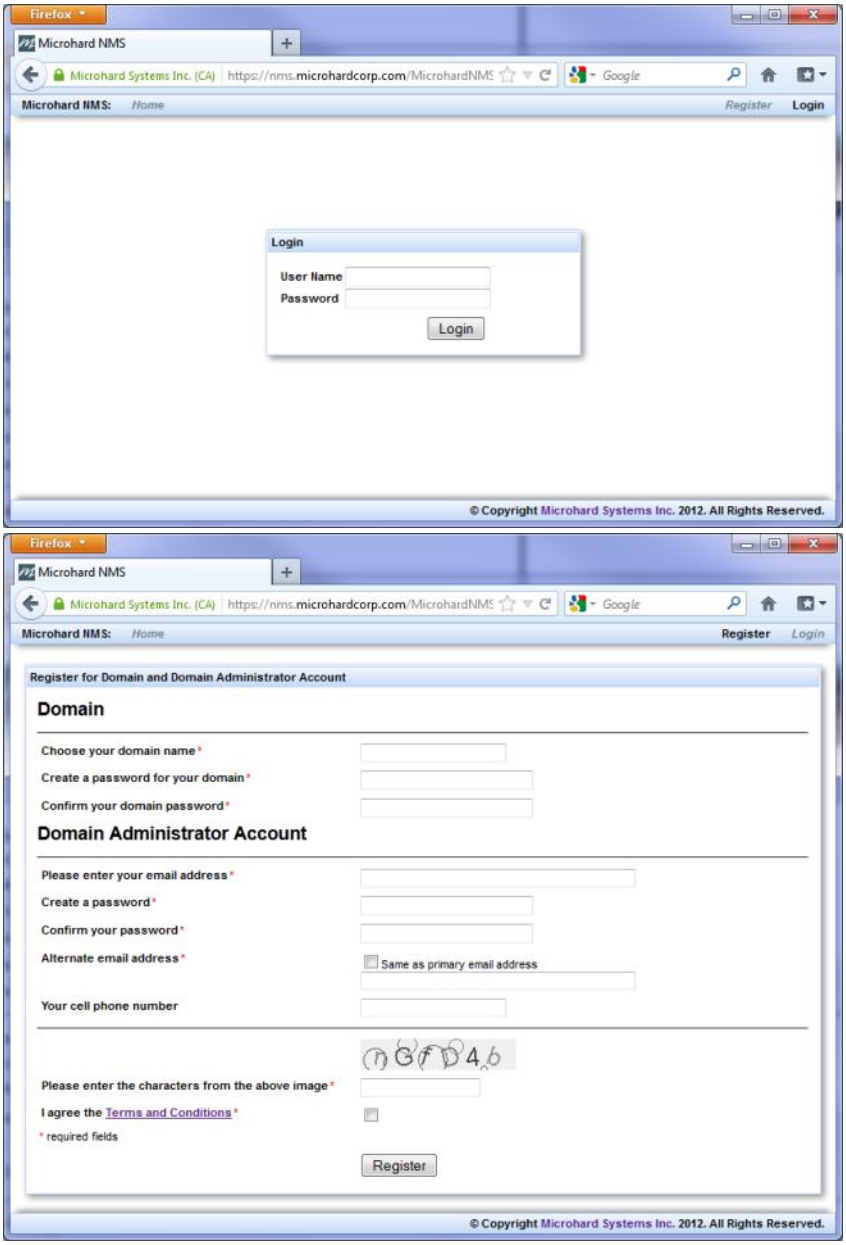


Image 4-10-3: NMS

4.0 Configuration

Domain Name: A logical management zone for 3G or 4G devices will report to on NMS, the logged data is separated from any other users that are using NMS. The Domain Name is required in every 3G or 4G device for it to report to right zone. Under this user domain, one can create and manage sub-domain. The sub-domain can only be created by the domain administrator, NOT by the NMS subscription page.

Domain Password: This password is used to prevent misuse of the domain. This needs to be entered into each 3G or 4G device for it to report to right zone.

Email Address: The email address entered here will be the login username. During the registration stage, a confirmation email will be sent by the NMS system for verification and confirmation to activate your account.

Once confirmed, this account will be the administrator of the domain. The administrator can manage sub-domain and user accounts that belong to this domain.

Once NMS has been configured, each IPn4G must be configured to report into NMS.

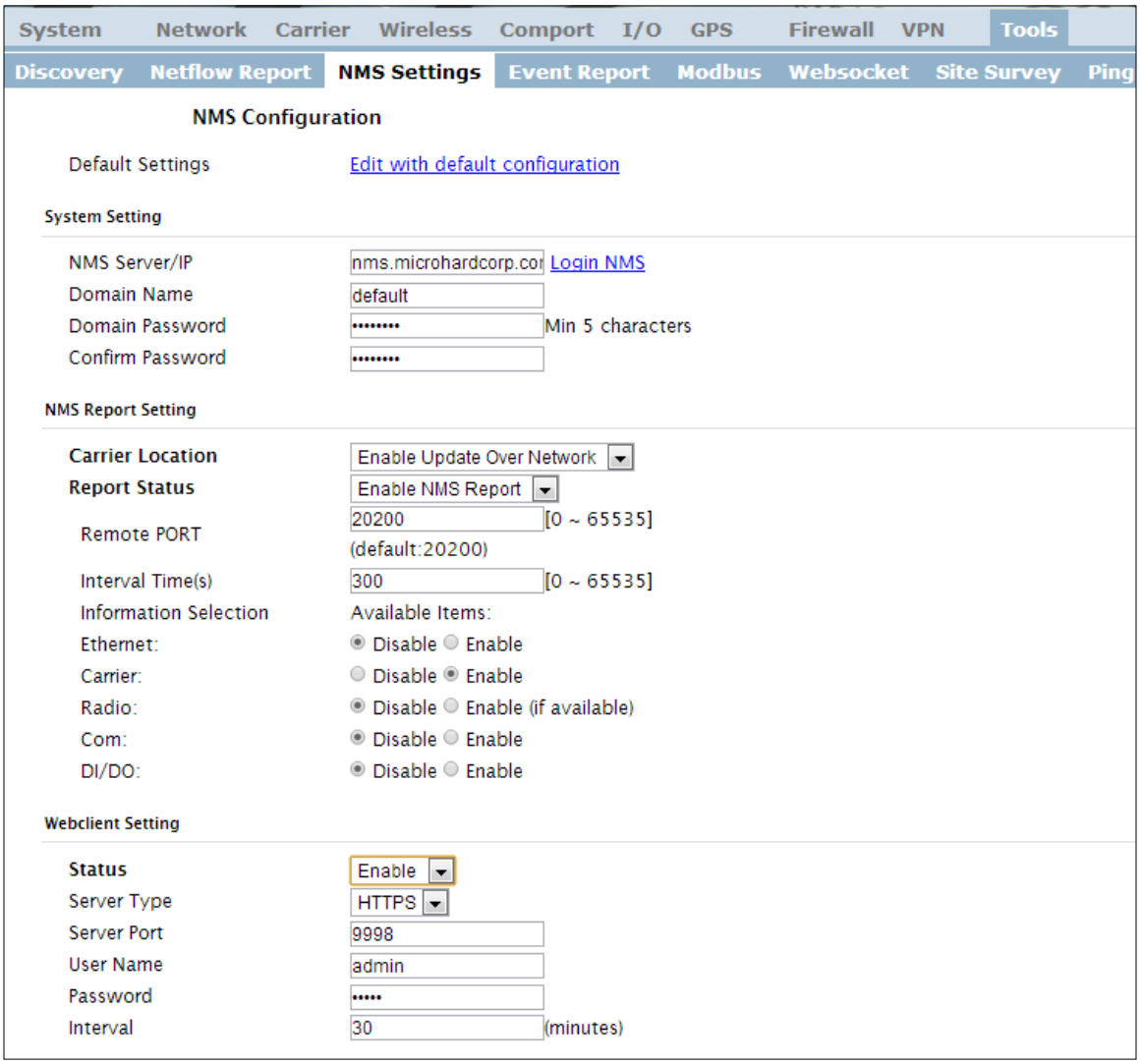


Image 4-10-4: NMS Settings

4.0 Configuration

Network Management System (NMS) Configuration

Default Settings

The default Settings link will reset the configuration form to the default factory values. The form still needs to be submitted before any changes will occur.

NMS Server/IP

The default server address for NMS is nms.microhardcorp.com. The NMS can also be hosted privately, and if that is the case, enter the address here.

Values (IP/Name)

nms.microhardcorp.com

Domain Name / Password

This is the domain name and password that was registered on the NMS website, it must be entered to enable reporting to the NMS system.

Values (chars)

default

NMS Report Setting

Carrier Location

Enable or Disable location estimation via carrier connection. When enabled, the IPn4G will consume some data to retrieve location information from the internet.

Values (chars)

Disable/Enable

Report Status

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

Values (chars)

Enable NMS Report
Disable NMS Report

Remote Port

This is the port to which the UDP packets are sent, and the NMS system is listening on. Ensure this matches what is configured on NMS. The default is 20200.

Values (UDP Port#)

20200

Interval(s)

The Interval defines how often data is reported to NMS. The more often data is reported, the more data is used, so this should be set according to a user's data plan. (0 to 65535 seconds)

Values (seconds)

300

4.0 Configuration

Information Selection

The IPn4G can report information about the different interfaces it has. By default the IPn4G is set to send information about the Carrier, such as usage and RSSI. Statistical and usage data on the Radio (WiFi), Ethernet and Serial interfaces can also be reported.

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

Values (check boxes)

Ethernet
Carrier
Radio
COM
DI / DO

Webclient Setting

Status

The Web Service can be enabled or disabled. This service is used to remotely control the IPn4G. 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 IPn4G checks with the NMS System to determine if there are any tasks to be completed. Carrier data will be consumed every time the device probes the NMS system.

Values (min)

60

4.0 Configuration

4.10.4 Tools > Event Report

4.10.4.1 Event Report > Configuration

Event Reporting allows the IPn4G to send periodic updates via UDP packets. These packets are customizable and can be sent to up to 3 different hosts, and at a programmable interval. The event packet can report information about the modem such as the hardware/ software versions, core temperature, supply voltage, etc; carrier info such as signal strength (RSSI), phone number, RF Band; or about the WAN such as if the assigned IP Address changes. All events are reported in binary.

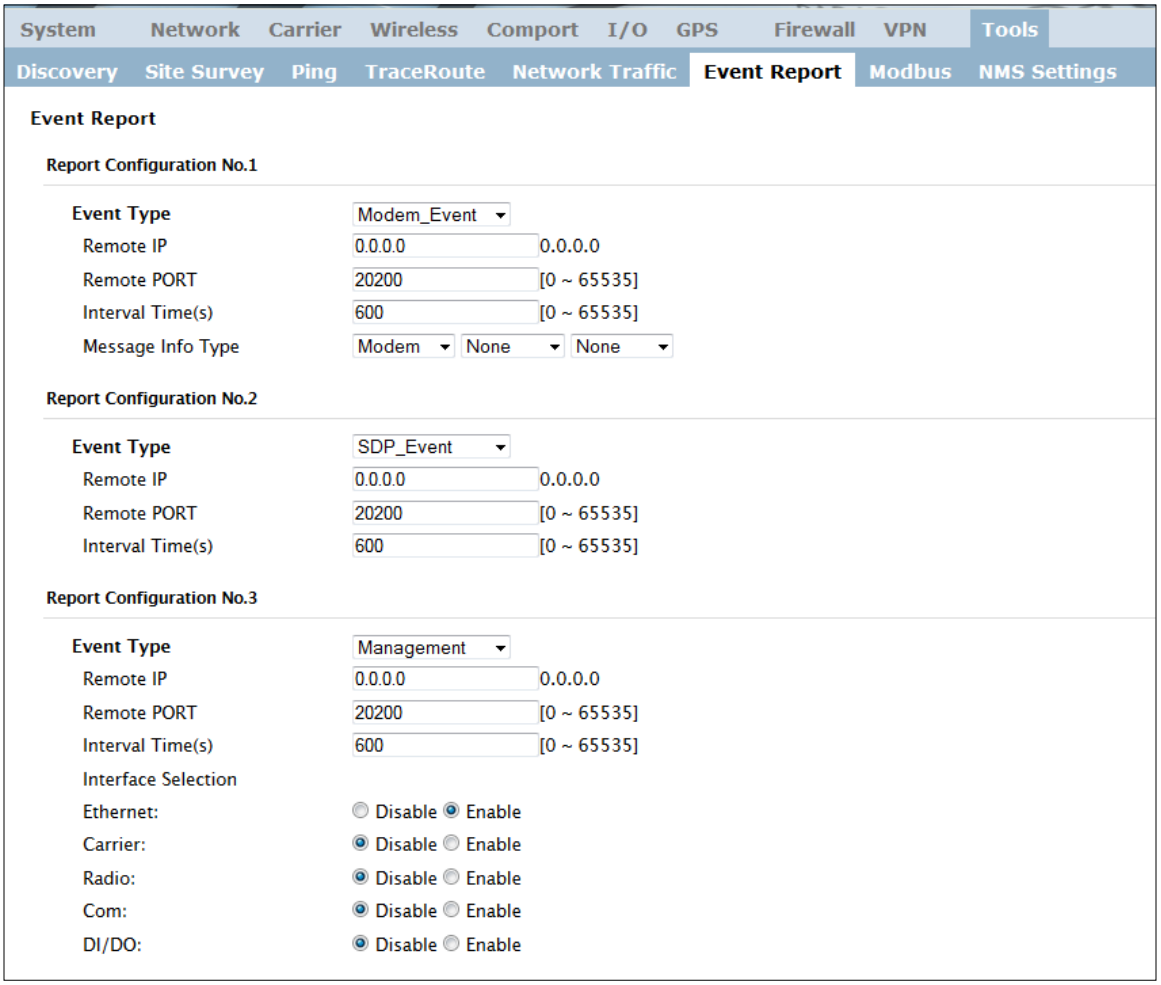


Image 4-10-5: Tools > Event Report

Event Type	Values (selection)
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.	Modem_Event SDP_Event Management

4.0 Configuration

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 (Port #)** **20200**

Interval Time(s)	
This is the interval time in seconds, that the IPn4G will send the configured UDP message to the Remote IP and Port specified.	**Values (seconds)** **600**

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

4.10.4.2 Event Report > Message Structure

Modem_event message structure

- fixed header (fixed size 20 bytes)
- Modem ID (uint64_t (8 bytes))
- Message type mask (uint8_t(1 byte))
- reserved
- packet length (uint16_t(2 bytes))

Note: packet length = length of fixed header + length of message payload.

Message type mask

Modem info -	2 bits 00 no 01 yes (0x1)
Carrier info -	2 bits 00 no 01 yes (0x4)
WAN Info -	2 bits 00 no 01 yes (0x10)

sdp_event message structure

- spd_cmd (1 byte(0x01))
- content length (1 byte)
- spd_package - same as spd response inquiry package format

4.0 Configuration

4.10.4.3 Event Report > Message Payload

Modem info:

Content length	-	2 BYTES (UINT16_T)
Modem name	-	STRING (1-30 bytes)
Hardware version	-	STRING (1-30 bytes)
Software version	-	STRING (1-30 bytes)
Core temperature	-	STRING (1-30 bytes)
Supply voltage	-	STRING (1-30 bytes)

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.

4.0 Configuration

4.10.5 Tools > Modbus

4.10.5.1 Modbus > TCP Modbus

The IPn4G can be configured to operate as a TCP/IP or Serial (COM) Modbus slave and respond to Modbus requests and report various information as shown in the Data Map.

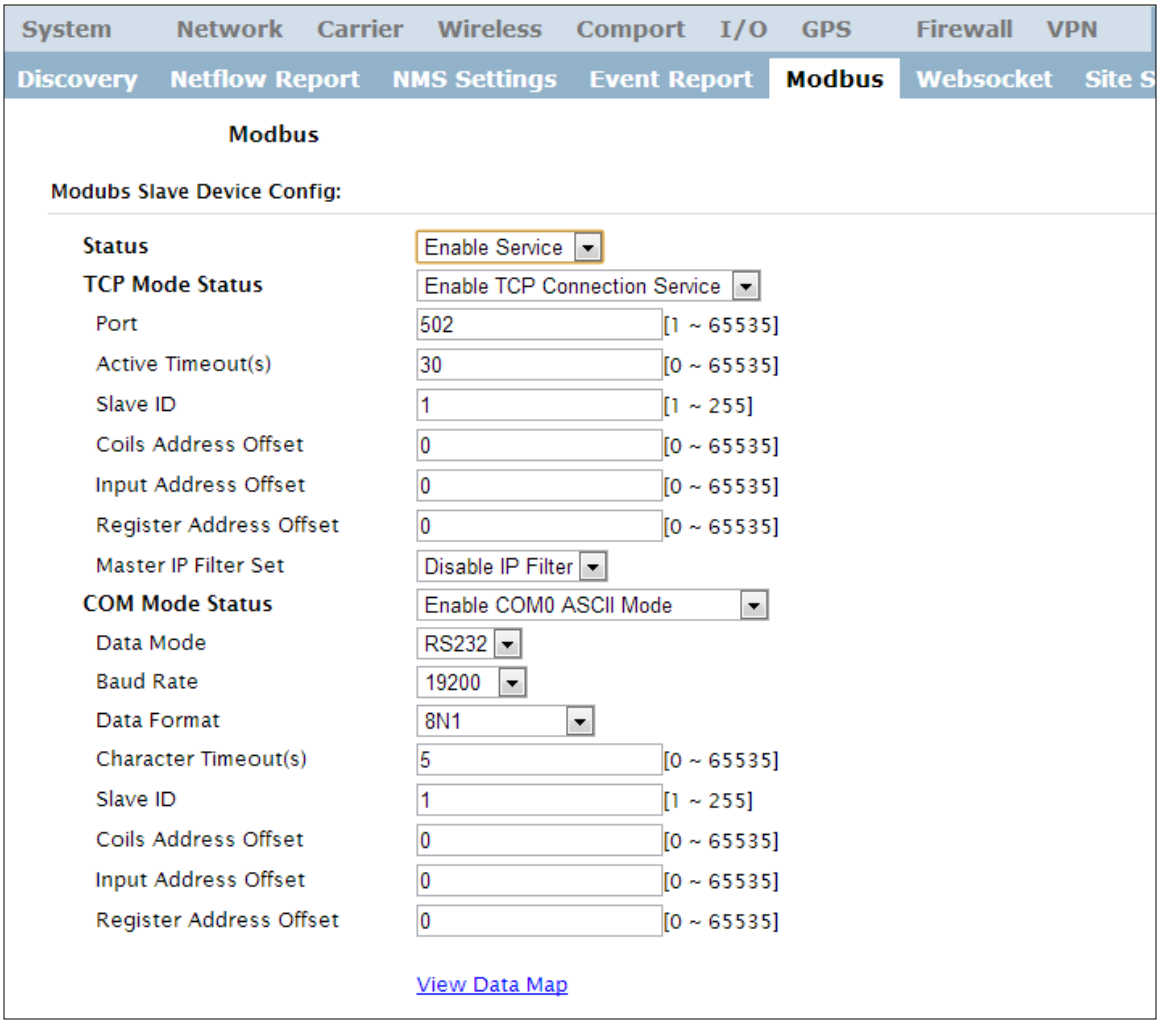


Image 4-10-6: Modbus

Status	Values (selection)
Disable or enable the Modbus service on the IPn4G.	**Disable Service** Enable Service

4.0 Configuration

TCP Mode Status	
Disable or enable the Modbus TCP Connection Service on the IPn4G.	**Values (selection)** **Disable** **Enable**

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

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

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

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

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

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

Master IP Filter Set	
It is possible to only accept connections from specific Modbus Master IP's, to use this feature enable the Master IP Filter and specify the IP Addresses in the fields provided.	**Values (selection)** **Disable /** Enable

4.0 Configuration

4.10.5.2 Modbus > COM (Serial) Modbus

The IPn4G can also participate in serial based Modbus, to configure and view the serial Modbus settings, the COM1 port must first be disabled in the ***Comport > Settings*** menu. Only the settings that are different from TCP Modbus will be discussed.

COM Mode Status	Enable COM ASCII Mode	
Data Mode	RS232	
Baud Rate	19200	
Data Format	8N1	
Character Timeout(s)	5	[0 ~ 65535]
Slave ID	1	[1 ~ 255]
Coils Address Offset	0	[0 ~ 65535]
Input Address Offset	0	[0 ~ 65535]
Register Address Offset	0	[0 ~ 65535]

Image 4-10-7: Tools > 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	57600	14400	3600
460800	38400	**9600**	2400
230400	28800	7200	1200
115200	19200	4800	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	8O1	7E1
8N2	7N1	7O1
8E1	7N2	7E2
		7O2

4.0 Configuration

4.10.5.3 Modbus > Modbus Data Map

Modbus Data Map

Coil Bits (Output and Internal Status):

Bit Address	Hex Format	Definition
0	0x0000	OUTPUT 1
1	0x0001	OUTPUT 2
2	0x0002	OUTPUT 3
3	0x0003	OUTPUT 4
9	0x0009	COM2 Status
12	0x000c	LAN/eth0 Status
13	0x000d	WAN/eth1 Status
16	0x0010	Carrier Status
18	0x0012	Wifi Status
22	0x0016	GPS Status
23	0x0017	Location Over Network
24	0x0018	Event UDP Report 1
25	0x0019	Event UDP Report 2
26	0x001a	Event UDP Report 3
27	0x001b	NMS Report
28	0x001c	Web Client Service
29	0x001d	Firewall Status
40	0x0028	SYSTEM Reboot

Input Bits:

Bit Address	Hex Format	Definition
0	0x0000	INPUT 1
1	0x0001	INPUT 2
2	0x0002	INPUT 3
3	0x0003	INPUT 4

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)
8	0x0008	Core Temperature(C)
9	0x0009	Carrier Received Bytes(MB)
10	0x000a	Carrier Transmitted Bytes(MB)
11	0x000b	GPS Altitude(m)
12	0x000c	GPS Latitude High 2 Bytes
13	0x000d	Latitude Low 2 Bytes(x1000000)
14	0x000e	GPS Longitude High 2 Bytes
15	0x000f	Longitude Low 2 Bytes(x1000000
18	0x0012	COM2 Baud Rate(/100)(bps)
19	0x0013	COM2 Data Format...

Modem Model Types:

Type ID	Definition
0	Unknow
6	IPn3G
7	VIP4G
8	IPn4G

Com Data Format Definition:

Com Data Format Definition:

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

Image 4-10-8: Tools > Modbus Data Map

4.0 Configuration

4.10.6 Tools > Websocket

The Websocket service is a feature of HTML5.0 or later. Web Socket is designed to be implemented in web browsers and web servers to allow XML scripts to access the HTML web service with a TCP socket connection.

It is mainly used for two purposes:

- refreshing page information without refreshing the entire page to reduce network stream.
- to integrate internet applications with xml to get required information in real time.

Currently we provide four types of information as configured:

- GPS Coordinate Information
- GPS NMEA Data
- Carrier Information
- Comport Data

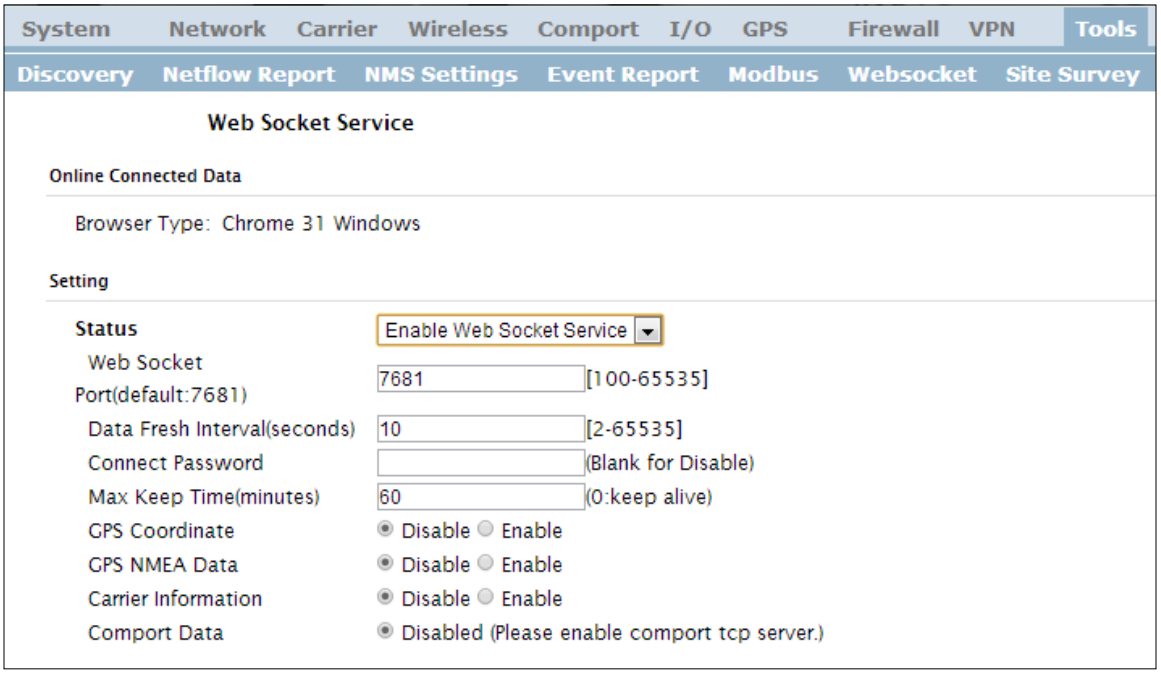


Image 4-10-9: Tools > Web Socket Service

Status	
Enable or disable the web socket service in the IPn4G.	**Values (selection)** Enable / **Disable**

Web Socket Port	
Enter the desired web socket TCP port number. The default is 7681, and the valid range is 100 to 65535.	**Values (TCP port)** **7681**

4.0 Configuration

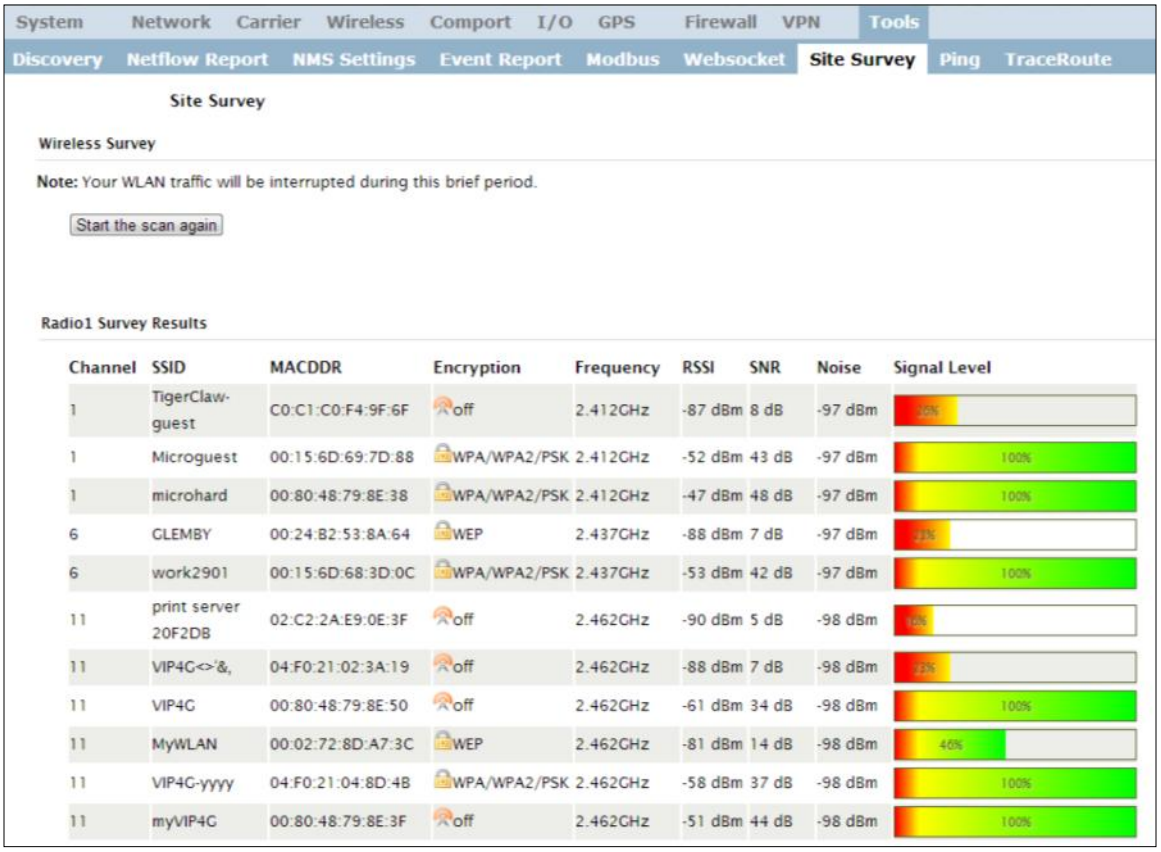
Data Fresh Intervals	
Enter in the time at which data is to be refreshed. The default is 10 seconds, the valid range is 2 to 65535 seconds.	**Values (seconds)** 10
Connect Password	
For added security a password can be required to connect to the web socket service. To disable, leave this field blank. The default is disabled.	**Values** *(blank)*
Max Keep Time	
This field determines how long the web socket is open once started/ enabled. The default is 60 mins, a value of zero means the service with continue to run indefinitely.	**Values (minutes)** **60**
GPS Coordinate	
If enabled the IPn4G will report GPS coordinate data to the websocket.	**Values (selection)** **Disable** / Enable
GPS NMEA Data	
If enabled the IPn4G will report GPS NMEA data to the websocket.	**Values (selection)** **Disable** / Enable
Carrier Information	
If enabled the IPn4G will report carrier information to the websocket.	**Values (selection)** **Disable** / Enable
Comport Data	
If enabled, and the COM1 port is configured for TCP Server, the comport data will be reported to the web socket.	**Values (selection)** **Disable** / Enable

4.0 Configuration

4.10.7 Tools > Site Survey

Wireless Survey

The Wireless Survey feature will scan the available wireless channels for any other 802.11 wireless networks in proximity to the IPn4G. The Survey will display the Channel number the other networks are operating on, the MAC address, Encryption Type, Frequency and general signal level and quality information. This can be useful for finding available networks, or troubleshooting connection and sensitivity problems. If there are other networks operating on the same frequency, or a channel close to the one chosen, it can then be decided to try to use another channel.



Channel	SSID	MACDDR	Encryption	Frequency	RSSI	SNR	Noise	Signal Level
1	TigerClaw-guest	C0:C1:C0:F4:9F:6F	off	2.412GHz	-87 dBm	8 dB	-97 dBm	25%
1	Microguest	00:15:6D:69:7D:88	WPA/WPA2/PSK	2.412GHz	-52 dBm	43 dB	-97 dBm	100%
1	microhard	00:80:48:79:8E:38	WPA/WPA2/PSK	2.412GHz	-47 dBm	48 dB	-97 dBm	100%
6	CLEMBY	00:24:B2:53:8A:64	WEP	2.437GHz	-88 dBm	7 dB	-97 dBm	21%
6	work2901	00:15:6D:68:3D:0C	WPA/WPA2/PSK	2.437GHz	-53 dBm	42 dB	-97 dBm	100%
11	print server 20F2DB	02:C2:2A:E9:0E:3F	off	2.462GHz	-90 dBm	5 dB	-98 dBm	16%
11	VIP4G<>'&,	04:F0:21:02:3A:19	off	2.462GHz	-88 dBm	7 dB	-98 dBm	23%
11	VIP4G	00:80:48:79:8E:50	off	2.462GHz	-61 dBm	34 dB	-98 dBm	100%
11	MyWLAN	00:02:72:8D:A7:3C	WEP	2.462GHz	-81 dBm	14 dB	-98 dBm	46%
11	VIP4G-yyyy	04:F0:21:04:8D:4B	WPA/WPA2/PSK	2.462GHz	-58 dBm	37 dB	-98 dBm	100%
11	myVIP4G	00:80:48:79:8E:3F	off	2.462GHz	-51 dBm	44 dB	-98 dBm	100%

Image 4-10-10: Tools > Site Survey

4.0 Configuration

4.10.8 Tools > Ping

Network Tools Ping

The Network Tools Ping feature provides a tool to test network connectivity from within the IPn4G unit. A user can use the Ping command by entering the IP address or host name of a destination device in the Ping Host Name field, use Count for the number of ping messages to send, and the Packet Size to modify the size of the packets sent.

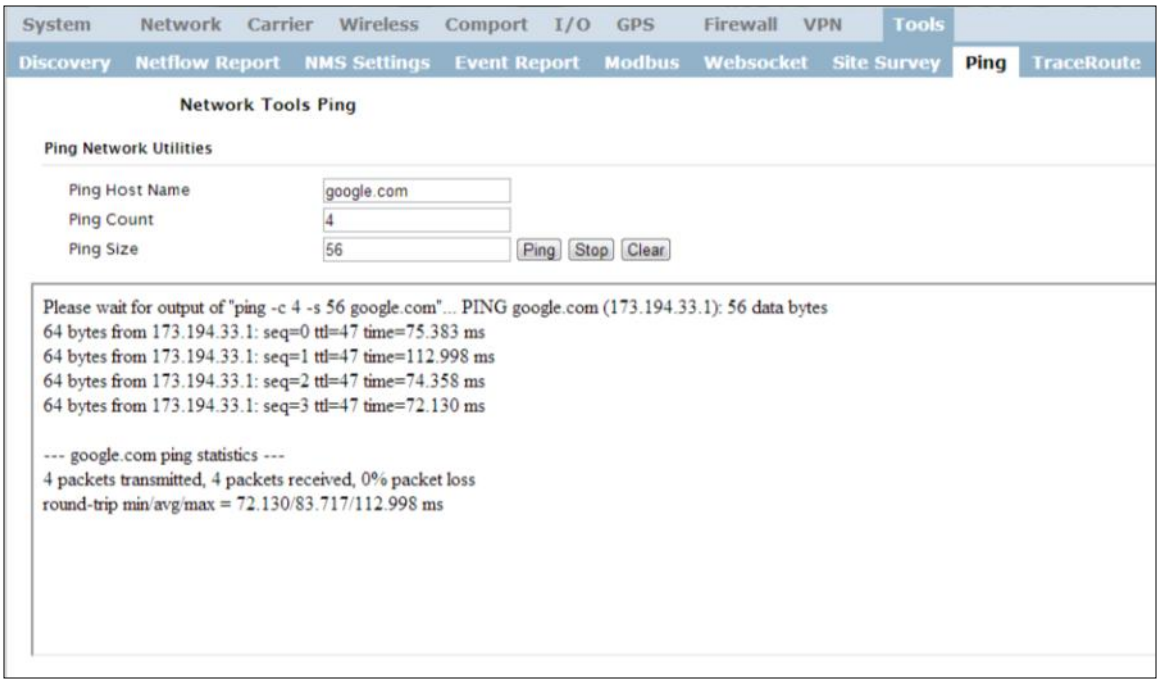


Image 4-10-11: Tools > Ping

4.0 Configuration

4.10.9 Tools > TraceRoute

Network TraceRoute

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

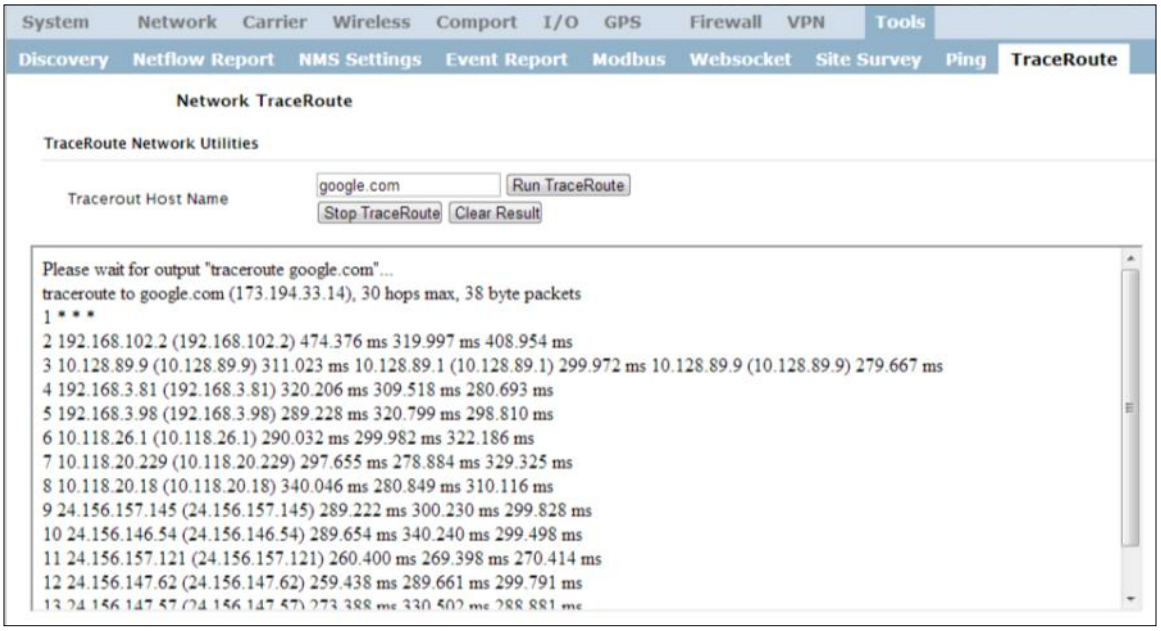


Image 4-10-12: Tools > TraceRoute

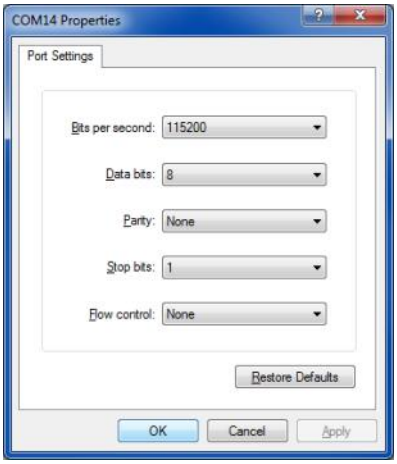
5.0 AT Command Line Interface

5.1 AT Command Overview

AT Commands can be issued to configure and manage the IPn4G, via the front serial port (COM1), or by TCP/IP (telnet).

5.1.1 Serial Port

To connect and access the AT Command interface on the IPn4G, a physical connection must be made on the RS232 DB9 serial port on the front of the IPn4G labeled 'COM1'. A terminal emulation program (Hyperterminal, Tera Term, ProComm, Putty etc) can then be used to communicate with the IPn4G. The port settings of this port can be modified by changing the settings of COM1, in the configuration menus.



Default Settings:

Baud rate: **115200**

Data bits: **8**

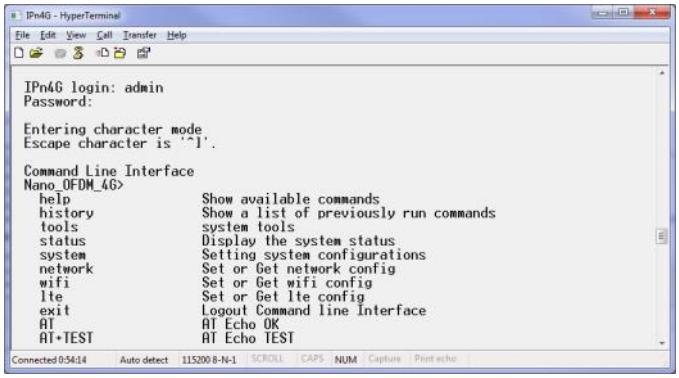
Parity: **None**

Stop Bits: **1**

Flow Control: **None**

Image 5-1: COM1 Port Settings

Once communication is established, a login is required to access the AT Command interface, once logged in, the AT Command Line Interface menu is displayed. Type "?" or Help to list the menu commands.



Default Settings:

IPn4G login: **admin**

Password: **admin**

Image 5-2: AT Command Window

5.0 AT Command Line Interface

5.1.2 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the IPn4G. The default port is TCP Port 23. A telnet session can be made to the unit using any Telnet application (Windows Telnet, Tera Term, ProComm etc). Once communication is established, a login is required to continue.

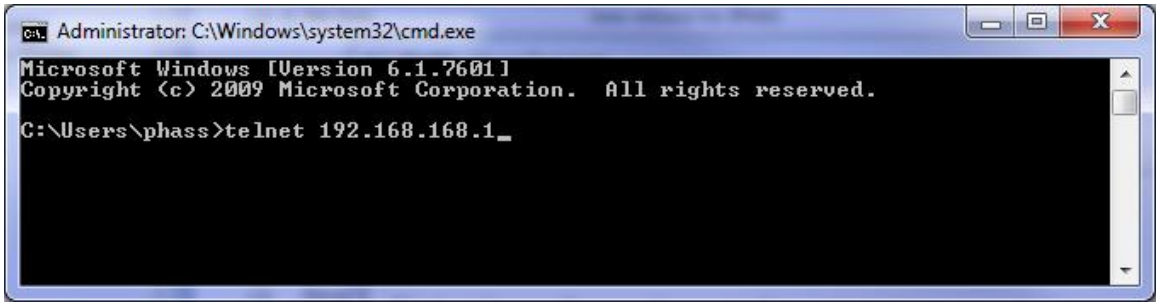


Image 5-3: Establishing a Telnet Session

A session can be made to the WAN IP Address (if allowed in the firewall settings) for remote configuration, or to the local RJ45 interface (default IP: 192.168.168.1).

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. (Type “?” or Help to list the commands)

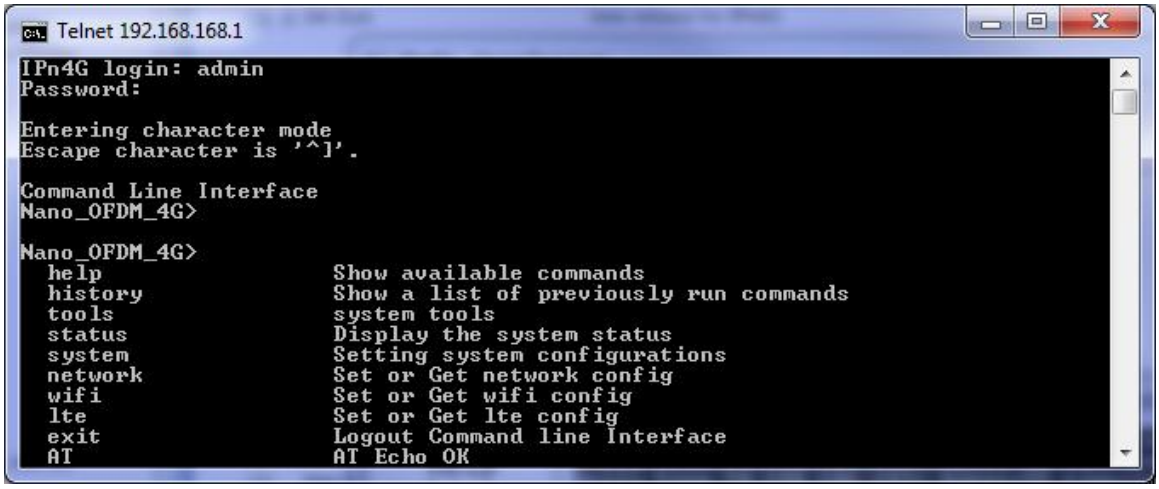


Image 5-4: Telnet AT Command Session

5.0 AT Command Line Interface

5.2 AT Command Syntax

The follow syntax is used when issuing AT Commands on the IPn4G

- 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:

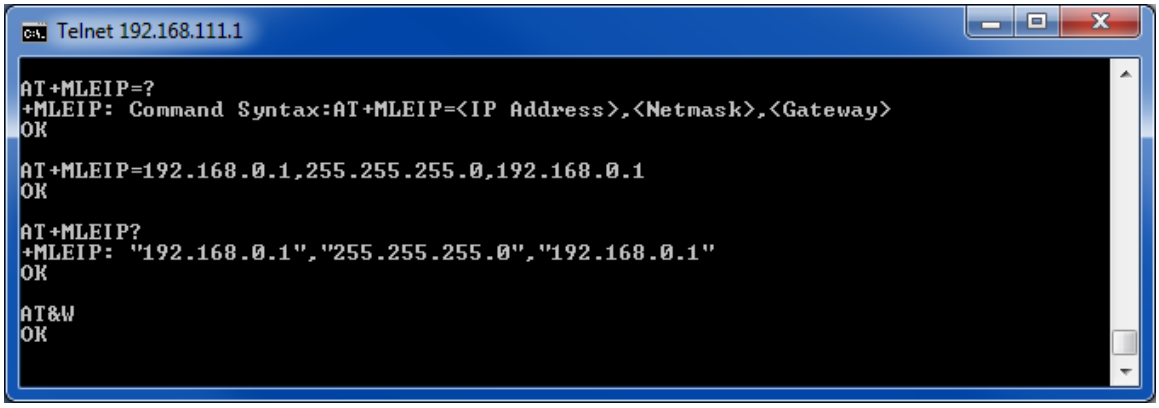


Image 5-5: Telnet AT Command Syntax

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.

5.0 AT Command Line Interface

5.3 Supported AT Commands

AT

Description	Command Syntax
Echo OK.	**AT <enter>**

Example

Input:
AT <enter>
Response:
OK

AT+TEST

Description	Command Syntax
Echo TEST	**AT+TEST <enter>**

Example

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

ATH

Description	Command Syntax
Show a list of previously run commands.	**ATH <enter>**

Example

Input:
ATH <enter>
Response:
AT Command history: 1. ATH 2. ATL 3. ATH

AT&R

Description	Command Syntax
Read modem profile to editable profile. (Reserved)	**AT&R <enter>**

Example

Input:
AT&R <enter>
Response:
OK

5.0 AT Command Line Interface

AT&V

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

Example

Input:
AT&V <enter>
Response:
&V:
  hostname:IPn4G
  timezone:MST7MDT,M3.2.0,M11.1.0
  systemmode:gateway
  time mode:sync
OK

AT&W

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

Example

Input:
AT&W <enter>
Response:
OK

AT+MREB

Description	Command Syntax
Reboots the modem.	**AT+MREB <enter>**

Example

Input:
AT+MREB <enter>
Response:
OK. Rebooting...

5.0 AT Command Line Interface

ATA

Description

Quit. Exits AT Command session and returns you to login prompt.

Command Syntax

ATA <enter>

Example

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

ATO

Description

Quit. Exits AT Command session and returns you to login prompt.

Command Syntax

ATO <enter>

Example

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

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=4035553776 <enter>

4035553776 Test <ctrl+z>

Response:
OK

5.0 AT Command Line Interface

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+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=1 <enter>

Response:
AT+CMGL=1
+CMGL: 0,"REC READ","+14035553776",,"2013/10/04,11:12:27-06"
Test Message 1
+CMGL: 1,"REC READ","+14035553776",,"2013/10/04,11:12:53-06"
Test Message 2
+CMGL: 2,"REC READ","+14035553776",,"2013/10/04,11:13:06-06"
Another test message!

OK

5.0 AT Command Line Interface

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+GMR

Description

Modem Record Information

Command Syntax

AT+GMR <enter>

Example

Input:
AT+GMR <enter>
Response:
+GMR:
 Hardware Version:v1.0.0 Software Version:v1.1.0 build 1060
 Copyright: 2012 Microhard Systems Inc.
 System Time: Mon Dec 2 16:03:51 2013
OK

AT+GMI

Description

Get Manufacturer Identification

Command Syntax

AT+GMI=<enter>

Example

Input:
AT+GMI<enter>

Response:
+GMI: 2012 Microhard Systems Inc.
OK

5.0 AT Command Line Interface

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:012773002108403, IMSI:302720406982933
OK

AT+CCID

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

Example

Input:
AT+CCID<enter>
Response:
+CCID: 89302720401025355531
OK

5.0 AT Command Line Interface

AT+MSYSI

Description

System Summary Information

Command Syntax

AT+MSYSI <enter>

Example

Input:
AT+MSYSI <enter>
Response:
Carrier:
IMEI:012773002108403
SIMID:89302720401025355531
IMSI:302720406982933
Phone Num: +15878938645
Status: CONNECTED
Network: ROGERS
RSSI:WCDMA RSSI : 57
Temperature:61 degC
Ethernet Port:
MAC:00:0F:92:00:B5:EE
IP:192.168.168.1
MASK:255.255.255.0
Wan MAC:00:A0:C6:00:00:00
Wan IP:74.198.186.197
Wan MASK:255.255.255.252
System:
Device:IPn4G
Product:IPn4G+WIFI
Image:IPn4G
Hardware:v1.0.0
Software:v1.1.0 build 1060

Copyright: 2012 Microhard Systems Inc.
Time: Mon Dec 2 16:14:44 2013

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

AT+MMNAME

Description

Modem Name / Radio Description. 30 chars.

Command Syntax

AT+MMNAME=<modem_name>

Example

Input: (To set value)
AT+MMNAME=IPn4G_CLGY<enter>
Response:
OK

Input: (To retrieve value)
AT+MMNAME=?<enter>
Response:
+MMNAME: IPn4G_CLGY
OK

5.0 AT Command Line Interface

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=192.168.168.1,255.255.255.0,192.168.168.1 <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=192.168.168.100,192.168.168.200 <enter>
Response:
OK

5.0 AT Command Line Interface

AT+MEMAC

Description

Retrieve the MAC Address of the local Ethernet interface.

Command Syntax

AT+MEMAC <enter>

Example

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

AT+MSIP

Description

Set LAN static IP

Command Syntax

AT+MSIP=<static IP address> <enter>

Example

Input:
AT+MSIP=192.168.168.1 <enter>
Response:
+MSIP: setting and restarting network...
OK

AT+MSCT

Description

Set LAN Connection Type.

Command Syntax

AT+MSCT=<Mode>
Mode:
0 DHCP
1 Static IP

Example

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

5.0 AT Command Line Interface

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+MPIPP

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

Description

Enable/Disable IP-Passthrough

Command Syntax

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

Example

Input:
AT+MPIPP=1 <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)

Example

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

5.0 AT Command Line Interface

AT+MRTF

Description

Reset the modem to the factory default settings stored in non-volatile (NV) memory. Unit will reboot with default settings.

Command Syntax

AT+MRTF <action>
Action:
0 pre-set action
1 confirm action
OK

Example

Input:
AT+MRTF=1 <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=<Mode>[,<Interval_s>,<Reboot Time Limit_s>]
Mode:
0 Disable
1 Enable
Reboot Time Limit:300-60000

Example

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

AT+MSCMD

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.

Example

Input:
AT+MSCMD=1,1,403556767,4057890909<enter>
Response:
OK

Command Syntax

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

5.0 AT Command Line Interface

AT+MDISS

Description

Configure discovery mode service used by IPn4G and utilities such as “IP Discovery”.

Command Syntax

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

Example

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

AT+MPWD

Description

Used to set or change the ADMIN password for the IPn4G.

Command Syntax

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

Example

Input:
AT+MPWD=admin,admin<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

5.0 AT Command Line Interface

AT+MIKAC

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

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

Description

Select DDNS service provider, and login credentials as required for DDNS services.

Command Syntax

AT+MDDNS=<service type>,<host>,<user name>,<password>
service type:
0 changeip
1 dyndns
2 eurodyndns
3 hn
4 noip
5 ods
6 ovh
7 regfish
8 tzo
9 zoneedit

Example

Input:
AT+MDDNS=0,user.dydns.org,user,password <enter>
Response:
OK

5.0 AT Command Line Interface

AT+MEURD1
AT+MEURD2
AT+MEURD3

Description

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

Example

Input:
AT+MIKAC=www.google.com,600,10<enter>
Response:
OK

Command Syntax

AT+MEURD1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Ti me_s>]
Mode:
0 Disable
1 Moden Event Report
2 SDP Event Report
3 Management Report

AT+MNMSR

Description

Define NMS Report.

Example

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

Command Syntax

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

AT+MGPSR1
AT+MGPSR2
AT+MGPSR3
AT+MGPSR4

Description

Define GPS Report No.1/2/3/4.

Example

Input:
AT+MGPSR1=1,192.168.168.25,20175,600 <enter>
Response:
OK

Command Syntax

AT+MGPSR1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Ti me_s>]
Mode:
0 Disable
1 Enable UDP Report

5.0 AT Command Line Interface

AT+MIS

Description

Module Input Status.

Command Syntax

AT+MIS

Example

Input:
AT+MIS <enter>
Response:
+MIS: available input status
INPUT 1: 0 open
OK

AT+MOS

Description

Module Output Status.

Command Syntax

AT+MOS=<Mode>[,<Setting No.>,<Status>]
Mode:
0 All Output Status
1 Output Setting
Setting No.: 1, 2, 3, 4(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:
OK

5.0 AT Command Line Interface

ATL

Description

Lists all available AT Commands.

Command Syntax

ATL <enter>

Example

ATL <enter>

AT Commands available:

AT	AT Echo OK
AT+TEST	AT Echo TEST
ATH	Show a list of previously run AT commands
ATL	List all available AT commands
AT&R	Reserved
AT&V	Display modem active profile
AT&W	Reserved
AT+MREB	Reboot the modem
ATA	Quit
ATO	Quit
AT+CMGS	Send SMS
AT+CMGR	Read SMS with changing status
AT+CMGL	List SMSs with changing status
AT+CMGD	Delete SMSs
AT+GMR	Modem Record Information
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+MSYSI	System summary information
AT+MMNAME	Modem Name Setting
AT+MLEIP	Set the IP address of the modem LAN 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+MSIP	Set LAN static IP
AT+MSCT	Set LAN Connection Type
AT+MNTP	Define NTP server
AT+MPIPP	Enable or disable IP-Passthrough
AT+MCNTO	Set console timeout
AT+MRTF	Reset the modem to the factory default settings from non-volatile (NV) memory
AT+MTWT	Enable or disable traffic watchdog timer used to reset the modem
AT+MSCMD	Enable or disable system sms command service
AT+MDISS	Set discovery service used by the modem
AT+MPWD	Set password
AT+MIKACE	Enable or disable ICMP keep-alive check
AT+MIKAC	Set ICMP keep-alive check
AT+MDDNSE	Enable or disable DDNS
AT+MDDNS	Set DDNS
AT+MEURD1	Define Event UDP Report No.1
AT+MEURD2	Define Event UDP Report No.2
AT+MEURD3	Define Event UDP Report No.3
AT+MNMSR	Define NMS Report
AT+MGPSR1	Define GPS Report No.1
AT+MGPSR2	Define GPS Report No.2
AT+MGPSR3	Define GPS Report No.3
AT+MGPSR4	Define GPS Report No.4

5.0 AT Command Line Interface

AT+MIS	Module Input status
AT+MOS	Module Output status and setting

Appendix A: Serial Interface

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

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

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

The signals in the asynchronous serial interface are described below:

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

Appendix B: IP-Passthrough Example (Page 1 of 2)

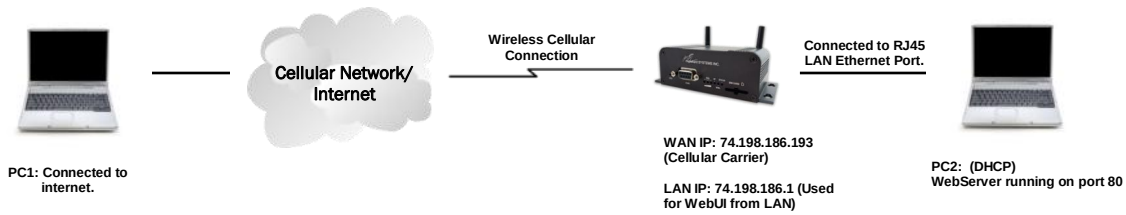
By completing the Quick Start process, a user should have been able to log in and set up the IPn4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, a common application of the IPn4G is to access connected devices remotely. In order to do this, the IPn4G 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 IPn4G and the connected device/PC to work with IP-Passthrough. IP-Passthrough means that the IPn4G is transparent, and all outside (WAN) traffic is simply sent directly to a single device connected to the physical LAN RJ-45 port on the IPn4G (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 IPn4G.

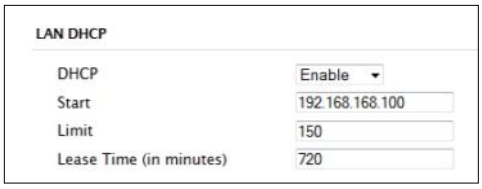
IP-Passthrough is ideal for applications where only a single device is connected to the IPn4G, and other features of the IPn4G are not required. When in pass-through mode, most features of the IPn4G are bypassed, this includes the serial ports, the GPS features, VPN, the Firewall, and much more. The advantage of IP-Passthrough is that the configuration is very simple.

In the example below we have a IPn4G 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 IPn4G, the IPn4G would then automatically assign, via DHCP, the WAN IP to the attached PC2, creating a transparent connection.



Step 1

Log into the IPn4G (Refer to Quick Start), and ensure that DHCP is enabled on the **Network > LAN** page.



Step 2

Since PC2 requires port 80 to be used as its Web server port, port 80 cannot be used on the IPn4G, by default it retains this port for remote configuration. To change the port used by the IPn4G, navigate to the **System > Settings** page as seen below. For this example we are going to change it to port 8080. When changing port numbers on the IPn4G, it is recommended to reboot the unit before continuing, remember the new WebUI port is now 8080 when you log back into the IPn4G. (e.g. 192.168.168.1:8080).

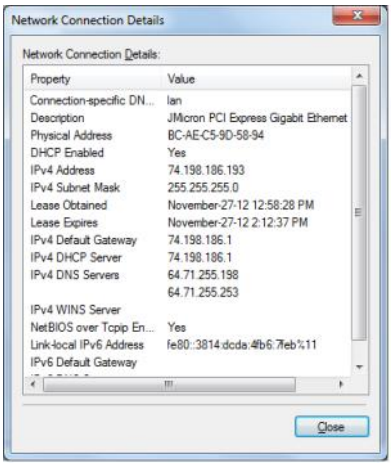
Appendix B: IP-Passthrough Example (Page 2 of 2)

Step 3

Now IP-Passthrough can be enabled on the IPn4G. Under the ***Carrier > Settings*** tab, IP-Passthrough can be found. To enable this feature, select "Ethernet" from the drop down box. Once the changes are applied, whichever device is physically connected to the LAN RJ45 port, will dynamically be assigned the WAN IP Address. In this example, this would be 74.198.186.193.

The default IP address of 192.168.168.1 on the LAN is no longer available, but it is still possible to access and configure the IPn4G 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).

Step 4



Attach the remote device or PC to the RJ45 port of the IPn4G. The end device has to be set up for DHCP to get an IP address from the IPn4G. 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 IPn4G has a IP Address of 74.198.186.193, which is the IP address assign by the cellular carrier for the modem.

Step 5 (Optional)

IP-Passthrough operation can also be verified in the IPn4G. Once IP-Passthrough is enabled you can access the IPn4G WebUI by one of the following methods:

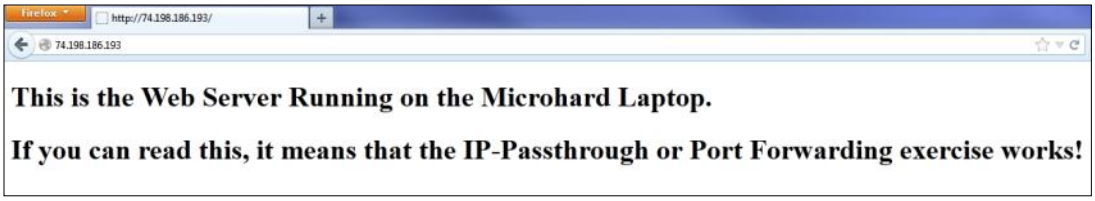
- Remotely on the WAN side (usually the internet), using the WAN IP, and the port specified for HTTP operation (or, if enabled, by using the HTTPS (443) ports), in this example with would be 74.198.186.193:8080.
- On the LAN side, by entering in the first 3 octets of the WAN IP and .1 for the fourth, so in our example 74.198.186.1:8080.

Once logged in, navigate to the ***Carrier > Status*** page. Under WAN IP Address it should look something like shown in the image to the right, 74.198.186.193 on LAN.

Connection Duration	1 min 43 sec
WAN IP Address	74.198.186.193 on LAN
DNS Server 1	64.71.255.198

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 IPn4G. 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 IPn4G into a web browser. As seen below, when the IP Address of the IPn4G is entered, the data is passed through to the attached PC. The screen shot below shows that our test setup was successful.



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

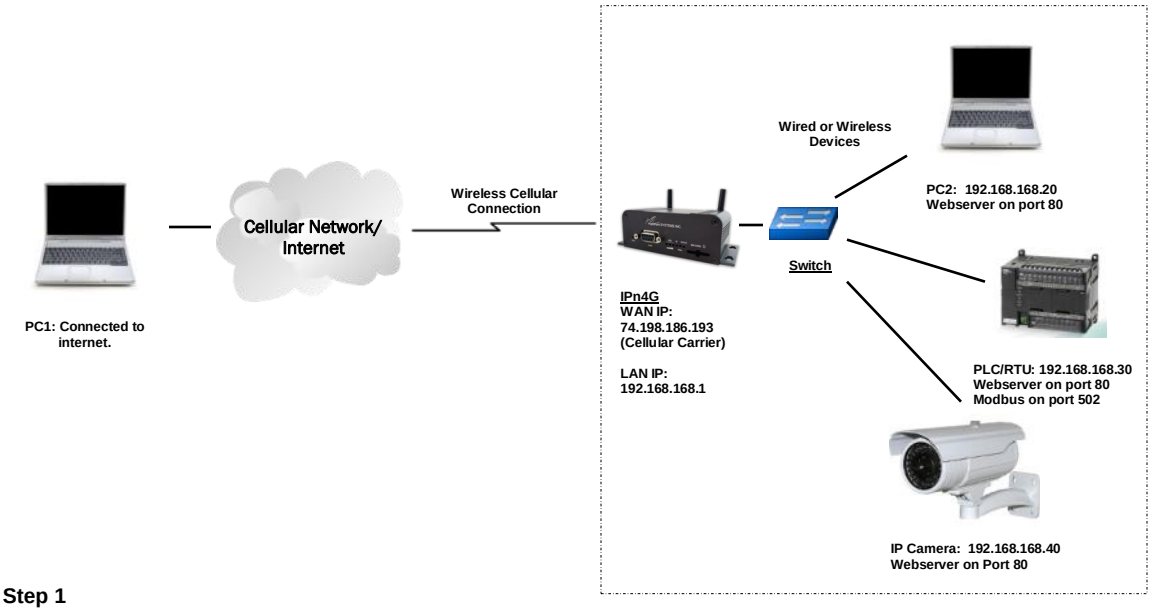
By completing the Quick Start process, a user should have been able to log in and set up the IPn4G to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the IPn4G is to access connected devices remotely. In order to do this, the IPn4G 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 IPn4G, or if other features of the IPn4G are required (Serial Ports, Firewall, GPS, etc). In port forwarding, the IPn4G 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 IPn4G does this with each and every incoming packet.

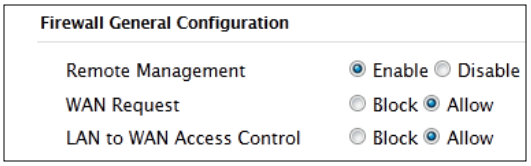
DMZ (a form of port forwarding) is useful for situations where there are multiple devices connected to the IPn4G, but all incoming traffic is destined for a single device. It is also popular to use DMZ in cases where a single device is connected but several ports are forwarded and other features of the IPn4G are required, since in passthrough mode all of these features are lost.

Consider the following example. A user has a remote location that has several devices that need to be accessed remotely. The User at PC1 can only see the IPn4G directly using the public static IP assigned by the wireless carrier, but not the devices behind it. In this case the IPn4G 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 IPn4G.



Step 1

Log into the IPn4G (Refer to Quick Start), and ensure that the ***Firewall*** is enabled. This can be found under ***Firewall > General.*** Also ensure that ***WAN Request*** is set to Allow, which allows traffic to come in from the WAN/4G, or that sufficient ***Rules*** or ***IP lists*** have been setup to allow specific traffic to pass through the IPn4G. Once that is complete, remember to "Submit" the changes.



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

Step 2

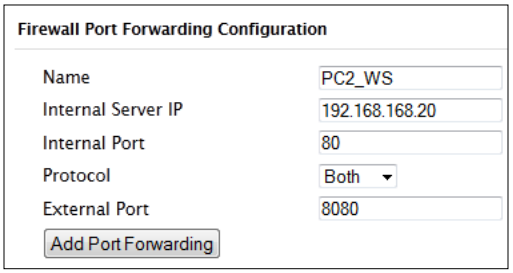
Determine which external ports (WAN) are mapped to which internal IP Addresses and Ports (LAN). It is important to understand which port, accessible on the outside, is connected or mapped to which devices on the inside. For this example we are going to use the following ports, in this case it is purely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

Description	WAN IP	External Port	Internal IP	Internal Port
IPn4G WebUI	74.198.186.193	80	192.168.168.1	80
PC2 Web Server	74.198.186.193	8080	192.168.168.20	80
PLC Web Server	74.198.186.193	8081	192.168.168.30	80
PLC Modbus	74.198.186.193	10502	192.168.168.30	502
Camera Web Server	74.198.186.193	8082	192.168.168.40	80

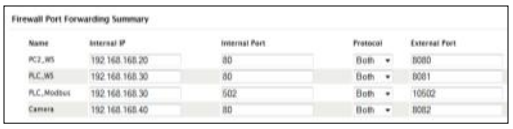
Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this is fine because they are located on different IP addresses, and the different external ports mapped by the IPn4G (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 IPn4G itself. To create port forwarding rules, Navigate to the ***Firewall > Port Forwarding*** menu. When creating rules, each rules requires a unique name, this is only for reference and can be anything desired by the user. Click on the **"Add Port Forwarding"** button to add each rule to the IPn4G.



Once all rules have been added, the IPn4G configuration should look something like what is illustrated in the screen shot to the right. Be sure to **"Submit"** the Port Forwarding list to the IPn4G.



For best results, reboot the IPn4G.

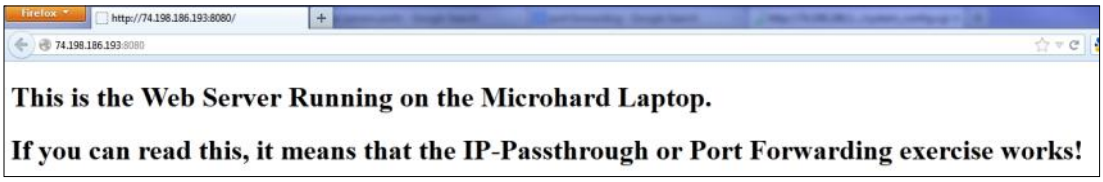
Step 4

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 IPn4G should be accessible remotely. To access the devices:

For the Web Server on the PC, use a browser to connect to 74.198.186:193:8080, in this case the same webserver is running as in the IP-Passthrough example, so the result should be as follows:



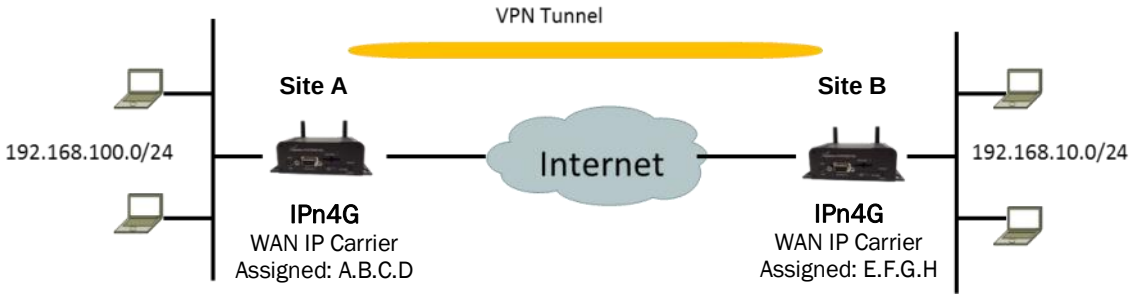
To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.

Appendix D: VPN Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the IPn4G 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 IPn4G is to access connected devices remotely. In addition to Port Forwarding and IP-Passthrough, the IPn4G 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 IPn4G 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 IPn4G devices, each with a public IP address. At least one of the modems require a static IP address. VPN tunnels can also be created using the IPn4G to existing VPN capable devices, such as Cisco or Firebox.

Example: IPn4G to IPn4G (Site-to-Site)



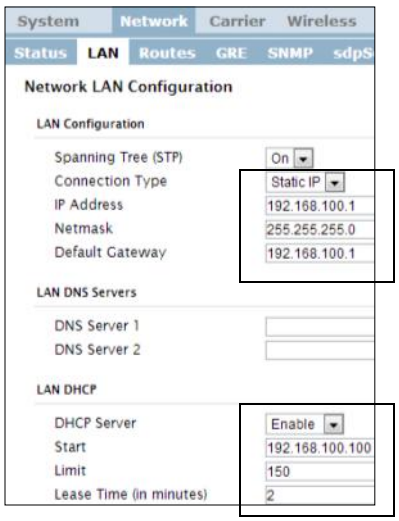
Step 1

Log into each of the IPn4Gs (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 IPn4G. Once that is complete, remember to "Apply" the changes.

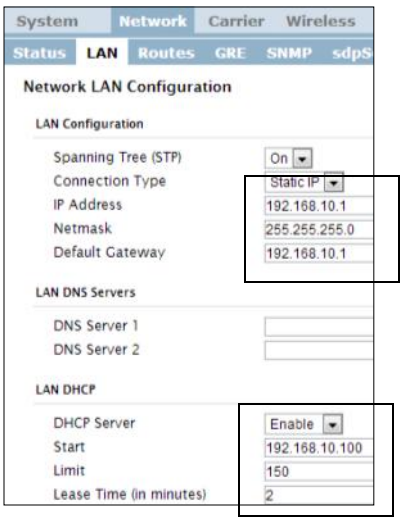
Step 2

Configure the LAN IP and subnet for each IPn4G. The subnets must be different and cannot overlap.

Site A



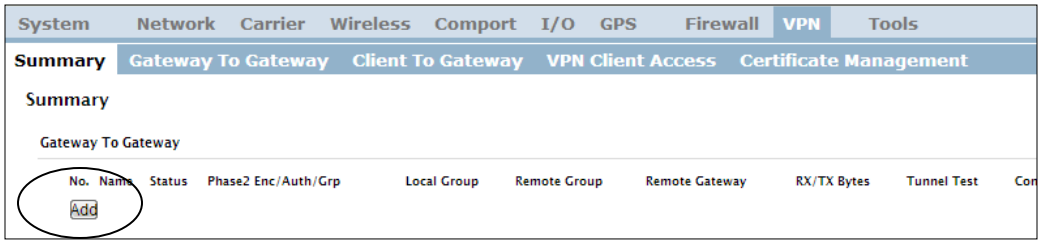
Site B



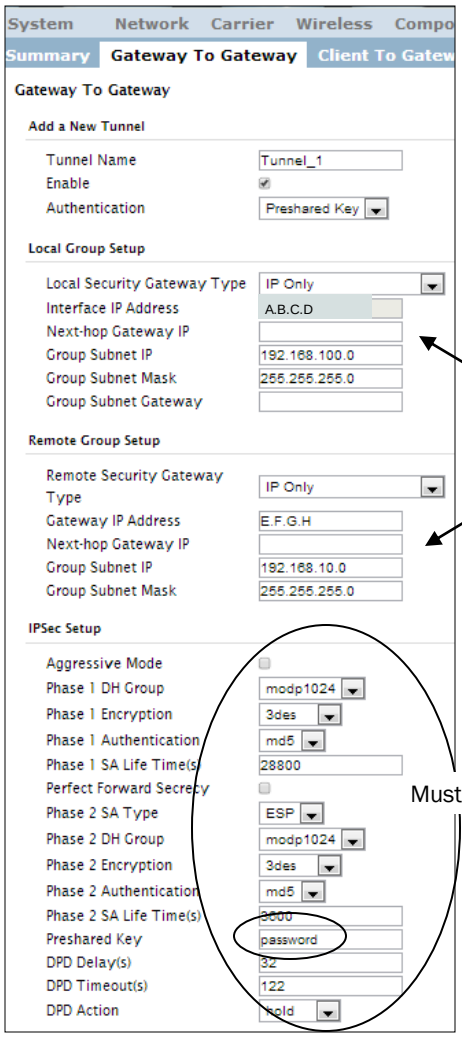
Appendix D: VPN Example (Page 2 of 2)

Step 3

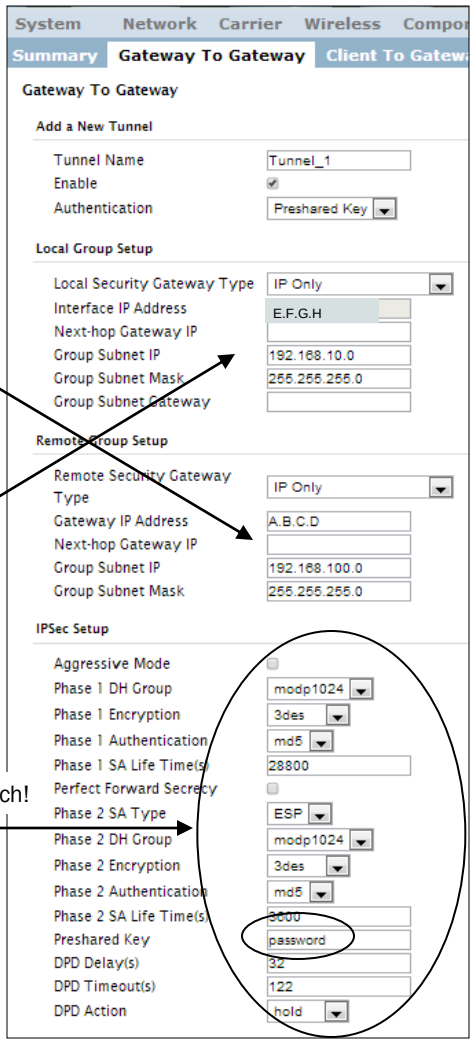
Add a VPN Gateway to Gateway tunnel on each IPn4G.



Site A



Site B



Step 4

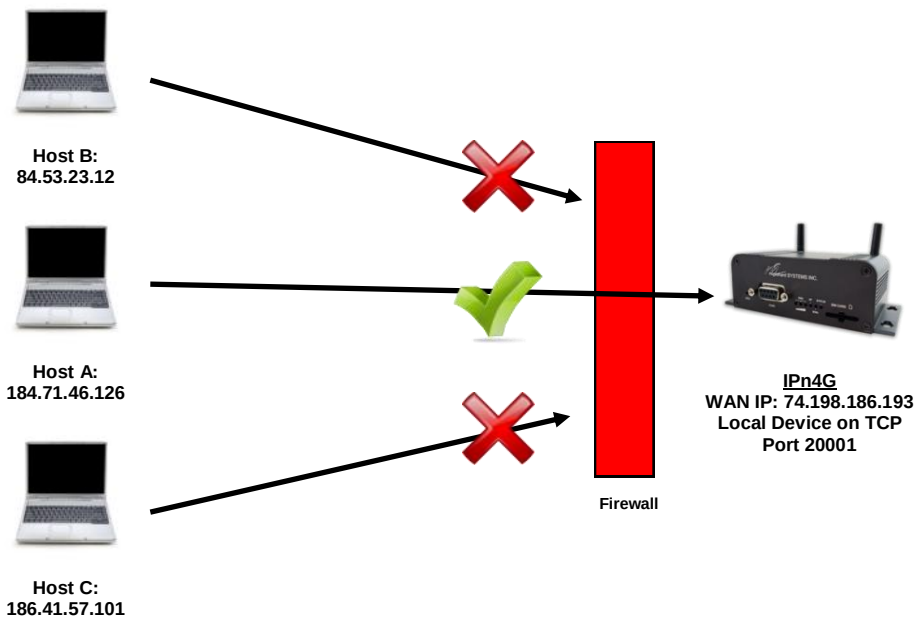
Submit changes to both units. It should be possible to ping and reach devices on either end of the VPN tunnel if both devices have been configured correctly and have network connectivity.

Appendix E: Firewall Example (Page 1 of 2)

By completing the Quick Start process, a user should have been able to log in and set up the IPn4G 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 IPn4G 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 IPn4G is paramount for a secure deployment. The firewall features of the IPn4G allow a user to limit access to the IPn4G 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 IPn4G 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 IPn4G and attached device, including the remote management features.



Step 1

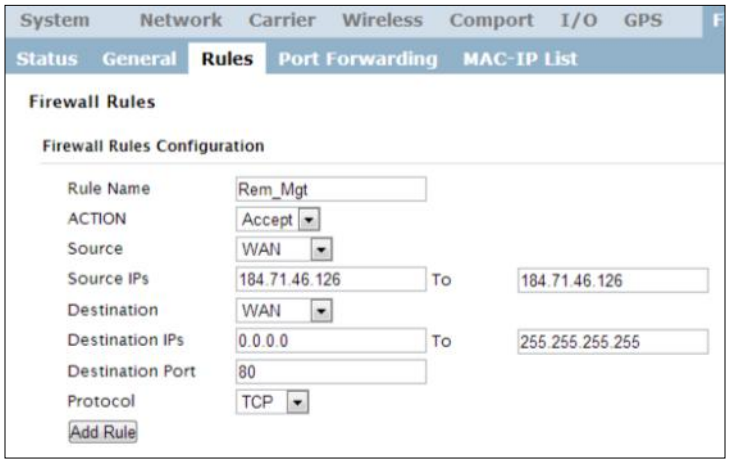
Log into the IPn4G (Refer to Quick Start). Navigate to the Firewall > General tab as shown below and ensure that the Firewall is turned on by enabling the ***Firewall Status***. Next block all WAN traffic by setting the ***WAN Request*** to Block, and disable ***Remote Management***. Be sure to Apply the settings. At this point it should be impossible to access the IPn4G from the WAN.

Appendix E: Firewall Example (Page 2 of 2)

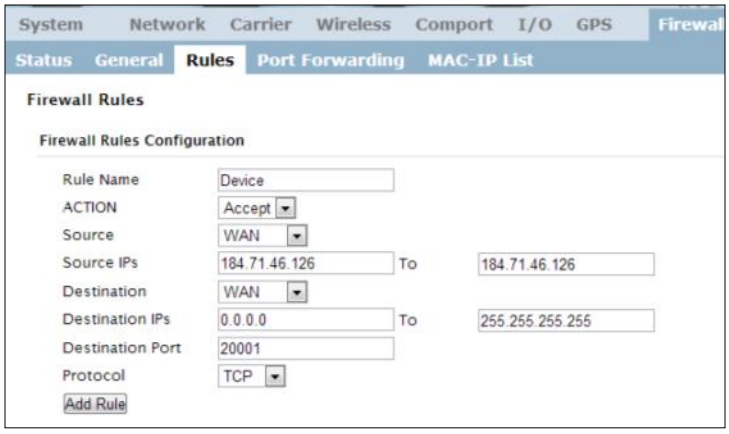
Step 2

Under the Rules tab we need to create two new rules. A rule to enable Host A access to the Remote Management Port (TCP Port 80), and another to access the device attached the to serial port (WAN TCP Port 20001).

Rule 1



Rule 2



After each rule is created be sure to click the ***ADD Rule*** button, once both rules are created select the ***Submit*** button to write the rules to the IPn4G. The Firewall Rules Summary should look like what is shown below.

Step 3

Test the connections. The IPn4G should only allow connections to the port specified from the Host A. An alternate means to limit connections to the IPn4G to a specific IP would have been to use the MAC-IP List Tool. By using Rules, we can not only limit specific IP's, but we can also specify ports that can be used by an allowed IP address.

Appendix F: Troubleshooting

Below is a number of the common support questions that are asked about the IPn4G. The purpose of the section is to provide answers and/or direction on how to solve common problems with the IPn4G.

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 IPn4G. For instructions of how to log into the IPn4G refer to the Quick Start.

Question: *What is the default IP Address of the IPn4G?*

Answer: The default IP address for the LAN (the RJ45 connector on the back of the unit) is 192.168.168.1.

Question: *What is the default login for the IPn4G?*

Answer: The default username is ***admin****, the default password is* ***admin****.*

Question: *What information do I need to get from my wireless carrier to set up the IPn4G?*

Answer: The APN is required to configure the IPn4G to communicate with a wireless carrier. Some carriers also require a username and password. The APN, username and password are only available from your wireless carrier.

Newer units may support an AUTO APN feature, which will attempt to determine the APN from a preconfigured list of carriers and commonly used APN's. This is designed to provide quick network connectivity, but will not work with private APN's. Success with AUTO APN will vary by carrier.

Question: *How do I reset my modem to factory default settings?*

Answer: If you are logged into the IPn4G navigate to the System > Maintenance Tab. If you cannot log in, power on the IPn4G and wait until the status LED in on solid (not flashing). Press and hold the CONFIG button until the unit reboots (about 8-10 seconds).

Question: *I can connect the Carrier, but I can't access the Internet/WAN/network from a connected PC?*

Answer: Ensure that you have DHCP enabled or manually set up a valid IP, Subnet, Gateway and DNS set on the local device.

Question: *I connected a device to the serial port of the IPn4G and nothing happens?*

Answer: In addition to the basic serial port settings, the IP Protocol Config has to be configured. Refer to the COM0/1 Configuration pages for a description of the different options.

Appendix F: Troubleshooting

Question: *How do I access the devices behind the modem remotely?*

Answer: To access devices behind the IPn4G remotely, several methods can be used:

A. IP Passthrough - The IPn4G 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 ***Enabled***. 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'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.

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.

Appendix F: Troubleshooting

Question: *Why does my modem reset every 10 minutes (or other time)?*

Answer: There are a number of processes in the IPn4G 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. Traffic Watchdog - Detects if there is any Wireless Traffic between the IPn4G and the Cellular Carrier. Will reboot modem when timer expires unless there is traffic. Carrier > Traffic Watchdog.
2. Keepalive - Attempts to contact a configured host on a defined basis. Will reboot modem if host is unreachable. Enabled by default to attempt to ping 8.8.8.8. May need to disable on private networks, or provide a reachable address to check. Access via Carrier > Keepalive.
3. Local Device Monitor - The IPn4G will monitor a local device, if that device is not present the IPn4G may reboot. Network > LocalMonitor.

Question: *How do I set up VPN?*

Answer: Refer to the VPN Appendix for an example.

microhard SYSTEMS INC.

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

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