

Operating Manual

IPn4Gii / IPn3Gii

IPn4Gii 4G/LTE Dual Ethernet/Serial/USB Gateway
IPn3Gii 3G/HSPA+ Dual Ethernet/Serial/USB Gateway

Document: IPn3Gii+IPn4Gii Operating Manual.v1.3.pdf
FW: v1.2.0 Build 1038

May 2015



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 ANY DAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY MICROHARD SYSTEMS INC. ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.

Proprietary Rights

The Buyer hereby acknowledges that Microhard Systems Inc. has a proprietary interest and intellectual property rights in the Hardware, Software and/or Products. The Purchaser shall not (i) remove any copyright, trade secret, trademark or other evidence of Microhard Systems Inc.'s ownership or proprietary interest or confidentiality other proprietary notices contained on, 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 / Exigences Réglementaires



WARNING

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

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



WARNING

MAXIMUM EIRP

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

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



WARNING

EQUIPMENT LABELING / ÉTIQUETAGE DE L'ÉQUIPEMENT

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

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

SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE :

IPn3Gii

IPn4Gii

FCCID: XPYLISAU230
IC: 8595A-LISAU230

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

FCCID: R17LN930
IC: 5131A-LN930

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

IPn4Gii - Verizon

FCCID: R5Q-TOBYL100
IC: 8595B-TOBYL100

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received including interference that may cause undesired operation.

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

CSA Class 1 Division 2 Option

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

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

In such a case the following must be met:

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

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

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

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

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

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

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

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

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

Dans un tel cas, la suivante doit être remplie:

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

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

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

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

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

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

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

Revision History

Revision	Description	Initials	Date
0.0	Preliminary.	PEH	Mar 2014
1.0	First Release. Based on Firmware v1.2.0 Build 1008	PEH	July 2014
1.1	Updated to reflect default IP change to 192.168.168.1 for all unit types. v1.2.0 Build 1015.	PEH	Sept 2014
1.2	Updated to align with firmware version 1.2.0 Build 1016. Added MultiWAN, updated Carrier Dual SIM. Added TAIP, Added Websocket, Updated I/O, Updated screenshots throughout, misc corrections.	PEH	Sept 2014
1.21	Updated to notify users must configure firewall and/or appropriate rules to use IP-Passthrough.	PEH	Oct 2014
1.22	Removed AT+CMGS (Not currently Supported), Added Current Consumption.	PEH	Feb 2015
1.3	Updated to align with firmware version v1.2.0-r1038	PEH	May 2015

Table of Contents

1.0 Overview	10
1.1 Performance Features.....	10
1.2 Specifications.....	11
1.3 RF Performance.....	13
2.0 QUICK START	15
2.1 Installing the SIM Card	15
2.2 Getting Started with Cellular	15
3.0 Hardware Features	19
3.1 IPnXGii	19
3.1.1 IPnXGii Mechanical Drawings	20
3.1.2 IPnXGii Connectors & Indicators.....	21
3.1.2.1 Front.....	21
3.1.2.2 Rear	22
4.0 Configuration.....	23
4.0 Web User Interface.....	23
4.0.1 Logon Window.....	24
4.1 System.....	25
4.1.1 Summary.....	25
4.1.2 Settings	26
Host Name	26
Console Timeout.....	26
Date/Time.....	27
NTP Server Settings	28
4.1.3 Services	29
SSH.....	29
Telnet	29
HTTP/HTTPS	29
4.1.4 Keepalive.....	30
4.1.5 Maintenance	32
Firmware Upgrade	32
Reset to Default.....	32
Backup & Restore Configurations	33
4.1.6 Reboot.....	34
4.2 Network	35
4.2.1 Summary.....	35
4.2.2 LAN	36
4.2.3 WAN.....	39
4.2.4 DHCP (MAC Binding)	41
4.2.5 DDNS.....	42
4.2.6 Routes.....	43
4.2.6 Ports (Switch)	44
4.2.7 Device List.....	44

Table of Contents

4.3 Carrier	45
4.3.1 Status.....	45
4.3.2 Settings.....	46
Dual Cards Management.....	47
4.3.3 SMS.....	51
4.3.4 SMS Config.....	52
4.3.5 Data Usage.....	55
4.4 Firewall	58
4.4.1 Summary.....	58
4.4.2 General.....	59
4.4.3 Port Forwarding.....	61
4.4.4 MAC-IP List.....	63
4.4.5 Rules.....	65
4.4.6 Firewall Default.....	67
4.5 VPN	68
4.5.1 Summary.....	68
4.5.2 Gateway to Gateway.....	69
4.5.3 Client to Gateway (L2TP Client).....	74
4.5.4 GRE.....	76
4.5.5 L2TP Users.....	79
4.5.6 Certificates.....	80
4.6 MultiWAN	81
4.6.1 Status.....	81
4.6.2 Settings.....	82
4.7 Serial	84
4.7.1 Summary.....	84
4.7.2 RS232/Console/RS485 Settings.....	85
Data Baud Rate.....	86
IP Protocol Config.....	89
TCP Client.....	89
TCP Server.....	89
TCP Client/Server.....	90
UDP Point-to-Point.....	90
UDP Point-to-Multipoint (P).....	90
UDP Point-to-Multipoint (MP).....	91
UDP Multipoint-to-Multipoint.....	91
SMTP Client.....	92
PPP.....	92
GPS Transparent Mode.....	93
4.8 USB	94
4.8.1 Summary.....	94
4.8.2 Serial.....	95
4.8.3 NDIS.....	96
4.9 I/O	97
4.9.1 Summary.....	97

Table of Contents

4.10 GPS	99
4.10.1 Location	99
4.10.2 Settings.....	100
4.10.3 Report	101
4.10.4 GPSTGate.....	103
4.10.5Recorder	106
4.10.6 Load Record.....	107
4.10.7 TAIP.....	110
4.11 Applications	112
4.11.1 Modbus	112
4.11.1.1 TCP Modbus.....	112
4.11.1.2 Serial (COM) Modbus.....	114
4.11.1.3 Modbus Data Map.....	115
4.11.2 Netflow Report	116
4.11.3 Local Monitor	118
4.11.4 Event Report.....	119
4.11.4.1 Configuration	119
4.11.4.2 Message Structure.....	120
4.11.4.2 Message Payload.....	120
4.11.5 Websocket.....	122
4.11.6 Diagnostics	124
Network Ping.....	124
Network Trace Route	124
4.12 Admin	125
4.12.1 Users	125
4.12.2 Authentication (RADIUS).....	127
4.12.3 NMS	128
4.12.4 SNMP	132
4.12.5 Discovery.....	135
4.12.6 Power Saving Modes	136
4.12.7 Logout.....	137
5.0 AT Command Line Interface	138
5.1 AT Command Overview	138
5.1.1 Serial Port.....	138
5.1.2 Telnet.....	139
5.2 AT Command Syntax	140
5.3 Supported AT Commands	141
Appendices	174
Appendix A: Serial Interface	174
Appendix B: IP-Passthrough Example.....	175
Appendix C: Port Forwarding Example.....	177
Appendix D: VPN (Site to Site) Example	179
Appendix E: Firewall Rules Example	181
Appendix F: Troubleshooting.....	183

1.0 Overview

The IPn4Gii & IPn3Gii products are high-performance Cellular Dual Ethernet/Serial/USB Gateways, equipped with dual RJ45 Ethernet Ports, dual SIM capability, 8x Programmable Analog I/O, Optional Standalone GPS, and up to three serial communication ports. One each of RS232, RS485 and a RS232 Console port, which can be used as an additional data port.

The IPnXGii utilizes the cellular infrastructure to provide network access to wired devices anywhere cellular coverage is supported by a cellular carrier. The IPn3Gii supports up to 21Mbps downloads, when connected to a HSPA+ enabled carrier, or global fallback to 3G/Edge networks for areas without HSPA+. The IPn4Gii supports 4G/LTE connections with blazing fast speeds.

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

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

1.1 Performance Features

Key performance features of the IPnXGii include:

- Fast, reliable connection speeds to 4G, 3G, LTE, and HSPA Networks (varies by model)
- 8x Programmable Analog/Digital Inputs OR up to 8 Digital Outputs
- DMZ and Port Forwarding
- Dual 10/100 Ethernet Ports (WAN/LAN)
- Standalone GPS (TCP Server/UDP/SMTP Reporting)
- User interface via local console, telnet, web browser
- Compatibility with virtually all PLCs, RTUs, and serial devices through either RS232, RS422, or RS485 interfaces.
- Local & remote wireless firmware upgradable
- User configurable Firewall with IP/MAC ACL
- IP/Sec secure VPN and GRE Tunneling
- Industrial Temperature Rating (-40°C to +85°C)

1.0 Overview

1.2 Specifications

IPn3Gii

- IPn3Gii Supported Bands:** UMTS/HSPA FDD Bands [MHz] - Six band
 Band I (2100MHz), Band II (1900MHz), Band IV (1700MHz), Band V (850MHz), Band VI (800MHz), Band VIII (900Hz)
 3GPP Release 7
 5.76 Mb/s uplink, 21.1 Mb/s downlink
 or 5.76 Mb/s uplink, 7.2 Mb/s downlink
- IPn3Gii Data Features:** HSDPA cat 14, up to 21.1 Mb/s DL
 GPRS multi-slot class 125, coding scheme CS1-CS4, up to 85.6 kb/s DL/UL
 EDGE multi-slot class 125, coding scheme MCS1-MCS9, up to 236.8 kb/s DL/UL
 CSD GSM max 9.6 kb/s
 UMTS max 64 kb/s
- IPn3Gii TX Power:** WCDMA/HSDPA/HSUPA Power Class
 · Power Class 3 (24 dBm) for WCDMA/HSDPA/HSUPA mode
 GSM/GPRS Power Class
 · Power Class 4 (33 dBm) for GSM/E-GSM bands
 · Power Class 1 (30 dBm) for DCS/PCS bands
 EDGE Power Class
 · Power Class E2 (27 dBm) for GSM/E-GSM bands
 · Power Class E2 (26 dBm) for DCS/PCS bands

IPn4Gii

- IPn4Gii Supported Bands:** LTE FDD (Bands 1-5,7,8,13,17,18,19,20)
 UMTS | DC-HSPA+ (Bands 1,2,4,5,8)
 GSM | GPRS | EDGE (Bands 2,3,5,8)
 3GPP Protocol Stack Release 9
- IPn4Gii Data Features:** LTE: DL 100 Mbps, UL 50 Mbps
 HSPA+: DL 42 Mbps, UL 5.7 Mbps
 HSPA+: DL 21 Mbps, UL 5.7 Mbps
 WCDMA: DL/UL 384 kbps
 EDGE Class 33: DL/UL 236.8 kbps
 GPRS Class 33: DL/UL 85.6kbps

General

- Serial Interface:** RS232, RS485, RS422
Serial Baud Rate: 300bps to 921kbps
USB: USB 2.0
 USB Console Port
 USB to Serial Data Routing
 USB to Ethernet Data Routing (NDIS)
 USB OTG (Host)

Current Consumption:
 (@12VDC)

Model	AVG Serial Data	AVG Ethernet Data	TX Max. Peak
IPn3Gii	130mA	140mA	215mA
IPn4Gii	130mA	145mA	250mA

1.0 Overview

General Specifications (Continued)

Ethernet:	2 x 10/100 BaseT, Auto - MDI/X, IEEE 802.3
I/O:	8x Programmable Analog/Digital Inputs or up to 8x Digital Outputs 60mA current sink on open drain
SIM Card:	Dual: 1.8 / 3.0V
PPP Characteristics:	Dial on Demand/Idle Time
Network Protocols:	TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP, QoS
Management:	Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade, RADIUS authentication, IPsec VLAN
Diagnostics:	Temperature, RSSI, remote diagnostics
Input Voltage:	7-30 VDC
Power over Ethernet:	Passive PoE on Ethernet Port (WAN)
GPS:	Sensitivity: - Autonomous acquisition: -145 dBm - Tracking Sensitivity: -158 dBm (50% valid fixes) Position Accuracy: - Tracking L1, CA code - 12 Channels - Max. update rate 1 Hz Error calculated location less than 11.6 meters 67% of the time, and less than 24.2 meters 95% of the time.

Environmental

Operation Temperature:	-40°F(-40°C) to 185°F(85°C)
Humidity:	5% to 95% non-condensing

Mechanical

Dimensions:	2.21" (56mm) X 3.85" (97mm) X 1.46" (37mm)
Weight:	Approx. 245 grams
Connectors:	Antenna(s): CELL, DIV, GPS: SMA Female ANT3: RP-SMA Female
	Data, etc: Data: DE-9 Female (Front RS232) Ethernet : 2x RJ-45

GPS Antenna Requirements:

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

1.0 Overview

1.3 IPn3Gii RF Performance

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

Table 1-1: IPn3Gii Operating RF Frequency Bands

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

Table 1-2: IPn3Gii Receiver sensitivity performance

1.0 Overview

1.3 IPn3Gii RF Performance (continued...)

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

Table 1-3: IPn3Gii Transmitter maximum output power

2.0 Quick Start

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

Note that the units arrive from the factory with the Local Network setting configured as 'Static' (IP Address 192.168.168.1, 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 IPnXGii unit.

2.1 Installing the SIM Card

- ✓ Before the IPnXGii can be used on a cellular network a valid **SIM Card** for your Wireless Carrier must be installed. Insert the SIM Card into the slot as shown, the top SIM slot is for SIM1:



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



SIM Card Slot



2.2 Getting Started with Cellular

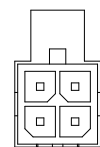
- ✓ Connect the Antenna's to the applicable **ANTENNA** jack's of the IPnXGii.



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

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

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

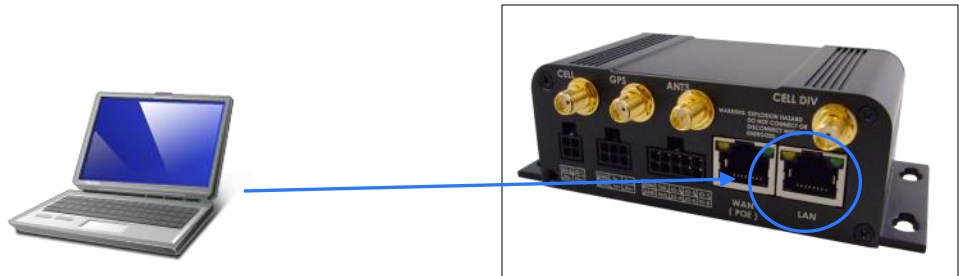


7-30VDC

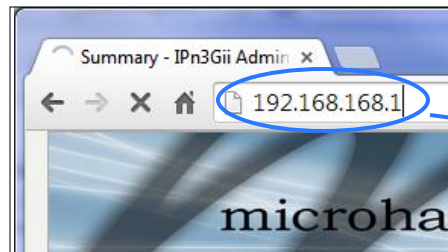


2.0 Quick Start

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



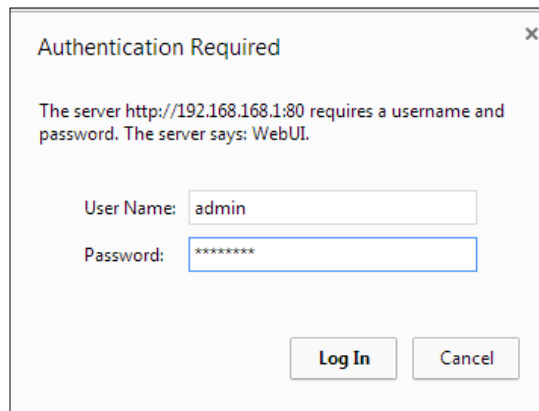
- ✓ Open a Browser Window and enter the IP address **192.168.168.1** into the address bar.



The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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



The Factory default login:

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



The factory default login:

User name: admin
Subnet: admin

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

2.0 Quick Start

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

System	Network	Carrier	Firewall	VPN	MULTIWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary Settings Services Keepalive Maintenance Reboot											
System Information											
System Information											
Host Name	IPn4Gii_MKT	Description	IPn4Gii								
Product Name	IPn4Gii	System Date	2015-03-31 14:45:40								
Hardware Version	Rev A	System Uptime	7 min								
Software Version	v1.2.0 build 1036	Temperature(°C)	37.7								
Build Time	2015-03-30 15:43:19	Supply Voltage (V)	11.82								
Carrier Information											
Module Status	Enabled	IMEI	356406060021903								
Current APN	wrstat.bell.ca	IMSI	302610012606734								
Connection Status	Connected	SIM Card	READY								
Network	Bell	SIM Number (ICCID)	89302610203010832398								
Home/Roaming	Home	Phone Number	15874327939								
Current Technology	LTE	Cell ID	28963586								
Frequency Band(MHz)	BAND_LTE_4	LAC	11204								
IP Address	184.151.220.2	RSSI (dBm)	-90 dBm 								
DNS Server 1	70.28.245.227	RSRP/Q (dBm/dB)	-88 / -7								
DNS Server 2	184.151.118.254	SINR (dB)	15								



Auto APN: The IPnXGii 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.

System	Network	Carrier	Firewall	VPN	MULTIWAN	Serial	USB	I/O	GPS	Applications	Admin
Status Settings SMS SMSConfig DataUsage											
Carrier Configuration											
General											
Carrier status	Enable										
IP-Passthrough	Disable										
SIM Selection	Dual SIM Cards										
Dual Cards Management											
Primary Slot	SIM Card-1										
Start Over	Enable										
Switch Over	Enable										
Switch Timeout(in seconds)	600										
Keepalive	Enable										
SIM Card-1 (Top slot) Settings											
SIM Number(ICCID)	89302610203010832398										
Data Roaming	Disable										
Carrier Operator	Auto										
Technologies Mode	AUTO Advanced										
APN	wrstat.bell.ca										
<input type="checkbox"/> Advanced+											
<input type="checkbox"/> Network+											
SIM Card-2 (Bottom slot) Settings											
SIM Number(ICCID)	N/A										
Data Roaming	Disable										
Carrier Operator	Auto										
Technologies Mode	AUTO Advanced										
APN	auto										
<input type="checkbox"/> Advanced+											
<input type="checkbox"/> Network+											

- ✓ Once the APN and any other required information is entered to connect to your carrier, click on "Submit".
- ✓ *Verizon Models do not require a APN and will Auto Connect if a valid SIM card is inserted.*

2.0 Quick Start

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status Settings SMS SMSConfig DataUsage											
Carrier Status											
Carrier Status - LN930											
Current APN	wrstat.bell.ca		Core Temperature(°C)	36							
Activity Status	Connected		IMEI	356406060021903							
Network	Bell		SIM PIN (Card-1)	READY							
Home/Roaming	Home		SIM Number (ICCID)	89302610203010832398							
Service Mode	E-UTRAN		Phone Number	15874327939							
Service State	E-UTRAN		RSSI (dBm)	-90 							
Cell ID	28963586		RSRP/Q (dBm/dB)	-87 / -6							
LAC	11204		SINR (dB)	17							
Current Technology	LTE		Connection Duration	10 min 16 sec							
Available Technology	LTE,UMTS,GSM		WAN IP Address	184.151.220.2							
Frequency Band(MHz)	BAND_LTE_4		DNS Server 1	70.28.245.227							
			DNS Server 2	184.151.118.254							



Ensure the default passwords are changed.



Set up appropriate firewall rules to block unwanted incoming data.

- ✓ 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 IPnXGii is successfully connected to your Cellular Carrier.
- ✓ To access devices connected to IPnXGii remotely, one or more of the following must be configured: IP-Passthrough, Port Forwarding, DMZ. Another option would be to set up a VPN.
- ✓ Ensure that all default passwords are changed to limit access to the modem.
- ✓ For best practices and to limit data charges it is critical to properly set up the firewall. (Especially important for Public Static IP addresses.)

3.0 Hardware Features

3.1 IPnXGii

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



Image 3-1: Front View of IPnXGii



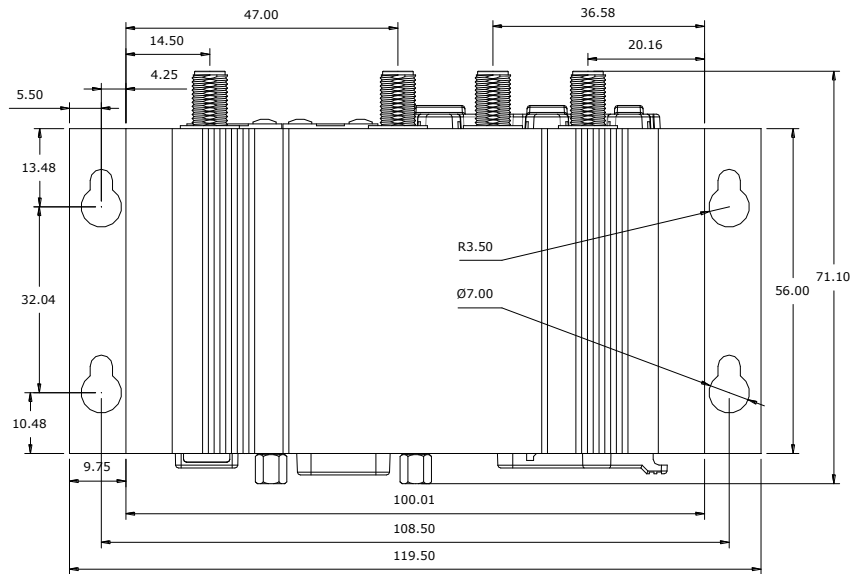
Image 3-2: Rear View of IPnXGii

The IPnXGii Hardware Features Include:

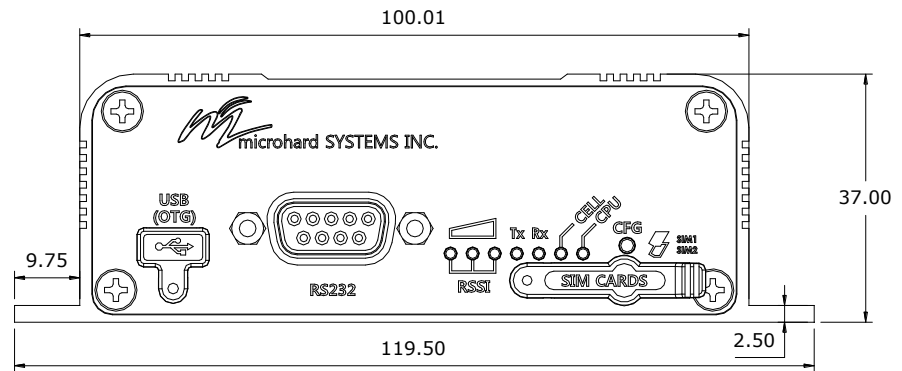
- Standard Connectors for:
 - 2 Ethernet Ports (RJ45 - WAN/LAN)
 - Data Port (RS232/DB9)
 - COM2 Port (RS232/Console)
 - 4-Pin: MATE-N-LOK Type Connector for Power / I/O 1/2
 - 6-Pin: MATE-N-LOK Type Connector for RS485 Data
 - 10-Pin: MATE-N-LOK Type Connector for RS232 Console / I/O 3-8
 - Cellular Antenna (SMA Female Antenna Connection x2)
 - ANT3 Antenna (RP-SMA Female Antenna Connection) (Future)
- Status/Diagnostic LED's for RSSI(x3), Tx, Rx, CELL, CPU
- Dual SIM (standard size) Card Slots
- CFG Button for factory default / firmware recovery operations
- Mounting Holes

3.0 Hardware Features

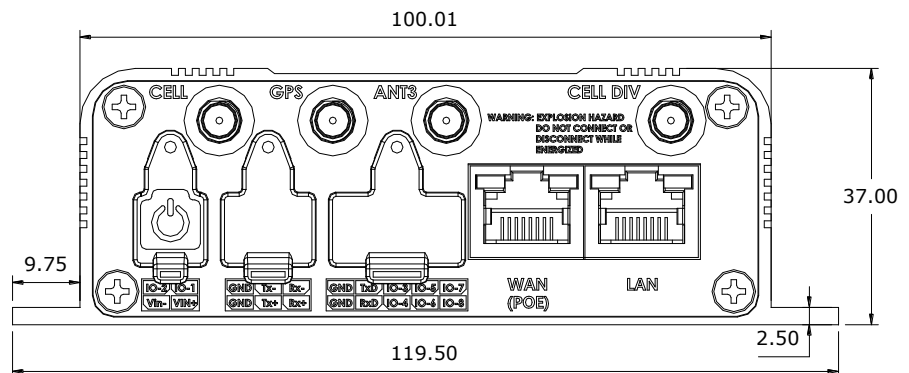
3.1.1 Mechanical Drawings



Drawing 3-1: IPnXGii Top View Dimensions



Drawing 3-2: IPnXGii Front View Dimensions



Drawing 3-3: IPnXGii Rear View Dimensions

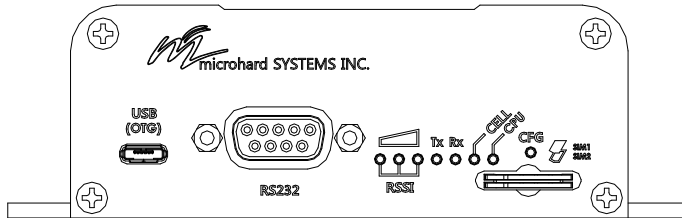
Note: All dimension units: Millimeter

3.0 Hardware Features

3.1.2 Connectors and Indicators

3.1.2.1 Front

On the front of the IPnXGii is the RS232 (COM2) port, CFG Button, RSSI, Tx, RX, CELL & CPU LED's as described below:



Drawing 3-4: IPnXGii Front View

The **RS232** port is used for serial communication to serial based end devices. (300bps to 921kbps)

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

Tx(Red)/Rx(Green) LED's - The Tx/Rx LED's indicate carrier (cellular) traffic. Also, during system bootup, the RF & SGNL LED's will flash.

CELL LED - Indicates internal cellular module has power.

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.

CPU LED - The Status LED indicates that power has been applied to the module. Flashing indicates bootup or firmware upgrade status.

SIM Cards - These slots are used to install SIM card (s) provided by the cellular carrier to enable communication to their cellular network. Ensure that the SIM card is installed properly by paying attention to the diagram printed above the SIM card slot. The system will detect which slot is used.

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 3-1: RS232 Pin Assignment

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



The factory default network settings:

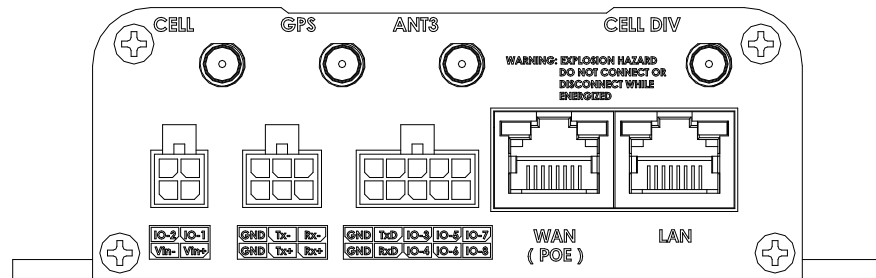
IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

3.0 Hardware Features

3.1.2 Connectors and Indicators

3.1.2.2 Rear

On the back of the IPnXGii is the Console port (RS232 - Rx/Tx), RS485/422 interface, Programmable I/O, Dual Ethernet Ports (WAN/LAN) 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 ANT3



Drawing 3-5: IPnXGii Rear View

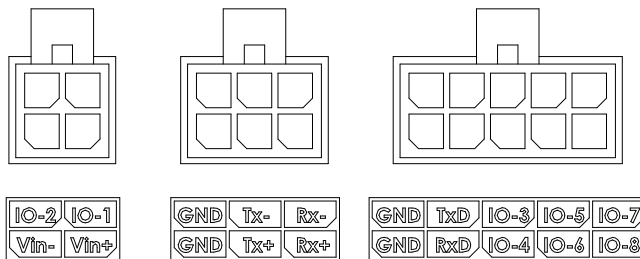
The **Console (RS232 –Tx/Rx)** on the rear of the unit is used for:

- AT Command Interface
- RS232 serial data (TX, RX)

The **RS422/485 Port** is a standalone port that can be used in addition to the RS232 Data Port.

Programmable I/O– The IPnXGii has 8 programmable Analog/Digital Inputs or 8x Digital Outputs. Maximum recommended load for the output pin is 150mA @ 30 Vdc (Vin).

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



Name	Input or Output
Tx+	O
Tx-	O
Rx+	I
Rx-	I
Vin -	
Vin +	I

Table 3-4: Data RS422/485, Vin Pin Assignments



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

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

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

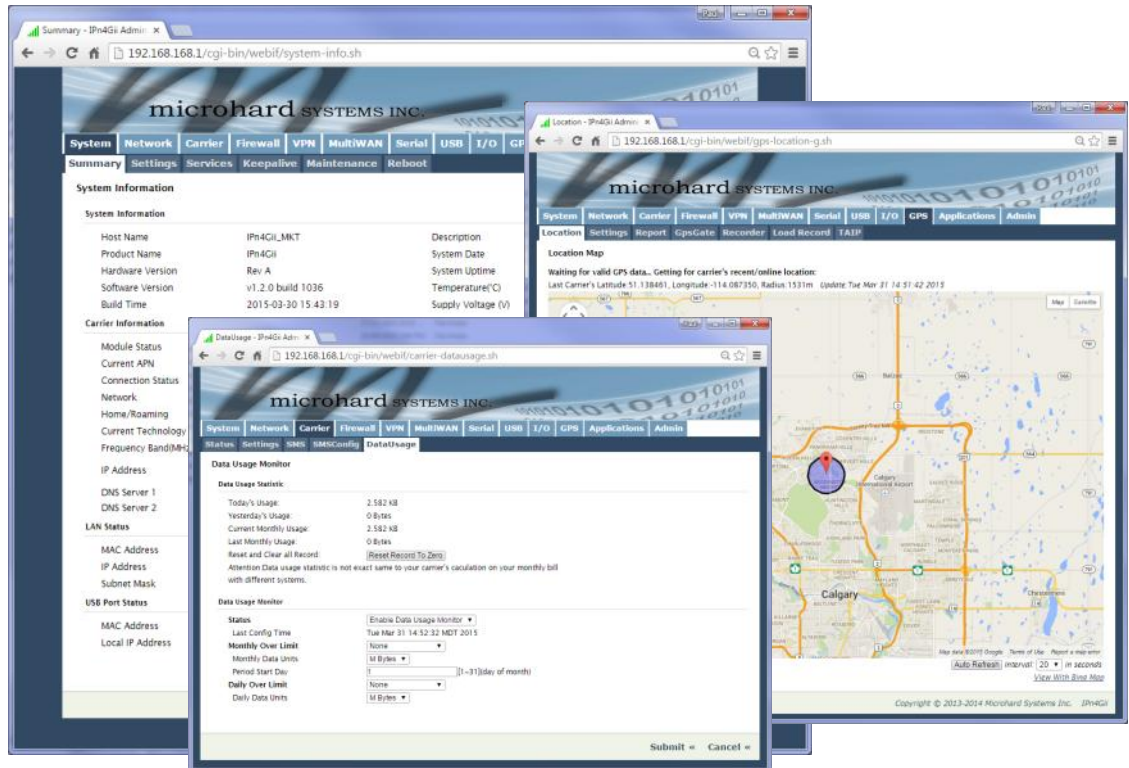


Image 4-0-1: WebUI



The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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

- configure a static IP Address on your PC to match the default subnet **or** if your PC is configured for DHCP, simply connect a PC to the LAN port of the IPnXGii and it will be assigned a IP address automatically.
- connect the IPnXGii ETHERNET(LAN) port to PC NIC card using an Ethernet cable
- apply power to the IPnXGii and wait approximately 60 seconds for the system to load
- open a web browser and enter the factory default IP address(192.168.168.1) of the unit:
- logon window appears; log on using default Username: **admin** Password: **admin**
- use the web browser based user interface to configure the IPnXGii 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 IPnXGii using a Web Browser, the Logon window will appear.

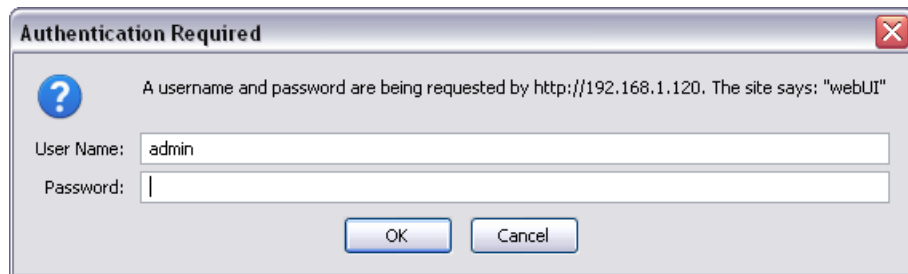


Image 4-0-2: Logon Window



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.

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

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



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

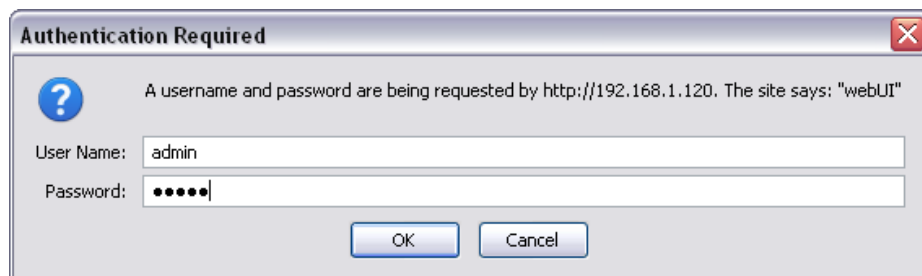


Image 4-0-3: Logon Window : Password Entry

4.0 Configuration

4.1 System

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

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

4.1.1 System > Summary

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

The screenshot displays the 'System Summary' page of the IPn4Gii web interface. The page is titled 'microhard SYSTEMS INC.' and features a navigation bar with tabs for System, Network, Carrier, Firewall, VPN, MultiWAN, Serial, USB, I/O, GPS, Applications, and Admin. The 'System' tab is selected, and the 'Summary' sub-tab is active. The main content area is divided into four sections: System Information, Carrier Information, LAN Status, and USB Port Status. Each section contains a table of key system parameters and their current values.

System Information			
Host Name	IPn4Gii_MKT	Description	IPn4Gii
Product Name	IPn4Gii	System Date	2015-03-31 14:53:25
Hardware Version	Rev A	System Uptime	15 min
Software Version	v1.2.0 build 1036	Temperature(°C)	38.9
Build Time	2015-03-30 15:43:19	Supply Voltage (V)	11.79
Carrier Information			
Module Status	Enabled	IMEI	356406060021903
Current APN	wrstat.bell.ca	IMSI	302610012606734
Connection Status	Connected	SIM Card	READY
Network	Bell	SIM Number (ICCID)	89302610203010832398
Home/Roaming	Home	Phone Number	15874327939
Current Technology	LTE	Cell ID	28963586
Frequency Band(MHz)	BAND_LTE_4	LAC	11204
IP Address	184.151.220.2	RSSI (dBm)	-90 dBm
DNS Server 1	70.28.245.227	RSRP/Q (dBm/dB)	-87 / -7
DNS Server 2	184.151.118.254	SINR (dB)	16
LAN Status			
MAC Address	00:0F:92:02:16:E1	Connection Type	bridge
IP Address	192.168.168.1	Mode	static
Subnet Mask	255.255.255.0	Gateway	N/A
USB Port Status			
MAC Address	00:0F:92:04:16:E1	Subnet Mask	255.255.255.0
Local IP Address	192.168.111.1	Host IP Address	192.168.111.2

At the bottom right of the summary area, there is a 'Stop Refreshing' button and an 'Interval: 20(s)' label. The footer of the page reads 'Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii'.

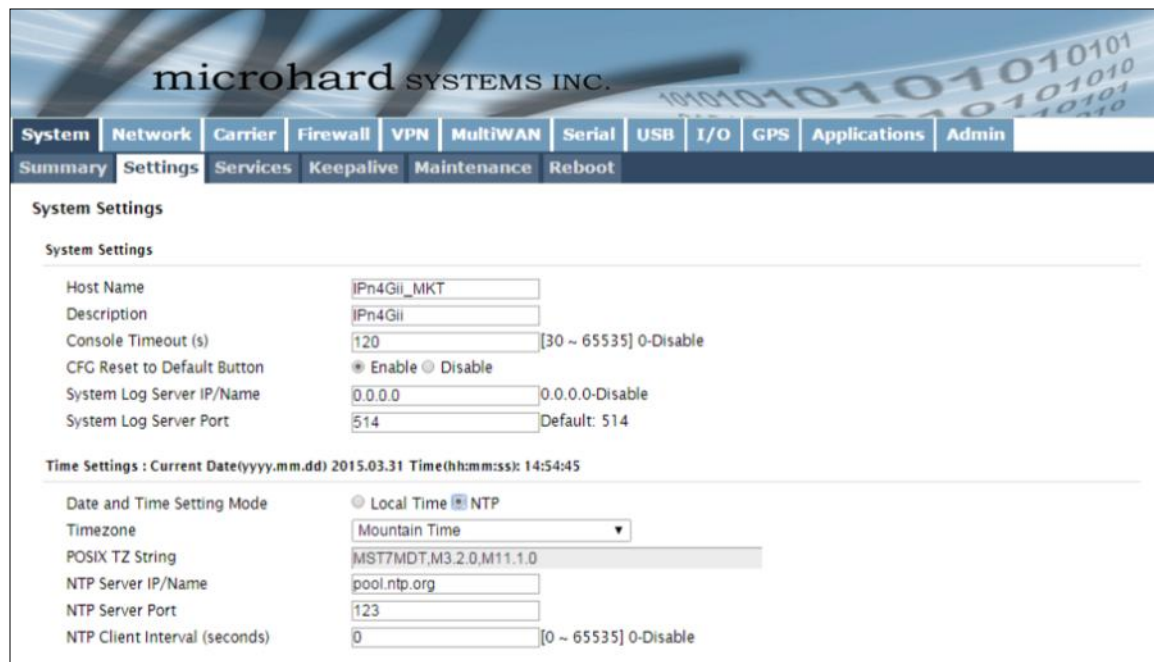
Image 4-1-1: System Info Window

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, Description, Console Timeout and System Log server settings.



microhard SYSTEMS INC.

System Network Carrier Firewall VPN MultiWAN Serial USB I/O GPS Applications Admin

Summary Settings Services Keepalive Maintenance Reboot

System Settings

System Settings

Host Name IPn4Gii_MKT

Description IPn4Gii

Console Timeout (s) 120 [30 ~ 65535] 0-Disable

CFG Reset to Default Button Enable Disable

System Log Server IP/Name 0.0.0.0 0.0.0.0-Disable

System Log Server Port 514 Default: 514

Time Settings : Current Date(yyyy.mm.dd) 2015.03.31 Time(hh:mm:ss) 14:54:45

Date and Time Setting Mode Local Time NTP

Timezone Mountain Time

POSIX TZ String MST7MDT,M3.2.0,M11.1.0

NTP Server IP/Name pool.ntp.org

NTP Server Port 123

NTP Client Interval (seconds) 0 [0 ~ 65535] 0-Disable

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

Host Name

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

Values (characters)

IPnXGii (**varies**)
up to 30 characters

Console Timeout (s)

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

Values (seconds)

60
0-65535

CFG Reset to Default Button

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

Values (Selection)

Enable
Disable

4.0 Configuration

System Syslog Server IP

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

IP Address

0.0.0.0

System Syslog Server Port

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

UDP Port

514

Time Settings

The IPnXGii 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.

Time Settings : Current Date(yyyy.mm.dd) 2015.03.31 Time(hh:mm:ss): 14:54:45

Date and Time Setting Mode Local Time NTP

Date (yyyy.mm.dd)

Time (hh:mm:ss)

Time Settings : Current Date(yyyy.mm.dd) 2015.03.31 Time(hh:mm:ss): 14:54:45

Date and Time Setting Mode Local Time NTP

Timezone

POSIX TZ String

NTP Server IP/Name

NTP Server Port

NTP Client Interval (seconds) [0 ~ 65535] 0-Disable

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 IPnXGii lose power for some reason.

Values (yyyy-mm-dd)

2011.04.01 (varies)

4.0 Configuration

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

4.0 Configuration

4.1.3 System > Services

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

Image 4-1-5: System > Services

FTP

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

Values (port)

Enable / Disable

Telnet

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

Values (port)

23

SSH

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

Values (port)

22

Web UI

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

Values (selection)

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).

HTTP/HTTPS
HTTP
HTTPS

4.0 Configuration

4.1.4 System > Keepalive

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



Image 4-1-6: Carrier > Keepalive

Keep Alive

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

Values (Selection)

Enable / Disable

Traffic Check

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

Values (Selection)

Enable / Disable

CLI Activity

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

Values (Selection)

Enable / Disable

Web UI Activity

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

Values (Selection)

Enable / Disable

4.0 Configuration

	Type
<p>Once the connection is lost, the modem will send one of the requests to the remote host to determine the connection status. If the modem fails to get the response, it will re-send the request within the seconds specified by Keepalive Interval below:</p> <p>ICMP: Send a "ping" request HTTP: Send a "wget" request to a HTTP server DNS Lookup: Send a "dslookup" request to a DNS server</p>	<p>Values (Selection)</p> <p>ICMP HTTP DNS Lookup</p>
<p>Specify a IP Address or Domain that is used to test the modems connection. The modem will send out the connection requests to the specified Host.</p>	<p>Host Name</p> <p>Values (IP or Domain)</p> <p>8.8.8.8</p>
<p>The Interval value determines the frequency, or how often, the unit will send out PING messages to the Host.</p>	<p>Keepalive Interval</p> <p>Values (seconds)</p> <p>60</p>
<p>The Keepalive Retry is the maximum number of connection failures such as "Host unreachable" the unit will attempt before the unit will reboot itself to attempt to correct connection issues. The default number is 20, and valid value is from 10 to 200.</p>	<p>Keepalive Retry</p> <p>Values (number)</p> <p>10</p>

4.0 Configuration

4.1.5 System > Maintenance

Firmware Upgrade

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	Settings	Services	Keepalive	Maintenance	Reboot						
System Maintenance											
Version Information											
Product Name	Hardware Type	Build Version	Build Date	Build Time							
IPn4Gii	Rev A	v1.2.0 build 1038	2015-04-16	17:17:54							
Firmware Upgrade											
Erase Current Configuration	Keep ALL Configuration										
Firmware Image	Choose file No file chosen										
Upgrade	Upgrade Firmware										
Reset to Default											
Reset to Default	Reset to Default	<input checked="" type="checkbox"/> Keep Carrier Settings									
Backup Configuration											
Name this configuration	MicrohardIPn4Gii.config										
Backup	Backup Configuration										
Restore Configuration											
Restore Configuration file	Choose file No file chosen										
Check Configuration file	Check Restore File										

Image 4-1-7: Maintenance > Firmware Upgrade

Erase Current Configuration

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

Values (check box)

unchecked

Firmware Image

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

Values (file)

(no default)

Reset to Default

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

4.0 Configuration

Backup & Restore Configuration

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

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

Name this Configuration / Backup Configuration

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

Restore Configuration file / Check Restore File / Restore

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

4.0 Configuration

4.1.6 System > Reboot

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

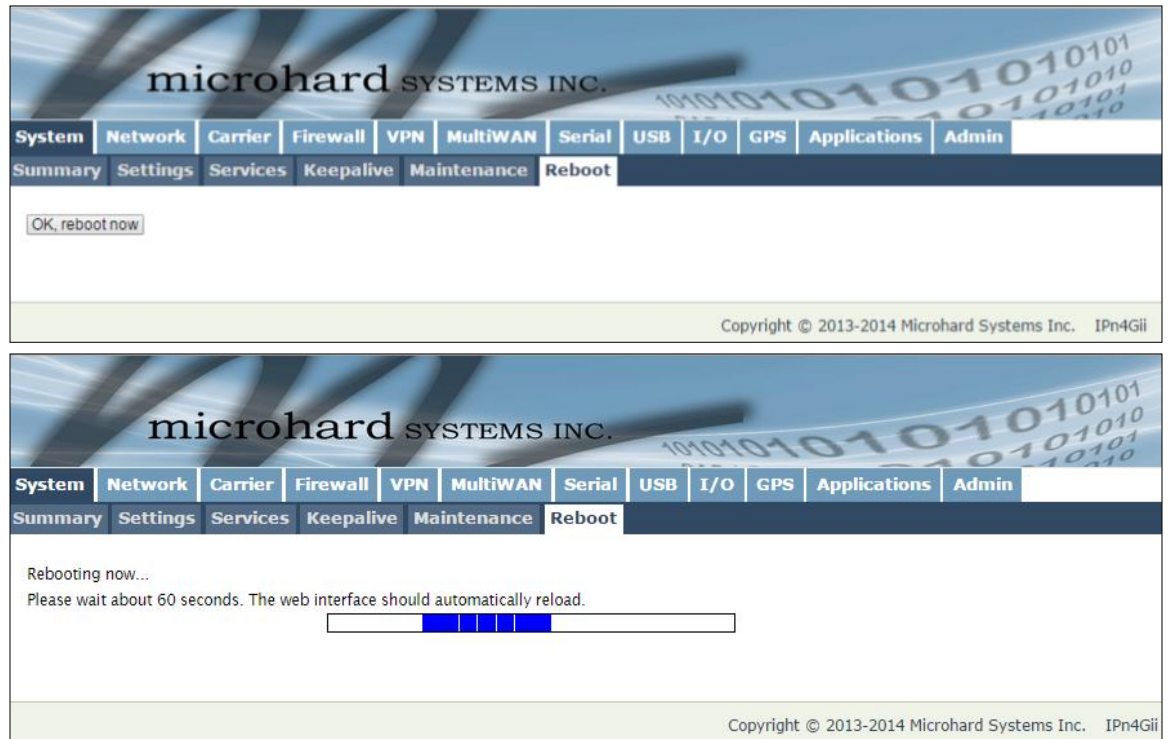


Image 4-1-9: System > Reboot

4.0 Configuration

4.2 Network

4.2.1 Network > Summary

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				
Network Status											
LAN Port Status											
General Status											
IP Address	192.168.168.1	Connection Type	static	Subnet Mask	255.255.255.0	MAC Address	00:0F:92:02:16:E1				
Traffic Status											
Receive bytes	64.992KB	Receive packets	569	Transmit bytes	202.568KB	Transmit packets	569				
WAN2 Port Status											
General Status											
IP Address	184.151.220.2	Connection Type	static	Subnet Mask	255.255.255.255	MAC Address	00:0F:92:FE:00:01				
Traffic Status											
Receive bytes	465B	Receive packets	4	Transmit bytes	818B	Transmit packets	10				
USB Port Status											
General Status											
IP Address	192.168.111.1	Connection Type	static	Subnet Mask	255.255.255.0	MAC Address	00:0F:92:04:16:E1				
Traffic Status											
Receive bytes	0B	Receive packets	0	Transmit bytes	168B	Transmit packets	2				
Default Gateway											
Gateway	184.0.0.1										
DNS											
DNS Server(s)	70.28.245.227 184.151.118.254										
IPv4 Routing Table											
Destination	Gateway	Subnet Mask	Flags	Metric	Ref	Use	Interface				
0.0.0.0	184.0.0.1	0.0.0.0	UG	0	0	0	(br-wan2)				
169.254.0.0	0.0.0.0	255.255.0.0	U	0	0	0	(br-lan)				
184.0.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	(br-wan2)				
192.168.111.0	0.0.0.0	255.255.255.0	U	0	0	0	(br-usb)				
192.168.168.0	0.0.0.0	255.255.255.0	U	0	0	0	(br-lan)				

Image 4-2-1: Network > Network Status

4.0 Configuration

4.2.2 Network > LAN



The factory default network settings:

IP: 192.168.168.1
 Subnet: 255.255.255.0
 Gateway: 192.168.168.1

LAN Port Configuration

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List			
LAN Port Configuration										
LAN Configuration										
Connection Type		Static IP ▾								
IP Address		192.168.168.1								
Subnet Mask		255.255.255.0								
Default Gateway										
DHCP Server										
Mode ⓘ		Enable ▾								
Start IP ⓘ		100								
Limit ⓘ		150								
Lease Time (in minutes) ⓘ		720								
Alternate Gateway										
Preferred DNS server										
Alternate DNS server										

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



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

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

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

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



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

Connection Type

Values (selection)

DHCP
Static

This selection determines if the IPnXGii 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.

IP Address

Values (IP Address)

192.168.168.1

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

4.0 Configuration



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

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



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

In typical networks, a router acts as a gateway.



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

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 IPnXGii 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 it 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.

LAN DHCP

A IPnXGii 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 IPnXGii. The LAN DHCP service is available for each interface, and is located in the add/edit interface menus.

DHCP Server	
Mode ⓘ	Enable ▾
Start IP ⓘ	100
Limit ⓘ	150
Lease Time (in minutes) ⓘ	720
Alternate Gateway	
Preferred DNS server	
Alternate DNS server	

Image 4-2-3: Network > DHCP Server

Mode

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

Values (selection)

On / Off

4.0 Configuration

	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 IPnXGii.	Values (integer) 150
	Lease Time
The DHCP lease time is the amount of time before a new request for a network address must be made to the DHCP Server.	Values (minutes) 720
	Alternate Gateway
Specify an alternate gateway for DHCP assigned devices if the default gateway is not to be used.	Values (IP Address) (IP Address)
	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)



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'.

4.0 Configuration

4.2.3 Network > WAN

WAN Configuration

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				
WAN Port Configuration											
Configuration											
Working Mode		Independent WAN									
WAN Configuration											
Connection Type		Static IP									
IP Address		<input type="text"/>									
Subnet Mask		<input type="text"/>									
Default Gateway		<input type="text"/>									
Default Route		Yes									
DNS Servers											
Mode		Manual									
Primary DNS		<input type="text"/>									
Secondary DNS		<input type="text"/>									

Image 4-2-4: Network > WAN Configuration



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

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

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

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

Working Mode

Values (selection)

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

Independent WAN
Bridged with LAN Port
 Independent LAN

Connection Type

Values (selection)

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

DHCP
 Static

IP Address

Values (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.

(no default)

Netmask

Values (IP Address)

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.

(no default)

4.0 Configuration

Default Gateway

If the IPnXGii 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)

WAN DNS Servers

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

Values (IP Address)

(no default)

4.0 Configuration

4.2.4 Network > DHCP

The DHCP menu allows a user to view the current DHCP assignments and remaining lease time, as well as logically bind a MAC address to an IP address. This is often used in cases where it is desired to use DHCP to assign IP addresses, but a known address must be given to specific devices (e.g. Port Forwarding). To configure the actual DHCP server, and to assign the valid IP Address ranges, use the configuration tools under the LAN menu.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				
DHCP Configuration											
Static IP addresses (for DHCP)											
Name		<input type="text"/>									
MAC Address		<input type="text"/>									
IP Address		<input type="text"/>									
<input type="button" value="Add static IP"/>											
Static Addresses											
MAC Address	IP Address	Name	NetStatus								
Active DHCP Leases											
MAC Address	IP Address	Name	Expires in								
There are no known DHCP leases.											
<input type="button" value="Release All"/> <input type="button" value="Refresh"/>											

Image 4-2-5: Network > DHCP Leases

NAME

For future reference purposes, you must name the MAC binding rules.

Values

(no default)

MAC Address

Enter the physical MAC address of the device or interface that will be assigned the specified IP Address if it requests a DHCP address.

Values

(no default)

IP Address

Enter the IP address to be assigned to the MAC address. Ensure this is a valid address on the current subnet.

Values

(no default)

4.0 Configuration

4.2.5 Network > DDNS

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				

DDNS Configuration

Configuration

DDNS status:

Network:

Service:

User Name:

Password:

Host:

Image 4-2-6: Carrier > Traffic Watchdog

DDNS Status

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

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 IPnXGii as assigned by the DDNS provider.

Values (domain name)

(none)

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 IPnXGii where to send data.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				

Static Routes Configuration

Static Route Configuration

Name	<input type="text" value="route1"/>
Destination	<input type="text" value="192.168.168.0"/>
Gateway	<input type="text" value="192.168.168.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Interface	<input type="text" value="LAN"/>

Static Route Summary

Name	Destination	Gateway	Subnet Mask	Interface
route1	192.168.168.0	192.168.168.1	255.255.255.0	LAN

Image 4-2-7: Network > Routes

	Name
Routes can be names for easy reference, or to describe the route being added.	Values (characters) <i>(no default)</i>
Destination	
Enter the network IP address for the destination.	Values (IP Address) <i>(192.168.168.0)</i>
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
<p>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.</p>		<p>Values (Integer)</p> <p>255.255.255.0</p>
		Interface
<p>Define the exit interface. Is the destination a device on the LAN, LAN1 (If physical WAN port is bridged as an independent LAN), 3G/4G (cellular), USB or the WAN?</p>		<p>Values (Selection)</p> <p>LAN / LAN1 / WAN / Cell / USB None</p>

4.2.7 Network > Ports

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				
Ethernet Port Configuration											
Port	Mode	Auto-Negotiation		Speed		Duplex					
WAN	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> On <input type="radio"/> Off		<input checked="" type="radio"/> 100Mbit/s <input type="radio"/> 10Mbit/s		<input checked="" type="radio"/> Full <input type="radio"/> Half					
LAN	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> On <input type="radio"/> Off		<input checked="" type="radio"/> 100Mbit/s <input type="radio"/> 10Mbit/s		<input checked="" type="radio"/> Full <input type="radio"/> Half					
Ethernet Port Status											
Port	Linked	Auto-Negotiation		Speed		Duplex					
WAN	no	on		10Mb/s		Half					
LAN	yes	on		100Mb/s		Full					

Image 4-2-8: Network > Ports

4.2.8 Network > Device List

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	LAN	WAN	DHCP	DDNS	Routes	Ports	Device List				
Network Device List											
MAC Address		IP Address			Ageing Timer						
00:80:c8:3c:fb:fb		192.168.168.200			0.19						

Image 4-2-9: Network > Device List

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 IPnXGii. 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.

The screenshot displays the Carrier Status window with the following data:

Carrier Status - LN930			
Current APN	wrstat.bell.ca	Core Temperature(°C)	36
Activity Status	Connected	IMEI	356406060021903
Network	Bell	SIM PIN (Card-1)	READY
Home/Roaming	Home	SIM Number (ICCID)	89302610203010832398
Service Mode	E-UTRAN	Phone Number	15874327939
Service State	E-UTRAN	RSSI (dBm)	-90
Cell ID	28963586	RSRP/Q (dBm/dB)	-88 / -7
LAC	11204	SINR (dB)	13
Current Technology	LTE	Connection Duration	23 hour 22 min 54 sec
Available Technology	LTE,UMTS,GSM	WAN IP Address	184.151.220.2
Frequency Band(MHz)	BAND_LTE_4	DNS Server 1	70.28.245.227
		DNS Server 2	184.151.118.254
Received Packet Statistics		Transmitted Packet Statistics	
Receive bytes	45.339KB	Transmit bytes	21.038KB
Receive packets	557	Transmit packets	230
Receive errors	0	Transmit errors	0
Drop packets	0	Drop packets	0

Stop Refreshing Interval: 20 (in seconds)

Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii

Image 4-3-1: Carrier > Status

Not all statistics parameters displayed are applicable.

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

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

4.0 Configuration

4.3.2 Carrier > Settings

The parameters within the Carrier Configuration menu must be input properly; they are the most basic requirement required by your cellular provider for network connectivity. The IPn3Gii/4Gii can support dual SIM cards, as described below either slot can be specified as the primary slot and if a connectivity issue occurs, the unit can be configured to automatically switch to the alternate SIM card.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status	Settings	SMS	SMSConfig	DataUsage							
Carrier Configuration											
General											
Carrier status	Enable ▼										
IP-Passthrough	Disable ▼										
SIM Selection	Dual SIM Cards ▼										
Dual Cards Management											
Primary Slot	SIM Card-1 ▼										
Start Over	Enable ▼										
Switch Over	Enable ▼										
Switch Timeout(in seconds)	600										
Keepalive	Enable ▼										
SIM Card-1 (Top slot) Settings											
SIM Number(ICCID)	89302610203010832398										
Data Roaming	Disable ▼										
Carrier Operator	Auto ▼										
Technologies Mode	AUTO ▼ Advanced										
APN	wrstat.bell.ca										
<input type="checkbox"/> Advanced+											
<input checked="" type="checkbox"/> Network+											

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

IP-Passthrough

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

Values (Selection)

Disable
Ethernet (LAN)
WAN

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

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

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

4.0 Configuration

SIM Selection

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

This behavior can be modified using the *Dual Cards Management* section below.

Values (Selection)

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

Dual Cards Management

Primary Slot

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

Values (Selection)

SIM Card-1
SIM Card-2

Start Over

Start Over allows the IPnXGii to use the secondary slot to establish a connection with the cellular carrier in the case that the primary card is not installed or is otherwise not functioning.

Values (Selection)

Enable / Disable

Switch Over

If enabled this feature allows the IPnXGii to switch from the currently connected SIM (Carrier), to the alternate after it has determined that the current carrier is not reachable. The Switch Timeout determines when this will happen.

Values (Selection)

Enable / Disable

Switch Timeout

The amount of inactivity(time) to the current SIM (Carrier), before the IPnXGii will switch to the alternate SIM(Carrier).

Values (Selection)

600

Keepalive

This allows the IPnXGii to use the currently configured System > Keepalive settings to determine how to check if the IPnXGii has lost connection to the current Carrier/SIM.

Values (Selection)

Enable / Disable

4.0 Configuration

SIM Card-1 Settings

Data Roaming

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

Values (Selection)

Enable / **Disable**

Carrier Operator

In some cases, a user may want to lock onto certain carrier to avoid data roaming. There were four options presented to a user to choose from, Auto, SIM based, Scan & Select and Fixed.

Values (Selection)

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

Auto
Based on SIM
Manual
Fixed

Technologies Mode

Select the valid types of Carrier connections allowed. For example if set to auto the IPn3Gii will connect to any data type. If set to 3G-WCDMA only, the IPn3Gii will only allow connection to 3G related technologies, and not allow the device to connect to lesser (slower) technologies.

Values (IPn3Gii)

AUTO
3G-WCDMA Only
2G-GPRS Only

Values (IPn4Gii)

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

Verizon IPn4Gii Models: AUTO:LTE Only

APN (Access Point Name)

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

Values (characters)

auto

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

Connect Mode (Verizon)

IPn4Gii Verizon models initialized on the Verizon network will automatically configure the required settings needed to establish a connection with Verizon as a Wireless Carrier.

Values (characters)

Verizon Auto Connection
Defined Network (Test)

4.0 Configuration

Advanced+

SIM Pin

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

Values (characters)

(none)

Authentication

Sets the authentication type required to negotiate with peer.

Values (Selection)

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

Device decide (AUTO)

PAP
CHAP
No Auth

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

User Name

A User Name may be required for authentication to a remote peer. Although usually not required for dynamically assigned IP addresses from the wireless carrier. Varies by carrier.

Values (characters)

Carrier/peer dependant

Password

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

Values (characters)

Carrier/peer dependant

Dial-on-Demand (3G)

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

Values (selection)

Disable / Enable

Dial Number (3G)

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

Values (String)

*99***1#

Dialing Max Retries (3G)

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

Values

0-100

Idle Time Out (3G)

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

Values (seconds)

0-65535

4.0 Configuration

Connect Time Out (3G)

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

Values (seconds)

0-65535

Connect String (3G)

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

Values (string)

CONNECT

Network+

IP Address

In some cases the Static IP address must be entered in this field if assigned by a wireless carrier. In most cases the IP will be read from the SIM card and this field should be left at the default value.

Values (IP Address)

(none)

Use Remote DNS

If enabled the Bullet will use the DNS server as specified automatically by the service provider.

Values (selection)

Enable / Disable

Default Route

Use this interface as the default route for all outbound traffic unless specified in the Network > Routes table.

Values (Selection)

Yes / No

IP-Passthrough Mode

When unit is set to operate in IP-Passthrough mode in the general settings, this will allow the unit to automatically assign the carrier IP to the end device or use the specified Gateway /Netmask.

Values (Selection)

Auto / Manual

DNS-Passthrough

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

Values (Selection)

Enable / Disable

SIM Card-2 Settings

Settings for SIM Card-2 are identical to that of SIM Card-1, refer to the previous section for information on how to configure SIM Card-2.

4.0 Configuration

4.3.3 Carrier > SMS

SMS Command History

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status	Settings	SMS	SMSConfig	DataUsage							
SMS Command History											
From	Send Time	Content	Result								
+14036129217	15/04/15,12:30:01-16	MSC#REBOOT	Run:reboot @Wed Apr 15 10:29:46 2015								
+14036129217	15/04/15,12:32:33-16	MSC#REBOOT	Expired, no running. @Wed Apr 15 10:33:15 2015								
+14036129217	15/04/15,12:35:48-16	MSC#REBOOT	Run:reboot @Wed Apr 15 10:35:49 2015								
SMS Untreated In SIM Card											
No.	From	Time	Content								
1	+14036129217	15/04/15,12:26:40-16	This is an service alert. Tech on site. Delete Reply								
2	+14036129217	15/04/15,12:27:33-16	Site address is 123 Main Street Delete Reply								
3	+14036129217	15/03/24,18:36:53-16	Message received! OK Delete Reply								
<input type="button" value="Delete All Above SMS"/> <input type="button" value="Send New SMS"/>											

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

Send SMS Message

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status	Settings	SMS	SMSConfig	DataUsage							
SMS Send											
Finished send to:4036129217											
Send text: This is a test message. #1 of ?											
New SMS											
Send To: <input type="text"/>											
Text: <input type="text"/>											
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>											
SMS Send History											
Send To	Send Time	Content	Result								
4036129217	Wed Apr 15 10:40:22 2015	This is a test message. #1 of ?	Succeed to send.								

Image 4-3-4: SMS > SMS Send

4.0 Configuration

4.3.4 Carrier > SMS Config

SMS messages can be used to remotely reboot or trigger events in the IPnXGii. 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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status	Settings	SMS	SMSConfig	DataUsage							
SMS Configuration											
System SMS Command:											
Status	Enable SMS Command ▼										
Set Phone Filter	Enable Phone Filter ▼										
Valid Phone Numbers:											
Phone No.1	<input type="text"/>										
Phone No.2	<input type="text"/>										
Phone No.3	<input type="text"/>										
Phone No.4	<input type="text"/>										
Phone No.5	<input type="text"/>										
Phone No.6	<input type="text"/>										

Image 4-3-5: 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 IPnXGii:

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#MIOP5 open I/O ouput5
 MSC#MIOP6 open I/O ouput6
 MSC#MIOP7 open I/O ouput7
 MSC#MIOP8 open I/O ouput8
 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#MIOC5 close I/O ouput5
 MSC#MIOC6 close I/O ouput6
 MSC#MIOC7 close I/O ouput7
 MSC#MIOC8 close I/O ouput8
 MSC#EURD0 trigger event report0
 MSC#EURD1 trigger event report1
 MSC#EURD2 trigger event report2
 MSC#EURD3 trigger event report3
 MSC#GPSR0 trigger gps report0
 MSC#GPSR1 trigger gps report1
 MSC#GPSR2 trigger gps report2
 MSC#GPSR3 trigger gps report3

Set Phone Filter

If enabled, the IPnXGii 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

System SMS Alert:

Status Enable SMS Alert ▾

Received Phone Numbers:

Phone No.1

Phone No.2

Phone No.3

Phone No.4

Phone No.5

Phone No.6

Alert Condition Settings:

Time Interval(s) [5~65535]

RSSI Check Enable RSSI Check ▾

Low Threshold(dBm): default: -99

Carrier Network Enable Roaming Check ▾

Home/Roaming Status: ▾

Ethernet Enable Ethernet Check ▾

Link Status: ▾

IO Status Disable IO Check ▾

[View Alert SMS Record](#)

Image 4-3-6: SMS > SMS Alerts

	Status
<p>Enable SMS Alerts. IF enabled SMS alerts will be send when conditions are met as configured to the phone numbers listed.</p>	<p>Values (Selection)</p> <p>Enable / Disable</p>
	Received Phone Numbers
<p>SMS Alerts can be sent to up to 6 different phone numbers that are listed here.</p>	<p>Values (Selection)</p> <p>(no default)</p>
	Time Interval(s)
<p>SMS alerts, when active, will be sent out at the frequency defined here.</p>	<p>Values (Seconds)</p> <p>300</p>
	RSSI Check
<p>Enable or disable the RSSI alerts.</p>	<p>Values (Selection)</p> <p>Disable RSSI check Enable RSSI check</p>

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 IPnXGii can send alerts based on the roaming status. Data rates during roaming can be expensive and it is important to know when a device has started roaming.

Values (Selection)

In Roaming
Changed or In Roaming
Changed to Roaming

Ethernet

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

Values (Selection)

Disable Ethernet check
Enable Ethernet check

Ethernet Link Status

The status of the Ethernet Link of the LAN (RJ45) can be used to send SMS Alerts. The link status may indicate an issue with the connected device.

Values (Selection)

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

I/O Status

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

Values (Selection)

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

4.0 Configuration

4.3.5 Carrier > Data Usage

The Data Usage tool on the IPnXGii 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 IPnXGii.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Status	Settings	SMS	SMSConfig	DataUsage							
Data Usage Monitor											
Data Usage Statistic											
Today's Usage: 19.891 KB											
Yesterday's Usage: 39.040 KB											
Current Monthly Usage: 1.539 MB											
Last Monthly Usage: 3.209 KB											
Reset and Clear all Record: Reset Record To Zero											
Attention:Data usage statistic is not exact same to your carrier's caculation on your monthly bill with different systems.											
Data Usage Monitor											
Status: <input type="checkbox"/> Enable Data Usage Monitor											
Last Config Time: Tue Mar 31 14:52:32 MDT 2015											
Monthly Over Limit: <input type="checkbox"/> Send Notice SMS											
Monthly Data Units: M Bytes											
Data Limit: 500 [1~65535]											
Period Start Day: 1 [1~31](day of month)											
Phone Number: +1403											
Daily Over Limit: <input type="checkbox"/> Send Notice Email											
Daily Data Units: M Bytes											
Data Limit: 50 [1~65535]											
Mail Subject: Daily Data Usage Notice											
Mail Server(IP/Name): smtp.gmail.com:465 (xxx:port)											
User Name: @gmail.com											
Password: ***											
Authentication: None											
Mail Recipient: host@ (xx@xx.xx)											

Image 4-3-7: Carrier > Data Usage

Status	Values (selection)
Disable	Enable

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

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 4-3-9: Data Usage > SMS Config

Monthly/Daily Data Unit

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

Values (selection)

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

Data Limit

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

Values (1-65535)

500

Period Start Day

For Monthly tracking, select the day the billing/data cycles begins. On this day each month the IPnXGii 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 4-3-10: 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 Firewall

4.4.1 Firewall > Summary

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin																																																																																																																																																																																																																																																																																														
<div style="display: flex; border-bottom: 1px solid black;"> Summary General Port Forwarding MAC-IP List Rules Firewall Default </div> <p>Firewall Status</p> <p>Status and Rules All <input type="button" value="Check"/></p> <p>Target Filter</p> <p>Chain INPUT (policy ACCEPT 0 packets, 0 bytes)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>838</td> <td>42587</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>ctstate RELATED,ESTABLISHED</td> </tr> <tr> <td>2</td> <td>29</td> <td>1518</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>lo</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>3</td> <td>5</td> <td>260</td> <td>syn_flood</td> <td>tcp</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>tcp flags:0x17/0x02</td> </tr> <tr> <td>4</td> <td>30</td> <td>2541</td> <td>input_rule</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>5</td> <td>30</td> <td>2541</td> <td>input</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> <p>Chain FORWARD (policy DROP 0 packets, 0 bytes)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>0</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>ctstate RELATED,ESTABLISHED</td> </tr> <tr> <td>2</td> <td>0</td> <td>0</td> <td>forwarding_rule</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>3</td> <td>0</td> <td>0</td> <td>forward</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>4</td> <td>0</td> <td>0</td> <td>reject</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> <p>Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>868</td> <td>111K</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td>ctstate RELATED,ESTABLISHED</td> </tr> <tr> <td>2</td> <td>29</td> <td>1518</td> <td>ACCEPT</td> <td>all</td> <td>--</td> <td>*</td> <td>lo</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>3</td> <td>4</td> <td>160</td> <td>output_rule</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>4</td> <td>4</td> <td>160</td> <td>output</td> <td>all</td> <td>--</td> <td>*</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> <p>Chain dropBrute (2 references)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Chain forward (1 references)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> <td>0</td> <td>zone_lan_forward</td> <td>all</td> <td>--</td> <td>br-lan</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>2</td> <td>0</td> <td>0</td> <td>zone_wan2_forward</td> <td>all</td> <td>--</td> <td>br-wan2</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> <tr> <td>3</td> <td>0</td> <td>0</td> <td>zone_lan_forward</td> <td>all</td> <td>--</td> <td>br-usb</td> <td>*</td> <td>0.0.0.0/0</td> <td>0.0.0.0/0</td> <td></td> </tr> </tbody> </table> <p>Chain forwarding_lan (1 references)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Chain forwarding_rule (1 references)</p> <table border="1"> <thead> <tr> <th>num</th> <th>pkts</th> <th>bytes</th> <th>target</th> <th>prot</th> <th>opt</th> <th>in</th> <th>out</th> <th>source</th> <th>destination</th> <th>options</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>												num	pkts	bytes	target	prot	opt	in	out	source	destination	options	1	838	42587	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	2	29	1518	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0		3	5	260	syn_flood	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	4	30	2541	input_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0		5	30	2541	input	all	--	*	*	0.0.0.0/0	0.0.0.0/0		num	pkts	bytes	target	prot	opt	in	out	source	destination	options	1	0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	2	0	0	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0		3	0	0	forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0		4	0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0		num	pkts	bytes	target	prot	opt	in	out	source	destination	options	1	868	111K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	2	29	1518	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0		3	4	160	output_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0		4	4	160	output	all	--	*	*	0.0.0.0/0	0.0.0.0/0		num	pkts	bytes	target	prot	opt	in	out	source	destination	options												num	pkts	bytes	target	prot	opt	in	out	source	destination	options	1	0	0	zone_lan_forward	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0		2	0	0	zone_wan2_forward	all	--	br-wan2	*	0.0.0.0/0	0.0.0.0/0		3	0	0	zone_lan_forward	all	--	br-usb	*	0.0.0.0/0	0.0.0.0/0		num	pkts	bytes	target	prot	opt	in	out	source	destination	options												num	pkts	bytes	target	prot	opt	in	out	source	destination	options											
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
1	838	42587	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED																																																																																																																																																																																																																																																																																															
2	29	1518	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
3	5	260	syn_flood	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02																																																																																																																																																																																																																																																																																															
4	30	2541	input_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
5	30	2541	input	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
1	0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED																																																																																																																																																																																																																																																																																															
2	0	0	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
3	0	0	forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
4	0	0	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
1	868	111K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED																																																																																																																																																																																																																																																																																															
2	29	1518	ACCEPT	all	--	*	lo	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
3	4	160	output_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
4	4	160	output	all	--	*	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
1	0	0	zone_lan_forward	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
2	0	0	zone_wan2_forward	all	--	br-wan2	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
3	0	0	zone_lan_forward	all	--	br-usb	*	0.0.0.0/0	0.0.0.0/0																																																																																																																																																																																																																																																																																																
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															
num	pkts	bytes	target	prot	opt	in	out	source	destination	options																																																																																																																																																																																																																																																																																															

Image 4-4-1: Firewall > Status

4.0 Configuration

4.4.2 Firewall > General

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

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

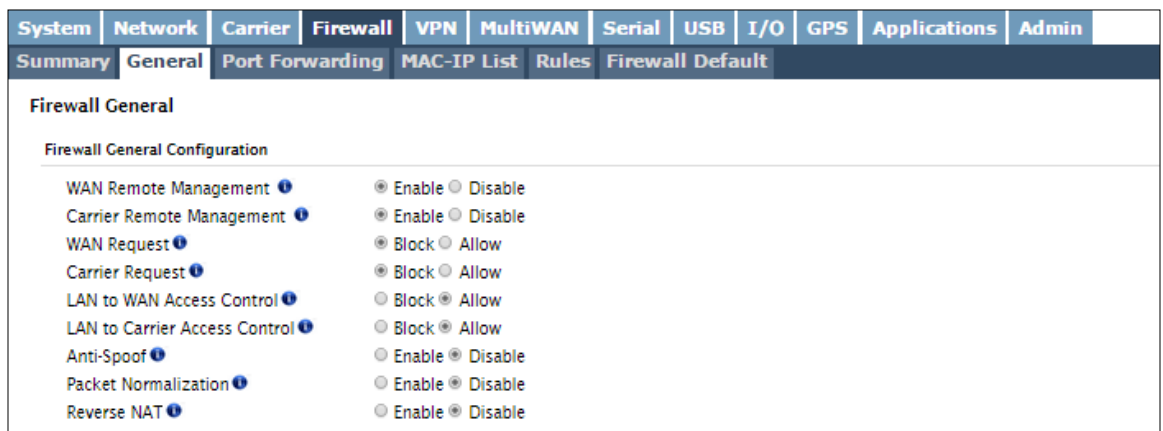


Image 4-4-2: Firewall > General



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

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



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

WAN Remote Management

Allow remote management of the IPnXGii on the WAN side using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or Cellular if enabled)..

Values

Enable / Disable

Carrier Remote Management

Allow remote management of the IPnXGii from the Cellular side of using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN (or WAN if enabled)..

Values

Enable / Disable

WAN Request

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

Values

Block / Allow

Carrier Request

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

Values

Block / Allow

4.0 Configuration

LAN to WAN Access Control

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

Values

Block / **Allow**

LAN to Carrier Access Control

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

Values

Block / **Allow**

Anti-Spoof

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

Values

Enable / **Disable**

Packet Normalization

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

Values

Enable / **Disable**

Reverse NAT

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

Values

Enable / **Disable**

4.0 Configuration

4.4.3 Firewall > Port Forwarding

The IPnXGii 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 IPnXGii. 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 IPnXGii, in this case all traffic is passed to a single device connected to the RJ45 port of the IPnXGii, The device must be set for DHCP, as the IPnXGii 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 IPnXGii, as well as all other features of the IPnXGii such as COM, VPN, GPS etc.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default						

Firewall Port Forwarding

Notice

Port Forwarding Rules are taken into consideration after the General firewall settings are applied. If the WAN and/or cellular traffic is blocked, additional rules must be created:

1. Add rules in the Rules configuration to open ports or allow IP addresses.
2. Create a IP/Mac List to allow desired connections.

Firewall DMZ Configuration

DMZ Mode:

DMZ Source:

DMZ Server IP:

Exception Port:

Firewall Port Forwarding Configuration

Name:

Source:

Internal Server IP:

Internal Port:

Protocol:

External Port:

Firewall Port Forwarding Summary

Name	Source	Internal IP	Internal Port	Protocol	External Port
forward1	Carrier	192.168.2.1	3000	TCP	2000

Image 4-4-3: Firewall > Port Forwarding



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

DMZ Mode
Values (selection)
Disable / Enable

Enable or disable DMZ Mode. DMZ can be used to forward all traffic to the DMZ Server IP listed below.

4.0 Configuration



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

DMZ Source	
Select the source for the DMZ traffic, either Carrier or from the WAN port..	Values (selection)
	Carrier / WAN
DMZ Server IP	
Enter the IP address of the device on the LAN side of the IPnXGii where all the traffic will be forwarded to.	Values (IP Address)
	192.168.100.100
Exception Port	
Enter a exception port number that will NOT be forwarded to the DMZ server IP. Usually a configuration or remote management port that is excluded to retain external control of the IPnXGii.	Values (Port #)
	0
Firewall Port Forwarding Configuration	
Name	
This is simply a field where a convenient reference or description is added to the rule. Each Forward must have a unique rule name and can use up to 10 characters.	Values (10 chars)
	Forward
Source	
Select the source for the traffic, from either the 3G/Cellular or from the WAN.	Values (selection)
	Carrier / WAN
Internal Server IP	
Enter the IP address of the intended internal (i.e. on LAN side of IPnXGii) server. This is the IP address of the device you are forwarding traffic to.	Values (IP Address)
	192.168.2.1
Internal Port	
Target port number of the internal server on the LAN IP entered above.	Values (Port #)
	3000
Protocol	
Select the type of transport protocol used. For example Telnet uses TCP, SNMP uses UDP, etc.	Values (selection)
	TCP / UDP / Both
External Port	
Port number of the incoming request (from 4G/WAN-side).	Values (Port #)
	2000

4.0 Configuration

4.4.4 Firewall > MAC-IP List

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default						
Firewall MAC/IP List											
Firewall MAC List Configuration											
Name	mac1										
Action	Accept ▼										
Mac Address	00:00:00:00:00:00										
Add Mac List											
Firewall IP List Configuration											
Name	ip1										
Action	Accept ▼										
Source	None ▼										
Source IPs	<input checked="" type="radio"/> IP range <input type="radio"/> Subnet / prefix										
	0.0.0.0	To									0.0.0.0
Destination IPs	<input checked="" type="radio"/> IP range <input type="radio"/> Subnet / prefix										
	0.0.0.0	To									0.0.0.0
Add IP List											
Firewall MAC List Summary											
Name	Action	Mac Address									
Firewall IP List Summary											
Name	Action	Src	Src IP From	Src IP To	/Prefix	Dest IP From	Dest IP To	/Prefix			

Image 4-4-5: 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.	Values (selection)
ACCEPT will allow a connection, while REJECT (error) and DROP (quietly dropped), will refuse connections.	ACCEPT DROP REJECT

Firewall IP List Configuration

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

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

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

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

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

4.0 Configuration

4.4.5 Firewall > Rules

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

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



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

Appendix D: Firewall Example

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	General	Port Forwarding	MAC-IP List	Rules	Firewall Default						
Firewall Rules											
Firewall Rules Configuration											
Rule Name	rule1										
ACTION	Accept										
Source	None										
Source IPs	<input checked="" type="radio"/> IP range <input type="radio"/> Subnet / prefix 0.0.0.0 To 0.0.0.0										
Destination	None										
Destination IPs	<input checked="" type="radio"/> IP range <input type="radio"/> Subnet / prefix 0.0.0.0 To 0.0.0.0										
Destination Port	0										
Protocol	TCP										
Add Rule											
Firewall Rules Summary											
Name	Action	Src	Src IP From	Src IP To	/Prefix	Dest	Dest IP From	Dest IP To	/Prefix	Dest Port	Protocol

Image 4-4-6: Firewall > Rules

Rule Name

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

Values (10 Chars)

characters

Action

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

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

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

Values (selection)

ACCEPT
DROP
REJECT

Source

Select the zone which is to be the source of the data traffic. 3G/Cellular applies to the connection to the cellular carrier. The LAN/LAN1/USB refers to local connections on the IPnXGii.

Values

LAN/LAN1/WAN/Cell/USB/
None

4.0 Configuration

<p>Match incoming traffic from the specified source IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</p>	<p>Source IPs</p> <p>Values (IP Address)</p> <p>192.168.0.0 to 192.168.0.0</p>
<p>Select the zone which is the intended destination of the data traffic. 3G/4G applies to the wireless connection to the cellular carrier and the LAN, LAN1, USB refers to local connections on the IPnXGii.</p>	<p>Destination</p> <p>Values (selection)</p> <p>LAN/LAN1/Cell/WAN/USB None</p>
<p>Match incoming traffic from the specified destination IP range. Boxes accept single IP Addresses without network masks, example: 192.168.1.0 to 192.168.1.255 represents all IP Addresses in the 192.168.1.0/24 network. (Put same IP in both boxes for a single IP match.)</p>	<p>Destination IPs</p> <p>Values (IP Address)</p> <p>192.168.0.0 to 192.168.0.0</p>
<p>Match incoming traffic directed at the given destination port or port range.</p> <p>(To specify a port range use a From:To (100:200) format)</p>	<p>Destination Port</p> <p>Values (port)</p> <p>0</p>
<p>The protocol field defines the transport protocol type controlled by the rule.</p>	<p>Protocol</p> <p>Values</p> <p>TCP UDP Both ICMP</p>

4.0 Configuration

4.4.6 Firewall > Firewall Default

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

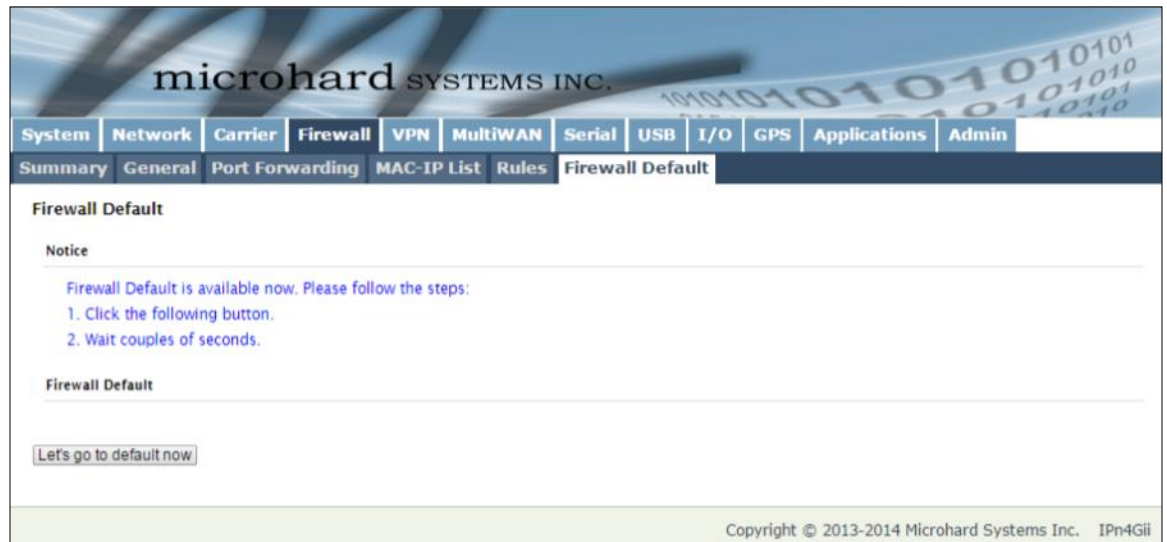


Image 4-4-7: Firewall > Firewall Default

4.0 Configuration

4.5 VPN

4.5.1 VPN > Summary

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

The screenshot displays the VPN configuration summary page. At the top, there is a navigation menu with tabs for System, Network, Carrier, Firewall, VPN (selected), MultiWAN, Serial, USB, I/O, GPS, Applications, and Admin. Below the menu, there are sub-tabs for Summary, Gateway To Gateway, Client To Gateway, GRE, L2TP Users, and Certificates. The main content area is titled 'Summary' and contains several sections:

- Gateway To Gateway:** A table with columns: No., Name, Status, Phase2 Enc/Auth/Grp, Interface, Local Group, Remote Group, Remote Gateway, RX/TX Bytes, Tunnel Test, and Config. An 'Add' button is present below the table.
- L2TP Client To Gateway:** A table with columns: No., Name, Status, Interface, Local/Remote IP Address, Server Gateway, Start Time, Duration, RX/TX Bytes, Tunnel Test, and Config. An 'Add' button is present below the table.
- L2TP Server:** A table with columns: Status, Interface, Local IP, Client IP Range Start, Client IP Range End, and Config. Two rows are shown: one for 'WAN' and one for '4G', both with a status of 'disable'. 'Edit' buttons are present for each row.
- L2TP Connection List:** A table with columns: No., Remote Address, L2TP IP Address, Start Time, Duration, RX Bytes, and TX Bytes.
- OpenVPN Server - Connection List:** A table with columns: No., Client Name, Remote Address, Virtual IP, Start Time, TCP/UDP RX Bytes, and TCP/UDP TX Bytes.
- OpenVPN Client - Connection Status:** A table with columns: No., VPN Virtual IP Address, TUN RX Bytes, TUN TX Bytes, TCP/UDP RX Bytes, and TCP/UDP TX Bytes.
- GRE Tunnels List:** A table with columns: No., Name, Status, Multicast, ARP TTL, IPsec, Local Tunnel IP, Local Gateway, Local Subnet, Remote Gateway, Remote Subnet, RX/TX Bytes, Tunnel Test, and Config. An 'Add' button is present below the table.
- L2TP Users:** A table with columns: No., Username, and Config. An 'Add' button is present below the table.

Image 4-5-1: VPN > Summary

4.0 Configuration

4.5.2 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 IPnXGii and another device (another IPnXGii 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.

System	Network	Carrier	Firewall	VPN	MultIWAN	Serial	USB	I/O	GPS	Applications	Admin
<div style="display: flex; border-bottom: 1px solid black; margin-bottom: 5px;"> Summary Gateway To Gateway Client To Gateway GRE L2TP Users Certificates </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Gateway To Gateway</p> <p>Add a New Tunnel</p> <p>Tunnel Name <input type="text"/></p> <p>Enable <input checked="" type="checkbox"/></p> <p>Authentication Preshared Key ▼</p> <p>Interface 4G ▼</p> <hr/> <p>Local Group Setup</p> <p>Local Security Gateway Type IP Only ▼</p> <p>Interface IP Address 184.151.220.2</p> <p>Next-hop Gateway IP <input type="text"/></p> <p>Group Subnet Gateway <input type="text"/></p> <p>Group Subnet IP/Mask - 1 / 255.255.255.0</p> <p style="text-align: right;">Add Remove</p> <hr/> <p>Remote Group Setup</p> <p>Remote Security Gateway Type IP Only ▼</p> <p>Gateway IP Address <input type="text"/></p> <p>Next-hop Gateway IP <input type="text"/></p> <p>Group Subnet IP/Mask - 1 / 255.255.255.0</p> <p style="text-align: right;">Add Remove</p> <hr/> <p>IPSec Setup</p> <p>Aggressive Mode <input type="checkbox"/></p> <p>Phase1 Strict Mode: <input type="checkbox"/></p> <p>Phase 1 DH Group modp1024 ▼</p> <p>Phase 1 Encryption 3des ▼</p> <p>Phase 1 Authentication md5 ▼</p> <p>Phase 1 SA Life Time(s) 28800</p> <p>Perfect Forward Secrecy <input type="checkbox"/></p> <p>Phase 2 SA Type ESP ▼</p> <p>Phase2 Strict Mode: <input type="checkbox"/></p> <p>Phase 2 DH Group modp1024 ▼</p> <p>Phase 2 Encryption 3des ▼</p> <p>Phase 2 Authentication md5 ▼</p> <p>Phase 2 SA Life Time(s) 3600</p> <p>Preshared Key <input type="text"/></p> <p>DPD Delay(s) 32</p> <p>DPD Timeout(s) 122</p> <p>DPD Action hold ▼</p> </div>											

Image 4-5-2: 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 IPnXGii, 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

<p>Group Subnet Mask</p> <p>Specify the subnet mask of the local network address.</p>	<p>Values (IP Address)</p> <p>255.255.255.0</p>
<p>Group Subnet Gateway</p> <p>Enter the Gateway for the local group network.</p>	<p>Values (IP Address)</p> <p>(no default)</p>
<p>Remote Group Setup</p>	
<p>Remote Security Gateway Type</p> <p>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)</p>	<p>Values (selection)</p> <p>IP Only IP + Server ID Dynamic IP + Server ID</p>
<p>Gateway IP Address</p> <p>If the remote VPN router has a static IP address, enter the IP address of the remote VPN Gateway here.</p>	<p>Values (IP Address)</p> <p>(no default)</p>
<p>Server ID</p> <p>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 @<u>name</u>, where name can be anything. Both routers must know each others names to establish a connection.</p>	<p>Values (IP Address)</p> <p>(no default)</p>
<p>Next-hop Gateway IP</p> <p>Next-hop Gateway means the next-hop gateway IP address for the local or remote gateway participant's connection to the public network.</p>	<p>Values (IP Address)</p> <p>(no default)</p>
<p>Subnet IP Address</p> <p>Define the remote network by specifying the local subnet.</p>	<p>Values (IP Address)</p> <p>(no default)</p>
<p>Subnet Mask</p> <p>Specify the subnet mask of the remote network address.</p>	<p>Values (IP Address)</p> <p>255.255.255.0</p>

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

4.5.3 VPN > Client To Gateway (L2TP Client)

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #2c4e64; color: white; padding: 2px; margin-bottom: 5px;"> Summary Gateway To Gateway Client To Gateway GRE L2TP Users Certificates </div> <div style="margin-bottom: 10px;"> <p>L2TP Client</p> <p>Add a New Tunnel</p> <p>Tunnel Name <input type="text"/></p> <p>Enable <input checked="" type="checkbox"/></p> <p>IPsec <input checked="" type="checkbox"/></p> <p>Interface <input type="text" value="4G"/></p> </div> <div style="margin-bottom: 10px;"> <p>Local Group Setup</p> <p>Local Security Gateway Type <input type="text" value="IP Only"/></p> <p>Interface IP Address <input type="text" value="184.151.220.2"/></p> <p>Next-hop Gateway IP <input type="text"/></p> </div> <div style="margin-bottom: 10px;"> <p>Remote Group Setup</p> <p>Remote Security Gateway Type <input type="text" value="IP + Server ID"/></p> <p>Gateway IP Address <input type="text"/></p> <p>Server ID <input type="text"/></p> <p>Next-hop Gateway IP <input type="text"/></p> <p>Group Subnet IP <input type="text"/></p> <p>Group Subnet Mask <input type="text" value="255.255.255.0"/></p> </div> <div style="margin-bottom: 10px;"> <p>PPP Setup</p> <p>Idle time before hanging up <input type="text" value="0"/> [0...65535](s)</p> <p>PAP <input type="checkbox"/> Unencrypted Password</p> <p>CHAP <input checked="" type="checkbox"/> Challenge Handshake Authentication Protocol</p> <p>User Name <input type="text"/></p> <p>Redial <input checked="" type="checkbox"/></p> <p>Redial attempts <input type="text" value="3"/></p> <p>Time between redial attempts <input type="text" value="15"/></p> </div> <div style="margin-bottom: 10px;"> <p>IPSec Setup</p> <p>Authentication <input type="text" value="Preshared Key"/></p> <p>Phase 1 SA Life Time(s) <input type="text" value="28800"/></p> <p>Perfect Forward Secrecy <input type="checkbox"/></p> <p>Phase 2 SA Life Time(s) <input type="text" value="3600"/></p> <p>Preshared Key <input type="text"/></p> <p>DPD Delay(s) <input type="text" value="32"/></p> <p>DPD Timeout(s) <input type="text" value="122"/></p> <p>DPD Action <input type="text" value="clear"/></p> <p><input type="checkbox"/> Advanced-</p> </div> </div>											

Image 4-5-3: 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 IPnXGii WAN (3G/Cellular) IP Address.

Values (IP Address)

Current IP

Remote Gateway IP Address

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

Values (IP Address)

none

Remote Server ID

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

Values

none

Remote Subnet IP

In order to communicate with the devices on the other side of the tunnel, the IPnXGii 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

4.5.4 Network > GRE

GRE Configuration

The IPnXGii 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.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	Gateway To Gateway	Client To Gateway	GRE	L2TP Users	Certificates						
Add a New Tunnel											
Name	<input type="text"/>										
Enable	<input type="checkbox"/>										
Multicast	<input type="checkbox"/>										
TTL	<input type="text"/>										
Key	<input type="text"/>										
ARP	<input type="checkbox"/>										
NAT	<input type="checkbox"/>										
Interface	4G ▼										
Local Setup											
Gateway IP Address	<input type="text"/>										
Tunnel IP Address	<input type="text"/>										
Netmask	<input type="text"/>										
Subnet IP Address	<input type="text"/>										
Subnet Mask	<input type="text"/>										
Remote Setup											
Gateway IP Address	<input type="text"/>										
Subnet IP Address	<input type="text"/>										
Subnet Mask	<input type="text"/>										
IPsec Setup											
Enable	None ▼										

Image 4-5-4: Network > Edit/Add GRE Tunnel

Name
<p>Each GRE tunnel must have a unique name. Up to 10 GRE tunnels are supported by the IPnXGii.</p>
<p>Values (Chars(32))</p> <p>gre</p>
Enable
<p>Enable / Disable the GRE Tunnel.</p>
<p>Values (selection)</p> <p>Disable / Enable</p>

4.0 Configuration

Multicast	
Enable / Disable Multicast support over the GRE tunnel.	Values (selection) Disable / Enable
TTL	
Set the TTL (Time-to-live) value for packets traveling through the GRE tunnel.	Values (value) 1 - 255
Key	
Enter a key is required, key must be the same for each end of the GRE tunnel.	Values (chars) (none)
ARP	
Enable / Disable ARP (Address Resolution Protocol) support over the GRE tunnel.	Values (selection) Disable / Enable

Local Setup

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

Gateway IP Address	
This is the WAN IP Address of the IPnXGii, this field should be populated with the current WAN IP address.	Values (IP Address) (varies)
Tunnel IP Address	
This is the IP Address of the local tunnel.	Values (IP Address) (varies)
Netmask	
Enter the subnet mask of the local tunnel IP address.	Values (IP Address) (varies)
Subnet IP Address	
Enter the subnet address for the local network.	Values (IP Address) (varies)

4.0 Configuration

Subnet Mask

The subnet mask for the local network/subnet.

Values (IP Address)

(varies)

Remote Setup

The remote setup tells the IPnXGii 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 IPnXGii 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

This is the IP Address of the remote network, on the remote side of the GRE Tunnel.

Values (IP Address)

(varies)

Subnet Mask

This 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

4.5.5 VPN > L2TP Users

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

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

Username

Enter a username for the user being set up.

Values (characters)

(no default)

New Password

Enter a password for the use.

Values (characters)

(no default)

Confirm New Password

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

Values (IP Address)

(no default)

4.0 Configuration

4.5.6 VPN > Certificate Management

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary	Gateway To Gateway	Client To Gateway	GRE	L2TP Users	Certificates						
Certificates											
X509 Root Certificates											
No.	Name		Config.								
Import Certificate:	<input type="button" value="Choose file"/>	No file chosen	<input type="button" value="Import"/>								
X509 Certificates											
No.	Name		Config.								
Import Certificate:	<input type="button" value="Choose file"/>	No file chosen	<input type="button" value="Import"/>								
X509 Private Keys											
No.	Name		Config.								
Import Private key:	<input type="button" value="Choose file"/>	No file chosen	<input type="button" value="Import"/>								
X509 Certificates Revocation Lists											
No.	Name		Config.								
Import Certificate:	<input type="button" value="Choose file"/>	No file chosen	<input type="button" value="Import"/>								

Image 4-5-7: VPN > Certificate Management

4.0 Configuration

4.6 MultiWAN

4.6.1 MultiWAN > Status

The IPnXGii is capable of having 2 WAN connections, one connected to the physical WAN port on the modem and the Cellular WAN connection to the wireless carrier. The MultiWAN section allows a user to define how traffic uses these WAN's.

The main purpose of the MultiWAN feature is to use one network for a primary connection, such as a local, wired ISP for broadband access, and if that connection fails or is offline, the modem can automatically switch to an alternate network connection such as the Cellular connection.

The Status menu gives an overview of both WAN connections and their configuration. WAN group 1 is the wired WAN and WAN group 2 is the Cellular connection to a wireless carrier.

The screenshot displays the MultiWAN Status page. At the top, there is a navigation menu with tabs for System, Network, Carrier, Firewall, VPN, MultiWAN (selected), Serial, USB, I/O, GPS, Applications, and Admin. Below the menu, there are sub-tabs for Status and Settings. The main content area is titled 'Multi WAN Status' and contains two sections: 'Multi WAN GROUP 1' and 'Multi WAN GROUP 2'. Each section lists configuration details for its respective WAN connection.

Multi WAN GROUP 1	
WAN Name	WAN [Primary]
IP Address	10.10.10.10
Gateway	10.10.10.10
DNS	
Status	x

Multi WAN GROUP 2	
WAN Name	Carrier
IP Address	184.151.220.2
Gateway	184.0.0.1
DNS	70.28.245.227 184.151.118.254
Status	UP

At the bottom right of the status area, there is a 'Stop Refreshing' button and the text 'Interval: 20 (in seconds)'. The footer of the page reads 'Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii'.

Image 4-6-1: MultiWAN > Status

4.0 Configuration

4.6.2 MultiWAN > Settings

The following section describes the parameters required for MultiWAN for failover purposes. The configuration for each interface is identical, so will only be described once.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
<div style="display: flex; border-bottom: 1px solid black;"> Status Settings </div> <h4 style="margin-top: 10px;">Multi WAN Configuration</h4> <p>Configuration</p> <p>Multi Wan status Enable ▼</p> <p>Primary Connection WAN ▼</p> <p>WAN Interface</p> <p>Health Monitor Interval 5 sec. ▼</p> <p>Health Monitor ICMP Host 8.8.8.8</p> <p>Health Monitor ICMP Timeout 3 sec. ▼</p> <p>Attempts Before WAN Failover 3 ▼</p> <p>Attempts Before WAN Recovery 3 ▼</p> <p>Failover Traffic Destination Carrier ▼</p> <p>Carrier Interface</p> <p>Health Monitor Interval 5 sec. ▼</p> <p>Health Monitor ICMP Host 8.8.8.8</p> <p>Health Monitor ICMP Timeout 3 sec. ▼</p> <p>Attempts Before Carrier Failover 3 ▼</p> <p>Attempts Before Carrier Recovery 3 ▼</p> <p>Failover Traffic Destination WAN ▼</p>											

Image 4-6-2: MultiWAN > Settings

Multi Wan status

Enable or disable MultiWan. To use MultiWan, the WAN (wired) must be configured as independent in the Network > WAN settings, and a DHCP or Static IP Address set.

Values (selection)

Enable / **Disable**

Primary Connection

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

Values (selection)

WAN
Carrier
Load Balancer
Fast Balancer

Health Monitor Interval

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

Values (selection)

5,10,20,30,60,120(sec.)
Disable

4.0 Configuration

Health Monitor ICMP Host

This is the IP Address or domain name of a valid reachable host that can be used to determine link health.

Values (Address)

8.8.8.8

Health Monitor ICMP Timeout

This is the amount of time the Health Monitor will wait for a response from the ICMP Host.

Values (selection)

1, 2, **3**, 4, 5, 10 (seconds)

Attempts Before WAN/Carrier Failover

This is the number of attempts the modem will attempt to reach the ICMP host before going into failover and switching WAN interfaces.

Values (selection)

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

Attempts Before WAN/Carrier Recovery

The IPnXGii will continue to monitor the failed interface, even after failover has occurred. This defines the number of successful attempts required before recovering the failed interface.

Values (selection)

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

Failover Traffic Destination

Select the interface to use once failover has occurred.

Values (selection)

Carrier or WAN

Disable

Load Balancer Compatibility

Fast Balancer Compatibility

4.0 Configuration

4.7 Serial

4.7.1 Serial > Summary

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

The screenshot shows the configuration interface for the IPn4Gii device. The top navigation bar includes tabs for System, Network, Carrier, Firewall, VPN, MultiWAN, Serial, USB, I/O, GPS, Applications, and Admin. The 'Serial' tab is selected, and the 'Summary' sub-tab is active. The main content area is titled 'Comport Status' and is divided into three sections: RS232 Port Status, Console Port Status, and RS485 Port Status.

RS232 Port Status

General Status			
Port Status	Baud Rate	Connect As	Connect Status
Enable	9600	TCP Server	Active (1)

Traffic Status			
Receive bytes	Receive packets	Transmit bytes	Transmit packets
21413	507	9469	9435

Console Port Status

Port Console is in console mode

RS485 Port Status

General Status			
Port Status	Baud Rate	Connect As	Connect Status
Enable	9600	UDP Point to Multipoint(MP)	Not Active

Traffic Status			
Receive bytes	Receive packets	Transmit bytes	Transmit packets
0	0	0	0

Stop Refreshing Interval: 20 (in seconds)

Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii

Image 4-7-1: Serial > Summary

4.0 Configuration

4.7.2 Serial > COM1/COM2/RS485

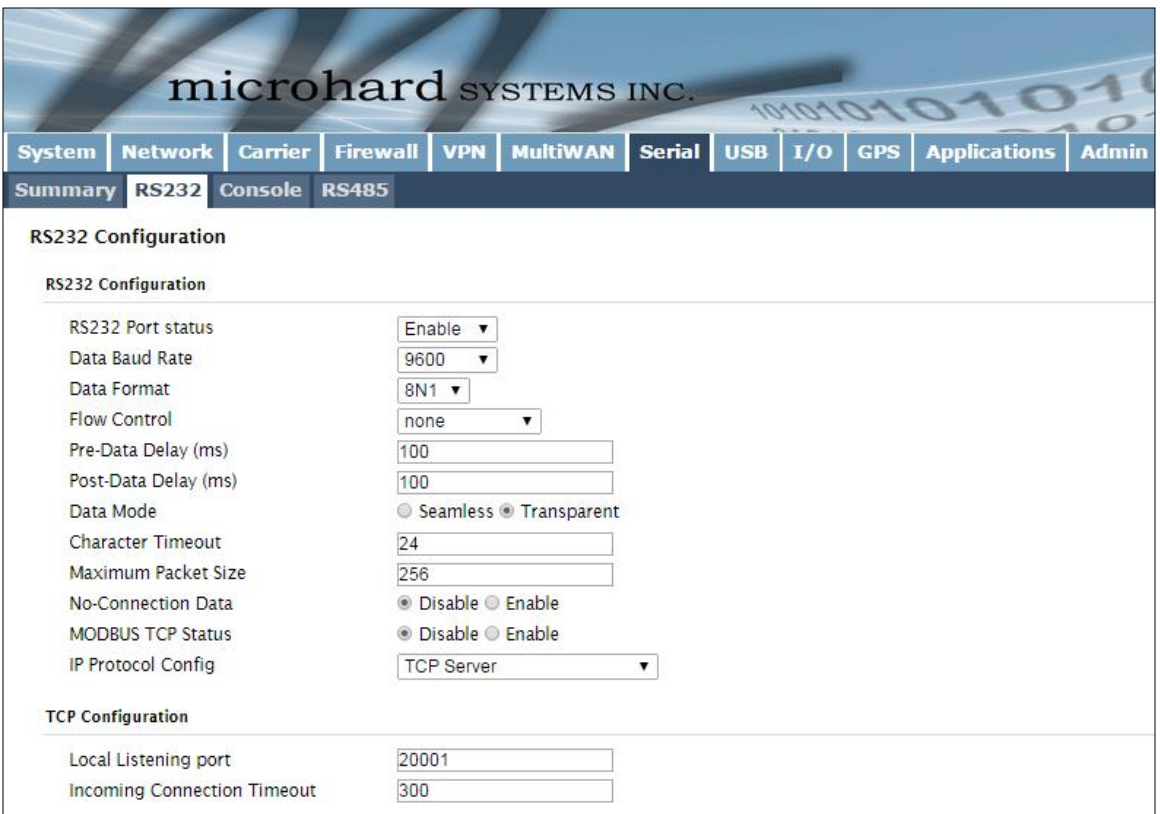
This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the IPnXGii network on another IPnXGii serial port. The fully-featured RS232 interface supports hardware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

The IPnXGii is equipped with 3 Serial Communication Ports as described below:

RS232 - The primary RS232 data port for end devices. It is located on the front panel of the IPnXGii. The COM1 RS232 port supports full handshaking.

Console - By default this port is configured as a console port and is used for diagnostics and configuration using a AT Command set. It is located on the back of the IPnXGii, and only supports asynchronous (TX/RX) communications. It can be configured as a data port, but is limited in which features are available (TCP and UDP only)

RS485 - The RS485 port is used as a data port for RS485 devices. In the IPnXGii it is a fully independent serial data port with full support.



microhard SYSTEMS INC.

System Network Carrier Firewall VPN MultiWAN Serial USB I/O GPS Applications Admin

Summary RS232 Console RS485

RS232 Configuration

RS232 Configuration

RS232 Port status

Data Baud Rate

Data Format

Flow Control

Pre-Data Delay (ms)

Post-Data Delay (ms)

Data Mode Seamless Transparent

Character Timeout

Maximum Packet Size

No-Connection Data Disable Enable

MODBUS TCP Status Disable Enable

IP Protocol Config

TCP Configuration

Local Listening port

Incoming Connection Timeout

Image 4-7-2: Comport > Settings Configuration

4.0 Configuration

Com Port Status

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

Values (selection)

Disabled / Enable

Data Baud Rate

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

Values (bps)

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



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

Data Format

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

Values (selection)

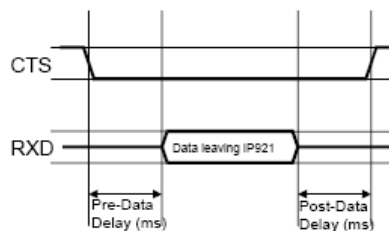
8N1	7N2
8N2	7E1
8E1	7O1
8O1	7E2
7N1	7O2



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

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 IPnXGii 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
Data Mode	
This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the IPnXGii.	Values (selection)
	Seamless / Transparent
When set to Seamless, the serial port server will add a gap between data frames to comply with the MODBUS protocol for example. See 'Character Timeout' below for related information.	
Character Timeout	
In Seamless mode (see Data Mode described on the preceding page), this setting determines when the serial server will consider the recently-received incoming data as being ready to transmit. As per the MODBUS standard, frames will be marked as 'bad' if the time gap between frames is greater than 1.5 characters, but less than the Character Timeout value.	Values (characters)
	24
The serial server also uses this parameter to determine the time gap inserted between frames. It is measured in 'characters' and related to baud rate.	
Example: If the baud rate is 9600bps, it takes approximately 1ms to move one character. With the Character Timeout set to 4, the timeout period is 4ms. When the calculated time is less than 3.5ms, the serial server will set the character timeout to a minimum value of 3.5ms.	
If the baud rate is greater than 19200bps, the minimum character timeout is internally set to 750us (microseconds).	
Maximum Packet Size	
Defines the buffer size that the serial server will use to receive data from the serial port. When the server detects that the Character Timeout criteria has been met, or the buffer is full, it packetizes the received frame and transmits it.	Values (bytes)
	1024
No-Connection Data	
When enabled the data will continue to buffer received on the serial data port when the radio loses synchronization. When disabled the IPnXGii will disregard any data received on the serial data port when radio synchronization is lost.	Values (selection)
	Disable / Enable

4.0 Configuration

MODBUS TCP Status

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

Values (selection)

Disable / Enable

MODBUS TCP Protection Key

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

Values (string)

1234

4.0 Configuration

IP Protocol Config

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

The protocol selected in the IP Protocol Config field will determine which configuration options appear in the remainder of the COM1/COM2/RS485 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

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



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

- **Remote Server Address**
IP address of a TCP server which is ready to accept serial port data through a TCP connection. For example, this server may reside on a LAN network server.
Default: **0.0.0.0**
- **Remote Server Port**
A TCP port which the remote server listens to, awaiting a session connection request from the TCP Client. Once the session is established, the serial port data is communicated from the Client to the Server.
Default: **20001**
- **Outgoing Connection Timeout**
This parameter determines when the IPnXGii 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 IPnXGii 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...)



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.

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

UDP Point-to-Point: In this configuration the IPnXGii will send serial data to a specifically-defined point, using UDP packets. This same IPnXGii 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**

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



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 be members of the specific multicast group.

- **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 IPnXGii 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 (IPnXGii 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).
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 IPnXGii 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**

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

- **PPP Mode**
Can be set for Active or Passive. If set for Active, the PPP server will initiate the PPP connection with a PPP client. The server will periodically send out link requests following PPP protocol. If set to Passive, the PPP server will not initiate the PPP connection with PPP client. The server will wait passively for the client to initiate connection.
Default: **Passive**
- **Expected String**
When a client (PC or device) initiates a PPP session with the modem, this is the handshaking string that is expected in order to allow a connection. Generally this does not need to be changed.
Default: **CLIENT**
- **Response String**
This is the handshaking string that will be sent by the modem once the expected string is received. Generally this does not need to be changed.
Default: **CLIENTSERVER**

4.0 Configuration

IP Protocol Config (Continued...)

- **PPP LCP Echo Failure Number**
 The PPP server will presume the peer to be dead if the LCP echo-requests are sent without receiving a valid LCP echo-reply. If this happens, PPP server will terminate the connection. Use of this option requires a non-zero value for the LCP Echo Interval parameter. This option can be used to enable PPP server to terminate after the physical connection has been broken (e.g., the modem has hung up).
 Default: **0**
- **PPP LCP Echo Interval**
 The PPP server will send an LCP echo-request frame to the peer every 'n' seconds. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the LCP-echo-failure option to detect that the peer is no longer connected.
 Default: **0**
- **PPP Local IP**
 Enter the local PPP IP Address, the IP Address of the IPn4G COM0 Port.
 Default: **192.168.0.1**
- **PPP Host IP**
 Enter the PPP Host IP here. This is the IP of the PC or attached device.
 Default: **192.168.0.99**
- **PPP Idle Timeout(s)**
 It is the timeout for tearing down the ppp connection when there is no data traffic within the time interval. When there is data coming, new ppp connection will be created.
 Default: **30**

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:

```

GPS - HyperTerminal
File Edit View Call Transfer Help
$GPVTG,.T,.M,.N,.K*4E
$GPGSV,1,1,00*79
$GPGGA,,,,,0,,,,,*66
$GPRMC,.V,,,,,N*53
$GPGSA,A,1,,,,,*1E
$GPVTG,.T,.M,.N,.K*4E
$GPGSV,1,1,00*79
$GPGGA,,,,,0,,,,,*66
$GPRMC,.V,,,,,N*53
$GPGSA,A,1,,,,,*1E
Connected 0:08:02 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
  
```

Image 4-7-4: RS232 > GPS Transparent Mode

4.0 Configuration

4.8 USB

4.8.1 USB > Summary

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

- OTG Mode
Displays the current mode of the USB port.
- Serial Status
Display of chosen protocol with respect to serial gateway function.
- NDIS Status
Displays the statistics of the NDIS Ethernet Interface.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Summary Serial NDIS											
USB Summary											
OTG Mode	Device										
Serial Mode	Data										
NDIS Mode	Standalone										
Serial Status											
General Status											
Port Status	Baud Rate	Connect As		Connect Status							
Enable	115200	TCP Server		Not Active							
Traffic Status											
Receive bytes	Receive packets	Transmit bytes		Transmit packets							
0	0	0		0							
NDIS Status											
General Status											
IP Address	Connection Type	Net Mask		MAC Address							
192.168.111.1	Standalone: static	255.255.255.0		00:0F:92:04:16:E1							
Traffic Status											
Receive bytes	Receive packets	Transmit bytes		Transmit packets							
0B	0	0B		0							
[Stop Refreshing] Interval: 20 (in seconds)											
Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii											

Image 4-8-1: USB > Summary

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

To use the Serial or NDIS function of the IPnXGii, you must first attain and install the USB drivers.

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

Please register and login into:

<http://www.microhardcorp.com/support>

4.0 Configuration

4.8.2 USB > Serial

Console Mode:

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

Data Mode:

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial
<div style="display: flex; border-bottom: 1px solid black;"> Summary Serial NDIS </div> <h3>Serial Configuration</h3> <p>Serial Configuration</p> <p>USB Device Serial Mode <input type="radio"/> Console <input checked="" type="radio"/> Data</p> <hr/> <p>Data Baud Rate <input type="text" value="115200"/></p> <p>Data Format <input type="text" value="8N1"/></p> <p>Data Mode <input type="radio"/> Seamless <input checked="" type="radio"/> Transparent</p> <p>Character Timeout <input type="text" value="24"/></p> <p>Maximum Packet Size <input type="text" value="256"/></p> <p>No-Connection Data <input type="radio"/> Disable <input checked="" type="radio"/> Enable</p> <p>TCP MODBUS Status <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>TCP MODBUS Protection Status <input checked="" type="radio"/> Disable <input type="radio"/> Enable</p> <p>TCP MODBUS Protection Key <input type="text" value="1234"/></p> <p>IP Protocol Config <input type="text" value="TCP Server"/></p> <hr/> <p>TCP Configuration</p> <p>Local Listening port <input type="text" value="20003"/></p> <p>Incoming Connection Timeout <input type="text" value="300"/></p>						

For more information about any of the Data Port field parameters refer to **RS232 Configuration**.

Image 4-8-2: USB Configuration Data Port

4.0 Configuration

4.8.3 USB > NDIS

NDIS Mode:

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
<div style="display: flex; justify-content: space-between;"> Summary Serial NDIS </div> <p>NDIS Configuration</p> <p>NDIS Configuration</p> <p>NDIS Mode <input type="radio"/> Bridge to LAN <input checked="" type="radio"/> Standalone</p> <hr/> <p>Local IP Address <input type="text" value="192.168.111.1"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Host IP Address <input type="text" value="192.168.111.2"/></p>											

Image 4-8-3: USB Configuration: NDIS

NDIS Mode

In standalone Mode the USB port will act as a separate NIC for the IPnXGii. In Bridge Mode the USB port will use the same settings as the rear Ethernet port.

Values (selection)

Bridge / **Standalone**

Local IP Address

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

Values

192.168.111.1

Subnet Mask

This will be the Subnet Mask automatically assigned to the device (PC) connected to the USB port of the IPnXGii

Values

255.255.255.0

Host IP

This will be the IP Address automatically assigned to the device (PC) connected to the USB port of the IPnXGii

Values

192.168.111.2

4.0 Configuration

4.9 I/O

4.9.1 I/O > Settings

The IPnXGii has 8 programmable I/O's, which can be used with various alarms and sensors for monitoring, telling the modem when certain events have occurred, such as an intrusion alarm on a door, etc. Any of the I/O's can also be programmed to operate as a output, that can be used to drive external relays to remotely control equipment and devices. The I/O pins are available on the back connector shared with the input power (1&2), as well as the 10 pin connector (I/O 3 - 8).

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

Name	Mode	Output Control
I/O1	<input checked="" type="radio"/> Input <input type="radio"/> Output	
I/O2	<input checked="" type="radio"/> Input <input type="radio"/> Output	
I/O3	<input checked="" type="radio"/> Input <input type="radio"/> Output	
I/O4	<input checked="" type="radio"/> Input <input type="radio"/> Output	
I/O5	<input type="radio"/> Input <input checked="" type="radio"/> Output	<input checked="" type="radio"/> Open <input type="radio"/> Close
I/O6	<input type="radio"/> Input <input checked="" type="radio"/> Output	<input checked="" type="radio"/> Open <input type="radio"/> Close
I/O7	<input type="radio"/> Input <input checked="" type="radio"/> Output	<input checked="" type="radio"/> Open <input type="radio"/> Close
I/O8	<input type="radio"/> Input <input checked="" type="radio"/> Output	<input checked="" type="radio"/> Open <input type="radio"/> Close

status	Name	Mode	Status	Meter(V)
	I/O1	Input	High	12.19
	I/O2	Input	High	2.83
	I/O3	Input	High	2.81
	I/O4	Input	High	2.81
	I/O5	Output	Open High	2.83
	I/O6	Output	Open High	2.81
	I/O7	Output	Open High	2.81
	I/O8	Output	Open High	2.80

Image 4-9-1: I/O Settings

Settings

The Settings menu is used to configure a I/O as either a Input or an Output. If configured as an output, the user can also set the output as open or closed. The output pin on the IPnXGii can be used to provide output signals, which can be used to drive an external relay to control an external device. See **Table 4-8-1** for I/O specifications.

Status

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

4.0 Configuration

Name	Description	Parameter	Min.	Typ.	Max	Units
I/O 1 - 8 (Input)	Input low state voltage range	VIL	-0.5	0	1.2	V
	Input high state voltage range	VIH	1.5	3.3	30	V
	Input leakage current (3.3 VDC IN)	IIN	—	58	—	μA
	Typical application input source is a dry switch contact to ground. Pin includes an internal 56KΩ resistor pull up to 3.3 VDC.					
I/O 1 - 8 (Output)	Open drain drive to ground	I _{dc}	—	100	110	mA
	Maximum open circuit voltage applied	V _{oc}	—	3.3	30	V
	Typical application is to drive a relay coil to ground.					

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

4.0 Configuration

4.10 GPS

4.10.1 GPS > Location

Location Map

The location map shows the location on the IPnXGii. 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.

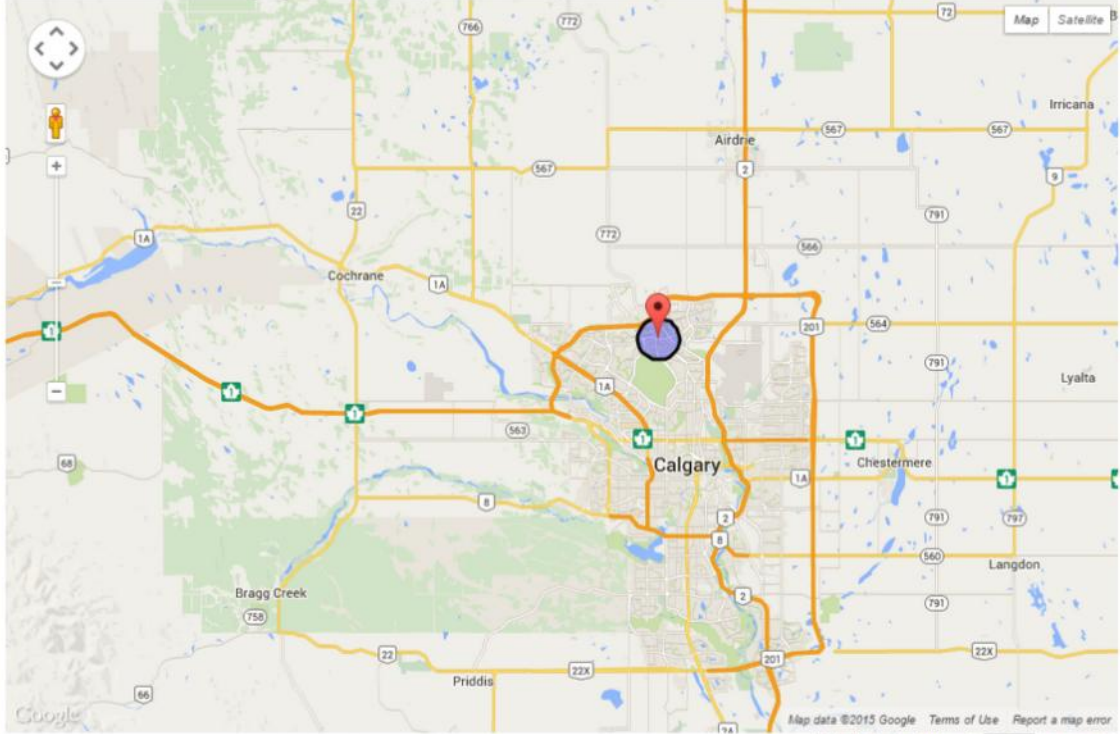
System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
<div style="border: 1px solid black; padding: 5px;"> <div style="background-color: #2e5496; color: white; padding: 2px;"> Location Settings Report GpsGate Recorder Load Record TAIP </div> <div style="padding: 5px;"> <p>Location Map</p> <p>Waiting for valid GPS data... Getting for carrier's recent/online location: Last Carrier's Latitude:51.142868, Longitude:-114.104850, Radius:1743m <i>Update:Wed Apr 15 14:01:53 2015</i></p>  <p style="font-size: small; text-align: right;">Map data ©2015 Google Terms of Use Report a map error Auto Refresh Interval: 20 in seconds View With Bing Map</p> <p style="font-size: x-small; text-align: right;">Copyright © 2013-2014 Microhard Systems Inc. IPn4Gii</p> </div> </div>											

Image 4-10-1: GPS > Location Map

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

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

4.0 Configuration

4.10.2 GPS > Settings

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

Image 4-10-2: GPS > Settings

GPS Status

Enable or disable the GPS polling function of the IPnXGii.

Values

Disable / Enable

GPS Source

The IPnXGii contains an standalone GPS module built into the unit. To use the GPS features of the IPnXGii a cellular antenna must be connected to the GPS Antenna Port.

Values

Standalone GPS

TCP Port

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

Values

2947

4.0 Configuration

4.10.3 GPS > Report

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Location		Settings	Report	GpsGate	Recorder	Load Record	TAIP				
GPS Report Configuration											
GPS Report No.1											
Report Define		UDP Report ▾									
Time Interval	600 (s)										
Message 1	ALL NMEA ▾										
Message 2	None ▾										
Message 3	None ▾										
Message 4	None ▾										
Trigger Set	Only Timer ▾										
Local Streaming	Disable ▾										
UDP Remote IP	0.0.0.0										
UDP Remote PORT	20175 [0~65535]										
GPS Report No.2											
Report Define		Email Report ▾									
Time Interval	600 (s)										
Message 1	ALL NMEA ▾										
Message 2	None ▾										
Message 3	None ▾										
Message 4	None ▾										
Trigger Set	Only Timer ▾										
Mail Subject	GPSReportMessage2										
Mail Server(IP/Name)	smtp.gmail.com:465 (xxx:port)										
User Name	@gmail.com										
Password	***										
Authentication	None ▾										
Mail Recipient	host@ (xx@xx.xx)										
GPS Report No.3											
Report Define		Disable ▾									
GPS Report No.4											

Image 4-10-3: GPS > GPS Report

Report Define

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

Values (selection)

- Disable
- UDP Report
- Email Report

Time Interval

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

Values (seconds)

600

4.0 Configuration

Message 1-4

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

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

Values (selection)

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

Trigger Set

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

Values (selection)

Only Timer
 Timer AND Distance
 Timer OR Distance

Distance Set

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

Values (meters)

1000

UDP Remote IP / Port

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

Values (Address/Port)

0.0.0.0 / 20175

Mail Subject

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

Values (characters)

1000

Mail Server

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

Values (Address:port)

smtp.gmail.com:465

Username / Password

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

Values (characters)

Username / password

Mail Recipient

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

Values (characters)

host@email.com

4.0 Configuration

4.10.4 GPS > GpsGate

The IPnXGii 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 IPnXGii can communicate with GpsGate via Tracker Mode and TCP/IP. (UDP reporting can also send information to GpsGate, see the GPS > Report - UDP Reports)

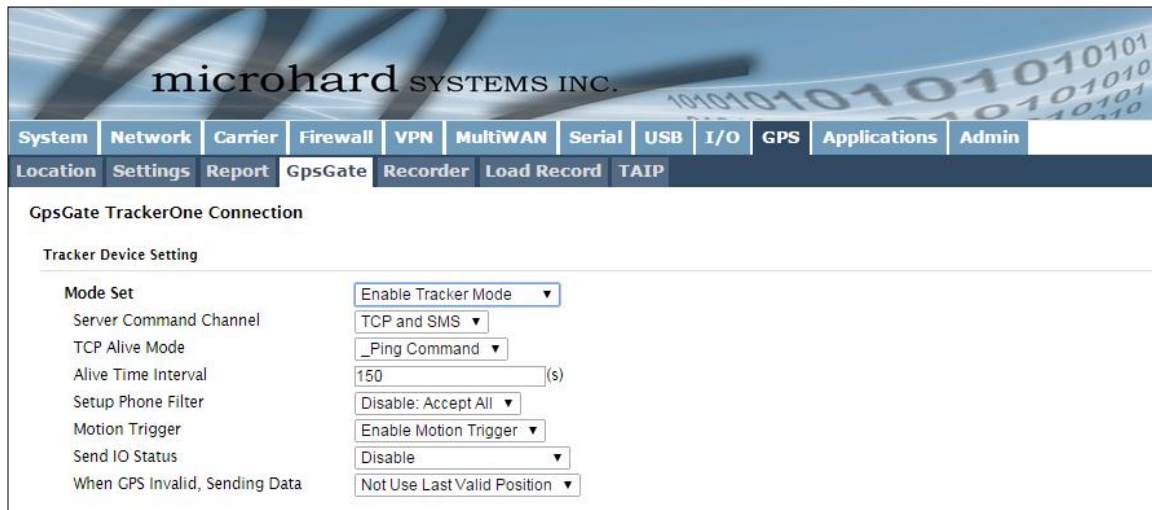


Image 4-10-4: GPS > GpsGate Tracker Mode

GpsGate - Tracker Mode

Mode Set

Enable GpsGate Tracker Mode or TCP modes. In tracker mode The IPnXGii and GpsGate software will communicate via TCP/IP, however if a connection is not available it will attempt to use SMS messaging.

Values (selection)

Disable
 Enable Tracker Mode
 Enable TCP Send Mode

Server Command Channel

By default IPnXGii and GpsGate will use TCP and SMS to ensure communication between each other. It is also possible to specify TCP or SMS communication only. Initial setup in Tracker mode must be via SMS.

Values (seconds)

TCP and SMS
 TCP Only
 SMS Only

TCP Alive Mode / Alive Time Interval

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

Values (seconds)

150

4.0 Configuration

Setup Phone Filter

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

Values (selection)

Disable: Accept All
Enable Filter

Motion Trigger

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

Values (selection)

Disable
Enable Motion Trigger

Send IO Status

When enabled, the IPnXGii 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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications
Location	Settings	Report	GpsGate	Recorder	Load Record	TAIP				
GpsGate TrackerOne Connection										
Tracker Device Setting										
Mode Set	Enable TCP Send Mode ▼									
Server Address/IP	0.0.0.0									
Server Port	30175									
Server Interval	60 (s)									
Motion Distance	100 (m)									
Send IO Status	Disable ▼									
When GPS Invalid, Sending Data	Not Use Last Valid Position ▼									

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

4.0 Configuration

<p>Enable GpsGate Tracker Mode or TCP modes. In TCP Mode the IPnXGii will establish a connection with the GpsGate Server directly without the SMS setup process. If the TCP connection is not available, the IPnXGii will continue to try to connect every few seconds.</p>	<p style="text-align: right;">Mode Set</p> <p>Values (selection)</p> <p>Disable Enable Tracker Mode Enable TCP Send Mode</p>
<p>Enter the IP Address of the server running the GpsGate application.</p>	<p style="text-align: right;">Server Address / IP</p> <p>Values (IP Address)</p> <p>0.0.0.0</p>
<p>Enter the TCP Port of the server running the GpsGate application.</p>	<p style="text-align: right;">Server Port</p> <p>Values (Port)</p> <p>30175</p>
<p>Define the interval at which the IPnXGii will send data to the GpsGate Server.</p>	<p style="text-align: right;">Server Interval</p> <p>Values (seconds)</p> <p>60</p>
<p>Set the motion threshold in which the IPnXGii will be triggered to send location data.</p>	<p style="text-align: right;">Motion Distance</p> <p>Values (meters)</p> <p>100</p>
<p>When enabled, the IPnXGii will send the current status of the Digital I/O inputs and/or outputs to the GpsGate Server.</p>	<p style="text-align: right;">Send IO Status</p> <p>Values (selection)</p> <p>Disable Send Input Status Send Output Status Send Input&Output Status</p>
<p>Specify what happens when the GPS data is invalid, either use the last valid position or do not use the last valid position.</p>	<p style="text-align: right;">When GPS Invalid, Sending Data</p> <p>Values (selection)</p> <p>Not Use Last Valid Position Use Last Valid Position</p>

4.0 Configuration

4.10.5 GPS > Recorder

The IPnXGii can be configured to record events based on time intervals, and/or an event trigger and store them in non-volatile memory. These events can then be viewed within the WebUI, on a map, or sent to a remote server in a number of different formats.

GPS Recorder Service

Current GPS Information

Local Time:	Wed Mar 26 15:26:59 MDT 2014
Satellites In View:	15
Satellites tracked:	10
Latitude:	51.142662,N
Longitude:	-114.075531,W
Altitude:	1130.2
Speed:	0(Km/h)
Orientation:	0(Degree to North)
NMEA UTC Time:	26/03/2014 21:26:59

GPS Recorder Setting

Status	<input type="text" value="Enable GPS Recorder"/>
Record Feature Selections:	(Record Items among 16,000~36,000.)
Time Interval	<input type="text" value="30"/> [30~65535](s)
DI/DO Changed	<input type="text" value="Record"/>
Speed	<input type="text" value="Record"/>
Over Speed	<input type="text" value="120"/> [Min 30](Km/h)
Orientation	<input type="text" value="Record"/>
Orientation Changed	<input type="text" value="60"/> [5~180](180:Disable)
Carrier RSSI Level	<input type="text" value="Record"/>
Altitude	<input type="text" value="Record"/>

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

Status

Use the Status parameter to enable the GPS recording functionality of the IPnXGii. The total number of records that can be recorded varies between 16,000 and 36,000, depending on the number of GPS parameters that are recorded.

Values (selection)

Disable
Enable GPS Recorder

Time Interval

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

Values (seconds)

300

DI/DO Changed

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

Values (selection)

Record / **Don't Record**

4.0 Configuration

	Speed
Select Record to include the current speed in the reported data.	Values (selection) Record / Don't Record
	Over Speed
Trigger a GPS record entry when the speed has exceeded the configured threshold. A minimum of 30 Km/hr is required.	Values (Km/hr) 120
	Orientation
Select Record to record the current orientation when a GPS entry is recorded. (Degree to North).	Values (selection) Record / Don't Record
	Orientation Changed
Record a GPS, regardless of the time interval, if the orientation of the unit changes. (5 ~ 180: 180 = Disable)	Values (5 ~ 180) 60
	Carrier RSSI Level
Select Record to record the current 3G/Cellular RSSI level when a GPS entry is recorded. (-dB).	Values (selection) Record / Don't Record
	Altitude
Select Record to record the current Altitude when a GPS entry is recorded (meters).	Values (selection) Record / Don't Record

4.0 Configuration

4.10.6 GPS > Load Record

Data that has been recorded and saved by the IP3Gii can then be viewed or sent to a remote server in various formats. The data recorded can also be viewed directly by selecting "View Data" and the data can be traced on a map (internet access required), by selecting "Trace Map", or "Quick Trace". The screenshots below show the raw data that can be viewed and the Trace Map/Quick Trace output.

GPS Record Review and Load Service

Current Position Record

Start Time(UTC)	End Time(UTC)	Select	Review/Operation
2014-03-26 15:19:14	2014-03-27 16:30:14	<input type="checkbox"/>	View Data Trace Map
2014-03-27 16:30:14 ...		<input type="checkbox"/>	View Data Trace Map
		<input type="checkbox"/>	Select All Quick Trace

Send Record To Server

Record Time Range: Please Select Above Items

Send Mode/Protocol:

Server Address/IP:

Server Port:

GPS Record Review

Record Time(UTC)	Latitude	Longitude	Input	Output	Speed	Angle	RSSI	Altitude
2014-03-26 15:19:14	51.142761	-114.075417	0000	0000	0		-59	1108
Local Record			0000	0000			54	

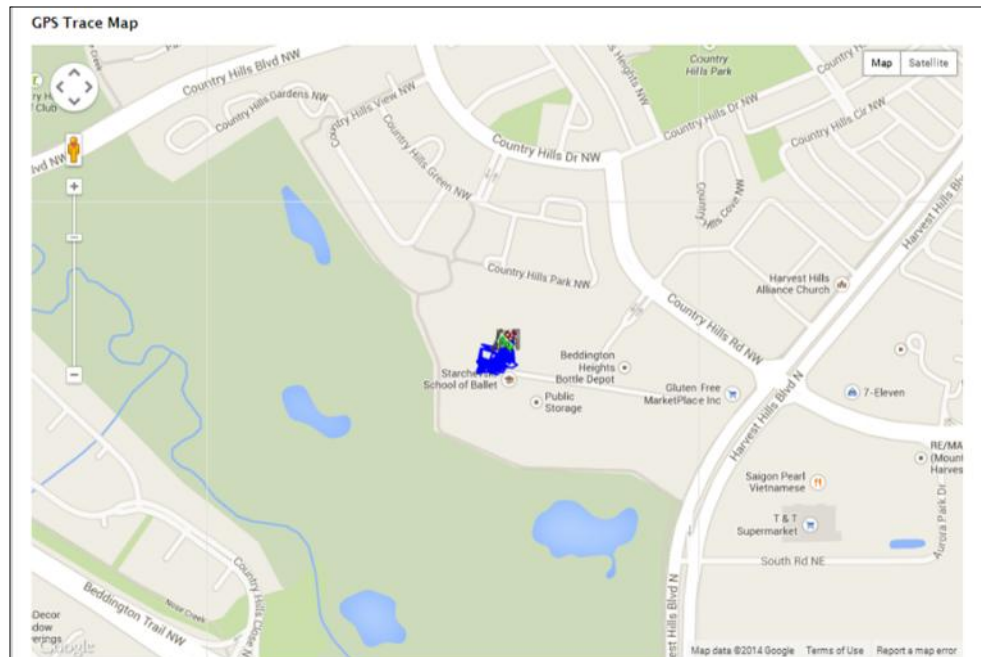


Image 4-10-7: GPS > GPS Load Record

4.0 Configuration

Record Time Range

Check the boxes next to the records listed above that are to be sent to the server.

Values (selection)

(no default)

Send Mode / Protocol

Specify the data format / protocol type for the data to be sent.

Values (selection)

NMEA via UDP
NMEA via TCP
GpsGate via UDP
GpsGate via TCP
Plain Text via UDP
Plain Text via TCP

Server Address/IP

Enter the address or IP address of the remote server to which the data is to be sent.

Values (IP)

nms.microhardcorp.com

Server Port

Enter the UDP/TCP port number of the remote server to which the data is to be sent.

Values (Port)

30175

4.0 Configuration

4.10.7 GPS > TAIP

The IPnXGii has the ability to send GPS data in TAIP (Trimble ASCII Interface Protocol) format to up to 4 different TAIP servers. The following section describes the configuration parameters required to initialize TAIP reporting.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Location	Settings	Report	GpsGate	Recorder	Load Record	TAIP					
TAIP Configuration											
Settings No.1											
TAIP service status	Enabled ▾										
Remote TAIP Server	0.0.0.0										
Socket Type	UDP ▾										
Remote TAIP Port	21000										
Message Type	RPV ▾										
Interval	5 (s)										
Vehicle ID	0000 4 Alphanumeric characters										
Settings No.2											
TAIP service status	Disabled ▾										
Settings No.3											
TAIP service status	Disabled ▾										
Settings No.4											
TAIP service status	Disabled ▾										

Image 4-10-8: GPS > TAIP

TAIP service status

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

Values (selection)

Enable / **Disable**

Remote TAIP Server

Enter the IP Address of the Remote TAIP Server.

Values (IP Address)

0.0.0.0

Socket Type

Select the socket type that is used by the Remote TAIP server. Select TCP or UDP, this will define how the connection (TCP) or data is sent (UDP) to the server.

Values (selection)

UDP / TCP

Remote TAIP Port

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

Values (TCP/UDP)

UDP / TCP

4.0 Configuration

	Message Type
Select between RPV and RLN message types.	Values (selection)
RPV - Position/Velocity RLN - Long Navigation Message	RPV / RLN
	Interval
Set the frequency at which TAIP messages are reported to the remote server. The unit used is seconds, and the default value is 60 seconds.	Values (seconds)
	60
	Vehicle ID
Set the Vehicle ID using 4 alpha-numeric characters.	Values (chars)
	0000

4.0 Configuration

4.11 Applications

4.11.1 Applications > Modbus

4.11.1.1 Modbus > TCP Modbus

The IPnXGii 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.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin																																				
<table border="1"> <thead> <tr> <th>Modbus</th> <th>Netflow Report</th> <th>LocalMonitor</th> <th>Event Report</th> <th>Websocket</th> <th>Diagnostics</th> </tr> </thead> </table>												Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics																														
Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics																																										
<p>Modbus</p> <p>Modbus Slave Device Config:</p> <table> <tr> <td>Status</td> <td>Enable Service ▾</td> </tr> <tr> <td>TCP Mode Status</td> <td>Enable TCP Connection Service ▾</td> </tr> <tr> <td>Port</td> <td>502 [1 ~ 65535]</td> </tr> <tr> <td>Active Timeout(s)</td> <td>30 [0 ~ 65535]</td> </tr> <tr> <td>Slave ID</td> <td>1 [1 ~ 255]</td> </tr> <tr> <td>Coils Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> <tr> <td>Input Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> <tr> <td>Register Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> <tr> <td>Master IP Filter Set</td> <td>Disable IP Filter ▾</td> </tr> <tr> <td>COM Mode Status</td> <td>Enable COM1 ASCII Mode ▾</td> </tr> <tr> <td>Baud Rate</td> <td>19200 ▾</td> </tr> <tr> <td>Data Format</td> <td>8N1 ▾</td> </tr> <tr> <td>Flow Control</td> <td>none ▾</td> </tr> <tr> <td>Character Timeout(s)</td> <td>5 [0 ~ 65535]</td> </tr> <tr> <td>Slave ID</td> <td>1 [1 ~ 255]</td> </tr> <tr> <td>Coils Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> <tr> <td>Input Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> <tr> <td>Register Address Offset</td> <td>0 [0 ~ 65535]</td> </tr> </table> <p>View Data Map</p>												Status	Enable Service ▾	TCP Mode Status	Enable TCP Connection Service ▾	Port	502 [1 ~ 65535]	Active Timeout(s)	30 [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]	Master IP Filter Set	Disable IP Filter ▾	COM Mode Status	Enable COM1 ASCII Mode ▾	Baud Rate	19200 ▾	Data Format	8N1 ▾	Flow Control	none ▾	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]
Status	Enable Service ▾																																														
TCP Mode Status	Enable TCP Connection Service ▾																																														
Port	502 [1 ~ 65535]																																														
Active Timeout(s)	30 [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]																																														
Master IP Filter Set	Disable IP Filter ▾																																														
COM Mode Status	Enable COM1 ASCII Mode ▾																																														
Baud Rate	19200 ▾																																														
Data Format	8N1 ▾																																														
Flow Control	none ▾																																														
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 4-11-1: Applications > Modbus

Status

Disable or enable the Modbus service on the IPnXGii.

Values (selection)

Disable Service
Enable Service

TCP Mode Status

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

Values (selection)

Disable
Enable

4.0 Configuration

	Port
Specify the Port in which the Modbus TCP service is to listen and respond to polls.	Values (Port #) 502
	Active Timeout(s)
Define the active timeout in seconds.	Values (seconds) 30
	Slave ID
Each Modbus slave device must have a unique address, or Slave ID. Enter this value here as required by the Modbus Host System.	Values (value) 1
	Coils Address Offset
Enter the Coils Address offset as required by the Master.	Values (value) 0
	Input Address Offset
Enter the Input Address offset as required by the Master.	Values (value) 0
	Register Address Offset
Enter the Register Address offset as required by the Master.	Values (value) 0
	Master IP Filter Set
It is possible to only accept connections from specific Modbus Master IP's, to use this feature enable the Master IP Filter and specify the IP Addresses in the fields provided.	Values (selection) Disable / Enable

4.0 Configuration

4.11.1.2 Modbus > COM (Serial) Modbus

The IPnXGii 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 4-11-2: Applications > 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

4.10.1.3 Modbus > Modbus Data Map

Modbus Data Map			Registers:		
Supported Function Codes: 1---Read Coils 2---Read Inputs 3---Read Registers 5---Write Single Coil 6---Write Single Register Data Address = Offset + Basic Address			16 Bits Address Hex Format Definition		
Coil Bits (Output(if config) and Internal Status):					
Bit Address	Hex Format	Definition	0	0x0000	Modem Model Type...
1	0x0001	OUTPUT 1	1	0x0001	Build Version
2	0x0002	OUTPUT 2	2	0x0002	Modem ID Highest 2 Bytes
3	0x0003	OUTPUT 3	3	0x0003	Modem ID Higher 2 Bytes
4	0x0004	OUTPUT 4	4	0x0004	Modem ID Lower 2 Bytes
5	0x0005	OUTPUT 5	5	0x0005	Modem ID Lowest 2 Bytes
6	0x0006	OUTPUT 6	6	0x0006	RSSI(mdb)
7	0x0007	OUTPUT 7	7	0x0007	VDC(x100)(V)
8	0x0008	OUTPUT 8	8	0x0008	Core Temperature(C)
9	0x0009	COM1 Status	9	0x0009	Carrier Received Bytes(MB)
12	0x000c	COM2 Status	10	0x000a	Carrier Transmitted Bytes(MB)
13	0x000d	LAN/eth0 Status(Read)	11	0x000b	GPS Altitude(m)
16	0x0010	WAN/eth1 Status(Read)	12	0x000c	GPS Latitude High 2 Bytes
22	0x0016	Carrier Status	13	0x000d	Latitude Low 2 Bytes(x1000000)
23	0x0017	GPS Status	14	0x000e	GPS Longitude High 2 Bytes
24	0x0018	Location Over Network	15	0x000f	Longitude Low 2 Bytes(x1000000)
25	0x0019	Event UDP Report 1	16	0x0010	COM1 Baud Rate(/100)(bps)
26	0x001a	Event UDP Report 2	17	0x0011	COM1 Data Format...
27	0x001b	Event UDP Report 3	18	0x0012	COM2 Baud Rate(/100)(bps)
28	0x001c	NMS Report	19	0x0013	COM2 Data Format...
29	0x001d	Web Client Service	Modem Model Types:		
32	0x0020	Firewall Status	Type ID	Definition	
40	0x0028	Carrier Connection(Read)	0	Unknow	
		SYSTEM Reboot	6	IPn3G	
			7	VIP4G	
			8	IPn4G	
			9	IPn3Gii	
			10	IPn4Gii	
Input Bits:(if config)					
Bit Address	Hex Format	Definition			
0	0x0000	INPUT 1			
1	0x0001	INPUT 2			
2	0x0002	INPUT 3			
3	0x0003	INPUT 4			
4	0x0004	INPUT 5			
5	0x0005	INPUT 6			
6	0x0006	INPUT 7			
7	0x0007	INPUT 8			
Com Data Format Definition:					
Type ID	Definition				
0	Unknow				
1	8N1				
2	8N2				
3	8E1				
4	8O1				
5	7N1				
6	7N2				
7	7E1				
8	7O1				
9	7E2				
10	7O2				

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

4.0 Configuration

4.11.2 Applications > Netflow Report

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications
Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics					
Netflow Report										
Report Configuration No.1										
Status	Enable ▾									
Source Address	0.0.0.0									Default 0.0.0.0
Interface	ALL ▾									
Remote IP	0.0.0.0									
Remote Port	2055									[0 ~ 65535]
Filter expression										
Version	V5 ▾									
Report Configuration No.2										
Status	Disable ▾									
Report Configuration No.3										
Status	Disable ▾									

Image 4-11-4: Applications > Netflow Report

Status

Enable / Disable Netflow Reporting.

Values (selection)

Disable / Enable

Source Address

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

Values (IP Address)

0.0.0.0

Interface

Select between LAN, WAN and Carrier interfaces, or capture data from all interfaces.

Values (selection)

LAN / WAN / Carrier / ALL

4.0 Configuration

Remote IP

The Remote IP is the IP Address of the NetFlow collector where the flow reports are be sent.

Values (IP Address)

0.0.0.0

Remote Port

Enter the Remote Port number.

Values (IP Address)

0

Filter expression

Filter expression selects which packets will be captured. If no expression is given, all packets will be captured. Otherwise, only packets for which expression is `true` will be captured. Example: `tcp&&port 80`

Values (chars)

(no default)

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

4.0 Configuration

4.11.3 Applications > Local Monitor

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics						
Local Device Monitor											
Monitor Settings											
Status	Enable Local Device Monitor ▼										
IP Mode	Fixed Local IP ▼										
Local IP Setting	0.0.0.0 [0.0.0.0]										
Status Timeout	10 [5~65535](s)										
Waiting DHCP Timeout	60 [30~65535](s)										

Image 4-11-5: Applications > 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 IPnXGii 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 IPnXGii will wait to detect the monitored device. At this time the IPnXGii will restart the DHCP service. (5-65535 seconds)

Values (seconds)

10

Waiting DHCP Timeout

This field defines the amount of time the IPnXGii will wait to detect the monitored device before it will reboot the modem. (30-65535 seconds)

Values (seconds)

60

4.0 Configuration

4.11.4 Applications > Event Report

4.11.4.1 Event Report > Configuration

Event Reporting allows the IPnXGii 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.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics						
Event Report											
Report Configuration No.1											
Event Type	Modem_Event ▾										
Remote IP	0.0.0.0		0.0.0.0								
Remote PORT	20200		[0 ~ 65535]								
Interval Time(s)	600		[0 ~ 65535]								
Interface Selection											
Modem:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable										
Carrier:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable										
WAN:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable										
Report Configuration No.2											
Event Type	SDP_Event ▾										
Remote IP	0.0.0.0		0.0.0.0								
Remote PORT	20200		[0 ~ 65535]								
Interval Time(s)	600		[0 ~ 65535]								
Report Configuration No.3											
Event Type	Management ▾										
Remote IP	0.0.0.0		0.0.0.0								
Remote PORT	20200		[0 ~ 65535]								
Interval Time(s)	600		[0 ~ 65535]								
Interface Selection											
Ethernet:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										
Carrier:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable										
Com:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										
IO:	<input type="radio"/> Disable <input checked="" type="radio"/> Enable										
USB:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										

Image 4-11-6: Applications > Event Report

Event Type

This box allows the selection of the type of event to be reported. The default is disabled. If Modem_event is selected, additional options appear to the right and allow for customization of the event reported via Messages. If Management is selected, additional check boxes appear below to select the interfaces to report to the Microhard NMS system.

Values (selection)

Modem_Event
SDP_Event
Management

Remote IP

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

Values (IP Address)

0.0.0.0

4.0 Configuration

	Remote Port
Specify the UDP port number of the Remote IP Address.	Values (Port #)
*Default Port Numbers for Microhard NMS (20100 for modem events, 20200 for Management)	20200
	Interval Time(s)
This is the interval time in seconds, that the IPnXGii will send the configured UDP message to the Remote IP and Port specified.	Values (seconds)
	600
	Message Info Type
When Modem_Event is selected, up to three different payloads can be selected.	Values (seconds)
	Modem Carrier WAN

4.11.4.2 Event Report > Message Structure

Modem_event message structure

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

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

Message type mask

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

sdp_event message structure

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

4.0 Configuration

4.11.4.3 Event Report > Message Payload

Modem info:

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

Carrier info:

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

WAN Info:

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

Message Order:

Messages will be ordered by message type number.

For example,

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

If message type mask = 0x4, the eurd package will be equipped by header+carrier information.

If message type mask = 0x11, the eurd package will be equipped by header+modem information+wanip information.

a fixed message tail

content length --- 2 BYTES(UINT16_T)	
product name --- STRING(1—64 bytes)	
image name --- STRING(1—64 bytes)	
domain name --- STRING(1—64 bytes)	
domain password --- STRING(32 bytes)	// MD5 encryption
module list --- 5 BYTES	// radio, ethernet, carrier, usb, com

4.0 Configuration

4.11.5 Applications > Websocket

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

It is mainly used for two purposes:

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

Currently we provide four types of information as configured:

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Modbus	Netflow Report	LocalMonitor	Event Report	Websocket	Diagnostics						
Web Socket Service											
Online Connected Data											
Browser Type: Chrome 41 Windows											
Setting											
Status	Enable Web Socket Service ▾										
Web Socket Port(default:7681)	7681	[100-65535]									
Data Fresh Interval(seconds)	10	[2-65535]									
Connect Password		(Blank for Disable)									
Max Keep Time(minutes)	60	(0:keep alive)									
GPS Coordinate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										
GPS NMEA Data	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										
Carrier Information	<input checked="" type="radio"/> Disable <input type="radio"/> Enable										
Comport Data	<input checked="" type="radio"/> Disabled (Please enable comport tcp server.)										

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

Status

Enable or disable the web socket service in the modem.

Values (selection)

Enable / Disable

Web Socket Port

Enter the desired web socket TCP port number. The default is 7681, and the valid range is 100 to 65535.

Values (TCP port)

7681

4.0 Configuration

	Data Fresh Intervals
Enter in the time at which data is to be refreshed. The default is 10 seconds, the valid range is 2 to 65535 seconds.	Values (seconds)
	10
	Connect Password
For added security a password can be required to connect to the web socket service. To disable, leave this field blank. The default is disabled.	Values
	<i>(blank)</i>
	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 will continue to run indefinitely.	Values (minutes)
	60
	GPS Coordinate
If enabled the modem will report GPS coordinate data to the websocket.	Values (selection)
	Disable / Enable
	GPS NMEA Data
If enabled the modem will report GPS NMEA data to the websocket.	Values (selection)
	Disable / Enable
	Carrier Information
If enabled the modem will report carrier information to the websocket.	Values (selection)
	Disable / Enable
	Comport Data
If enabled, and the RS232 port is configured for TCP Server, the comport data will be reported to the web socket.	Values (selection)
	Disable / Enable

4.0 Configuration

4.11.6 Applications > Diagnostics

Network Tools Ping

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

The screenshot shows the 'Diagnostics' tab selected in the top navigation bar. Under 'Network Tools', the 'Ping' option is selected. The configuration fields are: Ping Host Name: google.com, Ping Count: 4, and Ping Size: 56. There are 'Start', 'Stop', and 'Clear' buttons. Below the form, the output of the ping test is displayed:

```
PING google.com (184.150.182.158): 56 data bytes
64 bytes from 184.150.182.158: seq=0 ttl=51 time=86.827 ms
64 bytes from 184.150.182.158: seq=1 ttl=51 time=88.253 ms
64 bytes from 184.150.182.158: seq=2 ttl=51 time=77.175 ms
64 bytes from 184.150.182.158: seq=3 ttl=51 time=75.149 ms

--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 75.149/81.851/88.253 ms
```

Image 4-11-8: Diagnostics > Ping

Network Tools Trace Route

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.

The screenshot shows the 'Diagnostics' tab selected in the top navigation bar. Under 'Network Tools', the 'Trace Router' option is selected. The configuration field is: Tracerout Host Name: google.com. There are 'Start', 'Stop', and 'Clear' buttons. Below the form, the output of the trace route test is displayed:

```
Begin Ping test ...
Begin tracerout test ...
traceroute to google.com (184.150.182.187), 30 hops max, 38 byte packets
 1 172.25.7.185 (172.25.7.185) 75.174 ms 56.706 ms 58.456 ms
 2 172.25.7.201 (172.25.7.201) 61.687 ms 77.621 ms 79.350 ms
 3 172.25.16.181 (172.25.16.181) 79.948 ms 77.763 ms 80.158 ms
 4 172.25.21.10 (172.25.21.10) 79.071 ms 69.612 ms 79.451 ms
 5 172.25.20.14 (172.25.20.14) 79.776 ms 69.057 ms 79.532 ms
 6 172.25.16.2 (172.25.16.2) 79.717 ms 78.842 ms 78.260 ms
 7 204.101.4.225 (204.101.4.225) 103.854 ms 85.758 ms 71.363 ms
 8 core2-calgaryqa_4-0-0.net.bell.ca (64.230.118.246) 91.887 ms 89.437 ms core1-calgaryqa_4-0-0.net.bell.ca (64.230.118.244) 7
 9 core4-calgaryqa_ge10-0-0.net.bell.ca (64.230.118.220) 89.873 ms core3-calgaryqa_ge9-0-0.net.bell.ca (64.230.118.216) 91.858
10 core4-calgary68_ge5-1-0.net.bell.ca (64.230.77.222) 79.220 ms 89.366 ms 79.771 ms
11 tcore3-vancouver_tengige0-15-0-5.net.bell.ca (64.230.77.137) 101.420 ms 91.374 ms core4-vancouver_pos11-1-0.net.bell.ca (64.
12 agg1-vancouver_te7-0-0.net.bell.ca (64.230.123.229) 89.712 ms agg2-vancouver_te5-0-0.net.bell.ca (64.230.123.233) 89.684 ms
```

Image 4-11-9: Diagnostics > Trace Route

4.0 Configuration

4.12 Admin

4.12.1 Admin > Users

Password Change

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Users	Authentication	NMS	SNMP	Discovery	PowerSaving	Logout					

Access Control

Password Change

User Name : admin

New Password : (min 5 characters)

Confirm Password: [Change Passwd](#)

Add User: (Note: Changes will not take effect until the system is rebooted)

Username : (5-32 characters)

Password (5-32 characters)

Confirm Password

System [Hide Submenu](#) ▼

Network [Hide Submenu](#) ▼

Carrier [Hide Submenu](#) ▼

Firewall [Hide Submenu](#) ▼

VPN [Hide Submenu](#) ▼

MultiWAN [Hide Submenu](#) ▼

Serial [Hide Submenu](#) ▼

USB [Hide Submenu](#) ▼

I/O [Hide Submenu](#) ▼

GPS [Hide Submenu](#) ▼

Applications [Hide Submenu](#) ▼

Admin [Hide Submenu](#) ▼

Add User [Add User](#)

Users Summary

No users defined.

Image 4-12-1: Users > Password Change

New Password

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

Values (characters)

admin

Confirm Password

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

Values (characters)

admin

4.0 Configuration

Add Users

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

Add User: (Note: Changes will not take effect until the system is rebooted)

Username : (5-32 ch)

Password (5-32 ch)

Confirm Password

System ▾

Network ▾

Carrier ▾

Firewall ▾

VPN ▾

MultiWAN ▾

Serial ▾

USB ▾

I/O ▾

GPS ▾

Applications ▾

Admin ▾

Add User

Users Summary

No users defined.

System	Show Submenu ▾
Settings	Disable ▾
Services	Disable ▾
Keepalive	Disable ▾
Maintenance	Disable ▾
Reboot	Disable ▾
Network	Show Submenu ▾
Summary	Disable ▾
LAN	Disable ▾
WAN	Disable ▾
DHCP	Disable ▾
DDNS	Disable ▾
Routes	Disable ▾
Ports	Disable ▾
DeviceList	Disable ▾
Carrier	Show Submenu ▾
Status	Disable ▾
Settings	Disable ▾
SMS	Disable ▾
SMSConfig	Disable ▾
DataUsage	Disable ▾
Firewall	Show Submenu ▾
Summary	Disable ▾
General	Disable ▾
PortForwarding	Disable ▾
MACIPLIST	Disable ▾
Rules	Disable ▾
FirewallDefault	Disable ▾
VPN	Hide Submenu ▾
MultiWAN	Hide Submenu ▾
Serial	Hide Submenu ▾
USB	Hide Submenu ▾
I/O	Hide Submenu ▾
CPS	Hide Submenu ▾
Applications	Hide Submenu ▾
Admin	Hide Submenu ▾
Add User	Add User

Image 4-12-2: Access Control > Users

Username

Enter the desired username. Minimum of 5 characters and maximum of 32 characters. 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

4.12.2 Admin > Authentication

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

- Local

Using the Admin or Upgrade access and associated passwords - the authentication is done 'locally' within the IPnXGii, and

- RADIUS&Local

RADIUS authentication (using a specific user name and password supplied by your RADIUS Server Administrator) - this authentication would be done 'remotely' by a RADIUS Server; if this authentication fails, proceed with Local authentication as per above.



RADIUS: Remote Authentication Dial In User Service. An authentication, authorization, and accounting protocol which may be used in network access applications.

A RADIUS server is used to verifying that information is correct.

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Users	Authentication	NMS	SNMP	Discovery	PowerSaving	Logout					
Authentication Configuration											
Authentication Server: <input type="radio"/> Local <input checked="" type="radio"/> Local&RADIUS											
Remote Server IP Address: <input type="text" value="0.0.0.0"/>											
Remote Server IP Port: <input type="text" value="1812"/> [Default: 1812]											
Shared Secret: <input type="text" value="nosecret"/>											
SSH Login Black List											
No IP address is blocked.											

Image 4-12-3: Authentication Configuration

Authentication Server

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

Values

Local
Local&RADIUS

Remote Server IP Address

In this field, the IP address of the RADIUS server is to be entered if RADIUS&Local has been selected as the Authorization Mode.

Values

Valid RADIUS server IP address

0.0.0.0

RADIUS Secret

If the Authorization Mode has been set to RADIUS&Local, obtain the RADIUS Secret for his particular client from your RADIUS Server Administrator and enter it into this field.

Values

nosecret

4.0 Configuration

4.12.3 Admin > NMS Settings

The Microhard NMS is a no cost server based monitoring and management service offered by Microhard Systems Inc. Using NMS you can monitor online/offline units, retrieve usage data, perform backups and centralized upgrades, etc. The following section describes how to get started with NMS and how to configure the IPnXGii 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.

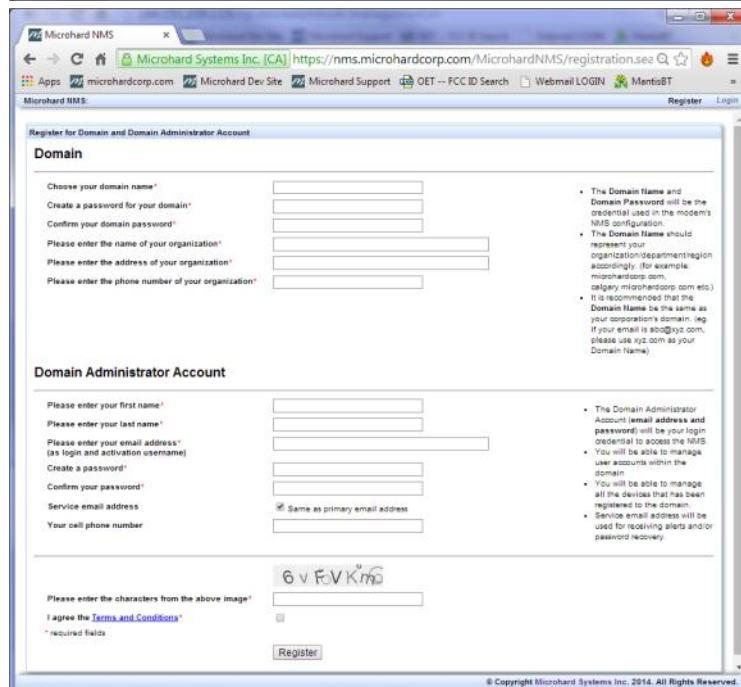
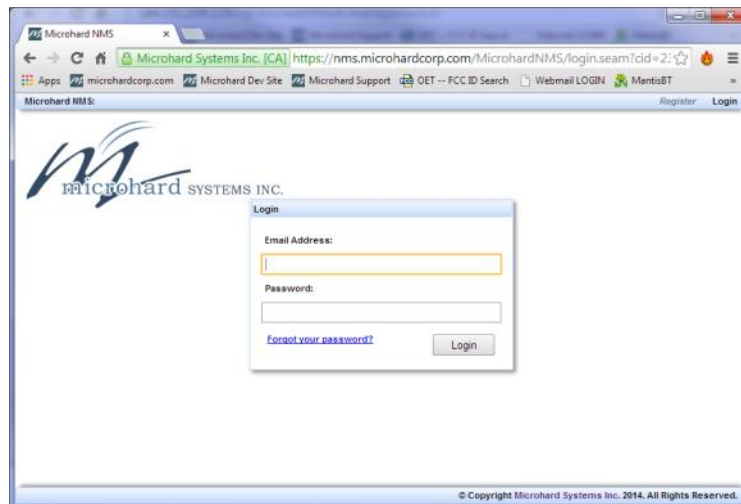


Image 4-12-4: NMS

4.0 Configuration

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

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

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

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

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

System	Network	Carrier	Firewall	VPN	MultIWAN	Serial	USB	I/O	GPS	Applications	Admin
Users	Authentication	NMS	SNMP	Discovery	PowerSaving	Logout					
NMS Configuration											
Default Settings						Edit with default configuration					
System Setting											
NMS Server/IP			nms.microhardcorp.com			Login NMS					
Domain Name			default								
Domain Password			*****			Min 5 characters					
Confirm Password			*****								
NMS Report Setting											
Carrier Location			Enable Update Over Network ▼								
Report Status			Enable NMS Report ▼								
Remote PORT			20200			[0 ~ 65535](Default:20200)					
Interval Time(s)			300			[0 ~ 65535]					
Information Selection			Available Items:								
Ethernet:			<input checked="" type="radio"/> Disable <input type="radio"/> Enable								
Carrier:			<input type="radio"/> Disable <input checked="" type="radio"/> Enable								
Com:			<input type="radio"/> Disable <input type="radio"/> Enable								
IO:			<input type="radio"/> Disable <input checked="" type="radio"/> Enable								
USB:			<input type="radio"/> Disable <input type="radio"/> Enable								
Webclient Setting											
Status			Enable ▼								
Server Type			HTTPS ▼								
Server Port			9998								
User Name			admin								
Password			****								
Interval			30			(Minutes)					

Image 4-12-5: NMS Settings

4.0 Configuration

Network Management System (NMS) Configuration

Default Settings

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

NMS Server/IP

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

Values (IP/Name)

nms.microhardcorp.com

Domain Name / Password

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

Values (chars)

default

NMS Report Setting

Carrier Location

Enable or Disable location estimation via carrier connection. When enabled, the IPnXGii 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	
<p>The IPnXGii can report information about the different interfaces it has. By default the IPnXGii 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.</p> <p>The more that is reported, the more data that is sent to the NMS system, be aware of data plan constraints and related costs.</p>	<p>Values (check boxes)</p> <p>Ethernet Carrier Radio COM DI / DO</p>
Webclient Setting	
	Status
<p>The Web Service can be enabled or disabled. This service is used to remotely control the IPnXGii. It can be used to schedule reboots, firmware upgrade and backup tasks, etc.</p>	<p>Values (chars)</p> <p>Disable/Enable</p>
	Server Type
<p>Select between HTTPS (secure), or HTTP server type.</p>	<p>Values (chars)</p> <p>HTTPS/ HTTP</p>
	Server Port
<p>This is the port where the service is installed and listening. This port should be open on any installed firewalls.</p>	<p>Values (Port#)</p> <p>9998</p>
	Username / Password
<p>This is the username and password used to authenticate the unit.</p>	<p>Values (seconds)</p> <p>admin/admin</p>
	Interval
<p>The Interval defines how often the IPnXGii 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.</p>	<p>Values (min)</p> <p>60</p>

4.0 Configuration

4.12.4 Admin > SNMP

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

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

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

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

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

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

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

The pages that follow describe the different fields required to set up SNMP on the IPnXGii. 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.



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.

4.0 Configuration

SNMP Settings

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Users	Authentication	NMS	SNMP	Discovery	PowerSaving	Logout					
SNMP Settings											
SNMP Settings											
SNMP Agent Status	Enable ▾										
Read Only Community Name	public										
Read Write Community Name	private										
Listening Port	161										
SNMP Version	Version 3 ▾										
V3 User Name	V3user										
V3 User Read Write Limit	Read Only ▾										
V3 User Authentication Level	AuthNoPriv ▾										
V3 Authentication Protocol	MD5 ▾										
V3 Authentication Password	00000000 8 to 255 characters										
SNMP Trap Settings											
SNMP Trap Status	Enable ▾										
Trap Community Name	TrapUser										
Trap Manage Host IP	0.0.0.0 0.0.0.0-Disable										
Auth Failure Traps	Disable ▾										
Download MIB File											
Get MIB File											

Image 4-12-6: Network > SNMP

SNMP Operation Mode

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

Values (selection)

Disable / V1&V2c&V3

Read Only Community Name

Effectively a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ priority.

Values (string)

public

Read Only Community Name

Also a plain-text password mechanism used to weakly authenticate SNMP queries. Being part of the community allows the SNMP agent to process SNMPv1 and SNMPv2c requests. This community name has only READ/WRITE priority.

Values (string)

private

SNMP V3 User Name

Defines the user name for SNMPv3.

Values (string)

V3user

4.0 Configuration

V3 User Read Write Limit

Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.

Values (selection)

Read Only / Read Write

V3 User Authentication Level

Defines SNMPv3 user's authentication level:

NoAuthNoPriv: No authentication, no encryption.
AuthNoPriv: Authentication, no encryption.
AuthPriv: Authentication, encryption.

Values (selection)

NoAuthNoPriv
AuthNoPriv
AuthPriv

V3 User Authentication Password

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

Values (string)

00000000

V3 User Privacy Password

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

Values (string)

00000000

SNMP Trap Version

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

Values (string)

V1 Traps V2 Traps
V3 Traps V1&V2 Traps
V1&V2&V3 Traps

Auth Failure Traps

If enabled, an authentication failure trap will be generated upon authentication failure.

Values (selection)

Disable / Enable

Trap Community Name

The community name which may receive traps.

Values (string)

TrapUser

Trap Manage Host IP

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

Values (IP Address)

0.0.0.0

4.0 Configuration

4.12.5 Admin > Discovery

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

The screenshot shows the 'Discovery' configuration page. The 'Discovery server status' is set to 'Enable'. The 'Server Port' is set to '20097'. The 'Network Discovery' table has columns for MAC Address, IP Address, Description, Product Name, and Firmware Ver. A button labeled 'Start discovery network now' is located at the bottom of the table.

Image 4-12-7: Admin > Discovery Settings

Discovery Service Status

Use this option to disable or enable the discovery service.

Values (selection)

Disable / **Discoverable** /
Changable

Server Port Settings

Specify the port running the discovery service on the IPnXGii unit.

Values (Port #)

20077

4.0 Configuration

4.12.6 Admin > Power Saving

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

System	Network	Carrier	Firewall	VPN	MultiWAN	Serial	USB	I/O	GPS	Applications	Admin
Users	Authentication	NMS	SNMP	Discovery	PowerSaving	Logout					
PowerSaving											
Current Status		POWER_ON (Disabled)									
Power Saving Control		Supply Voltage ▾									
Low Shutdown Voltage(V)		11 (Default:11)									
Recover Voltage(V)		12.5 (Default:12.5)									
Power Saving Control		Timer Schedule ▾									
		Always On Always Off									
Daily Hour Schedule		0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23									
Power Saving Control		Sniff Mode ▾									
Idle Time(minutes)		5 [1 ~ 65535]									
Alive Check Options		<input checked="" type="checkbox"/> LAN <input type="checkbox"/> RS232									
Sleep Time(minutes)		55 [1 ~ 65535]									
Wake Up Trigger		<input type="checkbox"/> LAN <input type="checkbox"/> RS232									

Image 4-12-8: Admin > Power Saving

Power Saving Control

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

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

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

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

Values (selection)

Disable
 Supply Voltage
 Timer Schedule
 Sniff Mode

4.0 Configuration

4.12.7 System > Logout

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

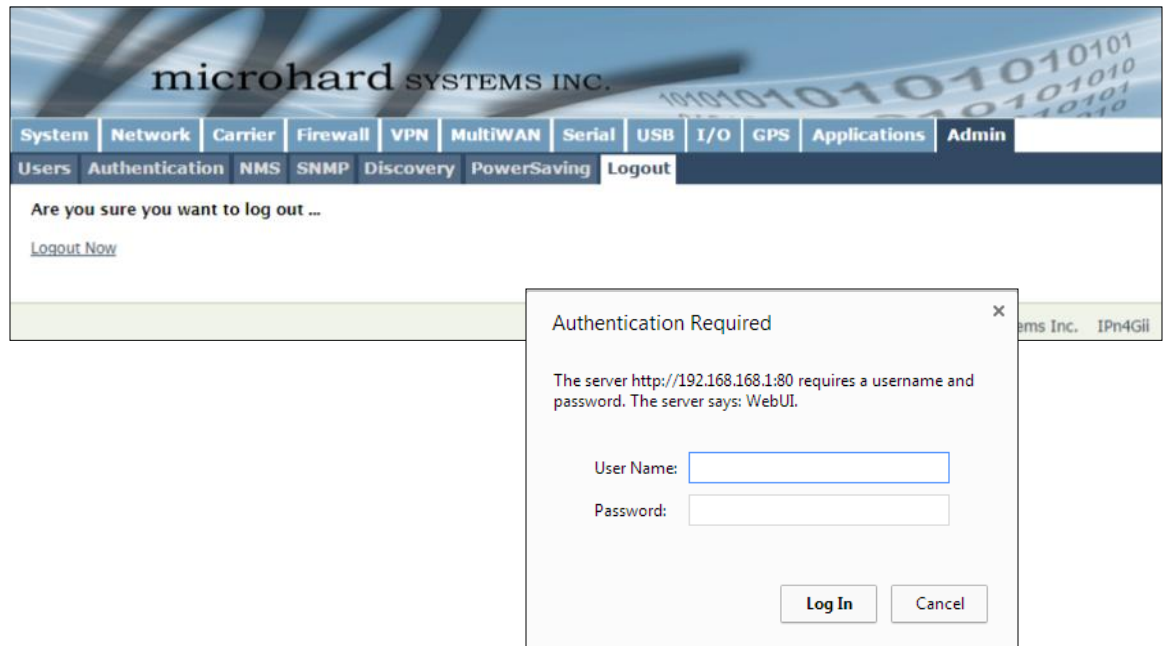


Image 4-12-9: System > logout

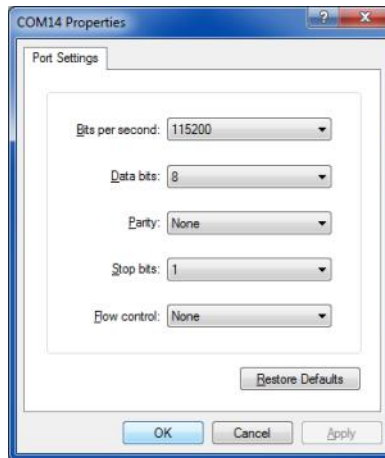
5.0 AT Command Line Interface

5.1 AT Command Overview

AT Commands can be issued to configure and manage the IPnXGii, via the back serial port (Console), or by TCP/IP (telnet).

5.1.1 Serial Port

To connect and access the AT Command interface on the IPnXGii, a physical connection must be made on the Console (TX/RX) serial port on the back of the IPnXGii. A terminal emulation program (Hyperterminal, Tera Term, ProComm, Putty etc) can then be used to communicate with the IPnXGii. The port settings of this port can be modified by changing the settings of the Console Port, in the Serial configuration menus.



Default Settings:

Baud rate: **115200**

Data bits: **8**

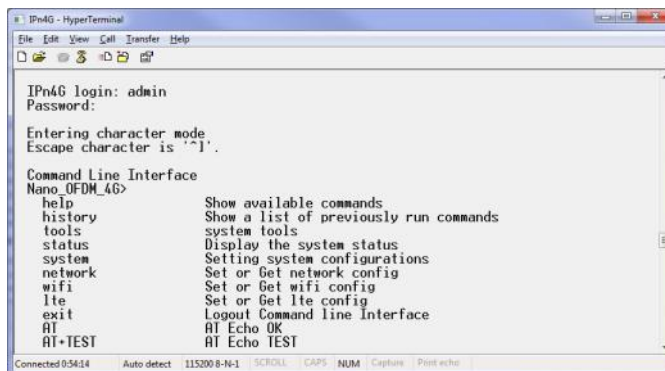
Parity: **None**

Stop Bits: **1**

Flow Control: **None**

Image 5-1: Console Port Settings

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



Default Settings:

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

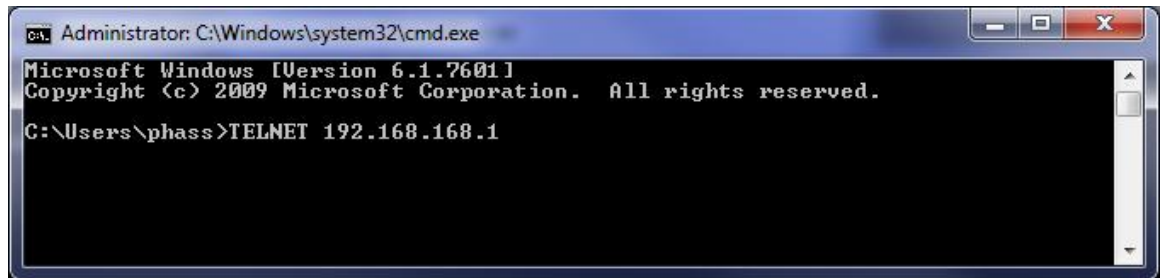


Image 5-3: Establishing a Telnet Session

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

Once a session is established a login is required to continue. As seen in the Serial port setup, the default login is **admin**, and the password is **admin**. Once verified, the AT Command Line Interface menu is shown and AT Commands can now be issued. (Type "?" or Help to list the commands).



The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

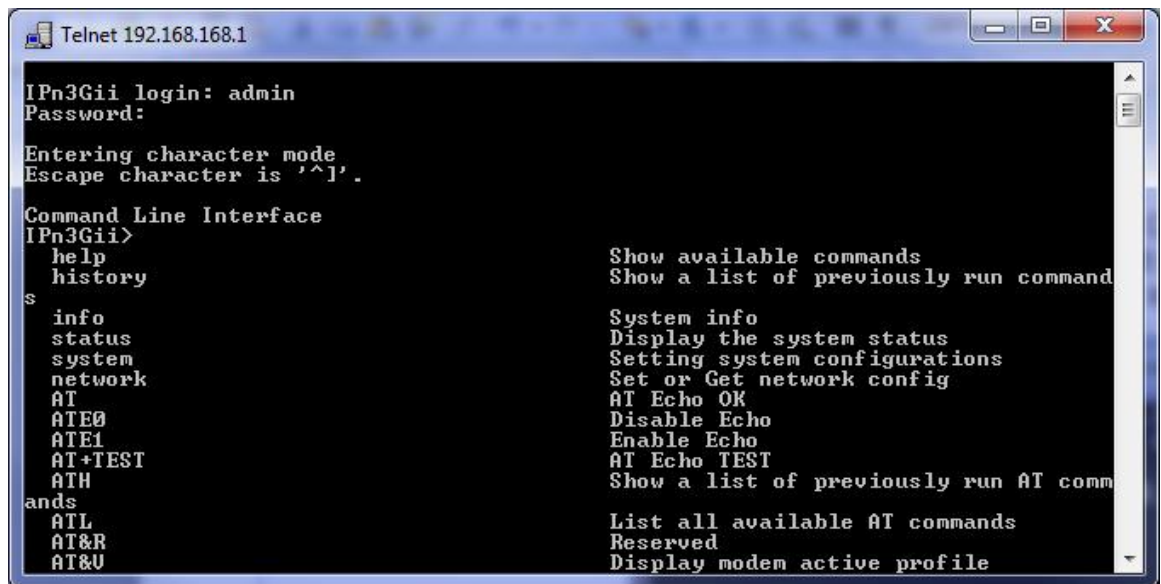


Image 5-4: Telnet AT Command Session

5.0 AT Command Line Interface

5.2 AT Command Syntax

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

- 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
```

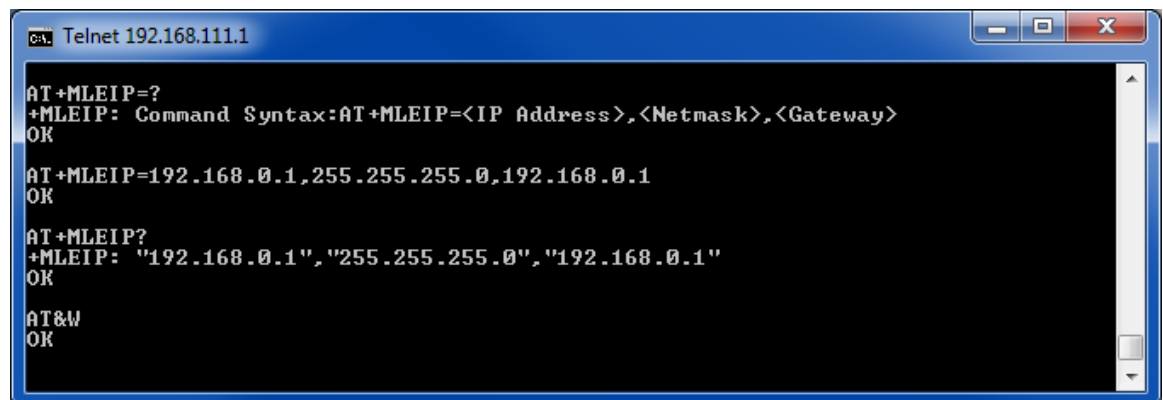
Setting a value:

```
AT+MLEIP=192.168.168.1,255.255.255.0,192.168.168.1 <Enter>
OK
```

Query a setting:

```
AT+MLEIP? <Enter>
+MLEIP: "192.168.168.1", "255.255.255.0", "192.168.168.1"
OK
```

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



```

ca. Telnet 192.168.111.1
AT+MLEIP=?
+MLEIP: Command Syntax:AT+MLEIP=<IP Address>,<Netmask>,<Gateway>
OK
AT+MLEIP=192.168.0.1,255.255.255.0,192.168.0.1
OK
AT+MLEIP?
+MLEIP: "192.168.0.1", "255.255.255.0", "192.168.0.1"
OK
AT&W
OK
```

Image 5-5: Telnet AT Command Syntax

Once AT commands are entered, they must be saved into the file system to enable the changes.

AT&W	Saves changes.
ATO or ATA	Exits the AT Command Line Interface, if used before AT&W, changes are discarded.

5.0 AT Command Line Interface

5.3 Supported AT Commands

AT

Description

Echo OK.

Command Syntax

AT <enter>

Example

Input:

AT <enter>

Response:

OK

ATE0

Description

Disables Local Echo.

Command Syntax

ATE0 <enter>

Example

Input:

ATE0 <enter>

Response:

OK

ATE1

Description

Enables Local Echo.

Command Syntax

ATE1 <enter>

Example

Input:

ATE1 <enter>

Response:

OK

AT+TEST

Description

Echo TEST

Command Syntax

AT+TEST <enter>

Example

Input:

AT+TEST <enter>

Response:

AT ECHO TEST:

:0

5.0 AT Command Line Interface

ATH

Description

Show a list of previously run commands.

Command Syntax

ATH <enter>

Example

Input:

ATH <enter>

Response:

AT Command history: 1. ATH 2. ATL 3. ATH

AT&R

Description

Read modem profile to editable profile. (Reserved)

Command Syntax

AT&R <enter>

Example

Input:

AT&R <enter>

Response:

OK

AT&V

Description

Read modem active profile.

Command Syntax

AT&V <enter>

Example

Input:

AT&V <enter>

Response:

&V:

hostname:Bullet

timezone:MST7MDT,M3.2.0,M11.1.0

systemmode:gateway

OK

5.0 AT Command Line Interface

AT&W

Description

Reserved.

Command Syntax

AT&W <enter>

Example

Input:

AT&W <enter>

Response:

OK

AT+MREB

Description

Reboots the modem.

Command Syntax

AT+MREB <enter>

Example

Input:

AT+MREB <enter>

Response:

OK. Rebooting...

ATA

Description

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

Command Syntax

ATA <enter>

Example

Input:

ATA <enter>

Response:

OK

Bullet Login:

5.0 AT Command Line Interface

ATO

Description

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

Command Syntax

ATO <enter>

Example

Input:

ATA <enter>

Response:

OK

Bullet 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

Check modem's phone number.

Command Syntax

AT+CNUM <enter>

Example

Input:

AT+CNUM <enter>

Response:

+CNUM: "+15875558645"

OK

AT+CIMI

Description

Check modem's IMEI and IMSI numbers.

Command Syntax

AT+CIMI <enter>

Example

Input:

AT+CIMI <enter>

Response:

+CIMI: IMEI:012773002108403, IMSI:302720406982933

OK

AT+CCID

Description

Check modem's SIM card number.

Command Syntax

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:352237050025180
SIMID:89302610402015463536
IMSI:302610010578158

Status:Connected

Network:Bell

RSSI:-73

Temperature:40

Ethernet Port:

MAC:00:0F:92:00:D4:BB

IP:192.168.168.1

MASK:255.255.255.0

Wan MAC:00:0F:92:00:D4:BB

Wan IP:0.0.0.0

Wan MASK:0.0.0.0

System:

Device:Bullet

Product:Bullet

Image:Bullet

Hardware:Rev A

Software:v1.2.0 build 1007

Copyright: 2013-2014 Microhard Systems Inc.

Time: Thu Jul 10 09:48:28 2014

AT+MMNAME

Description

Modem Name / Radio Description. 30 chars.

Command Syntax

AT+MMNAME=<modem_name>

Example

Input: (To set value)

AT+MMNAME=Bullet_CLGY<enter>

Response:

OK

Input: (To retrieve value)

AT+MMNAME=?<enter>

Response:

+MMNAME: Bullet_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

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

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+MSCMD

Description

Enable/Disable SMS Commands and if configured the phone filter list.

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

Example

Input:

AT+MSCMD=1,1,403556767,4057890909<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MDISS

Description

Configure discovery mode service used by Bullet 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 Bullet.

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.dyndns.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 Time_s>]

Mode:

- 0 Disable
- 1 Modem 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 Time_s>]

Mode:

- 0 Disable
- 1 Enable UDP Report

5.0 AT Command Line Interface

AT+MCTPS1

Description

Enable/Disable the Com1 serial port.

Command Syntax

AT+MCTPS1=<Mode>

Mode:

0 Disable
1 Enable

Example

Input:

AT+MCTPS1=0<enter>

Response:

OK

AT+MCTBR1

Description

Set Comport baud rate.

Command Syntax

AT+MCTBR1=<Baud Rate>

Baud Rate:

0 300
1 600
2 1200
3 2400
4 3600
5 4800
6 7200
7 9600
8 14400
9 19200
10 28800
11 38400
12 57600
13 115200

Example

Input:

AT+MCTBR1=13<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTDF1

Description

Set Comport data format

Example

Input:
AT+MCTDF1=0<enter>
Response:
OK

Command Syntax

AT+MCTDF1=<data format>
Data Format:
0 8N1
1 8N2
2 8E1
3 8O1
4 7N1
5 7N2
6 7E1
7 7O1
8 7E2
9 7O2

AT+MCTDM1

Description

Set Comport data mode.

Example

Input:
AT+MCTDM1=1<enter>
Response:
OK

Command Syntax

AT+MCTDM1=<Data Mode>
Data Mode:
0 Seamless
1 Transparent

AT+MCTCT1

Description

Set Comport character timeout.

Example

Input:
AT+MCTCT1=0<enter>
Response:
OK

Command Syntax

AT+MCTCT1=<timeout_s>

5.0 AT Command Line Interface

AT+MCTMPS1

Description

Set Comport data format

Command Syntax

AT+MCTMPS1=<size>

Example

Input:

AT+MCTMPS1=1024<enter>

Response:

OK

AT+MCTP1

Description

Set Comport port priority.

Command Syntax

AT+MCTP1=<Mode>

Mode:

- 0 Normal
- 1 Medium
- 2 High

Example

Input:

AT+MCTP1=0<enter>

Response:

OK

AT+MCTNCDI1

Description

Enable/Disable Comport port no-connection data intake.

Command Syntax

AT+MCTNCDI1=<Mode>

Mode:

- 0 Disable
- 1 Enable

Example

Input:

AT+MCTNCDI1=1<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTMTC1

Description

Set Comport modbus TCP configuration.

Command Syntax

AT+MCTMTC1=<Status>, <Protection status>, <Protection Key>

Status and Protection Status:

- 0 Disable
- 1 Enable

Example

Input:

AT+MCTMTC1=0,0,1234<enter>

Response:

OK

AT+MCTIPM1

Description

Set the Comport serial port IP Protocol Mode.

Command Syntax

AT+MCTIPM1=<Mode>

Mode:

- 0 TCP Client
- 1 TCP Server
- 2 TCP Client/Server
- 3 UDP Point to Point
- 4 UDP Point to Multipoint(P)
- 5 UDP Point to Multipoint(MP)
- 6 UDP Multipoint to Multipoint
- 7 SMTP Client
- 9 SMS Transparent Mode
- 11 GPS Transparent Mode

Example

Input:

AT+MCTIPM1=1<enter>

Response:

OK

AT+MCTTC1

Description

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

Command Syntax

AT+MCTTC1=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>

Example

Input:

AT+MCTTC1=0.0.0.0,20002,60<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTTS1

Description

Set TCP Server parameters when IP Protocol Mode is set to TCP Server.

Example

Input:
AT+MCTTS1=0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTS1=<Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:
0 Monitor
1 Multi-polling

AT+MCTTCS1

Description

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

Example

Input:
AT+MCTCS1=0.0.0.0,20002,60,0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTCS1=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>, <Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:
0 Monitor
1 Multi-polling

AT+MCTUPP1

Description

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

Example

Input:
AT+MCTUPP1=0.0.0.0,20002,20002,10<enter>
Response:
OK

Command Syntax

**AT+MCTUPP1=<Remote Server IP>, <Remote Server Port>, <Liste
ner Port>, <UDP timeout_s>**

5.0 AT Command Line Interface

AT+MCTUPMP1

Description

Set UDP Point-to-Multipoint as point parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (P)

Command Syntax

AT+MCTUPMP1=<Multicast IP>, <Multicast Port>, <Listener Port>, <Time to live>

Example

Input:

AT+MCTUPMP1=224.1.1.2,20002,20012,1<enter>

Response:

OK

AT+MCTUPMM1

Description

Set UDP Point-to-Multipoint as MP parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (MP)

Command Syntax

AT+MCTUPMM1=<Remote IP>, <Remote Port>, <Multicast IP>, <Multicast Port>

Example

Input:

AT+MCTUPMM1=0.0.0.0,20012,224.1.1.2,20002<enter>

Response:

OK

AT+MCTUMPMP1

Description

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

Command Syntax

AT+MCTUMPMP1=<Multicast IP>, <Multicast Port>, <Time to live>, <Listen Multicast IP>, <Listen Multicast Port>

Example

Input:

AT+MCTUMPMP1=224.1.1.2,20012,1,224.1.1.2,20012<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTPS2

Description

Enable/Disable the Com2 serial port.

Command Syntax

AT+MCTPS2=<Mode>

Mode:

- 0 Disable
- 1 Enable

Example

Input:

AT+MCTPS2=0<enter>

Response:

OK

AT+MCTBR2

Description

Set Comport baud rate.

Command Syntax

AT+MCTBR2=<Baud Rate>

Baud Rate:

- 0 300
- 1 600
- 2 1200
- 3 2400
- 4 3600
- 5 4800
- 6 7200
- 7 9600
- 8 14400
- 9 19200
- 10 28800
- 11 38400
- 12 57600
- 13 115200

Example

Input:

AT+MCTBR2=13<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTDF2

Description

Set Comport data format

Example

Input:
AT+MCTDF2=0<enter>
Response:
OK

Command Syntax

AT+MCTDF2=<data format>

Data Format:

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

AT+MCTDM2

Description

Set Comport data mode.

Example

Input:
AT+MCTDM2=1<enter>
Response:
OK

Command Syntax

AT+MCTDM2=<Data Mode>

Data Mode:

0 Seamless
1 Transparent

AT+MCTCT2

Description

Set Comport character timeout.

Example

Input:
AT+MCTCT2=0<enter>
Response:
OK

Command Syntax

AT+MCTCT2=<timeout_s>

5.0 AT Command Line Interface

AT+MCTMPS2

Description

Set Comport data format

Command Syntax

AT+MCTMPS2=<size>

Example

Input:

AT+MCTMPS2=1024<enter>

Response:

OK

AT+MCTP2

Description

Set Comport port priority.

Command Syntax

AT+MCTP2=<Mode>

Mode:

- 0 Normal
- 1 Medium
- 2 High

Example

Input:

AT+MCTP2=0<enter>

Response:

OK

AT+MCTNCDI2

Description

Enable/Disable Comport port no-connection data intake.

Command Syntax

AT+MCTNCDI2=<Mode>

Mode:

- 0 Disable
- 1 Enable

Example

Input:

AT+MCTNCDI2=1<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTMTC2

Description

Set Comport modbus TCP configuration.

Command Syntax

AT+MCTMTC2=<Status>, <Protection status>, <Protection Key>

Status and Protection Status:

- 0 Disable
- 1 Enable

Example

Input:

AT+MCTMTC2=0,0,1234<enter>

Response:

OK

AT+MCTIPM2

Description

Set the Comport serial port IP Protocol Mode.

Command Syntax

AT+MCTIPM2=<Mode>

Mode:

- 0 TCP Client
- 1 TCP Server
- 2 TCP Client/Server
- 3 UDP Point to Point
- 4 UDP Point to Multipoint(P)
- 5 UDP Point to Multipoint(MP)
- 6 UDP Multipoint to Multipoint
- 7 SMTP Client
- 9 SMS Transparent Mode
- 11 GPS Transparent Mode

Example

Input:

AT+MCTIPM2=1<enter>

Response:

OK

AT+MCTTC2

Description

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

Command Syntax

AT+MCTTC2=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>

Example

Input:

AT+MCTTC2=0.0.0.0,20002,60<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MCTTS2

Description

Set TCP Server parameters when IP Protocol Mode is set to TCP Server.

Example

Input:
AT+MCTTS2=0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTS2=<Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:
0 Monitor
1 Multi-polling

AT+MCTTCS2

Description

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

Example

Input:
AT+MCTCS2=0.0.0.0,20002,60,0,100,20002,300<enter>
Response:
OK

Command Syntax

AT+MCTTCS2=<Remote Server IP>, <Remote Server Port>, <Outgoing timeout_s>, <Polling Mode>, <Polling timeout_s>, <Local Listener Port>, <Connection timeout_s>

Polling Mode:
0 Monitor
1 Multi-polling

AT+MCTUPP2

Description

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

Example

Input:
AT+MCTUPP2=0.0.0.0,20002,20002,10<enter>
Response:
OK

Command Syntax

AT+MCTUPP2=<Remote Server IP>, <Remote Server Port>, <Listener Port>, <UDP timeout_s>

5.0 AT Command Line Interface

AT+MCTUPMP2

Description

Set UDP Point-to-Multipoint as point parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (P)

Command Syntax

AT+MCTUPMP2=<Multicast IP>, <Multicast Port>, <Listener Port>, <Time to live>

Example

Input:

AT+MCTUPMP2=224.1.1.2,20002,20012,1<enter>

Response:

OK

AT+MCTUPMM2

Description

Set UDP Point-to-Multipoint as MP parameters when IP Protocol Mode is set to UDP Point-to-Multipoint (MP)

Command Syntax

AT+MCTUPMM2=<Remote IP>, <Remote Port>, <Multicast IP>, <Multicast Port>

Example

Input:

AT+MCTUPMM2=0.0.0.0,20012,224.1.1.2,20002<enter>

Response:

OK

AT+MCTUMPMP2

Description

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

Command Syntax

AT+MCTUMPMP2=<Multicast IP>, <Multicast Port>, <Time to live>, <Listen Multicast IP>, <Listen Multicast Port>

Example

Input:

AT+MCTUMPMP2=224.1.1.2,20012,1,224.1.1.2,20012<enter>

Response:

OK

5.0 AT Command Line Interface

AT+MIOMODE

Description

Get/Set IO input or output mode.

Example

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

Input:
AT+MIOMODE?
Response:
+MIOMODE: IO port mode
Mode1: 0 Input
Mode2: 0 Input
OK

Command Syntax

AT+MIOMODE=<Index>,<Mode>

Index:

The index of IO port, 1 to 2

Mode:

0 Input
1 Output

AT+MIOOC

Description

Get/Set output control

Example

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

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

Command Syntax

AT+MIOOC=<Index>,<Output Control>

Index:

The index of IO port, 1 to 2

Output Control:

0 Open
1 Close

5.0 AT Command Line Interface

AT+MIOSTATUS

Description

Get IO Status

Command Syntax

AT+MIOMODE <enter>

Example

Input:

AT+MIOSTATUS <enter>

Response:

+MIOSTATUS: IO status
iodigiival1=Fault
iodigiival2=High
OK

AT+MIOMETER

Description

Get IO meter (V)

Command Syntax

AT+MIOMETER <enter>

Example

Input:

AT+MIOMETER <enter>

Response:

+MIOMETER: IO meter(V)
iovolts1=12.25
iovolts2=2.74
OK

AT+IMEI

Description

Get Modem's IMEI

Command Syntax

AT+IMEI <enter>

Example

Input:

AT+IMEI <enter>

Response:

+IMEI: 352237050103870
OK

5.0 AT Command Line Interface

AT+IMSI

Description

Get Modem's IMSI

Command Syntax

AT+IMSI <enter>

Example

Input:

AT+IMSI <enter>

Response:

+IMSI: 302610012606734

OK

AT+IMSI

Description

Get Modem's IMSI

Command Syntax

AT+IMSI <enter>

Example

Input:

AT+IMSI <enter>

Response:

+IMSI: 302610012606734

OK

AT+NETRSSI

Description

Get Modem's RSSI

Command Syntax

AT+NETRSSI <enter>

Example

Input:

AT+NETRSSI <enter>

Response:

+NETRSSI:-65

OK

5.0 AT Command Line Interface

AT+POWERIN

Description

Get Modem's Supply Voltage

Command Syntax

AT+POWERIN <enter>

Example

Input:
AT+POWERIN <enter>
Response:
+POWERIN: 11.77
OK

AT+BOARDTEMP

Description

Get Modem's Board Temperature (C)

Command Syntax

AT+BOARDTEMP <enter>

Example

Input:
AT+BOARDTEMP <enter>
Response:
+BOARDTEMP: 44.79
OK

AT+WANIP

Description

Get Modem's WAN IP

Command Syntax

AT+WANIP <enter>

Example

Input:
AT+WANIP <enter>
Response:
+WANIP: 74.186.198.97
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
ATEO	Disable Echo
ATE1	Enable Echo
AT+TEST	AT Echo TEST
ATH	Show a list of previously run AT commands
ATL	List all available AT commands
AT&R	Reserved
AT&V	Display modem active profile
AT&W	Reserved
AT+MREB	Reboot the modem
ATA	Quit
ATO	Quit
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 of 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

(Continued...)

5.0 AT Command Line Interface

AT+MCTPS1	Enable or disable com1 port
AT+MCTBR1	Set com1 port baud rate
AT+MCTDF1	Set com1 port data format
AT+MCTDM1	Set com1 port data mode
AT+MCTCT1	Set com1 port character timeout
AT+MCTMPS1	Set com1 port maximum packet size
AT+MCTP1	Set com1 port priority
AT+MCTNCDI1	Enable or disable com1 port no-connection data intake
AT+MCTMTC1	Set com1 port modbus tcp configuration
AT+MCTIPM1	Set com1 port IP protocol mode
AT+MCTTC1	Set com1 port tcp client configuration when IP protocol mode be set to TCP Client
AT+MCTTS1	Set com1 port tcp server configuration when IP protocol mode be set to TCP Server
AT+MCTTCS1	Set com1 port tcp client/server configuration when IP protocol mode be set to TCP Client/Server
AT+MCTUPP1	Set com1 port UDP point to point configuration when IP protocol mode be set to UDP point to point
AT+MCTUPMP1	Set com1 port UDP point to multipoint as point configuration when IP protocol mode be set to UDP point to multipoint(P)
AT+MCTUPMM1	Set com1 port UDP point to multipoint as MP configuration when IP protocol mode be set to UDP point to multipoint(MP)
AT+MCTUMPMP1	Set com1 port UDP multipoint to multipoint configuration when IP protocol mode be set to UDP multipoint to multipoint
AT+MCTPS2	Enable or disable com2 port
AT+MCTBR2	Set com2 port baud rate
AT+MCTDF2	Set com2 port data format
AT+MCTDM2	Set com2 port data mode
AT+MCTCT2	Set com2 port character timeout
AT+MCTMPS2	Set com2 port maximum packet size
AT+MCTP2	Set com2 port priority
AT+MCTNCDI2	Enable or disable com2 port no-connection data intake
AT+MCTMTC2	Set com2 port modbus tcp configuration
AT+MCTIPM2	Set com2 port IP protocol mode
AT+MCTTC2	Set com2 port tcp client configuration when IP protocol mode be set to TCP Client
AT+MCTTS2	Set com2 port tcp server configuration when IP protocol mode be set to TCP Server
AT+MCTTCS2	Set com2 port tcp client/server configuration when IP protocol mode be set to TCP Client/Server
AT+MCTUPP2	Set com2 port UDP point to point configuration when IP protocol mode be set to UDP point to point
AT+MCTUPMP2	Set com2 port UDP point to multipoint as point configuration when IP protocol mode be set to UDP point to multipoint(P)
AT+MCTUPMM2	Set com2 port UDP point to multipoint as MP configuration when IP protocol mode be set to UDP point to multipoint(MP)
AT+MCTUMPMP2	Set com2 port UDP multipoint to multipoint configuration when IP protocol mode be set to UDP multipoint to multipoint
AT+MIOMODE	Get/Set IO input or output mode
AT+MIOOC	Get/Set output control
AT+MIOSTATUS	Get IO status
AT+MIOMETER	Get IO meter(V)
AT+IMEI	Get Modem's IMEI
AT+IMSI	Get Modem's IMSI
AT+NETRSSI	Get Modem's RSSI
AT+POWERIN	Get Modem's Voltage
AT+BOARDTEMP	Get Modem's Temperature
AT+WANIP	Get Modem's WAN IP

Appendix A: Serial Interface

Module (DCE)	Signal	Host (e.g. PC) (DTE)	
1	DCD →	IN	Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE, informing the DTE that a carrier is present).
2	RX →	IN	The interface conforms to standard RS-232 signals, so direct connection to a host PC (for example) is accommodated.
3	← TX	OUT	
4	← DTR	OUT	
5	SG		
6	DSR →	IN	
7	← RTS	OUT	
8	CTS →	IN	The signals in the asynchronous serial interface are described below:

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

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

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

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)

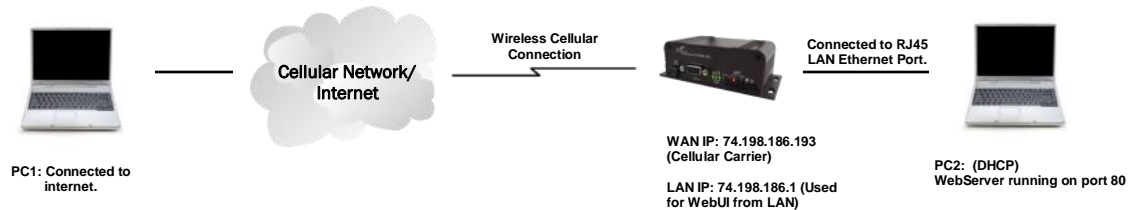
By completing the Quick Start process, a user should have been able to log in and set up the IPnXGii to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, a common application of the IPnXGii is to access connected devices remotely. In order to do this, the IPnXGii 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 IPnXGii and the connected device/PC to work with IP-Passthrough. IP-Passthrough means that the IPnXGii 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 IPnXGii (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 IPnXGii.

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

In the example below we have a IPn3Gii 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 IPn3Gii, the IPn3Gii would then automatically assign, via DHCP, the WAN IP to the attached PC2, creating a transparent connection.



Step 1

Log into the IPn3Gii (Refer to Quick Start), and ensure that DHCP is enabled on the **Network > LAN** page.

DHCP Server	
Mode	Enable
Start IP	192.168.0.100
Limit	150
Lease Time (in minutes)	720

Step 2

Since PC2 requires port 80 to be used as its Web server port, port 80 cannot be used on the IPn3Gii, by default it retains this port for remote configuration. To change the port used by the IPn3Gii, navigate to the **System > Services** page. For this example we are going to change it to port 8080. When changing port numbers on the IPn3Gii, it is recommended to reboot the unit before continuing, remember the new WebUI port is now 8080 when you log back into the IPn3Gii. (e.g. 192.168.168.1:8080).

Services Status			
FTP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		Update
Telnet	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Port <input type="text" value="23"/>	Update
SSH	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Port <input type="text" value="22"/>	Update
Web UI	<input checked="" type="radio"/> HTTP/HTTPS <input type="radio"/> HTTP <input type="radio"/> HTTPS	Port <input type="text" value="8080"/> HTTP/ <input type="text" value="443"/> HTTPS	Update

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

Step 3

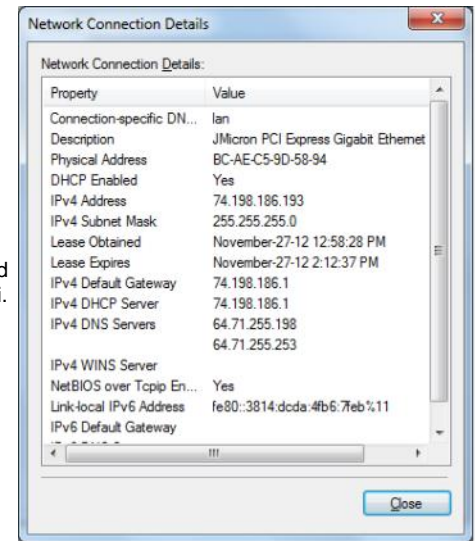
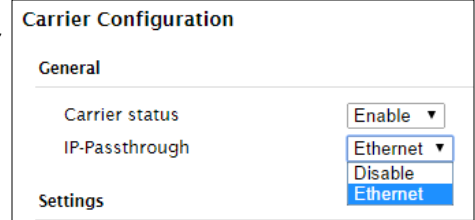
Now IP-Passthrough can be enabled on the IPn3Gii. Under the **Carrier > Settings** tab, IP-Passthrough can be found. To enable this feature, select "Ethernet" from the drop down box. Once the changes are applied, whichever device is physically connected to the LAN RJ45 port, will dynamically be assigned 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 IPn3Gii on the LAN side, by using the X.X.X.1 IP Address, where the first 3 octets of the WAN IP are used in place of the X's. (e.g. 74.198.186.1, and remember the HTTP port in this example was changed to 8080).

The firewall must be configured and/or rules must be created to allow Carrier traffic. See Firewall Example for more information.

Step 4

Attach the remote device or PC to the RJ45 port of the IPn3Gii. The end device has to be set up for DHCP to get an IP address from the IPn3Gii. 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 IPn3Gii 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 IPn3Gii. Once IP-Passthrough is enabled you can access the IPn3Gii WebUI by one of the following methods:

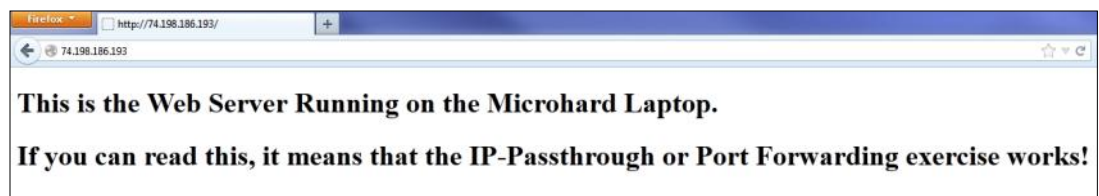
- Remotely on the WAN side (usually the internet), using the WAN IP, and the port specified for HTTP operation (or, if enabled, by using the HTTPS (443) ports), in this example with would be 74.198.186.193:8080.
- On the LAN side, by entering in the first 3 octets of the WAN IP and .1 for the fourth, 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 IPn3Gii. 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 IPn3Gii into a web browser. As seen below, when the IP Address of the IPn3Gii 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)

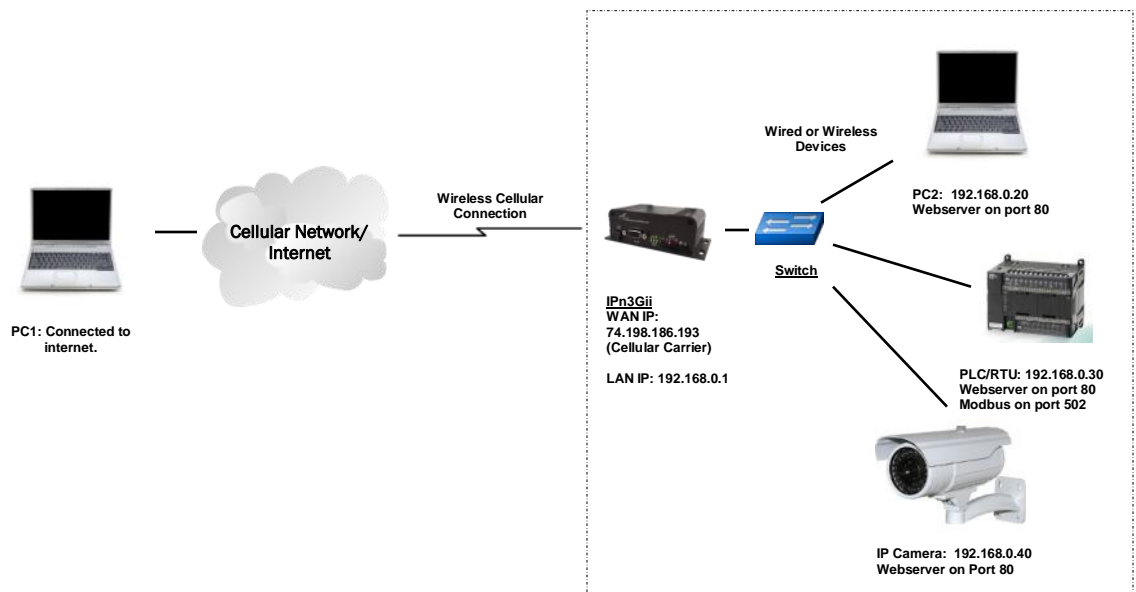
By completing the Quick Start process, a user should have been able to log in and set up the IPnXGii to work with their cellular carrier. By completing this, the modem is ready to be used to access the internet and provide mobile connectivity. However, one of the main applications of the IPnXGii is to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

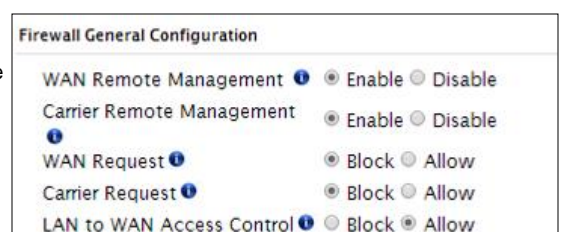
DMZ (a form of port forwarding) is useful for situations where there are multiple devices connected to the IPnXGii, but all incoming traffic is destined for a single device. It is also popular to use DMZ in cases where a single device is connected but several ports are forwarded and other features of the IPnXGii 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 IPn3Gii directly using the public static IP assigned by the wireless carrier, but not the devices behind it. In this case the IPn3Gii 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 IPn3Gii.



Step 1

Log into the IPn3Gii (Refer to Quick Start), and ensure that the **Firewall** is enabled. This can be found under **Firewall > General**. Also ensure that that sufficient **Rules** or **IP lists** have been setup to allow specific traffic to pass through the IPn3Gii. See the Firewall Example in the next Appendix for information on how to allow connections from an IP or to open ports. Once that is complete, remember to "Submit" the changes.



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

Step 2

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

Description	WAN IP	External Port	Internal IP	Internal Port
IPn3Gii WebUI	74.198.186.193	80	192.168.0.1	80
PC2 Web Server	74.198.186.193	8080	192.168.0.20	80
PLC Web Server	74.198.186.193	8081	192.168.0.30	80
PLC Modbus	74.198.186.193	10502	192.168.0.30	502
Camera Web Server	74.198.186.193	8082	192.168.0.40	80

Notice that to the outside user, the IP Address for every device is the same, only the port number changes, but on the LAN, each external port is mapped to an internal device and port number. Also notice that the port number used for the configuration GUI for all the devices on the LAN is the same, this is fine because they are located on different IP addresses, and the different external ports mapped by the IPn3Gii (80, 8080, 8081, 8082), will send the data to the intended destination.

Step 3

Create a rule for each of the lines above. A rule 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 IPn3Gii itself. To create port forwarding rules, Navigate to the **Firewall > Port Forwarding** menu. When creating rules, each rule 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 IPn3Gii.

Once all rules have been added, the IPn3Gii 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 IPn3Gii.

Name	Source	Internal IP	Internal Port	Protocol	External Port
PC2_WS	Carrier	192.168.0.20	80	TCP	8080
PLC_WS	Carrier	192.168.0.30	80	TCP	8081
PLC_modbus	Carrier	192.168.0.30	502	TCP	10502
Camera	Carrier	192.168.0.40	80	TCP	8082

For best results, reboot the IPn3Gii.

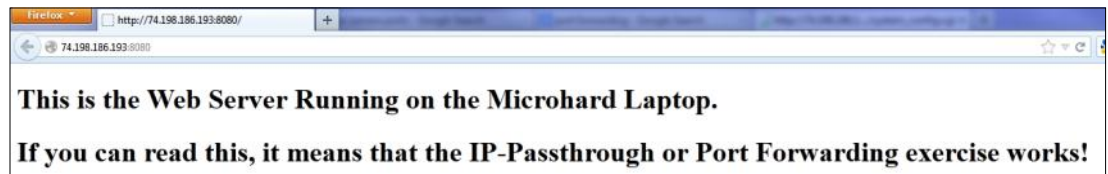
Step 4

Configure the static addresses on all attached devices. Port forwarding requires that all the attached devices have static IP addresses, this ensures 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 IPn3Gii 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:

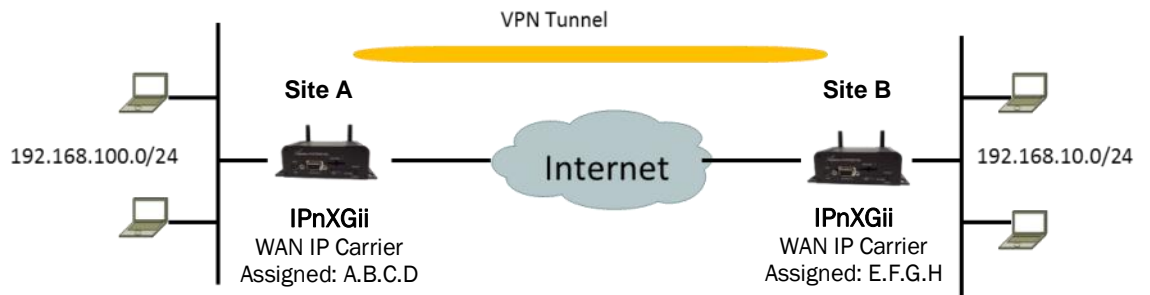
To access the other devices/services: For the PLC Web Server: 74.198.186.193:8081, for the Camera 74.198.186.193:8082, and for the Modbus on the PLC telnet to 74.198.186.193:10502 etc.

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 IPnXGii 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 IPnXGii is to access connected devices remotely. In addition to Port Forwarding and IP-Passthrough, the IPnXGii 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 IPnXGii 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 IPnXGii 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 IPnXGii to existing VPN capable devices, such as Cisco or Firebox.

Example: IPnXGii to IPnXGii (Site-to-Site)



Step 1

Log into each of the IPnXGii's (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 IPnXGii. Once that is complete, remember to "Apply" the changes.

Step 2

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

Site A

System	Network	Carrier	Wireless
Status	LAN	Routes	GRE SNMP sdpS
Network LAN Configuration			
LAN Configuration			
Spanning Tree (STP)	On		
Connection Type	Static IP		
IP Address	192.168.100.1		
Netmask	255.255.255.0		
Default Gateway	192.168.100.1		
LAN DNS Servers			
DNS Server 1			
DNS Server 2			
LAN DHCP			
DHCP Server	Enable		
Start	192.168.100.100		
Limit	150		
Lease Time (in minutes)	2		

Site B

System	Network	Carrier	Wireless
Status	LAN	Routes	GRE SNMP sdpS
Network LAN Configuration			
LAN Configuration			
Spanning Tree (STP)	On		
Connection Type	Static IP		
IP Address	192.168.10.1		
Netmask	255.255.255.0		
Default Gateway	192.168.10.1		
LAN DNS Servers			
DNS Server 1			
DNS Server 2			
LAN DHCP			
DHCP Server	Enable		
Start	192.168.10.100		
Limit	150		
Lease Time (in minutes)	2		

Appendix D: VPN Example (Page 2 of 2)

Step 3

Add a VPN Gateway to Gateway tunnel on each IPnXGii.

System	Network	Carrier	Firewall	VPN	Serial	USB	I/O	GPS	Applications	Admin																						
Summary Gateway To Gateway Client To Gateway GRE VPN Client Access Certificate Management																																
Summary Gateway To Gateway																																
<table border="1"> <thead> <tr> <th>No.</th> <th>Name</th> <th>Status</th> <th>Phase2 Enc/Auth/Grp</th> <th>Interface</th> <th>Local Group</th> <th>Remote Group</th> <th>Remote Gateway</th> <th>RX/TX Bytes</th> <th>Tunnel Test</th> <th>Config.</th> </tr> </thead> <tbody> <tr> <td colspan="11"> <div style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 5px;">Add</div> </td> </tr> </tbody> </table>											No.	Name	Status	Phase2 Enc/Auth/Grp	Interface	Local Group	Remote Group	Remote Gateway	RX/TX Bytes	Tunnel Test	Config.	<div style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 5px;">Add</div>										
No.	Name	Status	Phase2 Enc/Auth/Grp	Interface	Local Group	Remote Group	Remote Gateway	RX/TX Bytes	Tunnel Test	Config.																						
<div style="border: 1px solid black; border-radius: 50%; width: 30px; height: 30px; display: flex; align-items: center; justify-content: center; margin: 5px;">Add</div>																																

Site A

Summary	Gateway To Gateway	Client To Gateway
Gateway To Gateway Add a New Tunnel		
Tunnel Name: Tunnel_1 Enable: <input checked="" type="checkbox"/> Authentication: Preshared Key		
Local Group Setup		
Local Security Gateway Type: IP Only Interface IP Address: A.B.C.D Next-hop Gateway IP: Group Subnet IP: 192.168.100.0 Group Subnet Mask: 255.255.255.0 Group Subnet Gateway:		
Remote Group Setup		
Remote Security Gateway Type: IP Only Gateway IP Address: E.F.G.H Next-hop Gateway IP: Group Subnet IP: 192.168.10.0 Group Subnet Mask: 255.255.255.0		
IPsec Setup		
Aggressive Mode: <input type="checkbox"/> Phase 1 DH Group: modp1024 Phase 1 Encryption: 3des Phase 1 Authentication: md5 Phase 1 SA Life Time(s): 28800 Perfect Forward Secrecy: <input type="checkbox"/> Phase 2 SA Type: ESP Phase 2 DH Group: modp1024 Phase 2 Encryption: 3des Phase 2 Authentication: md5 Phase 2 SA Life Time(s): 3600 Preshared Key: password DPD Delay(s): 32 DPD Timeout(s): 122 DPD Action: hold		

Site B

Summary	Gateway To Gateway	Client To Gateway
Gateway To Gateway Add a New Tunnel		
Tunnel Name: Tunnel_1 Enable: <input checked="" type="checkbox"/> Authentication: Preshared Key		
Local Group Setup		
Local Security Gateway Type: IP Only Interface IP Address: E.F.G.H Next-hop Gateway IP: Group Subnet IP: 192.168.10.0 Group Subnet Mask: 255.255.255.0 Group Subnet Gateway:		
Remote Group Setup		
Remote Security Gateway Type: IP Only Gateway IP Address: A.B.C.D Next-hop Gateway IP: Group Subnet IP: 192.168.100.0 Group Subnet Mask: 255.255.255.0		
IPsec Setup		
Aggressive Mode: <input type="checkbox"/> Phase 1 DH Group: modp1024 Phase 1 Encryption: 3des Phase 1 Authentication: md5 Phase 1 SA Life Time(s): 28800 Perfect Forward Secrecy: <input type="checkbox"/> Phase 2 SA Type: ESP Phase 2 DH Group: modp1024 Phase 2 Encryption: 3des Phase 2 Authentication: md5 Phase 2 SA Life Time(s): 3600 Preshared Key: password DPD Delay(s): 32 DPD Timeout(s): 122 DPD Action: hold		

Must Match!

Step 4

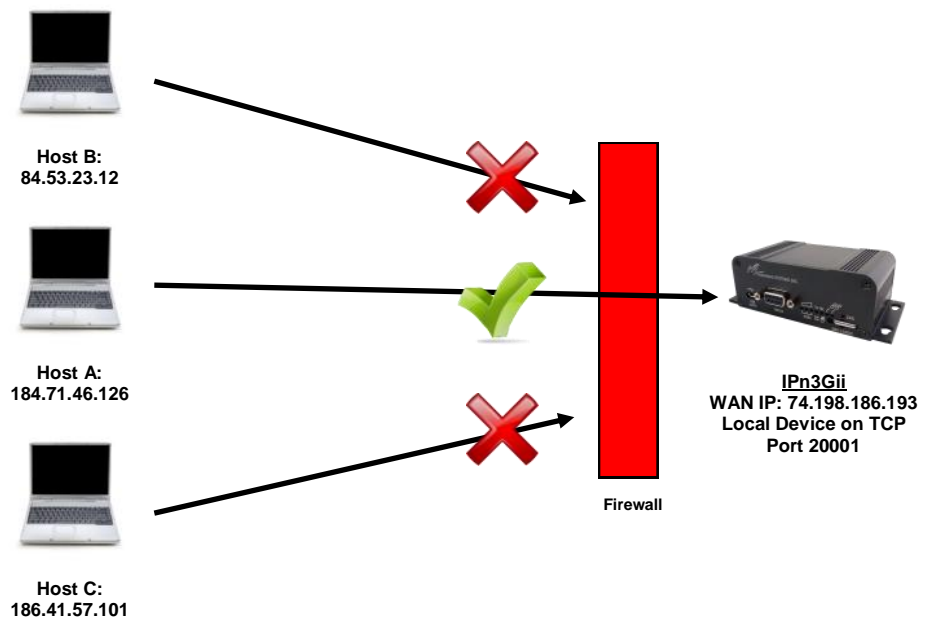
Submit changes to both units. It should be possible to ping and reach devices on either end of the VPN tunnel if both devices have been configured correctly and have network connectivity.

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 IPnXGii 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 IPnXGii 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 IPnXGii is paramount for a secure deployment. The firewall features of the IPnXGii allow a user to limit access to the IPnXGii 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 IPn3Gii 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 IPn3Gii and attached device, including the remote management features.



Step 1

Log into the IPn3Gii (Refer to Quick Start). Navigate to the Firewall > General tab as shown below and block all Carrier traffic by setting the **Carrier Request** to Block, and disable **Carrier Remote Management**. Be sure to Apply the settings. At this point it should be impossible to access the IPn3Gii from the Cellular Connection.



Appendix E: Firewall Example (Page 2 of 2)

Step 2

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

Rule 1

System Network Carrier Firewall VPN Serial USB I/O

Summary General Port Forwarding MAC-IP List Rules Firewall

Firewall Rules

Firewall Rules Configuration

Rule Name: Rem_Mgt

ACTION: Accept

Source: Carrier

Source IPs: 184.71.46.126 To 184.71.46.126

Destination: WAN

Destination IPs: 0.0.0.0 To 255.255.255.255

Destination Port: 80

Protocol: TCP

Add Rule

Rule 2

System Network Carrier Firewall VPN Serial USB I/O GP

Summary General Port Forwarding MAC-IP List Rules Firewall Default

Firewall Rules

Firewall Rules Configuration

Rule Name: Device

ACTION: Accept

Source: Carrier

Source IPs: 184.71.46.126 To 184.71.46.126

Destination: WAN

Destination IPs: 0.0.0.0 To 255.255.255.255

Destination Port: 20001

Protocol: TCP

Add Rule

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 IPn3Gii. The Firewall Rules Summary should look like what is shown below.

Name	Action	Src	Src IP From	Src IP To	Dest	Dest IP From	Dest IP To	Destination Port	Protocol	
Rem_Mgt	Accept	WAN	184.71.46.126	184.71.46.126	WAN	0.0.0.0	255.255.255.255	80	TCP	Remove Rule
Device	Accept	WAN	184.71.46.126	184.71.46.126	WAN	0.0.0.0	255.255.255.255	20001	TCP	Remove Rule

Step 3

Test the connections. The IPn3Gii should only allow connections to the port specified from the Host A. An alternate means to limit connections to the IPn3Gii 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 IPnXGii. The purpose of the section is to provide answers and/or direction on how to solve common problems with the IPnXGii.

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

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

Answer: The IPnXGii has two interfaces that are available for local configuration. The default IP address for the LAN (the RJ45 connector on the back of the unit) is 192.168.168.1. The default IP address for the USB (requires drivers to be installed), is 192.168.111.1.

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

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 IPnXGii?*

Answer: The APN is required to configure the IPnXGii 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 IPnXGii navigate to the System > Maintenance Tab. If you cannot log in, power on the IPnXGii and wait until the status LED is 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 IPnXGii 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 IPnXGii remotely, several methods can be used:

A. IP Passthrough - The IPnXGii is transparent and the connected device can be access directly. Refer to The IP-Passthrough Appendix for a detailed example of how this may be deployed.

B. Port Forwarding/DMZ - Individual external WAN ports are mapped to internal LAN IP's and Ports. See the Port-Forwarding Appendix for a detailed example.

C. VPN - A tunnel can be created and full access to remote devices can be obtained. Required the use of multiple modems or VPN routers. See the VPN Appendix on an example of how to set up a VPN.

Question: *I have Internet/Carrier access but I cannot ping the device remotely?*

Answer: Ensure that appropriates Rules have been created in the Firewall to allow traffic.

Question: *I'm using IP-Passthrough but the serial ports won't work?*

Answer: When using IP-Passthrough, the Carrier IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result serials port will not work. The only port not being passed through is the remote management port (default port 80), which can be changed in the security settings.

Question: *I'm using IP-Passthrough but the modem won't take my Firewall settings?*

Answer: When using IP-Passthrough, the Carrier IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. As a result the firewall settings have no effect on the unit, and is automatically disabled.

Question: *I cannot get IP-Passthrough to work?*

Answer: When using IP-Passthrough, the Carrier IP is assigned to the device connected to the Ethernet port, all traffic is passed through to that device. 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 IPnXGii that ensure that the unit is communicating at all times, and if a problem is detected will reboot the modem to attempt to resolve any issues:

1. Keepalive - Attempts to contact a configured host on a defined basis. Will reboot modem if host is unreachable. Enabled by default to attempt to ping 8.8.8.8. May need to disable on private networks, or provide a reachable address to check. Access via Carrier > Keepalive.
3. Local Device Monitor - The IPnXGii will monitor a local device, if that device is not present the IPnXGii may reboot. Network > LocalMonitor.

Question: *How do I set up VPN?*

Answer: Refer to the VPN Appendix for an example.



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

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