# ViPR™
# Narrowband IP Modem/Router

User Manual
PN 001-5008-000 Rev 5
Revised July 2009

**REVISION HISTORY**

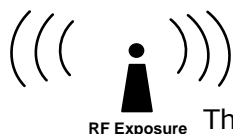| REV | DATE | REVISION DETAILS |
|-----|------|------------------|
| 0 | Jan 11, 2008 | Initial Release as 001-5008-000. |
| 1 | May 2008 | Update Dual Port ViPR information. |
| 2 | September 2008 | Added information about SNMP.<br>Updated Firmware Upgrade instructions. |
| 3 | December 2008 | Added information about TCP Client Server Mode.<br>Added information about Saving/Restoring User Configuration files. |
| 4 | April 2009 | Added information about V1.5 ViPR code release.<br>Added information about TCP Proxy Feature.<br>Added note to RF Acknowledgment section.<br>Corrected ViPR Power Cable Part in Accessory Table.<br>Added specifications and part number for 900 MHz ViPR.<br>Updated RF Exposure Compliance requirements.<br>Added section 2.10, Choosing an IP Addressing Scheme |
| 5 | July 2009 | Added information about V1.6 ViPR code release.<br>Added information about Listen Before Transmit Disable feature.<br>Added section about RF MAC override feature.<br>Added section about the Periodic Reset feature.<br>Added screen shot and information for the "Add Static Entry" function |

**IMPORTANT NOTICE**

Because of the nature of wireless communication, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors), or be totally lost. Significant delays or losses of data are rare when wireless devices such as the ViPR are used in a normal manner with a well-constructed network. ViPR should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. CalAmp accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using ViPR, or for the failure of ViPR to transmit or receive such data.

**RF EXPOSURE COMPLIANCE REQUIREMENTS**

**RF Exposure** The ViPR radio is intended for use in the Industrial Monitoring and Control and SCADA markets. The ViPR unit must be professionally installed and must ensure a minimum separation distance listed in the table below between the radiating structure and any person. An antenna mounted on a pole or tower is the typical installation and in rare instances, a 1/2-wave whip antenna is used.

|  | Antenna Gain | | |
|---|---|---|---|
|  | **5 dBi** | **10 dBi** | **15 dBi** |
| Min Safety Distance (VHF @ max Power) | 123cm | 218.8cm | 389cm |
| Min Safety Distance (UHF @ max Power) | 105.7cm | 188cm | 334.4cm |
| Min Safety Distance (900 MHz @ max power) | 63.8cm | 115 cm | 201.7 cm |

**Note: It is the responsibility of the user to guarantee compliance with the FCC MPE regulations when operating this device in a way other than described above.**

The ViPR radio uses a low power radio frequency transmitter. The concentrated energy from an antenna may pose a health hazard. People should not be in front of the antenna when the transmitter is operating.

The installer of this equipment must ensure the antenna is located or pointed such that it does not emit an RF field in excess of Health Canada limits for the general population. Recommended safety guidelines for the human exposure to radio frequency electromagnetic energy are contained in the Canadian Safety Code 6 (available from Health Canada) and the Federal Communications Commission (FCC) Bulletin 65.

Any changes or modifications not expressly approved by the party responsible for compliance (in the country where used) could void the user's authority to operate the equipment.

**TABLE OF CONTENTS**

## 1 VIPR OVERVIEW

This document provides information required for the operation and verification of the Dataradio ViPR Narrowband IP Modem/Router. The information in this manual makes the assumption the user's PC has an NIC (Network Interface Card) with TCP/IP implemented. Setup requires the knowledge and authorization to modify the TCP/IP settings for the NIC.

Changing or installing new IP addresses in a network can cause serious network problems. If you have any questions or concerns, contact the Network Administrator for your system.

### 1.1 GENERAL DESCRIPTION

ViPR provides any IP-enabled device with connectivity to transmit narrowband data. This DSP-based radio was designed for SCADA, telemetry and industrial applications in the 136-174 MHz, 215-240 MHz VHF, 406.1-512 MHz UHF, and 928-960 MHz frequency ranges.

ViPR supports serial and Ethernet/IP Remote Terminal Units (RTU) and programmable logic controllers (PLC). It is standard IEEE 802.3 compliant. ViPR supports any protocol running over IPv4 (including ICMP, IPinIP, IPSec, RSVP, TCP and UDP protocols). It provides MAC layer bridging and HTTP, ARP, and static routing packet forwarding.

### 1.2 OPERATIONAL CHARACTERISTICS

The ViPR product has the following operational characteristics:

- Frequency range of 136-174 MHz, 215-240 MHz, 406.1-470 MHz, 450-512 MHz, or 928-960 MHz.
- User-selectable data rates
- Built-in transceiver adjustable from 1 to 10 watts (8 watts max for 900MHz)
- Used as an access point or an end point with each configurable in (a) Bridge mode for quick setup of units on same network or (b) Router mode for advanced networks
- Embedded web server to access status and/or setup information
- Remote access for over-the-air system firmware upgrades
- Wide input power range of 10 to 30 volts DC
- AES 128-bit data encryption (Applies to Serial and IP connections)
- Superior data compression (zlib compression algorithm applies to Serial and IP connections)
- Native UDP and TCP/IP support
- Online and Offline Diagnostics
- Supports up to 32 different frequency channel pairs
- Industrial operating temperature range of -30 to +60 C
- Rugged die-cast aluminum and steel case

These features provide system benefits that give users:

**Rugged Packaging**.  ViPR is housed in a compact and rugged cast aluminum case.  Built for industrial applications in a variety of environments, ViPR operates over an extended temperature range and provides worry-free operation in the roughest environments.

**Simple Installation**.  Basic installation typically utilizes an omni-directional antenna at the master station or Relay Point and a directional antenna at each remote site not a Relay Point. See Section 2 for information on Site and Antenna Selection. For basic service, just hook up an antenna, connect your Ethernet LAN to the ViPR's LAN port, apply primary power, check and set a few operating parameters and you are done.

**Flexible Management**. Configuration, commissioning, maintenance and troubleshooting can be done locally or remotely. There are no physical switches or adjustments; all operating parameters are set via a web browser. The Dual-Port ViPR provides a receive antenna connector allowing for unique customer applications requiring additional receive filtering, external PA(s), and other options.

**Long Range**. Narrowband configurations allow better coverage over harsh terrain.

### 1.3   PHYSICAL DESCRIPTION

ViPR consists of two logic PCBs, one that includes the modem circuitry and the other the radio module.  Both are installed in a cast aluminum case.  The unit is not hermetically sealed and should be mounted in a suitable enclosure when dust, moisture, and/or a corrosive atmosphere are anticipated.

The ViPR is designed for easy installation and configuration; the ViPR features no external or internal switches or adjustments.  All operating parameters are set via an internal web browser.

### 1.3.1  Front Panel
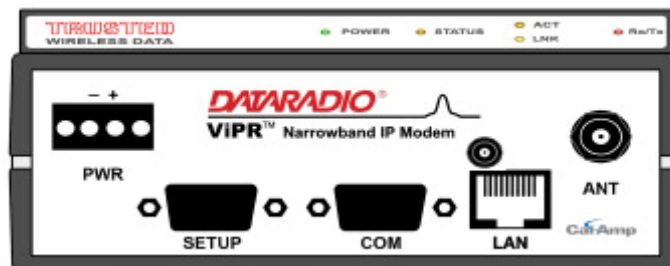


Figure 1.1 ViPR Front Panel (Dual-port model shown)

As shown in Figure 1.1, the front panel has the following connections:

- (1) RJ-45 LAN 10 BaseT Ethernet connection with Auto-MDIX
- (1) 50-ohm TNC female Antenna connector
- (1) 50-ohm SMA female receive antenna connector (Dual-Port models only)
- (1) Right-angle power connector (10-30 VDC)
- (2) DE-9F RS-232 ports
- For Dual-port ViPR connections, see Section 1.3.6.

### 1.3.2  LED Panel

The LED panel has five Tri-Color LEDs. The functionality of each LED is shown in Table 1.1.

*Table 1.1 ViPR LED Functionality*

| LED | Color | Definition |
|-----|-------|------------|
| Power | Green | ViPR ready, normal operations |
|  | Red | ViPR hardware fault |
| Status | Green | ViPR no faults, normal operations |
|  | Blinking Green | ViPR scanning for neighbors |
|  | Red | ViPR has a fault condition, check unit status |
|  | Amber (Solid or Blinking) | ViPR detects high background noise |
| ACT | Blinking Green | Ethernet activity detected on PHY link (RJ45) |
|  | Off | No Ethernet activity on PHY link (RJ45) |
| Lnk | Green | Ethernet connection established (RJ45) |
|  | Off | No Ethernet connection (RJ45) |
| Rx/Tx | Green | Receiving data |
|  | Red | Transmitting data |

### 1.3.3  Ethernet LAN Port

The Ethernet LAN port is an RJ-45 receptacle with a 10 BaseT Ethernet connection and Auto-MDIX feature.  Table 1.2 shows pin-out descriptions for the RJ-45 port.

*Table 1.2 Pin-out for IEEE-802.3 RJ-45 Receptacle Contacts*

| Contact | 10 Base-T Signal |
|---------|------------------|
| 1 | TXP[1] |
| 2 | TXN[1] |
| 3 | RXP[1] |
| 4 | SPARE |
| 5 | SPARE |
| 6 | RXN[1] |
| 7 | SPARE |
| 8 | SPARE |
| SHELL | Shield |
| (1) The name shows the default function. Given the Auto-MDIX capability of the Ethernet transceiver, TX and RX function could be swapped. | |

### 1.3.4  SETUP and COM Ports

The SETUP and COM serial connections are DE-9F RS-232 ports.

Serial port considerations:

- ViPR radio modem SETUP and COM ports are Data Communication Equipment (DCE) devices
- In general, equipment connected to the ViPR's SETUP / COM serial port is Data Terminal Equipment (DTE) and a straight-through cable is recommended.

    Note: If a DCE device is connected to the ViPR SETUP / COM port, a null modem cable/adapter is required.

The pin-out for the SETUP and COM ports are shown in Table 1.3.

*Table 1.3 Pin-out for DCE SETUP and COM port, 9 Contact DE-9 Connector*

| Contact | EIA-232F Function | Signal Direction |
|---------|-------------------|------------------|
| 1 | DCD[1] | DTE ← DCE |
| 2 | RXD | DTE ← DCE |
| 3 | TXD | DTE → DCE |
| 4 | DTR | DTE → DCE |
| 5 | GND | DTE --- DCE |
| 6 | DSR[2] | DTE ← DCE |
| 7 | RTS[1] | DTE → DCE |
| 8 | CTS[1] | DTE ← DCE |
| 9 | RING [3] | DTE --- DCE |
| (1) Programmable. | | |
| (2) Always asserted | | |
| (3) For future use | | |

The DCD, DTR, RTS and CTS control lines are programmable.  Refer to section 6.4 for serial port control line configurations.

### 1.3.5  Power Connector

The ViPR is supplied with a right-angle power connector (10-30 VDC). Table 1.4 shows the pin-out of the power connector.

*Table 1.4 Pin-out of the power connector*

| Contact # (Left to Right) | Color | Description |
|---------------------------|-------|-------------|
| 4 | | Fan Power Output (5V) |
| 3 | Black | Ground |
| 2 | Red | Positive (10-30) VDC |
| 1 | White | Enable |

*Note: The White Enable line must be tied to the red positive lead of the connector for the ViPR to function.*

### 1.3.6 Antenna Connector

The standard ViPR has a 50-ohm TNC female antenna connector. This connection functions for both transmit and receive.

The Dual-Port ViPR has a 50-ohm TNC female antenna connector functioning for transmit (only) and a 50-ohm SMA female antenna connector functioning for receive (only). The separate receive antenna connector allows for unique customer applications that require additional receive filtering, external PA(s) and other options.

***Warning: The transmit antenna port must not be connected directly to the receive antenna port of the Dual-Port ViPR. Excessive power into the receive antenna port will damage the radio. Input power to the receiver should not exceed 17 dBm (50mW).***

To reduce potential interference, the antenna type and its gain should be chosen to ensure the effective isotropic radiated power (EIRP) is not more than required for successful communication.

### 1.3.7 Chassis Dimensions

*Figure 1.2 shows the dimensions of the ViPR Chassis and mounting plate.*
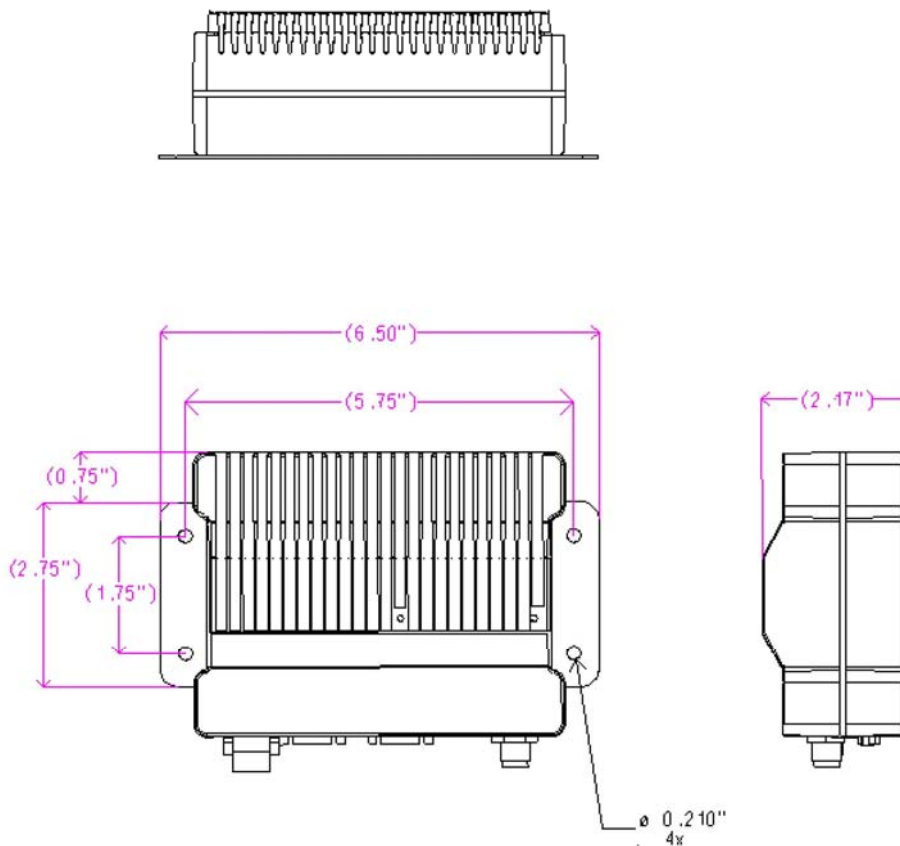


*Figure 1.2 ViPR Chassis Dimensions (units are in inches)*

## 1.4  PART NUMBERS AND AVAILABILITY

### 1.4.1  ViPR Radio

Table 1.5 provides a breakdown of the ViPR part number 140-50X8-Y0Z.

*Table 1.5 - Part Number Breakdown*

| Model Number | Description | Frequency Range |
|---|---|---|
| 140-5018-500 | Standard VHF ViPR | 136 - 174 MHz |
| 140-5028-502 | Standard VHF ViPR 200 | 215 – 240 MHz |
| 140-5048-300 | Standard UHF ViPR Range 3 | 406.1 - 470 MHz |
| 140-5048-500 | Standard UHF ViPR Range 5 | 450 – 512 MHz |
| 140-5098-500 | Standard 900MHz ViPR | 928 – 960 MHz |
|  |  |  |
| 140-5018-501 | Dual Port VHF ViPR | 136 - 174 MHz |
| 140-5028-503 | Dual Port VHF ViPR 200 | 215 – 240 MHz |
| 140-5048-301 | Dual Port UHF ViPR Range 3 | 406.1 - 470 MHz |
| 140-5048-501 | Dual Port UHF ViPR Range 5 | 450 – 512 MHz |
| 140-5098-501 | Dual Port 900MHz ViPR | 928 – 960 MHz |

### 1.4.2  Accessories and Options

Tables 1.6-1.8 list standard accessories (including antenna, feedline, and connectors) tested and approved for use with the ViPR.

*Table 1.6 - Accessories*

| ITEM | PART NUMBER |
|---|---|
| ViPR Power Cable | 897-5008-010 |
| ViPR Demo Kit* – VHF - 136-174, 215-240 MHz | 250-5018-500 |
| ViPR Demo Kit* – UHF - 406-470 MHz | 250-5048-300 |
| ViPR Demo Kit* – UHF - 450-512 MHz | 250-5048-500 |
| Factory Installed ViPR Fan Kit | 150-5008-001 |
| Field Installed ViPR Fan Kit** | 150-5008-002 |
| TNC-Male to N-Male 18" | 250-0697-103 |
| TNC-Male to N-Male 48" | 250-0697-104 |
| TNC-Male to N-Male 72" | 250-0697-105 |
| TNC-Male to N-Female 18" | 250-0697-106 |

*\* The ViPR Demo Kit includes two of each of the following: ViPR, rubber duck antennas, adapters, attenuators, power cables, and power supplies.*
*\*\* The field install Fan Kit is available for all UHF/900 ViPRs (140-5048-xxx/140-5098-xxx) but is only available for VHF models (140-5018-xxx) with RF revision 0.3 or greater (shipping Fall 2008). Contact CalAmp Technical Support for more information.*

*Table 1.7 Antenna Kits*

| ITEM | PART NUMBER |
|------|-------------|
| Antenna Kit*: 138-143 MHz 6.5 dBd | 250-0211-007 |
| Antenna Kit*: 138-143 MHz 9.5 dBd | 250-0211-010 |
| Antenna Kit*: 143-148 MHz 6.5 dBd | 250-0211-107 |
| Antenna Kit*: 143-138 MHz 9.5 dBd | 250-0211-110 |
| Antenna Kit*: 148-152 MHz 6.5 dBd | 250-0211-207 |
| Antenna Kit*: 148-152 MHz 9.5 dBd | 250-0211-210 |
| Antenna Kit*: 152-157 MHz 6.5 dBd | 250-0211-307 |
| Antenna Kit*: 152-157 MHz 9.5 dBd | 250-0211-310 |
| Antenna Kit*: 157-163 MHz 6.5 dBd | 250-0211-407 |
| Antenna Kit*: 157-163 MHz 9.5 dBd | 250-0211-410 |
| Antenna Kit*: 163-169 MHz 6.5 dBd | 250-0211-507 |
| Antenna Kit*: 163-169 MHz 9.5 dBd | 250-0211-510 |
| Antenna Kit*: 169-174 MHz 6.5 dBd | 250-0211-607 |
| Antenna Kit*: 169-174 MHz 9.5 dBd | 250-0211-610 |
| Antenna Kit*: 216-222 MHz 6.5 dBd | 250-0221-007 |
| Antenna Kit*: 216-222 MHz 9.5 dBd | 250-0221-010 |
| Antenna Kit*: 450-470 MHz, 7 dBd | 250-0241-507 |
| Antenna Kit*: 450-470 MHz, 10 dBd | 250-0241-510 |
| Antenna Kit*: 890-960 MHz, 6.4 dBd | 250-5099-011 |
| Antenna Kit*: 890-960 MHz, 10 dBd | 250-5099-021 |

*Kits include premium antenna, mounting bracket, surge protector, grounding kit, cable ties, 18" TNC male to N-male jumper cable and weather kit. UHF/900 kits include 25 feet of LMR400 antenna feedline. Feedline is available for VHF kits in 25 or 50 feet lengths.*

*Table 1.8 - Feedline and Connectors*

| ITEM | PART NUMBER |
|------|-------------|
| 25 feet antenna feedline (LMR400), N-Male | 250-0200-025 |
| 50 feet antenna feedline (LMR400), N-Male | 250-0200-055 |
| Barrel Connector, RF1 N type, Female | 250-0200-100 |

## 1.5   PRODUCT WARRANTY

It is our guarantee that every ViPR Radio modem will be free from physical defects in material and workmanship for TWO YEARS from the date of purchase when used within the limits set forth in Appendix A: Specifications.

The manufacturer's warranty statement is available in Appendix B. If the product proves defective during the warranty period, contact our Customer Service Department to obtain a Return Material Authorization (RMA). BE SURE TO HAVE THE EQUIPMENT MODEL, SERIAL NUMBER, AND BILLING & SHIPPING ADDRESSES AVAILABLE WHEN CALLING. You may also request an RMA online at www.calamp.com/component/option,com_rma/

**FACTORY AND TECHNICAL SUPPORT**
M-F 7:30-4:30 CST

CalAmp Wireless DataCom
299 Johnson Ave., Ste 110, Waseca, MN 56093
Tel 507.833.8819; Fax 507.833.6758
Email imcsupport@calamp.com

## 1.6  RMA REQUEST

When returning a product, mark the RMA clearly on the outside of the package. Include a complete description of the problem and the name and telephone number of a contact person.  RETURN REQUESTS WILL NOT BE PROCESSED WITHOUT THIS INFORMATION.

**Contact Customer Service:**
299 Johnson Ave., Ste 110
Waseca, MN 56093
Tel 1.507.833.8819

BE SURE TO HAVE THE EQUIPMENT MODEL AND SERIAL NUMBER, AND BILLING AND SHIPPING ADDRESSES ON HAND WHEN CALLING.

For units in warranty, customers are responsible for shipping charges to CalAmp Wireless DataCom. For units returned out of warranty, customers are responsible for all shipping charges. Return shipping instructions are the responsibility of the customer.

## 1.7  DOCUMENTATION AND DOWNLOADS

CalAmp reserves the right to update its products, software, or documentation without obligation to notify any individual or entity. Product updates may result in differences between the information provided in this manual and the product shipped.  For access to the most current product documentation and application notes, visit www.calamp.com/home/download_library.html

## 2   SYSTEM ARCHITECTURE AND NETWORK PLANNING

This section briefly discusses network architecture (including basic network types), interfacing modems and DTE, data protocols for efficient channel operation, addressing, and repeaters.

ViPR is designed to replace wire lines in SCADA, telemetry and control applications. The Ethernet and RS-232 serial port allows direct connection to Programmable Logic Controllers (PLCs) or Remote Terminal Units (RTUs).  A SCADA system is defined as one or more centralized control sites used to monitor and control remote field devices over wide areas. For example, a regional utility may monitor and control networks over an entire metropolitan area.  Industry sectors with SCADA systems include energy utilities, water and wastewater utilities, and environmental groups.

The ViPR is intended for use in the Industrial Monitoring and SCADA market.  The range of the ViPR is dependent on terrain, RF (radio frequency) path obstacles, and antenna system design.  This section provides tips for selecting an appropriate site, choosing an antenna system, and reducing the chance of harmful interference.

### 2.1   SINGLE COVERAGE AREA

In a network topology with only a single coverage area (all units can talk to one another directly), there are several common system configurations.
The most common is for one unit to be designated as a master and the rest designated as remotes.  Another system configuration is Report-by-Exception.

### 2.2   MASTER/REMOTE

In a ViPR network, ViPRs are not programmed to be masters or remotes.  All ViPRs in a network can be configured the same.  However, a unit can be configured as an Access Point. The unit configured as an Access Point would allow access to the Internet, but an Access Point is not required in all networks.  Most SCADA networks have a "polling master", but the polling master is not necessarily configured any different than the remotes.  It is the responsibility of the polling master to control RF traffic so RF collisions do not occur.

**Note: In a radio system, only one radio should transmit at a time.  If two radios transmit at the same time to another radio, RF collisions occur.  Collisions will slow data traffic and possibly corrupt data.**

The ViPR has RF collision avoidance technology (checks the air wave for a carrier before transmitting) and Ethernet CSMA (Carrier Sense Multiple Access). CSMA is an Ethernet collision avoidance mechanism technology built into to all Ethernet connections. These technologies still need to be supplemented by the HMI/PLC polling master to optimize RF data traffic.

Some HMI/PLC Ethernet applications may depend solely on Ethernet CSMA to control the flow of messages to avoid RF collisions in a ViPR network.  This may flood the network with multiple polling messages, making it difficult for the RTUs to acquire the airwave to transmit their reply messages.  This will cause the RTUs to compete for airtime and a dominant RTU may be created.

While the dominant RTU/radio is transmitting, the other RTUs will send their reply messages to their connected ViPR.  ViPRs will buffer reply messages because the dominant RTU/radio is transmitting (carrier is present).  A ViPR will buffer (while a carrier is present) a reply message until it can capture the airwave (carrier absent) to transmit.  There could be five or six RTU/radios in a small system (or 10 or 20 in a large system), which could be trying to

capture the airwaves to transmit.  The RTUs will not respond in the order they were polled but will respond when they are ready and have captured the airwaves. The dominant RTU is created because it happens to reply at just the right time and be in the right order in the polling sequence.

A common method for a polling master to manage RF traffic is for the HMI/PLC polling master to poll one remote at a time.  The next polling message is not sent until the current message has been completed ("Done") or has timed out. This prevents more than one outstanding polling message.  Ladder logic programs typically refer to these parameters as the message "Done" and "Error" bits.  The "Done" and "Error" bits parameter values can be adjusted for longer timeout values, if required.

Because the ViPR has the ability to use two completely different and separate SCADA polling protocols, it is important to have interaction between the two protocols.  The ViPR can send out an Ethernet TCP/IP polling message and also an RS232 polling message, which may or may not be generated by the same HMI/PLC. CalAmp recommends the user program the polling sequence in each protocol with logic that interacts with the other's protocol "Done" and "Error" bits.  The Ethernet polling protocol would not be allowed to send a message until the current Ethernet message is either "Done" or "Error" **and** the previous RS232 message are either "Done" or "Error" bits are set.  The RS232 polling protocol would also have a similar logic.

## 2.3  POINT-TO-POINT

A point-to-point network is the most simple of all networks, and may be used for connecting a pair of PC's, a host computer and a terminal, a SCADA polling master and one remote, mobile applications (like in-vehicle GPS receivers and base stations) or a wide variety of other networking applications.

System configurations indicated above allow for either Ethernet or serial interfaces.  In bridge mode, all the network devices are on the same IP subnet. In router mode, the Ethernet connection on the polling master unit and the remote(s) use different IP subnets. A hub or switch may be used to allow multiple devices to connect to the ViPR radio modem. Serial connections are transparent pass-through connections, allowing the use of legacy serial devices in the ViPR product environment.



ViPR (a) Master          ViPR (b) Remote

*Figure 2.1 – Point-to-Point Network*

### 2.3.1  Point-to-Multipoint

A Point-to-Multipoint network is a common network type used in SCADA or other polling systems.  The single polling master station communicates with any number of remotes and controls the network by issuing polls and waiting for remote responses.  Individual PLC/RTU remotes manage addressing and respond when their individual addresses are queried.  PLC/RTU unit addresses are maintained in a scanning list stored in the host program or master terminal device at the SCADA host site.  Communications equipment is transparent and does not interact with specific remotes; all data is coupled to the host on a single data line (such a network is commonly used with synchronous radio modems and asynchronous radio modems).



*Figure 2.2 – Point to Multipoint Network*

### 2.3.2  Report by Exception

In a true Report by Exception configuration, the remotes send data to the master only when an event or exception has occurred in the remote.  However, most Report by Exception systems have a master/remote polling component. The master polls the remotes once every hour or half-hour to ensure there is still a valid communication path.  In a Report by Exception configuration, there will not be a master controlling RF traffic and RF collisions will often occur.  The ViPR has several collision avoidance features to help minimize collisions.  The ViPR is a "polite radio".  The ViPR will check the RF traffic on the receive channel before transmitting.  If there is no RF traffic present (no carrier present) it will transmit.  If there is RF traffic (carrier present) the ViPR will buffer the data.  The ViPR will transmit the buffered data when there is no RF traffic present (no carrier present).

## 2.4 EXTENDING THE COVERAGE AREA WITH A RELAY POINT

The ViPR has a Relay Point feature that allows a unit to relay data from one RF coverage area to another RF coverage area. When units are spread over two or more coverage areas, the user must identify the devices forming the backbone between coverage areas so any unit can talk to any other regardless of their locations.  There can be multiple Relay Points in the system extending the coverage over several hops.
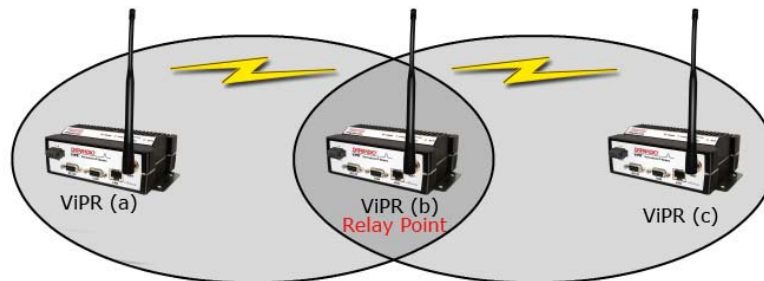


*Figure 2.3 - Two Coverage Areas*

The unit forming the backbone between the coverage areas must be configured to repeat all necessary information from one coverage area to the next.  This unit must have the Relay Point parameter enabled (See Section 6.1).

### 2.4.1  Understanding RF Path Requirements

Radio waves are propagated when electrical energy produced by a radio transmitter is converted into magnetic energy by an antenna.  Magnetic waves travel through space.  The receiving antenna intercepts a very small amount of this magnetic energy and converts it back into electrical energy that is amplified by the radio receiver.  The energy received by the receiver is called the Received Signal Strength Indication (RSSI) and is measured in dBm.

A radio modem requires a minimum amount of received RF signal to operate reliably and provide adequate data throughput.  This is the radio's receiver sensitivity.  In most cases, spectrum regulators will define or limit the amount of signal that can be transmitted and it will be noted on the FCC license.  This is the effective isotropic radiated power (EIRP). Transmitted power decays with distance and other factors as it moves away from the transmitting antenna.

## 2.5  SITE SELECTION AND SITE SURVEY

### 2.5.1  Site Selection

For a successful installation, careful thought must be given to selecting the site for each radio. Suitable sites should provide the following:

- Protection from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna, interface, or other cabling
- Antenna location with an unobstructed transmission path to all remote radios in the system

These requirements can be quickly determined in most cases.

### 2.5.2  Site Survey

A Site Survey is an RF propagation study of the RF path between two points or between one point and multiple points.  UHF radio signals travel primarily by line of sight and obstructions between the sending and receiving stations will affect system performance. Signal propagation is also affected by attenuation from obstructions such as terrain, foliage, or buildings in the transmission path.  A Site Survey is recommended for most projects to determine the optimal RF paths for each link.  This is especially true when more than one RF coverage area is required.  A Site Survey will determine the best unit location for the Relay Points.

### 2.6   SELECTING ANTENNA AND FEEDLINE

The ViPR can be used with a variety of antenna types. The exact style used depends on the physical size and layout of a system. The ViPR device has been tested and approved with antennas having a maximum gain of 10 dBi.

### 2.6.1  Antenna Gain

Antenna gain is usually measured in comparison to a dipole.  A dipole acts much like the filament of a flashlight bulb: it radiates energy in almost all directions.  One bulb like this would provide very dim room lighting.  Add a reflector capable of concentrating all the energy into a narrow angle of radiation and you have a flashlight.  Within that bright spot on the wall, the light might be a thousand times greater than it would be without the reflector.  The resulting bulb-reflector combination has a gain of 1000, or 30 dB, compared to the bulb alone.  Gain can be achieved by concentrating the energy both vertically and horizontally, as in the case of the flashlight and Yagi antenna.  Gain can be also be achieved by reducing the vertical angle of radiation, leaving the horizontal alone.  In this case, the antenna will radiate equally in all horizontal directions, but will take energy that otherwise would have gone skywards and use it to increase the horizontal radiation.

The required antenna impedance is 50 ohms.  To reduce potential radio interference, the antenna type and its gain should be chosen to ensure the effective isotropic radiated power (EIRP) is not more than required for successful communication.

See Table 1.7 for a list of tested antenna recommendations. These antennas are FCC approved for use with the ViPR. Similar antenna types from other manufacturers are equally acceptable. It is important to follow the manufacturer's recommended installation procedures and instructions when mounting any antenna.

### 2.6.2  Omni Directional Antenna

In general, an omni directional antenna should be used at a master station and Relay Points.  This allows equal coverage to all of the remote locations. Omni directional antennas are designed to radiate the RF signal in a 360-degree pattern around the antenna.  Short range antennas such as folded dipoles and ground independent whips are used to radiate the signal in a ball shaped pattern while high gain omni antennas, such as a collinear antenna, compress the RF radiation sphere into the horizontal plane to provide a relatively flat disc shaped pattern that travels further because more of the energy is radiated in the horizontal plane.

### 2.6.3  Yagi Antenna

At remote locations (not used as a Relay Point), a directional Yagi is generally recommended to minimize interference to and from other users.

### 2.6.4  Vertical Dipoles

*Vertical dipoles are very often mounted in pairs, or sometimes groups of 3 or 4, to achieve even coverage and to increase gain. The vertical collinear antenna usually consists of several elements stacked one above the other to achieve similar results.*

*Figure 2.4 - Antenna Types*

| Omni (Vertical Collinear) | Yagi | Vertical Dipole |
|---|---|---|
| | | |
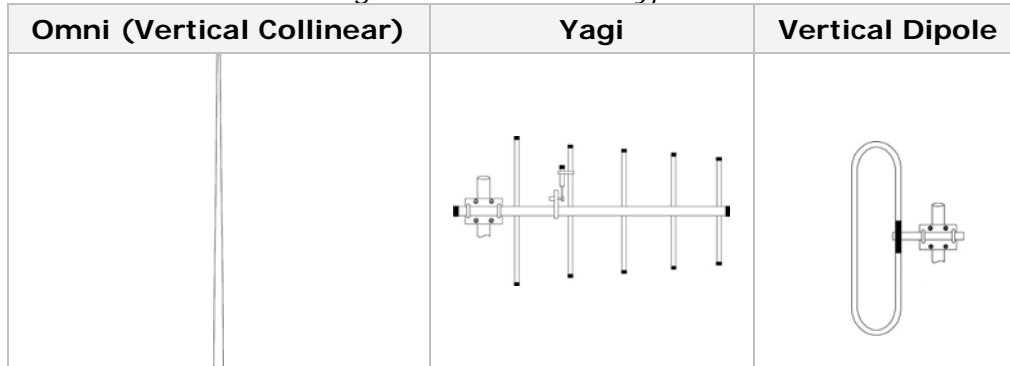
### 2.6.5  Feedline

The choice of feedline should be carefully considered.  Poor quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception.  The cable should be kept as short as possible to minimize signal loss. See Table 2.1 for a list of feedline recommendations.

*Table 2.1 - Transmission Loss (per 100 Feet)*

| Cable Type | Frequency Range | | |
|---|---|---|---|
| | VHF | UHF | 900 MHz |
| LMR-400 | 1.5 dB | 2.7 dB | 3.9 dB |
| 1/2" Heliax | 0.68 dB | 1.51 dB | 2.09 dB |
| 7/8" Heliax | 0.37 dB | 0.83 dB | 1.18 dB |
| 1 5/8" Heliax | 0.22 dB | 0.51 dB | 0.69 dB |

Outside cable connections should have a weather kit applied to each connection to prevent moisture.  Feedline connections should be routinely inspected to minimize signal loss through the connection.  A 3 dB loss in signal strength due to cable loss and/or bad connections represents a 50% reduction in signal strength.

### 2.6.6  RF Exposure Compliance Requirements

The ViPR radio is intended for use in the Industrial Monitoring and Control and SCADA markets. The ViPR unit must be professionally installed and must ensure a minimum separation distance listed in the table below between the radiating structure and any person.  An antenna mounted on a pole or tower is the typical installation and in rare instances, a 1/2-wave whip antenna is used.

*Table 2.2 – RF Exposure Compliance Minimum Safety Distances*

|  | Antenna Gain | | |
|---|---|---|---|
|  | **5 dBi** | **10 dBi** | **15 dBi** |
| Min Safety Distance (VHF @ max power) | 123cm | 218.8cm | 389cm |
| Min Safety Distance (UHF @ max power) | 105.7cm | 188cm | 334.4cm |
| Min Safety Distance (900 MHz @ max power) | 63.8cm | 115 cm | 201.7 cm |

**Note: It is the responsibility of the user to guarantee compliance with the FCC MPE regulations when operating this device in a way other than described above.**

The ViPR radio uses a low power radio frequency transmitter. The concentrated energy from an antenna may pose a health hazard. People should not be in front of the antenna when the transmitter is operating.

**RF Exposure**

The installer of this equipment must ensure the antenna is located or pointed such that it does not emit an RF field in excess of Health Canada limits for the general population. Recommended safety guidelines for the human exposure to radio frequency electromagnetic energy are contained in the Canadian Safety Code 6 (available from Health Canada) and the Federal Communications Commission (FCC) Bulletin 65.

Any changes or modifications not expressly approved by the party responsible for compliance (in the country where used) could void the user's authority to operate the equipment.

## 2.7   TERRAIN AND SIGNAL STRENGTH

A line of sight path between stations is highly desirable and provides the most reliable communications link in all cases.  A line of sight path can often be achieved by mounting each station antenna on a tower or other elevated structure that raises it high enough to clear surrounding terrain and other obstructions.

The requirement for a clear transmission path depends on the distance to be covered by the system.  If the system is to cover a limited distance, say 3-5 miles, then some obstructions in the transmission path may be tolerable.  For longer-range systems, any obstruction could compromise the performance of the system, or block transmission entirely.

The signal strength (RSSI) at the receiver must exceed the receiver sensitivity by an amount known as the fade margin to provide reliable operation under various conditions. Fade margin (expressed in dB) is the maximum tolerable reduction in received signal strength, which still provides an acceptable signal quality.  This compensates for reduced signal strength due to multi-path, slight antenna movement or changing atmospheric losses.  CalAmp recommends a 30 dB fade margin for most projects.  Table 2.3 shows the RSSI versus Reliability.

*Table 2.3 RSSI Reliability*

| RSSI | Reliability |
|---|---|
| **-100 dBm** | Approximately 50% reliability. Fading may cause frequent data loss. |
| **-90 dBm** | Approximately 90% reliability. Fading will cause occasional data loss. |
| **-80 dBm** | Approximately 99% reliability. Reasonable tolerance to most fading. |
| **-70 dBm** | Approximately 99.9% reliability with high tolerance to fading. |

## 2.8   RADIO INTERFERENCE

Interference is possible in any radio system.  However, since the ViPR is designed for use in a licensed system, interference is less likely because geographic location and existing operating frequencies are normally taken into account when allocating frequencies.

The risk of interference can be further reduced through prudent system design and configuration.  Allow adequate separation between frequencies and radio systems. Keep the following points in mind when setting up your radio system.

a.  Systems installed in lightly populated areas are least likely to encounter interference, while those in urban and suburban areas are more likely to be affected by other devices.

b.  Directional antennas should be used at the remote end of the link.  They confine the transmission and reception pattern to a comparatively narrow beam, which minimizes interference to and from stations located outside the pattern.

c.  If interference is suspected from another system, it may be helpful to use antenna polarization opposite to the interfering system's antennas.  An additional 20 dB (or more) of attenuation to interference can be achieved by using opposite antenna polarization.

d.  Check with your CalAmp sales representative or CalAmp Technical Services for additional options.  The Technical Services group has qualified personnel to help resolve your RF issues.

## 2.9   IP FORWARDING MODES

### 2.9.1  Bridge Mode

Bridge mode requires less setup than Router mode.  In Bridge mode, the IP Router does not contain IP/Network properties accessible through the network; they are transparent to the network.  Only the PC Server and the RTU Client's Network properties need configuration. The Server's Gateway will direct the Server to all remote Clients on the network.  The PC Server will broadcast to all the RTU Clients bridged to the PC Server.  Bridge mode may be used when all devices are located on the same Local Area Network (LAN). Figure 2.5 shows a ViPR Bridge Mode configuration.
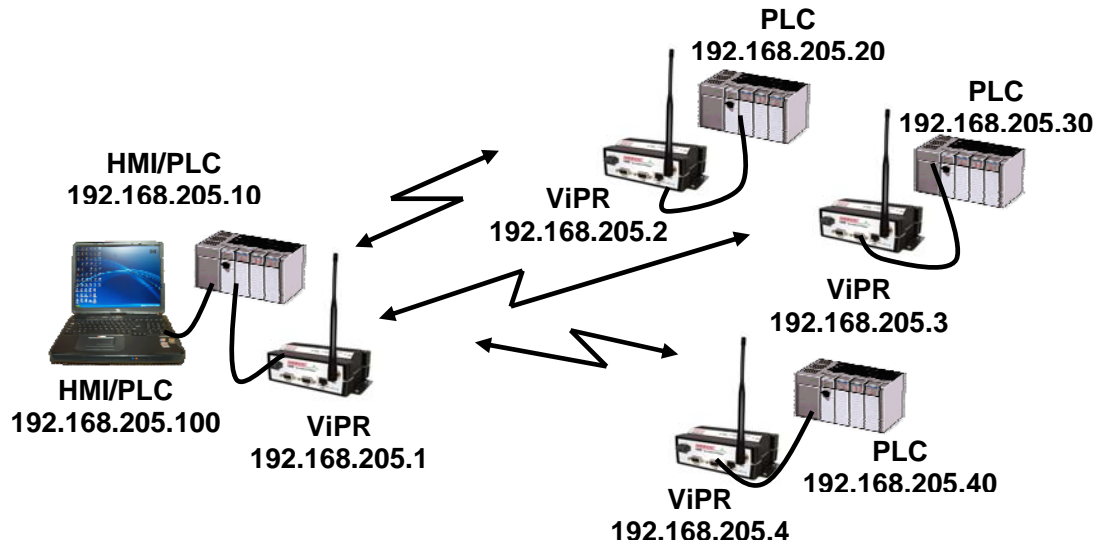
*Figure 2.5 ViPR Bridge Mode Configuration*

### 2.9.2  Router Mode

Router mode provides network configuration flexibility and adds RF diagnostics capability for ViPR wireless modems.  Router mode also allows greater flexibility in using different protocols.  Diagnostics can be retrieved through the Ethernet port of the ViPR.  This configuration is recommended for users who have IT/Network support readily available to them and the authorization required to make changes in the network.  Router mode requires set up of IP/Ethernet and Serial IP addresses. Figure 2.6 shows a ViPR Router Mode configuration.
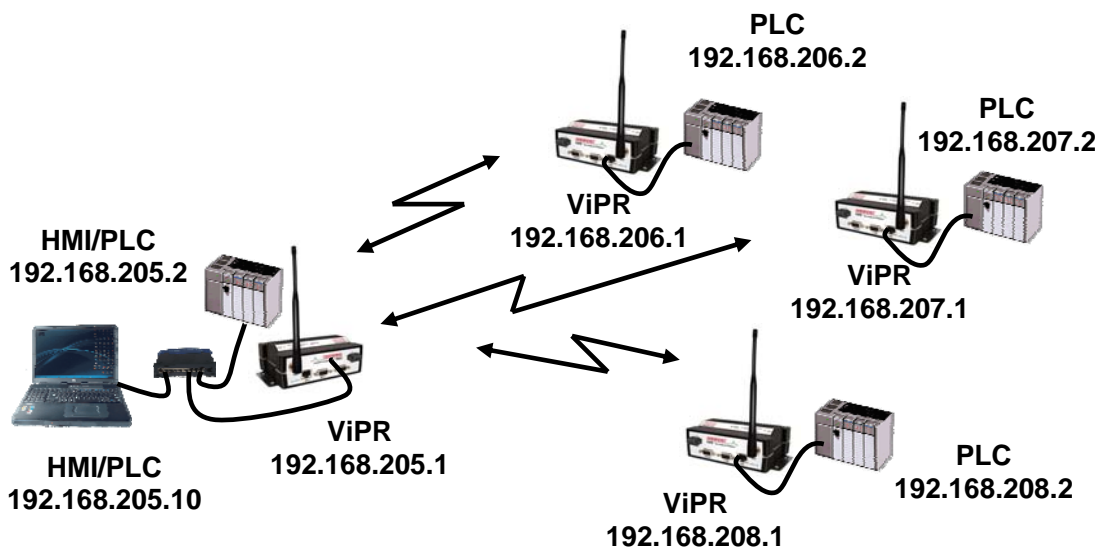


*Figure 2.6 ViPR Router Mode Configuration*

### 2.10 CHOOSING AN IP ADDRESSING SCHEME

All Ethernet capable devices, or hosts, have at least one IP address and subnet mask assigned to it.  The IP address identifies that specific device and the subnet mask tells the device which other IP addresses it can directly communicate with.

The ViPR ships from the factory with a default Ethernet IP address of 192.168.205.1 and a subnet mask of 255.255.255.0.  (This is sometimes written in shorthand notation as: 192.168.205.1/24 since the subnet mask 255.255.255.0 contains 24 ones then 8 zeros when it is converted to binary.)

The default subnet of the ViPR consists of addresses from 192.168.205.0 to 192.168.205.255.  The first and last IP address of each subnet is reserved, no matter what the subnet size is.  The first IP address in the subnet is the Network ID.  The last IP address in the subnet is the Broadcast Address.  In the ViPR's example, IP addresses 192.168.205.0 and 192.168.205.255 are reserved, and any address(es) from 192.168.205.1 to 192.168.205.254 are valid and may be assigned to a host.

When any host needs to communicate with another device that is not within the same local area network it will first send the data packet to the gateway or router.  The gateway or router will forward the packet to the desired location.  Often times a packet will pass through several gateways or routers to get to its final destination.

### 2.10.1 Bridge Mode

In Bridge mode each ViPR has only one IP address.  Each ViPR in the network must be on the same network and have the same subnet mask.  It is recommended that each ViPR be assigned a unique IP address.

**Bridge Mode Example 1:**
>    *Ethernet Subnet Mask for all units:  255.255.255.0*
>
>    | | |
>    |---|---|
>    | *Network ID:* | *192.168.205.0* |
>    | *ViPR #1:* | *192.168.205.1 / 24* |
>    | *ViPR #2:* | *192.168.205.2 / 24* |
>    | *ViPR #3:* | *192.168.205.3 / 24* |
>    | *PLC/RTU #1:* | *192.168.205.4 / 24* |
>    | *PLC/RTU #2:* | *192.168.205.5 / 24* |
>    | *Computer #1:* | *192.168.205.6 / 24* |
>    | *...* | |
>    | *PLC/RTU #100:* | *192.168.205.253 / 24* |
>    | *ViPR #100:* | *192.168.205.254 / 24* |
>    | *Broadcast Address:* | *192.168.205.255* |
>
>    *All units are on the 192.168.205.0 network and all units have the same subnet mask. Because of this, all units can communicate directly with each other. There are 254 valid IP addresses that may be assigned to hosts on the network.*

**Bridge Mode Example 2:**
   *Ethernet Subnet Mask for all units: 255.255.0.0*

   *Network ID:            172.20.0.0*
   *Computer #1:           172.20.0.1 / 16*
   *ViPR #1:               172.20.0.2 / 16*
   *ViPR #2:               172.20.0.3 / 16*
   *...*
   *ViPR #105:             172.20.136.125 / 16*
   *Computer #302:         172.20.138.205 / 16*
   *...*
   *PLC/RTU #500:          172.20.255.253 / 16*
   *Computer #500:         172.20.255.254 / 16*
   *Broadcast Address:     172.20.255.255*

   *This example is similar to Bridge Mode Example #1 except there are 65534 valid IP
   addresses that may be assigned to hosts on the network.*

### 2.10.2 Router Mode

In Router mode, each ViPR has two IP addresses, an Ethernet IP address and an RF IP
Address.  By default each ViPR will have the same Ethernet IP Address (192.168.205.1) and
will have a unique RF IP address which is assigned at the factory.  The RF IP address will
always have the form 10.x.y.z where x, y, and z is based on the last 6 digits of the unit's
MAC address.

In Router mode, each ViPR must have its Ethernet IP Address on a **<u>unique</u>** network.  In
addition, all ViPRs must have their RF IP addresses on the **<u>same</u>** network.  The default
network is 10.0.0.0/8.  **For consistent and reliable communication, the RF network
should not overlap or contain any of the IP Addresses in the Ethernet networks.**

**Router Mode Example 1:**
   *Ethernet Subnet Mask: May vary from ViPR to ViPR.*
   *RF Subnet Mask for all units: 255.0.0.0*

   *ViPR #1 Eth IP Address: 192.168.205.1 / 24        RF IP Address: 10.11.12.25 / 8*
   *   Computer #1:         192.168.205.2 / 24*

   *ViPR #2 Eth IP Address: 192.168.206.1 / 24        RF IP Address: 10.9.7.251 / 8*
   *   PLC #2:              192.168.206.2 / 24*
   *   Computer #2:         192.168.206.3 / 24*

   *ViPR #3 Eth IP Address: 192.168.207.1 / 24        RF IP Address: 10.8.0.52 / 8*
   *   PLC #3:              192.168.207.2 / 24*
   *   Computer #3:         192.168.207.3 / 24*

   *ViPR #4 Eth IP Address: 172.21.51.105 / 16        RF IP Address: 10.0.1.11 / 8*
   *   PLC #4:              172.21.51.106 / 16*

   *In this example, each ViPR has an Ethernet IP address on a unique network. For ViPRs
   #1, #2, and #3, each network connected to their local Ethernet ports has 254 valid IP
   addresses that may be assigned to other hosts.  The network connected to ViPR #4's
   local Ethernet port has 65534 valid IP addresses.*

*Note 1: All the ViPRs' RF IP addresses are on the same network. Because they are using the 10.0.0.0/8 network, all ViPRs may use the default RF IP address programmed by the factory.*

*Note 2: All the ViPR Ethernet IP addresses are on different networks.*

*Note 3: Computers, PLCs, RTUs, or other Ethernet capable devices can be connected up to each ViPR's local Ethernet interface. That device must be set with an IP address on the same network as the Ethernet interface of the ViPR it is connected with.*

**Router Mode Example 2:**
*Ethernet Subnet Mask for all units: 255.255.255.240*
*RF Subnet Mask for all units:* **255.255.0.0**

*ViPR #1 Eth IP Address: 10.200.1.1 / 28*      *RF IP Address: 10.0.0.1 / 16*
*ViPR #2 Eth IP Address: 10.200.1.17 / 28*     *RF IP Address: 10.0.0.2 / 16*
*ViPR #3 Eth IP Address: 10.200.1.33 / 28*     *RF IP Address: 10.0.0.3 / 16*
*ViPR #4 Eth IP Address: 10.200.1.49 / 28*     *RF IP Address: 10.0.0.4 / 16*
*...*
*ViPR #177 Eth IP Address: 10.200.12.1 / 28*    *RF IP Address: 10.0.0.177 / 16*
*ViPR #178 Eth IP Address: 10.200.12.17 / 28*   *RF IP Address: 10.0.0.178 / 16*
*...*

*Each ViPR has an Ethernet IP address on a unique network.*

*In this example, each network connected to the ViPR's local Ethernet port has 14 valid IP addresses that may used for the ViPR, PLCs, RTUs, computers, or other Ethernet equipment that may be connected.*

*The subnet mask of the RF IP addresses has been changed to ensure that the RF IP network does not overlap any of the Ethernet networks. In this scenario, the RF IP addresses must be manually programmed to ensure that every ViPR has an RF IP address in the network and that no RF IP address is used twice.*

## 3  DATARADIO VIPR QUICK START

### 3.1  SETUP AND CONFIGURATION

It is easy to set up a ViPR network to verify basic unit operation and experiment with network designs and configurations.

It is important to use a network IP subnet address different from others currently in use in your test area.  This will eliminate unnecessary disruption of traffic on the existing network while you become familiar with the ViPR.

### 3.2  INSTALL THE ANTENNA

An RX/TX antenna is required for basic operation. For demo units only, connect the antenna as shown in Figure 3.1 to provide stable radio communications between demo devices.



20 dB, 5 watt max, attenuator
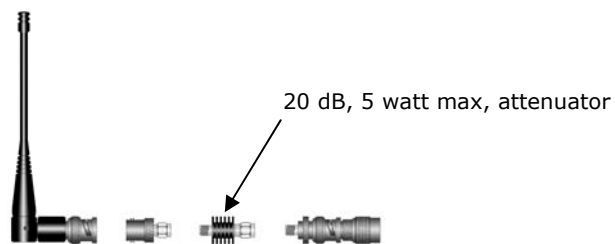
*Figure 3.1 -Demo Antenna Assembly*

**Note:**
It is important to use attenuation between all demo units in the test network to reduce the amount of signal strength in the test environment.

### 3.3  PC LAN SETUP

On a PC running MS-Windows with an existing LAN connection, connect to the Ethernet input of the ViPR and complete the steps in section 3.3.1

### 3.3.1  Front Panel Connections

Front panel connections include: (For Dual-port ViPR connections see Section 1.3.6.)

(1) RJ-45 10 BaseT Ethernet Connection
(1) 50-ohm TNC female transmit antenna connector
(1) 50-ohm SMA female receive antenna connector (Dual-port models only)
(1) Right-angle power connector (10-30 VDC)
(2) DE-9F RS-232 ports
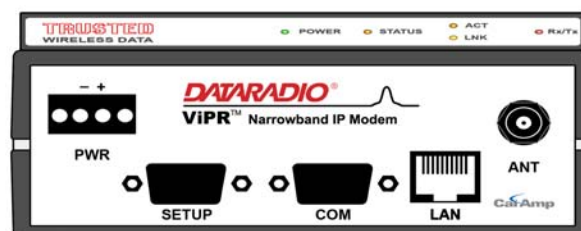


*Figure 3.2 Front Panel (Standard model shown)*

STEP 1:    From the Start menu on your PC, select Settings > Control Panel > Network Connections

STEP 2:    Right click the Local Area Connection icon to open the Properties box.
Scroll through the list and highlight Internet Protocol (TCP/IP).
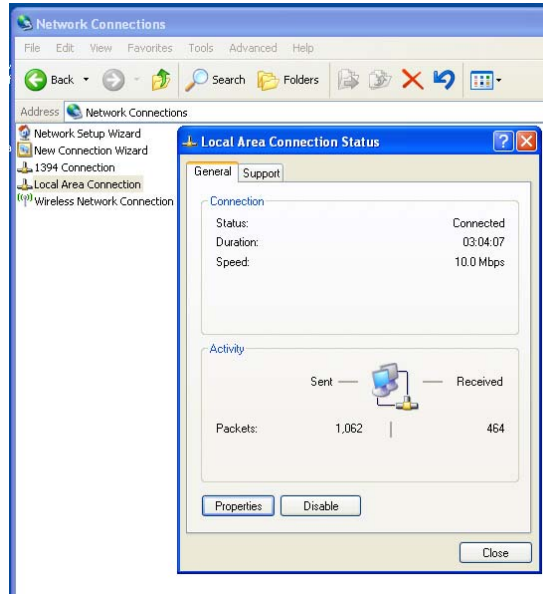Click Properties to open the TCP/IP Properties box.



*Figure 3.4 PC LAN Setup*

STEP 3:    Select Use the Following IP Address and enter the following values:

IP Address:       192.168.205.254
Subnet Mask:      255.255.255.0
Default Gateway: (leave empty)
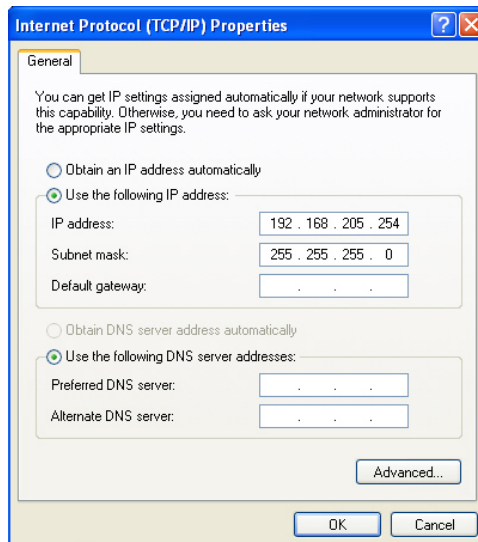


*Figure 3.5 PC LAN Setup: Step 3*

STEP 4: Click OK to apply your changes and complete the connection process. Some Operating systems may require a reboot to complete the connection process.

## 3.4 MEASURE AND CONNECT PRIMARY POWER

Primary power for the ViPR must be within 10-30 VDC and be capable of providing a minimum of 10 watt supply for Tx @ 1W, 40 watt supply for Tx @ 5W, or 60 watt supply for Tx @ 10 W. (In ViPR Demo Kits, a power connector with screw-terminals is provided with each unit.) Observe proper polarity when connecting the cables to the Power Supply. (White wire must be connected to red wire.)

## 3.5 CONNECT VIPR TO PROGRAMMING PC

Connect a PC's Ethernet port to the LAN port using a CAT 5 Ethernet cable.  The LINK LED should light.



*Figure 3.6 Connect Power and Ethernet cable to the ViPR.*

On your Internet browser address line, type the factory-default IP address: 192.168.205.1. Press Enter to open the Network Password screen.

### 3.5.1 Initial Installation Login

For an initial installation, enter any User Name of 1 to 15 characters and the default Password ADMINISTRATOR (upper case letters).  Click OK.  The web interface WELCOME screen opens. Once setup is completed, change the ViPR login password (See Section 8.1).

## 3.6 CONFIGURE YOUR VIPR USING THE SETUP WIZARD

ViPR units are programmed using the web interface.  Log into the ViPR web interface as described in Initial Installation Login.  Follow the instructions below to configure the ViPR using the setup wizard.  All units are factory programmed with an IP address of 192.168.205.1.  Repeat these steps to program additional ViPR units.

STEP 1: Station Name: Assign a unique Station Name
        IP Forwarding Mode: Select Bridge (Mode)
        Relay Point:  Select No
        Access Point:  Select No
        Click "Apply" Click "Next"

*Figure 3.7 Using the Setup Wizard: Step 1*

STEP 2:     Each ViPR is programmed with these defaults:
            IP Address:  192.168.205.1
            Network Mask:  255.255.255.0
            Default Gateway:  0.0.0.0



*Figure 3.8 Using the Setup Wizard: Step 2*

To monitor or change configuration remotely, each unit requires a unique IP Address. When configuring more than one unit, be sure to increment IP addresses. Click "Apply".  Click "Next".

STEP 3:        Verify FCC license before completing this step.
               Channel ID:  Enter 1 for Channel ID
               Channel Type:  Select Channel Type
               RX Frequency:  Enter RX Frequency
               TX Frequency:  Enter TX Frequency
               TX Power:  Enter 5 W
               Set Active Channel:  Select Yes
               Click "Apply" Click "Next"



*Figure 3.9 Using the Setup Wizard: Step 3*

STEP 4:    The ViPR uses AES-128 bit encryption to protect your data from
           intrusion. Use of encryption is optional but we strongly recommend
           it for network configuration.  The encryption phrase/key must be common
           to all units in a network.

           **Encryption Disabled**
           Encryption:  Click Disabled
           Click "Apply". Click "Next".

           **Encryption Enabled**
           Encryption:  Click Enabled
           Encryption Pass Phrase:  Enter an encryption phrase
           Note this phrase for reference later
           Click "Apply". Click "Next".

*Figure 3.10 Using the Setup Wizard: Step 4*

STEP 5:   Click "Done" before completing the remaining steps.
Note: If the "Done" button is not clicked on new units, the units will not transmit.

To save the network configuration parameters of your ViPR, click the "Save Config" command button. You will see a green success icon on the bottom left of the page when save is complete.



*Figure 3.11 Using the Setup Wizard: Step 5*

If you have changed any parameters marked with a yellow "!" icon, you must cycle power to the unit using the "Reset Unit" button.

Your unit is now functioning in Bridge Mode.

## 3.7   CHECK FOR NORMAL OPERATION

To simulate data traffic over the radio network, connect a PC or LAN to the Ethernet port of the ViPR and PING each unit in the network multiple times.  Refer to section 10.1 to utilize the ViPR PING utility.

## 4    VIPR WEB MANAGEMENT

A built-in web server makes configuration and status monitoring possible from any browser-equipped computer, either locally or remotely.  Status, configuration, and online help are available without requiring special client software.  Setup is password-protected to avoid tampering or unauthorized changes.

Both the configuration parameters and operating firmware can be updated remotely, even over the RF network itself, using the standard FTP protocol.

### 4.1    NAVIGATING THE NETWORK MANAGEMENT SYSTEM

The Web Interface is subdivided in two frames:  the left frame allows the user to navigate the main menu, while the right main frame displays the selected page.
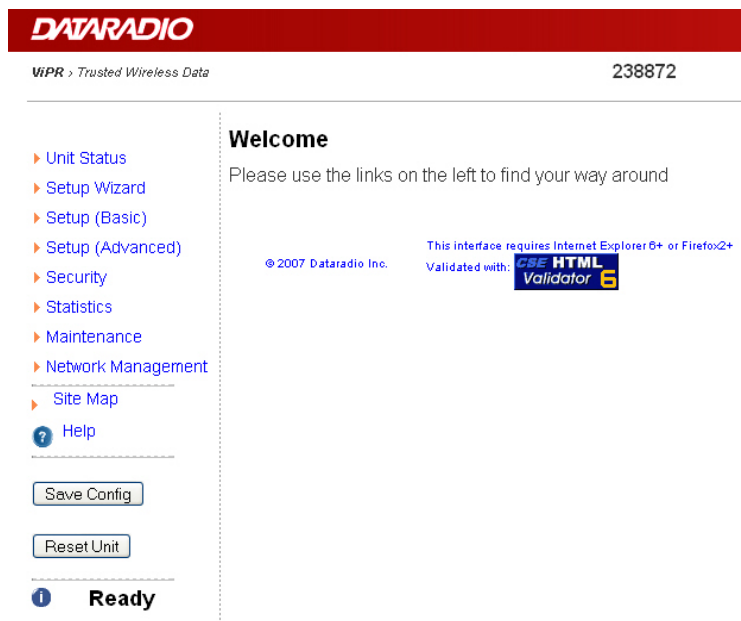


*Figure 4.1 ViPR Welcome Screen*

### 4.2    MAIN MENU

VIPR Main menu grants the user access to Unit Status, Setup Wizard, Basic and Advanced Setup, Security, Statistics, Maintenance, and Network Management.

### 4.2.1   Network Management System Commands

The remaining buttons on the Navigator frame are used to save your configurations and reset the unit.

▪   **Apply**

This command button writes to RAM.  When making an entry into a dialog box, click "Apply" when you are satisfied with the changes to temporarily apply the value(s) entered to the relevant parameter(s).  **Failure to use the "Apply" command button before leaving a web page will result in the loss of entered selections, addresses, and values.**

- **Cancel**

The "Cancel" command only affects the dialog boxes or radio buttons in the opened window.

- **Save Config**

This command button saves the ViPR parameters into flash memory.  Failure to use this command button will result in the loss of temporarily entered parameters when the unit is reset.

- **Reset Unit**

Once satisfied all parameters have been applied and saved, use the "Reset Unit" command button to make flash changes permanent.  When a unit is reset, a 20-second station reset timer counts down.  Status reports Ready when reset is complete.

## 5    UNIT STATUS

The Unit Status windows display device General and Diagnostic information.

### 5.1    UNIT IDENTIFICATION AND STATUS



*Figure 5.1 – Unit Status ⇨ General Web Page*

▪  **Banner**

The unit identification and status banner displays ViPR software revision information for the ViPR device.  Have this information available if contacting CalAmp support.
The banner should read: Dataradio ViPR FAMA UHFVHF PROD Vx.y_Rxxx, where:

| Product Name | ViPR |
|---|---|
| Protocol Name | Licensed |
| Band(s) of Operation | VHF 136-174 MHz,VHF 200 215-240 MHz |
| | UHF 406.1-512 MHz, 900 928-960 MHz |
| Production Build | Vx.y Rxxx where |
| | Vx.y is Major.minor version number, and |
| | Rxxx is Sequential Package Release Build Number |

▪  **Station Name**

Displays the name of the connected unit. Configured under Setup (Basic) ⇨ General ⇨ Station Name.

▪  **Local Time**

Displays time zone configuration using UTC time and the configured Time Zone.  An SNTP server can be specified under Setup (Advanced) ⇨ Time Source.  The time will reset to the default setting if power is cycled on the ViPR unit and no SNTP server is configured.

- **CWID**

Continuous Wave Identification - Default = Disabled
Allows the user to broadcast their FCC call sign.
CWID Call sign is the user's FCC call sign to be broadcast.
CWID Interval is the time interval in minutes that the call sign will be broadcasted.
CWID can be configured under Setup (Basic) ⇨ General.

- **IP Forwarding Mode**

Displays IP forwarding mode (Bridge or Router). The IP Forwarding Mode can be configured
under Setup (Basic) ⇨ General ⇨ IP Forwarding Mode.

- **Station relay point**

Displays if the unit is being used as a relay point (Yes or No). The Station Relay Point can be
configured under Setup (Basic) ⇨ General ⇨ Station relay point.

- **On-line diagnostics Interval**

Displays the time interval in seconds when the On-line Diagnostics will be transmitted. This
interval can be configured under Setup (Basic) ⇨ General ⇨ On-line diagnostics interval.

- **Unit Status**

Displays the status of the ViPR and reports any errors.  If you do not receive the OK
indicator (EX. Error: Power On Self Test FAILURE, Warning: Radio TX Synthesizer lock
failure N/A), use the ACKNOWLEGDE UNIT STATUS and REFRESH buttons to reset the
modem.  If the problem persists, contact CalAmp Technical Services for additional
information.

*Have the displayed Unit Status message available if contacting CalAmp support. This
information is also required if returning a unit for service under RMA.*

- **Refresh**

Button will refresh the parameters on the current page.

- **Acknowledge Unit Status**

This button allows the user to acknowledge and clear errors.

Errors remain stored, even after cycling power, to aid in troubleshooting intermittent faults.
Press the "Acknowledge Unit Status" button to return web page displays and Status LED
function to normal operation.


## 5.2  DIAGNOSTICS

ViPR units continually monitor and report on their environmental and operating conditions.

### 5.2.1  Local Diagnostics

Local Diagnostics can be accessed by loading the Unit Status ⇨ Diagnostics web page from
the ViPR.

*Figure 5.2 – Unit Status ⇨ Diagnostics Web Page*

- **Date and time**

Displays the time and date.  To set the time, an SNTP server must be setup under Setup (Advanced) ⇨ Time Source.  The SNTP server must also be accessible via the user's LAN or Internet connection.

- **Time since reset**

Displays the amount of time since the unit was last reset.  [DD,HH,MM,SS], Days, Hours, Minutes, Seconds

- **Modem Firmware Version**

Displays the modem firmware version of the unit.

- **Radio Firmware Version**

Displays the radio firmware version of the unit.

- **RSSI from RF-MAC**

Displays the Received Signal Strength Indication (RSSI) from the unit with the MAC address displayed.  The RSSI displayed range is from approximately -50 dBm to -120 dBm.  At signal strengths greater than -50 dBm, the radio will still operate but will not display an accurate RSSI value.

- **DC Input Voltage**

Displays the DC Input Voltage for the unit.

- **TX Frequency**

Displays the current operating transmit frequency for the active channel.  Setup (Basic) ⇨ Channel Table ⇨ TX

- **RX Frequency**

Displays the current operating receiver frequency for the active channel.  Setup (Basic) ⇨ Channel Table ⇨ RX

- **Transmit Power Level**

Displays the programmed power level for the active channel.  Setup (Basic) ⇨ Channel Table ⇨ PA Power

- **Transceiver Temperature**

Displays the transceiver's internal temperature in Celsius or Fahrenheit.  Setup (Advanced) ⇨ User Settings

- **PA Forward Power**

Displays the actual measured forward power of the transmitter.  If the measured forward power drops 1 dB or more below the user configured power level, this line will report "(fault)".  When the forward power is within range, this line will report "(normal)".  The ViPR radio can be configured to send an SNMP trap (or alarm) if the Forward Power goes into a "fault" state.

- **PA Reverse Power**

Displays the actual measured reverse power of the transmitter.  If the measured reverse power increases to within 3 dB of the user configured power level, this line will report "(fault)".  When the reverse power is within range, this line will report "(normal)".  The ViPR radio can be configured to send an SNMP trap if the Reverse Power goes into a "fault" state.

- **Power state**

Indicates if the unit is running at full power or at a reduced power. The TX power will foldback when the temperature is too hot or the Power Amp (PA) current is too high. In extreme cases of high temperature or high current, the ViPR transmitter will shutdown completely to protect the radio from permanent damage.

When the ViPR is at Full power this line will report "(normal").  If the ViPR's PA goes into Foldback or Shutdown this line will report "(fault)".  The ViPR radio can be configured to send an SNMP trap if the Power State reports a fault.

- **Refresh**

This button will refresh the current page's parameters.

### 5.2.2  Online Diagnostics

Transmission of online diagnostics may be enabled or disabled at any station or stations without affecting their ability to communicate with other stations. Online Diagnostics can be sent anywhere, including being back-hauled. Back hauling adds to the network traffic flow and must be taken into account when designing a network. If a return flow is necessary, it needs to be reduced substantially to have a minimal effect on the network.

ViPR can support up to 4 diagnostics socket connections at once. This may be used, for instance, to carry out monitoring at a main office and at up to three separate field locations.

It is also possible one of the four connections use a serial port instead by enabling it on the ViPR's web browser interface.

▪ **Output Format**

The online diagnostic output is man/machine readable, ASCII, comma-delimited format. Any reader program used (or written) must decode the VERSION FIELD and check for type 1 as more types may be released in the future.

From a Command Prompt window, type *telnet nnn.nnn.nnn.nnn 6272* and the unit's online diagnostic output will display on the screen (where nnn.nnn.nnn.nnn is your unit's IP address in dot decimal format). Note: no overhead is generated in the ViPR unit if no online diagnostic connection is actually made.

```
      Host       Ver   #   Int Flags   Source          Destination       A     B     C     D     E     F   G
[00:00:01:2A],    1,  11, 300, 0x01, [192.168.206.5], [192.168.43.43],  35,  122,  157,    0,   50,    1,  10,
[00:00:01:2A],    1,  11, 300, 0x01, [192.168.98.98], [192.168.43.43],  32,   75,  134,  125,   51,    1,   0,
[00:00:01:2A],    1,  11, 300, 0x01, [192.168.205.1], [192.168.2.2],    36,   62,  178,    0,   52,    2,  50,
[00:00:01:2A],    1,  11, 300, 0x01, [192.168.43.43], [192.168.2.2],    36,   51,   28,   27,   52,    2,   3,
[00:00:01:2A],    1,  11, 300, 0x01, [192.168.205.1], [192.168.2.2],    36,   62,  146,    0,   52,    2,  50,
```

*Figure 5.3 – Diagnostic output sample*

*Table 5.1 – Online Diagnostics Output Sample Definitions*

| | |
|---|---|
| Host | MAC address of the station where diagnostic measurements are being collected. The host will collect diagnostic message from itself and all remote units with IPSD enabled. IPSD can be enabled/disabled under Setup (Advanced) ⇨ IP Services. |
| Ver | Version of the online diagnostics. Different versions may have different parameters. This document describes Version 1. |
| # | Number of items that follow in the online diagnostic message. |
| Period | PERIOD (Seconds). Specifies the time between the generation of online diagnostic messages from the source station. |
| Flags | Online Diagnostic Flags. (CalAmp specific) |
| Source | Source Address. In Bridge mode, this address displays the MAC address of the source ViPR. In Router mode, this address displays the IP Address of the source ViPR. The source is the ViPR station generating the diagnostic message. This is also the source station from the point of view of the RSSI measurements |
| Destination | Destination Address. In Bridge Mode, this address displays the MAC address of the destination ViPR. In Router Mode, this address displays the IP Address of the destination ViPR. This is the destination station from the point of view of RSSI measurements. |
| A | Temperature of the source ViPR in Celsius or Fahrenheit. Temperature units can be configured on the source ViPR under Setup (Advanced) User ⇨ Settings. |
| B | Source supply voltage in excess of 8 volts, shown in 10ths of volts. Supply voltage = (ODM_reading / 10) + 8 A reading of 35 shall be interpreted as 11.5V. |

| | |
|---|---|
| C | RSSI measured at the source ViPR for the last message received from the destination ViPR. This is also referred to as the Local RSSI. The value displayed shall be interpreted as shown in Table 5.2. |
| D | RSSI measured at the destination ViPR for the last message received from the source ViPR.  This is also referred to as the Remote RSSI.  The value displayed shall be interpreted as shown in Table 5.2. |
| E | Radio/antenna forward power measured in 10ths of watts at the source ViPR.  A value of 51 shall be interpreted as 5.1W. |
| F | Radio/antenna reverse power measured in 10ths of watts at the source ViPR.  A value of 2 shall be interpreted as 0.2W. |
| G | PER measured at the source. This is calculated as the percentage of packets rejected due to an invalid header/checksum over the total number of packets received. To fit a small unsigned integer, this value is multiplied by 1000 and its max value limited at 255.  A reading of 2 means 0.002% of packets were rejected. |

*Table 5.2 – Online Diagnostics RSSI Display*

| VALUE | RSSI | NOTES |
|---|---|---|
| 0 | NA | The RSSI Value is not Available |
| 1 | $\geq$ -60.25 dBm | The RSSI Value is greater than –60.25 dBm |
| 20 | -65.00 dBm | |
| 255 | $\leq$ -123.75 dBm | RSSI is less than –123.75 dBm |
| X | | RSSI = -60 – (X * 0.25), for X not equal to 0 |

## 6    SETUP (BASIC)

### 6.1    GENERAL SETUP

**General Setup**

| | |
|---|---|
| **Station Name** | Percy |
| **IP Forwarding Mode** ⚠ | ⦿ Bridge  ○ Router |
| **Bridge Forwarding** | ○ Everything<br>⦿ IP and ARP types only |
| **Note: when selecting Router forwarding mode,<br>all relevant IP settings must be configured** | |
| **Relay Point** | ○ Yes  ⦿ No |
| **Access Point** ⚠ | ○ Yes  ⦿ No |
| **CWID** | ○ Enabled  ⦿ Disabled |
| **CWID Call sign** | |
| **CWID Interval** | 30      minutes |
| **On-line diagnostics Interval** | 300     seconds |
| **Unit Automatic Reset** | ○ Enabled  ⦿ Disabled |
| **Unit Reset Interval** | 1440    minutes |

Apply   Cancel

If you "Apply" changes to any parameters marked ⚠ you will need to do a "Save Config" and a "Reset Unit".

*Figure 6.1 Setup (Basic)*

▪   **Station Name**

Station name identifier – Enter a string up to forty characters in length.

▪   **IP Forwarding Mode**

Bridge / Router, Default = Bridge mode

Bridge Mode:  Bridge mode is the simplest configuration for the ViPR radio and should only be used for small networks.  In Bridge mode, all the ViPRs and all the Hosts/PCs connected to the ViPRs must be on the same IP subnet.  Figure 6.2 illustrates ViPR bridge mode configuration.  Ethernet messages are sent over the air as broadcast messages.  All the other ViPRs in the network will receive the message and relay it to their local area network. If the Com Ports are configured for Serial/RF Bridge mode on all the ViPRs in the network, then each message that is transmitted into one ViPR's Com Port will be received by all the other ViPRs in the network and transmitted out their Com Ports.

Note: This configuration can be substituted for a traditional serial RS232 radio system configuration.  The ViPR in bridge mode is a drop in replacement for a serial radio.

**Bridge Mode**
**Subnet 192.168.205.0**

**PLC**
**192.168.205.20**

**PLC**
**192.168.205.30**

**HMI/PLC**
**192.168.205.10**

**ViPR**
**192.168.205.2**

**ViPR**
**192.168.205.3**

**HMI/PLC**
**192.168.205.10**

**ViPR**
**192.168.205.1**

**PLC**
**192.168.205.4**

**ViPR**
**192.168.205.4**

*Figure 6.2 ViPR Bridge Mode Configuration.*

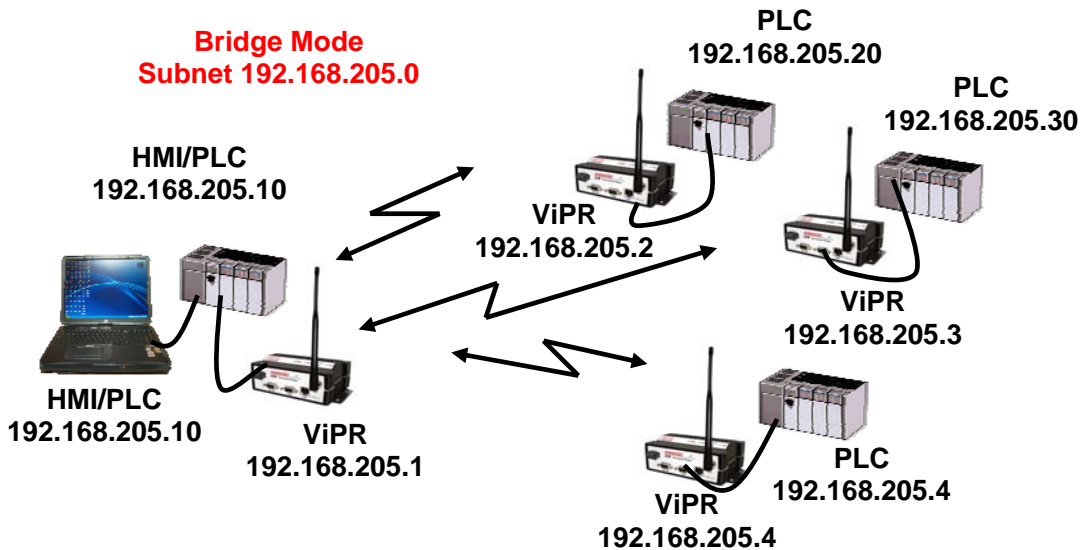**Router Mode:**  Router mode offers several advantages over Bridge mode and can be used for simple or complex networks.  In Router mode, each ViPR must be configured for a unique IP subnet.  Figure 6.3 represents a ViPR router mode configuration. Ethernet messages will be routed to the intended recipient ViPR and will be discarded by other ViPRs that overhear the message that was not intended for them.  The user can specify the route a multiple hop message will travel and thus can channel the traffic throughout the ViPR network to give a more reliable connection or perhaps relieve traffic congestion on a large network.  In Router mode, the user has access to the RSSI for each ViPR that is one hop away.  In Router mode, several retry mechanisms can be enabled which often yields a more stable and reliable link.  (See section 12, Network Optimization, for more details.)  Also, the user will have access to more advanced IP configuration settings such as Network Address Translation (NAT).

**Router Mode, Different Subnets**
**192.168.205.0, 192.168.206.0,**
**192.168.207.0, 192.168.208.0**

**PLC**
**192.168.206.2**

**PLC**
**192.168.207.2**

**HMI/PLC**
**192.168.205.2**

**ViPR**
**192.168.206.1**

**ViPR**
**192.168.207.1**

**HMI/PLC**
**192.168.205.100**

**ViPR**
**192.168.205.1**

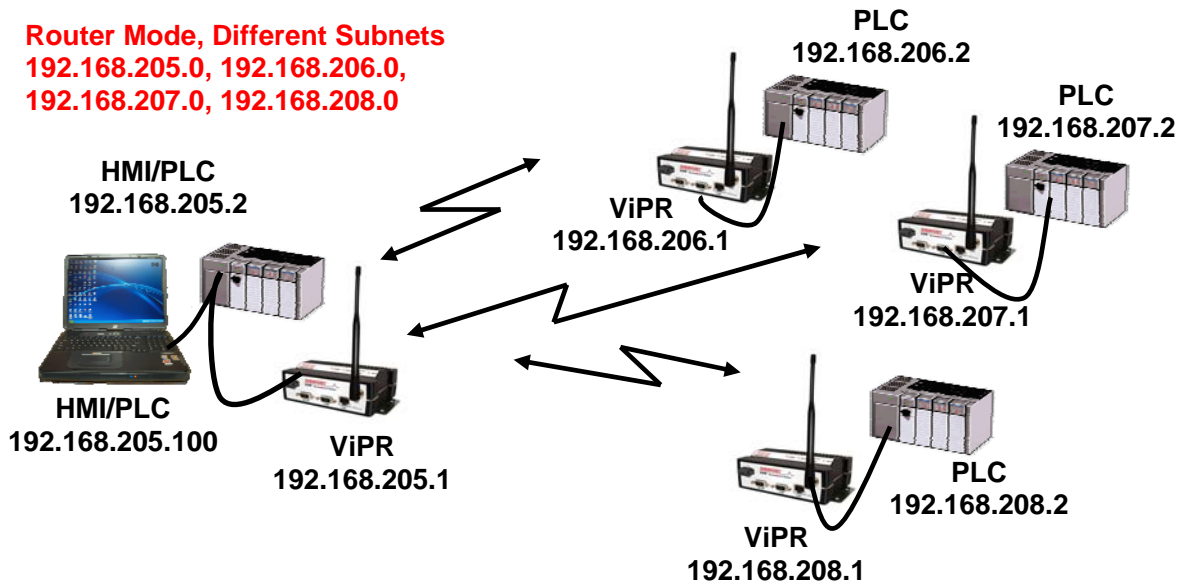**PLC**
**192.168.208.2**

**ViPR**
**192.168.208.1**

*Figure 6.3 ViPR Router Mode Configuration*

- **Bridge Forwarding**

Everything / IP and ARP types only
By default, the ViPR only forwards IP and ARP packets (Ethernet II types: 0x0800, 0x0806).
By selecting the "Everything" setting, the ViPR will forward all 802.3 Ethernet II packet
types.  Use this setting to transport protocols such as IPX, 802.1Q, etc. Note that this option
is not available in Router mode because the ViPR will automatically forward all packets per
its routing table.

- **Relay Point**

Yes/No (default)
For units that are spread over multiple RF coverage areas, the user needs to identify the
ones that will form the backbone between the coverage areas so that any unit can talk to
any other unit in the network regardless of their locations.  These units are called Relay
Point units.  A Relay Point provides store and forward repeating for all traffic in Bridge mode
and for broadcast packets in Router mode.  Selecting this parameter will force the unit to
repeat all necessary information from one coverage area to the next.  Multiple Relay Points
can be configured in parallel to provide redundancy in the network; however, having
redundant relay points may slow the flow of traffic.

- **Access Point**

Yes/No (default)
This is the default gateway (WAN access) of a ViPR network. *One, and only one, access
point may be defined for each ViPR network*.  All ViPRs in the network will set their default
route to point towards the Access Point.  (An Access Point can only be configured in Router
mode.)

- **CWID**

Enabled/Disabled (default).
Enabling CWID allows the unit to broadcast the FCC Call Sign in Morse code at a certain
interval.

CWID Call sign is the FCC Call sign to be broadcast.
CWID Interval is the time interval after which the call sign will be broadcast.

- **On-line diagnostics Interval**

The on-line diagnostic interval is the time interval in which the unit will broadcast the
diagnostic string.  Please refer to section 5.2.2 for detailed information about the format of
the diagnostic string.

- **Unit Automatic Reset**

Enabling this option will make the radio completely shut down and restart after a set period
of time.  The time between resets (in minutes) can be specified in the Unit Reset Interval
field.

## 6.2  IP SETTINGS

**IP Settings**

| Ethernet Interface | | |
|---|---|---|
| **DHCP Client** ⚠ | ⊙Static  ○Dynamic | |
| **IP Address** ⚠ | 192.168.205.1 | (default: 192.168.205.1) |
| **Netmask** ⚠ | 255.255.255.0 | (default: 255.255.255.0) |
| **DHCP Server** ⚠ | ⊙Enabled  ○Disabled | |
| **Start Address** ⚠ | 192.168.205.2 | |
| **Number of leases** ⚠ | 10 | |
| **Lease duration** ⚠ | 0    Minutes (0:Infinite) | |
| **Gateway** ⚠ | 0.0.0.0 | |
| **MTU** ⚠ | 1500 | (default: 1500) |
| **MAC Address** | 00:0A:99:00:0E:81 | |

| RF Interface | | |
|---|---|---|
| **IP Address** ⚠ | 10.0.14.129 | (default: 10.0.14.129) |
| **Netmask** ⚠ | 255.0.0.0 | (default: 255.0.0.0) |
| **MTU** ⚠ | 1500  bytes | (default: 1500 bytes) |
| **MAC Address** ⚠ | 00:0E:81 | (default: 00:0E:81) |

| **Default Gateway** | 0.0.0.0 | |

[Apply]  [Cancel]

If you "Apply" changes to any parameters marked ⚠ you will need to do a "Save Config" and a "Reset Unit".

*Figure 6.4 – Setup (Basic) ⇨ IP Settings Web Page*

### 6.2.1  Ethernet Interface

▪ **DHCP Client**

DHCP Client: Static (default) or Dynamic.  When the unit is in Router mode, Static mode allows the user to set the IP address of the unit.  Dynamic mode will set the unit to be a DHCP client, which will allow the unit to accept an IP address from an external DHCP server. When the unit is configured for Bridge mode, the Dynamic option is disabled and the user must enter in a specific IP Address.

NOTE:  Activating this option will reset the IP address of the unit.  If your network supports the DHCP Server capability, make sure the IP address assigned by the DHCP server will be accessible to you.  If your network does not support DHCP server capability, the unit will be reset to the default (192.168.205.1) IP address within the first 2 minutes.

To activate, select the "DHCP Client" radio button, click on the "Apply" button, click on the "Save Config" button, and reboot the ViPR.

▪ **IP Address**

Set to a valid unique IP address for each individual unit (default: 192.168.205.1).  In Bridge mode, all the ViPRs must be configured for the same IP subnet.  In Router mode, each ViPR must be configured for a unique subnet.

- **Netmask**

Set to a valid IP Netmask for each individual unit (depends on customer's IP network topology, default: 255.255.255.0).

- **DHCP Server**

DHCP Server Disabled, Enabled (Default). The Dynamic Host Configuration Protocol provides a framework for passing configuration information.

E.g.:  Assigns IP address to Hosts (i.e. PC/RTU) on a TCP/IP network.

- **Start Address**

Pool of addresses allocated for DHCP purpose.  If a unit is configured as a DHCP Server, this field represents the start IP address pool managed by the DHCP Server.  Normally, ViPR automatically calculates the Lease Start Address (equal to Ethernet IP Address plus one).

- **Number of Leases**

Maximum number of DHCP client(s) a unit can serve.

- **Lease Duration**

The period over which the IP Address allocated to a DHCP client is referred to as a "lease". Lease Duration is the amount entered in minutes.  If 0 (zero) is entered, the lease will not expire.

- **Gateway**

The Gateway text box displays the IP address of the gateway assigned by the DHCP server. In Router mode, the default (preset) gateway is the IP address of the unit itself.  In Bridge mode, the default (preset) gateway is 0.0.0.0.  To override the default setting, enter a valid IP address in the text field.

- **MTU**

Maximum Transfer Unit - Default = 1500 bytes.  The MTU is the maximum number of bytes the unit will send in a packet.  The input range is from 576 to 1500.

- **MAC Address**

The Ethernet MAC address (media access control) is the unique address that a manufacturer assigns to each networking device.  AA:BB:CC:DD:EE:FF  The user can not change the Ethernet MAC address.

### 6.2.2  RF Interface

- **IP Address**

The RF IP address (default: assigned by factory based on the unit's MAC address) is the RF IP address that is used when sending data and control packets in a ViPR network.

- **Netmask**

The Netmask (default: 255.0.0.0) is set to a valid common RF IP Netmask for all units in a ViPR network.

- **MTU**

Maximum Transfer Unit - Default = 1500 bytes.  The Maximum transfer unit is the maximum number of bytes the unit will send in a packet.  The input range is from 576 to 1500.

- **MAC**

The RF MAC is a shortened version of the Ethernet MAC address which is used to identify the radio to other ViPRs on the network.  The default RF MAC address is assigned by the factory and is equal to the last six digits of the Ethernet MAC address (DD:EE:FF).  The user can override the default RF MAC address by entering the new RF MAC address in the MAC address field under the RF Interface section.

When the network is configured for router mode, this feature is useful when replacing a ViPR in the field with a new one.  The new ViPR can be programmed to have the same RF MAC, Ethernet IP Address, and RF IP Address as the ViPR that is being replaced.  When the new ViPR is installed, neighboring ViPRs in the network will not know the original ViPR was replaced.  Neighboring ViPRs will not need to have their neighbor tables updated.

The RF MAC address must be unique for each ViPR in the network.  This applies to both Bridge and Router mode configurations.

### 6.2.3  Default Gateway

The Default Gateway (default: 0.0.0.0) allows the user to enter in the IP address of the access point to be used as the gateway to the management network.  If there is one ViPR configured as an Access Point in the network, all the other ViPRs will set their Default Gateway equal to the RF IP address of the Access Point.

### 6.3  CHANNEL TABLE

The Channel Table will display the Transmit Frequency, Receive Frequency, Transmit Power, and Channel Type for each channel in the unit.

**CHANNEL TABLE**

| RADIO CAPABILITIES | | |
|---|---|---|
| **Rx Frequency Range** | Min 406.125000 MHz | Max 470.000000 MHz |
| **Tx Frequency Range** | Min 406.125000 MHz | Max 470.000000 MHz |
| **Output Power Range** | Min 1.0 Watts | Max 10.0 Watts |

| CURRENT RADIO SETTINGS | | | |
|---|---|---|---|
| **RX Frequency** | 461.350000 MHz | **Output Power** | 5.0 Watts |
| **TX Frequency** | 466.350000 MHz | **Channel Type** | 32 Kbps in 25 KHz |

| CHANNELS | | | | |
|---|---|---|---|---|
| ○ Transmitter Disabled | | | | |
| **#** | **RX (MHz)** | **TX (MHz)** | **PA Power (Watts)** | **Channel Type** |
| ⊙ 1 | 461.350000 | 466.350000 | 5.0 | 32 Kbps in 25 KHz |
| ○ 2 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 3 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 4 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 5 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 6 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 7 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 8 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |
| ○ 9 | 000.000000 | 000.000000 | 5.0 | 16 Kbps in 12.5 KHz |

*Figure 6.5 – Setup (Basic) ⇨ Channel Table Web Page*

- **Radio Capabilities**

Tx & Rx Frequency Range and Output Power Range is factory set.

140-5018-500/501:  VHF, 136.000-174.000 MHz, 1-10W
140-5028-502/503:  VHF, 215.000-214.000 MHz, 1-10W
140-5048-300/301:  UHF Range 3, 406.125-470.000 MHz, 1-10W
140-5048-500/501:  UHF Range 5, 450.000-511.975 MHz, 1-10W
140-5098-500/501:  900, 928.000-960.000 MHz, 1-8W


- **Current Radio Settings**

Displays the current Rx & Tx Frequencies, Output Power, and Channel Type programmed into the radio.

- **Channels**

Transmitter Disabled radio button is set at the factory to disable the radio until a valid frequency has been entered.  The radio will not transmit until a valid frequency has been entered and the transmitter has been enabled.

There are 32 channels available in the ViPR.  The radio button beside each channel will select that channel as the active channel.  Each channel can operate in simplex (one frequency) or half duplex (pair of frequencies) mode.  The transmit power output level can be set for each channel. The channel type can be selected for each channel.  All ViPRs in a network must be set to the same channel type.

Note: It is the installer's responsibility to check the FCC license to determine the correct parameters and settings for channel frequencies, power level, and channel type.

## 6.4   SERIAL PORTS SETUP

The ViPR has two serial ports.  Either port can be configured to send data over the air, connect to the CLI (command line interface), report online diagnostics, or be custom configured to send/receive data on a specific port to/from a specific IP address.

By default the Setup port is configured to connect to the CLI at 19200 baud.  The Com port is configured to send data in DOX mode at 9600 baud.  By default the Com port will send data as a UDP multicast message to all the other ViPRs on the network (10.255.255.255) on port 6278.  When DOX mode is selected on the Setup port, the Setup port will send data as a UDP multicast message to all the other ViPRs on the network on port 6277.  If other configurations are needed, the ViPR allows for custom configuration of the transport protocol, IP Addresses, and ports the Setup port and Com port will connect with.

The serial custom configuration will allow the user to program the serial port as a terminal server.  A terminal server will translate the serial protocol to an Internet Protocol (IP).  A terminal server will wrap serial data presented at the serial port in an IP package (IP header and associated checksums).  When an IP message is sent to the terminal server's corresponding IP address, the IP package is stripped off.

A terminal server will not translate HMI/PLC polling message protocols that are not designed to be wrapped in an IP package. Most SCADA protocols are not designed to be used with a terminal server. As an example, the Modbus RTU message is a serial protocol. The Modbus TCP/IP protocol is an Ethernet IP protocol. The Modbus RTU message cannot be wrapped in an IP package to form a Modbus TCP/IP polling message. A protocol translation must take place. A device can be purchased that will perform the translation. Please contact your local SCADA dealer or CalAmp Tech Support to determine if your SCADA protocol can be used with a terminal server.

After any settings on this page are updated, press the "Apply" button. Wait for the page to reload then press the "Save Config" button then the "Reset Unit" button to update the changed serial port settings.

**Serial Ports Setup**

| SETUP PORT⚠ | COM PORT⚠ |
|---|---|
| ☑ **Enabled** | ☑ **Enabled** |
| **Speed** 19200 ▾ | **Speed** 9600 ▾ |
| **Data bits** ○7 ⦿8 | **Data bits** ○7 ⦿8 |
| **Stop bits** ⦿1 ○2 | **Stop bits** ⦿1 ○2 |
| **Parity** ○Odd ○Even ⦿None | **Parity** ○Odd ○Even ⦿None |
| **DCD Control** | **DCD Control** |
| Never asserted ▾ | Envelope mode ▾ |
| **Packet Forwarding Threshold** | **Packet Forwarding Threshold** |
| 4 ▾ MARK character time | 4 ▾ MARK character time |
| **Flow Control** | **Flow Control** |
| CTS-based ▾ | None ▾ |
| **Connection Control** | **Connection Control** |
| Switched (DTR bringup/teardown) ▾ | Permanent (3-wire) ▾ |
| **IP Gateway Service** | **IP Gateway Service** |
| ⦿ CLI Service | ○ CLI Service |
| ○ Serial/RF bridge - DOX mode | ⦿ Serial/RF bridge - DOX mode |
| ○ Online Diagnostics | ○ Serial/RF bridge - RTS/CTS mode |
| ○ Custom | ○ Online Diagnostics |
| | ○ Custom |
| **IP Gateway Transport** | **IP Gateway Transport** |
| TCP Client ▾ | UDP ▾ |
| Local IP Address 0.0.0.0 | Local IP Address 0.0.0.0 |
| Local Port Number # 1024 | Local Port Number # 6278 |
| Remote IP Address 127.0.0.1 | Remote IP Address 10.255.255.255 |
| Remote Port Number # 23 | Remote Port Number # 6278 |
| TCP Keepalive 0 (minutes) | TCP Keepalive 0 (minutes) |
| **Status: DOWN** | **RTS/CTS mode settings** |
| | CTS assertion delay 4 ms |
| | CTS negation delay 4 ms |
| | ☐ Send all buffered data before negating CTS |
| | ☐ Fragment large messages |
| | ☐ Discard all buffered data when entering flow control |
| | **Status: READY** |

Apply | Cancel | Refresh

If you "Apply" changes to any parameters marked ⚠ you will need to do a "Save Config" and a "Reset Unit".

*Figure 6.6 – Setup (Basic) ⇨ Serial Ports Web Page*

### 6.4.1  Basic Settings

- **Enabled Checkbox**

There are independent check boxes to activate SETUP PORT and/or COM PORT.

- **Speed**

The Setup port can be configured for 300, 1200, 2400, 4800, 9600, or 19200 Baud Rate. The Com port can be configured for 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 Baud Rate.

The default is 19200 for the SETUP port and 9600 for the COM port. The Baud Rate should be configured to match the settings of the connected device.

- **Data bits**

Number of bits making up the data word. The default is 8. This should be configured to match the settings of the connected device.

- **Stop bits**

Marks the end of the serial port data byte. The default is 1. This should be configured to match the settings of the connected device.

- **Parity**

Added to identify the sum of bits as odd or even. The default is none. This should be configured to match the settings of the connected device.

- **DCD Control**

The DCD (Data Carrier Detect) line can be set for one of the following:  Always Asserted, Never Asserted, or Envelope Mode (the DCD will be asserted only when data is present at the serial port).

- **Packet Forwarding Threshold**

Mark Character time allows the user to change time based on the character length to forward the packet.

- **Flow Control**

Allows the user to implement RTS/CTS flow control or no flow control.  Note: Request to Send and Clear to Send flow control will require a 5 wire connection to the Setup Port or Com Port.

- **Connection Control**

Select "Permanent (3-wire)" when the serial port is always enabled or "Switched (DTR bringup/teardown)" when DTR is used to enable/disable the serial connection.  This should be configured to match the settings of the connected device.

### 6.4.2  IP Gateway Service

The serial ports can be configured to provide several different services as listed below.

- **CLI Service**

Command Line Interface
Access to the Command Line Interface command shell is password protected and is reserved for authorized Dataradio maintenance personnel.

- **Serial/RF Bridge - DOX mode**

3 wire connection required.  Data is sent whenever it is present at the port.  Flow control is not required.  The IP Gateway service will use UDP transport protocol to send and receive messages.

- **Serial/RF Bridge - RTS/CTS mode**

5 wire connection required.  Data is sent after the device raises the RTS and the ViPR returns a CTS signal to the device.

- **Online Diagnostics**

TCP/IP based RF diagnostics for the entire ViPR network will be collected and sent to the serial port.

- **Custom**

Choosing Custom enables the user to specify the IP Gateway Transport configuration.  The defaults are CLI Service for SETUP port and Serial/RF Bridge for COM port.

### 6.4.3  IP Gateway Transport

The ViPR allows the user to select between two commonly used protocols for sending data to/from the serial port.  The first method, TCP, provides a reliable method of transmission, with acknowledgements and retries built into the protocol.  The TCP protocol requires several handshaking messages to open a connection, close a connection, and to acknowledge that a packet has been received correctly.  These handshaking messages will add some extra traffic to the network.

The second method, UDP, is a simpler method of sending data.  Connections do not need to be opened or closed before sending data, as in TCP.   Therefore, no extra handshaking is needed.  However, there is no acknowledgements or retries built into the UDP protocol.

Note: The ViPR can be configured to use RF acknowledgements and will retransmit a failed message over the air that does not successfully reach the next ViPR.  This acknowledgement/retry scheme is built into the ViPR and is independent of any TCP or UDP retries and will operate no matter which protocol is being used (TCP, UDP, or others).

- **TCP Overview**

The TCP protocol uses a client/server model.  A connection must be established between the client and the server before any data is sent.  The TCP client is responsible for initiating the connection between the client and server.  The TCP server will listen for any TCP clients that want to connect.  Neither the client nor the server can send data before the connection is opened.  Once the connection is open, data can flow freely in either direction.

- **TCP Server**

In TCP Server mode the ViPR will listen on the Local IP Address and Port Number for any requests to open a TCP connection.  The TCP Server can have up to 255 clients connected at

one time.  Data received from any client will be forwarded to the serial port.  Data received from the serial port will be forwarded to every client with an open connection.  If no open connections exist the data will be discarded.

The ViPR TCP server will leave the TCP connection open indefinitely, whether or not data is being sent.  However, if the ViPR is unable to send data successfully to the TCP Client (ie. no TCP acknowledgements are received from the remote endpoint) the ViPR's terminal server will close the faulty TCP connection.

- **TCP Client**

In TCP Client mode, the ViPR will try to establish a connection with a remote TCP Server.  Once the connection is established, data can flow freely in either direction.  If the connection is closed for any reason, the ViPR will try to reestablish the TCP connection.

TCP Client mode can be used with the Connection Control set to "Switched (DTR bringup/teardown).  In this mode, the DTR line on the serial port can be used to open and close the TCP connection.

- **UDP**

In UDP mode, the ViPR will always be listening on the Local IP address and Port Number.  Received data that is addressed to this IP address and Port will be immediately output on the serial port.  Any data received from the serial port will be sent to the Remote IP address and Port Number.

- **TCP CLIENT/SERVER MODE**

In this mode of operation, the unit acts as a TCP server and a TCP client. Data received from any remote endpoint is sent over the serial port. Data received from the serial port is sent to every remote endpoint connected to the TCP client/server.

The unit will try to establish a TCP connection to the remote endpoint defined by these two parameters when there is data received on the serial port AND there is no TCP connections already established.

- **IP Gateway Transport Parameters**

| | UDP MODE | TCP CLIENT MODE | TCP SERVER MODE | TCP CLIENT/SERVER MODE |
|---|---|---|---|---|
| **LOCAL PORT** | **REQUIRED**<br><br><u>Value</u><br>1-65535 | **UNUSED**<br><br><u>Value</u><br>IP stack decides the value. | **REQUIRED**<br><br><u>Value</u><br>1-65535<br>Do not use: 20, 21, 23, 123, 520, 5002, 6254 to 6299, 7000 to 7100 | **REQUIRED**<br><br><u>Value</u><br>1-65535 |
| **LOCAL IP ADDRESS** | **REQUIRED**<br><br><u>Value</u><br>0.0.0.0 (let IP stack decide)<br>*OR*<br>• IP address of ETH/RF interface | **REQUIRED**<br><br><u>Value</u><br>0.0.0.0 (let IP stack decide)<br>*OR*<br>IP address of ETH/RF interface | **REQUIRED**<br><br><u>Value</u><br>0.0.0.0 (let IP stack decide)<br>*OR*<br>IP address of ETH/RF interface | **REQUIRED**<br><br><u>Value</u><br>0.0.0.0 (let IP stack decide)<br>*OR*<br>IP address of ETH/RF interface |
| **REMOTE PORT** | **REQUIRED**<br><br><u>Value</u><br>1-65535 | **REQUIRED**<br><br><u>Value</u><br>1-65535 | **UNUSED**<br><br><u>Value</u><br>N/A | **REQUIRED**<br><br><u>Value</u><br>• 1-65535 |
| **REMOTE IP ADDRESS** | **REQUIRED**<br><br><u>Value</u><br>Unicast, Broadcast, or Multicast IP address | **REQUIRED**<br><br><u>Value</u><br>Unicast IP address | **UNUSED**<br><br><u>Value</u><br>N/A | **REQUIRED**<br><br><u>Value</u><br>• Unicast IP address |
| **TCP Keepalive** | **UNUSED** | **OPTIONAL**<br><br><u>Value</u><br>0 - 1440 (min)<br>(0: TCP Keepalive disabled). | **OPTIONAL**<br><br><u>Value</u><br>0 - 1440 (min)<br>(0: TCP Keepalive disabled). | **OPTIONAL**<br><br><u>Value</u><br>0 - 1440 (min)<br>(0: TCP Keepalive disabled). |

*Table 6.1 TCP/UDP Parameter Usage*

▪ **Local IP Address**

The local IP address can be set to one of three values as shown in the table below: Ethernet IP address, RF IP address, or either (0.0.0.0).

| Local IP Address | Receiving Description | Sending Description |
|---|---|---|
| Ethernet IP Address | Any IP message received over the RF or Ethernet interface with a destination address and port equal to the Ethernet IP address and the local port # will be received and sent to the serial port.  IP messages matching the RF IP address will be ignored. | All messages received by the serial port are sent over the RF or Ethernet interface with the Ethernet IP address as the source address. |
| RF IP Address | Any IP message received over the RF or Ethernet interface with a destination address and port equal to the RF IP address and the local port # will be received and sent to the serial port. Messages matching the Ethernet IP address will be ignored. | All messages received by the serial port are sent over the RF or Ethernet interface with the RF IP address as the source address. |
| 0.0.0.0 | Any IP message received over the RF or Ethernet interface with a destination address and port equal to the RF IP address or the Ethernet IP address and the local port # will be received and sent to the serial port. | Messages sent over the Ethernet interface will have a source address equal to the Ethernet IP address.  Messages sent over the RF interface will have a source address equal to the RF IP address. |

*Table 6.1 Local IP Address Description*

▪ **Local IP Port #**

For TCP Client and UDP socket connections, set to any value between 1 and 65535. For TCP Server socket connections, set to any value between 1 and 65535, but must not be set to one of the following values or fall within the following ranges of values: 20, 21, 23, 123, 520, 5002, 6254 to 6299, 7000 to 7100. If a reserved port is selected, the parameter configuration will be accepted, but no socket connection will be established to accept connections from remote endpoints.  Note: Firewalls are set to block certain ports such as 6666.  Please check your firewall settings to determine which ports will be blocked.

▪ **Remote IP Address**

Enter a valid unicast (TCP Client & UDP modes) or multicast/broadcast IP address (UDP mode only) that the unit can connect to.

▪ **Remote IP Port #**

For TCP Client and UDP modes, set to any value between 1 and 65536.

001-5008-000 rev5_2.doc                                                                                   Page 55

- **TCP Keepalive**

The TCP Keepalive feature will transmit a short Keepalive message to test the TCP connection if there is no data transferred through an open TCP connection after X number of minutes.  If the keepalive message is received successfully by the remote endpoint the TCP connection will remain open.  If the keepalive message is not received successfully the ViPR will close the existing TCP connection.

To disable this feature, set the TCP Keepalive to "0". With the TCP Keepalive feature disabled, the ViPR will leave the TCP connection open indefinitely.  An existing TCP connection will only close if the remote endpoint closes the connection, the ViPR's serial port is disabled, or if the ViPR is unable to successfully communicate with the remote endpoint during a data transmission.

### 6.4.4  RTS/CTS Mode Settings

- **CTS Assertion Delay**

The time in milliseconds the data will be delayed after the CTS has been sent.

- **CTS Negation Delay**

The time in milliseconds the CTS will be kept asserted after the last character has been transmitted.

- **Send all buffered data before negating CTS**

All the data will be sent before the ViPR drops the CTS control line.

- **Fragment large messages**

Allows the user's data to be fragmented into smaller messages.

- **Discard all buffered data when entering flow control**

The data in the serial port buffer will be discarded and only new data will be processed under the flow control.

## 7 SETUP (ADVANCED)

### 7.1 RF OPTIMIZATIONS

**RF optimizations**

| MAC Advanced Settings | |
|---|---|
| **Duplicates Detection Period** | 5000 ms [1000-15000] |
| **Retries** | 1 |
| **RTS Threshold** | 128 bytes [0-RF_MTU] |
| **Carrier Sense Level Threshold** | -110.000000 dBm |
| **Listen Before Transmit** | Enabled (listen to noise and data) ▾ |

Apply  Cancel

If you "Apply" changes to any parameters marked ⚠ you will need to do a "Save Config" and a "Reset Unit".

*Figure 7.1 Setup (Advanced) ⇨ RF Optimizations Web Page*

### 7.1.1 MAC Advanced Settings

▪ **Duplicates Detection Period**

Default = 5000 ms. This parameter specifies the time period in milliseconds the ViPR will look for a duplicate message being sent, such as control and relay messages. If a duplicate message is detected it will not be forwarded. Certain protocols such as Modbus cannot tolerate hearing duplicate messages (echoes). The duplicate messages will not be sent to the Serial ports or forwarded to the Ethernet connection. Larger values should be used for lower over-the-air (OTA) speeds and longer path networks.

▪ **Retries**

Default = 1. This parameter specifies the number of times the MAC layer in the ViPR will try to resend a packet if the unit does not receive an acknowledgement reply from the receiving ViPR. Increasing the retries may improve marginal RF paths. For retries to be enabled, RF Acknowledgments must be enabled and can be configured under Setup (Advanced) ⇨ IP Optimization.

▪ **RTS Threshold**

Default = 128.

The ViPR utilizes the FAMA-NCS (for floor acquisition multiple access with non-persistent carrier sensing) protocol. The FAMA-NCS protocol tries to assure that a single ViPR is able to send data packets free of collisions to a given receiver at any given time. FAMA-NCS is based on a three-way handshake between the sender and receiver in which the sender uses non-persistent carrier sensing to transmit a request-to-send (RTS) and the receiver sends a clear-to-send (CTS). RTS/CTS handshaking protocol enables the ViPR network to avoid collisions in networks with multiple coverage areas. Before transmitting an RTS frame, a ViPR listens to the channel to determine if it is already in use. If the channel is busy, the unit calculates a random back off period to wait before sensing the channel again.

The RTS threshold parameter specifies how large a packet must be before the unit will use RTS/CTS handshaking in the over-the-air protocol.  A value of 0 means the ViPR will always use over-the-air RTS/CTS handshaking.  A value equal to the RF_MTU (OTA maximum transmit unit) means the ViPR will never use RTS/CTS handshaking.  A value of 128 means the ViPR will use RTS/CTS for packets larger than 128 bytes.

**Note: This should not be confused with RTS/CTS for RS232 Serial ports**.

### 7.1.2  Carrier Sense Level Threshold

Default = -110 dBm.  This is the threshold the ViPR uses to determine whether a received RF signal is a valid message or unwanted noise.  If an RF level higher than the Carrier Sense Level Threshold is detected, the ViPR will attempt to decode the signal and will not transmit until the RF level drops.  Outgoing data will be buffered until the channel is available.  The carrier sense may be raised to prevent false carrier sense detection if the network is installed in a noisy environment.  In certain situations where the ambient RF noise level is very low, the carrier sense level threshold can be lowered to gain extra receive sensitivity.  (The ViPR's specified receive sensitivity depends upon the channel bandwidth/speed being used.  Refer to the product specification in Appendix A for details.)

### 7.1.3  Listen Before Transmit

Default = Enabled (listen to noise and data).  The ViPR radio has the ability to receive on the Rx frequency to determine if the RF channel is busy.  When the RF channel is busy the ViPR can buffer any data that needs to be sent over the air and will transmit when the RF channel is free.  There are three modes available in the ViPR for the Listen Before Transmit feature. They are described in the following paragraphs.

**Enabled (listen to noise and data):** This is the default mode for the ViPR.  The ViPR will monitor the RF level on the receive channel.  When the received level is above the carrier sense threshold the ViPR will try to receive and decode any and all messages from remote ViPRs.  In this mode, the ViPR will wait to transmit any data until the received level falls below the carrier sense threshold.  The received level will rise above the carrier sense threshold due to several scenarios:

> 1) The ViPR is receiving valid data
> 2) The ViPR is not receiving data because two or more ViPRs are transmitting at the same time causing a collision
> 3) The ViPR is not receiving data because the RF level is right at or below data sensitivity or
> 4) There is interference from another RF system or electrical devices on the frequency that the ViPR is operating on.

In any of these scenarios, the ViPR waits to transmit any data until the RF level falls below the carrier sense threshold.  This ensures that the data will have the best chance of reaching its destination.

**Enabled (listen to data only)**:  In this mode, the ViPR will monitor the RF level on the receive channel.  When the received level is above the carrier sense threshold the ViPR will try to receive and decode any and all messages from remote ViPRs.

When data is ready to transmit, the ViPR will first check the receive level.  If the receive level is below the carrier sense threshold, the ViPR will immediately transmit data.  If the receive level is above the carrier threshold, the ViPR will try to determine if it is receiving valid data or just noise.  If it is receiving noise, the ViPR will go ahead and transmit.  If it is receiving valid data, the ViPR will wait until the complete packet has been received before transmitting.  The ViPR will typically take somewhere between 5 ms to 250 ms to determine if it is receiving valid data or just noise.

**Disabled**:  In this mode, the ViPR will attempt to receive/decode data when the received RF level is above the carrier sense threshold.  When the ViPR has data to transmit it will immediately transmit the data.  The ViPR will immediately stop receiving any packets and will transmit over any other ViPRs that are on the air and over any interference that may be in the area.

This mode should only be used in a polling type environment where the user has strict control over the traffic that is generated.

## 7.2   IP SERVICES

- **RIPV2**

  Enabled, Disabled (default).  Router Information Protocol v2 is a dynamic IP routing protocol based on the distance vector algorithm and is only used in Router Mode.  RIPV2 is responsible for passing router information to other routers in the network.

- **IPSD**

  Enabled (default), Disabled.  I/P Services Delivery allows the generation of locally provided I/P Services such as online diagnostics, etc.

- **NAT**

  Enabled, Disabled (default).  Network Address Translation (NAT) is a method by which IP addresses are mapped from one address space to another.  In a ViPR, it is normally used on the WAN side of an IP network to hide local IP addresses from an external IP network (example: the Internet).

## IP Services Setup

| RIPV2 ⚠ | ○ Enabled ⦿ Disabled |
|---|---|
| IPSD⚠ | ⦿ Enabled ○ Disabled |
| NAT⚠ | ○ Enabled ⦿ Disabled |

| | SNMP |
|---|---|
| SNMP AGENT⚠ | ⦿ Enabled<br>○ Disabled |
| ○ Add⚠<br>○ Delete | [                    ] |
| Trap IP List | 192.168.206.100<br>192.168.205.20<br>192.168.205.10 |
| MIB | Download mibs.zip |

### NAT Private Network Table

| | IP Address | Netmask | Enable |
|---|---|---|---|
| ETH⚠ | 192.168.254.0 | 255.255.255.252 | ☐ |
| RF⚠ | 10.0.0.0 | 255.0.0.0 | ☐ |
| USER1⚠ | 0.0.0.0 | 255.255.255.255 | ☐ |
| USER2⚠ | 0.0.0.0 | 255.255.255.255 | ☐ |
| USER3⚠ | 0.0.0.0 | 255.255.255.255 | ☐ |
| | Clear Table | | |

*Figure 7.2 Setup (Advanced) ⇨ IP Services Web Page*

### NAT Port Forwarding Table

| Protocol | Public Port Number<br>First    Last | Private IP Address | Private Port Number | Enable |
|---|---|---|---|---|
| ⚠ [  ▾] | 0 - 0 | 0.0.0.0 | 0 | ☐ |
| ⚠ [  ▾] | 0 - 0 | 0.0.0.0 | 0 | ☐ |
| ⚠ [  ▾] | 0 - 0 | 0.0.0.0 | 0 | ☐ |
| ⚠ [  ▾] | 0 - 0 | 0.0.0.0 | 0 | ☐ |
| ⚠ [  ▾] | 0 - 0 | 0.0.0.0 | 0 | ☐ |
| | Clear Table | | | |

*Figure 7.3 Setup (Advanced) ⇨ IP Services Web Page (NAT Port Forwarding)*

### 7.2.1  SNMP

This section is only available when the appropriate feature key is installed in the ViPR.
Contact CalAmp for information about obtaining and installing the SNMP feature.

SNMP (Simple Network Management Protocol) is used by network management systems to
manage and monitor network-attached devices. SNMP is based on the manager/agent
model consisting of a manager, an agent, a database of management information, managed
objects, and the network protocol. The manager provides the interface between the human

network manager and the management system. The agent provides the interface between the manager and the physical devices being managed (7.4). SNMP uses basic messages (*such as GET, GET-NEXT, SET, and TRAP*) to communicate between the manager and the agent.
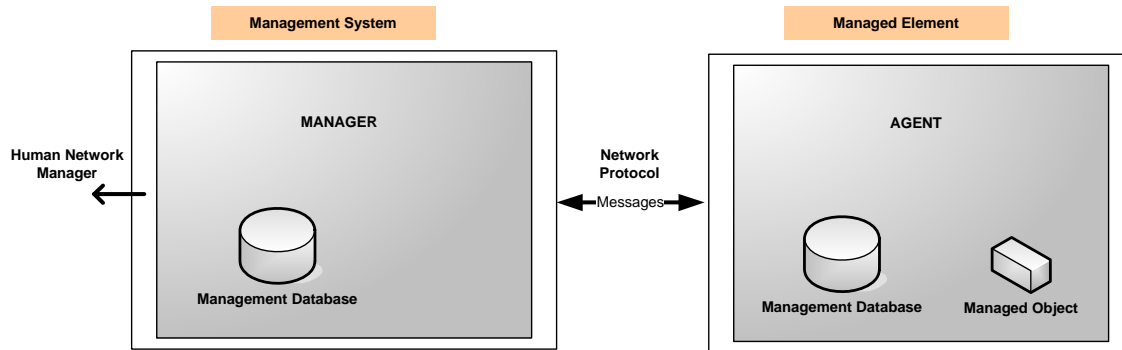


*Figure 7.4 - SNMP: manager/agent model*

Traps:  Traps (or alarms) can be automatically generated by the ViPR radio modem whenever the forward or reverse power goes out of specification. These traps can be sent to a user specified IP address or addresses.  Use the following steps to enable traps:

   1) Enable SNMP (Setup (Advanced) – IP Services)
   2) Enter IP Addresses into Trap IP List. (Setup (Advanced) – IP Services)
   3) Enable Individual Traps. (Setup (Advanced) – Alarm Reporting)

Trap IP List: This list shows the user programmed IP addresses where the ViPR will send SNMP traps.  To add an IP Address to the list, select the 'Add' radio button, enter the IP Address into the text box, and then click the 'Apply' button at the bottom of the page. When the page is refreshed the new IP address will appear in the Trap IP List.  To delete an IP Address from the list, select the 'Delete' radio button, enter the IP Address to delete into the text box, and then click the 'Apply' button at the bottom of the page.


The ViPR is compatible with SNMP version 2.

▪ **MIB**

The manager and agent use a Management Information Base (MIB), a logical, hierarchically organized database of network management information. MIB comprises a complete collection of objects used to manage entities in a network. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and SNMP messages.

▪ **ViPR MIB File**

Each ViPR unit firmware package is bundled with three MIB files (found inside mibs.zip file):
- *dataradio-regs.mib*: contains a top level set of managed object definitions aimed at managing Dataradio products
- *1213.mib*: contains a set of managed object definitions aimed at managing TCP/IP-based internets
- *ipr.mib*: contains a set of managed object definitions aimed at managing Dataradio ViPR modems

▪ **OID**

In SNMP, each object has a unique OID consisting of numbers separated by decimal points. These object identifiers naturally form a tree.  Figure 7.5 illustrates this tree-like structure for *1213.mib,* which comes bundled the ViPR unit package.  A path to any object can be easily traced starting from the root (top of the tree).  For example, object titled "SNMP" has a unique OID: 1.3.6.1.2.1.11.  The MIB associates each OID with a label (e.g. "SNMP") and various other parameters.  When an SNMP manager wants to obtain information on an object, it will assemble a specific message (e.g. GET packet) that includes the OID of the object of interest.  If the OID is found, a response packet is assembled and sent back.  If the OID is not found, a special error response is sent that identifies the unmanaged object.
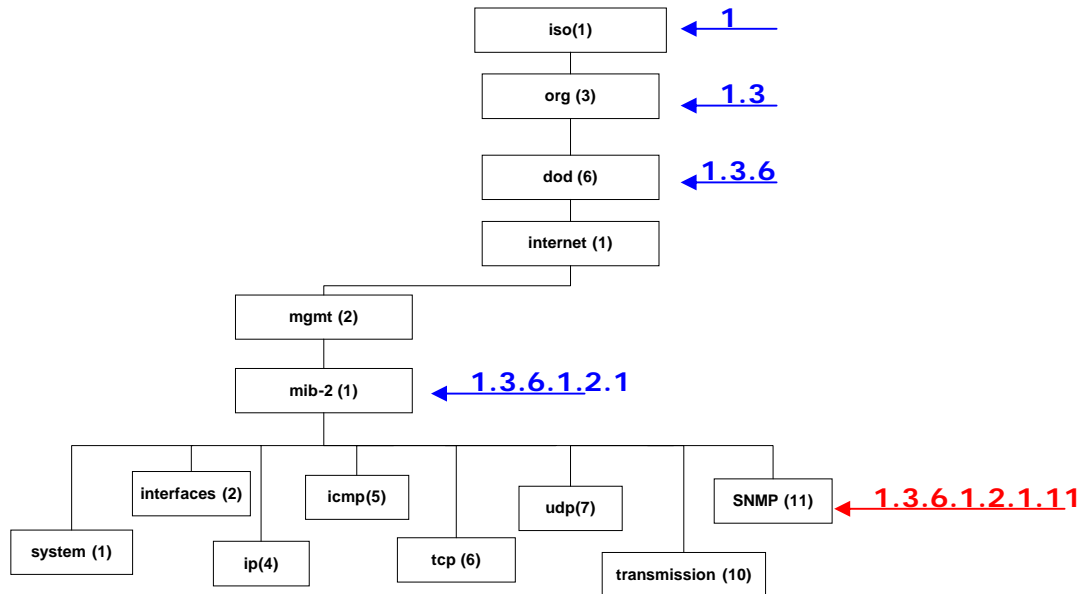


*Figure 7.5 - Branch of the 1234.mib OID tree*

▪ **MIB Browser**

CalAmp recommends opening all MIB files with a MIB browser.  For simple networks, a basic, free application such as "iReasoning MIB browser" could be used.  However, for managing complex networks CalAmp recommends a more advanced software application, such as "Castle Rock SNMPc Network Manager".  In a MIB browser, each object (or node) can be selected and its properties (including its OID) can be observed.

> *Note: Both "Read Community" and "Write Community" passwords are required to operate SNMP MIB.  For all ViPR radio modems the same password is used for both read and write.  This password is the same password used to access the ViPR web pages.*

▪ **ipr.mib**

Figure 7.6 shows top-level objects of the ipr.mib file:

- *viprIdentity*
- *viprSettings*
- *viprStatistics*
- *viprDiagonistics*
- *viprNeighbors*

- *viprControl*
- *viprOptions*

These seven branches expand into additional branches and leaves. Again, all ipr.mib objects can be accessed through a MIB browser.
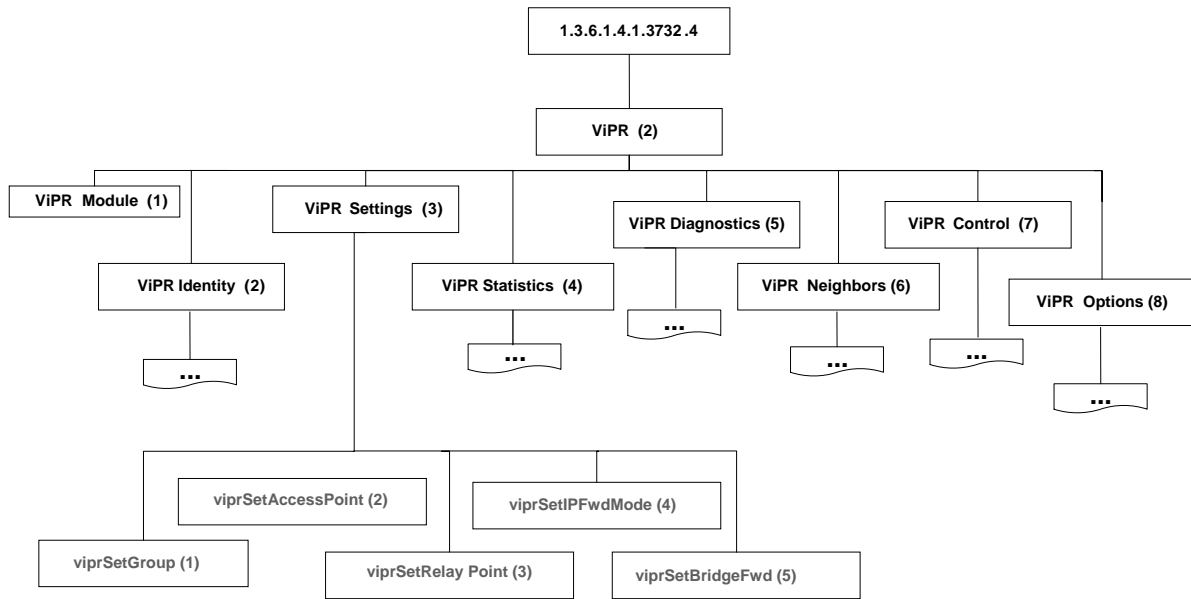


*Figure 7.6 -  ViPR OID Tree*

### 7.2.2  NAT Overview

The purpose of the NAT protocol is to hide a private IP network from a public network. The mechanism serves both as a firewall and to save IP address space.

The NAT enabled device translates the source address of packets transiting from the private network to the public network.  The original IP source address gets replaced by the NAT enabled device's IP address (address of the outgoing interface).  The NAT module creates an address translation table that is used when traffic is coming back from the public network to the private network.

```
Packet (1)
Source Address 192.168.205.2
Destination Address 172.31.5.2

Packet (1)
Source Address 172.31.5.1
Destination Address 172.31.5.2

192.168.205.1          172.31.5.1

Host 1                 NAT Enabled Device          Host 2
192.168.205.2                                      172.31.5.2

Packet (2)                          Packet (2)
Source Address 172.31.5.2           Source Address 172.31.5.2
Destination Address 192.168.205.2   Destination Address 172.31.5.1

Private Network 192.168.205.0       Public Network 172.31.5.0
```

*Figure 7.7 Basic NAT Operation*

In our example, Host 1 sends a packet to Host 2. The Host 2 device does not see the private IP address of Host 1. When Host 2 sends a reply to Host 1, Host 2 uses the destination IP address 172.31.5.1, which is translated back to the appropriate destination IP address by the NAT enabled device.  (See Figure 7.7)

NAT does a lot more than just translation of the source IP address.  For the UDP and TCP protocol, NAT will also translate the source port numbers.  Special handling is also done for more specific protocols like FTP (port 21) and Modbus (port 502).

### 7.2.3  NAT on ViPR

The user can select which of two interfaces (Ethernet or RF) will be considered private.  The following examples illustrate how to configure the ViPRs.  The examples use a private network of 192.168.205.X and a public network of 172.31.5.X.

### 7.2.4  Ethernet Interface Private

Figure 7.8 shows the NAT enabled for the Eth interface.

*Figure 7.8 Nat on ViPR: NAT enabled, Eth interface considered private*

Figure 7.9 shows a ViPR configuration protecting ViPR (1) Ethernet interface IP address from hosts located on a public network.
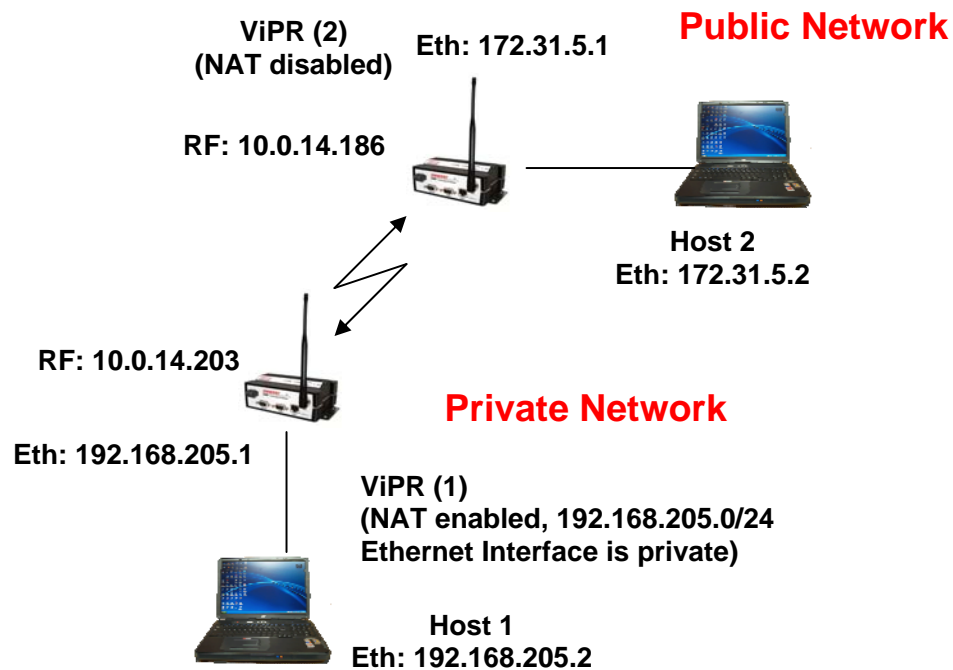


*Figure 7.9 ViPR NAT Enabled, Ethernet interface considered private*

An IP packet whose source IP address originates from the Ethernet network and is sent towards the RF network, will have its source IP address replaced by the RF IP address of ViPR(1) as shown in Figure 7.10.
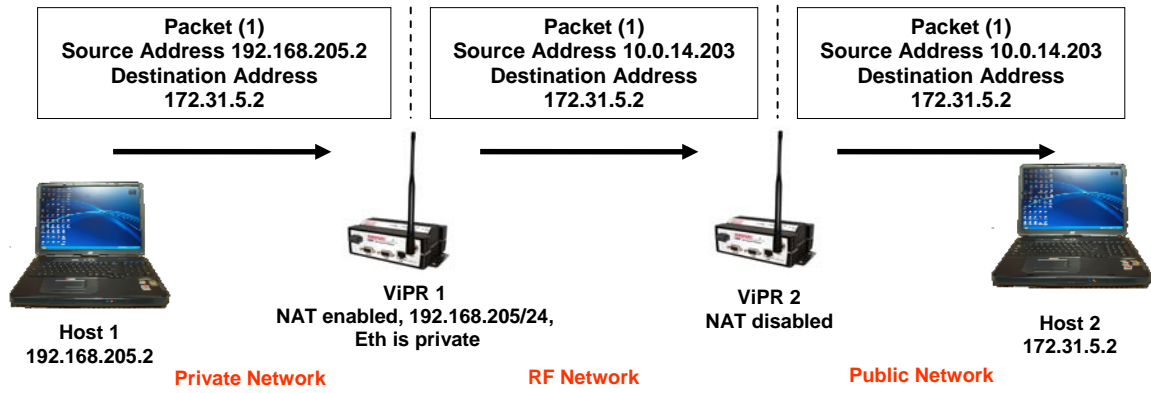
*Figure 7.10 Private to Public Packet flow*

**Note: Host 1 will be able to ping Host 2, however Host 2 will not be able to ping or originate a message to Host 1 when NAT Eth enabled.**

### 7.2.5  RF Interface Private

Figure 7.11 shows the NAT enabled for the RF interface.



*Figure 7.11 NAT on ViPR: RF interface considered private*

Figure 7.12 shows a ViPR configuration protecting ViPR (2) RF interface **and** ViPR (1) Ethernet interface from hosts located on a public network.
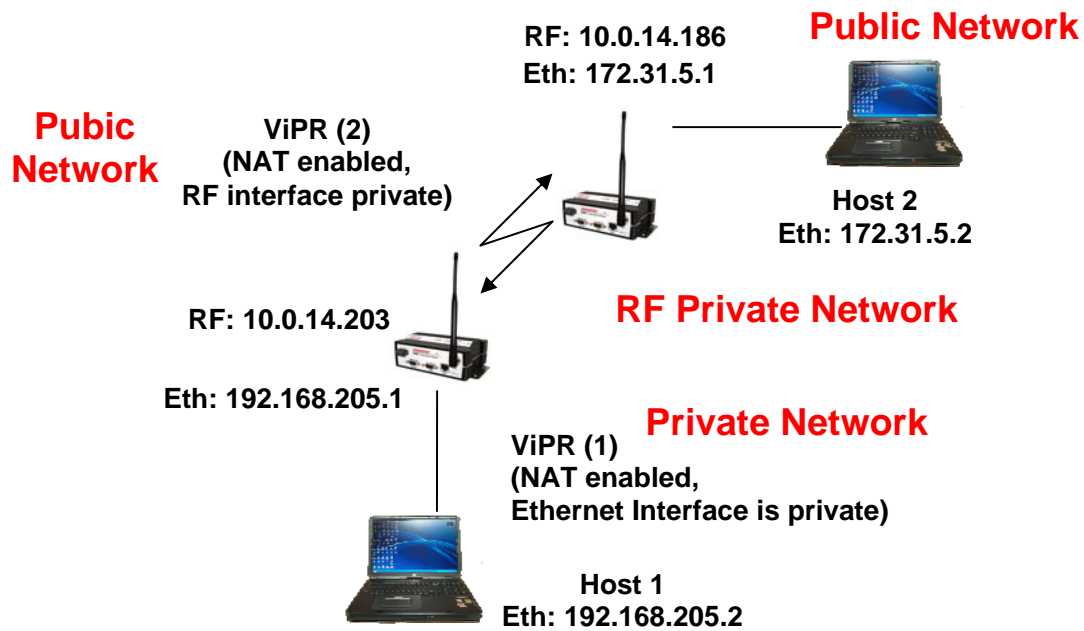


*Figure 7.12 NAT on ViPR: Private RF interface and Private Eth interface*

An IP packet whose source IP address originates from the RF network and is sent towards the Ethernet network will have its source IP address replaced by the Ethernet IP address of ViPR (2).  Notice in this configuration the Ethernet IP address for ViPR (1) is considered private **and** the RF IP address for ViPR (2) is considered private. Figure 7.13 shows how the packets will be modified as the packets pass through the network.
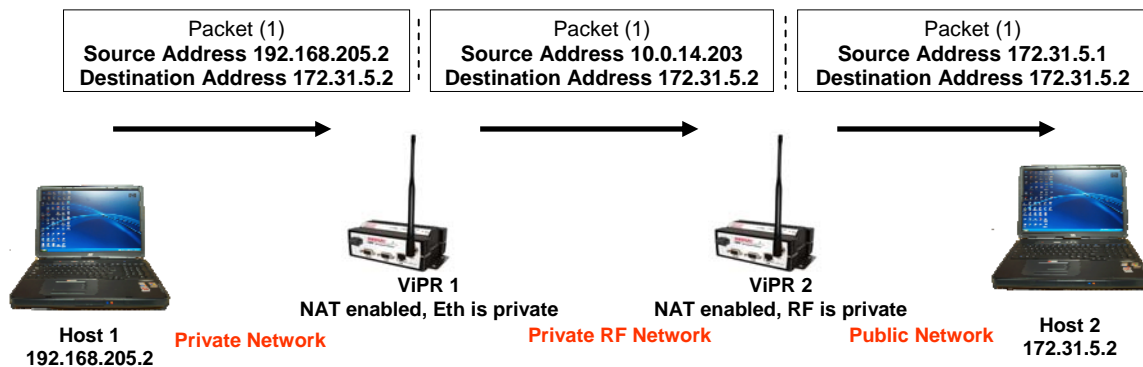


*Figure 7.13 Packet flow Private Eth and RF interface*

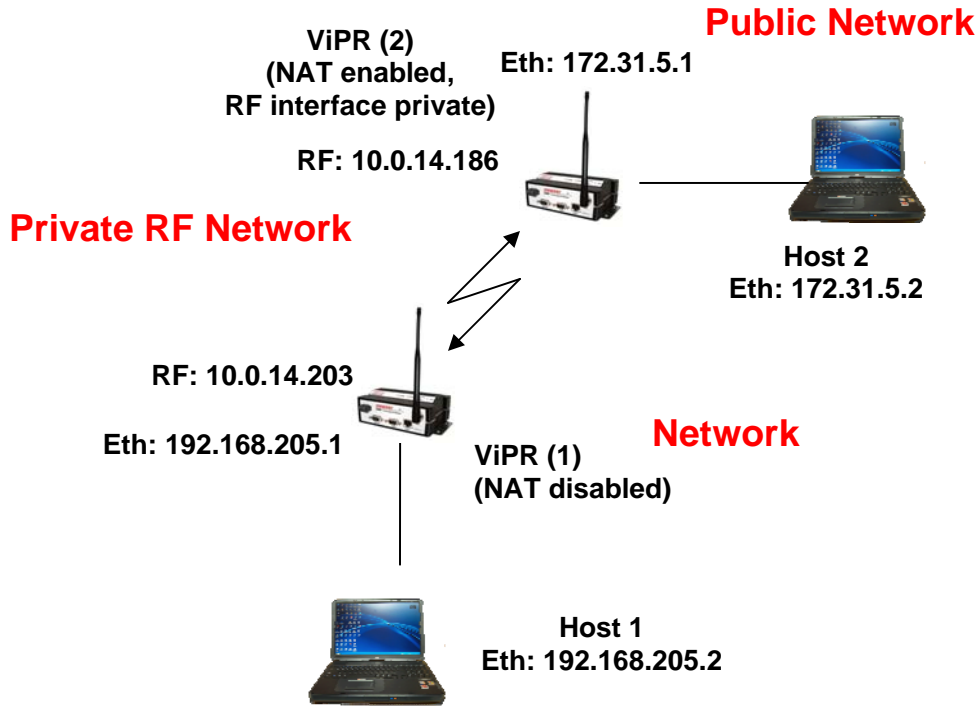In example Figure 7.14, the RF interface of ViPR (2) is considered private.  NAT is disabled for ViPR (1).

*Figure 7.14 NAT on ViPR: RF interface considered private*

Notice in Figure 7.15 that when Host 1 sends a packet, the source IP address is not changed by ViPR (2) because the source does not originate from the private RF network.
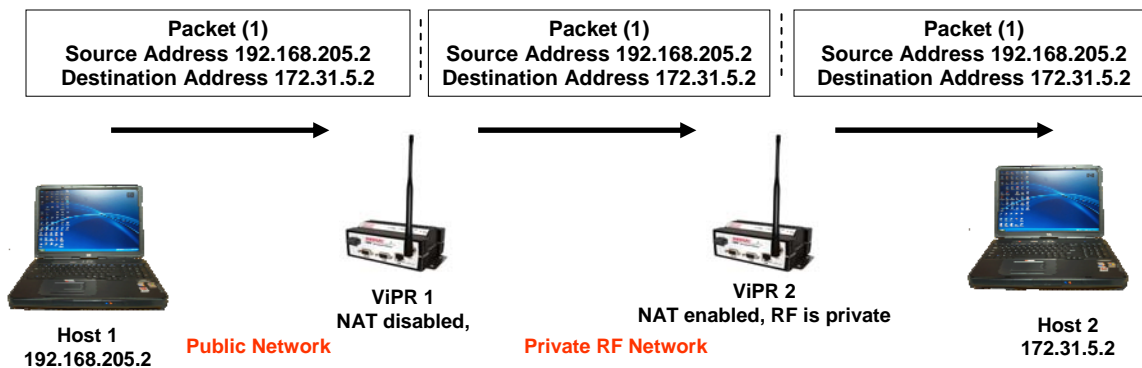


*Figure 7.15 Packet flow, RF interface considered private*

In the previous example, ViPR (1) was changing the source IP address of the packet, making the ViPR (2) believe that the packet was originating from the RF network.

### 7.2.6  User NAT Entries

The user can add three USER IP addresses that will be considered private. Figure 7.16 shows USER1 192.168.205.125 and USER2 192.168.205 will be considered private.  If

USER3 192.168.205.87 is connected to the ViPR, but not added to the table, USER3 192.168.205.87 would not be considered private.



*Figure 7.16 NAT on ViPR: USER1 and USER2 considered private*

### 7.2.7  NAT Port Forwarding

The NAT Port Forwarding table allows the user to specify a particular public port or range of ports to be forwarded to the private network hidden by the Network Address Translation Table. The user can also select between TCP and UDP protocols. Figure 7.17 shows the NAT Eth IP subnet 192.168.205.0 will be hidden from the Public Network. Any TCP packets sent to the ViPR with port number 2000 will be redirected to the Private IP Address and Private Port Number entered in the NAT Port Forwarding Table as shown in Figure 7.17.



*Figure 7.17 NAT on ViPR: Port 2000 is redirected to 192.168.205.125:23*

Figure 7.18 shows the Private Network 192.168.205.0 being protected from the Public Network 172.31.5.0. ViPR (1) NAT Eth interface is enabled and ViPR (2) NAT is disabled. The Host 172.31.5.2 cannot send packets directly to the Private Network because it is hidden.  In this example, remember that Host 172.31.5.2 thinks the IP packets are coming from 10.0.14.203.
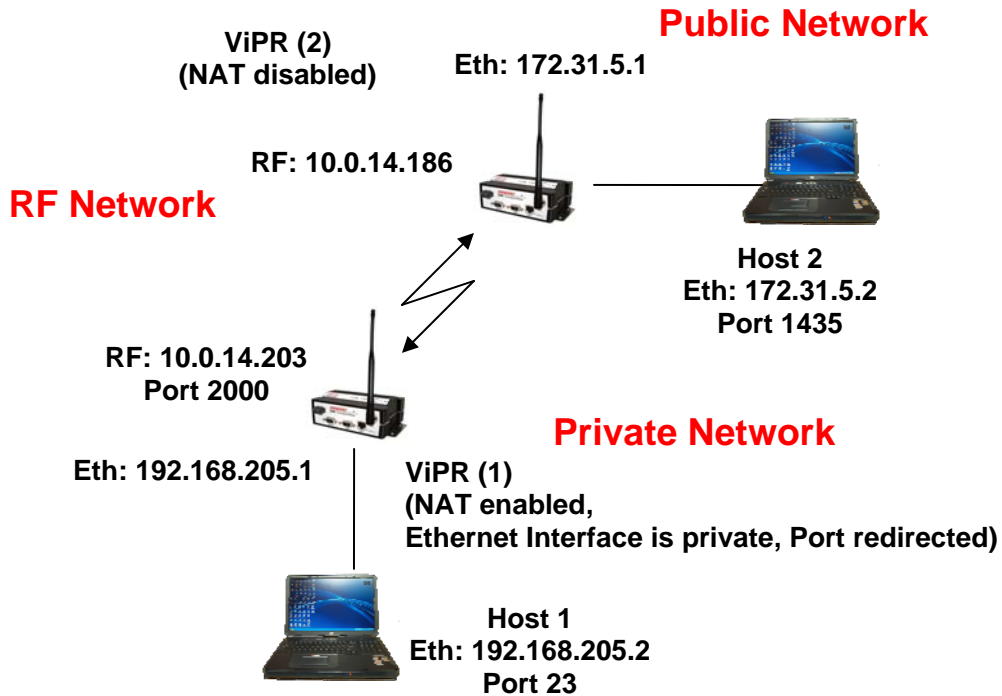


*Figure 7.18 NAT on ViPR: Port 2000 is redirected to 192.168.205.125:23*

When Host 172.31.5.2 wants to send packets to Host 192.168.205.2 the packets are sent to 10.0.14.203.  NAT port translation allows Host 172.31.5.2:1435 (port 1435) to send TCP packets to 192.168.205.5:23 (port 23) by sending the packets to 10.0.14.203:2000 (port 2000).  Figure 7.19 shows how the packets would be modified as they moved through the network.
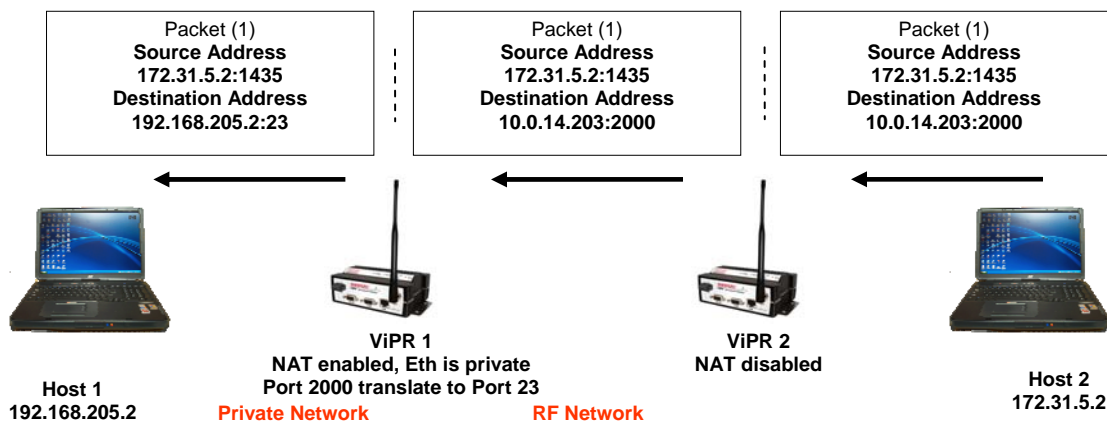


*Figure 7.19 Packet flow, Port redirection*

### 7.3  IP ADDRESSING

There are some SCADA PLC protocols that use different IP addressing modes.  GE's Global Data protocol has the ability to send out a group message command to remote PLCs.  The group message is actually a multicast message.  The Multicast feature allows the user to add or delete a remote's IP address.



*Figure 7.20 Setup (Advanced) ⇨ IP Addressing Modes Web Page*

### 7.3.1  Broadcast Mode

▪ **Directed Broadcast**

Select: Enabled, Disabled; Default: Enabled.
Controls forwarding of Directed Broadcast packets

▪ **Limited Broadcast**

Select: Enabled, Disabled; Default: Disabled.
Controls forwarding of Limited Broadcast packets

▪ **Convert Multicast to Broadcast**

Select: Enabled, Disabled; Default: Disabled.

### 7.3.2  Multicast Mode

▪ **Multicast**

Select: Enabled, Disabled; Default: Disabled.
Controls forwarding of Multicast packets (based on the MULTICAST ADDRESS LIST).
Multicast can be used when one-to-many communications is required.

▪ **Address List**

ADD or DELETE IP Address of the device to be added or removed.  Only valid multicast addresses are accepted and displayed in the ADDRESS LIST.

When an IP packet is received via the Ethernet LAN and the destination IP address matches one of the multicast IP address in the list, it is forwarded over the RF network.  Remote units will then send it over the remote LAN to the appropriate device(s).

## 7.4   IP OPTIMIZATION

IP Optimization is only available in Router Mode.



*Figure 7.21 Setup (Advanced) ⇨ IP Optimization Web Page*

- **Router Mode - RF ACK**

RF Acknowledgements - Default = Disabled.
If RF ACK is enabled, the receiving ViPR will reply with a quick acknowledgement message to the sending ViPR to indicate that it has received the packet successfully.  If the sending ViPR does not receive the acknowledgement, it will assume the message was lost and will try to resend the message.  The number of retries can be specified.

TCP packets are always retried regardless of the "RF ACK" parameter (unless OIP Retries is set to 0).  Other types of packets are only retried if RF ACK is enabled.

- **Router Mode - OIP Retries**

Number of OIP retries - Default = 2.
This parameter specifies the number of retries that the OIP layer will attempt if an acknowledgement message is not received from the destination ViPR.  Retries are only enabled if Router mode is selected and RF ACK is turned on.  The number of retries should be increased if a there is a marginal RF path to another unit.

- **TCP Proxy**

The TCP proxy optimizes the throughput of a TCP connection by removing some of the TCP packets from the Airlink.  A ViPR receiving a TCP packet over the air sends an RF acknowledgment to the sending unit.  If the sending ViPR receives the RF acknowledgement, it knows the packet made it across the Airlink successfully.  When the TCP proxy is enabled and the TCP packet contained data, the sending ViPR immediately generates a TCP ACK to the sending host (RTU, PLC, PC, etc).  When the destination host receives the TCP packet, it generates a TCP ACK back to the source.  This TCP ACK is captured by the ViPR not sent over the Airlink.

In the example below (Figure 7.22) the following events occur in this order:
1) Host A sends TCP data packet to ViPR A.
2) ViPR A transmits packet over the air to ViPR B.
3) ViPR B immediately responds with an RF acknowledgment and sends the TCP data packet to Host B.
4) ViPR A hears an RF acknowledgement from ViPR B and generates a TCP ACK to send to Host A.  Host B receives the original TCP data packet and generates a TCP ACK to send back over the network.
5) ViPR B receives the TCP ACK but does not send it over the air saving bandwidth on the Airlink

| (1) TCP Packet over Ethernet | (2) TCP Packet over Airlink | (3) TCP Packet over Ethernet |
|---|---|---|

ViPR A
TCP Proxy Enabled

ViPR B
TCP Proxy Enabled

Host A

Host B

| (4) When ViPR A hears RF ACK it generates a TCP ACK and sends it to Host A | (3) RF ACK over Airlink (5) TCP ACK is not transmitted | (4) Host B generates TCP ACK. |
|---|---|---|
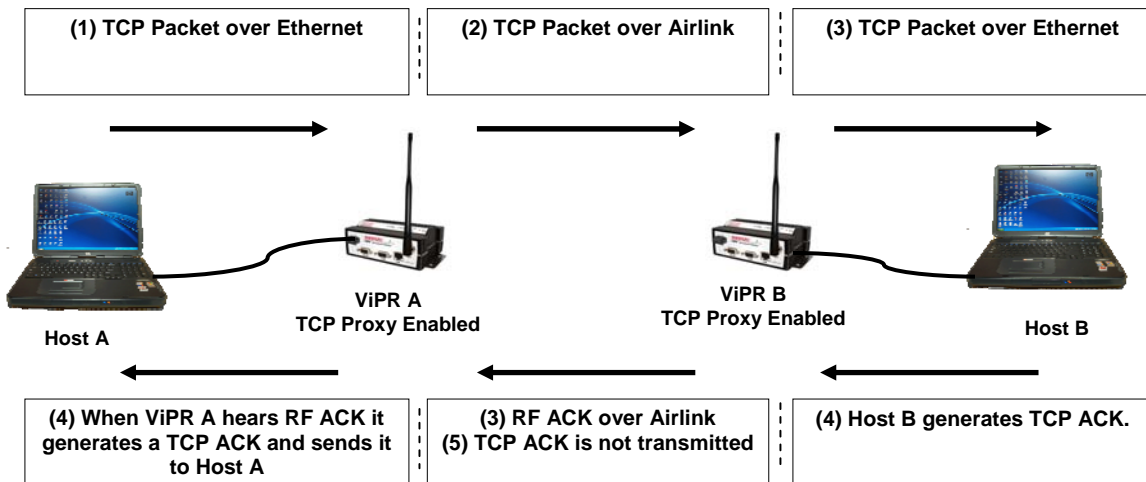
*Figure 7.22 TCP Proxy Example*

## 7.5  IP ROUTING (TABLE/ENTRIES)

**IP Routing**

**Routing Table**

| # | Destination Network | | Gateway | | Type |
|---|---|---|---|---|---|
| | IP Address | Netmask | IP Address | RF MAC | |
| 1 | 10.0.0.0 | 255.0.0.0 | 10.0.14.180 | | Connected |
| 2 | 10.0.14.180 | 255.255.255.255 | 10.0.14.180 | | Connected |
| 3 | 192.168.205.0 | 255.255.255.0 | 192.168.205.1 | | Connected |
| 4 | 192.168.205.1 | 255.255.255.255 | 192.168.205.1 | | Connected |
| 5 | 192.168.206.0 | 255.255.255.0 | 10.0.14.198 | 00:0E:C6 | Proprietary |
| 6 | 192.168.207.0 | 255.255.255.0 | 10.0.15.212 | 00:0F:D4 | Proprietary |

Refresh

**Routing Entries**

| Destination Network | | Gateway | |
|---|---|---|---|
| IP Address | Netmask | IP Address | RF MAC Address |
| | | | |

Add  Delete

*Figure 7.23 Setup (Advanced) ⇨ IP Routing Web Page*

▪ **Routing Table**

Displays the table of IP routes that are active in the ViPR. The routing table will be populated by the Neighbor Discovery process and/or by manual entries.

▪ **Destination Network**

Displays the IP Address and Netmask of a route.

▪ **Gateway**

Displays the IP Address and the RF MAC address (if route is pointing to another ViPR) of the destination gateway.

▪ **Type**

There are three different types of routes:

Connected:   Direct physical connection on the Ethernet port.
Static:   User-defined routes.
Proprietary:  Routes learned by the ViPR unit that point to over-the-air destinations.

▪ **Routing Entries**

This section allows the user to manually enter new routes or delete existing routes.

## 7.6  TIME SOURCE



*Figure 7.24 Setup (Advanced) ⇨ Time Source*

### 7.6.1  SNTP

Simple Network Time Protocol (SNTP) is a protocol for synchronization of clocks of computer systems (ViPRs) over the Internet.  When SNTP client is enabled the ViPR will poll the time server for the time information update.

- **Client**

Select: Enabled, Disabled; Default: Disabled

- **Server Address**

Default: 0.0.0.0
Enter the IP Address of the SNTP Server in dot decimal format.

- **Period**

Default: 64
Enter the period (in seconds) at which the SNTP Server is polled.

- **SNTP UTC Time**

0 (default)
Displays the last update received from the SNTP Server (in seconds).

### 7.6.2  Time Zone

- **Time Zone**

Select from List: local time zone; Default: (GMT) Greenwich Mean Time

- **Daylight Saving**

Select: Enabled, Disabled; Default: Disabled

## 7.7 ALARM REPORTING

**Diagnostics settings**

| Alarm Reporting | |
|---|---|
| Forward Power Alarm & Notification | ○ Enabled ⊙ Disabled |
| Reverse Power Alarm & Notification | ○ Enabled ⊙ Disabled |
| PA Power Alarm & Notification | ○ Enabled ⊙ Disabled |

Apply   Cancel

*Figure 7.25 Setup (Advanced) ⇨ Alarm Reporting*

The ViPR radio can be enabled to report several different types of alarms using the SNMP protocol.  If SNMP is enabled (Setup (Advanced) – IP Services) and reporting is enabled for a specific alarm, the ViPR will send an SNMP Trap to each of the IP addresses listed in the Trap IP List (Setup (Advanced) – IP Services) whenever an alarm occurs.

If the condition that caused the alarm clears, the ViPR will send a second SNMP Trap to each of the IP addresses listed in the Trap IP List, indicating that the error has cleared.

### 7.7.1 Forward Power Alarm & Notification

The Forward Power Alarm will trigger when the measured forward power drops 1 dB or more below the user configured transmit power.  The Forward Power Alarm SNMP trap is generated when this condition occurs.  When the forward power returns to within 0.8 dB of the wanted power the error is cleared and a second notification is sent indicating the error has cleared.

For example, assume the ViPR is programmed to transmit at 10W.  If the measured forward power drops below 7.9W then the error is detected and the SNMP Trap or Alarm is generated.  If the forward power then rises above 8.3W the error is cleared and a second SNMP Trap or Notification is generated.

### 7.7.2 Reverse Power Alarm & Notification

The Reverse Power Alarm will warn the user of a major problem with the Power Amplifier or Antenna, such as the antenna becoming disconnected. The alarm will trigger when the measured reverse power increases to within 3 dB of the user configured transmit power. The Reverse Power Alarm SNMP trap is generated when this condition occurs.  When the reverse power drops 5 dB below of the wanted power the error is cleared and a second notification is sent indicating the error has cleared.

For example, assume the ViPR is programmed to transmit at 10W.  If the measured reverse power increases above 5.0W then the error is detected and the SNMP Trap or Alarm is generated.  If the reverse power then drops below 3.1W the error is cleared and a second SNMP Trap or Notification is generated.

### 7.7.3  PA Power Alarm & Notification
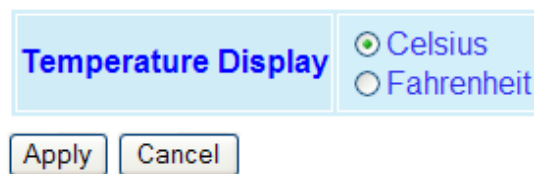
The PA Power Alarm & Notification will warn the user when the power amplifier goes into either a Foldback or Shutdown State.  The power amplifier will first go into the Foldback state if the PA temperature gets too hot.  In the foldback state, the ViPR will cut the transmit power in half every 4 minutes until the PA has cooled off.  The transmit power will not be reduced further if the power is originally set for 1W or reaches 1W due to foldback.

If the temperature continues to increase, the PA may go into Shutdown mode.  If this happens, another SNMP trap will be generated, indicating that the PA is Shutdown.  The ViPR will not transmit until the unit cools down.  This trap will not be sent over the air and will only be sent out the Ethernet interface.

When the temperature drops back to a safe level, the ViPR will resume transmitting at full power and the PA Power Notification SNMP Trap will be generated to indicate that the ViPR is operating at full power again.

### 7.8  USER SETTINGS

**User Settings**

| Temperature Display | ⊙ Celsius<br>○ Fahrenheit |
|---|---|

Apply  Cancel

*Figure 7.26 Setup (Advanced) ⇨ User Settings*

- **Temperature Display**

Select Celsius, Fahrenheit; Default: Celsius

## 8   SECURITY

Password Control and Access Control options offer user access to passwords, encryption settings, and access control tables.

The ViPR uses Advanced Encryption Standard (AES) 128 encryption.  AES 128 is a block cipher adopted as an encryption standard by the government.  The encryption is applied to the data passing through the Ethernet port and the serial ports.



*Figure 8.1 Security Web Page*

### 8.1   USER ID AND PASSWORD

▪ **User ID**

Enter a string up to 15 alphanumeric characters.

▪ **Old Password**

Default: ADMINISTRATOR
         (Case sensitive)

▪ **New Password**

Passwords are case sensitive and must be 8-15 characters in length.

*Warning: Ensure the passwords are recorded for future reference.  If your password is lost, contact CalAmp Technical Services to obtain a backdoor password.*

### 8.2 ENCRYPTION

▪ **Encryption**

Select: Enabled, Disabled; Default: Enabled.
ViPR offers 128-bit AES encryption.

▪ **Encryption Pass Phrase**

Default: Dataradio
Enter an encryption key composed of a string of up to 160 characters that will serve as the encryption pass phrase.

▪ **Encryption Key**

The encryption key generated is for display only and does not need to be recorded.
Ex. b3 35 b0 7b ba 8d eb 5d 44 66 3c 3a a7 16 f1 80

# 9 STATISTICS

The statistics page reports the amount of traffic received and sent by each of the three interfaces:  Ethernet, Serial, and RF.  This page also reports statistics gathered from the airlink that can indicate the quality of the RF links.

Note: All definitions given below use the following convention:
RX (or Input) = data received from a lower network layer
TX (or Output) = data transmitted to a lower network layer

Cycling power to the ViPR or pressing the "Clear (Zero) Interface Stats" button will reset all statistics to zero.

### Interfaces

| Ethernet | |
|---|---|
| **LAN**<br>RX Pkts<br>TX Pkts | 253<br>238 |

| Serial | | | |
|---|---|---|---|
| **Setup**<br>RX Bytes<br>TX Bytes<br>RX Pkts<br>TX Pkts | 0<br>0<br>0<br>0 | **COM**<br>RX Bytes<br>TX Bytes<br>RX Pkts<br>TX Pkts | 30000<br>1000<br>120<br>4 |

| RF | | | |
|---|---|---|---|
| **OIP sublayer**<br>RX Pkts<br>TX Pkts | 92<br>120 | **Airlink sublayer**<br>RX Ctrl Pkts<br>RX Data Pkts<br>TX Ctrl Pkts<br>TX Data Pkts | 325<br>92<br>290<br>129 |

| Airlink error detection | |
|---|---|
| Reliable service msg success count | 120 |
| Reliable service msg failure count | 0 |
| Total retry count | 0 |
| Noise detected count | 0 |
| Rx total "other" count | 0 |

Refresh    Clear (Zero) Interface Stats

*Figure 9.1 – Statistics Web Page*

## 9.1 ETHERNET (LAN)

▪ **RX Pkts (LAN)**

The total number of input packets received by the Ethernet interface.

- **TX Pkts (LAN)**

The total number of output packets transmitted by the Ethernet interface.

## 9.2   SERIAL

- **RX Bytes**

The total number of input bytes received by the port.

- **TX Bytes**

The total number of output bytes transmitted by the port.

- **RX Pkts**

The total number of input packets received by the port.

- **TX Pkts**

The total number of output packets transmitted by the port.

## 9.3   RF

- **RX Pkts (OIP Sublayer)**

The total number of input packets received by RF-OIP interface.

- **TX Pkts (OIP Sublayer)**

The total number of output packets transmitted by RF-OIP interface.

- **RX Ctrl Pkts (Airlink Sublayer)**

The total number of control packets received over-the-air.  These packets may be RTS/CTS messages or RF Acknowledgements.

- **RX Data Pkts (Airlink Sublayer)**

The total number of input data packets received over-the-air.

- **TX Ctrl Pkts (Airlink Sublayer)**

The total number of output control packets transmitted over-the-air.  These packets may be RTS/CTS messages or RF Acknowledgements.

- **TX Data Pkts (Airlink Sublayer)**

The total number of output data packets transmitted over-the-air.

## 9.4   AIRLINK ERROR DETECTION

Airlink parameters provide the user with RF link quality information.

- **Reliable Service Msg Success Count**

The number of service messages that succeeded.  RF Acknowledgements must be enabled in order to generate a Reliable Service Message.  RF Acknowledgements can be configured under Setup (Advanced) ⇨ IP Optimization (Router Mode Only).

- **Reliable Service Msg Failure Count**

The number of service messages that failed.

- **Total Retry Count**

The total number of retries for service messages.

- **Noise Detected Count**

The number of noise (non ViPR carrier) detected instances above the carrier sense level.  If the Noise detected count is high, it may be an indication the Carrier Sense Threshold should be raised.

- **RX Total "Other" Count**

This is the total number of messages the ViPR overheard that were intended for another station.  These messages are discarded.
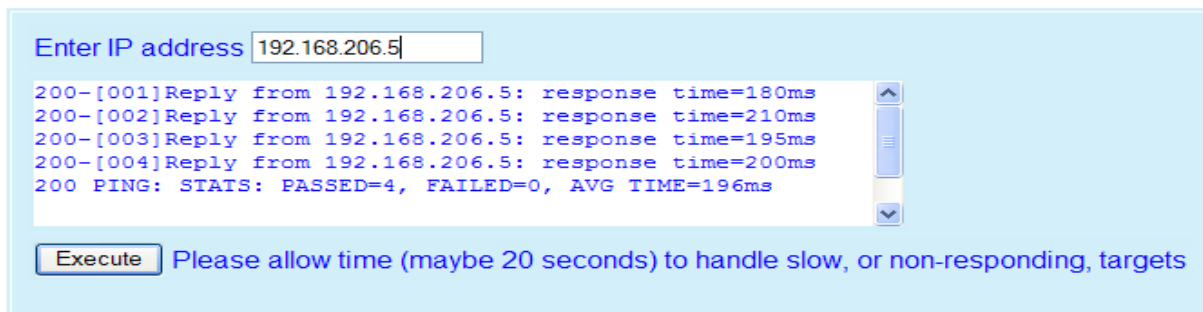
# 10 MAINTENANCE

## 10.1 PING TEST

The ping command is a network tool used to test whether a particular host is reachable on the IP network. It works by sending an ICMP packet (echo request) to a target host and listening for the ICMP echo response. Ping estimates the round trip time (in ms) and records any packet loss.

  a.  Enter IP Address

  b.  Press EXECUTE button

  c.  Allow up to 20 seconds to handle slow, or non-responding targets

### Ping Test

Enter IP address 192.168.206.5

```
200-[001]Reply from 192.168.206.5: response time=180ms
200-[002]Reply from 192.168.206.5: response time=210ms
200-[003]Reply from 192.168.206.5: response time=195ms
200-[004]Reply from 192.168.206.5: response time=200ms
200 PING: STATS: PASSED=4, FAILED=0, AVG TIME=196ms
```
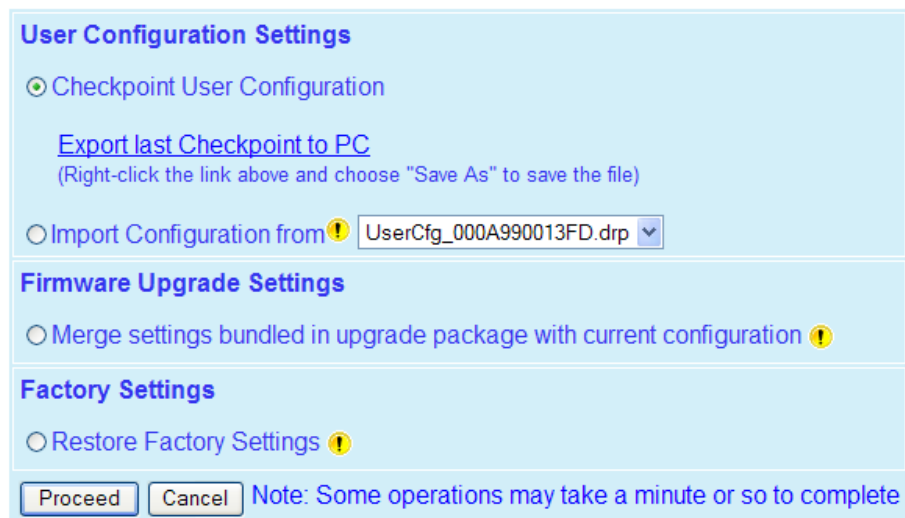
Execute  Please allow time (maybe 20 seconds) to handle slow, or non-responding, targets

*Figure 10.1 – Maintenance ⇨ Ping Test Web Page*

## 10.2 UNIT CONFIGURATION CONTROL

The Config Control web page grants the user access to the configuration settings below.  A user must click "Proceed" to execute the commands available on this screen.

### Unit Configuration Control

**User Configuration Settings**

⊙ Checkpoint User Configuration

   Export last Checkpoint to PC
   (Right-click the link above and choose "Save As" to save the file)

○ Import Configuration from ⚠ UserCfg_000A990013FD.drp ⌄

**Firmware Upgrade Settings**

○ Merge settings bundled in upgrade package with current configuration ⚠

**Factory Settings**

○ Restore Factory Settings ⚠

Proceed  Cancel  Note: Some operations may take a minute or so to complete

*Figure 10.2 – Maintenance ⇨ Config Control Web Page*

### 10.2.1  User Configuration Settings

▪ **Checkpoint User Configuration**

Select "Checkpoint User Configuration" radio button to create a checkpoint of all the user configurable settings in the ViPR.  Click "Proceed" to save these settings into the configuration file.  The configuration settings of the ViPR will be written to the UserCfg_*macaddress*.drp file (where *macaddress* is the ViPR's Ethernet MAC address. Example: UserCfg_000A990013FD.drp).  The new configuration set overwrites previously saved settings.

The configuration file contains all user settings that can be configured on any of the web pages as well as several additional parameters that can only be configured using the CLI (command line interface.)  Also, portions of the Routing Table and portions of the Neighbor Table are saved into the configuration file as described below.  The ViPR's password is not saved into nor restored from the configuration file.

<u>Neighbor Table</u>
**Dynamic Neighbors**:  Not Saved.  Dynamic neighbors are created and deleted automatically by the neighbor discovery algorithm and are not saved in the configuration file.

**Locked Neighbors**: Saved and Restored.  Locked neighbors are created automatically by the neighbor discovery algorithm but are not deleted automatically.  These entries are saved into the configuration file.

**Static Neighbors**:  Saved and Restored.  Static neighbors are created manually by the user.  These entries are saved into the configuration file.

<u>Routing Table</u>
**Connected Route**:  Not Saved.  These routes point to a direct physical connection on the Ethernet port and are created dynamically based on the ViPR's Ethernet IP address.

**Proprietary Route**:  Not Saved.  Routes added due to an entry in the neighbor table. These routes will be automatically recreated for each remote ViPR in the neighbor table.

**Static Route**:  Saved and Restored.  Static routes are created manually by the user.  These routes are saved into the configuration file.

▪ **Export Config from Last Checkpoint to PC**

Right Click this link, then select "Save Target As" to save the configuration file to a PC.  A save dialog box will appear.  Select the file name and folder to save the configuration file to and click save.

The configuration file may be renamed, if desired, (must keep the .drp extension) then reloaded back into the original ViPR or into another ViPR by using an FTP client program. Do not load more than 5 separate configuration files into a single ViPR.  Loading many configuration files into a ViPR may use up an excessive amount of memory and may cause the ViPR to malfunction.  After saving the configuration file back into the ViPR with an FTP Client, select "Restore User Configuration Checkpoint" and follow the instructions below.

▪ **Restore User Configuration Checkpoint**

To restore a user configuration file, click the "Restore User Configuration Checkpoint" radio button.  The drop down combo box will show all the .drp files (configuration files) in the

ViPR.  Select the configuration file to load and click on "Proceed".  Click "Save Config" then "Reset Unit" to complete the process and store these settings to the unit.

▪ **Firmware Upgrade Settings**

Merge settings bundled in upgrade package with current configuration - merges upgraded settings with the current configuration.  Select the "Merge Settings..." radio button and click "Proceed".  Click "Save Config" then "Reset Unit" to complete the process.

Note:  The "firmware upgrade" process will replace the ViPR existing configuration with the firmware bundled with the upgrade package.

▪ **Factory Settings**

Restore Factory Settings restores all settings to the default factory configuration.
If at any time you wish to restore factory settings, simply select the "Restore Factory Settings" radio button and click "Proceed".  Click "Save Config" then "Reset Unit" to complete the process.

*Important note:*
*Activating "Restore Factory Settings" will reset the IP address of the unit.*
*Review your record of the original ViPR factory settings before proceeding with the Restore Factory Settings.*

## 10.3 PACKAGE CONTROL

The Package Control web page is used for verifying a field upgrade of the ViPR radio modem firmware.  If the installation was successful, the web page will indicate "Pass".  If the installation is unsuccessful, the web page will indicate "Fail" and an error message will specify which files are missing/corrupt.

If an upgrade problem arises, click the "Package Control" once more and have the results available when contacting CalAmp Technical Support.

The Package Validation window is for reference only. No user configuration is available on this page.

**Package Validation**

```
200-Package Name: distrib.pkg
200-Minor: 0
200-Major: 1
200 Package distrib.pkg is valid
Result: PASS
```

*Figure 10.3 – Maintenance ⇨ Package Control Web Page*

## 10.4  NET TESTS

The Net Tests web page allows the user to test the reliability of the RF link.  Test packets are generated and transmitted with a special ViPR specific test bit set in the header to identify the packet as a test packet.  The receiving ViPR listens for these test packets and

counts the number of packets it receives successfully. The test results can be viewed on the receiving ViPR.

**Warning: When the unit is in test mode, it will not respond to RF activity from other ViPR units. Test mode cannot be enabled (active) for more than 15 minutes. After 15 minutes, test mode will be automatically disabled and normal communications will resume.**

**Net Tests**

| Net Test Setup | | |
|---|---|---|
| **Destination RF MAC address** | 0xFFFFFFFF | Default: 0xFFFFFFFF Range: [1 - 0x00FFFFFF] |
| **Number of packets to transmit** | 1000 | Default: 1 |
| **Delay between packets** | 50 | Default: 0 [msec] |
| **Packet data pattern** | ○ Fixed ⊙ Random | |
| **Packet data type** | ○ ASCII ⊙ Binary | |
| **Length of data payload** | 250 | Default: 2 Range: [2 - 1500] |
| **Lock PTT between packets** | ○ ON ⊙ OFF | Default: OFF |
| **!!! Warning !!! The test mode cannot be enabled (active) for more than 15 minutes !!!** | | |
| **Test Mode** | ⊙ Enabled ○ Disabled | |
| | Start Test   Stop Test   Show Stats   Clear Stats | |

*Figure 10.4 – Maintenance ⇨ Net Tests Web Page*

**10.4.1  Net Test Setup**

▪ **Destination RF MAC address**

The user enters the RF MAC address of the ViPR unit they wish to connect to.  Format 0x00000FD4.  The default RF MAC address is 0xFFFFFFFF, which will send a broadcast packet to all ViPRs listening for the test packets.

▪ **Number of packets to transmit**

This is the total number of packets transmitted during the test.

▪ **Delay between packets**

The user can enter a delay in milliseconds between the packets being sent. Note:  If a delay is not present between packets, it may appear the transmitter does not unkey and is only sending one long continuous packet.

▪ **Packet data pattern**

The user can choose between a Fixed or Random data pattern.  Fixed data is highly compressible; random data is not.  Note:  The ViPR has a data compression algorithm that compresses the data before transmitting it.

- **Packet data type**

Choose from ASCII or Binary (Hex) formats.  ASCII data type is also highly compressible.
Note: Random Binary data best simulates PLC SCADA data.

- **Length of data payload**

Enter the length of the data to be transmitted.  Note: A typical SCADA value would be
between 10 to 250 bytes. The maximum value is equal to the MTU set in each ViPR unit.

- **Lock PTT between packets**

If the "Off" option is chosen and enough delay has been added between packets, the ViPR
will stop transmitting between packets. If "On" is selected the ViPR will continuously
transmit between packets.

- **Test Mode**

Clicking the "Enable" radio button will put the ViPR into test mode and the ViPR will
immediately begin listening for test packets transmitted from a remote unit.  As the unit
receives test packets, the statistics will be updated.  The statistics can be viewed by clicking
the "Show Stats" button.  Click the "Start Test" button to have the ViPR start transmitting
test packets to a remote unit.

- **Start Test**

Starts the test.  When this button is clicked, the ViPR will begin transmitting test packets.
The "Start Test" button does not need to be clicked on the receiving ViPR.  The ViPR will
start listening for test packets as soon as the Test Mode "Enabled" radio button is selected.

- **Stop Test**

Stops the test. When this button is clicked, the ViPR will stop transmitting test packets.

- **Show Stats**

Clicking the "Show Stats" button will cause a pop up window that displays the test statistics.
Note:  The user should use this feature on the receiving unit to monitor the Net test.  This
window will also display the RSSI value from the transmitting unit.

- **Clear Stats**

Clears the results of the test.

### 10.4.2  Net Test Results

Click on the "Show Stats" button to display the test results.  A typical results page with the
results from the transmitting ViPR is shown below.  The left column lists current results.
The right column shows results from the last time the stats were refreshed.

- **Stats from Transmitting Unit**

In this example, 1000 of 1000 packets were successfully transmitted.  (Note:  This doesn't
imply how many packets were successfully received.  Check the stats on the receiving ViPR
for this information.)

## Net Test Statistics

**RSSI Display**

```
Net Test Statistics

    Net test RX Packets:. . . . . . 0              0
    RSSI: 0.000      [dBm] from [00:00:00]

    Net test TX Packets:. . . . . . 1000           1000
    Net test TX Conf: . . . . . . . 1000           1000
    Net test TX Failed: . . . . . . 0              0

    Net test: 1000 of 1000 packets completed.
```

RSSI (dBm)
Range (-120:-40)

-50
-60
-70
-80 dBm
-90
-100
-110

[ Refresh ] [ Zero Stat ]

**Ready**
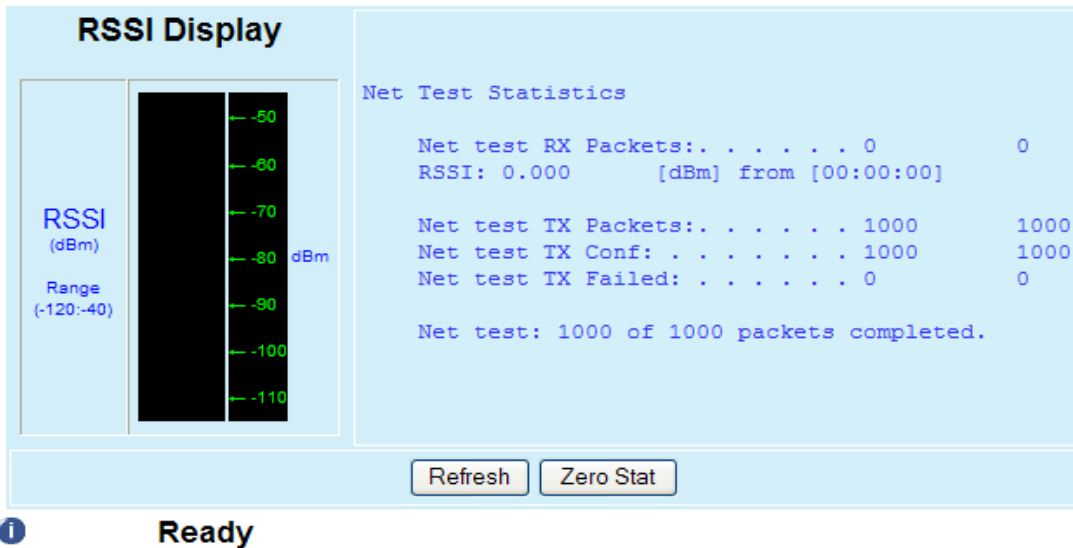
*Figure 10.5 – Net Test Statistics (Transmitting Unit) Web Page*

- **Stats from Receiving Unit**

In this example, 1000 test packets were successfully received and the RSSI from unit 00:01:2A (the sending ViPR) was –66.523 dBm.

## Net Test Statistics

**RSSI Display**

```
Net Test Statistics

    Net test RX Packets:. . . . . . 1000           1000
    RSSI: -66.523    [dBm] from [00:01:2A]

    Net test TX Packets:. . . . . . 0              0
    Net test TX Conf: . . . . . . . 0              0
    Net test TX Failed: . . . . . . 0              0

    Net test: 50 of 50 packets completed.
```

RSSI (dBm)
Range (-120:-40)

-50
-60
-70
-80 dBm
-90
-100
-110

[ Refresh ] [ Zero Stat ]

**Ready**
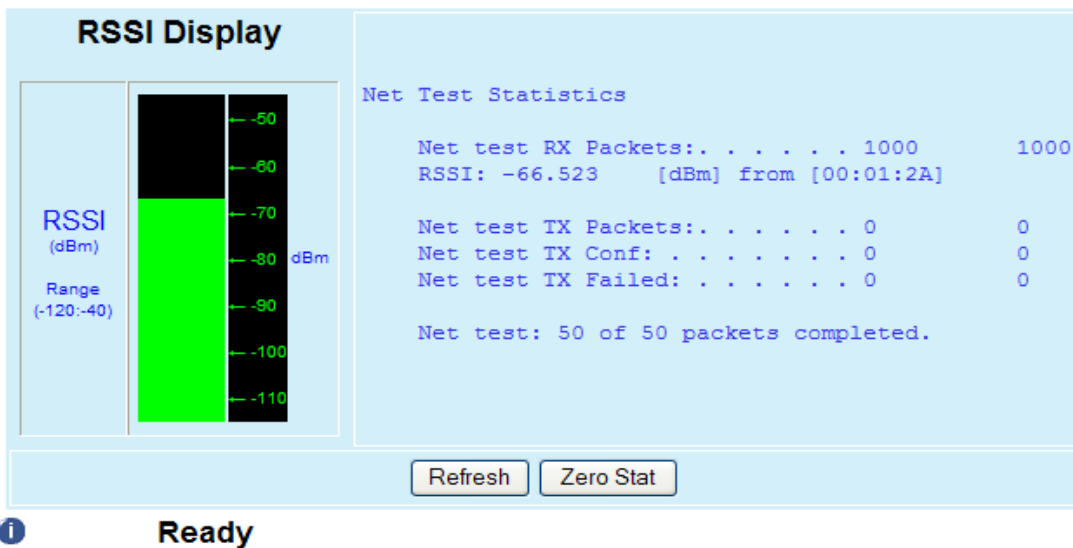
*Figure 10.6 – Net Tests Statistics (Receiving Unit) Web Page*

## 10.5 RF TESTS

▪ **Test Tones**

Allows the user to choose from Unmodulated, Random Data, and 1 KHz Sine Wave test tone.

The test tone will transmit for 20 seconds when the "Start Test" button is clicked.  The "Stop Test" button will end the test immediately.  Note:  This test may cause other ViPRs to stop transmitting for the duration of the test.  ViPR units have a feature that checks if another carrier (RX frequency signal) is present.  If a carrier is detected, the ViPR will not transmit until the carrier is no longer present.



*Figure 10.7 – Maintenance ⇨ RF Tests Web Page*

## 10.6 FEATURE OPTIONS

The Feature Option web page lists the available add on features and shows which features are currently installed in the ViPR.

| Option # | Name | Description |
|----------|------|-------------|
| 009 | SNMP | Allows SNMP agent activation on the unit. |

*Table 10.1 – Available Feature Options*

## 11 NEIGHBOR MANAGEMENT

Each unit is equipped with a powerful neighbor discovery module whose purpose is to detect all units in the RF network and add all necessary IP routes required to reach neighboring units. **The neighbor discovery module only operates when the unit is configured in router mode**. ViPRs discover other ViPRs by sending and receiving neighbor discovery control messages.

There are three modes of operations (Manual-Scan, Auto-Scan, Disabled); five states of operations (Ready, Scanning for Neighbors, Disabled, Saving Neighbor Table, Testing Connectivity); and three types of Neighbor Table entries (Static, Dynamic, Locked).

### 11.1 USER INTERFACE

The User Interface grants access to ViPR Neighbor Management options and displays information about local status, discovered neighbors, and control operations.



*FIGURE 11.1 - NEIGHBOR DISCOVERY USER INTERFACE*

### 11.2 NEIGHBOR DISCOVERY (MODES)

Neighbor Discovery mode must be configured the same for each ViPR in the network.

### 11.2.1 Manual-SCAN

Manual-Scan is the default mode of operation. The ViPR starts in the "Ready" state. In the "Ready" state, the unit is quiet (no neighbor discovery control messages are sent).  If the user presses the "Force Scan" button, the unit goes into the "Scanning for Neighbors" state. If other units are in the "Scanning for Neighbors" state, the unit will automatically be triggered to go into the "Scanning for Neighbors" state.

In the "Scanning for Neighbors" state, the ViPR is learning about other units and the other units are learning about this unit.  The unit goes from the "Scanning for Neighbors" state to the "Saving Neighbor Table" state when it doesn't learn anything new for a given amount of time.

In the "Saving Neighbor Table" state, the content of the neighbor table is saved in nvram (nonvolatile ram).  If the unit reboots, the content of the neighbor table is restored from the nvram.

The unit goes from the "Saving Neighbor Table" state to the "Ready" state.

### 11.2.2 Auto-SCAN

In the Auto-Scan mode, ViPR begins "Scanning for Neighbors".  In the "Scanning for Neighbors" state, ViPR discovers other ViPR units in the network and other ViPR units learn about the ViPR initiating the scan.

ViPR goes from "Scanning for Neighbors" state to "Ready" state when it doesn't discover another ViPR for a given amount of time.

In "Ready" state, ViPR will generate a "keep alive" packet periodically. In "Ready" state, ViPR performs broken link detection. ViPR is monitoring the "keep alive" packets of other ViPRs (1 hop away).  ViPR knows the interval period for other ViPRs generating their "keep alive" packets.  If ViPR (A) fails to receive four "keep alive" packets in a row from ViPR (B), ViPR (A) removes ViPR (B) from its neighbor table and goes into the "Scanning for Neighbors" state.

If a user presses the "Force Scan" button, ViPR goes into the "Scanning for Neighbors" state.  If other ViPRs are in the "Scanning for Neighbors" state, ViPR will automatically go into "Scanning for Neighbors" state.

Note: Care should be taken when selecting Auto-Scan mode for the permanent operating mode of a ViPR network.  Auto-Scan mode could generate a large number of neighbor discovery control messages in a large ViPR network

### 11.2.3 Disabled

In the disabled state, ViPR does not send neighbor discovery packets, nor does it process neighbor discovery packets generated by other ViPRs.  The user can enter static entries in the Neighbor Table.

### 11.3 LOCAL STATUS

Local Status displays operating state information about the local discovery module.  The device shown in Figure 11.2 is currently Scanning for Neighbors.  See below for additional Discovery States.

*Figure 11.2 ViPR "Scanning for Neighbors"*

### 11.3.1 Neighbor Discovery States

- **Ready**

The neighbor discovery module is in a "Ready" state when it is not scanning for other units.

If the ViPR is operating in Manual-Scan, it does nothing.

If the ViPR is operating in Auto-Scan, it monitors the "keep alive" packets of other units and sends its own "keep alive" packet periodically.

- **Scanning For Neighbors**

The neighbor discovery module is trying to learn about other units.  Other units are learning about this unit.

- **Saving Neighbor Table**

In this state, the ViPR is saving all neighbor entries of type "Dynamic" into Nvram.  When the save is complete, all these entries are now of type "Locked". This state only occurs when the neighbor discovery module operates in Manual-Scan mode.

- **Testing Connectivity**

The neighbor discovery module is verifying the ViPR units in the neighbor table are reachable by sending them an alive-request and waiting for an alive-response. Round trip time must not exceed 10 seconds.  The alive-request is only sent once.

- **Disabled**

The neighbor discovery module is disabled.

### 11.3.2    Neighboring ViPRs Found

Displays the number of ViPRs discovered.

### 11.3.3   Discovery Duration

Discovery Duration is the time it took for the ViPR unit to complete the neighbor discovery learning process.

### 11.4 DISCOVERED VIPR NEIGHBORS

Each entry in the Neighbor Table represents a remote ViPR.  See Figure 11.1: Discovered ViPR Neighbors.

### 11.4.1  Information on Neighboring ViPRs

- **RF MAC Address**

Identifies each entry uniquely. The user can click the RF MAC ADDRESS entries to display the details of the selected device in the Neighbor Node Detail window.

- **RF IP Address and Ethernet IP Address**

Used to build the routing table.

- **Discovery Mode**

Represents the Mode of operation of the remote Unit.  See 11.2 for more information on Neighbor Discovery Modes.

### 11.4.2  Neighbor Table Entry Type

- **Static**

This entry has been defined by the user.  The entry type can only be removed by the user. This entry cannot be replaced by a "Dynamic" or "Locked" entry.

"Static" neighbor entries can be added in any neighbor discovery mode.

If the user presses the "Save" button from the web page, all "Static" neighbor entries are saved in nvram.  They are recovered after a reboot.

- **Dynamic**

A "Dynamic" neighbor entry is one that has been learned by the neighbor discovery algorithm. It can be updated or deleted by the neighbor Discovery algorithm when it detects changes in the topology.

- **Locked**

A "Locked" neighbor entry is a "Dynamic" neighbor entry saved into nvram. The "Locked" neighbor entry behaves like a "Dynamic" neighbor except it is saved into nvram and will be recovered after a reboot.

### 11.4.3 Route to Neighboring ViPRs

- **Hop Count and Next Hop**

Indicates the route the remote ViPR can be reached - when HOP COUNT is 1, the device can be reached directly. When HOP COUNT is more than 1, it can be reached by passing though another ViPR as identified by the NEXT HOP field.

### 11.5 CONTROL OPERATIONS

- **Clear List**

Clears the entries in the list and routing tables. If Auto-Scan is enabled, the neighbor list will be repopulated automatically. If Manual-Scan is enabled, the neighbor list can be repopulated by clicking the "Force Scan" button.

- **Force Scan**

Starts the Scanning for Neighbors process.

- **Test Connectivity**

Pings each ViPR in the list to ensure an RF path between the units.

- **Add Static Entry**

| Add static neighbor entry | | | |
|---|---|---|---|
| RF MAC Address | 80:01:0A | | |
| RF IP Address | 10.128.1.10 | RF netmask | 255.0.0.0 |
| Ethernet IP Address | 192.168.206.1 | Ethernet netmask | 255.255.255.0 |
| Hop Count | 1 | | |
| Next Hop | 80:01:0A | | |
| Description | ViPR #2 | | |
| Attributes | ☐ Access Point ☐ Relay Point ☐ TCP Proxy ☐ NAT | | |

Apply   Cancel

By pressing the "Add Static Entry" button, a popup appears and the user can add a new static neighbor entry. To create the new neighbor, completely fill in all the information asked for in the pop-up window. The requested fields are described below. Finally, the user must press the "Apply" and "Save Config" buttons for the new entry to be added to the

network Routing Table.  When a Static Neighbor entry is created, all IP routes to that neighbor are created.

RF MAC Address:    The default RF MAC address is the last six digits of the Ethernet MAC that is found on the label on the bottom of the ViPR.  Also you can verify the current RF MAC that is being used in the remote radio by checking the Setup (Basic) ⇨ IP Settings web page of the remote unit.  Enter the current RF MAC address of the remote radio into this field.

RF IP Address:     Enter the RF IP address of the remote ViPR.
RF netmask:        Enter the RF netmask of the remote ViPR.
Ethernet IP Address: Enter the Ethernet IP address of the remote ViPR.
Ethernet netmask:  Enter the Ethernet netmask of the remote ViPR.

                   The RF IP address, RF netmask, Ethernet IP Address, and Ethernet netmask can all be obtained from the Setup (Basic) ⇨ IP Settings web page of the remote unit.

Hop Count:         Enter the number of RF hops required to reach the remote ViPR.
Next Hop:          Enter the RF MAC address of the next ViPR that data packets must first go to before being repeated on to the remote ViPR.  If the ViPR you are adding is only one hop away, enter the RF MAC address of the ViPR you are adding.

                   If you are setting up a system with multiple hops (with relay/repeater points), you must first enter remote ViPRs into the neighbor table that are 1 hop away before adding ViPRs that are 2 or more hops away.  This insures that the ViPR will recognize the RF MAC address of the "Next Hop" ViPR as you setup routes to ViPRs that are 2 or more hops away.

Description:       Enter the Station Name of the remote ViPR.  The Station Name can be obtained from the Setup (Basic) ⇨ General Settings web page of the remote unit.

Attributes:        Check the attributes that the remote ViPR has enabled: Access Point, Relay Point, TCP Proxy, and/or NAT (Network Address Translation).

**NOTE:**
Static Entries can replace dynamic entries.
Static neighbor entries do not age out.
Static neighbor entries are stored even when neighbor discovery is disabled.

▪ **Delete Entry**

By pressing the "Delete Entry" button, a popup appears and the user can specify the neighbor entry to be deleted.  Enter the RF MAC address of the neighbor to be deleted.  The neighbor entry can be a dynamic or static entry.

The neighbor discovery module updates ViPR's Routing Table when entries are added or deleted from the Neighbor Table.  See Section 7.5: IP Routing for more information.

## 11.6 PRIMARY AND BACKUP ROUTE SELECTION

If the user clicks on the RF MAC Address of a Unit in the neighbor table, the Neighbor Node Detail window appears with a full description of the selected device.

*Figure 11.3 - Neighbor Node Detail Window*

The Neighbor Discovery module will keep track of two routes determined by the shortest hop count to any given ViPR - the primary route and the backup route (if a route is detected).  Users can override the Neighbor Discovery selection by pressing the "Toggle Primary/Backup Routes" button.  The backup route will become the active route.

In certain applications, it may be necessary to edit Primary and/or Backup routes.  Select the desired unit; enter the RF MAC Address in the appropriate NEXT HOP field and the Hop Count to reach that unit.  Then press the "Apply" button.  If a route from ViPR #1 to ViPR #3 goes through ViPR #2.  The route selected must be edited in ViPR #1 and ViPR #3.  The routing path must use the same ViPRs going out and coming back.

**IMPORTANT!**
If the user changes the selection made by the Neighbor Discovery module, the neighbor entry will be changed from a dynamic entry to a static entry.

## 11.7 NETWORK STATUS

Network Status displays the Station Status, Neighbor Discovery (ND) mode and Command Status for each RF-MAC address in the Neighbor List.  The commands are generated on the Neighbor Management Maintenance page. If the command fails, the status will indicate either failure or Response Timeout



*Figure 11.4 Network Status*

To query the ViPR for the status of all its neighbors, select the Get Status option then press the "Apply" button under Network Management ⇨ Maintenance.

## 11.8 MAINTENANCE

The Network Maintenance page allows the user to make changes to a single ViPR unit or the entire ViPR network.  This allows the user to make changes to the remote units' neighbor tables.



*Figure 11.5 Network Maintenance*

▪ **Delete Station**

The user enters the RF MAC Address of the station to be deleted from the Neighbor Table of all ViPRs in the network.

▪ **Replace Station**

The user enters the old RF MAC Address (the unit to be replaced) and the new RF MAC Address (that will replace the old ViPR).  This will update the Neighbor Table of all the ViPRs in the network.

▪ **Change ND mode**

The user can change the Neighbor Discovery mode of all ViPRs in the network to Manual-Scan, Auto-Scan, or Disable.

▪ **Save Configuration**

This will send a save configuration command to all ViPRs in the network.

▪ **Get Status**

This will send a "Get Status" command to all ViPRs in the network.  The status will be displayed on the Network Management ⇨ Status page.

- **Single Station**

Single Station allows the user to enter the single RF MAC Address of the ViPR module commands will be sent to. If this option is selected, the command will be sent to an individual ViPR instead of being sent to all ViPRs in the Network.

- **Apply**

The commands will not be sent until the "Apply" button is clicked.


## 11.9 RECOMMENDED NEIGHBOR DISCOVERY MODES OF OPERATIONS

CalAmp recommends Auto-Scan be limited to ViPR networks of two to ten units. If Auto-Scan mode is used, be aware the Neighbor Discovery learning process may slow responses in SCADA networks from remote units or capture the RF channel so remotes cannot respond to a Master.

Manual-Scan is recommended for most projects.

Disabled is recommended in projects where the customer does not want RF paths to deviate from RF engineered (RF Site Survey completed) paths.

## 12  NETWORK OPTIMIZATION

### 12.1 MAXIMIZING TCP/IP THROUGHPUT

After optimizing the Airlink, if there appears to be an unexplained speed loss, you can attempt to maximize TCP/IP throughput.

TCP/IP throughput can be a challenge to measure as performance is related not only to the RF link, but how well flow-control is implemented in the TCP/IP stack and each application's design. ViPR has been optimized with this in mind. When the TX/RX LED flashes green or red, this indicates data is moving across the network.  It also indicates (by the LED OFF periods) when data is not moving across the RF network at full rated speed.  OFF periods indicate the application has not presented data to the ViPR radio modem.

Using different client/server combinations or applications may show improvements.  For instance, one FTP server may work 30% faster than another; the buffer management is quicker to respond or has bigger message buffers – yet run at nearly the same speed over a pure Ethernet (no RF) link.

Network Address Translation (NAT), payload data compression, and encryption have little effect other than adding a small latency to the flow of traffic.

### 12.2 MAXIMIZING THROUGHPUT WITH A WEAK RF LINK

Further performance optimization can be done via the User Interface Setup web pages. Fundamental adjustments, described in the following paragraphs, can be changed singularly or in conjunction with each other.

#### 12.2.1  Use Router Mode with RF Acknowledgements Enabled

Selecting Router mode and enabling RF Acknowledgements is highly recommended when running over a weak RF link. This mode ensures several levels of retry mechanisms are at work, each optimized to minimize TCP flow control delays or prevent a dropped TCP/IP link. It requires some IP route planning to and from ViPR units, but is well worth the increase in link stability over the simple Bridge mode.

RF Acknowledgements can be enabled on ViPR web pages under Setup (Advanced) ⇨ IP Optimization. RF Acknowledgements must be enabled or disabled on all ViPRs in the network.

ViPRs are tested for BER at the factory with the optimizations described above. The units are configured for Router Mode, RF Acknowledgements are enabled, MAC retries are set for 2, and OIP retries are set for 2.

#### 12.2.2  Reduce RF Network Bit Rate

ViPR has two speeds of operation available for each of the three channel bandwidths. The faster speeds in each bandwidth utilize 4-level FSK (frequency shift keying.)  The slower speeds in each bandwidth utilize 2-level FSK, yielding a higher Signal-to-Noise level resulting in better sensitivity.  Normally the system is able to utilize the faster bit rate. However, if the system has a very low signal level (-95 dBm or less) or the RF signal levels are close to an elevated noise floor level, you can try running at a slower over-the-air speed for the system's bandwidth. It may result in better overall performance.

### 12.2.3  Increase OIP and MAC Retries Limit

OIP retries and MAC retries are only available in Router mode.  The MAC Retry Limit is normally set to 1 and the OIP Retry Limit is normally set to 2.  Gradually increasing these limits (up to 3 in extreme cases), may provide a slower, but more reliable link impossible with weak signals.  Use in conjunction with the slower over-the-air network bit rate for the system's bandwidth.

The number of MAC retries can be configured on the ViPR's web pages under Setup (Advanced) ⇨ RF Optimizations.  The number of OIP retries can be configured under Setup (Advanced) ⇨ IP Optimization.

# 13 UPGRADING YOUR FIRMWARE

The ViPR radio modem firmware is field-upgradeable using the unit's Ethernet port. The process involves connecting to the IP address of the ViPR from a host PC and transferring firmware files via a Files Transfer Protocol (FTP) program.

There are two sets of code in the ViPR Radio.  The first set of code is the Modem Firmware and must be updated every time a software upgrade is needed.  The revision number for the Modem Firmware is listed under the "REV" column in the table below.  The second set of code is the Radio Firmware.  This firmware resides on the ViPR transceiver PC Board and requires the user to manually start the upgrade process.   It is likely the Radio Firmware will not have to be upgraded each time the Modem Firmware is upgraded.

The first upgrade step involves using an FTP program to load the Modem Firmware into the ViPR.  Do this by following the steps outlined in section 13.2.  The Modem Firmware package will contain the new Radio Firmware file (vipr_radio.bin), if any, and will be uploaded along with the other Modem Firmware files.

The second upgrade step, if needed, involves connecting to the ViPR's CLI (command line interface) and executing the upgrade command as outlined in section 13.3.

## 13.1 SOFTWARE RELEASE HISTORY

| REV | DATE | REVISION DETAILS |
|-----|------|------------------|
| 1.0 | 12-17-2007 | Initial Release |
| 1.1 | 01-08-2008 | Eliminate false error reporting on web pages |
| 1.2 | 01-15-2008 | Radio firmware update:  ViPR-02_10-R<br>   - Delay turning on fan to reduce surge current when starting to transmit<br>   - When ending transmit in ETSI mode, some of the transmitter stages were not being controlled correctly |
| 1.3 | 09-22-2008 | Added SNMP Feature<br>   - SNMP is tied to a Feature Key and requires license.opt file with the correct pass code to operate.<br><br>Radio firmware update: ViPR-2_20-R<br>    - Includes upgrade to enable Forward and Reverse Power SNMP traps. |
| 1.4 | 12-16-2008 | - Added TCP Client/Server Mode for the serial ports.<br>- Updated the user interface for saving and restoring a ViPR User Configuration.<br>- Bug fix related to generation of incomplete IP Routing Table when setting up a system with many hops.<br>- Updated reporting for DSP alarms. |

| 1.5 | 4-3-2009 | - Added TCP Proxy Feature<br>- Added support for 900 MHz ViPR<br>- Added support for ViPR Infrastructure<br><br>Radio firmware update: ViPR-03_00-R<br>    - Added support for 900 MHz ViPR and for ViPR Infrastructure |
|-----|----------|-------------------------------------------------------------|
| 1.6 | 6-9-2009 | - Added Listen Before Talk Disable Feature<br>- Added RF MAC override Feature<br>- Added Periodic Reset Timer<br>- Bug fix related to Power PC lockup when resetting the DSP. |

## 13.2 UPGRADE MODEM FIRMWARE PROCEDURE

1. Using a file decompression program, such as WinZIP™ (built into WinXP), right-click and select the EXPAND TO option.  Expand the contents of the firmware upgrade package to a directory of your choice on the host PC.

2. Using an FTP program of your choice, establish a connection to the unit's IP address. The unit may prompt the user for a "Username" and "Password" depending of the FTP application used.

3. Transfer all files in the upgrade package. Occasionally, long pauses, on the order of 30 to 45 seconds, are possible when storing the file in the unit's flash file system.

   *Warning: Only transfer Dataradio ViPR files. Do not transfer any zip folders that might be included in the firmware upgrade package.*

*Failure to follow the recommended procedure as detailed above may result in unit becoming unresponsive.*

4. If you are upgrading from version 1.2 or older, transfer the license.opt file corresponding to the ViPR's MAC Address.  The license.opt file will enable the SNMP feature and is tied to the ViPR's MAC Address.  Contact CalAmp for information about obtaining the SNMP feature.

5. Once the file transfer is complete, cycle power and allow the unit to boot.  The ViPR should return to its pre-update state.

Note:
After resetting, the Status LED should be steady green.  If it is steady red, the FTP transfer may not have been successful or the firmware is corrupt.  See Verify File Integrity below.

## 13.3 UPGRADE RADIO FIRMWARE

If the radio firmware revision has been upgraded in the new package, follow these steps to complete the upgrade process.

1. First upgrade the ViPR Modem Firmware as outlined in section 13.2

2. Telnet into the ViPR or access the CLI (command line interface) through the serial port.

   Example:  Telnet using Windows Command Prompt program.
   Open Windows Command Prompt.  Type the following command then press enter:
       telnet *vipr_ip_address*
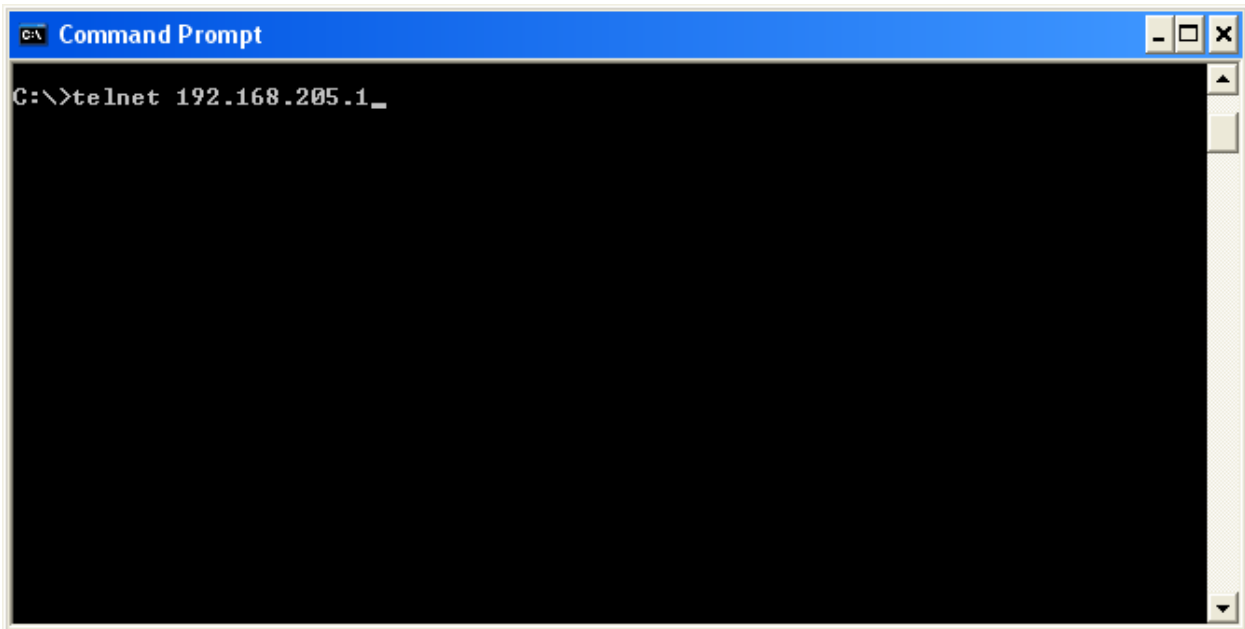
*Figure 13.1 Use Windows Command Prompt to Telnet to ViPR Radio.*

3. Enter in your username and password.
4. Type the following command then press enter:
   *radio.upload.firmware.binary –v –f vipr_radio.bin*

   You should see the following message in return:
   100-Loading file "vipr_radio.bin"...
   100-File imported successfully.
   100-Entering flash programming mode...
   100-Erasing flash...
   100-Programming flash...
   100-Restarting radio...
   200-OK.
   200 Done
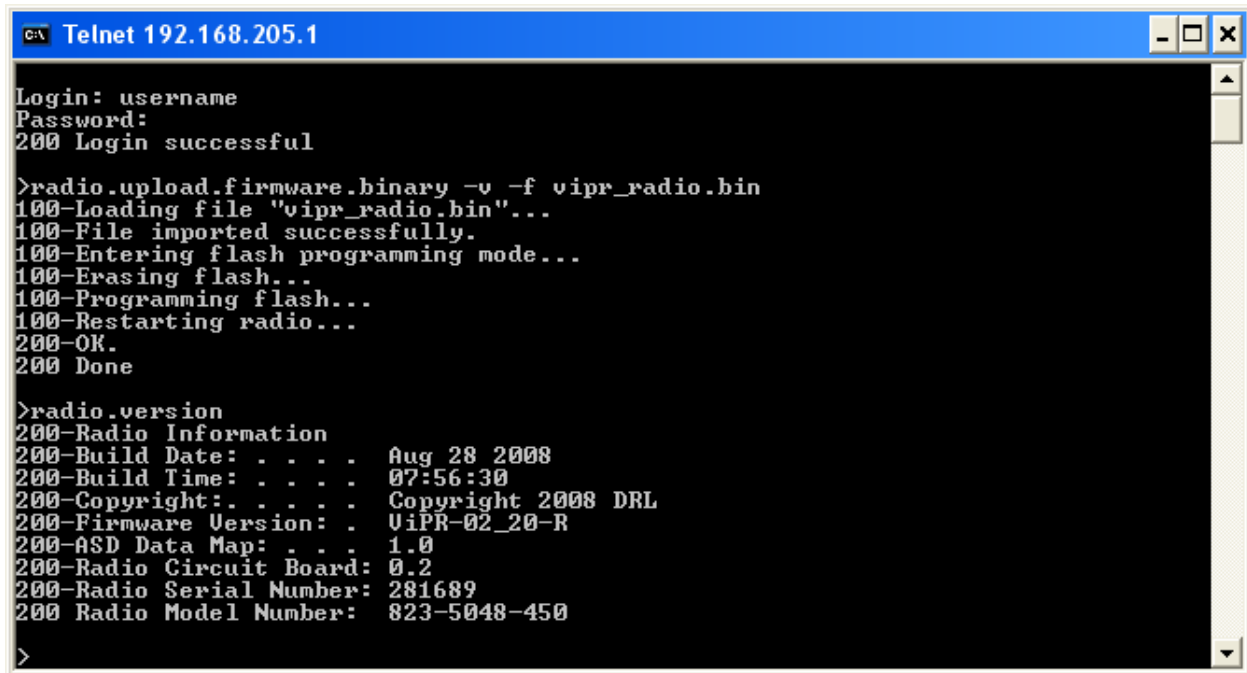
Type the following command, then press enter to verify the radio firmware is the most recent:
   *radio.version*

   You should see a message similar to this:
   200-Radio Information
   200-Build Date: . . . . Aug 28 2008
   200-Build Time: . . . . 07:56:30
   200-Copyright:. . . . . Copyright 2008 DRL
   200-Firmware Version: . ViPR-02_20-R
   200-ASD Data Map: . . . 1.0
   200-Radio Circuit Board: 0.2
   200-Radio Serial Number: 281689
   200 Radio Model Number:  823-5048-450

   Check that the "Firmware Version:" shows the latest firmware revision.

*Figure 13.2 Using Windows Command Prompt to upgrade Radio Firmware.*

5.  Restart the ViPR.
    Tip:  You can restart the ViPR by typing "*stationreset*" in the CLI then pressing enter.

**13.4 VERIFY FILE INTEGRITY**

1.  Using your browser, connect to the unit's IP address.

2.  Enter the user name and password.  Allow the Welcome page to load.

3.  In the left pane, select UNIT STATUS.  The Unit Identification and Status pane should display the newly upgraded firmware in its Banner and the H/W Status should also show Ok.

4.  In the left pane, select MAINTENANCE ⇨ PACKAGE CONTROL.  Wait a few moments for the results to display.

If the message in the result screen points out that file(s) failed the integrity check, retry the FTP transfer for the failed files(s) again.  If the problem persists, please have the PACKAGE CONTROL results ready and contact CalAmp Technical Services at the numbers provided in the front of this manual.

These specifications are typical and subject to change without notice.

| GENERAL | VHF | UHF | 900 |
|---|---|---|---|
| Frequency Range (MHz) | 136 – 174 MHz<br>215 – 240 MHz | 406.125 – 470.000 MHz,<br>450.000 - 511.975 MHz | 928 – 960 MHz |
| Frequency Stability | 1.0 ppm | 1.0 ppm | 1.5 ppm |
| Channel Bandwidth | 6.25 kHz<br>12.5 kHz<br>25 kHz | 6.25 kHz<br>12.5 kHz<br>25 kHz | 12.5 kHz<br>25 kHz |
| Modes of Operation | Simplex, Half-Duplex | | |
| Frequency Increment | 1.25 kHz | | |
| Power Source | 10-30 VDC, Negative GND | | |
| RF Impedance | 50 Ω | | |
| Operating Temperature | -30° to + 60° C | | |
| Storage Temperature | -40° to + 85° C, 95% non-condensing RH | | |
| Operating Humidity | 5% to 95% non-condensing RH | | |
| Rx Current Drain at 25°C | DC Input 10V | DC Input 20V | DC Input 30V |
|  | 520 mA (max)<br>450 mA (typ) | 270 mA (max)<br>240 mA (typ) | 190 mA (max)<br>170 mA (typ) |
| Tx Current Drain at 25°C | Power Out    DC Input 10V | DC Input 20V | DC Input 30V |
|  | Max Pwr    5.8 A (max)<br>3.6 A (typ) | 2.5 A (max)<br>1.8 A (typ) | 1.6 A (max)<br>1.2 A (typ) |
|  | 30 dBm (1W)    1.6 A (max)<br>1.2 A (typ) | 0.8 A (max)<br>0.6 A (typ) | 0.6 A (max)<br>0.4 A (typ) |
| Cold start | 20 seconds | | |
| Nominal Dimensions | 5.50" W x 2.125" H x 4.25" D (13.97 x 5.40 x 10.8 cm) | | |
| Shipping Weight | 2.4 lbs. (1.1 Kg) | | |
| Mounting Options | Mounting plate/pattern & DIN Rail | | |
| Fan Output | 5VDC, 400mA max. | | |

| TRANSMITTER | VHF | UHF | 900 |
|---|---|---|---|
| Tx Frequencies | 136 - 174 MHz<br>215 – 240 MHz | 406.125 – 470.000 MHz,<br>450.000 - 511.975 MHz | 928 - 960 MHz |
| Carrier Output Power | 1-10 Watts<br>Adjustable | 1-10 Watts<br>Adjustable | 1-8 Watts<br>Adjustable |
| Duty Cycle | 100% (Power Foldback Allowed for High Temperatures) | | |
| Radiated Spurious Emissions | Per FCC/Regulatory | | |
| Conducted Spurious Emissions | <-65 dBc | | |
| Transmitter Stability into VSWR: | > 10:1 (Power Foldback Allowed) | | |
| RX to TX Time | < 2ms | | |
| Channel Switching Time | < 15 ms (Band-End to Band-End) | | |

| RECEIVER | VHF | UHF | | 900 |
|---|---|---|---|---|
| RX Frequencies | 136 - 174 MHz<br>215 – 240 MHz | 406.125 – 470.000 MHz,<br>450.000 - 511.975 MHz | | 928 - 960 MHz |
| | 25 kHz Channel | 12.5 KHz Channel | | 6.25 kHz Channel |
| Data Sensitivity @ $10^{-6}$ Bit Error Rate (BER) (Maximum) | **VHF/UHF**<br>-111 dBm @ 16kb/s<br>-103 dBm @ 32kb/s<br><br>**900 MHz**<br>-108 dBm @ 16kb/s<br>-101 dBm @ 32kb/s | **VHF/UHF**<br>-114 dBm @ 8kb/s<br>-106 dBm @ 16kb/s<br><br>**900 MHz**<br>-109 dBm @ 8kb/s<br>-103 dBm @ 16kb/s | | **VHF/UHF**<br>-112 dBm @ 4kb/s<br>-103 dBm @ 8kb/s |
| Data Sensitivity @ $10^{-6}$ Bit Error Rate (BER) (Typical) | **VHF/UHF**<br>-114 dBm @ 16kb/s<br>-106 dBm @ 32kb/s<br><br>**900 MHz**<br>-111 dBm @ 16kb/s<br>-104 dBm @ 32kb/s | **VHF/UHF**<br>-116 dBm @ 8kb/s<br>-109 dBm @ 16kb/s<br><br>**900 MHz**<br>-112 dBm @ 8kb/s<br>-106 dBm @ 16kb/s | | **VHF/UHF**<br>-115 dBm @ 4kb/s<br>-106 dBm @ 8kb/s |
| Adjacent Channel Rejection | **VHF/UHF**<br>> 75 dB<br><br>**900 MHz/ VHF 200**<br>> 70 dB | **VHF/UHF**<br>> 60 dB<br><br>**900 MHz**<br>> 60 dB | | **VHF/UHF**<br>> 45 dB |
| Spurious Response Rejection | > 75 dB | | | |
| Intermodulation Rejection | > 75 dB | | | |
| TX to RX Time | < 1ms | | | |
| Channel Switching Time | < 15ms (Band-End to Band-End) | | | |
| Receive Input Power | 17 dBm (50mW) max. | | | |

| MODEM/LOGIC | 25 kHz Channel | 12.5 KHz Channel | 6.25 kHz Channel |
|---|---|---|---|
| Data Rate (Selectable) | 16 kbps, 32 kbps | 8 kbps, 16 kbps | 4 kbps, 8 kbps |
| Modulation Type | 2FSK, 4FSK | | |
| Addressing | IP | | |

| SETUP and COM Port | |
|---|---|
| Interface | EIA-232F DCE |
| Data Rate | Setup Port: 300 – 19,200 bps (Default: 19.2 Kbps)<br>Com Port: 300 – 115,200 bps (Default: 9.6 Kbps) |

| Display | |
|---|---|
| 5 Tri-color status LEDs | Power, Status, Activity, Link, Rx/Tx |

| Connectors | | |
|---|---|---|
| Antenna Connector | TNC female (Tx/Rx) | |
| Serial Setup Port | DE-9F | |
| Serial Terminal Server | DE-9F | |
| Ethernet RJ-45 | 10 BaseT auto-MDIX | |
| Power - I/O | Power Header | Power Plug |
| | DRL p/n 415-7108-113 (Weidmüller p/n 1615550000) 4 Pin, 3.5mm, Power Header | DRL p/n 897-5008-010 (Weidmüller p/n 1639260000) 4 Pin, 3.5mm, Power Plug Cable: 60 inches Connections: Fan Output, Ground, Power, Enable |

| Diagnostics | |
|---|---|
| Message elements | Temperature, Voltage, Local RSSI, Remote RSSI, Forward Power, Reverse Power, Packet Error Rate |

| FCC / IC / UL Certifications | | | |
|---|---|---|---|
| | FCC | IC (DOC) | UL |
| 136 – 174 MHz | NP4-5018-500 | 773B-5018500 | Pending |
| 216 - 222 MHz | NP4-5028-502 | 773B-5028502 | Pending |
| 406.1 - 512 MHz | NP4-5048-300 | 773B-5048300 | Pending |
| 928 - 960 MHz | NP4-5098-500 | 773B-5098500 | Pending |

CalAmp warrants to the original purchaser for use ("Buyer") that data telemetry products manufactured by DRL ("Products") are free from defects in material and workmanship and will conform to DRL's published technical specifications for a period of, except as noted below, two (2) years from the date of shipment to Buyer. DRL makes no warranty with respect to any equipment not manufactured by DRL, and any such equipment shall carry the original equipment manufacturer's warranty only. DRL further makes no warranty as to and specifically disclaims liability for, availability, range, coverage, grade of service or operation of the repeater system provided by the carrier or repeater operator. Any return shipping charges for third party equipment to their respective repair facilities are chargeable and will be passed on to the Buyer.

If any Product fails to meet the warranty set forth above during the applicable warranty period and is returned to a location designated by DRL. DRL, at its option, shall either repair or replace such defective Product, directly or through an authorized service agent, within thirty (30) days of receipt of same. No Products may be returned without prior authorization from DRL. Any repaired or replaced Products shall be warranted for the remainder of the original warranty period. Buyer shall pay all shipping charges, handling charges, fees and duties for returning defective Products to DRL or DRL's authorized service agent. DRL will pay the return shipping charges if the Product is repaired or replaced under warranty, exclusive of fees and duties. Repair or replacement of defective Products as set forth in this paragraph fulfills any and all warranty obligations on the part of DRL.

This warranty is void and DRL shall not be obligated to replace or repair any Products if (i) the Product has been used in other than its normal and customary manner; (ii) the Product has been subject to misuse, accident, neglect or damage or has been used other than with DRL approved accessories and equipment; (iii) unauthorized alteration or repairs have been made or unapproved parts have been used in or with the Product; or (iv) Buyer failed to notify DRL or DRL's authorized service agent of the defect during the applicable warranty period. DRL is the final arbiter of such claims.

THE AFORESAID WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED AND IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. DRL AND BUYER AGREE THAT BUYER'S EXCLUSIVE REMEDY FOR ANY BREACH OF ANY OF SAID WARRANTIES IT AS SET FORTH ABOVE. BUYER AGREES THAT IN NO EVENT SHALL DRL BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT OR EXEMPLARY DAMAGES WHETHER ON THE BASIS OF NEGLIGENCE, STRICT LIABILITY OR OTHERWISE. The purpose of the exclusive remedies set forth above shall be to provide Buyer with repair or replacement of non-complying Products in the manner provided above. These exclusive remedies shall not be deemed to have failed of their essential purpose so long as DRL is willing and able to repair or replace non-complying Products in the manner set forth above.

This warranty applies to all Products sold worldwide. Some states do not allow limitations on implied warranties so the above limitations may not be applicable. You may also have other rights, which vary from state to state.

EXCEPTIONS

ONE YEAR:       Labor to replace defective parts in repeaters or base stations
THIRTY DAY:     Tuning and adjustment of telemetry radios
NO WARRANTY:  Fuses, lamps and other expendable parts

**Access Point**. Communication hub for users to connect to a LAN. Access Points are important for providing heightened wireless security and for extending the physical range of wireless service accessibility

**Airlink**. Physical radio frequency connections used for communications between units

**ARP**. Address Resolution Protocol – Maps Internet address to physical address

**Backbone**. The part of a network connecting of the bulk of the systems and networks together - handling the most data

**Bandwidth**. The transmission capacity of a given device or network

**Browser**. An application program providing the interface to view and interact with all the information on the World Wide Web

**COM Port**. Both RS-232 serial communications ports of the ViPR wireless radio modem. Configured as DCE and designed to connect directly to a DTE

**Default Gateway**. A device forwarding Internet traffic from your local area network

**DCE (Data Communications Equipment)**. This designation is applied to equipment like modems. DCE is designed to connect to DTE

**DHCP (Dynamic Host Configuration Protocol)**. A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses

**DNS (Domain Name Server)**. Translates the domain name into an IP address

**Domain**. A specific name for a network of computers

**DTE (Data Terminal Equipment)**. This designation is applied to equipment such as terminals, PCs, RTUs, PLCs, etc. DTE is designed to connect to DCE

**Dynamic IP Address**. A temporary IP address assigned by a DHCP server

**Ethernet**. IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium

**Firewall**. A set of related programs located at a network gateway server that protects the resources of a network from users on other networks

**Firmware**. The embedded programming code running a networking device

**Fragmentation**. Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet

**FTP (File Transfer Protocol)**. A protocol used to transfer files over a TCP/IP network

**Gateway**. A device interconnecting networks with different, incompatible communications protocols

**HDX (Half Duplex)**. Data transmission occurring in two directions over a single line, using separate Tx and Rx frequencies, but only *one direction at a time*

**HTTP (HyperText Transport Protocol)**. Communications protocol used to connect to servers on the World Wide Web

**IPCONFIG**. A Windows 2000 and XP utility that displays the IP address for a particular networking device

**MAC (Media Access Control)**. The unique address a manufacturer assigns to each networking device

**MTU (Maximum Transmission Unit)** The largest TCP/IP packet hardware can carry

**NAT (Network Address Translation)**. NAT technology translates IP addresses of a local area network to a different IP address for the Internet

**Network**. A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users

**Network speed**. Bit rate on the RF link between units in a network

**Node**. A network junction or connection point, typically a computer or work station

**OIP (Optimized IP)**. Compresses TCP and UDP headers, and filters unnecessary

acknowledgments. OIP makes the most use of the available bandwidth

**OTA (Over the Air)**. Standard for the transmission and reception of application-related information in a wireless communications system

**PHY**. A PHY chip (called PHYceiver) provides the interface to Ethernet transmission medium. Its purpose is digital access of the modulated link (usually used together with an MII-chip). The PHY defines data rates and transmission method parameters

**Ping (Packet Internet Groper)**. An Internet utility used to determine whether a particular IP address is online

**PLC (Programmable Logic Controller)**. An intelligent device that can make decisions, gather and report information, and control other devices

**RIPv2**. Dynamic IP routing protocol based on the distance vector algorithm

**Router**. A networking device connecting multiple networks

**RS-232**. Industry–standard interface for data transfer

**RTU (Remote Terminal Unit)**. A SCADA device used to gather information or control other devices

**SCADA (Supervisory Control And Data Acquisition)**. A general term referring to systems gathering data and/or performing control operations

**SNTP (Simple Network Time Protocol)** Protocol for synchronizing clocks of computer systems over packet-switched, variable-latency data networks. Uses UDP as its transport layer

**Static IP Address**. A fixed address assigned to a computer or device connected to a network

**Static Routing**. Forwarding data in a network via a fixed path

**Subnet Mask**. An Ethernet address code determining network size

**Switch**. A device connecting computing devices to host computers, allowing a large number of devices to share a limited number of ports

**TCP (Transmission Control Protocol)**. A network protocol for transmitting data that requires acknowledgement from the recipient of data sent

**TCP/IP (Transmission Control Protocol/Internet Protocol)**. A set of protocols for network communications

**Telnet**. User command and TCP/IP protocol used for accessing remote PCs

**TFTP (Trivial File Transfer Protocol)**. UDP/IP based file transfer protocol

**Topology**. The physical layout of a network

**Transparent**. Device capable of transmitting all data without regard to special characters, etc

**Terminal Server**. Acts as a converter between Ethernet/IP and RS-232 protocols

**UDP (User Datagram Protocol)**. Network protocol for transmitting data that does not require acknowledgement from the recipient of the sent data

**Upgrade**. To replace existing software or firmware with a newer version

**URL (Universal Resource Locator)**. The address of a file located on the Internet

**About CalAmp**

CalAmp is a leading provider of wireless communications products that enable anytime/anywhere access to critical information, data and entertainment content. With comprehensive capabilities ranging from product design and development through volume production, CalAmp delivers cost-effective high quality solutions to a broad array of customers and end markets.  CalAmp is the leading supplier of Direct Broadcast Satellite (DBS) outdoor customer premise equipment to the U.S. satellite television market.  The Company also provides wireless data communication solutions for the telemetry and asset tracking markets, private wireless networks, public safety communications and critical infrastructure and process control applications.  For additional information, please visit the Company's website at www.calamp.com.