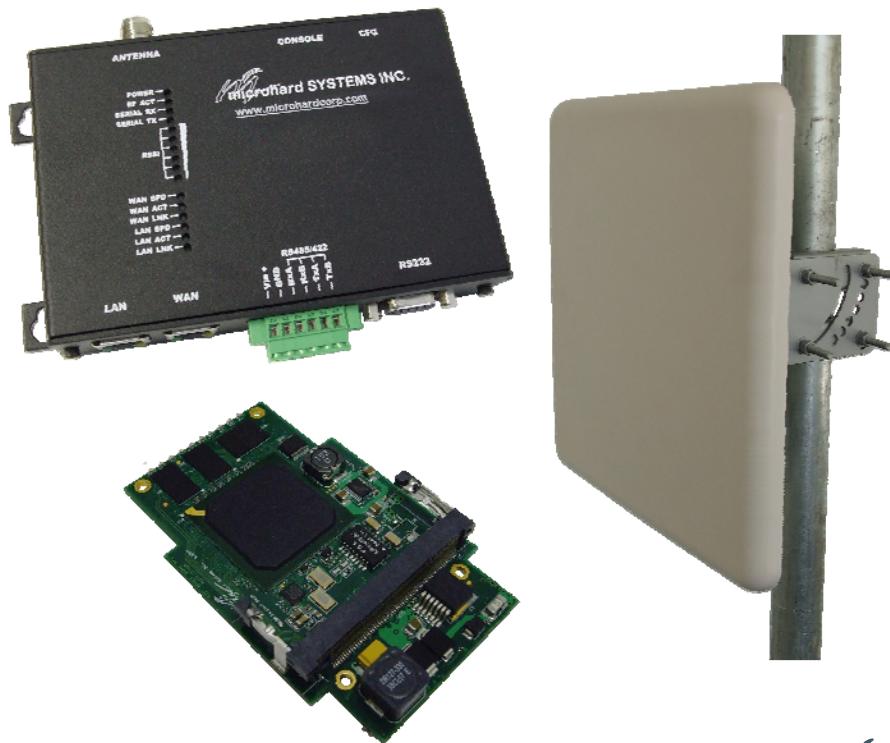


# Operating Manual

VIP2.0 Series  
OFDM Broadband Ethernet Bridge/Serial Gateway  
Document: VIP2.0 Series Operating Manual.v1.0

October 2011



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

Phone: (403) 248-0028  
Fax: (403) 248-2762  
[www.microhardcorp.com](http://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 Disclaimers**

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

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

### **Indemnification**

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

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

### **Proprietary Rights**

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

## Important User Information (continued)

---

### About This Manual

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

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

**Caution or Warning**

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

**Point to Remember**

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

**Tip**

An idea or suggestion to improve efficiency or enhance usefulness.

**Information**

Information regarding a particular technology or concept.

## Important User Information (continued)

---

### Regulatory Requirements

**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 | Description      | Initials | Date     |
|----------|------------------|----------|----------|
| 1.0      | New WebUI Format | PEH      | Oct 2011 |
|          |                  |          |          |
|          |                  |          |          |
|          |                  |          |          |

## Table of Contents

|  |           |
|--|-----------|
| <b>1.0 Overview .....</b>                              | <b>10</b> |
| 1.1 Performance Features .....                         | 10        |
| 1.2 Specifications .....                               | 12        |
| <b>2.0 QUICK START.....</b>                            | <b>14</b> |
| 2.1 Getting Started .....                              | 14        |
| 2.2 Simple Access Point and Station .....              | 17        |
| 2.2.1 Configuring the Access Point .....               | 17        |
| 2.2.2 Configuring the Station/Client.....              | 19        |
| 2.2.3 Testing the Connection .....                     | 21        |
| 2.3 Simple Mesh Network .....                          | 22        |
| 2.3.1 Configuring the Mode Points .....                | 22        |
| <b>3.0 Hardware Features .....</b>                     | <b>25</b> |
| 3.1 VIP Series .....                                   | 25        |
| 3.1.1 VIP Mechanical Drawings .....                    | 26        |
| 3.1.2 VIP Connections.....                             | 27        |
| 3.1.2.1 Front.....                                     | 27        |
| 3.1.2.2 Rear .....                                     | 29        |
| 3.1.3 VIP Indicators .....                             | 30        |
| 3.2 SVIP .....   | 31        |
| 3.2.1 SVIP Mechanical Drawings .....                   | 32        |
| 3.2.2 SVIP Pin-outs .....                              | 33        |
| 3.2.3 SVIP Indicators.....                             | 36        |
| 3.3 VIP4900/5800-ANT .....                             | 37        |
| 3.3.1 VIP4900/5800-ANT Mechanical Drawings .....       | 38        |
| <b>4.0 Operating Modes .....</b>                       | <b>40</b> |
| 4.1 Access Point (AP) .....                            | 40        |
| 4.2 Station/Client (ST) .....                          | 40        |
| 4.3 Repeater.....                                      | 41        |
| 4.4 Mesh Point .....                                   | 41        |
| <b>5.0 Network Topologies .....</b>                    | <b>42</b> |
| 5.1 Access Point (AP) to Station (ST) .....            | 42        |
| 5.2 AP to Multiple STs.....                            | 42        |
| 5.3 AP with Multiple STs to AP with Multiple STs ..... | 42        |
| 5.4 AP with Repeaters .....                            | 43        |
| 5.5 Mesh .....   | 43        |
| <b>6.0 Configuration.....</b>                          | <b>44</b> |
| 6.0 Web User Interface .....                           | 44        |
| 6.0.1 Logon Window.....                                | 45        |
| 6.1 System .....                                       | 46        |
| 6.1.1 Info.....  | 46        |
| 6.1.2 Settings.....                                    | 47        |
| Host Name.....   | 47        |
| Default System Mode (Bridge/Router) .....              | 47        |
| Date/Time .....  | 48        |
| NTP Server Settings.....                               | 49        |
| HTTP Port Settings.....                                | 49        |

## Table of Contents

---

|            |                                       |           |
|------------|---------------------------------------|-----------|
| 6.1.3      | Access Control .....                  | 50        |
|            | Password Change .....                 | 50        |
|            | Users .....                           | 50        |
| 6.1.4      | Maintenance .....                     | 52        |
|            | Version Information .....             | 52        |
|            | Firmware Upgrade.....                 | 52        |
|            | Reset to Default.....                 | 53        |
|            | Backup & Restore Configurations ..... | 53        |
| 6.1.5      | Reboot .....                          | 54        |
| <b>6.2</b> | <b>Network .....</b>                  | <b>55</b> |
| 6.2.1      | Status .....                          | 55        |
| 6.2.2      | Networks.....                         | 56        |
|            | LAN Configuration .....               | 57        |
|            | WAN Configuration.....                | 58        |
|            | DNS Configuration.....                | 58        |
| 6.2.3      | DHCP .....                            | 59        |
|            | LAN DHCP .....                        | 59        |
|            | Active DHCP Leases.....               | 59        |
| 6.2.4      | SNMP .....                            | 60        |
| 6.2.5      | sdpServer .....                       | 63        |
|            | Discovery Server Status.....          | 63        |
| <b>6.3</b> | <b>Wireless.....</b>                  | <b>64</b> |
| 6.3.1      | Status .....                          | 64        |
|            | General Status.....                   | 64        |
|            | Traffic Status .....                  | 64        |
| 6.3.2      | Radio1 .....                          | 65        |
|            | Radio Phy Configuration .....         | 65        |
|            | Radio Virtual Interface.....          | 67        |
|            | Operating Mode.....                   | 68        |
|            | TX Rate .....                         | 68        |
|            | TX Power.....                         | 69        |
|            | SSID .....                            | 69        |
|            | Encryption Type.....                  | 70        |
|            | MAC Filter.....                       | 71        |
| <b>6.4</b> | <b>Comport .....</b>                  | <b>72</b> |
| 6.4.1      | Status .....                          | 72        |
| 6.4.2      | Com1 .....                            | 73        |
|            | Data Baud Rate .....                  | 74        |
|            | IP Protocol Config.....               | 77        |
|            | TCP Client .....                      | 77        |
|            | TCP Server.....                       | 77        |
|            | TCP Client/Server..                   | 78        |
|            | UDP Point-to-Point .....              | 78        |
|            | UDP Point-to-Multipoint (P) .....     | 78        |
|            | UDP Point-to-Multipoint (MP)          | 79        |
|            | UDP Multipoint-to-Multipoint .....    | 79        |
|            | SMTP Client.....                      | 80        |
| <b>6.5</b> | <b>Status .....</b>                   | <b>81</b> |
| 6.5.1      | DHCP .....                            | 81        |
|            | ARP Cache .....                       | 81        |
| 6.5.2      | Mesh.....                             | 82        |
|            | Mesh Routing Table .....              | 82        |

## Table of Contents

---

|   |               |
|---|---------------|
| <b>6.6 Tools .....</b>                                | <b>83</b>     |
| 6.6.1 Discovery .....                                 | 83            |
| 6.6.2 Site Survey .....                               | 84            |
| Wireless Survey.....                                  | 84            |
| 6.6.3 Ping .....                                      | 85            |
| 6.6.4 TraceRoute .....                                | 86            |
| 6.6.5 Network Traffic .....                           | 87            |
| <b>6.7 Logout .....</b>                               | <b>88</b>     |
| 6.7.1 Logout .....                                    | 88            |
| <br><b>Appendices .....</b>                           | <br><b>89</b> |
| Appendix A: Serial Interface.....                     | 89            |
| Appendix B: VIP Mechanical Drawing.....               | 90            |
| Appendix C: SVIP Mechanical Drawing .....             | 91            |
| Appendix D: VIP4900/5800-ANT Mechanical Drawing ..... | 92            |
| Appendix E: SVIP Interface Schematic (Sample) .....   | 93            |
| Appendix F: Firmware Recovery.....                    | 95            |

## 1.0 Overview



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.

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<sup>1</sup> frequency band, employing OFDM technology. The VIP4900 operates in the 4.9 GHz Public Safety Band.

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

### 1.1 Performance Features

Key performance features of the VIP Series include:

- transmission within a public, license-exempt band of the radio spectrum<sup>1</sup> - 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...

<sup>1</sup> 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)
- Mesh
- remote administration
- easy to manage through user interface, or SNMP
- 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

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

#### Electrical/General

|                           |   |
|---------------------------|---|
| <b>Frequency:</b>         | <b>VIP2400:</b> 2.4000 - 2.4835 GHz<br><b>VIP4900:</b> 4.9425 - 4.9875 GHz<br><b>VIP5800:</b> 5.7250 - 5.8750 GHz         |
| <b>Spread Method:</b>     | ODFM/QPSK/16QAM/64QAM   |
| <b>Radio Operation</b>    | <b>VIP2400:</b> 802.11b/g<br><b>VIP4900:</b> 802.11a<br><b>VIP5800:</b> 802.11a   |
| <b>TX Power:</b>          | 6 dBm - 30 dBm (Selectable)   |
| <b>Channel Bandwidth:</b> | 5/10/20/40 MHz (Selectable)   |
| <b>Error Detection:</b>   | ARQ   |
| <b>Data Encryption:</b>   | WEP, WPA(PSK), WPA2(PSK), WPA+WPA2 (PSK)<br>(Subject to Export Restrictions)  |
| <b>Range:</b>             | Up to 10+ miles (16km) (Antenna Dependant)  |
| <b>Sensitivity:</b>       | <b>VIP2400:</b> -97 dBm<br><b>VIP4900:</b> -94 dBm<br><b>VIP5800:</b> -94 dBm   |
| <b>Serial Baud Rate:</b>  | 300bps to 921kbps   |
| <b>Ethernet:</b>          | 10/100 BaseT, Auto - MDI/X, IEEE 802.3  |
| <b>Link Rate:</b>         | 6 Mbps - 54 Mbps (Auto or Selectable)   |
| <b>Network Protocols:</b> | TCP, UDP, TCP/IP, TFTP, ARP, ICMP, DHCP, HTTP, HTTPS*, SSH*, SNMP, FTP, DNS, Serial over IP<br>(* Only available in -AES) |
| <b>Operating Modes:</b>   | Access Point, Client/Station, Repeater, Mesh Point  |
| <b>Management:</b>        | Local Serial Console, Telnet, WebUI, SNMP, FTP & Wireless Upgrade   |
| <b>Diagnostics:</b>       | Status LED's, RSSI, remote diagnostics, SNR, TX/RX CCQ  |

## 1.0 Overview

### 1.2 Specifications (Continued)

#### Environmental

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

**Humidity:** 5% to 95% non-condensing

#### Mechanical

##### Dimensions:

**Enclosed:** 5.30" (135mm) X 3.50" (89mm) X 1.46" (37mm)

**SVIP:** 4.02" (102mm) X 2.55" (65mm) X 0.75" (19mm)

**-ANT:** 12.0" (305mm) X 12.0" (305mm) X 2.75" (70mm)

##### Weight:

**Enclosed:** Approx. 420 grams

**SVIP:** Approx. 100 grams

**-ANT:** Approx. 2.2 kg

##### Connectors:

**Antenna:** Enclosed: RP-TNC Female Bulkhead

SVIP: MMCX

-ANT: Optional (N-Female)

**Data, etc:** RS232 Data: DE-9 Female

Ethernet : RJ-45

## 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.

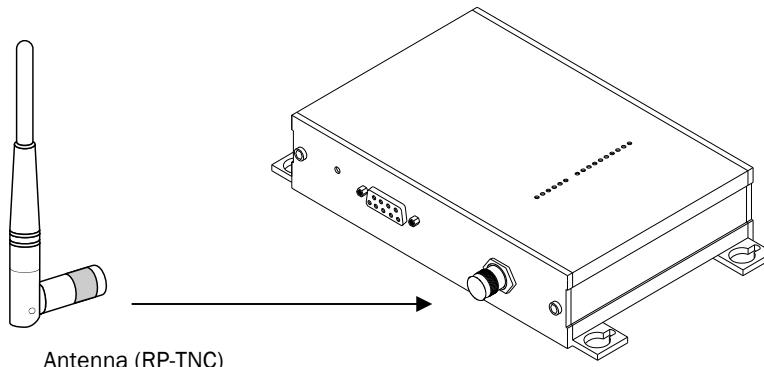
Note that the units arrive from the factory with a Radio Configuration of 'Access Point' and the Local Network setting configured as 'Static' (IP Address 192.168.168.1, Subnet Mask 255.255.255.0).

### 2.1 Getting Started



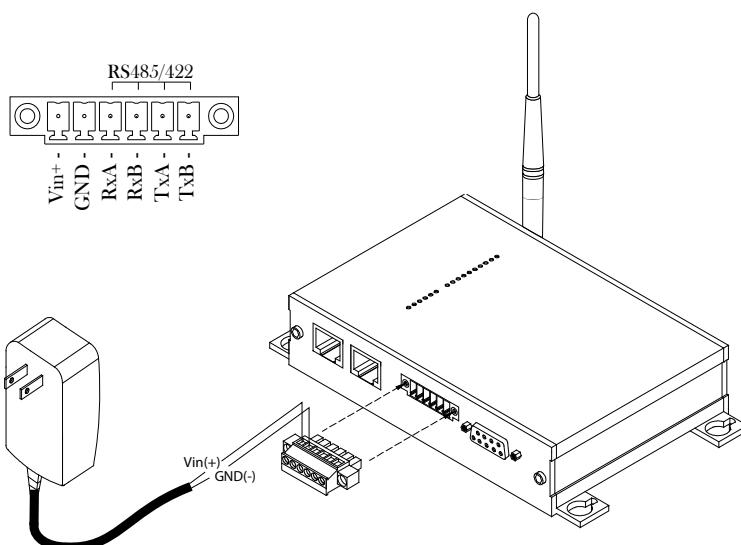
To reset to factory defaults, press and hold the CFG button for 8 seconds with the VIP powered up. The LED's will flash quickly and the VIP will reboot with factory defaults.

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



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

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

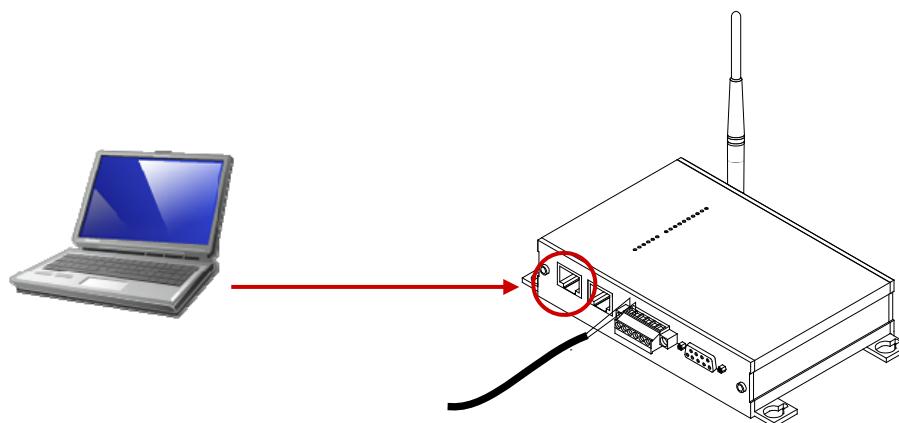


## 2.0 Quick Start

- ✓ 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 factory default network settings:

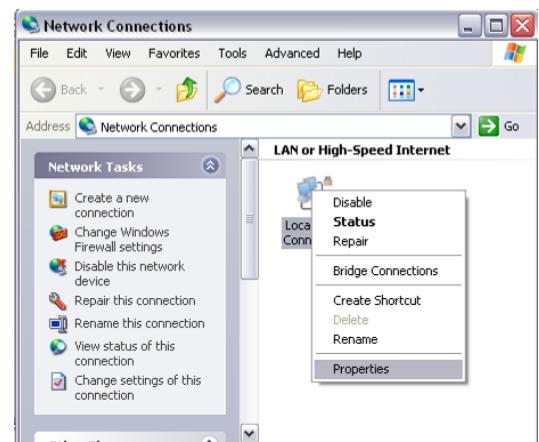
**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**

- ✓ The PC must have its Network Setting (TCP/IP Properties) set to STATIC with an IP Address of (e.g.) 192.168.168.10 and a Subnet Mask of 255.255.255.0

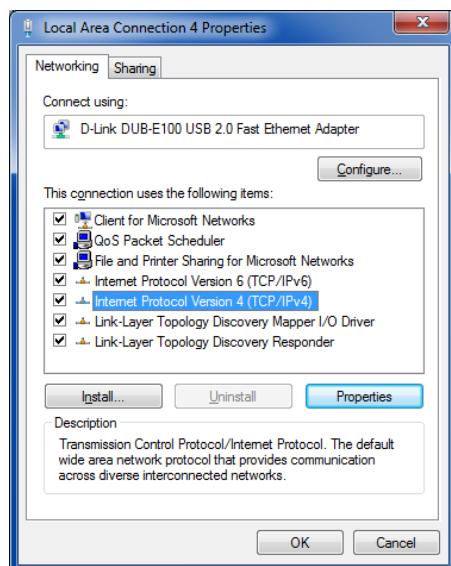
In **Windows XP** the TCP/IP Properties can be found in:

Start > Settings > Network Connections

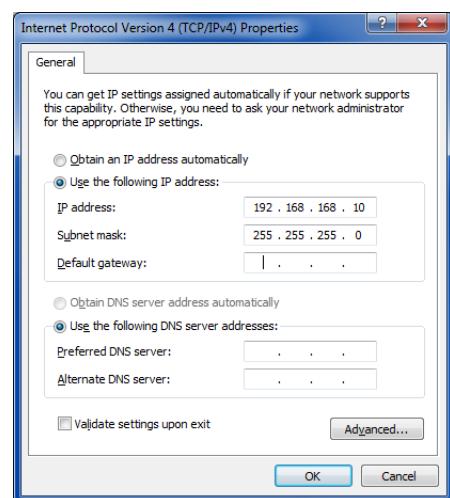
Select the *Local Area Connection* and right click and select **Properties**.



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



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



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

IP Address: **192.168.168.10**  
Subnet Mask: **255.255.255.0**

Click **OK**

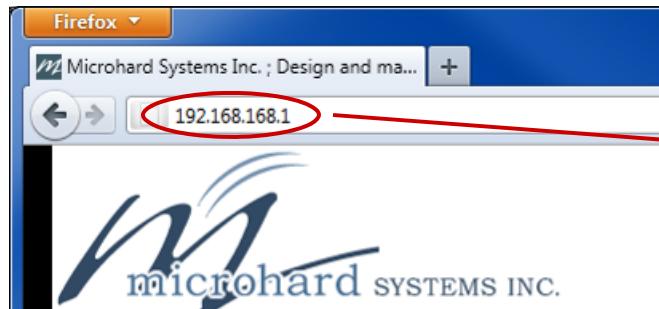
## 2.0 Quick Start

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



The factory default network settings:

**IP: 192.168.168.1**  
**Subnet: 255.255.255.0**



192.168.168.1

- ✓ 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**

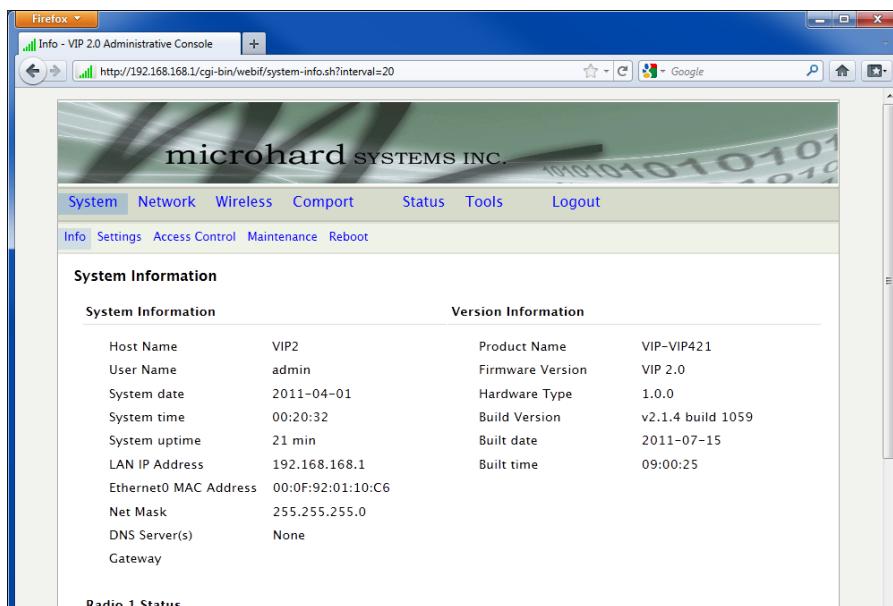
It is always a good idea to change the default admin login for future security.



The Factory default login:

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

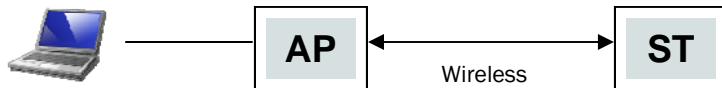
- ✓ Once successfully logged in, the Welcome Window will be displayed.



## 2.0 Quick Start

### 2.2 Simple Access Point and Station/Client

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/Client (ST). This example will show the basic steps required to set up each unit so that a simple network will be established.



#### 2.2.1 Configuring the Access Point

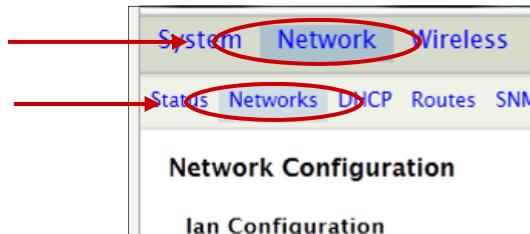
- ✓ Use [Section 2.1 Getting Started](#) to connect, power up and log in to a VIP Series unit.
- ✓ Give the VIP Series unit a unique IP address.



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

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

Select **Networks** from the submenu list.



| Network Configuration |                |
|-----------------------|----------------|
| Ian Configuration     |                |
| Connection Type       | Static IP      |
| IP Address            | 192.168.168.11 |
| Netmask               | 255.255.255.0  |
| Default Gateway       |                |

Refer to [Section 6.2.2 Networks](#) for additional information.

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

Enter the following Network Information:

**IP Address:** 192.168.168.11  
**IP Subnet Mask:** 255.255.255.0

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

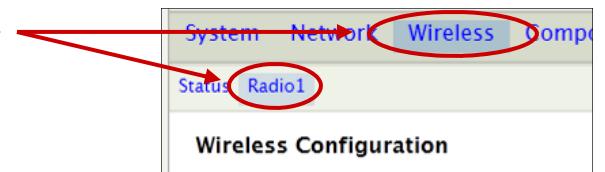
Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.

## 2.0 Quick Start

### 2.2.1 Configuring the Access Point (Con't)

- ✓ Configure the VIP Series as a Access Point

Select **Wireless** from the top/main navigation, and then **Radio1** from the submenu list.



| Radio1 Virtual Interface |  |
|--------------------------|--|
| Network                  | lan <input type="button" value="▼"/>   |
| Mode                     | <input type="button" value="Access Point"/> <input type="button" value="▼"/> |
| TX Rate                  | Auto <input type="button" value="▼"/>  |

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

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

**TESTSSID**

|                 |   |
|-----------------|---|
| TX Rate         | Auto <input type="button" value="▼"/>   |
| Tx Power        | 17 dbm <input type="button" value="▼"/> |
| WDS             | 10 dbm                                  |
| ESSID Broadcast | 11 dbm                                  |
| SSID            | 12 dbm                                  |
| Encryption Type | 13 dbm                                  |
| MAC Filter      | 14 dbm                                  |
|                 | 15 dbm                                  |
|                 | 16 dbm                                  |
|                 | 17 dbm                                  |
|                 | 18 dbm                                  |
|                 | 19 dbm                                  |

|                 |   |
|-----------------|---|
| Mode            | Access Point <input type="button" value="▼"/>                 |
| TX Rate         | Auto <input type="button" value="▼"/>                         |
| Tx Power        | 17 dbm <input type="button" value="▼"/>                       |
| WDS             | <input checked="" type="radio"/> On <input type="radio"/> Off |
| ESSID Broadcast | <input checked="" type="radio"/> On <input type="radio"/> Off |
| SSID            | <b>TESTSSID</b> <input type="button" value="▼"/>              |
| Encryption Type | Disabled <input type="button" value="▼"/>                     |

For bench or close proximity testing it is best to use a lower power setting to prevent RF saturation. Select 17dBm from the **TX Power** setting.

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

Refer to [Section 6.3 Wireless](#) for additional information.

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



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

## 2.0 Quick Start

### 2.2.2 Configuring the Station/Client

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

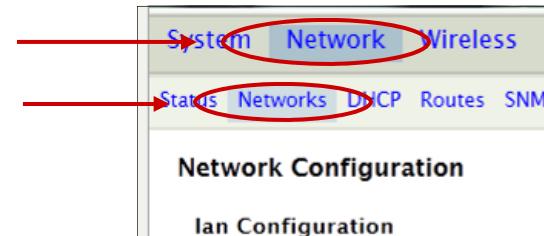
- ✓ Use ***Section 2.1 Getting Started*** to connect, power up and log in to a second VIP Series unit.
- ✓ Give the VIP Series unit an unique IP address.



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

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

Select **Networks** from the submenu list.



**Network Configuration**

**Ian Configuration**

|                 |                |
|-----------------|----------------|
| Connection Type | Static IP      |
| IP Address      | 192.168.168.12 |
| Netmask         | 255.255.255.0  |
| Default Gateway | 192.168.168.11 |

Refer to [Section 6.2.2 Networks](#) for additional information.

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

Enter the following Network Information:

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

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

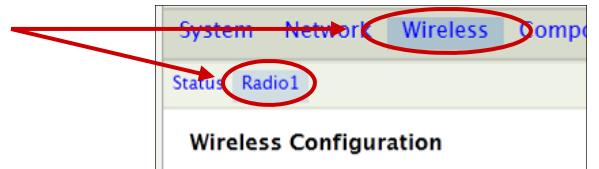
Once the IP Address is changed, you will need to type the new address into your browser to continue the configuration.

## 2.0 Quick Start

### 2.2.2 Configuring the Station/Client (Continued)

- ✓ Configure the VIP Series as a Station/Client.

Select **Wireless** from the top/main navigation, and then **Radio1** from the submenu list.



Radio1 Virtual Interface

Network

Ian

Mode

Client

TX Rate

Auto

Tx Power

17 dbm

WDS

Off

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

**TESTSSID**

TX Rate

Auto

Tx Power

17 dbm

WDS

Off

ESSID Broadcast

On

SSID

TESTSSID

Encryption Type

Disabled

MAC Filter

None

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

Mode

Client

TX Rate

Auto

Tx Power

17 dbm

WDS

On

ESSID Broadcast

On

SSID

TESTSSID

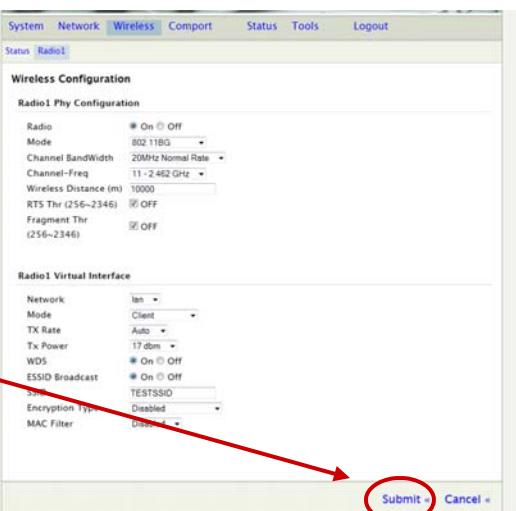
Encryption Type

Disabled

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

Refer to [Section 6.3 Wireless](#) for additional information.

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



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

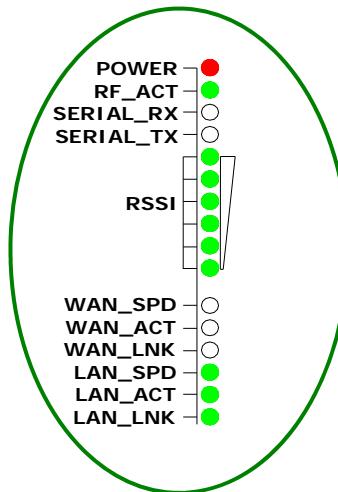
## 2.0 Quick Start

### 2.2.3 Testing the connection

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

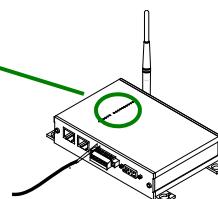


RSSI LED's that are 'cycling' or 'scanning' indicate that the unit is searching for a signal.

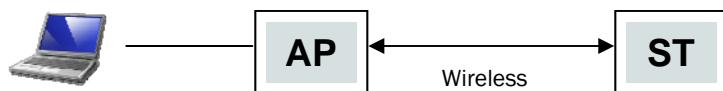


The **RSSI** LED's represent signal strength, the more LED's that are illuminated, the stronger the signal.

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/Client.



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

Log into the unit.

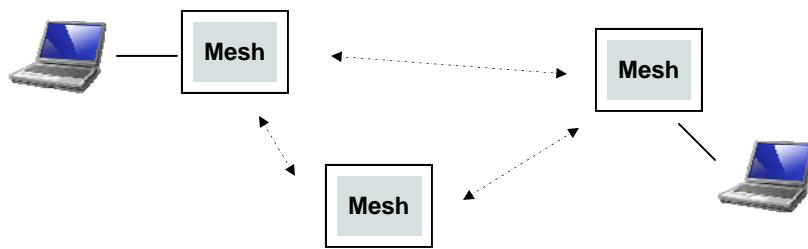
The System Info screen should be displayed

| System Information    |                   |                     |
|-----------------------|-------------------|---------------------|
| System Information    |                   | Version Information |
| Host Name             | CLGYCL1           | Product Name        |
| User Name             | admin             | Firmware Vers       |
| System date           | 2011-04-01        | Hardware Typ        |
| System time           | 01:07:06          | Build Version       |
| System uptime         | 1:05              | Built date          |
| LAN IP Address        | 192.168.168.12    | Built time          |
| Ethernet0 MAC Address | 00:0F:92:01:44:AA |                     |

## 2.0 Quick Start

### 2.3 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.



#### 2.3.1 Configuring the Mesh Node(s)

- ✓ Use [Section 2.1 Getting Started](#) to connect, power up and log in to a VIP Series unit.
- ✓ Configure all VIP Series units as Bridges.

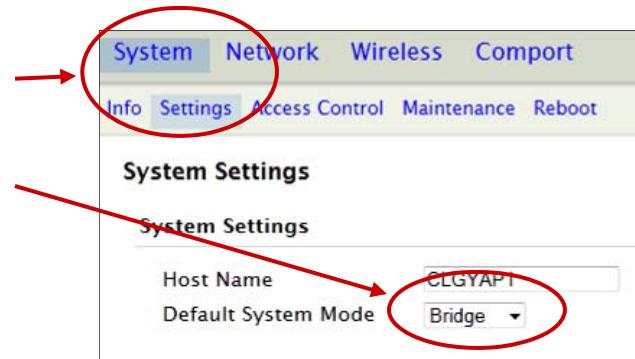


The configuration of each Mesh Node is very similar, the difference between units being each unit requires a different IP address.

Select **System > Settings** from the top navigation.

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

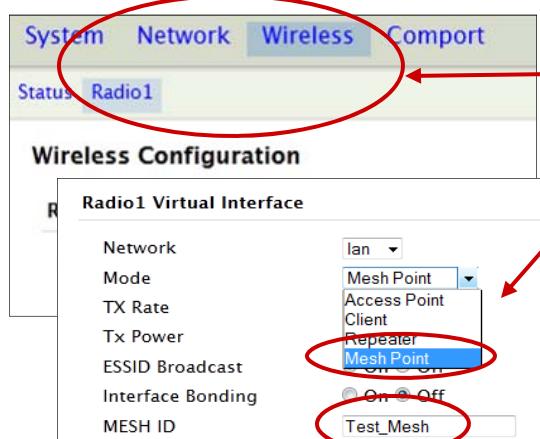
Click on the **Submit** button to write the changes to the VIP.



- ✓ Configure all VIP Series units as a Mesh nodes.



Each unit in a Mesh network must have the same MESH ID.



Select **Wireless > Radio1** from the top navigation.

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

Enter a unique **MESH ID**.

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

## 2.0 Quick Start

### 2.3.1 Configuring the Mesh Node (s) (Continued)

- ✓ Assign each VIP unit a unique IP Address.



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

Select **Network > Networks** from the top navigation.



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

| Network Configuration |                |
|-----------------------|----------------|
| lan Configuration     |                |
| Connection Type       | Static IP ▾    |
| IP Address            | 192.168.168.11 |
| Netmask               | 255.255.255.0  |
| Default Gateway       |                |

Refer to [Section 6.2.2 Networks](#) for additional information.

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

Assign each VIP a unique IP address.

Network Information for first VIP unit:

**IP Address:** 192.168.168.11  
**IP Subnet Mask:** 255.255.255.0

Network Information for second VIP unit:

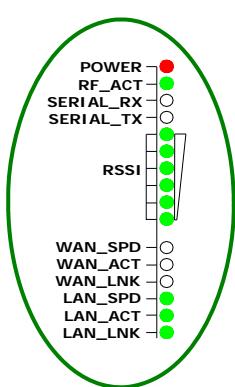
**IP Address:** 192.168.168.12  
**IP Subnet Mask:** 255.255.255.0

Network Information for Third VIP unit:

**IP Address:** 192.168.168.13  
**IP Subnet Mask:** 255.255.255.0

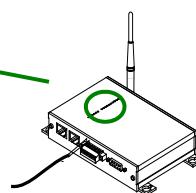
Click on the **Submit** button to write the changes to the VIP Series.

- ✓ 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.

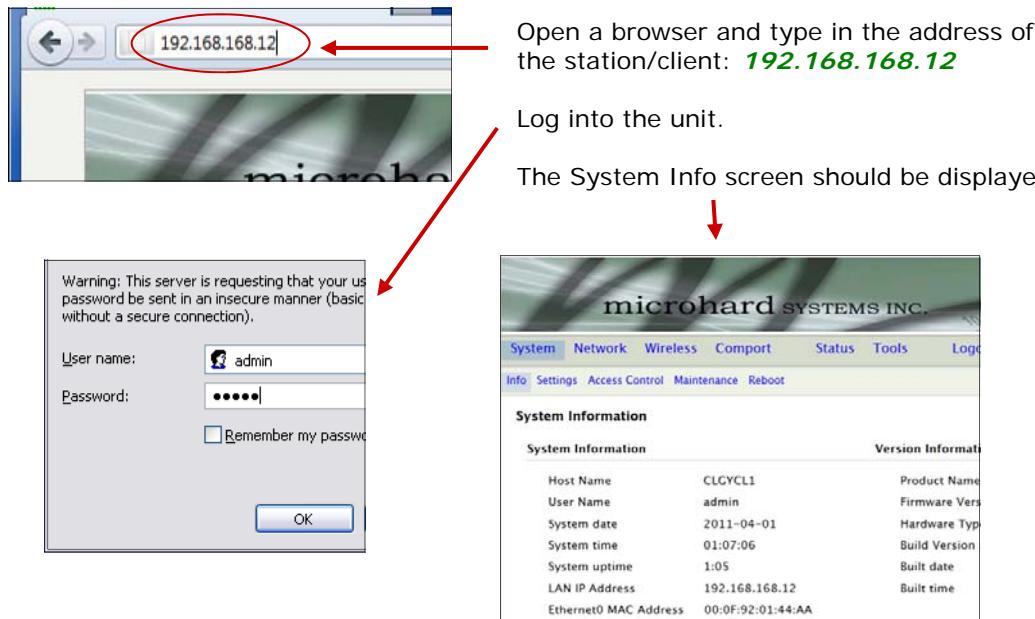
The **RF\_ACT** should be ON or Flashing to indicate activity over the RF Link.



## 2.0 Quick Start

### 2.3.1 Configuring the Mesh Node (s) (Continued)

- ✓ 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.



- ✓ Repeat for each Mesh Node.

## 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*

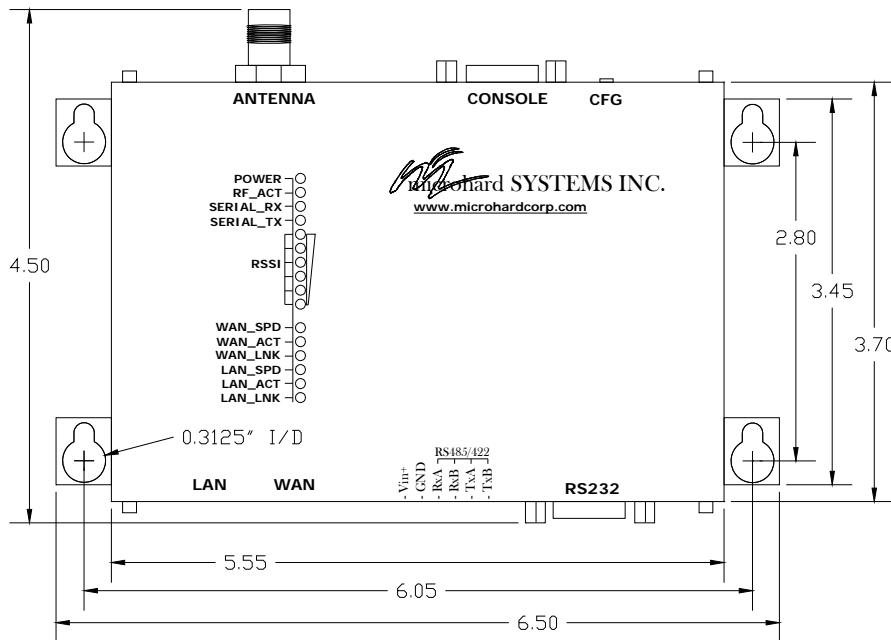
Any VIP Series may be configured as an Access Point (Router or Bridge), Station, Repeater or Mesh Node. This versatility is very convenient from a 'sparing' perspective, as well for convenience in becoming very familiar and proficient with using the device: if you are familiar with one unit, you will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

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

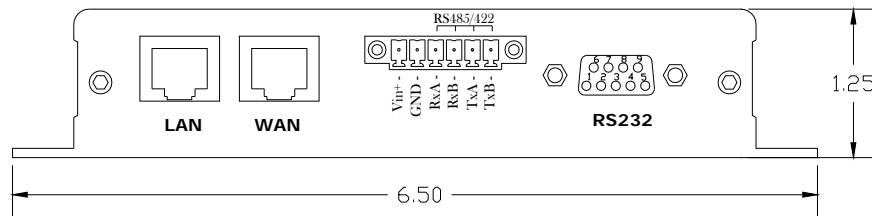
- Standard Connectors for:
  - Dual Ethernet Ports (RJ45)
  - Console Configuration Port (RS232/DB9)
  - Data Port (RS232/DB9)
  - Phoenix Type Connector for Power and RS485/422 Data Port
  - RP-TNC Antenna Connection
- Status/Diagnostic output signals for system status, RSSI, Ethernet etc.
- CFG Button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

## 3.0 Hardware Features

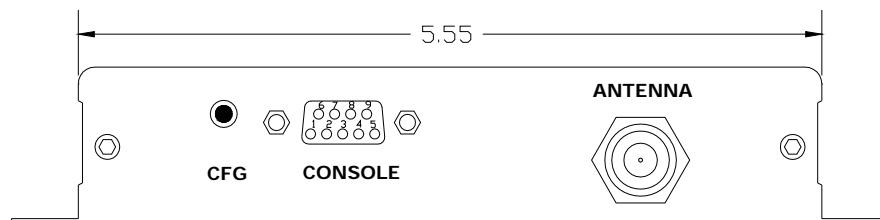
### 3.1.1 Mechanical Drawings



Drawing 3-1: VIP Top View Dimensions



Drawing 3-2: VIP Front View Dimensions



Drawing 3-3: VIP Rear View Dimensions

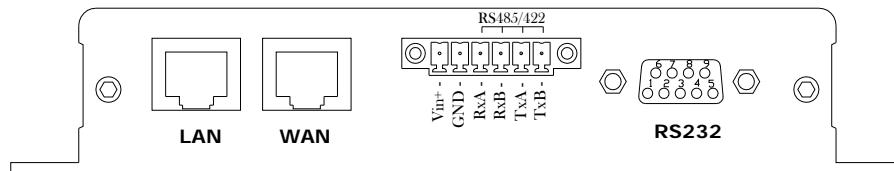
**Note: All dimension units: Inches**

## 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

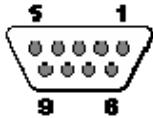


**Caution:** Using a power supply that does not provide proper voltage may damage the VIP Series unit.

- 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 for RS232 serial data (300 baud to 230.4kbps) communications.

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

### 3.0 Hardware Features



See [Appendix A](#) for a full description of the COM1 RS-232 interface functions.

| Pin Name | No. | Description         | In/<br>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          |



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

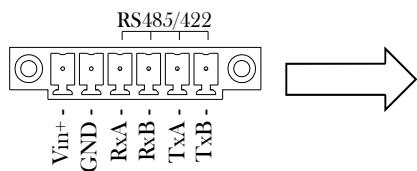


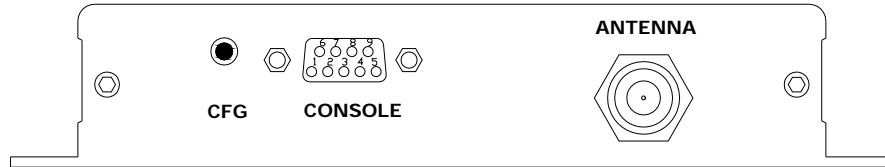
Table 3A: COM1 DE9S Pin Assignment

| Pin Name | No. | Description                              | In/<br>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: 192.168.168.1  
Subnet: 255.255.255.0  
Gateway: 192.168.1.1**

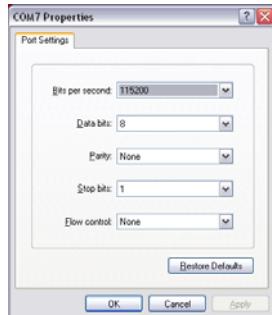
**With these settings a web browser can be used to configure the unit.**

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:**

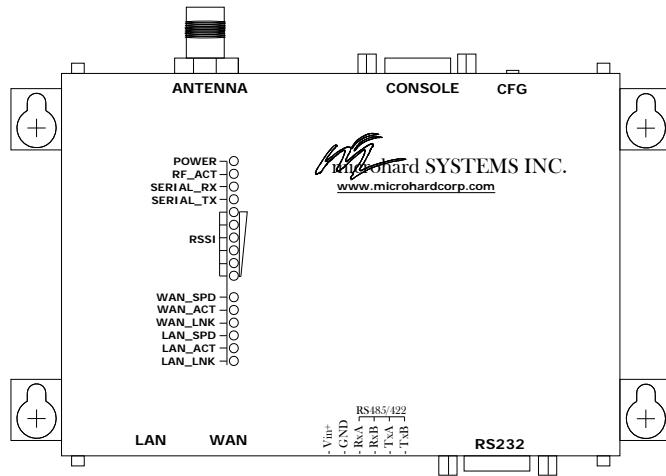
Bits per Second: **115,200**  
Data Bits: **8**  
Parity: **None**  
Stop bits: **1**  
Flow control: **None**

#### 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.



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

#### RF\_ACT

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

#### 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*

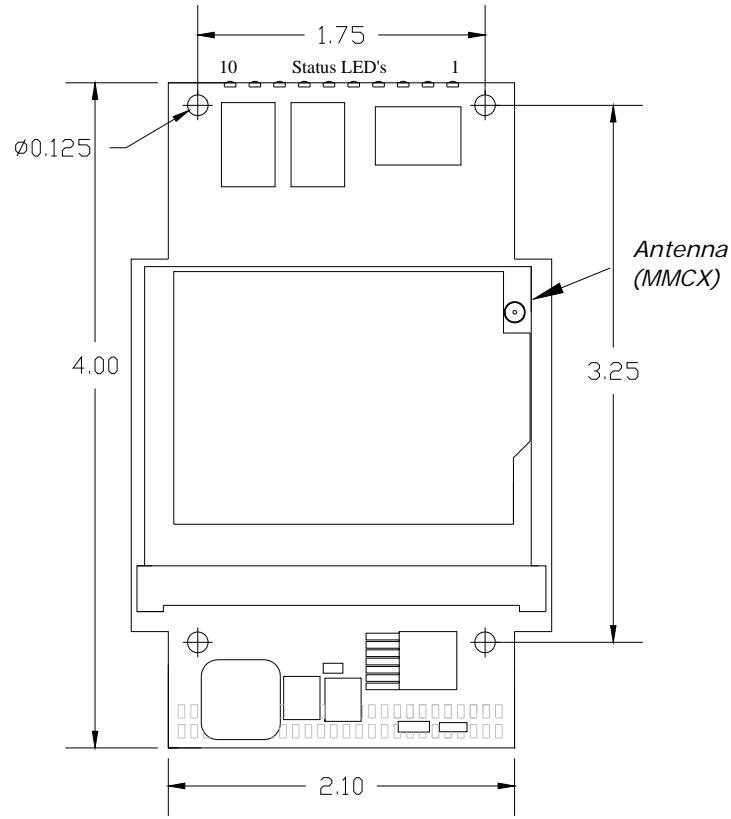
The SVIP Series OEM module features include:

- 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.

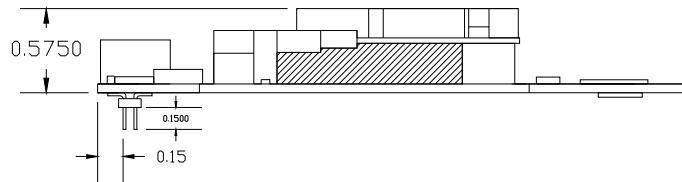
The Pin-out and signal descriptions are described on the following pages. An example customer interface schematic can be found in Appendix I.

## 3.0 Hardware Features

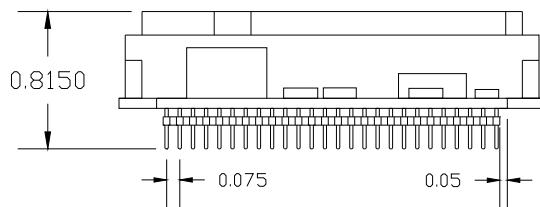
### 3.2.1 SVIP Mechanical Drawings



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

| SVIP<br>JP4 |              |
|-------------|--------------|
| Vcc         | 1            |
| Vcc         | 3            |
| GND         | 5            |
| GND         | 7            |
| NC          | 9            |
| NC          | 11           |
| NC          | 13           |
| NC          | 15           |
| NC          | 17           |
| TXD0        | 19           |
| NC          | 21           |
| CTS0        | 23           |
| RTS0        | 25           |
| !RXD1       | 27           |
| DTR0        | 29           |
| GND         | 31           |
| CAT6        | 33           |
| CAT3        | 35           |
| LINK LED    | 37           |
| RXD0_485    | 39           |
| DE_485      | 41           |
| !RE_485     | 43           |
| NC          | 45           |
| RSSI_LED3   | 47           |
| RSSI_LED2   | 49           |
| RSSI_LED1   | 51           |
|             | 2            |
|             | 4            |
|             | 6            |
|             | 8            |
|             | 10           |
|             | 12           |
|             | 14           |
|             | 16           |
|             | 18           |
|             | 20           |
|             | 22           |
|             | 24           |
|             | 26           |
|             | 28           |
|             | 30           |
|             | 32           |
|             | 34           |
|             | 36           |
|             | 38           |
|             | 40           |
|             | 42           |
|             | 44           |
|             | 46           |
|             | 48           |
|             | 50           |
|             | 52           |
|             |              |
|             | VRF          |
|             | !CONFIG      |
|             | +3V3 FPGA    |
|             | +3V3         |
|             | NC           |
|             | RTS1         |
|             | TXD1         |
|             | DCD0         |
|             | DSR0         |
|             | GND          |
|             | CAT1         |
|             | CAT2         |
|             | ACTIVITY LED |
|             | !RXD0_232    |
|             | !RSMODE      |
|             | !RESET       |
|             | NC           |
|             | SYS LED      |
|             | TX LED       |
|             | RX LED       |



*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/<br>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

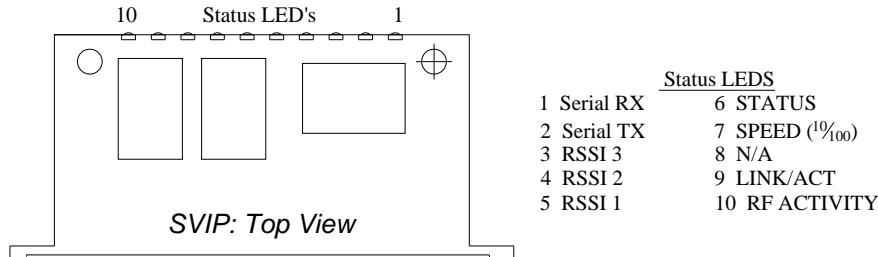
| Pin Name     | No.   | Description   | In/<br>Out |
|--------------|-------|---|------------|
| CAT6         | 33    | Ethernet RJ45 Pin 6.  |            |
| CAT1         | 34    | Ethernet RJ45 Pin 1.  |            |
| CAT3         | 35    | Ethernet RJ45 Pin 3.  |            |
| CAT2         | 36    | 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.



*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

### 3.3 VIP4900/5800-ANT

The VIP Antenna Series introduces a single unit solution, which integrates a VIP Series unit inside a weather resistant high gain antenna. The VIP4900/5800-ANT can operate as a Access Point, Station/Client, Repeater or Mesh Point 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*

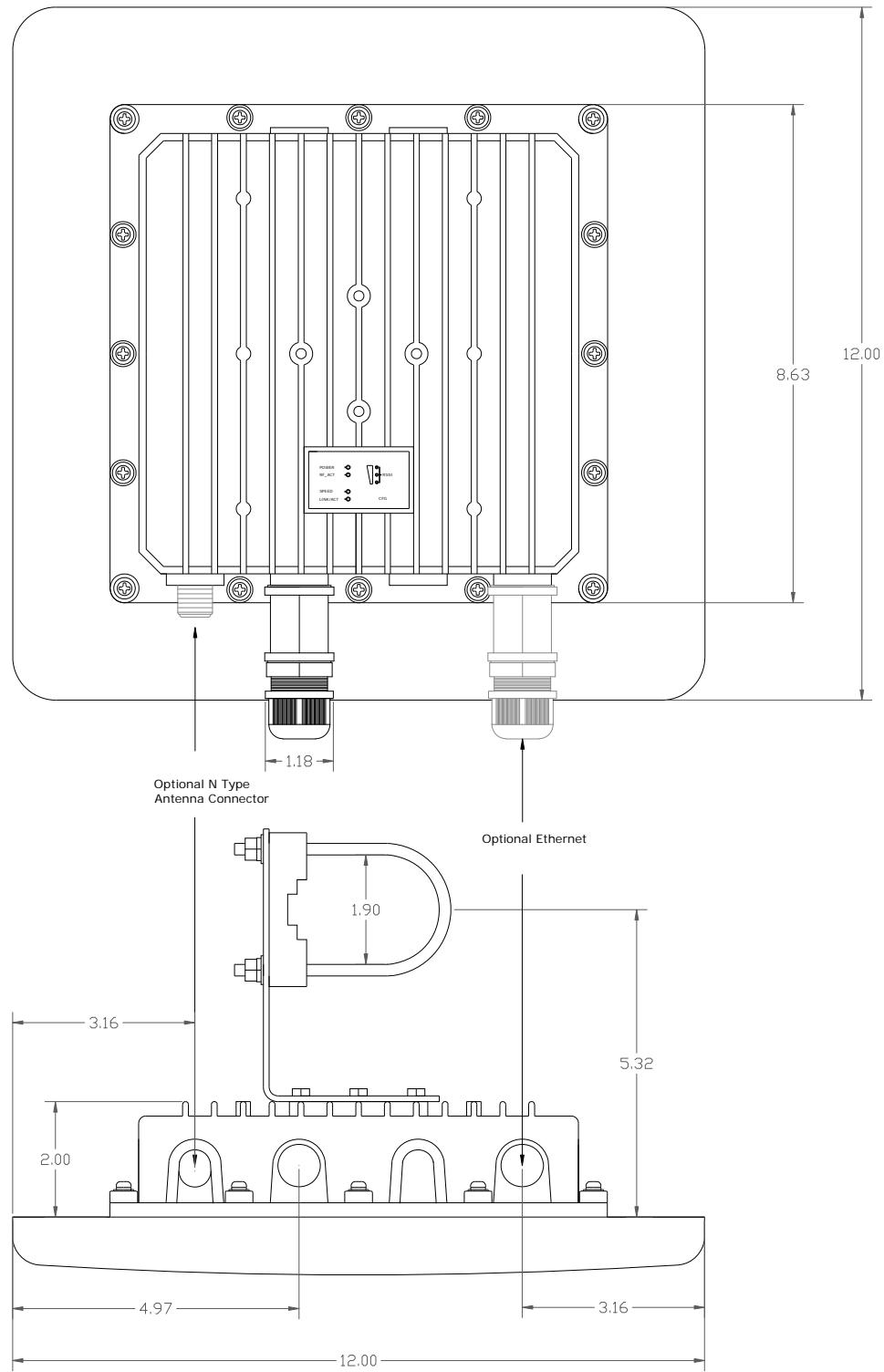
The VIP Antenna Series feature include:

- 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 (192.168.168.1), or otherwise set IP address must be known for local configuration through the LAN interface.

## 3.0 Hardware Features

### 3.3.1 VIP4900/5800-ANT Mechanical Drawings

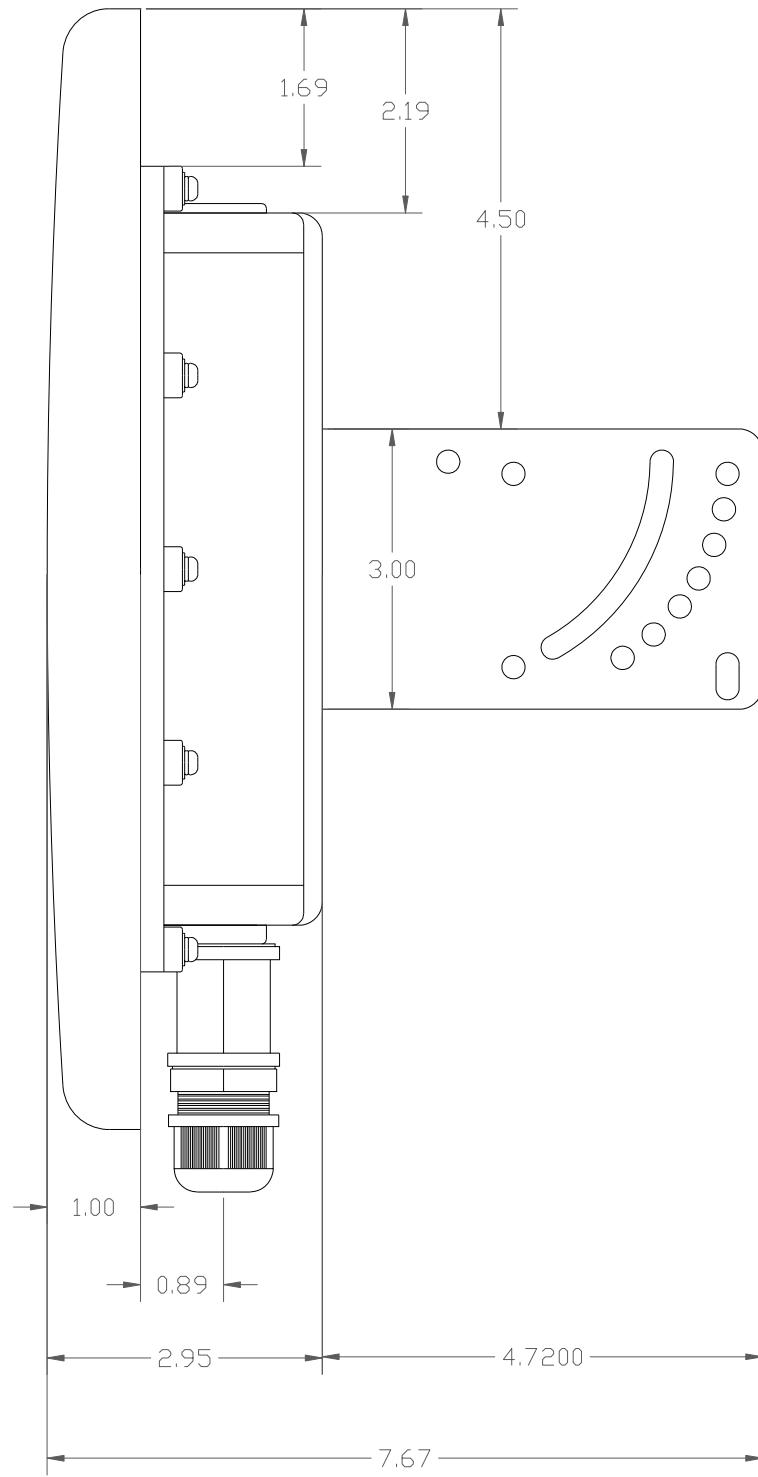


**Note: All dimension units: Inches**

Drawing 3-11: VIP Antenna Series Back & Bottom View

## 3.0 Hardware Features

### 3.2.1 VIP4900/5800-ANT Mechanical Drawings



**Note: All dimension units: Inches**

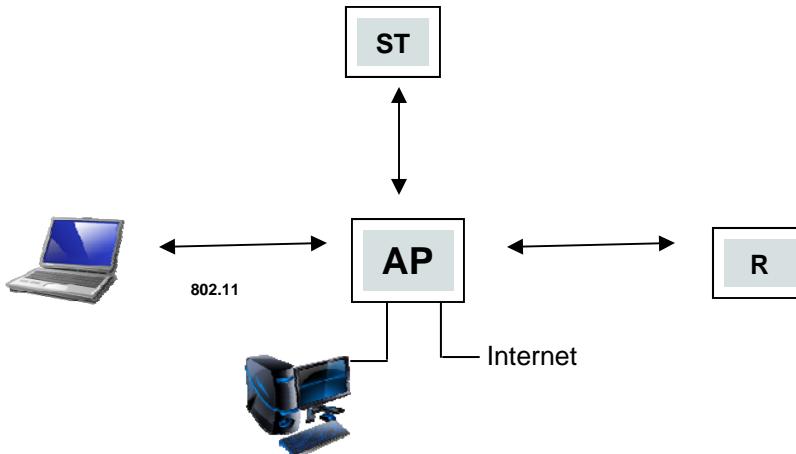
Drawing 3-12: VIP Antenna Series Side View

## 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.

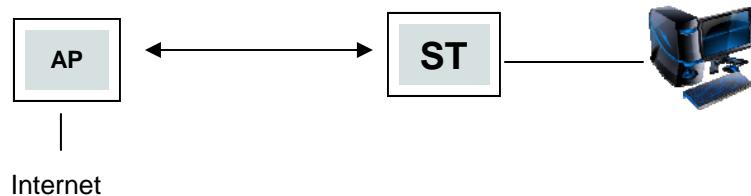
### 4.1 Access Point

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

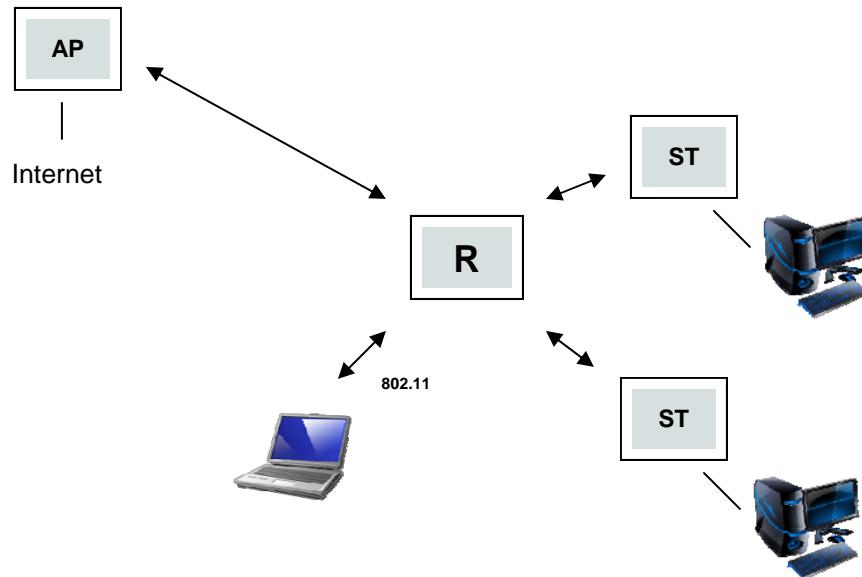
When operating as a station the VIP series can provide a single wireless connection to an access point or a repeater. A station allows a wired Ethernet or serial device access to the wireless network.



## 4.0 Operating Modes

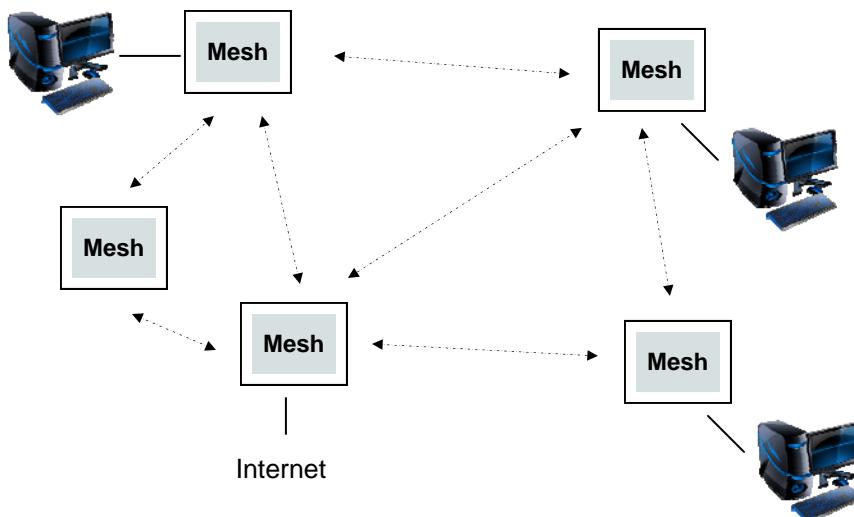
### 4.3 Repeater

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.

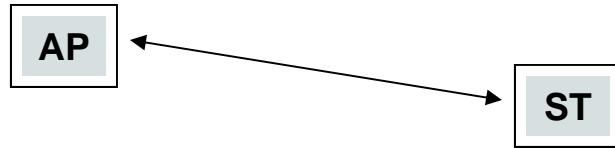


## 5.0 Network Topologies

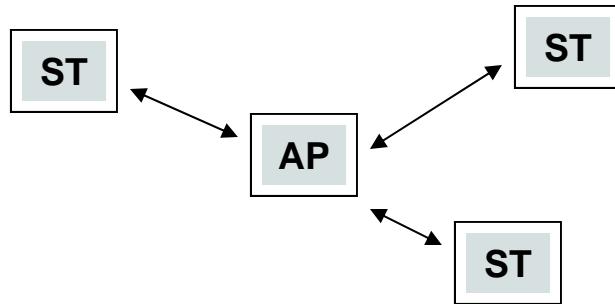
### 5.1 Access Point to Station



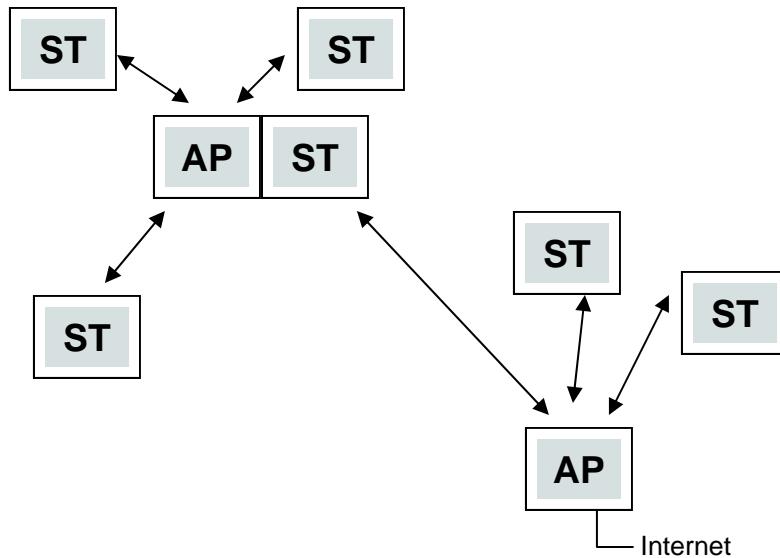
The network topology determines the paths available for the movement of data.



### 5.2 Access Point to Multiple Stations



### 5.3 Access Point with Multiple Stations to AP with Multiple STs

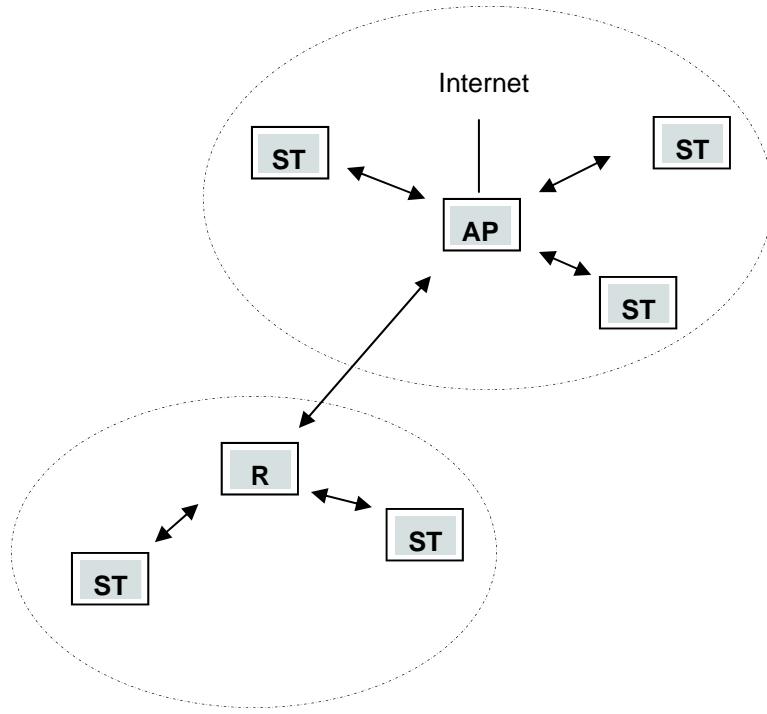


## 5.0 Network Topologies

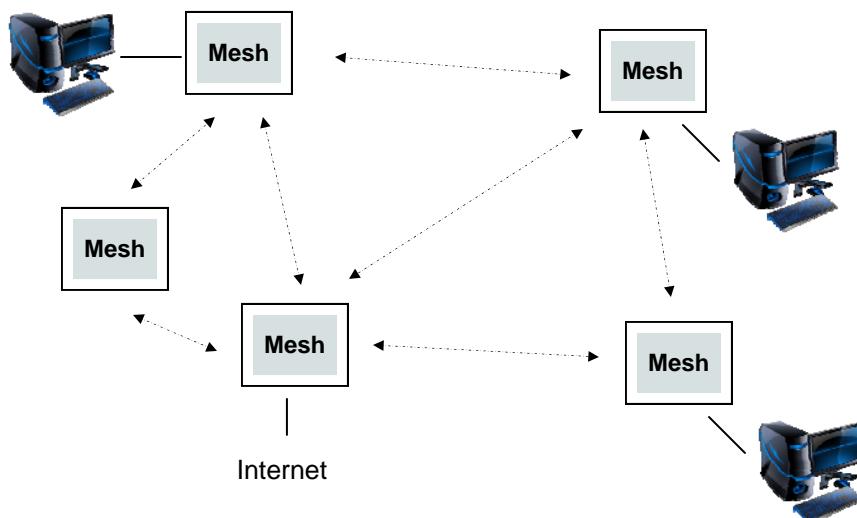
### 5.4 Access Point with Repeater



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



### 5.4 Mesh



## 6.0 Configuration

### 6.0 Web User Interface

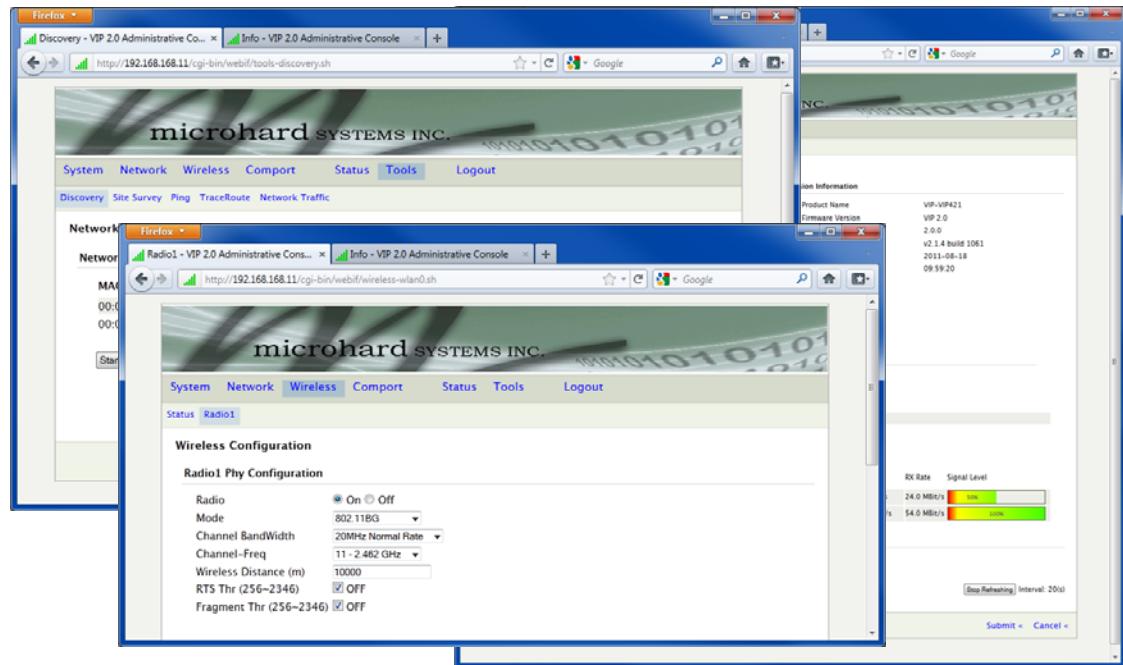


Image 6-1: WebUI

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

- configure a static IP Address on your PC to 192.168.168.10 (or any address on the 192.168.168.X subnet other than 192.168.168.1)
- connect VIP Series ETHERNET port to PC NIC card using an Ethernet **crossover** cable
- apply power to the VIP Series and wait approximately 60 seconds for the system to load
- open a web browser and enter the factory default IP address of the unit: 192.168.168.1
- logon window appears; log on using default Username: **admin** Password: **admin**
- use the web browser based user interface to configure the VIP as required.
- refer to [\*\*Section 2.0: Quick Start\*\*](#) for step by step instructions.

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

## 6.0 Configuration

### 6.0.1 Logon Window

Upon successfully accessing the VIP Series using a Web Browser, the Logon window will appear.



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



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



Image 6-2: Logon Window

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

The default password is: **admin**

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

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

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



Image 6-3: Logon Window : Password Entry

## 6.0 Configuration

### 6.1 System

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

- Info - Status summary of entire radio including network settings, version information, and radio connection status.
- Settings - Host Name, Default System Mode (Bridge or Router), System Time/Date, HTTP Port for the WebUI,
- Access Control - Change passwords, create new users
- Maintenance - Version information, firmware Upgrades, reset to defaults, configuration backup and restore.

#### 6.1.1 System > Info

The System Info screen is displayed immediately after initial login, showing a summary and status of all the functions of the VIP Series in a single display. This information includes LAN & WAN network information, version info and radio status as seen below.

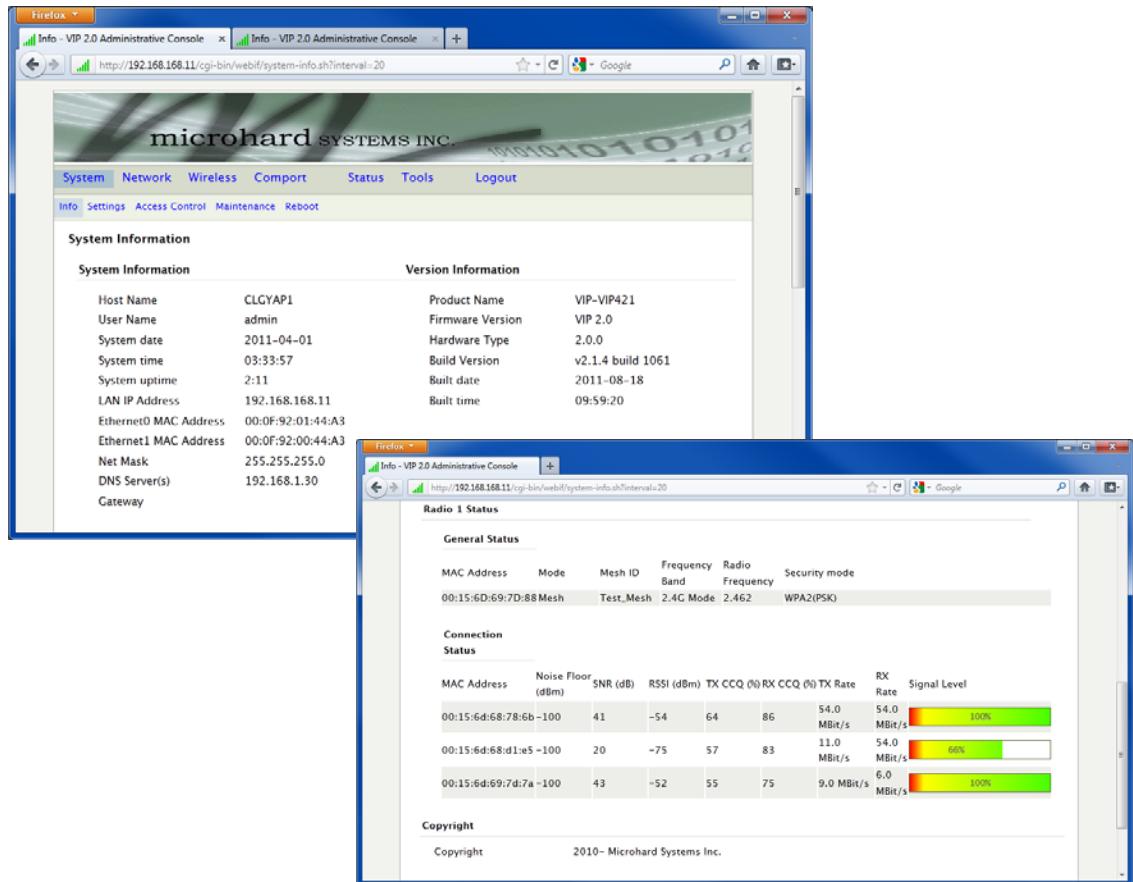


Image 6-4: System Info Window

## 6.0 Configuration

### 6.1.2 System > Settings

#### System Settings

Options available in the System Settings menu allow for the configuration of the Host Name and Default System Mode.

The screenshot shows the 'System Settings' page of the microhard VIP2.0 Series web interface. At the top, there's a navigation bar with links for System, Network, Wireless, Comport, Status, Tools, Logout, Info, Settings, Access Control, Maintenance, and Reboot. The 'Settings' link is currently selected. Below the navigation, the title 'System Settings' is displayed. Under 'System Settings', there are two main sections: 'System Settings' and 'Time Settings'. In the 'System Settings' section, the 'Host Name' is set to 'CLGYAP1' and the 'Default System Mode' is set to 'Bridge'. In the 'Time Settings' section, the current date is listed as '2011.04.01' and the current time is '21:38:13'. Below these settings, there's a 'Web Configurator Settings' section with an 'HTTP Port' field set to '80'.

Image 6-5: System Settings > System Settings

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



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

The Host Name 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. It has no bearing on the unit's operation.

Determines whether the VIP unit will operate as 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.

#### Host Name

##### Values (characters)

VIPnnnn

up to 30 characters

#### Default System Mode

##### Values (selection)

Bridge  
Router

## 6.0 Configuration



Network Time Protocol (NTP) can be used to synchronize the time and date of computer systems with a centralized, referenced server. This can help ensure all systems on a network have the same time and date.

### Time Settings

The VIP can be set to use a local time source, thus keeping time on its own, or it can be configured to synchronize the date and time via a NTP Server. The options and menus available will change depending on the current setting of the Date and Time Setting Mode, as seen below.

|   |   |
|---|---|
| <b>Time Settings : Current Date(yyyy.mm.dd) 2011.04.01 Time(hh:mm:ss): 21:38:13</b> |   |
| Date and Time Setting Mode  | <input type="button" value="Use Local Time Source"/>                  |
| Date (yyyy.mm.dd)   | 2011.04.01  |
| Time (hh:mm:ss)   | 21:38:12  |
| <b>Time Settings : Current Date(yyyy.mm.dd) 2011.04.01 Time(hh:mm:ss): 05:16:37</b> |   |
| Date and Time Setting Mode  | <input type="button" value="Synchronize Date And Time Over Network"/> |
| Timezone  | <input type="button" value="Mountain Time"/>                          |
| POSIX TZ String   | MST7MDT,M3.2.0,M11.1.0  |
| NTP Server  | pool.ntp.org  |
| NTP Server Port   | 123   |
| <a href="#">Remove NTP Server</a><br><a href="#">Add NTP Server</a>                 |   |

Image 6-6: System Settings > Time Settings

### Date and Time Setting Mode

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

#### Values (selection)

**Use Local Time Source**  
Synchronize Date And Time Over Network

### Date

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

#### Values (yyyy-mm-dd)

**2011.04.01** (varies)

### Time

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 (hh:mm:ss)

**11:27:28** (varies)

## 6.0 Configuration

| Timezone  |                               |
|---|-------------------------------|
| If connecting to a NTP time server, specify the timezone from the dropdown list.          | <b>Values (selection)</b>     |
|   | User Defined (or out of date) |
| POSIX TZ String   |                               |
| This displays the POSIX TZ String used by the unit as determined by the timezone setting. | <b>Values (read only)</b>     |
|   | (varies)                      |
| NTP Server  |                               |
| Enter the IP Address or domain name of the desired NTP time server.                       | <b>Values (address)</b>       |
|   | pool.ntp.org                  |
| NTP Port  |                               |
| Enter the IP Address or domain name of the desired NTP time server.                       | <b>Values (port#)</b>         |
|   | 123                           |

### Web Configurator Settings

The last section of the System Setting menu allows the configuration of the HTTP Port used for the web server of the WEBUI.

| Web Configurator Settings                   |                                 |
|---|---------------------------------|
| HTTP Port                                   | <input type="text" value="80"/> |
| <a href="#">Submit</a> << <a href="#">C</a> |                                 |

Image 6-7: System Settings > Web Configurator Settings

| HTTP Port   |                       |
|---|-----------------------|
| The default web server port for the web based configuration tools used in the VIP is port 80. Change as required, but keep in mind that if a non standard port is used, it must be specified in a internet browser to access the unit. (example: http://192.168.168.1:8080) | <b>Values (port#)</b> |
| 80  |                       |

## 6.0 Configuration

### 6.1.3 System > Access Control

#### Password Change

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

The screenshot shows the 'Access Control' interface with the 'Password Change' tab selected. It includes fields for 'User Name : admin', 'New Password (min 5 characters)', 'Confirm Password', and a 'Change Passwd' button. Below this, the 'Users' section indicates 'No users defined.' A note at the bottom states '( Note: Changes will not take effect until the system is rebooted )'. There is also a 'Add User' form with fields for 'Username', 'Password (min 5 characters)', 'Confirm Password', and a 'Add User' button.

*Image 6-8: Access Control > Password Change*

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

#### New Password

##### Values (characters)

admin

min 5 characters

#### Confirm Password

##### Values (characters)

admin

min 5 characters

## 6.0 Configuration

### 6.1.3 System > Access Control

#### Users

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

| Users  |                                   | Network         |            |
|--|-----------------------------------|-----------------|------------|
| Test1  | <a href="#">Remove user Test1</a> | Status          | Disabled ▾ |
| <b>Add User:</b> ( Note: Changes will not take effect until the system is rebooted ) |                                   | Networks        | Disabled ▾ |
| Username   | <input type="text"/>              | DHCP            | Disabled ▾ |
| Password (min 5 characters)  | <input type="password"/>          | SNMP            | Disabled ▾ |
| Confirm Password   | <input type="password"/>          | sdpServer       | Disabled ▾ |
| <input type="button" value="Add User"/>  |                                   | <b>Status</b>   |            |
|  |                                   | DHCP Clients    | Disabled ▾ |
|  |                                   | Mesh            | Disabled ▾ |
| <b>ACL User: Test1</b>   |                                   | <b>System</b>   |            |
| <b>Comport</b>   |                                   | Info            | Disabled ▾ |
| Status   | Disabled ▾                        | Settings        | Disabled ▾ |
| Com1   | Disabled ▾                        | Access Control  | Disabled ▾ |
| <b>Logout</b>  |                                   | Maintenance     | Disabled ▾ |
| Logout   | Disabled ▾                        | Reboot          | Disabled ▾ |
|  |                                   | <b>Tools</b>    |            |
|  |                                   | Discovery       | Disabled ▾ |
|  |                                   | Site Survey     | Disabled ▾ |
|  |                                   | Ping            | Disabled ▾ |
|  |                                   | TraceRoute      | Disabled ▾ |
|  |                                   | Network Traffic | Disabled ▾ |
|  |                                   | <b>Wireless</b> |            |
|  |                                   | Status          | Disabled ▾ |
|  |                                   | Radio1          | Disabled ▾ |

Image 6-9: Access Control > Users

| Username  | Values (characters)                                   |
|---|---|
| Enter the desired username. Minimum of 5 character and maximum of 32 character. Changes will not take effect until the system has been restarted. | (no default)<br>Min 5 characters<br>Max 32 characters |
| Password / Confirm Password   | Values (characters)                                   |
| Passwords must be a minimum of 5 characters. The Password must be re-entered exactly in the Confirm Password box as well.                         | (no default)<br>min 5 characters                      |

## 6.0 Configuration

### 6.1.4 System > Maintenance

#### Version Information

Detailed version information can be found on this display. The Product Name, Firmware Version, Hardware Type, Build Version, Build Date and Build Time can all be seen here, and may be requested from Microhard Systems to provide technical support.



*Image 6-10: Maintenance > Version Information / Firmware Upgrade*

#### Firmware Upgrade

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

|                             |                          |
|-----------------------------|--------------------------|
| Erase Current Configuration | <input type="checkbox"/> |
| Values (check box)          | unchecked                |
| Firmware Image              | <input type="file"/>     |
| Values (file)               | (no default)             |

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

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

## 6.0 Configuration

### 6.1.4 System > Maintenance

#### Reset to Default

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

|  |   |   |
|--|---|---|
| <b>Reset to Default</b>                |   |   |
| Reset to Default Configuration         | <input type="button" value="Reset to Default"/> |   |
| <b>Backup Configuration</b>            |   |   |
| Name this configuration                | VIP421  | <input type="button" value="Backup Configuration"/> |
| <b>Restore Configuration</b>           |   |   |
| Restore Configuration file             | <input type="button" value="Browse..."/>        | <input type="button" value="Check Restore File"/>   |
| <b>Restore Configuration</b>           |   |   |
| The configuration looks good!          |   |   |
| Config file Name                       | AP1CONFIG                                       |   |
| Generated                              | Fri Apr 1 02:20:06 UTC 2011                     |   |
| Vendor                                 | 2010- Microhard Systems Inc.                    |   |
| Product                                | VIP-VIP421                                      |   |
| Hardware Type                          | 2.0.0   |   |
| <input type="button" value="Restore"/> |   |   |

Image 6-11: Maintenance > Reset to Default / Backup & Restore Configuration

#### Backup & Restore Configuration

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

#### Name this Configuration / Backup Configuration

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

#### Restore Configuration file / Check Restore File / Restore

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

## 6.0 Configuration

### 6.1.5 System > Reboot

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

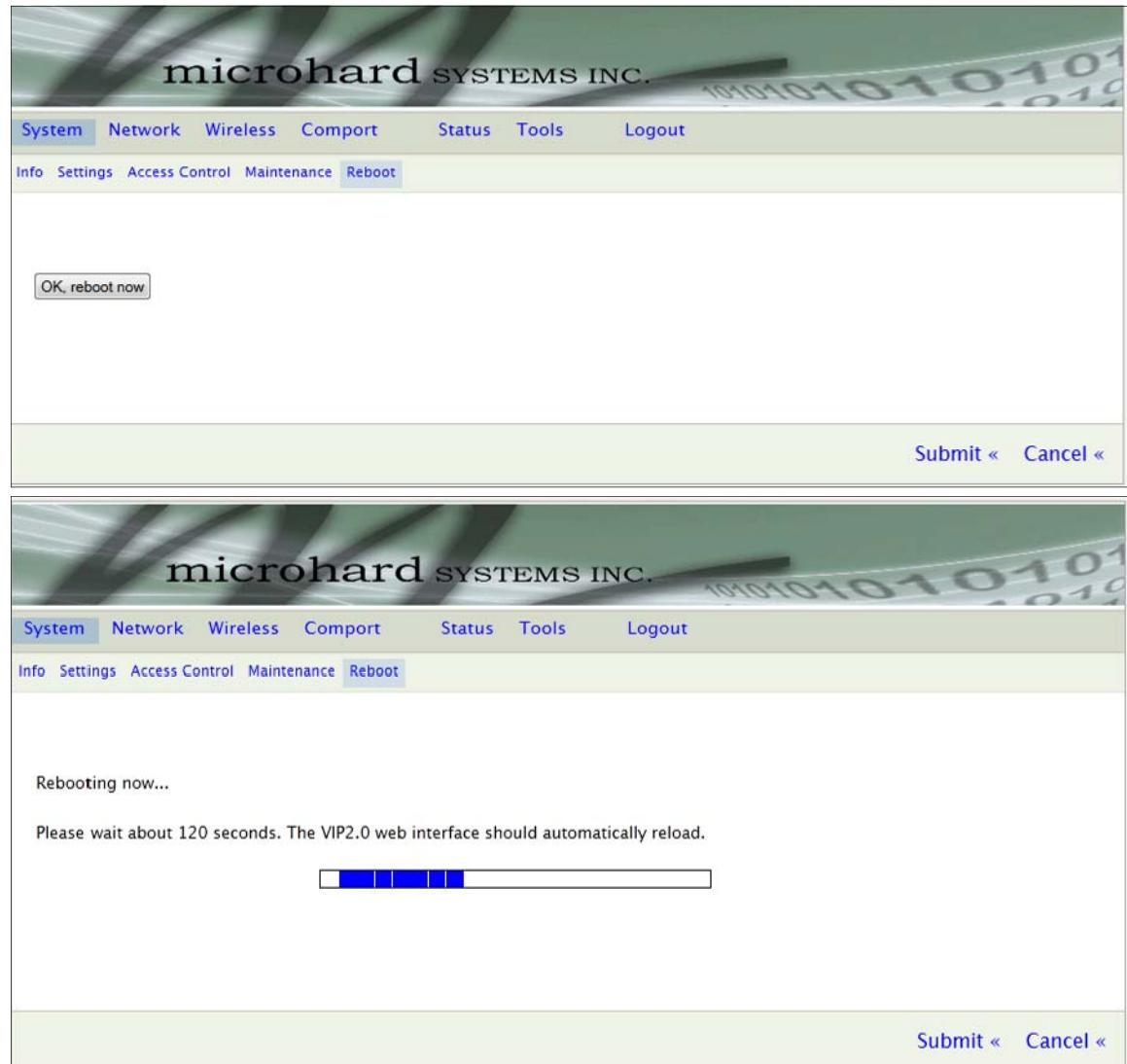


Image 6-12: System > Reboot

## 6.0 Configuration

### 6.2 Network

#### 6.2.1 Network > Status

The Network Status display gives a overview of the currently configured network interfaces including the Connection Type (Static/DHCP), IP Address, Net Mask, Gateways, and DNS Servers. The WAN interface will only be shown if the Default System Mode of the VIP is configured as a **Router** in the System > Settings tab. In **Bridge** mode, only the LAN interface will be shown.

The screenshot shows a web-based configuration interface for a microhard VIP2.0 Series device. The top navigation bar includes links for System, Network (which is selected), Wireless, Comport, Status, Tools, and Logout. Below the navigation is a secondary menu with links for Status, Networks, DHCP, SNMP, and sdpServer. The main content area is titled "Network Status" and contains four sections: "lan", "wan", "Default Gateway", and "DNS".

**lan**

|                 |                   |
|-----------------|-------------------|
| Connection Type | static            |
| IP Address      | 192.168.168.11    |
| Net Mask        | 255.255.255.0     |
| MAC Address     | 00:0F:92:00:44:A3 |

**wan**

|                 |                   |
|-----------------|-------------------|
| Connection Type | static            |
| IP Address      | 192.168.1.200     |
| Net Mask        | 255.255.255.0     |
| MAC Address     | 00:0F:92:01:44:A3 |

**Default Gateway**

|         |             |
|---------|-------------|
| Gateway | 192.168.1.1 |
|---------|-------------|

**DNS**

|               |              |
|---------------|--------------|
| DNS Server(s) | 192.168.1.30 |
|---------------|--------------|

Interval: 20 (in seconds)

Submit « Cancel «

Image 6-13: Network > Network Status

## 6.0 Configuration

### 6.2.2 Network > Networks

#### Network Configuration

The Networks menu is where the local Ethernet interfaces can be configured. As mentioned in the Network Status menu, the WAN options will only be presented if the VIP is configured as a **Router**. If configured as a **Bridge** only the LAN interface can be configured.

The screenshot shows the 'Network Configuration' page of the microhard VIP2.0 Series web interface. The top navigation bar includes links for System, Network (which is selected), Wireless, Comport, Status, Tools, and Logout. Below this is a secondary navigation bar with links for Status, Networks (selected), DHCP, SNMP, and sdpServer. The main content area is titled 'Network Configuration'.

**Ian Configuration:**

|                 |                |
|-----------------|----------------|
| Connection Type | Static IP      |
| IP Address      | 192.168.168.11 |
| Netmask         | 255.255.255.0  |
| Default Gateway | [empty]        |

**Ian DNS Servers:** A text input field with an 'Add' button.

**wan Configuration:**

|                 |               |
|-----------------|---------------|
| Connection Type | Static IP     |
| IP Address      | 192.168.1.200 |
| Netmask         | 255.255.255.0 |
| Default Gateway | 192.168.1.1   |

**wan DNS Servers:** A list containing '192.168.1.30' with a 'Remove' link, and an 'Add' button.

At the bottom right are 'Submit' and 'Cancel' buttons.

Image 6-14: Network > Network Configuration

## 6.0 Configuration



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

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

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

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



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



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.

### LAN Configuration

The LAN submenu, along with the Wireless Configuration settings, are the minimum required when implementing any VIP Series network. It must be defined if the unit is to be either:

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

|  |   |          |         |           |       |        |
|--|---|----------|---------|-----------|-------|--------|
| System   | Network   | Wireless | Comport | Status    | Tools | Logout |
| Status   | Networks  | DHCP     | SNMP    | sdpServer |       |        |
| <b>Network Configuration</b>   |   |          |         |           |       |        |
| <b>Ian Configuration</b>   |   |          |         |           |       |        |
| Connection Type  | <input style="border: 1px solid black; padding: 2px; margin-right: 10px;" type="button" value="Static IP"/> <input type="text" value="192.168.168.11"/> |          |         |           |       |        |
| IP Address   | <input type="text" value="192.168.168.11"/>   |          |         |           |       |        |
| Netmask  | <input type="text" value="255.255.255.0"/>  |          |         |           |       |        |
| Default Gateway  | <input type="text"/>  |          |         |           |       |        |
| <b>Ian DNS Servers</b>   |   |          |         |           |       |        |
| <input type="text"/> <input style="border: 1px solid black; padding: 2px;" type="button" value="Add"/> |   |          |         |           |       |        |

Image 6-15: Network Configuration > LAN Configuration

#### Connection Type

##### Values (selection)

DHCP  
Static

#### IP Address

##### Values (IP Address)

192.168.168.1

#### Netmask

##### Values (IP Address)

255.255.255.0

## 6.0 Configuration



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

In typical networks, a router acts as a gateway.



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](http://www.microhardcorp.com) (for example) into the URL line of a web browser, the website 'could not be found'.

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 Connection Type (see previous page) is selected to be DHCP, the DHCP server will populate this field with the appropriate gateway address.

In a very small network, 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 it does not know where to send, send it to the gateway. If necessary - and applicable - the gateway can forward the packet onwards to another network.

### Default Gateway

#### Values (IP Address)

(no default)

### LAN DNS Servers

#### Values (IP Address)

(no default)

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

## WAN Configuration

If the VIP Series is configured as a Router, the options to configure the WAN network information will be displayed. In Router mode the VIP WAN port is connected to a different network or subnet than the LAN port. The configuration of the WAN interface is identical to the LAN interface, so refer back to the previous section for information about the Connection Type, IP Address, Netmask, Default Gateway and WAN DNS Servers.

### wan Configuration

|                 |  |
|-----------------|--|
| Connection Type | Static IP                                  |
| IP Address      | <input type="text" value="192.168.1.200"/> |
| Netmask         | <input type="text" value="255.255.255.0"/> |
| Default Gateway | <input type="text" value="192.168.1.1"/>   |

### wan DNS Servers

192.168.1.30 [Remove](#)

[Add](#)

Image 6-16: Network Configuration > WAN Configuration

## 6.0 Configuration



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

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

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

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



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.)

### 6.2.3 Network > DHCP

#### DHCP Configuration

A VIP Series unit may be configured to provide dynamic host control protocol (DHCP) service to all attached (either wired or wireless-connected) devices.

| System                    |   | Network | Wireless        | Comport | Status | Tools     | Logout |
|---------------------------|---|---------|-----------------|---------|--------|-----------|--------|
|                           |   | Status  | Networks        | DHCP    | SNMP   | sdpServer |        |
| <b>DHCP Configuration</b> |   |         |                 |         |        |           |        |
| <b>Ian DHCP</b>           |   |         |                 |         |        |           |        |
| DHCP                      | <input checked="" type="radio"/> On <input type="radio"/> Off |         |                 |         |        |           |        |
| Start                     | 192.168.168.100   |         |                 |         |        |           |        |
| End                       | 192.168.168.250   |         |                 |         |        |           |        |
| Lease Time (in minutes)   | 720   |         |                 |         |        |           |        |
| <b>Active DHCP Leases</b> |   |         |                 |         |        |           |        |
| MAC Address               | IP Address  | Name    | Expires in      |         |        |           |        |
| bc:ae:c5:9d:58:94         | 192.158.168.236   | Joh-PC  | 12h 0sec        |         |        |           |        |
| 00:0f:92:00:44:aa         | 192.158.168.157   | +       | 11h 59min 50sec |         |        |           |        |

Image 6-17: Network > DHCP Configuration

#### DHCP

The option is used to enable or disable the DHCP service for devices connected to the LAN Port and devices connected through a Wireless connection. This includes VIP connected as clients and other wireless devices such as 802.11 connections.

#### Values (selection)

On / Off

#### Start / End IP Address Range

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

#### Values (IP Address)

(varies)

#### Lease Time

#### Values (minutes)

(minutes)

The DHCP lease time is the amount of time before a new request for a network address must be made to the DHCP Server.

#### Active DHCP Leases

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

## 6.0 Configuration

### 6.2.4 Network > SNMP

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:



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.

- 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 VIP 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 an object to a specified value, send a value in response to a received command, and send a value in response to an event (trap).

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

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

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

## 6.0 Configuration

### SNMP Settings

| System                       |   | Network | Wireless    | Comport   | Status | Tools | Logout |
|------------------------------|---|---------|-------------|-----------|--------|-------|--------|
| Status                       | Networks  | DHCP    | <b>SNMP</b> | sdpServer |        |       |        |
| <b>SNMP Settings</b>         |   |         |             |           |        |       |        |
| <b>SNMP Settings</b>         |   |         |             |           |        |       |        |
| SNMP Operation Mode          | <input type="radio"/> Disable <input checked="" type="radio"/> V1&V2c&V3    |         |             |           |        |       |        |
| Read Only Community Name     | <input type="text"/>  |         |             |           |        |       |        |
| Read Write Community Name    | <input type="text"/>  |         |             |           |        |       |        |
| SNMP V3 User Name            | <input type="text"/>  |         |             |           |        |       |        |
| V3 User Read Write Limit     | <input type="radio"/> Read Only <input checked="" type="radio"/> Read Write |         |             |           |        |       |        |
| V3 User Authentication Level | NoAuthNoPriv <select> </select>   |         |             |           |        |       |        |
| V3 Authentication Password   | <input type="text"/>  |         |             |           |        |       |        |
| V3 Privacy Password          | <input type="text"/>  |         |             |           |        |       |        |
| SNMP Trap Version            | V1 Traps <select> </select>   |         |             |           |        |       |        |
| Auth Failure Traps           | <input type="radio"/> Disable <input checked="" type="radio"/> Enable       |         |             |           |        |       |        |
| Trap Community Name          | <input type="text"/>  |         |             |           |        |       |        |
| Trap Manage Host IP          | <input type="text"/>  |         |             |           |        |       |        |

Image 6-18: Network &gt; SNMP

#### SNMP Operation Mode

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

#### Values (selection)

Disable / V1&V2c&V3

#### Read Only Community Name

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

#### Values (string)

public

#### Read Only Community Name

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

#### Values (string)

private

#### SNMP V3 User Name

Defines the user name for SNMPv3.

#### Values (string)

V3user

## 6.0 Configuration

| <b>V3 User Read Write Limit</b>   |   |
|---|---|
| Defines accessibility of SNMPv3; If Read Only is selected, the SNMPv3 user may only read information; if Read Write is selected, the SNMPv3 user may read and write (set) variables.      | <b>Values (selection)</b><br><br>Read Only / Read Write   |
| <b>V3 User Authentication Level</b>   |   |
| Defines SNMPv3 user's authentication level:<br><br>NoAuthNoPriv: No authentication, no encryption.<br>AuthNoPriv: Authentication, no encryption.<br>AuthPriv: Authentication, encryption. | <b>Values (selection)</b><br><br>NoAuthNoPriv<br>AuthNoPriv<br>AuthPriv                             |
| <b>V3 User Authentication Password</b>  |   |
| SNMPv3 user's authentication password. Only valid when V3 User Authentication Level set to AuthNoPriv or AuthPriv.  | <b>Values (string)</b><br><br>00000000  |
| <b>V3 User Privacy Password</b>   |   |
| SNMPv3 user's encryption password. Only valid when V3 User Authentication Level set to AuthPriv (see above).  | <b>Values (string)</b><br><br>00000000  |
| <b>SNMP Trap Version</b>  |   |
| Select which version of trap will be sent should a failure or alarm condition occur.  | <b>Values (string)</b><br><br>V1 Traps      V2 Traps<br>V3 Traps      V1&V2 Traps<br>V1&V2&V3 Traps |
| <b>Auth Failure Traps</b>   |   |
| If enabled, an authentication failure trap will be generated upon authentication failure.   | <b>Values (selection)</b><br><br>Disable / Enable   |
| <b>Trap Community Name</b>  |   |
| The community name which may receive traps.   | <b>Values (string)</b><br><br>TrapUser  |
| <b>Trap Manage Host IP</b>  |   |
| Defines a host IP address where traps will be sent to (e.g. SNMP management system PC IP address).  | <b>Values (IP Address)</b><br><br>0.0.0.0   |

## 6.0 Configuration

### 6.2.5 Network > sdpServer

#### sdpServer Settings

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



Image 6-19: Network > sdpServer Settings

#### Discovery Service Status

Use this option to disable or enable the discovery service.

#### Values (selection)

Disable / Discoverable /  
Changable

#### Server Port Settings

Specify the port running the discovery service on the VIP series unit.

#### Values (Port #)

20097

## 6.0 Configuration

### 6.3 Wireless

#### 6.3.1 Wireless > Status

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

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

**Traffic Status** shows statistics about the transmitted and received data.

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

The screenshot displays the Microhard VIP2.0 Series configuration interface. The top navigation bar includes links for System, Network, Wireless (which is selected and highlighted in blue), Comport, Status, Tools, and Logout. Below the navigation is a secondary header with Status and Radio1 tabs, where Status is selected.

**Wireless Interfaces**

**Radio 1 Status**

**General Status**

| MAC Address       | Mode         | SSID     | Frequency Band | Radio Frequency | Security mode |
|-------------------|--------------|----------|----------------|-----------------|---------------|
| 00:15:6D:69:7D:88 | Access Point | TESTSSID | 2.4G Mode      | 2.462           | WPA2(PSK)     |

**Traffic Status**

| Receive bytes | Receive packets | Transmit bytes | Transmit packets |
|---------------|-----------------|----------------|------------------|
| 1.09188GB     | 879973          | 77.4855MB      | 699144           |

**Connection Status**

| MAC Address           | Noise Floor (dBm) | SNR (dB) | RSSI (dBm) | TX CCQ (%) | RX CCQ (%)  | TX Rate     | RX Rate | Signal Level |
|-----------------------|-------------------|----------|------------|------------|-------------|-------------|---------|--------------|
| 00:15:6d:69:7d:7a-100 | 41                | -54      | 93         | 96         | 54.0 MBit/s | 54.0 MBit/s |         |              |

Stop Refreshing Interval: 20(s)

Image 6-20: Network > sdPServer Settings

## 6.0 Configuration

### 6.3.2 Wireless > Radio1

#### Radio1 Phy Configuration

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

The screenshot shows a web-based configuration interface for a Microhard VIP2.0 Series device. The top navigation bar includes links for System, Network, Wireless (which is highlighted in blue), Comport, Status, Tools, and Logout. Below the navigation is a secondary level of navigation with Status and Radio1 selected. The main content area is titled "Wireless Configuration" and "Radio1 Phy Configuration". Under this, there are several configuration options with dropdown menus and input fields:

- Radio: On (radio button selected)
- Mode: 802.11BG
- Channel BandWidth: 20MHz Normal Rate
- Channel-Freq: 11 - 2.462 GHz
- Wireless Distance (m): 10000
- RTS Thr (256~2346): OFF (checkbox checked)
- Fragment Thr (256~2346): OFF (checkbox checked)

Image 6-21: Wireless > Radio Configuration

This option is used to turn the radio module on or off. If turned off Wireless connections can not be made. The default is On.

**Values (selection)**

On / Off

The 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) and 802.11g (up to 54 Mbps).

**Values (VIP2400)**

IEEE 802.11B ONLY  
IEEE 802.11BG

**Values (VIP4900)**

IEEE 802.11A

**Values (VIP5800)**

IEEE 802.11A

## 6.0 Configuration

| Channel BandWidth  |  |   |
|--|--|---|
| Values (selection)   |  |   |
| Channel-Freq   |  |   |
| <p>Normally the default Channel Bandwidth of 20 MHz is used. Lower channel bandwidth may provide longer distance and be less susceptible to noise but at the trade off of data rates. Higher channel bandwidth may provide greater data rates but will more susceptible to noise and produce shorter distance potentials.</p>  |  |   |
| Values (VIP2400)   | Values (VIP4900)   | Values (VIP5800)  |
| <b>Auto</b><br>Channel 01 : 2.412 GHz<br>Channel 02 : 2.417 GHz<br>Channel 03 : 2.422 GHz<br>Channel 04 : 2.427 GHz<br>Channel 05 : 2.432 GHz<br>Channel 06 : 2.437 GHz<br>Channel 07 : 2.442 GHz<br>Channel 08 : 2.447 GHz<br>Channel 09 : 2.452 GHz<br>Channel 10 : 2.457 GHz<br>Channel 11 : 2.462 GHz  | <b>Auto</b><br>Channel 05 : 4.9425 GHz<br>Channel 10 : 4.9450 GHz<br>Channel 15 : 4.9475 GHz<br>Channel 20 : 4.9500 GHz<br>Channel 25 : 4.9525 GHz<br>Channel 30 : 4.9550 GHz<br>Channel 35 : 4.9575 GHz<br>Channel 40 : 4.9600 GHz<br>Channel 45 : 4.9625 GHz<br>Channel 50 : 4.9650 GHz<br>Channel 55 : 4.9675 GHz<br>Channel 60 : 4.9700 GHz<br>Channel 65 : 4.9725 GHz<br>Channel 70 : 4.9750 GHz<br>Channel 75 : 4.9775 GHz<br>Channel 80 : 4.9800 GHz<br>Channel 85 : 4.9825 GHz<br>Channel 90 : 4.9850 GHz<br>Channel 95 : 4.9875 GHz | <b>Auto</b><br>Channel 36: 5.18 GHz<br>Channel 40: 5.2 GHz<br>Channel 44: 5.22 GHz<br>Channel 48: 5.24 GHz<br>Channel 149 : 5.745 GHz<br>Channel 153 : 5.765 GHz<br>Channel 157 : 5.785 GHz<br>Channel 161 : 5.805 GHz<br>Channel 165 : 5.825 GHz |
| Wireless Distance  |  |   |
| The Wireless Distance parameter allows a user to set the expected distance the wireless signal needs to travel. The default is 10km, so the VIP series will assume that the signal may need to travel up to 10km so it sets various internal timeouts to account for this travel time. Longer distances will require a higher setting, and shorter distances may perform better if the setting is reduced. |  |   |
| Values (meters)  |  |   |
| 10000  |  |   |

## 6.0 Configuration

| RTS Thr (256 ~ 2346)   |
|--|
| Once the RTS Threshold defined packet size is reached, the system will invoke RTS/CTS flow control. A large RTS Threshold will improve bandwidth, while a smaller RTS Threshold will help the system recover from interference or collisions caused by obstructions. |
| Values (selection)   |

On / OFF

| Fragment Thr (256 ~ 2346)   |
|---|
| The Fragmentation Threshold allows the system to change the maximum RF packet size. Increasing the RF packet size reduces the need to break packets into smaller fragments. Increasing the fragmentation threshold slightly may improve performance if a high packet error rate is experienced. |
| Values (selection)  |

On / OFF

### Radio1 Virtual Interface

The bottom section of the Wireless Configuration provides for the configuration of the Mode of the Wireless interface, the TX power, Wireless Network information, and Wireless Encryption.

| Radio1 Virtual Interface |   |
|--------------------------|---|
| Network                  | lan <input type="button" value="▼"/>                          |
| Mode                     | Access Point <input type="button" value="▼"/>                 |
| TX Rate                  | Auto <input type="button" value="▼"/>                         |
| Tx Power                 | 17 dbm <input type="button" value="▼"/>                       |
| WDS                      | <input checked="" type="radio"/> On <input type="radio"/> Off |
| ESSID Broadcast          | <input checked="" type="radio"/> On <input type="radio"/> Off |
| SSID                     | TESTSSID <input type="text"/>                                 |
| Encryption Type          | WPA2 (PSK) <input type="button" value="▼"/>                   |
| WPA PSK                  | •••••••••• <input type="text"/>                               |
| Show password            | <input type="checkbox"/>                                      |
| MAC Filter               | Disabled <input type="button" value="▼"/>                     |

Image 6-22: Wireless > Radio Configuration

| Network   |
|---|
| Choose between LAN or WAN for the Wireless interface. If the unit is configured as a Bridge, only the LAN option will appear in the drop down list. |
| Values (selection)  |

LAN  
WAN

## 6.0 Configuration

| 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.

### Values (selection)

Access Point  
Client  
Repeater  
Mesh Point

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

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

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

| TX 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 (VIP4900/5800) |
|----------------------|-----------------------|
| <b>Auto</b>          | <b>Auto</b>           |
| 1 Mbps (802.11b,g)   | 6 Mbps                |
| 2 Mbps (802.11b,g)   | 9 Mbps                |
| 5.5 Mbps (802.11b,g) | 12 Mbps               |
| 11 Mbps (802.11b,g)  | 18 Mbps               |
| 6 Mbps (802.11g)     | 24 Mbps               |
| 9 Mbps (802.11g)     | 36 Mbps               |
| 12 Mbps (802.11g)    | 48 Mbps               |
| 18 Mbps (802.11g)    | 54 Mbps               |
| 24 Mbps (802.11g)    |                       |
| 36 Mbps (802.11g)    |                       |
| 48 Mbps (802.11g)    |                       |
| 54 Mbps (802.11g)    |                       |

## 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).**



**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.



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.

### 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 (selection)

|               |               |
|---------------|---------------|
| 6 dBm         | 18 dBm        |
| 7 dBm         | 19 dBm        |
| 8 dBm         | 20 dBm        |
| 9 dBm         | 21 dBm        |
| 10 dBm        | 22 dBm        |
| 11 dBm        | 23 dBm        |
| 12 dBm        | 24 dBm        |
| 13 dBm        | 25 dBm        |
| 14 dBm        | 26 dBm        |
| 15 dBm        | 27 dBm        |
| 16 dBm        | 28 dBm        |
| <b>17 dBm</b> | <b>29 dBm</b> |
|               | 30 dBm        |

### WDS

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

#### Values (selection)

On / Off

### ESSID Broadcast

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

#### Values (selection)

On / Off

### 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.

#### Values (string)

wlan0

### MESH ID

In Mesh Networks, this must be the same for all VIP units participating, similar to the SSID for other wireless networks.

#### Values (string)

(no default)

## 6.0 Configuration



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.

| Encryption Type  | Values (selection)  |
|--|---|
| Security options are dependent on the version type. This section describes all available options. Export versions may not have all optional available to meet regulatory requirements set government policies. | <b>Disabled</b><br>WEP<br>WPA (PSK)<br>WPA2 (PSK)<br>WPA+WPA2 (PSK) |
| <b>WEP:</b> 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:  |   |
|  |   |

Image 6-23: Encryption Type > WEP

- Key Generation  
4 complex WEP keys may be generated based on the supplied Passphrase

Procedure: Input a Key Phrase, select the type of Key to be generated using the Generate Key soft button.

Using the same Passphrase 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.

**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.

| Show Password  | Values (selection) |
|--|--------------------|
| Check this box to show the currently configured password for WPA/WPA2 encryption passphrase. | <b>unchecked</b>   |

## 6.0 Configuration

| MAC Filter         |  |
|--------------------|--|
| Values (selection) |  |
| Disabled           |  |
| Allow              |  |
| Deny               |  |

The MAC filter can be used to control which devices connect to the VIP Series based on their Wireless MAC addresses. If this option is set for Deny, any MAC addresses listed in the MAC list will not be allowed to connect to the VIP. If Allow is used, only devices listed in the MAC list can connect to the VIP.

|                      |                                     |
|----------------------|-------------------------------------|
| MAC Filter           | <input type="button" value="Deny"/> |
| <b>MAC List</b>      |                                     |
| FE:06:88:CD:23:F4    | <a href="#">Remove</a>              |
| <input type="text"/> | <input type="button" value="Add"/>  |

Image 6-24: Wireless Configuration > MAC List

## 6.0 Configuration

### 6.4 Comport

#### 6.4.1 Comport > Status

The Status window gives a summary of the COM1 Serial port on the VIP Series. The Status window shows if the com port has been enabled, how it is configured (Connect As), and the connection status.

The screenshot displays the 'Comport Status' page with the following details:

**Com1 Port Connection Status**

|                     |            |
|---------------------|------------|
| Com1 Port status    | Enable     |
| Com1 Connect As     | TCP Server |
| Com1 Connect Status | Active     |

**Com1 Port Received Packet Statistics**

|                   |     |
|-------------------|-----|
| Receive bytes     | 412 |
| Receive packets   | 352 |
| Receive errors    | 0   |
| Drop packets      | 0   |
| Receive fifo      | 0   |
| Receive frame     | 0   |
| Compressed        | 0   |
| Receive multicast | 0   |

**Com1 port Transmitted Packet Statistics**

|                   |     |
|-------------------|-----|
| Transmit bytes    | 211 |
| Transmit packets  | 157 |
| Transmit errors   | 0   |
| Drop packets      | 0   |
| Transmit fifo     | 0   |
| Collisions        | 0   |
| Transmit carrier  | 0   |
| Transmit compress | 0   |

Buttons at the bottom right: Stop Refreshing, Interval: 20 (in seconds), Submit, Cancel.

Image 6-25: Comport > Comport Status

## 6.0 Configuration

### 6.4 Comport

#### 6.4.2 Comport > COM1

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 disabled.

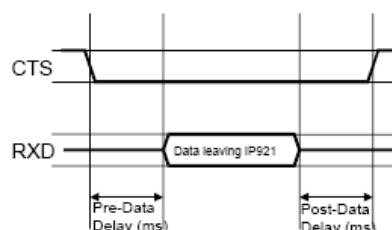
|                              |   |          |         |        |       |        |
|------------------------------|---|----------|---------|--------|-------|--------|
| System                       | Network   | Wireless | Comport | Status | Tools | Logout |
| Status Com1                  |   |          |         |        |       |        |
| <b>Comport Configuration</b> |   |          |         |        |       |        |
| <b>com1 Configuration</b>    |   |          |         |        |       |        |
| Com1 Port status             | <input type="radio"/> Disable <input checked="" type="radio"/> Enable                           |          |         |        |       |        |
| Channel Mode                 | RS232   |          |         |        |       |        |
| Data Baud Rate               | 9600  |          |         |        |       |        |
| Data Format                  | 8N1   |          |         |        |       |        |
| Flow Control                 | none  |          |         |        |       |        |
| Pre-Data Delay (ms)          | 100   |          |         |        |       |        |
| Post-Data Delay (ms)         | 100   |          |         |        |       |        |
| Data Mode                    | <input checked="" type="radio"/> Seamless <input type="radio"/> Transparent                     |          |         |        |       |        |
| Character Timeout            | 0   |          |         |        |       |        |
| Maximum Packet Size          | 1024  |          |         |        |       |        |
| Priority                     | <input checked="" type="radio"/> Normal <input type="radio"/> Medium <input type="radio"/> High |          |         |        |       |        |
| No-Connection Data           | <input checked="" type="radio"/> Disable <input type="radio"/> Enable                           |          |         |        |       |        |
| MODBUS TCP Status            | <input type="radio"/> Disable <input checked="" type="radio"/> Enable                           |          |         |        |       |        |
| MODBUS TCP Protection Status | <input checked="" type="radio"/> Disable <input type="radio"/> Enable                           |          |         |        |       |        |
| MODBUS TCP Protection Key    | 1234  |          |         |        |       |        |
| IP Protocol Config           | TCP Server  |          |         |        |       |        |
| <b>TCP Configuration</b>     |   |          |         |        |       |        |
| Local Listening port         | 20001   |          |         |        |       |        |
| Incoming Connection Timeout  | 300   |          |         |        |       |        |

Image 6-26: Comport > Com1 Configuration

## 6.0 Configuration

| Com1 Port Status   |                    |
|--|--------------------|
| Select operational status of the Com1 Serial Port. The port is disabled by default.  | Values (selection) |
| Disabled / Enable  |                    |
| 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 (selection) |
| RS232<br>RS485<br>RS422  |                    |
| Data Baud Rate   |                    |
| The serial baud rate is the rate at which the modem is to communicate with the attached local asynchronous device.<br>*COM2 data baud rate maximum is 115200bps.                       | Values (bps)       |
| 921600 <b>9600</b><br>460800      7200<br>230400      4800<br>115200      3600<br>57600      2400<br>38400      1200<br>28800      600<br>19200      300<br>14400                      |                    |
| Data Format  |                    |
| This setting determines the format of the data on the serial port. The default is 8 data bits, No parity, and 1 Stop bit.  | Values (selection) |
| 8N1      7N2<br>8N2      7E1<br>8E1      7O1<br>8O1      7E2<br>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 VIP Series uses the CTS signal to gate the output data on the serial port.



Values (selection)

None  
Hardware  
CTS Framing

Drawing 6A: CTS Output Data Framing

## 6.0 Configuration

|   |                            |
|---|----------------------------|
|   | <b>Pre-Data Delay</b>      |
| Refer to <b>Drawing 6A</b> on the preceding page.   | <b>Values (time (ms) )</b> |
|   | 100                        |
|   | <b>Post-Data Delay</b>     |
| Refer to <b>Drawing 6A</b> on the preceding page.   | <b>Values (time (ms) )</b> |
|   | 100                        |
|   | <b>Date Mode</b>           |
| This setting defines the serial output data framing. In Transparent mode (default), the received data will be output promptly from the VIP Series.  | <b>Values (selection)</b>  |
|   | Seamless / Transparent     |
| When set to Seamless, the serial port server will add a gap between data frames to comply with the MODBUS protocol for example. See 'Character Timeout' on the next page for related information.   | <b>Character Timeout</b>   |
| 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. | <b>Values (characters)</b> |
|   | 0                          |
| 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).   |                            |
|   | <b>Maximum Packet Size</b> |
| 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.   | <b>Values (bytes)</b>      |
|   | 1024                       |
|   | <b>Priority</b>            |
| This setting effects the quality of service associated with the data traffic on the COM port.   | <b>Values (selection)</b>  |
|   | Normal / Medium / High     |

## 6.0 Configuration

| No-Connection Data  | Values (selection)      |
|---|-------------------------|
| 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. | <b>Disable</b> / Enable |
| MODBUS TCP Status   | Values (selection)      |
| This option will enable or disable the MODBUS decoding and encoding features.   | <b>Disable</b> / Enable |
| MODBUS TCP Protection   | Values (selection)      |
| 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.  | <b>Disable</b> / Enable |
| MODBUS TCP Protection Key   | Values (string)         |
| MODBUS encryption key used for the MODBUS TCP Protection Status feature.  | 1234                    |

## 6.0 Configuration



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



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



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

Requires more bandwidth than UDP.

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

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

#### Values (selection)

|                                    |
|------------------------------------|
| TCP Client                         |
| TCP Server                         |
| TCP Client/Server                  |
| UDP Point-to-Point                 |
| UDP Point-to-Multipoint (P)        |
| <b>UDP Point-to-Multipoint(MP)</b> |
| UDP Multipoint-to-Multipoint       |
| SMTP Client                        |
| C12.22                             |

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

- **Remote Server Address**

IP address of a TCP server which is ready to accept serial port data through a TCP connection. For example, this server may reside on a LAN network server.

Default: **0.0.0.0**

- **Remote Server Port**

A TCP port which the remote server listens to, awaiting a session connection request from the TCP Client. Once the session is established, the serial port data is communicated from the Client to the Server.

Default: **20001**

- **Outgoing Connection Timeout**

This parameter determines when the IP Series will terminate the TCP connection if the connection is in an idle state (i.e. no data traffic on the serial port).

Default: **60** (seconds)

**TCP Server:** In this mode, the 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

### IP Protocol Config (Continued...)



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

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



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



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.

**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.

**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 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)**

## 6.0 Configuration

### IP Protocol Config (Continued...)



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

**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**

#### UDP Multipoint-to-Multipoint

- **Multicast IP Address**

A valid multicast address the unit will use to send multicast UDP packets upon receiving them at its serial port.

Default: **224.1.1.1**

- **Multicast Port**

UDP port that the packets are sent to. Multipoint stations should be configured to listen to this port in order to receive multicast packets.

Default: **20011**

- **Time to Live**

Time to live for the multicast packets.

Default: **1 (hop)**

- **Listening Multicast IP Address**

A valid multicast address the unit is to listen to receive multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.

Default: **224.1.1.1**

- **Listening Multicast Port**

UDP port that the unit will listen to for multicast UDP packets sent by another UDP Multipoint-to-Multipoint unit.

Default: **20011**

## 6.0 Configuration

### IP Protocol Config (Continued...)

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



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

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

## 6.0 Configuration

### 6.5 Status

#### 6.5.1 Status > DHCP Clients

##### DHCP Leases

The DHCP Leases menu displays any DHCP leases that have been assigned by the DHCP service. The MAC address, IP Address, Name and the amount of time remaining in the lease are displayed. If the unit has been reset, it may not list all leases until the DHCP client renew their leases.

The screenshot shows a web-based management interface for a microhard VIP2.0 Series device. The top navigation bar includes links for System, Network, Wireless, Comport, Status (which is highlighted), Tools, and Logout. Below the navigation is a secondary menu with links for DHCP Clients (which is also highlighted) and Mesh. The main content area is titled "DHCP Leases". A table header defines columns for MAC Address, IP Address, Name, and Expires in. Below the table, a note states: "DHCP Leases: DHCP leases are assigned to network clients that request an IP address from the DHCP server of the router. Clients that requested their IP lease before this router was last rebooted may not be listed until they request a renewal of their lease." Under the "Additional information" section, there is a table for the Address Resolution Protocol Cache (ARP). This table has columns for MAC Address, IP Address, HW Type, Flags, and Mask. One entry is shown: MAC Address 00:80:c8:3c:fb:fb, IP Address 192.168.168.254, HW Type ETHER, Flags C (completed), and Mask \*. At the bottom right of the content area are "Submit" and "Cancel" buttons.

Image 6-27: Status > DHCP Clients

##### Additional Information - ARP Cache

The current Address Resolution Protocol (ARP) Cache can be viewed here, showing the MAC address and IP Address of any attached devices. This will show any device or PC connected by a wireless link, or directly connected to the LAN or WAN port, using Static or DHCP addressing.

## 6.0 Configuration

### 6.5.2 Status > Mesh

#### Mesh Routing Table

In a Mesh network, the Mesh Routing Table will give a user information about the Next Hop Wireless MAC address and the exit interface for data. Mesh data paths are constantly changing, so this table only gives a picture of the routing paths at any given moment. It is most useful to determine if all devices in the Mesh network are participating in data exchange.

The screenshot shows a web-based management interface for a microhard VIP2.0 Series device. The top navigation bar includes links for System, Network, Wireless, Comport, Status (which is highlighted in blue), Tools, and Logout. Below the navigation is a secondary menu with DHCP Clients and Mesh selected. The main content area is titled "Mesh Routing Table" and displays a table of three entries:

| Destination       | Next Hop          | Interface |
|-------------------|-------------------|-----------|
| 00:15:6d:68:d1:e5 | 00:15:6d:68:d1:e5 | wlano     |
| 00:15:6d:69:7d:7a | 00:15:6d:69:7d:7a | wlano     |
| 00:15:6d:68:78:6b | 00:15:6d:68:78:6b | wlano     |

At the bottom right of the table area are "Submit" and "Cancel" buttons.

Image 6-28: Status > Mesh Routing Table

## 6.0 Configuration

### 6.6 Tools

#### 6.6.1 Tools > Discovery

##### Network Discovery

The Network discovery tool allows the VIP Series unit to send a broadcast to all VIP units on the same network. Other VIP units on the network will respond to the broadcast and report their MAC address, IP address (With a hyperlink to that units WebUI page), description, firmware version, operating mode, and the SSID (regardless of whether it was set to broadcast or not).

The discovery service can be a useful troubleshooting tool and can be used to quickly find and identify other VIP units on the network. It can be disabled from the Network > sdpServer menu.

The screenshot shows a web-based interface for a Microhard VIP2.0 Series device. The top navigation bar includes links for System, Network, Wireless, Comport, Status, Tools (which is selected and highlighted in blue), and Logout. Below the navigation is a sub-menu with links for Discovery, Site Survey, Ping, TraceRoute, and Network Traffic. The main content area is titled "Network Discovery". Under this title, there is a table with the following data:

| MAC Address       | IP Address                     | Description | Product Name | Firmware Ver | Mode | SSID      |
|-------------------|--------------------------------|-------------|--------------|--------------|------|-----------|
| 00:0F:92:00:44:AA | <a href="#">192.168.168.12</a> | CLGYCL1     | VIP          | v2.1.4-1061  | mesh | Test_Mesh |
| 00:0F:92:00:44:A3 | <a href="#">192.168.168.11</a> | CLGYAP1     | VIP          | v2.1.4-1061  | mesh | Test_Mesh |
| 00:0F:92:00:36:73 | <a href="#">192.168.168.13</a> | CLGRYNE13   | VIP          | v2.1.4-1062  | mesh | Test_Mesh |

At the bottom of the table area is a button labeled "Start discovery network again".

Image 6-27: Tools > Discovery

## 6.0 Configuration

### 6.6.2 Tools > Site Survey

#### Wireless Survey

The Wireless Survey feature will scan the available wireless channels for any other wireless networks in proximity to the VIP. The Survey will display the Channel number the other networks are operating on, the MAC address, Encryption Type, Frequency and general signal level and quality information. This can be useful for finding available networks, or troubleshooting connection and sensitivity problems. If there are other networks operating on the same frequency, or a channel close to the one chosen, it can then be decided to try to use another channel.

The screenshot shows the 'Site Survey' page of the microhard VIP2.0 Series web interface. The top navigation bar includes links for System, Network, Wireless, Comport, Status, Tools (which is selected), and Logout. Below the navigation is a sub-menu with Discovery, Site Survey (selected), Ping, TraceRoute, and Network Traffic. The main content area is titled 'Site Survey' and contains the message 'Please wait, the scan needs some time ...'. A note below states 'Note: Your WLAN traffic will be interrupted during this brief period.' with a 'Start the scan again' button. The section 'Radio1 Survey Results' displays a table of survey data:

| Channel | SSID      | MAC DDR           | Encryption   | Frequency | RSSI    | SNR    | Noise    | Signal Level                       |
|---------|-----------|-------------------|--------------|-----------|---------|--------|----------|------------------------------------|
| 3       | VIPnnnn   | 00:15:6D:68:CD:6D | off          | 2.422GHz  | -66 dBm | 29 dBm | -99 dBm  | <div style="width: 96%;">96%</div> |
| 4       | work2901  | 00:15:6D:68:3D:0C | WPA/WPA2/PSK | 2.427GHz  | -80 dBm | 15 dBm | -98 dBm  | <div style="width: 50%;">50%</div> |
| 11      | Test_Mesh | 00:15:6D:69:7D:7A | off          | 2.462GHz  | -88 dBm | 7 dBm  | -100 dBm | <div style="width: 23%;">23%</div> |

Image 6-28: Tools > Site Survey

## 6.0 Configuration

### 6.6.3 Tools > Ping

#### Network Tools Ping

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

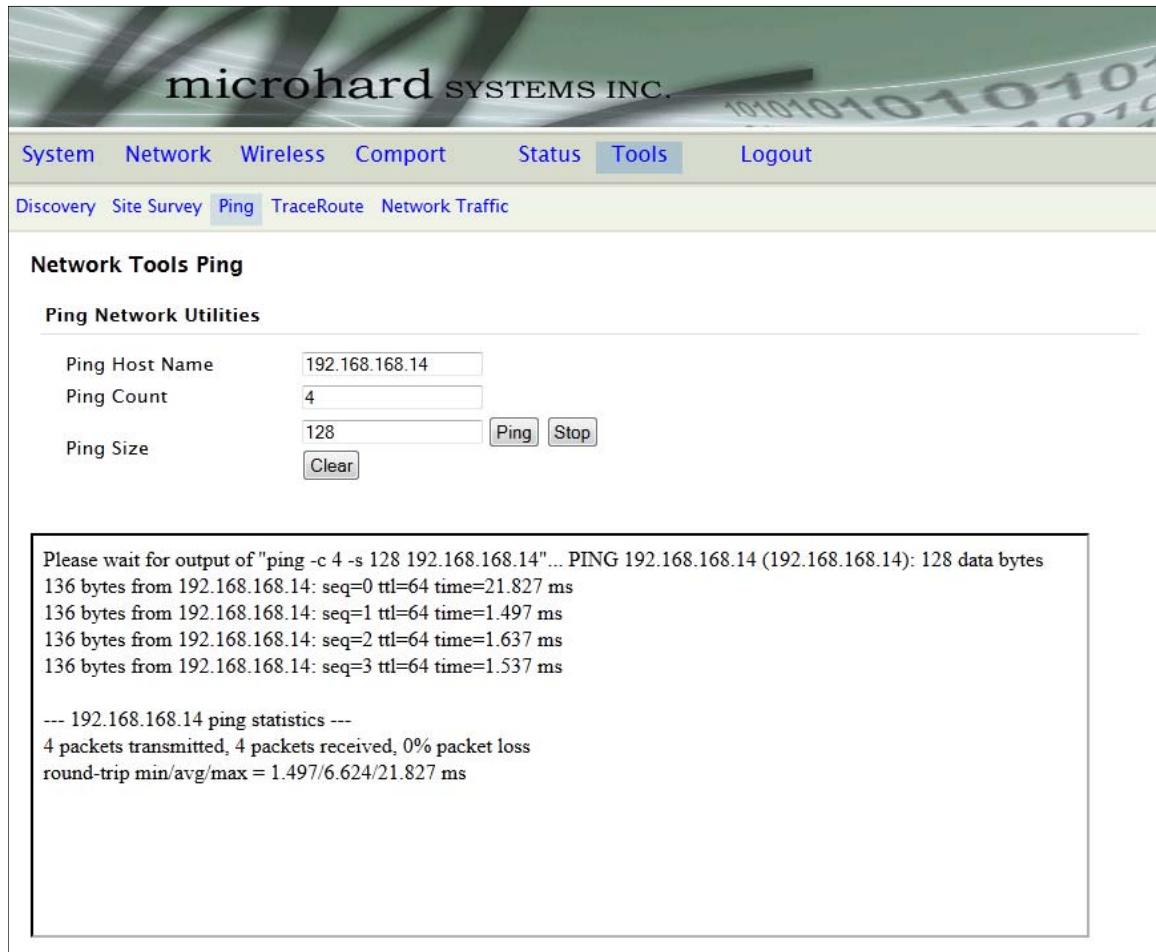


Image 6-29: Tools > Ping

## 6.0 Configuration

### 6.6.4 Tools > TraceRoute

#### Network TraceRoute

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

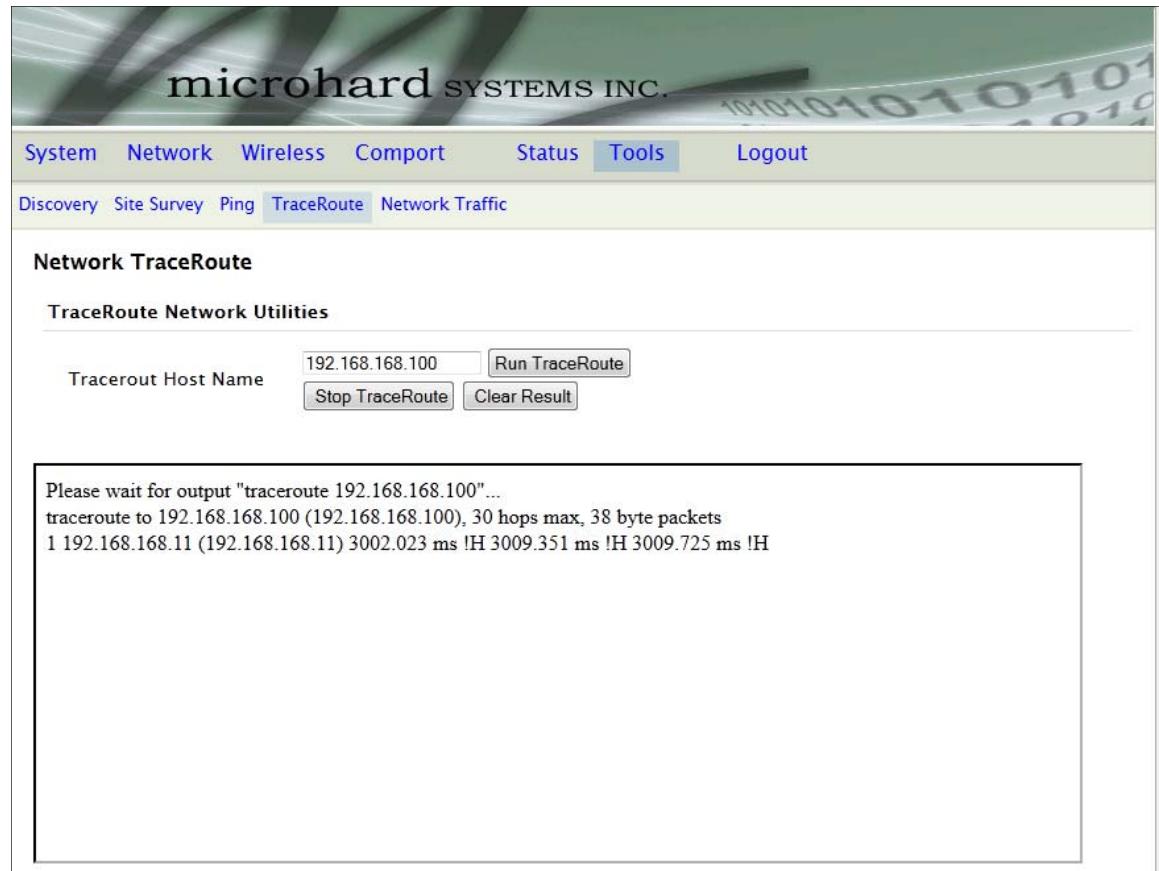


Image 6-30: Tools > TraceRoute

## 6.0 Configuration

### 6.6.5 Tools > Network Traffic

#### Network Traffic Monitor Tool

The Tools > Network Traffic tab displays a graphical display of all data Traffic on the VIP Series.

- |                                |   |
|--------------------------------|---|
| <b><i>br-lan</i></b>           | Shows an overview of all data sent or received by the VIP Series. A summary of the data of the current day and the current month is shown.  |
| <b><i>br-lan / hourly</i></b>  | Shows the traffic volumes (TX = green, RX = grey) at hourly intervals during the current 24 hour period. This could be useful to see when the most or least amount of traffic is present. |
| <b><i>br-lan / daily</i></b>   | Shows the total data received and transmitted for the day, as well as the average rate of data.   |
| <b><i>br-lan / monthly</i></b> | Shows the total data received and transmitted for the current month, as well as the average rate of data.   |
| <b><i>br-lan / Top 10</i></b>  | Show the top 10 days with the most data sent or received.   |

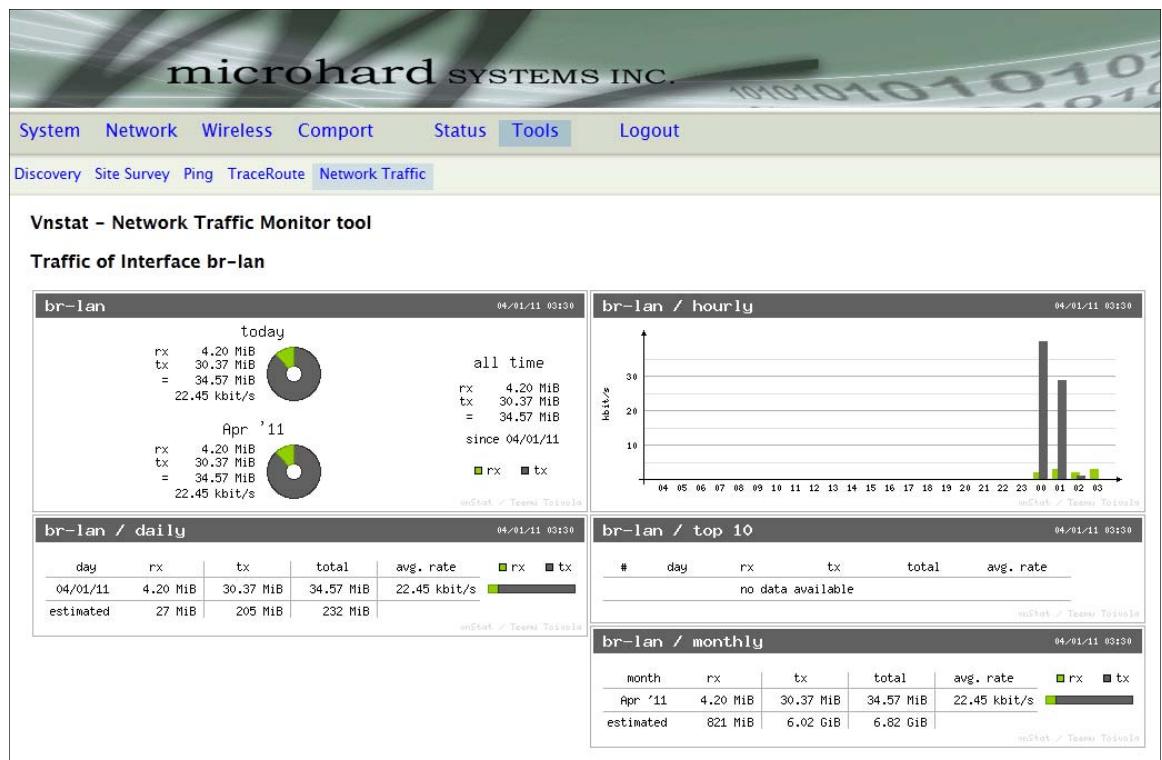


Image 6-31: Tools > Network Traffic

## 6.0 Configuration

### 6.7 Logout

#### 6.7.1 Logout > Logout

The logout menu allows a user to log out of the current session.

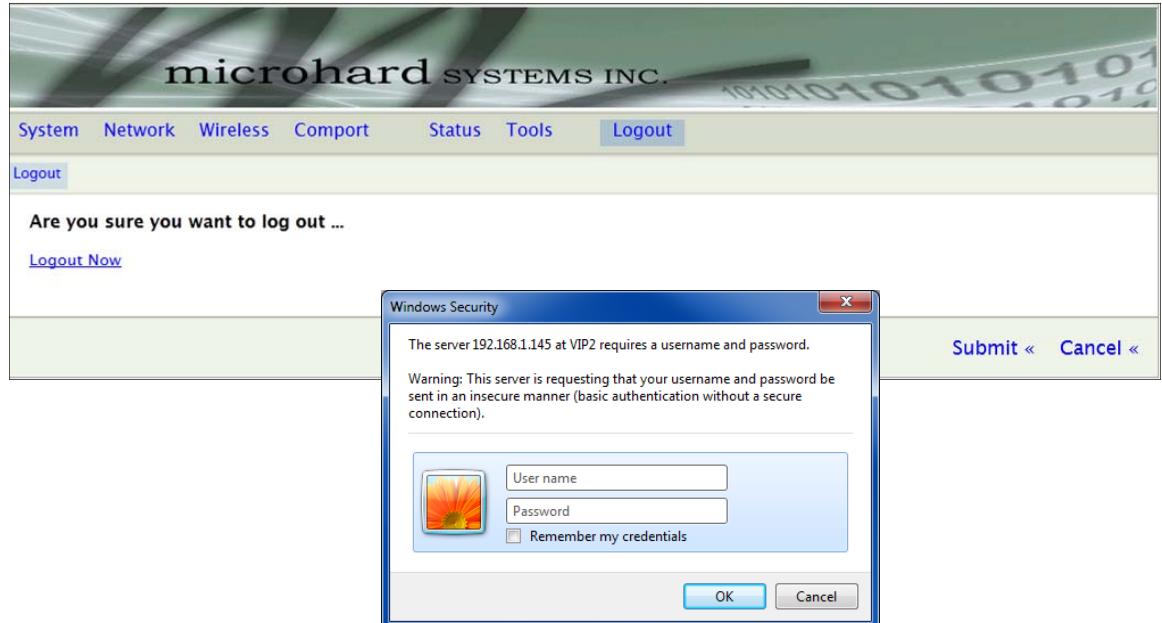


Image 6-32: Tools > Logout

## Appendix A: Serial Interface

---

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

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

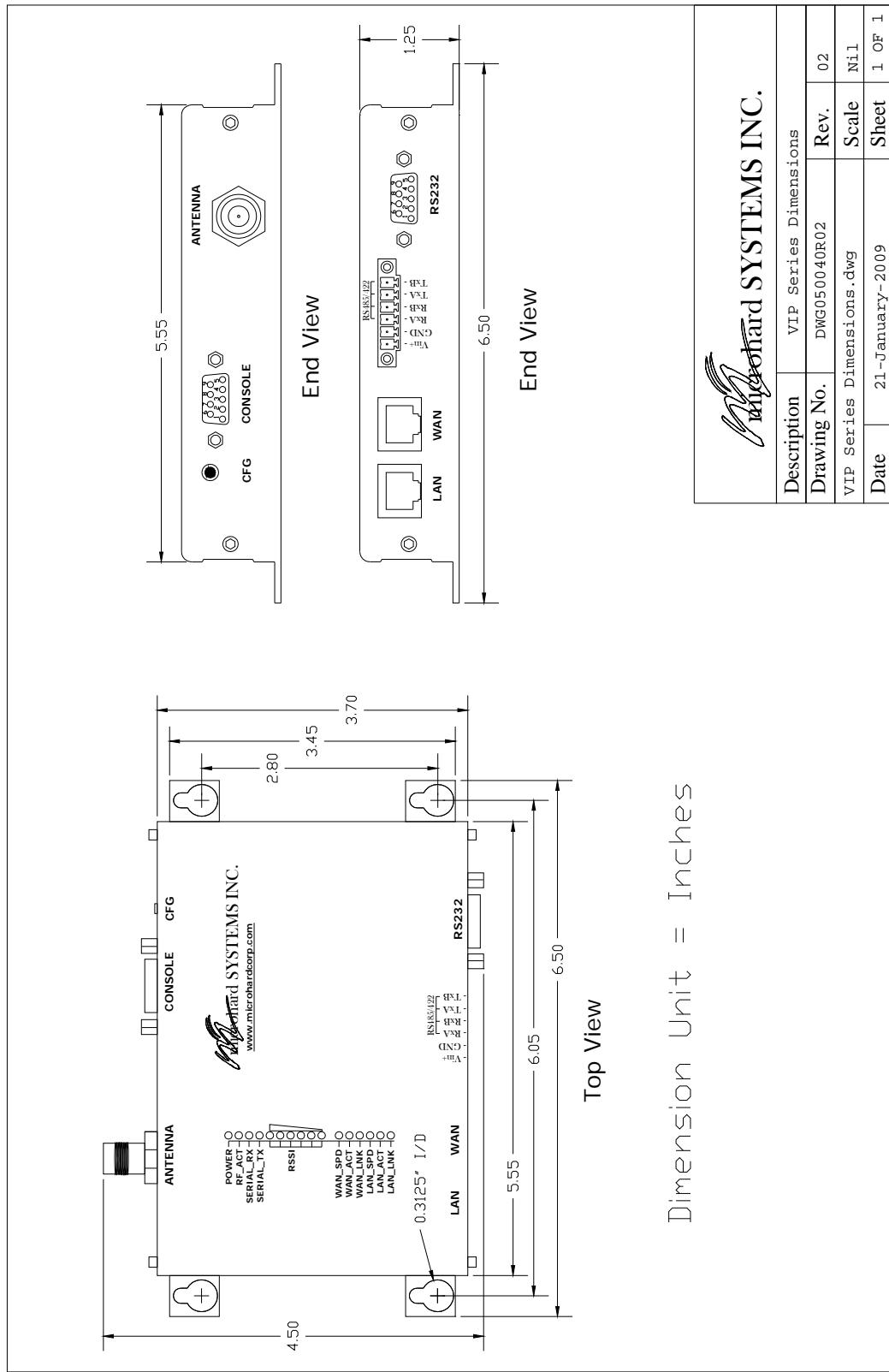
**CTS** *Clear to Send* - Output from Module - A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.

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.

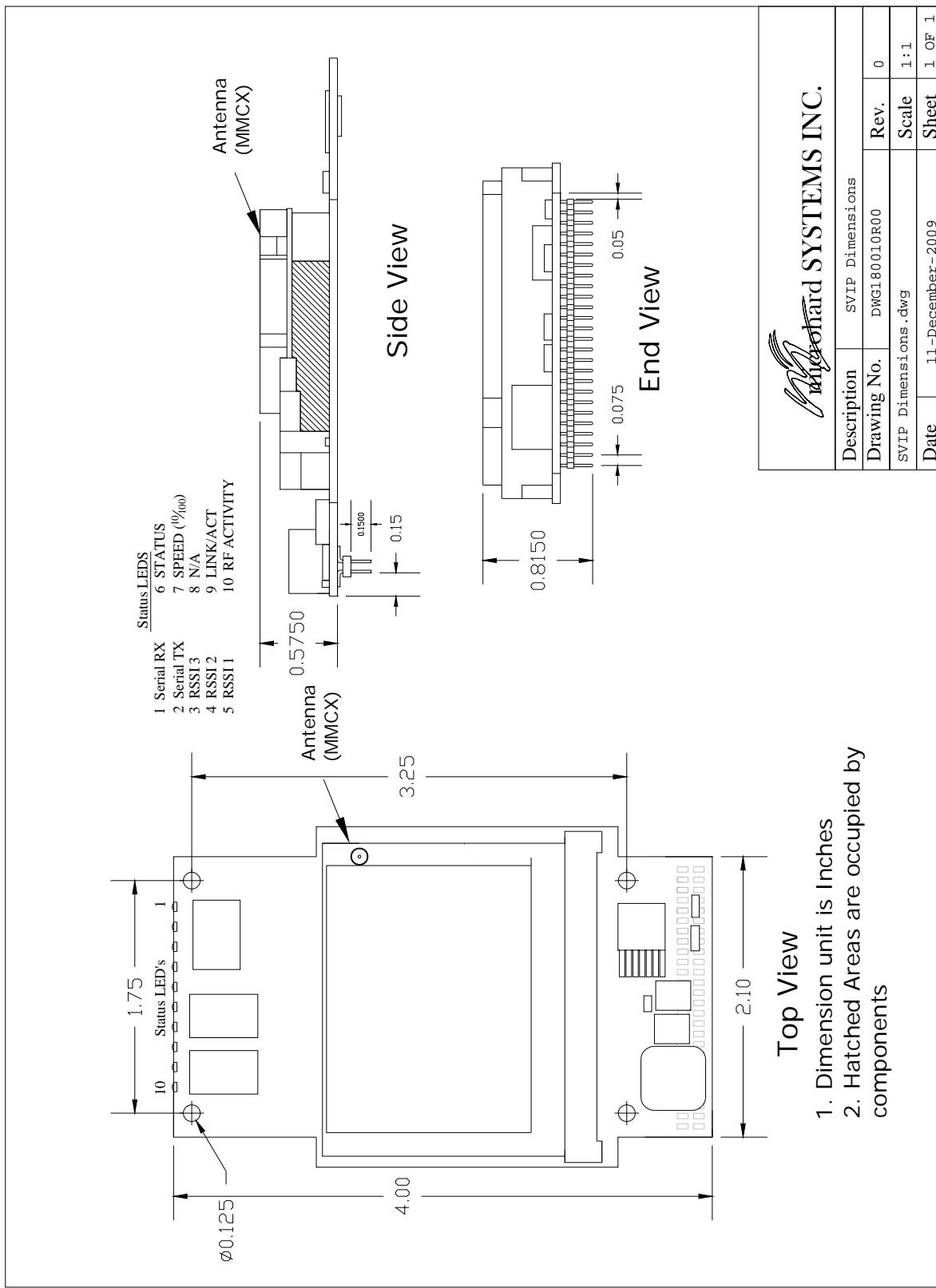
"DCE" and "module" are often synonymous since a module is typically a DCE device.

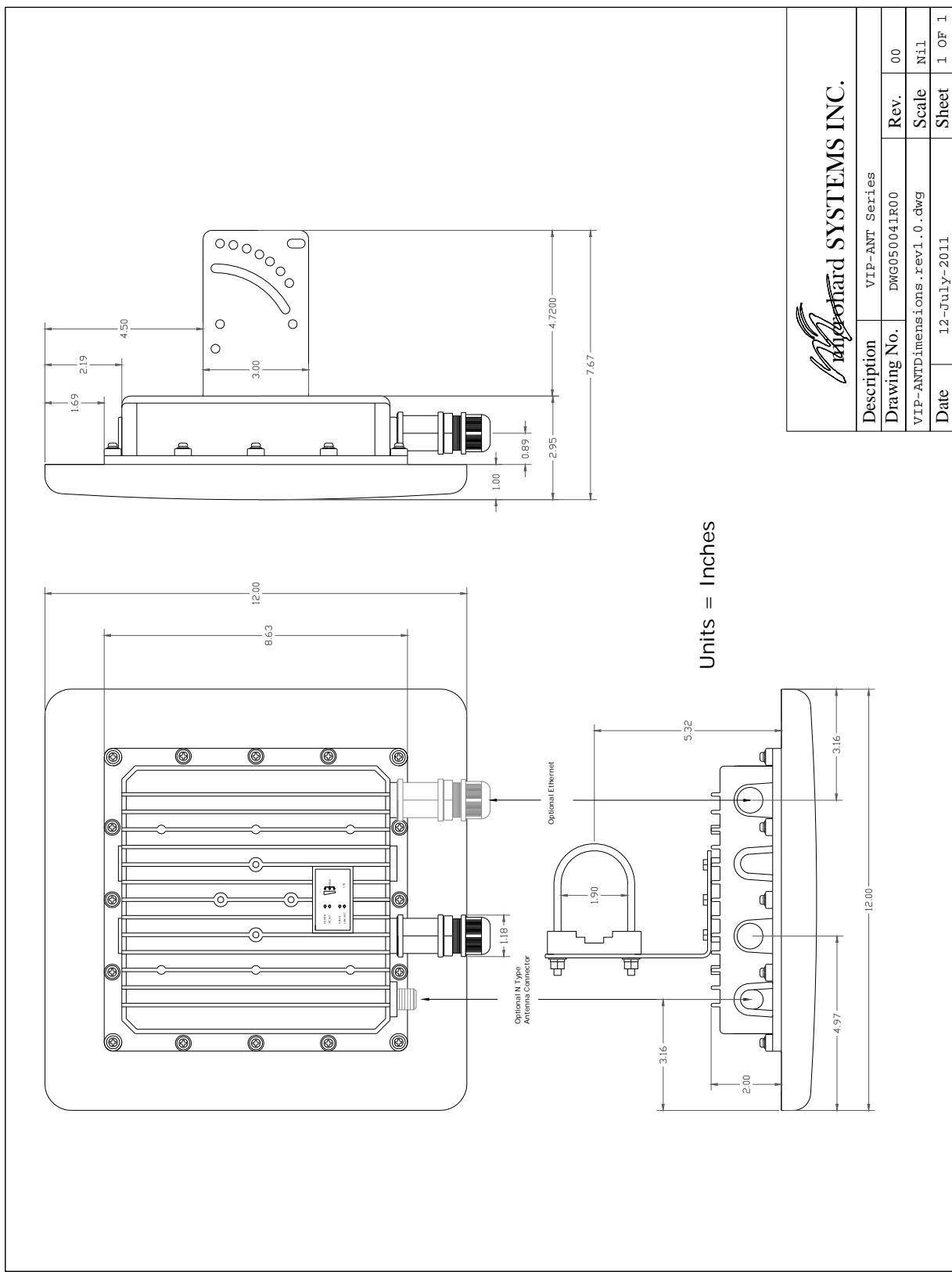
"DTE" is, in most applications, a device such as a host PC.

## Appendix B: VIP Mechanical Drawing

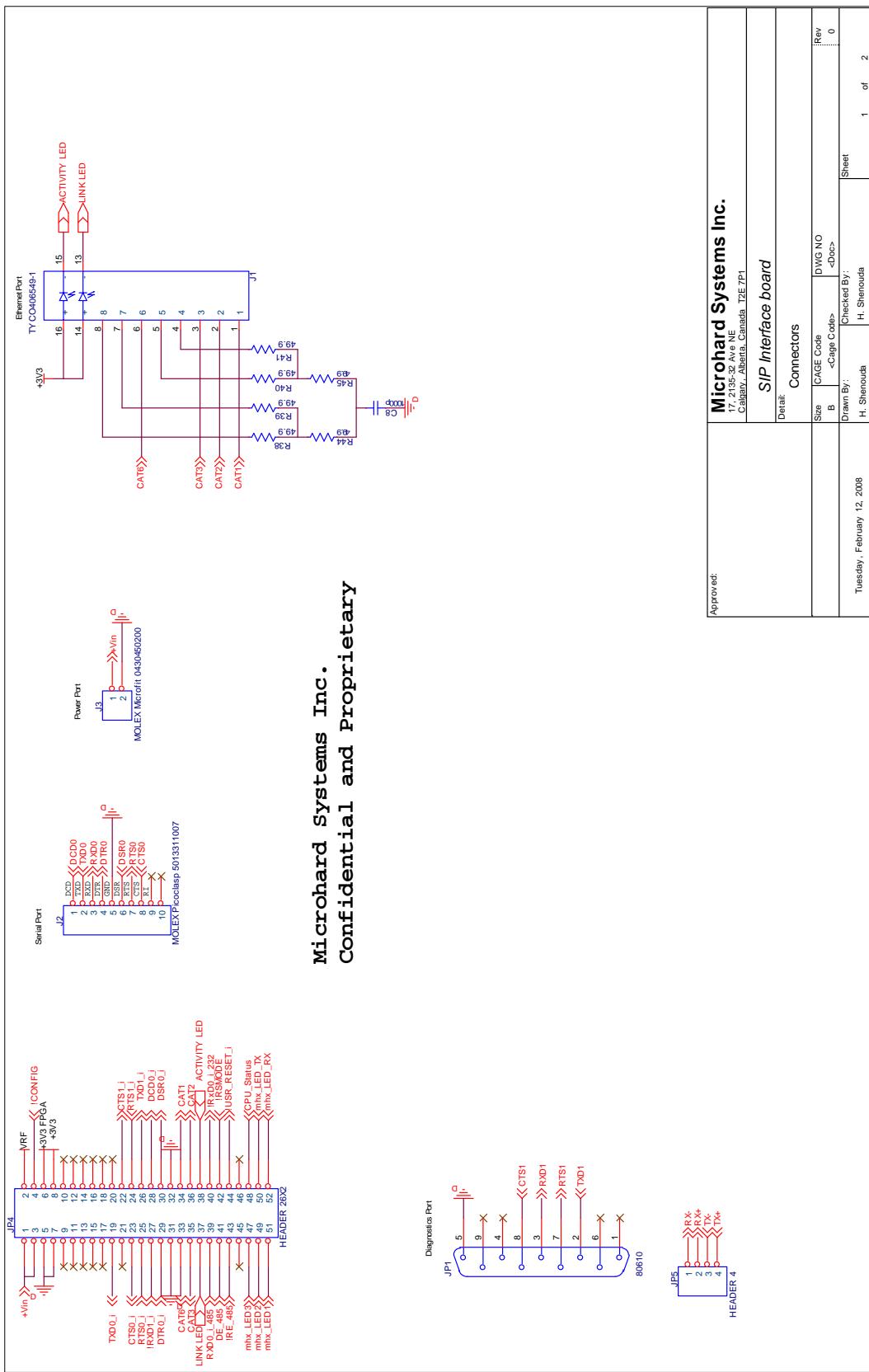


## Appendix C: SVIP Mechanical Drawing

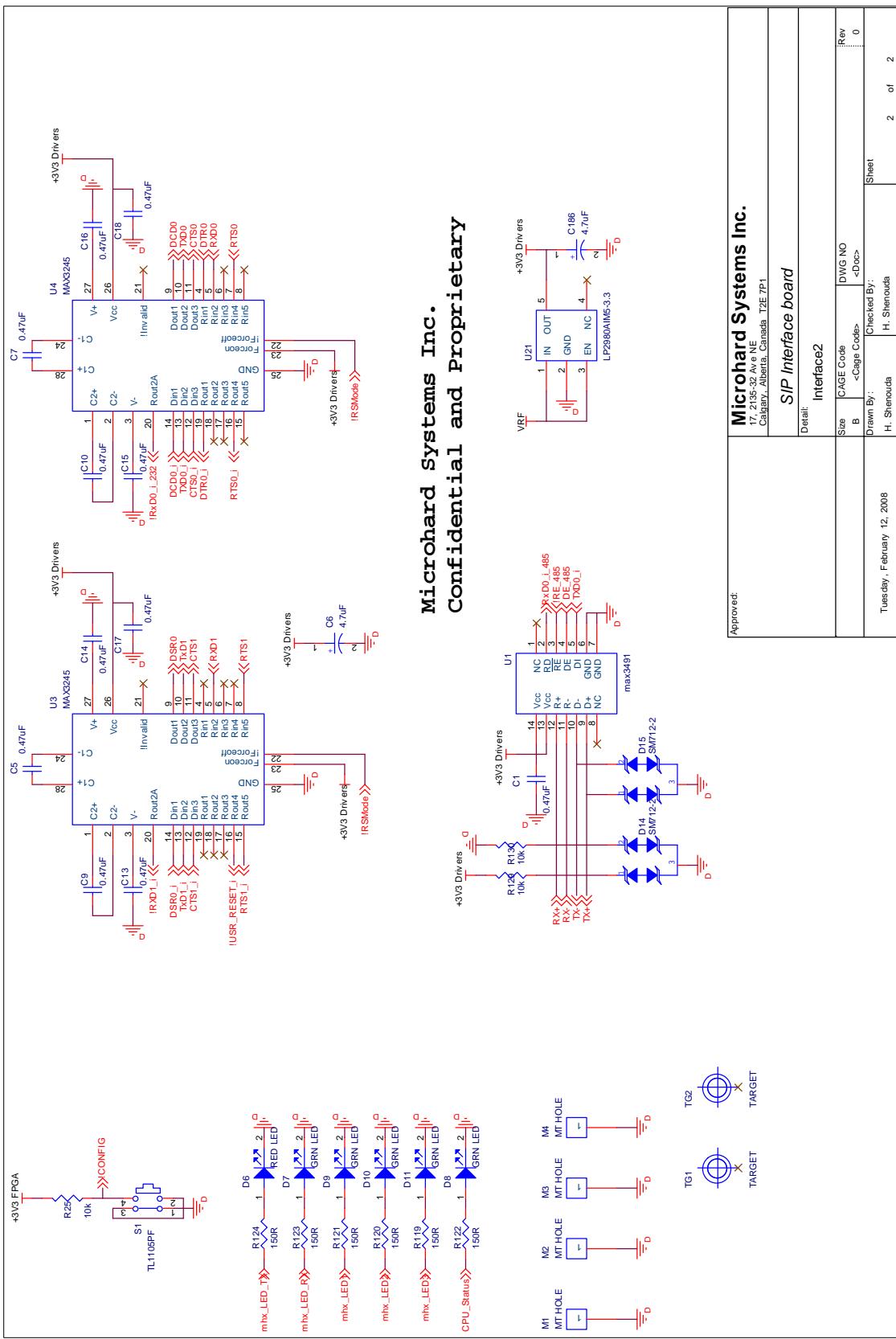


**Appendix D: VIP4900/5800-ANT Mechanical Drawing**

## Appendix E: SVIP Interface Schematic (Sample)



## Appendix E: SVIP Interface Schematic (Sample)



## Appendix F: 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

microhard SYSTEMS INC.

**VIP2.0 Series**



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

Phone: (403) 248-0028  
Fax: (403) 248-2762  
[www.microhardcorp.com](http://www.microhardcorp.com)