microhard SYSTEMS INC.

Operating Manual

pX2

1W OEM 802.11b/g/n Ethernet/Serial WIFI Router

Document: pX2 Operating Manual.v1.1.2.pdf
FW: v1.3.0 Build 1012

January 2016

microhard SYSTEMS INC.

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

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

Important User Information

Warranty

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

Warranty Disclaims

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

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

Indemnification

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

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

Proprietary Rights

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

Important User Information (continued)

About This Manual

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

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

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

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

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

Information
Information regarding a particular technology or concept.

Important User Information (continued)

Regulatory Requirements / Exigences Réglementaires

WARNING:

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23 cm 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 used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

WARNING:

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.

WARNING:

Changes or modifications not expressly approved by Microhard Systems Inc. could void the user's authority to operate the equipment. This device has been tested with UFL to Reverse Polarity SMA connectors with the antennas listed in Appendix A When integrated in OEM products, fixed antennas require installation preventing end-users from replacing them with non-approved antennas. Antennas not listed in the tables must be tested to comply with FCC Section 15.203 (unique antenna connectors) and Section 15.247 (emissions).

WARNING:

MAXIMUM EIRP

FCC Regulations allow up to 36 dBm equivalent isotropically radiated power (EIRP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed 36 dBm.

WARNING:

EQUIPMENT LABELING

The FCC and IC numbers depend on the model of the radio module. Do NOT use the Marketing Name of the product but the Model to distinguish the Certifications Numbers. This device has been modularly approved. The manufacturer, product name, and FCC and Industry Canada identifiers of this product must appear on the outside label of the end-user equipment.

WARNING:

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:
(1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE: px2

FCCID: NS915PX2
IC: 3143A-15PX2

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

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

Important User Information (continued)

Regulatory Requirements / Exigences Réglementaires

WARNING:

Pour satisfaire aux exigences de la FCC d'exposition RF pour la base et mobiles sur une distance de séparation de 23 cm ou plus doit être maintenue entre l'antenne de cet appareil et des personnes lors de fonctionnement du dispositif. Pour assurer la conformité des opérations au 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:

Son fonctionnement est soumis aux deux conditions suivantes : (1) ce dispositif ne doit pas causer d'interférences nuisibles et (2) cet appareil doit accepter toute interférence reçue, incluant les interférences qui peuvent provoquer un fonctionnement indésirable .

WARNING:

Les changements ou modifications non expressément approuvés par Microhard Systems Inc. pourraient annuler l'autorité de l'utilisateur à utiliser l'équipement . Ce dispositif a été testé avec MCX et connecteurs SMA à polarité inverse sur les antennes répertoriées à l'annexe A Lorsqu'il est intégré dans les produits OEM , antennes fixes nécessitent une installation empêchant les utilisateurs finaux de les remplacer par des antennes non approuvées . Antennes ne figurant pas dans les tableaux doivent être testés pour se conformer à la Section 15.203 (connecteurs d'antenne uniques) et à la Section 15.247 (émissions) .

WARNING:

MAXIMUM PIRE
Règlement FCC permettent jusqu'à 36 dBm puissance isotrope rayonnée équivalente (PIRE) . Par conséquent, la somme de la puissance émise (en dBm), la perte de câblage et le gain d'antenne ne peut pas dépasser 36 dBm.

WARNING:

ÉQUIPEMENT DE MARQUAGE
Les numéros FCC et IC dépendent du modèle du module radio . Ne pas utiliser le nom marketing du produit, mais le modèle de distinguer les numéros Certifications . Ce dispositif a été approuvé de façon modulaire . Le fabricant , nom du produit, et les identificateurs de la FCC et d'Industrie Canada de ce produit doivent figurer sur l'étiquette à l'extérieur de l'équipement de l'utilisateur final .

WARNING:

Cet appareil est conforme aux CNR exempts de licence d'Industrie Canada . Son fonctionnement est soumis aux deux conditions suivantes : (1) Ce dispositif ne peut causer des interférences ; et (2) Ce dispositif doit accepter toute interférence , y compris les interférences qui peuvent causer un mauvais fonctionnement de l'appareil.

SAMPLE LABEL REQUIREMENT / EXIGENCE D'ÉTIQUETTE: px2

FCCID: NS915PX2
IC: 3143A-15PX2

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

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

Important User Information (continued)

Regulatory Requirements / Exigences Réglementaires

Co-Location with Cellular Modems

The maximum calculated MPE ratio for the EUT with 2 dBi dipole antenna is 0.238, this configuration can be co-located with other antennas provided the sum of the MPE ratios for all the other simultaneous transmitting antennas incorporated in a host device is < 1.0 - 0.238 < 0.762. The following co-location were evaluated for mobile configurations:

1. EUT with 2 dBi dipole antenna co-located with Data Card Module (FCC ID RI7LN930, IC: 5131A-LN930)
2. EUT with 2 dBi dipole antenna co- located with LTE Data Transmitter Module (FCC ID R5Q-TOBYL100, IC 8595B-TOBYL100)
3. EUT with 2 dBi dipole antenna co- located with GSM/UMTS/LTE Data Module (FCC ID XPYTOBYL200, IC 8595A-TOBYL200)

Co - localisation avec Cellular Modem

Le maximum calculé rapport EMT pour l'EST avec antenne dipôle 2 dBi est de 0,238 , cette configuration peut être co-située avec d'autres antennes à condition que la somme des rapports MPE pour tous les autres antennes de transmission simultanées incorporés dans un dispositif hôte est < 1,0 à 0,238 < 0,762 . Le co- emplacement suivant ont été évalués pour les configurations mobiles :

1. EUT avec 2 dBi antenne dipôle co-localisé avec module de carte de données (FCC ID RI7LN930 , IC : 5131A - LN930)
2. EUT avec 2 dBi antenne dipôle co- localisé avec LTE données Module émetteur (FCC ID R5QTOBYL100 , IC 8595B - TOBYL100)
3. EUT avec 2 dBi antenne dipôle situé coopération avec les réseaux GSM / UMTS / LTE du module de données (FCC ID XPYTOBYL200 , IC - 8595A TOBYL200)

Revision History

Revision	Description	Initials	Date
0.0	Preliminary Release. Based on Firmware v1.0.0 Build 1003	PEH	July 2015
0.1	Added pX2 Development Board	PEH	Sept 2015
0.2	Added/Updated AT Commands as of firmware v1.3.0-r1007-13	PEH	Sept 2015
0.3	Updated Network Section	PEH	Oct 2015
0.31	AT Command Corrections	PEH	Oct 2015
1.0	Updated to firmware 1.3.0 Build 1010	PEH	Dec 2015
1.1	Updated Network > WAN, Firewall > Port forwarding Firewall > Rules. Updated AT Commands.	PEH	Dec 2015
1.1.1	Updated to firmware 1.3.0 Build 1011-60	PEH	Jan 2016
1.1.2	Updated to firmware 1.3.0 Build 1012	PEH	Jan 2016

Table of Contents

Table of Contents

Table of Contents

1.0 Overview

The pX2 is a feature rich, high power, OEM, 802.11 Ethernet/Serial WIFI Router. The pX2 is designed to provide high performance 802.11b/g/n WIFI capabilities in a compact and rugged OEM module for system integration. The PX2 features dual 10/100 Ethernet, Serial (RS232) Gateway and 802.11 WIFI capabilities for wireless applications

The pX2 can be configured using a built-in WebUI interface which does not require any additional software or tools to setup or download. The unit can operate as a Access Point, providing 802.11b/g/n WIFI to wireless devices. It can also operate in Station or Repeater modes to establish workstations and/or long range wireless links between locations.

Providing reliable wireless Ethernet bridge functionality as well gateway service for most equipment types which employ an RS232 interface, the pX2 can be used in various types of applications such as:

- High-speed backbone
- IP video surveillance
- Voice over IP (VoIP)
- Ethernet wireless extension
- Mobile Internet
- Legacy network/device migration
- SCADA (PLC's, Modbus, Hart)
- Display Signs
- Fleet Services

1.1 Performance Features

Key performance features of the pX2 include:

- High Power Tx (up to 1W) w/ Excellent Rx Sensitivity
- Up to 150 Mbps data rate
- Support for 802.11b/g/n Devices
- Firewall with ACL Security, Port Forwarding
- Full Scale Access Point, AP Station
- Multiple SSID Support
- Serial Gateway (RS232)
- Dual 10/100 Ethernet Ports
- RSSI LED pins for Antenna Alignments
- Industrial grade operating temperature (-40oC to +85oC)
- Administration via local console, telnet, web browser, SNMP
- Local and remote wireless firmware upgradable

1.0 Overview

1.2 Specifications

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

Electrical/General

Frequency:	2.4000 - 2.4835 GHz
Link Rate:	Up to 150 Mbps
Radio Operation	802.11b/g/n
TX Power:	11 dBm - 30 dBm (Selectable)
Channel Bandwidth:	20 or 40 MHz (Selectable)
Error Detection/Control:	ARQ/FEC
Data Encryption*:	WEP, WPA(PSK), WPA2(PSK), WPA+WPA2 (PSK) (May require an export permit)
Range:	Up to 10 miles (16km) (Antenna Dependant)
Serial Port:	300bps to 921kbps - RS232 (Tx, Rx, RTS, CTS, DTR, DSR)
Ethernet:	Dual 10/100 BaseT, Auto - MDI/X, IEEE 802.3
Network Protocols:	TCP, UDP, TCP/IP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP (*May require an export permit)
Operating Modes:	Access Point, Client/Station, Repeater, Mesh Point
Management:	Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade
Diagnostics:	Status LED's, RSSI, remote diagnostics, SNR, TX/RX CCQ
Input Voltage:	Vcc: 3.3 VDC Nominal (+/- 0.3V) Vrf: 3.3 to 5.0 VDC (5V for 1W output)

Environmental

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

Mechanical

Dimensions:	1.05" (26.5mm) X 1.3" (33mm) X 0.13" (3.5mm)
Weight:	Approx. 5 grams
Connectors:	Antenna: UFL Data: 80 Pin SMT

1.0 Overview

1.3 Performance Specifications

Rate	Mode	Tx Power (Vpa=5V)	Receive
1 Mbps	802.11b	30 dBm	-97 dBm ±1 dB
2 Mbps	802.11b	30 dBm	-96 dBm ±1 dB
5.5 Mbps	802.11b	30 dBm	-95 dBm ±1 dB
11 Mbps	802.11b	30 dBm	-92 dBm ±1 dB
6 Mbps	802.11g	30 dBm	-94 dBm ±1 dB
9 Mbps	802.11g	30 dBm	-93 dBm ±1 dB
12 Mbps	802.11g	30 dBm	-91 dBm ±1 dB
18 Mbps	802.11g	30 dBm	-90 dBm ±1 dB
24 Mbps	802.11g	28 dBm	-86 dBm ±1 dB
36 Mbps	802.11g	28 dBm	-83 dBm ±1 dB
48 Mbps	802.11g	26 dBm	-77 dBm ±1 dB
54 Mbps	802.11g	26 dBm	-75 dBm ±1 dB
MCS0	802.11n (HT20)	30 dBm	-96 dBm ±1 dB
MCS1	802.11n (HT20)	30 dBm	-95 dBm ±1 dB
MCS2	802.11n (HT20)	30 dBm	-92 dBm ±1 dB
MCS3	802.11n (HT20)	28 dBm	-90 dBm ±1 dB
MCS4	802.11n (HT20)	28 dBm	-86 dBm ±1 dB
MCS5	802.11n (HT20)	26 dBm	-83 dBm ±1 dB
MCS6	802.11n (HT20)	26 dBm	-77 dBm ±1 dB
MCS7	802.11n (HT20)	26 dBm	-75 dBm ±1 dB
MCS0	802.11n (HT40)	30 dBm	-94 dBm ±1 dB
MCS1	802.11n (HT40)	30 dBm	-93 dBm ±1 dB
MCS2	802.11n (HT40)	30 dBm	-90 dBm ±1 dB
MCS3	802.11n (HT40)	28 dBm	-89 dBm ±1 dB
MCS4	802.11n (HT40)	28 dBm	-84 dBm ±1 dB
MCS5	802.11n (HT40)	26 dBm	-81 dBm ±1 dB
MCS6	802.11n (HT40)	26 dBm	-75 dBm ±1 dB
MCS7	802.11n (HT40)	26 dBm	-73 dBm ±1 dB

Table 1-1: pX2 Performance Specifications

2.0 Quick Start

This QUICK START guide will walk you through the setup and configuration of a few basic applications. The QUICK START will rely on the *WebUI* for configuration. This walkthrough also assumes the units used are installed in microhard interface/ development boards or custom boards that allow access to the LAN port. See the appropriate section for pin-outs.

Note that the units arrive from the factory with a Radio Configuration of 'Access Point' and the Local Network setting configured as 'Static' (IP Address **192.168.168.1**, Subnet Mask 255.255.255.0). DHCP is enabled by default, and will assign an IP to a connected device.

2.1 Getting Started

To reset to factory defaults, press and hold the CONFIG for 8 seconds with the pX2 powered up. The pX2 will reboot with factory default settings.

- ✓ Connect an appropriate Antenna to the ***ANTENNA*** connector of the pX2.
- ✓ Connect and/or apply a suitable power source to the unit.
- ✓ Connect A PC to the ***LAN*** port (eth0) of the pX2, using an Ethernet Cable.
- ✓ The PC must have its Network Setting (TCP/IP Properties) set to DHCP (The modem will assign a IP address to you), or STATIC with an IP Address of (e.g.) 192.168.168.10 and a Subnet Mask of 255.255.255.0.

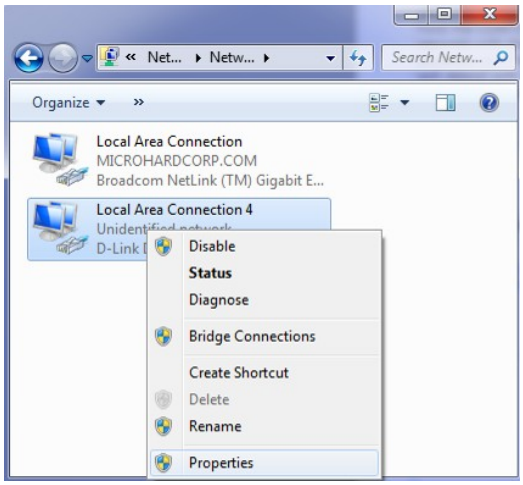
The factory default network settings:

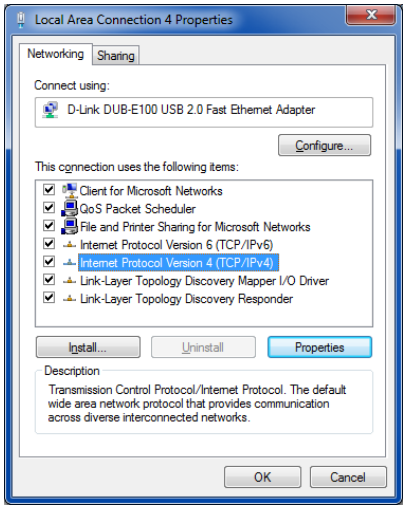
IP: 192.168.168.1
Subnet: 255.255.255.0

To set a Static IP, in ***Windows 7*** the TCP/ IP Properties can be found in:

Start > Search Bar "Network and Sharing Center"

Select *"Change Adapter Settings" on the left menu, and the right click the* Ethernet adapter connected to the pX2.





Select ***Internet Protocol (TCP/IPv4)*** and then ***Properties.***

2.0 Quick Start

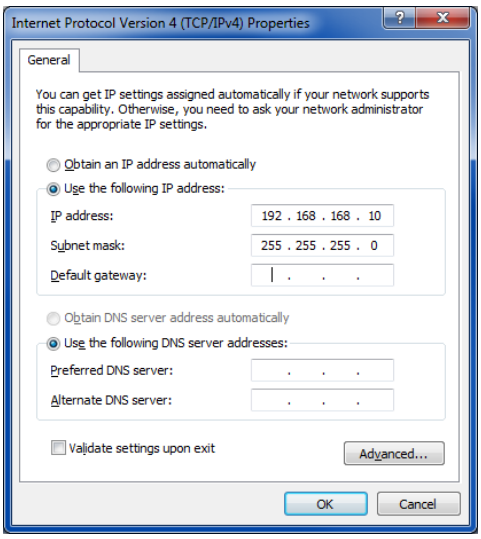
The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0

Select ***Use the following IP address*** and enter the values below as shown:

IP Address: 192.168.168.10
Subnet Mask: 255.255.255.0

Click ***OK***

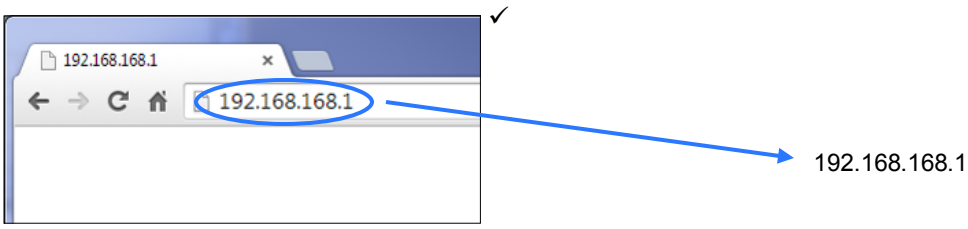


The factory default login:

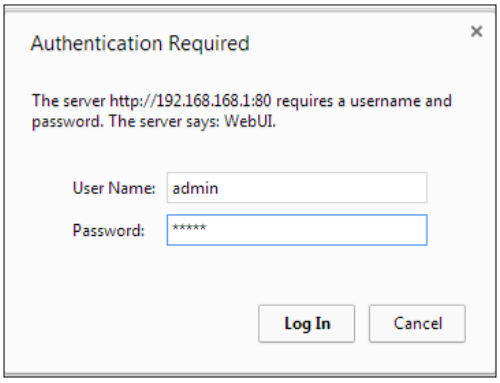
User name: admin
Subnet: admin

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

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



✓ The pX2 will then ask for a Username and Password. Enter the factory defaults listed below.



The Factory default login:

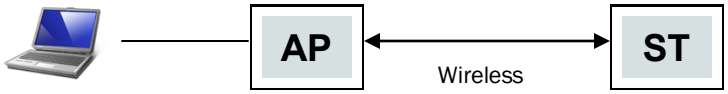
User name: **admin**
Password: **admin**

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

2.0 Quick Start

2.2 Simple Access Point and Station/Client

This **Quick Start** example requires (2) pX2 modules, one will be configured as a Access Point (AP), the second unit will be configured as a Station/Client (ST). This example will show the basic steps required to set up each unit so that a simple network will be established.



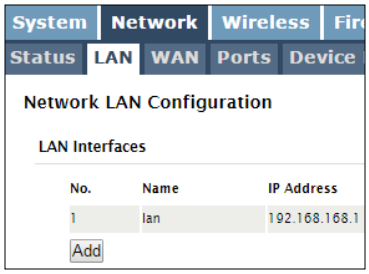
2.2.1 Configuring the Access Point

✓ Use ***Section 2.1*** *Getting Started* to connect, power up and log in to a pX2 unit.

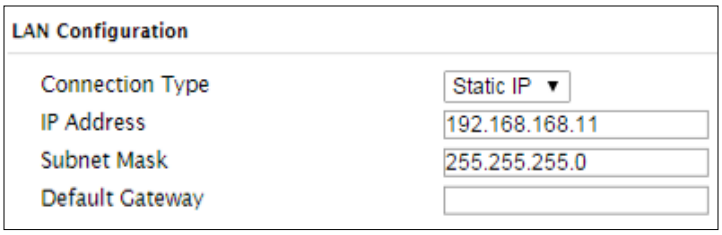
✓ Give the pX2 unit a unique IP address.

Select ***Network*** from the top/main navigation.

Select ***LAN*** from the submenu list, and then select *Edit.*



To connect to an existing network, contact your Network Administrator for valid network settings.



Choose *Static IP* for the ***Connection Type***.

Enter the following Network Information:

IP Address: 192.168.168.11
IP Subnet Mask: 255.255.255.0

Click on the **Submit** button to write the changes to the pX2. The **Cancel** button will revert back to last values saved to the unit.

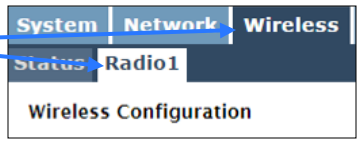
Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.

2.0 Quick Start

2.2.1 Configuring the Access Point (Con't)

✓ Configure the pX2 as an Access Point

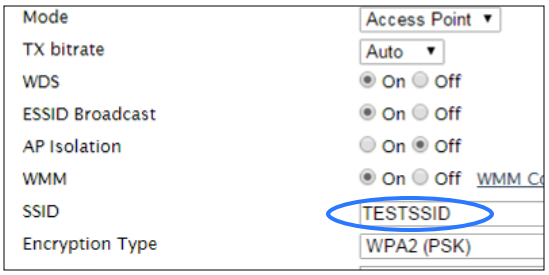
Select ***Wireless*** from the top/main navigation, and then *Radio1* from the sub-menu list.

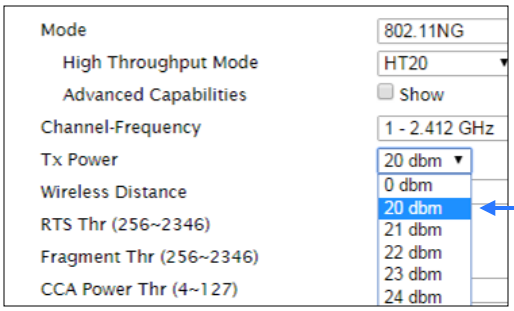


In the Radio1 Virtual Interface section, select Access Point from the ***Mode*** dropdown box.

Enter a unique ***SSID*** as shown.

TESTSSID



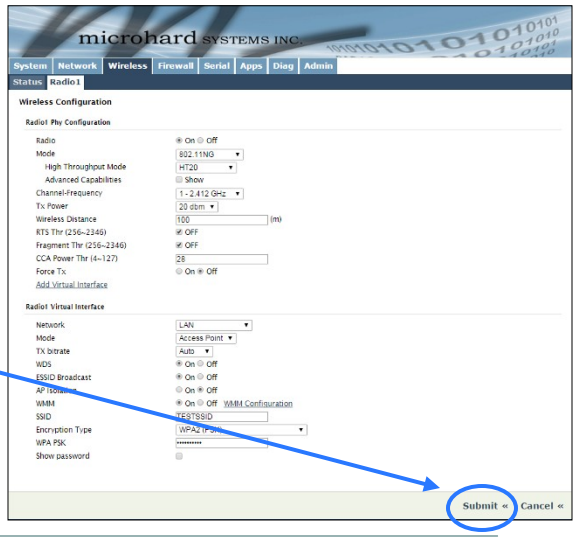


For bench or close proximity testing it is best to use a lower power setting to prevent RF saturation. Select 20dBm from the ***TX Power*** setting.

If any additional settings need to be changed, ensure they are also changed on the Station.

The remaining settings in the ***Wireless*** menu should be left as defaults for this exercise.

Click on the **Submit** button to write the changes to the pX2. The **Cancel** button will revert back to previously saved values.



2.0 Quick Start

2.2.2 Configuring the Station/Client

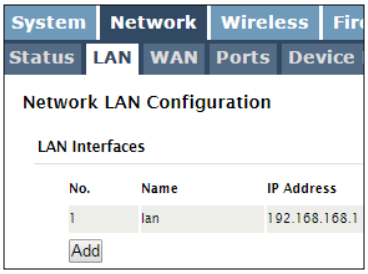
The following procedure describes the steps required to set up a pX2 unit as a Station/Client (ST). A Station provides a single wireless connection (i.e to an Access Point) and provides a wired connection to a PC or other devices.

✓ Use ***Section 2.1*** *Getting Started* to connect, power up and log in to a second pX2 unit.

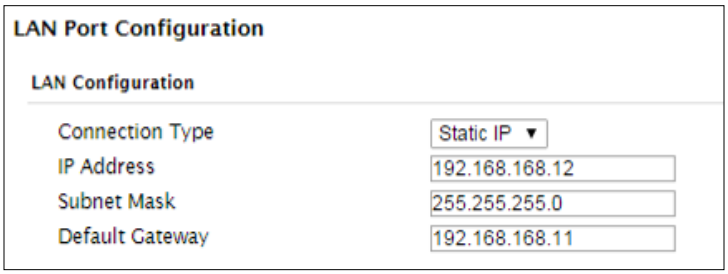
✓ Give the pX2 a unique IP address.

Select ***Network*** from the top/main navigation.

Select ***LAN*** from the submenu list, and then select *Edit*.



To connect to an existing network, contact your Network Administrator for valid network settings.



Choose *Static IP* for the ***Connection Type***.

Enter the following Network Information:

IP Address: 192.168.168.12
IP Subnet Mask: 255.255.255.0
Default Gateway: 192.168.168.11

Click on the **Submit** button to write the changes to the pX2. The **Reset** button will revert back to last values saved to the unit.

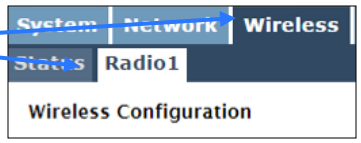
Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.

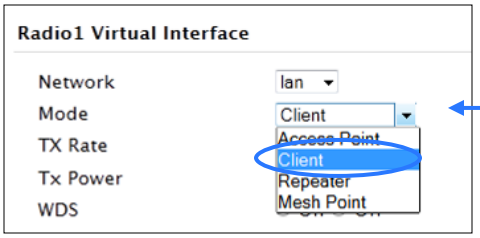
2.0 Quick Start

2.2.2 Configuring the Station/Client (Continued)

✓ Configure the pX2 as a Station/Client.

Select ***Wireless*** from the top/main navigation, and then *Radio1* from the sub-menu list.

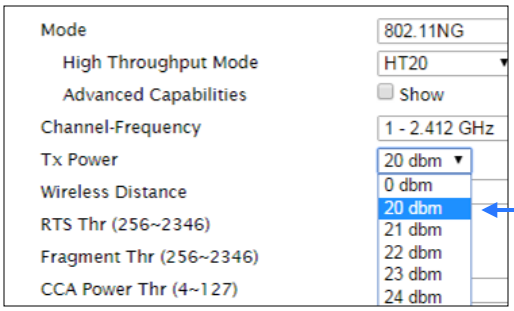




In the Radio1 Virtual Interface section, select Client from the ***Mode*** dropdown box.

Enter a unique ***Network Name(SSID)*** as shown.

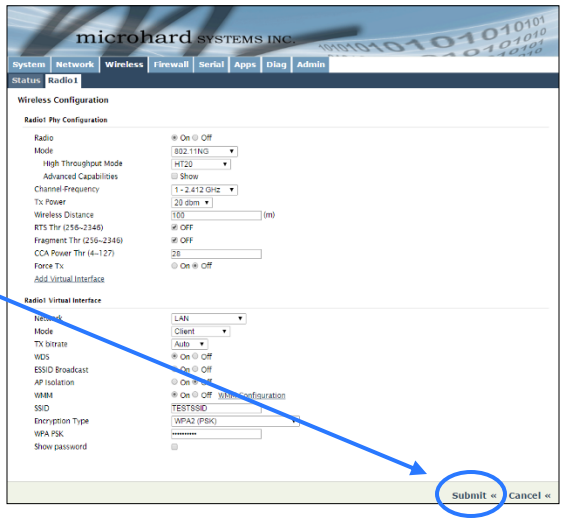
TESTSSID



For bench or close proximity testing it is best to use a lower power setting to prevent RF saturation. Select 20dBm from the ***TX Power*** setting.

The remaining settings in the ***Wireless*** menu should be left as defaults for this exercise.

Click on the **Submit** button to write the changes to the pX2. The **Cancel** button will revert back to previously saved values



If any additional settings need to be changed, ensure they are also changed on the Station.

2.0 Quick Start

2.2.3 Testing the Connection

✓ Visually check to see if the pX2 units are communicating.

RSSI LED's that are 'cycling' or 'scanning' indicate that the unit is searching for a signal.

The ***RSSI*** LED's represent signal strength, the more LED's that are illuminated, the stronger the signal. The ***Wireless > Status*** window also has a Connection Status section as seen below:

Radio 1 Status

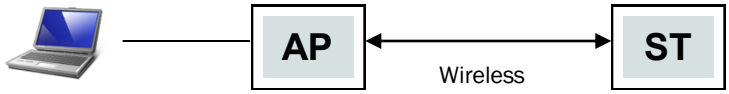
General Status

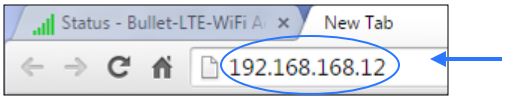
MAC Address	Mode	SSID	Radio Frequency	Security mode
00:0F:92:FA:01:12	Station	TESTSSID	2.462	None

Connection Status

MAC Address	Noise Floor (dBm)	SNR (dB)	RSSI (dBm)	TX CCQ (%)	RX CCQ (%)	TX Rate	RX Rate	Signal Level
00:0f:92:fa:01:11	-101	33	-62	93	98	48.0 MBit/s	48.0 MBit/s	100%

✓ With the PC connected to the Access Point (AP), type in the IP address of the Station (ST) into the URL address bar of your browser. You should be able to connect, log in and view the WebUI of the Station via the wireless connection.





Open a browser and type in the address of the station/client: ***192.168.168.12***

Log into the unit.

The System Summary screen should be displayed

If any additional settings need to be changed, ensure they are also changed on the Station/Client.

3.0 Hardware Features

3.1 pX2 OEM Module

The pX2 modems are available as a low cost OEM modules. This OEM version supplies all the required raw signals to allow the unit to be tightly integrated into applications to efficiently maximize space and power requirements. The Microhard development board can provide a convenient evaluation platform to test and design with the module. (Contact Microhard Systems for details)

Any pX2 module may be configured as a Access Point (AP), AP Station, or Repeater. This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming familiar and proficient with using the module: if you are familiar with one unit, you will be familiar with all units.

Image 3-1: pX2 Top View

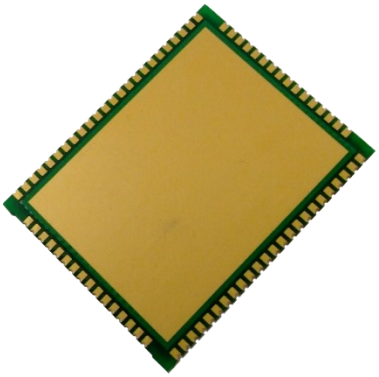
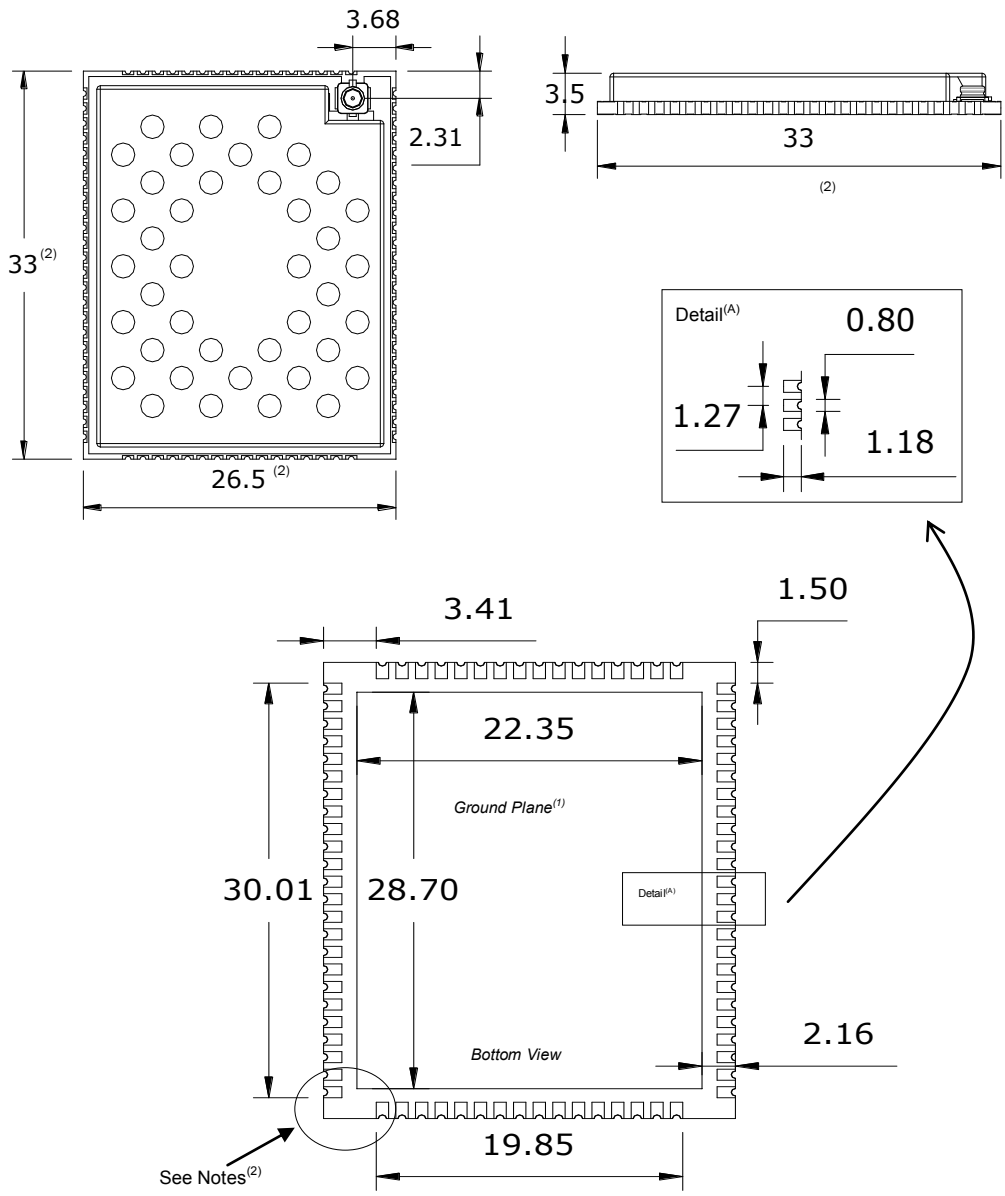


Image 3-2: pX2 Bottom View

3.0 Hardware Features

3.1.1 Mechanical Drawings

The pX2 OEM Modules have an extremely small form factor as seen *below*.



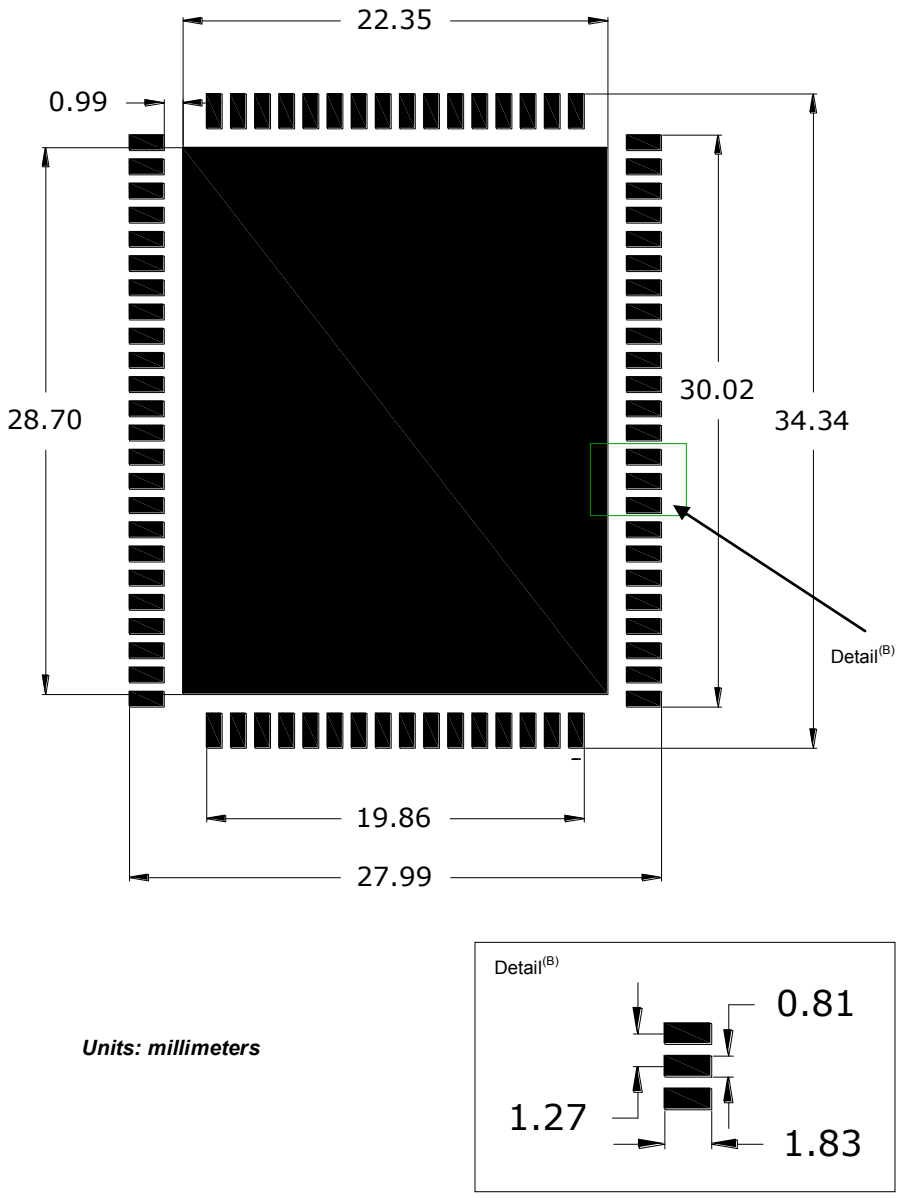
Units: millimeters

1. Ground plane must be connected to GND for required heat dissipation.
2. Due to manufacturing methods additional PCB material may be present on the corners that cannot be removed. Designs should allow for a small tolerance of this additional material, ± 0.25mm

Drawing 3-1: pX2 OEM Mechanical

3.0 Hardware Features

3.1.2 Recommended Solder Mask (Pad Landing)

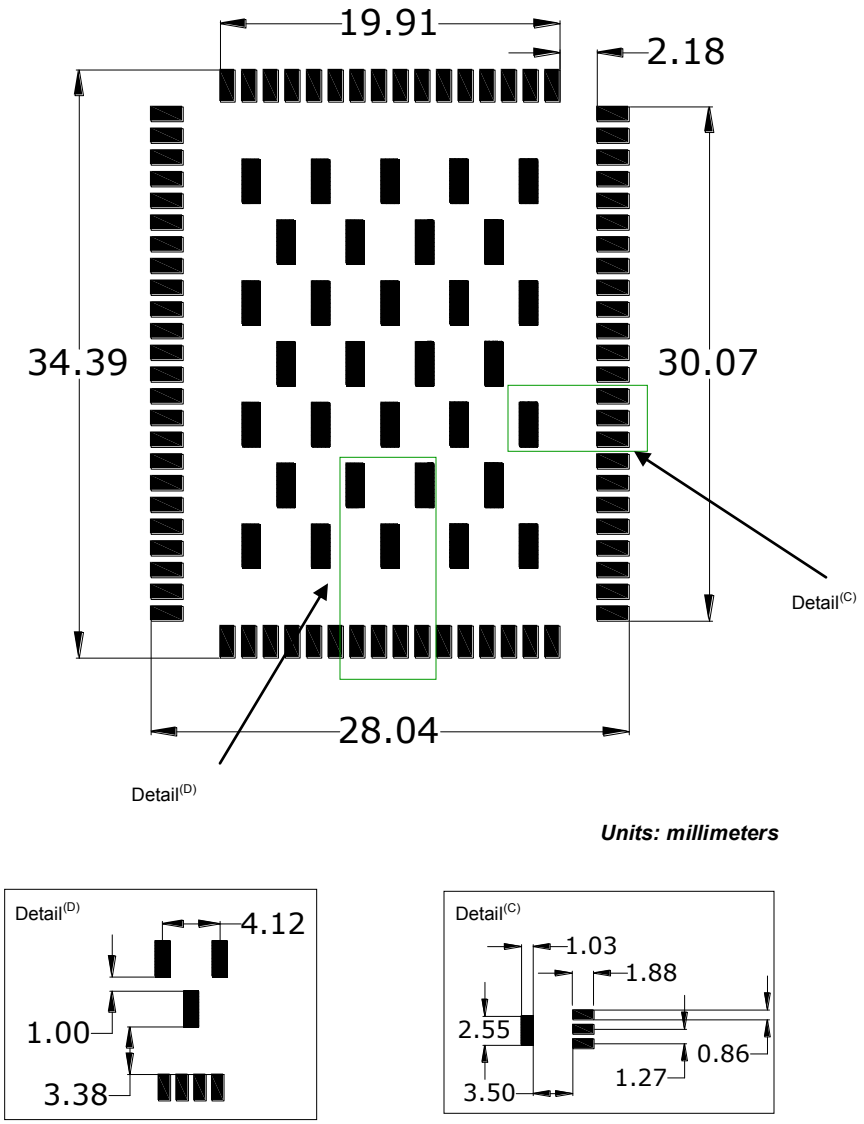


Units: millimeters

Drawing 3-2: pX2 Recommended Solder Mask

3.0 Hardware Features

3.1.3 Recommended Solder Paste Pattern



Drawing 3-3: pX2 Recommended Solder Paste

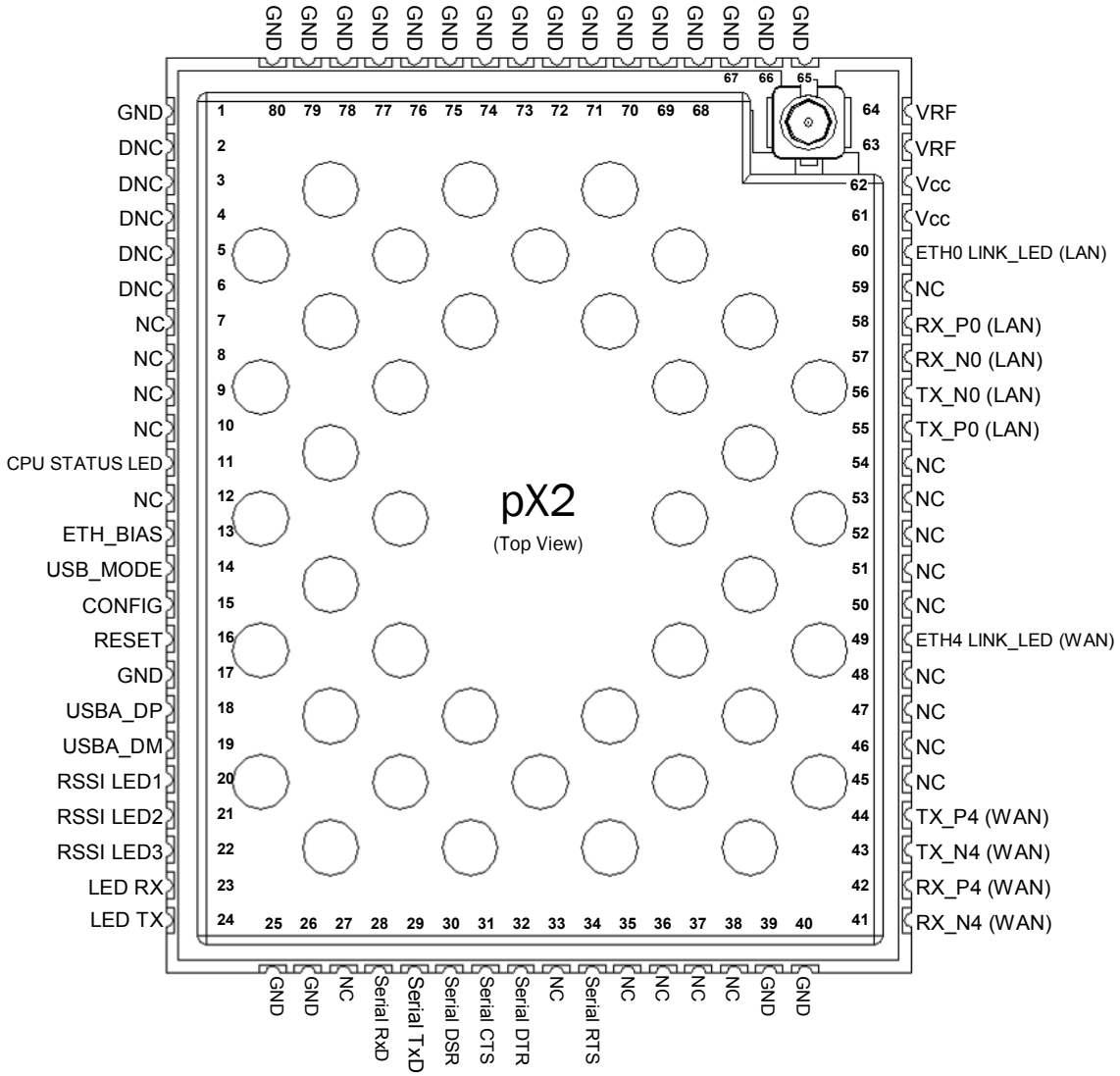
3.1.4 OEM Connectors

Antenna
All pX2 OEM Modules use an UFL connector for the antenna connection.

Data
The interface to the pX2 OEM module is a tight integration using 80 pad SMT connections.

3.0 Hardware Features

3.1.5 Pico OEM Pin Descriptions



Drawing 3-4: pX2 80-pin OEM Connection Info

Inputs and outputs are 3.3V nominal (3.0V min — 3.6V max) unless otherwise specified.

The above drawing depicts a top view of the pX2 OEM Module. The corner pads (1, 25, 41, and 65) are printed directly on the bottom of the PCB for easy identification.

A full description of the connections and function of each pin is provided on the pages that follow.

3.0 Hardware Features

Caution: During power up or reset, output pins from the Pico are in an unknown state. It is advised to use pull up or pull down resisters as appropriate.

Pin Name	No.	Description	Dir
GND	*1,17,25-26,39-40,65-80*	Ground reference for logic, radio, and I/O pins.	
DNC	2,3,4,5,6	Reserved for factory use only.	
NC	7,8,9,10,12,27, 33,35,36,37,38, 45,46,47,48,50, 51,52,53,54,59	**Currently Not Supported. For Future Expansion**	
CPU STATUS LED	11	Active high output indicates CPU/Module status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
ETH_BIAS	13	Bias Voltage to Ethernet PHY transformer	
USB_MODE	14	Indicates if the interface is in host/device mode. 0 = Device, 1 = Host.	I
Config	15	Active low. In normal mode, pull it low and hold for more than 8 seconds will reset the system to default settings. Pull it low upon power up will put the module into recovery mode.	I
RESET	16	Active low input will reset module	I
USBDP	18	USB D- signal; carries USB data to and from the USB 2.0 PHY	
USBDM	19	USB D+ signal; carries USB data to and from the USB 2.0 PHY	
LED_1 (RSSI1)	20	Receive Signal Strength Indicator 1. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_2 (RSSI2)	21	Receive Signal Strength Indicator 2. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_3 (RSSI3)	*22*	Receive Signal Strength Indicator 3. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	*O*
LED_RX	23	Active high output indicates receive and synchronization status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
LED_TX	24	Active high output indicates module is transmitting data over the RF channel. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
Serial RxD	28	Receive Data. Logic level input into the modem. It is recommended to wire this pin out through a zero ohm resister to a header and jumper block for external access to the serial port for modem recovery procedures.	I
Serial TxD	29	Transmit Data. Logic level Output from the modem. It is recommended to wire this pin out through a zero ohm resister to a header and jumper block for external access to the serial port for modem recovery procedures.	O
Serial DSR	30	Data Set Ready. Active low output. *The DSR line set high enables the transmitter of the RS485 driver.*	O
Serial CTS	31	Clear To Send. Active low output.	O
Serial DTR	32	Data Terminal Ready. Active Low output.	O
Serial RTS	34	Request To Send. Active low input.	I

Table 3-1: pX2 Pin Description

All serial communications signals are logic level (0 and 3.3V). DO NOT connect RS-232 level (+12, -12VDC) signals to these lines without shifting the signals to logic levels.

3.0 Hardware Features

Pin Name	No.	Description	Dir
RX_N4	41	Ethernet Port 4 (WAN) Receive Pair	
RX_P4	42		
TX_N4	43	Ethernet Port 4 (WAN) Transmit Pair	
TX_P4	44		
ETH4 LINK_LED	49	Active high output indicates Ethernet port 4 link status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
TX_P0	55	Ethernet Port 0 (LAN) Transmit Pair	
TX_N0	56		
RX_N0	57	Ethernet Port 0 (LAN) Receive Pair	
RX_P0	58		
ETH0 LINK_LED	60	Active high output indicates Ethernet port 0 link status. Active high, cannot drive LED directly. Requires current limiting resistor. 8mA maximum.	O
Vdd	61,62	Positive voltage supply voltage for the digital section of the module (3.3V).	I
Vpa	63,64	Positive voltage supply voltage for the radio module (3.3-5V).	I

Table 3-1: pX2 Pin Description (continued)

Caution: During power up or reset, output pins from the Pico are in an unknown state. It is advised to use pull up or pull down resisters as appropriate.

All serial communications signals are logic level (0 and 3.3V). DO NOT connect RS-232 level (+12, -12VDC) signals to these lines without shifting the signals to logic levels.

See ***Appendix D: Sample Interface Schematic*** for a sample schematic that can be used to interface to the pX2 OEM module.

3.0 Hardware Features

3.2 pX2 Development Board

The pX2 Development board provides a platform in which to test and evaluate the operation of the pX2 without the need to design a custom interface PCB right from the start. The pX2 includes a socket to insert the pX2 and provides standard interfaces/indicators for:

- Ethernet
- RS232 Serial Port
- USB Port (Not currently supported)
- Power (9-30 VDC)
- CPU Status LED
- Tx/Rx LED's
- RSSI (x3) LED's
- Config Button (Reset/Recovery Operations)
- Vpa (3/5V) Jumper Block

Image 3-3: pX2 Development Board

3.0 Hardware Features

3.2.1 pX2 Development Board Connectors & Indicators

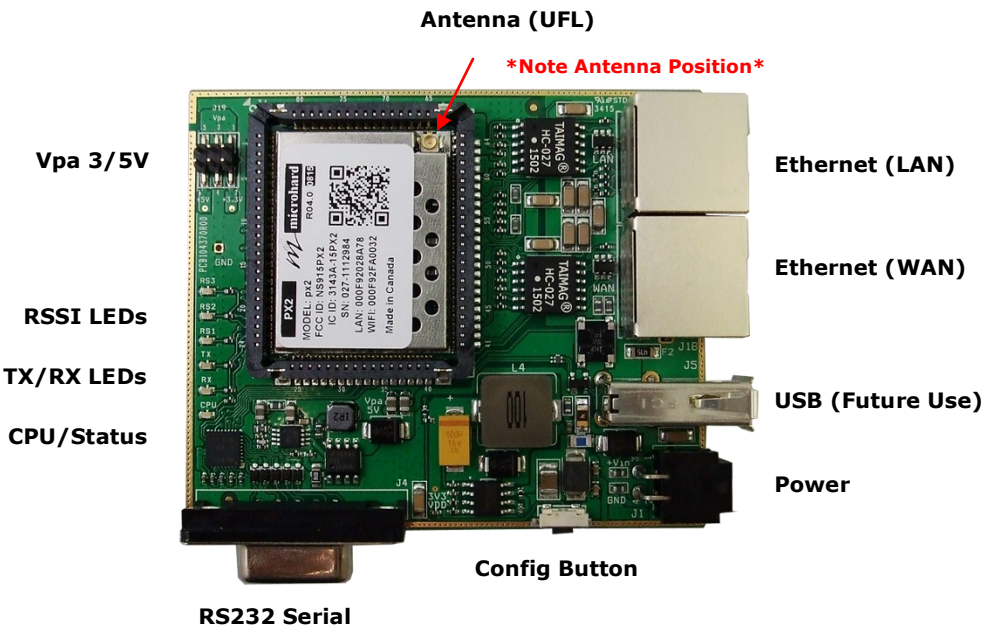


Figure 3-1: pX2 Development Board

Antenna:

The pX2 OEM module uses a UFL connector, Ensure proper orientation as seen above to prevent damage to the pX2 module and to the development board.

Ethernet LAN:

The Ethernet LAN port is a standard RJ45 port to connect local network devices. The default IP address for this port is *192.168.168.1*.

Ethernet WAN:

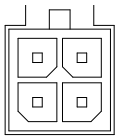
The Ethernet WAN port is a standard RJ45 Port that can be used as a separate WAN port for Router functions, or can be bridged (via software) to the LAN as a additional switch port for local devices.

The pX2 development board can be powered using Passive PoE on the WAN port using a PoE injector that meets the following requirements:

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-

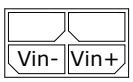
Table 3-2: Ethernet (WAN) PoE Connections

Power



Power:

The pX2 development board can powered using an input voltage in the 9-30 VDC range.



3.0 Hardware Features

Config Button:

The Config button on the pX2 can be used to either reset the modem into its factory default configuration, or it can be used to perform a firmware recovery procedure.

Factory Default Settings: While power applied and the pX2 in an operational state, press and hold the *Config* Button for 8-10 seconds or until the module reboots. It will reboot with the factory default configuration settings.

Firmware Recovery: To load the firmware on the unit it is recommended to use the normal WebUI to perform a firmware update (Maintenance). In the event that the firmware cannot be loaded using the standard WebUI (non responsive unit), pressing and holding the *Config* Button while powering-up the module will force the pX2 into a firmware recovery mode. There are 3 main modes, HTTP, TFTP and Master Reset. The table below shows the time required to hold the *Config* button while power is applied:

0 to 5 seconds HTTP Recovery	5 to 10 seconds TFTP Recovery	10 to 15 seconds Master Reset	15+ seconds No Effect

HTTP Recovery: Set an IP on a PC to 192.168.1.1. Open a web browser and Navigate to 192.168.1.39. This will open a simple webpage which will allow a firmware file to be loaded.

TFTP Recovery: Set an IP on a PC to 192.168.1.1. Use a TFTP session to push the firmware file to the modems recovery IP of 192.168.1.39. See Appendix for Firmware Recovery Procedure.

Master Reset: Runs Master Reset, file system is erased.

RS232 Serial:

The RS232 Serial data port can be used to communicate with RS232 Serial devices or it can be configured to operate as a console port. See Table 3-3 for pin assignments.

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

Table 3-3: Data RS232 Pin Assignment

CPU/Status:

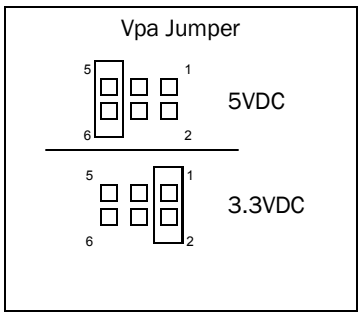
The CPU/Status LED indicates that power has been applied to the module. A Solid LED indicates normal operation, while flashing indicates boot or firmware upgrade status.

TX/RX LEDs:

The TX/RX LEDs indication wireless traffic to/from the pX2 module.

RSSI LEDs:

The RSSI LEDs indicate the Received Signal Strength on the Wireless Link. On a Access Point it will indicate an average RSSI value based on connected units. On a Client/Station the RSSI LEDs will represent the signal strength between the Station and the AP it is connected to. (The more LEDs illuminated, the stronger the signal)



Vpa 3/5V:

The Vpa jumper allows the radio inside the pX2 to be connected to 3.3 or 5VDC. For the pX2 to operate at maximum output Transmit (Tx) power of 1 Watt (30dBm), the Vpa jumper must be set to 5VDC (Pin 5+6).

4.0 Configuration

4.0 Web User Interface

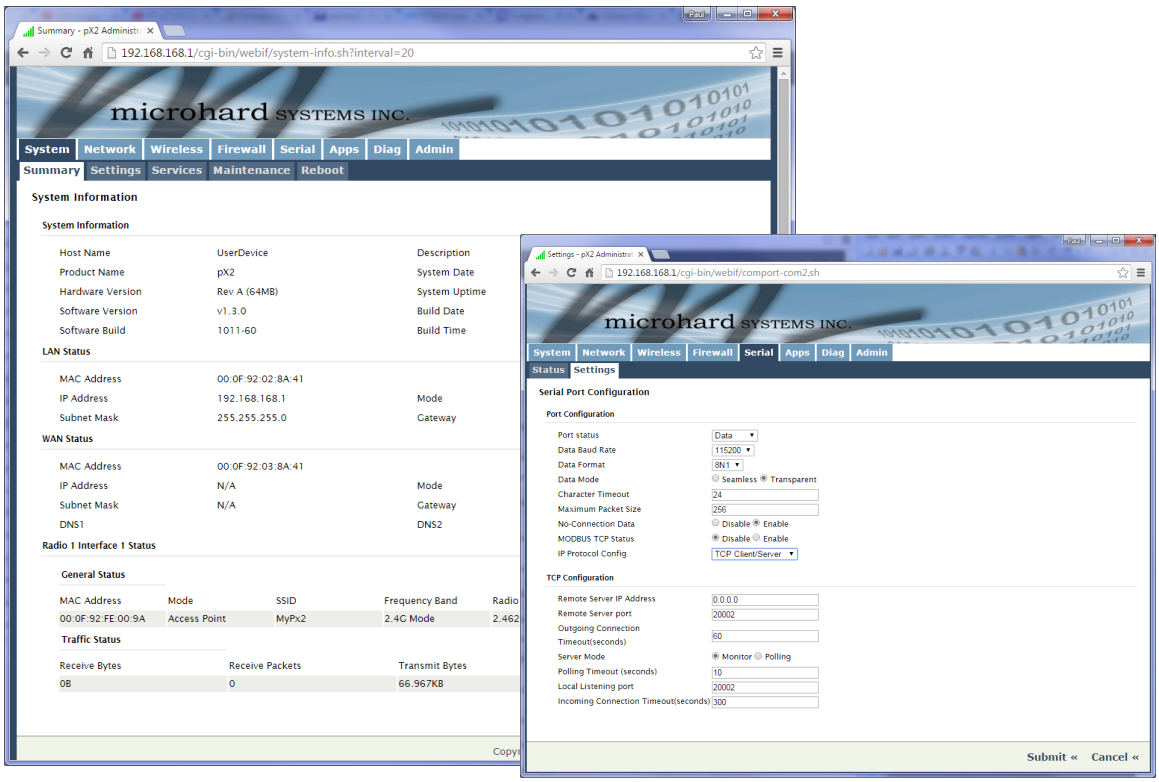


Image 4-0-1: WebUI

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

Initial configuration of an pX2 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 PX2 and it will be assigned a IP address automatically.
- connect the pX2 ETHERNET(LAN) port to PC NIC card using an Ethernet cable
- apply power to the pX2 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 pX2 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 pX2 using a Web Browser, the Logon window will appear.

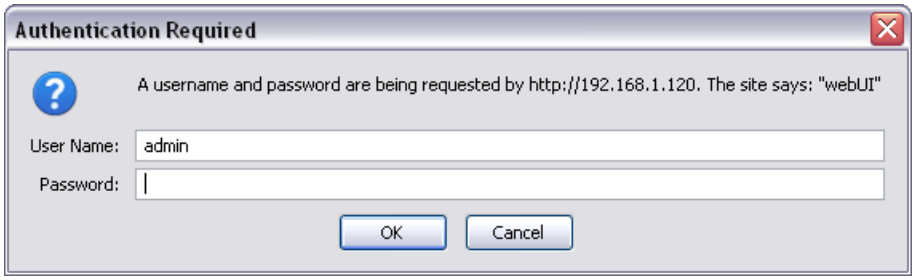


Image 4-0-2: Logon Window

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

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

The default password is: **admin**

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

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

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

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

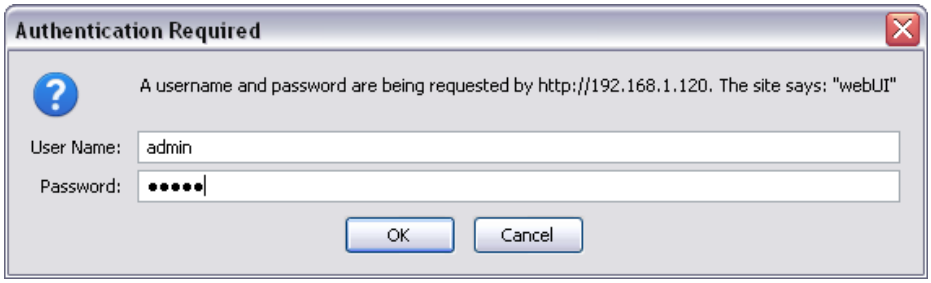


Image 4-0-3: Logon Window : Password Entry

4.0 Configuration

4.1 System

The main category tabs located at the top of the navigation bar separate the configuration of the pX2 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.
- 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 pX2 in a single display. This information includes System Status, Carrier Status, Cellular & LAN network information, version info, etc.

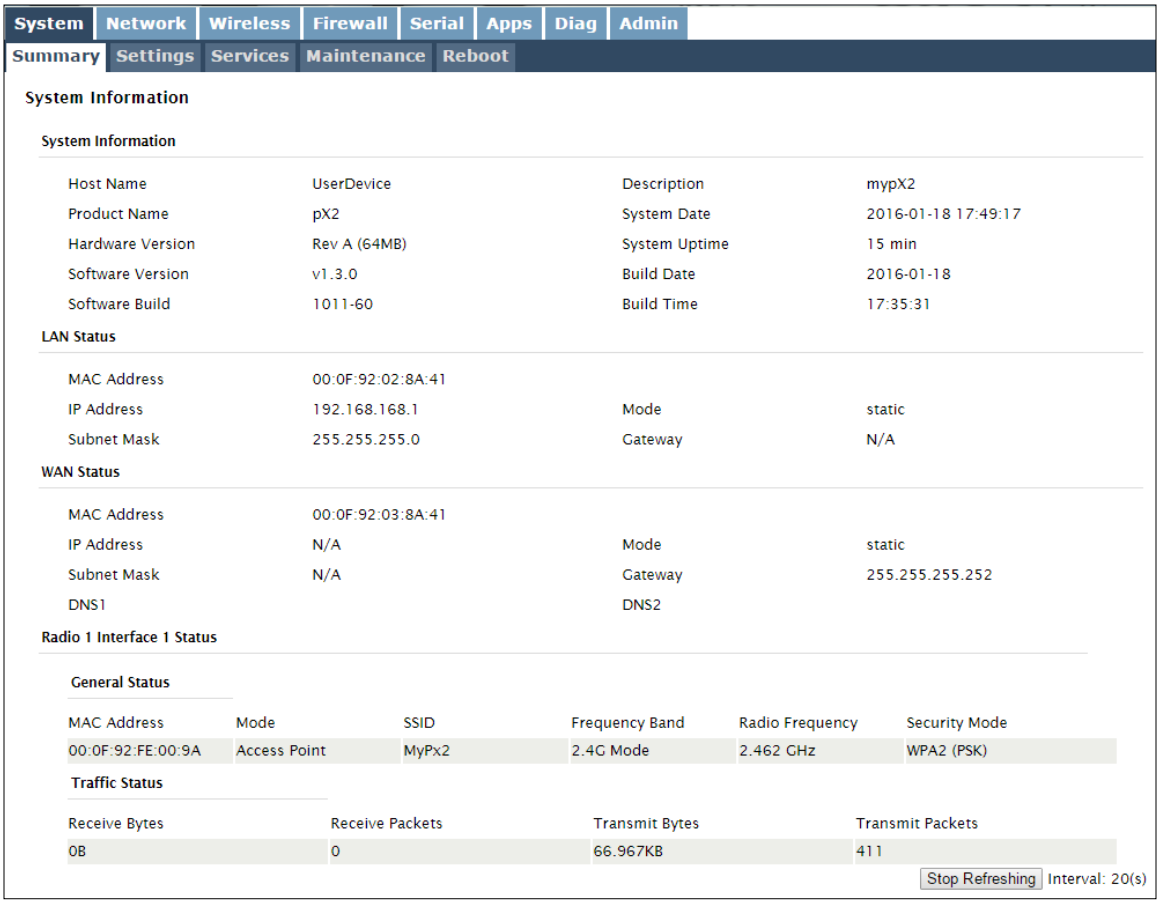


Image 4-1-1: System Summary Window

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, System Log server and System Time settings.

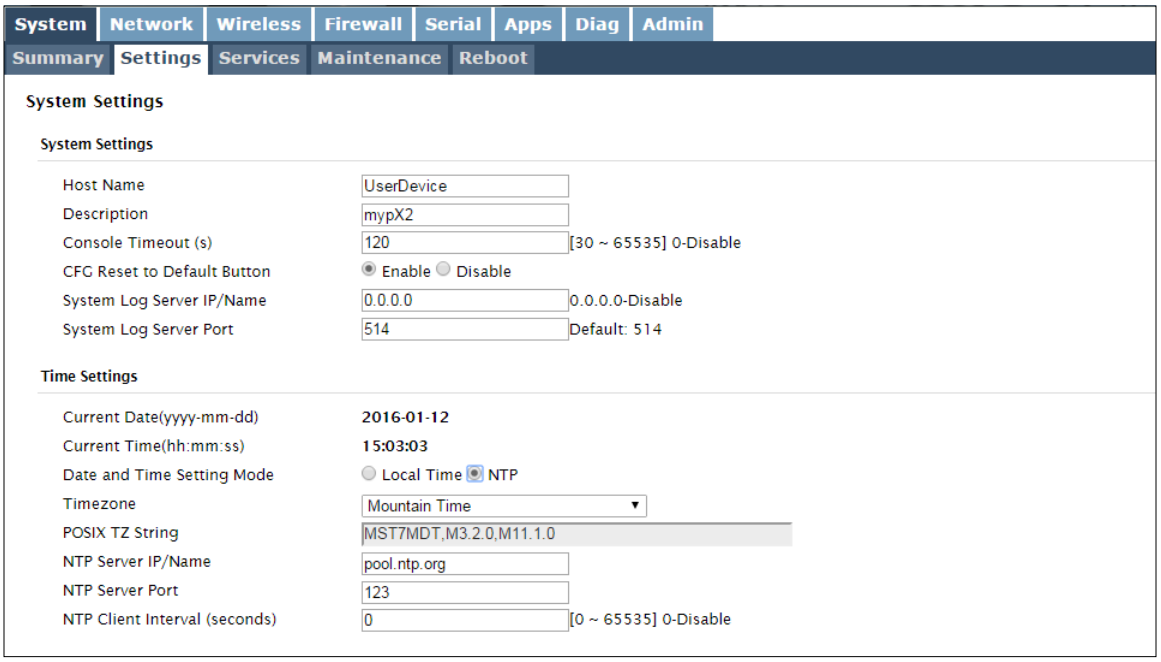


Image 4-1-2: System Settings > System Settings

Host Name

The Host Name is a convenient identifier for a specific pX2 unit. This feature is most used when accessing units remotely: a convenient cross-reference for the unit's WAN IP address. This name appears when logged into a telnet session.

Values (characters)

pX2 **(varies)**

up to 64 characters

Description

The description is a text field that can be used to describe the unit or system. This value can be viewed on the System > Summary screen.

Values (characters)

pX2 **(varies)**

up to 64 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

4.0 Configuration

CFG Reset to Default Button

Enabled by default, when the CFG button on the front of the pX2 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

System Log Server IP

The pX2 can report system level events to a third party System Log server, which can be used to monitor events reported by the PX2.

IP Address

0.0.0.0

System Log Server Port

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

UDP Port

514

Time Settings

The pX2 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.

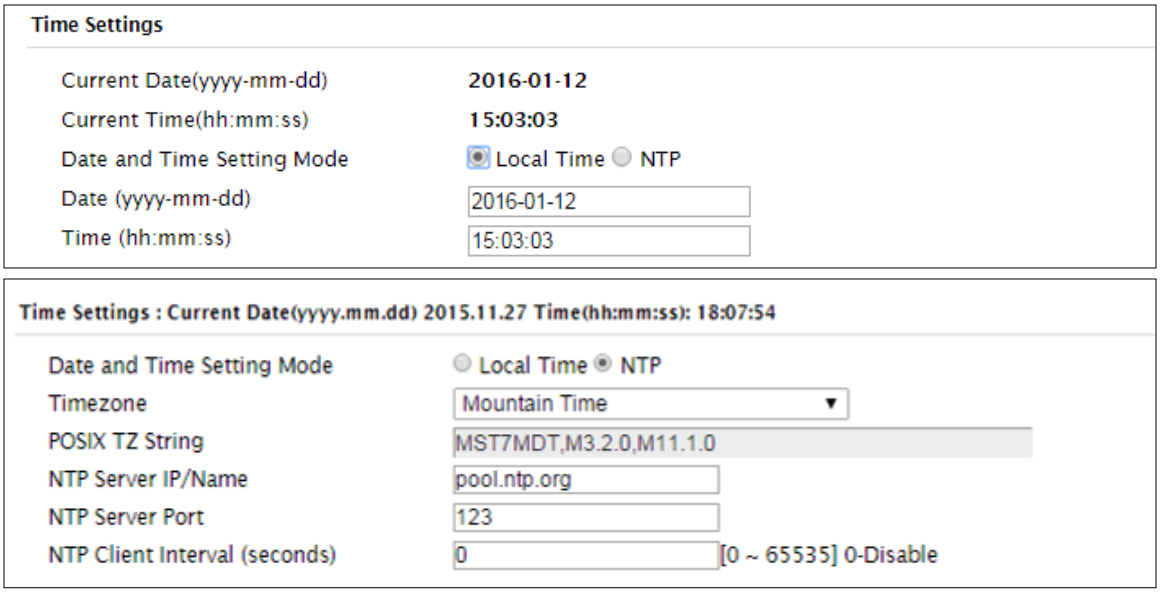


Image 4-1-3: System Settings > Time Settings

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.

Date and Time Setting Mode

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

Values (selection)

Local Time
NTP

4.0 Configuration

Date	
The calendar date may be entered in this field. Note that the entered value is lost should the pX2 lose power for some reason.	**Values (yyyy-mm-dd)** **2016-01-12** *(varies)*
Time	
The time may be entered in this field. Note that the entered value is lost should the pX2 lose power for some reason.	**Values (hh:mm:ss)** **11:27:28** *(varies)*
Timezone	
If connecting to a NTP time server, specify the time zone from the dropdown list.	**Values (selection)** *(varies)*
POSIX TZ String	
This displays the POSIX TZ String used by the unit as determined by the Timezone setting.	**Values (read only)** *(varies)*
NTP Server	
Enter the IP Address or domain name of the desired NTP time server.	**Values (address)** **pool.ntp.org**
NTP Port	
Enter the IP Address or domain name of the desired NTP time server.	**Values (port#)** **123**
NTP Client Interval	
By default the modem only synchronizes the time and date during system boot up (default: 0), but it can be modified to synchronize at a regular interval. *This process does consume data and should be set accordingly.*	**Values (seconds)** **0**

4.0 Configuration

4.1.3 System > Services

Certain services in the pX2 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.

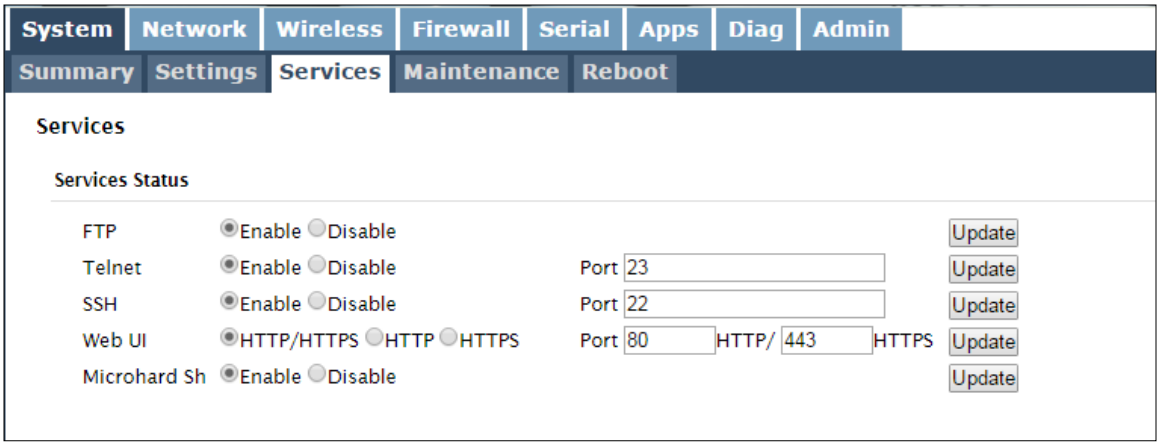


Image 4-1-4: System > Services

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 pX2. 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 pX2. The port used by the SSH service can also be modified. The default is 22.

Values (port)

22

Web UI

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

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

Values (selection)

HTTP/HTTPS
HTTP
HTTPS

Microhard Sh is reserved for internal use.

4.0 Configuration

4.1.4 System > Maintenance

Firmware Upgrade

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

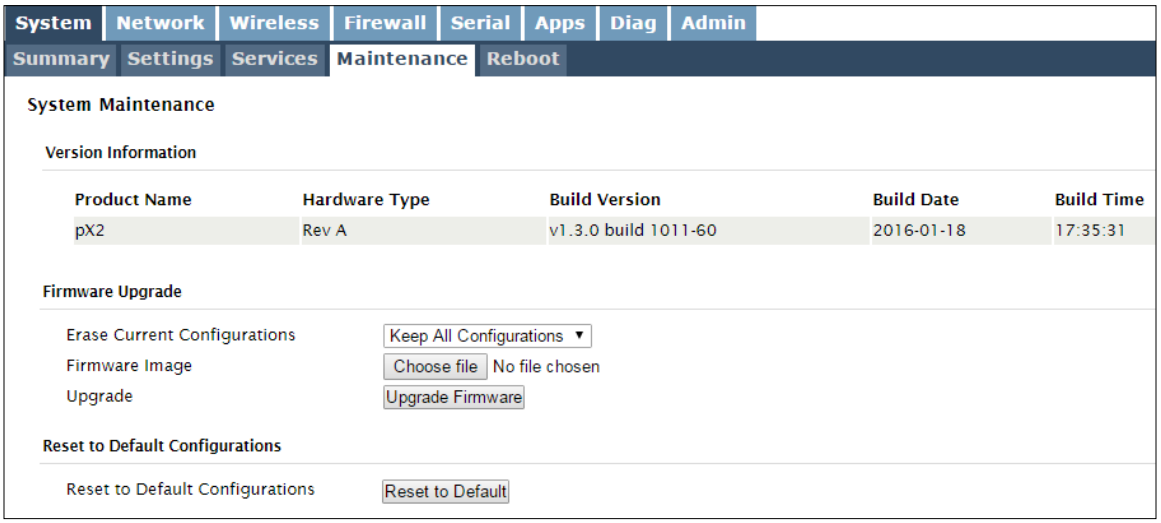


Image 4-1-5: Maintenance > Firmware Upgrade

Erase Current Configuration	Values (check box)
Choose to keep or erase the current configuration. Erasing the configuration of the pX2 unit during the upgrade process will upgrade, and return the unit to factory defaults, including the default IP Address and password.	**Keep ALL Configuration** Erase Configuration

Firmware Image	Values (file)
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.	*(no default)*

Reset to Default

The pX2 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 pX2 can be backed up to a file at any time using the Backup Configuration feature. The file can the be restored using the Restore Configuration feature. It is always a good idea to backup any configurations in case of unit replacement. The configuration files cannot be edited offline, they are used strictly to backup and restore units.

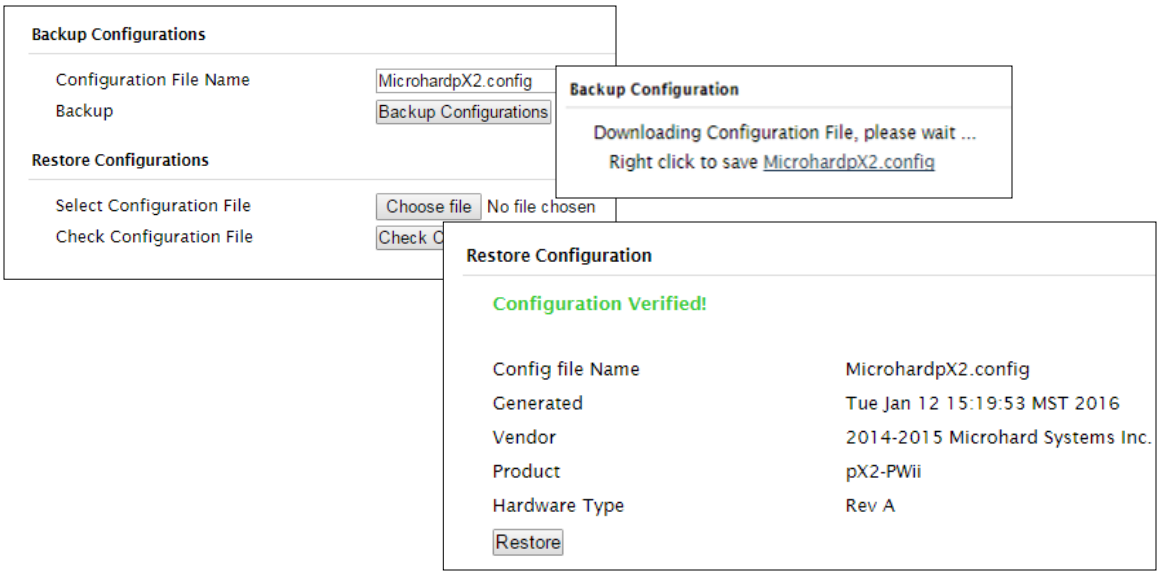


Image 4-1-6: Maintenance > Reset to Default / Backup & Restore Configuration

Configuration File Name / Backup

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

Select Configuration file / Check Configuration 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

4.1.5 System > Reboot

The pX2 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.

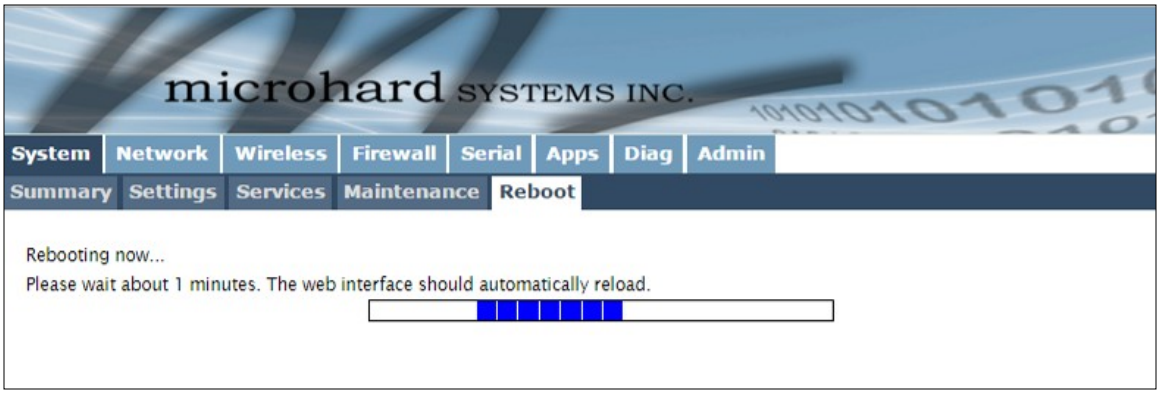


Image 4-1-7: System > Reboot

4.0 Configuration

4.2 Network

4.2.1 Network > Status

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 | Wireless | Firewall | Serial | Apps | Diag | Admin

Status | LAN | WAN | Ports | Device List

Network Status

LAN Port Status

General Status

IP Address	Connection Type	Subnet Mask	MAC Address
192.168.168.1	static	255.255.255.0	00:0F:92:02:8A:41

Traffic Status

Receive bytes	Receive packets	Transmit bytes	Transmit packets
577.029KB	5495	455.050KB	3723

WAN Port Status

General Status

IP Address	Connection Type	Subnet Mask	MAC Address
N/A	dhcp	N/A	00:0F:92:03:8A:41

Traffic Status

Receive bytes	Receive packets	Transmit bytes	Transmit packets
0B	0	0B	0

Default Gateway

Gateway None

DNS

DNS Server(s) None

IPv4 Routing Table

Destination	Gateway	Subnet Mask	Flags	Metric	Ref	Use	Interface
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

LAN Port Configuration

The LAN Ethernet port(s) on the pX2 are for connection of devices on a local network. By default, this port has a static IP Address. It also, by default is running a DHCP server to provide IP Addresses to devices that are connected to the physical LAN port (directly or via a switch).

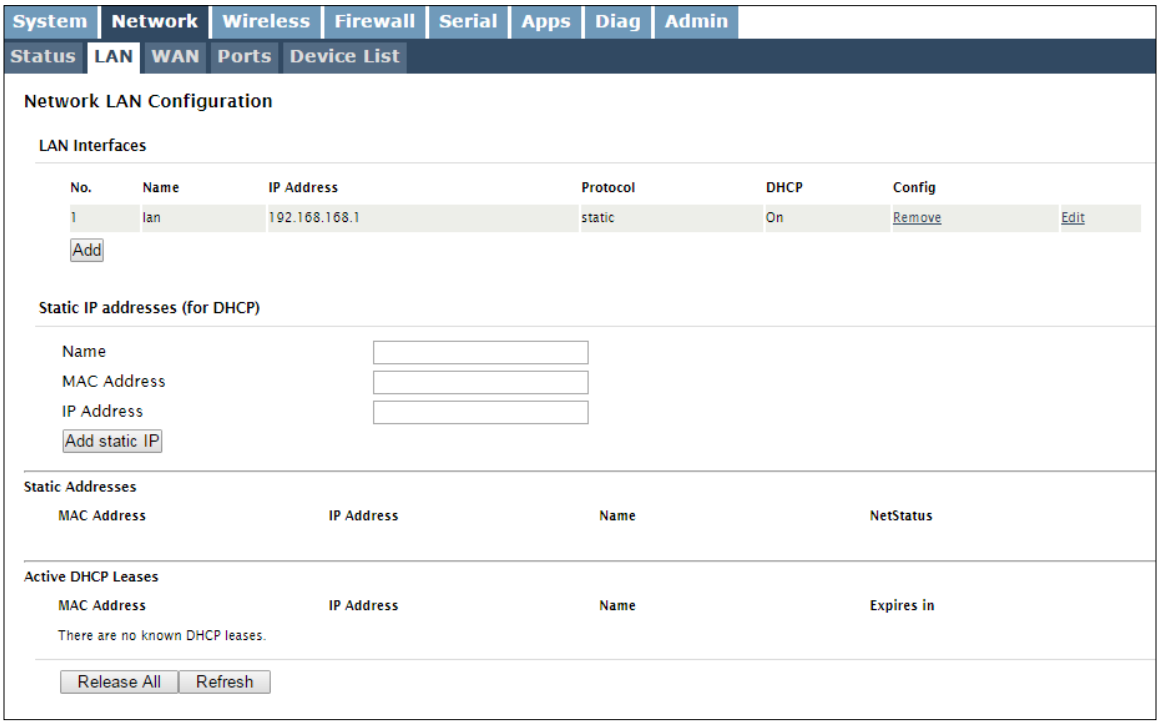


Image 4-2-2: Network > Network LAN Configuration

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

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

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

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

LAN Add/Edit Interface

The pX2 has the capability to have multiple SSID's for the WiFi radio. New Interfaces can be added for additional SSID's, providing, if required, separate subnets for each SSID. By default any additional interfaces added will automatically assign IP addresses to connecting devices via DHCP. Additional interfaces can only be used by additional WIFI SSID's (virtual interfaces).

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

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

4.0 Configuration

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

Spanning Tree (STP)

This option allows the pX2 to participate in the Spanning Tree protocol with other devices to prevent local loops. By default this is disabled.

Values (selection)

Off
On

Connection Type

This selection determines if the pX2 will obtain an IP address from a DHCP server on the attached network, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

Values (selection)

DHCP
Static

IP Address

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

Values (IP Address)

192.168.168.1

A 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.

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 pX2 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 GATEWAY is a point within a network that acts as an entrance to another network.

In typical networks, a router acts as a gateway.

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

DNS

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

Values (IP Address)

(no default)

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

4.0 Configuration

LAN DHCP

A pX2 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 pX2. The LAN DHCP service is available for each interface, and is located in the add/edit interface menus.

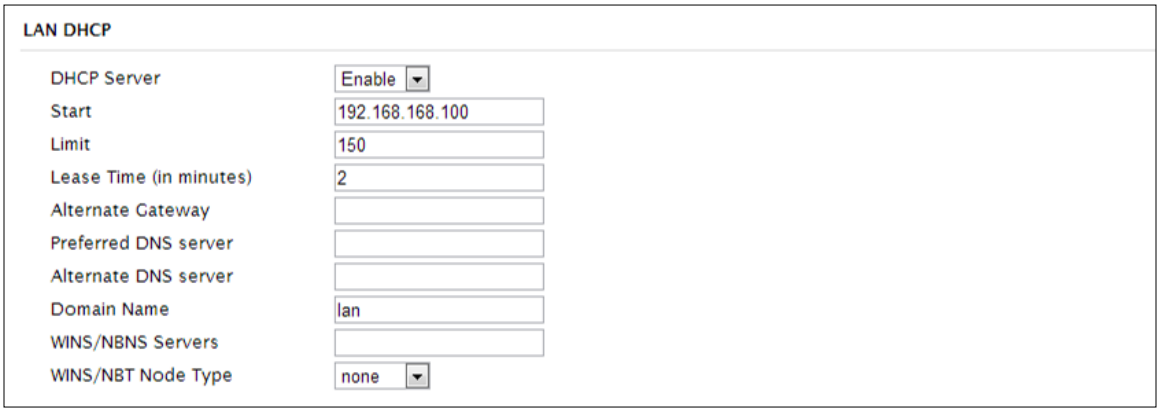


Image 4-2-4: Network > DHCP Server

DHCP Server

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

Values (selection)

Enable / Disable

Start

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

Values (IP Address)

192.168.168.100

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.)

Limit

Set the maximum number of IP addresses that can be assigned by the pX2.

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)

4.0 Configuration

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

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

Preferred DNS Server

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

Values (IP Address)

(IP Address)

Alternate DNS Server

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

Values (IP Address)

(IP Address)

Domain Name

Enter the Domain Name for the DHCP devices.

Values (string)

(IP Address)

WINS/NBNS Servers

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

Values (IP/Domain)

(no default)

WINS/NBT Node Type

Select the method used to resolve computer names to IP addresses. Four name resolution methods are available:
B-node: broadcast
P-node: point-to-point
M-node: mixed/modified
H-node: hybrid

Values (selection)

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

4.0 Configuration

Static IP Addresses (for DHCP)

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

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

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

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

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

Static Addresses

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

Active DHCP Leases

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

4.0 Configuration

4.2.3 Network > WAN

WAN Configuration

The WAN configuration refers to the wired WAN connection on the pX2. The WAN port can be used to connect the pX2 to other networks, the internet and/or other network resources.

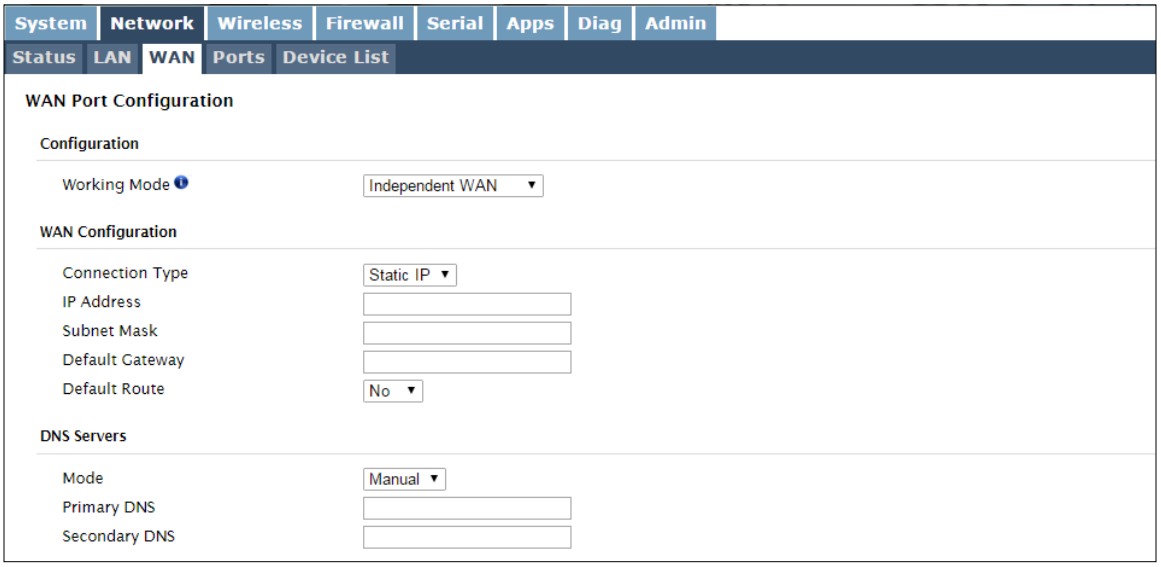


Image 4-2-6: Network > WAN Configuration

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

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

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

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

Working Mode

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

Values (selection)

Independent WAN
Bridged with LAN Port
Independent LAN

Connection Type

This selection determines if the pX2 will obtain an WAN IP address from a DHCP server, or if a static IP address will be entered. If a Static IP Address is chosen, the fields that follow must also be populated.

Values (selection)

DHCP
Static

IP Address

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

Values (IP Address)

(no default)

Netmask

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

Values (IP Address)

(no default)

4.0 Configuration

Default Gateway

If the pX2 is integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

Values (IP Address)

(no default)

Default Route

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

Values (selection)

No / Yes

DNS Servers

The following section will allow a user to specify DNS Server(s) to be used by the WAN interface of the pX2.

Mode

Select between Manual or Auto for DNS server(s) for the WAN interface. If set to Auto the pX2 will try to automatically detect the DNS servers to use, which is normally the case when the WAN is DHCP. Manual required the DNS addresses to be known and entered below.

Values (selection)

Manual / **Auto**

Primary DNS

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

Values (IP Address)

(no default)

Secondary DNS

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

Values (IP Address)

(no default)

4.0 Configuration

4.2.4 Network > Ports

The Network > Ports menu can be used to determine the characteristics of the physical Ethernet interfaces on the pX2. As seen below the Mode (Auto/Manual), Auto-Negotiation, Speed (10/100Mbit/s) and the Duplex (Full/Half) can all be configured on the pX2.

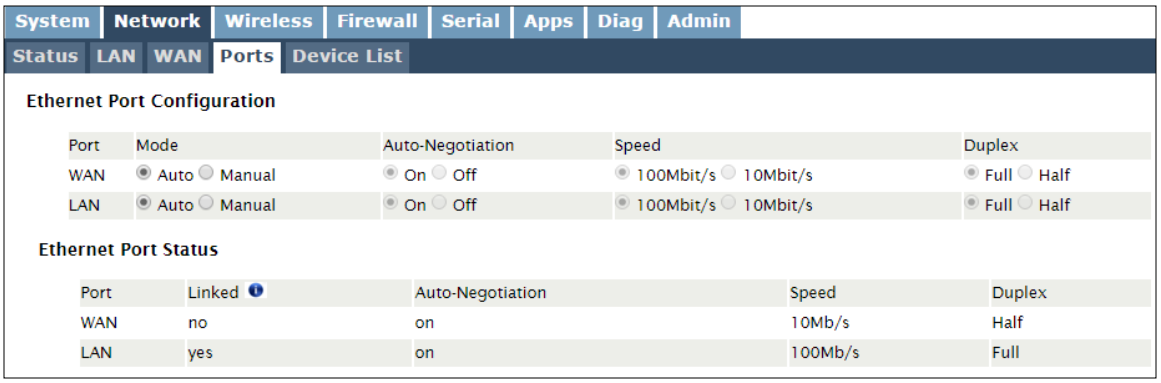


Image 4-2-6: Network > Ports

Mode

If set to Auto, the pX2 will negotiate and determine the best connection speed and mode.

Values (selection)

Auto / Manual

Auto-Negotiation

Enable or disable auto-negotiation.

Values (selection)

On / Off

Speed

If the mode and auto negotiation are set you manual the connection speed can be specified.

Values (selection)

100Mbit/s / 10 Mbit/s

Duplex

Selection between full or half duplex for the direction of data.

Values (selection)

Full / Half

4.0 Configuration

4.2.4 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 (s) are displayed, including those connected through a hub or switch.

Image 4-2-7: Network > Device List

4.0 Configuration

4.3 Wireless (WiFi)

4.3.1 Wireless > Status

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

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

Traffic Status shows statistics about the transmitted and received data.

The pX2 shows information about all Wireless connections in the **Connection Info** section. The Wireless MAC address, Noise Floor, Signal to Noise ratio (SNR), Signal Strength (RSSI), The transmit and receive Client Connection Quality (CCQ), TX and RX data rates, and a graphical representation of the signal level or quality.

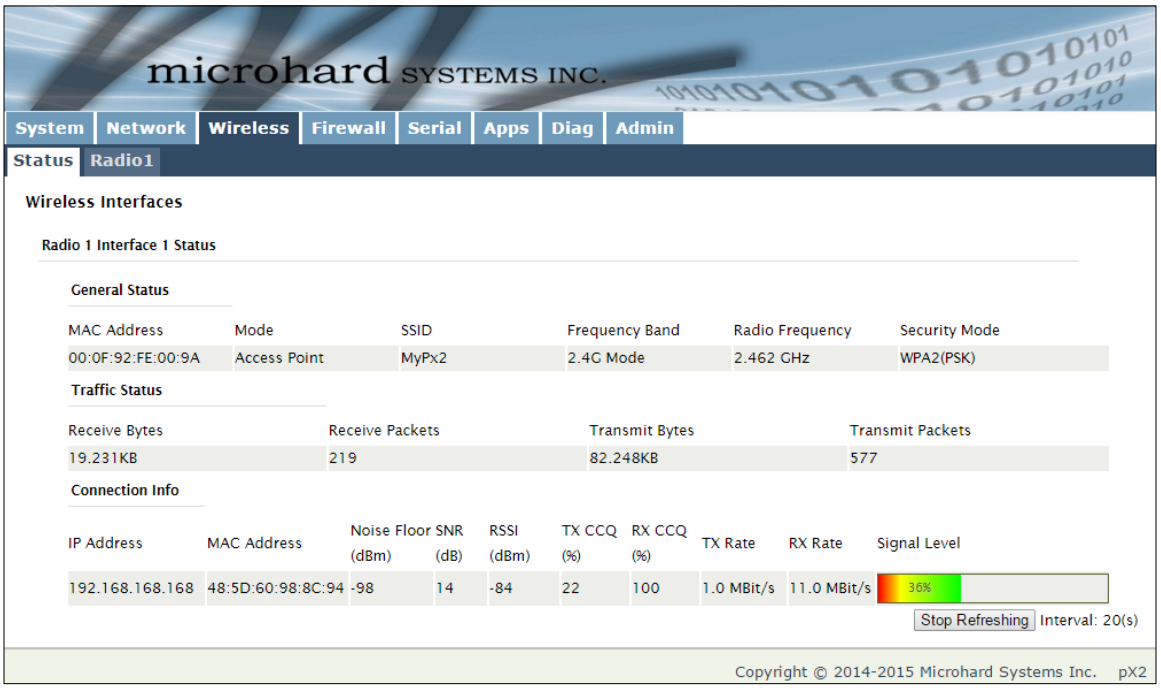


Image 4-3-1: Wireless > Status

4.0 Configuration

4.3.2 Wireless > Radio1

Radio1 Phy Configuration

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

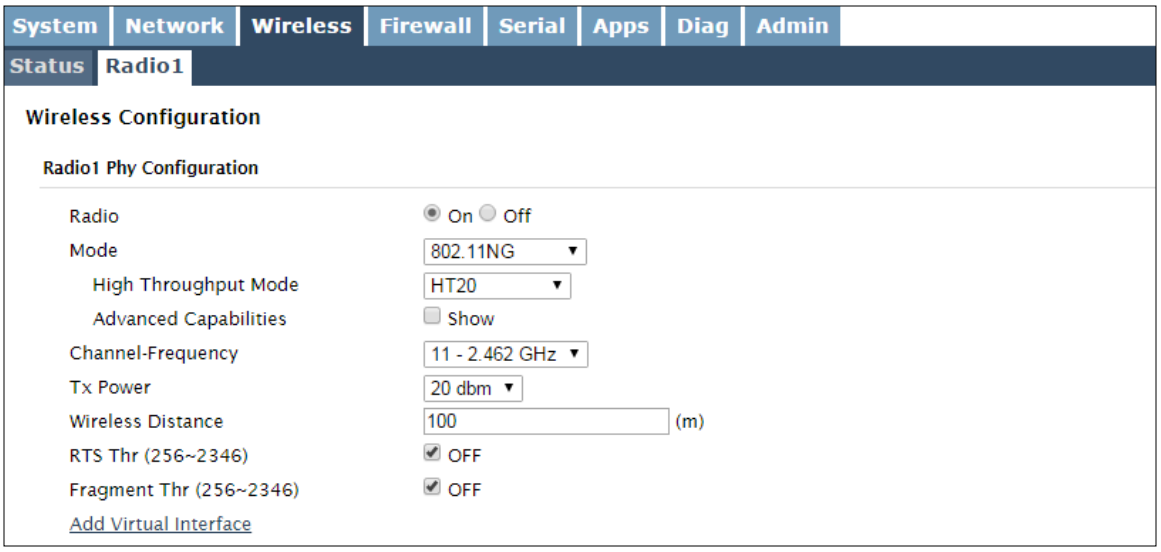


Image 4-3-2: Wireless > Radio Configuration

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

Mode	
The Mode defines which wireless standard to use for the wireless network. The pX2 supports the 802.11b/g/n modes seen here. Select the appropriate operating mode from the list. The options below are dependant and vary on the operating mode chosen here.	**Values (selection)** 802.11B ONLY 802.11BG 802.11NG

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

4.0 Configuration

High Throughput Mode

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

Values (selection)

HT20
HT40-
HT40+

Advanced Capabilities (Only shown if box is checked)

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

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

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

Channel-Freq

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

Values (selection)

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

TX Power

This setting establishes the transmit power level which will be presented to the antenna connector of the pX2. Unless required, the Tx Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

Values (selection)

20 dBm	25 dBm
21 dBm	26 dBm
22 dBm	27 dBm
23 dBm	28 dBm
24 dBm	29 dBm
	30 dBm

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

4.0 Configuration

Wireless Distance

The Wireless Distance parameter allows a user to set the expected distance the WiFi signal needs to travel. The default is 100m, so the pX2 will assume that the signal may need to travel up to 100m so it sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced.

Values (meters)

100

RTS Thr (256 ~ 2346)

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

Values (selection)

On / **OFF**

Fragment Thr (256 ~ 2346)

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

Values (selection)

On / **OFF**

4.0 Configuration

Radio1 Virtual Interface

The bottom section of the Wireless Configuration provides for the configuration of the Operating Mode of the Wireless Interface, the TX power, Wireless Network information, and Wireless Encryption. The pX2 can support multiple virtual interfaces. These interfaces provide different SSID's for different users, and can also be assigned to separate subnets (Network Interfaces) to prevent groups from interacting.

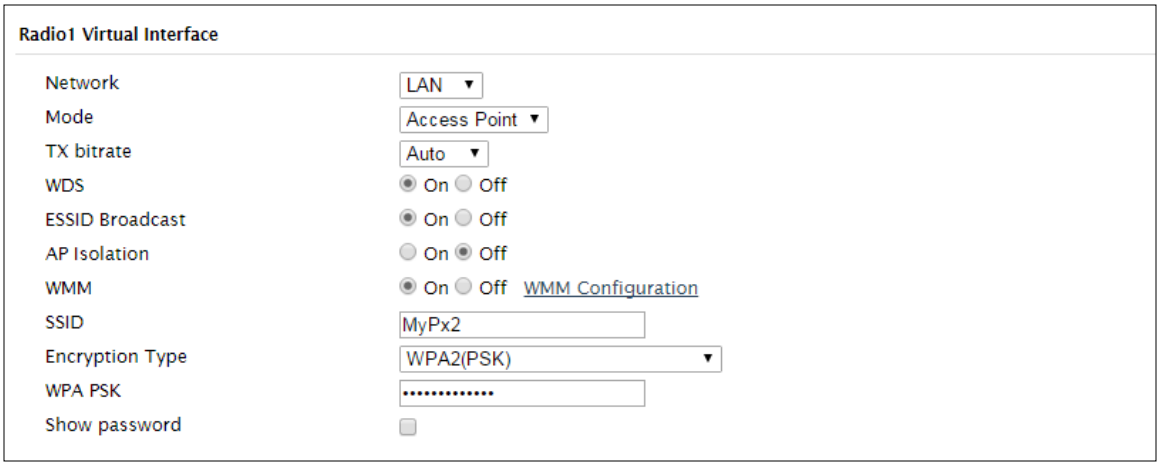


Image 4-3-3: Wireless > Radio Configuration

Network

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

Values (selection)

LAN
(Additional Interfaces…)

Mode

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

If more than 1 Virtual Interface (more than 1 SSID) has been defined, the pX2 can **ONLY** operate as a Access Point, and will be locked into this mode.

Values (selection)

Access Point
Client
Repeater
Mesh Point

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

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

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

4.0 Configuration

TX bitrate

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

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

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

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

WDS

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

Values (selection)

On / Off

ESSID Broadcast

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

Values (selection)

On / Off

MESH ID

When set in Mesh Mode, the MESH ID must be the same for all pX2 units participating, similar to the SSID for other wireless networks.

Values

(no default)

AP Isolation

When AP Isolation is enabled wireless devices connected to this SSID will not be able to communicate with each other. In other words if the pX2 is being used as a Access Point for many wireless clients, AP Isolation would provide security for those clients by not allowing access to any other wireless device.

Values (selection)

On / **Off**

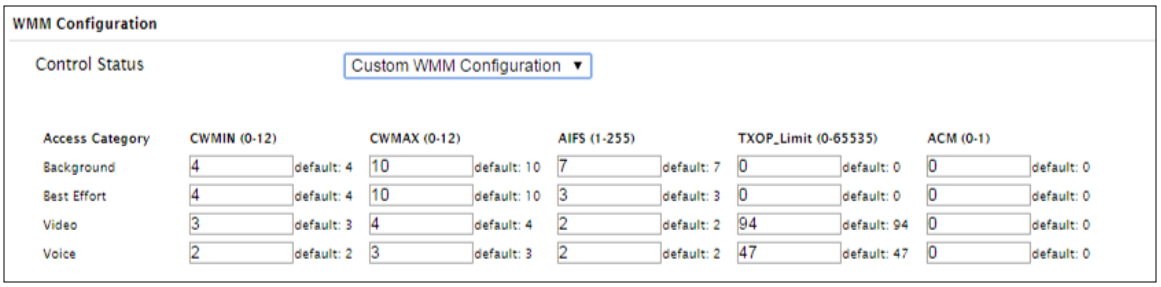
4.0 Configuration

WMM

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

Values (selection)

On / **Off**



SSID

All devices connecting to the pX2 in a given network must use the SSID of the pX2. This unique network address is not only a security feature for a particular network, but also allows other networks - with their own unique network address - to operate in the same area without the possibility of undesired data exchange between networks.

Values (string)

pX2

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

Encryption Type

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

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

Values (selection)

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

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

WPA PSK

This is the password, or preshared key that is required by any device to connect to the wireless interface of the pX2. It is **strongly recommended** to always have a password defined, and changed from the factory default.

Values (string)

0123456789

Show Password

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

Values (selection)

unchecked

4.0 Configuration

RADIUS IP Address	
If using Enterprise (RADIUS) encryption, enter the IP Address of the RADIUS authentication server here.	**Values (IP Address)** *(no default)*

RADIUS Port	
If using Enterprise (RADIUS) encryption, enter the port number of the RADIUS authentication server here.	**Values (port)** *(no default)*

RADIUS Server Key	
This is the password, or preshared key that is required by any device to connect to the wireless interface of the pX2. It is **strongly recommended** to always have a password defined, and changed from the factory default.	**Values (selection)** **0123456789**

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.

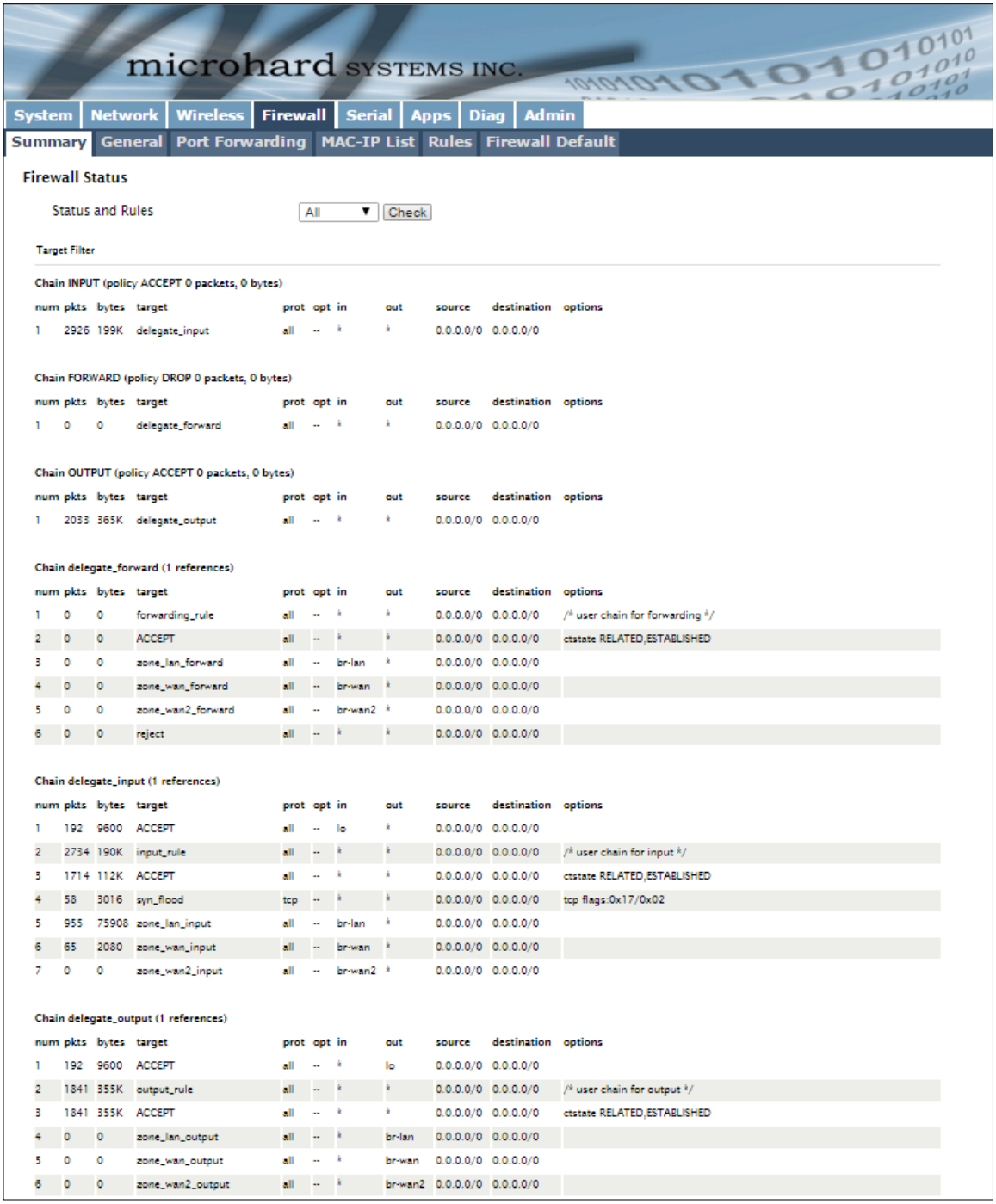


Image 4-4-1: Firewall > Status

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.

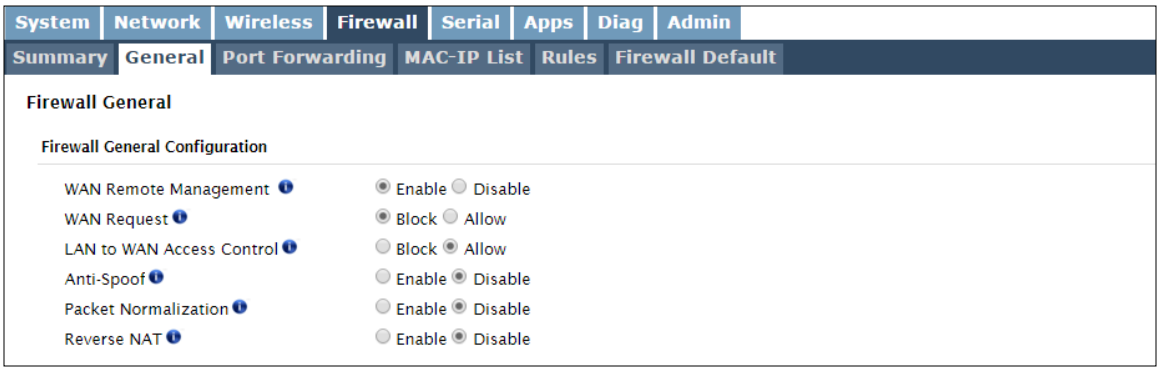


Image 4-4-2: Firewall > General

WAN Remote Management

Allow remote management of the pX2 on the WAN side using the WebUI on port 80(HTTP), and 443 (HTTPS). If disabled, the configuration can only be accessed from the LAN.

Values

Enable / Disable

WAN Request

When Blocked the pX2 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

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**

Anti-Spoof

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

Values

Enable / **Disable**

Packet Normalization

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

Values

Enable / **Disable**

4.0 Configuration

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 pX2 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 pX2. 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 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.

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.

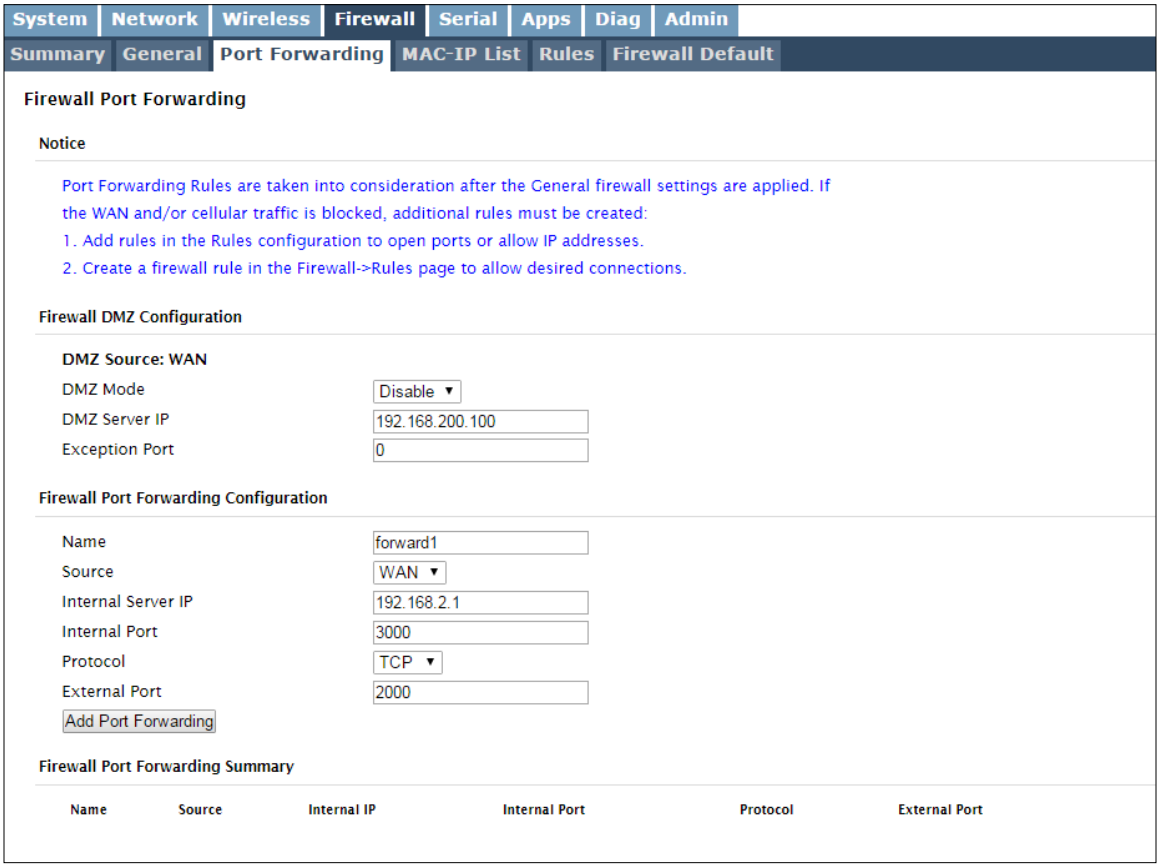


Image 4-4-3: Firewall > Port Forwarding

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

DMZ Server IP	
Enter the IP address of the device on the LAN side of the pX2 where all the traffic will be forwarded to.	**Values (IP Address)** **192.168.100.100**

4.0 Configuration

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 pX2.	**Values (Port #)** **0**

Firewall Port Forwarding 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.

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 WIFI or from the WAN.	**Values (selection)** **WAN** / WIFI

Internal Server IP	
Enter the IP address of the intended internal (i.e. on LAN side of the pX2) 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 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 pX2, by restricting or allowing connections based on the MAC address. IP List configuration can be used to define who or what can access the pX2, 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 Access Control to provide secure access to the physical ports of the pX2.

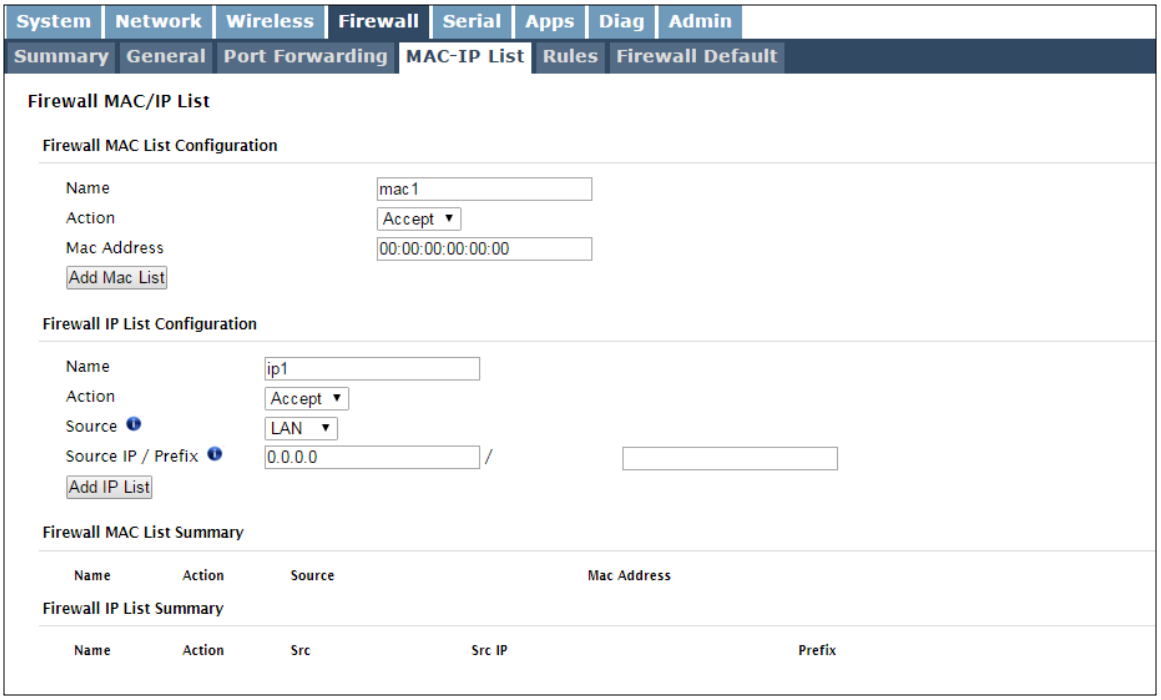


Image 4-4-4: Firewall > MAC-IP List

Firewall MAC List Configuration

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

MAC Address	Values (MAC Address)
Specify the MAC Address to be added to the list. Must be entered in the correct format as seen above. Not case sensitive.	**00:00:00:00:00:00**

4.0 Configuration

Firewall MAC List Configuration (Continued)

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

Firewall IP List Configuration

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

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

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

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

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

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

Appendix D: Firewall Example

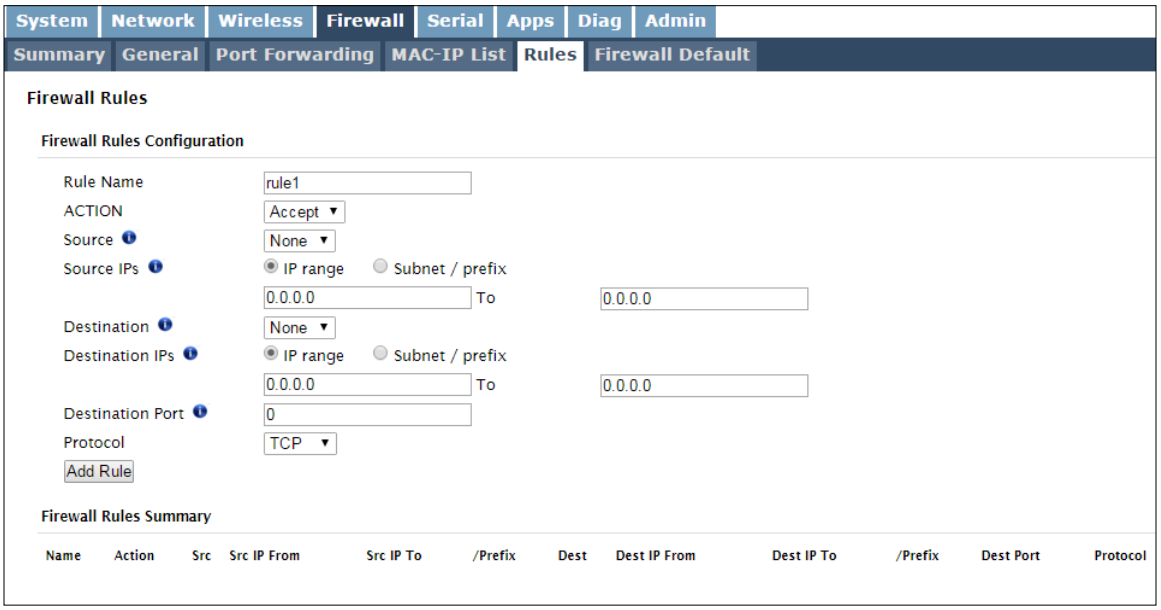


Image 4-4-5: Firewall > Rules

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

Values (selection)

ACCEPT
DROP
REJECT

Source

Select the zone which is to be the source of the data traffic. The LAN/ LAN1 refers to local connections on the pX2.

Values

LAN/LAN1/WAN/WIFI/
None

4.0 Configuration

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

Destination	
Select the zone which is the intended destination of the data traffic.	**Values (selection)** LAN/LAN1/WAN/WIFI **None**

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

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

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

4.0 Configuration

4.4.6 Firewall > Default

The firewall can be returned to default setting without requiring the entire modem to be reset to defaults. It is recommended to restart the modem once changes to the firewall or a reset is performed.

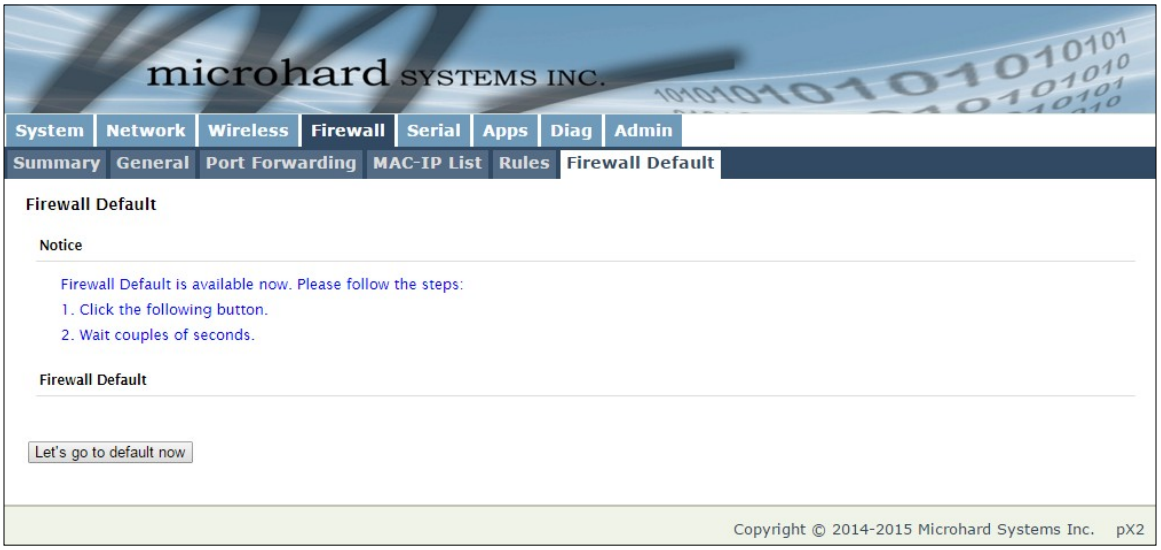


Image 4-4-6: Firewall > Default

4.0 Configuration

4.5 Serial

4.5.1 Serial > Summary

The Serial > Summary window gives a summary of the RS232 Serial Data Port located on the side of the pX2, the port uses a standard DB-9 connector.

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

General Status

- Port Status - Shows if the RS232 has been enabled in the configuration.
- Baud Rate - The current baud rate used to interface with the connected device.
- Connect As - The type of IP Protocol Config is displayed here (TCP, UDP, SMTP, PPP, etc)
- Connect Status - Shows if there are any current connections / if the port is active.

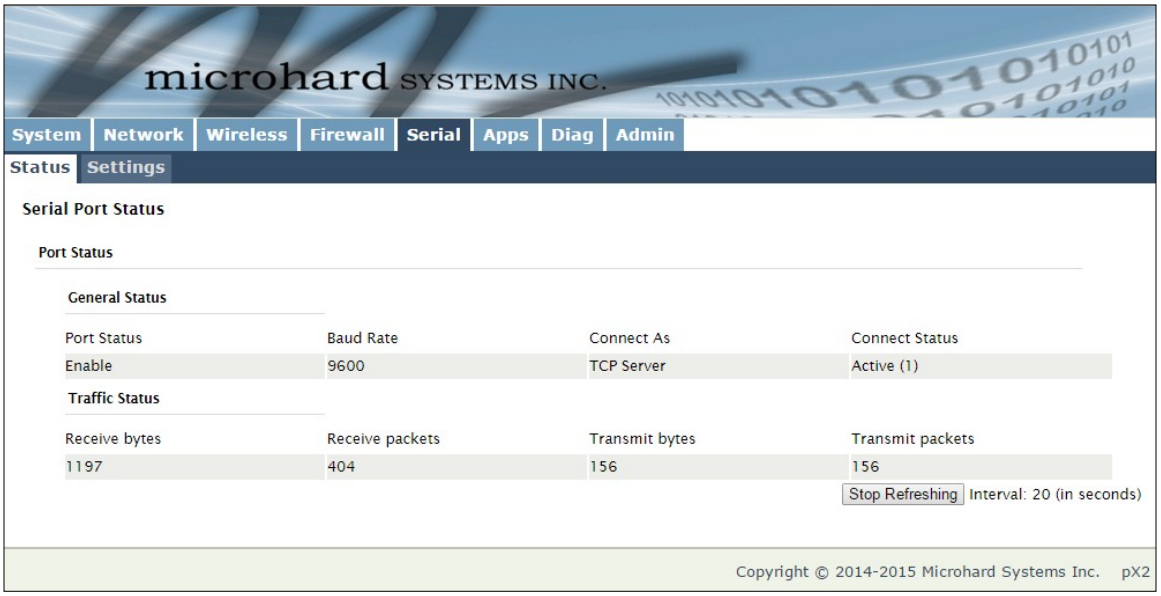


Image 4-5-1: Serial > Summary

4.0 Configuration

4.6.2 Serial > Settings

This menu option is used to configure the serial device server for the serial communications port. Serial device data may be brought into the IP network through TCP, UDP, or multicast; it may also exit the pX2 network on another pX2 serial port. The fully-featured RS232 interface supports hardware handshaking.

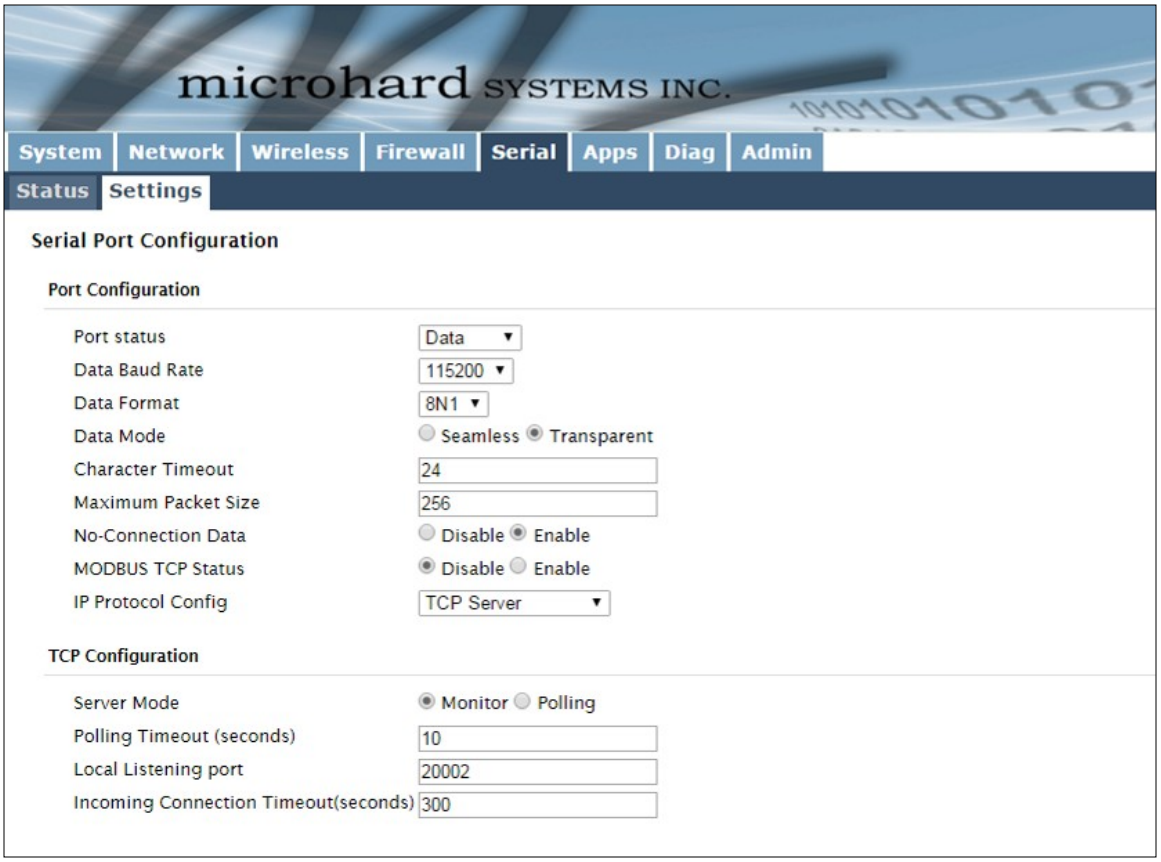


Image 4-5-2: Serial > Settings Configuration

4.0 Configuration

Port Status

Select operational status of the Serial Port. The port is in console mode by default.

Values (selection)

Data / **Console**

Data Baud Rate

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

Values (bps)

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

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

Data Format

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

Values (selection)

8N1
8E1
8O1

Data Mode

This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the pX2.

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).

4.0 Configuration

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)** **256**

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 pX2 will disregard any data received on the serial data port when radio synchronization is lost.	**Values (selection)** **Disable** / Enable

MODBUS TCP Status	
This option will enable or disable the MODBUS decoding and encoding features.	**Values (selection)** **Disable** / Enable

4.0 Configuration

IP Protocol Config

This setting determines which protocol the serial server will use to transmit serial port data over the pX2 network.

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

Values (selection)

TCP Client
TCP Server
TCP Client/Server
UDP Point-to-Point
PPP

TCP Client: When TCP Client is selected and data is received on its serial port, the pX2 takes the initiative to find and connect to a remote TCP server. The TCP session is terminated by this same unit when the data exchange session is completed and the connection timeout has expired. If a TCP connection cannot be established, the serial port data is discarded.

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

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

- **Outgoing Connection Timeout**
  This parameter determines when the pX2 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)

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

TCP Server: In this mode, the pX2 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)

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.

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 pX2 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 PX2 will send serial data to a specifically-defined point, using UDP packets. This same pX2 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 Timeout(s)**
  UDP Timeout in seconds.
  Default: **10**

4.0 Configuration

IP Protocol Config (Continued…)

PPP: The serial port 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 PX2.

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

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

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

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

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

- PPP Local IP
  Enter the local PPP IP Address, the IP Address of the pX2 COM Port.
  Default: **192.168.0.1**

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

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

4.0 Configuration

4.6 Apps

4.6.1 Apps > Event Report

4.6.1.1 Event Report > Configuration

Event Reporting allows the pX2 to send periodic updates via UDP packets. These packets are customizable and can be sent to up to 3 different hosts, and at a programmable interval. The event packet can report information about the modem such as the hardware/ software versions, core temperature, supply voltage, etc; carrier info such as signal strength (RSSI), phone number, RF Band; or about the WAN such as if the assigned IP Address changes. All events are reported in binary.

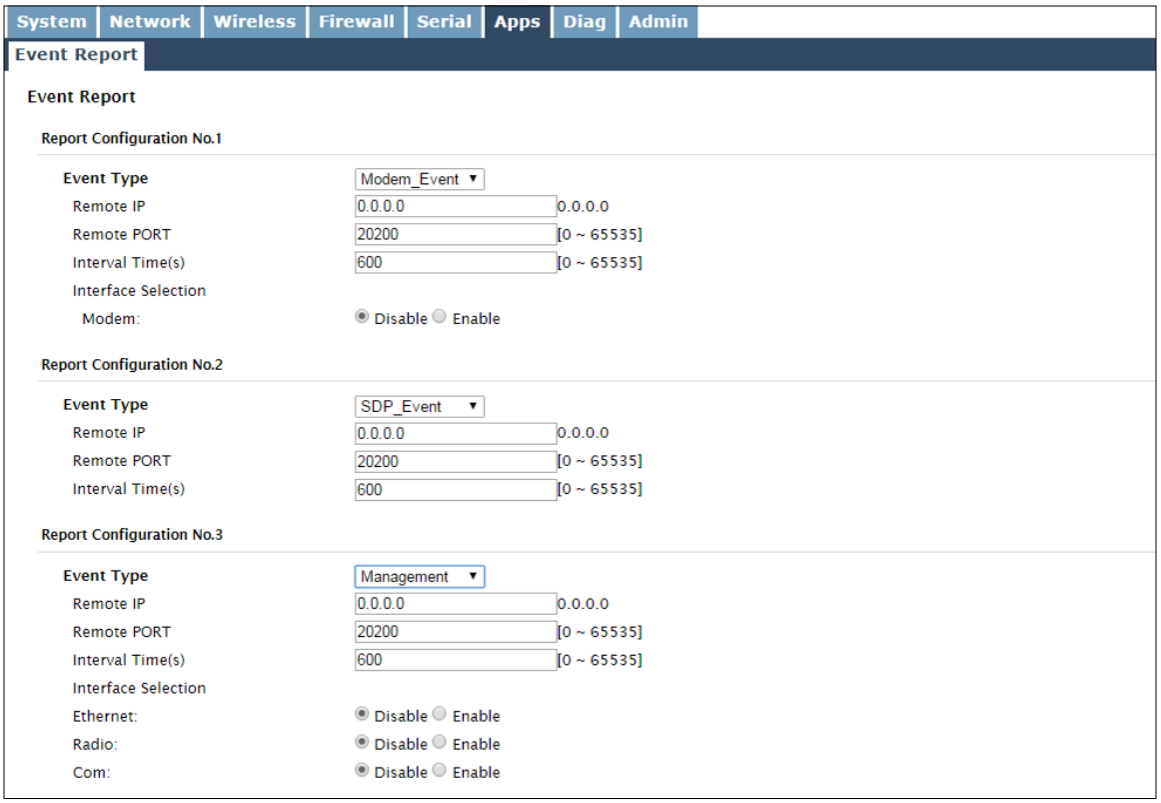


Image 4-6-1: Applications > Event Report

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

Remote IP	
Enter the IP Address of a reachable host to send the UDP packets	**Values (IP Address)** **0.0.0.0**

4.0 Configuration

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

Interval Time(s)	
This is the interval time in seconds, that the pX2 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**

4.6.1.2 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

4.6.1.3 Event Report > Message Payload

Modem info:

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

Carrier info:

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

WAN Info:

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

Message Order:

Messages will be ordered by message type number.

For example,

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

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

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

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

4.0 Configuration

4.7 Diag

4.7.1 Diag > Ping

The Network Tools Ping feature provides a tool to test network connectivity from within the pX2 unit. A user can use the Ping command by entering the IP address or host name of a destination device in the Ping Host Name field, use Count for the number of ping messages to send, and the Packet Size to modify the size of the packets sent.

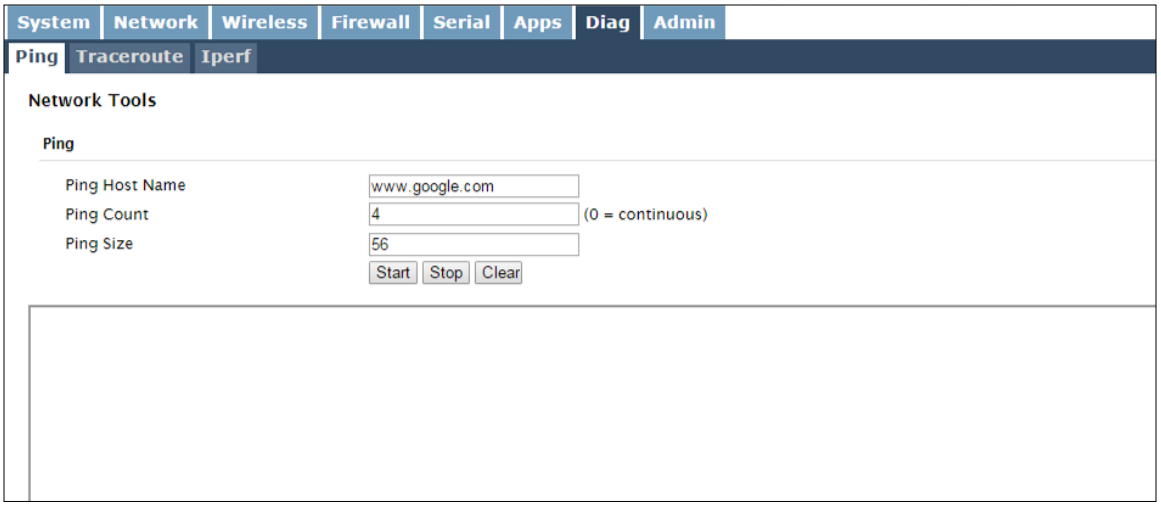


Image 4-7-1: Diagnostics > Ping

4.7.2 Diag > Traceroute

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

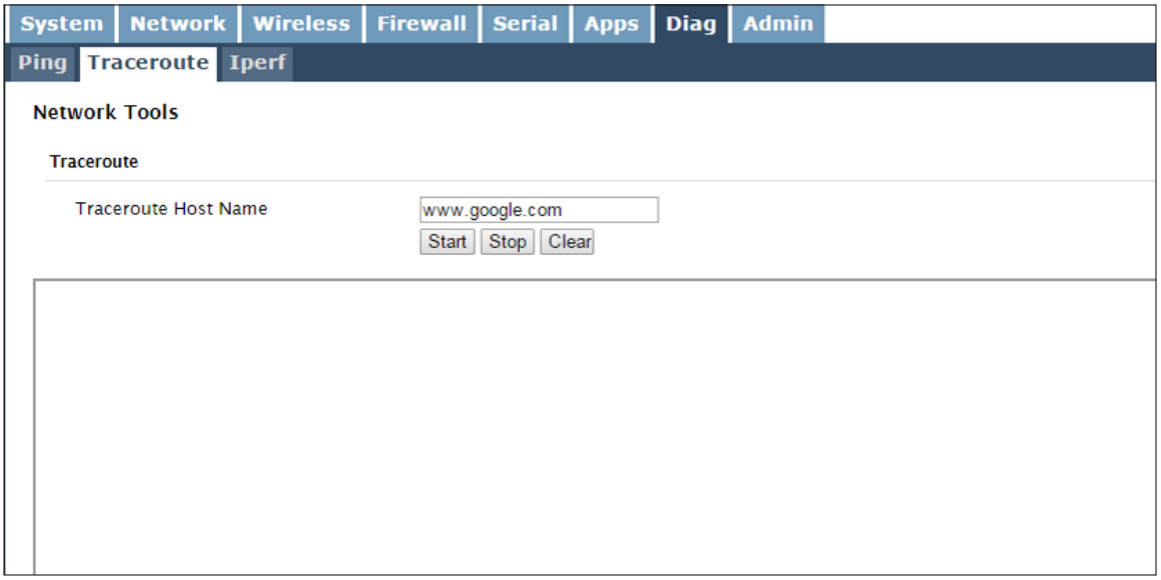


Image 4-7-2: Diagnostics > Trace Route

4.0 Configuration

4.7.3 Diag > Iperf

The pX2 features an integrated Iperf server/client to use to measure and analyze throughput of TCP/UDP packets to and/or from the pX2. Iperf is a 3rd party utility that can be loaded on any PC to measure network performance. For additional information about Iperf, please visit the Iperf website.

The pX2 can be configured to operate as a Server, listening for an incoming connection from another device (with Iperf), or PC running an Iperf client. If set to Iperf client, the pX2 will connect to or send packets to a specified Iperf server.

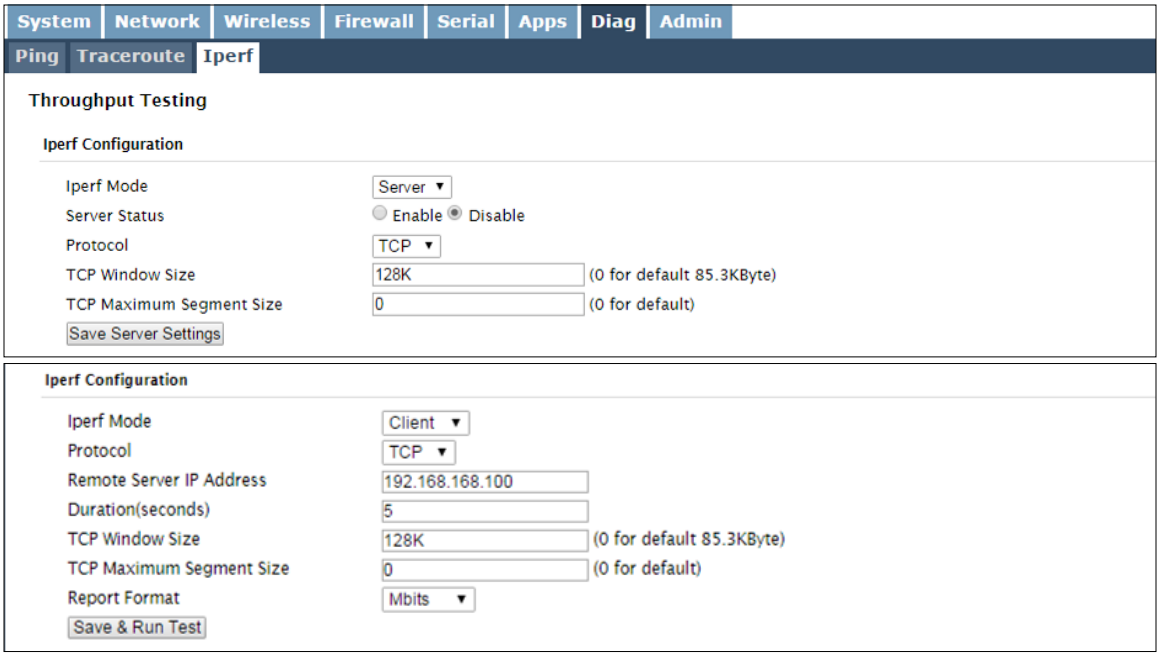


Image 4-7-3: Diag > Iperf

Iperf Mode	
Select between an Iperf Server (listens for incoming connections) and client (initiates a connection with a server)	**Values (selection)** **Server** / Client

Server Status	
If the Iperf mode to set to Server, this Server Status allows a user to Enable or Disable the server.	**Values (selection)** **Enable** / Disable

Protocol	
Select the type of packets to be sent to test the throughput. TCP packets are connection oriented and require additional overhead for the handshaking that occurs, while UDP is a connectionless, best effort oriented protocol.	**Values (selection)** **TCP** / UDP

4.0 Configuration

4. Admin

4.8.1 Admin > Users

Password Change

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

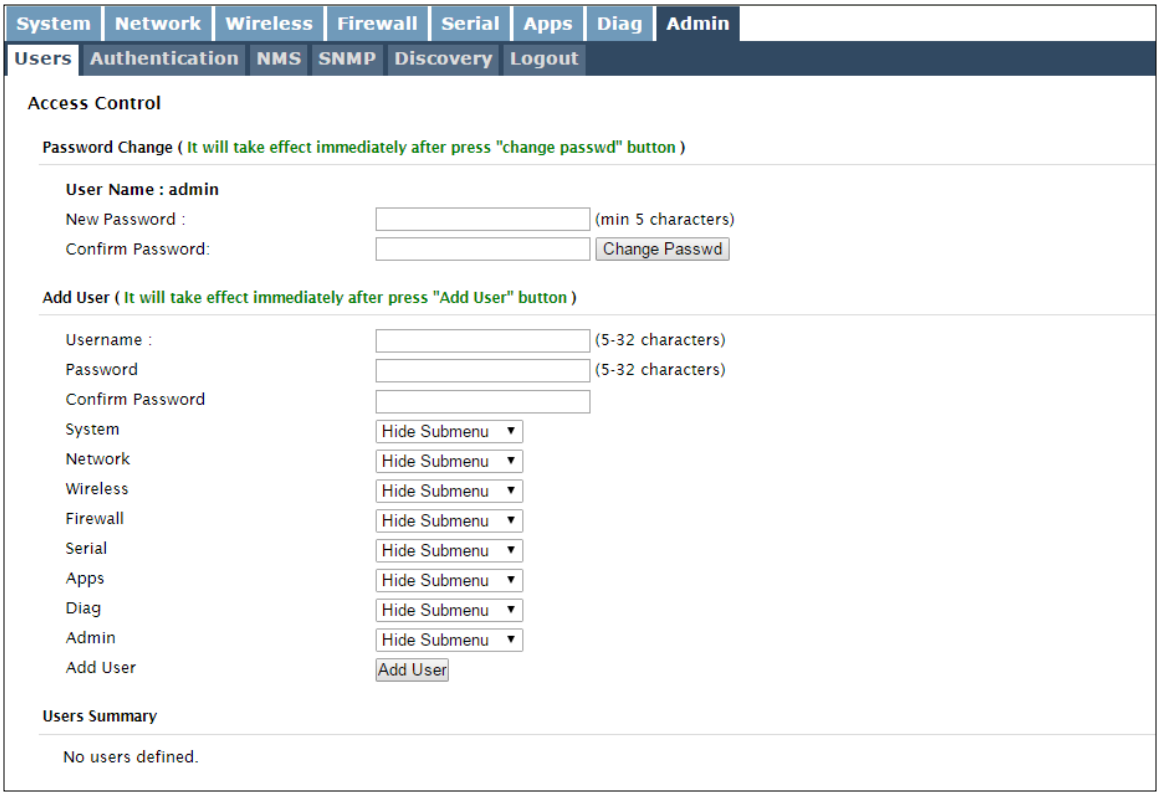


Image 4-8-1: Users > Password Change

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

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

4.0 Configuration

Add Users

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

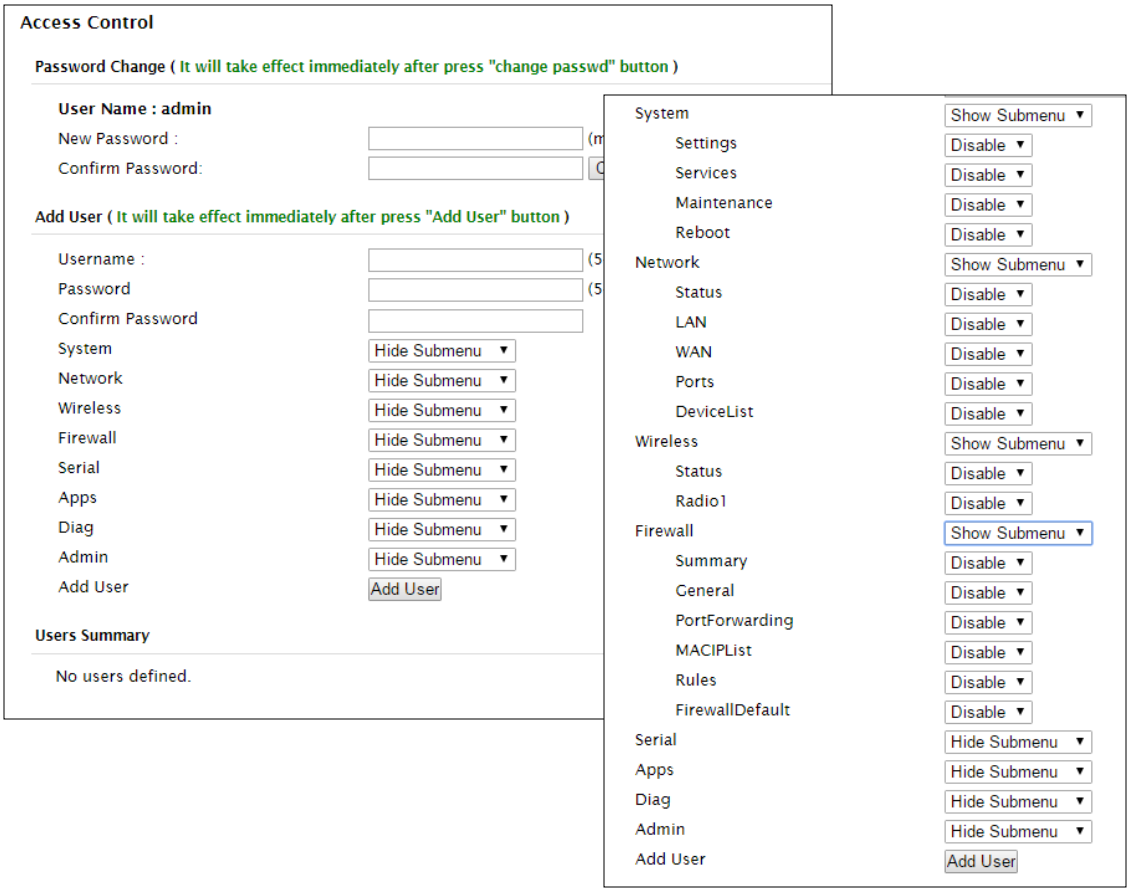


Image 4-8-2: Access Control > Users

Username

Enter the desired username. Minimum or 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted.

Values (characters)

(no default)
Min 5 characters
Max 32 characters

Password / Confirm Password

Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.

Values (characters)

(no default)
min 5 characters

4.0 Configuration

4.8.2 Admin > Authentication

There are two methods whereby a user may be authenticated for access to the pX2:

- Local

  Using the Admin or Upgrade access and associated passwords - the authentication is done 'locally' within the pX2, and

- RADIUS&Local

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

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

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

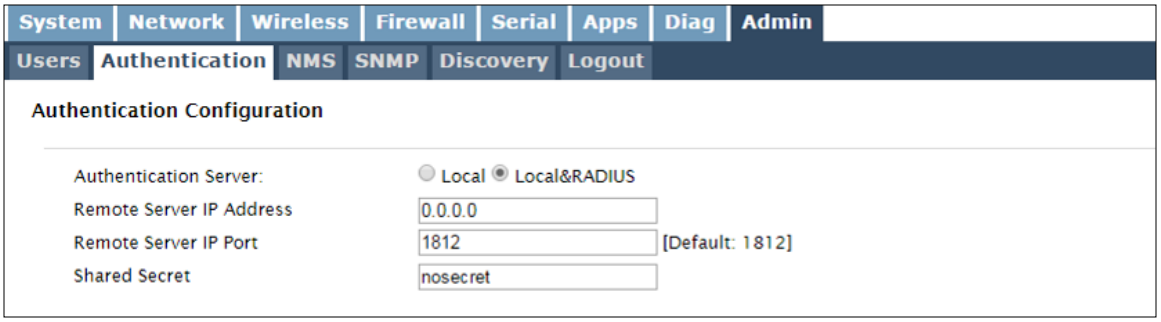


Image 4-8-3: Authentication Configuration

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

Shared 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

Specific RADIUS Server secret

nosecret

4.0 Configuration

4.8.3 Admin > NMS Settings

The Microhard NMS is a no cost hosted 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 pX2 to report to NMS. Units must have internet access to use NMS capabilities.

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.

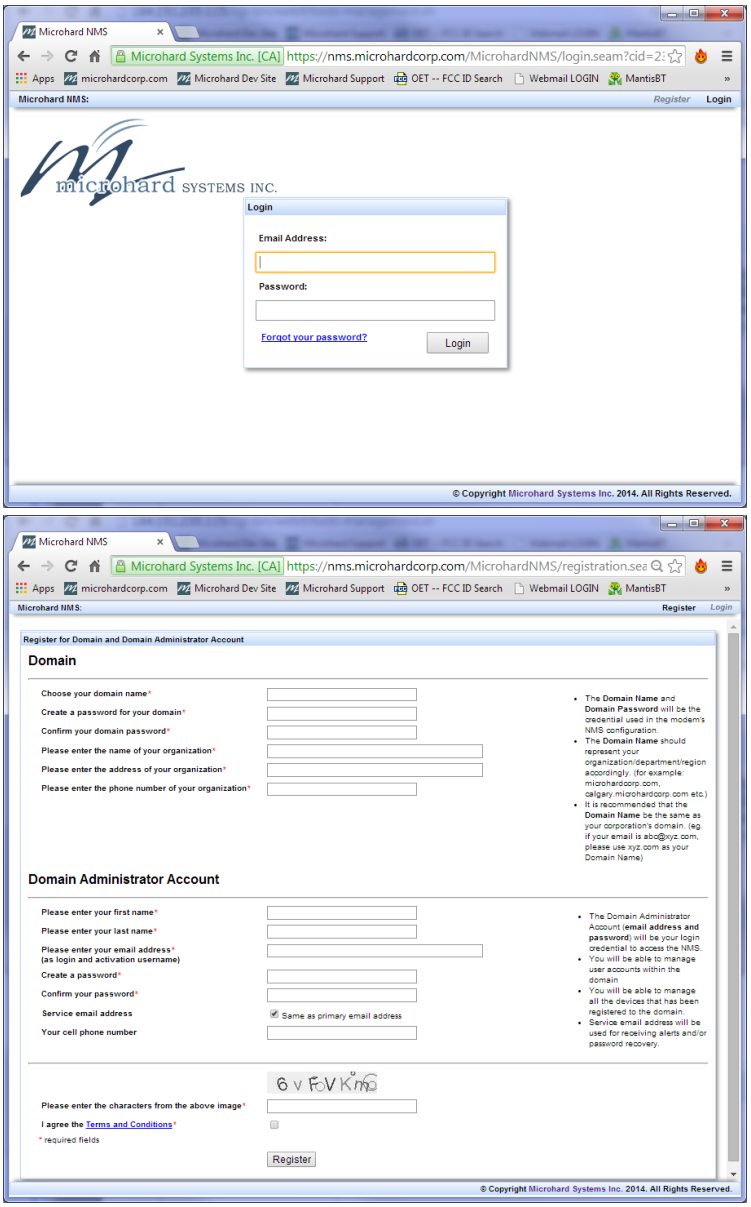


Image 4-8-4: NMS

4.0 Configuration

Domain Name: A logical management zone for devices to report to NMS, the logged data is separated from any other users that are using NMS. The Domain Name is required in every 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 device for it to report to right domain.

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 pX2 must be configured to report into NMS.

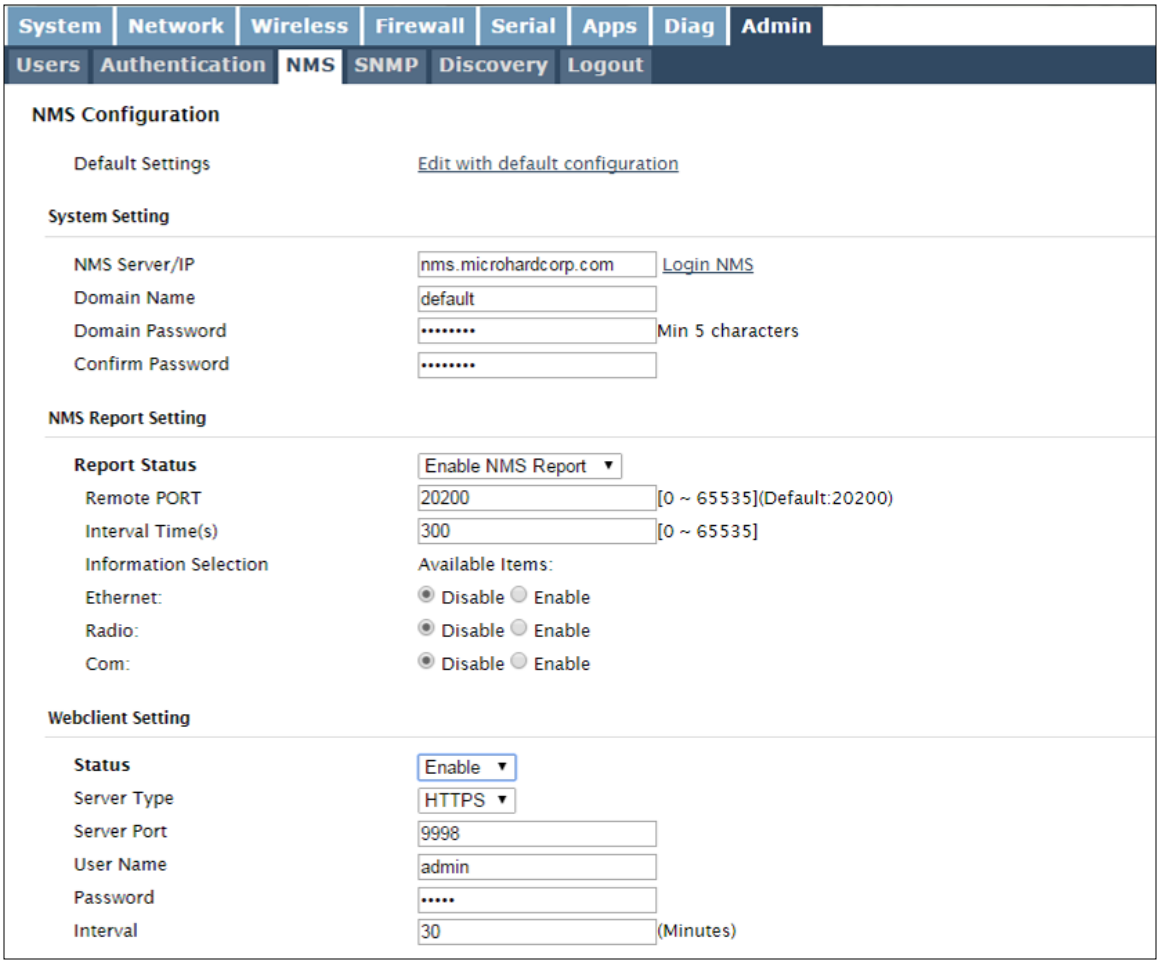


Image 4-8-5: NMS Settings

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.

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 pX2 will consume some data to retrieve location information from the internet.

Values (chars)

Disable/Enable

Report Status

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

Values (chars)

Enable NMS Report
Disable NMS Report

Remote Port

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

Values (UDP Port#)

20200

Interval(s)

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

Values (seconds)

300

4.0 Configuration

Information Selection

The pX2 can report information about the different interfaces it has. The more that is reported, the more data that is sent to the NMS system, be aware of data plan constraints and related costs.

Values (check boxes)

Ethernet
Radio
COM

Webclient Setting

Status

The Web Service can be enabled or disabled. This service is used to remotely control the pX2. It can be used to schedule reboots, firmware upgrade and backup tasks, etc.

Values (chars)

Disable/Enable

Server Type

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

Values (chars)

HTTPS/ HTTP

Server Port

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

Values (Port#)

9998

Username / Password

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

Values (seconds)

admin/admin

Interval

The Interval defines how often the pX2 checks with the NMS System to determine if there are any tasks to be completed. Data will be consumed every time the device probes the NMS system.

Values (min)

60

4.0 Configuration

4.8.4 Admin > SNMP

The pX2 may be configured to operate as a Simple Network Management Protocol (SNMP) agent. Network management is most important in larger networks, so as to be able to manage resources and measure performance. SNMP may be used in several ways:

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

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

Managed networked devices are referred to as SNMP agents.

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the pX2. 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 pX2 are hosted under private enterprise number **21703**.

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

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

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

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

The pages that follow describe the different fields required to set up SNMP on the PX2. MIBS may be requested from Microhard Systems Inc.

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

4.0 Configuration

SNMP Settings

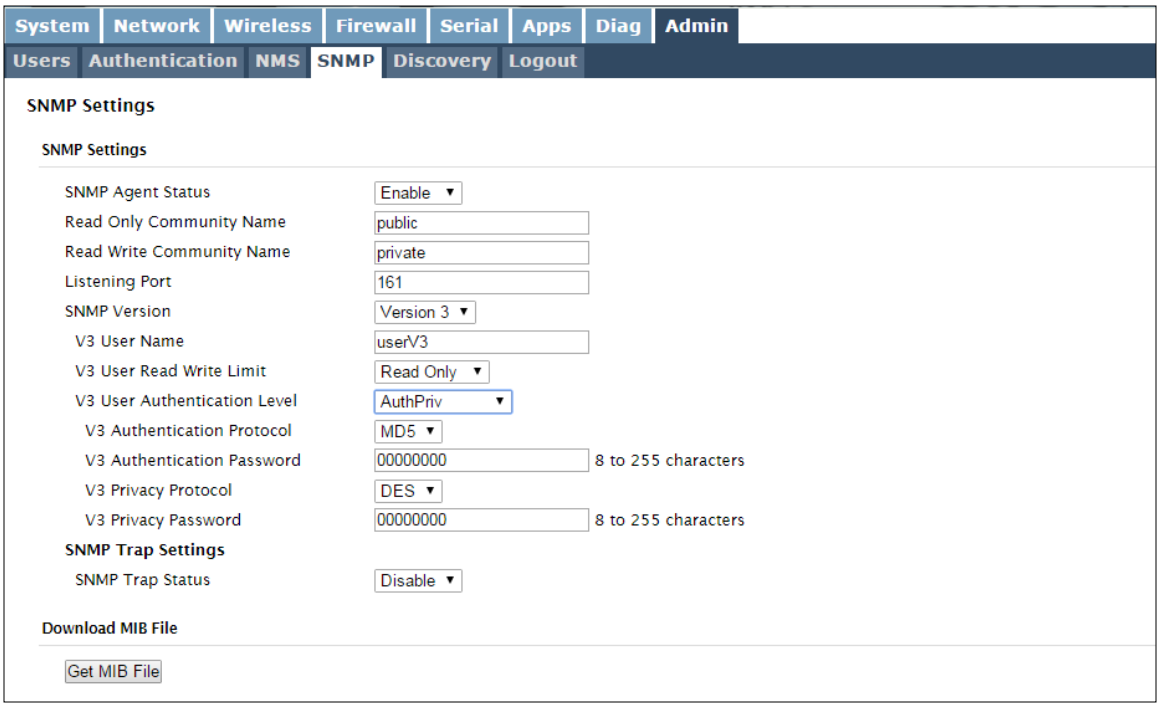


Image 4-8-6: Admin > SNMP

SNMP Agent Status

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 / Enable

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 Write 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

Listening Port

Enter the UDP port on which the pX2 listens for incoming SNMP get/set messages. The default is port 161.

Values (UDP Port)

161

4.0 Configuration

SNMP Version

Select the SNMP version used. Only SNMP version 1 & 2 support SNMP traps (See MIB).

Values (selection)

Version 1 / **Version 2** / Version 3

SNMP V3 User Name

Defines the user name for SNMPv3.

Values (string)

V3user

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

Auth Failure Traps

If enabled, an authentication failure trap will be generated upon authentication failure. (SNMP v1 & v2 only).

Values (selection)

Disable / Enable

Trap Community Name

The community name which may receive traps. (SNMP v1 & v2 only).

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). (SNMP v1 & v2 only).

Values (IP Address)

0.0.0.0

4.0 Configuration

4.8.5 Admin > Discovery

Server Status Settings

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

Image 4-8-7: Admin > Discovery

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

Server Port Settings	
Specify the port running the discovery service on the pX2 unit.	**Values (Port #)** 20097

Network Discovery

The Network discovery tool allows the pX2 to send a broadcast to all Microhard devices on the same network. Other units on the network will respond to the broadcast and report their MAC address, IP address (With a hyperlink to that units WebUI page), description, firmware version.

The discovery service can be a useful troubleshooting tool and can be used to quickly find and indentify other units on the network.

4.0 Configuration

4.8.6 Admin > Logout

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

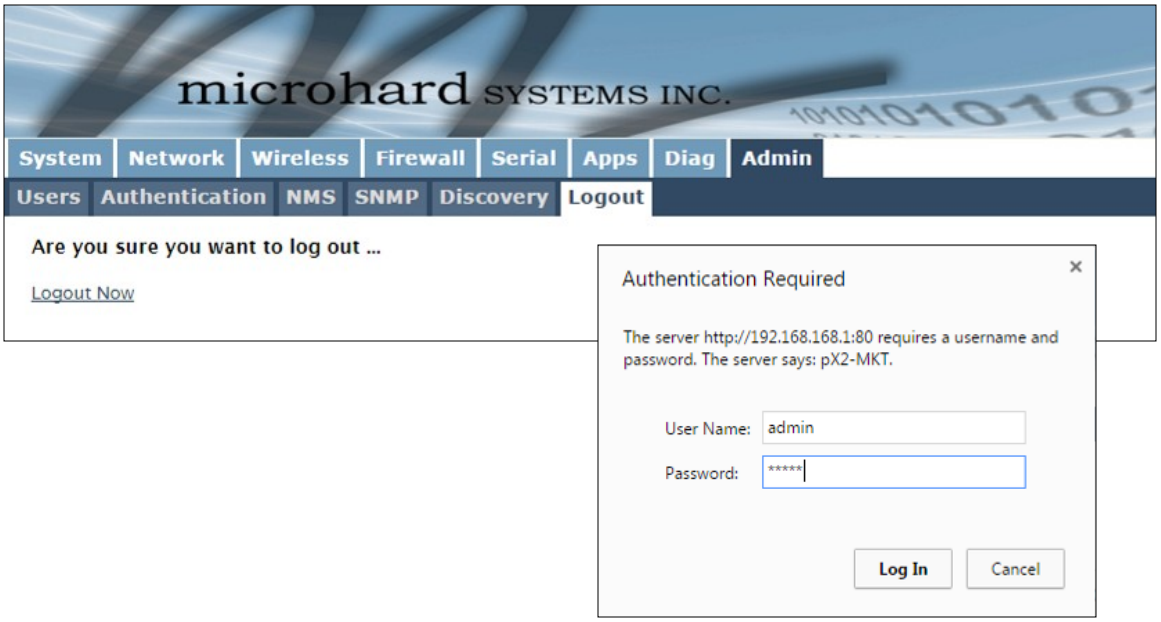


Image 4-8-8: Admin > logout

5.0 AT Command Line Interface

5.1 AT Command Overview

AT Commands can be issued to configure and manage the pX2, via TCP/IP (telnet).

5.1.1 Telnet (TCP/IP)

Telnet can be used to access the AT Command interface of the pX2. 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.

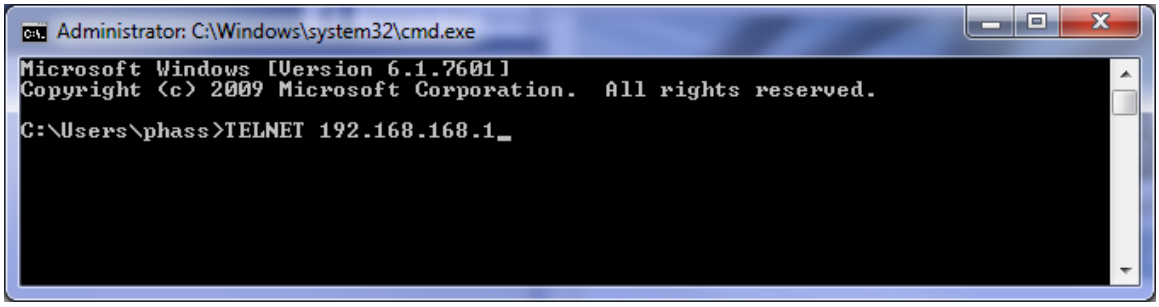


Image 5-1: Establishing a Telnet Session

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.

The factory default network settings:

IP: 192.168.168.1
Subnet: 255.255.255.0
Gateway: 192.168.168.1

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

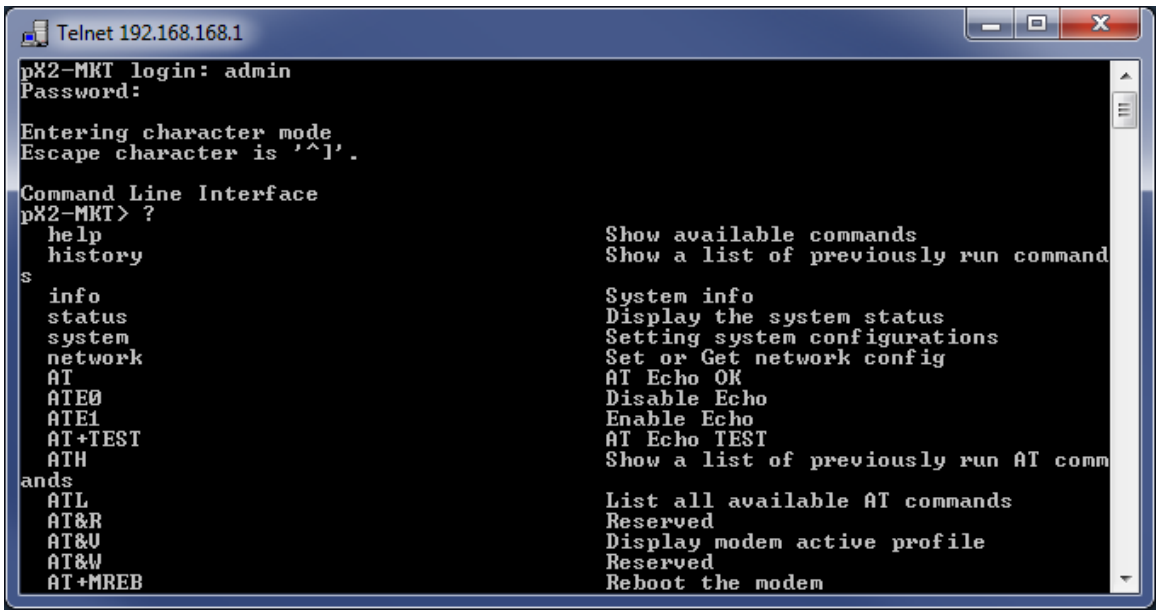


Image 5-2: Telnet AT Command Session

5.0 AT Command Line Interface

5.2 AT Command Syntax

The follow syntax is used when issuing AT Commands on the pX2

- 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:

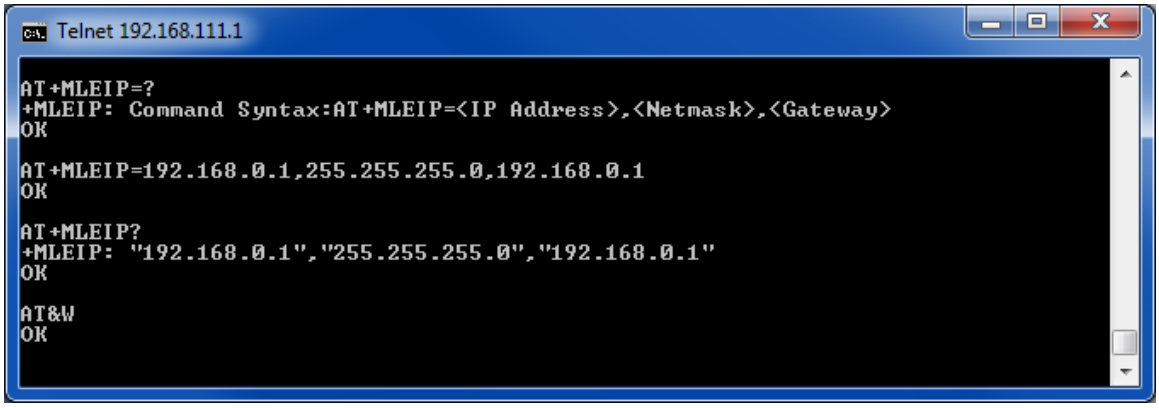


Image 5-3: Telnet AT Command Syntax

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

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

5.0 AT Command Line Interface

5.3 Supported AT Commands

AT

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

Example

Input:
AT <enter>
Response:
OK

ATE0

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

Example

Input:
ATE0 <enter>
Response:
OK

ATE1

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

Example

Input:
ATE1 <enter>
Response:
OK

AT+TEST

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

Example

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

5.0 AT Command Line Interface

ATH

Description

Show a list of previously run commands.

Command Syntax (Effect: Immediate)

ATH <enter>

Example

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

ATL

Description

Show a list of all available AT Commands.

Command Syntax (Effect: Immediate)

ATL <enter>

Example

Input:
ATL <enter>
Response:
AT Commands available:

```
  AT            AT Echo OK
  ATE0          Disable Echo
  ATE1          Enable Echo
  AT+TEST       AT Echo TEST
  ATH           Show a list of previously run AT commands
  ATL           List all available AT commands
  AT&R          Reserved
  AT&V          Display modem active profile
  AT&W          Enable configurations you have been entered
  ATA           Quit
  ATO           Quit
  AT+MSNTP      Get/Set NTP server
  AT+MSCNTO     Get/Set console timeout
.
.
.
<Output Omitted>
```

AT&R

Description

Read modem profile to editable profile. (Reserved)

Command Syntax (Effect: Immediate)

AT&R <enter>

Example

Input:
AT&R <enter>
Response:
OK

5.0 AT Command Line Interface

AT&V

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

Example

Input:
AT&V <enter>
Response:
&V:
  hostname:pX2
  timezone:MST7MDT,M3.2.0,M11.1.0
  systemmode:gateway
  time mode:local
OK

AT&W

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

Example

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

ATA

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

Example

Input:
ATA <enter>
Response:
OK
PX2 Login:

5.0 AT Command Line Interface

ATO

Description

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

Command Syntax (Effect: Immediate)

ATO <enter>

Example

Input:
ATO <enter>
Response:
OK
PX2 Login:

AT+MSCNTO

Description

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

Command Syntax (Effect: AT&W)

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

Example

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

AT+MSPWD

Description

Used to set or change the ADMIN password.

Command Syntax (Effect: Immediate)

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

Example

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

5.0 AT Command Line Interface

AT+MSGMI

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

Example

Input:
AT+MSGMI<enter>

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

AT+MSSYSI

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

Example

Input:
AT+MSSYSI <enter>
Response:
Ethernet Port:
  MAC:00:0F:92:02:8A:41
  IP:192.168.221.222
  MASK:255.255.255.0
  Wan MAC:00:00:00:00:00:00
  Wan IP:0.0.0.0
  Wan MASK:0.0.0.0
System:
  Device:pX22
  Product:pX2
  Image:PWii
  Hardware:Rev A
  Software:v1.3.0 build 1007-13

Copyright: 2014-2015 Microhard Systems Inc.
Time: Mon Sep 21 15:28:58 2015

5.0 AT Command Line Interface

AT+MSGMR

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

Example

Input:
AT+MSGMR <enter>
Response:
+MSGMR:
 Hardware Version:Rev A Software Version:v1.3.0 build 1007-13
 Copyright: 2014-2015 Microhard Systems Inc.
 System Time: Mon Sep 21 15:30:06 2015
OK

AT+MSMNAME

Description	Command Syntax (Effect: AT&W)
Modem Name / Radio Description. 30 chars.	**AT+MSMNAME=<modem_name>**

Example

Input: (To set value)
AT+MSMNAME=PX2_CLGY<enter>
Response:
OK

Input: (To retrieve value)
AT+MSMNAME?<enter>
Response:
Host name:pX22
OK

AT+MSRTF

Description	Command Syntax (Effect: Immediate)
Reset the modem to the factory default settings from non-volatile memory.	**AT+MSRTF=<Action>** Action: 0 pre-set action 1 confirm action

Example

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

5.0 AT Command Line Interface

AT+MSREB

Description	Command Syntax (Effect: Immediate)
Reboot the pX2.	**AT+MSREB <enter>**

Example

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

AT+MSNTP

Description	Command Syntax (Effect: AT&W)
Get/Set NTP Server.	**AT+MSNTP=<status>[,<NTP server>[.<Port>]]** Status: 0 Local Time 1 NTP

Example

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

AT+MSSYSLOG

Description	Command Syntax (Effect: AT&W)
Get/Set syslog server	**AT+MSSYSLOG=<Server>[,<Port>]** Server : Valid IP Address or Name. 0.0.0.0 - Disable. 1 to 256 characters Port: 1 to 65535. Default is 514

Example

Input:
AT+MSSYSLOG=192.168.168.35,514<enter>
Response:
OK

Input:
AT+MSSYSLOG?
Response:
Syslog Server : 192.168.168.35
Syslog Port : 514
OK

5.0 AT Command Line Interface

AT+MNLAN

Description

Show/Add/Edit/Delete the network interface.

Command Syntax (Effect: AT&W)

AT+MNLAN
AT+MNLAN=<LAN Name>
AT+MNLAN=<LAN Name>,DEL
AT+MNLAN=<LAN Name>,ADD/EDIT,<Protocol>[,<IP>,<Netmask>[,<Gateway>,<DNS>[,<STP>]]]
Where <Protocol>=0
AT+MNLAN=<LAN Name>,ADD/EDIT,<Protocol>[,<STP>[,Route]]
Where <Protocol>=1
AT+MNLAN=<LAN Name>,EDIT,<Protocol>[,<IP>,<Netmask>[,<STP>[,Route]]]
Where <Protocol>=2 and <LAN Name>="lan"

Parameters:

LAN Name:	Name of Network LAN interface
Operation:	ADD - Add a new LAN interface
	EDIT - Edit an exsiting LAN interface
	DEL - Delete an existing LAN interface
Protocol:	0 - Static IP
	1 - DHCP with LAN alias disabled
	2 - DHCP with LAN alias enabled, for "lan"
IP Address:	Valid IP address
Netmask:	Valid netmask
Gateway:	Valid IP address. 0 - Reset gateway
DNS:	Valid IP address. 0 - Reset DNS
STP:	0 - Spanning Tree Off
	1 - Spanning Tree On
Route:	0 - No
	1 - Yes

Example

Input:
AT+MNLAN?
Response:
1. lan: [static], [192.168.168.1/255.255.255.0], LAN DHCP [On], STP [off]
OK

5.0 AT Command Line Interface

AT+MNLANDHCP

Description

Get/Set LAN DHCP server running on the Ethernet interface.

Command Syntax (Effect: AT&W)

AT+MNLANDHCP=<LAN Name>[,<Mode>[,<Start IP>, <Limit>[,<Lease Time>,<Alt. Gateway>, <Pre. DNS>, <Alt. DNS>,<WINS/NBNS Servers>,<WINS/NBT Node>]]]

LAN Name: Name of Network LAN interface
Mode: 0 - Disable DHCP Server
1 - Enable DHCP Server
Start IP: The starting address DHCP assignable IP Addresses
Limit: The maximum number of IP addresses. min=0 max=16777214
Lease Time: The DHCP lease time in minutes. min=0 max=214748364
Alt. Gateway: Alternate Gateway for DHCP assigned devices if the default gateway is not to be used
Pre. DNS: Preferred DNS server address to be assigned to DHCP devices
Alt. DNS: Alternate DNS server address to be assigned to DHCP devices
WINS/NBNS Server : WINS/NBNS Servers
WINS/NBT Node : WINS/NBT Node Type
0 - none
1 - b-node
2 - p-node
3 - m-node
4 - h-node

Example

Input:
AT+MNLANDHCP=lan<enter>
Response:

```
 LAN Name      : lan
 Mode          : 1 - DHCP Server enabled
 Start IP      : 192.168.168.100
 Limit         : 150
 Lease Time    : 720m
 Alt. Gateway  :
 Pre. DNS      :
 Alt. DNS      :
 WINS/NBNS Server :
 WINS/NBT Node : 0 - none
OK
```

5.0 AT Command Line Interface

AT+MNWAN

Description

Show/Add/Edit/Delete the WAN interface.

Command Syntax (Effect: AT&W)

AT+MNWAN=<Mode>[,<Protocol>[,<Route>][,<IP>,<Netmask>[,<Gateway>]]]
Usage:
AT+MNWAN
AT+MNWAN=<Mode>,<Protocol>,<Route>,<IP>,<Netmask>[,<Gateway>]
Where <Mode>=0 and <Protocol>=0
AT+MNWAN=<Mode>,<Protocol>,<Route>
Where <Mode>=0 and <Protocol>=1
AT+MNWAN=<Mode>
Where <Mode>=1
AT+MNWAN=<Mode>,<Protocol>,<IP>,<Netmask>[,<Gateway>]
Where <Mode>=2 and <Protocol>=0
AT+MNWAN=<Mode>,<Protocol>
Where <Mode>=2 and <Protocol>=1
Parameters:
Mode: 0 - Independent WAN
1 - Bridge with LAN Port
2 - Independent LAN
Protocol: 0 - Static IP
1 - DHCP
IP: Valid IP address
Netmask: Valid netmask
Gateway: Valid IP address. 0 - Reset
Route: Default Route
0 - No
1 - Yes

Example

Input:
AT+MNWAN?
Response:

```
Working Mode     : Independent WAN
WAN Configuration
 Connection Type : Static IP
  IP Address     : 10.10.10.254
  Netmask        : 10.10.10.10.1
  Default Gateway: 255.255.255.252
 DefaultRoute    : No
DNS Server
 Mode            : manual
  Primary DNS    :
  Secondary DNS  :
OK
```

5.0 AT Command Line Interface

AT+MNWANDNS

Description

Get/Set DNS Server when WAN set to independent WAN.

Command Syntax (Effect: AT&W)

AT+MNWANDNS=[<Mode>[,<Primary DNS>,<Secondary DNS>]]

Parameters:
Mode : 0 - Auto
1 - Manual
Primary DNS : Valid IP Address
Secondary DNS : Valid IP address

AT+MNWANLANDHCP

Description

Get/Set LAN DHCP when WAN set to Independent LAN

Command Syntax (Effect: AT&W)

AT+MNWANLANDHCP=[<Mode>[,<Start IP>,<Limit>,<Lease Time>[,<Alt.Gateway>,<Pre.DNS>,<Alt.DNS>]]]
Usage:
AT+MNWANLANDHCP
AT+MNWANLANDHCP=<Mode>
Where <Mode>=0
AT+MNWANLANDHCP=<Mode>,<Start IP>,<Limit>,<Lease Time>[,<Alt.Gateway>,<Pre.DNS>,<Alt.DNS>] Where <Mode>=1
Parameters:
Mode : 0 - Disable DHCP Server
1 - Enable DHCP Server
Start IP : The starting address DHCP assignable IP Addresses
Limit : The maximum number of IP addresses. min=0 max=16777214
Lease Time : The DHCP lease time in minutes. min=0 max=214748364
Alt. Gateway : Alternate Gateway for DHCP assigned devices if the default gateway is not to be used
Pre. DNS : Preferred DNS server address to be assigned to DHCP devices
Alt. DNS : Alternate DNS server address to be assigned to DHCP devices

Example

Input:
AT+MNWANLANDHCP?
Response:
Mode : 1 - DHCP Server enabled
Start IP :
Limit :
Lease Time :
Alt. Gateway :
Pre. DNS :
Alt. DNS :
OK

5.0 AT Command Line Interface

AT+MNIPMAC

Description

Show/Add/Delete/Release/ReleaseAll the MAC-IP Address binding.

Command Syntax (Effect: AT&W)

AT+MNIPMAC=<Operation>[,<Name>[,<IP Address>,<MAC Address>]]
Operation: SHOW - Show the details of the MAC-IP address binding
ADD - Add a new MAC-IP address binding
DEL - Delete an existing MAC-IP address binding
RELEASE - Release the active DHCP lease
RELEASEALL - Release all active DHCP leases
Name: Name of the MAC-IP binding
IP Address : Valid IP address
MAC Address: The physical MAC address of the device or interface
Usage:
AT+MNIPMAC
AT+MNIPMAC=SHOW,<Name>
AT+MNIPMAC=ADD,<Name>,<IP Address>,<MAC Address>
AT+MNIPMAC=DEL,<NAME>
AT+MNIPMAC=RELEASE,<NAME>
AT+MNIPMAC=RELEASEALL

Example

Input:
AT+MNIPMAC=add,PC,192.168.168.150,0A0B0C0D0E0F<enter>
Response:
OK

Input:
AT+MNIPMAC?
Response:
1: PC, 192.168.168.150, 0A0B0C0D0E0F, Not active
OK

Input:
AT+MNIPMAC=RELEASEALL<enter>
Response:
Network DHCP server is restarted.
OK

5.0 AT Command Line Interface

AT+MNEMAC

Description

Retrieve the MAC Address of the local Ethernet interface.

Command Syntax

AT+MNEMAC <enter>

Example

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

AT+MNPORT

Description

Get/set the Ethernet port configuration.

Command Syntax (Effect: AT&W)

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

Ethernet Port:	0 - WAN
	1 - LAN
Mode:	0 - Auto
	1 - Manual
Auto-Neg:	0 - Off
	1 - On
Speed:	0 - 10
	1 - 100
Duplex:	0 - Full
	1 - Half

Example

Input:
AT+MNPORT<enter>
Response:
0: LAN1: Mode: auto
1: LAN2: Mode: auto
OK

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

5.0 AT Command Line Interface

AT+MCPS2

Description

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

Command Syntax (Effect: AT&W)

AT+MCPS2=<Mode>
Mode:
0 Console
1 Data

Example

Input:
AT+MCPS2=0<enter>
Response:
OK

AT+MCBR2

Description

Get/Set Serial port baud rate.

Command Syntax (Effect: AT&W)

AT+MCBR2=<Baud Rate>
Baud Rate:
0 300
1 600
2 1200
3 2400
4 3600
5 4800
6 7200
7 9600
8 14400
9 19200
10 28800
11 38400
12 57600
13 115200
14 230400
15 460800
16 921600

Example

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

AT+MCDF2

Description

Get/Set Serial port data format

Command Syntax (Effect: AT&W)

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

Example

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

5.0 AT Command Line Interface

AT+MCDM2

Description	Command Syntax (Effect: AT&W)
Set Serial port data mode.	**AT+MCDM2=<Data Mode>** Data Mode: 0 Seamless 1 Transparent

Example

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

AT+MCCT2

Description	Command Syntax (Effect: AT&W)
Set Comport character timeout.	AT+MCCT2=<timeout_s> (0 to 65535 seconds)

Example

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

AT+MCMPS2

Description	Command Syntax (Effect: AT&W)
Get/Set Serial port maximum packet size.	**AT+MCMPS2=<size>** size: 0 to 65535

Example

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

5.0 AT Command Line Interface

AT+MCNCDI2

Description

Enable/Disable Serial port no-connection data intake.

Command Syntax (Effect: AT&W)

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

Example

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

AT+MCMTC2

Description

Get/Set Serial port modbus TCP configuration.

Command Syntax (Effect: AT&W)

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

Example

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

AT+MCIPM2

Description

Set the Serial port IP Protocol Mode.

Command Syntax (Effect: AT&W)

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

Example

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

5.0 AT Command Line Interface

AT+MCTC2

Description

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

Command Syntax (Effect: AT&W)

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

Example

Input:
AT+MCTC2=0.0.0.0,20002,60<enter>
Response:
OK

AT+MCTS2

Description

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

Command Syntax (Effect: AT&W)

AT+MCTS2=<Local Listener Port>,<Connection timeout_s>
Local Listener Port : 1 to 65535
Connection timeout_s: 0 to 65535

Example

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

AT+MCTCS2

Description

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

Command Syntax (Effect: AT&W)

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

Example

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

5.0 AT Command Line Interface

AT+MCUPP2

Description

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

Command Syntax (Effect: AT&W)

AT+MCUPP2=<Remote IP>,<Remote Port>,<Listener Port>
Remote IP : valid IP address
Remote Port : 1 to 65535
Listener Port: 1 to 65535

Example

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

AT+MCSMTP2

Description

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

Command Syntax (Effect: AT&W)

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

5.0 AT Command Line Interface

AT+MCPPP2

Description

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

Command Syntax (Effect: AT&W)

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

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

Example

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

5.0 AT Command Line Interface

AT+MAEURD1
AT+MAEURD2
AT+MAEURD3

Description

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

Example

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

Command Syntax (Effect: AT&W)

AT+MAEURD1=<Mode>[,<Remote IP>,<Remote Port>,<Interval Time> [,Interfaces]]
Mode : 0 Disable
1 Modem Event Report
2 SDP Event Report
3 Management Report
Remote IP : valid IP address
Remote Port : 0 to 65535
Interval Time: 0 to 65535 seconds
Interfaces : (optional) 0 Disable; 1 Enable Modem, Carrier and WAN for Modem Event Report. For instant, "1,1,1" to enable all interfaces Ethernet, Carrier, USB, COM and IO for Management Report. For instant, "0,0,0,0,0" to disable all interfaces

AT+MANMSR

Description

Define NMS Report.

Example

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

Command Syntax (Effect: AT&W)

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

AT+MANMSRV

Description

Get/Set NMS Server.

Example

Input:
AT+MANMSSRV=nms.microhardcorp.com,mytech,mypassword,mypassword
Response:
OK

Command Syntax (Effect: AT&W)

AT+MANMSSRV[=<Server>, <Name>, <Password>, <Confirm Password>]
<Server>:
NMS Server/IP. 1 to 63 characters
<Name>:
Domain Name. 1 to 63 characters
<Password>:
Domain Password. 5 to 63 characters
<Confirm Password>:
Same as <Password>. 5 to 3 characters

5.0 AT Command Line Interface

AT+MAWSCLIENT

Description

Get/Set Web Service Client.

Command Syntax (Effect: AT&W)

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

Example

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

AT+MADISS

Description

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

Command Syntax (Effect: AT&W)

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

Example

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

5.0 AT Command Line Interface

AT+MASNMP

Description

Get/Set SNMP service.

Command Syntax (Effect: AT&W)

AT+MASNMP[=<Mode>[,<ROCommunity>,<RWCommunity>,<Port>,<Version>]]
Mode: 0 - Disable
1 - Enable
ROCommunity: Read Only Community Name 1 to 31 characters
RWCommunity: Read Write Community Name 1 to 31 characters
Port: Listening Port 0 to 65535. Default is 161
Version: SNMP version
1 - Version 1
2 - Version 2
3 - Version 3 (Use AT+MASNMPV3 to set Authentication and Privacy parameters)

Example

Input:
AT+MASNMP=1,public,private,161,2<enter>
Response:
OK

AT+MASNMPTRAP

Description

Get/Set SNMP trap.

Command Syntax (Effect: AT&W)

AT+MASNMPTRAP[=<Mode>[,<Name>,<IP>[,<AuthFailureTraps>]]
<Mode>:
0 - Disable
1 - Enable
<Name>:
Trap Community Name. 1 to 63 characters
<IP>:
Trap Manage Host IP. Default 0.0.0.0 (Disable)
<AuthFailureTraps>:
0 - Disable
1 - Enable
Usage:
AT+MASNMPTRAP
AT+MASNMPTRAP=0
AT+MASNMPTRAP=1[,<Name>,<IP>[,<AuthFailureTraps>]]

5.0 AT Command Line Interface

AT+MAATH

Description

Get/Set Authentication configuration.

Examples

Input:
AT+MAAUTH?
Response:
+MAAUTH:
  Mode : 1 - Local&RADIUS
  ServerIP : 8.8.8.8
  ServerPort : 1812
  SharedSecret : test
OK

Input:
AT+MAAUTH=0
Response:
OK

Input:
AT+MAAUTH
Response:
+MAAUTH:
  Mode : 0 - Local
OK

Command Syntax (Effect: AT&W)

AT+MAAUTH[=<Mode>,<ServerIP>,<ServerPort>[,<SharedSecret>]]
<Mode>:
  0 - Local
  1 - Local&RADIUS
<ServerIP>:
  Remote Server IP Address
<ServerPort>:
  Remote Server IP Port. 0 to 65535. Default is 1812
<SharedSecret>:
  0 to 63 characters
Usage:
  AT+MAAUTH
  AT+MAAUTH=0
  AT+MAAUTH=1[,<ServerIP>,<ServerPort>[,<SharedSecret>]]

5.0 AT Command Line Interface

AT+MASNMPV3

Description

Get/Set SNMP version 3.

Command Syntax (Effect: AT&W)

AT+MASNMPV3=<UserName>,<RWLimit>,<AuthLevel>[,<Auth>,<AuthPassword> <Privacy> [,<PrivacyPassword>]]
UserName: V3 User Name 1 to 31 characters
RWLimit: V3 User Read Write Limit
0 - Read Only
1 - Read Write
AuthLevel: V3 User Authentication Level
0 - NoAuthNoPriv
1 - AuthNoPriv
2 - AuthPriv
Auth: V3 Authentication Protocol
0 - MD5
1 - SHA
AuthPassword: V3 Authentication Password 1 to 255 characters
Privacy: V3 Privacy Protocol
0 - DES
1 - AES
PrivacyPassword: V3 Privacy Password 1 to 255 characters
Usage:
AT+MASNMPV3=<UserName>,<RWLimit>,0 If <AuthLevel>=0 (NoAuthNoPriv)
AT+MASNMPV3=<UserName>,<RWLimit>,1,<Auth>,<AuthPassword> If <AuthLevel>=1 (AuthNoPriv)
AT+MASNMPV3=<UserName>,<RWLimit>,2,<Auth>,<AuthPassword>,<Privacy>,<PrivacyPassword> If <AuthLevel>=2 (AuthPriv)

Example

Input:
AT+MASNMPV3 <enter>
Response:
+MASNMPV3:
UserName : userV3
RWLimit : Read Only
AuthLevel : NoAuthNoPriv
OK

5.0 AT Command Line Interface

AT+MWRADIO

Description

Get/Set radio status, on or off.

Example

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

Command Syntax (Effect: AT&W)

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

AT+MWMODE

Description

Get/Set radio mode.

Example

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

Command Syntax (Effect: AT&W)

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

AT+MWTXPOWER

Description

Get/Set radio TX Power.

Example

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

Command Syntax (Effect: AT&W)

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

5.0 AT Command Line Interface

AT+MWDISTANCE

Description

Get/Set radio Wireless Distance.

Example

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

Command Syntax (Effect: AT&W)

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

AT+MWCHAN

Description

Set radio channel

Example

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

Command Syntax (Effect: AT&W)

AT+MWCHAN=<Channel>
Available radio channels for mode 11ng and high throughput mode HT20:
0 - auto
1 - 1
2 - 2
3 - 3
4 - 4
5 - 5
6 - 6
7 - 7
8 - 8
9 - 9
10 - 10
11 - 11

AT+MWHTMODE

Description

Get/Set radio high throughput mode.

Example

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

Command Syntax (Effect: AT&W)

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

5.0 AT Command Line Interface

AT+MWMPDUAGG

Description

Get/Set radio MPDU Aggregation.

Command Syntax (Effect: AT&W)

AT+MWMPDUAGG=<MPDU Aggregation>
MPDU Aggregation:
0 - Disable
1 - Enable

Example

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

AT+MWSHORTGI

Description

Get/Set radio short GI

Command Syntax (Effect: AT&W)

AT+MWSHORTGI=<Short GI>
Short GI:
0 - Disable
1 - Enable

Example

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

AT+MWHTCAPAB

Description

Get Radio HT Capabilities Info

Command Syntax

AT+MWHTCAPAB

Example

Input:
AT+MWHTCAPAB <enter>
Response:
+MWHTCAPAB: HT Capabilities Info -
OK

5.0 AT Command Line Interface

AT+MWAMSDU

Description

Get radio maximum AMSDU (byte).

Command Syntax

AT+MWAMSDU

Example

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

OK

AT+MWAMPDU

Description

Get radio maximum AMPDU (byte).

Command Syntax

AT+MWAMPDU

Example

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

OK

5.0 AT Command Line Interface

AT+MWRTSTHRESH

Description

Get/Set radio RTS Threshold.

Command Syntax (Effect: AT&W)

AT+MWRTSTHRESH=<RTS Threshold>
RTS Threshold:

0	Disabled
256-2346	Enabled with the value

Example

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

AT+MWFRAGTHRESH

Description

Get/Set radio Fragment Threshold.

Command Syntax (Effect: AT&W)

AT+MWFRAGTHRESH=<Fragmentation Threshold>
Fragmentation Threshold:

0	Disabled
256-2346	Enabled with the value

Example

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

AT+MWCCATHRESH

Description

Get/Set radio CCA Threshold.

Command Syntax (Effect: AT&W)

AT+MWCCATHRESH=<CCA Threshold>
CCA Threshold:
Range of values: 4-127

Example

Input:
AT+MWCCATHRESH=28 <enter>
Response:
OK

5.0 AT Command Line Interface

AT+MWIFACE

Description

List/Add/Delete radio virtual interface.

Example

Input:
AT+MWIFACE=0 <enter>
Response:
Radio Virtual Interface [0]:
  Network : lan
  Mode : ap
  TX bitrate : auto
  ESSID Broadcast : Off
  AP Isolation : Off
  SSID : PWii
  Encryption Type : psk2
  WPA PSK : 1234567890
OK

Command Syntax (Effect: AT&W)

List one or all radio virtual interface(s) :
AT+MWIFACE=0[,<Index>]
Add one radio virtual interface :
AT+MWIFACE=1
Delete one radio virtual interface :
AT+MWIFACE=2,<Index>
Index:
Radio Virtual Interface Index: 0-3

AT+MWNETWORK

Description

Get/Set radio virtual interface: Network

Example

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

Command Syntax (Effect: AT&W)

AT+MWNETWORK=[<Index>[,<Network>]]
Index:
  Radio Virtual Interface Index: 0-3
Network:
  Radio Virtual Interface Network:
    0 - LAN
    1 - lan1

AT+MWSSID

Description

Get/Set radio virtual interface: SSID

Example

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

Command Syntax (Effect: AT&W)

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

5.0 AT Command Line Interface

AT+MWDEVICEMODE

Description

Get/Set radio virtual interface: Mode

Example

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

Command Syntax (Effect: AT&W)

AT+MWDEVICEMODE=[<Index>[,<Device Mode>]]
Index:
  Radio Virtual Interface Index: 0-3
Device Mode:
  Radio Virtual Interface Mode:
    0 - Access Point
    1 - Client
    2 - Repeater

AT+MWRATE

Description

Get/Set radio virtual interface: TX bit rate

Example

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

Command Syntax (Effect: AT&W)

AT+MWRATE=[<Index>[,<TX bitrate>]]
Index:
  Radio Virtual Interface Index: 0-3
TX bitrate:
  Radio Virtual Interface TX bitrate:
    0 - auto
    1 - mcs-0
    2 - mcs-1
    3 - mcs-2
    4 - mcs-3
    5 - mcs-4
    6 - mcs-5
    7 - mcs-6
    8 - mcs-7
    9 - mcs-8
    10 - mcs-9
    11 - mcs-10
    12 - mcs-11
    13 - mcs-12
    14 - mcs-13
    15 - mcs-14
    16 - mcs-15

5.0 AT Command Line Interface

AT+MWSSIDBCAST

Description

Get/Set radio virtual interface: ESSID Broadcast.

Example

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

Command Syntax (Effect: AT&W)

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

AT+MWAPISOLATION

Description

Get/Set radio virtual interface: AP Isolation

Example

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

Command Syntax (Effect: AT&W)

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

5.0 AT Command Line Interface

AT+MWENCRYPT

Description

Get/Set radio virtual interface: Encryption Type

Example

Input:
AT+MWENCRYPT=0,1,#microhard123 <enter>
Response:
OK

Input:
AT+MWENCRYPT> <enter>
Response:
+MWENCRYPT: Virtual Interface 0:
Encryption Type: 1 - WPA (PSK)
Password: #microhard123
OK

Command Syntax (Effect: AT&W)

For PSK, **AT+MWENCRYPT=[<Index>, [<Encryption Type>[,<PSK Password>]]]**

For RADIUS, **AT+MWENCRYPT=[<Index>, [<Encryption Type>[,<RADIUS Server Key> [,<RADIUS IP Address>,<RADIUS Port>]]]]**

<Index>
Radio Virtual Interface Index: 0-3
<Encryption Type>
Radio Virtual Interface Encryption Type:
0 - Disabled
1 - WPA (PSK)
2 - WPA2 (PSK)
3 - WPA+WPA2 (PSK)
4 - WPA Enterprise (RADIUS)
5 - WPA2 Enterprise (RADIUS)
6 - WPA+WPA2 Enterprise (RADIUS)
<PSK Password>:
Min 8 characters, Max 63 characters
<RADIUS Server Key>:
Min 4 characters, Max 63 characters
<RADIUS IP Address>:
Valid IP address
<RADIUS Port>:
Valid port 0 - 65535

AT+WSCAN

Description

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

Example

Input:
AT+WSCAN <enter>
Response:
Varies

Command Syntax

AT+WSCAN <enter>

5.0 AT Command Line Interface

AT+MWRSSI

Description

Get radio (WIFI) RSSI.

Command Syntax

AT+MWRSSI <enter>

Example

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

5.0 AT Command Line Interface

ATL

Description

Lists all available AT Commands.

Command Syntax

ATL <enter>

Example

```
ATL <enter>

AT Commands available:
pX2-Test> ?
  Help                  Show available commands
  History               Show a list of previously run commands
  Info                  System info
  Status                Display the system status
  System                Setting system configurations
  Network               Set or Get network config
  AT                    AT Echo OK
  ATE0                  Disable Echo
  ATE1                  Enable Echo
  AT+TEST               AT Echo TEST
  ATH                   Show a list of previously run AT commands
  ATL                   List all available AT commands
  AT&R                  Reserved
  AT&V                  Display modem active profile
  AT&W                  Enable configurations you have been entered
  ATA                   Quit
  ATO                   Quit
  AT+MSCNTO             Get/Set console timeout
  AT+MSPWD              Set password
  AT+MSGMI              Get manufacturer Identification
  AT+MSSYSI             Get system summary information
  AT+MSGMR              Get modem Record Information
  AT+MSMNAME            Get/Set modem Name Setting
  AT+MSRTF              Reset the modem to the factory default settings of  from non-volatile (NV) memory
  AT+MSREB              Reboot the modem
  AT+MSNTP              Get/Set NTP server
  AT+MSSYSLOG           Get/Set syslog server
  AT+MNLAN              Show/Add/Edit/Delete the network LAN interface
  AT+MNLANDHCP          Get/Set LAN DHCP server running on the Ethernet interface
  AT+MNIPMAC            Show/Add/Delete/Release/ReleaseAll the MAC-IP address binding
  AT+MNEMAC             Get the MAC address of local Ethernet interface
  AT+MNPORT             Get/set the Ethernet port configuration
  AT+MCPS2              Get/Set Serial port
  AT+MCBR2              Get/Set Serial port baud rate
  AT+MCDF2              Get/Set Serial port data format
  AT+MCDM2              Get/Set Serial port data mode
  AT+MCCT2              Get/Set Serial port character timeout
  AT+MCMPS2             Get/Set Serial port maximum packet size
  AT+MCNCDI2            Get/Set Serial port no-connection data intake
  AT+MCMTC2             Get/Set Serial port modbus tcp configuration
  AT+MCIPM2             Get/Set Serial port IP protocol mode  AT+MCTC2 Get/Set Serial port tcp client
                        configuration when IP protocol mode is TCP Client
  AT+MCTS2              Get/Set Serial port tcp server configuration when IP protocol mode is TCP Server
  AT+MCTCS2             Get/Set Serial port tcp client/server configuration when IP protocol mode is TCP Client/
                        Server
  AT+MCUPP2             Get/Set Serial port UDP point to point configuration when IP protocol mode is UDP point
                        to point
  AT+MCSMTP2            Get/Set Serial port SMTP client configuration when IP protocol mode is SMTP client
  AT+MCPPP2             Get/Set Serial port PPP configuration when IP protocol mode is PPP
  AT+MAEURD1            Get/Set Event UDP Report No.1
  AT+MAEURD2            Get/Set Event UDP Report No.2
  AT+MAEURD3            Get/Set Event UDP Report No.3
```

Continued...

5.0 AT Command Line Interface

AT+MANMSR	Get/Set NMS Report
AT+MADISS	Get/Set discovery service used by the modem
AT+MAWSCLIENT	Get/Set Web service client
AT+MASNMP	Get/Set SNMP service
AT+MASNMPV3	Get/Set SNMP Version 3
AT+MWRADIO	Get/Set radio status, On or Off
AT+MWMODE	Get/Set radio mode
AT+MWTXPOWER	Get/Set radio Tx power
AT+MWDISTANCE	Get/Set radio Wireless Distance
AT+MWCHAN	Get/Set radio channel
AT+MWHTMODE	Get/Set radio high throughput mode
AT+MWMPDUAGG	Get/Set radio MPDU Aggregation
AT+MWSHORTGI	Get/Set radio short GI
AT+MWHTCAPAB	Get radio HT Capabilities Info
AT+MWAMSDU	Get radio maximum AMSDU (byte)
AT+MWAMPDU	Get radio maximum AMPDU (byte)
AT+MWRTSTHRESH	Get/Set radio RTS Threshold
AT+MWFRAGTHRESH	Get/Set radio Fragment Threshold
AT+MWCCATHRESH	Get/Set radio CCA Power Threshold
AT+MWIFACE	List/Add/Delete radio virtual interface
AT+MWNETWORK	Get/Set radio virtual interface: Network
AT+MWSSID	Get/Set radio virtual interface: SSID
AT+MWDEVICEMODE	Get/Set radio virtual interface: Mode
AT+MWRATE	Get/Set radio virtual interface: TX bitrate
AT+MWSSIDBCAST	Get/Set radio virtual interface: ESSID Broadcast
AT+MWAPISOLATION	Get/Set radio virtual interface: AP Isolation
AT+MWENCRYPT	Get/Set radio virtual interface: Encryption Type
AT+MWSCAN	Get radio scanning information
AT+MWRSSI	Get radio RSSI

6.0 Installation

The are a number of factors to consider when preparing to deploy a radio network, several of which have been touched-upon or detailed elsewhere within this manual. Following is a listing of a number of factors, in no particular order:

The installation, removal, or maintenance of any antenna system components must be undertaken only by qualified and experienced personnel.

Network Topology

The pX2 currently supports Access Point (AP), Repeater, and Client/Station modes which can create either Point to Multipoint or Point to Point topologies.

Throughput

The pX2 is capable of up to a link rate of 150 Mbps. The network topology has an effect on how this available throughput is 'shared' between all nodes on the network.

Distance

The physical distance between the modems dictates such things as required antenna performance and heights. When contemplating antenna types, keep in mind the directivity (omnidirectional or directional) of the antennas being used.

Terrain

Along with distance, the terrain is a very important consideration with respect to antenna height requirements. The term 'line-of-sight' (LOS) refers to being able to 'see' one location from another - a minimum requirement for a radio signal path. In addition to LOS, adequate clearance must also be provided to satisfy 'Fresnel Zone' requirements - an obstruction-free area much greater than the physical LOS, i.e. LOS is not enough to completely satisfy RF path requirements for a robust communications link.

Transmit Power

Having read thus far through the factors to be considered, it should be clear that they are all interrelated. Transmit power should be set for the minimum required to establish a reliable communications path with adequate fade margin. Required transmit power is dictated primarily by distance, antenna type (specifically the 'gain' of the antennas being used), and the receive sensitivity of the distant modem. Cable and connector losses (the physical path from the modem's 'antenna connector' to the antenna's connector) must also be taken into account.

Receive Sensitivity

The Pico Series has exceptional receive sensitivity, which can produce a number of benefits, such as: added fade margin for a given link, being able to use less expensive coaxial cable or antenna types, being able to operate at greater distances for a given distant transmitter power (perhaps negating the requirement for a Repeater site!). Distance, antenna gain, transmit power, and receive sensitivity are critical 'numbers' for radio path calculations. Fortunately, the Pico Series features the maximum available transmit power combined with exceptional receive sensitivity - two 'numbers' which will produce the most favorable path calculation results.

6.0 Installation

Fade Margin

When all radio path numbers are being considered and hardware assumptions are being made, another factor to consider is the 'fade margin' of the overall system. The fade margin is the difference between the anticipated receive signal level and the minimum acceptable receive level (receive sensitivity). Being that the Pico Series performs to exacting specifications, the overall deployment should be such that the modems may be utilized to their full potential to provide a reliable and robust communications link. A typical desired fade margin is in the order of 20dB, however oftentimes a 10dB fade margin is acceptable.

Frequency

The 900MHz frequency range is not effected by rain to any significant degree, and is also able to penetrate through foliage and 'around obstacles' to a certain degree. This being the case, some may choose to scrimp on the physical deployment, particularly when it comes to antenna (tower) heights. Path calculations provide results which specify 'required' antenna heights. For cost savings and in taking advantage of the characteristics of the frequency range, sometimes the height requirements are not adhered to: this may result in unreliable communications.

Power Requirements

The Pico Series may be integrated into a system (Development Board, or custom) which accepts a range of DC input voltages (supply current requirements must also be met). In some deployments, power consumption is critical. A number of features related to minimizing power consumption are available with the pX2 such the ability to operate at lower transmit power given the receive sensitivity of the distant modem.

Interference

The frequency hopping spread spectrum (FHSS) operation of the Pico Series most often allows it to work well in an environment within which there may be sources of in-band interference. Frequency Restriction (Hopping Zones) is a built-in feature which may be utilized to avoid specific frequencies or ranges of frequencies; the Spectrum Analyzer function may be used to identify areas of potential interference. Cavity filters are also available if required: contact Microhard Systems Inc. for further information.

6.0 Installation

6.1 Path Calculation

FCC regulations allow for up to 36dBi effective isotropic radiated power (EIRP). The sum (in dBm) of the transmitted power, the cabling loss, and the antenna gain cannot exceed 36dBi.

Assuming adequate antenna heights, a basic formula to determine if an adequate radio signal path exists (i.e. there is a reasonable fade margin to ensure reliability) is:

Fade Margin = System Gain - Path Loss

where all values are expressed in dB.

As discussed on the previous page, a desired fade margin is 20dB.

System gain is calculated as follows:

System Gain = Transmitter Power + (Transmitter Antenna Gain - Transmitter Cable and Connector Losses) + (Receiver Antenna Gain - Receiver Cable and Connector Losses) + | Receiver Sensitivity |.

where all values are expressed in dB, dBi, or dBm, as applicable.

Assuming a path loss of 113dB for this example, the fade margin = 143-113 = 30dB.
30dB exceeds the desired fade margin of 20dB, therefore this radio communications link would be very reliable and robust.

On the following page are examples of actual path loss measurements taken in an open rural environment; the path loss numbers do not apply to urban or non-LOS environments.

Example:

Tx power = 30dBm
Tx antenna gain = 6dBi
Tx cable/connector loss = 2dB
Rx antenna gain = 3dBi
Rx cable/connector loss = 2dB
Rx sensitivity = -108dBm

System Gain = [30+(6-2)+(3-2)+108]dB
= [30+4+1+108]dB
= 143dB.

6.0 Installation

Distance (km)	Master Height (m)	Remote Height (m)	Path Loss (dB)
5	15	2.5	116.5
5	30	2.5	110.9
8	15	2.5	124.1
8	15	5	117.7
8	15	10	105
16	15	2.5	135.3
16	15	5	128.9
16	15	10	116.2
16	30	10	109.6
16	30	5	122.4
16	30	2.5	128.8

Table 6-1: Path Loss

To satisfy FCC radio frequency (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, operation at less than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

Never work on an antenna system when there is lightning in the area.

6.2 Installation of Antenna System Components

The installation, removal, or maintenance of any antenna system components must be undertaken only by qualified and experienced personnel.

6.2.1 Antennas

The two most common types of antenna are the omnidirectional ('omni') and directional (Yagi).

An **omni** typically has 3-6dBi gain and spreads its energy in all directions (hence the name 'omnidirectional'). The 'pattern' of the energy field is in the shape of a donut, with the antenna mounted vertically at the centre. This vertical-mounted antenna produces a signal which is vertically 'polarized'.

A **Yagi** has a more focused antenna pattern, which results in greater gain: commonly, 6-12dBi. The pattern of a Yagi is in the shape of a large raindrop in the direction in which the antenna is pointed. If the elements of the Yagi are perpendicular to the ground (most common orientation) the radiated signal will be vertically polarized; if parallel to the ground, the polarization is horizontal.

The network topology, application, and path calculation are all taken into consideration when selecting the various antenna types to be used in a radio network deployment.

6.0 Installation

6.2.2 Coaxial Cable

The following types of coaxial cable are recommended and suitable for most applications (followed by loss at 2.4GHz, in dB, per 100 feet):

- LMR 195 (10.7)
- LMR 400 (3.9)
- LMR 600 (2.5)

For a typical application, LMR 400 may be suitable. Where a long cable run is required - and in particular within networks where there is not a lot of margin available - a cable with lower loss should be considered.

When installing cable, care must be taken to not physically damage it (be particularly careful with respect to not kinking it at any time) and to secure it properly. Care must also be taken to affix the connectors properly - using the proper crimping tools - and to weatherproof them.

Direct human contact with the antenna is potentially unhealthy when a pX2 is generating RF energy.

Always ensure that the pX2 equipment is powered down (off) during installation.

6.2.3 Surge Arrestors

The most effective protection against lightning-induced damage is to install two lightning surge arrestors: one at the antenna, the other at the interface with the equipment. The surge arrestor grounding system should be fully interconnected with the transmission tower and power grounding systems to form a single, fully integrated ground circuit. Typically, both ports on surge arrestors are N-type female.

To comply with FCC regulations, the maximum EIRP must not exceed 36dBm.

6.2.4 External Filter

Although the Pico Series is capable of filtering-out RF noise in most environments, there are circumstances that require external filtering. Paging towers and cellular base stations in close proximity to the pX2's antenna can desensitize the receiver. Microhard Systems Inc.'s external cavity filter eliminates this problem. The filter has two N-female connectors and should be connected inline at the interface to the RF equipment.

All installation, maintenance, and removal work must be done in accordance with applicable codes.

Appendix A: Serial Interface

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

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

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

The signals in the asynchronous serial interface are described below:

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

RX *Receive Data* - Output from Module - Signals transferred from the PX2 are received by the DTE via RX.

TX *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the PX2.

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: Firmware Recovery Procedure

In event that your unit becomes unresponsive it may be required to perform a firmware recovery procedure outlined below:

1. Download and save firmware file in a local folder, for example C:\;

2. Separate the PC from the network and set IP to static:

   192.168.1.1
   255.255.255.0

3. Connect PC Ethernet port to the Ethernet port of the modem to be recovered

4. Start a ping on the PC

   C:\>ping 192.168.1.39 -t
   Pinging 192.168.1.39 with 32 bytes of data:
   Request timed out.
   Request timed out.

5. Power cycle modem while pressing and holding CFG (Config) button;

6. Release the CFG button when ping responded:

   C:\>ping 192.168.1.39 -t
   Pinging 192.168.1.39 with 32 bytes of data:
   Request timed out.
   Request timed out.
   Request timed out.
   Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.39: bytes=32 time<1ms TTL=128
   Reply from 192.168.1.39: bytes=32 time<1ms TTL=128

Note, If ping responds as shown above, then you can probably recover the unit, please proceed. Otherwise, send the unit back for RMA.

7. Now use TFTP to push firmware file into the corrupted unit:

   For example, on Windows XP using following command line:

   tftp -i 192.168.1.39 put pX2-v1_1_0-r1003.bin (use the filename saved).

8. Wait until above command to successfully transferred the image, similar message should show

   Transfer successful: xxxxxxx bytes in 5 seconds, nnnnnnn bytes/s, note the number might change for different firmware file

Note, if you see message above, the unit will re-flash itself and reboot, otherwise call for help or send back for RMA.

9. Wait for the unit to recover and reboot.

Appendix C: Approved Antennas

This radio transmitter (IC:3143A-15PX2) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Cet émetteur radio (IC:3143A-15PX2) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous avec le gain maximal admissible indiqué . Types d'antennes ne figurant pas dans cette liste, ayant un gain supérieur au gain maximum indiqué pour ce type, sont strictement interdits pour une utilisation avec cet appareil.

	Part Number	Description
Rubber Ducky		
	MHS031100	2dBi,2.4GHz Rubber Ducky Antenna RPTNC Swivel
	MHS031110	2dBi, 2.4GHz Rubber Ducky Antenna Reverse SMA Swivel
	MHS031120	2dBi, 2.4GHz Rubber Ducky Antenna Reverse SMA Straight
Yagi Antennas		
	MHS034100	9 dBi, 2.4GHz Yagi Directional Antenna RPTNC Pigtail
	MHS034000	12 dBi, 2.4GHz Yagi Directional Antenna RPTNC Pigtail
	MHS034120	14 dBi, 2.4GHz Yagi Directional Antenna RPTNC Pigtail
	MHS034150	14.5 dBi, 2.4GHz Yagi Directional Antenna RPTNC Pigtail
Patch Antennas		
	MHS034200	8 dBi, 2.4GHz Mini Flat Patch Directional Antenna RPTNC Pigtail
	MHS034210	14 dBi, 2.4GHz Flat Patch Directional Antenna RPTNC Pigtail
Omni Directional		
	MHS031260	5 dBi, Omni Directional Antenna RPTNC Pigtail
	MHS034000	6 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail
	MHS031340	8 dBi, Omni Directional Antenna RPTNC Pigtail
	MHS034020	10.5 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail
	MHS034030	12 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail
	MHS034040	15 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail

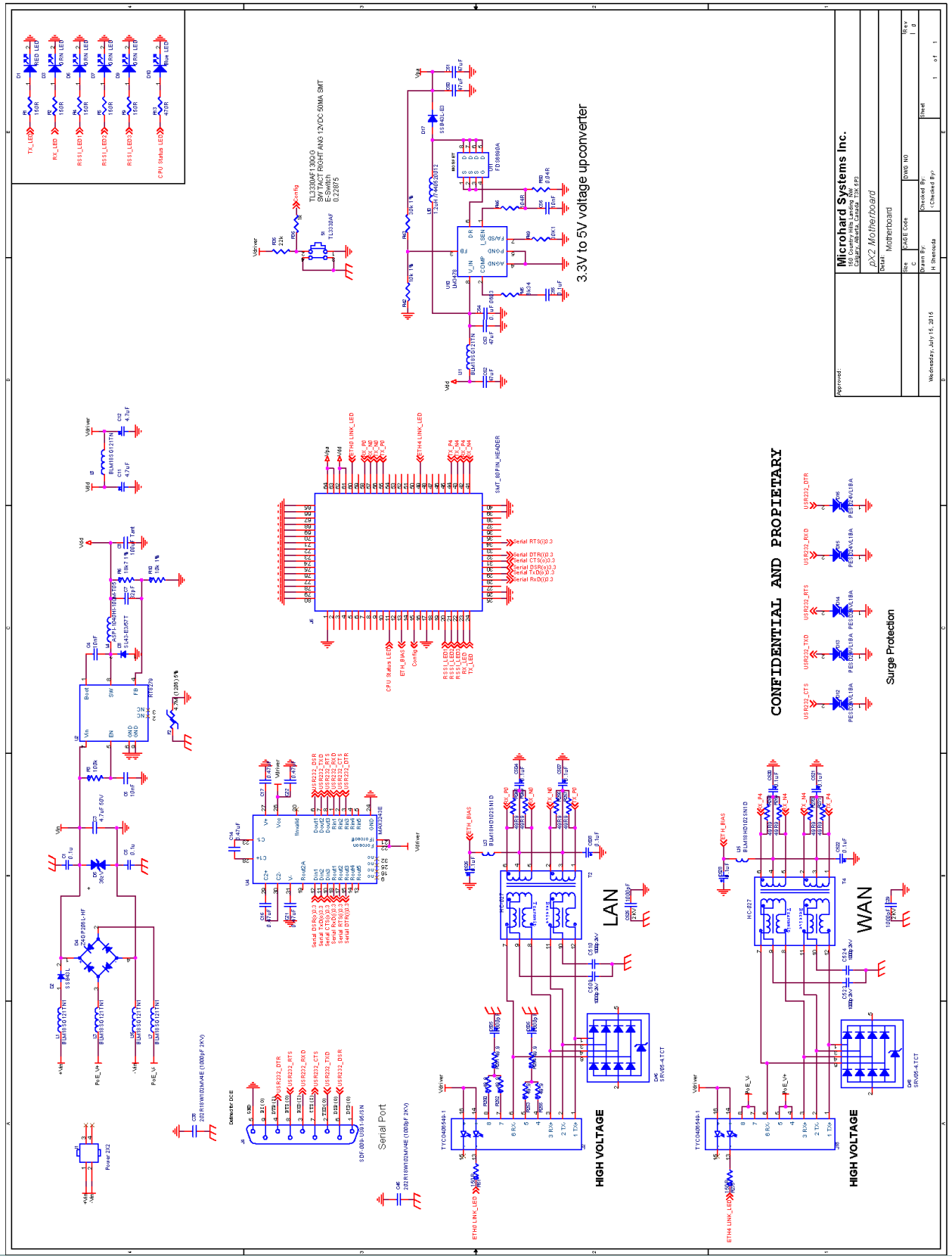
WARNING:

Changes or modifications not expressly approved by Microhard Systems Inc. could void the user's authority to operate the equipment. This device has been tested with UFL connectors with the antennas listed in Appendix A When integrated in OEM products, fixed antennas require installation preventing end-users from replacing them with non-approved antennas. Antennas not listed in the tables must be tested to comply with FCC Section 15.203 (unique antenna connectors) and Section 15.247 (emissions). Please Contact Microhard Systems Inc. if you need more information.

Industry Canada: This device has been designed to operate with the antennas listed above, and having a maximum gain of 15 dBi. Antennas not included in this list or having a gain greater than 15 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication. This Class B digital apparatus complies with Canadian ICES-003.

Industrie Canada: Cet appareil a été conçu pour fonctionner avec les antennes énumérées ci-dessus, et ayant un gain maximal de 15 dBi. Antennes pas inclus dans cette liste ou présentant un gain supérieur à 15 dBi sont strictement interdits pour une utilisation avec cet appareil. L'impédance d'antenne requise est de 50 ohms. Pour réduire les interférences radio potentielles pour les autres utilisateurs, le type d'antenne et son gain doivent être choisis afin que la puissance isotrope équivalente (PIRE) ne soit pas supérieure à celle requise pour une communication réussie rayonnée. Cet appareil numérique de classe B est conforme à la norme ICES -003 du Canada.

Appendix D: Sample Interface Schematic



Appendix E: Troubleshooting

Below is a number of the common support questions that are asked about the pX2. The purpose of the section is to provide answers and/or direction on how to solve common problems with the pX2.

Question: *What is the default IP Address of the pX2?*

Answer: The default IP address for the LAN is 192.168.168.1.

Question: *What is the default login for the pX2?*

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

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

Answer: If you are logged into the pX2 navigate to the System > Maintenance Tab. If you cannot log in, power on the pX2 and wait until the modem complete the boot up process. Press and hold the CONFIG button until the unit reboots (about 8-10 seconds).

Question: *I connected a device to the serial port of the pX2 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.

Additional topics will be added in future releases.

microhard SYSTEMS INC.

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

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