Operating Manual

IP9xx Series
900MHz Wireless Ethernet Bridge/Serial Gateway
Document: IP9xx Series.OM.F200.Rev3.3

September 2010

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.

WARNING

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:

For IP921/SIP921 OEM Series
921 Series

FCCID: NS906P21
IC: 3143A-06P21

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 IP920A OEM Series, IP920LC
920 Series

FCCID: NS905P20
IC: 3143A-05P20

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 3.3 September 2010

Added VLAN Information, misc formatting and updates.

Revision 3.2 April 22, 2008

Added SIP921 Section

Revision 3.1 December 01, 2007

Based on: Ref. 6.1.2 FPGA Version 1R4, Software Version 2.0.0; Ref. 6.1.8/Radio Info. Version 3.1092ip
Updated formatting, added Appendix C.

Revision 3.0 May 07, 2007

Based on: Ref. 6.1.2 FPGA Version 1R4, Software Version 2.0.0; Ref. 6.1.8/Radio Info. Version 3.1092ip

Revision 2.0 November 20, 2006

Based on: Ref. 6.1.2 FPGA Version 1R4, Software Version 1.3.4; Ref. 6.1.8/Radio Info. Version 3.1082ip

Table of Contents

continued...

Table of Contents (continued)

Table of Contents (continued)

Appendices

1.0 Overview

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

A ROUTER forwards data across internetworks (different subnets).

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.

The IP Series is a high-performance wireless ethernet bridge and serial gateway. Alternately, a Master 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 IP Series operates within the 902-928MHz ISM frequency band, employing frequency hopping spread spectrum (FHSS) and also, for 1.1Mbps operation, digital transmission service (DTS) technology.

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.

The small size and superior performance of the IP Series makes it

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

ideal for many applications. Some typical uses for this modem:

1.1 Performance Features

- 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

Key performance features of the IP Series include:

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

1.0 Overview

1.2 Specifications

Refer to the Specifications Sheet supplied to you for your particular model.

1.0 Overview

- 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
- 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 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.

2.0 Quick Start

This QUICK START guide will enable you to promptly establish basic IP connectivity between a pair of 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 IP Series (with (or set to) factory default configura tion), each with Power Adapter and Rubber Ducky Antenna
- 1 PC with NIC (ethernet) card
- 1 Crossover patchcable (ethernet)*

*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 IP Series.
- Connect the Power Adapters to available 120VAC outlets, and to the IP Series. The SYS LED will blink for approximately 1 minute while it readies itself for operation.

To ensure that the 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.

- Using CROSSOVER ethernet patchcable, connect PC NIC card to rear ETHERNET connection on 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 IP Series into the URL address line.
- Refer to Section 6.1.1 re LogOn.

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 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 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 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 Crossover patchcable (ethernet)*
- 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 IP Series.
- Connect the Power Adapters to available 120VAC outlets, and to the IP Series.

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

- Connect the MHS Diagnostic Cable to COM2 (front) of one IP Series and the other end to an available COM port on the PC.
- 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

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

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

Remove the connection from the MASTER IP Series's COM2 port and move it to the other 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 IP Series configured above is now the REMOTE IP Series for your Point-to-Point IP Series network.

With these two 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

To connect an IP Series to a PC, an ethernet CROSSOVER (not a straight-through) cable must be used.

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 patchcable into the rear ETHERNET RJ45 connector at the rear of the MASTER IP Series.
- Using a CROSSOVER cable, connect the PC's NIC card RJ45 jack to the ETHERNET RJ45 connector on the REMOTE 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 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 IP Series are illuminated.
- Verify TX (red) LED activity on the front of each IP Series.
- Observe the rear of each 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 Features

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

Any IP Series 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 device: if you are familiar with one unit, you will be familiar with all units.

3.1 IP9xx Connections

3.1.1 Front

Image 3A: Front View of IP Series

On the front of the IP Series are, from left to right:

- COM2 Port (DCE)
- CFG pushbutton
- TX LED
- RX LED
- SYS LED
- RSSI LEDs (3)

3.0 Hardware Features

The **COM2** Port (DCE) is used for two purposes:

- Text User Interface (local console port) at 115.2kbps (using MHS-supplied BLACK RJ45-DE9 cable (P/N MHS044000) and HyperTerminal (or equivalent).
- User data (serial, RS-232, wired for RxD, TxD, and SG)

The COM2 port is NOT an Ethernet port.

DO NOT connect to COM2 pins other than those identified in Table 3A, and for their described function.

Pin Name	No.	Description	In/ Out
RxD	2	Receive Data	O
TxD	3	Transmit Data	I
SG	5	Signal Ground	

Table 3A: COM2 Pin Description

The CFG button (and 'default' IP address 192.168.1.39) are ONLY used for the purpose of upgrading firmware.

The 'default' IP address is NOT available for accessing the Web User Interface.

CFG Button

Holding this button depressed while powering-up the 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.

(For more information on performing a firmware upgrade, see Appendix B and Section 6.1.9.1.)

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.

3.0 Hardware Features

3.1.2 Rear

COM1 Port (DCE) on the rear of the IP Series is used for RS232 serial data (300 baud to 230.4kbps) communications.

RS422/485 Port used to interface the IP Series to a DTE with the same interface type (300 baud to 921kbps).

Either the RS232 or RS422/485 interface is used for 'COM1' data traffic.

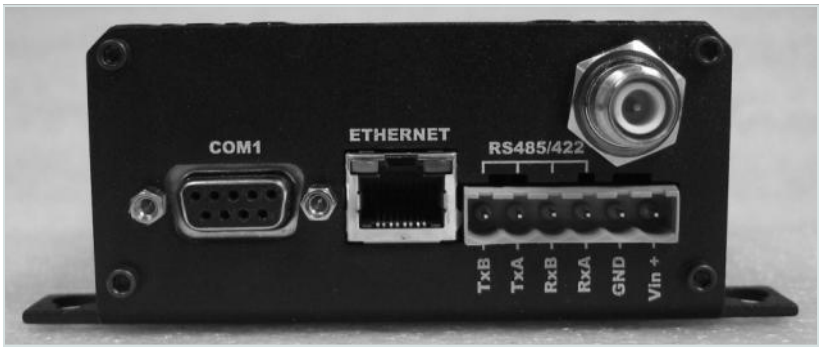
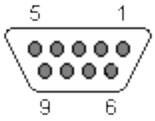


Image 3B: Rear View of IP Series



See Appendix F for a full description of the COM1 RS-232 interface functions.

Pin Name	No.	Description	In/ Out
DCD	1	Data Carrier Detect	O
RXD	2	Receive Data	O
TXD	3	Transmit Data	I
DTR	4	Data Terminal Ready	I
SG	5	Signal Ground	
DSR	6	Data Set Ready	O
RTS	7	Request To Send	I
CTS	8	Clear To Send	O

Table 3B: COM1 (RS-232) Pin Assignment

3.0 Hardware Features

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

Caution: DO NOT connect POWER to the DATA SIGNAL pins of the Phoenix-type connector.

Pin Name	No.	Description	In/ Out
TxB (D+)	1	Non-Inverting Driver Output	O
TxA (D-)	2	Inverting Driver Output	O
RxB (R+)	3	Non-Inverting Driver Input	I
RxA (R-)	4	Inverting Driver Input	I
GND	5	Ground (Power and Signal)	
Vin+	6	Positive Voltage Supply Input (12-30VDC)	I

Table 3C: Phoenix-type Connector Pin Assignment

Antenna Connector

The IP Series uses a reverse polarity TNC (RP-TNC) connector. Microhard Systems Inc. can provide external cabling and antennas suited to a variety of applications where the standard rubber ducky antenna is not adequate.

Refer to Appendix D for a listing of approved antennas.

3.0 Hardware Features

3.2 IP9xx Indicators

3.2.1 Front Indicators

Alarm LED (Amber)

Located at top/left of COM2 port, illuminates when there is a load/ transmitter impedance mismatch—indicating a possible problem in the antenna system.

MHX Status LED (Green)

Located at top/right of COM2 port, illuminates when the MHX core module is powered-up and okay.

TX LED

The transmit (TX) LED is illuminated when the IP Series is transmitting data wirelessly.

RX LED

This LED, when illuminated, indicates that the modem is synchronized and/or receiving valid packets of data.

SYS LED

The System Status LED operation is described in the following table:

System Mode	SYS LED Status
Normal	On
Recovery	Fast Blink (3 per second)
Loading (e.g. on normal power-up)	Slow Blink (1 every 2 seconds)
Upgrading	Slow Blink (1 every 2 seconds)

Table 3D: SYS LED Operation

DO NOT cycle power during the 'Upgrading' process: doing so will corrupt the flash file system and the IP Series will not boot properly. If this occurs, the system can only be restored using the recovery procedure.

Upon initial application of power the SYS 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 Features

Receive Signal Strength Indicator (RSSI) (3x Green) LEDs

As the received signal strength increases, so does the number of illuminated RSSI LEDs, starting with the furthest left. RSSI is calculated based on the last four valid recieved packets. For robust wireless communications performance, strive for a minimum of 2 RSSI LEDs being lit.

Initially, a remote unit's RSSI LED's will 'scan' (cycle from right to left, each LED being on for 300ms in turn). Once the unit acquires synchronization with the network, a 'steady' RSSI reading will be displayed.

A Master updates its RSSI indication upon receiving valid packets from remote units. It takes into consideration packets received from both Repeaters and Remotes.

A Repeater will base its RSSI reading on valid packets received from Slaves; if the Slaves are silent for 2 seconds, the Repeater will display an RSSI value based on valid packets received from the Master.

Signal strength is calculated based on the last four valid received packets with correct CRC.

When initially cabling between devices, pay close attention to the Activity LED to confirm that proper patchcable types are being used.

3.2.2 Rear Indicators

Collision LED (Amber)

Located at top/left of the ETHERNET connector, illuminates when there is a collision on the ethernet interface.

Activity LED (Green)

Located at top/right of the ETHERNET connector, illuminates when there is data activity present on the ethernet interface.

3.0 Hardware Features

3.3 SIP921 Connections

The SIP921 introduces a small form factor and single header interface for complete integration into OEM applications. The SIP921 incorporates all of the IP9xx functionality, features, configuration and performance into a single module.

Image 3C: Bottom View of SIP921 Module

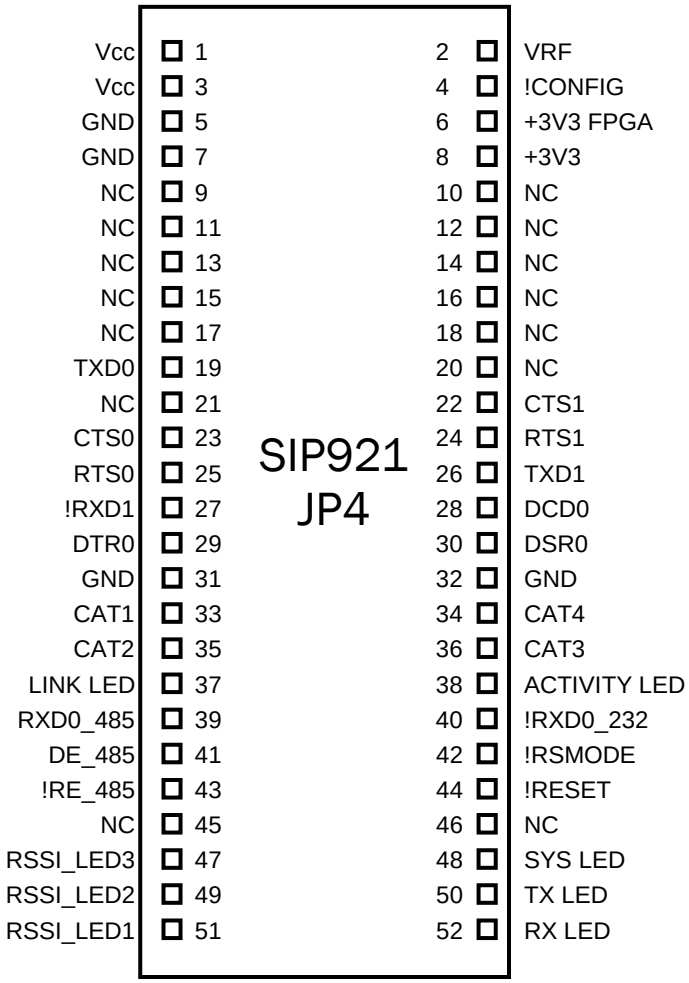
The SIP Series OEM module features include:

- Single OEM header.
- Ready-to-wire Ethernet.
- Dedicated diagnostics serial port (TTL).
- TTL Level Data Port fully equipped with the signals necessary to derive RS232/485/422 interfaces.
- Status/Diagnostic output signals for system status, RSSI, Ethernet etc.

The Pin-out and signal descriptions are described on the following pages. An example customer interface schematic can be found in Appendix G.

3.0 Hardware Features

3.3.1 SIP921 Pin-Out Description



Drawing 1: SIP921 52-pin OEM Connector Pin-out

Pins 9-18 are reserved for factory use. Do not use these pins for any other purpose.

Inputs and outputs are TTL Level unless otherwise specified.

The above drawing depicts a bottom view of the SIP921 connector. The corner pins (1, 2, 51, and 52) 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.

3.0 Hardware Features

Pin Name	No.	Description	In/ Out
Vcc	1,3	Positive supply voltage for the module (9-30 VDC)	I
VRF	2	Voltage Output (4.5VDC)	O
!CONFIG	4	Active low input signal to put the module into FLASH FILE SYSTEM RECOVERY mode.	I
GND	5,7	Ground reference for logic, radio and I/O pins.	
+3V3 FPGA	6	Voltage Output ON during sleep mode. (3.3VDC)	O
+3V3	8	Voltage Output OFF during sleep mode. (3.3VDC)	O
NC	9-18	*Reserved for factory use.*	
TXD0	19	Data Port. Transmit Data. Logic Level Output from the modem.	O
NC	20-21	*Reserved for future use.*	
CTS1	22	Diagnostics Port. Clear To Send. Active low output.	O
CTS0	23	Data Port. Clear To Send. Active low output.	O
RTS1	24	Diagnostics Port. Request To Send. Active low input.	I
RTS0	25	Data Port. Request To Send. Active low input.	I
TXD1	26	Diagnostics Port. Transmit Data. Logic level output from modem.	O
RXD1	27	Diagnostics Port. Receive Data. Logic level input into the modem.	I
DCD0	28	Data Port. Data Carrier Detect. Active low output.	O
DTR0	29	Data Port. Data Terminal Ready. Active low input.	I
DSR0	30	Data Port. Data Set Ready. Active low output.	O
GND	31-32	Ground reference for logic, radio, and I/O pins	

Table 3E: SIP921 Pin-Out Description

3.0 Hardware Features

Pin Name	No.	Description	In/ Out
CAT1	33	Ethernet RJ45 Pin 1.	
CAT4	34	Ethernet RJ45 Pin 4.	
CAT2	35	Ethernet RJ45 Pin 2.	
CAT3	36	Ethernet RJ45 Pin 3.	
LINK LED	37	Ethernet LINK LED	O
ACTIVITY LED	38	Ethernet Activity LED	O
RXD0_485	39	Data Port. RS485 Receive Data Logic level input into the modem.	I
RXD0_232	40	Data Port. RS232 Receive Data Logic level input into the modem.	I
DE_485	41	Date Port. RS485 Driver Output Enable. Avtive High Output.	O
!RSMODE	42	Sleep mode indication output. Active Low.	O
!RE_485	43	Data Port. RS485 Receiver Output Enable. Active low output.	O
!RESET	44	Active low input will reset module	I
NC	45-46	*Reserved for future use.*	
RSSI_LED3	47	Receive Signal Strength Indicator 3.	O
RSSI_LED2	49	Receive Signal Strength Indicator 2.	O
RSSI_LED1	51	Receive Signal Strength Indicator 1.	O
SYS LED	48	This output indicates system status. Normal Operation = Solid, Recovery = Fast Blink (3/s), Loading/Upgrading = Slow Blink (1 every 2s)	O
TX LED	50	Output indicates module is transmitting data over the RF channel.	O
RX LED	52	Output indicates receive and synchronization status.	O

Table 3E: SIP921 Pin-Out Description (continued)

4.0 Operating Modes

An 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 IP Series at the Repeater site in a 'back-to-back' configuration. One 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 IP Series configuration.

Throughout this manual, '**R**emote' refers to a **R**emote as defined in Section 4.4; the general term '**r**emote' applies to an IP Series Repeater and/or Remote - i.e. non-Master

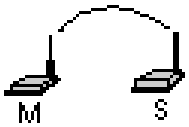
4.3 Remote

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.

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

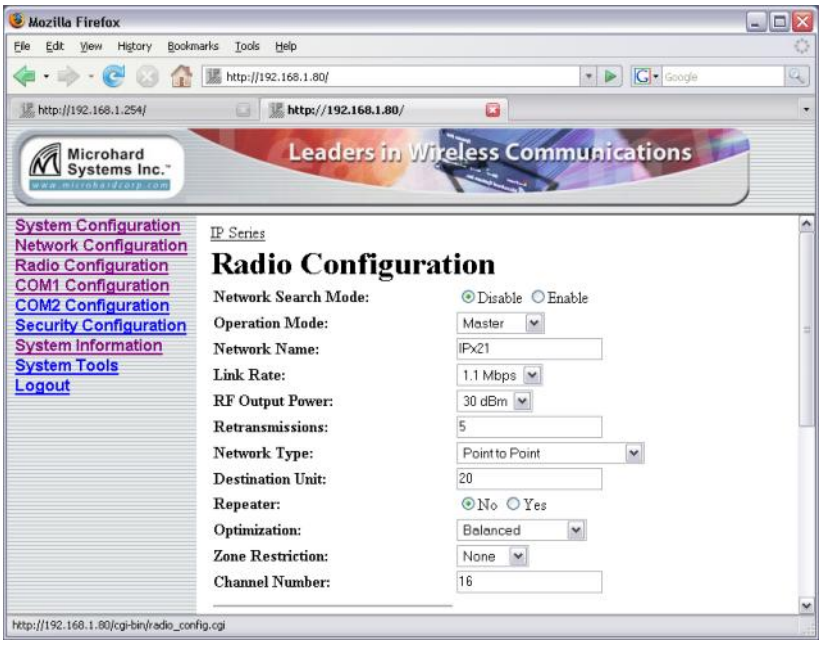


Image 5A: PTP Example 5.1.1: Master

Example 5.1.1

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.

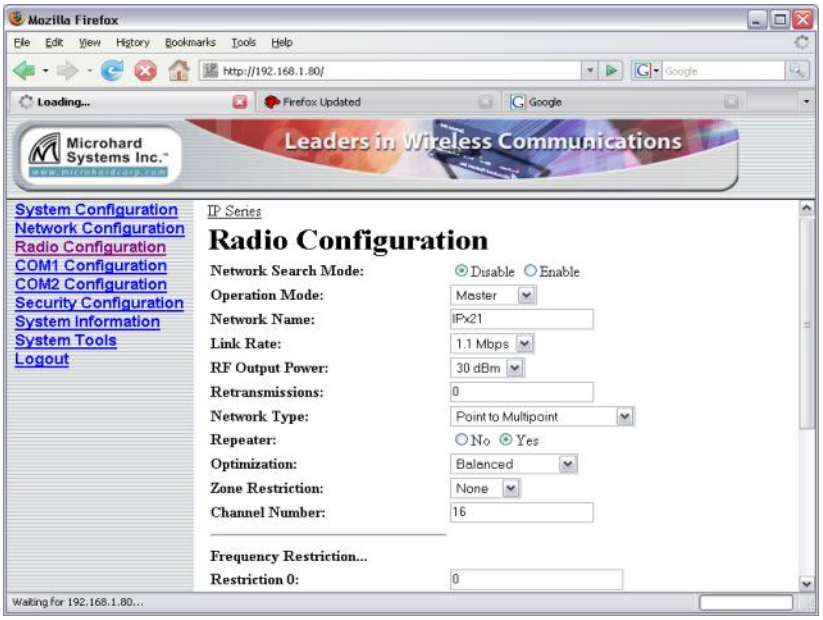


Image 5C: PMP Example 5.2.1: Master

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)

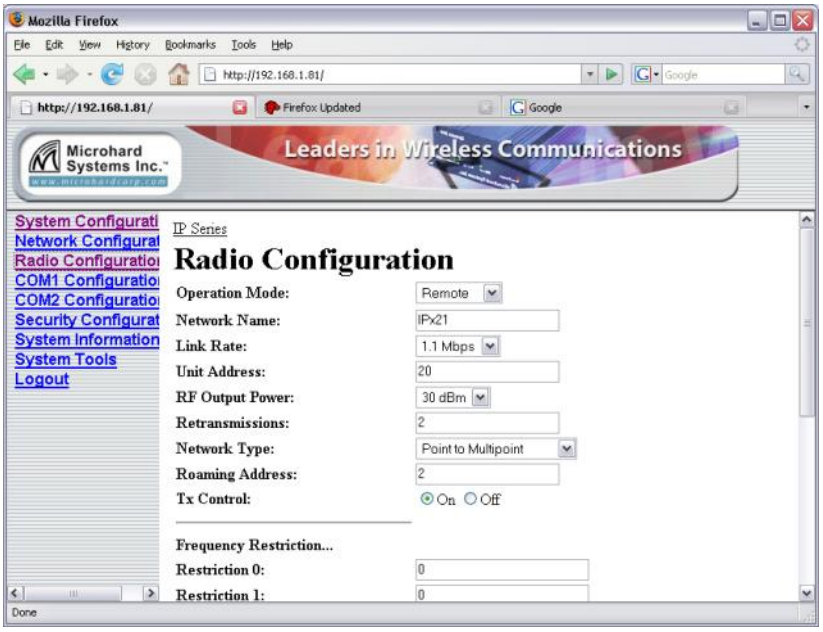


Image 5E: PMP Example 5.2.1: Remote 20

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

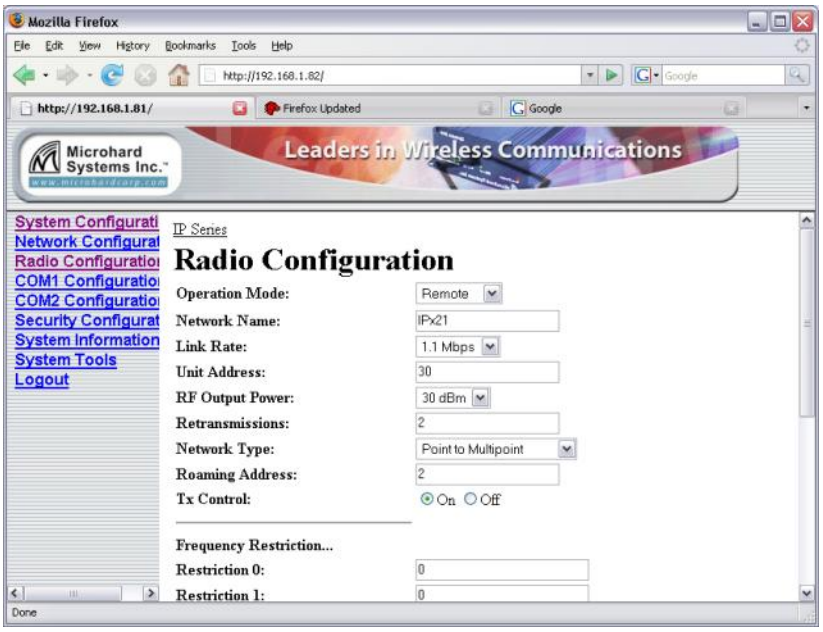


Image 5F: PMP Example 5.2.1: Remote 30

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 IP Series must reside in an office at a separate location.

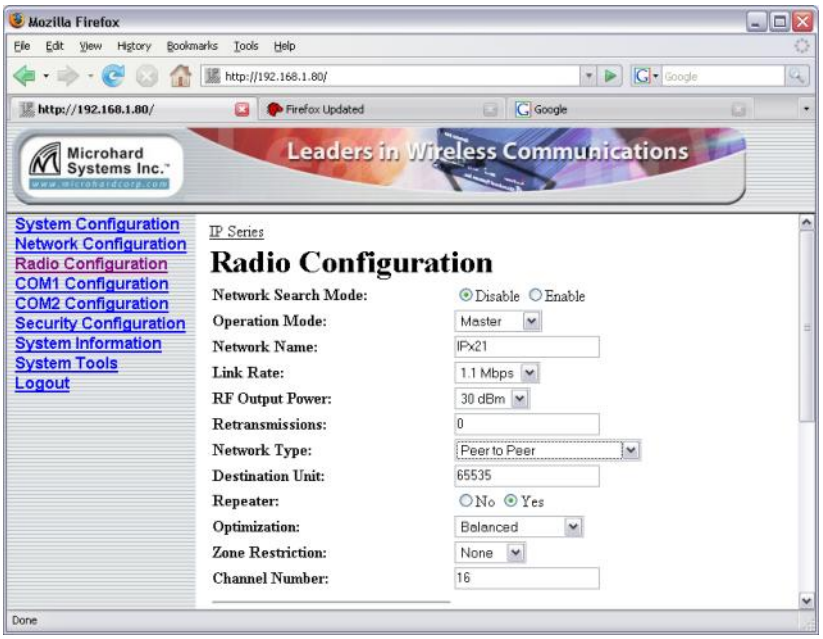


Image 5G: P2P Example 5.3.1: Master

All 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)

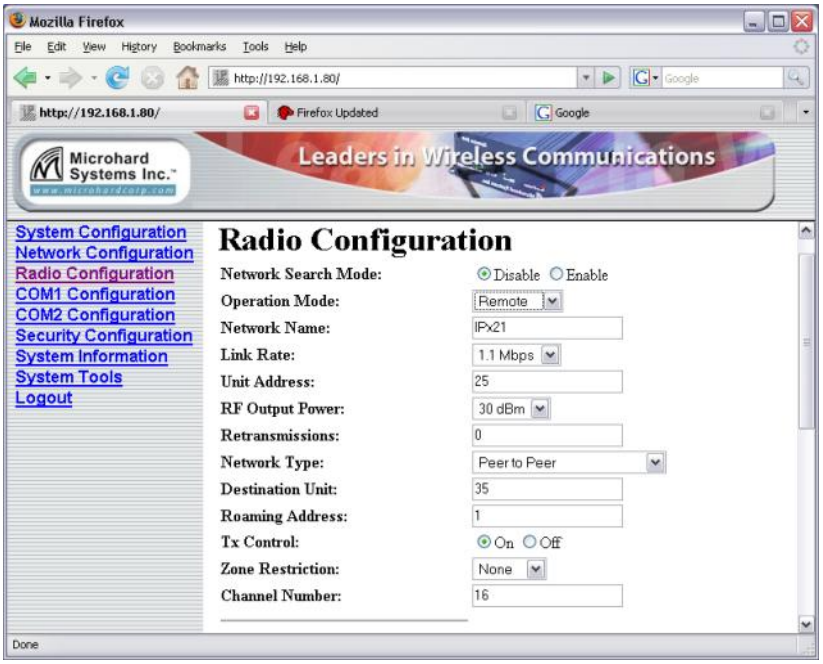


Image 5H: P2P Example 5.3.1: Remote 25

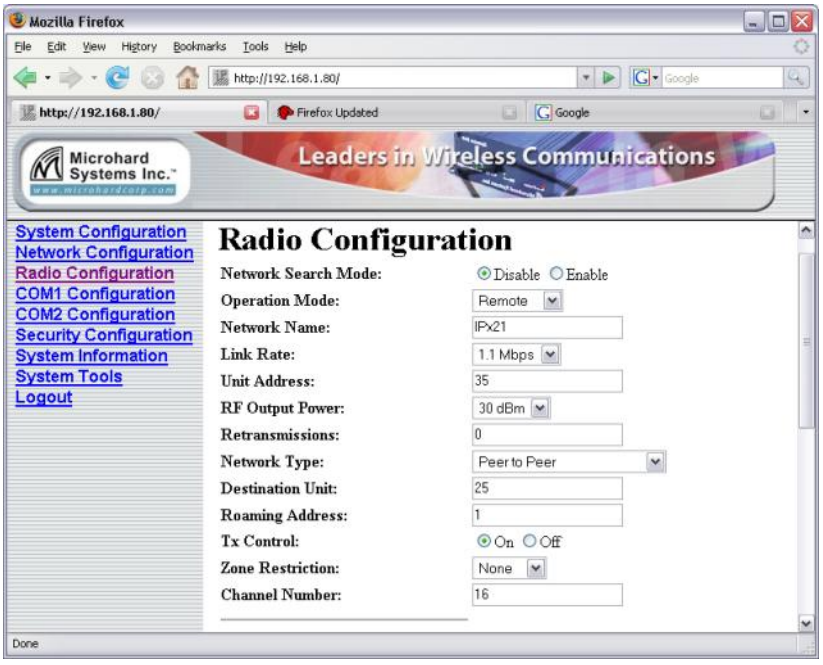


Image 5I: P2P Example 5.3.1: Remote 35

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.

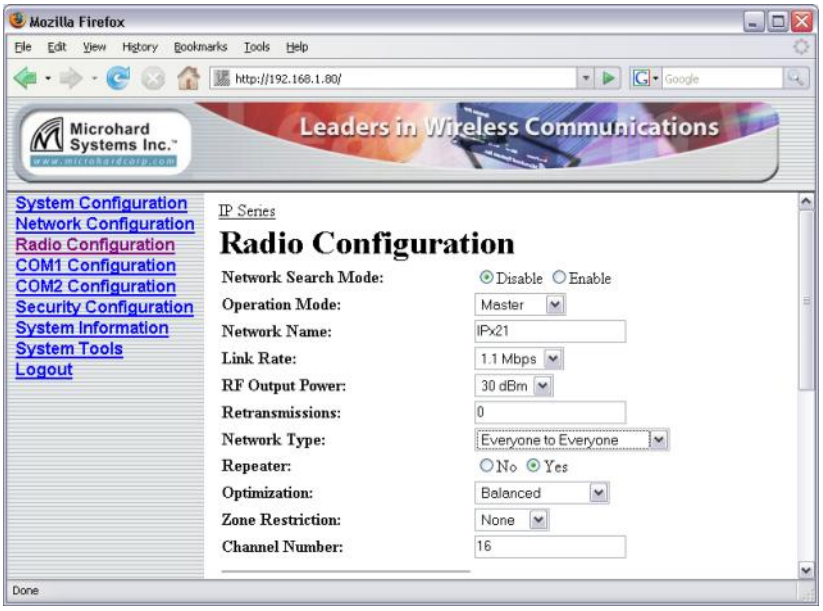


Image 5J: E2E Example 5.4.1: Master

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

5.0 Network Topologies

Example 5.4.1 (continued)

Each unit must have its own unique Unit Address.

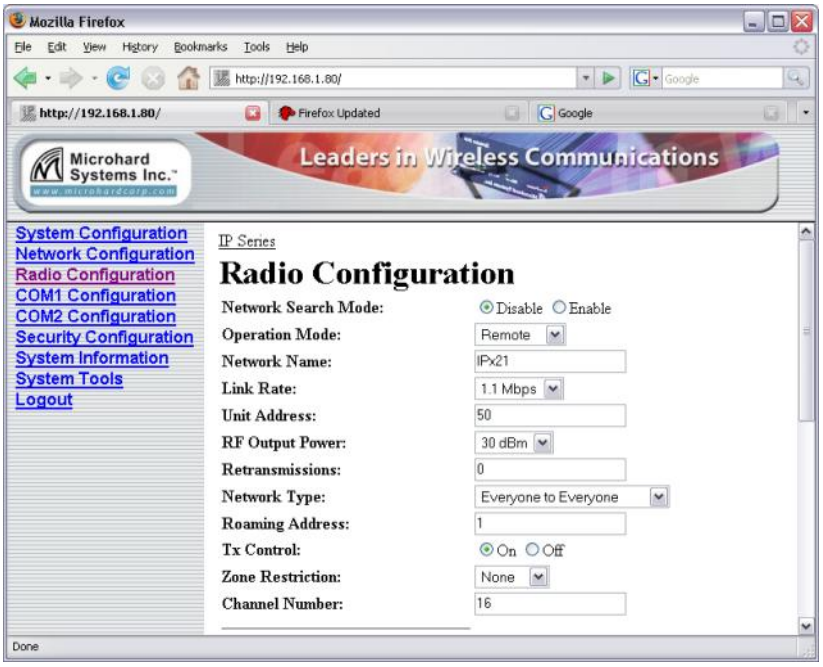


Image 5K: E2E Example 5.4.1: Remote

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.

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, Microhard Systems Inc. DE9-RJ45 Diagnostics Cable (P/N MHS044000, black), and a PC running terminal communications program (e.g. HyperTerminal), 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

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.

6.1 Web User Interface

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

- connect IP Series ETHERNET port to PC NIC card using an ethernet **crossover** cable
- apply power to the IP Series and wait approximately 1 minute for the system to load
- run Microhard Systems Inc. DiscoverIP Utility on the PC (see Appendix A for complete details on this convenient utility)
- within the DiscoverIP Utility window, click on the desired unit's IP address (verify displayed MAC address with MAC address printed on sticker on bottom of unit)
-
- logon window appears; log on
- configure IP Series as desired.

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 IP Series using a Web Browser, the Logon window will appear.

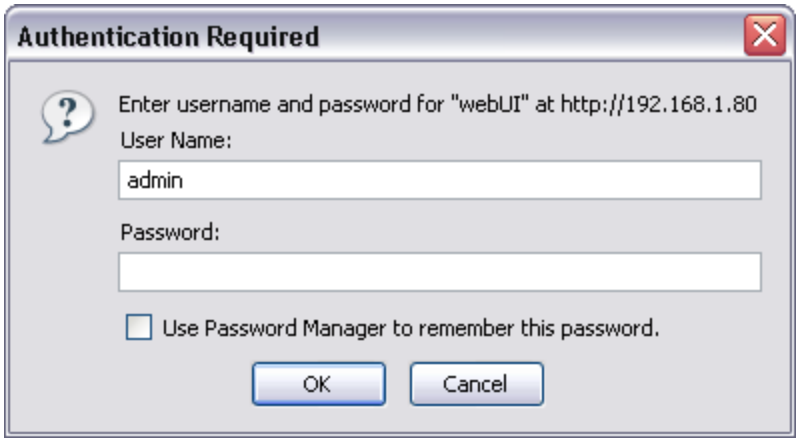


Image 6A: Logon Window

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.

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.

6.0 Configuration

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

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

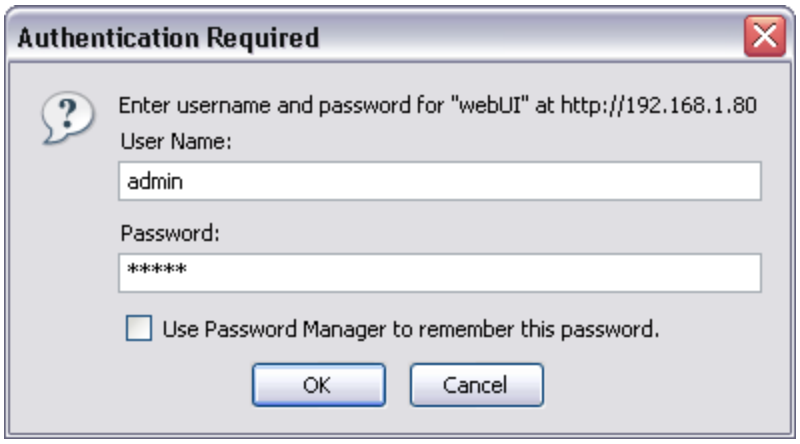


Image 6B: Logon Window With Password Input

Soft Buttons

- OK
  Inputs the selected values into the IP Series for processing.

- Cancel
  Cancels the logon process.

6.0 Configuration

6.1.2 Welcome Window

The Welcome window displays the specific 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.

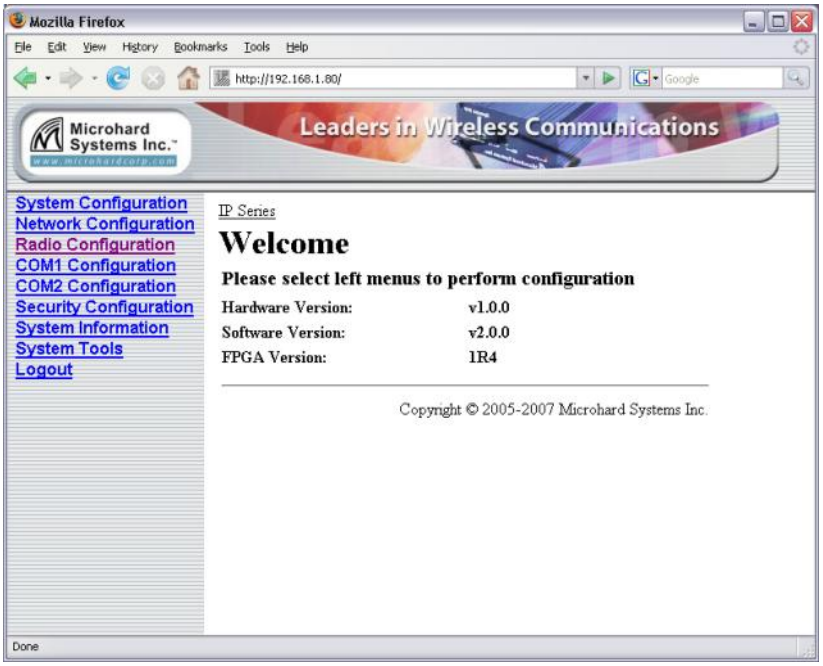


Image 6C: Welcome Window

Also displayed is various 'version' information:

- Hardware Version - applicable to the motherboard of the IP Series
- Software Version - this software resides on the motherboard and is also referred to as the unit's 'firmware'
- FPGA Version - Field Programmable Gate Array - resides on the motherboard and relates to the interface between the motherboard and radio module

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.

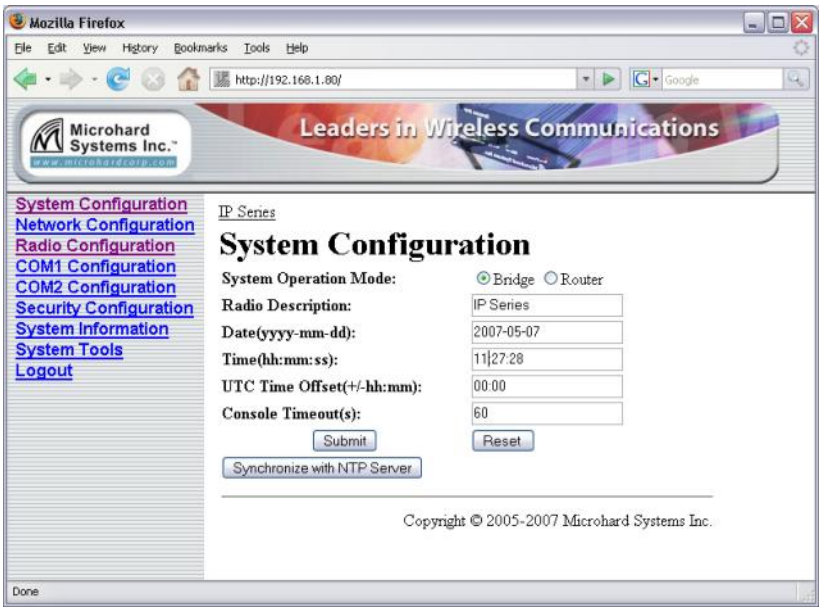


Image 6D: System Configuration Window

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.

Select the System Operation Mode 'first', i.e. prior to configuring other options within the unit.

Values
Bridge
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 IP Series network.

Radio Description

The Radio Description is simply a convenient identifier for a specific 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 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 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

6.0 Configuration

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

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 IP Series memory.

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

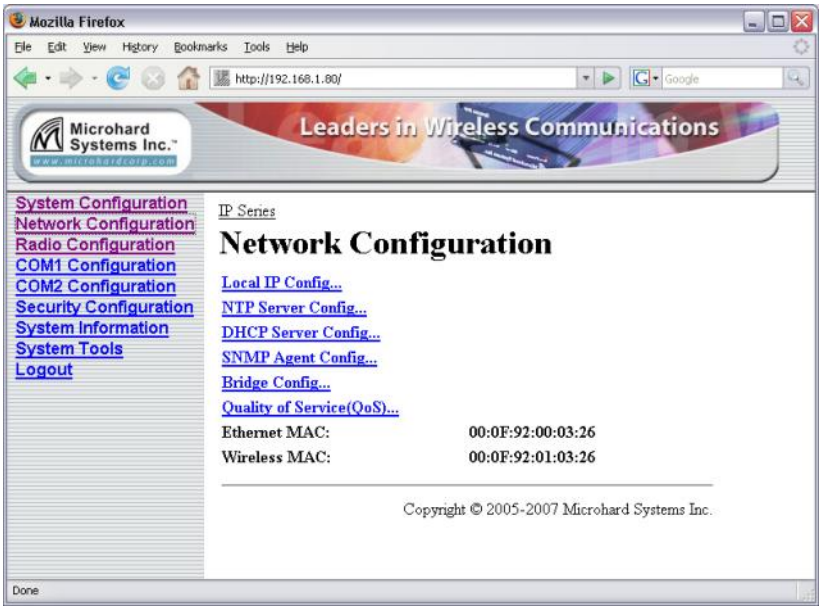


Image 6E: Network Configuration, Top Level Menu

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

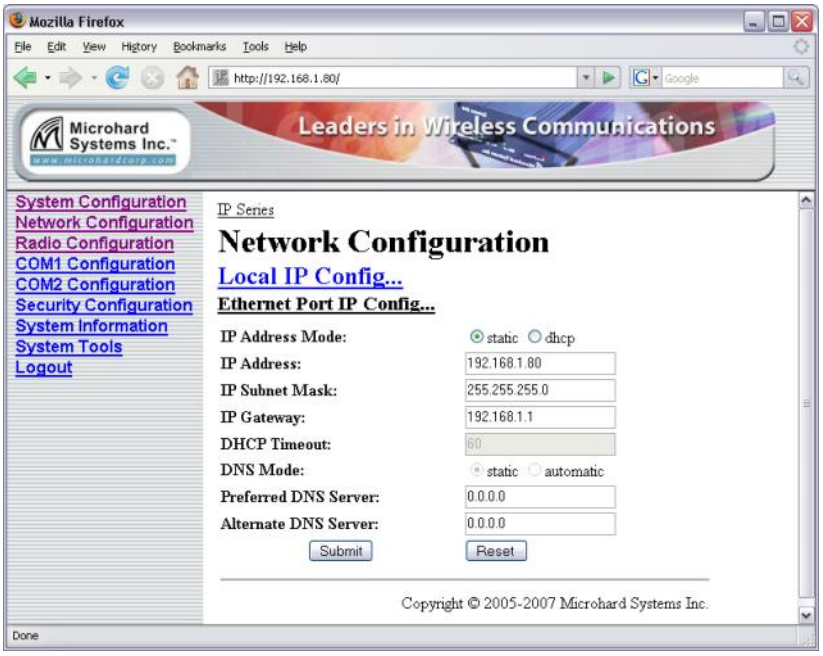


Image 6F: Network Configuration (Bridge), Local IP Configuration Submenu

IP Address Mode

If 'static' is selected, the three following fields (see Image 6F) are to be manually populated with values which will suit the network/ devices to which the IP Series is connected.

continued...

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 (continued)

If 'DHCP' is selected, the three following fields (see Image 6F) will be automatically populated by the DHCP server. The DHCP Timeout value may be manually modified from the factory default value.
Note that the factory default setting is DHCP.

Values

dhcp

static
dhcp

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

IP Address

If DHCP is selected (see above), a unique IP address will be assigned to the 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

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.

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.

If DHCP mode is selected (see above/top), the DHCP server will populate this field.

Values

255.255.255.0

valid value is specific to the network

6.0 Configuration

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

In typical networks, a router acts as a gateway.

IP Gateway

If the IP Series devices 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 (see previous page) 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 IP Series's 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

DHCP Timeout

This value determines for how long the 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

6.0 Configuration

DNS Mode

The setting determines whether the IP Series unit 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 IP Series memory.
- Reset
  Restore 'currently' modified parameter values to those which were previously written into IP Series memory.

6.0 Configuration

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

6.1.4.1 Local IP Configuration

6.1.4.1.2 Router

If the 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.

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 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

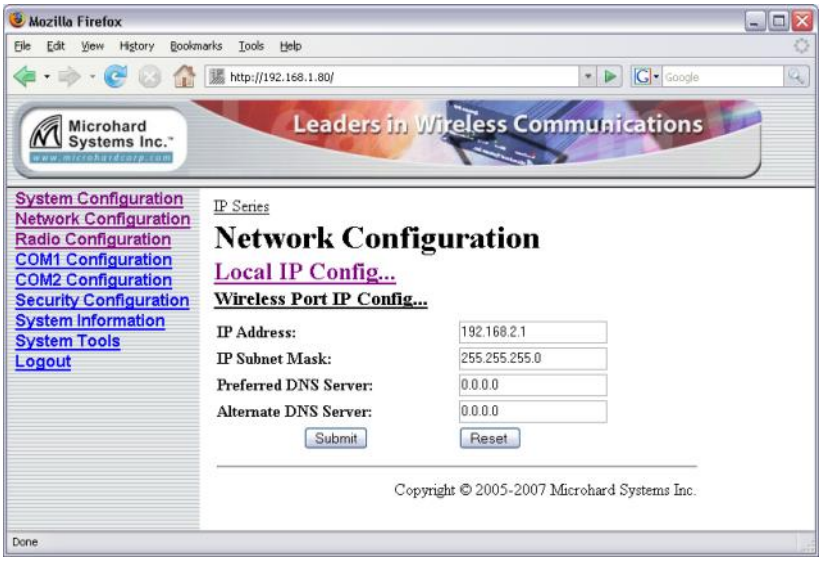


Image 6H: Network Configuration (Router), Wireless Port IP Configuration Submenu

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 address

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 address

Soft Buttons

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

6.0 Configuration

6.1.4.1.2.2 VPN Configuration

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

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

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 Status

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

Values

Enable

Enable
Disable

VPN Admin Password

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

Values

admin

32 characters maximum

6.0 Configuration

VPN Admin Repeat Password

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

Values

admin

32 characters maximum

Soft Buttons

- Submit
  Write parameter values into IP Series memory.
- Reset
  Restore ‘currently’ modified parameter values to those which were previously written into IP Series memory.

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 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

Disable
Enable

6.0 Configuration

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'

Soft Buttons

- Submit
  Write parameter values into IP Series memory.

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

6.0 Configuration

6.1.4.3 DHCP Server Configuration

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

6.1.4.3.1 Bridge

The 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 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 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 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 IP Series or other IP-based device attached to the LAN).

6.0 Configuration

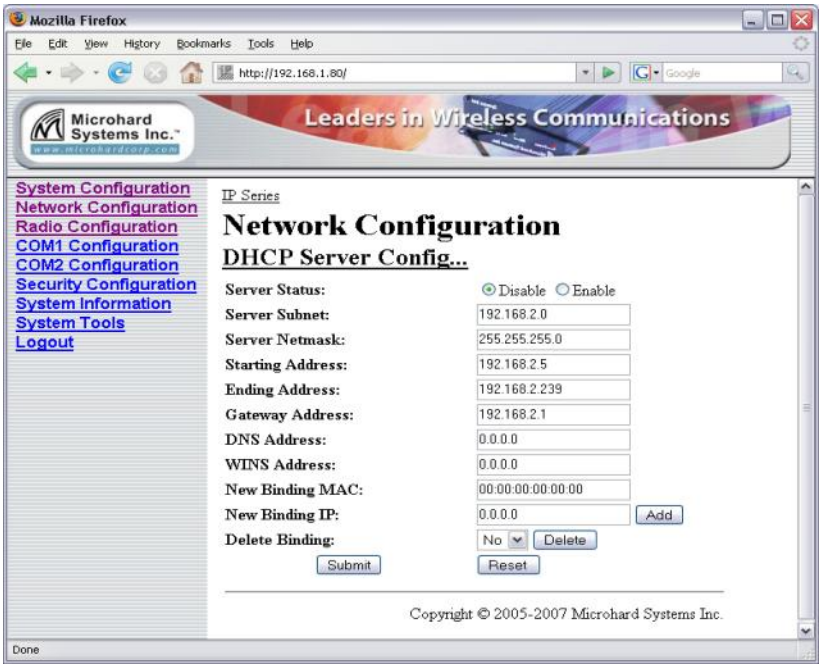


Image 6J: Network Configuration, DHCP Server Config. Submenu

Prior to enabling this service, verify that there are no other devices - either wired (e.g. LAN) or wireless (e.g. another IP Series) 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

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

6.0 Configuration

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

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

6.0 Configuration

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

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 IP Series, 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

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

6.0 Configuration

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 the IP Series's 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 IP Series memory.

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

6.0 Configuration

6.1.4.4 SNMP Agent Configuration

The 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 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 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.

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.

6.0 Configuration

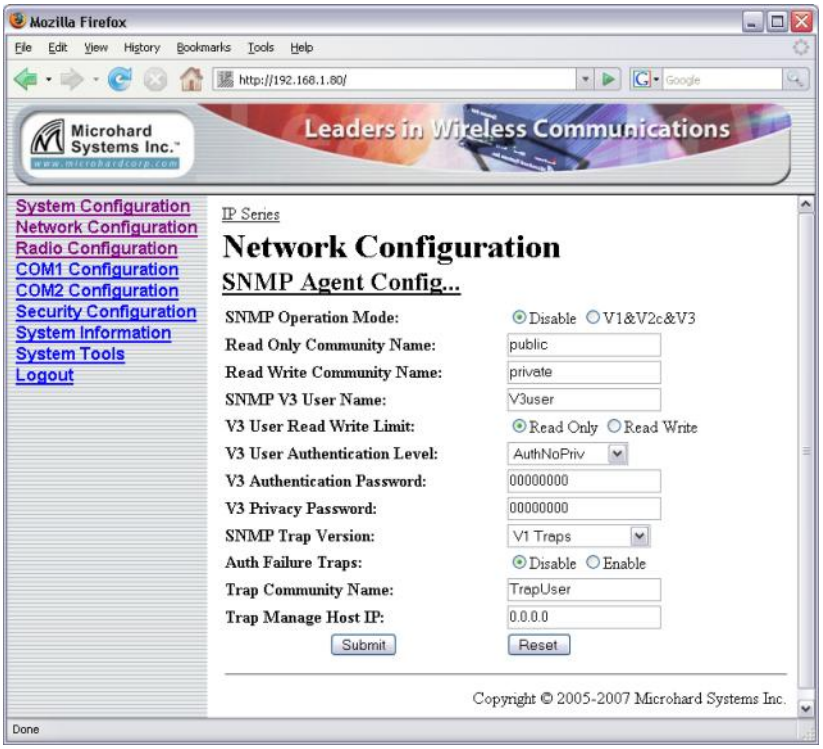


Image 6K: Network Configuration, SNMP Agent Config. Submenu

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

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.

continued...

6.0 Configuration

Read Only Community Name (continued)

Values

public

character string

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 Only
Read Write

6.0 Configuration

V3 User Authentication Level

Defines SNMPv3 user's authentication level.

NoAuthNoPriv: No authentication, no encryption.

AuthNoPriv: Authentication, no encryption.

AuthPriv: Authentication, encrpytion.

Values

NoAuthNoPriv

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

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

Disable
Enable

Trap Community Name

The community name which may receive traps.

Values

TrapUser

character string

6.0 Configuration

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 address

Soft Buttons

- Submit
  Write parameter values into IP Series memory.

- Reset
  Restore 'currently' modified parameter values to those which were previously written into IP Series 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 within the IP Series: On or Off.

Values
On
On Off

Soft Buttons

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

6.0 Configuration

6.1.4.6 Quality of Service

Quality of Service (QoS) may be applied to various data which enter the 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.

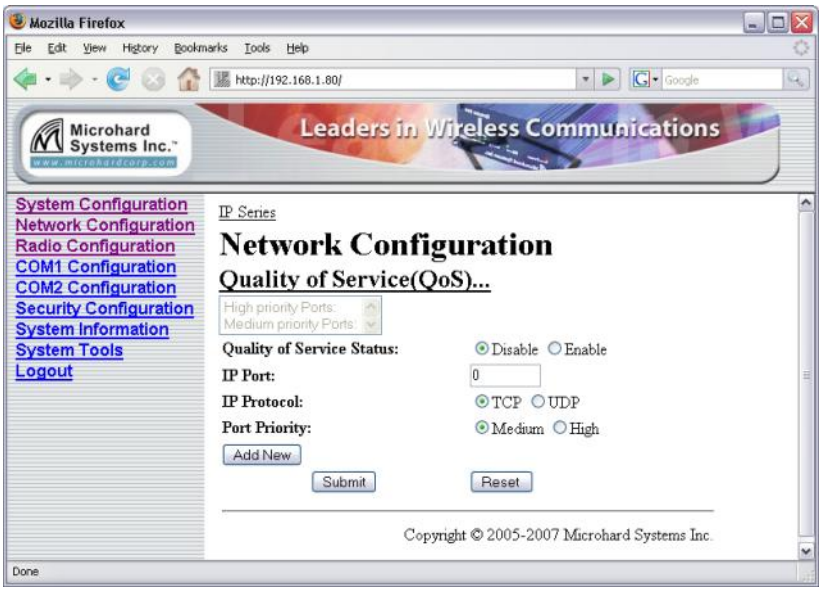


Image 6M: Network Configuration, Quality of Service Submenu

Quality of Service Status

If Enabled, the defined protocols and ports will have the QoS service applied to them.

Values

Disable

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:

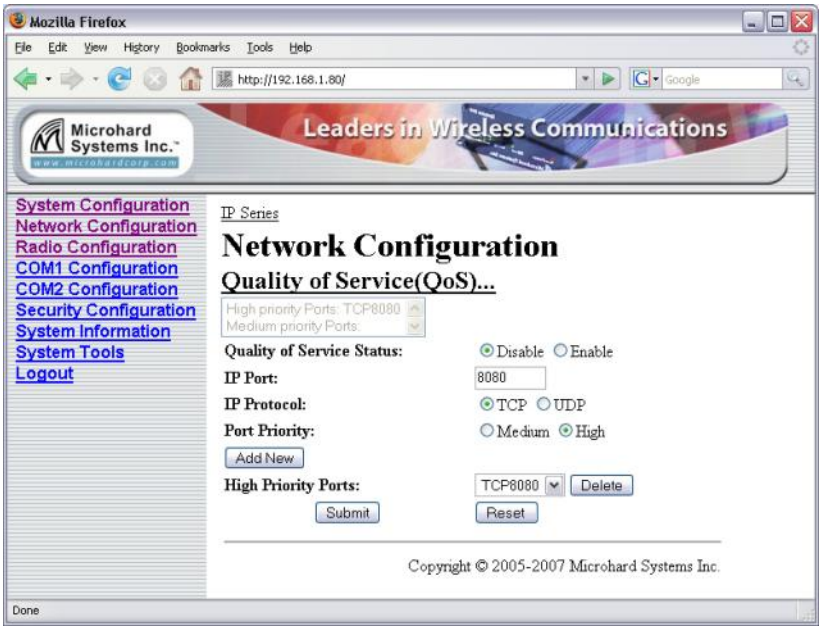


Image 6N: Network Configuration, QoS Example

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

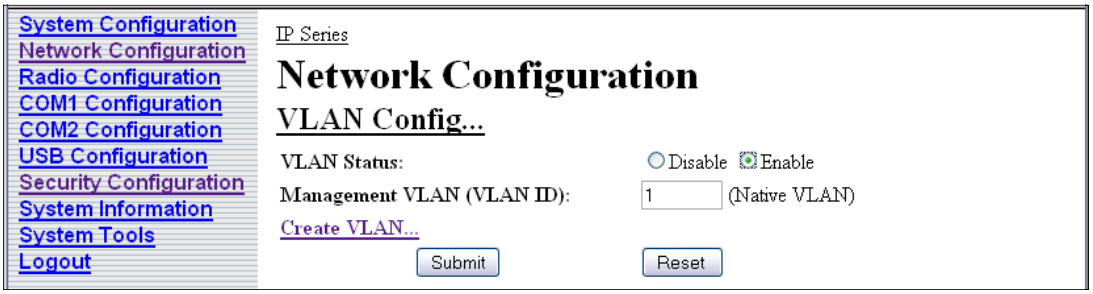
As ports are defined, the mini window and list boxes (specific to Priority) become populated. To DELETE any defined port, simply select it via the appropriate list box and click the DELETE soft button.

6.0 Configuration

6.1.4.7 VLAN

The IP Series implementation of VLAN (Virtual LAN) is currently only supported when the unit is configured in Bridge Mode. Once configured VLAN functionality can be provided as a VLAN filter, a VLAN tagger or a VLAN blocker. VLAN compatible devices can be configured to provide a VLAN TAG in the ethernet frame. Using this tag, data can be virtually filtered or blocked, and data from unsupported devices (serial data, etc) can be tagged, then filtered or blocked as required. This can be done at the wired and/or wireless ports eliminating unwanted or unneeded data, providing additional security and conserving valuable bandwidth.

VLAN: A virtual LAN is a group of hosts that communicate as if they were attached to the same broadcast domain, not dependant upon their actual physical location.



Management VLAN is used for purposes such as telnet, SNMP, and syslog. By default, VLAN 1 is the management VLAN.

Primary VLAN (VLAN 1) is a logic VLAN tag which can not be created or altered by the users. All Ethernet frames without a VLAN tag (i.e. Untagged frames) will be treated in this logic VLAN.

User VLANs (VLAN 2 – 4094) are actual VLANs which can be created or deleted by the users. All Ethernet frames in this VLAN will contain the specified VLAN tag.

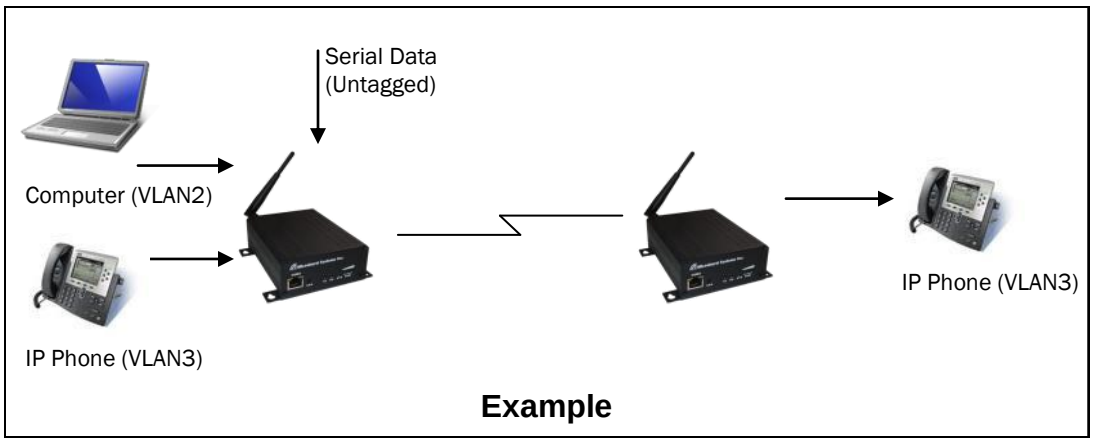
Once VLAN is enabled, but before any VLANs are created other than the primary VLAN (VLAN1), the unit will actually pass any untagged frames and drop any VLAN tagged frames. VLAN ID's can then be created, lets say 2, 3. Once VLAN 2 and 3 are created a user can define on the Wired Port and Wireless port what happens to the data. There are 3 options in the list: filter, tag and exclude. When you specify "Filter" option on both ports (by default), the unit will then pass all untagged frames as well as frames tagged with VLAN ID 2 and 3. By this mean we can eliminate unwanted wireless traffic and save our valuable bandwidth. When you specify "Tag" option on the Wired Port and "Filter" option on the Wireless port, the unit will then "tag" those untagged frames entering wired port with VLAN id 2 (or 3) and pass them on the wireless port. You may also specify "Exclude" option on either Wired port or Wireless port, which means frames with VLAN id 2 (or 3) will be blocked at the Wired or Wireless port specifically.

By default the management VLAN is set to Primary VLAN (VLAN 1). You may change it to any user VLAN, let's say VLAN 3, all frames generated from this unit, for example the serial data, will be tagged as VLAN ID 3. It can be passed or dropped by itself, depending on the VLAN setting on the bridge. You can only telnet or web access the unit by VLAN 3 in this case.

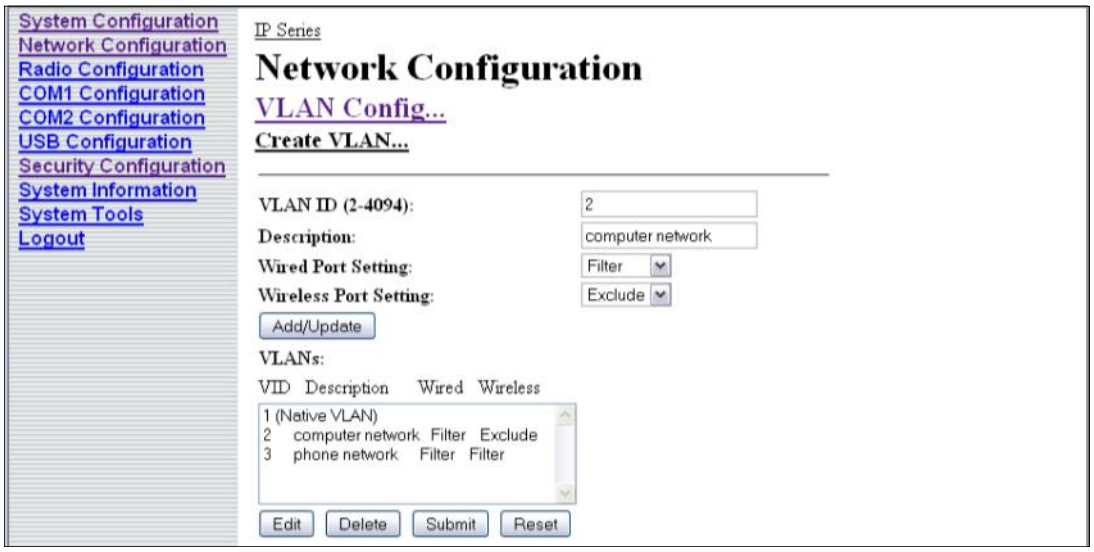
6.0 Configuration

6.1.4.7 VLAN (Continued)

In the example below, The VLAN feature can be used to filter data so that only the data between the IP Phones (VLAN3) are transmitted on the wireless link.



Example



VLAN Status	
Use the VLAN Status option to enable or disable the VLAN functionality on the radio. The default value is **disable**.	**Values (selection)** **Disable /** enable

Management VLAN (VLAN ID)	
Once VLAN us enabled, it uses a default value of 1 for the Native VLAN for management purposes.	**Values** **1**

6.0 Configuration

6.1.4.7 VLAN (Continued)

	VLAN ID (2 - 4094)
This is the user defined VLAN ID, this can be any number between 2 and 4094.	**Values (2 - 4094)** **2**
	Description
User set description of the VLAN's use (computer network, phone system, etc)	**Values** **characters**
	Wired Port Setting
Fliters, Tags, or Excludes the data on the wired port based on the VLAN ID. Filter: Passes data along that has the current VLAN ID Tag: Tags untagged data with the current VLAN ID Exclude: Blocks any data with the current VLAN ID	**Values (selection)** **Filter** Tag Exclude
	Wireless Port Setting
Fliters, Tags, or Excludes the data on the wireless port based on the VLAN ID. Filter: Passes data along that has the current VLAN ID Tag: Tags untagged data with the current VLAN ID Exclude: Blocks any data with the current VLAN ID	**Values (selection)** **Filter** Tag Exclude

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 IP Series must also be known.

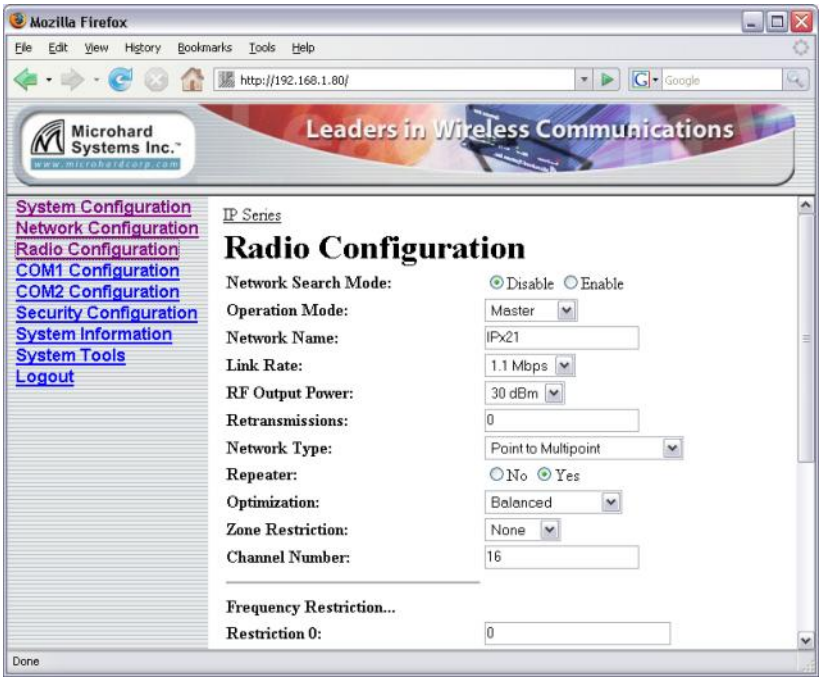


Image 6O: Radio Configuration Menu (upper portion)

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.

continued...

6.0 Configuration

Network Search Mode (continued)

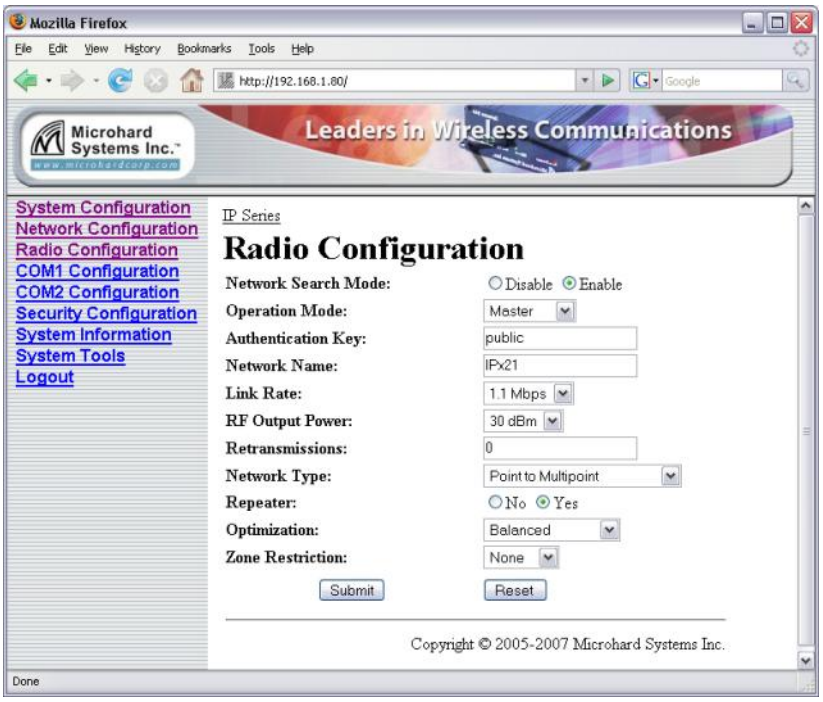


Image 6P: Radio Configuration Menu (upper portion), with Network Search Mode Enabled

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 IP Series: Master, Repeater, or Remote. An IP Series may be configured for any role required within a radio network. This is convenient for reasons of familiarity with any/all units, as well as for hardware sparing purposes.

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.

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

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).

Values

Remote

Master
Repeater
Remote

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.

continued...

6.0 Configuration

Authentication Key (continued)

Values

Public

Character string

Network Name

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.

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

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.

Values

default is model-dependent

character string

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 IP Series in a network must use the same Link Rate.

Values

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

6.0 Configuration

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.

Unit Address

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

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.

RF Output Power

This setting establishes the transmit power level which will be presented to the antenna connector at the rear of the 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)

6.0 Configuration

Retransmissions

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

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.

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 (below).

PTP: 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.

Values
0-255
5

Network Type

Defines the type of RADIO network (see Section 5.0 for a detailed description of network topologies).

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

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).

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.

continued...

6.0 Configuration

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.

Network Type (continued)

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.

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).

Values

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

6.0 Configuration

Destination Unit

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

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.

Values

1-65535

Tx Control

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

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

Off configures the IP Series 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

6.0 Configuration

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.

Roaming Address

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

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 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.

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

6.0 Configuration

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

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.

continued…

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 6A: 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 6B: Restricted Bands for UA1 at 1.1Mbps Link Rate

Values

None

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

6.0 Configuration

Channel Number

This setting applies only if the Link Rate is set to 1.1Mbps.

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 1.1Mbps 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

6.0 Configuration

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.

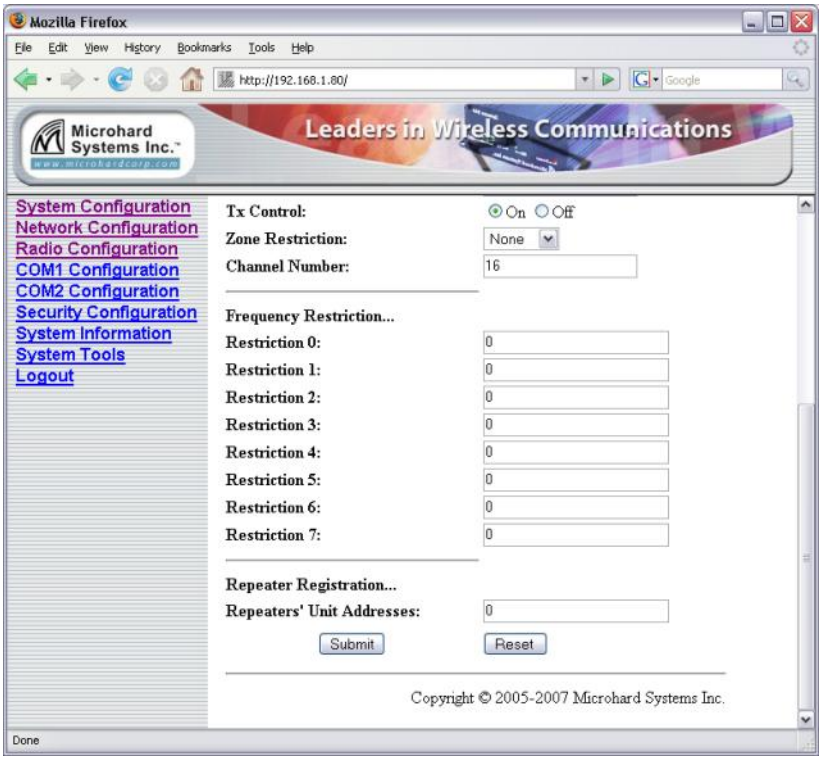


Image 6Q: Radio Configuration Menu (lower portion)

Frequency Restriction

By default, the IP Series will hop on frequencies across the entire 902-928MHz ISM band. 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 6.1.8.4 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.

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

continued...

6.0 Configuration

Frequency Restriction (continued)

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 IP Series (with 345kbps as an available Link Rate) with a Link Rate of 345kbps to not operate on channels 1 through 10.

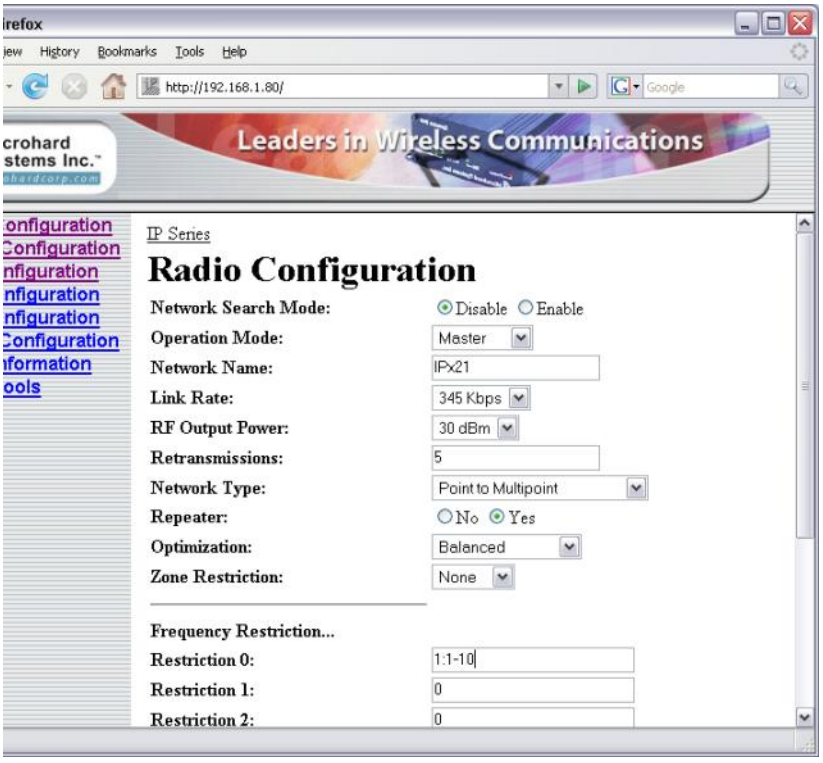


Image 6R: Frequency Restriction, 345kbps

Use the Radio Channels Noise Level tool (see Section 6.1.8.4) to help identify the frequency/ range of possible interfering signals within the 902-928MHz ISM band, and then use the Frequency Restriction feature to configure the IP Series to avoid them.

6.0 Configuration

Frequency Restriction (continued)

With the IP Series having the option of, and configured for, a Link Rate of 1.1Mbps, 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

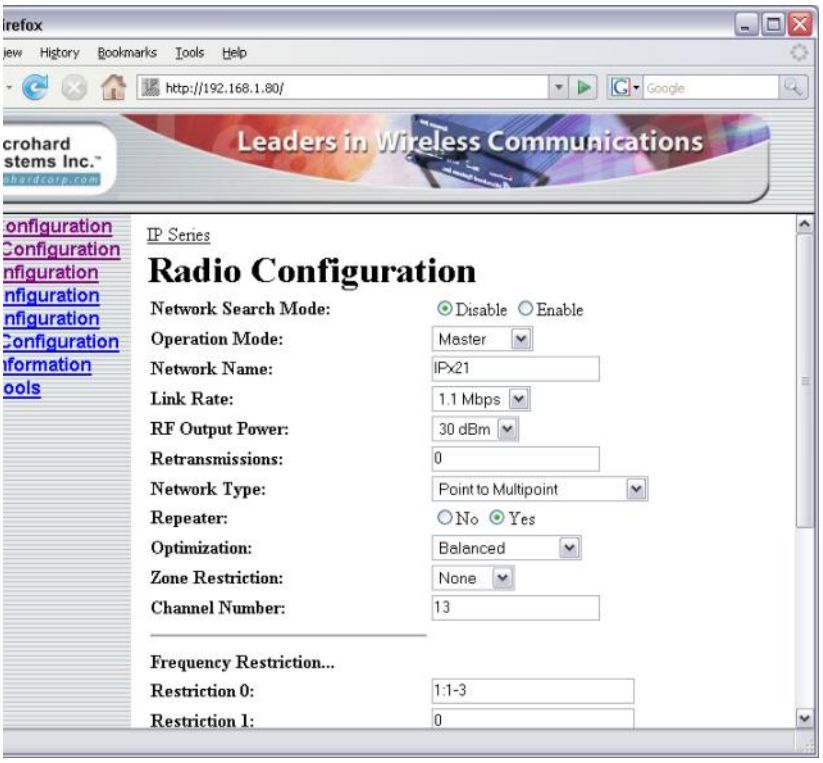


Image 6S: Frequency Restriction, 1.1Mbps

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

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 IP Series.

The following image depicts an example:

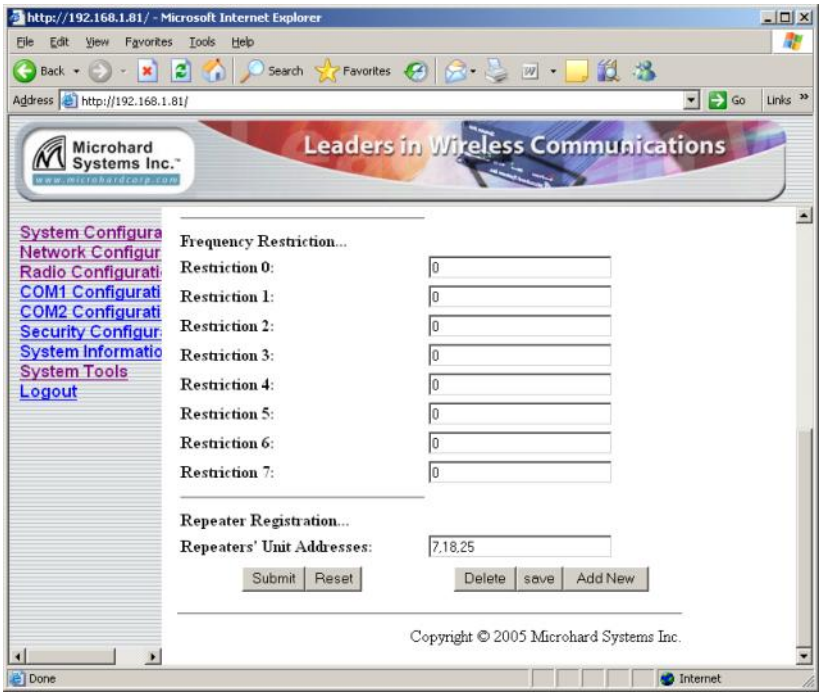


Image 6T: Repeater Registration

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 IP Series's Repeater Registration field.

Format:

x,y,z

where

x, y, and z are Repeater UAs,

6.0 Configuration

Soft Buttons

- Delete
  Delete the displayed Network Profile.
- save
  Save the displayed Network Profile.
- Add New
  Add a new Network Profile.
- Submit
  Write parameter values into IP Series memory.
- Reset
  Restore ‘currently’ modified parameter values to those which were previously written into IP Series memory.

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, the rear DE9 connector on the IP Series, and
- COM2, the front RJ45 connector, respectively.

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

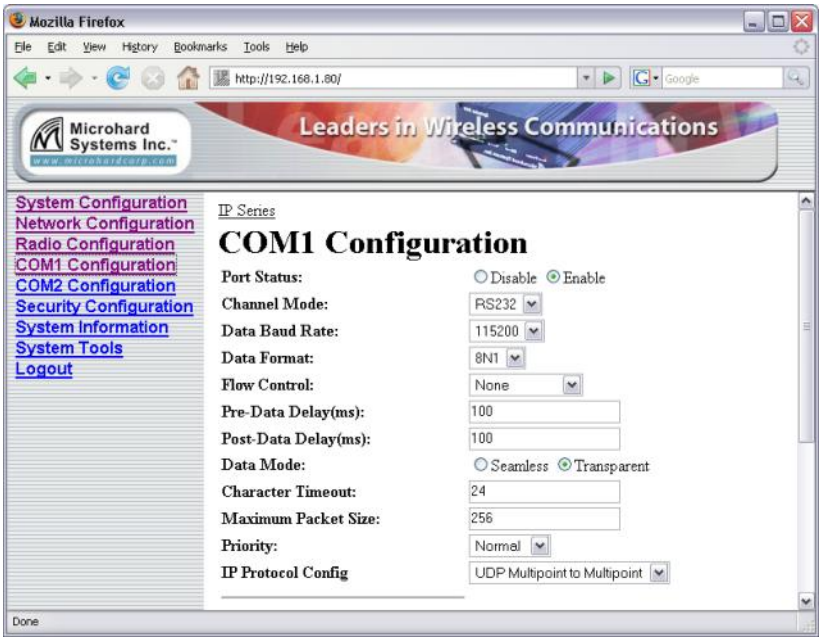


Image 6U: COM1 Configuration Menu (upper portion)

6.0 Configuration

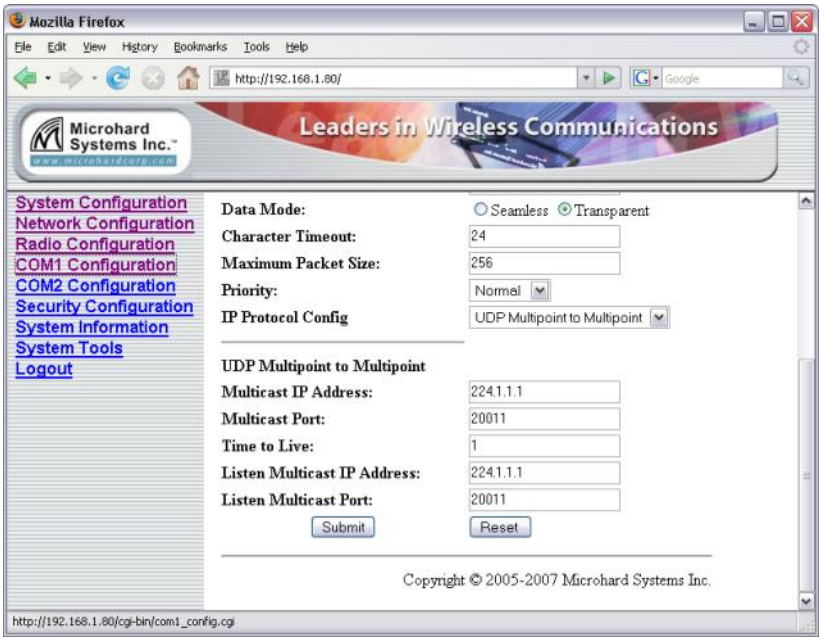


Image 6V: COM1 Configuration Menu (lower portion)

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. When an interface other than RS232 is selected, the DE9 port will be inactive.

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

...continued

6.0 Configuration

Channel Mode (continued)

Values

RS232
RS485 (2 wire)
RS422 (4 wire)

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

Data Format

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

Values

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

6.0 Configuration

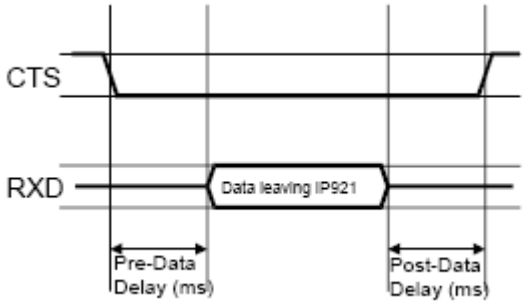
Software flow control (XON/ XOFF) is not supported.

Flow Control

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

When CTS Framing is selected, the 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.



Drawing 6A: CTS Output Data Framing

Values

None
Hardware
CTS Framing

Pre-Data Delay (ms)

Refer to Figure b on the preceding page.

*COM2 does not support this function.

Values

ms

100

6.0 Configuration

Post-Data Delay (ms)

Refer to Figure b 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 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. See 'Character Timeout' on the next page for related information.

Values

Seamless
Transparent

Character Timeout

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

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.

continued...

6.0 Configuration

Character Timeout (continued)

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).

Values

characters

4

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.

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

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

Requires more bandwidth than UDP.

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 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.

- 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 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 Server: In this mode, the 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**

continued...

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.

IP Protocol Config (continued)

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

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

continued...

6.0 Configuration

IP Protocol Config (continued)

UDP Point-to-Point: In this configuration the IP Series will send serial data to a specifically-defined point, using UDP packets. This same IP Series 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 IP Series which is to send multicast UDP packets; typically, the MASTER in the IP Series network.

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

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

continued...

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.

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.

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).

IP Protocol Config (continued)

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

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

- Remote Port
  The UDP port associated with the Remote IP Address (above). In the case of this 'Remote' being the Master 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**

continued...

6.0 Configuration

IP Protocol Config (continued)

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**

SMTP Client: If the 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**

continued...

6.0 Configuration

IP Protocol Config (continued)

- 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

Soft Buttons

- Submit
  Write parameter values into IP Series memory.

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

6.0 Configuration

6.1.7 Security Configuration

There is significant security inherent in the IP Series'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

6.1.7.1 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

Do not forget the admin password as, if lost, it cannot be recovered.

New Password/Repeat Password
Values
character string
admin

Soft Buttons

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

6.0 Configuration

6.1.7.2 Upgrade Password Configuration

The Upgrade Password protects the IP Series 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
Values
character string
admin

Soft Buttons

- Submit
  Write parameter values into IP Series memory.

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

6.0 Configuration

6.1.7.3 Wireless Encryption Configuration

There are 2 encryption levels for the 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 IP Series does require that the corresponding decryption algorithm be applied to the output data of the receiving IP Series 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 IP Series 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**

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.

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.

6.0 Configuration

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

Encryption Type (continued)

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

Soft Buttons

- Generate Key (applicable to WEP modes only)
  Click to have a selected Key generated based upon a user-input Key Phrase.

- Submit
  Write parameter values into IP Series memory.

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

6.0 Configuration

6.1.7.4 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 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 IP Series on the network.

Discoverable: This unit will appear as existing on an 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.

continued...

6.0 Configuration

Discovery Service (continued)

Values

Disable
Discoverable
Changeable

Soft Buttons

- Submit
  Write parameter values into IP Series memory.

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

6.0 Configuration

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 IP Series accessible via the network, the user will arrive at the unit's LogOn window.

For a secure connection, see

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

The IP Series has a built-in Web server.

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.

6.1.7.5 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 **Discoverable** Changeable

continued...

6.0 Configuration

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.

Soft Buttons

- Submit
  Write parameter values into IP Series memory.
- Reset
  Restore ‘currently’ modified parameter values to those which were previously written into IP Series memory.

6.0 Configuration

6.1.7.6 Authentication Configuration

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

6.0 Configuration

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

Soft Buttons

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

6.0 Configuration

6.1.7.7 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 IP Series' User Interface and related protocols.

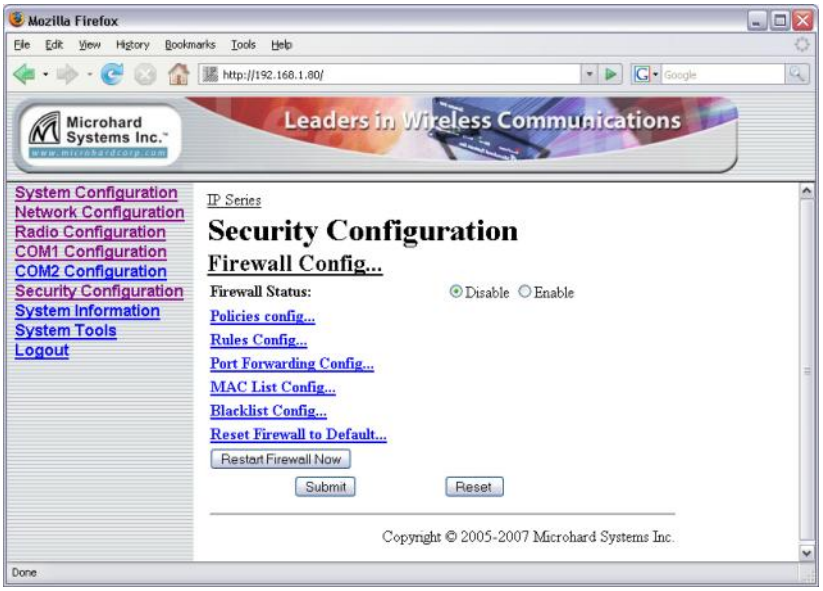


Image 6AE: Security Config. Menu, Firewall Configuration Submenu

Firewall Status

Disabled by default. When enabled, the firewall settings are in effect.

Values

Disable
Enable

6.0 Configuration

6.1.7.7.1 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 IP Series units, whether a Master, Repeater, or Remote.

Values

WAN
LAN
FW
VPN
all

6.0 Configuration

Destination Zone

Select the zone which is the intended desination of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all IP Series units, whether a Master, Repeater, or Remote.

Values

WAN
LAN
FW
VPN
all

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

6.0 Configuration

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

6.0 Configuration

6.1.7.7.2 Rules Configuration

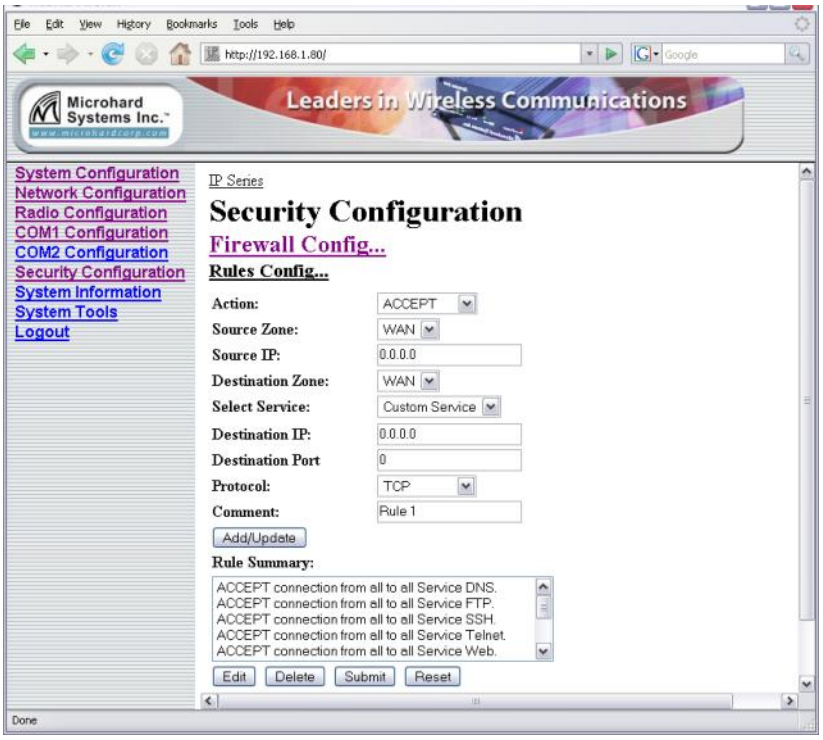


Image 6AG: Firewall Configuration, Rules Config. Submenu

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

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 IP Series 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 desination of the data traffic. WAN applies to the wired connection and LAN to the wireless, on all IP Series units, whether a Master, Repeater, or Remote.

Values

WAN
LAN
FW
VPN
all

6.0 Configuration

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 pulldown 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

Destination Port

This field is configured if defining a Custom Service (ref. Select Service field).

Values

0

valid port number

6.0 Configuration

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

6.1.7.7.3 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

6.1.7.7.4 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

6.0 Configuration

MAC Address

Specify the MAC Address to be added to the list.

Values

00:00:00:00:00:00

valid MAC address

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

6.1.7.7.5 Blacklist Configuration

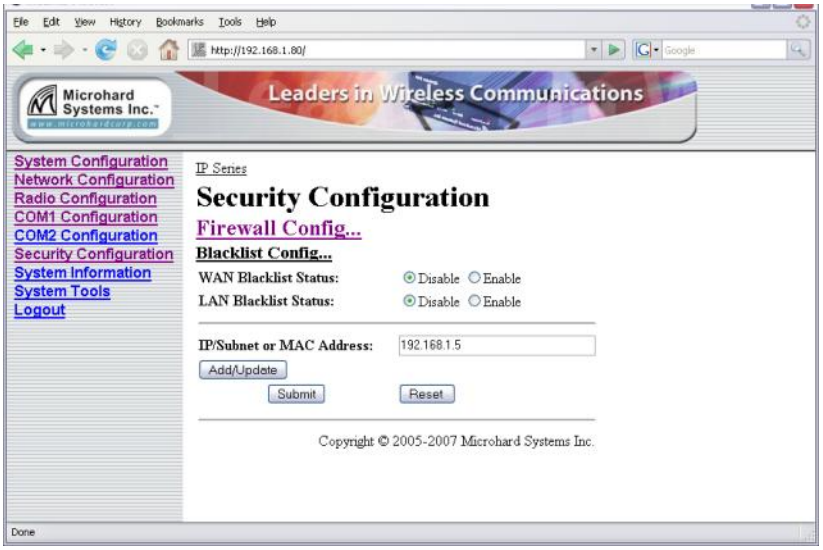


Image 6AJ: Firewall Configuration, Blacklist Configuration Submenu

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

6.0 Configuration

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

6.1.7.7.6 Reset Firewall to Default

Image 6AK: Reset Firewall to Default

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

6.0 Configuration

Soft Buttons

- Add New/Save
  Add a new MAC Address with specific restrictions
- Add New
  Add a new port restriction configuration
- Delete
  Delete the chosen/highlighted restriction
- Submit
  Write parameter values into IP Series memory.
- Reset
  Restore ‘currently’ modified parameter values to those which were previously written into IP Series memory.

6.0 Configuration

6.1.8 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.

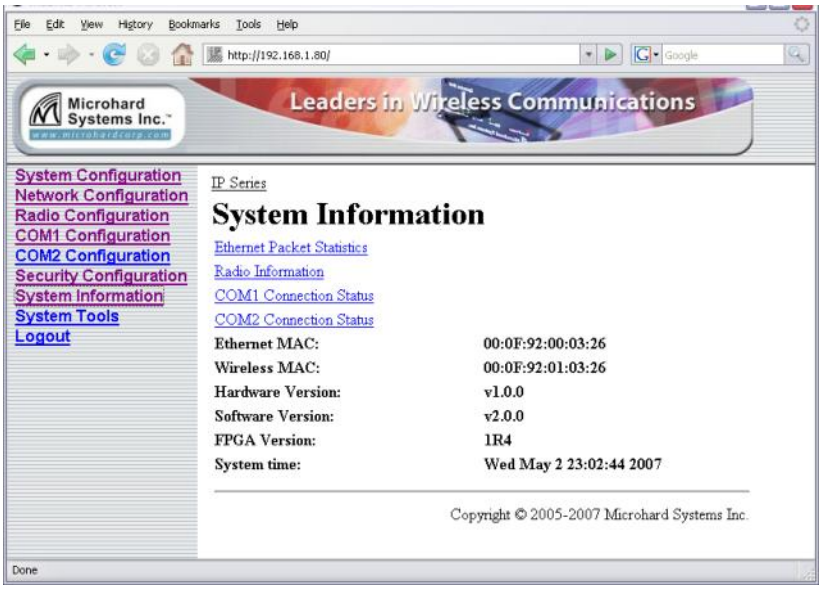


Image 6AL: System Information Menu

The four selectable System Information options provide information which refreshes automatically. If desired, the Refresh soft button (which appears on all options) may be also be used to initiate a 'manual' refresh.

Soft Buttons

- Refresh
  Request refresh of information displayed.

continued...

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.

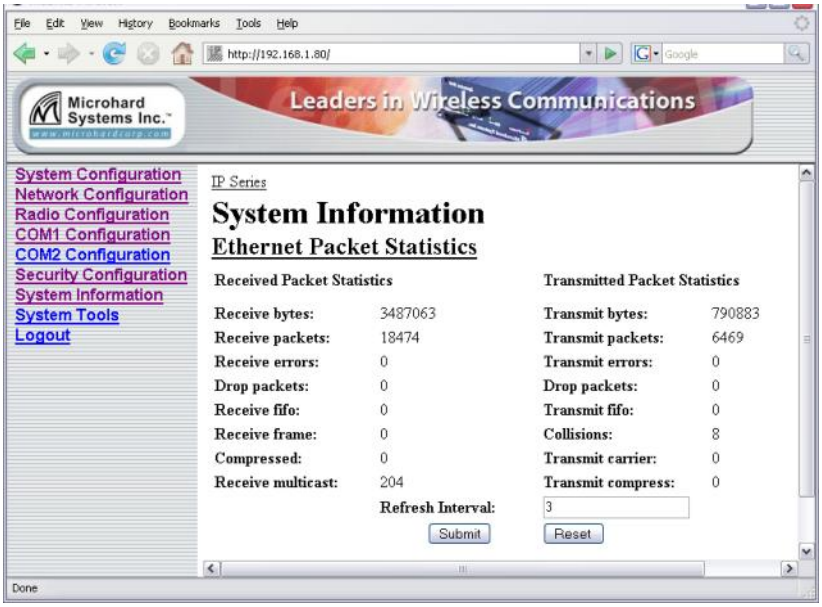


Image 6AM: System Information Menu, Ethernet Packet Statistics

6.0 Configuration

Radio Information

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

- Serial Number
  Serial number of radio (RF) module within IP Series.

- Version
  Firmware version within radio module.

- Temperature (C)
  Temperature as measured within the radio module.

- Voltage (V)

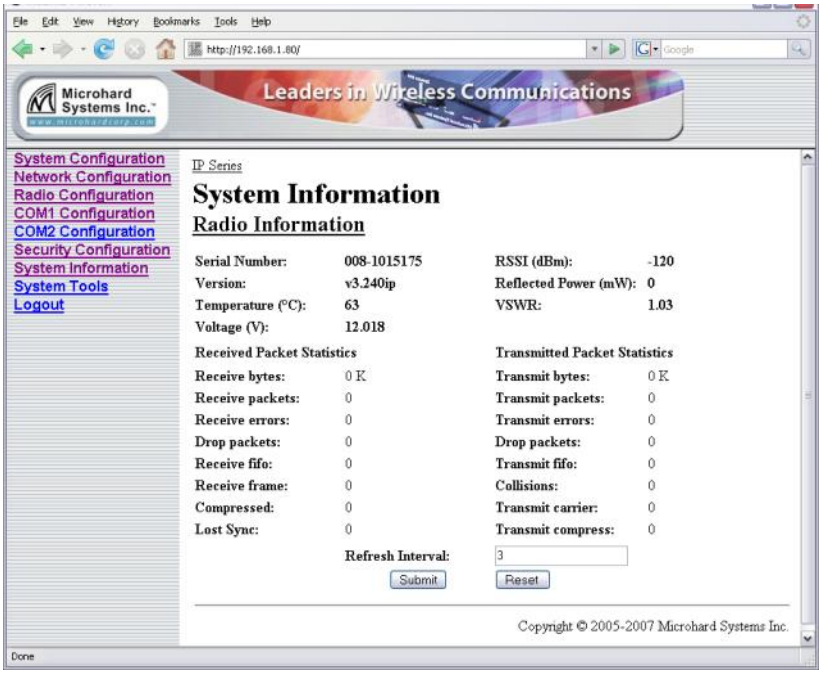


Image 6AN: System Information Menu, Radio Information

- RSSI (dBm)
  Receive Signal Strength Indicator measurement.

continued...

6.0 Configuration

Radio Information (continued)

- Reflected Power (mW)
  Of the power being transmitted 'out' of the modem, this number indicates the amount being 'returned' (due to impedance mismatch for whatever reason).

- VSWR
  Voltage Standing Wave Ratio. Ideally 1:1 (or 1.00), this value gives an indication of how much power is being reflected back to the IP Series from the antenna system relative to how much is being transmitted.

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 IP Series being viewed has lost synchronization with the Master IP Series.

6.0 Configuration

COM1 Connection Status

This window displays information related to the primary RS-232 serial interface (COM1 on the rear of the IP Series).

- 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'.

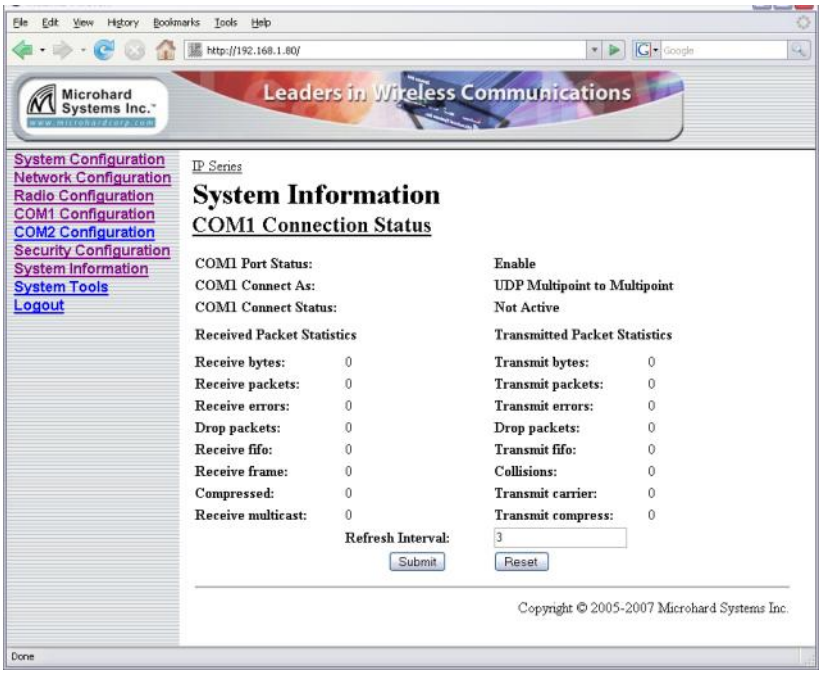


Image 6AO: System Information Menu, COM1 Connection Status

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 Connection Status

This window displays information related to the COM2 port located on the front of the 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'.

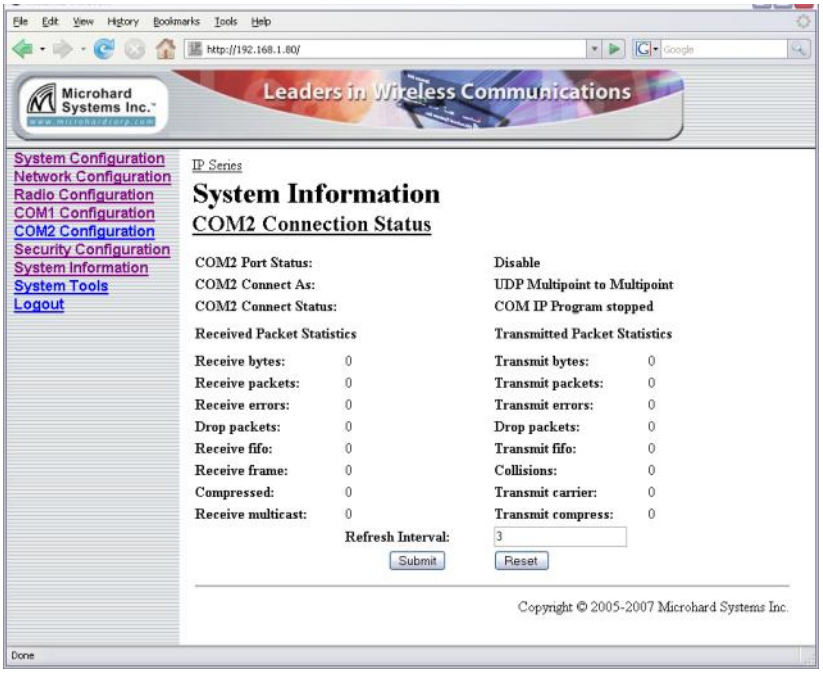


Image 6AP: System Information Menu, COM2 Connection Status

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

6.1.9 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 IP Series.

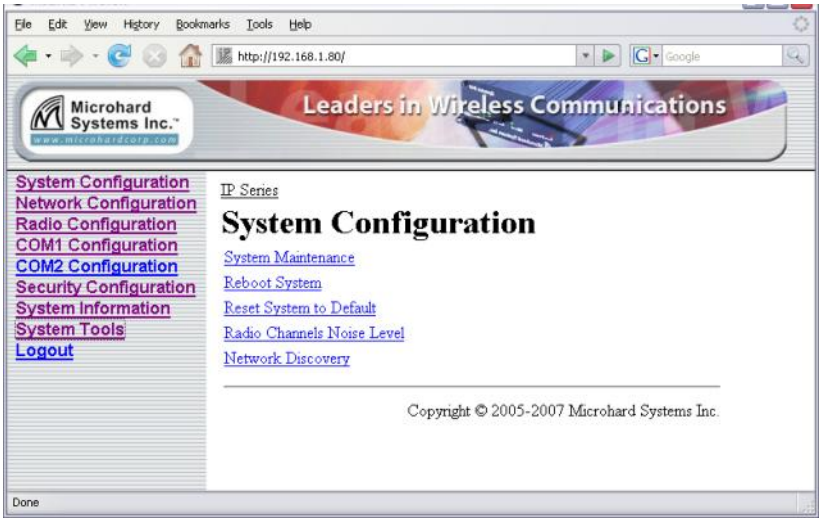


Image 6AQ: System Tools Menu

6.0 Configuration

6.1.9.1 System Maintenance

System Settings 'view' produces a long listing of all settings of the unit under scrutiny. Download affords the opportunity to download the various values.

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.)

Selecting the FTP Upgrade link will result in the prompt shown below. Default Password: '**admin**'.

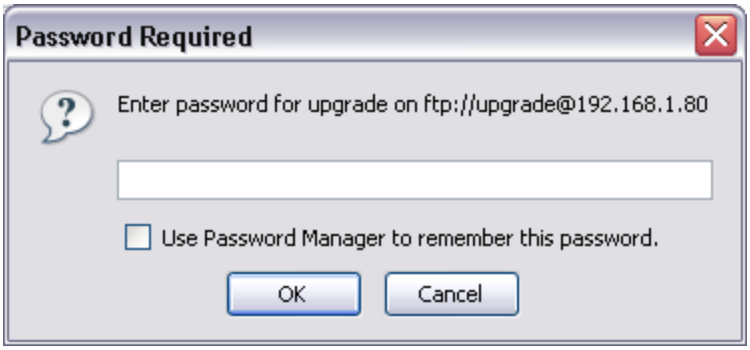


Image 6AS: System Tools Menu, Password

6.0 Configuration

6.1.9.2 Reboot System

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

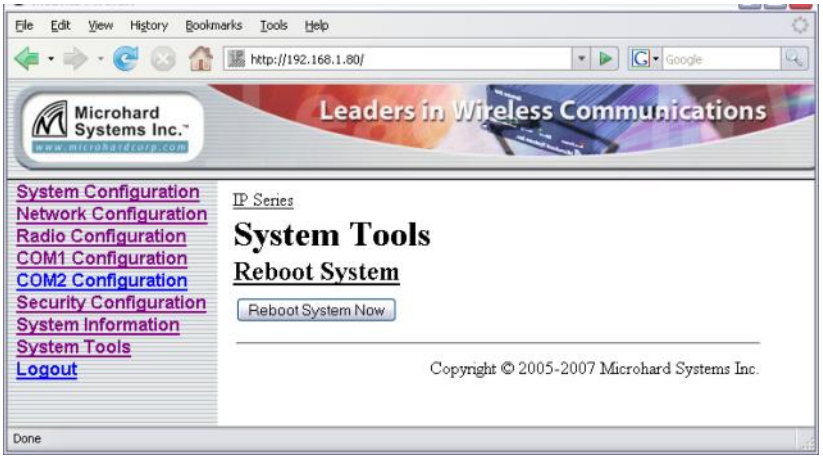


Image 6AT: System Tools Menu, Reboot System

6.0 Configuration

6.1.9.3 Reset System to Default

There are many configuration options for the IP Series.

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.

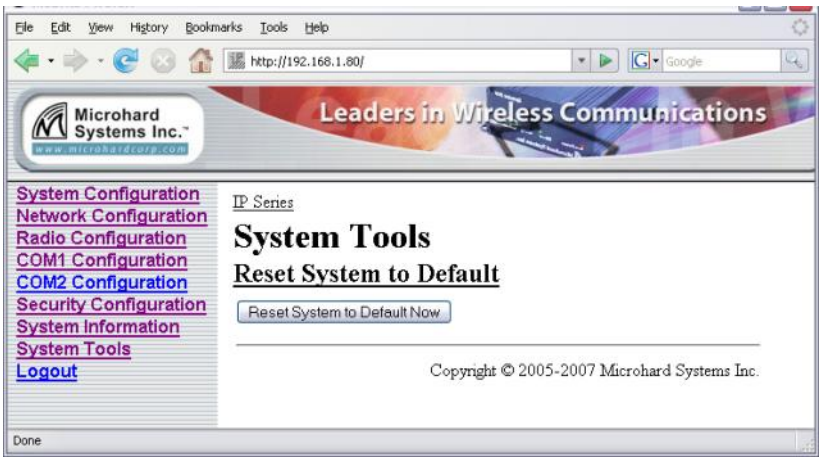


Image 6AU: System Tools Menu, Reset System to Default

6.0 Configuration

6.1.9.4 Radio Channels Noise Level

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

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

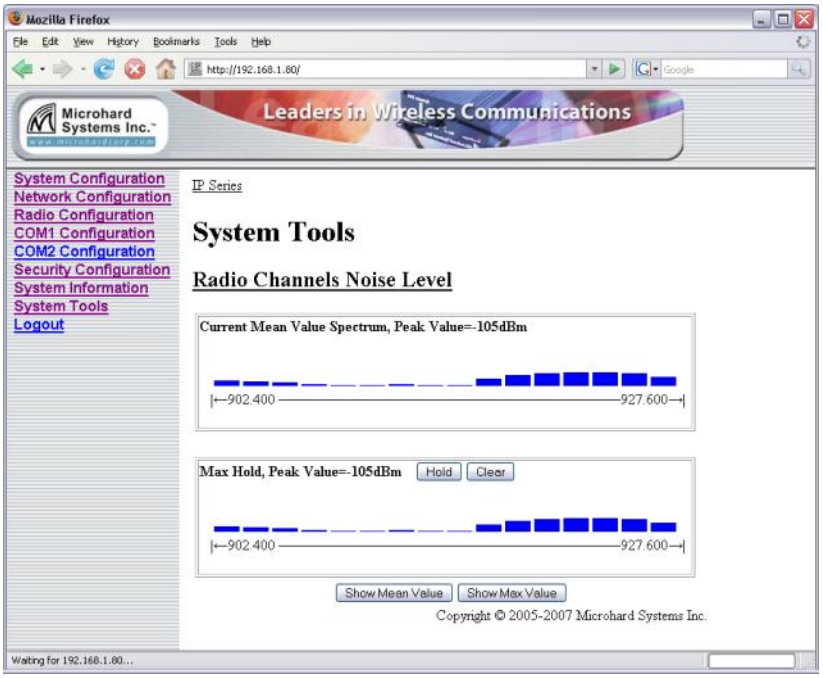


Image 6AV: System Tools, Radio Channels Noise Level, Mean Value

Moving the PC's cursor over ('mouse over') a particular channel will display the following for that channel:

- Channel Number
- Frequency (MHz)
- Noise Level (dBm)

continued...

6.0 Configuration

To view the maximum (peak) noise level, click the Show Max Value soft button. Move the PC's cursor over the various channels to view the measured values.

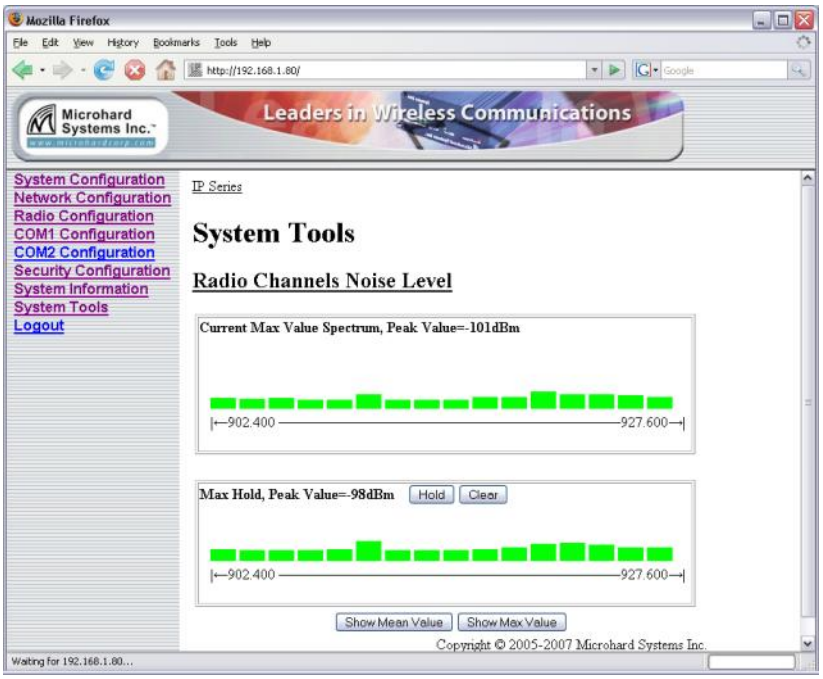


Image 6AV: System Tools, Radio Channels Noise Level, Max Value

Soft Buttons

- 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

6.1.9.5 Network Discovery

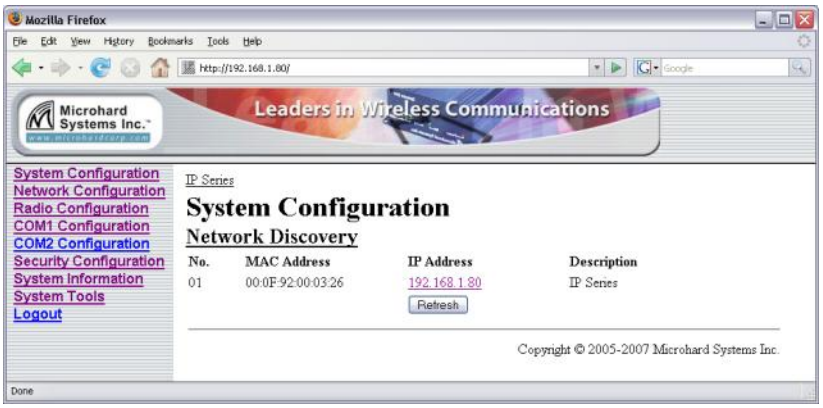


Image 6AW: System Tools, Network Discovery

Soft Buttons

- 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

6.1.9.6 Logout

The Logout menu informs the user how to log out of the Web User Interface.

Image 6AW: Logout Window

6.0 Configuration

6.2 Text User Interface

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

- connect the IP Series's front panel COM2 port to an available COM port on your PC, using the MHS-supplied Diagnostic Cable (black).
- 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 IP Series and wait approximately 1 minute for the system to load - you will observe various text appearing in the terminal program window, culminating in the IPx21 login prompt which can be seen in the screen capture below:

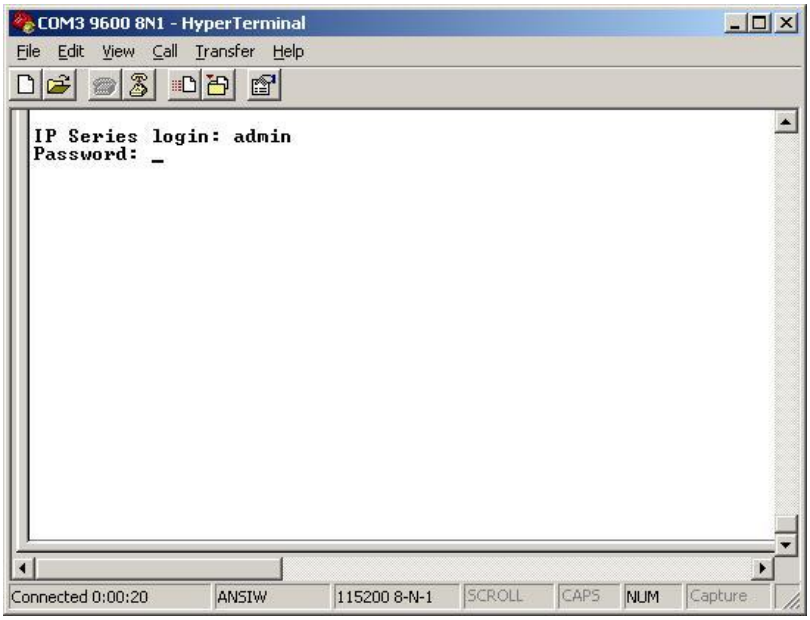


Image 6AX: Text User Interface, Login Prompt

- 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

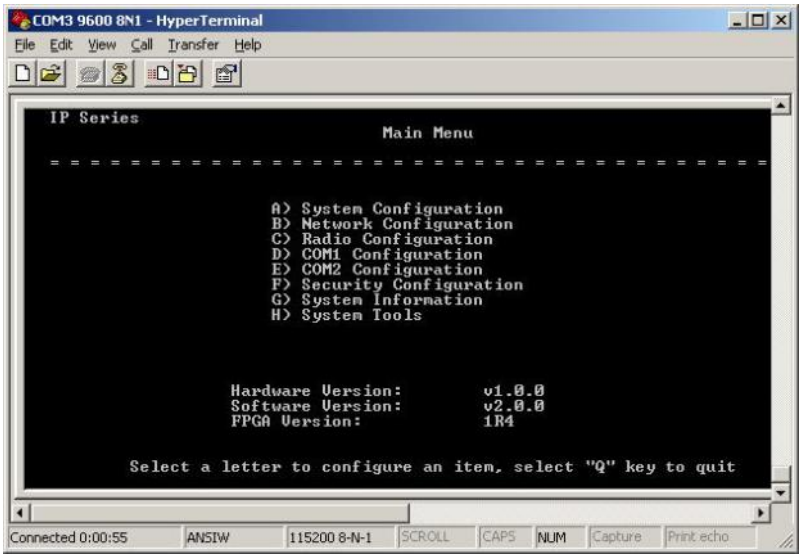


Image 6AX: Text User Interface, Main Menu

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.

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:

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

continued...

6.0 Configuration

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

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

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

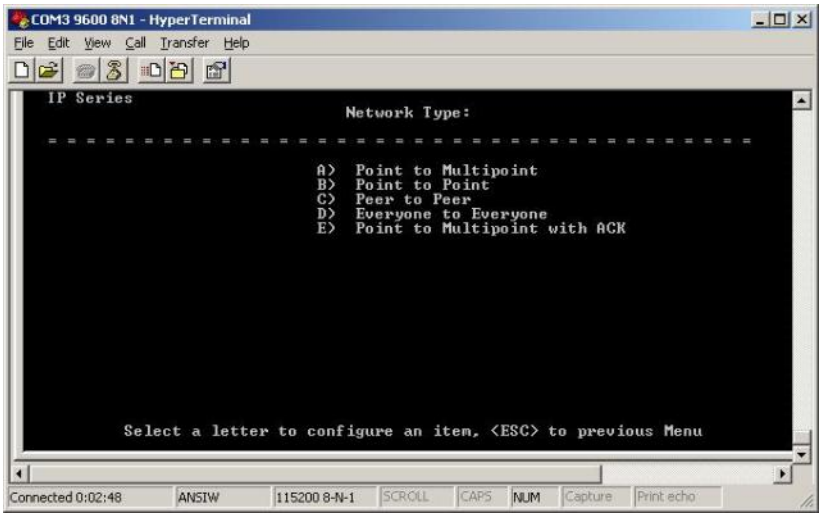


Image 6AZ: Text User Interface, Radio Menu, Network Type

6.0 Configuration

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

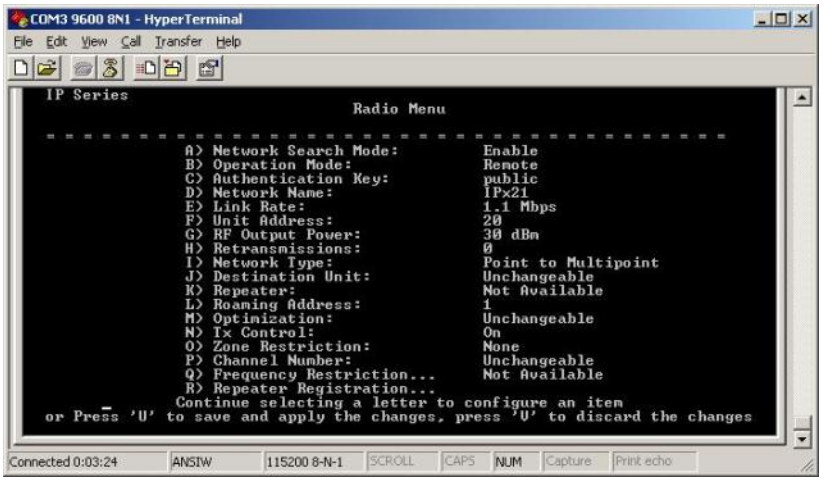


Image 6BA: Text User Interface, Radio Menu, Save Option

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

Be certain to SAVE any desired configuration changes.

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

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 IP Series will support. Determine which topology is suited to your specific requirements.

Throughput

The 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 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 being used, and 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.

7.0 Installation

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

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 Spectra 920A 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.

7.0 Installation

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

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.

7.1 Path Calculation

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 - Re ceiver 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

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

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

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

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.

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 Spectra 920A is generating RF energy. Always ensure that the Spectra 920A 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.

7.0 Installation

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

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

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.

7.2.3 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.

7.0 Installation

7.2.4 External Filter

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

Although the Spectra 920A 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 Spectra 920A 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

This utility maybe be used to 'discover' the IP Series 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:

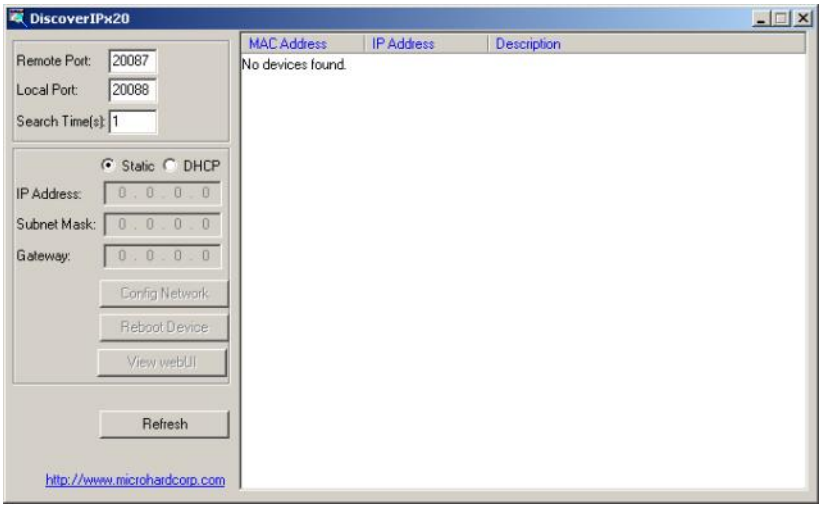


Image A1: *Initial Display*

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

In the sample, there is one IP Series connected to same network to which the PC is connected. Activating the Refresh soft button results in the IP Series being discovered by the utility:

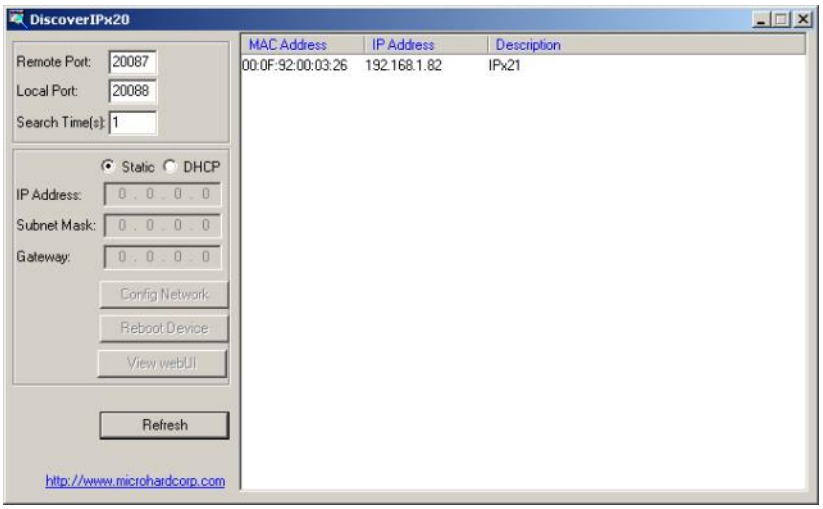


Image A2: *IP Series Discovered*

Appendix A: DiscoverIP Utility

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

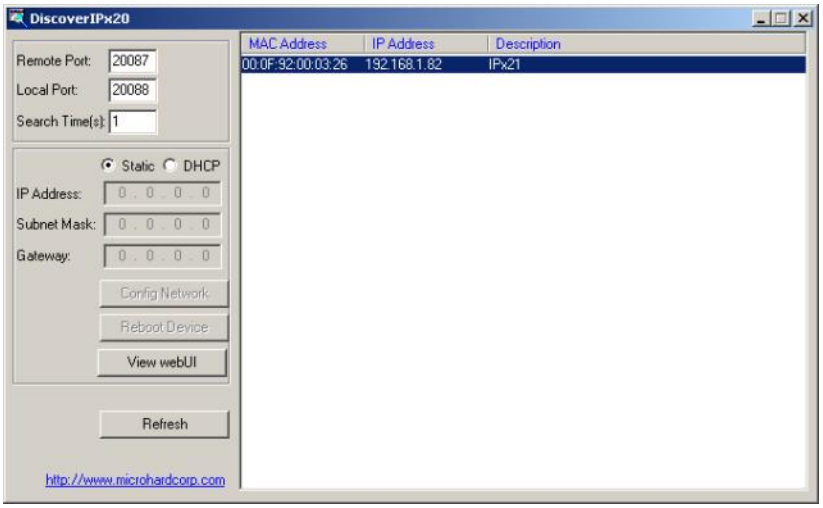


Image A3: *Select Target IP Series*

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

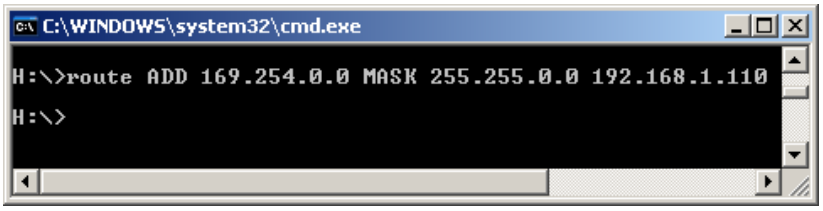


Image A4: *Add Route*

(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: Upgrade Process (DOS Prompt)

1.0 Overview

An IP920/IP921 can be upgraded with one of the two images, package upgrade image and recovery upgrade image. The package **(.pkg)** upgrade will keep current settings inside the unit, while the recovery **(.img)** upgrade will reset settings to factory default.

Package upgrade takes less time than recovery upgrade, the unit will reboot automatically after the image is successfully written into the unit. If a package upgrade failed for any reason, recovery procedure still can be used to completely upgrade the unit.

DO NOT kill or close the FTP session while SYS LED is flashing after upgrade command was issued.

1.1 Package Upgrade (.pkg)

This section describes the procedure to upgrade an IP920/IP921 unit with package upgrade file (*.pkg).

- Download upgrade package and put it into a known directory;
- Start up a command line window from the system;
- Change current directory to where the package file is located;
- Start a FTP session as shown below;

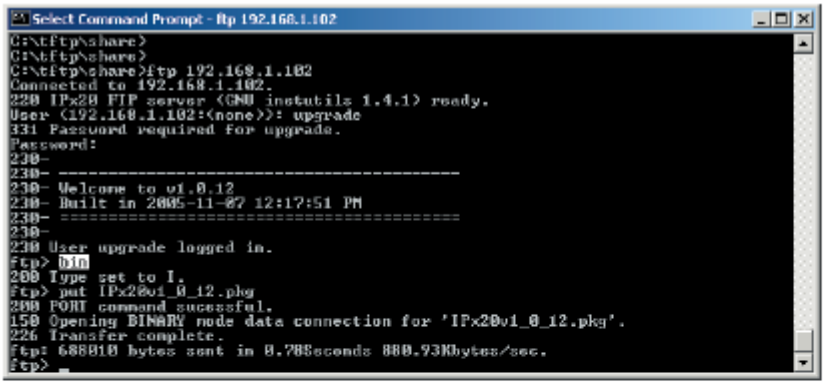


Figure 1 Command Line Package Upgrade

- Provide proper user name and password to login;
- Change transfer protocol to **BINARY** mode;
- Push package upgrade file into the system with "put" command;
- Package upgrade takes up to 2 minutes to complete. Wait until "SYS" LED stop flashing.
- If "SYS" LED doesn't come back to solid ON, the unit need to be manually restarted.

Appendix B: Upgrade Procedure (DOS Prompt)

1.2 Recovery Upgrade (.img)

In case the unit needs to be upgraded from recovery mode, the following procedure should be taken. Recovery images have file extension *.img.

- Download recovery image and save it into a known directory;
- Start up a command line window from the system;
- Change current directory to where the package file is located;
- Cycle power on the IP920/IP921 unit with CFG button pressed and held down until "SYS" LED is observed in fast flash mode;
- Start a FTP session as shown below; the IP address is set to a default **192.168.1.39**;

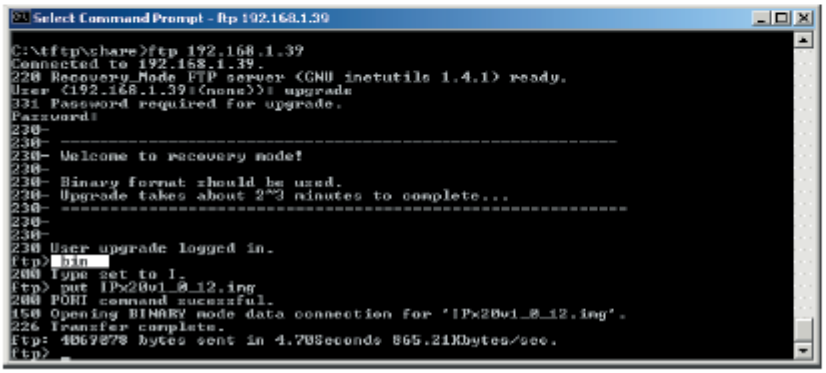


Figure 2 Command Line Recovery

- Provide proper user name and password to login;
- Change transfer protocol to **BINARY** mode;
- Push package upgrade file into the system with "put" command;
- Package upgrade takes more than 2 minutes to complete. The "SYS" LED changes from fast flash to slow flash to indicate upgrading is in process;
- The unit automatically reboots after the recovery procedure is completed.

Appendix C: RS485 Wiring

The IP9xx 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 IP9xx seize control of the line at the proper time when it is to transmit data.

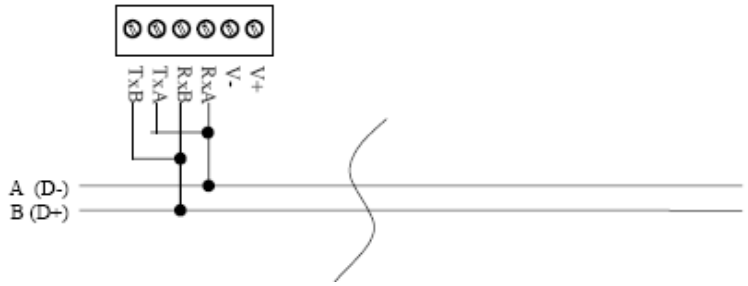


Figure C1: 2-Wire RS485 Wiring

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.

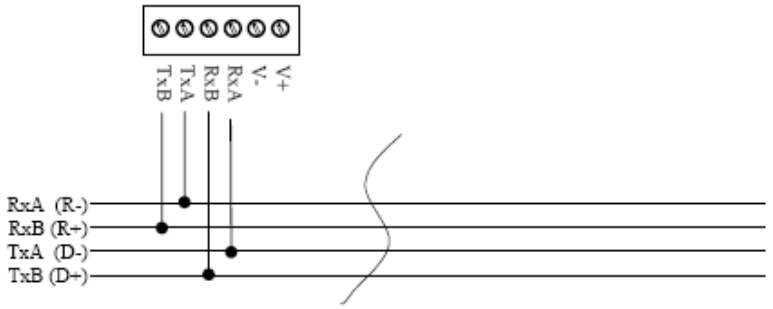


Figure C2: 4-Wire RS485 Wiring

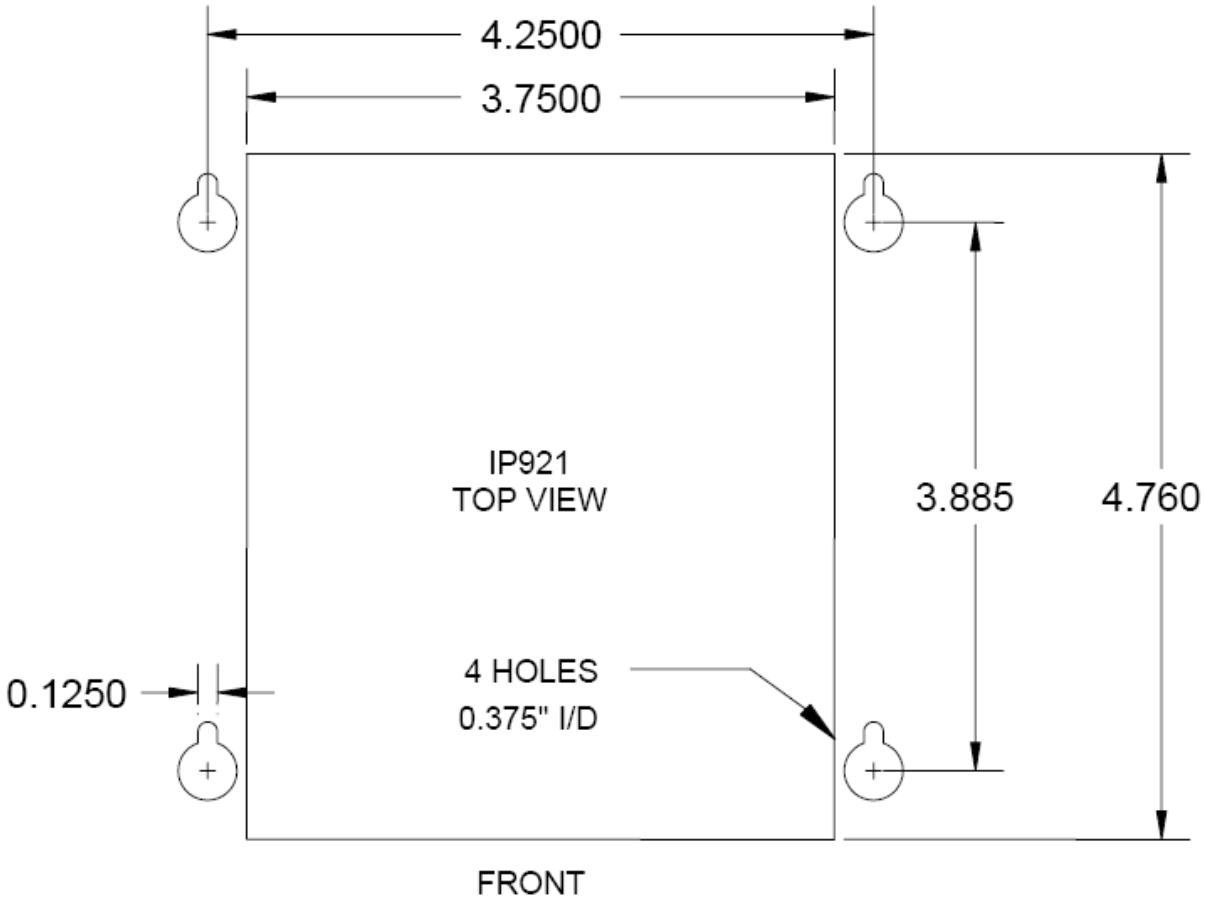
Appendix D: Approved Antennas

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 E: Mounting Dimensions



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.

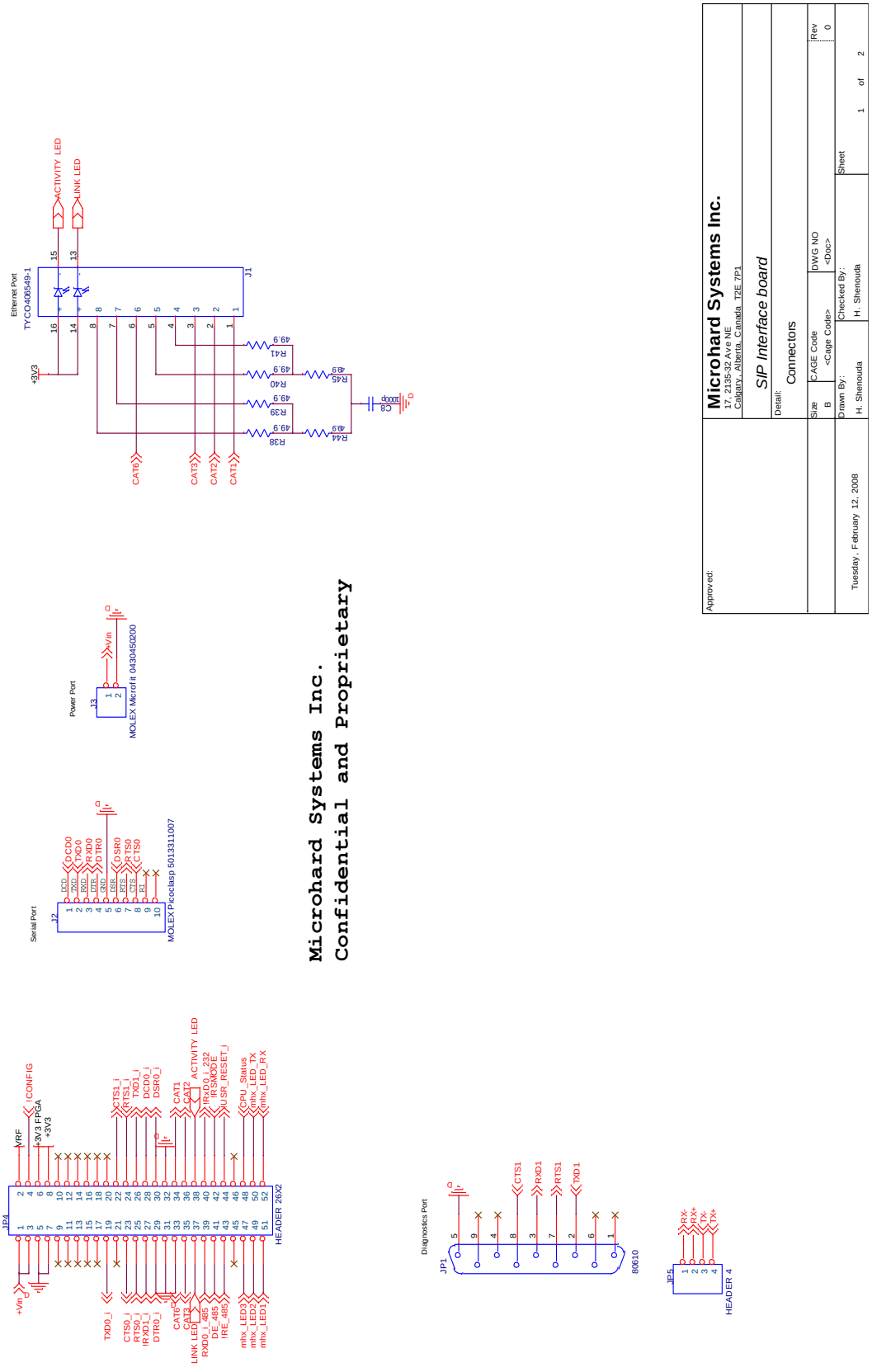
RTS *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

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.

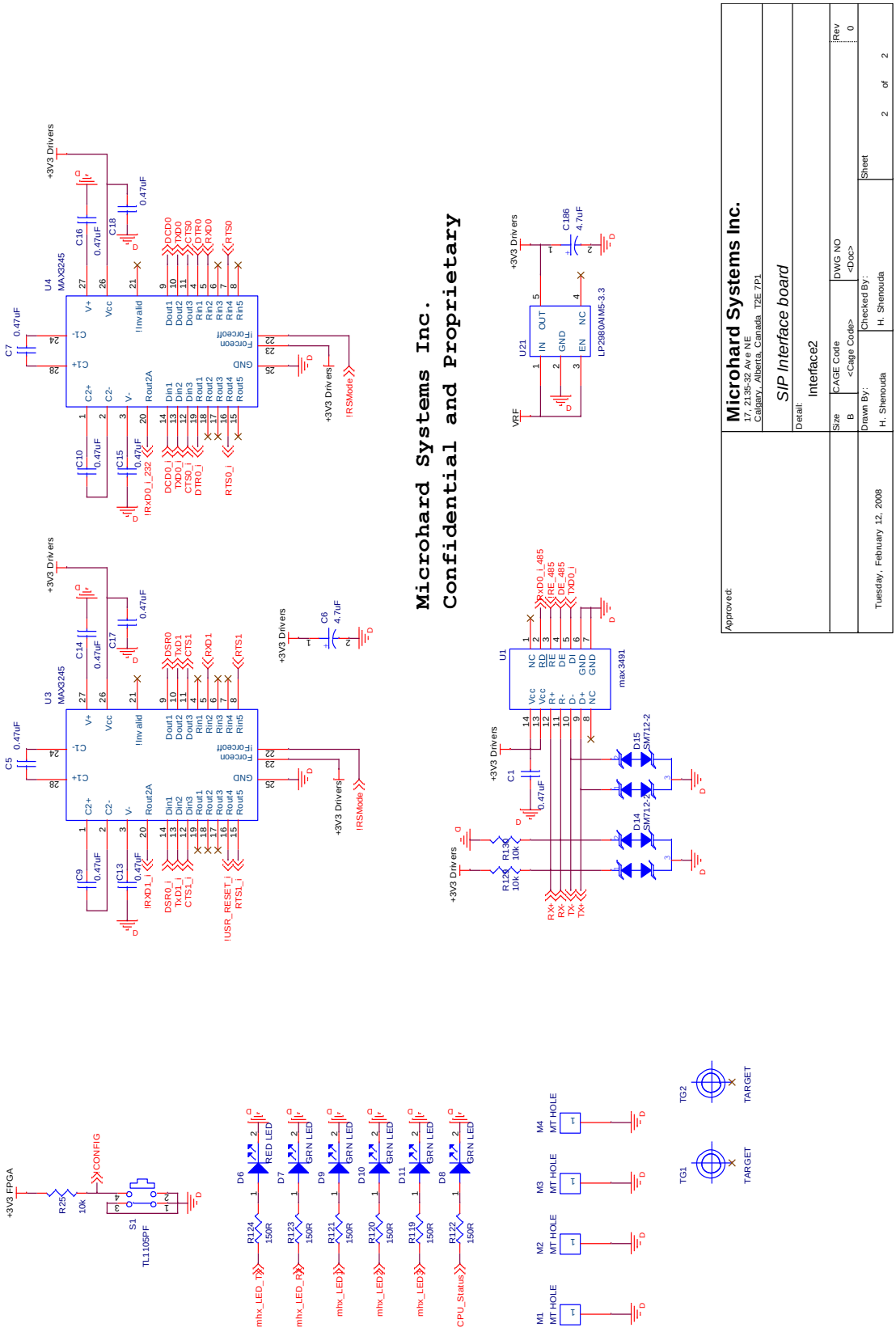
Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

"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: SIP Interface Schematic



Appendix G: SIP Interface Schematic (Page 2)



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

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