Operating Manual

VIP Series
OFDM Broadband Ethernet Bridge/Serial Gateway
Document: VIP Series Operating Manual.v1.41

June 2010

microhard SYSTEMS INC.

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

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

Important User Information

Warranty

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

Warranty Disclaims

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

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

Indemnification

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

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

Proprietary Rights

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

Important User Information (continued)

About This Manual

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

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

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

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

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

Information
Information regarding a particular technology or concept.

Important User Information (continued)

Regulatory Requirements

WARNING

To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 23cm or greater for the VIP2400 utilizing a 3dBi antenna, or 3.5m or greater for the VIP5800 utilizing a 34dBi antenna, should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna being used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

WARNING

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

WARNING

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

CSA Class 1 Division 2 Option

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

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

In such a case the following must be met:

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

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

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

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

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

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

Revision History

Revision 1.41	June 2010
Correction to Diagram 5.3	
Revision 1.4	June 2010
Updated Address.	
Revision 1.34	May 2010
Corrected SVIP CAT Pins, Misc Formatting, Embedded Links	
Revision 1.33	February 24, 2010
Added Simple Mesh Network to Quick Start section.	
Revision 1.31 - 1.32	February 19, 2010
Revamped Quick Start, Misc Formatting Changes	
Revision 1.3	January 22, 2010
Formatting, Section Renumbering/ordering, Network Diagrams, TOC updates etc	
Revision 1.2	January 13, 2010
Added SVIP Pin-outs, Added Mechanical Drawings, Misc. Formatting, MESH, Router	
Revision 1.1	October 1, 2009
Updated C1D2, Added Mechanical Drawings, Misc. Formatting	
Revision 1.0	August 24, 2007
Initial Release [Based on: Hardware Version 0.5.0; Software Version 0.1.0	

Table of Contents

Table of Contents (continued)

Table of Contents (continued)

Table of Contents (continued)

Appendices

1.0 Overview

The VIP Series is a high-performance wireless OFDM ethernet bridge and serial gateway. Alternately, a VIP Series unit configured as an access point (AP) may be further 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 VIP Series operates within either the 2400MHz or 5800MHz (model-dependent) license-exempt[1] frequency band, employing OFDM 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 VIP Series makes it ideal for many applications. Some typical applications include:

- high-speed backbone
- IP video surveillance
- voice over IP (VoIP)
- ethernet wireless extension
- legacy network/device migration
- SCADA (PLC's, Modbus, Hart)
- facilitating internetwork wireless communications

OFDM (Orthogonal Frequency Division Multiplexing) is an optimized modulation technique which uses many small simultaneous carriers to transmit data.

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.

1.1 Performance Features

Key performance features of the VIP Series include:

- transmission within a public, license-exempt band of the radio spectrum[1] - this means that the units may be used without access fees or recurring charges (such as those incurred by cellular airtime)
- long range
- transparent, low latency link providing reliable wireless serial and IP/ethernet communications
- each unit supports all modes of operation
- flexible wireless networking
- fastest serial rates: 300 baud to 921kbps
- communicates with virtually all PLCs, RTUs, and serial devices through either RS232, RS422, or RS485 interface

Continued...

1 license-exempt within North America

1.0 Overview

- serial gateway port supports legacy serial devices, including RTS, CTS, DSR, DTR, and DCD
- up to 54Mbps data rate
- adaptive modulation
- LAN and WAN dual ports
- WDS station bridge
- user-configurable firewall functions
- comprehensive encryption support (not available on export versions)
- authenticator and supplicant
- RADIUS server authentication
- Mesh
- remote administration
- easy to manage through user interface, or SNMP
- VPN support
- quality of service (QoS) support
- wireless firmware upgrade capable
- system wide remote diagnostics
- advanced security features
- industrial temperature specifications
- DIN rail mountable
- Optional Class 1 Div 2

With the ability to carry both serial and IP traffic, the VIP Series supports not only network growth, but also provides the opportunity to migrate from asynchronous serial devices connected today to IP-based devices in the future.

1.0 Overview

1.2 Specifications

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

2.0 Quick Start

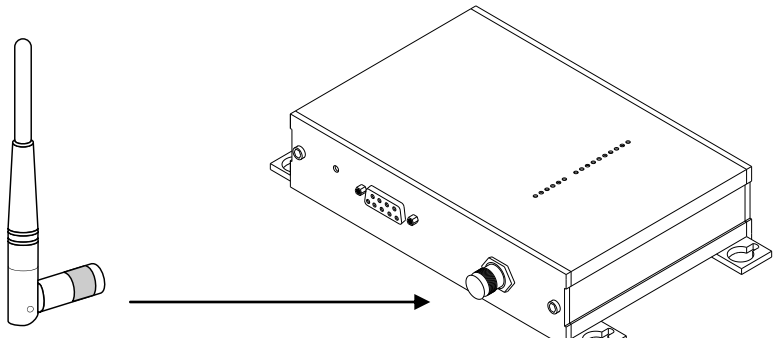
This QUICK START guide will walk you through the setup and configuration of a few basic applications. The QUICK START will rely on the *WebUI* for configuration. A text based configuration can also be performed via the *Console* RS232 port on the VIP Series, but is not the focus of this walkthrough. This walkthrough also assumes the units used are VIP units, the setup for SVIP or VIP-ANT will use the same concepts, but the hardware setup will be different than shown. See the appropriate sections for pin-outs and initial setup.

Note that the units arrive from the factory with a Radio Configuration of 'Station' 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 Getting Started

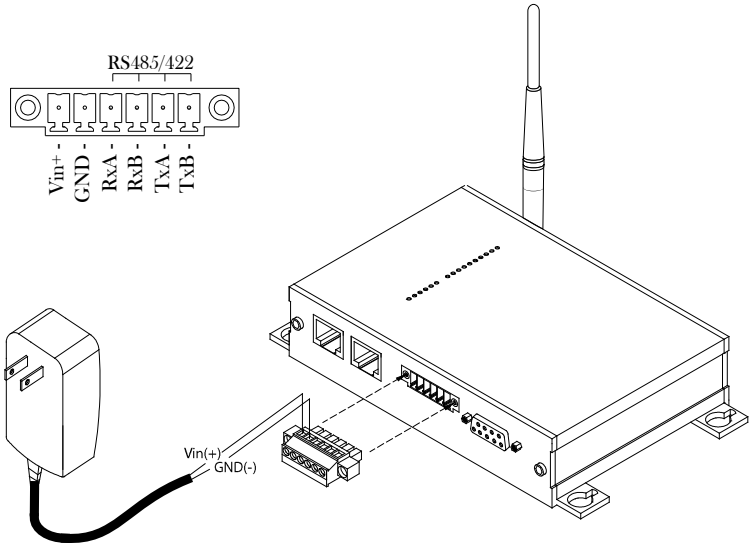
To reset to factory defaults, press and hold the CFG button for 8 seconds with the VIP powered up. The LED's will flash quickly and the VIP will reboot with factory defaults.

✓ Connect the included Rubber Ducky Antenna to the ***ANTENNA*** jack of the VIP Series.



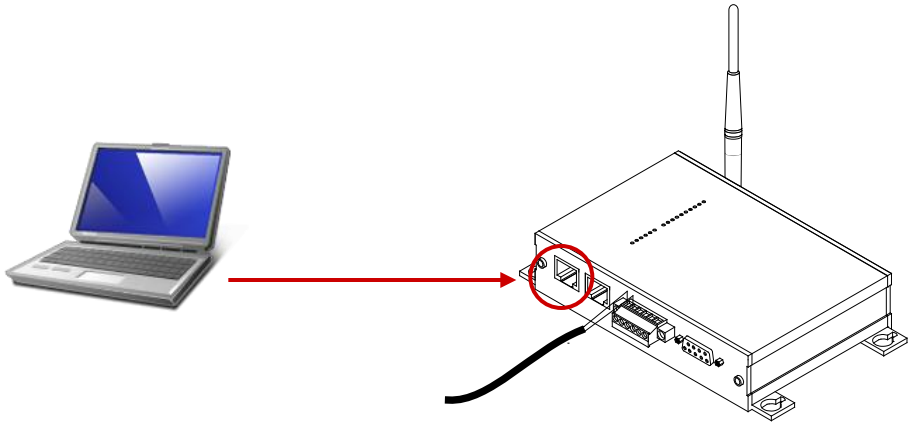
✓ Connect the Phoenix-Type Connector to the power adapter as shown below and apply power to the unit.

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



2.0 Quick Start

✓ Connect A PC to the ***LAN*** port of the VIP Series, using an Ethernet Cable.



Older models of the VIP may not support Auto Crossover, and will require a **CROSSOVER** Ethernet Cable.

✓ The PC must have its Network Setting (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

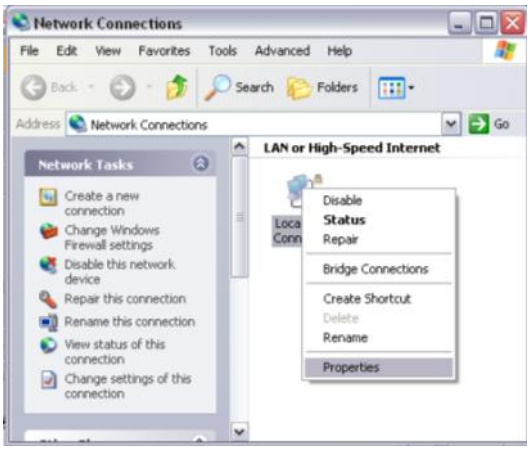
The factory default network settings:

IP: 192.168.1.254
Subnet: 255.255.255.0
Gateway: 192.168.1.1

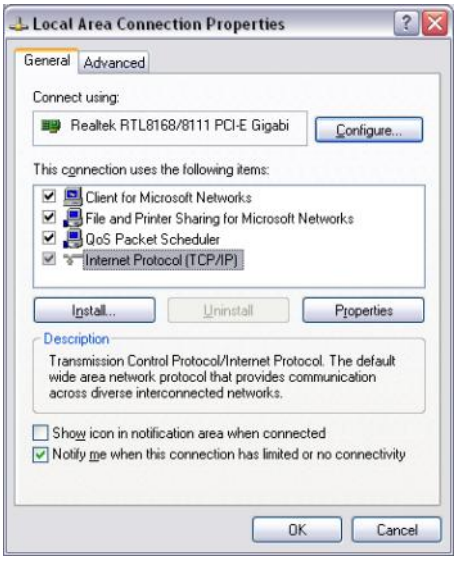
In ***Windows XP*** the TCP/IP Properties can be found in:

Start > Settings > Network Connections

Select the *Local Area Connection* and right click and select ***Properties***.



Select ***Internet Protocol (TCP/IP)*** and then ***Properties***

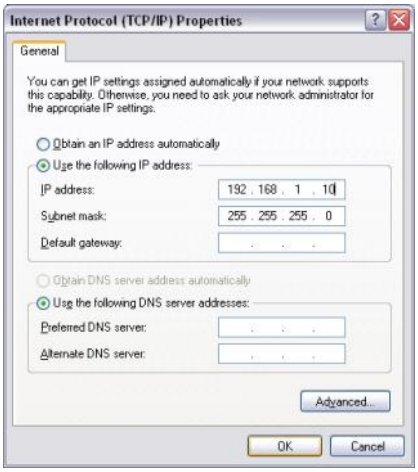


The Console Port of the VIP can also be used to configure the network settings.

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

IP Address: 192.168.1.10
Subnet Mask: 255.255.255.0

Click ***OK***

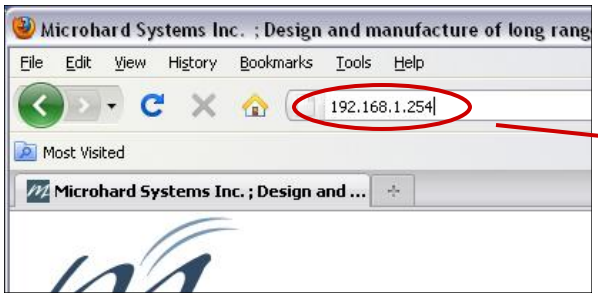


2.0 Quick Start

✓ Open a Browser Window and enter the IP address 192.168.1.254 into the address bar.

The factory default network settings:

IP: 192.168.1.254
Subnet: 255.255.255.0
Gateway: 192.168.1.1



192.168.1.254

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

The factory default login:

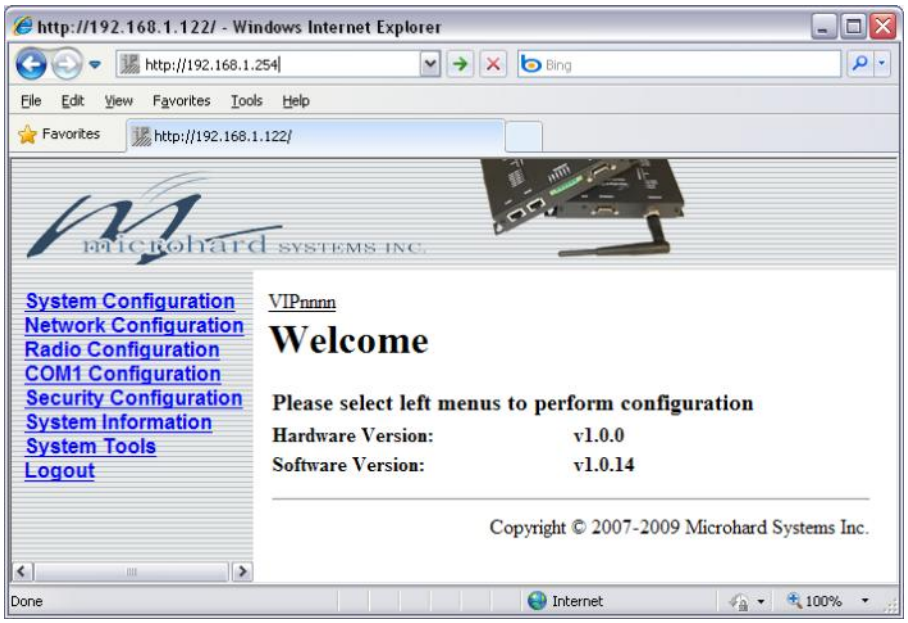
User name: admin
Subnet: admin

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

The Factory default login:

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

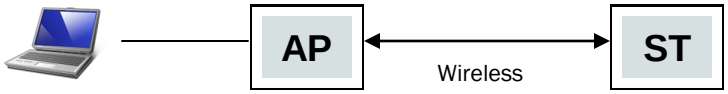
✓ Once successfully logged in, the Welcome Window will be displayed.



2.0 Quick Start

2.2 Simple Access Point and Station

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



2.2.1 Configuring the Access Point

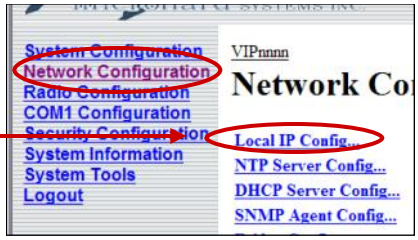
✓ Use ***Section 2.1*** *Getting Started* to connect, power up and log in to a VIP Series unit.

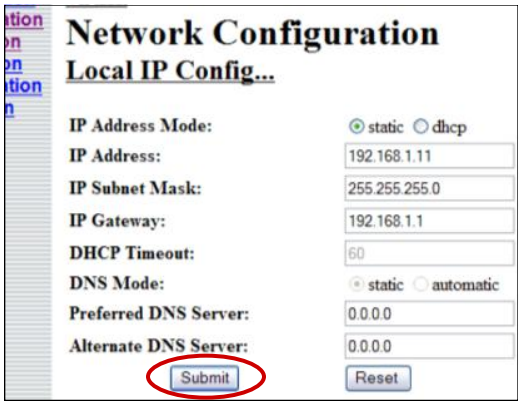
✓ Give the VIP Series unit a unique IP address.

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

Select ***Network Configuration*** from the left side navigation.

Select ***Local IP Config...*** from the displayed list.





Choose *static* for the ***IP Address Mode***.

Enter the following Network Information:

IP Address: 192.168.1.11
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

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

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

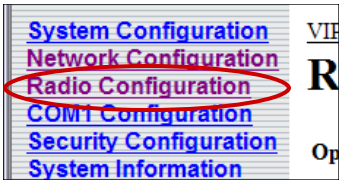
Refer to **Section 6.1.4.1** *Local IP Configuration* for additional information.

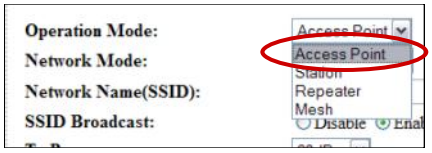
2.0 Quick Start

2.2.1 Configuring the Access Point (Con't)

✓ Configure the VIP Series as a Access Point

Select ***Radio Configuration*** from the left side navigation.

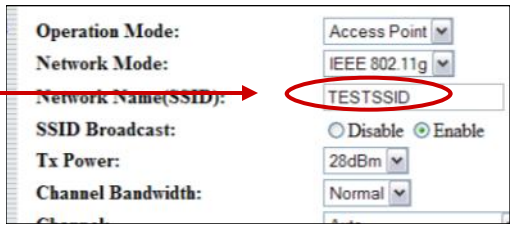


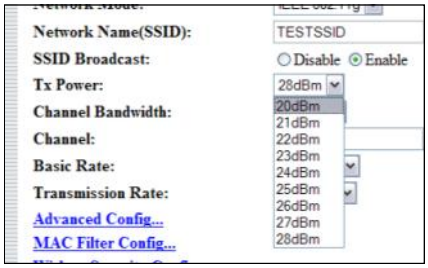


Select Access Point from the ***Operation Mode*** dropdown box.

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

TESTSSID





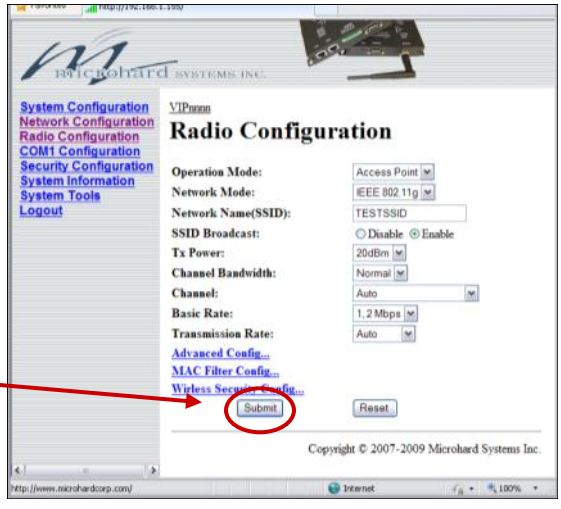
For testing it is best to use the lowest power setting to prevent RF saturation. Select 20dBm from the ***TX Power*** setting.

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

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

Refer to **Section 6.1.5** *Radio Configuration* for additional information.

Click on the **Submit** button to write the changes to the VIP Series. The **Reset** button will revert back to previously saved values



2.0 Quick Start

2.2.2 Configuring the Station

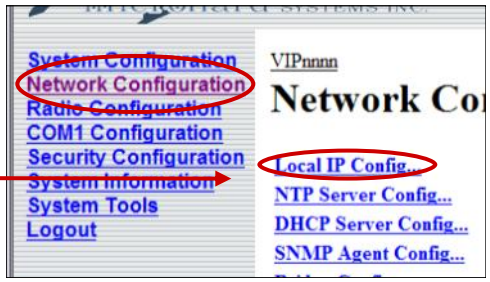
The following procedure describes the steps required to set up a VIP Series unit as a Station (ST). A Station provides a single wireless connection (i.e to an Access Point) and provides a wired connection to a PC or other devices.

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

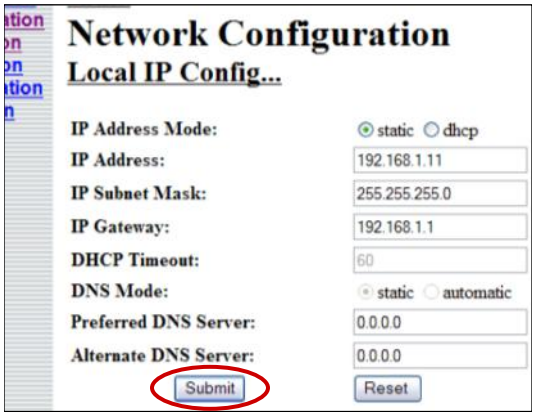
✓ Give the VIP Series unit an unique IP address.

Select ***Network Configuration*** from the left side navigation.

Select ***Local IP Config...*** from the displayed list.



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



Choose *static* for the ***IP Address Mode***.

Enter the following Network Information:

IP Address: 192.168.1.12
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

Click on the **Submit** button to write the changes to the VIP Series. The **Reset** button will revert back to previously saved values.

Refer to **Section 6.1.4.1** *Local IP Configuration* for additional information.

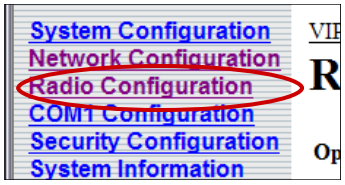
Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.

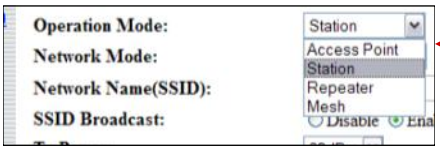
2.0 Quick Start

2.2.2 Configuring the Station (Continued)

✓ Configure the VIP Series as a Station.

Select ***Radio Configuration*** from the left side navigation.

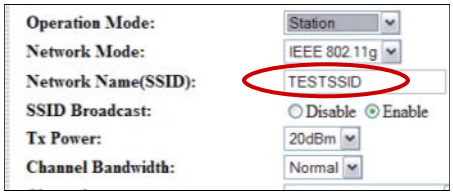


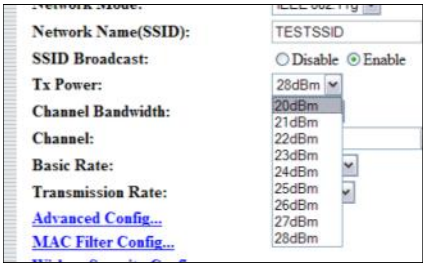


Select Station from the ***Operation Mode*** dropdown box.

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

TESTSSID



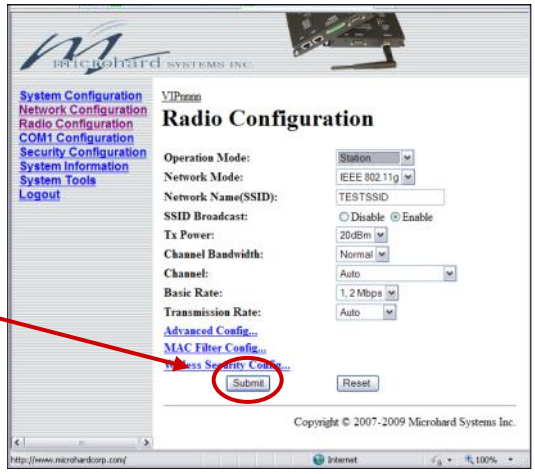


For testing it is best to use the lowest power setting to prevent RF saturation. Select 20dBm from the ***TX Power*** setting.

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

Refer to **Section 6.1.5** *Radio Configuration* for additional information.

Click on the **Submit** button to write the changes to the VIP Series. The **Reset** button will revert back to previously saved values



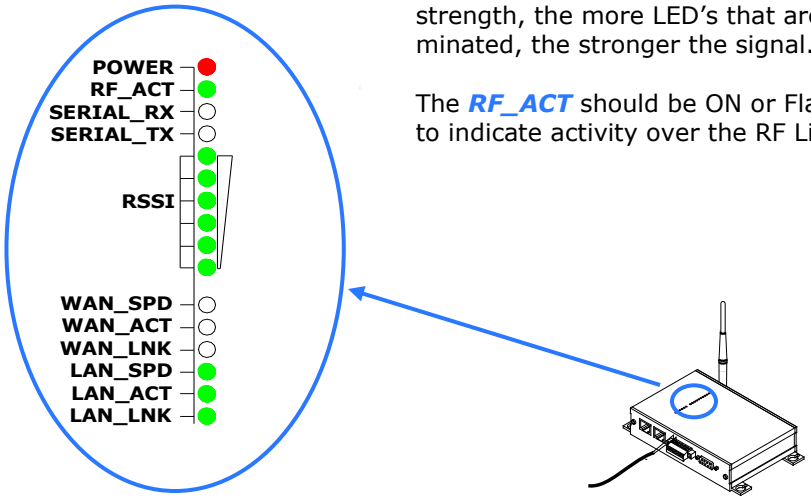
If any additional settings need to be changed, ensure they are also changed on the Station.

2.0 Quick Start

2.2.3 Testing the connection

✓ Visually check to see if the VIP Series units are communicating.

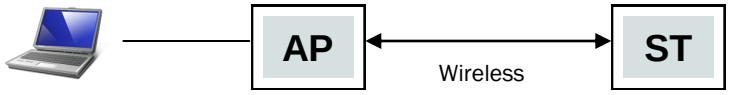
RSSI LED's that are 'cycling' or 'scanning' indicate that the unit is searching for a signal.



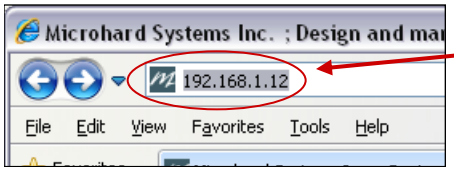
The ***RSSI*** LED's represent signal strength, the more LED's that are illuminated, the stronger the signal.

The ***RF_ACT*** should be ON or Flashing to indicate activity over the RF Link.

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



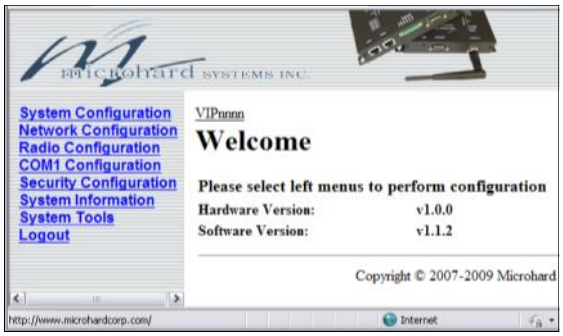
If any additional settings need to be changed, ensure they are also changed on the Station.



Open a browser and type in the address of the station: ***192.168.1.12***

Log into the unit.

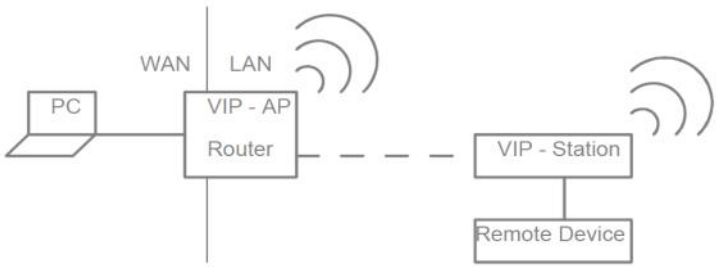
The welcome screen should be displayed



2.0 Quick Start

2.3 VIP in Router Mode

This **Quick Start** example requires (2) VIP Series units, one will be configured as a Access Point (AP) to be used as a Router, the second unit will be configured as a Station (ST) connected to a PC or remote device. This example will show the basic steps required to set up each unit so that a simple network will be established.



2.3.1 Configuring the Access Point in Router mode

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

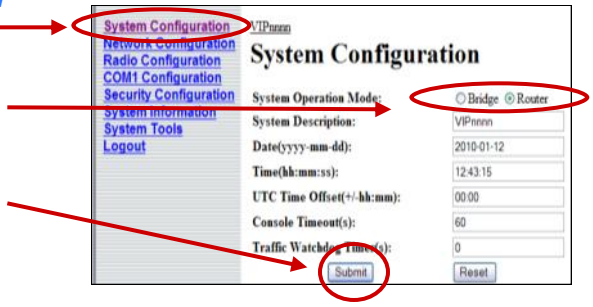
To connect to an existing network, contact your Network Administrator for valid network settings.

✓ Configure the VIP Series unit as a Router.

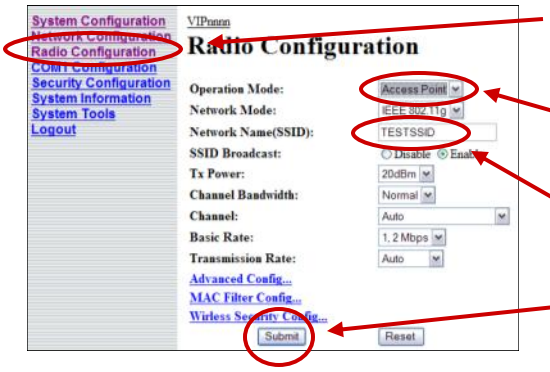
Select ***System Configuration*** from the left side navigation.

Select Router for the ***System Operating Mode***.

Click on the **Submit** button to write the changes to the VIP.



✓ Configure the VIP Series unit as a Access Point.



Select ***Radio Configuration*** from the left side navigation.

Select Access Point from the ***Operation Mode*** dropdown box.

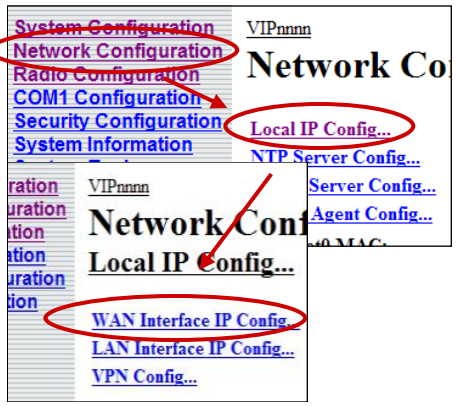
Enter a unique ***Network Name (SSID)***.

Click on the **Submit** button to write the changes to the VIP.

2.0 Quick Start

2.3.1 Configuring the Access Point in Router mode (Con't)

✓ Configure the WAN Interface. In router mode the ethernet interface is split into two parts, WAN and LAN.



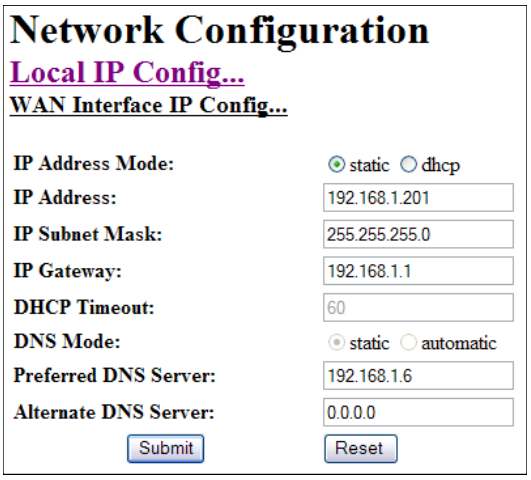
From ***Network Configuration*** select ***Local IP Config***.

Select ***WAN Interface IP Config***.

In ***dhcp*** mode *IP* settings are assigned automatically by DHCP server. Select *static* mode for ***IP Address Mode*** and **DNS mode** to manually enter *IP* settings as follows:

IP Address Mode: Static
IP Address: 192.168.1.201
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

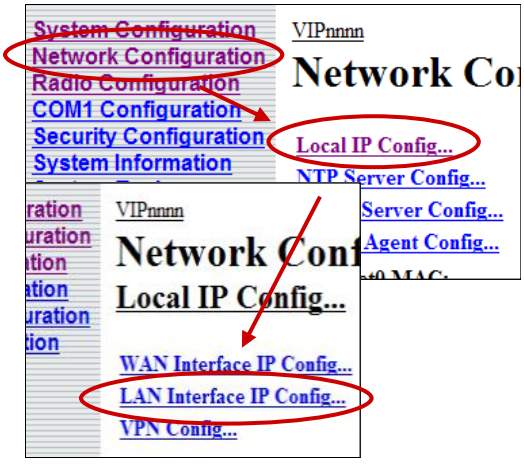
Preferred DNS Server: 192.168.1.6
Alternate DNS Server: 0.0.0.0



✓ Configure the LAN Interface.

From ***Network Configuration*** select ***Local IP Config***.

Select ***LAN Interface IP Config***.



2.0 Quick Start

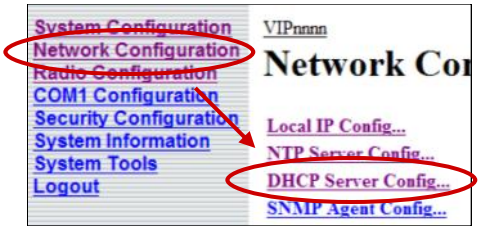
2.3.1 Configuring the Access Point in Router mode (Con't)

✓ Configure the LAN Interface. (Con't)

Enter the following network settings for the ***LAN Interface IP Config...***:

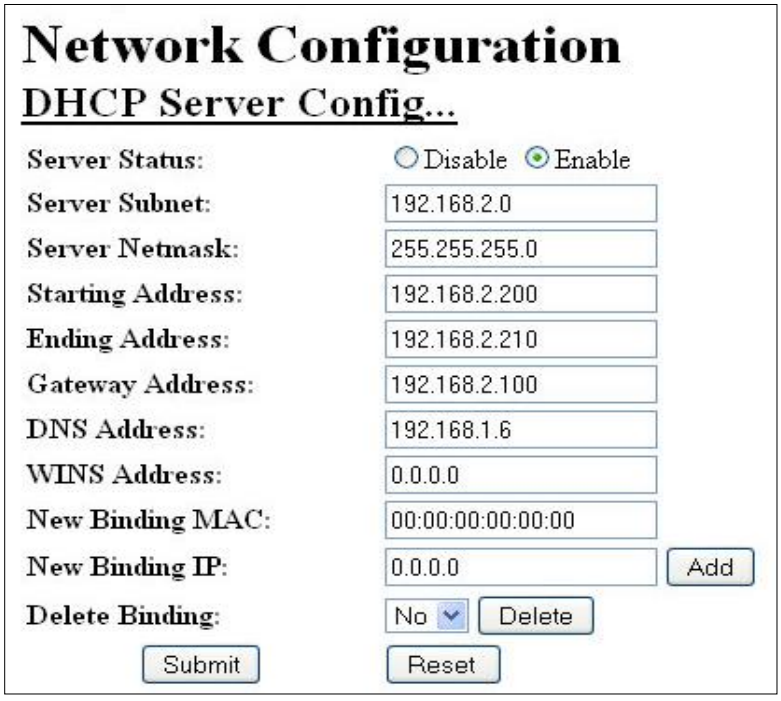
IP Address: 192.168.2.201
IP Subnet Mask: 255.255.255.0

✓ Configure the DHCP Server, Enter the values as shown below. Alternatively remote devices can have static IP addresses.



From ***Network Configuration*** select ***DHCP Server Config...***

Enter the ***DHCP Server Config...*** information as shown below:



2.0 Quick Start

2.3.2 Configuring the Station (For AP Router)

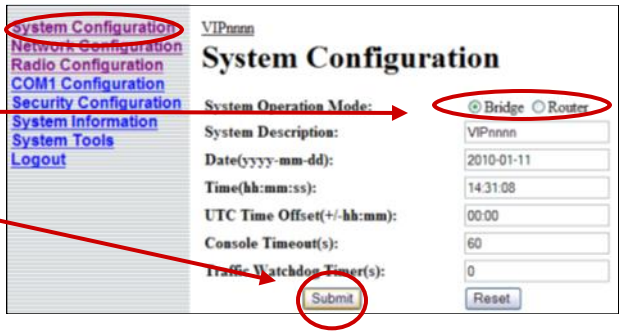
✓ Use ***Section 2.1*** *Getting Started* to connect, power up and log in to a second VIP Series unit to be used on the wireless network.

✓ Configure the unit as a Bridge.

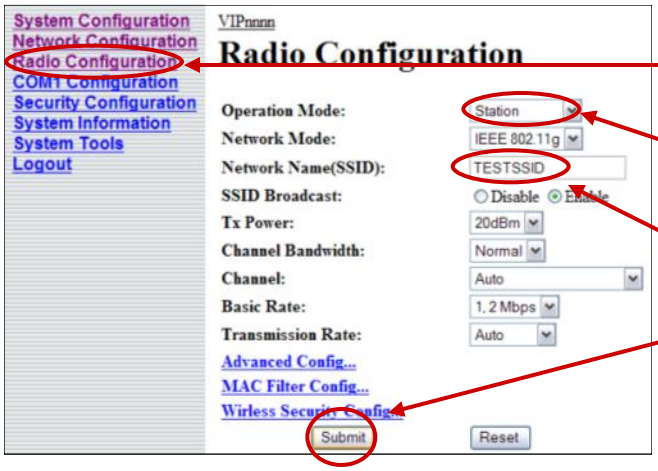
Select ***System Configuration*** from the left side navigation.

Select Bridge for the ***System Operating Mode***.

Click on the **Submit** button to write the changes to the VIP.



✓ Configure the unit as a Station.



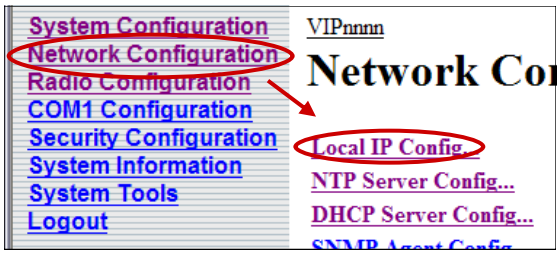
Select ***Radio Configuration*** from the left side navigation.

Select Station from the ***Operation Mode*** dropdown box.

Enter a ***Network Name(SSID)*** matching the one entered for the Access Point.

Click on the **Submit** button to write the changes to the VIP.

✓ Configure the Network Settings.

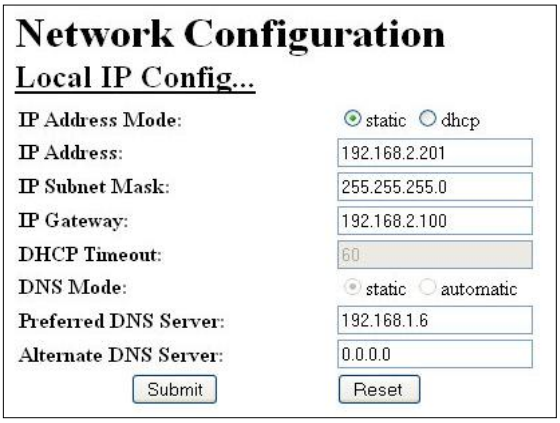


From ***Network Configuration*** select ***Local IP Config...***

2.0 Quick Start

2.3.2 Configuring the Station (For AP Router)

✓ Configure the Network Settings. (Continued)



In *dhcp* mode Network *IP* settings are assigned automatically by the DHCP server configured on the VIP Access Point.

Optionally *IP* settings can be entered manually by selecting *static* mode as below.

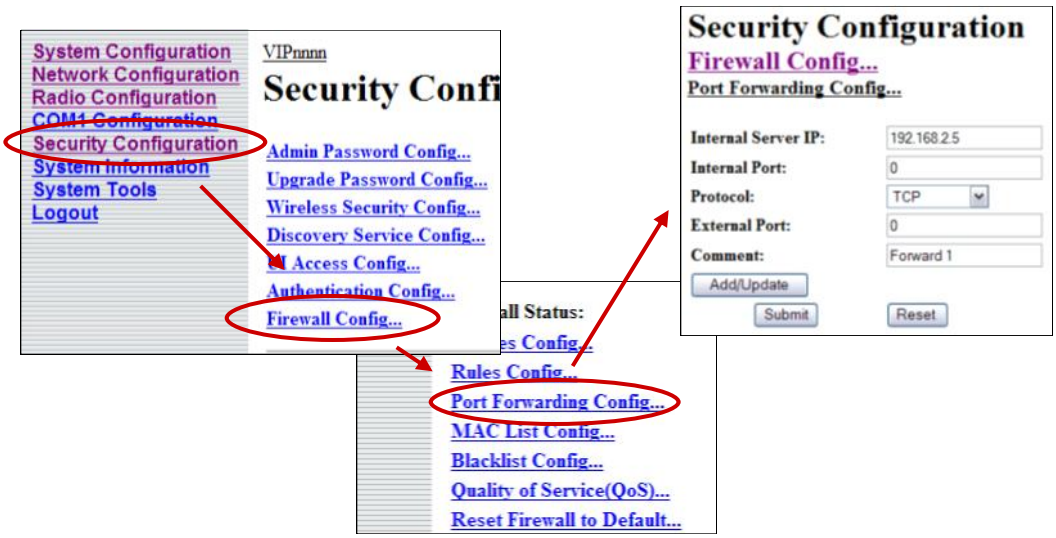
IP Address Mode: Static
IP Address: 192.168.2.201
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.2.100

Preferred DNS Server: 192.168.1.6
Alternate DNS Server: 0.0.0.0

✓ In this configuration, devices on the Local Area Network can talk to each other and communicate with the devices on the Wide Area Network as well. But devices on the WAN can't initiate communications with devices on the LAN.

2.3.3 Port Forwarding Configuration

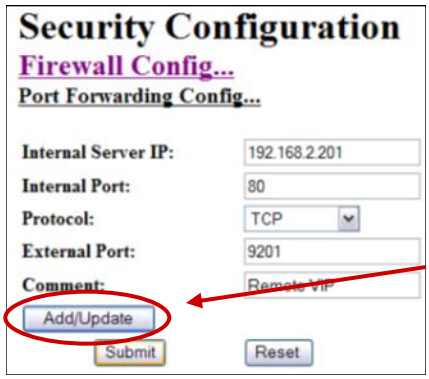
✓ On the VIP Access Point configured in ***Section 2.3.1 Configuring the Access Point in Router Mode***, select **Security Configuration** → **Firewall Config** → **Port Forwarding Config**.



2.0 Quick Start

2.3.3 Port Forwarding Configuration (Continued)

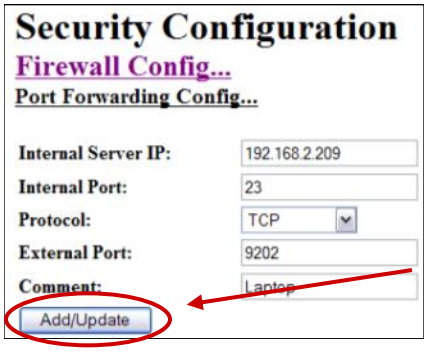
✓ Add two devices to the list, and configure as follows.



First device, remote VIP
Internal Server IP: 192.168.2.201
Internal Port: 80
Protocol: TCP
External Port: 9201
Comment: Remote VIP

Click the **Add/Update** button once all the fields are populated as described above.

The entry should be added to the ***Port Forwarding Summary*** as seen below:

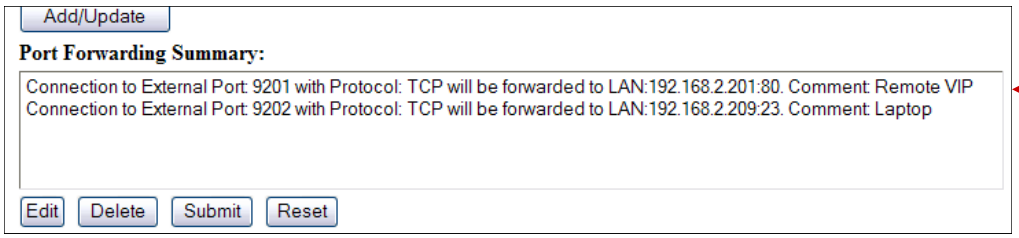


Second device, remote computer
Internal Server IP: 192.168.2.209
Internal Port: 23
Protocol: TCP
External Port: 9202
Comment: Laptop

Click the **Add/Update** button once all the fields are populated as described above.

The entry should be added to the ***Port Forwarding Summary*** as seen below:

Once all entries are entered, click the **Submit** button to write the changes to the VIP.



2.0 Quick Start

2.3.3 Port Forwarding Configuration (Continued)

✓ Turn on the Firewall.

Click on ***Firewall Config...*** from the last menu or **Security Coniguration** > ***Firewall Config...***

Select the *Enable* option from the ***Firewall Status:.***

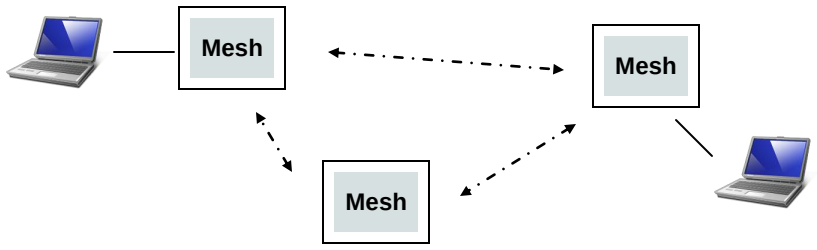
Click on the **Submit** button to send the changes to the VIP Series.

✓ Once the firewall is enabled, you can login into a remote IP from any browser with the following command: <192.168.1.201:9201> or the remote laptop with telnet if the telnet service is enabled: <telnet 192.168.1.201.9202>

2.0 Quick Start

2.4 Simple Mesh Network

This **Quick Start** example requires (2 or more) VIP Series units, This example will show the basic steps required to set up each unit so that a simple Mesh network will be established.

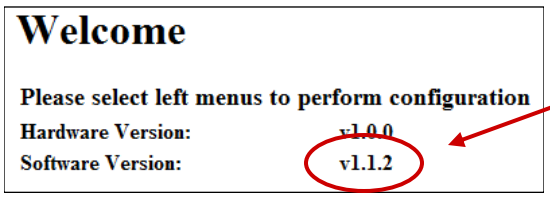


2.4.1 Configuring the Mesh Node(s)

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

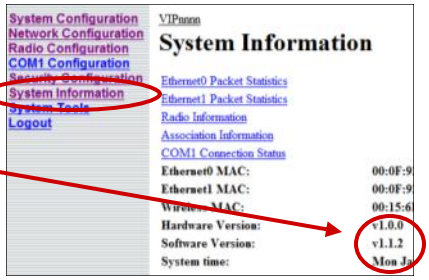
✓ Ensure Mesh Networking is supported by confirming that the software version of each VIP is v1.0.10 or later.

The configuration of each Mesh Node is very similar, the difference between units being each unit requires a different IP address.



From the **Welcome** screen you can see the current hardware and software versions of the VIP.

The software version can also be found in the ***System Information*** menu on the left side navigation

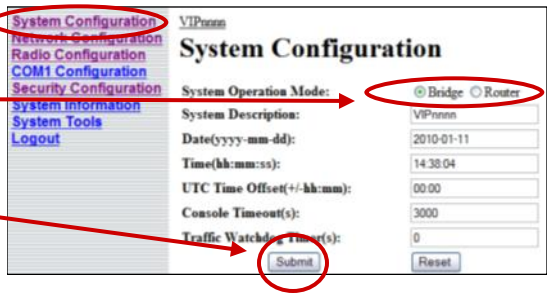


✓ Configure all VIP Series units as Bridges.

Select ***System Configuration*** from the left side navigation.

Select Bridge for the ***System Operating Mode***.

Click on the **Submit** button to write the changes to the VIP.

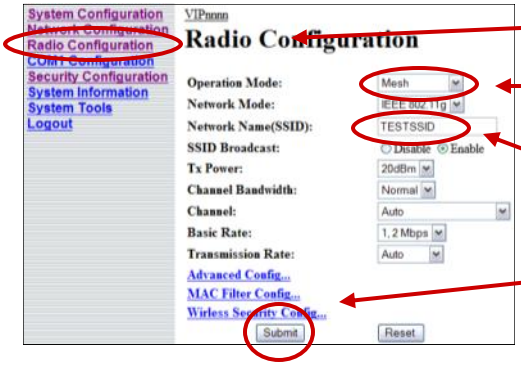


2.0 Quick Start

2.4.1 Configuring the Mesh Node (s) (Continued)

✓ Configure all VIP Series units as a Mesh nodes.

Each unit in a Mesh network must have the same SSID



Select ***Radio Configuration*** from the left side navigation.

Select Mesh from the ***Operation Mode*** dropdown box.

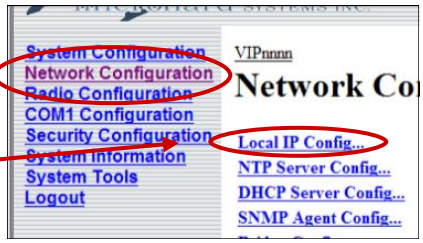
Enter a unique ***Network Name (SSID)***.

Click on the **Submit** button to write the changes to the VIP.

✓ Assign each VIP unit a unique IP Address.

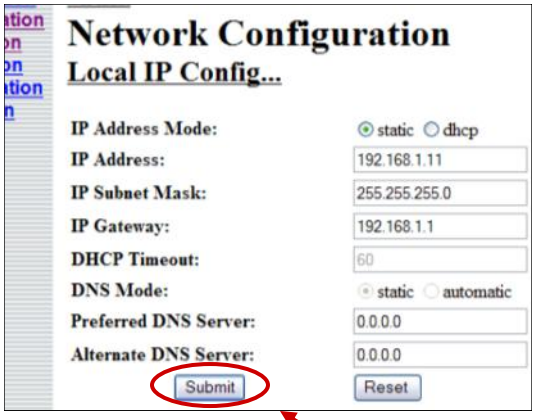
Select ***Network Configuration*** from the left side navigation.

Select ***Local IP Config...*** from the displayed list.



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

Each unit in a Mesh network must have a different IP address.



Refer to **Section 6.1.4.1** *Local IP Configuration* for additional information.

Choose *static* for the ***IP Address Mode***.

Assign each VIP a unique IP address.

Network Information for first VIP unit:
IP Address: 192.168.1.**11**
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

Network Information for second VIP unit:
IP Address: 192.168.1.**12**
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

Network Information for Third VIP unit:
IP Address: 192.168.1.**13**
IP Subnet Mask: 255.255.255.0
IP Gateway: 192.168.1.1

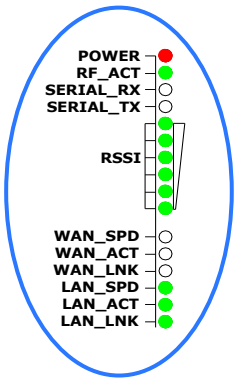
Click on the **Submit** button to write the changes to the VIP Series. The **Reset** button will revert back to previously saved values.

2.0 Quick Start

2.4.1 Configuring the Mesh Node (s) (Continued)

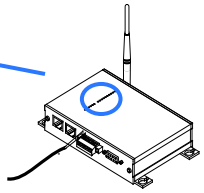
✓ Configure any additional VIP units as Mesh Nodes as required. Ensure each unit has a unique IP address. All units must also be on the same SSID.

✓ Once all units are configured and running, visually check to see if the VIP Series units are communicating by looking at the RSSI LED's on the VIP Series units.

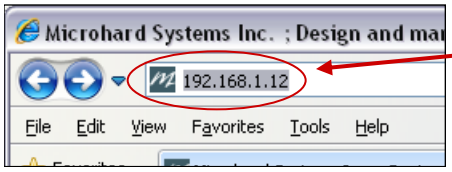


The ***RSSI*** LED's represent signal strength, the more LED's that are illuminated, the stronger the signal. Each unit should have several solid RSSI LED's once wireless communications have been established.

The ***RF_ACT*** should be ON or Flashing to indicate activity over the RF Link.



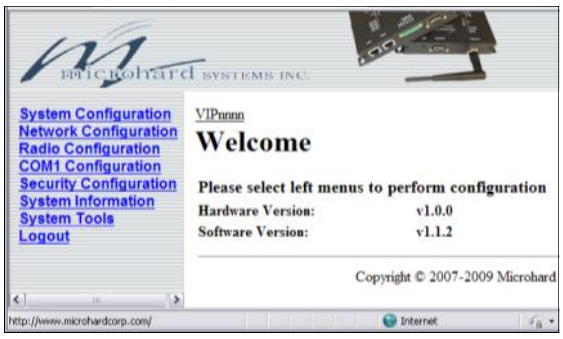
✓ To test the Mesh Network type in the IP address of any of the Mesh Nodes into a browser, a connection should be able to be made to each unit wirelessly.



Open a browser and type in the address of a Mesh Node: ***192.168.1.12***

Log into the unit.

The welcome screen should be displayed



✓ Repeat for each Mesh Node.

2.0 Quick Start

2.5 Text UI Method

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

2.51 Required Materials

- 2 IP Series (with factory default configuration), each with Power Adapter and 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 9-wire straight-through serial cable

*dependent on desired test set-up

2.52 Set-Up Procedure

- Connect antenna to each VIP Series unit.
- Connect the Power Adapters to available 120VAC outlets, and to the VIP Series unit.
- Connect the 9-wire serial cable to CONSOLE (rear) of one VIP Series unit 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**.

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

continued...

2.0 Quick Start

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

View the PC's NETWORK SETTINGS (TCP/IP Properties) to determine an appropriate IP Address, Subnet Mask, and Gateway for the 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(s) so as not to potentially create an IP address conflict.

- Input suitable (for your PC/network) values for:
    - **IP Address**
    - **Subnet Mask**
    - **Gateway**
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] twice to return to the MAIN MENU.
- Select Option **C: Radio Configuration**, then
    - **A: Operation Mode**, then
        - **A: Access Point**
- 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 Access Point (AP) for your wireless network.

Remove the serial cable connection from the Access Point's CONSOLE port and move it to the CONSOLE port of the other VIP Series unit.

- 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
    - **A: Operation Mode**, then
        - **B: Station**
- Press **U** to SAVE the configuration changes.
- Press [***Esc***] to return to the MAIN MENU.
- Press **Q** to Quit.

The VIP Series configured above is now the STATION for your wireless network.

With these two VIP Series units 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 (6 top panel green LEDs) are illuminated.

Next, the ethernet connections will be made.

continued...

2.0 Quick Start

2.6 Testing IP Data Traffic

To connect a VIP Series unit to the network connection of 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 (wired Local Area Network) 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 LAN (RJ45) connector of the Access Point.
- Using a CROSSOVER cable, connect the PC's NIC card (RJ45) jack to the LAN (RJ45) connector on the Station.

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 VIP Series unit, 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 VIP Series are illuminated.
- Verify RF_ACT (red) LED activity on the front of each IP Series.
- Observe the top of each IP Series, specifically the green LAN_LNK LED: it should be illuminated (indicating proper cabling) and the green LAN_ACT LED should also be flickering—indicating DATA traffic at the LAN 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

3.1 VIP Series

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

Image 3A: Front View of VIP Series

Image 3B: Rear View of VIP Series

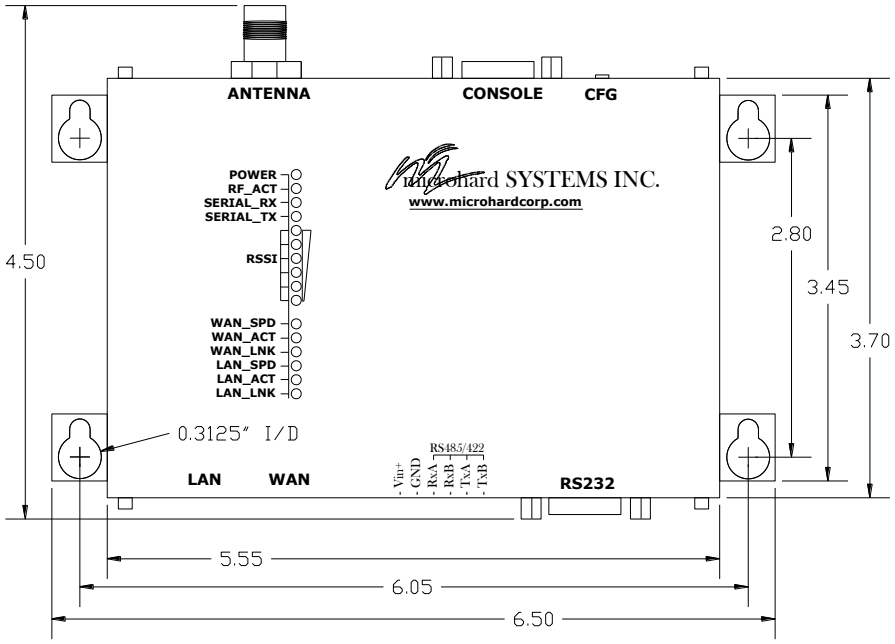
Any VIP Series may be configured as an Access Point (Router or Bridge), Station, Repeater or Mesh Node. This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the device: if you are familiar with one unit, you will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

The stand alone/enclosed version of the VIP Series features:

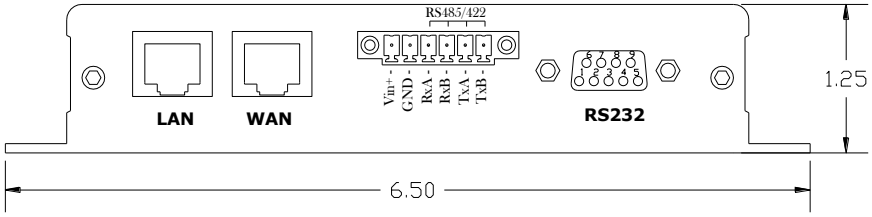
- Standard Connectors for:
  - Dual Ethernet Ports (RJ45)
  - Console Configuration Port (RS232/DB9)
  - Data Port (RS232/DB9)
  - Phoenix Type Connector for Power and RS485/422 Data Port
  - RP-TNC Antenna Connection
- Status/Diagnostic output signals for system status, RSSI, Ethernet etc.
- CFG Button for firmware recovery operations
- Mounting Holes

3.0 Hardware Features

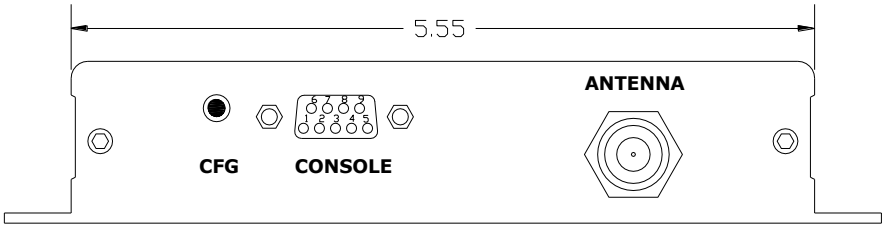
3.1.1 Mechanical Drawings



Drawing 3-1: VIP Top View Dimensions



Drawing 3-2: VIP Front View Dimensions



Drawing 3-3: VIP Rear View Dimensions

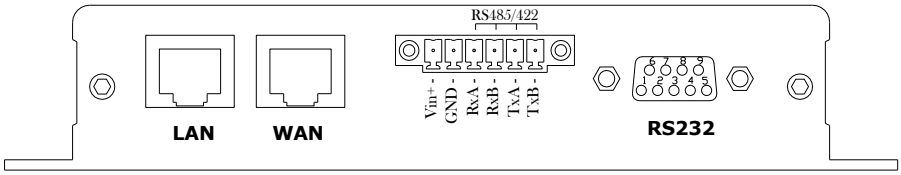
Note: All dimension units: Inches

3.0 Hardware Features

3.1.2 Connections

3.1.2.1 Front

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



Drawing 3-4: VIP Front View

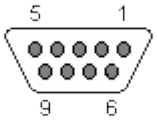
- LAN port
  - RJ45 Connection for the LAN Port.
- WAN port
  - RJ45 Connection for the WAN Port.
- Phoenix-Type Connector: (*Dinkle: EC381-RML-06P*)
  - Vin+ (DC Supply In 9-30 VDC)
  - GND (DC Supply Ground)
  - RxA (RS485/422 RX+)
  - RxB (RS485/422 RX-)
  - TxA (RS485/422 TX+)
  - TxB (RS485/422 TX-)
  - RS485/422 Connections: Used to interface the VIP Series unit to a DTE with the same interface type (300 baud to 921kbps).
- RS232

  (DCE) on the rear of the VIP Series unit is used forRS232 serial data (300 baud to 230.4kbps) communications.

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

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

3.0 Hardware Features

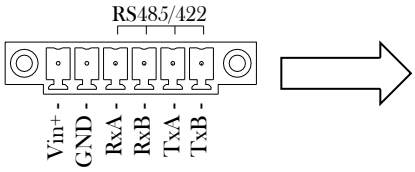


*See **Appendix F** for a full description of the COM1 RS-232 interface functions.*

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 3A: COM1 DE9S Pin Assignment

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

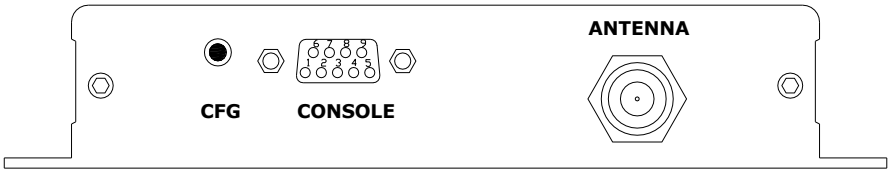


Pin Name	No.	Description	In/ Out
TxB (D+)	1	Non-Inverting Driver Output	O
TxA (D-)	2	Inverting Driver Output	O
RxB (R+)	3	Non-Inverting Driver Input	I
RxA (R-)	4	Inverting Driver Input	I
GND	5	Ground (Power and Signal)	
Vin+	6	Positive Voltage Supply Input (12-30VDC)	I

Table 3B: Phoenix-type Connector Pin Assignment

3.0 Hardware Features

3.1.2.2 Rear



Drawing 3-5: VIP Rear View

CFG Button

Holding this button for 8 seconds while the VIP Series is powered up and running, will cause the unit to reset and load factory default settings:

IP: 192.168.1.254
Subnet: 255.255.255.0
Gateway: 192.168.1.1

With these settings a web browser can be used to configure the unit.

Holding this button depressed while powering-up the VIP 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, Section 6.1.9.1.)

CONSOLE Port

The CONSOLE Port (DE9S, DCE) is used for accessing the Text User Interface (Text UI) of the VIP Series unit.

Default Console Port Settings:

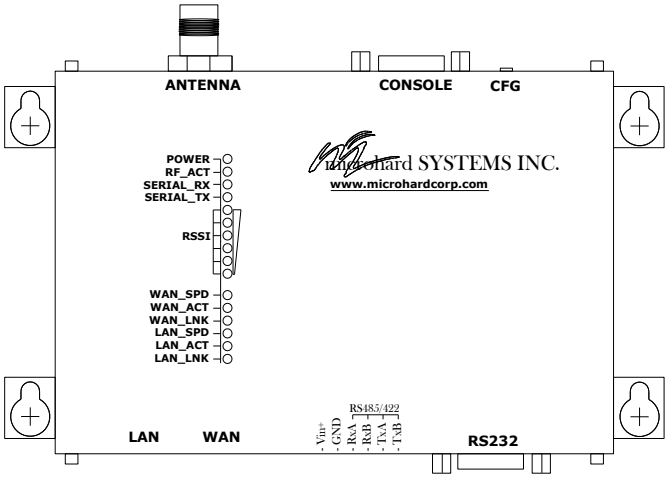
Bits per Second: 115,200
Data Bits: 8
Parity: None
Stop bits: 1
Flow control: None

Antenna Connector

The VIP Series uses a reverse polarity TNC (RP-TNC) connector. Microhard Systems Inc. can provide external cabling and antennas suited to a variety of applications.

3.0 Hardware Features

3.1.3 Indicators



Drawing 3-6: VIP Indicators

Power (Red)
ON indicates DC supply power is being supplied to the unit.

RF_ACT
Illuminates when the unit is transmitting out of its antenna port.

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

COM1_RX
Indicates receive data which was received from the wireless (via antenna) connection is exiting the unit via COM1 towards the DTE.

COM1_TX
Indicates transmit data being input to the VIP Series COM1 wired connection.

RSSI (6 LEDs)
Indicate the received signal strength. If these units are 'scanning', that indicates no reception. Otherwise, from 1 to 6 LEDs will be illuminated, with all 6 being illuminated representing a strong signal.

WAN_SPD
OFF=10Mbps, ON=100Mbps on wired WAN connection.

WAN_ACT
Indicates data activity on the WAN connection.

WAN_LNK
ON indicates a properly-wired WAN connection.

LAN_SPD
OFF=10Mbps, ON=100Mbps on wired LAN connection.

LAN_ACT
Indicates data activity on the LAN connection.

LAN_LNK
ON indicates a properly-wired LAN connection.

3.0 Hardware Features

3.2 SVIP

The SVIP introduces a OEM solution with a single header interface for complete integration into OEM applications. The SVIP incorporates all of the VIP functionality, features, configuration and performance into a single module.

Image 3C: Top View of SVIP Module

Image 3D: Bottom View of SVIP Module

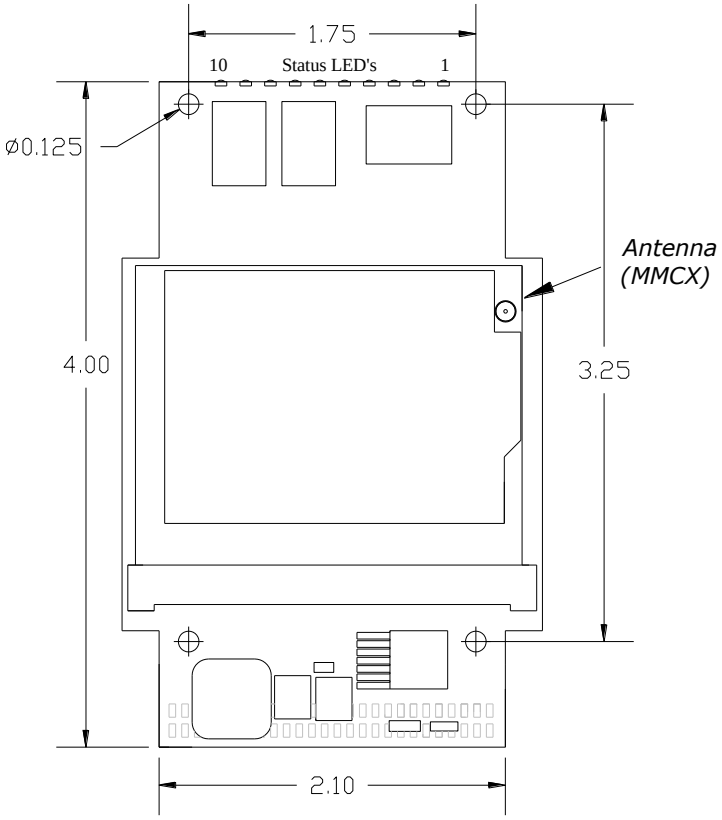
The SVIP Series OEM module features include:

- Single OEM header.
- Single LAN Port (Dual Ports not available on SVIP)
- 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.

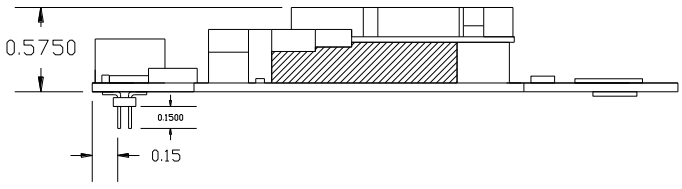
The Pin-out and signal descriptions are described on the following pages. An example customer interface schematic can be found in Appendix I.

3.0 Hardware Features

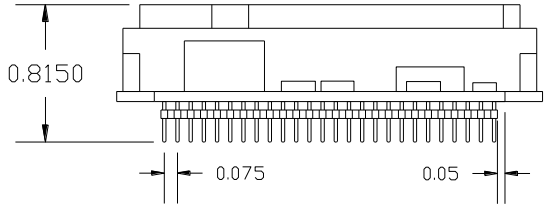
3.2.1 SVIP Mechanical Drawings



Drawing 3-7: SVIP Top View Dimensions



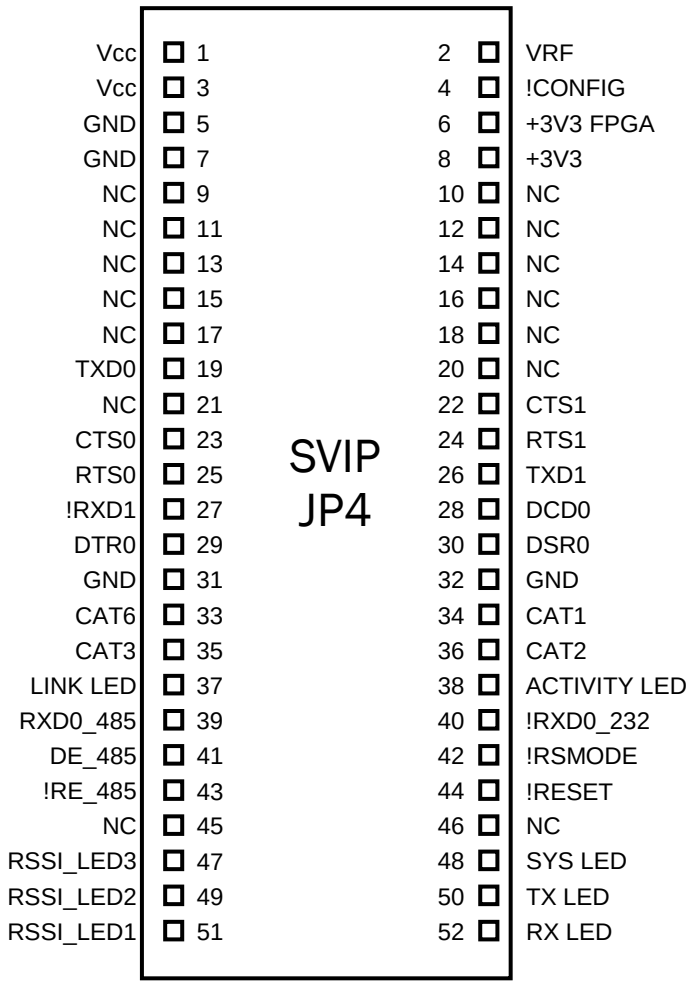
Drawing 3-8: SVIP Side View Dimensions



Drawing 3-9: SVIP End View Dimensions

3.0 Hardware Features

3.2.2 SVIP Pin-Out Description



Drawing 3-10: SVIP 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 SVIP JP4 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 3C: SVIP Pin-Out Description

3.0 Hardware Features

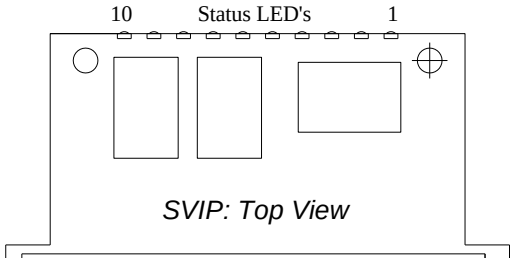
Pin Name	No.	Description	In/ Out
CAT6	33	Ethernet RJ45 Pin 6.	
CAT1	34	Ethernet RJ45 Pin 1.	
CAT3	35	Ethernet RJ45 Pin 3.	
CAT2	36	Ethernet RJ45 Pin 2.	
LINK LED	37	Ethernet LINK LED	O
ACTIVITY LED	38	Ethernet Activity LED	O
RXD0_485	39	Data Port. RS485 Receive Data Logic level input into the modem.	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 3C: SVIP Pin-Out Description (continued)

3.0 Hardware Features

3.2.3 SVIP Indicators

The SVIP has several LED's to indicate the operational status and activity of the SVIP.



Status LEDS	
1 Serial RX	6 STATUS
2 Serial TX	7 SPEED (10/100)
3 RSSI 3	8 N/A
4 RSSI 2	9 LINK/ACT
5 RSSI 1	10 RF ACTIVITY

Drawing 3-10: SVIP Indicators

1. Serial RX
Indicates receive data which was received from the wireless (via antenna) connection is exiting the unit via COM1 towards the DTE.

2. Serial TX
Indicates transmit data being input to the SVIP Series COM1 wired connection.

3 - 5. RSSI (3 LEDs)
Indicate the received signal strength. If these units are 'scanning', that indicates no reception. Otherwise, from 1 to 6 LEDs will be illuminated, with all 6 being illuminated representing a strong signal.

6. STATUS
This LED indicates the System Status. During normal operation this LED will be on.

7. SPEED
OFF=10Mbps, ON=100Mbps on wired LAN connection.

8. N/A
This LED is not used at this time and is reserved for future development.

9. LINK/ACT
ON indicates a properly-wired LAN connection.

10. RF ACTIVITY
Illuminates when the unit is transmitting out of its antenna port.

3.0 Hardware Features

3.2 VIP5800-ANT

The VIP Antenna Series introduces a single unit solution, which integrates a VIP Series unit inside a weather resistant high gain antenna. The VIP5800-ANT can operate as a Access Point, or Repeater providing wireless access anywhere. Utilizing PoE (Power over Ethernet) technology, only a single connection needs to be made to provide all power and data requirements to make the unit operational.

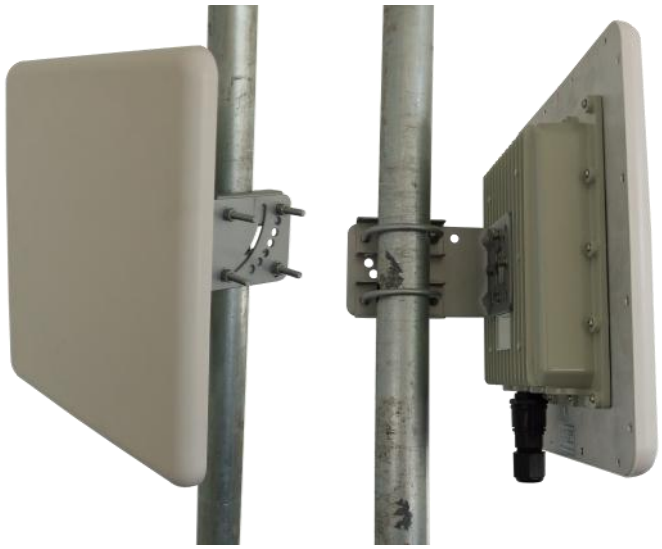


Image 3E: VIP Antenna Series

The VIP Antenna Series feature include:

- Weather Resistant Pole Mounted Enclosure
- Built in high gain antenna
- Single Ethernet/PoE connection, for Ethernet and Power
- PoE Injector and AC Power Adapter
- Remote Configuration

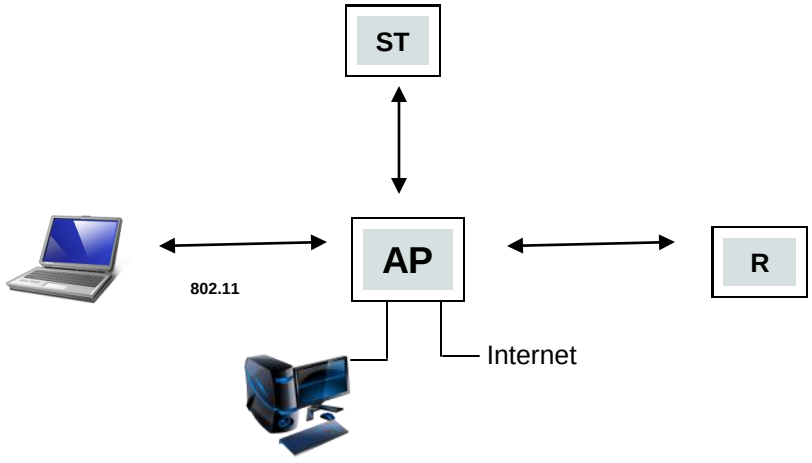
The setup and configuration is done using the Web Interface discussed in Section 6. The default IP address (192.168.1.254), or otherwise set IP address must be known for local configuration through the LAN interface.

4.0 Operating Modes

Each VIP Series Radio can be configured to perform an operational mode defined by the role the unit will perform in the overall network architecture. Any unit can be configured to be an AP, Station, Repeater or Mesh Node, as required. This is convenient in a maintenance and sparing perspective as a single unit could potentially be configured and deployed to replace any unit in the network as required.

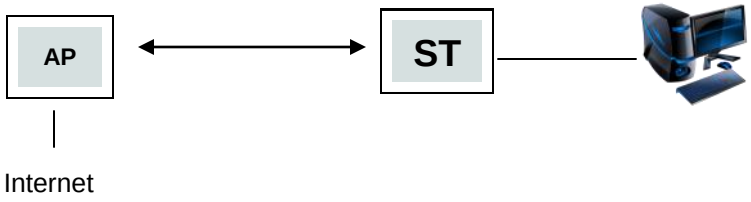
4.1 Access Point

When configured as an access point (AP) the VIP Series will provide a wireless connections to other devices such as other VIP Series units configured as Stations or Repeaters, or other supported wireless devices such as laptops equipped with a compatible wireless card. For example the VIP2400 can support 802.11b and 802.11g network cards. Additionally, an Access Point can be configured as a router or bridge.



4.2 Station

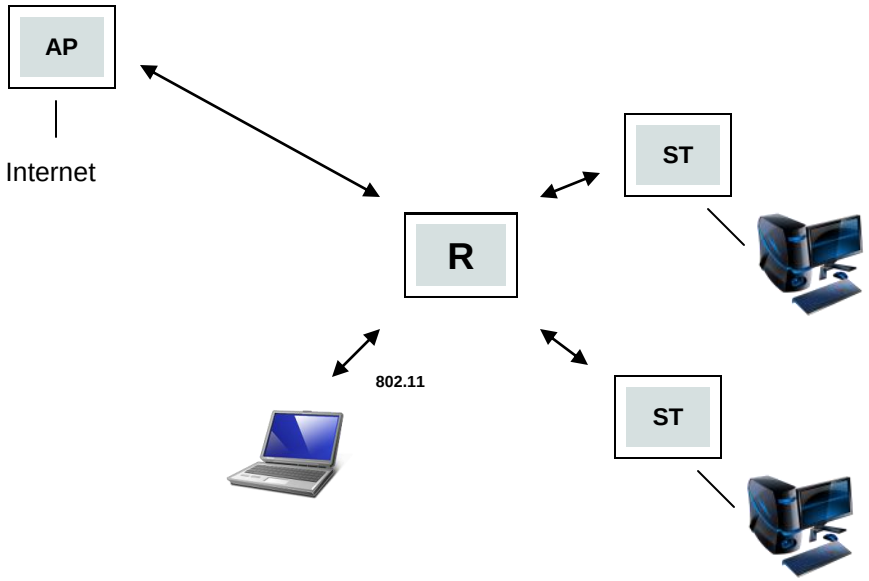
When operating as a station the VIP series can provide a single wireless connection to an access point or a repeater. A station allows a wired ethernet or serial device access to the wireless network.



4.0 Operating Modes

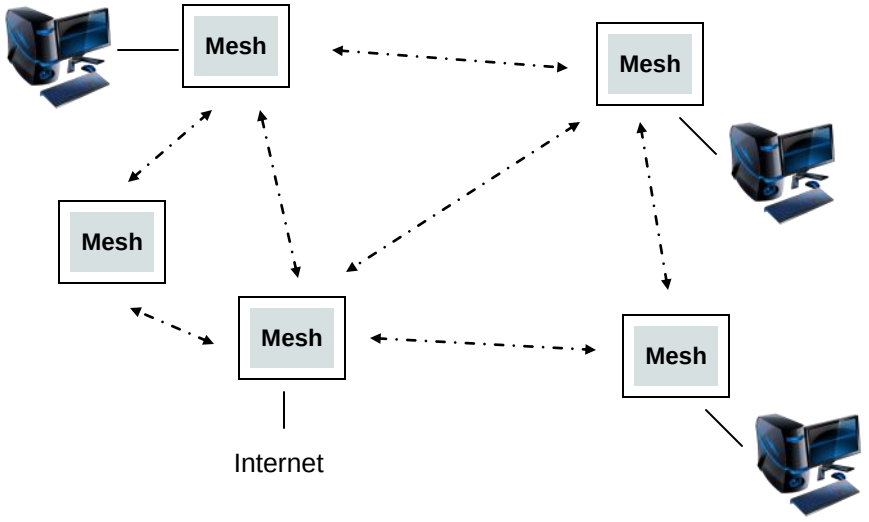
4.3 Repeater

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



4.4 Mesh Node

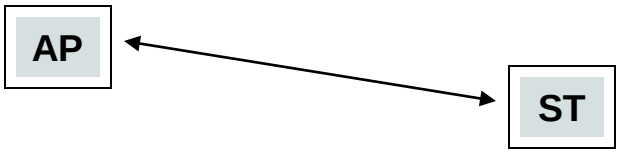
Units can be configured as a Mesh "Node". When multiple units are configured as a Mesh nodes, they automatically establish a network between nodes within range as required by the flow of data. A Mesh Node can then be used as a wireless bridge for a wired ethernet or serial device similar to a Station.



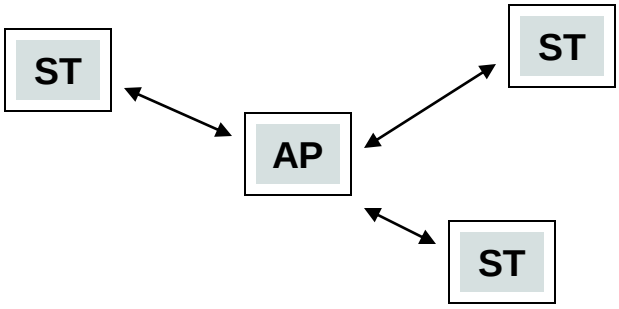
5.0 Network Topologies

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

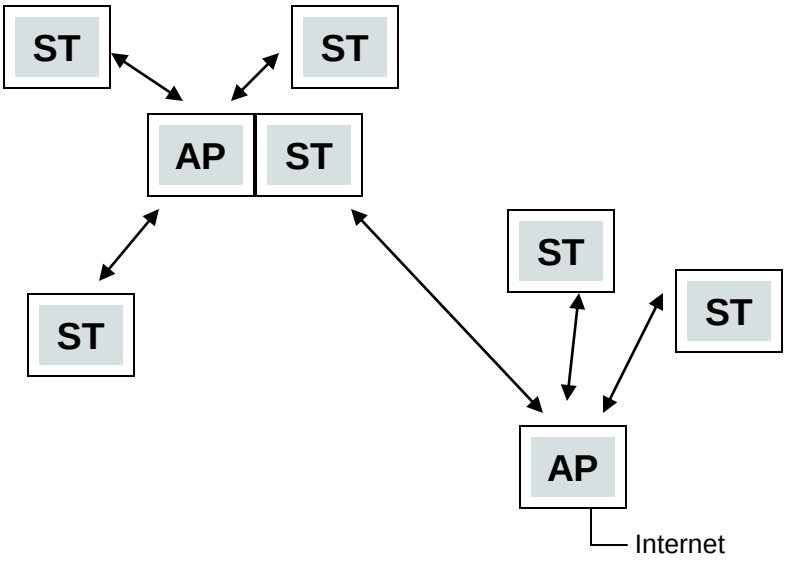
5.1 Access Point to Station



5.2 Access Point to Multiple Stations



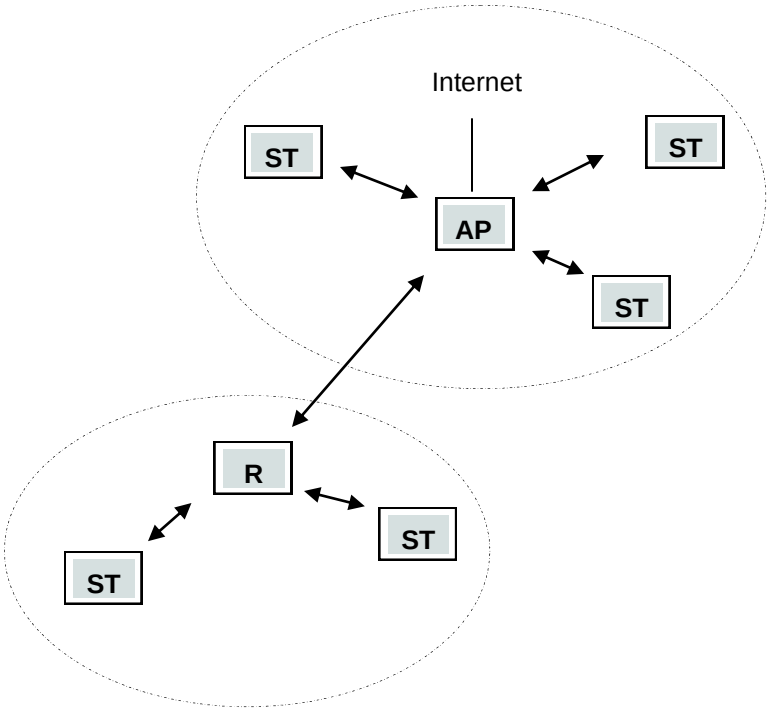
5.3 Access Point with Multiple Stations to AP with Multiple STs



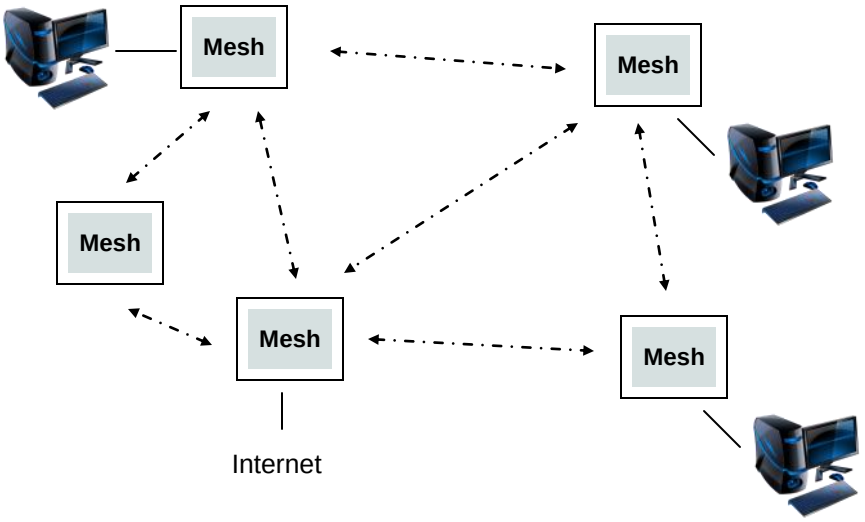
5.0 Network Topologies

5.4 Access Point with Repeater

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



5.4 Mesh



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 VIP Series:

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

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

- CONSOLE connector and a PC running terminal communications program (e.g. HyperTerminal), or
- LAN (ethernet) (RJ45) port, ethernet crossover cable, and PC running Web Browser application.

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

6.0 Configuration

6.1 Web User Interface

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

- connect VIP Series ETHERNET port to PC NIC card using an ethernet **crossover** cable
- apply power to the VIP Series and wait approximately 40 seconds for the system to load
- open a web browser and enter the factory default IP address of the unit: 192.168.1.254
- logon window appears; log on
- configure VIP 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 VIP Series using a Web Browser, the Logon window will appear.

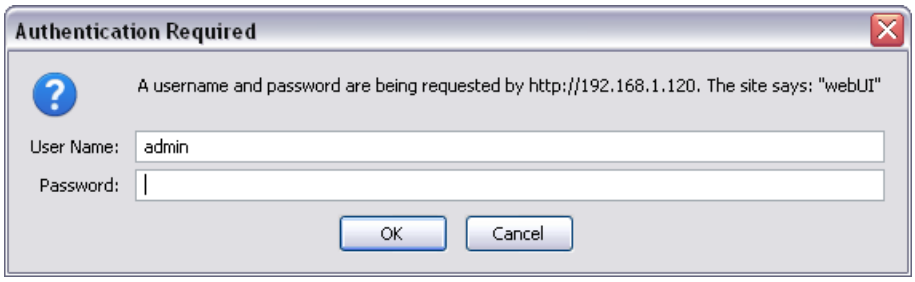


Image 6A: Logon Window

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**

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.

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

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

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

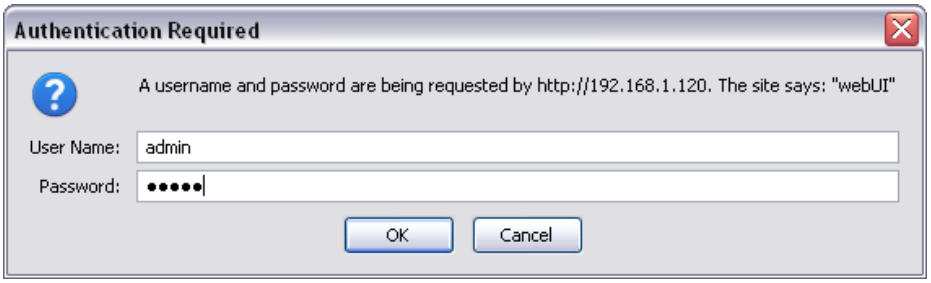


Image 6B: Logon Window : Password Entry

Soft Buttons

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

- Cancel
  Cancels the logon process.

6.0 Configuration

6.1.2 Welcome Window

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

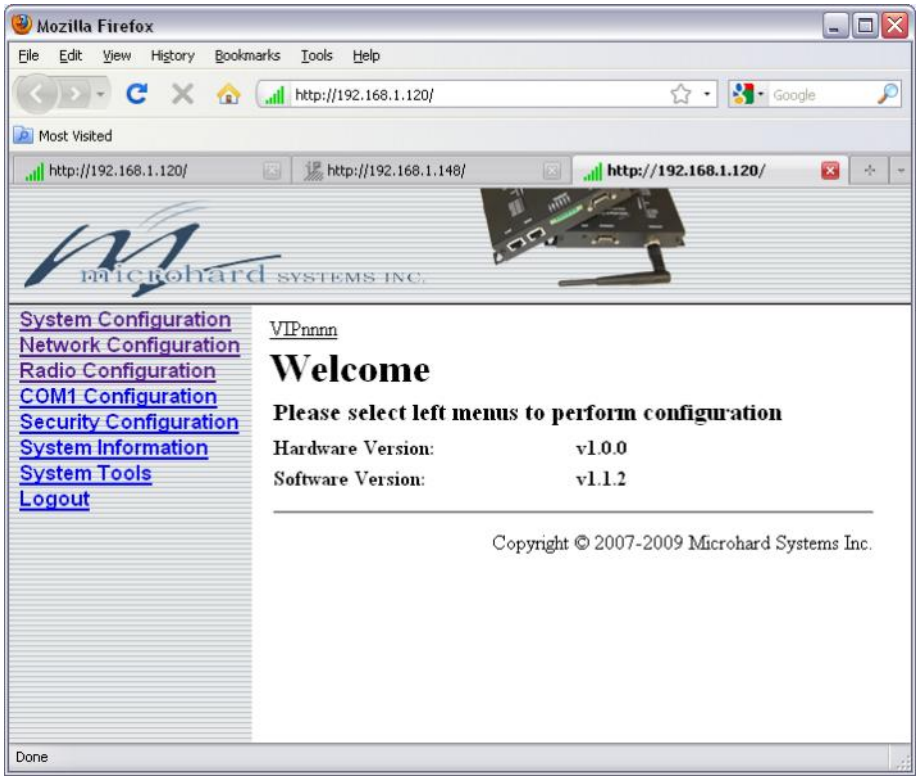


Image 6C: Welcome Window

Also displayed is various 'version' information:

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

6.0 Configuration

6.1.3 System Configuration

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

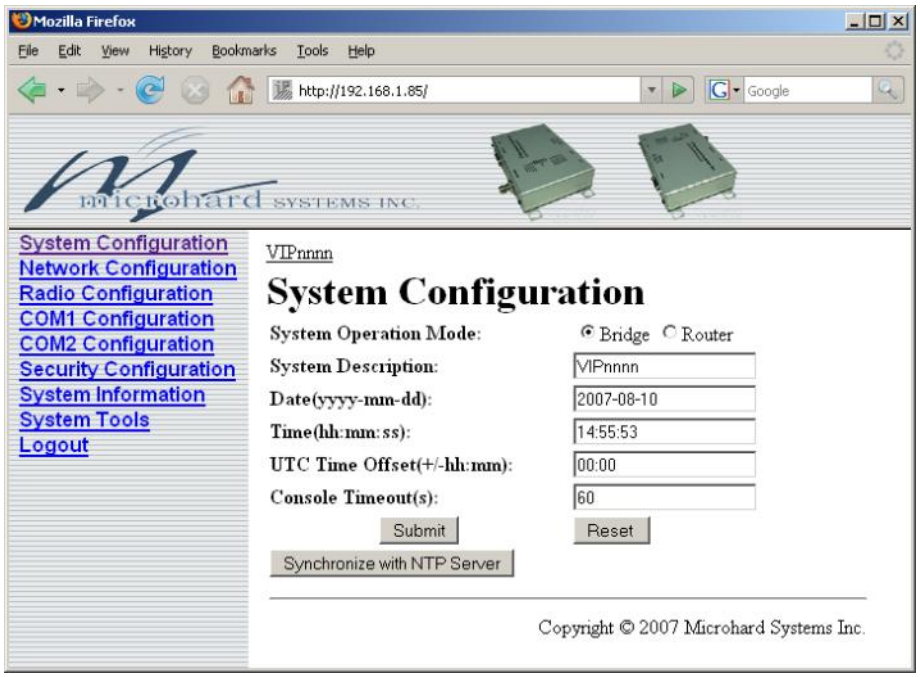


Image 6D: System Configuration Window

System Operation Mode

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

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

Values
Bridge
Bridge Router

6.0 Configuration

The System Description must not be confused with the **Network Name (SSID)** (Radio Configuration menu). The Network Name MUST be exactly the same on each unit within a VIP Series network.

System Description

The System Description is simply a convenient identifier for a specific VIP Series unit, e.g. Tower 7, 456 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

VIPnnnn

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 VIP 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 time may be entered in this field. Note that the entered value is lost should the VIP 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 will timeout after becoming inactive.

Values

seconds

60

0-65535

Soft Buttons

- Synchronize with NTP Server
  Used 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 the VIP Series' memory.

- Reset
  Restore 'currently' modified parameter values to those which were previously written into the VIP 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 a VIP Series network.

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

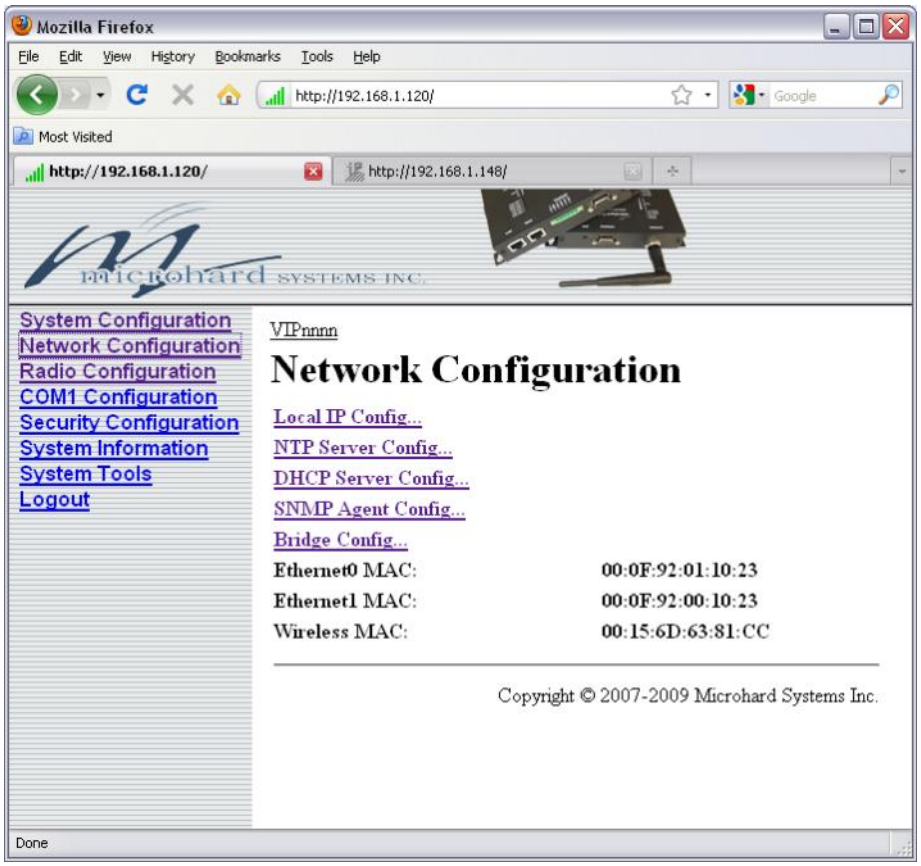


Image 6E: Network Configuration, Top Level Menu

The Ethernet0 MAC address (as displayed above) applies to the wired WAN connection; Ethernet1 MAC is for the wired LAN connection.

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 VIP 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.

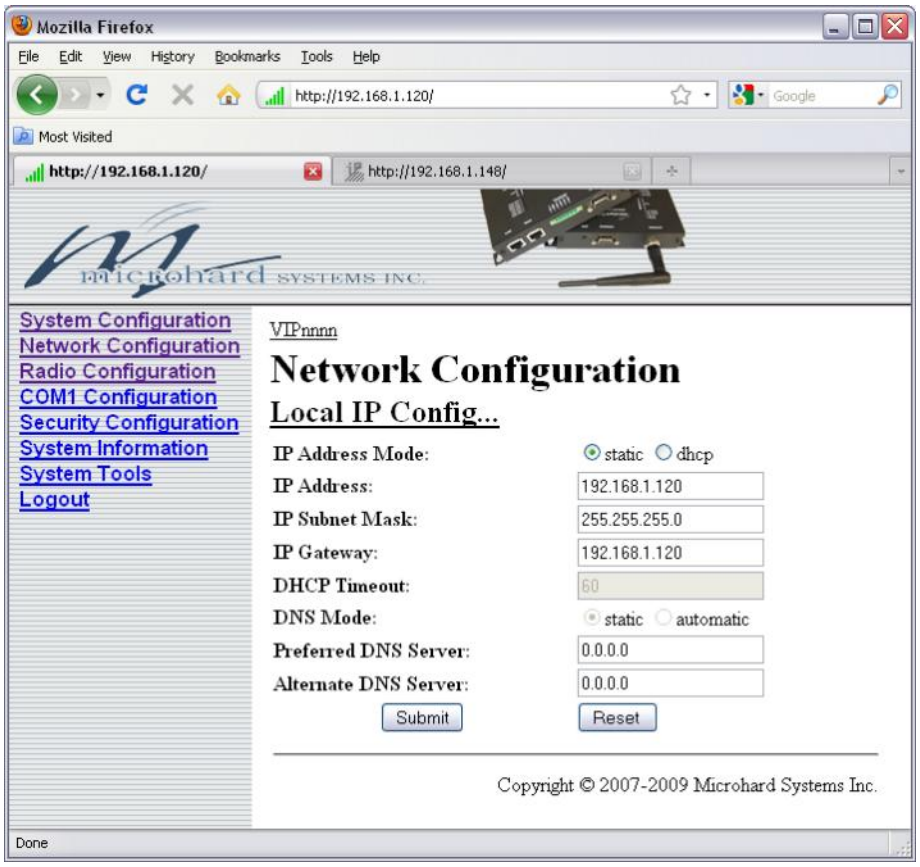


Image 6F: Network Configuration (Bridge), Local IP Configuration Submenu

IP Address Mode

If 'static' is selected, the three following fields are to be manually populated with values which will suit the network/devices to which the VIP 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

IP Address

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

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

Values

192.168.1.254

valid value is specific to the network

Subnet Mask

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

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

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

If DHCP mode is selected (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

IP Gateway

If the VIP 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.

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.

In a very small network, 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 VIP Series units are being used, make the gateway of VIP Series No. 1 = VIP address of VIP Series No. 2; gateway of VIP Series No. 2 = VIP address of VIP Series No. 1. The idea behind this approach is: If a VIP 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 VIP 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 VIP Series unit 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

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

6.0 Configuration

6.1.4.1 Local IP Configuration

6.1.4.1.2 Router

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

Only a VIP Series Access Point should be configured as a Router.

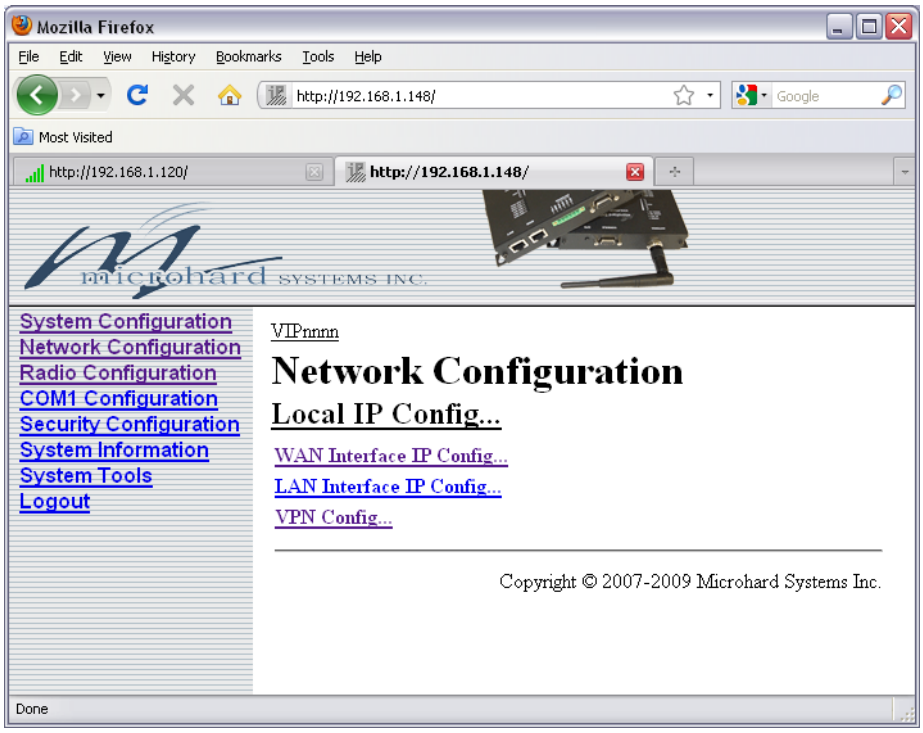


Image 6G: Network Configuration (Router), Local IP Config Submenu

6.0 Configuration

6.1.4.1.2.1 WAN Configuration

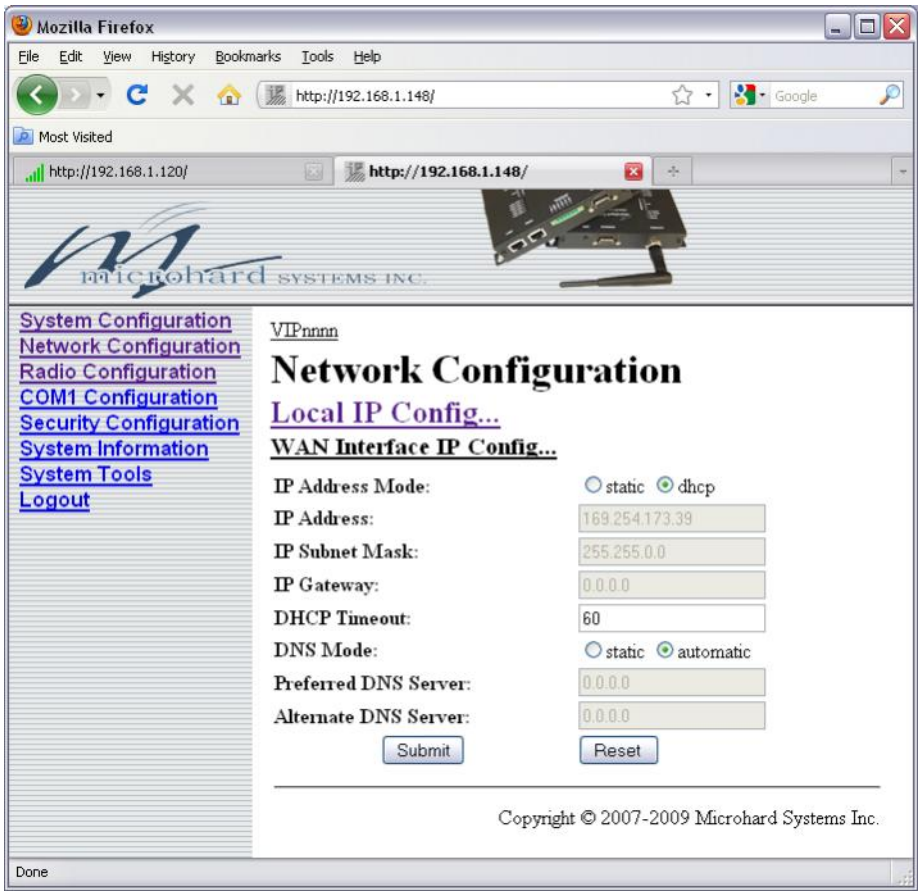


Image 6H: Network Configuration (Router), WAN Interface IP Config

If in ROUTER mode and the address mode is DHCP (default) and there is no wired WAN connection (i.e. to network with a DHCP server), all 6 RSSI LEDs will flash simultaneously to indicate that there is something amiss.

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

IP Address Mode

Values

static
dhcp

IP Address

Desired IP address of unit.

Values

192.168.2.1
valid value is specific to the network, typically a Class C private IP

6.0 Configuration

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

Gateway

IP address of gateway.

Values

192.168.1.1

valid value is specific to the network

DHCP Timeout

This value determines for how long the VIP Series unit 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

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

6.0 Configuration

6.1.4.1.2.2 LAN Configuration

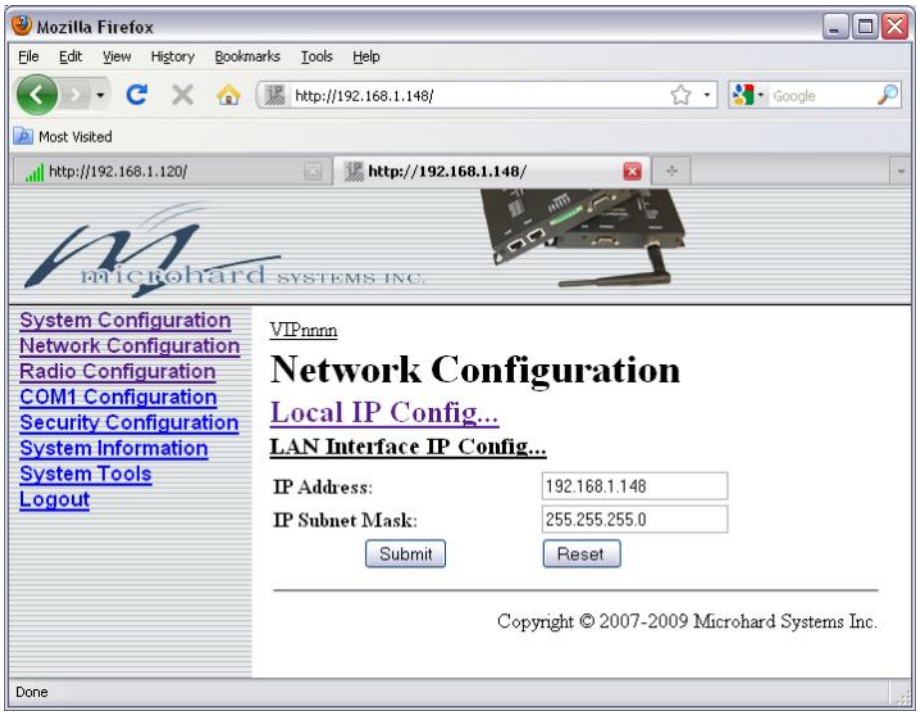


Image 6I: Network Configuration (Router), LAN Interface IP Config

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

192.168.1.254
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

6.1.4.1.2.3 VPN Configuration

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

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

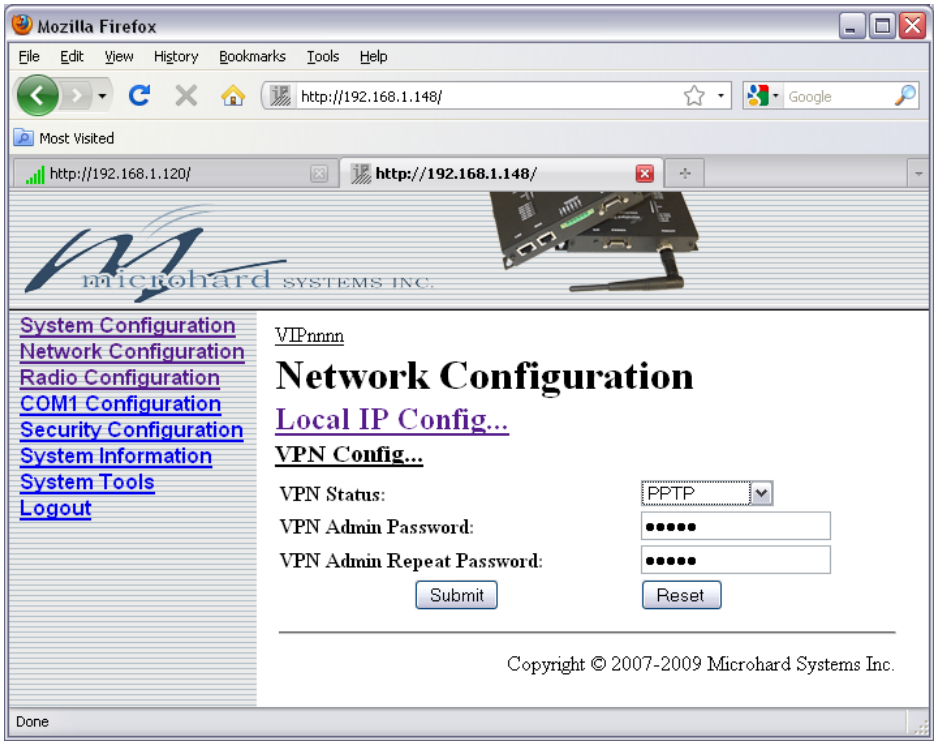


Image 6J: Network Configuration (Router), VPN Configuration Submenu

VPN Status

Select PPTP (Point-to-Point Tunneling Protocol) and L2TP/IPSEC (Layer 2 Tunneling Protocol) ; Disable disables it.

Values

Disable
PPTP
L2TP/IPSEC

VPN Admin Password / VPN Admin Repeat Password

Select a unique password of 32 characters maximum, case-sensitive. Repeat it in the next box to ensure it is correct and as intended.

Values

admin
32 characters maximum

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.

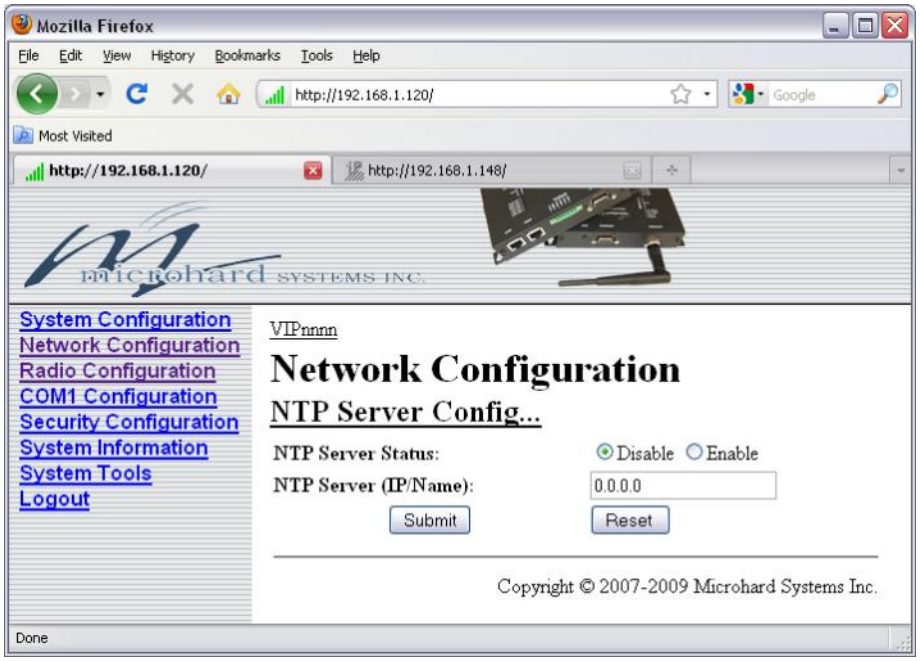


Image 6K: Network Configuration, NTP Server Configuration Submenu

NTP Server Status

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

Values

Disable
Enable

NTP Server (IP/Name)

IP address or domain name for an accessible NTP server is to be entered in this field if the NTP Server Status is configured as ENABLED.

Values

0.0.0.0
valid NTP server IP address or 'name'

6.0 Configuration

6.1.4.3 DHCP Server Configuration

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

6.1.4.3.1 Bridge

A VIP Series unit 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

A VIP Series Access Point 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 VIP 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 VIP Series Access Point, noting that such a DHCP Server service must not be enabled on any other VIP Series units or devices which reside on the same network segment.

With this service enabled on the Access Point, 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 (not 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 a VIP Series or other IP-based device attached to the LAN).

6.0 Configuration

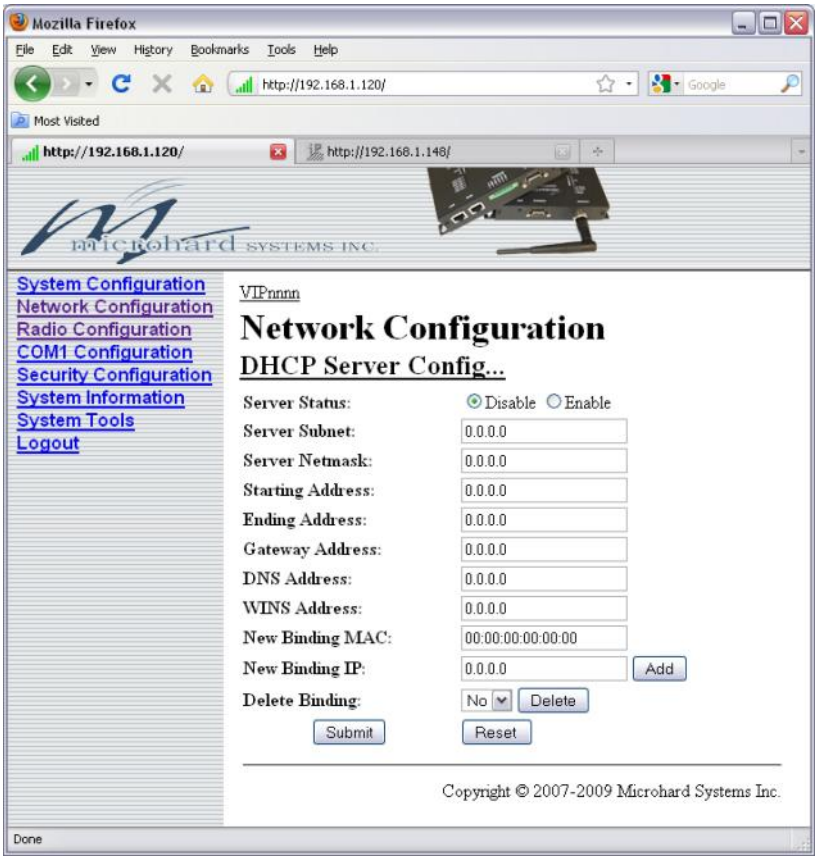


Image 6L: Network Configuration, DHCP Server Configuration Submenu

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

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

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 Address

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

Values

0.0.0.0

Valid WINS IP address

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

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

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.

6.0 Configuration

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.

The MAC address of the unit may be viewed on the Network Configuration menu of the unit.

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

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 VIP Series' 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 the VIP 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 VIP 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 VIP 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

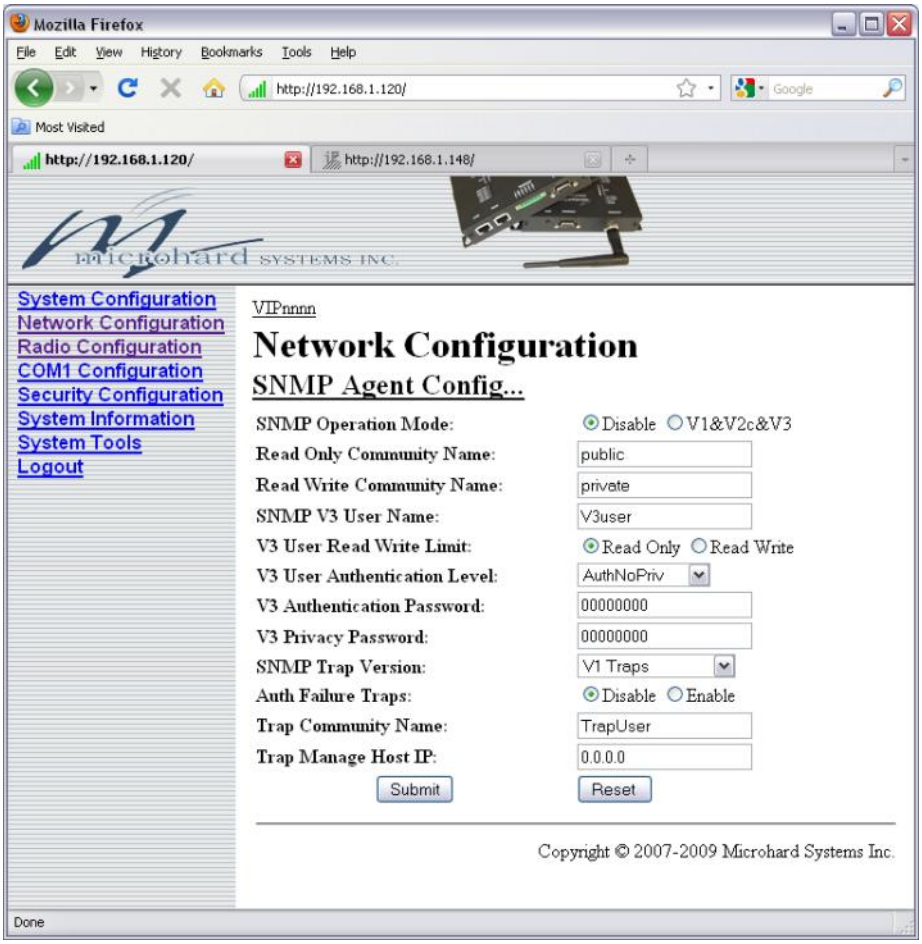


Image 6M: Network Configuration, SNMP Agent Configuration Submenu

SNMP Operation Mode

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

Values

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 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
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

SNMP Trap Version

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

Values

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

6.0 Configuration

Auth Failure Traps

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

Values

Disable
Enable

Trap Community Name

The community name which may receive traps.

Values

TrapUser

character string

Trap Manage Host IP

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

Values

0.0.0.0

applicable host's IP address

Soft Buttons

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

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 6N: Network Configuration, Bridge Configuration Submenu

Spanning Tree Protocol Status
Selection of STP operational status within the VIP Series: On or Off.

Values
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

6.1.5 Radio Configuration
6.1.5.1 Operational Mode

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, Section 4.0) of the specific VIP Series unit must also be known.

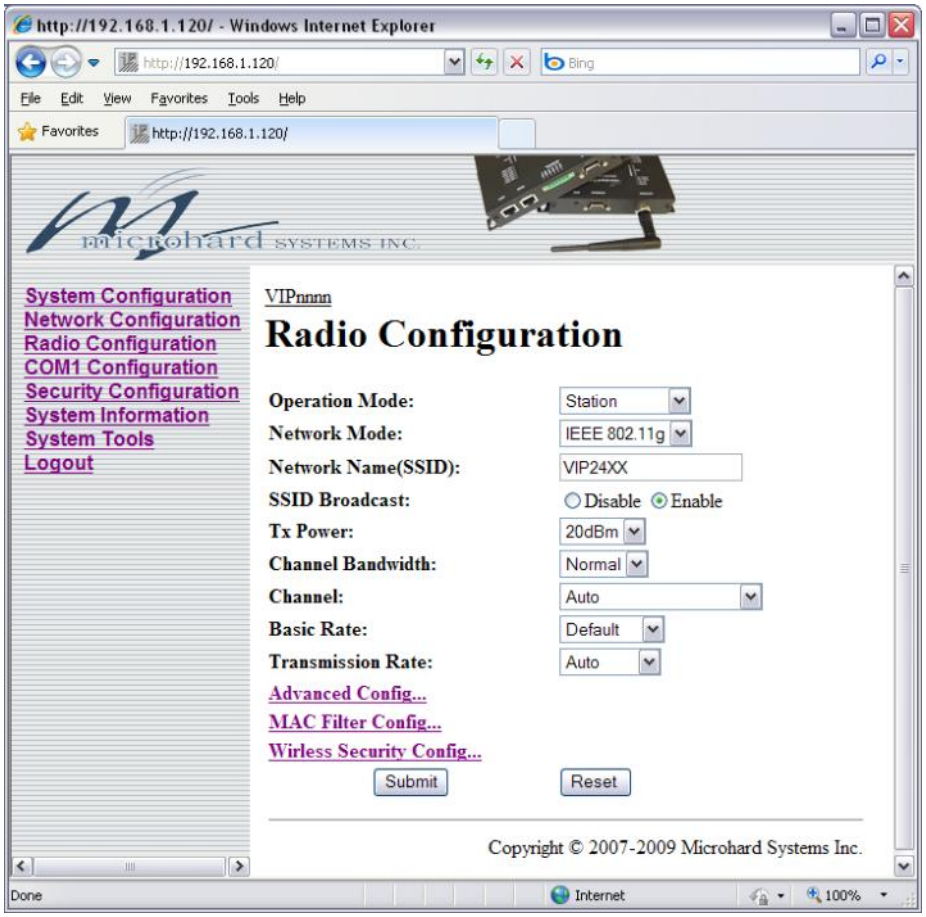


Image 6O: Radio Configuration Menu

6.0 Configuration

Operation Mode

There are four available selections for the unit's mode of operation:

- Access Point
  An Access Point may provide a wireless data connection to many clients, such as stations, repeaters, or other supported wireless devices such as laptops etc.
- Station
  A Station may sustain one wireless connection, i.e. to an Access Point.
- Repeater
  A Repeater can be connected to an Access Point to extend the range and provide a wireless data connection to many clients, such as stations.
- Mesh
  Units can be configured as a Mesh "Node". When multiple units are configured as a Mesh node, they automatically establish a network between each other. SSID for each radio in a Mesh network must be the same.

Values
Access Point
Station
Repeater
Mesh

Network Mode

The Network mode defines which wireless standard to use for the wireless network. The VIP5800/4900 supports 802.11a (up to 54 Mbps), while the VIP2400 supports both 802.11b (up to 11 Mbps) or 802.11g (up to 54 Mbps).

Values (VIP2400)	Values (VIP4900)	Values (VIP5800)
IEEE 802.11b IEEE 802.11g	IEEE 802.11a	IEEE 802.11a

6.0 Configuration

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.

Network Name (SSID)

All VIP Series in a given network must have the same Network Name. This unique network address is not only a security feature for a particular network, but also allows other networks - with their own unique network address - to operate in the same area without the possibility of undesired data exchange between networks.

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

Values

VIPnnnn
character (up to 32) string, case sensitive

Second Network Name (SSID)

This option only appears when the Operation Mode is configured as Repeater. In a repeater the (first) Network Name is set to connect to the Access Point (AP) from which the repeater linked to. The Second Network Name is the network to which all subtending devices will connect.

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

Values

VIPnnnn
character (up to 32) string, case sensitive

SSID Broadcast

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

Values

Enable
Disable

6.0 Configuration

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

Tx Power

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

Values

dBm (mW equivalent)

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

Channel Bandwidth

Not currently used.

Values

Normal

Channel

The Channel setting allows configuration of which channel to operate on, in the case of the VIP2400, auto can be chosen where the unit will pick a channel to operate. If a link cannot be established it will try another channel. The VIP5800 requires that a channel be chosen.

Values (VIP2400)

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

Values (VIP5800)

Channel 149 : 5.745 GHz
Channel 152(T) : 5.760 GHz
Channel 153 : 5.765 GHz
Channel 157 : 5.785 GHz
Channel 160(T) : 5.800 GHz
Channel 161 : 5.805 GHz
Channel 165 : 5.825 GHz

6.0 Configuration

Basic Rate

This is the rate at which the broadcast and beacon signals are transmitted for basic wireless operation. This is for internal use, and is not generally required to be changed.

Values (VIP2400)	Values (VIP5800)
1,2Mbps	**6,9Mbps**
Default	Default
All	All

Transmission Rate

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

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

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

Values (VIP2400)	Values (VIP5800/4900)
Auto	**Auto**
1 Mbps (802.11b,g)	6
2 Mbps (802.11b,g)	9
5.5 Mbps (802.11b,g)	12
11 Mbps (802.11b,g)	18
6 Mbps (802.11g)	24
9 Mbps (802.11g)	36
12 Mbps (802.11g)	48
18 Mbps (802.11g)	54
24 Mbps (802.11g)	
36 Mbps (802.11g)	
48 Mbps (802.11g)	
54 Mbps (802.11g)	

6.0 Configuration

6.1.5.2 Advanced Configuration

The Advanced Radio Configuration is a general category menu which allows the configuration of the most basic or system level settings that are not normally required to changed, but are available for network fine tuning and/or troubleshooting. It is best not to change these setting unless required or advised my Microhard Systems Inc.

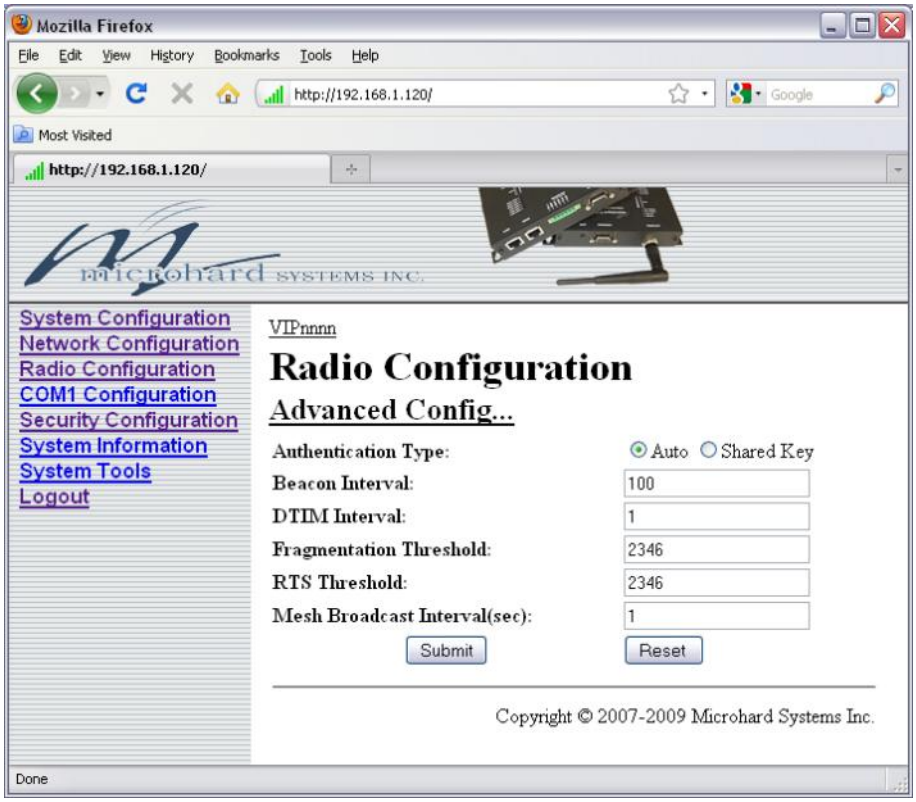


Image 6P: Radio Configuration Menu , Advanced Configuration Submenu

Authentication Type	
When a station sends data to an Access Point or Repeater it must identify or authenticate itself. Auto: Uses either Open System or Shared Key Authentication as required. Shared Key: Assumes both stations have the same shared key or passphrase.	**Values** **Auto** Shared Key

6.0 Configuration

Advanced Configuration (continued)

Beacon Interval

The beacon packets are used and required for basic system synchronization, providing timing and other information. The default value is 100 milliseconds.

Values

100

Fragmentation Threshold

The fragmentation threshold allows a user to change the maximum RF packet size. Increasing the RF packet size reduces the need to break packets into smaller fragments. The default value is 2346. The maximum value is 2432. Increasing the fragmentation threshold slightly may improve performance if a high packet error rate is experienced.

Values

2346

RTS Threshold

Once the RTS Threshold defined packet size is reached, the system will invoke RTS/CTS flow control. A large RTS Threshold will improve bandwidth, while a smaller RTS Threshold will help the system recover from interference or collisions caused by obstructions. The default value is 2346.

Values

2346

Mesh Broadcast Interval

The frequency of the Mesh Broadcast Interval used for synchronizing the Mesh network. The default value is 1 second.

Values

1

6.0 Configuration

6.1.5.3 MAC Filter Configuration

MAC Filter configuration enables or disables the ability for the VIP to filter wireless connections made to the VIP unit by MAC Address.

Image 6Q: Radio Configuration Menu , MAC Filter Configuration Submenu

MAC Filter Status	
This option will disable or enable the use of MAC Address Filtering. If enabled when a connection is made the MAC address of the connecting device is compared to the MAC Filter list. Depending on the MAC List Policy setting, the connection will be allowed or denied.	**Values** **Disable** Enable

MAC List Policy	
Setting the MAC List Policy to **Deny**, will deny access to any MAC Addresses listed in the MAC Filter List. Using the **Permit Only** option will only allow connections to the MAC Address listed in the MAC Filter List.	**Values** **Deny** Permit Only

6.0 Configuration

New MAC Address

Use this field to enter a new MAC Address to use for filtering. Once entered use the **Add/Update** soft button to add the entry to the MAC Filter List. This list will only appear once an entry is made.

MAC Filter List

Image 6R: Radio Configuration Menu , MAC Filter List

The MAC Filter List, is a list of MAC address that are either forbidden or allowed to connect to the VIP series Radio. The MAC List Policy defines this relationship.

Use the available soft buttons to Edit or Delete entries. Use the Submit Button to write the table to the VIP or use the Reset button to revert to the previously stored list.

6.0 Configuration

6.1.5.4 Wireless Security Configuration

Wireless Security Configuration

See **Section 6.1.7.3** for a full description of the Wireless Security Configuration of the VIP Series.

Image 6S: Radio Configuration Menu , Wireless Security Configuration Submenu

Security Mode

Select the type of wireless security to be used. Once WEP or WPA is selected the configuration options appear. Refer to **Section 6.1.7.3** for additional information on these settings.

Values

Disable
WEP
WPA

6.0 Configuration

6.1.6 COM1 (Serial) Configuration

6.1.6.1 Serial Port Parameters

This menu option is used to configure the serial device server for the serial communications port.

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

The fully-featured RS232 interface supports hardware handshaking. By default, this port is enabled.

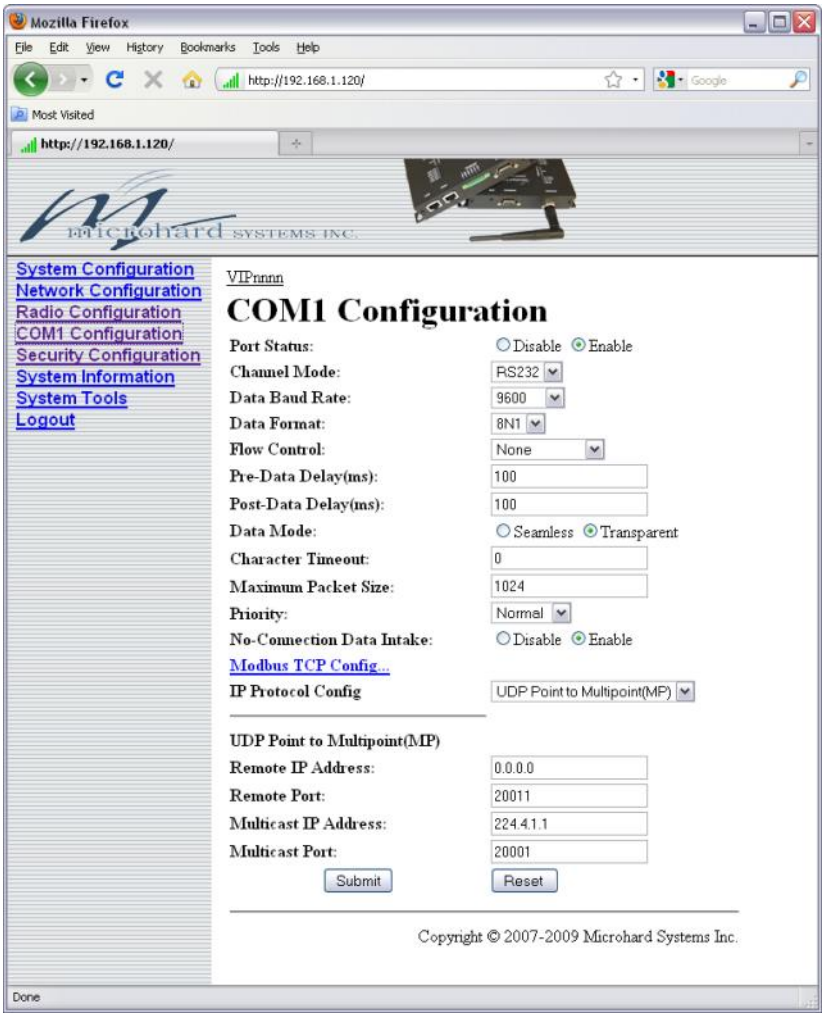


Image 6T: COM1 Configuration Menu

6.0 Configuration

Port Status

Select operational status of port. Enabled by default.

Values

Enable
Disable

Channel Mode

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

Values

RS232
RS485
RS422

Data Baud Rate

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

6.0 Configuration

Data Format

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

Values

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

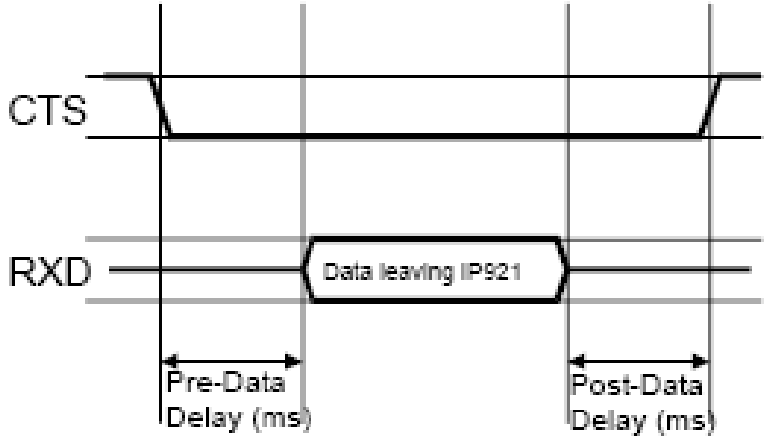
Flow Control

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

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

*COM2 does not support Flow Control.

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



Drawing 6A: CTS Output Data Framing

Values

None
Hardware
CTS Framing

6.0 Configuration

Pre-Data Delay (ms)

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

Values

100 (ms)

Post-Data Delay (ms)

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

Values

100 (ms)

Data Mode

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

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

0 (characters)

6.0 Configuration

Maximum Packet Size

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

Values

Bytes

1024

Priority

This setting effects the quality of service associated with the data traffic on the COM port.

Values

Normal
Medium
High

No-Connection Data Intake

When enabled the data will continue to buffer received on the serial data port when the radio loses synchronization. When disabled the VIP will disregard any data received on the serial data port when radio synchronization is lost.

Values

Enable
Disable

6.0 Configuration

6.1.6.2 Modbus TCP Config

Additional settings are available for Modbus applications. Once selected the *Modbus TCP Config* menu will appear as shown below:

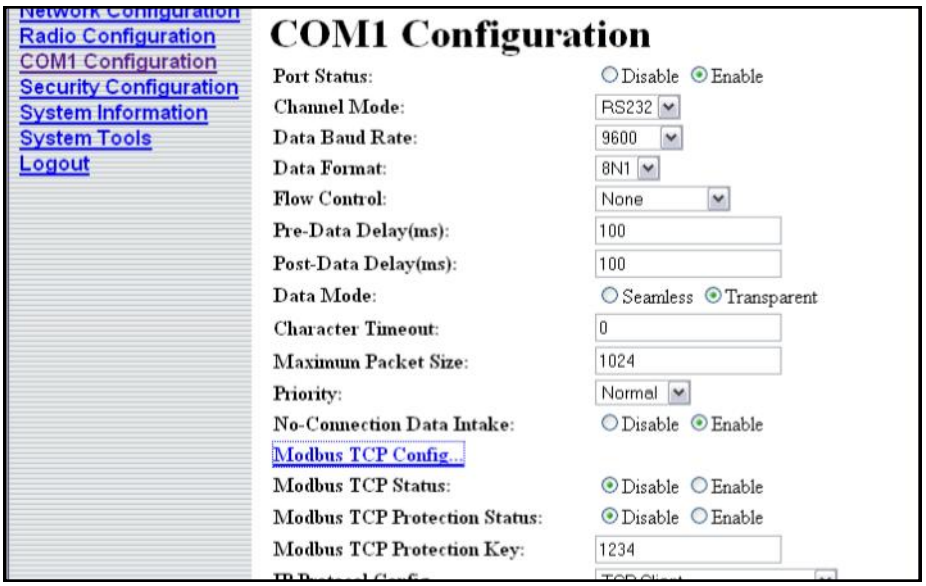


Image 6U: Modbus TCP Config

Modbus TCP Status

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

Values

Disable
Enable

Modbus TCP Protection Status

The field allows the Modbus TCP Protection Status flag to be enabled or disabled. If enabled the Modbus data will be encrypted with the Modbus Protection Key.

Values

Disable
Enable

Modbus Protection Key

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

Values

1234

6.0 Configuration

6.1.6.3 IP Protocol Configuration

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

IP Protocol Config

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

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

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

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

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

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

Requires more bandwidth than UDP.

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

- Local Listening Port
  The TCP port which the Server listens to. It allows a TCP connection to be created by a TCP Client to carry serial port data.
  Default: **20001**
- Incoming Connection Timeout
  Established when the TCP Server will terminate the TCP connection is the connection is in an idle state.
  Default: **300** (seconds)

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)

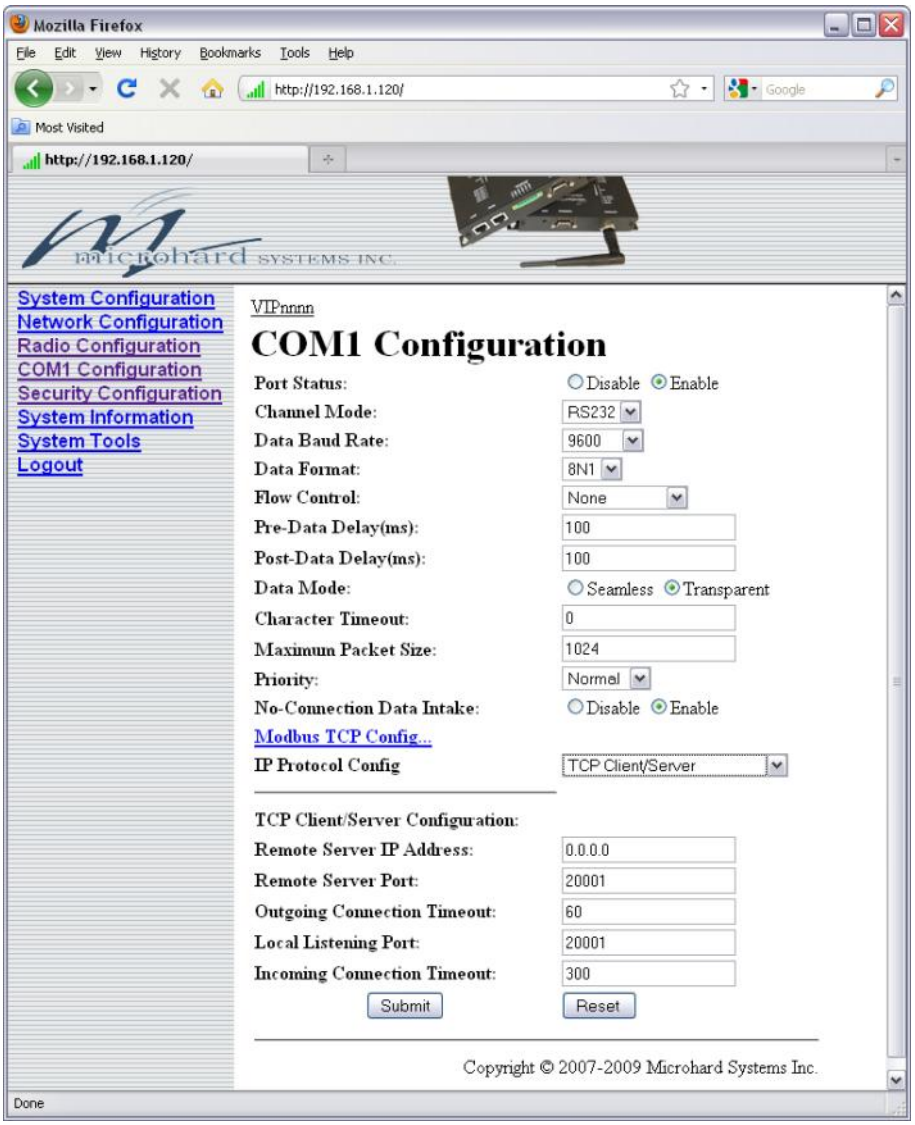


Image 6V: COM1 Configuration Menu

TCP Client/Server: In this mode, the VIP Series unit 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 VIP Series unit will send serial data to a specifically-defined point, using UDP packets. This same VIP Series unit 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 Access Point in the VIP Series network.

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

- Multicast IP Address
  A valid multicast address this unit uses to send multicast UDP packets upon receiving data from the serial port. The default value is a good example of a valid multicast address.
  Default: **224.1.1.1**
- Multicast Port
  A UDP port that this 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 VIP Series unit.
  Default: **20001**
- Listening Port
  The UDP port that this unit receives incoming data on from multiple remote units.
  Default: **20011**
- Time to Live
  Time to live for the multicast packets.
  Default: **1** (hop)

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

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

continued...

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 (VIP 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 Access Point.
  Default: **0.0.0.0**

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

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

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

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 the VIP Series' memory.

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

6.0 Configuration

6.1.7 Security Configuration

There are numerous security features available for the VIP Series, both as standard and optional items.

Image 6W: Security Configuration Menu

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 Configuration Submenu

6.0 Configuration

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

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

New Password/Repeat Password
Values
character string
admin

6.1.7.2 Upgrade Password Configuration

The Upgrade Password protects the VIP Series unit 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 Configuration, Upgrade Password Configuration Submenu

New Password/Repeat Password
Values
character string
admin

6.0 Configuration

6.1.7.3 Wireless Security Configuration

Security options are dependent on the version type. This section describes all available options.

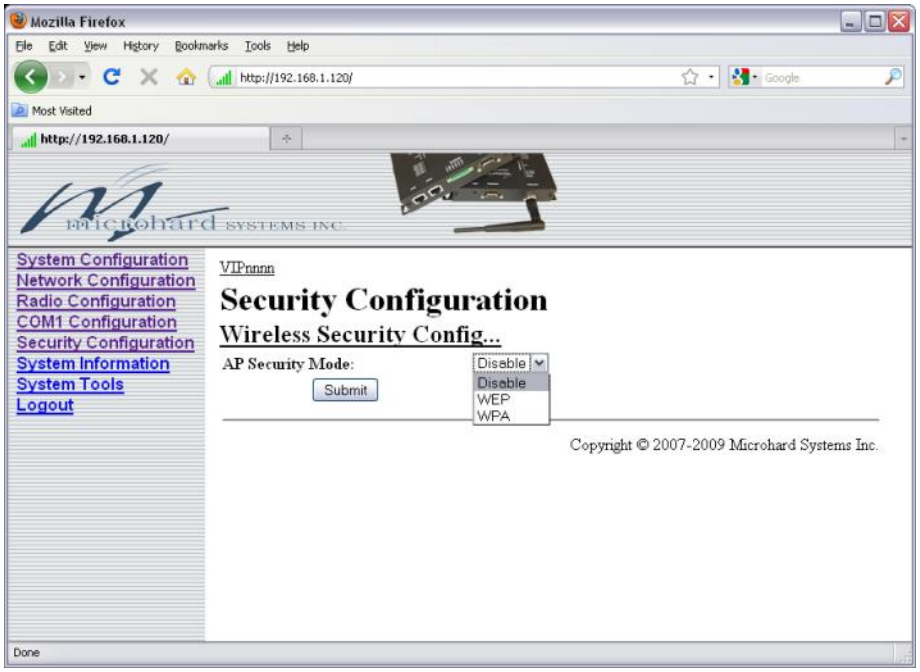


Image 6Z Security Configuration, Wireless Security Configuration Submenu

Only 40-bit encrpytion available for EXPORT VERSIONS.

Security Mode

By default, the Security Mode is Disabled (no encryption). A number of Security Modes are available (dependent on the version of VIP Series unit), requiring varying degrees of configuration.

Values

Disable
WEP
WPA

6.0 Configuration

Security Mode (continued)

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

The image below shows the associated configuration options:

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 Configuration, WEP Submenu

- WEP Default Key
  Select Key 1, 2, 3, or 4 as the default key.

- WEP Encryption
  Select either;
  64-bit (5 characters, 10 hex digits), or
  128-bit (13 characters, 26 hex digits)

128-bit encryption offers stronger encryption than 64-bit, but adds more overhead on the data.

- 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.

continued...

6.0 Configuration

Security Mode (continued)

Using the same Key Phrase(s) on all VIP Series units within the network will generate the same Keys on all units. All units must operate with the same Key selected.
Alternately, key phrases may be entered manually into each Key field.
Default: **0000**

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

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

The image below shows the associated configuration options:

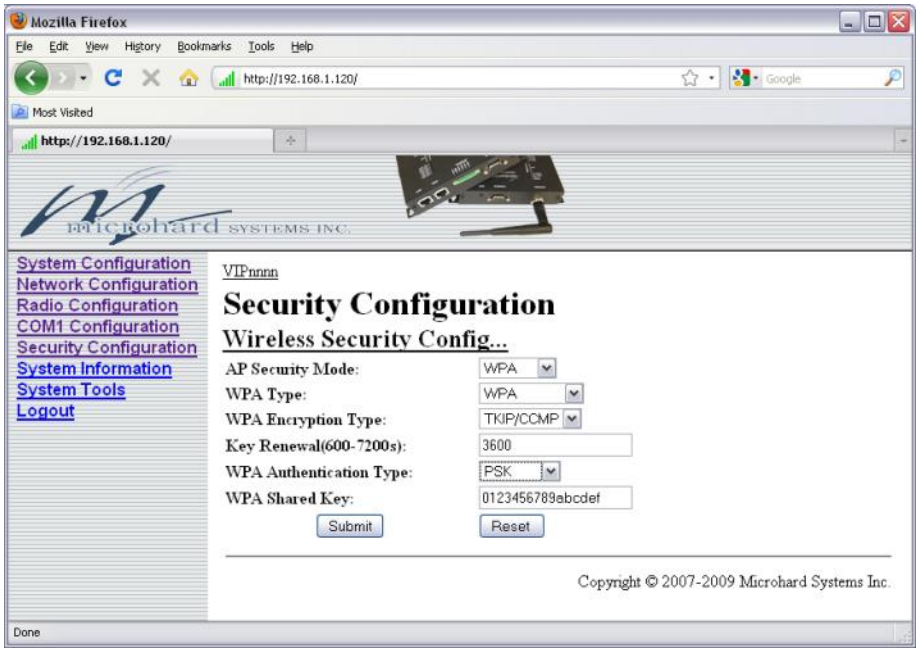


Image 6AB: Wi-Fi Protected Access, WPA Submenu

6.0 Configuration

6.1.7.4 Discovery Service Configuration

This configuration selection will determine whether or not this modem may be 'discovered'. The choice is typically based-upon network security considerations.

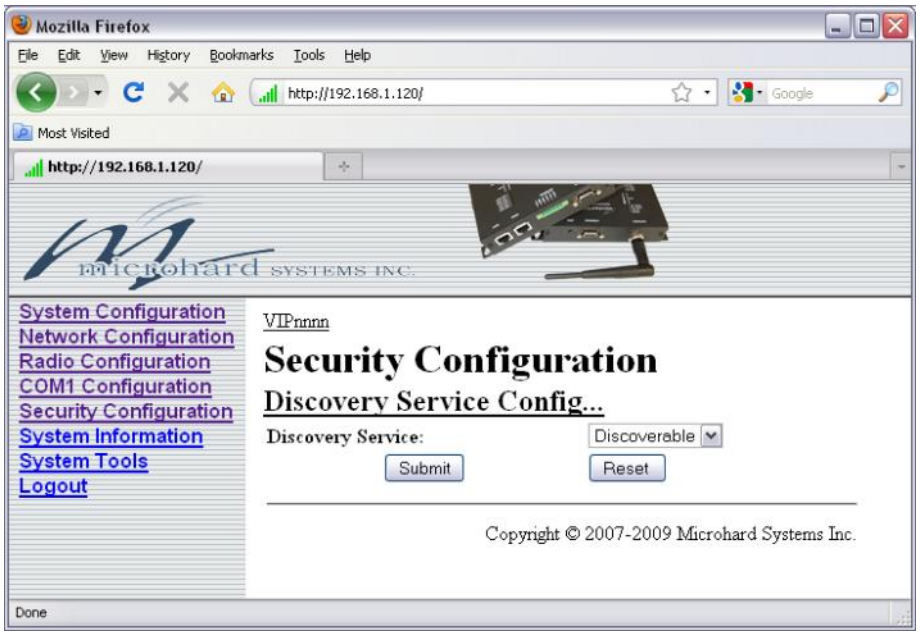


Image 6AC: Security Configuration Menu, Discovery Service Submenu

Discovery Service

Disable: This unit will not appear to exist when another unit attempts to discover it.

Discoverable: This unit will appear to exist when another VIP Series unit attempts to discover it.

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

Values

Disable
Discoverable
Changeable

6.0 Configuration

6.1.7.5 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.

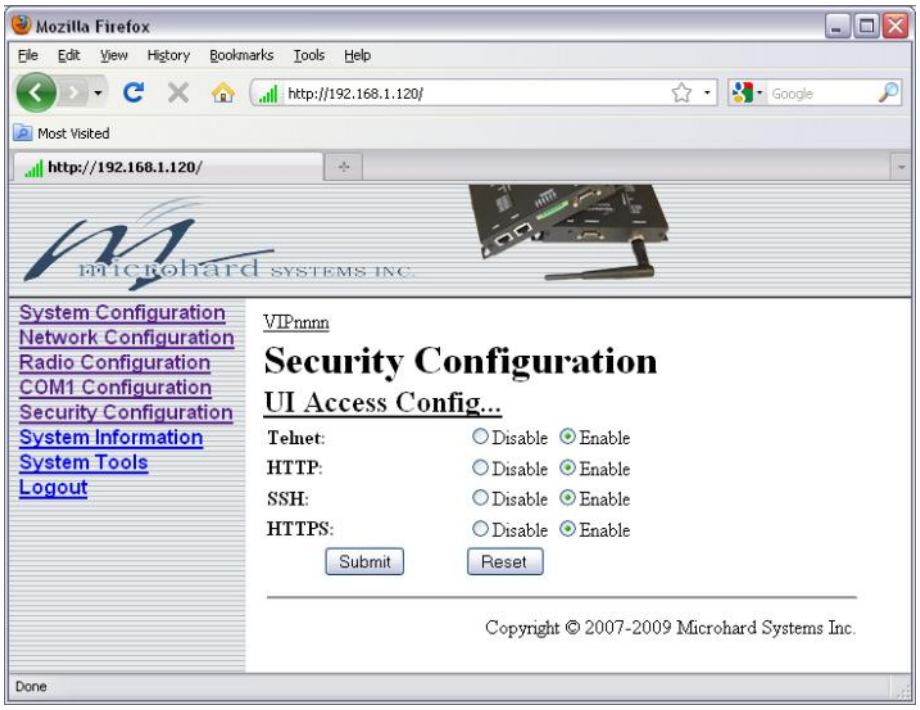


Image 6AD: Security Configuration Menu, UI Access Configuration Submenu

UI Access Configuration
Values
Disable **Enable**

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

Format, from DOS prompt:
>telnet 192.168.1.80
where the IP address is that of the target device.

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

For a secure connection, see 'SSH' below.

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.

6.0 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 VIP Series unit, 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.

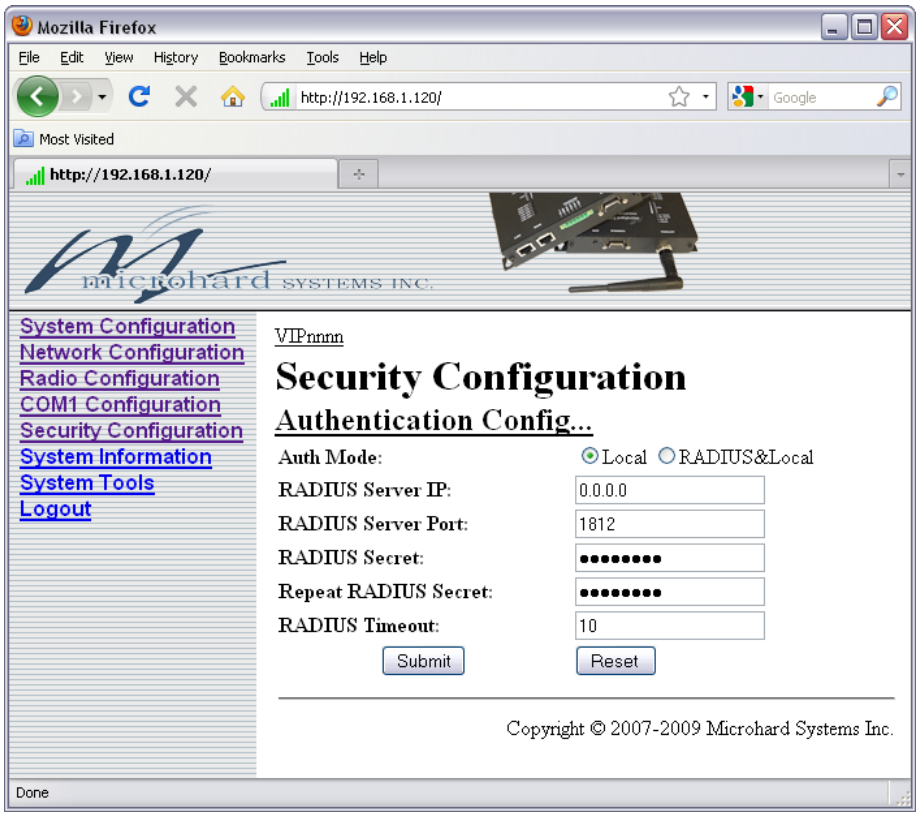


Image 6AE: Security Configuration Menu, Authentication Configuration Submenu

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 VIP 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 VIP Series' User Interface and related protocols.

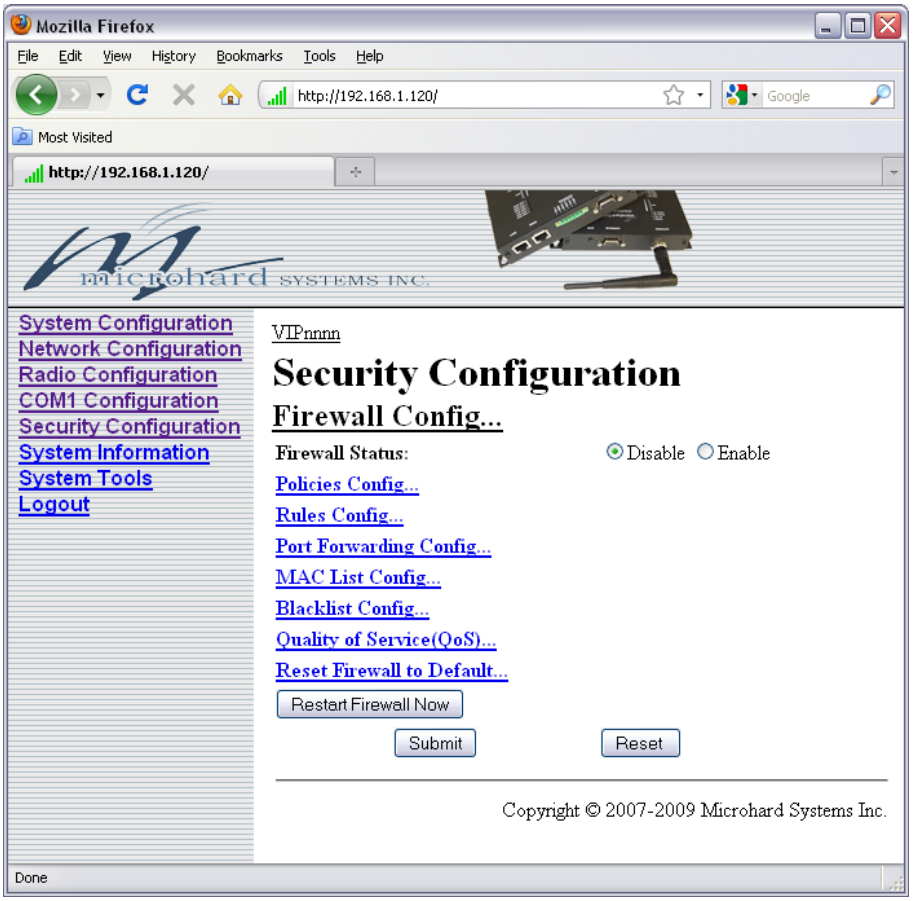


Image 6AF: Security Configuration Menu, Firewall Configuration Submenu

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

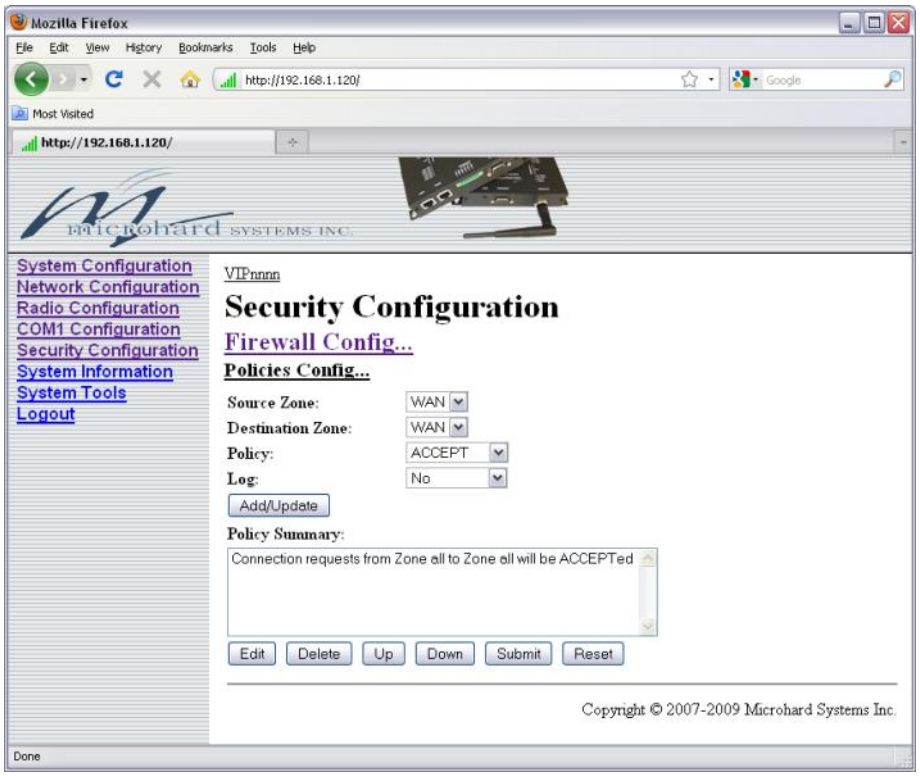


Image 6AG: Firewall Configuration, Policies Configuration Submenu

Source Zone

Select the zone which is to be the source of the data traffic.

Values
WAN
LAN
FW
VPN
all

6.0 Configuration

Destination Zone

Select the zone which is the intended destination of the data traffic.

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

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

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

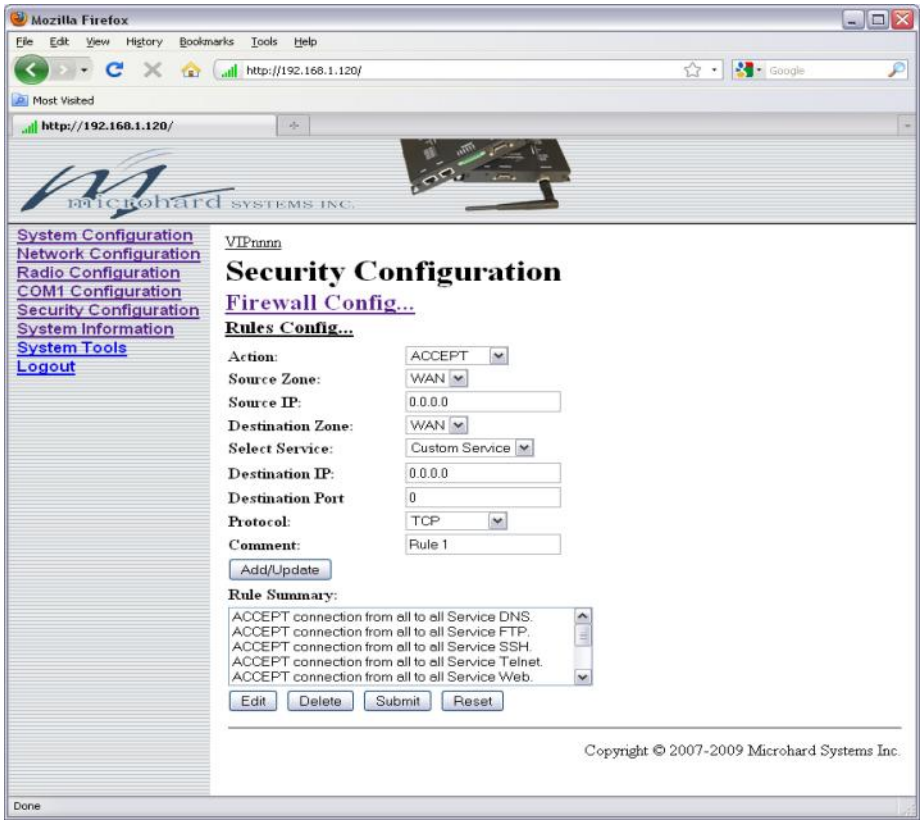


Image 6AH: Firewall Configuration, Rules Configuration Submenu

Action

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

Values

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

6.0 Configuration

Source Zone

Select the zone which is to be the source of the data traffic.

Values

WAN
LAN
FW
VPN
all

Source IP

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

Values

0.0.0.0

valid IP address

Destination Zone

Select the zone which is the intended destination of the data traffic.

Values

WAN
LAN
FW
VPN
all

Select Service

This field allows for the rule to be applied to either a Custom Service (defined further down the menu) or for one of many predefined services available via a pulldown menu.

Values

Custom Service

or select from a long listing of predefined services

6.0 Configuration

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

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

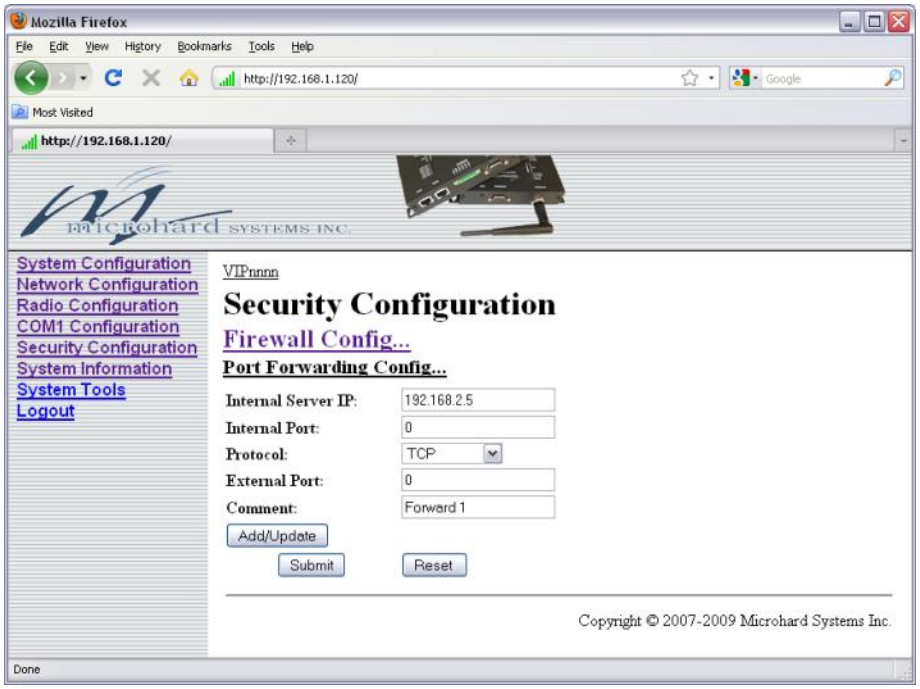


Image 6AI: Firewall Configuration, Port Forwarding Configuration Submenu

Internal Server IP

Enter the IP address of the intended internal 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 server.

Values

TCP
TCP:SYN
UDP
ICMP
IPP2P
IPP2P:UDP
IPP2P:all
All

External Port

Port number of incoming request.

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

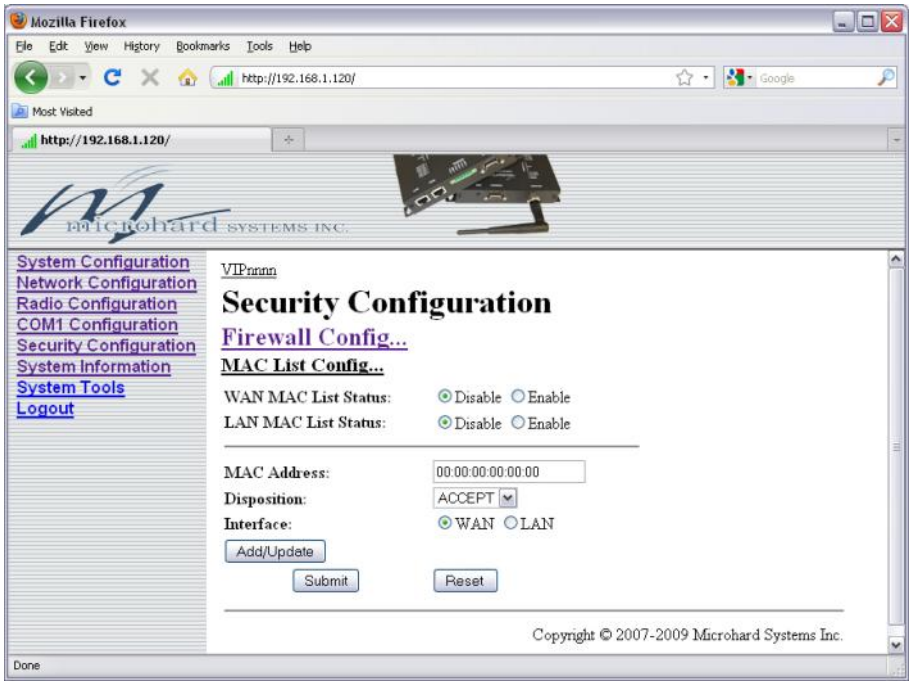


Image 6AJ: Firewall Configuration, MAC List Configuration Submenu

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

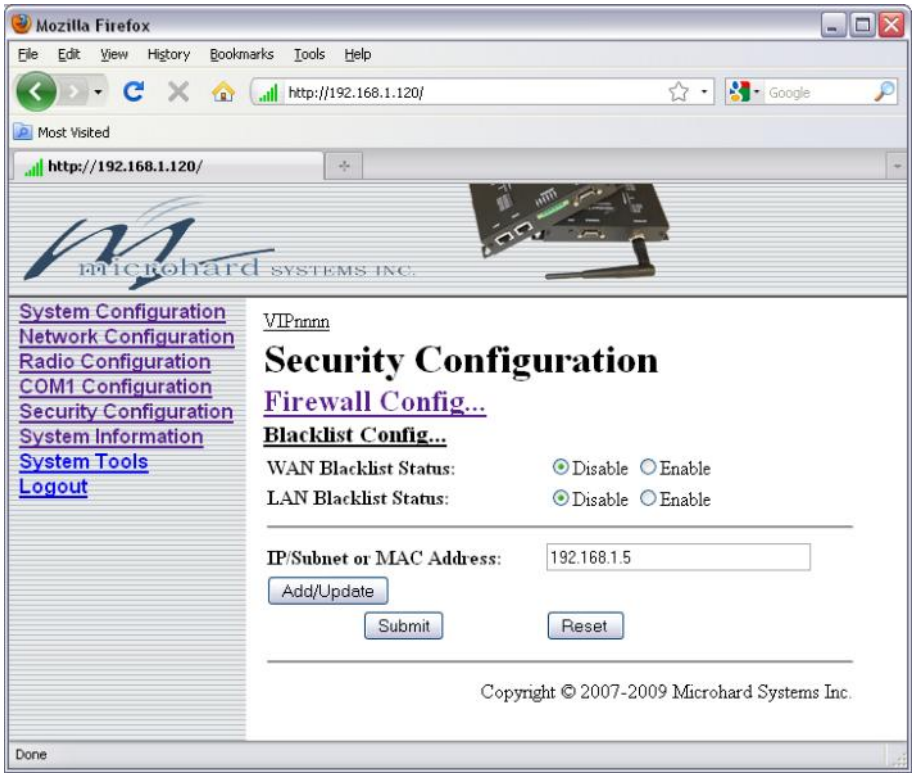


Image 6AK: Firewall Configuration, Blacklist Configuration Submenu

WAN Blacklist Status

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

Values

Disable
Enable

LAN Blacklist Status

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

Values

Disable
Enable

IP/Subnet or MAC Address

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

Values

192.168.1.5

valid IP address

6.0 Configuration

6.1.7.7.6 Quality of Service (QoS)

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

Type of Service Config

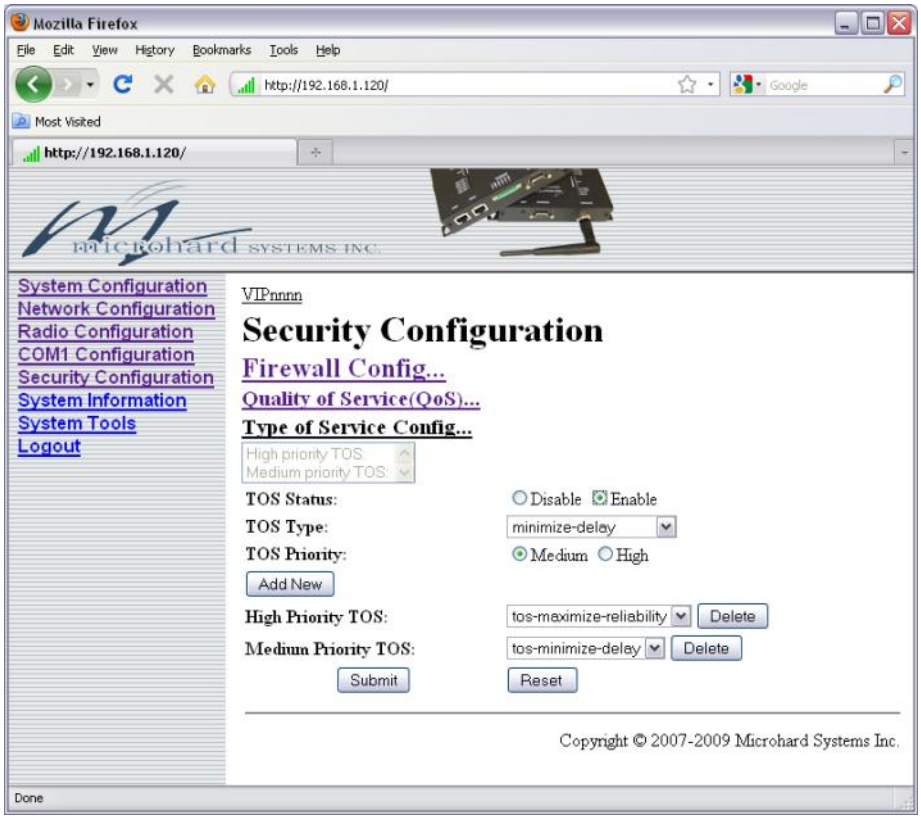


Image 6AL: Firewall Configuration, Quality of Service (QoS) Menu

TOS Status

Enables or disables the use of the *Type of Service* features of the VIP Series modem, which is a policy based type of routing.

Values

Disable
Enable

6.0 Configuration

TOS Type

Selects the Type of Service categories to assign priority.

Values

minimize-delay
maximize-throughput
maximize-reliability
minimize-cost
normal-service

TOS Priority

Selects the priority of the Type of Service entries above. Choose between medium and high priority. Once the above fields have been completed use the Add New button to add the TOS to the Priority list.

Values

medium
high

High Priority TOS

This drop down box lists the configured and active TOS entries, marked as High Priority. Once complete use the Submit button to write the changes to the VIP or Reset to revert back to the previously entered list.

Values

minimize-delay
maximize-throughput
maximize-reliability
minimize-cost
normal-service

Medium Priority TOS

This drop down box lists the configured and active TOS entries, marked as Medium Priority. Once complete use the Submit button to write the changes to the VIP or Reset to revert back to the previously entered list.

Values

minimize-delay
maximize-throughput
maximize-reliability
minimize-cost
normal-service

6.0 Configuration

Custom Ports Config

Custom Ports Config allows the priority of data on specific TCP and UDP ports to be set as medium or high to sure critical data on these ports is delivered.

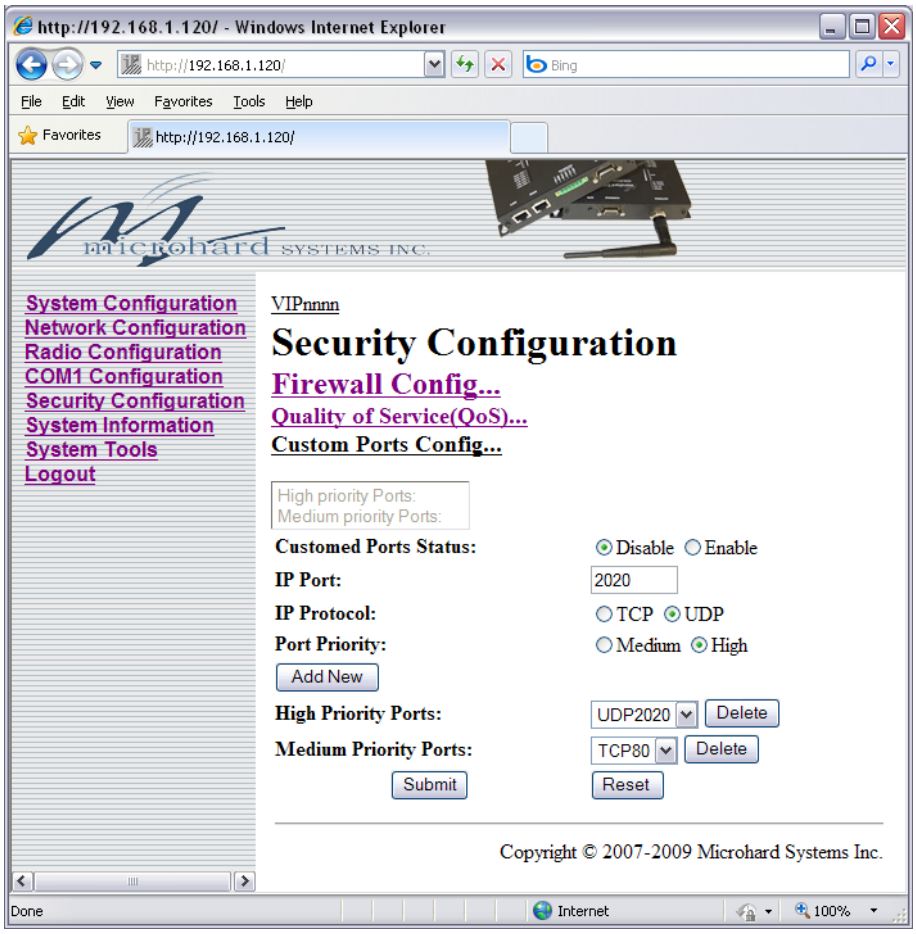


Image 6AM: Firewall Configuration, QoS Custom Ports Configuration Menu

Customed Ports Status

Enable or Disable the use of priority based QoS on specific TCP and/or UDP ports.

Values

Disable
Enable

6.0 Configuration

IP Port

Enter value of the TCP or UDP port to be assigned priority.

Values

TCP/UDP Port #

(1 - 65535)

IP Protocol

Define as either a TCP or UDP port.

Values

TCP
UDP

Port Priority

Assign medium or high priority for the port defined above. Once complete use the Add New button to add the port to the Port Priority Lists below.

Values

Medium
High

High Priority Ports

This drop down box lists the configured and active IP Ports, marked as High Priority. Once complete use the Submit button to write the changes to the VIP or Reset to revert back to the previously entered list.

Values

TCP/UDP Port #'s

Medium Priority Ports

This drop down box lists the configured and active IP Ports, marked as Medium Priority. Once complete use the Submit button to write the changes to the VIP or Reset to revert back to the previously entered list.

Values

TCP/UDP Port #'s

6.0 Configuration

6.1.7.7.7 Reset Firewall to Default

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

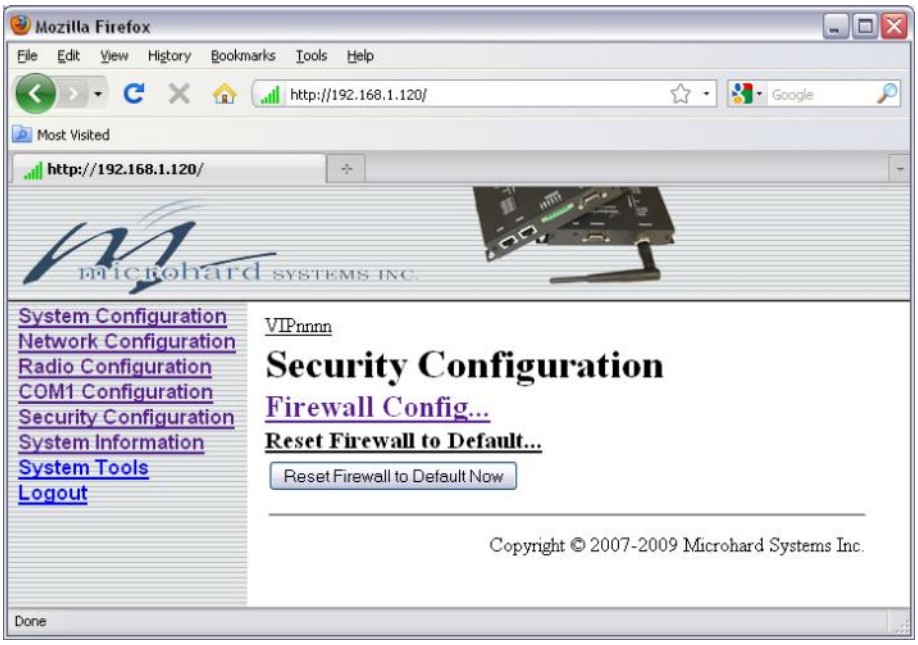


Image 6AN: Reset Firewall to Default

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.

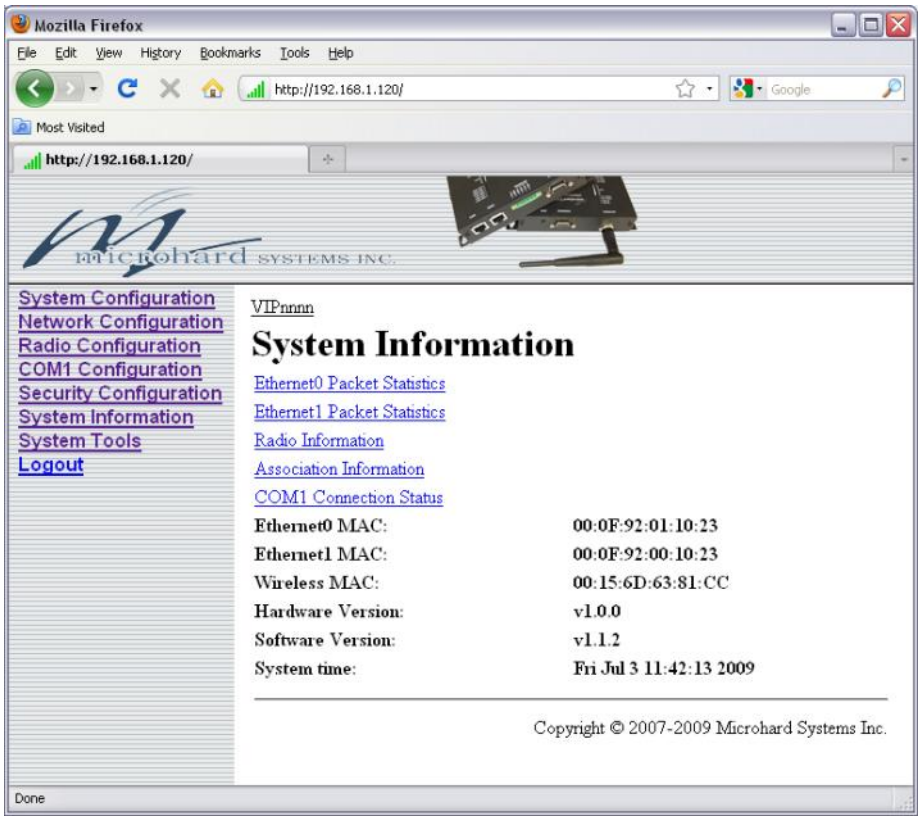


Image 6AO: System Information Menu

6.0 Configuration

Ethernet0 Packet Statistics

The Ethernet0 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 VIP Series unit, respectively.

Errors which are counted include alignment, frame check sequence (FCS), frame too long, and internal MAC.

The dropped packet count could increment if, for example, the network layer was too busy to accept the data.

The FIFO errors are related to interface-specific hardware.

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

The Transmit Carrier count relates to carrier sense errors.

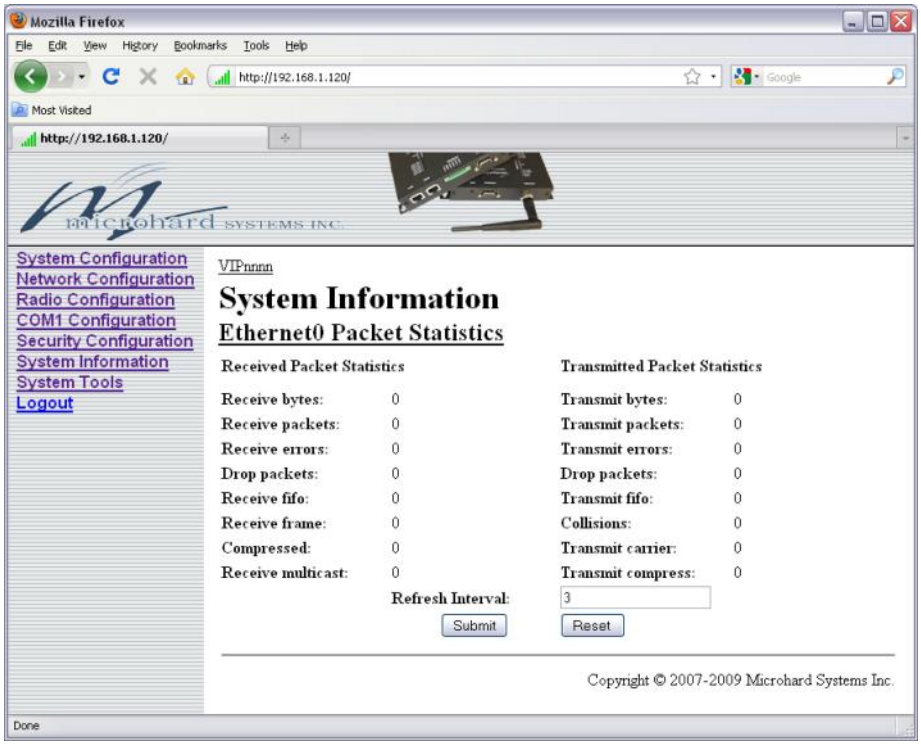


Image 6AP: System Information Menu, Ethernet0 Packet Statistics

6.0 Configuration

Ethernet1 Packet Statistics

The Ethernet1 Packets Statistics window displays a variety of parameters which apply to the traffic through, and status of, the physical ethernet port (hardware interface) on the rear of the IP Series.

Received and Transmitted information are applicable to the local data traffic into and out of the IP Series, respectively.

Errors which are counted include alignment, frame check sequence (FCS), frame too long, and internal MAC.

The dropped packet count could increment if, for example, the network layer was too busy to accept the data.

The FIFO errors are related to interface-specific hardware.

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

The Transmit Carrier count relates to carrier sense errors.

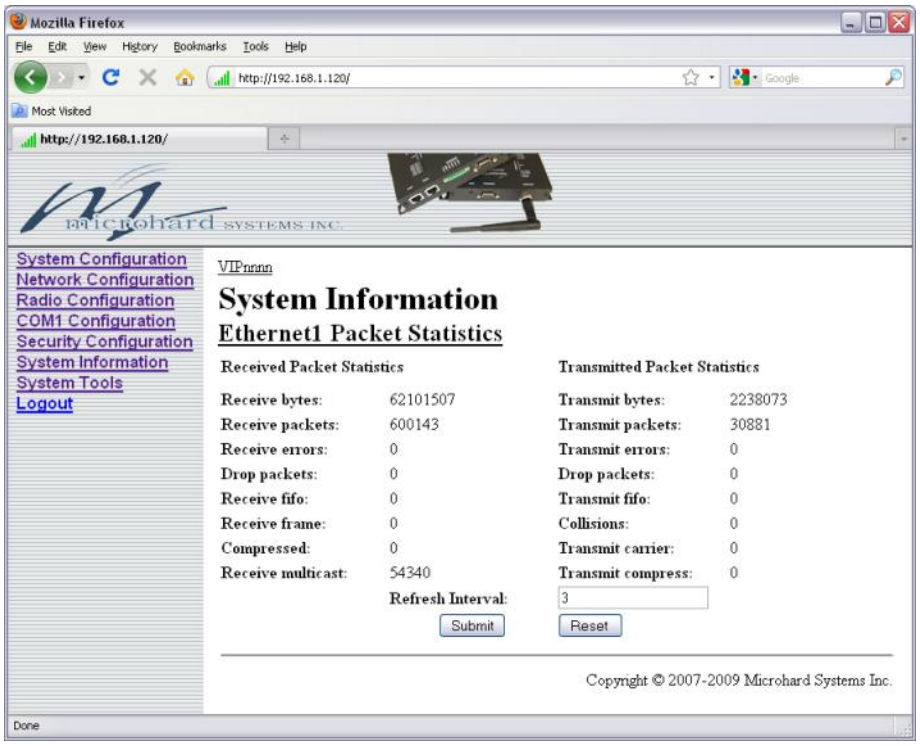


Image 6AQ: System Information Menu, Ethernet1 Packet Statistics

6.0 Configuration

Radio Information

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

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 VIP Series unit being viewed has lost synchronization with the VIP Series Access Point.

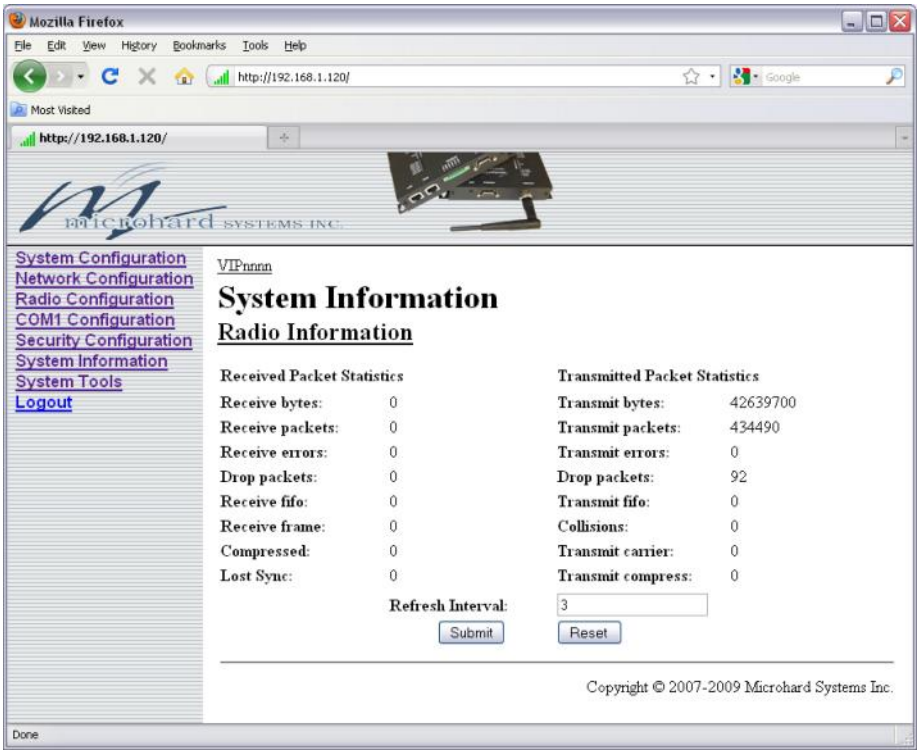


Image 6AR: System Information Menu, Radio Information

6.0 Configuration

Association Information

ADDR
MAC address of associated device

AID
Association ID

CHAN
Operating channel being used.

RATE
Current data (transmission) rate

RSSI
Receive signal strength indication

DBM
Receive signal in dBm

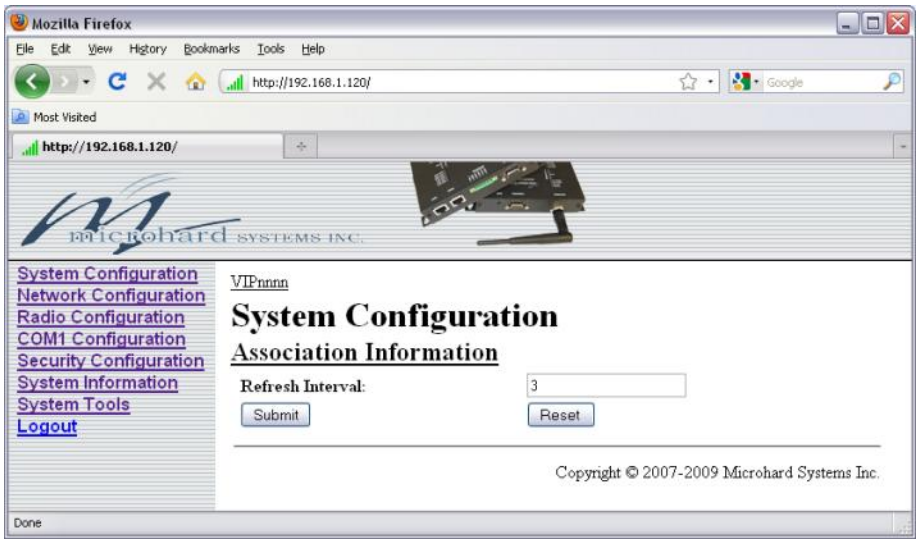


Image 6AS: System Information Menu, Association Information

6.0 Configuration

COM1 Connection Status

This window displays information related to the COM1 serial interface.

- 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'.

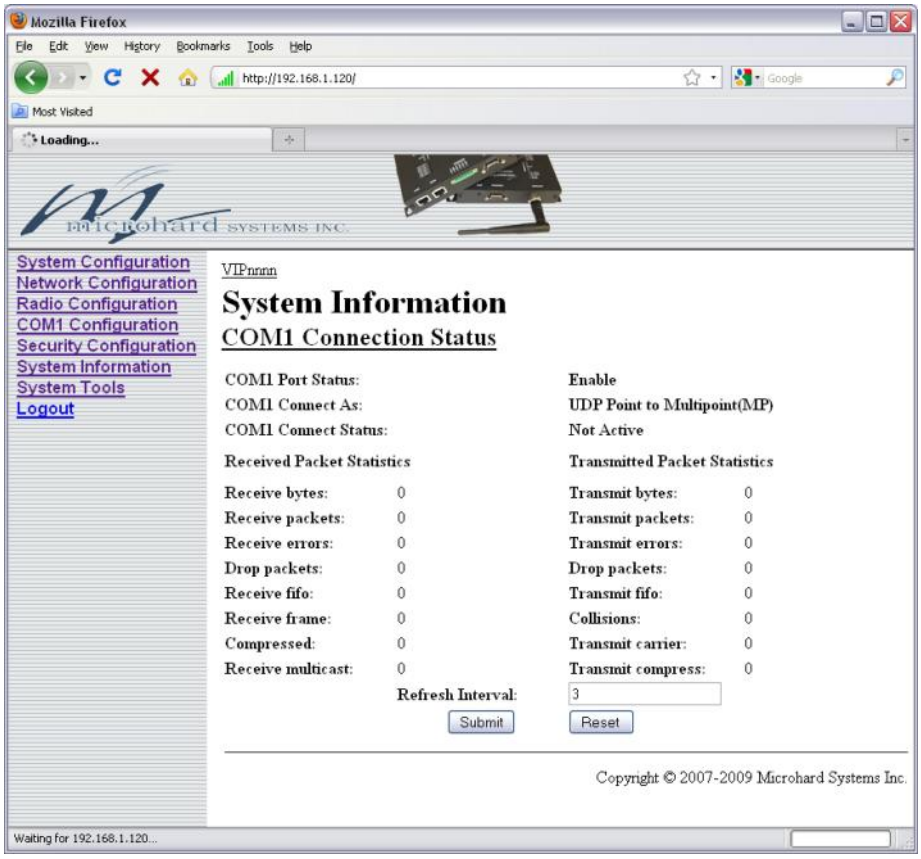


Image 6AT: System Information Menu, COM1 Connection Status

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 serial 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 to use the network discovery function to potentially discover other VIP Series units.

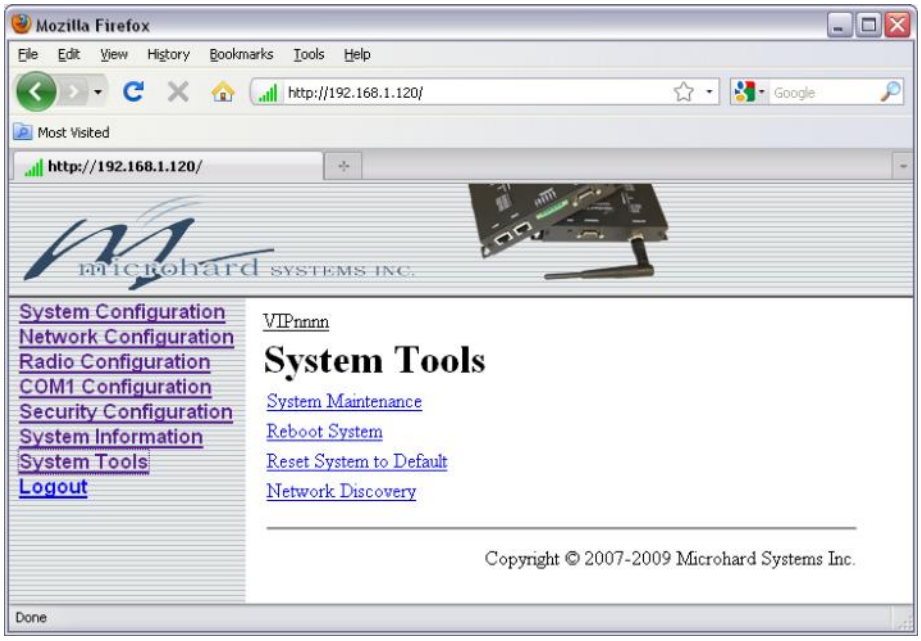


Image 6AU: System Tools Menu

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.

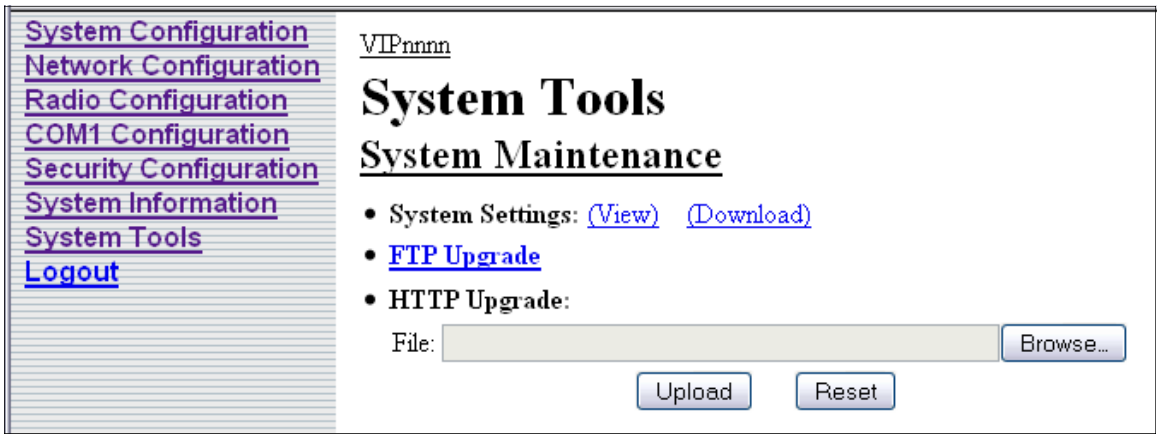


Image 6AV: System Tools Menu, System Maintenance

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

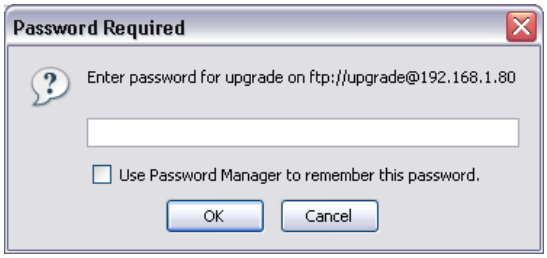


Image 6AW: System Tools Menu, Password

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

See Appendix for Package upgrade or recover upgrades using a command prompt

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.

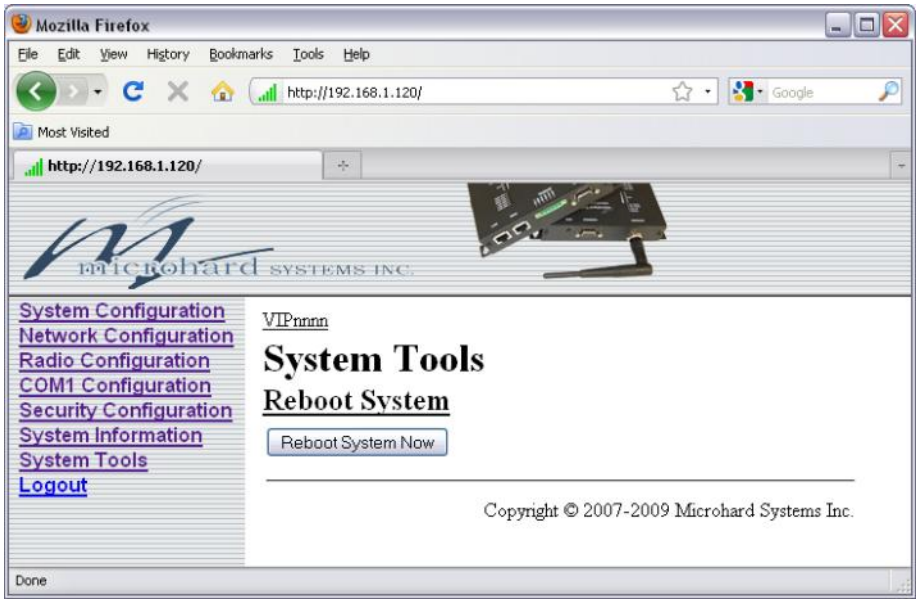


Image 6AX: System Tools Menu, Reboot System

6.0 Configuration

6.1.9.3 Reset System to Default

There are many configuration options for the VIP 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.

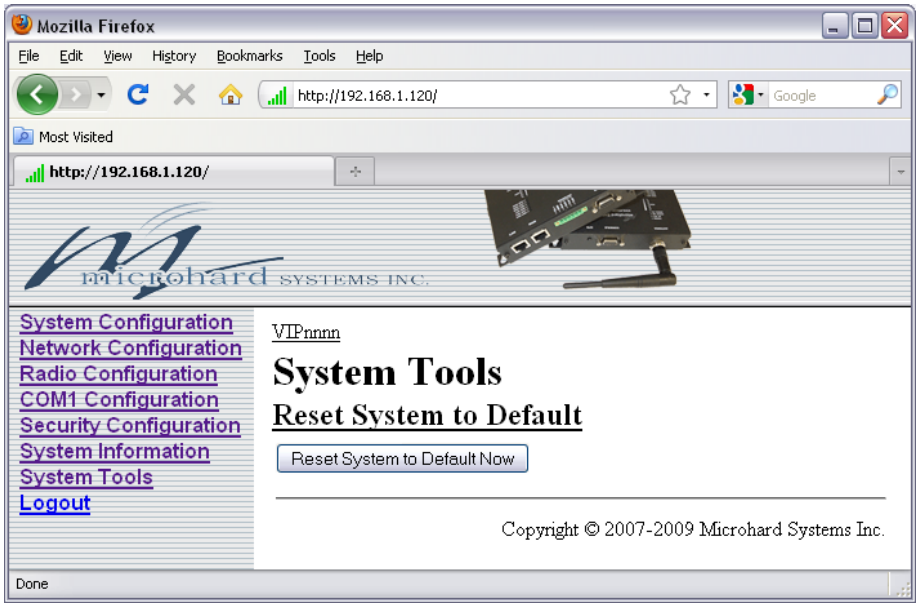


Image 6AY: System Tools Menu, Reset System to Default

6.0 Configuration

6.1.9.4 Network Discovery

This is used to discover other VIP Series networks via wireless or wired connections. Note that the other units must be 'discoverable' or 'changeable' (as set in their configuration menu).

Image 6AZ: System Tools, Network Discovery

6.1.9.5 Logout

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

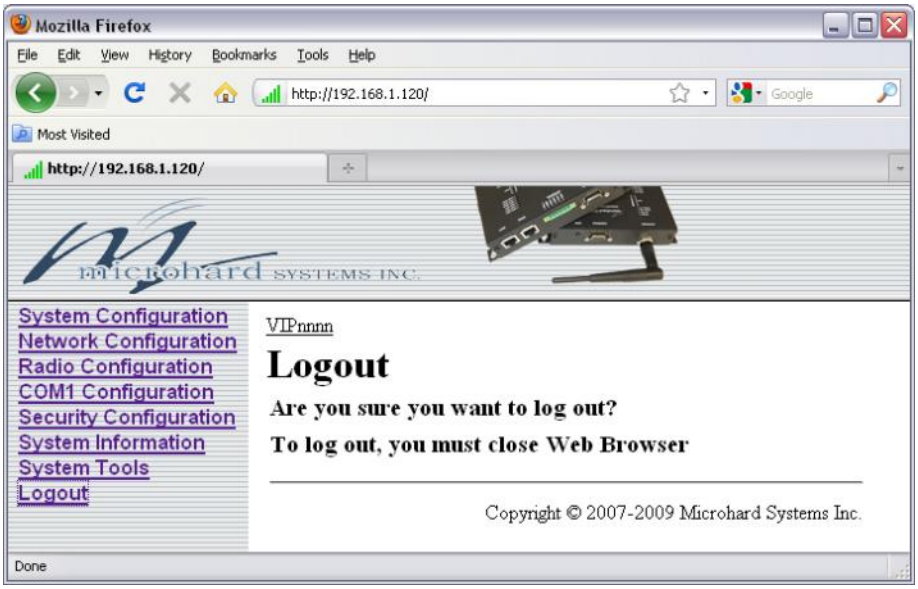


Image 6BA: Logout Window

6.0 Configuration

6.2 Text User Interface

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

- connect the VIP Series's CONSOLE port to an available COM port on your PC, using a straight-through 9-pin serial cable.
- run a terminal program (e.g. HyperTerminal) for the connected PC COM port, configured for 115200bps, 8 data bits, no parity, and 1 stop bit. Flow control should be set to 'none'.
- apply power to the VIP Series and wait approximately 40 seconds for the system to load - you will observe various text appearing in the terminal program window, culminating in the VIP Series login prompt which can be seen in the screen capture below:

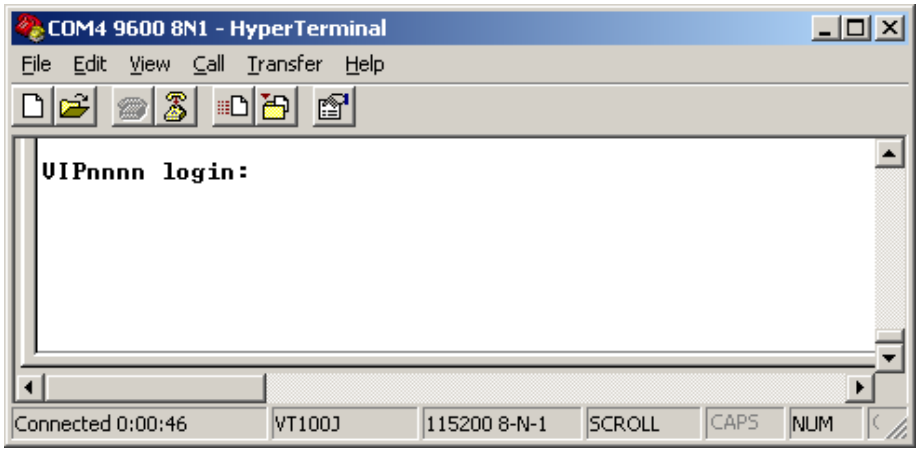


Image 6BB: Text User Interface, Login Prompt

- 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]*

6.0 Configuration

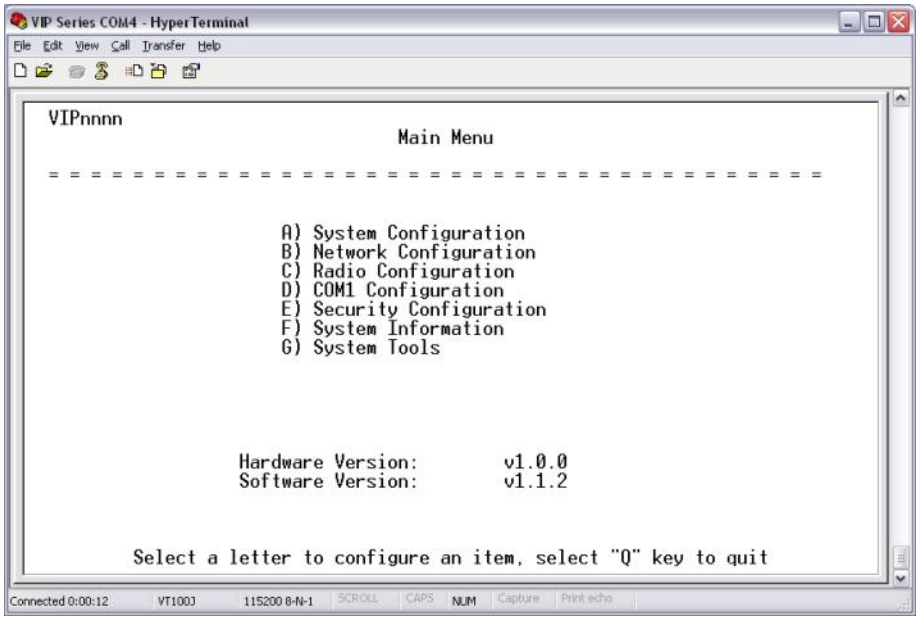


Image 6BC: Text User Interface, Main Menu

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 VIP Series unit 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 a VIP Series unit using the Text UI. The following steps pertaining to configuring the Radio portion of the unit will highlight those differences:

continued...

6.0 Configuration

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

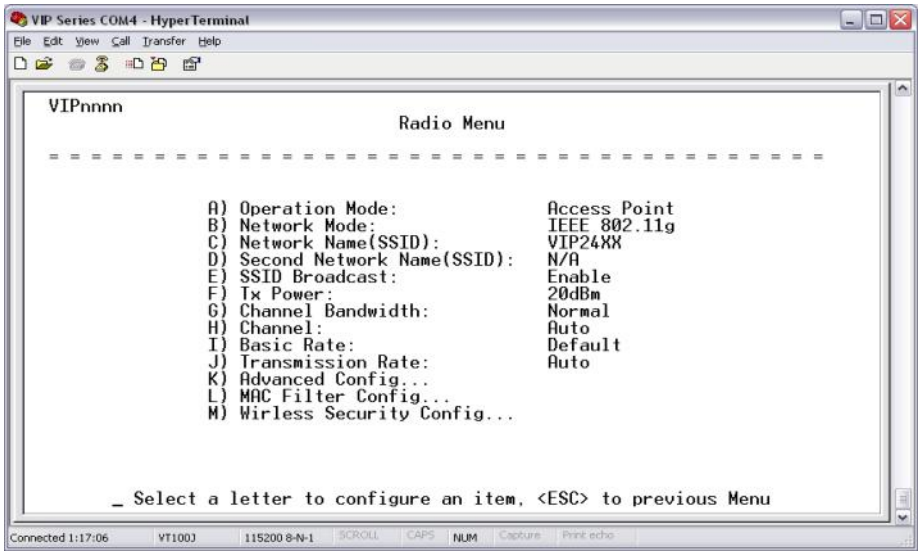


Image 6BD: Text User Interface, Radio (Configuration) Menu

- Select ‘A’ to change the Operation Mode. The image below will appear. Select ‘B’ to choose ‘Station’.

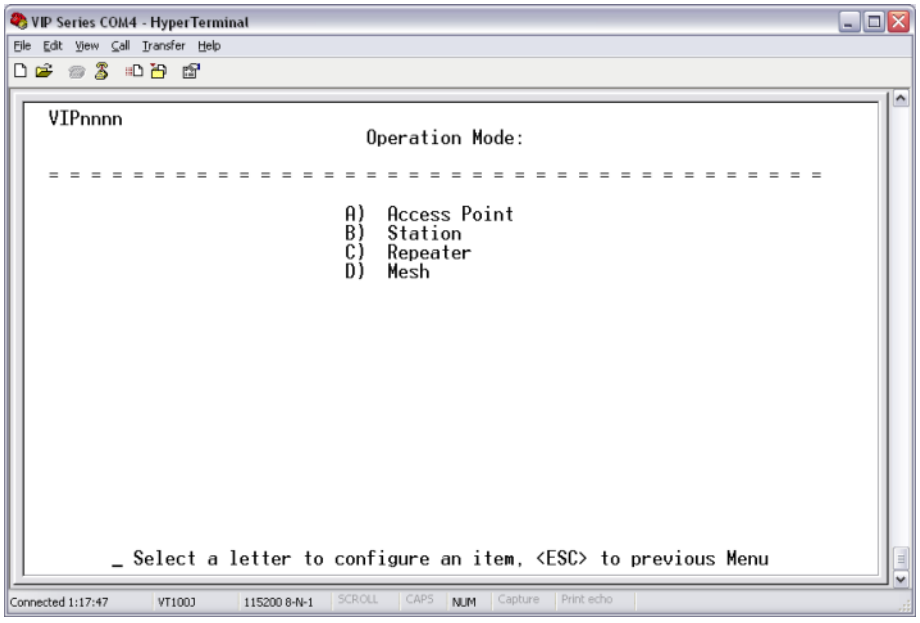


Image 6BE: Text User Interface, Radio Menu, Network Type

6.0 Configuration

- Having selected ‘B’. the Radio Menu appears showing the newly-selected Operation Mode:

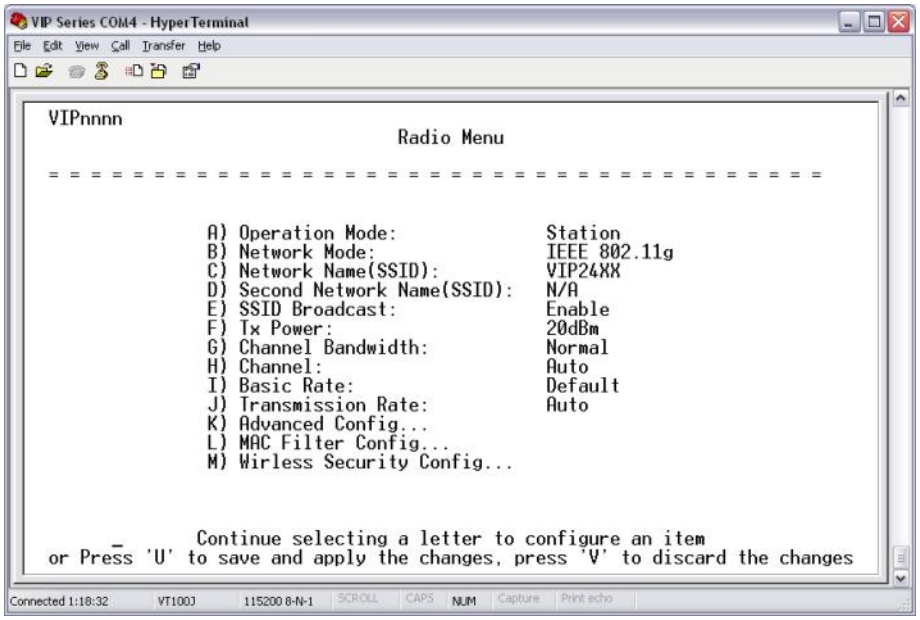


Image 6BF: Text User Interface, Radio Menu, Save Option

- 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.

Appendix F: Serial Interface

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

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

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

The signals in the asynchronous serial interface are described below:

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

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

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

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

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

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

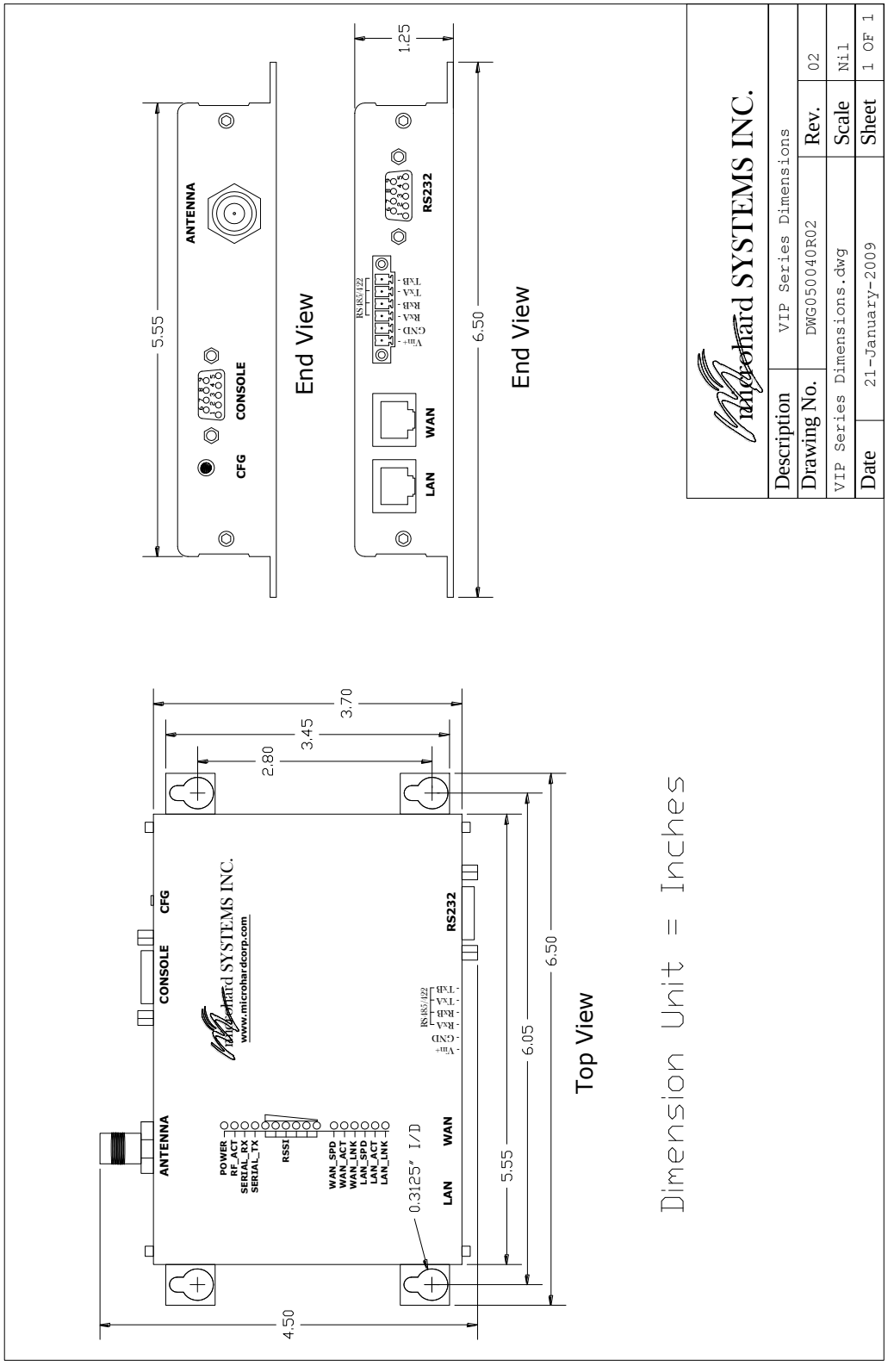
RTS *Request to Send* - Input to Module - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

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

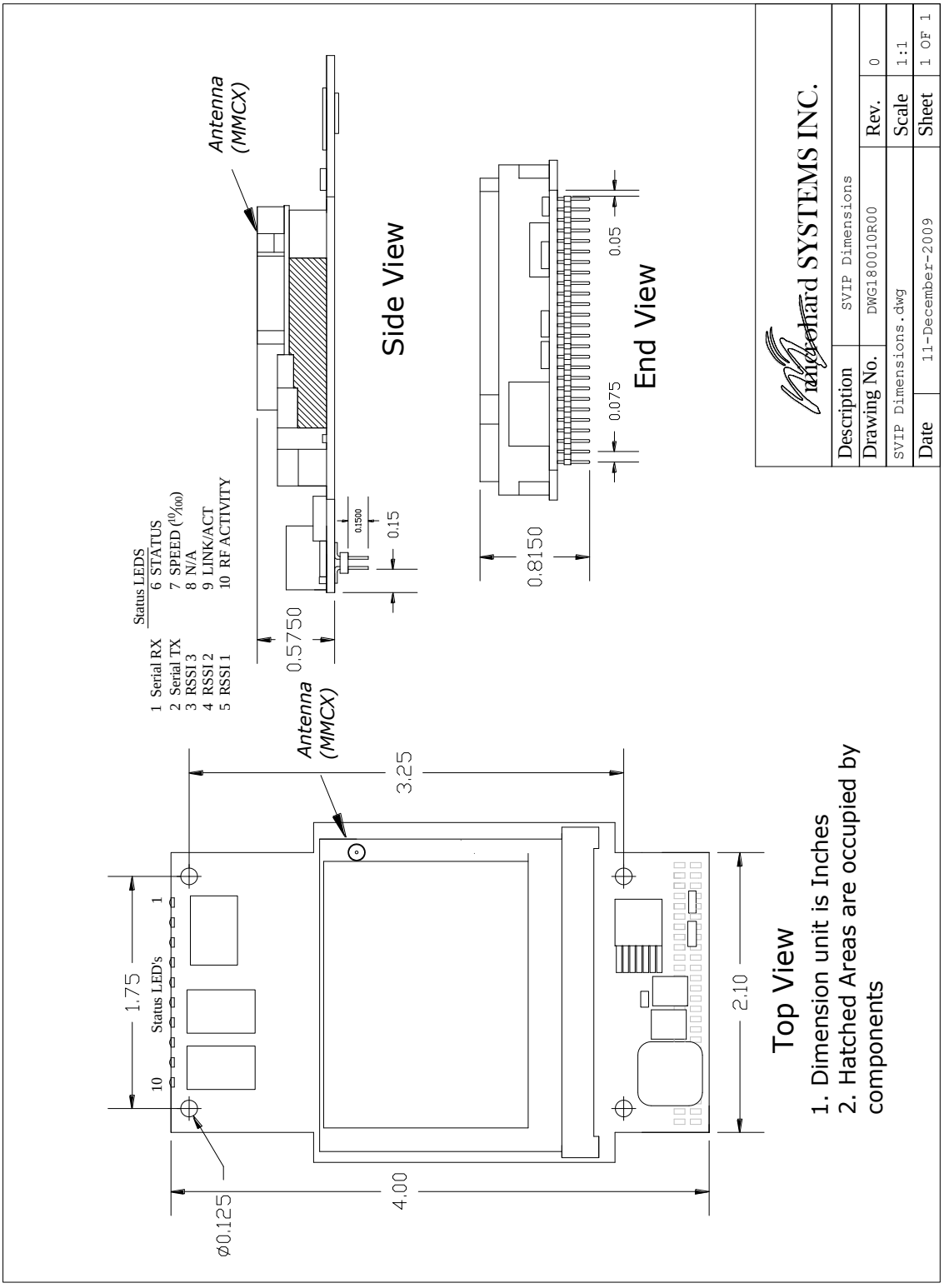
Notes: It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the module (DCE); the module transmits data on the RX line, and receives on TX.

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

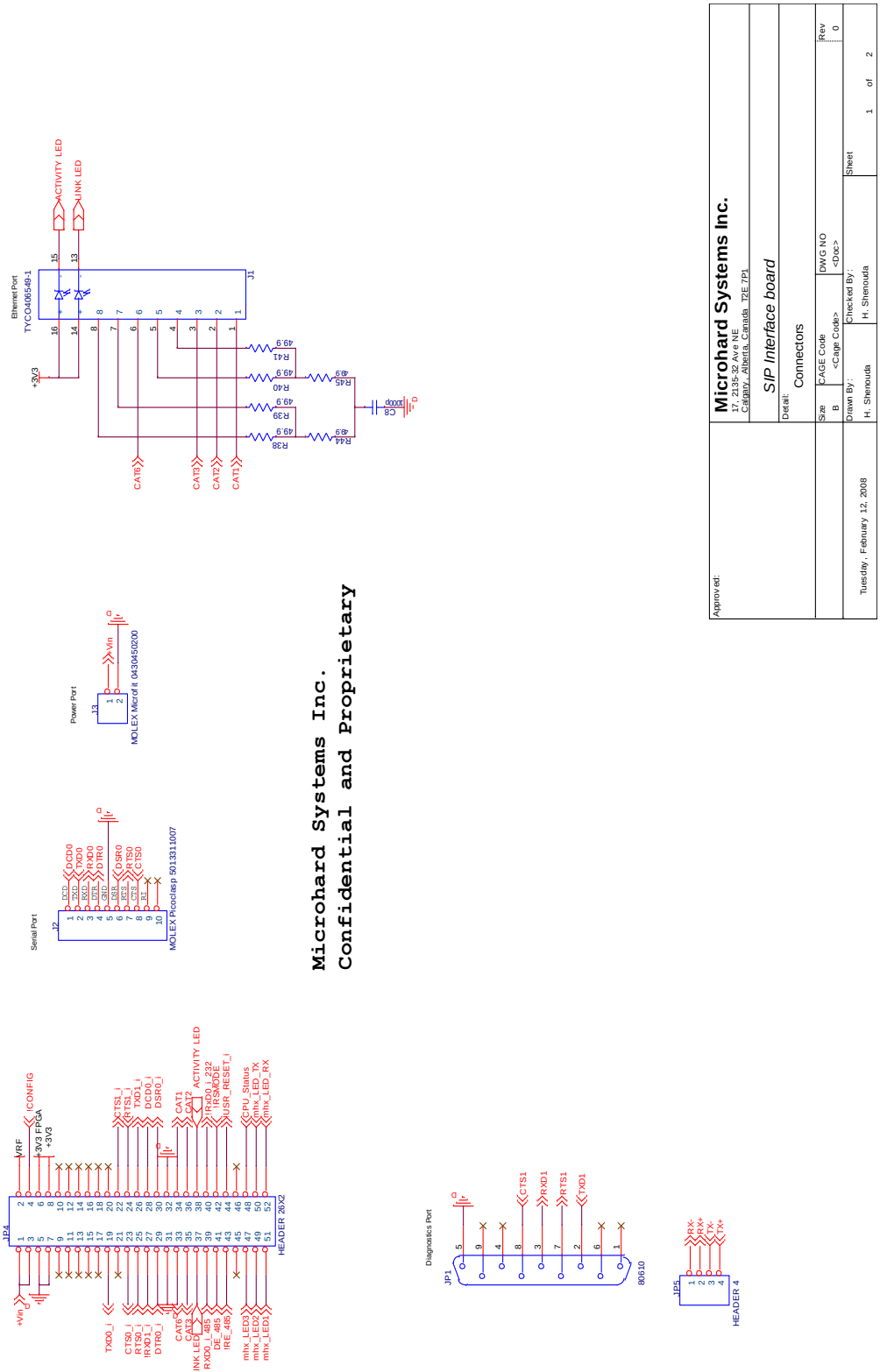
Appendix G: VIP Mechanical Drawing



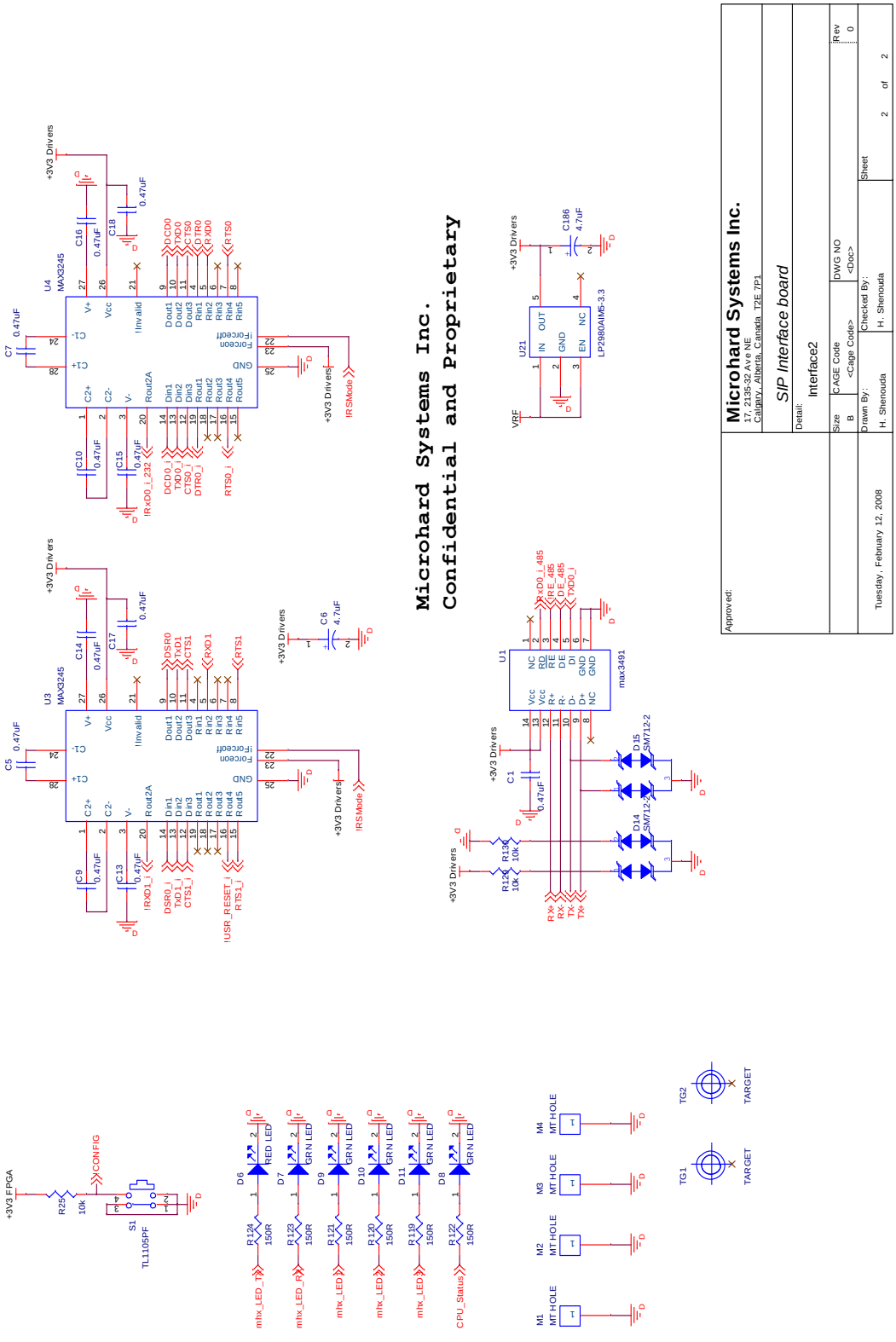
Appendix H: SVIP Mechanical Drawing



Appendix I: SVIP Interface Schematic (Sample)



Appendix I: SVIP Interface Schematic (Sample)



Appendix I: Firmware Upgrade / Recovery

Package upgrade or recovery upgrade can be used. Package upgrade will keep settings intact. Recovery upgrade will upgrade a unit completely, it can also be used to recovery from a corrupted system.

Package upgrade (*.pkg)

Ø Download upgrade package and put it into a known directory;

Ø Start up a command line window from the system;

Ø Change current directory to where the package file is located;

Ø Start a FTP session to the unit;

Ø Provide proper user name and password to login; (username: upgrade; passwd: admin)

Ø Change transfer protocol to *BINARY* mode;

Ø Push package upgrade file into the system with “put” command;

Ø Package upgrade takes up to 2 minutes to complete.

Recovery upgrade (*.img)

Ø Download recovery image and save it into a known directory;

Ø Start up a command line window from the system;

Ø Change current directory to where the package file is located;

Ø Cycle power on the unit with CFG button pressed and held down until “RSSIs, TX and RX” LED is observed in flash mode;

Ø Start a FTP session to IP address *192.168.1.39 from LAN port*;

Ø Provide proper user name and password to login (username: upgrade; passwd: admin);

Ø Change transfer protocol to *BINARY* mode;

Ø Push package upgrade file into the system with “put” command;

Ø Package upgrade takes more than 2 minutes to complete.

Ø The unit automatically reboots after the recovery procedure is completed

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

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