microhard SYSTEMS INC.

Operating Manual

Nano IP Series
900 MHz / 2.4 GHz Wireless Ethernet Bridge/Serial Gateway
Document: Nano IP Series.v2.01.pdf

October 2015

microhard SYSTEMS INC.

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

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

Important User Information

Warranty

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

Warranty Disclaims

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

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

Indemnification

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

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

Proprietary Rights

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

Important User Information (continued)

About This Manual

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

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

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

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

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

Information
Information regarding a particular technology or concept.

Important User Information (continued)

Regulatory Requirements

WARNING

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

WARNING

This device can only be used with Antennas listed in Appendix D. Please contact Microhard Systems Inc. if you need more information or would like to order an antenna.

WARNING

MAXIMUM EIRP

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

EQUIPMENT LABELING

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.

SAMPLE LABEL REQUIREMENT:

IPn920S and IPn920F

FCCID: NS908P24
IC: 3143A-08P24

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.

IPn920T

FCCID: NS908P25
IC: 3143A-08P25

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.

For IPn2420F

FCCID: NS911P31
IC: 3143A-11P31

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.

IPn2420T

FCCID: NS912P32
IC: 3143A-12P32

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.

CSA Class 1 Division 2 Option

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

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

In such a case the following must be met:

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

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

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

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

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

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

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

Revision History

Revision 2.01 October 2015

Added note(s) indicating sleep mode(s) not supported on IPn2420 models.

Revision 2.0 June 2015

Updated Antenna connector for RPSMA Female, Updated Drawings & Images, Misc Corrections

Revision 1.9 August 2013

Added FCC/IC ID'sfor IPn2420F/T models. Updated approved antennas, adjusted OEM drawings, misc formatting.

Revision 1.8 July 2013

Added Passive PoE info for enclosed units/motherboards shipped after March 1, 2013, misc updates and corrections. Updated Images. Removed HV option. Updated Recovery Procedure.

Revision 1.7 April 2012

Updated pictures for new enclosure. Misc formatting. Updated TCP Server description.

Revision 1.5 June 2010

Updated Address Information

Revision 1.4 May 2010

Corrected drawing for Nano IP Motherboard. Misc formatting.

Revision 1.3 March 2010

Updated screen shots, added sections for sleep modes, power saving, new drawings etc.

Revision 1.2 March 2010

Major reformatting, updated all screen shots, Nano IP Layout Drawing, Added additional USB Updated Discover IP, etc.

Revision 1.1 March 2010

Added USB, misc formatting, updated some webUI

Initial Release April 2009

Table of Contents

continued...

Table of Contents (continued)

Table of Contents (continued)

1.0 Overview

The Nano IP Series is a high-performance wireless Ethernet bridge and serial gateway. Alternately, a Master Nano IP Series unit may be configured to operate as a wireless Ethernet router (and serial gateway).

When properly configured and installed, long range communications at very high speeds can be achieved.

The Nano IP Series operates within the 902-928MHz, or 2.4-2.4835 GHz ISM frequency bands, employing frequency hopping spread spectrum (FHSS) and, for 1.2Mbps operation, digital transmission service (DTS) technology.

A BRIDGE separates two network segments within the same logical network (subnet).

They provide reliable wireless Ethernet bridge functionality as well gateway service for asynchronous data transfer between most equipment types which employ an RS232, RS422, or RS485 interface.

A ROUTER forwards data across internetworks (different subnets).

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

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

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

The serial data is encapsulated within UDP or TCP packets.

1.1 Performance Features

Key performance features of the Nano IP Series include:

- transmission within a public, license-exempt band of the radio spectrum[1] - this means that the modems may be used without access fees or recurring charges (such as those incurred by cellular airtime)
- maximum allowable transmit power (1 Watt)
- longest range
- transparent, low latency link providing reliable wireless IP/Ethernet communications with constant baud rate over distance
- each unit supports all modes of operation (Master, Repeater, Remote)
- Repeater may also be used concurrently as a Remote unit
- flexible wireless networking: point-to-point, point-to-multipoint, peer-to-peer, store and forward repeater

1 920-928MHz or 2.4-2.4835GHz, which is license-exempt within North America, may need to be factory-configured differently for other areas: contact Microhard Systems Inc.

1.0 Overview

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

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

1.0 Overview

1.2 Nano IP Series Specifications

Electrical/General

Frequency:	IPn920: 902 - 928 MHz IPn2420: 2.4000 - 2.4835 GHz
Spreading Method:	Frequency Hopping /DTS
Band Segments:	Selectable via Freq. Restriction
Error Detection:	32 bits of CRC, ARQ
Data Encryption:	128-bit WEP/WPA (Canada & USA only. Not available for export, see **–AES/EXP** options) **-AES** - Optional 128/256-bit AES Encryption, Secure Shell, HTTPS (Requires Export Permit Outside Canada & USA) **-EXP** - Export Version, Removes all encryption.
Range:	IPn920: Up to 30+ miles (50+km) @ 1.2 Mbps Up to 60+ miles (100+ km) @ 172 kbps IPn2420: Up to 15+ miles (25+km) @ 1.2 Mbps Up to 30+ miles (50+km) @ 172 kbps
Output Power:	100mW to 1W (20-30dBm)
Sensitivity:	-108 dBm @ 172kbps link rate -106 dBm @ 230kbps link rate -97 dBm @ 1.2 Mbps link rate
Serial Baud Rate:	300bps to 921kbps
USB:	USB 2.0
Ethernet:	10/100 BaseT, Auto - MDI/X, IEEE 802.3
Link Rate:	115 kbps to 1.2 Mbps (options vary by model)
Network Protocols:	TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP, QoS (* Only available in –AES)
Operating Modes:	Master, Slave, Repeater
Management:	Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade, RADIUS authentication, VLAN
Diagnostics:	Battery Voltage, Temperature, RSSI, remote diagnostics
Core Voltage:	OEM: 3.3VDC Nominal (+/- 0.3V) Enclosed/MB: 7-30 VDC
Power over Ethernet:	Passive PoE on Ethernet Port (Enclosed/Motherboard)

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

Tip: Future enhancements of the Nano Series products may require higher current requirements than listed. It is good design practice to over spec power supplies to allow for future design options.

1.0 Overview

1.2 Nano IP Series Specifications (Continued)

Environmental

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

Humidity: 5% to 95% non-condensing

Mechanical

Dimensions:

IPn920-OEM:	1.25” (32mm) X 2.0” (51mm) X 0.50”(13mm)
IPn920-ENC:	2.25” (57mm) X 3.75” (95mm) X 1.5” (38mm)
IPn2420-OEM:	1.25” (32mm) X 2.0” (51mm) X 0.60”(15mm)
IPn2420-ENC:	2.25” (57mm) X 3.75” (95mm) X 1.5” (38mm)

Weight (Including Radio:

OEM:	Approx. 25 grams
Enclosed:	Approx. 240 grams
w/Motherboard:	Approx. 70 grams

Connectors:

Antenna: OEM: MMCX
Enclosed: Reverse Polarity SMA (RPSMA) Female Bulkhead

Data, etc: AVX-Kyocera 5046 Series 60 pin board to board connectors.

Nano IP OEM Module: 14-5046-060-630-829+

Motherboard: 24-5046-060-600-829+ (**Nano IP mating connector**)

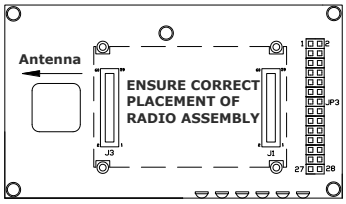
Microhard Systems Inc Part Number: MHS030510 (Strips of 100)

2.0 Quick Start

This QUICK START guide will enable you to promptly establish basic IP connectivity between a pair of Nano IP Series in a point-to-point (ref. 5.1) configuration.

Note that the units arrive from the factory with a Radio Configuration of 'Remote' and the Local Network setting configured as 'Static' (IP Address **192.168.1.254**, Subnet Mask **255.255.255.0**, and Gateway 192.168.1.1).

2.1 Factory Default/Reset Method



2.11 Required Materials

- 2 Nano IP Series (with (or set to) factory default configuration), each with Power Adapter and Rubber Ducky Antenna
- 1 PC with NIC (Ethernet) card
- 1 Ethernet patch cable*

*dependent on desired test set-up

2.12 Set-Up Procedure

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

- Connect a Rubber Ducky antenna to each Nano IP Series.
- Connect the Power Adapters to available 120VAC outlets, and to the Nano IP Series. The SYS LED will blink for approximately 1 minute while it readies itself for operation.
- Using the Ethernet patch cable, connect PC NIC card to rear ETHERNET connection on Nano IP Series. (PC must have its Network Settings (TCP/IP Properties) set to STATIC with an IP Address of (e.g.) 192.168.1.10 and a Subnet Mask of 255.255.255.0.)
- Open a Web Browser and enter the IP Address (192.168.1.254) of the Nano IP Series into the URL address line.
- Refer to Section 6.1.1 re LogOn.

To ensure that the Nano IP Series unit is at its DEFAULT factory settings, once it has powered-up and the SYS LED is ON (after 1 minute), press and hold the front CFG button for 8 seconds - the SYS LED will initially blink, then be on solid, and then the unit will reset.

Note: *Some* OEM customers will have *their* specific factory defaults loaded.

continued...

2.0 Quick Start

- Refer to Section 6.1.4.1 re Network (IP) Configuration and assign the unit a new unique IP Address.
- Refer to Section 5.1 and, as per the example settings given, configure unit as MASTER.
- Repeat the above for the other Nano IP Series, giving it a new unique IP Address and configuring it as a REMOTE (5.1).
- With both units powered-on, in proximity to each other, and configured as per the above, their RSSI LEDs should be illuminated, and their TX LED should be ON or flashing.
- With the PC connected to one of the Nano IP Series units, enter the IP Address of 'the other' unit: its LogOn window should appear via the wireless connection.

.

2.0 Quick Start

2.2 Text UI Method

(See Section 6.2 for more information re the Text User Interface.)

2.21 Required Materials

- 2 Nano IP Series (with factory default configuration), each with Power Adapter and Rubber Ducky Antenna
- 1 PC with NIC (ethernet) card and COM (serial) port with HyperTerminal (or equivalent) application
- 1 Available connection to LAN*
- 1 Ethernet Patch Cable
- 1 MHS Diagnostic Cable (P/N MHS044000, black)

*dependent on desired test set-up

2.22 Set-Up Procedure

- Connect a Rubber Ducky antenna to each Nano IP Series.
- Connect the 12V DC Power Adapters to available 120VAC outlets, and to the Nano IP Series.
- Connect a standard RS232 Cable to Diagnostic Port (COM2 -front) of one Nano IP Series and the other end to an available COM port on the PC.

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

- Run HyperTerminal (or equivalent terminal program) on the PC and configure it for the COM port chosen above, 115200bps, 8 data bits, no parity, 1 stop bit, and no flow control.
- Activate the HyperTerminal connection.
- A login prompt will appear. Enter **admin**.
- At the password prompt, enter **admin**.

continued...

2.0 Quick Start

- Select Option **B: Network Configuration**, then
    - A: **Local IP Config**, then
        - A: **IP Address Mode**, then
            - A: **static**

View the PC's NETWORK SETTINGS (TCP/IP Properties) to determine an appropriate IP Address, Subnet Mask, and Gateway for the Nano IP Series.

(For basic testing, the Gateway value is not critical.)

If a connection is being made to a network (LAN), check with the Network Administrator for an available static IP address(es) so as not to potentially create an IP address conflict.

- Input suitable (for your PC/network) values for:
    - **IP Address**
    - **Subnet Mask**
    - **Gateway**
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] twice to return to the MAIN MENU.
- Select Option **C: Radio Configuration**, then
    - **B: Operation Mode**, then
        - **A: Master**, then
    - **I: Network Type**, then
        - **B: Point-to-Point**, then
    - **J: Destination Unit**, then
      enter the number **20** [***Enter***]
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] to return to the MAIN MENU.
- Press **Q** to Quit.

The Nano IP Series configured above is now the MASTER Nano IP Series for your Point-to-Point Nano IP Series network.

Remove the connection from the MASTER Nano IP's Diagnostic (COM2) port and move it to the other Nano IP Series.

- Press [***Enter***]
- A login prompt will appear. Enter **admin**.
- At the password prompt, enter **admin**.

continued...

2.0 Quick Start

- Select Option **B: Network Configuration**, then
    - A: **Local IP Config**, then
        - A: **IP Address Mode**, then
            - A: **static**
- Input suitable (for your PC/network) values for:
    - **IP Address**
    - **Subnet Mask**
    - **Gateway**
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] twice to return to the MAIN MENU.
- Select Option **C: Radio Configuration**, then
    - **B: Operation Mode**, then
        - **C: Remote**, then
    - **F: Unit Address**, then
        - enter the number **20** [***Enter***]
    - **I: Network Type**, then
        - **B: Point-to-Point**, then
    - **J: Destination Unit**, then
      enter the number **1** [***Enter***]
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] to return to the MAIN MENU.
- Press **Q** to Quit.

The Nano IP Series configured above is now the REMOTE Nano IP Series for your Point-to-Point Nano IP Series network.

With these two Nano IP Series on a test bench, and configured as per the preceding, a wireless link will be present between the two units. This may be confirmed by noting that the RSSI (3 front panel LEDs) are illuminated.

Next, the ethernet connections will be made.

continued...

2.0 Quick Start

The Ethernet connections are dependent upon what is available to work with for the test configuration. For the purposes of this QUICK START, the assumption is that a LAN connection is available (with Internet connectivity) and that the PC is connected to this LAN.

- Disconnect the PC's LAN connection from its NIC card and insert the now 'loose end' of the Ethernet Patch Cable into the rear ETHERNET RJ45 connector at the rear of the MASTER Nano IP Series.
- Using a CROSSOVER cable, connect the PC's NIC card RJ45 jack to the ETHERNET RJ45 connector on the REMOTE Nano IP Series.

At this point there is a wireless connection between the PC and the LAN, and you should be able to go about your typical networking activities, including accessing the Internet (via the LAN).

Also, by opening a web browser and entering the IP address of either Nano IP Series, you will be taken to the respective unit's Web User Interface LOGIN window.

If communications not available as outlined above:

- Verify the RSSI LEDs on the front of each Nano IP Series are illuminated.
- Verify TX (red) LED activity on the front of each Nano IP Series.
- Observe the rear of each Nano IP Series, specifically the ETHERNET connection: the green LINK LED should be illuminated (indicating proper cabling) and the amber (ACTIVITY LED) should also be flickering—indicating DATA traffic at the ETHERNET connector.
- If using Windows XP, the firewall function could inhibit desired data traffic. Anti-virus software may also have a negative impact.

3.0 Hardware Description

3.1 Nano IP OEM Module

The Nano IP Series Modems are available in both OEM and Enclosed packages. The 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 Enclosed version of the Nano Series modem allows for a fully operational table top or mountable solution. The various interface cards and development boards can provide a convenient evaluation platform or an in between end solution.

The Nano IP OEM module is typically complemented by interface circuitry (e.g. power, data interface) for most applications. Nano IP Motherboard provides much of this interface circuitry to aid in the integration or evaluation of the Nano IP module.

The Nano Enclosed Modem supplies all required interface circuitry and all that is required are general user interfaces (RS232, antenna, power).

Any Nano IP module may be configured as a Master, Repeater (or Repeater/Slave), or Slave.

This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the module: if you are familiar with one unit, you will be familiar with all units.

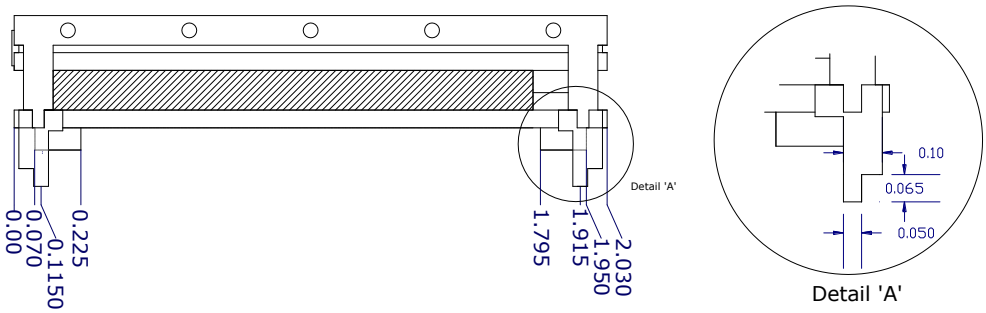
Image 3-1: Nano IP OEM Bottom View

Image 3-2: Nano IP OEM Top View

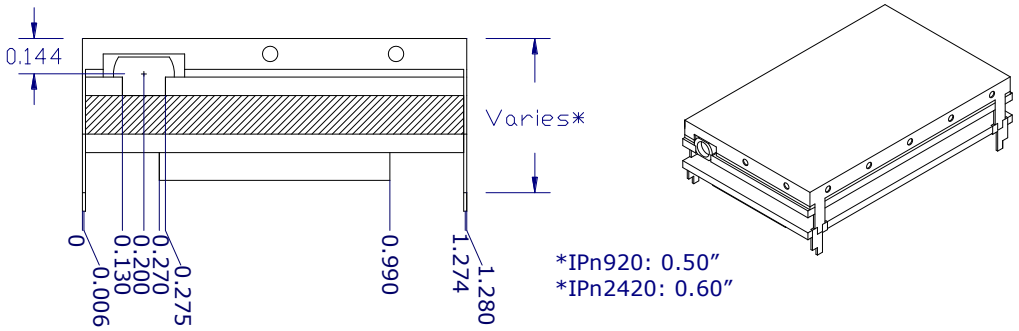
3.0 Hardware Description

3.1.1 Nano IP OEM Mechanical Drawing

The Nano IP Series OEM Module has an extremely small form factor as see in *Drawing 3-3* and *Drawing 3-4* below. ***Refer to the Appendix for detailed connector placement and dimensions.***



Drawing 3-3: Nano IP OEM Side View



Drawing 3-4: Nano IP OEM Front View

Notes: The dimension unit is inches.

3.1.2 Nano OEM Connectors

Antenna
The Nano IP OEM Module uses an MMCX connector.

Data
The Data connectors use AVX-Kyocera 5046 Series 60 pin board to board connectors. The manufacturers part numbers are listed below, or the mating connector is available directly from Microhard Systems.

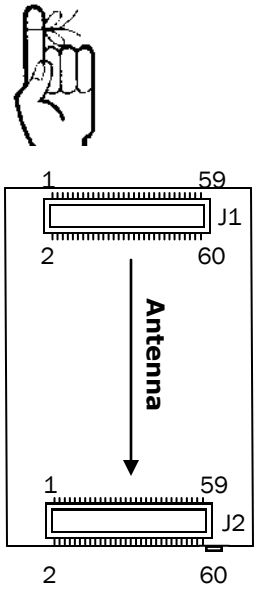
AVX-Kyocera Part Number: 24-5046-060-600-829+
Microhard Systems Inc Part Number: MHS030510 (Strips of 100)

The above part numbers are for the mating connector required to interface to the Nano IP Series Modems.

To assist in the layout or circuits required to interface with the Nano Series Modems, see the *Appendix*.

3.0 Hardware Description

3.1.3 Nano IP OEM Pin-Out Description



Nano IP Connector Placement

NC	2		1	ETH_LINK_ACT_LED
NC	4		3	ETH_SPEED_LED
NC	6		5	Vclock
NC	8		7	NC
ETH_CAT6	10		9	NC
ETH_CAT3	12		11	!WAKEUP_usr
ETH_CAT2	14		13	!CONFIG
ETH_CAT1	16		15	!RESET
COM2_RxD	18		17	Vbat
COM2_TxD	20		19	!RSMode
LED_RX	22		21	USB_DDM
LED_TX	24		23	USB_CNX
RSSI3_LED	26	Nano IP (J1)	25	USB_DDP
RSSI2_LED	28		27	Reserved
RSSI1_LED	30		29	Reserved
COM1_CTS	32		31	Reserved
COM1_RTS	34		33	Reserved
COM1_DSR	36		35	USR_1
COM1_RING	38		37	USR_2
COM1_DTR	40		39	USR_3
COM1_TxD	42		41	NC
COM1_RxD	44		43	NC
COM1_DCD	46		45	NC
!RE_485	48		47	NC
DE_485	50		49	NC
GND	52		51	Vcc (3.3V)
GND	54		53	Vcc (3.3V)
GND	56		55	Vcc (3.3V)
GND	58		57	Vcc (3.3V)
GND	60		59	Vcc (3.3V)

Drawing 3-5: J1 60-pin OEM Connector Pin-out

Pins 2, 4, 6, and 8 are reserved for factory use. Do not use these pins for any other purpose.

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

The above drawing depicts a bottom view of the J1 connector. The corner pins (1, 2, 59, and 60) are printed directly upon it for convenient reference.

A full description of the various pin connections and functions is provided on the pages that follow.

See the *Appendix* for an example schematic for interfacing to the Nano IP OEM module.

3.0 Hardware Description

Pin Name	No.	Description	In/ Out
ETH_LINK_ACT_LED	1	Active Low. Ethernet LINK and ACTIVITY indication signal.	O
ETH_SPEED_LED	3	Active Low. Ethernet LINK and ACTIVITY indication signal.	O
NC	2,4,6,8	Reserved for factory use only (JTAG).	
Vclock	5	Reserved.	I
Reserved	7,9	*Reserved for future use.*	I
ETH_CAT6	10	Ethernet RJ45 Pin 6. Optional CAN bus (CAN+)	
ETH_CAT3	12	Ethernet RJ45 Pin 3. Optional CAN bus (CAN-)	
ETH_CAT2	14	Ethernet RJ45 Pin 2.	
ETH_CAT1	16	Ethernet RJ45 Pin 1.	
!WAKEUP_usr	11	Reserved	I
!CONFIG	13	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	15	Active low input will reset module	I
Vbat	17	Battery voltage sensing analog input line, up to 60VDC. A 10k-ohm resistor is required inline from the power source. Reading will be 0 if connected to GND (ground).	I
RSMode	19	Sleep mode indication output. Active low. Typically used to shutdown RS232 drivers.	O
COM2_RxD	18	Console Port receive data. Logic level output from Nano IP to a PC.	O
COM2_TxD	20	Console Port transmit data. Logic level input from a PC into the Nano IP.	I
USB_DM(-)	21	USB device negative data line.	
USB_CNX	23	USB 5V Monitoring	I
USB_DP(+)	25	USB device positive data line.	
Reserved	25,29,31,33	Reserved for future use.	
LED_RX	22	Active high output indicates receive and synchronization status. Can drive LED directly. Refer to section 3.4.2 for additional information about LED operation.	O
LED_TX	24	Active high output indicates module is transmitting data over the RF channel. Can drive LED directly. Refer to section 3.4.2 for additional information about LED operation.	O

Table 3-1: J1 Pin-Out Description

3.0 Hardware Description

Pin Name	No.	Description	In/ Out
RSSI3_LED	26	Receive Signal Strength Indicator 3. Active high, can drive LED directly. 1mA rating.	O
RSSI2_LED	28	Receive Signal Strength Indicator 2. Active high, can drive LED directly. 1mA rating.	O
RSSI1_LED	30	Receive Signal Strength Indicator 1. Active high, can drive LED directly. 1mA rating.	O
COM1_CTS	32	Data Port. Clear To Send. Active low output.	O
COM1_RTS	34	Data Port. Request To Send. Active low input.	I
COM1_DSR	36	Data Port. Data Set Ready. Active low output.	O
RING	38	Incoming RS232 or RS485/422 selector. Low for RS232 High for RS485/422	O
COM1_DTR	40	Data Terminal Ready. Active low input.	I
COM1_TxD	42	Data Port. Transmit Data. Logic level input into the modem.	I
COM1_RxD	44	Data Port. Receive Data. Logic level output from the modem.	O
COM1_DCD	46	Data Carrier Detect. Active low output.	O
USR_1,2,3	35,37,39	*Reserved for future use.*	
NC	41,43,45, 47,49	*Reserved for future use.*	
!RE_485	48	Data Port. RS485 Receiver Output Enable. Active Low Output.	O
DE_485	50	Data Port. RS485 Driver Output Enable. Active High Output.	O
Vcc	51,53,55, 57,59	Positive voltage supply voltage for the module (3.3V).	I
GND	52,54,56, 58,60	Ground reference for logic, radio, and I/O pins.	

Table 3-1: J1 Pin-Out Description (continued)

Pin Name	No.	Description	In/ Out
STATUS_LED	26	System Status Indicator. Active High, can drive LED directly. 8mA rating.	O
NC	All Other Pins	*Reserved for future use.*	O

Table 3-2: J2 Pin-Out Description (Optional)

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.

Serial RxD is the data received by the radio through the wireless link and output via the serial port; Serial TxD is the data received into module from the serial port and transmitted over the wireless link.

3.0 Hardware Description

3.2 Nano IP Motherboard & Enclosed

The Nano IP Motherboard and Nano IP Enclosed share the same signals, indicators, connections and operate identically so they will be described in the same section.

The Nano IP Motherboard can be used to quickly evaluate the features and performance of the Nano Series Modems, or it can be integrated entirely into applications as a quick and robust interface to the Nano Modems.

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

- Power
- Data (Serial) Interface
- Ethernet Interface
- USB Interface
- Indicators
- Antenna

Any Nano IP module may be configured as a Master, Repeater (or Repeater/Slave), or Slave.

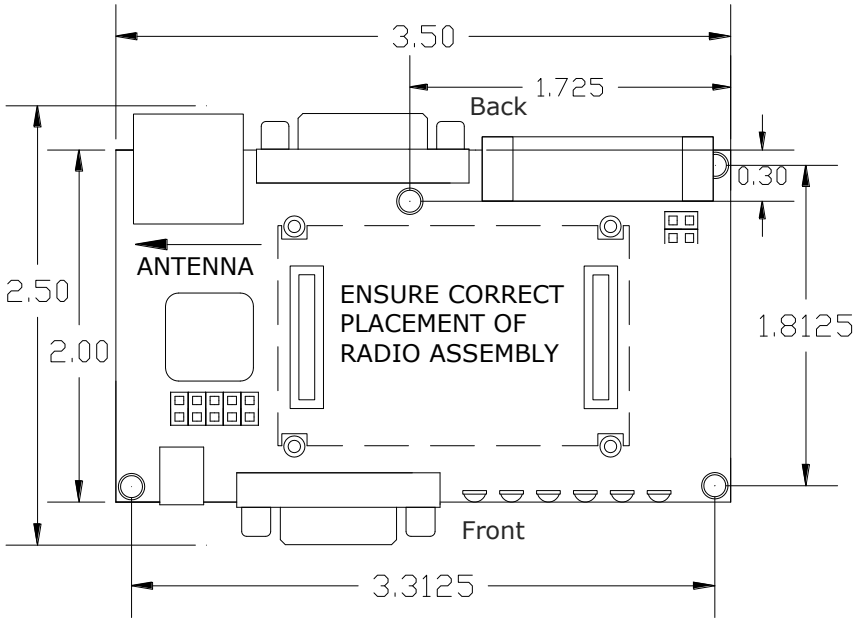
This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the module: if you are familiar with one unit, you will be familiar with all units.

Image 3-3: Nano IP Enclosed

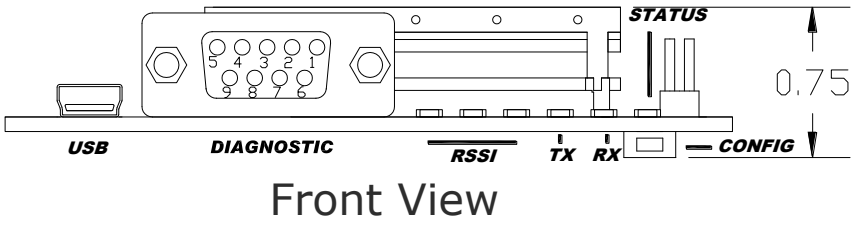
Image 3-4: Nano IP Motherboard

3.0 Hardware Description

3.2.1 Nano IP Motherboard Mechanical Drawings

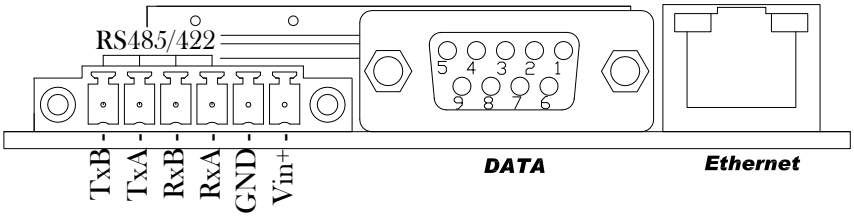


Drawing 3-6: Nano IP Motherboard Top View



Front View

Drawing 3-7: Nano IP Motherboard Top View



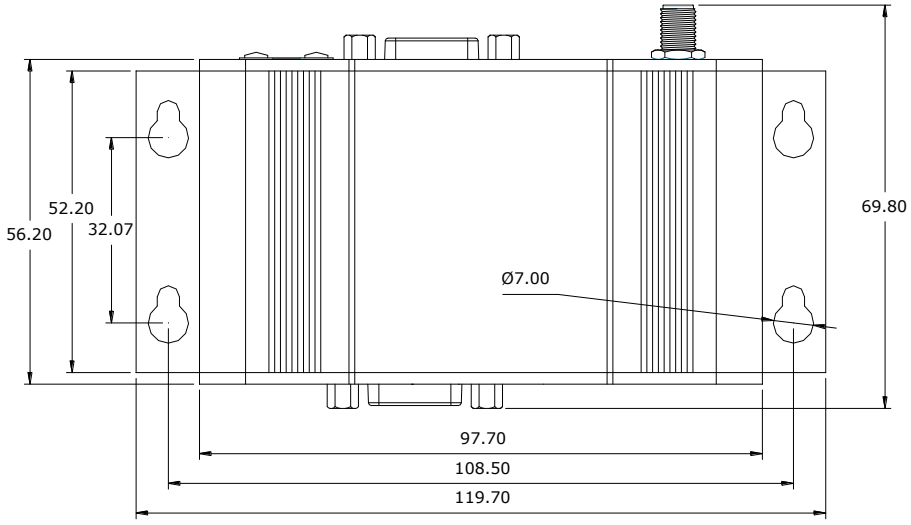
Back View

Drawing 3-8: Nano IP Motherboard Top View

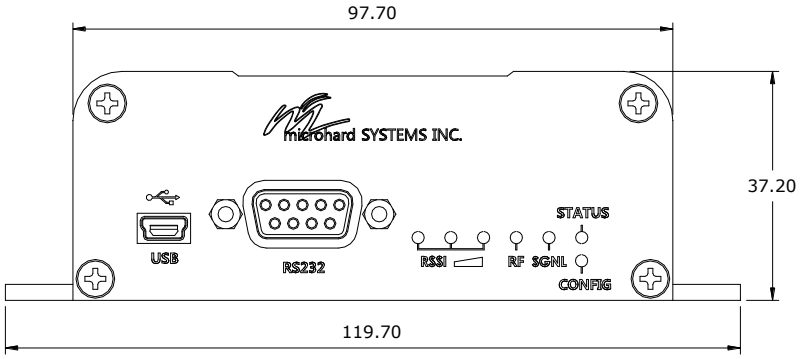
Notes: The dimension unit is inches.

3.0 Hardware Description

3.2.2 Nano IP Enclosed Mechanical Drawings (May 2015)



Drawing 3-9: Nano IP Enclosed Top View



Drawing 3-10: Nano IP Enclosed Front View

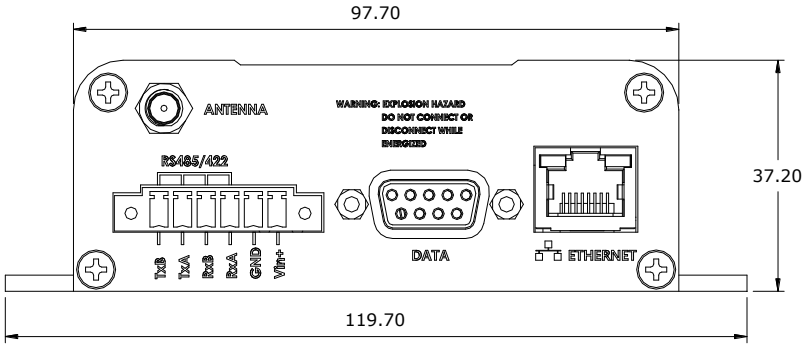
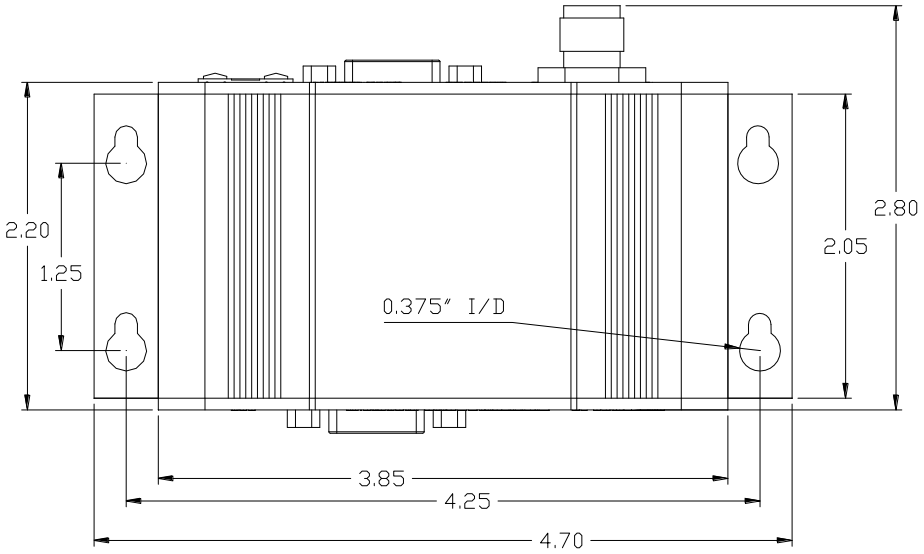


Image 3-11: Nano IP Enclosed Back View

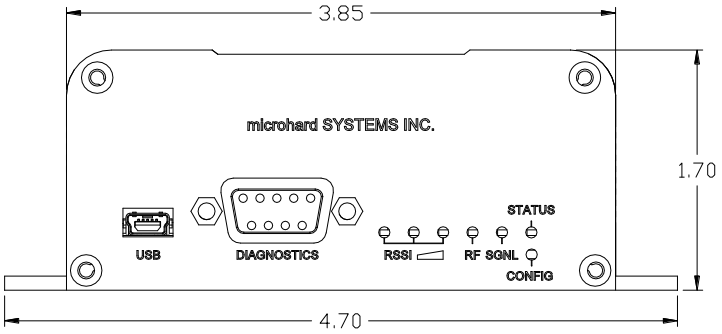
Notes: The dimension unit is mm.

3.0 Hardware Description

3.2.3 Nano IP Enclosed Mechanical Drawings (Old - Prior to May 2015)



Drawing 3-12: Nano IP Enclosed Top View



Drawing 3-13: Nano IP Enclosed Front View

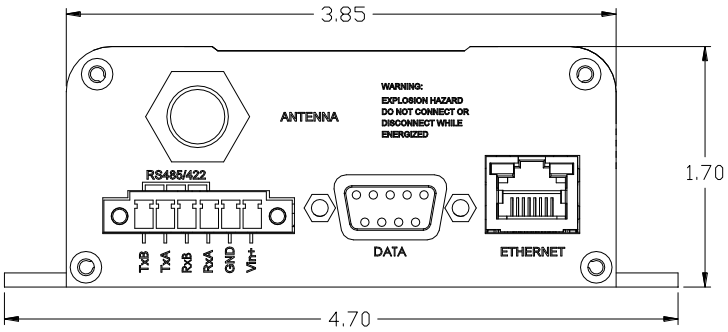


Image 3-14: Nano IP Enclosed Back View

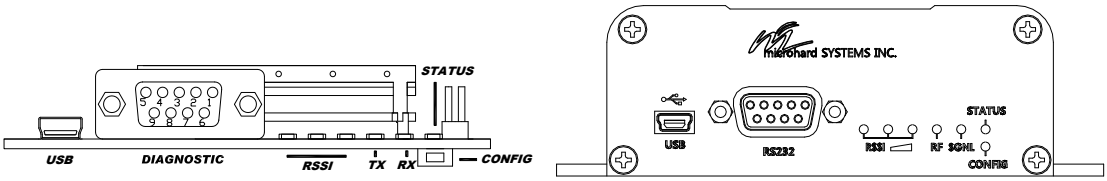
Notes: The dimension unit is inches.

3.0 Hardware Description

3.2.4 Connectors and Indicators

3.2.4.1 Front

On the front of the Nano IP Motherboard/Enclosed is the USB port, DIAGNOSTIC port, CONFIG Button, and the RSSI, STATUS, TX and RX LED's.



Drawing 3-15: Nano IP Motherboard and Enclosed Front View

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

The **USB** port can be used for: (See **Section 6.1.7** USB Configuration)

- Console Port
- Data Mode
- Storage Mode
- NDIS Mode

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

- Text User Interface (local console port) at 115.2kbps and HyperTerminal (or equivalent).
- User data (serial, RS-232, wired for RxD, TxD, and SG)

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

Table 3-3: Diagnostic Port RS232 Pin Assignment

CONFIG Button
Holding this button depressed while powering-up the Nano IP Series will boot the unit into FLASH FILE SYSTEM RECOVERY mode. The default IP address for system recovery (only - not for normal access to the unit) is static: 192.168.1.39.

If the unit has been powered-up for some time (>1 minute), depressing the CFG Button for 8 seconds will result in FACTORY DEFAULTS being restored, including a static IP address of 192.168.1.254. This IP address is useable in a Web Browser for accessing the Web User Interface.

TX LED (Red) / RX LED (Green)
When illuminated, the TX LED indicates that the modem is transmitting data over the air and the RX LED indicates that the modem is synchronized and has received valid packets

Receive Signal Strength Indicator (RSSI) (3x Green)
As the received signal strength increases, starting with the furthest left, the number of active RSSI LEDs increases. Signal strength is calculated based on the last four valid received packets with correct CRC. RSSI is also reported in S123.

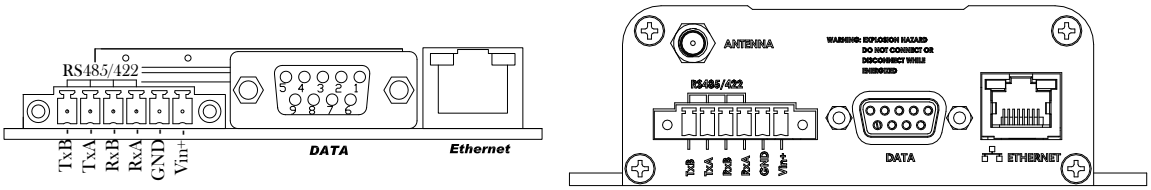
STATUS LED
Upon initial application of power the STATUS LED will be illuminated for approximately 20 seconds, after which time it will being to blink slowly (loading) for an additional 25 seconds, then stay ON _solid' (indicating it has achieved its specific operational status).

3.0 Hardware Description

3.2.4 Connectors and Indicators

3.2.4.2 Rear

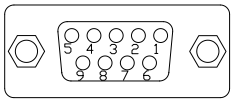
On the back of the Development Board is the Data port, RS485/422 interface, as well as the power connections.



Drawing 3-16: Nano Motherboard/Enclosed Rear View

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

- RS232 serial data (300-921kbps) when in **DATA MODE**, or
- for configuring the modem when in **COMMAND MODE**.

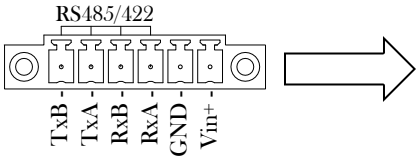


Name	Data Port	Input or Output
DCD	1	O
RXD	2	O
TXD	3	I
DTR	4	I
SG	5	
DSR	6	O
RTS	7	I
CTS	8	O
RING	9	O

Table 3-4: Data RS232 Pin Assignment

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

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



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

Table 3-5: RS422/485 / Vin Pin

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

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

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

Table 3-6: Ethernet PoE Connections

PoE only available on models shipped after March 1, 2013

4.0 Operating Modes

An Nano IP Series may be configured for any operating mode: this is very convenient for purposes of sparing and becoming familiar with their configuration menus.

4.1 Master

One per network, the source of synchronization for the system. The Master controls the flow of data through the system.

4.2 Repeater

Required only if necessary to establish a radio path between a Master and Remote(s); stores and forwards the data sent to it. Synchronizes to Master and provides synchronization to 'downstream' units.
If a local device is attached to a Repeater's serial data port, the Repeater will also behave as a Remote (aka Repeater/Remote).

As they are added to a radio network it is good practice to use the values 2-17, sequentially, for Repeater Unit Addresses.

Adding one or more Repeaters within a network will HALVE the throughput; the throughput is halved only once, i.e. it does not decrease with the addition of more Repeaters.

If there is a 'radio (signal) path' requirement to provide Repeater functionality, but throughput is critical, the repeating function may be accomplished by placing two Nano IP Series at the Repeater site in a 'back-to-back' configuration. One Nano IP Series would be configured as a Remote in the 'upstream' network; the other a Master in the 'downstream' network. Local connection between the modems would be accomplished with a crossover cable (for the ethernet connection). Each modem would require its own antenna; careful consideration should be given with respect to antenna placement and Nano IP Series configuration.

4.3 Remote

Endpoint/node within a network to which a local device is attached. Communicates with Master either directly or through one or more Repeaters. See Sections 5.3 and 5.4 for information regarding 'Slave-to-Slave' communications.

Throughout this manual, '**R**emote' refers to a **R**emote as defined in Section 4.3; the general term '**r**emote' applies to an IP Series Repeater and/or Remote - i.e. non-Master unit.

5.0 Network Topologies

The RADIO network topology determines the paths available for the movement of data.

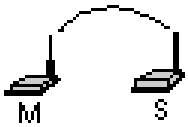
Take this important fact into consideration when selecting a network topology.

The IP Series may be configured to operate in a number of different operating modes and participate in various network topologies.

Note: This section describes radio network topologies in general and includes examples of corresponding Radio Configuration settings. Refer to section 6 for further detailed information regarding configuration options.

5.1 Point-to-Point (PTP)

In a Point-to-Point network, a path is created to transfer data between Point A and Point B, where Point A may be considered the Master modem and Point B a Remote. Such a PTP network may also involve one or more Repeaters (in a store-and-forward capacity) should the radio signal path dictate such a requirement. (Note that a Repeater may also concurrently function as a Remote, i.e. it may pass data to and from an attached device(s).)



A PTP configuration may also be used in a more dynamic sense: there may be many Remotes (and Repeaters) within such a network, however the Master may have its 'Destination Address' changed as and when required to communicate with a specific remote unit.

An example of a basic PTP network consisting of two IP Series is on the next page.

Notes re Example 5.1.1:

- Configuration options are based upon the chosen Operating Mode of the unit: select the Operating Mode first.
- The DESTINATION UNIT for the MASTER is the UNIT ADDRESS of the REMOTE, and vice versa (noting that the MASTER's Unit Address (not visible) is preset, and must remain as, '1').
- For a PTP system, RETRANSMISSIONS on a MASTER is not as critical a setting as it is in a Point-to-Multipoint (PMP) system.

5.0 Network Topologies

Example 5.1.1

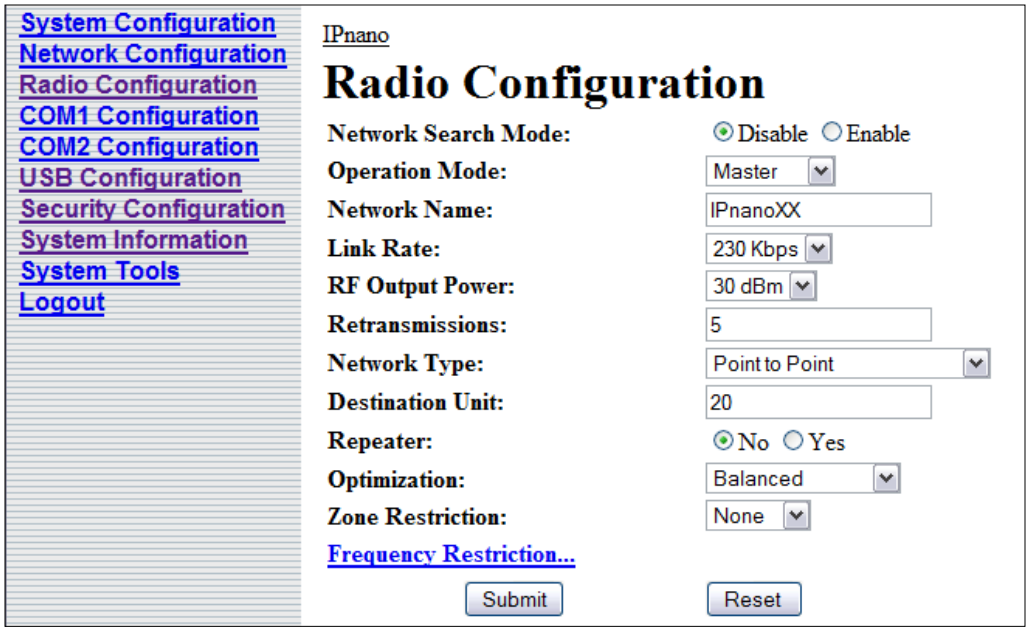


Image 5A: PTP Example 5.1.1: Master

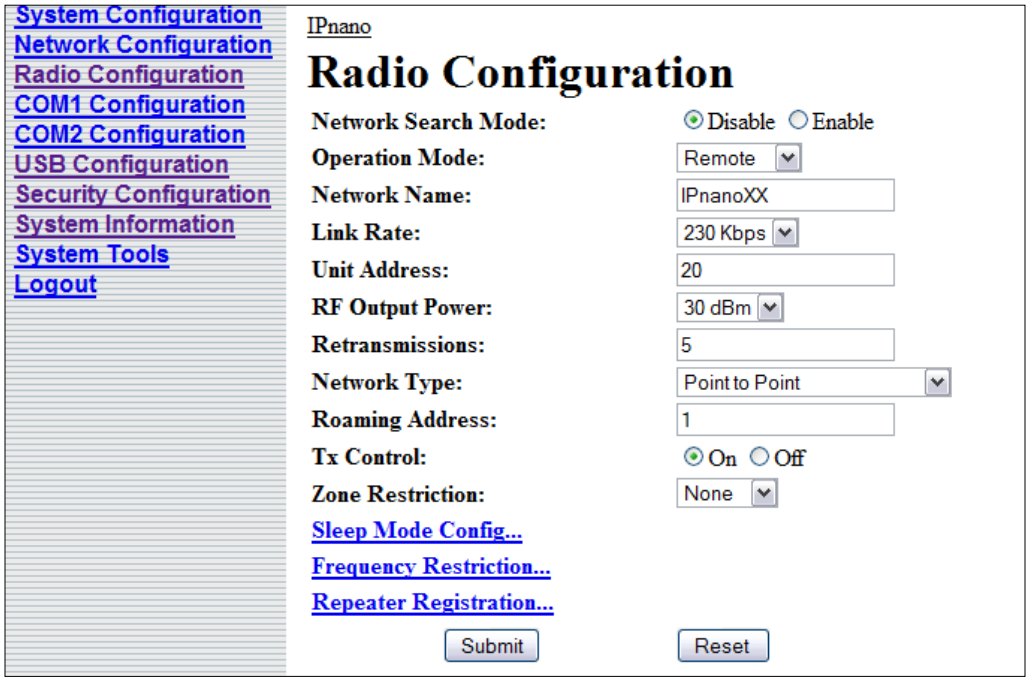
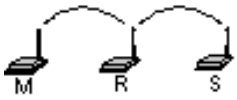


Image 5B: PTP Example 5.1.1: Remote

5.0 Network Topologies

5.2 Point-to-Multipoint (PMP)



In a Point-to-Multipoint network, a path is created to transfer data between the Master modem and numerous remote modems. The remote modems may simply be Remotes with which the Master communicates directly, and/or Remotes which communicate via Repeaters. Some or all of the Repeaters may also act as Remotes in this type of Network, i.e. the Repeaters are not only storing and forwarding data, but are also acting as Remotes. Such Repeaters may be referred to as 'Repeater/Remotes'.

Example 5.2.1

A 4-node network consisting of a Master, 1 Repeater, and 2 Remotes. 1 Remote is to communicate with the Master through a Repeater; the other is to communicate directly with the Master.

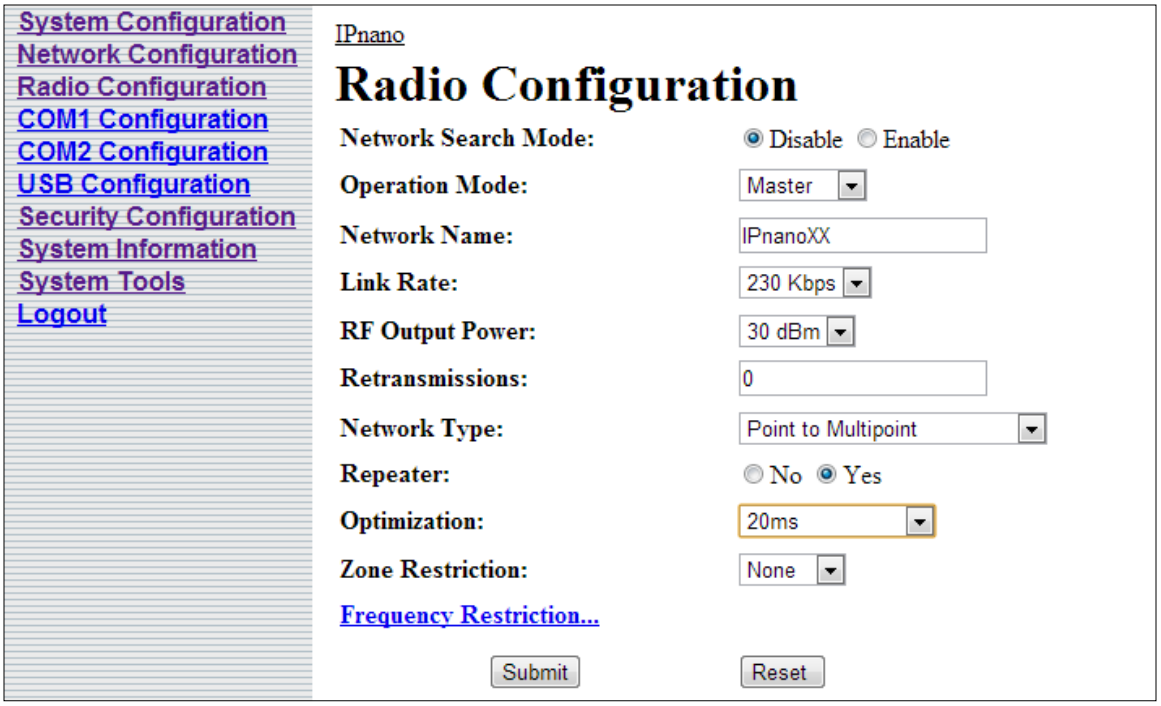


Image 5C: PMP Example 5.2.1: Master

Refer to Section 6.1.4 for important information regarding the configuration of a PMP Master's Retransmissions.

- There is no DESTINATION UNIT displayed as, in PMP, the DESTINATION is preset to 65535: the BROADCAST address ('multipoint').
- RETRANSMISSIONS are set to 0. Refer to Section 6.1.4 for more information.
- There is a REPEATER in this example network, therefore the MASTER's 'Repeater' configuration option is set to Yes.

5.0 Network Topologies

Example 5.2.1 (continued)

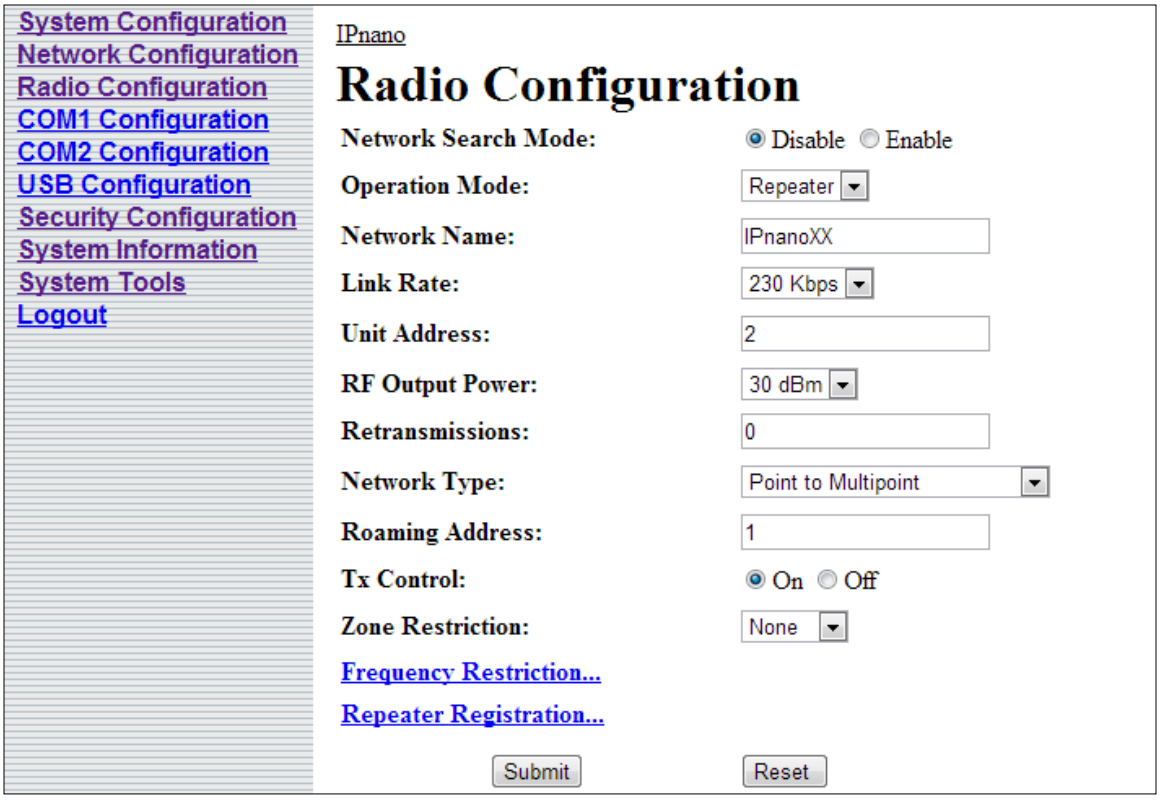


Image 5D: PMP Example 5.2.1: Repeater

When bench testing PMP with a REPEATER in the network, configure the REMOTE to synchronize to the REPEATER via the REMOTE's ROAMING ADDRESS field. If this is not done, with the REMOTE in close proximity to the MASTER and its ROAMING set as 1 (default), the REMOTE will simply synchronize with (and pass data directly to) the MASTER, bypassing the REPEATER altogether.

- The ROAMING address for the REPEATER is set to 1: the UNIT ADDRESS of the MASTER. This means that this REPEATER will synchronize to, and communicate directly with, the MASTER.

- There is no DESTINATION UNIT field for remote units in a PMP network: the destination is predefined as '1' (the MASTER 'point').

On the following page are the configurations for the REMOTES.

- Remote 20's ROAMING ADDRESS is set to 2, the UNIT ADDRESS of the REPEATER. This Remote will synchronize to the Repeater and communicate via the Repeater to the Master.

- Remote 30's ROAMING ADDRESS is set to 1 (the UNIT ADDRESS of the MASTER): it will synchronize to, and communicate directly with, the MASTER.

5.0 Network Topologies

Example 5.2.1 (continued)

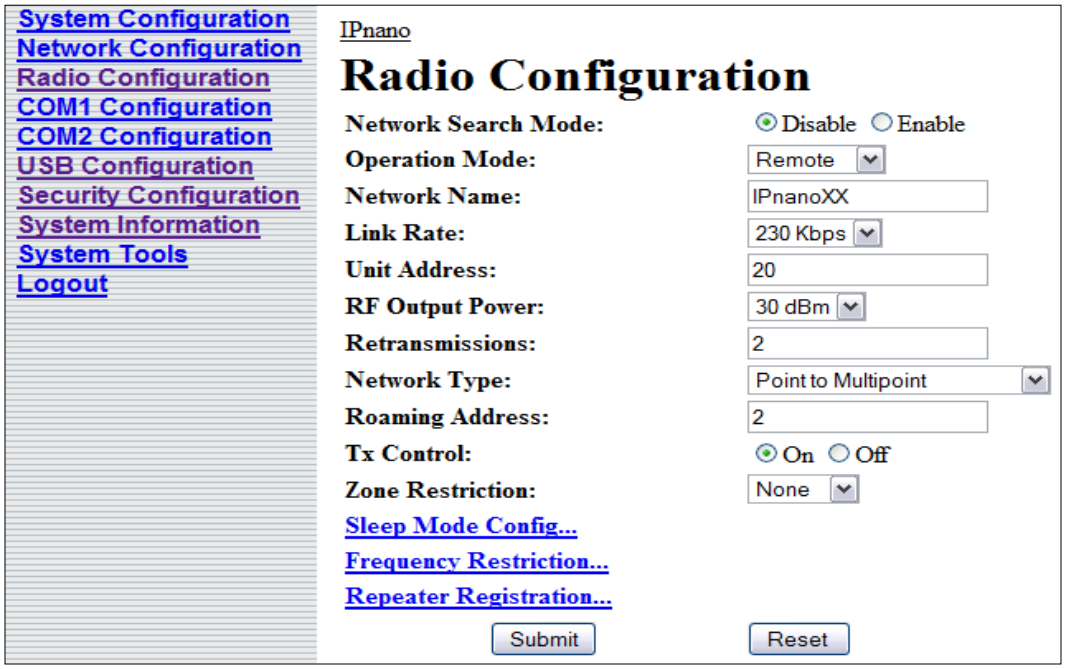


Image 5E: PMP Example 5.2.1: Remote 20

Each modem in any network must have a unique Unit Address.

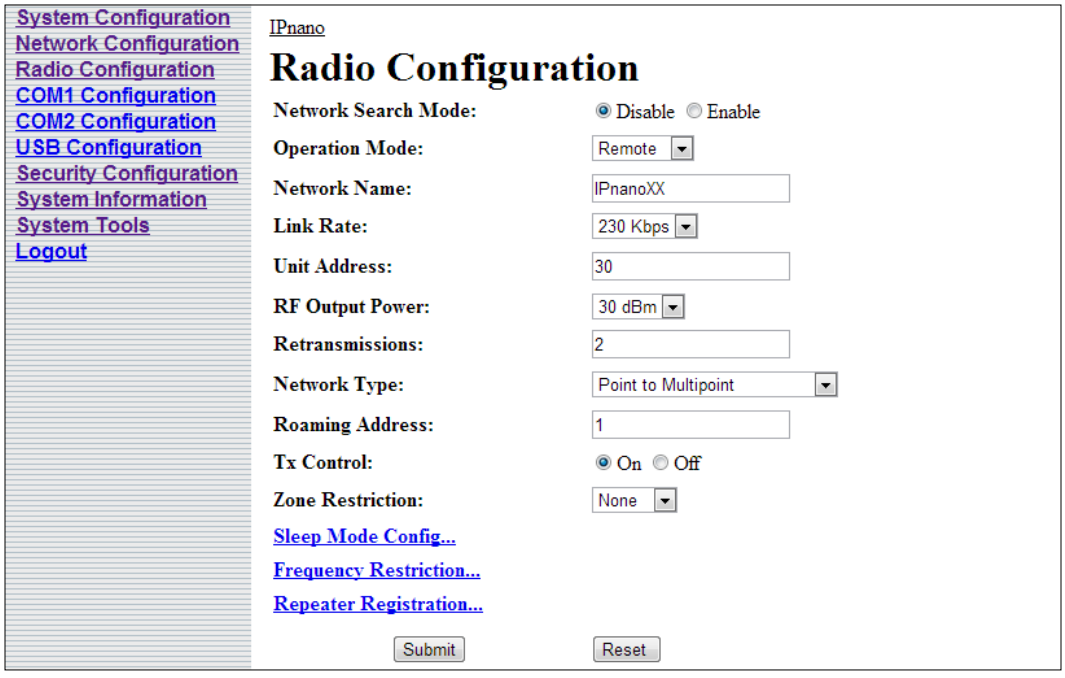


Image 5F: PMP Example 5.2.1: Remote 30

5.0 Network Topologies

5.3 Peer-to-Peer (P2P)

P2P mode is used for communications between pairings of remote modems,

e.g. Remote 20 can exchange data with (only) Remote 30, Remote 21 can exchange data with (only) Remote 35, etc.

The Master will resend the data incoming to it from both Remotes to both/all Remotes; one Remote's data has a Destination Unit being the other Remote and vice versa.

A P2P network requires a Master modem.

The data being transmitted from one Remote to another in P2P mode is transferred via the Master.

Example 5.3.1

A device located at a pump station must communicate bi-directionally with another device at a water tank. The MASTER Nano IP Series must reside in an office at a separate location.

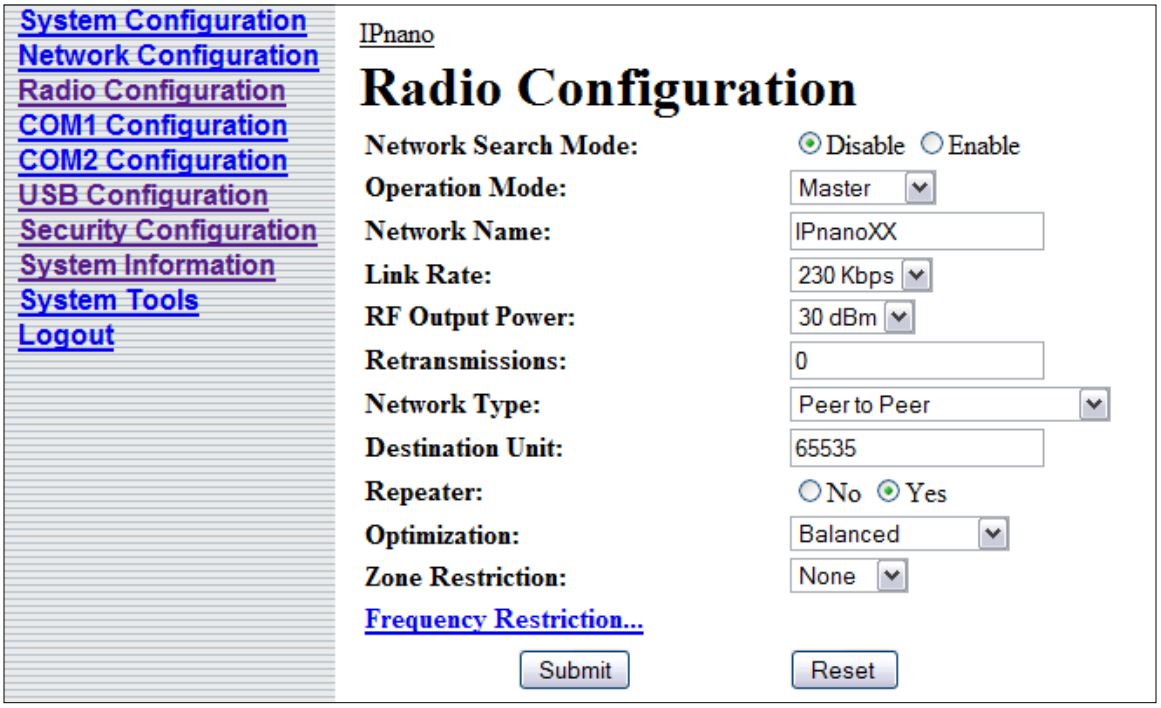


Image 5G: P2P Example 5.3.1: Master

All Nano IP Series within a particular network must be configured to have the same Network Type.

continued...

5.0 Network Topologies

Example 5.3.1 (continued)

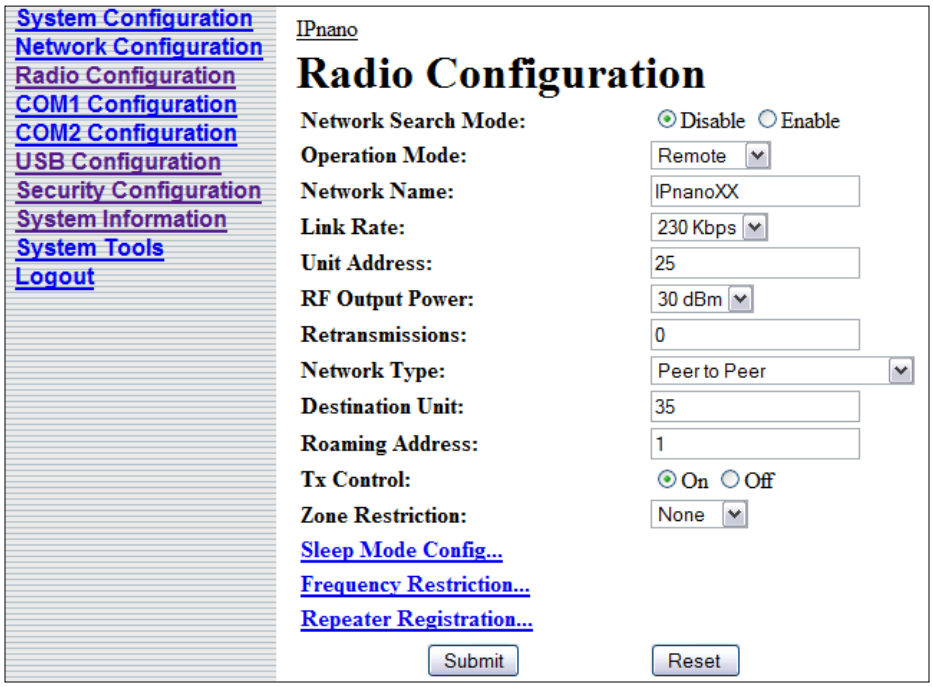


Image 5H: P2P Example 5.3.1: Remote 25

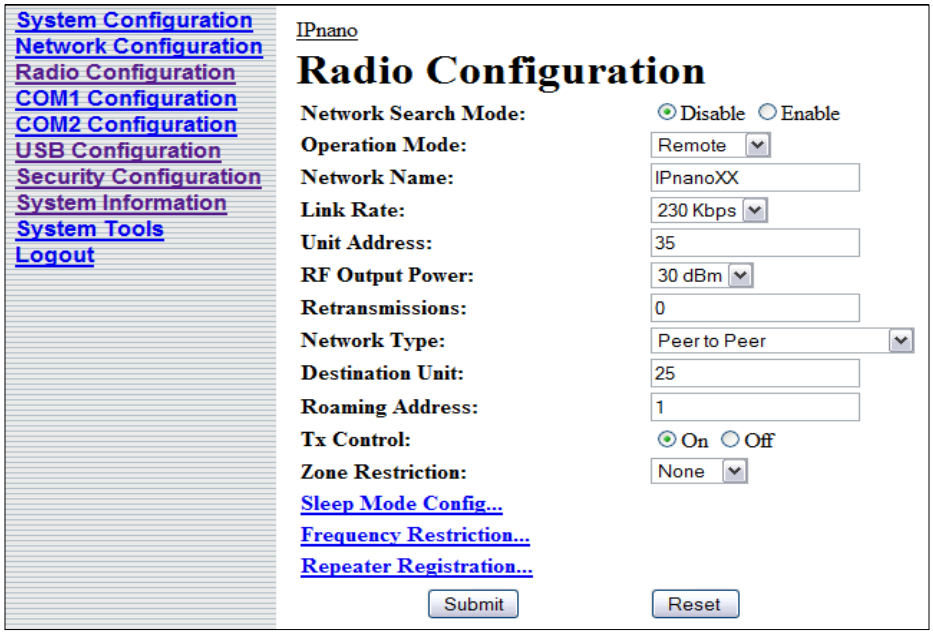


Image 5I: P2P Example 5.3.1: Remote 35

5.0 Network Topologies

5.4 Everyone-to-Everyone (E2E)

E2E mode is used for communications between all remote modems,

i.e. data from every modem is broadcast to every other modem in the network.

Considering the amount of data re-broadcasting (via the Master), it is a very bandwidth-intensive network topology.

An E2E network requires a Master modem.

The data being transmitted from remote units in an E2E network travels to the Master and is then re-broadcast to all other remotes.

Example 5.4.1

1 Master and 3 remote units must all communicate with each other.

- There is no DESTINATION UNIT configuration option as the DESTINATION is pre-defined to be the broadcast address (65535) when in E2E mode.

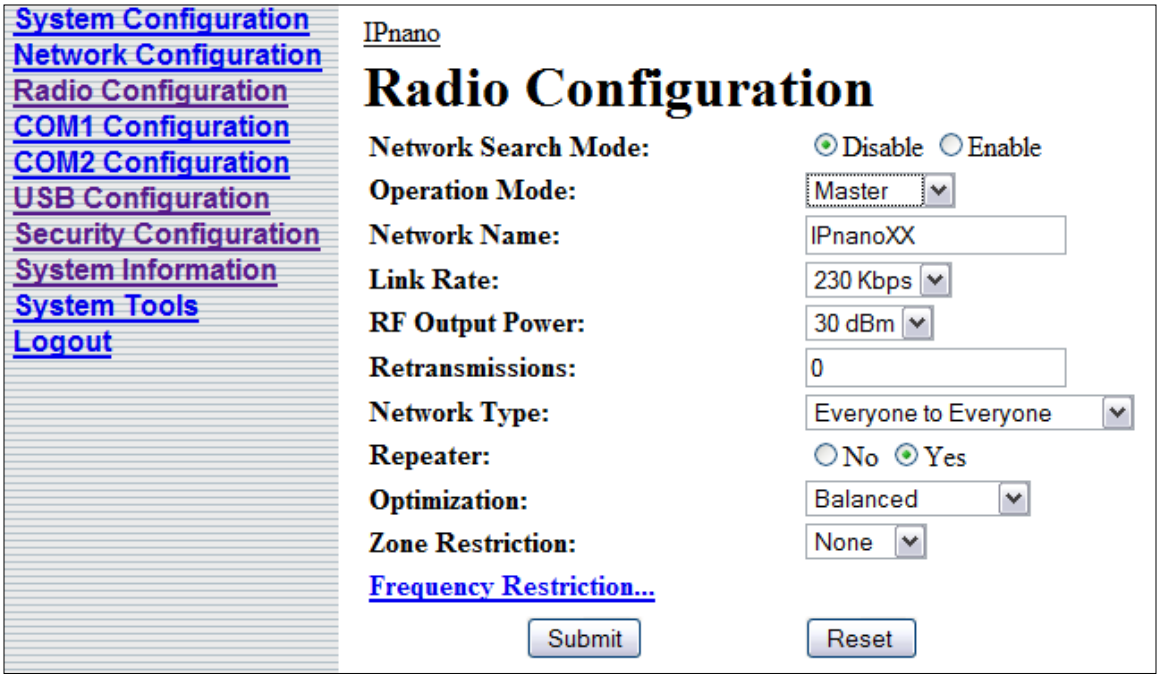


Image 5J: E2E Example 5.4.1: Master

5.0 Network Topologies

Example 5.4.1 (continued)

The Remotes will all be configured as per the above screen capture, with the exception of the UNIT ADDRESS. Each Remote (of the 3 in this example) must have its own unique UNIT ADDRESS, e.g. 50, 51, and 52.

Each unit must have its own unique Unit Address.

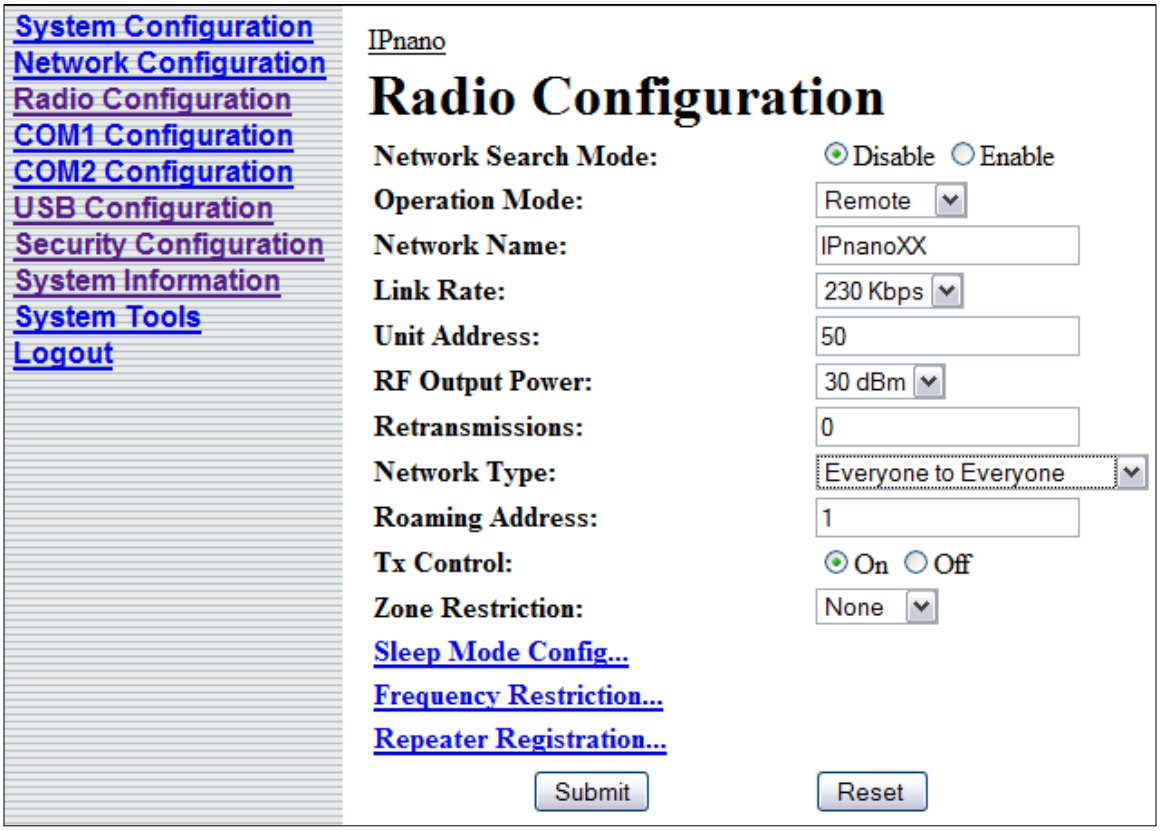


Image 5K: E2E Example 5.4.1: Remote

6.0 Configuration

The following factors must be considered when preparing to configure the modems:

- the application
- network topology
- physical distribution of the network
- data interface requirements

Components involved in the configuration process of the IP Series:

- interfacing with the modem, and
- selecting and inputting the desired operational parameters

Interfacing to the IP Series for the purpose of initially configuring it may be accomplished in one of two ways:

- front COM2 connector, a PC running terminal communications program (e.g. Hyper-Terminal), or
- rear ETHERNET (RJ45) port, ethernet crossover cable, and PC running Microhard Systems Inc. DiscoverIP utility and Web Browser application.

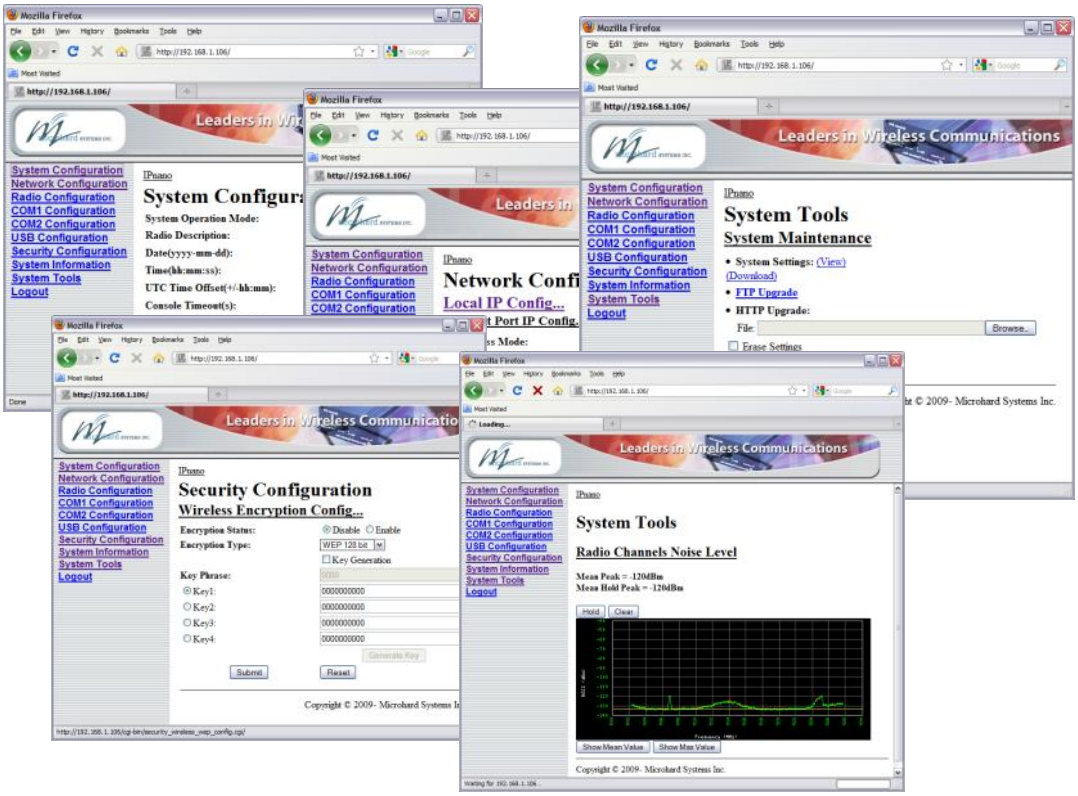
All configuration of the IP Series is accomplished with a PC. There are no DIP switches to set; switches which may subsequently become inadvertently misadjusted or intermittent.

6.0 Configuration

6.1 Web User Interface

The modem will arrive from the factory with DHCP enabled and a unique random Class D IP address.

The DiscoverIP utility is utilized to 'discover' the IP address of the IP Series (not other devices on network) so that you may specifically address it (in Web Browser URL line) for configuration purposes.



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

- Remotely or locally configure a Nano IP unit, including:
  - Operating Mode (Bridge, Router)
  - Network settings
  - Radio configuration
  - Serial Port configuration
  - Security
  - USB
- Retrieve unit revisions
- Update system firmware
- Much more...

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

6.0 Configuration

6.1.1 Logon Window

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

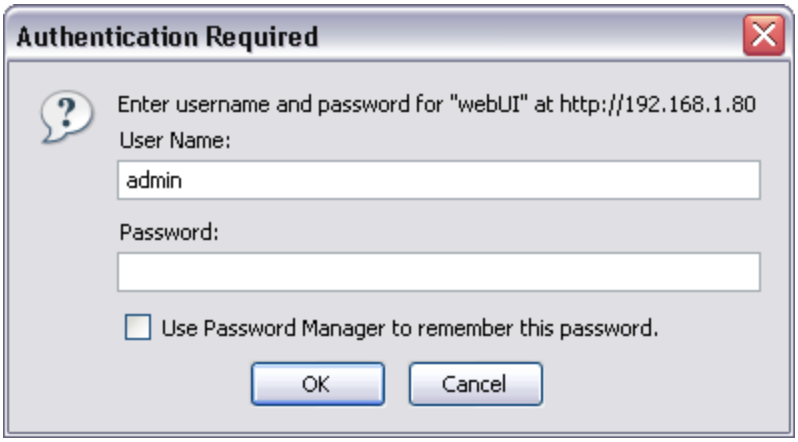


Image 6A: Logon Window

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

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

The default password is: **admin**

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

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

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

It is advisable to change the login Password (see Section 6.1.6.1). Do not FORGET the new password as it cannot be recovered.

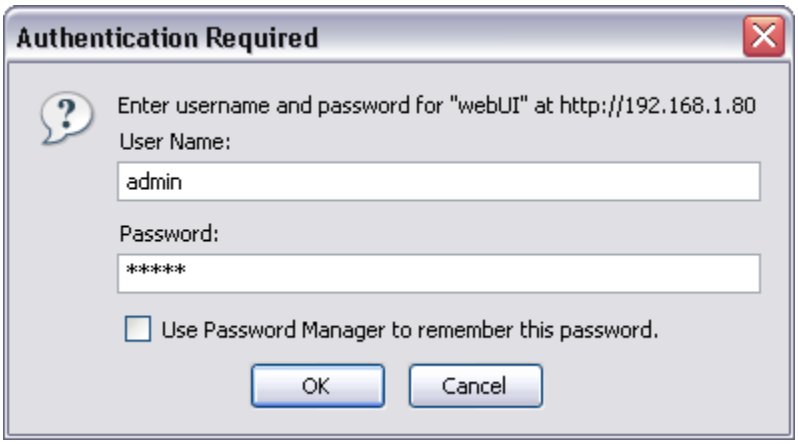


Image 6B: Logon Window With Password Input

6.0 Configuration

6.1.2 Welcome Window

The Welcome window displays the specific Nano IP Series' name (entered as the Radio Description in the System Configuration menu). This name quickly confirms the 'identity' of the unit being perused and appears in all menu windows.

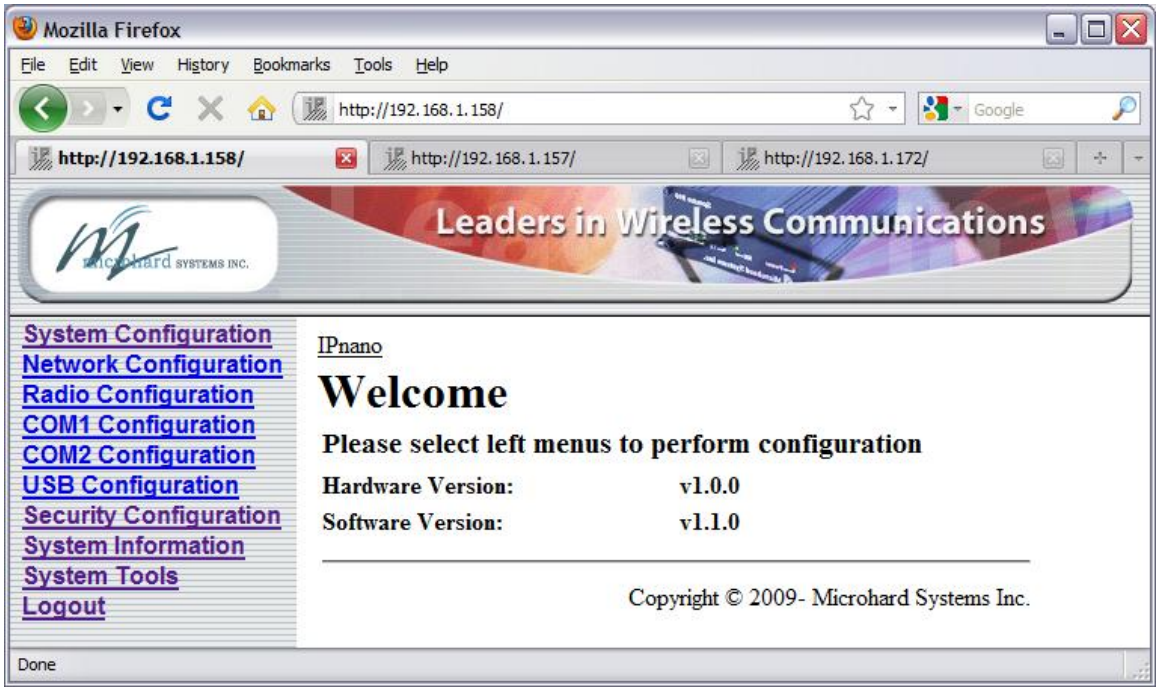


Image 6C: Welcome Window

Also displayed is various 'version' information:

- Hardware Version - applicable to the motherboard of the Nano IP Series
- Software Version - this software resides on the motherboard and is also referred to as the unit's 'firmware'

6.0 Configuration

6.1.3 System Configuration

As per the previous section, the Radio Description is defined within this menu, as are an assortment of other configuration options.

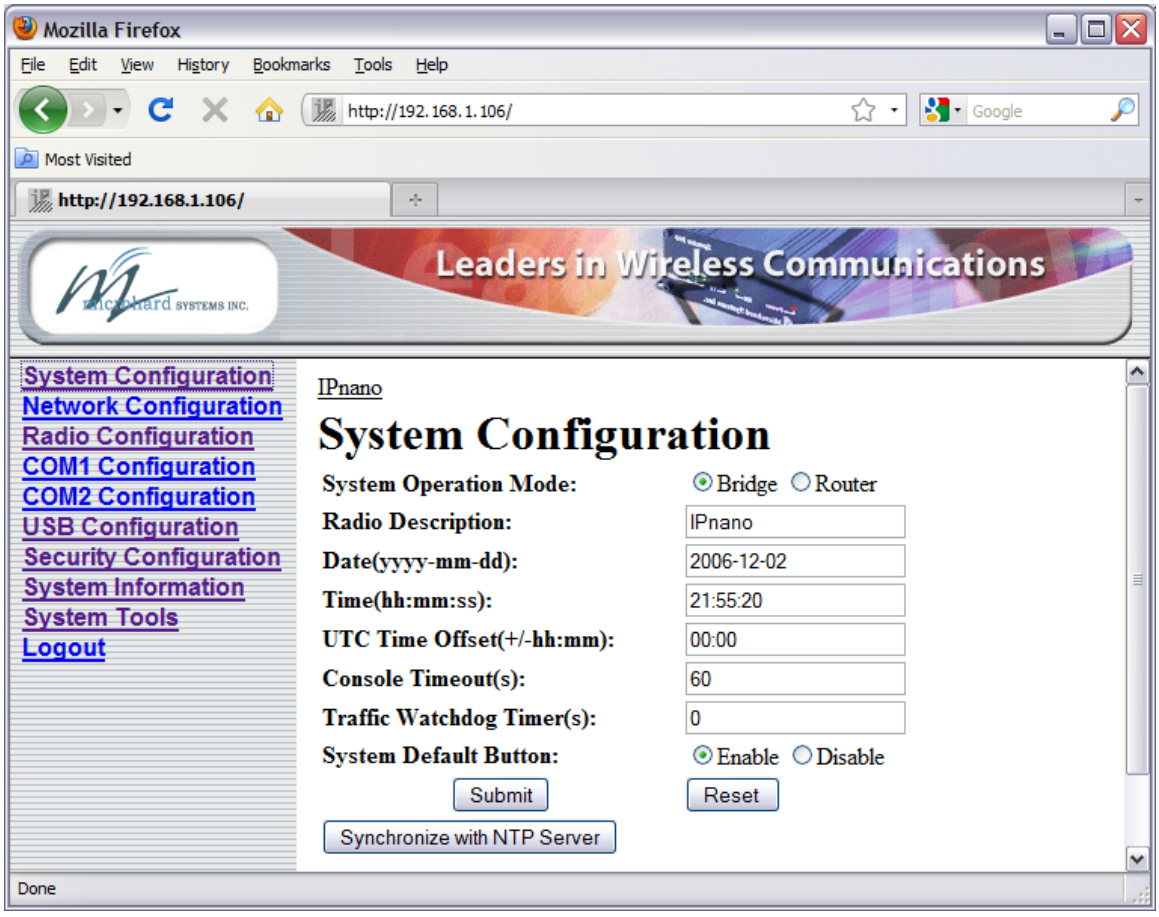


Image 6D: System Configuration Window

System Operation Mode	
The radio button options presented here determine whether the IP Series unit will operate at a BRIDGE or a ROUTER. Only a MASTER unit should ever be configured as a router.	**Values**
	Bridge
Select the System Operation Mode 'first', i.e. prior to configuring other options within the unit.	Bridge Router

6.0 Configuration

The Radio Description must not be confused with the **Network Name** (Radio Configuration menu). The Network Name MUST be exactly the same on each unit within an Nano IP Series network.

Radio Description

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

Values

Default is model-dependent

up to 30 characters

Date (yyyy-mm-dd)

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

Values

2007-05-07 *(varies)*
valid date values, where

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

Time (hh:mm:ss)

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

Values

11:27:28 *(varies)*
valid time values, where

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

UTC Time Offset (+/-hh:mm)

Input the Universal Coordinated Time offset in this field, if so desired. + indicates that local time is ahead of UTC time; - behind.

Values

00:00

valid time values, where

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

Console Timeout (s)

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

Values

seconds

60
0-65535

6.0 Configuration

Traffic Watchdog Timer (s)	
The Traffic Watchdog Timer will reset the unit if there has been no RF activity in the configured time. 0 = Disabled (default)	**Values** seconds **0** 0-65535

System Default Button	
Enabled by default, when the CONFIG button on the front of the Nano IP 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 setting will not be overwritten.	**Values** **Enable** Disable

Soft Buttons

- **Synchronize with NTP Server**
  Useable to have related parameters on this page updated with current time values when valid NTP Server information has been configured and the service is enabled within the modem (see Section 6.1.3.2 for additional information).

- **Submit**
  Write parameter values into memory.

- **Reset**
  Restore ‘currently’ modified parameter values to those which were previously written into memory.

6.0 Configuration

6.1.4 Network Configuration

The Network Configuration menu consists of a number of submenus, all of which provide various options pertaining to configuring the units to be part of an IP network. These settings do not effect the 'radio' communications network aspect of the system, however, be mindful of the Network Type (Radio Configuration menu) as that dictates the possibilities for the flow of network data.

For a basic implementation, only the Local IP Configuration (submenu) options need to be defined.

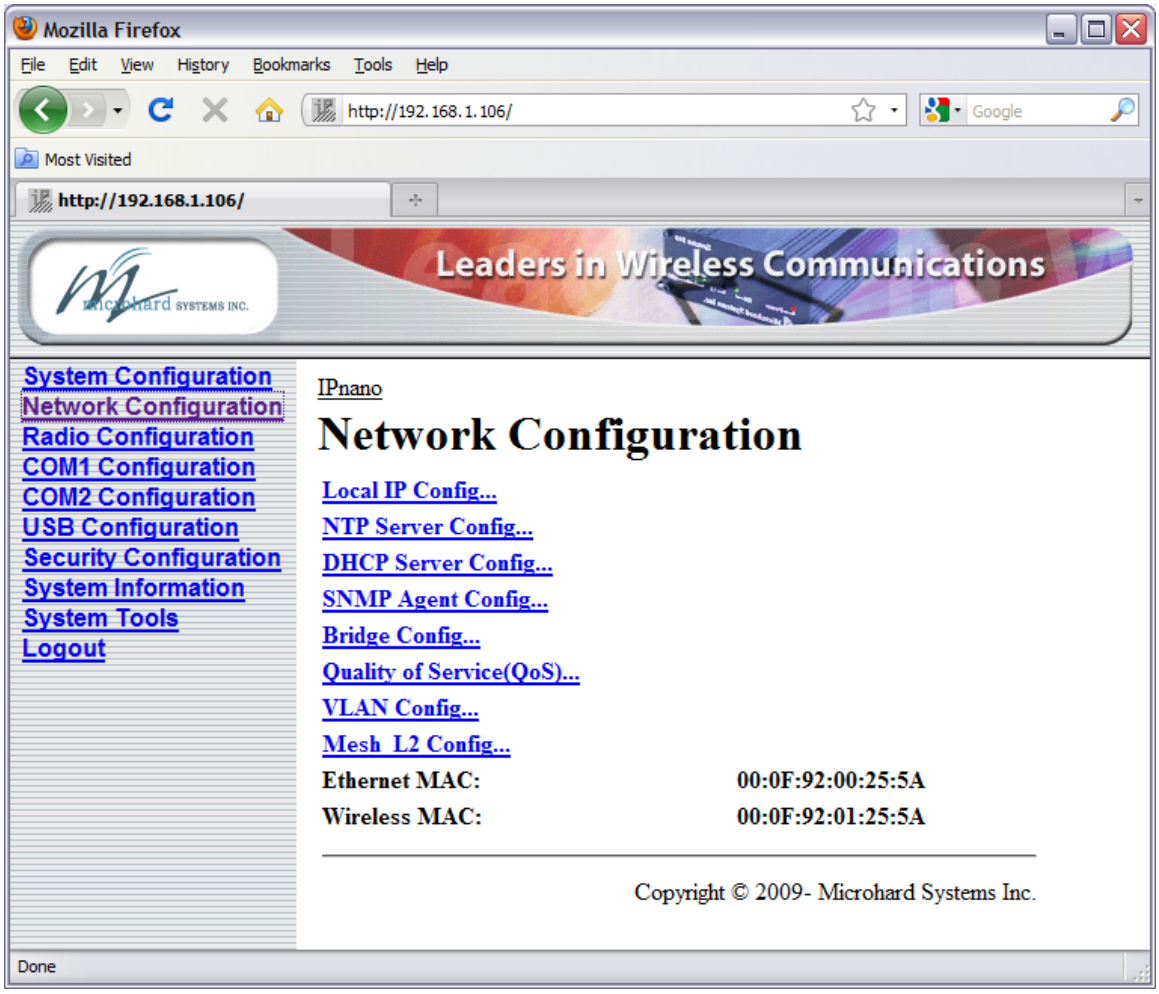


Image 6E: Network Configuration, Top Level Menu

The Ethernet MAC address (as displayed above) is that of the ETHERNET interface located at the rear of the Nano IP Series.

The Wireless MAC address is for internal purposes.

6.0 Configuration

6.1.4.1 Local IP Configuration

6.1.4.1.1 Bridge

This submenu, along with Radio Configuration settings, are the minimum which must be considered when implementing any Nano IP Series network.

It must be determined if the unit is to be either:

- assigned an IP address (by a DHCP server), or
- given a static (unchanging) IP address.

Once the above is ascertained, the items within this submenu may be configured.

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.

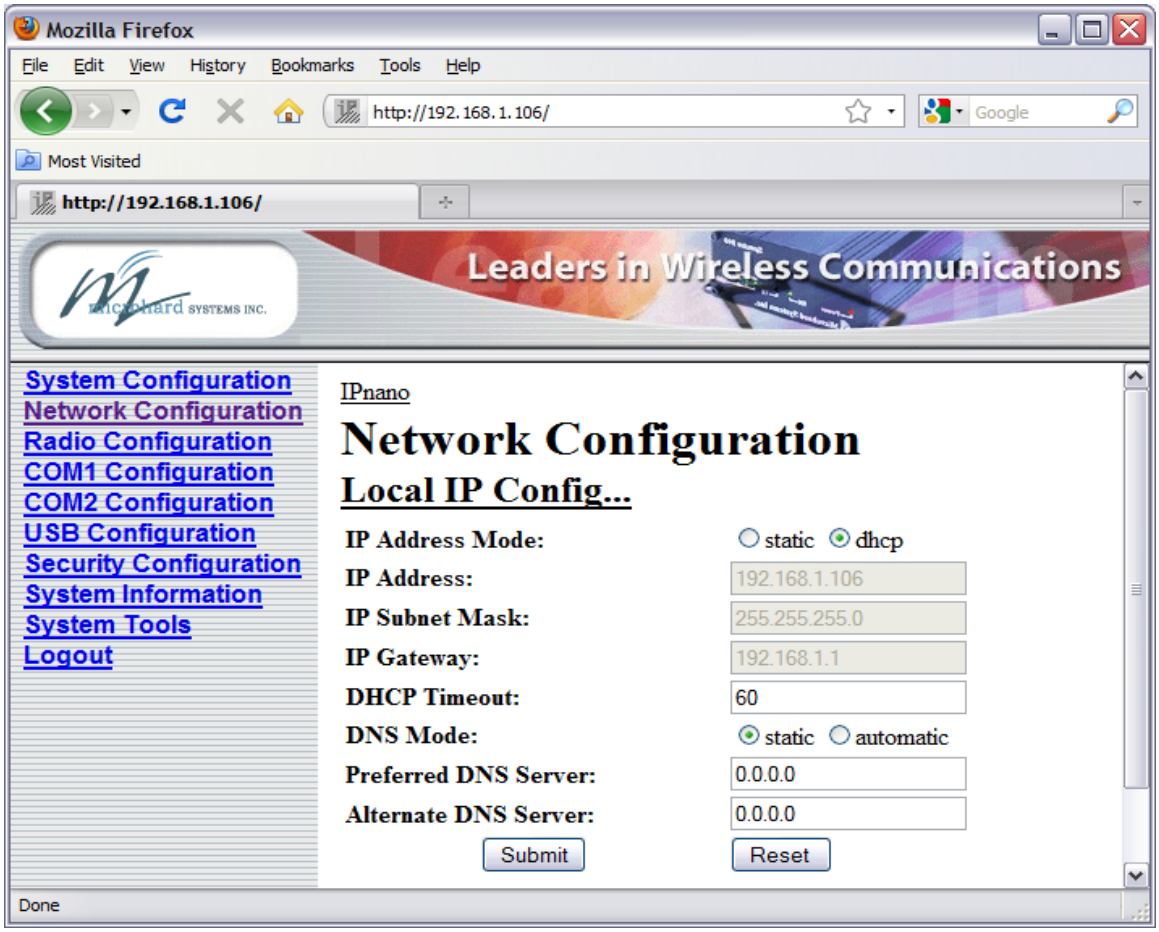


Image 6F: Network Configuration (Bridge), Local IP Configuration Submenu

6.0 Configuration

If DHCP mode is selected, but there is no DHCP server available, after the DHCP timeout period the units will default to function simply as a 'wireless bridge'.

IP Address Mode

If 'static' is selected, the three following fields are to be manually populated with values which will suit the network/devices to which the Nano IP Series is connected.

If 'DHCP' is selected, the three following fields will be automatically populated by the DHCP server. The DHCP Timeout value may be manually modified from the factory default value.

Values

static
dhcp

IP Address

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

If DHCP is selected (see above), a unique IP address will be assigned to the Nano IP Series; if STATIC IP address mode has been selected, enter a suitable value for the specific network.

Values

192.168.1.254

valid value is specific to the network

Subnet Mask

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.

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

If DHCP mode is selected, the DHCP server will populate this field.

Values

255.255.255.0

valid value is specific to the network

IP Gateway

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

In typical networks, a router acts as a gateway.

If the Nano IP Series units are integrated into a network which has a defined gateway, then, as with other hosts on the network, this gateway's IP address will be entered into this field. If there is a DHCP server on the network, and the IP Address Mode is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

In a very small network (e.g. point-to-point, and STATIC IP Address Mode), the gateway value is not critical. The IP address of the most significant device on the overall network may be entered, or, if only two Nano IP Series units are being used, make the gateway of IP Series No. 1 = IP address of IP Series No. 2; gateway of IP Series No. 2 = IP address of IP Series No. 1. The idea behind this approach is: If an IP Series at 'one end' of a wireless link receives a packet it is unsure where to send, send it to the other end of the wireless link (i.e. the other IP Series) where it was quite likely destined.

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.

Values

192.168.1.1

valid value is specific to the network

6.0 Configuration

DHCP Timeout

This value determines for how long the Nano IP Series will await to receive information from a DHCP server. If this timeout expires, the unit will assign itself a random Class D IP address (and subnet mask) and function simply as a wireless bridge.

Values

seconds

60
1-65535

DNS Mode

The setting determines whether the Nano IP Series will have its DNS Server information entered manually (static) or if it will obtain the information (provided it is available) via the connected network.

Values

static
automatic

Preferred DNS Server

If DNS Mode is static, enter valid IP Address of accessible Preferred DNS Server in this field.

Values

0.0.0.0
valid DNS Server IP address

Alternate DNS Server

If DNS Mode is static, enter valid IP Address of accessible Alternate DNS Server in this field.

Values

0.0.0.0
valid DNS Server IP address

Soft Buttons

- Submit
  Write parameter values into Nano IP Series memory.

- Reset
  Restore 'currently' modified parameter values to those which were previously written into Nano IP Series memory.

6.0 Configuration

6.1.4.1 Local IP Configuration

6.1.4.1.2 Router

If the Nano IP Series unit has been configured as a Router (under the System Configuration menu), the Network Configuration will present some additional options to those presented if the unit was configured as a Bridge.

Only the MASTER Nano IP Series unit may be configured as a Router.

The Ethernet Port IP Configuration applies to the 'wired' port (at rear of IP Series unit), which may also be considered as the WAN (Wide Area Network) port.

The Wireless Port IP Configuration applies to the LAN (Local Area Network): the LAN consists of the devices, and Nano IP Series units, connected to each other via the wireless (radio) network.

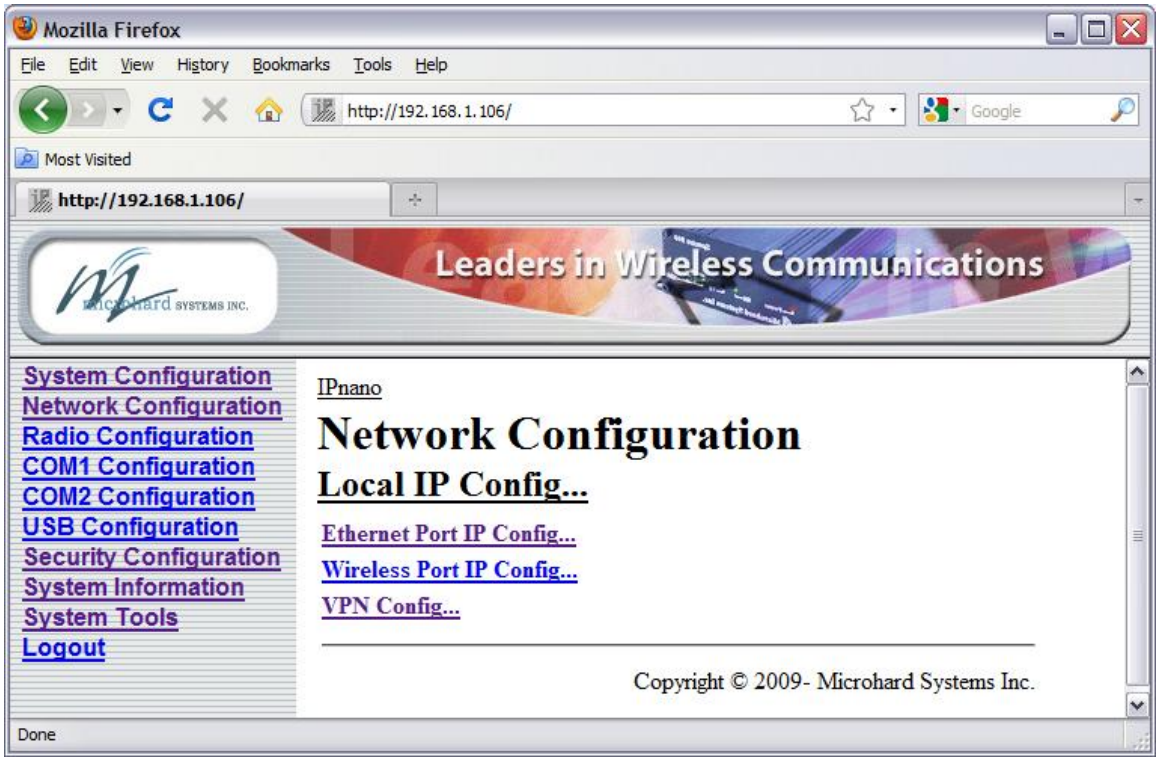


Image 6G: Network Configuration (Router), Local IP Configuration Submenu

Refer to the preceding section for configuring the Ethernet Port, keeping in mind that the settings apply only to the 'wired' connection of the MASTER unit.

There are two other options to be discussed further on the following pages:

- Wireless Port IP Configuration
- VPN Configuration

6.0 Configuration

6.1.4.1.2.1 Wireless Port IP Configuration

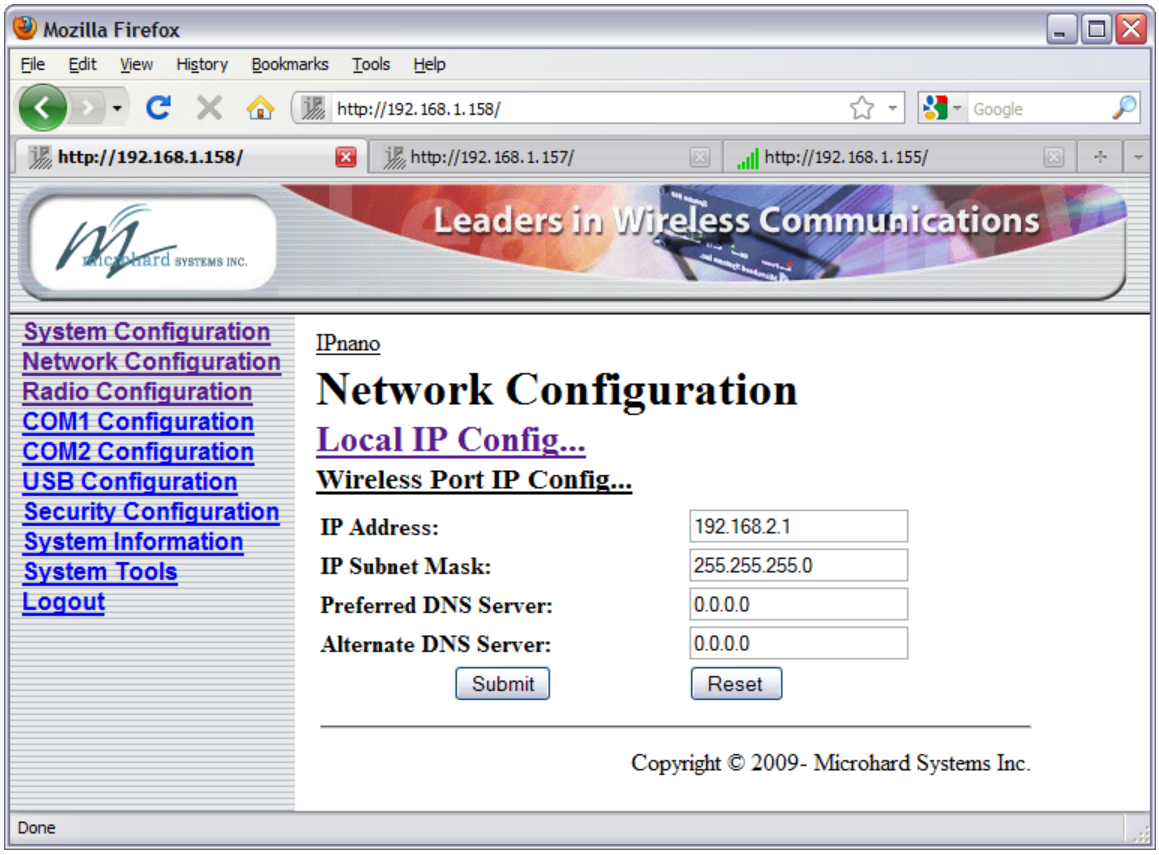


Image 6H: Network Configuration (Router), Wireless Port IP Configuration Submenu

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

IP Address	
This address MUST be STATIC (i.e. DHCP is not applicable).	**Values** **192.168.2.1** valid value is specific to the network, typically a Class C private IP

Subnet Mask	
For a small private network with IP addresses appearing similar to 192.168.1.xx (Class C address), the standard 255.255.255.0 subnet mask may be applicable.	**Values** **255.255.255.0** valid value is specific to the network

6.0 Configuration

Preferred DNS Server	
If applicable, enter valid IP address of Preferred DNS Server which exists within the LAN (the wireless subnet) in this field.	**Values** **0.0.0.0** valid DNS Server IP

Alternate DNS Server	
If applicable, enter valid IP address of Alternate DNS Server which exists within the LAN (the wireless subnet) in this field.	**Values** **0.0.0.0** valid DNS Server IP

Soft Buttons

- Submit
  Write parameter values into memory.
- Reset
  Restore 'currently' modified parameter values to those which were previously written into memory.

6.0 Configuration

6.1.4.1.2.2 VPN Configuration

A Virtual Private Network (VPN) may be configured to enable a direct communications link between one device on the WAN and another on the LAN.

VPN: Virtual Private Network. A communications path connecting a device on a WAN with a device on a LAN.

Image 6I: Network Configuration (Router), VPN Configuration Submenu

VPN Status

Enable (default) enables the service; Disable disables it.

Values

Enable
Disable

VPN Admin Password

Select a unique password of 32 characters maximum, case-sensitive.

Values

admin
32 characters maximum

VPN Admin Repeat Password

Enter the same unique password of 32 characters maximum, case-sensitive, which was entered in the preceding/above field.

6.0 Configuration

6.1.4.2 NTP Server Configuration

The Network Time Protocol (NTP) feature may be ENABLED, provided there is an NTP server available and its IP address or 'name' is entered in the appropriate field.

NTP may be used to synchronize the time in the Nano IP Series within a network to a reference time source.

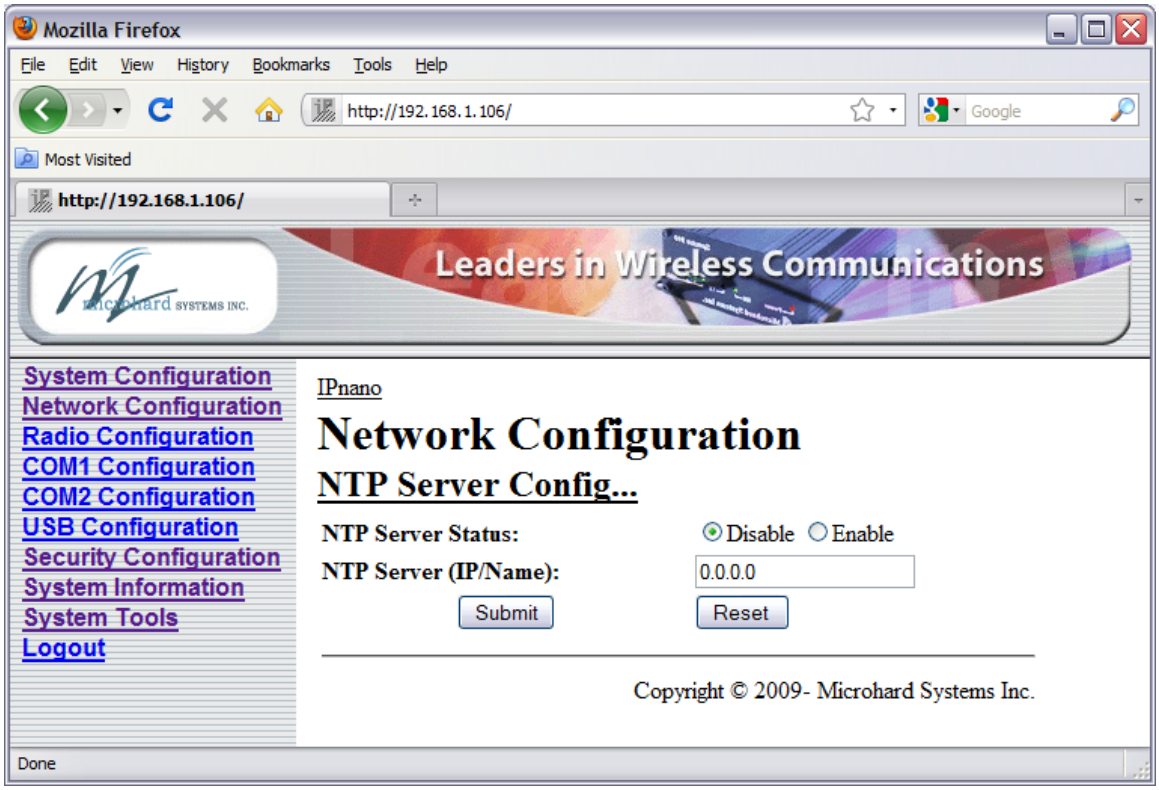


Image 6G: Network Configuration, NTP Server Config. Submenu

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

NTP Server (IP/Name)	
IP address or domain name for NTP server (on local LAN or website (provided that Internet access is available)) is to be entered in this field if the NTP Server Status is configured as ENABLED.	**Values** **0.0.0.0** valid NTP server IP address or 'name'

6.0 Configuration

6.1.4.3 DHCP Server Configuration

There is a difference in how the DHCP Server operates based on whether the Nano IP Series unit (Master) is configured to function as a bridge or a router.

6.1.4.3.1 Bridge

The Nano IP Series Master may be configured to provide dynamic host control protocol (DHCP) service to all attached (either wired or wireless-connected) devices.

Configuration field descriptions are discussed in the following section.

6.1.4.3.2 Router

An Nano IP Series Master may be configured to provide dynamic host control protocol (DHCP) service for an entire LAN (or section thereof). Recall that the LAN consists of wirelessly connected Nano IP Series units and those IP addressable devices which are connected to them. If this feature is to be utilized, it would be enabled on the Master Nano IP Series unit, noting that such a DHCP Server service must not be enabled on any other IP Series units or devices which reside on the same network segment.

With this service enabled on the Master, it can assign IP addresses (as well as subnet mask and gateway) to the LAN radios and IP devices attached to them provided they are set for DHCP as opposed to static.

The DHCP Server may also be used to manage up to five MAC address bindings. MAC address binding is employed when certain devices are to be assigned specific IP addresses (effectively issuing them a 'static' IP address). Such devices are identified by their unique MAC address: the DHCP Server ensures that a specified IP address is assigned to a specific MAC address (hence, device - either an Nano IP Series or other IP-based device attached to the LAN).

6.0 Configuration

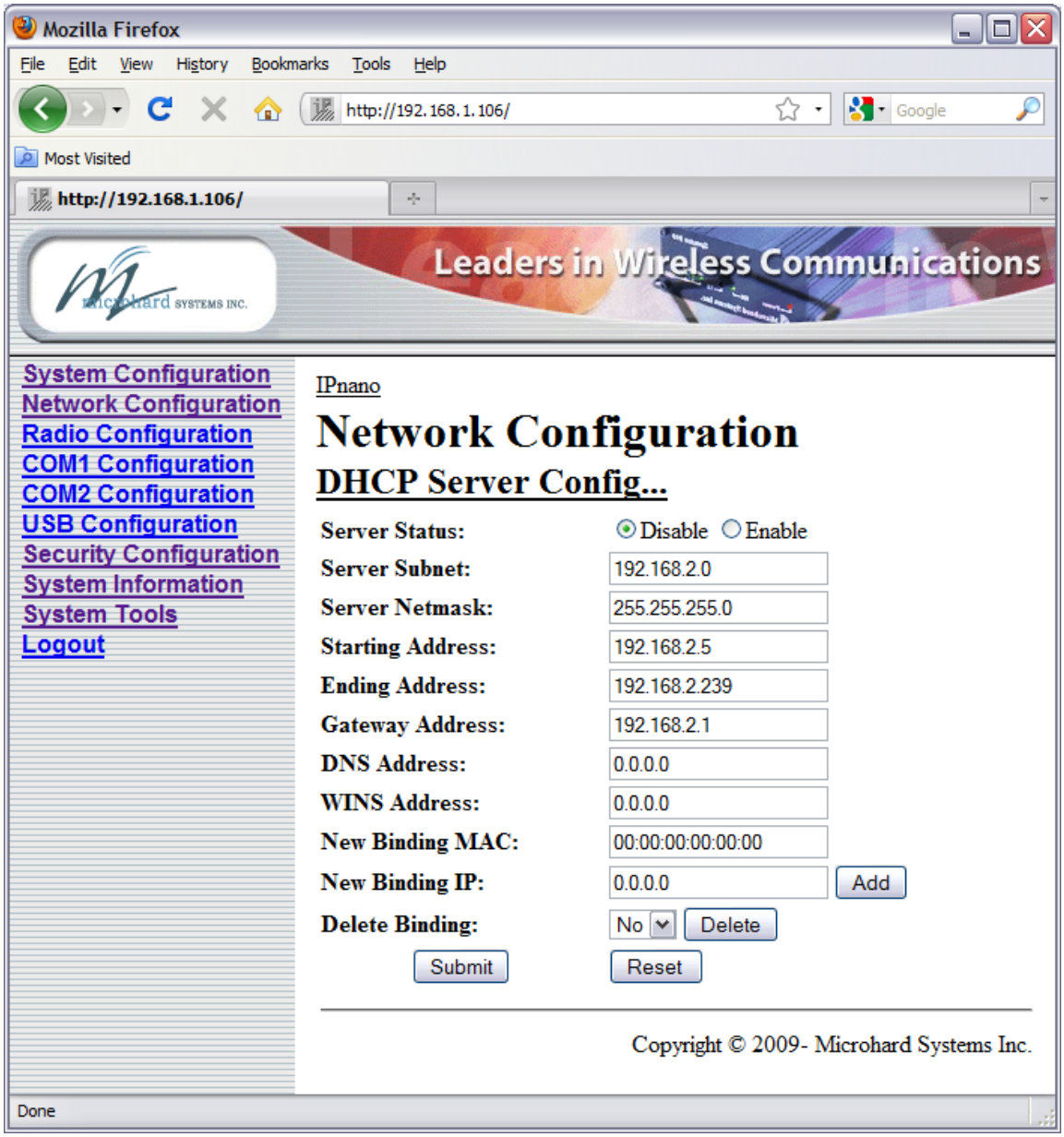


Image 6J: Network Configuration, DHCP Server Config. Submenu

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

Server Status

Choose to enable or disabled the DHCP Server service. Note that there can only be one such service residing on a network segment - otherwise, duplicate IP addresses could be assigned and exist on a network, which would result in problems. Devices on the network, which are intended to receive IP address information from this DHCP Server, must have their local IP settings set for 'DHCP' (as opposed to 'static')

Values

Disable
Enable

6.0 Configuration

Server Subnet

Not to be confused with the Server Netmask (see below). Enter the network's 'root' address, e.g. if devices are to be assigned addresses such as 192.168.1.5 and 192.168.1.6, enter 192.168.1.0 in this field.

Values

192.168.2.0

valid server subnet value for specific network

Server Netmask

In this field, input the subnet mask which is to be applied to the network. For basic, small, private networks, a Class C subnet mask such as 255.255.255.0 could be used.

Values

255.255.255.0

valid subnet mask value for specific network

Starting Address

This is the starting ('lower boundary') IP address of the range of IP addresses (also known as 'IP address pool') to be issued by the DHCP Server to the applicable devices on the network.

Values

192.168.2.5

IP address as per above

Ending Address

This is the ending ('upper boundary') IP address of the range of IP addresses to be issued by the DHCP Server to the applicable devices on the network.

Values

192.168.2.239

IP address as per above

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').

Gateway Address

Input the address of the desired gateway.

Values

192.168.2.1

IP address as per above

DNS Address

Input the IP address of the Domain Name Service (DNS) to be provided by this DHCP Server.

Values

0.0.0.0

Valid DNS IP address

6.0 Configuration

WINS: Windows Internet Naming Service keeps track of which IP address is assigned to which computer on a Windows network: a process known as name resolution. It automatically updates, which is particularly important on a network where DHCP is in use.

WINS Address

Windows Internet Naming Service (WINS) address to be provided by this server.

Values

0.0.0.0
Valid WINS IP address

New Binding MAC

In this field, input the MAC address (in specified format) of the device to which a specific IP address is to be bound.

For the Nano IP, the MAC address of the unit may be found on the label on the bottom of the unit, or it may be viewed on the Network Configuration menu of that unit.

Values

00:00:00:00:00:00

MAC address of target device

An address binding is a mapping between a specific IP address and the MAC address of a specific client.

New Binding IP

Enter the IP address - from within the range identified with the Starting Address and Ending Address parameters input previously - which is to be 'bound' to the MAC address identified in the New Binding MAC field (described above).

Values

0.0.0.0

IP address from within range identified in Starting Address and Ending Address fields

Soft Buttons

- Add
  After entering a New Binding MAC address and a New Binding IP address, click this soft button to ADD this new binding relationship.

  Once 'added', the new relationship will be given a number (e.g. Bound 1) and appear at the lower portion of the DHCP Server Config. menu display, showing both the MAC and corresponding IP address.

  Note that the ADD action must be followed by SUBMIT for the changes to be written to memory.

- Delete
  If binding relationships are present, the drop down box (to left of Delete soft button) may be used to select a particular binding, and the DELETE soft button used to delete it.

- Submit
  Write parameter values into memory.

- Reset
  Restore 'currently' modified parameter values to those which were previously written into memory.

6.0 Configuration

6.1.4.4 SNMP Agent Configuration

The Nano IP Series 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: Simple Network Management Protocol provides a method of managing network devices from a single PC running network management software.

Managed networked devices are referred to as SNMP agents.

SNMP may be used in several ways:

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

A SNMP management system (a PC running SNMP management software) is required for this service to operate. This system must have full access to the IP Series network. Communications is in the form of queries (information requested by the management system) or traps (information initiated at, and provided by, the SNMP agent in response to predefined events).

Objects specific to the Nano IP Series 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.

6.0 Configuration

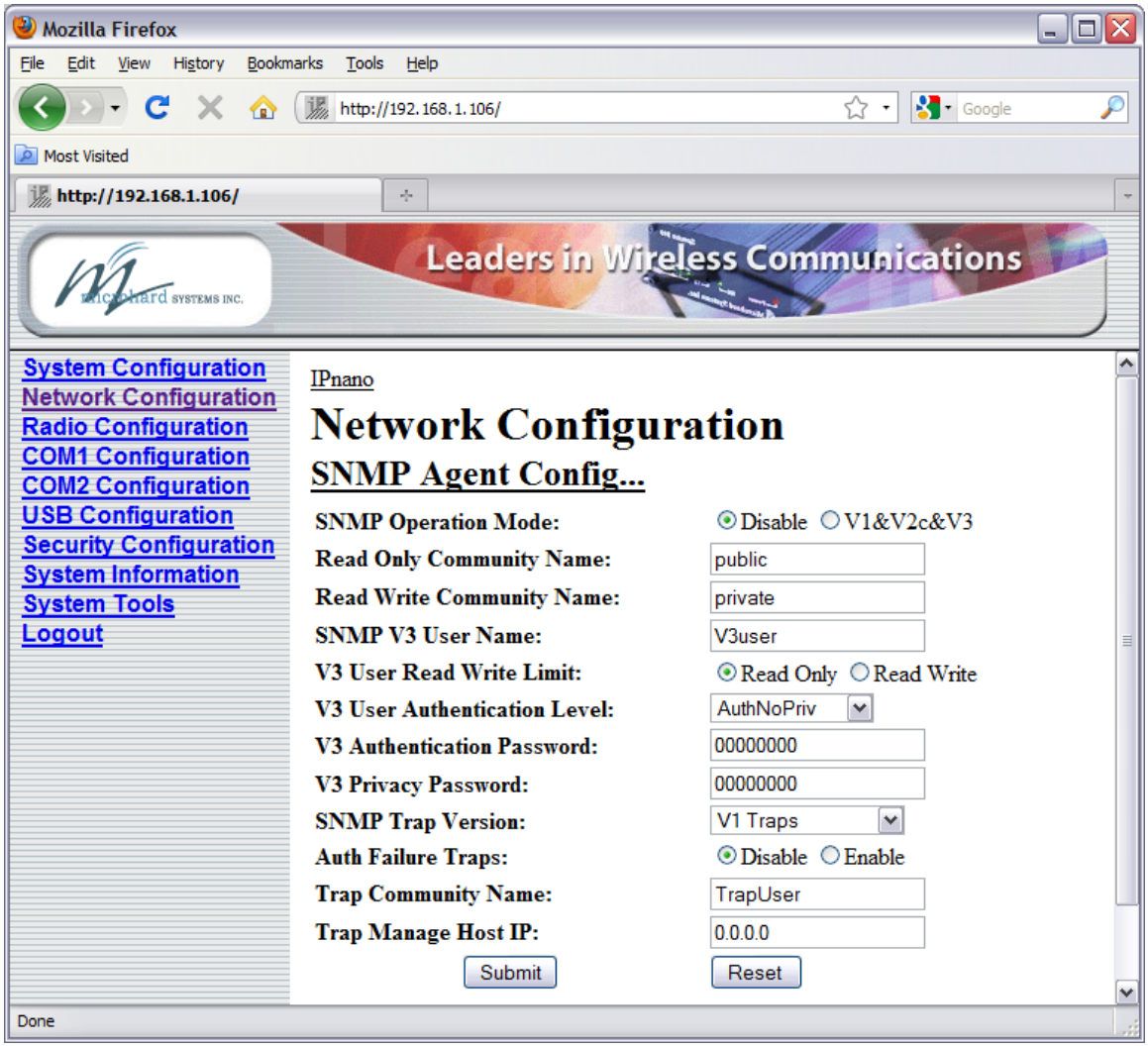


Image 6K: Network Configuration, SNMP Agent Config. Submenu

SNMP Operation Mode

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

Values

Disable
V1&V2&V3

Read Only Community Name

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

Values

public

character string

6.0 Configuration

Read Write Community Name

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

Values

private

character string

SNMP V3 User Name

Defines the user name for SNMPv3.

Values

V3user

character string

V3 User Read Write Limit

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

Values

Read Only
Read Write

V3 User Authentication Level

Defines SNMPv3 user's authentication level.

NoAuthNoPriv: No authentication, no encryption.

AuthNoPriv: Authentication, no encryption.

AuthPriv: Authentication, encrpytion.

Values

NoAuthNoPriv
AuthNoPriv
AuthPriv

V3 Authentication Password

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

Values

00000000

character string

V3 Authentication Password

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

Values

00000000

character string

6.0 Configuration

SNMP Trap Version

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

Values

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

Auth Failure Traps

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

Values

Disable
Enable

Trap Community Name

The community name which may receive traps.

Values

TrapUser

character string

Trap Manage Host IP

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

Values

0.0.0.0

applicable host's IP

Soft Buttons

- Submit
  Write parameter values into memory.
- Reset
  Restore 'currently' modified parameter values to those which were previously written into memory.

6.0 Configuration

6.1.4.5 Bridge Configuration

In most deployments, Spanning Tree Protocol (STP) will not be required. It does consume a small amount of bandwidth. The default is 'On'. If desired, change the status to 'Off'.

Note that this menu item will not appear if the IP Series unit is configured to be a router.

STP: Spanning Tree Protocol is a link management protocol which will accommodate the availability of redundant data paths but inhibit the possibility of a loop being created: a loop could create endless traffic 'around' a LAN, consuming much of the bandwidth.

Image 6L: Network Configuration, Bridge Config. Submenu

Spanning Tree Protocol Status	
Selection of STP operational status: On or Off.	**Values** **On** Off

Soft Buttons

- Submit
  Write parameter values into memory.
- Reset
  Restore 'currently' modified parameter values to those which were previously written into memory.

6.0 Configuration

6.1.4.6 Quality of Service

Quality of Service (QoS) may be applied to various data which enter the Nano IP Series. This section describes configuring QoS for data which enters via the ethernet port.

QoS: Quality of Service is applied to networks where it is desired to give particular data traffic/ protocol(s) priority over other data traffic.

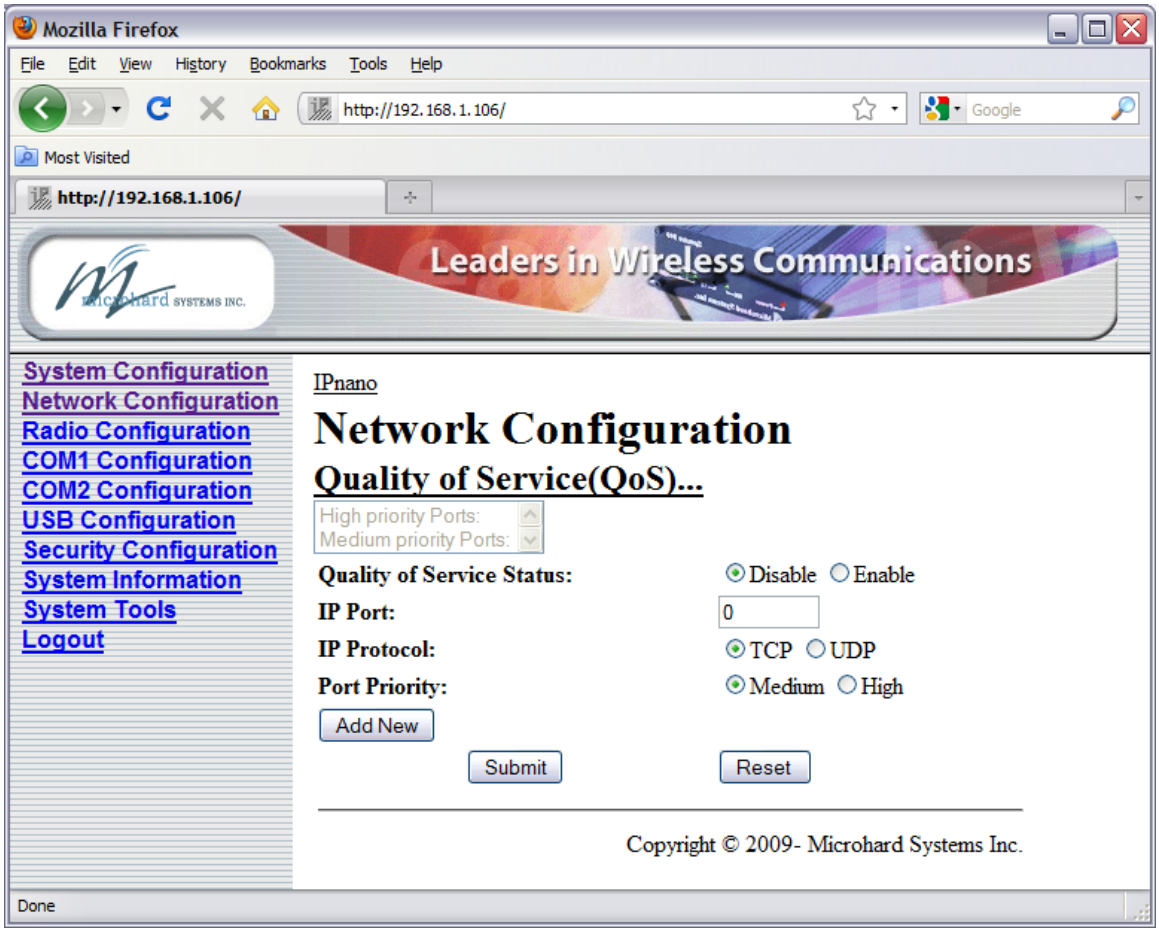


Image 6M: Network Configuration, Quality of Service Submenu

Quality of Service Status	
If Enabled, the defined protocols and ports will have the QoS service applied to them.	**Values** **Disable** Enable

To define particular ports, protocol, and priority to be assigned, see the example of such a configuration exercise on the following page.

6.0 Configuration

Example 6.1.4.6.1

Assume that we want to add high priority to TCP traffic on Port 8080:

- In the IP Port field, enter 8080.
- Select the radio button for TCP.
- Select the radio button for High Priority.
- Click the ADD NEW soft button.
- Click the SUBMIT soft button.

The following screen capture shows the result of the above actions:

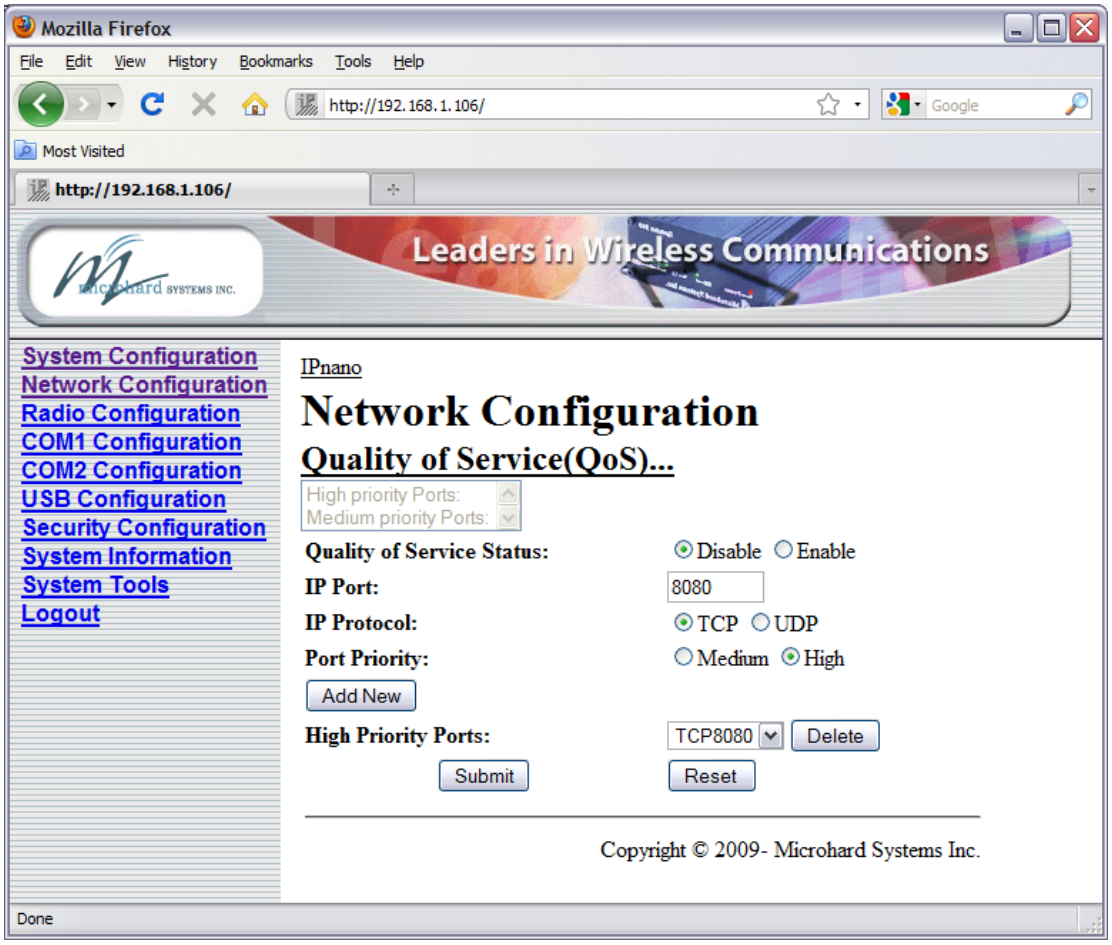


Image 6N: Network Configuration, QoS Example

The mini window shows port 8080, TCP traffic, as having High Priority. To apply the configuration: select Enable and SUBMIT.

As ports are defined, the mini window and list boxes (specific to Priority) become populated. To DELETE any defined port, simply select it via the appropriate list box and click the DELETE soft button.

6.0 Configuration

6.1.5 Radio Configuration

The parameters within the Radio Configuration menu must be input properly; they are the most basic requirement for radio network connectivity.

Prior to configuration, the network topology must be known (see Section 5.0); the role (operating mode) of the specific Nano IP Series must also be known.

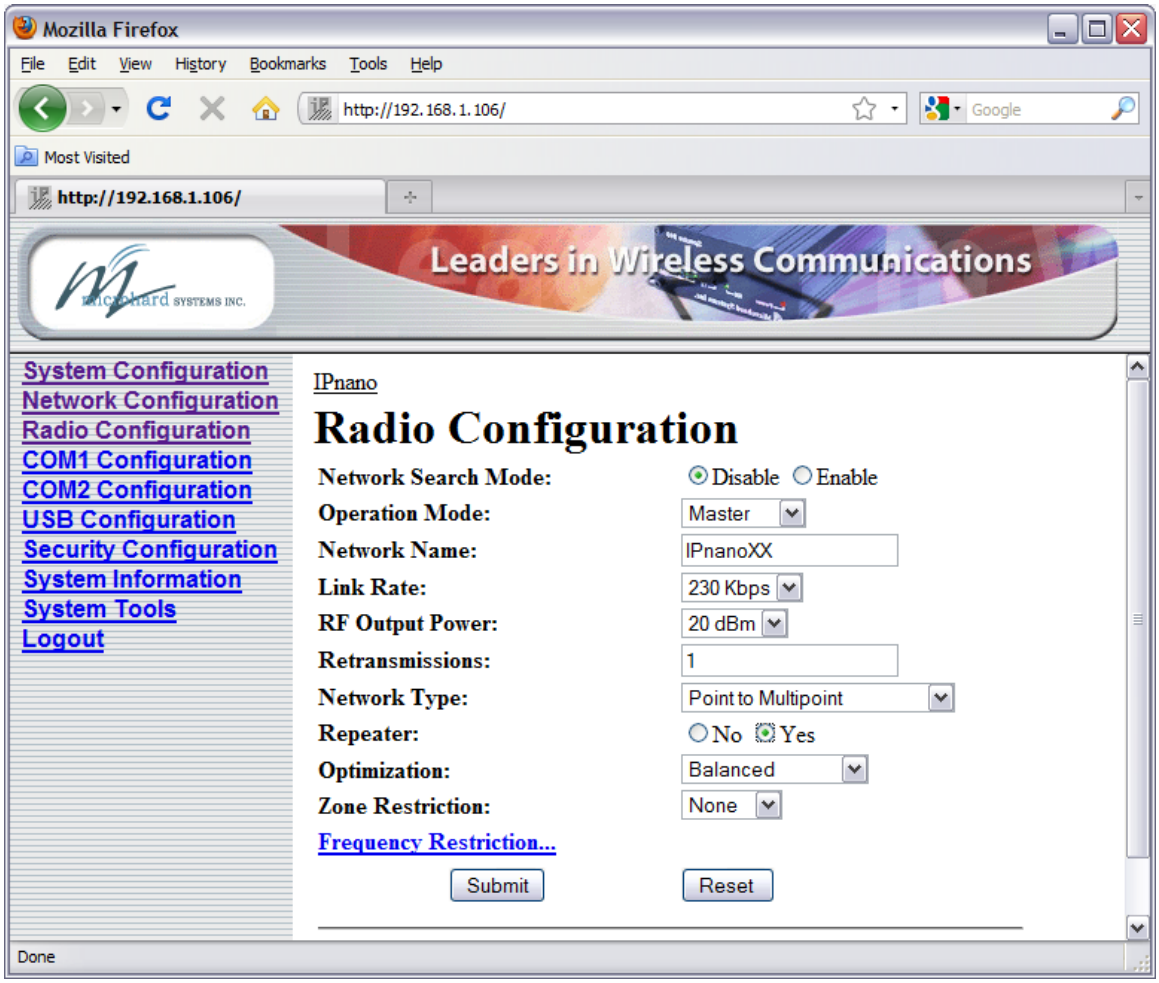


Image 6O: Radio Configuration Menu (upper portion)

Network Search Mode

The above screen capture depicts Radio Configuration menu option with Network Search Mode disabled. On the following page, the screen capture shows what configuration options are available when Network Search Mode is enabled.

6.0 Configuration

Network Search Mode (continued)

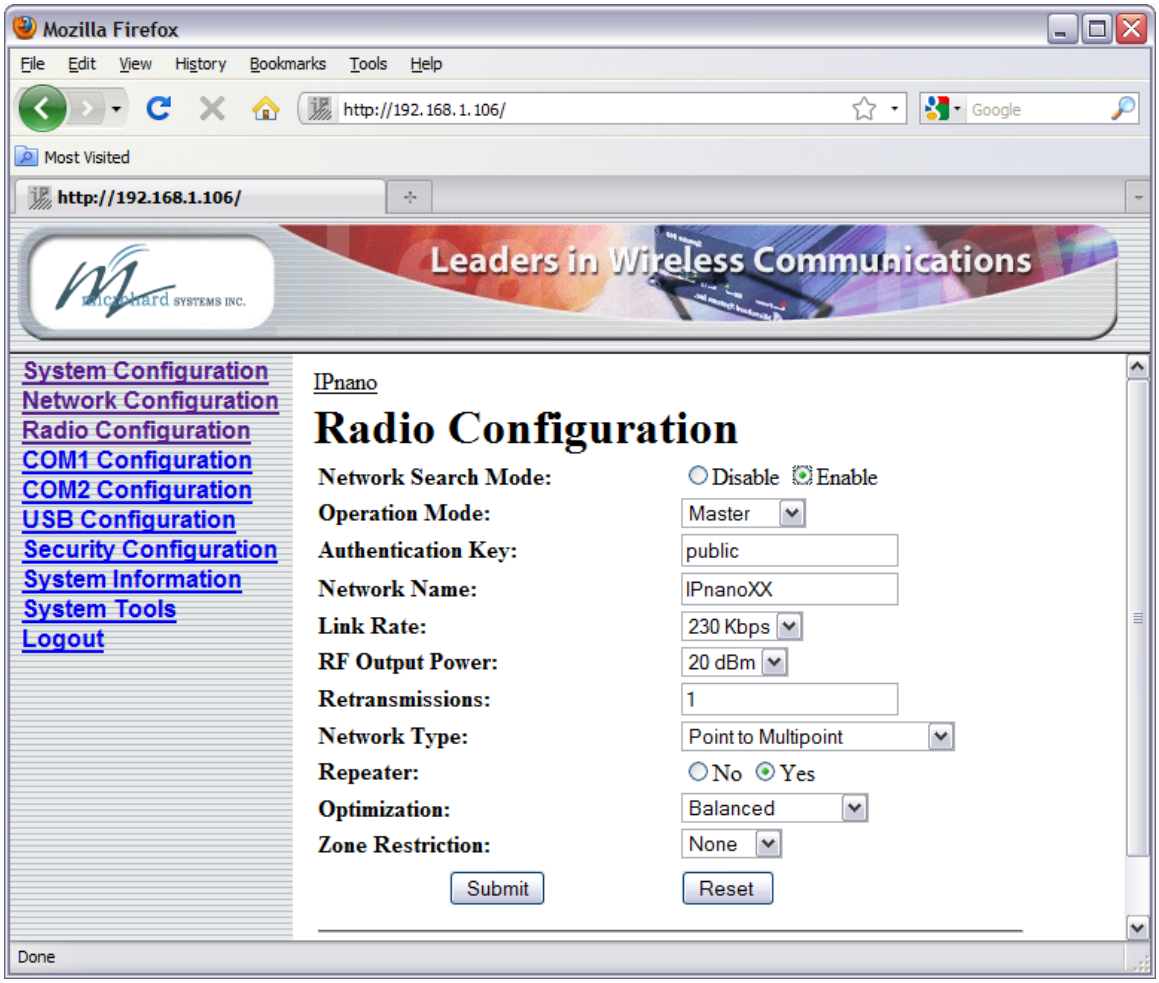


Image 6P: Radio Configuration Menu (upper portion), with Network Search Mode Enabled

With Network Search Mode enabled, Master units with the same authentication key may be found by Remote units even if they have different network names. This feature, which must be enabled on all participating units, allows for 'roaming' between networks.

Values

Disable

Disable
Enable

6.0 Configuration

Operation Mode

Select the mode of operation for the Nano IP Series: Master, Repeater, or Remote. A Nano IP Series may be configured for any role required within a radio network. This is convenient for reasons of familiarity, as well as for hardware sparing purposes.

Values

Master
Repeater
Remote

Master: Only one per network. For all Network Types data either originates at, is destined to, or 'passes through' the Master.

The selected Operation Mode will effect which configuration options are presented.

i.e. There are settings which apply to a Master which do not apply, and are therefore not presented, for a Remote.

Repeater: May act simply as a 'Repeater' to store and forward data to/from an upstream unit to/from a downstream unit (e.g. when there is a long distance between the latter units), or, may act as a Repeater/Remote in which case the above function is performed AND the unit may also exchange data as a Remote within the network.

If 1 or more repeaters are to be in a network, on the Master (only) the Repeater(s) YES configuration must be selected.

If 2 or more repeaters are to be in a network: the above 'YES' setting applies as does the requirement for Repeater Registration (discussed further on in this section).

Remote: Interfaces with remote devices and communicates with Master either directly or via Repeater(s). Communications between 2 or more Remotes is possible - through the Master - see Network Types (further on in this section, and also refer to Section 5.3, 5.4).

Authentication Key

The Authentication Key is used to define the network search group: Masters with the same key can be found by Remotes with different Network Names.

Values

Public

Character string

Network Name

All Nano IP Series in a given network must have the same Network Name. 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

default is model-dependent

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.

Referring to the Network Profile configuration (detailed previously in this section), the Network Name can also be used as the single parameter to change when a Remote is to 'switch' from operating between distinct networks.

The Network Name is also taken into consideration in the frequency hopping algorithm: change the Network Name and the hopping pattern will change.

6.0 Configuration

Link Rate

This is the RF communications Link Rate. A lower link rate offers better receive sensitivity performance; a higher link rate, better throughput. All Nano IP Series in a network must use the same Link Rate.

Values

default value and available rate(s) are model-dependent

Unit Address

If the Operation Mode is set to MASTER, the Unit Address field will NOT be displayed in the Radio Configuration menu.

By setting the unit to Master, its Unit Address will be 1.

The unit address is, and must be, a unique identifier of each modem in a network.

The Master has by default, and must retain, a unit address of 1; 65535 is the broadcast address.

Values

number varies

2-65534

RF Output Power

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.

This setting establishes the transmit power level which will be presented to the antenna connector at the rear of the Nano IP Series.

Unless required, the RF Output Power should be set not for maximum, but rather for the minimum value required to maintain an adequate system fade margin.

Values

dBm (mW equivalent)

20 (100)
21 (125)
22 (160)
23 (200)
24 (250)
25 (320)
26 (400)
27 (500)
28 (630)
29 (800)
30 (1000)

Retransmissions

In a PMP system, set Retransmissions to the minimum value required as, effectively, the data throughput from Master to Remotes is divided by 1 plus the Retransmissions value.

This register determines the maximum amount of times that a packet will be retransmitted (in addition to the initial transmission), noting the following specific behaviors in various network topologies:

Values

5
0-255

PMP: Master will retransmit each data packet the exact number of times specified in the Retransmissions field; Remote will retransmit only if necessary, and then only until a given packet is acknowledged or the value of the Remote's Retransmissions field is reached (after which it will discard the packet if retransmission not successful). *See also 'PMP with ACK" described in the Network Type.

PTP: Nano IP Series will retransmit to its counterpart only if necessary, and to a maximum number of the value specified in its Retransmissions field. Packet is discarded if retransmissions are not successful. Recipients of packets will discard any duplicates.

6.0 Configuration

Network Type

Defines the type of RADIO network (see Section 5.0)

Values

Point-to-Multipoint
Point-to-Point
Peer-to-Peer
Everyone-to-Everyone
PMP with ACK

In a **point-to-multipoint (PMP)** network, the Master broadcasts data to all units, and all remote units send their data (ultimately) to the Master.

A **point-to-point (PTP)** network involves a Master and a Slave (with 0 or more Repeaters between them).

ALL modems in a network must have the SAME value for Network Type.

Peer-to-Peer (P2P) supports communication (through the Master) between 2 (typically remote) units.

In an **Everyone-to-Everyone (E2E)** network, all units communicate with all other units, through the Master. Note that this mode is very bandwidth-intensive.

Point-to-Multipoint with ACK is a configuration whereby the Network functions as a Point-to-Multipoint, but the Retransmissions behave as a combination of PTP and PMP in that: If retransmissions are set to 5 (for example) on the Master, and the packets it sends to the Remotes result in an ACK being received by each of the Remotes in the network, the Master will not send the data again (refer to the PMP behavior described in the preceding Retransmissions section). If, however, the Master does NOT receive an ACK from all Remotes in the network, it will then revert to sending the data again, to the maximum number of Retransmissions specified, for a period of one minute, after which time it will revert to behaving as it did originally.

Keep in mind that the Network Type determines the path that data will take.

i.e. In a PMP system, the data flows from the Master to Remotes, and from Remotes to the Master. If a ping to Remote B was sent to Remote A, it will not arrive as the data cannot travel from Remote to Remote. Similarly, a ping to a Repeater from a Remote will not arrive either: the destination for a Remote in a PMP system is the Master - not a Repeater, even though it appears in the data 'path' to the Master.

This mode of operation is particularly well-suited to fixed PMP networks when multipoint operation is required as is maximum throughput.

The selected Network Type will effect the Radio Configuration menu somewhat, i.e. If Point-to-Multipoint is selected for a Remote, there is no menu item for a Destination Address as the destination is - must be - the Master (Unit Address 1).

Destination Unit

As the name implies, this register specifies the ultimate destination for an Nano IP's data. Different network topologies dictate the configuration of the Destination Unit (address):

Values

1-65535

For a Remote in a **Point-to-Multipoint** network, this menu option will not appear: by definition, the destination is the Master (UA = 1). For the Master in PMP, its Destination Unit (Address) is 65535—the broadcast address as it sends its data to all points.

In a **Point-to-Point** configuration, the destination is to be specified (for a Remote: the Master); in the Master's Radio Configuration, specify the Unit Address of the Remote Unit to which it is to send its data.

In **Peer-to-Peer**, the Remotes are configured with the target peer's UA as the Destination Address, the Master with 65535; in **Everyone-to-Everyone**, the Destination Address for ALL units is 65535 - the broadcast address - as every unit sends its data to every other unit (through the Master). E2E is a very bandwidth intensive network topology.

6.0 Configuration

Tx Control

This configuration option does not apply to a Master Nano IP.

On (the default) permits the Nano IP to transmit, i.e. RF emissions are enabled.

Off configures the Nano IP for RECEIVE ONLY. If 'Off' is selected, 'On' may only be selected LOCALLY or via a special UDP packet sent from the DiscoverIP Utility.

Values

On
Off

Roaming Address

When bench testing 3 IP Series for a Master-Repeater-Remote link, be sure to set the Remote's Roaming Address to the Unit Address (UA) of the Repeater, and the Repeater's Roaming Address to the UA (1) of the Master.

This will ensure that data is routed from the Remote through the Repeater to the Master; otherwise, if the Remote's Roaming Address is left at the default value of 1, the Remote will communicate directly with the Master, bypassing the Repeater altogether.

This feature allows a Remote unit to synchronize with a specified 'upstream' unit (either Master or Repeater). The options are as follows:

65535: With this value as its Roaming Address, a Remote will synchronize with an upstream unit which has the same Network Name as the Remote. Should that upstream unit fail, this Remote will attempt to synchronize with another 'upstream' unit within the same network (i.e. same Network Name). This ability is particularly well-suited to mobile applications.

1-254: In most static (fixed) networks, where there are no Repeaters, the default value of 1 is maintained: All Slaves synchronize to the Master (whose unit address is 1).

In networks where Repeaters are present, the value of a Remote's Roaming Address typically corresponds to the particular upstream modem with which a particular Remote is intended to communicate, e.g. Slave with Unit Address 3 may have a Roaming Address of 2, where the modem with Unit Address 2 is a Repeater between the Slave and the Master; the Repeater will have a Roaming Address of 1 as it is to synchronize to the Master.

The Roaming Address dictates to which IP Series (by Unit Address (UA)) a Remote (or Repeater) will 'look' or 'attach to' for its upstream signal path.

See the description of Network Profile earlier in this section for more information about roaming-type options. The Network Profile allows for roaming between networks whereas the Roaming Address provides for roaming within a network.

Values

65535 full roaming

1-254 specific (fixed) unit address (Master or Repeater) with which to associate

1

6.0 Configuration

Repeater

This setting applies to the Master only.

The default value is No, stating there are no Repeaters in the network.

If there are 1 or more Repeaters in the network, configure this setting as Yes.

Values

No
Yes

With one or more Repeaters in the system, a network's throughput is divided in half. Exercising the option of back-to-back 'Repeaters' - which requires 2 Nano IP Series at a 'Repeater' site - eliminates the division of bandwidth.

If there is more than one Repeater in a network, the Repeaters should be 'registered'. See 'Repeater Registration' further along in this section re how to accomplish this.

Optimization

This setting applies to the Master only.

'Balanced' is the default setting and is typically the best choice for 'Optimization'. The other options are High Throughput (when throughput is a priority) and Low Latency (best suited to small packets).

Optimization is a trade-off between throughput and latency.

Values

High Throughput
Balanced
Low Latency

Channel Number

This setting applies and will appear only if the Link Rate is set to 1.2Mbps.

Channel Number defines the number of channels the unit will hop on. The minimum number is 4. (Digital Transmission System (DTS) technology is applied at the 1.2Mbps link rate.)

(This setting does not apply if the Link Rate is 345kbps because of the 64 channels that are available, the unit must hop on exactly 50 - there is not option to either increase or decrease this amount.)

Values

4-16

16

Zone Restriction

Zone restriction dictates within which band (zone) of frequencies that a particular unit will operate.

Using zones simplifies network deployment by providing a convenient reference (e.g. Zone 1) within which a given network can operate, thereby minimizing the potential for internetwork interference. This is particularly useful when used in conjunction with Network Search Mode to facilitate minimal interference among adjacently deployed networks.

The tables on the following page illustrate the various zones and their associated frequency restrictions. Note that there is a difference between zone 'values' depending on the Wireless Link Rate selected. Currently Zone restriction is only supported on models with 345kpbs, and 1.2Mbps link rates available.

6.0 Configuration

Zone Restriction (continued)

Zone No.	Restrict From Start (MHz)	Restrict To End (MHz)	Restrict From Start (MHz)	Restrict to End (MHz)
1	923.200	927.600		
2	902.400	902.800	924.000	927.600
3	902.400	903.600	924.800	927.600
4	902.400	904.400	925.600	927.600
5	902.400	905.200	926.400	927.600
6	902.400	906.000	927.200	927.600
7	902.400	906.800		
8	912.800	917.200		

Table 6-1: Restricted Bands for UA1 at 345kbps Link Rate

Zone No.	Restrict From Start (MHz)	Restrict To End (MHz)	Restrict From Start (MHz)	Restrict to End (MHz)
1	909.750	926.250		
2	902.400	905.250	912.750	926.250
3	902.400	908.250	915.750	926.250
4	902.400	911.250	918.750	926.250
5	902.400	914.250	921.750	926.250
6	902.400	917.250	924.750	926.250
7	902.400	920.250		
8	906.750	923.250		

Table 6-2: Restricted Bands for UA1 at 1.1Mbps Link Rate

Values

None

Zone 1, 2, 3, 4, 5, 6, 7, and 8

6.0 Configuration

6.1.5.1 Radio Configuration > Sleep Mode Config (Remote)

Sleep modes are not supported on the IPn2420 models.

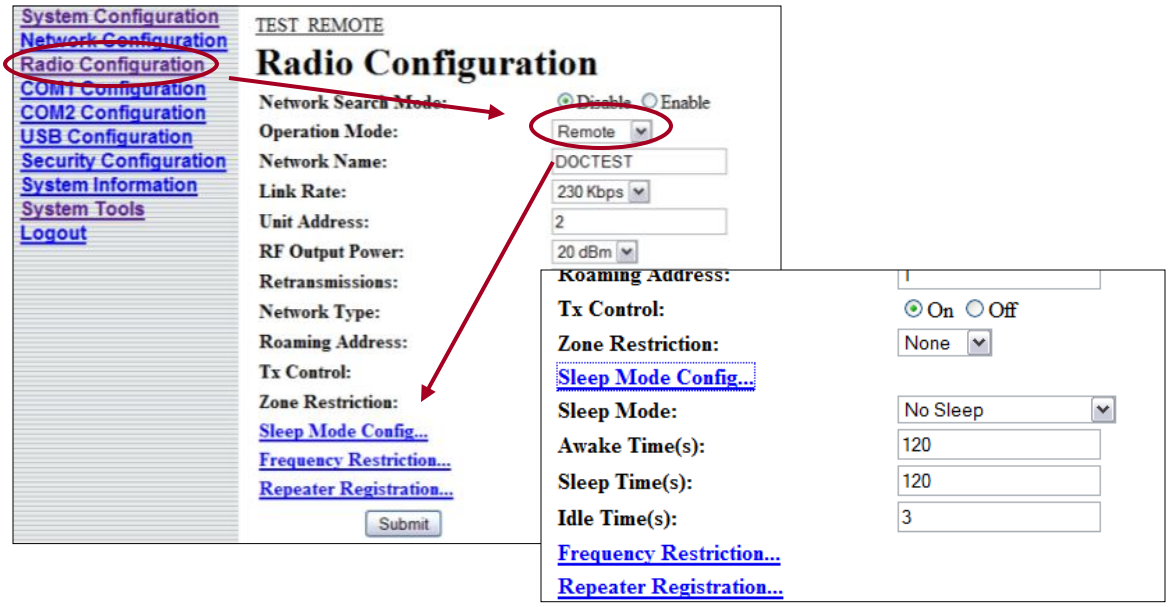


Image 6P: Sleep Mode - Remotes

When a unit is configured as a Remote, an additional option for ***Sleep Mode Config…*** will appear as shown above. (Not available on IPn2420 models).

Sleep Mode	Values
No Sleep: Sleep mode is disabled by default.	**No Sleep**
Auto Wakeup: Unit will wakeup from activity on serial port, Ethernet port or radio data, if the *Radio Awake Time* is a nonzero value. Power consumption is about 35-45 mA @ 12VDC.	Auto Wakeup
Serial Port Wakeup: Unit will wakeup from serial port or radio data if *Radio Awake Time* is nonzero value. Power consumption is about 15-25mA @ 12VDC.	Serial Port Wakeup
Ethernet Port Wakeup: Unit will wakeup from Ethernet port or radio data if *Radio Awake Time* is a nonzero value. Power consumption is about 30-40mA @ 12VDC.	Ethernet Port Wakeup
Power Shutdown: Timer control shutdown mode. Controlled by *Radio Awake Time* and *Radio Sleep Time* parameters. System will reboot when the radio wakes up. Power consumption is about 1mA @ 12 VDC.	Power Shutdown

6.0 Configuration

The Nano IP will enter sleep mode after 60 seconds when the system is rebooted.

Awake Time	
Defines how long the unit will keep awake. If set to 0, the radio will not wakeup until data is received from the serial or ethernet port.	**Values (seconds)** 0 - 65535

Sleep Time	
Defines how long the unit will sleep. If set to 0, the radio will not enter sleep mode.	**Values (seconds)** 0 - 65535

Idle Time	
System idle time before going into sleep mode cycle.	**Values (seconds)** 1 - 65535

6.0 Configuration

6.1.5.2 Radio Configuration > Frequency Restriction

Scrolling down the Radio Configuration menu reveals further configuration options: Frequency Restriction and Repeater Registration. Typically the former is not required; the latter only applies if there are 2 or more Repeaters in your network.

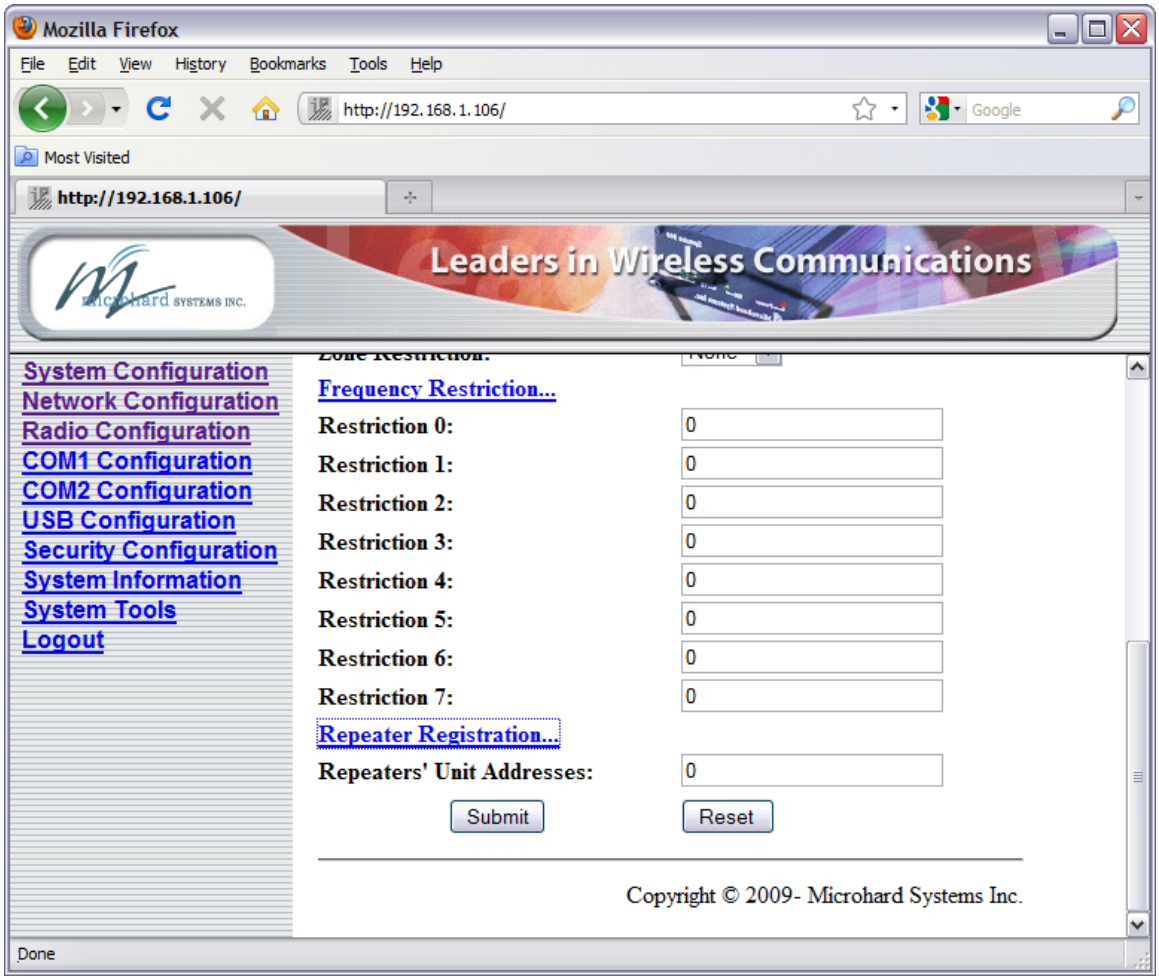


Image 6Q: Radio Configuration Menu (lower portion)

All modems in the network must have the same frequency restriction configured within them.

By default, the Nano IP will hop on frequencies across the entire 902-928MHz or 2.4000-2.4835 GHz ISM bands. For some applications or within certain operating environments it may be desired to prohibit the modem from operating on specific frequencies or range(s) of frequencies.

(See Section 6.1.10.4 for a description of the Radio Channel Noise Levels tool.)

The modem will not allow 'too many' frequencies to be restricted; it requires a certain amount of bandwidth within which to operate to comply with regulations.

6.0 Configuration

The input format is:

UA: channel number, or
UA: channel number-channel number z, or
UA: channel number,<no space>chnl number-chnl number

where UA is the Unit Address, and
channel number is the channel number (not frequency) of the channel to be restricted.

The input formats above describe single channel, range of channels, or a combination thereof. A number of input fields may be used, or a combination of restrictions input in one field.

The image below shows an example of configuring an Nano IP Series (with 345kbps as an available Link Rate) with a Link Rate of 345kbps to not operate on channels 1 through 10.

Use the Radio Channels Noise Level tool (see Section 6.1.10.4) to help identify the frequency/ range of possible interfering signals within the 900 MHz or 2.4GHz ISM bands, and then use the Frequency Restriction feature to configure the Nano IP to avoid them.

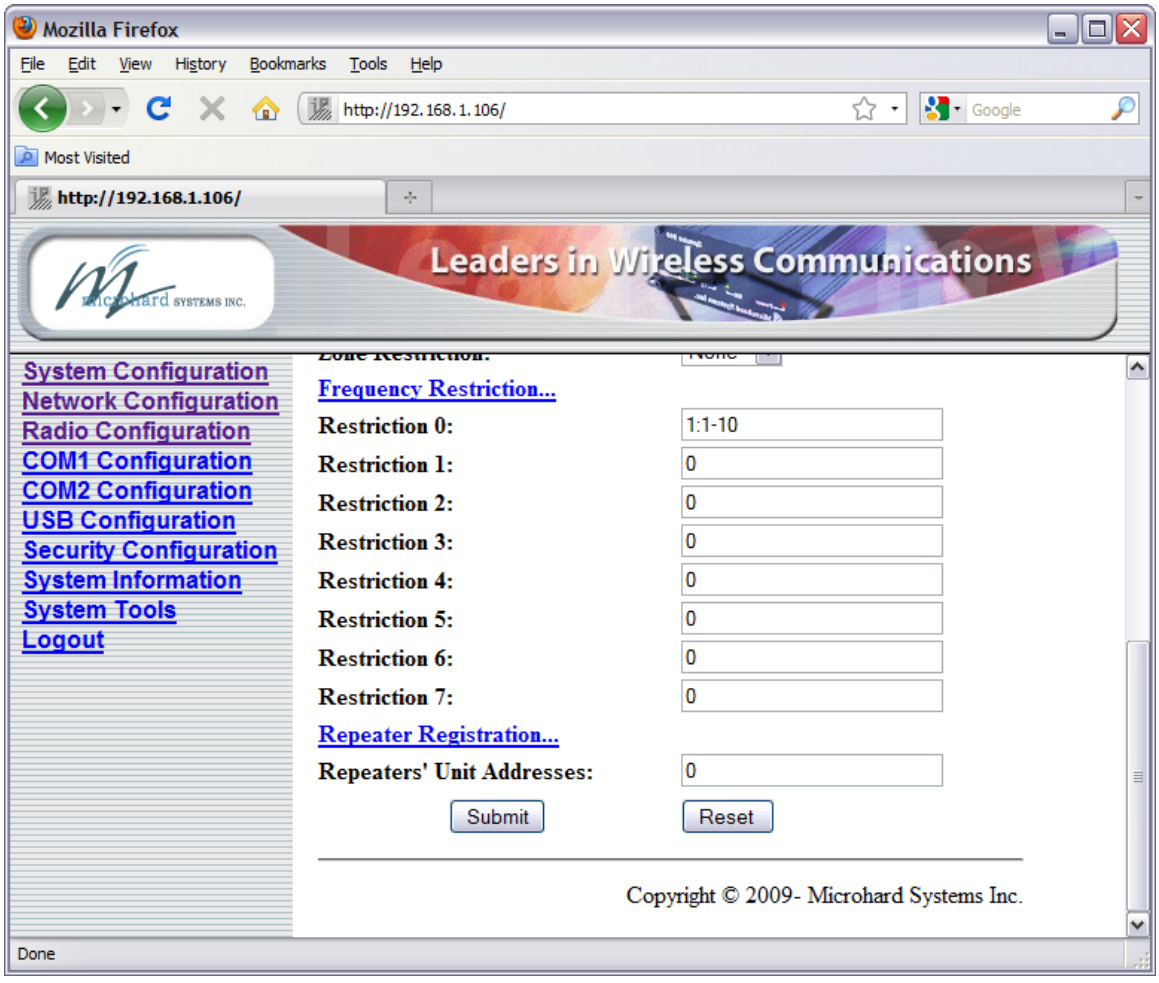


Image 6R: Frequency Restriction, 345kbps

6.0 Configuration

Frequency Restriction (continued)

Channel Numbers can be calculated based on the frequency and link rate (determines channel spacing).

For 900 MHz Models:

Channel 1 is at 902.4MHz. Therefore, to calculate the frequency of channel n:

Freq channel n = 902.4 + ((n-1) x CW) MHz.

Use the provided table below to calculate the channel number:

The listed channel number calculations are based on standard North America country codes. For non standard versions and alternate country codes contact Microhard Systems Inc for more information.

Link Rate	Start freq. (MHz)	Channel Space (MHz)	# of Channels
115kbps	902.400	.280	90
172kbps	902.400	.280	90
230kbps	902.400	.280	90
345kbps	902.400	.400	63
1.2 Mbps	903.750	1.500	15

Table 6-3: Channel Spacing 900MHz

Example:

The frequency of channel 78 of a unit using a link rate of 230kbps is:

Freq channel 78 = 902.4 + ((78-1) x 0.280)
= 902.4 + (77 x 0.280)
= 902.4 + 21.56
= 923.96 MHz

Use the Radio Channels Noise Level tool (see Section 6.1.10.4) to help identify the frequency/ range of possible interfering signals within the 900 MHz or 2.4GHz ISM bands, and then use the Frequency Restriction feature to configure the Nano IP to avoid them.

For 2.4 GHz Models:

Channel 1 is at 2401.6 MHz. Therefore, to calculate the frequency of channel n:

Freq channel n = 2401.6 + ((n-1) x CW) MHz.

Use the tables below to calculate the channel number:

Link Rate	Start freq. (MHz)	Channel Space (MHz)	# of Channels
115kbps	2401.600	.280	272
172kbps	2401.600	.280	272
230kbps	2401.600	.280	272
345kbps	2401.600	.400	191
1.2 Mbps	2401.600	1.500	50

Table 6-4: Channel Spacing 2.4GHz

Example:

The frequency of channel 172 of a unit using a link rate of 345kbps is:

Freq channel 172 = 2401.6 + ((172-1) x 0.400)
= 2401.6 + (171 x 0.400)
= 2401.6 + 68.4
= 2470.000 MHz

6.0 Configuration

Frequency Restriction (continued)

With the Nano IP Series having the option of, and configured for, a Link Rate of 1.2Mbps, the Frequency Restriction input format remains the same (as for 345kbps described previously), however, the Channel Number must be reduced by the number of channels restricted, i.e. If Channels 1-3 are restricted, the Channel Number is to be decreased from 16 to 13, as per the following example (image below):

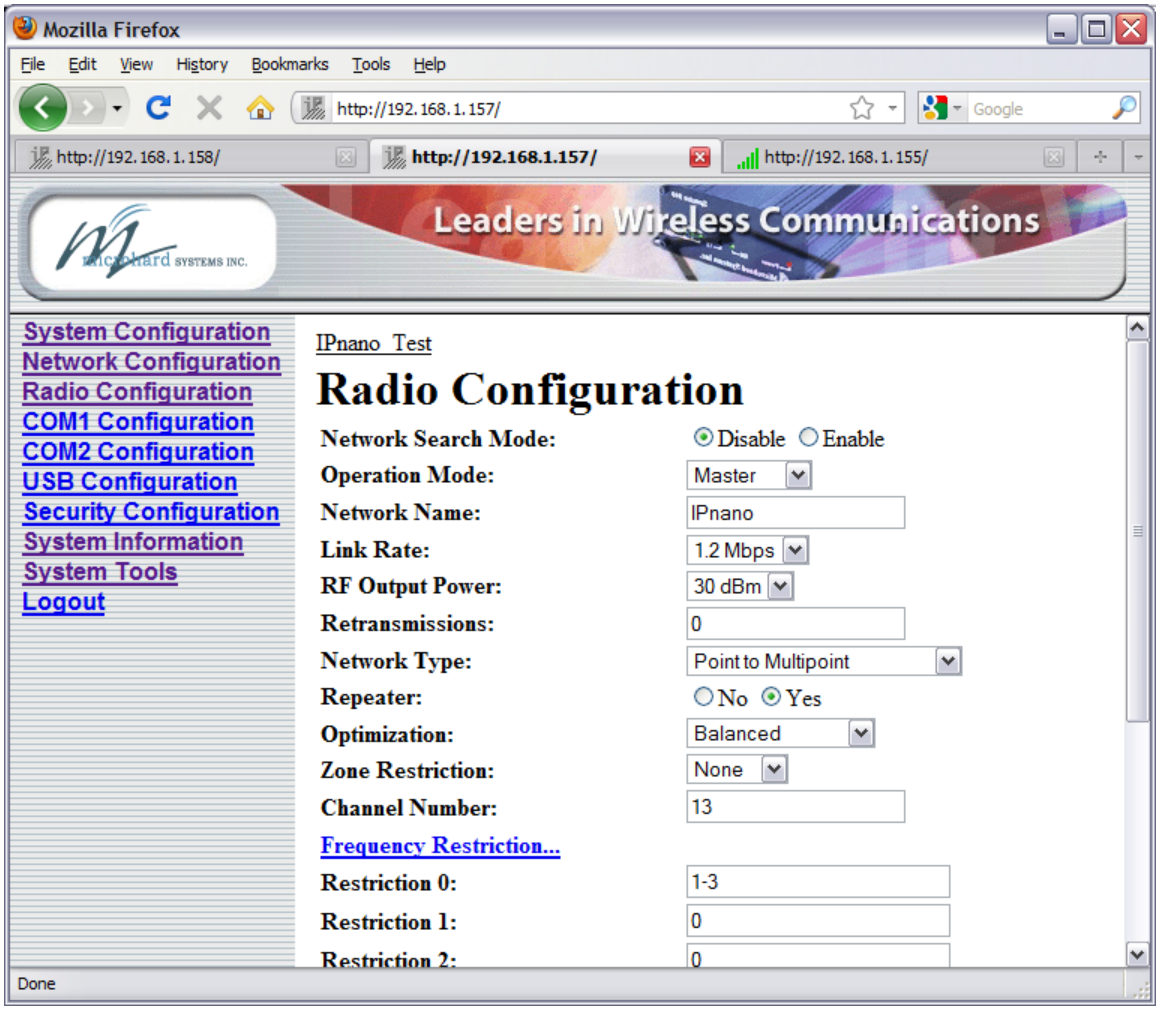


Image 6S: Frequency Restriction, 1.2Mbps

The Frequency Restriction 'value' must be input into EVERY MODEM in a network. Oftentimes the applicable Unit Address (as input in the format detailed previously) will be '1' - indicating that that the Master modem - to which other units synchronize - will not be transmitting on the specified channel(s). All units in the system will use this information - as input into each one of them - to generate the appropriate hopping pattern for the network.

6.0 Configuration

6.1.5.3 Radio Configuration > Repeater Registration

In order to ensure that generated hopping patterns are orthogonal to each other (thereby minimizing possible interference between network segments), if there is more than 1 Repeater in a network, ALL Repeaters must be registered in EVERY Nano IP Series.

The following image depicts an example:

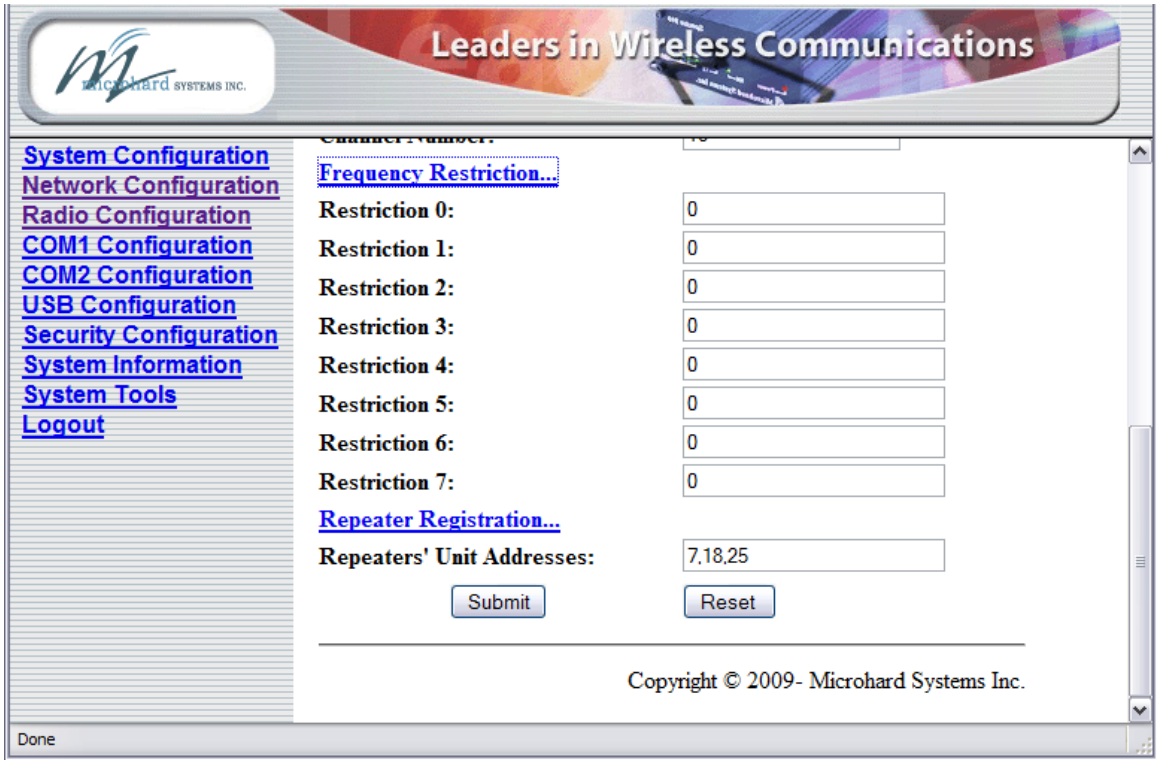


Image 6T: Repeater Registration

In the above example, there is a total of 3 Repeaters in the system, with Unit Addresses of 7, 18, and 25. Again, these Repeater UAs must be added into each/every Nano IP's Repeater Registration field.

Format:

x,y,z

where

x, y, and z are Repeater UAs,
noting that there is no SPACE after the commas.

6.0 Configuration

6.1.6 COM1 and COM2 Configuration

The menus 'COM1 Configuration' and 'COM2 Configuration' are used to configure the serial device server for the serial communications ports:

- COM1 (DATA), the rear DE9 connector on the Nano IP Series, and
- COM2 (DIAGNOSTIC), the front DE9 connector, respectively.

Serial device data may be brought into a LAN network through TCP, UDP, or multicast; it may also exit the Nano IP Series network on another Nano IP's serial port.

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

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

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

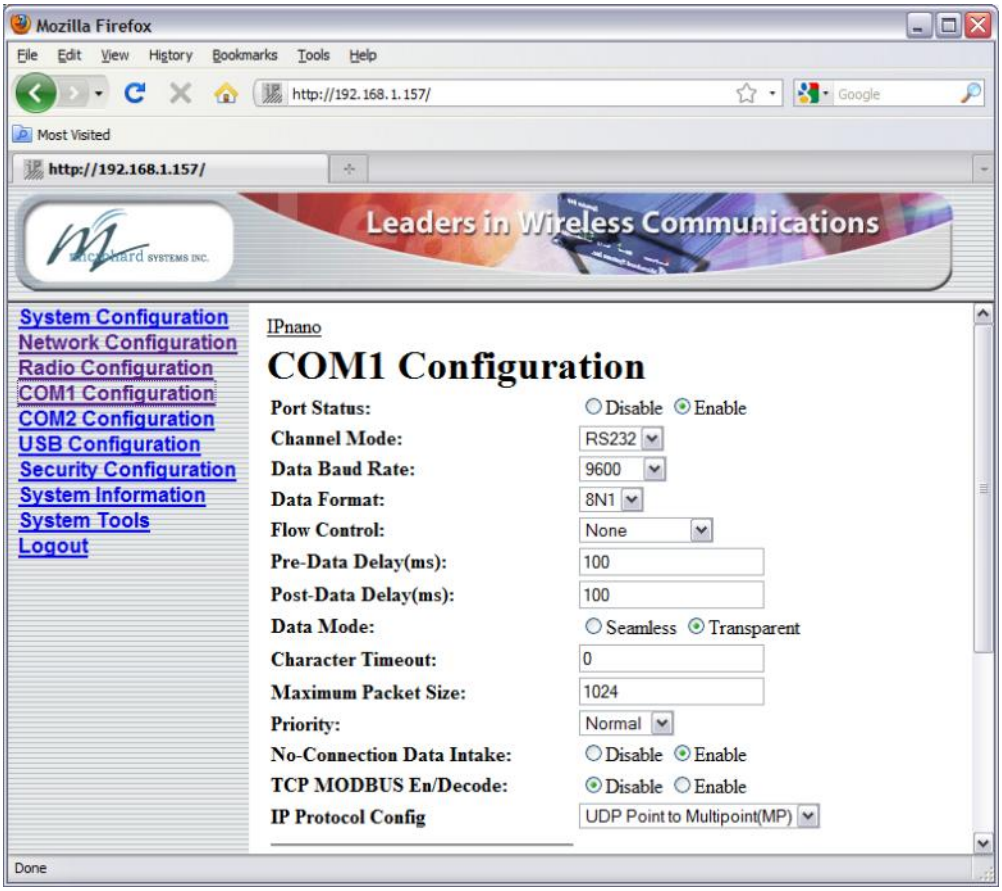


Image 6U: COM1 Configuration Menu (upper portion)

6.0 Configuration

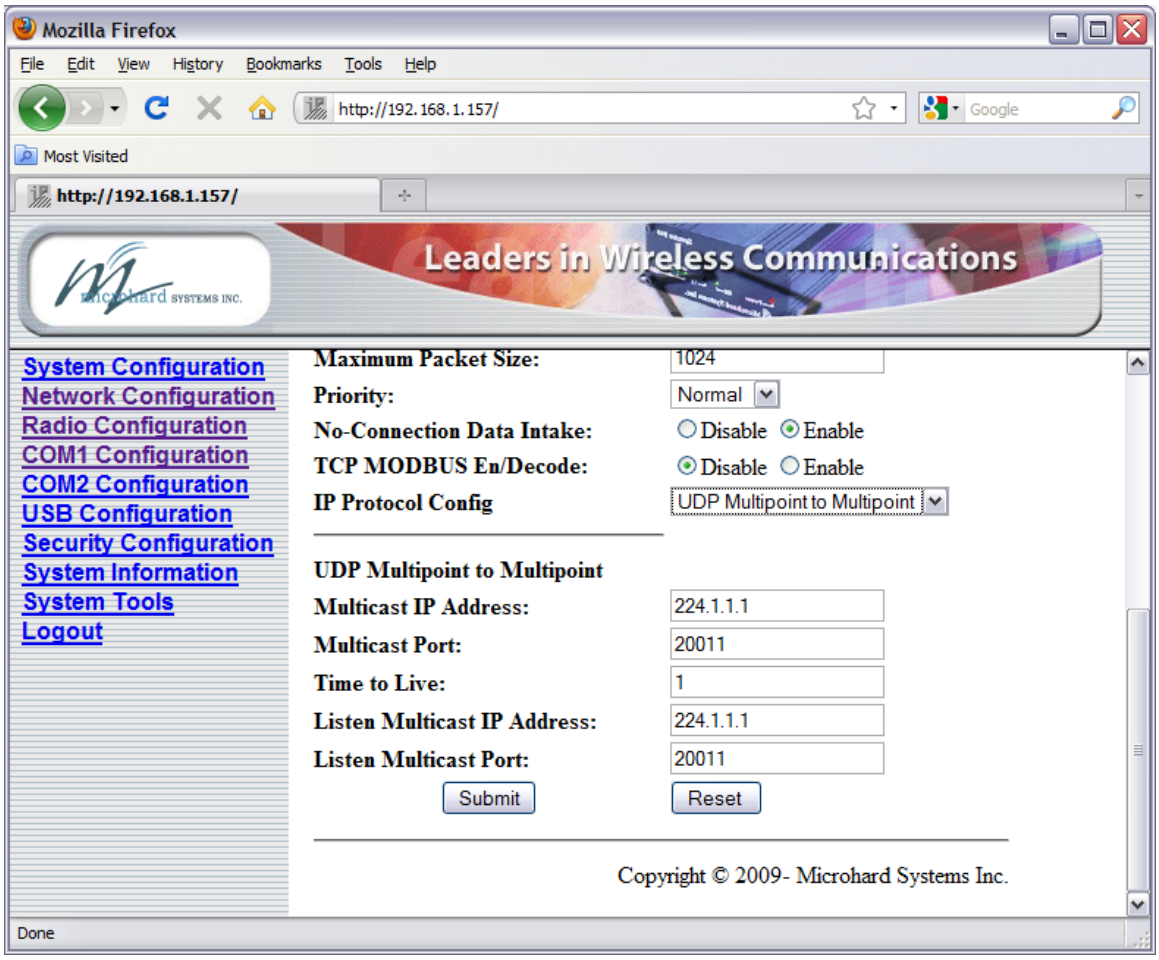


Image 6V: COM1 Configuration Menu (lower portion)

Port Status

Select operational status of port. Enabled by default.

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

Values

Enable
Disable

Channel Mode

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

*COM2 / DIAGNOSTIC is RS232 only, 3-wire (TxD, RxD, and SG).

Values

RS232
RS485 (Half Duplex)
RS422 (Full Duplex)

6.0 Configuration

Data Baud Rate

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

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

Values

bits per second (bps)

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

Data Format

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

Values

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

Flow Control

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

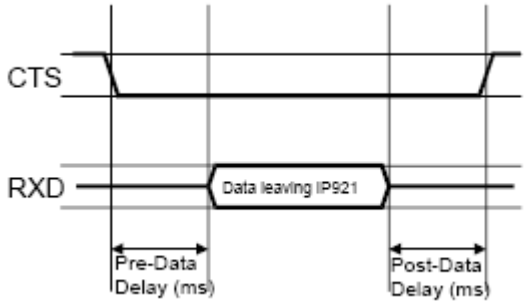
When CTS Framing is selected, the Nano IP Series uses the CTS signal to gate the output data on the serial port. Figure 6A below illustrates the timing of framed output data.

*COM2 does not support Flow Control.

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

Values

None
Hardware
CTS Framing



Drawing 6A: CTS Output Data Framing

6.0 Configuration

Pre-Data Delay (ms)

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

*COM2 does not support this function.

Values

ms
100

Post-Data Delay (ms)

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

*COM2 does not support this function.

Values

ms
100

Data Mode

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

Values

Seamless
Transparent

Character Timeout

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

Values

characters
4

The serial server also uses this parameter to determine the time gap inserted between frames. It is measured in 'characters' and related to baud rate.

Example: If the baud rate is 9600bps, it takes approximately 1ms to move one character. With the Character Timeout set to 4, the timeout period is 4ms. When the calculated time is less than 3.5ms, the serial server will set the character timeout to a minimum value of 3.5ms. If the baud rate is greater than 19200bps, the minimum character timeout is internally set to 750us (microseconds).

Maximum Packet Size

Defines the buffer size that the serial server will use to receive data from the serial port. When the server detects that the Character Timeout criteria has been met, or the buffer is full, it packetizes the received frame and transmits it.

Values

Bytes
1024

Priority

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

Values

Normal
Medium
High

6.0 Configuration

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

IP Protocol Config

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

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

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

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

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

- Outgoing Connection Timeout
  This parameter determines when the Nano IP Series will terminate the TCP connection if the connection is in an idle state (i.e. no data traffic on the serial port).
  Default: **60** (seconds)

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

Requires more bandwidth than UDP.

TCP Server: In this mode, the Nano IP 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)
- Monitor / Multi-Polling
  Monitor mode, the TCP Server sends data collected from serial port(COM1) to all the connected TCP Clients. Multi-polling Mode, the TCP Server sends data collected from serial port(COM1) to the connected TCP client which is the last one that sent the data(request) to the TCP Server.

TCP Client/Server: In this mode, the Nano IP 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.

6.0 Configuration

A UDP or TCP port is an application end-point. The IP address identifies the device and, as an extension of the IP address, the port essentially 'fine tunes' where the data is to go 'within the device'.

Be careful to select a port number that is not predetermined to be associated with another application type, e.g. HTTP uses port 80.

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

- Remote IP Address
  IP address of distant device to which UDP packets are sent when data received at serial port.
  Default: **0.0.0.0**
- Remote Port
  UDP port of distant device mentioned above.
  Default: **20001**
- Listening Port
  UDP port which the IP Series listens to (monitors). UDP packets received on this port are forwarded to the unit's serial port.
  Default: **20001**

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

Multicast is a one-to-many transmission of data over an IP network. It is an efficient method of transmitting the same data to many recipients. The recipients must me members of the specific multicast group.

- Multicast IP Address
  A valid multicast address this unit uses to send multicast UDP packets upon receiving data from the serial port. The default value is a good example of a valid multicast address.
  Default: **224.1.1.1**
- Multicast Port
  A UDP port that this Nano IP will send UDP packets to. The Multipoint (MP - see the UDP Point-to-Multipoint (MP) description) stations should be configured to listen to this point in order to receive multicast packets from this Nano IP Series.
  Default: **20001**
- Listening Port
  The UDP port that this unit receives incoming data on from multiple remote units.
  Default: **20011**
- Time to Live
  Time to live for the multicast packets.
  Default: **1** (hop)

TTL: Time to Live is the number of hops a packet can travel before being discarded.

In the context of multicast, a TTL value of 1 restricts the range of the packet to the same subnet.

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

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

6.0 Configuration

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

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

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

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

UDP Multipoint-to-Multipoint

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

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

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

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

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

6.0 Configuration

IP Protocol Config (continued)

SMTP Client: If the Nano IP Series network has Internet access, this protocol may be used to send the data received on the serial port (COM1), in a selectable format (see Transfer Mode (below)), to an e-mail addressee. Both the SMTP Server and the e-mail addressee must be 'reachable' for his feature to function.

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

- Mail Subject
  Enter a suitable 'e-mail subject' (e-mail heading).
  Default: **COM1 Message**
- Mail Server (IP/Name)
  IP address or 'Name' of SMTP (Mail) Server.
  Default: **0.0.0.0**
- Mail Recipient
  A valid e-mail address for the intended addressee, entered in the proper format.
  Default: **host@**
- Message Max Size
  Maximum size for the e-mail message.
  Default: **1024**
- Timeout (s)
  How long the unit will wait to gather data from the serial port before sending an e-mail message; data will be sent immediately upon reaching Message Max Size.
  Default: **10**
- Transfer Mode
  Select how the data received on COM1 is to be sent to the email addressee. Options are: Text, Attached File, Hex Code.
  Default: **Text**

Note: COM2 does not support this mode.

Values

TCP Client
TCP Server
TCP Client/Server
UDP Point-to-Point
UDP Point-to-Multipoint (P)
UDP Point-to-Multipoint(MP)
UDP Multipoint-to-Multipoint
SMTP Client

6.0 Configuration

6.1.7 USB Configuration

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

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

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

Storage Mode When configured in Storage Mode the Nano IP appears as a USB Mass Storage device to a host system and emulates a USB memory stick. It has been formatted as MSDOS (for Windows) file system.

NDIS Mode Provides support for sending and receiving Ethernet frames. Mini USB port can be used as a network interface card.

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

Please register and login into:

http://www.microhardcorp.com/support, then locate the drivers in the following location:

Support Center » Downloads » Spread Spectrum » Nano IP Series » Utilities

Image 6W: USB Configuration Menu

6.0 Configuration

USB Device Port Mode

Console Mode:
Console Mode is enable by default. Mini USB port acts as a console port.

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

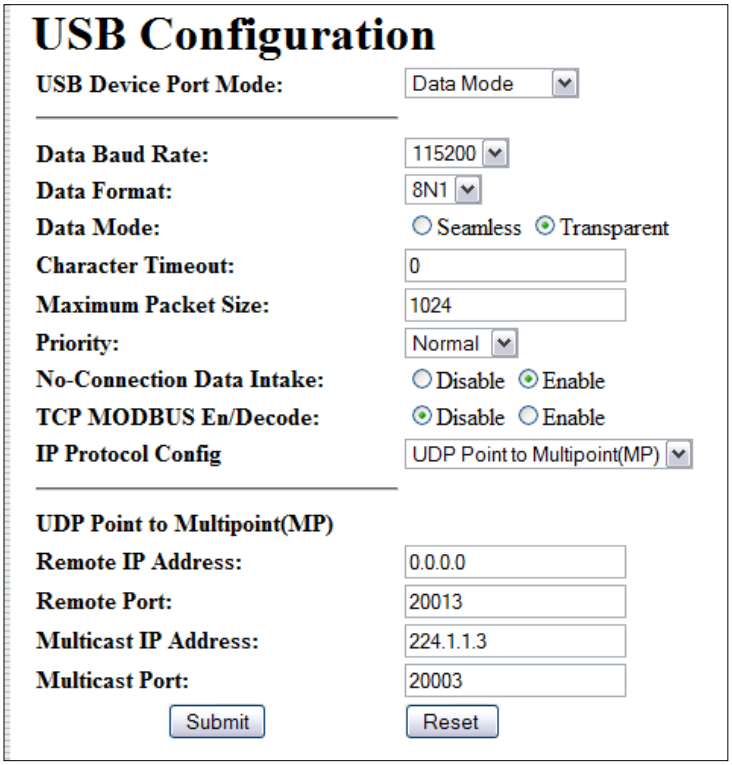


Image 6X: USB Configuration Data Port

For more information about any of the Data Port field parameters refer to ***Section 6.1.6:*** COM1 and COM2 Configuration.

Storage Mode:
Storage Mode is disable by default. This setting determines device will acts as a USB Mass Storage disk drive with capacity of 2MB.

Values

Console Mode
Data Mode
Storage Mode
NDIS Mode

6.0 Configuration

USB Device Port Mode (Continued)

NDIS Mode:
NDIS Mode is disabled by default. This setting will create a interface on a host system named usb0 and the device will act as a network interface card.

Bridge
If the unit has been configured as a Bridge (under the System Configuration menu), the USB NDIS interface will add itself in bridge automatically.

Router
If the unit has been configured as a Router (under the System Configuration menu), the Network Configuration will present a additional options for USB NDIS.

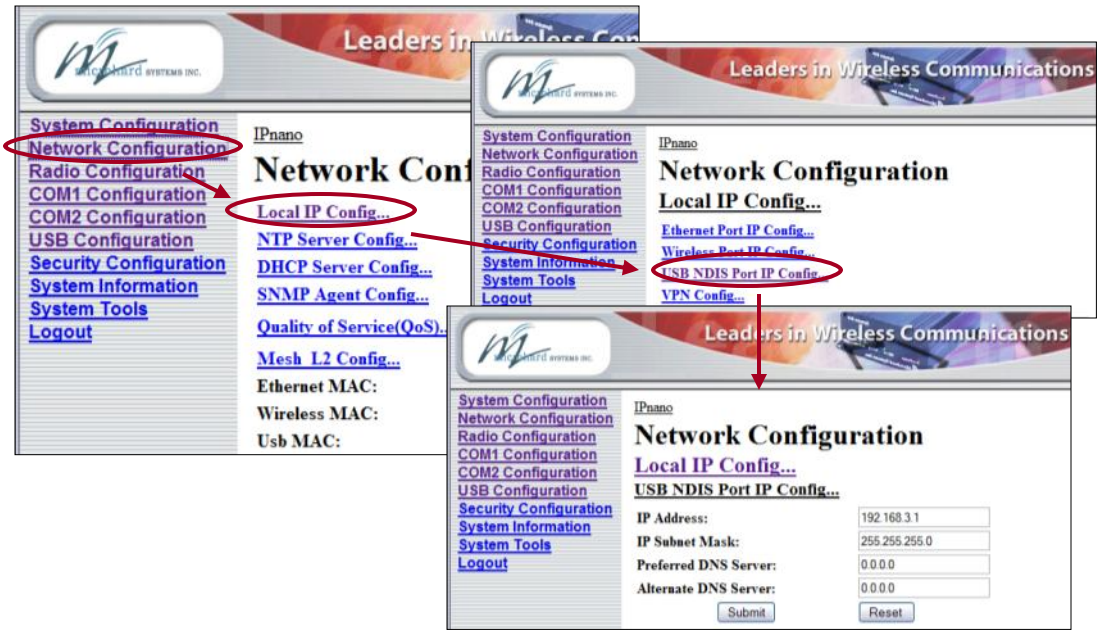


Image 6Y: USB Network Configuration (Router)

USB NDIS Port IP Configuration submenu
IP Address
This address MUST be STATIC (i.e. DHCP is not applicable).

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

Preferred DNS Server
If applicable, enter the IP address of Preferred DNS Server which exists within the LAN.

Alternate DNS Server
If applicable, enter the IP address of Alternate DNS Server which exists within the LAN.

6.0 Configuration

USB Mode System Information

Various information is available in the System Information menu that applies to the USB functions of the Nano IP Series.

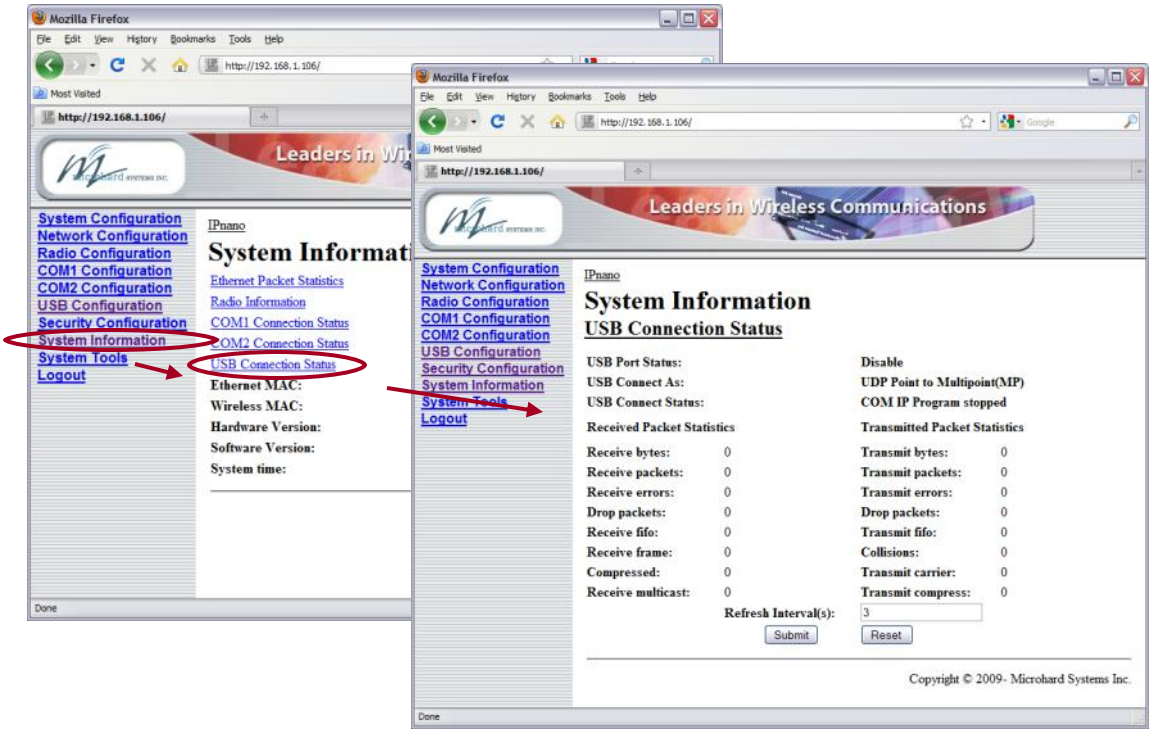


Image 6Y: USB Connection Status

USB Port Status
Display the Status of USB Port. Configure via USB Configuration menu.

USB Connect As
Display of chosen protocol with respect to serial gateway function. Configure via USB Configuration menu.

USB Connect Status
If port is enabled and there is data traffic, this will display 'Active'.

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

6.0 Configuration

6.1.8 Security Configuration

There is significant security inherent in the Nano IP's proprietary design and technology implementation. There are additional security features available, both as standard and optional items.

Image 6W: Security Configuration Menu

6.0 Configuration

6.1.8.1 Admin Password Configuration

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

Image 6X: Security Config., Admin Password Config. Submenu

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

6.0 Configuration

6.1.8.2 Upgrade Password Configuration

The Upgrade Password protects the Nano IP from having a package upgrade performed by an unauthorized person. It is recommended that the default password be changed when the system is deployed.

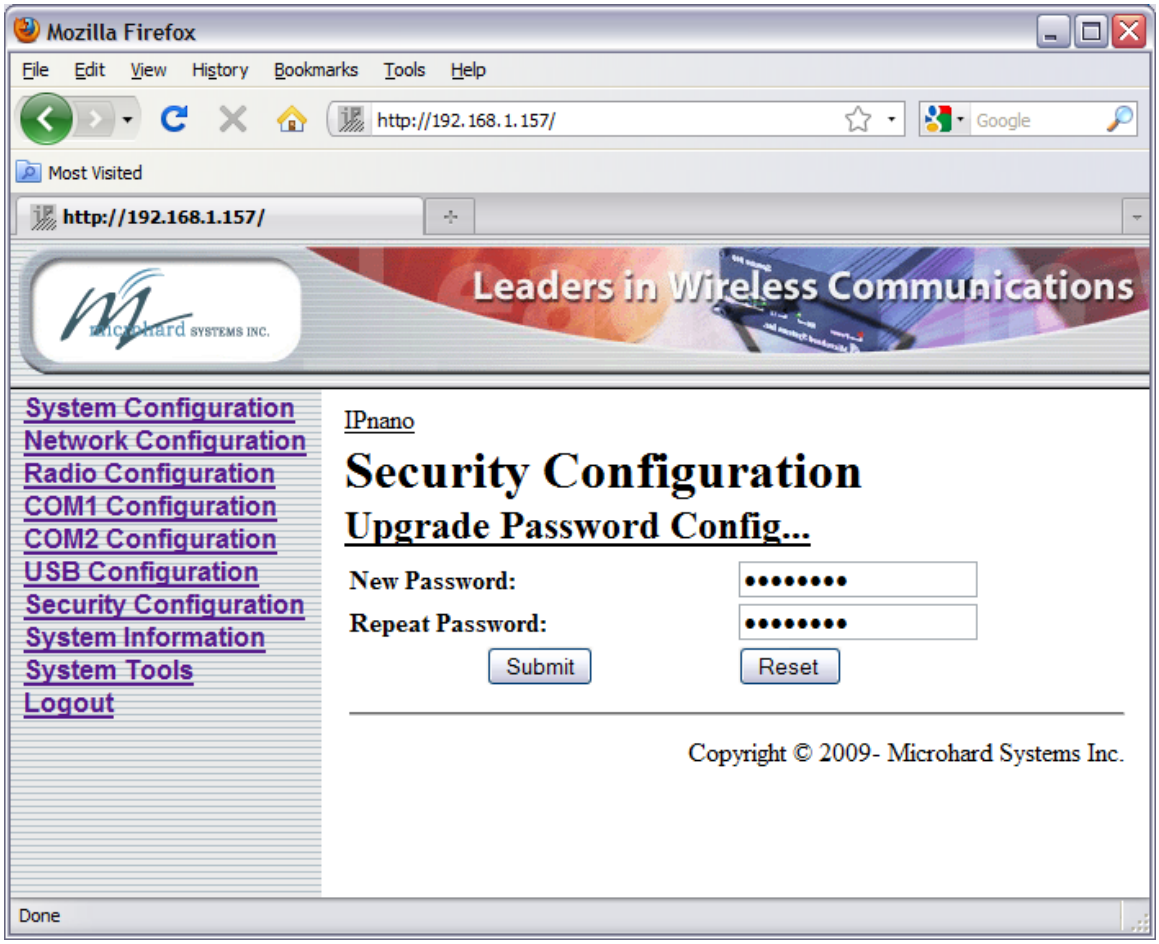


Image 6Y: Security Config., Upgrade Password Config. Submenu

New Password/Repeat Password

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

Values

character string

admin

6.0 Configuration

6.1.8.3 Wireless Encryption Configuration

There are 2 encryption levels for the Nano IP Series:

- Medium
- High

Medium and High levels are NOT AVAILABLE FOR EXPORT. High level is optional within North America: Contact Microhard Systems Inc. for more information.

Encryption not available for EXPORT VERSIONS.

Medium and High levels are discussed further in this section.

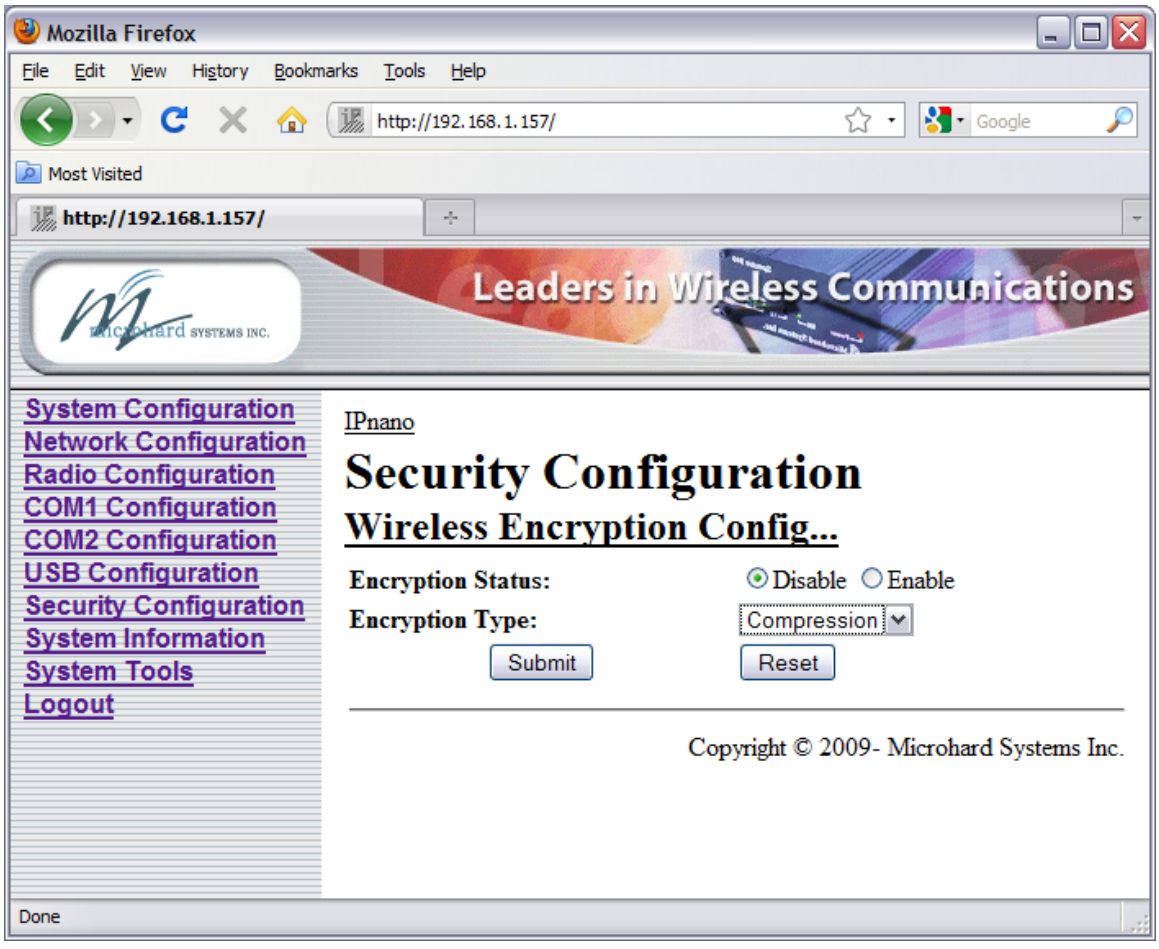


Image 6Z: Security Config., Wireless Encryption Config. Submenu

Encryption Status	
By default, the Encryption Status is Disabled. If Enabled, a number of Encryption Types are available, requiring varying amounts of configuration.	**Values** **Disable** Enable

6.0 Configuration

Encryption Type

Compression: Although not encryption per se, applying a compression algorithm to the input data within the transmitting Nano IP Series does require that the corresponding decryption algorithm be applied to the output data of the receiving unit to make it meaningful.

Compression requires processing time. Depending on the nature of the data, throughput may be either enhanced or not effected by the compression process.

WEP 64-bit: Wired Equivalency Protocol (WEP) encryption adds some overhead to the data, thereby negatively effecting throughput to some degree.

The image below shows the associated configuration options:

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

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

Image 6AA: Wireless Encryption Config., WEP 64-bit Submenu

continued...

6.0 Configuration

Encryption Type (continued)

- ***Key Generation***
  4 complex WEP keys may be generated by using 4 different simple key phrases in this field.
  Procedure: Input a Key Phrase, select the Key (via radio button beside Key number), then click the Generate Key soft button. Do the same for the remaining keys, using a different key phrase each time.
  Using the same Key Phrase(s) on all Nano IP's in the network will generate the same Keys on all units. All units must operate with the same Key selected.
  Alternately, 10-character key phrases may be entered manually into each Key field.
  Default: **0000**

- Key Phrase
  These Keys are used to encrypt and decrypt the data.
  Leave selected (via radio button) the Key number that the network is to use.
  Default: **0000000000**

WPA: Wi-Fi Protected Access provides stronger encryption than WEP. It uses the Temporal Key Integrity Protocol (TKIP) (and the same RC4 algorithm as WEP does) for encryption; its strength lies in it uses of sophisticated key management.

WPA is based on a subset of the 802.11i protocol.

WEP 128-bit: 128-bit encryption offers stronger encryption that 64-bit, but adds more overhead on the data. The configuration for WEP 128-bit is the same as for 64-bit; see the preceding text.

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

AES: Advanced Encryption Standard is a very robust symmetric encryption algorithm.

AES 128-bit (optional for North America): Very strong encryption. Basically the same configuration as for WEP applies. Input up to 4 unique Keys of 16 characters each.

AES 256-bit (optional for North America): Extremely strong encryption with a Key length double that of 128-bit AES. Basically the same configuration as for WEP applies. Input up to 4 unique Keys of 32 characters each.

Values

Compression
WEP 64-bit
WEP 128-bit
WPA
AES 128-bit*
AES 256-bit*

*optional for North America

6.0 Configuration

6.1.8.4 Discovery Service Configuration

This configuration relates to the Microhard Systems Inc. DiscoverIP utility.

The configuration selection will determine whether or not this modem may be discovered using the utility, and whether or not changes may be made to the Nano IP Series via the utility. The choice is typically based-upon network security considerations.

See Appendix A for a complete description of the DiscoverIP utility.

Image 6AB: Security Config. Menu, Discovery Service Submenu

Discovery Service

Disable: This unit will not appear to exist when the DiscoverIP utility is used to search for Nano IP / IP Series on the network.

Discoverable: This unit will appear as existing on an Nano IP Series network when the DiscoverIP utility is used to search for units.

Changeable: The unit will be discoverable, and certain specific configuration commands may be sent to it.

Values

Disable
Discoverable
Changeable

6.0 Configuration

6.1.8.5 UI (User Interface) Access Configuration

User Interface (UI) Access Configuration. By default, all UI access options are available, and include:

- Telnet
- HTTP
- SSH (if optioned)
- HTTPS (if optioned)

For security reasons, any or all may be disabled.

Image 6AC: Security Config. Menu, UI Access Config. Submenu

UI Access Configuration
Values
Disable Enable

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

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

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

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

SSH: Secure Shell. A protocol used to create a secure connection between two devices. It provides authentication and encryption.
Designed as a replacement for Telnet, which is not secure.

HTTPS: HyperText Transfer Protocol Secure. HTTP over SSL. A protocol used for the secure (using encryption and decryption) transfer of Web pages.

SSL: Secure Sockets Layer. An application layer protocol for managing the security of data transmissions in a network. Uses encryption, decryption, and public-and-private keys.

6.0 Configuration

6.1.8.6 Authentication Configuration

There are two methods whereby a user may be authenticated for access to the Nano IP Series:

- Local

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

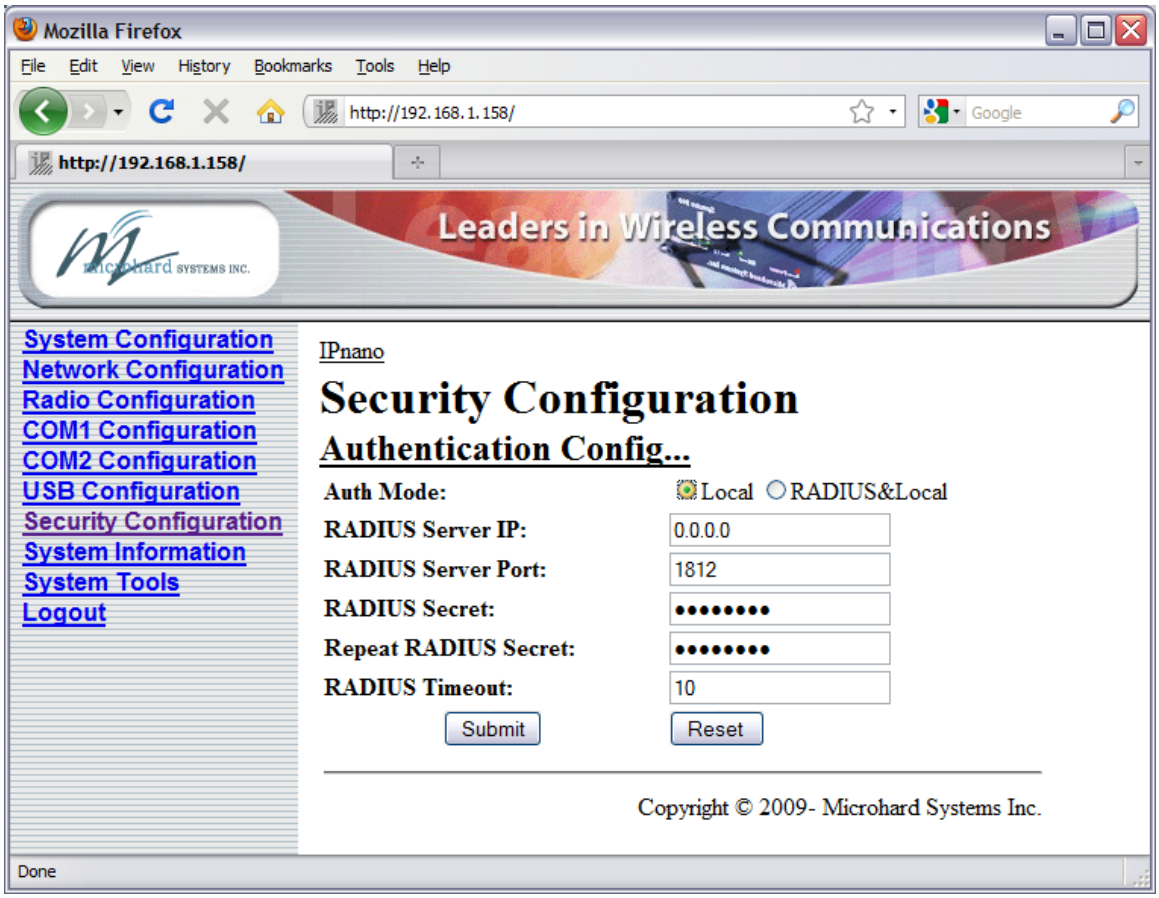


Image 6AD: Security Config. Menu, Authentication Config. Submenu

6.0 Configuration

Auth Mode

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

Values

Local
RADIUS&Local

RADIUS Server IP

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

Values

Valid RADIUS server IP address

0.0.0.0

RADIUS Server Port

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

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

Values

Applicable RADIUS Server Port number

1812

RADIUS Secret

If the IP Series' Authorization Mode has been set to RADIUS&Local, obtain the RADIUS Secret for his particular client from your RADIUS Server Administrator and enter it into this field, and the following field. (You will also want to obtain the applicable RADIUS User Name from your RADIUS Server Administrator.)

Values

Specific RADIUS Server secret

nosecret

Repeat RADIUS Secret

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

Values

Specific RADIUS Server secret

nosecret

RADIUS Timeout

Amount of time to wait for RADIUS authentication.

Values

10
1-65535
seconds

6.0 Configuration

6.1.8.7 Firewall Configuration

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

This security feature differs from those discussed in the 'UI Configuration' section; the UI Configuration is specifically for configuring the Nano IP's User Interface and related protocols.

Image 6AE: Security Config. Menu, Firewall Configuration Submenu

	Firewall Status
Disabled by default. When enabled, the firewall settings are in effect.	**Values** **Disable** Enable

6.0 Configuration

6.1.8.7.1 Policies Configuration

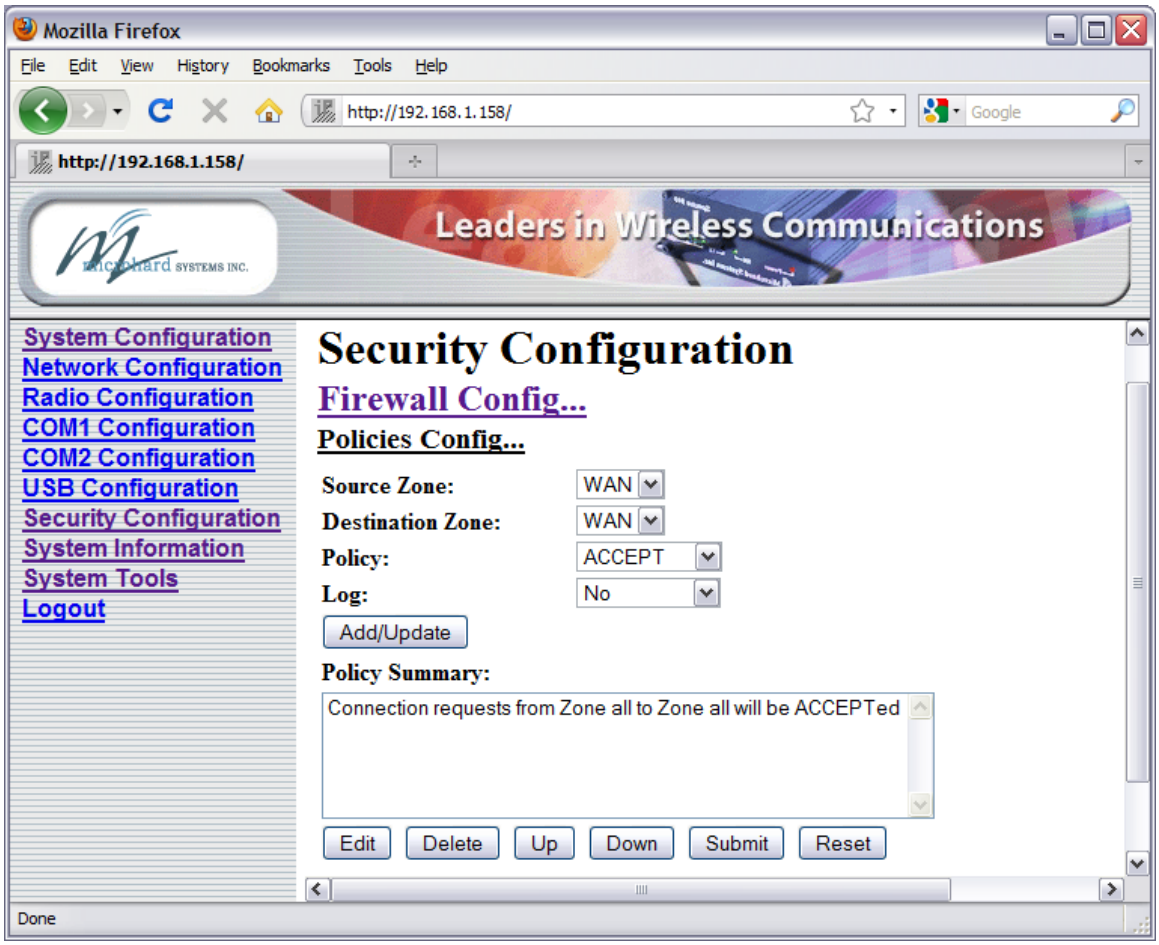


Image 6AF: Firewall Configuration, Policies Config. Submenu

Source Zone	
Select the zone which is to be the source of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all Nano IP Series units, whether a Master, Repeater, or Remote.	**Values** **WAN** LAN FW VPN all

Destination Zone	
Select the zone which is the intended destination of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all Nano IP Series units, whether a Master, Repeater, or Remote.	**Values** **WAN** LAN FW VPN all

6.0 Configuration

Policy	
Select the policy (action) which is to apply. ACCEPT (traffic) is the default. DROP results in a 'silent' drop of the traffic whereas REJECT will result in a message (e.g. 'destination unreachable) being sent from the intended destination back to the source.	**Values** **ACCEPT** DROP REJECT QUEUE>future use CONTINUE>future use NONE>future use

Log	
If, in the Policy configuration, DROP or REJECT has been selected, this field may be defined as to how to tag associated messages.	**Values** No Emergency Alert Critical Error Warning Notice Information Debug

Policy Summary

List of current policies. Use the Edit, Delete, Up, Down to modify the polices.

Use Submit to write policies to Nano IP and make active, use the Reset button to revert back to the policies currently stored in the Nano IP.

6.0 Configuration

6.1.8.7.2 Rules Configuration

Rules take precedence over Policies. They are configured to 'fine tune' firewall settings.

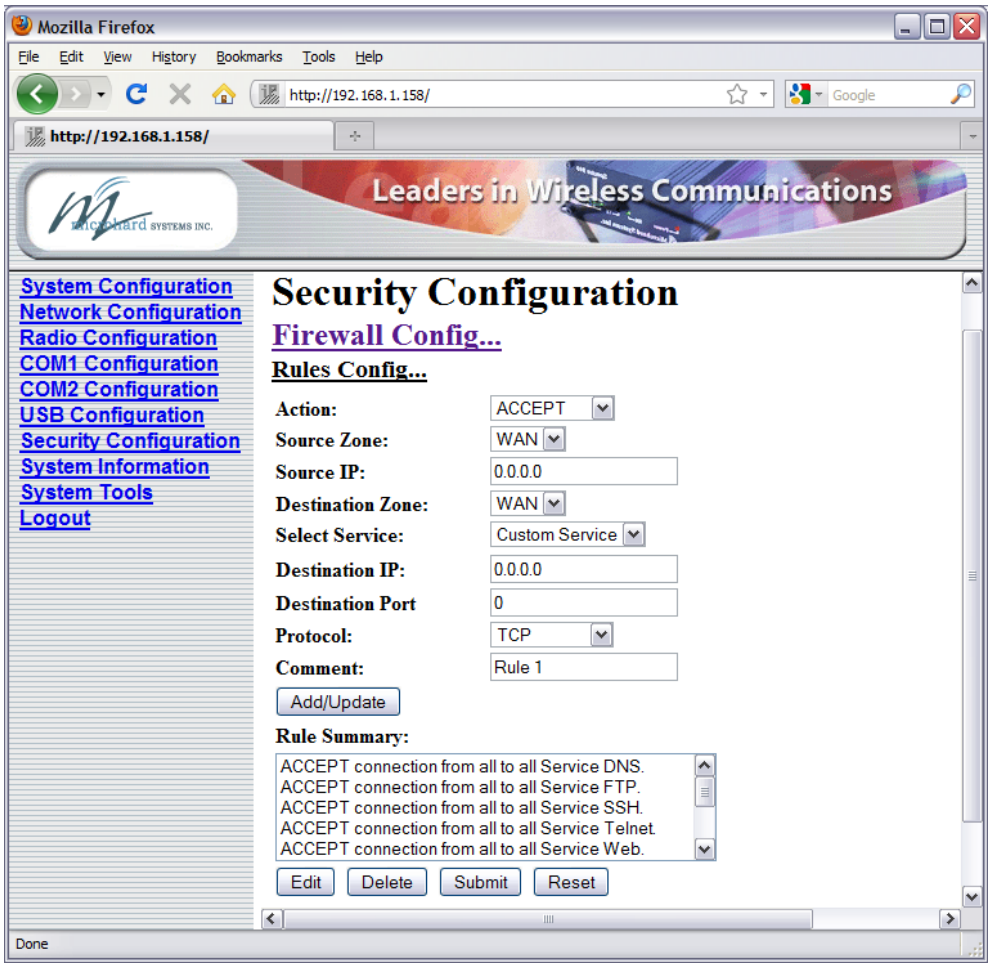


Image 6AG: Firewall Configuration, Rules Config. Submenu

Action

Define the action which is to be taken by the defined rule.

Values

ACCEPT
ACCEPT+>future
NONAT>future
DROP
REJECT
DNAT
SAME>future
REDIRECT>future
CONTINUE>future
LOG
QUEUE>future

6.0 Configuration

Source Zone	
Select the zone which is to be the source of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all units, whether a Master, Repeater, or Remote.	**Values** **WAN** LAN FW VPN all

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

Destination Zone	
Select the zone which is the intended destination of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all units, whether a Master, Repeater, or Remote.	**Values** **WAN** LAN FW VPN all

Select Service	
This field allows for the rule to be applied to either a Custom Service (defined further down the menu) or for one of many predefined services available via a pull down menu.	**Values** **Custom Service** or select from a long listing of predefined services

Destination IP	
If a valid IP address is specified, the action will apply against that address; otherwise, leaving the default value of 0.0.0.0 in this field results in the action applying to all destination IP addresses.	**Values** **0.0.0.0** valid IP address

6.0 Configuration

	Destination Port
This field is configured if defining a Custom Service (ref. Select Service field).	**Values** **0** valid port number
	Protocol
This field is configured if defining a Custom Service (ref. Select Service field).	**Values** **TCP** TCP:SYN UDP ICMP IPP2P IPP2P:UDP IPP2P:all All
	Comment
This is simply a field where a convenient reference or description may be added to the rule.	**Values** **Rule 1** descriptive comment

6.0 Configuration

6.1.8.7.3 Port Forwarding Configuration

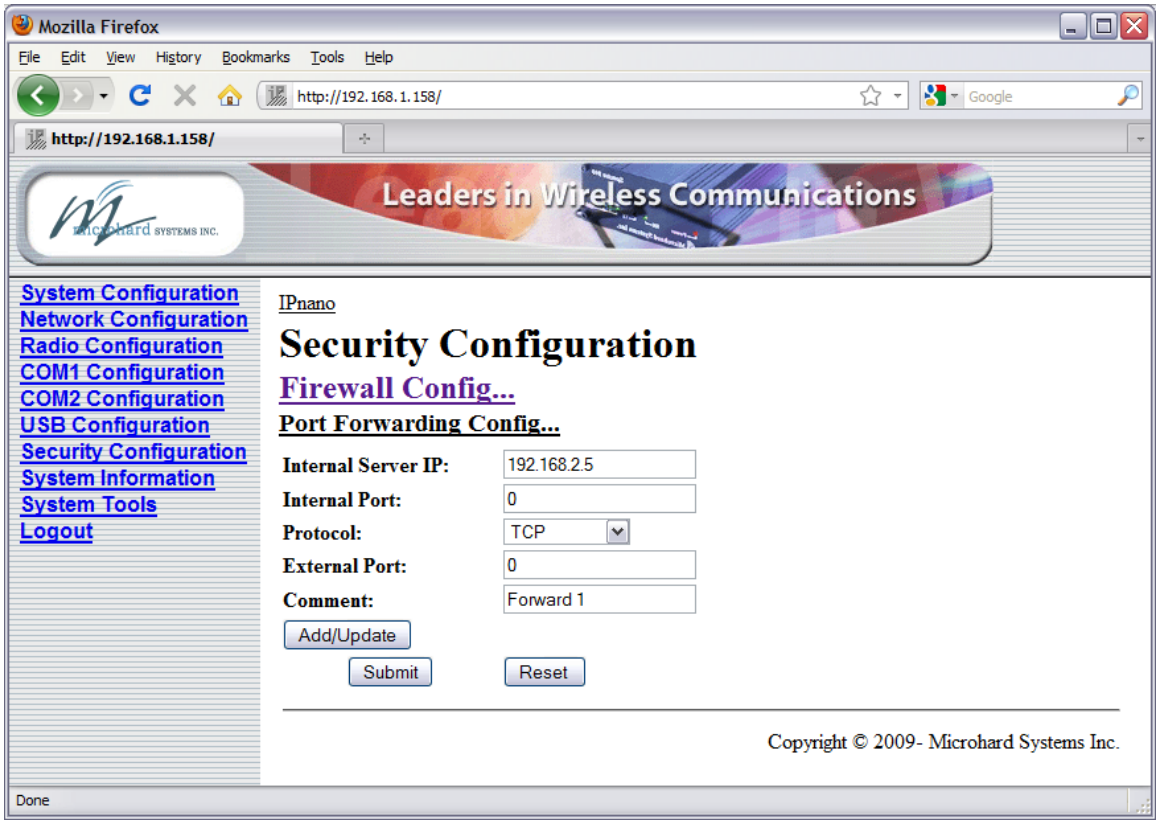


Image 6AH: Firewall Configuration, Port Forwarding Config. Submenu

	Internal Server IP
Enter the IP address of the intended internal (i.e. on LAN side of IP Series unit configured as a Router) server.	**Values** **192.168.2.5** valid IP address
	Internal Port
Target port number of internal server.	**Values** **0** valid port number

6.0 Configuration

	Protocol
Enter the IP address of the intended internal (i.e. on LAN side of IP Series unit configured as a Router) server.	**Values** **TCP** TCP:SYN UDP ICMP IPP2P IPP2P:UDP IPP2P:all All
	External Port
Port number of incoming request (from WAN-side device).	**Values** **0** valid port number
	Comment
This is simply a field where a convenient reference or description may be added to the rule.	**Values** **Forward 1** descriptive comment

6.0 Configuration

6.1.8.7.4 MAC List Configuration

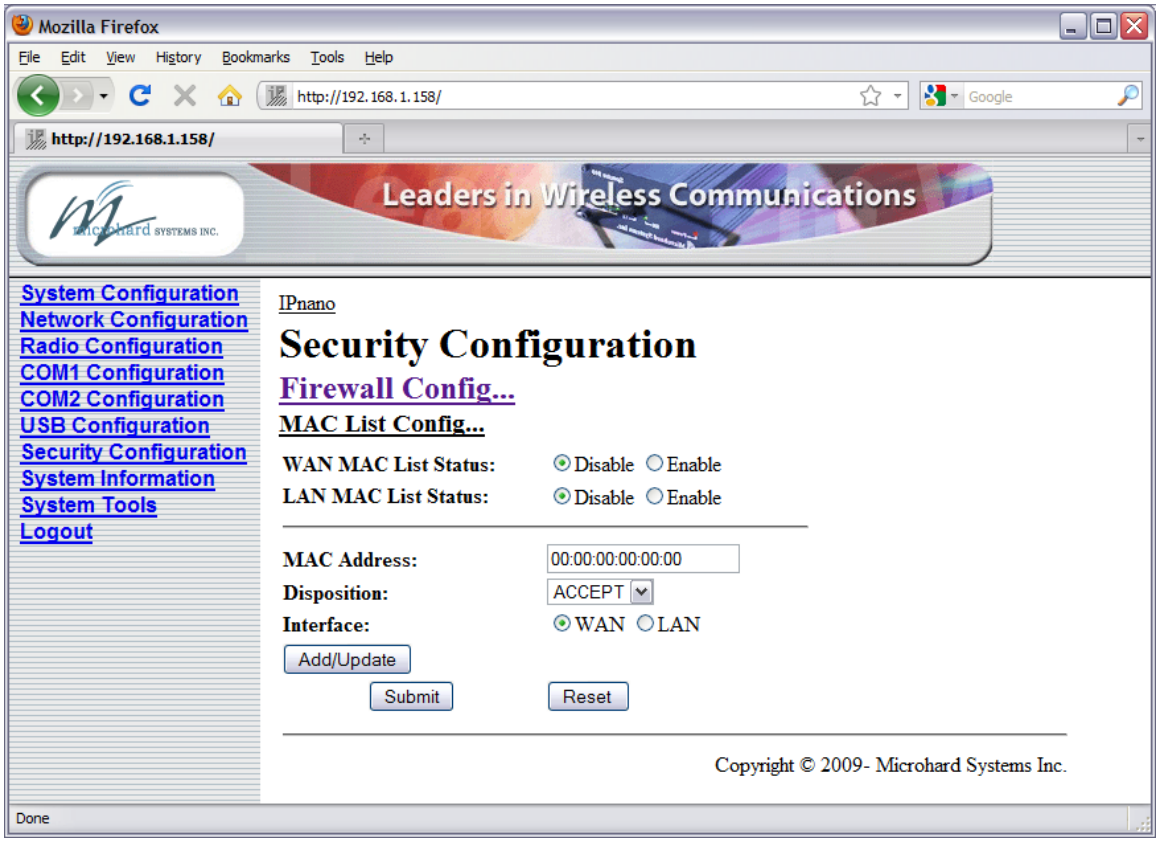


Image 6AI: Firewall Configuration, MAC List Config. Submenu

WAN MAC List Status

Enable or disable the WAN MAC list. List takes precedence over Rules.

Values

Disable
Enable

LAN MAC List Status

Enable or disable the LAN MAC list. List takes precedence over Rules.

Values

Disable
Enable

MAC Address

Specify the MAC Address to be added to the list.

Values

00:00:00:00:00:00

valid MAC address

6.0 Configuration

	Disposition
Determines the action to be taken on data traffic associated with the specified MAC address.	**Values** **ACCEPT** DROP REJECT
	Interface
Select which interface the defined MAC address is connected to.	**Values** **WAN** LAN

6.0 Configuration

6.1.8.7.5 Blacklist Configuration

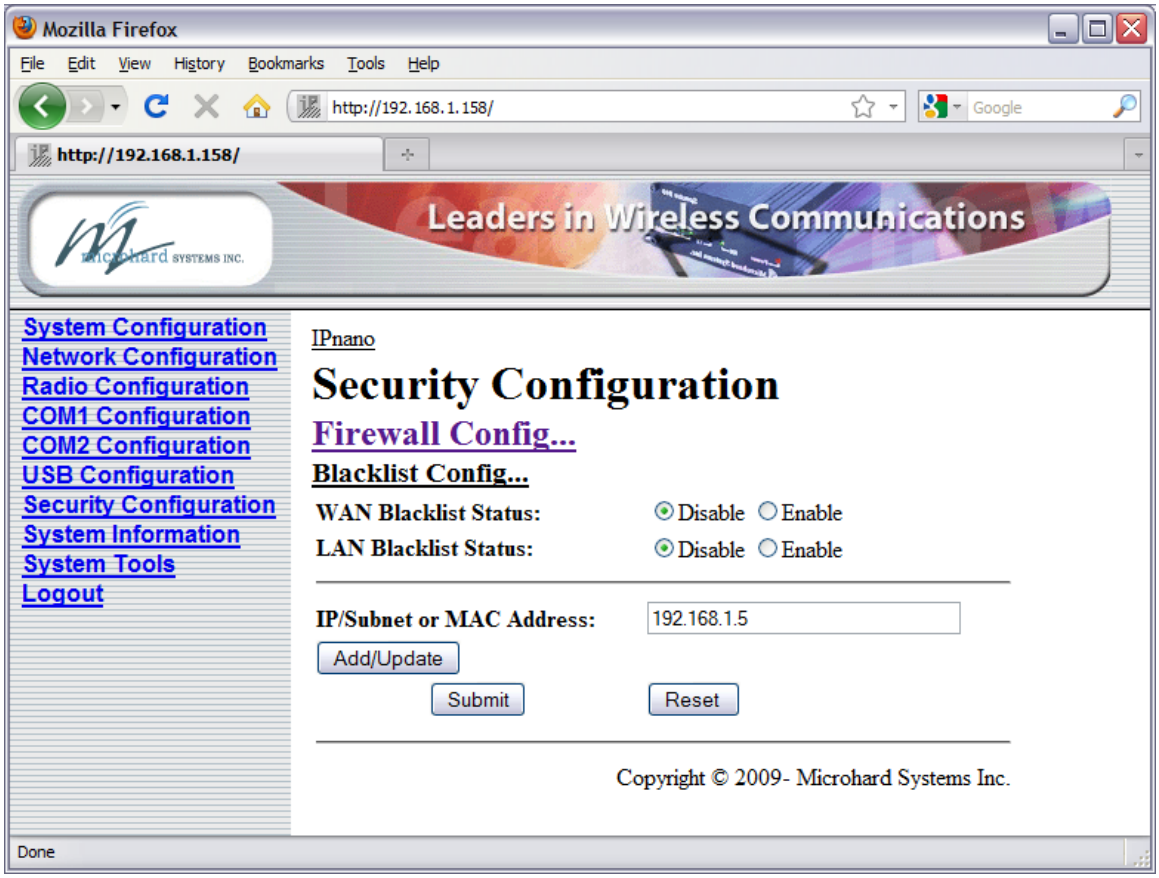


Image 6AJ: Firewall Configuration, Blacklist Configuration Submenu

WAN Blacklist Status

Enable or disable the WAN blacklist. List takes precedence over all other firewall settings.

Values

Disable
Enable

LAN Blacklist Status

Enable or disable the LAN blacklist. List takes precedence over all other firewall settings.

Values

Disable
Enable

IP/Subnet or MAC Address

Enter the IP/Subnet or MAC address of the device to be blacklisted. All data traffic associated with this address will be blocked.

Values

192.168.1.5
valid IP address

6.0 Configuration

6.1.8.7.6 Reset Firewall to Default

This menu provides a soft button which, when selected, will reset the firewall settings to factory defaults.

Image 6AK: Reset Firewall to Default

6.0 Configuration

6.1.9 System Information

The System Information menu affords a selection of a number of very useful tools for diagnostic and statistical purposes.

The information accessible via this menu, particularly when accessed on remote units wirelessly, provides an excellent aid to troubleshooting and network management.

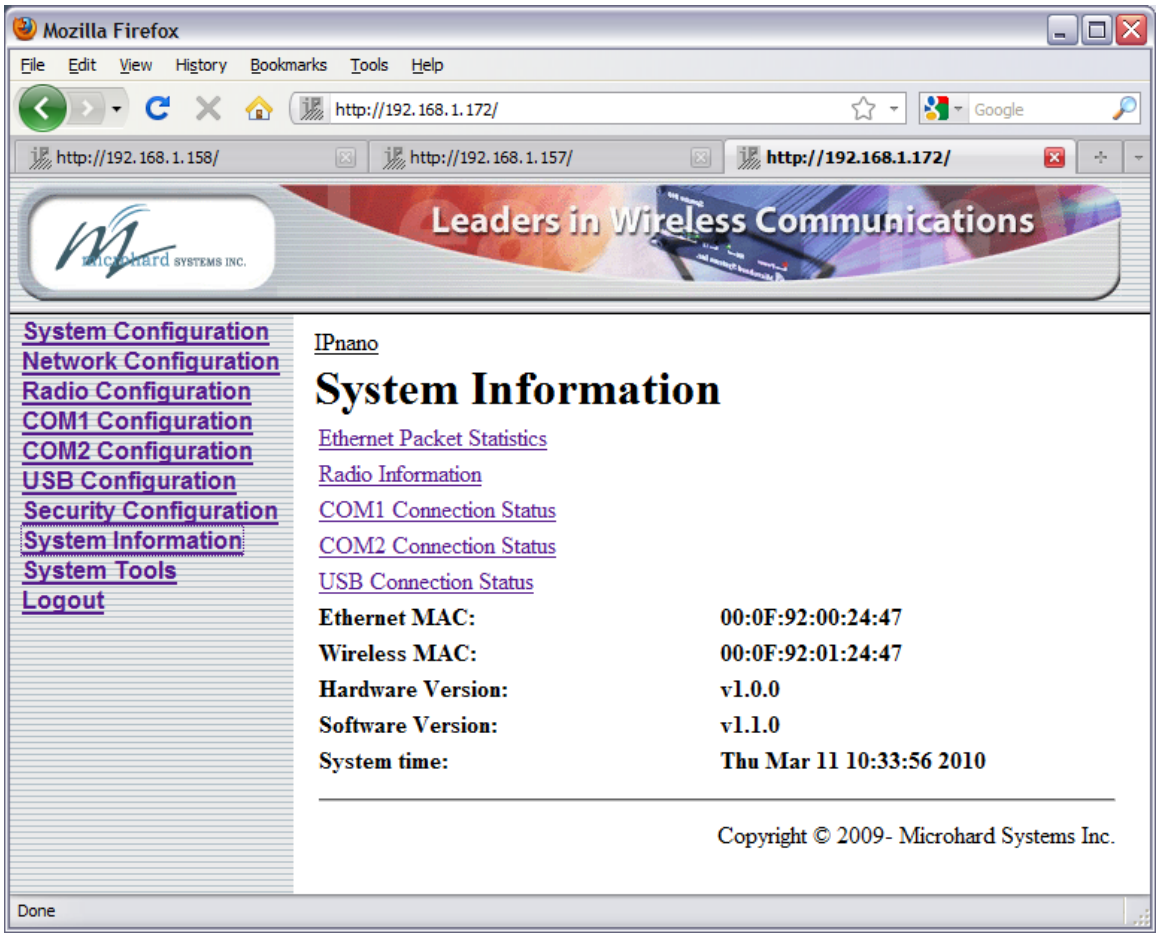


Image 6AL: System Information Menu

The five selectable System Information options provide information which refreshes automatically. Detailed statistical and status information about Ethernet Packets, Radio, COM (1/2) and USB ports can be found in the submenu's accessed from this screen. If desired, your browsers' ***Refresh*** button (F5) may be used to initiate a 'manual' refresh.

6.0 Configuration

Ethernet Packet Statistics

The Ethernet Packets Statistics window displays a variety of parameters which apply to the traffic through, and status of, the physical ethernet port (hardware interface) on the rear of the IP Series.

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

The FIFO errors are related to interface-specific hardware.

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

The Transmit Carrier count relates to carrier sense errors.

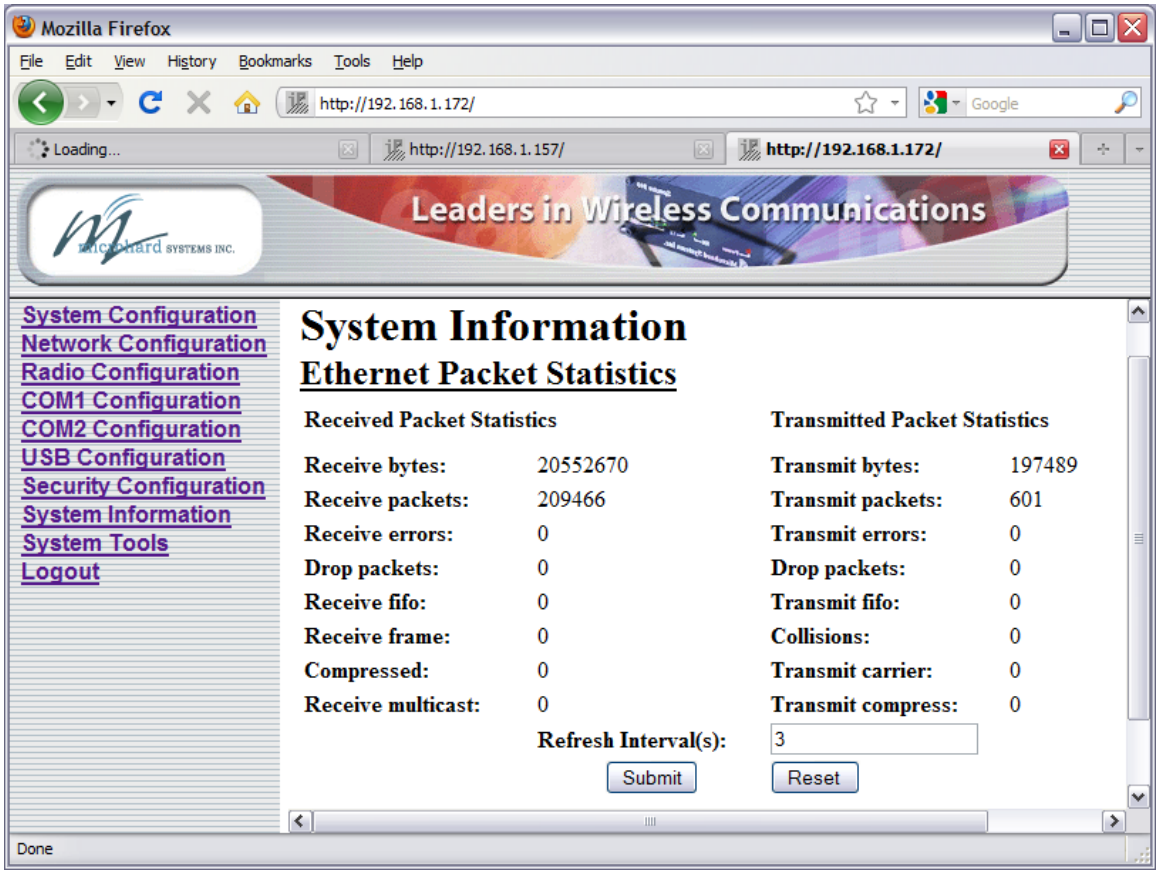


Image 6AM: System Information Menu, Ethernet Packet Statistics

6.0 Configuration

Radio Information

The Radio Information window provides information related to the 'radio' (wireless) portion of the Nano IP.

- Serial Number
  Serial number of radio (RF) module within Nano IP.
- Version
  Firmware version within radio module.
- Temperature (C)
  Temperature as measured within the radio module.
- Voltage (V)
  Supply voltage as measured on motherboard.
- RSSI (dBm)
  Receive Signal Strength Indicator measurement.

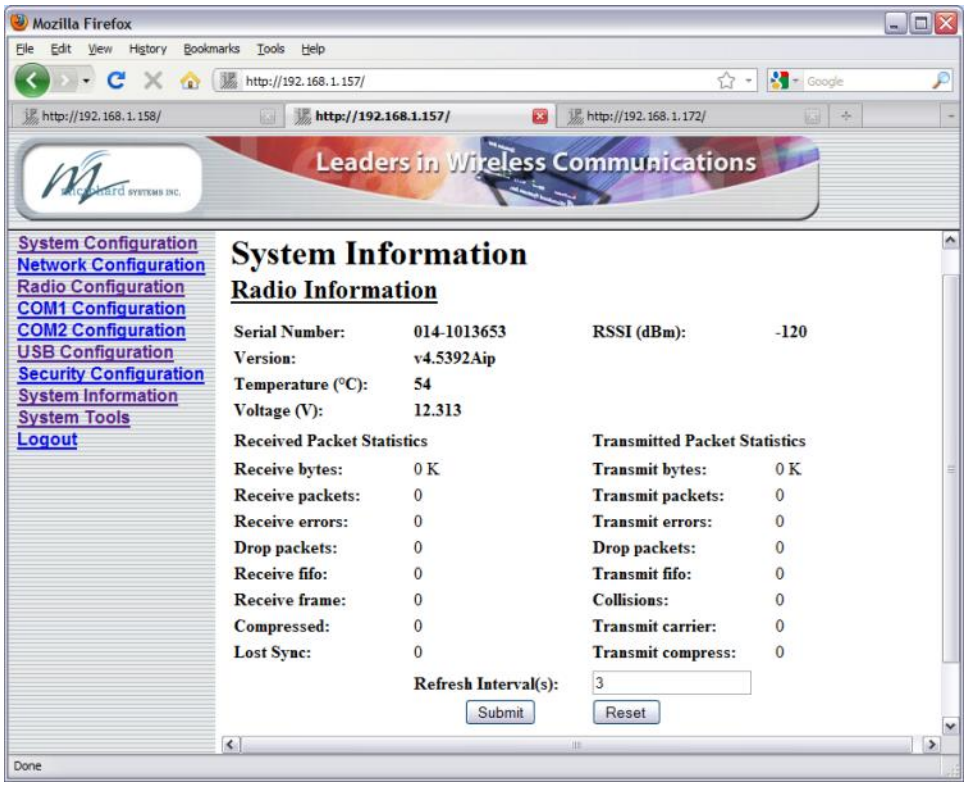


Image 6AN: System Information Menu, Radio Information

Not all statistics parameters displayed are applicable.

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

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

Lost Sync indicates how many times the Nano IP being viewed has lost synchronization with the Master Nano IP.

6.0 Configuration

COM1 (DATA) Connection Status

This window displays information related to the primary RS-232 serial interface (DATA on the rear of the Nano IP).

- COM1 Port Status
  Enabled by default.
  Configure via COM1 Configuration menu.
- COM1 Connect As
  Display of chosen protocol with respect to serial gateway function.
  Configure via COM1 Configuration menu.
- COM1 Connect Status
  If port is enabled and there is data traffic, this will display 'Active'.

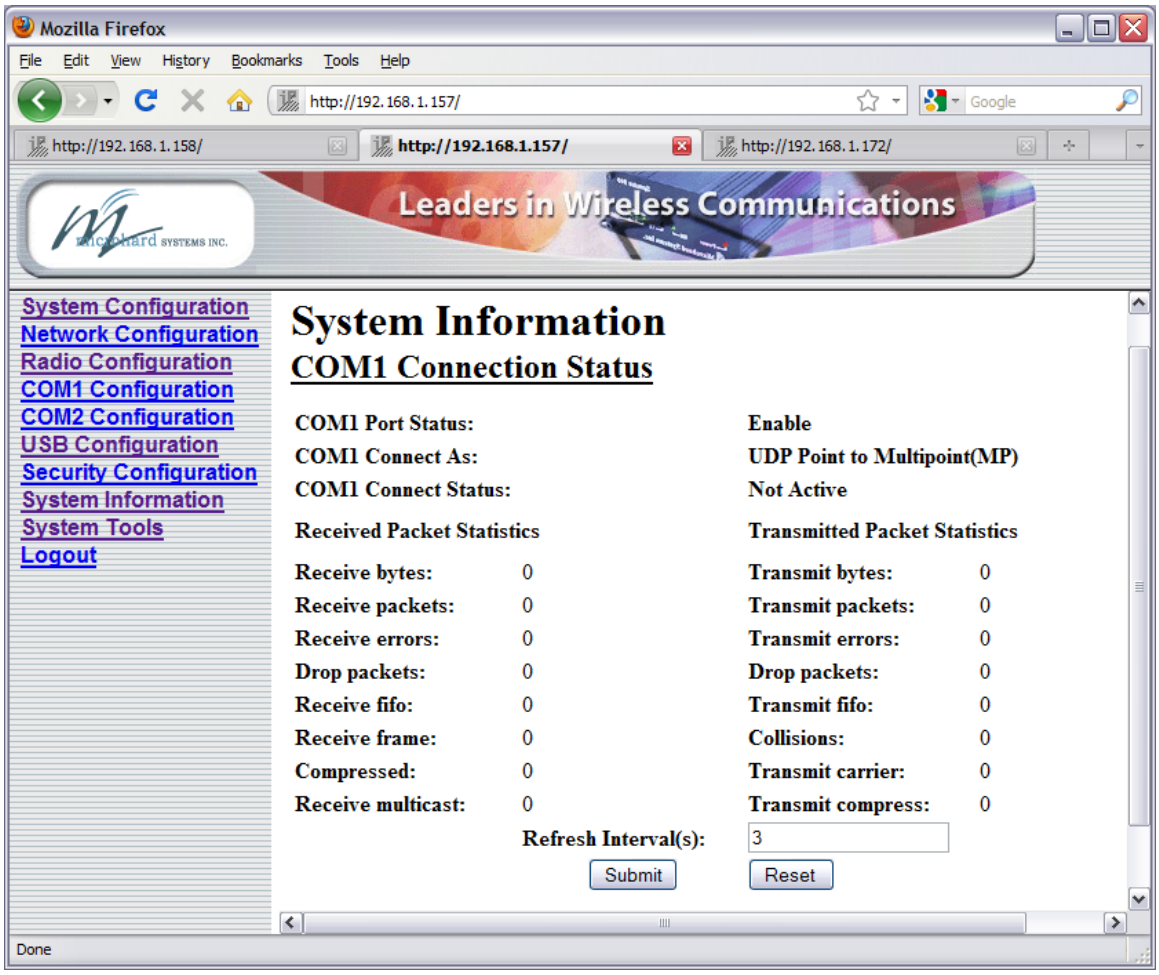


Image 6AO: System Information Menu, COM1 Connection Status

The other displayed parameters are not all applicable. Of most use are the transmitted and received bytes/packets: these will indicate if data is coming into and out of the RS-232 port.

6.0 Configuration

COM2 (Diagnostic) Connection Status

This window displays information related to the COM2 (Diagnostic) port located on the front of the Nano IP Series.

- COM2 Port Status
  Disabled (for 'data' traffic) by default. Being 'disabled' enables the port to be used for the Text User Interface.
  Configure via COM2 Configuration menu.
- COM2 Connect As
  Display of chosen protocol with respect to serial gateway function.
  Configure via COM2 Configuration menu.
- COM2 Connect Status
  If port is enabled and there is data traffic, this will display 'Active'.

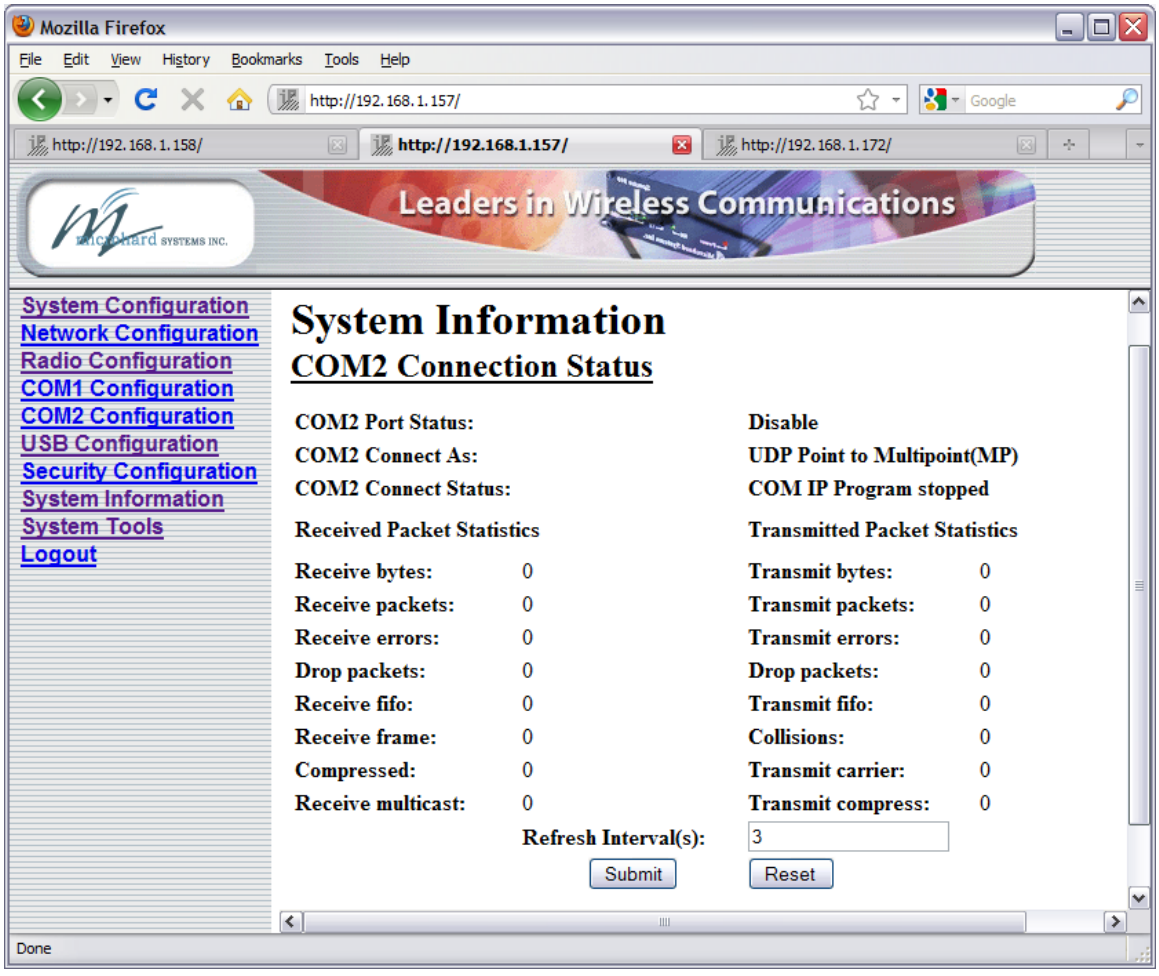


Image 6AP: System Information Menu, COM2 Connection Status

The other displayed parameters are not all applicable. Of most use are the transmitted and received bytes/packets: these will indicate if data is coming into and out of the COM2 port.

6.0 Configuration

USB Connection Status

This window displays information related to the USB port located on the front of the Nano IP Series.

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

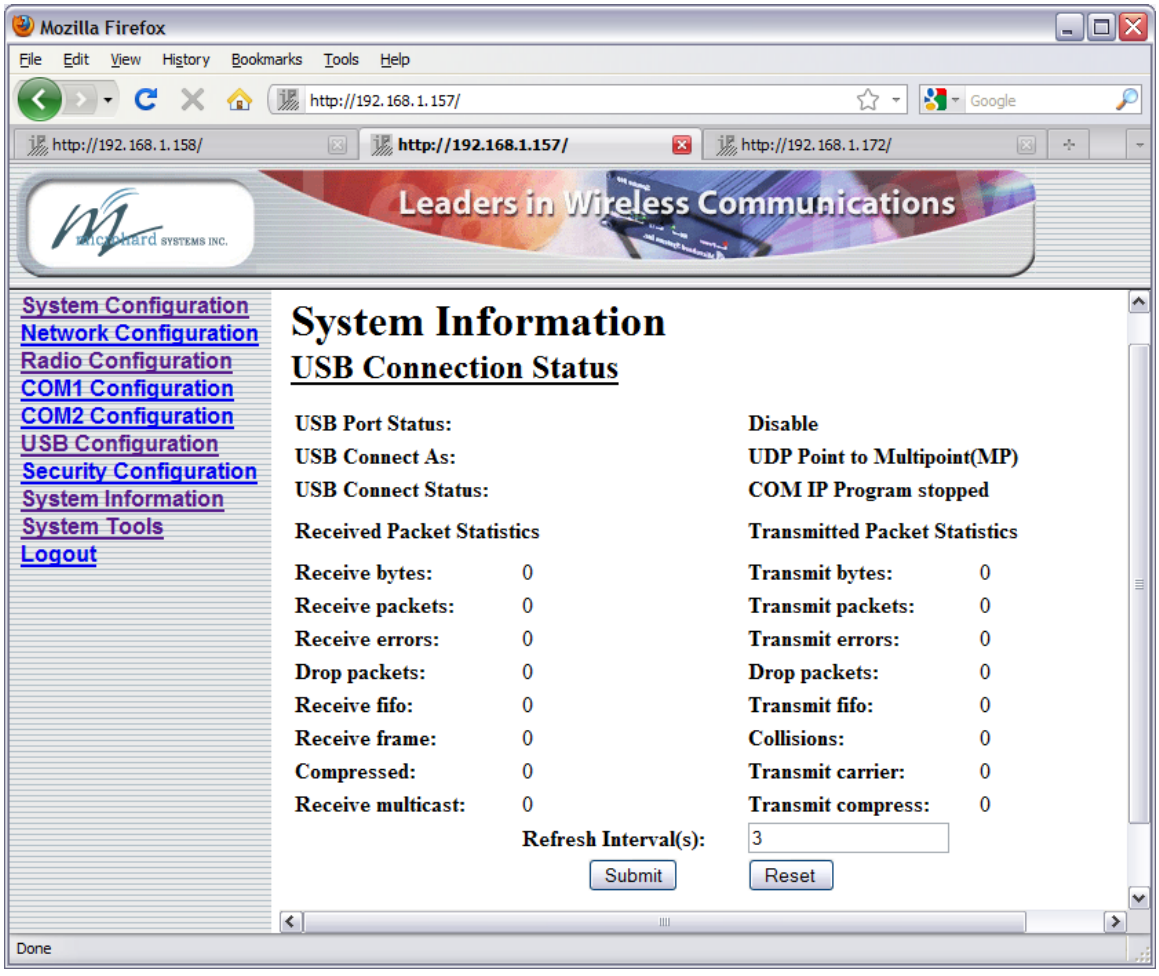


Image 6AP: System Information Menu, USB Connection Status

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

6.0 Configuration

6.1.10 System Tools

This menu is used for performing system maintenance (upgrades), rebooting the system (locally or remotely), resetting the system to factory default settings, and for monitoring the radio channel noise within the operating frequency range of the Nano IP Series.

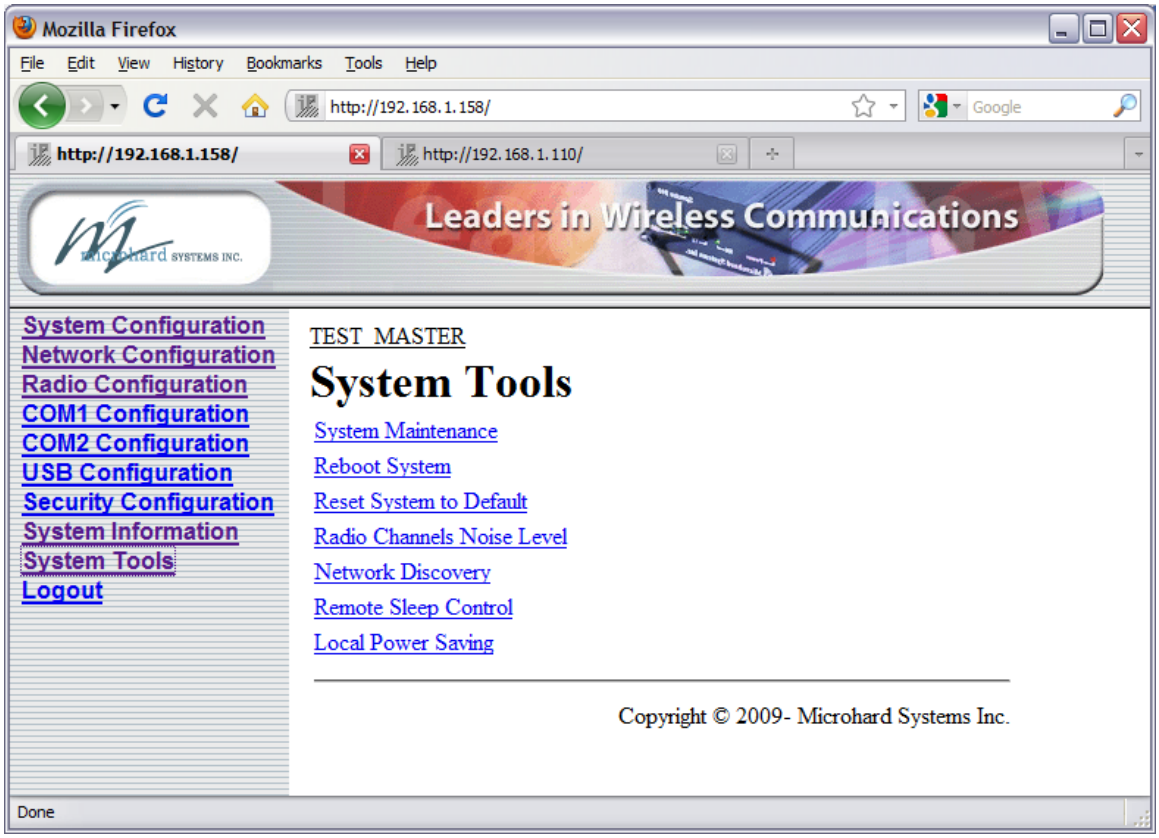


Image 6AQ: System Tools Menu - Master

6.0 Configuration

6.1.10.1 System Tools > System Maintenance

The System Maintenance menu allows a user to view all system settings using the ***System Settings*** *'View'* option. This produces a long listing of all settings of the unit under scrutiny. Selecting '*Download'* affords the opportunity to download the various values. This file may be useful for reference or requested by Microhard Support to aid is any required troubleshooting or application analysis.

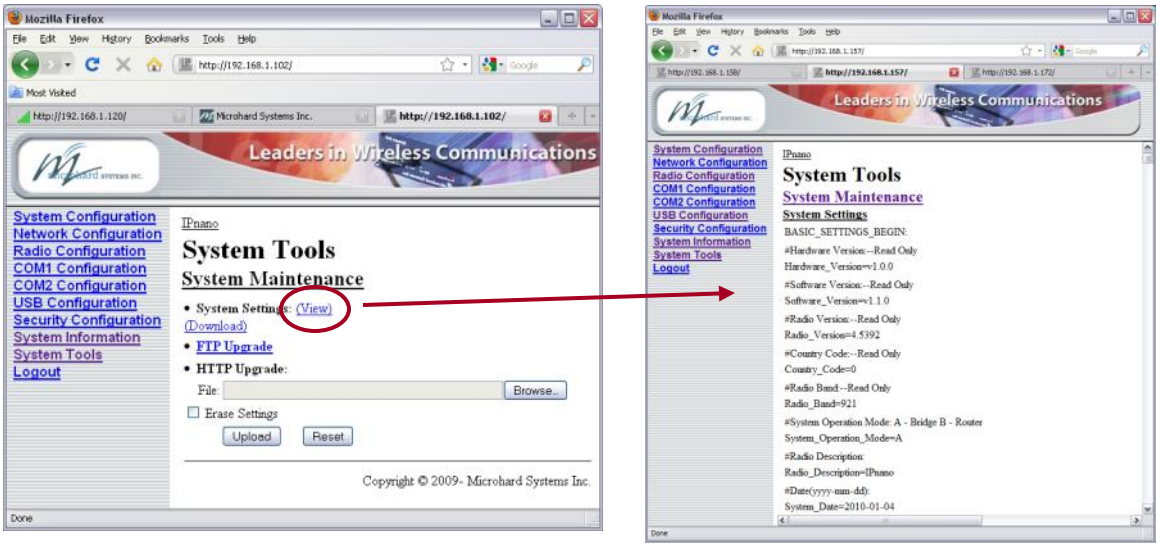


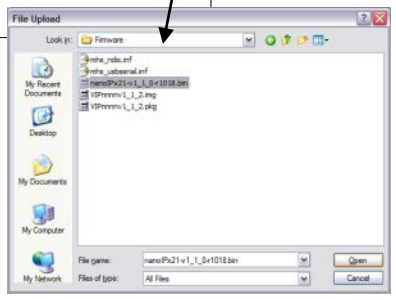
Image 6AR: System Tools Menu, System Maintenance

Not all types and versions of web browser applications support the FTP upgrade method described on this page. (If supported, remote units may also be upgraded wirelessly.)

Image 6AS: System Tools Menu, Password

The FTP Upgrade is used to update the system software in the Nano IP. Selecting the FTP Upgrade link will result in the prompt shown below. Default User Name is '**upgrade**', Default Password is '**admin**'.

HTTP Upgrade is another option to upgrade the Nano IP's system software (firmware). Select the Browse button to locate the upgrade file provided my Microhard Systems.



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

The Upload button will begin the process. It can take several minutes to complete.

6.0 Configuration

6.1.10.2 System Tools > Reboot System

This feature is particularly useful for rebooting remote units. It has the same effect as power cycling the unit.

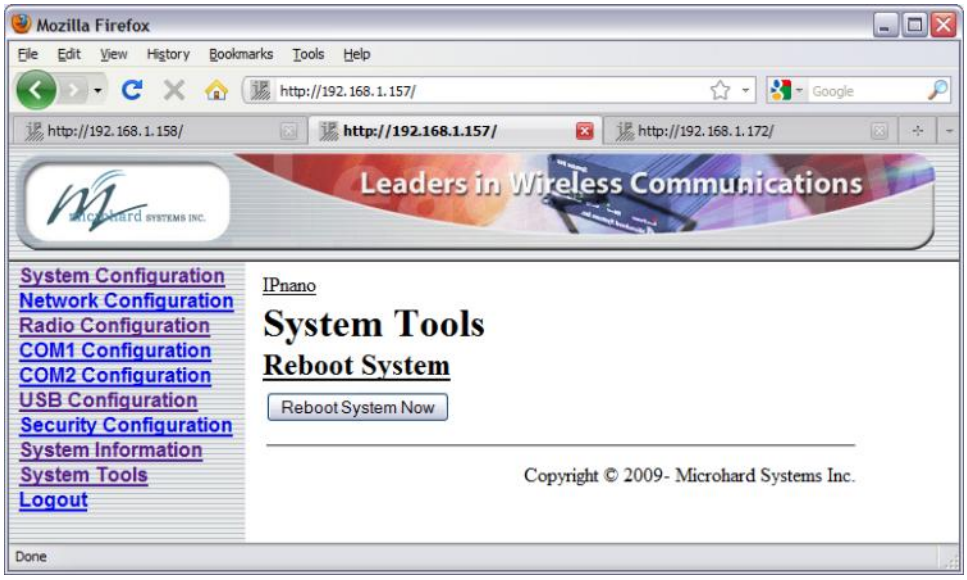


Image 6AT: System Tools Menu, Reboot System

6.1.10.3 System Tools > Reset System to Default

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

Image 6AU: System Tools Menu, Reset System to Default

6.0 Configuration

6.1.10.4 System Tools > Radio Channels Noise Level

This tool may be used to measure and observe the mean (average) and peak (max) noise levels in the operating frequency range of the Nano IP Series.

When a Radio Channels Noise Level measurement is taken, the Nano IP goes 'offline' with respect to data transfer.

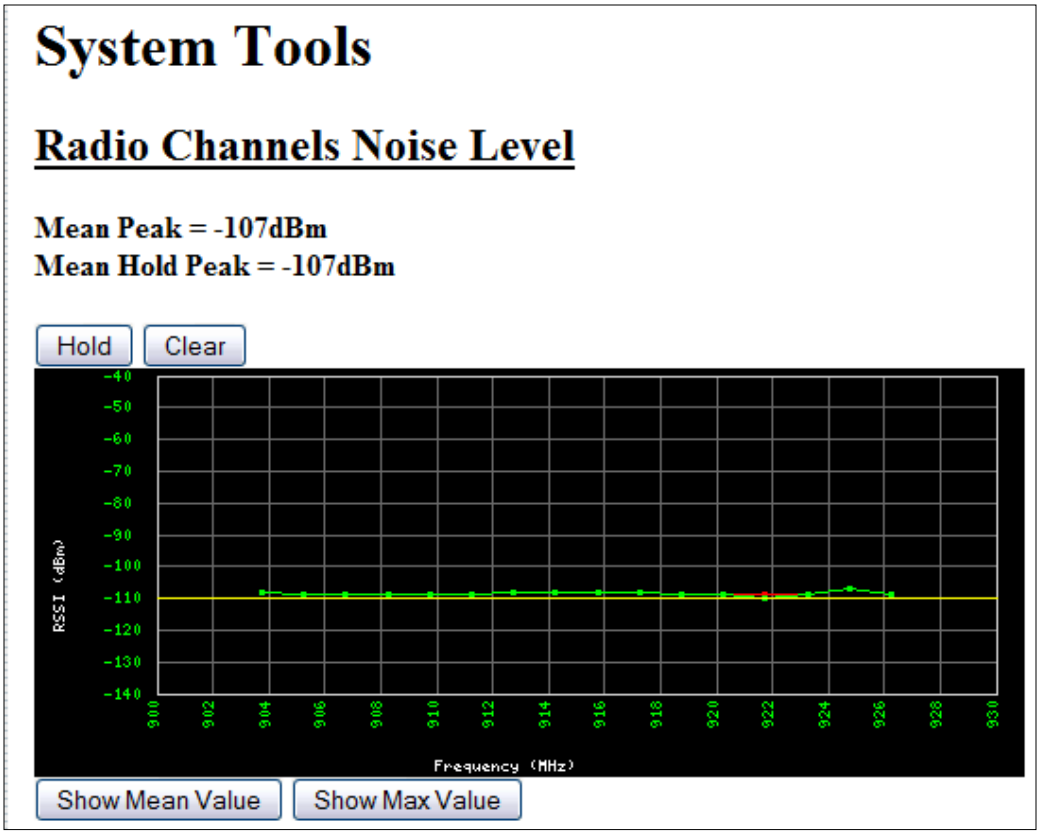


Image 6AV: System Tools, Radio Channels Noise Level, Mean Value

- **Hold**
  Do not refresh currently displayed values.
- **Clear**
  Clear current values and take new measurements.
- **Show Mean Value**
  Display the mean (average) values of noise level measurements.
- **Show Max Value**
  Display the maximum (peak) measured noise levels.

6.0 Configuration

6.1.10.5 System Tools > Network Discovery

This tool may be used to search the current network to find additional Nano IP and/or IP Series units and report the IP Address, Unit Address and Description of each unit. The Refresh button will force the Nano IP to search the network.

Image 6AW: System Tools, Network Discovery

6.1.10.6 System Tools > Remote Sleep Control (Master)

Remote Sleep Control allows basic remote configuration of the sleep properties of remote units. Any sleep configuration parameters sent from a Master unit will overwrite any existing sleep settings in the remote unit. (Sleep mode is not available on IPn2420 models)

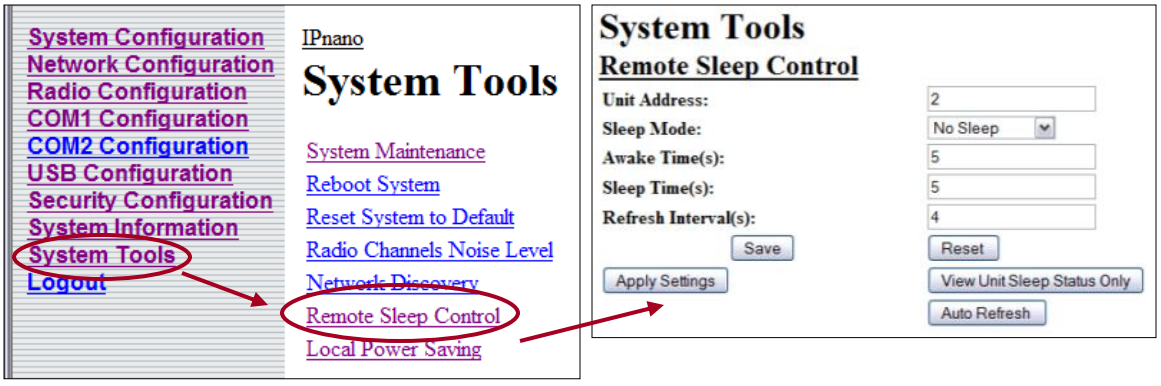


Image 6AX: Remote Sleep Control

6.0 Configuration

Sleep mode is not available on IPn2420 models.

Remote Sleep Control

Image 6AY: Remote Sleep Control

Unit Address: Unit Address of the remote unit where the sleep commands are sent.

Sleep Mode:
No Sleep: No sleep settings.

Radio Sleep: Shuts down radio module when not in use for the configured amount of time.. IP/CPU Module is still active during radio sleep. Unit will re-sync and transmit data in ~1 second upon wakeup. Will wakeup on timer and/or activity.

System Sleep: Shuts down entire unit. Will wakeup on timer and/or activity. Upon wake up system will restart and re-sync and transmit data in ~60 seconds.

Awake Time (s): Defines how long the unit will keep awake. If set to 0, the unit will not wakeup until data is received on the serial or ethernet port. Valid range in seconds (s) is 0 - 65535.

Sleep Time (s): Defines how long the unit will sleep. If set to 0, the unit will not enter sleep mode. Valid range is 0 - 65535 (s).

Refresh Interval (s): Refresh Timer to automatically refresh the web browser.

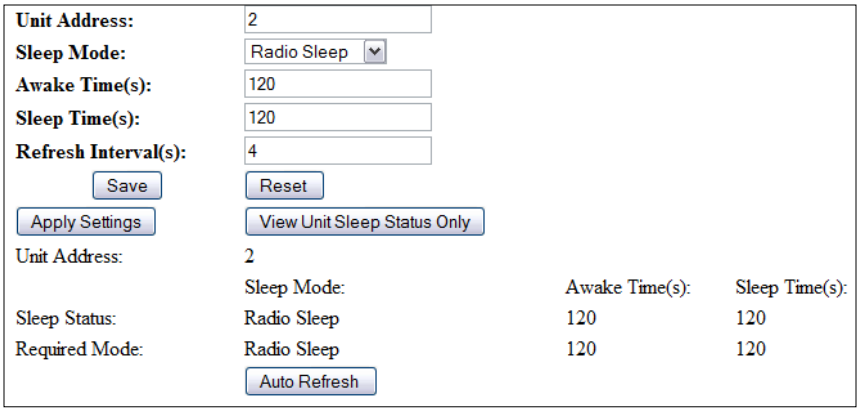


Image 6AZ: Remote Sleep Control

Save: Writes values entered in the boxes above to the Master units memory.

Apply Settings: Writes values in Master units memory to the remote unit.

Reset: Resets values shown in the boxes above to the values stored in the Master unit.

View Unit Sleep Status Only: Retrieves the sleep settings stored on the remote unit.

Auto Refresh: Forces the browser to refresh.

6.0 Configuration

6.1.10.7 System Tools > Local Power Saving (Master)

When the unit is configured as a ***Master*** in the Radio Configuration menu, settings for ***Local Power Saving*** will be listed under the System Tools Menu. The Local Power Saving Modes provide power saving options for when the Master unit is not transmitting or receiving data.

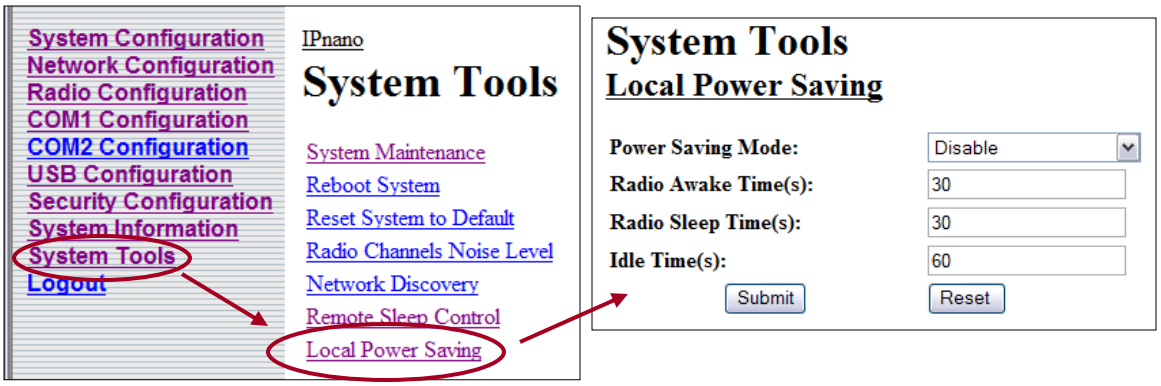


Image 6BA: System Tools: Local Power Saving

Radio will enter Power Saving Mode 60 seconds after system boot up.

Power Saving Mode

Disable: Power Saving Mode is disabled by default.

Auto Wakeup: Unit will wakeup from activity on serial port, Ethernet port or radio data, if the *Radio Awake Time* is a nonzero value. Power consumption is about 35-45 mA @ 12VDC.

Serial Port Wakeup: Unit will wakeup from serial port or radio data if *Radio Awake Time* is nonzero value. Power consumption is about 15-25mA @ 12VDC.

Ethernet Port Wakeup: Unit will wakeup from Ethernet port or radio data if *Radio Awake Time* is a nonzero value. Power consumption is about 30-40mA @ 12VDC.

Power Shutdown: Timer control shutdown mode. Controlled by *Radio Awake Time* and *Radio Sleep Time* parameters. System will reboot when the radio wakes up. Power consumption is about 1mA @ 12 VDC.

Values

Disable
Auto Wakeup
Serial Port Wakeup
Ethernet Port Wakeup
Power Shutdown

Radio Awake Time

Defines how long the radio will keep awake. If set to 0, the radio will not wakeup until received data from the port configured in the **Power Saving Mode** (Serial or Ethernet ports).

Values (seconds)

30
0 - 65535

6.0 Configuration

	Radio Sleep Time
Defines how long the radio will sleep. If set to 0, the radio will not enter sleep mode.	**Values (seconds)** **30** 0 - 65535

	Idle Time
Defined the amount of system idle time required before going entering power saving mode cycle.	**Values (seconds)** **60** 0 - 65535

6.1.10.8 Logout

The Logout menu informs the user how to log out of the Web User Interface, by closing the current web browser session.

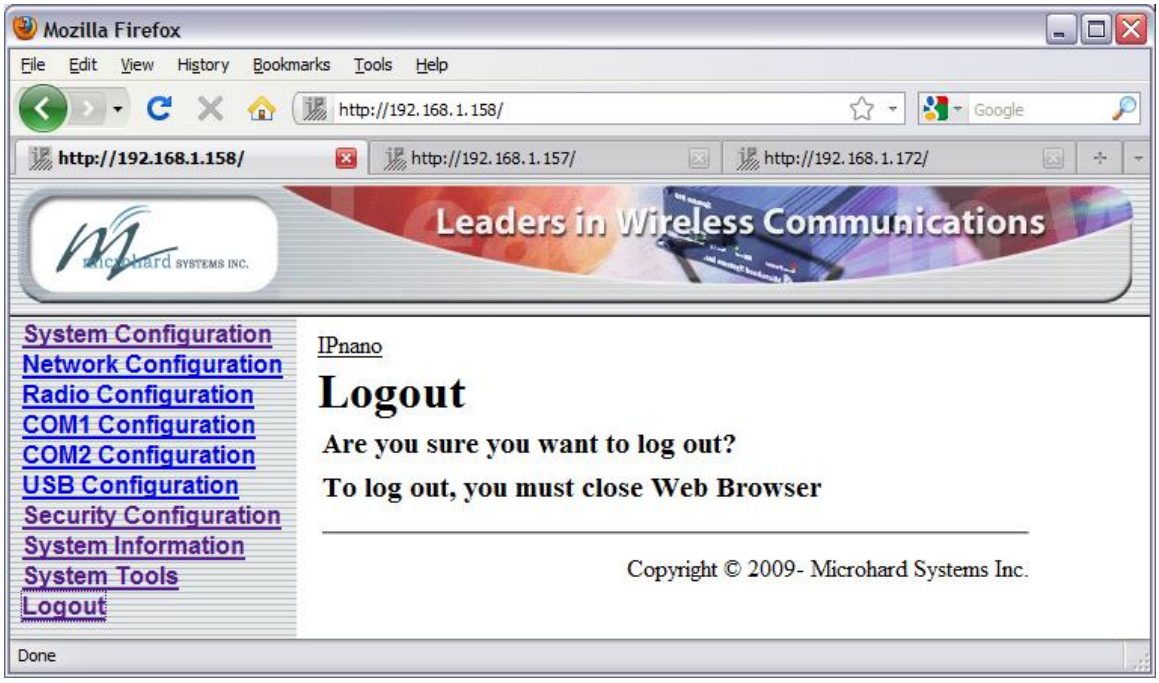


Image 6BB: Logout Window

6.0 Configuration

6.2 Text User Interface

Initial configuration of an Nano IP Series using the Text User Interface (Text UI) method involves the following steps:

- connect the Nano IP's front panel Diagnostic (COM2) port to an available COM port on your PC, using a standard RS232 cable.
- run a terminal program (e.g. HyperTerminal) for the connected PC COM port, configured for 115200bps, 8 data bits, no parity, and 1 stop bit. Flow control should be set to 'none'.
- apply power to the Nano IP Series and wait approximately 1 minute for the system to load - you will observe various text appearing in the terminal program window. Once the Nano IP has completed its boot up procedure a login prompt will be displayed as seen below:

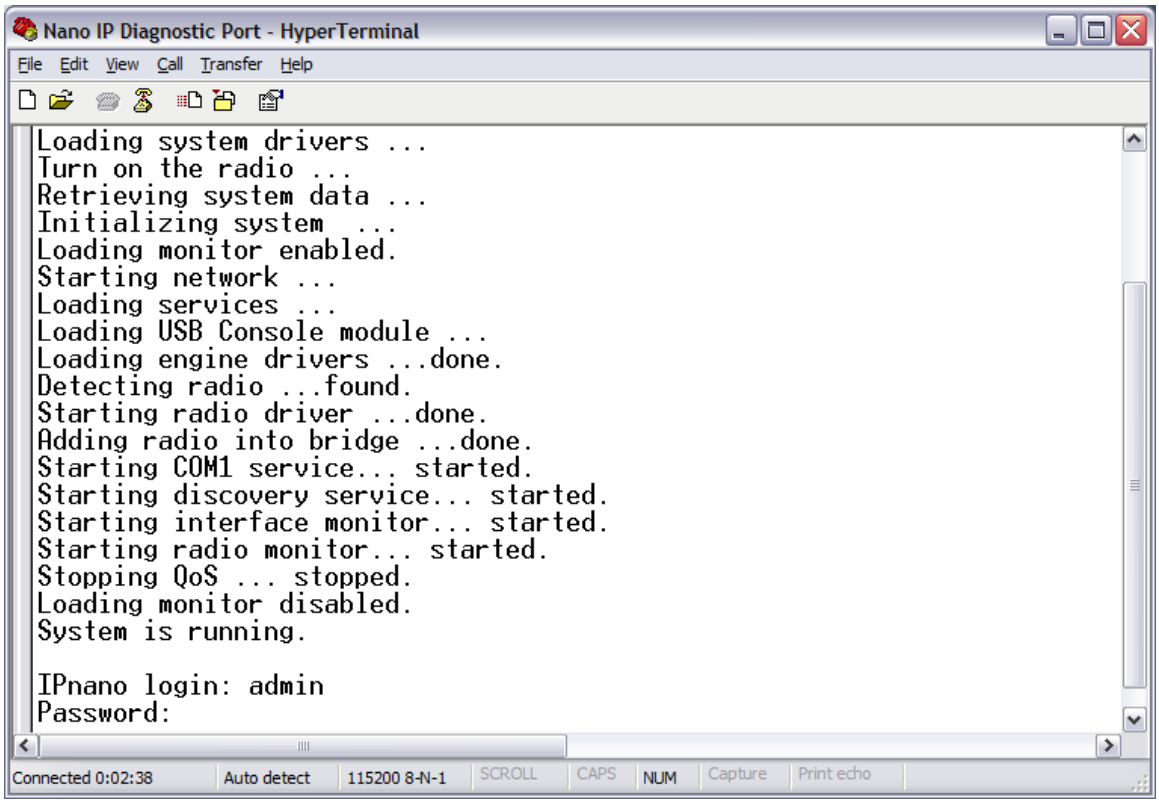


Image 6BC: Text User Interface, Login Prompt

- Enter the default login name (provided it was not changed via the Web User Interface at an earlier time): **admin** *[Enter]*
- Enter the default password (if still applicable): **admin** *[Enter]*

continued...

6.0 Configuration

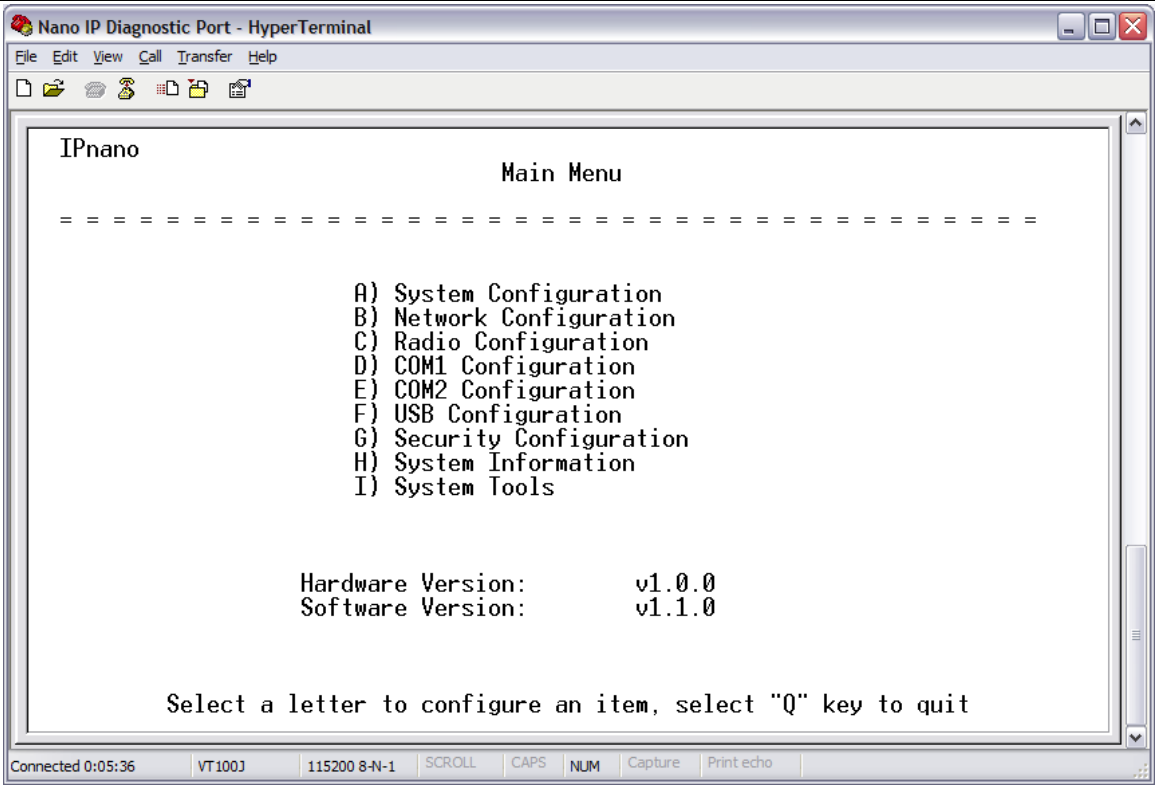


Image 6BD: Text User Interface, Main Menu

Upon successful login, the above Main Menu will appear.

Refer to the detailed information within the Web User Interface section (6.1) of this manual for a detailed explanation of all of the configuration options. All options presented within the Web UI are available via the Text UI.

There is a PING tool which may be found via the Text UI (System Tools Menu) which is not available in the Web UI.

An advantage of using the Text UI as opposed to using the Web UI for configuring the IP Series is that with the Text UI there is no need to concerned with the unit's IP address or subnet.

There are some subtle differences in configuring the IP Series using the Text UI. The following steps pertaining to configuring the Radio portion of the unit will highlight those differences:

6.0 Configuration

- Select ‘C’ on the Main Menu to be directed to the Radio Menu (see below):

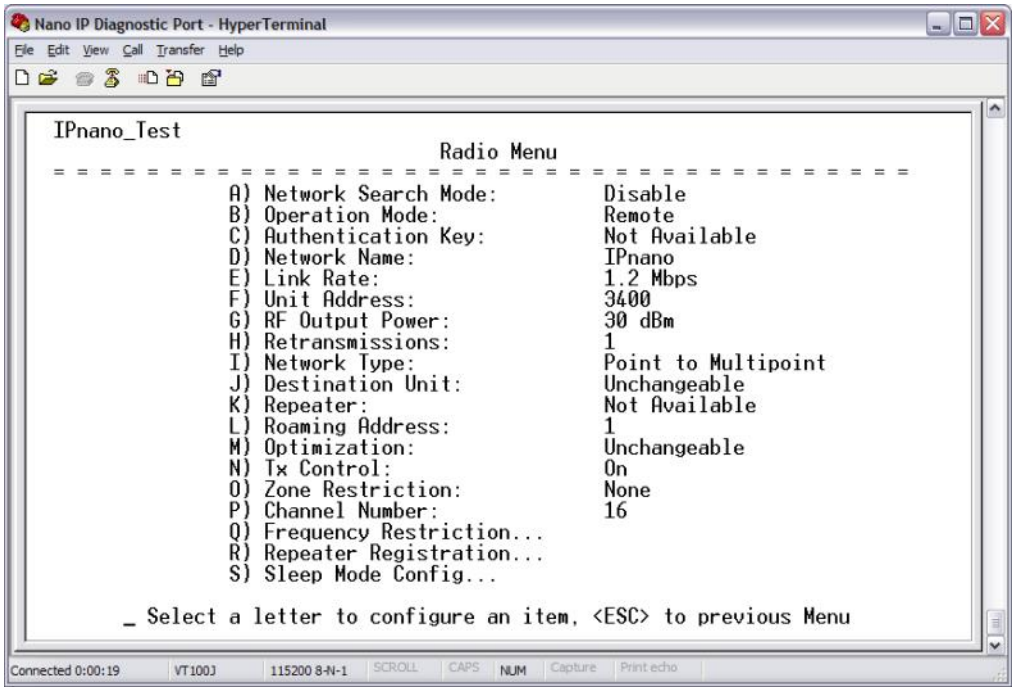


Image 6BE: Text User Interface, Radio (Configuration) Menu

- Select ‘I’ to change the Network Type. The following will appear:

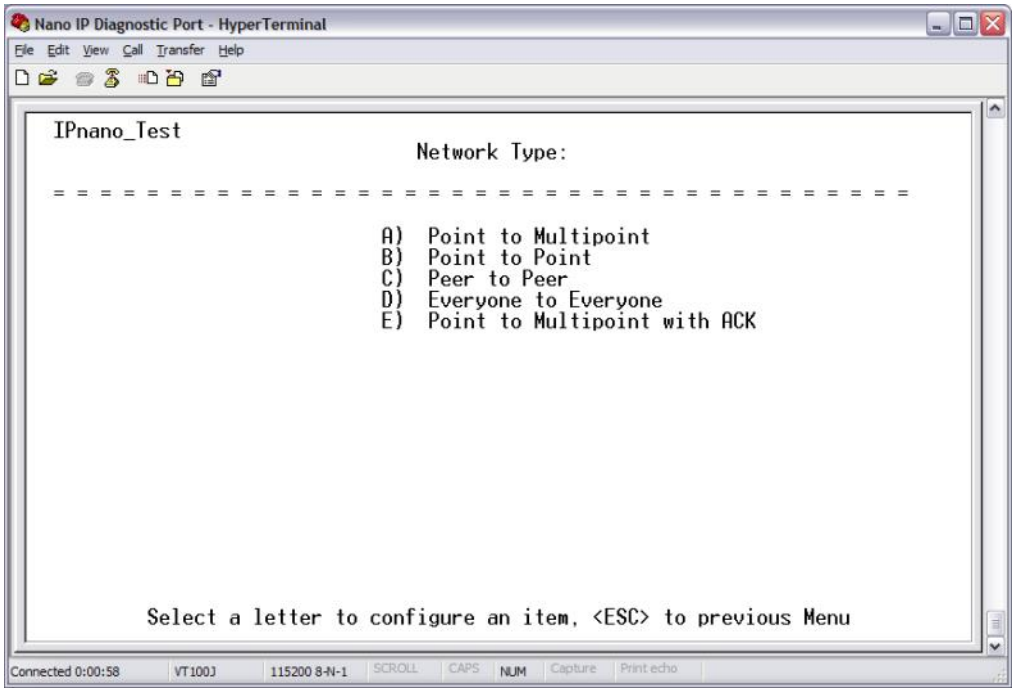


Image 6BF: Text User Interface, Radio Menu, Network Type

6.0 Configuration

- Having selected 'A' - Point-to-Multipoint - the Radio Menu appears showing the newly-selected Network Type:

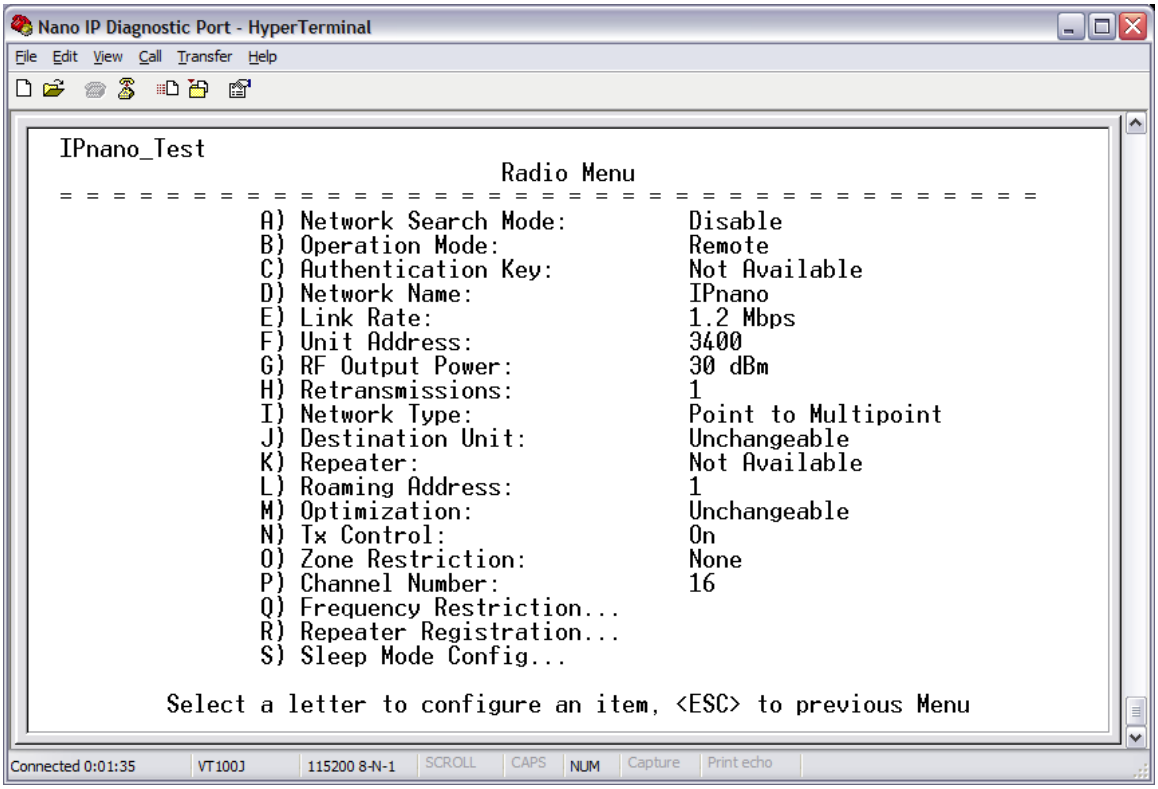


Image 6BG: Text User Interface, Radio Menu, Save Option

Be certain to SAVE any desired configuration changes.

This action is the same as activating the SUBMIT soft button when using the Web UI.

- Press '**U**' to save and apply the changes, or press '**V**' to discard them.

As can be seen in the preceding screen captures, the ***[Esc]*** key is used to 'back up' to the previous menu.

When at the Main Menu, the '**Q**' may be used to Quit the Text UI: the IP Series will display the login prompt.

7.0 Installation

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

There 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:

Network Topology

Section 5.0 detailed the various network topologies which the Nano IP Series will support. Determine which topology is suited to your specific requirements.

Throughput

The Nano IP Series is capable of significant data throughput. 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 Nano IP Series dictates such things as required antenna performance and heights, and whether or not a Repeater(s) is required. When contemplating antenna types and Repeater sites, keep in mind the directivity (omnidirectional or directional) of the antennas, also recall the effect of a Repeater on throughput (see Section 4.4).

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 IP Series. 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 Nano IP 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 Nano IP Series features the maximum available transmit power combined with exceptional receive sensitivity - two 'numbers' which will produce the most favorable path calculation results.

7.0 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 Nano IP 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 900MHz frequency range, sometimes the height requirements are not adhered to: this may result in unreliable communications.

Power Requirements

The IP Series accepts a range of DC input voltages (keep in mind that supply current requirements must also be met). In some deployments, power consumption is critical. Power consumption for the IP Series may be minimized by reducing the transmit power, given the receive sensitivity of the distant modem.

Interference

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

7.0 Installation

7.1 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 7.1.1:

Tx power = 30dBm
Tx antenna gain = 6dBi
Tx cable/connector loss = 2dB
Rx antenna gain = 3dBi
Rx cable/connector loss = 2dB
Rx sensitivity = -105dBm

System Gain = 30+(6-2)+(3-2)
+105
= 30+4+1+105
= 140dB.

7.0 Installation

Distance (km)	Base Height (m)	Mobile 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 7A: 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.

Once the equipment is deployed, average receive signal strength may be viewed in the System Information, Radio Information display.

7.2 Installation of Antenna System Components

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

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

7.0 Installation

7.2.1 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.

Direct human contact with the antenna is potentially unhealthy when a Nano IP is generating RF energy. Always ensure that the Nano IP equipment is powered down (off) during installation.

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.

In a long-range PTP network, Yagi antennas should be considered. There antennas will provide for the most focused 'RF connection' between the two sites.

In a PMP network where remotes are located in all directions from the Master, the Master site will have an omni so that it can communicate with all remotes; the remotes, however, may all employ Yagi antennas 'pointed at' the Master.

Typically a Repeater site will employ an omni such that it can readily receive an RF transmission from one direction and be able to readily transmit it in another.

If an application involves remotes which are not stationary (e.g. mobile application), all sites would likely use omni antennas so that wherever the units may be, there should be antenna pattern coverage.

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

The path calculation (see Section 7.1) will determine the antenna gain requirements. Refer to the beginning of this section to review the various factors which must be considering when deploying a network. Do not discount the importance of the REQUIRED HEIGHT for the antennas within your network.

7.2.2 Coaxial Cable

The following types of coaxial cable are recommended and suitable for most applications (followed by loss at 900MHz, 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.

7.0 Installation

7.2.3 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.

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

7.2.4 External Filter

Although the Nano IP 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 Nano IP 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.

Appendix A: DiscoverIP Utility

The DiscoverIP utility can be used to 'discover' any Nano IP and/or IP Series units that are 'reachable' via the connection made to the PC on which it is running. It will discover units that are 'wired' or have 'wireless' connectivity.

Upon launching the application, the following is displayed:

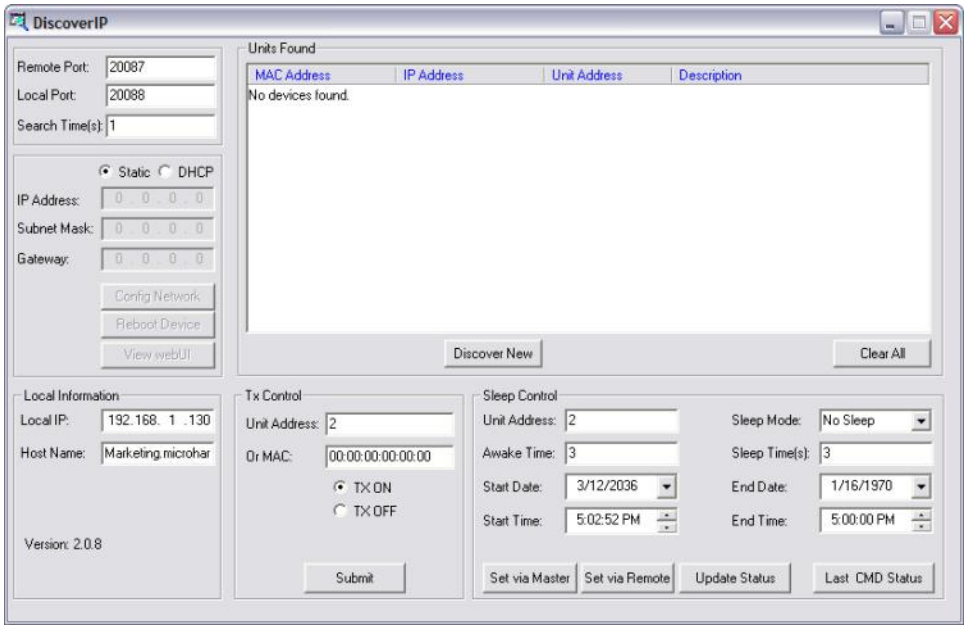


Image A1: *Initial Display*

See Section 6.1.7.4 re configuring the Nano IP Series to be, or not be, 'discoverable'.

In the sample, there is three Nano IP units connected to same network to which the PC is connected. Activating the 'Discover New' button results in the Nano IP Series being discovered by the utility:

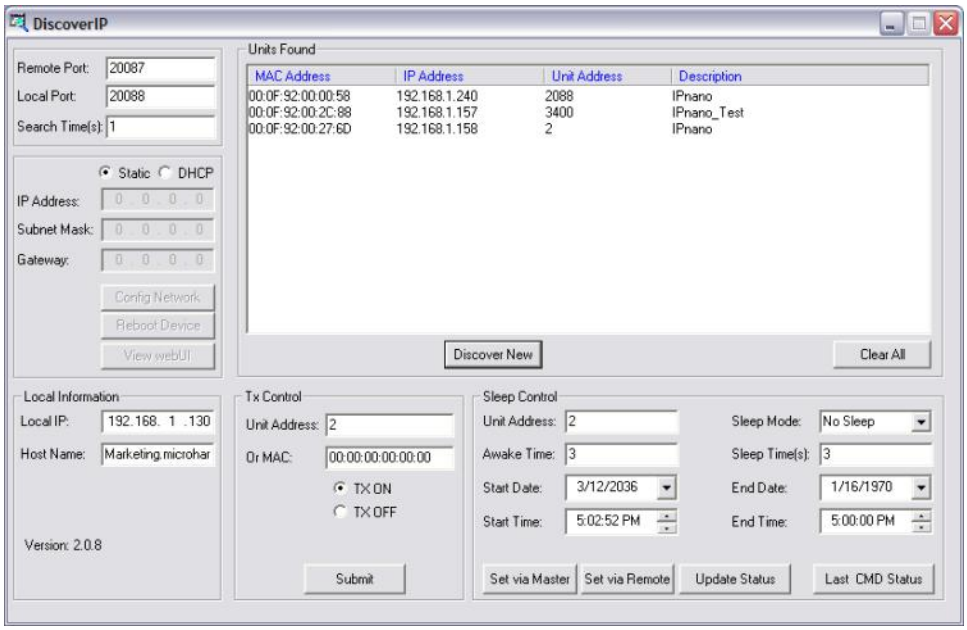


Image A2: *Nano IP Series Discovered*

Appendix A: DiscoverIP Utility

Verify that the PC's Network Settings (TCP/IP Properties) are suited to establishing a connection with the Nano IP Series.

To view the Web User Interface (Web UI) of a particular unit, either (a) highlight the target unit and click the View WebUI soft button, or (b) double click on the MAC or IP address, or Description of the target unit.

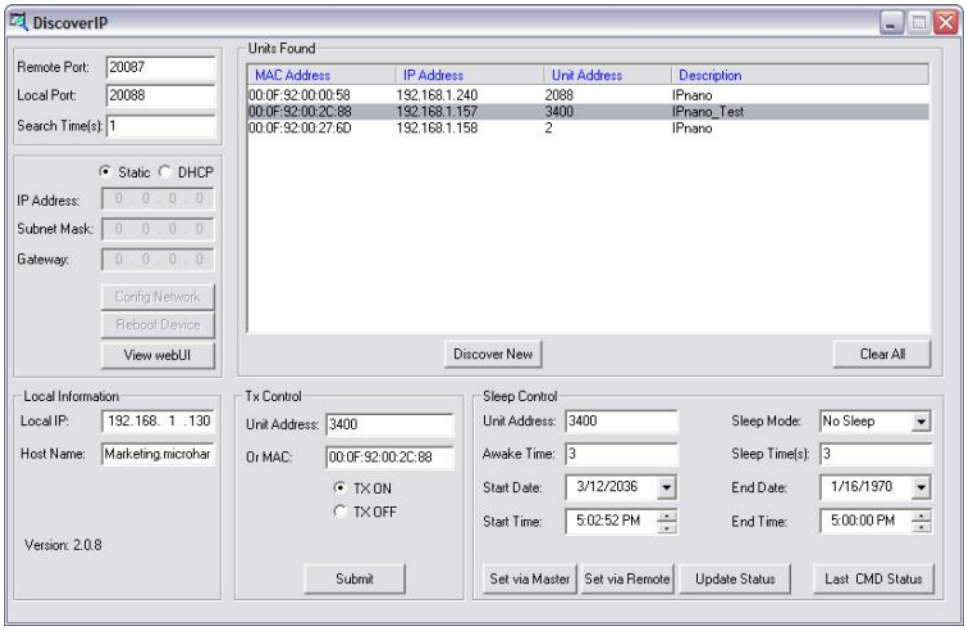


Image A3: *Select Target Nano IP Series*

Selecting either method (above) will launch the PC's web browser to the IP Series Logon window.

If it would be necessary but is not convenient to change the TCP/IP Properties settings on the PC note the following:

When received from the factory, the units are configured as DHCP, with an IP Address of 169.254.x.x, and Subnet Mask of 255.255.0.0.

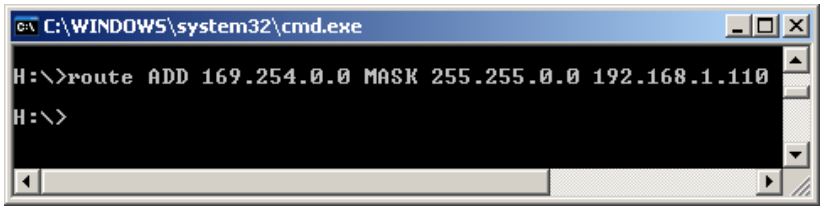


Image A4: *Add Route*

Go to the DOS prompt on the PC and, for each time you connect to an IP Series (with ethernet cable), enter
(Replace 192.168.1.110 with the IP Address of your PC.)

After the route has been added, you should be able to access the unit's WebUI logon page as detailed above.

Appendix B: Firmware Recovery Process

The following procedure outlines the steps required to recover a IP Nano Series should it need to be completely reloaded. This procedure will wipe out all configuration settings and return the device to factory default settings.

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

2. Separate your PC from the your network if attached, and set IP to static
192.168.1.1
255.255.255.0

3. Connect the PC Ethernet port to the Ethernet port of the IP Nano 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 Nano IP while press and hold CFG button;

6. Release the CFG button when ping begins to respond:
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, contact Microhard Systems Inc for additional help and/or troubleshooting.

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 nanoIPx21v1_1_22-r1044.bin (or the file saved).

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

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

Note, if you see message above, the unit will re-flash itself and reboot.

9. Now, wait for the unit to recover and reboot.

Appendix C: RS485 Wiring

The Nano IP Series can be connected into a 2– or 4-wire RS485 network. A transmission line termination should be placed only on the extreme ends of the data line if the RS485 network runs at high speed and the cable run is very long.

2-Wire

Figure C1 illustrates a typical 2-wire RS485 wiring configuration. The cable pair is shared for both transmit and receive data: it is very important that the Nano IP Series seize control of the line at the proper time when it is to transmit data.

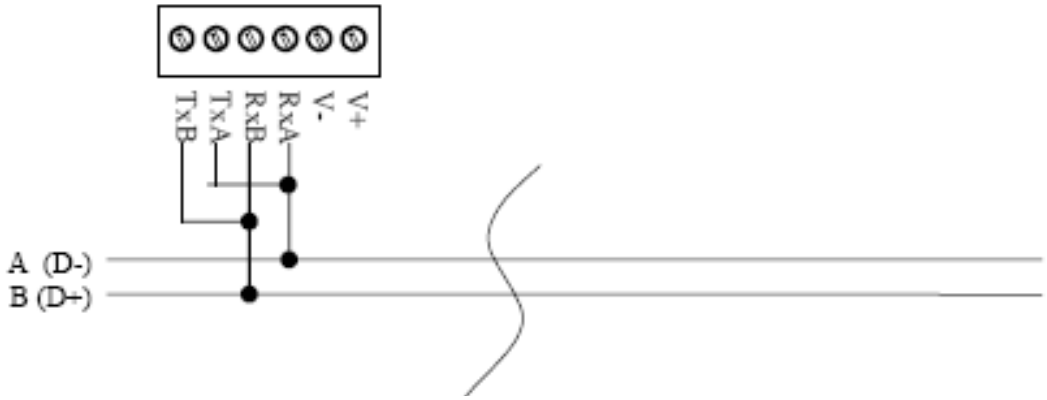


Figure C1: 2-Wire RS485 Wiring

4-Wire

In a 4-wire network, one node will be the master and all other nodes will be remotes. The master node may talk to all remote nodes, yet each remote may only communicate with the one master. Since the remote nodes never 'hear' each other, a remote node could not conceivably reply incorrectly to another remote's communication.

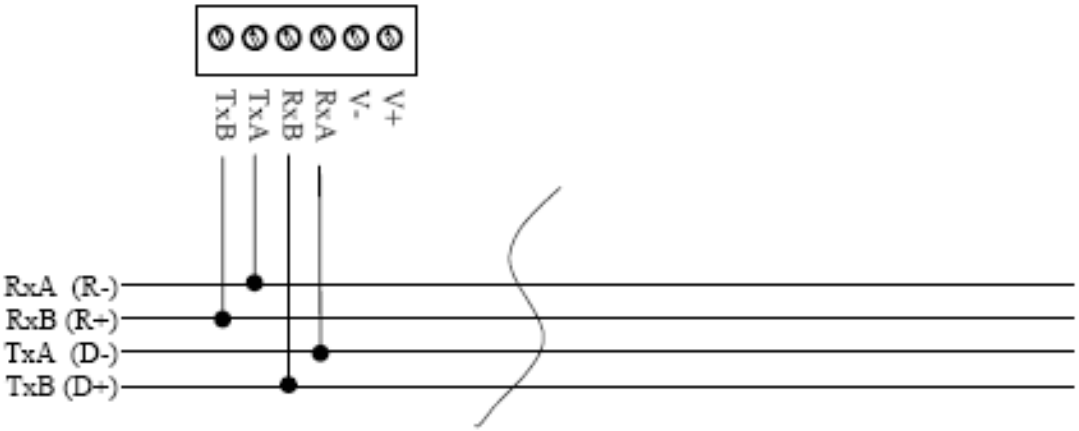


Figure C2: 4-Wire RS485 Wiring

Appendix D: Approved Antennas (900 MHz)

Nano 920 Series - 900 MHz Antennas

Group	Part Number	Description
Quarter Wave		
	MHS031010	<1.5dBi, 900MHz 1/4 Wave Antenna Reverse SMA Right Angle
	MHS031020	<1.5dBi, 900MHz 1/4 Wave Antenna Reverse SMA Straight
	MHS031030	<1.5dBi, 900MHz 1/4 Wave Antenna Reverse SMA Right Angle MHS
	MHS031040	<1.5dBi, 900MHz 1/4 Wave Antenna Reverse SMA Straight MHS
	MHS031050	<1.5dBi, 900MHz 1/4 Wave Antenna MCX Right Angle MHS
	MHS031060	<1.5dBi, 900MHz 1/4 Wave Antenna Reverse SMA Straight
Rubber Ducky		
	MHS031000	2dBi, 900MHz Rubber Ducky Antenna RPTNC Swivel
	MHS031070	2dBi, 900MHz Rubber Ducky Antenna Reverse SMA Swivel
	MHS031080	2dBi, 900MHz Rubber Ducky Antenna Reverse SMA Straight
Transit Antennas		
	MHS031210	3dBd, 900 MHz Transit Antenna with Ground Plane
	MHS031220	3dBd, 900MHz Transit Antenna No Ground Plane
	MHS031230	3dBd, 900MHz Transit Antenna Permanent Mount GP
	MHS031240	3dBd, 900MHz Transit Antenna Permanent Mount NGP
		Mounts for Transit Antennas have a RPTNC Pigtail
Yagi Antennas		
	MHS031311	6dBd, 900MHz Yagi Directional Antenna Antenex, RPTNC Pigtail
	MHS031431	6.5dBd, 900MHz Yagi Directional Antenna Bluewave, RPTNC Pigtail
	MHS031501	9dBd, 900MHz Yagi Directional Antenna Antenex, RPTNC Pigtail
	MHS031441	10dBd, 900 MHz Yagi Directional Antenna Bluewave, RPTNC Pigtail
	MHS031451	11dBd, 900 MHz Yagi Directional Antenna Bluewave, RPTNC Pigtail
	MHS031401	12dBd, 900MHz Yagi Directional Antenna Antenex, RPTNC Pigtail
	MHS031411	12dBd, 900MHz Yagi Directional Antenna Bluewave, RPTNC Pigtail
Omni Directional		
	MHS031251	3dBd, 900MHz Omni Directional Antenna Antenex, RPTNC Pigtail
	MHS031461	3dBd, 900 MHz Omni Directional Antenna Bluewave, RPTNC Pigtail
	MHS031321	6dBd, 900MHz Omni Directional Antenna Antenex, RPTNC Pigtail
	MHS031471	6dBd, 900 MHz Omni Directional Antenna Bluewave, 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 MCX and 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). Please Contact Microhard Systems Inc. if you need more information.

Appendix D: Approved Antennas (2.4 GHz)

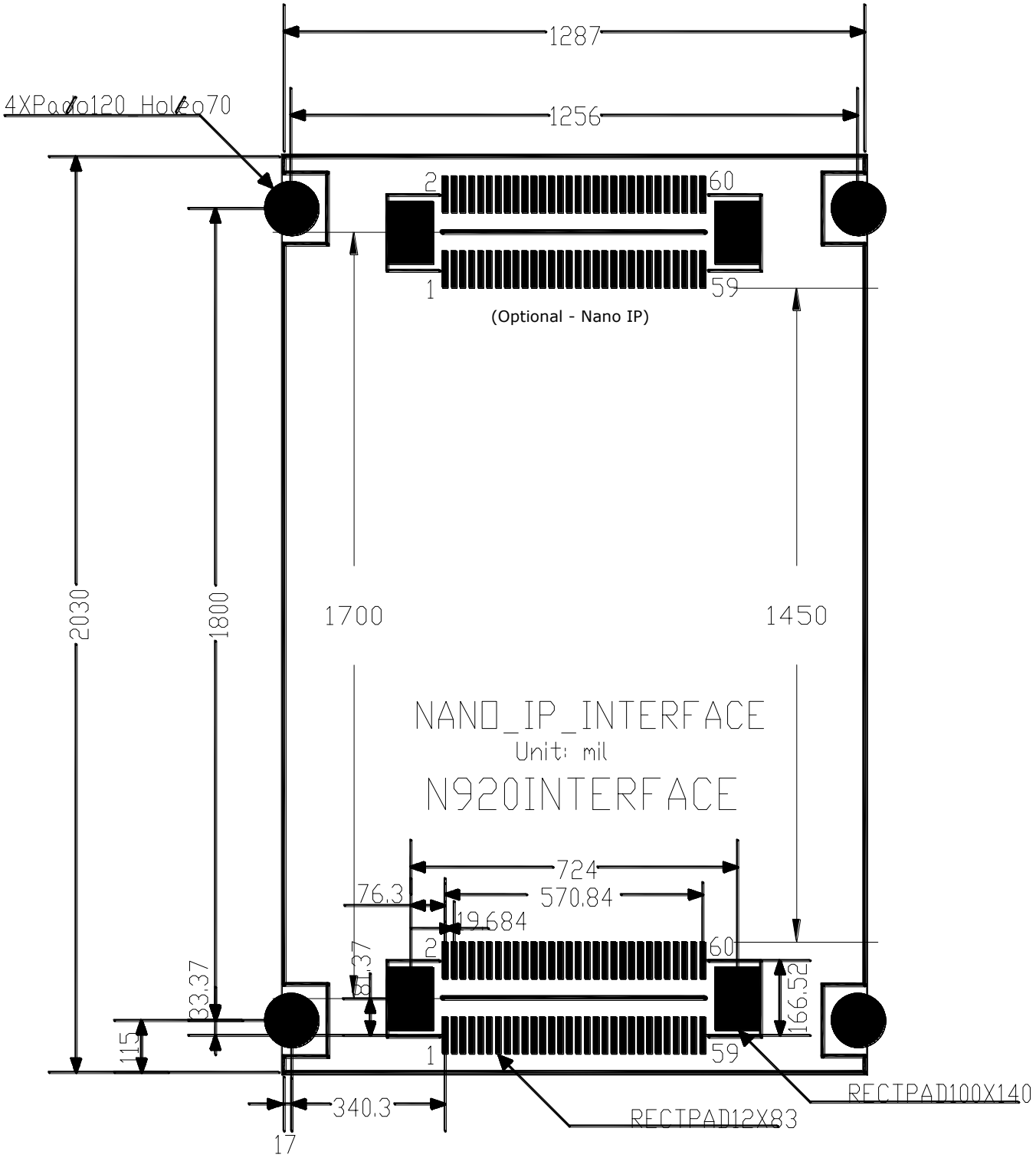
Nano 2420 Series - 2.4 GHz Antennas

Group	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
Patch Antennas		
	MHS034200	8dBi, 2.4GHz Mini Flat Patch Directional Antenna RPTNC Pigtail
	MHS034210	14dBi, 2.4GHz Flat Patch Directional Antenna RPTNC Pigtail
Yagi Antennas		
	MHS034100	9 dBi, 2.4GHz Yagi Directional RPTNC Pigtail
	MHS034110	12 dBi, 2.4GHz Yagi Directional RPTNC Pigtail
	MHS034120	14 dBi, 2.4GHz Yagi Directional RPTNC Pigtail
	MHS034150	14.5 dBi, 2.4GHz Yagi Directional RPTNC Pigtail
Omni Directional		
	MHS031260	5 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail
	MHS034000	6 dBi, 2.4GHz Omni Directional Antenna RPTNC Pigtail
	MHS031340	8 dBi, 2.4GHz 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 MCX and 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). Please Contact Microhard Systems Inc. if you need more information.

Appendix E: Nano IP OEM Layout



Appendix F: Serial Interface

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

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

The interface conforms to standard RS-232 signals without level shifting, so direct connection to a host microprocessor is possible.

The signals in the asynchronous serial interface are described below:

DCD *Data Carrier Detect* - Output from Module - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another MHX 920A.

RX *Receive Data* - Output from Module - Signals transferred from the MHX 920A are received by the DTE via RX.

TX *Transmit Data* - Input to Module - Signals are transmitted from the DTE via TX to the MHX 920A.

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

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

DSR *Data Set Ready* - Output from Module - Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the module's equivalent of the DTR signal.

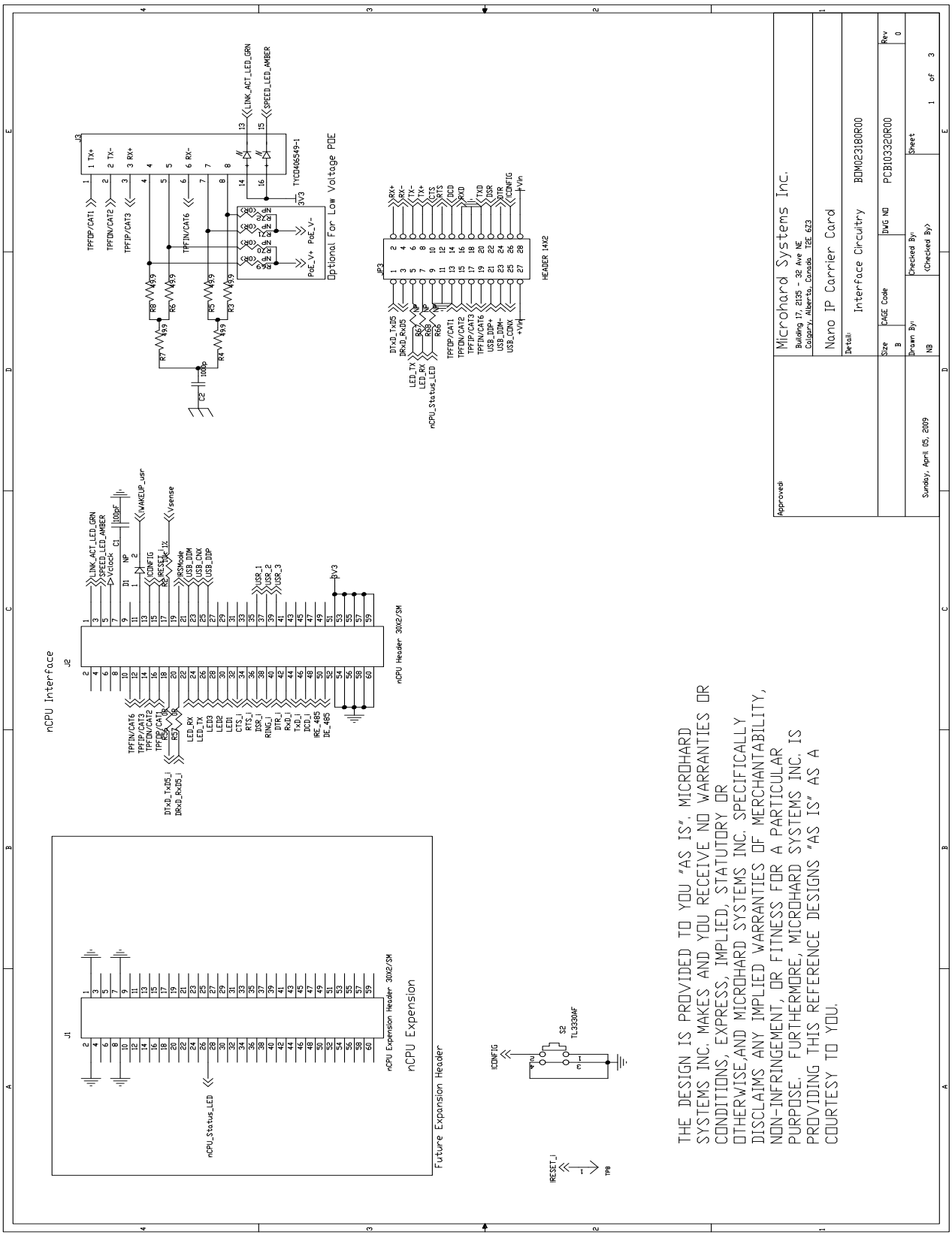
RTS *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

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

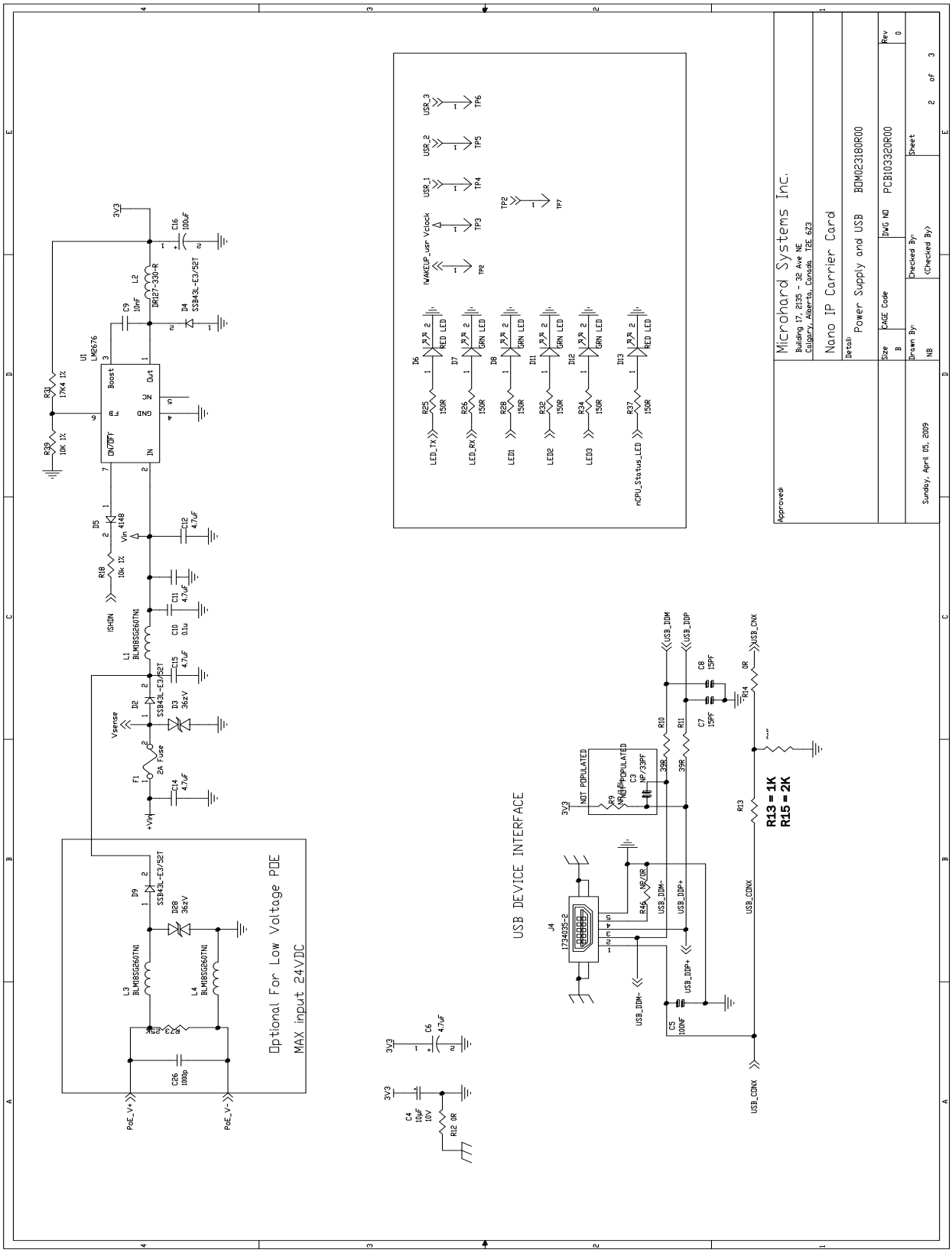
Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

"DCE" and "module" are often synonymous since a module is typically a DCE device.
"DTE" is, in most applications, a device such as a host microprocessor.

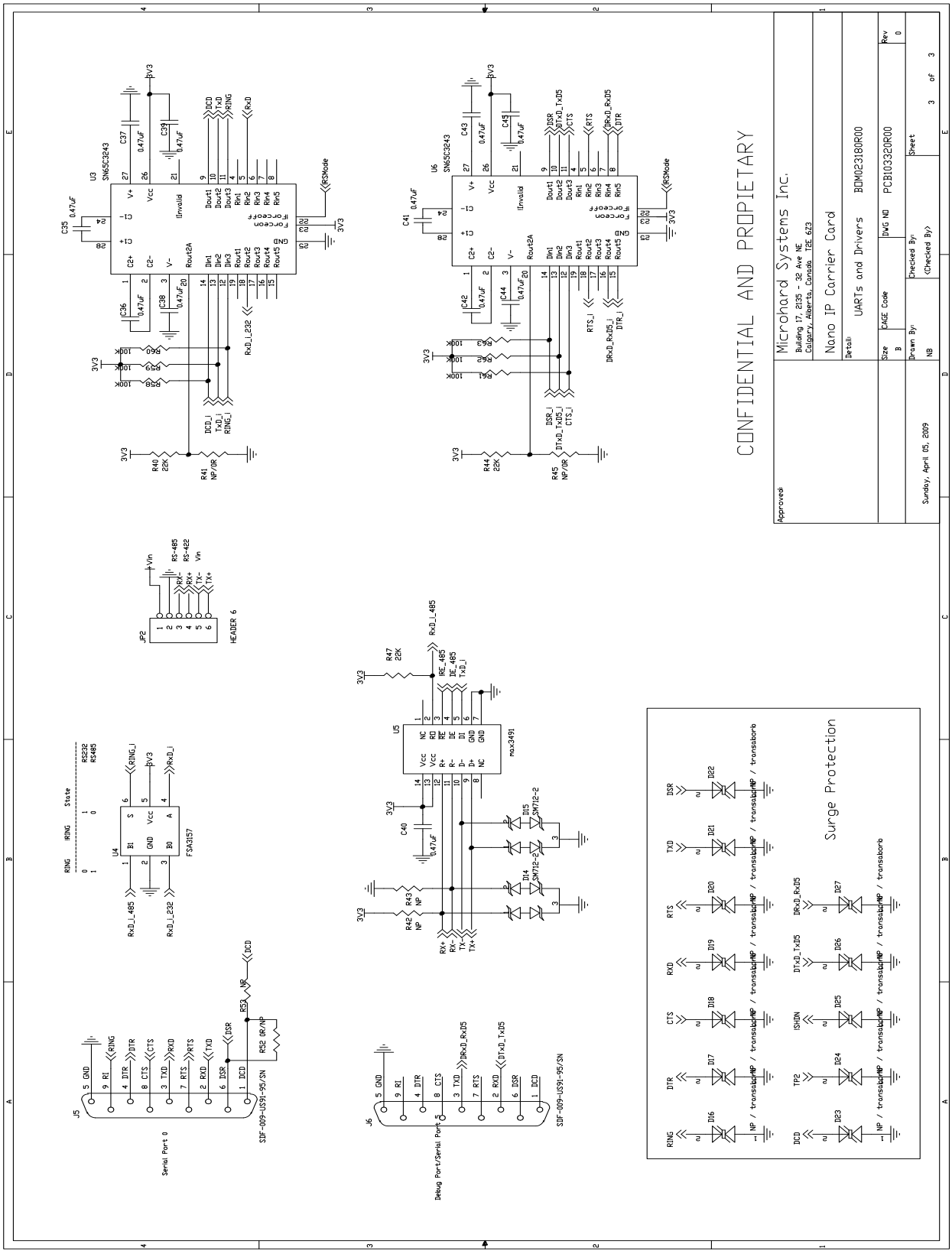
Appendix G: Nano IP Motherboard Schematic (Page 1 of 3)



Appendix G: Nano IP Motherboard Schematic (Page 2 of 3)



Appendix G: Nano IP Motherboard Schematic (Page 3 of 3)



microhard SYSTEMS INC.

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

Phone: (403) 248-0028
Fax: (403) 248-2762